गृह मंत्रालय
MINISTRY OF
HOME AFFAIRS

राष्ट्रीय न्यायिक विज्ञान विश्वविद्यालय
National Forensic Sciences University

Network Security & Forensics



Dr. Lokesh Chouhan

Dean Academics and Associate Professor

गृह मंत्रालय
MINISTRY OF
HOME AFFAIRS

राष्ट्रीय न्यायालयिक विज्ञान विश्वविद्यालय
(राष्ट्रीय महत्त्व का संस्थान, गृह मंत्रालय, भारत सरकार)
National Forensic Sciences University
(An Institution of National Importance under Ministry of Home Affairs, Government of India)

E-Mail: Lokeshchouhan@gmail.com, Lokesh.chouhan_goa@nfsu.ac.in

Mob: +91-898924399, 9827235155

Overview of the Course

Theory

- **Basics of Networking**
- **Penetration Testing**
- **Cryptography**
- **Wireless Network Security**
- **Network Forensics**

Lab

- VMware for Linux or windows
- Wireshark
- report an incident on CERT-IN
- pgportal.gov.in
- Browser Security
- Cryptography Prog.
- Linux/Windows Security Tools

Overview of the Course

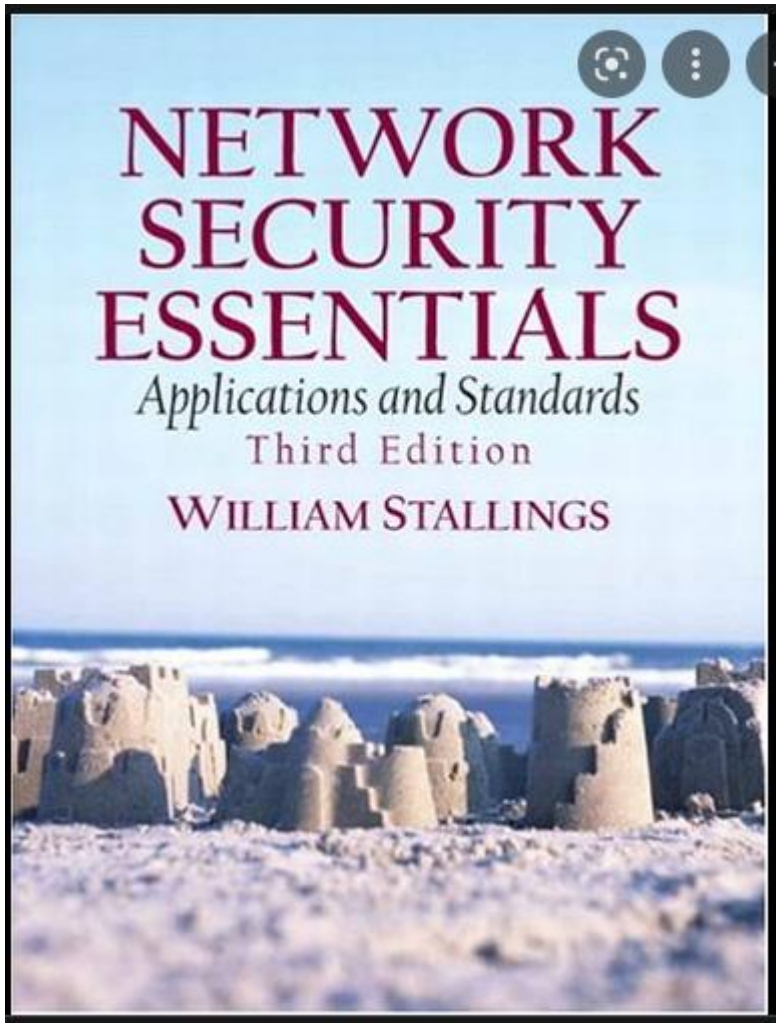
Books

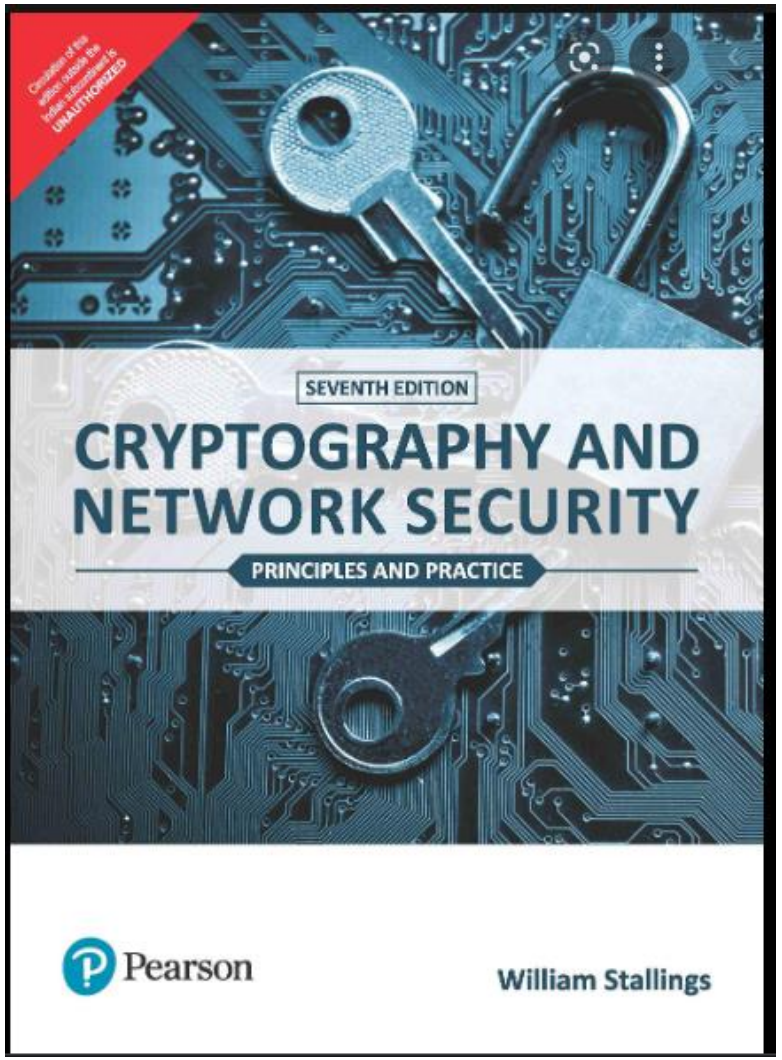
1. Stallings, W., Network Security Essentials: applications and standards. 3rd ed. Pearson Education India, 2007.
2. Stallings, W., Cryptography and Network Security: Principles and Practice. 6th ed. Pearson, 2004.
3. Forouzan, B.A., Cryptography & Network Security. Tata McGraw-Hill Education, 2010 2.
4. Kahate, A. Cryptography and Network Security. McGraw-Hill Higher Ed., 2009.
5. Michael Gregg, Build Your Own Security Lab: A Field Guide for Networking Testing.
6. Sherri Davidoff and Jonathan Ham, Network Forensics Tracking Hackers through Cyberspace.
7. Mastering Wireless Penetration Testing for Highly Secured Environments by Aaron Johns
8. Chris McNab, Network Security Assessment: Know Your Network 9. Cameron Buchanan and Vivek Ramachandran, Kali Linux Wireless Penetration Testing Beginner's Guide

Marks Distribution

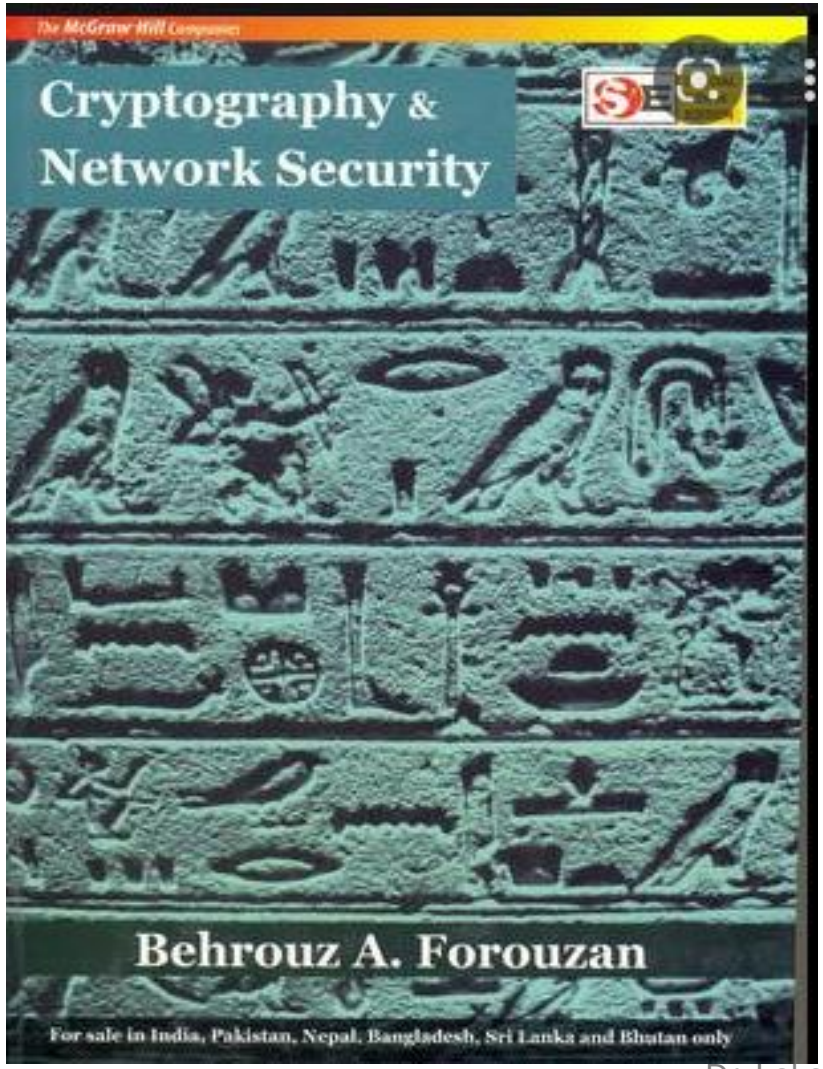
TE-1	25 Marks
TE-2	25 Marks
Mid Sem	50 Marks
End Semester	100 Marks
Total	**200 Marks**

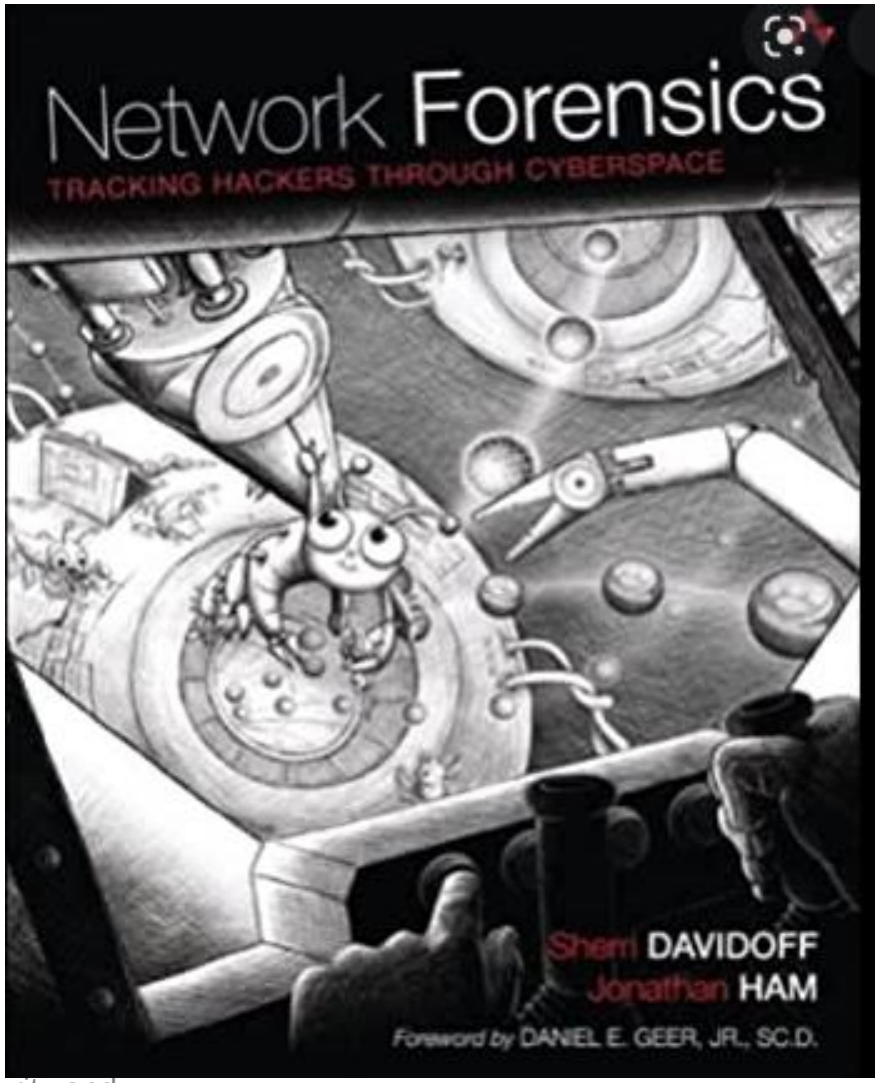
Books


NETWORK
SECURITY
ESSENTIALS
Applications and Standards
Third Edition
WILLIAM STALLINGS

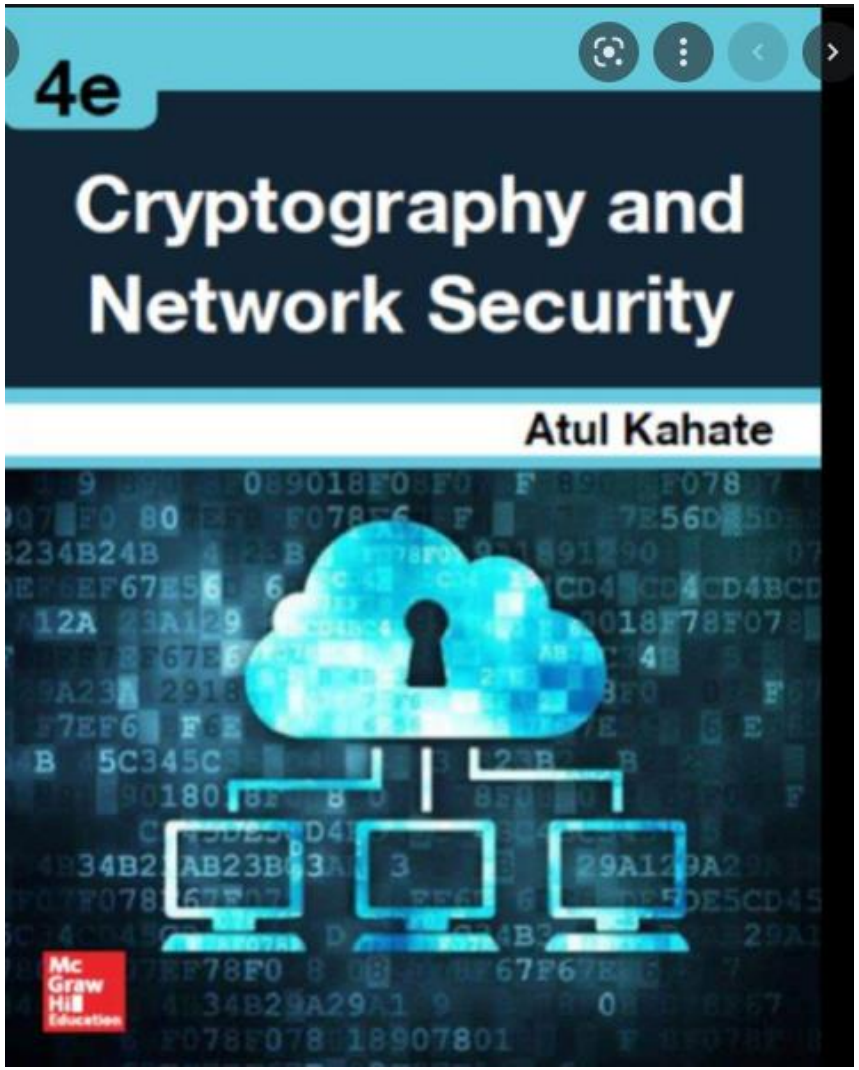

SEVENTH EDITION
CRYPTOGRAPHY AND
NETWORK SECURITY
PRINCIPLES AND PRACTICE
Pearson
William Stallings

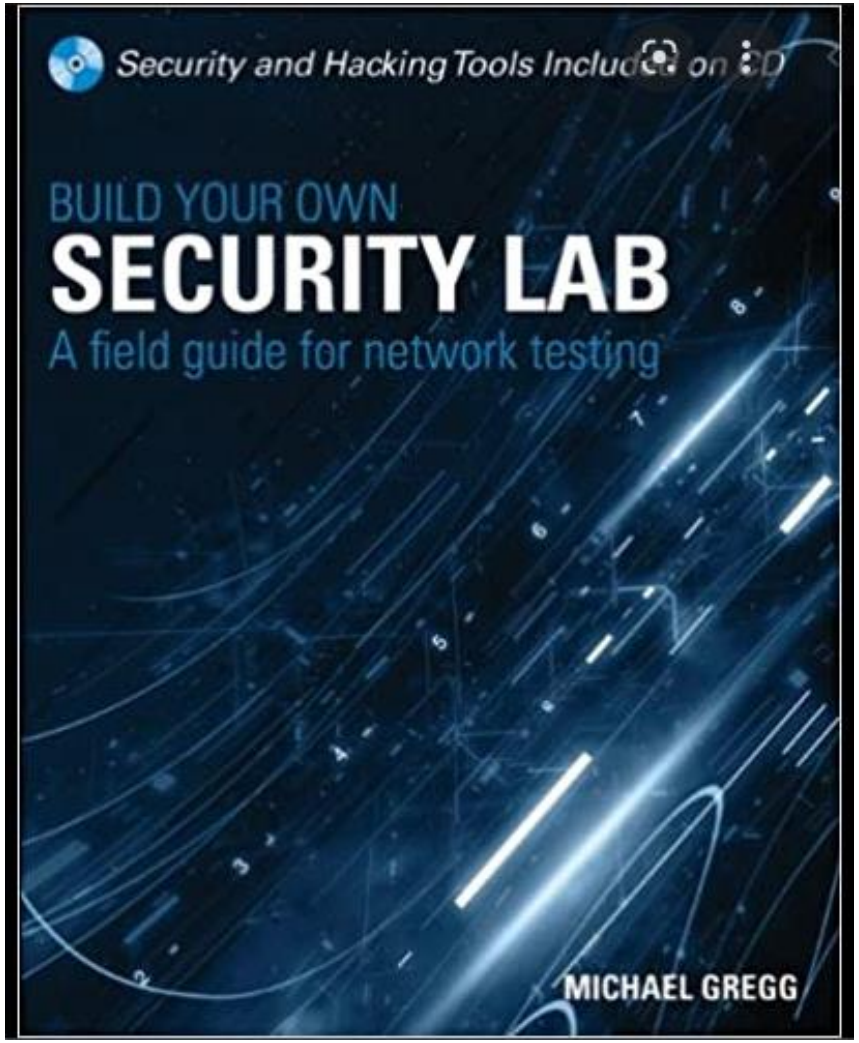
Books


Cryptography &
Network Security
Behrouz A. Forouzan
For sale in India, Pakistan, Nepal, Bangladesh, Sri Lanka and Bhutan only

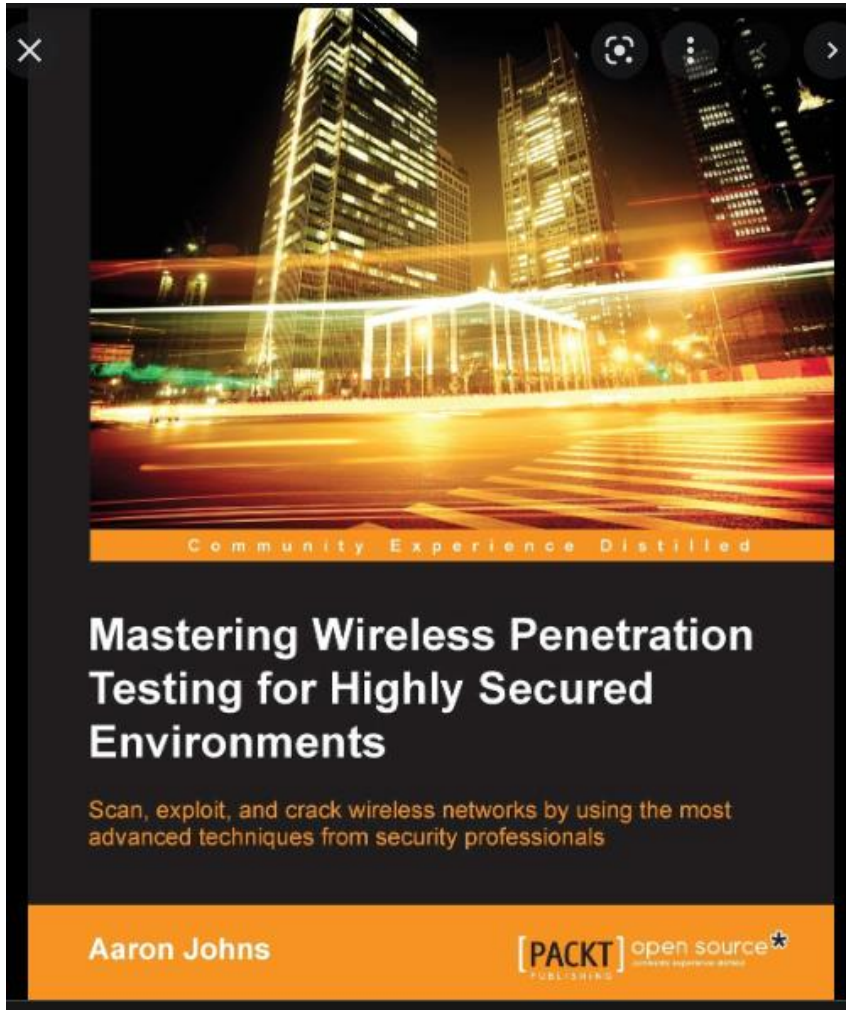

Network Forensics
TRACKING HACKERS THROUGH CYBERSPACE
Sherri DAVIDOFF
Jonathan HAM
Foreword by DANIEL E. GEER, JR., SC.D.

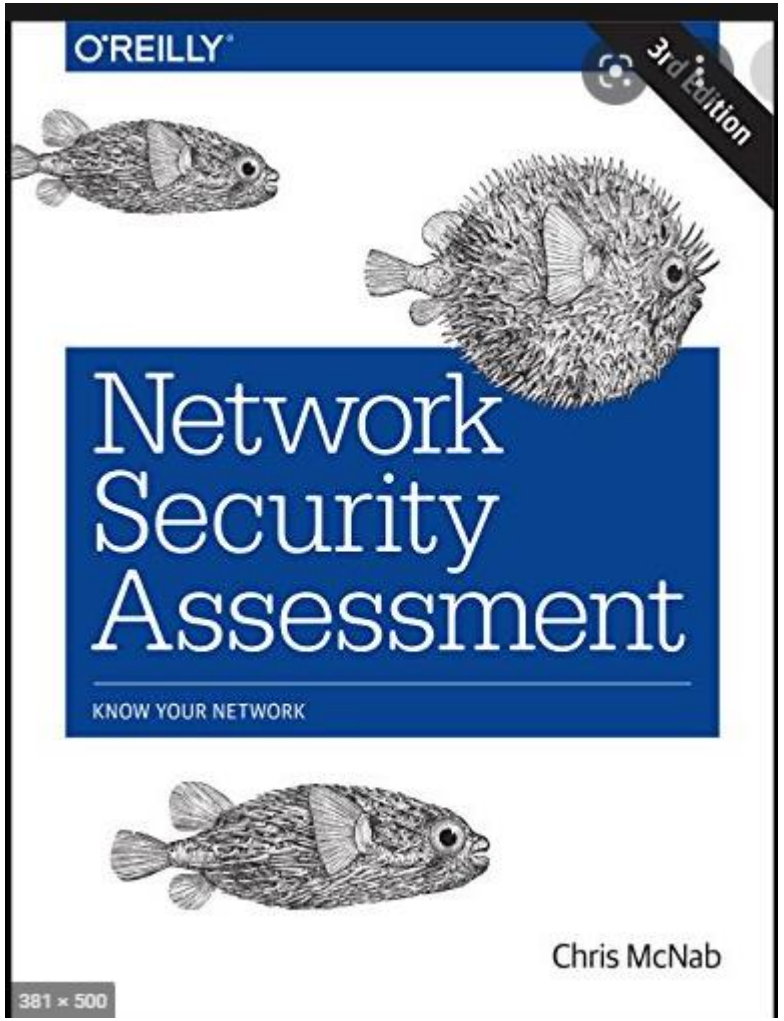
Books


4e
Cryptography and Network Security
Atul Kahate
Mc Graw Hill Education


Security and Hacking Tools Included on CD
BUILD YOUR OWN
SECURITY LAB
A field guide for network testing
MICHAEL GREGG

Books


Community Experience Distilled
Mastering Wireless Penetration Testing for Highly Secured Environments
Scan, exploit, and crack wireless networks by using the most advanced techniques from security professionals
Aaron Johns
[PACKT] open source

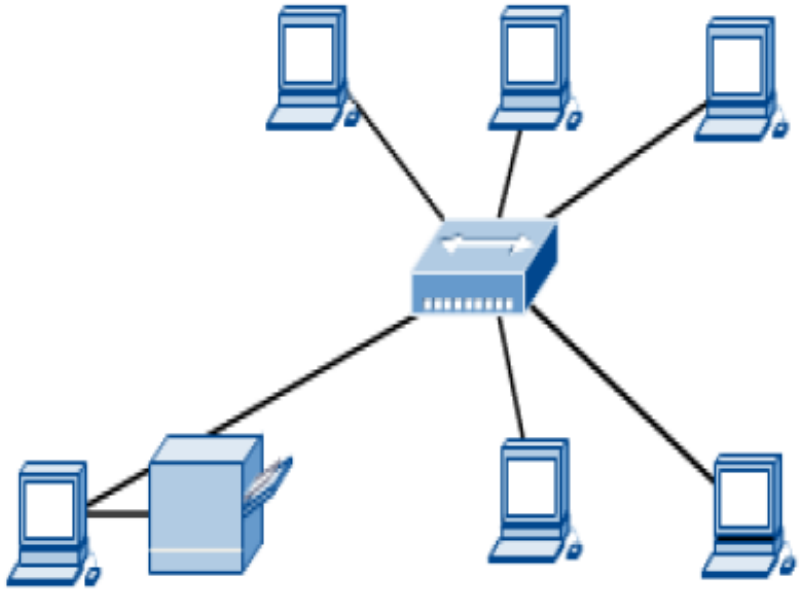

O'REILLY
3rd Edition
Network Security Assessment
KNOW YOUR NETWORK
Chris McNab
381 × 500

Unit-1 **Basics of Networking**

- ISO/OSI, TCP-IP, Networking devices: Host, Hub, Bridge, Switch, Router and its functioning, Perimeter devices: IDS, IPS, Firewall and its functioning. NOC, SOC, SIEM, Servers: DNS, DHCP, Proxy, Mail and Application servers. Threat, vulnerability, attack surface, attack vector, exploit. Common attacks and countermeasures: Phishing attack, ARP poising, MAC flooding, DoS and DDoS.

Computer Networks

- Computer network connects two or more autonomous computers.



- The computers can be geographically located anywhere.

Introduction to Computer Networks

LAN, MAN & WAN

- Network in small geographical Area (Room, Building or a Campus) is called LAN (Local Area Network)
- Network in a City is call MAN (Metropolitan Area Network)
- Network spread geographically (Country or across Globe) is called WAN (Wide Area Network)

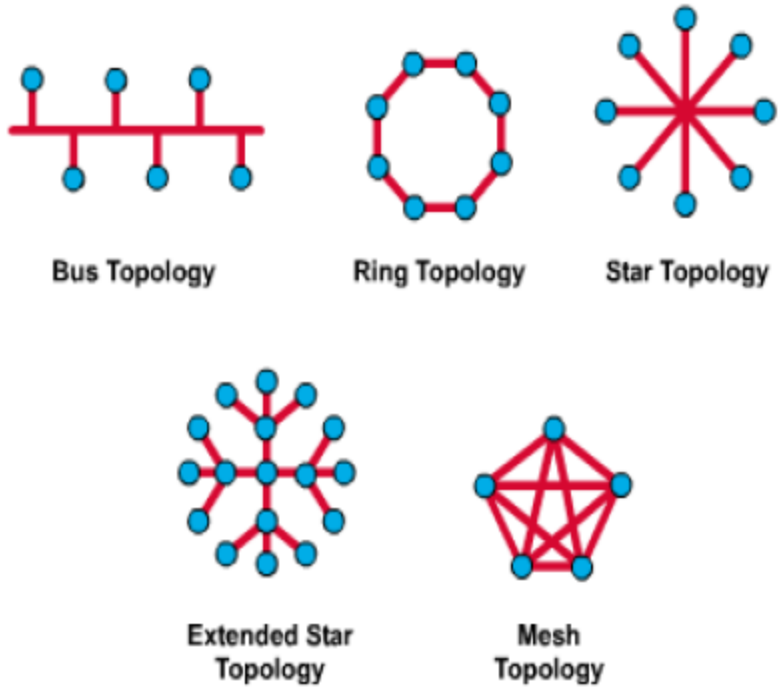
Applications of Networks

- **Resource Sharing**
  - Hardware (computing resources, disks, printers)
  - Software (application software)
- **Information Sharing**
  - Easy accessibility from anywhere (files, databases)
  - Search Capability (WWW)
- **Communication**
  - Email
  - Message broadcast
- **Remote computing**
- **Distributed processing (GRID Computing)**

Introduction to Computer Networks

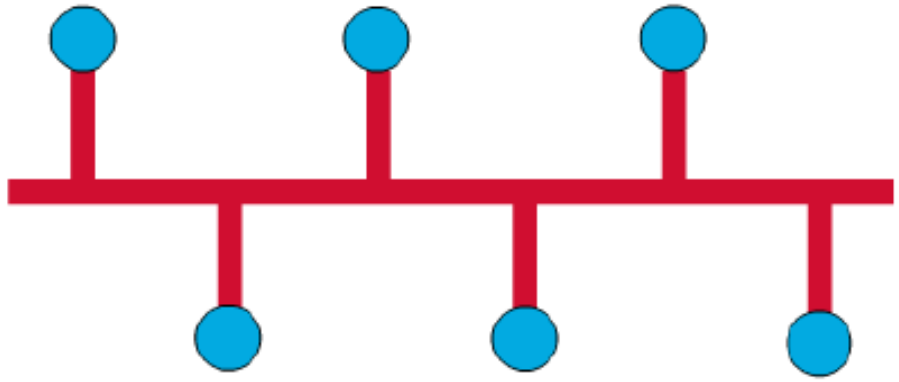
Network Topology

- The network topology defines the way in which computers, printers, and other devices are connected. A network topology describes the layout of the wire and devices as well as the paths used by data transmissions.



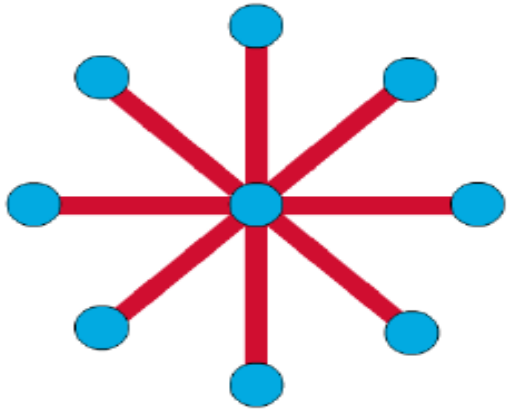
Bus Topology

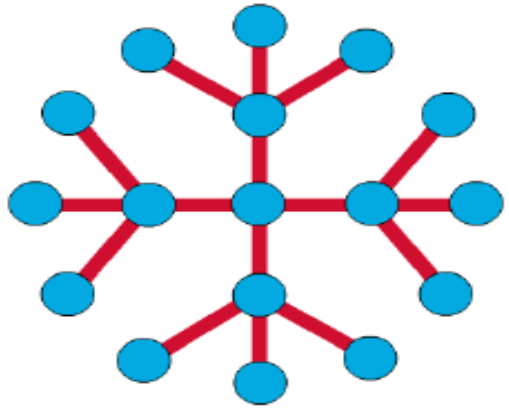
- Commonly referred to as a linear bus, all the devices on a bus topology are connected by one single cable.



