Enterprise Network Devices

INFO-6078 – Managing Enterprise Networks

FANSHAWE

Representing Network Devices

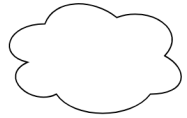
Hub

Switch

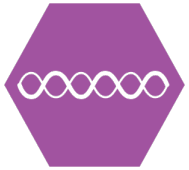
Layer 3 Switch

Modem

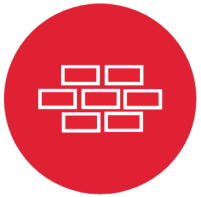
Router



WAN Connection



Wireless Access Point



Firewall

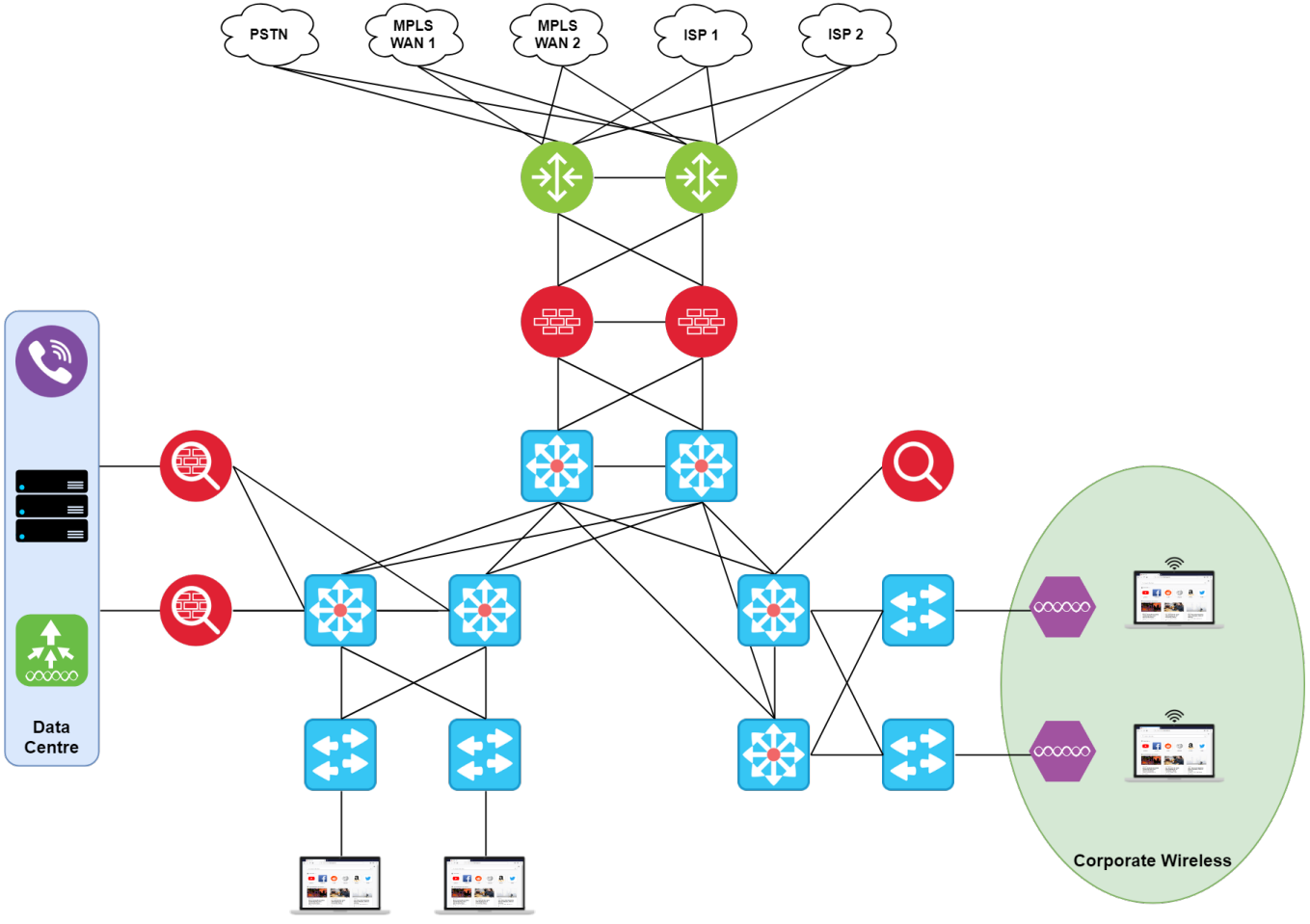
Intrusion Detection System

Intrusion Prevention System

Proxy Server

Media Converter

Representing Networks



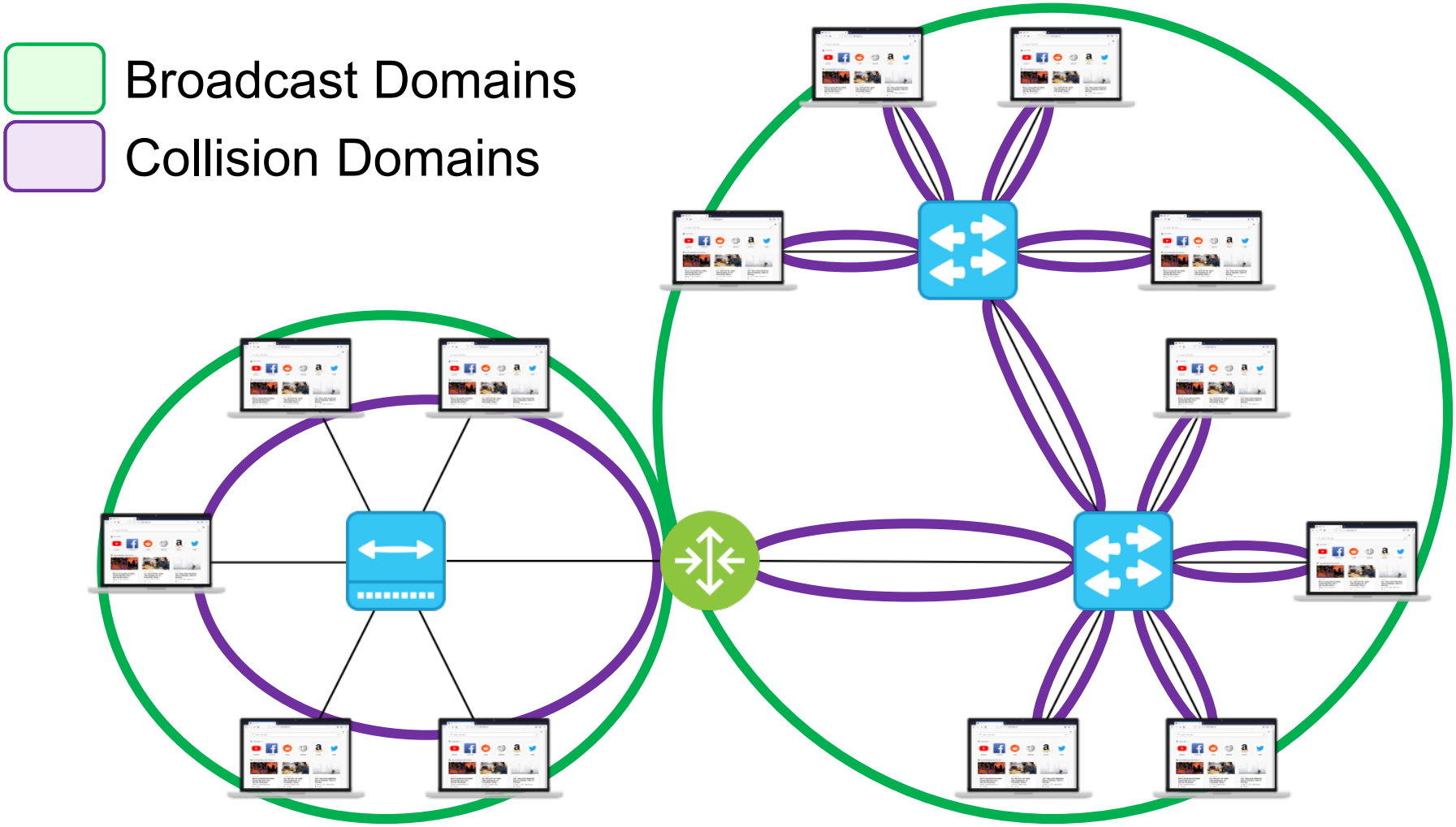
Broadcast & Collision Domains

- **Broadcast Domain**
  - A logical division of a network where all devices can reach each other using a layer 2 broadcast frame
  - Broadcast domains are only separated by layer 3 devices, such as a layer 3 switch setup with inter-VLAN routing or a router
  - When utilizing VLANs, each VLAN is a separate broadcast domain
- **Broadcast Domain Control**
  - By taking advantage of a private VLAN, broadcast domains can be strictly controlled, where broadcasts are only forwarded if sent by specific devices

