CECS 303 Networks and Networks Security

CHAPTER 1
Fundamental Concepts

Jose Tamayo, M.S.
Computer Engineering & Computer Science
California State University, Long Beach

Notes by: Shin Bongsik, **A Practical Introduction to Enterprise Network and Security Management (ed 2017) Ch1**

Main objectives of this chapter:

- Key elements of a computer network
- Methods used by network nodes to distribute data
- Directionality in data propagation
- Network topologies focusing on physical layouts
- Classification of networks in terms of their scope

Main objectives of this chapter (cont'd)

- Subnetwork versus inter-network
- Key measures of network performance
- Binary, decimal, and hexadecimal numbering systems
- Addressing methods: Internet protocol (IP) and media access control (MAC)

Network Elements

- Host
  - Client – Server
  - P2P
  - NIC
- Intermediary Devices
  - Router
  - Switches
  - Hub
  - Wireless Access Points
  - Wireless Bridges

Network Elements (cont'd)

- Network Link
  - Guided
  - Unguided
- Applications
- Data Messages
- Protocols

Modes of Communication

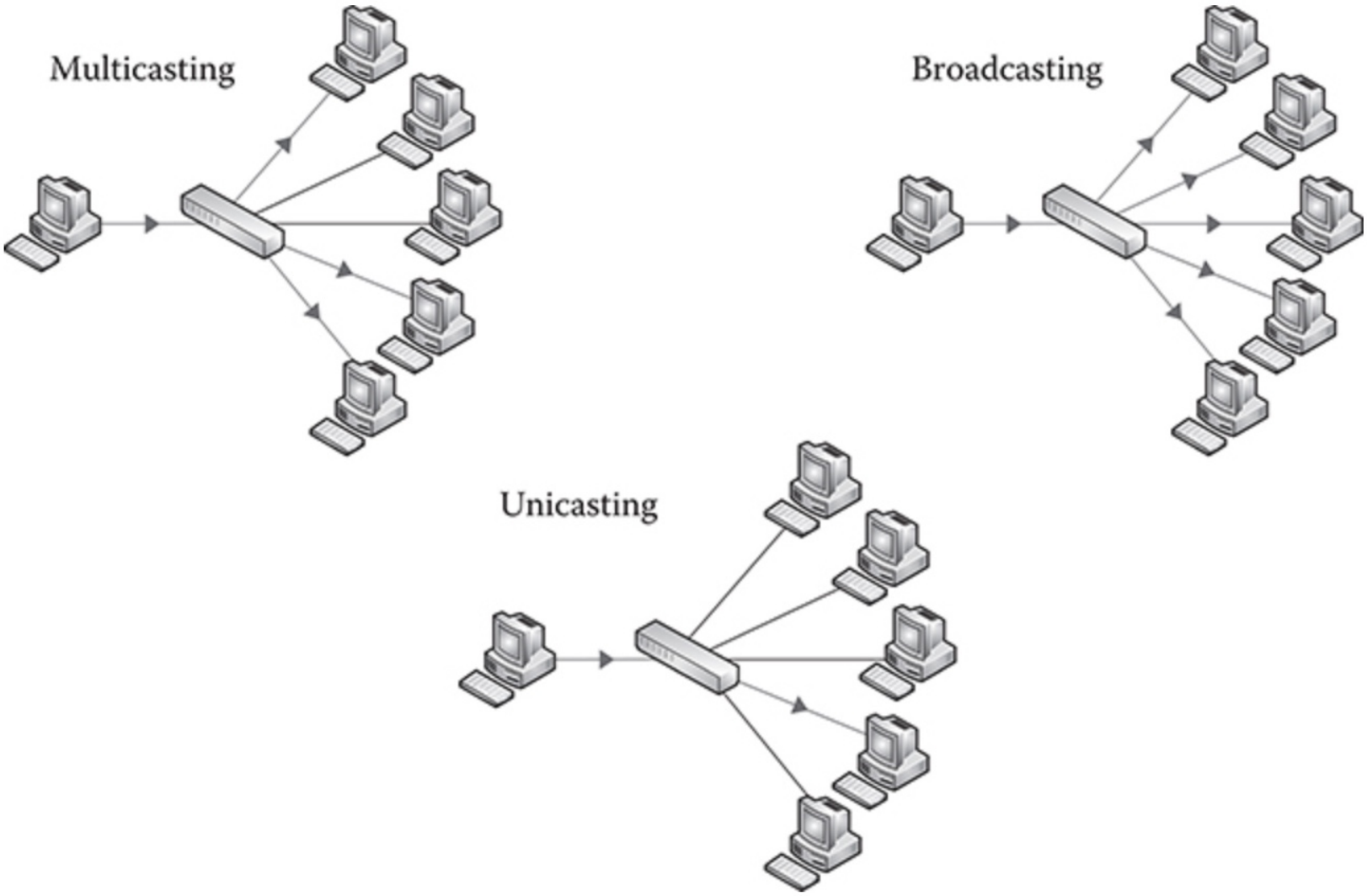


Figure 1.8 Multicasting, broadcasting, and unicasting.

Direction of Data Exchange

- Simplex
- Half-duplex
- Full-duplex

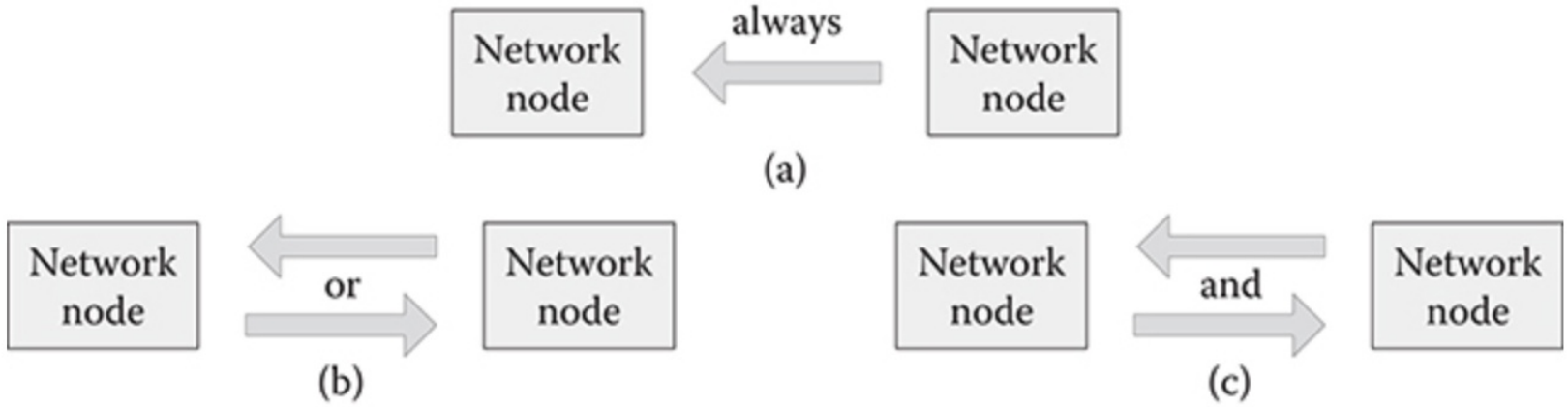


Figure 1.9 (a) Simplex, (b) half-duplex, and (c) full-duplex transmissions.

Network Topology

- Point-to-Point
  - Dedicated connection between two hosts/nodes
- Bus
  - Shared inline connection among nodes, single point of failure
- Ring
  - Shared ring connection, single point failure
- Star
  - Centralized connections in an intermediary device
- Mesh
  - Each node in the topology interconnect to all the others nodes
- Tree
  - All nodes are connected in a hierarchical fashion where the top node is the root

Classification of Networks

- PAN
- LAN
- MAN
- WAN
- IoT

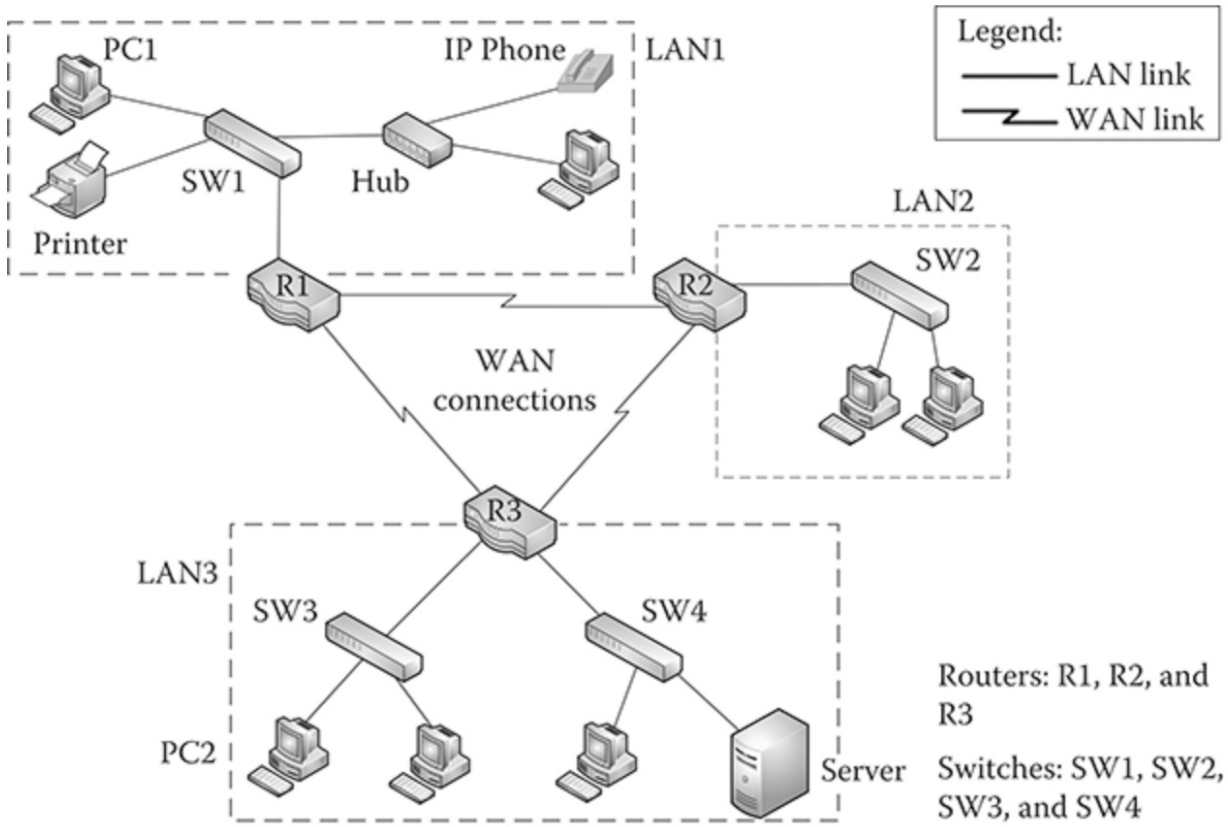


Figure 1.6 A hypothetical enterprise network.

Subnetwork vs Inter-Network

Refer to Figure 1.6 and answer the following questions:

- How many subnetworks are there in each LAN?
- If PC1 in LAN1 sends a file to a printer in LAN1, is this inter-networking?
- If PC1 in LAN1 sends a request message to a server in LAN3, is this inter-networking?
- If PC1 in LAN1 connects to an IP Phone in LAN1, is this inter-networking?
- If PC2 and a server in LAN3 exchange messages, is this inter-networking?

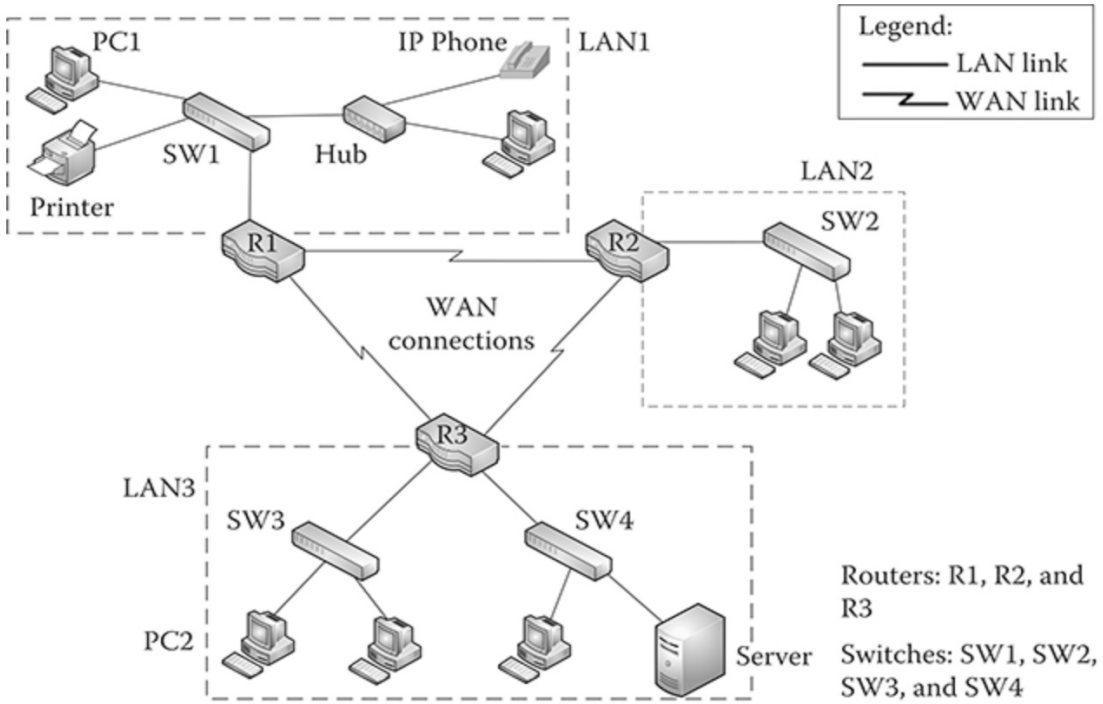


Figure 1.6 A hypothetical enterprise network.

Measures of Network Performance

- Capacity (aka throughtput) vs Goodput
- Delay
- Reliability and QoS

Table 1.1 Metrics of Storage versus Network Capacity

Storage/Memory Capacity	Network Capacity in Data Rate
KB (Kilobyte) = 1000 bytes	Kbps (kilobits/s) = 1000 bits/s
MB (Megabyte) = 1 million bytes	Mbps (Megabits/s) = 1 million bits/s
GB (Gigabyte) = 1 billion bytes	Gbps (Gigabits/s) = 1 billion bits/s
TB (Terabyte) = 1 trillion bytes	Tbps (Terabits/s) = 1 trillion bits/s
PB (Petabyte) = 1 quadrillion bytes	Pbps (Petabits/s) = 1 quadrillion bits/s

Numbering Systems

- Binary
- Decimal
- Hexadecimal

Hexadecimal		Decimal		Binary
A	→	10	→	1010
A	←	10	←	1010

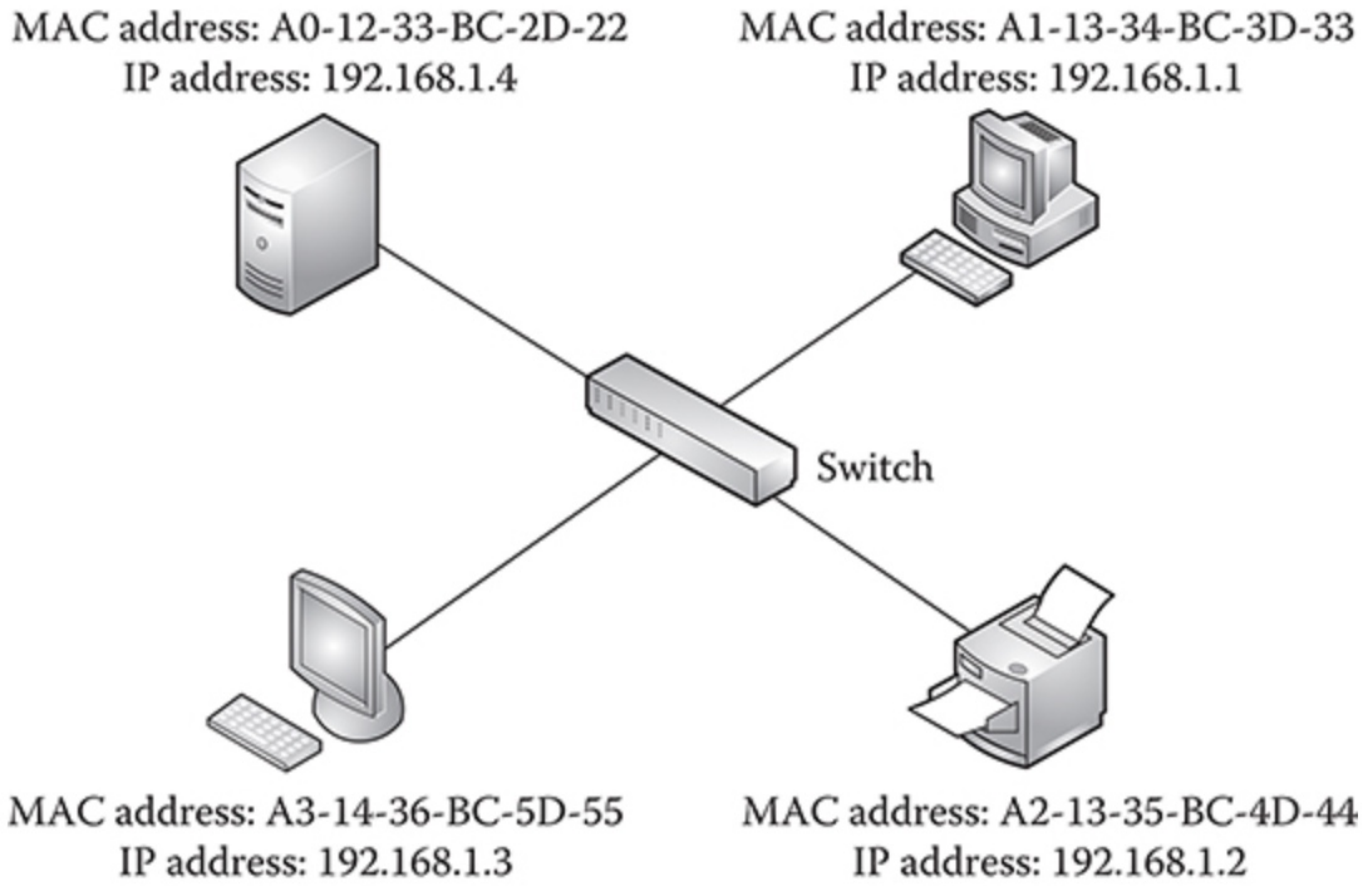
Initial binary combination (8 bits)	0	1	0	1	1	0	1	0
Power of two	2^7	2^6	2^5	2^4	2^3	2^2	2^1	2^0
Decimal position values	128	64	32	16	8	4	2	1
Add decimal values of nonzero binary positions		64		+16	+8		+2	= 90

Network Addressing

- Characterizing Network Addressing
  - Permanency
  - Accessibility
  - Privacy
- MAC Addresses (aka Physical Addresses)
  - First 6 values are the OUI
- IP Addresses
  - Private
  - Public

Network Addressing (cont'd)

- Pairing of MAC and IP Addresses



Chapter Summary

- A computer network is made up of various hardware and software components
- Data communications between network nodes are in the forms of *unicasting*, *broadcasting*, and *multicasting*
- Data flows between two network nodes can be *simplex*, *half-duplex*, and *full-duplex*
- Network topology refers to the layout of the network nodes and links. Among the different network topologies are point-to-point, bus, star, ring, mesh, and tree

Chapter Summary (cont'd)

- Computer networks are classified into four types: PANs, LANs, MANs, and WANs
- The subnetwork is formed when intermediary devices including hubs, bridges, wireless access points, and switches interconnect host computers. The router is used to tie multiple subnetworks to form an inter-network
- Network performance measures include capacity, delay, and reliability. QoS represents a network's ability in guaranteeing performance.

Chapter Summary (cont'd)

- Three different numbering systems: binary, decimal, and hexadecimal. The preference on the usage context

- Network nodes transport data relying on standardized address information. MAC and IP addresses are paired to accomplish such task.

CECS 303 Networks and Networks Security

Architectures and Standards
Chapter 2

Jose Tamayo, M.S.
Computer Engineering & Computer Science
California State University, Long Beach

2.2 TCP/IP vs. OSI Architectures

- *Standard architecture:* a framework that *broadly* defines necessary networking functions in the multi-layer structure

TCP/IP	OSI	Hybrid	Layer	Key Tasks
Application	Application	Application	5	Application-Application Communications
	Presentation			
	Session			
Transport	Transport	Transport	4	Packet delivery across subnetworks (inter-networking)
Internet	Network	Internet	3	
Network Access	Data link	Data link	2	Packet delivery within a single subnetwork (intra-networking)
	Physical	Physical	1	

Figure 2.1 TCP/IP and OSI layers

2.2.3 Protocol Data Units

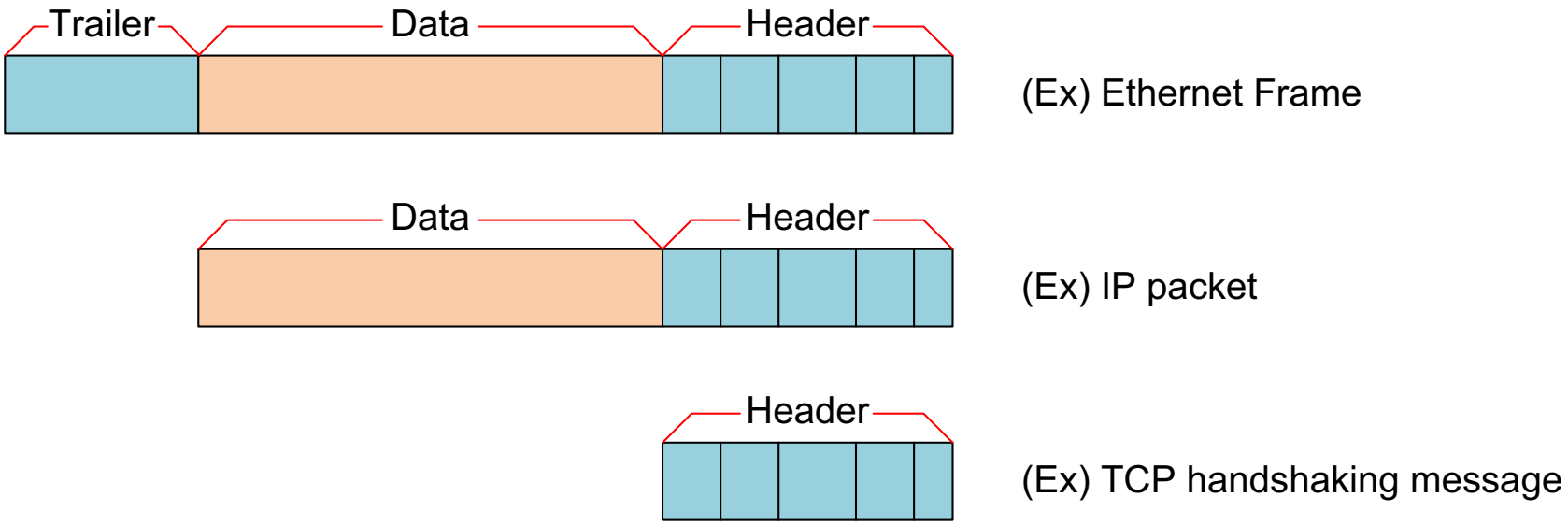


Figure 2.2 Three possible formats of protocol data units

2.3 Layer Functions

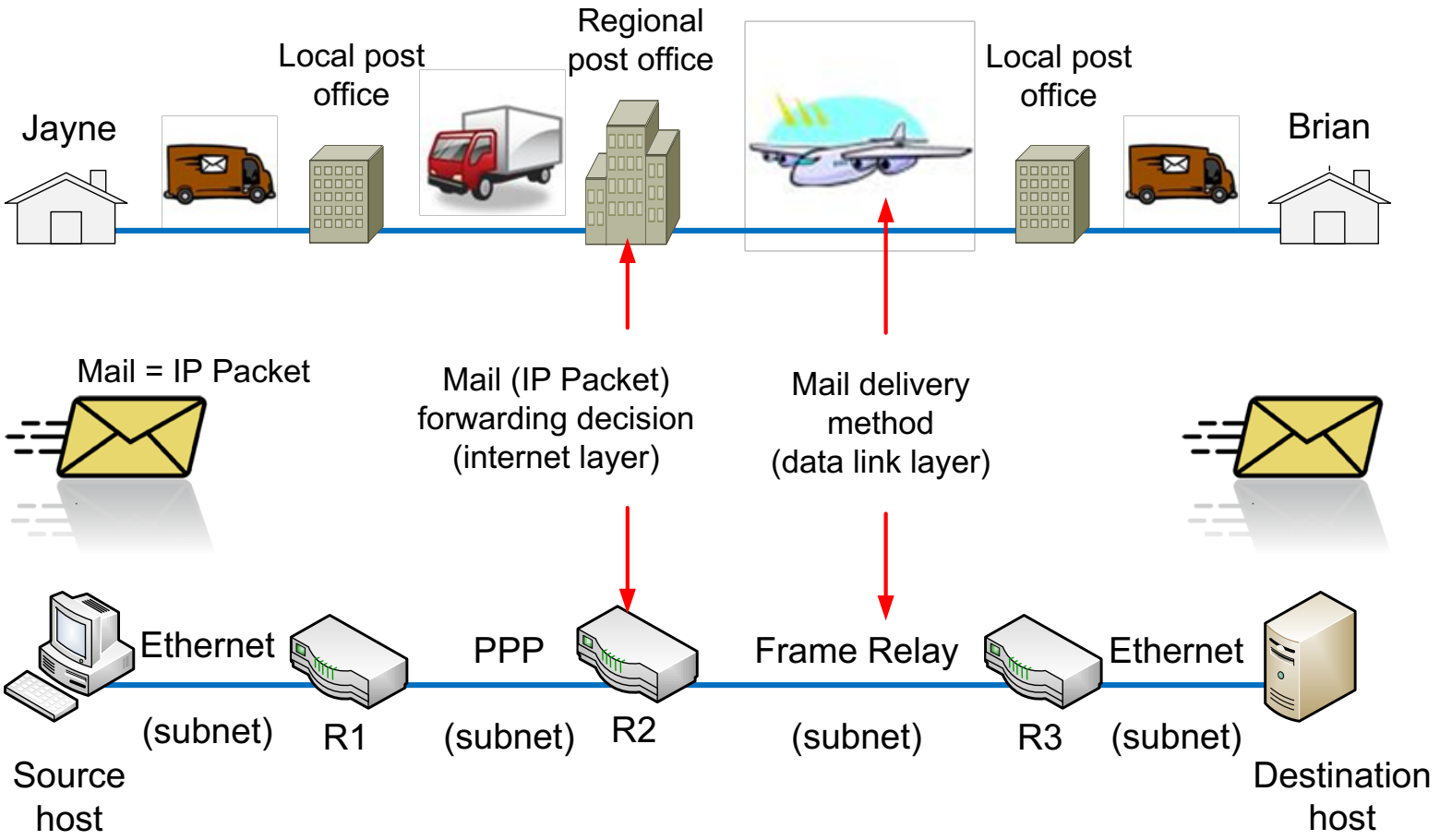
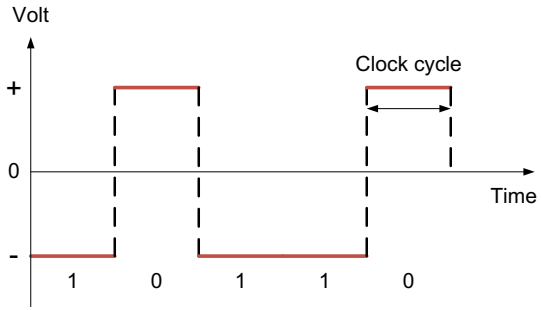
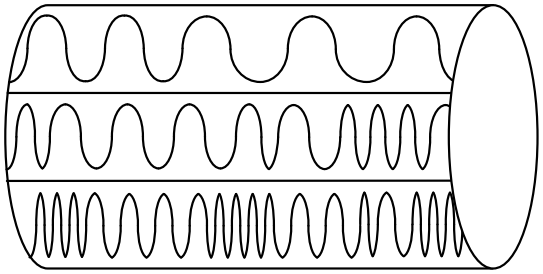


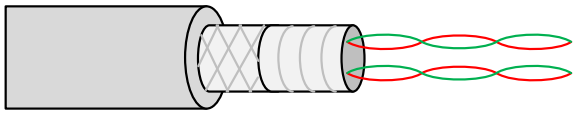
Figure 2.3 A real-life analogy of layer functions

2.4 Physical Layer (Layer 1)

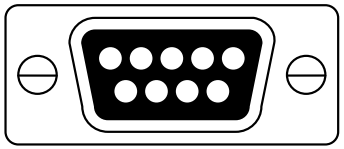




Signal multiplexing



Cable



Port / Interface

Figure 2.6 Select physical layer standards

2.5 Data Link Layer (Layer 2)

- Intra-networking (within a subnetwork)
- LAN or WAN data links: frames, switching
- Only a single delivery path (a data link) active between any two nodes.

