COMPUTER SECURITY

Chapter 6: Network Security

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

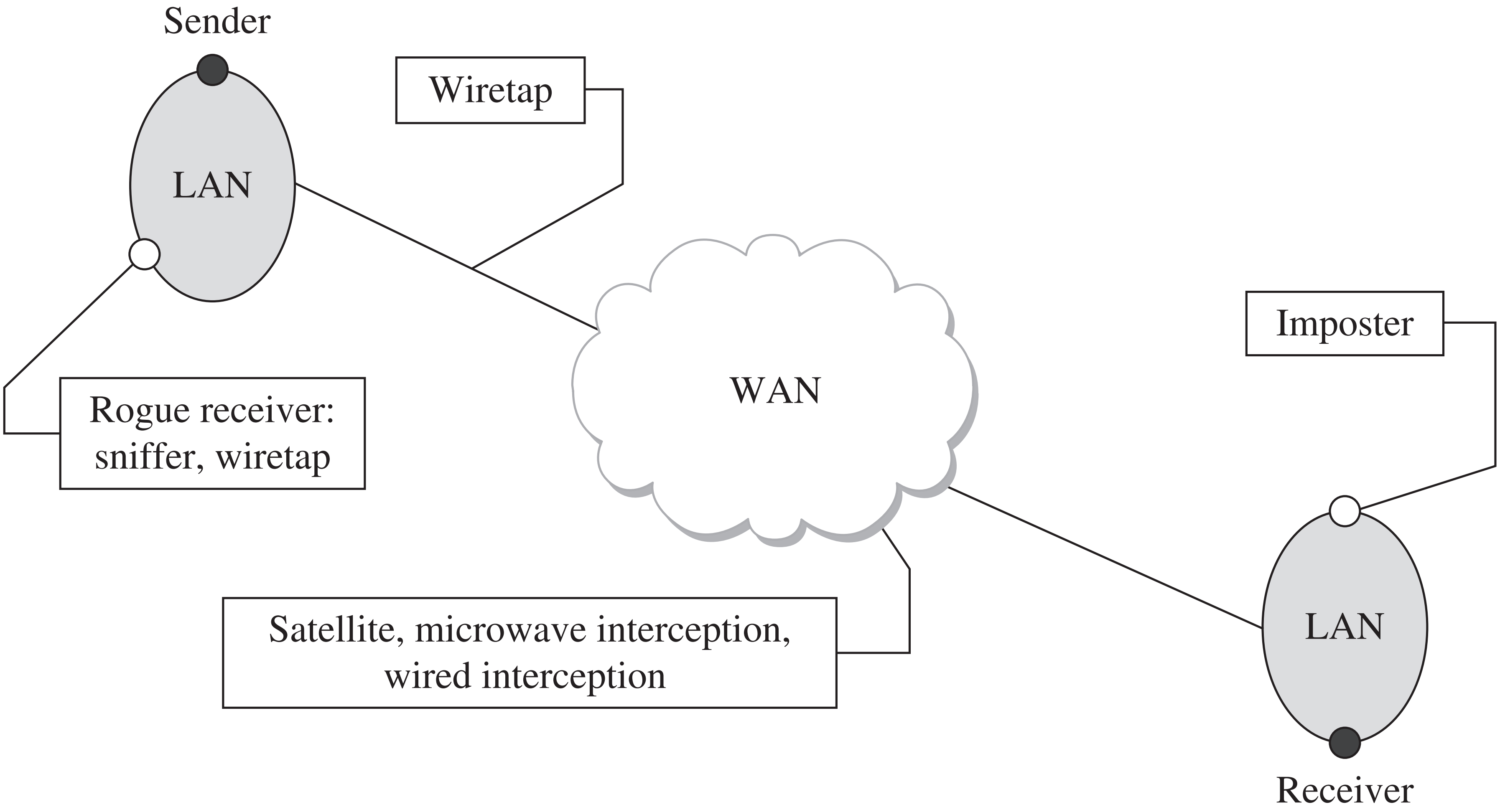
Communication Media Vulnerability

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

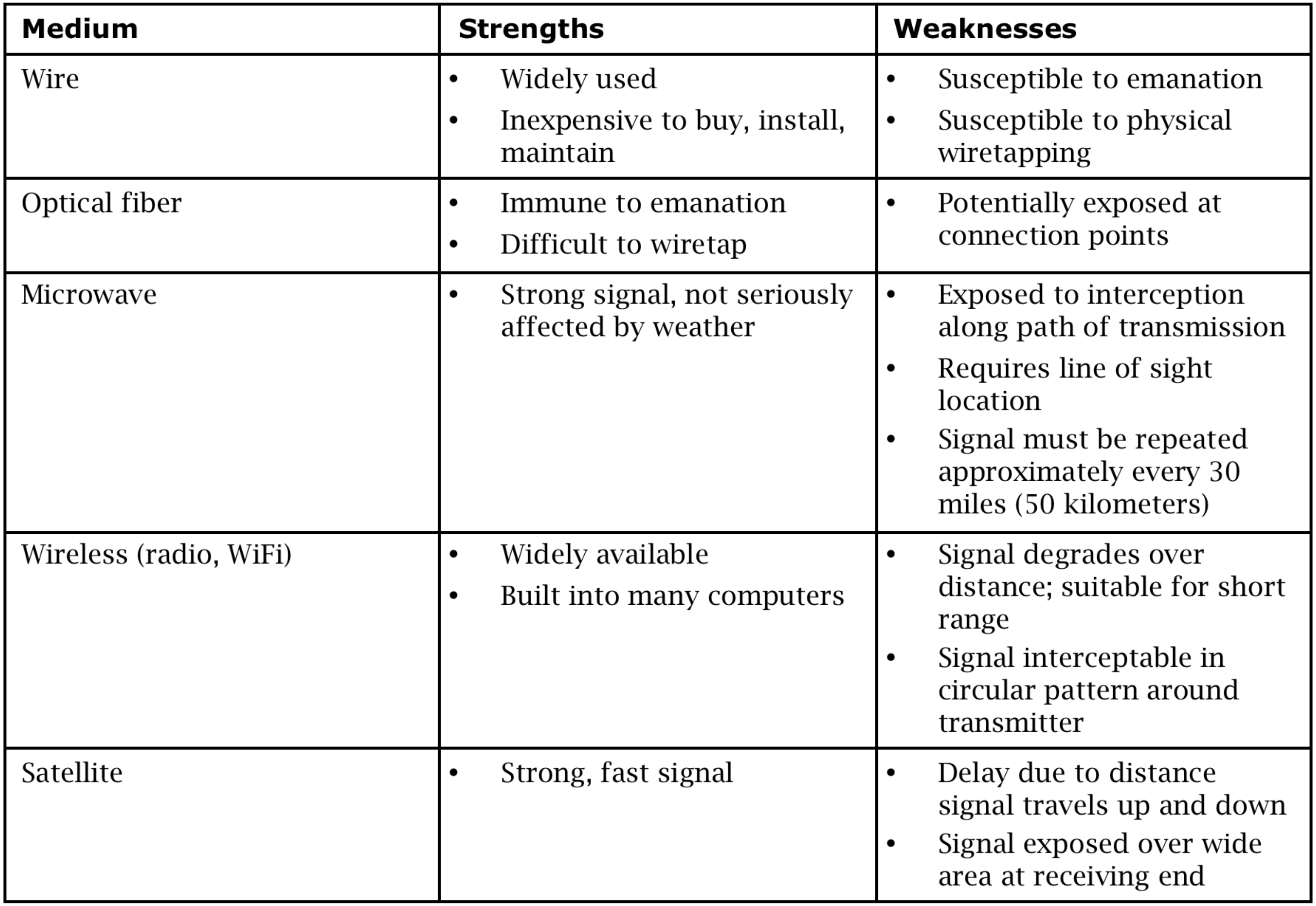
Communication Media Vulnerability

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

Communication Media Vulnerability

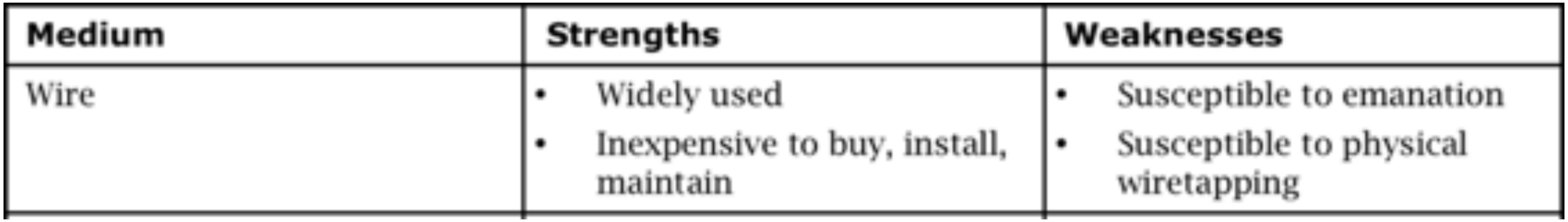

Sender
Wiretap
LAN
WAN
Imposter
Rogue receiver: sniffer, wiretap
Satellite, microwave interception, wired interception
LAN
Receiver