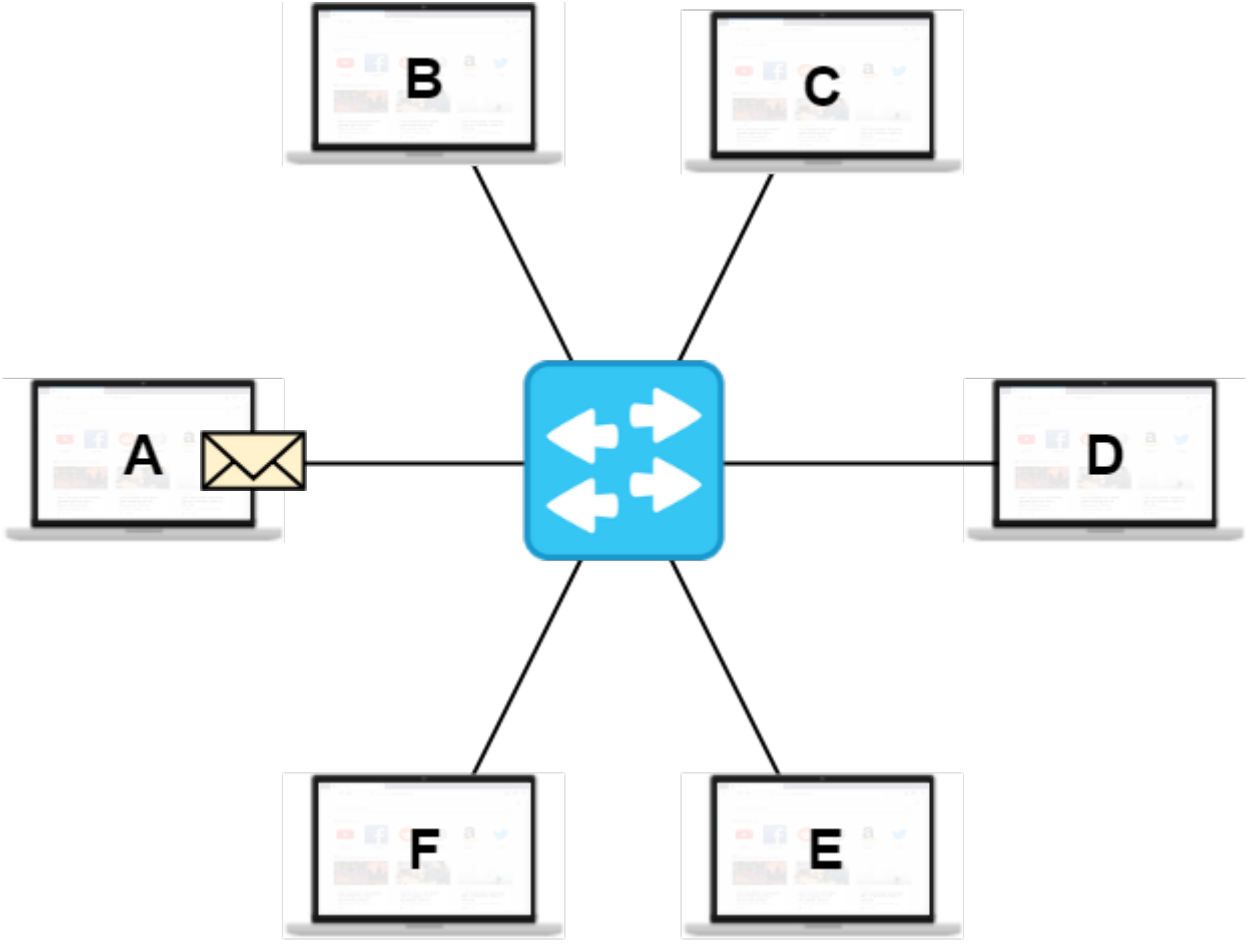
Broadcast & Collision Domains

- **Collision Domain**
  - A network segment where devices can transmit at the same time and cause a data collision
  - Devices are generally connected with a shared media or through a repeater
  - A wireless network (SSID) operates within a single collision domain
  - Carrier sense multiple access with collision avoidance (CSMA/CA) is required for operation

