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

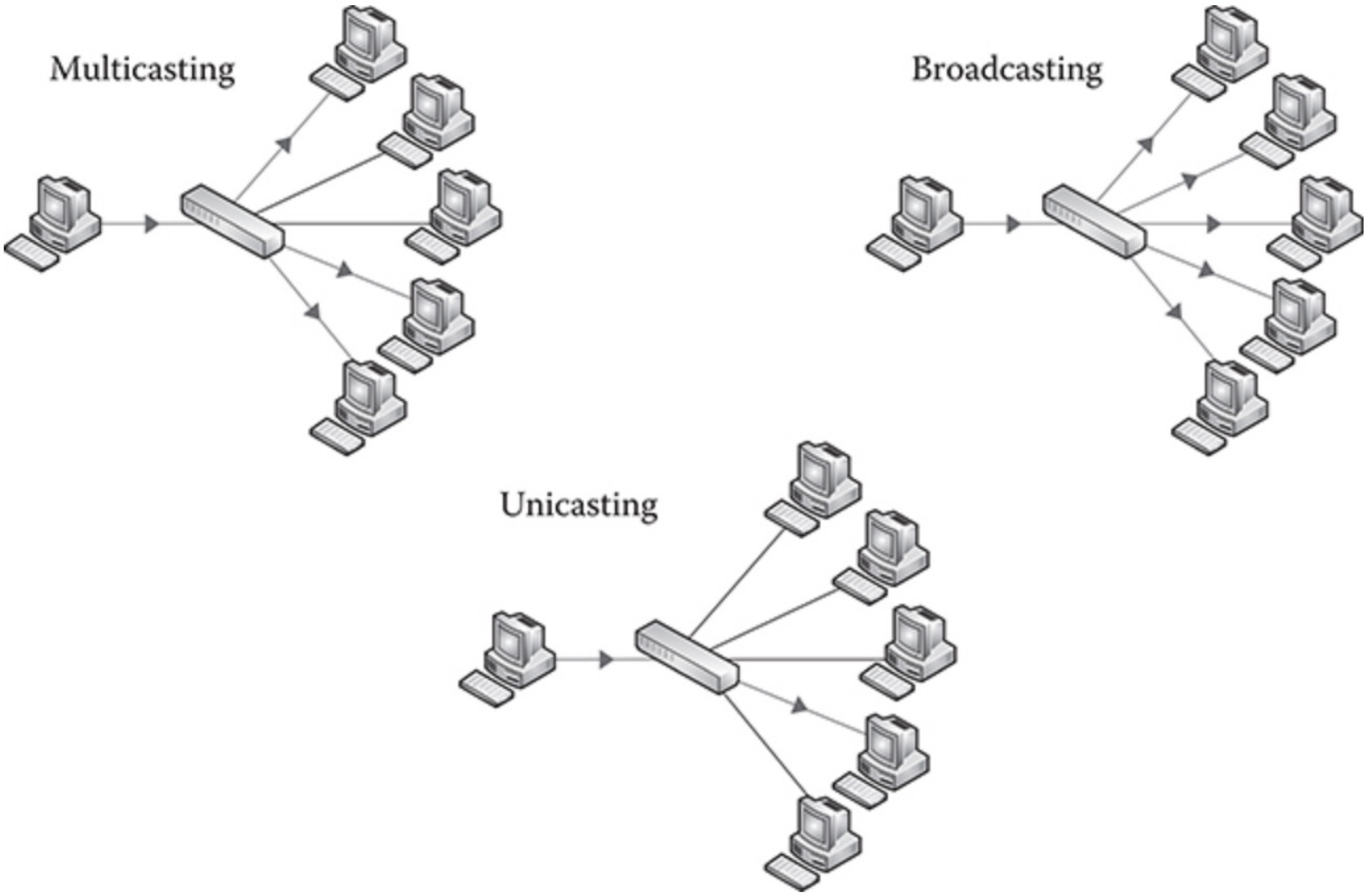


Figure 1.8 Multicasting, broadcasting, and unicasting.

Direction of Data Exchange

- Simplex
- Half-duplex
- Full-duplex

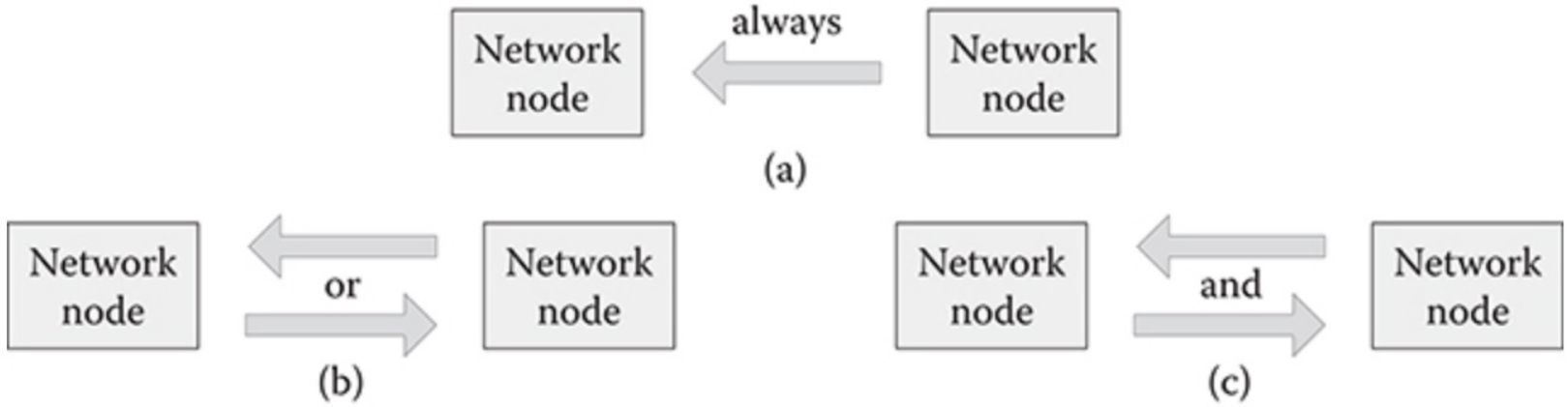


Figure 1.9 (a) Simplex, (b) half-duplex, and (c) full-duplex transmissions.

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

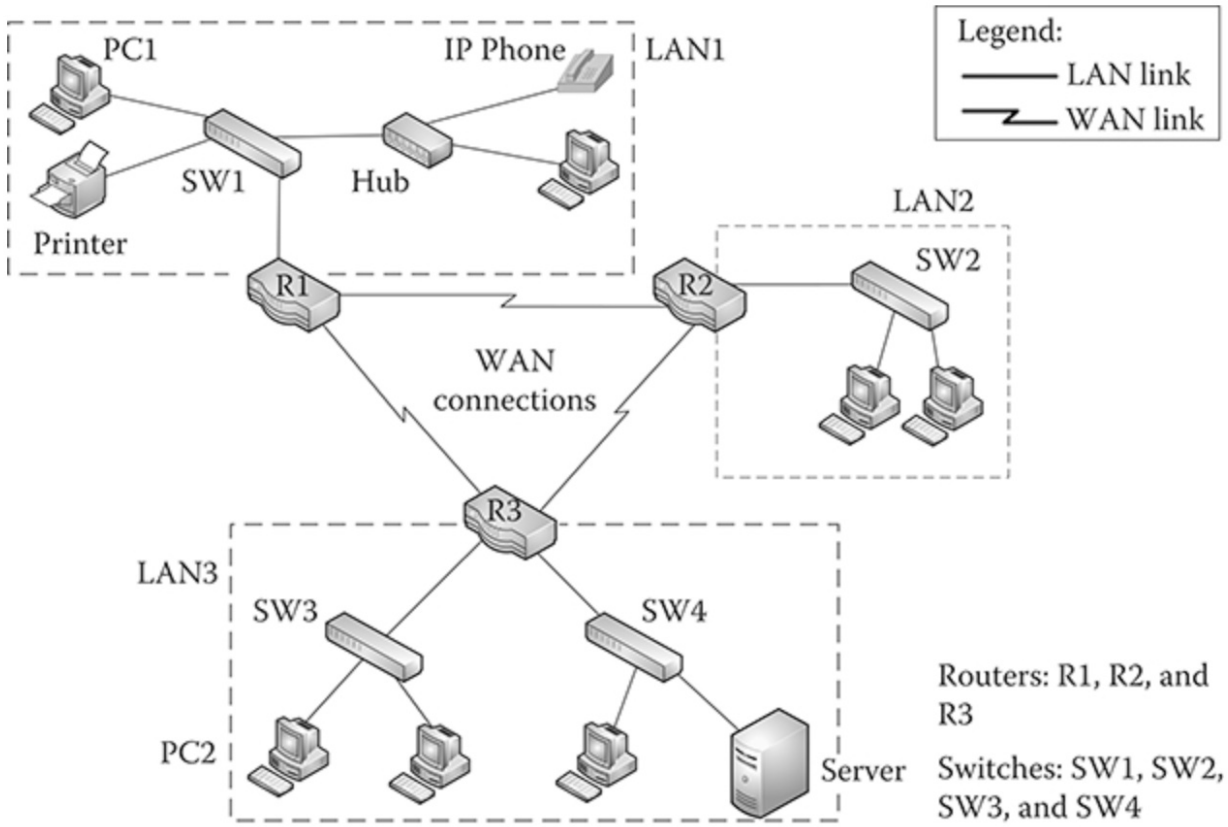


Figure 1.6 A hypothetical enterprise network.

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?

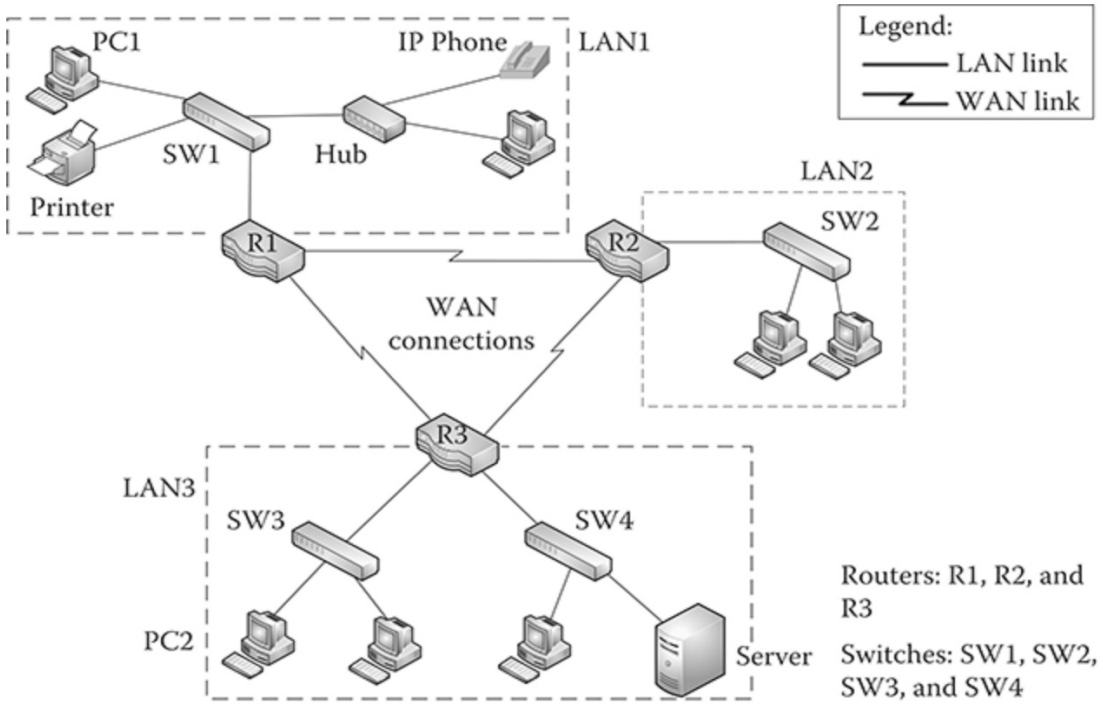


Figure 1.6 A hypothetical enterprise network.

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

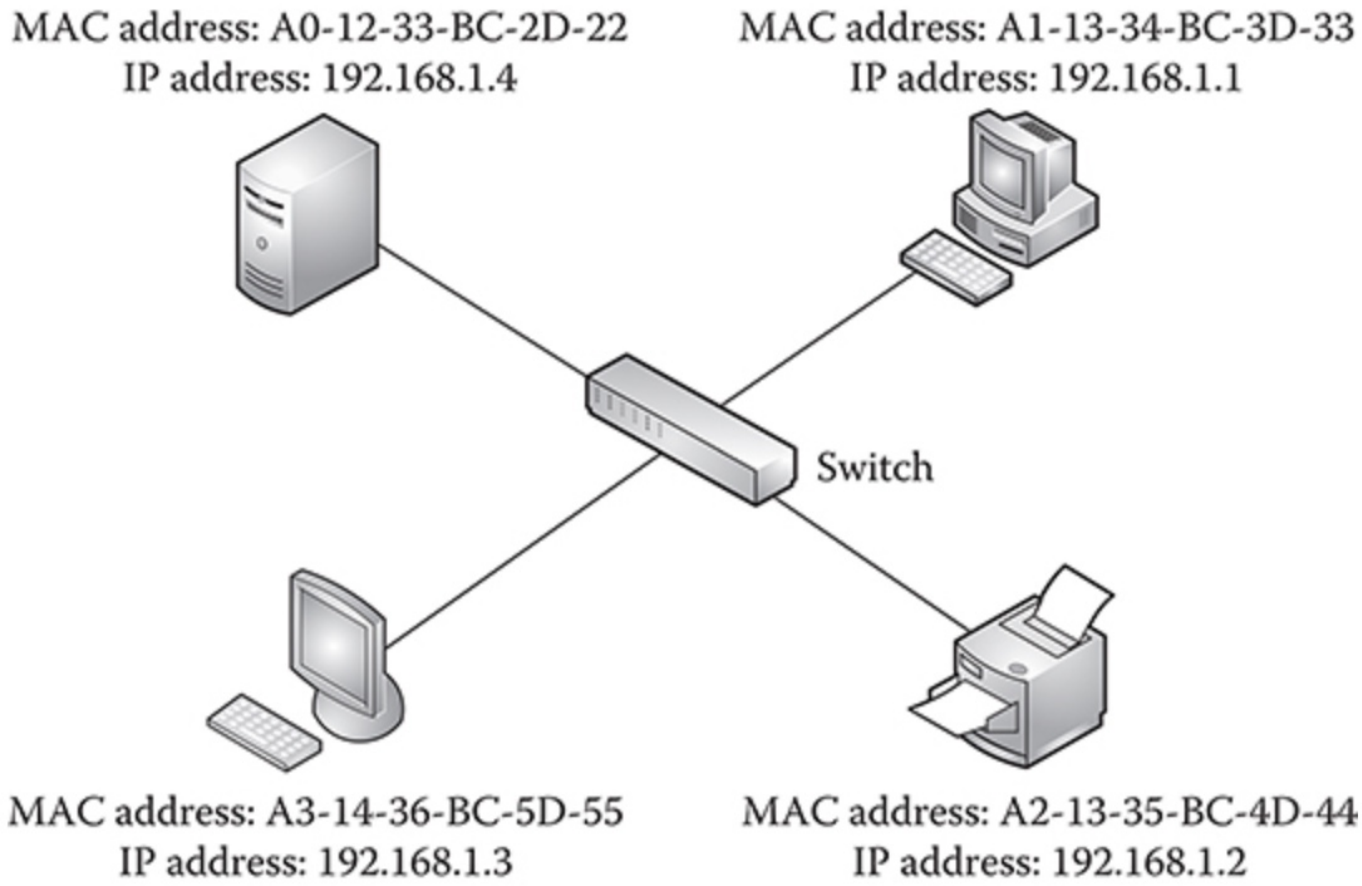
Initial binary combination (8 bits)	0	1	0	1	1	0	1	0
Power of two	2^7	2^6	2^5	2^4	2^3	2^2	2^1	2^0
Decimal position values	128	64	32	16	8	4	2	1
Add decimal values of nonzero binary positions		64		+16	+8		+2	= 90

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

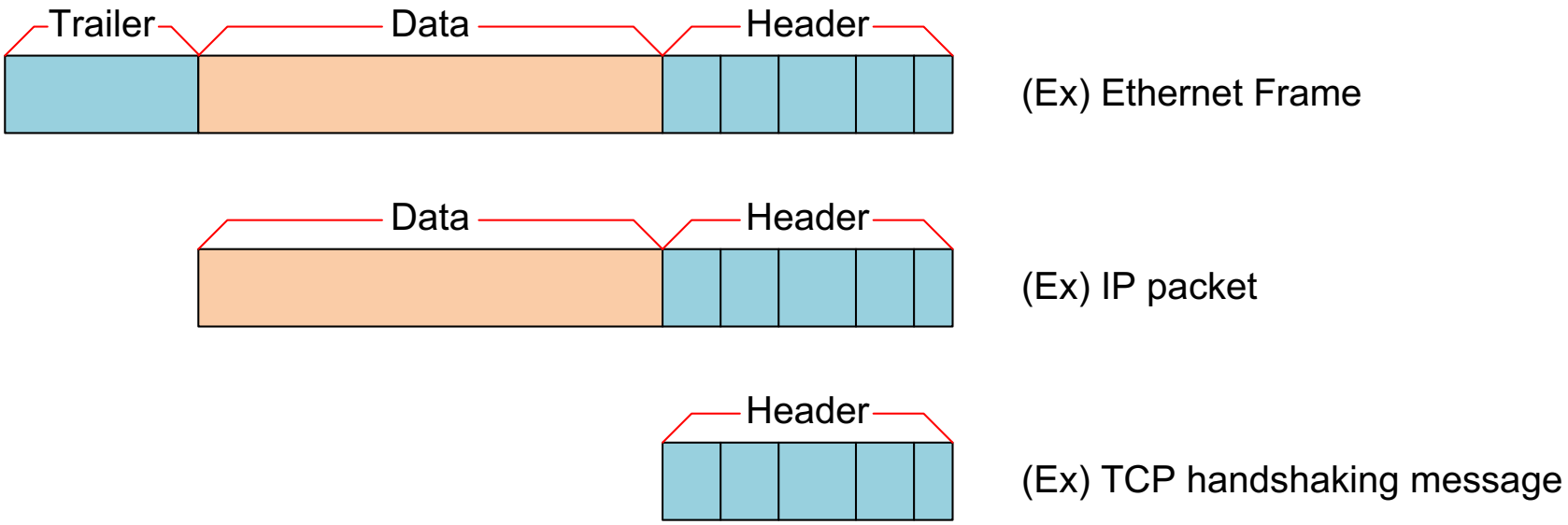


Figure 2.2 Three possible formats of protocol data units

2.3 Layer Functions

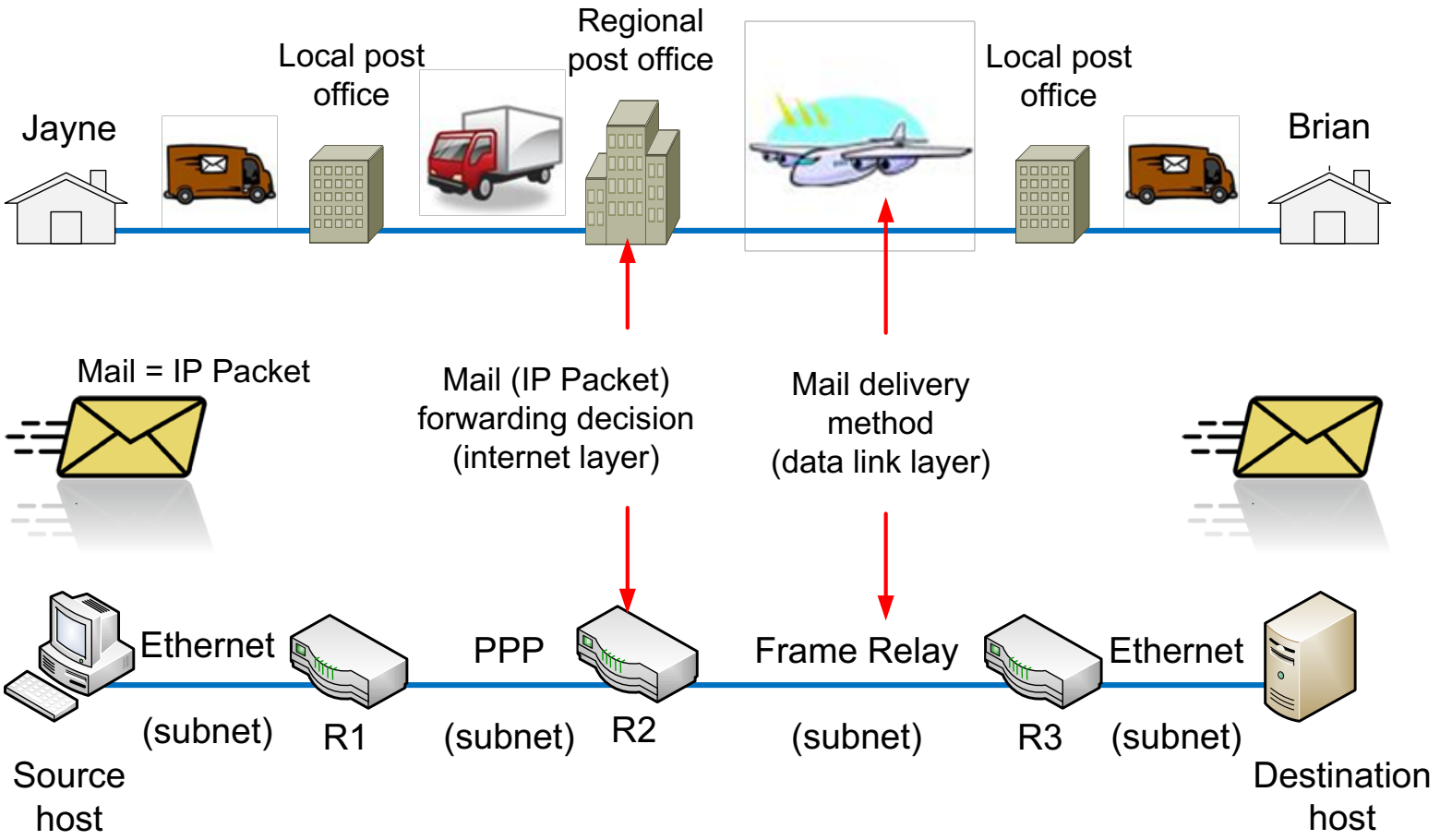
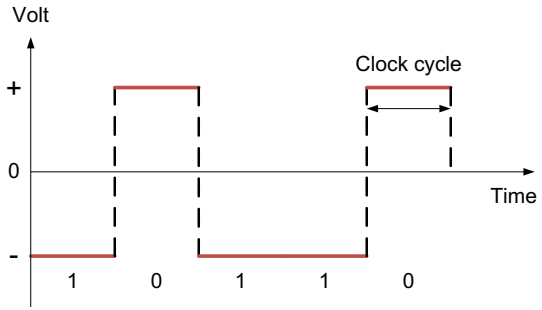
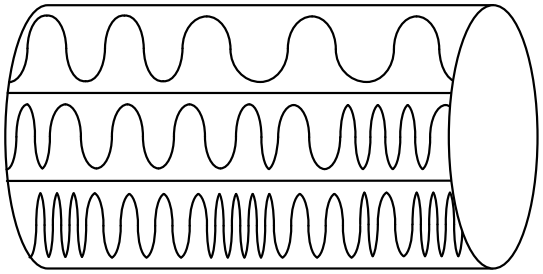


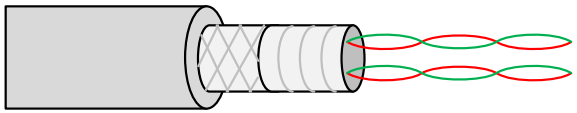
Figure 2.3 A real-life analogy of layer functions

2.4 Physical Layer (Layer 1)

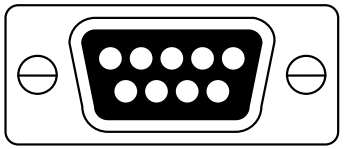




Signal multiplexing



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.