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

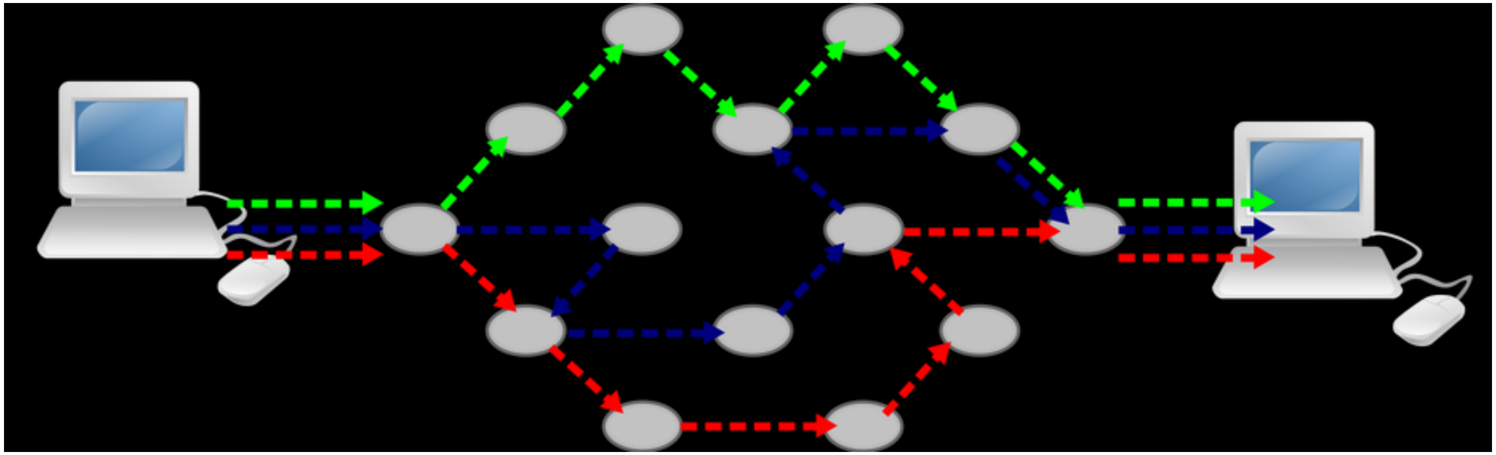
* Emanation = “the action or process of issuing from a source.”

- 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



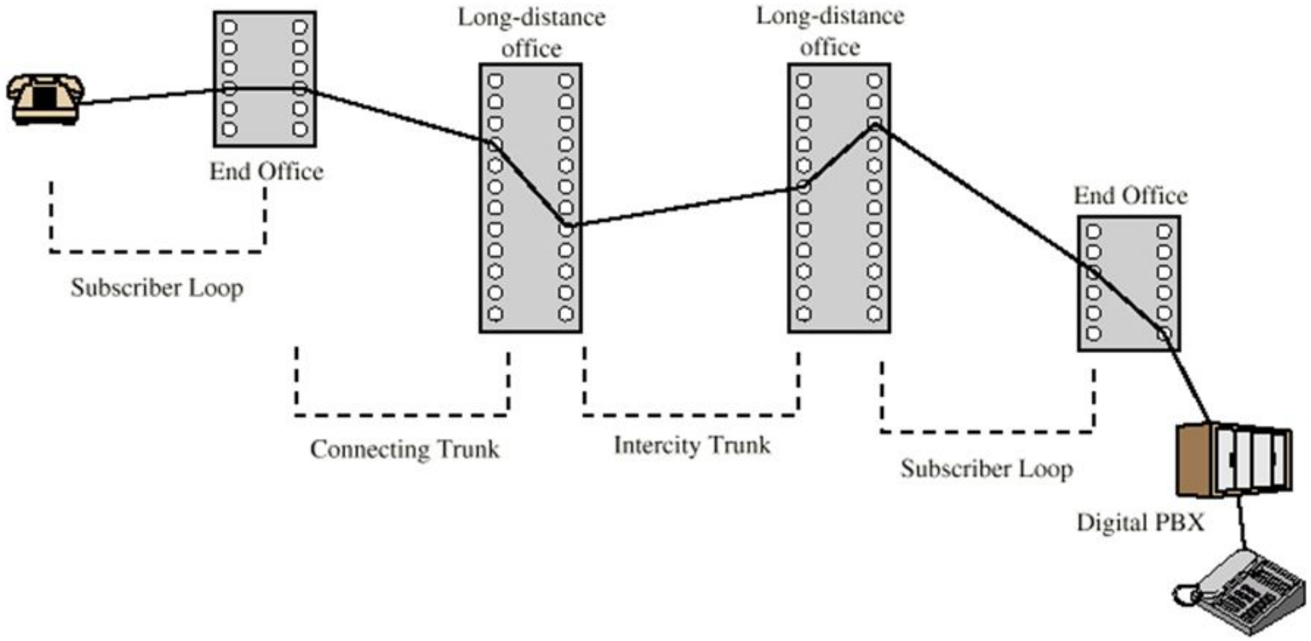
http://www.apposite-tech.com/blog/uncategorized/packet-switching-vs-circuit-switching/

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

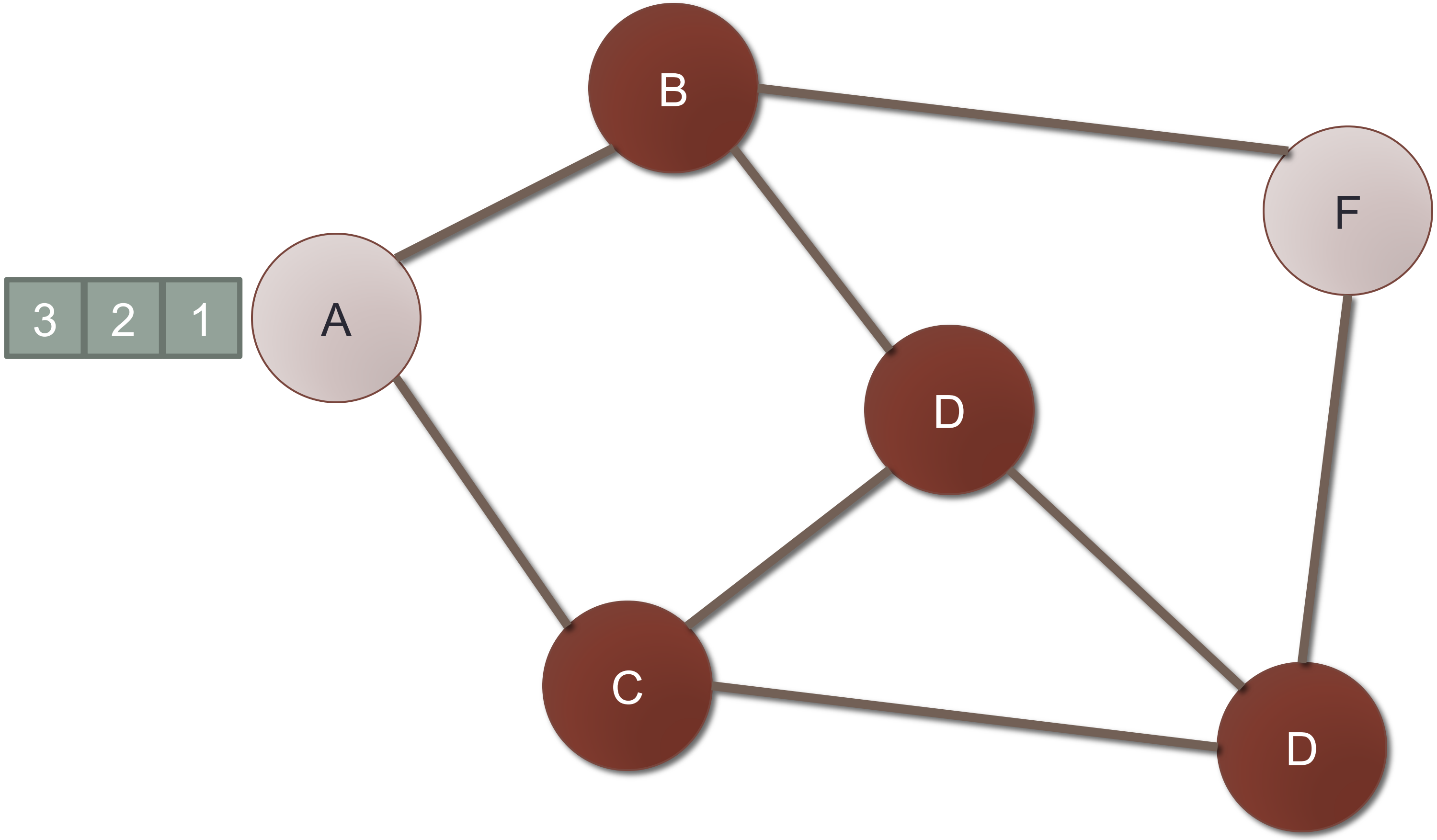
- Packet switching
  - Internet
  - Data split into packets
  - Packets transported independently through network
  - Each packet handled on a best efforts basis
  - Packets may follow different routes

