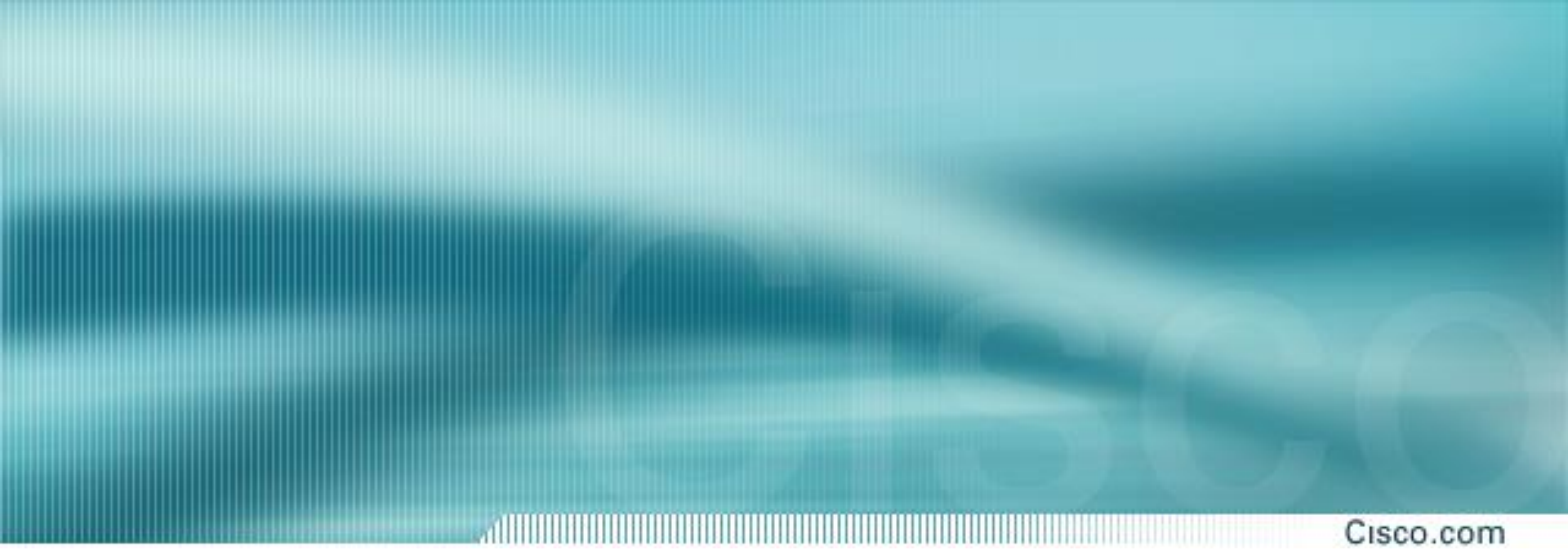
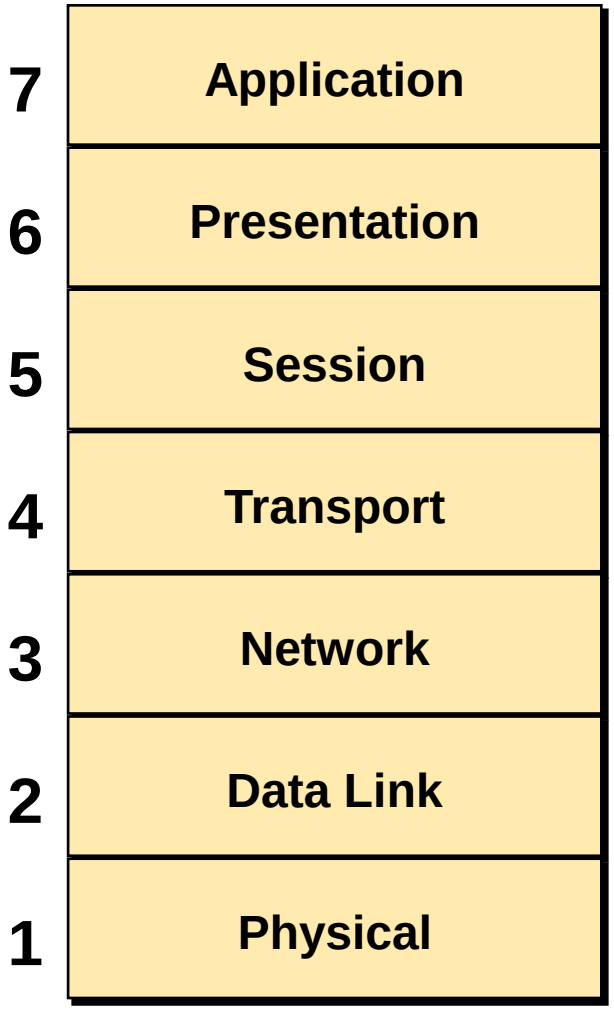