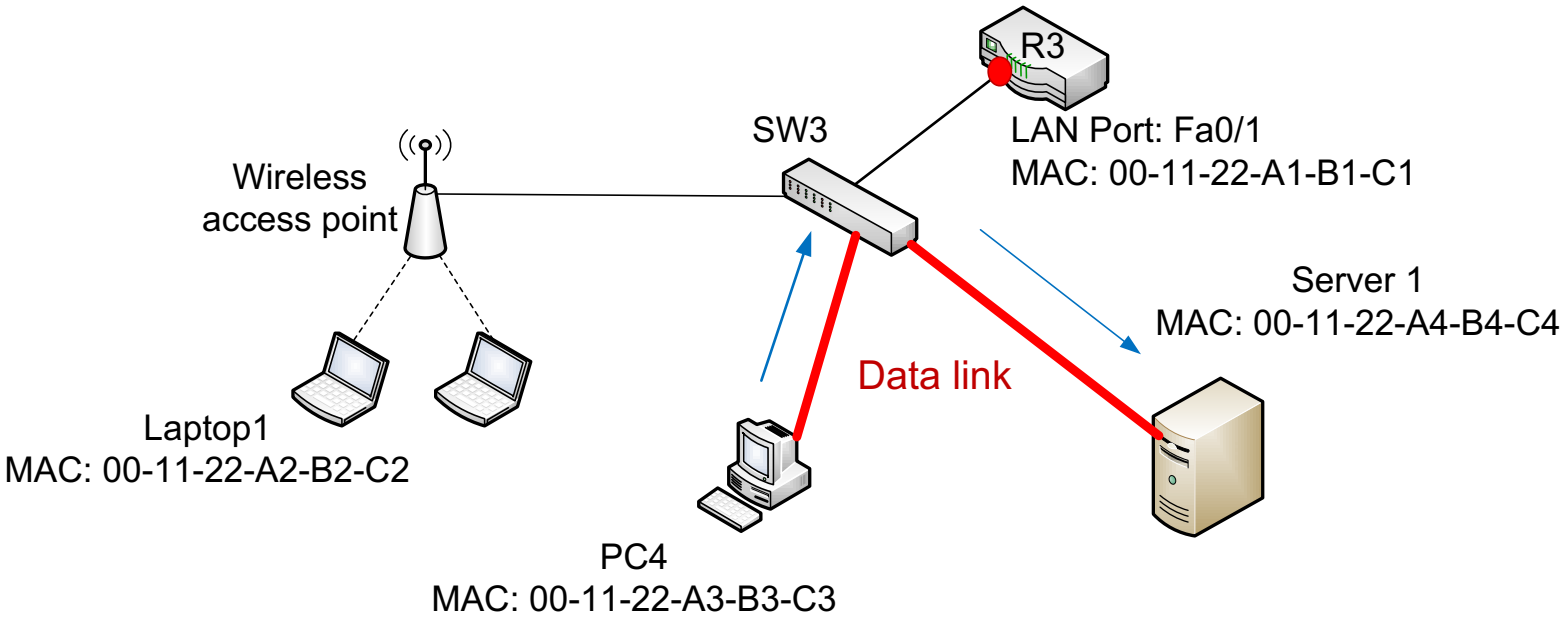


Figure 2.7 Use of MAC addressing for intra-networking

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)

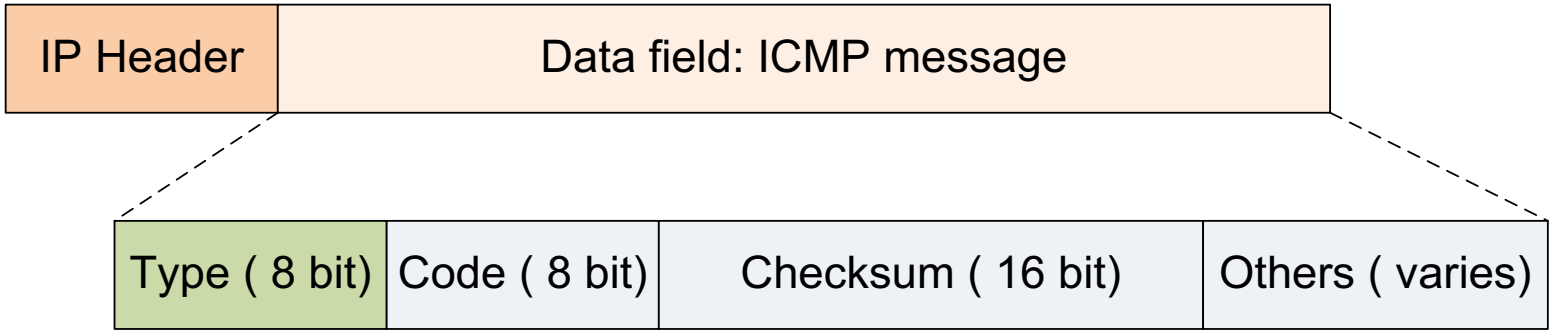
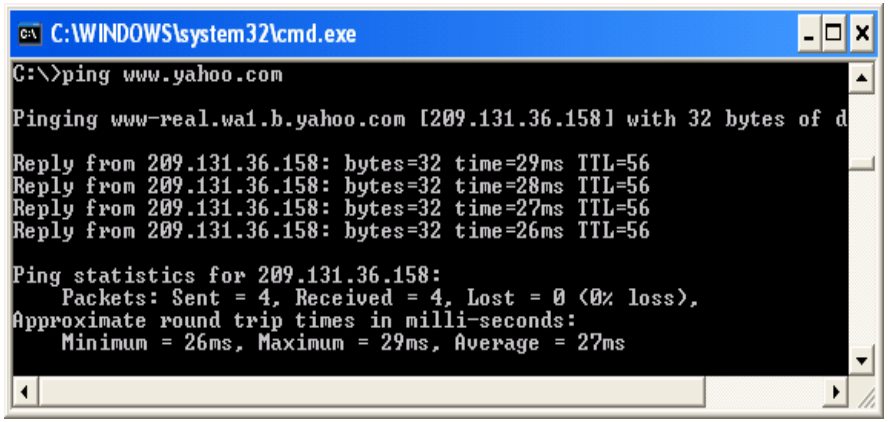


Figure 2.9 The structure of an ICMP packet

- 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)

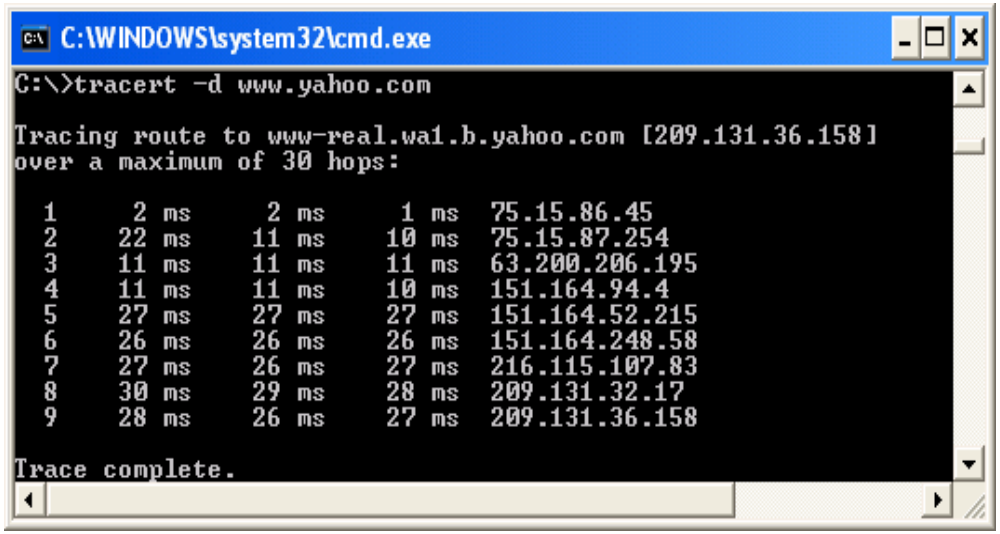


Figure 2.11 A Demonstration of *tracert*

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*

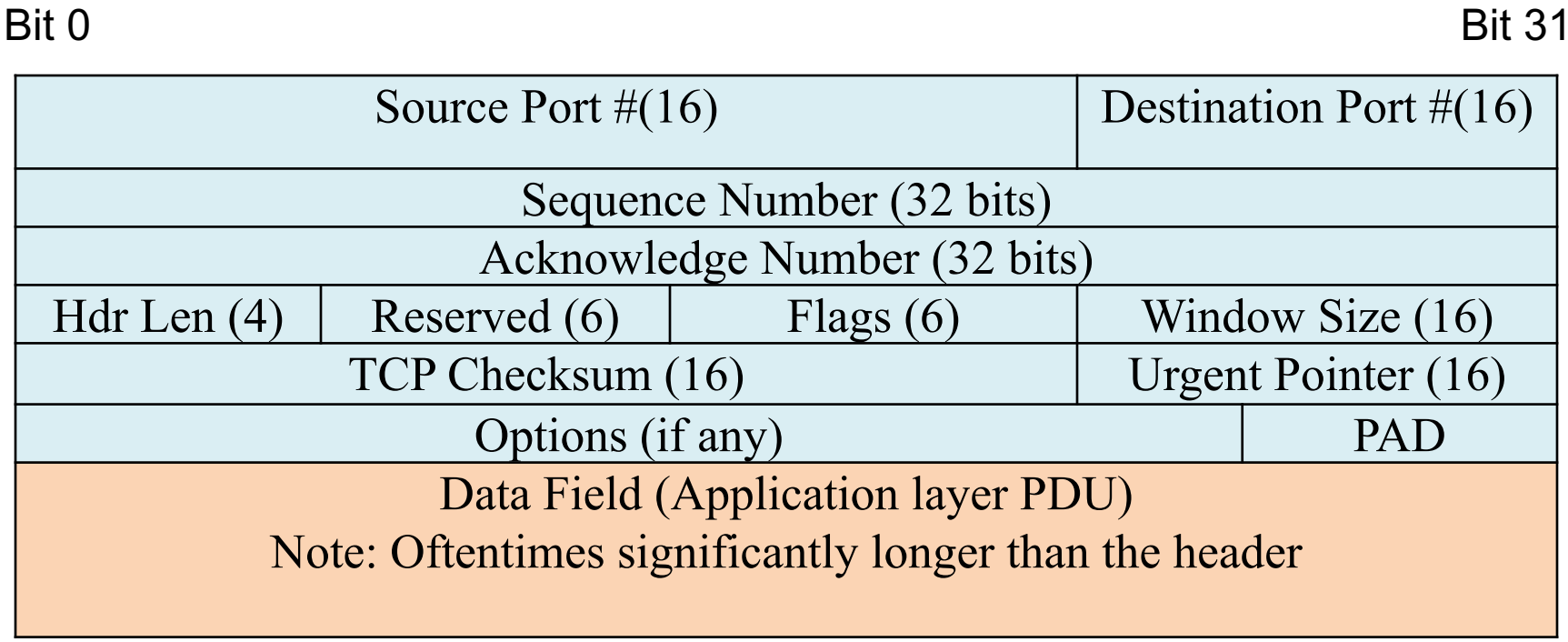


Figure 2.12 TCP segment

2.7 Transport Layer (Layer 4)

UDP: No flow control, no error control

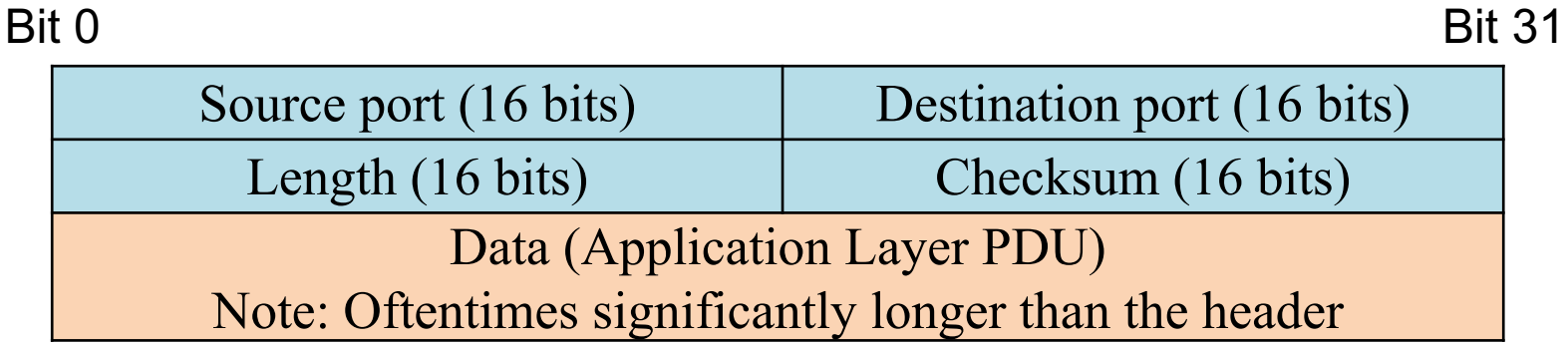
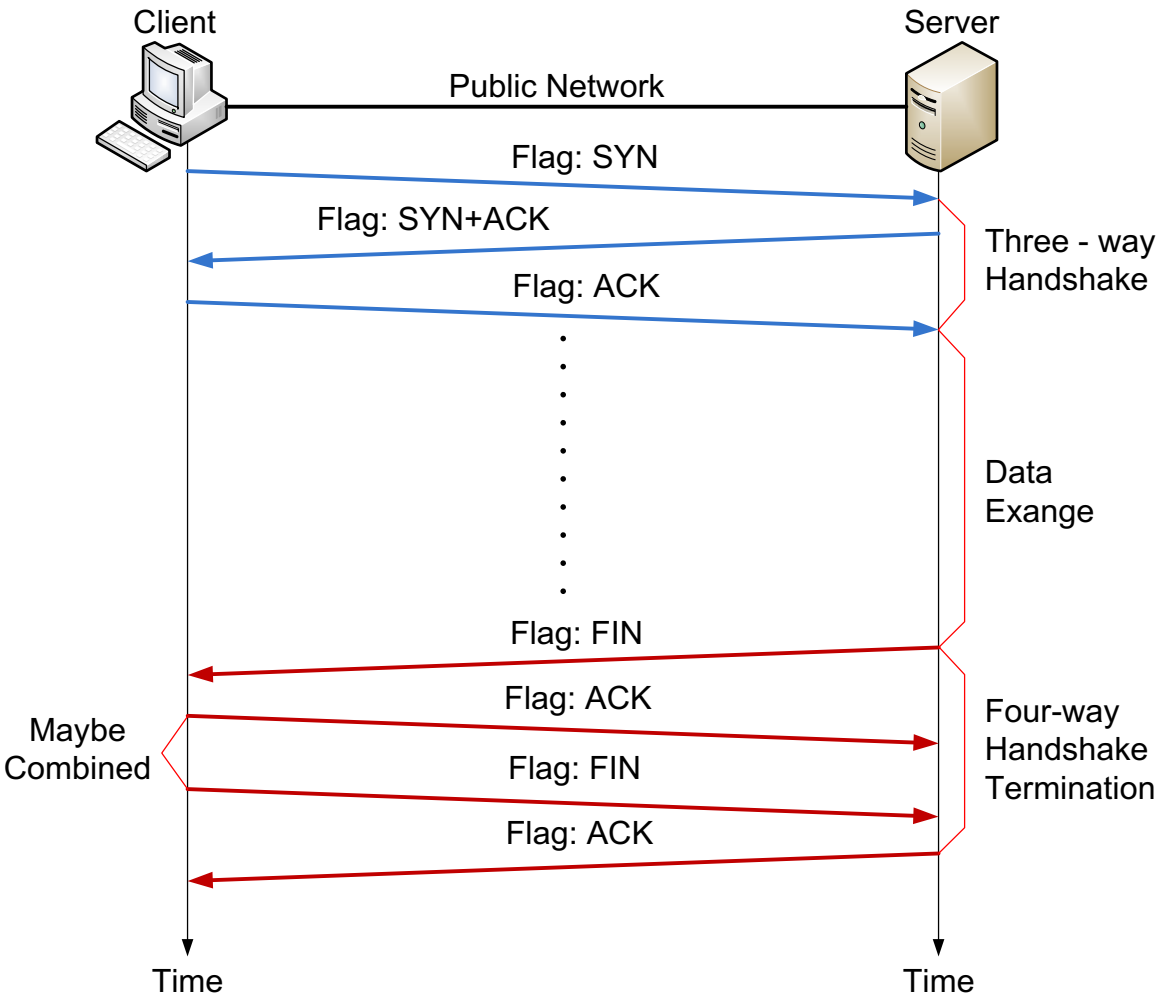


Figure 2.13 UDP datagram

2.7 Transport Layer (Layer 4)

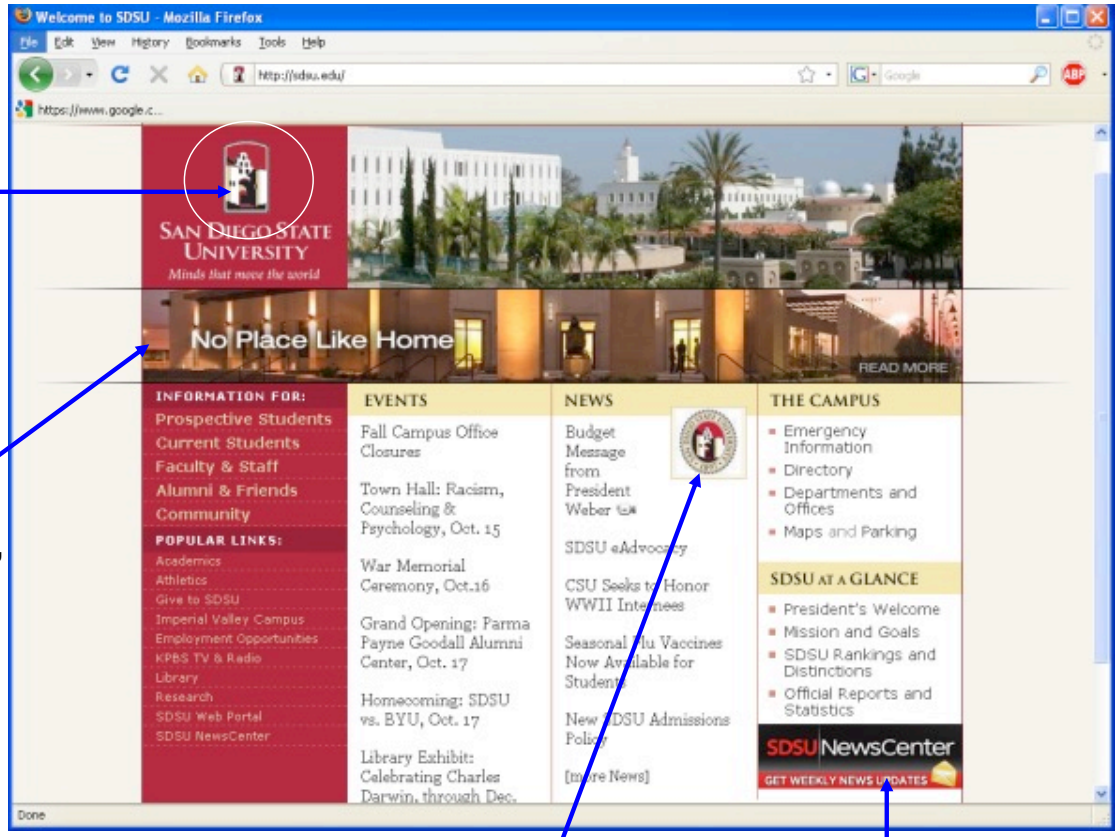
2.7.2 Session management (with TCP)

