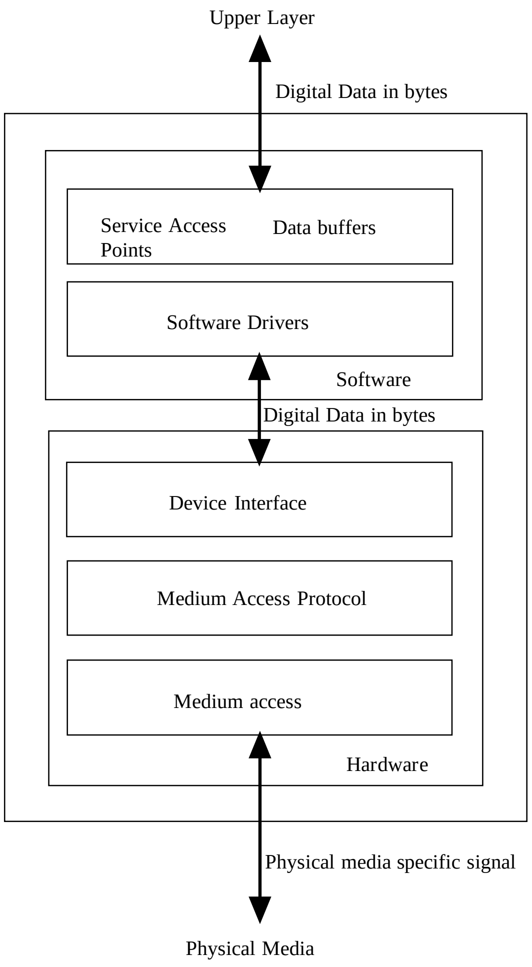
CprE 530

Lecture 6

Topics

- Lower Layer Security
- Physical Layer Overview
- Common attack methods
- Ethernet

