Chapter 4: Networking and the Internet

Ref: Computer Science: An Overview
Tenth Edition

by
J. Glenn Brookshear

Lecture Given by Dr. Syed Khaldoon Khurshid

Chapter 4: Networking and the Internet

- 4.1 Network Fundamentals
- 4.2 The Internet
- 4.3 The World Wide Web
- 4.4 Internet Protocols
- 4.5 Security

Networking Basics

Network Classifications

- Scope
  - Local area network (LAN)
  - Metropolitan area (MAN)
  - Wide area network (WAN)
- Ownership
  - Closed versus open
- Topology (configuration)
  - Bus (Ethernet)
  - Star (Wireless networks with central Access Point)

Figure 4.1 **Network topologies**

a. Bus

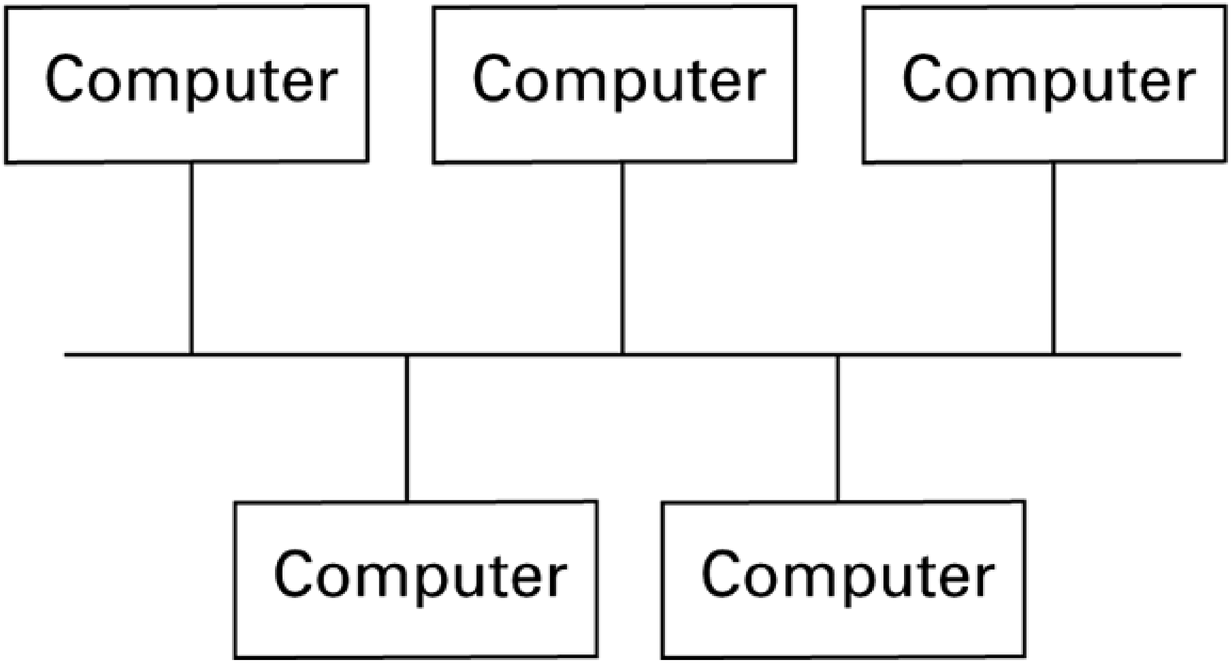
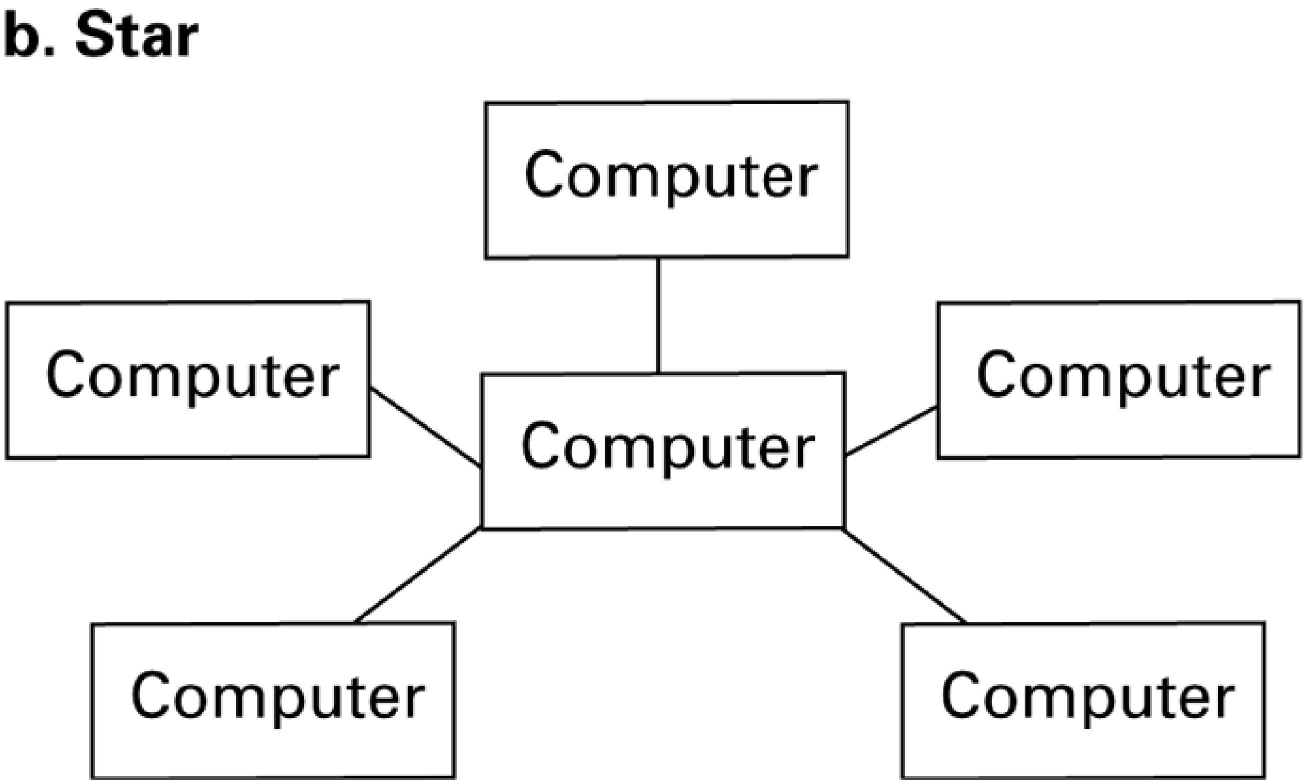


