Introduction to Network Security

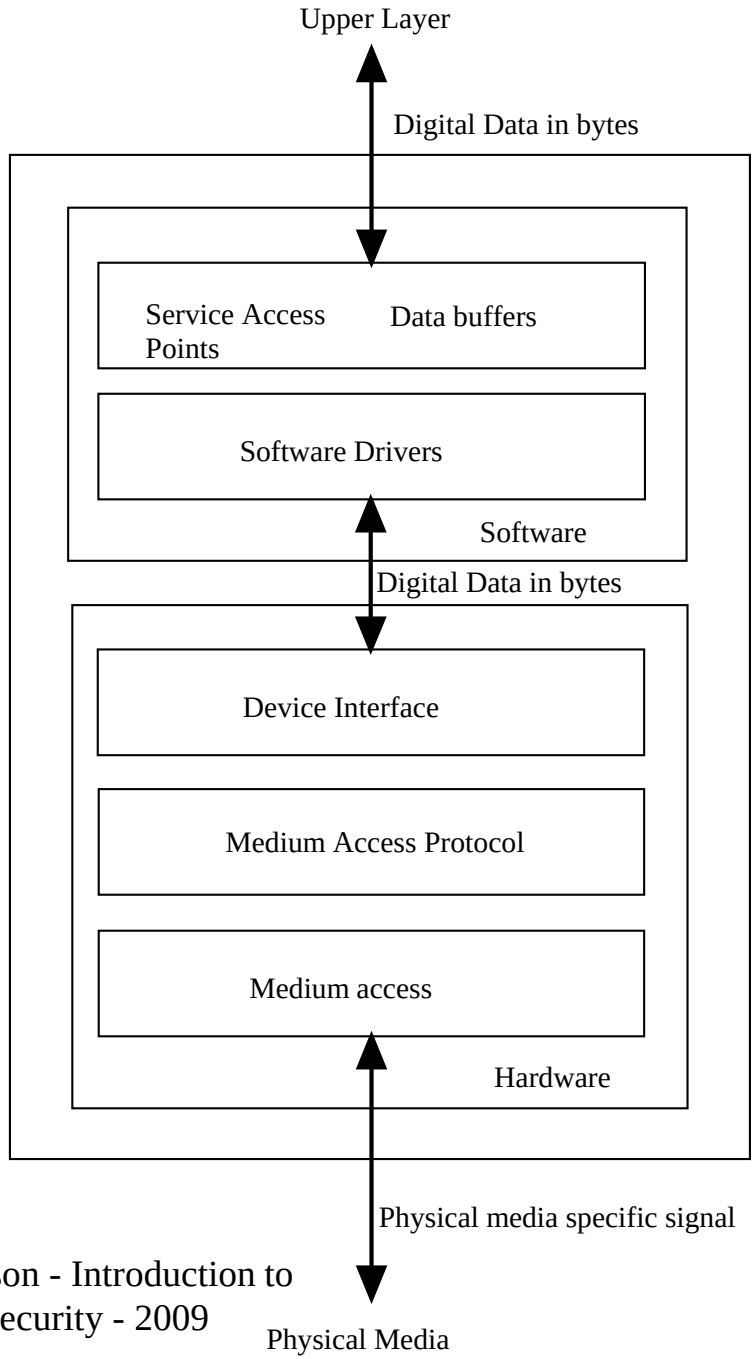
Chapter 5

Physical Network Layer

Topics

- Lower Layer Security
- Physical Layer Overview
- Common attack methods
- Ethernet
- Wireless Security
- General Mitigation Methods

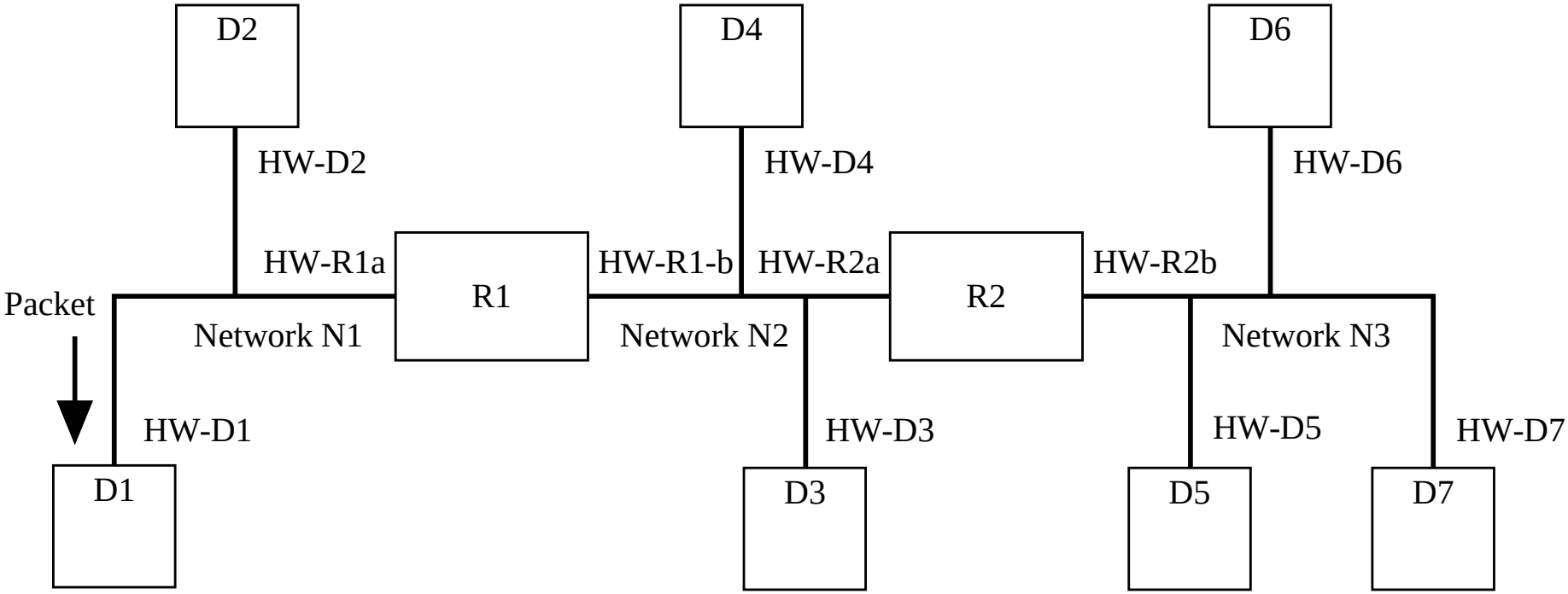
Physical Network Layer



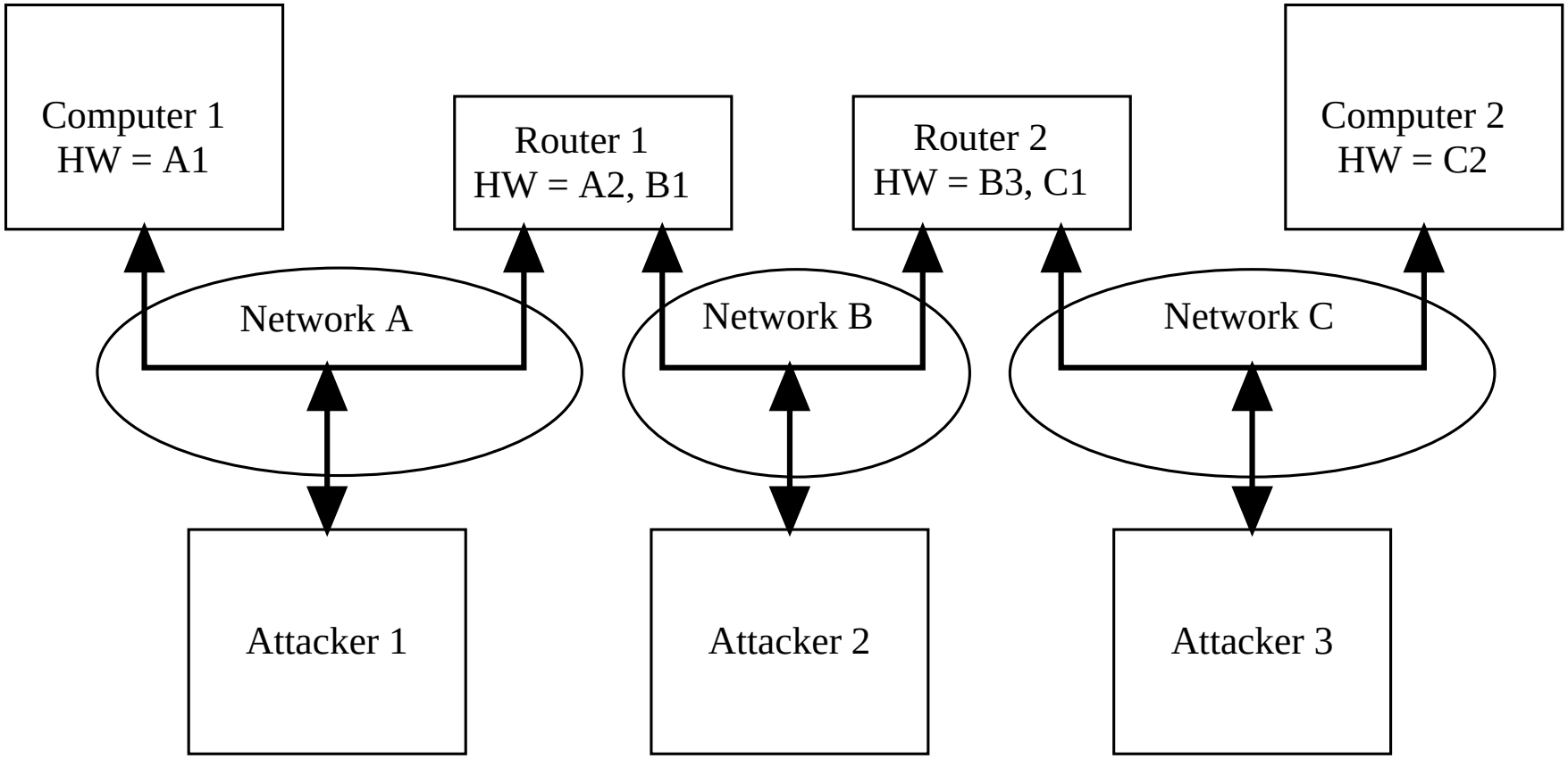
Common Attack Methods

- Spoofing
- Sniffing
- Physical Attacks

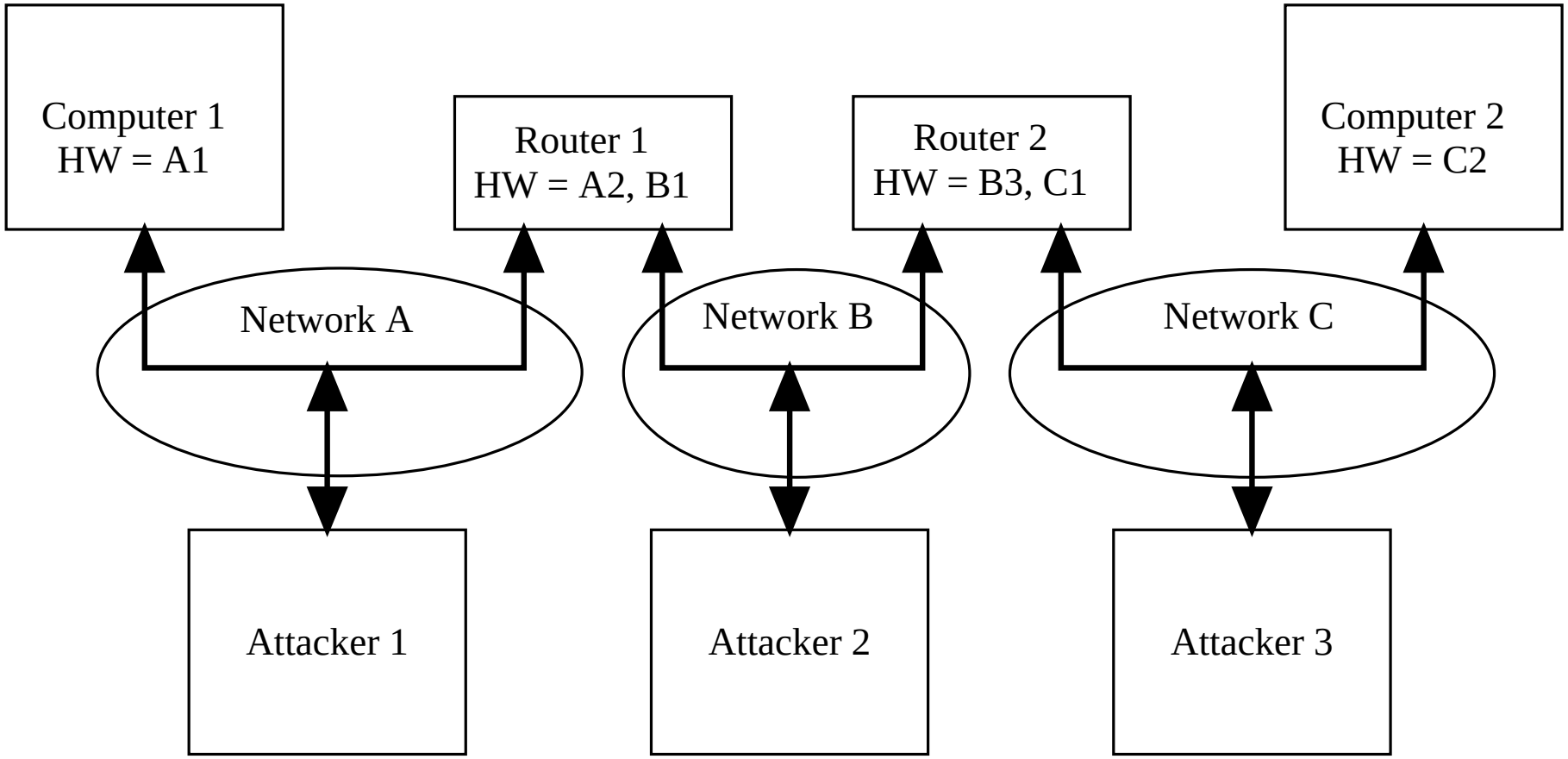
Hardware Addressing



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)