Networking Fundamentals

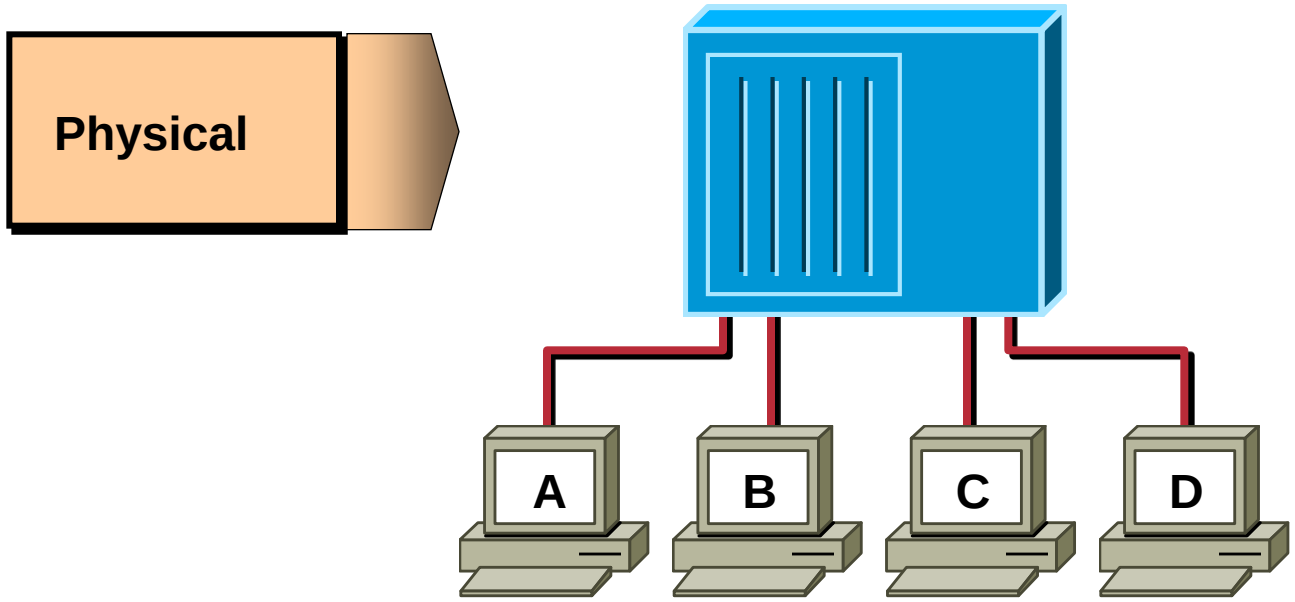
Networking Devices:
Review from module one

Networking Devices

- **Layer 5-7 – Firewalls, IPS**
- **Layer 3,4 - Routers**
- **Layer 2 – Bridges/Switches**
- **Layer 1 - Hubs**



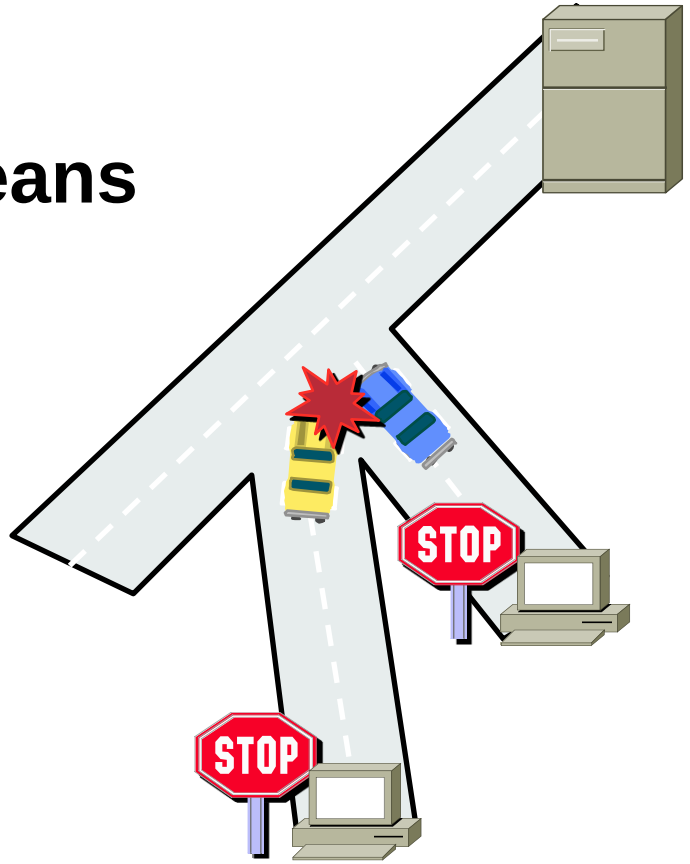
Hubs Operate at Physical layer



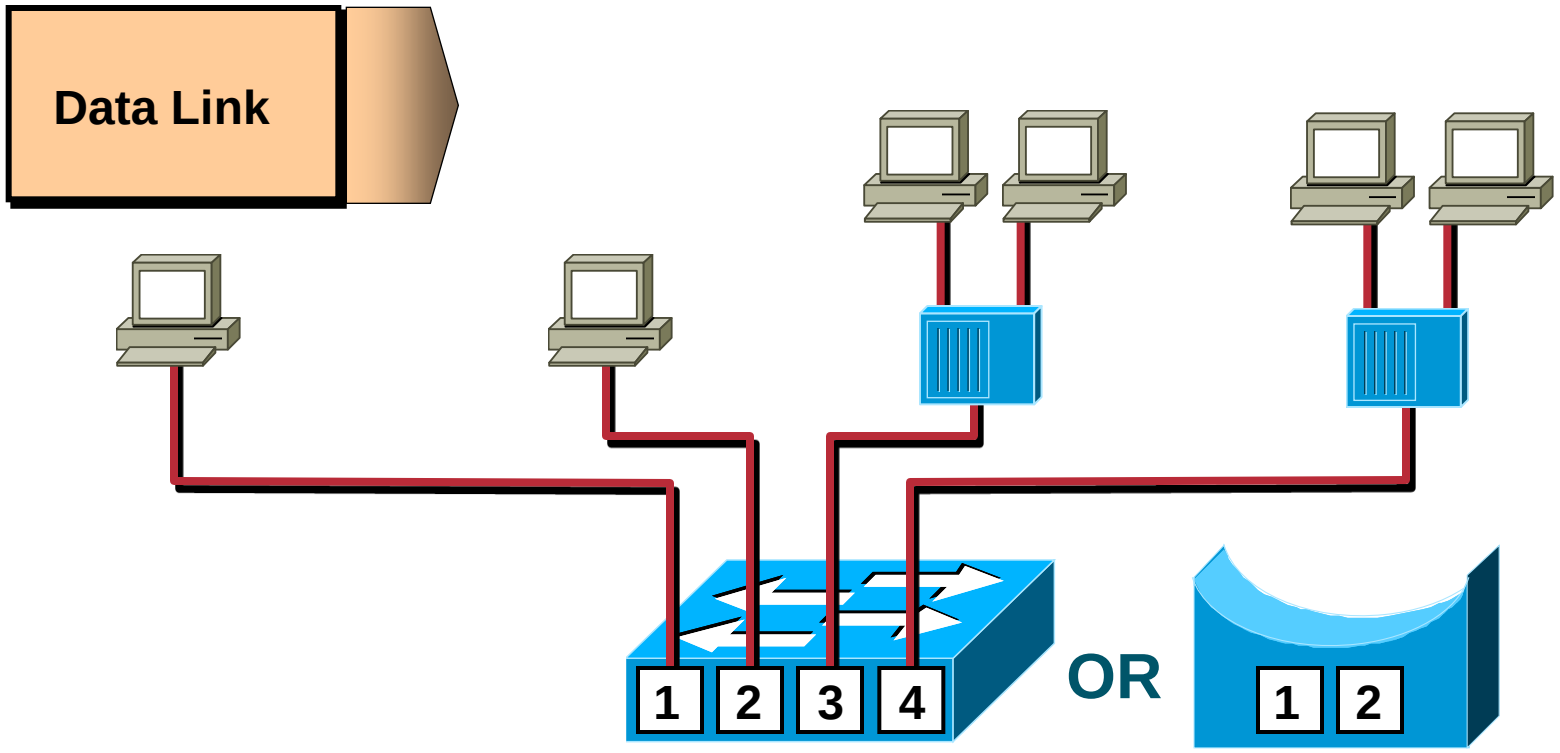
- All devices in the same collision domain
- All devices in the same broadcast domain
- Devices share the same bandwidth

