CISC 7320X - COMPUTER SECURITY

Chapter 6: Networks

From *Security in Computing, Fifth Edition*, by Charles P. Pfleeger, et al. (ISBN: 9780134085043). Copyright 2015 by Pearson Education, Inc. All rights reserved.

Objectives for Chapter 6

- Networking basics
- Network threats and vulnerabilities
- WiFi security
- Denial-of-service attacks
- Network encryption concepts and tools
- Types of firewalls and what they do
- Intrusion detection and prevention systems
- Security information and event management tools

Network Transmission Media

- Cable
- Optical fiber
- Microwave
- WiFi
- Satellite communication

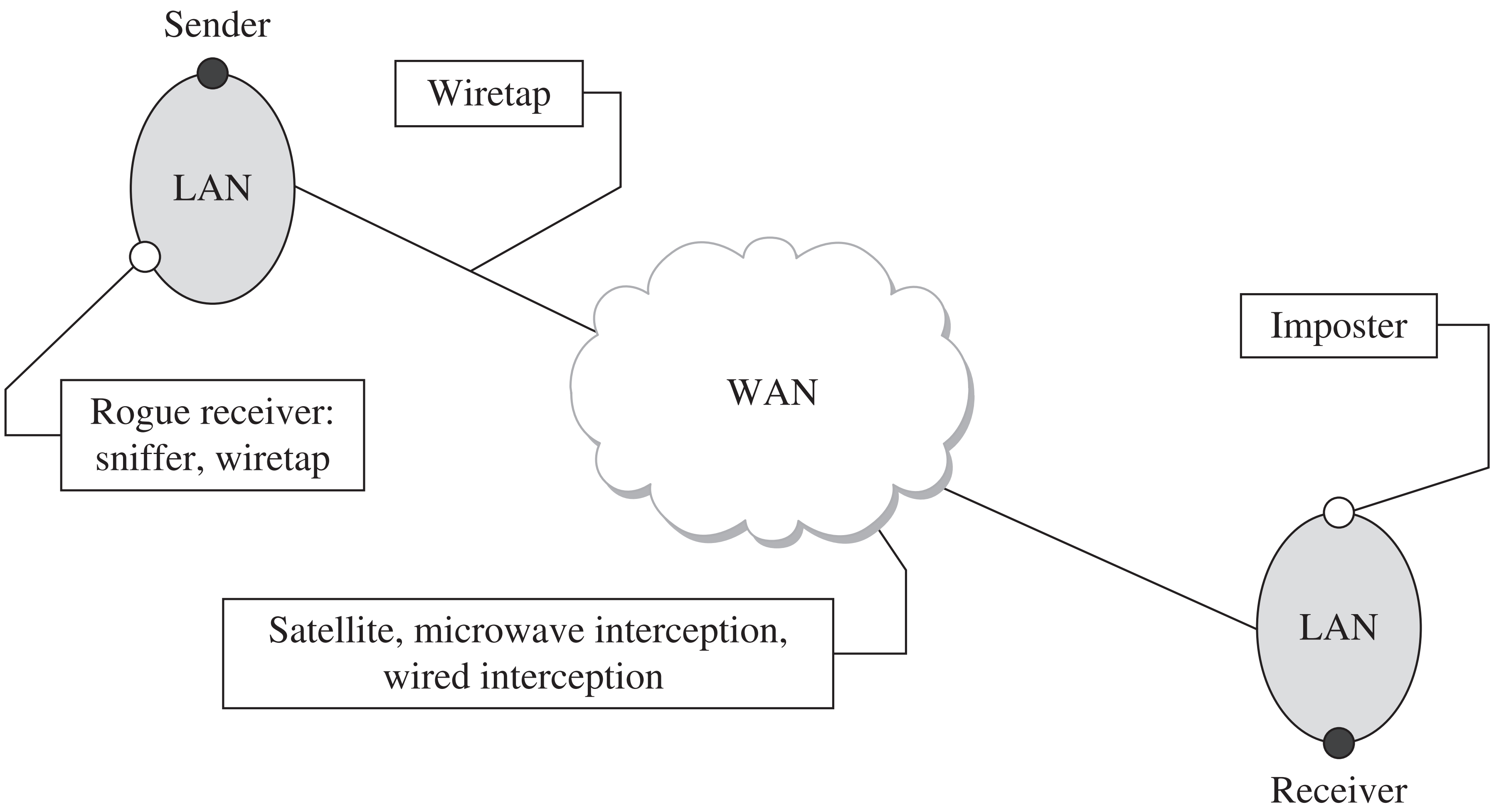
Communication Media Vulnerability

- Each transmission media has different physical properties
  - Those properties will influence their susceptibility to different kinds of attack

Communication Media Vulnerability

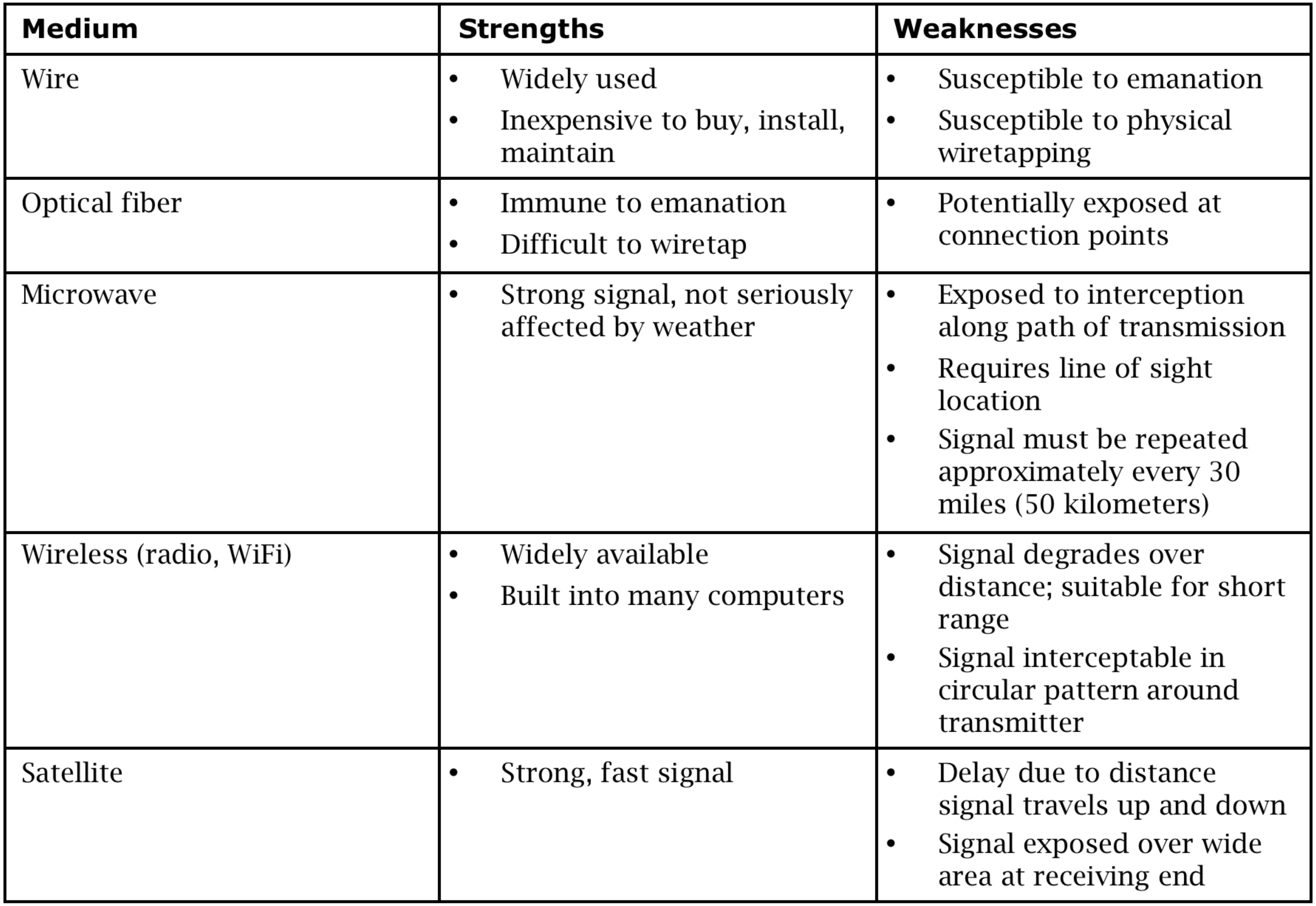
- There are different touch points where attackers can take advantage of communication media:
  - Wiretaps
  - sniffers and rogue receivers
  - Interception
  - impersonation

Communication Media Vulnerability



From *Security in Computing, Fifth Edition*, by Charles P. Pfleeger, et al. (ISBN: 9780134085043). Copyright 2015 by Pearson Education, Inc. All rights reserved.

Communication Media Pros/Cons



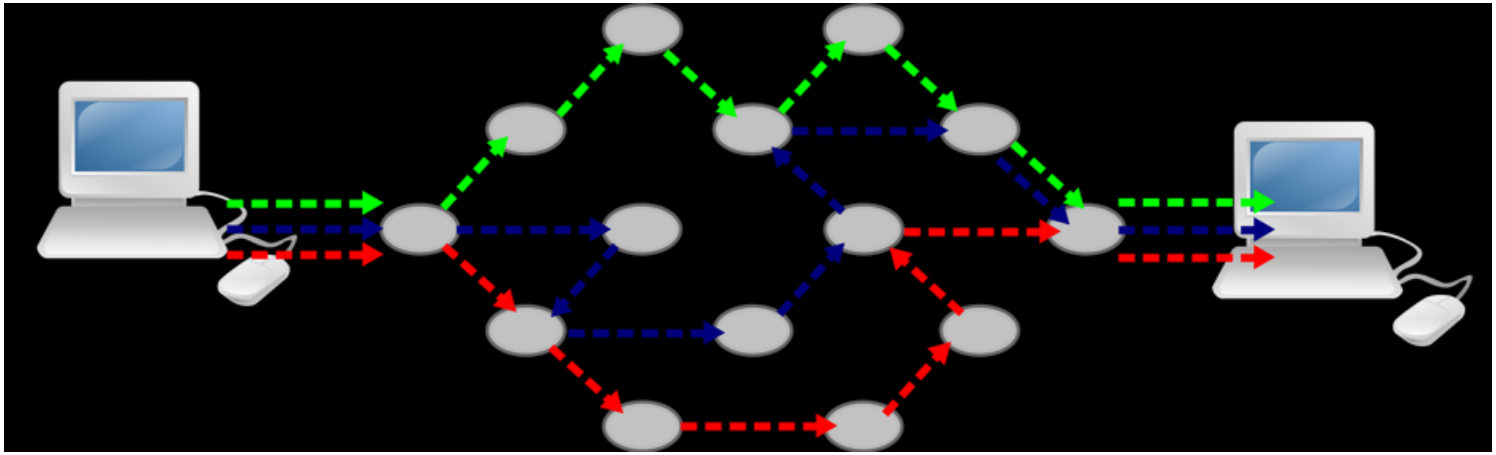
Medium	Strengths	Weaknesses
Wire	• Widely used • Inexpensive to buy, install, maintain	• Susceptible to emanation • Susceptible to physical wiretapping
Optical fiber	• Immune to emanation • Difficult to wiretap	• Potentially exposed at connection points
Microwave	• Strong signal, not seriously affected by weather	• Exposed to interception along path of transmission • Requires line of sight location • Signal must be repeated approximately every 30 miles (50 kilometers)
Wireless (radio, WiFi)	• Widely available • Built into many computers	• Signal degrades over distance; suitable for short range • Signal interceptable in circular pattern around transmitter
Satellite	• Strong, fast signal	• Delay due to distance signal travels up and down • Signal exposed over wide area at receiving end

From *Security in Computing, Fifth Edition*, by Charles P. Pfleeger, et al. (ISBN: 9780134085043). Copyright 2015 by Pearson Education, Inc. All rights reserved.

Computer Networks

https://nizamtaher.wordpress.com/topics/topic-1-introduction-of-computer-network/

Circuit and Packet Switching



http://www.apposite-tech.com/blog/uncategorized/packet-switching-vs-circuit-switching/

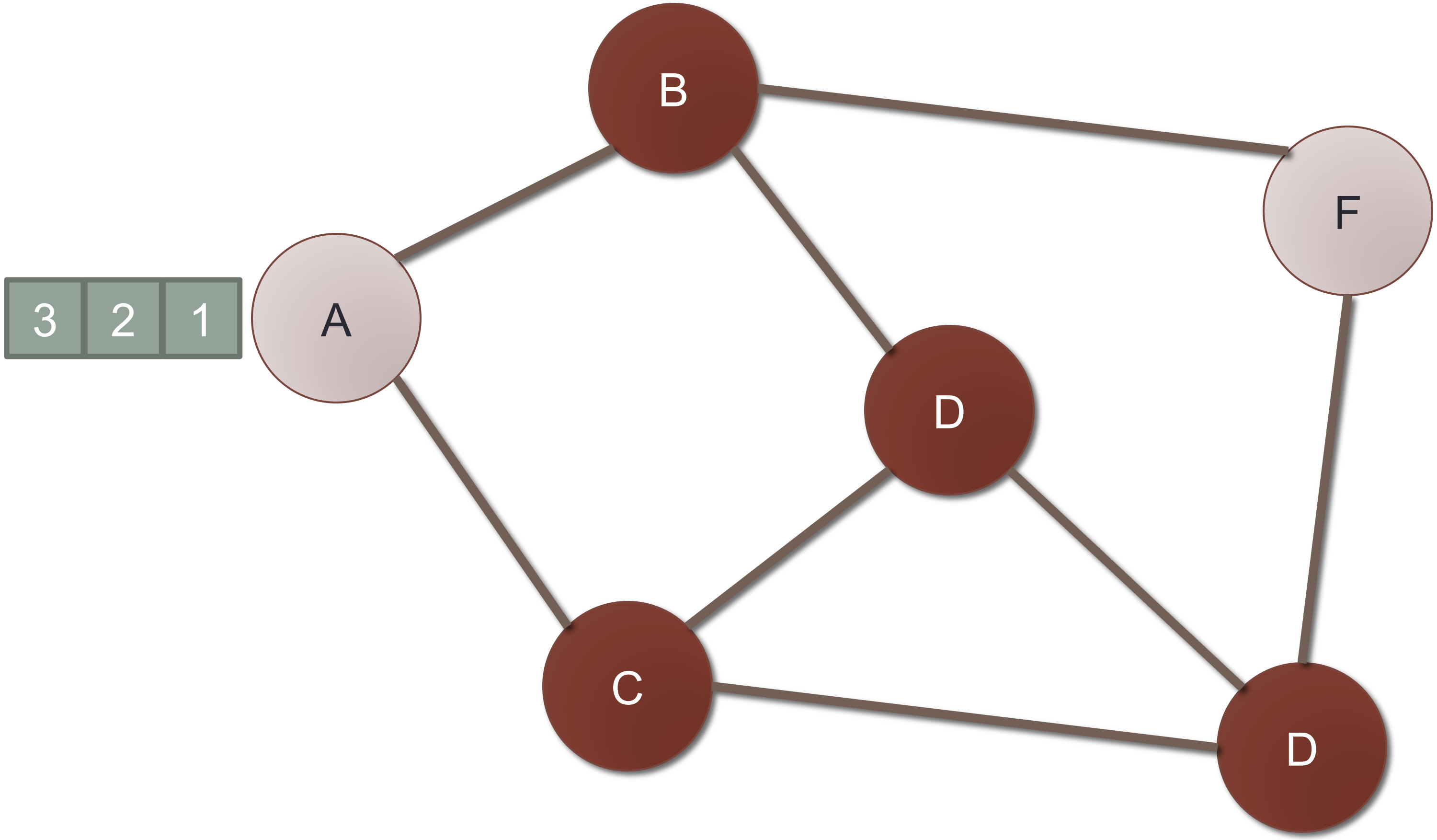
Circuit and Packet Switching

- Circuit switching
  - Legacy phone network
  - Single route through sequence of hardware devices established when two nodes start communication
  - Data sent along route
  - Route maintained until communication ends

- Packet switching
  - Internet
  - Data split into packets
  - Packets transported independently through network
  - Each packet handled on a best efforts basis
  - Packets may follow different routes

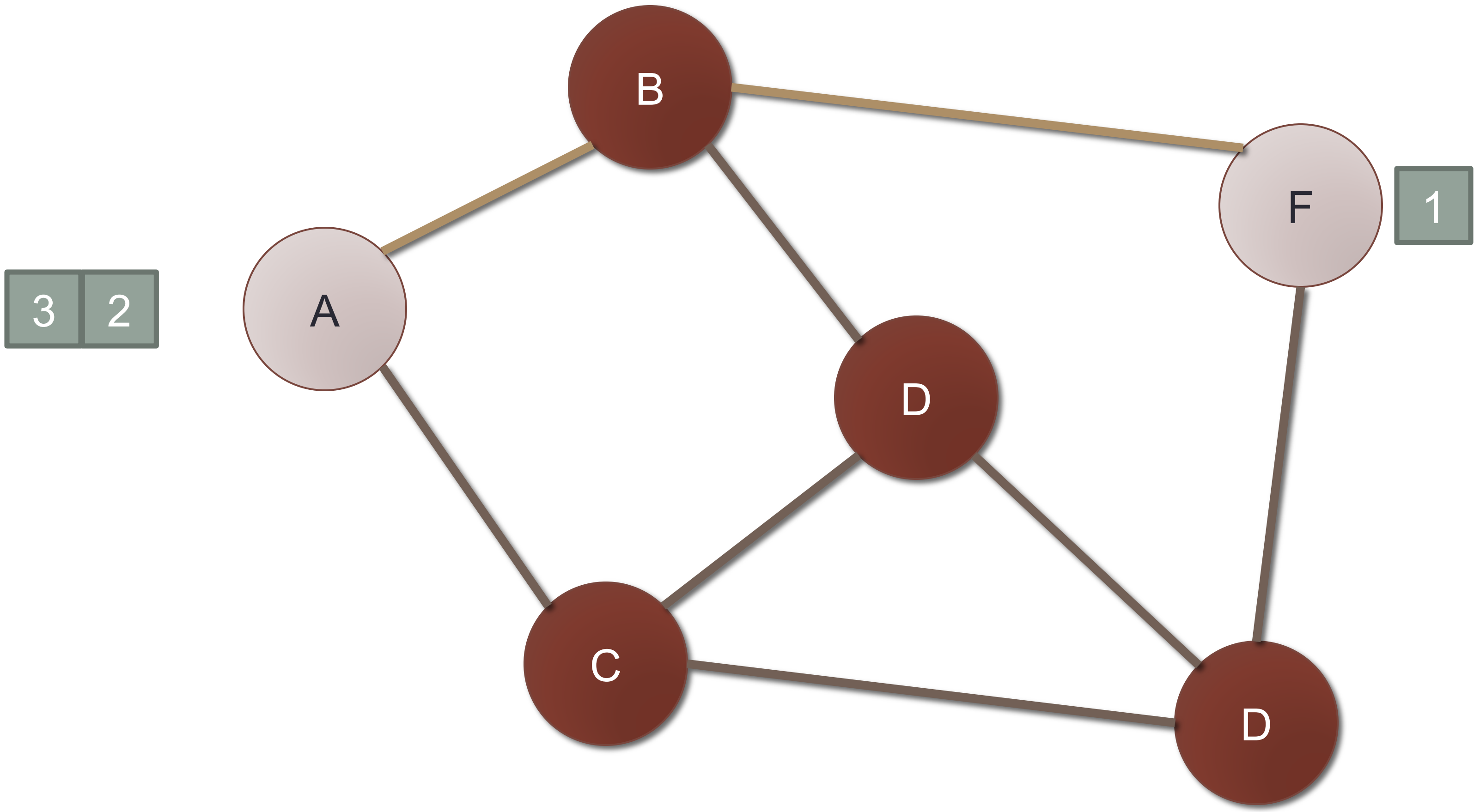
From *Security in Computing, Fifth Edition*, by Charles P. Pfleeger, et al. (ISBN: 9780134085043).