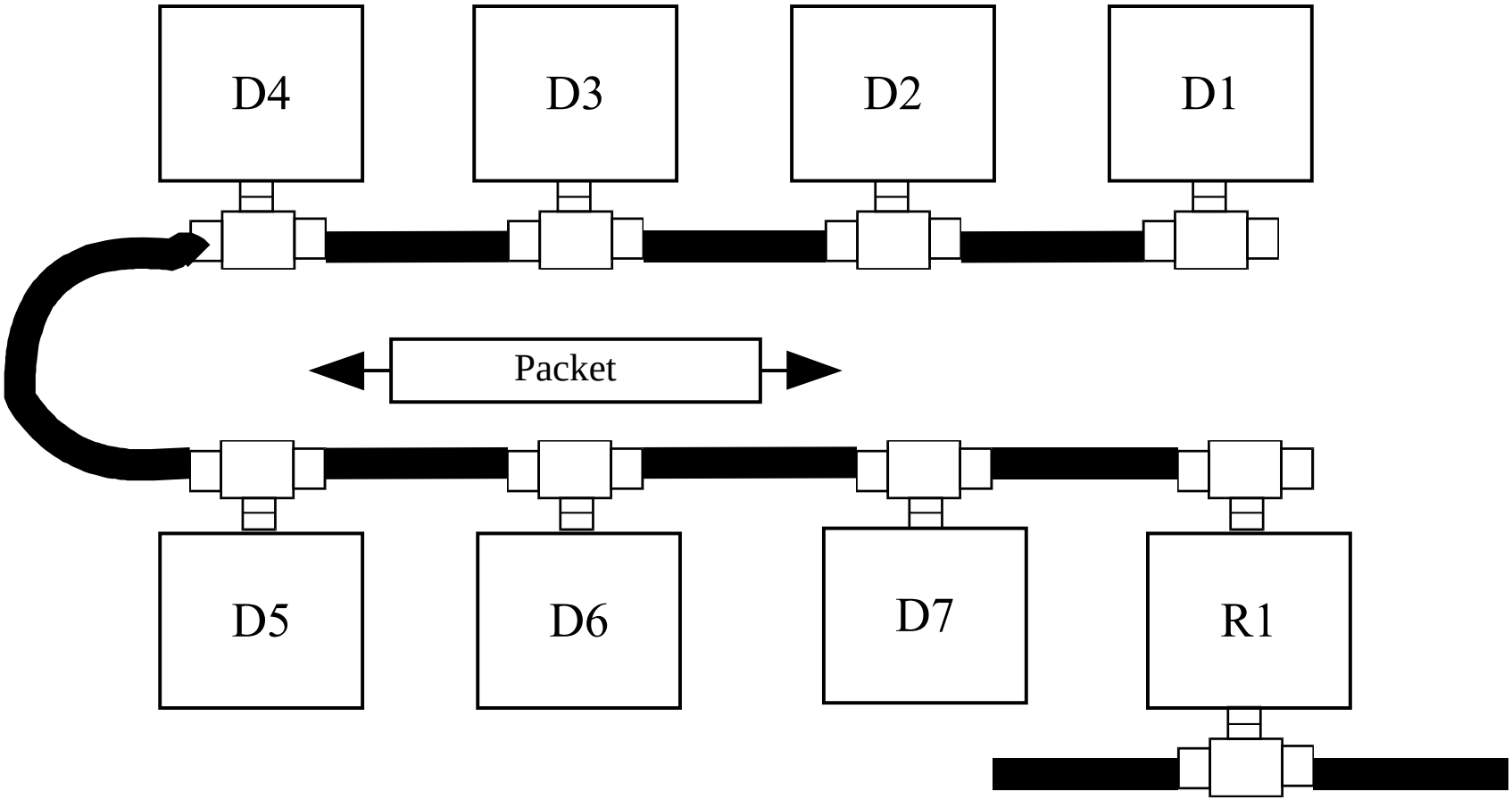
Ethernet

- 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

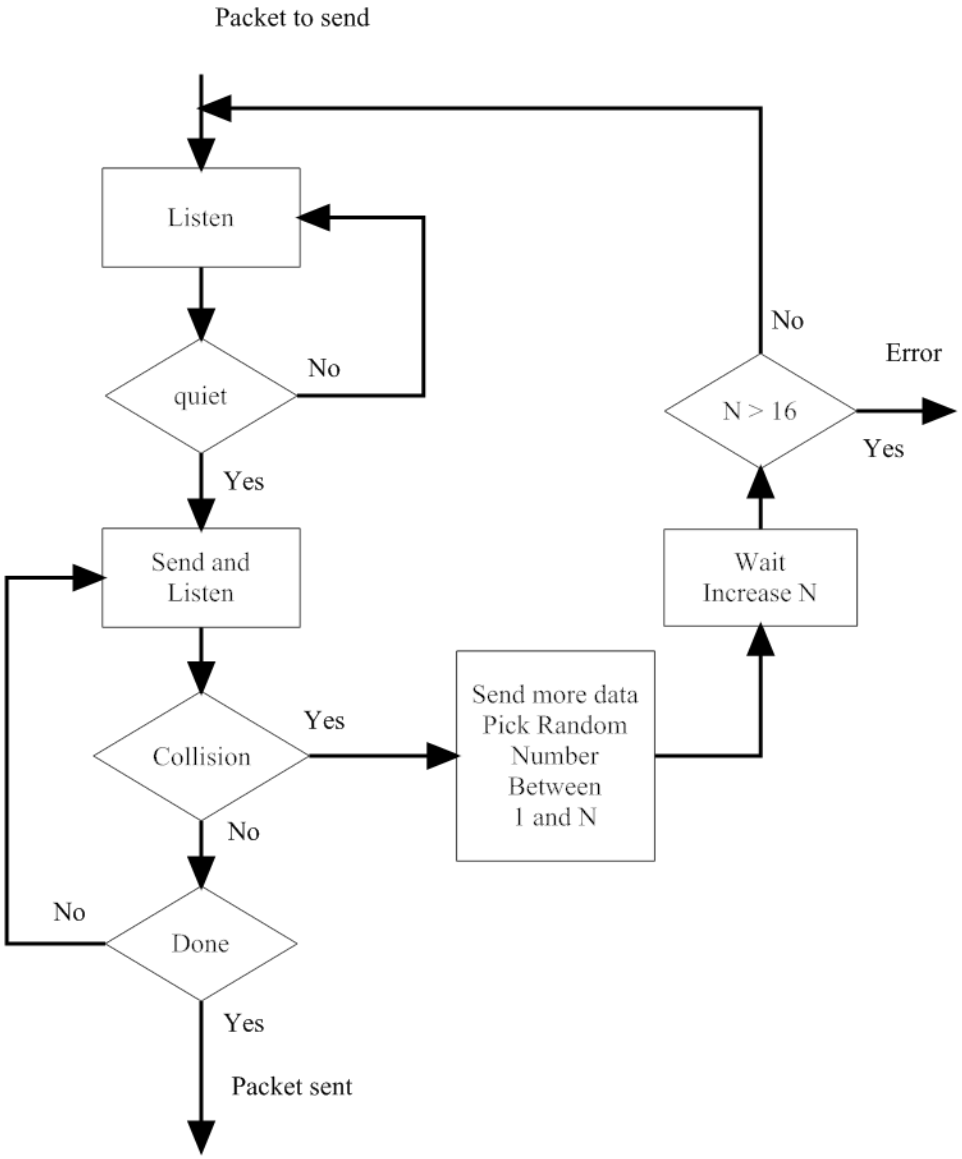


Figure 5.5 CSMA/CD Ethernet Protocol

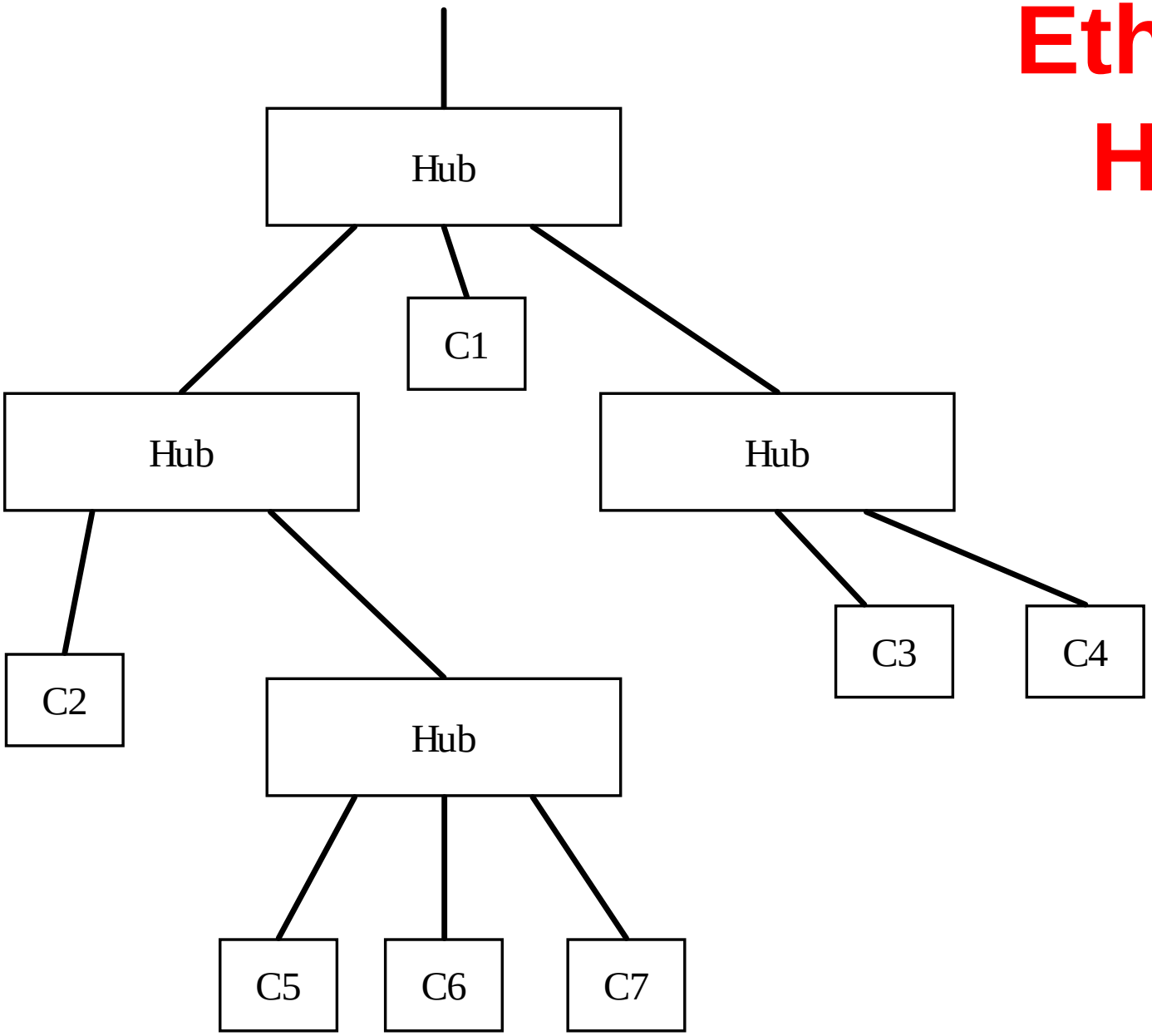
Ethernet Collision Domain

- 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

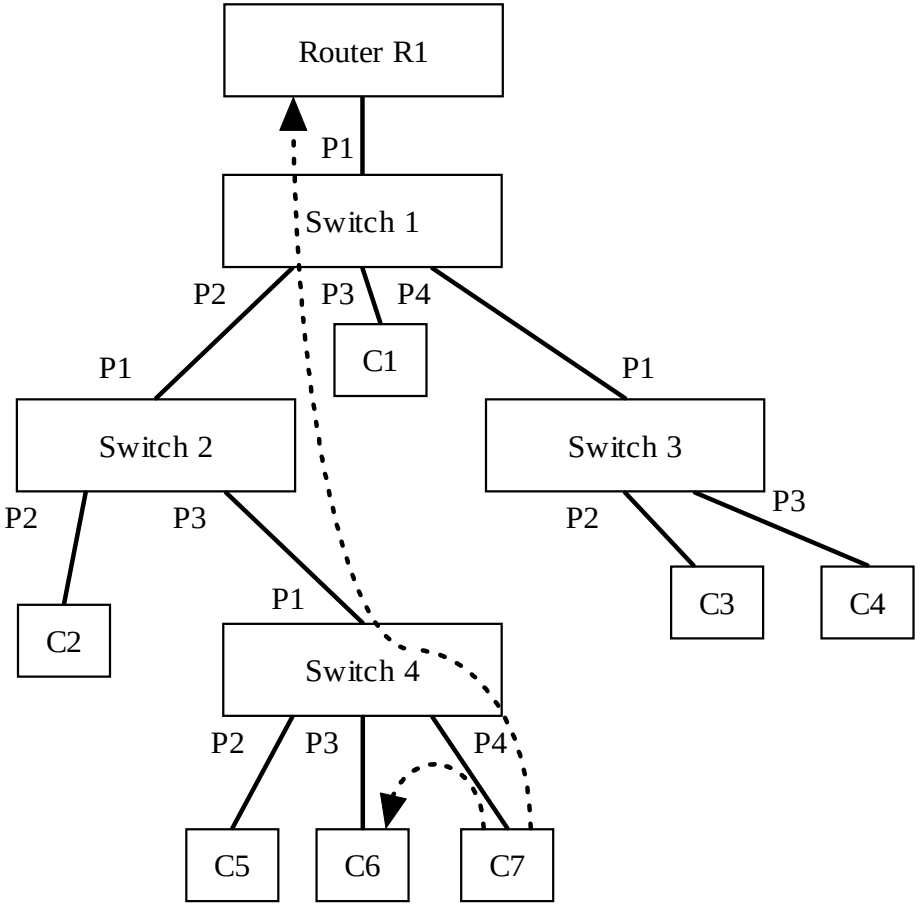
Ethernet Hubs



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



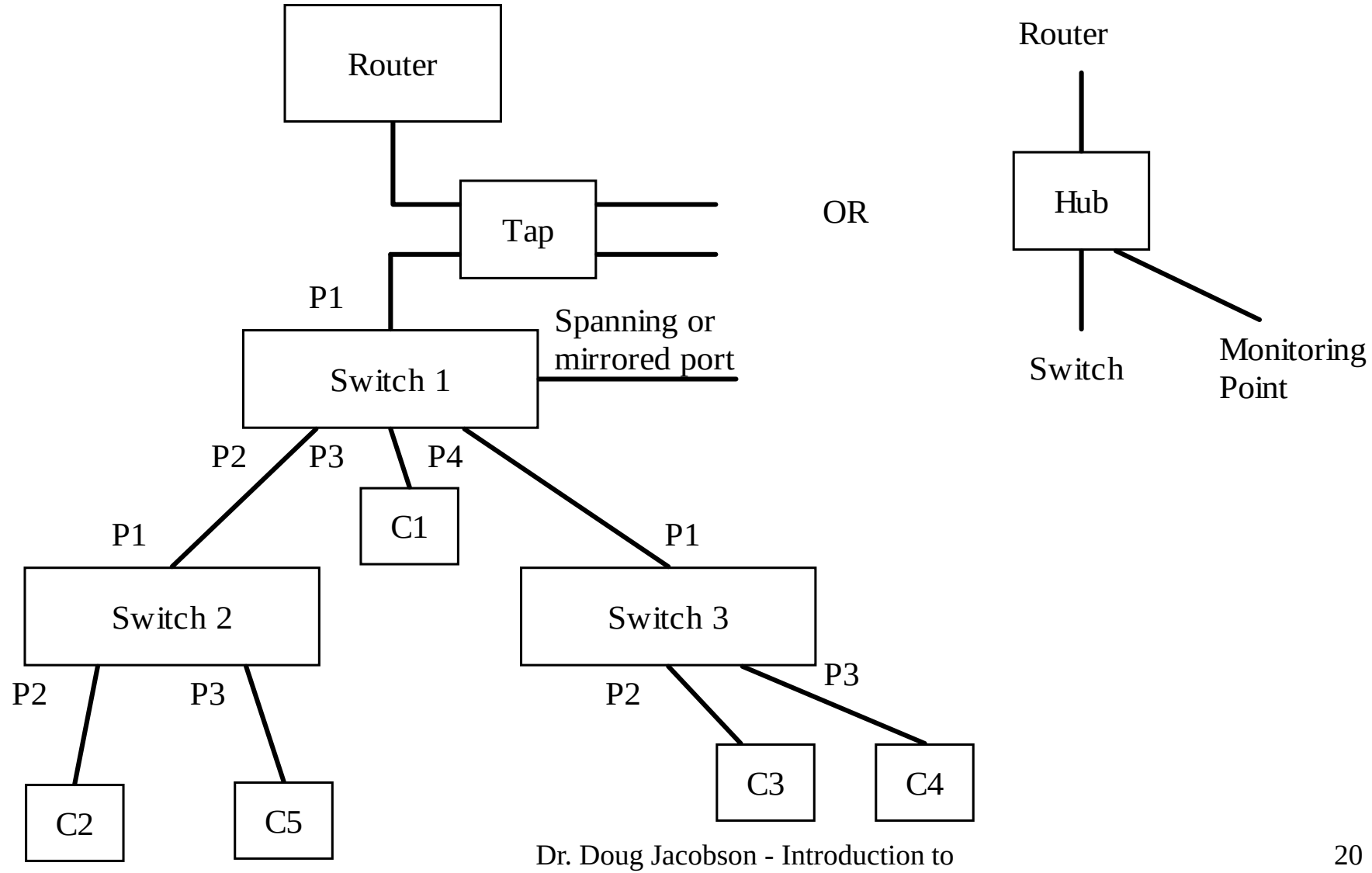
Port table, switch 2

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