Hubs: One Collision Domain

- **More end stations means more collisions**
- **CSMA/CD is used**

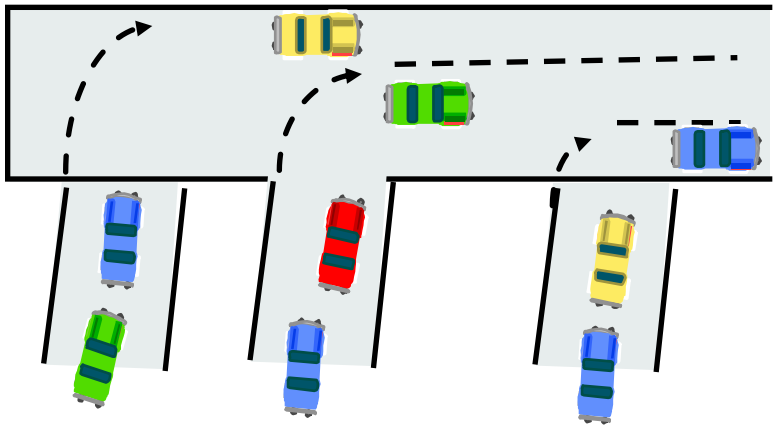


Switches and Bridges Operate at Data Link Layer

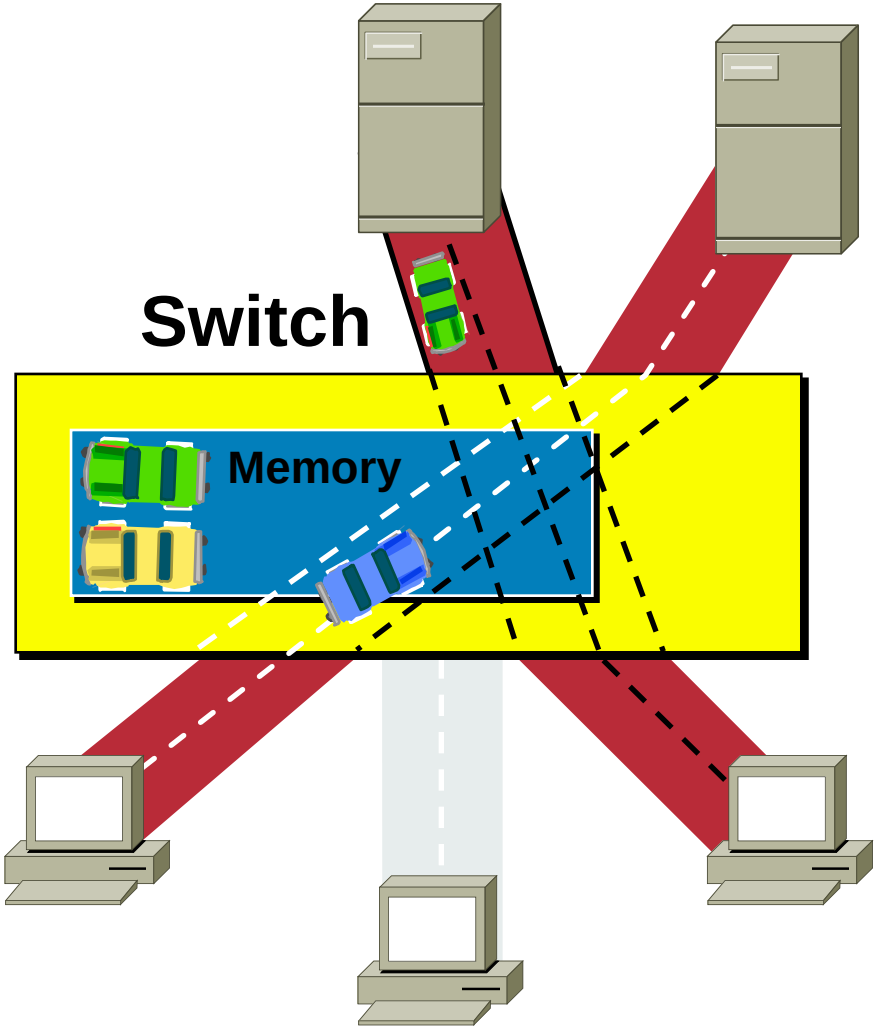


- **Each segment has its own collision domain**
- **All segments are in the same broadcast domain**

