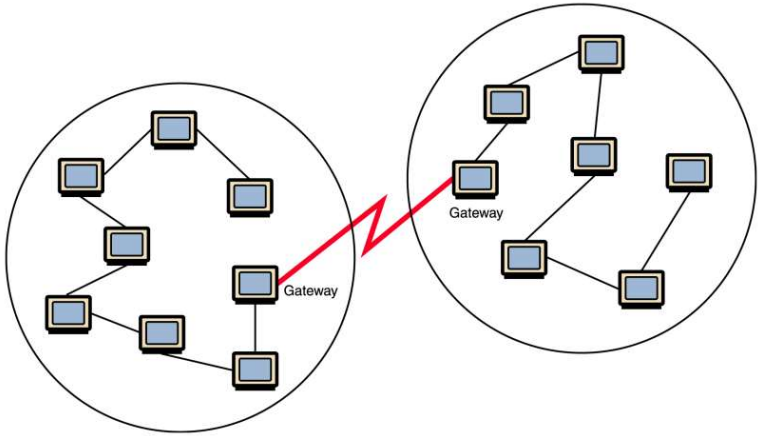
Networks

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



Overview

- **Network Topology**
  how is hardware (physically) connected?
- **Addressing**
  how is a message's destinations identified?
- **Message Delivery**
  should all data be sent in the same fashion?
- **Routing**
  what path through the network is taken?
- **Security**
  how can strangers pass (private) messages?

Networking key terms

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

Networking

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

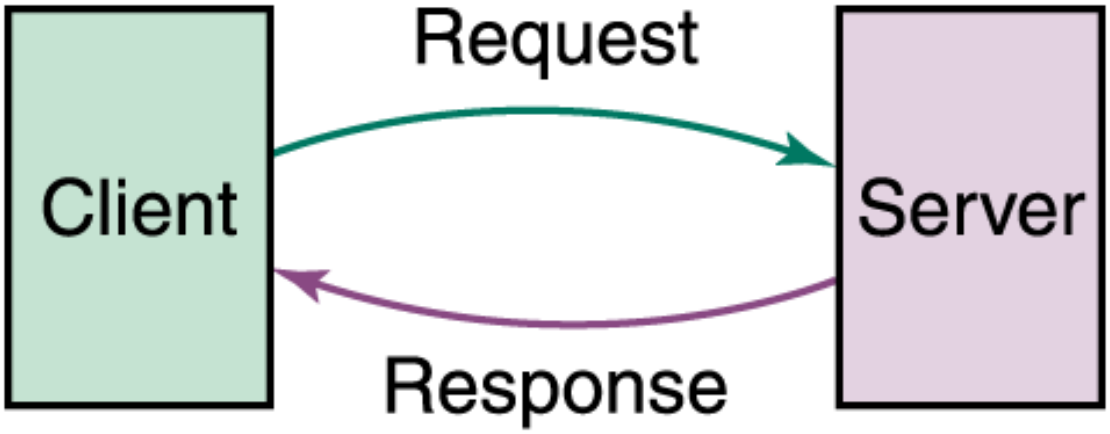


Figure 15.1 Client/Server interaction

Networking

Protocol

A set of rules that defines how data is formatted and processed on a network; i.e., rules that allow client/server interaction

File server

A computer that stores and manages files for multiple users on a network

Web server

A computer dedicated to responding to requests (from the browser client) for web pages

Issue 1: Topology

- If every pair of computers on a network had a dedicated communication link, passing messages would be direct and straightforward. (e.g., the “hotline” between the White House and Kremlin)
- Unfortunately, with hundreds, thousands or millions of computers on a network, they cannot all have direct links to each other.

