CISC 3325 – INFORMATION SECURITY

Chapter 6: Network Security

Rise of the Hackers

- Rise of the Hackers

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 BASICS

Network Transmission Media

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

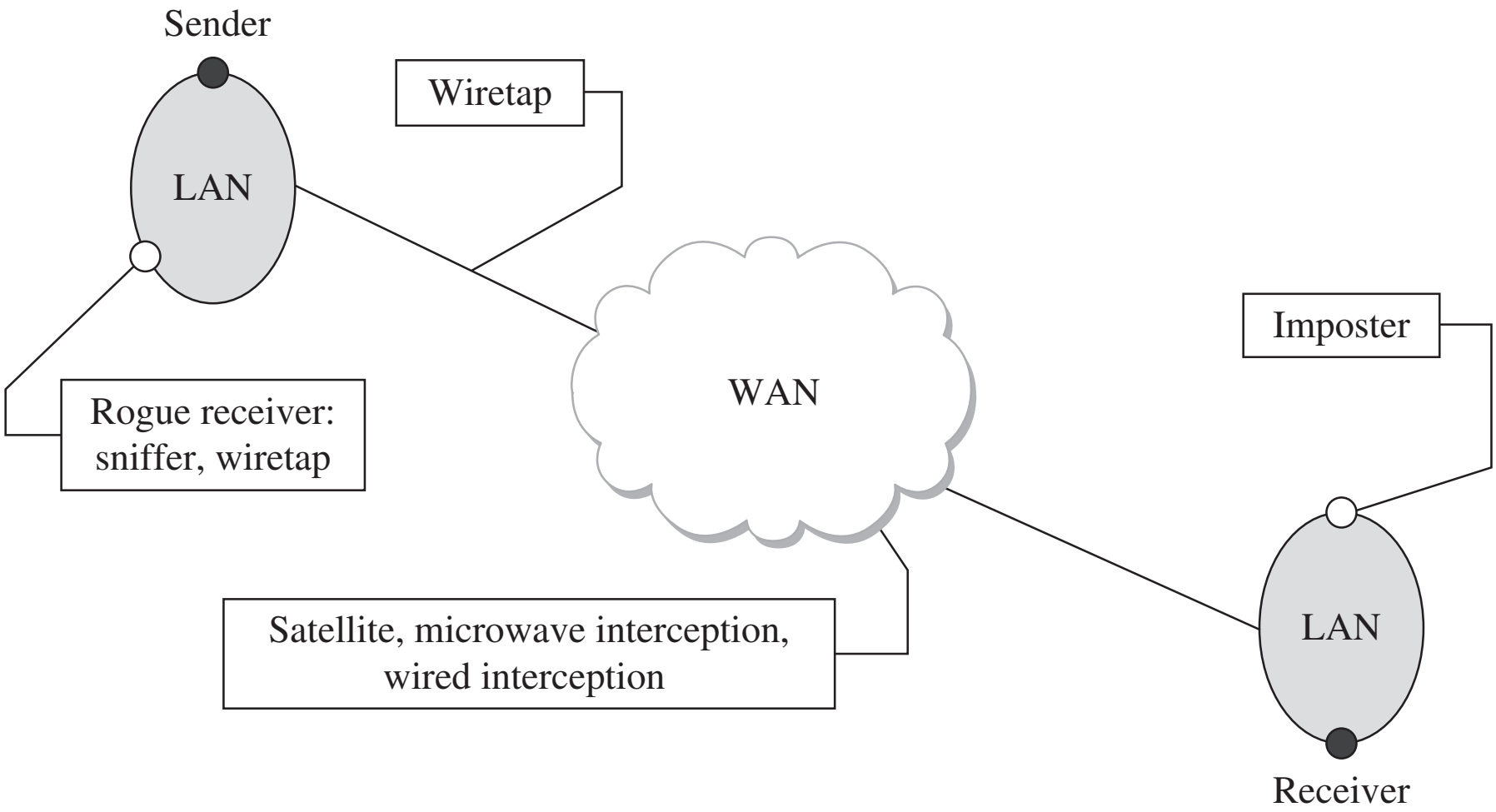
Communication Media Vulnerability

- 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



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

Communication Media Pros/Cons

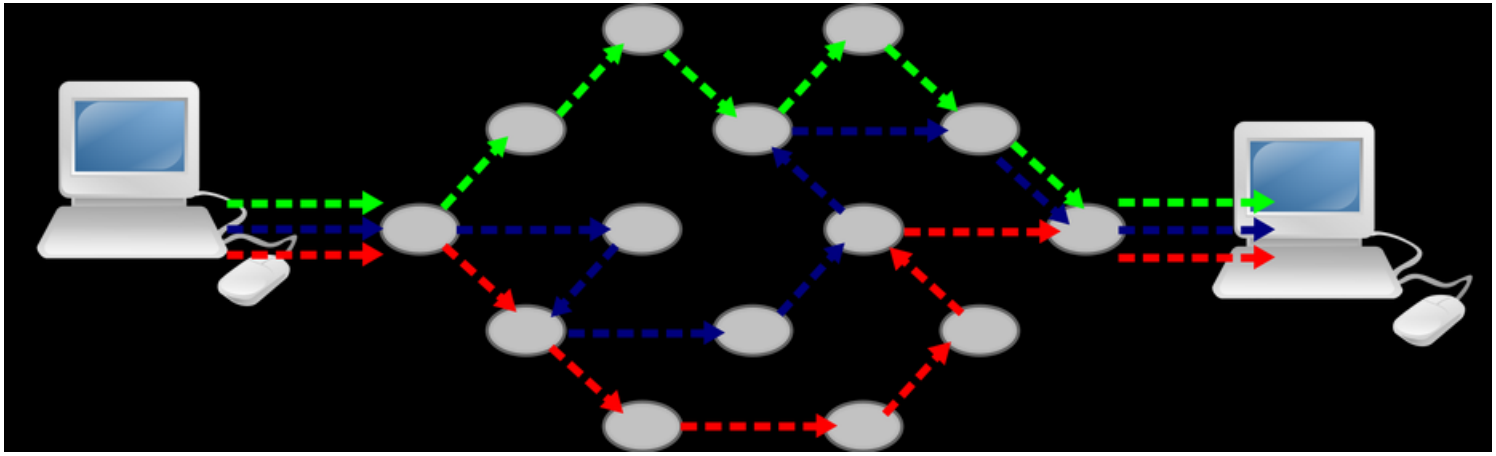
Medium	Strengths	Weaknesses
Wire	• Widely used • Inexpensive to buy, install, maintain	• Susceptible to emanation • Susceptible to physical wiretapping

* Emanation = “the action or process of issuing from a source.”
  - i.e., "the risk of radon gas emanation"

Computer Networks

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

Circuit and Packet Switching

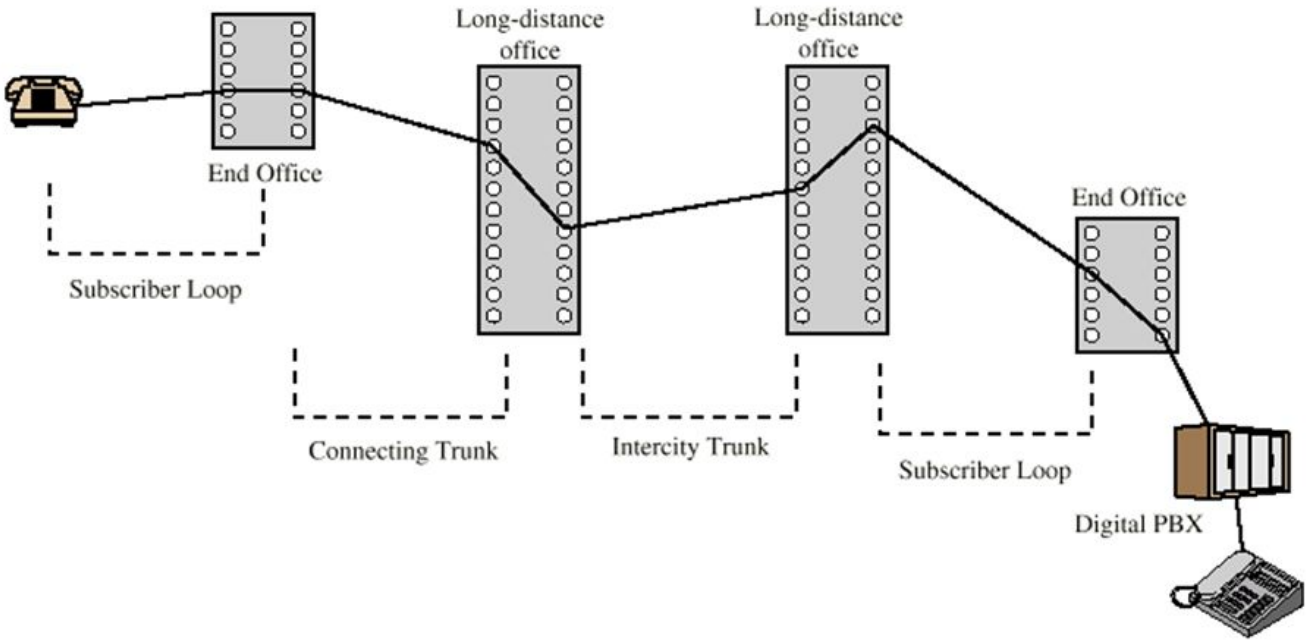


http://www.apposite-tech.com/blog/uncategorized/packet-switching-vs-circuit-switching/