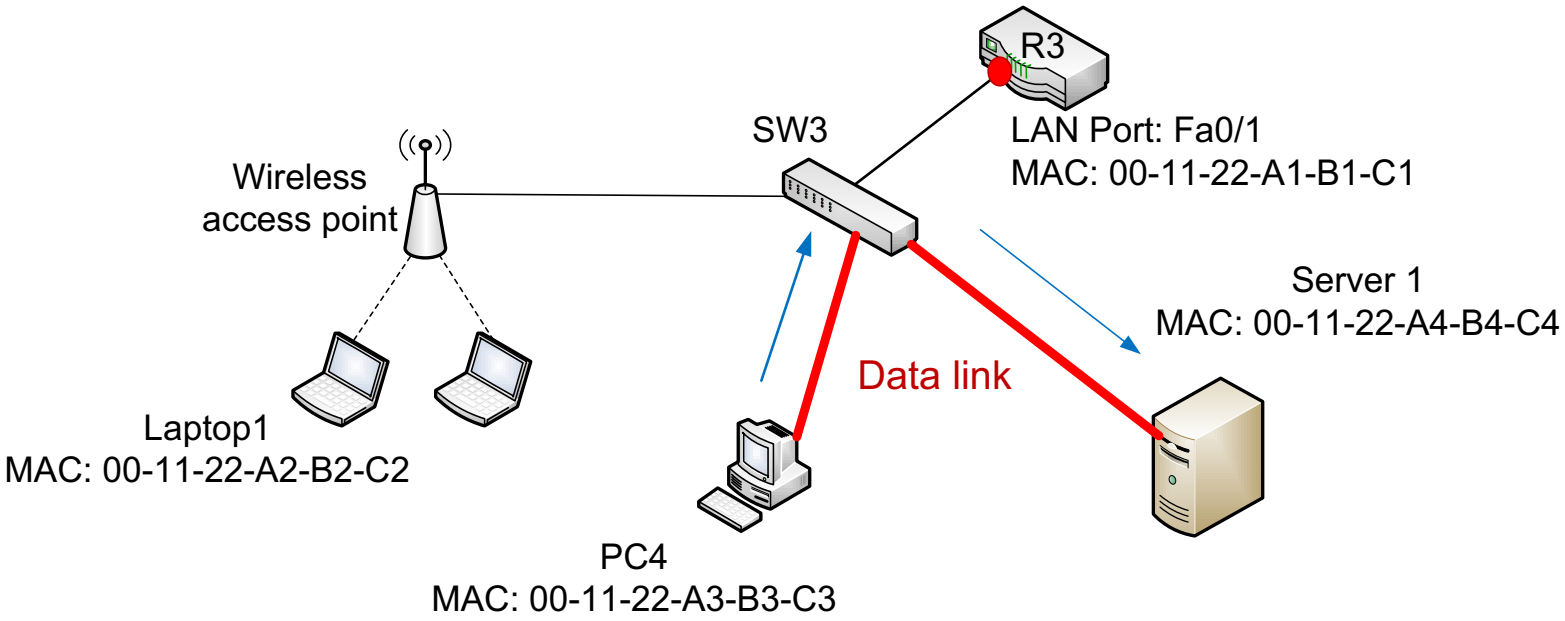


Figure 2.7 Use of MAC addressing for intra-networking

2.5 Data Link Layer (Layer 2) Header

Ethernet (802.3) Frame Format

7 bytes	1 byte	6 bytes	6 bytes	2 bytes	42 to 1500 bytes	4 bytes	12 bytes
Preamble	Start of Frame Delimiter	**Destination MAC Address**	**Source MAC Address**	Type	Data (payload)	CRC	Inter-frame gap

For TCP/IP communications, the payload for a frame is a packet

WiFi (802.11) Frame Format

2 bytes	2 bytes	6 bytes	6 bytes	6 bytes	2 bytes	6 bytes	0 to 2312 bytes	4 bytes
Frame Control	Duration	MAC Address 1 (Destination)	MAC Address 2 (Source)	MAC Address 3 (Router)	Seq Control	MAC Address 4 (AP)	Data (payload)	CRC

Image from: https://networkengineering.stackexchange.com/

2.6 Internet Layer (Layer 3)

2.6.1 Packet Creation and Routing Decision

Bit 0 Bit 31

Version 4 (= 0100)	Header Length (4 bits)	Diff-Serv (8 bits)	Total Length in Octets (16 bits)	
Identification (16 bits)			Flags (3 bits)	Fragment Offset (13 bits)
Time to Live (8 bits)	Protocol in the Data field (8bits)		Header Checksum (16 bits)	
Source IP address (32 bits)				
Destination IP address (32 bits)				
Options (if any)				Padding
Data Field (Transport Layer PDU) Note: Oftentimes significantly longer than the header				

Figure 2.8 IPv4's packet structure

2.6 Internet Layer (Layer 3)

2.6.2 Perform supervisory functions

- ICMP (Internet Control Message Protocol)

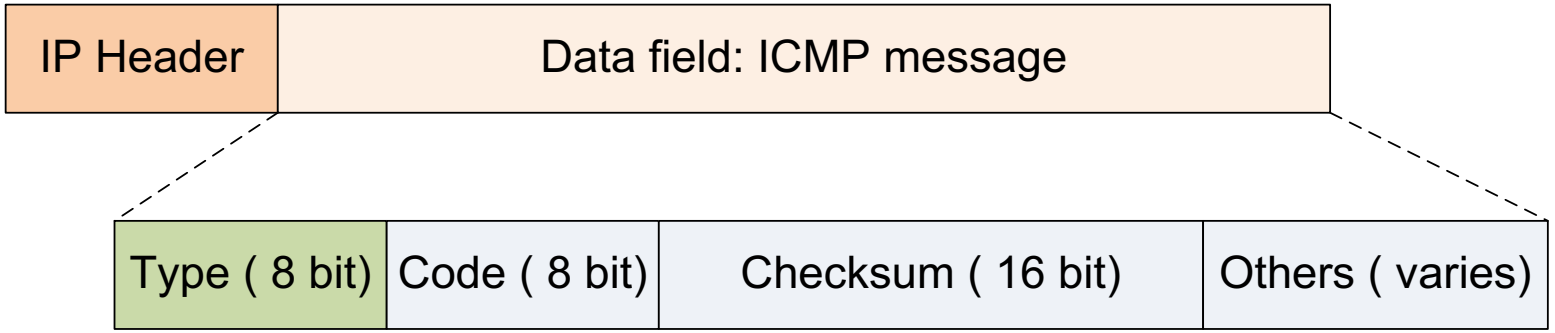
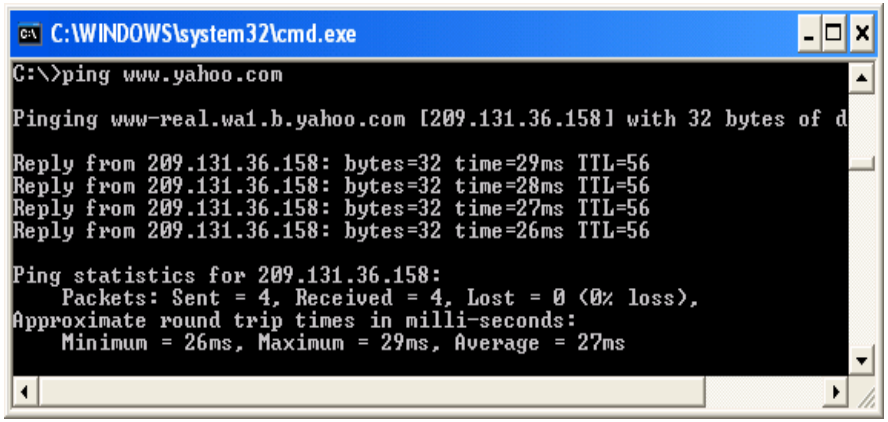


Figure 2.9 The structure of an ICMP packet

- Type field: Indicates supervisory function type.
- Examples : 0 (echo reply) and 8 (echo request)

ICMP Messages: Examples



Ping = echo request
(*Type value* = 8 in Figure 2.9)

Figure 2.10 A demonstration of pinging

Traceroute
(*Type value* = 30 in Figure 2.9)

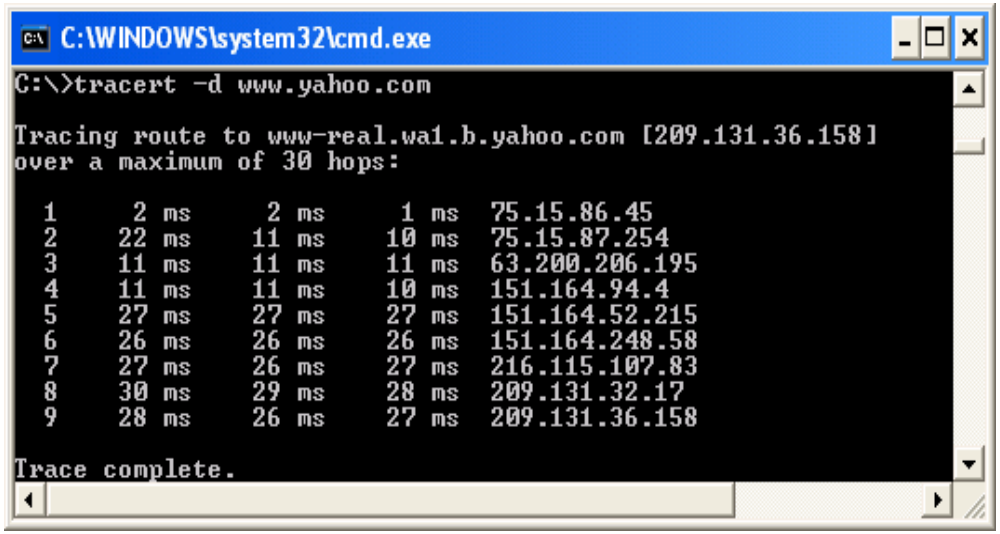


Figure 2.11 A Demonstration of *tracert*

2.7 Transport Layer (Layer 4)

- Key functions: handling of end-to-end (host-to-host) connectivity issues

(1) Provision of data integrity : TCP
(2) Session management : TCP
(3) Port management: TCP and UDP

2.7 Transport Layer (Layer 4)

2.7.1 Provision of data integrity (with TCP)

- Error control: acknowledgement (ACK)
- Flow control: *Window Size*

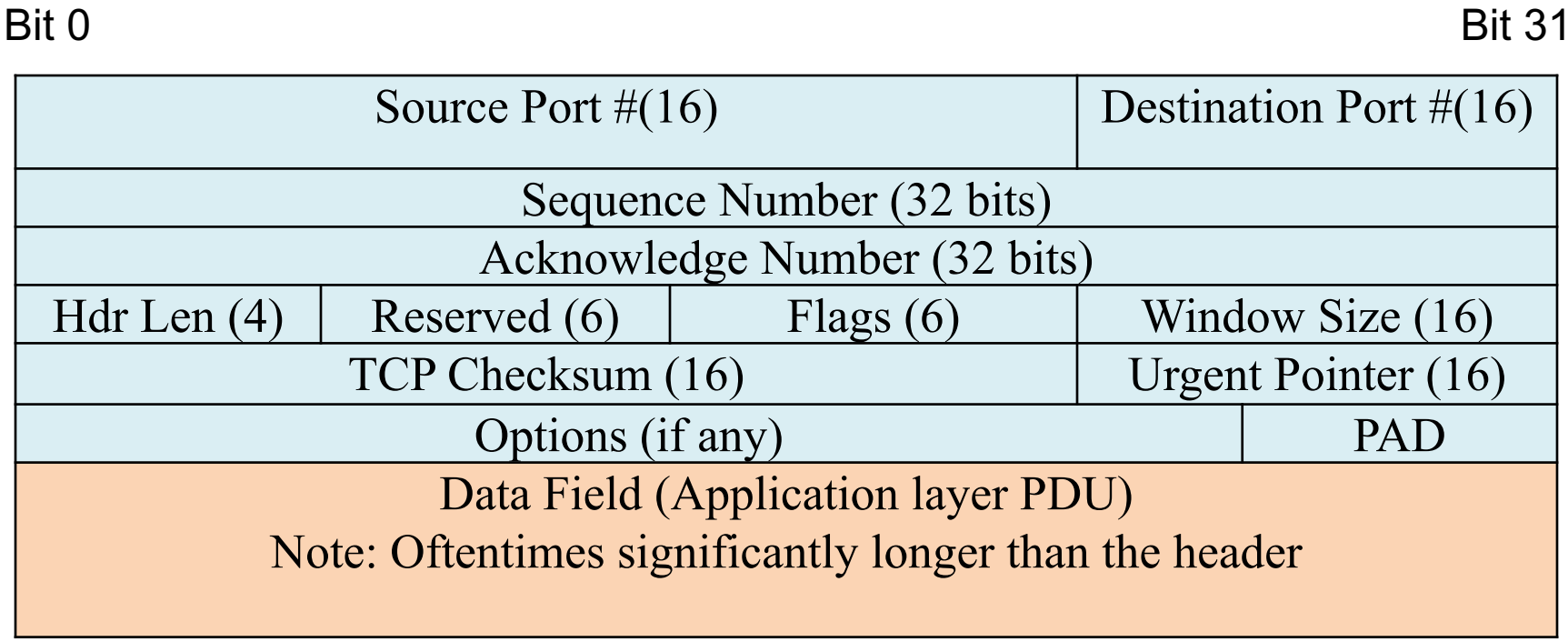


Figure 2.12 TCP segment

2.7 Transport Layer (Layer 4)

UDP: No flow control, no error control

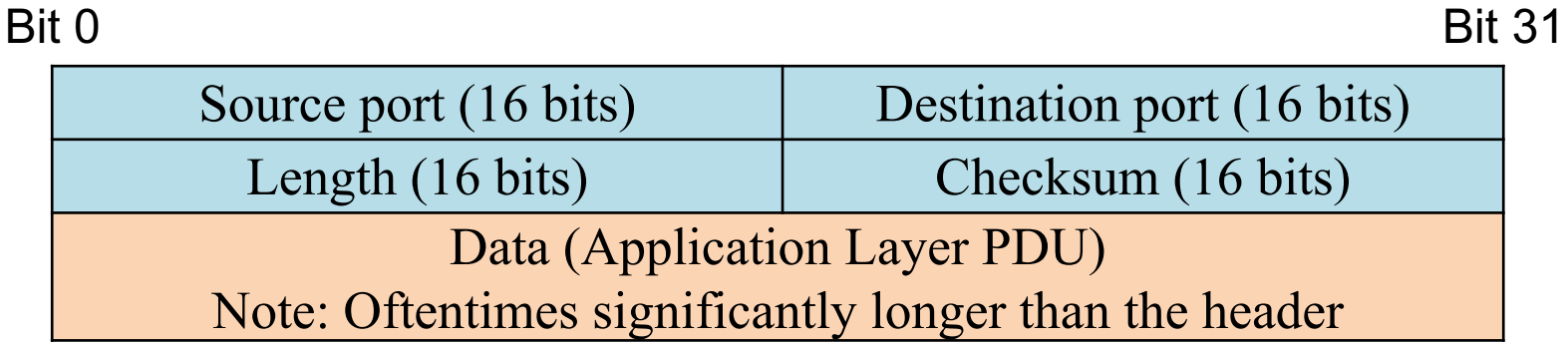
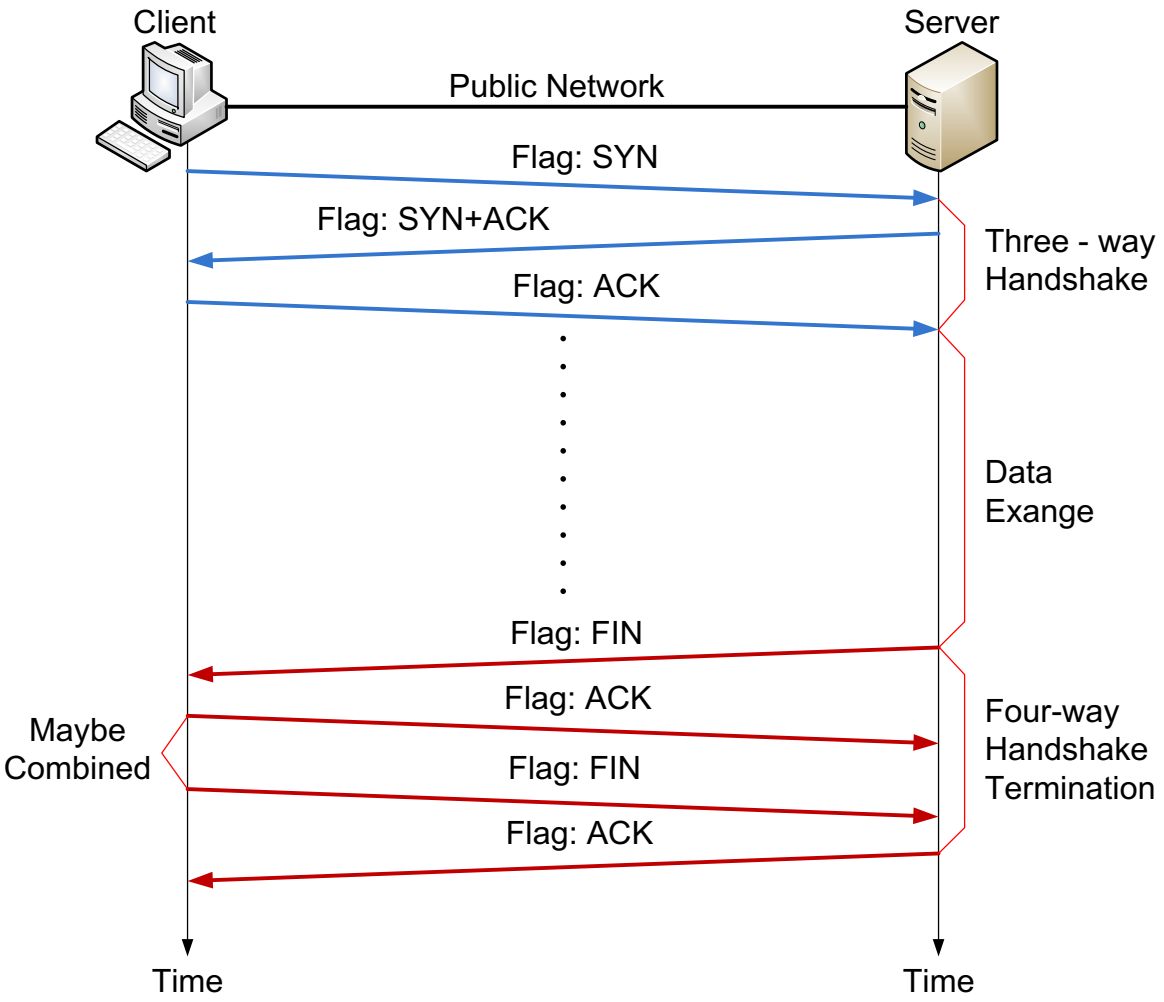


Figure 2.13 UDP datagram

2.7 Transport Layer (Layer 4)

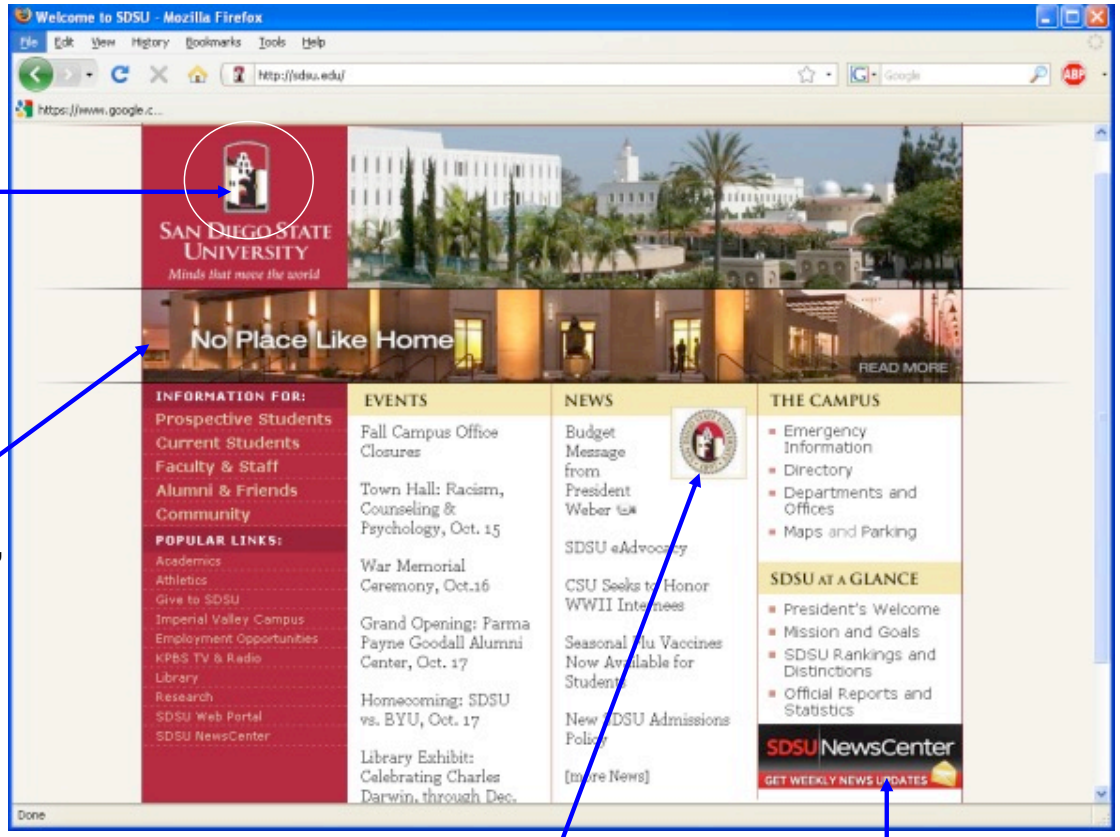
2.7.2 Session management (with TCP)

Figure 2.14



2.7 Transport Layer (Layer 4)

2.7.2 Session management (with TCP)



Object 1 (GIF image, 3122 bytes)

Object 2 (JPEG image, 15140 bytes)

Object 3 (JPEG image, 2169 bytes)

Object 4 (GIF image, 9913 bytes)

Figure 2.15

2.7 Transport Layer (Layer 4)

2.7.2 Session management (with TCP)

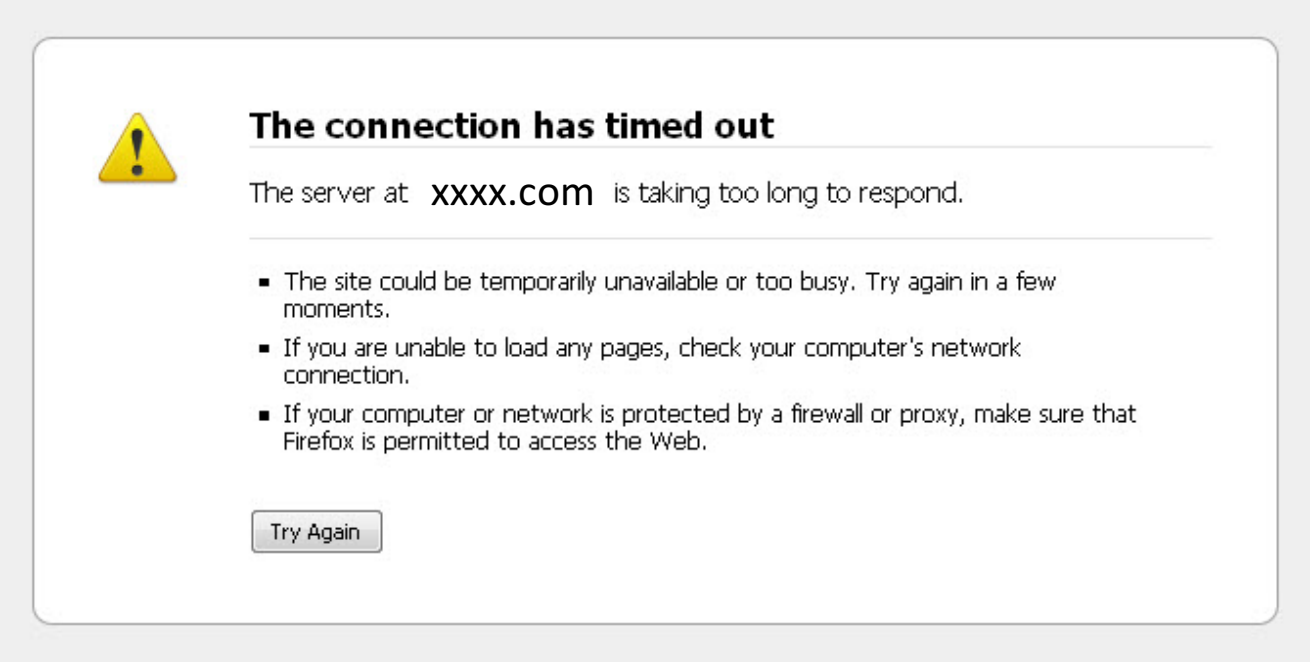


Figure 2.16 Notification of failed TCP handshaking

2.7 Transport Layer (Layer 4)

2.7.3 Port management (with TCP and UDP)

To identify an engaging "application" at the application layer

- Well-known Ports (0 through 1023)
- Registered Ports (1024 through 49151)
- Private/Dynamic Ports (49152 through 65535)

Application	Function/Description	Port #
Telnet	Remote access	23
FTP	File transfer protocol	20,21
SMTP	Simple mail transfer protocol	25
DNS	Domain name service	53
DHCP	Dynamic host configuration protocol	67,68
HTTP	Hypertext transfer protocol	80
POP3	Post office protocol	110

Table 2.2 Well-known port numbers

2.7 Transport Layer (Layer 4)

2.7.3 Port management (with TCP and UDP)

- A socket = an IP address: a port number

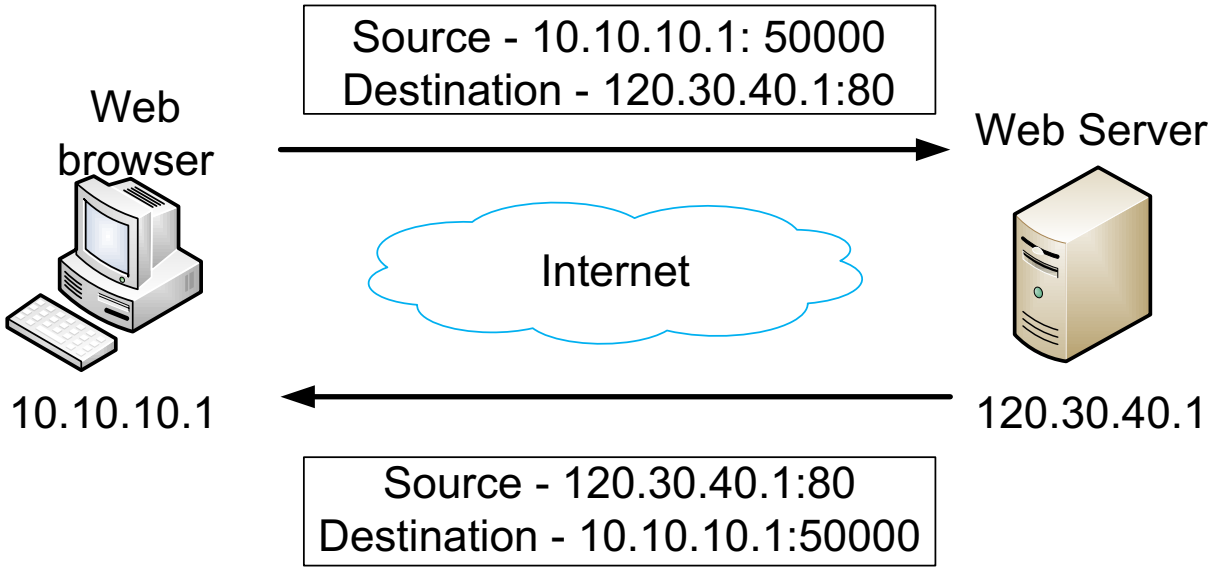


Figure 2.17 A demonstration of sockets

2.8 Application Layer (Layer 5)

Types	Applications programs	Standard protocols embedded
User application oriented	Email	SMTP POP3
	Conferencing	IRC (Internet Relay Chat)
	Remote file transfer	FTP (File Transfer Protocol)
	Remote access	SSH (Telnet, Secure Shell)
	World Wide Web	HTTP (Hyper Text Transfer Protocol)
	Network management	SNMP
	Voice over IP (Internet calls)	H.323
Common service oriented	Mapping between the IP address and the host name	DNS (Domain Name Service)
	Provision of temporary IP	DHCP

Table 2.3 Well-known application layer protocols

2.9 Layer Implementation

Layers	Key Functions	Implementation of layer functions	PDU name
Application	Application-to-application Communication	Applications (ex. browser)	No designated PDU name
Transport	Host-to-host (or end-to-end) handshaking Flow/error control	Operating system (ex. Windows)	TCP segment UDP datagram
Internet	Packet creation and routing decision for internetworking		Packet
Data link	Frame creation and switching for intranetworking	Network interface card (NIC)	Frame
Physical	Signal generation and delivery		No PDUs produced.

