Introduction to Network Security

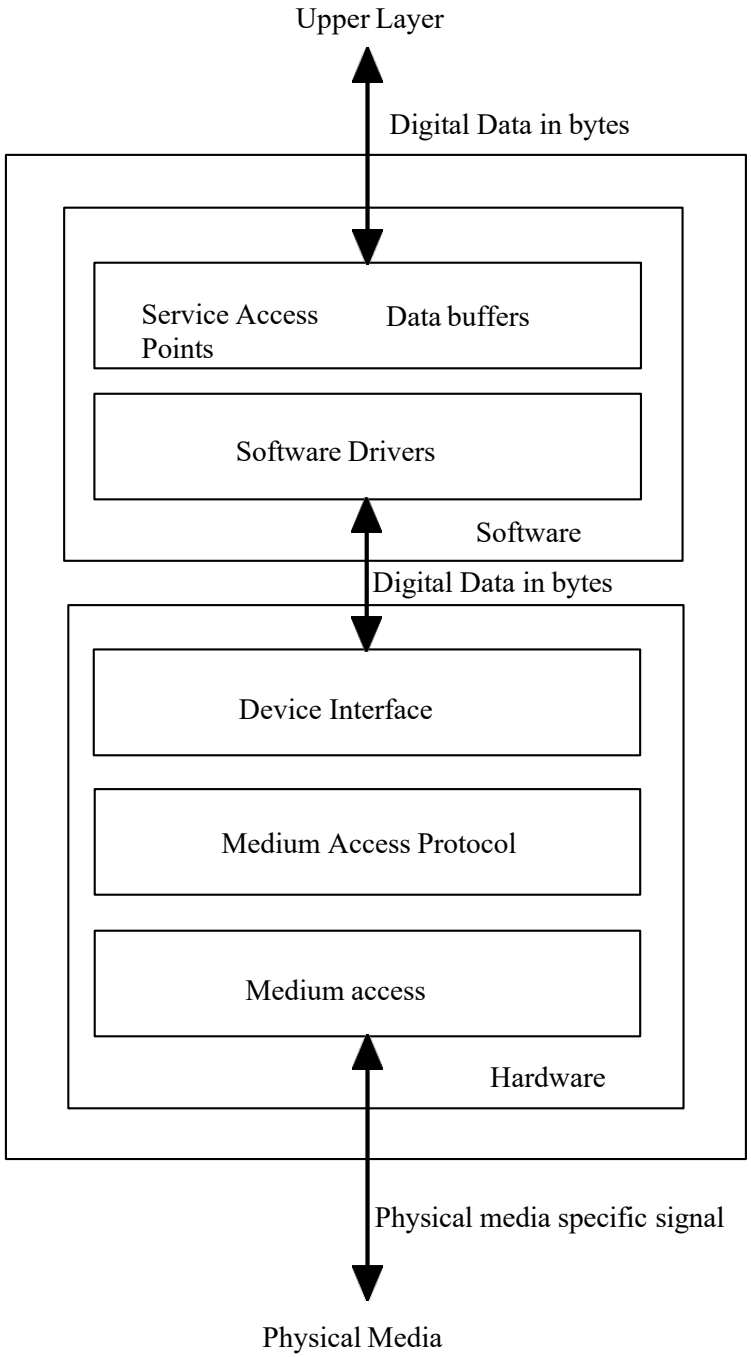
Chapter 5

Physical Network Layer

Topics

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

Physical Network Layer

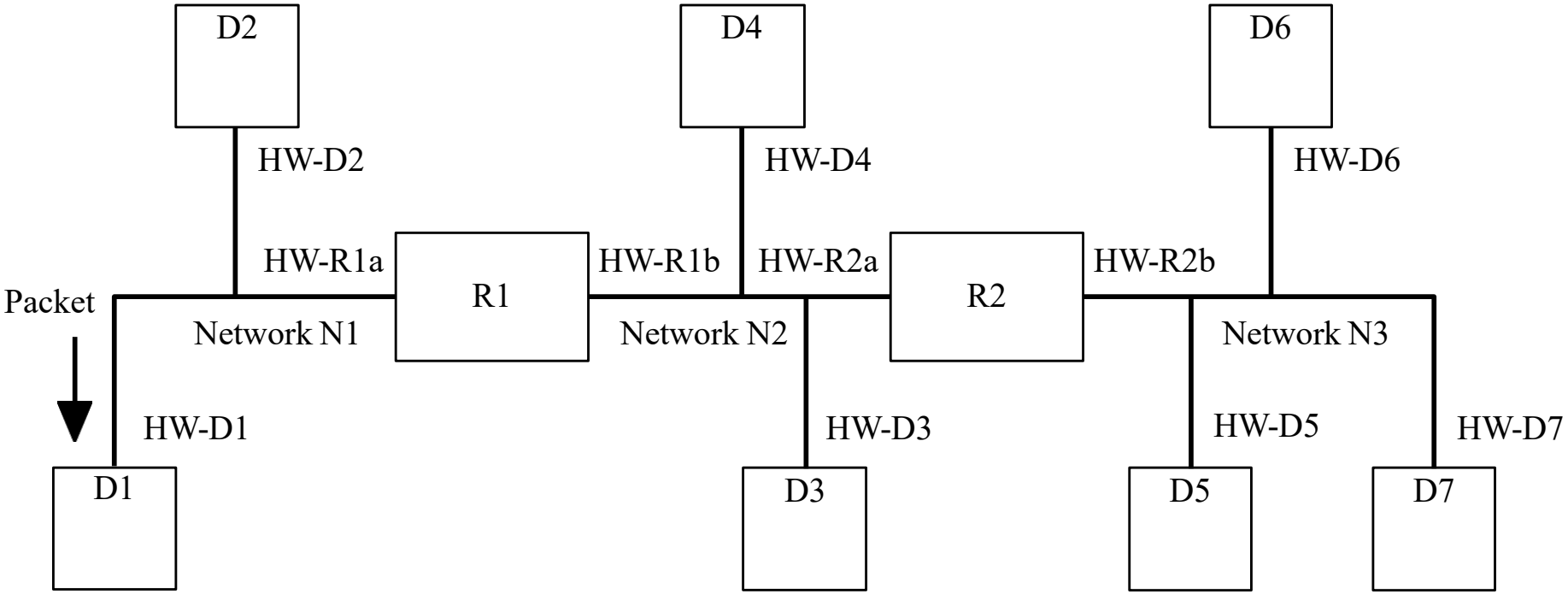


Common Attack Methods

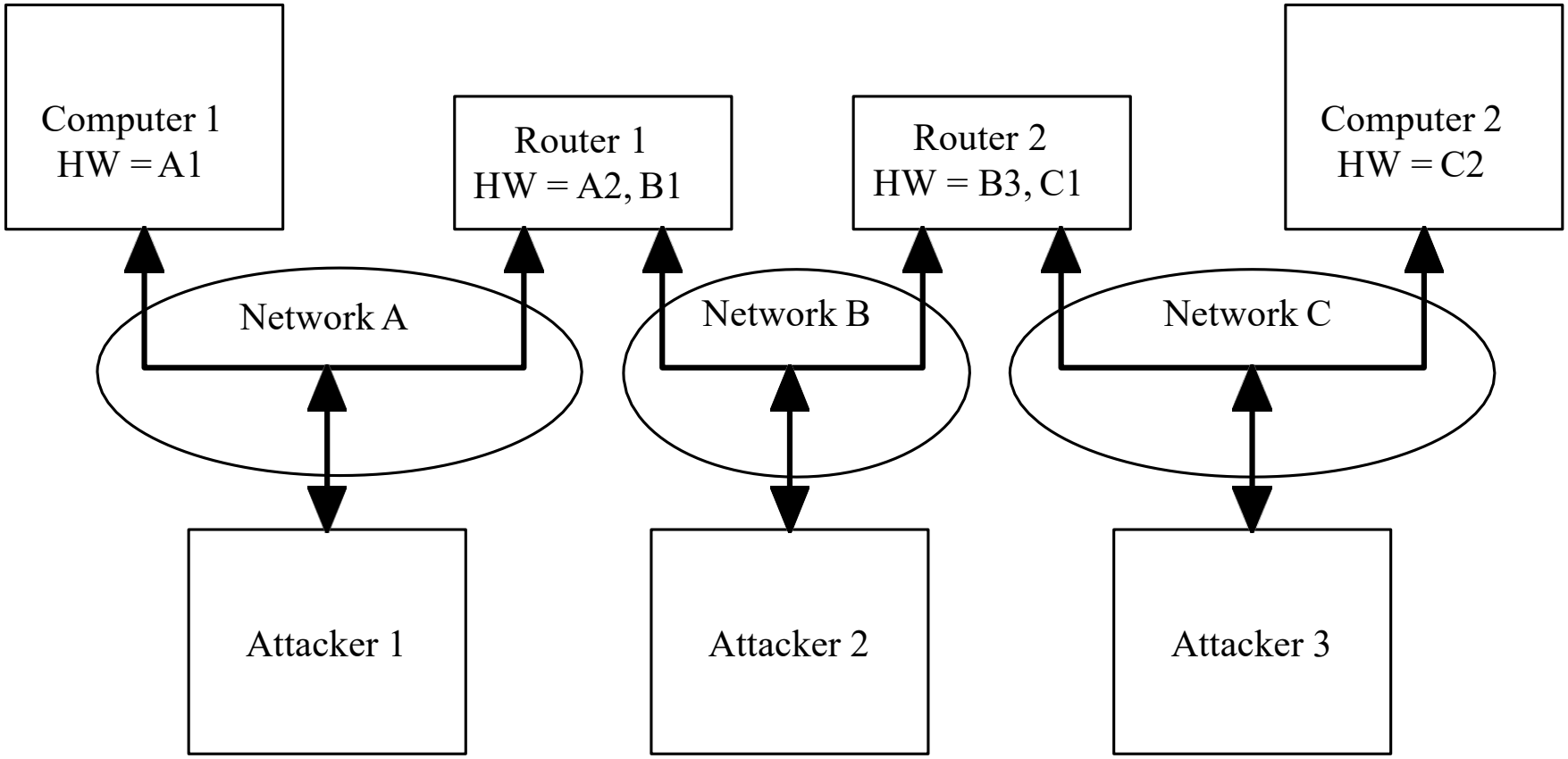
- Spoofing
- Sniffing
- Physical Attacks

?欺骗
?嗅探
?物理攻击

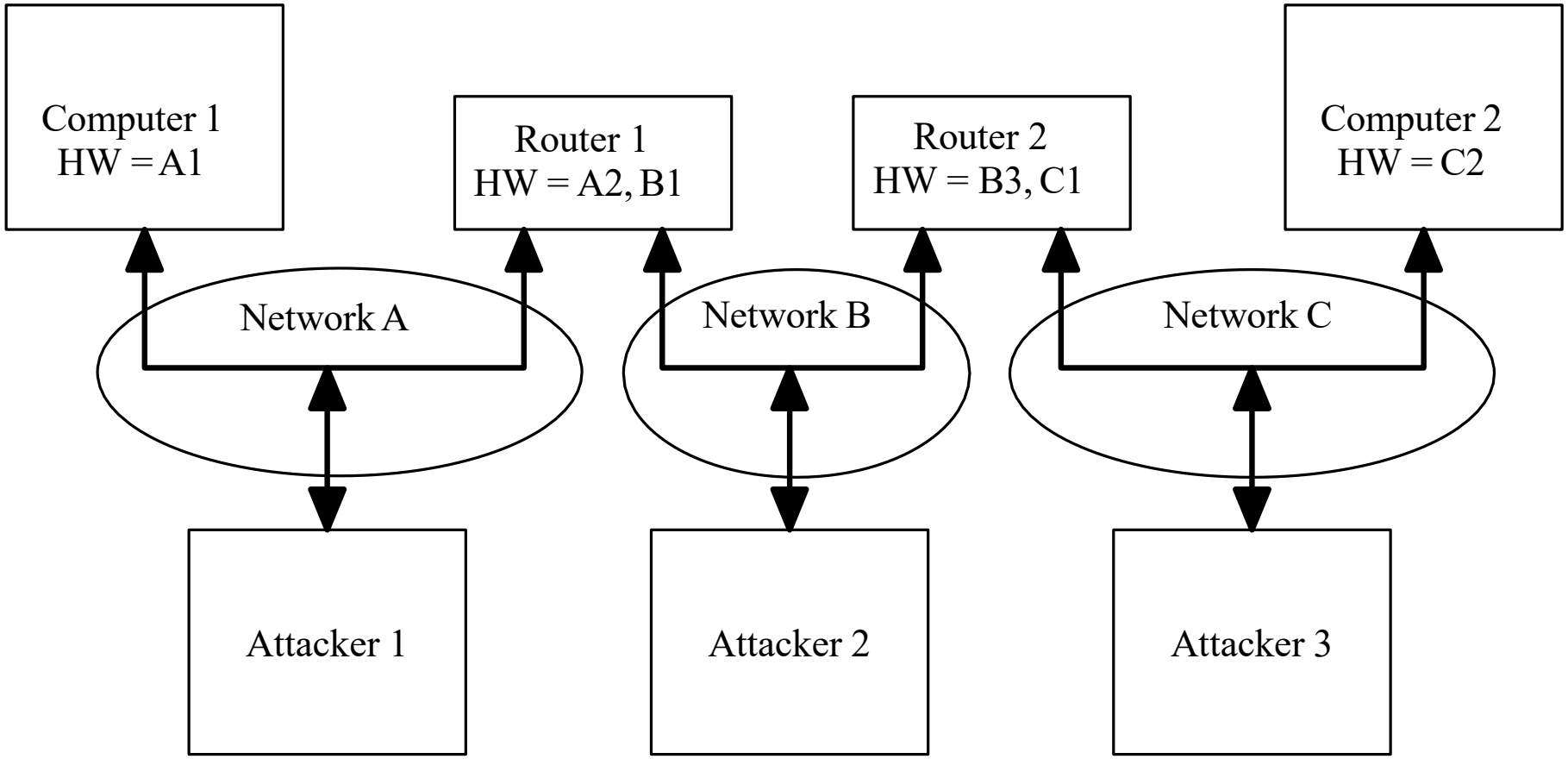
Hardware Addressing



Hardware Address Spoofing



Network Sniffing



Physical Attacks

- Bad network cable 网线损坏
- Network cable loop (both ends plugged into the same device) 网线环(两端插入同一设备)
- Bad network controller 坏的网络控制器
- Two network controllers with the same hardware address 两个具有相同硬件地址的网络控制器

Wired Network Protocols 有线网络协议

- Many protocols
  - Token Ring 、 Ethernet、 FDDI ….
- Local Area Networks (LAN)
  - Ethernet is the most common
- Wide Area Networks (WAN)

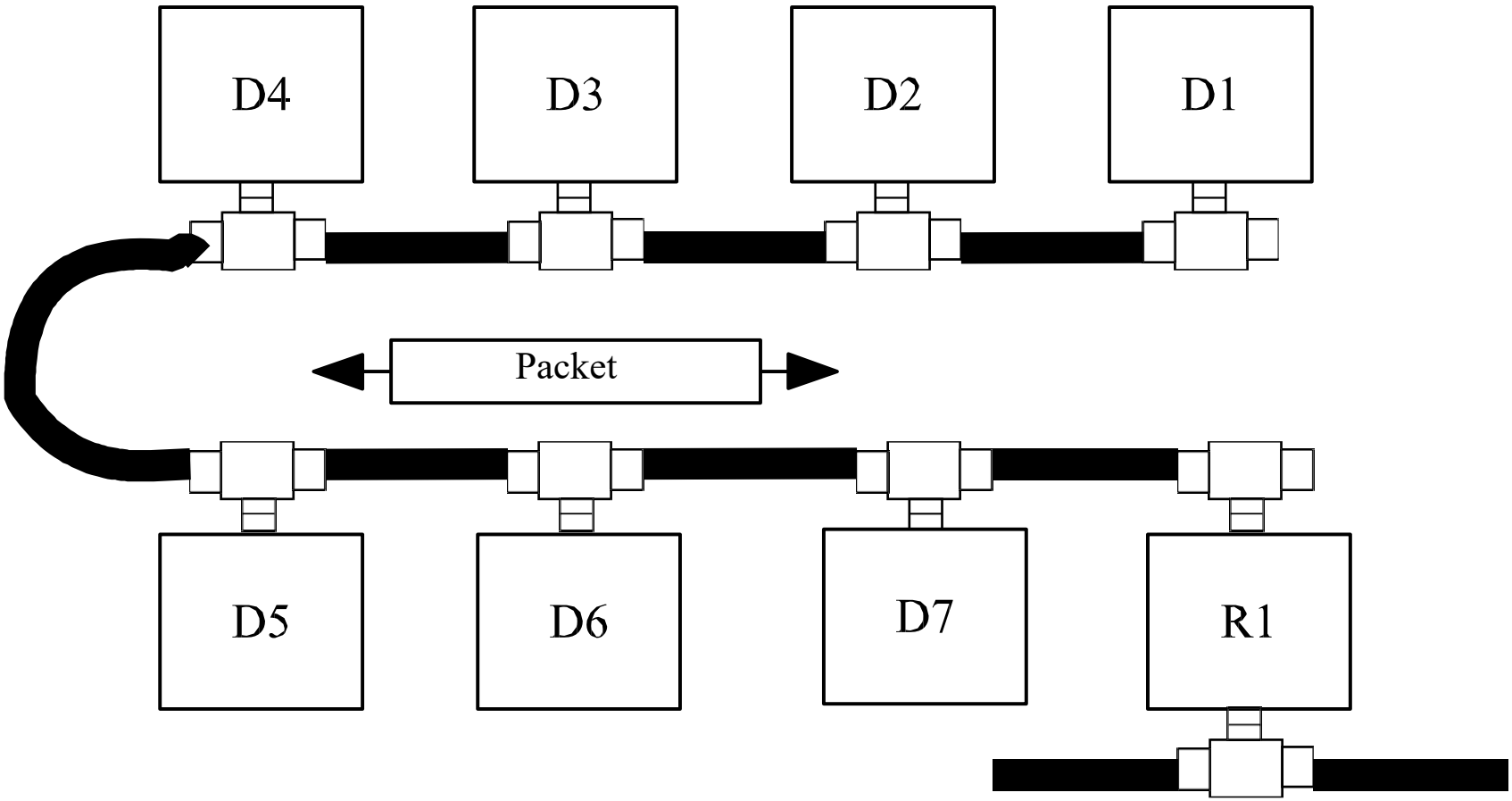
Ethernet

- 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 如果不止一个人同时说话，请后退
  - 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 使用最小数据包长度来保证碰撞可以被所有机器看到。这也限制了电缆的长度

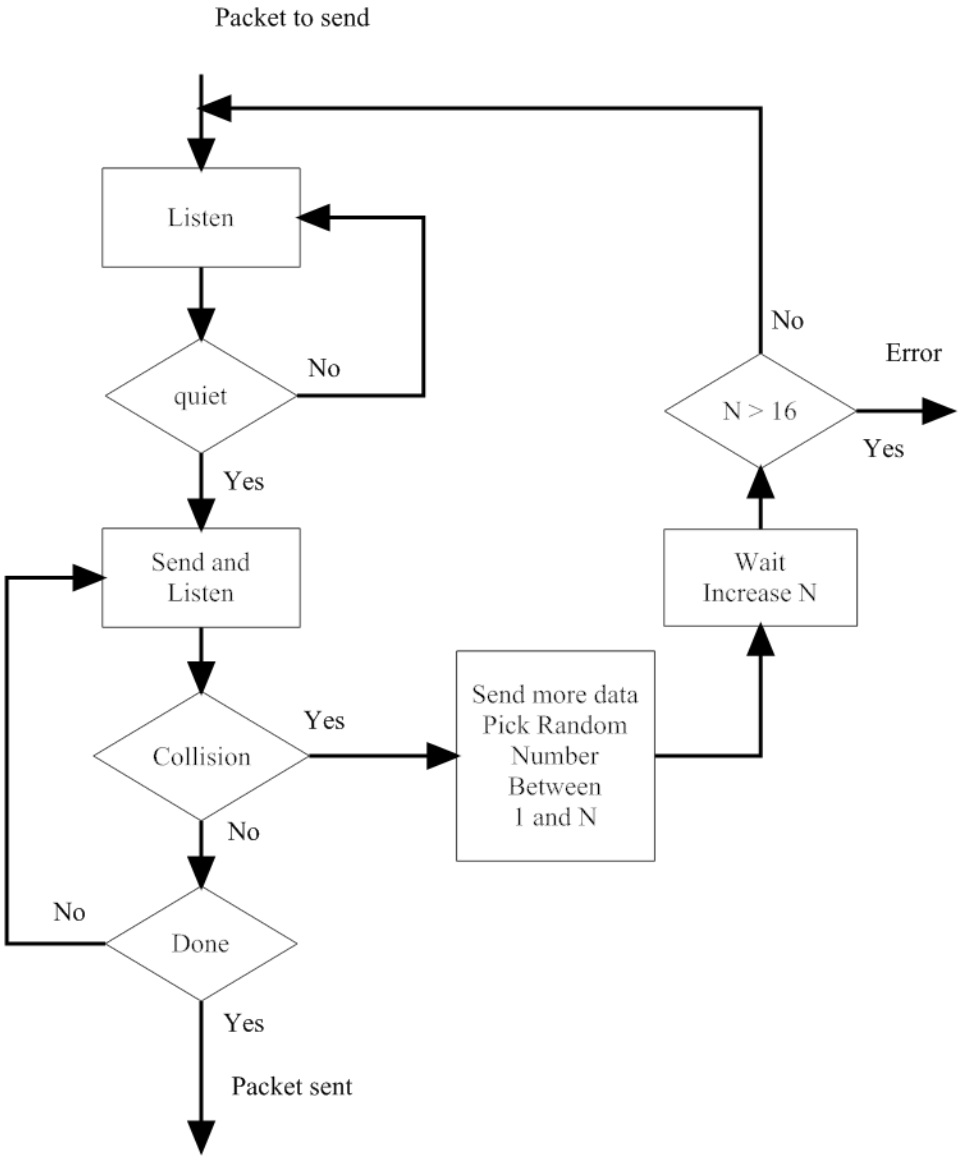


Figure 5.5 CSMA/CD Ethernet Protocol

Ethernet Collision Domain

以太网冲突域

- The range that is effected when a collision occurs. 碰撞发生时受到影响的范围
- 10Mbps Ethernet it is 2500 Meters