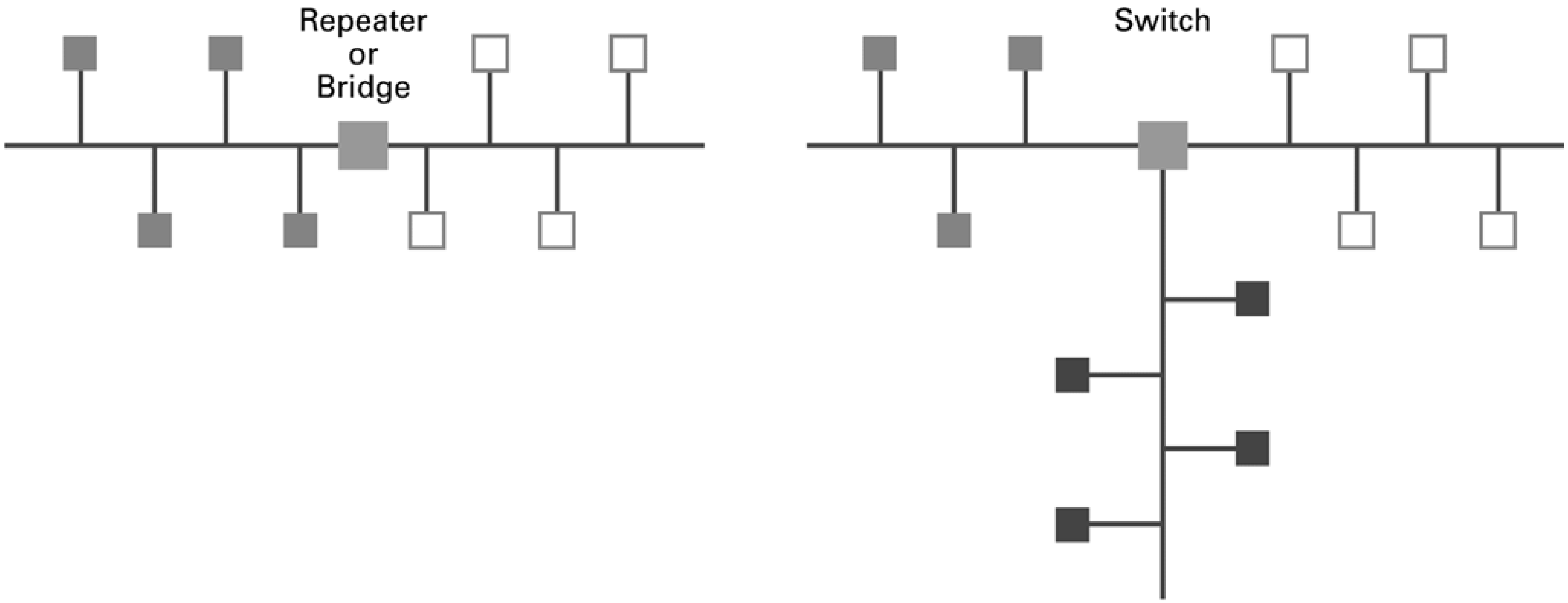
Figure 4.1 **Network topologies (continued)**



Connecting Networks

- **Repeater:** Extends a network
- **Bridge:** Connects two compatible networks
- **Switch:** Connect several compatible networks
- **Router:** Connects two incompatible networks resulting in a network of networks called an **internet**

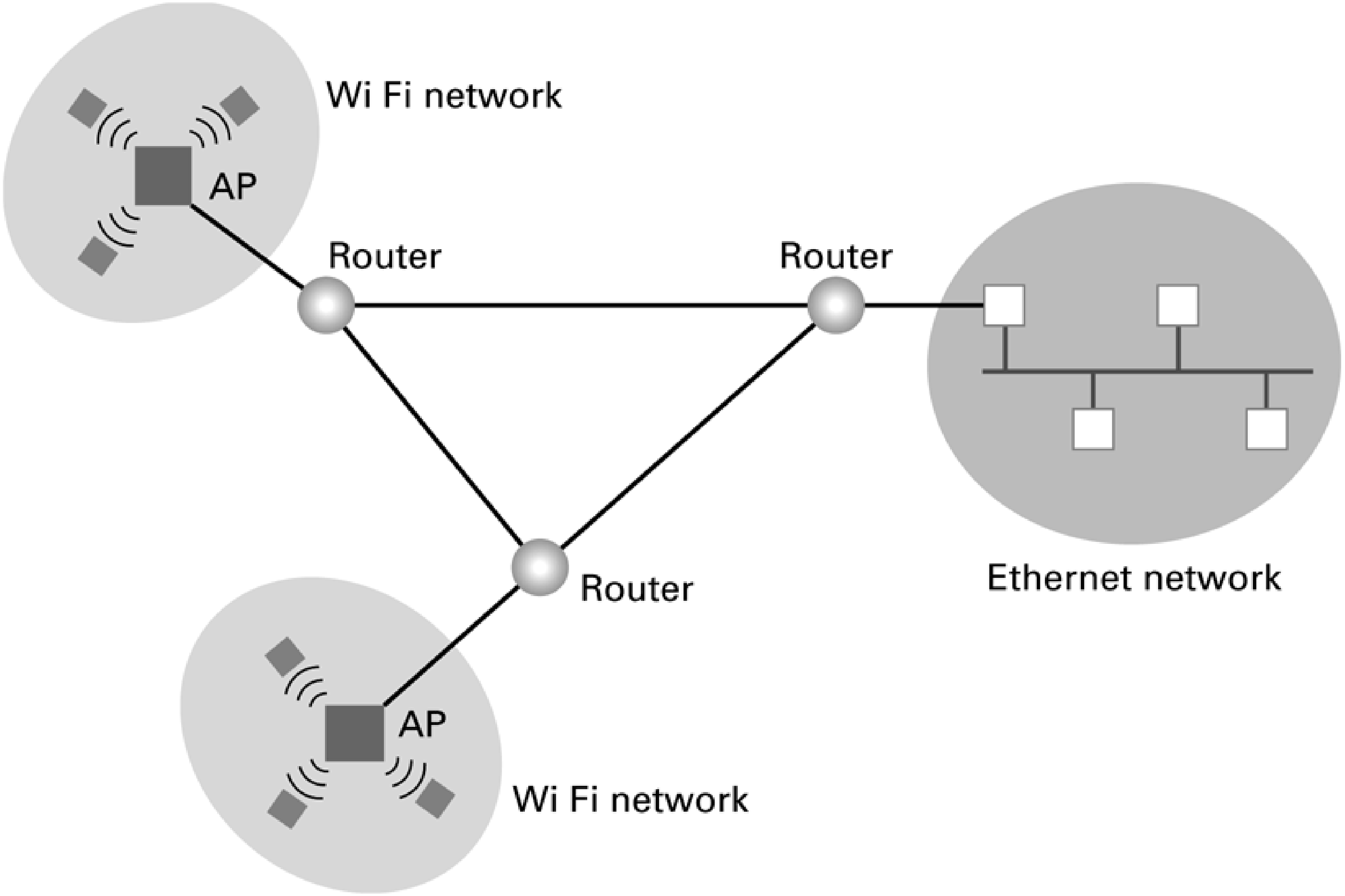
Figure 4.4 **Building a large bus network from smaller ones**



a. A repeater or bridge connecting two buses

b. A switch connecting multiple buses

Figure 4.5 **Routers connecting two WiFi networks and an Ethernet network to form an internet**



The Internet

The Internet

- The Internet: An internet that spans the world
  - Original goal was to develop a means of connecting networks that would not be disrupted by local disasters.
  - Today it has shifted from an academic research project to a commercial undertaking.

Internet Architecture

- Internet Service Provider (ISP)
- Access ISP: Provides connectivity to the Internet
  - Traditional telephone (dial up connection)
  - Cable connections
  - DSL
  - Wireless

Internet Addressing

- IP address: pattern of 32 or 128 bits often represented in dotted decimal notation
- Mnemonic address:
  - Domain names
  - Top-Level Domains
- Domain name system (DNS)
  - Name servers
  - DNS lookup

Internet Corporation for Assigned Names & Numbers (ICANN)

- Allocates IP addresses to ISPs who then assign those addresses within their regions.
- Oversees the registration of domains and domain names.