Circuit and Packet Switching

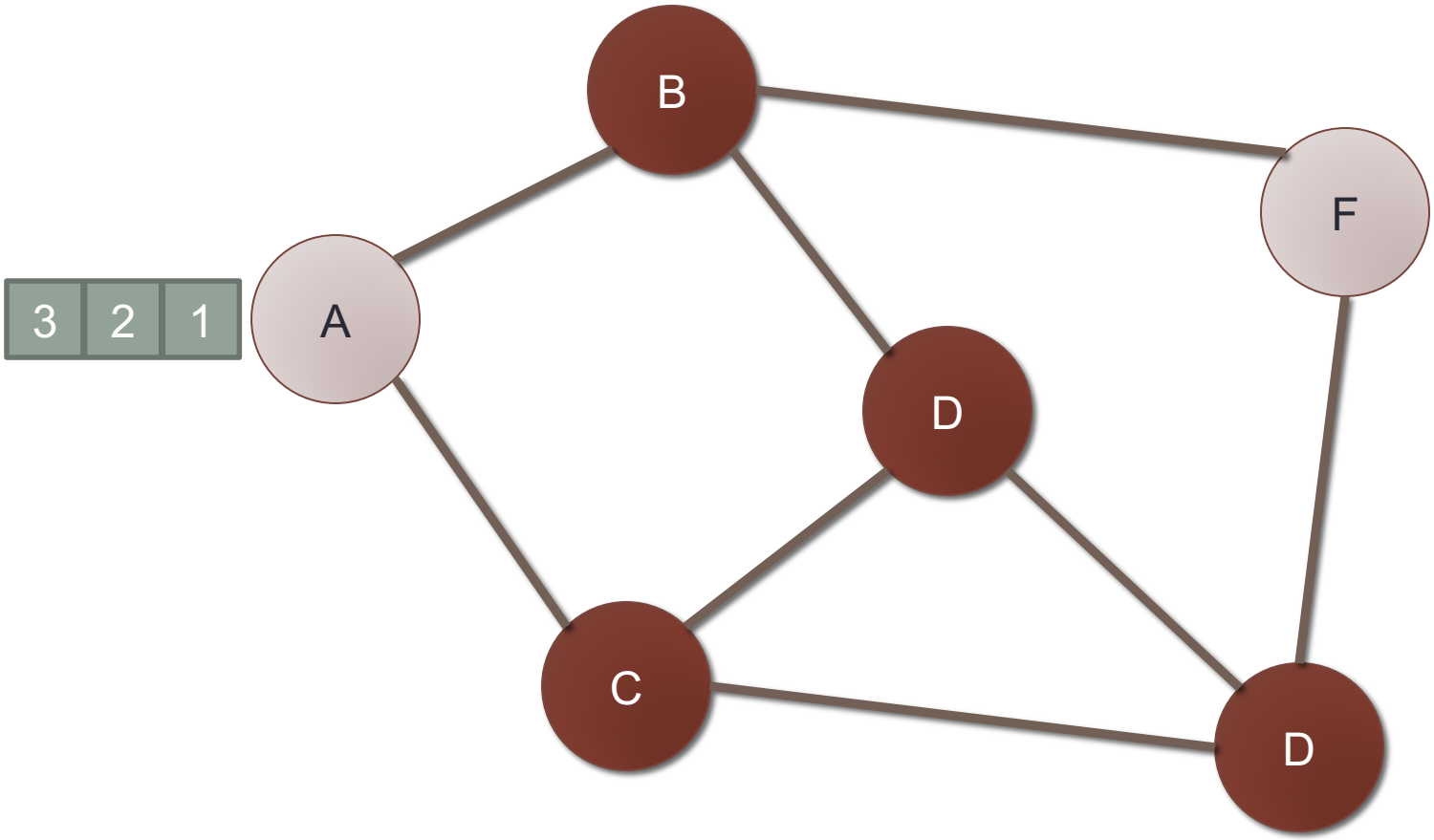
- Circuit switching
  - Legacy phone network
  - Single route through sequence of hardware devices established when two nodes start communication
  - Data sent along route
  - Route maintained until communication ends
- Packet switching
  - Internet
  - Data split into packets
  - Packets transported independently through network
  - Each packet handled on a best efforts basis
  - Packets may follow different routes