Packet Switching

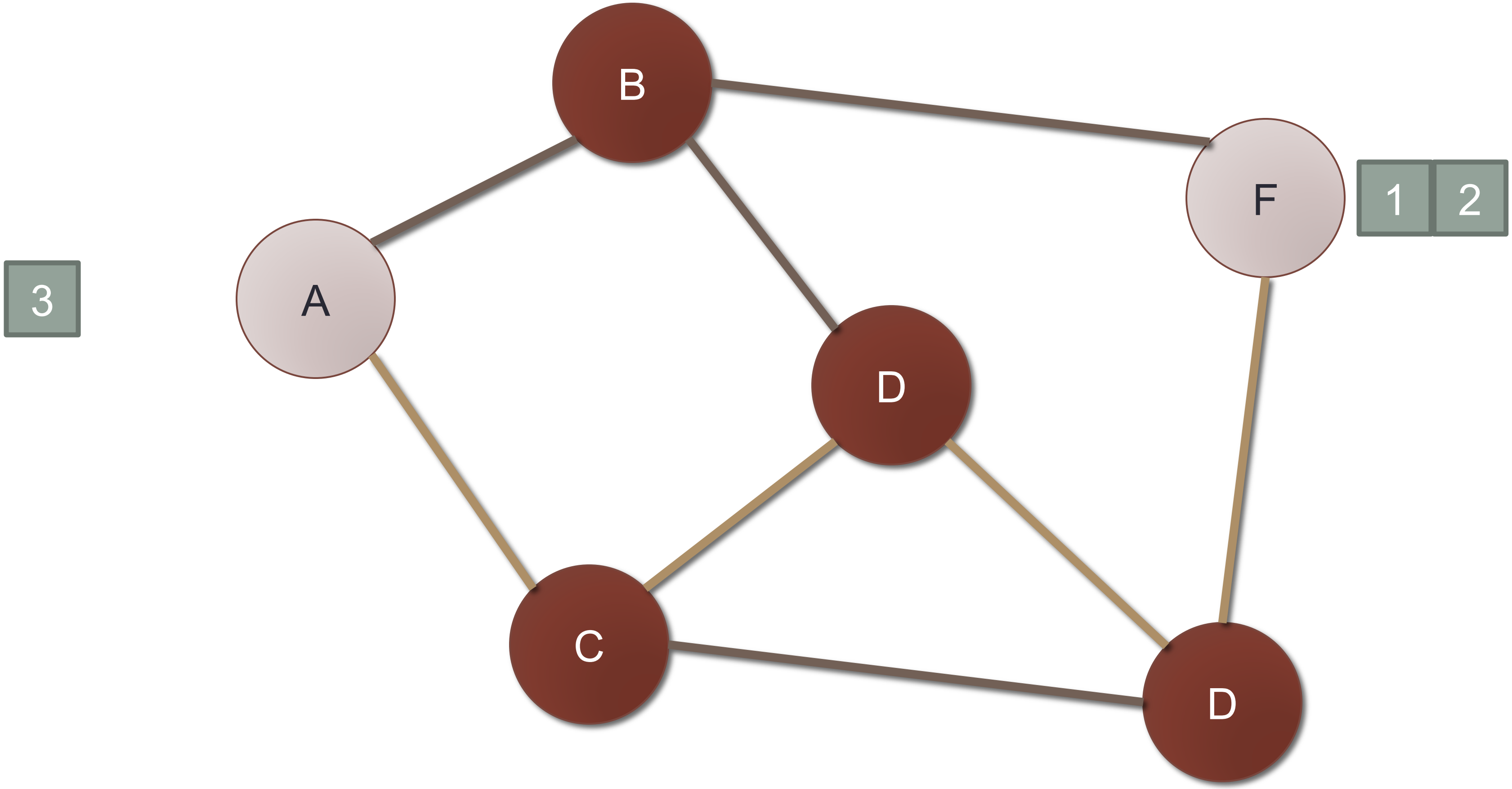


From *Security in Computing, Fifth Edition*, by Charles P. Pfleeger, et al. (ISBN: 9780134085043). Copyright 2015 by Pearson Education, Inc. All rights reserved.

Packet Switching

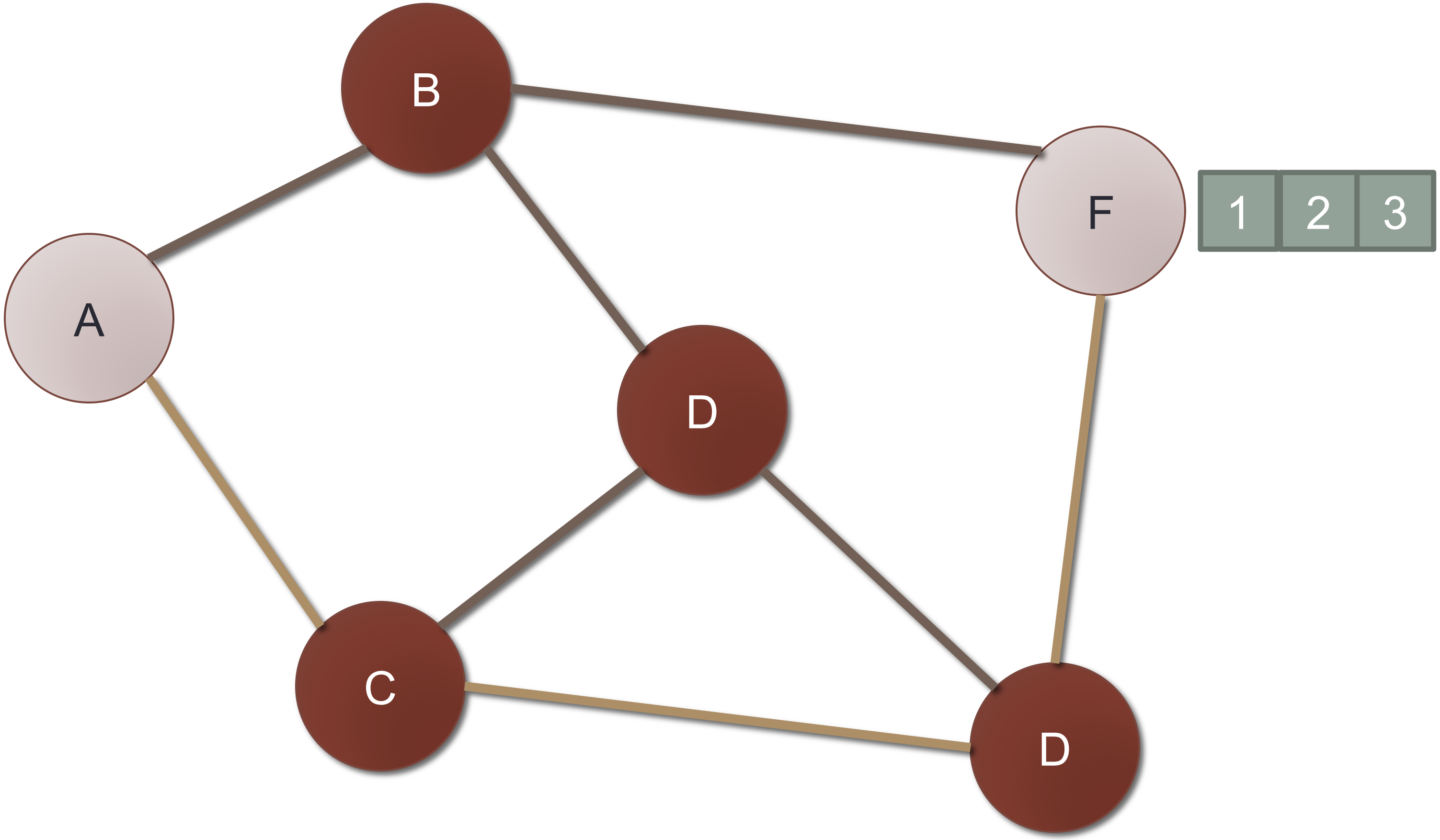


Packet Switching

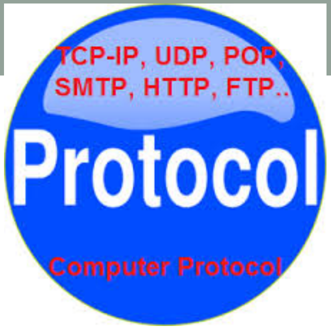


From *Security in Computing, Fifth Edition*, by Charles P. Pfleeger, et al. (ISBN: 9780134085043). Copyright 2015 by Pearson Education, Inc. All rights reserved.

Packet Switching



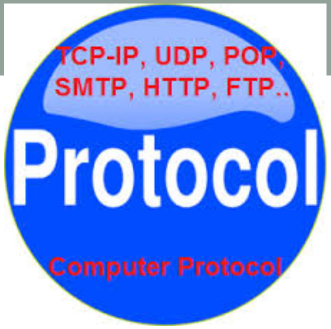
From *Security in Computing, Fifth Edition*, by Charles P. Pfleeger, et al. (ISBN: 9780134085043). Copyright 2015 by Pearson Education, Inc. All rights reserved.



Protocols

- A protocol defines the rules for communication between computers
- Protocols are broadly classified as connectionless and connection oriented

http://www.hinditechy.com/what-is-protocol-in-networking-hindi/

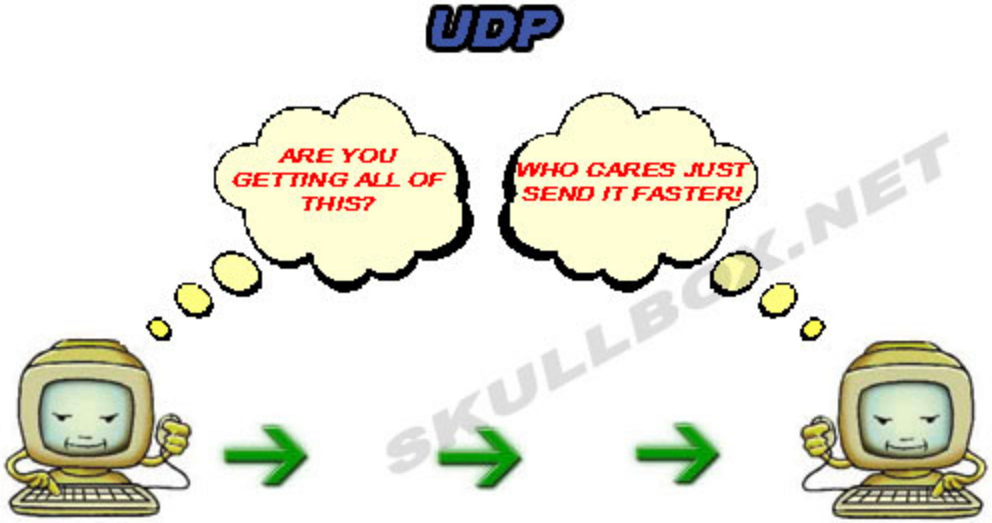


Protocols

- Connectionless protocol
  - Sends data out as soon as there is enough data to be transmitted
  - E.g., user datagram protocol (UDP)
- Connection-oriented protocol
  - Provides a reliable connection stream between two nodes
  - Consists of set up, transmission, and tear down phases
  - Creates virtual circuit-switched network
  - E.g., transmission control protocol (TCP)

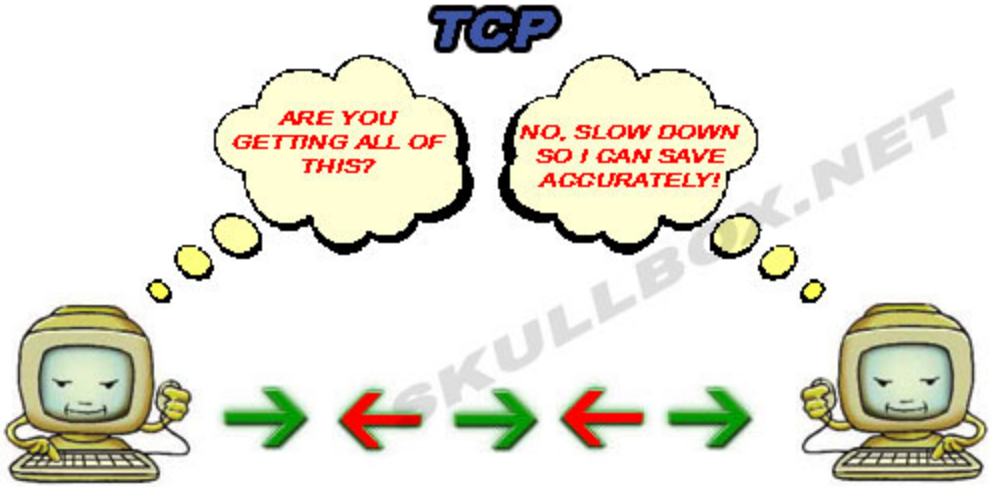
http://www.hinditechy.com/what-is-protocol-in-networking-hindi/

Connectionless protocol



https://www.b4x.com/android/forum/threads/question-about-two-way-communication-using-udp.17316/

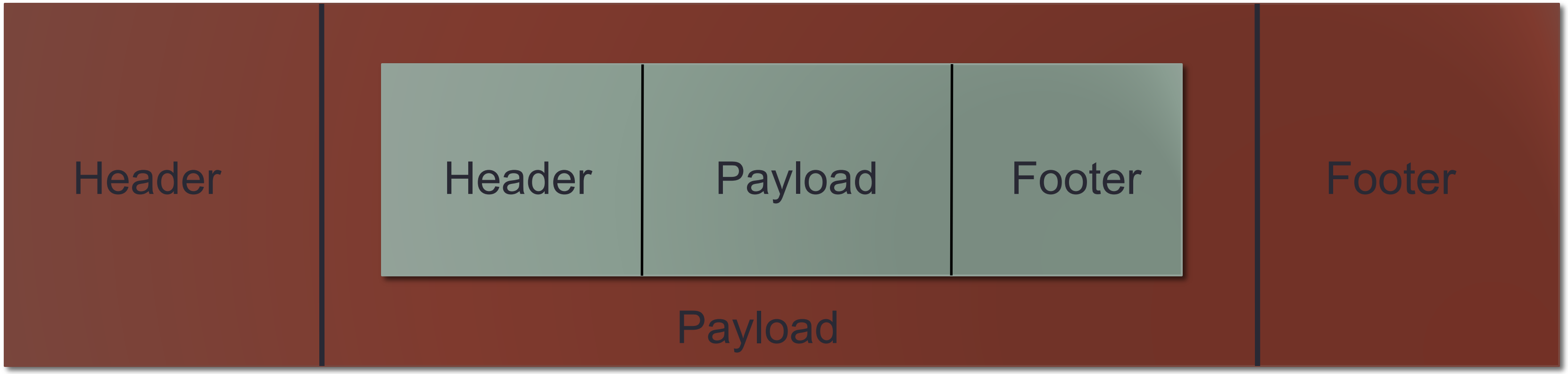
Connection-oriented protocol


TCP
ARE YOU GETTING ALL OF THIS?
NO, SLOW DOWN SO I CAN SAVE ACCURATELY!

From *Security in Computing, Fifth Edition*, by Charles P. Pfleeger, et al. (ISBN: 9780134085043). Copyright 2015 by Pearson Education, Inc. All rights reserved.

Encapsulation

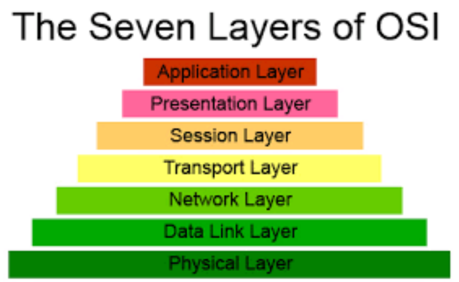
- A packet typically consists of
  - Control information for addressing the packet: header and footer
  - Data: payload
- A network protocol N1 can use the services of another network protocol N2
  - A packet p1 of N1 is encapsulated into a packet p2 of N2
  - The payload of p2 is p1
  - The control information of p2 is derived from that of p1



From *Security in Computing, Fifth Edition*, by Charles P. Pfleeger, et al. (ISBN: 9780134085043). Copyright 2015 by Pearson Education, Inc. All rights reserved.

From *Security in Computing, Fifth Edition*, by Charles P. Pfleeger, et al. (ISBN: 9780134085043). Copyright 2015 by Pearson Education, Inc. All rights reserved.