Traditional Internet Applications

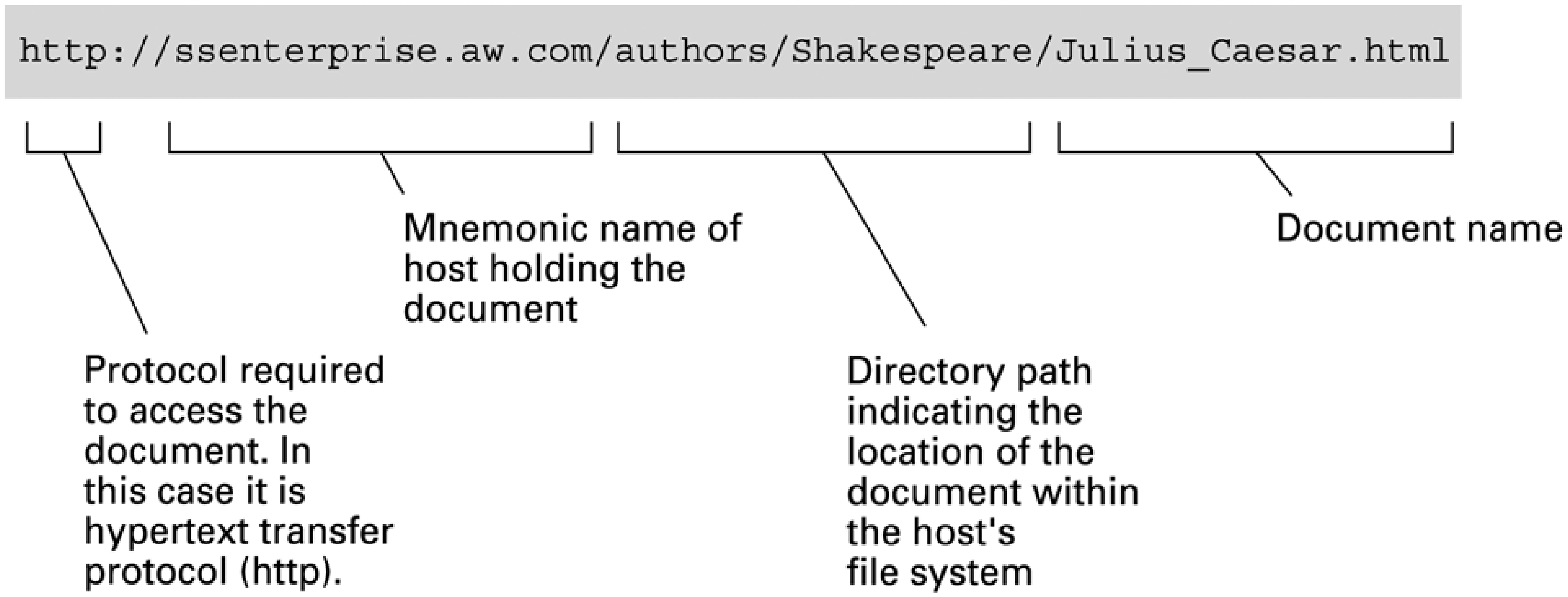
- Electronic Mail (email)
  - Domain mail server collects incoming mail and transmits outgoing mail
  - Mail server delivers collected incoming mail to clients via POP3 or IMAP
  - **Post Office Protocol 3 and Internet Message Access Protocol**
- **File Transfer Protocol (FTP)**
- Telnet and **Secure Shell (SSH)**

The World Wide Web

World Wide Web

- Hypertext and HTTP
- Browser gets documents from Web server
- Documents identified by URLs

Figure 4.8 **A typical URL**



```
http://ssenterprise.aw.com/authors/Shakespeare/Julius_Caesar.html
```

Protocol required to access the document. In this case it is hypertext transfer protocol (http).

Mnemonic name of host holding the document

Directory path indicating the location of the document within the host's file system

Document name

Hypertext Document Format

- Encoded as text file
- Contains tags to communicate with browser
  - Appearance
    - <h1> to start a level one heading
    - <p> to start a new paragraph
  - Links to other documents and content
    - <a href = . . . >
  - Insert images
    - <img src = . . . >

Protocols and Distributed Processes

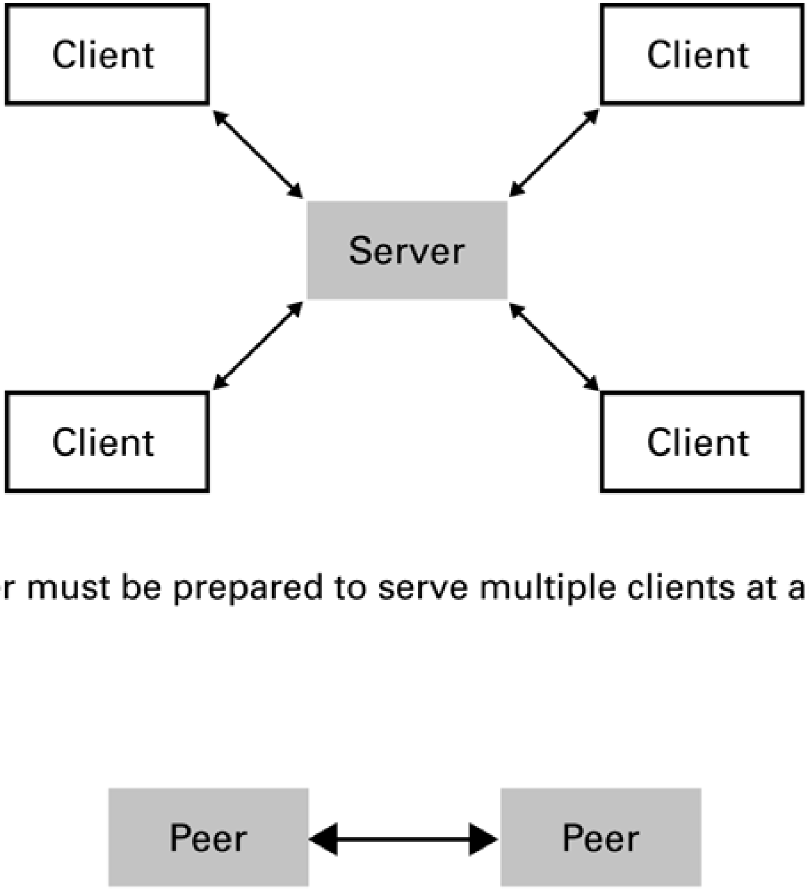
Distributed Systems

- Systems with parts that run on different computers
  - Infrastructure can be provided by standardized toolkits
    - Example: Enterprise Java Beans from Sun Microsystems
    - Example: .NET framework from Microsoft

Inter-process Communication

- Client-server
  - One server, many clients
  - Server must execute continuously
  - Client initiates communication
- Peer-to-peer (P2P)
  - Two processes communicating as equals
  - Peer processes can be short-lived

Figure 4.6 **The client/server model compared to the peer-to-peer model**



a. Server must be prepared to serve multiple clients at any time.

b. Peers communicate as equals on a one-to-one basis.

Client Side Versus Server Side

- Client-side activities
  - Examples: java applets, javascript, Macromedia Flash
- Server-side activities
  - Common Gateway Interface (CGI)
  - Servlets
  - PHP
- “Cloud computing”
  - Basically server-side computing when you don’t know which server is handling your job

Working with IP Addresses

Developed by Peter Smith
peter.joseph.smith@tafensw.edu.au

Introduction

- You can probably work with decimal numbers much easier than with the binary numbers needed by the computer.
- Working with binary numbers is time-consuming & error-prone.

Octets

- The 32-bit IP address is broken up into 4 octets, which are arranged into a dotted-decimal notation scheme.
- An octet is a set of 8 bits & not a musical instrument.
- Example of an IP version 4:

172.64.126.52

Thinking in Binary

- The binary system uses only 2 values “0 & 1” to represent numbers in positions representing increasing powers of 2.
- We all are accustomed to thinking & working in the decimal system, which is based on the number 10.

Thinking in Binary *(Cont.)*

- To most humans, the number 124 represents 100 + 20 + 4.
- To the computer, this number is 1111100, which is 64 (2^6) + 32 (2^5) + 16 (2^4) + 8 (2^3) + 4 (2^2) + 0 + 0

- Each position in a binary number represents, right to left, a power of two beginning with 2^0 & increasing by one power as it moves left: 2^0, 2^1, 2^2, 2^4, etc.

Converting to Decimal

- You'll need to convert binary to decimal & vice versa to compute subnets & hosts.
- So, it's time for a quick review lesson in binary-to-decimal conversion.
- There are 8 bits in an octet & each bit can only be a 1 or a 0.