Switches

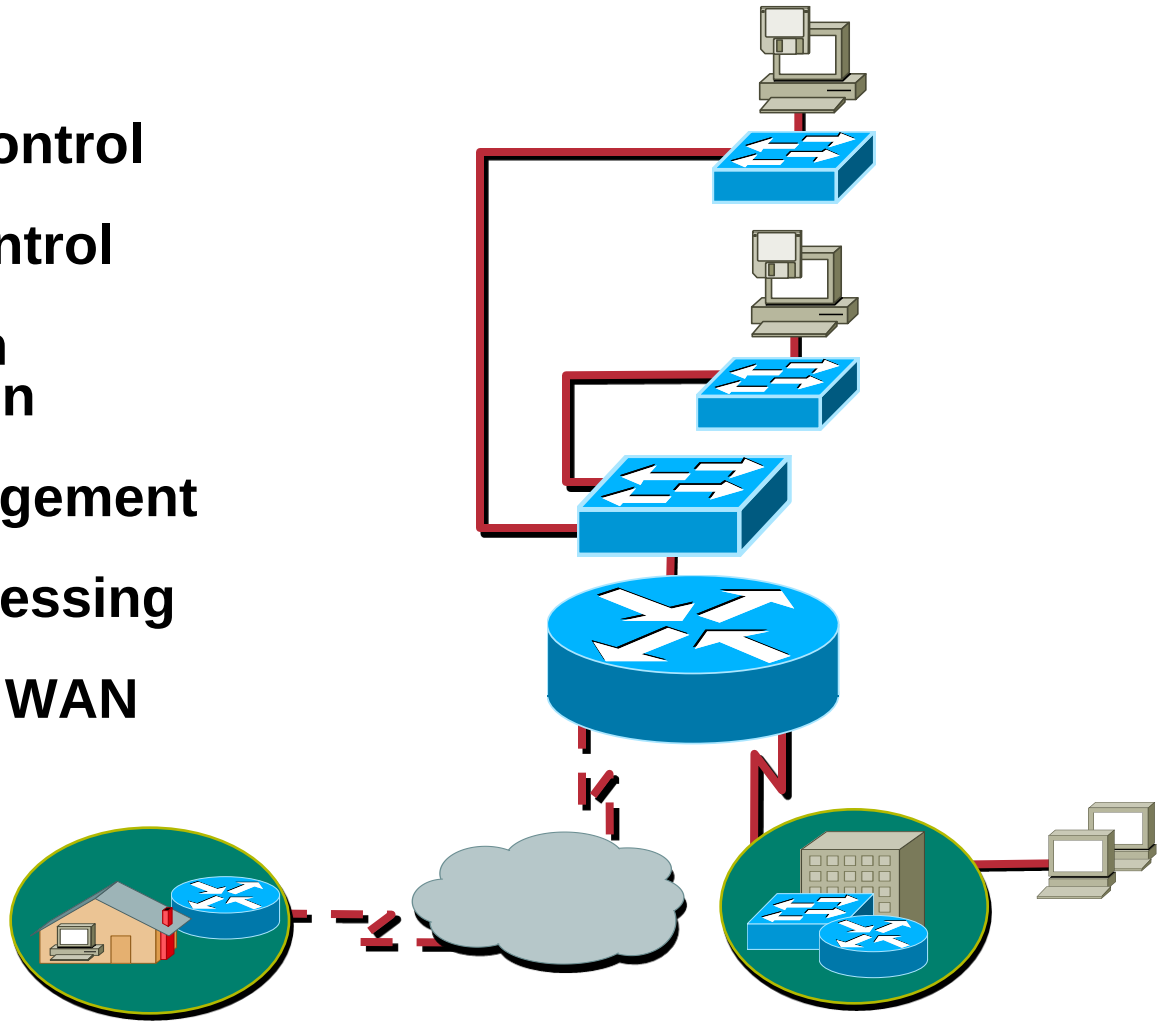


- **Each segment has its own collision domain**
- **Broadcasts are forwarded to all segments**

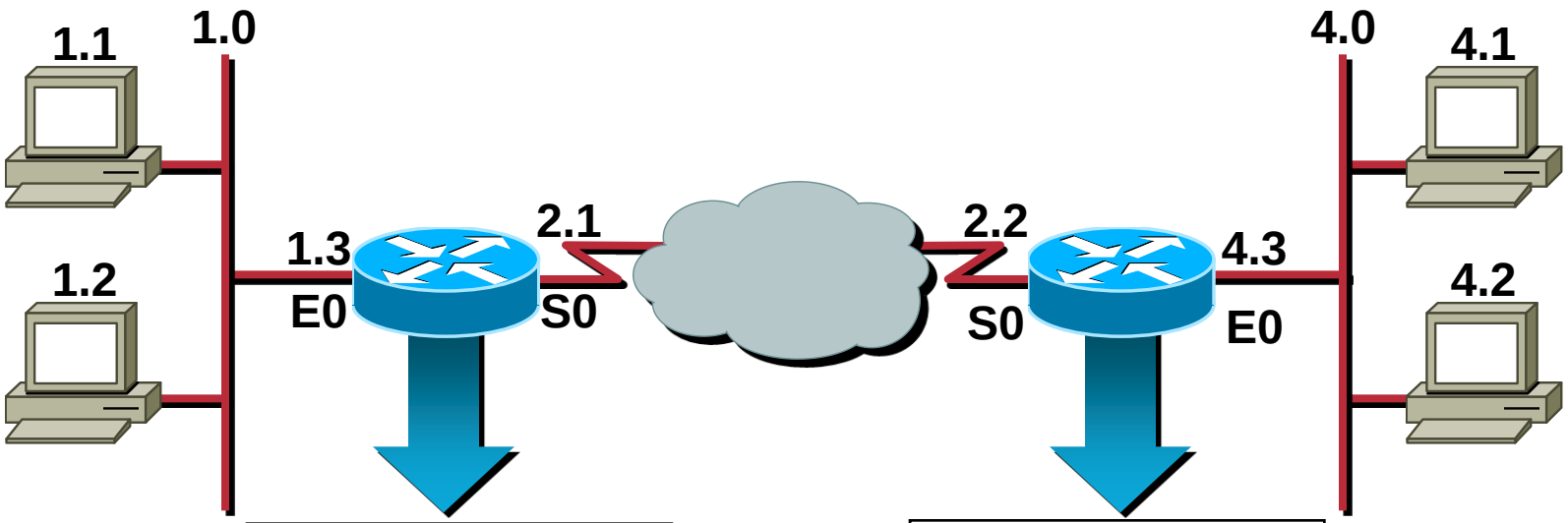


Routers: Operate at the Network Layer

- **Broadcast control**
- **Multicast control**
- **Optimal path determination**
- **Traffic management**
- **Logical addressing**
- **Connects to WAN services**



Network Layer Functions (cont.)