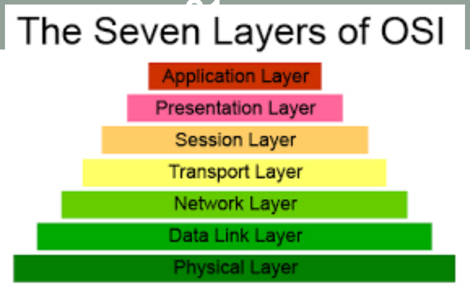
https://www.facebook.com/utplacentaencapsulation/



Network Layers

- Network models typically use a stack of layers
  - Higher layers use the services of lower layers via encapsulation
  - A layer can be implemented in hardware or software
  - The bottommost layer must be in hardware
- A network device may implement several layers

https://techiemaster.wordpress.com/2016/08/15/osi-layer/

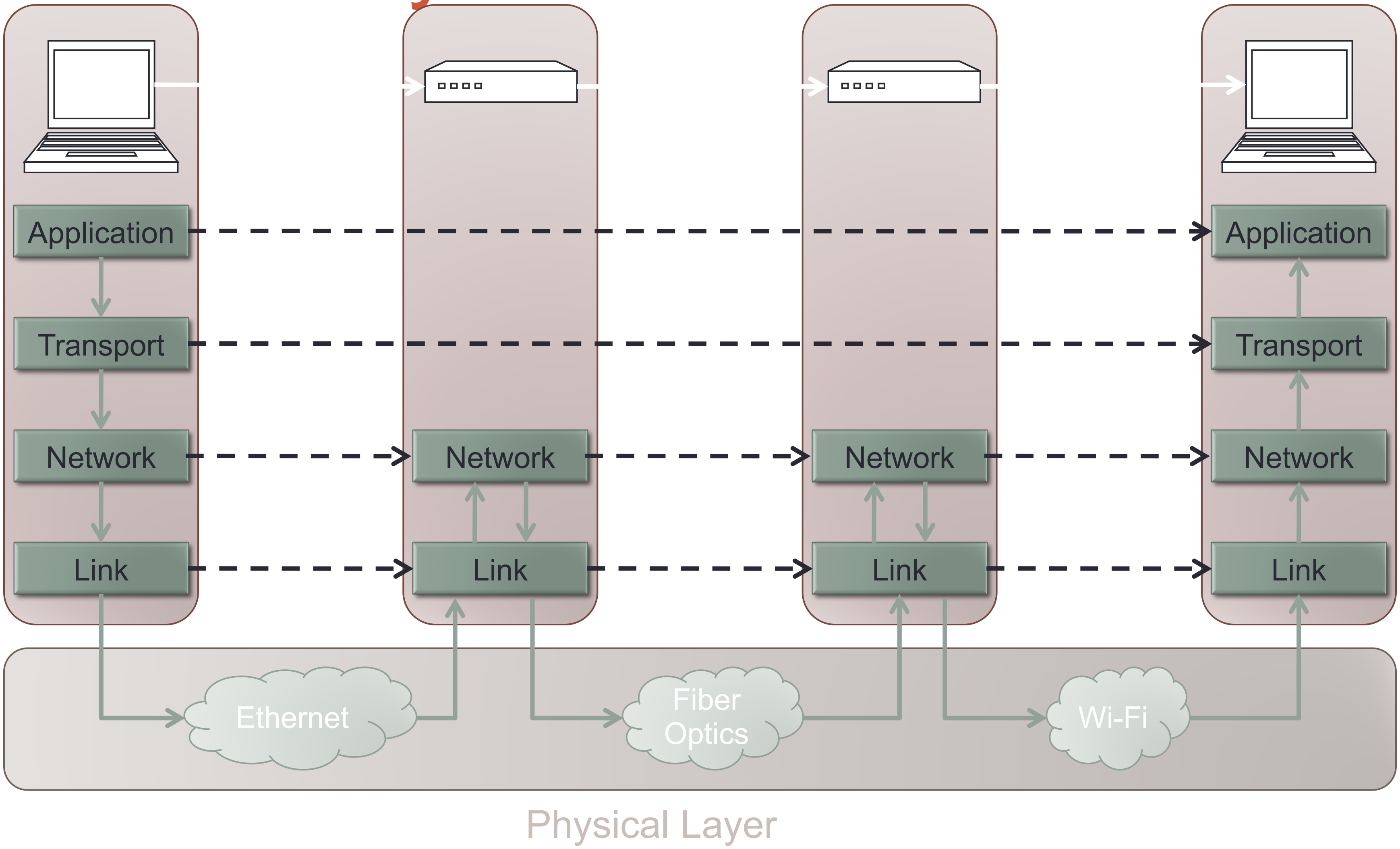


Network Layers

- A communication channel between two nodes is established for each layer
  - Actual channel at the bottom layer
  - Virtual channel at higher layers

https://techiemaster.wordpress.com/2016/08/15/osi-layer/

Internet Layers

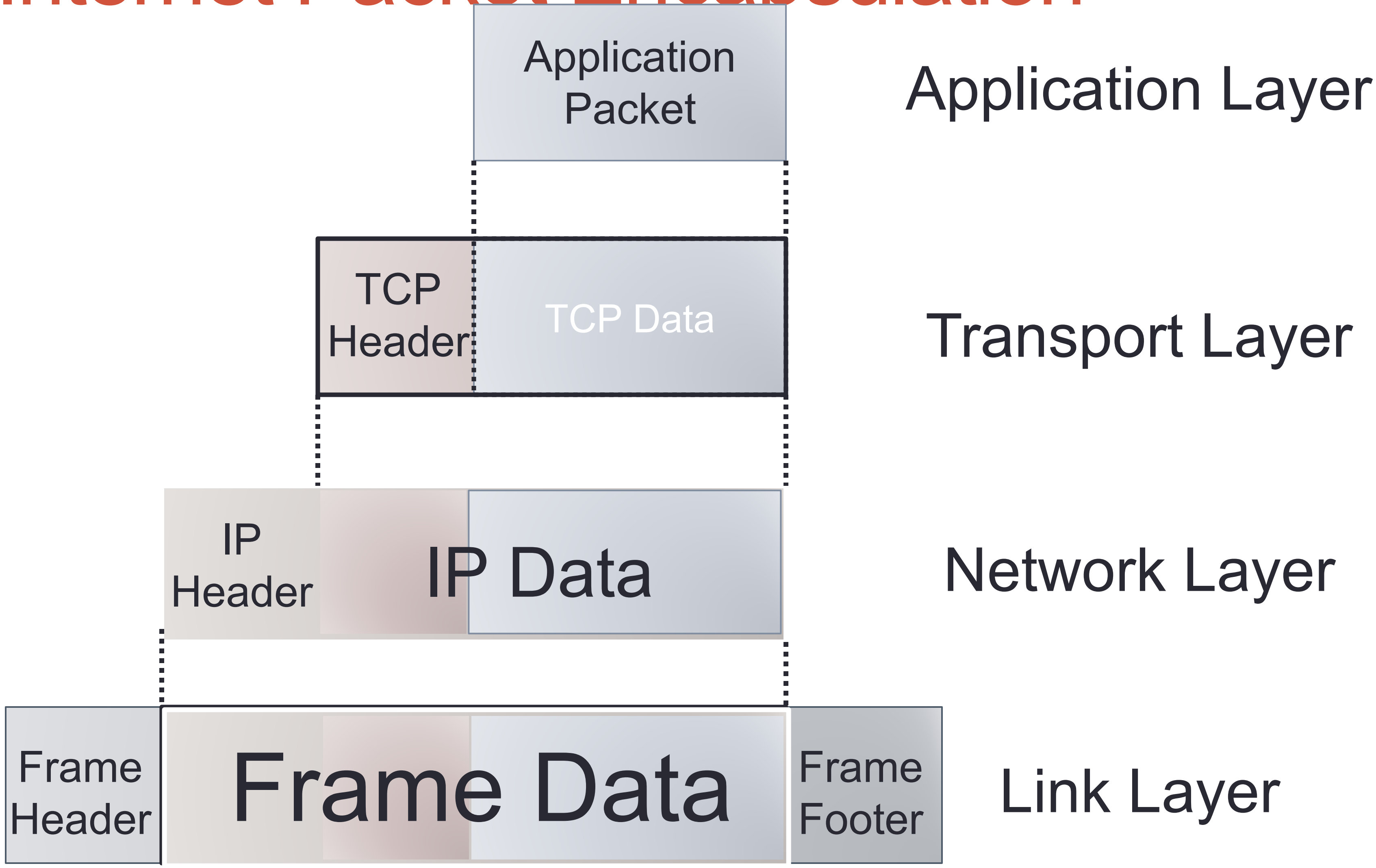


From *Security in Computing, Fifth Edition*, by Charles P. Pfleeger, et al. (ISBN: 9780134085043). Copyright 2015 by Pearson Education, Inc. All rights reserved.

Intermediate Layers

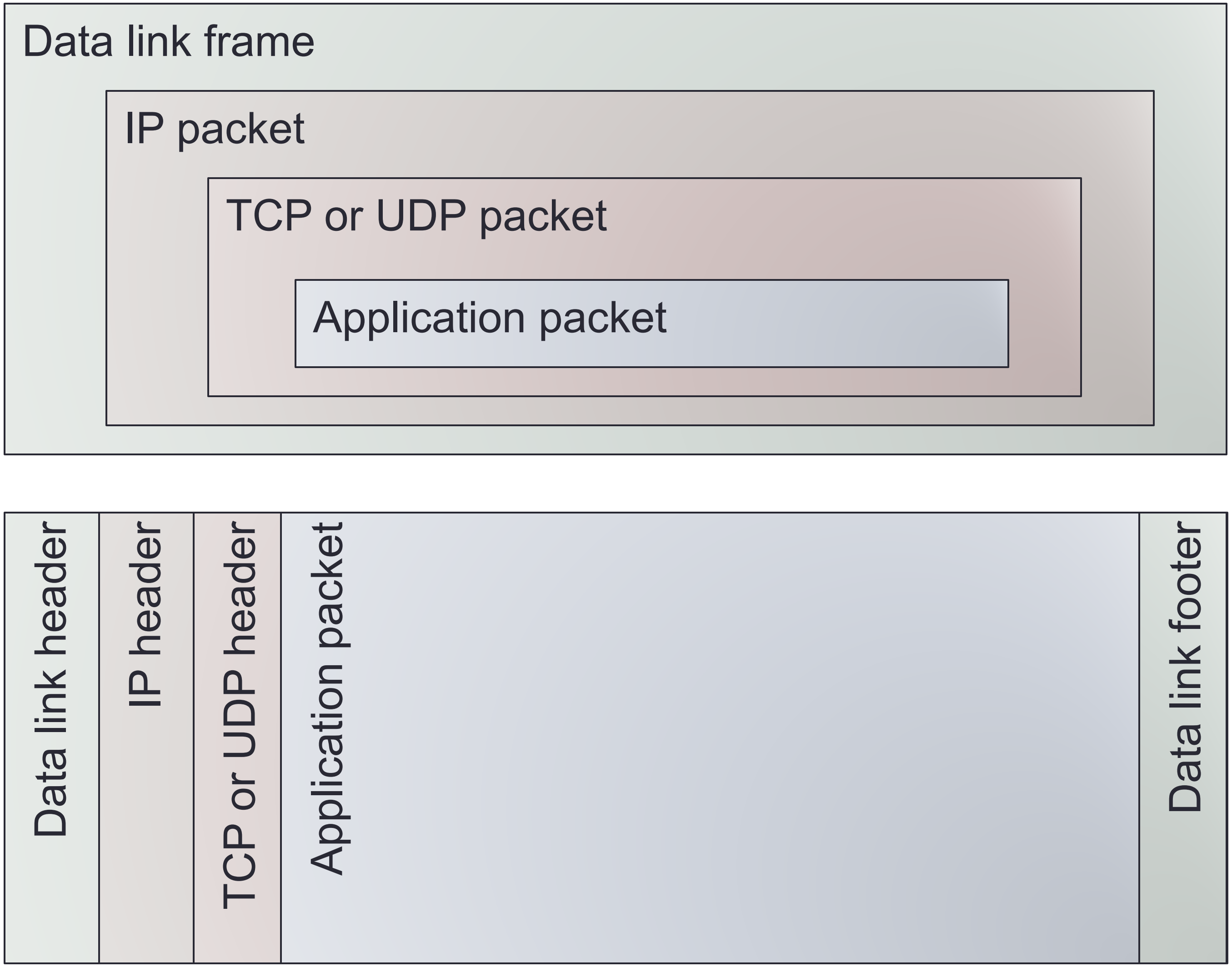
- Link layer
  - Local area network: Ethernet, WiFi, optical fiber
  - 48-bit media access control (MAC) addresses
  - Packets called frames
- Network layer
  - Internet-wide communication
  - Best efforts
  - 32-bit internet protocol (IP) addresses in IPv4
  - 128-bit IP addresses in IPv6
- Transport layer
  - 16-bit addresses (ports) for classes of applications
  - Connection-oriented transmission layer protocol (TCP)
  - Connectionless user datagram protocol (UDP)

Internet Packet Encapsulation



From *Security in Computing, Fifth Edition*, by Charles P. Pfleeger, et al. (ISBN: 9780134085043). Copyright 2015 by Pearson Education, Inc. All rights reserved.

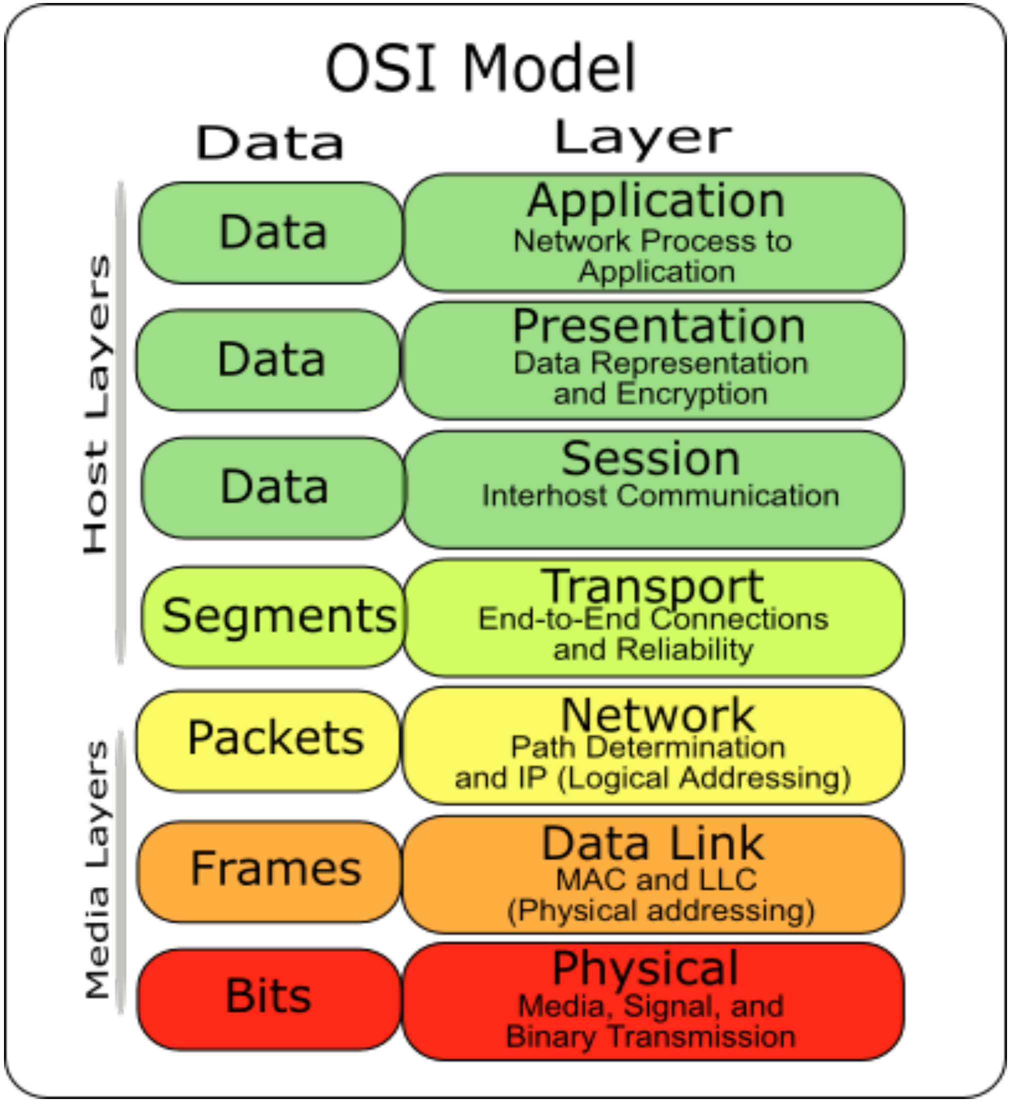
Internet Packet Encapsulation



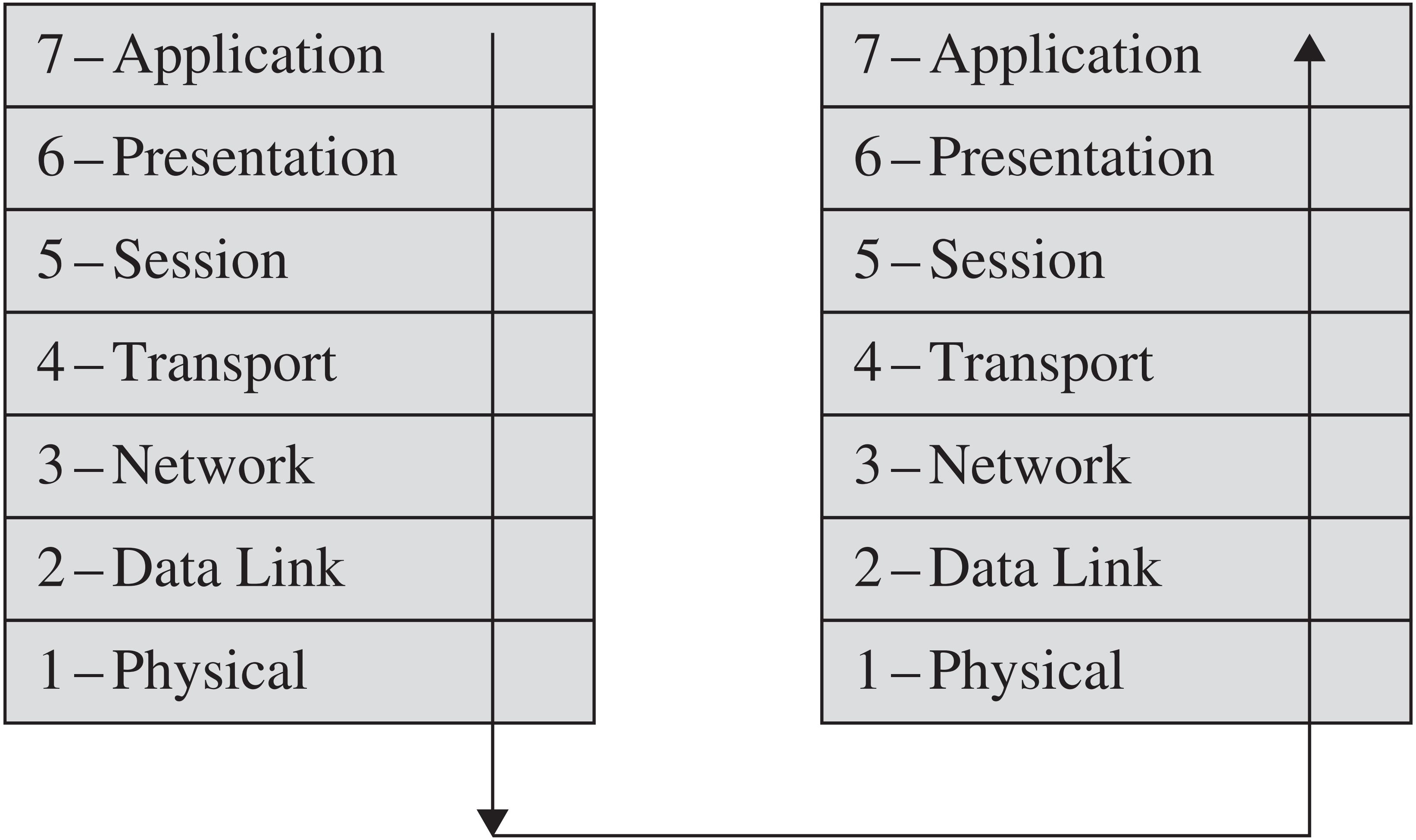
From *Security in Computing, Fifth Edition*, by Charles P. Pfleeger, et al. (ISBN: 9780134085043). Copyright 2015 by Pearson Education, Inc. All rights reserved.

The OSI Model

- The OSI (Open System Interconnect) Reference Model is a network model consisting of seven layers
- Created in 1983
- Promoted by the International Standard Organization (ISO)


OSI Model
Data
Layer
Host Layers
Media Layers
Data
Application
Network Process to Application
Data
Presentation
Data Representation and Encryption
Data
Session
Interhost Communication
Segments
Transport
End-to-End Connections and Reliability
Packets
Network
Path Determination and IP (Logical Addressing)
Frames
Data Link
MAC and LLC (Physical addressing)
Bits
Physical
Media, Signal, and Binary Transmission

The OSI Model



7 – Application

6 – Presentation

5 – Session

4 – Transport

3 – Network

2 – Data Link

1 – Physical

7 – Application

6 – Presentation

5 – Session

4 – Transport

3 – Network

2 – Data Link

1 – Physical

From *Security in Computing, Fifth Edition*, by Charles P. Pfleeger, et al. (ISBN: 9780134085043). Copyright 2015 by Pearson Education, Inc. All rights reserved.

The OSI Model

- The OSI model doesn’t map perfectly to the network protocol stack that was adopted in practice
- However, it is conceptually useful and stood the test of time.
- Most layers have their own vulnerabilities, attacks against, and countermeasures.
    - Useful attacks can occur at any layer, so all require protecting.