Physical Network Layer



Upper Layer

Digital Data in bytes

Service Access Points

Data buffers

Software Drivers

Software

Digital Data in bytes

Device Interface

Medium Access Protocol

Medium access

Hardware

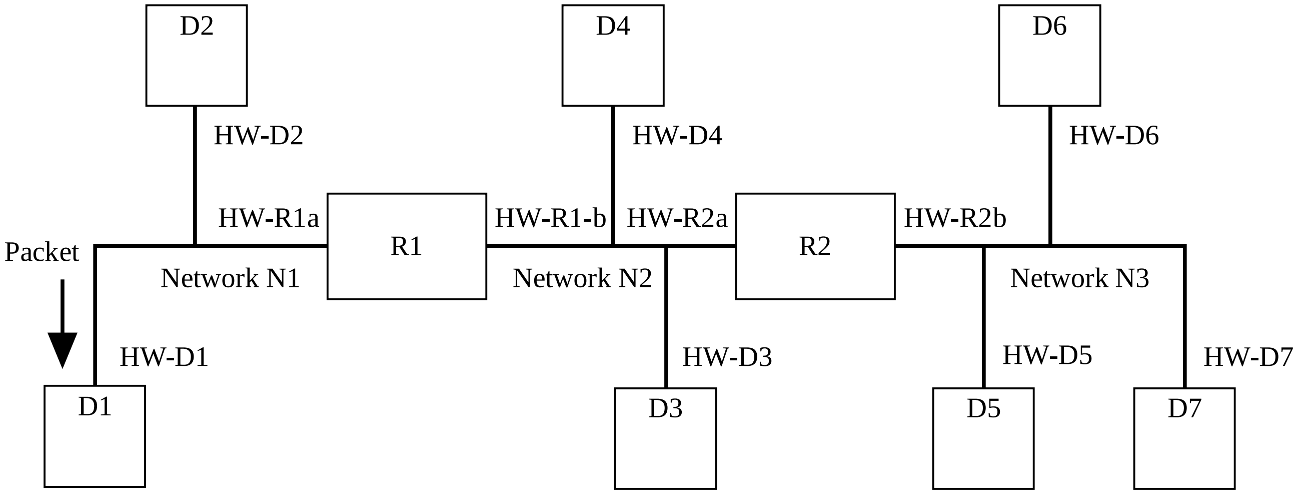
Physical media specific signal

Physical Media

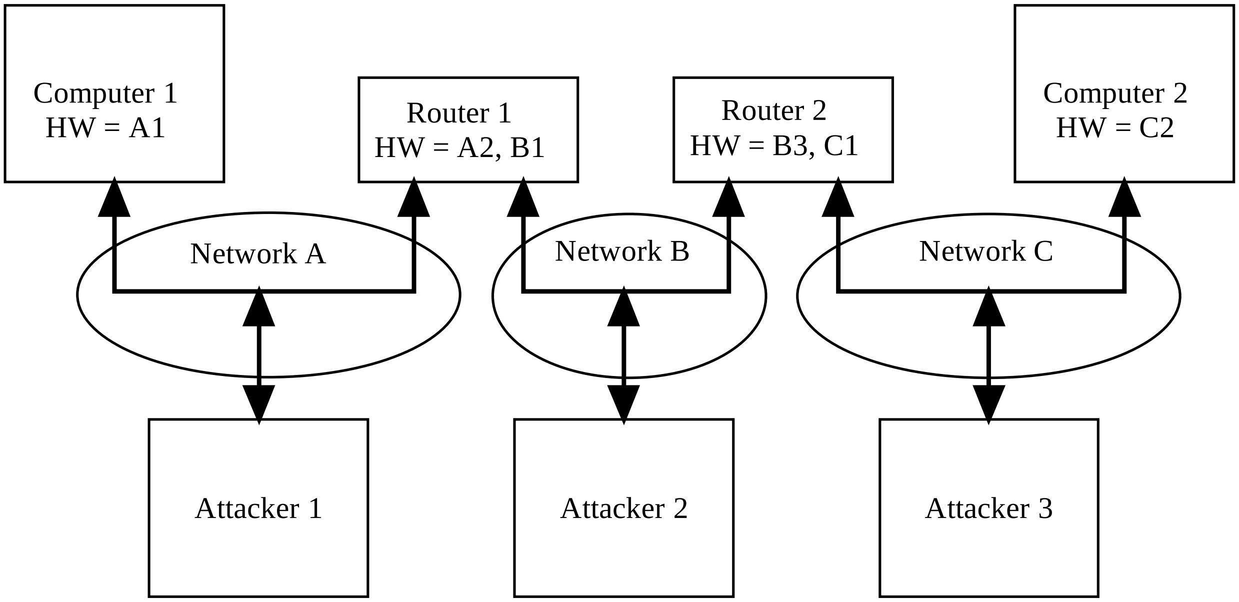
Common Attack Methods

- Spoofing
- Sniffing
- Physical Attacks

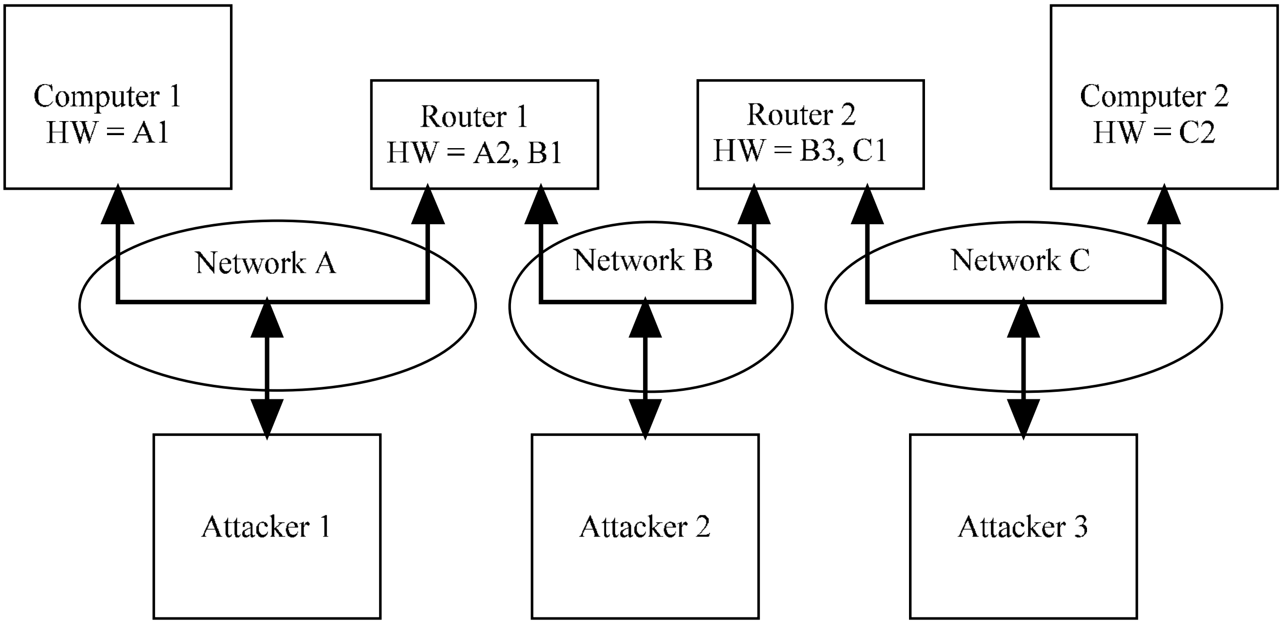
Hardware Addressing



Hardware Address Spoofing