Star & Tree Topology

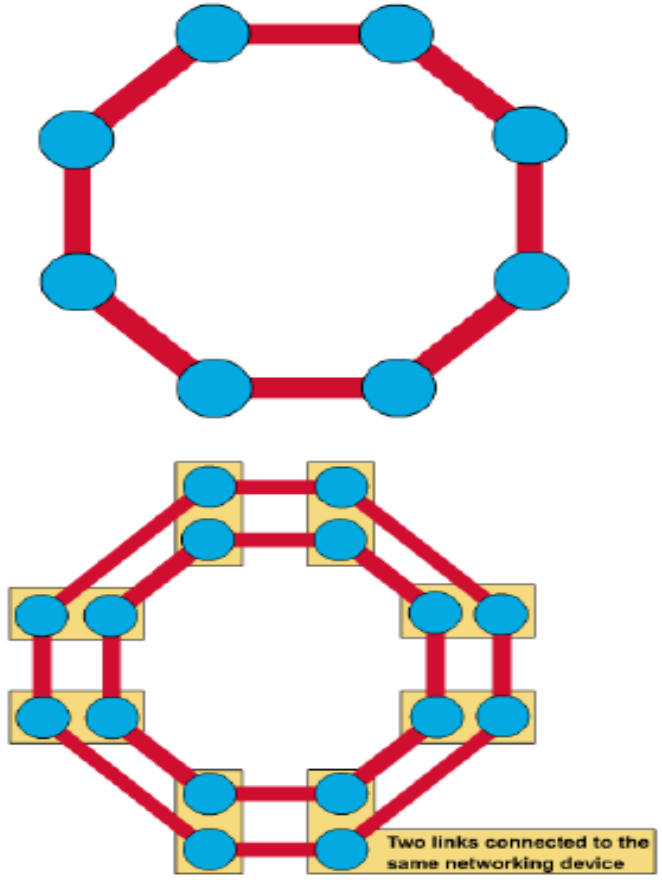
- The star topology is the most commonly used architecture in Ethernet LANs.
- When installed, the star topology resembles spokes in a bicycle wheel.
- Larger networks use the extended star topology also called tree topology. When used with network devices that filter frames or packets, like bridges, switches, and routers, this topology significantly reduces the traffic on the wires by sending packets only to the wires of the destination host.





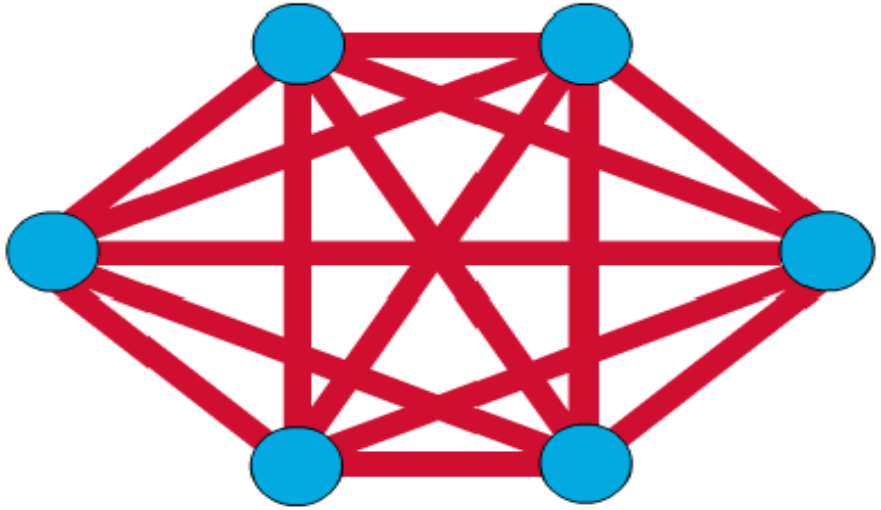
Ring Topology

- A frame travels around the ring, stopping at each node. If a node wants to transmit data, it adds the data as well as the destination address to the frame.
- The frame then continues around the ring until it finds the destination node, which takes the data out of the frame.
  - Single ring – All the devices on the network share a single cable
  - Dual ring – The dual ring topology allows data to be sent in both directions.



Mesh Topology

- The mesh topology connects all devices (nodes) to each other for redundancy and fault tolerance.
- It is used in WANs to interconnect LANs and for mission critical networks like those used by banks and financial institutions.
- Implementing the mesh topology is expensive and difficult.



Introduction to Computer Networks

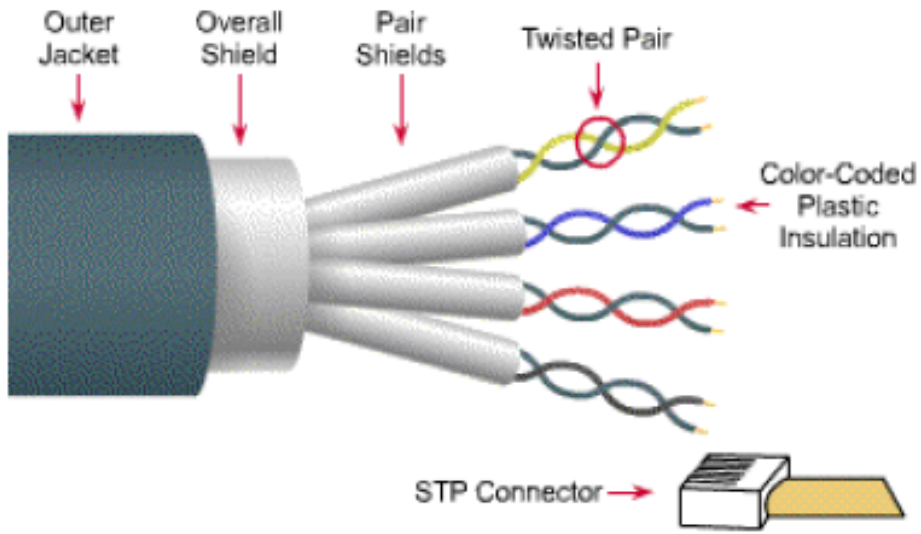
Network Components

- Physical Media
- Interconnecting Devices
- Computers
- Networking Software
- Applications

Introduction to Computer Networks

Networking Media

- Networking media can be defined simply as the means by which signals (data) are sent from one computer to another (either by cable or wireless means).



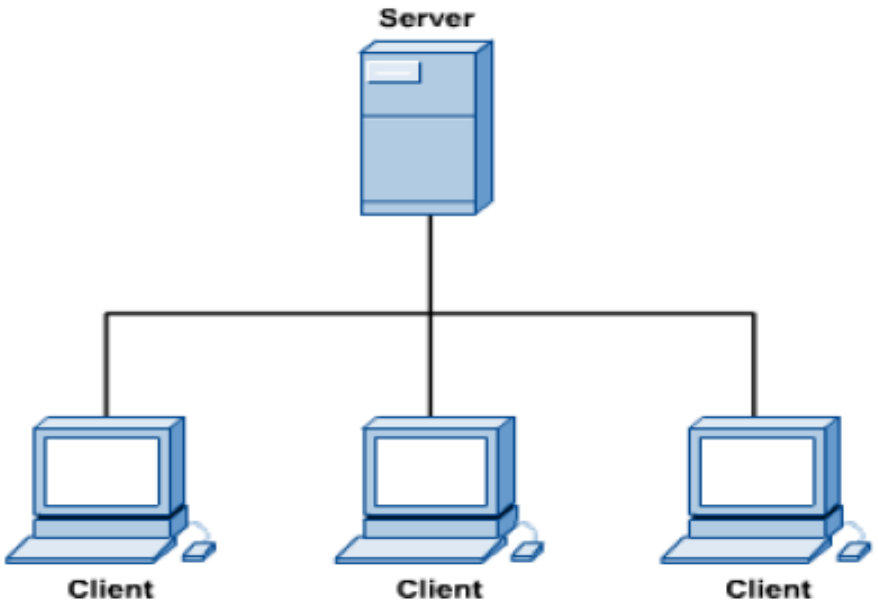
- Speed and throughput: 10-100 Mbps
- Cost per node: Moderately expensive
- Media and connector size: Medium to Large
- Maximum cable length: 100m (short)

Networking Devices

- HUB, Switches, Routers, Wireless Access Points, Modems etc.

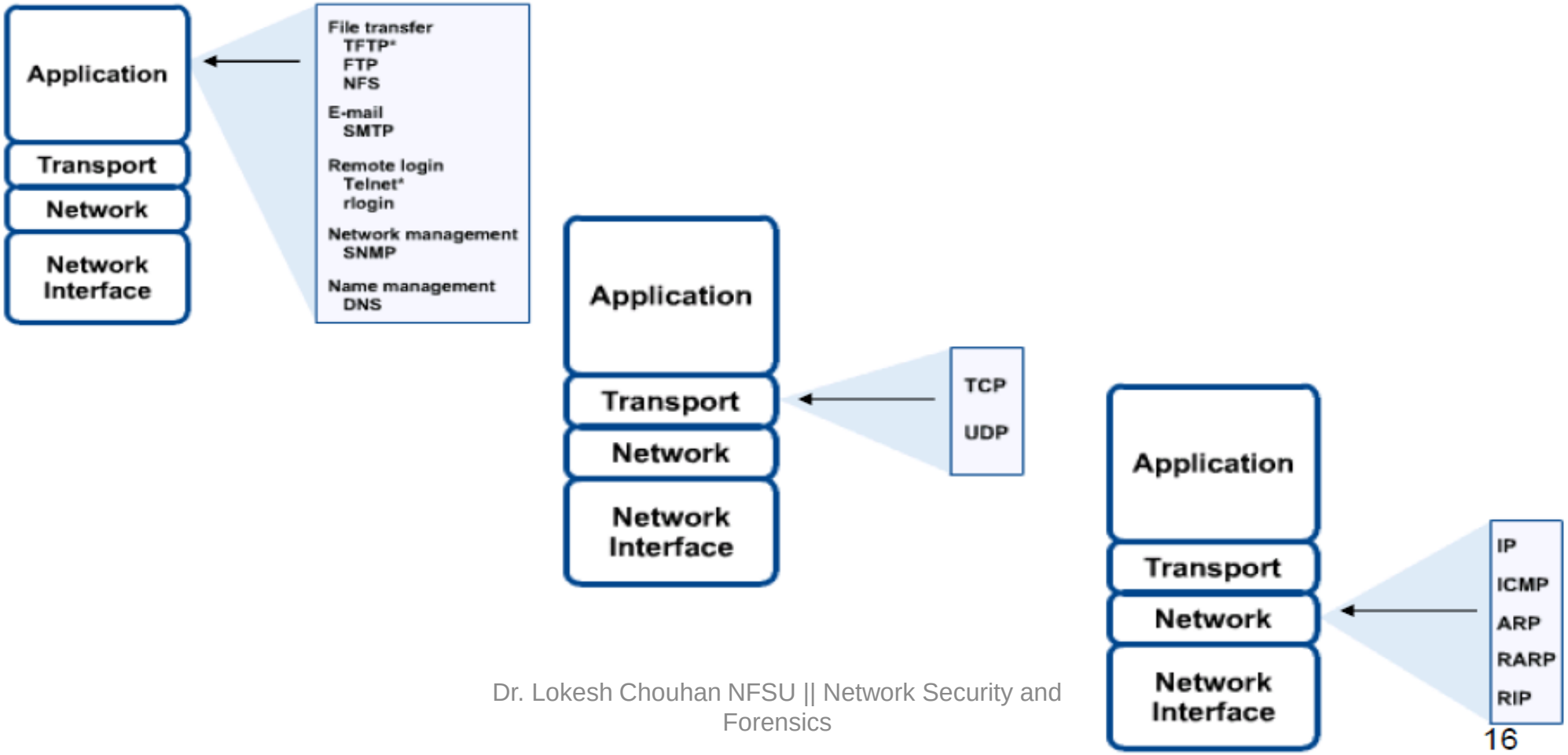
Computers: Clients and Servers

- In a client/server network arrangement, network services are located in a dedicated computer whose only function is to respond to the requests of clients.
- The server contains the file, print, application, security, and other services in a central computer that is continuously available to respond to client requests.



15

Networking Protocol: TCP/IP



Applications

- E-mail
- Searchable Data (Web Sites)
- E-Commerce
- News Groups
- Internet Telephony (VoIP)
- Video Conferencing
- Chat Groups
- Instant Messengers
- Internet Radio

Networking

Computer network

A collection of computing devices connected in order to communicate and share resources

Connections between computing devices can be physical using wires or cables or wireless using radio waves or infrared signals

Can you name some of the devices in a computer network?

Networking

Node (host)

Any device on a network

Data transfer rate (bandwidth)

The speed with which data is moved from one place to another on a network

Why is bandwidth so key?

Networking

Computer networks have opened up an entire frontier in the world of computing called the **client/server model**

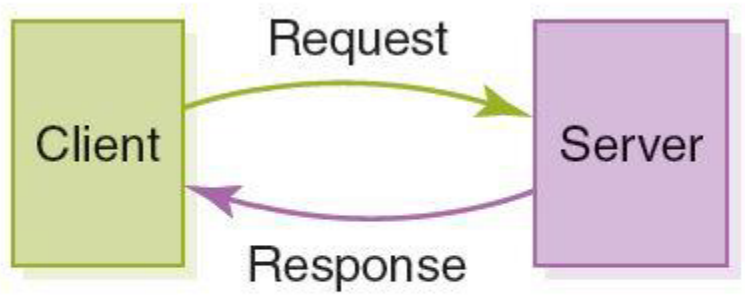


FIGURE 15.1 Client/server interaction

Networking

Protocol

A set of rules that defines how data is formatted and processed on a network

File server

A computer dedicated to storing and managing files for network users

Web server

A computer dedicated to responding to requests for web pages

P2P model

A decentralized approach that shares resources and responsibilities among many “peer” computers

Types of Networks

Local-area network (LAN)

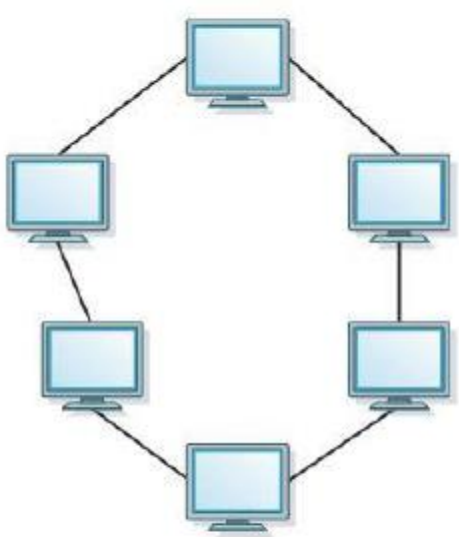
A network that connects a relatively small number of machines in a relatively close geographical area

Ring topology connects all nodes in a closed loop on which messages travel in one direction

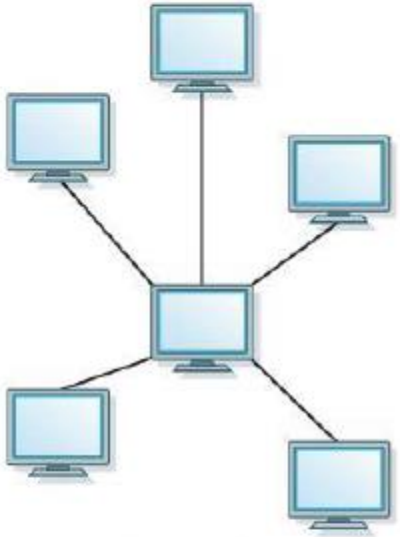
Star topology centers around one node to which all others are connected and through which all messages are sent

Bus topology nodes are connected to a single communication line that carries messages in both directions

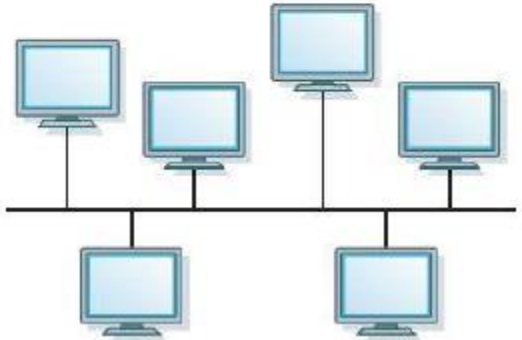
Types of Networks



Ring topology



Star topology



Bus topology

FIGURE 15.2 Network topologies

Ethernet

The industry standard bus technology for local-area networks

Types of Networks

Wide-area network (WAN)

A network that connects local-area networks over a potentially large geographic distance

Metropolitan-area network (MAN)

The communication infrastructures that have been developed in and around large cities

Gateway

One particular set up to handle all communication going between that LAN and other networks

Types of Networks

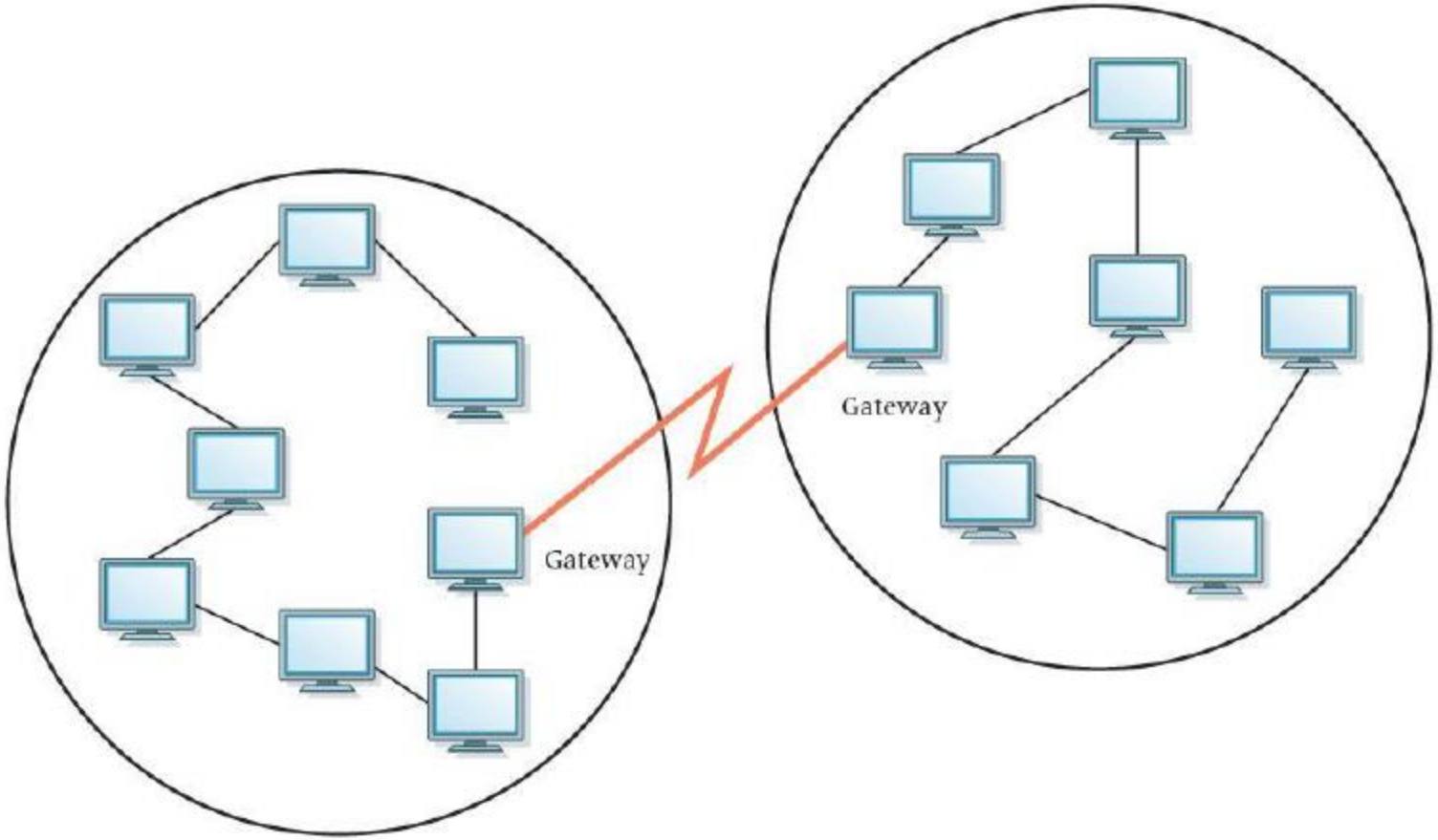


FIGURE 15.3 Local-area networks connected across a distance to create a wide-area network

Types of Networks

Internet

A wide area network that spans the planet

So, who owns the Internet?

Internet Connections

Wireless network

A network in which devices communicate with other nodes through a wireless access point

Bluetooth

A technology used for wireless communication over short distances

Internet Connections

Internet backbone

A set of high-speed networks that carry Internet traffic, provided by companies such as AT&T, Verizon, GTE, British Telecom, and IBM

Internet service provider (ISP)

An organization providing access to the Internet

Internet Connections

Various technologies available to connect a home computer to the Internet

Phone modem converts computer data into an analog audio signal for transfer over a telephone line, and then a modem at the destination converts it back again into data

Digital subscriber line (DSL) uses regular copper phone lines to transfer digital data to and from the phone company's central office

Cable modem uses the same line that your cable TV signals come in on to transfer the data back and forth

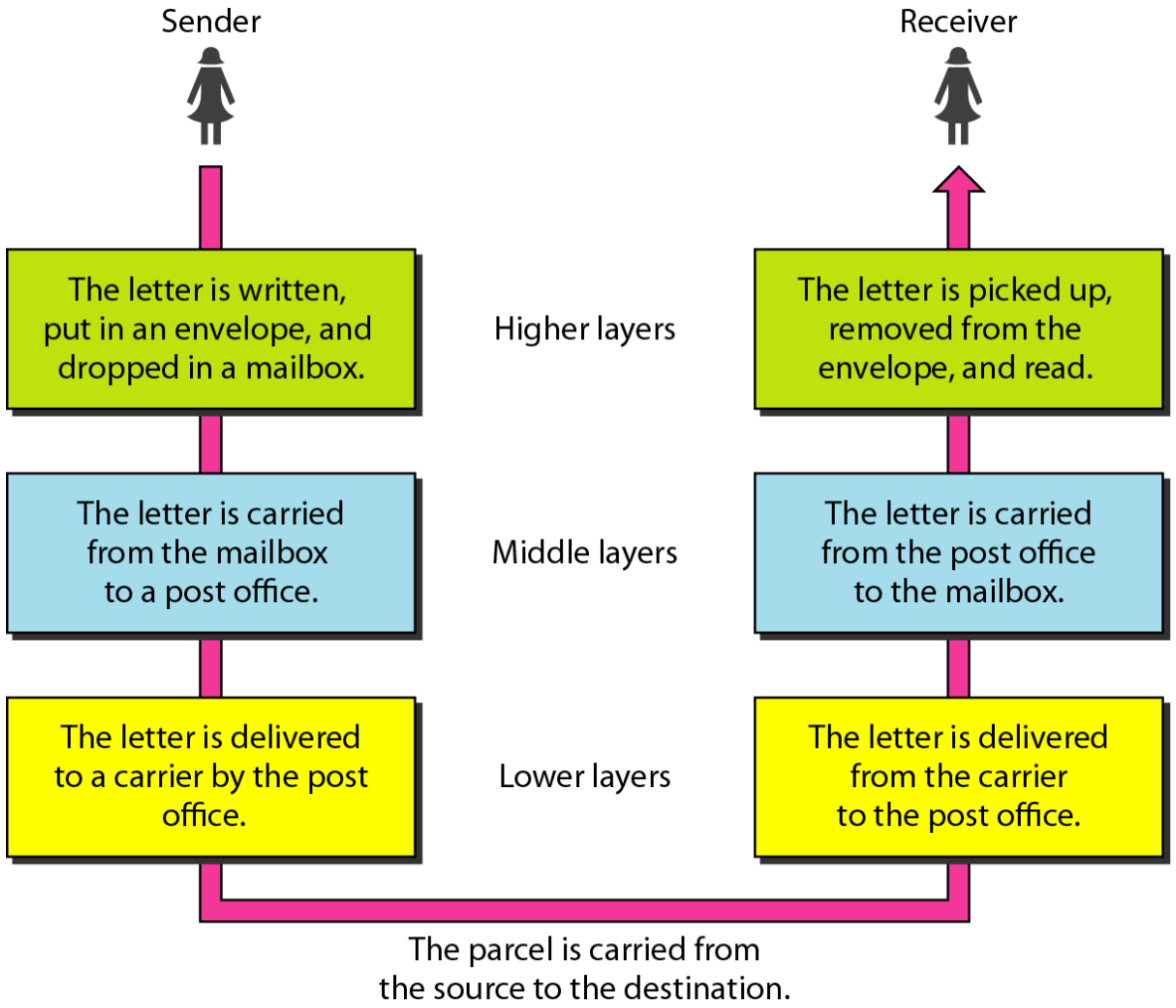
Internet Connections

Broadband

A connection in which transfer speeds are faster than 768 kilobits per second

- DSL connections and cable modems are broadband connections
- The speed for **downloads** (getting data from the Internet to your home computer) may not be the same as **uploads** (sending data from your home computer to the Internet)

Figure 2.1 Tasks involved in sending a letter



2-2 THE OSI MODEL

Established in 1947, the International Standards Organization (ISO) is a multinational body dedicated to worldwide agreement on international standards. An ISO standard that covers all aspects of network communications is the Open Systems Interconnection (OSI) model. It was first introduced in the late 1970s.

Topics discussed in this section:

Layered Architecture
Peer-to-Peer Processes
Encapsulation

Note

ISO is the organization.
OSI is the model.

Figure 2.2 *Seven layers of the OSI model*

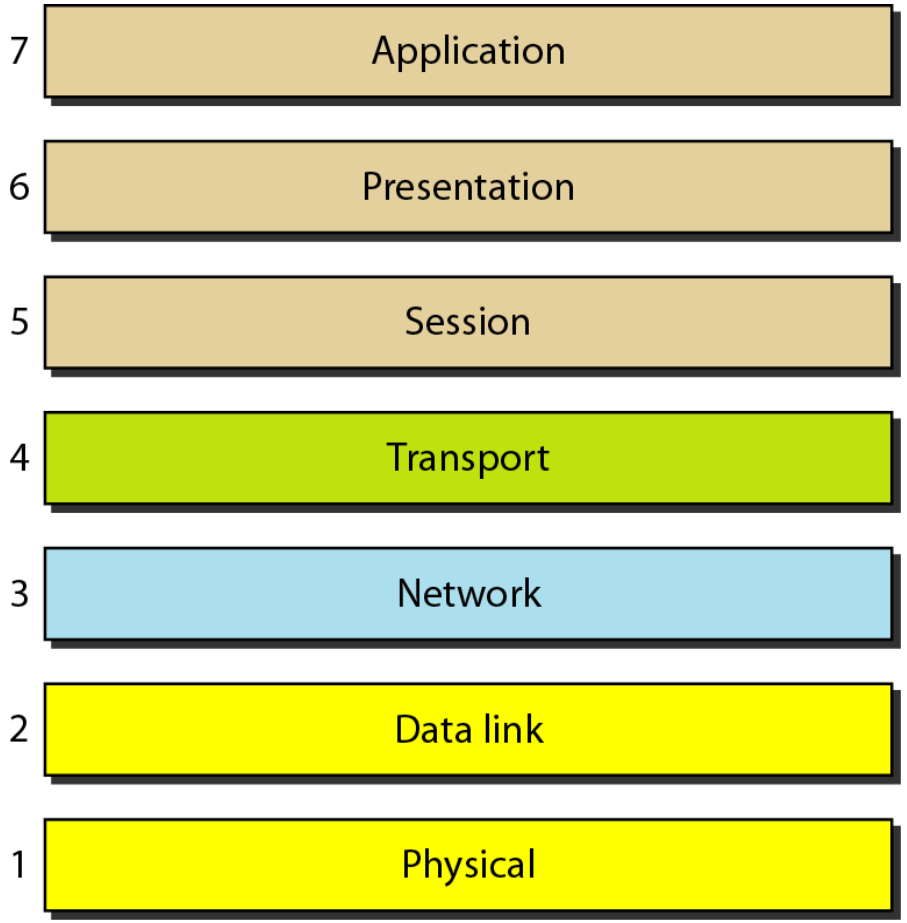


Figure 2.3 *The interaction between layers in the OSI model*

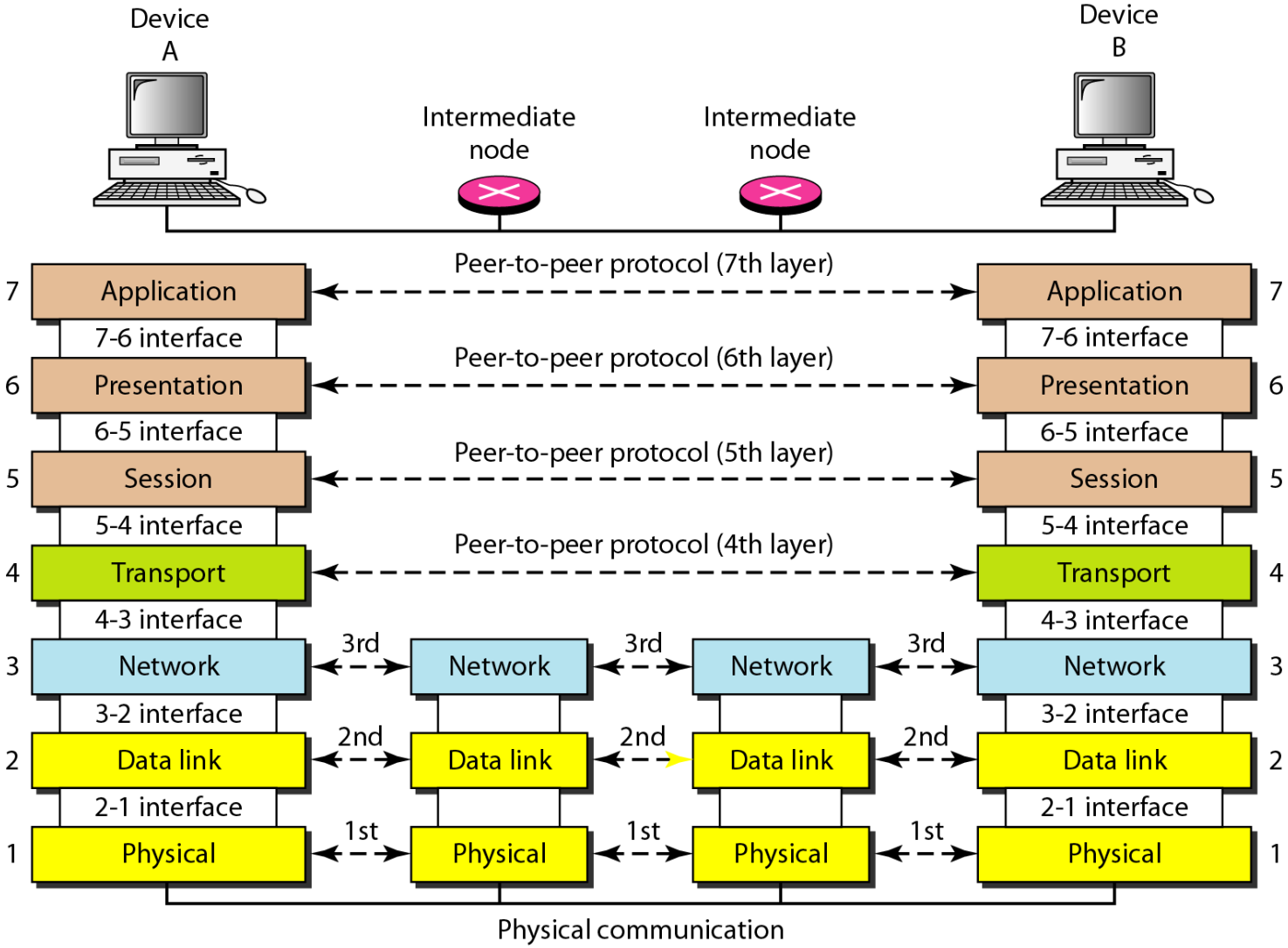
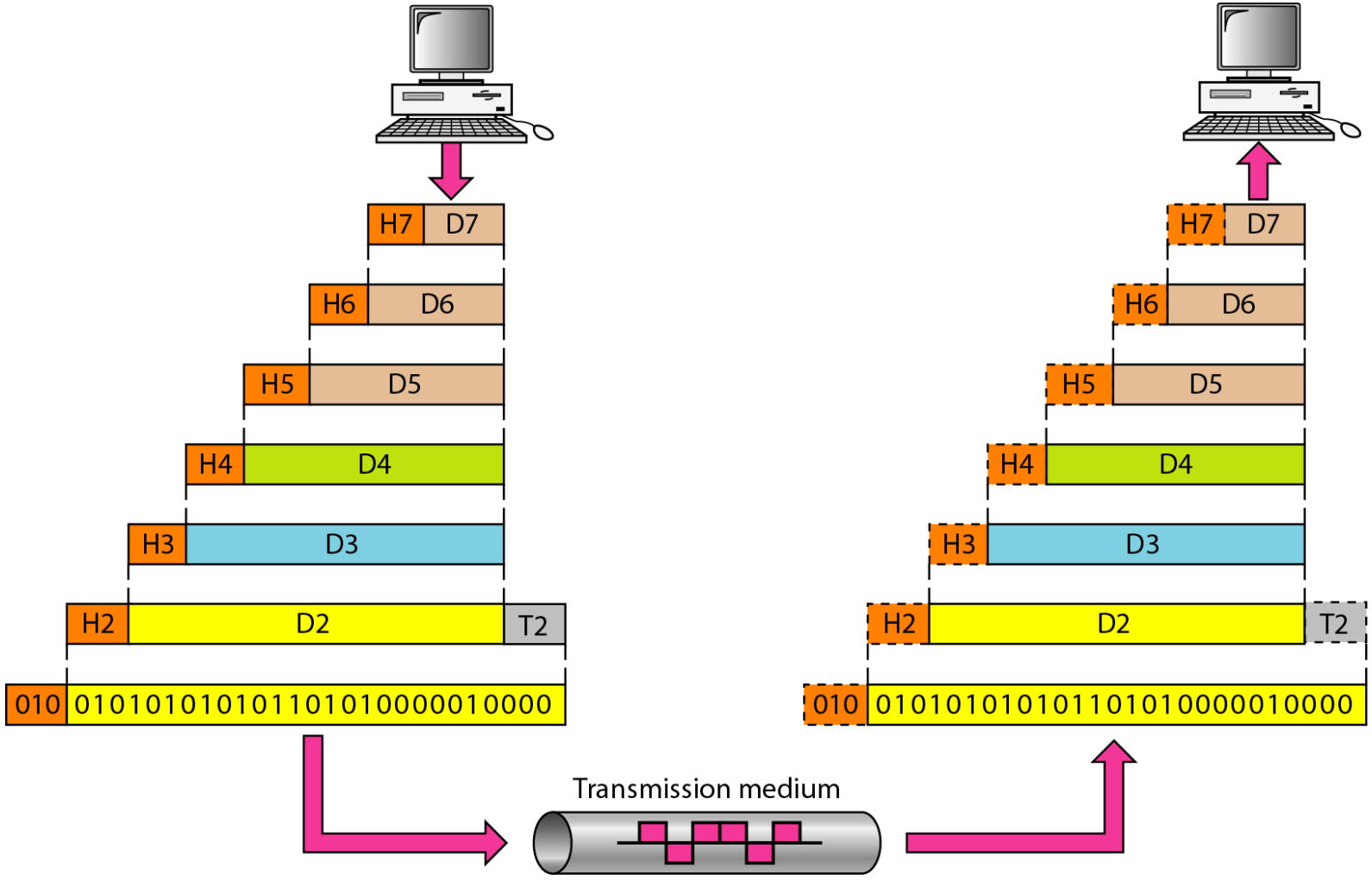