Public Circuit Switched Network

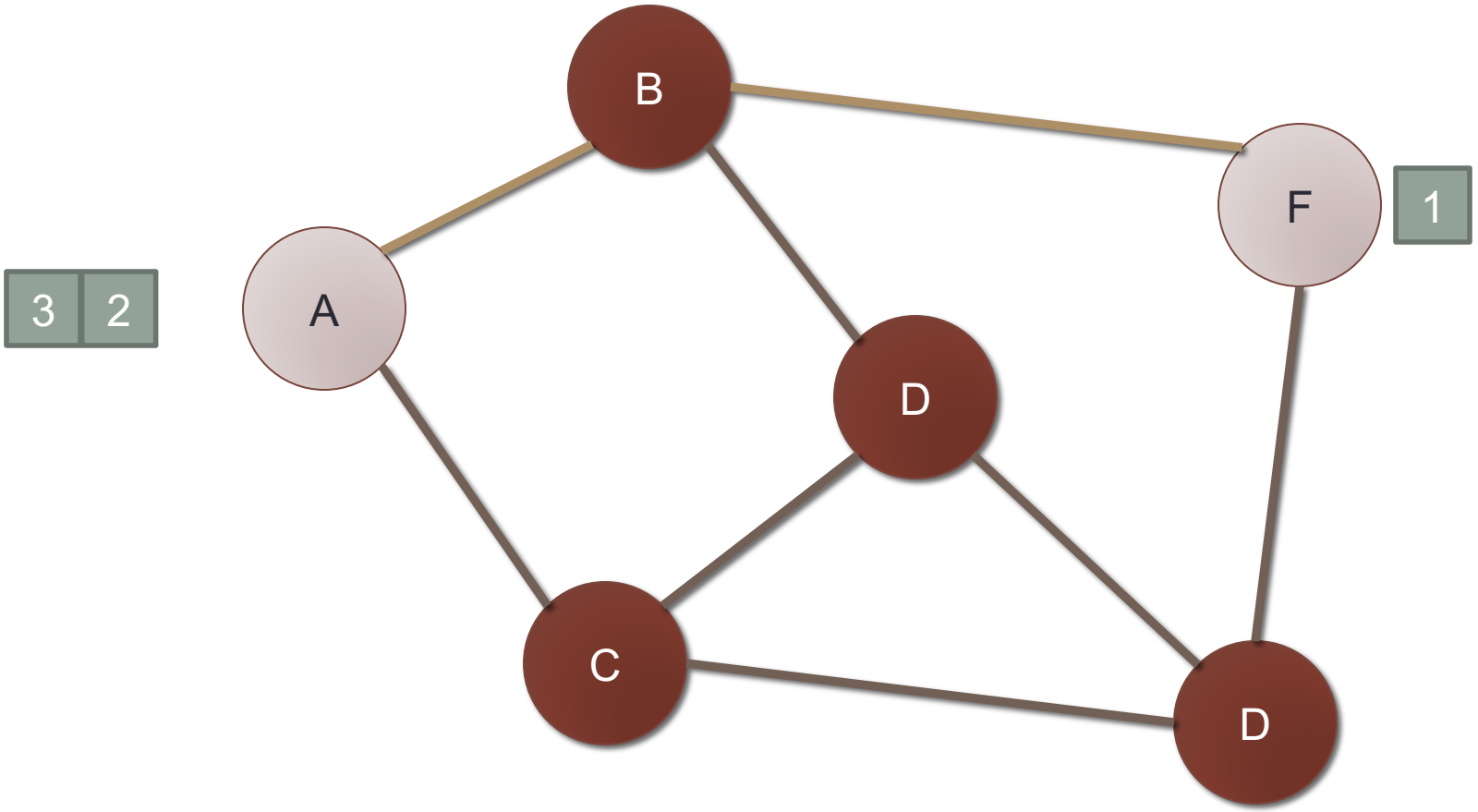


https://slideplayer.com/slide/8097672/

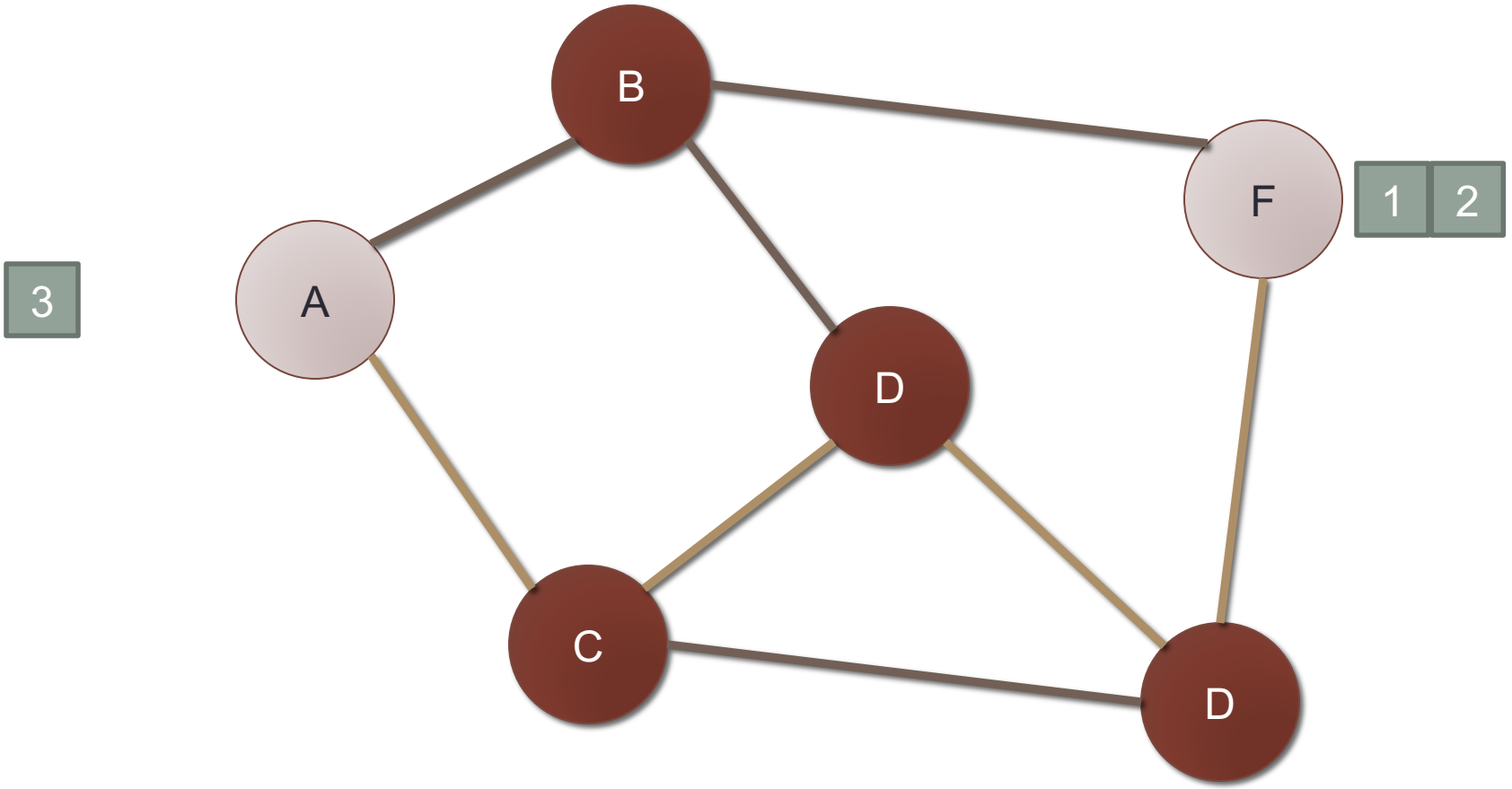
Packet Switching



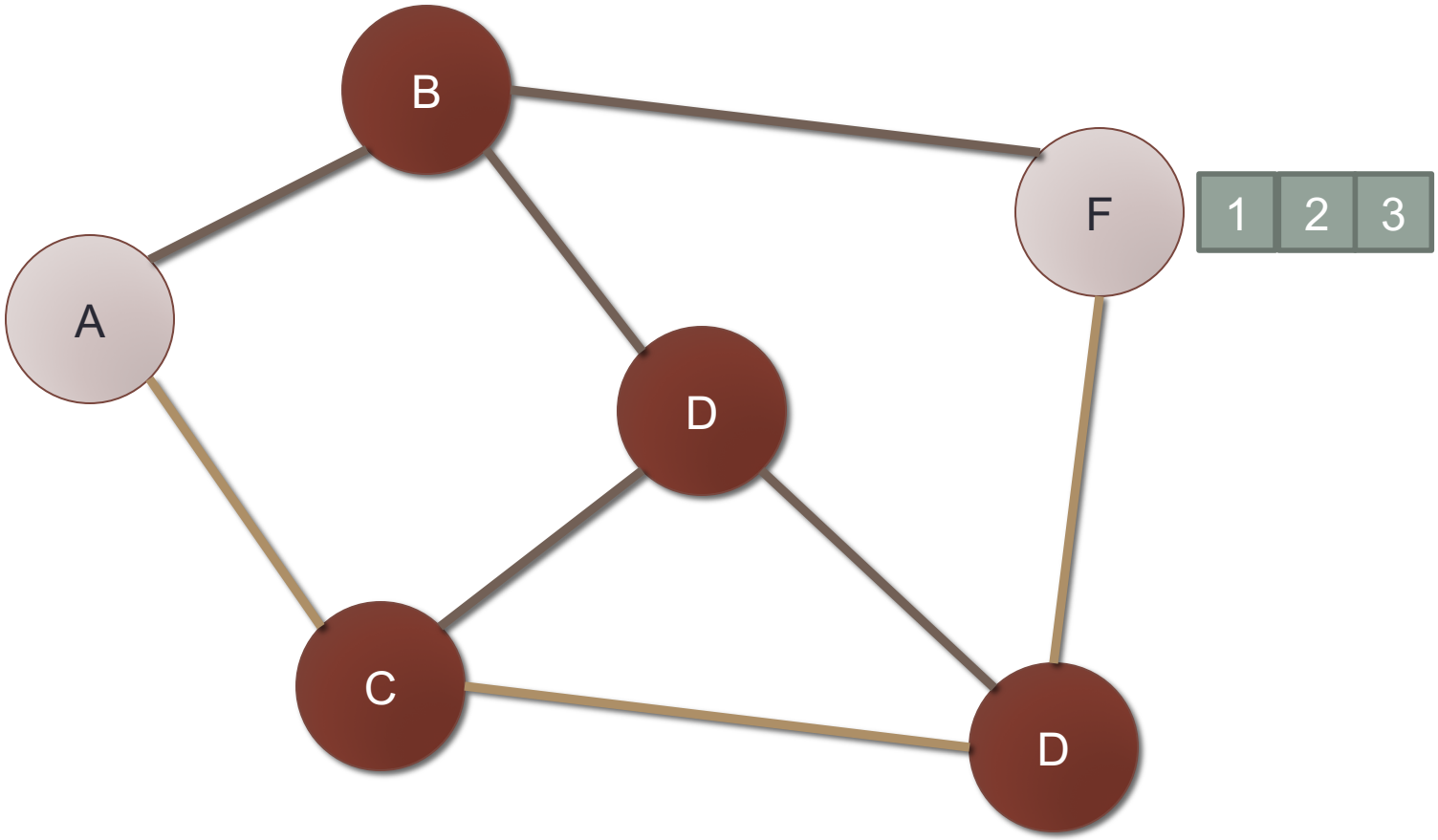
Packet Switching



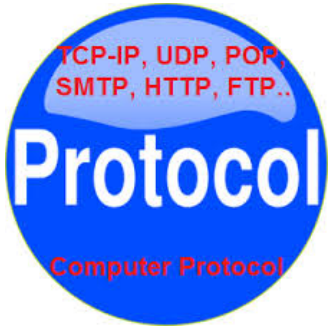
Packet Switching



Packet Switching



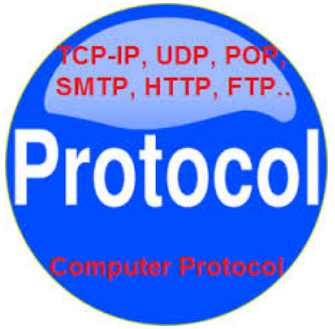
Protocols



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

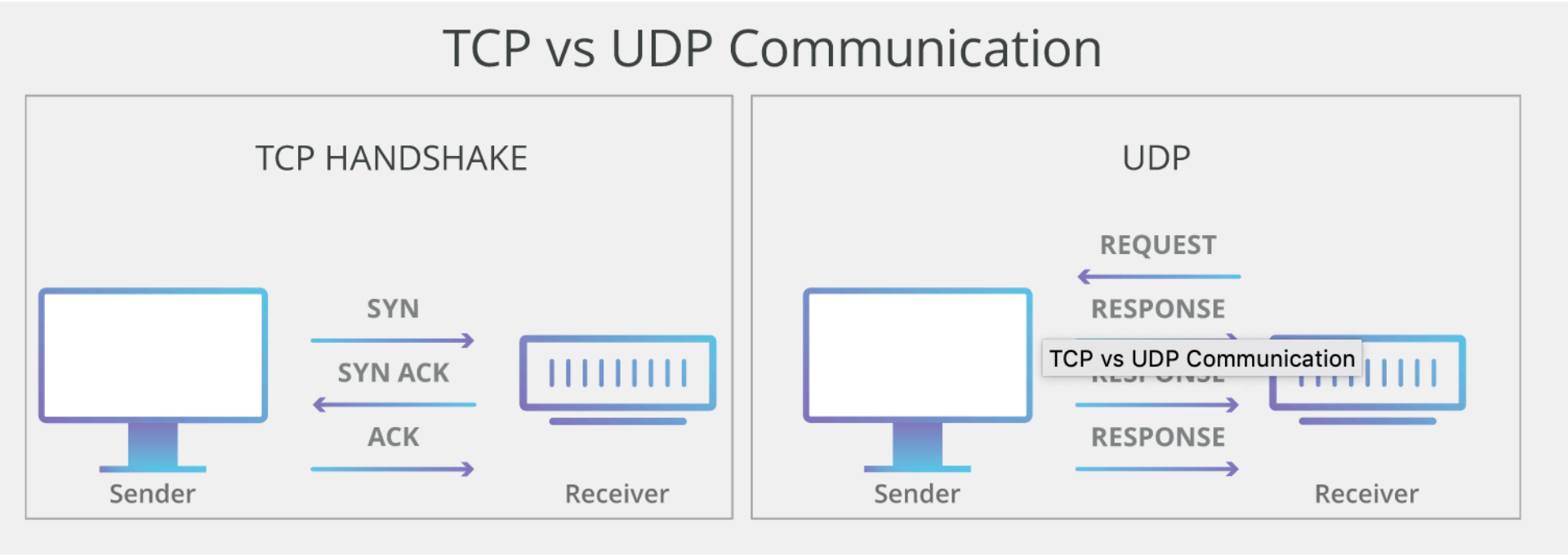
http://www.hinditechy.com/what-is-protocol-in-networking-hindi/

Protocols



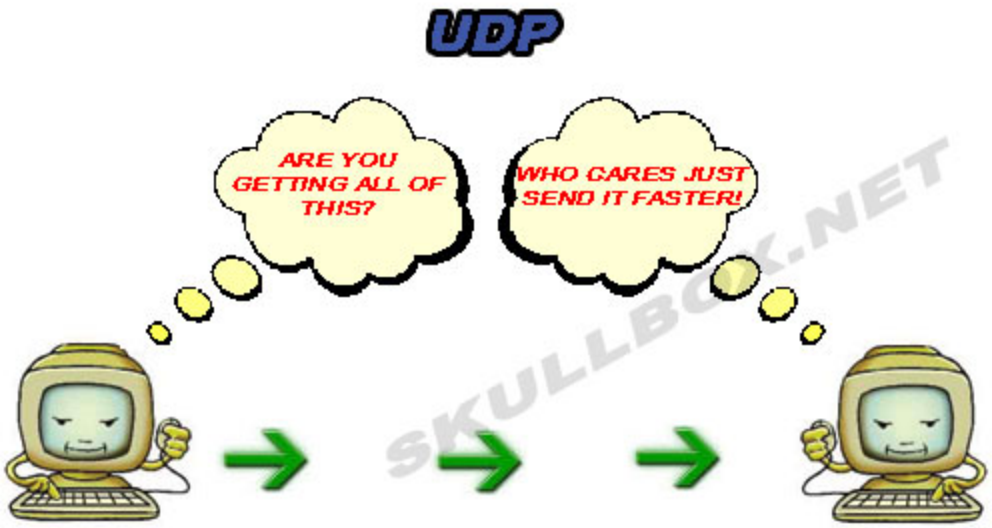
- Connectionless protocol
  - Sends data out as soon as there is enough data to be transmitted
  - E.g., user datagram protocol (UDP)
- Connection-oriented protocol
  - Provides a reliable connection stream between two nodes
  - Consists of set up, transmission, and tear down phases
  - Creates virtual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

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



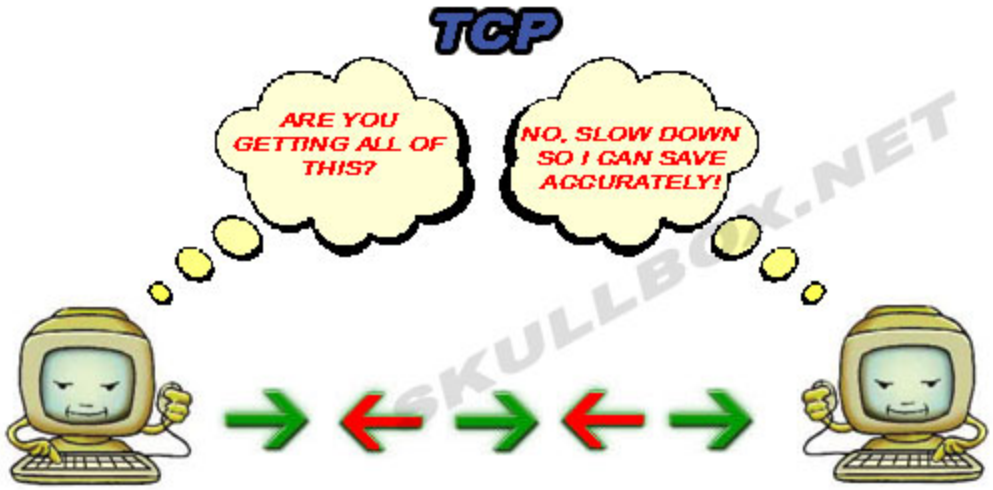
https://www.cloudflare.com/learning/ddos/glossary/user-datagram-protocol-udp/

