Cyber Security

5. Network Security I

Contents

1. Network Security Concepts
2. The Link Layer
3. The Network Layer
4. The Transport Layer
5. Denial-of-Service Attacks

1. Network Security Concepts

1.1 Network Topology

1.2 Internet Protocol Layers

1.3 Network Security Issues

1. Network Security Concepts

- The Internet was designed so that communication occurs through sequences of data packets.

- A data packet is a finite-length set of bits, which is divided into two parts.

  - A header : specifies where the packet is going and contains various overhead and bookkeeping details

  - A payload : is the actual information that is being communicated

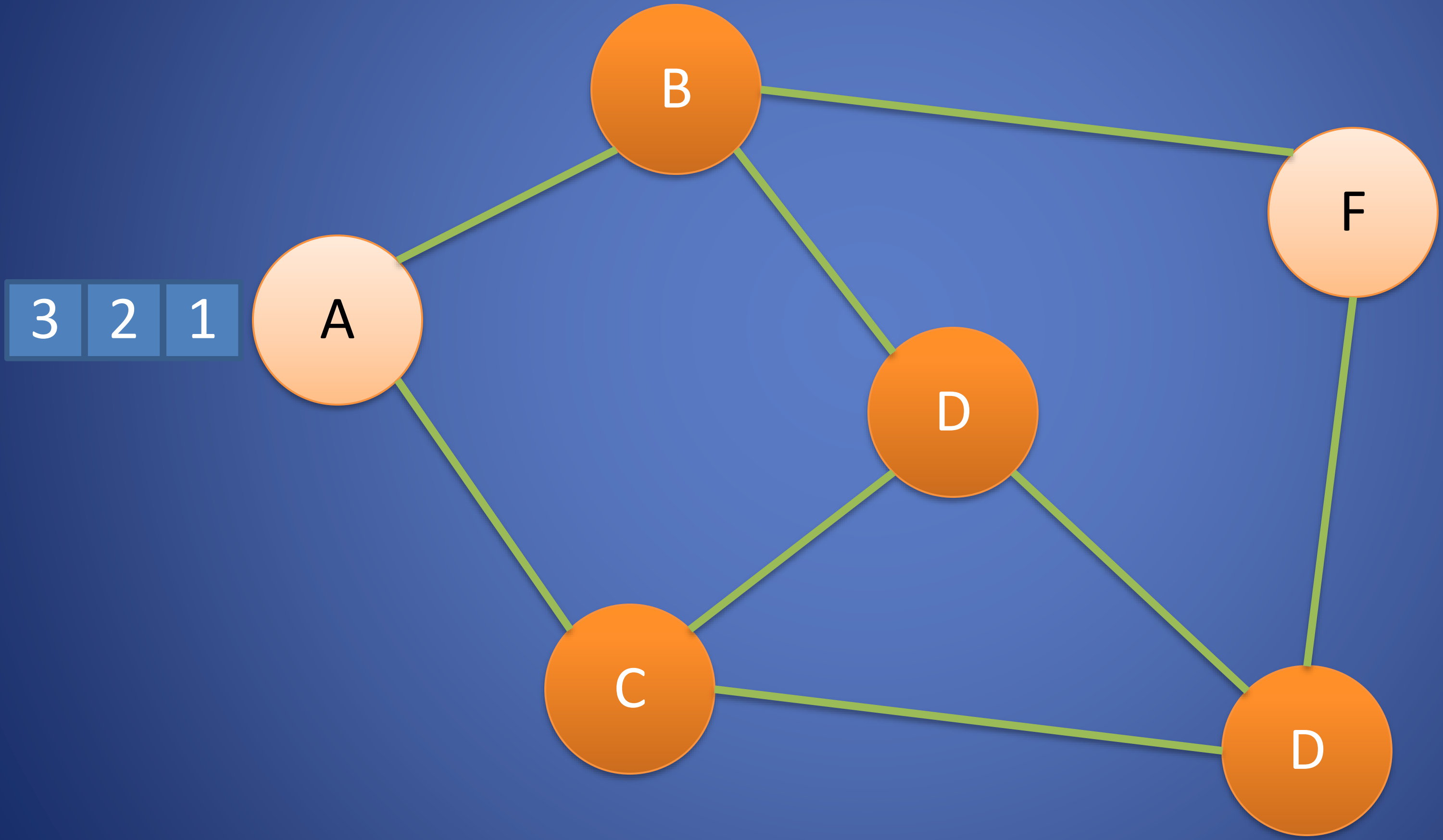
- So if two entities wish to communicate using the Internet, they must chop their messages into packets, attach a header on the front of each one, and then have those packets find their way through the Internet to reach their respective destinations.