Table 2.4 Key layer functions and their implementation

2.9 Layer Implementation

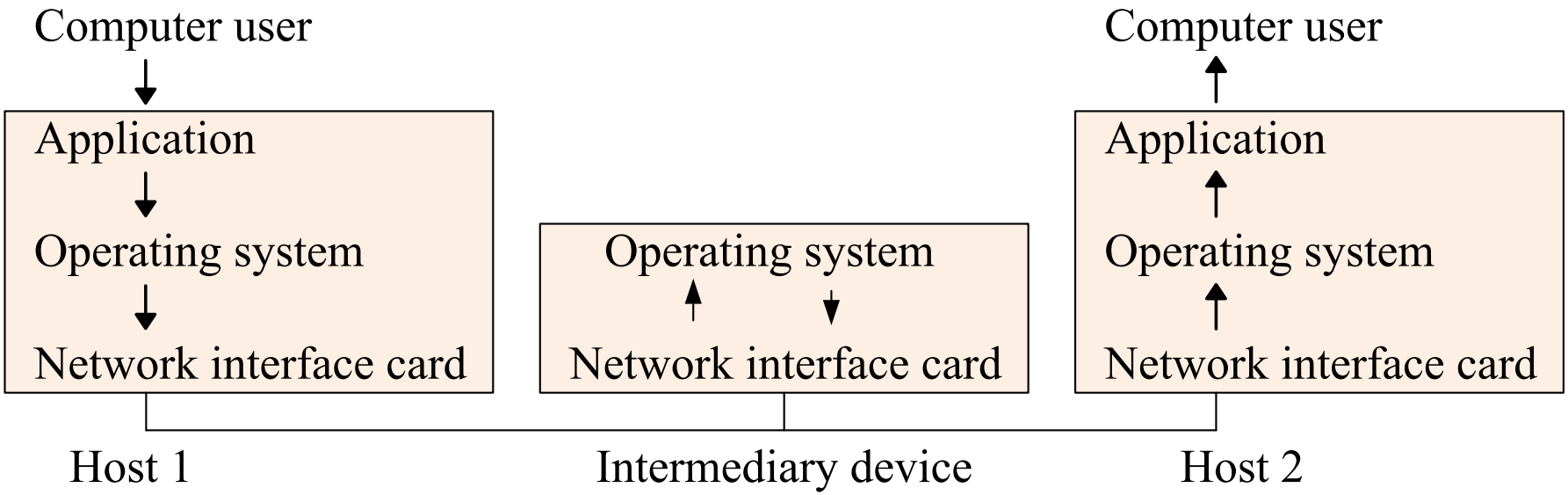


Figure 2.21 Hardware/software components of network nodes

2.10 Layer Processing

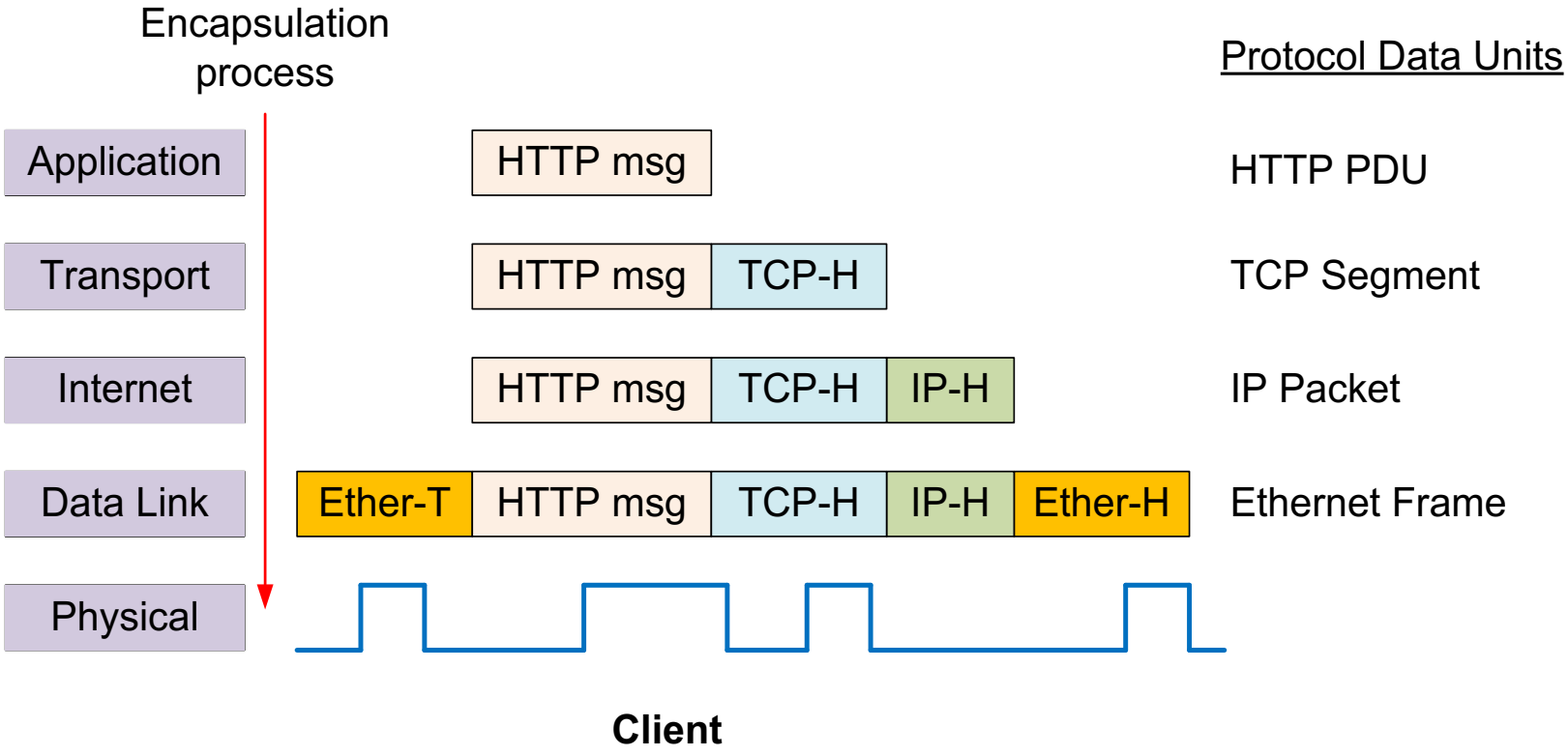


Figure 2.22 PDU encapsulation/de-encapsulation

2.10 Layer Processing

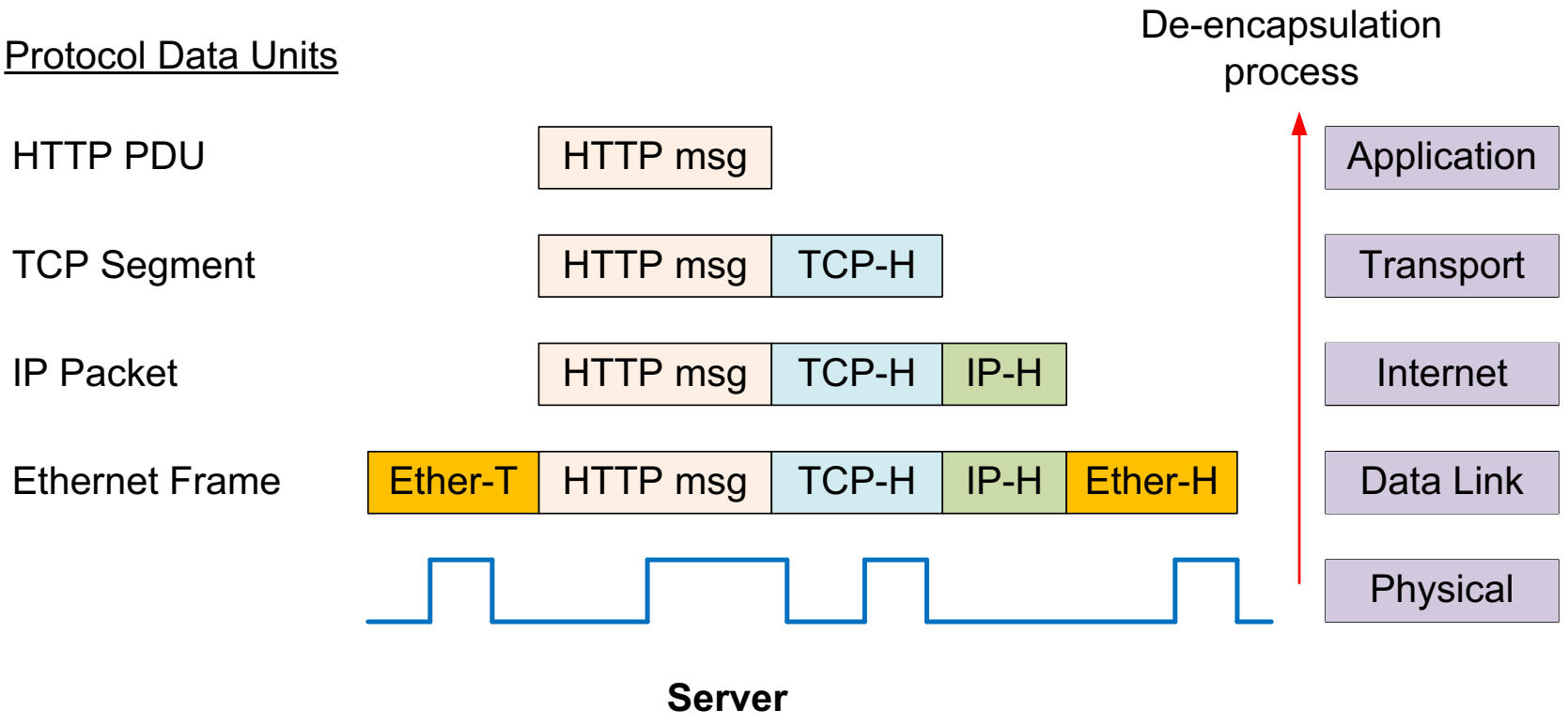


Figure 2.22 PDU encapsulation/de-encapsulation

2.10 Layer Processing

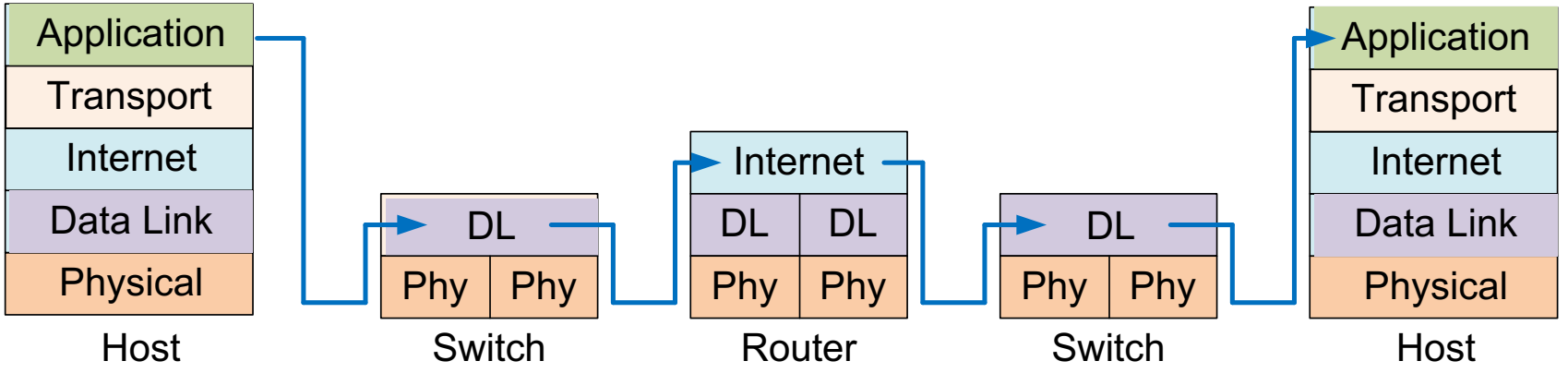


Figure 2.23 Layer processing by intermediary devices

2.10 Layer Processing

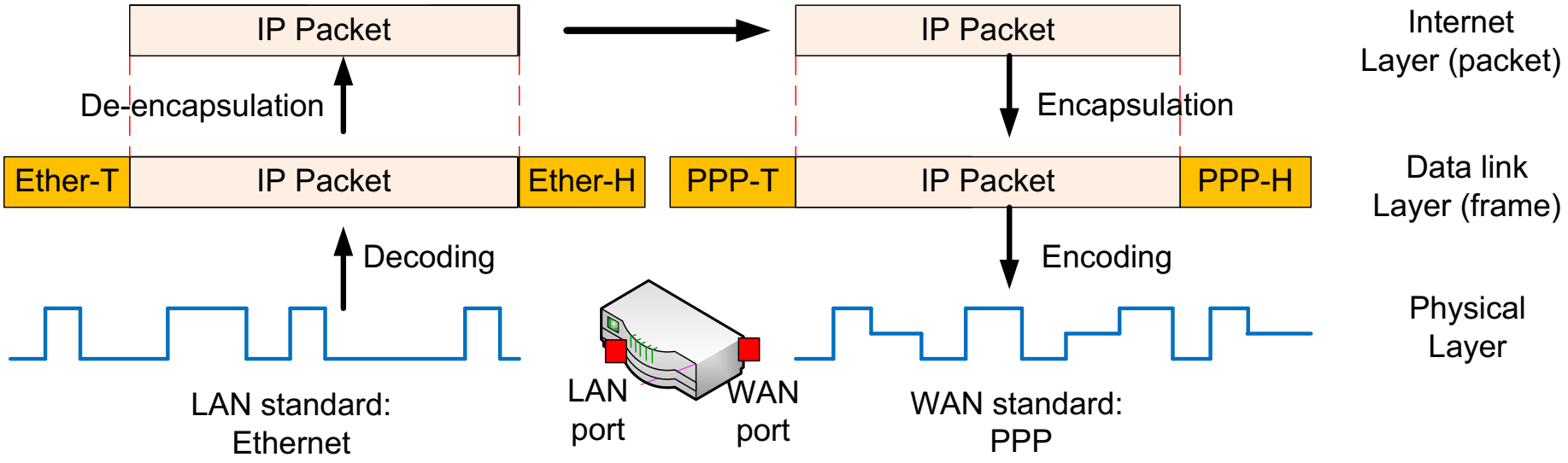


Figure 2.24 Packet de-encapsulation/encapsulation by the router

Recap

- Architectures and layers
- Protocol Data Units
- Layers in the hybrid architecture
- Key layer functions
- Implementation of layer functions on a host
- Layer processing (encapsulation and de-encapsulation)

End
Chapter 2

CECS 303 Networks and Networks Security

Intermediary Devices
Chapter 3

Jose Tamayo, M.S.
Computer Engineering & Computer Science
California State University, Long Beach

3.2 Intermediary Devices

3.2.1 Operational Layers

Layers	Intermediary (or Networking) Devices
Application	
Transport	
Internet	Routers, Layer 3 switches
Data Link	Bridges, Wireless Access Points, Switches
Physical	Hubs (Multiport Repeaters)

Table 3.1 Intermediary devices and their standard layers

3.2.2 Operating System Access

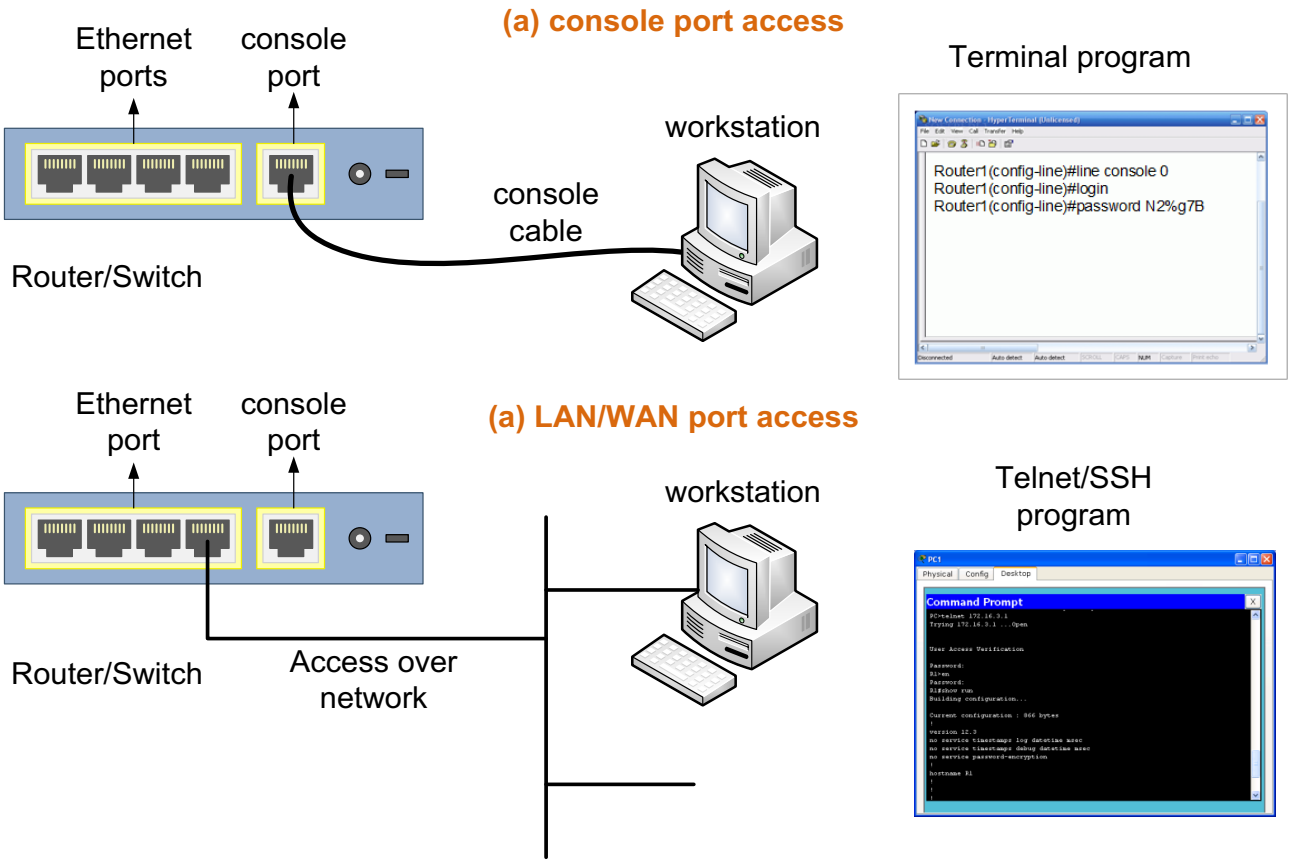


Figure 3.1 Managing an intermediary device

3.3 Hubs (Multi-port Repeaters)

- Multiport repeater
- Shared media
- Half-duplex mode
- MAC: CSMA/CD
- Security : Vulnerable to NIC's promiscuous mode

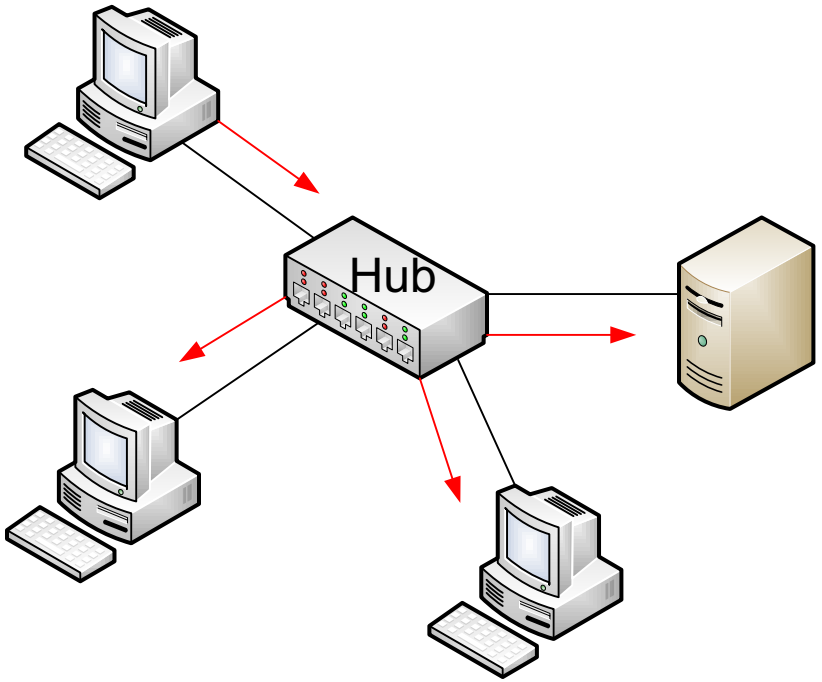


Figure 3.3 A small hub-based network

3.4 Bridges & Wireless Access Points

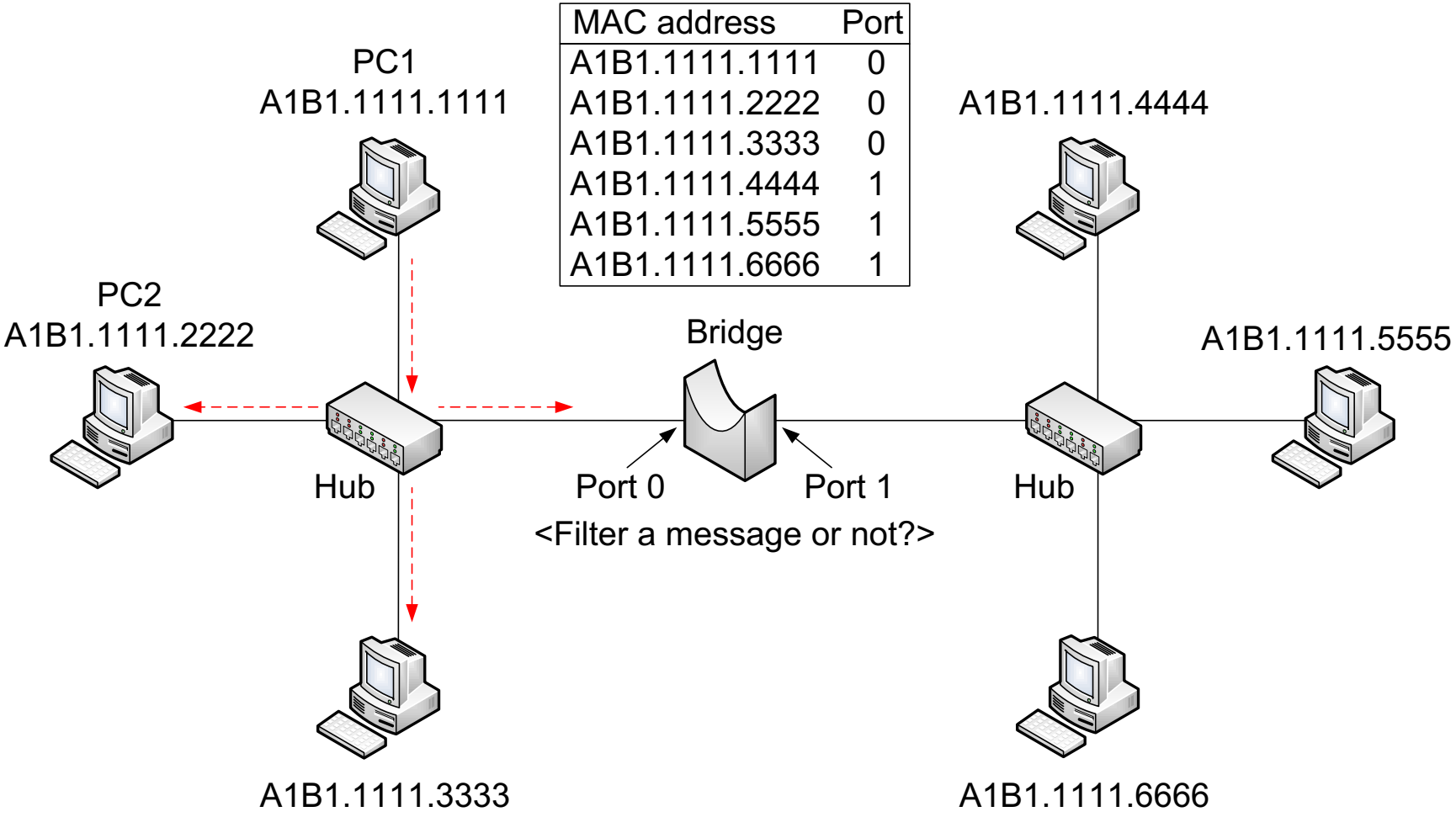
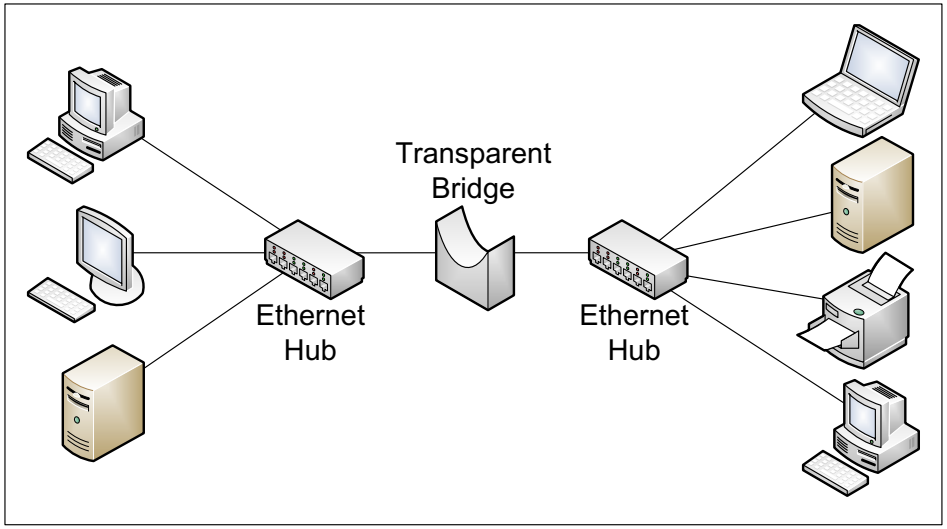


