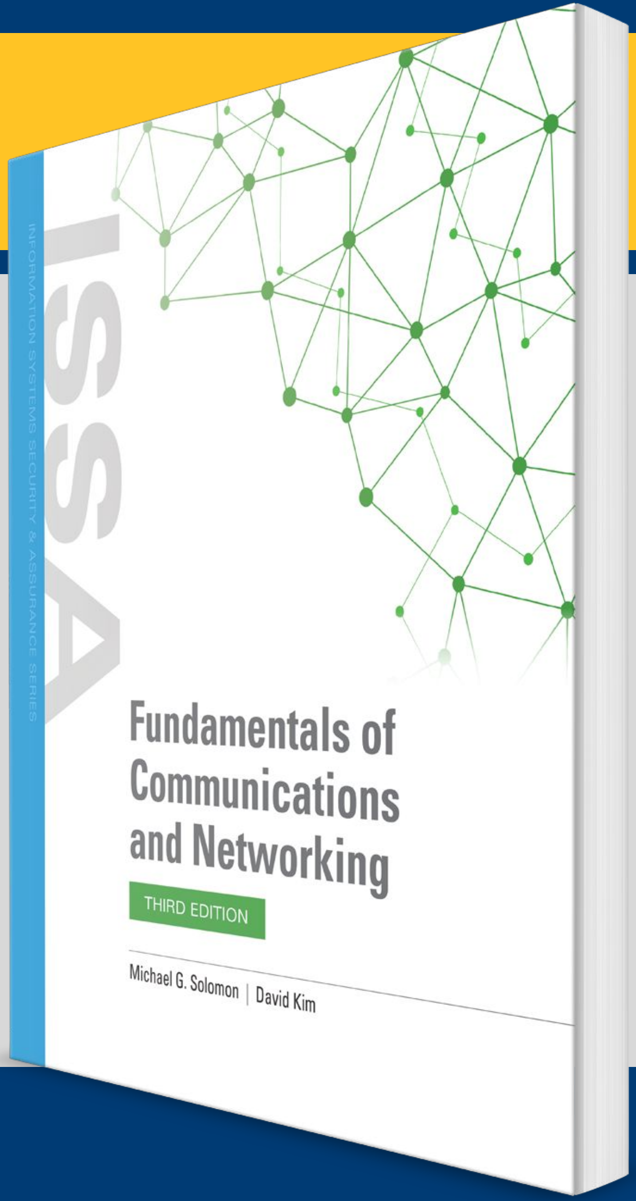
CHAPTER 3

Circuit-Switched, Packet-Switched, and IP-Based Communications


ISSA
INFORMATION SYSTEMS SECURITY & ASSURANCE SERIES
Fundamentals of Communications and Networking
THIRD EDITION
Michael G. Solomon | David Kim

Learning Objective(s) and Key Concepts

Learning Objective(s)

- Examine the TCP/IP protocol family and how IP is used to support voice, video, data, and Internet communications.

Key Concepts

- The OSI and TCP/IP Reference Models
- TCP/IP suite
- Network topologies
- Circuit and packet switching
- IP-based communications and convergence

Open Systems Interconnection Reference Model

- Defines and abstracts network communications
- Logical layers based on communication function
- Hosts interact on same layer

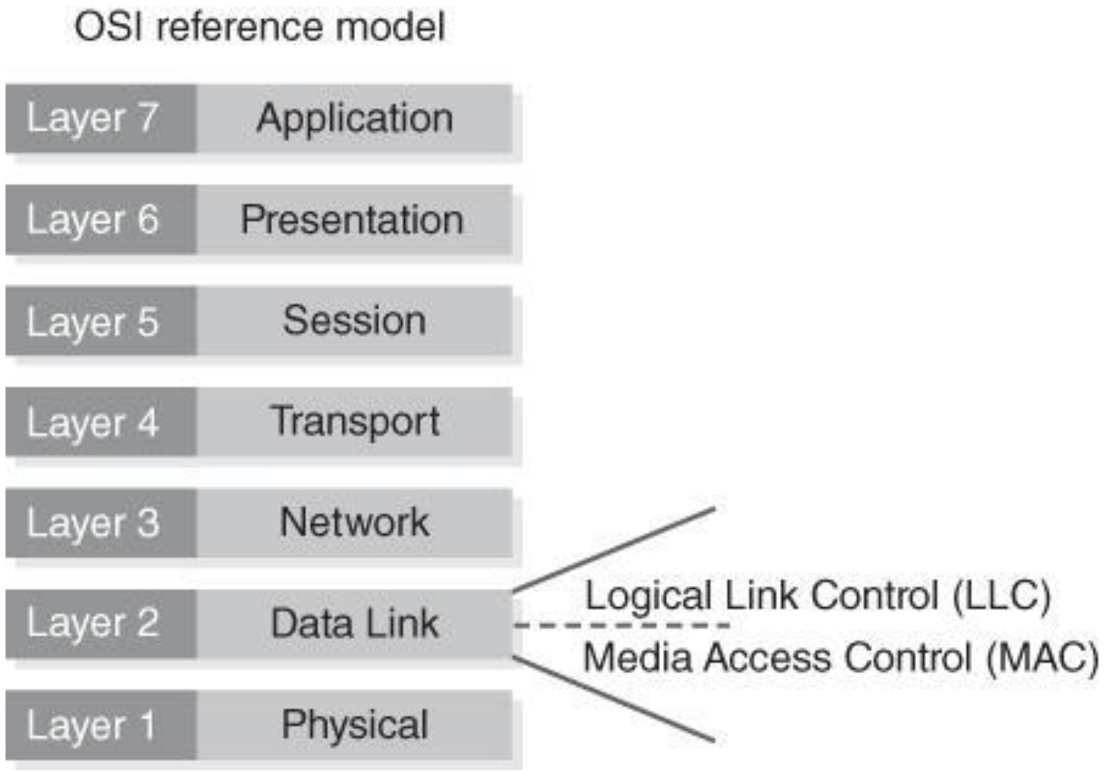


FIGURE 3-2 OSI Reference Model.

OSI Reference Model Layers with Protocols, Applications, and Devices (1 of 2)

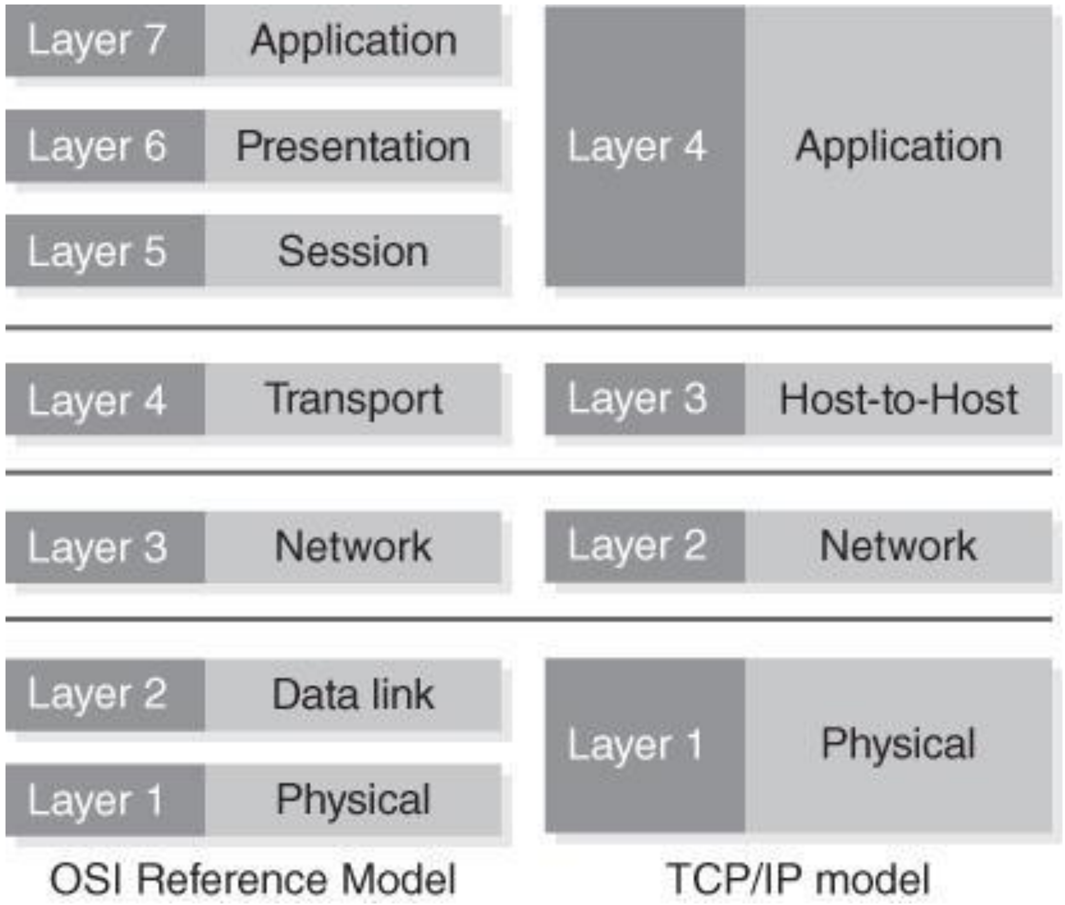
OSI Reference Model Layer	Common Protocols and Applications	Common Devices
Application	BitTorrent, DNC, DSNP, DHCP, FTP, HTTP(S), IMAP, MIME, NNTP, NTP, POP3, RADIUS, RDP, SMTP, SOAP, Telnet	Gateway, firewall, endpoint device (server, PC, mobile device, etc.)
Presentation	AFP, SSL, TLS	Gateway, firewall, server, PC
Session	L2F, L2TP, NetBIOS, NFS, RPC, SMB, SSH	Gateway, firewall, server, PC
Transport	AH (over IP/IPSec), BGP, ESP (over IP/IPSec), TCP, UDP, SPX	Gateway, firewall

OSI Reference Model Layers with Protocols, Applications, and Devices (2 of 2)

OSI Reference Model Layer	Common Protocols and Applications	Common Devices
Network	ICMP, IGMP, IGRP, IPv4, IPv6, IPSec, IPX, GRE, OSPF, RIP	Router, brouter, Layer 3 switch
Data Link	ARP, Ethernet (IEEE 802.3), FDDI, Frame Relay, IND, L2TP, PPP, MAC, NPD, RARP, STP, Token Ring, VLAN, Wi-Fi (IEEE 802.11), WiMax (IEEE 802.16), X.25	Bridge, modem, network card, Layer 2 switch
Physical	Bluetooth, DSL, Ethernet (Physical Layer), USB, Wi-Fi (Physical Layer)	Hub, repeater, cable, fiber, wireless

TCP/IP Reference Model

- Represents the same functionality as the OSI model, but several layers are combined
- Maps well to the TCP/IP protocol suite
- Describes how the Internet Protocol suite operates



OSI Reference Model		TCP/IP model	
Layer 7	Application	Layer 4	Application
Layer 6	Presentation		
Layer 5	Session		
Layer 4	Transport	Layer 3	Host-to-Host
Layer 3	Network	Layer 2	Network
Layer 2	Data link	Layer 1	Physical
Layer 1	Physical		

FIGURE 3-3 A comparison of the TCP/IP and OSI models.