Network Sniffing



Physical Attacks

- Bad network cable
- Network cable loop (both ends plugged into the same device)
- Bad network controller
- Two network controllers with the same hardware address

Wired Network Protocols

- Many protocols
- Local Area Networks (LAN)
  - Ethernet is the most common
- Wide Area Networks (WAN)

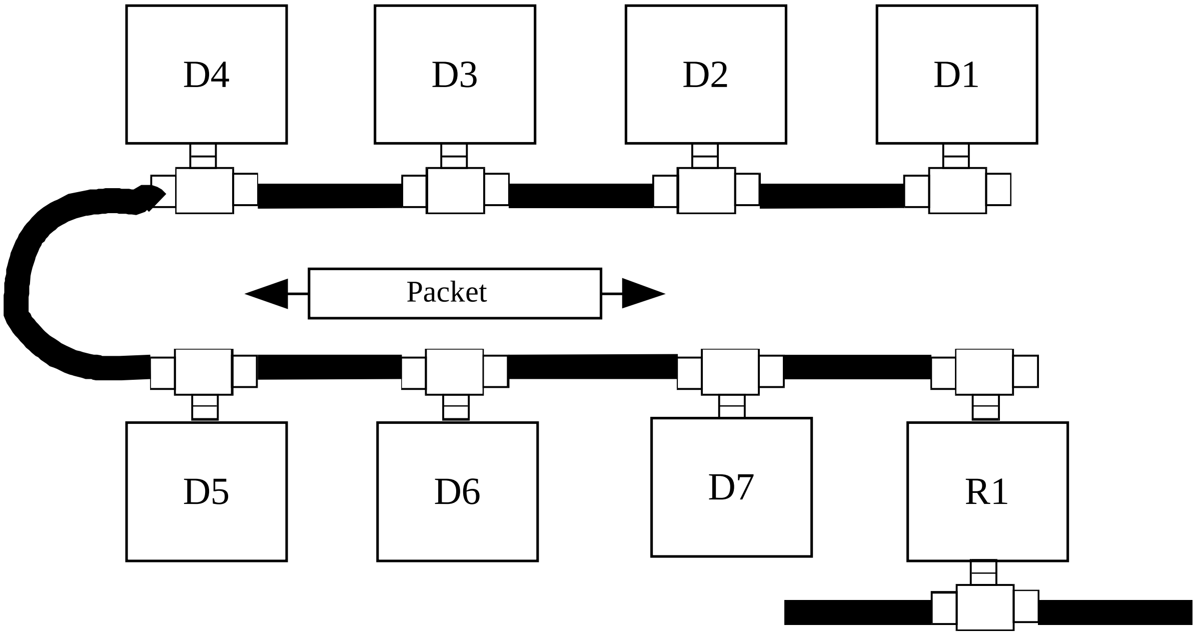
Ethernet

- Developed in 1973 by Xerox
- Speeds
  - 10 Mbps
  - 100 Mbps
  - 1000 Mbps (gigabit)
  - 10 Gigabit