Network Interfaces

- Network interface: device connecting a computer to a network
  - Ethernet card
  - WiFi adapter
- A computer may have multiple network interfaces
- Packets transmitted between network interfaces
- Most local area networks, (including Ethernet and WiFi) broadcast frames

Network Interfaces

- In regular mode, each network interface gets the frames intended for it
- Traffic sniffing can be accomplished by configuring the network interface to read all frames (promiscuous mode)

MAC Addresses

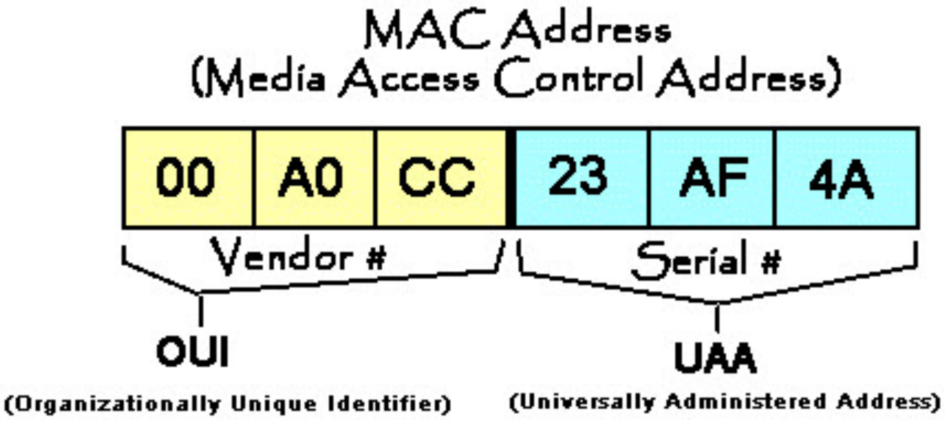
- Most network interfaces come with a predefined MAC address
- A MAC address is a 48-bit number usually represented in hex
  - E.g., 00-1A-92-D4-BF-86
- The first three octets of any MAC address are IEEE-assigned Organizationally Unique Identifiers
  - E.g., Cisco 00-1A-A1, D-Link 00-1B-11, ASUSTek 00-1A-92

From *Security in Computing, Fifth Edition*, by Charles P. Pfleeger, et al. (ISBN: 9780134085043). Copyright 2015 by Pearson Education, Inc. All rights reserved.

MAC Addresses

- The next three can be assigned by organizations as they please, with uniqueness being the only constraint
- Organizations can utilize MAC addresses to identify computers on their network
- MAC address can be reconfigured by network interface driver software

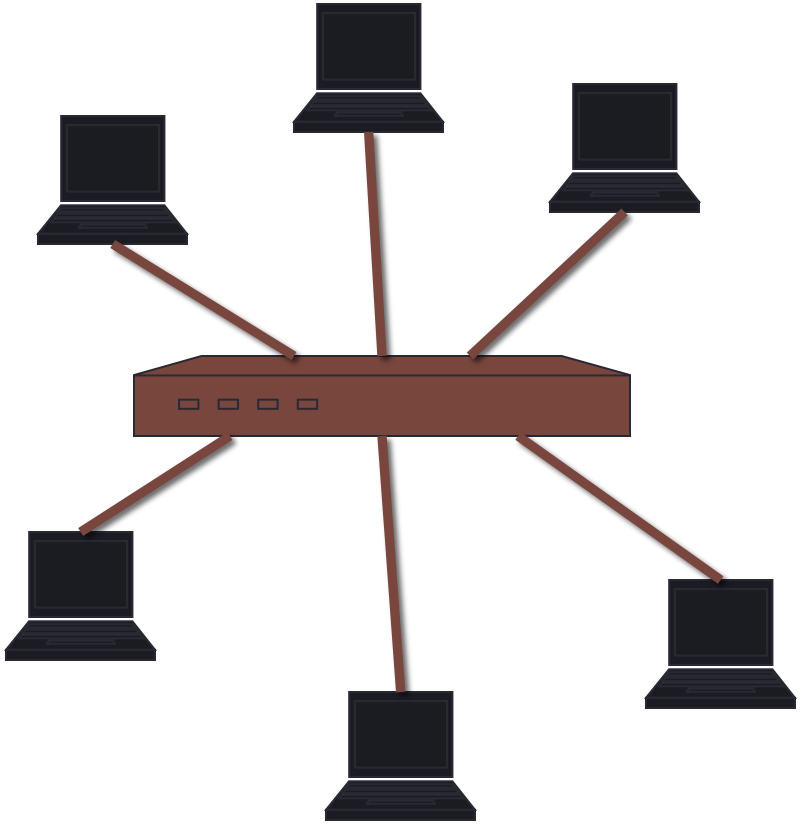
MAC Address


MAC Address
(Media Access Control Address)
00
A0
CC
23
AF
4A
Vendor #
Serial #
OUI
(Organizationally Unique Identifier)
UAA
(Universally Administered Address)

http://www.thewindowsclub.com/change-mac-address-in-windows

Switch

- A switch is a common network device
  - Operates at the link layer
  - Has multiple ports, each connected to a computer
- Operation of a switch
  - Learn the MAC address of each computer connected to it
  - Forward frames only to the destination computer

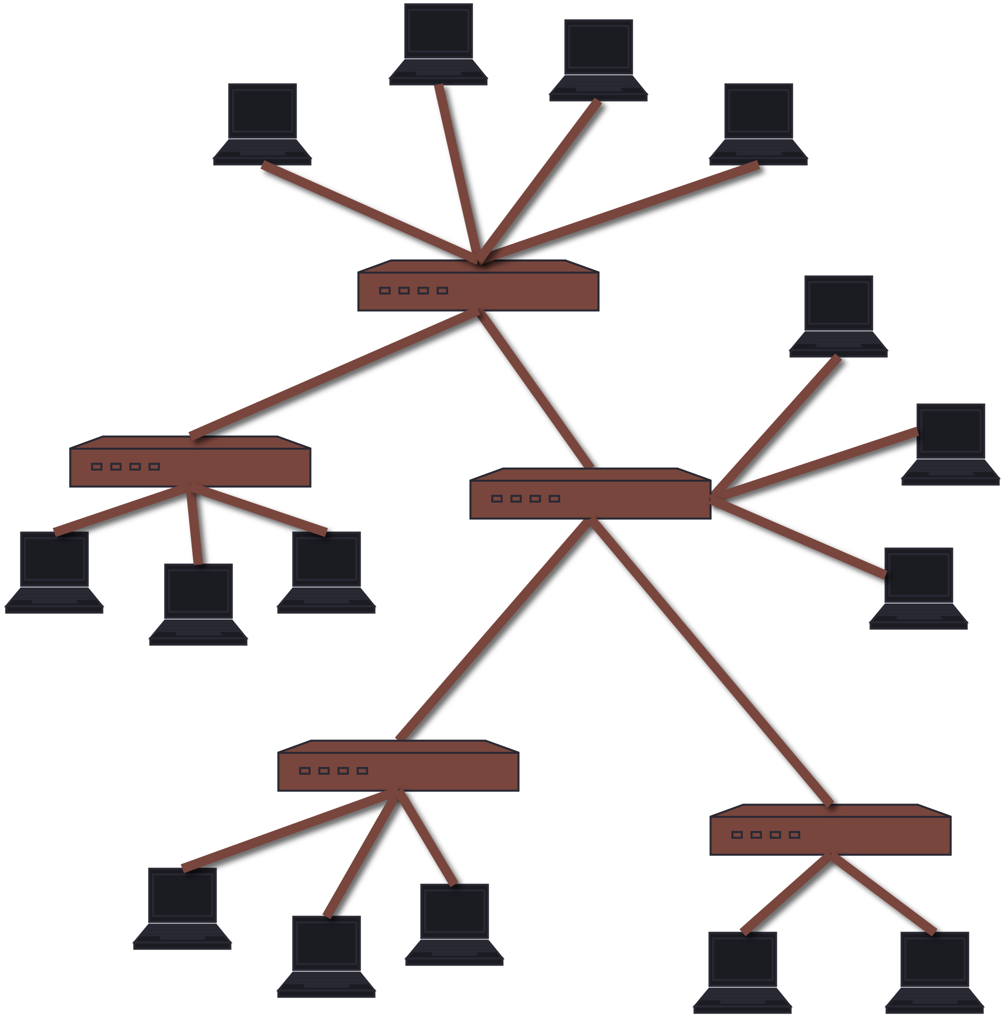


From *Security in Computing, Fifth Edition*, by Charles P. Pfleeger, et al. (ISBN: 9780134085043). Copyright 2015 by Pearson Education, Inc. All rights reserved.

Combining Switches

- Switches can be arranged into a tree
- Each port learns the MAC addresses of the machines in the subtree connected to it
- Fragments to unknown MAC addresses are broadcast
- Frames to MAC addresses in the same segment as the sender are ignored

Combining Switches



From *Security in Computing, Fifth Edition*, by Charles P. Pfleeger, et al. (ISBN: 9780134085043). Copyright 2015 by Pearson Education, Inc. All rights reserved.

MAC Address Filtering

- A switch can be configured to provide service only to machines with specific MAC addresses
- Allowed MAC addresses need to be registered with a network administrator

MAC Address Filtering

- A MAC spoofing attack impersonates another machine
  - Find out MAC address of target machine
  - Reconfigure MAC address of rogue machine
  - Turn off or unplug target machine
- Countermeasures
  - Block port of switch when machine is turned off or unplugged
  - Disable duplicate MAC addresses

Viewing and Changing MAC Addresses

- Viewing the MAC addresses of the interfaces of a machine
  - Linux: ifconfig
  - Windows: ipconfig /all
- Changing a MAC address in Linux
  - Stop the networking service: /etc/init.d/network stop
  - Change the MAC address: ifconfig eth0 hw ether <MAC-address>
  - Start the networking service: /etc/init.d/network start

Viewing and Changing MAC Addresses

- Changing a MAC address in Windows
  - Open the Network Connections applet
  - Access the properties for the network interface
  - Click “Configure …”
  - In the advanced tab, change the network address to the desired value
- Changing a MAC address requires administrator privileges

ARP

- The address resolution protocol (ARP) connects the network layer to the data layer by converting IP addresses to MAC addresses
- ARP works by broadcasting requests and caching responses for future use
- The protocol begins with a computer broadcasting a message of the form

  who has <IP address1> tell <IP address2>

From *Security in Computing, Fifth Edition*, by Charles P. Pfleeger, et al. (ISBN: 9780134085043).

ARP

- When the machine with <IP address1> or an ARP server receives this message, its broadcasts the response

  <IP address1> is <MAC address>

ARP

- The requestor’s IP address <IP address2> is contained in the link header
- The Linux and Windows command arp - a displays the ARP table

Internet Address	Physical Address	Type
128.148.31.1	00-00-0c-07-ac-00	dynamic
128.148.31.15	00-0c-76-b2-d7-1d	dynamic
128.148.31.71	00-0c-76-b2-d0-d2	dynamic
128.148.31.75	00-0c-76-b2-d7-1d	dynamic
128.148.31.102	00-22-0c-a3-e4-00	dynamic
128.148.31.137	00-1d-92-b6-f1-a9	dynamic

From *Security in Computing, Fifth Edition*, by Charles P. Pfleeger, et al. (ISBN: 9780134085043). Copyright 2015 by Pearson Education, Inc. All rights reserved.

ARP Spoofing

- The ARP table is updated whenever an ARP response is received
- Requests are not tracked
- ARP announcements are not authenticated
- Machines trust each other
- A rogue machine can spoof other machines

From *Security in Computing, Fifth Edition*, by Charles P. Pfleeger, et al. (ISBN: 9780134085043). Copyright 2015 by Pearson Education, Inc. All rights reserved.

ARP Poisoning (ARP Spoofing)

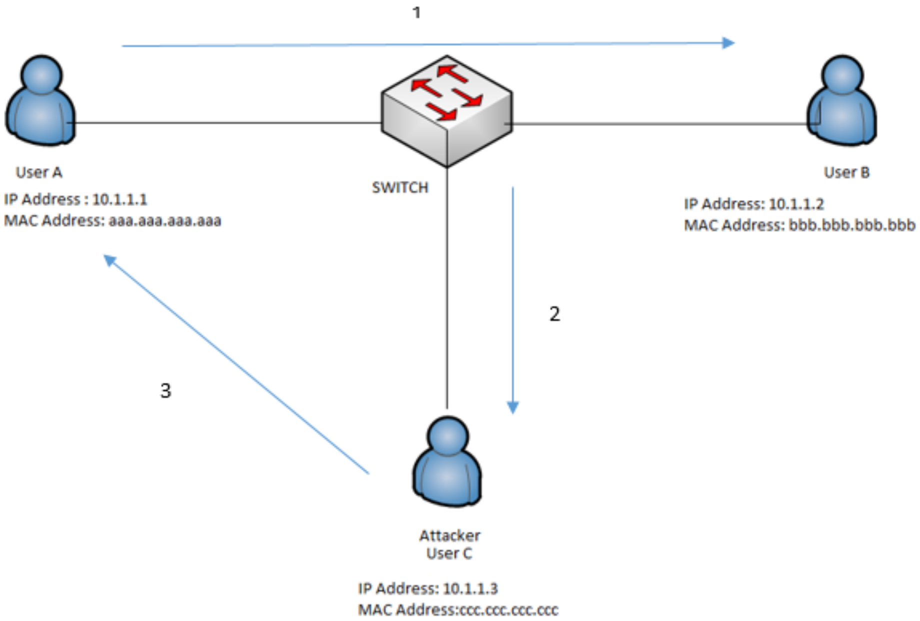
- According to the standard, almost all ARP implementations are stateless
- An arp cache updates every time that it receives an arp reply… even if it did not send any arp request!
- It is possible to "poison" an arp cache by sending gratuitous arp replies
- Using static entries solves the problem but it is almost impossible to manage!

From *Security in Computing, Fifth Edition*, by Charles P. Pfleeger, et al. (ISBN: 9780134085043). Copyright 2015 by Pearson Education, Inc. All rights reserved.

ARP Poisoning (ARP Spoofing)

- Attacker tries to map the MAC address with the IP address of a victim
- Once the MAC address is mapped, the attacker intercepts the data
- By using ARP spoofing attack, the attacker can steal or delete the data

From *Security in Computing, Fifth Edition*, by Charles P. Pfleeger, et al. (ISBN: 9780134085043).



https://www.safaribooksonline.com/library/view/ccna-security-210-260/9781787128873/5628067a-4601-4a57-a221-c08d777dc39c.x

ARP Poisoning Defenses

- Use ARP spoofing detection and prevention software
  - certifies or cross-checks ARP responses
  - AntiARP (Windows), ArpStar(Linux), etc.
- Using VPNs (Virtual Private Networks)
  - Uses an encrypted tunnel for data transmission
  - Data that goes through it is encrypted

ARP Spoofing

- ARP Implemented in IPv4, which still routes most Internet traffic today
- In Internet Protocol Version 6 (IPv6) networks, the functionality of ARP is provided by the Neighbor Discovery Protocol (NDP)

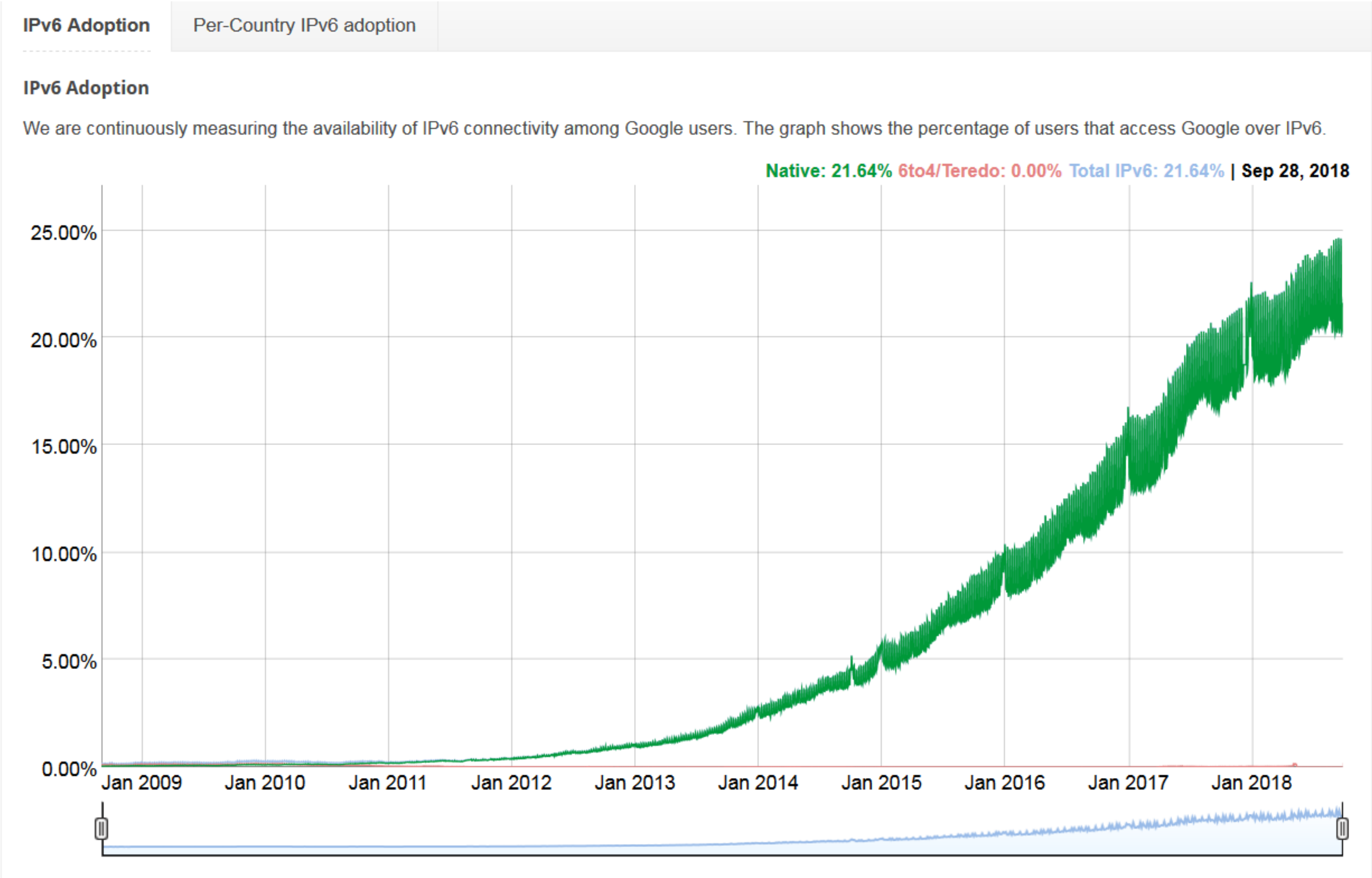
Neighbor Discovery Protocol (NDP) Advantages

- Less vulnerable to spoofing
- uses the Secure Neighbor Discovery (SEND) Protocol.
- Cryptographically generated addresses ensure that the claimed source of an NDP message is the owner of the claimed address

ARP Spoofing

- ARP Implemented in IPv4, which still routes most Internet traffic today
- In Internet Protocol Version 6 (IPv6) networks, the functionality of ARP is provided by the Neighbor Discovery Protocol (NDP)
  - However, IPv6 deployment is still ongoing

IPv6 adoption



IPv6 Adoption | Per-Country IPv6 adoption

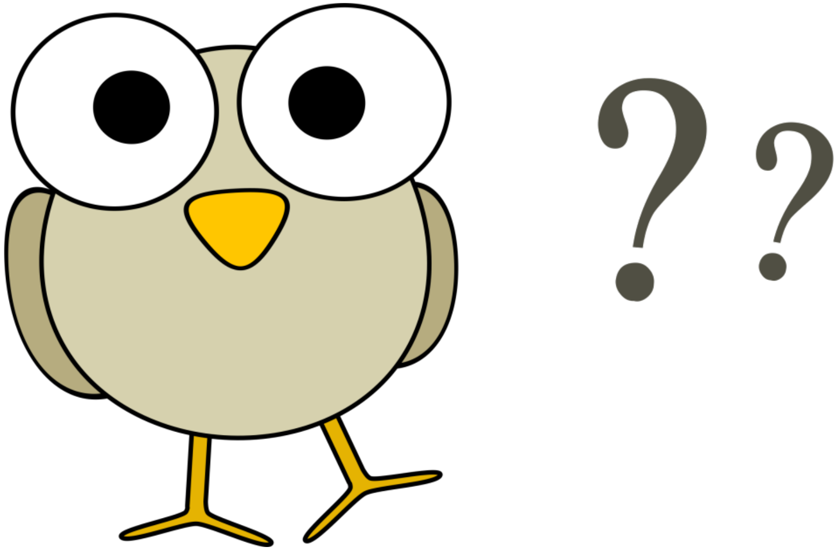
IPv6 Adoption

We are continuously measuring the availability of IPv6 connectivity among Google users. The graph shows the percentage of users that access Google over IPv6.

