Outline

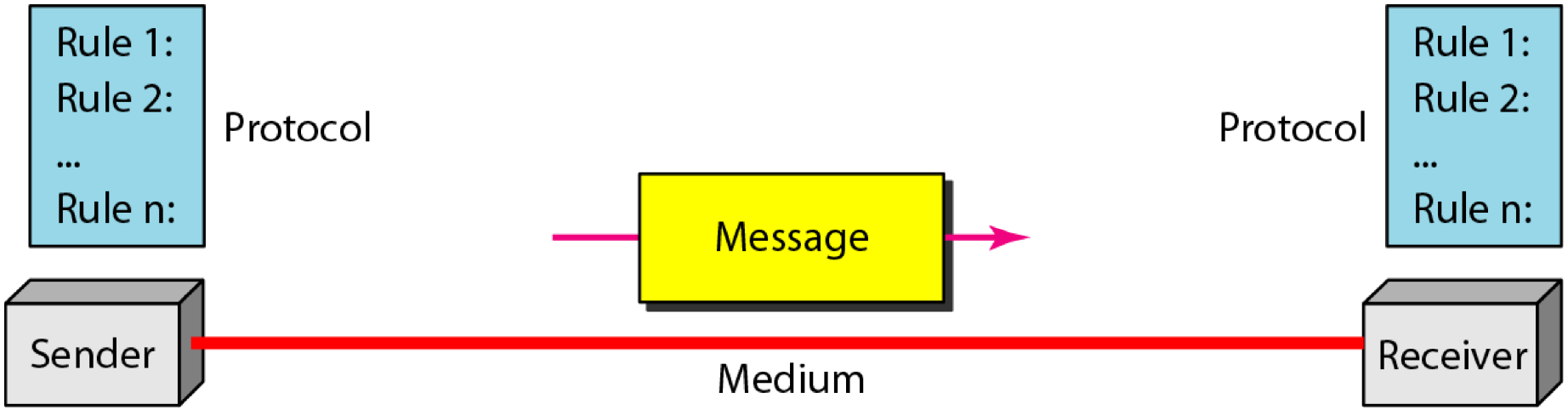
- Basics of Computer Networks
- Network Security

Data Communications

- The term telecommunication means communication at a distance. The word data refers to information presented in whatever form is agreed upon by the parties creating and using the data.

- Data communications are the exchange of data between two devices via some form of transmission medium such as a wire cable or wireless.

Components


Rule 1:
Rule 2:
...
Rule n:
Protocol
Message
Protocol
Rule 1:
Rule 2:
...
Rule n:
Sender
Medium
Receiver

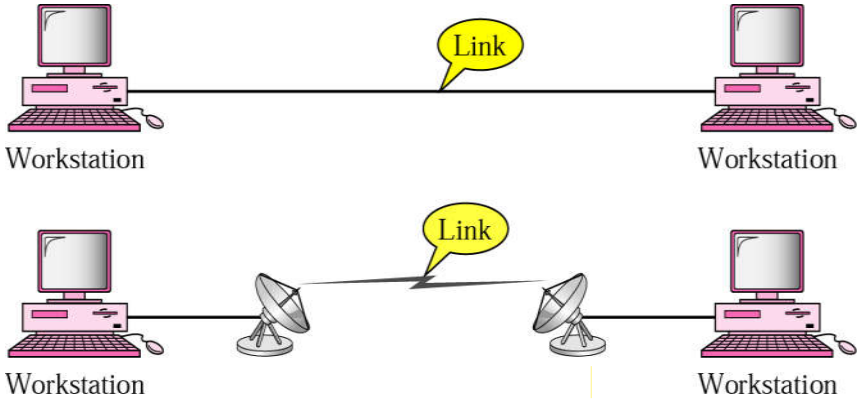
Computer Networks

- A network is a set of devices (nodes) connected by communication links.

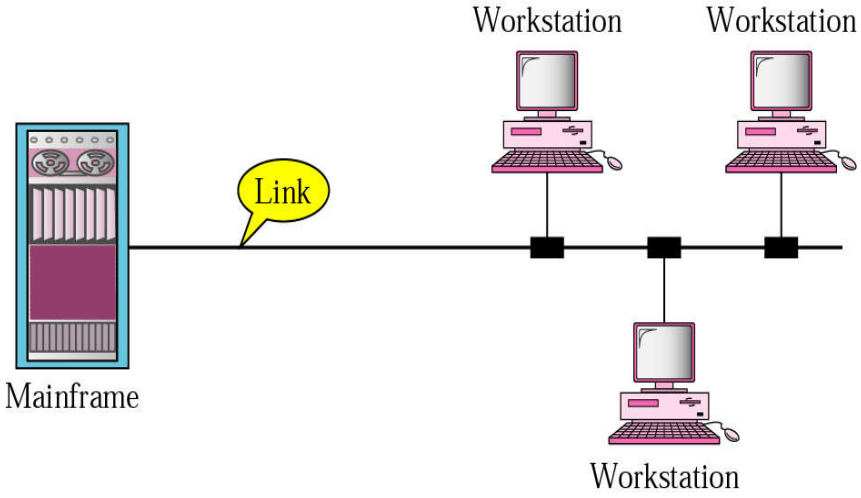
- A node can be a computer, printer, or any other device capable of sending and/or receiving data generated by other nodes on the network.

Types of connections

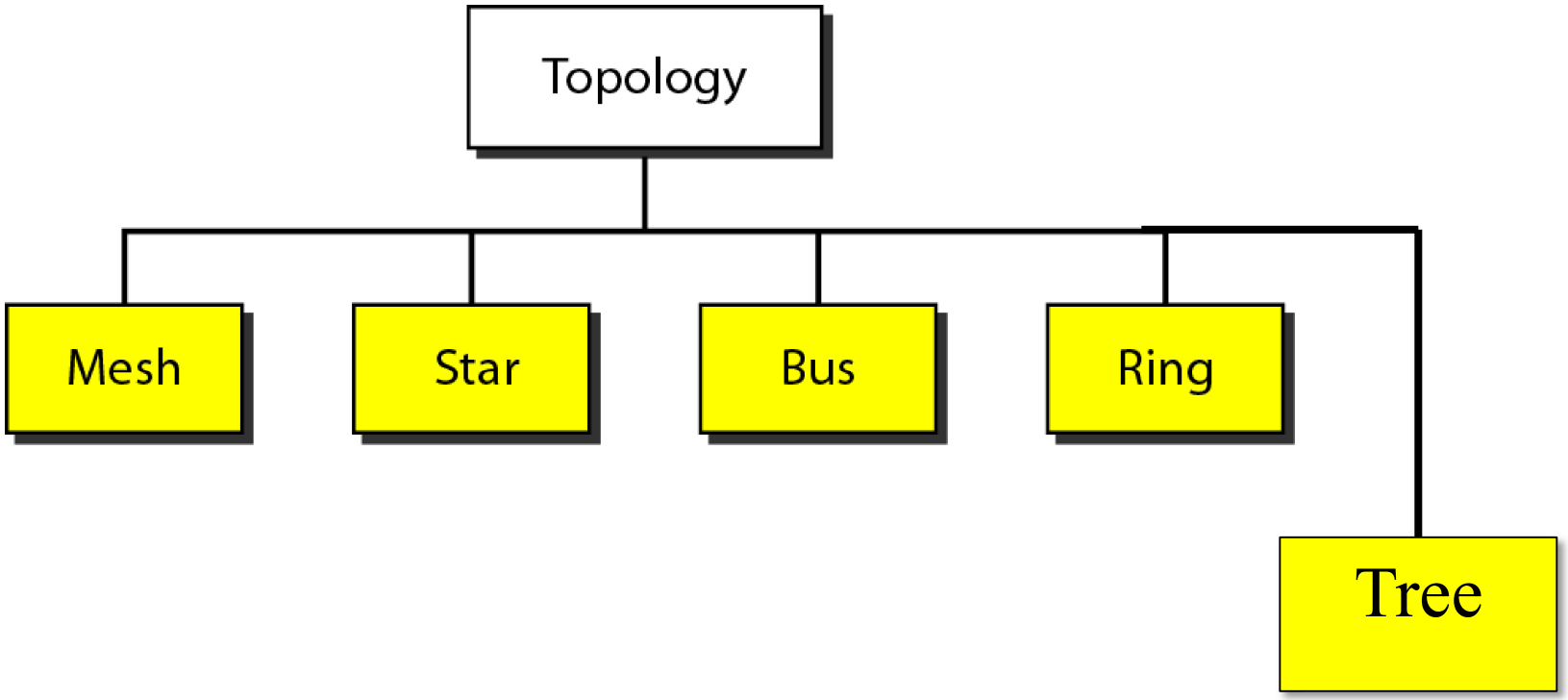
- Point to point
  - A dedicated link is provided between two devices