10Mbps的以太网是2500米

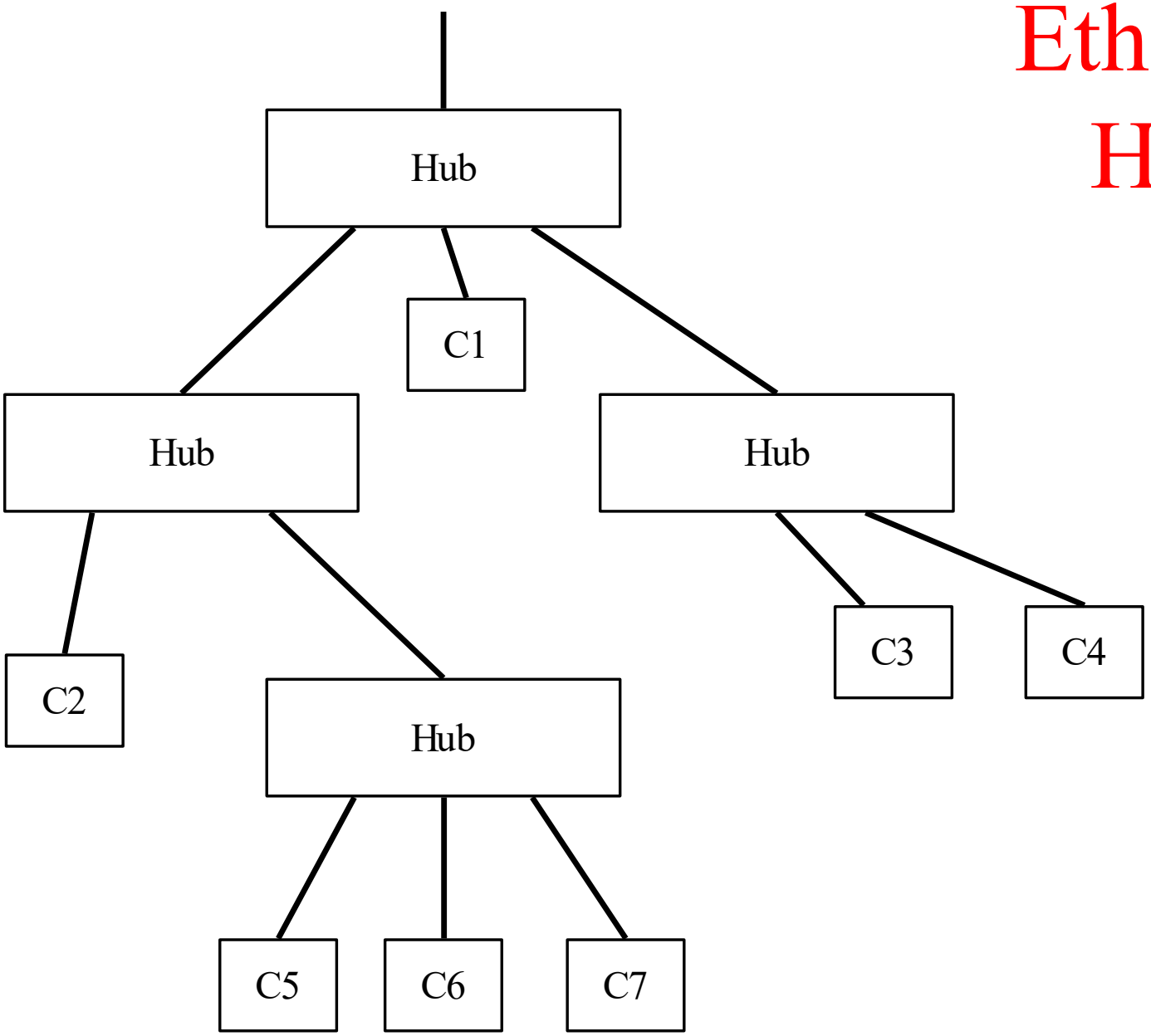
- This can be changed by using switches and routers (more later)

这可以通过使用交换机和路由器来改变

Connecting Devices 连接设备 /

- Repeater (physical layer only) 中继器 仅物理层
- Hub (multi port repeater) 集线器(多端口中继器)
- Bridge (layer 2 only) 桥接(仅限第2层)
- Router (layer 3) 路由器(第三层)
- Layer 2 switch
- Layer 3 switch

Ethernet Hubs

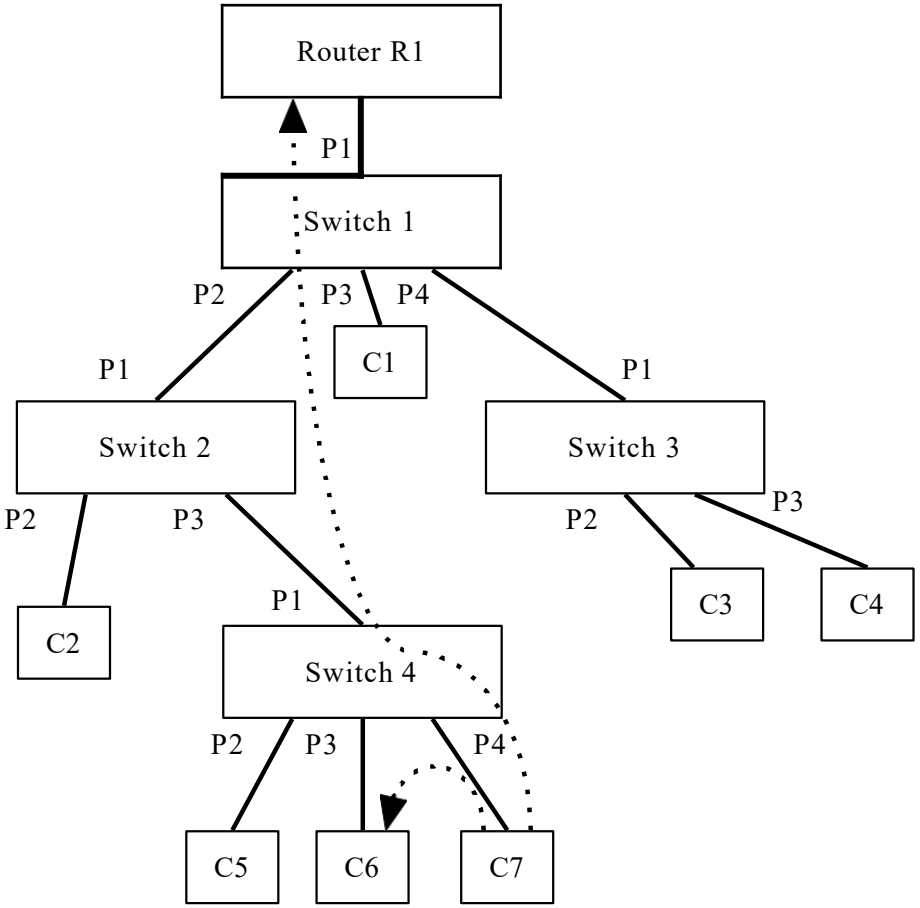


Ethernet switches 以太网交换机

- Collisions can slow the network down 碰撞会使网络变慢
- Switches create multiple collision domains
  交换机会创建多个冲突域
- Typically one machine per leg of the switch
  一般情况下，交换机的每条腿都有一台机器
- Switches only pass traffic to the leg of the switch where the destination is located
  交换机只将流量传递到目的地所在的交换机分支
- Switches reduce the traffic on each leg
  - Problem with network monitoring

交换机减少了每条腿上的交通流量
-网络监控问题

Ethernet Switch



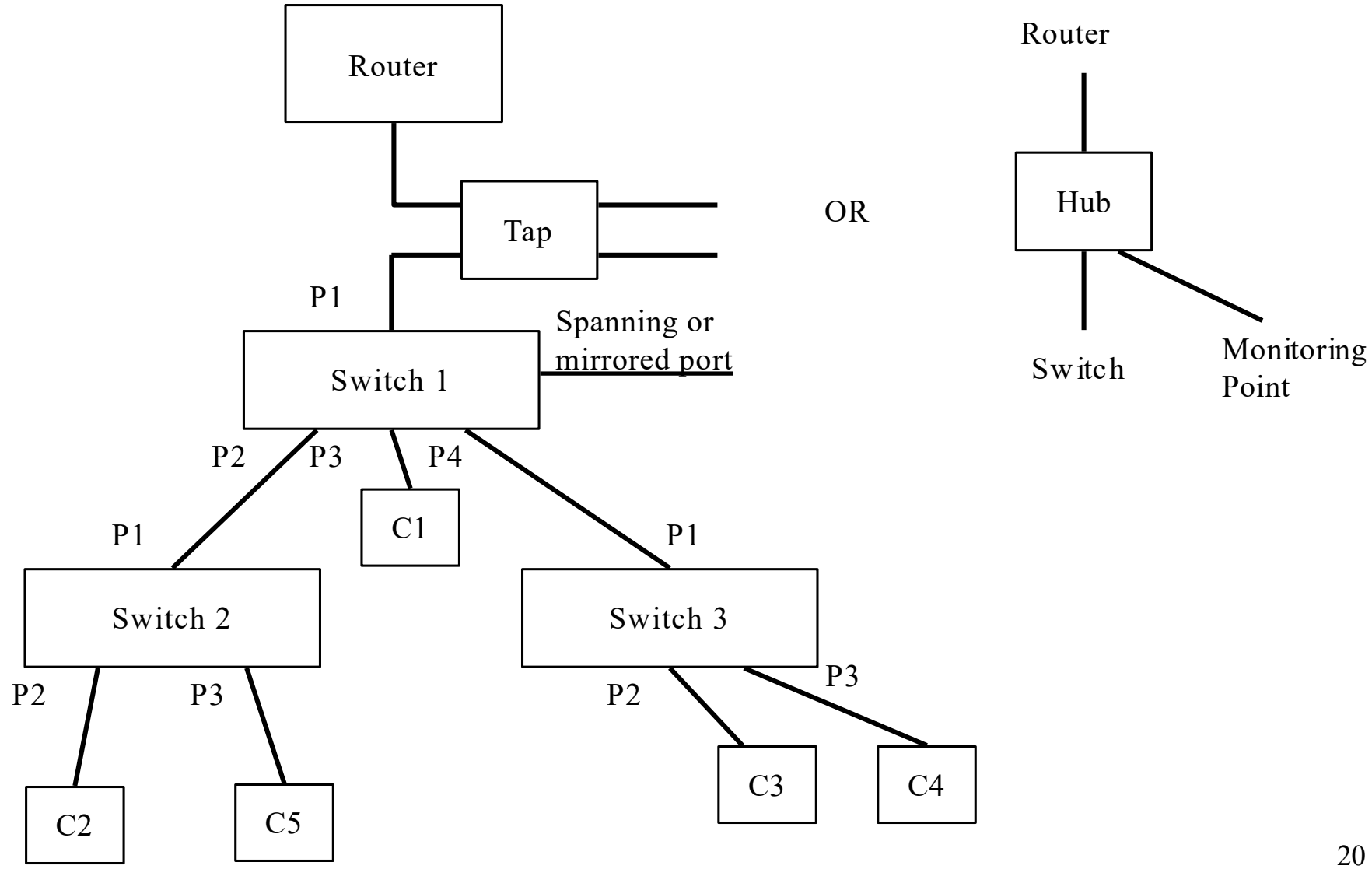
Port table, switch 2

Port	HW Address
P1	Uplink
P2	C2
P3	Multiple

Port table, switch 4

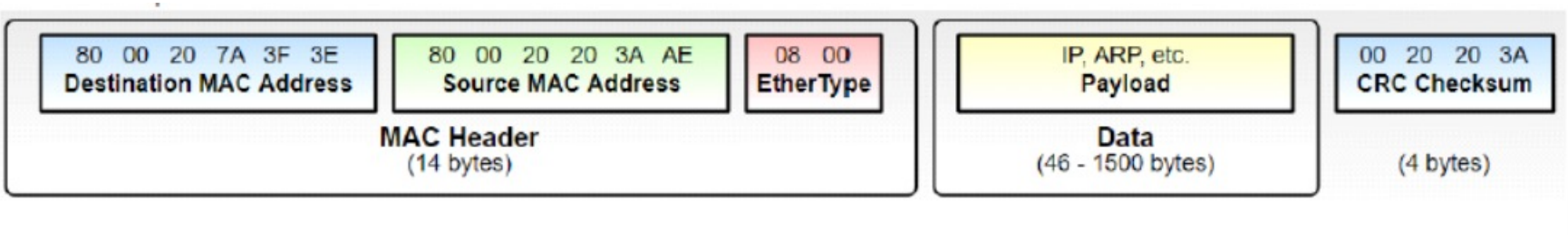
Port	HW Address
P1	Uplink
P2	C5
P3	C6
P4	C7

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
以太网地址

- Goal is to have all addresses globally unique 目标是使所有地址具有全局唯一性
- 6 bytes
  - Upper 3 bytes vendor code
  - Lower 3 bytes independent
- All 1's = broadcast address

Ethernet Type/length

如果值< 0x800，则它是一个长度字段，否则它是一个协议类型字段

- 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 将目的地址设置为广播地址会导致流量问题
  - Setting the source can cause switches to get confused 设置源会导致交换机混淆
- Mitigation 减轻
  - Very difficult to mitigate

Protocol-Based

- Protocol is simple and is in hardware
  协议很简单，而且是在硬件中，没有基于协议的漏洞

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

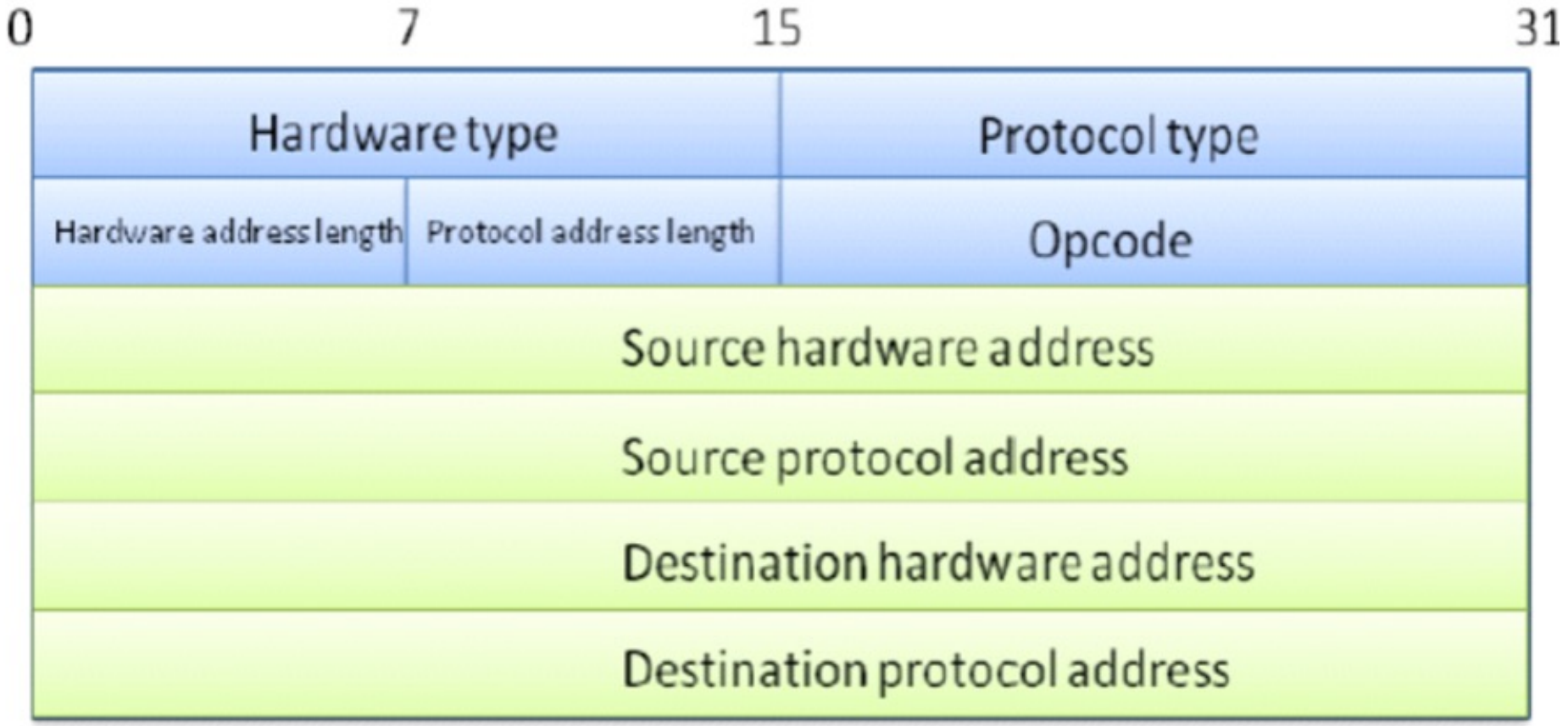
· 可以设置硬件地址
· 硬件地址用于交换机中的身份验证
· 硬件地址可用于验证网络中的设备

Authentication-Based

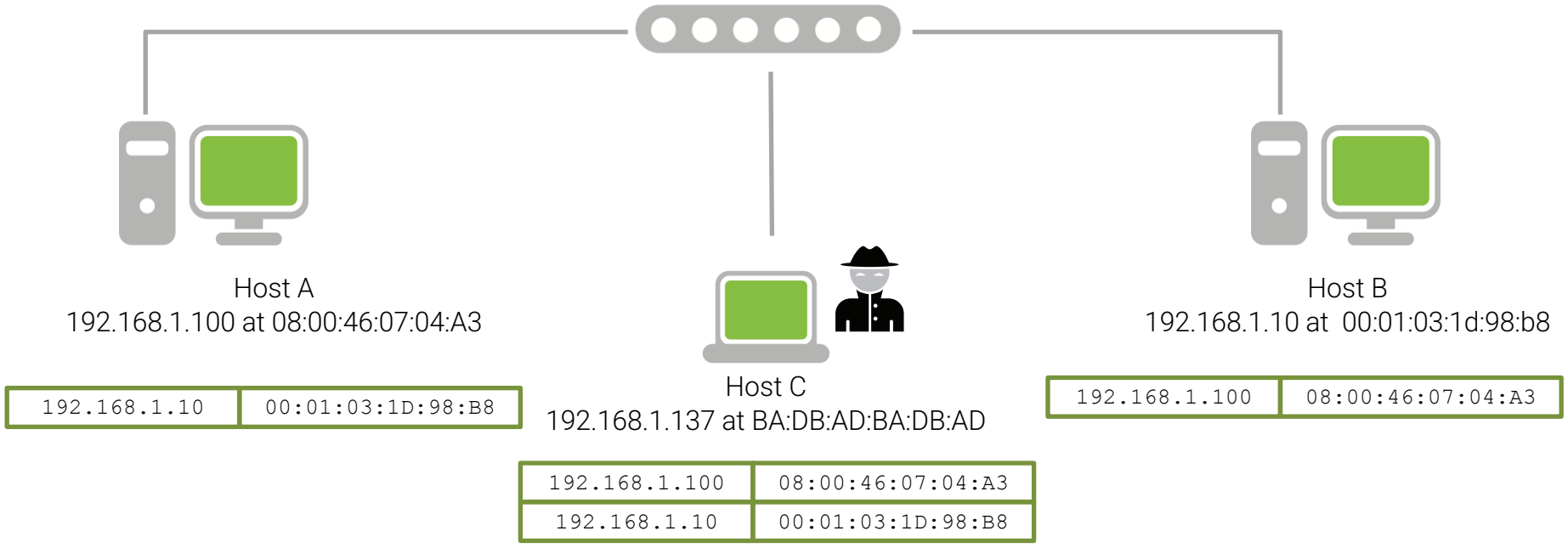
- Destination address spoofing
- Destination address is obtained dynamically via a protocol
- Trick a device into thinking you are the destination (ARP Poisoning)
- No good mitigation method