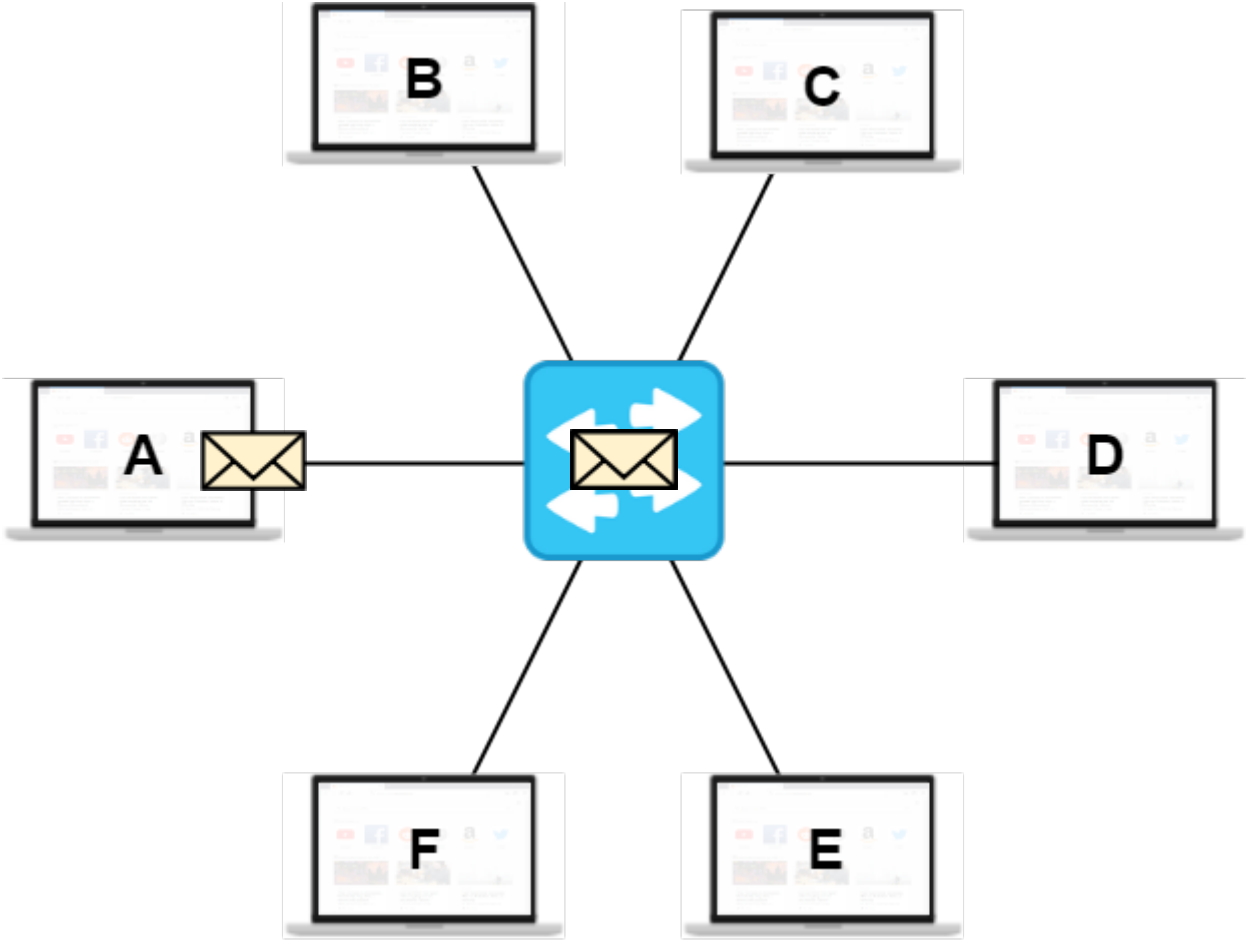
Broadcast & Collision Domains



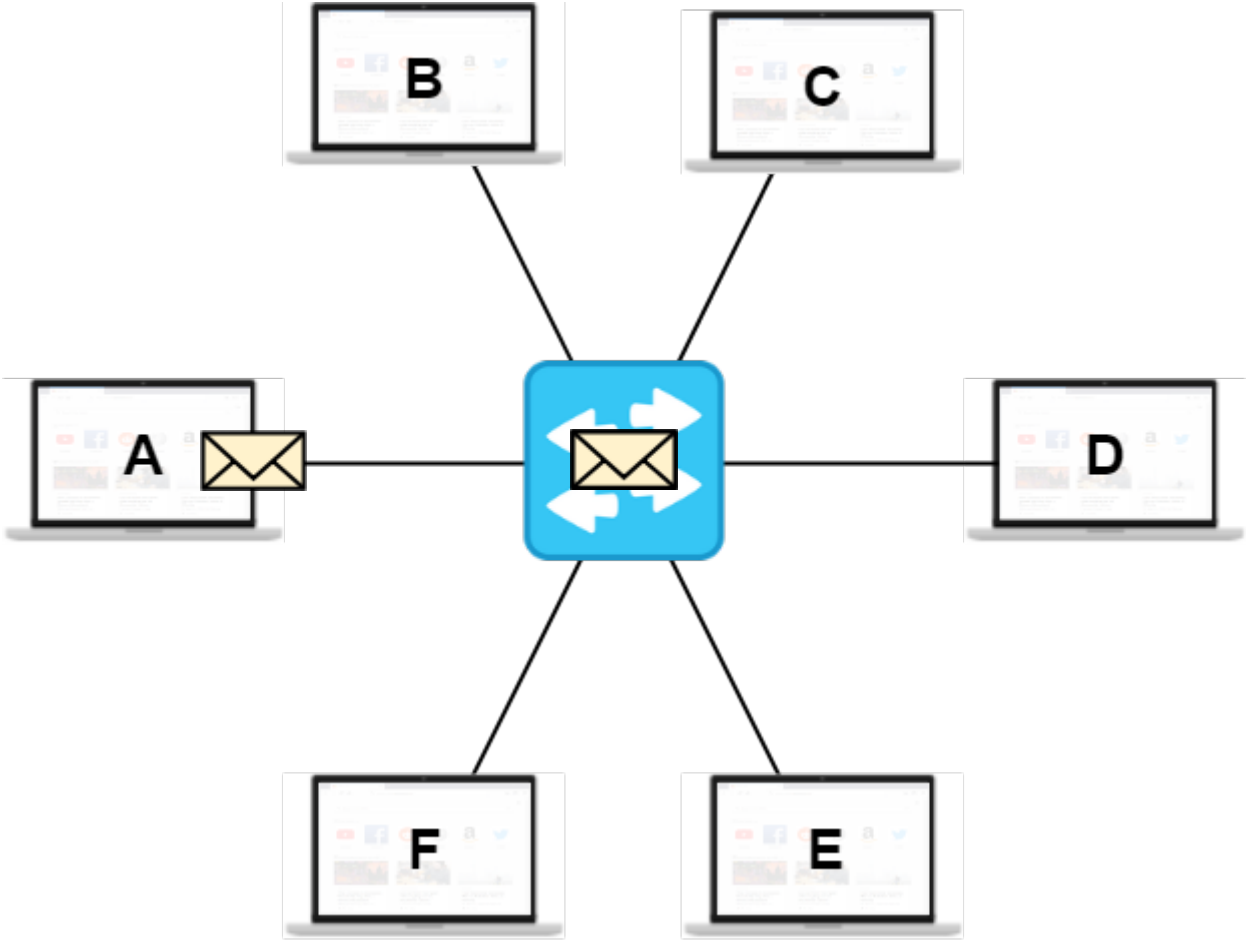
Transmission Types – Unicast



Transmission Types – Broadcast



Transmission Types – Multicast



Transmission Types – Multicast

- A multicast address is a logical address assigned to a host that should process traffic destined to only the members of the multicast group
- Multicast hosts do no need to exist in the same subnet
- IPv4 multicast address range from 224.0.0.0-239.255.255.255; however, only addresses in the range 239.0.0.0-239.255.255.255 can be used without prior authorization from IANA

Transmission Types – Multicast

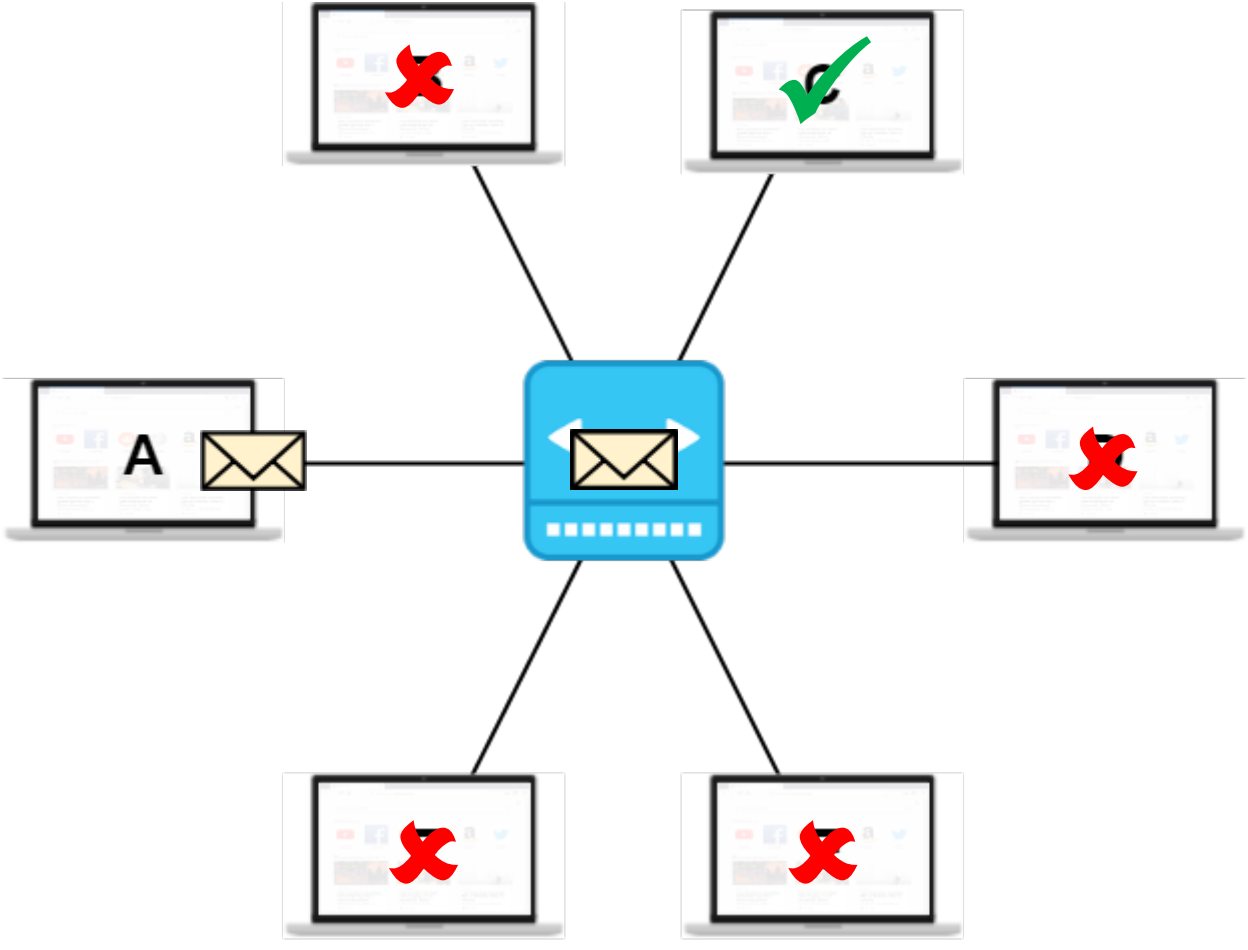
- IPv6 multicast addresses fall with the range FF00::/8, with specific scopes intended for specific purposes

Name	Prefix	Scope
Interface-Local	FF01	Spans a single interface. Useful only for loopback traffic
Link-Local	FF02	Spans the local link (LAN)
Admin-Local	FF04	Administratively configured
Site-Local	FF05	Spans a single site
Organization-Local	FF08	Spans multiple sites within an organization
Global scope	FF0E	Assigned by IANA. Globally relevent

Hub (Multiport Repeater)

- Simplest of all infrastructure devices
- Operates at layer 1 of the OSI Model
- Floods all received bits to all ports except the ingress port
- Increase the size of the collision domain
- Usually limited to 100 Mbps
- Operate in half-duplex mode
- Connects devices in a star topology
- Depreciated by IEEE 802.3

Hub (Multiport Repeater)