Network topology

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

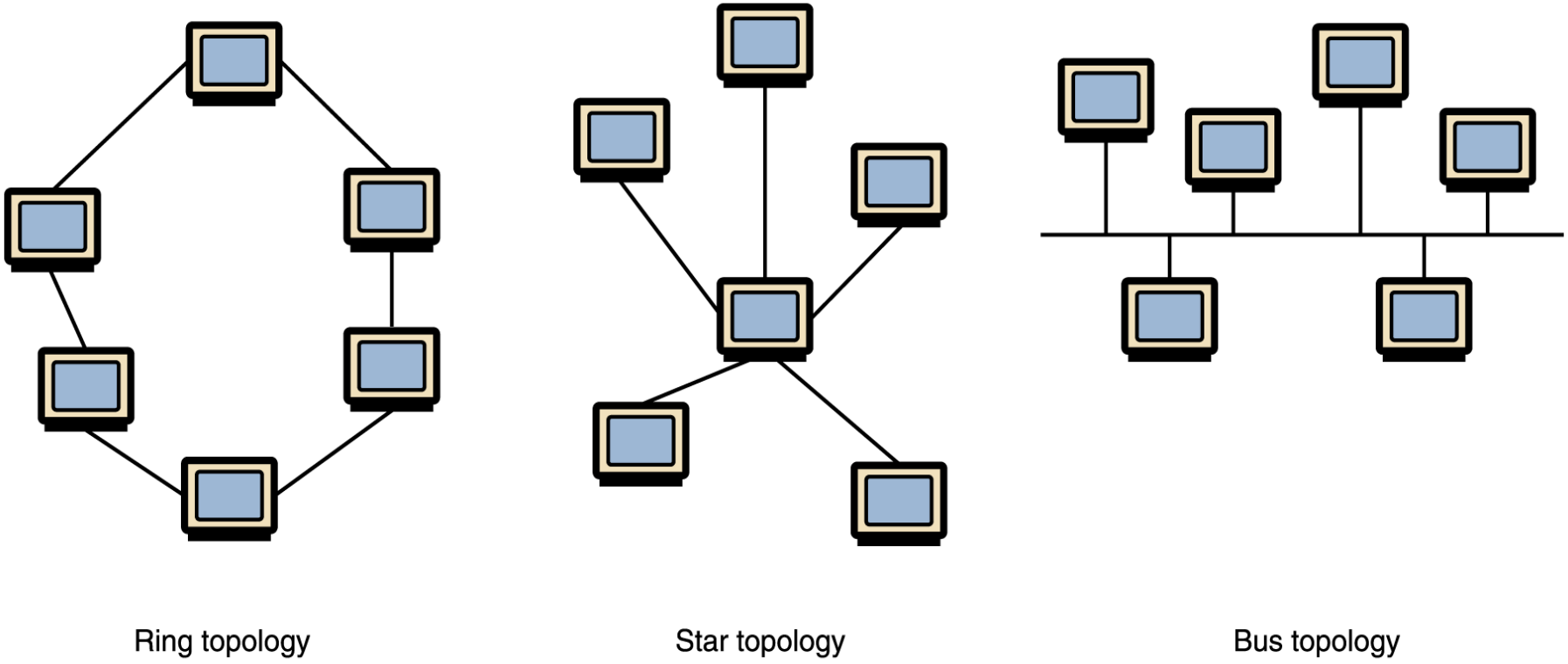


Figure 15.2 **Various network topologies**

Ethernet

The industry standard bus technology for local-area networks

Pros and Cons

Pro's and Con's

- Number of links (they cost money)
- Network Performance

  How efficient is communication?
- Network Reliability

  How does network respond to overload?

  How susceptible is network to collapse?