TCP/IP Reference Model Layers

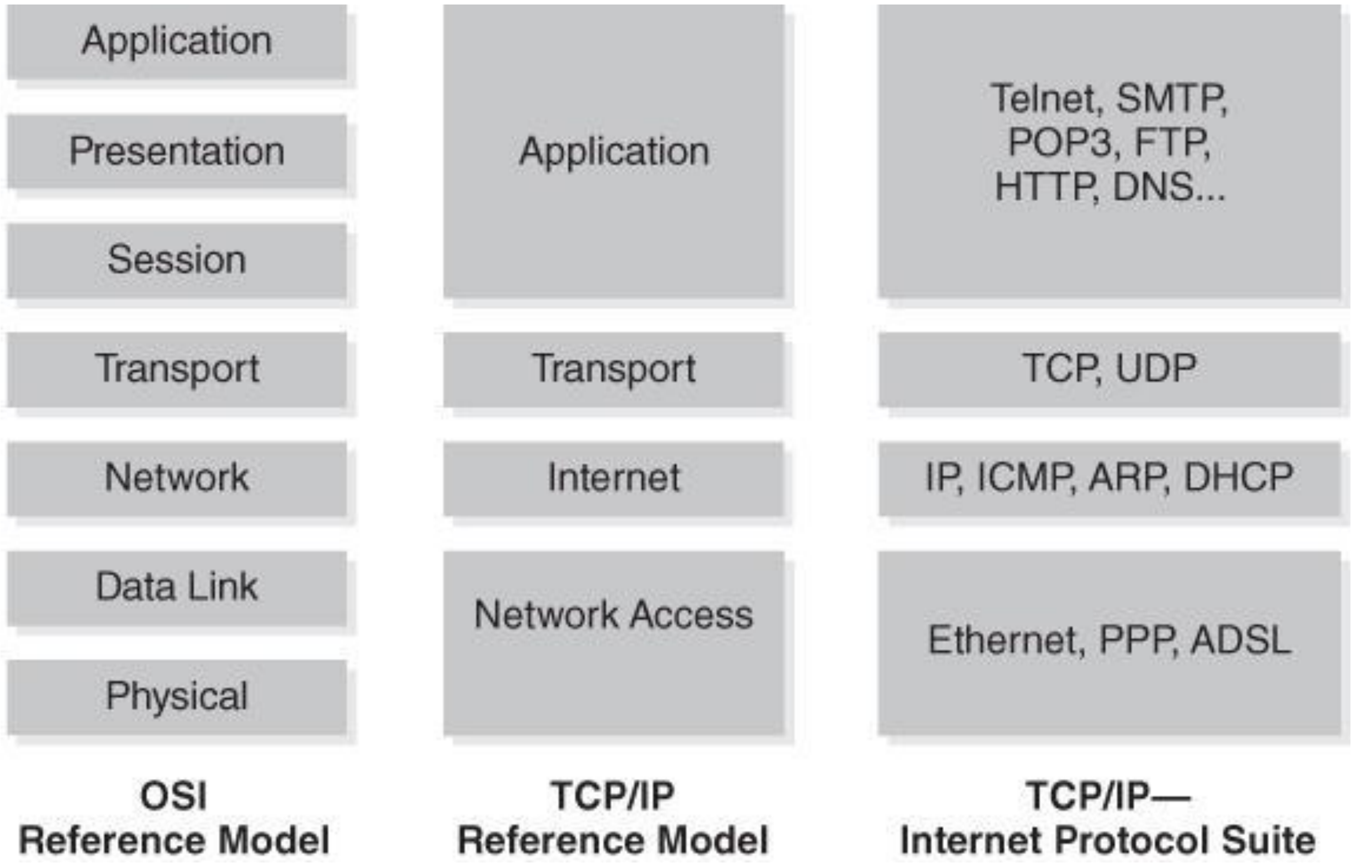
Application Layer	• Interacts with applications that need to gain access to network services
Transport Layer	• Segments the data and adds a checksum to properly validate data to ensure that it has not been corrupted
Internet Layer	• Handles the routing of packets as they move around the network
Network Access Layer	• Point at which the higher-layer protocols interface with the network transport media

TCP/IP Suite

- Provides all of the protocols necessary for applications to exchange messages and data using IP-based networks
- Supports communication across networks ranging from small LANs to the Internet
- TCP/IP family of protocols facilitate voice, video, data transfer, and Internet communications between devices located anywhere in the world

Nearly all Internet-capable operating systems and devices provide support for the protocols defined in the TCP/IP suite

The Main Protocols of the TCP/IP Suite in Relation to the Layers of the Two Reference Models



OSI Reference Model	TCP/IP Reference Model	TCP/IP—Internet Protocol Suite
Application	Application	Telnet, SMTP, POP3, FTP, HTTP, DNS...
Presentation		
Session		
Transport	Transport	TCP, UDP
Network	Internet	IP, ICMP, ARP, DHCP
Data Link	Network Access	Ethernet, PPP, ADSL
Physical		

FIGURE 3-4 The main protocols of the TCP/IP suite in relation to the layers of the two reference models.

Circuit Switching Versus Packet Switching

Types of Switched Networks

Circuit-switched network

- Two devices use the same path, or circuit, throughout a conversation
- Example: Plain old telephone service (POTS)

Packet-switched network

- Separates messages into smaller, manageable-sized chunks called packets
- Software applications may choose to use different packet sizes even when using the same protocol

Circuit-Switched Network

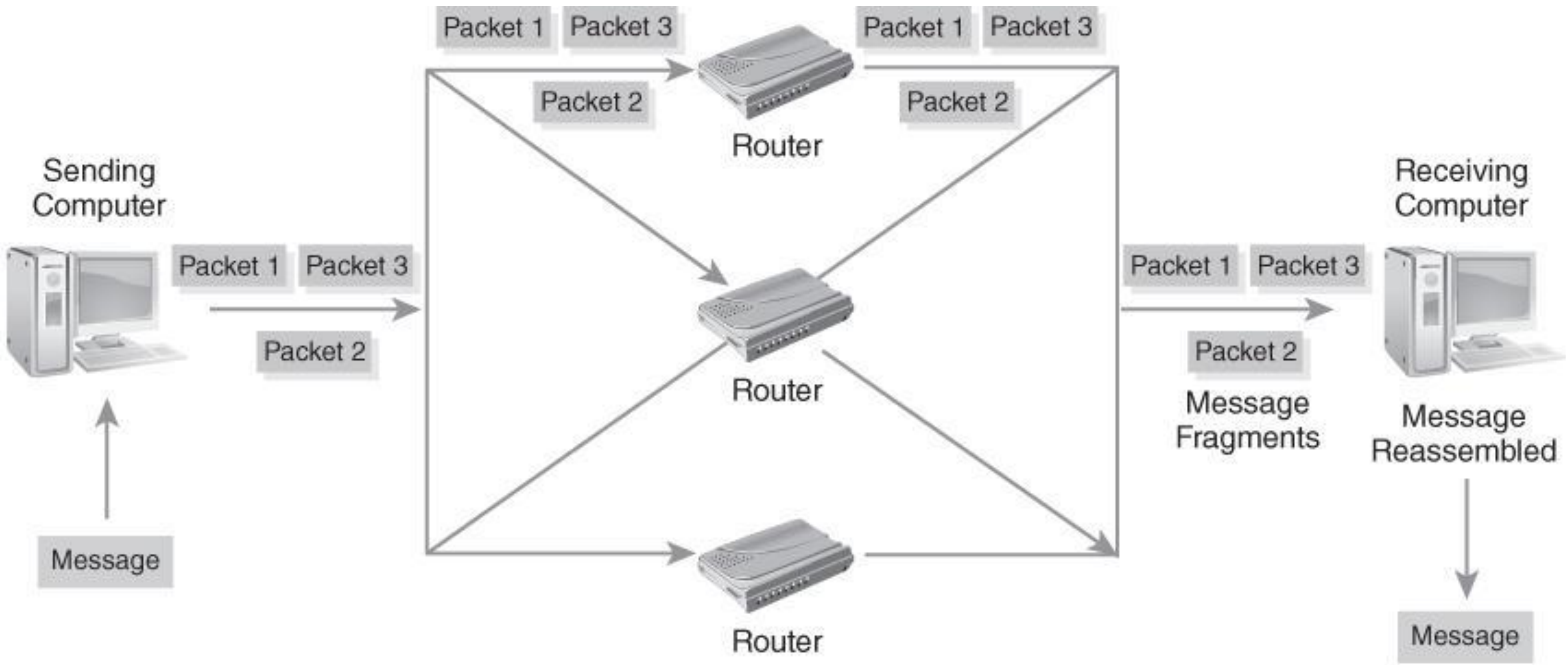


FIGURE 3-5 Circuit-switched network.

Packet-Switched Network

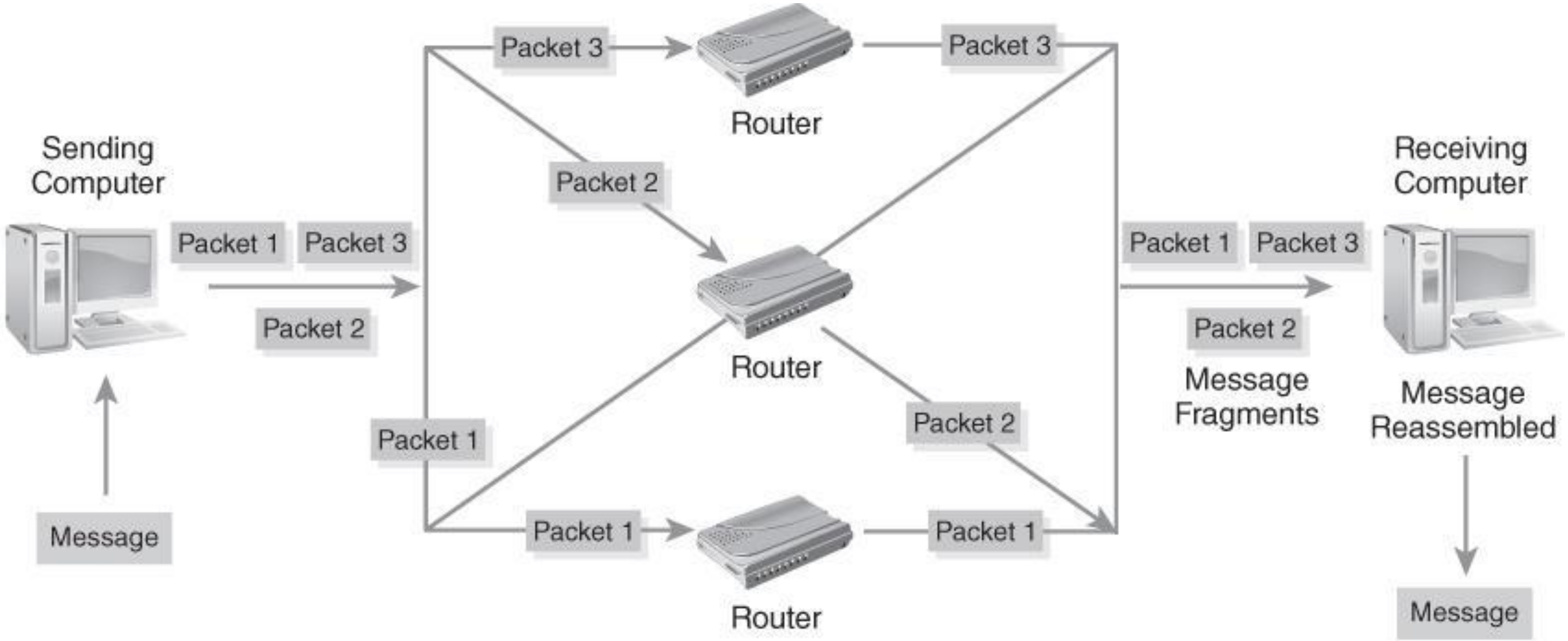


FIGURE 3-6 Packet-switched network.