Figure 3.4 An example of bridge table

3.4 Bridges & Wireless Access Points



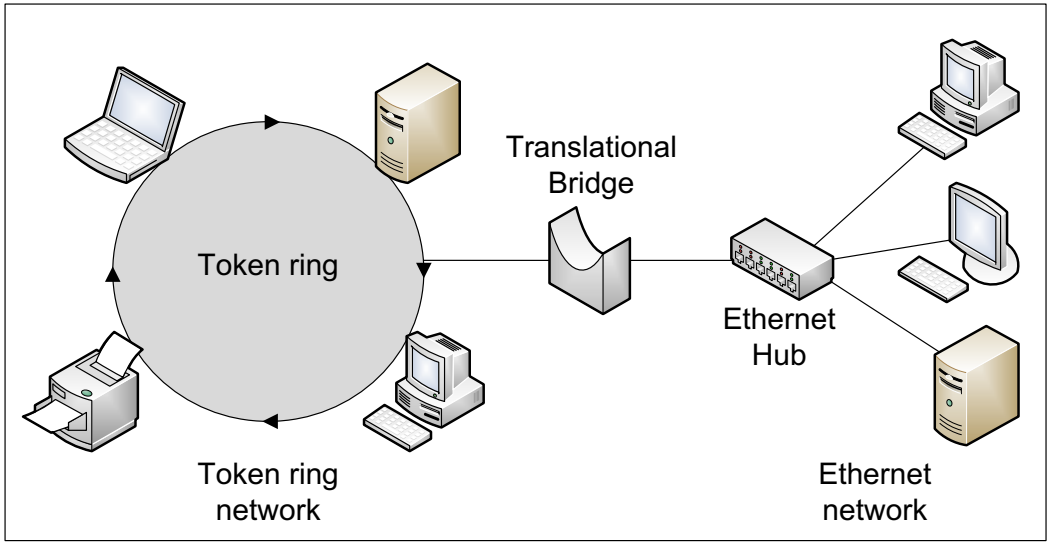


Figure 3.5

Transparent vs. translational bridges

3.4 Bridges & Wireless Access Points

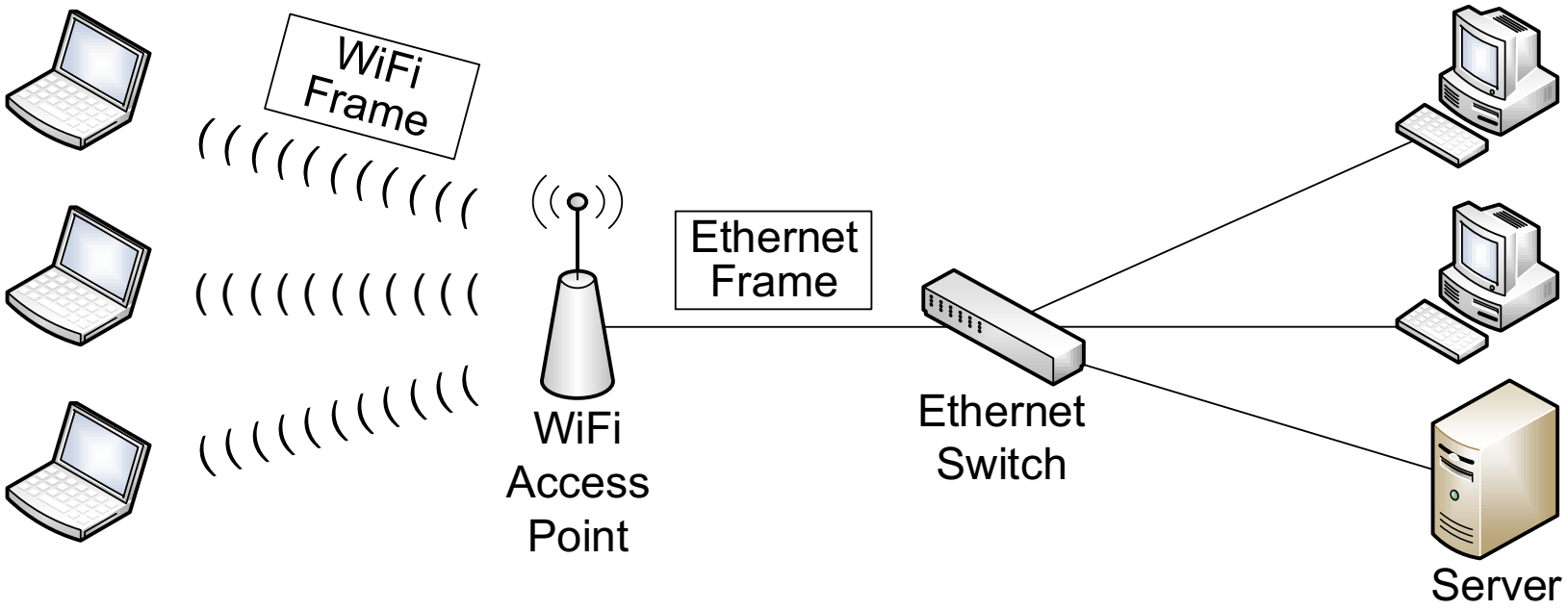


Figure 3.6 Wireless Access Point as a translational bridge

3.5 Switches
3.5.1 General Features

- Port density
- Wire speed
- Forwarding rate
- Aggregate throughput
- Non-blocking vs. blocking

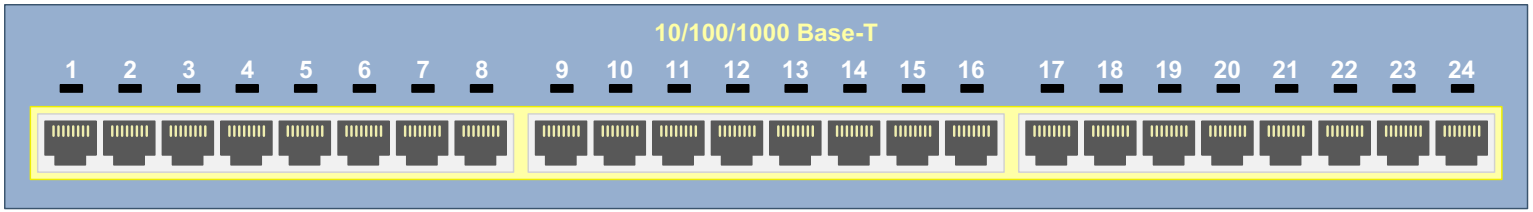


Figure 3.7 Ethernet switch – external view (not an actual product)

3.5.2 Switch Ports

Port full name	Abbreviation	MAC address
FastEthernet0/1	Fa0/1	0005.B119.6A01
FastEthernet0/2	Fa0/2	0005.B119.6A02
….		
….		
FastEthernet0/23	Fa0/23	0005.B119.6A03
FastEthernet0/24	Fa0/24	0005.B119.6A04
GigabitEthernet1/1	Gi1/1	0005.B119.7C03
GigabitEthernet1/2	Gi1/2	0005.B119.7C04

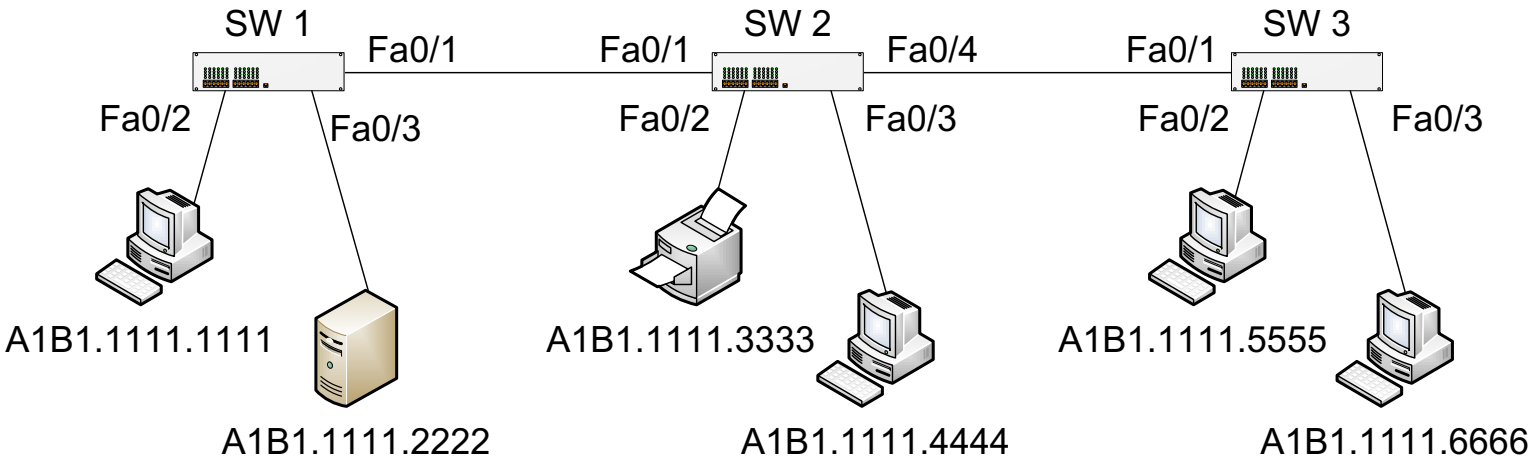
Table 3.3 Switch port naming (This is not a switch table)

3.5.3 Switch table

Destination MAC Address	Exit Port	Address Type	VLAN
0002.584B.16E0	FastEthernet 0/1	Static	1
00B0.D0F3.47AC	FastEthernet 0/2	Static	1
00C1.4AC7.23D2	FastEthernet 0/3	Dynamic	1
00B0.D045.963A	FastEthernet 0/3	Dynamic	1

Table 3.4 Demonstration of a switch table (an example)

3.5.3 Switch Table



SW 1

Port	MAC address
Fa0/1	A1B1.1111.3333
Fa0/1	A1B1.1111.4444
Fa0/1	A1B1.1111.5555
Fa0/1	A1B1.1111.6666
Fa0/2	A1B1.1111.1111
Fa0/3	A1B1.1111.2222

SW 2

Port	MAC address
Fa0/1	A1B1.1111.1111
Fa0/1	A1B1.1111.2222
Fa0/2	A1B1.1111.3333
Fa0/3	A1B1.1111.4444
Fa0/4	A1B1.1111.5555
Fa0/4	A1B1.1111.6666

SW 3

	?

Figure 3.8 Switches tables

3.5.4 Switch Types

- Non-managed vs. Managed Switches
- Store-and-forward vs. Cut-through Switches
- Symmetric vs. Asymmetric Switches
- Layer 2 vs. Layer 3 Switches
- Fixed, Stackable, and Modular Switches
- Power over Ethernet

Figure 3.12 Ethernet Layer 3 switch

Power over Ethernet (POE)

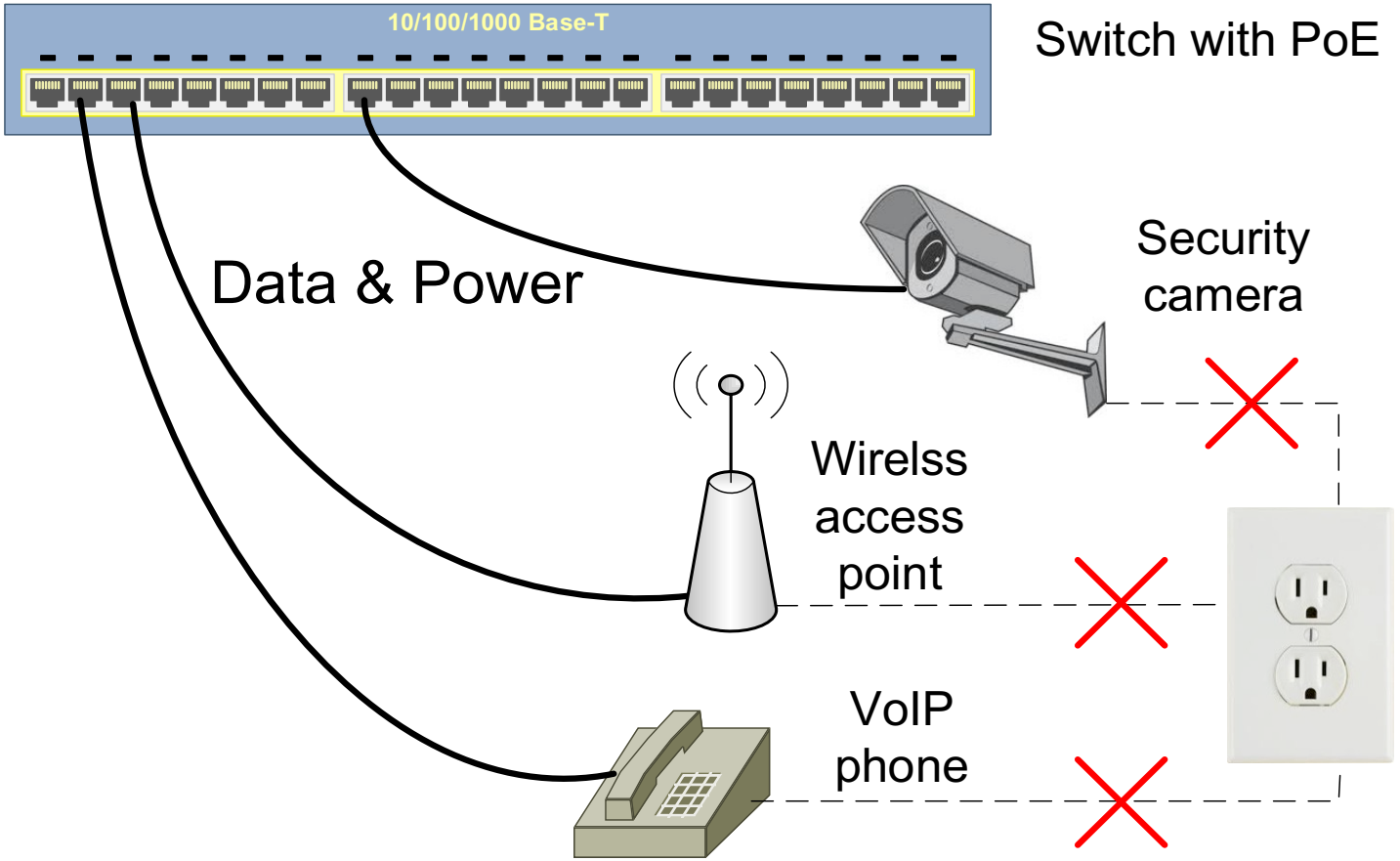


Figure 3.14 Power over Ethernet

3.5.5 Security

- Safeguarding switch ports
  - Allow only legitimate MAC addresses
  - Manually shutdown all unused ports
  - To prevent footprinting / reconnaissance
  - To prevent MAC address flooding

- Port mirroring
  - Mirror port

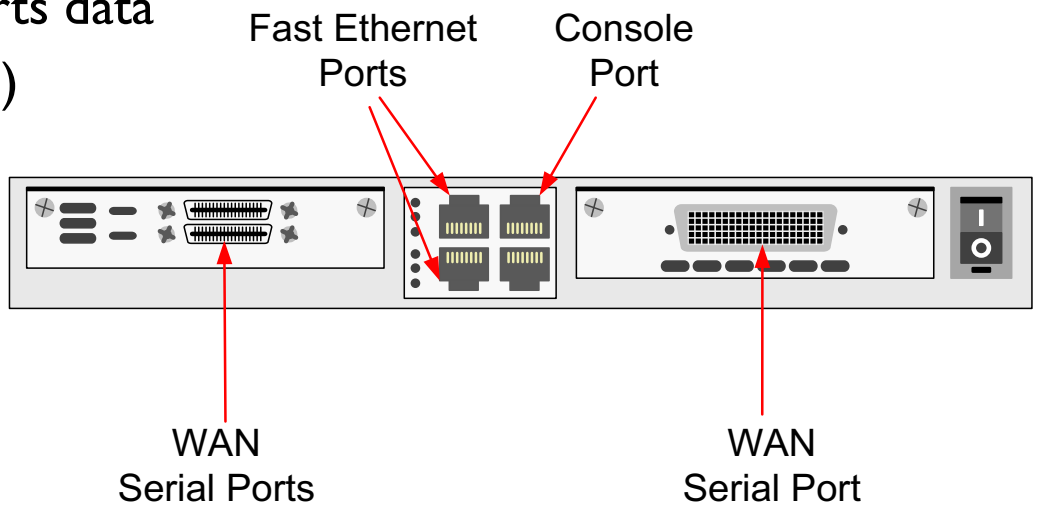
3.6 Routers

3.6.1 Two Primary Functions

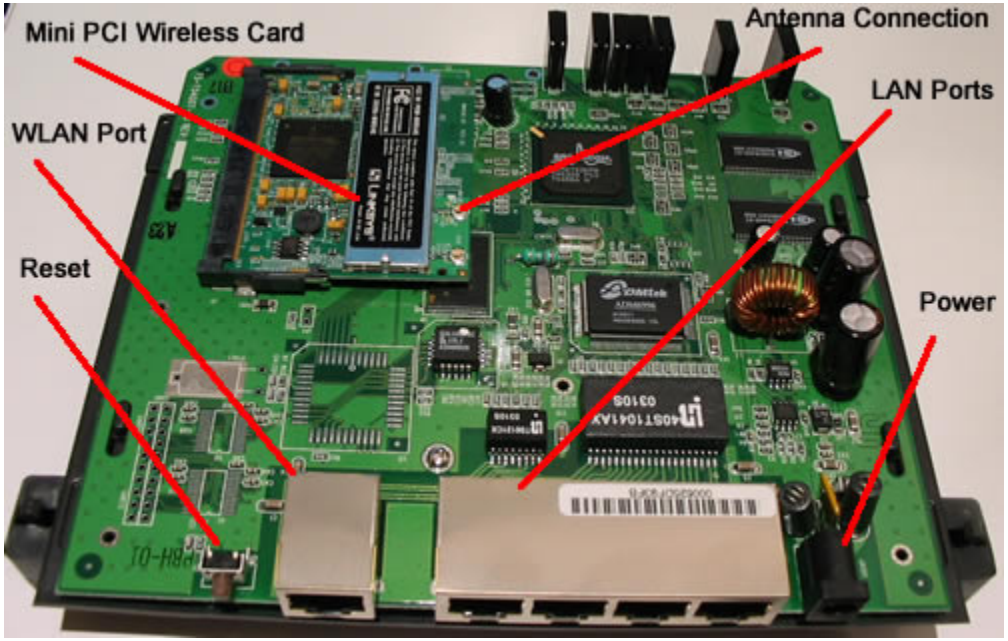
- *Routing table development and its update*
- *Packet forwarding*

3.6.2 Router Components

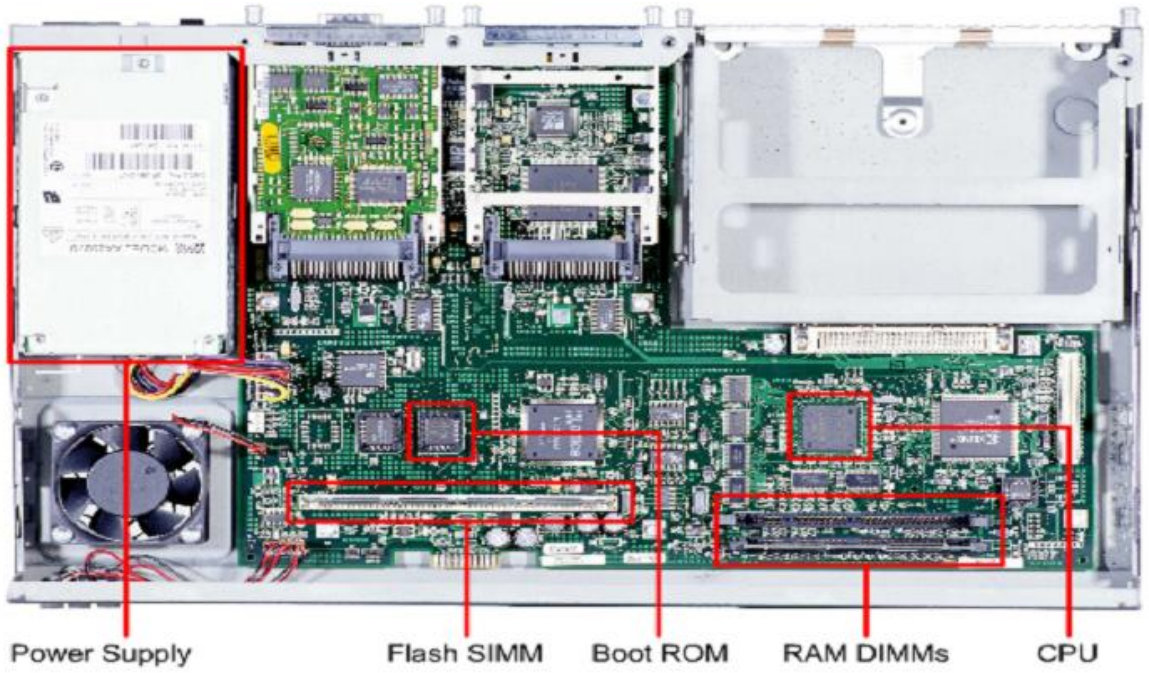
- Central processing unit (CPU)
- Memory: ROM, RAM, Non-volatile flash memory
- Operating System
- System bus that transports data
- Various ports (interfaces)



Inside the router (Extra)



http://wlanbook.com/wireless-access-point-router-autopsy/



http://engweb.info/courses/itcn/router_basics/router_basics_lecture_00.html

3.6.3 Router Ports & Naming

Example: Cisco router's port naming

- media type slot#/port#" or media type slot#/subslot#/port#

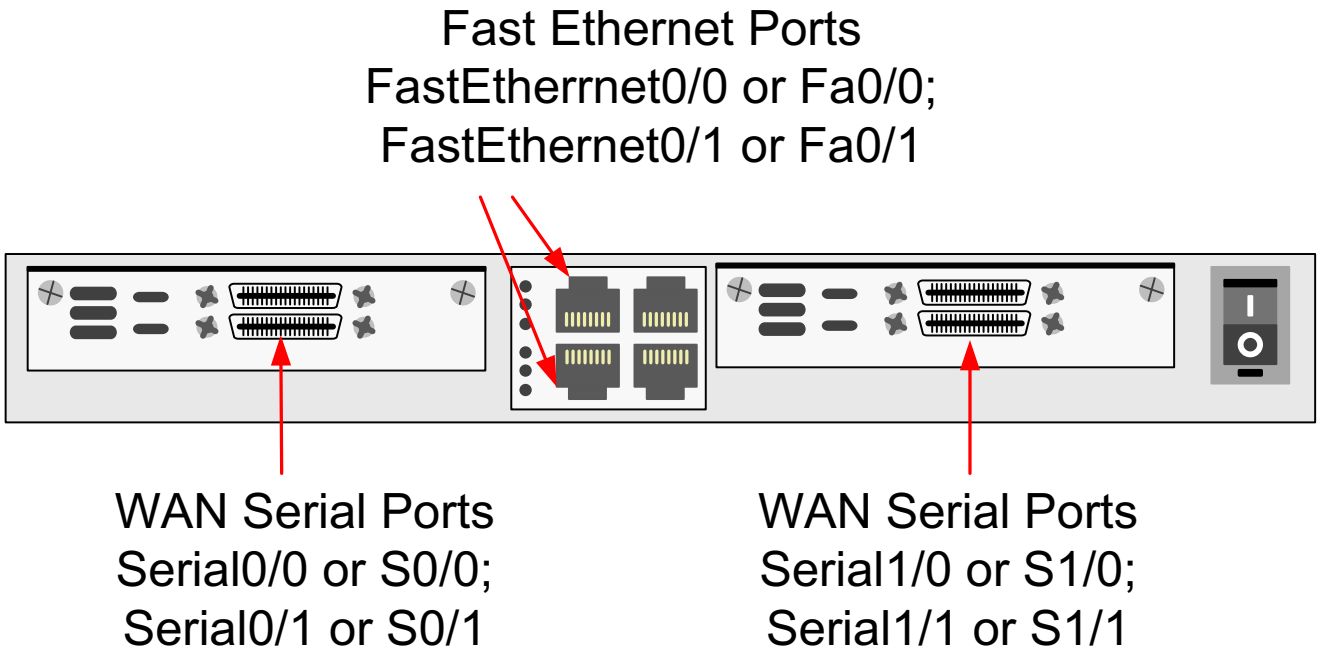


Figure 3.16 Cisco's LAN and WAN port naming (not an actual model)

3.6.4 Router Configuration

Basic Configuration

- Router naming (ex. R1)
- Setting up a password to allow protected access to OS
- IP assignment to LAN/WAN ports and their activation
- Manual entry of static routing paths to the routing table

3.6.4 Router Configuration

Advanced Features

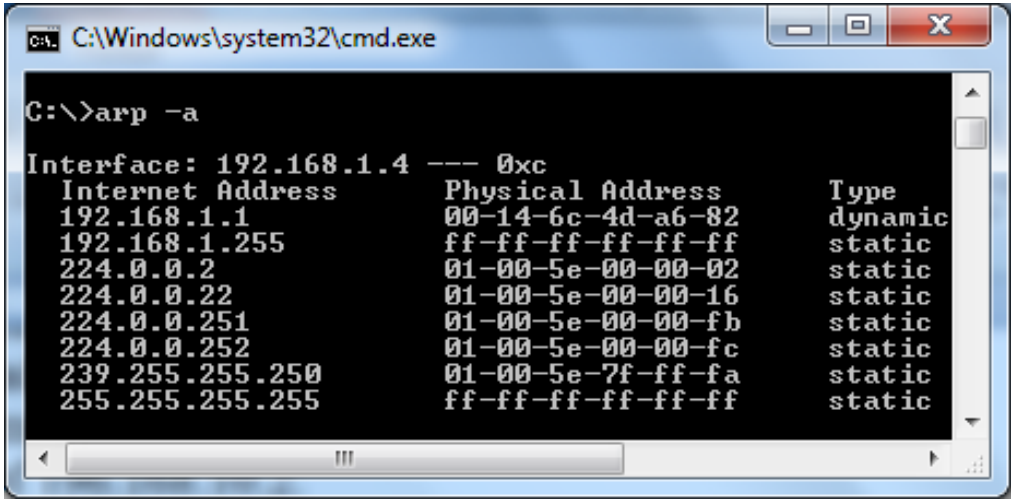
- Access control list (ACL)
- Network address translation (NAT)
- DHCP server
- Virtual Private Network (VPN)
- Intrusion Prevention System (IPS)
- Security auditing