Best choice depends on the size of the network

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

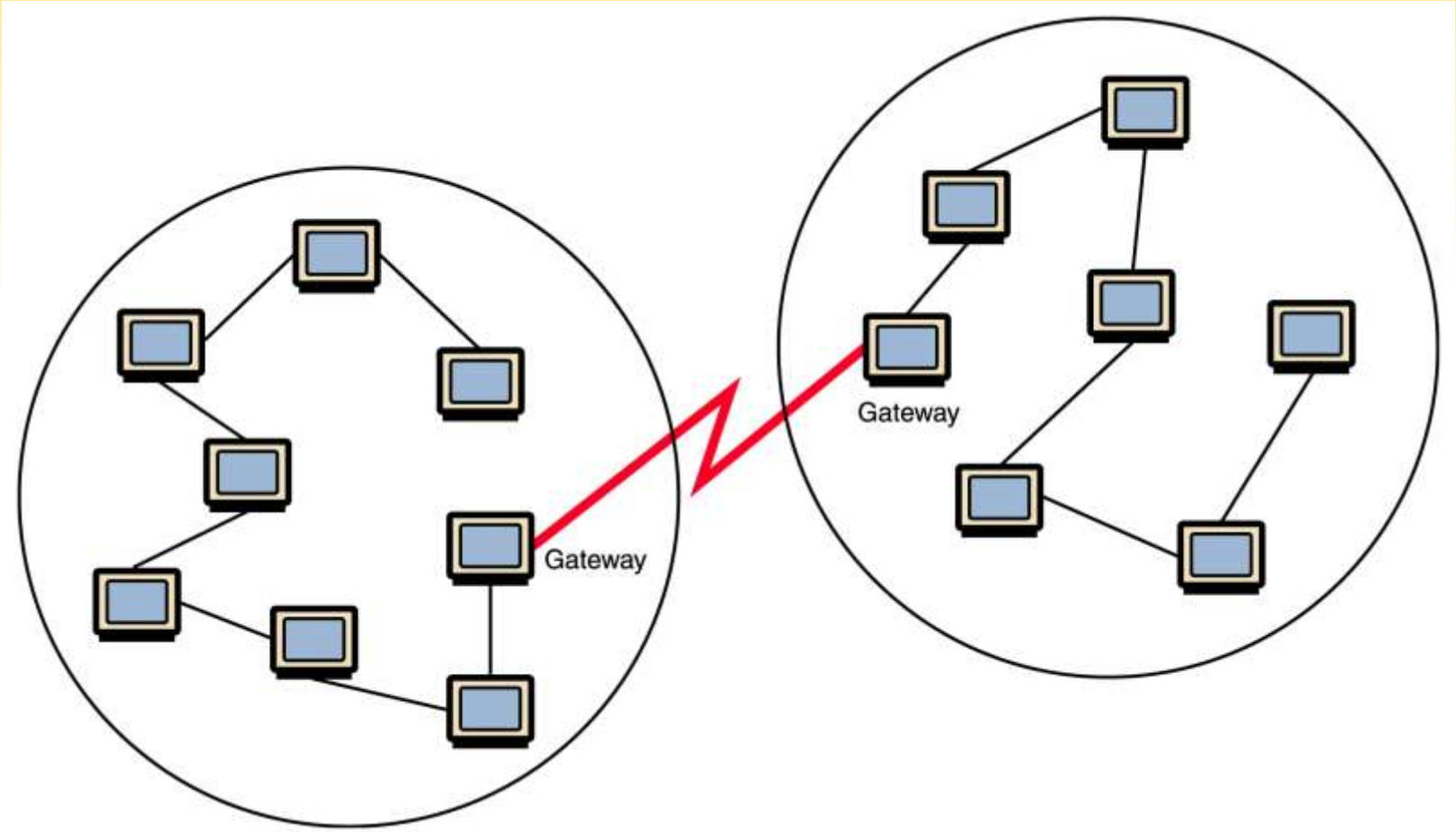


Figure 15.1 **Local-area networks connected across a distance to create a wide-area network**

Types of Networks

Internet

A wide area network that spans the planet

So, who owns the Internet?

Internet Connections

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)

A company that provides other companies or individuals with 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)

Issue 2: Addressing

If a device wants to send a message to another, how does it specify precisely which device?

To what *address*?

Network Addresses

Hostname

A name made up of words separated by dots that uniquely identifies a computer on the Internet:

Example: www.mathcs.slu.edu

IP address

An address made up of four one-byte numeric values separated by dots that uniquely identifies a computer on the Internet

Example: 192.0.0.1

Note: No direct way to translate between these!