- Multipoint
  - More than two specific devices share a single link



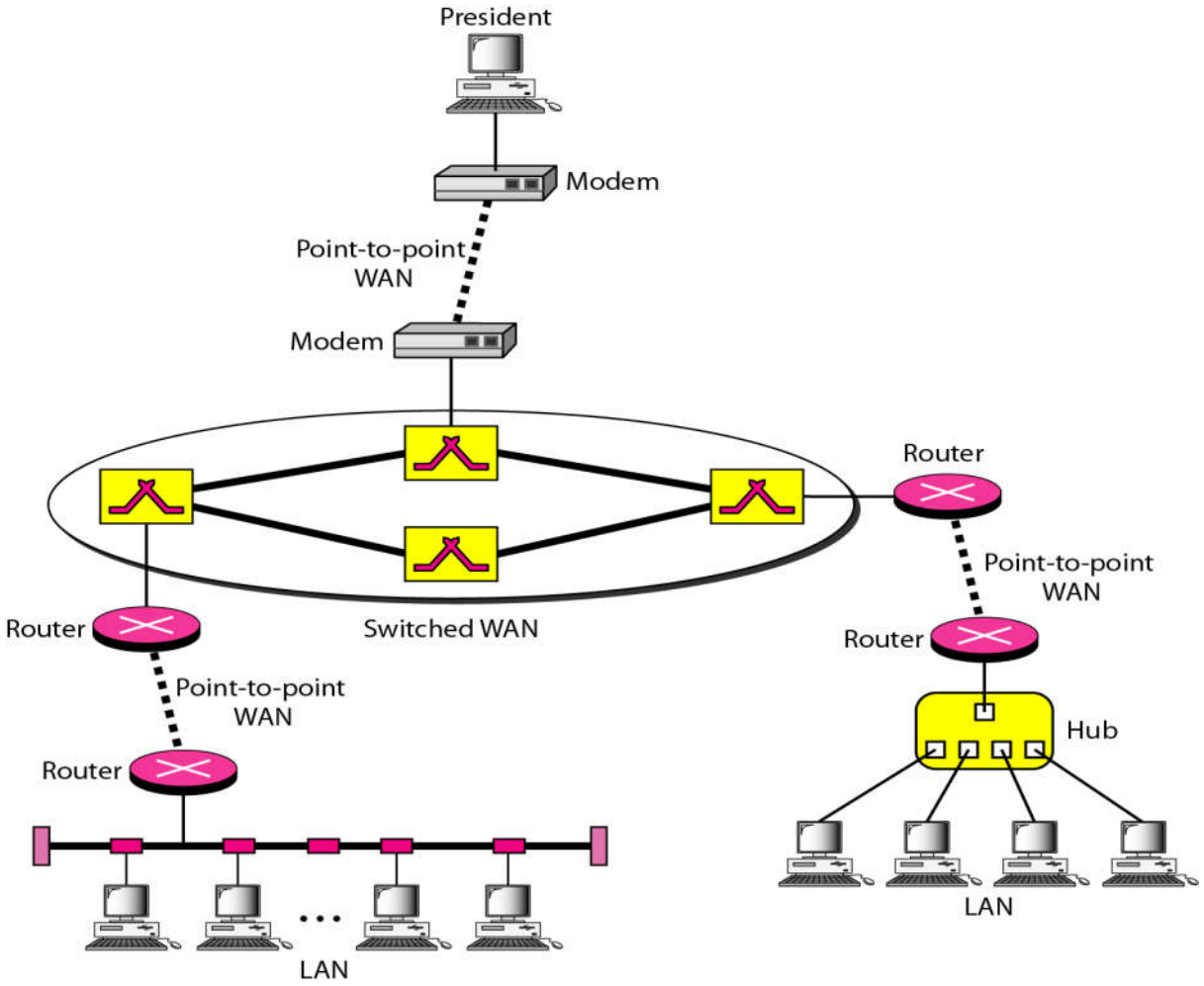
Physical Topology



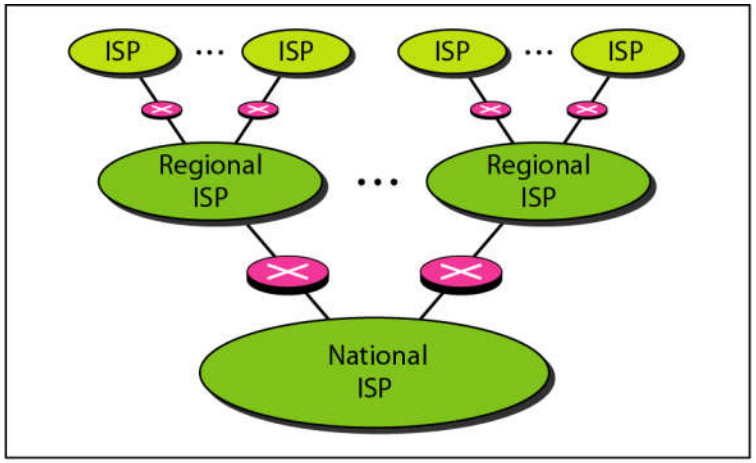
Categories of Networks

1. Local Area Network (LAN)
2. Wireless Local Area Network (WLAN)
3. Metropolitan Area Network (MAN)
4. Wide Area Network (WAN)

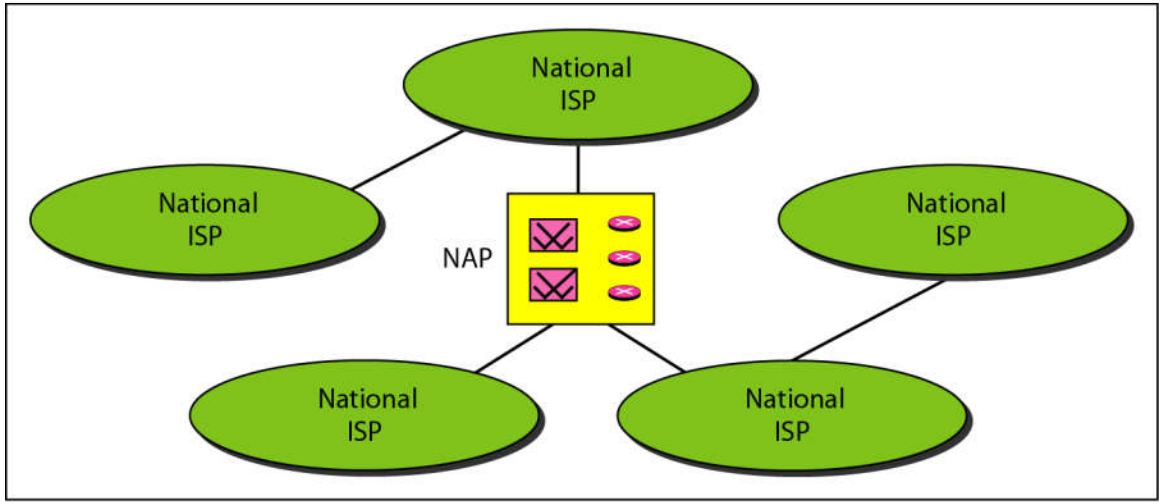
Interconnection of Networks: internet



Hierarchical organization of the Internet



a. Structure of a national ISP



b. Interconnection of national ISPs

Protocols and Standards

- Protocol is synonymous with rule.
- Standards are agreed-upon rules.

Protocols and Standards

Protocols

- Syntax → format of the data
- Semantics → meaning of each section
- Timing → when data should be sent and how fast.