Ethernet Transmission media

Name	Cable type	Speed	Maximum Distance between devices
10Base2	Coax	10 Mbps	185 meters
10BaseF	Fiber	10 Mbps	500 meters
10BaseT	Twisted Pair	10 Mbps	100 meters
100BaseT	Twisted Pair	100 Mbps	100 meters
100BaseFX	Fiber	100 Mbps	1000 meters
1000Base-X	Fiber or coax	1000 Mbps	Depends on cable type

Coaxial Ethernet



Ethernet Access Method

- CSMA/CD
  - – Listen
  - – Talk if no one else is talking
  - – Back off if more than one talks at a time
  - – Minimum packet length is used to guarantee that a collision can be seen by all machines. This also puts a limit on the length of the cable

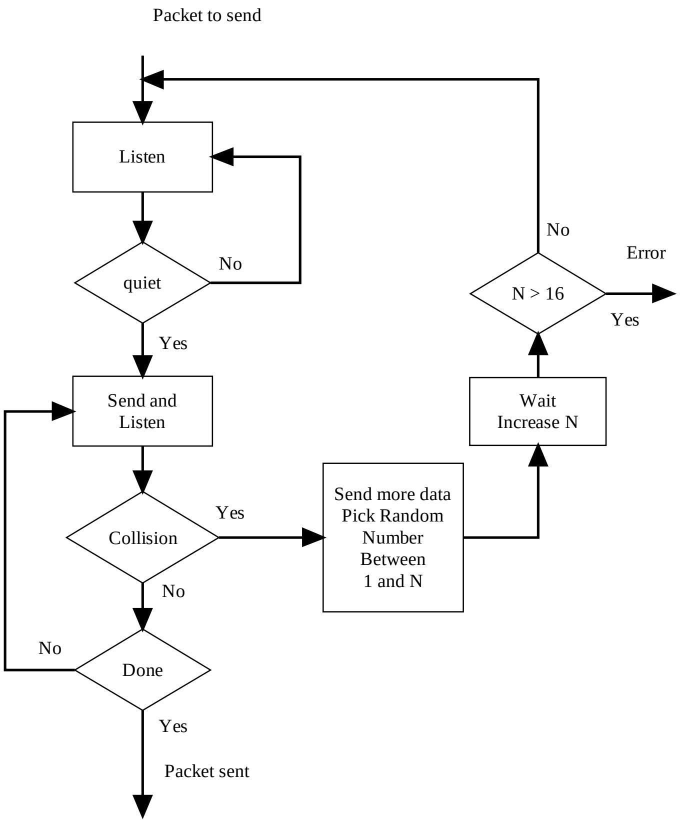


Figure 5.5 CSMA/CD Ethernet Protocol

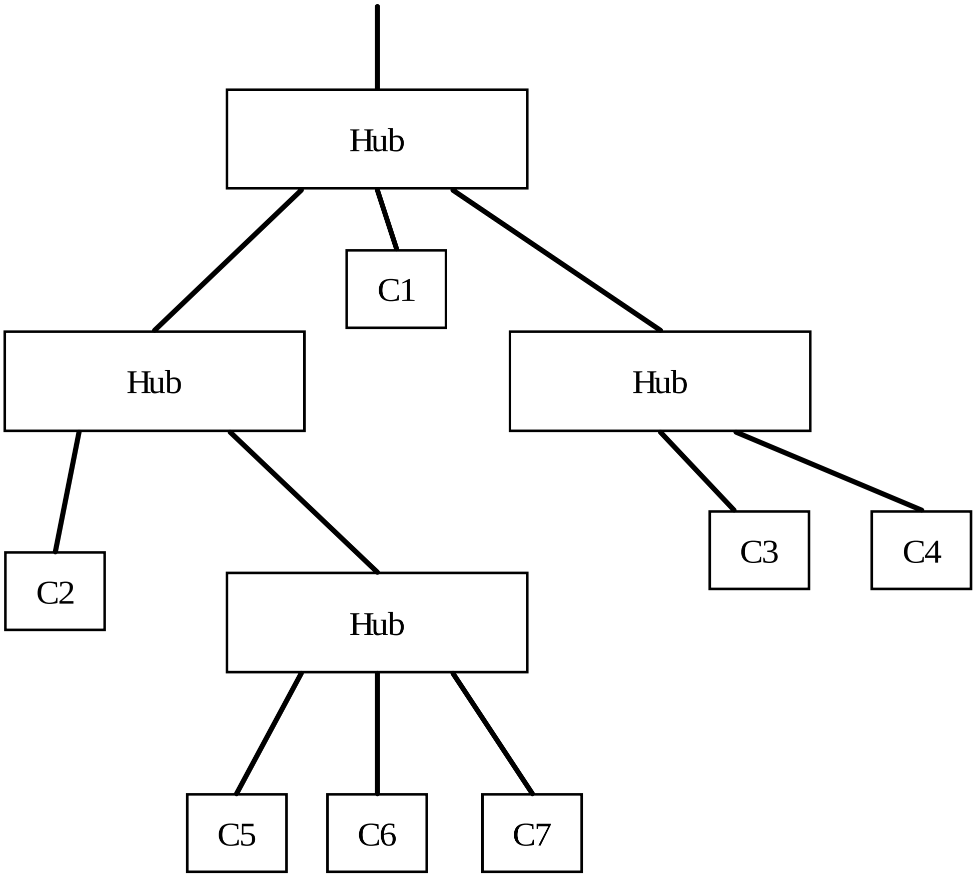