Native: 21.64% 6to4/Teredo: 0.00% Total IPv6: 21.64% | **Sep 28, 2018**

From *Security in Computing, Fifth Edition*, by Charles P. Pfleeger, et al. (ISBN: 9780134085043). Copyright 2015 by Pearson Education, Inc. All rights reserved.

- Questions?



Threats to Network Communications

- *Interception*, or unauthorized viewing
- *Modification*, or unauthorized change
- *Fabrication*, or unauthorized creation
- *Interruption*, or preventing authorized access

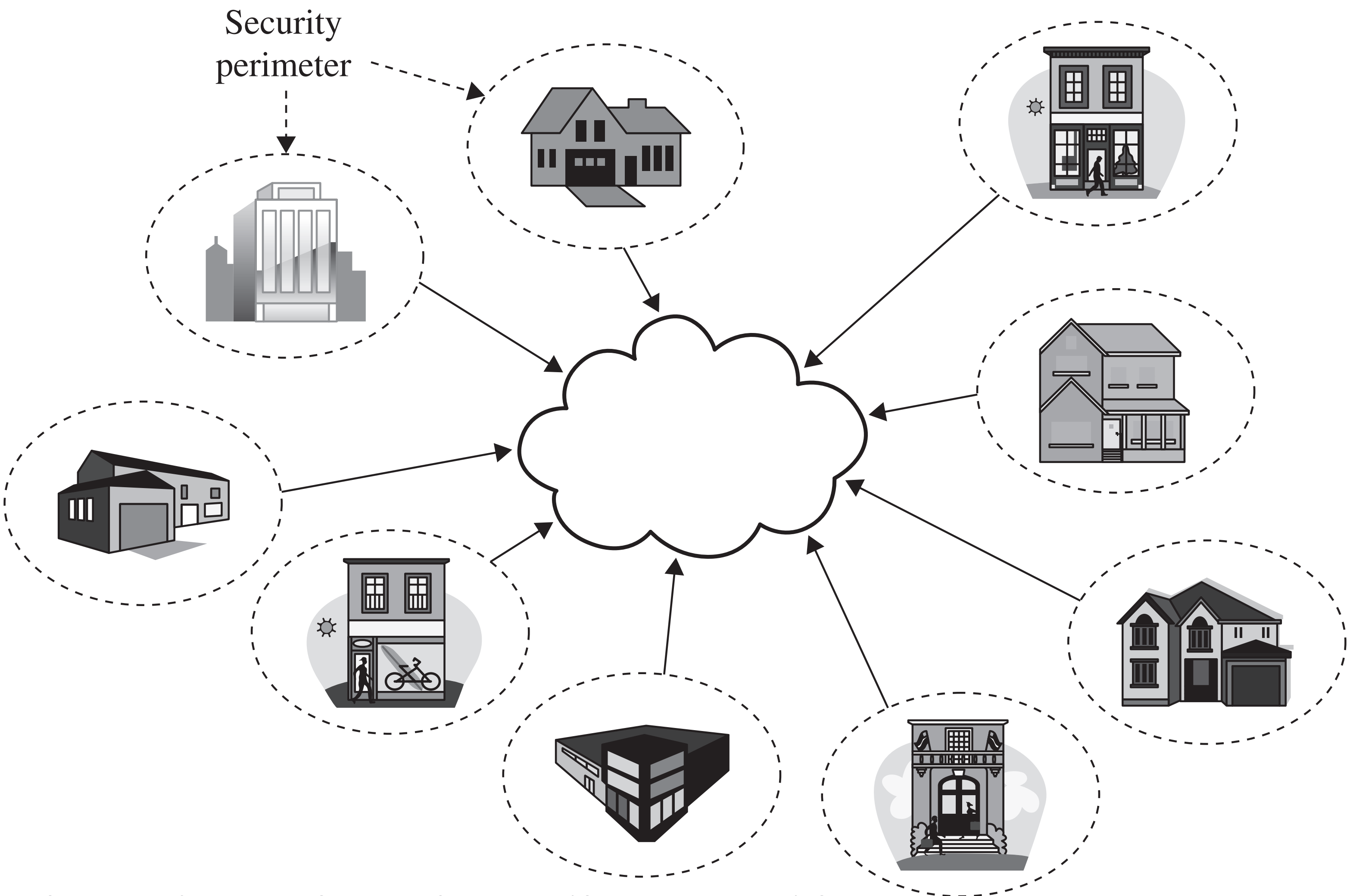
From *Security in Computing, Fifth Edition*, by Charles P. Pfleeger, et al. (ISBN: 9780134085043). Copyright 2015 by Pearson Education, Inc. All rights reserved.

Threats to Network Communications

- *Interception*, or unauthorized viewing
- *Modification*, or unauthorized change
- *Fabrication*, or unauthorized creation
- *Interruption*, or preventing authorized access

From *Security in Computing, Fifth Edition*, by Charles P. Pfleeger, et al. (ISBN: 9780134085043). Copyright 2015 by Pearson Education, Inc. All rights reserved.

Security Perimeters



From *Security in Computing, Fifth Edition*, by Charles P. Pfleeger, et al. (ISBN: 9780134085043). Copyright 2015 by Pearson Education, Inc. All rights reserved.

From *Security in Computing, Fifth Edition*, by Charles P. Pfleeger, et al. (ISBN: 9780134085043). Copyright 2015 by Pearson Education, Inc. All rights reserved.

Interception

- Each of these places is a security perimeter in and of itself
- Within each perimeter, you largely control your cables, devices, and computers
    - because of physical controls
        - => you don’t need to worry as much about protection

Interception

- But you have to make connections between security perimeters
  - => exposes you to all sort of cables, devices, and computers you can't control
  - Encryption is the most common and useful control for addressing this threat.

What Makes a Network Vulnerable to Interception?

- Anonymity
  - An attacker can attempt many attacks, anonymously, from thousands of miles away
- Many points of attack
  - Large networks mean many points of potential entry
- Sharing
  - Networked systems open up potential access to more users than do single computers

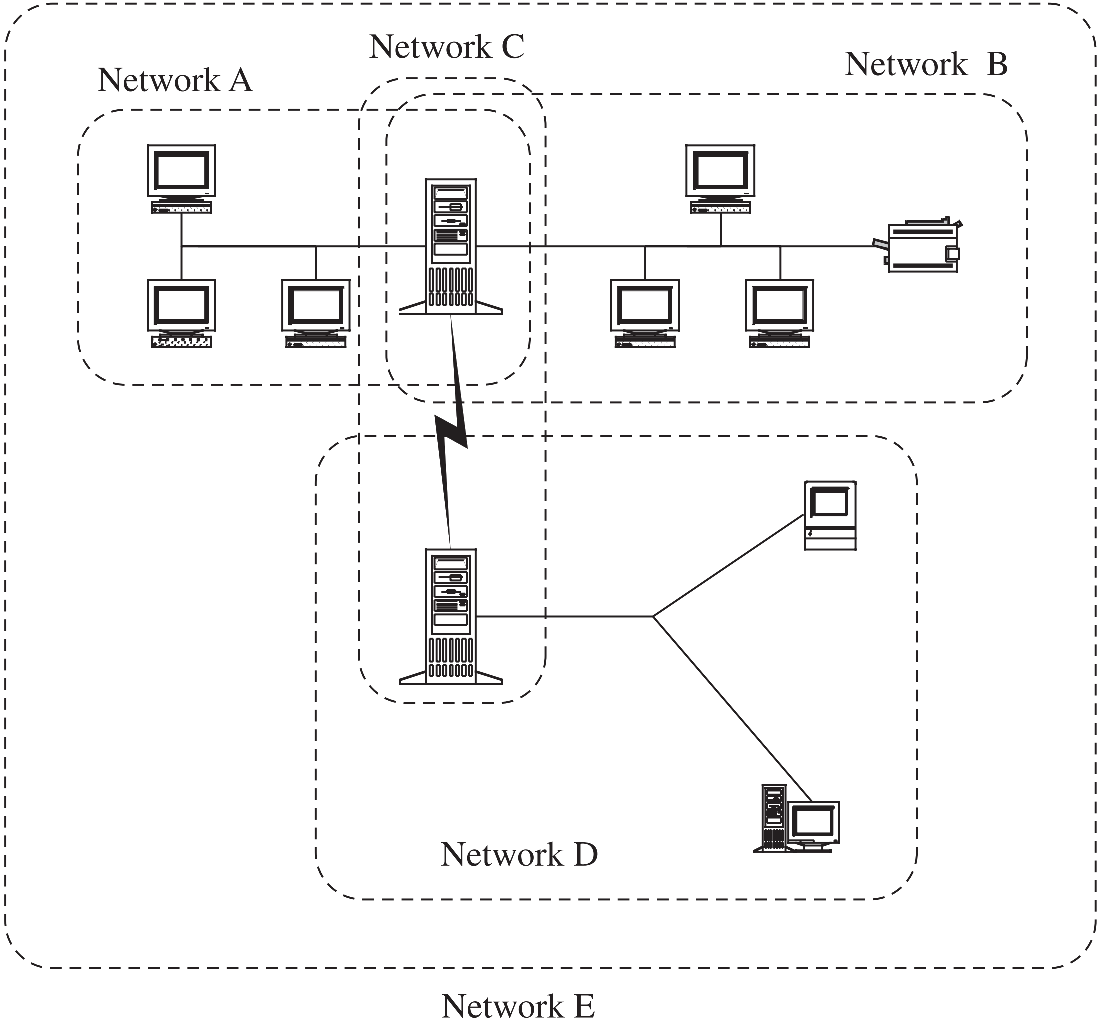
From *Security in Computing, Fifth Edition*, by Charles P. Pfleeger, et al. (ISBN: 9780134085043). Copyright 2015 by Pearson Education, Inc. All rights reserved.

What Makes a Network Vulnerable to Interception?

- System complexity
  - One system is very complex and hard to protect; networks of many different systems, with disparate OSs, vulnerabilities, and purposes are that much more complex
- Unknown perimeter
  - Networks, especially large ones, change all the time, so it can be hard to tell which systems belong and are behaving, and impossible to tell which systems bridge networks
- Unknown path
  - There may be many paths, including untrustworthy ones, from one host to another

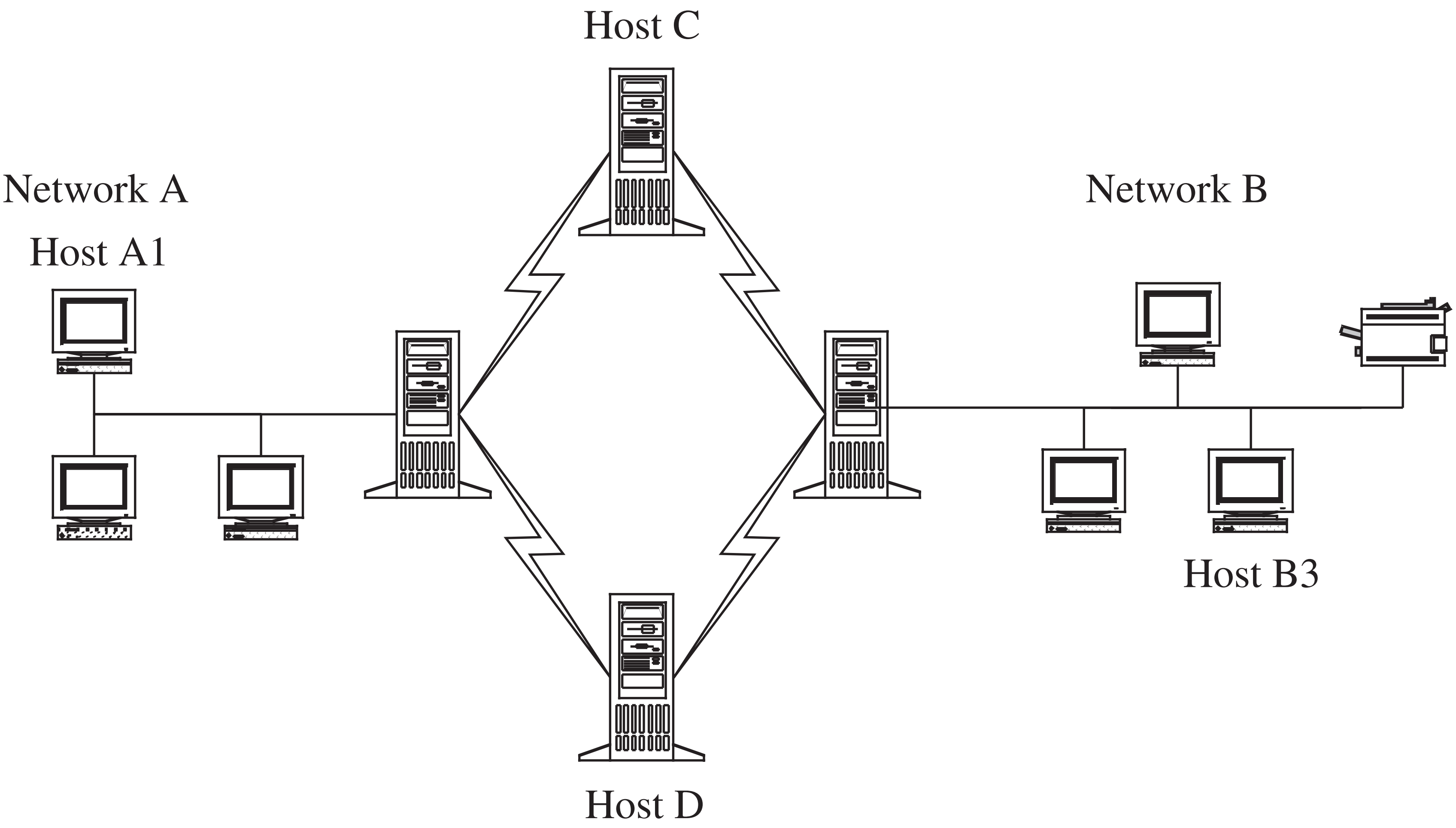
From *Security in Computing, Fifth Edition*, by Charles P. Pfleeger, et al. (ISBN: 9780134085043). Copyright 2015 by Pearson Education, Inc. All rights reserved.

Unknown Perimeter



From *Security in Computing, Fifth Edition*, by Charles P. Pfleeger, et al. (ISBN: 9780134085043). Copyright 2015 by Pearson Education, Inc. All rights reserved.

Unknown Path



From *Security in Computing, Fifth Edition*, by Charles P. Pfleeger, et al. (ISBN: 9780134085043). Copyright 2015 by Pearson Education, Inc. All rights reserved.

Threats to Network Communications

- *Interception*, or unauthorized viewing
- *Modification*, or unauthorized change
- *Fabrication*, or unauthorized creation
- *Interruption*, or preventing authorized access

From *Security in Computing, Fifth Edition*, by Charles P. Pfleeger, et al. (ISBN: 9780134085043). Copyright 2015 by Pearson Education, Inc. All rights reserved.

Modification and Fabrication

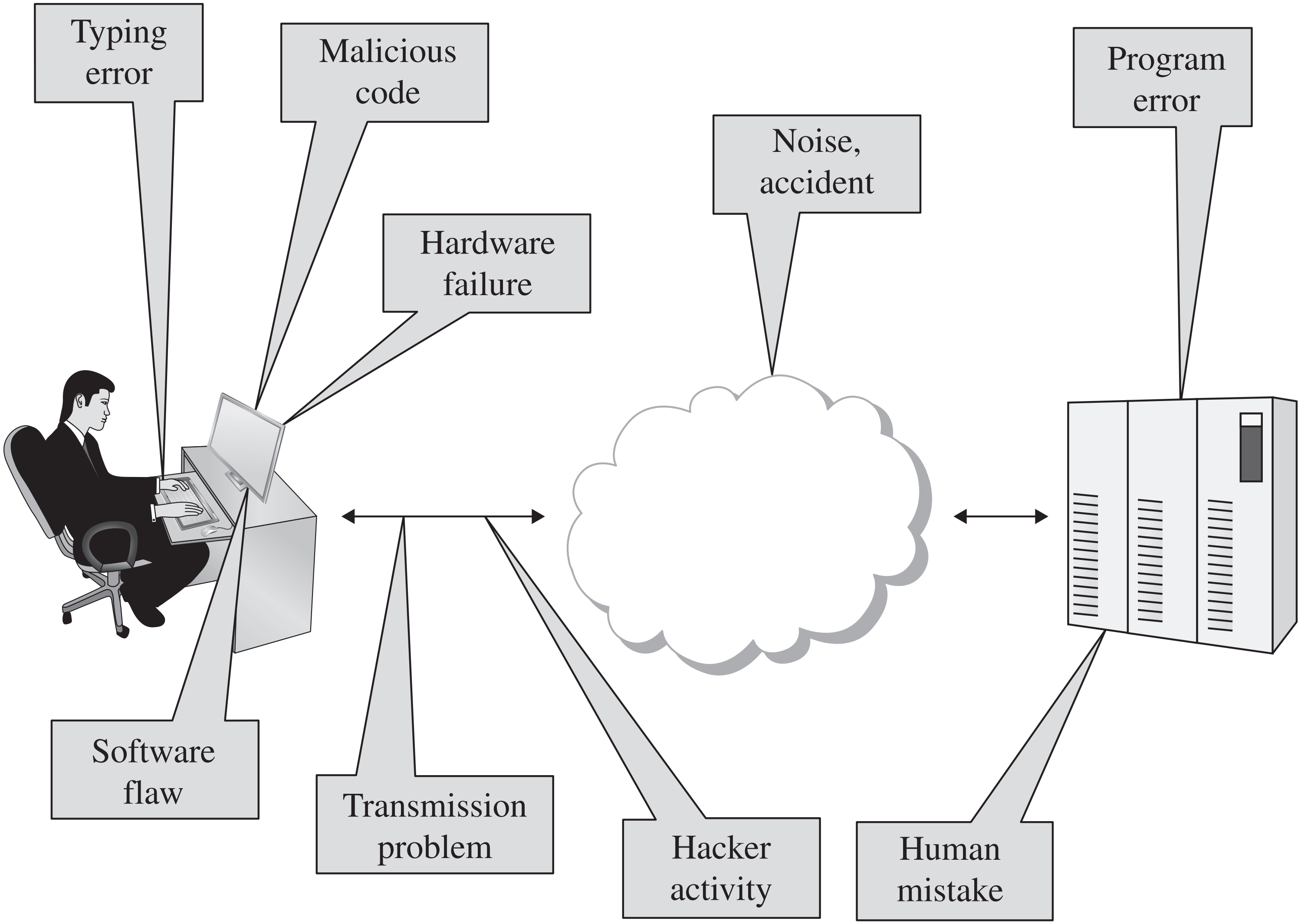
- Data corruption
  - May be intentional or unintentional, malicious or nonmalicious, directed or random
- Sequencing
  - Permuting the order of data, such as packets arriving in sequence
- Substitution
  - Replacement of one piece of a data stream with another

From *Security in Computing, Fifth Edition*, by Charles P. Pfleeger, et al. (ISBN: 9780134085043). Copyright 2015 by Pearson Education, Inc. All rights reserved.