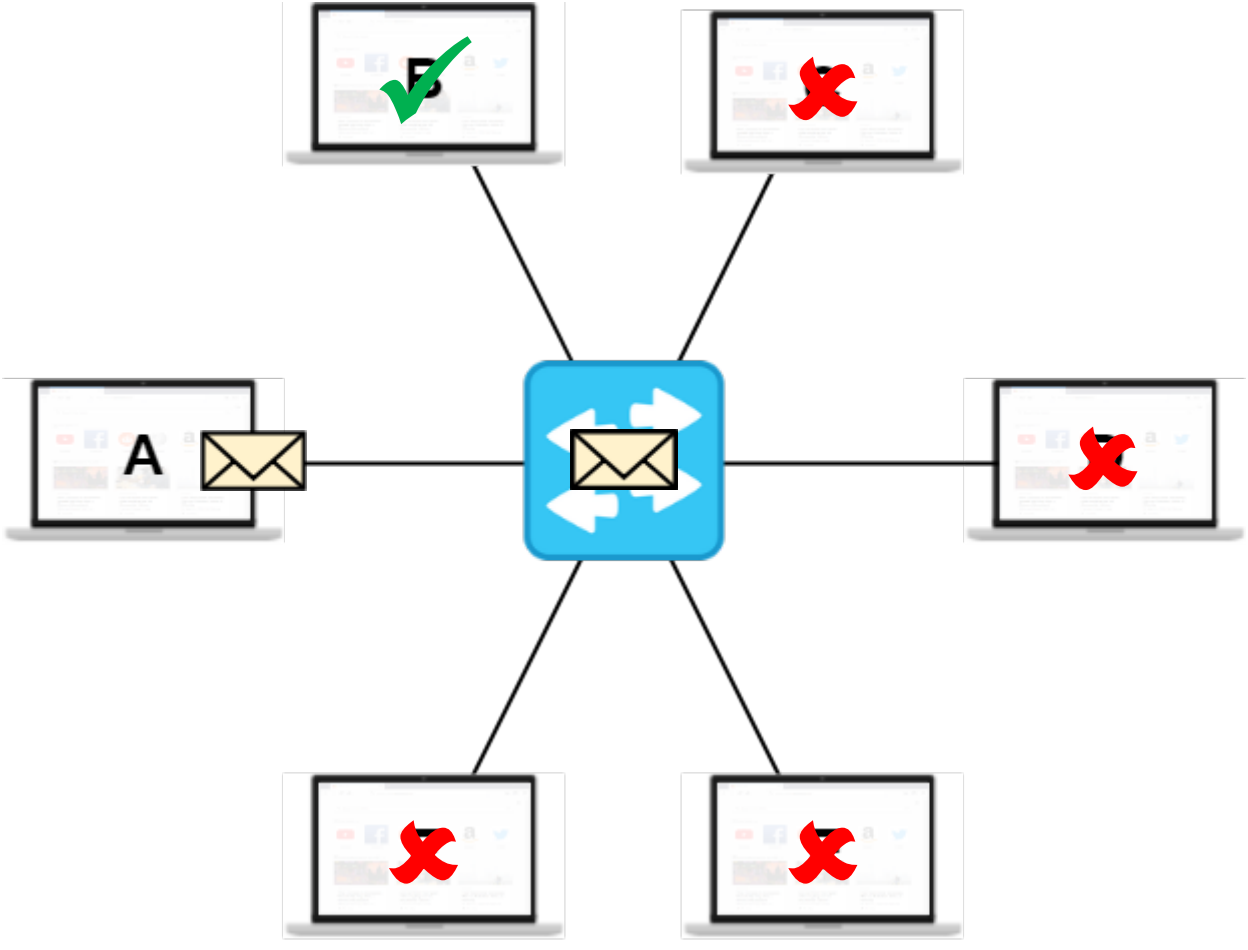
Switch

- Most common network device found in organizations
- A switch includes high-density ports to connect devices to the LAN
- Operates at layer 2 of the OSI model and can learn the MAC address of connected devices
- Can perform one of three actions on a frame that is received: flood, forward or filter

Switch

- Operates in full-duplex mode by default
- Each port of a switch operates with a single collision domain, but a switch is used to extend the reach of a broadcast domain
- Switches utilize application specific integrated circuits (ASICs) to make forwarding decisions
- Often combined with power deliver technologies, such as Power over Ethernet (PoE) to provide both a network connection and power to end devices such as wireless access points or voice over IP (VoIP) phones

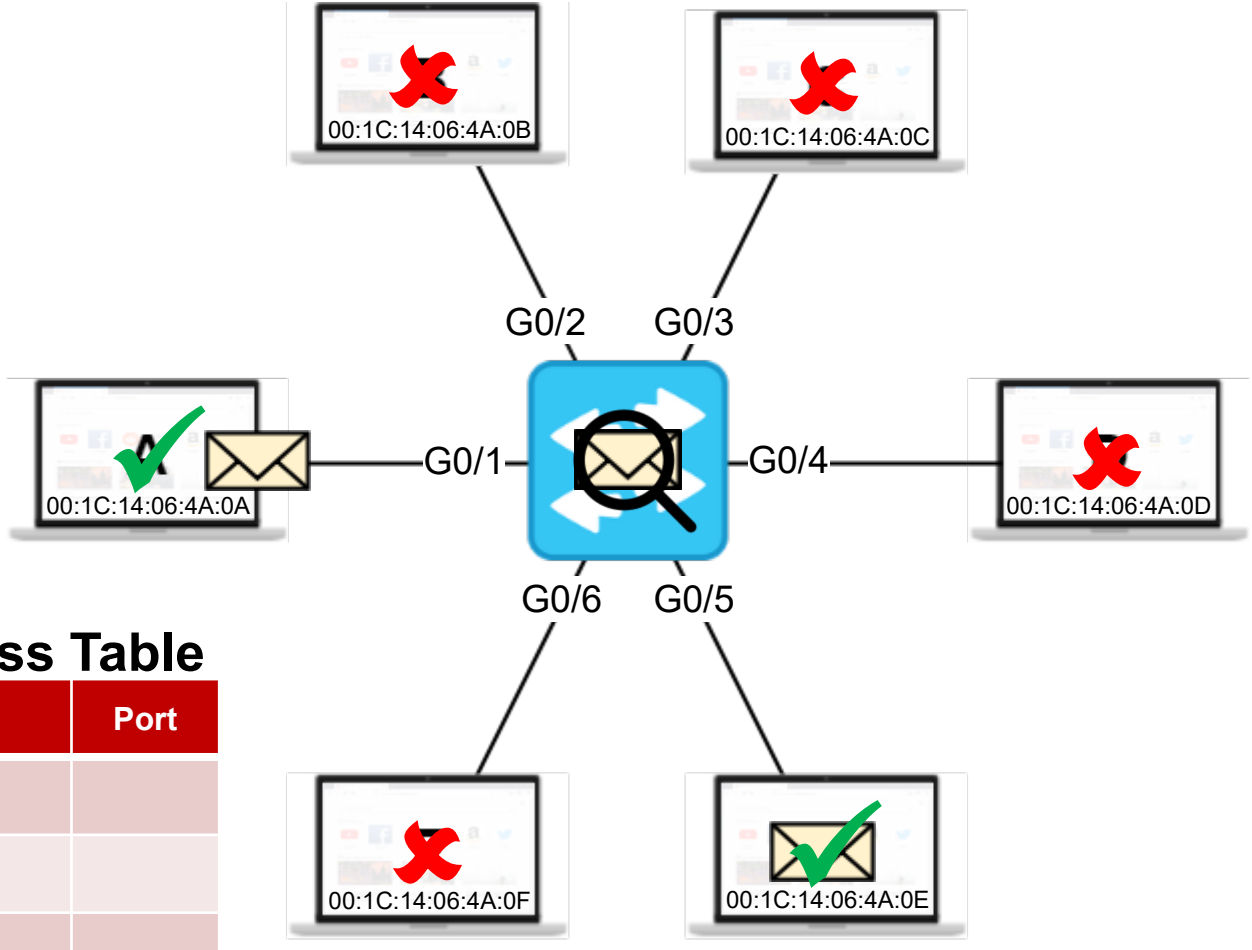
Switch - Flood



Switch – MAC Address Table

- Learning the MAC address of connected devices allows a switch to filter traffic and deliver it only to the appropriate destination
- MAC addresses and VLAN mappings are stored in the MAC Address table, located in random access memory (RAM)
- The MAC Address table is populated by reading the source MAC address of frames that the switch receives
- If a MAC address is not found in the table, the switch will flood the frame out all ports except the ingress port, much like a hub
- MAC addresses will be aged out of the table based on a user configurable value

Switch – MAC Address Table



MAC Address Table

MAC Address	Port

Switch – VLANs

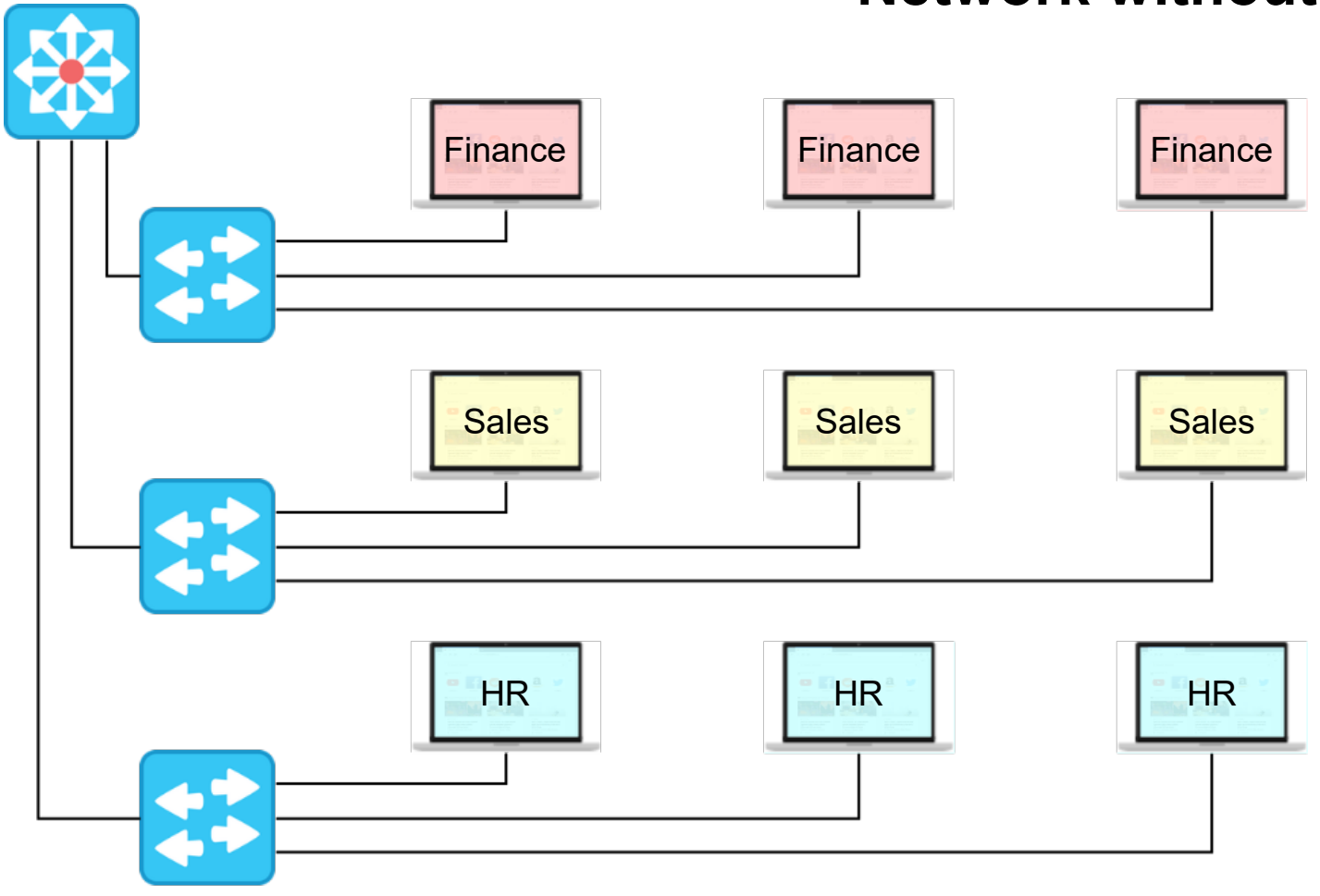
- A virtual local area network (VLAN) is a network segment that is isolated from other network segments at layer 2 of the OSI model
- VLAN are an abstraction layer applied to switches, and allow a single switch to participate in multiple logical network segments
- Additionally, multiple switches can work to group hosts into a single VLAN even if those hosts are connected to different switches