Public Circuit Switched Network

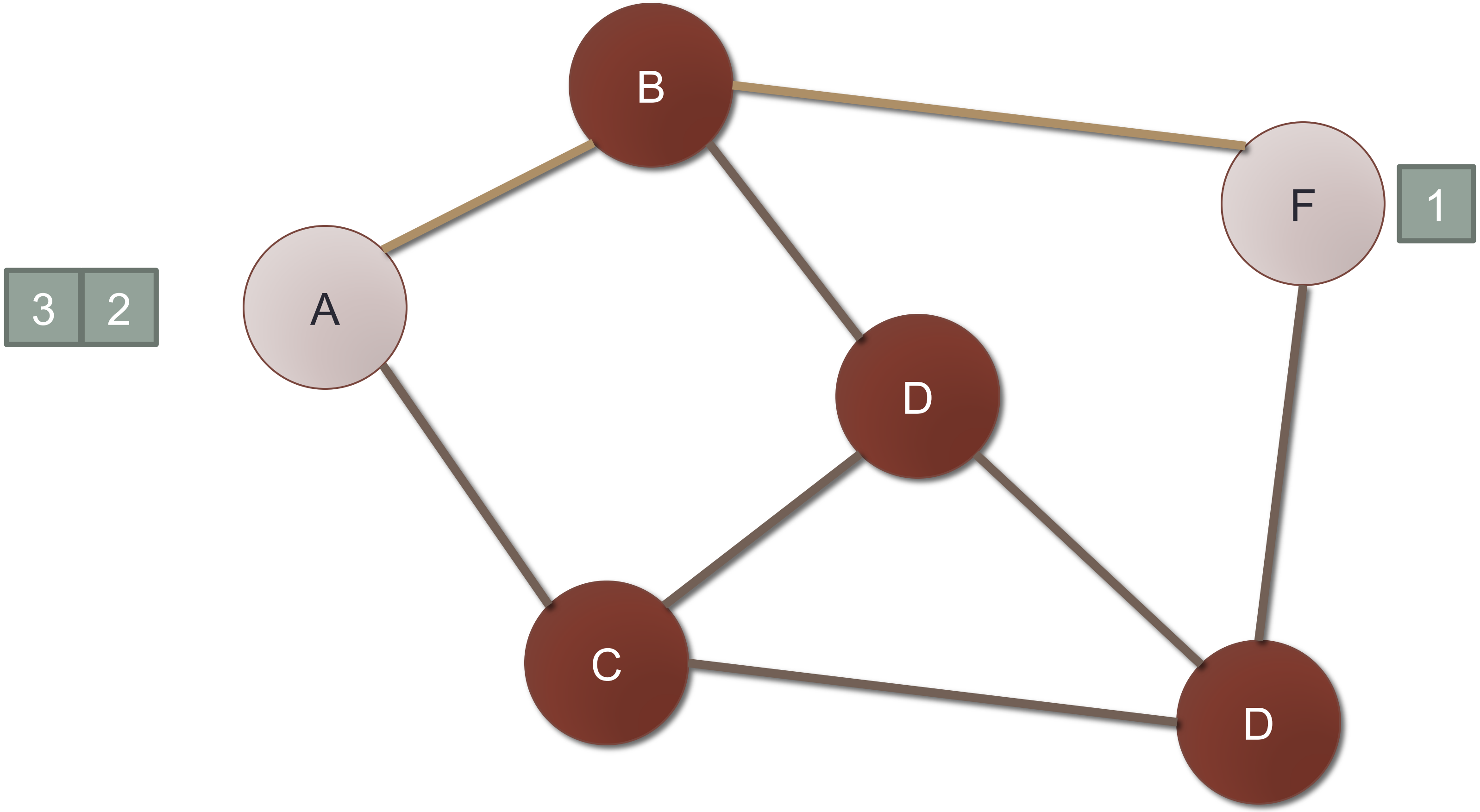


https://slideplayer.com/slide/8097672/

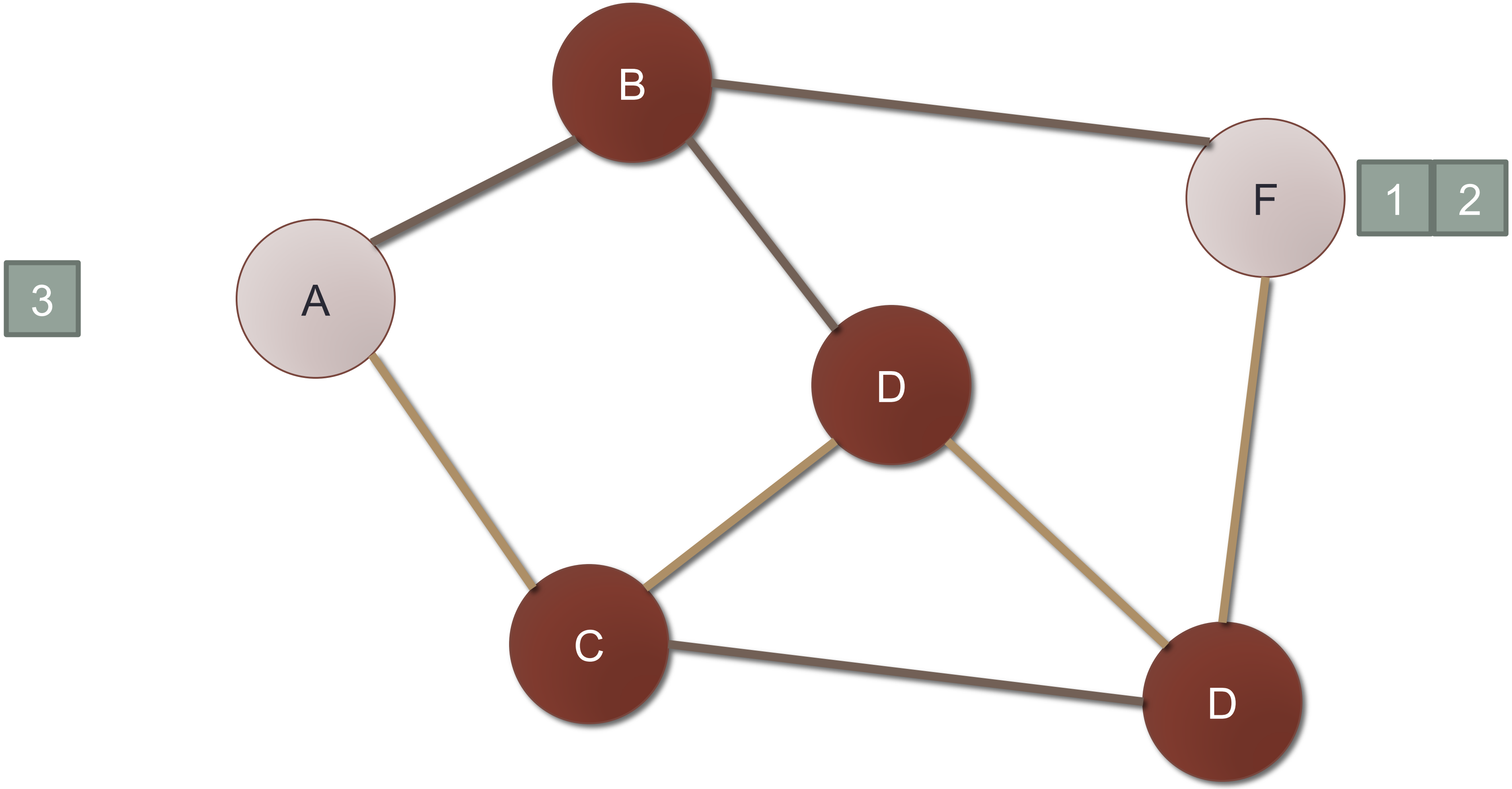
Packet Switching



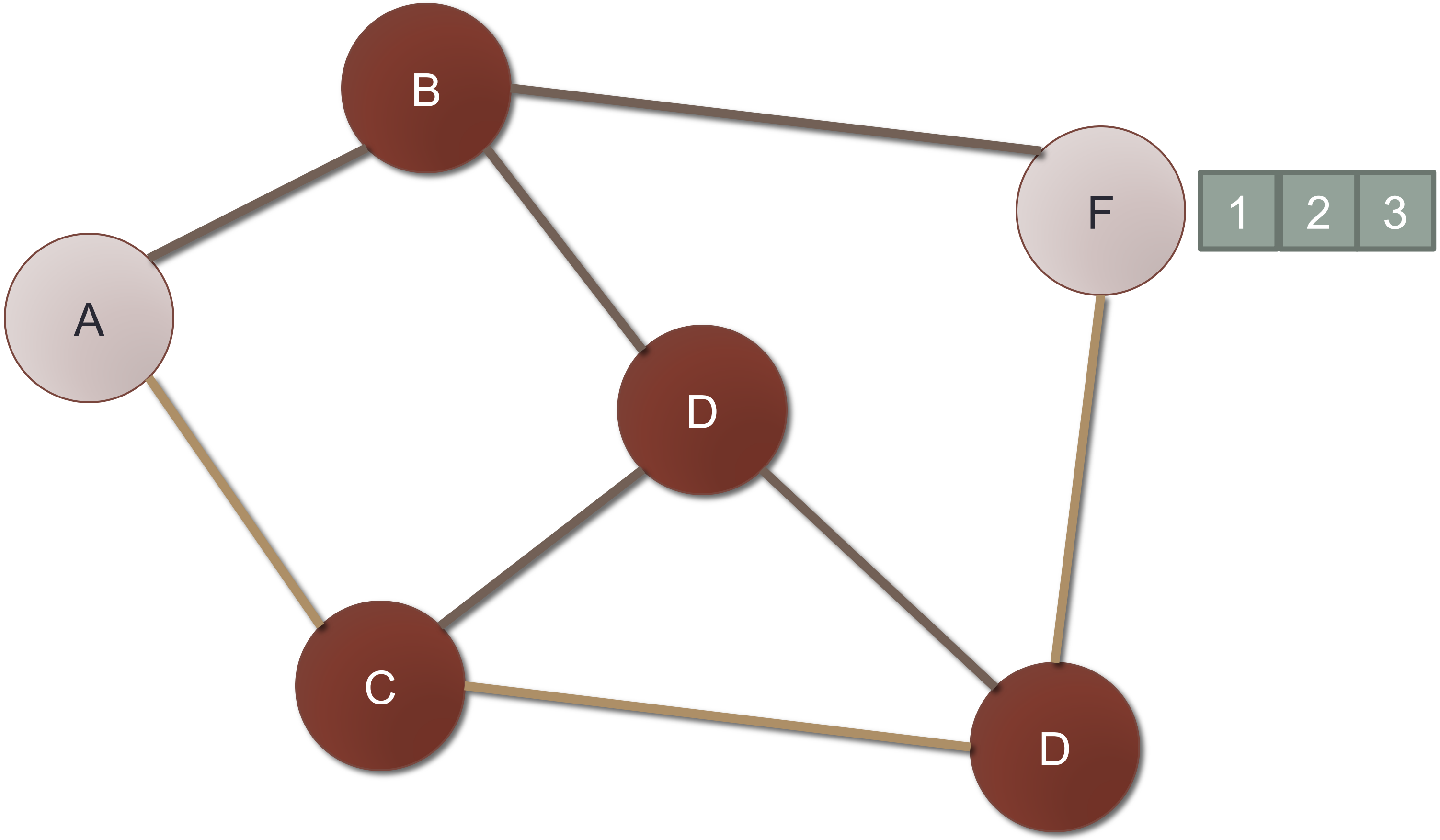
Packet Switching



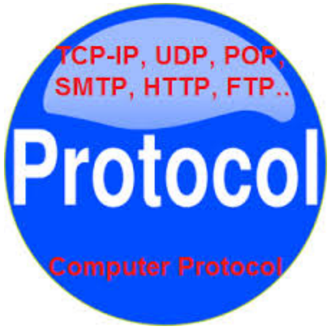