IP-Based Communications (1 of 2)

Transmission Control Protocol (TCP)

- Guarantees the delivery of a reliable stream of data between two computer programs
- One of the most popular protocols that organizations use to communicate on the Internet
- Operates at OSI Layer 4

Internet Protocol (IP)

- Makes it possible to deliver packets across a complex network to a destination
- Handles the routing decisions necessary to get packets from their source to the destination
- Operates at OSI Layer 3

IP-Based Communications (2 of 2)

- Applications are designed and built knowing that TCP/IP is the transport protocol of choice
- Standard is so prevalent that network presence is often expressed as an IP address
  - If you have an IP address, you’re on the network
- IP address identifies a device or computer to a network as a unique node
- Private IP addresses identify nodes within an organization
- Applications that want to communicate over networks only need to reference the IP address of the destination node

Network Topology Overview

- Network topology
  - The layout of how devices connect to a network
  - A map of the network that shows how devices connect to one another and how they use a connection medium to communicate
- A **node** (server, computer, smartphone, etc.) can physically connect to the network and has an assigned IP host address

Physical topology

The picture of the actual network devices and the medium the devices use to connect to the network

Logical topology

How the actual network works and how you transfer data in a network; view focuses more on how the network topology operates

Simple Network Diagram

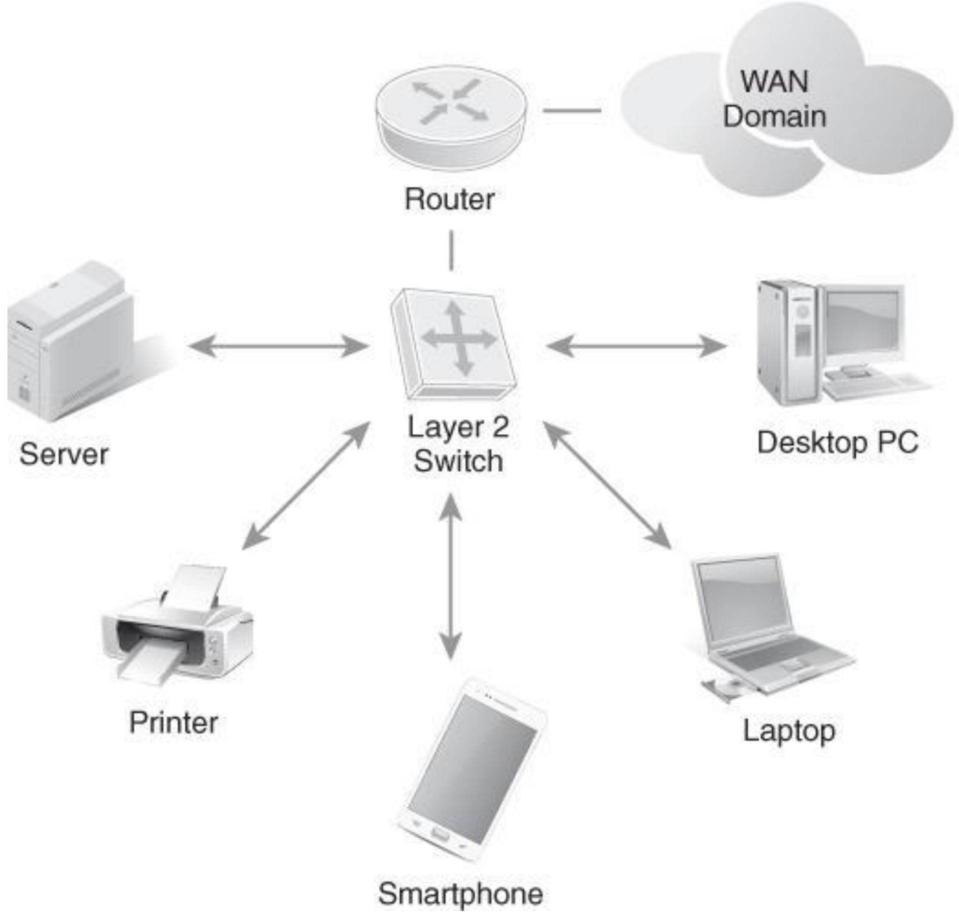


FIGURE 3-7 Simple network diagram.

Physical Network Topology

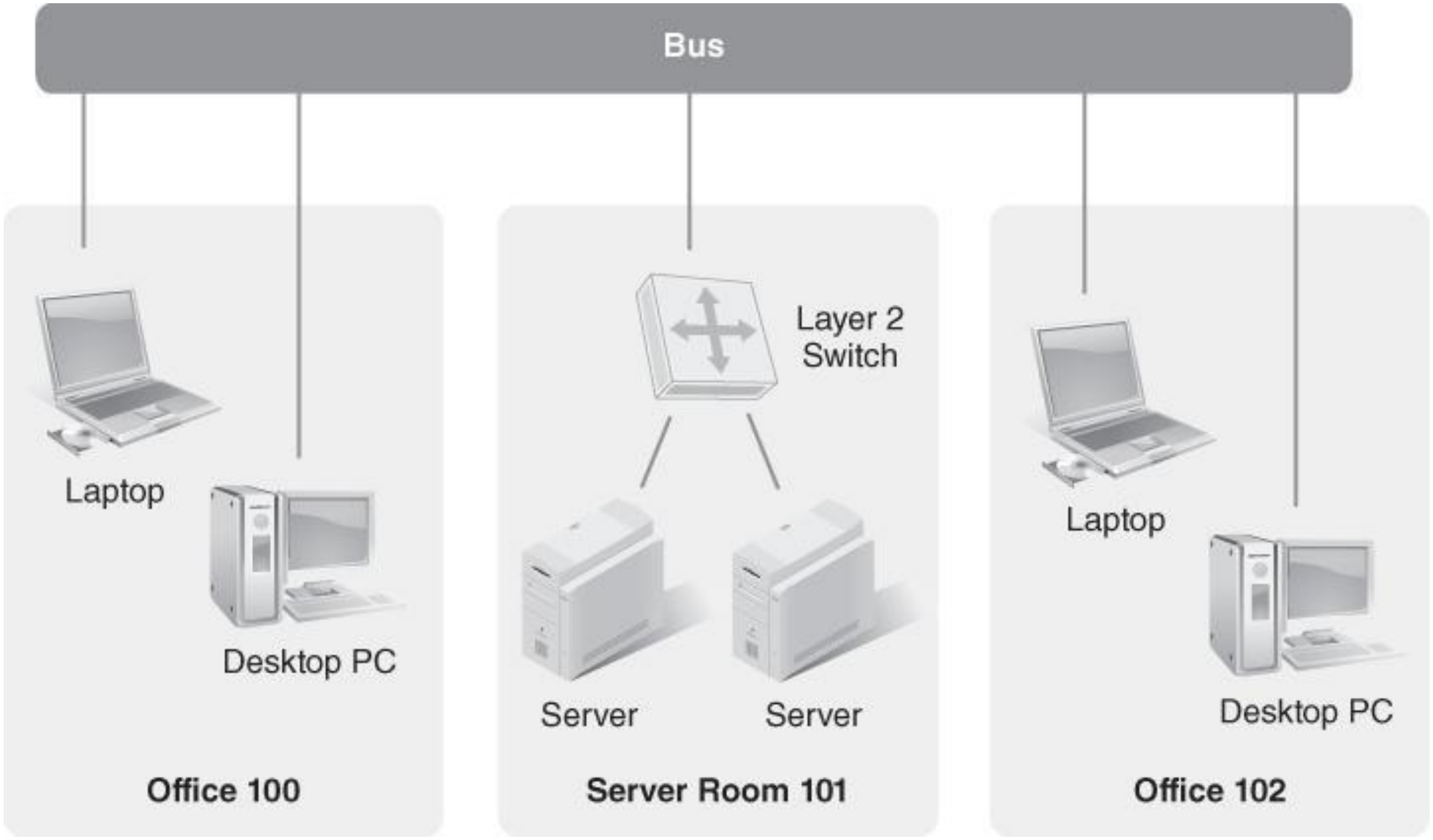


FIGURE 3-9 Physical network topology.