Circuit and Packet Switching

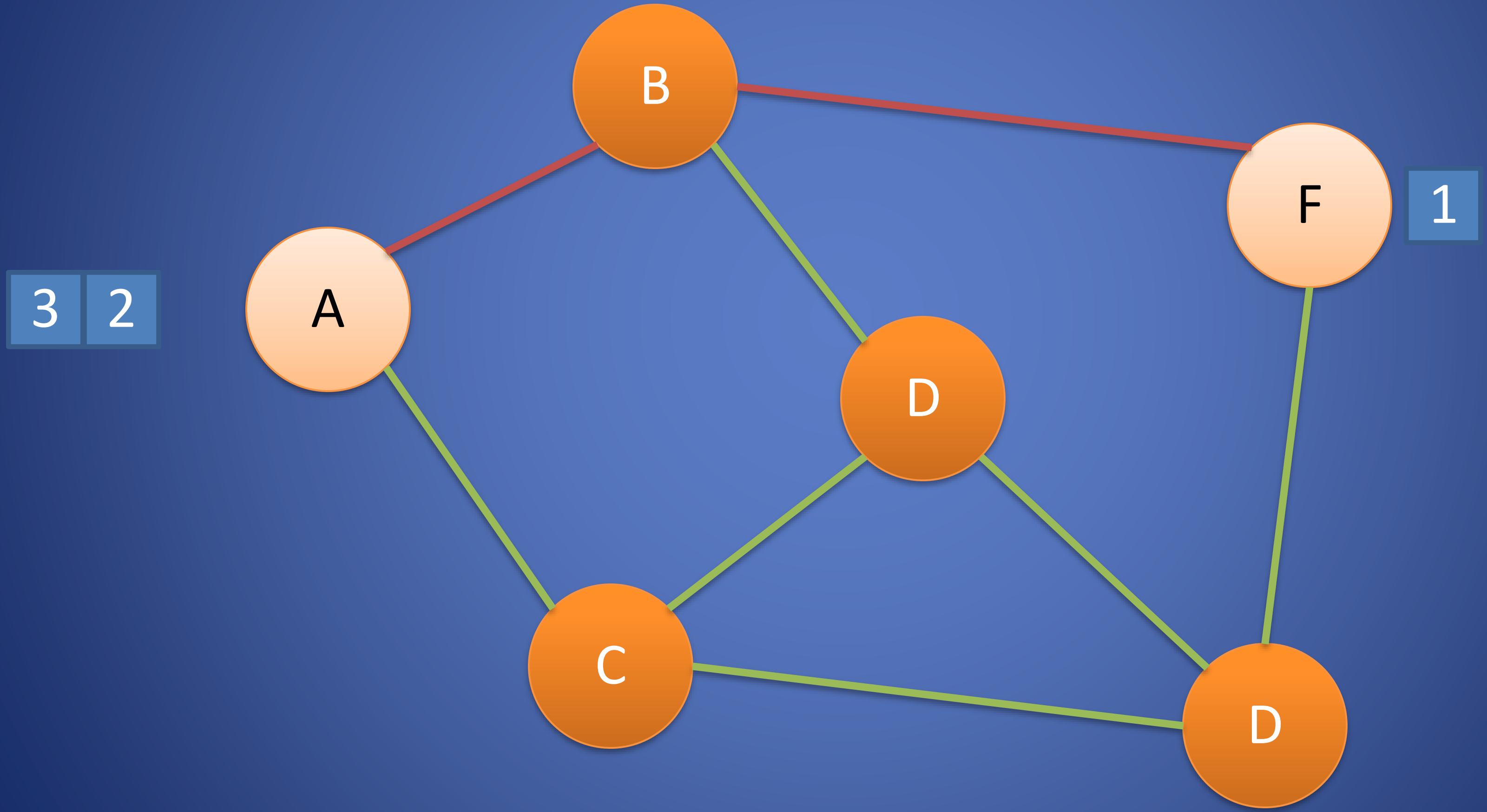
- Circuit switching
  - Legacy phone network
  - Single route through sequence of hardware devices established when two nodes start communication
  - Data sent along route
  - Route maintained until communication ends