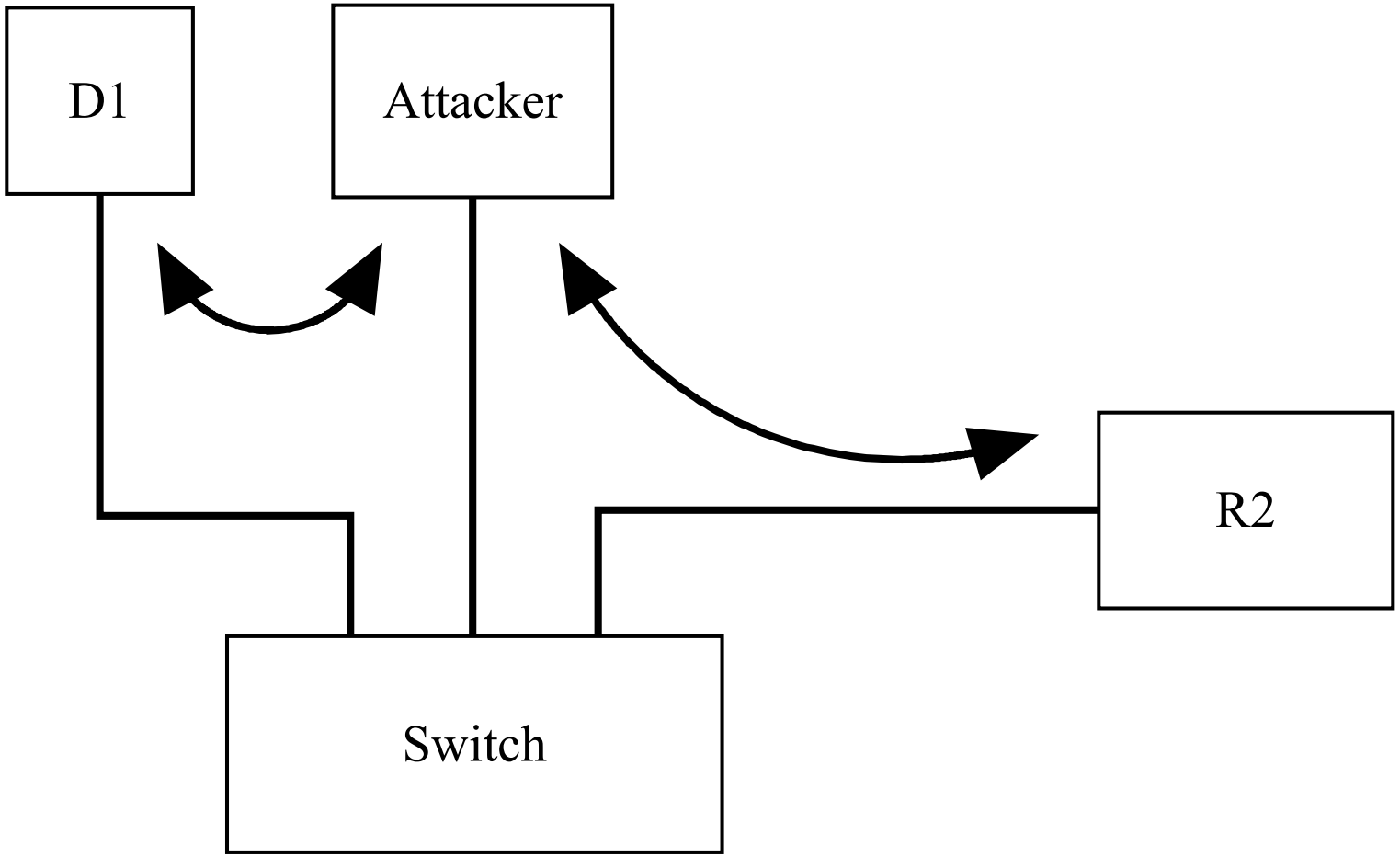
Authentication-Based

- 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

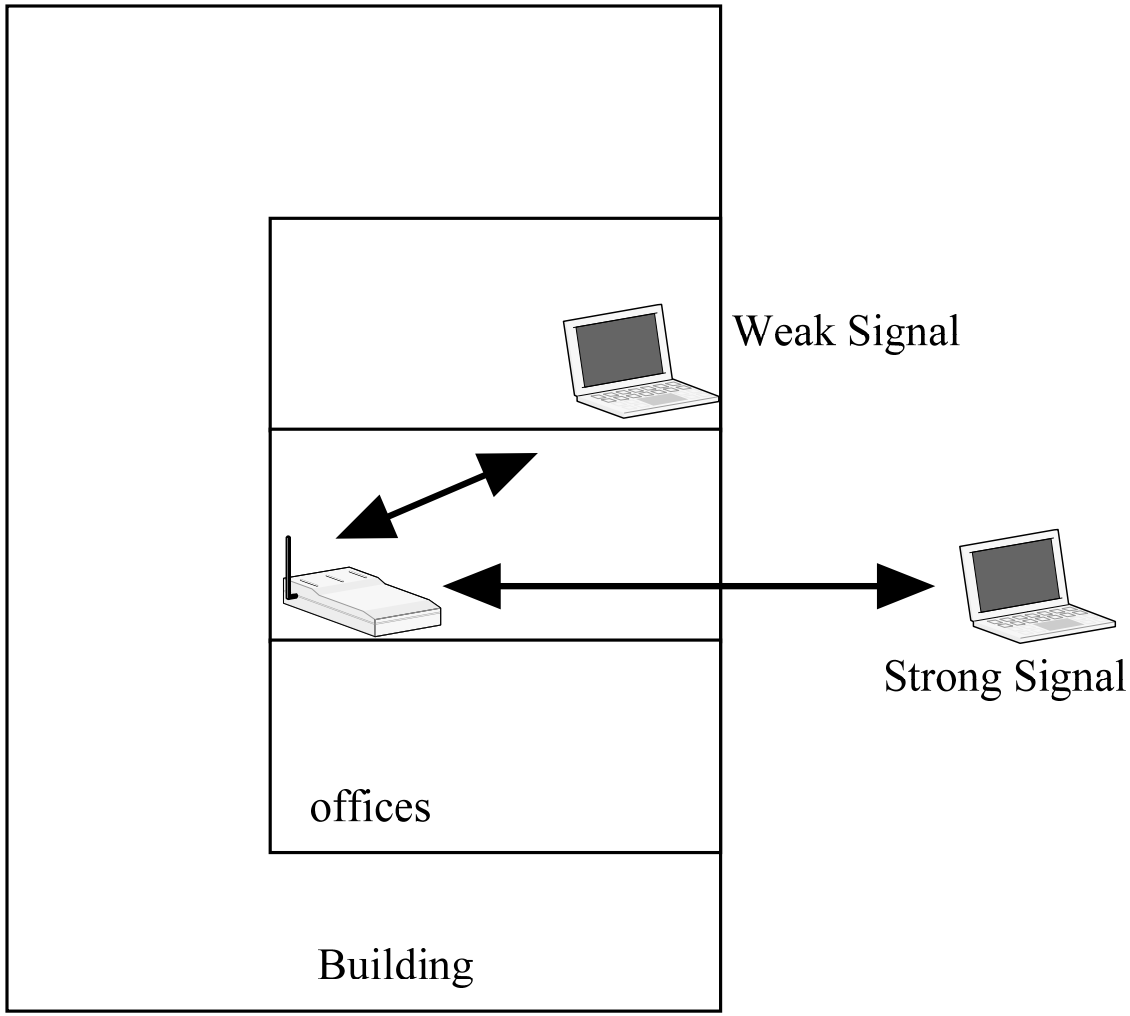
Wireless Security Topics

- Standards
- Devices
- Protocol
- Packet Format
- Vulnerabilities
- Mitigation

Wireless Standards

Name	Frequency	Data Rate	Max Distance
802.11a	5 GHz	54Mbps	30 meters
802.11b	2.4 GHz	11Mbps	30 meters
802.11g	2.4 GHz	11-54 Mbps	30 meters
802.11n	2.4 GHz	200-500 Mbps	50 meters

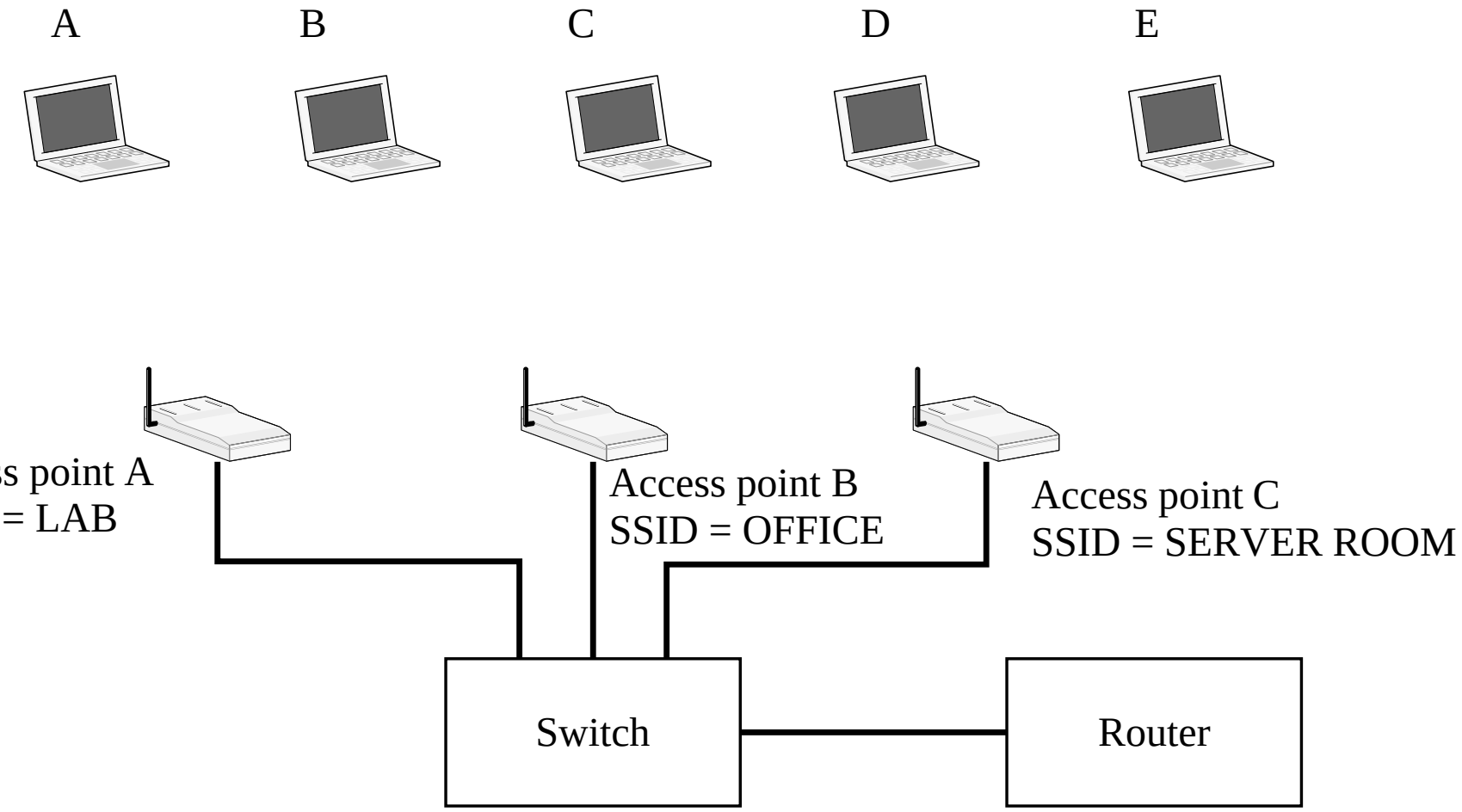
Signal Reflection



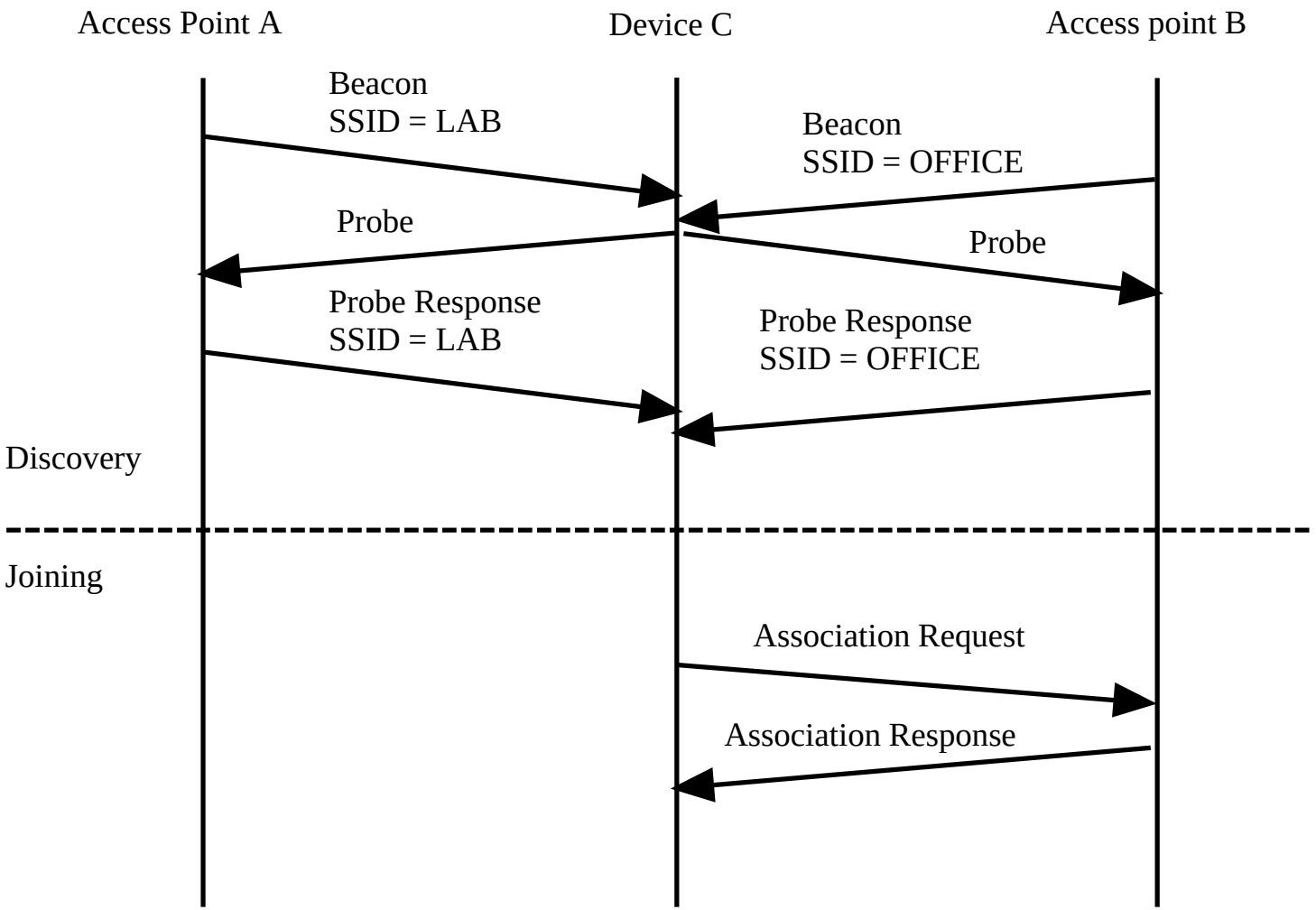