IP Addresses

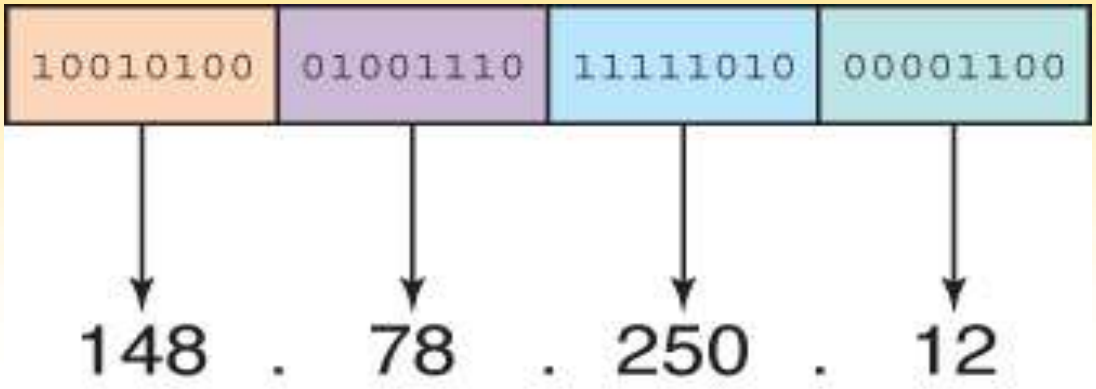


Figure 15.9
An IP address is stored in four bytes

- An **IP address** can be split into
  - **network address**, which specifies a specific network
  - **host number**, which specifies a particular machine in that network

Where does the host number come from?

Network Classes

- The first part of the IP address designates the network. The number of bits in the network address depends upon the size of the network
- Class A network: Designated by first byte
(very large; e.g., Apple has 17.x.x.x, MIT has 9.x.x.x)
- Class B network: Designated by first two bytes
(moderate size; e.g., SLU has 165.134.x.x)
- Class C network: Designated by first three bytes
(very small; e.g., Iowa Public Television iptv.org has 205.221.205.x)

IPv4 and IPv6

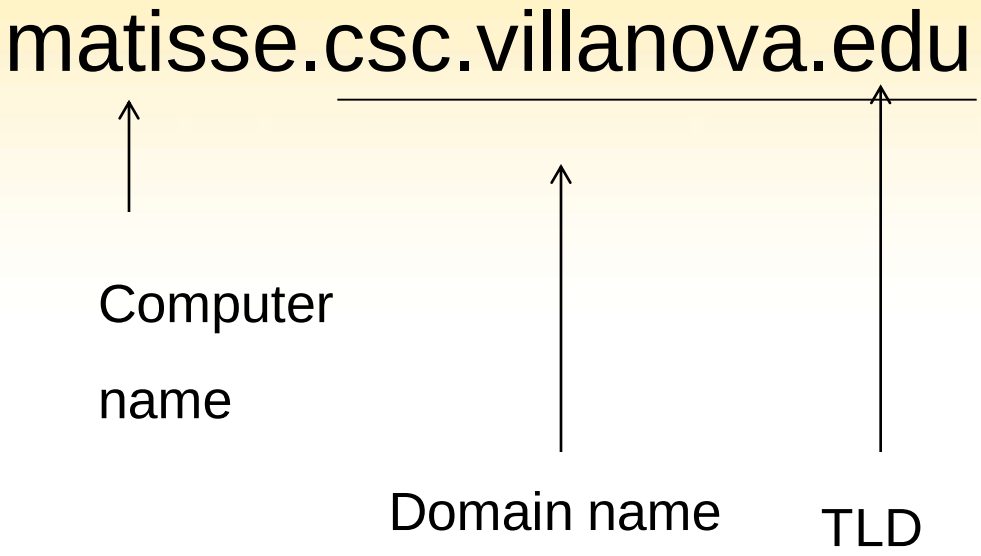
- IPv4 is the protocol using 32-bit addresses. It has been officially used since 1977
- IPv6 is a new protocol (defined in 1996) using 128-bit addresses. The Internet is in the process of transitioning to IPv6

With a vastly larger address space, it provides better separation of network location and host identity, allowing better portability when devices move from network to network.