3.7 Switching vs. Routing

1. Data link layer vs. internet layer
2. Connection-oriented vs. connection-less
3. Single delivery path vs. multiple delivery paths

3.8 Address Resolution Protocol

- Mapping between MAC and IP addresses



(a)

Internet address	Physical address	Interface(port)
172.16.10.1	00-23-4C-6A-64-29	FastEthernet0/0
172.16.5.1	00-23-4C-6D-7B-EF	FastEthernet0/1
172.16.7.1	00-23-4C-2C-8A-DE	FastEthernet0/2

(b)

Figure 3.17 Sample ARP table of host (a) and router (b)

3.8.2 ARP Usage Scenarios

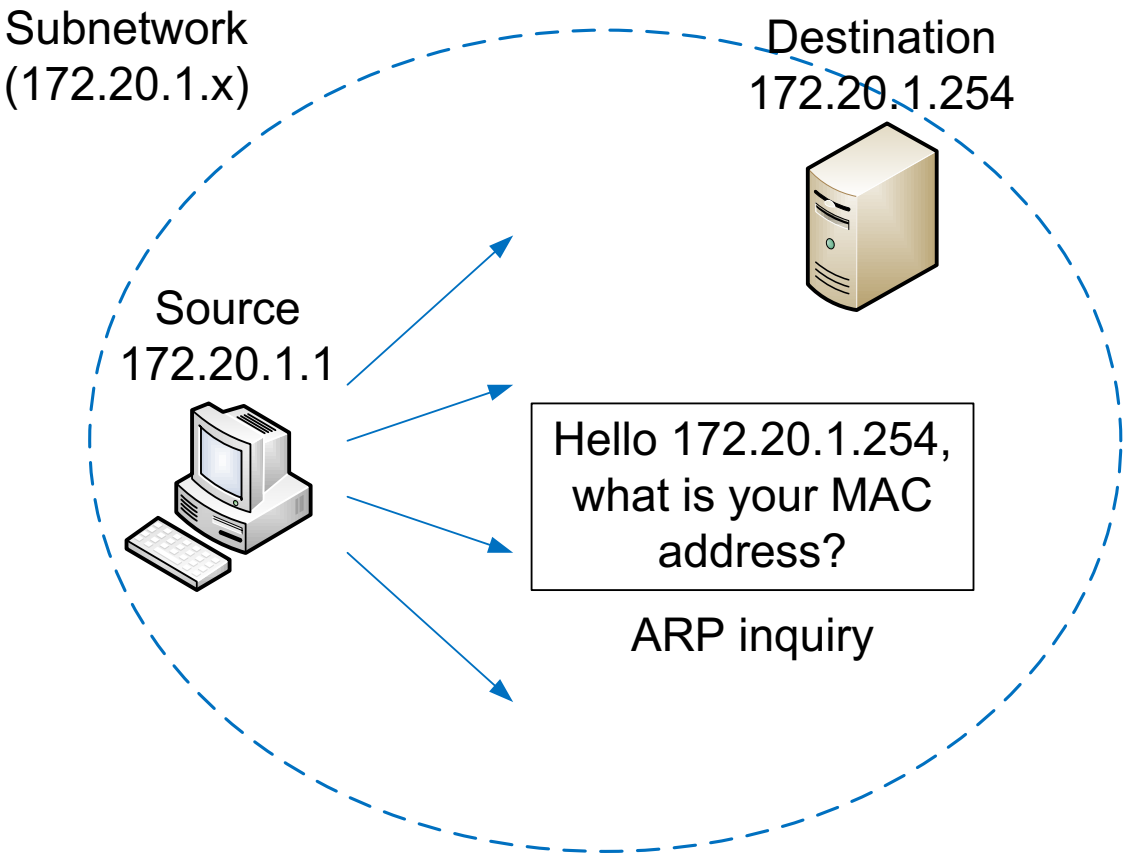


Figure 3.18 Scenario 1: host to host ARP inquiry

3.8.2 ARP Usage Scenarios

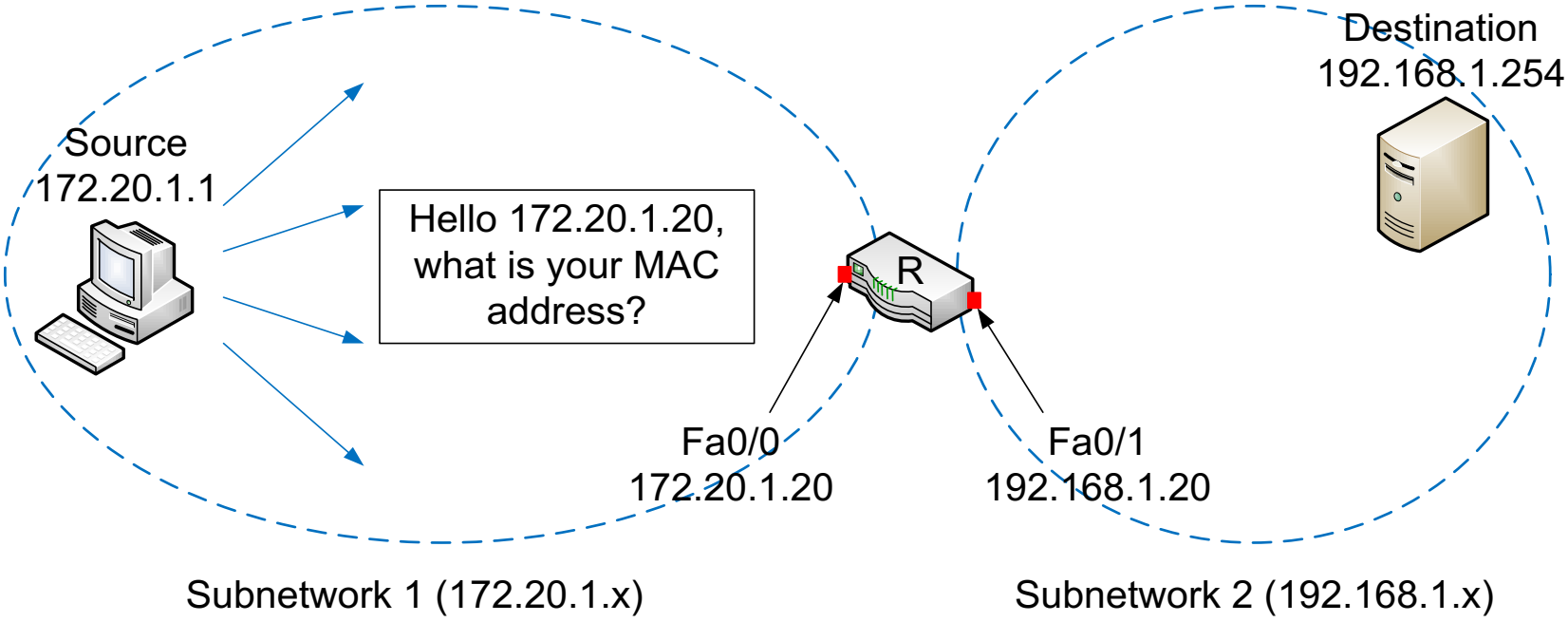


Figure 3.19 Scenario 2: host to router ARP inquiry

3.8.2 ARP Usage Scenarios

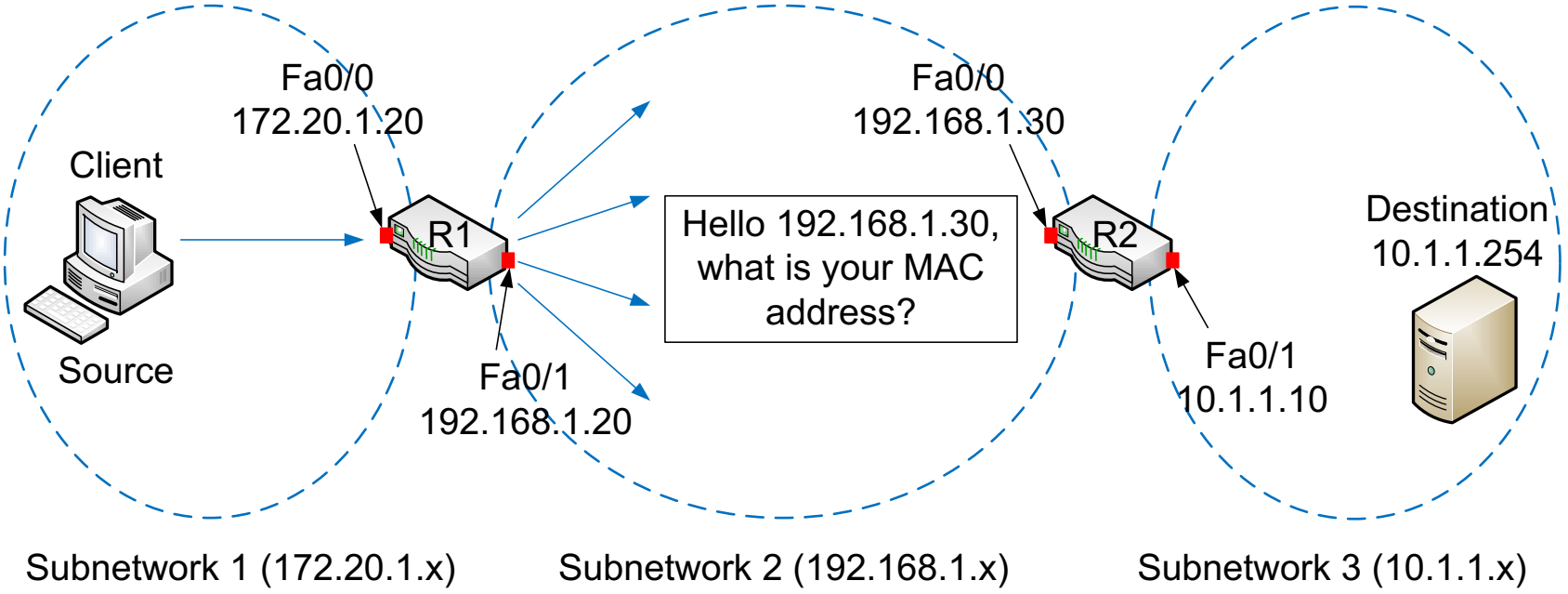


Figure 3.20 Scenario 3: router to router ARP inquiry

3.8.2 ARP Usage Scenarios

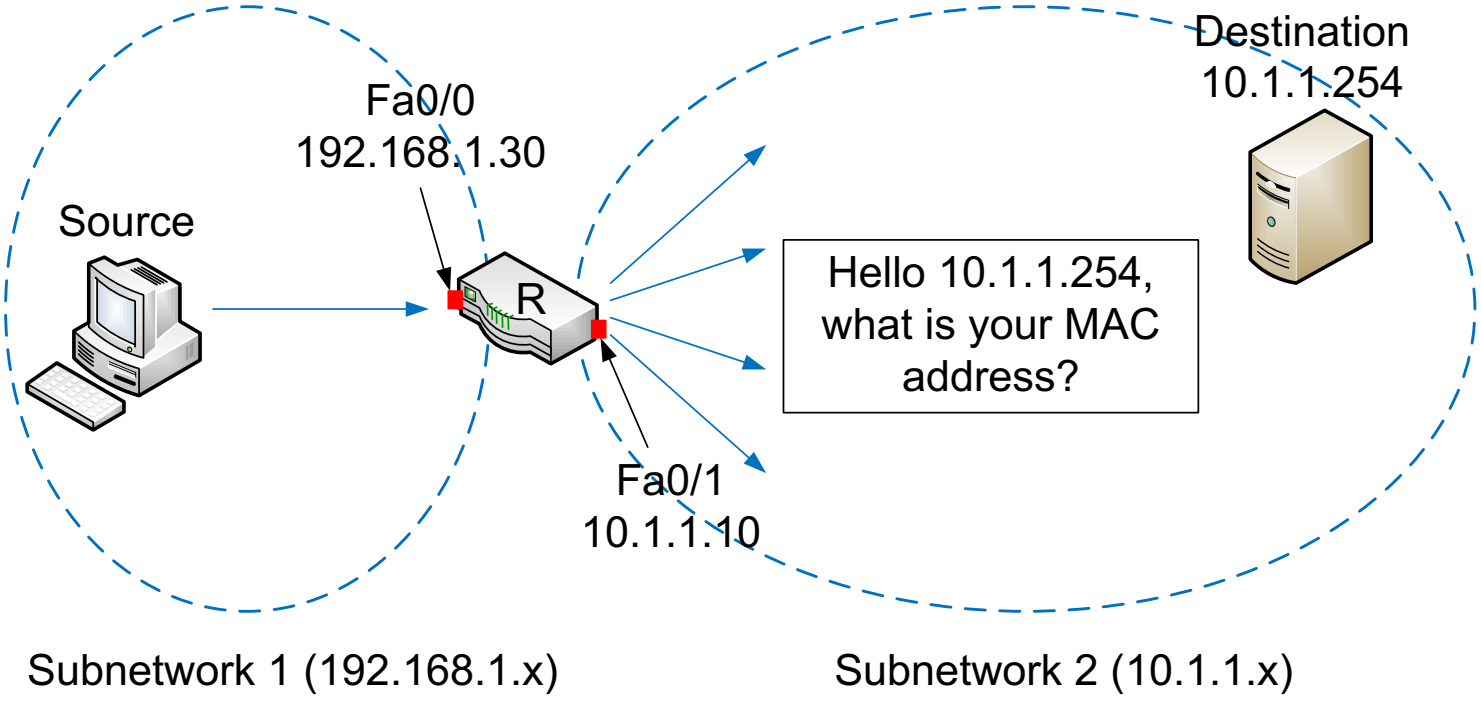


Figure 3.21 Scenario 4: router to host ARP inquiry

3.10 Collision vs. Broadcast Domains

Switch as a collision domain divider

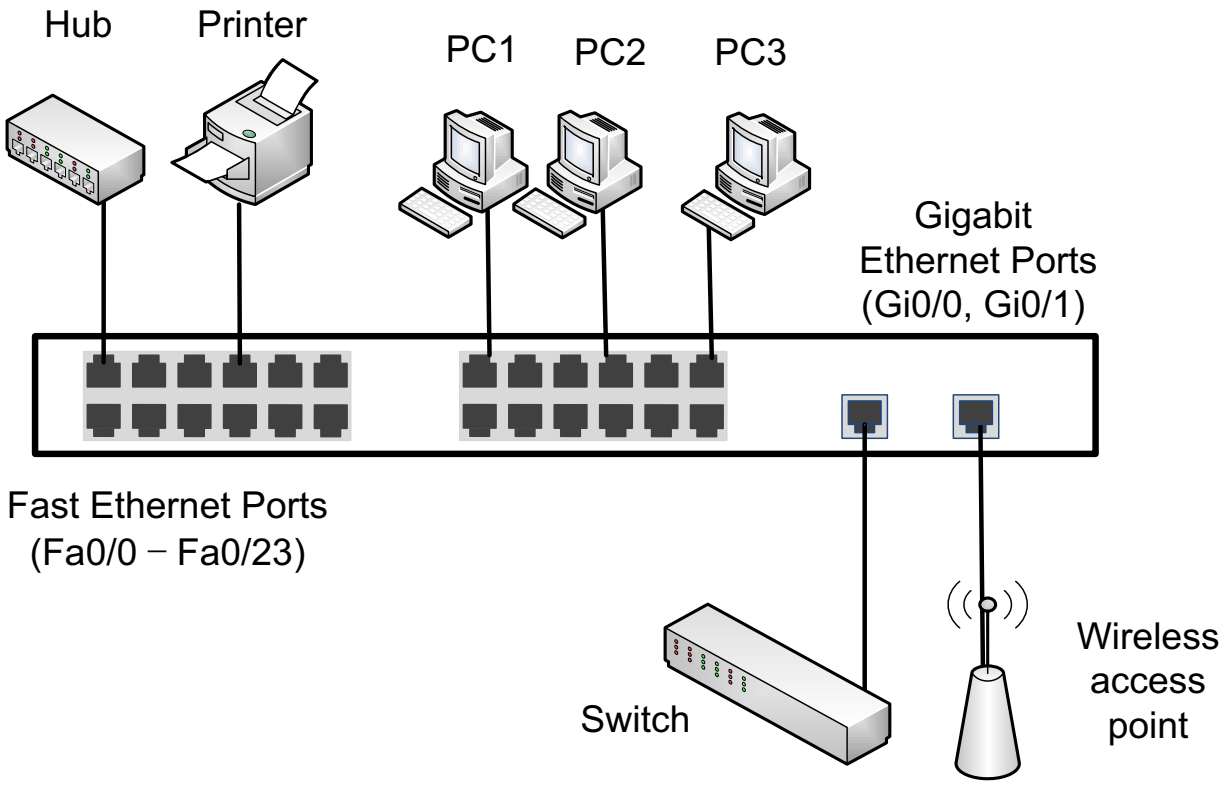


Figure 3.22 Switch as a collision domain divider

3.10 Collision vs. Broadcast Domains

- Collision domain types

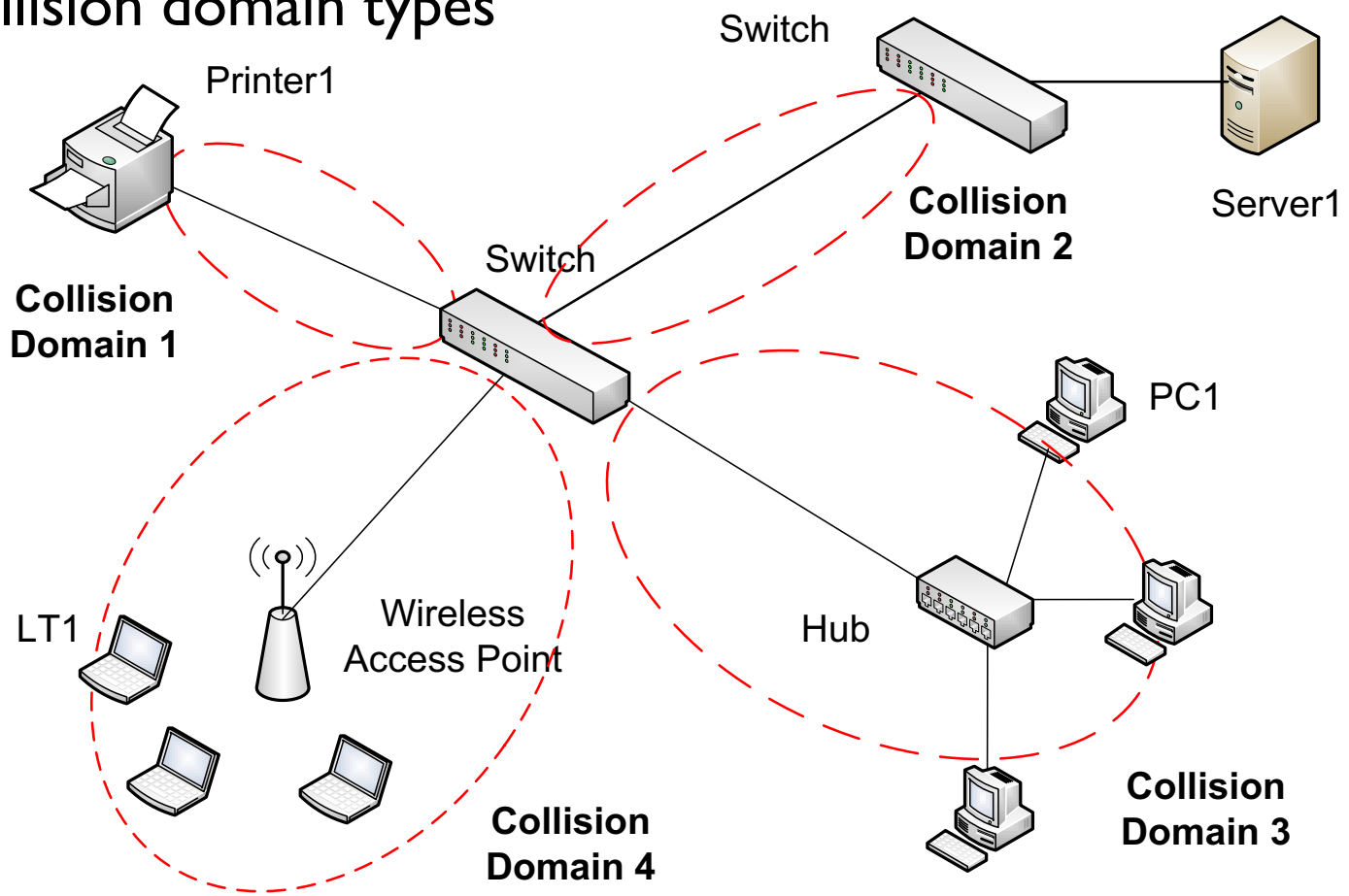


Figure 3.23 Types of collision domain

3.10 Collision vs. Broadcast Domains

- Router as broadcast domain divider

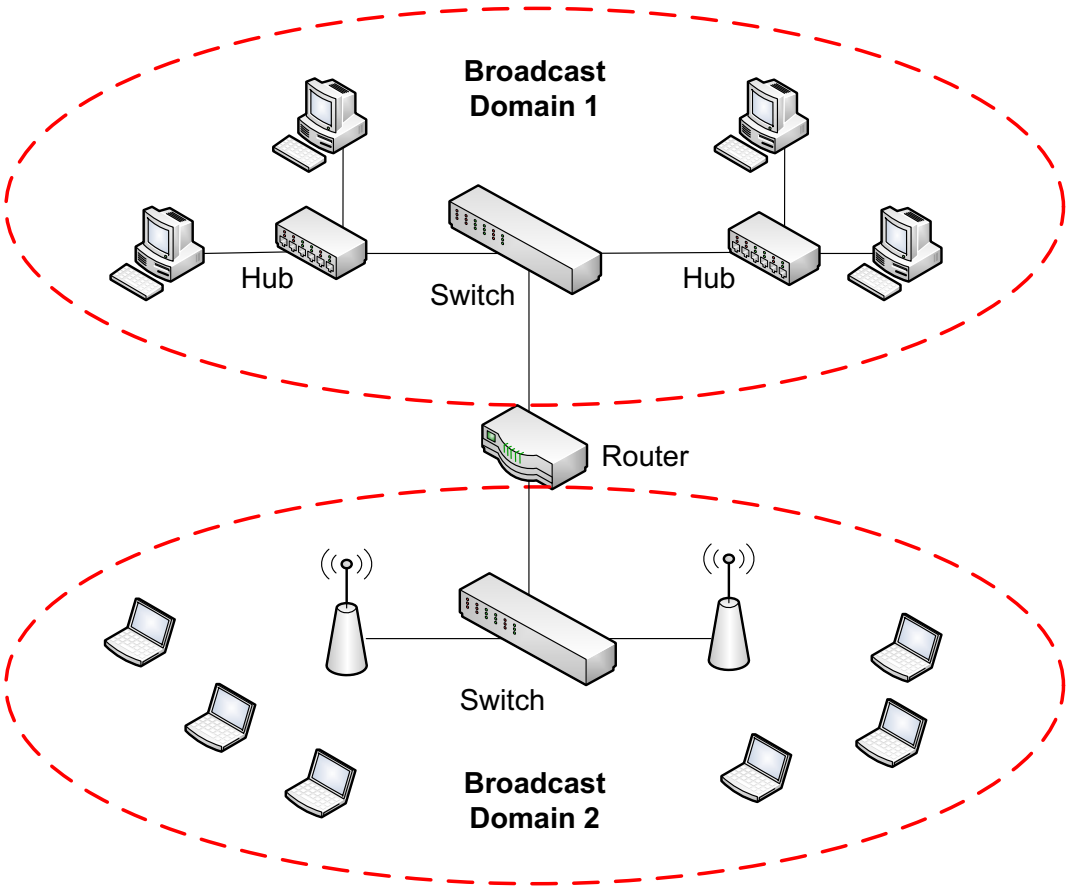
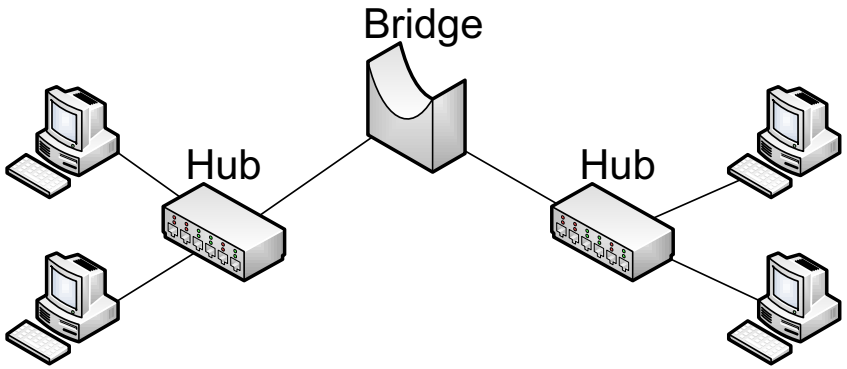
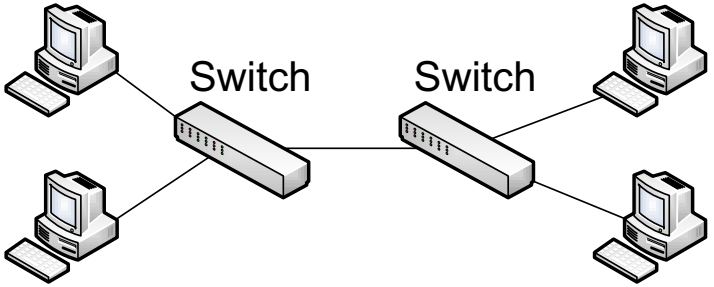
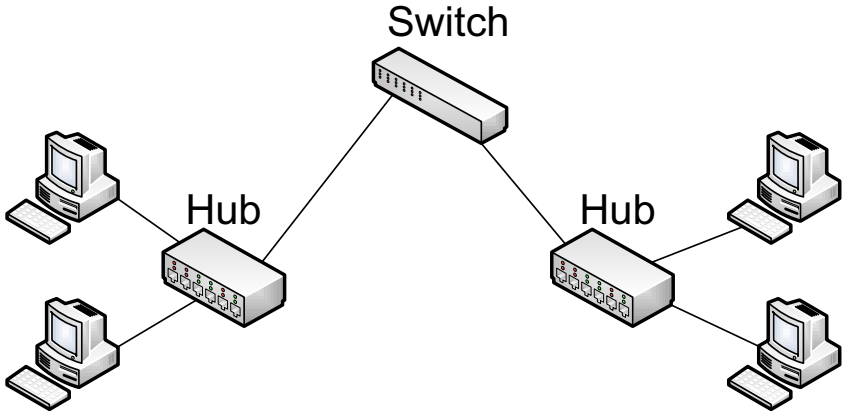