Converting to Decimal *(Cont.)*

- What then do you suppose is the largest decimal number that can be expressed in an octet?

Eight 1’s (1111 1111)

Converting to Decimal *(Cont.)*

- Now, what is its equivalent decimal value?

2^7	2^6	2^5	2^4	2^3	2^2	2^1	2^0
1	1	1	1	1	1	1	1
128	64	32	16	8	4	2	1

The binary number 1111 1111 converts into the decimal number:

128 + 64 + 32 + 16 + 8 + 4 + 2 + 1 = 255

Converting to Decimal *(Cont.)*

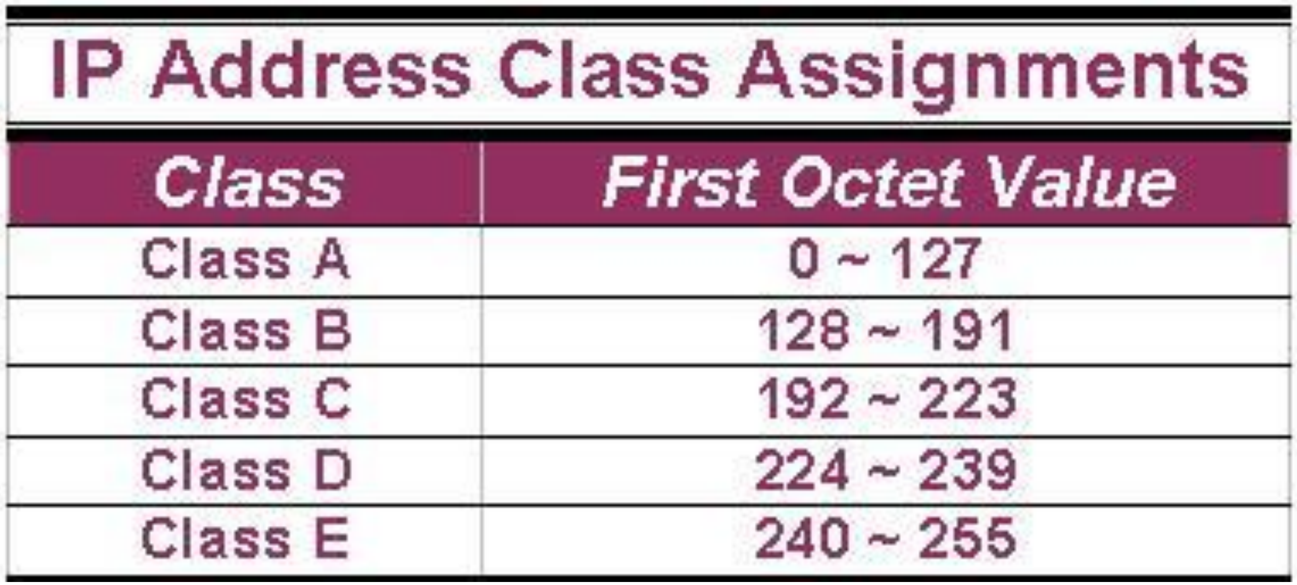
- Therefore, the largest decimal number that can be stored in an IP address octet is 255.
- The significance of this should become evident later in this presentation.

IP Address Classes

- IP addresses are divided into 5 classes, each of which is designated with the alphabetic letters A to E.
- Class D addresses are used for multicasting.
- Class E addresses are reserved for testing & some mysterious future use.

IP Address Classes *(Cont.)*

- The 5 IP classes are split up based on the value in the 1st octet:



IP Address Class Assignments

Class	First Octet Value
Class A	0 ~ 127
Class B	128 ~ 191
Class C	192 ~ 223
Class D	224 ~ 239
Class E	240 ~ 255

IP Address Classes *(Cont.)*

- Using the ranges, you can determine the class of an address from its 1st octet value.
- An address beginning with 120 is a Class A address, 155 is a Class B address & 220 is a Class C address.

Are You the Host or the Network?

- The 32 bits of the IP address are divided into Network & Host portions, with the octets assigned as a part of one or the other.

Network & Host Representation
By IP Address Class

Class	*Octet1*	*Octet2*	*Octet3*	*Octet4*
Class A	Network	Host	Host	Host
Class B	Network	Network	Host	Host
Class C	Network	Network	Network	Host

Are You the Host or the Network? *(Cont.)*

- Each Network is assigned a network address & every device or interface (such as a router port) on the network is assigned a host address.
- There are only 2 specific rules that govern the value of the address.

Are You the Host or the Network? *(Cont.)*

- A host address cannot be designated by all zeros or all ones.
- These are special addresses that are reserved for special purposes.

Class A Addresses

- Class A IP addresses use the 1st 8 bits (1st Octet) to designate the Network address.
- The 1st bit which is always a 0, is used to indicate the address as a Class A address & the remaining 7 bits are used to designate the Network.
- The other 3 octets contain the Host address.

Class A Addresses *(Cont.)*

- There are 128 Class A Network Addresses, but because addresses with all zeros aren’t used & address 127 is a special purpose address, 126 Class A Networks are available.

Class A Addresses *(Cont.)*

- There are 16,777,214 Host addresses available in a Class A address.
- Rather than remembering this number exactly, you can use the following formula to compute the number of hosts available in any of the class addresses, where "**n**" represents the number of bits in the host portion:

$(2^n - 2)$ = Number of available hosts

Class A Addresses *(Cont.)*

- For a Class A network, there are:

  $2^{24} - 2$ or 16,777,214 hosts.

- Half of all IP addresses are Class A addresses.
- You can use the same formula to determine the number of Networks in an address class.
- For Example: a Class A address uses 7 bits to designate the network, so $(2^{7} - 2) = 126$ or there can be 126 Class A Networks.

Class B IP Addresses

- Class B addresses use the 1st 16 bits (two octets) for the Network address.
- The last 2 octets are used for the Host address.
- The 1st 2 bit, which are always 10, designate the address as a Class B address & 14 bits are used to designate the Network. This leaves 16 bits (two octets) to designate the Hosts.