Standards

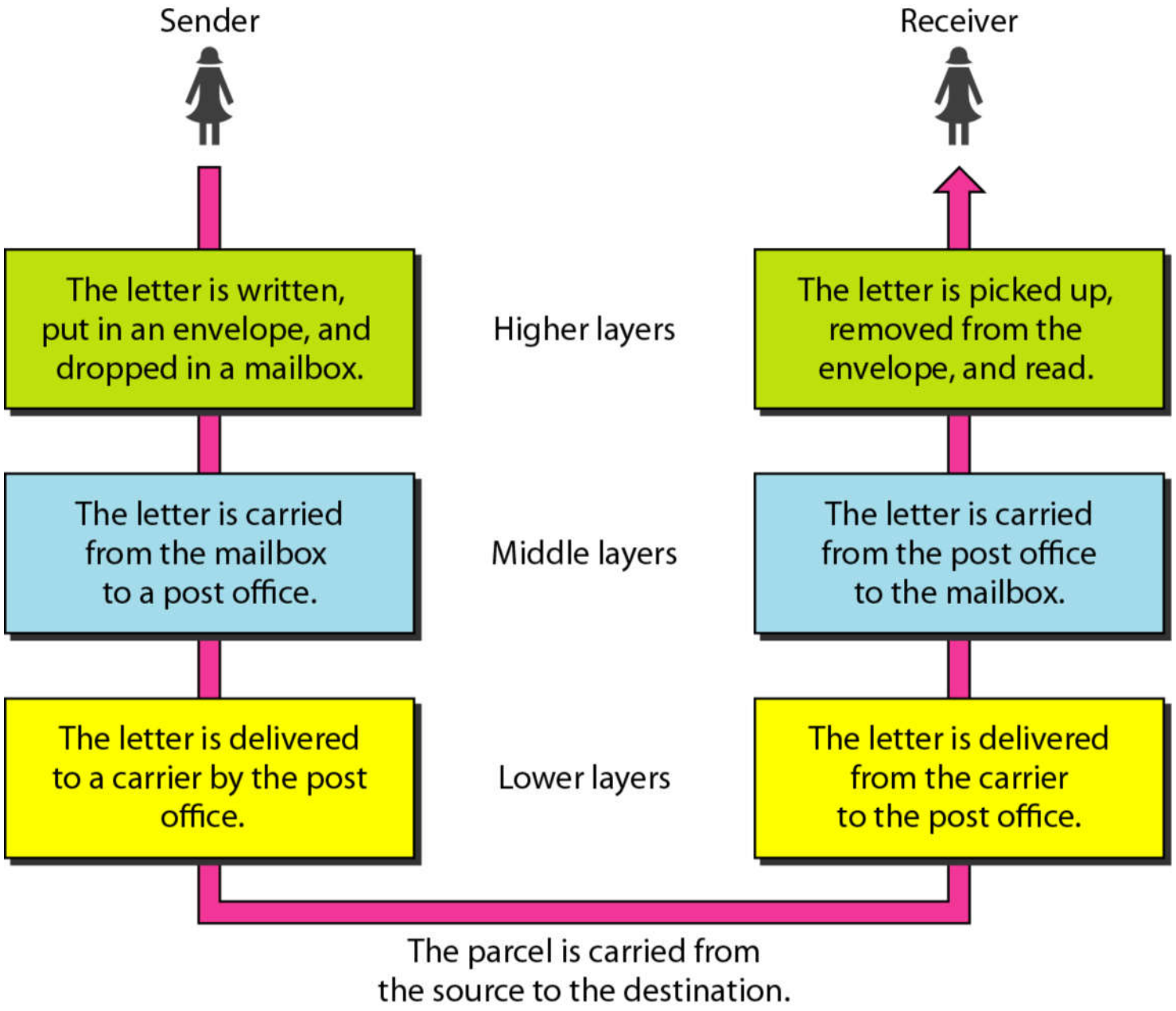
- De facto → by fact (not approved as a standard)
- De jure → by Law (approved)

Network Model

- A network model is a layered architecture
  - Task broken into subtasks
  - Implemented separately in layers in stack
  - Functions need in both systems
  - Peer layers communicate

- Protocol:
  - A set of rules that governs data communication
  - It represents an agreement between the communicating devices