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)

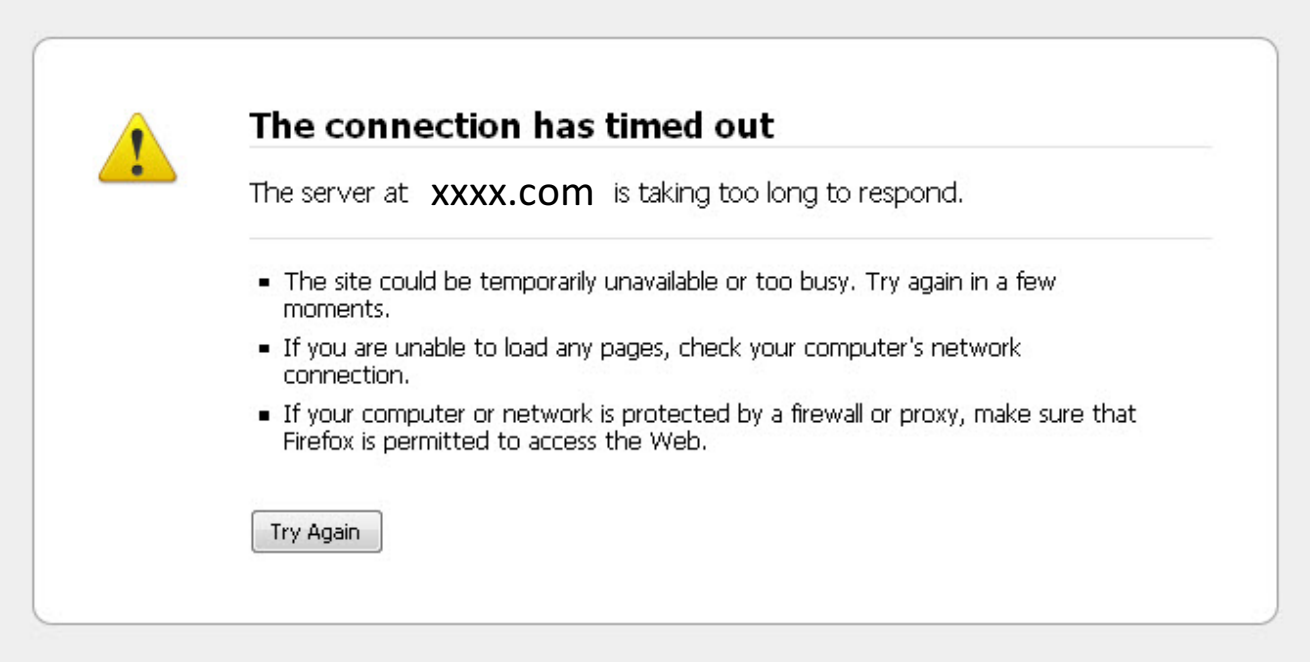


Figure 2.16 Notification of failed TCP handshaking

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

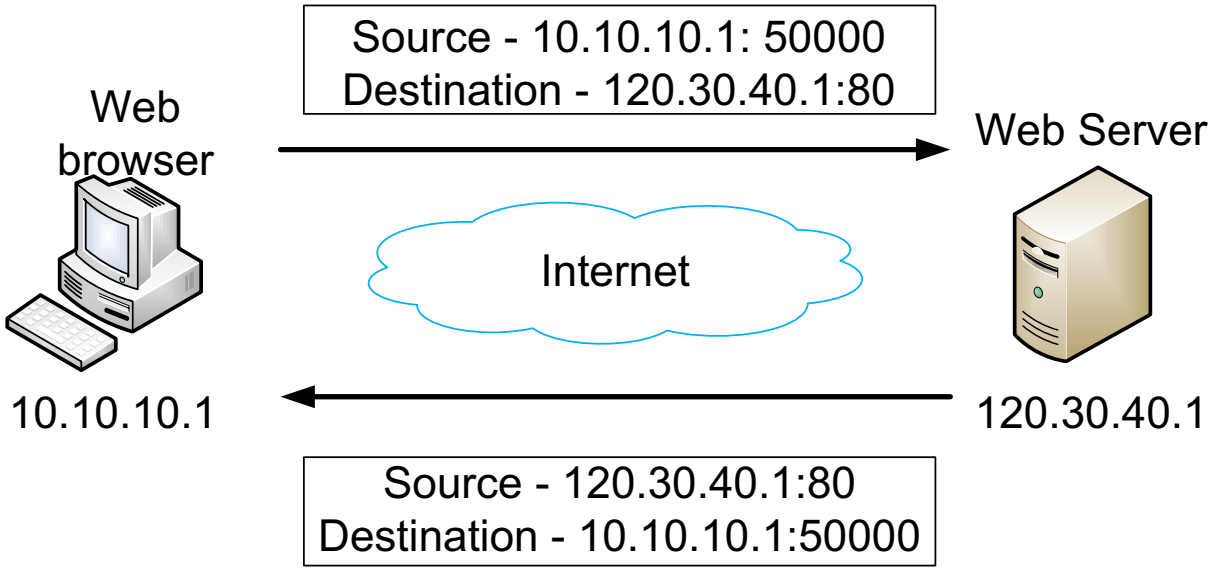


Figure 2.17 A demonstration of sockets

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

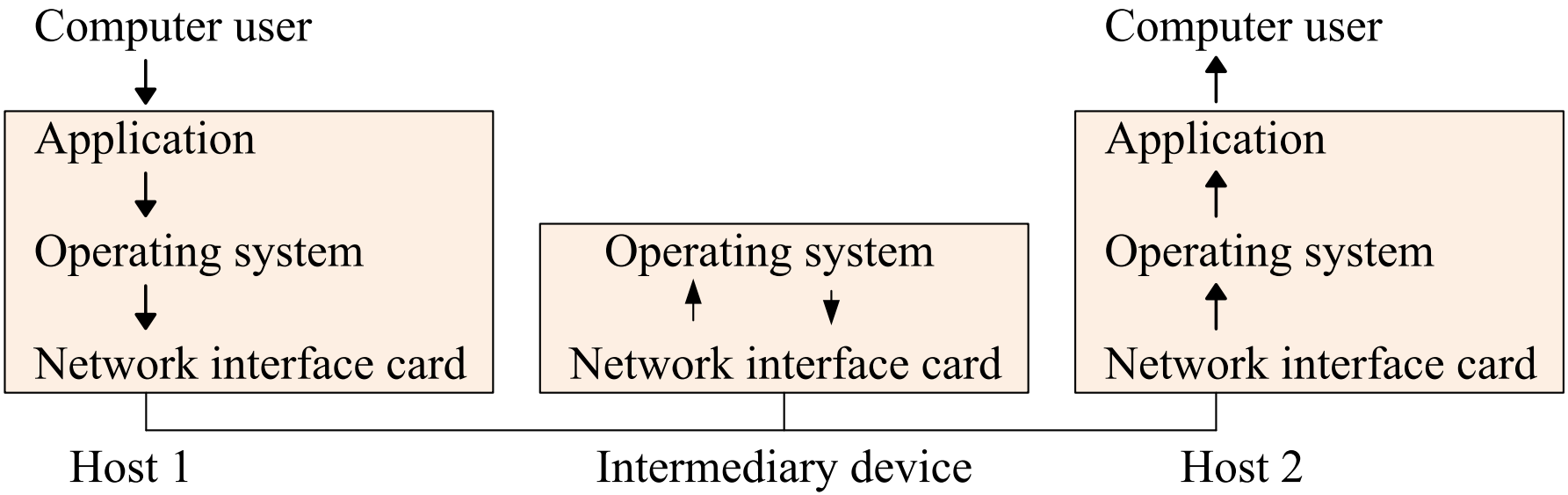


Figure 2.21 Hardware/software components of network nodes

2.10 Layer Processing

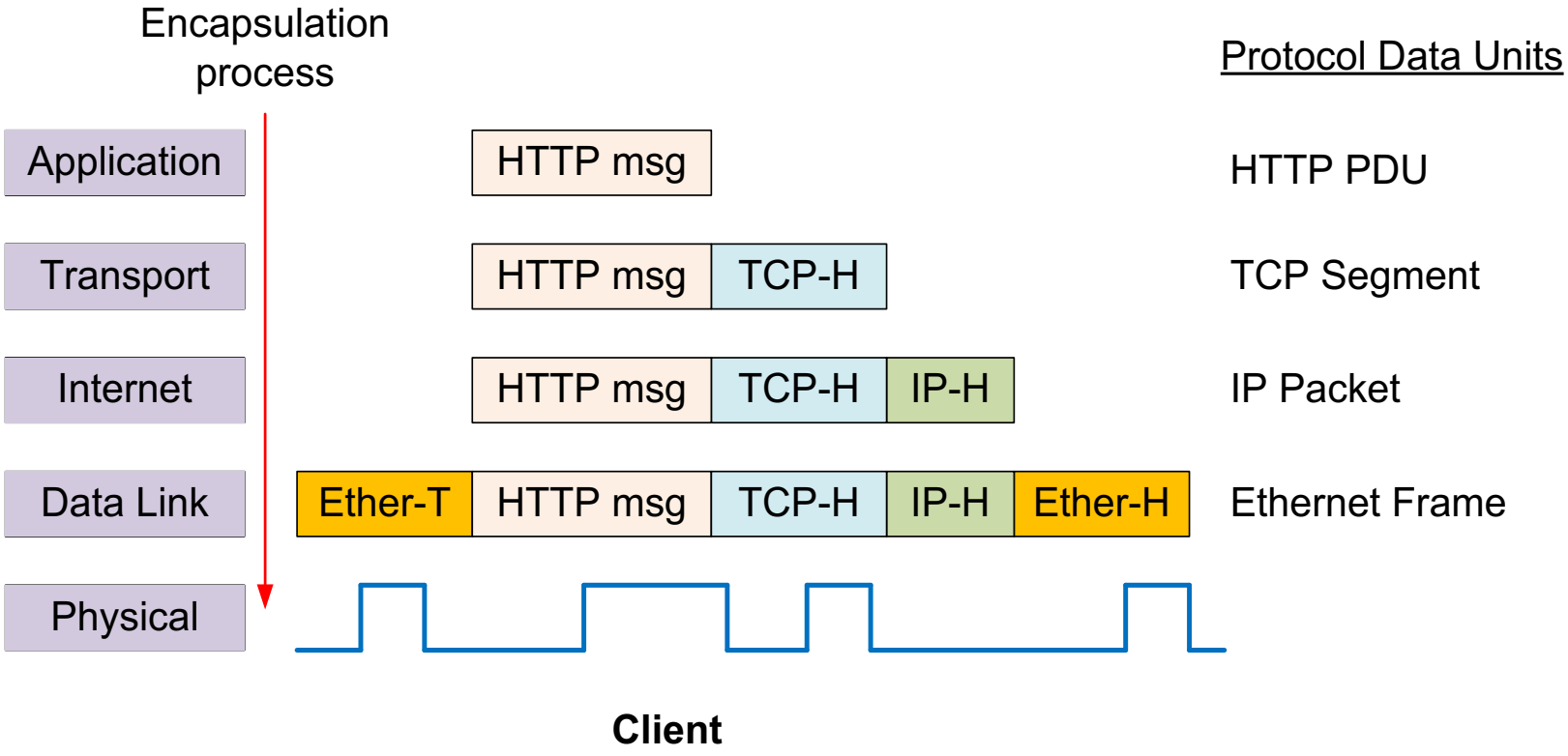


Figure 2.22 PDU encapsulation/de-encapsulation

2.10 Layer Processing

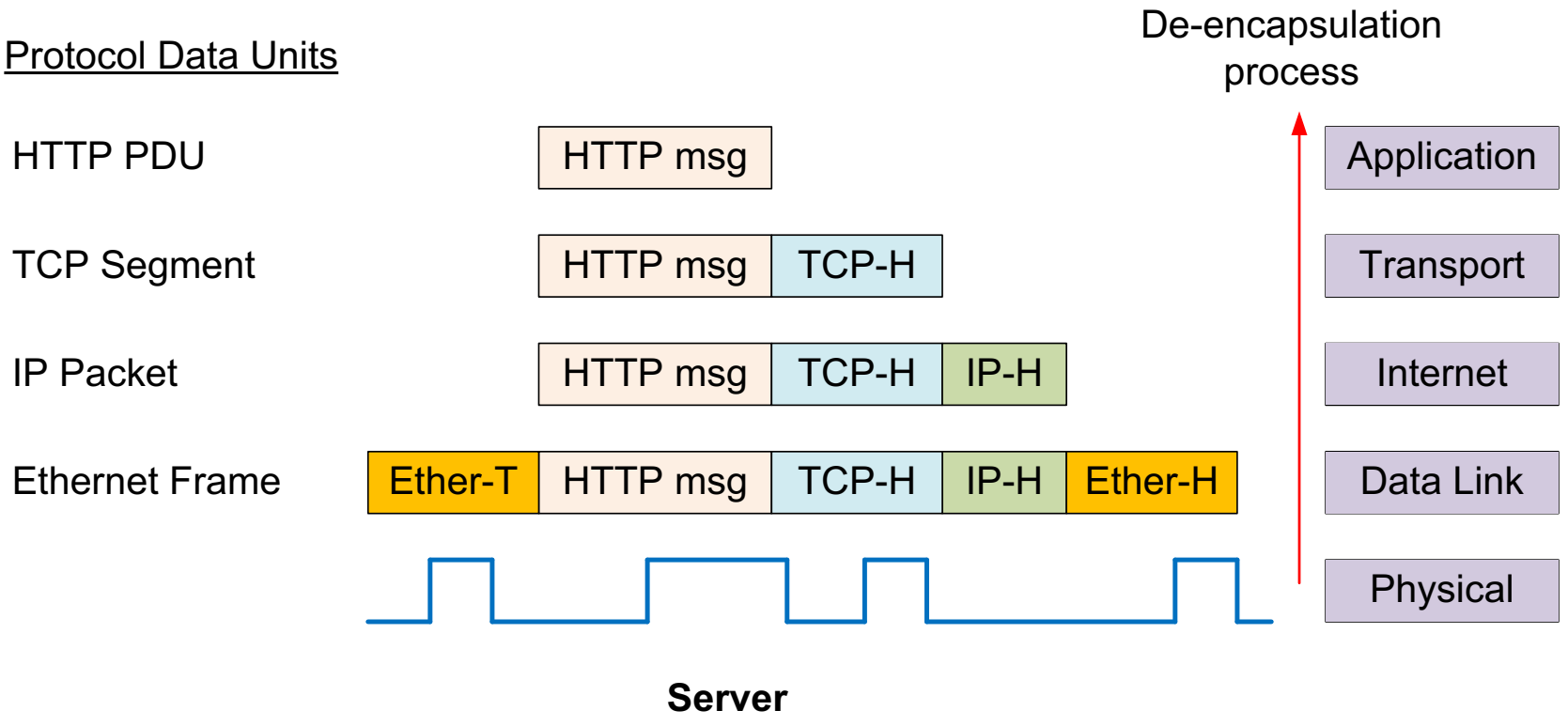


Figure 2.22 PDU encapsulation/de-encapsulation

2.10 Layer Processing

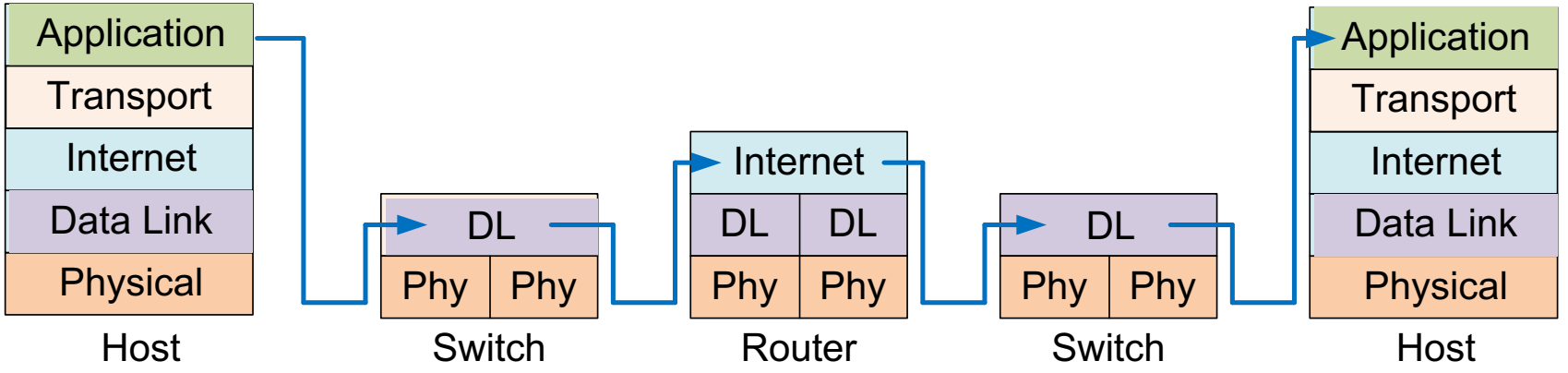


Figure 2.23 Layer processing by intermediary devices

2.10 Layer Processing

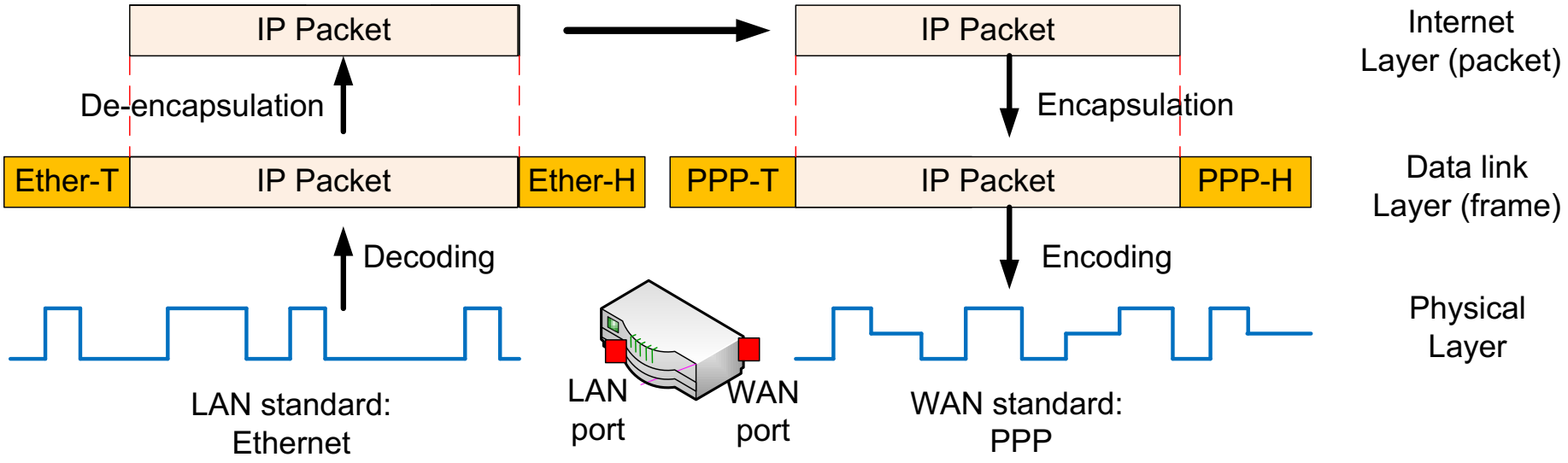


Figure 2.24 Packet de-encapsulation/encapsulation by the router

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

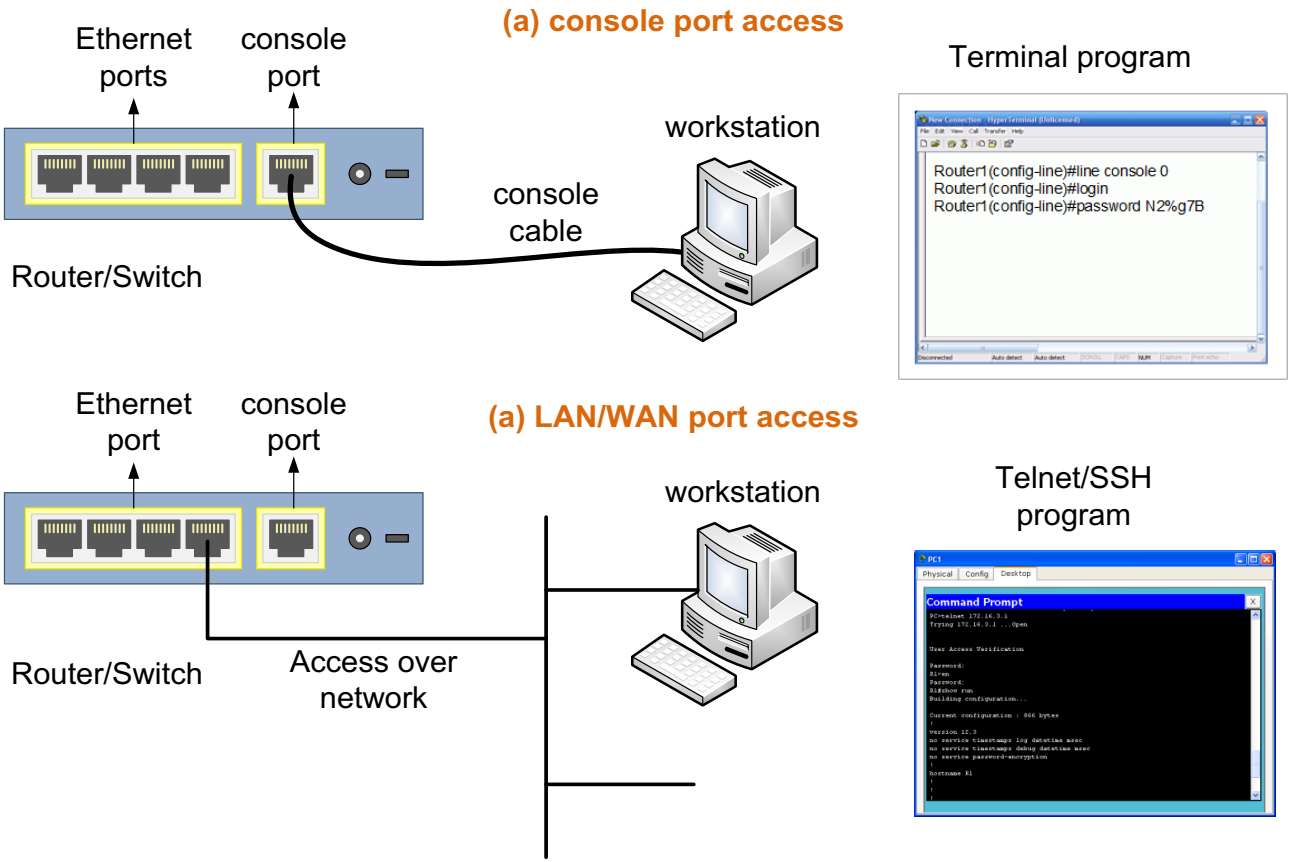