Ethernet Collision Domain

- The range that is effected when a collision occurs.
- 10Mbps Ethernet it is 2500 Meters
- This can be changed by using switches and routers (more later)

Connecting Devices

- Repeater (physical layer only)
- Hub (multi port repeater)
- Bridge (layer 2 only)
- Router (layer 3)
- Layer 2 switch
- Layer 3 switch

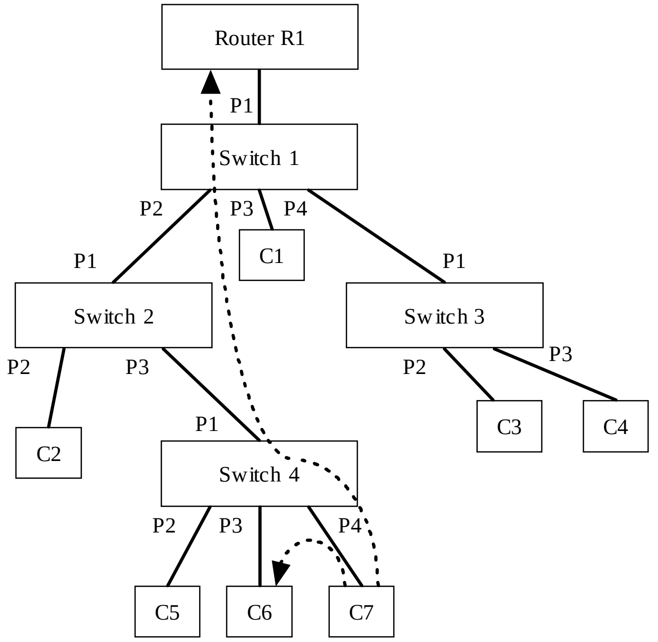
Ethernet Hubs



Ethernet switches

- Collisions can slow the network down
- Switches create multiple collision domains
- Typically one machine per leg of the switch
- Switches only pass traffic to the leg of the switch where the destination is located
- Switches reduce the traffic on each leg
  - Problem with network monitoring