- 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

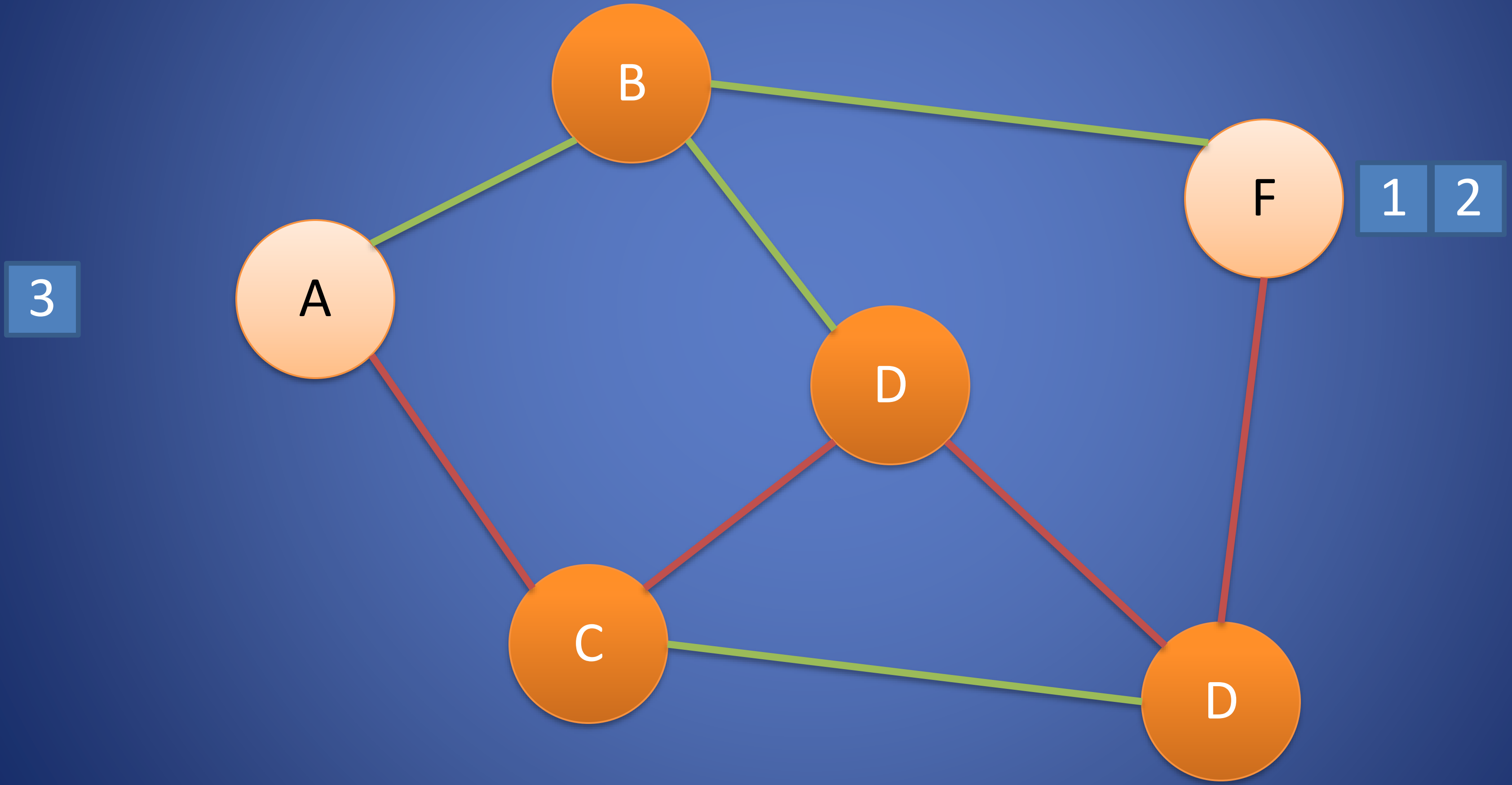
Packet Switching



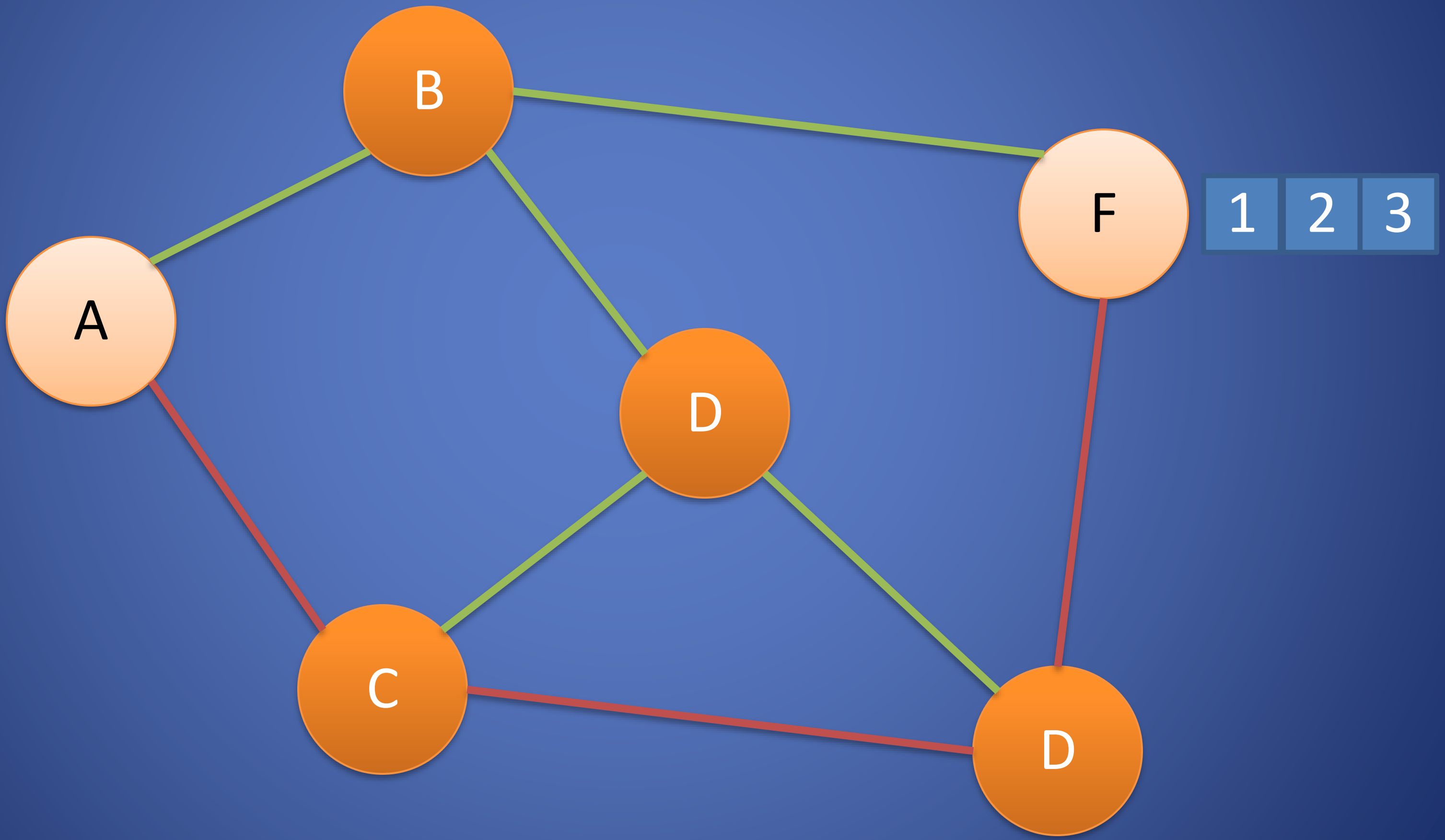
Packet Switching



Packet Switching



Packet Switching



1.1 Network Topology

- A network's connection structure is known as its network topology.

- The computers in a network are host nodes that can be sources and destinations of messages, and the routers in the network are communication nodes through which messages flow.