Figure 2.4 *An exchange using the OSI model*



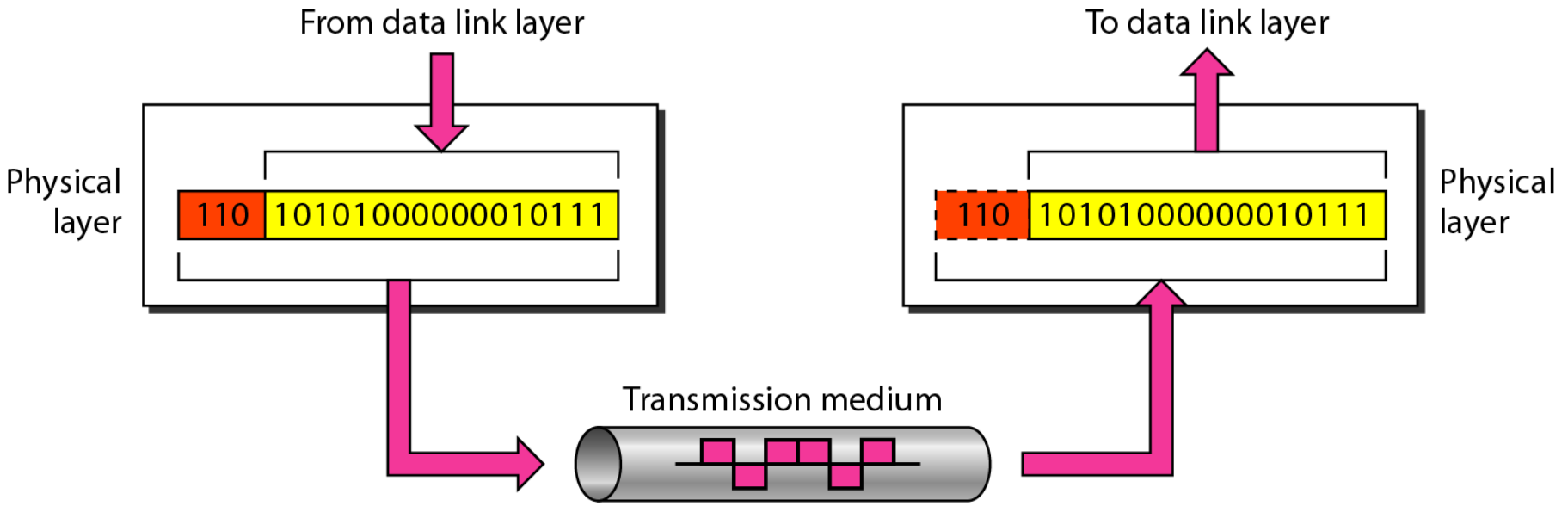
2-3 LAYERS IN THE OSI MODEL

In this section we briefly describe the functions of each layer in the OSI model.

Topics discussed in this section:

- Physical Layer
- Data Link Layer
- Network Layer
- Transport Layer
- Session Layer
- Presentation Layer
- Application Layer

Figure 2.5 *Physical layer*



Note

The physical layer is responsible for movements of individual bits from one hop (node) to the next.

Figure 2.6 *Data link layer*

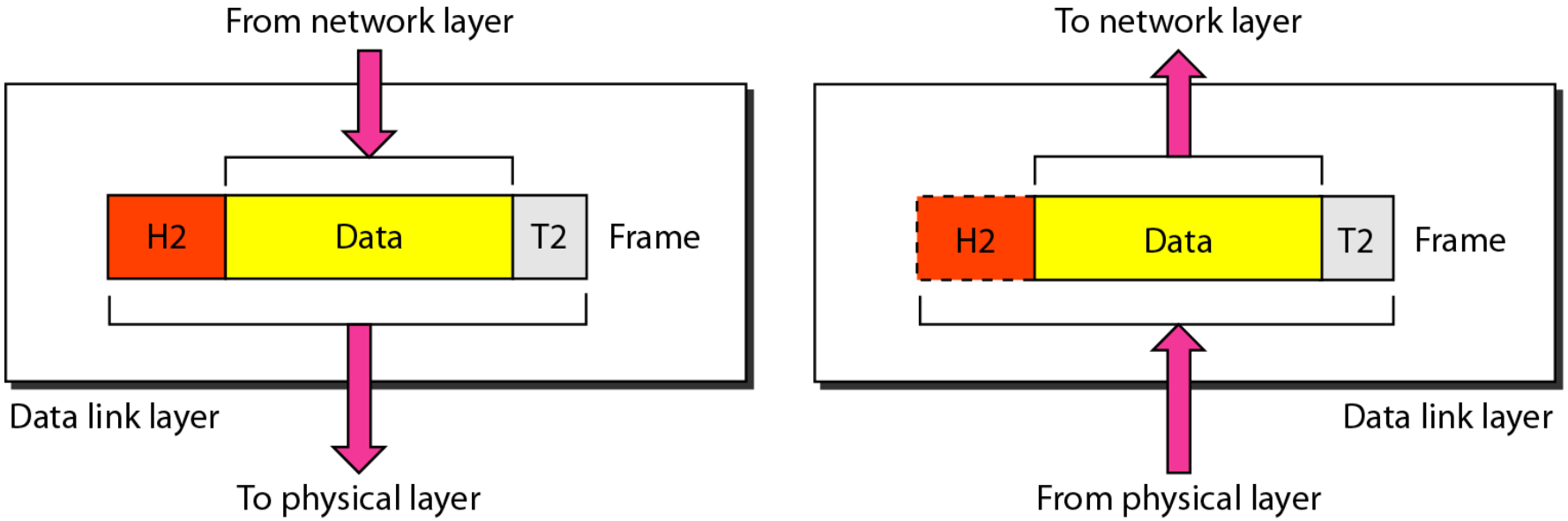


Figure 2.7 *Hop-to-hop delivery*

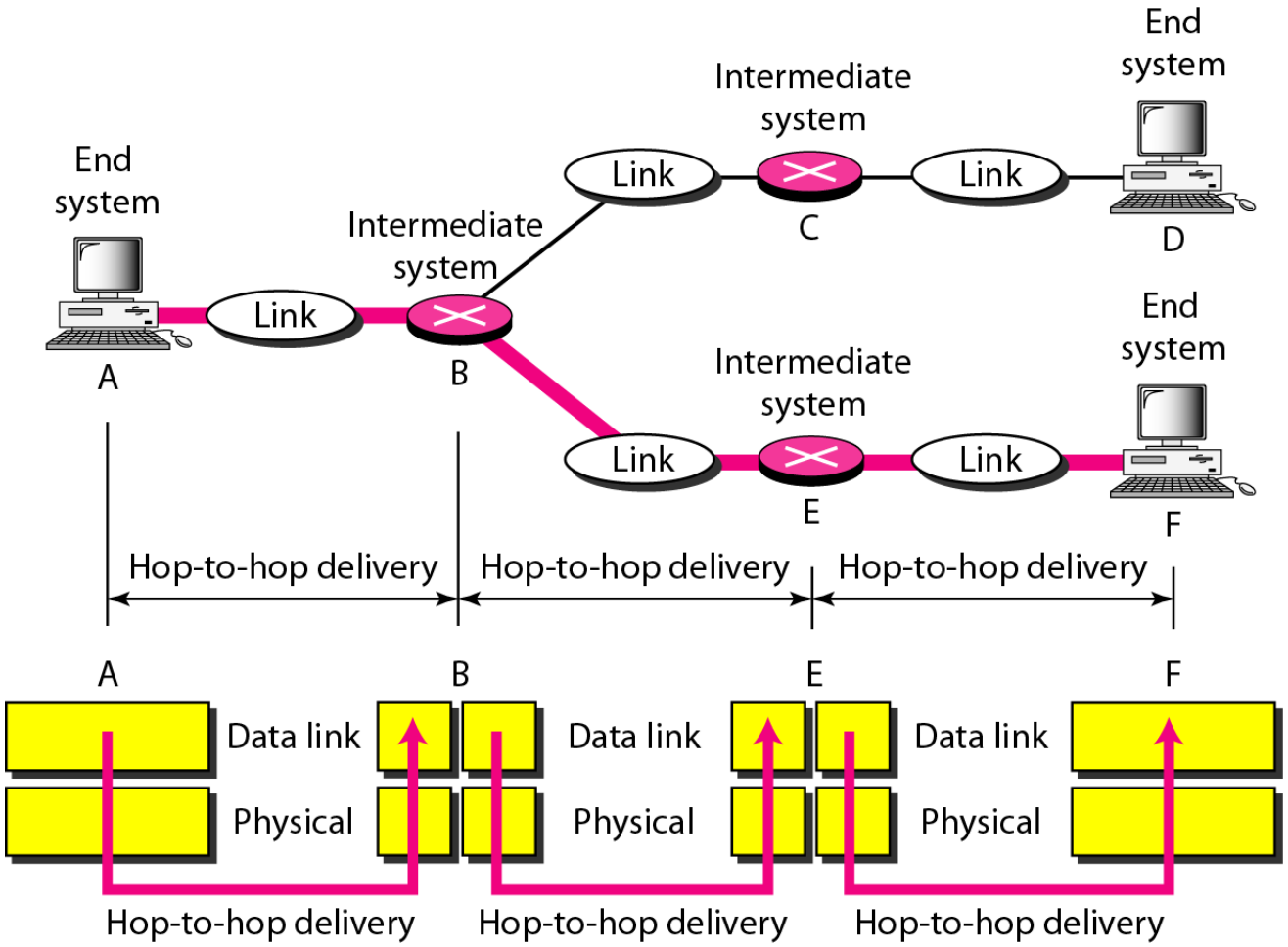
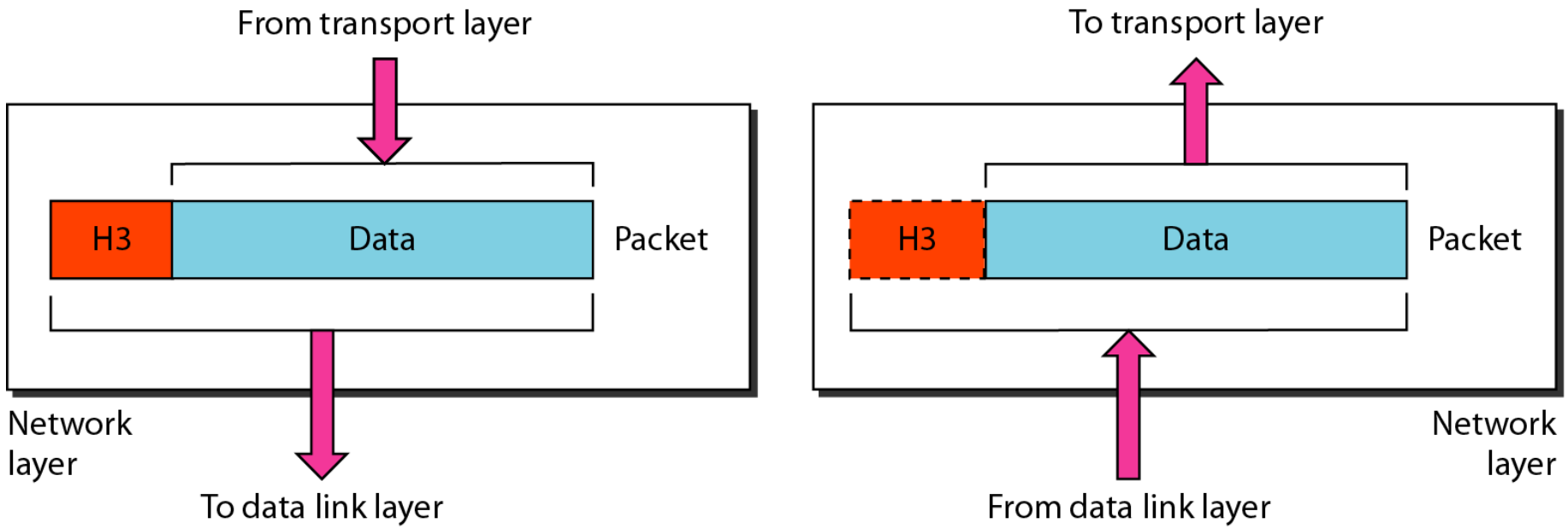


Figure 2.8 *Network layer*



Note

The network layer is responsible for the delivery of individual packets from the source host to the destination host.

Figure 2.9 *Source-to-destination delivery*

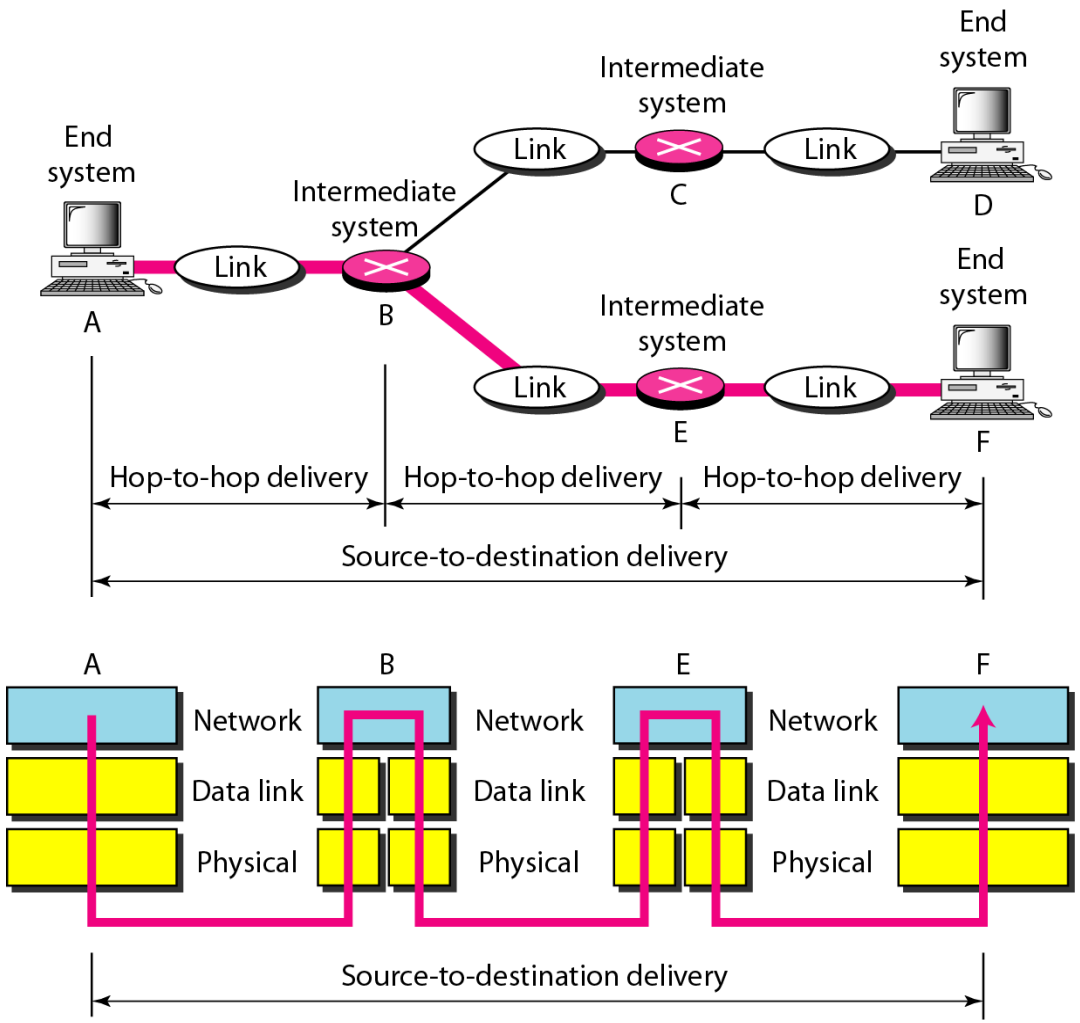
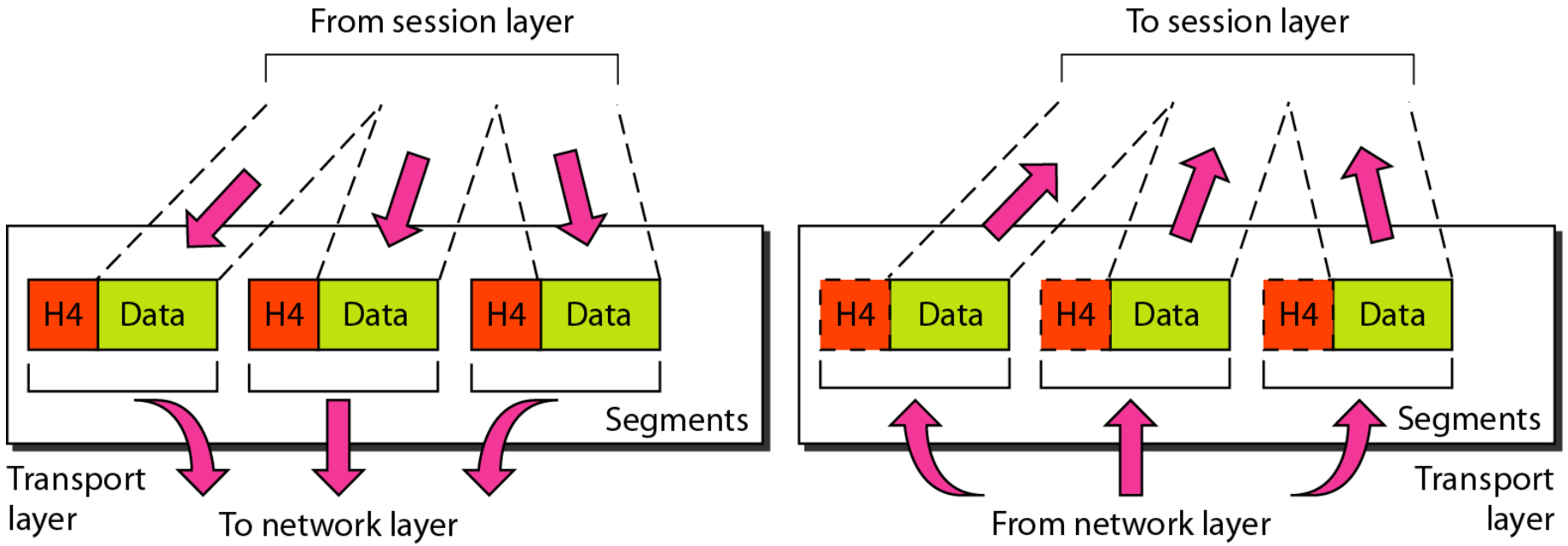


Figure 2.10 *Transport layer*



Note

The transport layer is responsible for the delivery of a message from one process to another.

Figure 2.11 *Reliable process-to-process delivery of a message*

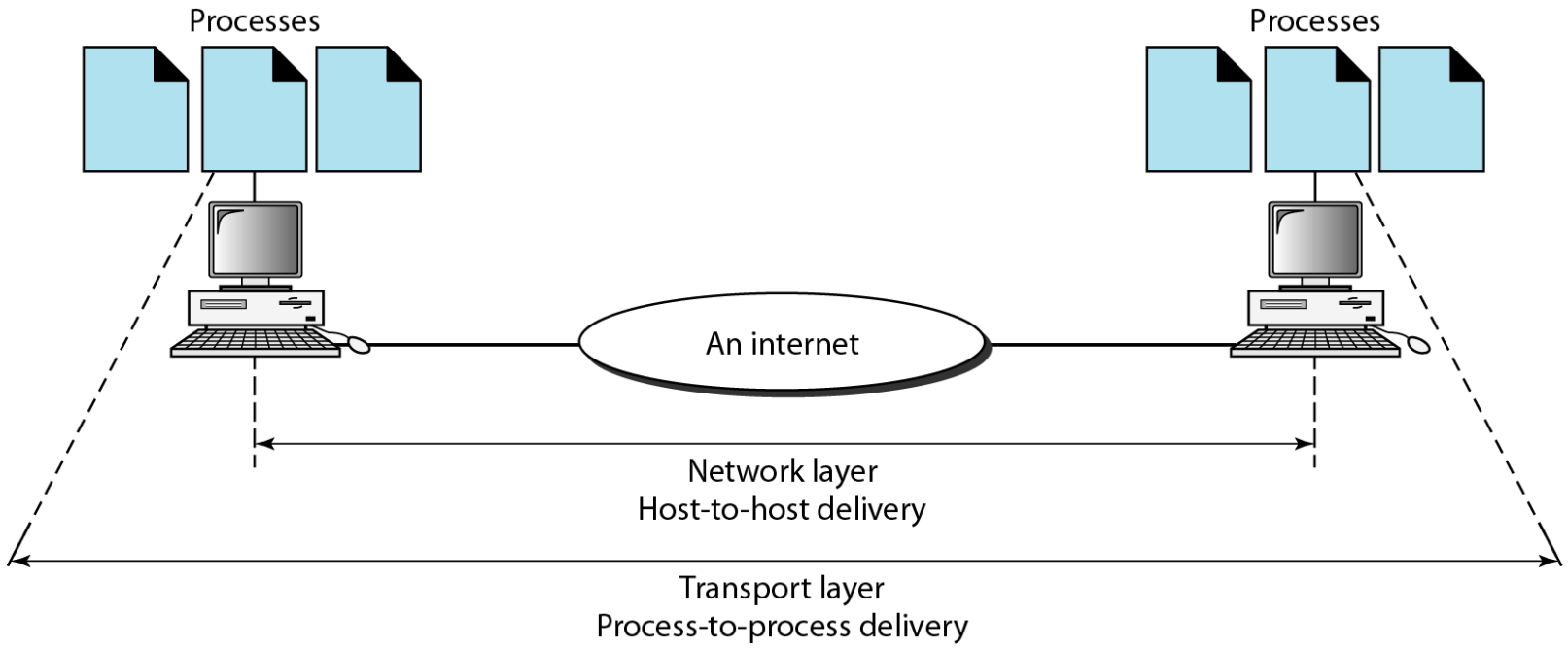
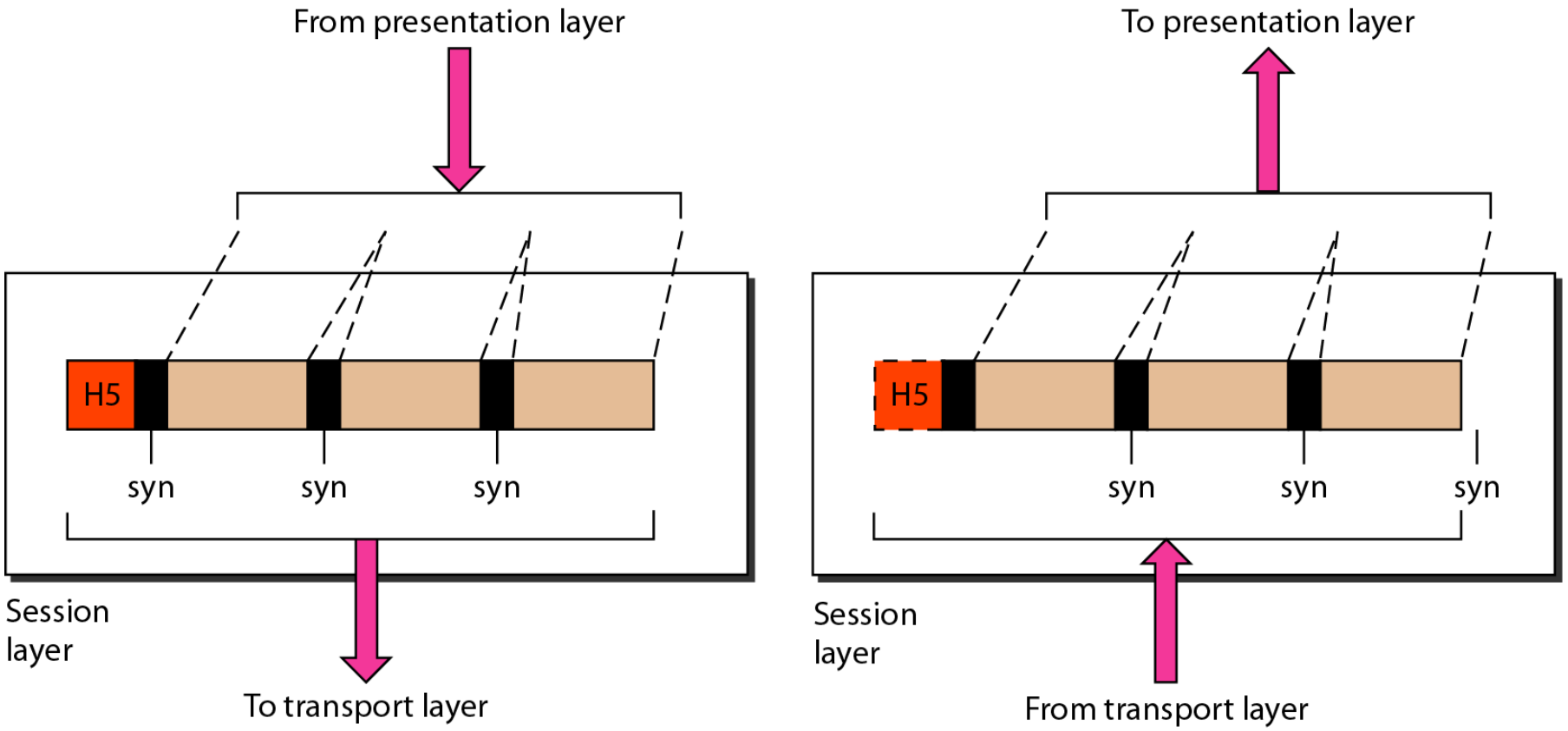


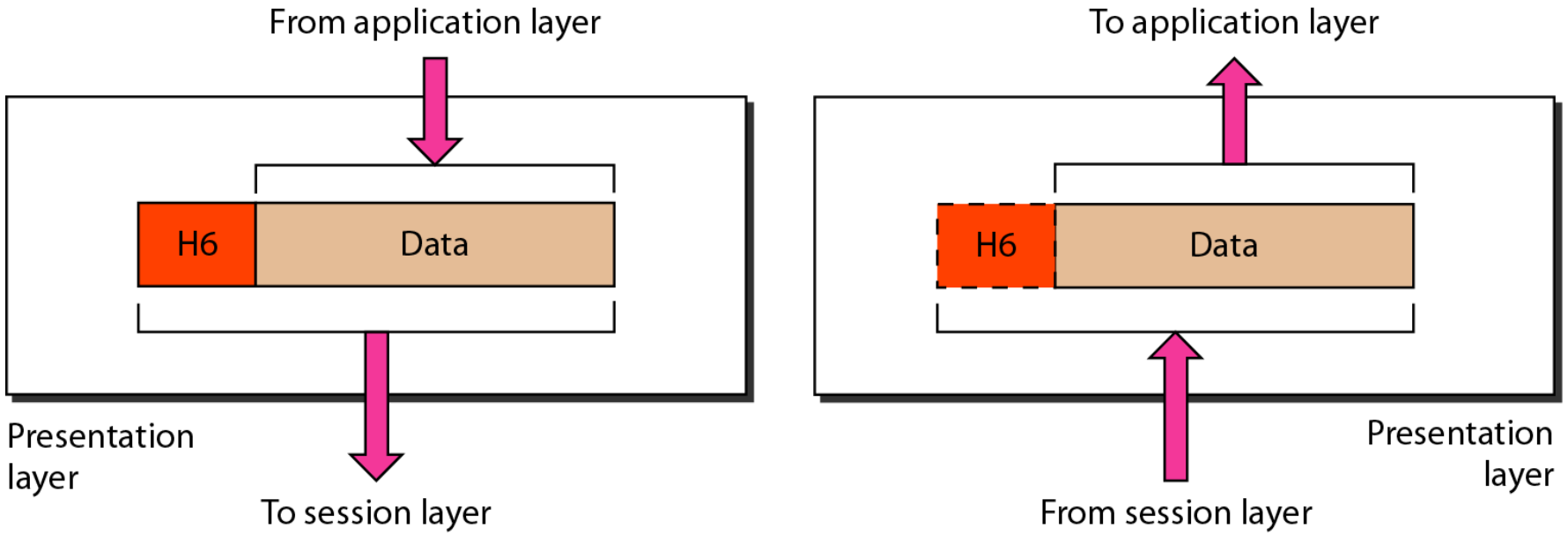
Figure 2.12 *Session layer*



Note

The session layer is responsible for dialog control and synchronization.