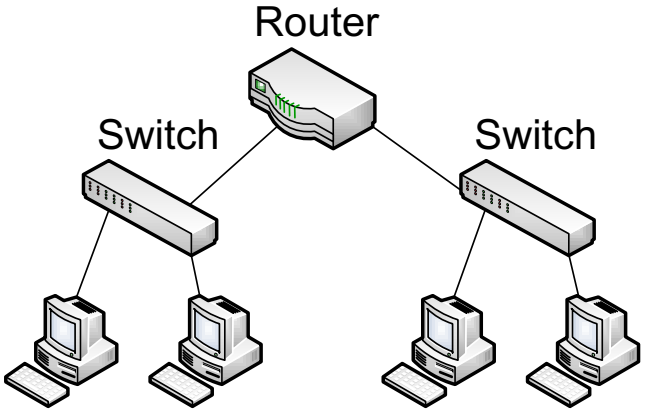
Figure 3.24
Two broadcast domains

3.10 Collision vs. Broadcast Domains Exercise









Recap

- Intermediary devices & their operational layers
- Accessing OS of intermediary devices
- General features of switches
- Switch types
- Primary router functions
- Differences between switching and routing
- Address resolution protocol (ARP)
- Collision domains
- Broadcast domains

End
Chapter 3

CECS 303 Networks and Networks Security

ETHERNET LAN
Chapter 7

Jose Tamayo, M.S.
Computer Engineering & Computer Science
California State University, Long Beach

7.2 ETHERNET Layers

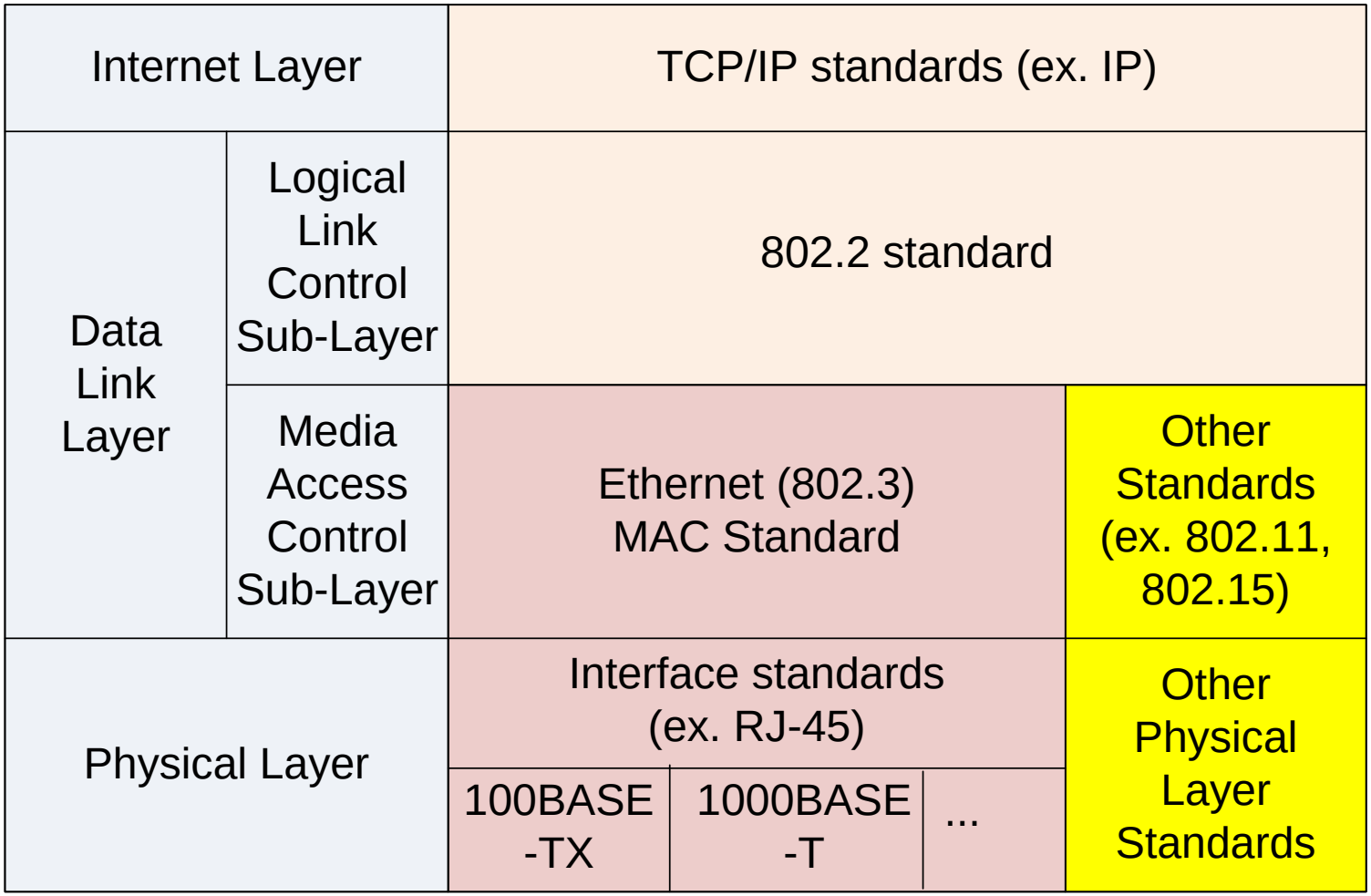


Figure 7.1 Layers of Ethernet (IEEE802.3) standard

7.3 ETHERNET Frame

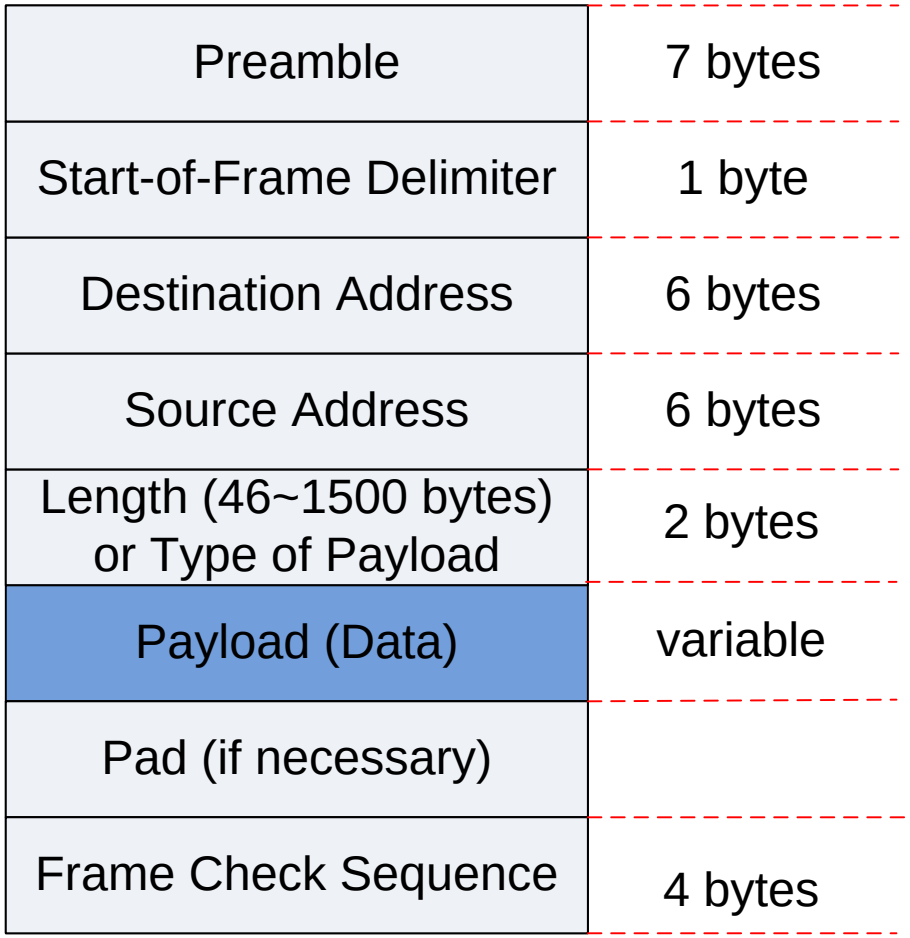


Figure 7.2 Ethernet frame

7.4 Ethernet LAN Design

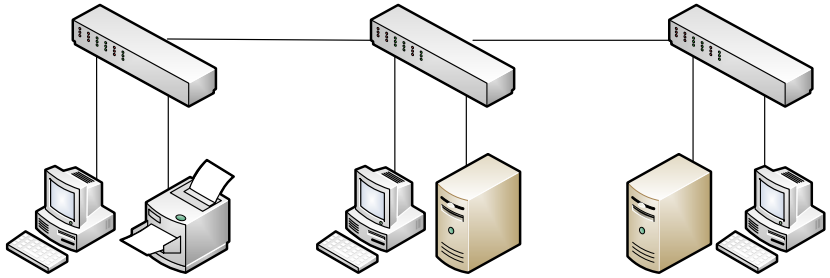


Figure 7.3 Ethernet with flat structure (logical view)

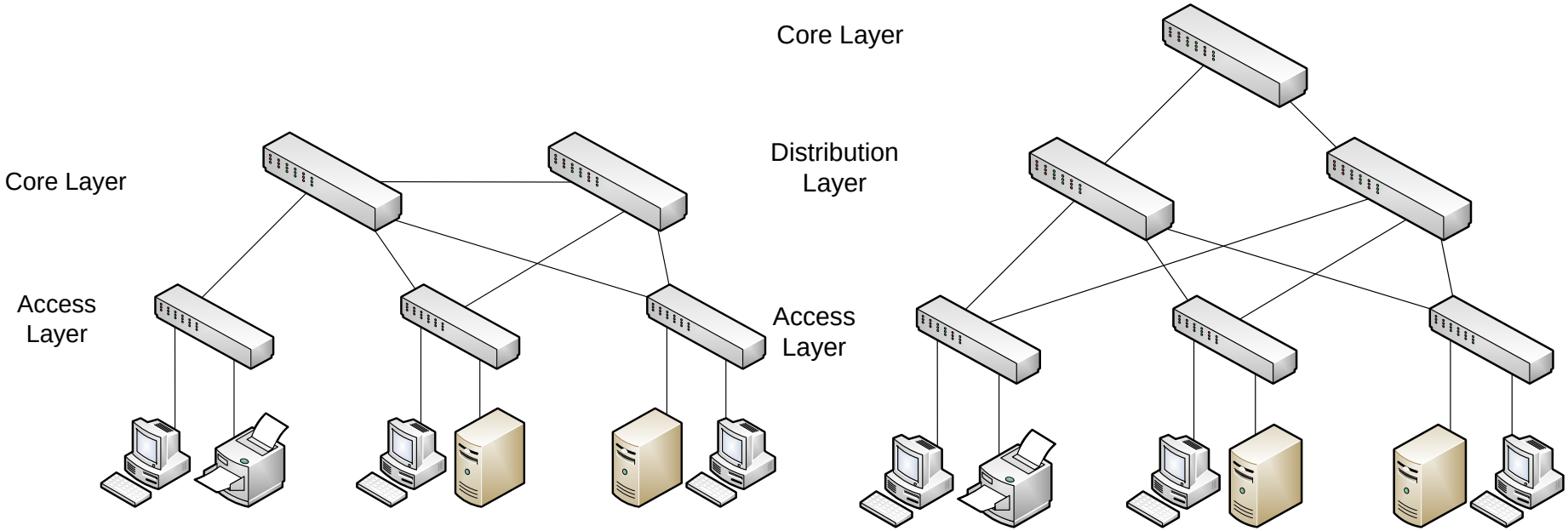


Figure 7.4 Two-tier vs. three-tier Ethernet LANs (logical view)

7.5 Spanning Tree Protocol (STP)

Link Redundancy

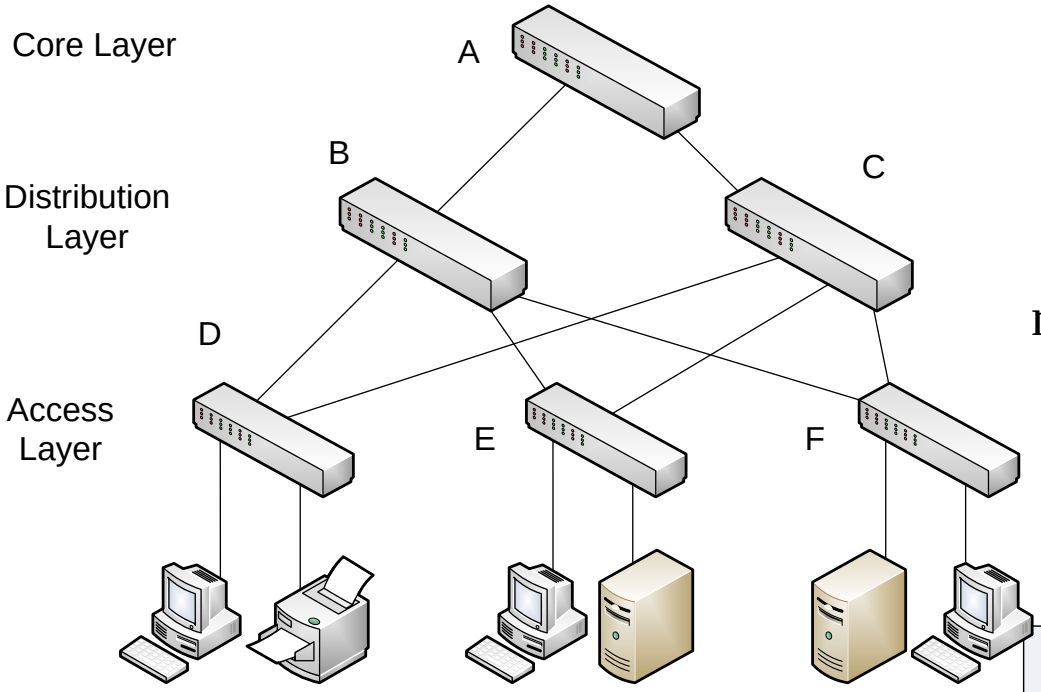


Figure 7.5 Availability of redundant paths (logical view)

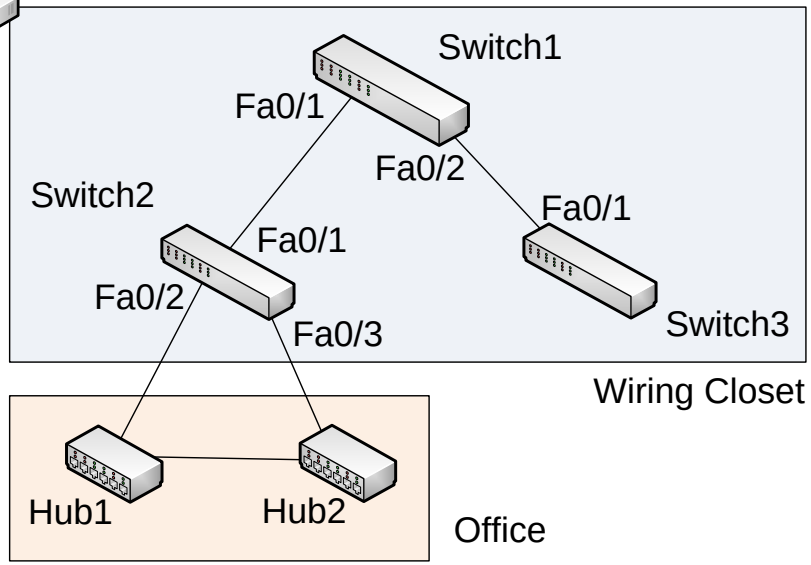


Figure 7.6 Network redundancy created at a work area

7.5 Spanning Tree Protocol (STP)

7.5.2 Protocols and Mechanism

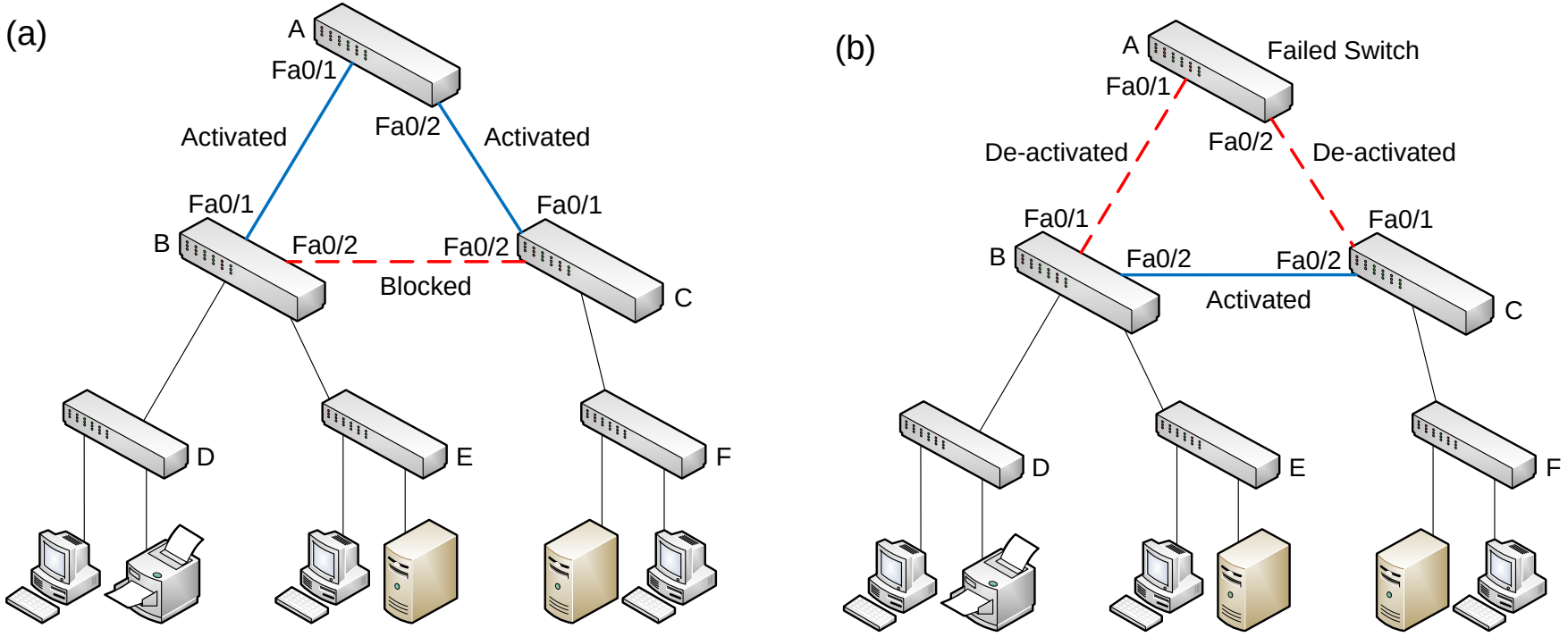


Figure 7.7 Demonstration of STP/RSTP (logical view)

7.5 Spanning Tree Protocol (STP)

- Blocking mode
- Forwarding mode
- Bridge Protocol Data Unit (BPDU) : Frames that contain information about spanning or rapid spanning tree protocol
  - By default, BPDUs are exchanged every 2 seconds

7.6 Link Aggregation

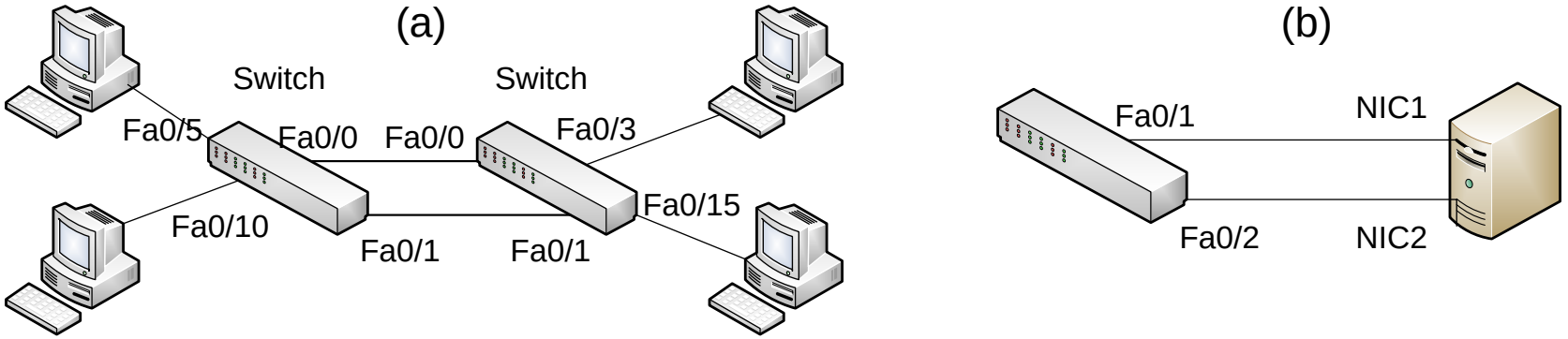


Figure 7.8 Usage of link aggregation

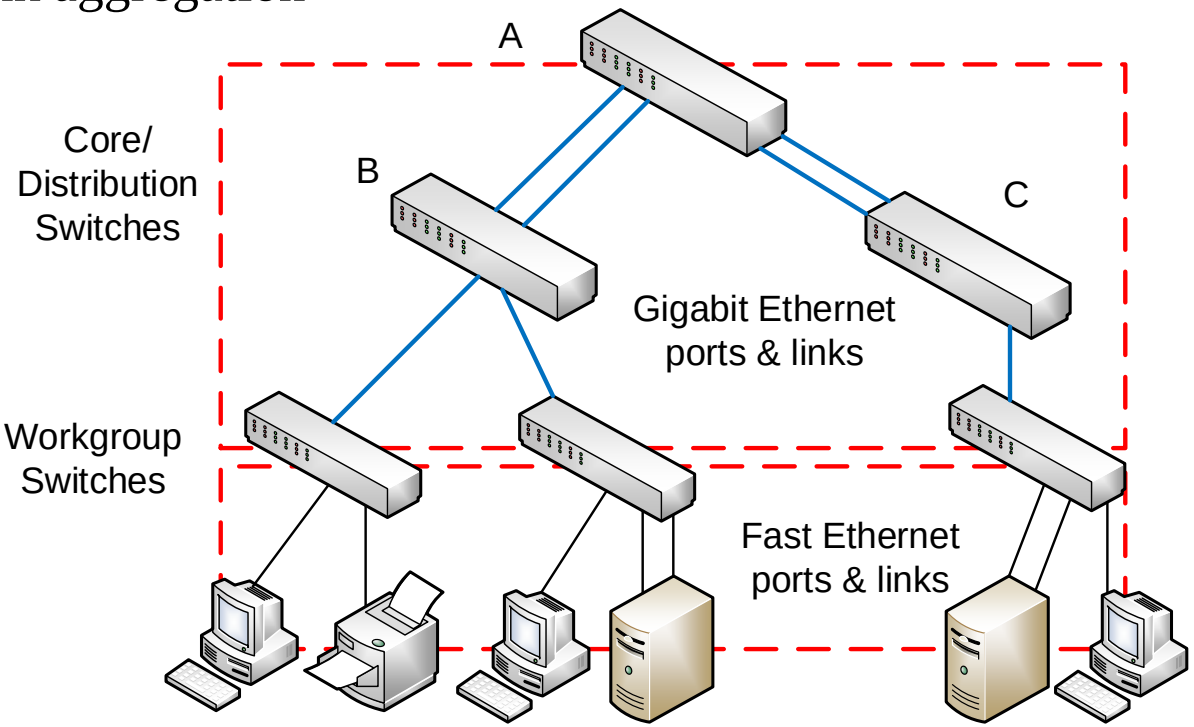


Figure 7.9
Link aggregation scenario

7.6 Link Aggregation

- *Link Aggregation Control Protocol* (LACP): IEEE Standard
- LACP supports bonding of up to 8 ports
- Industry products may support less than 8
- Example: Cisco products

#lacp (Note: activate LACP protocol)

#add port=1,3 (Note: port 1 and 3 are bonded)