Modification and Fabrication

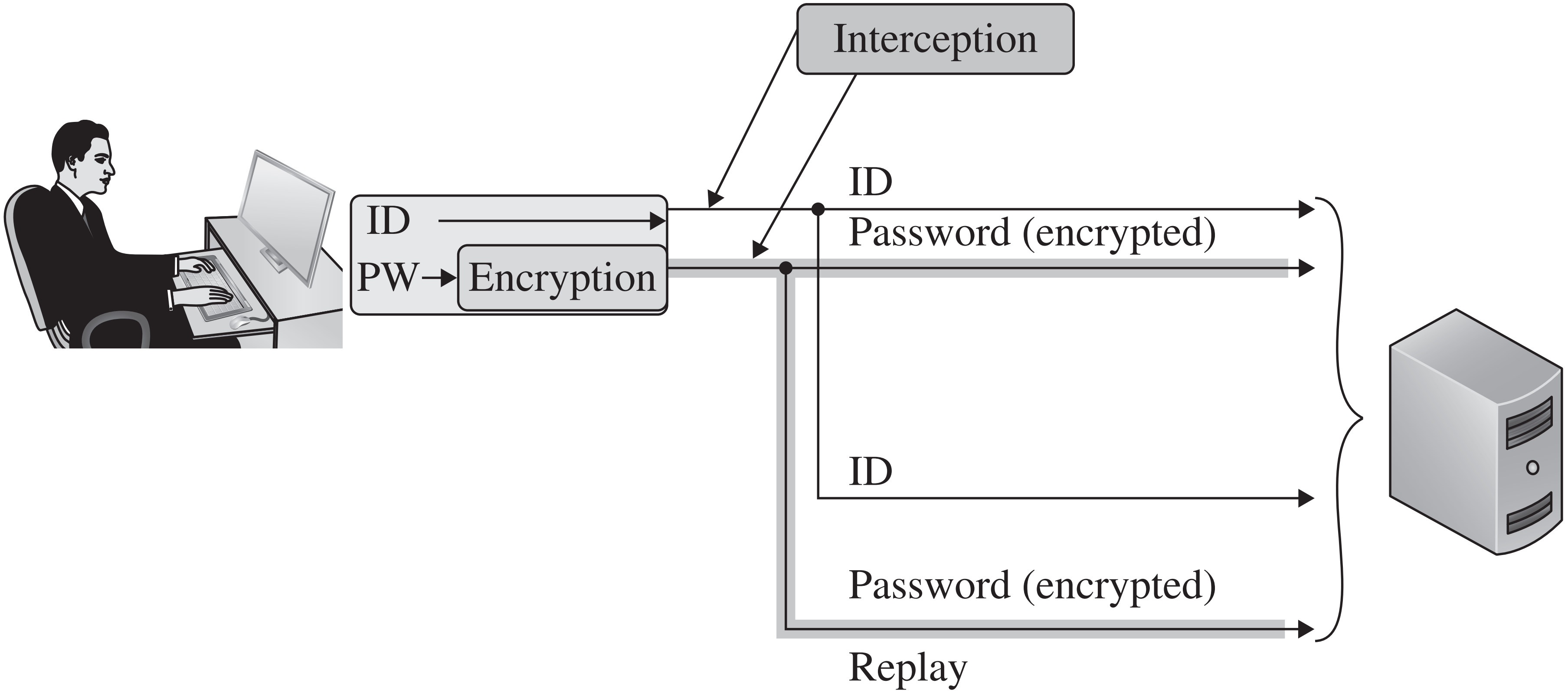
- Insertion
  - A form of substitution in which data values are inserted into a stream
- Replay
  - Legitimate data are intercepted and reused

Sources of Data Corruption



From *Security in Computing, Fifth Edition*, by Charles P. Pfleeger, et al. (ISBN: 9780134085043). Copyright 2015 by Pearson Education, Inc. All rights reserved.

Simple Replay Attack



From *Security in Computing, Fifth Edition*, by Charles P. Pfleeger, et al. (ISBN: 9780134085043). Copyright 2015 by Pearson Education, Inc. All rights reserved.

Threats to Network Communications

- *Interception*, or unauthorized viewing
- *Modification*, or unauthorized change
- *Fabrication*, or unauthorized creation
- *Interruption*, or preventing authorized access

Interruption: Loss of Service

- Routing
  - Internet routing protocols are complicated, and one misconfiguration can poison the data of many routers
- Excessive demand
  - Network capacity is finite and can be exhausted; an attacker can generate enough demand to overwhelm a critical part of a network
- Component failure
  - Component failures tend to be sporadic and unpredictable, and will cause loss of service if not planned for

Port Scanner

- an application designed to probe a server or host for open ports.
- May be used by:
  - Administrators, to verify security policies of their networks
  - Attackers, to identify network services running on a host and exploit vulnerabilities

From *Security in Computing, Fifth Edition*, by Charles P. Pfleeger, et al. (ISBN: 9780134085043).

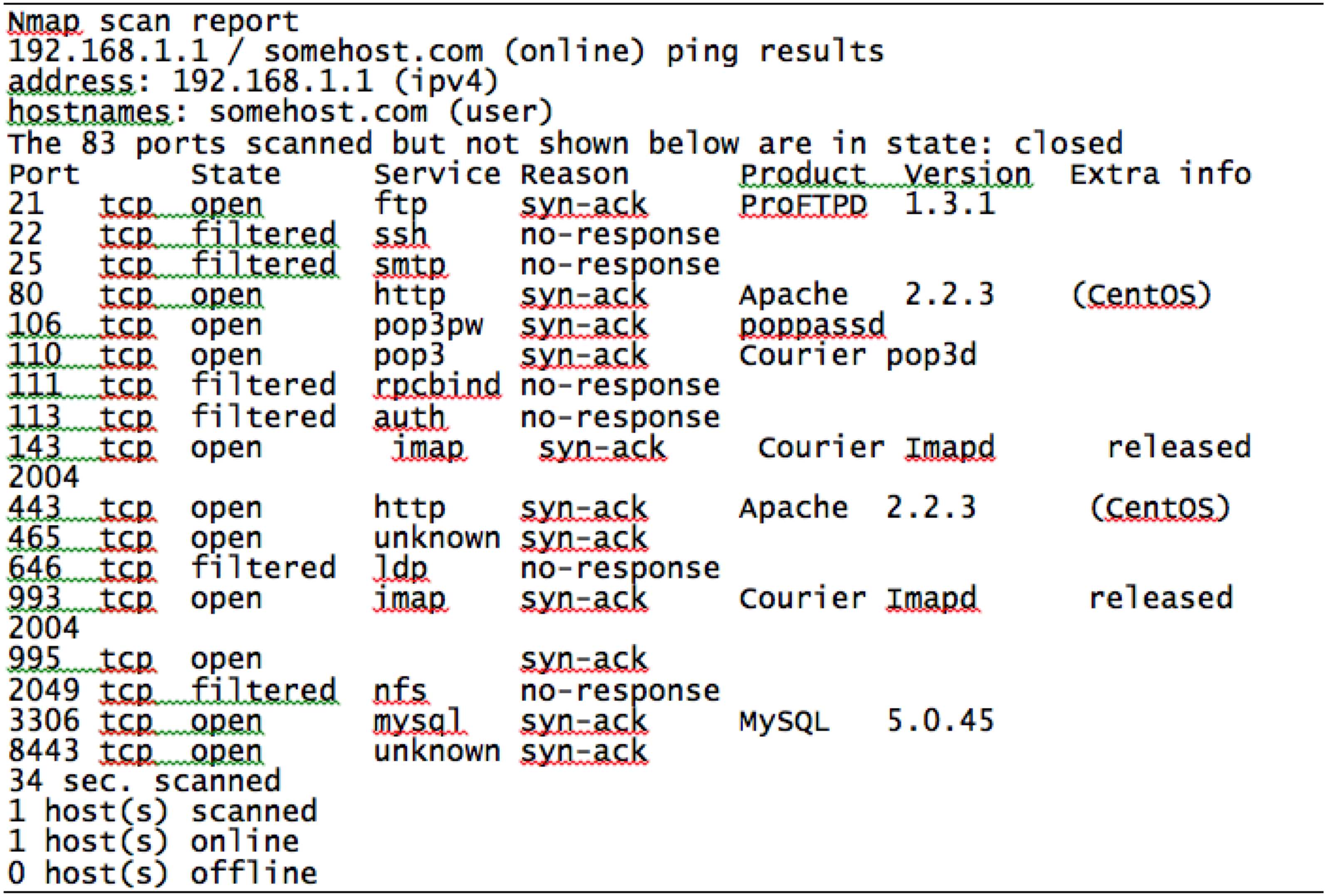
Port Scan

- A process that sends client requests to a range of server port addresses on a host
  - with the goal of finding an active port;
  - not a nefarious process in and of itself.
- Port scan can be used to determine services available on a remote machine
- The majority of uses of a port scan are not attacks

Port Scanning

- Post Scanning is a common first step to attacks
- Example: sample output from an NMAP port scan
    - Available Data: port, protocol, state, service, product, and version

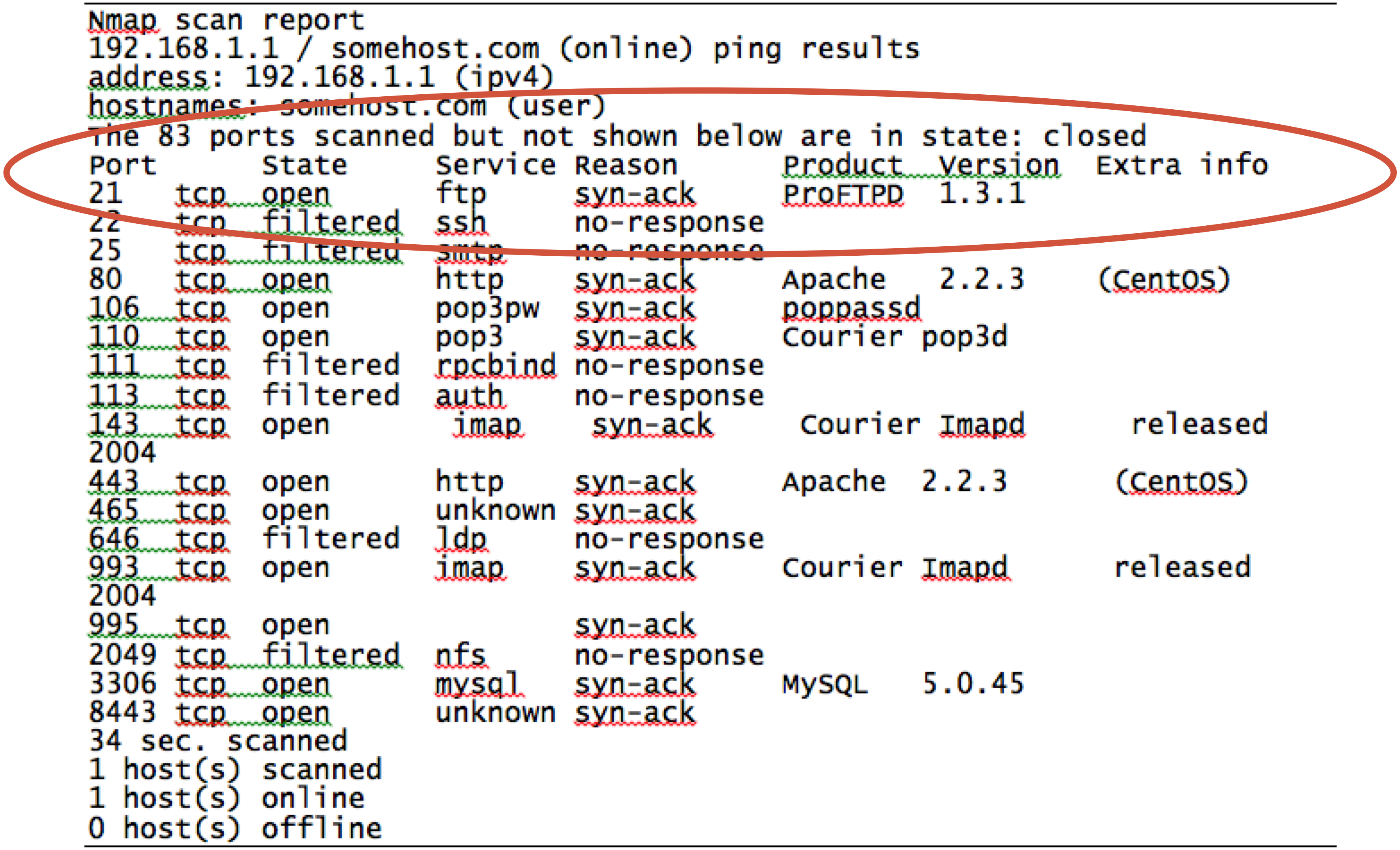
Port Scanning



```
Nmap scan report
192.168.1.1 / somehost.com (online) ping results
address: 192.168.1.1 (ipv4)
hostnames: somehost.com (user)
The 83 ports scanned but not shown below are in state: closed
Port      State     Service Reason      Product  Version  Extra info
21   tcp  open      ftp     syn-ack     ProFTPD  1.3.1
22   tcp  filtered  ssh     no-response
25   tcp  filtered  smtp    no-response
80   tcp  open      http    syn-ack     Apache   2.2.3    (CentOS)
106  tcp  open      pop3pw  syn-ack     poppassd
110  tcp  open      pop3    syn-ack     Courier pop3d
111  tcp  filtered  rpcbind no-response
113  tcp  filtered  auth    no-response
143  tcp  open       imap    syn-ack     Courier Imapd      released
2004
443  tcp  open      http    syn-ack     Apache  2.2.3      (CentOS)
465  tcp  open      unknown syn-ack
646  tcp  filtered  ldp     no-response
993  tcp  open      imap    syn-ack     Courier Imapd      released
2004
995  tcp  open              syn-ack
2049 tcp  filtered  nfs     no-response
3306 tcp  open      mysql   syn-ack     MySQL   5.0.45
8443 tcp  open      unknown syn-ack
34 sec. scanned
1 host(s) scanned
1 host(s) online
0 host(s) offline
```

From *Security in Computing, Fifth Edition*, by Charles P. Pfleeger, et al. (ISBN: 9780134085043). Copyright 2015 by Pearson Education, Inc. All rights reserved.

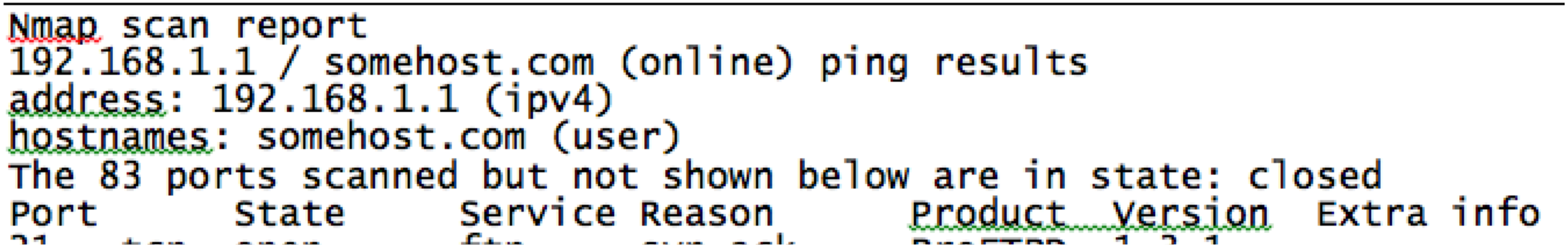
Port Scanning



```
Nmap scan report
192.168.1.1 / somehost.com (online) ping results
address: 192.168.1.1 (ipv4)
hostnames: somehost.com (user)
The 83 ports scanned but not shown below are in state: closed
Port         State      Service Reason        Product  Version  Extra info
21    tcp    open       ftp     syn-ack       ProFTPD  1.3.1
22    tcp    filtered   ssh     no-response
25    tcp    filtered   smtp    no-response
80    tcp    open       http    syn-ack       Apache   2.2.3    (CentOS)
106   tcp    open       pop3pw  syn-ack       poppassd
110   tcp    open       pop3    syn-ack       Courier pop3d
111   tcp    filtered   rpcbind no-response
113   tcp    filtered   auth    no-response
143   tcp    open        imap    syn-ack       Courier Imapd      released
2004
443   tcp    open       http    syn-ack       Apache  2.2.3      (CentOS)
465   tcp    open       unknown syn-ack
646   tcp    filtered   ldp     no-response
993   tcp    open       imap    syn-ack       Courier Imapd      released
2004
995   tcp    open               syn-ack
2049 tcp     filtered   nfs     no-response
3306 tcp     open       mysql   syn-ack       MySQL   5.0.45
8443 tcp     open       unknown syn-ack
34 sec. scanned
1 host(s) scanned
1 host(s) online
0 host(s) offline
```

From *Security in Computing, Fifth Edition*, by Charles P. Pfleeger, et al. (ISBN: 9780134085043). Copyright 2015 by Pearson Education, Inc. All rights reserved.

Port Scanning



```
Nmap scan report
192.168.1.1 / somehost.com (online) ping results
address: 192.168.1.1 (ipv4)
hostnames: somehost.com (user)
The 83 ports scanned but not shown below are in state: closed
Port        State      Service Reason      Product  Version   Extra info
```

From *Security in Computing, Fifth Edition*, by Charles P. Pfleeger, et al. (ISBN: 9780134085043). Copyright 2015 by Pearson Education, Inc. All rights reserved.

From *Security in Computing, Fifth Edition*, by Charles P. Pfleeger, et al. (ISBN: 9780134085043). Copyright 2015 by Pearson Education, Inc. All rights reserved.

NMAP Scanning

- NMap Scanning

- Nmap Firewall Scanning

Vulnerabilities in Wireless Networks

- Confidentiality
- Integrity
- Availability
- Unauthorized WiFi access

From *Security in Computing, Fifth Edition*, by Charles P. Pfleeger, et al. (ISBN: 9780134085043). Copyright 2015 by Pearson Education, Inc. All rights reserved.

Vulnerabilities in Wireless Networks

- Confidentiality
  - Because every message in WiFi is a broadcast, unencrypted messages can be read by anyone who’s listening and within range
- Integrity
  - When WiFi access points receive two streams of communication claiming to be the same computer, they necessarily accept the one with greater signal strength
    - This allows attackers to take over and forge sessions by spoofing legitimate computers and boosting signal strength

From *Security in Computing, Fifth Edition*, by Charles P. Pfleeger, et al. (ISBN: 9780134085043). Copyright 2015 by Pearson Education, Inc. All rights reserved.

Vulnerabilities in Wireless Networks

- Availability
  - In addition to the obvious availability issues, WiFi creates new availability problems
    - such as session hijacking, forced disassociation, and jamming.
- Unauthorized WiFi access:
  - Some form of cryptographic control is necessary to solve this

From *Security in Computing, Fifth Edition*, by Charles P. Pfleeger, et al. (ISBN: 9780134085043). Copyright 2015 by Pearson Education, Inc. All rights reserved.