Tasks involved in sending a letter



Layered Architecture: OSI Model

Layers

Layer 7. Application

Layer 6. Presentation

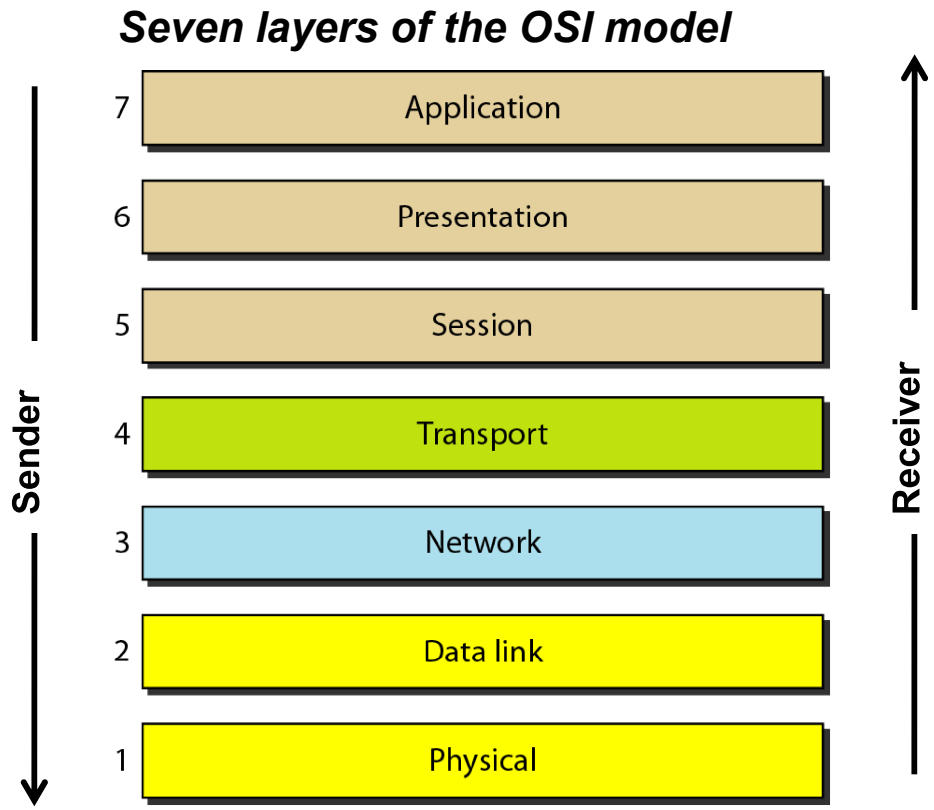
Layer 5. Session

Layer 4. Transport

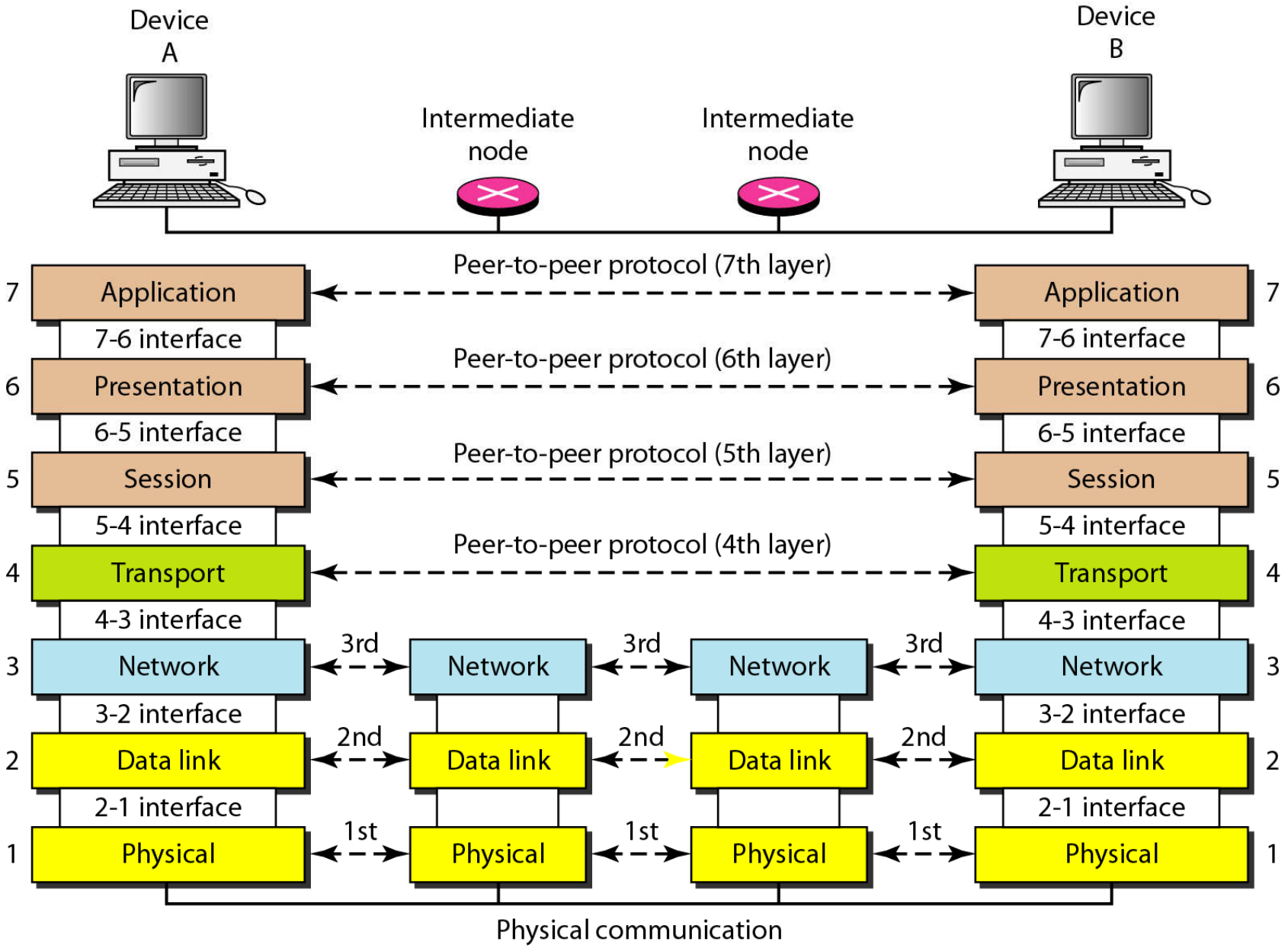
Layer 3. Network

Layer 2. Data Link

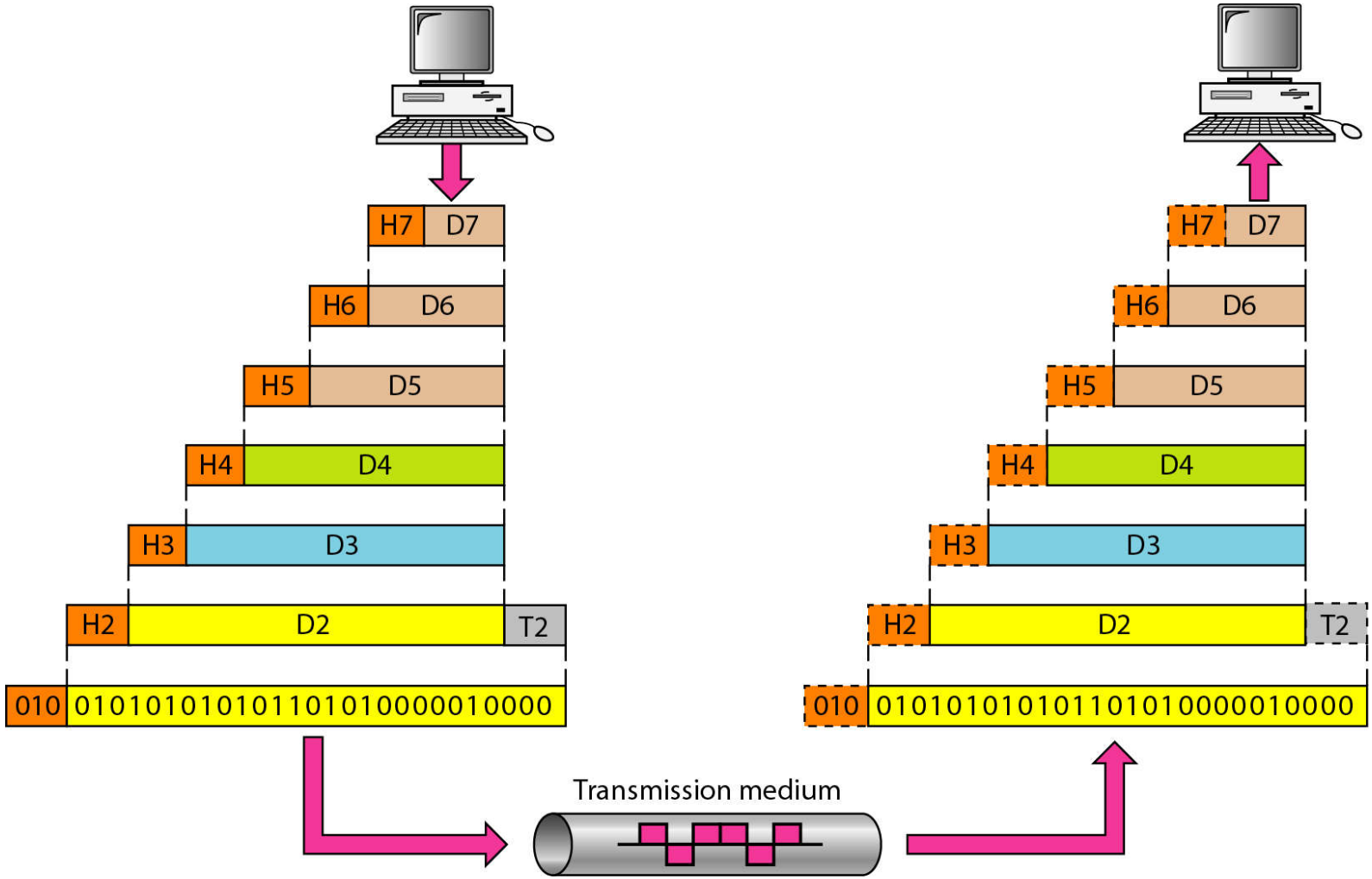
Layer 1. Physical



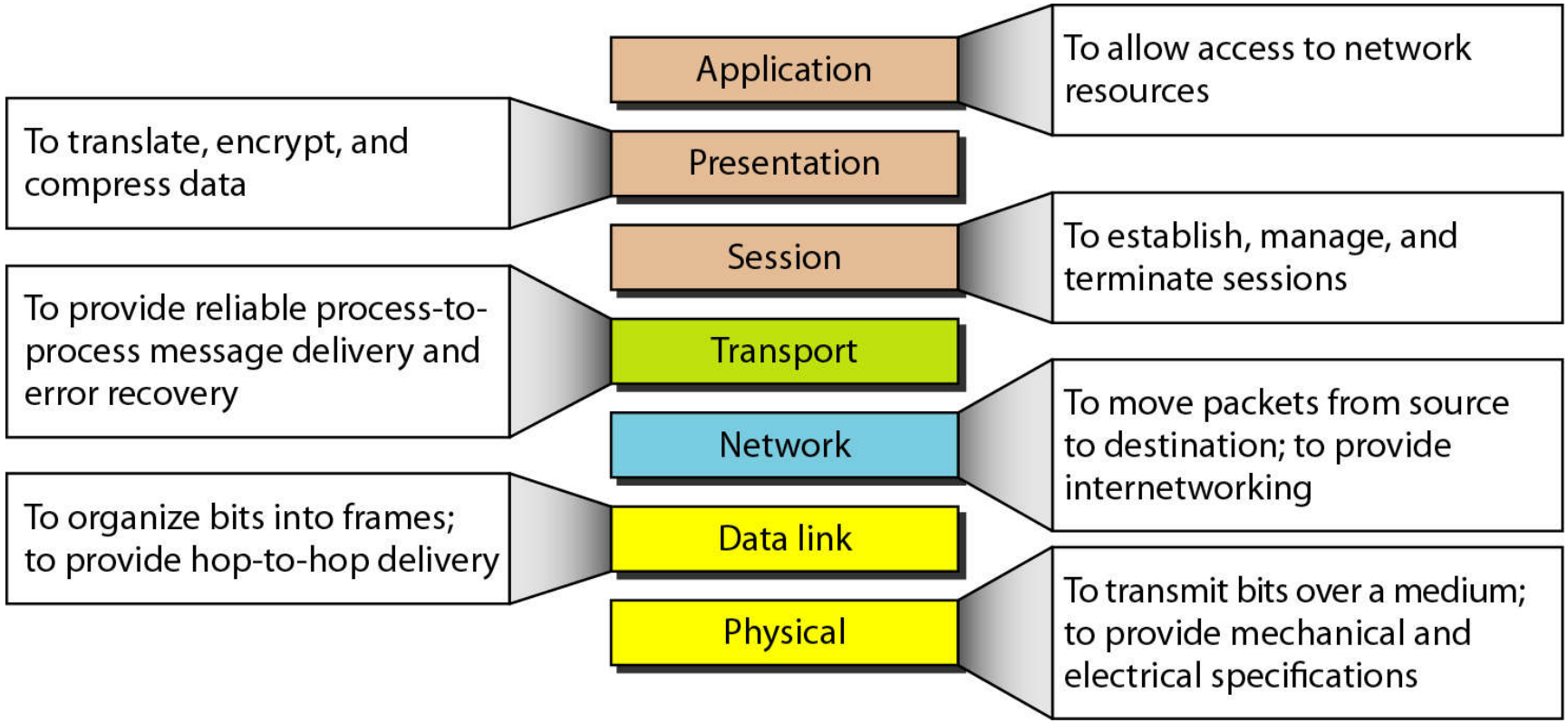
The interaction between layers in the OSI model