· 目的地址欺骗
· 目的地址通过协议动态获取
· 欺骗一个设备，让它以为你是目的地(ARP中毒)
· 没有好的缓解方法

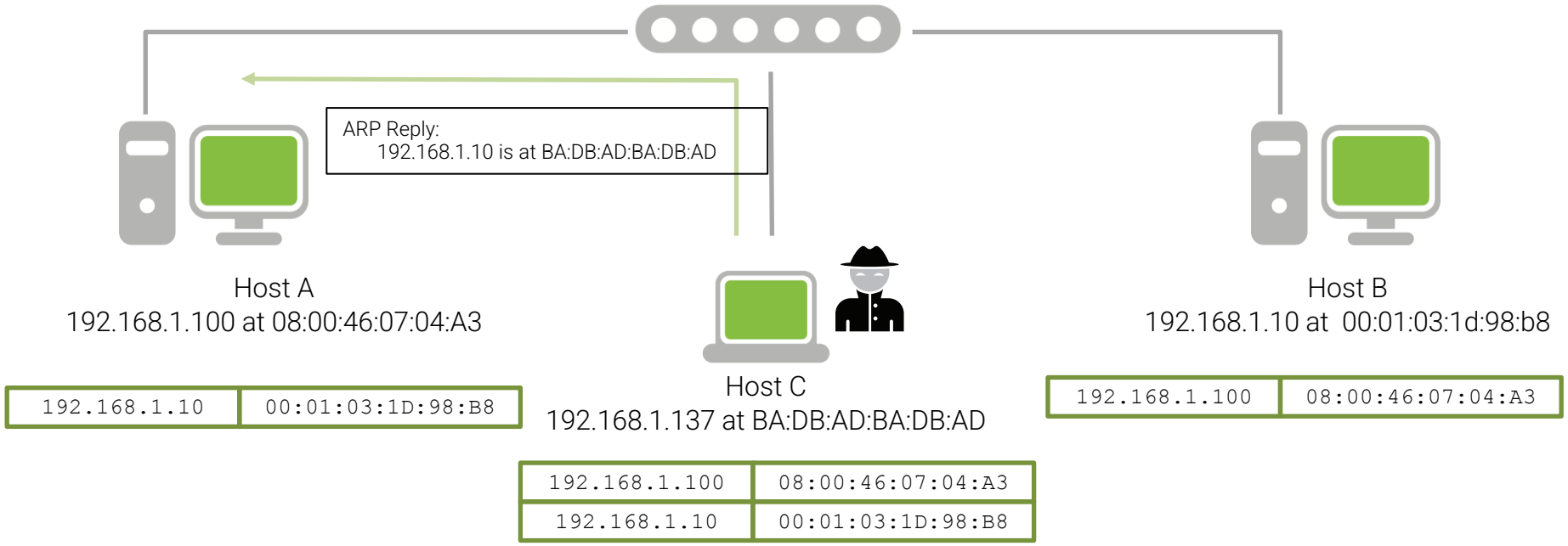
ARP Message Format



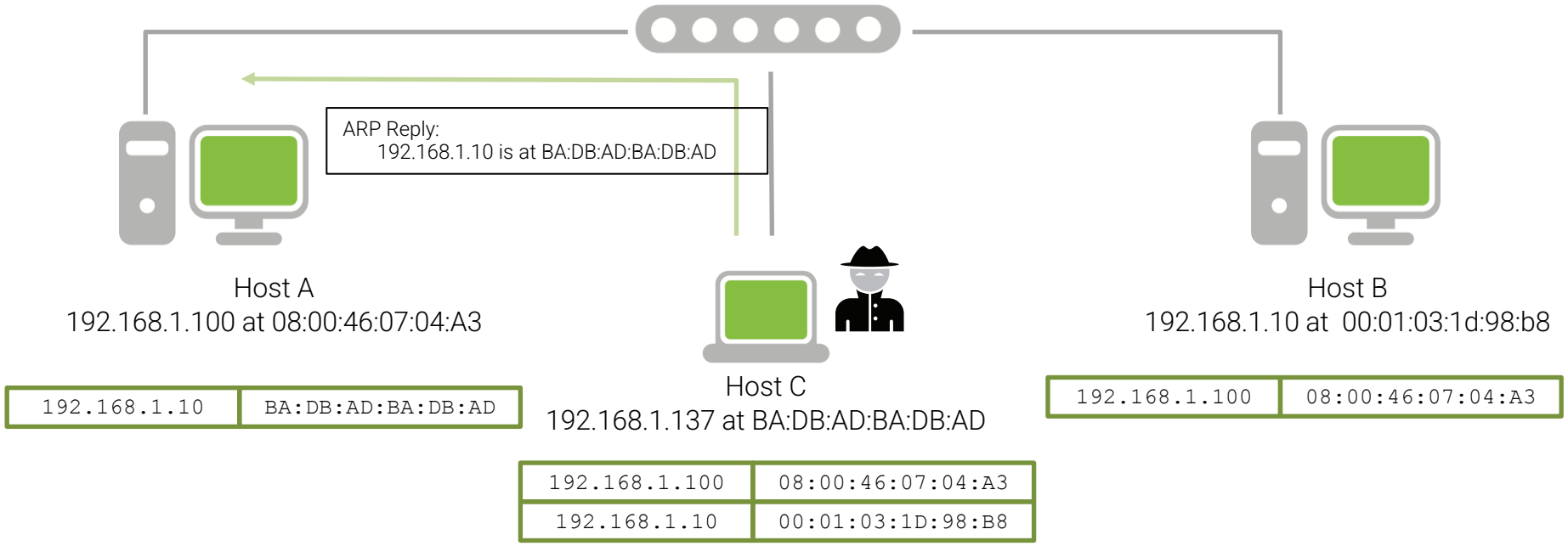
ARP Spoofing



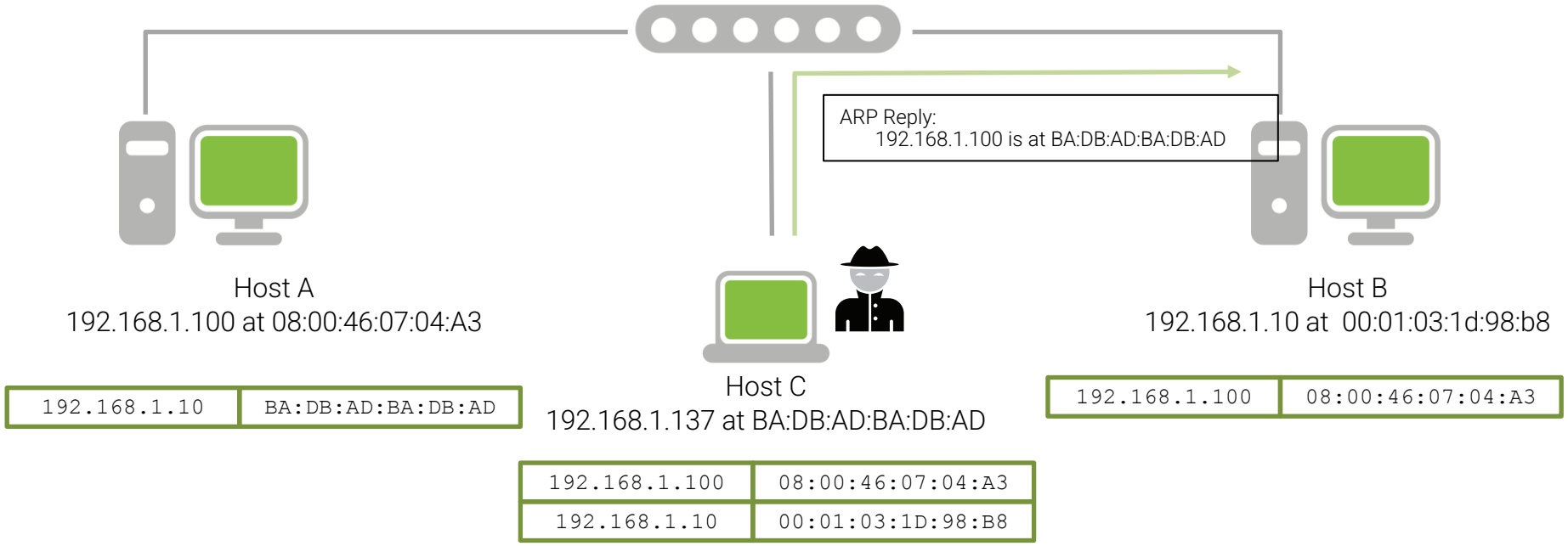
ARP Spoofing



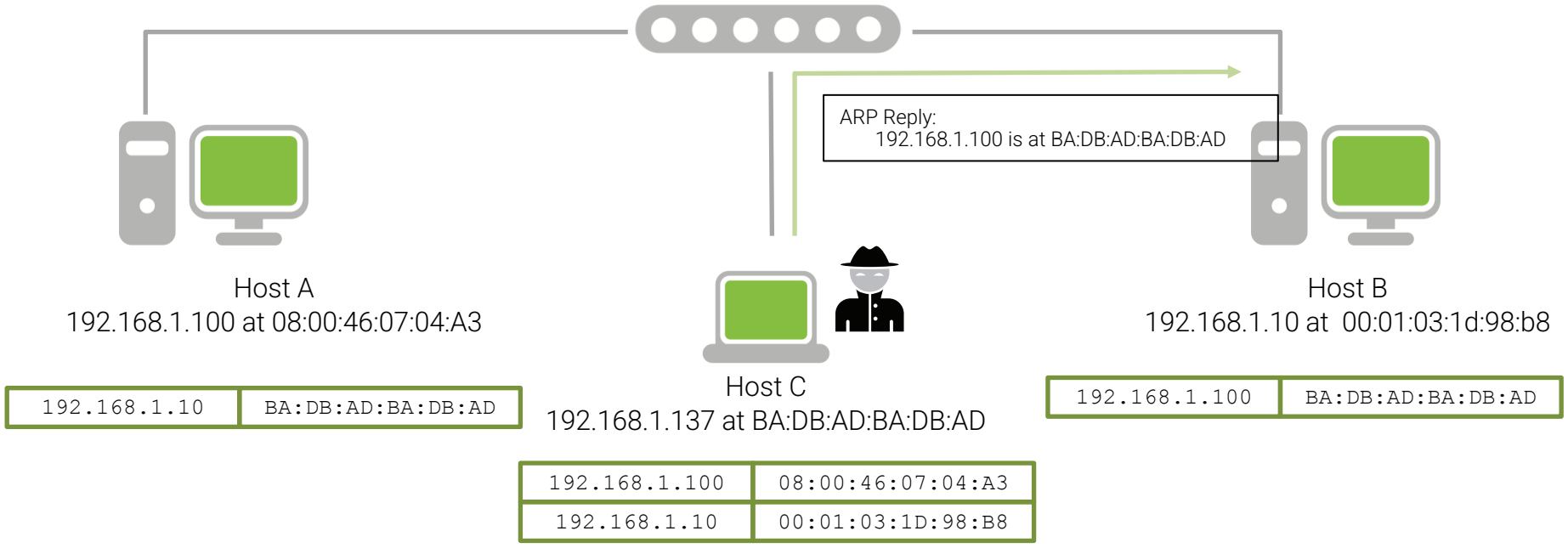
ARP Spoofing



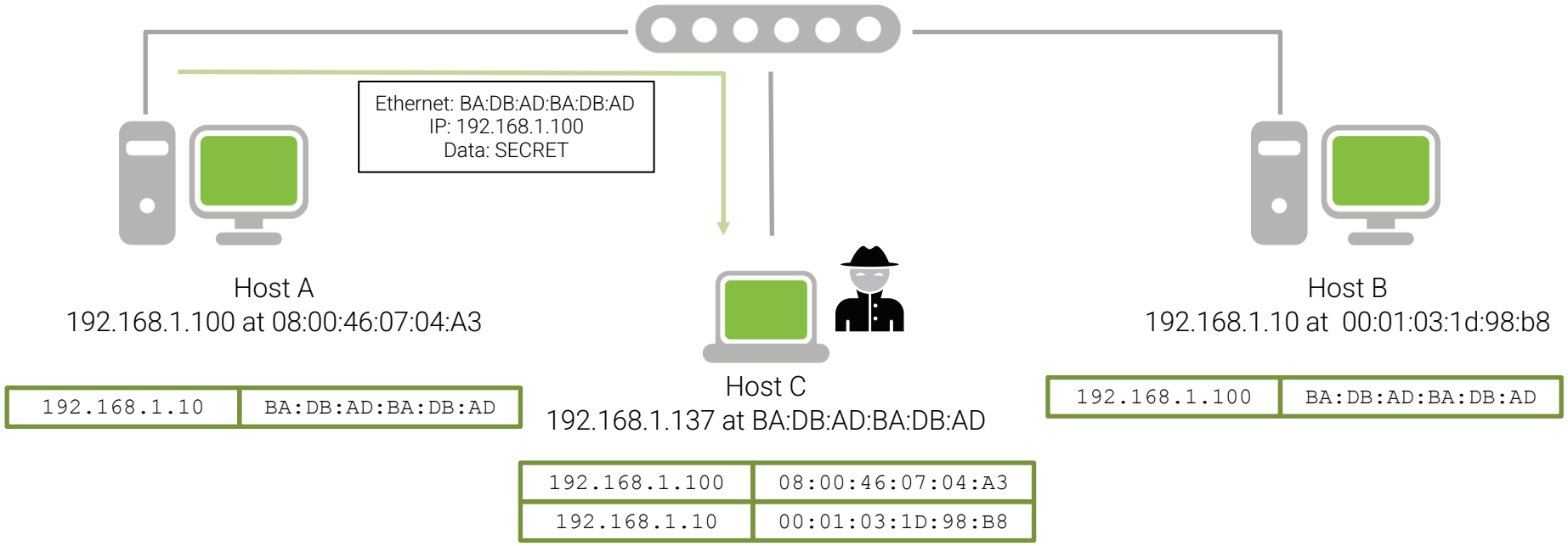
ARP Spoofing



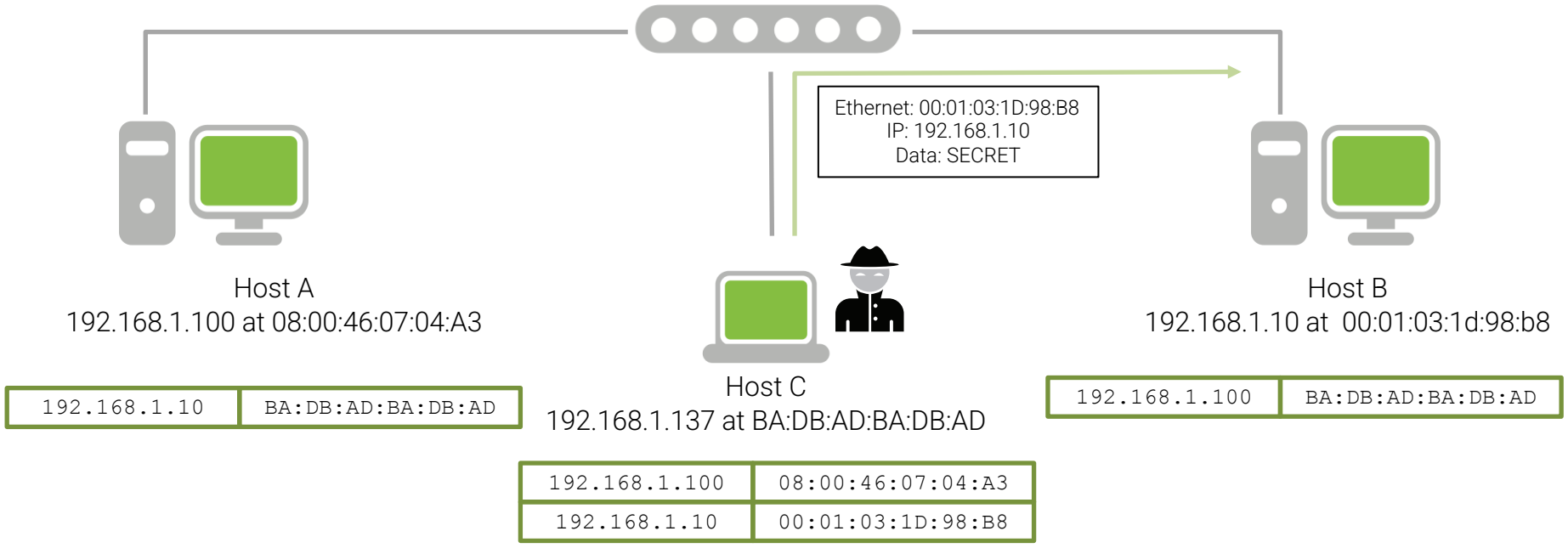
ARP Spoofing



ARP Spoofing



ARP Spoofing



Traffic-Based

- Attack
  - Ethernet controllers can be set in promiscuous mode which enables them to sniff traffic
    以太网控制器可以设置为混杂模式，使它们能够嗅探流量
- Mitigation
  - Encryption, VLAN (more later)
- Broadcast traffic can cause flooding, hard to flood unless directly connected to the LAN
  广播流量会引起泛滥，除非直接连接到局域网，否则很难泛滥
- No good mitigation for flooding
  没有很好的防洪措施

Wireless Security Topics

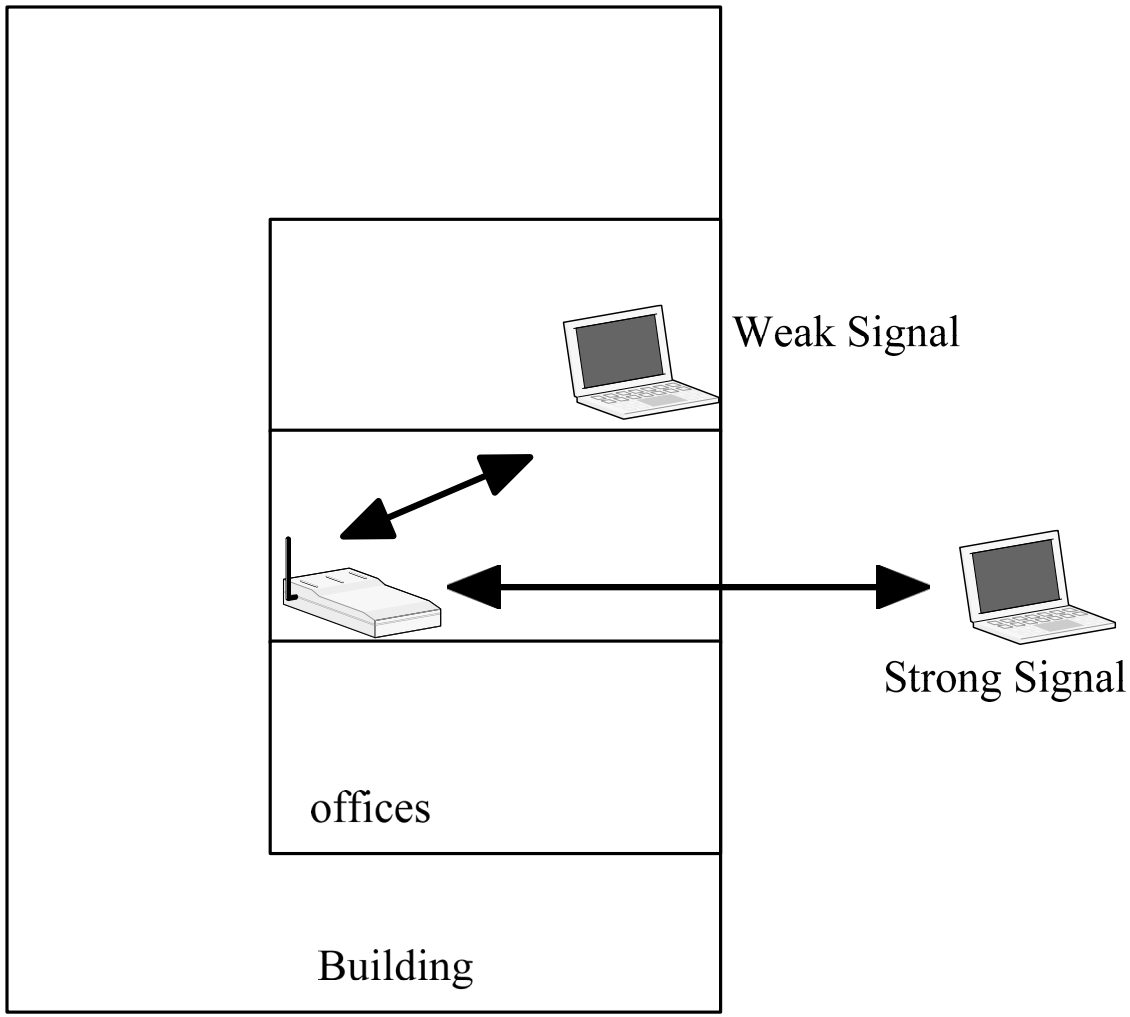
- Standards
- Devices
- Protocol
- Packet Format
- Vulnerabilities
- Mitigation