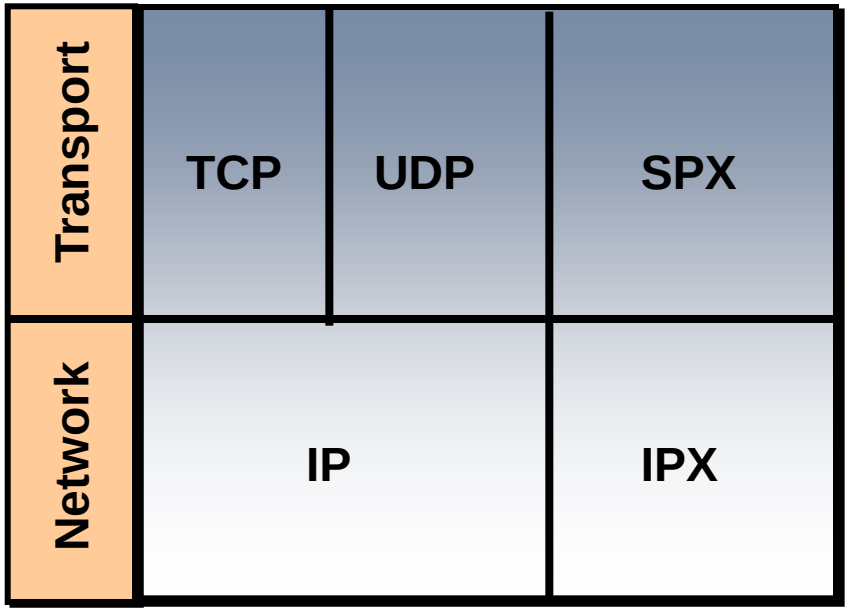
Routing Table		
NET	INT	Metric
1	E0	0
2	S0	0
4	S0	1

Routing Table		
NET	INT	Metric
1	S0	1
2	S0	0
4	E0	0

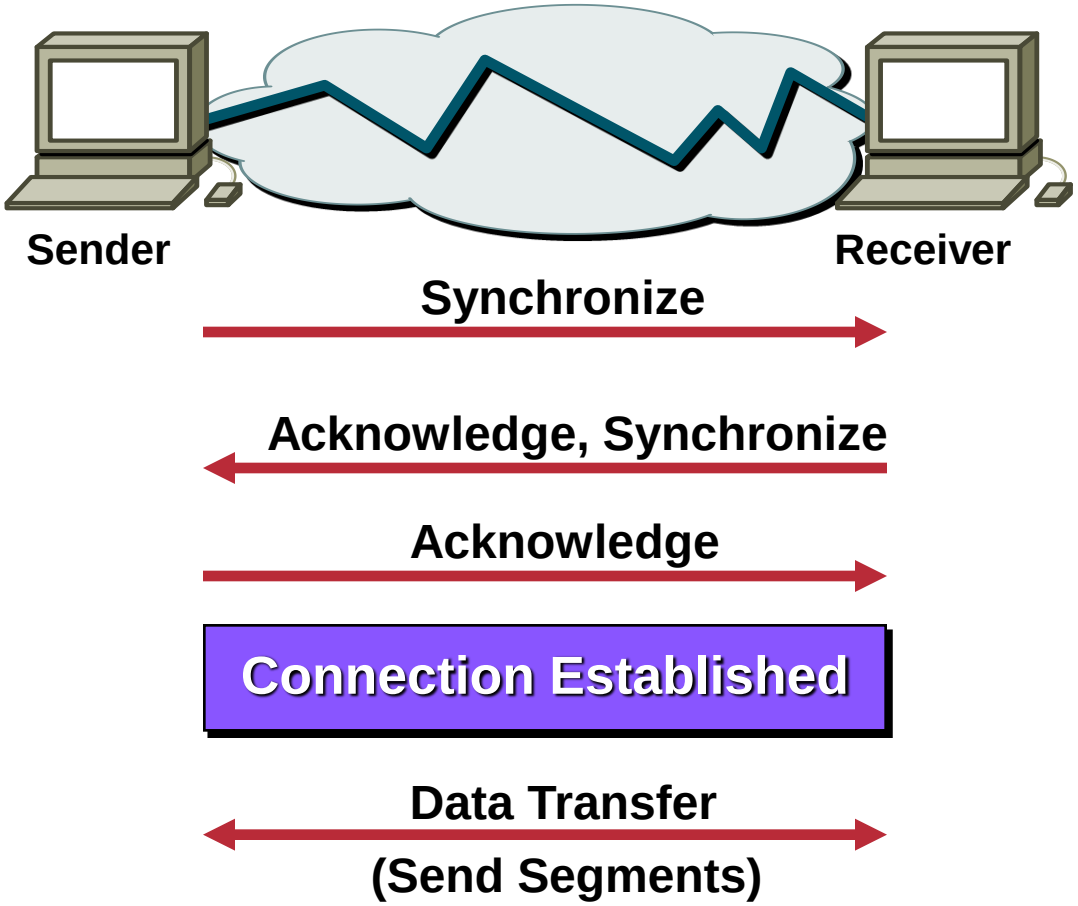
- Logical addressing allows for hierarchical network
- Configuration required
- Uses configured information to identify paths to networks