An exchange using the OSI model



Summary of layers



Summary of layers

OSI Model			
	Data unit	**Layer**	**Function**
User support layers	Data	7. Application	Network process to application
		6. Presentation	Data representation and encryption
		5. Session	Inter-host communication
User⇔ Network	Segment	4. Transport	End-to-end connections and reliability
Network support layers	Packet	3. Network	Path determination and logical addressing
	Frame	2. Data Link	Physical addressing
	Bit	1. Physical	Media, signal and binary transmission

Sender ↓

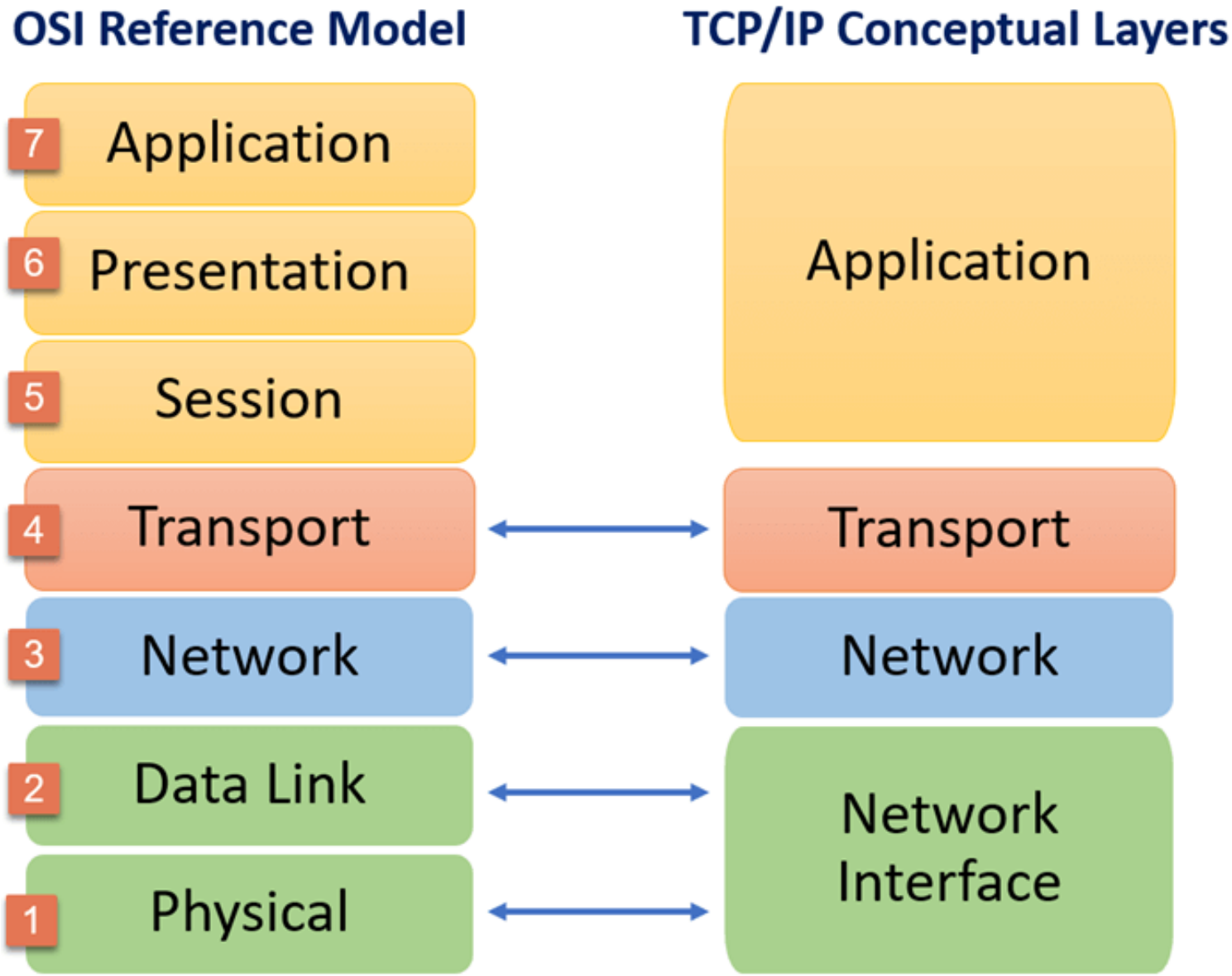
↑ Receiver

TCP/IP PROTOCOL SUITE

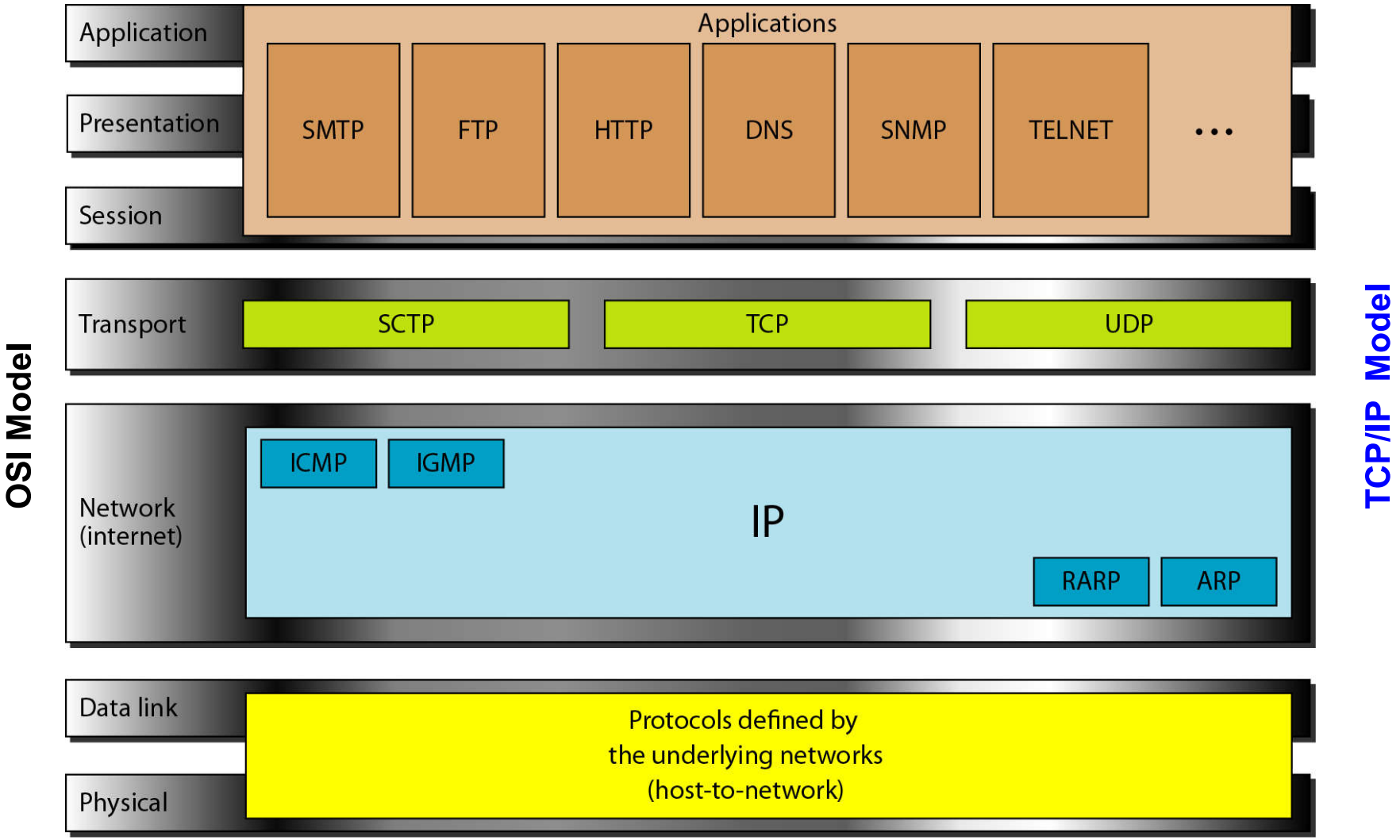
- The layers in the TCP/IP protocol suite do not exactly match those in the OSI model.
- The original TCP/IP protocol suite was defined as having four layers: host-to-network, internet, transport, and application.
- However, when TCP/IP is compared to OSI, we can say that the TCP/IP protocol suite is made of five layers: physical, data link, network, transport, and application.