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

信号反射

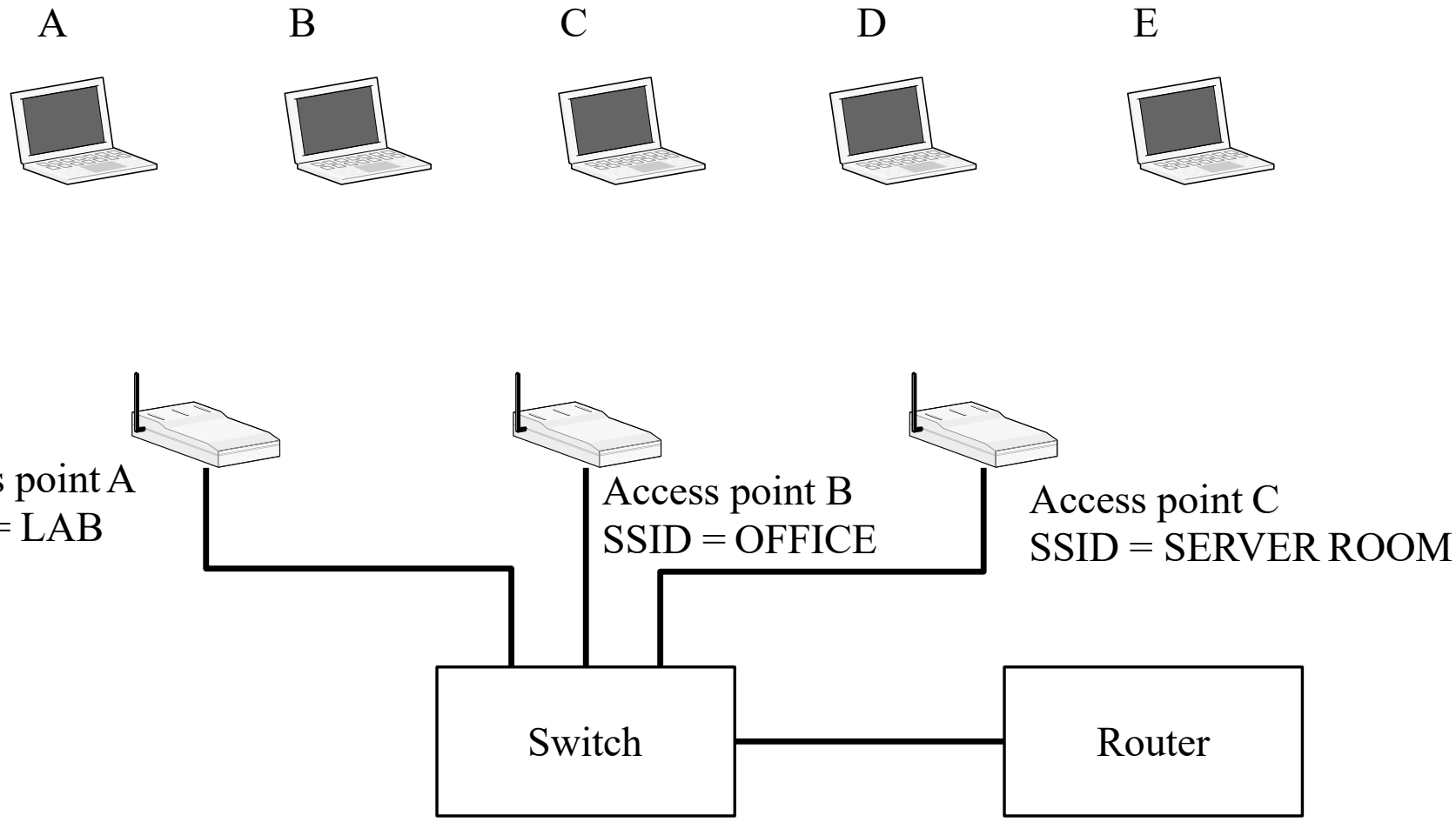


Wireless Ethernet 802.11

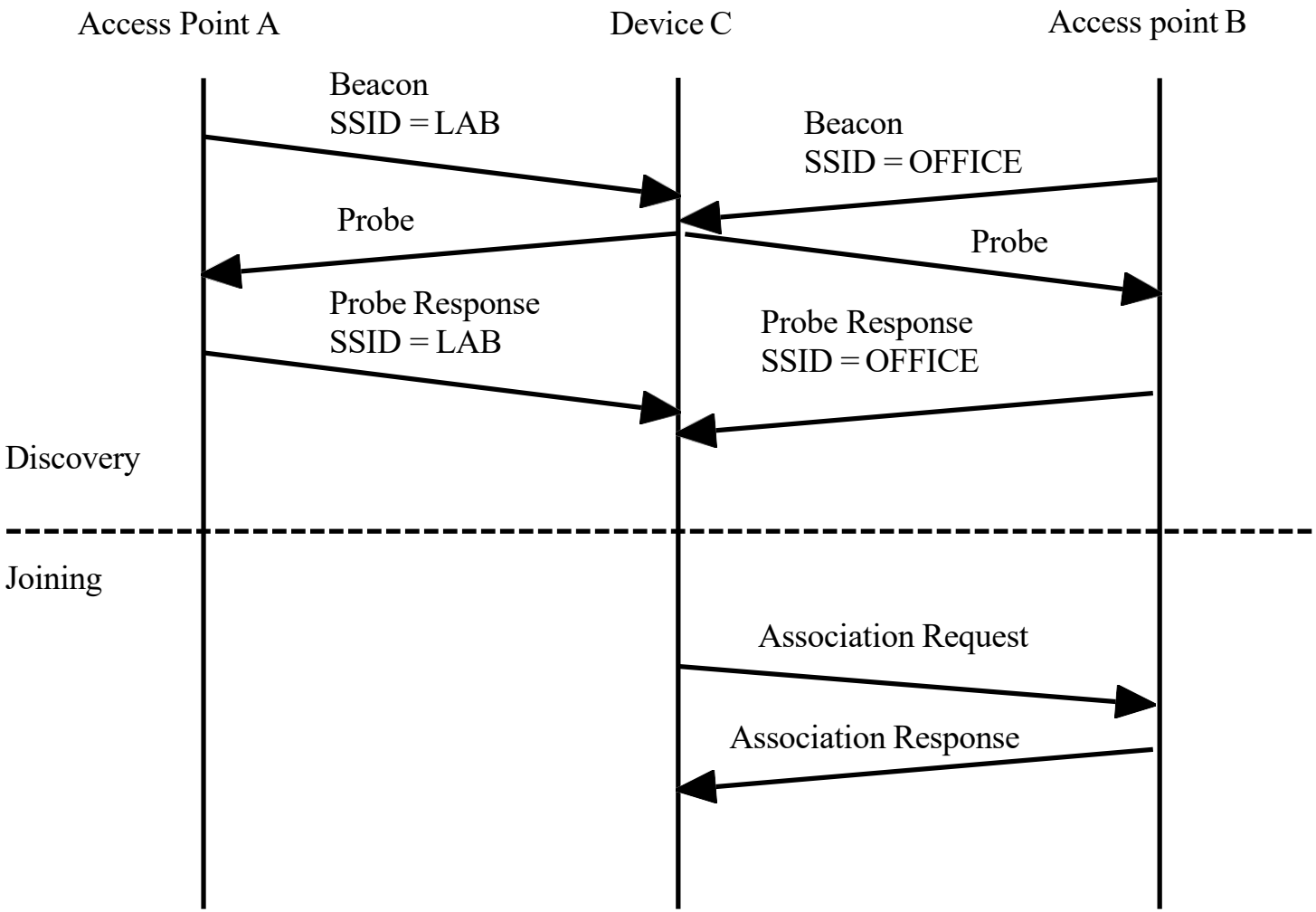
- Two topologies
  - IBSS Independent Basic Service Set
    - Ad-hoc, all stations are peers
  - ESS Extended Service Set
    - AP – Access points connected to a network
    - Station plus the AP form a BSS

Wireless Network Environment

无线网络



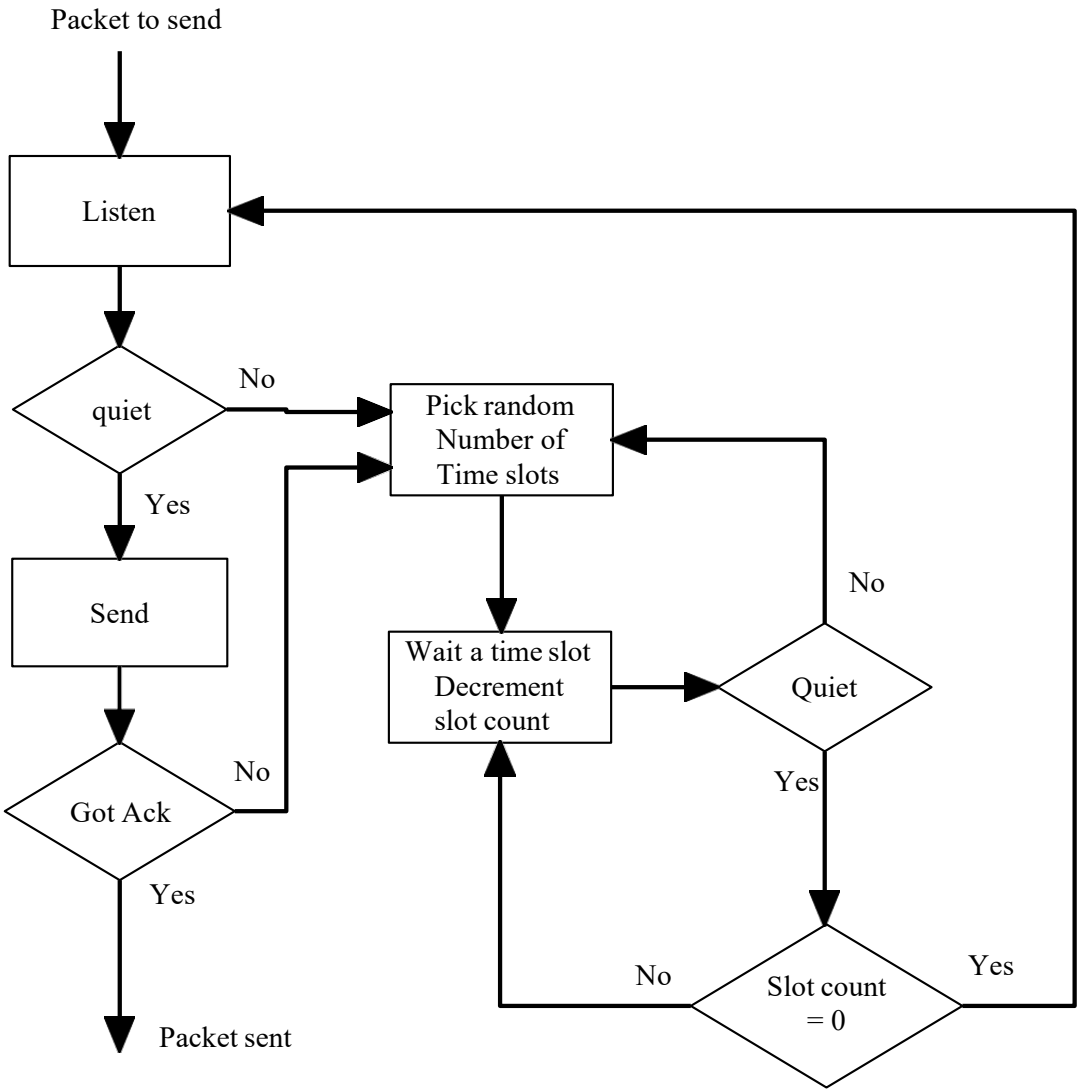
Discovery and joining



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



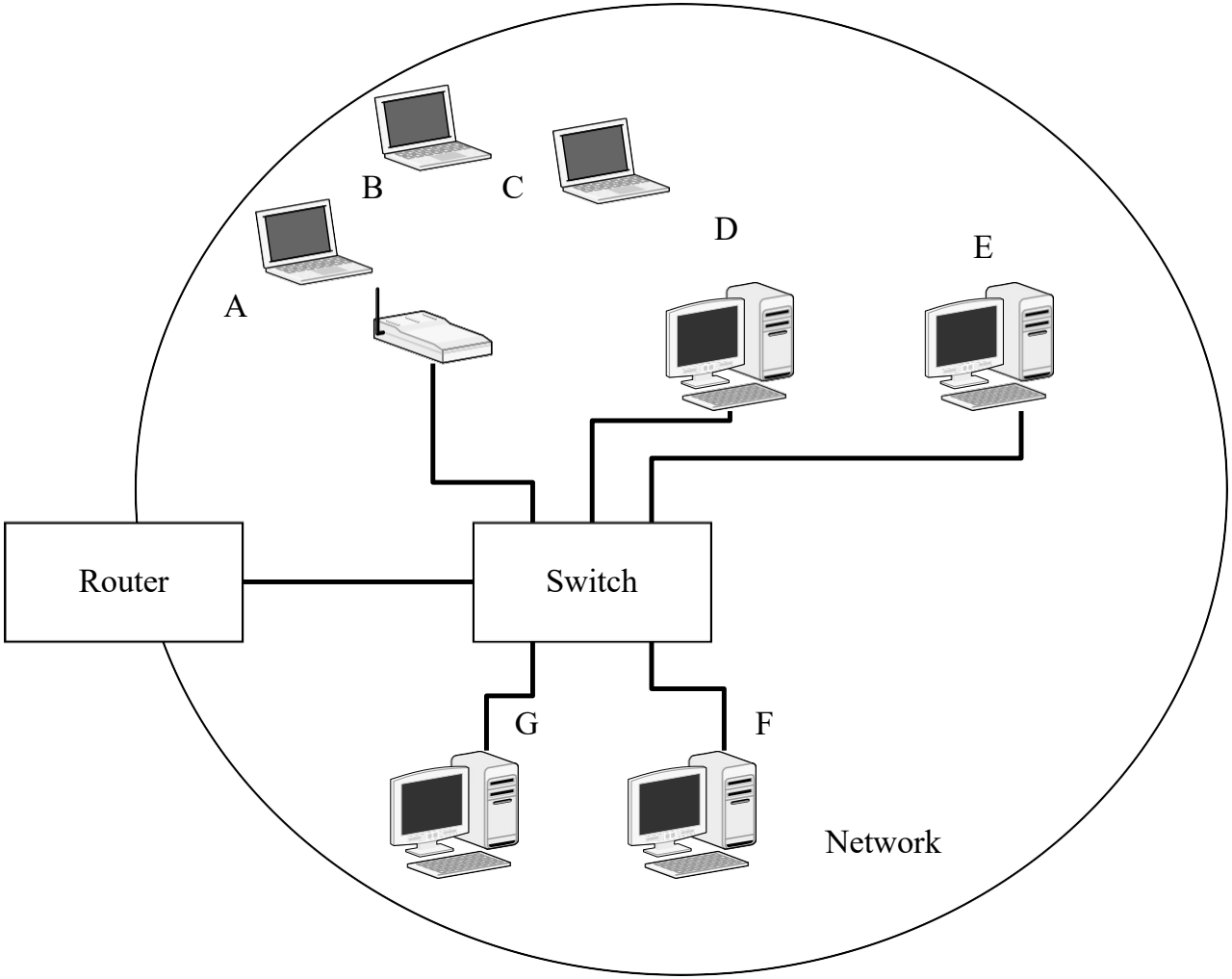
IEEE 802.11 Access Points

Two types

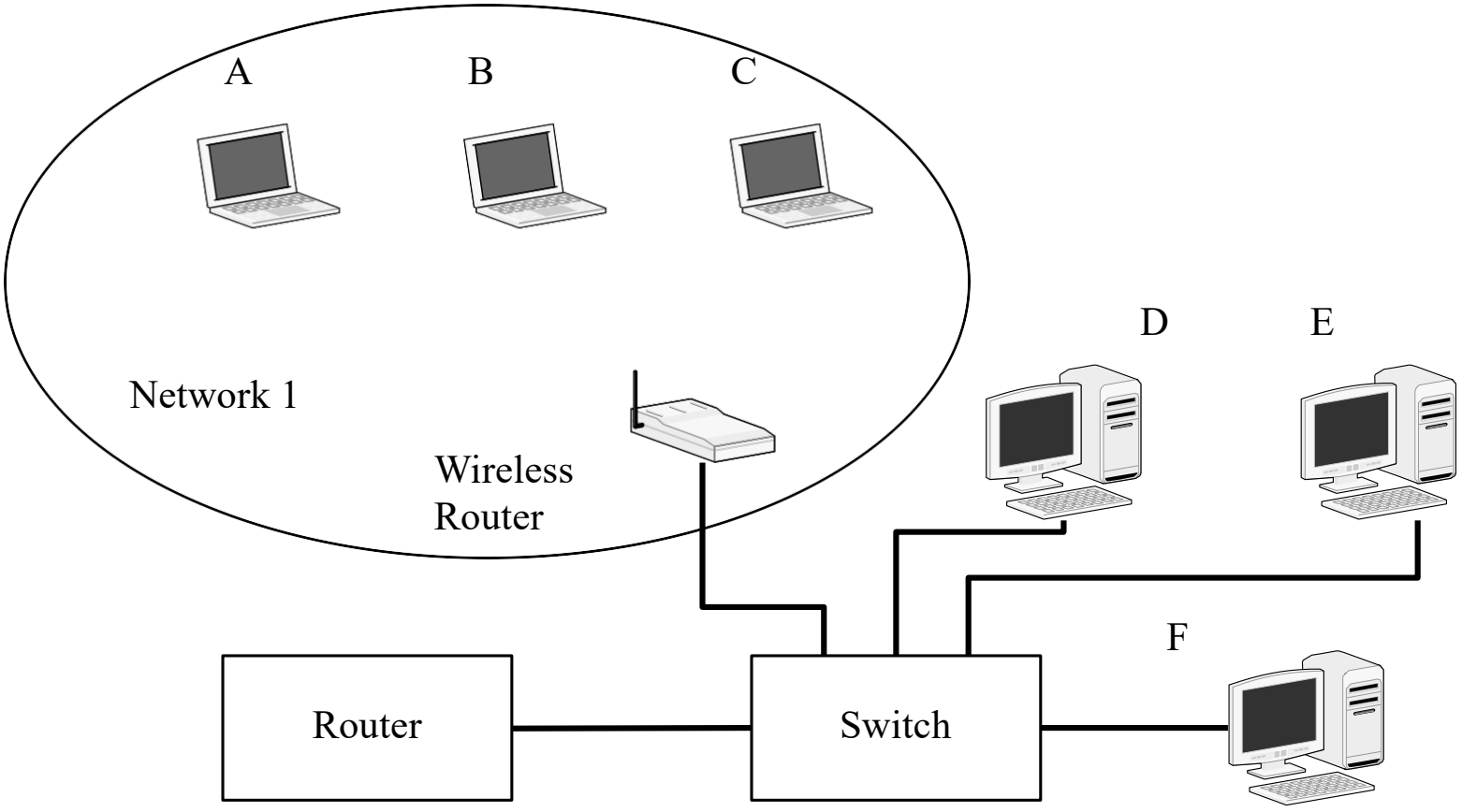
- Extended network扩展网络
  - Access point makes the wireless devices look like they are on the same network as the wired devices 接入点使无线设备看起来与有线设备在同一个网络上
- Wireless router 无线路由器
  - Access point acts as a router

    接入点充当路由器

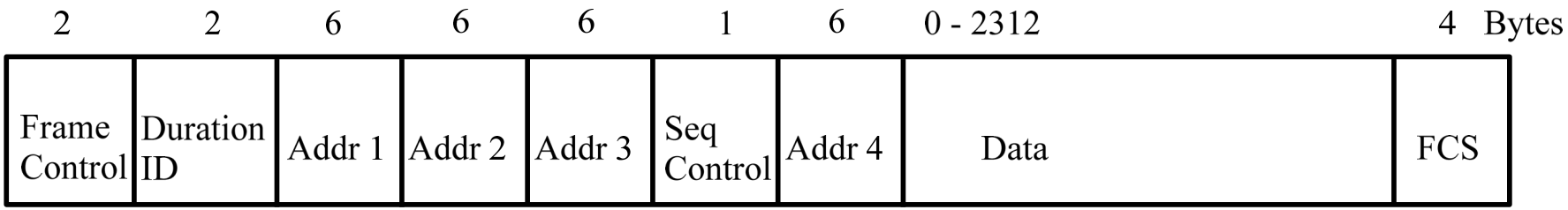
Extended Network



Wireless Router



802.11 Frame Format



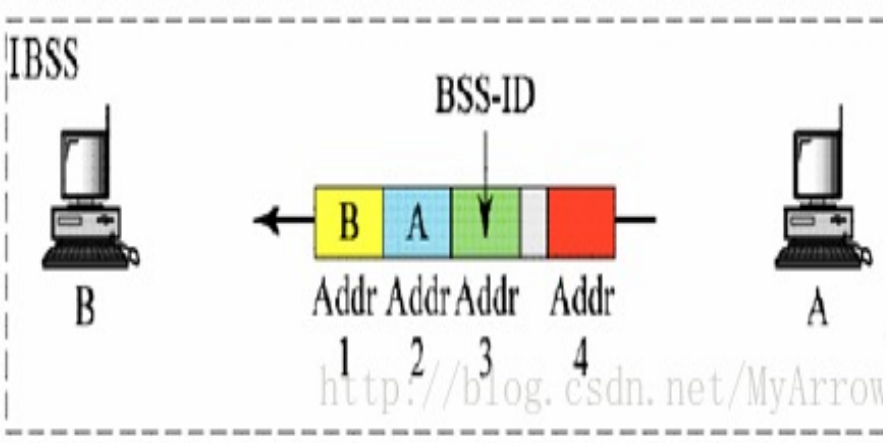
- Frame Control: Used to identify the frame type and other frame specific information. 帧控制:用于识别帧类型和其他帧特定信息。
- Duration/ID: Used to manage the access control protocol.
- Address 1: Used to identify the destination of the transmitted packet. This is used by the hardware controller to determine if the frame should be read. If it does not match the address of the controller the remainder of the frame is ignored.