Figure 3.1 Managing an intermediary device

3.3 Hubs (Multi-port Repeaters)

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

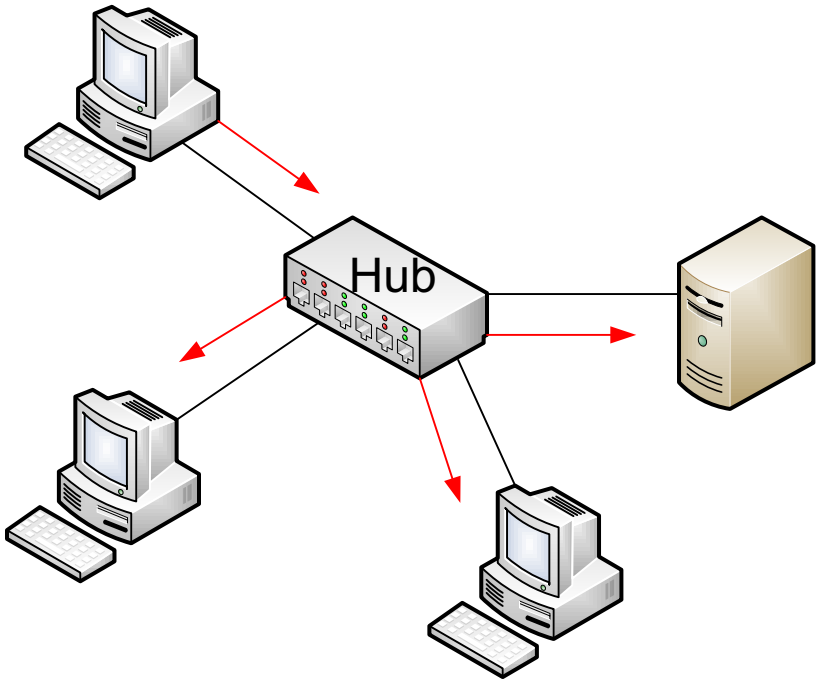


Figure 3.3 A small hub-based network

3.4 Bridges & Wireless Access Points

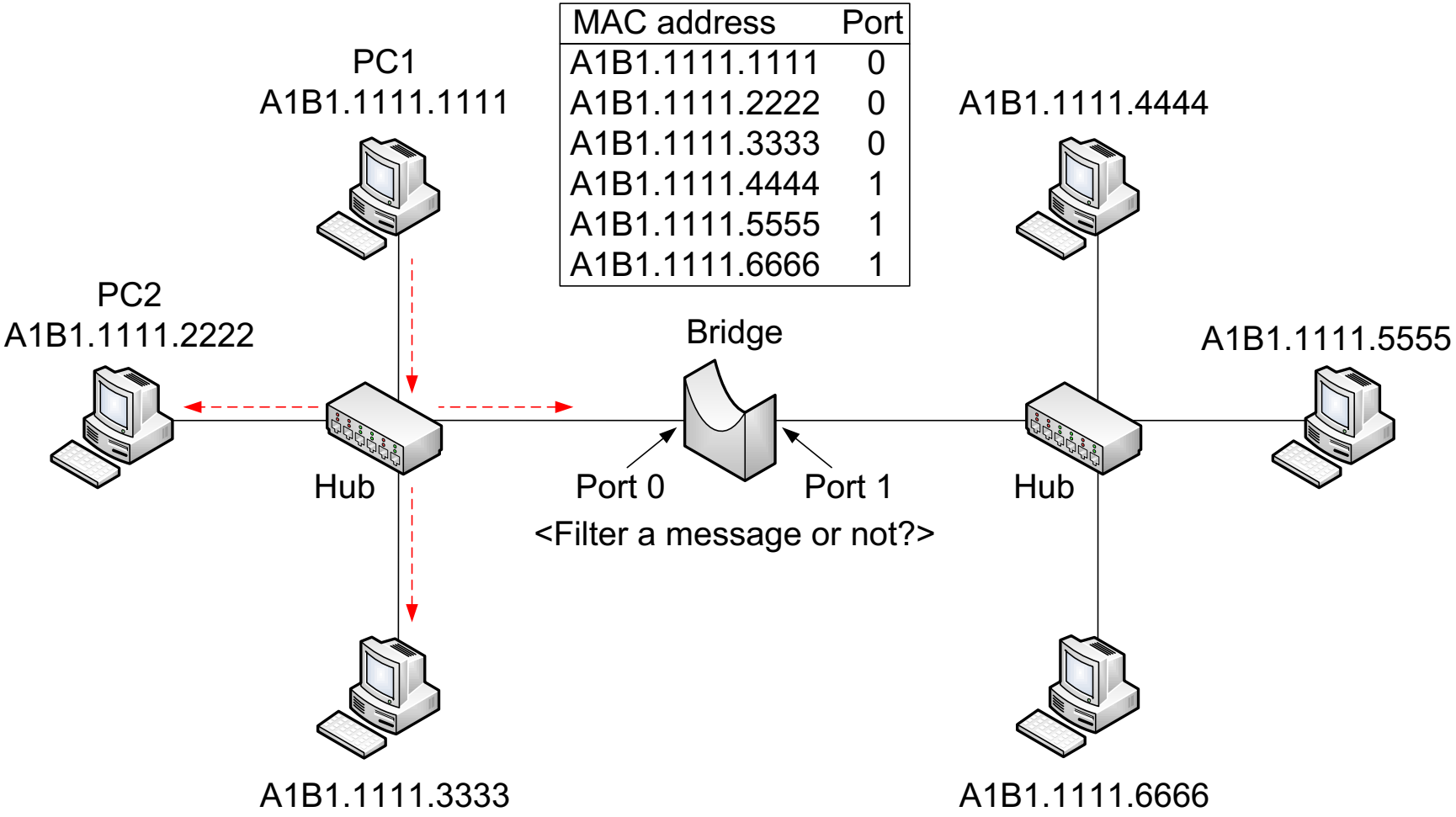
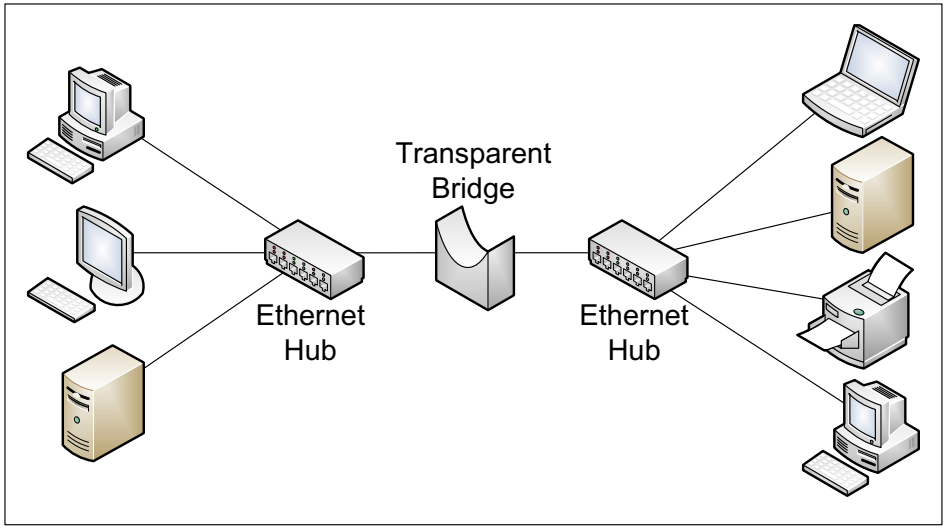


Figure 3.4 An example of bridge table

3.4 Bridges & Wireless Access Points



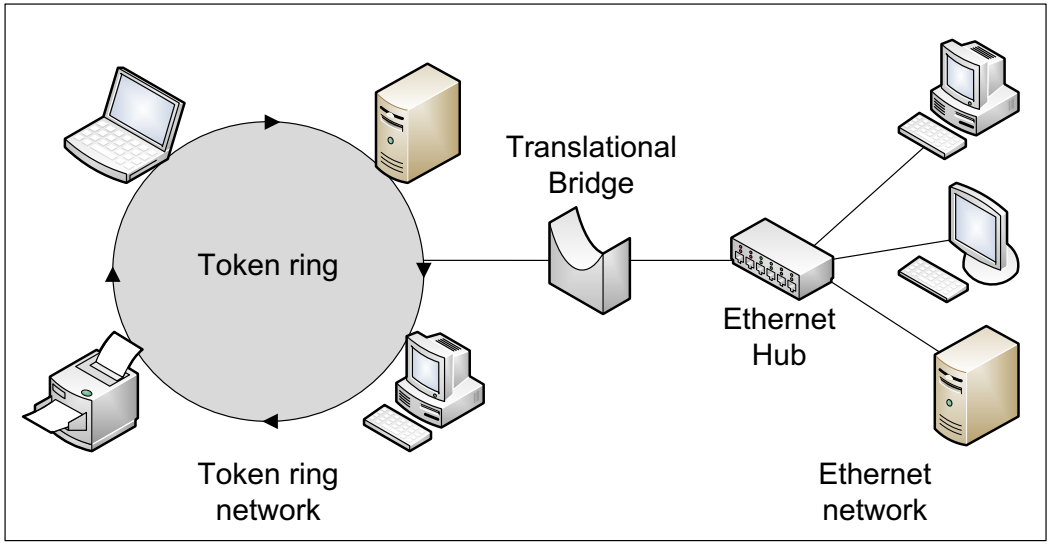


Figure 3.5

Transparent vs. translational bridges

3.4 Bridges & Wireless Access Points

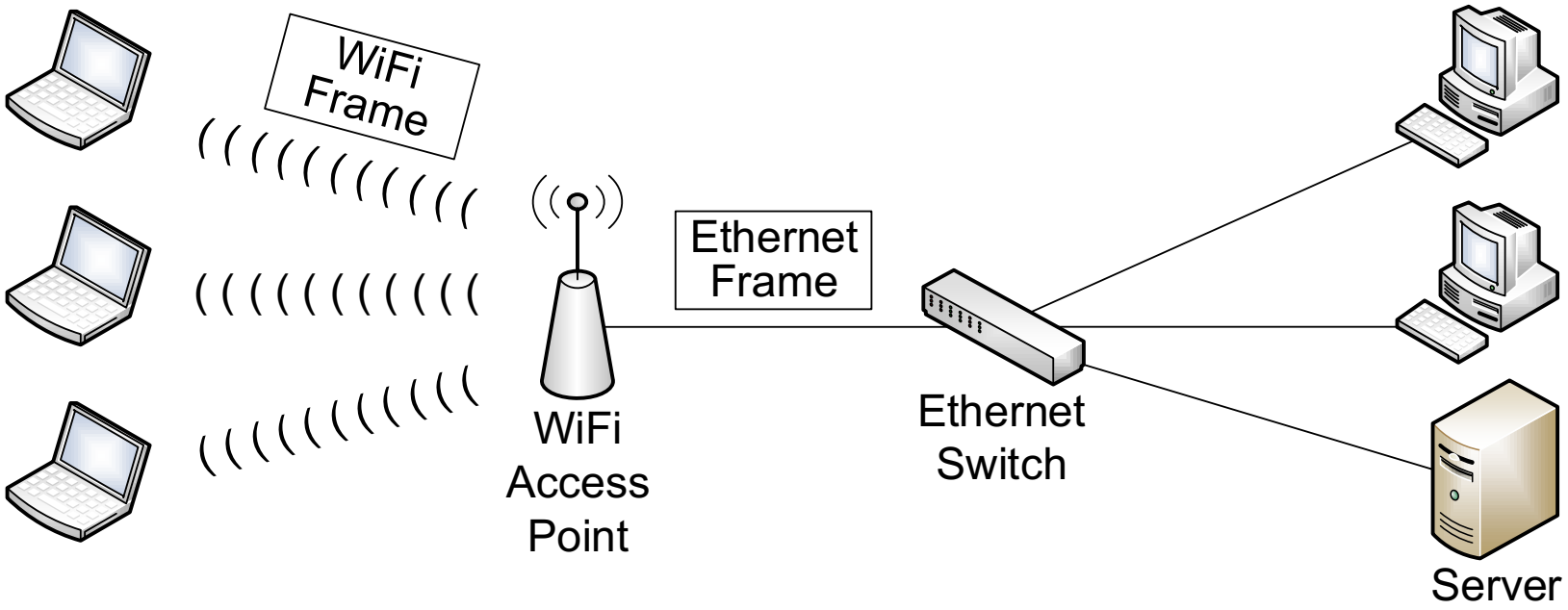


Figure 3.6 Wireless Access Point as a translational bridge

3.5 Switches
3.5.1 General Features

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

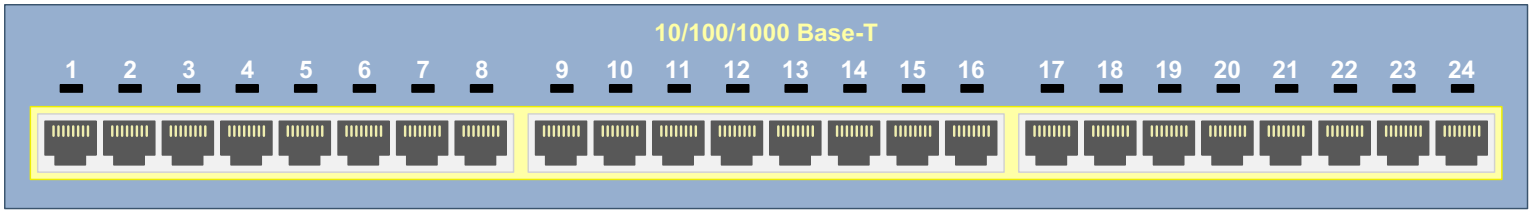


Figure 3.7 Ethernet switch – external view (not an actual product)

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

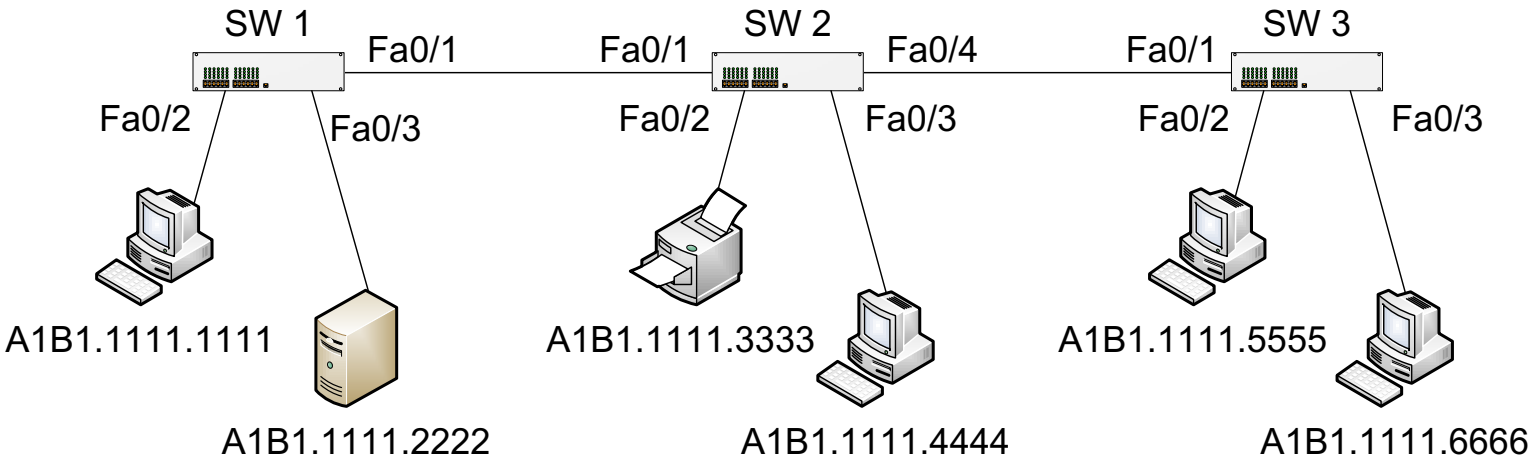
Table 3.3 Switch port naming (This is not a switch table)

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)