Switch – VLANs

- VLANs allow network administrators to prevent devices connected to the same switch from communicating, improving security, traffic management and simplicity
- VLANs utilize trunk links to aggregate traffic between network devices
- Utilizing a 4-byte 802.1Q VLAN tag, 4,094 individual VLANs can be created to segment traffic
- VLANs can be classified as end-to-end, or local
- In modern networks, local VLANs are used

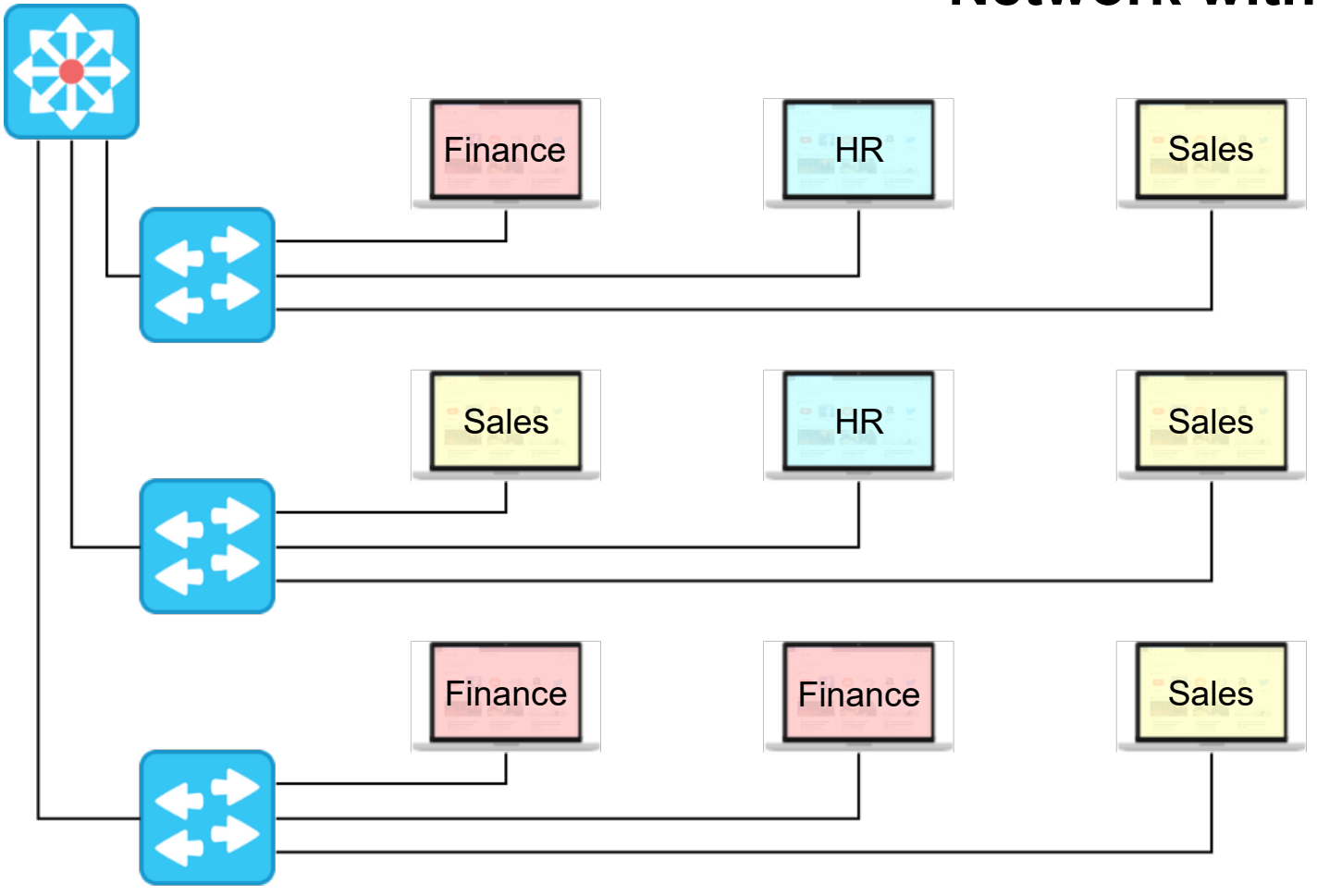
Switch – VLANS

Network without VLANs



Switch – VLANS

Network with VLANs



Switch – VLANs

- A number of VLAN types exist to support different needs:
  - **Data**
    - Configured to segregate user traffic into manageable groups
  - **Voice**
    - Configured to carry voice traffic
    - Usually given priority over other traffic types
  - **Default**
    - The VLAN that all ports are assigned to on a new unconfigured switch
    - Use of the default VLAN is not recommended in a production environment

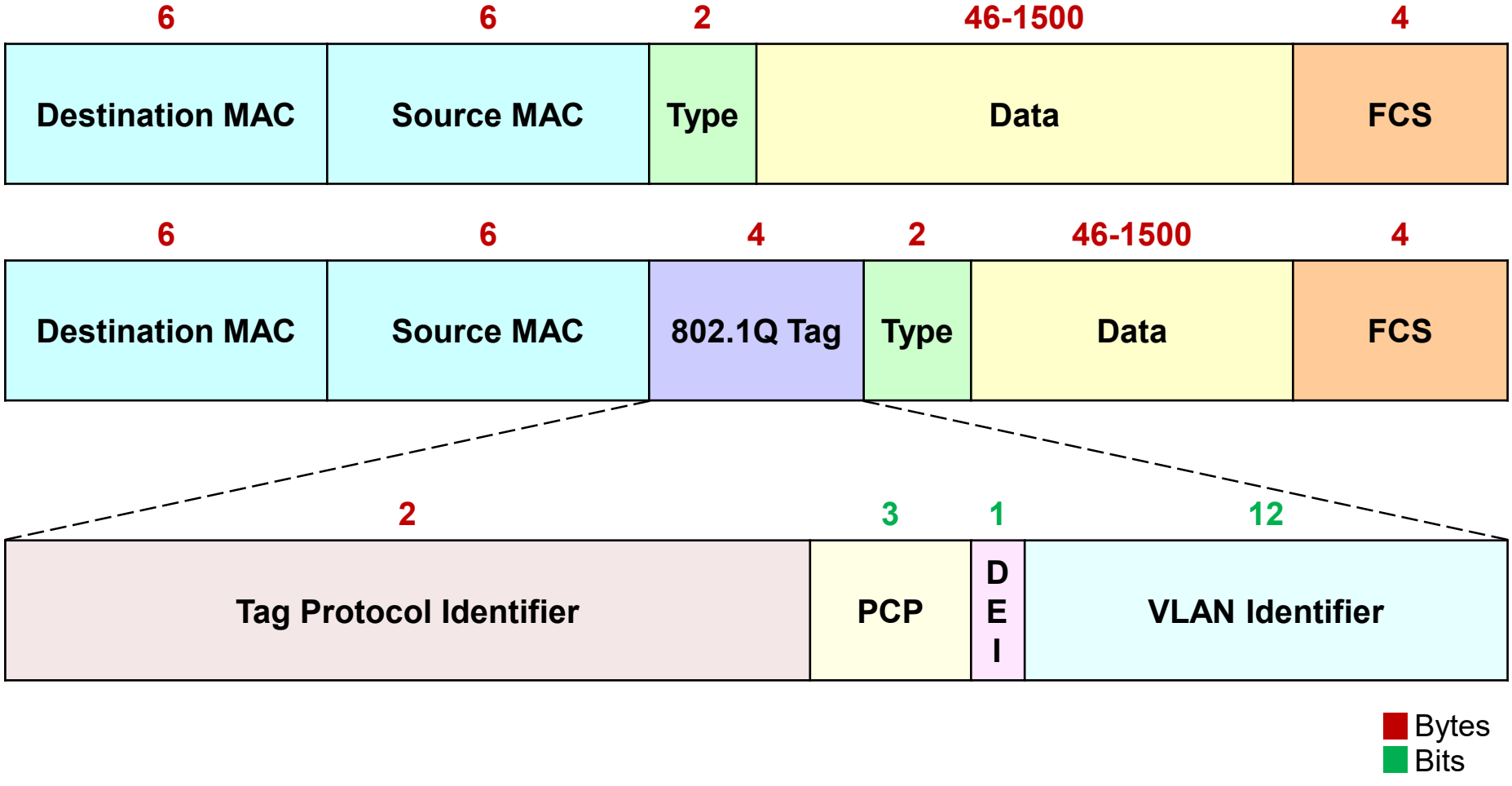
Switch – VLANs

- **Native**
  - Assigned to an 802.1Q trunk port
  - Represents untagged traffic that is received
- **Management**
  - Used to provide a segregated management subnet for network devices
- **Private**
  - Also known as port isolation
  - Prevents intra-VLAN communication except with a pre-defined uplink