Connectionless protocol



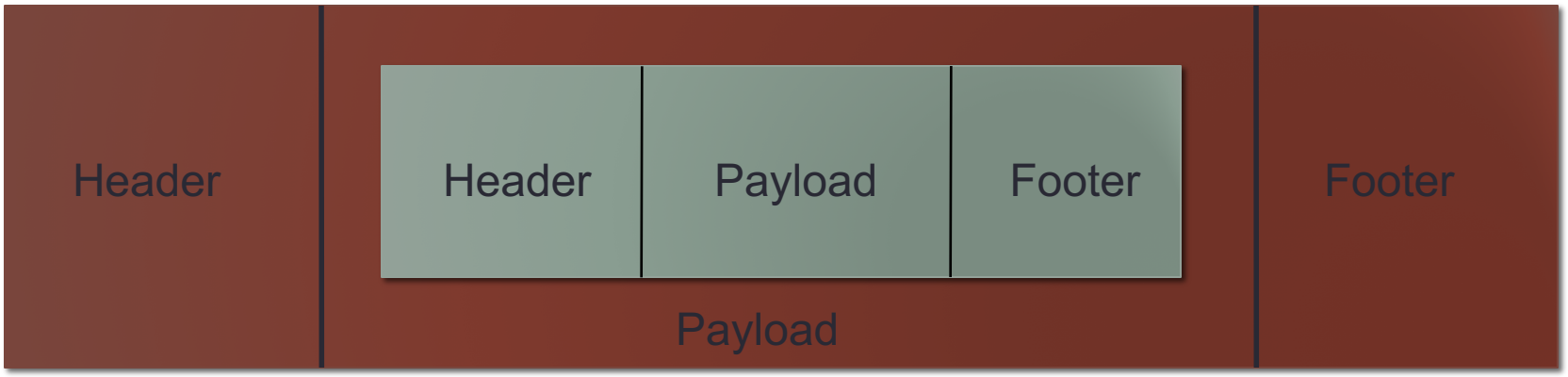
https://www.b4x.com/android/forum/threads/question-about-two-way-communication-using-udp.17316/