- Local Area Network(LAN) : a private network composed of computers in relatively close proximity to each other
- Wide Area Network(WAN) : composed of many machines and smaller networks spread out over great distances. (ex. Internet)

- The routers in WANs on the internet are partitioned into clusters, which are called autonomous systems(ASs). Each AS is controlled by a single organizational entity, which determines how packets will be routed among the nodes in that AS.

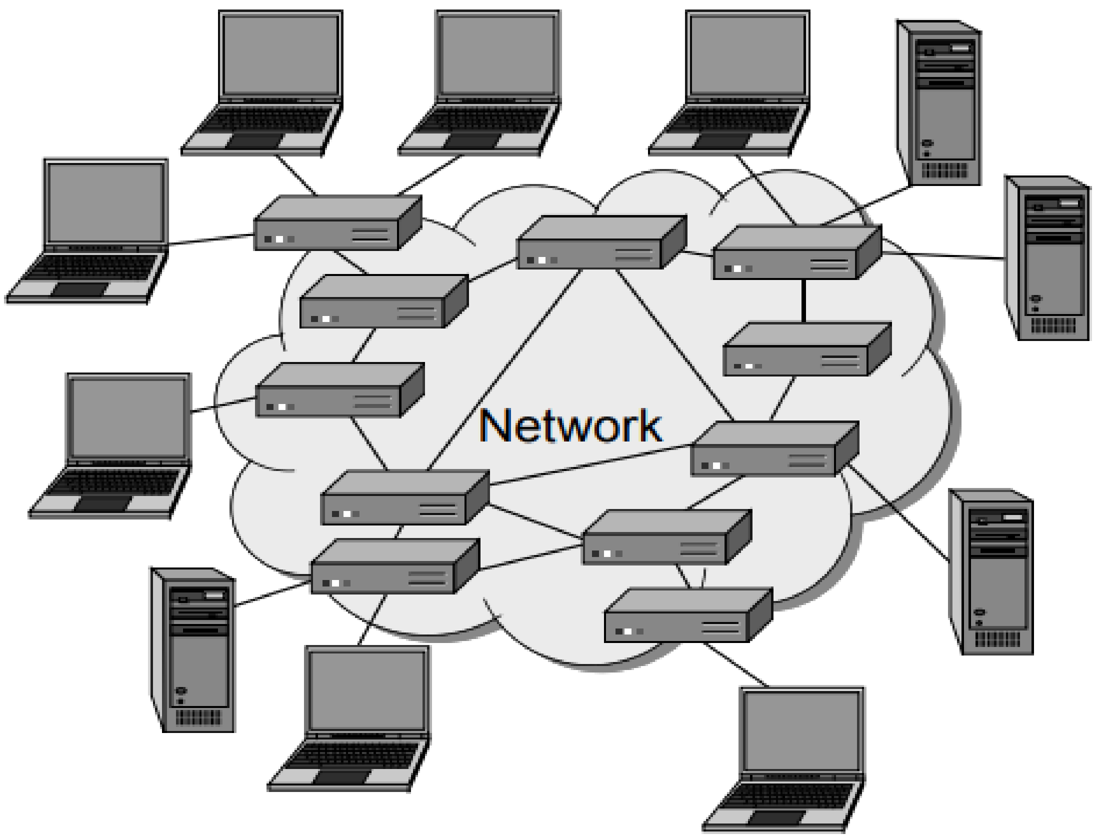


Figure 1: A computer network composed of host nodes (shown as computers on the periphery) and communication nodes (shown as routers in the interior).

1.2 Internet Protocol Layers

- The architecture of the Internet is modeled conceptually as being partitioned into layers, which collectively are called the Internet protocol stack.

- Each layer provides a set of services and functionality guarantees for higher layers and, to the extent possible, each layer does not depend on details or services from higher levels.

- The interface each layer provides to higher levels is designed to provide only the essential information from this layer that is needed by the higher levels—lower-level details are hidden from the higher levels.

Five Conceptual Layers for Internet Communication (1)

1. Physical layer. The task of the physical layer is to move the actual bits between the nodes of the network, on a best effort basis.
2. Link layer. The task of the link layer is to transfer data between a pair of network nodes or between nodes in a local-area network and to detect errors that occur at the physical layer.
3. Network layer. The task of the network layer, which is also known as the Internet layer for the Internet, is to provide for the moving of packets between any two hosts, on a best effort basis.
4. Transport layer. The task of the transport layer is to support communication and connections between applications, based on IP addresses and ports, which are 16-bit addresses for application-level protocols to use.
5. Application layer. The task of the application layer is to provide protocols that support useful functions on the Internet, based on the services provided by the transport layer.

Five Conceptual Layers for Internet Communication (2)