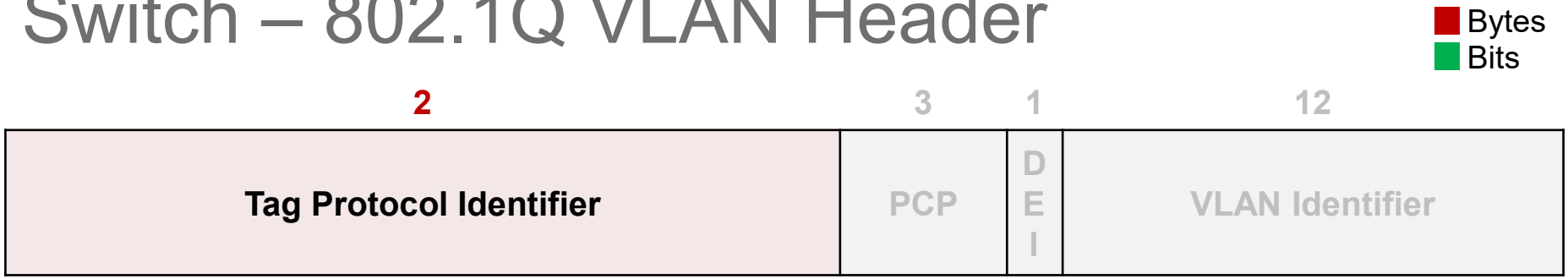
Switch – 802.1Q VLAN Header

- 802.1Q is a subset of the IEEE 802.1 working group
- Network devices use tagging to enable VLANs on a network
- When a frame enters a VLAN-aware network segment, an 802.1Q VLAN tag is added to the frame
- The 4 byte VLAN tag is inserted into the ethernet header between the source MAC and type fields
- If a frame in the VLAN-aware segment does not include a tag, it is considered to be a part of the native VLAN

Switch – 802.1Q VLAN Header

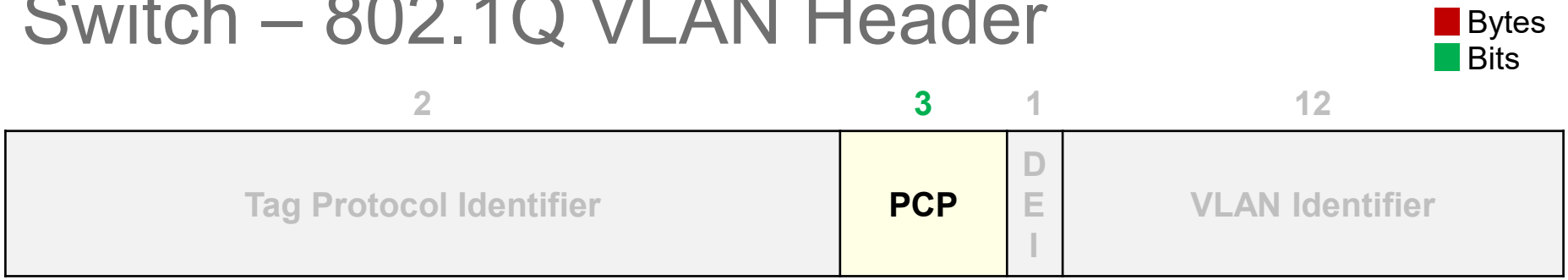


Switch – 802.1Q VLAN Header



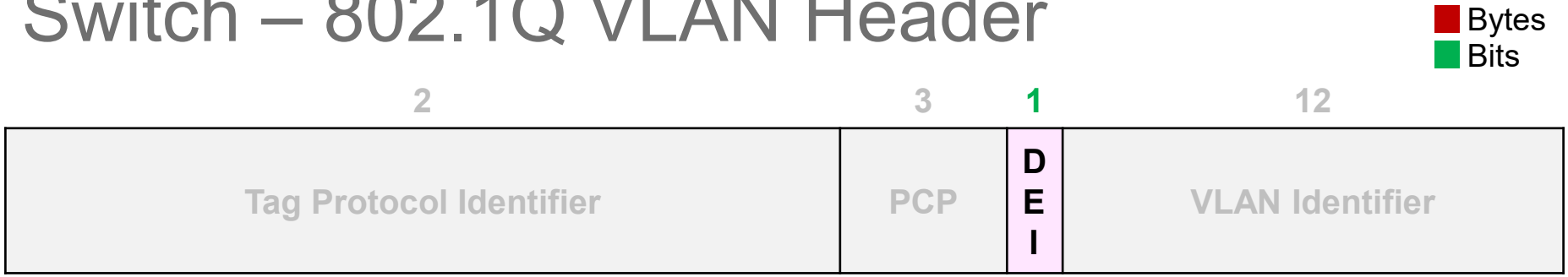
- **Tag Protocol Identifier**
  - The value 0x8100 used to identify a 802.1Q tagged frame
  - Located in the same position as the type field in an Ethernet frame

Switch – 802.1Q VLAN Header



- **Priority Code Point (PCP)**
  - Represents the 802.1p class of service
  - Possible values range from 0-8
  - Used to prioritize traffic at layer 2

Switch – 802.1Q VLAN Header



- **Drop Eligible Indicator (DEI) - formerly CFI**
  - Used to indicate a frame is eligible to be dropped when congestion is present
  - May me used alone, or in conjunction with PCP

Switch – 802.1Q VLAN Header

- **VLAN Identifier**
  - Represents the VLAN that the frame belongs to
  - Valid VLAN IDs range from 1-4094
  - The values 0x000 and 0xFFF are reserved

Switch – Port Types

- Switch port operate in one of three modes:
- **Access**
  - Connects to a single network device such as a server, printer, IP phone, etc.
  - Interface belongs to a single VLAN
- **Trunk**
  - Connects to other switches or routing devices
  - Frames from multiple VLANs are multiplexed and sent across the link

Switch – Port Types

- Switches read the frames VLAN ID tag to determine source and destination

- **Tagged**
  - The switch accepts tagged frames from one access device
  - Typically used to connect to servers running virtual machines
  - Cisco devices do not support interfaces in tagged mode

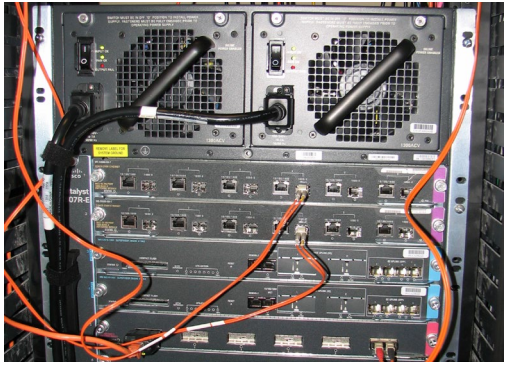
Switch - Configurations

- Switches are available in a variety of configurations that can be suited to their intended purpose:
- **Fixed**
  - Often the most cost effective option
  - Have a pre-determined port density
  - Typically not expandable
- **Stackable**
  - A cost friendly option
  - Each device has a pre-determined post density
  - Multiple devices can be configured to operate as a single device

Switch - Configurations

- When arranged in a stacked configuration, high-throughput interfaces connect the device to other switches in the stack

- **Modular**
  - Usually the most cost restrictive option
  - Allows for the addition of expansion modules to allow mode port density/faster interfaces to be added at a later date
  - Other application specific modules can also be added to the switch (firewall, wireless, network analysis)



Switch – Forwarding Methods

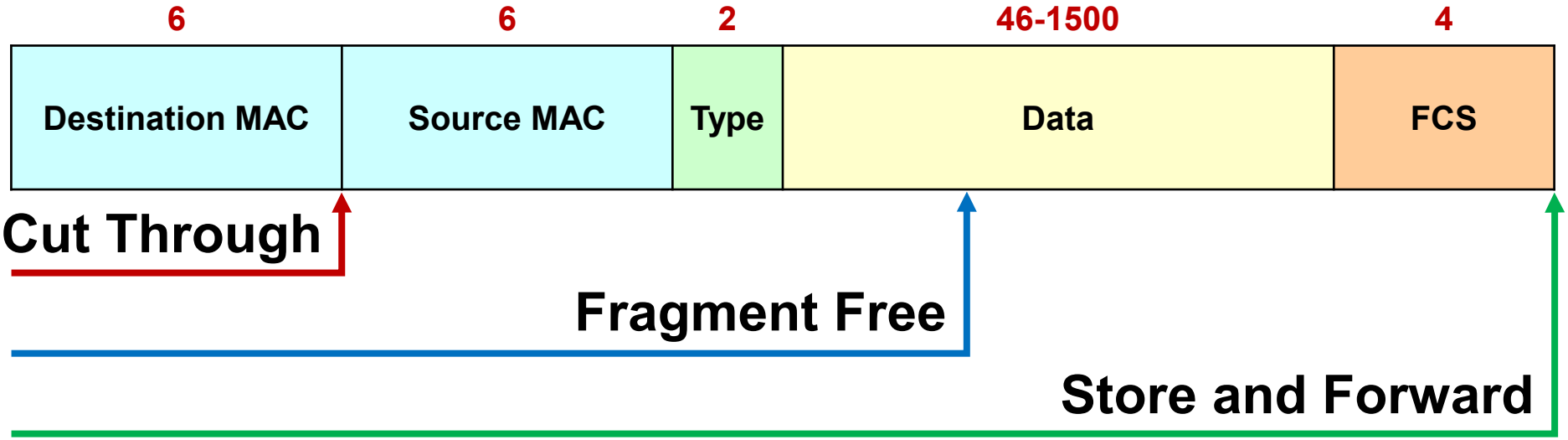
- Switches provide low latency forwarding of frames, but this latency varies based on the forwarding method in operation:
- **Store & Forward**
  - The default mode for most devices
  - Frames are buffered and checked for errors or corruption
  - If the frame passes the check, it is forwarded to the destination
  - If the frame is corrupt, it is discarded
  - Does not forward corrupt frames across the network, but incurs the most latency