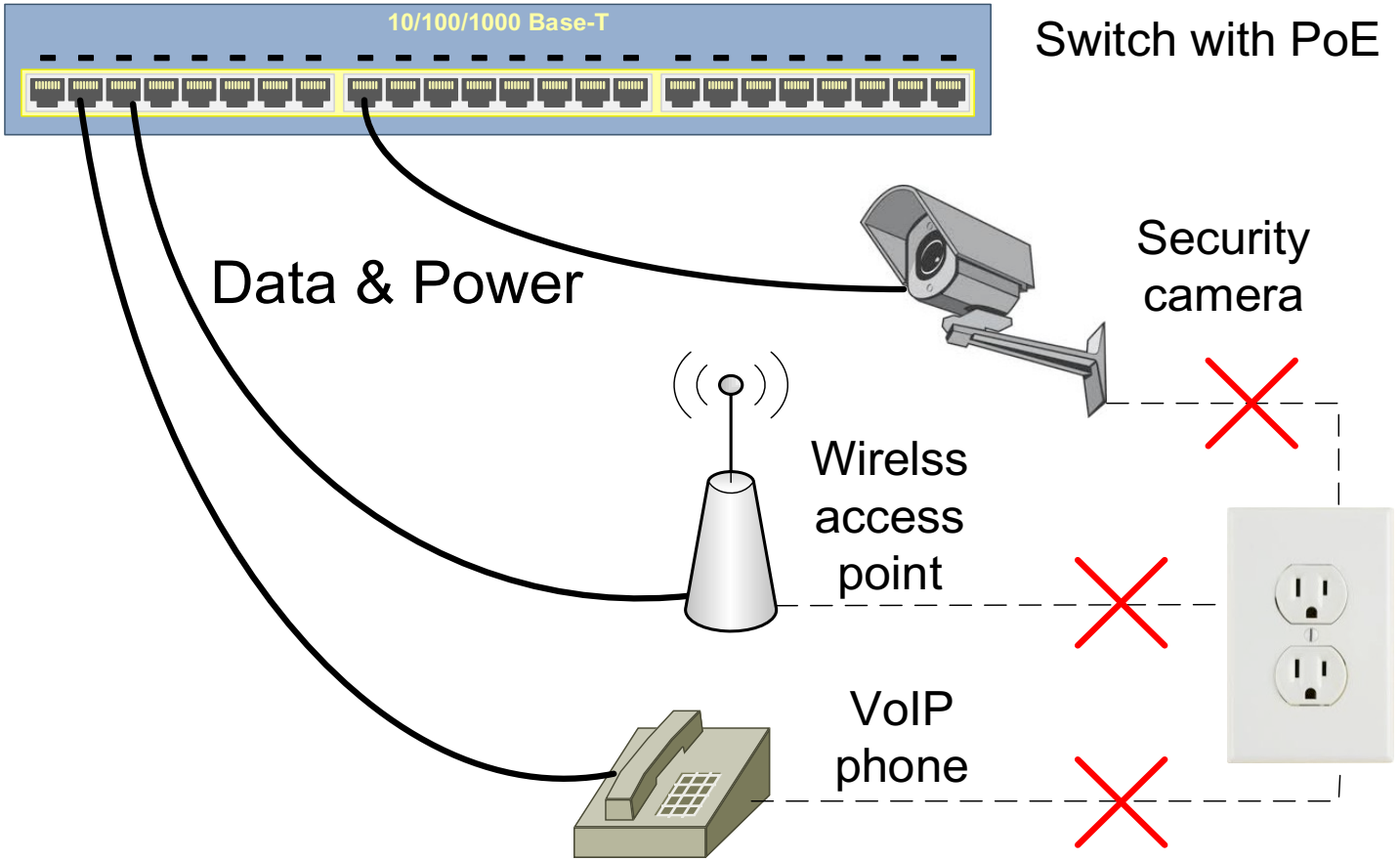


Figure 3.14 Power over Ethernet

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

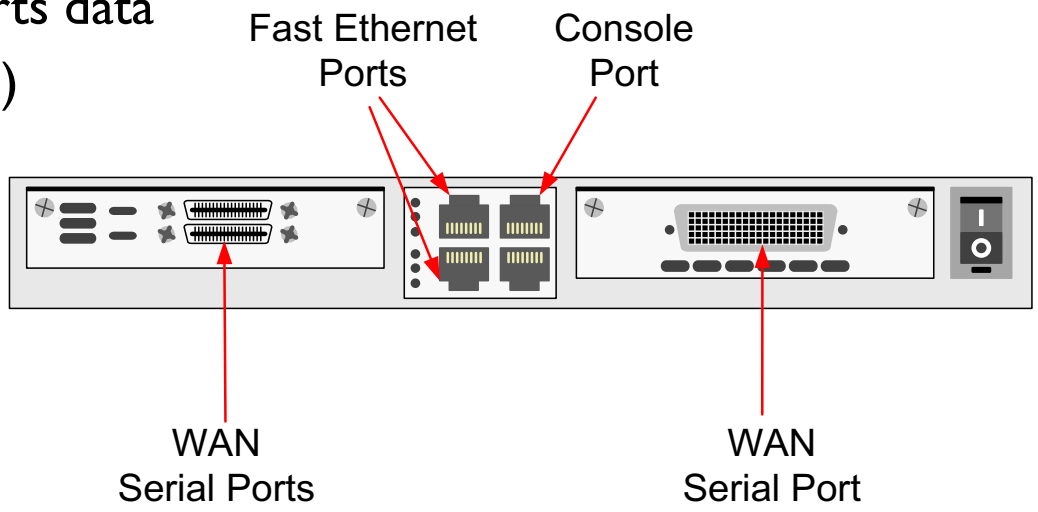
3.6 Routers

3.6.1 Two Primary Functions

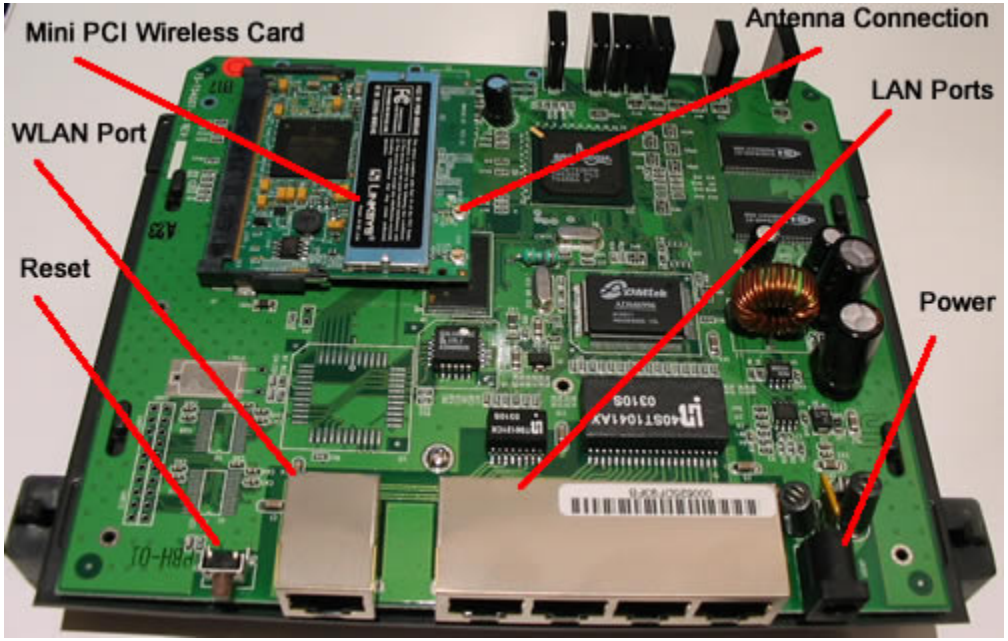
- *Routing table development and its update*
- *Packet forwarding*

3.6.2 Router Components

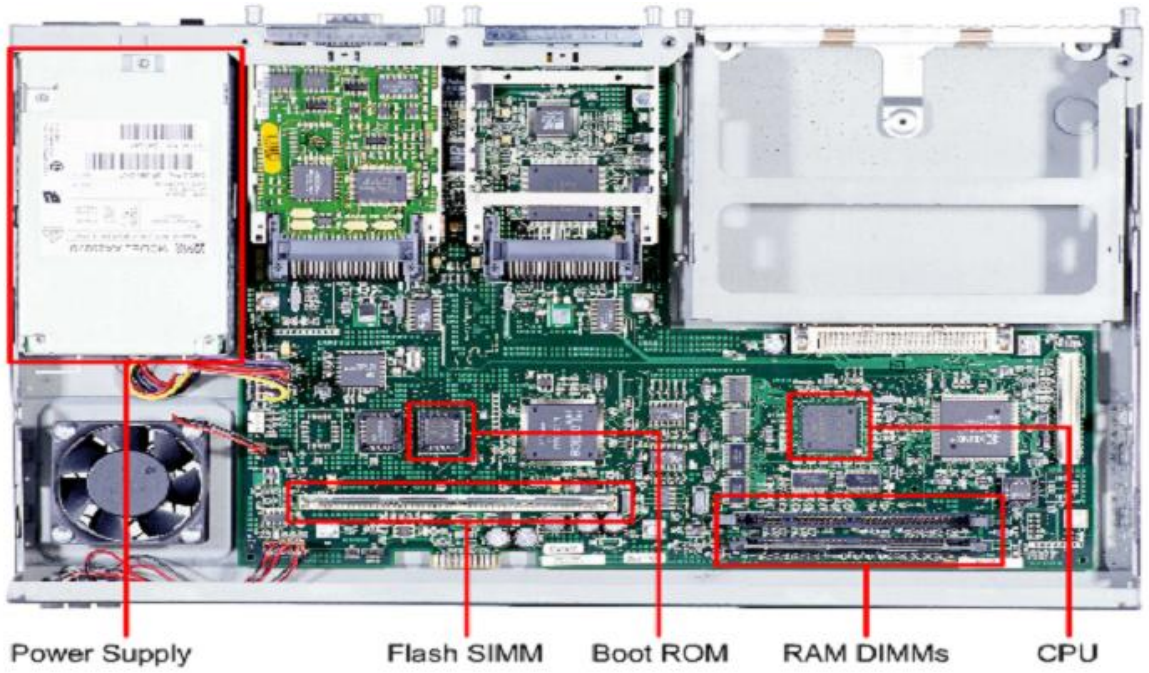
- Central processing unit (CPU)
- Memory: ROM, RAM, Non-volatile flash memory
- Operating System
- System bus that transports data
- Various ports (interfaces)



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#

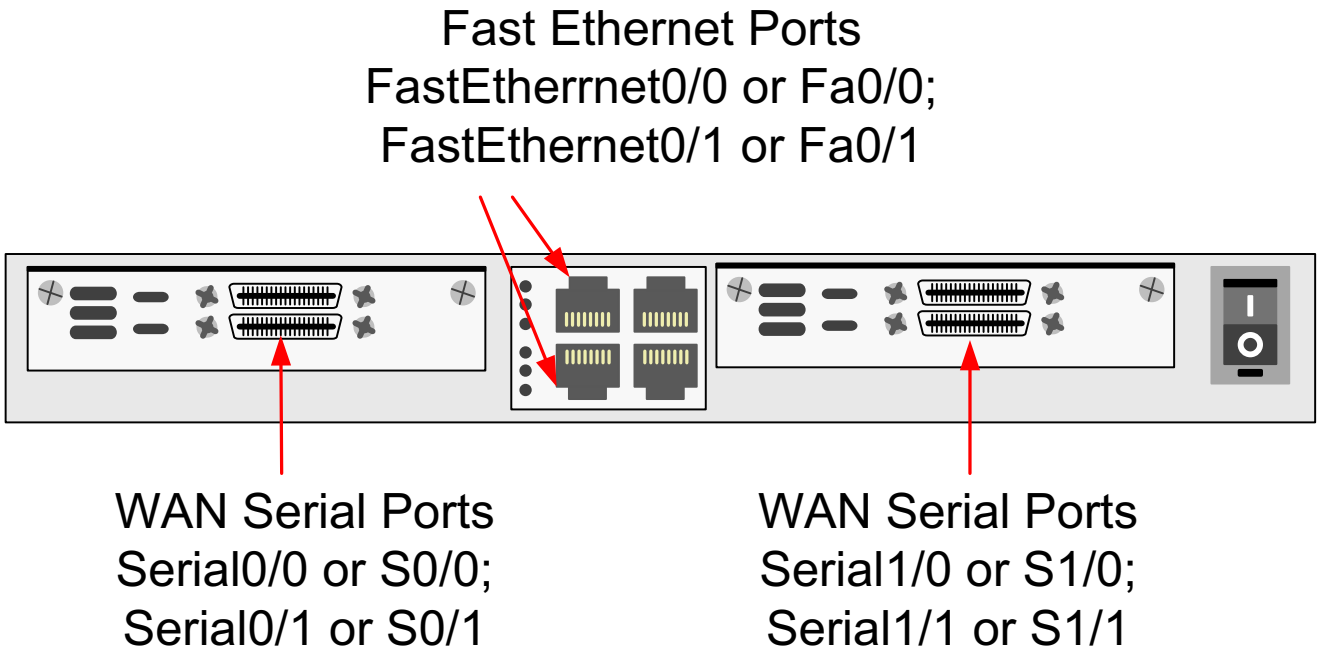


Figure 3.16 Cisco's LAN and WAN port naming (not an actual model)

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

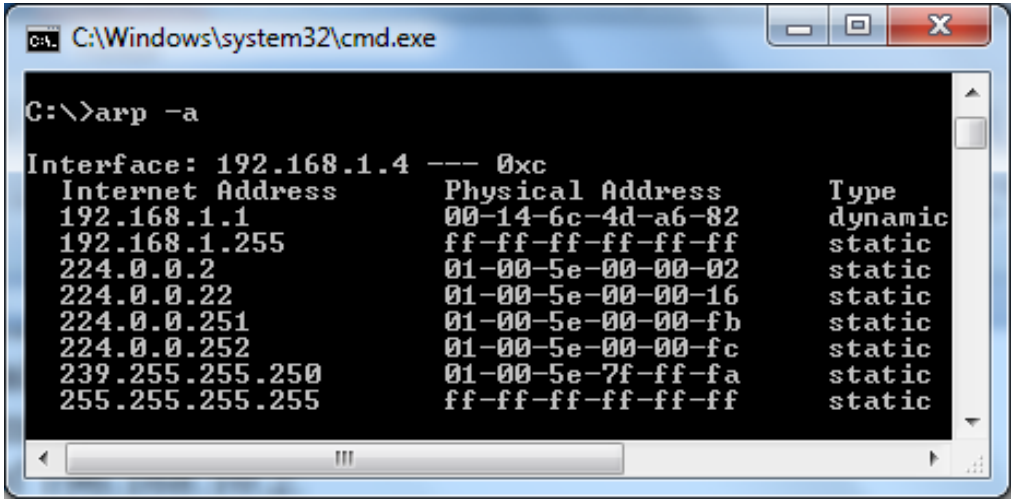
- Access control list (ACL)
- Network address translation (NAT)
- DHCP server
- Virtual Private Network (VPN)
- Intrusion Prevention System (IPS)
- Security auditing