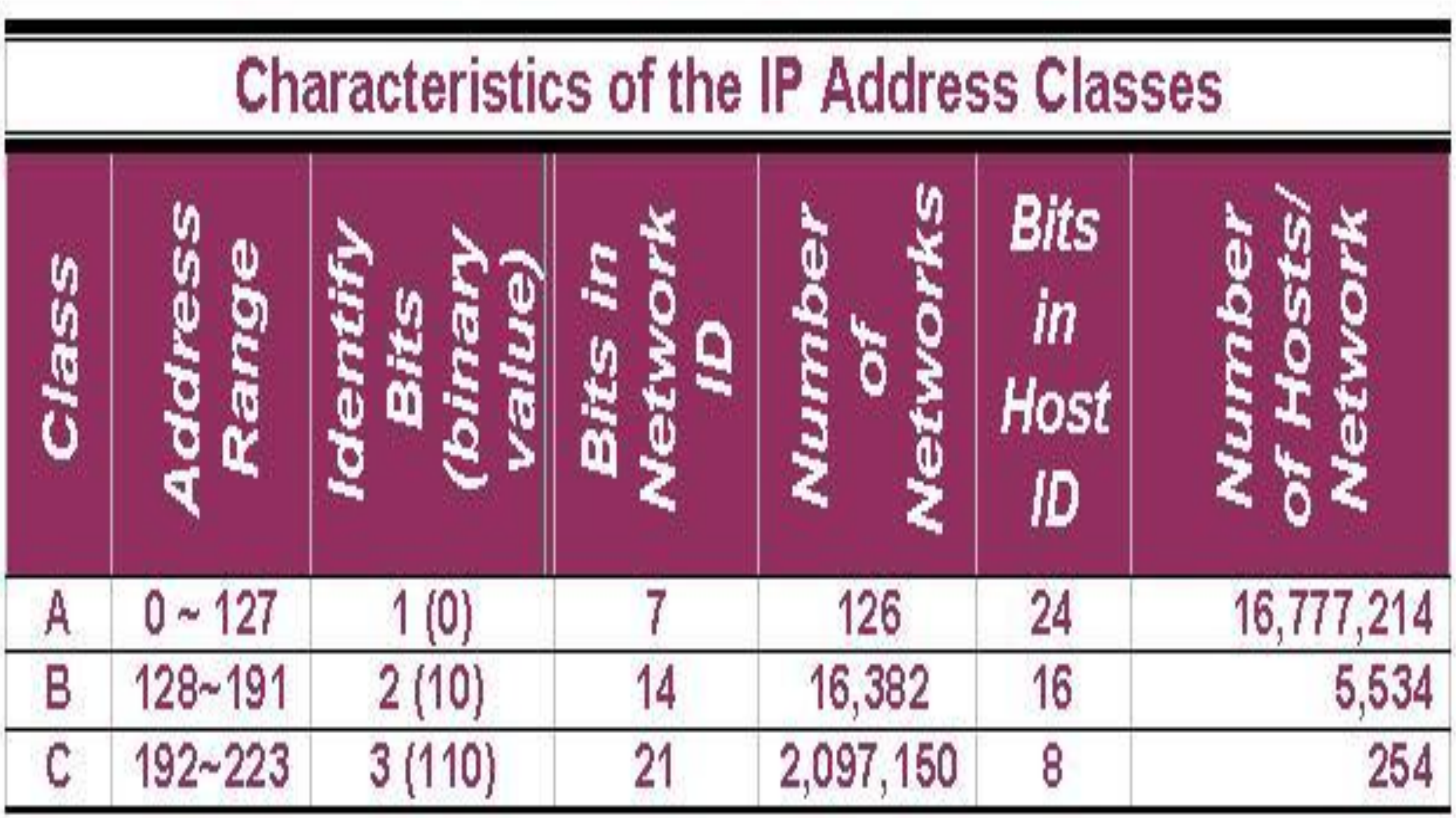
Class B IP Addresses *(Cont.)*

- So how many Class B Networks can there be?
- Using our formula, $(2^{14} – 2)$ there can be 16,382 Class B Networks & each Network can have $(2^{16} – 2)$ Hosts, or 65,534 Hosts.

Class C IP Addresses

- Class C addresses use the 1st 24 bits (three octets) for the Network address & only the last octet for Host addresses. The 1st 3 bits of all class C addresses are set to 110, leaving 21 bits for the Network address, which means there can be 2,097,150 (2^{21} – 2) Class C Networks, but only 254 (2^{8} – 2) Hosts per Network.

Summary of IP Addresses



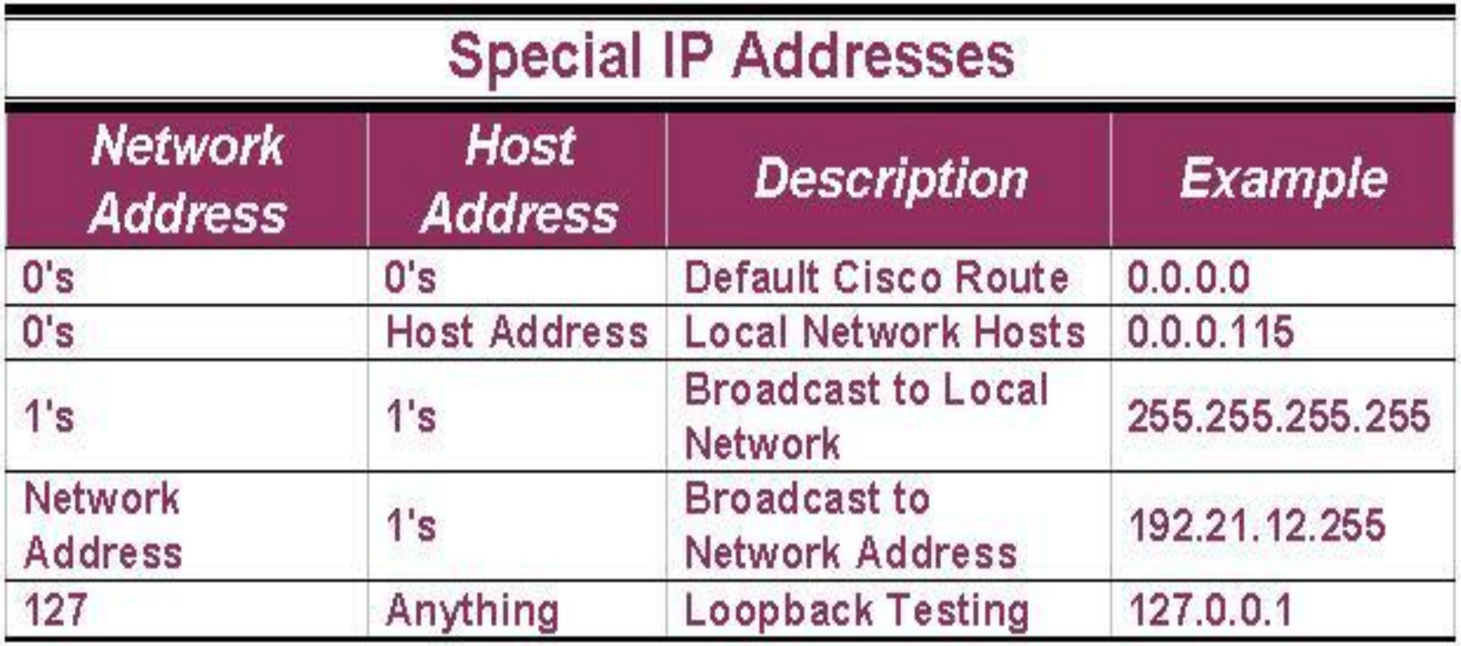
Characteristics of the IP Address Classes

Class	Address Range	Identify Bits (binary value)	Bits in Network ID	Number of Networks	Bits in Host ID	Number of Hosts/ Network
A	0 ~ 127	1 (0)	7	126	24	16,777,214
B	128~191	2 (10)	14	16,382	16	5,534
C	192~223	3 (110)	21	2,097,150	8	254

Special Addresses

- A few addresses are set aside for specific purposes.
- Network addresses that are all binary zeros, all binary ones & Network addresses beginning with 127 are special Network addresses.

Special Addresses *(Cont.)*



Special IP Addresses

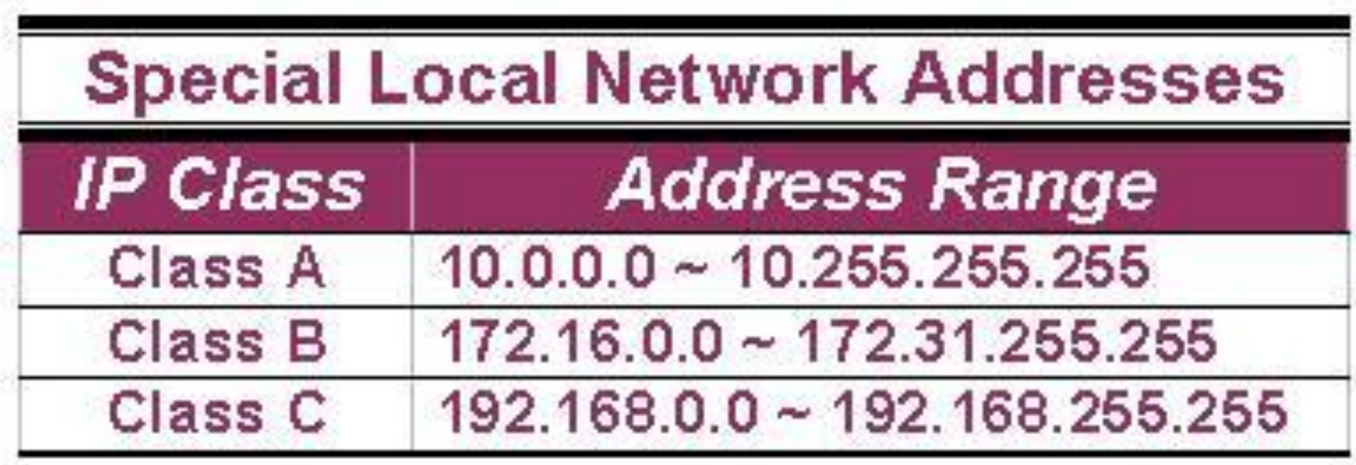
Network Address	Host Address	Description	Example
0's	0's	Default Cisco Route	0.0.0.0
0's	Host Address	Local Network Hosts	0.0.0.115
1's	1's	Broadcast to Local Network	255.255.255.255
Network Address	1's	Broadcast to Network Address	192.21.12.255
127	Anything	Loopback Testing	127.0.0.1