Packet Switching



Packet Switching



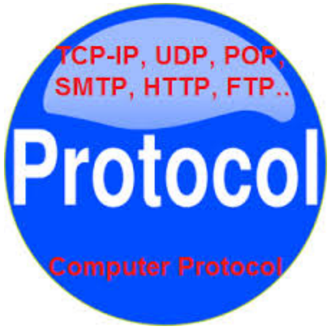
Protocols



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

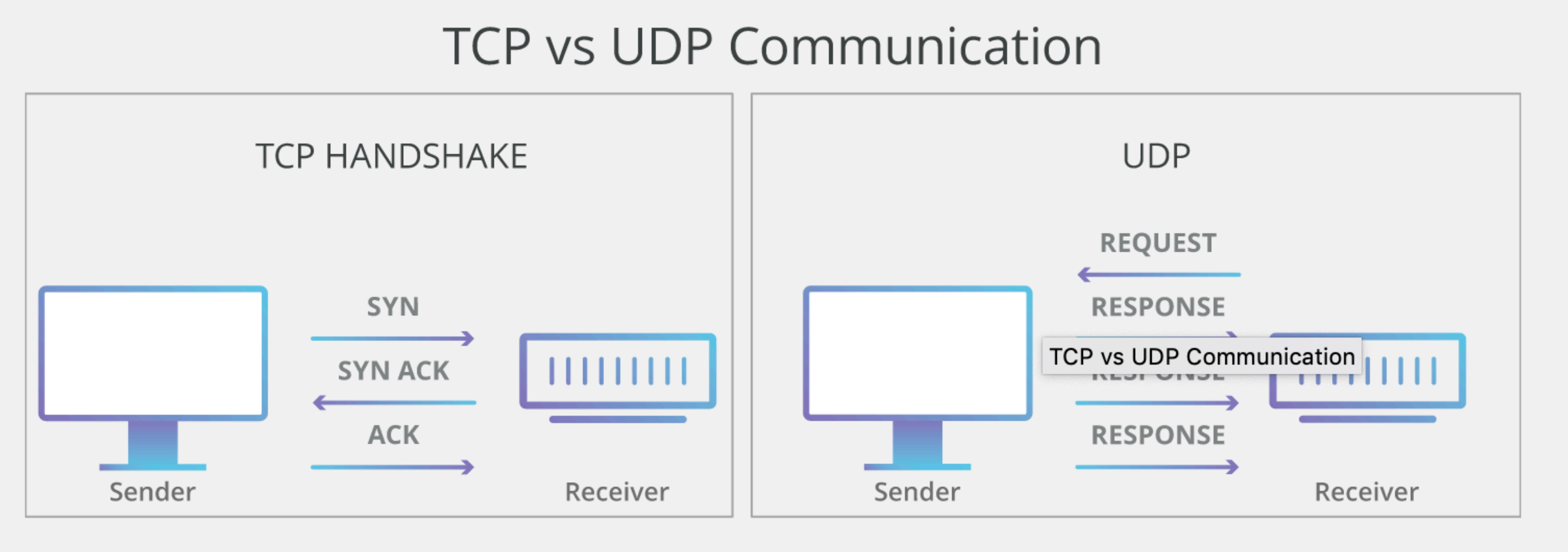
http://www.hinditechy.com/what-is-protocol-in-networking-hindi/