Switch – Forwarding Methods

- **Fragment Free**
  - The first 64 bytes are buffered and checked for consistency
  - After the first 64 bytes are buffered, the switch forwards the frame to the destination
  - Ensures that collision fragments are not forwarded across the network, but could forward other corrupted frames
  - Incurs moderate latency
- **Cut-Through**
  - The switch reads the frame until it know the destination MAC address, then forward the frame to the destination

Switch – Forwarding Methods

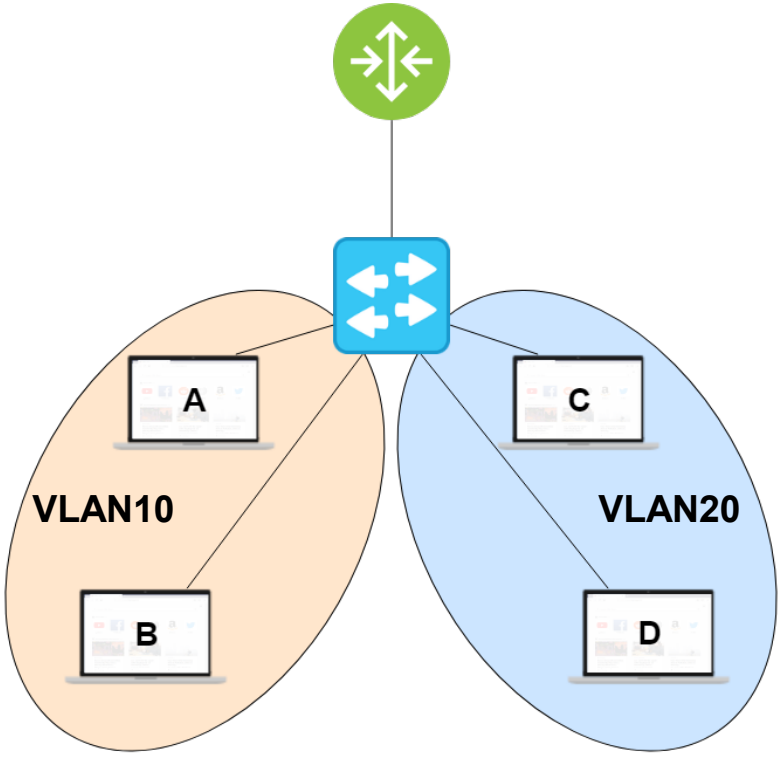
- Will forward collision fragments and other corrupted frames across the network
- Incurs the least amount of latency

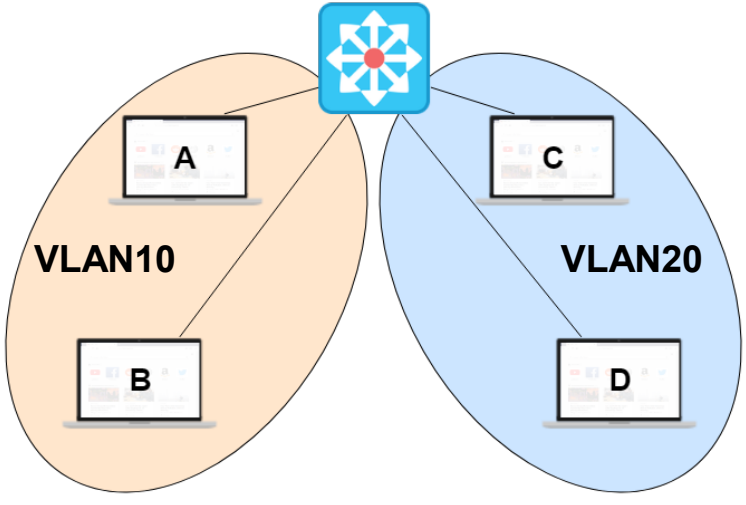


Layer 3 Switch

- A Layer 3 (multilayer) switch combines the high-speed switching capability of a layer 2 switch with additional functionality at layers 3 and 4 of the OSI model
- Layer 3 switches are capable of moving packets between subnets
- They can normally reduce latency in a network by reducing the distance to a routing device

Layer 3 Switch

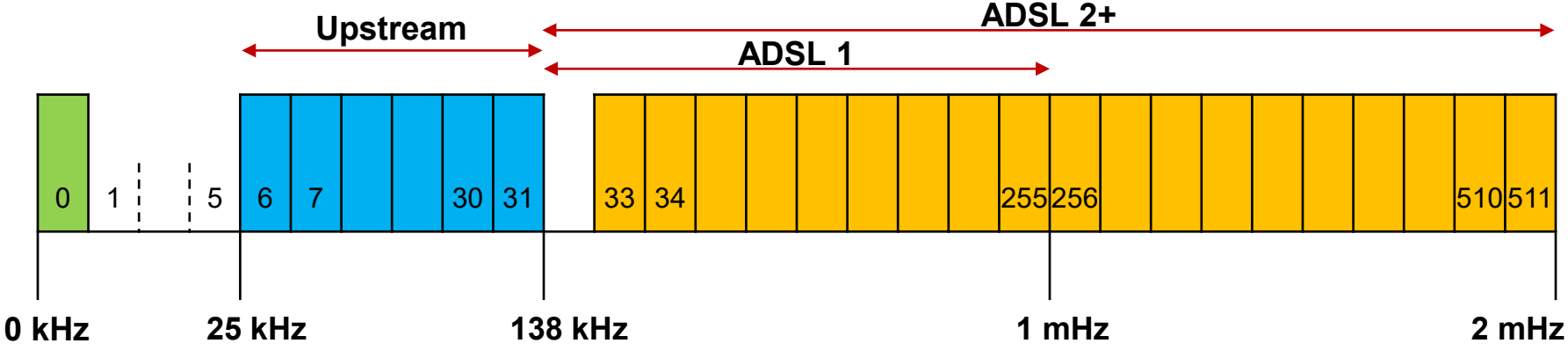




FANSHAWE

Modem

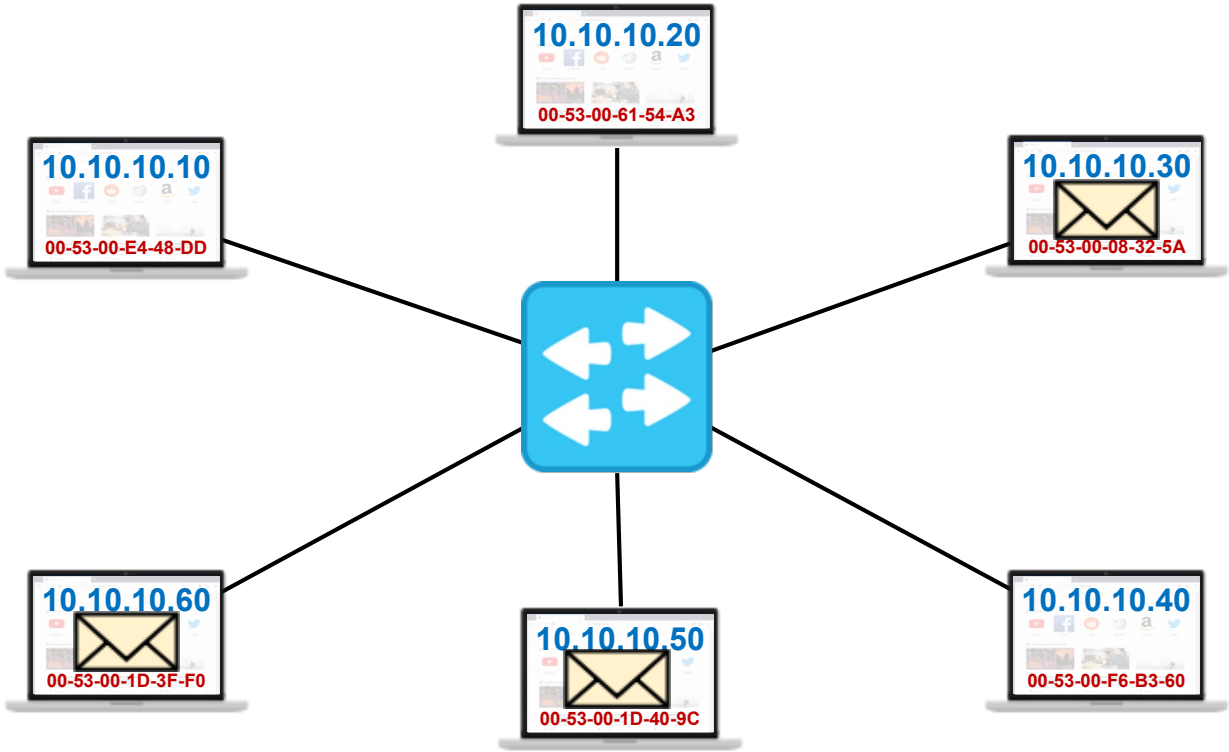
- Classically, a modem (modulator-demodulator) was a hardware device used to connect computers to networks by transmitting audio signals over telephones lines
- More modern references to the term modem describe digital subscriber line (DSL) modems, a device that connects to the phone line and utilizes the unused spectrum in the 25 kHz to 2+ mHz range in channels that are 4 kHz wide