Domain Name System

- A hostname generally consists of the computer name followed by **the domain name**
- csc.villanova.edu is the domain name
  - A domain name is separated into two or more sections that specify the organization, and possibly a subset of an organization, of which the computer is a part
  - Two organizations can have a computer named the same thing because the domain name makes it clear which one is being referred to

Domain Name System



Domain Name System

Top-Level Domain	General Purpose
.aero	Aerospace industry
.biz	Business
.com*	U.S. Commercial (unrestricted)
.coop	Cooperative
.edu*	U.S. Educational
.gov*	U.S. Government
.info	Information (unrestricted)
.int*	International organizations
.jobs	Employment
.mil*	U.S. Military
.museum	Museums
.name	Individuals and families
.net*	Network (unrestricted)
.org*	Nonprofit organization (unrestricted)
.pro	Certain professions

Figure 15.10 **Top-level domains, including some relatively new ones**

Domain Name System

Organizations based in countries other than the United States use a top-level domain that corresponds to their two-letter country codes

Country Code TLD	Country
.au	Australia
.br	Brazil
.ca	Canada
.gr	Greece
.in	India
.ru	Russian Federation
.uk	United Kingdom

Figure 15.11
Some of the top-level domain names based on country codes

Hostnames->IP addresses

- How is this conversion done?
  - Originally, there was one big table kept on a computer at Stanford. Whenever a computer needed to know an address, it would ask this computer.
  - But as the Internet grew, this computer was overloaded with requests and the underlying table was being updated too often.

Hostnames->IP addresses

- The **domain name system** (DNS) is chiefly used to translate hostnames into numeric IP addresses
  - DNS is an example of a distributed database. Many computer all over the Internet keep (partial) tables.
  - If a server can resolve the hostname, it does
  - If not, that server asks another domain name server for the translations. And so on…

Issue 3: Routing

- When you send something by US Mail:
  - You must give an address which uniquely identifies the recipient
  - You usually send everything in one package. Packages are not all the same size.
  - You do not know what physical route your package will take on its way to destination.
  - Are packages ever lost?
  - How fast would you like delivery to be?
  - Do you want confirmation of receipt?

Delivery on the Internet

- Many different types of data delivered
  - Instant Message (very short)
  - Email (size ranges)
  - Web Page Description (size ranges)
  - Photographs, MP3, software (large)
  - Streaming Radio/Music
  - Streaming Video
- Software protocols are used for delivery

Packet Switching

Packet

A unit of data sent across a network

Router

A network device that directs a packet between networks toward its final destination

Packet switching

Messages are divided into fixed-sized, numbered packets; packets are individually routed to their destination, then reassembled