Wireless Ethernet 802.11

- Two topologies
  - IBSS Independent Basic Service Set
    - Ad-hoc, all stations are peers
  - ESS Extended Service Set
    - AP – Access points connected to a network
    - Station plus the AP form a BSS

Wireless Network Environment



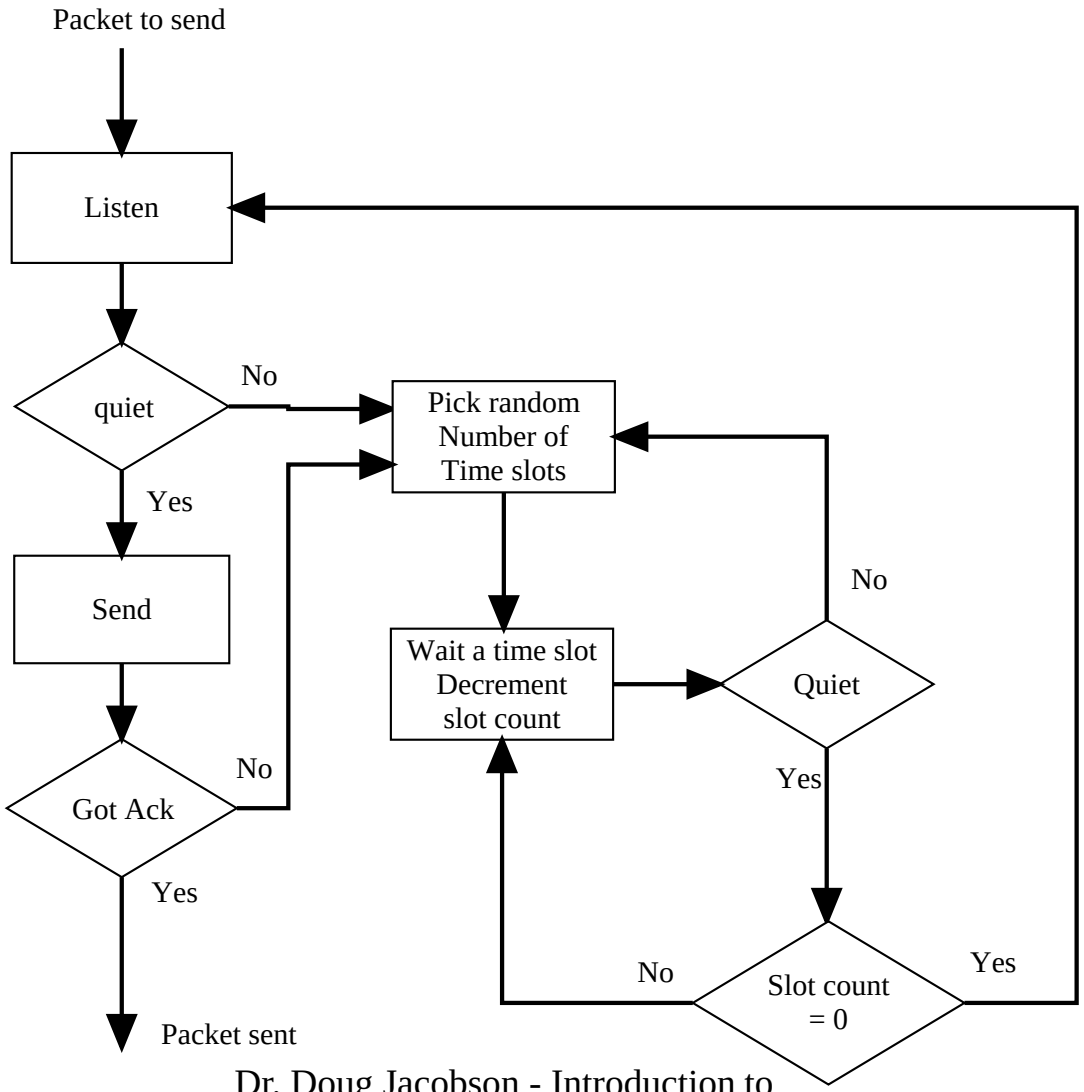
Discovery and joining



IEEE 802.11

- CSMA/CA
  - Wait till medium is free
  - Backoff after defer random amount
  - Exponential backoff for retransmission
  - Backoff timer resets if idle
  - Get an ACK if frame was received correctly