7.7 Virtual LANS (VLANS)

7.7.1 Background: Without VLANs

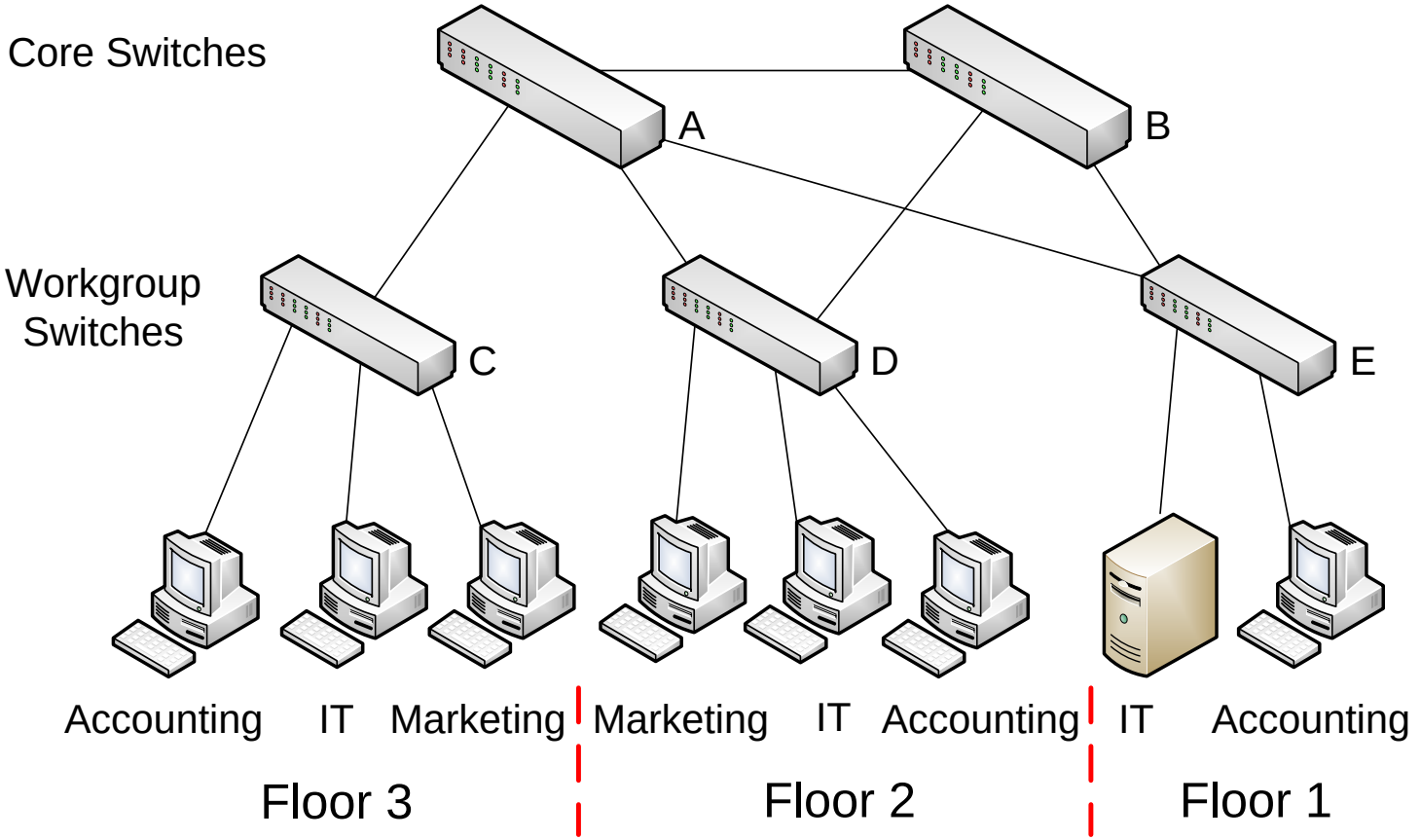


Figure 7.11 Logical layout of a LAN

7.7 Virtual LANS (VLANS)

7.7.1 Background: Without VLANs

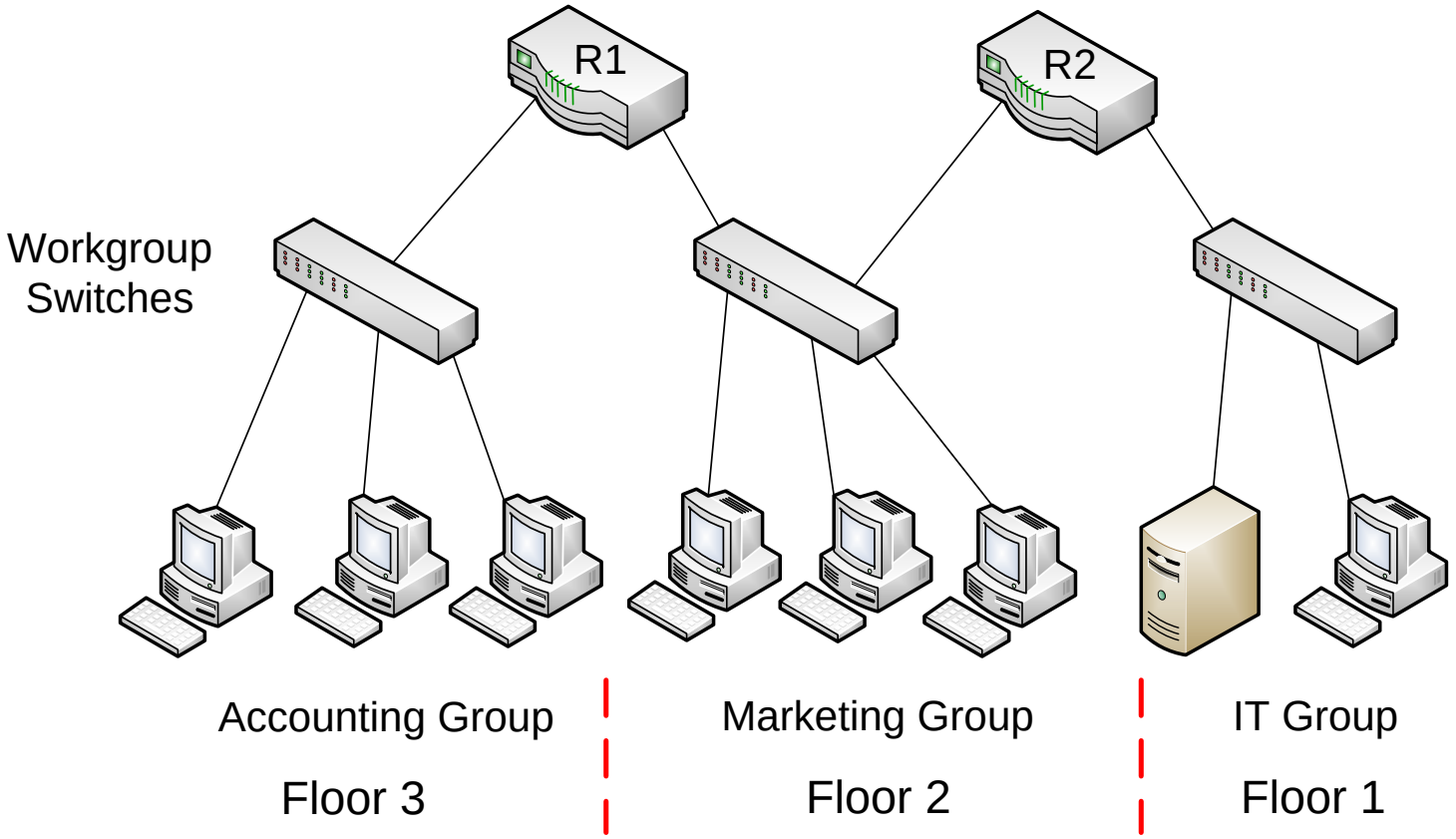


Figure 7.12 Router-based segmentation of a LAN

7.7 Virtual LANS (VLANS)

7.7.2 VLAN Concept

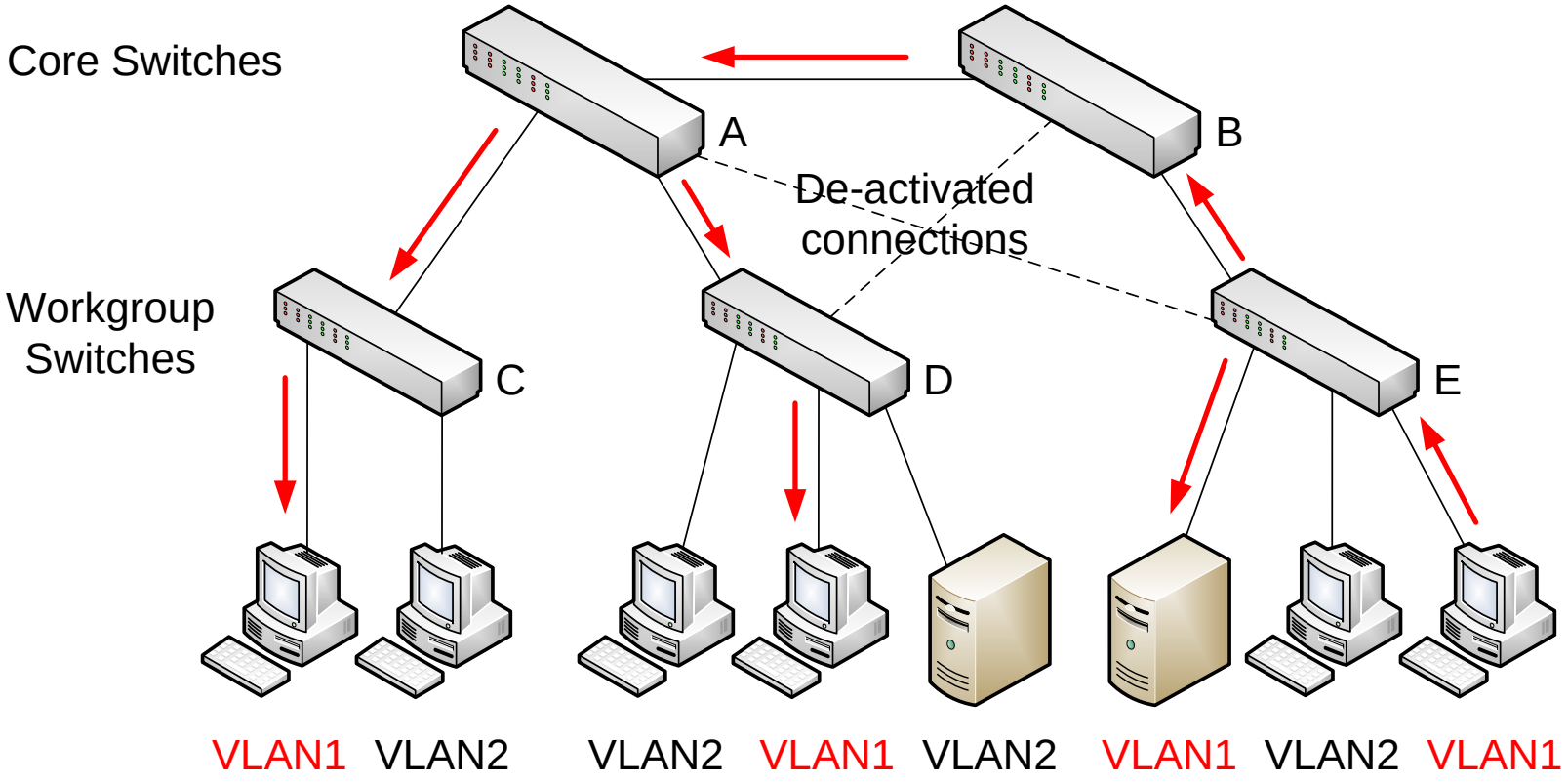


Figure 7.13 Broadcasting to nodes of a VLAN

7.8.1 Without VLANs

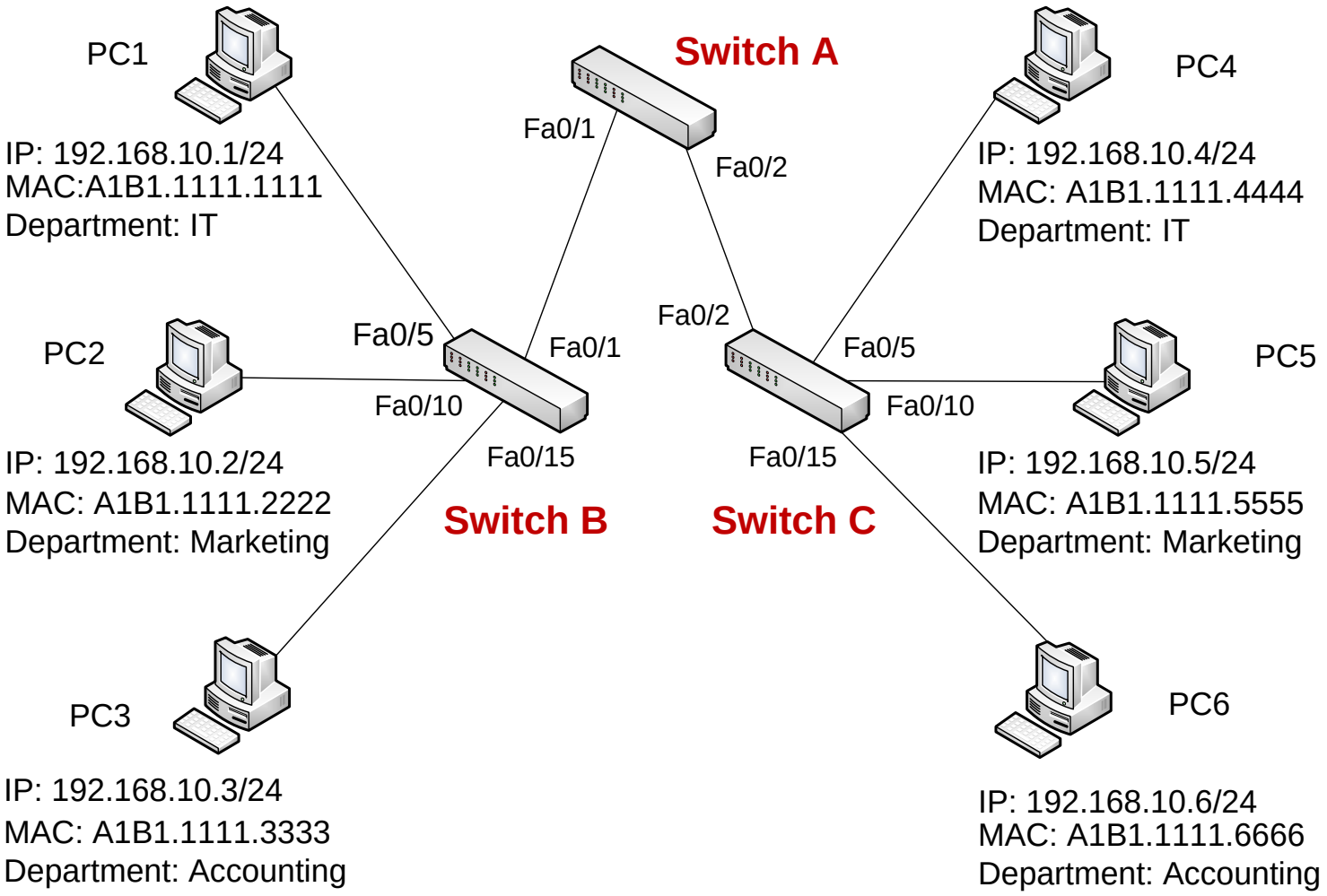
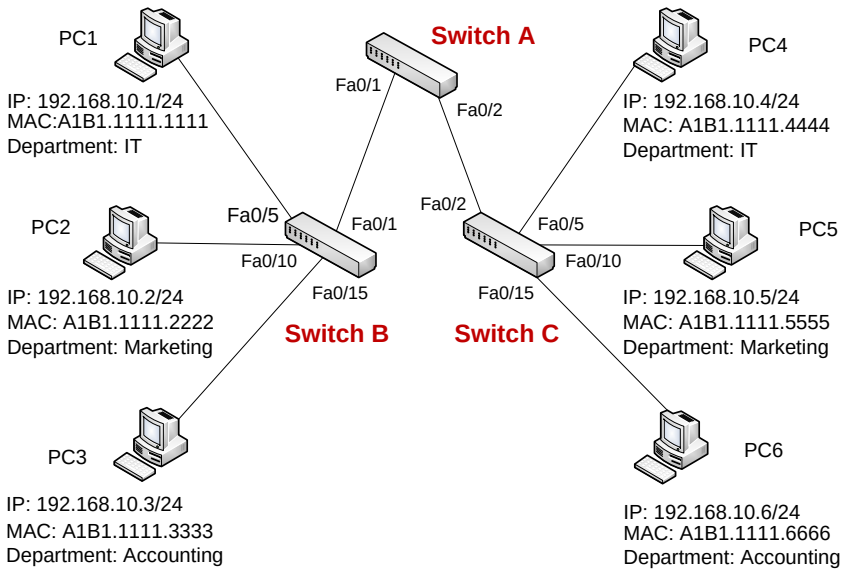


Figure 7.14 A hypothetical switched LAN

7.8.1 Without VLANs



VLANs are created on switches, not host nodes

MAC Address	Exit Port	VLAN ID
A1B1.1111.1111	FastEthernet 0/5	1
A1B1.1111.2222	FastEthernet 0/10	1
A1B1.1111.3333	FastEthernet 0/15	1
A1B1.1111.4444	FastEthernet 0/1	1
A1B1.1111.5555	FastEthernet 0/1	1
A1B1.1111.6666	FastEthernet 0/1	1

Table 7.1 Switch B's switch table with default VLAN

7.8.2 With VLANs

(1) Define VLANs on Switches

Example: Defining 3 VLANs on a Cisco switch

#vlan 10
#name IT
#vlan 20
#name Marketing
#vlan 30
#name Accounting

---

(2) Plan the range of trunk and access ports

Port Type	Port Ranges	VLAN IDs	VLAN Names
Trunk ports	Fa0/1 ~ Fa0/3		
	Fa0/4 ~ Fa0/8	VLAN 10	IT
Access ports	Fa0/9 ~ Fa0/14	VLAN 20	Marketing
	Fa0/15 ~ Fa0/24	VLAN 30	Accounting

Table 7.2 Sample assignment of switch ports to VLANs

7.8.2 With VLANs

(3) Assign access ports to VLANs: Cisco Example

Assigning an access port (Fa0/5) to VLAN 10 takes three commands entered successively into switch's operating system.

# *interface* Fa0/5	Note: Fa0/5 is to be configured
# *switchport mode* access	Note: Fa0/5 is an access port
# *switchport* access vlan 10	Note: assign Fa0/5 to VLAN 10

Setting up a switch port (Fa0/1) as a trunk port takes three commands entered in succession into switch's operating system.

# *interface* Fa0/1	Note: Fa0/1 is to be configured
# *switchport trunk encapsulation dot1q*	
	Note: Use 802.1Q (tagging protocol)
# *switchport mode* trunk	Note: Fa0/1 is a trunk port

7.8.3 How VLANs Work

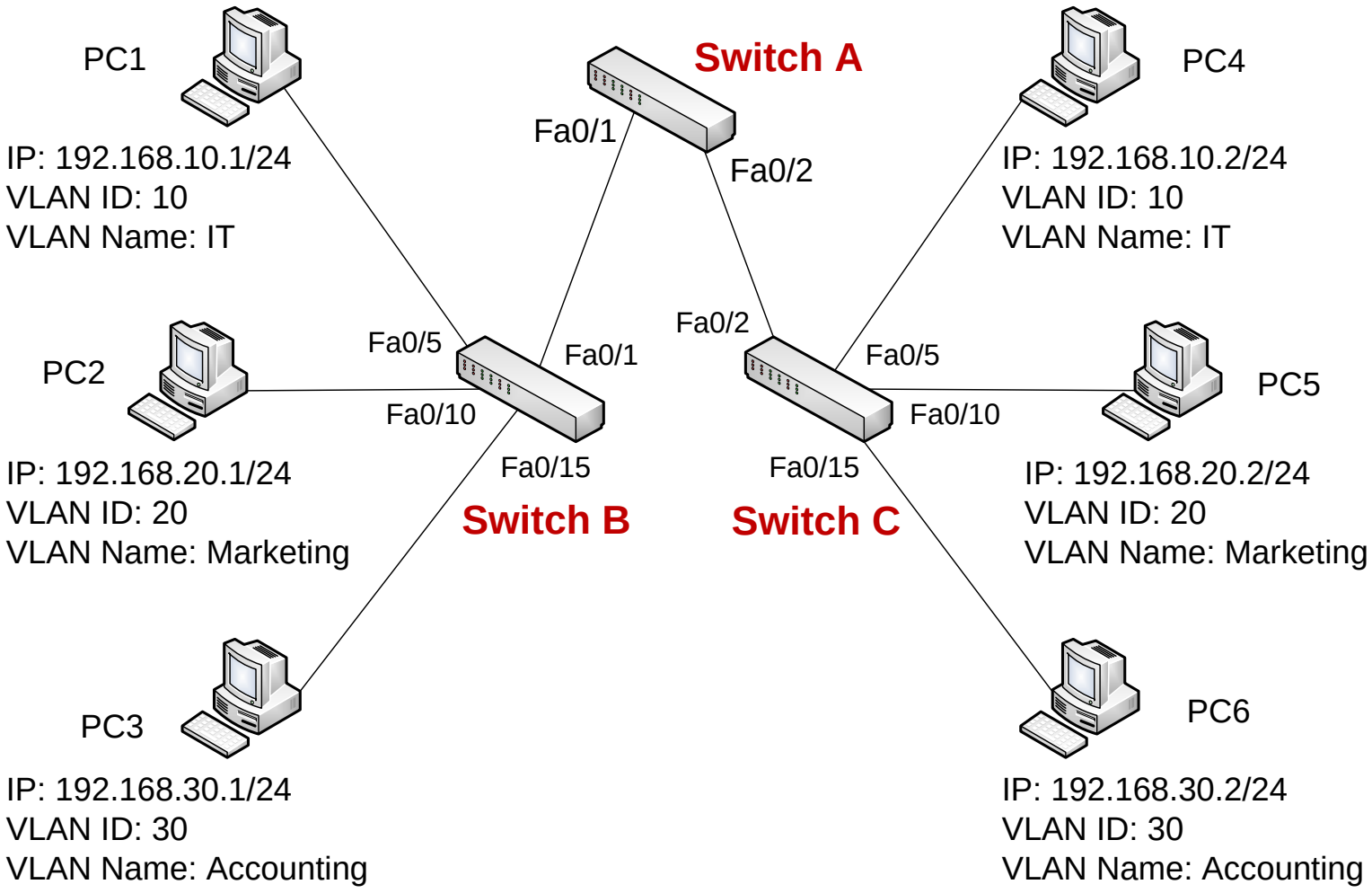
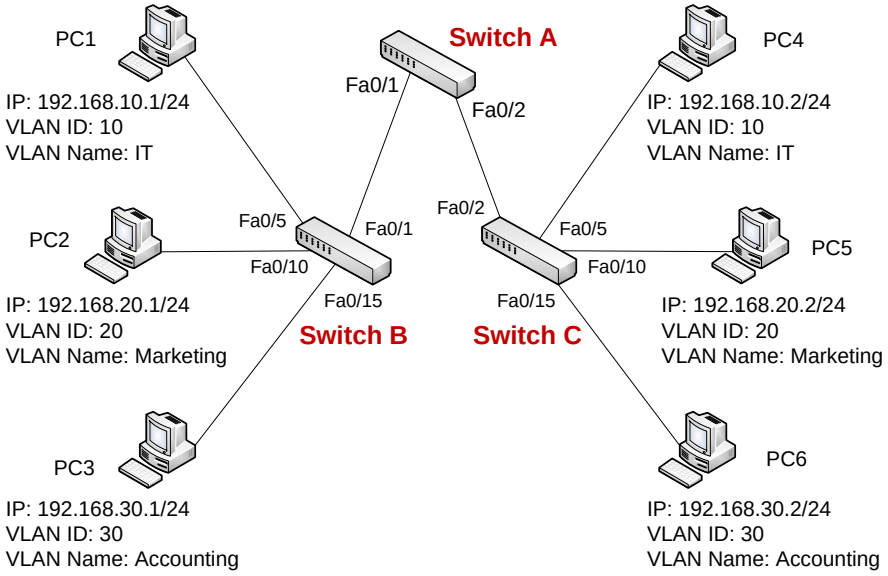


Figure 7.15 A switched LAN with three VLANs

7.8.3 How VLANs Work



MAC Address	Exit Port	VLAN ID
A1B1.1111.1111	FastEthernet 0/5	10
A1B1.1111.2222	FastEthernet 0/10	20
A1B1.1111.3333	FastEthernet 0/15	30
A1B1.1111.4444	FastEthernet 0/1	10
A1B1.1111.5555	FastEthernet 0/1	20
A1B1.1111.6666	FastEthernet 0/1	30

Table 7.3 Switch B's Switch table with three VLANs

7.8 VLAN Scenarios: With VLANs

7.8.4 VLAN ID vs. Subnet IP Assignment

VLAN ID	VLAN name	Subnet ID
10	IT	192.168.10.0/24
20	Marketing	192.168.20.0/24
30	Accounting	192.168.30.0/24