Protocols



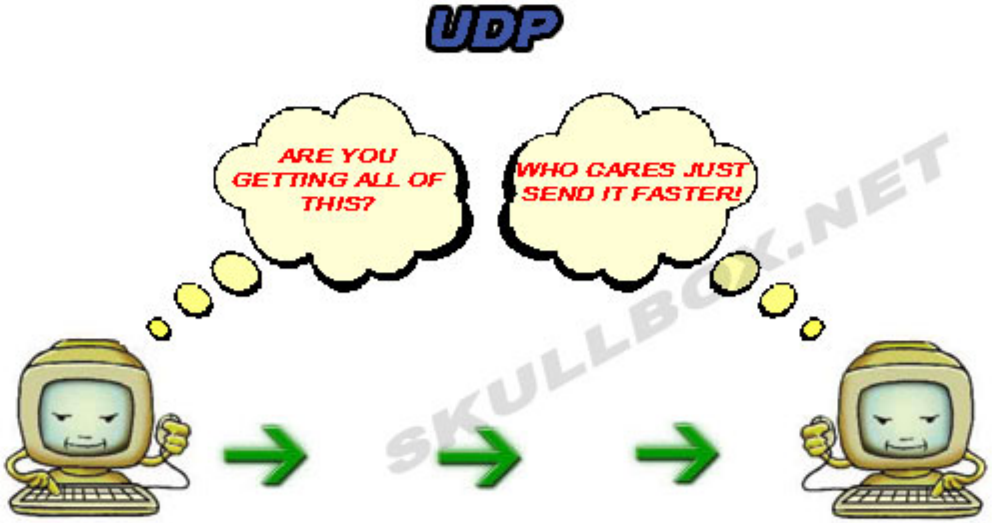
- Connectionless protocol
  - Sends data out as soon as there is enough data to be transmitted
  - E.g., user datagram protocol (UDP)
- Connection-oriented protocol
  - Provides a reliable connection stream between two nodes
  - Consists of set up, transmission, and tear down phases
  - Creates virtual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

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



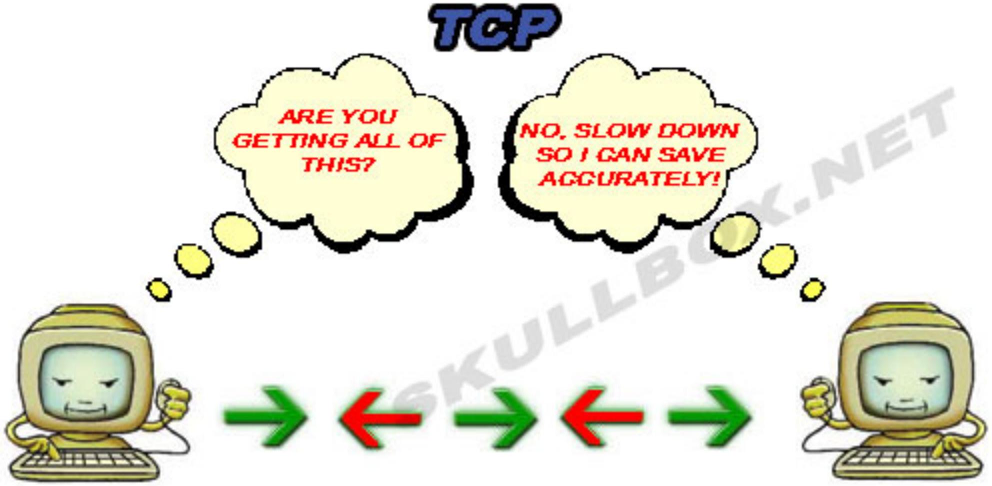
https://www.cloudflare.com/learning/ddos/glossary/user-datagram-protocol-udp/

Connectionless protocol



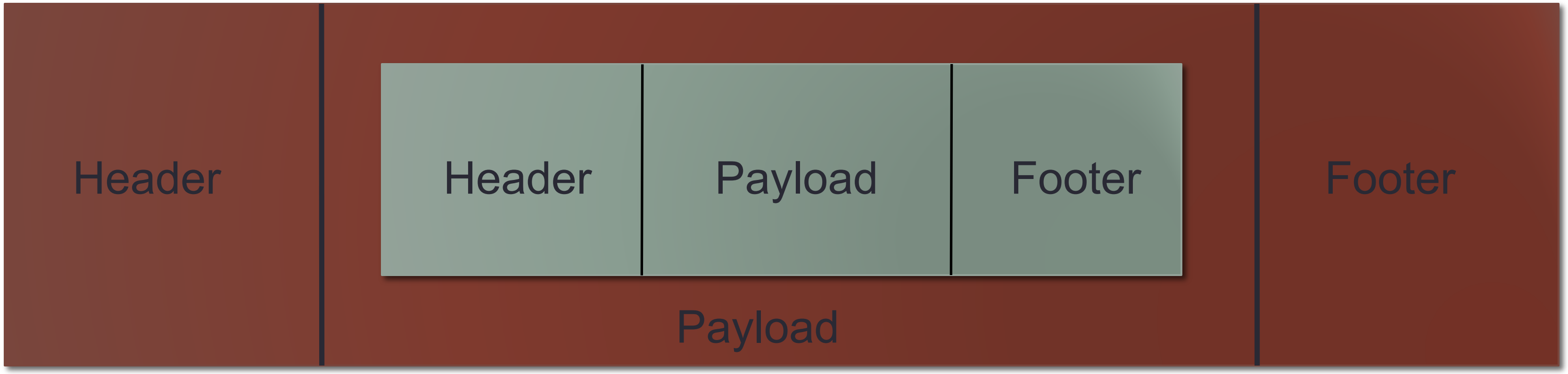
https://www.b4x.com/android/forum/threads/question-about-two-way-communication-using-udp.17316/