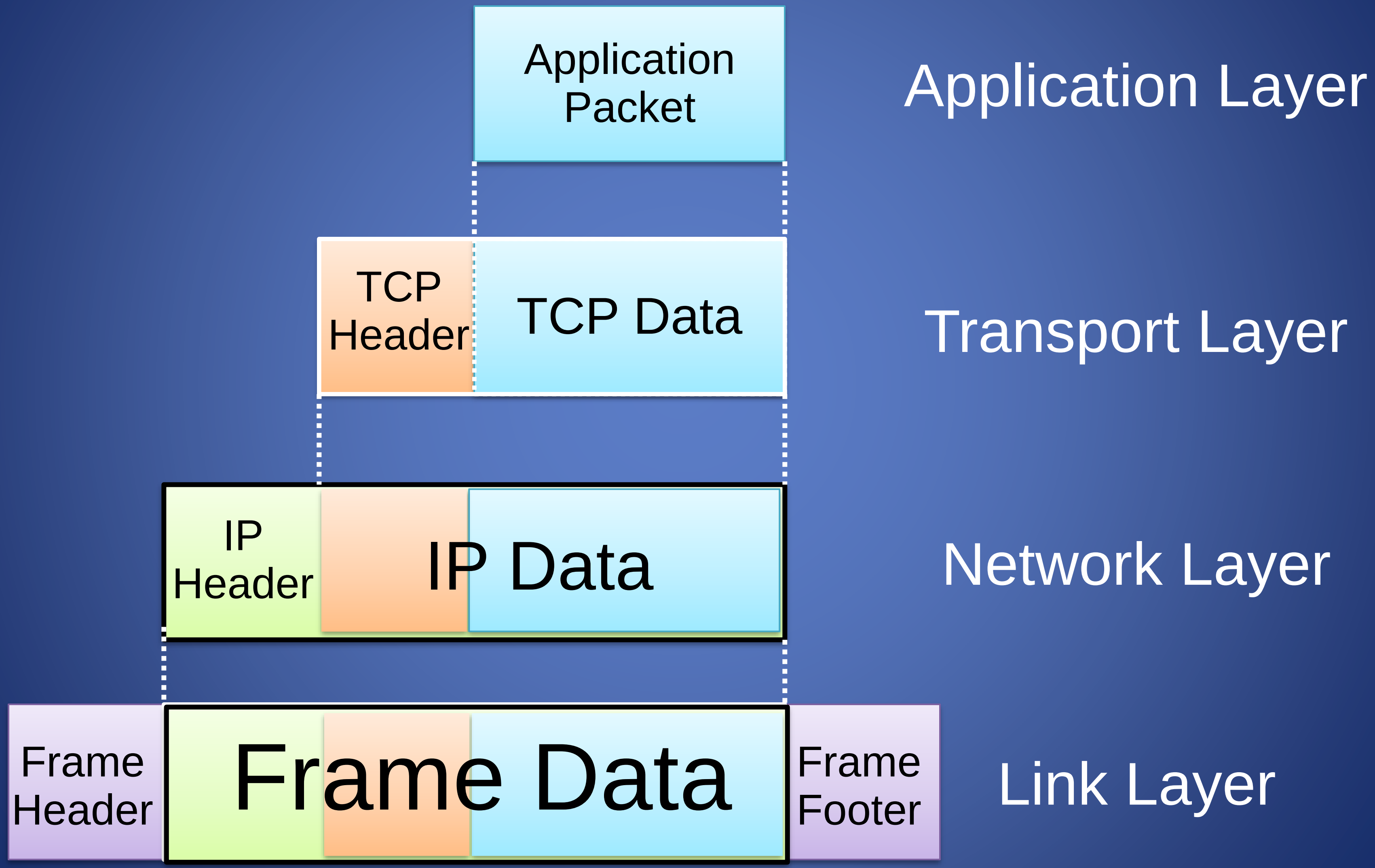
- The Open Systems Interconnection (OSI) model differs slightly from that above, in that it has seven layers, as the application layer is divided into a strict application layer, for host application-to-network processes, a presentation layer, for data representation, and session layer, for interhost communication.

- A packet for a given layer in this model consists of the data to be transmitted plus metadata providing routing and control information.

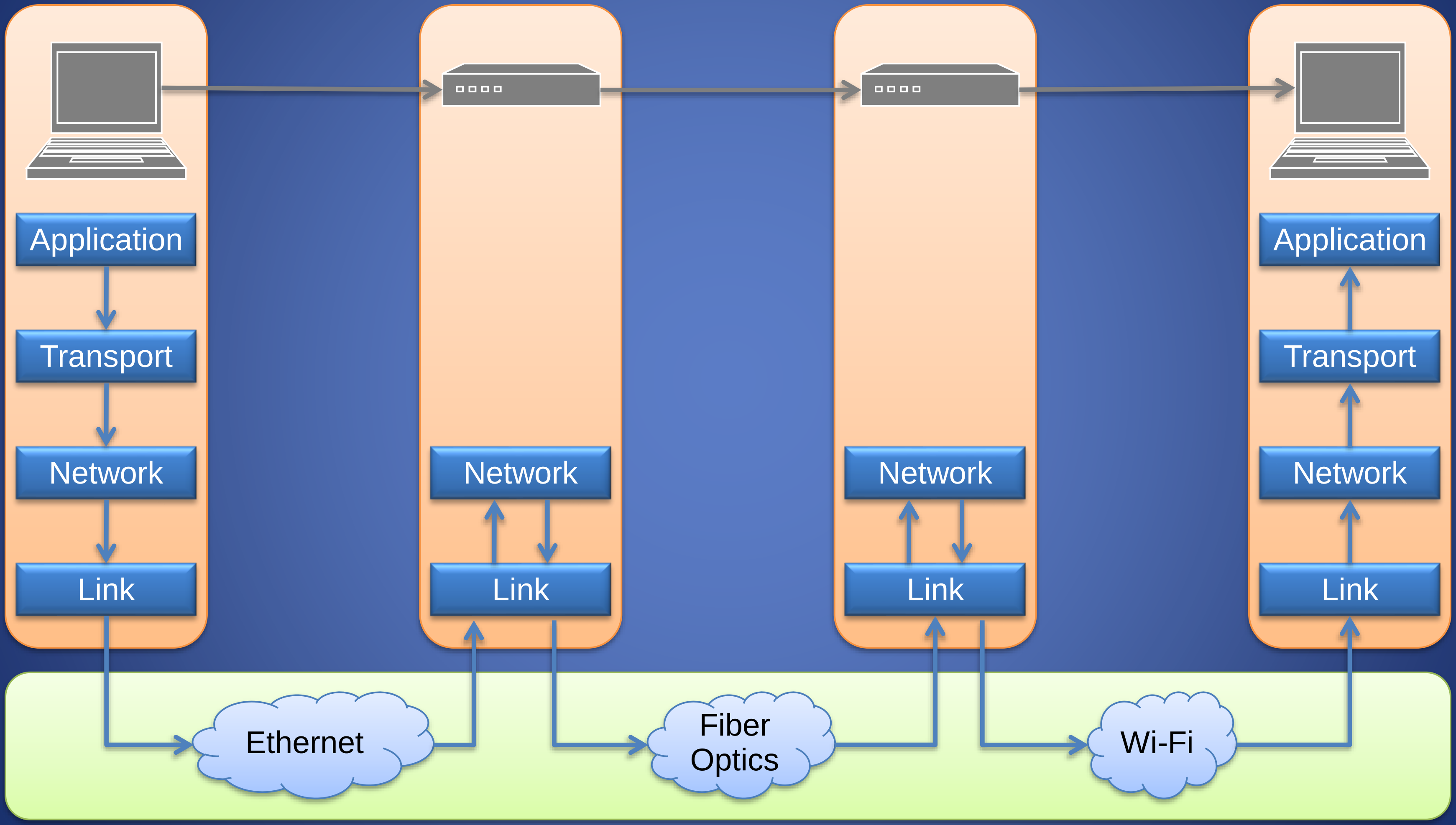
- The metadata is stored in the initial portion of the packet, called header and sometimes also in the final portion of the packet, called footer.