Logical Network Topology

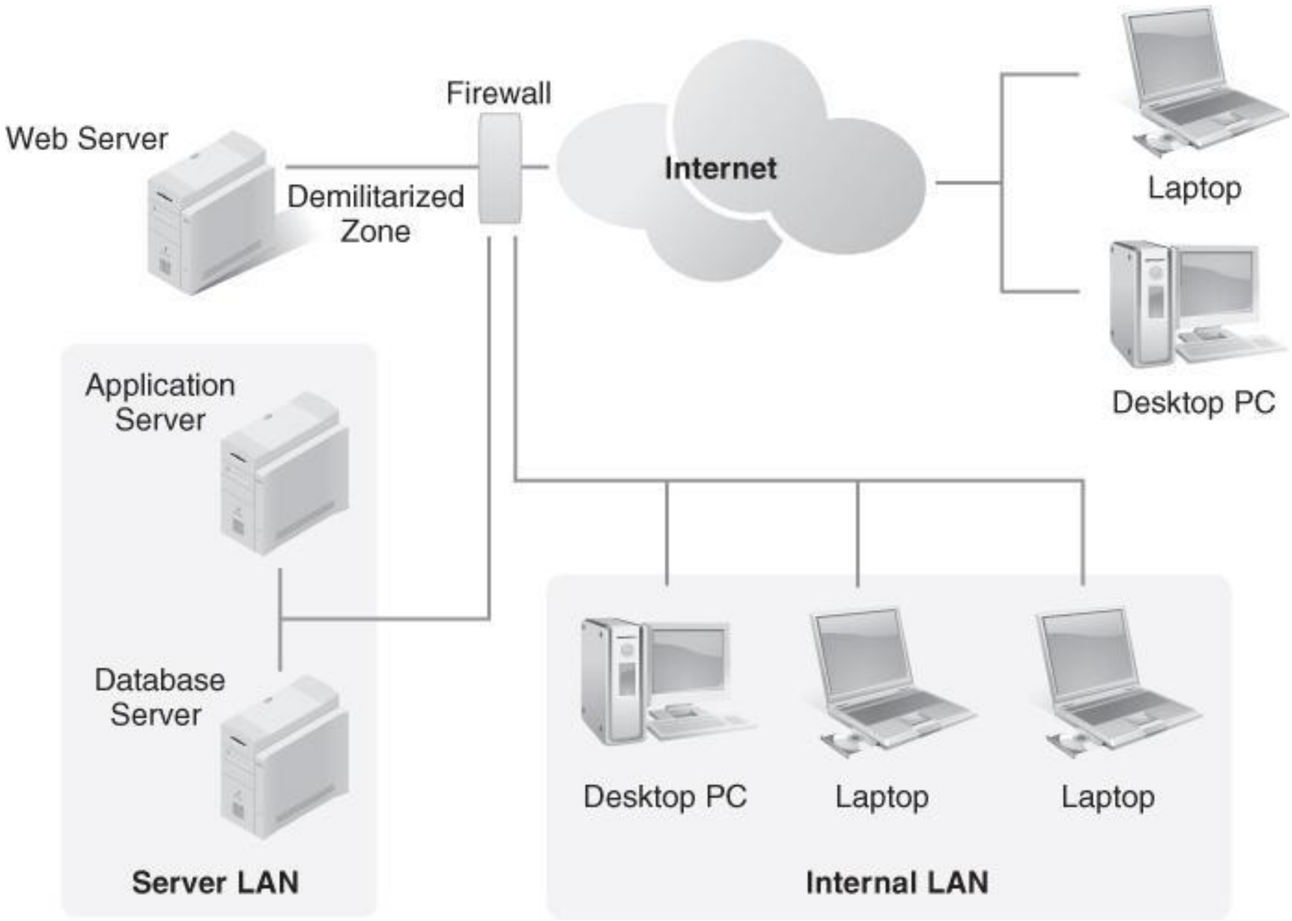


FIGURE 3-10 Logical network topology.

Common Network Topologies

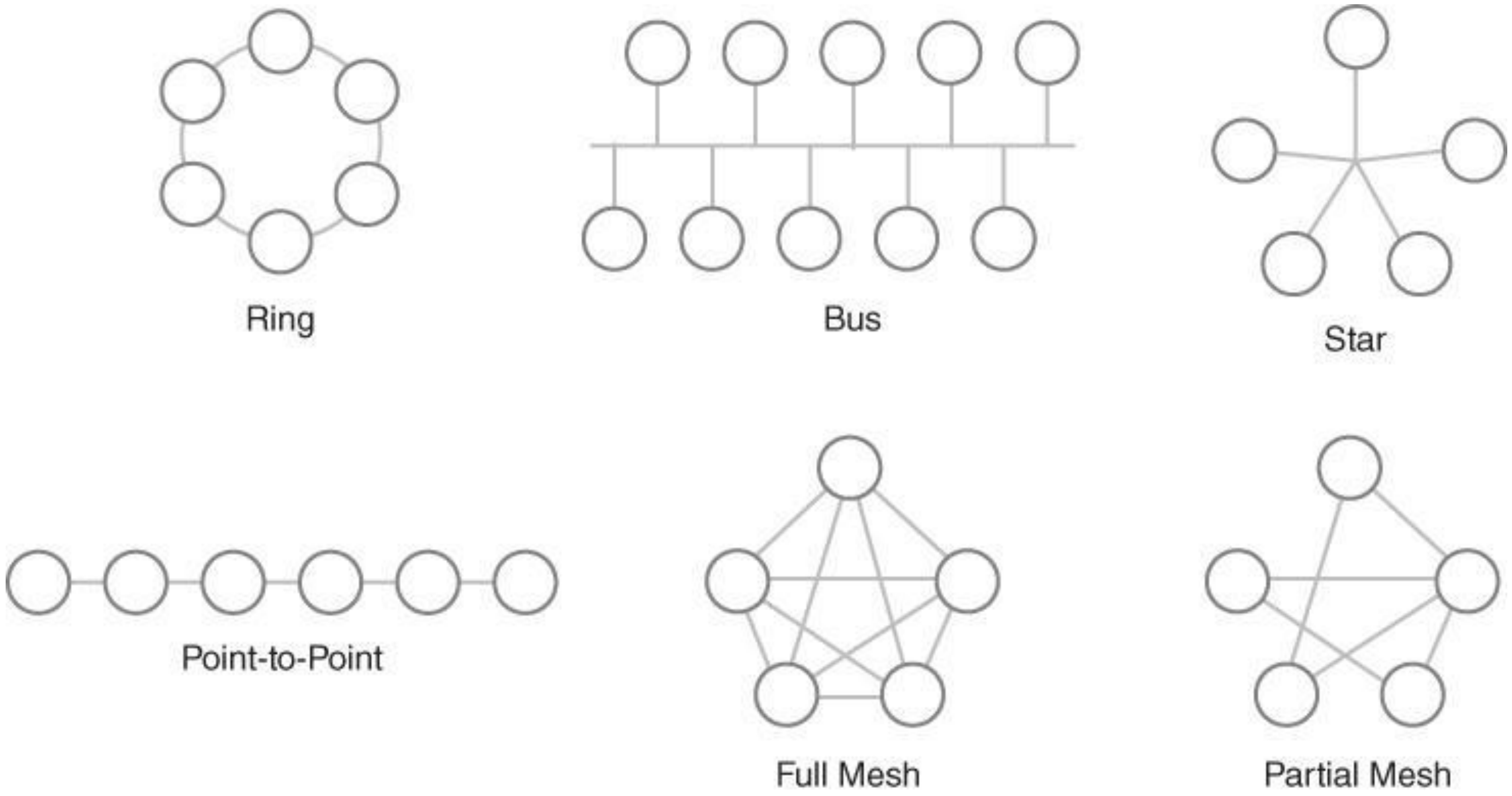


FIGURE 3-11 Common network topologies.

Point-to-Point Networks

- Networks that consist of computers or devices that connect directly to one another
- Difficult to add many devices because each new device requires a direct connection
- Found in very small environments that only need to connect a few PCs
- Are considered archaic

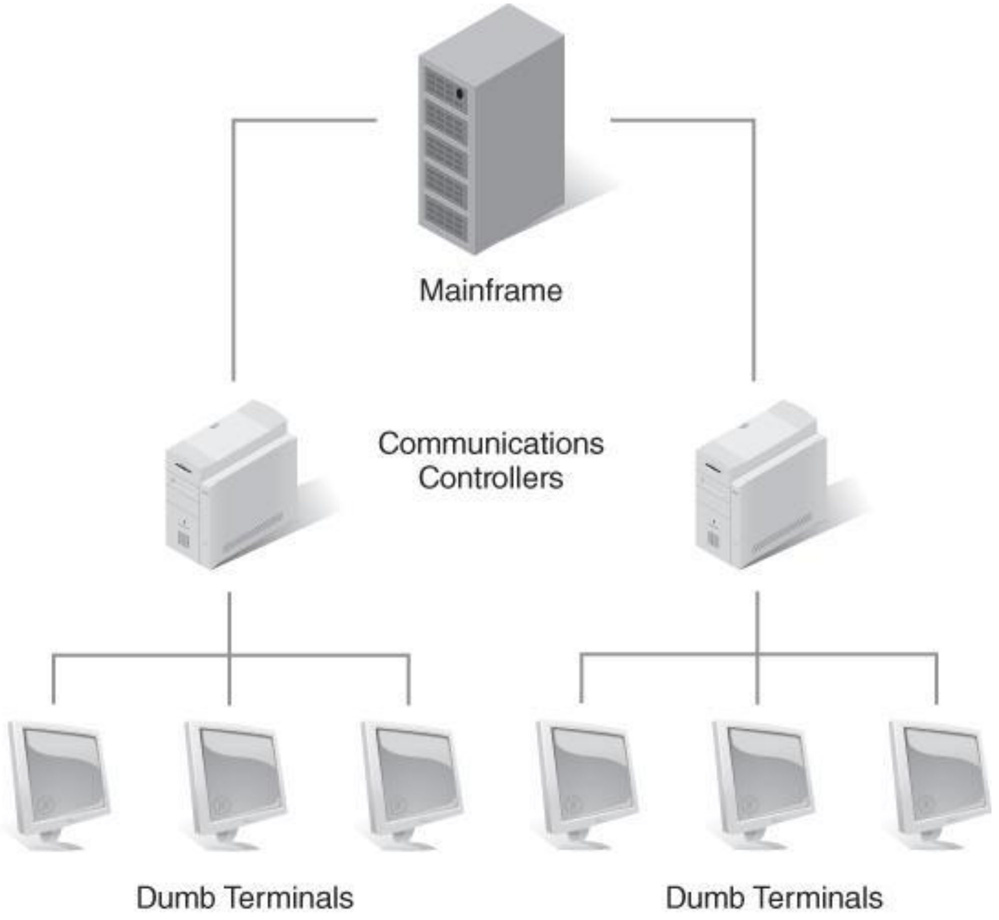
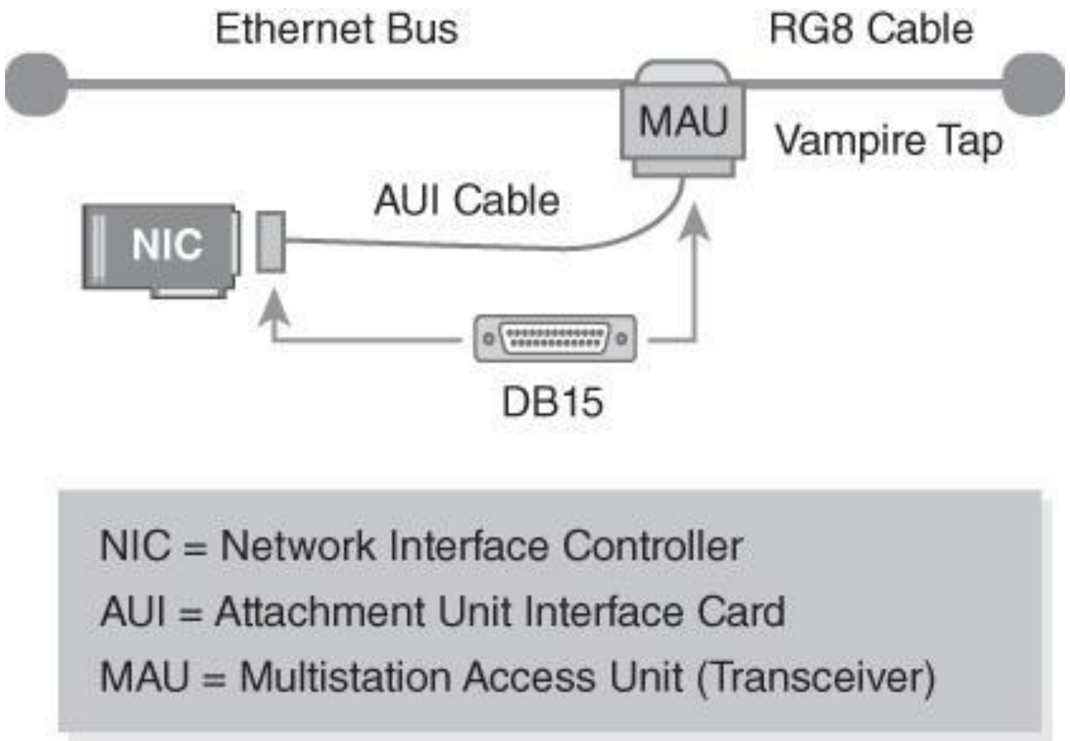


FIGURE 3-12 Point-to-point topology with legacy mainframe computers.