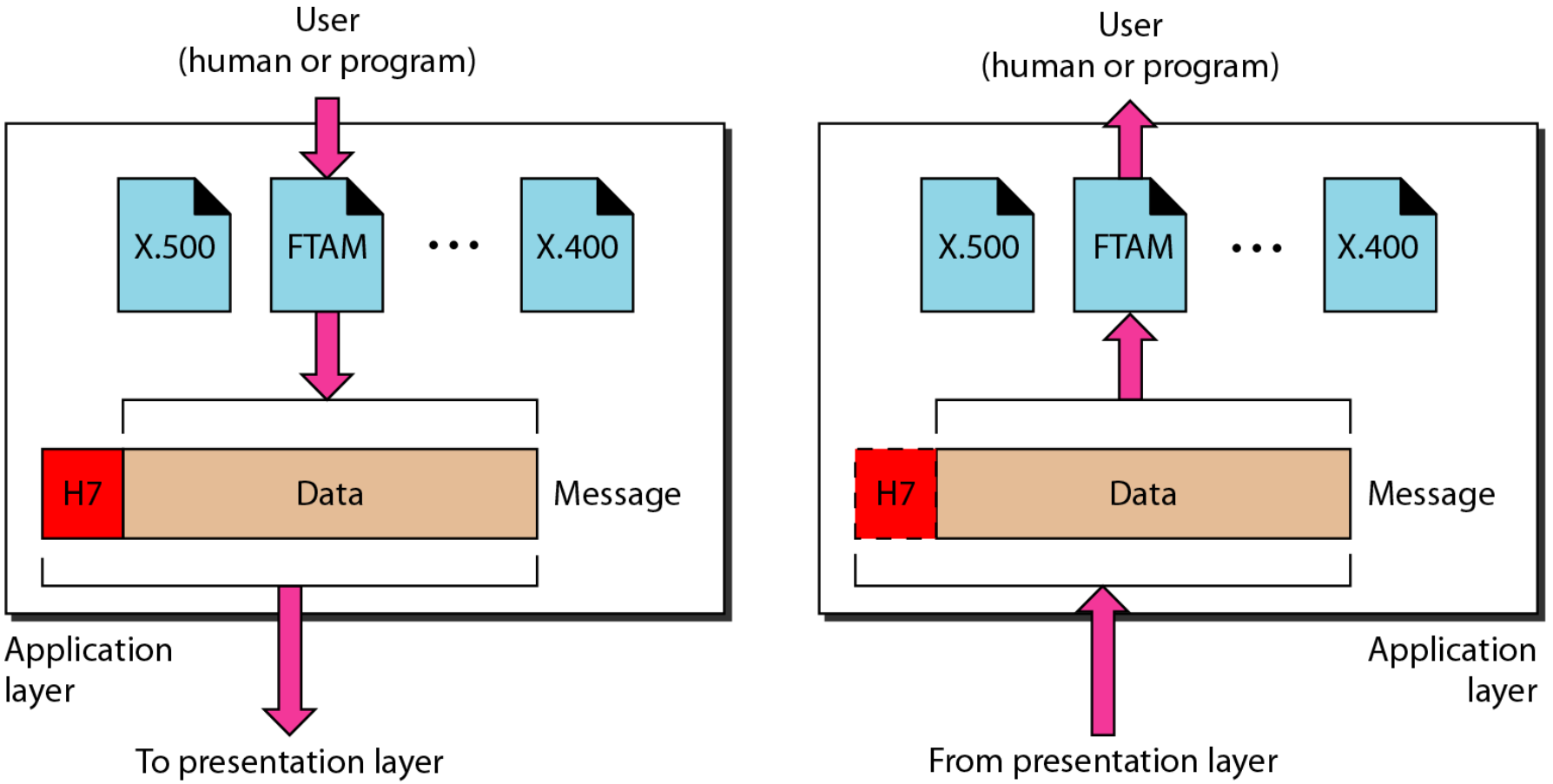
Figure 2.13 *Presentation layer*



Note

The presentation layer is responsible for translation, compression, and encryption.

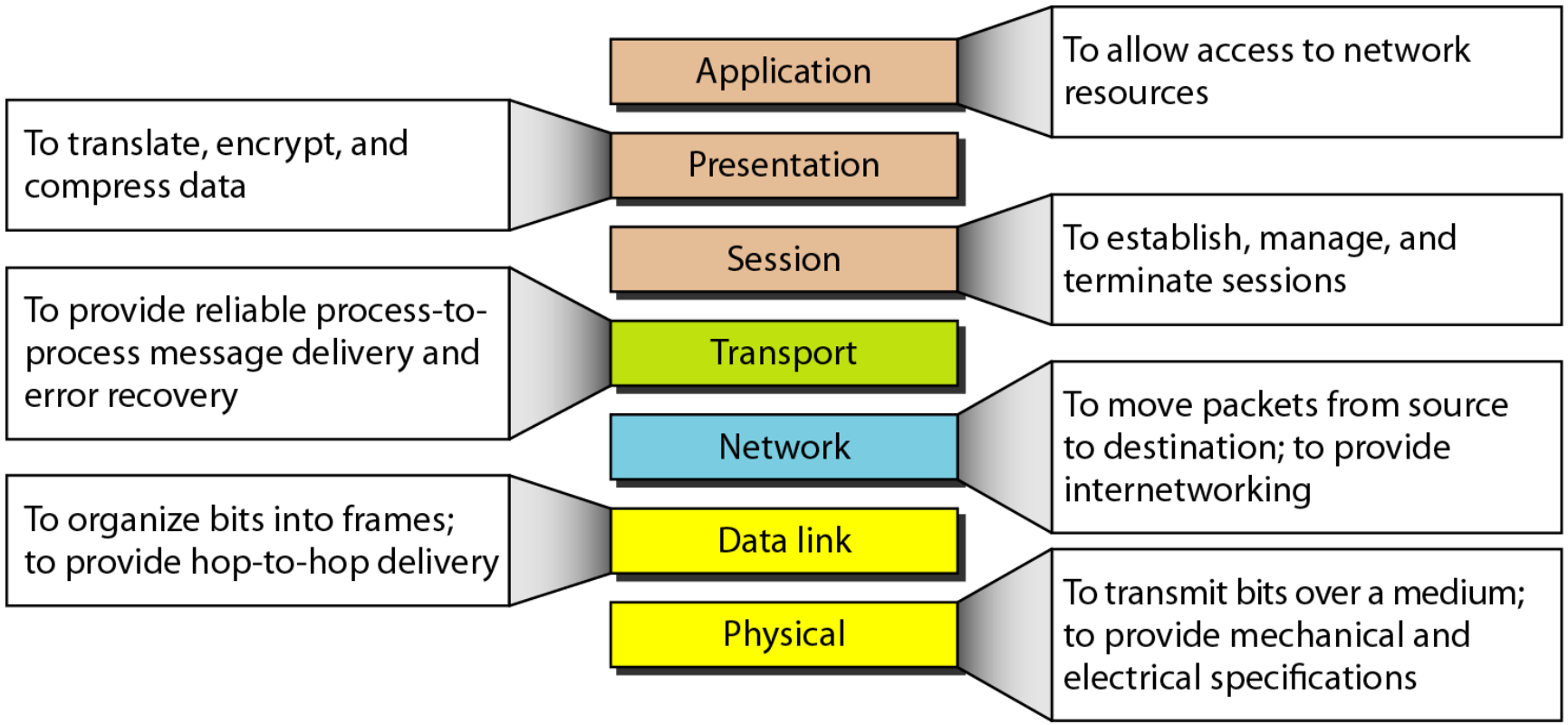
Figure 2.14 *Application layer*



Note

The application layer is responsible for providing services to the user.

Figure 2.15 *Summary of layers*



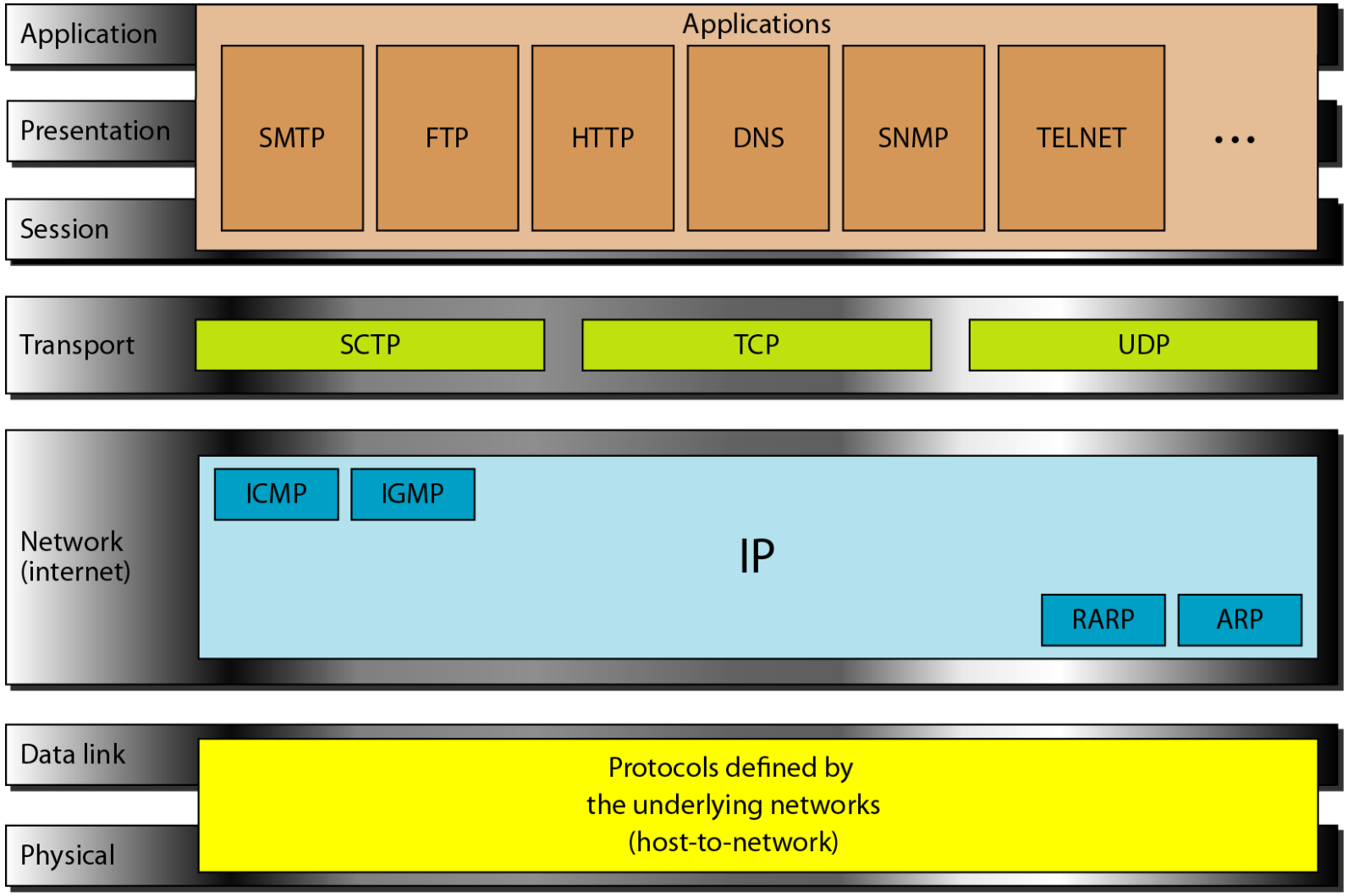
2-4 TCP/IP PROTOCOL SUITE

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.

Topics discussed in this section:

Physical and Data Link Layers
Network Layer
Transport Layer
Application Layer

Figure 2.16 *TCP/IP and OSI model*



2-5 ADDRESSING

Four levels of addresses are used in an internet employing the TCP/IP protocols: physical, logical, port, and specific.

Topics discussed in this section:

Physical Addresses
Logical Addresses
Port Addresses
Specific Addresses

Figure 2.17 *Addresses in TCP/IP*

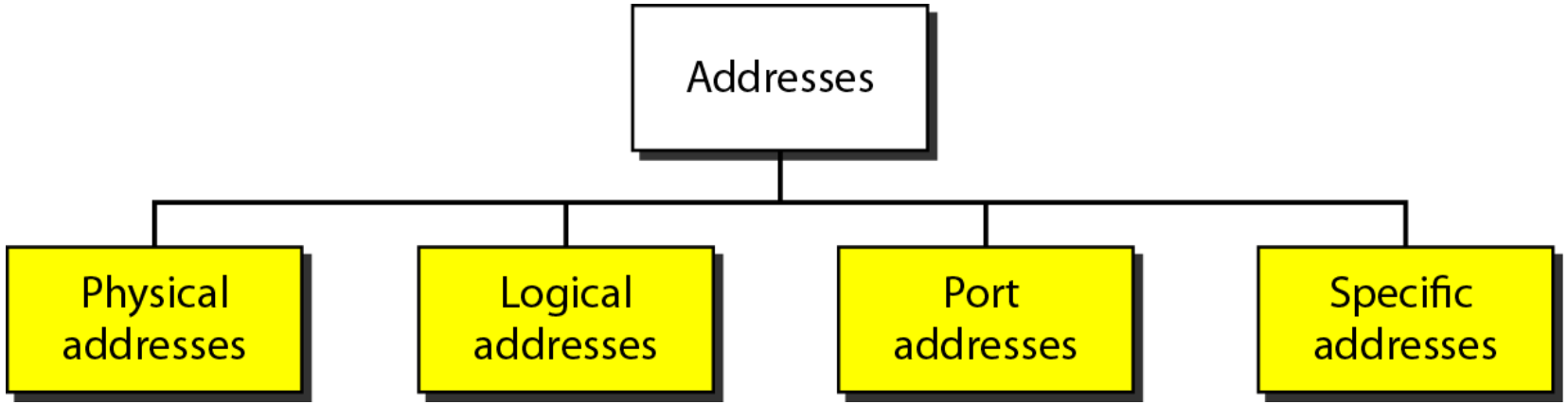
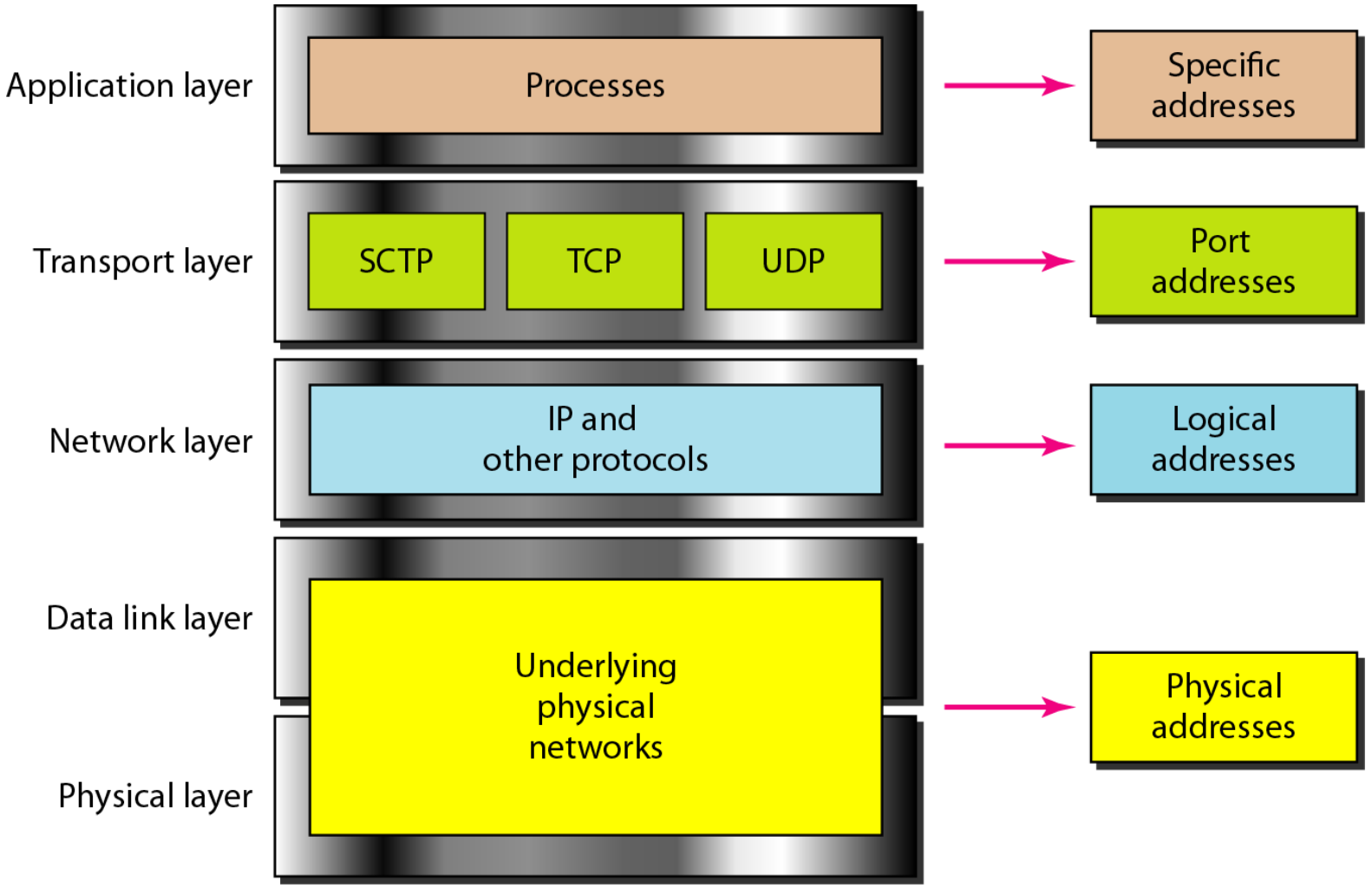


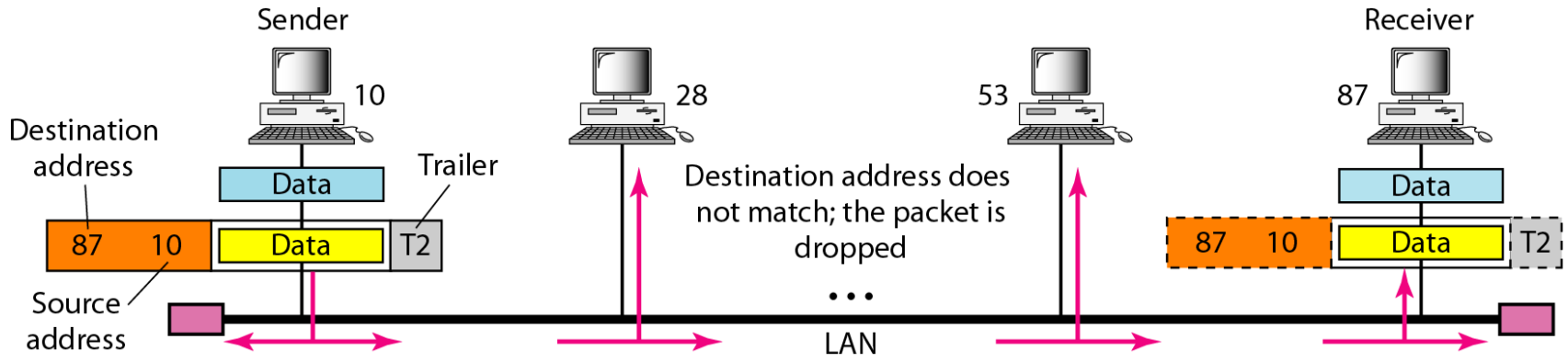
Figure 2.18 *Relationship of layers and addresses in TCP/IP*



Example 2.1

In Figure 2.19 a node with physical address 10 sends a frame to a node with physical address 87. The two nodes are connected by a link (bus topology LAN). As the figure shows, the computer with physical address 10 is the sender, and the computer with physical address 87 is the receiver.

Figure 2.19 *Physical addresses*



Example 2.2

Most local-area networks use a 48-bit (6-byte) physical address written as 12 hexadecimal digits; every byte (2 hexadecimal digits) is separated by a colon, as shown below:

07:01:02:01:2C:4B

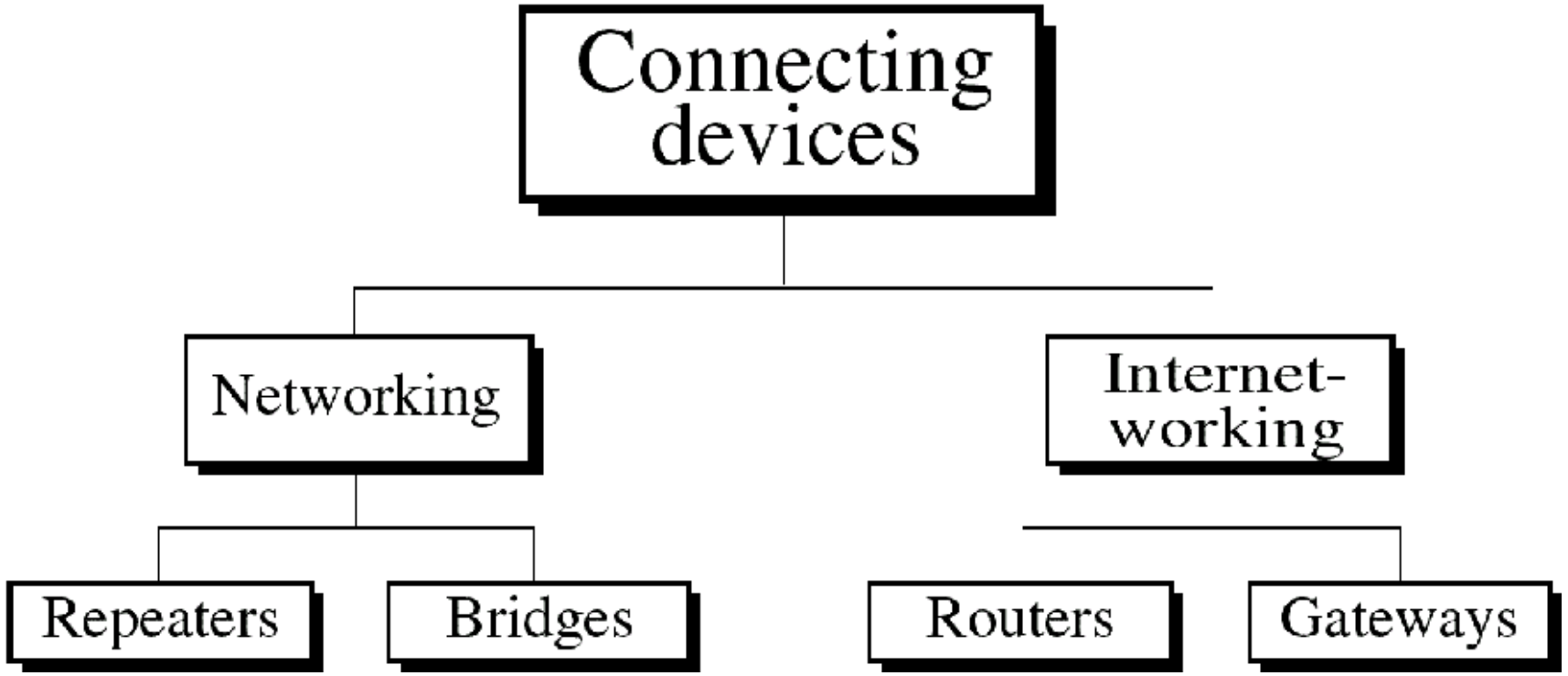
A 6-byte (12 hexadecimal digits) physical address.

Networking and Internetworking Devices(cont'd)

- An internet is an interconnection of individual networks. To creates an internet, we need internetworking devices called routers and gateways.
- An internet is different from the Internet.
- Internet is the name of a specific worldwide network.

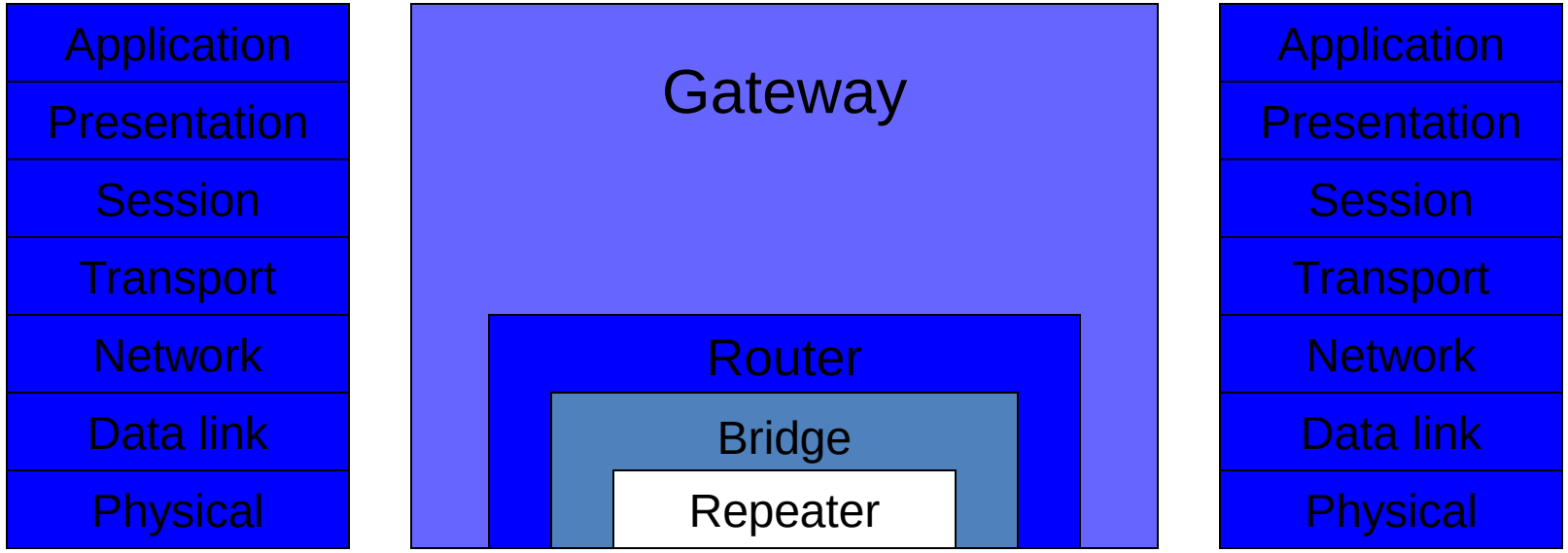
Networking and Internetworking Devices(cont'd)

- Connecting device



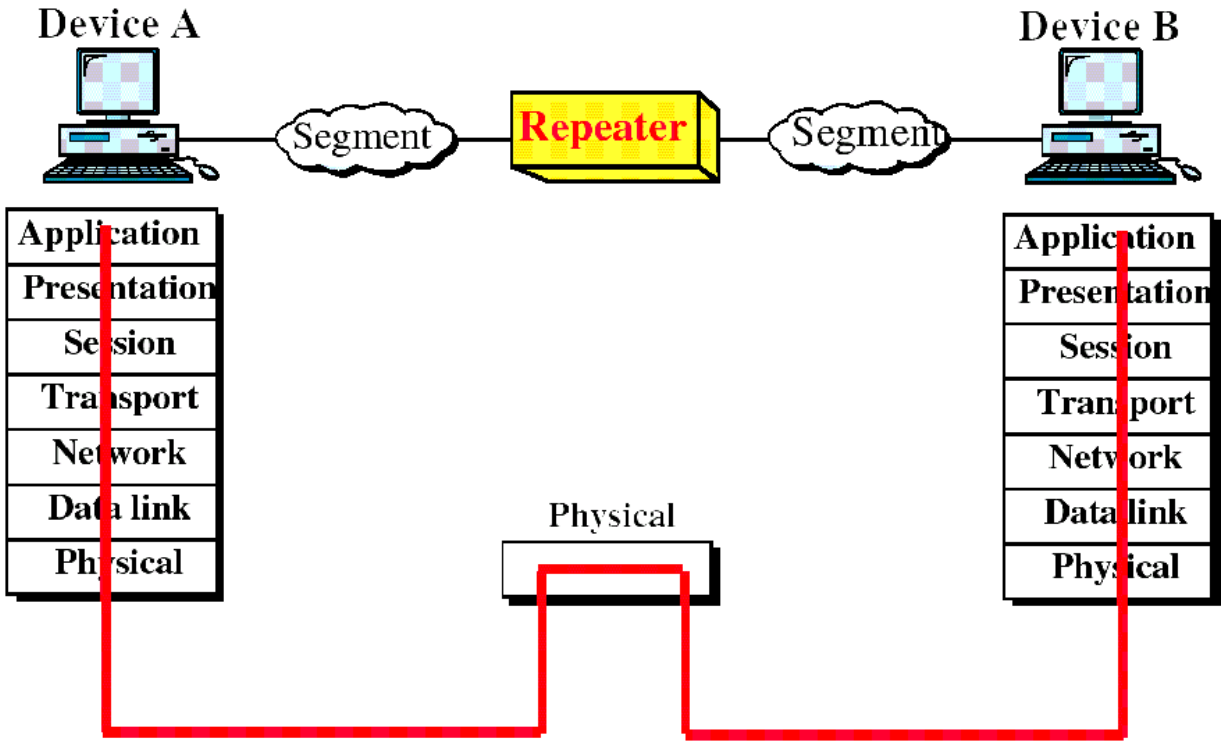
Networking and Internetworking Devices(cont'd)

- Connecting devices and the OSI model



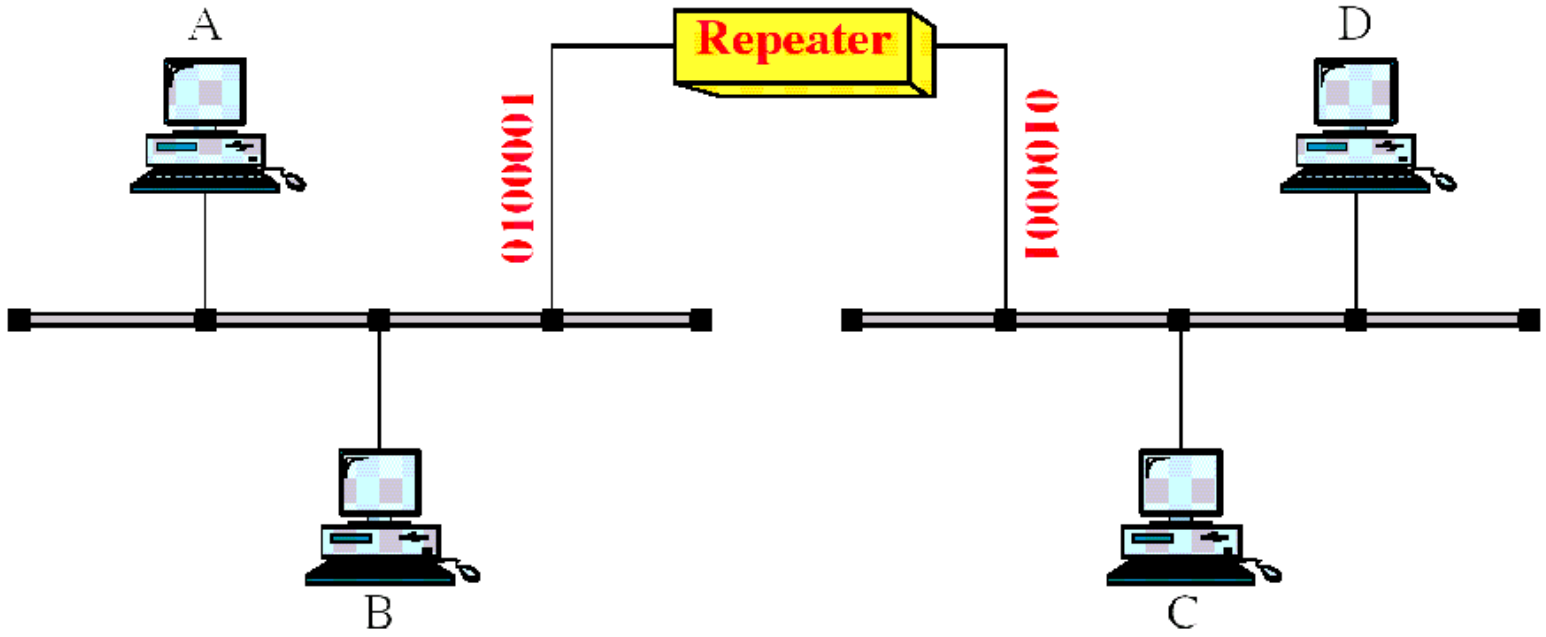
Repeaters

~ is an electronic device that operates on only the physical layer of the OSI model.