- The data portion of the packet is referred to as the payload. For all but the topmost layer, the payload stores a packet of the layer immediately above. This nesting of packets is called encapsulation.

Internet Packet Encapsulation



Internet Layers



Application

Transport

Network

Link

Network

Link

Network

Link

Application

Transport

Network

Link

Ethernet

Fiber Optics

Wi-Fi

Physical Layer

1.3 Network Security Issues

- Confidentiality : Standard protocols for each layer don’t encrypt the contents of either their headers or their data.
- Integrity : The headers and footers that encapsulate data packets have, at each layer, simple checksums to validate the integrity of data and/or header contents.
- Availability : A challenge for any network object that needs to be available on a 24/7 basis
- Assurance : If we want to introduce permissions and policies that control how data flows in a network, these have to be implemented as explicit additions.
- Authenticity : In the Internet Protocol stack, there is no notion of user identities.
- Anonymity : Since there is no default notion of identity of users of
- the Internet, it has a built-in anonymity.

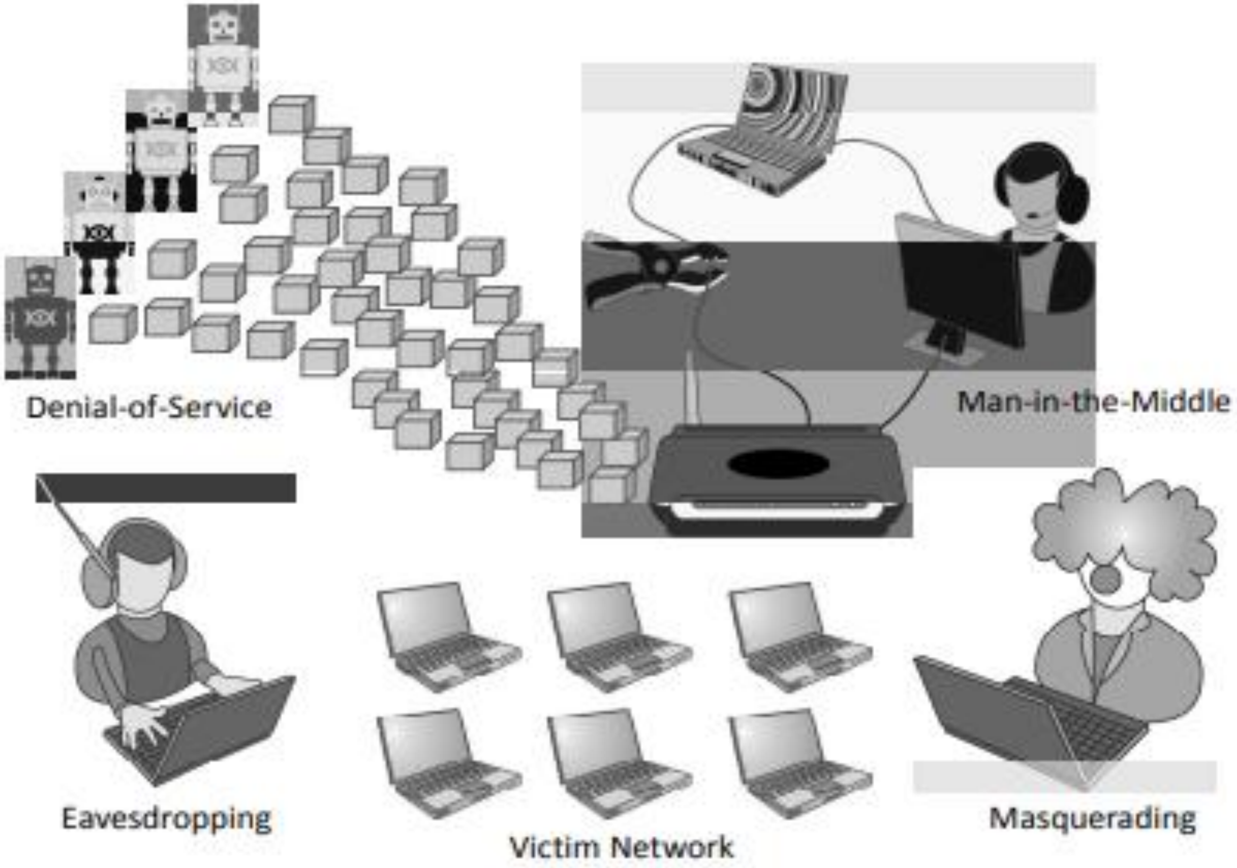


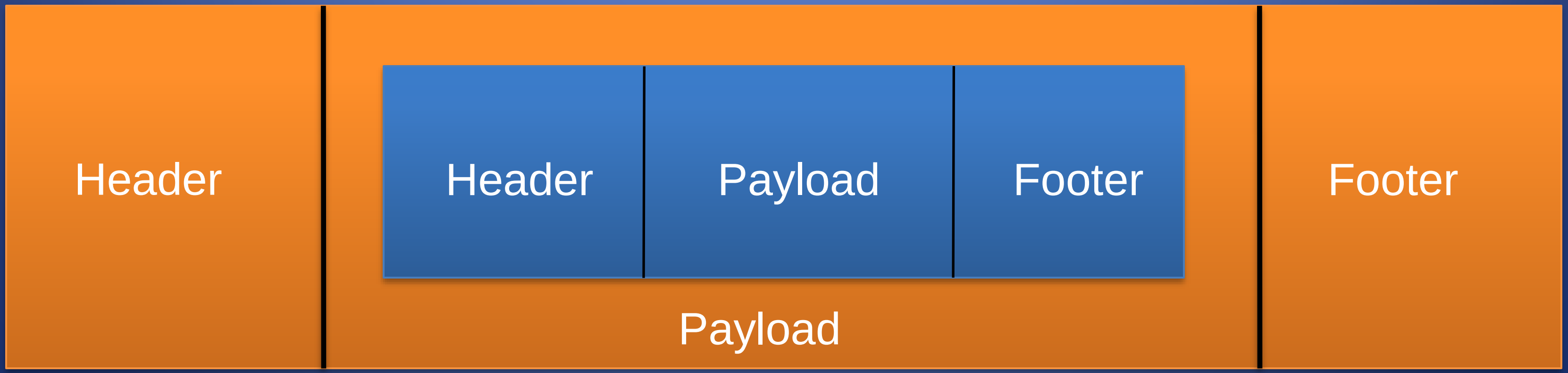
Figure 4: Some network-based attacks.