Bus Topology (1 of 2)

- Coaxial cable (bus) runs throughout a physical space; network devices attach to bus using an Ethernet transceiver
- Supports high-speed network communications
- Is simple to construct
- Is subject to physical distance limitations and maximum number of devices
- Only one device can communicate at a given time



NIC = Network Interface Controller

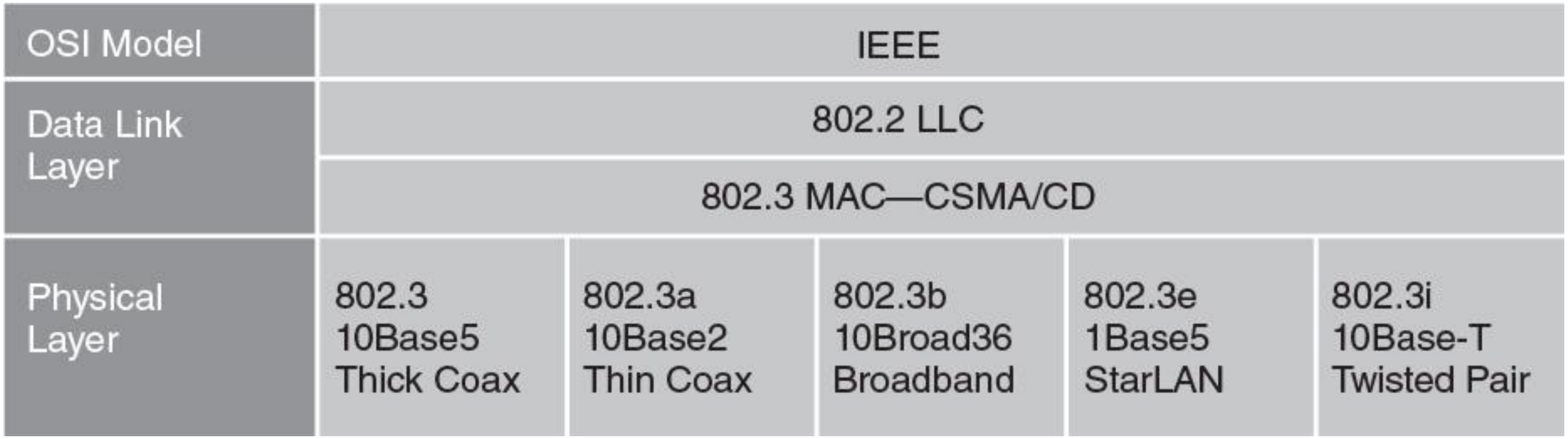
AUI = Attachment Unit Interface Card

MAU = Multistation Access Unit (Transceiver)

FIGURE 3-14 IEEE 802.3a CSMA/CD Ethernet bus topology.

Bus Topology (2 of 2)

- When two devices transmit at the same time, a collision occurs on the network
- Both devices must retransmit when the network is available
- Led to creation of IEEE 802.3 CSMA/CD (Carrier Sense Multiple Access with Collision Detection) and IEEE 802.5 token ring standards for local area networking



OSI Model	IEEE				
Data Link Layer	802.2 LLC				
	802.3 MAC—CSMA/CD				
Physical Layer	802.3 10Base5 Thick Coax	802.3a 10Base2 Thin Coax	802.3b 10Broad36 Broadband	802.3e 1Base5 StarLAN	802.3i 10Base-T Twisted Pair

FIGURE 3-15 IEEE 802.3 CSMA/CD standards.

Ring Topology

- All stations are connected in a logical ring
- Attached devices need permission to transmit on the network
- Permission is granted via a token (small frame) that circulates around the ring
- Unidirectional manner eliminates network transmission collisions
- A cut in the cable will break a ring network

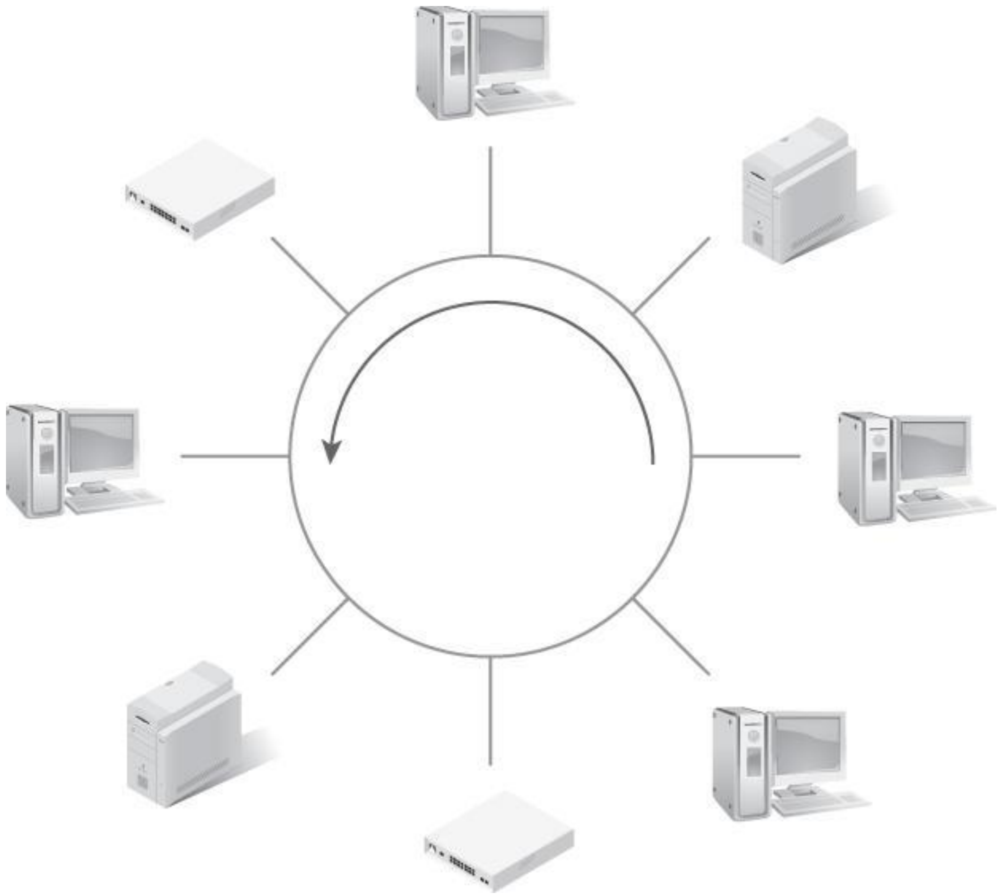


FIGURE 3-16 Token ring network—physical star, logical ring.

Star Topology

- Star-wiring cabling from a centrally located wiring closet creates Ethernet or token ring network
- Wiring creates a physical star, logical bus
- Can be supported by a hub or switch typically installed in a centrally located wiring closet
- Network-attached devices physically and electrically connect to network
- Fixes path length and attenuation issues

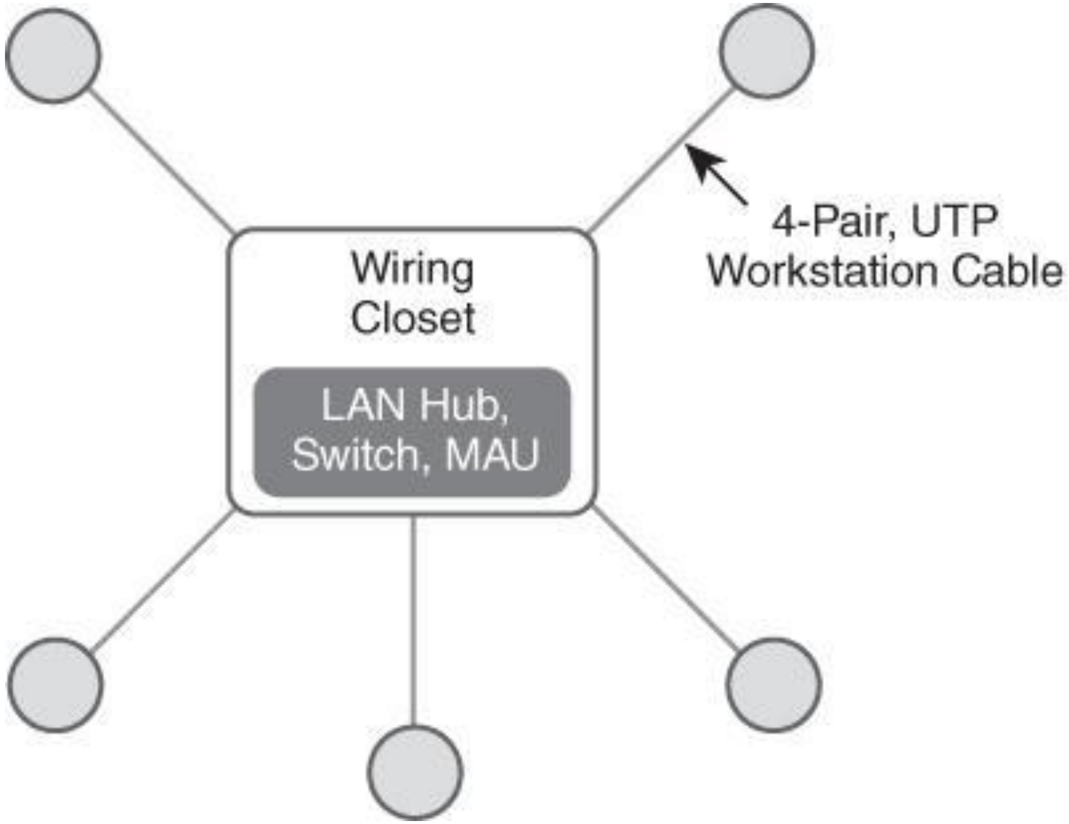


FIGURE 3-18 Physical star, logical ring topology.