Special Addresses *(Cont.)*

- Within each address class is a set of addresses that are set aside for use in local networks sitting behind a firewall or NAT (Network Address Translation) device or Networks not connected to the Internet.

Special Addresses *(Cont.)*

- A list of these addresses for each IP address class:



Special Local Network Addresses

IP Class	Address Range
Class A	10.0.0.0 ~ 10.255.255.255
Class B	172.16.0.0 ~ 172.31.255.255
Class C	192.168.0.0 ~ 192.168.255.255

Subnet Mask

- An IP address has 2 parts:
  - The Network identification.
  - The Host identification.
- Frequently, the Network & Host portions of the address need to be separately extracted.
- In most cases, if you know the address class, it’s easy to separate the 2 portions.

Subnet Mask *(Cont.)*

- With the rapid growth of the internet & the ever-increasing demand for new addresses, the standard address class structure has been expanded by borrowing bits from the Host portion to allow for more Networks.
- Under this addressing scheme, called Subnetting, separating the Network & Host requires a special process called Subnet Masking.

Subnet Mask *(Cont.)*

- The subnet masking process was developed to identify & extract the Network part of the address.
- A subnet mask, which contains a binary bit pattern of ones & zeros, is applied to an address to determine whether the address is on the local Network.
- If it is not, the process of routing it to an outside network begins.

Subnet Mask *(Cont.)*

- The function of a subnet mask is to determine whether an IP address exists on the local network or whether it must be routed outside the local network.
- It is applied to a message's destination address to extract the network address.
- If the extracted network address matches the local network ID, the destination is located on the local network.

Subnet Mask *(Cont.)*

- However, if they don’t match, the message must be routed outside the local network.
- The process used to apply the subnet mask involves Boolean Algebra to filter out non-matching bits to identify the network address.

Boolean Algebra

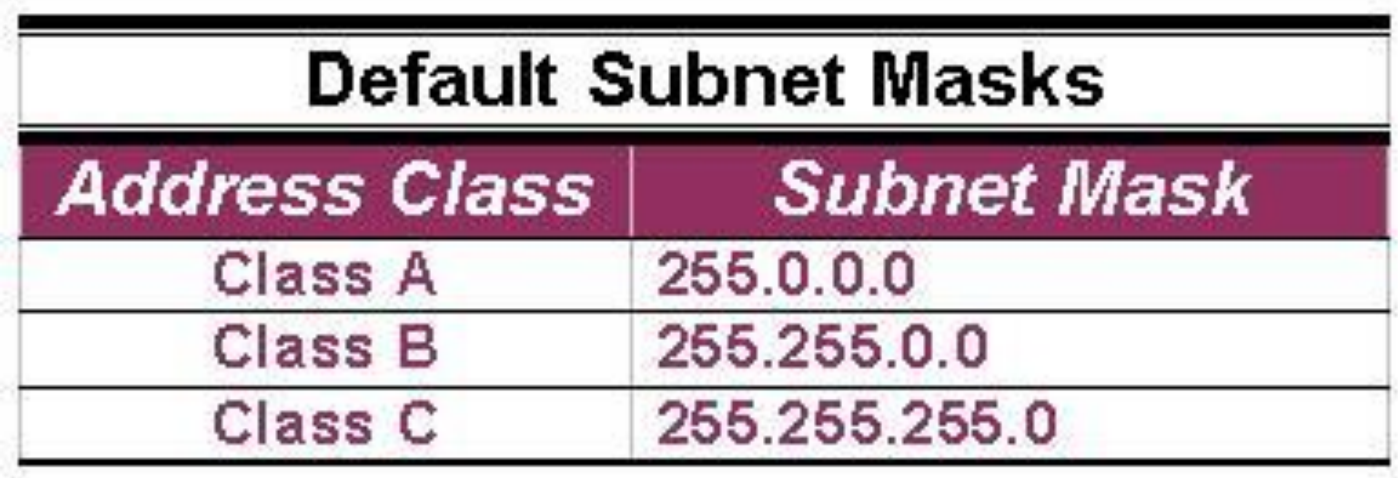
- Boolean Algebra is a process that applies binary logic to yield binary results.
- Working with subnet masks, you need only 4 basic principles of Boolean Algebra:
  - 1 and 1 = 1
  - 1 and 0 = 0
  - 0 and 1 = 0
  - 0 and 0 = 0

Boolean Algebra *(Cont.)*

- In another words, the only way you can get a result of a 1 is to combine 1 & 1. Everything else will end up as a 0.
- The process of combining binary values with Boolean Algebra is called Anding.

Default Standard Subnet Masks

- There are default standard subnet masks for Class A, B and C addresses:

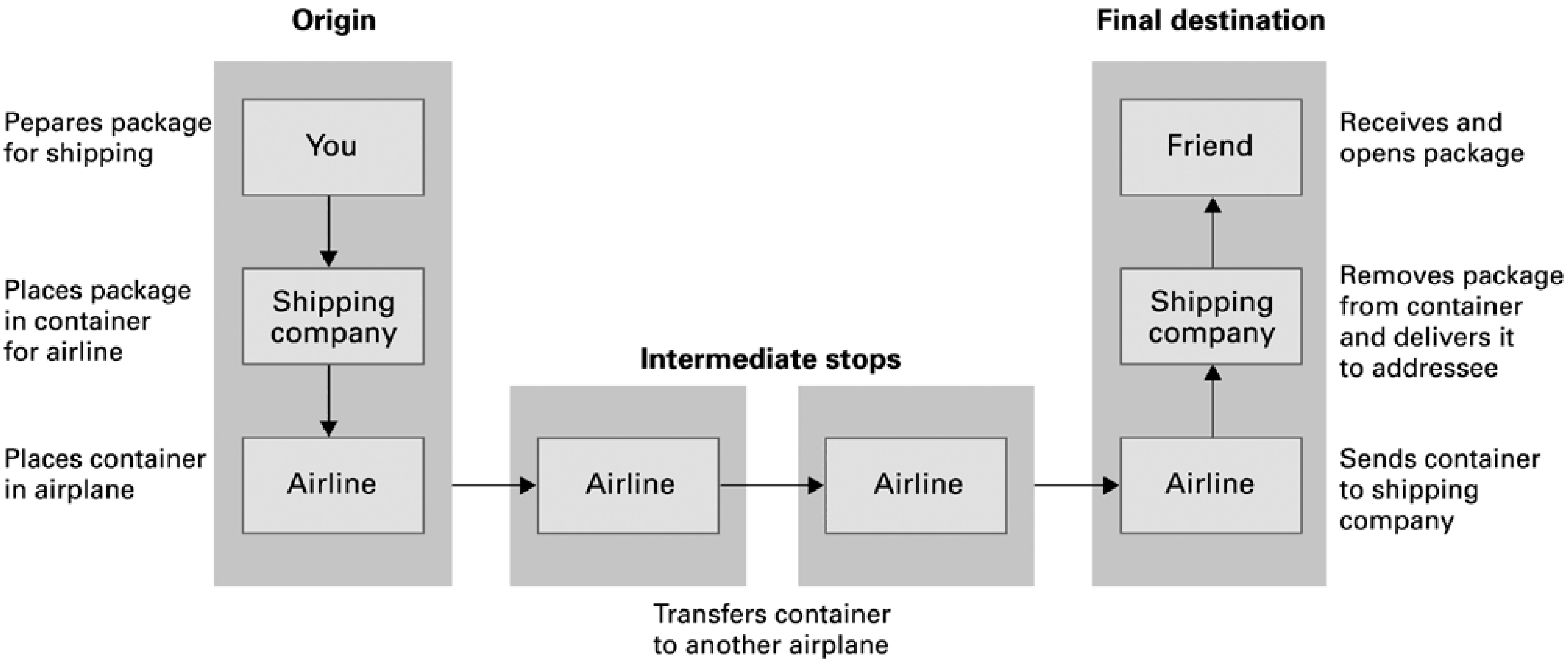


Default Subnet Masks

Address Class	Subnet Mask
Class A	255.0.0.0
Class B	255.255.0.0
Class C	255.255.255.0

Routing Messages

Figure 4.12: Package-shipping example


Origin
Final destination
Pepares package for shipping
You
Friend
Receives and opens package
Places package in container for airline
Shipping company
Shipping company
Removes package from container and delivers it to addressee
Intermediate stops
Places container in airplane
Airline
Airline
Airline
Airline
Sends container to shipping company
Transfers container to another airplane

Internet Software Layers

- **Application:** Constructs message with address
- **Transport:** Chops message into packets
- **Network:** Handles routing through the Internet
- **Link:** Handles actual transmission of packets

Figure 4.13: The Internet software layers

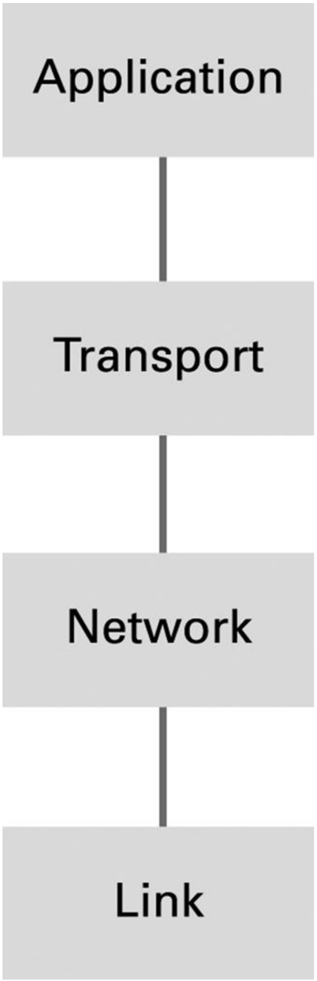
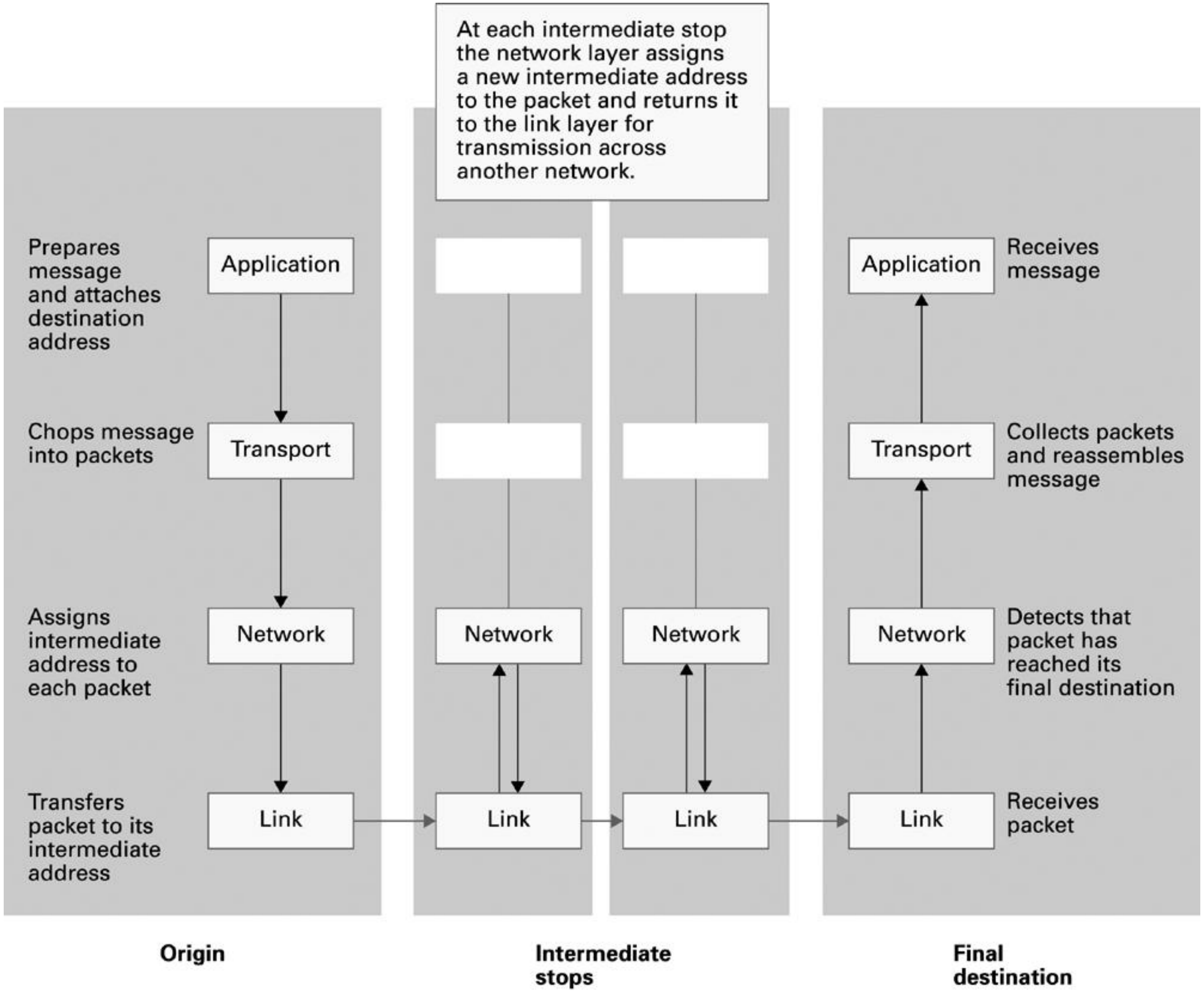