Connection-oriented protocol



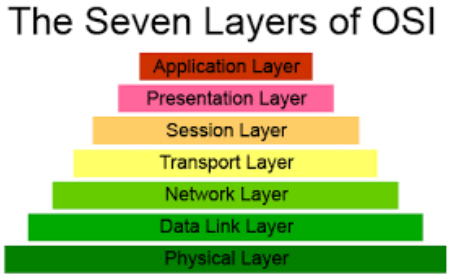
Encapsulation

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

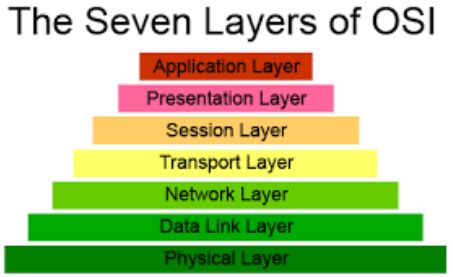
Network Layers



- 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/

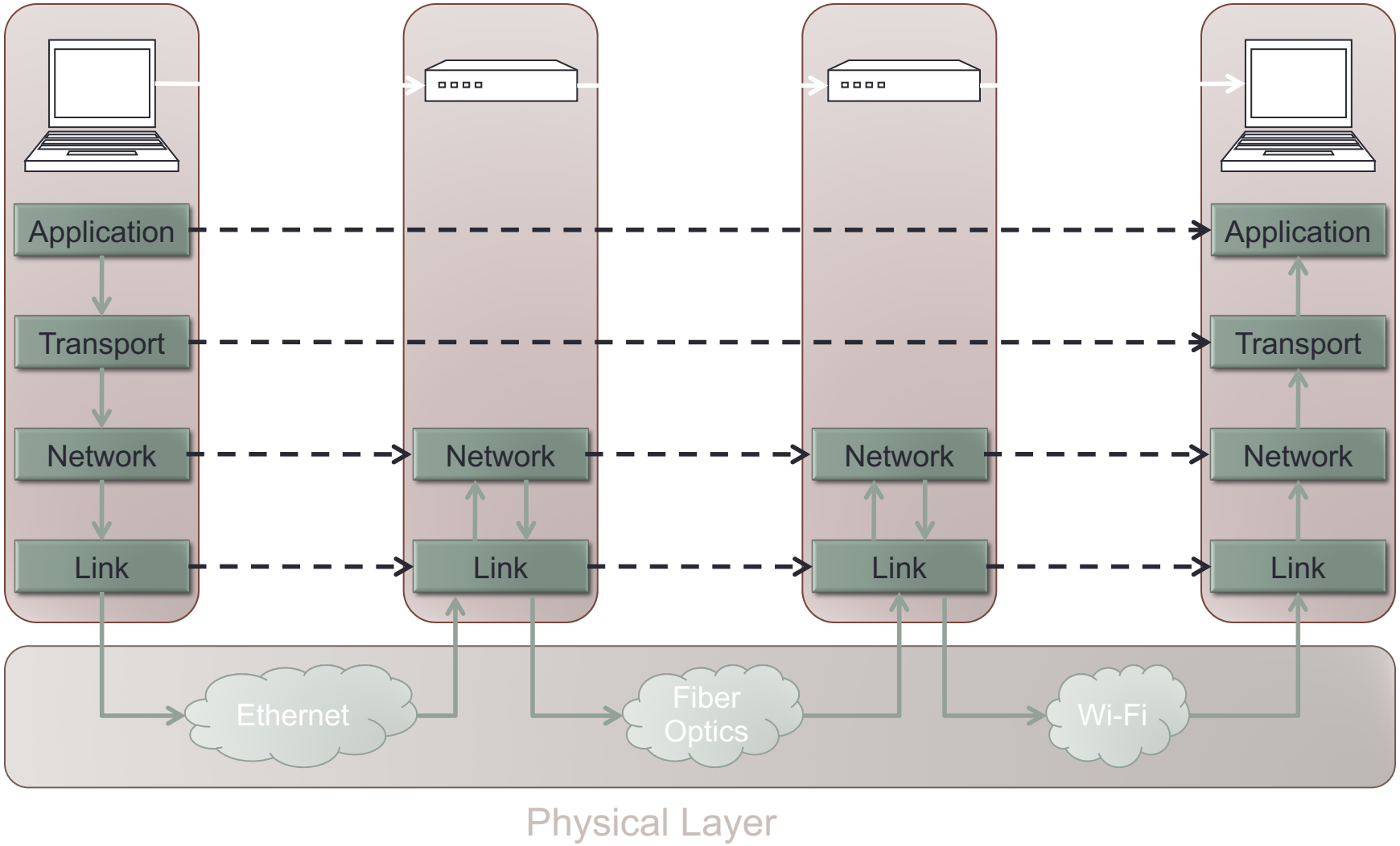
Network Layers



- 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/

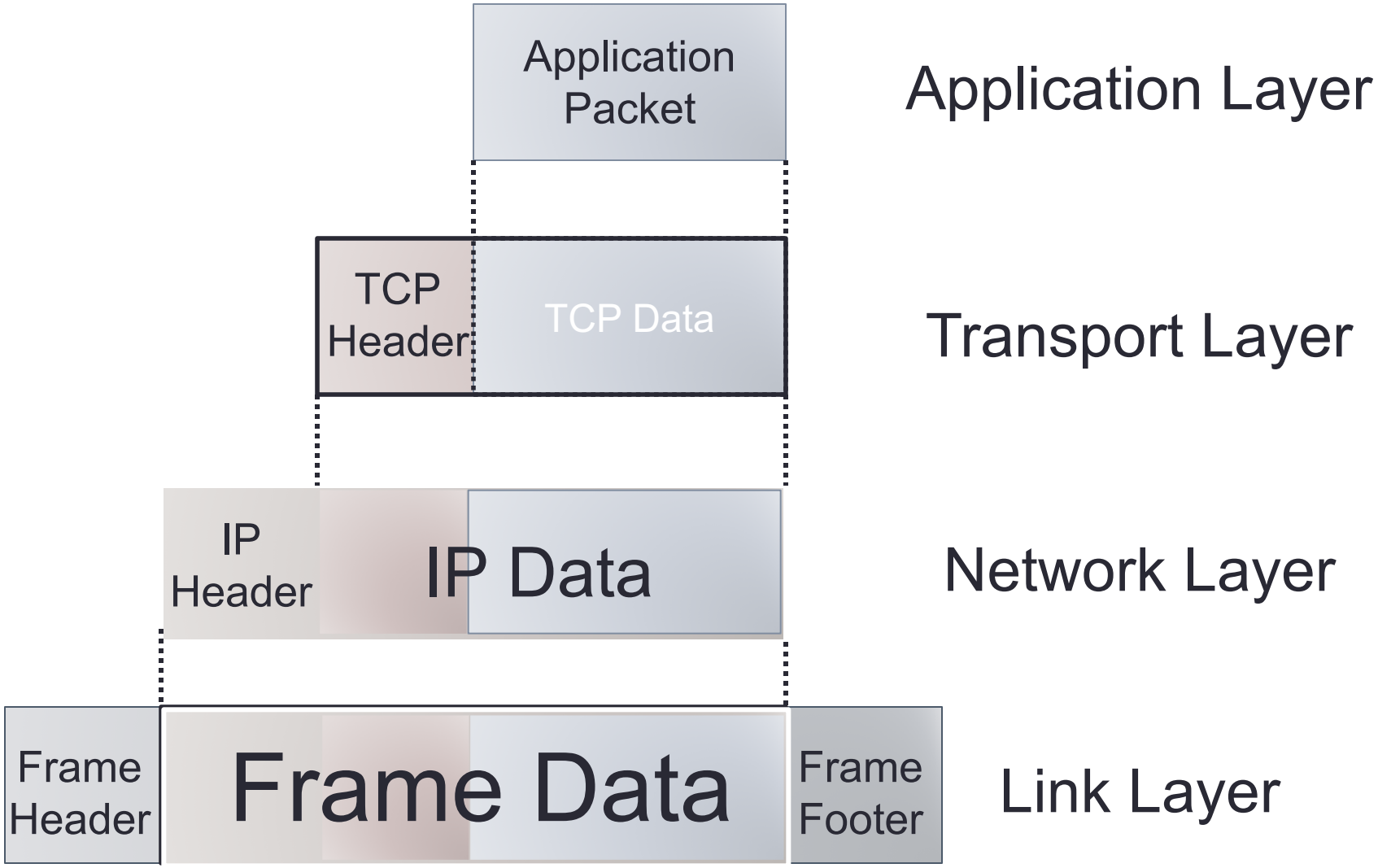
Internet Layers – TCP/IP model



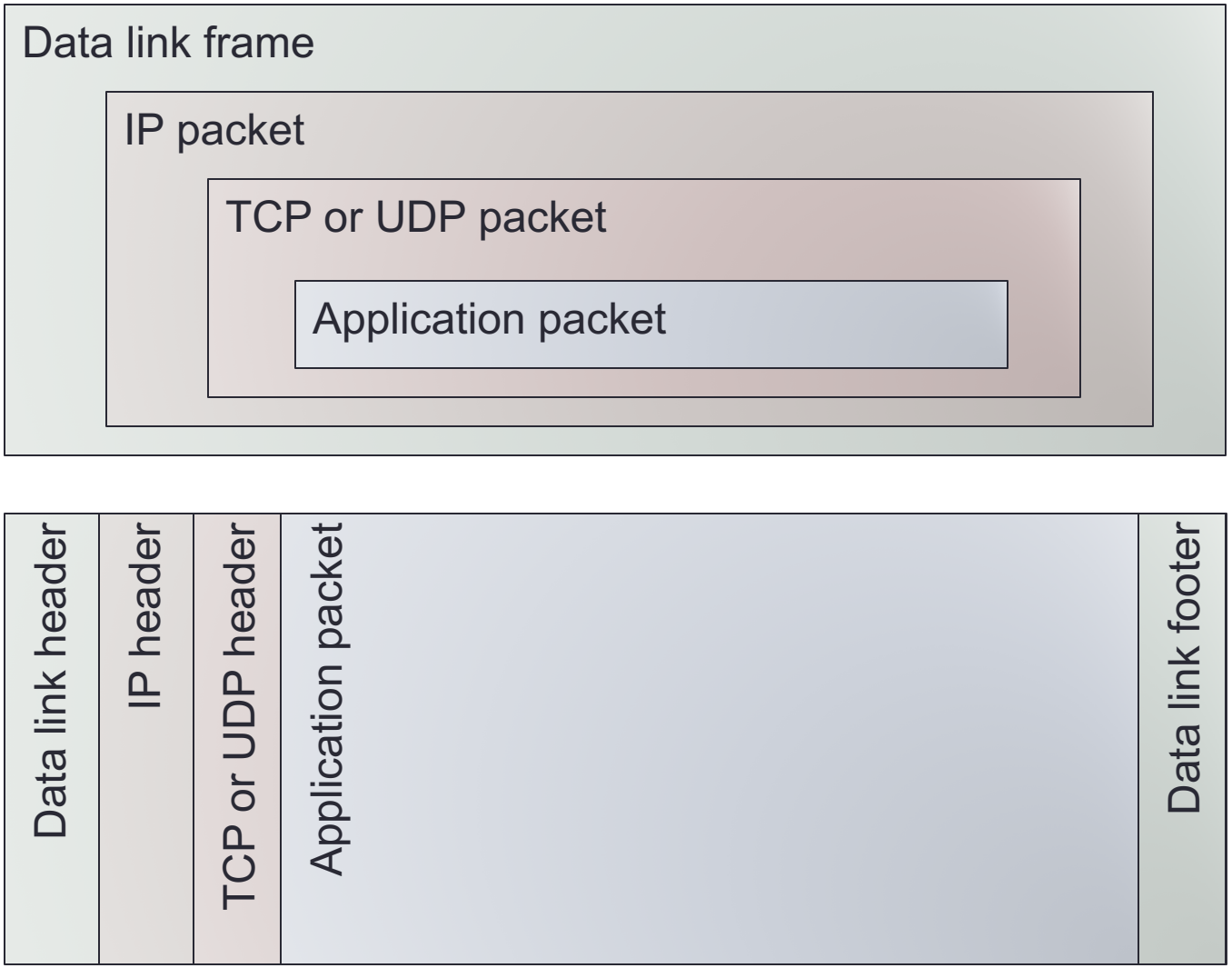
Intermediate Layers

- 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)

Packet Encapsulation – TCP/IP Model

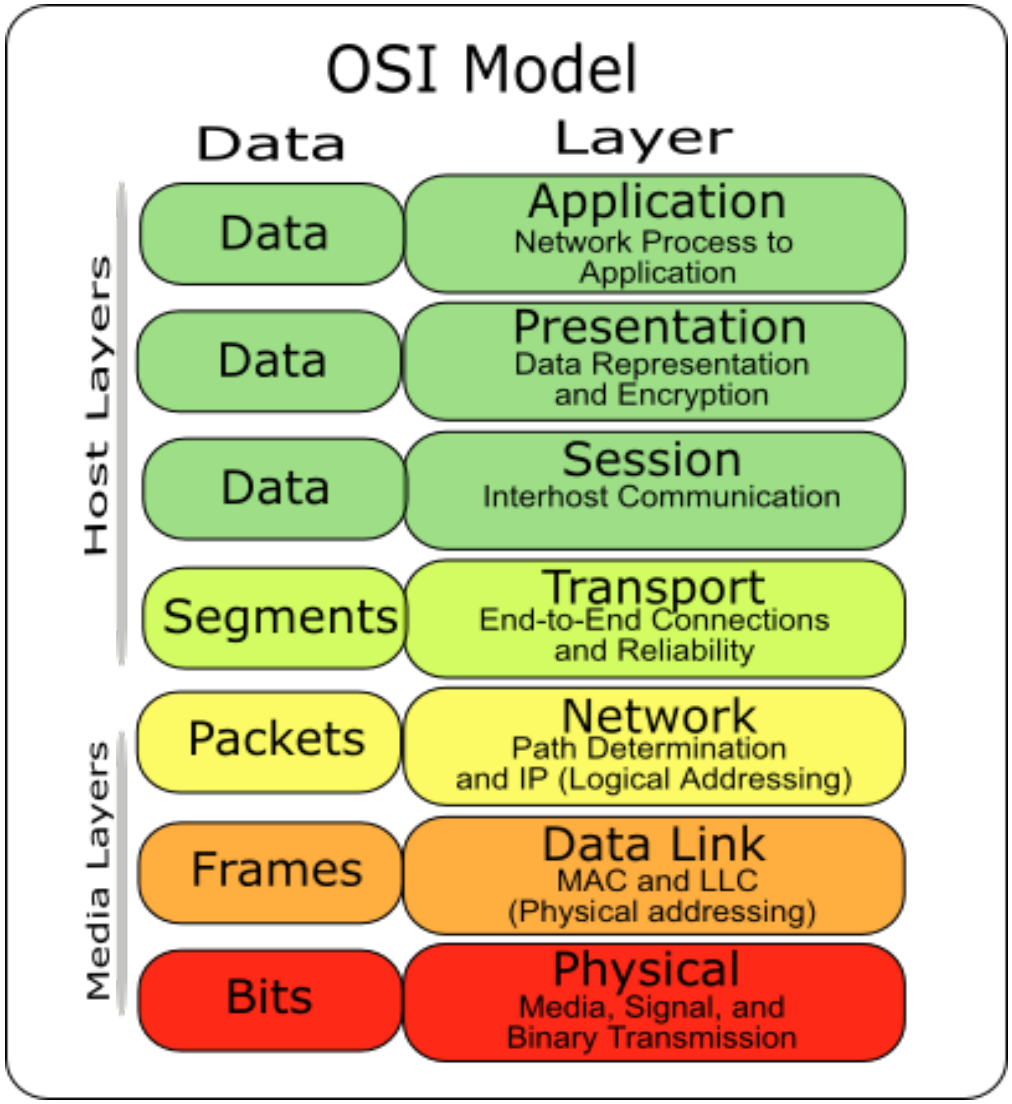


Internet Packet Encapsulation

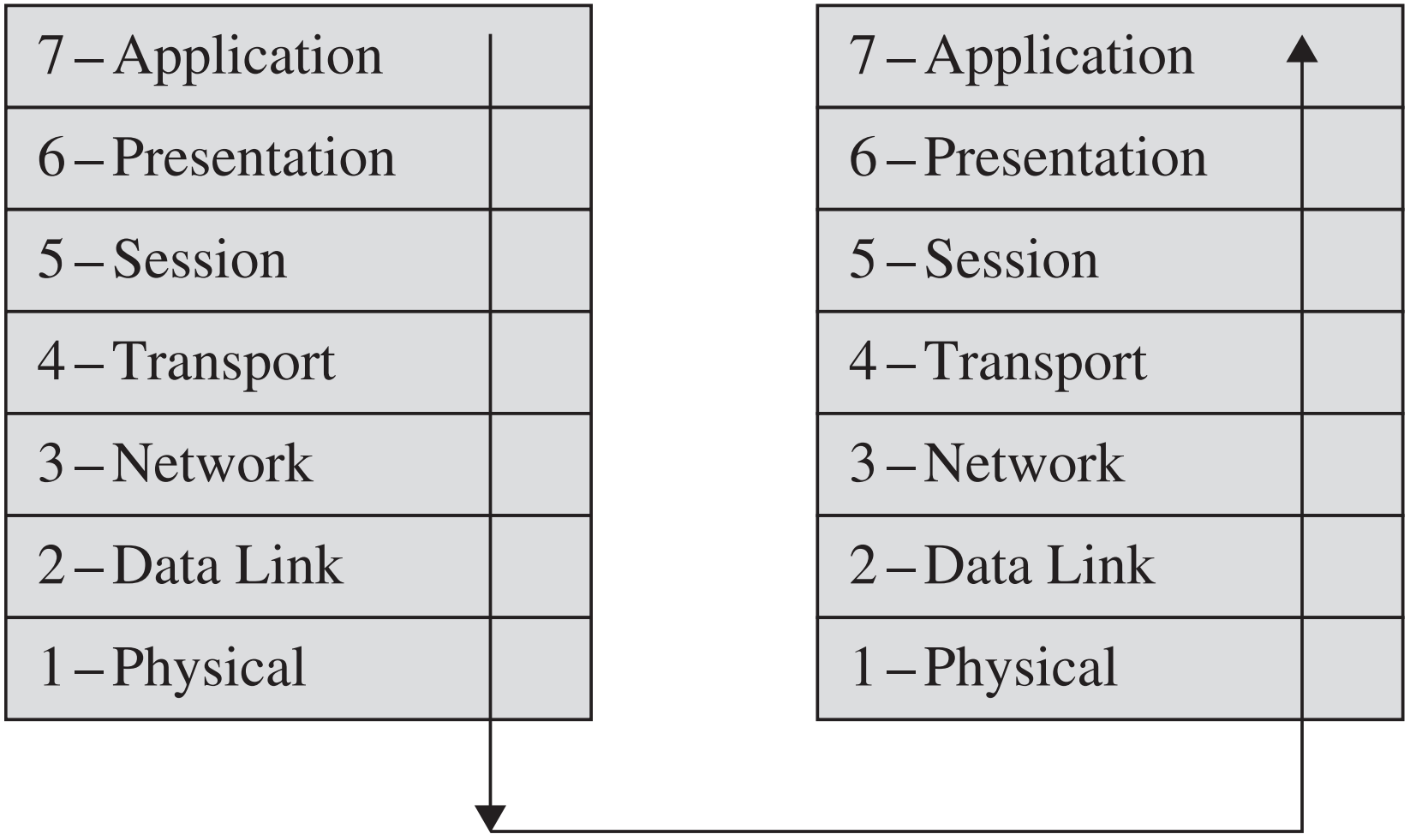


The OSI Model

- 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)



The OSI Model



The OSI Model

- The OSI model doesn't map perfectly to the network protocol stack 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

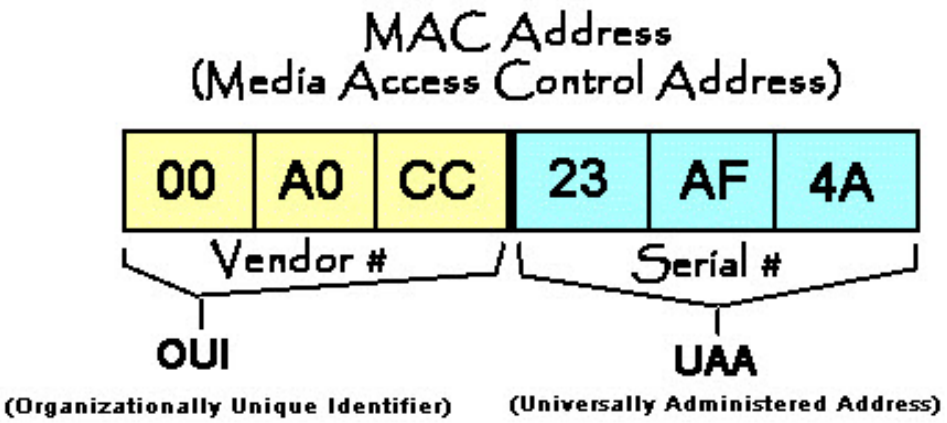
MAC Addresses

- 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 Addresses

- MAC addresses can be:
  - permanently burned in (BIA)
  - locally administered address (LAA) set by an administrator
- Examples:
  - A MAC address starting out with 00-08-74 for instance is assigned by Dell
  - one starting out with 00-0a-95 is assigned by Apple
- Despite the IEEE limitations on LAAs, most OSs allow you to specify an arbitrary MAC for an interface.