用于标识传输数据包的目的地。这被硬件控制器用来决定是否应该读取帧。如果它与控制器的地址不匹配，帧的剩余部分将被忽略

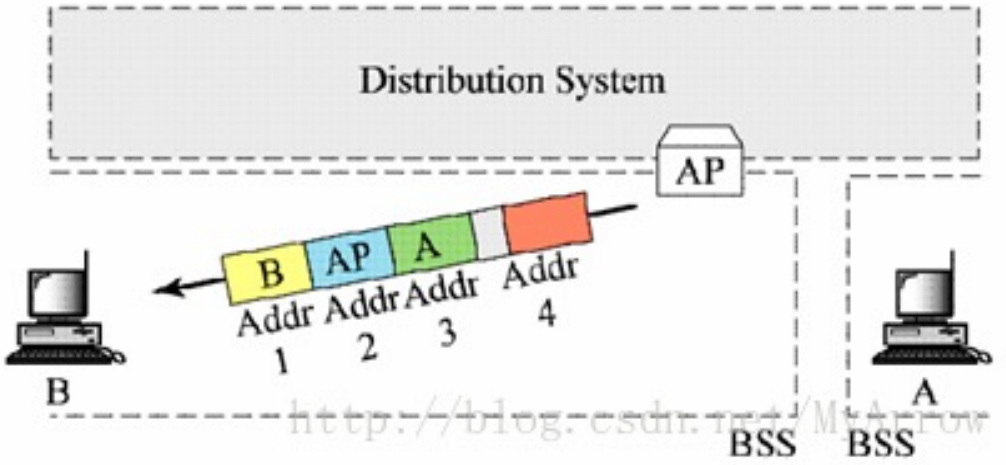
802.11 Frame Format

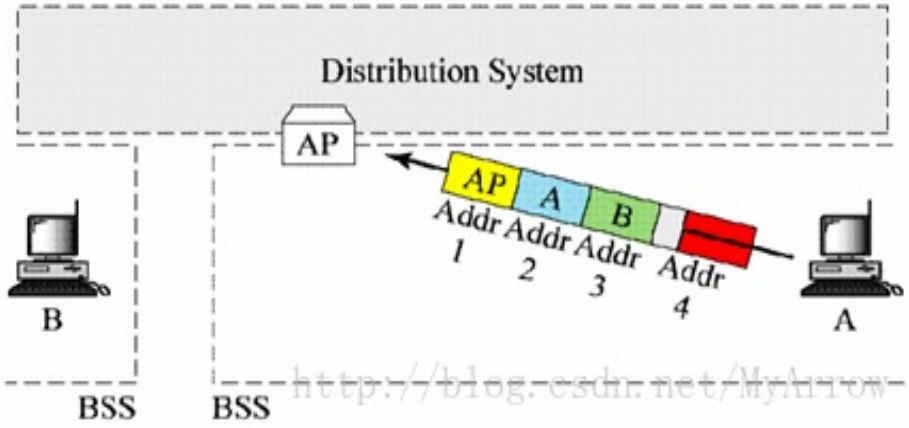
- Address 2: Address of the transmitting device.发送设备地址
- Address 3: Used when the access point is part of an extended network where the access point will relay the traffic. 当接入点是扩展网络的一部分时使用，其中接入点将中继流量
- Address 4: Used when the access point is part of an extended network where the access point will relay the traffic

A和B 在同一个IBSS，A->B (Ad hoc无线自组网中的数据帧的地址格式)。

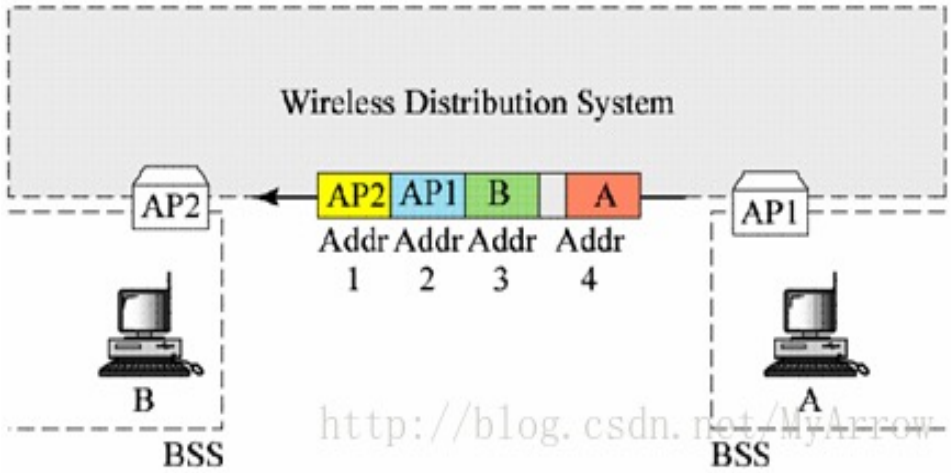


从AP发出的无线数据帧中的地址格式。





发到AP的无线数据帧中的地址格式。



通过无线分布系统传输的无线数据帧中的地址格式。

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.

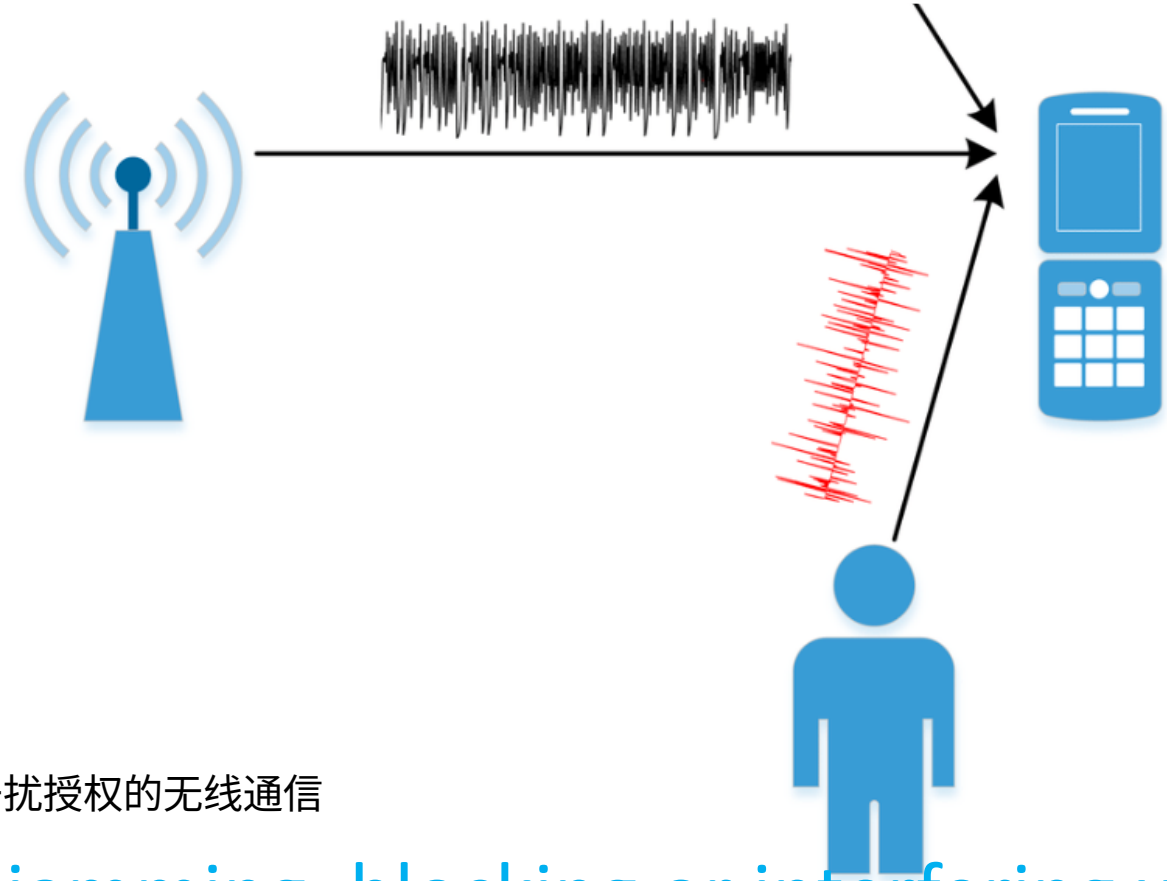
Header Based

- Setting the destination address as a broadcast address can cause traffic problems 将目的地址设置为广播地址会导致流量问题
- Denial of Service
  - Invalid headers will cause loss of access or loss of association 拒绝服务
    —无效的报头将导致访问或关联的丢失
- Not easy to fix
  不容易修复

Protocol-Based

- Protocol is simple and is in hardware
- Can transmit packets to cause Denial of service 传输数据包是否会导致拒绝服务
- Jamming of signals by ignoring the protocol 无视协议干扰信号
- Very hard to stop

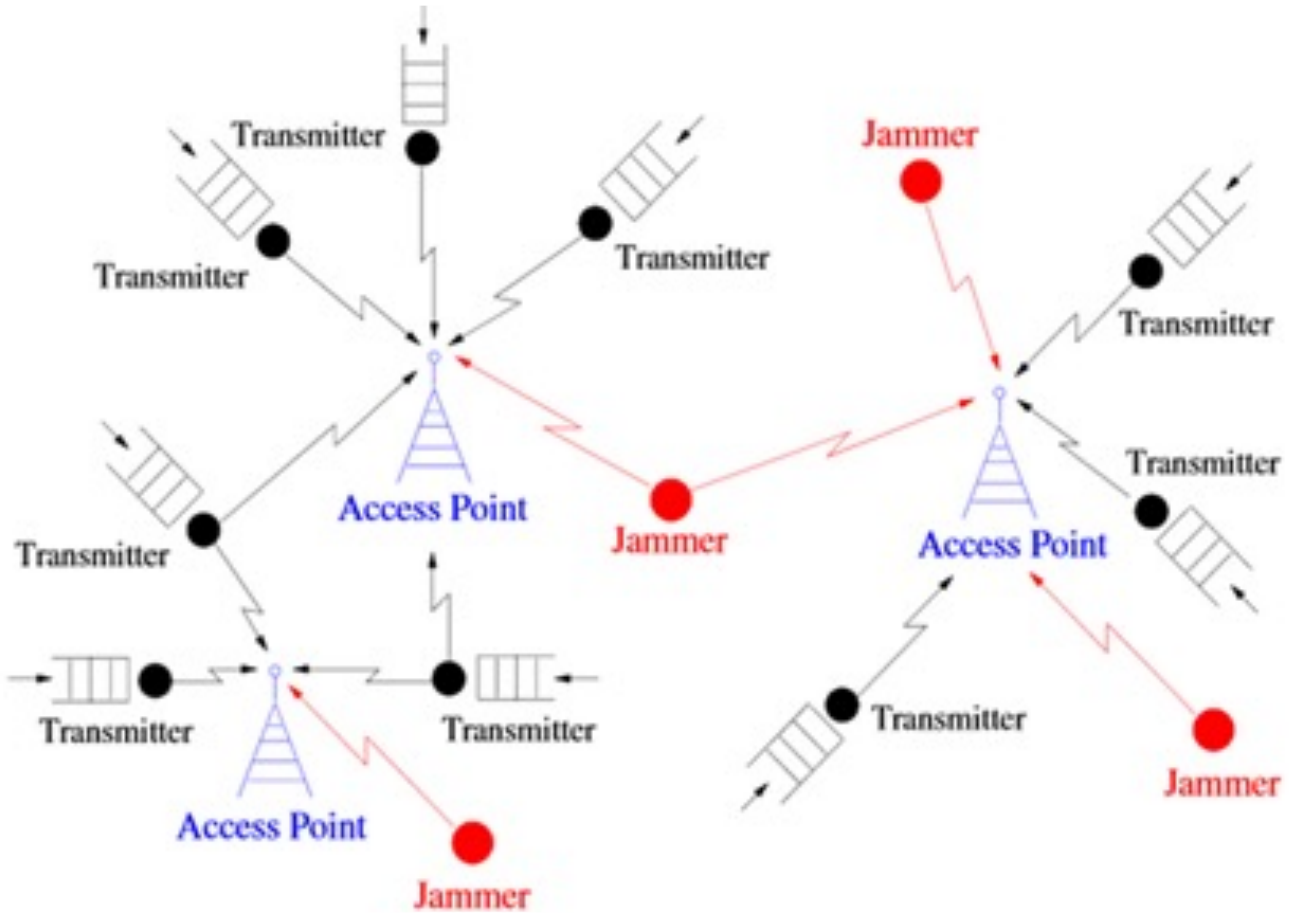
Jamming 干扰；堵塞



故意干扰、阻断或干扰授权的无线通信

deliberate jamming, blocking or interfering with authorized wireless communication

Jamming



an easy to launch wireless DoS attack

Protocol-Based

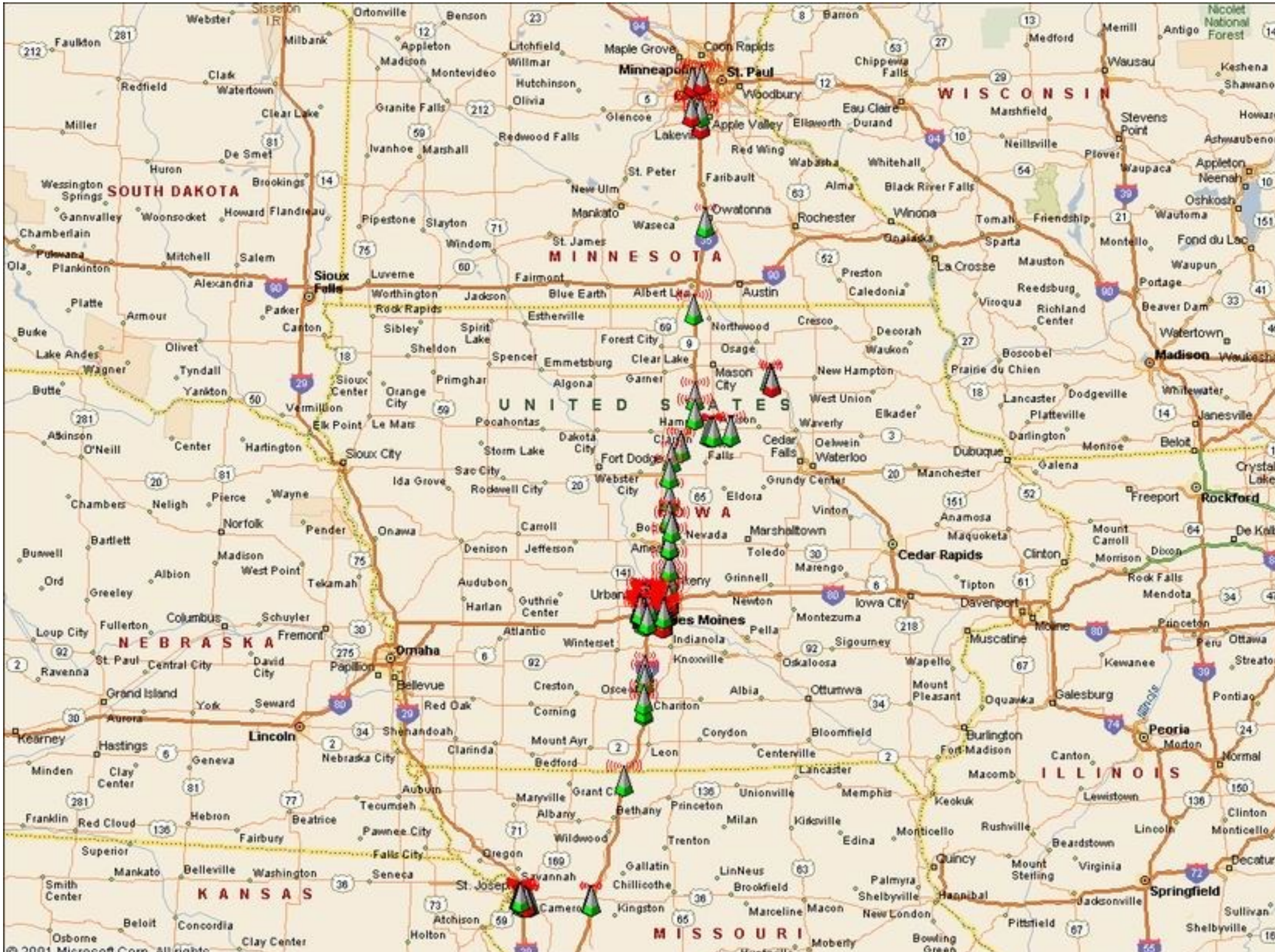
- Access point can broadcast its SSID
  - Wardriving
- www.wardriving.com
- www.worldwidewardrive.org

SSID discovery

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

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
Owatonna
Albert Lea
Mason City
Clear Lake
Fort Dodge
Ames
Des Moines
Osceola
St. Joseph
Cameron
Sioux Falls
Sioux City
Omaha
Lincoln
Cedar Rapids
Iowa City
Davenport
Waterloo
Rochester
La Crosse
Madison
Rockford
Peoria
Springfield
© 2001 Microsoft Corp. All rights

Wardriving

Mitigation:

- Turn off broadcast of SSID
- Use encryption or Network Access Control (NAC) (make it an authentication problem)