Physical and Data Link Layers
Network Layer
Transport Layer
Application Layer

TCP/IP PROTOCOL SUITE



TCP/IP PROTOCOL SUITE

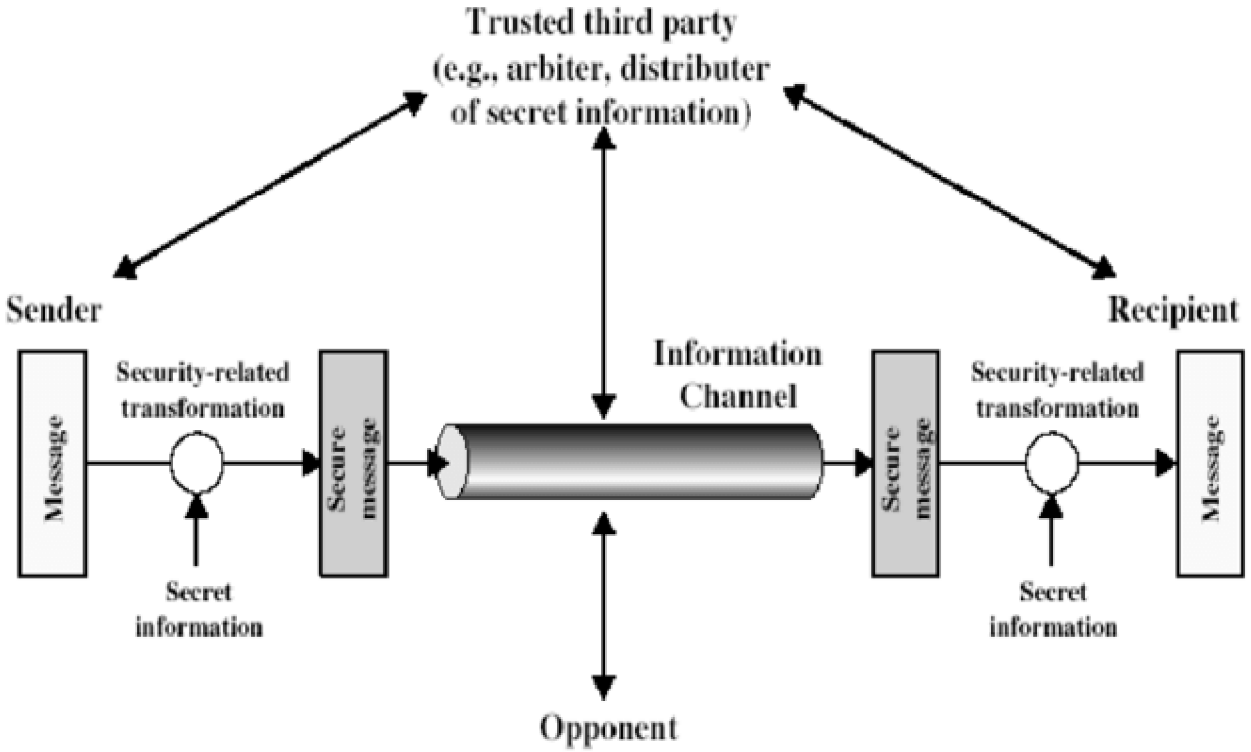


Transportation vs. Computer Networks

Transportation Network	Computer Network
Vehicles/People	Packets/Payload
Street address	IP address
Intersection	Bridge/router
Street, highway, path	Link/broadband/path
Traffic jam	Network congestion
Stop and go traffic light	Flow control
Taking alternative path	Alternative route
Collision	Collision of packets
HOV lane	Flow Priority
Following a route to school	Routing algorithm
…	…

Network Security

A Network Security Model exhibits how the security service has been designed over the network to prevent the opponent from causing a threat to the confidentiality or authenticity of the information that is being transmitted through the network.



Network Attacks

- A network attack is an attempt to gain unauthorized access to an organization's network, with the objective of stealing data or perform other malicious activity.

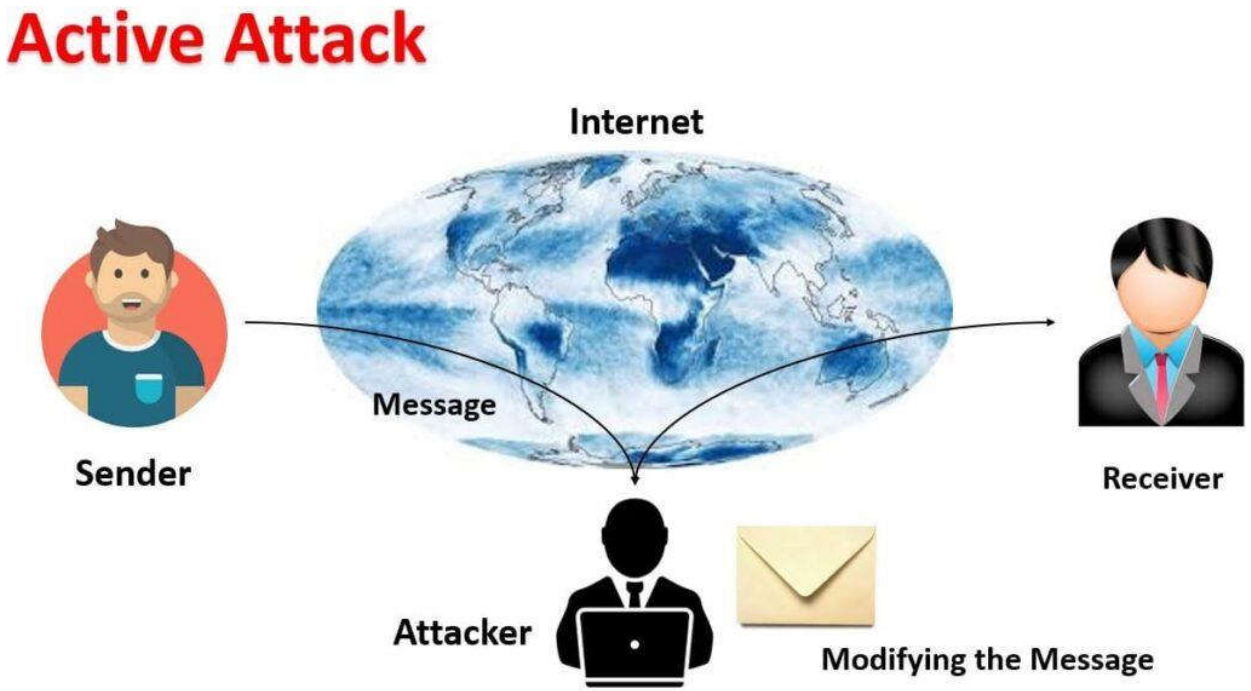
- There are two main types of network attacks:
  - Passive Attacks
  - Active Attacks

Passive Attacks

- Attackers gain access to a network and can monitor or steal sensitive information, but without making any change to the data, leaving it intact.

Active Attacks

- Attackers not only gain unauthorized access but also modify data, either deleting, encrypting or otherwise harming it.



Common Types of Network Attacks

- **Unauthorized access** refers to attackers accessing a network without receiving permission. Among the causes of unauthorized access attacks are weak passwords, lacking protection against social engineering, previously compromised accounts, and insider threats.
- **Distributed Denial of Service (DDoS) attacks:** Attackers build botnets, large fleets of compromised devices, and use them to direct false traffic at your network or servers. DDoS can occur at the network level, for example by sending huge volumes of SYN/ACC packets which can overwhelm a server, or at the application level, for example by performing complex SQL queries that bring a database to its knees.

Common Types of Network Attacks

- A **man in the middle attack** involves attackers intercepting traffic, either between your network and external sites or within your network. If communication protocols are not secured or attackers find a way to circumvent that security, they can steal data that is being transmitted, obtain user credentials and hijack their sessions.
- **Code and SQL injection attacks:** Many websites accept user inputs and fail to validate and sanitize those inputs. Attackers can then fill out a form or make an API call, passing malicious code instead of the expected data values. The code is executed on the server and allows attackers to compromise it.