IEEE 802.11 Protocol

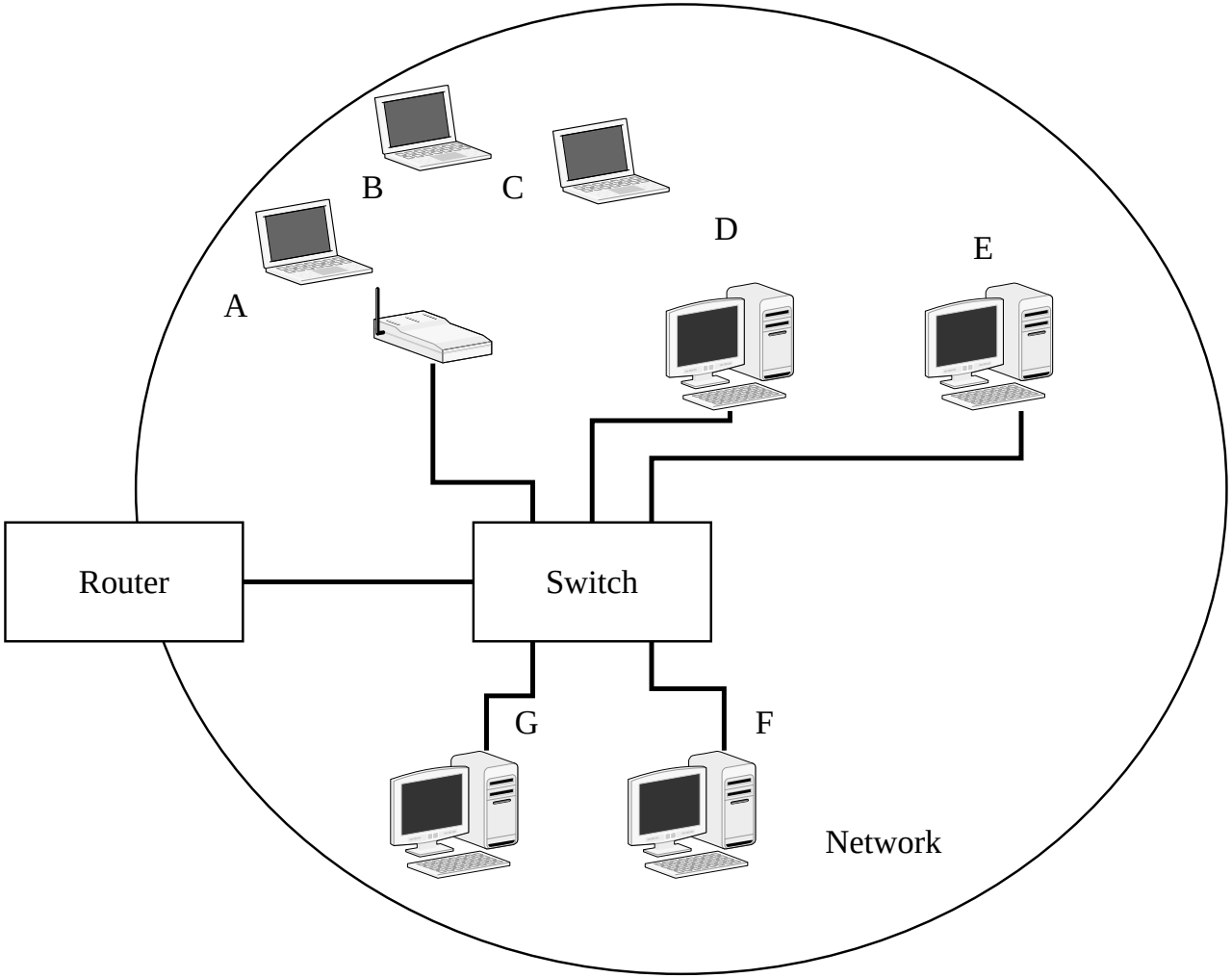


IEEE 802.11 Access Points

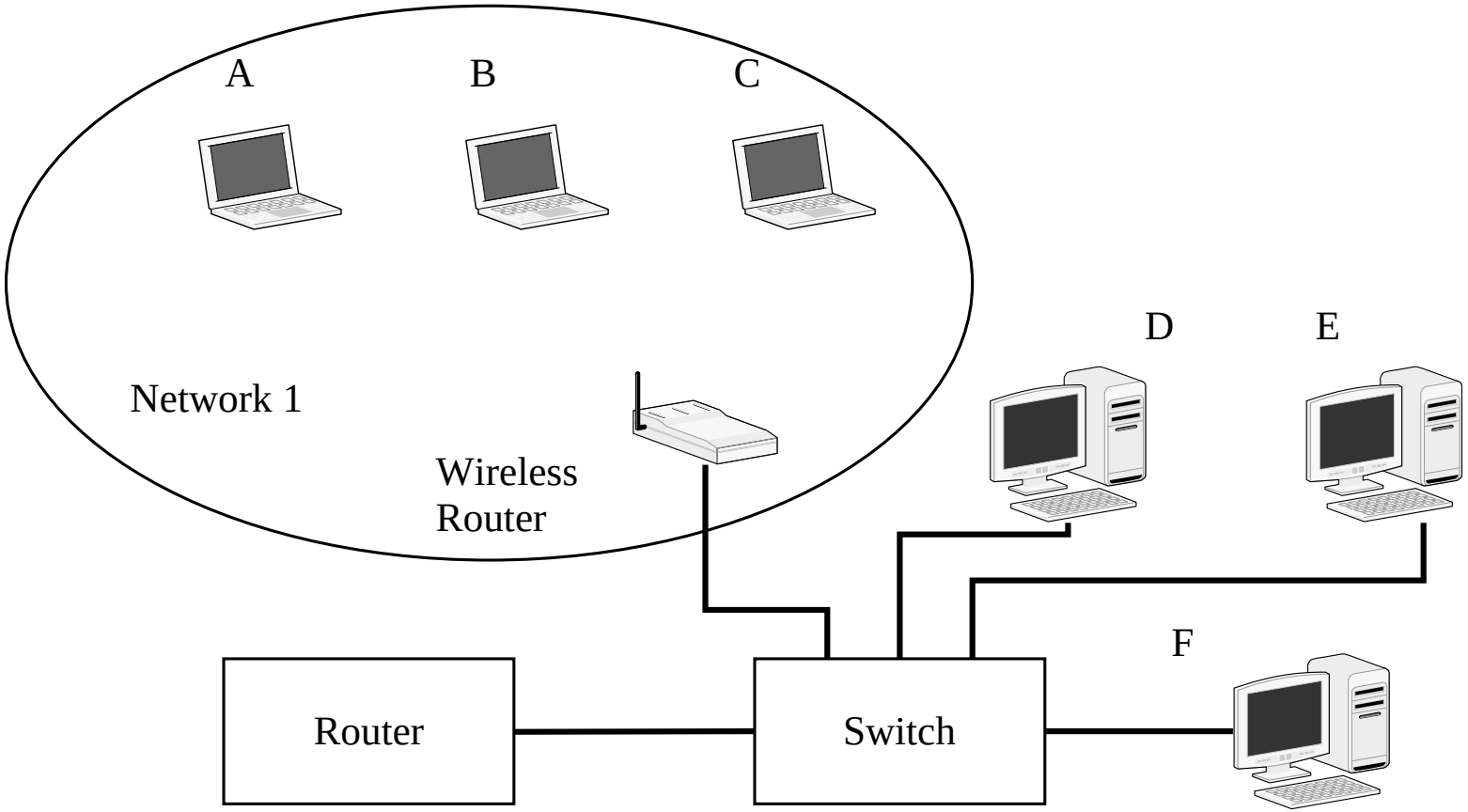
Two types

- Extended network
  - Access point makes the wireless devices look like they are on the same network as the wired devices
- Wireless router
  - Access point acts as a router

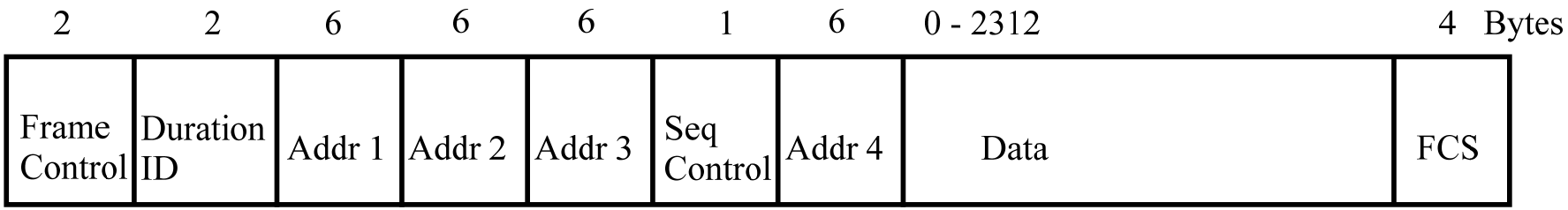
Extended Network



Wireless Router



802.11 Frame Format



- **Frame Control:** Used to identify the frame type and other frame specific information.
- **Duration/ID:** Used to manage the access control protocol.

Address 1: Used to identify the destination of the transmitted packet. This is used by the hardware controller to determine if the frame should be read. If it does not match the address of the controller the remainder of the frame is ignored.

802.11 Frame Format

- **Address 2:** Address of the transmitting device.
- **Address 3:** Used when the access point is part of an extended network where the access point will relay the traffic.
- **Address 4:** Used when the access point is part of an extended network where the access point will relay the traffic

802.11 Frame Format

- **Sequence Control:** Used by the acknowledgement process.
- **Data:** The data field contains the data. The data field length is limited to 2312 bytes. Wireless Ethernet does not have a minimum data length.
- **Frame Check Sequence (FCS):** This field is used to help verify that the frame has not been corrupted during transmission.