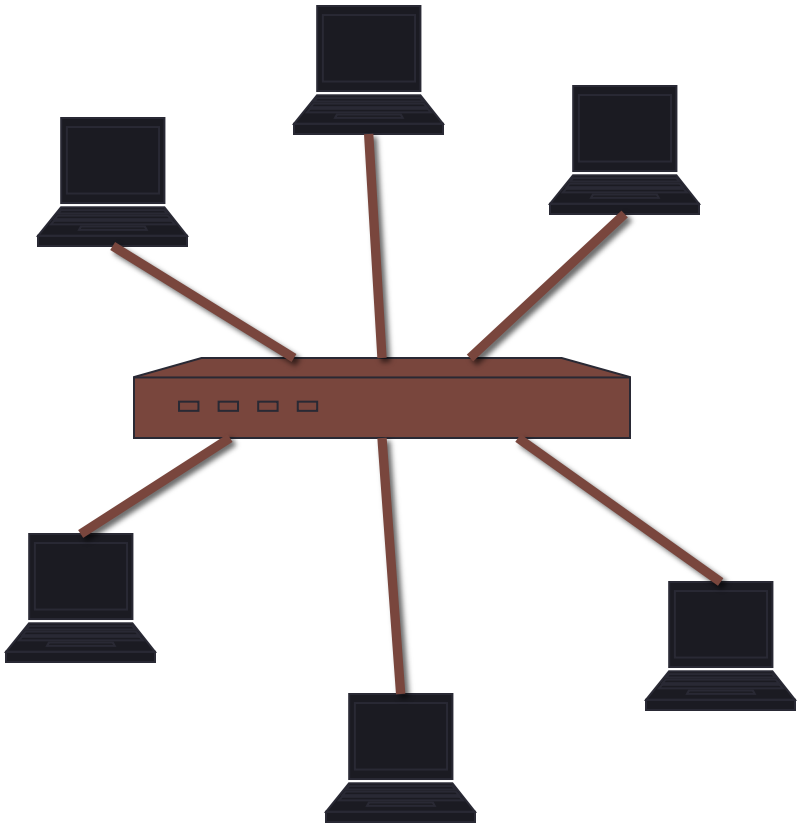
MAC Address



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

Switch

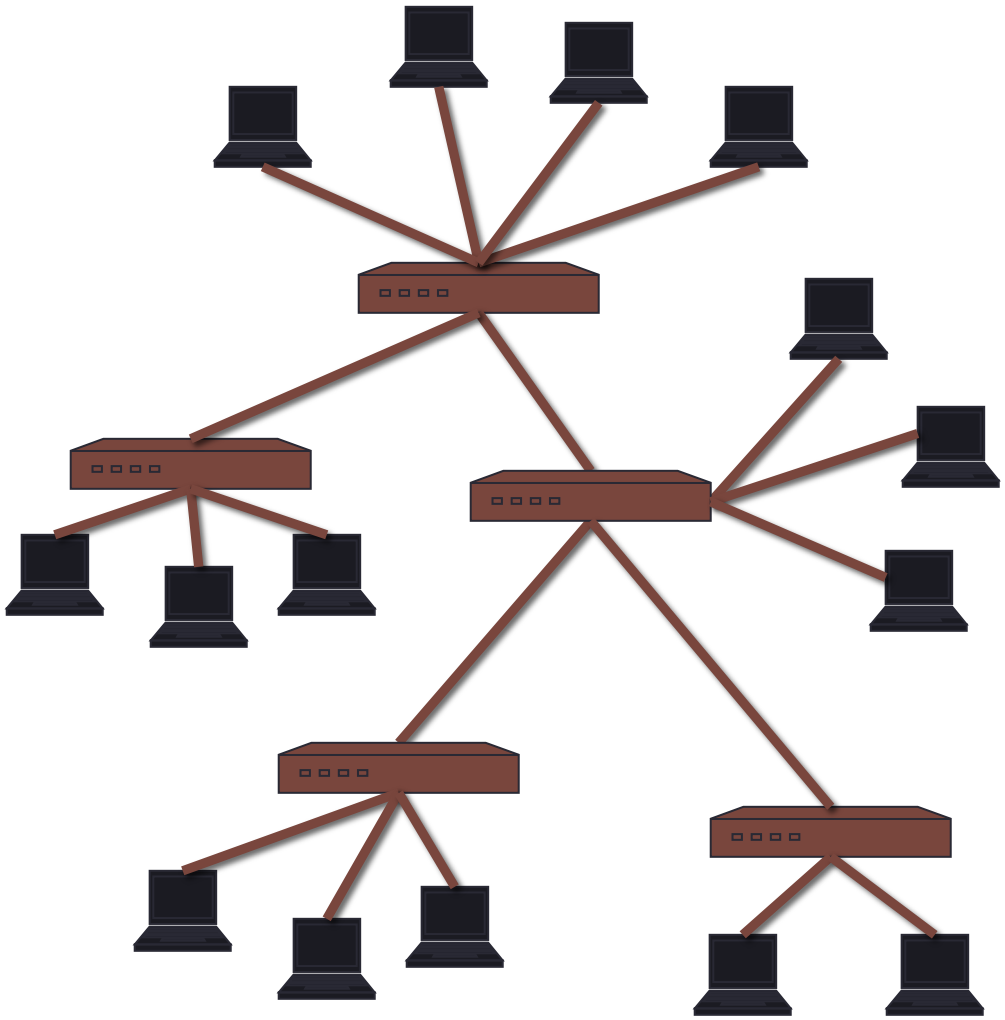
- A switch is a common network device
  - Operates at the link layer
  - Has multiple ports, each connected to a computer
- Operation of a switch
  - Learn the MAC address of each computer connected to it
  - Forward frames only to the destination computer



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



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 the MAC Addresses

- Viewing the MAC addresses of the interfaces of a machine
  - Linux: ifconfig
  - Windows: ipconfig /all

Changing MAC Addresses

- 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
- In other derivatives like FreeBSD, MacOSX and others stopping the network service is not required,
  - the hw flag is dropped
  - =>leading to a single command ifconfig eth0 ether <MAC-address>

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

NETWORKS ATTACK

Threats to Network Communications

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

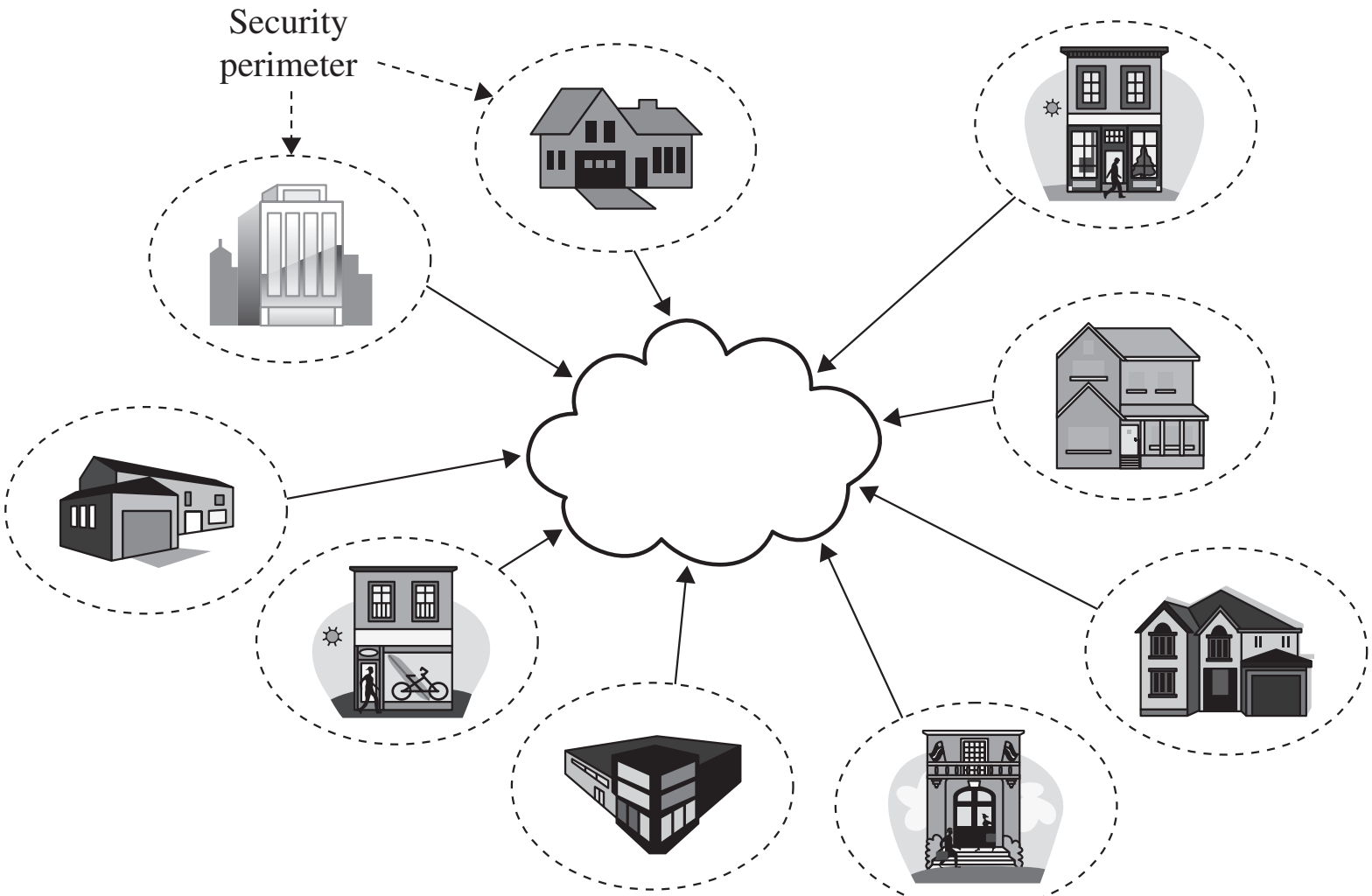
From *Security in Computing, Fifth Edition*, by Charles P. Pfleeger, et al. (ISBN: 9780134085043). Copyright 2015 by Pearson Education, Inc. All rights reserved.

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.