Packet Switching

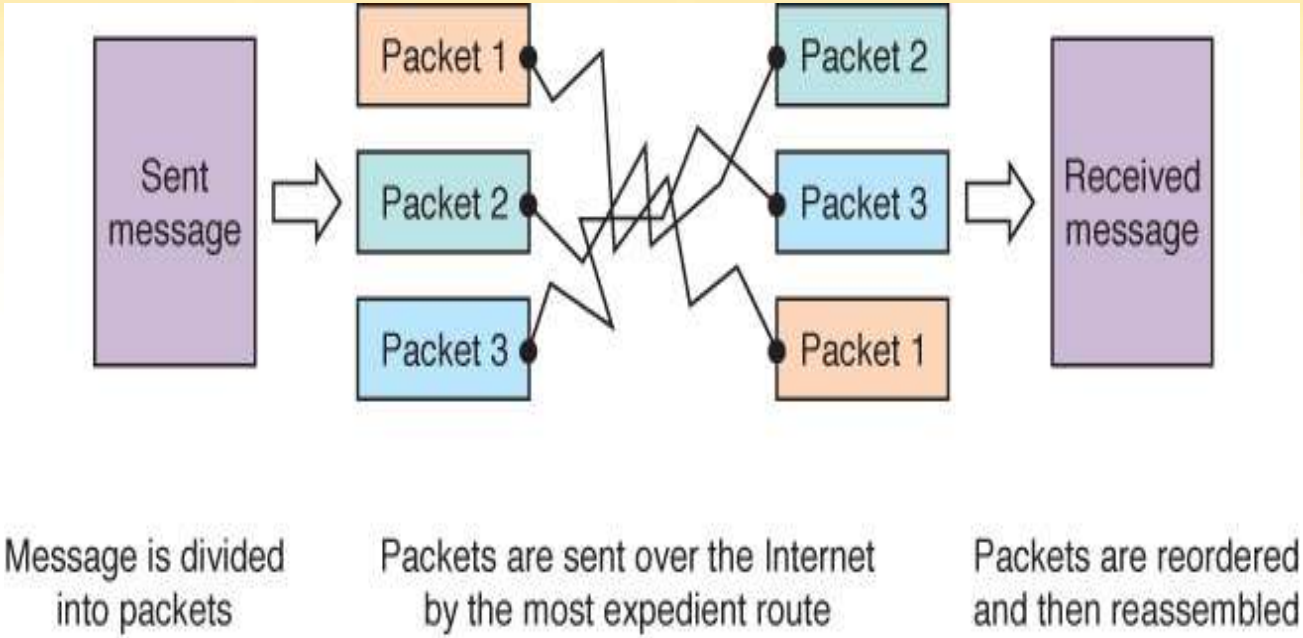


Figure 15.4
Messages sent by packet switching

Take a message, break it into three packets, and simulate this process

Open Systems

A logical progression...

Proprietary system

A system that uses technologies kept private by a particular commercial vendor

Interoperability

The ability of software and hardware on multiple machines and from multiple commercial vendors to communicate

Open systems

Systems based on a common model of network architecture and a suite of protocols used in its implementation

Open Systems

Number	Layer
7	Application layer
6	Presentation layer
5	Session layer
4	Transport layer
3	Network layer
2	Data Link layer
1	Physical layer

Figure 15.5 **The layers of the OSI Reference Model**

Open Systems Interconnection Reference Model

A seven-layer logical break down of network interaction to facilitate communication standards

Each layer deals with a particular aspect of network communication

Network Protocols

- Network protocols are layered such that each one relies on the protocols that underlie it
- Sometimes referred to as a **protocol stack**

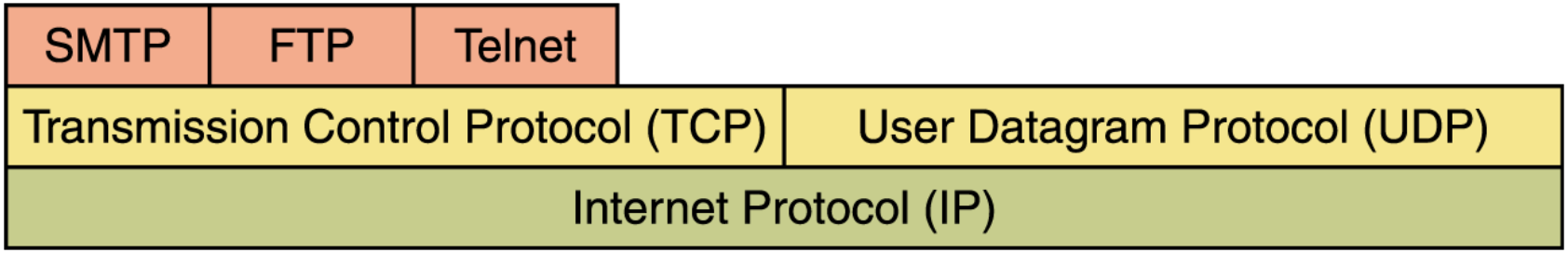


Figure 15.6 **Layering of key network protocols**

TCP/IP

Transmission Control Protocol (TCP)