Header Based

- Setting the destination address as a broadcast address can cause traffic problems
- Denial of Service
  - Invalid headers will cause loss of access or loss of association
- Not easy to fix

Protocol-Based

- Protocol is simple and is in hardware
- Can transmit packets to cause Denial of service
- Jamming of signals by ignoring the protocol
- Very hard to stop

Protocol-Based

- Access point can broadcast its SSID
  - Wardriving
- www.wardriving.com
- www.worldwidewardrive.org

Wardriving How easy

- One laptop with wireless
- Free software
- GPS optional


SOUTH DAKOTA
MINNESOTA
WISCONSIN
UNITED STATES
IOWA
NEBRASKA
ILLINOIS
KANSAS
MISSOURI
Minneapolis
St. Paul
Sioux Falls
Sioux City
Omaha
Lincoln
Des Moines
Madison
Rockford
Peoria
Springfield
Cedar Rapids
Davenport
Iowa City
Rochester
Owatonna
Austin
Mason City
Ames
Fort Dodge
Waterloo
Dubuque
La Crosse
Eau Claire
Wausau
Mankato
Faribault
Albert Lea
Northwood
Clear Lake
Forest City
Webster City
Nevada
Marshalltown
Newton
Indianola
Osceola
Chariton
Leon
Bethany
Cameron
St. Joseph
Kansas City
Grand Island
Kearney
Hastings
Norfolk
Fremont
Columbus
Council Bluffs
Bellevue
Papillion
© 2001 Microsoft Corp. All rights

Wardriving

Mitigation:

- Do we need to mitigate it?
- Turn off broadcast of SSID
- Use encryption or Network Access Control (NAC) (make it an authentication problem)

SSID discovery

- Sometimes additional information is provided by the SSID that could help an attacker
- Business name
- Home address or user's last name

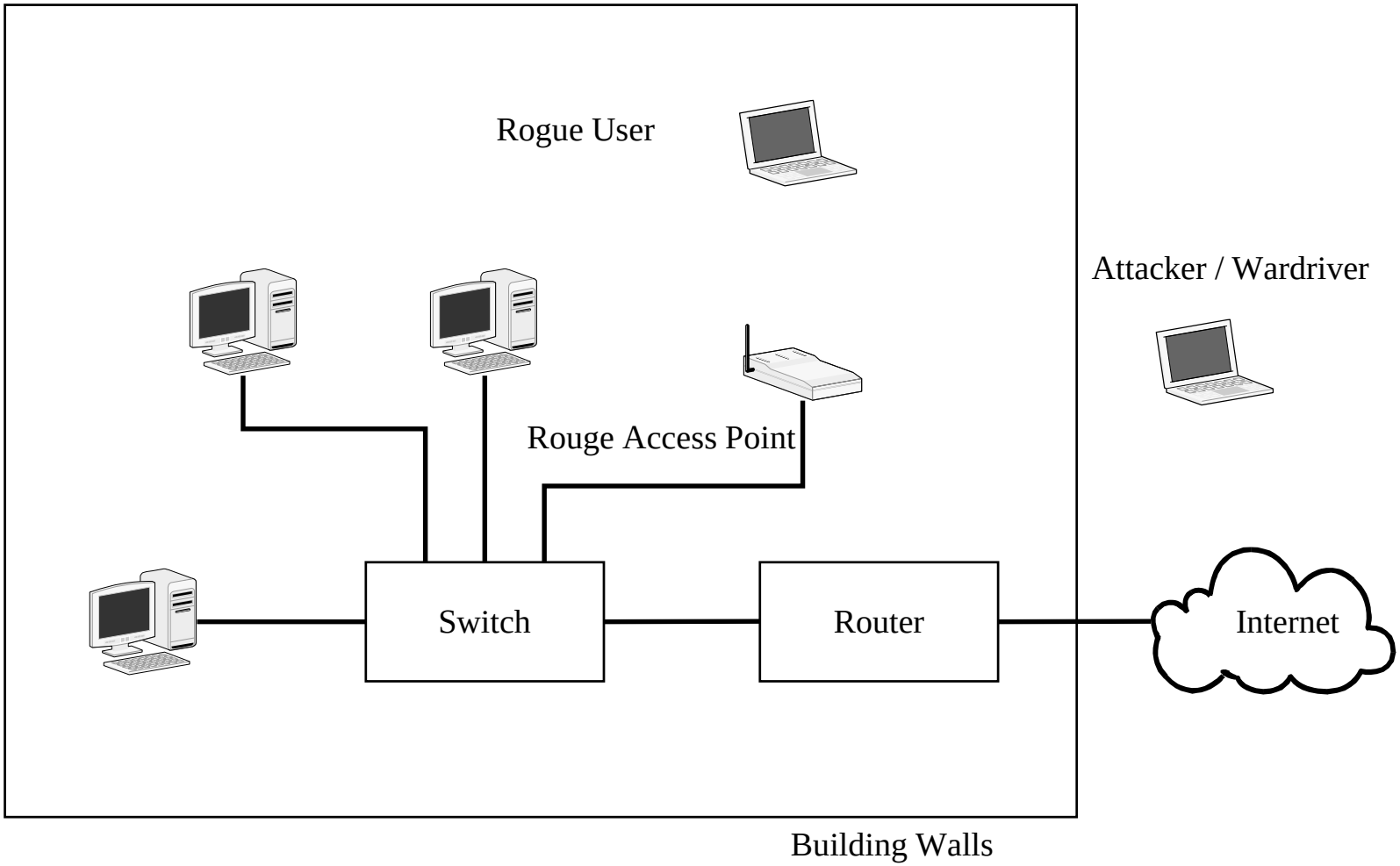
Authentication Based

- You can set the hardware address
- Hardware address is used as authentication in Access Points
- Device authentication
  - Access point authentication
  - Wireless device authentication
- Access point configuration authentication
  - Gaining access to the access point

Access point Authentication

- Rogue access point
  - Installed by valid user
- Fake Access point
  - Installed by attacker

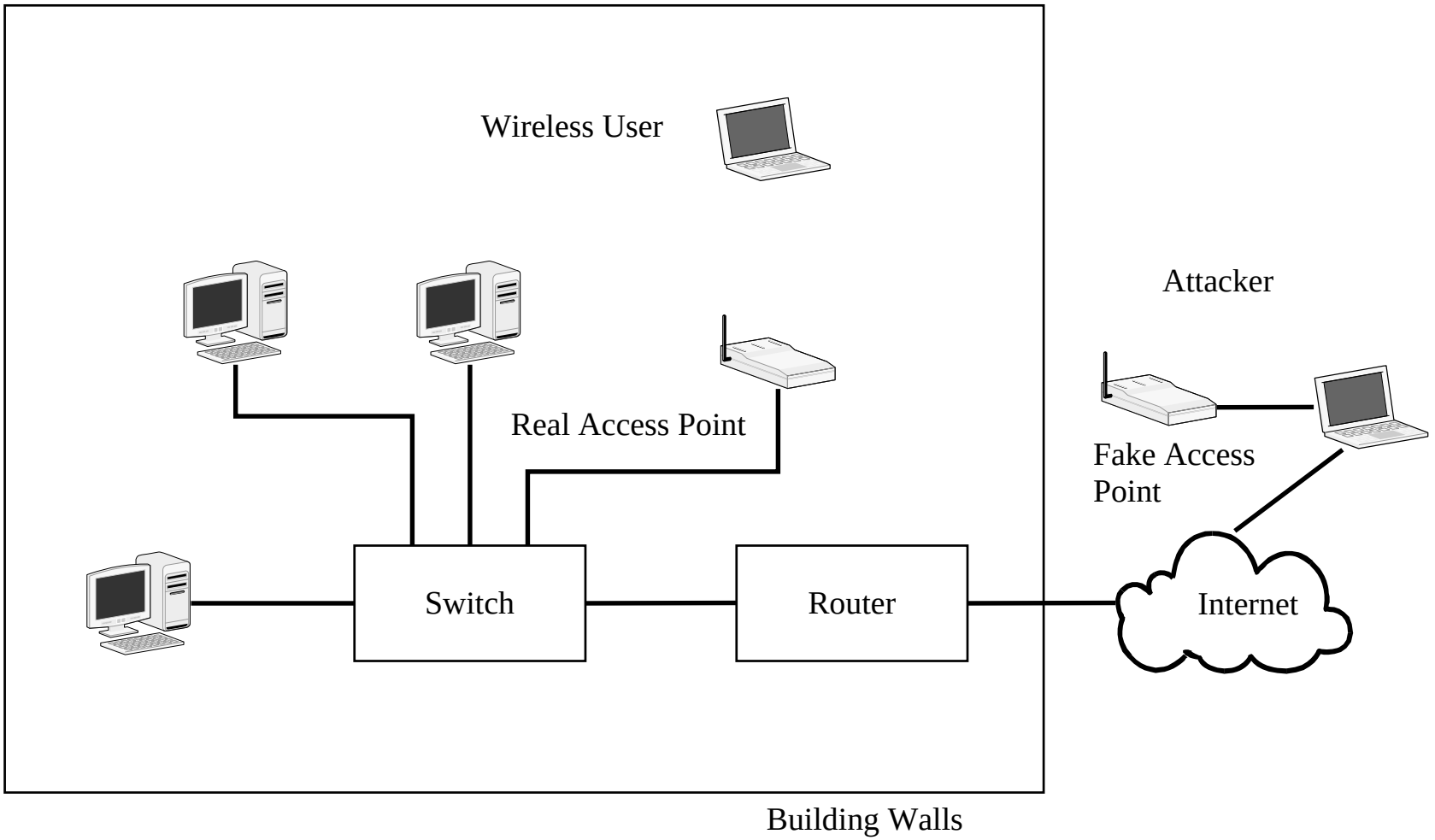
Rogue Access Point



Rogue Access Point

- Provides access to attacker
  - Intentional or unintentional
- Bypasses perimeter security mechanisms
- Hard to find and stop
  - Scan for SSID
  - Scan for wireless traffic
- NAC might provide some help.

Fake Access Point



Fake Access point

- Hard to fake an access point within an organization.
- Easier if the access point is a public access point with no encryption.
  - Not much to be gained by this

Access Point Configuration Authentication

- Access point are often configured over the network.
- They have default passwords
- An attacker could change security settings

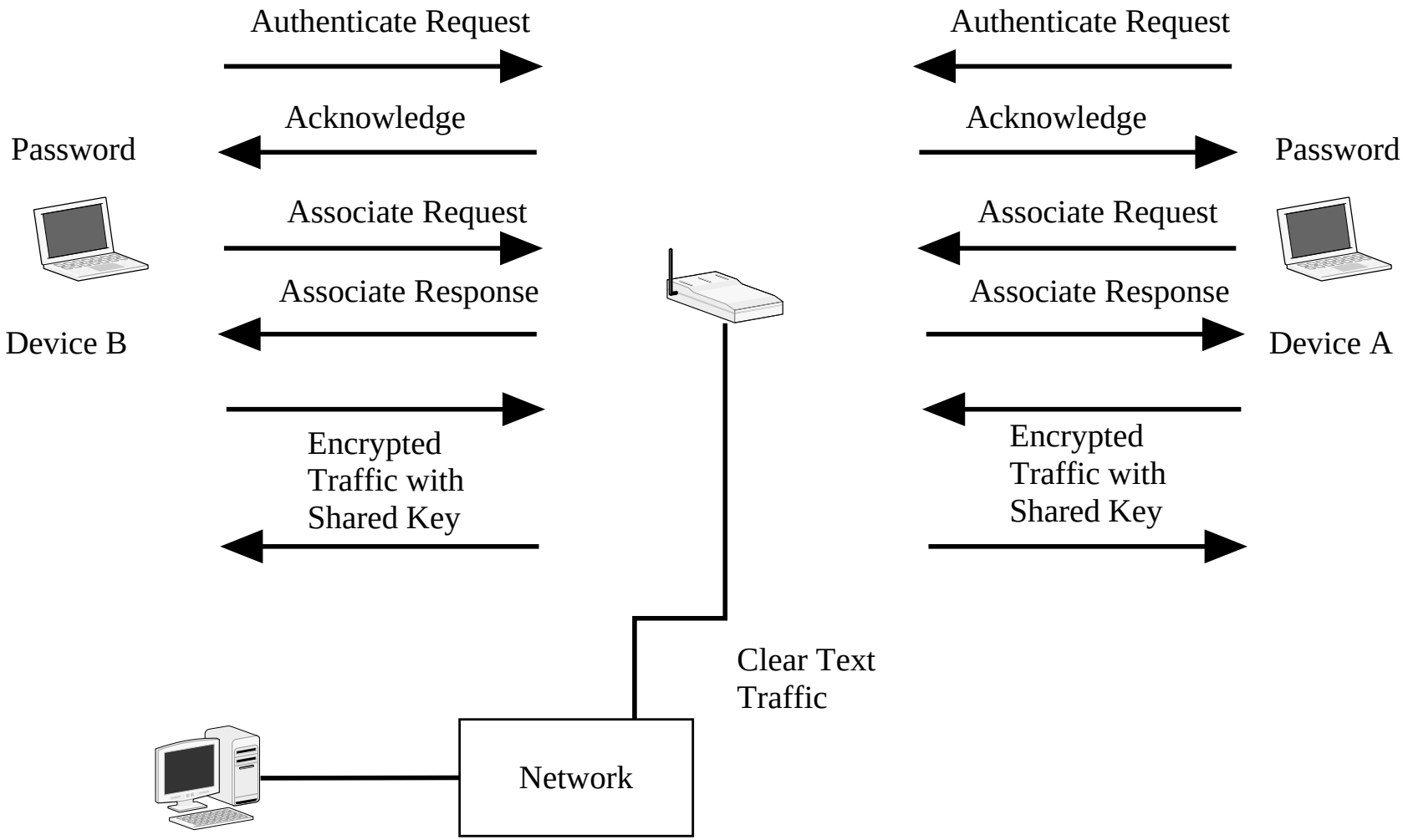
Traffic Based

- Ethernet controllers can be set in promiscuous mode which enables them to sniff traffic
- Broadcast traffic can cause flooding

Wired Equivalent Privacy (WEP)

- Shared keys
  - 40 bits
  - 128 bits
- Can be cracked if enough data is seen
- Aircrack will find a WEP key