LAN Hub versus LAN Switch

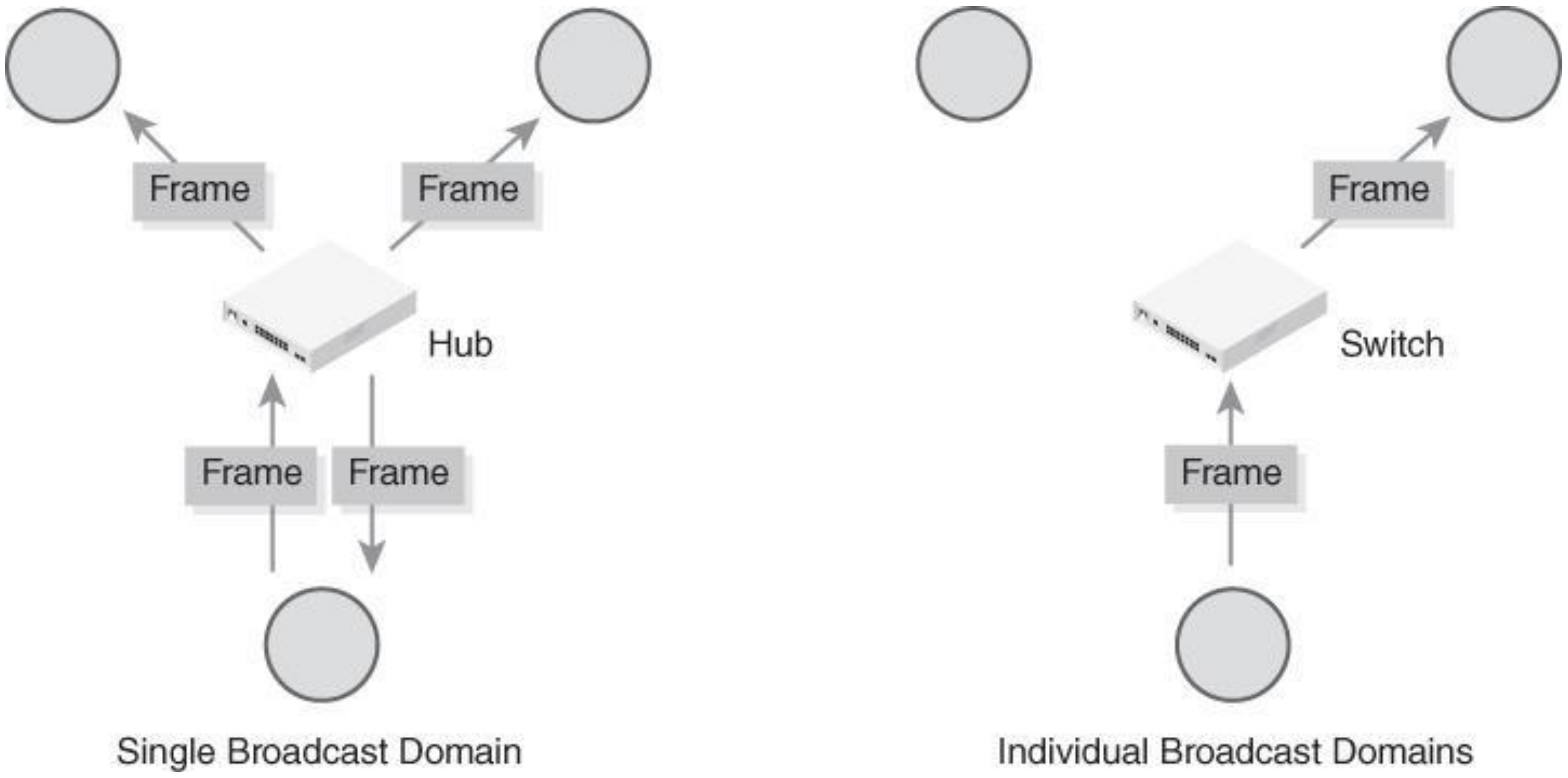


FIGURE 3-19 LAN hub versus LAN switch.

Mesh, Fully Connected Mesh, and Hybrid Topologies

Mesh topology

- A network layout in which all nodes are directly connected to all other nodes

Hybrid topology

- A network that contains several different topologies
- Can provide fault tolerance for some nodes while providing flexibility for other parts of the network

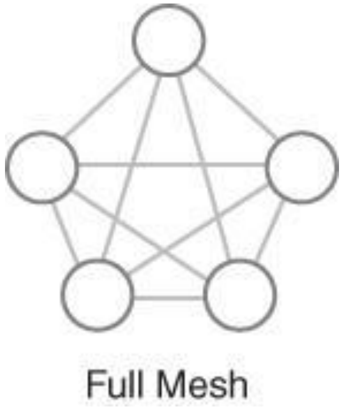


FIGURE 3-20 Fully connected mesh.

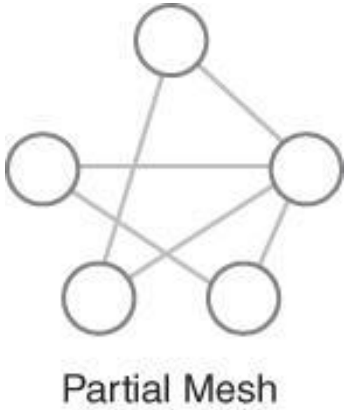


FIGURE 3-21 Partially connected mesh.

Internetworking

- **Internetworking** is a term used to describe connecting LANs together
- LANs communicate using protocols and the OSI model
- Different network devices interoperate at different layers of the protocol stack
- A **protocol stack** is how software operates at different layers of the OSI model
- Internetworking LANs must follow the OSI model protocol stack definition
- Thus, network devices must operate at either the Data Link Layer or the Network Layer

Internetworking at the Data Link Layer or Network Layer

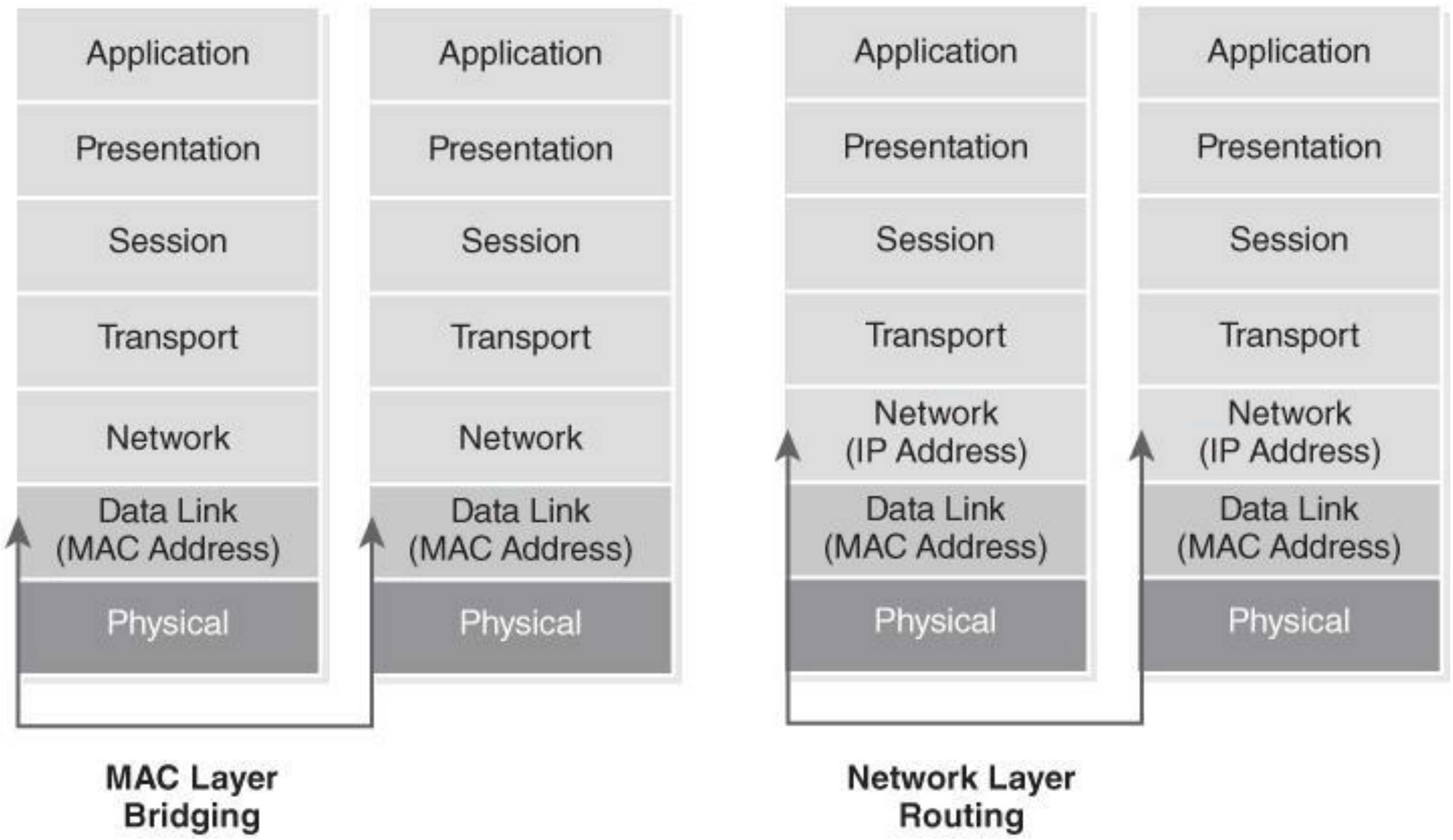


FIGURE 3-22 Internetworking at the Data Link Layer or Network Layer.

Internetworking Terms (1 of 2)

Client/server architecture

- Users interact with enterprise applications via local software running on client devices that use a network to connect to, and request services from, one or more servers
- Depends on client/server internetworking

Peer-to-peer internetworking

- The use of an enterprise network for peers to exchange messages without depending on a central server to manage connections or message handling

Most of today’s digital networks can support client/server and peer-to-peer communications

Internetworking Terms (2 of 2)

Intranet

- An internal network that only employees can access
- A private network within that organization's IP network infrastructure

Extranet

- A remotely accessible network that an organization makes accessible to its business partners and suppliers through the public Internet