7.9 VLAN Tagging/Trunking (IEEE 802.1Q)

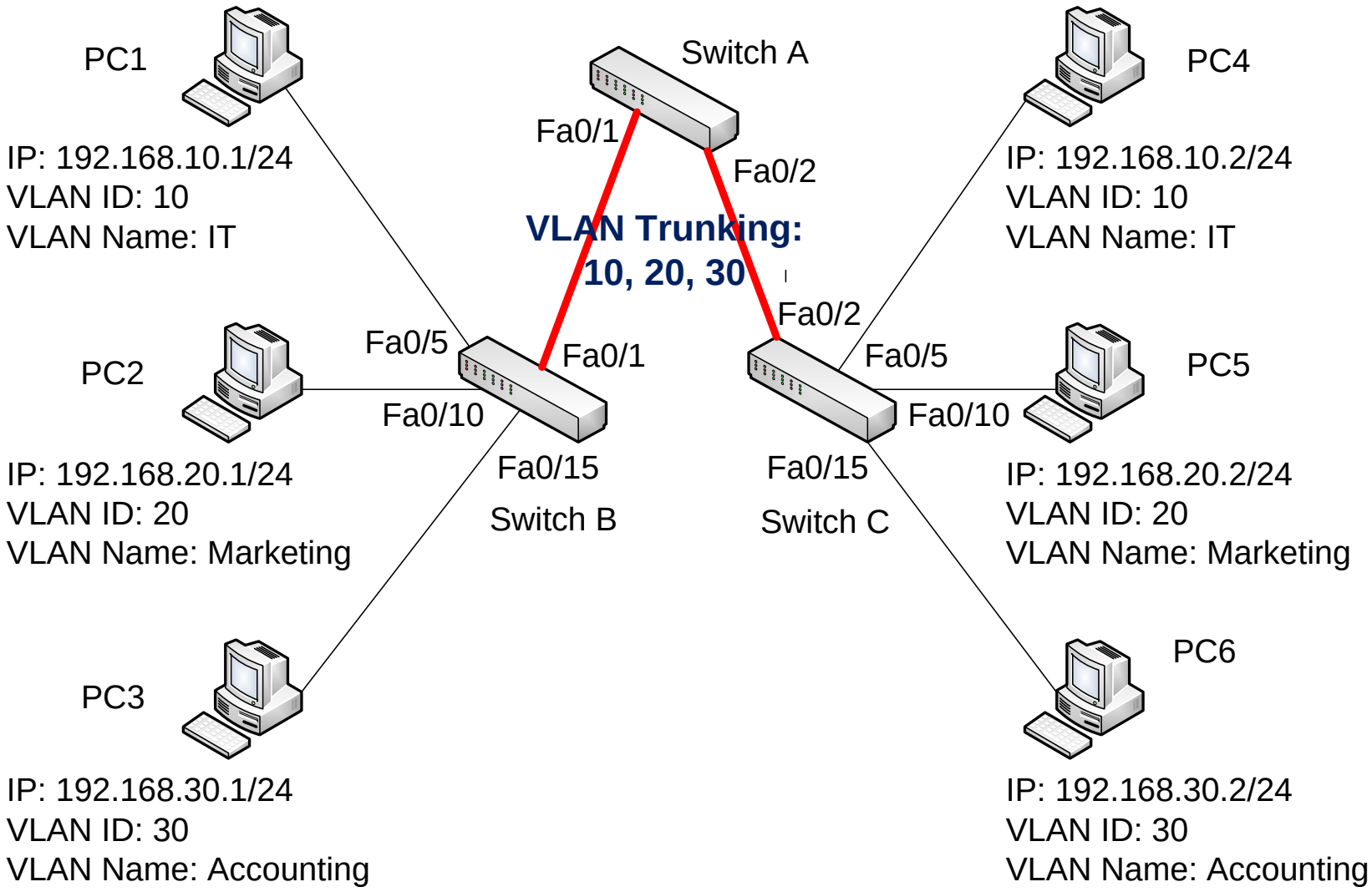


Figure 7.16 VLAN trunking

7.9.2 VLAN Tagging

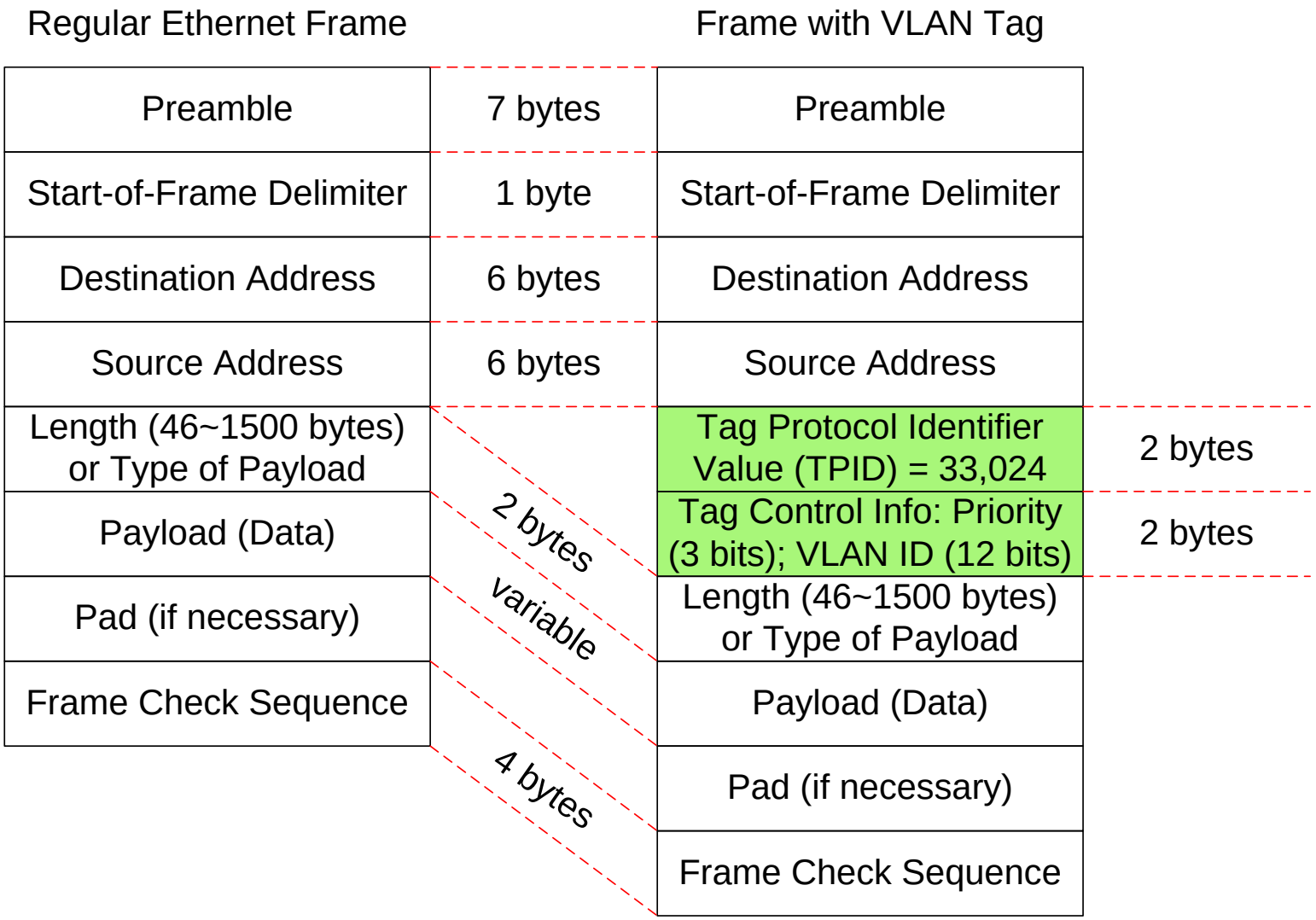


Figure 7.17 Ethernet frames: regular vs. VLAN tagged

7.9.3 VLAN Tagging/Untagging Process

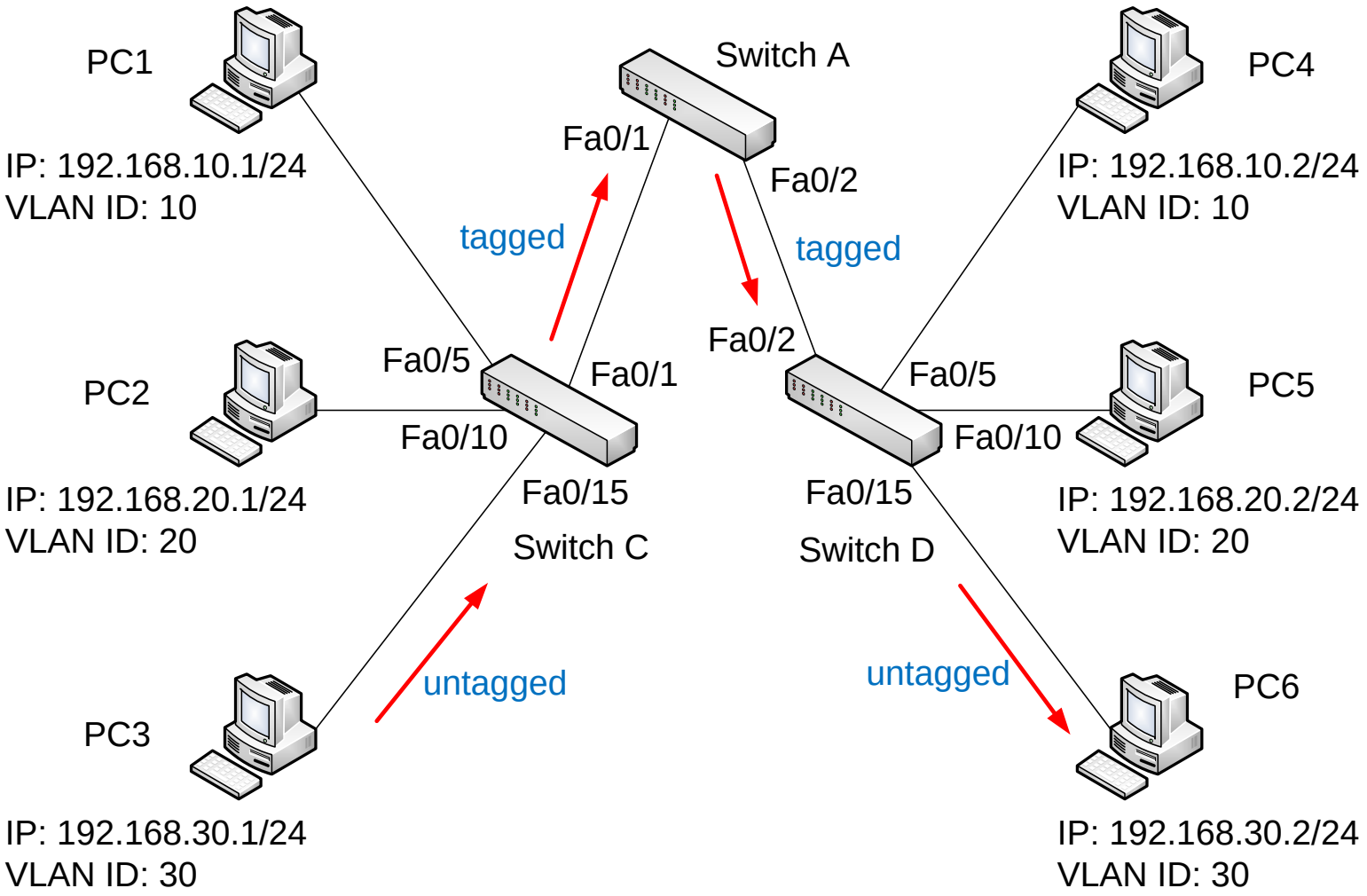


Figure 7.18 VLAN tagging and untagging

7.10 VLAN Types

Default VLAN

SwitchB#**show vlan**

VLAN	Name	Status	Ports
1	default	active	Fa0/1, Fa0/2, Fa0/3, Fa0/4, Fa0/5 Fa0/6, Fa0/7, Fa0/8, Fa0/9, Fa0/10 Fa0/11, Fa0/12, Fa0/13, Fa0/14, Fa0/15 Fa0/16, Fa0/17, Fa0/18, Fa0/19, Fa0/20 Fa0/21, Fa0/22, Fa0/23, Fa0/24

Figure 7.19 Default VLAN

7.10 VLAN Types

Data VLAN

SwitchB#**show vlan**

VLAN	Name	Status	Ports
10	IT	active	Fa0/4, Fa0/5, Fa0/6, Fa0/7, Fa0/8
20	Marketing	active	Fa0/9, Fa0/10, Fa0/11, Fa0/12, Fa0/13, Fa0/14
30	Accounting	active	Fa0/15, Fa0/16, Fa0/17, Fa0/18, Fa0/19, Fa0/20, Fa0/21, Fa0/22, Fa0/23, Fa0/24

Figure 7.20 Data VLANs

7.10 VLAN Types

Voice VLAN

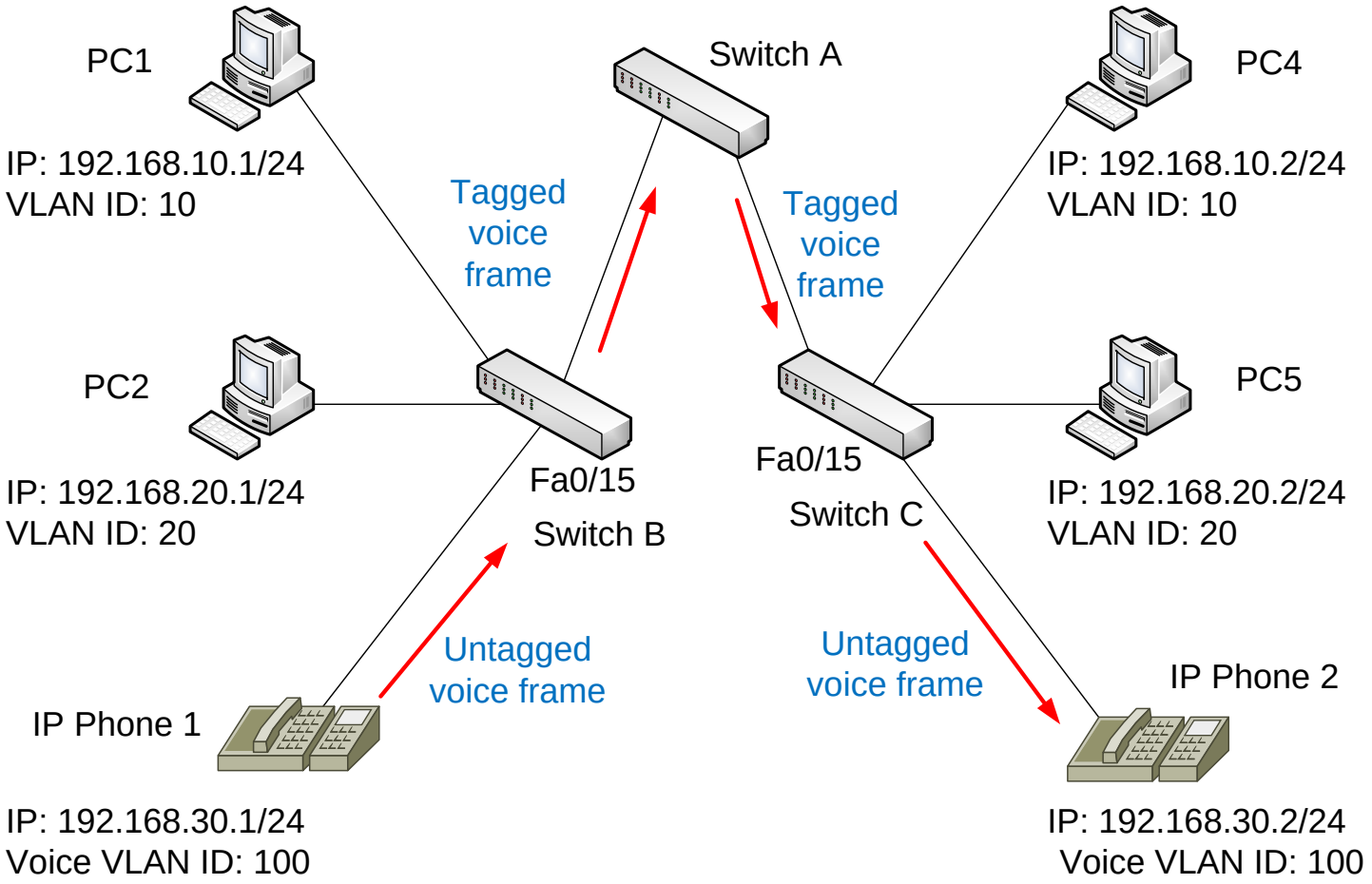
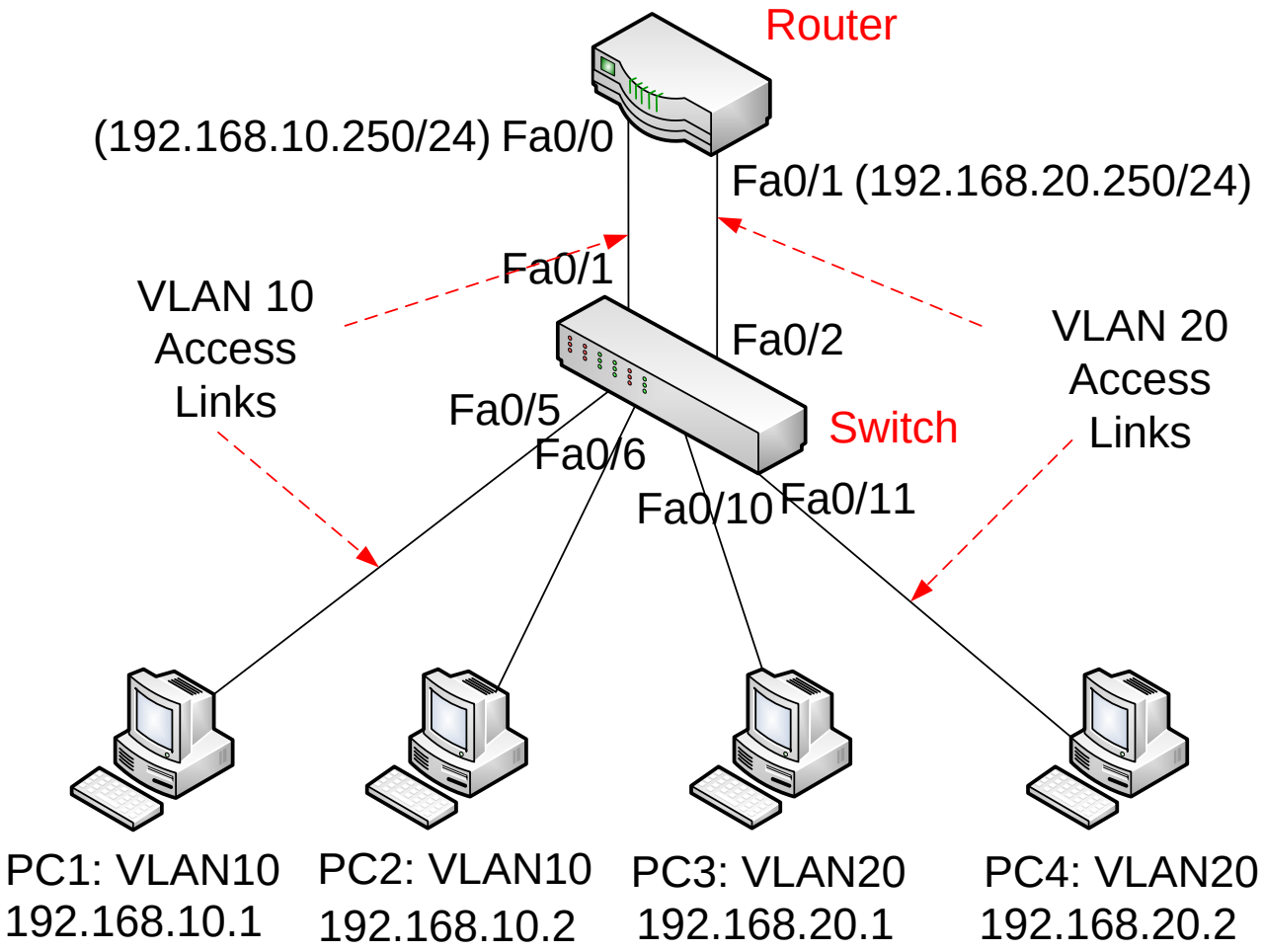


Figure 7.21 Demonstration of Voice VLAN

7.11 Inter-VLAN Routing

7.11.1 A Router Interface Per VLAN: Scenario 1

Figure 7.23
Assignment of a router port per VLAN



7.11 Inter-VLAN Routing

Sub-interfaces

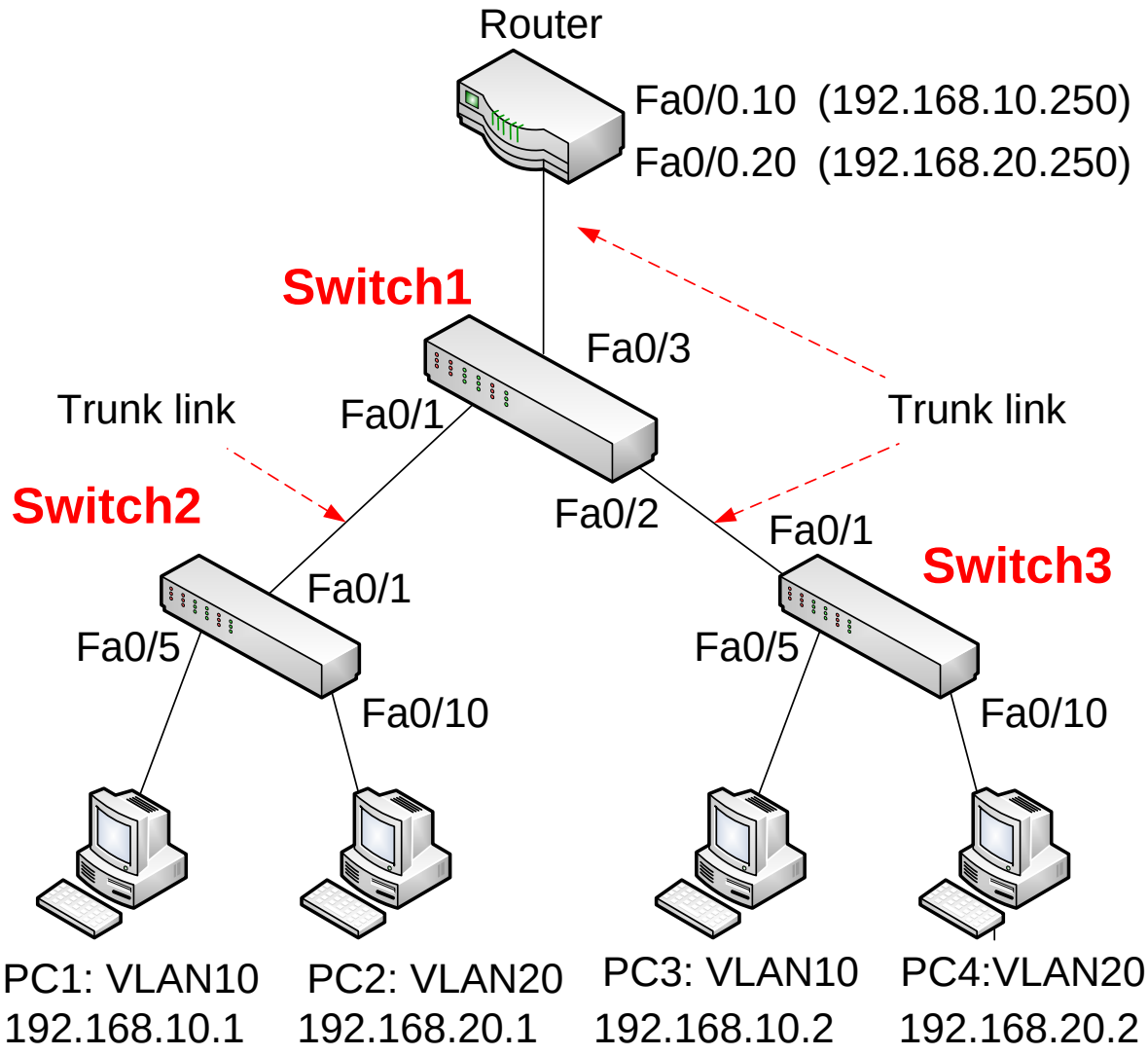


Figure 7.25
Inter-VLAN routing with sub-interfaces

7.11 Inter-VLAN Routing

7.11.2 Sub-Interfaces/Ports (Advanced)

Physical interface	Virtual interfaces (Sub-interfaces)	VLAN ID	IP address
Fa0/0	Fa0/0.10 Fa0/0.20	10 20	192.168.10.250 192.168.20.250

Table 7.5 Relationships between physical interface, virtual interfaces, VLAN IDs, and IP addresses (This is not a routing table.)

7.11 Inter-VLAN Routing

Sub-interfaces

Subnet ID	Subnet Mask	Exit port (Sub-Interface)
192.168.10.0	255.255.255.0	Fast Ethernet0/0.10
192.168.20.0	255.255.255.0	Fast Ethernet0/0.20

Table 7.6 Routing table entries with sub-interfaces (a simplified view)

Recap

- Layers of Ethernet standard
- Ethernet frame structure
- (Rapid) Spanning Tree Protocol
- Link aggregation
- Virtual LANs (VLANs)
- VLAN tagging
- VLAN types
- Inter-VLAN routing

End
Chapter 7

CECS 303 Networks and Networks Security

DNS and DHCP Support Applications
Chapter 10 SECTION 5

Jose Tamayo, M.S.
Computer Engineering & Computer Science
California State University, Long Beach

10.5 Client-Server Systems

10.5.2 DNS (Domain Name System)

Domain and Name Resolution

- Domain: A boundary within which an organization controls its network resources.
- Name resolution: Domain name ←→ IP address

Domain Hierarchy

- *Top level domains (TLD): generic TLD, country code TLDs*
- Second-level domain: sub-domain
- URL = protocol + domain name

Extra on DNS essentials

https://www.youtube.com/watch?v=4a3MGDAoljI

https://www.youtube.com/playlist?list=PL5DDE6309C9057EEA

10.5.2 DNS (Domain Name System)

DNS Architecture

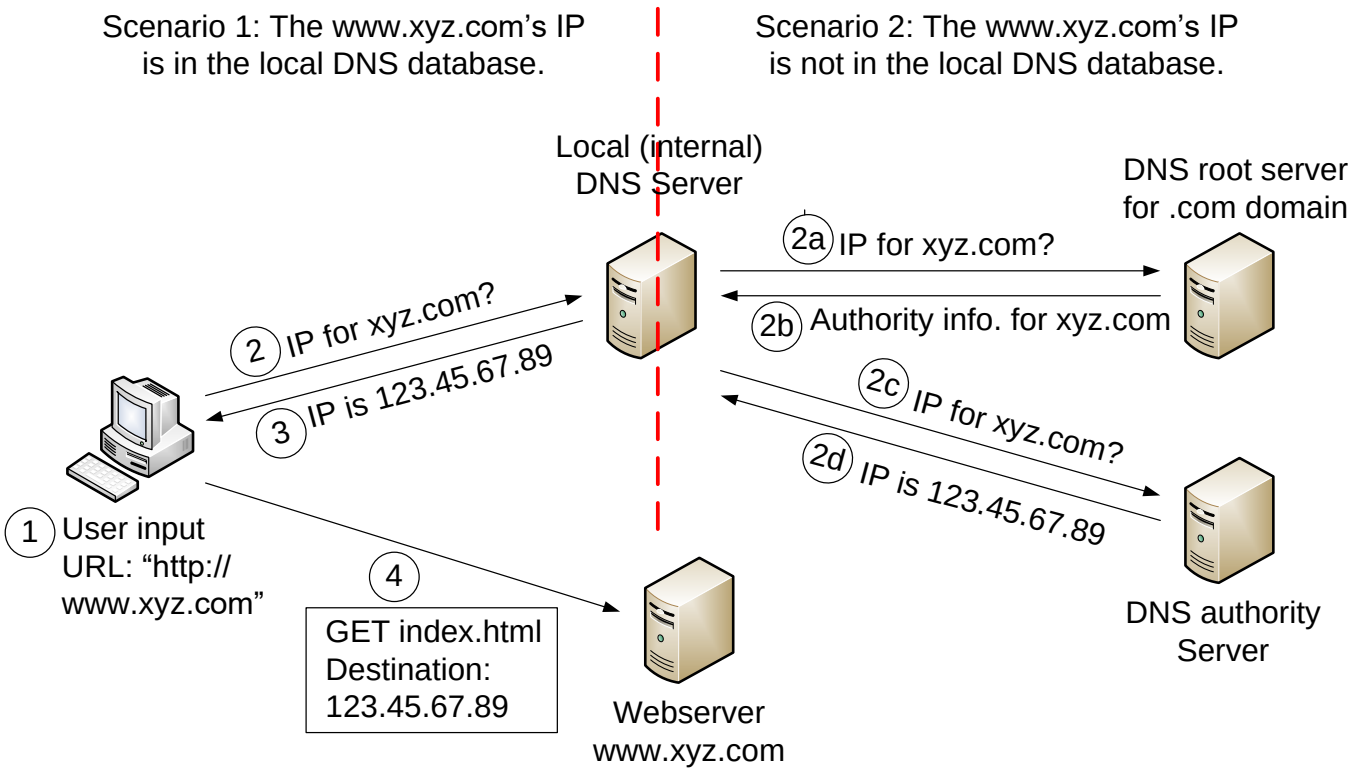


Figure 10.18

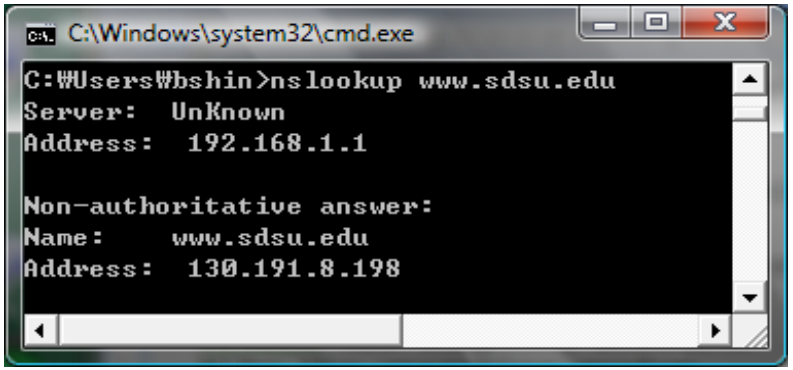


Figure 10.19 Sample *nslookup* inquiry

10.5 Client-Server Model

10.5.3 DHCP (Dynamic Host Configuration Protocol)

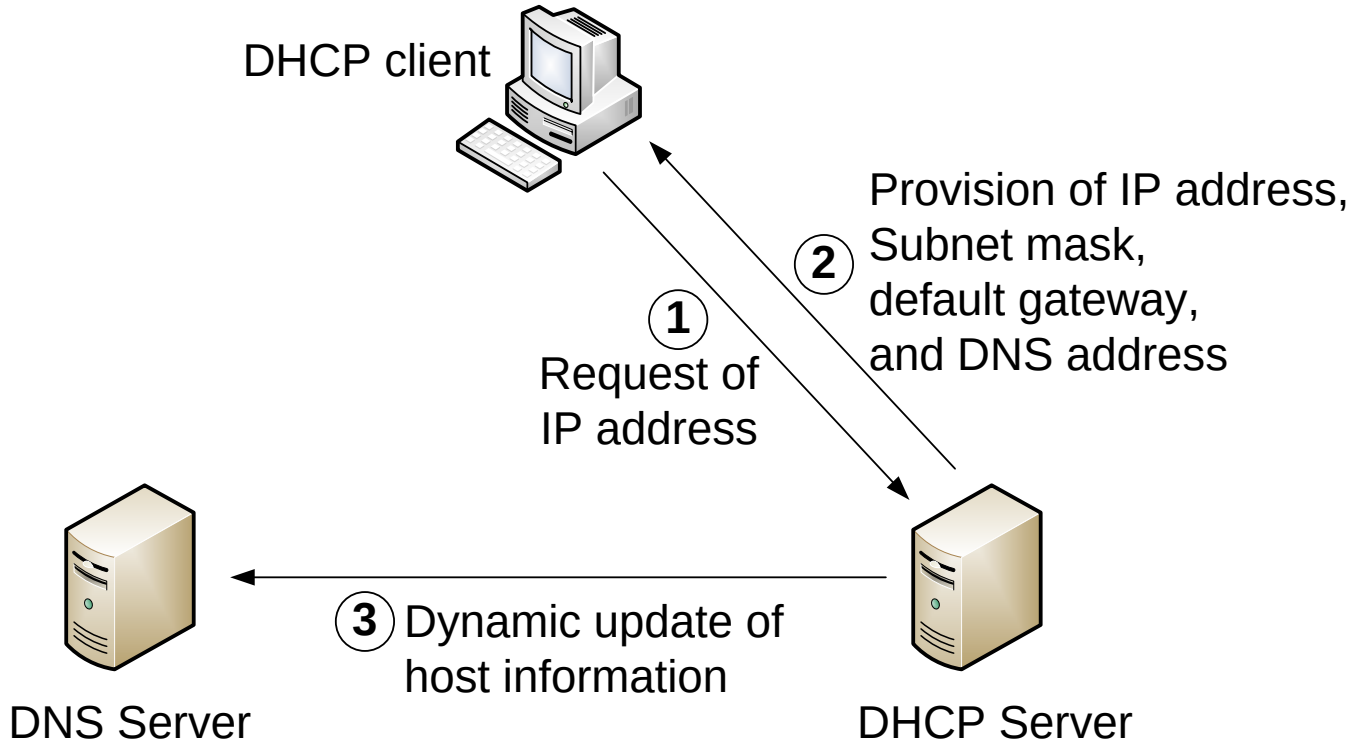


Figure 10.23 DHCP and dynamic IP assignment