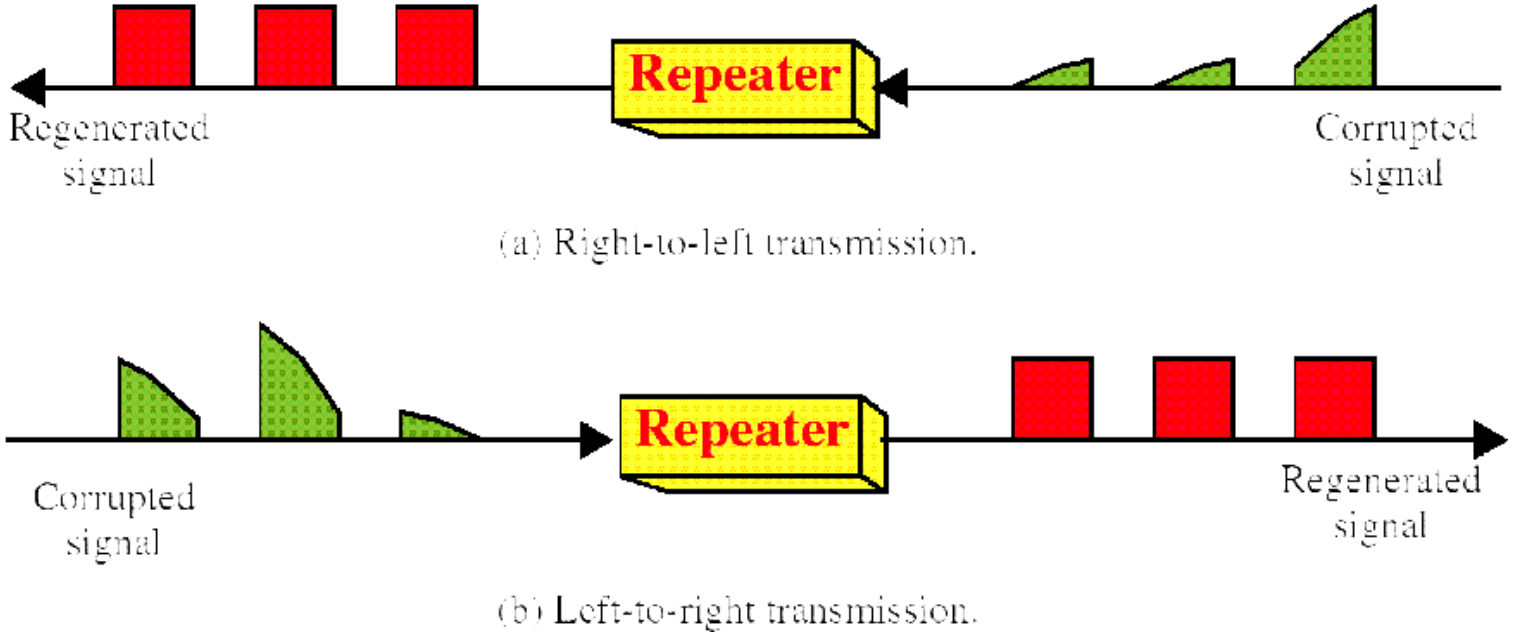
Repeaters(cont'd)

- Repeater allows us to extend only the physical length of a network.



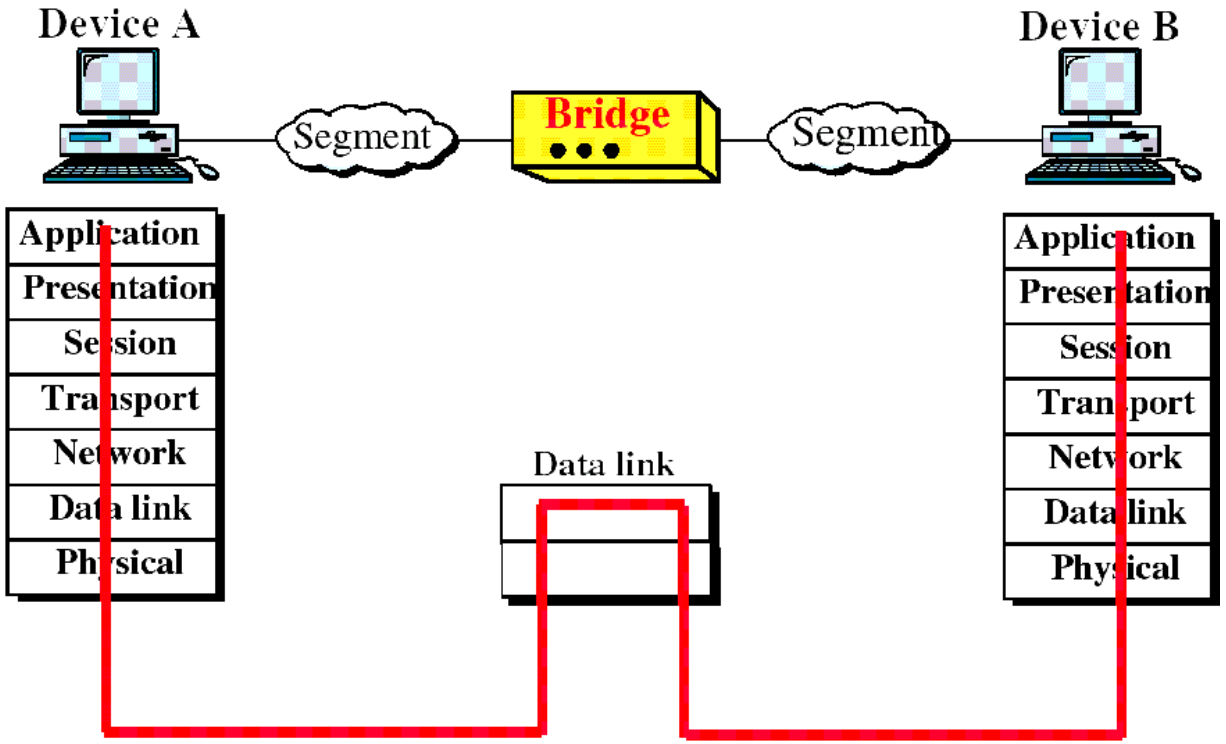
Repeaters(cont'd)

- Function of a repeater



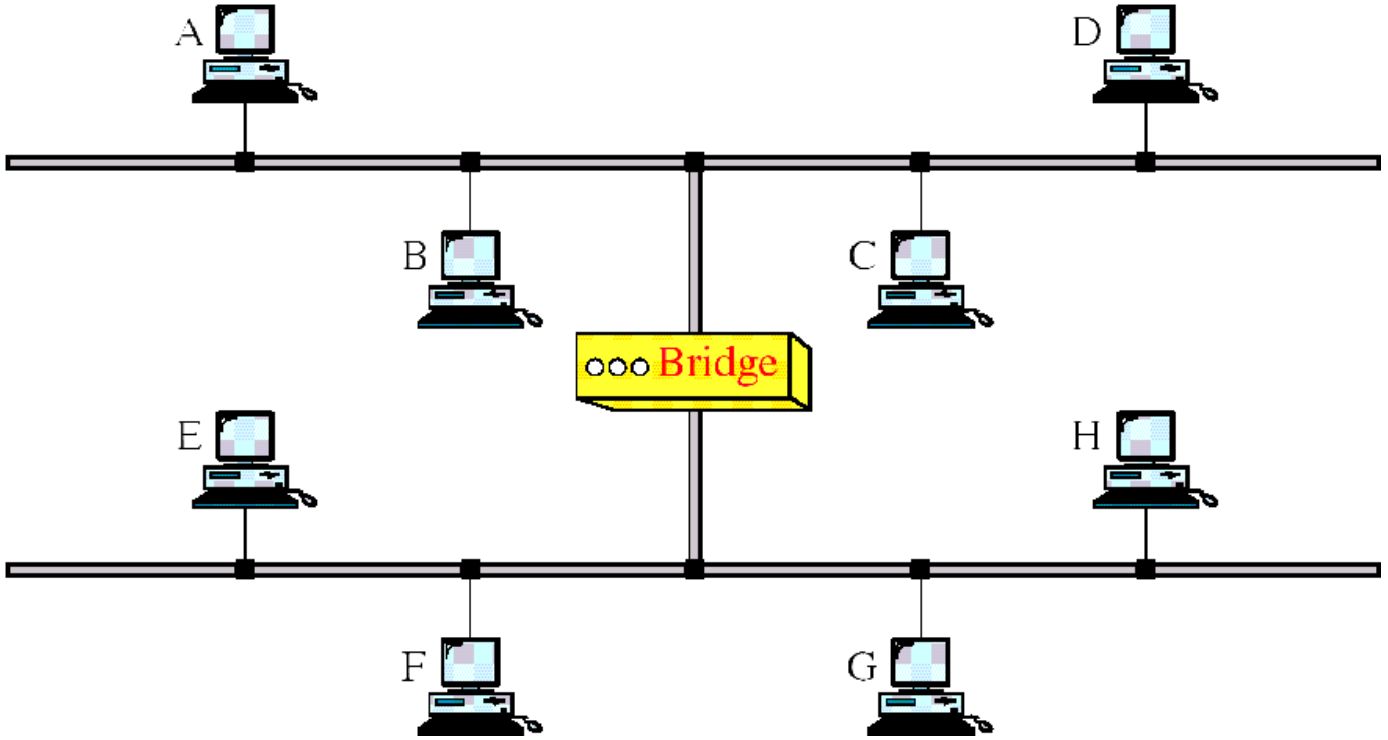
Bridges

~ operate in both the physical and the data link layers of the OSI model.



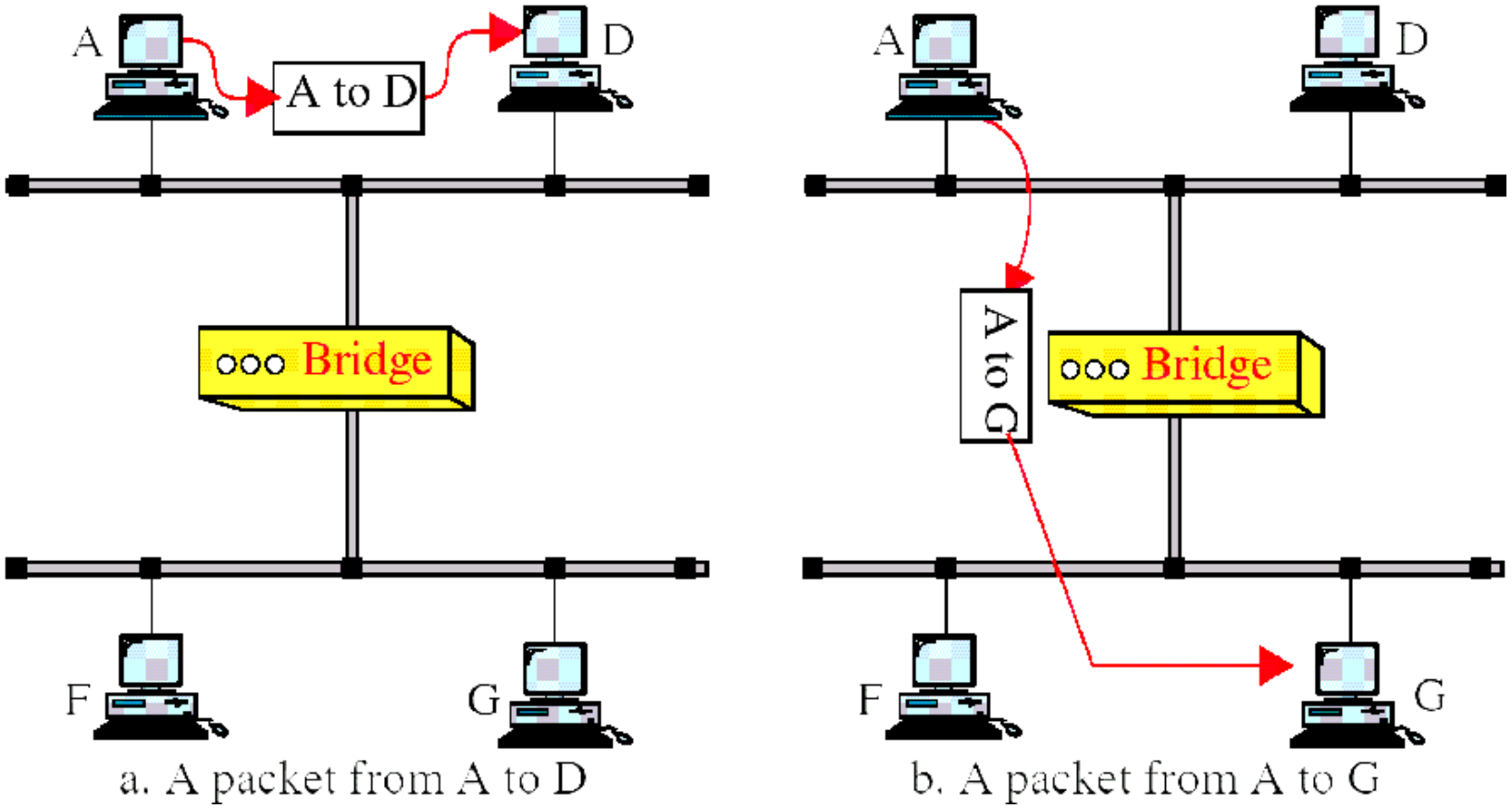
Bridges(cont'd)

- Bridges divide a large network into smaller segments



Bridges(cont'd)

- Function of a bridge

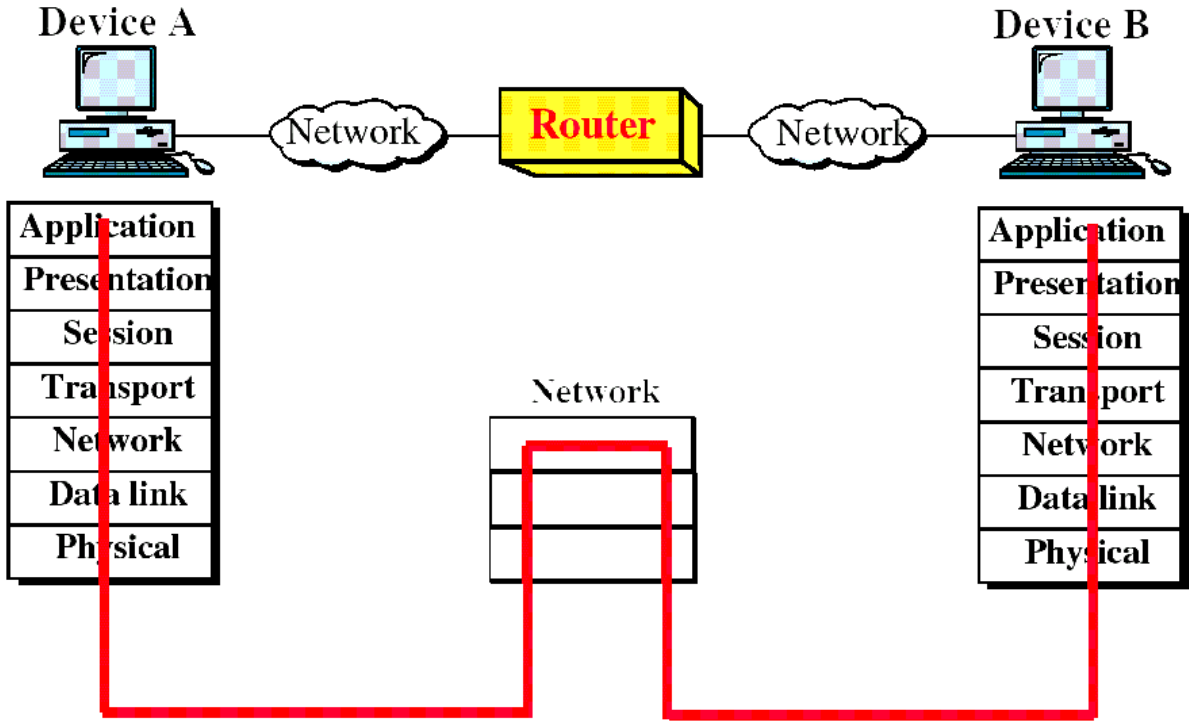


Bridges(cont'd)

- Types of Bridges
  - Simple Bridges
  - Learning Bridges
  - Multiport Bridges

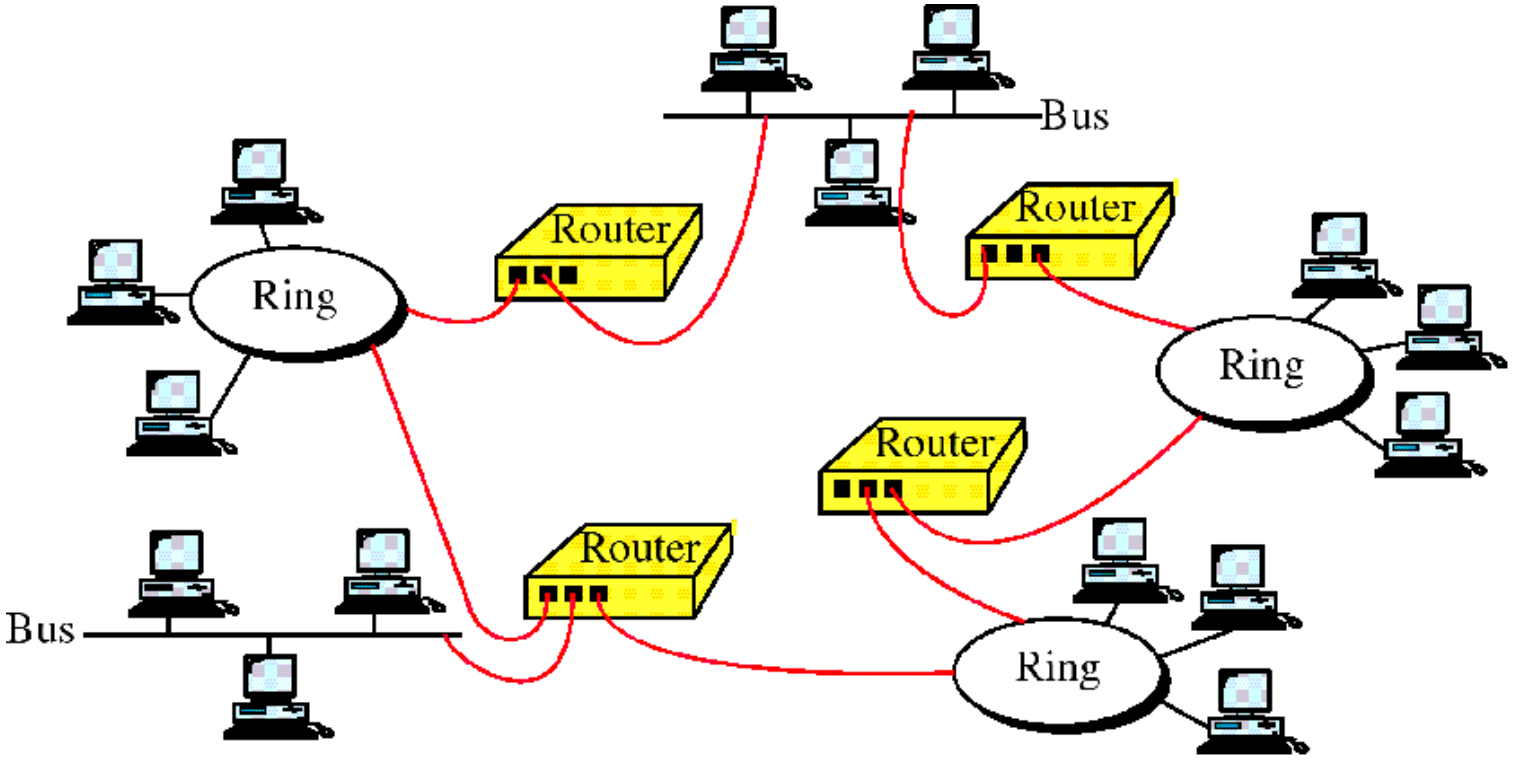
Routers

~ operate in the physical, data link, and network layers of the OSI model.



Routers(cont'd)

- Routers relay packets among multiple interconnected networks.

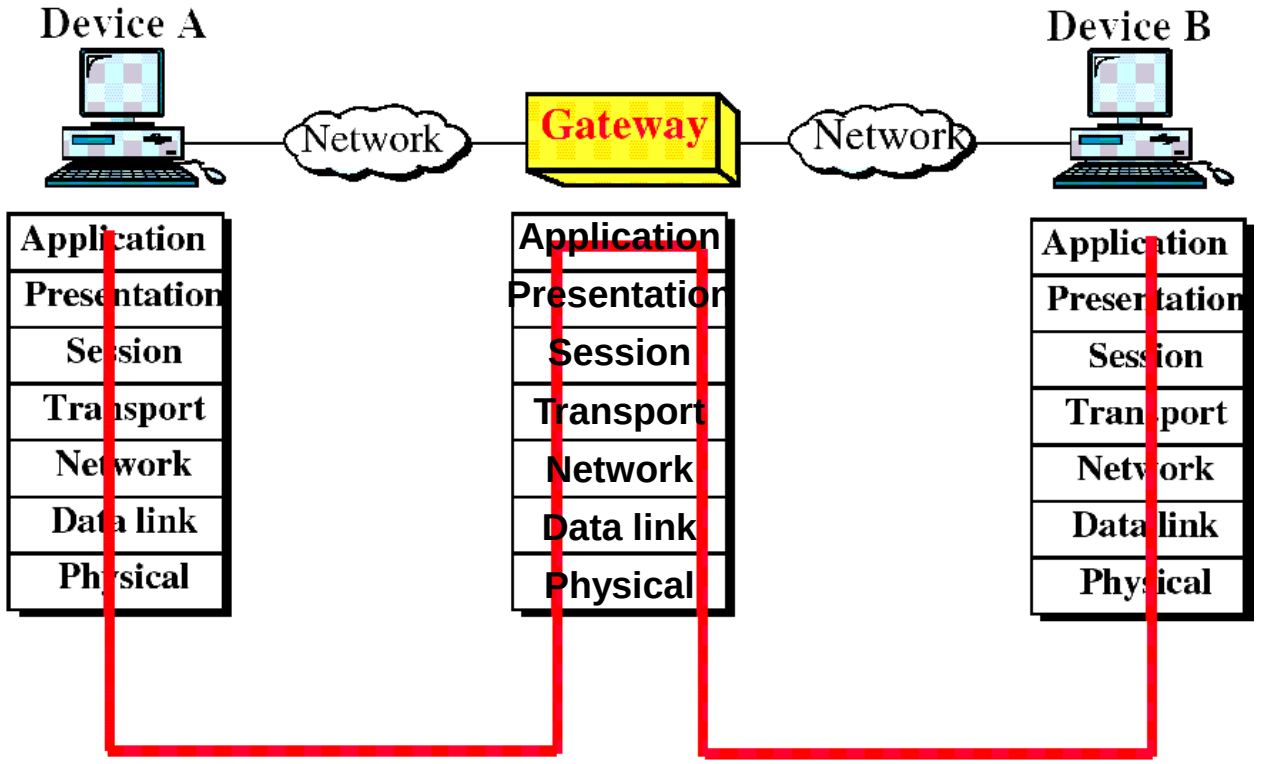


Routers(cont'd)

- Routing concepts
  - ~ Whenever there are multiple options, the router chooses the pathway.
  - – Least-Cost Routing
    - Which path does it choose?
    - Decision is based on efficiency(cheapest, fastest, shortest)
  - – Distributed Routing
  - – Packet Lifetime(number of hops)

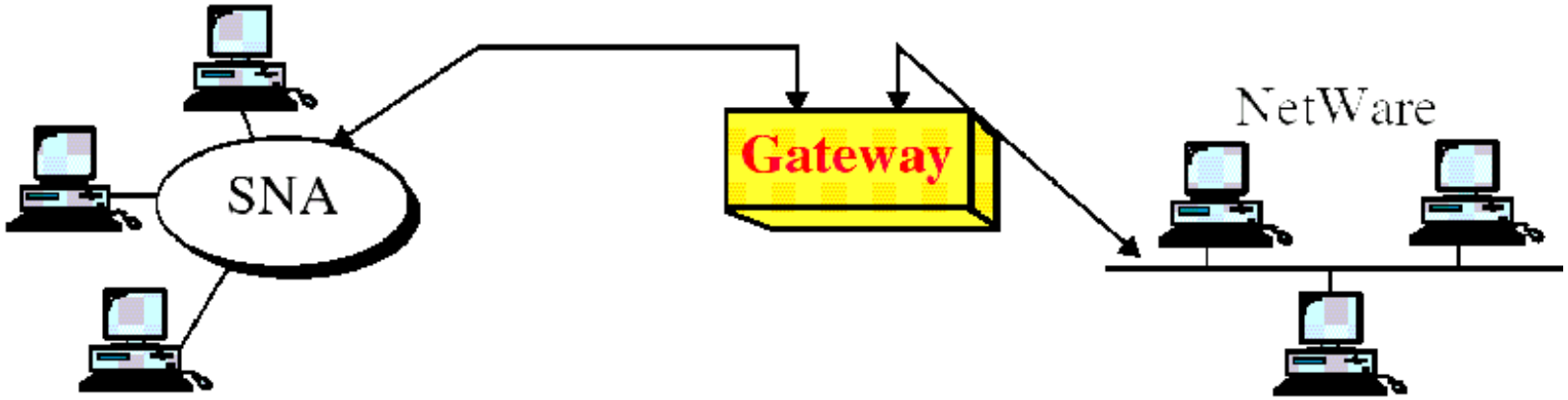
Gateways

~ potentially operate in all seven layers of the OSI model(protocol converter).



Gateways(cont'd)

- Gateway



Perimeter devices

- IDS,
- IPS,
- Firewall
- NOC,
- SOC,
- SIEM

Intrusion and Intrusion Detection

- Intrusion : Attempting to break into or misuse your system.
- Intruders may be from outside the network or legitimate users of the network.
- Intrusion can be a physical, system or remote intrusion.

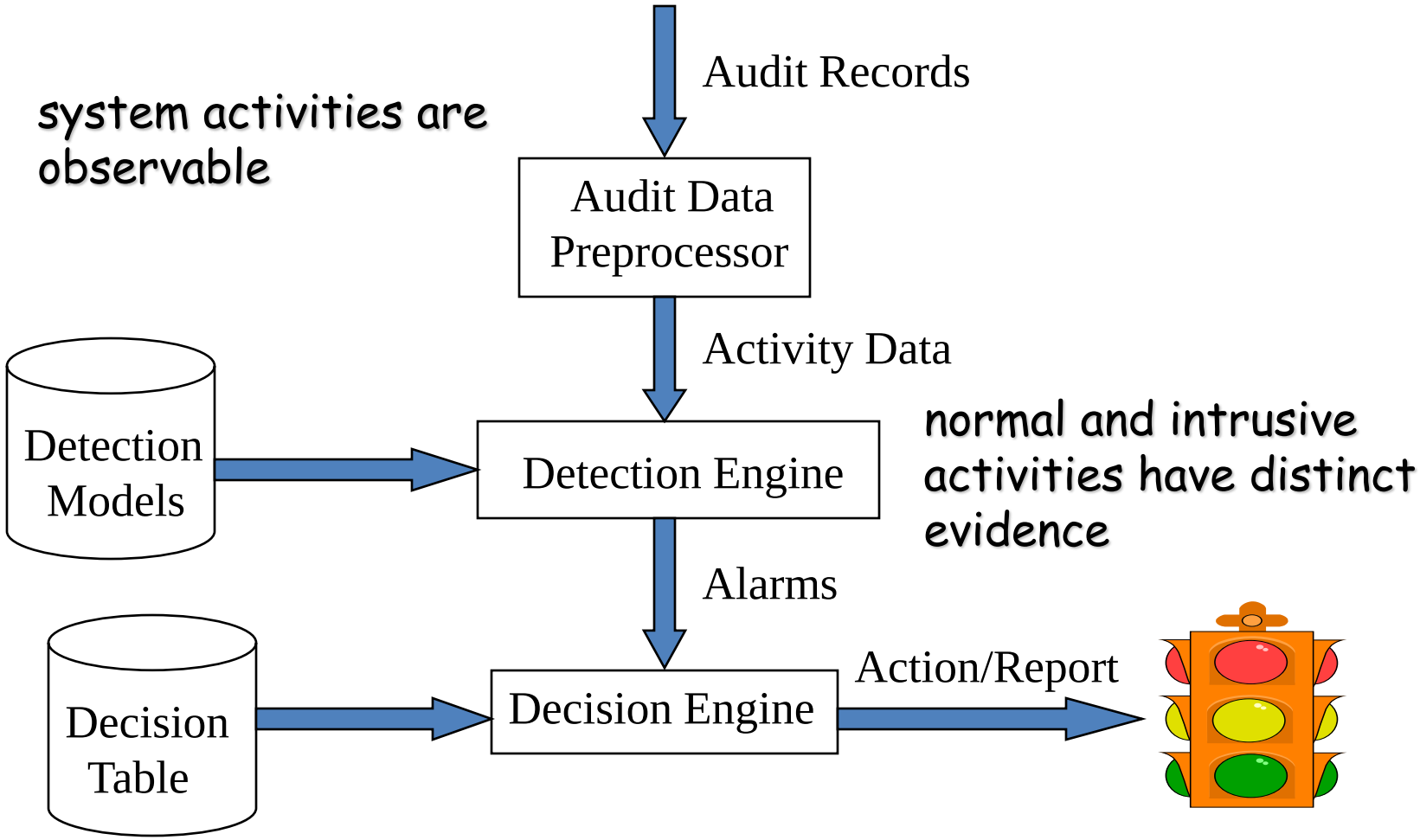
Intrusion detection

- Intrusion detection is the process of monitoring the events occurring in a computer system or network and analyzing them for signs of possible incidents, which are violations or imminent threats of violation of computer security policies, acceptable use policies, or standard security practices.

Intrusion prevention

- Intrusion prevention is the process of performing intrusion detection and attempting to stop detected possible incidents

Components of Intrusion Detection System



Security Infrastructure

- IDS are a dedicated assistant used to monitor the rest of the security infrastructure
- Today's security infrastructure are becoming extremely complex, it includes firewalls, identification and authentication systems, access control product, virtual private networks, encryption products, virus scanners, and more.
- All of these tools performs functions essential to system security. Given their role they are also prime target and being managed by humans, as such they are prone to errors.
- Failure of one of the above component of your security infrastructure jeopardized the system they are supposed to protect

- Firewalls and spam filters have simple rules such as to allow or deny protocols, ports or IP addresses.

Need for IDS

- Not all traffic may go through a firewall
  i:e modem on a user computer
- Not all threats originates from outside. As networks uses more and more encryption, attackers will aim at the location where it is often stored unencrypted (Internal network)
- Firewall does not protect appropriately against application level weaknesses and attacks
- Firewalls are subject to attacks themselves
- Protect against misconfiguration or fault in other security mechanisms

NOC vs SOC

- **The goal of a Network Operations Center (NOC) and a Security Operations Center (SOC) is to ensure that the corporate network meets business needs**.
- NOC: The NOC is the team within an organization that is responsible for ensuring that the corporate network infrastructure is capable of meeting the needs of the business. Every organization uses the corporate network for certain purposes, and the NOC optimizes and troubleshoots the corporate network to ensure that it is capable of meeting the needs of the business.