Ethernet Switch



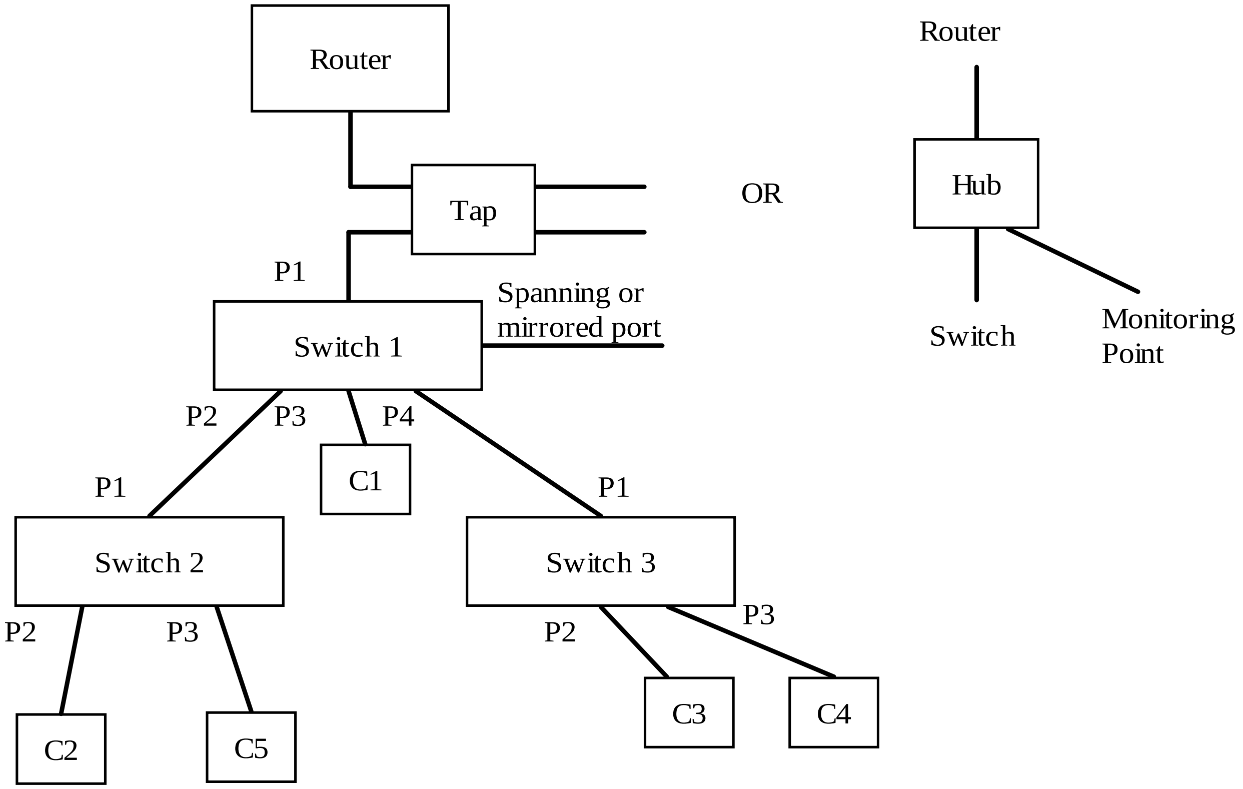
Port table, switch 2

Port	HW Address
P1	Uplink
P2	C2
P3	Multiple

Port table, switch 4

Port	HW Address
P1	Uplink
P2	C5
P3	C6
P4	C7

Ethernet Tap Points



Ethernet - Frame

Preamble (on wire only)	7 bytes
Start Frame Delimiter	1 bytes
Destination Address	6 Bytes
Source Address	6 Bytes
Type or Length	2 Bytes
Data	46-1500 Bytes
FCS	4 Bytes

Ethernet Addresses

- Goal is to have all addresses globally unique
- 6 bytes
  - Upper 3 bytes vendor code
  - Lower 3 bytes independent
- All 1’s = broadcast address