Intranets and Extranets

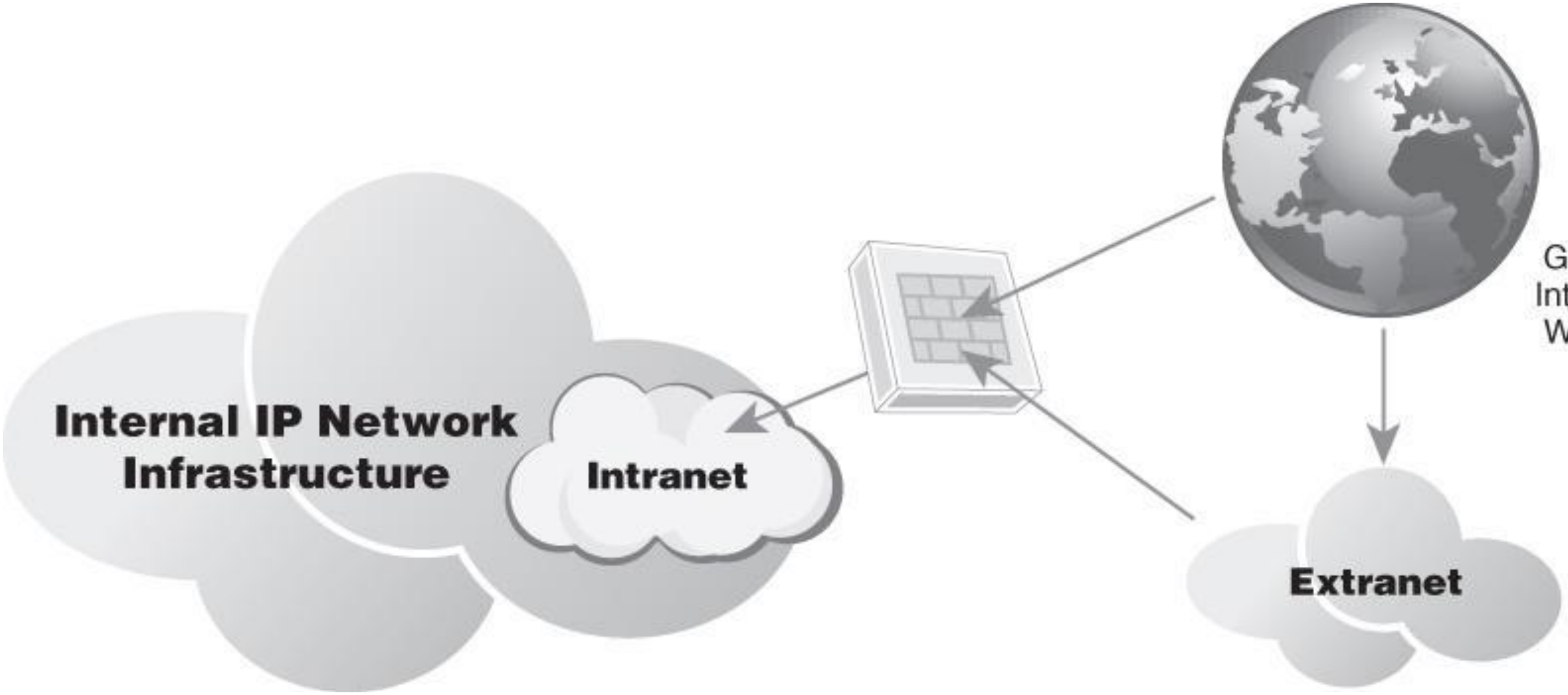
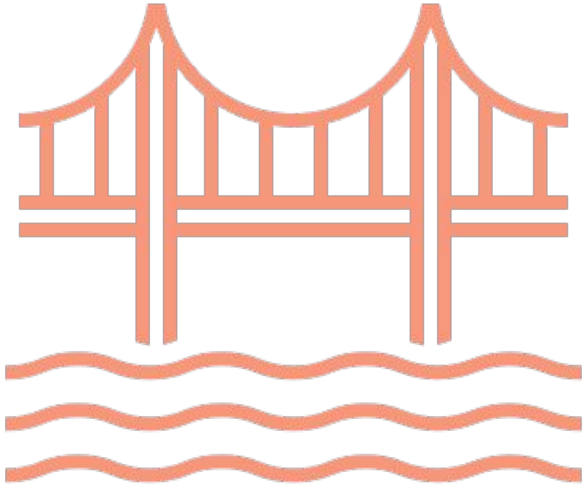


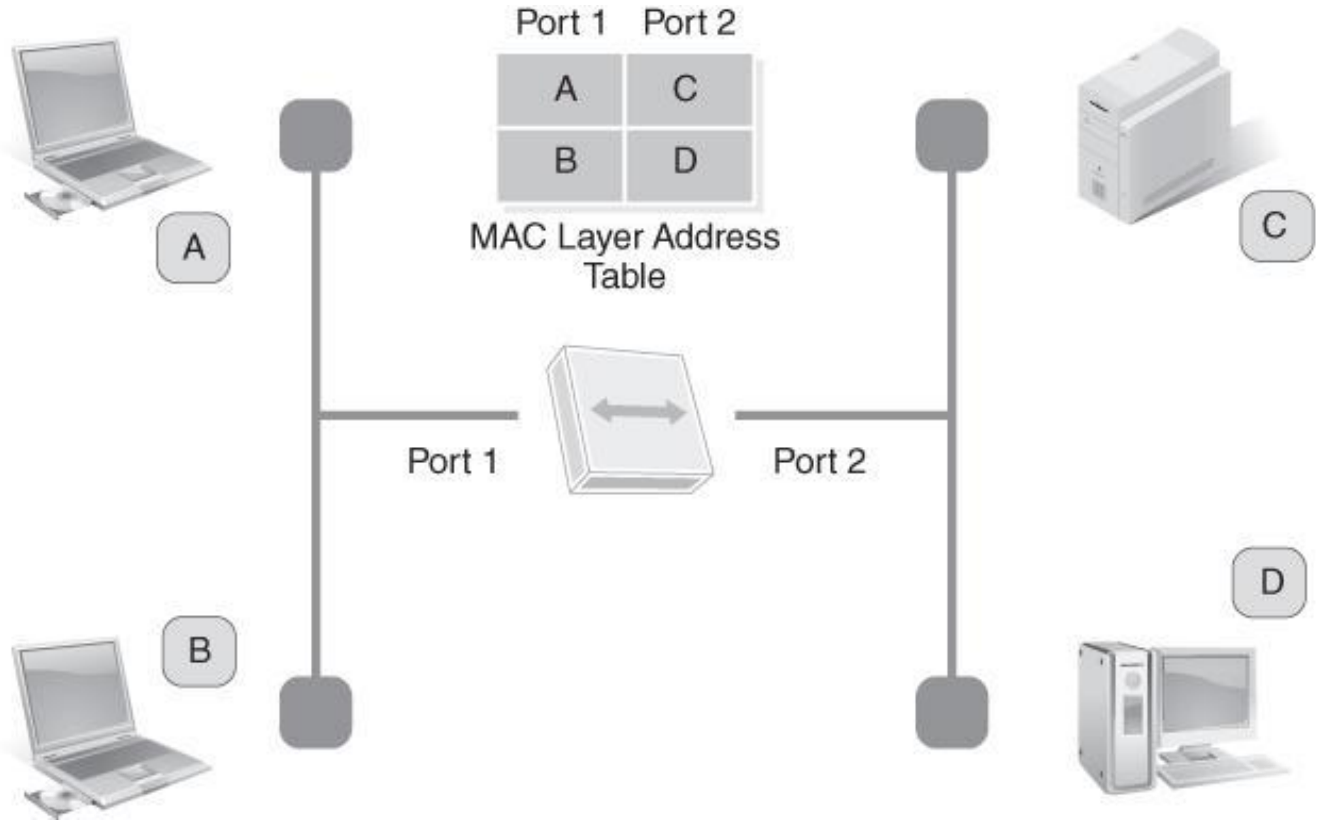
FIGURE 3-23 Intranets and extranets.

Internetworking with Bridges

- Internetworking at the Data Link Layer requires a bridge
- Easiest way to interconnect two networks is to place a MAC layer bridge in between the two networks
- Bridge
  - Examines the MAC address of each frame received
  - Makes a filtering or forwarding decision based on the MAC address forwarding table



MAC Address Forwarding Table



Port 1	Port 2
A	C
B	D

FIGURE 3-24 MAC address forwarding table.

Internetworking with Switches (1 of 2)

- Switch
  - Is essentially a bridge with more than two ports
  - Often has the capability to connect many devices and networks; a bridge generally connects two networks
  - Operates as an OSI Layer 2 device
  - Uses MAC addresses and builds address tables of devices connected to each physical port
- Switches that connect multiple devices or networks keep track of Media Access Control (MAC) addresses on all ports
- When the switch sees an Ethernet frame destined for a specific MAC address, it forwards that frame to that port

Internetworking with Switches (2 of 2)

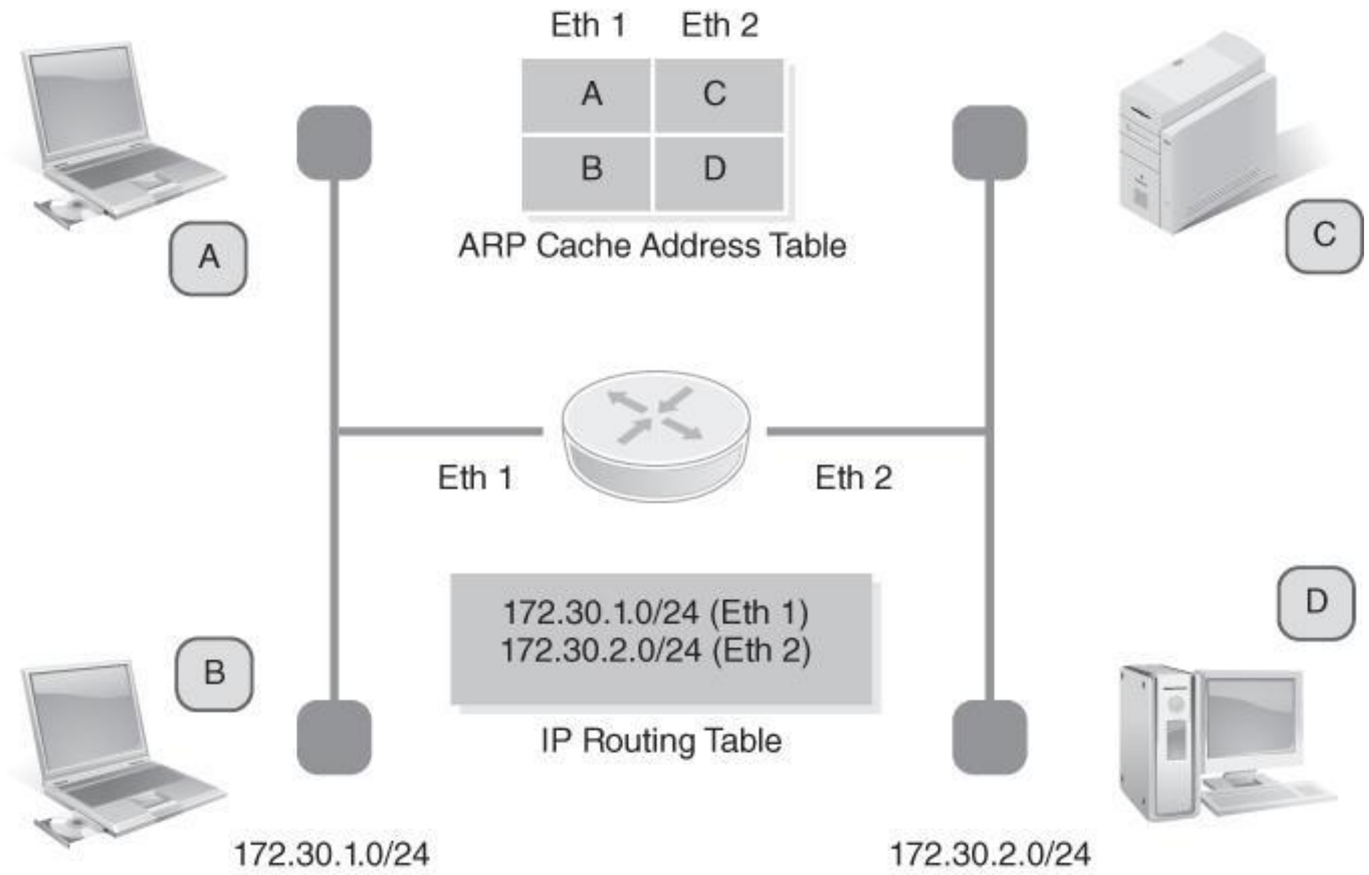
- **Layer 2 switches**
  - Operate at the Data Link Layer
  - Examine the MAC layer addresses of Ethernet frames

- **Layer 3 switches**
  - Operate at either the Data Link Layer or Network Layer
  - Typically have software that lets them function like Layer 2 switches or multiport bridges
  - Usually operate at the Network Layer that examines the network layer address within the Ethernet frame
  - Can look up the destination IP network number in their IP routing tables, and then make a path determination decision

Internetworking with Routers

- Router
    - Operates at the Network Layer
    - Is the same thing as a Layer 3 switch, but is typically used for WAN circuit connections, campus backbone connections, and building backbone connections
    - Can make intelligent decisions on where to send packets
        - Instead of just reading the MAC address and forwarding a packet based on a forwarding table, can see the packet’s Network Layer address or IP address
        - Network Layer address contains information about the destination network number and host number
        - Performs a path determination calculation to find the best path for the IP packets to traverse
    - Typically has redundant processors and plenty of memory
    - Takes longer to examine a packet than for a Layer 2 switch or bridge

Router ARP Cache Table and IP Routing Table



Eth 1	Eth 2
A	C
B	D

ARP Cache Address Table

172.30.1.0/24 (Eth 1)
172.30.2.0/24 (Eth 2)

IP Routing Table

FIGURE 3-25 Router ARP cache table and IP routing table.