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

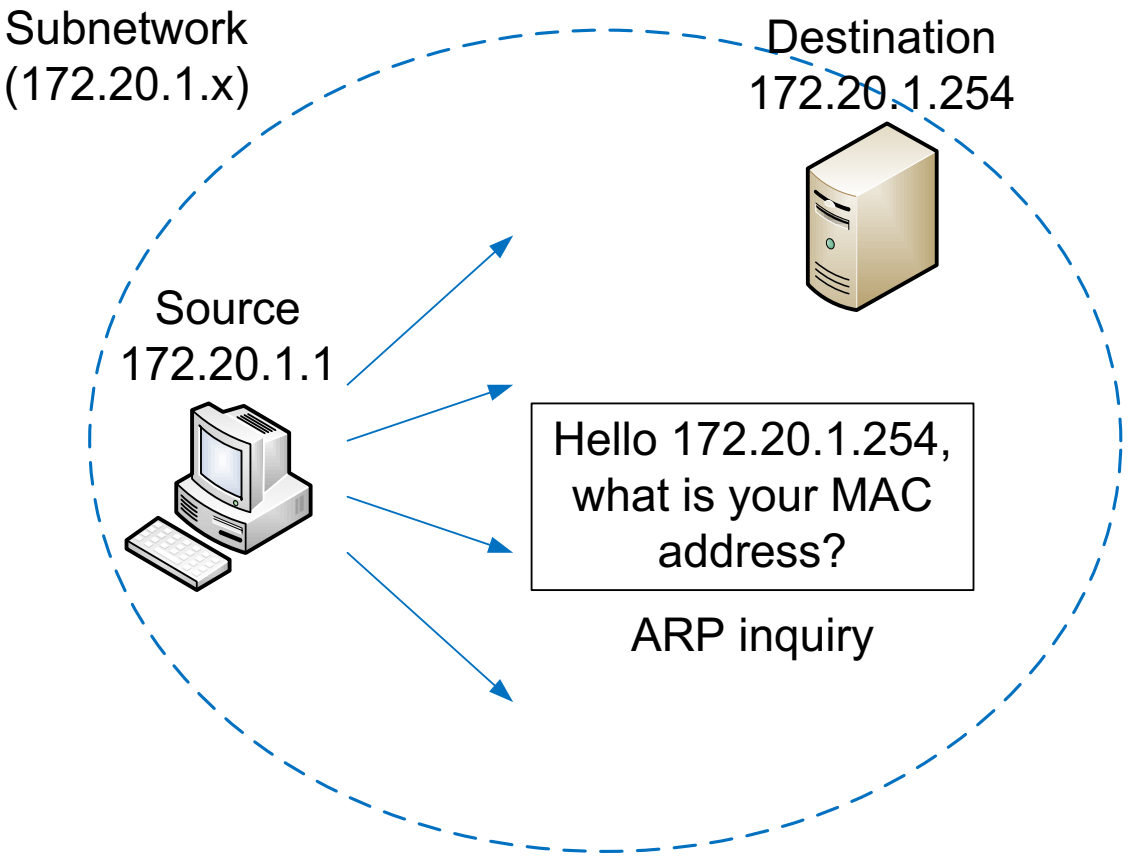


Figure 3.18 Scenario 1: host to host ARP inquiry

3.8.2 ARP Usage Scenarios

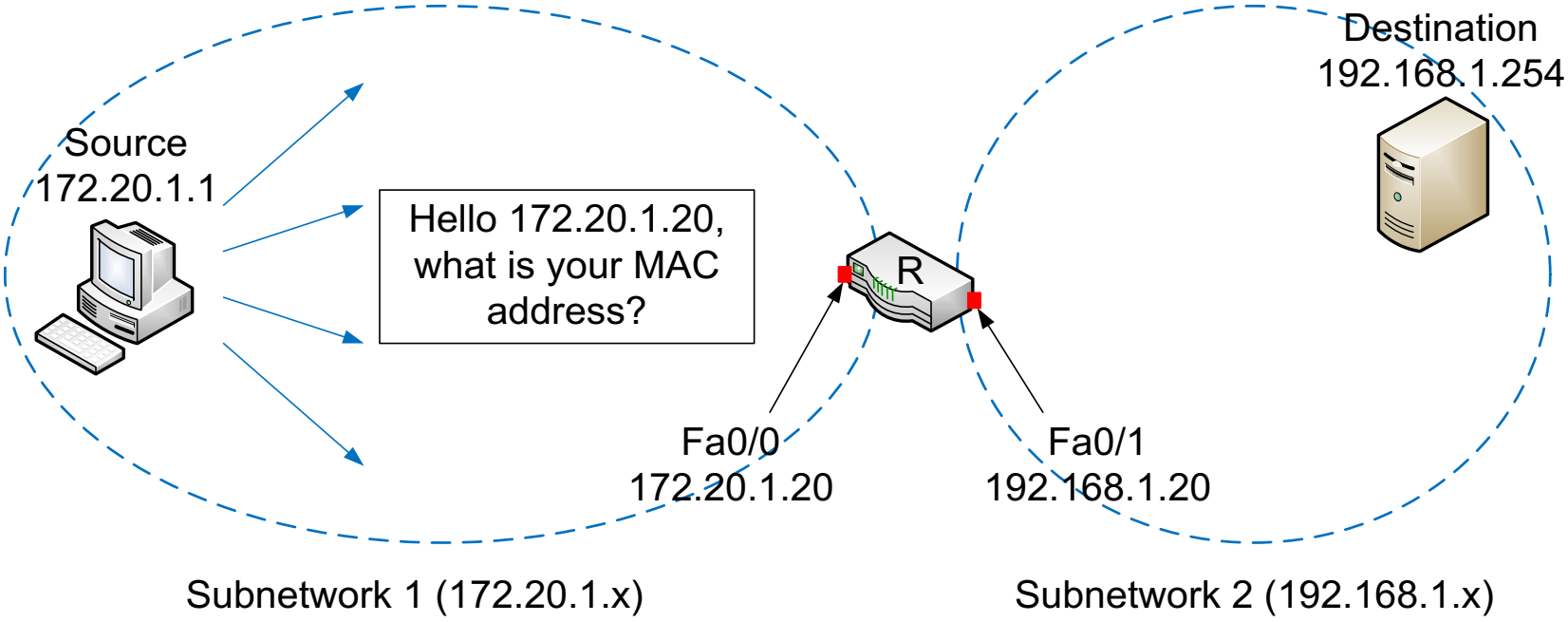


Figure 3.19 Scenario 2: host to router ARP inquiry

3.8.2 ARP Usage Scenarios

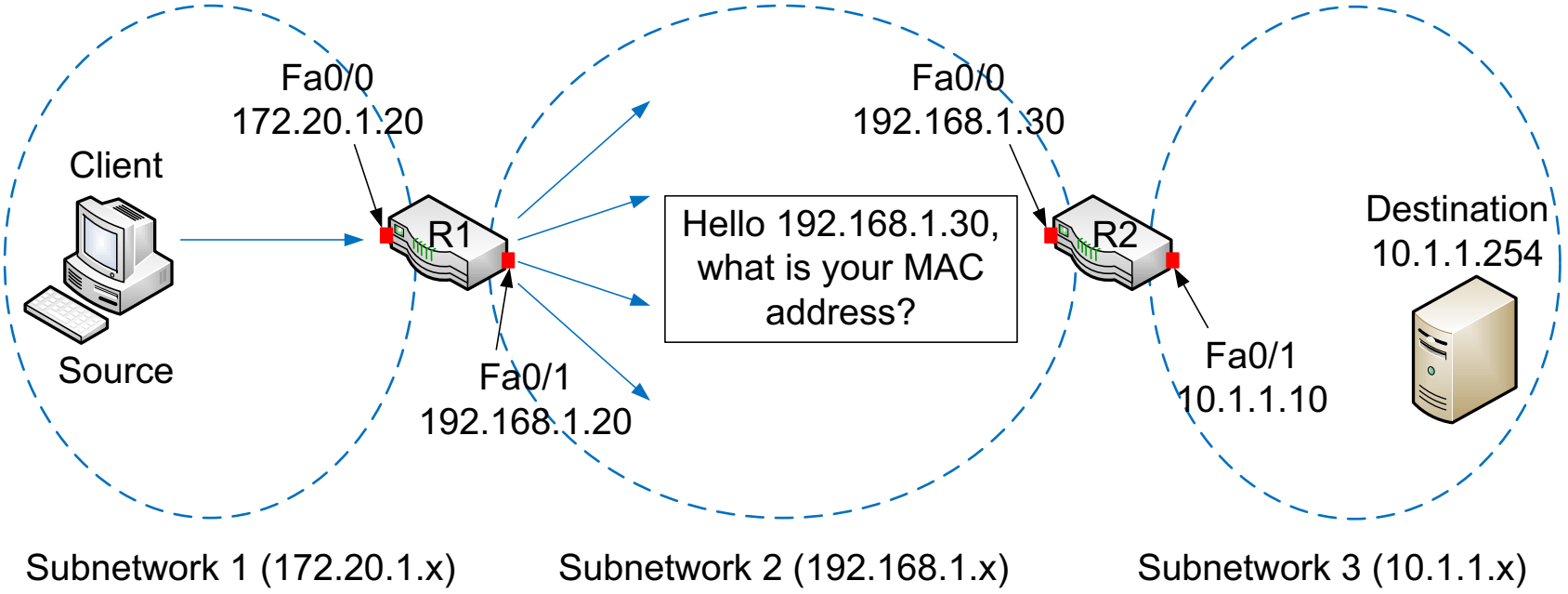


Figure 3.20 Scenario 3: router to router ARP inquiry

3.8.2 ARP Usage Scenarios

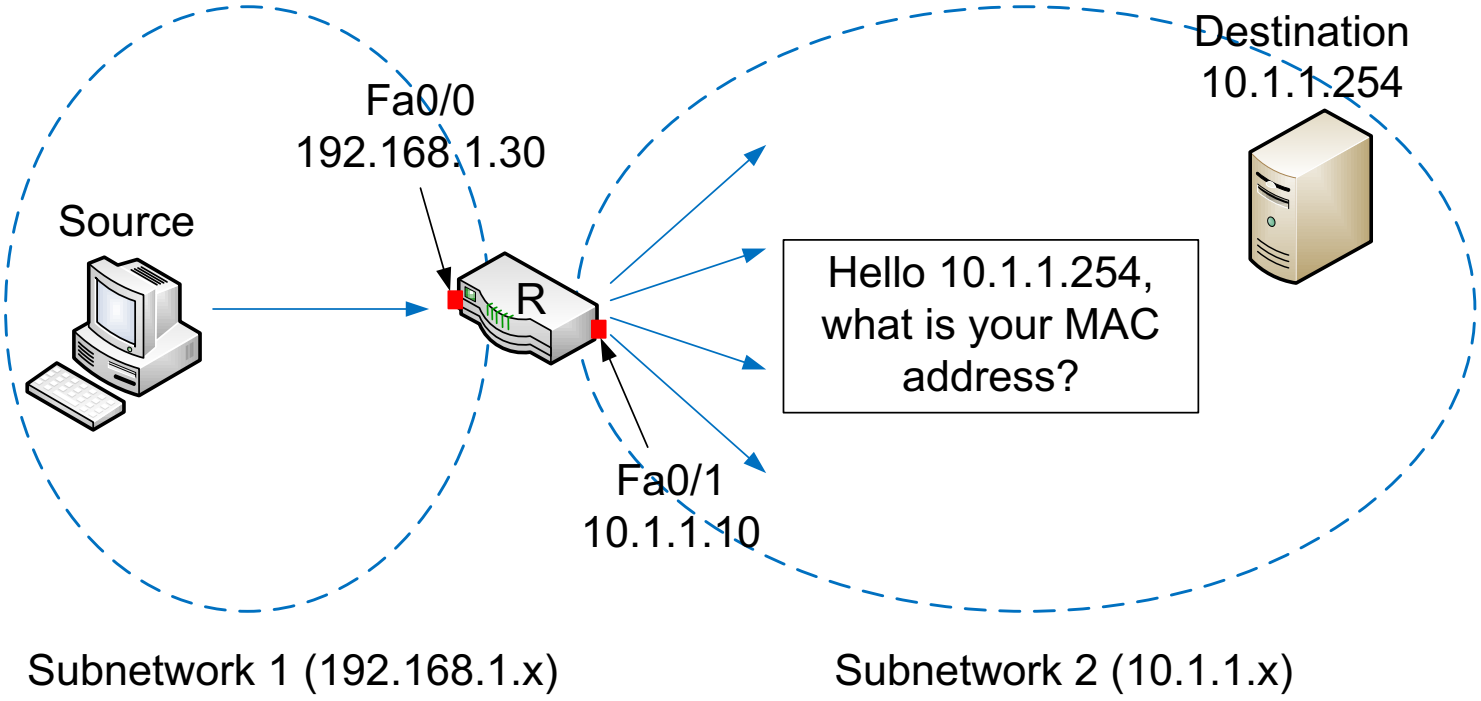


Figure 3.21 Scenario 4: router to host ARP inquiry

3.10 Collision vs. Broadcast Domains

Switch as a collision domain divider

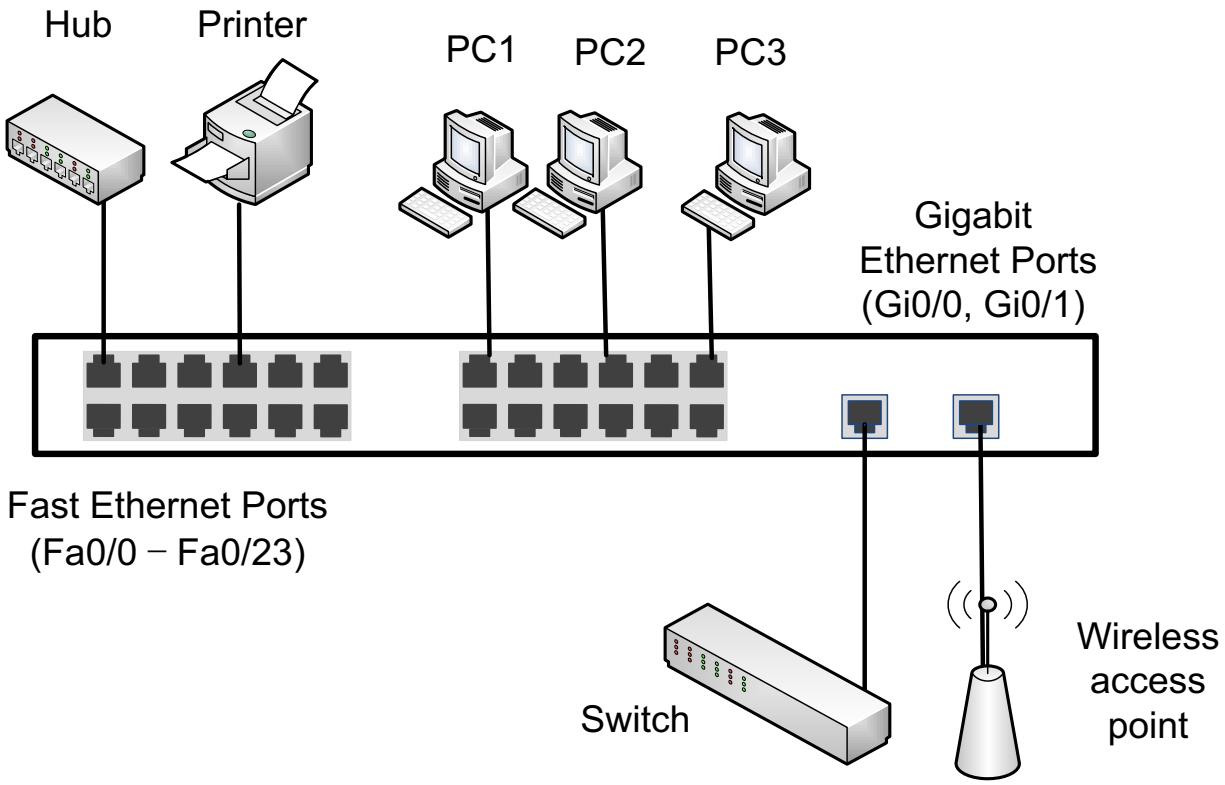


Figure 3.22 Switch as a collision domain divider

3.10 Collision vs. Broadcast Domains

- Collision domain types

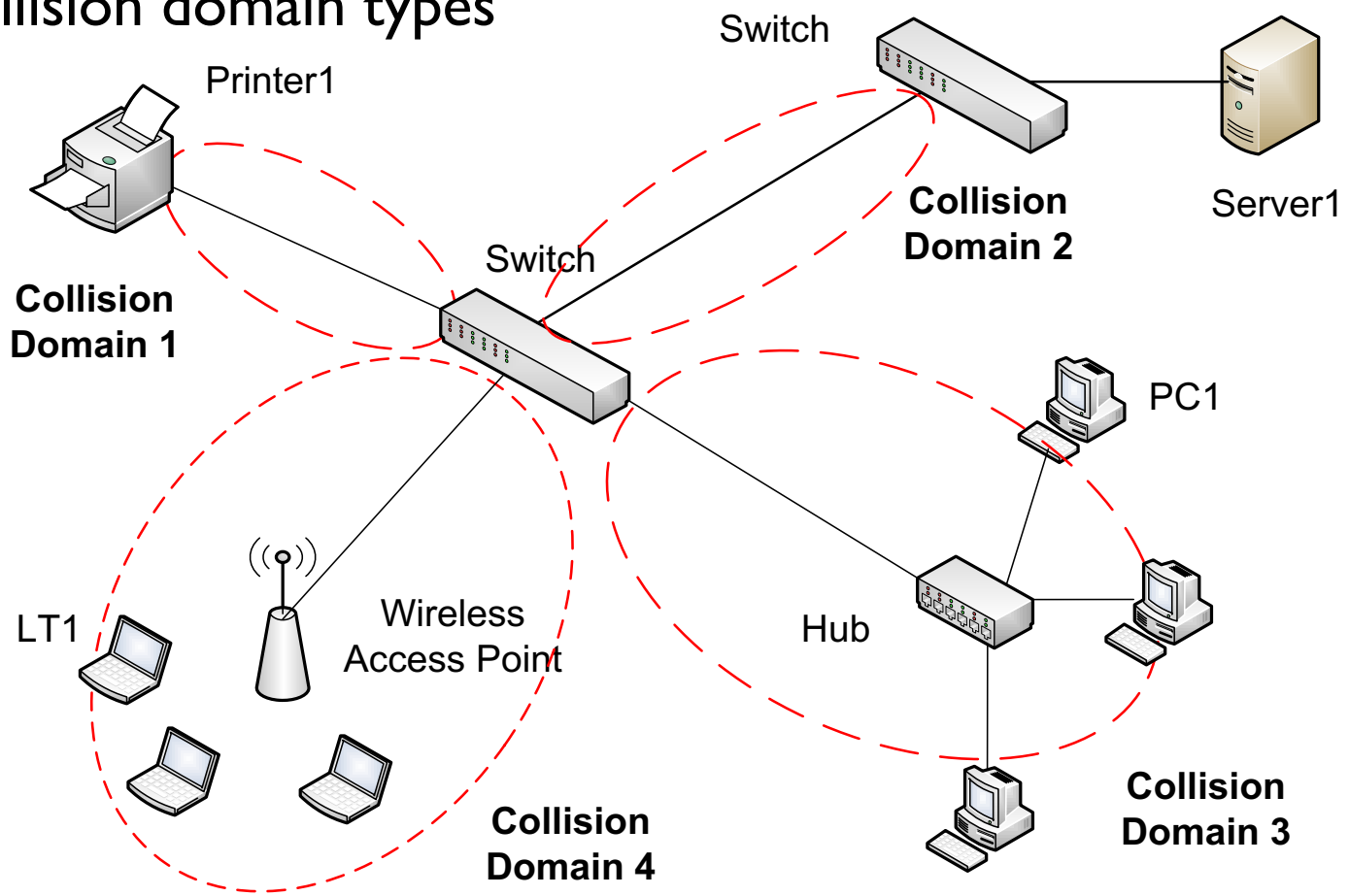


Figure 3.23 Types of collision domain

3.10 Collision vs. Broadcast Domains

- Router as broadcast domain divider

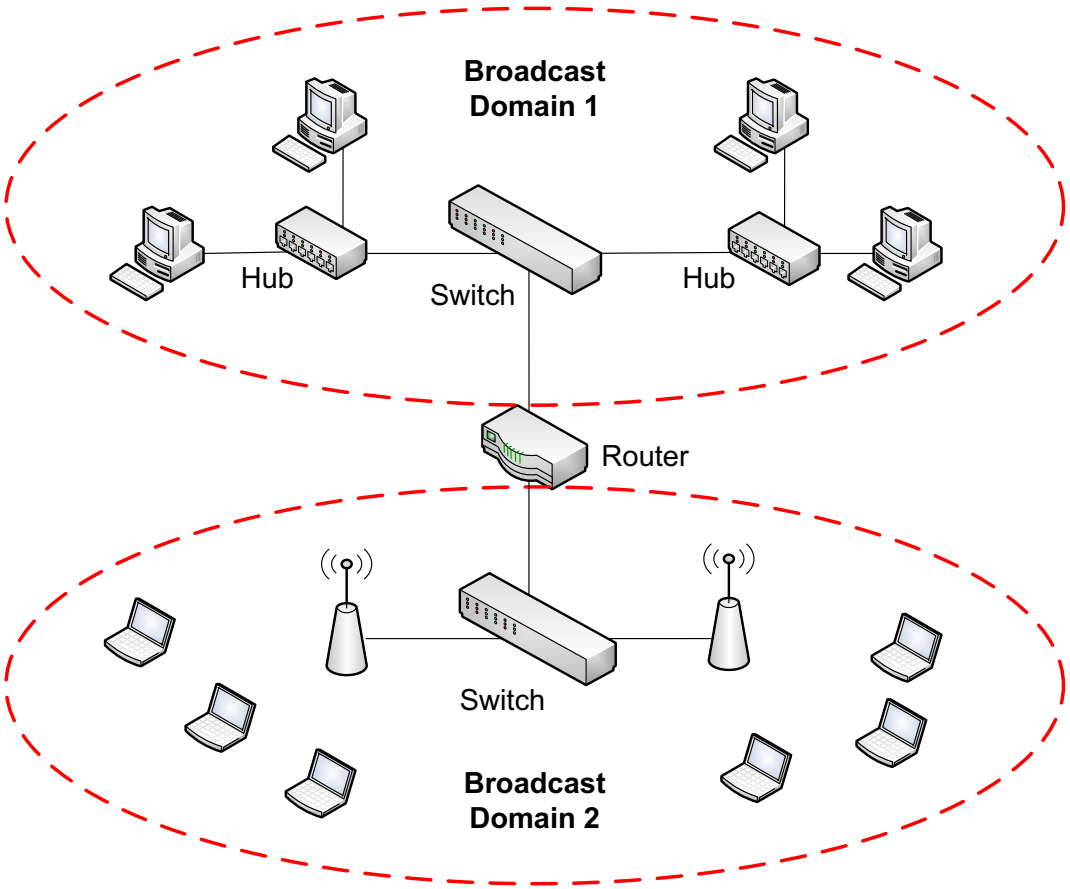
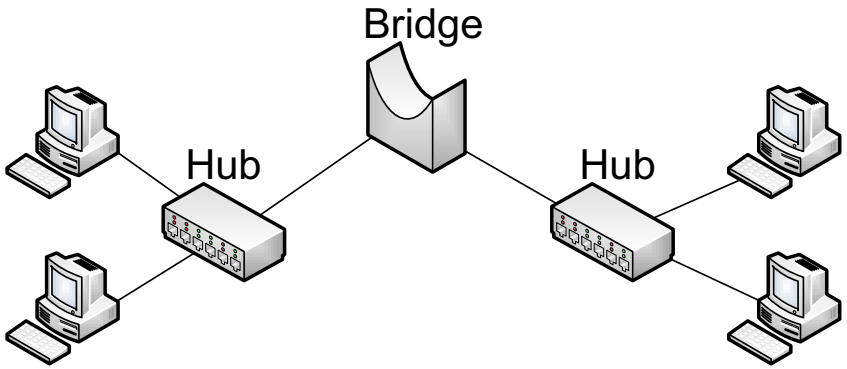
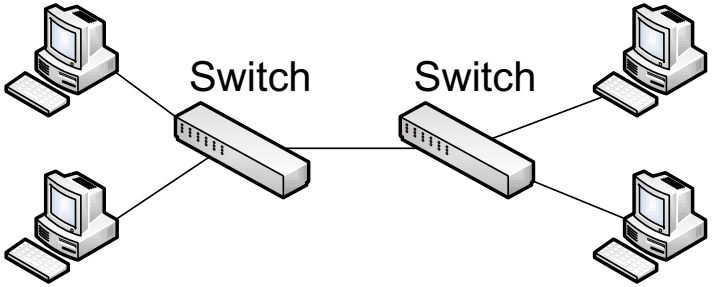
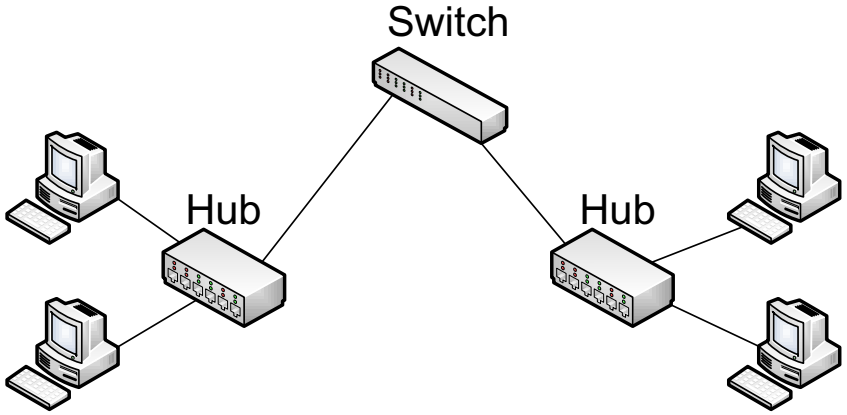