Transport Layer Functions

- **Distinguishes between upper layer applications**
- **Establishes end-to-end connectivity between applications**
- **Defines flow control**
- **Provides reliable or unreliable services for data transfer**

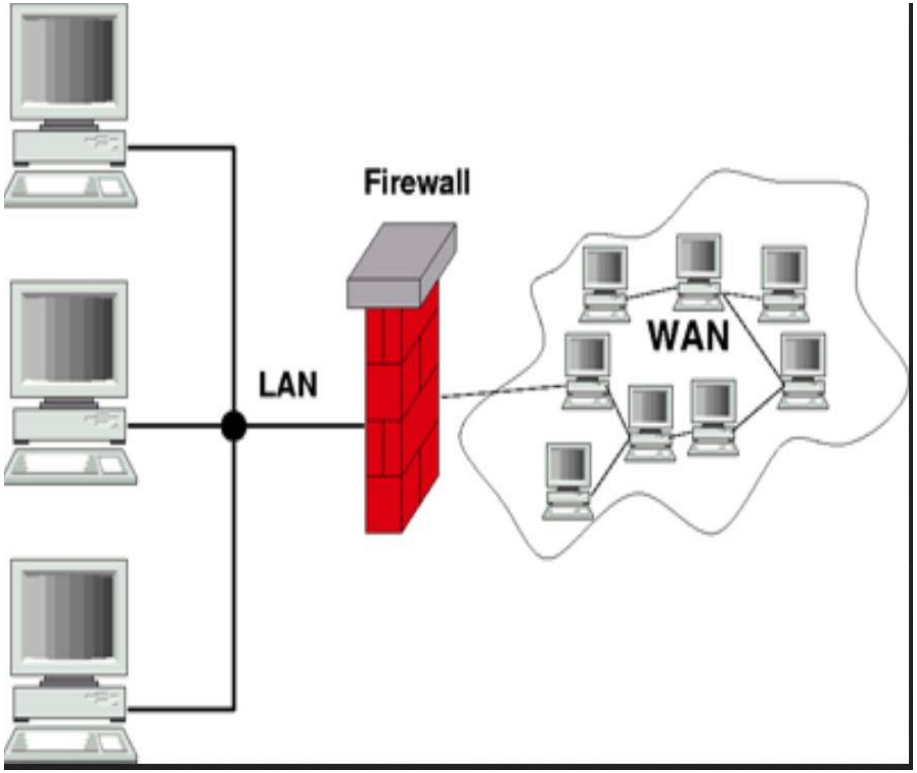


Reliable Transport Layer Functions



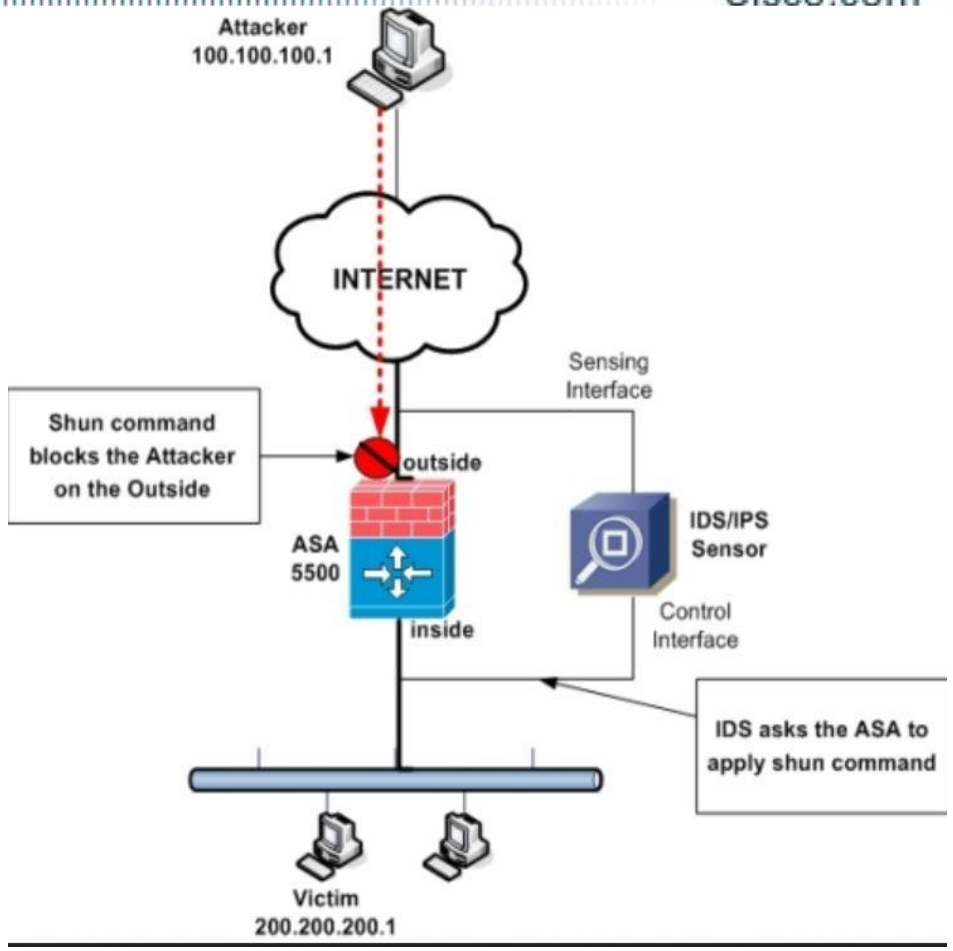
Firewalls: Operate at L2 – L7

- **Blocks unrequested traffic**
- **Allows return traffic from requested sessions**
- **Inspects for "impersonated" traffic**
- **Creates network boundaries**
- **Can be configured manually to allow or deny certain traffic**