Connection-oriented protocol


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

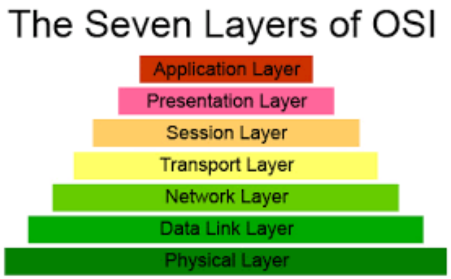
Encapsulation

- 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



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

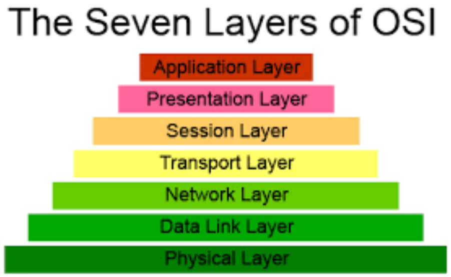
Network Layers



- 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/

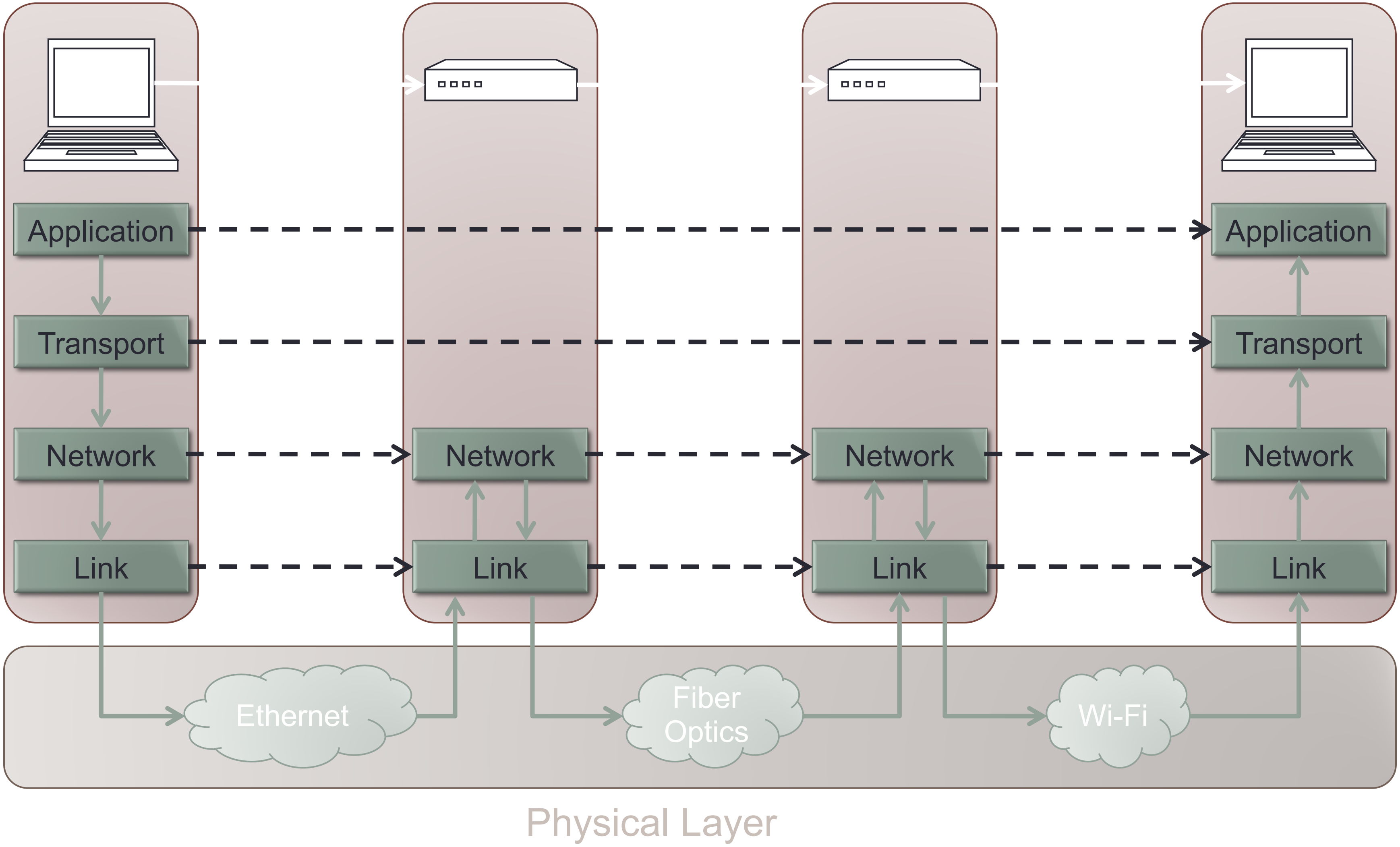
Network Layers



- 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/

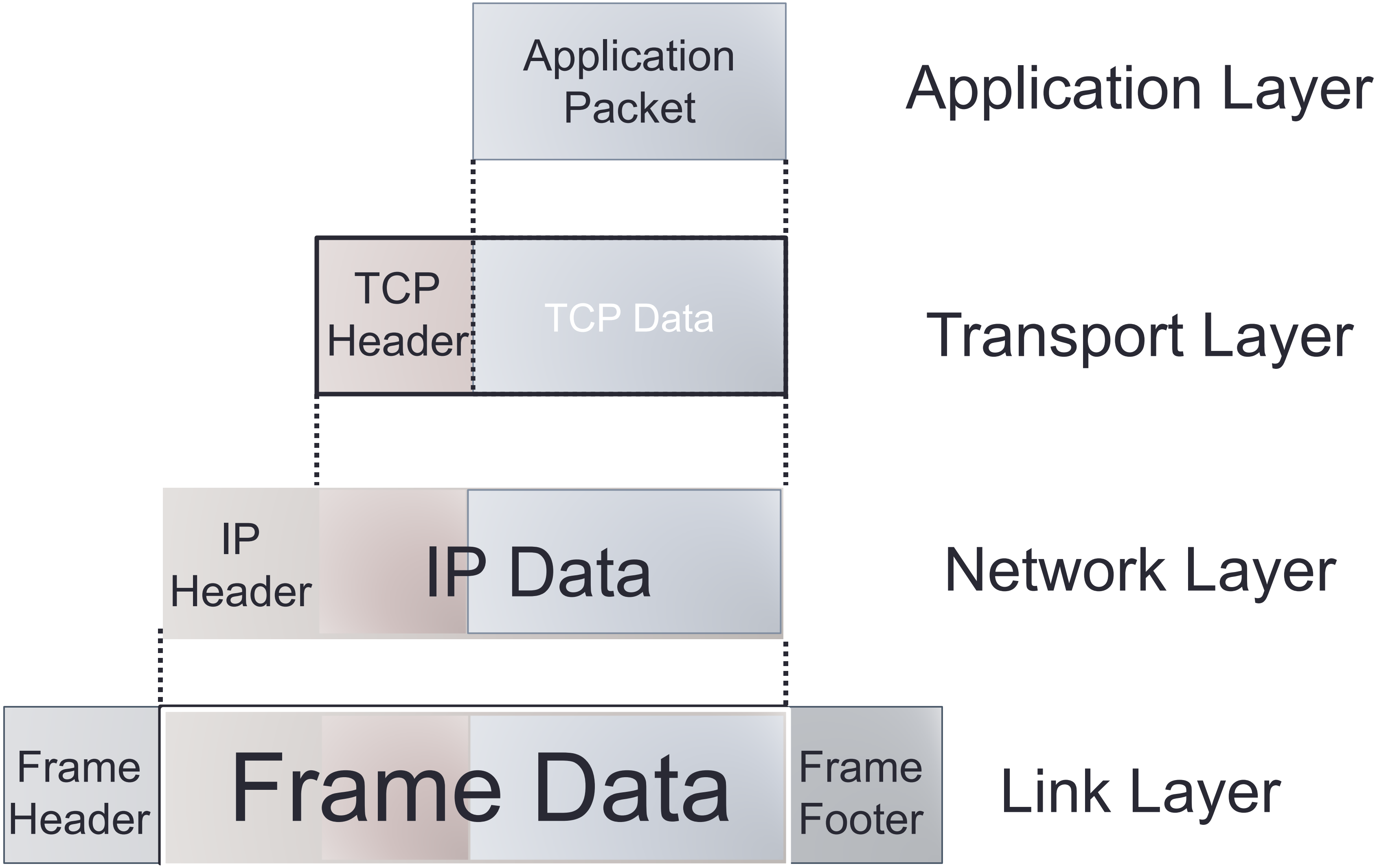