ARP Cache Querying

- Windows or Mac or Linux (Terminal)
  - `arp -a`
- In Wireshark
  - Filter for ‘arp’
- Security Consequences
  - ARP Cache Poisoning
    - A bad actor can fake MAC addresses on a network to fill everyone’s caches and direct traffic to them.
      - Modern switches can detect and defeat this - still, it’s a race to claim the mapping!
  - If the switch doesn’t know the ARP-port mapping, broadcast to all

Internetworking with a Bridge/Router

- Routers can examine packets only in formats they understand
- All network nodes must use protocols the routers understand; can cause challenges
- Nonroutable protocol does not have a Network Layer address; routable protocol has a Network Layer address that is routable
- Brouter
  - A device that can act as a bridge or router
  - Is the same thing as a Layer 3 switch with Layer 2 bridging software
  - Bridges Ethernet frames that are nonroutable and will route IP packets that are routable
  - Is a more flexible and powerful internetworking device for networks, given that it can interconnect LANs at the Data Link Layer or Network Layer

Internetworking with a Gateway

Interconnects two networks that use different protocols

Translates network packets from one network protocol to another (unlike a router)

Main job is to translate all incoming packets to a protocol compatible with the destination network

Is commonly placed at entry and exit points of a network

Commonly runs either as software on a computer or as a device that performs the same functions as a router - VMware, Docker, VirtualBox sets up multiple bridges internally

Switching Concepts

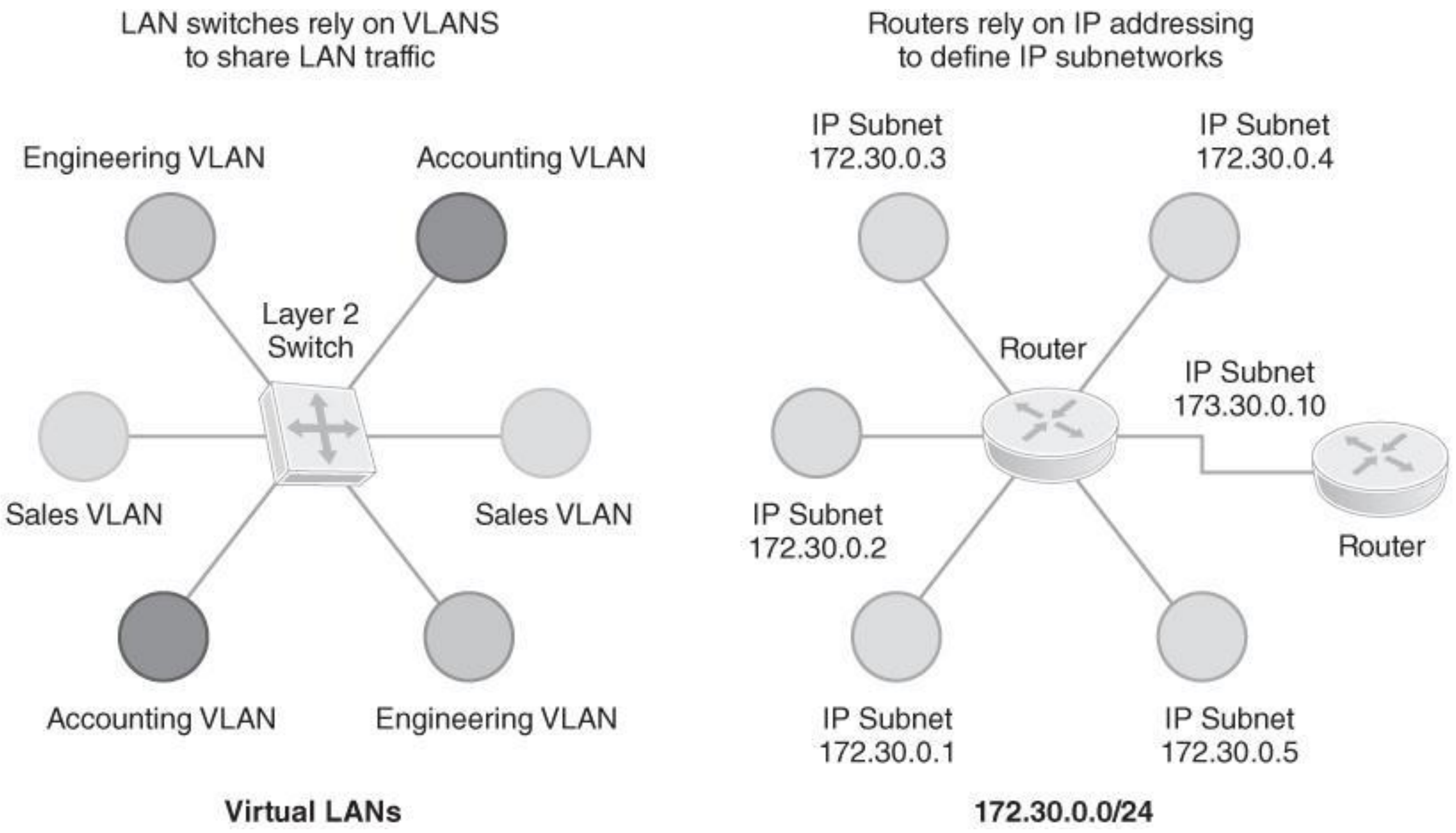


FIGURE 3-26 Physical versus logical network segmentation.

Switch Functionality

- Layer 2 versus Layer 3 workstation connectivity
- MAC addressing tables
- Forwarding/ filtering
- Preventing broadcast storms caused by loops
- Power over Ethernet (PoE) switch ports
- Virtual LANs (VLANs)
- Layer 2 or Layer 3 switch resiliency

Forwarding Methods

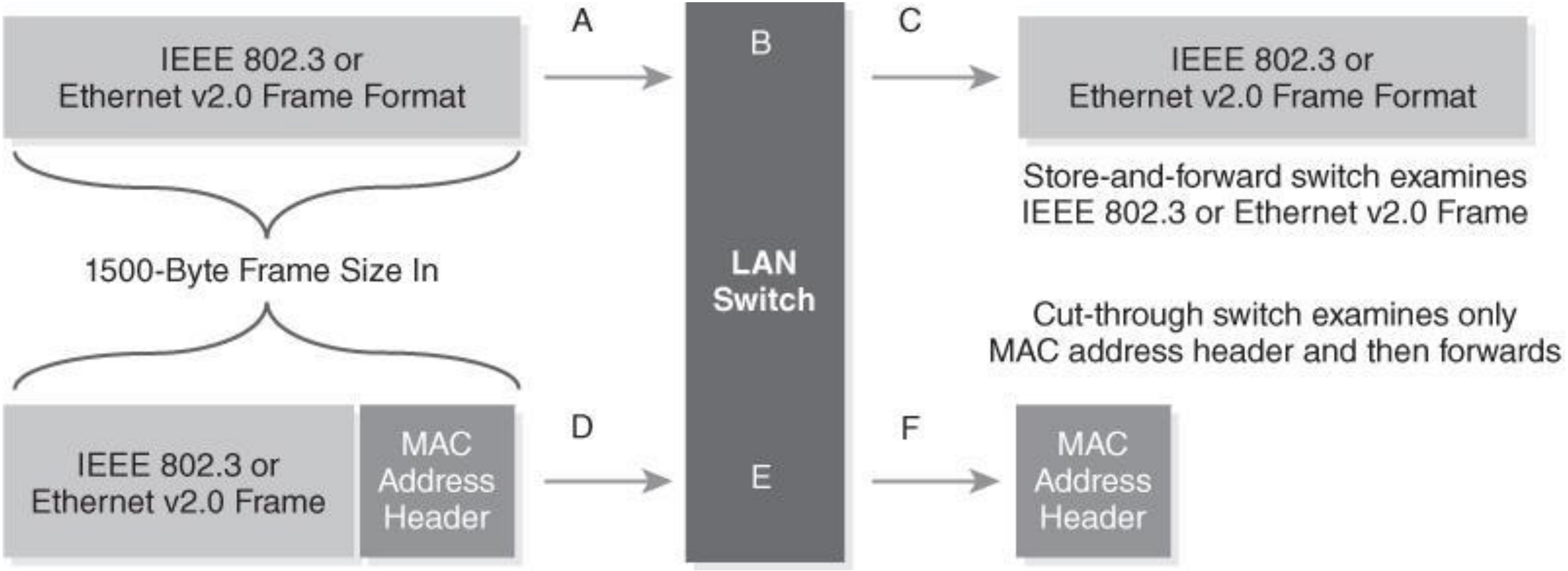

IEEE 802.3 or Ethernet v2.0 Frame Format
A
B
C
IEEE 802.3 or Ethernet v2.0 Frame Format
Store-and-forward switch examines IEEE 802.3 or Ethernet v2.0 Frame
1500-Byte Frame Size In
LAN Switch
Cut-through switch examines only MAC address header and then forwards
IEEE 802.3 or Ethernet v2.0 Frame
MAC Address Header
D
E
F
MAC Address Header

FIGURE 3-27 Forwarding methods.

Switch Forwarding Methods

Cut-through switching

As LAN switch reads the destination MAC address, it starts to forward the packet to the destination and does not examine the entire frame

Increases network throughput and performance

Store-and-forward switching

LAN switches must receive the entire Ethernet frame and make forwarding decision based on MAC address table

Device can drop any packets with errors prior to forwarding them

Uses less of a network's capacity but increases latency

Routing Concepts

Network layer address

Static route

Dynamic route

Mac: `netstat -rn` Windows: `route PRINT`

Resiliency and Redundancy

Layer 2 Resiliency

- Enabling resiliency protocols, such as Spanning Tree Protocol (STP) and Resilient Ethernet Protocol (REP), to avoid network communication interruptions

Layer 3 Resiliency

- Supporting alternate routes to a WAN when the primary route is unavailable
- Example: Cisco Hot Standby Routing Protocol (HSRP)

Virtual Networking Components

- Implementing some network devices as virtual machines (VMs) or containers, or building entire virtualized networks

Network Storage Types

- Implementing network storage devices as VMs; storage area networks and network attached storage

Summary

- The OSI and TCP/IP Reference Models
- TCP/IP suite
- Network topologies
- Circuit and packet switching
- IP-based communications and convergence