Protocols

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

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



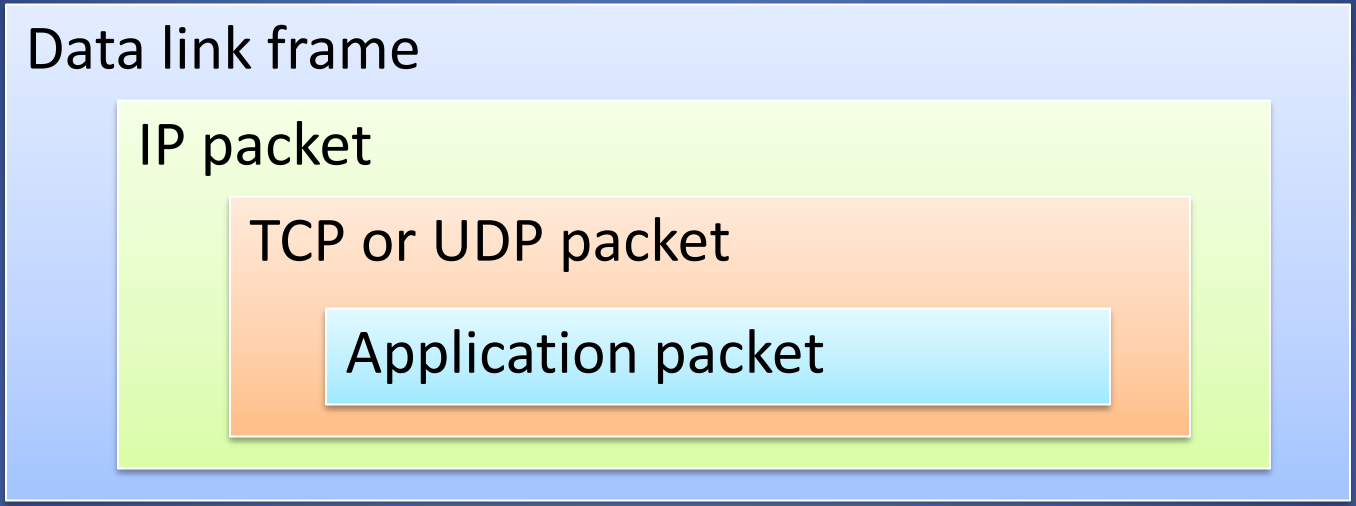
Network Layers

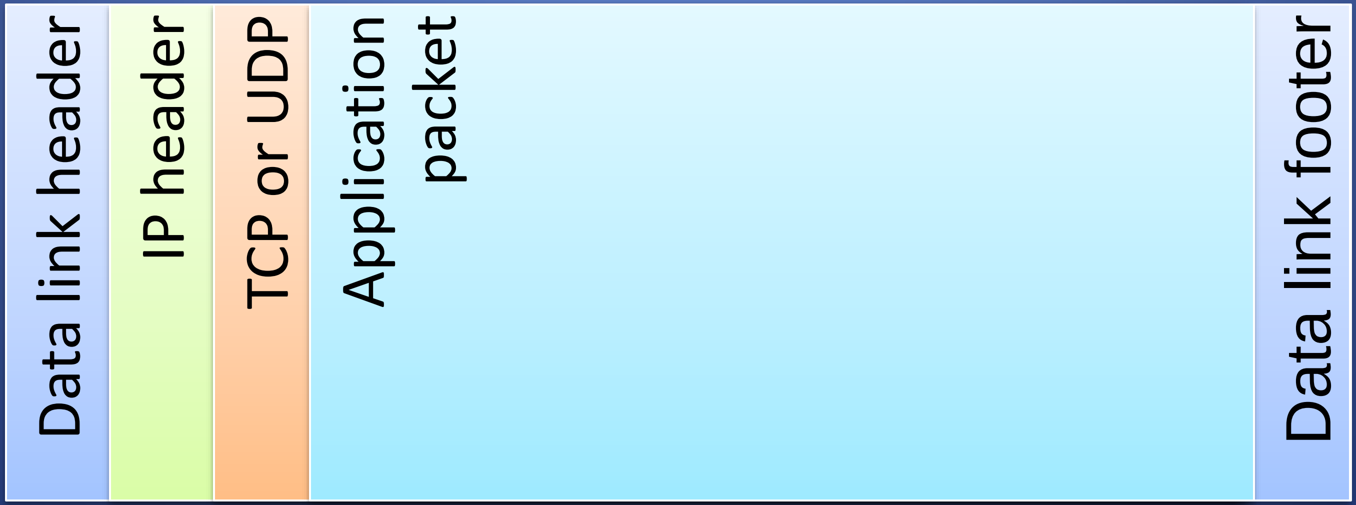
- Network models typically use a stack of layers
  - Higher layers use the services of lower layers via encapsulation
  - A layer can be implemented in hardware or software
  - The bottommost layer must be in hardware
- A network device may implement several layers
- A communication channel between two nodes is established for each layer