Internet Layers – TCP/IP model



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



Application Packet

Application Layer

TCP Header

TCP Data

Transport Layer

IP Header

IP Data

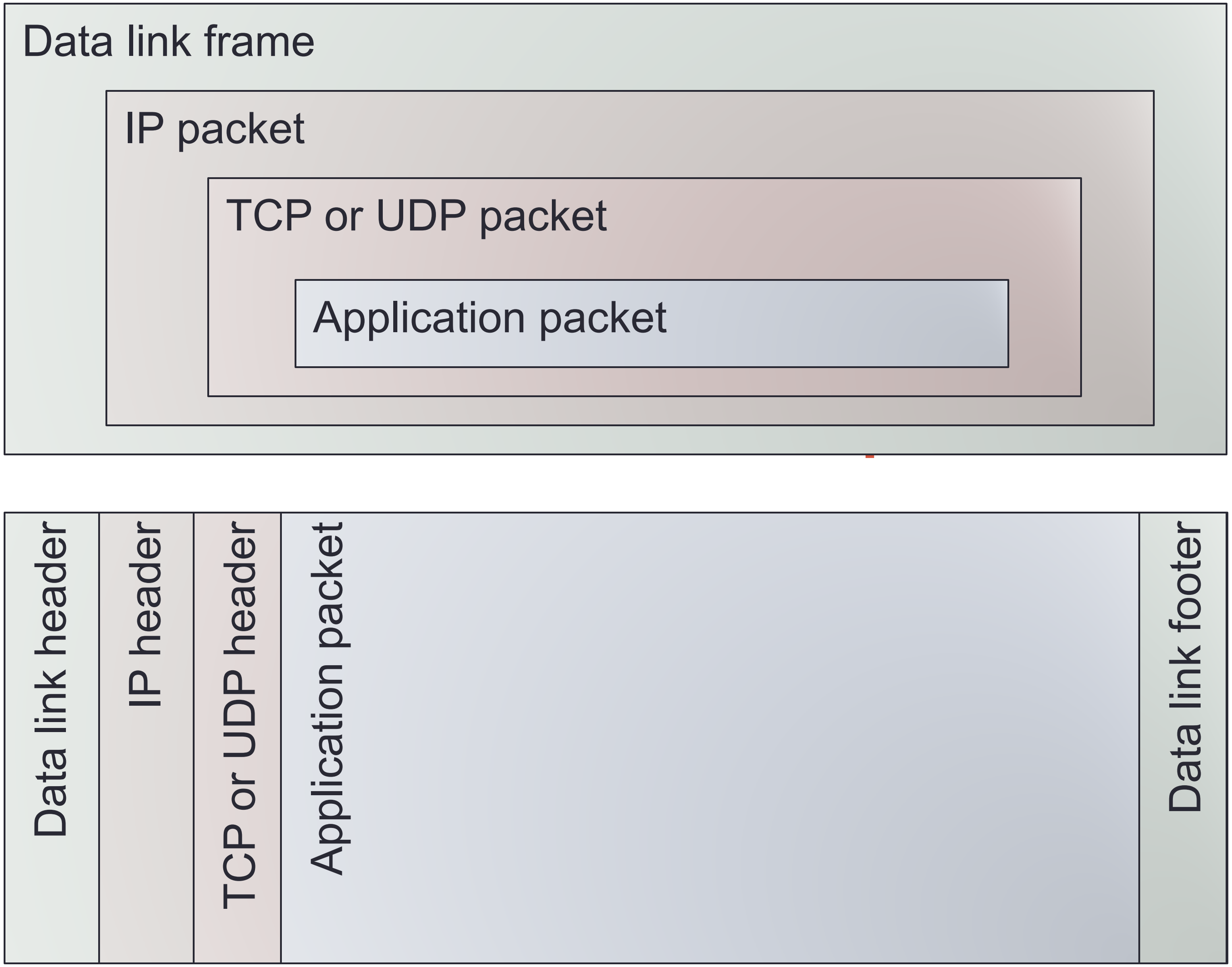
Network Layer

Frame Header

Frame Data

Frame Footer

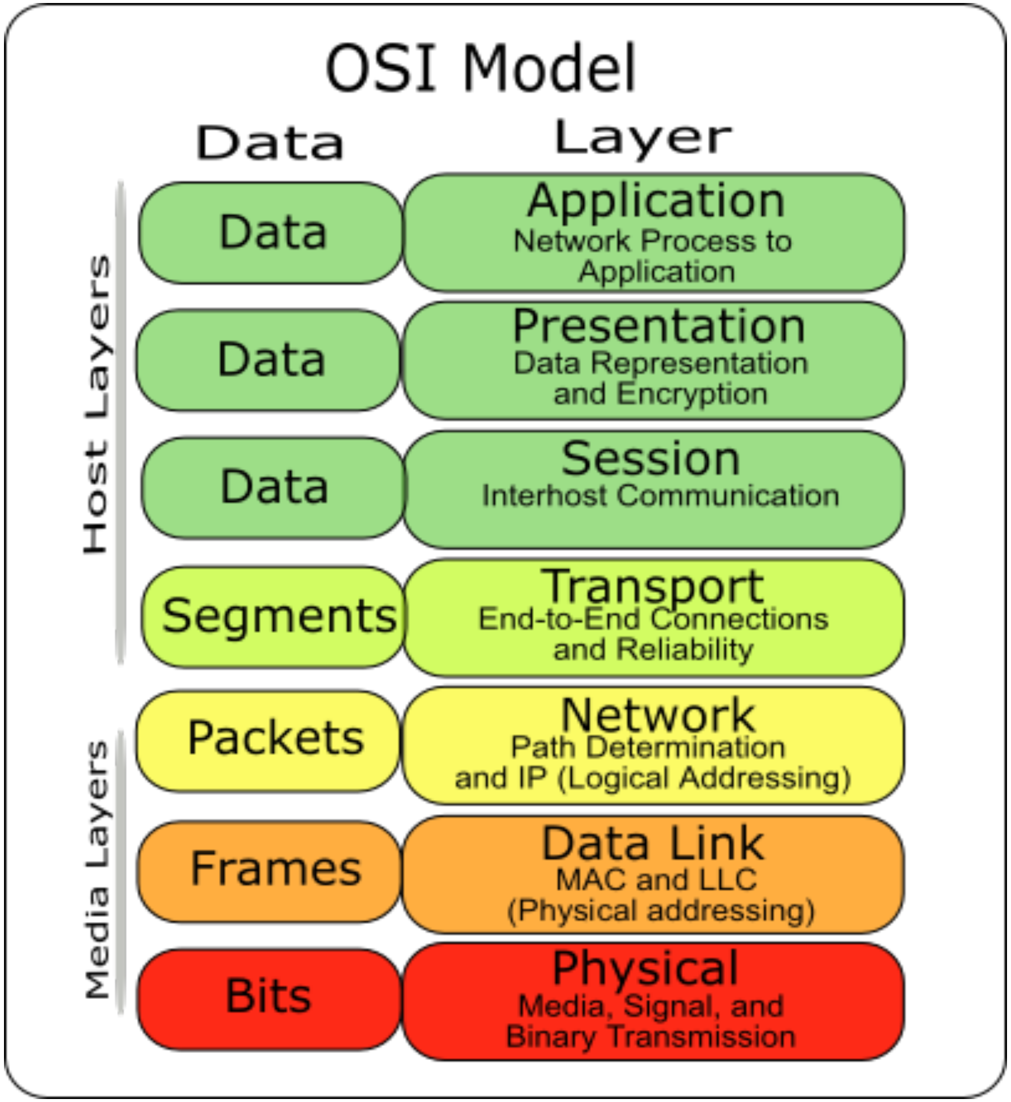
Link Layer



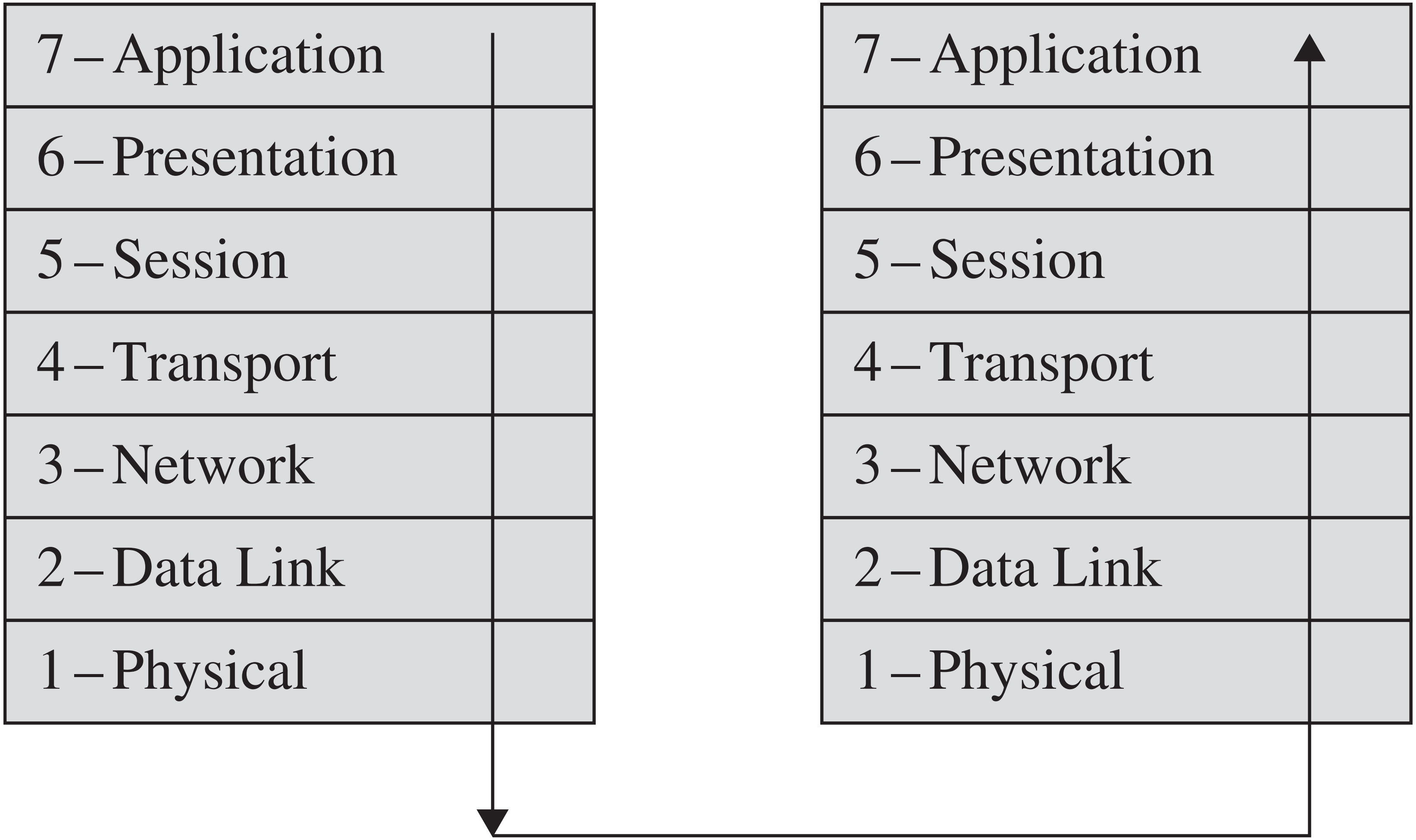
From *Security in Computing, Fifth Edition*, by Charles P. Pfleeger, et al. (ISBN: 9780134085043). Copyright 2015 by Pearson Education, Inc. All rights reserved.