NOC vs SOC

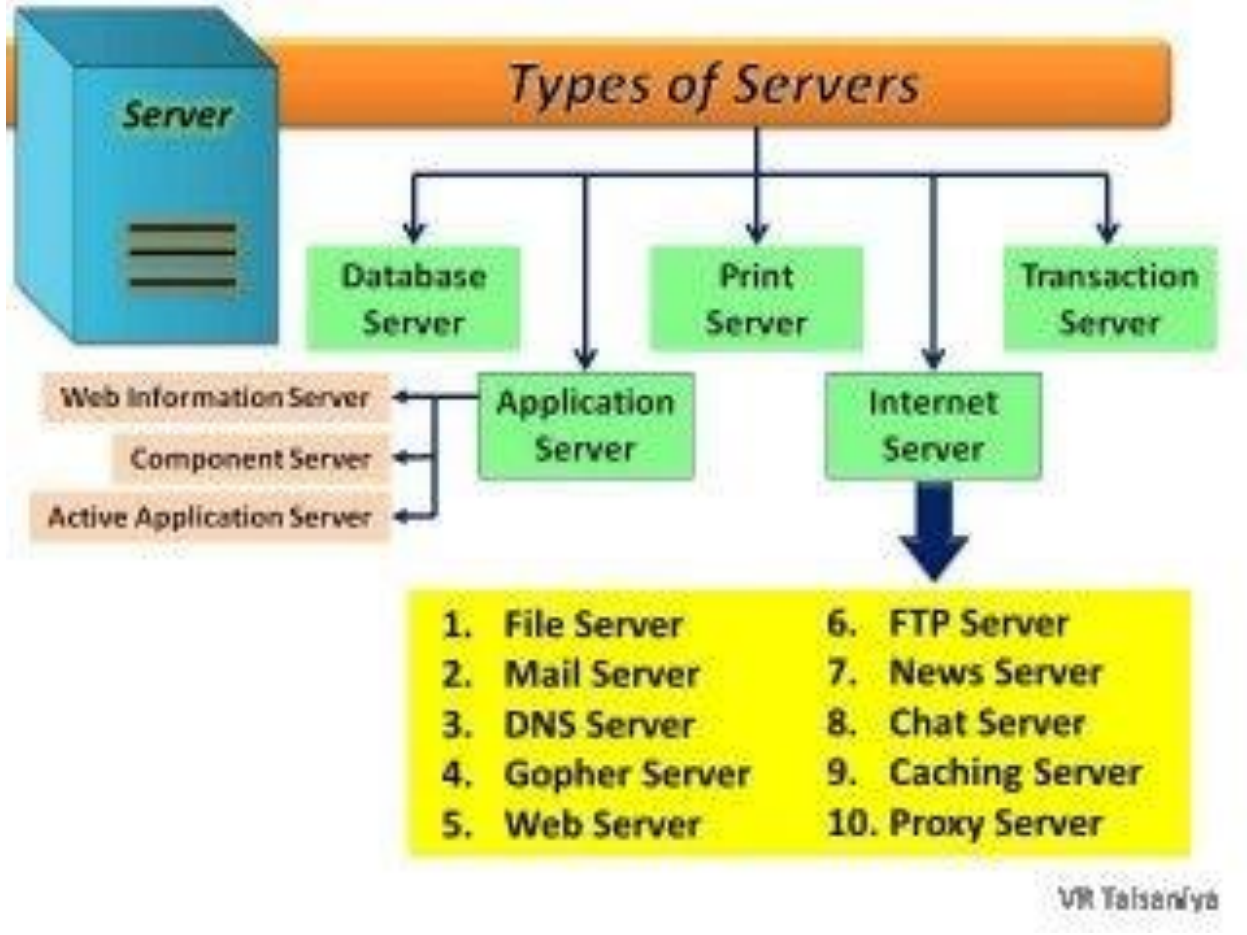
- SOC: An organization's SOC is responsible for protecting an organization against cyber threats. SOC analysts are responsible for hardening corporate assets to prevent attacks and performing incident detection and response in the event of a security incident. A corporate SOC may be internal or provided by a third party under a SOC as a Service model

SIEM

- **Security information and event management** is a field within the field of computer security, where software products and services combine security information management and security event management. They provide real-time analysis of security alerts generated by applications and network hardware.

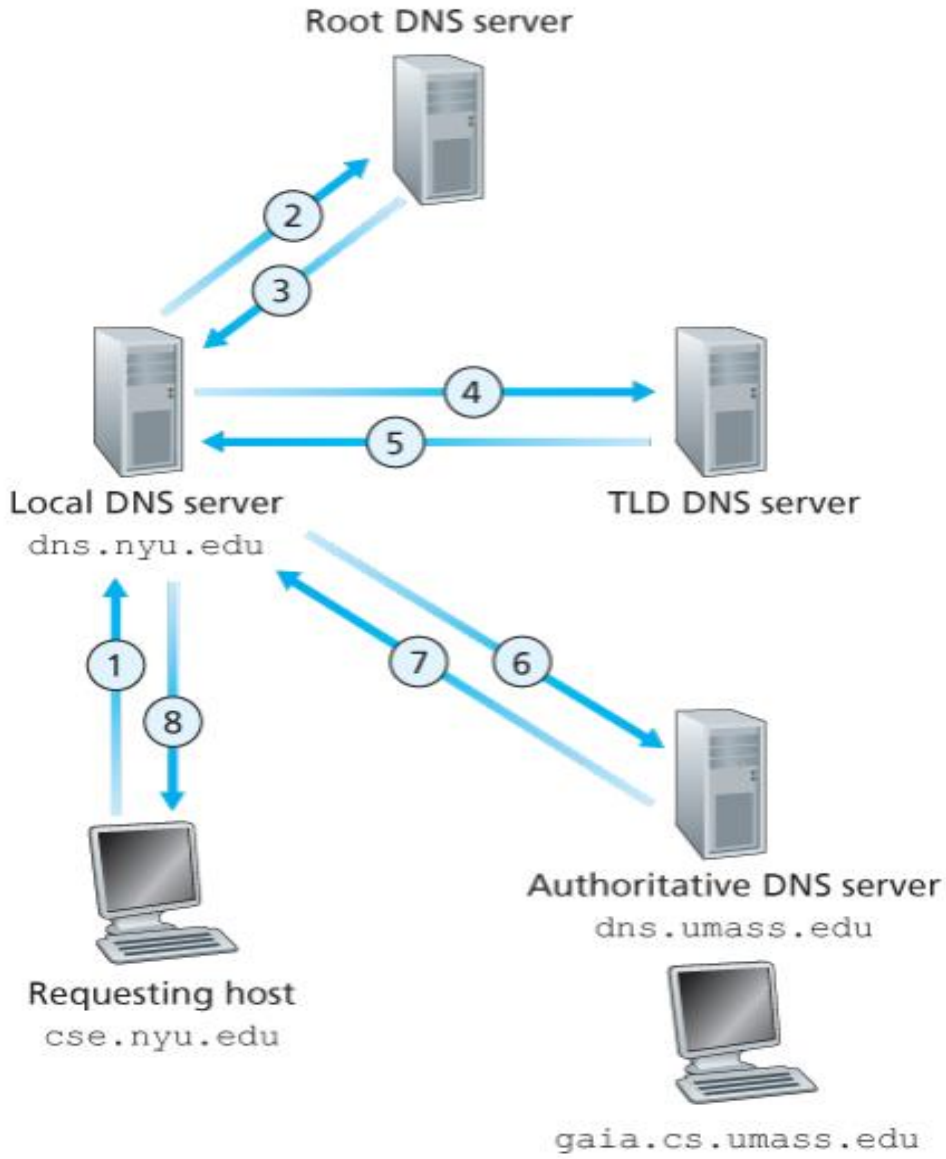
Types of Servers

- DNS,
- DHCP,
- Proxy, Mail and
- Application servers.



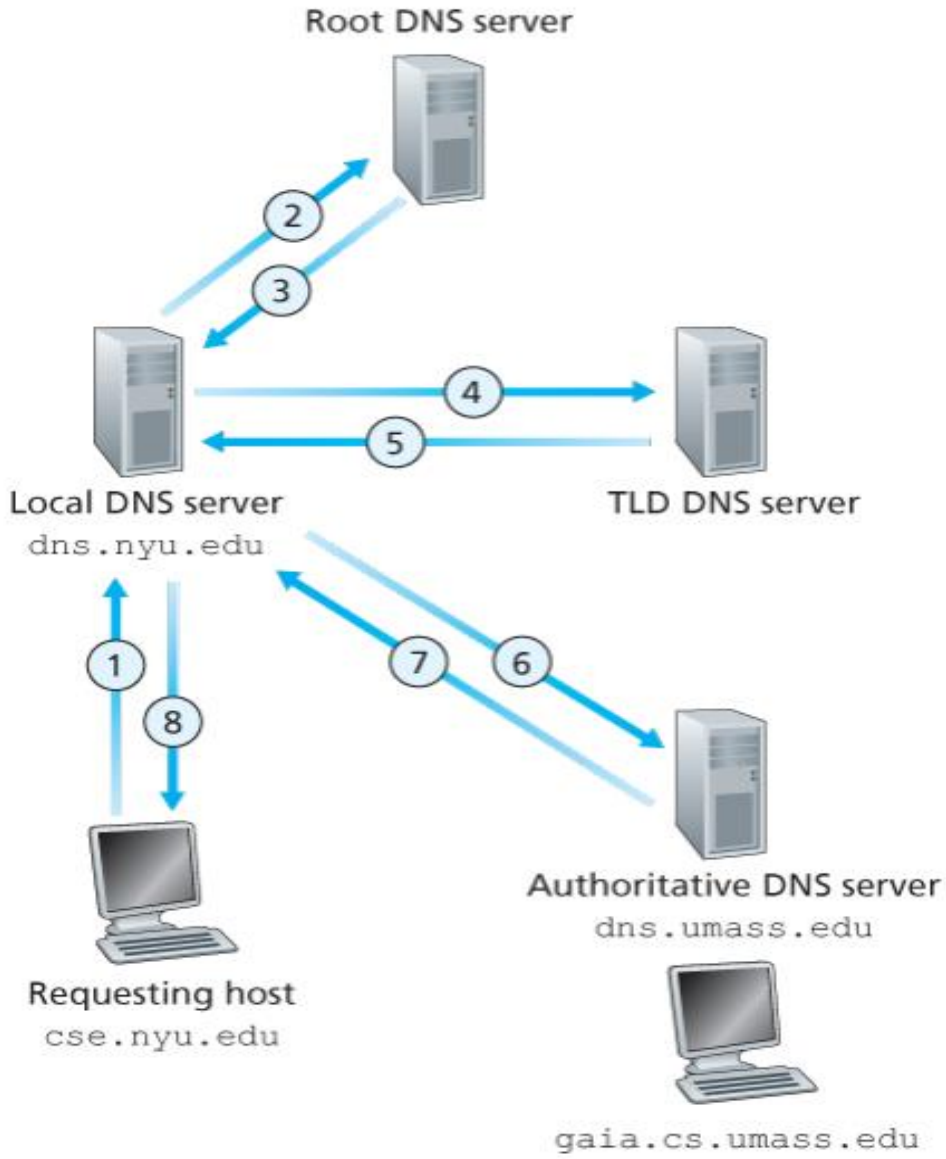
DNS

- When users type domain names into the URL bar in their browser, DNS servers are responsible for translating those domain names to numeric IP addresses, leading them to the correct website.



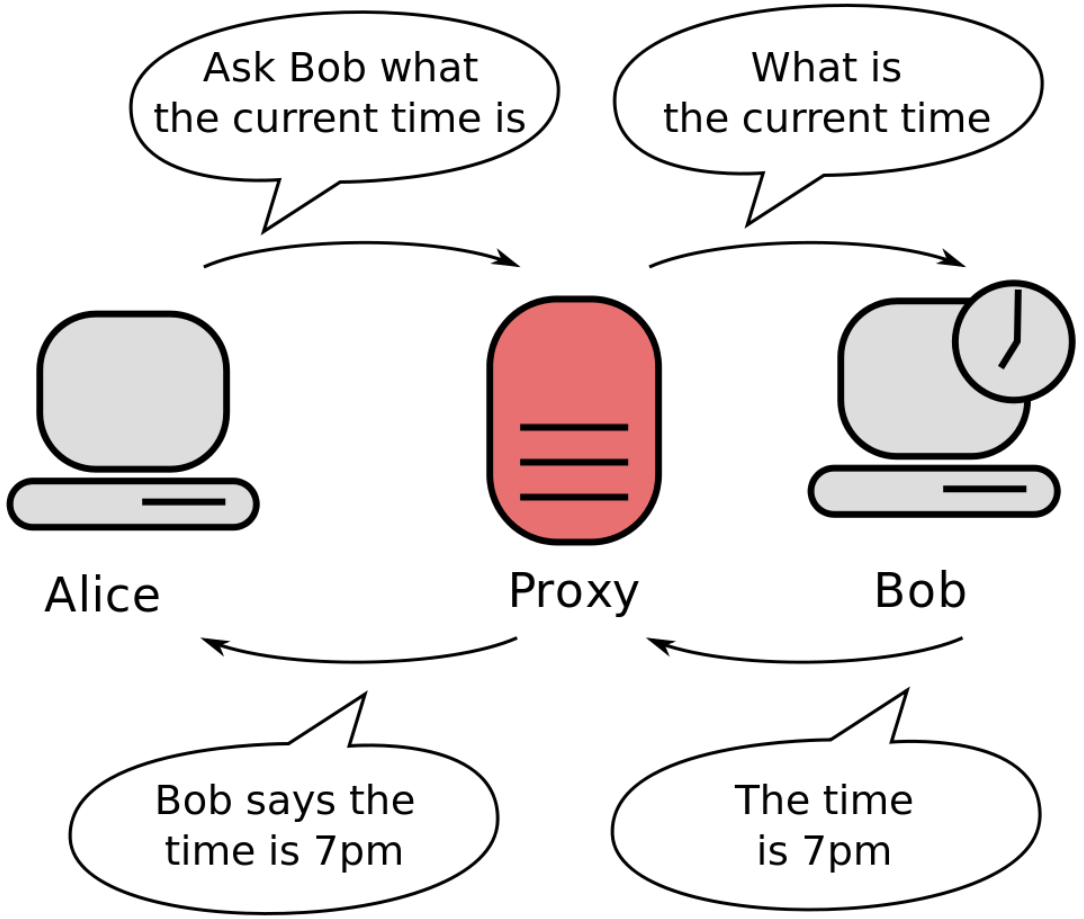
TLD

- A TLD nameserver **maintains information for all the domain names that share a common domain extension, such as .com, . net, or whatever comes after the last dot in a url**. For example, a .com TLD nameserver contains information for every website that ends in '.com'.



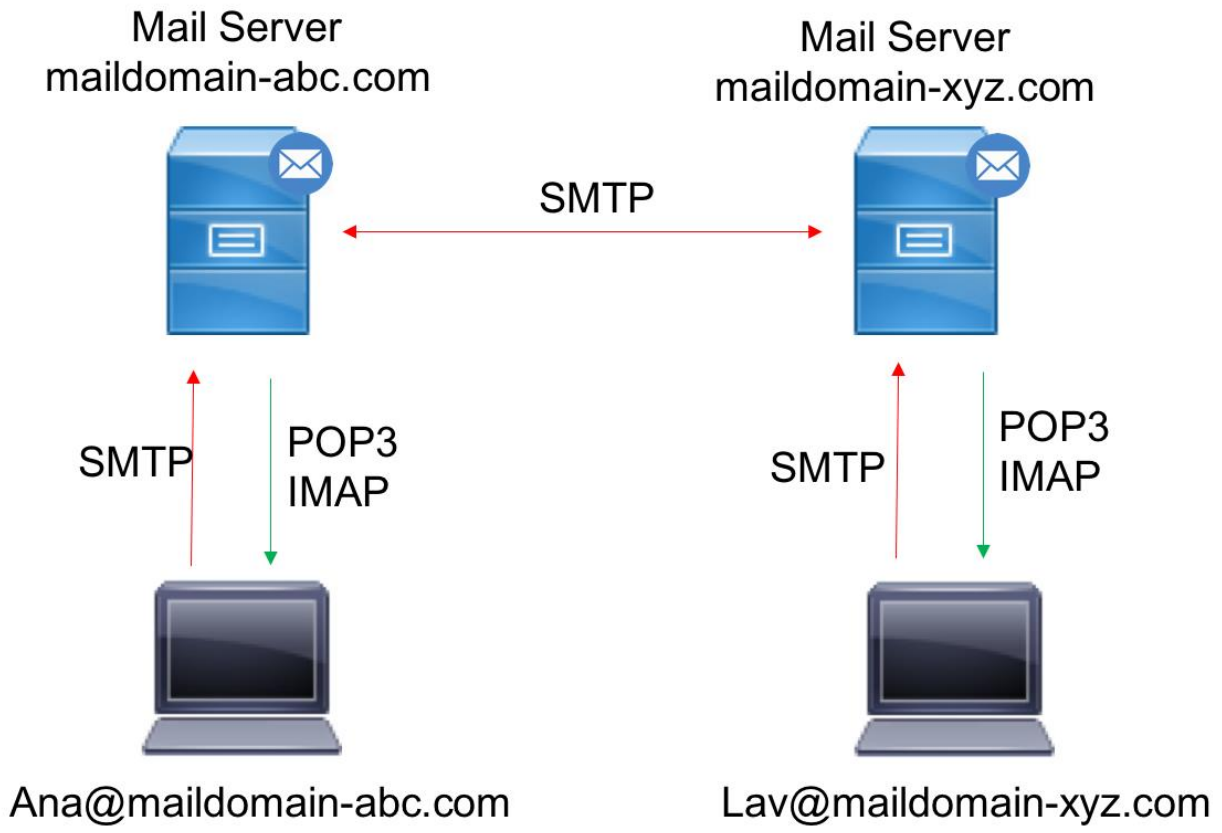
proxy server

- In computer networking, a proxy server is a server application that acts as an intermediary between a client requesting a resource and the server providing that resource.



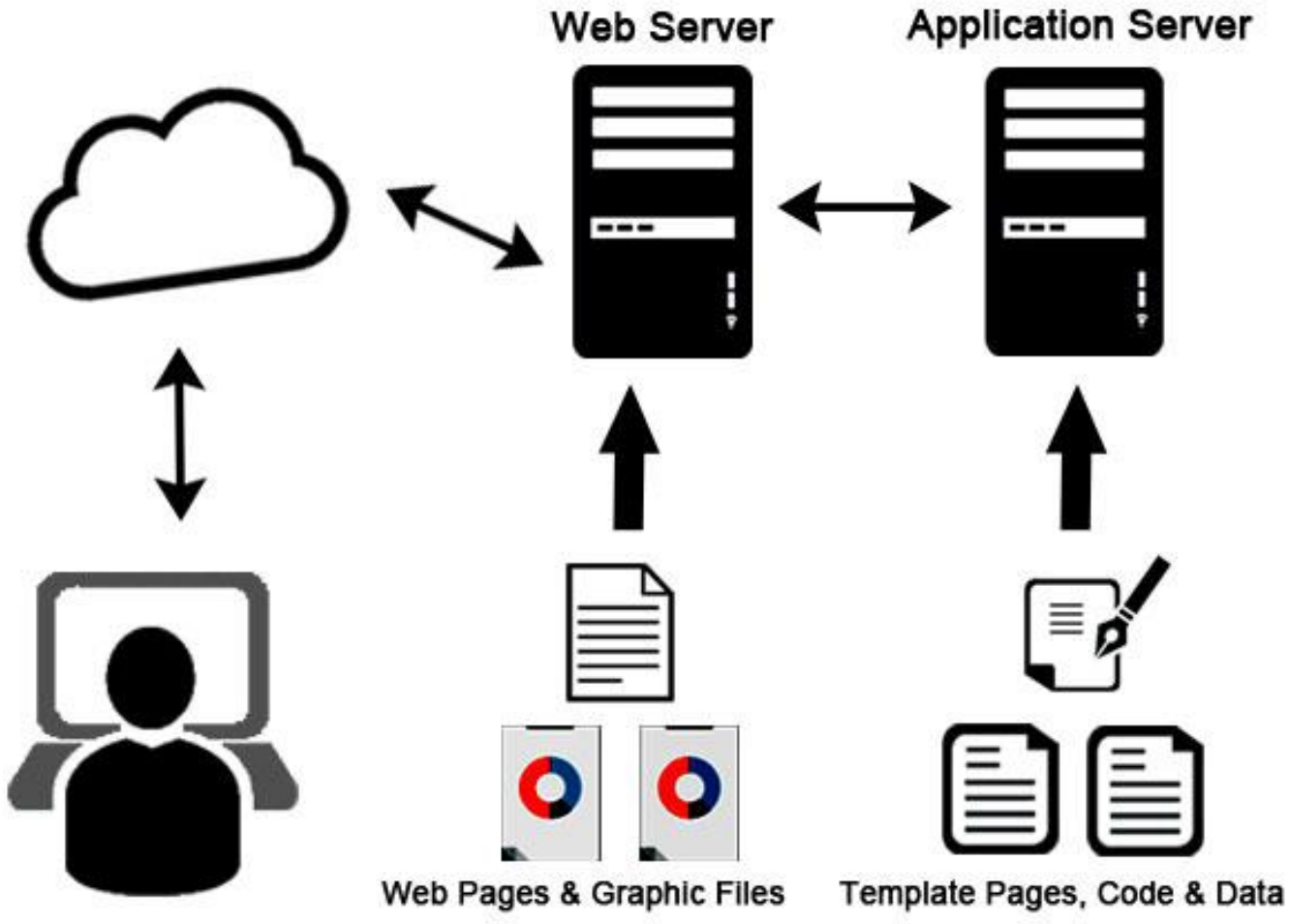
Mail Server

- A mail server -- also known as a mail transfer agent, or MTA; mail transport agent; mail router; or internet mailer -- is **an application that receives incoming email from local users and remote senders and forwards outgoing messages for delivery**.



application server

- An **application server** is a server that hosts applications or software that delivers a business application through a communication protocol.



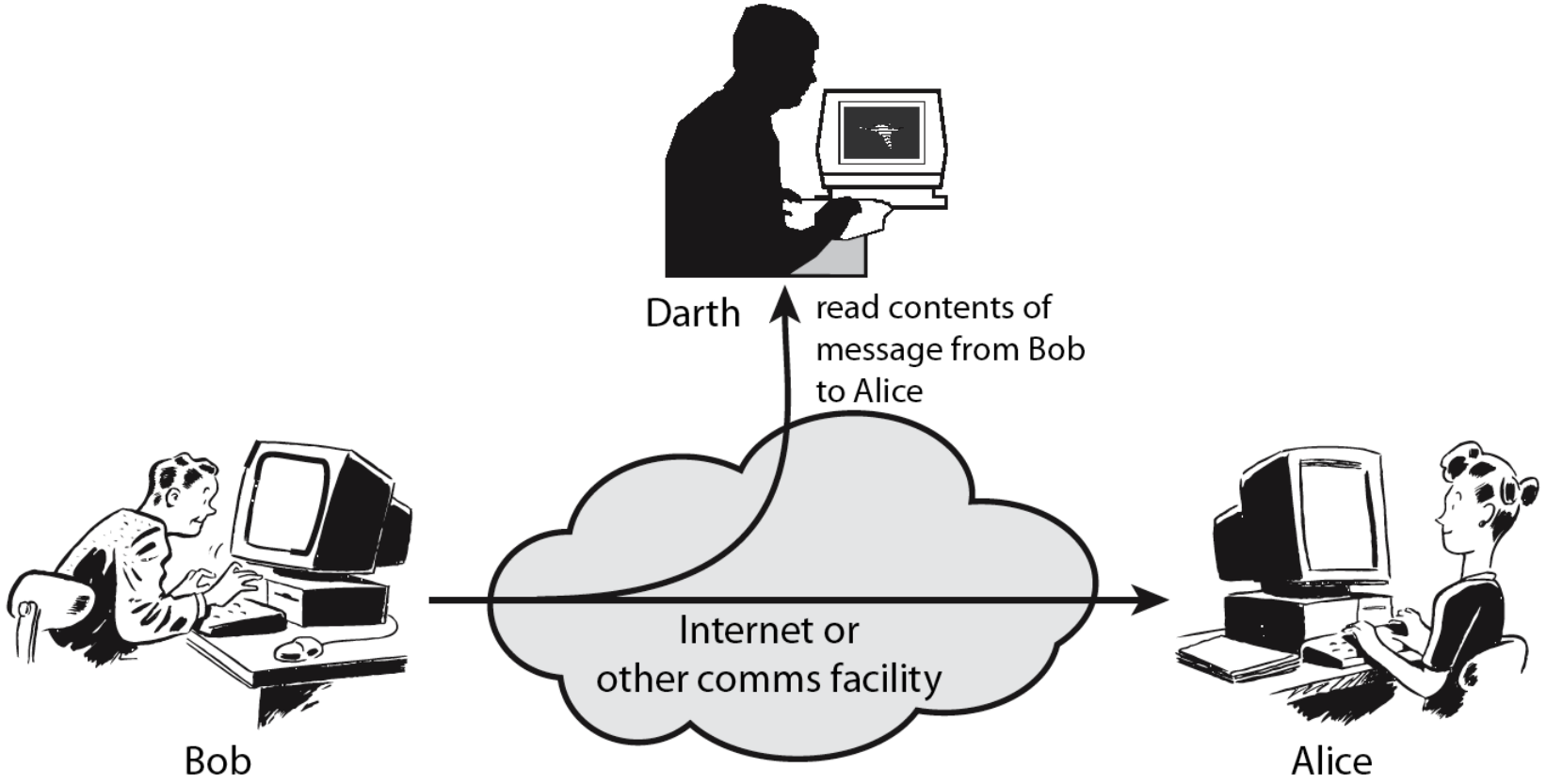
Services, Mechanisms, Attacks

- need systematic way to define requirements
- consider three aspects of information security:
  - **security attack**
  - **security mechanism**
  - **security service**
- consider in reverse order

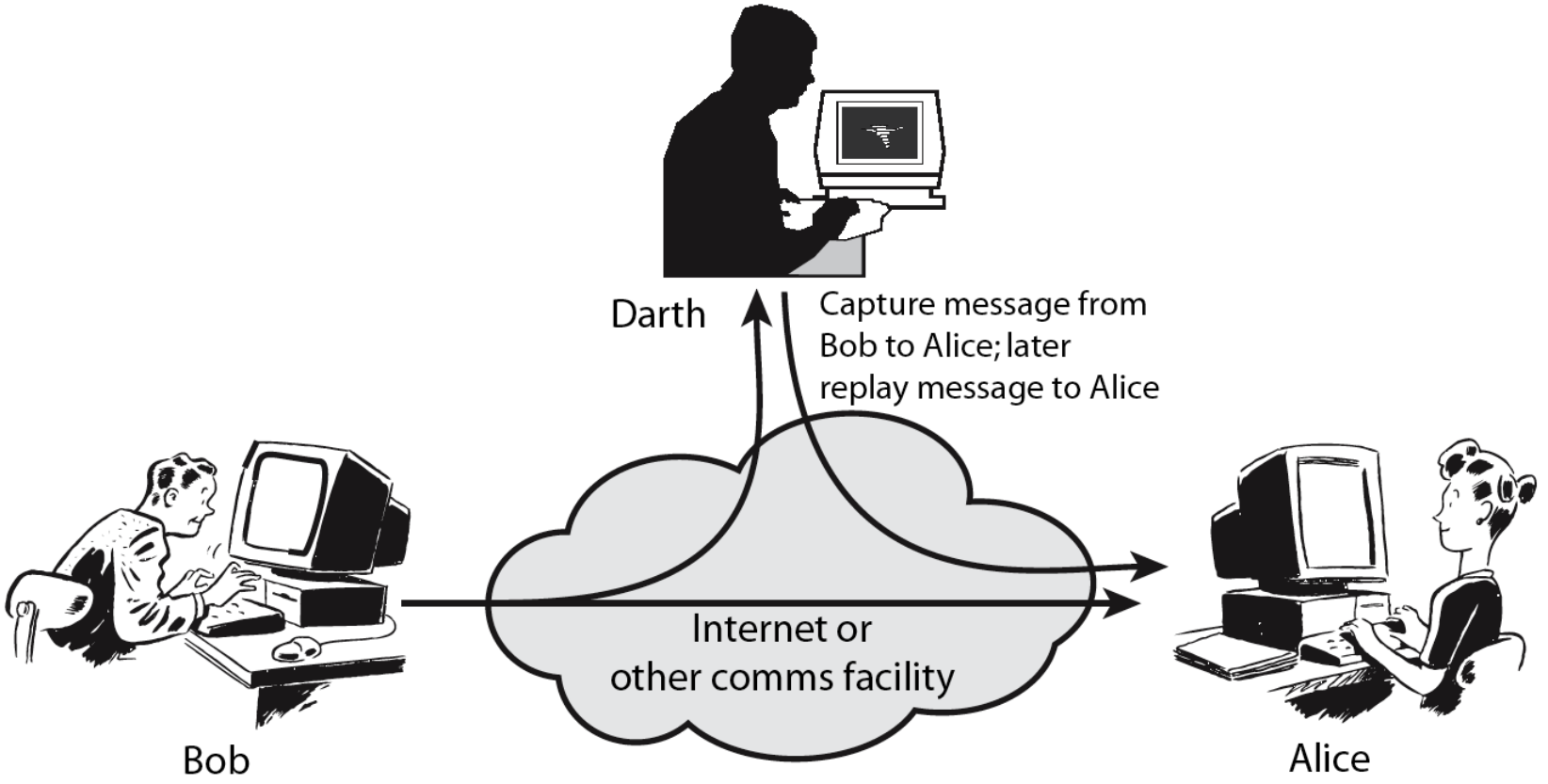
Attacks

- Passive attacks
  - Interception
    - Release of message contents
    - Traffic analysis
- Active attacks
  - Interruption, modification, fabrication
    - Masquerade
    - Replay
    - Modification
    - Denial of service