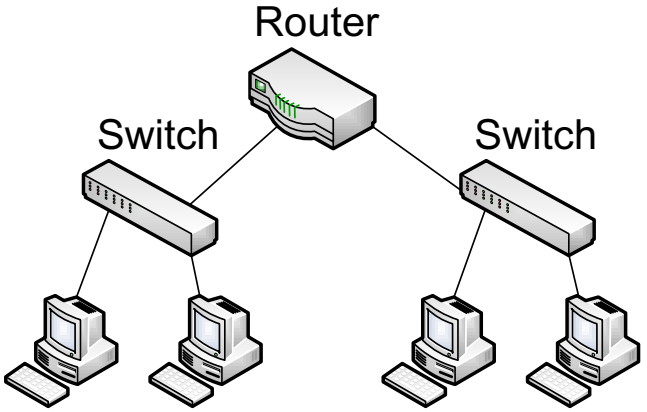
Figure 3.24
Two broadcast domains

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

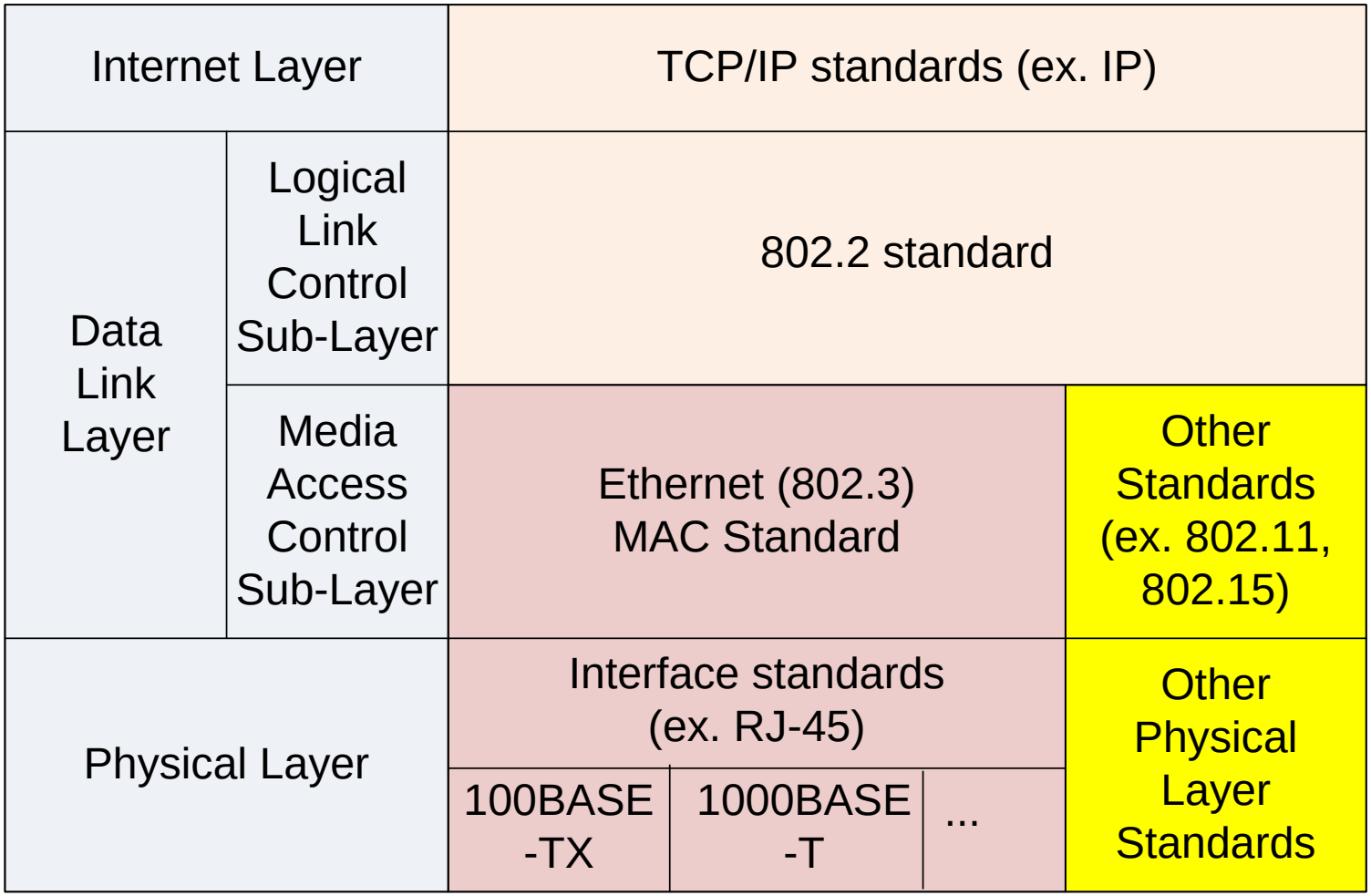


Figure 7.1 Layers of Ethernet (IEEE802.3) standard

7.3 ETHERNET Frame

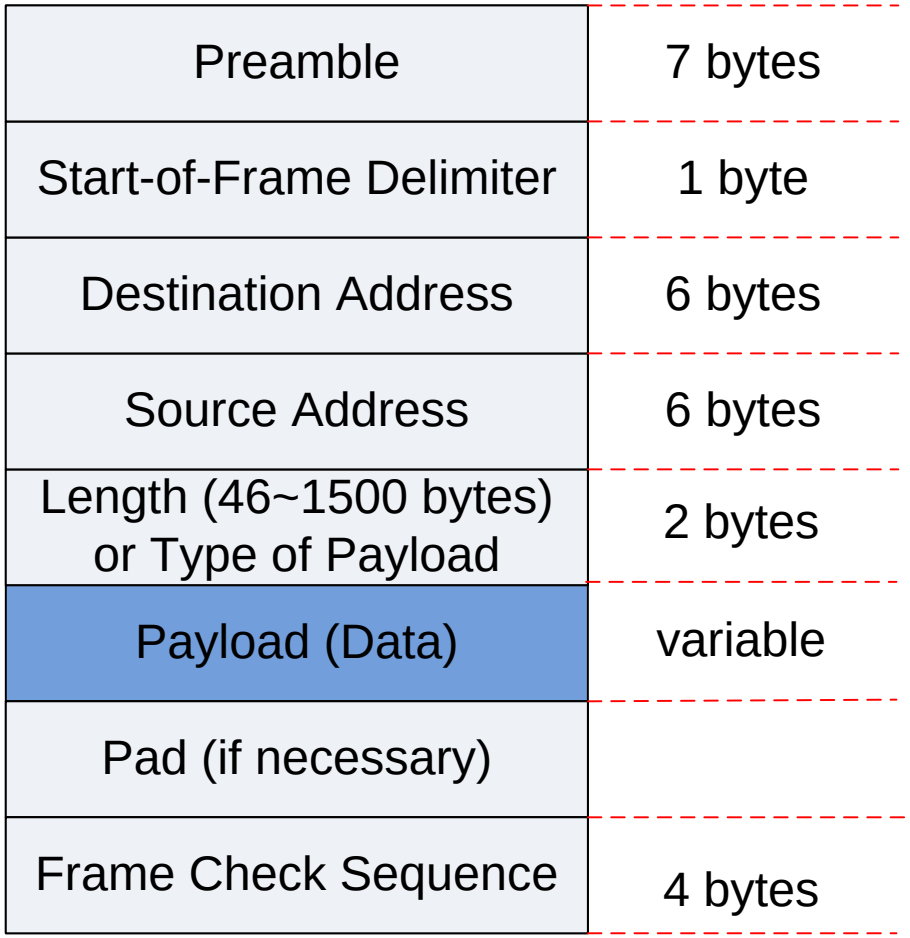


Figure 7.2 Ethernet frame

7.4 Ethernet LAN Design

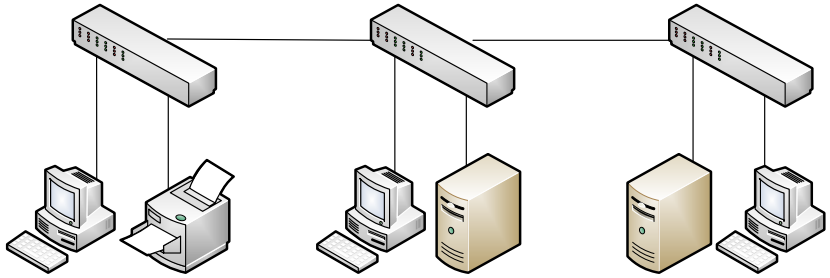


Figure 7.3 Ethernet with flat structure (logical view)

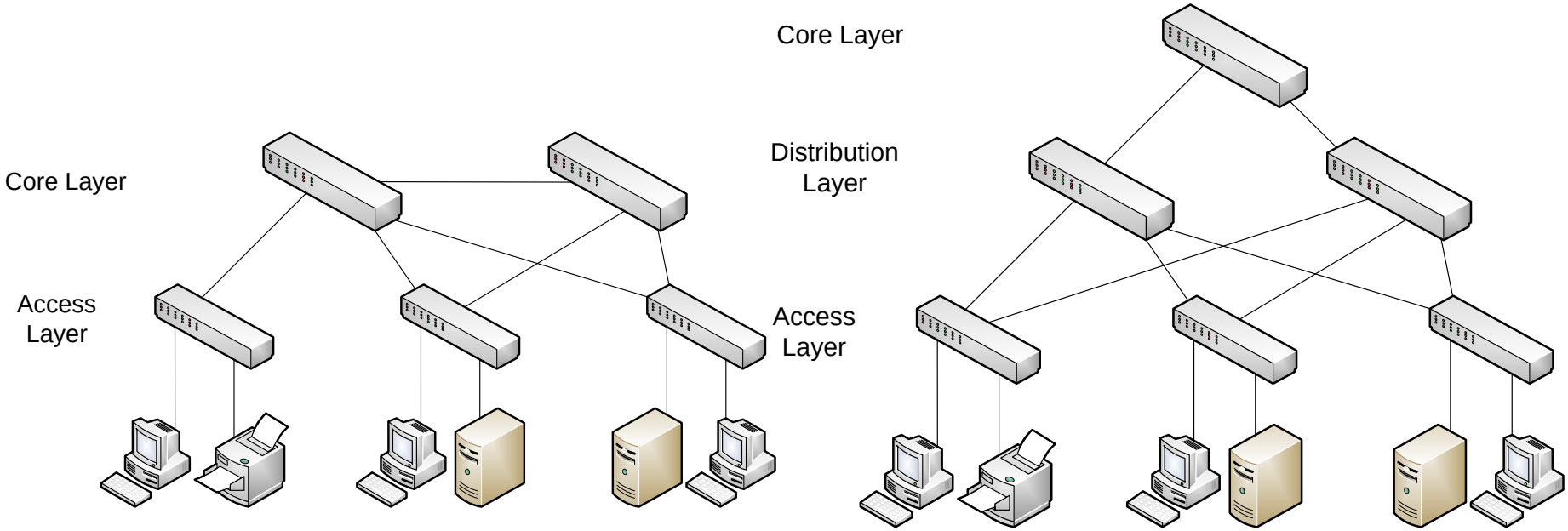


Figure 7.4 Two-tier vs. three-tier Ethernet LANs (logical view)

7.5 Spanning Tree Protocol (STP)

Link Redundancy

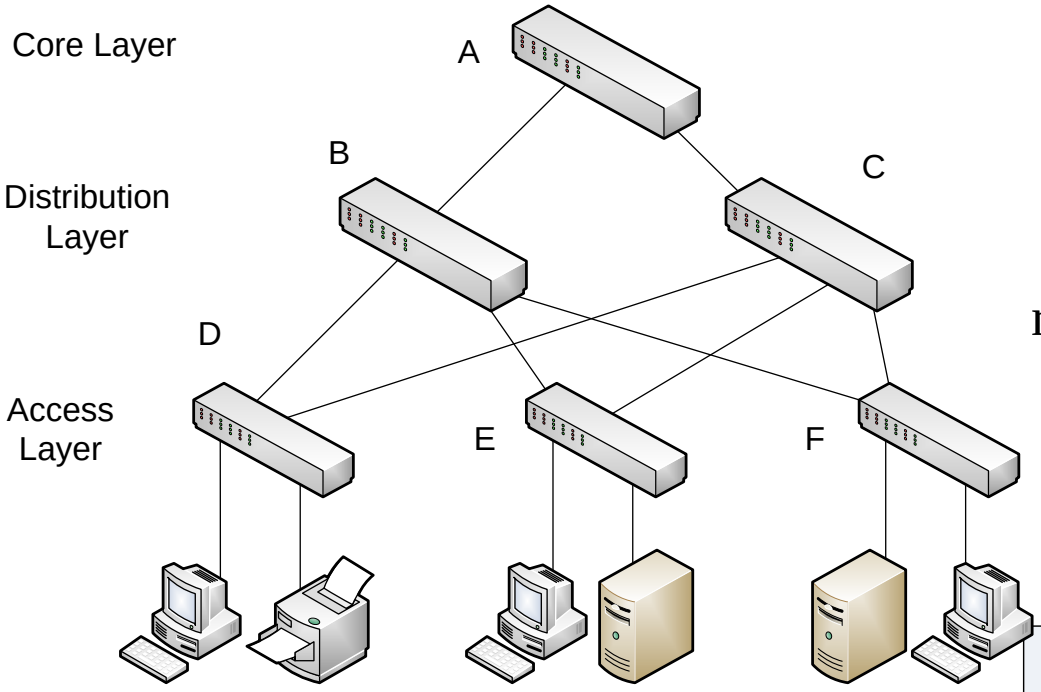


Figure 7.5 Availability of redundant paths (logical view)

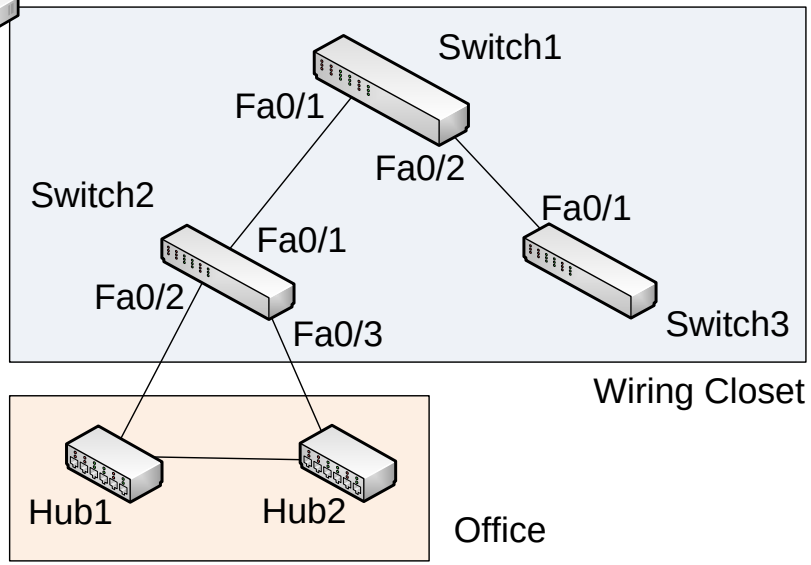


Figure 7.6 Network redundancy created at a work area

7.5 Spanning Tree Protocol (STP)

7.5.2 Protocols and Mechanism

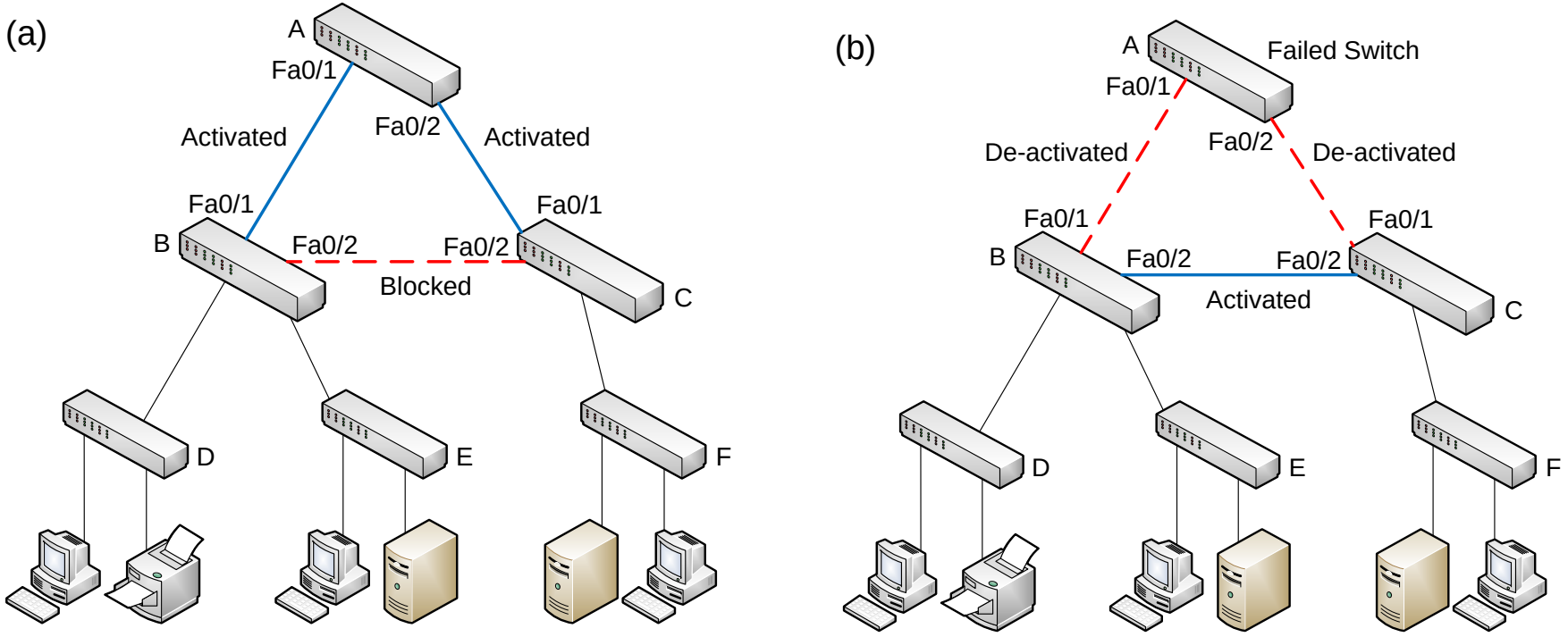


Figure 7.7 Demonstration of STP/RSTP (logical view)