Software that breaks messages into packets, hands them off to the IP software for delivery, and then orders and reassembles the packets at their destination

Internet Protocol (IP)

Software that deals with the routing of packets through the maze of interconnected networks to their final destination

TCP

- TCP = **Transmission Control Protocol (reliable, but less efficient)**
  - Before sending true message, it sends a warning message to recipient:
    "I'm about to send you a # of packets"
  - It then waits for an acknowledgement message from the recipient
    "okay, I'll watch for them"
  - This process establishes a "connection"

TCP

- Once “connection” is established:
  - Individual packets are sent
  - The receiver separately acknowledges each packet which arrives by sending an ACK. Or if the packet arrived damaged, a negative acknowledgement (NAK)
  - Sender will resend damaged packets. Also, if a long time passes without an ACK or NAK, it assumes the packet must have been lost, and so it resends.

UDP

- UDP stands for **User Datagram Protocol (more efficient, less reliable)**
  - Original device simply sends the packets and doesn't worry about whether they get lost.
- Which protocol would you choose for:
  - Email messages?
  - Streaming Audio?

Other protocols

Ping

A program used to test whether a particular network computer is active and reachable

Traceroute

A program that shows the route a packet takes across the Internet

High-Level Protocols

Other protocols build on TCP/IP protocol suite

- **Simple Mail Transfer Protocol (SMTP)** used to specify transfer of electronic mail
- **File Transfer Protocol (FTP)** allows a user to transfer files to and from another computer
- **Telnet** used to log onto one computer from another
- **Hyper Text Transfer Protocol (http)** allows exchange of Web documents

Which of these have you used?

High-Level Protocols

Protocol	Port
Echo	7
File Transfer Protocol (FTP)	21
Telnet	23
Simple Mail Transfer Protocol (SMTP)	25
Domain Name Service (DNS)	53
Gopher	70
Finger	79
Hypertext Transfer Protocol (HTTP)	80
Post Office Protocol (POP3)	110
Network News Transfer Protocol (NNTP)	119
Internet Relay Chat (IRC)	6667

Port
A numeric designation that corresponds to a particular high-level protocol

Figure 15.7
Some protocols and the ports they use

Issue #4: Routing

- Since there are not **direct** connections between all devices, the communication of messages will need to **routed** through intermediary nodes.
- Of course, there is (intentionally) more than one route between most pairs of nodes on the Internet.
- Deciding on an entire route from the origination is difficult, since it might require a map of the entire Internet.

Message Hops

- If a node has a packet to deliver to a destination, it does not plan the entire route.
- Instead, it simply decides on the single next "hop" for the packet. That is, it chooses one of its neighbors to send it too, and leaves the rest of the routine decisions to that neighbor (or others).

Routing Tables

- Each node has its personal **routing table** which it uses to decide where to pass packets, based on the destination.
- Many complications arise in having routing tables coordinated properly to avoid too many hops (or infinitely many hops in the case that a messages encounters a loop).
- Last resort: "Hot Potato" routing (random)

Final Issue: Security

- How can you pass messages “securely” on an open network like the Internet?
- Issues:
  - your message might be read by others
  - it could presumably even be modified
  - can others read/modify information on your computer which you did not intend to share?
  - can others disrupt efficiency of your system with unnecessary network activity?

Security Solutions

- Some possible techniques for security
  - A group can rely entirely on a private network for important communication.
  - Password Protection!
  - Perhaps your messages can be suitably **encrypted** so that anyone who intercepts it will not be able to understand it or to forward on a forgery.
  - A protected network could be connected to Internet through a single machine (“firewall”)

Firewalls

Firewall

A gateway machine and its software that protects a network by filtering the traffic it allows

Access control policy

A set of rules established by an organization that specify what types of network communication are permitted and denied

Have your messages ever been returned undelivered, blocked by a firewall?