Intrusion Prevention Systems: Operate at L3 – L7

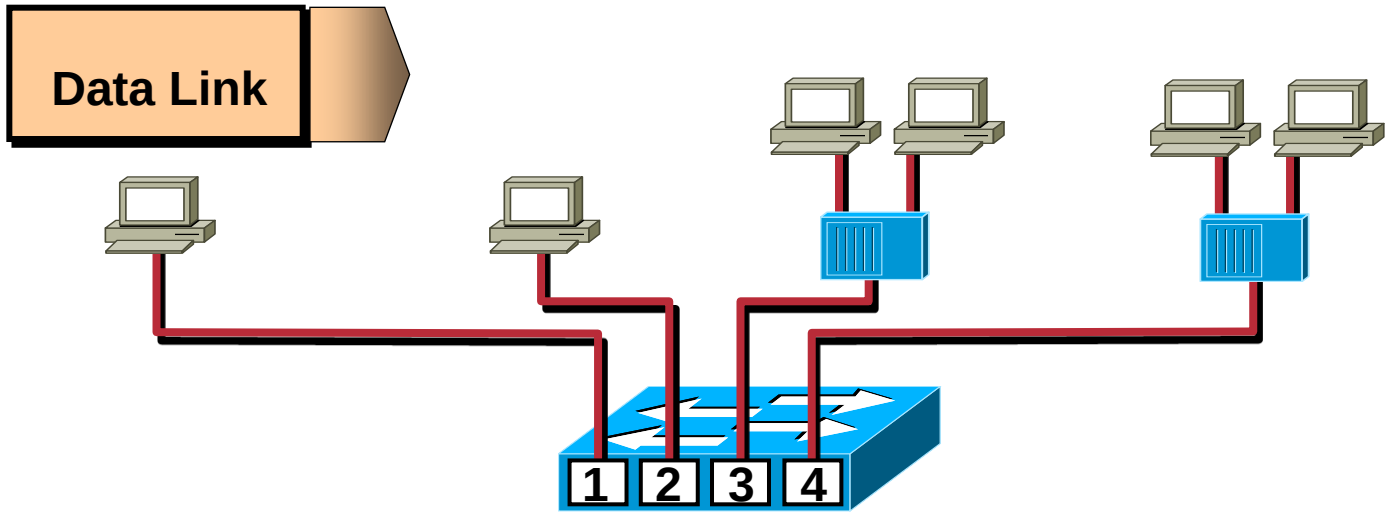
- **Inspects traffic for attacks**
- **Can be deployed in-line or out of band**
- **Can send alert or block suspicious traffic**
- **Differs from firewall in that it inspects allowed traffic for suspicious behavior**



Network Devices:

Where are these devices used in the network, and why?

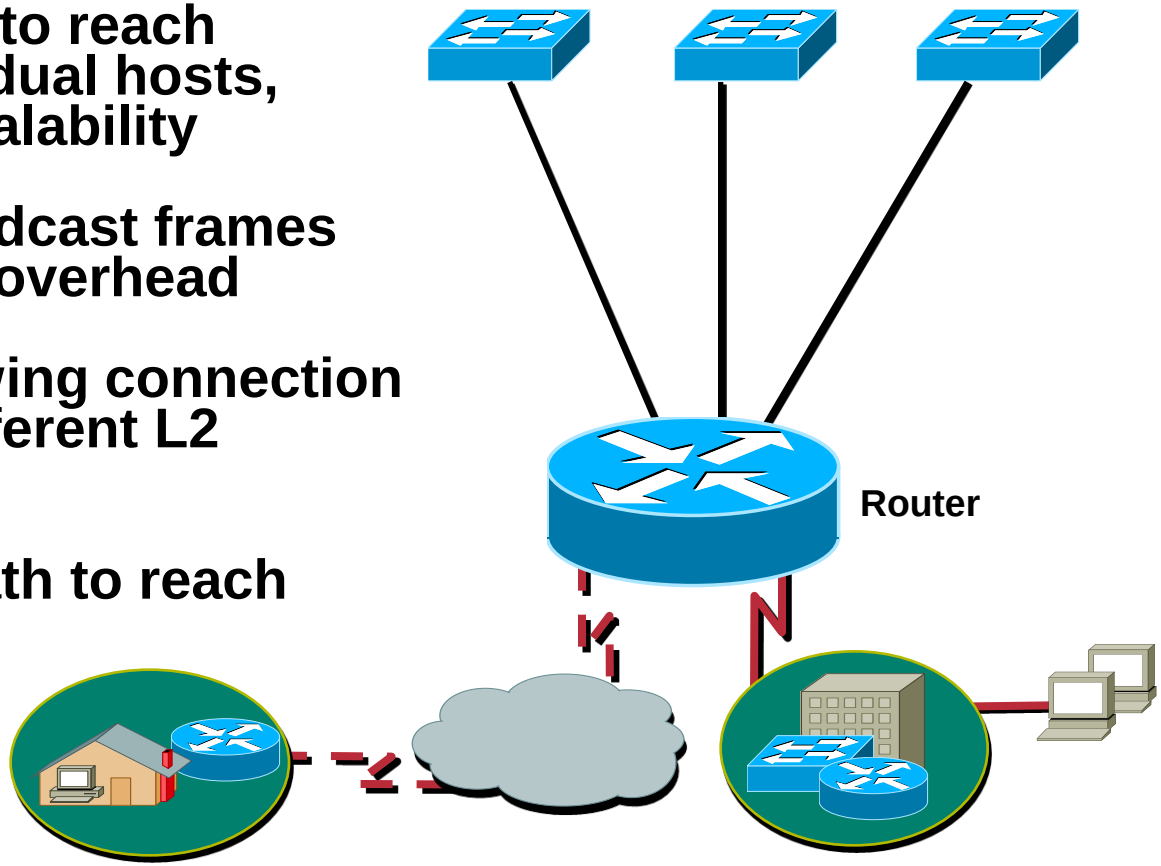
Switches



- **Switches are used to directly connect devices to the network**
- **They replaced hubs which are obsolete technology**
- **Switches keep a table of all MAC address on the LAN**
- **Switches deliver Ethernet frames to the MAC address of the device**