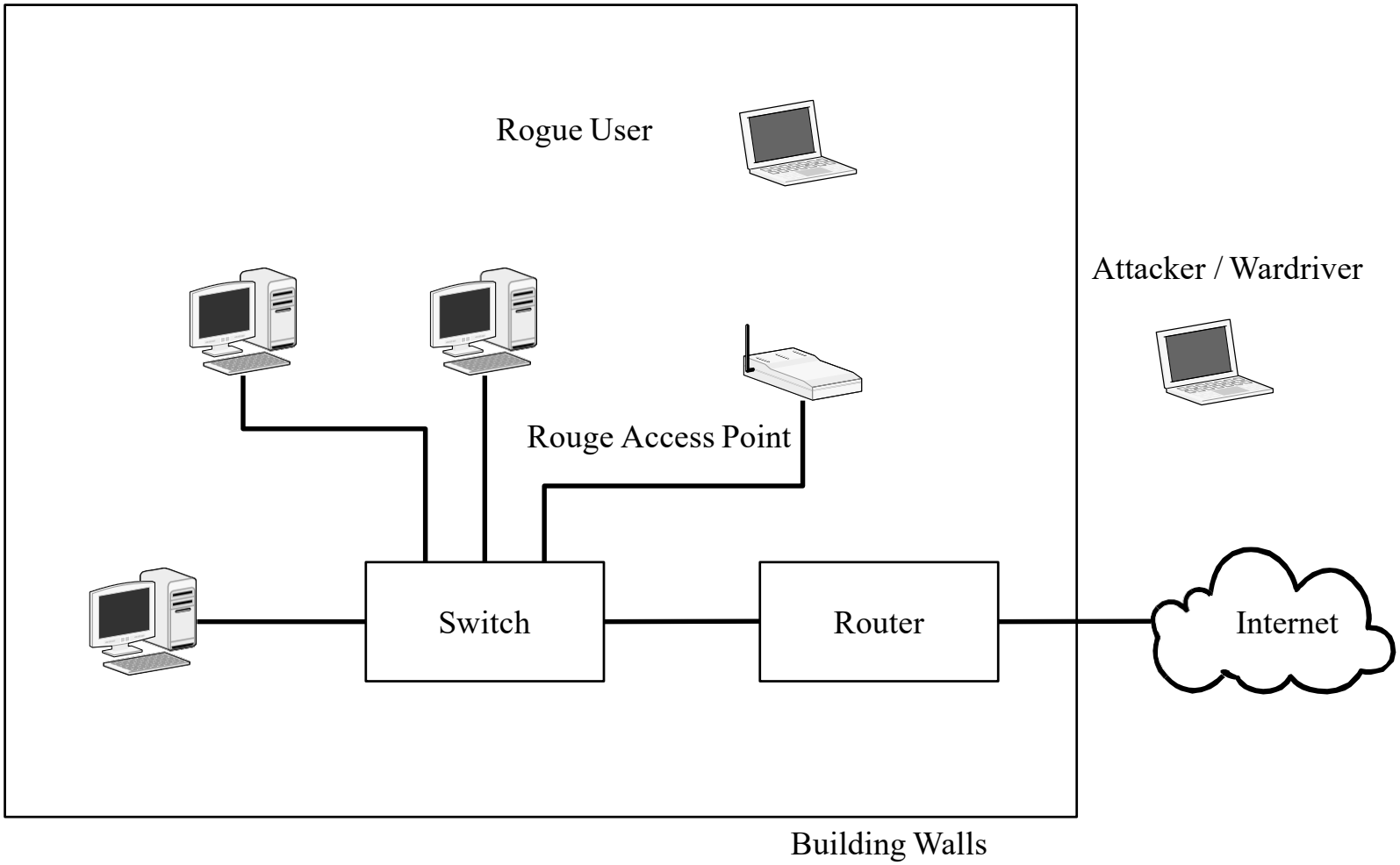
Authentication Based

- 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

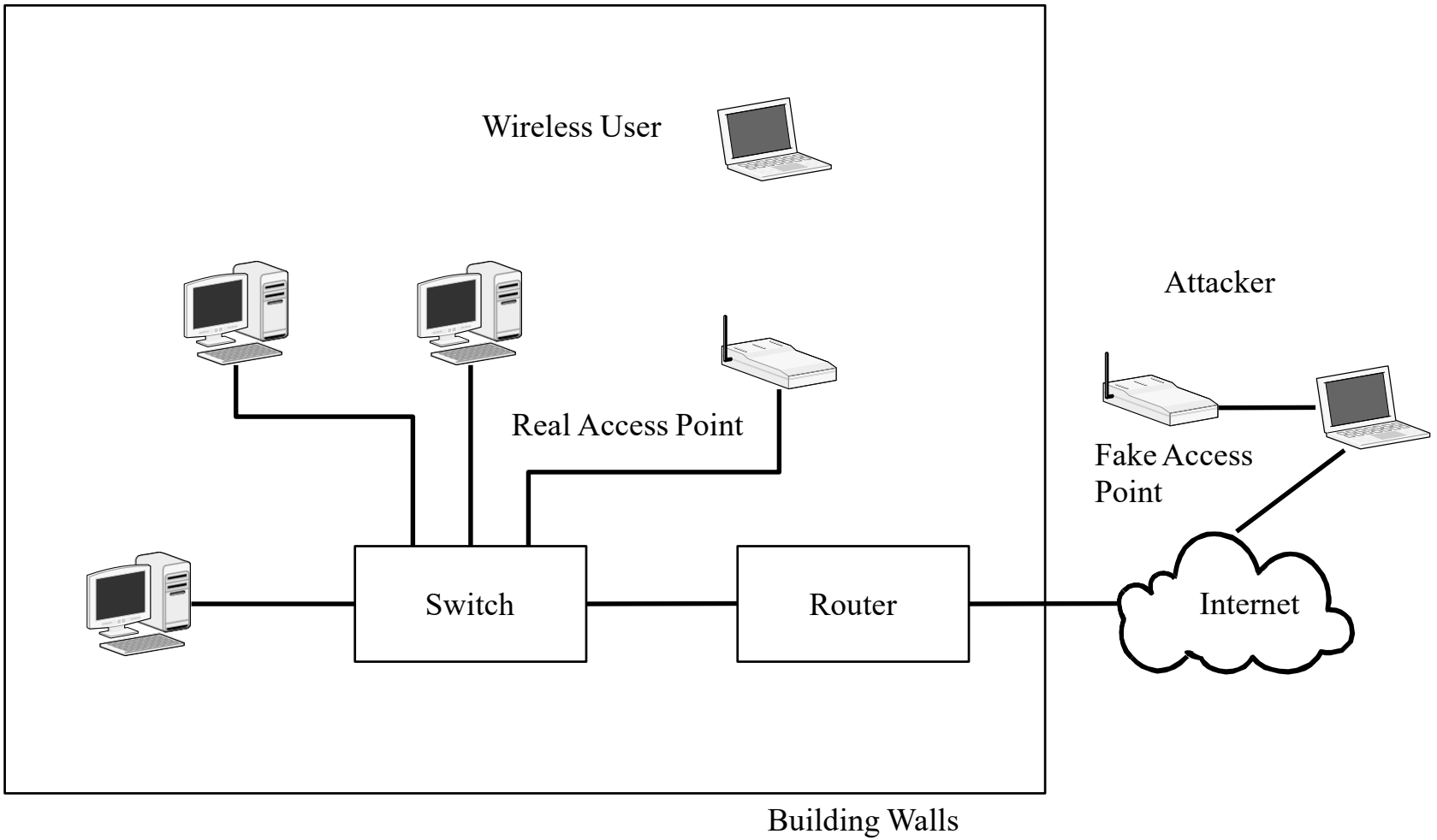
Rogue Access Point



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

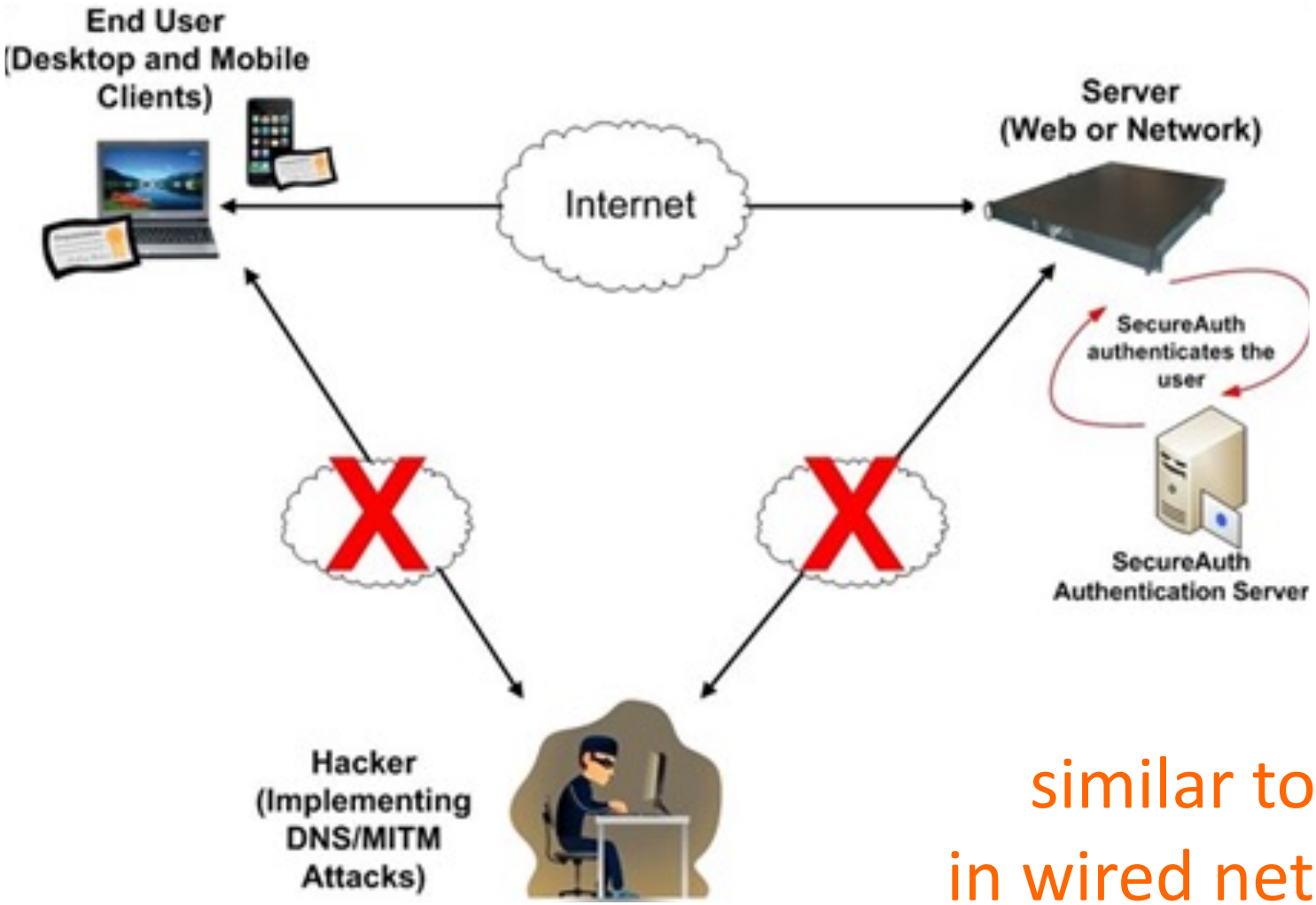
Access Point Configuration Authentication

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

Traffic Based

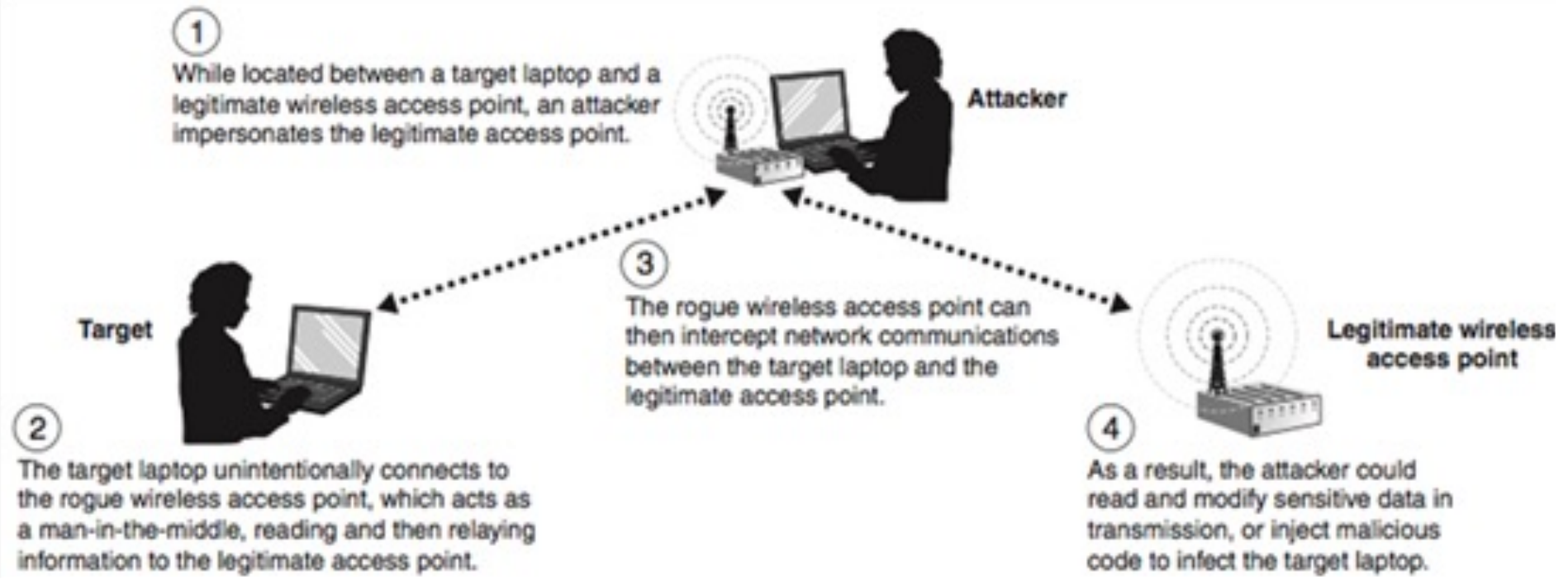
- Ethernet controllers can be set in promiscuous mode which enables them to sniff traffic
- Broadcast traffic can cause flooding

Man-In-The-Middle



similar to mitm
in wired networks

Frame Injection



based on mitm

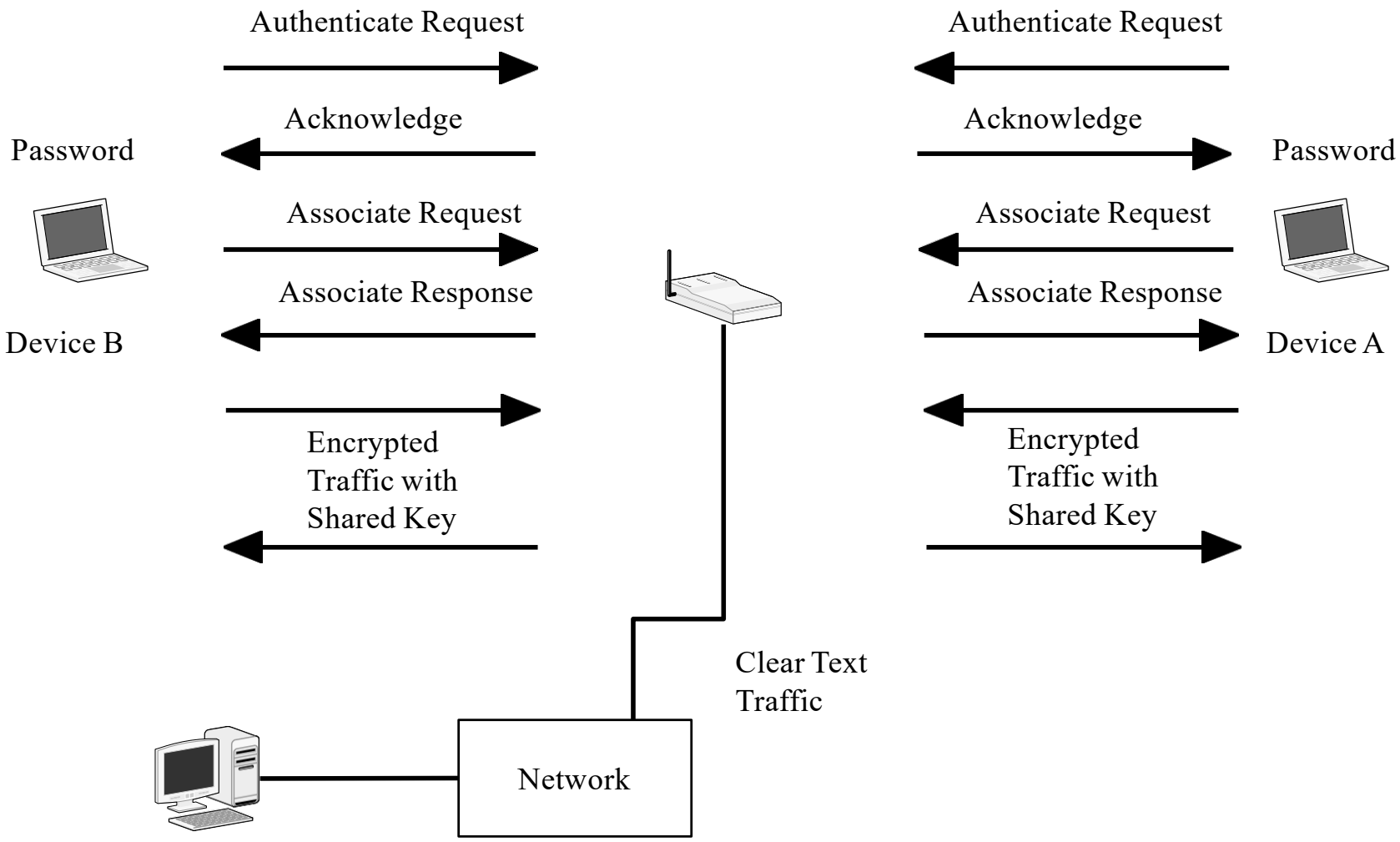
more actively inject frames

rather than simply intercept communication

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

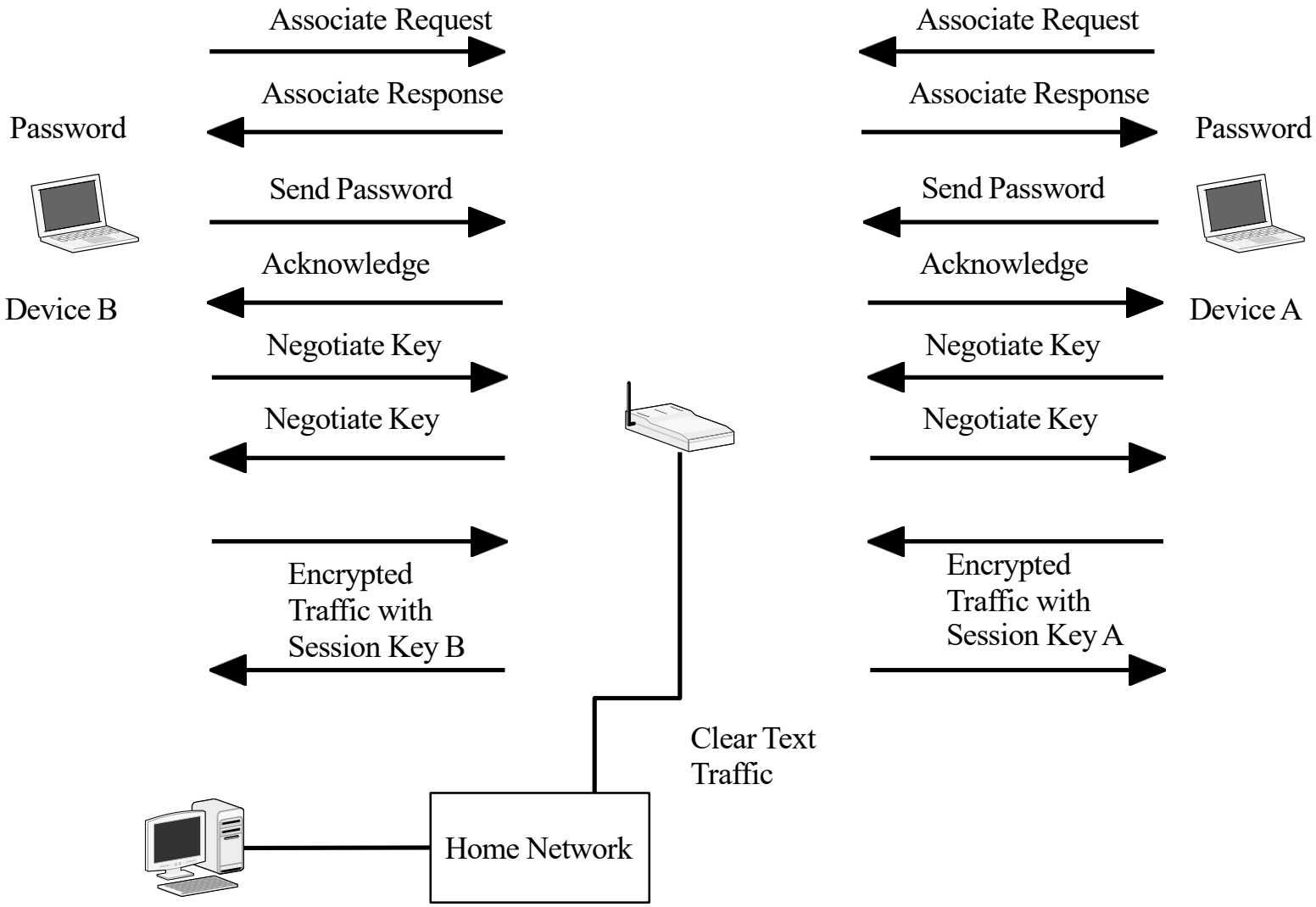
Wi-Fi Protected Access (WPA)

- 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

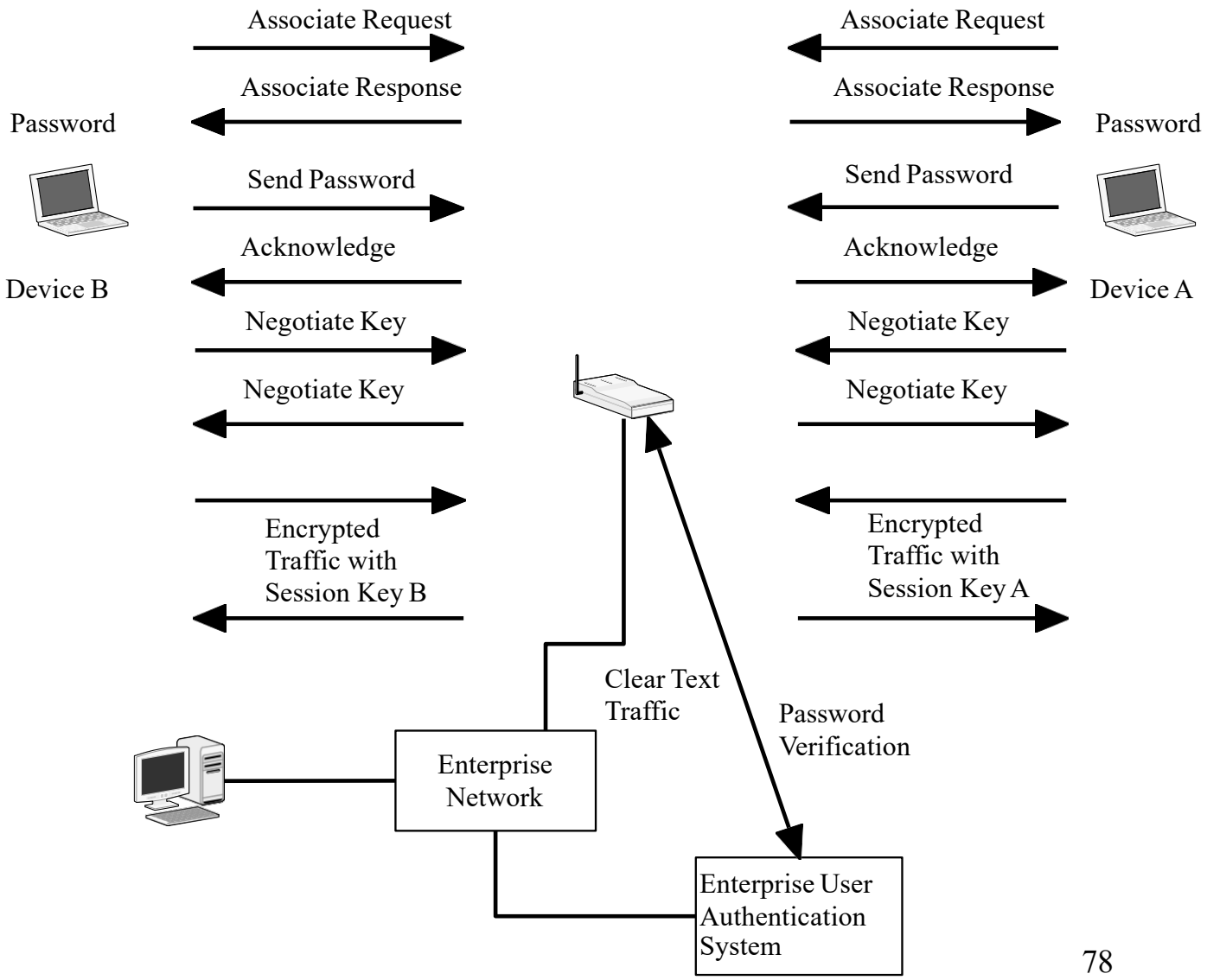
Home-Based WPA



WPA – enterprise

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

Enterprise WPA



Fragment and Forge:

Breaking Wi-Fi Through Frame Aggregation and Fragmentation

USENIX Security '21

Mathy Vanhoef

NEW YORK UNIVERSITY

Design flaws

Implementation Flaws

Design flaws

Implementation Flaws

Aggregation

Mixed key

Fragment cache

Implementation Flaws

Background

Sending small frames causes high overhead:

This can be avoided by aggregating frames:

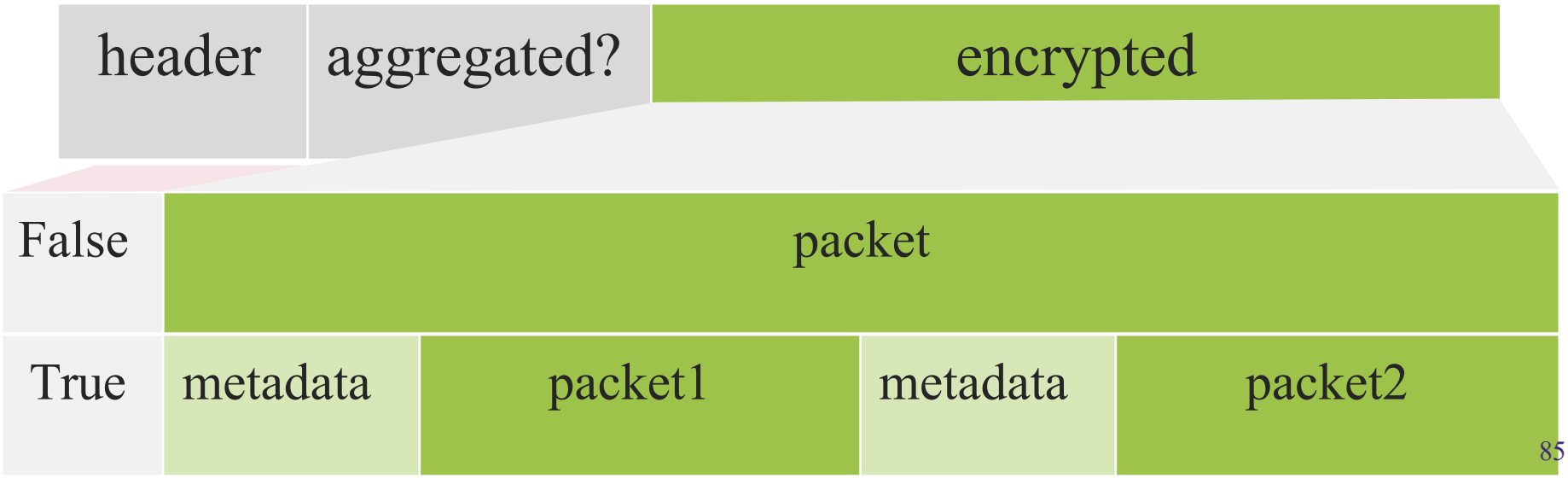
Background

Sending small frames causes high overhead:

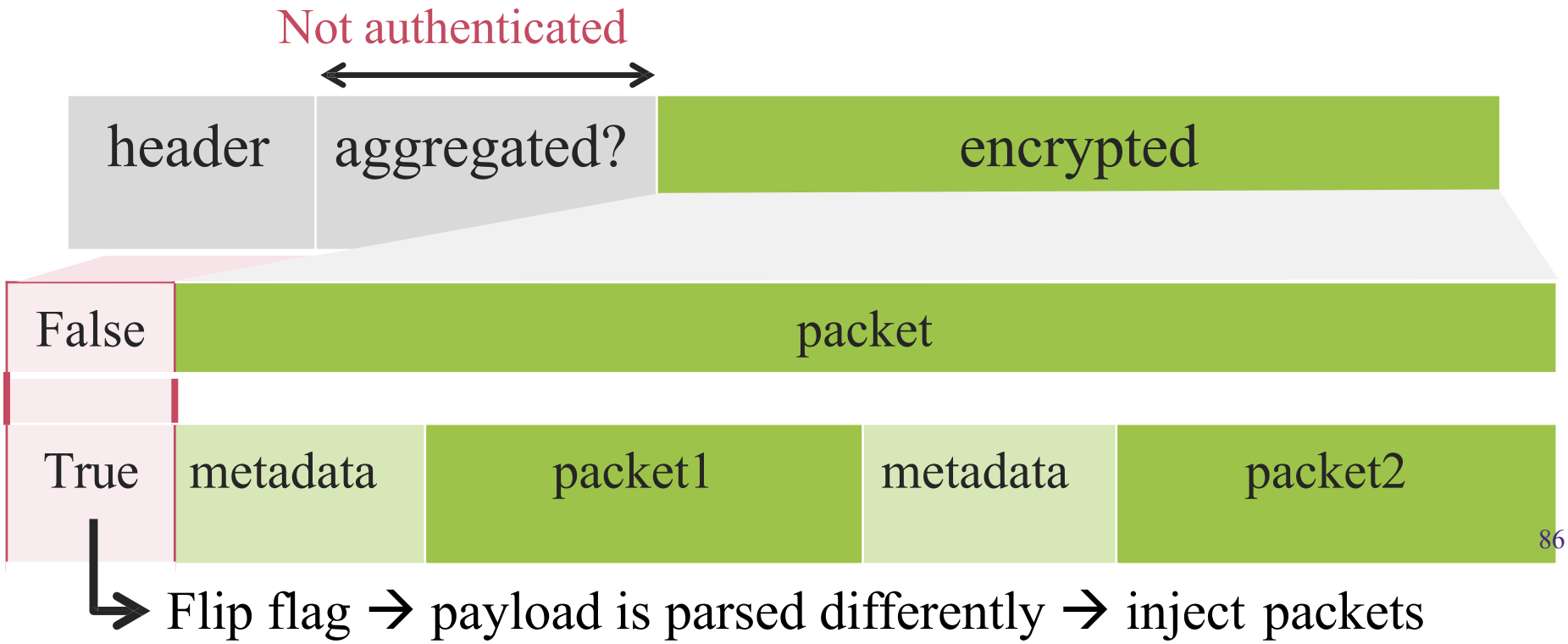
This can be avoided by aggregating frames:

Problem: how to recognize aggregated frames?