Failed Countermeasure: WEP

- Wired equivalent privacy (WEP), designed as the mechanism for securing those communications
    - at the same time as the original 802.11 WiFi standards
- Weaknesses in WEP first identified in 2001, four years after release
- More weaknesses were discovered over the course of years
    - until any WEP-encrypted communication could be cracked in a matter of minutes

How WEP Works

- Client and access point (AP) have a pre-shared key
- AP sends a random number to the client
  - which the client then encrypts using the key and returns to the AP
- The AP decrypts the number using the key and checks that it’s the same number
  - to authenticate the client
- Once the client is authenticated, the AP and client communicate
  - using messages encrypted with the key

WEP Weaknesses

- Weak encryption key
  - WEP allows to be either 64- or 128-bit, but 24 of those bits are reserved for initialization vectors (IV)
    - => reducing effective key size to 40 or 140 bits
  - Keys were either alphanumeric or hex phrases that users typed in
    - => therefore vulnerable to dictionary attacks
- Static key
  - the key was a value user typed in at the client and AP
  - users rarely changed those keys
    - => one key would be used for many months of communications

From *Security in Computing, Fifth Edition*, by Charles P. Pfleeger, et al. (ISBN: 9780134085043). Copyright 2015 by Pearson Education, Inc. All rights reserved.

WEP Weaknesses

- Weak encryption process
  - A 40-bit key can be brute forced easily
  - Flaws that were eventually discovered in the RC4 encryption algorithm WEP uses made the 104-bit keys easy to crack as well
- Weak encryption algorithm
  - WEP used RC4 in a strange way (always a bad sign)
    - => resulted in a flaw that allowed attackers to decrypt large portions of any WEP communication

From *Security in Computing, Fifth Edition*, by Charles P. Pfleeger, et al. (ISBN: 9780134085043). Copyright 2015 by Pearson Education, Inc. All rights reserved.

WEP Weaknesses (cont.)

- IV collisions
  - There were only 16 million possible values of IV
    - in practice, this is not that many to cycle through for cracking.
  - IV’s were not as randomly selected as desired
    - some values were much more common than others
- Faulty integrity check
  - WEP messages included a checksum to identify transmission errors
    - but did not use one that could address malicious modification

WEP Weaknesses (cont.)

- No authentication
    - Any client that knows the AP’s SSID and MAC address is assumed to be legitimate

WPA (WiFi Protected Access)

- WPA was designed as a replacement for WEP (2003)
  - quickly followed by WPA2 (in 2004), the algorithm that remains the standard today
- Non-static encryption key
  - WPA uses a hierarchy of keys:
    - New keys are generated for confidentiality and integrity of each session
    - encryption key is automatically changed on each packet
  - The keys that are most important are used in very few places and indirect ways
    - protecting them from disclosure

WPA (WiFi Protected Access)

- Authentication
  - WPA allows authentication by password, token, or certificate
- Strong encryption
  - WPA adds support for AES, a much more reliably strong encryption algorithm
- Integrity protection
  - WPA includes a 64-bit cryptographic integrity check

WPA (cont.)

- Session initiation
    - WPA sessions begin with authentication and a four-way handshake
        - => results in separate keys for encryption and integrity on both ends
- There are some attacks against WPA
    - they are either of very limited effectiveness or require weak passwords

Denial of Service (DoS)

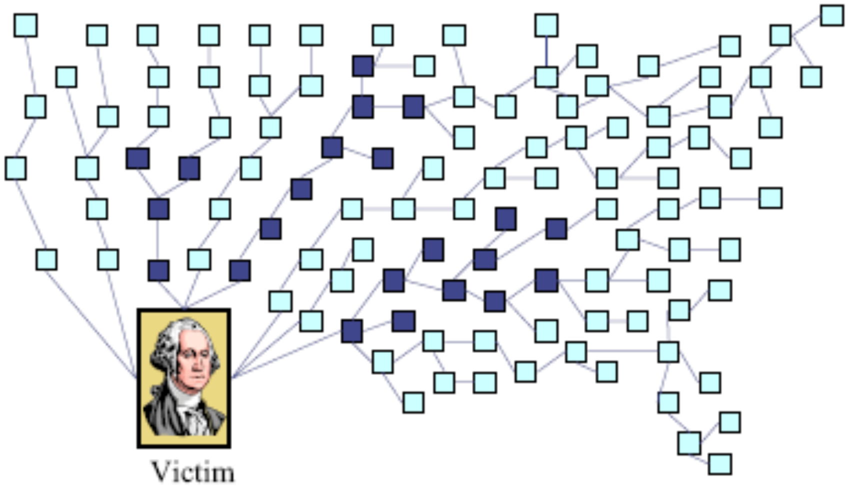
- DoS attacks are attempts to defeat a system’s availability
- Volumetric attacks
- Application-based attacks
- May result in disabled communications
- Hardware or software failure

From *Security in Computing, Fifth Edition*, by Charles P. Pfleeger, et al. (ISBN: 9780134085043). Copyright 2015 by Pearson Education, Inc. All rights reserved.

Denial of Service (DOS) Attack

- Send large number of packets to host providing service
  - Slows down or crashes host
  - Often executed by botnet
- Attack propagation
  - Starts at zombies
  - Travels through tree of internet routers rooted
  - Ends at victim
- IP source spoofing
  - Hides attacker
  - Scatters return traffic from victim

Source:
M.T. Goodrich, Probabalistic Packet Marking for Large-Scale IP Traceback, IEEE/ACM Transactions on Networking 16:1, 2008.



From *Security in Computing, Fifth Edition*, by Charles P. Pfleeger, et al. (ISBN: 9780134085043). Copyright 2015 by Pearson Education, Inc. All rights reserved.

DOS Attacks - Examples

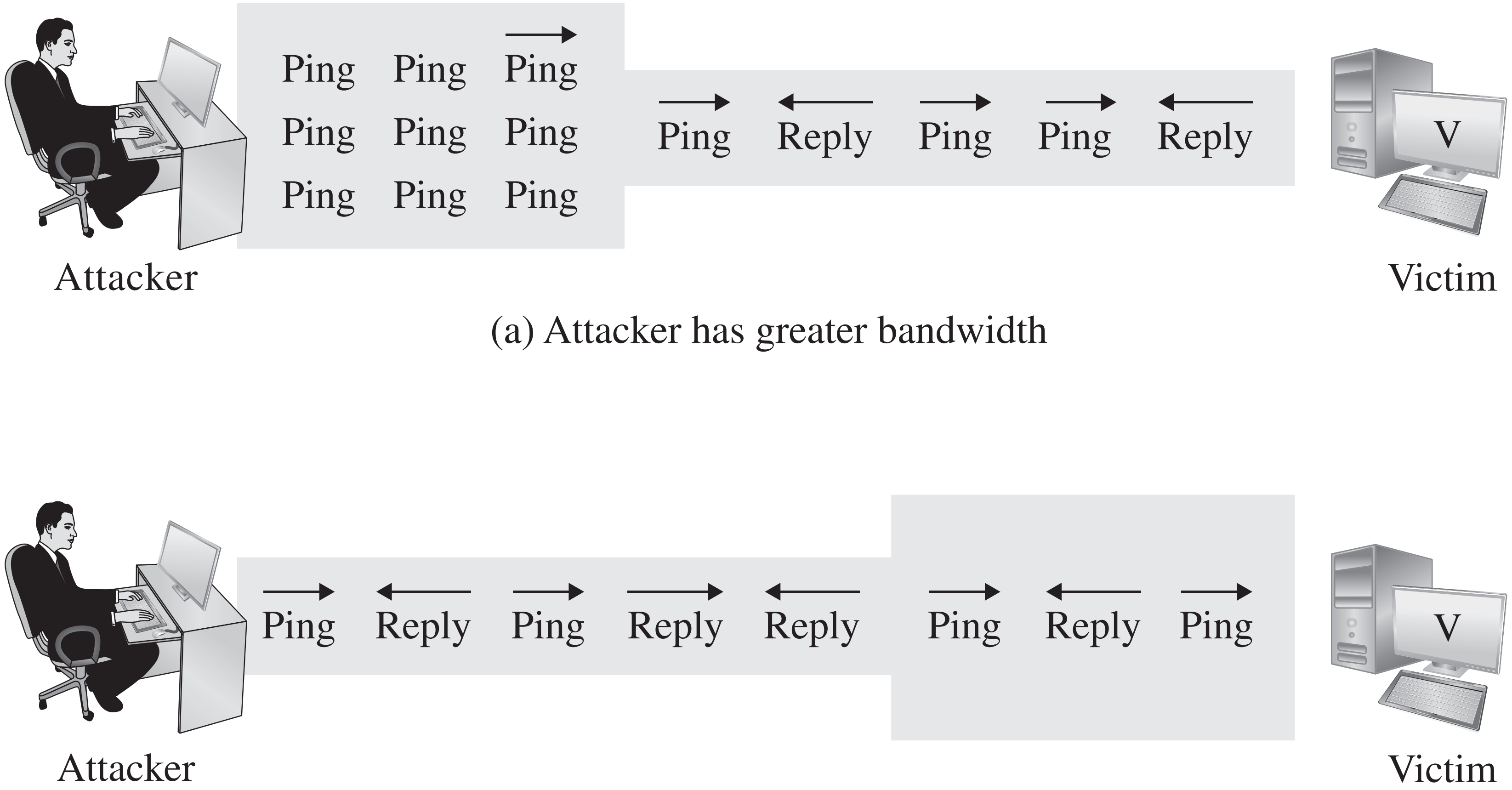
- SYN(PING) flood
- Smurf Attack
- Teardrop attack
- DNS Spoofing
- Session hijacking

From *Security in Computing, Fifth Edition*, by Charles P. Pfleeger, et al. (ISBN: 9780134085043). Copyright 2015 by Pearson Education, Inc. All rights reserved.

SYN (PING) Flood

- Typically DOS attack, though can be combined with other attack such as TCP hijacking
- Rely on sending TCP connection requests faster than the server can process them
- Attacker creates a large number of packets with spoofed source addresses and setting the SYN flag on these
- The server responds with a SYN/ACK for which it never gets a response (waits for about 3 minutes each)
- Eventually the server stops accepting connection requests, thus triggering a denial of service.

DoS Attack: Ping Flood



(a) Attacker has greater bandwidth

(b) Victim has greater bandwidth

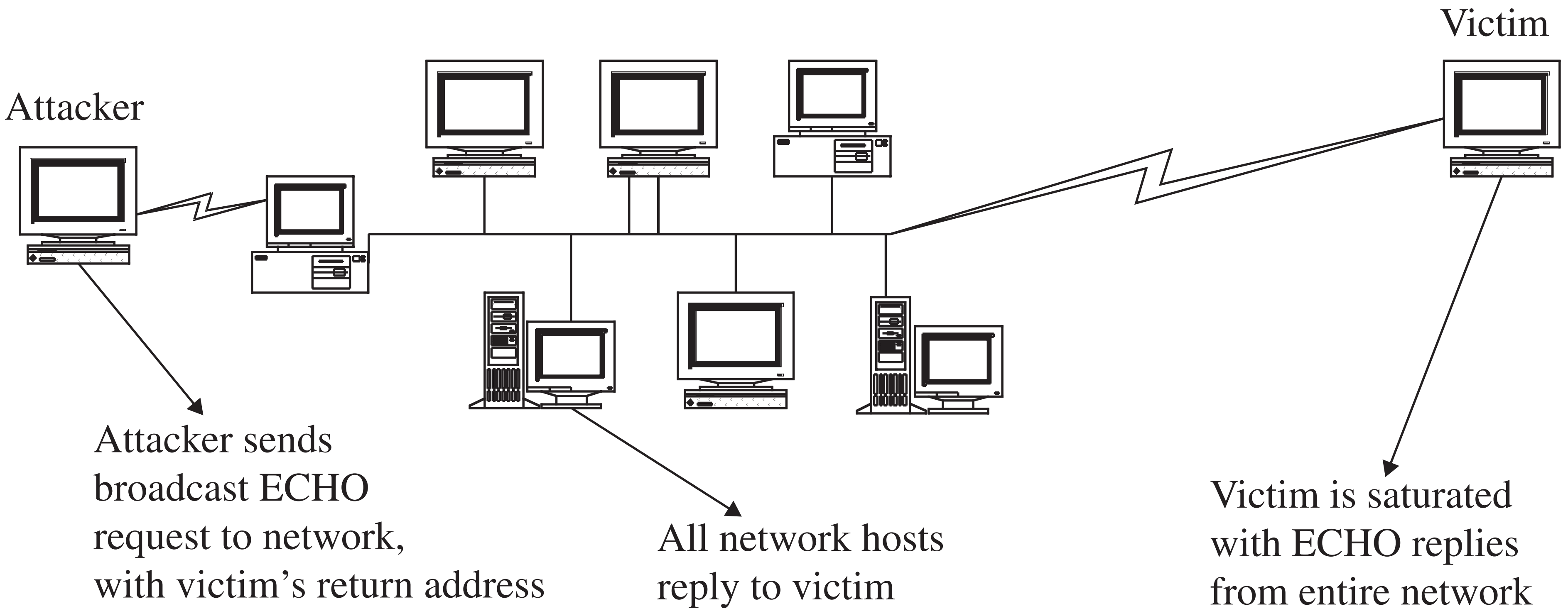
From *Security in Computing, Fifth Edition*, by Charles P. Pfleeger, et al. (ISBN: 9780134085043). Copyright 2015 by Pearson Education, Inc. All rights reserved.

From *Security in Computing, Fifth Edition*, by Charles P. Pfleeger, et al. (ISBN: 9780134085043). Copyright 2015 by Pearson Education, Inc. All rights reserved.

Smurf Attack

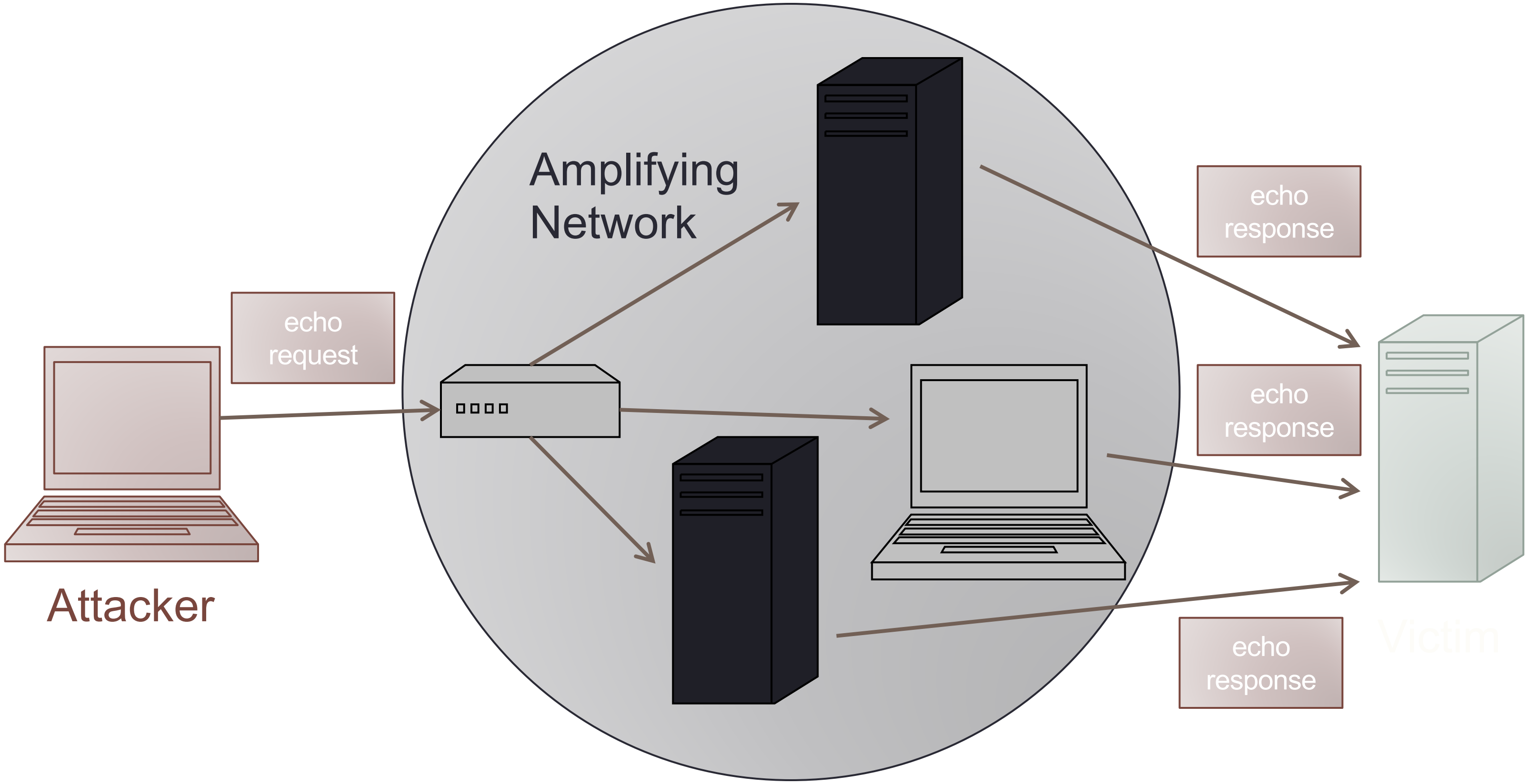
- Ping a broadcast address using a spoofed source address
- A distributed denial-of-service attack
    - Multiple systems flood the resources of a targeted system
- Most devices on a network will respond to this by sending a reply to the source IP address
- victim's computer will be flooded with traffic
    - If the number of machines on the network that respond to these packets is very large

DoS Attack: Smurf Attack


Victim
Attacker
Attacker sends broadcast ECHO request to network, with victim's return address
All network hosts reply to victim
Victim is saturated with ECHO replies from entire network

From *Security in Computing, Fifth Edition*, by Charles P. Pfleeger, et al. (ISBN: 9780134085043).

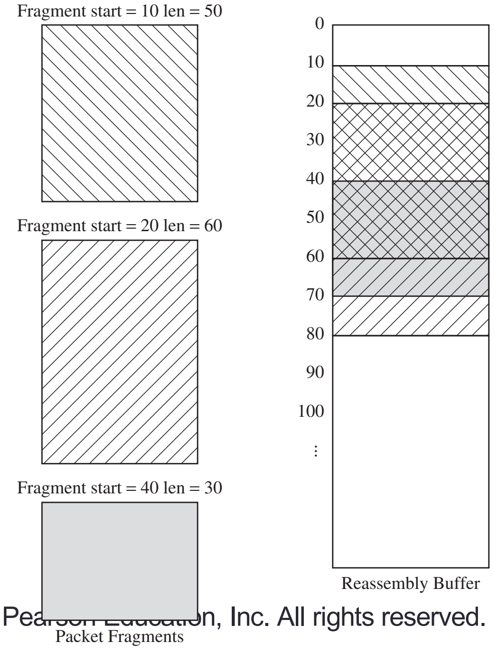
Smurf Attack



From *Security in Computing, Fifth Edition*, by Charles P. Pfleeger, et al. (ISBN: 9780134085043). Copyright 2015 by Pearson Education, Inc. All rights reserved.