WEP


Authenticate Request
Acknowledge
Password
Associate Request
Associate Response
Device B
Encrypted
Traffic with
Shared Key
Authenticate Request
Acknowledge
Password
Associate Request
Associate Response
Device A
Encrypted
Traffic with
Shared Key
Clear Text
Traffic
Network

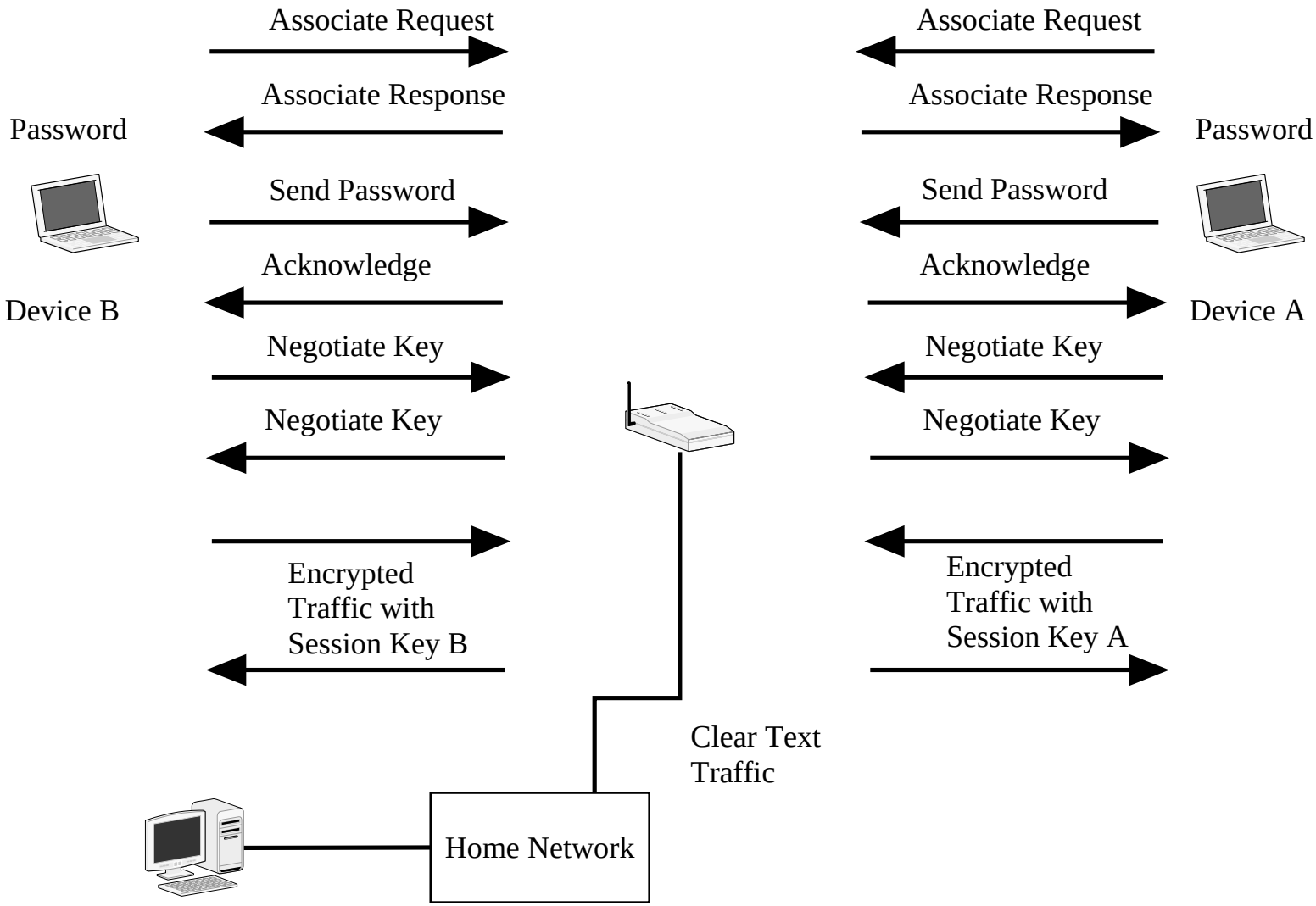
Wi-Fi Protected Access (WPA)

- Uses 802.1X + Extensible Authentication Protocol
  - Authentication with an auth server
- Encryption
  - Rc4
  - AES (WPA2)

WPA – Home use

- Uses a shared password for authentication
- If mobile password matches AP then encryption keys are exchanged
- New keys for each new association

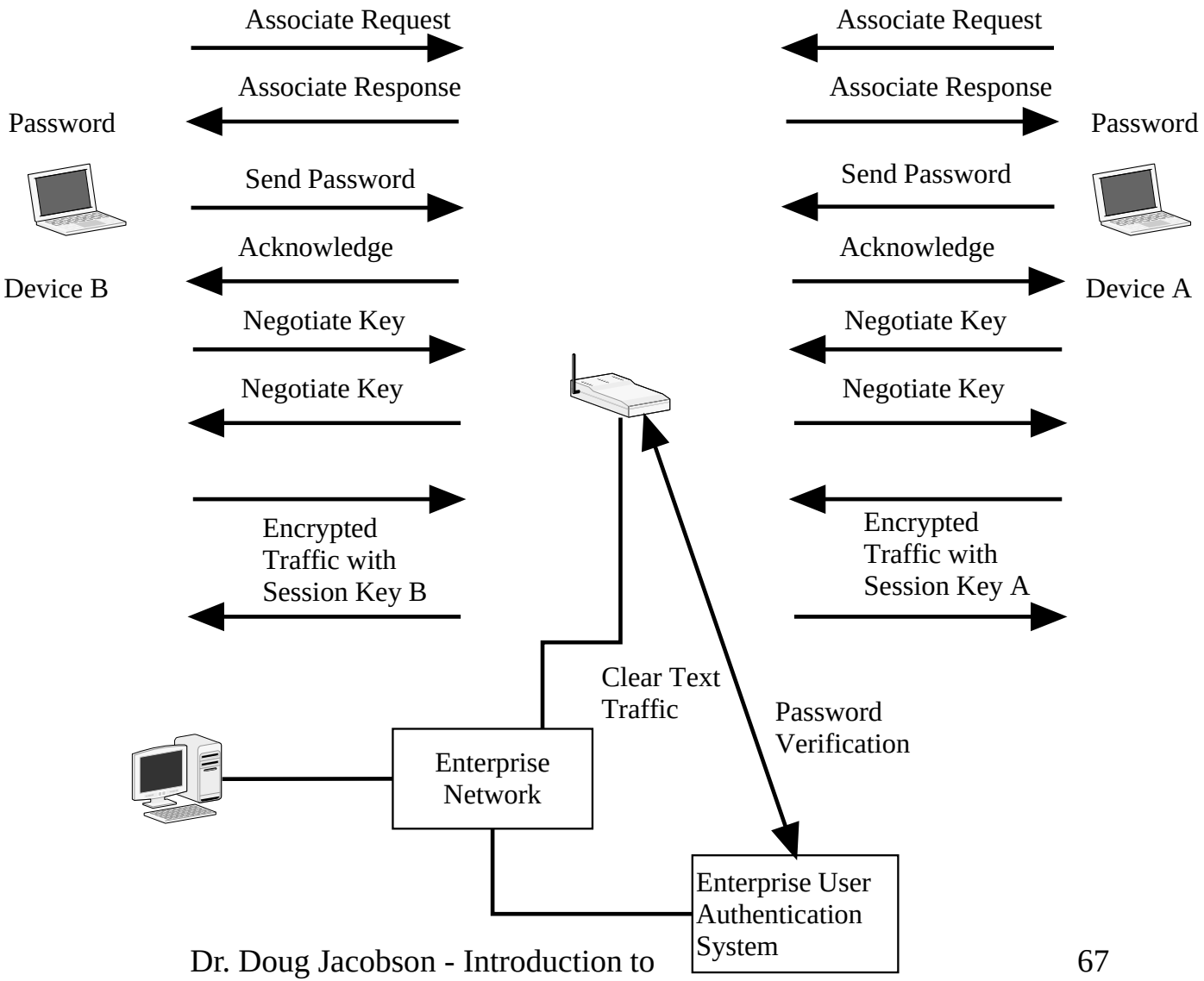
Home-Based WPA



WPA – enterprise

- Mobile associates with AP
- Mobile authenticates with auth server (using 802.1X)
- Authentication server distributes keys to AP and mobile

Enterprise WPA



Wireless (A world without perimeters)

- Wireless can create a new perimeter
  - Know access points
  - Unknown access points
- Treat your wireless access points the same as you would any remote access to your network.
  - Monitor it
  - Filter it
  - Protect it

Why is Wireless different?

- Most security models are based on a strong perimeter around an organization
- Wireless signals are not confined to the walls of an organization
- Wireless technology is plug and play
- Security makes wireless harder to use.

How to secure your wireless network

- Control your broadcast area
- Enable WEP, use WPA if possible
- Disable SSID Broadcast
  - More work to setup clients
- Change default AP settings
- Don’t choose descriptive SSID
- Restrict associations to MAC addresses