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

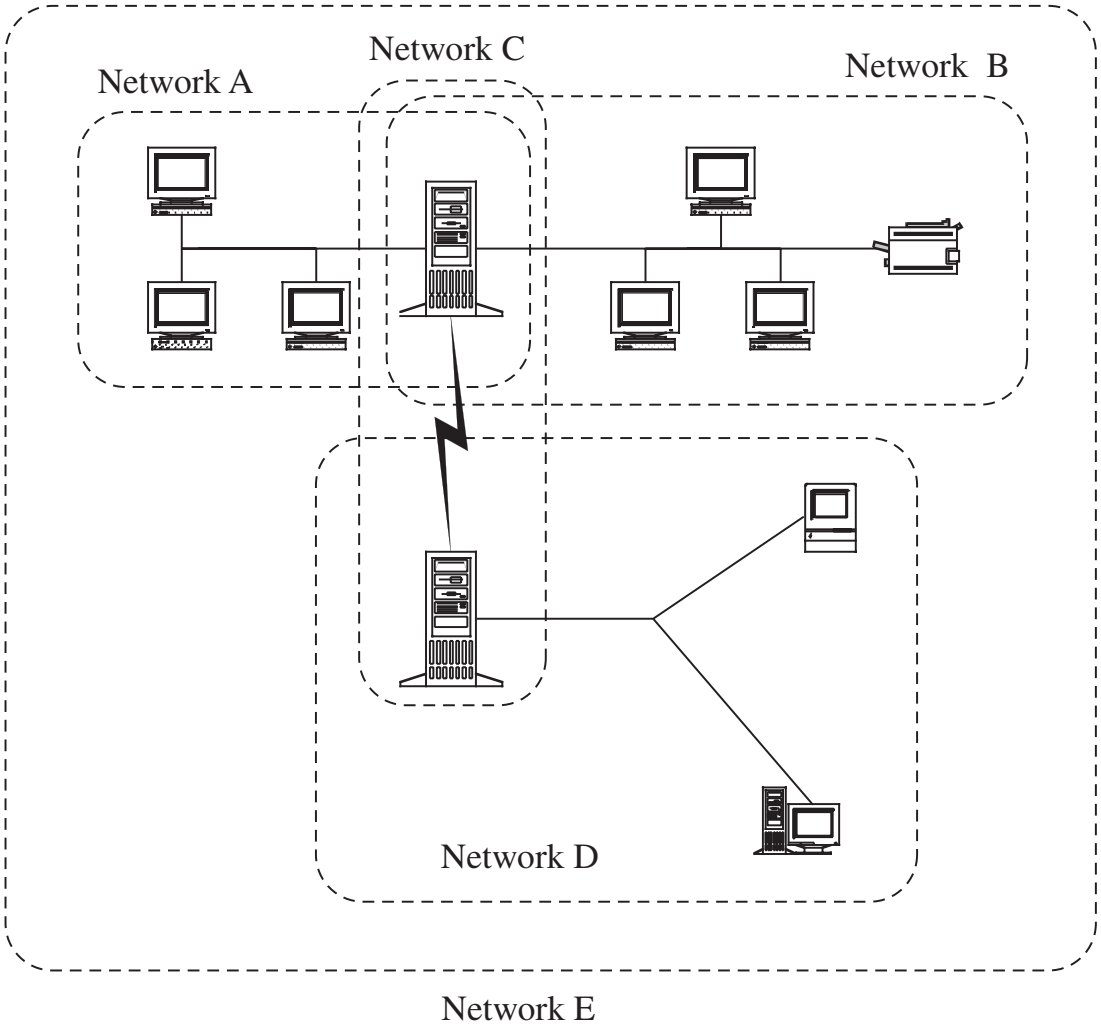
From *Security in Computing, Fifth Edition*, by Charles P. Pfleeger, et al. (ISBN: 9780134085043). Copyright 2015 by Pearson Education, Inc. All rights reserved.

What Makes a Network Vulnerable to Interception?

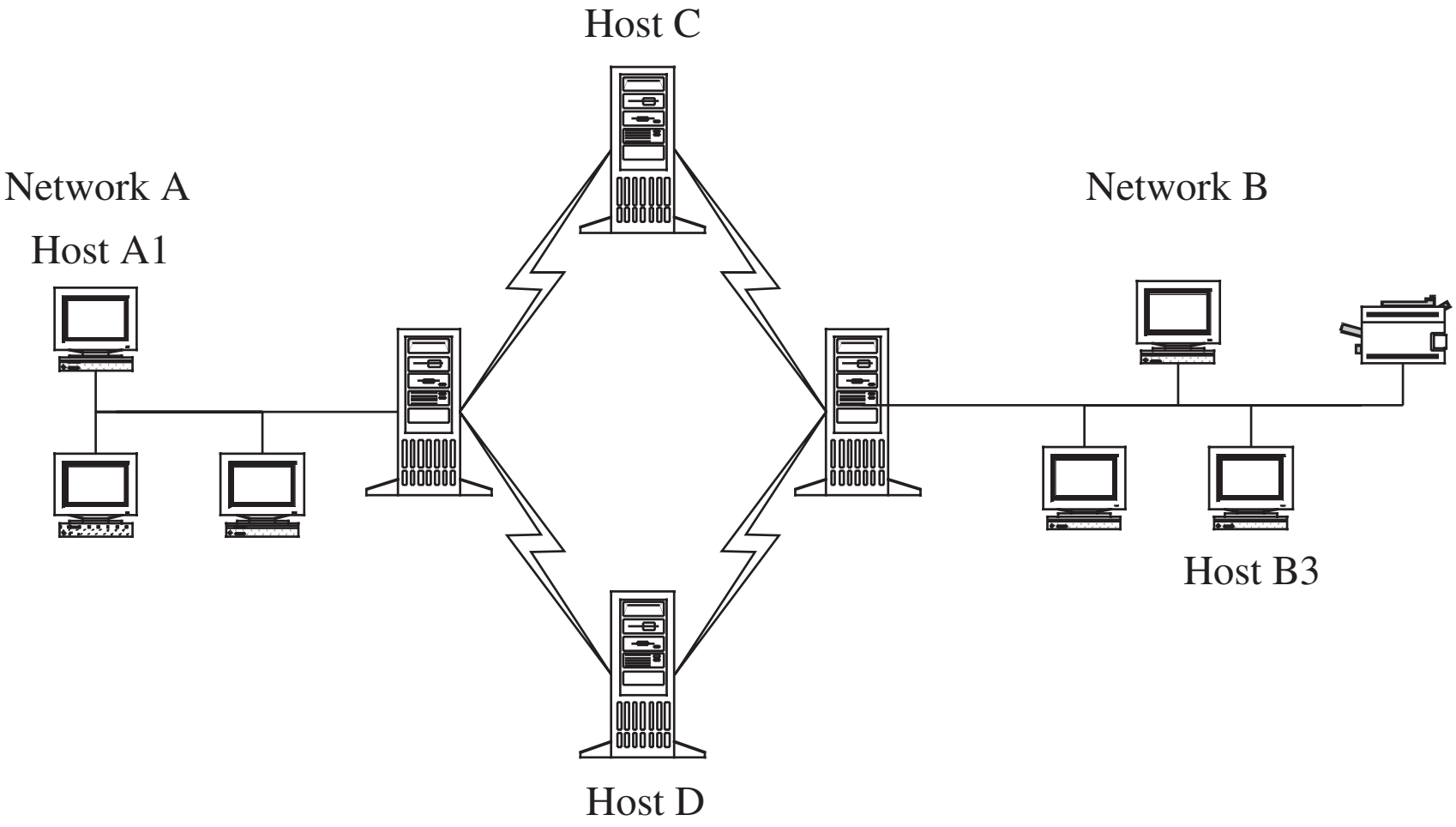
- Unknown perimeter
  - Networks, especially large ones, change all the time
    - it can be hard to tell which systems belong and are behaving, and impossible to tell which systems bridge networks
- Unknown path
  - There may be many paths, including untrustworthy ones, from one host to another

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



Unknown Path



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

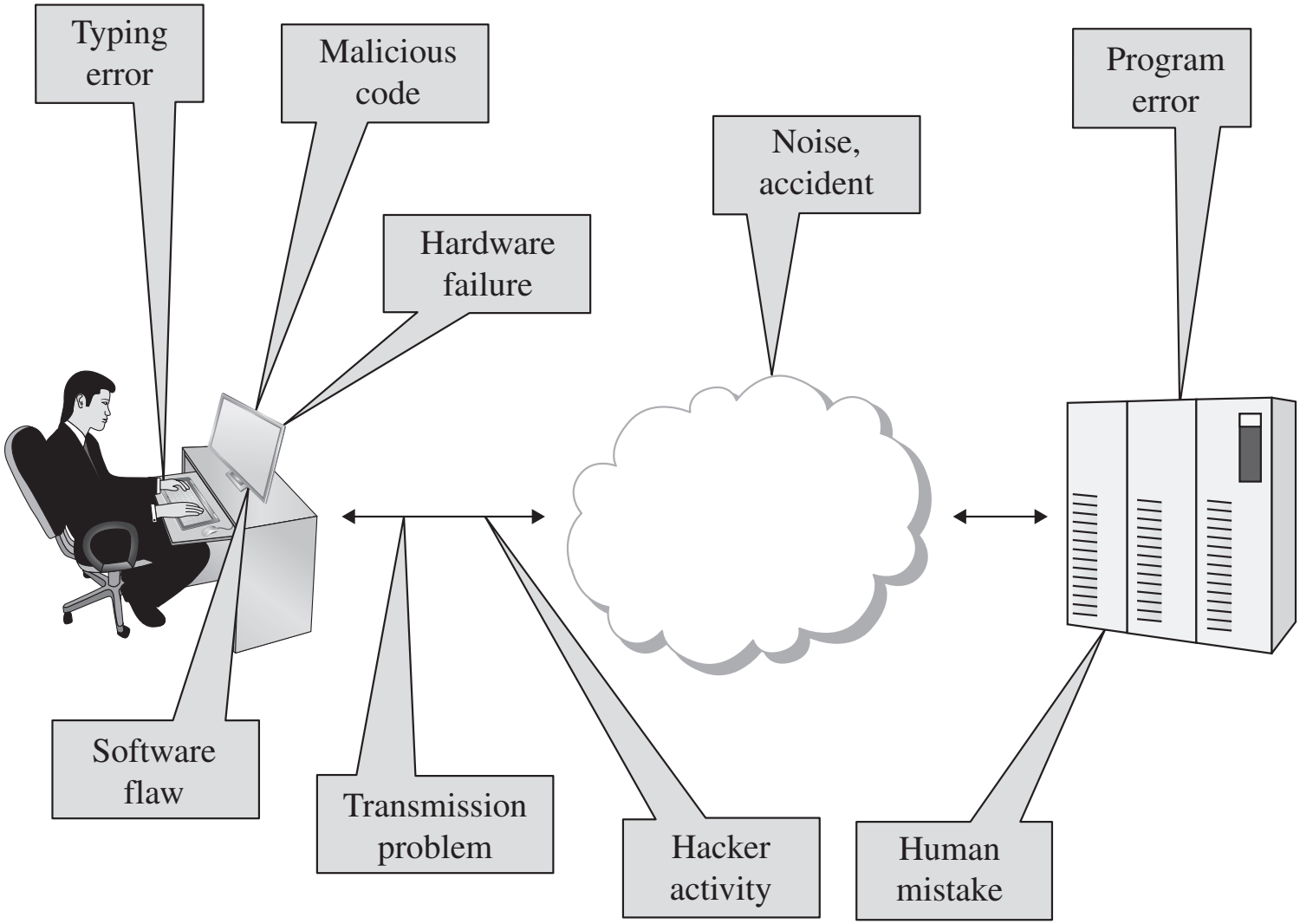
- Data corruption
  - May be intentional or unintentional, malicious or nonmalicious, directed or random
- Sequencing
  - Permuting the order of data, such as packets arriving in sequence
- Substitution
  - Replacement of one piece of a data stream with another