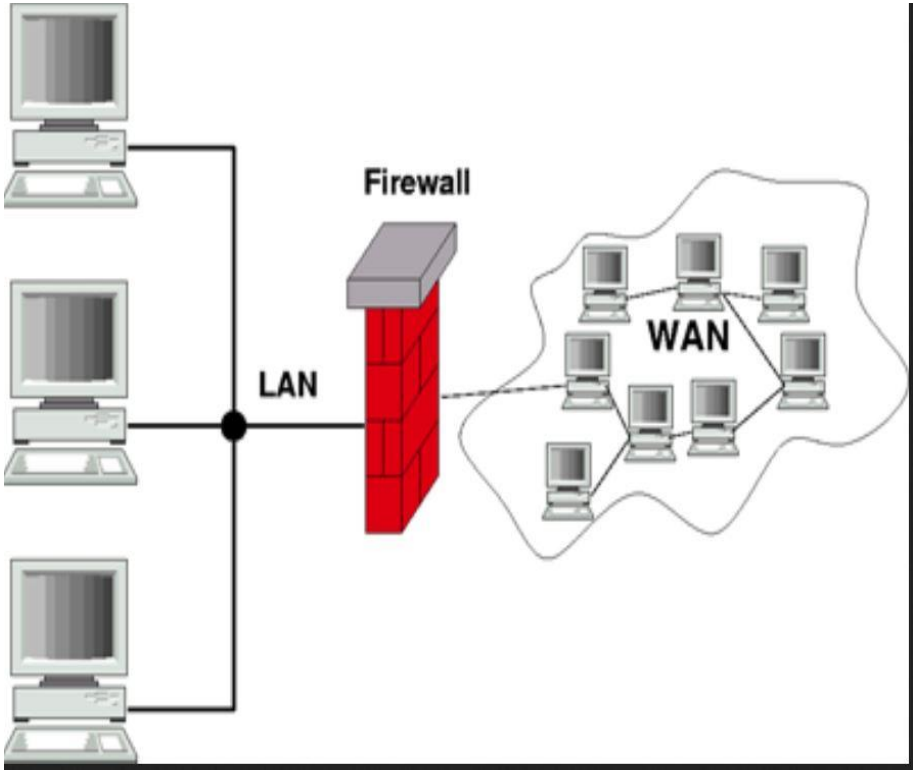
Router Functions

- **Typically aggregate LAN switches**
- **Keep a table of how to reach networks, not individual hosts, allowing network scalability**
- **Do not forward broadcast frames which reduces LAN overhead**
- **Strip L2 frame, allowing connection of networks with different L2 technologies**
- **Calculate optimal path to reach remote networks**



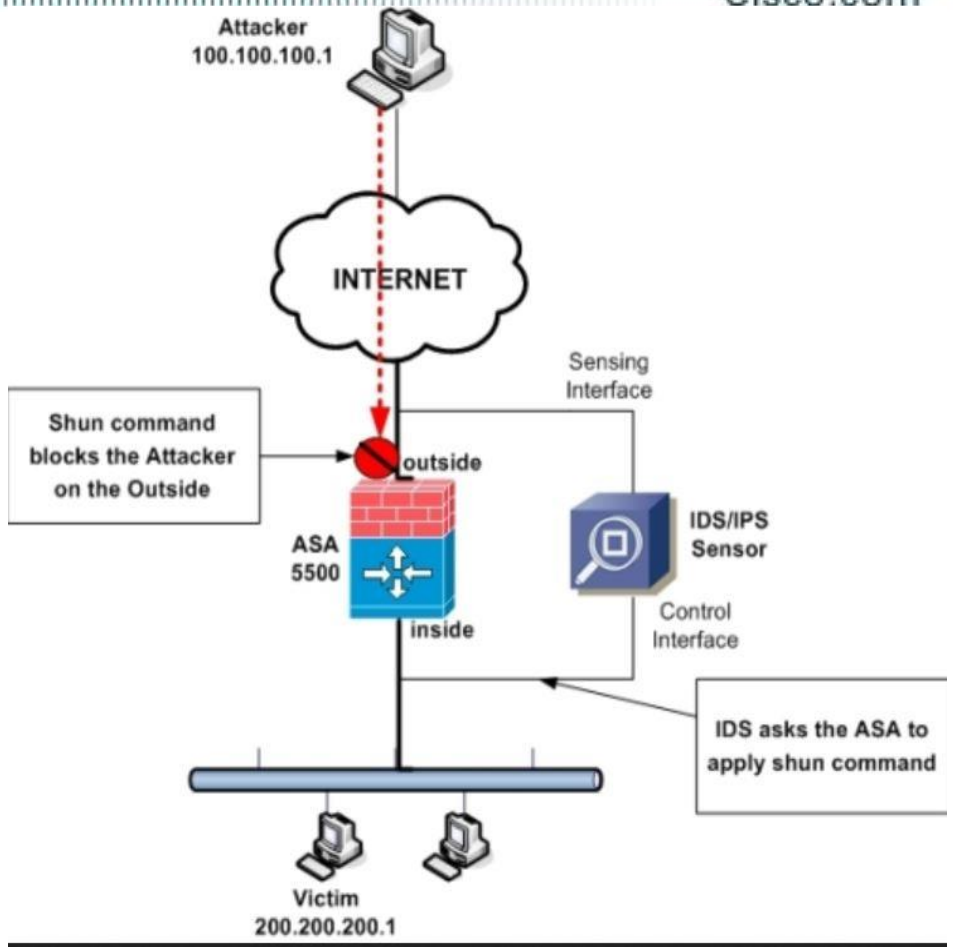
Firewalls

- Create a border between networks
- Implement security policy of allowed or denied traffic
- Commonly found at Internet border, or datacenter border
- Can often inspect up to L7 application layer



Intrusion Prevention Systems

- **Commonly deployed at Internet edge, or aggregation points in a campus**
- **Monitors traffic and alerts on suspicious behavior**
- **Inspects up to L7 application layer**




CISCO