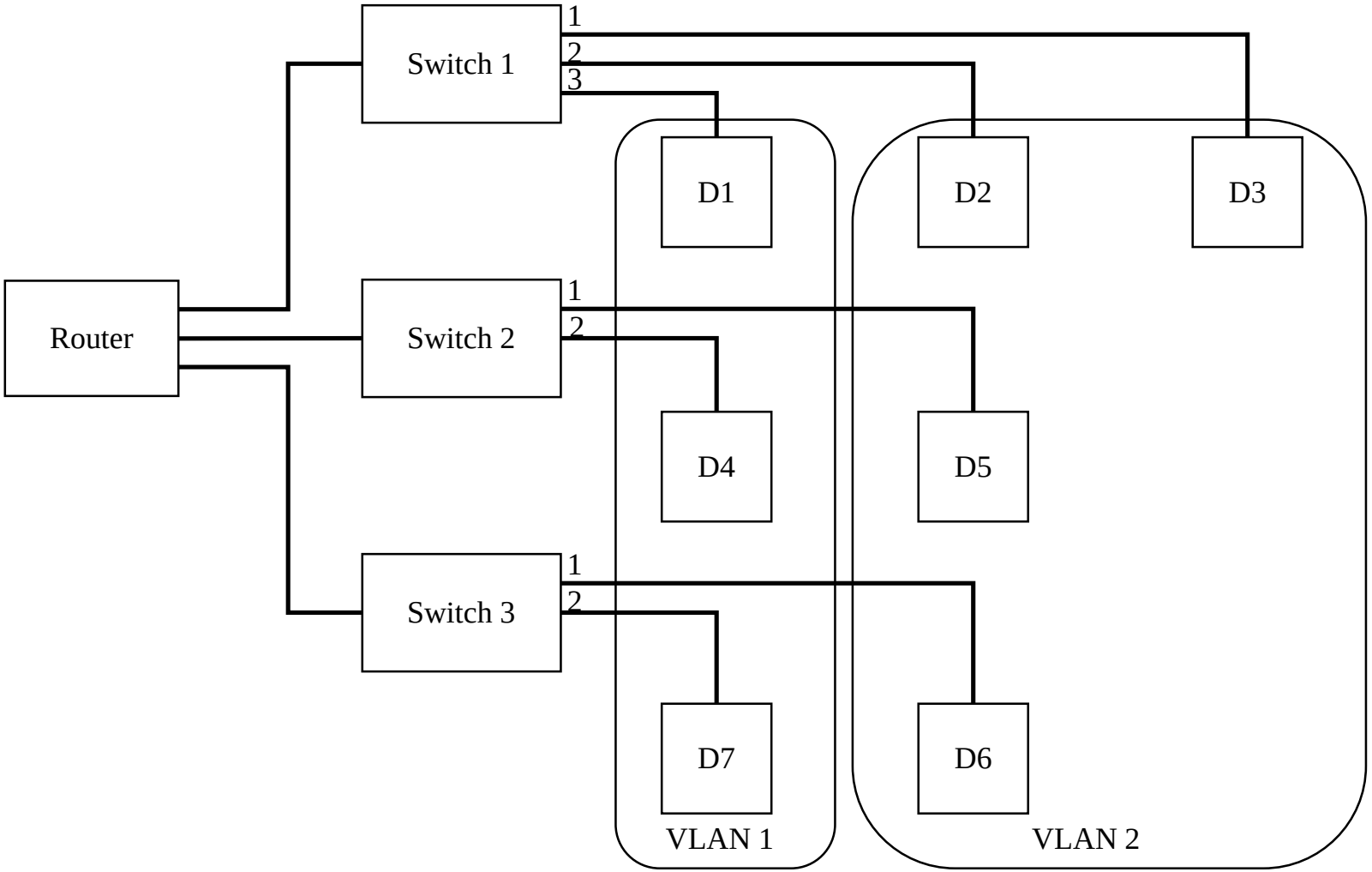
General Mitigation Methods

- VLAN
- NAC

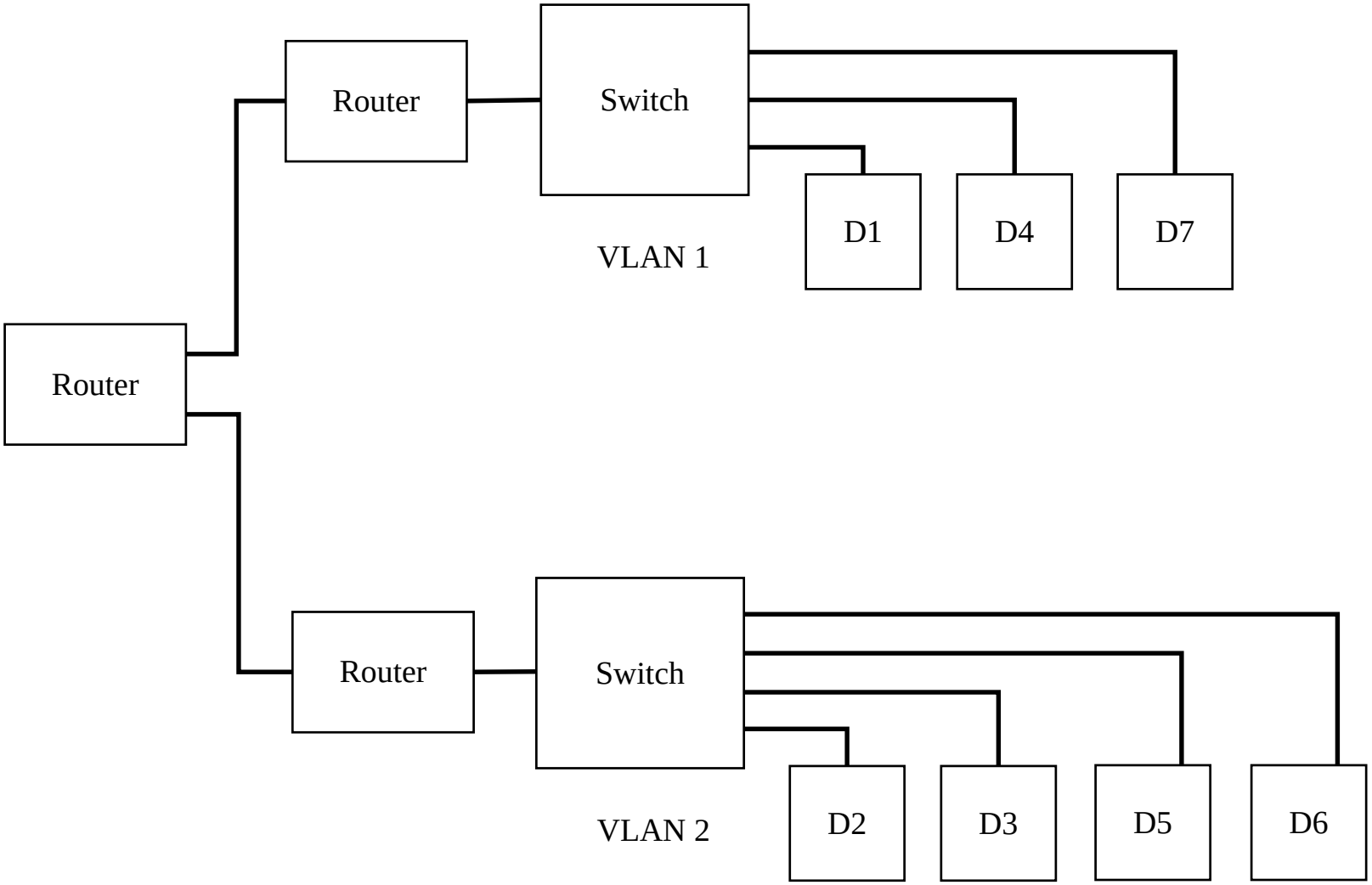
VLAN

- Virtual Local Area Network
  - Creates virtual networks where traffic is isolated between each VLAN based on the hardware address
- Two types
  - Static: each port on the switch is part of a VLAN
  - Dynamic: VLAN assignment is based on hardware address

VLAN


Switch 1
1
2
3
D1
D2
D3
Router
Switch 2
1
2
D4
D5
Switch 3
1
2
D7
D6
VLAN 1
VLAN 2

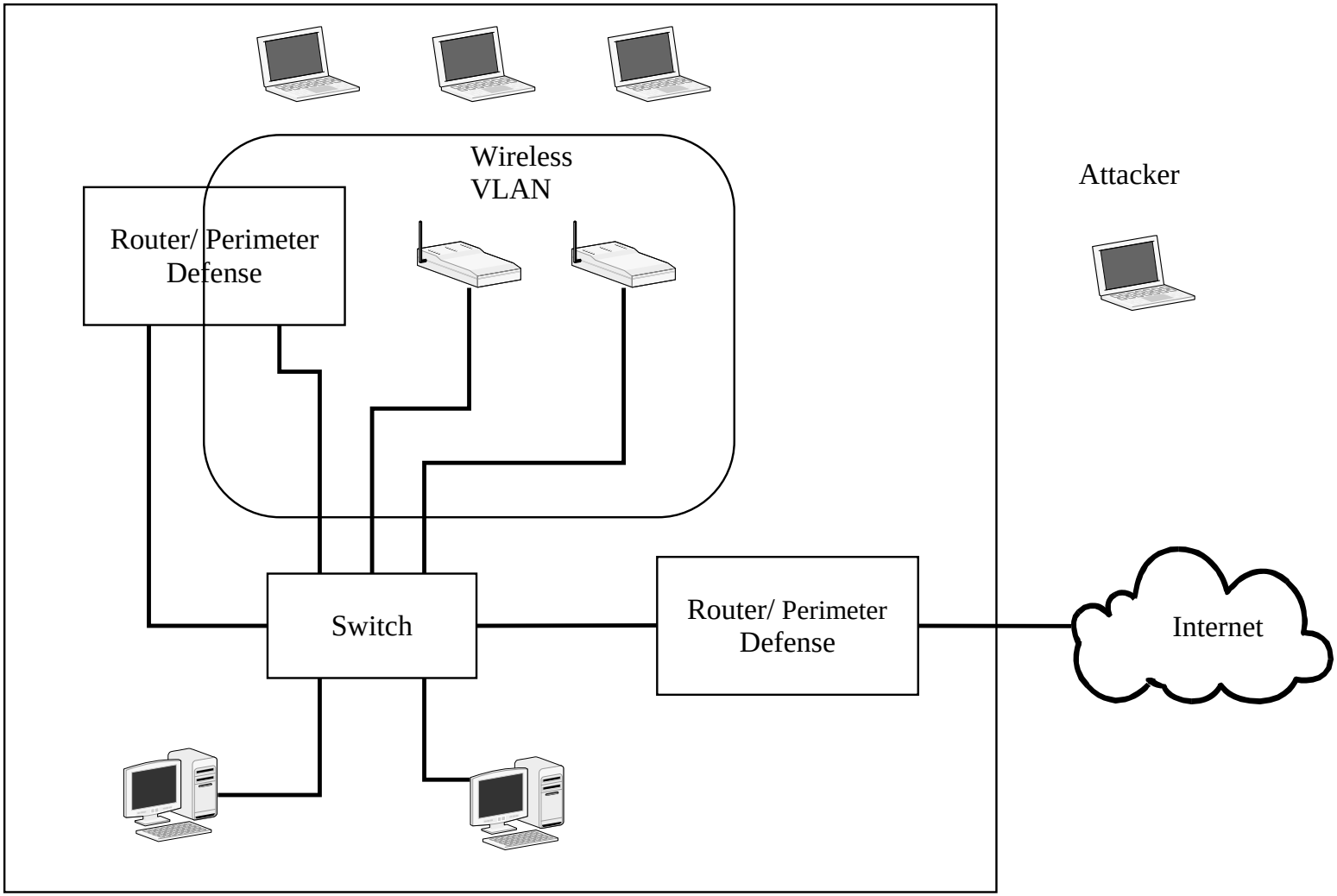
Logical View of VLAN



VLAN Security

- A VLAN will separate traffic, but will not protect devices inside a network from other devices in the same network
- Dynamic VLAN can be fooled by changing the MAC address
- Can help in wireless security

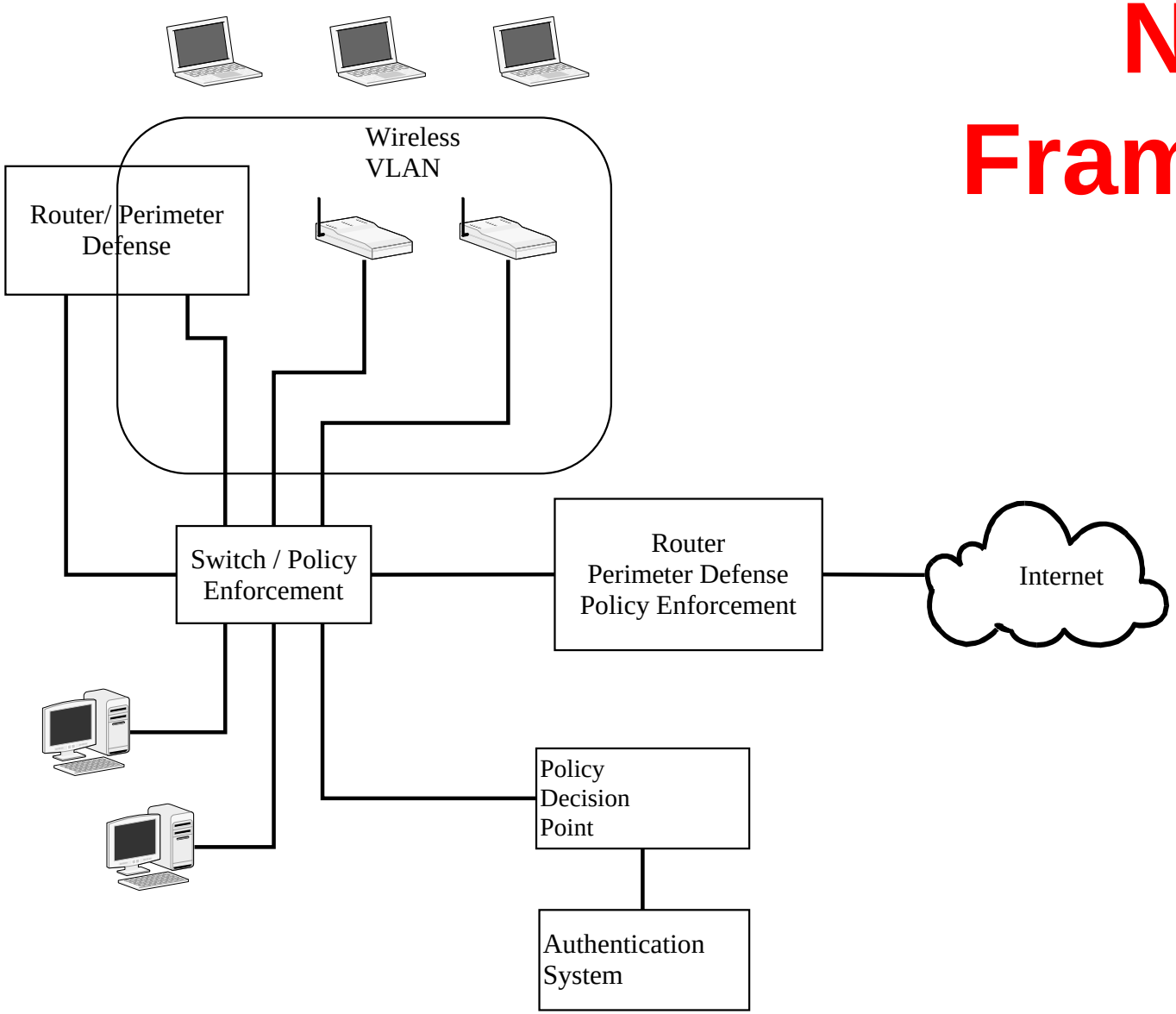
Wireless VLAN



Network Access Control

- Only allow trusted devices on the network
- A host has software that involves an assessment of the host (virus software, etc.)
- Hosts asks policy server if it can use the network
- Network will enforce the policy (limited or full access)

NAC Framework



NAC

- Limited use today
- Focuses on misconfigured or infected devices

Physical Network Security

- Protection methods are limited to local network
- Provides limited security