DoS Attack: Teardrop Attack

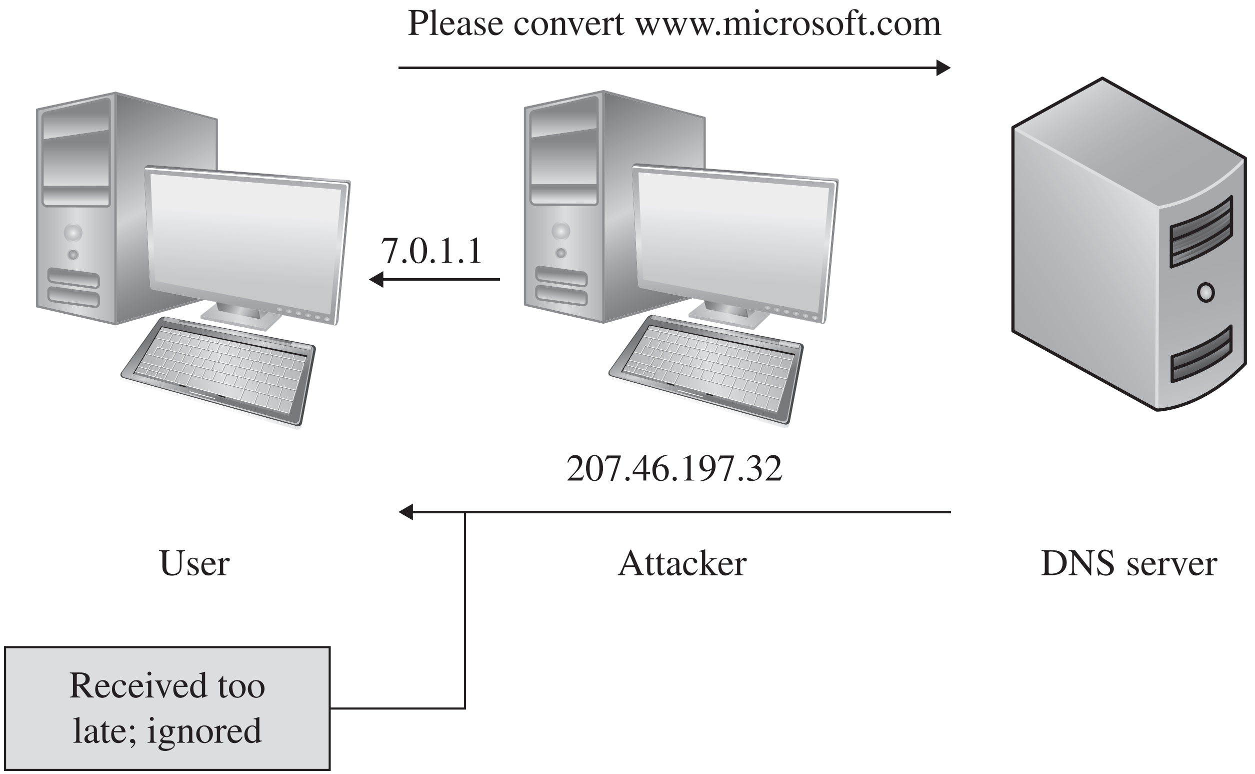
- The attacker sends packets that cannot possibly be reassembled (conflicting reassembly instructions)
- In extreme cases, this can cause the entire OS to lock up.


Fragment start = 10 len = 50
Fragment start = 20 len = 60
Fragment start = 40 len = 30
Packet Fragments
0
10
20
30
40
50
60
70
80
90
100
⋮
Reassembly Buffer

From *Security in Computing, Fifth Edition*, by Charles P. Pfleeger, et al. (ISBN: 9780134085043). Copyright 2015 by Pearson Education, Inc. All rights reserved.

DoS Attack: DNS Spoofing

- The attacker acts as the DNS server in order to redirect the user to malicious sites

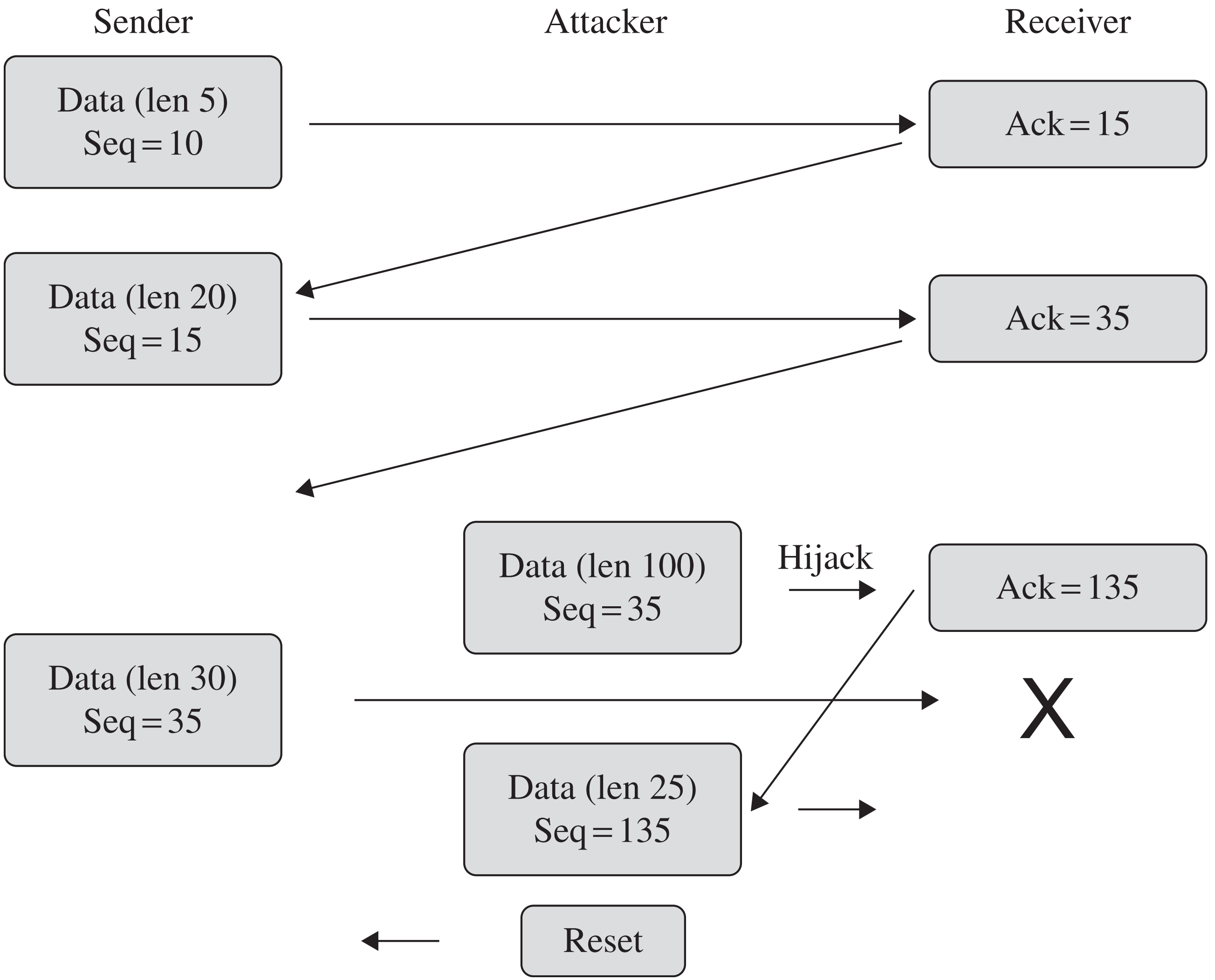


From *Security in Computing, Fifth Edition*, by Charles P. Pfleeger, et al. (ISBN: 9780134085043). Copyright 2015 by Pearson Education, Inc. All rights reserved.

DoS Attack: Session Hijacking

- An attacker is able to synchronize with a receiver while breaking synchronization with the sender and resetting sender’s connection.
- The attacker continues the TCP session while the sender thinks the connection just broke off

DoS Attack: Session Hijacking



From *Security in Computing, Fifth Edition*, by Charles P. Pfleeger, et al. (ISBN: 9780134085043). Copyright 2015 by Pearson Education, Inc. All rights reserved.

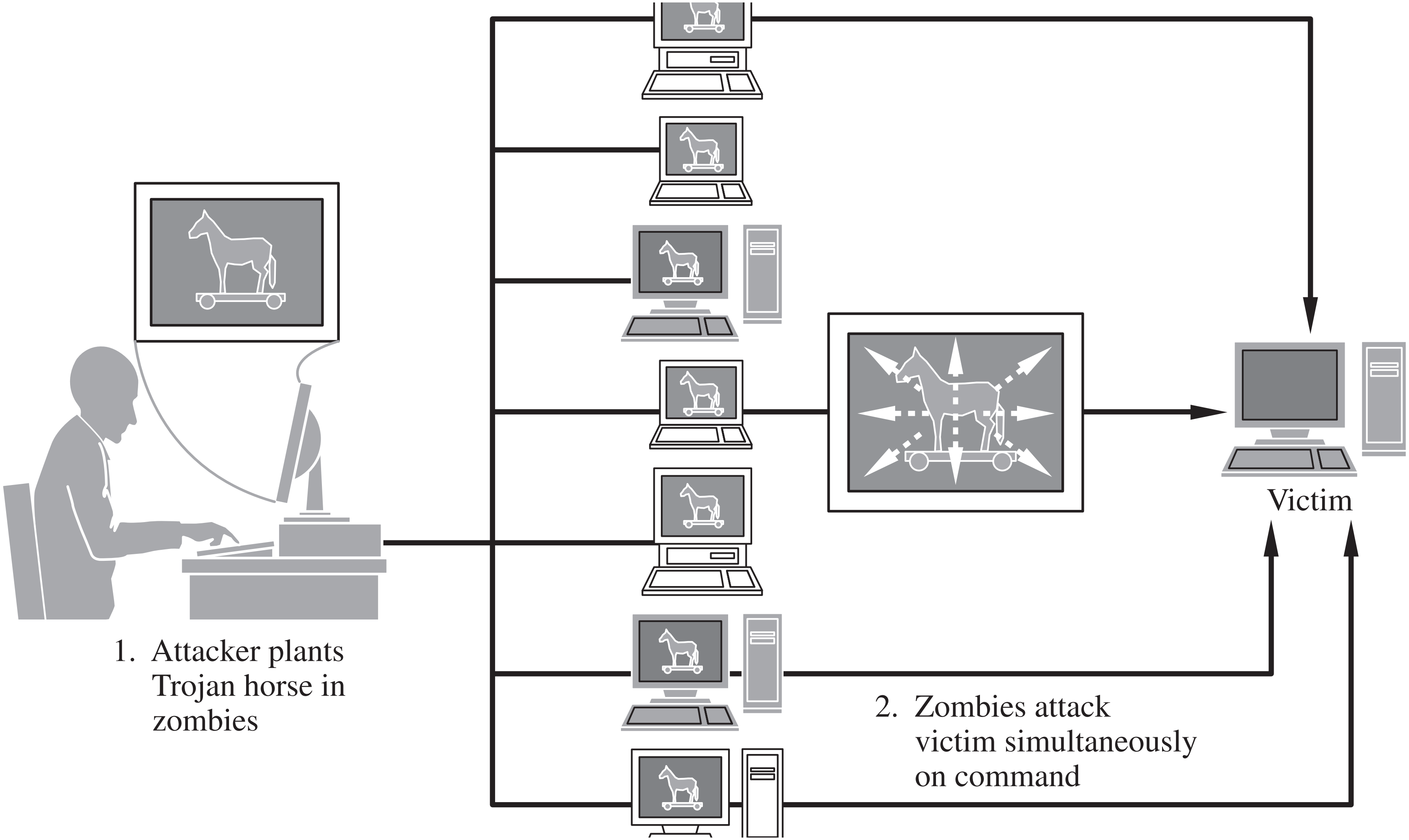
Distributed Denial of Service (DDoS)

- Conscript an army of compromised machines
  - to attack a victim
- Choose a victim
- Have the whole army unleash a DoS attack at once

- DDoS much more effective than traditional DoS attacks
  - employing a multiplied version of the same methods.

From *Security in Computing, Fifth Edition*, by Charles P. Pfleeger, et al. (ISBN: 9780134085043).

Distributed Denial of Service (DDoS)


Victim
1. Attacker plants Trojan horse in zombies
2. Zombies attack victim simultaneously on command

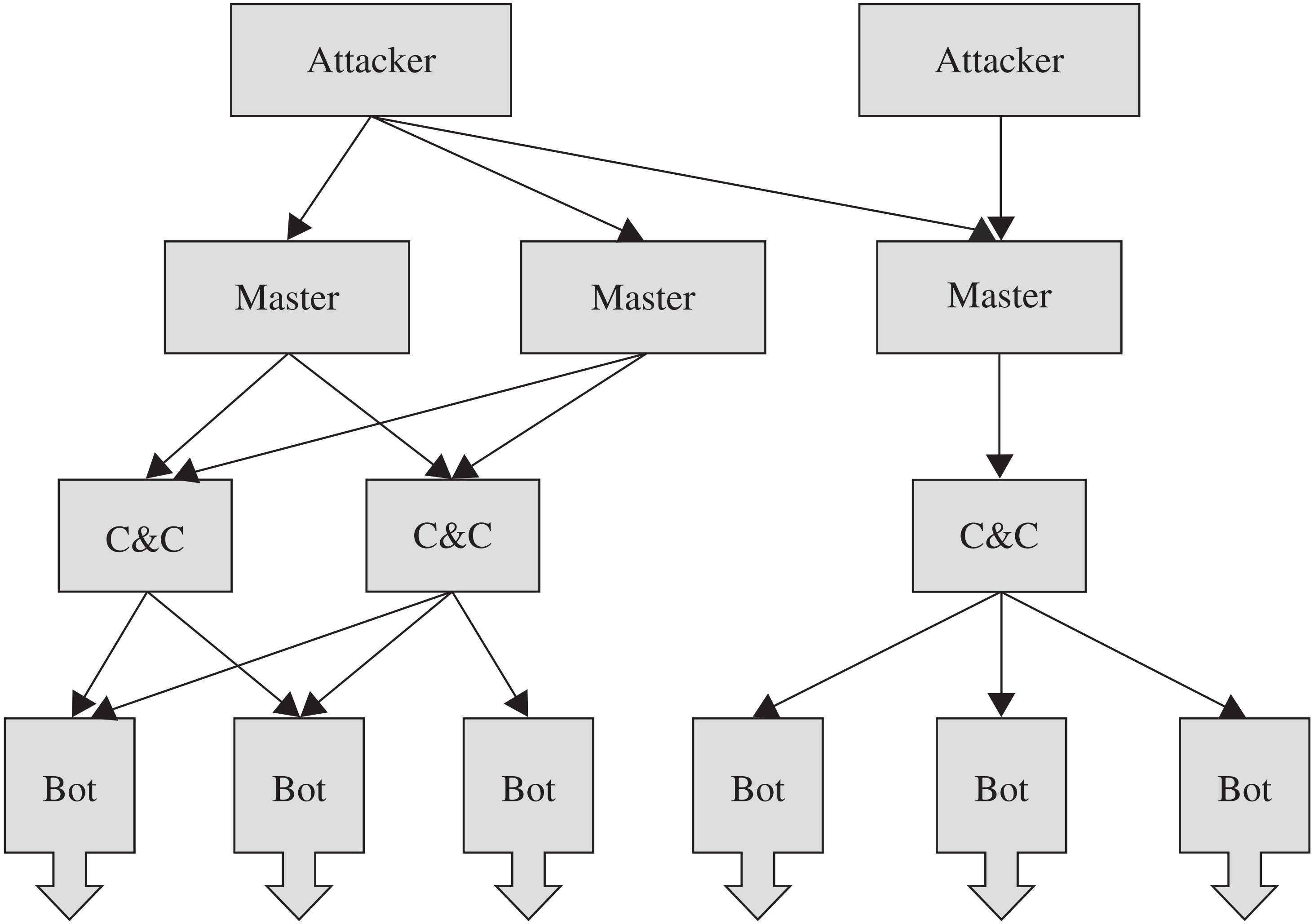
Botnets

- Botnets are networks of machines running malicious code under remote control.
- They often go undetected because they do little harm to the machines they run on.
- Botnets are often used to execute DDoS attacks.

Botnets

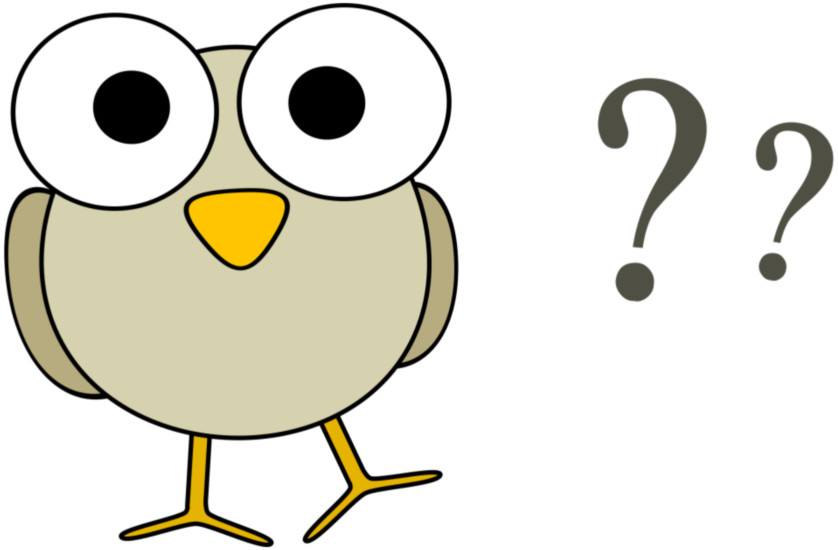
- Botnet command and control (C&C):
  - The attacker is separated from the bots by multiple layers
    - making the attacker difficult to trace.
  - Multiple redundant systems are built in
    - if one master or C&C node is taken down, the bots can continue to connect to the botnet.

Botnets



From *Security in Computing, Fifth Edition*, by Charles P. Pfleeger, et al. (ISBN: 9780134085043). Copyright 2015 by Pearson Education, Inc. All rights reserved.

- Questions?



From *Security in Computing, Fifth Edition*, by Charles P. Pfleeger, et al. (ISBN: 9780134085043).

COMPUTER SECURITY QUIZ

From *Security in Computing, Fifth Edition*, by Charles P. Pfleeger, et al. (ISBN: 9780134085043). Copyright 2015 by Pearson Education, Inc. All rights reserved.

Question 1

- Increased Traffic is due to a spike in network traffic from several sources. Assuming this is malicious, what is the MOST likely explanation?
  - A. A smurf attack
  - B. A flood guard attack
  - C. A denial-of-service (DoS) attack
  - D. distributed denial-of-service (DDoS) attack

Question 1

- Increased Traffic is due to a spike in network traffic from several sources. Assuming this is malicious, what is the MOST likely explanation?
  - A. A smurf attack
  - B. A flood guard attack
  - C. A denial-of-service (DoS) attack
  - [✓ D. distributed denial-of-service (DDoS) attack]

Question 1

- A distributed denial-of-service (DDoS) attack causes spikes in network traffic
  - as multiple systems attempt to connect to a server and deplete the target's resources
- A smurf attack is an attack using directed broadcasts
  - this might be a smurf attack if routers aren't blocking directed broadcasts, but it could also be another type of DDoS attack
- Flood guards protect against SYN flood attacks, and flood guards are not an attack method
- A DoS attack comes from a single system.

Question 2

- A SYN flood is an example of what type of attack?
  - A. Malicious code
  - B. Denial-of-service
  - C. Man-in-the-middle
  - D. Spoofing

Question 2

- A SYN flood is an example of what type of attack?
    - A. Malicious code
    - [✓ B. Denial-of-service]
    - C. Man-in-the-middle
    - D. Spoofing

- An attacker simply listens for all traffic being transmitted across a network, in the hope of viewing something such as a user ID and password combination. This is known as:
  - A. Malicious code
  - B. Denial-of-service
  - C. Man-in-the-middle
  - D. Sniffing

- An attacker simply listens for all traffic being transmitted across a network, in the hope of viewing something such as a user ID and password combination. This is known as:
  - A. Malicious code
  - B. Denial-of-service
  - C. Man-in-the-middle
  - [✓ D. Sniffing]

- Questions?