Firewalls

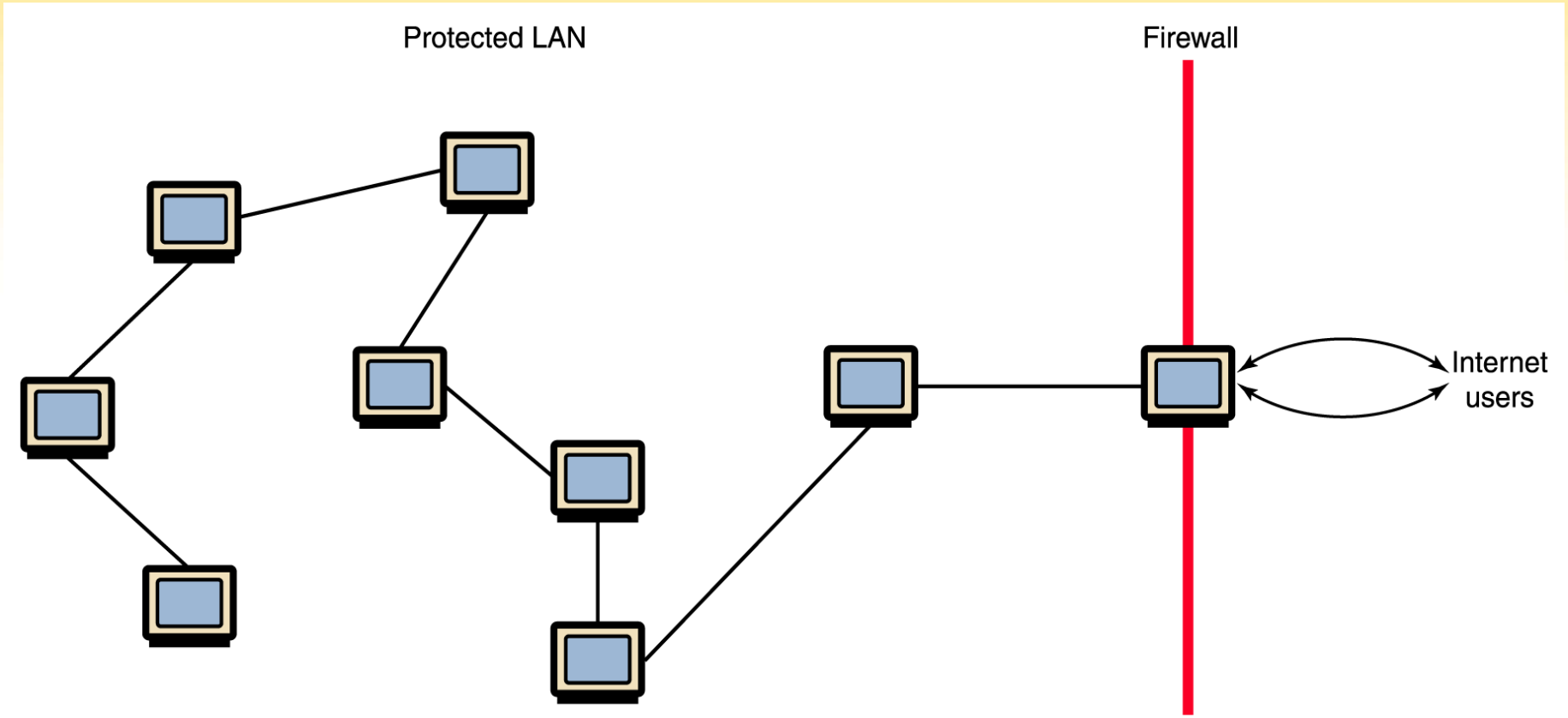


Figure 15.8 **A firewall protecting a LAN**

Social Networks

Social networks are a model (simulation) of how objects--individuals and organizations--interact

- Internal: Participants are within a closed or private community
- External: No restrictions on membership

Functionality

Participants can

- describe themselves
- set privacy settings
- block unwanted members
- have personal pages of pictures/bloggs
- form or be a member of a community within the larger community