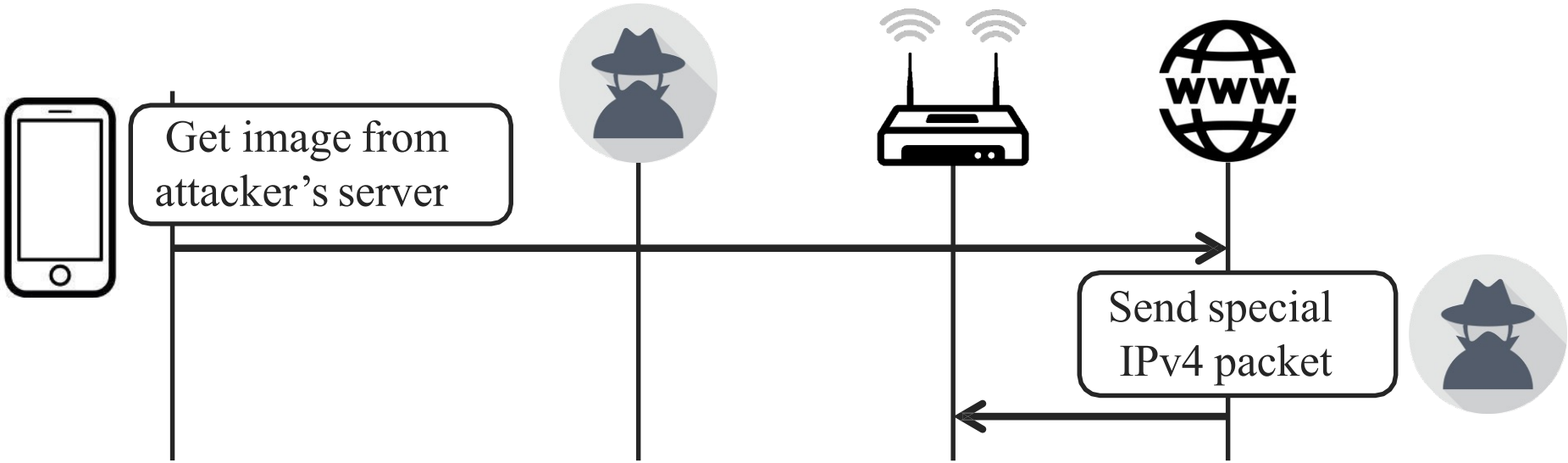
Aggregation design flaw



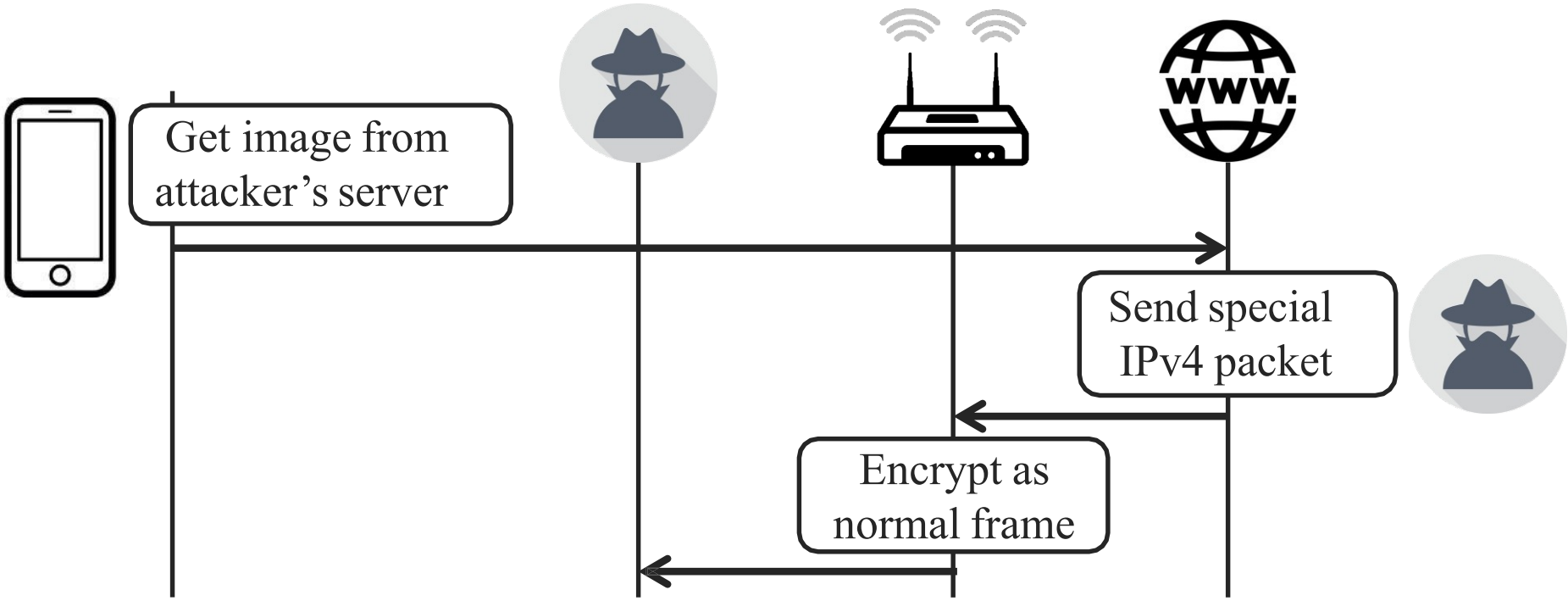
Aggregation design flaw



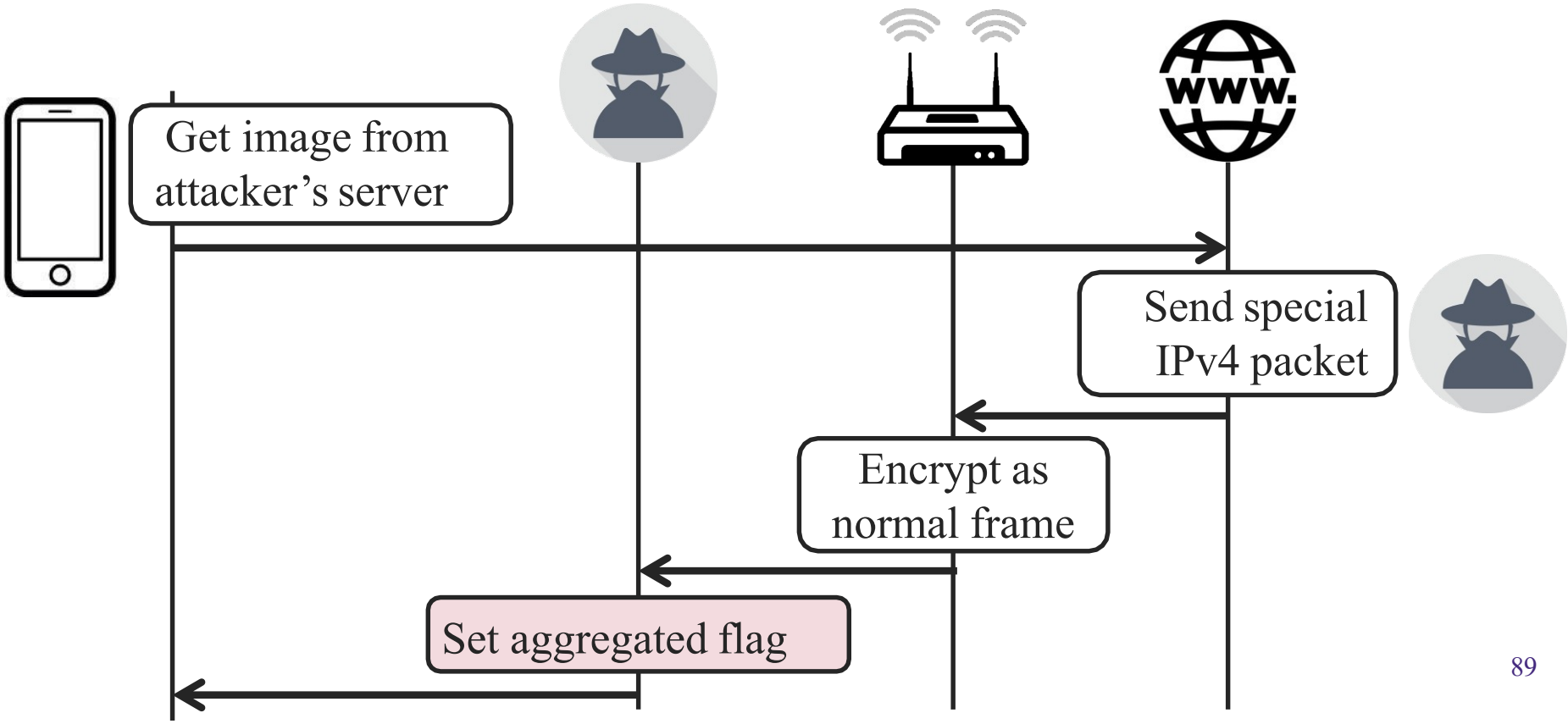
Exploit steps



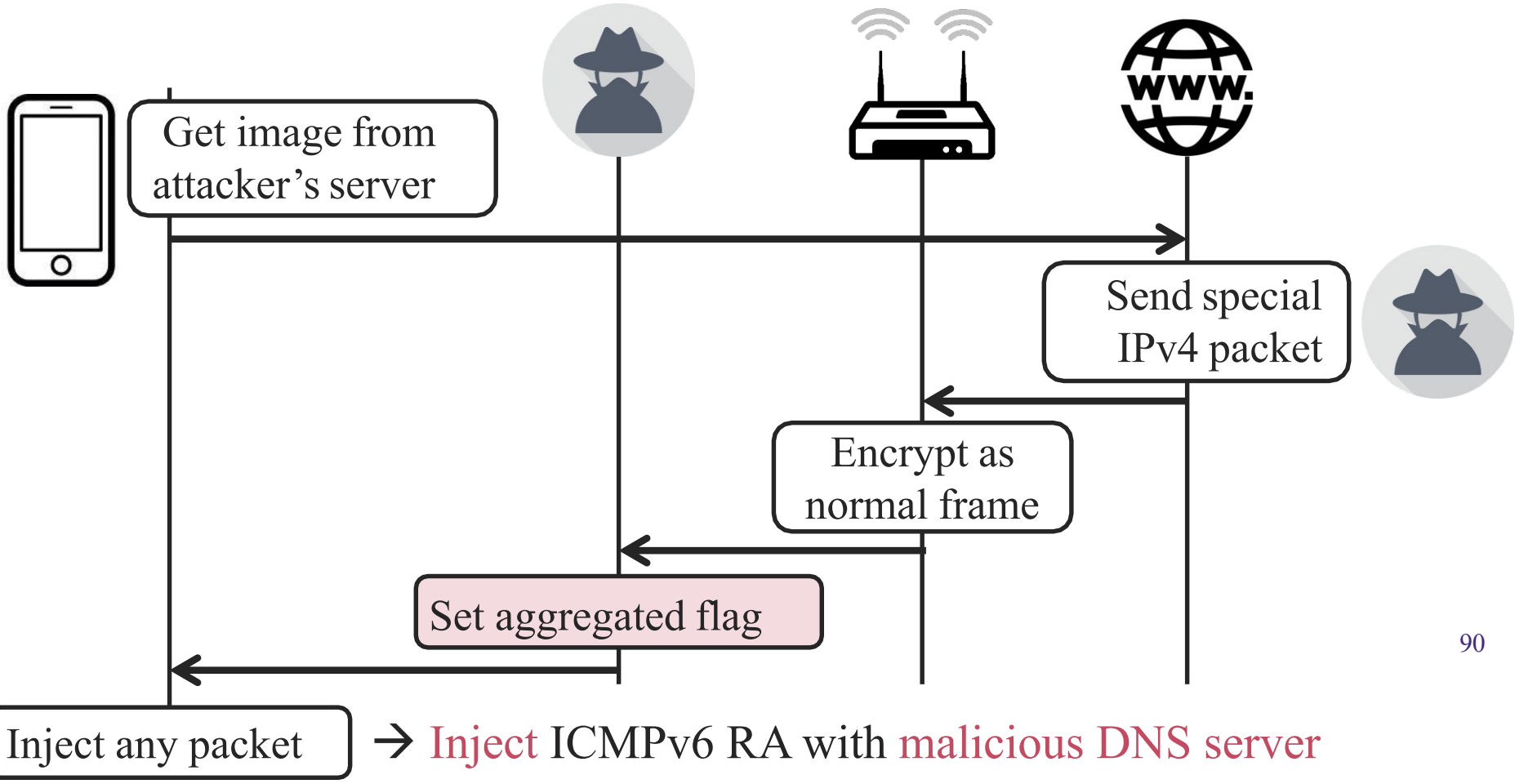
Exploit steps



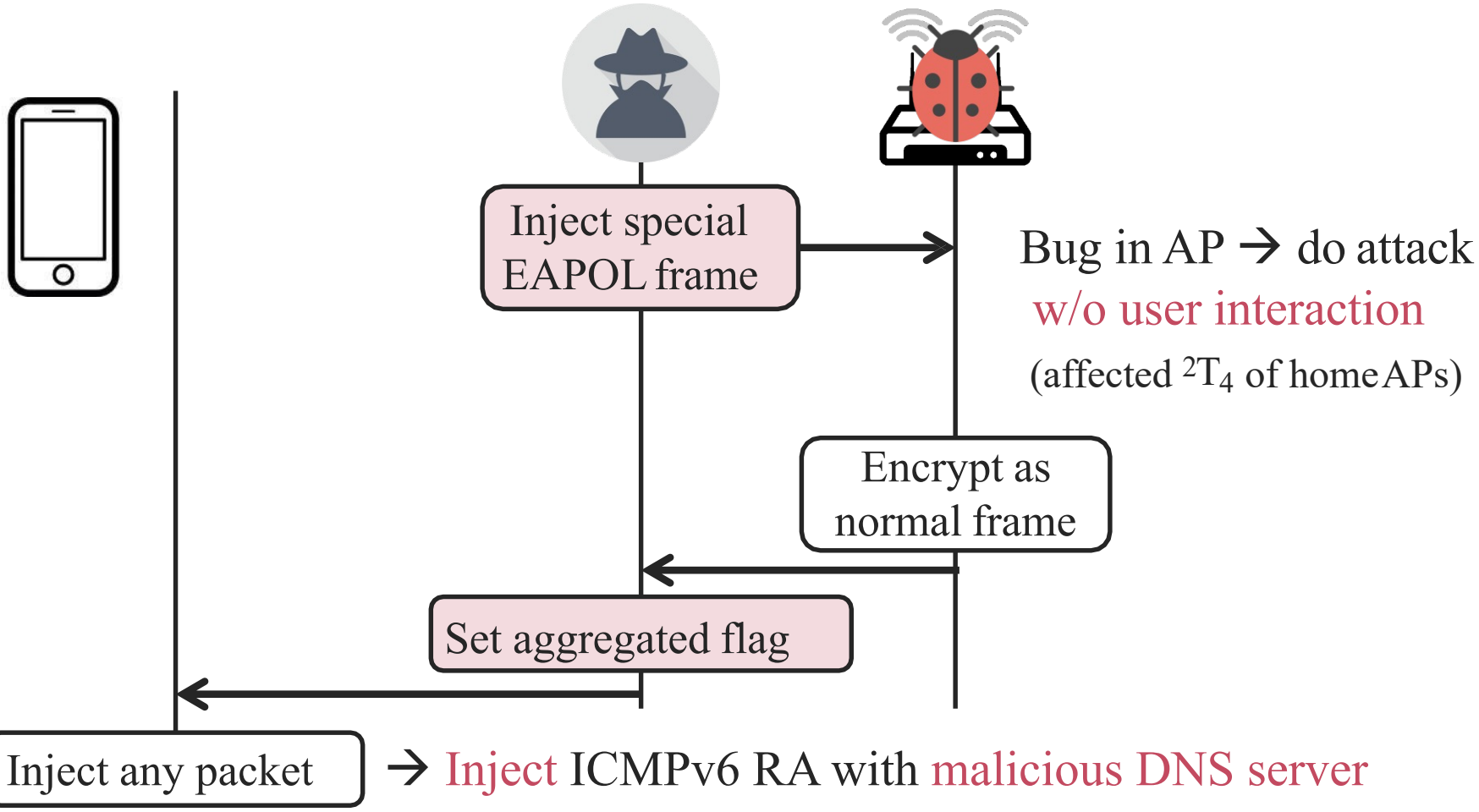
Exploit steps



Exploit steps



Exploit steps



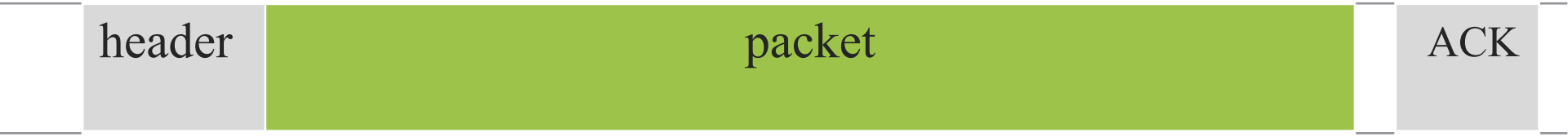
Mixed key

Fragment cache

Implementation Flaws

Background

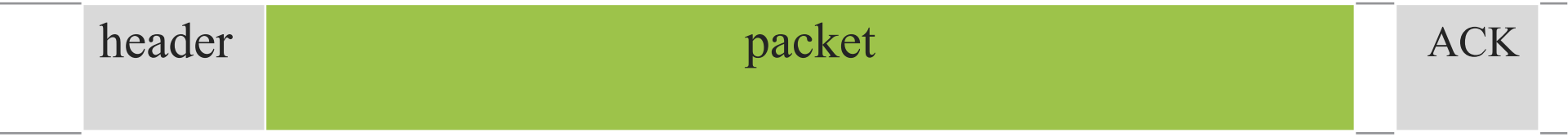
Large frames have a high chance of being corrupted:



Avoid by fragmenting & only retransmitting lost fragments:

Background

Large frames have a high chance of being corrupted:



Avoid by fragmenting & only retransmitting lost fragments:

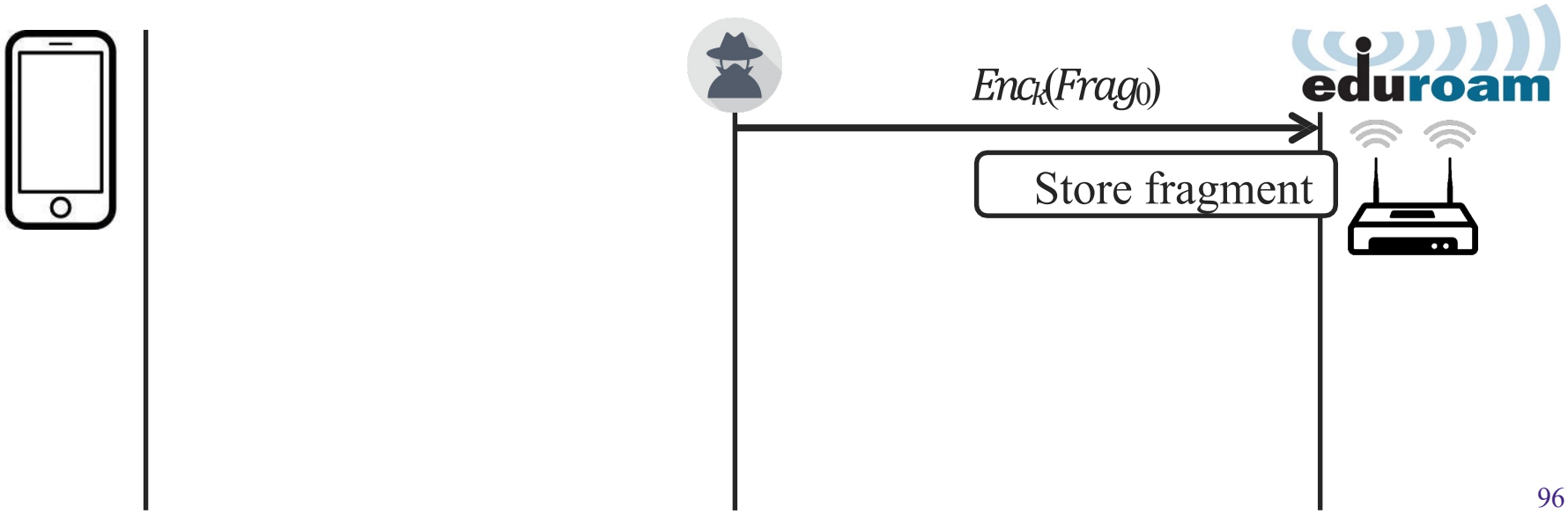
→ Protected header info defines place in original frame

Fragment cache design flaw

Fragments aren’t removed after disconnecting:

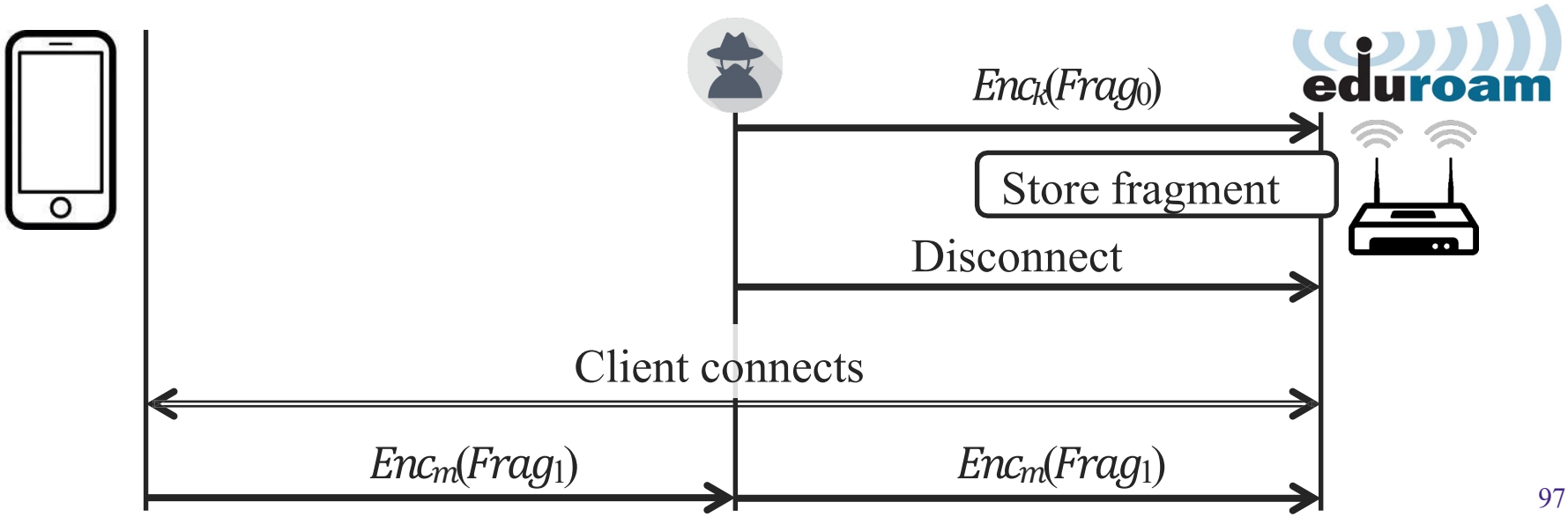
Fragment cache design flaw

Fragments aren't removed after disconnecting:



Fragment cache design flaw

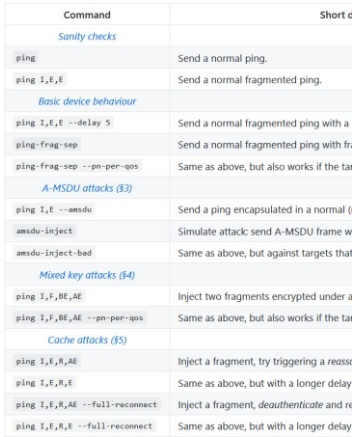
Fragments aren't removed after disconnecting:



› Attacker's $Frag_0$ and client's $Frag_1$ is reassembled

Created tool to test devices

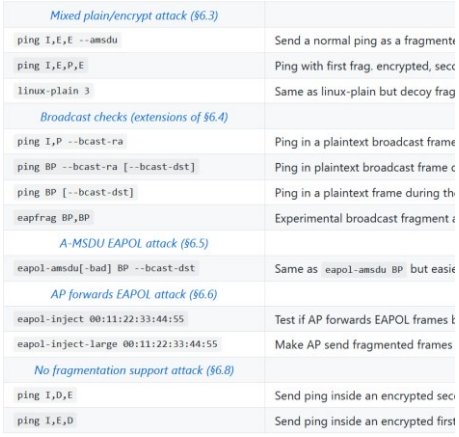
Has 45+ test cases for both clients and APs:



Command	Short d
Sanity checks	
`ping`	Send a normal ping.
`ping I,E,E`	Send a normal fragmented ping.
Basic device behaviour	
`ping I,E,E --delay 5`	Send a normal fragmented ping with a
`ping-frag-sep`	Send a normal fragmented ping with fr
`ping-frag-sep --pn-per-qos`	Same as above, but also works if the ta
A-MSDU attacks (§3)	
`ping I,E --amsdu`	Send a ping encapsulated in a normal (
`amsdu-inject`	Simulate attack: send A-MSDU frame w
`amsdu-inject-bad`	Same as above, but against targets that
Mixed key attacks (§4)	
`ping I,F,BE,AE`	Inject two fragments encrypted under a
`ping I,F,BE,AE --pn-per-qos`	Same as above, but also works if the ta
Cache attacks (§5)	
`ping I,E,R,AE`	Inject a fragment, try triggering a *reass*
`ping I,E,R,E`	Same as above, but with a longer delay
`ping I,E,R,AE --full-reconnect`	Inject a fragment, *deauthenticate* and re
`ping I,E,R,E --full-reconnect`	Same as above, but with a longer delay

Non-consecutive PNs attack (§6.2)	
`ping I,E,E --inc-pn 2`	Send a fragmented ping with non-
Mixed plain/encrypt attack (§6.3)	
`ping I,E,P`	Send a fragmented ping: first fragn
`ping I,P,E`	Send a fragmented ping: first fragn
`ping I,P`	Send a plaintext ping.
`ping I,P,P`	Send a fragmented ping: both frag
`linux-plain`	Mixed plaintext/encrypted fragmer
Broadcast fragment attack (§6.4)	
`ping I,D,P --bcast-ra`	Send a unicast ping in a plaintext b
`ping D,BP --bcast-ra`	Same as above, but frame is sent d
A-MSDU EAPOL attack (§6.5)	
`eapol-amsdu I,P`	Send a plaintext A-MSDU containir
`eapol-amsdu BP`	Same as above, but the frame is se
`eapol-amsdu-bad I,P`	Send malformed plain. A-MSDU co
`eapol-amsdu-bad BP`	Same as above, but the frame is se

Command	Short d
A-MSDU attacks (§3)	
`ping I,E --amsdu-fake`	If this test succeeds, the A-MSDU fl
`ping I,E --amsdu-fake --amsdu-spp`	Check if the A-MSDU flag is authen
Mixed key attacks (§4)	
`ping I,F,BE,E`	In case the new key is installed relat
`ping I,E,F,AE`	Variant if no data frames are accept
`ping I,E,F,AE --rekey-plain`	If the device performs the rekey ha
`ping I,E,F,AE --rekey-plain --rekey-req`	Same as above, and actively reques
`ping I,E,F,AE --rekey-early-install`	Install the new key after sending m
`ping I,E,F,E [--rekey-pl] [--rekey-req]`	Same as above 4 tests, but with lon
`ping I,F,BE,AE --freebsd`	Mixed key attack against FreeBSD c
Cache attacks (§5)	
`ping I,E,R,AE --freebsd [--full-reconnect]`	Cache attack specific to FreeBSD im
`ping I,E,R,AP --freebsd [--full-reconnect]`	Cache attack specific to FreeBSD im
`ping I,E,R,AP [--full-reconnect]`	Cache attack test where 2nd fragme



Mixed plain/encrypt attack (§6.3)	
`ping I,E,E --amsdu`	Send a normal ping as a fragmente
`ping I,E,P,E`	Ping with first frag. encrypted, secc
`linux-plain 3`	Same as linux-plain but decoy frag
Broadcast checks (extensions of §6.4)	
`ping I,P --bcast-ra`	Ping in a plaintext broadcast frame
`ping BP --bcast-ra [--bcast-dst]`	Ping in plaintext broadcast frame c
`ping BP [--bcast-dst]`	Ping in a plaintext frame during th
`eapfrag BP,BP`	Experimental broadcast fragment a
A-MSDU EAPOL attack (§6.5)	
`eapol-amsdu[-bad] BP --bcast-dst`	Same as `eapol-amsdu BP` but easie
AP forwards EAPOL attack (§6.6)	
`eapol-inject 00:11:22:33:44:55`	Test if AP forwards EAPOL frames b
`eapol-inject-large 00:11:22:33:44:55`	Make AP send fragmented frames
No fragmentation support attack (§6.8)	
`ping I,D,E`	Send ping inside an encrypted sec
`ping I,E,D`	Send ping inside an encrypted first

→ Available at https://github.com/vanhoefm/fragattack

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

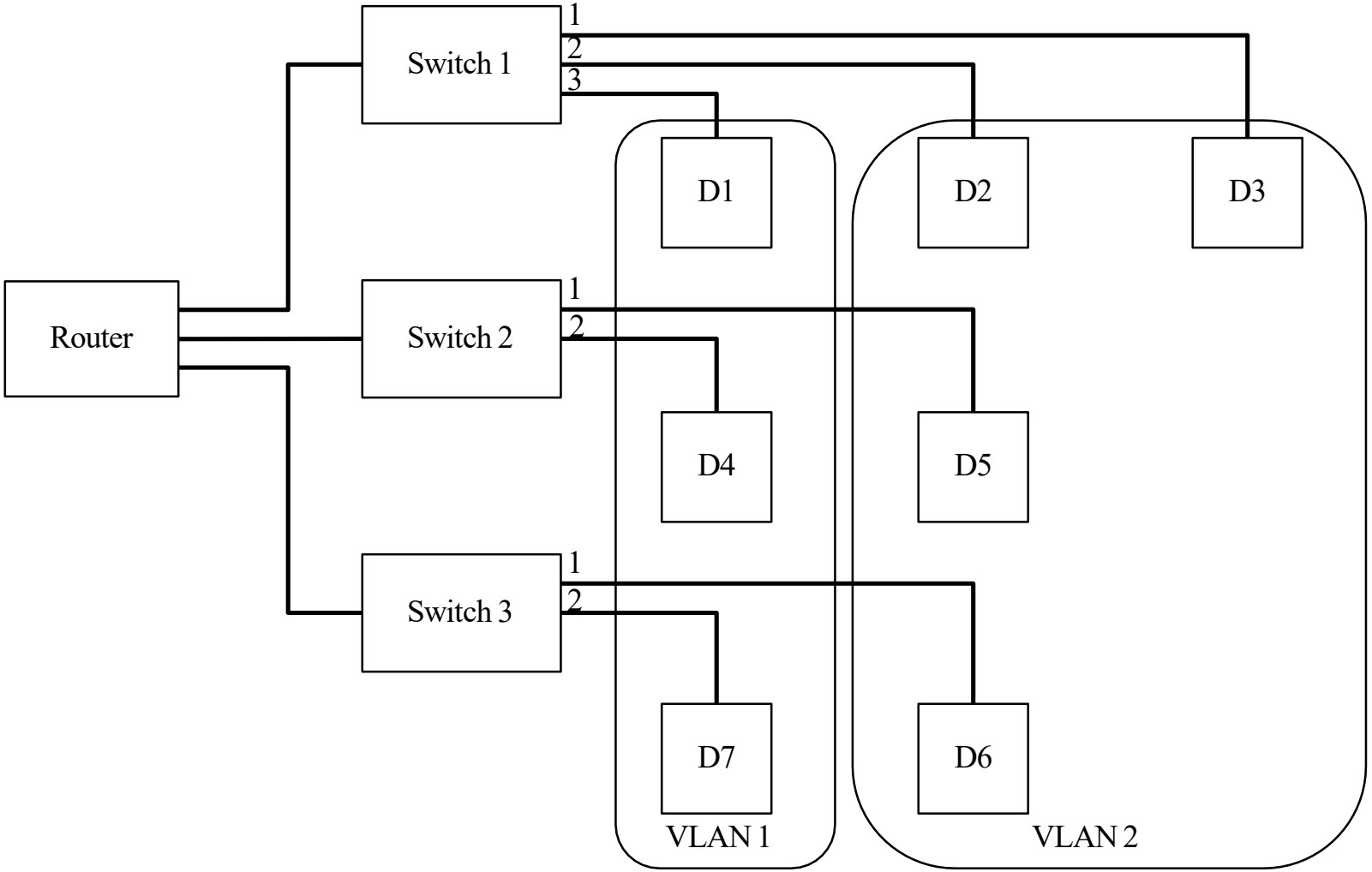
General Mitigation Methods

- VLAN
- NAC

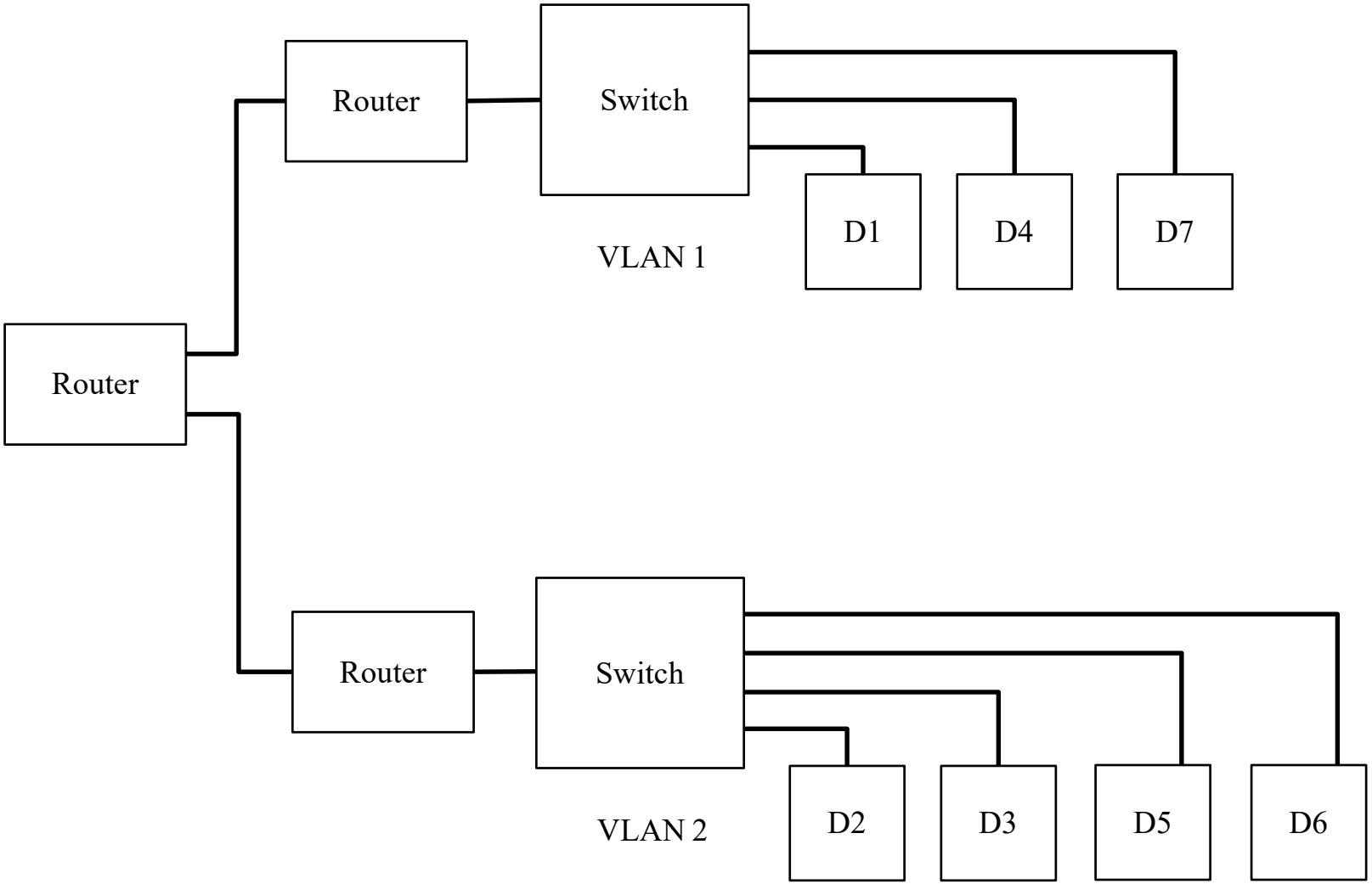
VLAN

- 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

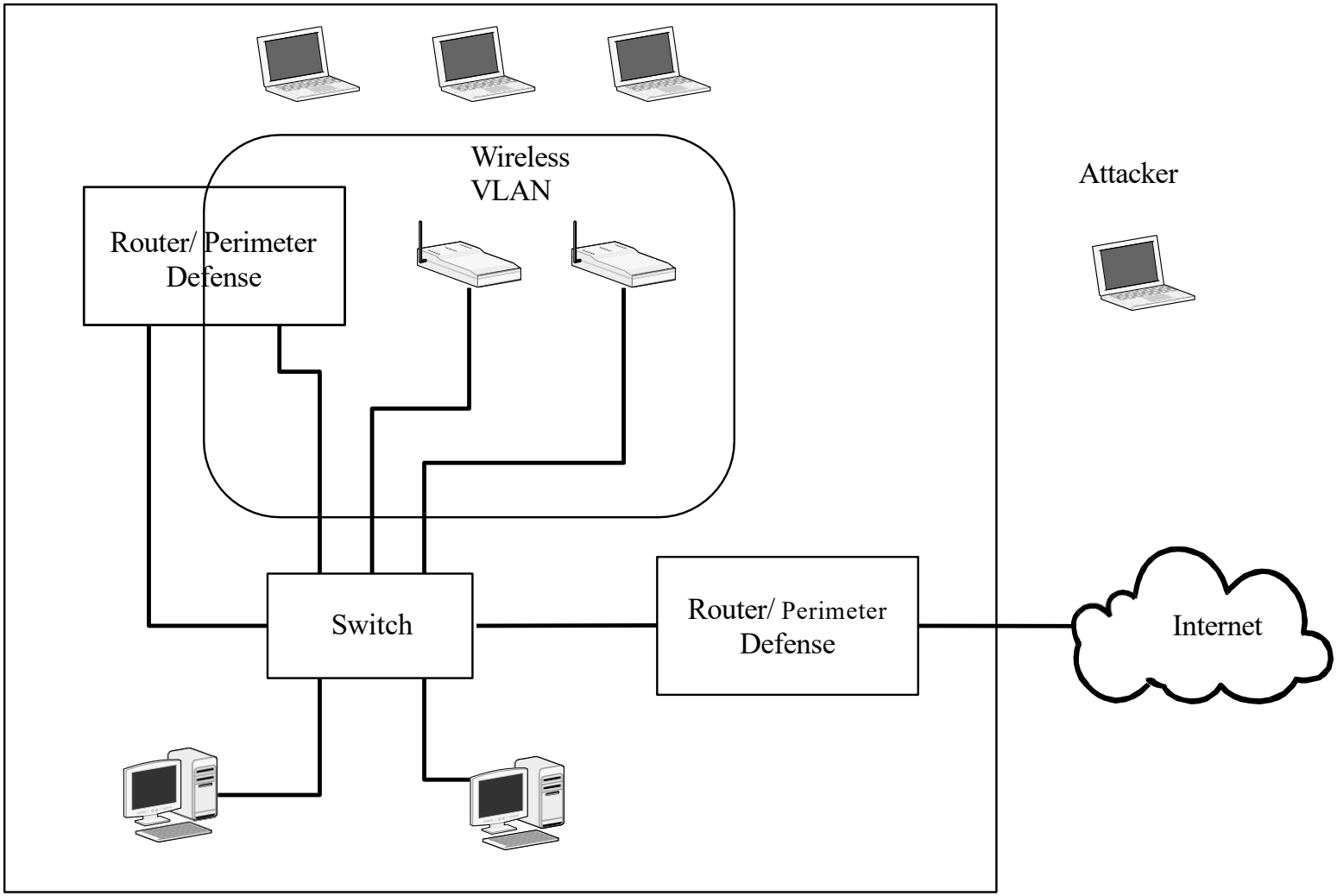
Logical View of VLAN



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