Common Types of Network Attacks

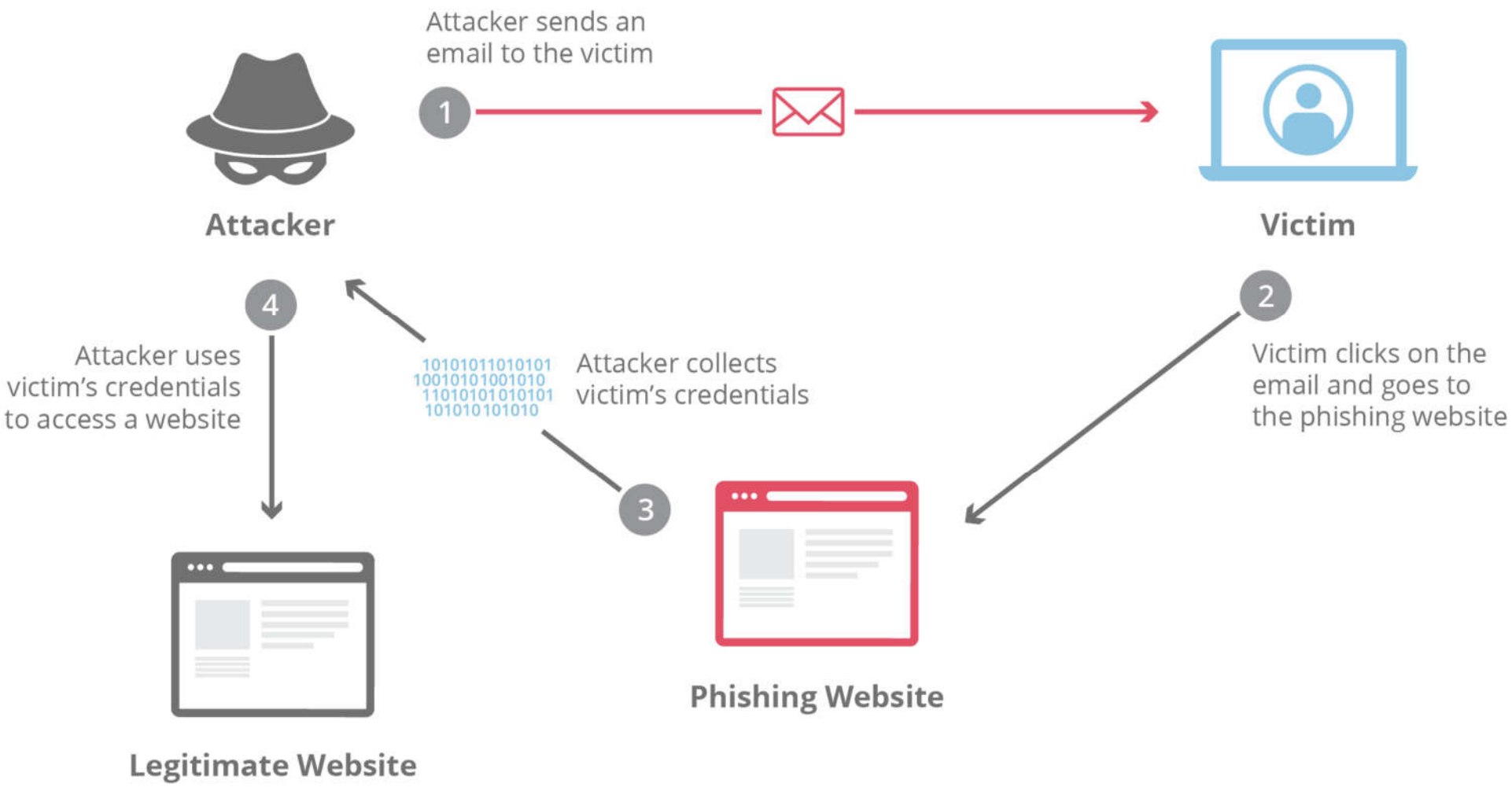
- **Privilege escalation:** Once attackers penetrate your network, they can use privilege escalation to expand their reach. Horizontal privilege escalation involves attackers gaining access to additional, adjacent systems, and vertical escalation means attackers gain a higher level of privileges for the same systems.
- **Insider threats** can come from anywhere, including current or former employees, vendors, contractors, partners, and so forth. Any "insider" with access to the organization's computer systems and data increases the risk of a network attack. Such attacks are difficult to detect and prevent because the attacker already has access to the systems and data inside the network.

Common Types of Network Attacks

- **Malware:** short for malicious software which is specifically designed to disrupt, damage, or gain authorized access to a computer system. Much of the malware out there today is self-replicating.

- **Phishing:** "Phishing" refers to an attempt to steal sensitive information, typically in the form of usernames, passwords, credit card numbers, bank account information or other important data in order to utilize or sell the stolen information. By masquerading as a reputable source with an enticing request, an attacker lures in the victim in order to trick them, similarly to how a fisherman uses bait to catch a fish.

Common Types of Network Attacks



Network Security Components

- Network security safeguards the network from different types of network attacks / threats.

- Implementing network security with various network security components is required to secure a network.

FireWalls

- Firewalls monitor and control incoming and outgoing network traffic based on predefined security rules.
- Firewalls can be hardware-based or software-based and are designed to prevent unauthorized access to the network.
- Network traffic is evaluated based on state, port and protocol, with filtering decisions made based on both administrator-defined security policy and static rules.
- About 40% of network security spending.

Intrusion Detection and Prevention Systems (IDPS):

- An Intrusion Detection System detects and alerts network administrators about any unauthorized or suspicious activities within a network.

- It monitors network traffic, analyzes patterns, and compares potential security breaches against known attack signatures or behavior anomalies.

Virtual Private Networks (VPNs)

- VPNs provide secure remote connectivity by creating a private and encrypted connection over a public network.

- By encrypting data and establishing secure tunnels, VPNs ensure the confidentiality and integrity of transmitted information, making them essential for secure remote access and site-to-site connectivity.

Network Access Control (NAC):

- NAC is a security solution that controls network access based on predefined policies. It ensures that only authorized users and devices can access the network and comply with the organization's security policies.

- It consists of policies, procedures, protocols, tools and applications that define, restrict and regulate what an individual or component can or cannot do on a network.

Antivirus and Antimalware Software:

- Antivirus and antimalware software protect against malicious software (malware) that can compromise network security.

- These software solutions scan files and applications for known malware signatures or suspicious behavior, enabling proactive detection and removal of potential threats.

Secure Sockets Layer/Transport Layer Security (SSL/TLS)