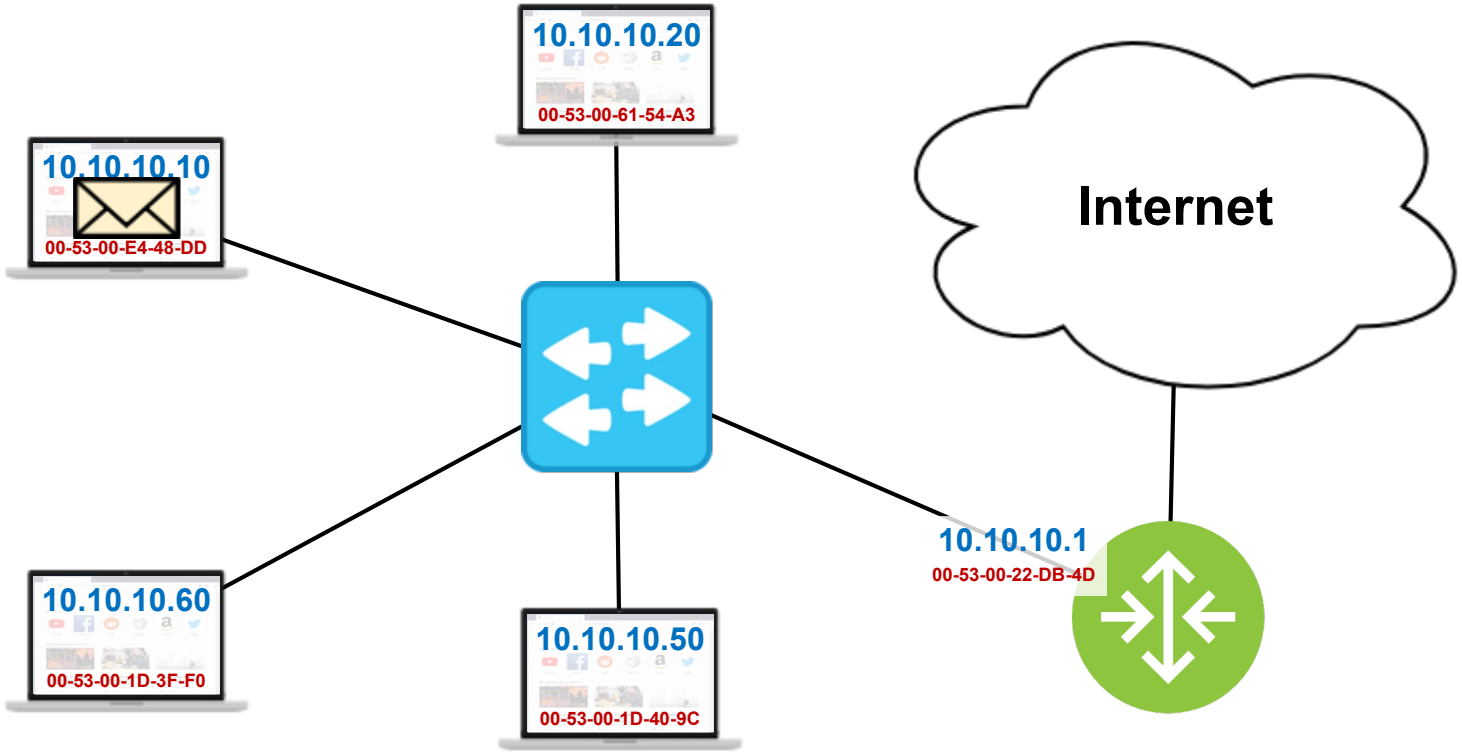
Router

- Routers operate at layer 3 of the OSI model
- When used in interconnected networks, routers can share path and availability information about destinations by means of dynamic routing protocols such as OSPF, BGP, RIP, EIGRP and ISIS
- Based on information learned from dynamic routing protocols and routes manually programmed by administrators, routers build a table of preferred paths to available destinations called the routing table

Router – Message Delivery – LAN



Router – Message Delivery – Remote



Router

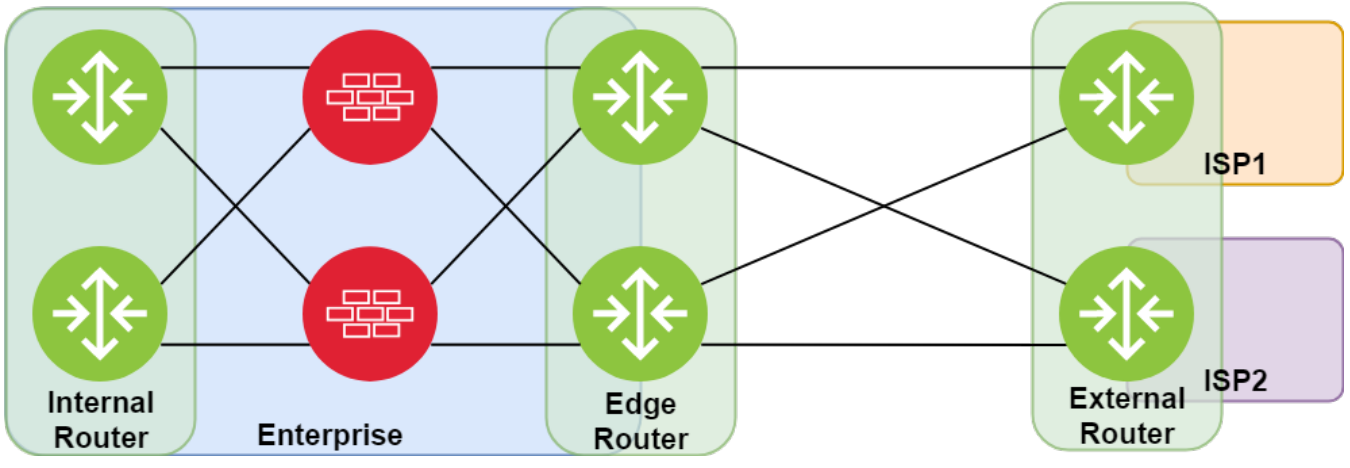
- **Static Routing**
  - Static routes are manually defined routes to a destination and configured by an administrator
  - Static routing is useful in environments where only a small number of routes are required as long as the routes do not frequently change
  - Often used in Stub networks
- **Default Route**
  - A default route is used to forward traffic when a more specific destination is not available
  - An interface that connects to the internet is often the exit interface for default routes
- **Dynamic Routing**
  - Dynamic routing protocols exchange destination information with peer routers running the same protocol

Router – Integrated Service Router

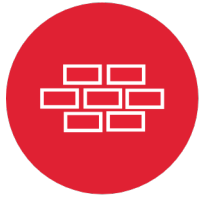
- An integrated service router (ISR) combines the functions of a router with additional capabilities normally provided by a device such as a switch or a firewall into a single device

Router – Router Locations

- Routers have different labels based on their location in relevance to an organization:
  - **Interior** – A router located internally within a company's infrastructure
  - **Exterior** – A router located on the internet
  - **Border/Edge** - A router that connects the internal network to an WAN/the Internet



Firewall



- A security appliance that performs filtering based on the network policies configured
- Software firewalls are common components of many network devices
- Firewalls may range from simple packet filters to application proxy filters

More on firewalls later in the course…

Intrusion Detection & Prevention System

- Intrusion detection & prevention systems scan network traffic for malicious content, and offer notification (IDS) or filtering (IPS) based on the result of the scan
- In addition to protecting internal hosts from external threats, IDPS protects the internal network against employee based hacking attempts

More on Intrusion Detection & Prevention Systems later in the course…

References

- Network Hub Image – Retrieved From: https://commons.wikimedia.org/wiki/File:HP_EtherTwist_Hub8.jpg
- Fixed Configuration Network Switch Image – Retrieved From: https://en.wikipedia.org/wiki/File:2550T-PWR-Front.jpg
- Modular Network Switch Image (cropped) – Retrieved From: https://commons.wikimedia.org/wiki/File:Coreswitch_(2634205113).jpg

References

- Home Router Image – Sam Churchill – Retrieved From: https://www.flickr.com/photos/32703995@N06/7335679950
- Enterprise Router Image – Retrieved From: https://commons.wikimedia.org/wiki/File:Juniper_Networks_SRX3400_service_gateway_and_security_appliance.jpg
- Stackable Network Switch Image (cropped) – Retrieved From: https://www.flickr.com/photos/dhabben/4729857587
- IPv4 Multicast Address ranges – RFC2365 – retrieved from: https://tools.ietf.org/html/rfc2365
- IPv6 Multicast Address ranges – RFC4291 – retrieved from: https://tools.ietf.org/html/rfc4291