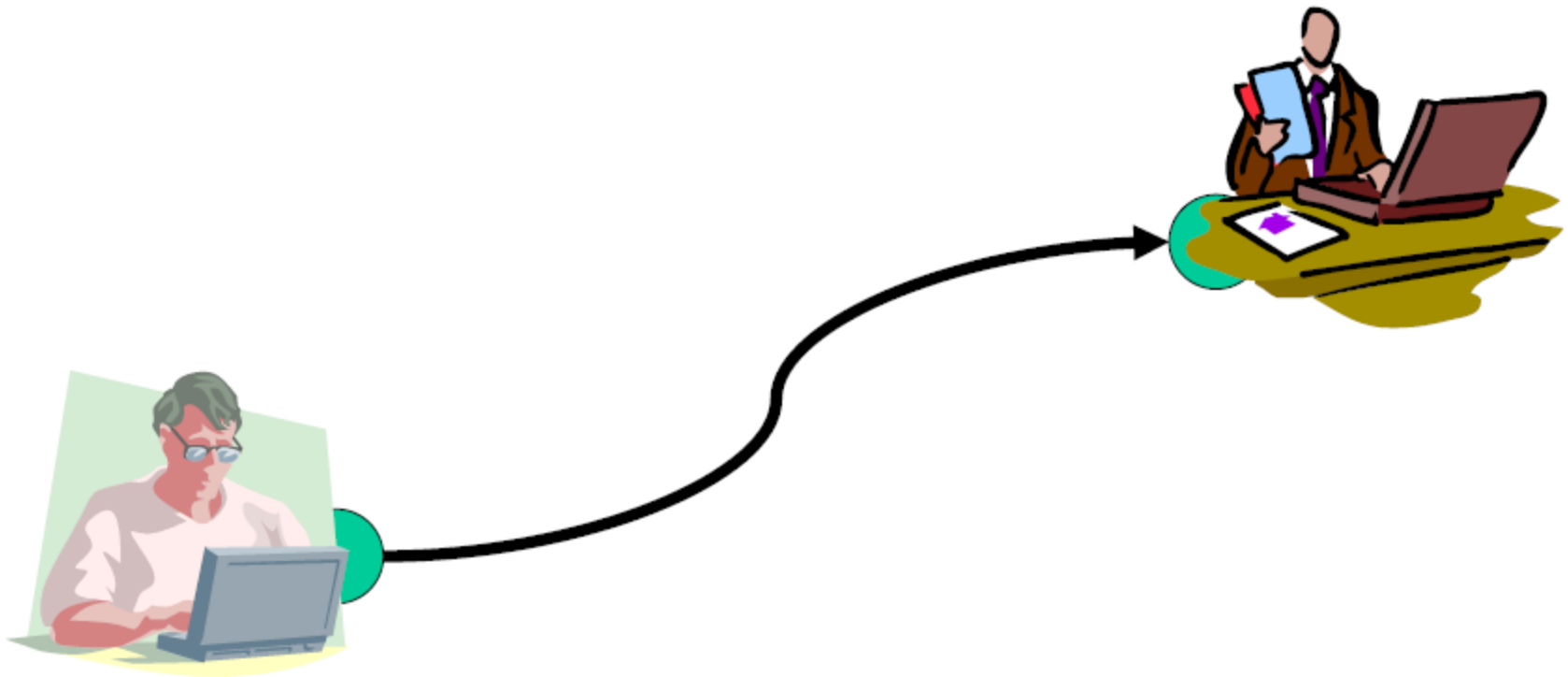
Passive Attacks



Active Attacks



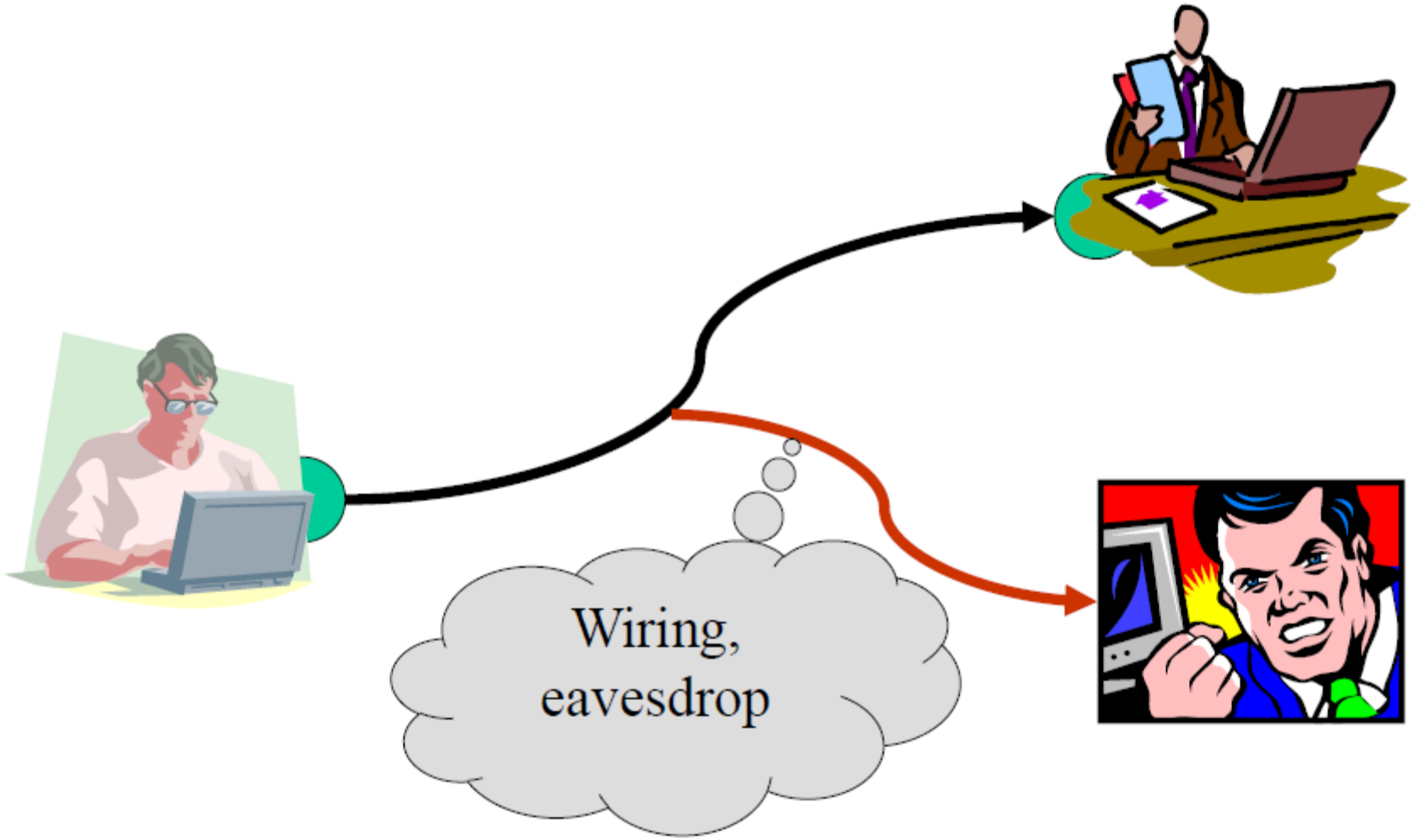
Information Transferring



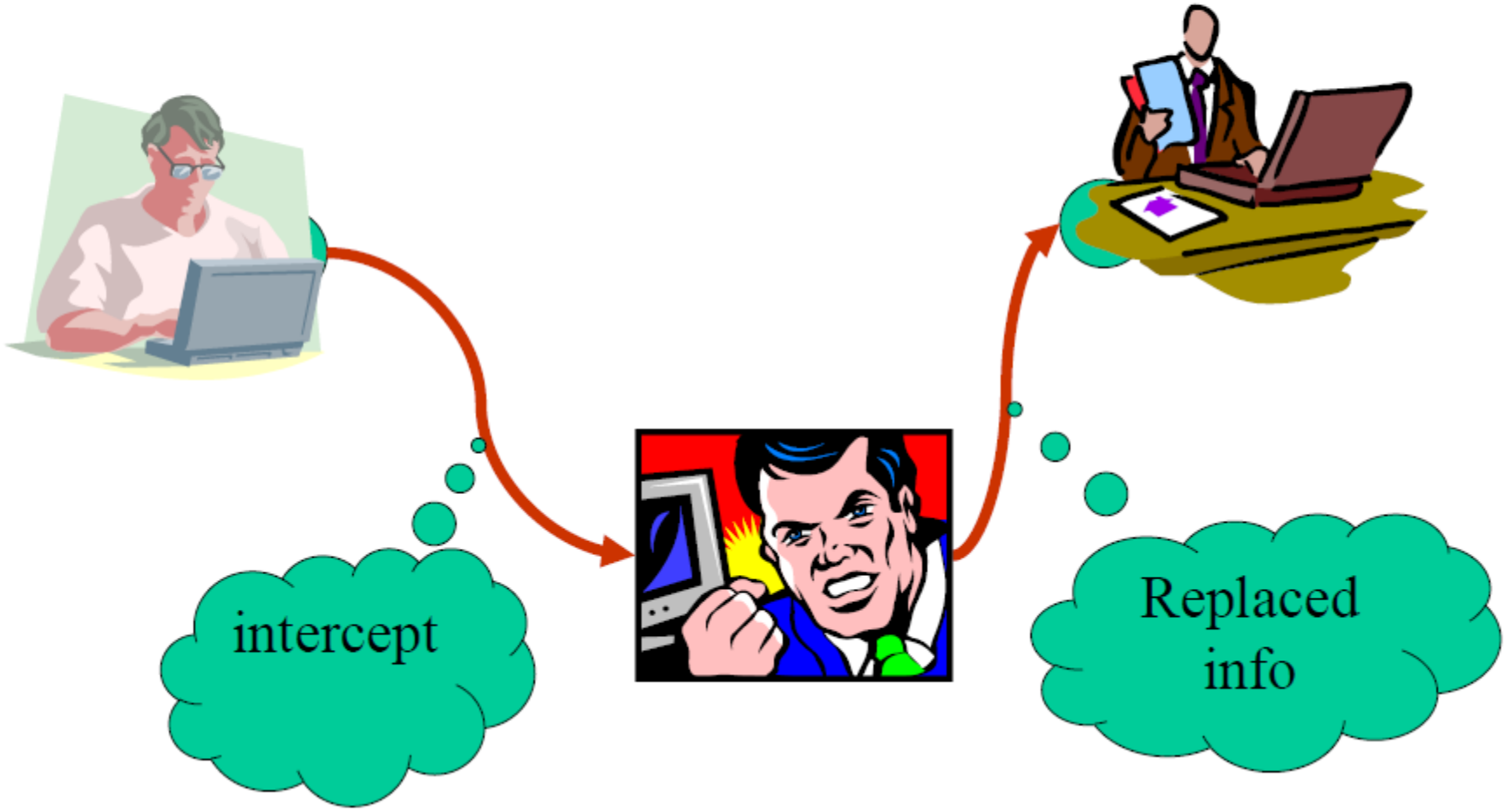
Attack: Interruption

Cut wire lines,
Jam wireless
signals,
Drop packets,

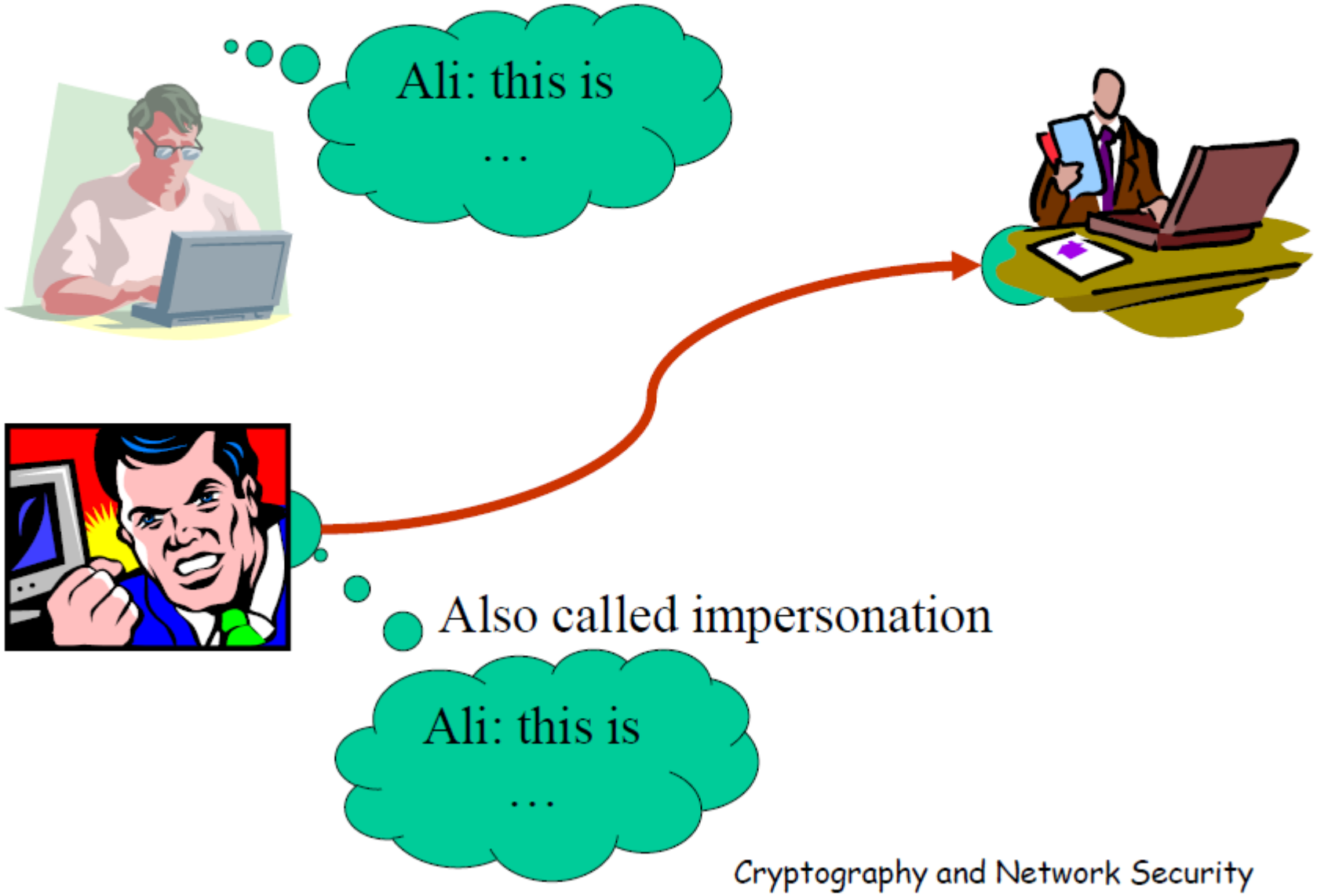
Attack: Interception



Attack: Modification



Attack: Fabrication



Security Service

- is something that enhances the security of the data processing systems and the information transfers of an organization
- intended to counter security attacks
- make use of one or more security mechanisms to provide the service
- replicate functions normally associated with physical documents
  - eg. have signatures, dates; need protection from disclosure, tampering, or destruction; be notarized or witnessed; be recorded or licensed

Security Mechanism

- a mechanism that is designed to detect, prevent, or recover from a security attack
- no single mechanism that will support all functions required
- however one particular element underlies many of the security mechanisms in use: **cryptographic techniques**
- hence our focus on this area

Security Attack

- any action that compromises the security of information owned by an organization
- information security is about how to prevent attacks, or failing that, to detect attacks on information-based systems
- have a wide range of attacks
- can focus of generic types of attacks
- note: often *threat* & *attack* mean same

OSI Security Architecture

- ITU-T X.800 Security Architecture for OSI
- defines a systematic way of defining and providing security requirements
- for us it provides a useful, if abstract, overview of concepts we will study

Security Services

- X.800 defines it as: a service provided by a protocol layer of communicating open systems, which ensures adequate security of the systems or of data transfers
- RFC 2828 defines it as: a processing or communication service provided by a system to give a specific kind of protection to system resources
- X.800 defines it in 5 major categories

Security Services (X.800)

- **Authentication** - assurance that the communicating entity is the one claimed
- **Access Control** - prevention of the unauthorized use of a resource
- **Data Confidentiality** –protection of data from unauthorized disclosure
- **Data Integrity** - assurance that data received is as sent by an authorized entity
- **Non-Repudiation** - protection against denial by one of the parties in a communication

Security Mechanisms (X.800)

- specific security mechanisms:
  - encipherment, digital signatures, access controls, data integrity, authentication exchange, traffic padding, routing control, notarization
- pervasive security mechanisms:
  - trusted functionality, security labels, event detection, security audit trails, security recovery

Classify Security Attacks as

- **passive attacks** - eavesdropping on, or monitoring of, transmissions to:
  - obtain message contents, or
  - monitor traffic flows
- **active attacks** – modification of data stream to:
  - masquerade of one entity as some other
  - replay previous messages
  - modify messages in transit
  - denial of service

Attack Surface

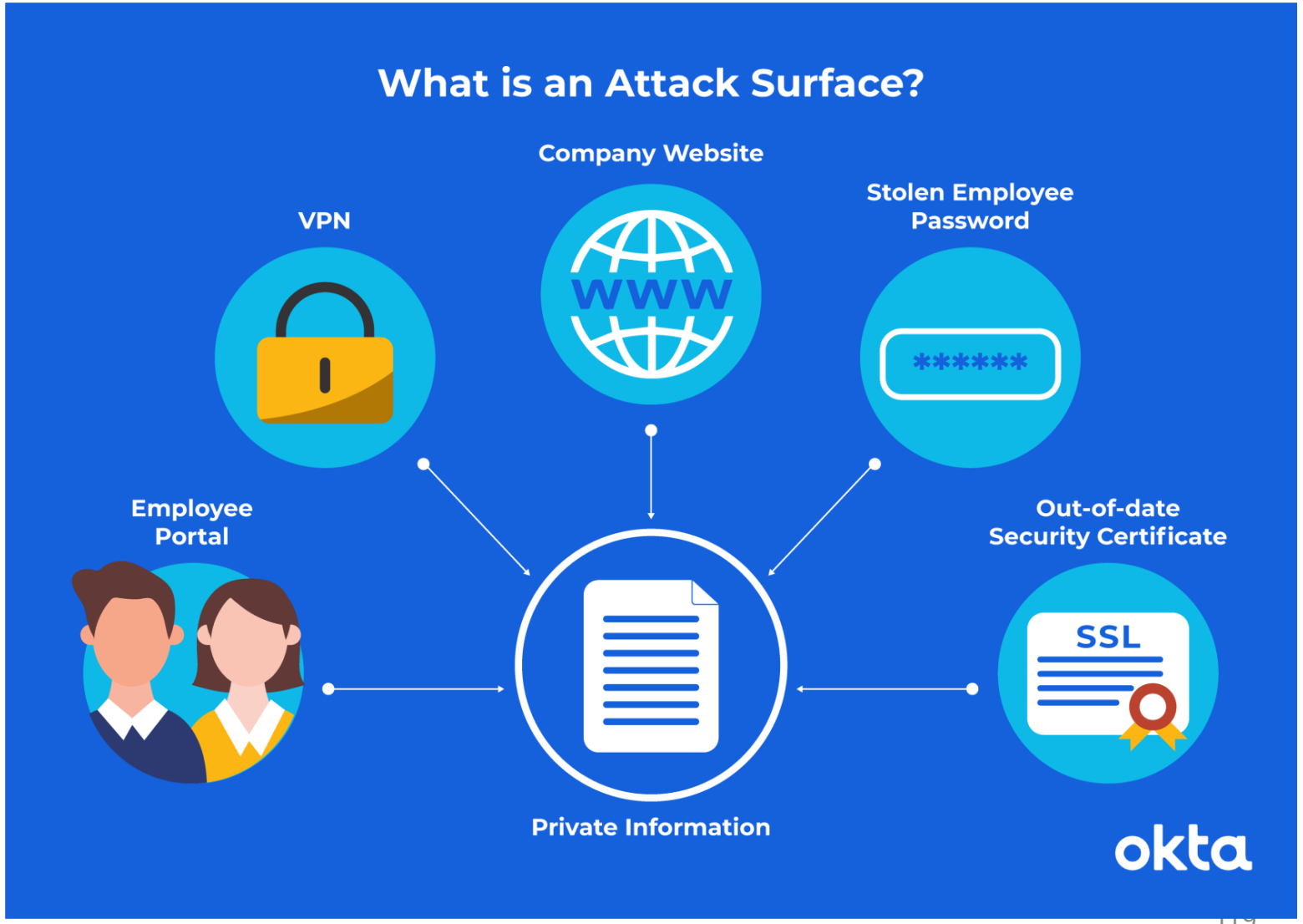
- An attack surface is the entire area of an organization or system that is susceptible to hacking.
- It's made up of all the points of access that an unauthorized person could use to enter the system.
- Once inside your network, that user could cause damage by manipulating or downloading data.

Attack Surface

- The smaller your attack surface, the easier it is to protect your organization.
- Conducting a surface analysis is a good first step to reducing or protecting your attack surface.
- Follow it with a strategic protection plan to reduce your risk of an expensive software attack or cyber extortion effort.

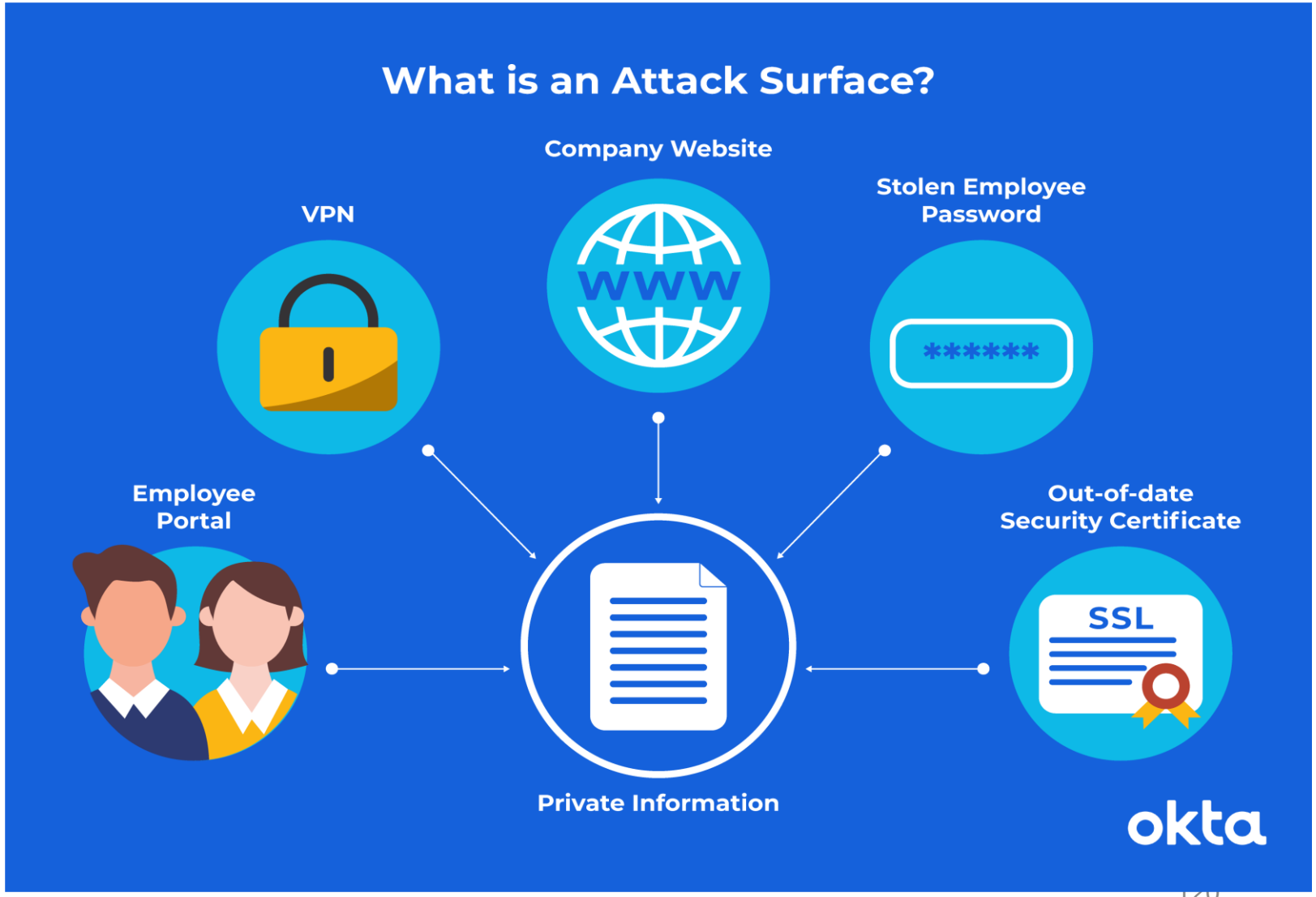
Attack Surface and Attack Vector

- An attack surface is essentially the entire external-facing area of your system.
- The model contains all of the attack vectors (or vulnerabilities) a hacker could use to gain access to your system.



Attack Surface and Attack Vector

- Vulnerabilities are everywhere, and often, they're exploited.
- For example, in 2014, reporters said nearly half of all Fortune 500 companies had employee email addresses and passwords exposed in hacker forums within the year.



Attack Vector

- In cybersecurity, an attack vector is a method of achieving unauthorized network access to launch a cyber attack.
- Attack vectors allow cybercriminals to exploit system vulnerabilities to gain access to sensitive data, personally identifiable information (PII), and other valuable information accessible after a data breach.
- Attack vectors are the landmarks on an attack surface. Each one represents vulnerabilities, such as access points, protocols, and services.

Attack Vector

Attack Vector	Issue	Solution
APIs	APIs can supercharge business growth, but they also put your company at risk if they are not properly secured.	Secure all APIs by using tokens, encryption, signatures, and other means to keep your organization protected.
Distributed denial of service (DDoS)	A DDoS attack floods a targeted server or network with traffic in an attempt to disrupt and overwhelm a service rendering inoperable.	Protect your business by reducing the surface area that can be attacked. This is done by restricting direct access to infrastructure like database servers. Control who has access to what using an identity and access management system.
Encryption	If your protocols are weak or missing, information passes back and forth unprotected, which makes theft easy.	Confirm all protocols are robust and secure.
Insiders	A disgruntled employee is a security nightmare. That worker could share some or part of your network with outsiders. That person could also hand over passwords or other forms of access for independent snooping.	Work with HR to put protocols in place, so you're ready if this situation occurs.
Malware	This is a nasty type of software designed to cause errors, slow your computer down, or spread viruses. Spyware is a type of malware, but with the added insidious purpose of collecting personal information.	Keeping abreast of modern security practices is the best way to defend against malware attacks. Consider a centralized security provider to eliminate holes in your security strategy.
Passwords	Weak passwords (such as 123456!) or stolen sets allow a creative hacker to gain easy access. Once they're in, they may go undetected for a long time and do a lot of damage.	Set up requirements to ensure all passwords are strong, or use multi-factor, or even passwordless authentication.
Phishing	A seemingly simple request for email confirmation or password data could give a hacker the ability to move right into your network. Many phishing attempts are so well done that people give up valuable info immediately.	Your IT team can identify the latest phishing attempts and keep employees apprised of what to watch out for.
Ransomware	Hackers move into your network, lock it down, and ask for money to release it. In 2019, more than 205,000 organizations faced a demand just like this.	Identify where your most important data is in your system, and create an effective backup strategy. Added security measures will better protect your system from being accessed.

Attack Vector Vs Attack Surface Vs Threat Vector?

- An **attack vector** is a method of gaining unauthorized access to a network or computer system.
- An **attack surface** is the total number of attack vectors an attacker can use to manipulate a network or computer system or extract data.
- **Threat vector** can be used interchangeably with attack vector and generally describes the potential ways a hacker can gain access to data or other confidential information.

Types of Attacks

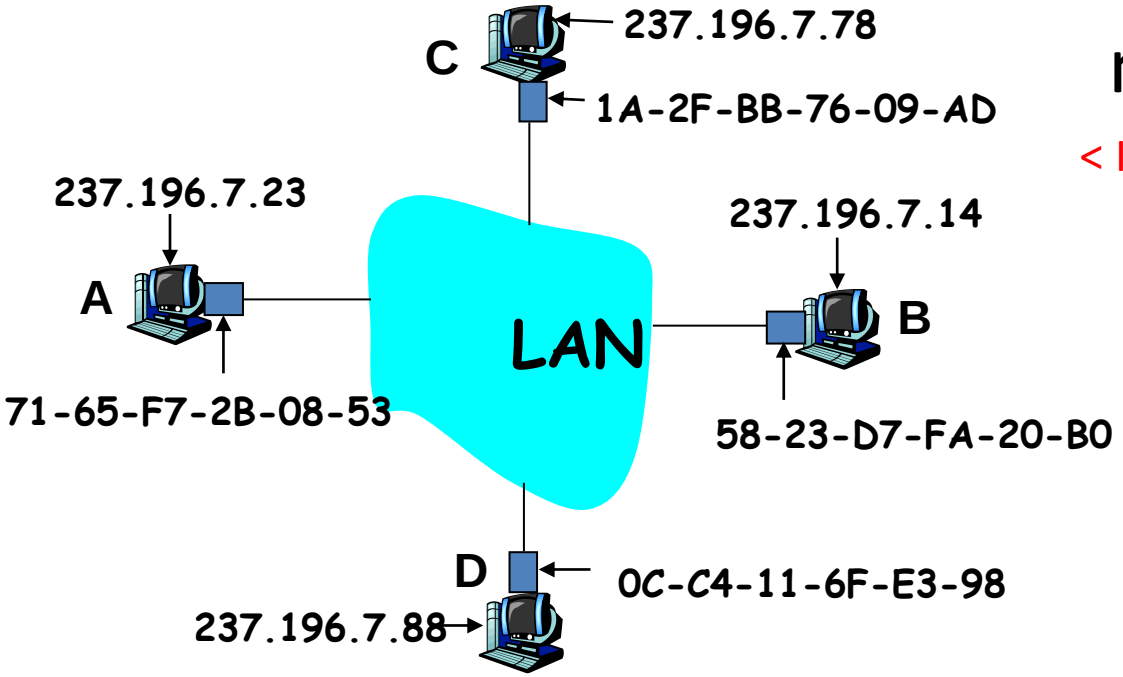
- ARP poising,
- Phishing attack,
- MAC flooding,
- DoS and
- DDoS.

MAC Addresses and ARP

- 32-bit IP address:
  - *network-layer* address
  - used to get datagram to destination IP subnet
- MAC (or LAN or physical or Ethernet) address:
  - Data link layer address
  - used to get datagram from one interface to another physically-connected interface (same network)
  - 48 bit MAC address (for most LANs) burned in the adapter ROM
  - Some Network interface cards (NICs) can change their MAC

ARP: Address Resolution Protocol

Question: how to determine MAC address of host B when knowing B's IP address?