Ethernet Type/length

- If value < 0x800 then it is a length field otherwise it is a protocol type field. Some common types are:

Hex	
0800	DoD Internet Protocol (IP)
0805	X.25 level 3
0806	Address Resolution Protocol (ARP)
6003	DECNET Phase IV
6004	Dec LAT
809B	EtherTalk
80F3	AppleTalk ARP

Attacks and vulnerabilities

- Header-based
- Protocol-based
- Authentication-based
- Traffic-based

Header-Based

- Attacks
  - Setting the destination address as a broadcast address can cause traffic problems
  - Setting the source can cause switches to get confused
- Mitigation
  - Very difficult to mitigate

Protocol-Based

- Protocol is simple and is in hardware

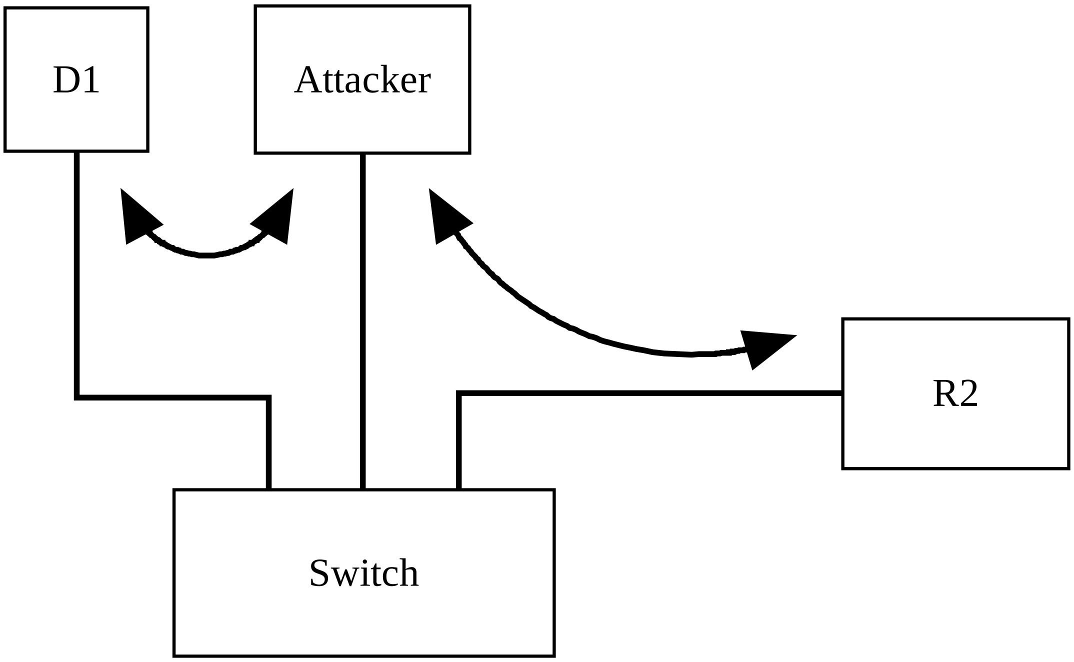
Authentication-Based

- You can set the hardware address
- Hardware address is used to authenticate in switches
- Hardware addresses can be used to authenticate devices in a network

Authentication-Based

- Destination address spoofing
- Destination address is obtained dynamically via a protocol
- Trick a device into thinking you are the destination (ARP Poisoning)
- No good mitigation method

ARP Poisoning



Authentication-Based

- Source Address Spoofing
- Source address if not used for authentication by default
- New security and network management methods are starting to use the source address to authenticate the device. (Network Access Control [NAC])
- More on NAC as a general countermeasure later

Traffic-Based

- Attack
  - Ethernet controllers can be set in promiscuous mode which enables them to sniff traffic
- Mitigation
  - Encryption, VLAN (more later)
- Broadcast traffic can cause flooding, hard to flood unless directly connected to the LAN
- No good mitigation for flooding