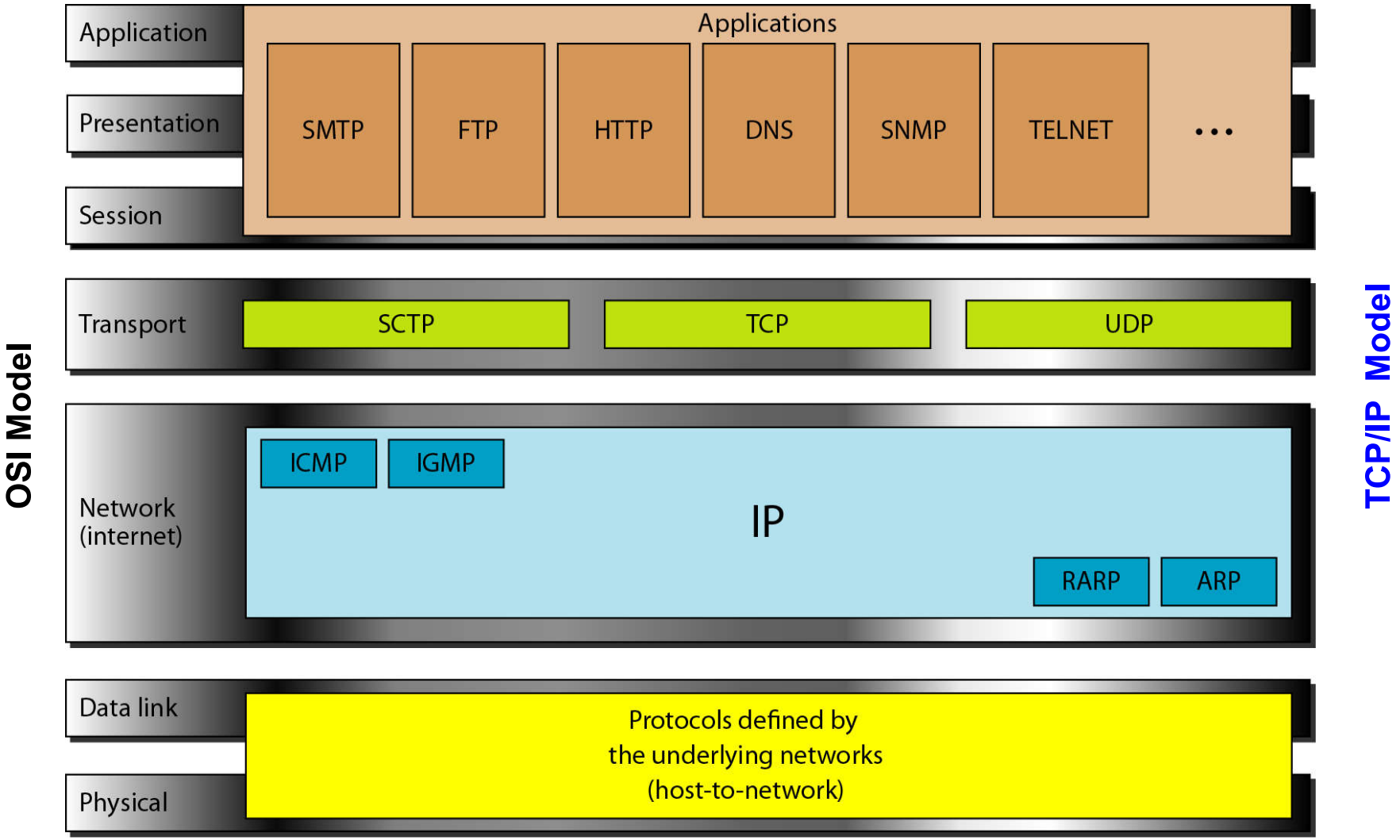
- SSL/TLS protocols provide secure communication over the internet by encrypting data exchanged between a client and a server.

- These protocols ensure that data transmitted between the two parties remain confidential and tamper-proof, making them vital for secure online transactions and communication.

Security Information and Event Management (SIEM) Systems

- SIEM systems collect, analyze, and correlate security event logs from various network devices, servers, and applications. By providing real-time monitoring and threat intelligence, SIEM systems enable early detection and response to security incidents, enhancing overall network security posture.

TCP/IP PROTOCOL SUITE



What is a Virtual Private Network (VPN)?

- A virtual private network, or VPN, is an encrypted connection over the Internet from a device to a network.

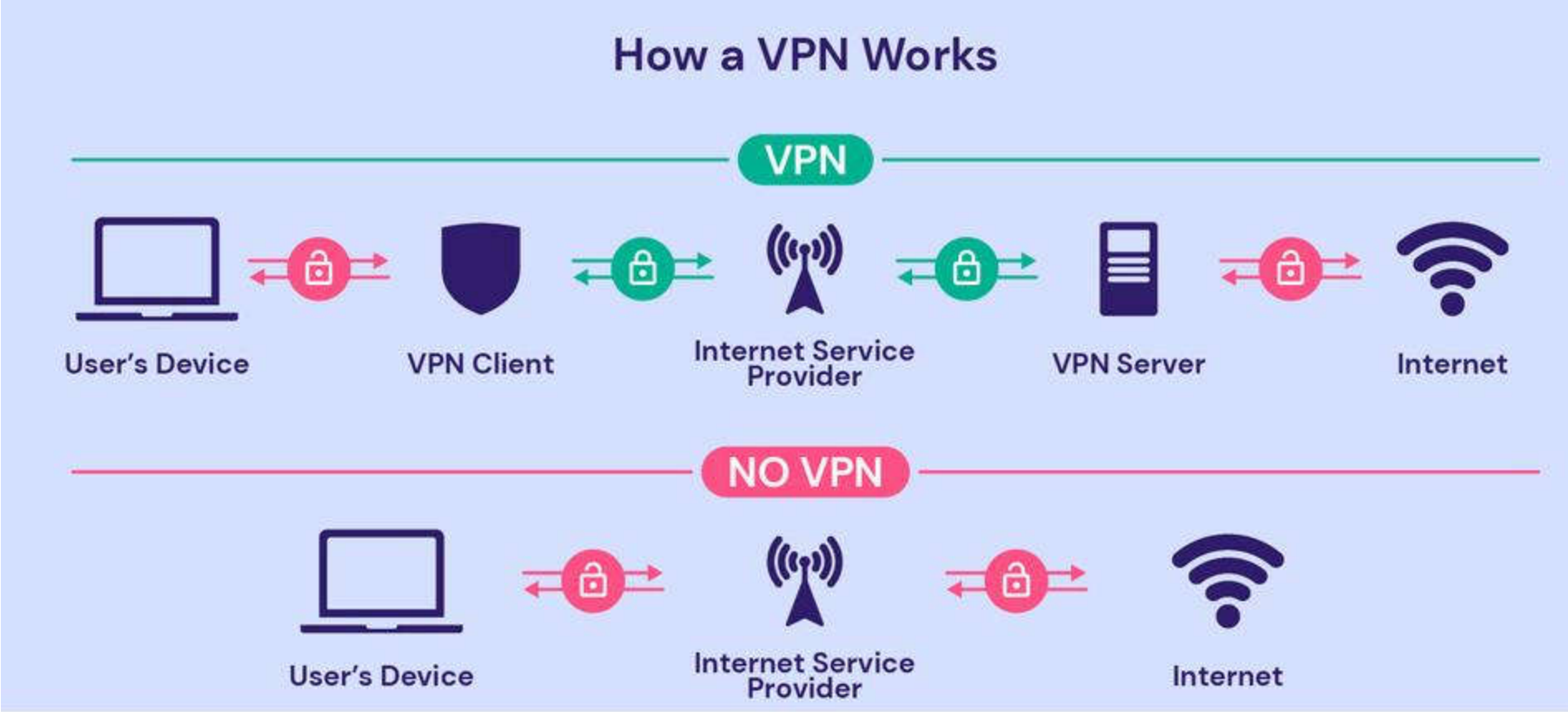
- The encrypted connection helps ensure that sensitive data is safely transmitted.

- VPN technology is widely used in corporate environments.

What is a Virtual Private Network (VPN)?

- Without a VPN, your IP address — a special number unique to your network — is visible to the web.
- A VPN masks your IP address by acting as an intermediary and rerouting your traffic.
- It also adds encryption, or a tunnel around your identity, as you connect.
- The combination of the VPN server and the encryption tunnel blocks your ISP, governments, hackers, and anyone else from spying on you as you navigate the web.

What is a Virtual Private Network (VPN)?



IP Security (IPsec)

- IPsec is a group of networking protocols used for setting up secure encrypted connections, such as VPNs, across publicly shared networks.
- IPsec is a group of protocols for securing connections between devices.
- IPsec helps keep data sent over public networks secure. It is often used to set up VPNs, and it works by encrypting IP packets, along with authenticating the source where the packets come from.
- Within the term "IPsec," "IP" stands for "Internet Protocol" and "sec" for "secure."

What protocols are used in IPsec?

- **Authentication Header (AH):** The AH protocol ensures that data packets are from a trusted source and that the data has not been tampered with, like a tamper-proof seal on a consumer product. These headers do not provide any encryption; they do not help conceal the data from attackers.
- **Encapsulating Security Protocol (ESP):** ESP encrypts the IP header and the payload for each packet — unless transport mode is used, in which case it only encrypts the payload. ESP adds its own header and a trailer to each data packet.

What protocols are used in IPsec?

- **Internet Key Exchange (IKE):** IKE protocol allows hosts at both ends of a VPN tunnel to encrypt and decrypt data packets using mutually agreed upon keys/certificate and method for encryption

IPsec modes

- **Transport mode** is used for end to end communications, for example, communication between a host and server.

- In this case, data contents (IP payload) are protected, but anyone looking at the network traffic can see network traffic patterns.

- In transport mode, the responsibility to perform any cryptographic operations like encryption etc. depends on the sender and receiver

IPsec modes

- **Tunnel mode** encrypts the entire IP packet.
- Usually, it is used to encrypt traffic between two routers/gateways connected over the Internet via IPSEC VPN tunnels.
- In tunnel mode, cryptographic operations like encryption etc., are handled by gateways/routers at both ends of the tunnels, in addition to the sender and receiver

How Does IPsec Work?