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

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

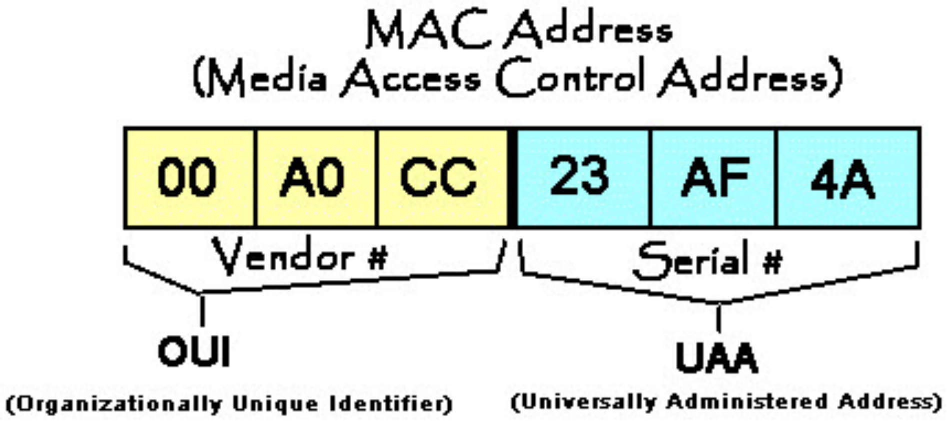
MAC Addresses

- 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

MAC Addresses

- Most OSs allow you to specify an arbitrary MAC for an interface
  - Despite the IEEE limitations on LAAs,

MAC Address



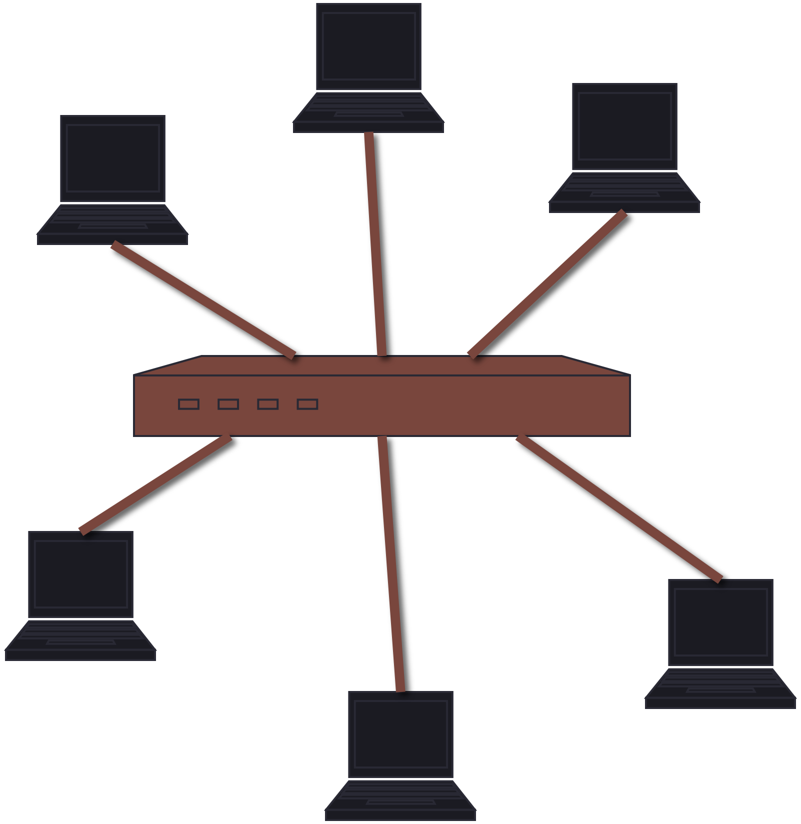
MAC Address
(Media Access Control Address)
Vendor #
Serial #
OUI
(Organizationally Unique Identifier)
UAA
(Universally Administered Address)

00	A0	CC	23	AF	4A

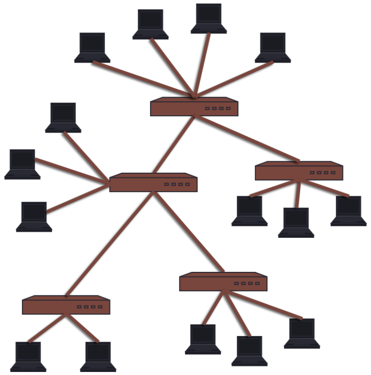
http://www.thewindowsclub.com/change-mac-address-in-windows

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

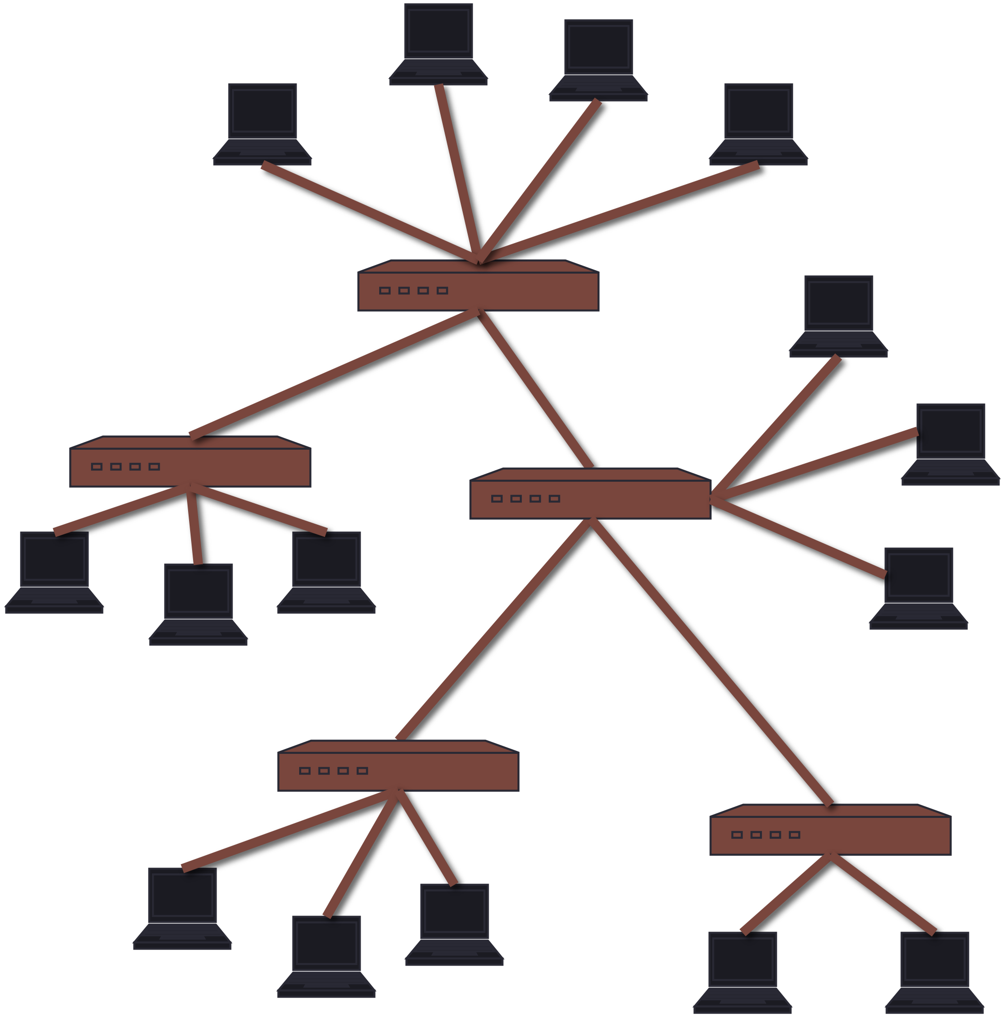


Combining Switches



- 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

- Questions?