  - Actual channel at the bottom layer
  - Virtual channel at higher layers

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)

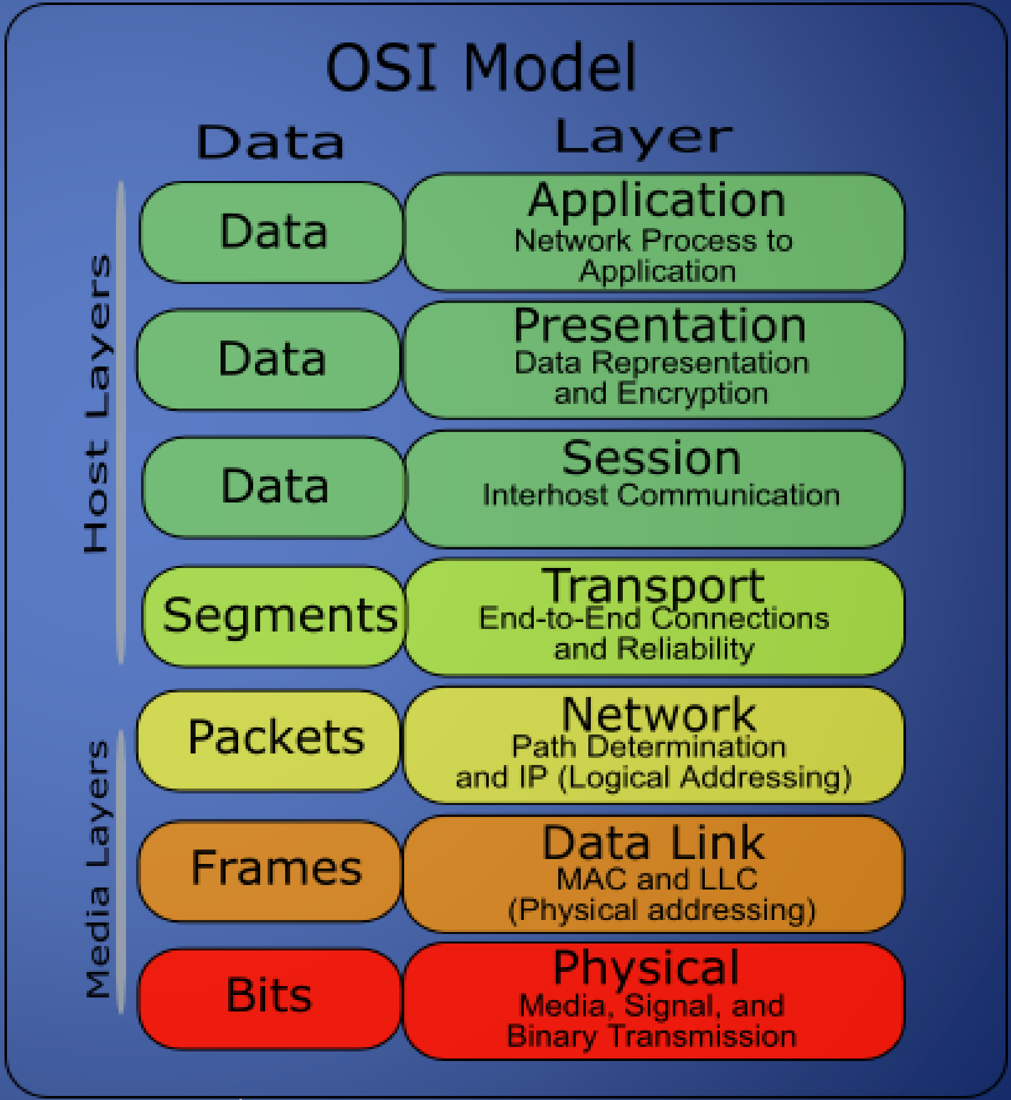
Internet Packet Encapsulation





The OSI Model

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



OSI Model

	Data	Layer
Host 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
Media Layers	Packets	Network Path Determination and IP (Logical Addressing)
	Frames	Data Link MAC and LLC (Physical addressing)
	Bits	Physical Media, Signal, and Binary Transmission