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

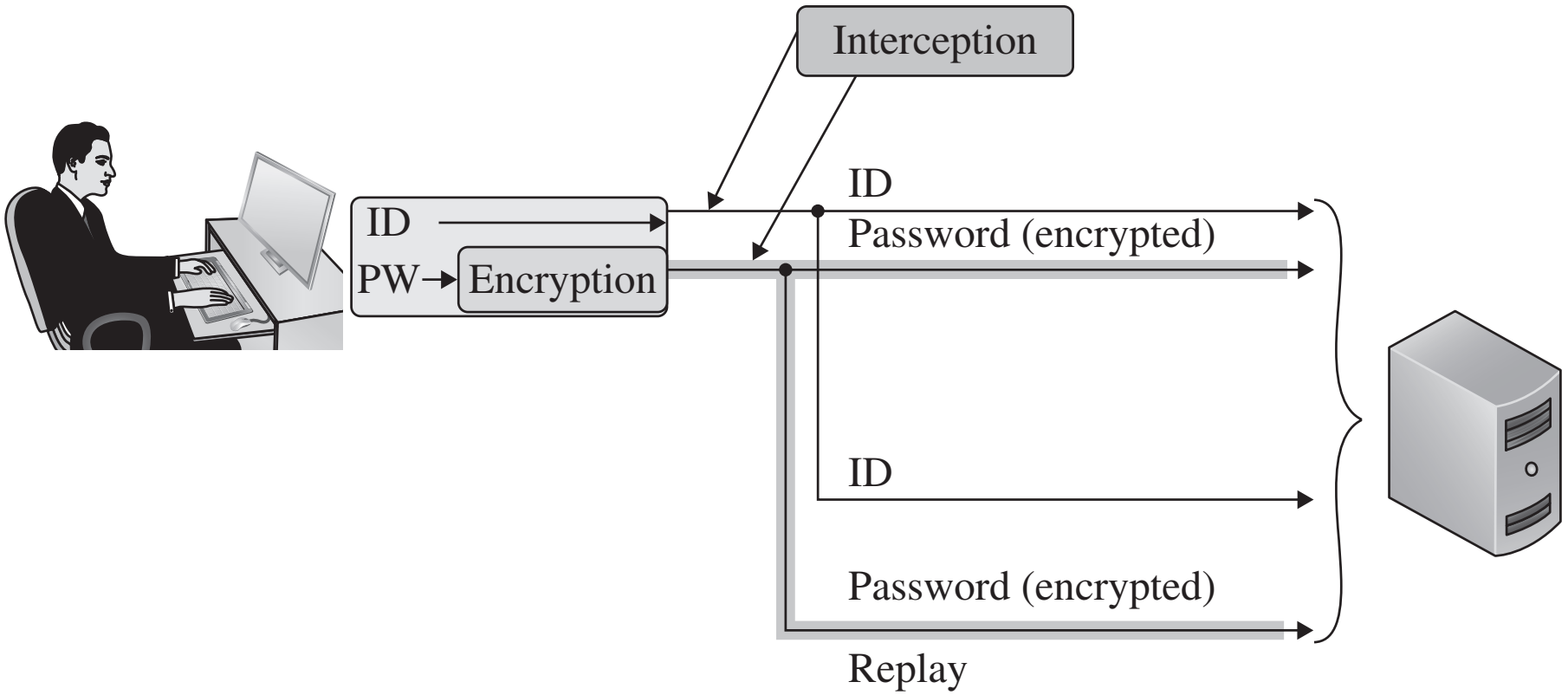
Modification and Fabrication

- 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



Simple Replay Attack



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

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
```

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
```

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.

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.

Wireless Security

- What are the current security options for protecting WIFI networks?
- Originally WEP was introduced as part of the original 802.11
- Designed to protect packets from eavesdroppers
- Not used today
  - Covered for historical reasons

Failed Countermeasure: WEP

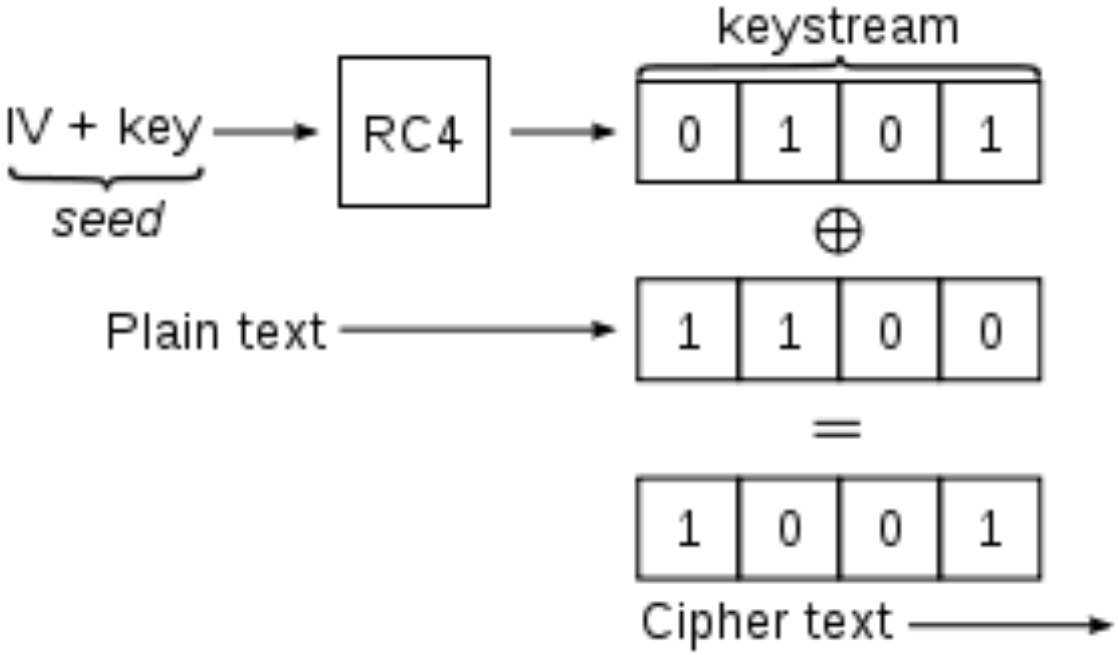
- Wired equivalent privacy (WEP), designed as the mechanism for securing those communications
  - Designed to provide similar security to wired communication
  - at the same time as the original 802.11 WiFi standards

Failed Countermeasure: WEP

- 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

WEP

- Basic WEP encryption: RC4 keystream XORed with plaintext



https://en.wikipedia.org/wiki/Wired_Equivalent_Privacy

How WEP Works

- Supported two system modes:
  - Open System Authentication
    - Clients did not supply credentials
    - Clients had to have pre-shared key to communicate with the AP
      - Or to be able to decrypt frames coming from AP
  - Shared Key Authentication

WEP Shared Key Authentication

- 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

WEP Shared Key Authentication (cont.)

- Once the client is authenticated, the AP and client communicate
  - using messages encrypted with the key
- Any issues with this?
  - Key and encrypted key sent in the clear
    - Vulnerable to cryptoanalysis attack
      - Both plaintext and ciphertext sent in the clear
  - However, not the main weakness in WEP

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 104 bits
  - Keys were either alphanumeric or hex phrases that users typed in
    - => therefore vulnerable to dictionary attacks

WEP Weaknesses

- 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
- 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

WEP Weaknesses

- 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
- 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
  - IV's were sent in plaintext

WEP Weaknesses (cont.)

- Faulty integrity check
  - WEP messages included a checksum to identify transmission errors
    - but did not use one that could address malicious modification
- No authentication
  - Any client that knows the AP's SSID and MAC address is assumed to be legitimate

WEP Weaknesses

- Today open source tools can show attacks on WEP key in minutes
  - Aircrack-ng, etc.
- Some legacy systems may still run WEP
  - Should not be used

Tutorial: Simple WEP Crack

Version: 1.20 January 11, 2010
By: darkAudax

Introduction

This tutorial walks you though a very simple case to crack a WEP key. It is intended to build your basic skills and get you familiar with the concepts. It assumes you have a working wireless card with drivers already patched for injection.

The basic concept behind this tutorial is using aireplay-ng replay an ARP packet to generate new unique IVs. In turn, aircrack-ng uses the new unique IVs to crack the WEP key. It is important to understand what an ARP packet is. This "What is an ARP?" section provides the details.

https://www.aircrack-ng.org/doku.php?id=simple_wep_crack

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
  - Designed to be compatible with old WPA-compatible hardware
    - With simple firmware update

WPA (WiFi Protected Access)

- Temporal Key Integrity Protocol (TKIP):
  - A secure key-derivation protocol
    - Incorporating IV into per-packet encryption key
  - A sequence counter implemented
    - Rejecting out-of-order packets, prevent replay attack
  - A 64 Message Integrity Check(MIC) introduced
    - Prevent forging or corruption of packets

WPA (WiFi Protected Access)

- Used RC4 cipher
  - But in a more secure way
    - Used key-mixing function to generate unique keys per packet
    - Generated 256-bit keys

WPA (WiFi Protected Access)

- 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
  - The user WI-FI password is used as one of the factors when deriving the encryption keys.

WPA (WiFi Protected Access)

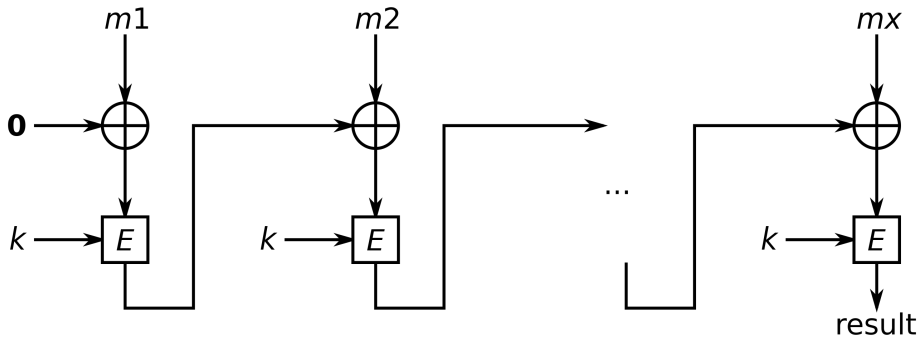
- Authentication
  - WPA allows authentication by password, token, or certificate
- Strong encryption
  - WPA adds support for AES, a much more reliably strong encryption algorithm
- Integrity protection
  - WPA includes a 64-bit cryptographic integrity check

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

WPA2

- The most secure protocol for wireless networks today
- Implemented counter mode CBC-MAC protocol
  - a technique for constructing a message authentication code from a block cipher



WPA2

- Based on AES
  - Not using RC4
- Allows for authenticated encryption
  - Data is confidential and authenticated
    - Authenticate and encrypt

- Questions?