- Each IP node (Host, Router) on LAN has ARP table
- ARP Table: IP/MAC address mappings for some LAN nodes

  < IP address; MAC address; TTL>

  - TTL (Time To Live): time after which address mapping will be forgotten (typically 20 min)

ARP

- 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>

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

  <IP address1> is <MAC address>

- 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
```

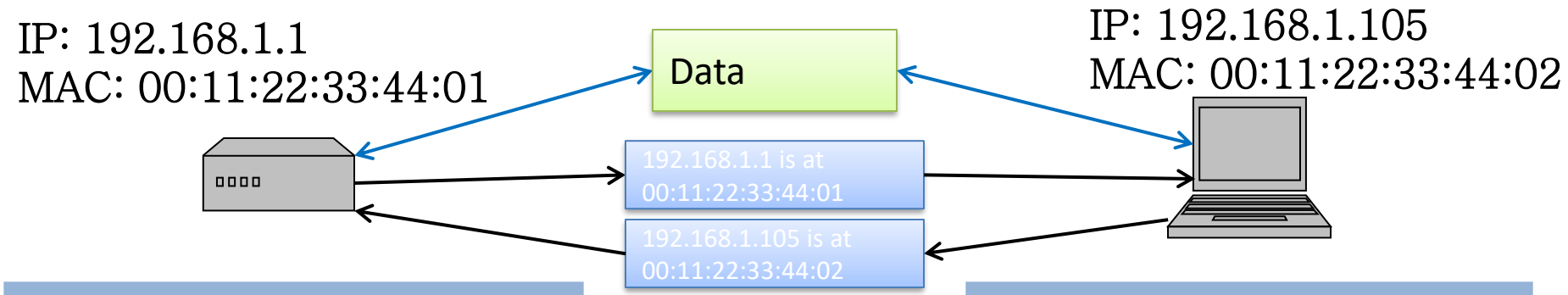
ARP Spoofing

- 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

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

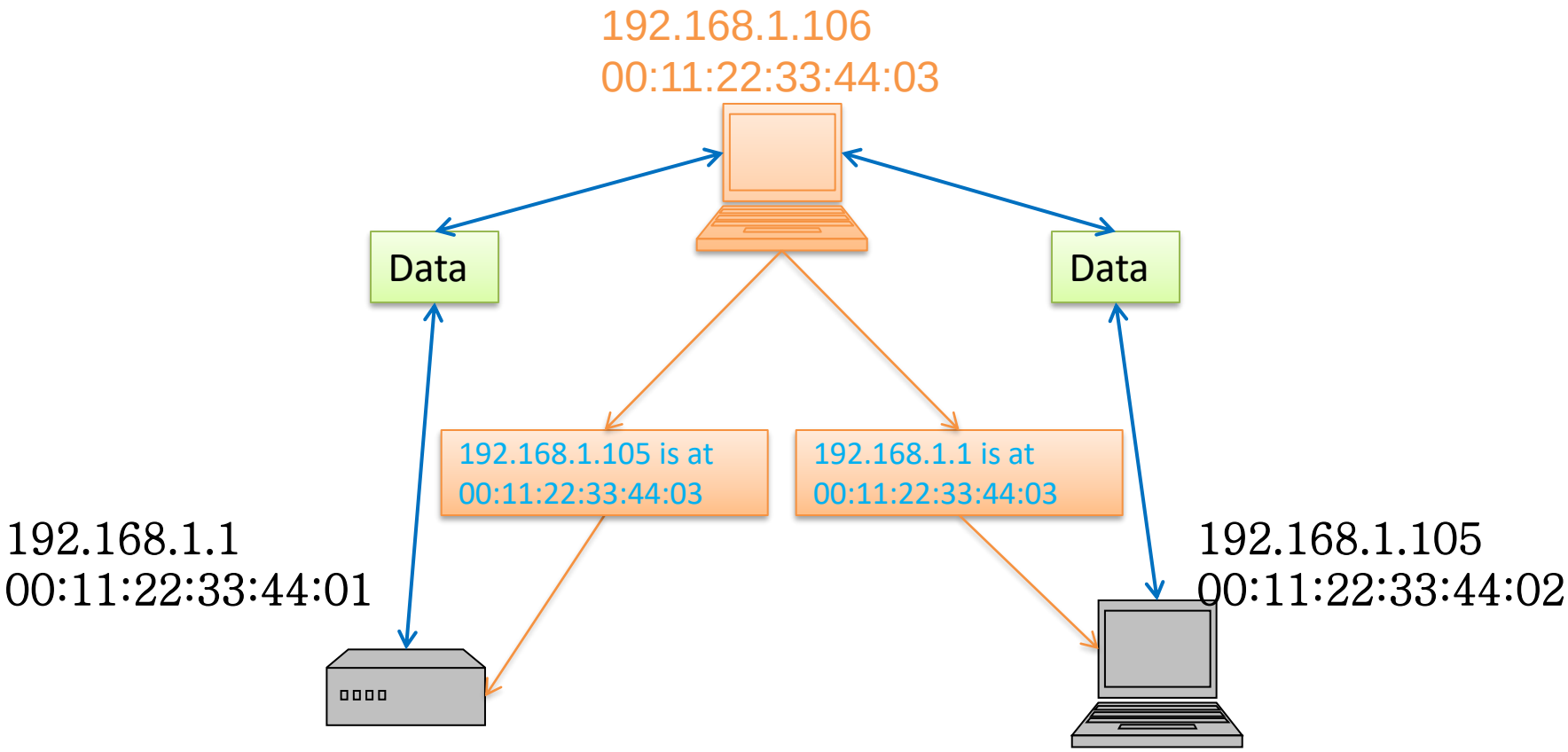
ARP Caches



ARP Cache	
192.168.1.**105**	00:11:22:33:44:**02**

ARP Cache	
192.168.1.**1**	00:11:22:33:44:**01**

Poisoned ARP Caches (man-in-the-middle attack)



Poisoned ARP Cache	
192.168.1.**105**	00:11:22:33:44:**03**

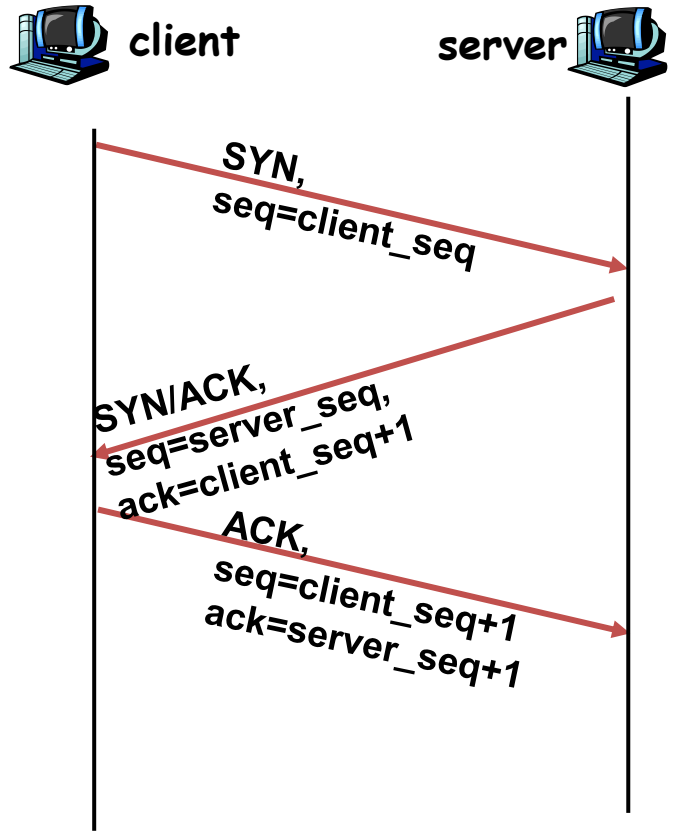
Poisoned ARP Cache	
192.168.1.**1**	00:11:22:33:44:**03**

ARP Spoofing

- Using static entries solves the problem but it is almost impossible to manage!
- Check multiple occurrence of the same MAC
  - i.e., One MAC mapping to multiple IP addresses (see previous slide's example)
- Software detection solutions
  - Anti-arpspoof, Xarp, Arpwatch

TCP Session Hijacking

- TCP connection has both sequence number and acknowledge number in each packet.
- The two ends negotiate what seq. and ack. Numbers to be used in TCP set up stage.
- seq and ack number size: 2^{32}
  - Makes seq/ack guessing very hard to achieve
  - Very hard to hijack an already setup TCP connection!



TCP Session Hijacking

- Possible when an attacker is on the same network segment as the target machine.
  - Attacker can sniff all back/forth tcp packets and know the seq/ack numbers.
  - Attacker can inject a packet with the correct seq/ack numbers with the spoofed IP address.
    - IP spoofing needs low-level packet programming, OS-based socket programming cannot be used!

TCP Session Hijacking

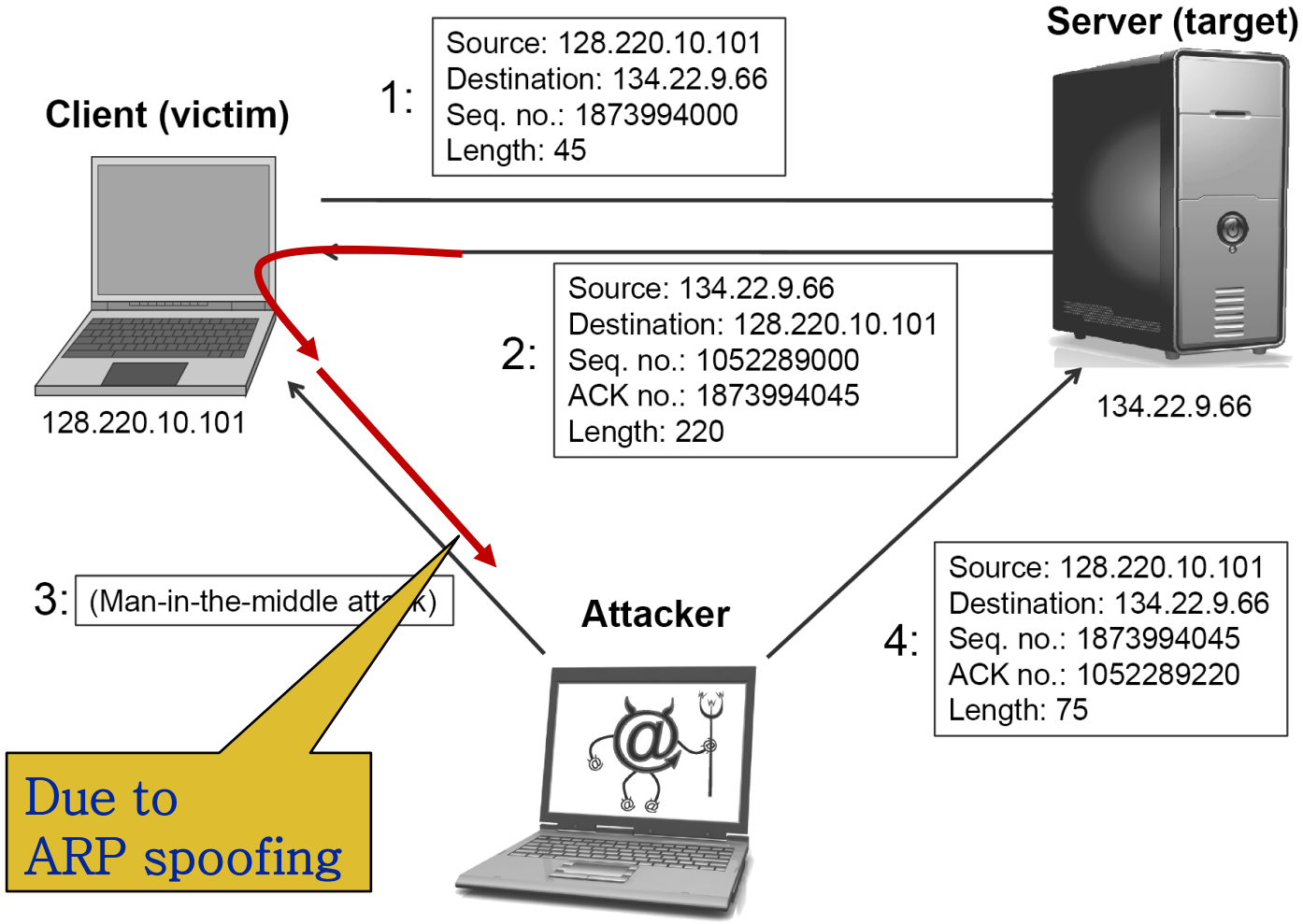
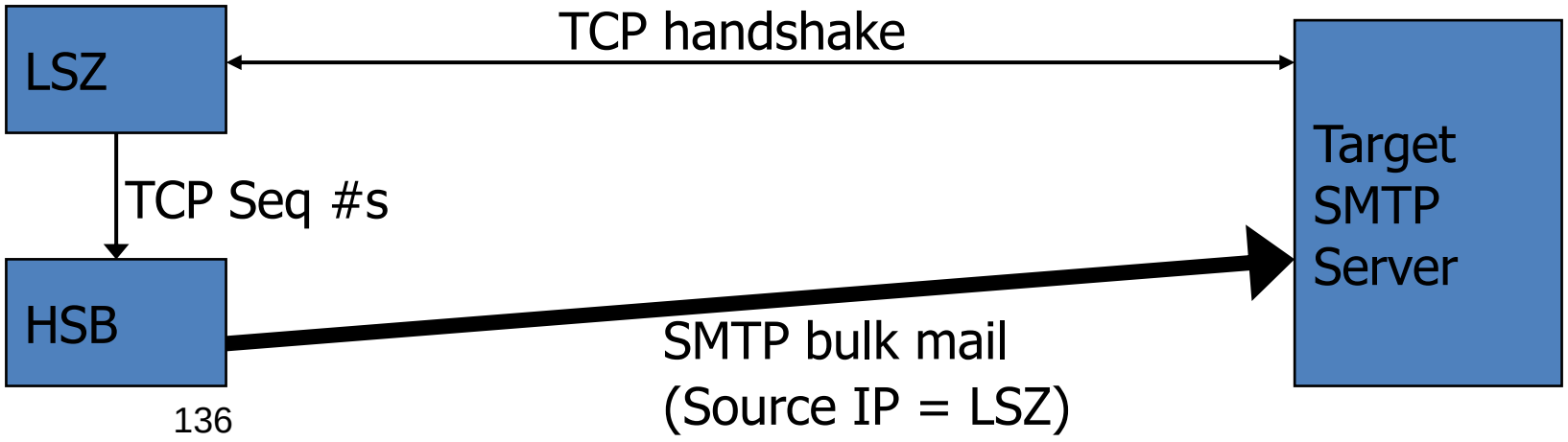


Figure 5.18: A TCP session hijacking attack.

TCP Session Hijacking

- Another way is “coordinated IP spoofing” by using two computers, such as the “Thin pipe / Thick pipe method” introduced in spam lecture:
  - High Speed Broadband connection (HSB)
  - Controls a Low Speed Zombie (LSZ)
  - Assumes no egress filtering at HSB’s ISP
  - Hides IP address of HSB. LSZ is blacklisted.



Denial-of-Service (DoS) Attack

- An attempt to make a computer or network resource unavailable to its intended users
  - DoS to the network bandwidth of targeted server
  - DoS to the computing resource of targeted server
    - Memory, CPU
  - DoS to the vulnerability in targeted server
    - Causing server OS crash (buffer overflow bug, logic bug, etc)
    - Causing server program crash (e.g., Apache, Sendmail, SQL)
- Distributed Denial-of-Service (DDoS) attack
  - Sending attack packets from multiple computers
  - Botnet is the root cause for DDoS attacks

Denial-of-Service (DoS) Attack

- Format:
  - Real IP-based attack using botnets
    - Attacker does not worry about exposing bots' IP addresses.
    - TCP flooding, UDP flooding, icmp flooding
  - Spoofed IP-based attack
    - SYN flooding with spoofed IPs.
  - Source address hiding attack
    - Smurf attack

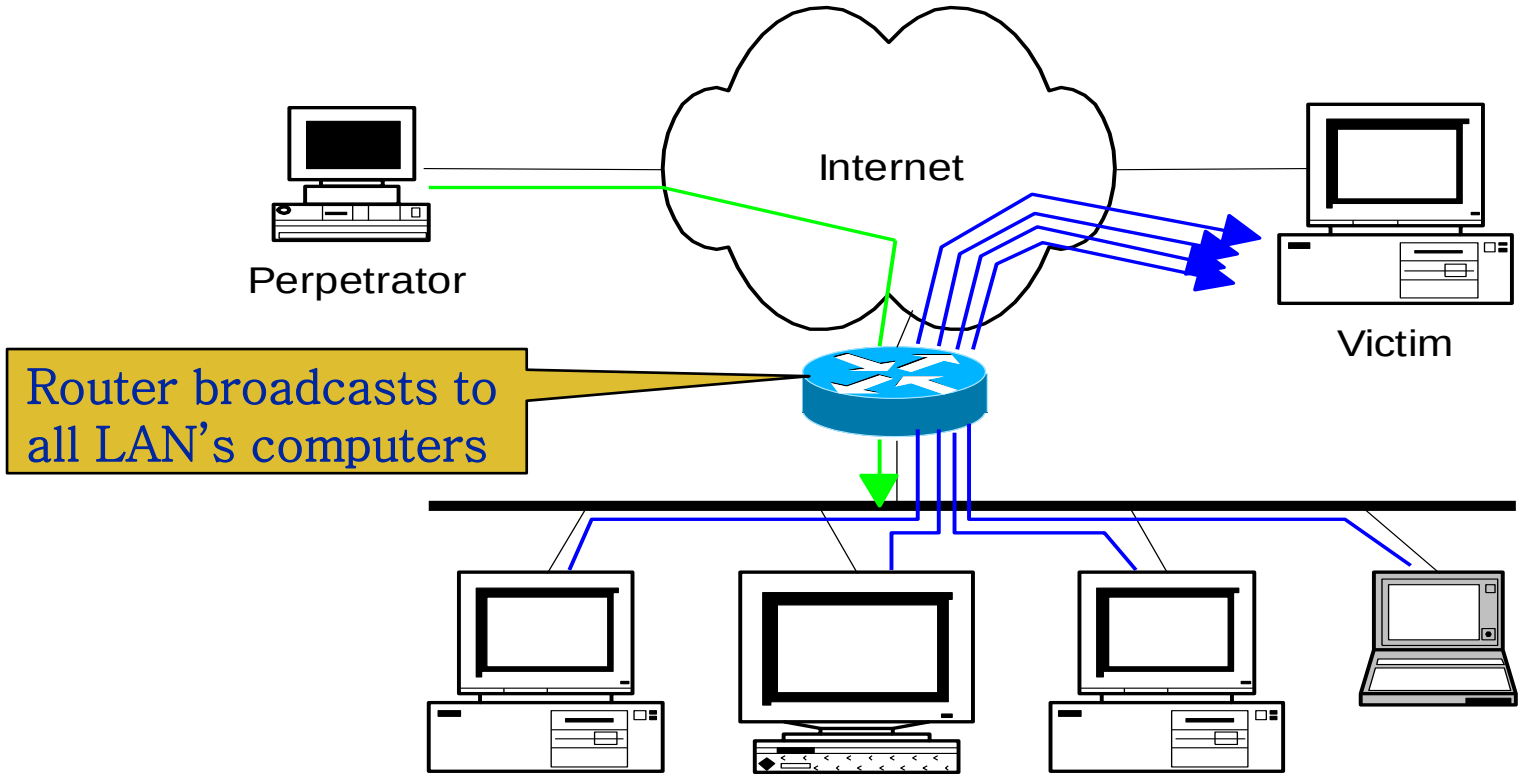
Smurf Attack

- Some contents from this link:
- *www.pentics.net/denial-of-service/.../ms**ppt**/19971027_**smurf.ppt***
- Uses ICMP echo/reply packets with broadcast networks to multiply traffic
- Requires the ability to send spoofed packets
- Abuses “bounce-sites” to attack victims
  - Traffic multiplied by a factor of 50 to 200

Description of Smurfing Attack

ICMP echo (spoofed source address of victim)
Sent to IP broadcast address

ICMP echo reply

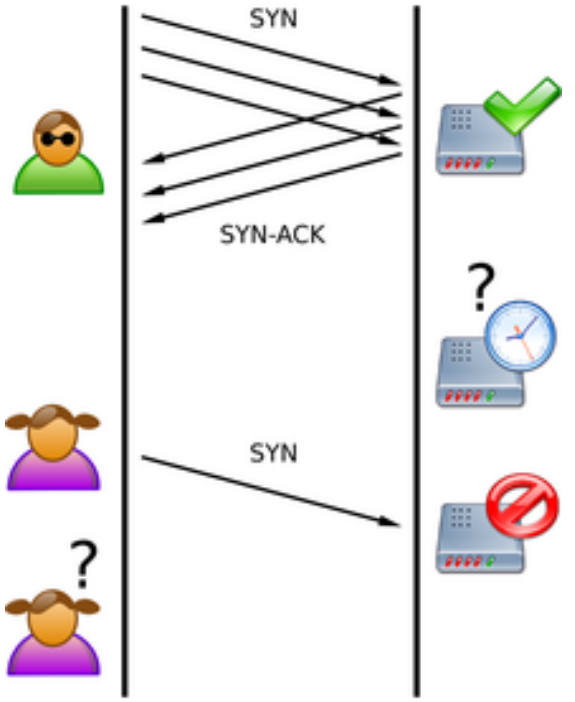


How to prevent being a “bounce site”

- Turn off directed broadcasts to subnets with 5 hosts or more
  - Cisco router: Interface command “no ip directed-broadcast”
- Use access control lists (if necessary) to prevent ICMP echo requests from entering your network
  - Probably not an elegant solution; makes troubleshooting difficult
  - But many networks are doing this now
- Encourage vendors to turn off replies for ICMP echos to broadcast addresses
  - Host Requirements RFC-1122 Section 3.2.2.6 states “An ICMP Echo Request destined to an IP broadcast or IP multicast address MAY be silently discarded.”
  - Patches are available for free UNIX-ish operating systems.

SYN Flooding Attack

- An attacker sends a large number of SYN requests to a target's system
  - Target uses too much memory and CPU resources to process these fake connection requests
  - Target's bandwidth is overwhelmed
- Usually SYN flood packets use spoofed source IPs
  - No TCP connection is set up (not like the TCP hijacking!)
  - Hide attacking source
  - Make the target very hard to decide which TCP SYN is attack and which TCP SYN is from legitimate users!

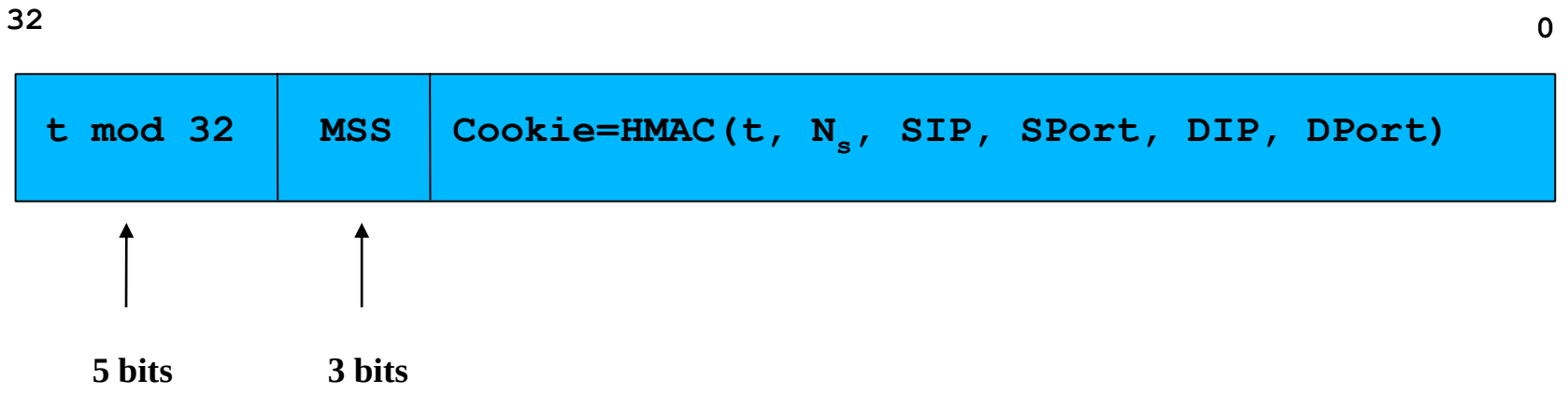


SYN Flood Defense: SYN Cookie

- Some contents from:
- http://www.cc.gatech.edu/classes/AY2007/cs7260_spring/lectures/L18.ppt
- General idea
  - Client sends SYN to server (client_seq number only)
  - Server responds to Client with SYN-ACK cookie
    - Server_sqn = f(src addr, src port, dest addr, dest port, rand)
    - Ack number is normal value: client_seq +1
    - Server does not save state
  - Honest client responds with ACK(client_ack = server_sqn+1)
  - Server checks response
  - If matches SYN-ACK, establishes connection

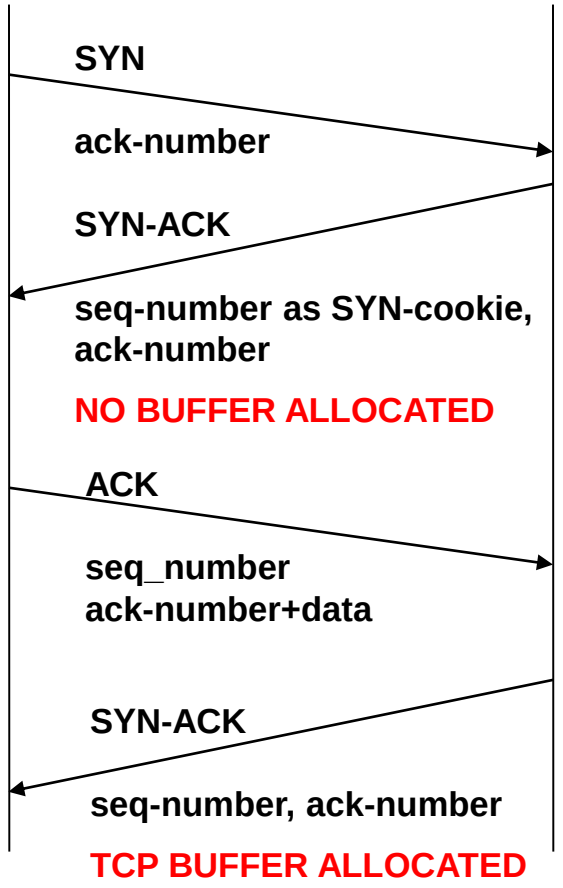
TCP SYN cookie

- TCP SYN/ACK server_seq encodes a cookie
  - 32-bit sequence number
    - **time mod 32:** counter to ensure sequence numbers increase every 64 seconds
    - **MSS:** encoding of server MSS (can only have 8 settings)
    - **Cookie:** easy to create and validate, hard to forge
      - Includes timestamp, nonce, 4-tuple



SYN Cookies

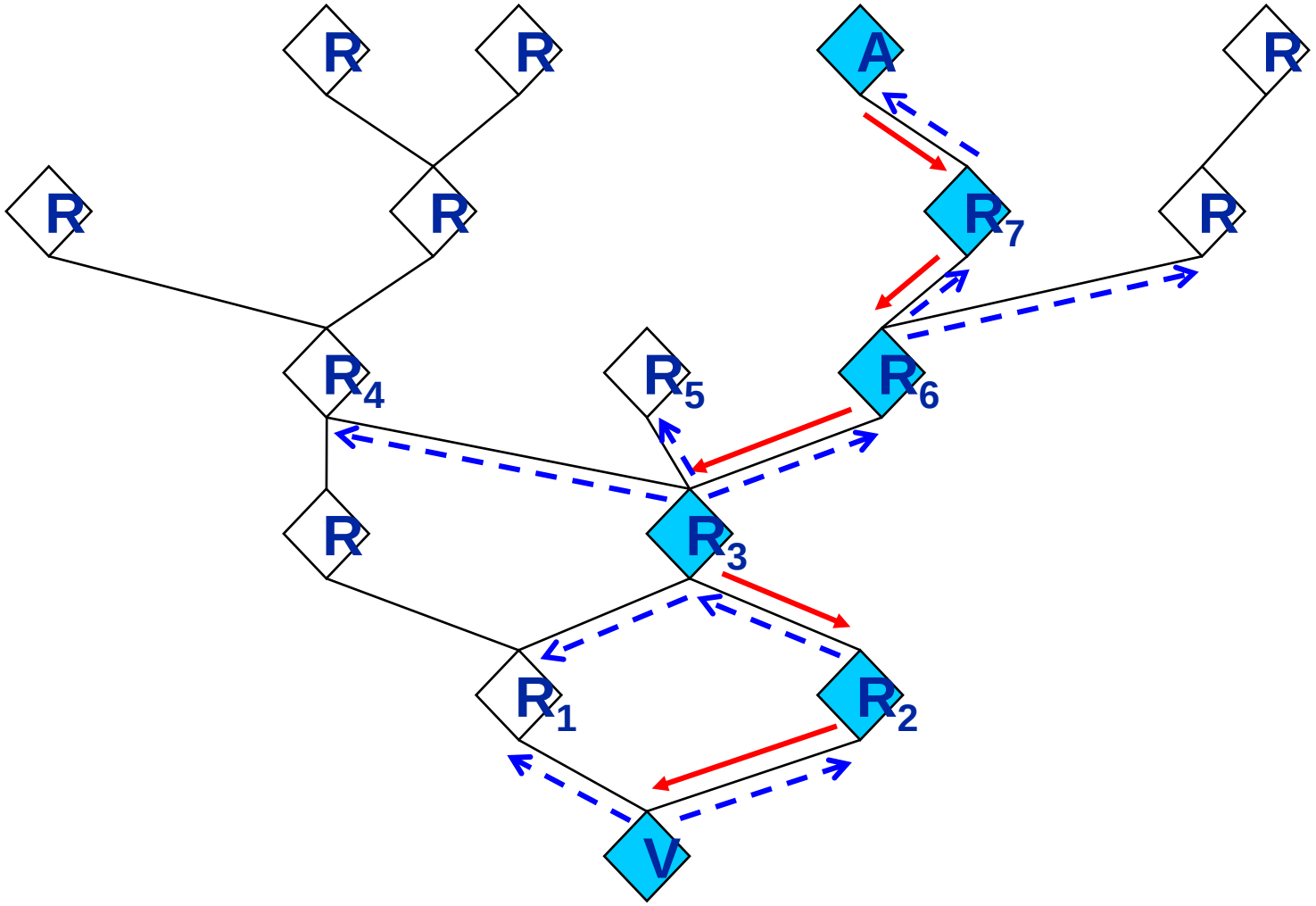
- **client**
  - sends SYN packet and ACK number to server
  - waits for SYN-ACK from server w/ matching ACK number
- **server**
  - responds w/ SYN-ACK packet w/ initial SYN-cookie sequence number
  - Sequence number is cryptographically generated value based on client address, port, and time.
- **client**
  - sends ACK to server w/ matching sequence number
- **server**
  - If ACK is to an unopened socket, server validates returned sequence number as SYN-cookie
  - If value is reasonable, a buffer is allocated and socket is opened



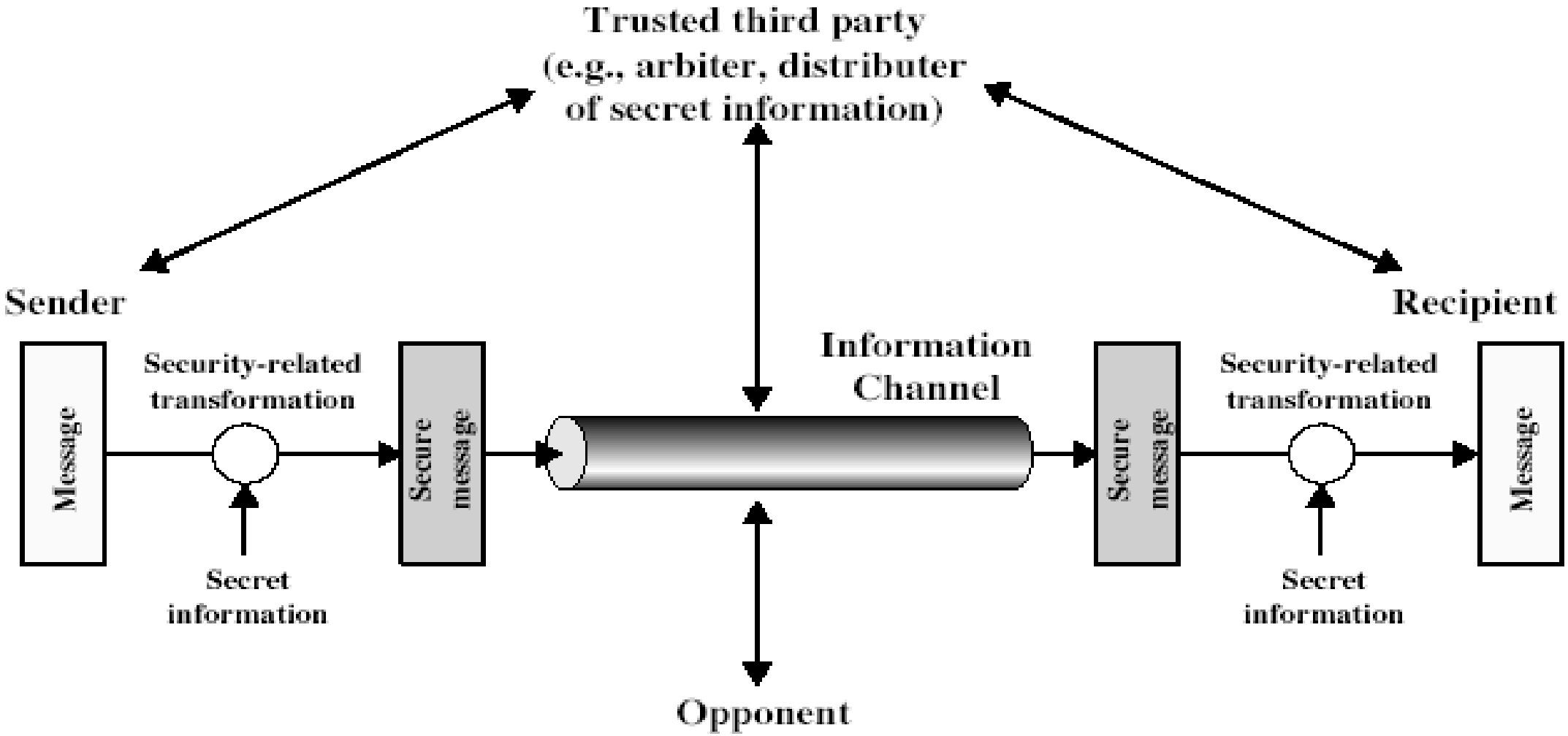
SYN Cookies Limitation

- Windows has not adopted SYN cookies
- Some Linux distributions have used it
- Maximum segment size can only be 8 possible values
- Do not allow the use of TCP option field
  - Many TCP option fields have been used by many programs

IP Traceback



Model for Network Security



Model for Network Security

- using this model requires us to:
  - design a suitable algorithm for the security transformation
  - generate the secret information (keys) used by the algorithm
  - develop methods to distribute and share the secret information
  - specify a protocol enabling the principals to use the transformation and secret information for a security service

Dr. Lokesh Chouhan
NFSU Goa
Lokesh.chouhan_goa@nfsu.ac.in