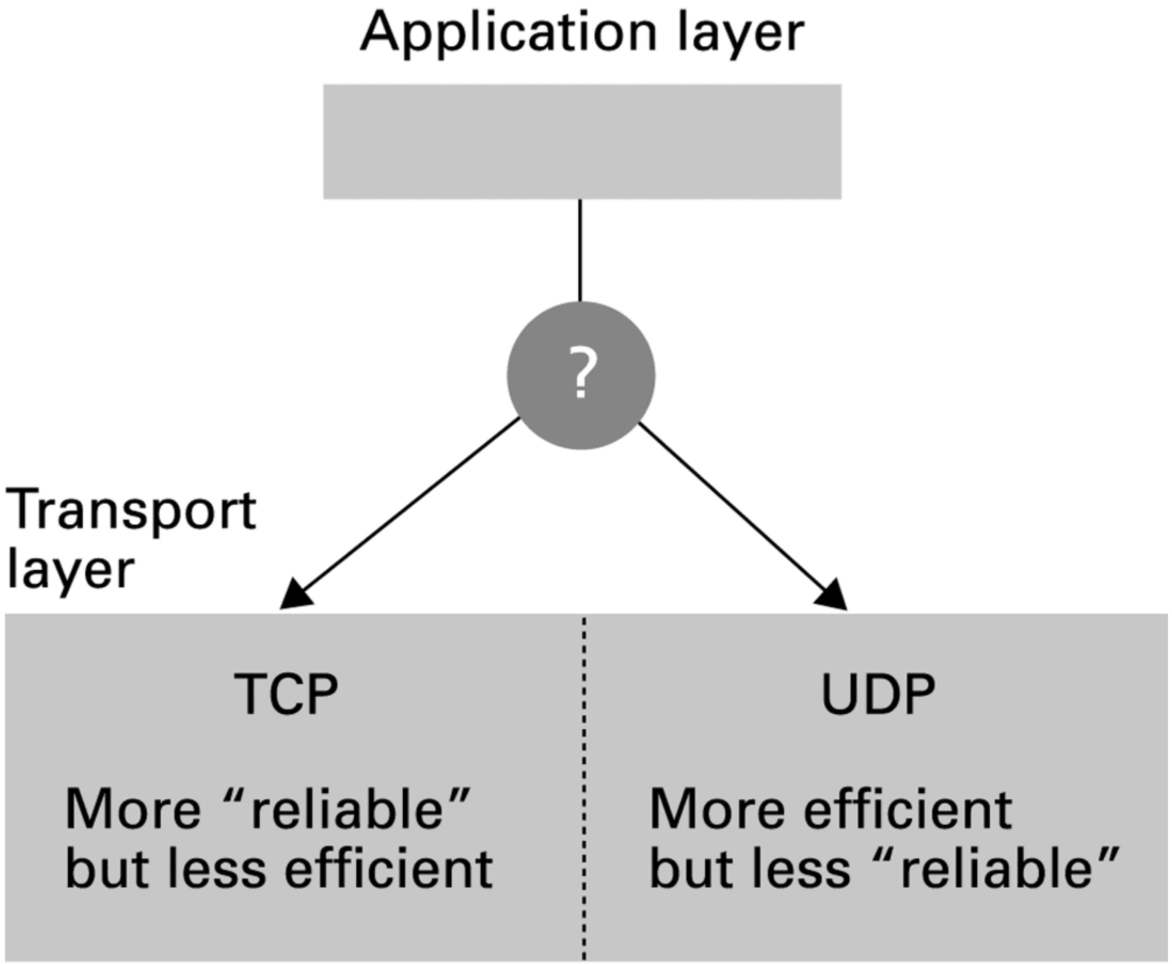
Figure 4.14: Following a message through the Internet


At each intermediate stop the network layer assigns a new intermediate address to the packet and returns it to the link layer for transmission across another network.
Prepares message and attaches destination address
Application
Chops message into packets
Transport
Assigns intermediate address to each packet
Network
Transfers packet to its intermediate address
Link
Network
Link
Network
Link
Application
Receives message
Transport
Collects packets and reassembles message
Network
Detects that packet has reached its final destination
Link
Receives packet
Origin
Intermediate stops
Final destination

TCP/IP Protocol Suite

- Transport Layer
  - TCP
  - UDP
- Network Layer
  - IP (IPv4 and IPv6)

Figure 4.15: Choosing between TCP and UDP


Application layer
?
Transport layer
TCP
More "reliable" but less efficient
UDP
More efficient but less "reliable"

Network Security

Security

- Attacks
  - Malware (viruses, worms, Trojan horses, spyware, phishing software)
  - Denial of service
  - Spam
- Protection
  - Firewalls
  - Spam filters
  - Proxy servers
  - Antivirus software

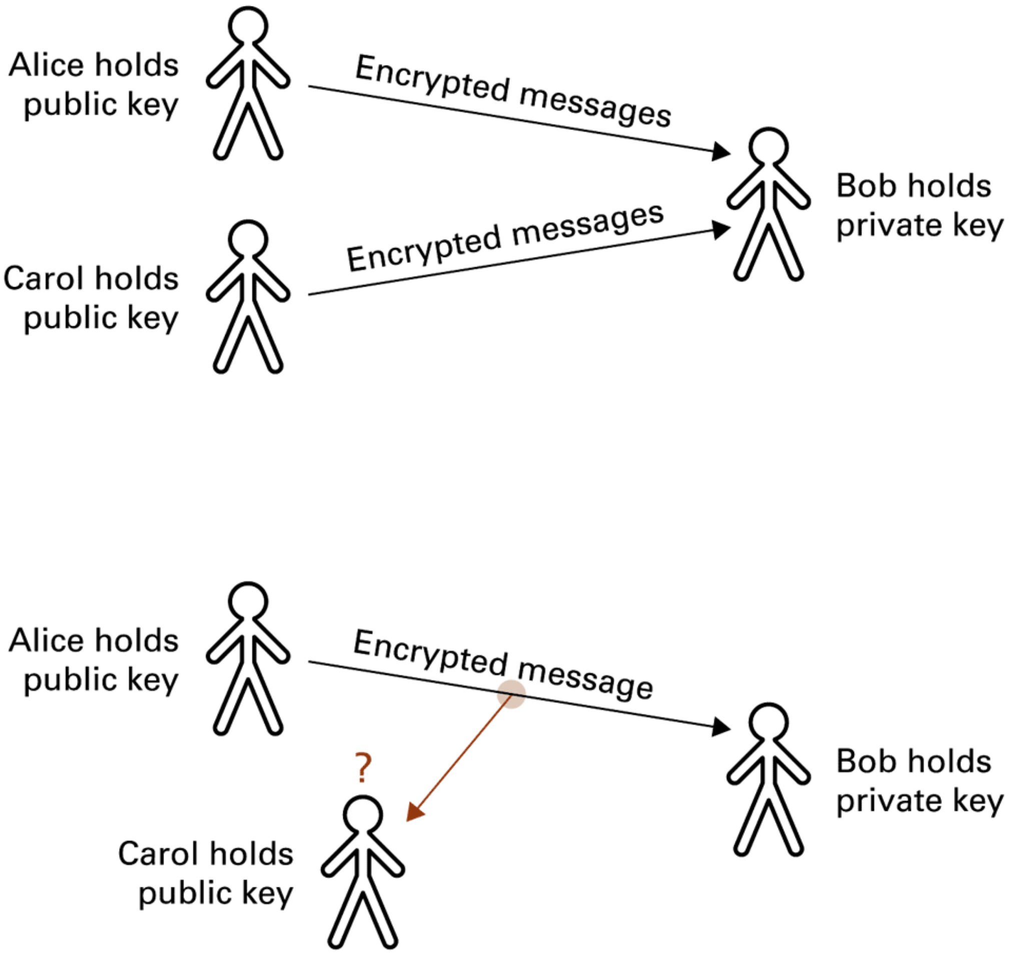
Encryption

- **FTPS**
  - File Transfer Protocol (**FTP**) that adds support for the Transport Layer Security (TLS) and the Secure Sockets Layer (SSL) cryptographic protocols
- **HTTPS**
  - **HTTPS (**Hypertext Transfer Protocol**)** (also called HTTP over TLS, HTTP over SSL, and HTTP Secure) is a protocol for secure communication over a computer network which is widely used on the Internet
- **SSL**
  - **SSL** (Secure Sockets Layer) is the standard security technology for establishing an encrypted link between a web server and a browser. This link ensures that all data passed between the web server and browsers remain private and integral.

Encryption

- Public-key Encryption
  - Public key: Used to encrypt messages
  - Private key: Used to decrypt messages
- Certificates and Digital Signatures

Figure 4.16: **Public-key encryption**



Both Alice and Carol can send encrypted messages to Bob.

Carol cannot decrypt Alice's message even though she knows how Alice encrypted it.

Any
Questions