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

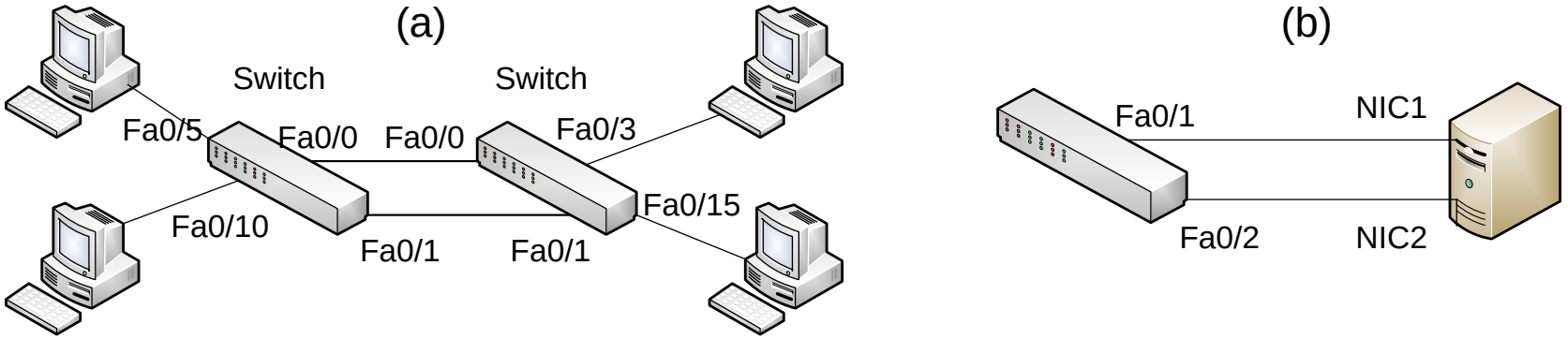


Figure 7.8 Usage of link aggregation

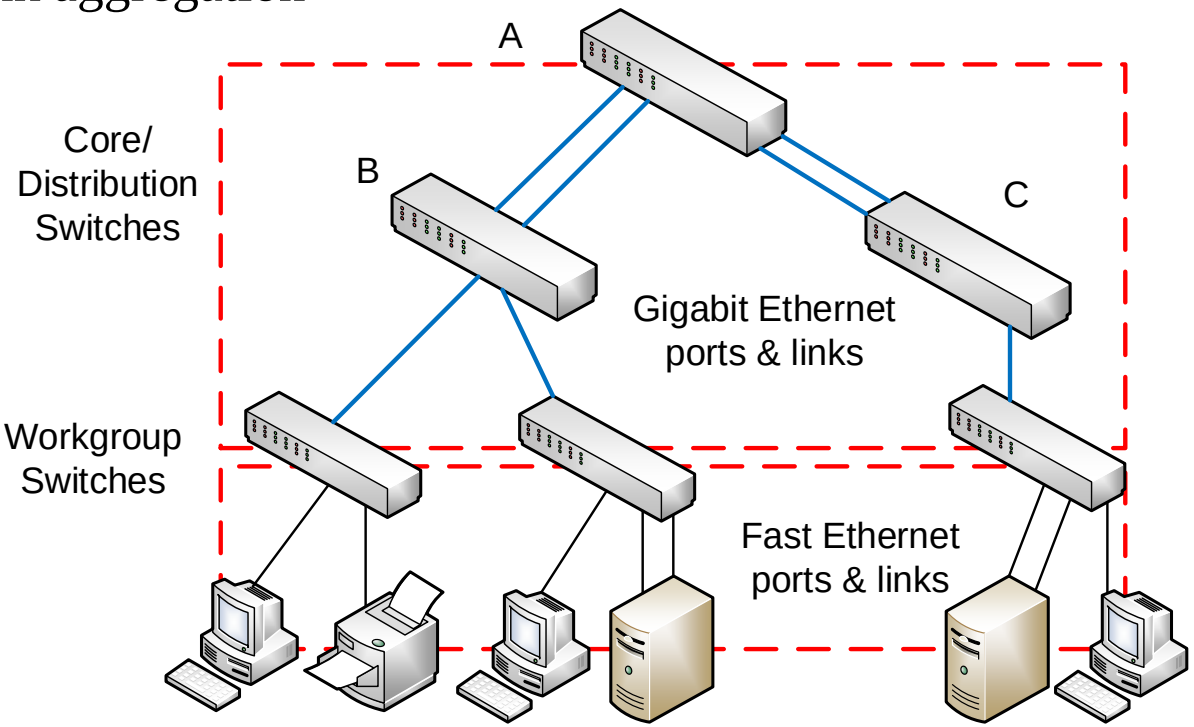


Figure 7.9
Link aggregation scenario

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

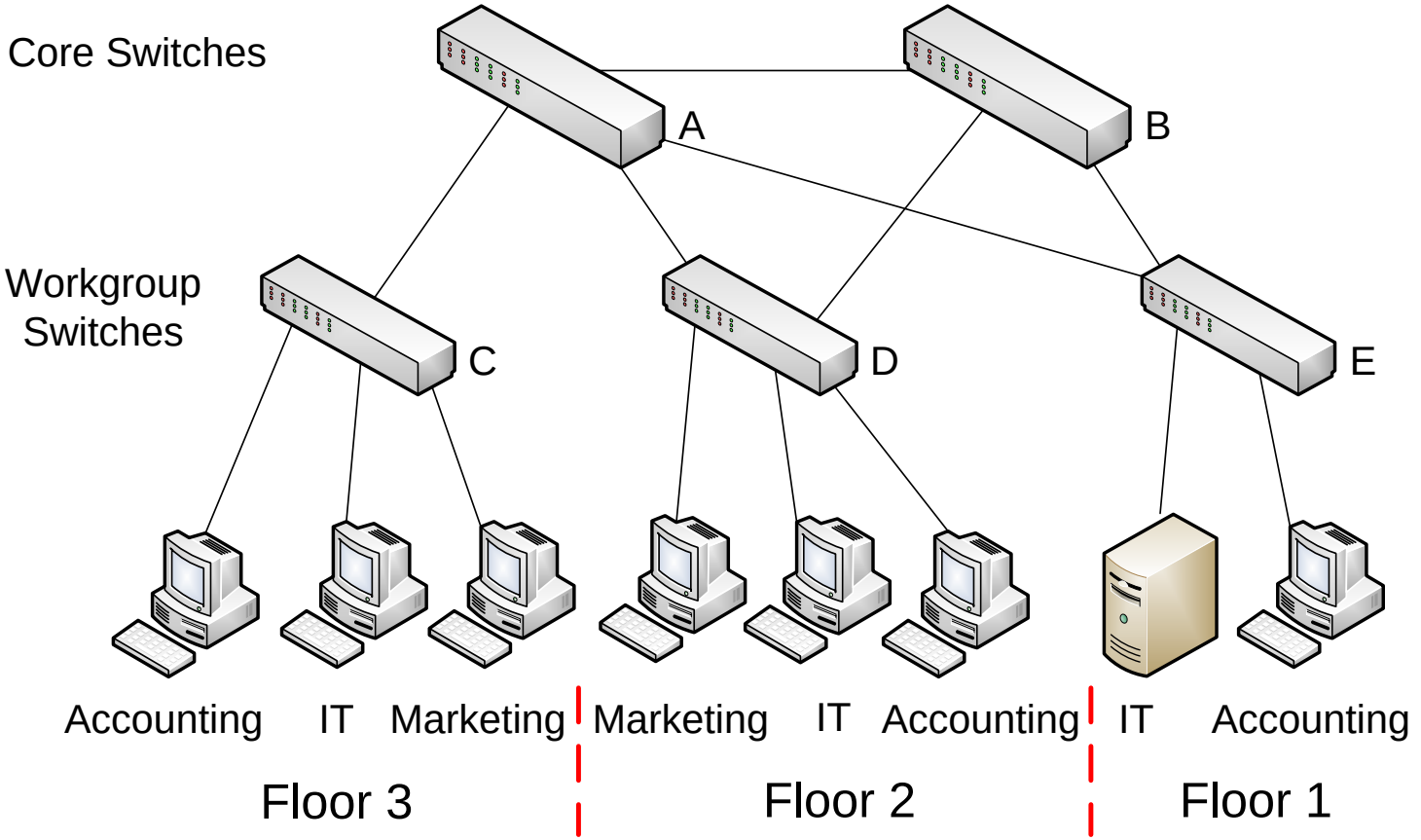


Figure 7.11 Logical layout of a LAN

7.7 Virtual LANS (VLANS)

7.7.1 Background: Without VLANs

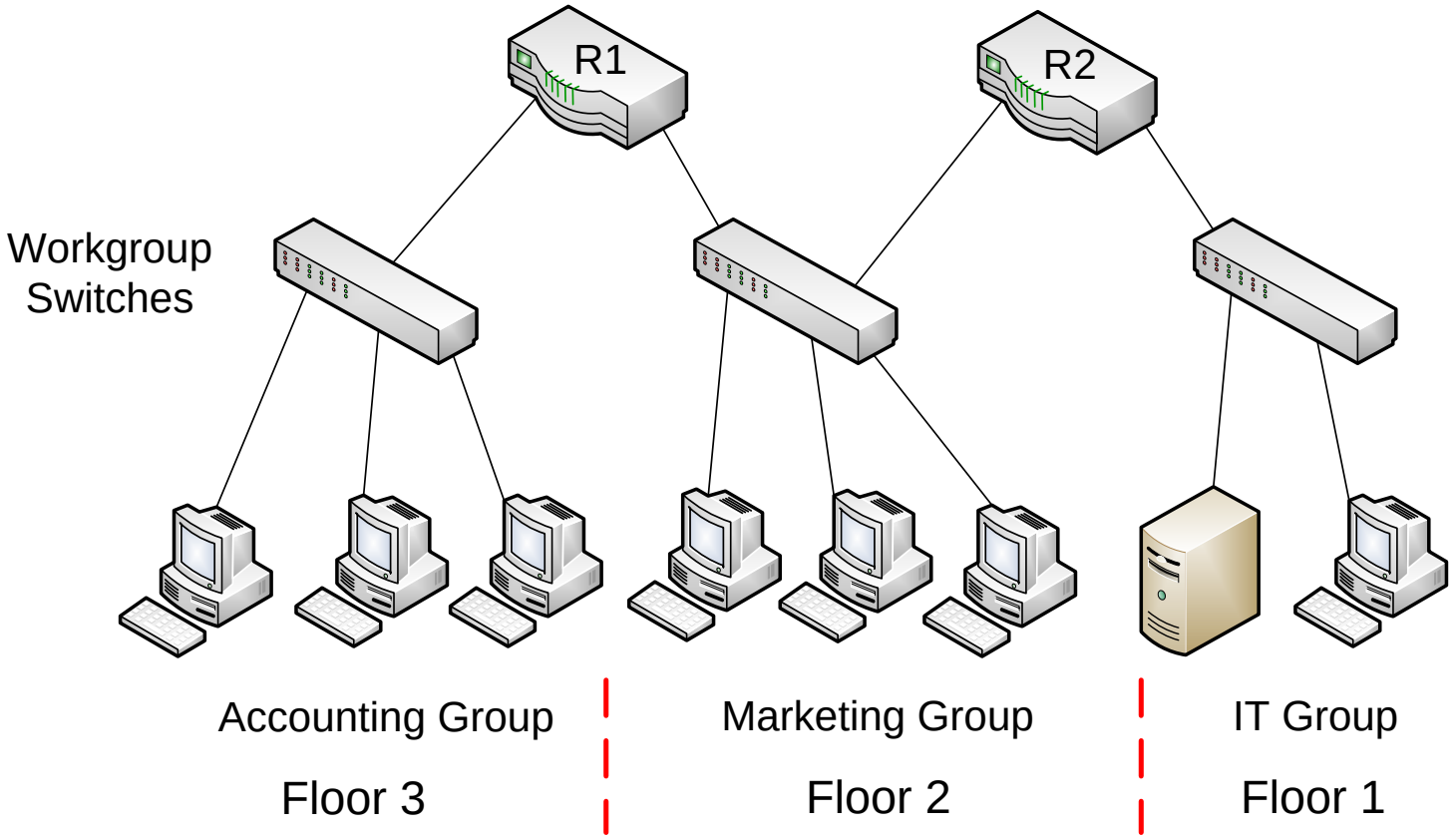


Figure 7.12 Router-based segmentation of a LAN

7.7 Virtual LANS (VLANS)

7.7.2 VLAN Concept

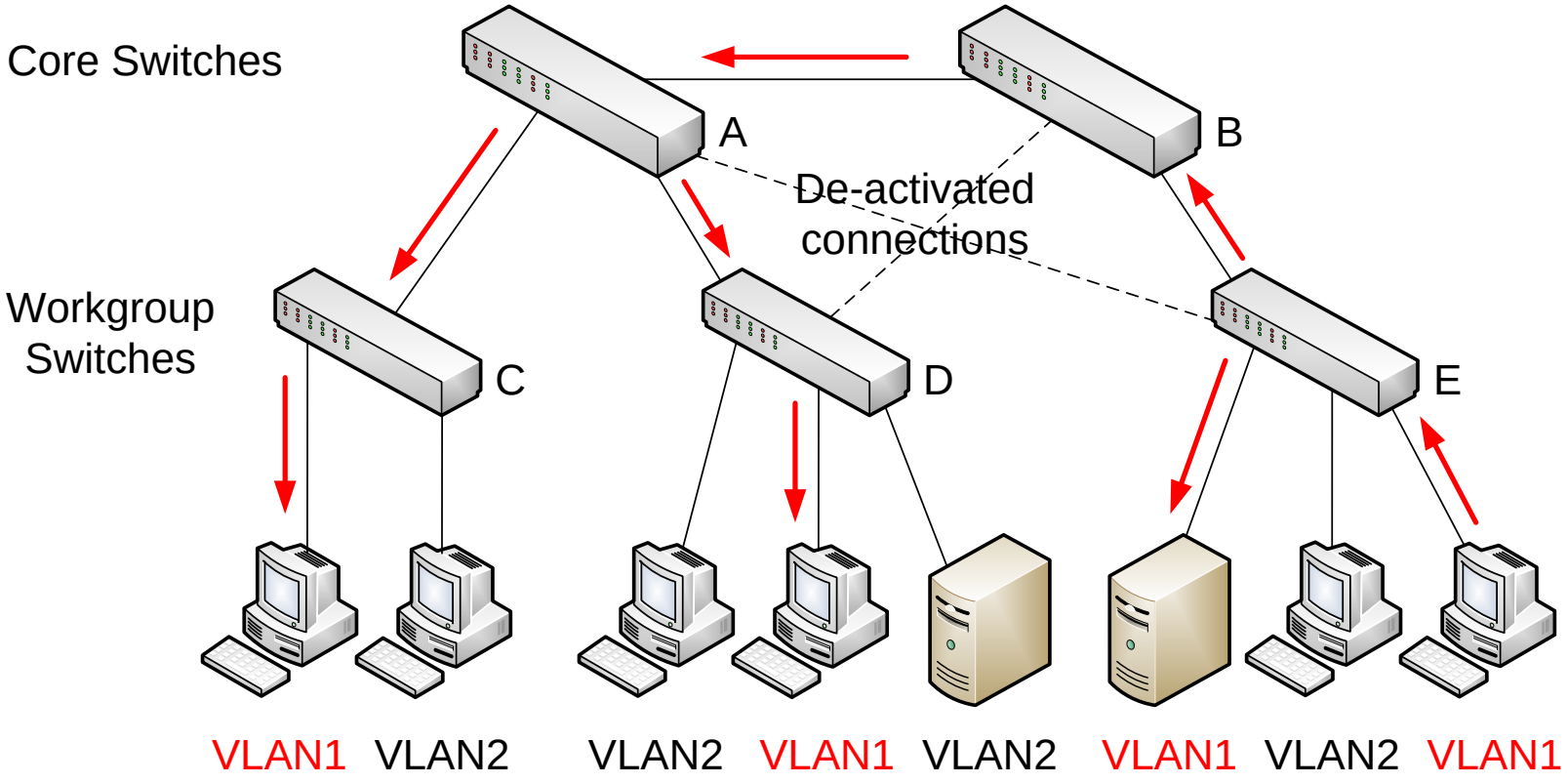


Figure 7.13 Broadcasting to nodes of a VLAN

7.8.1 Without VLANs

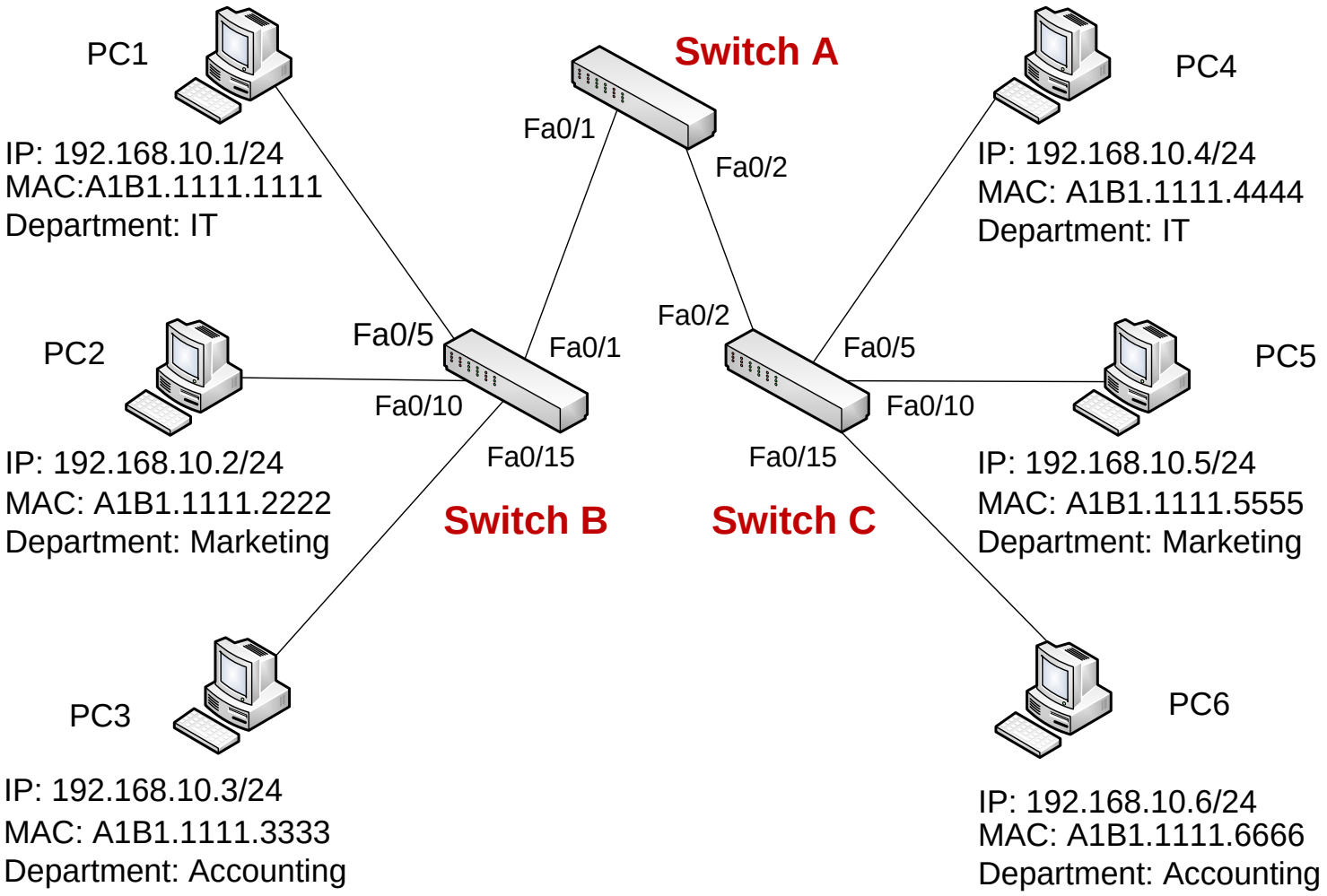
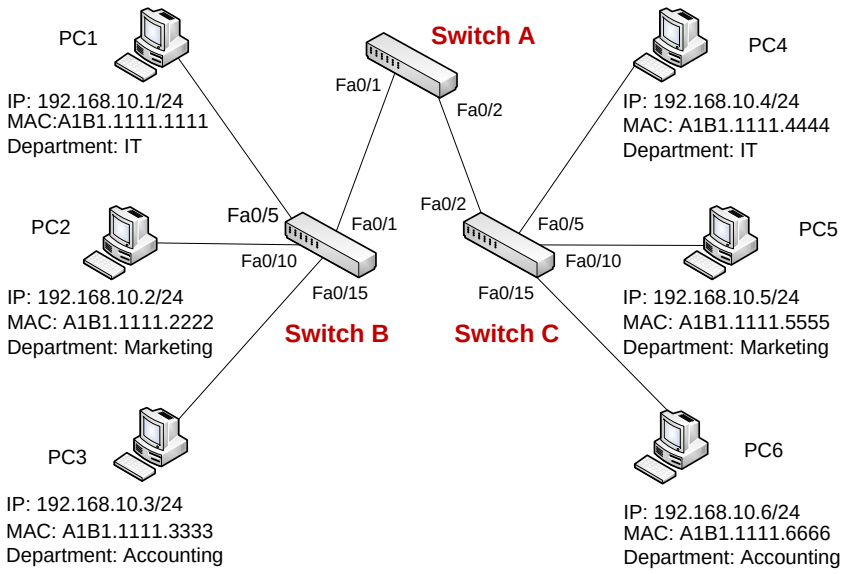


Figure 7.14 A hypothetical switched LAN

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

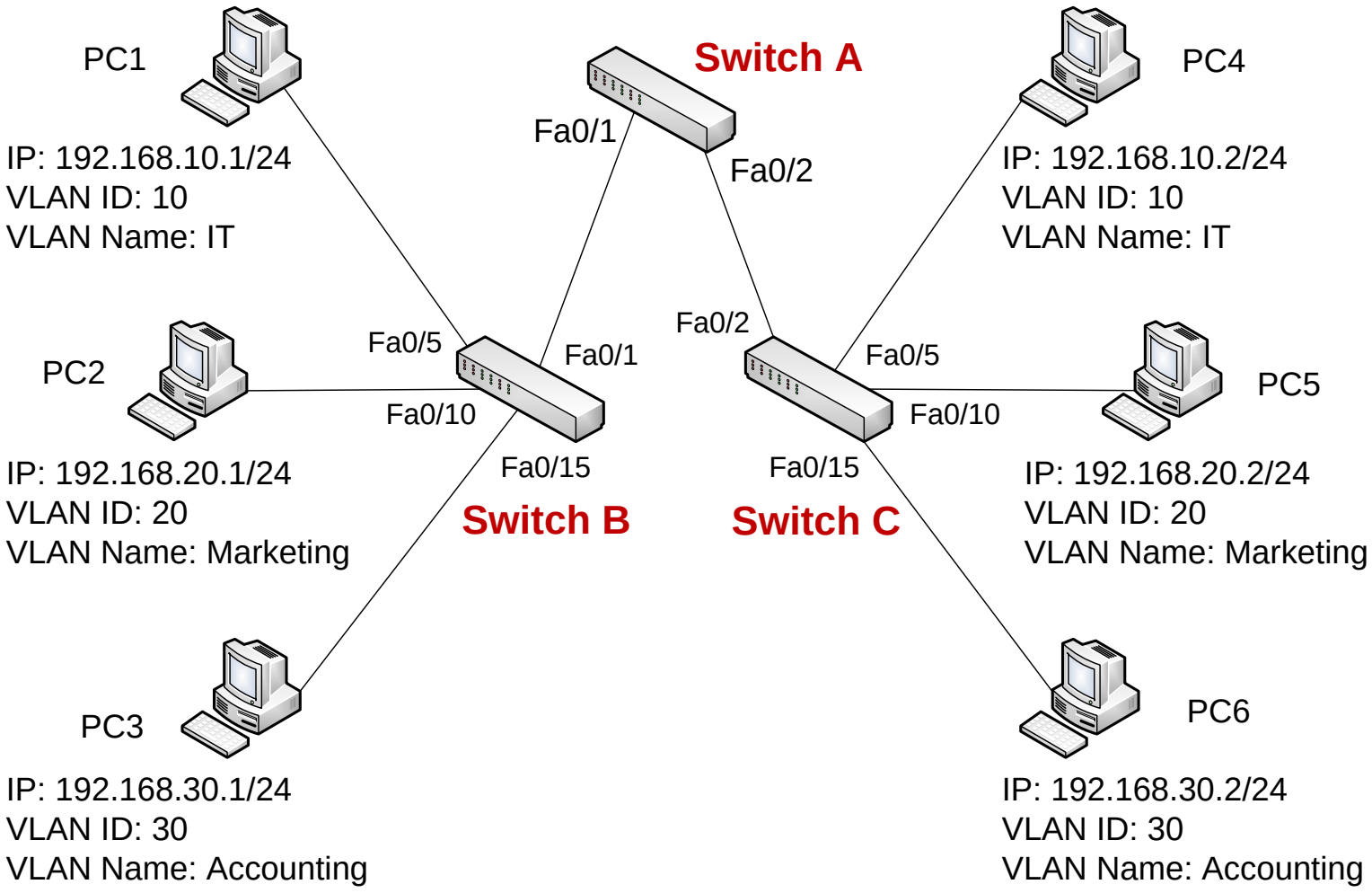
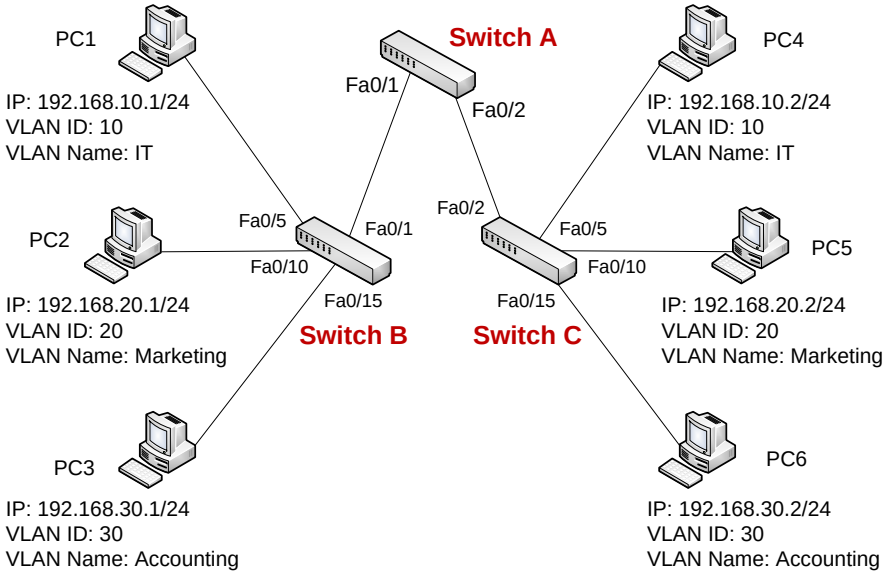


Figure 7.15 A switched LAN with three VLANs

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)

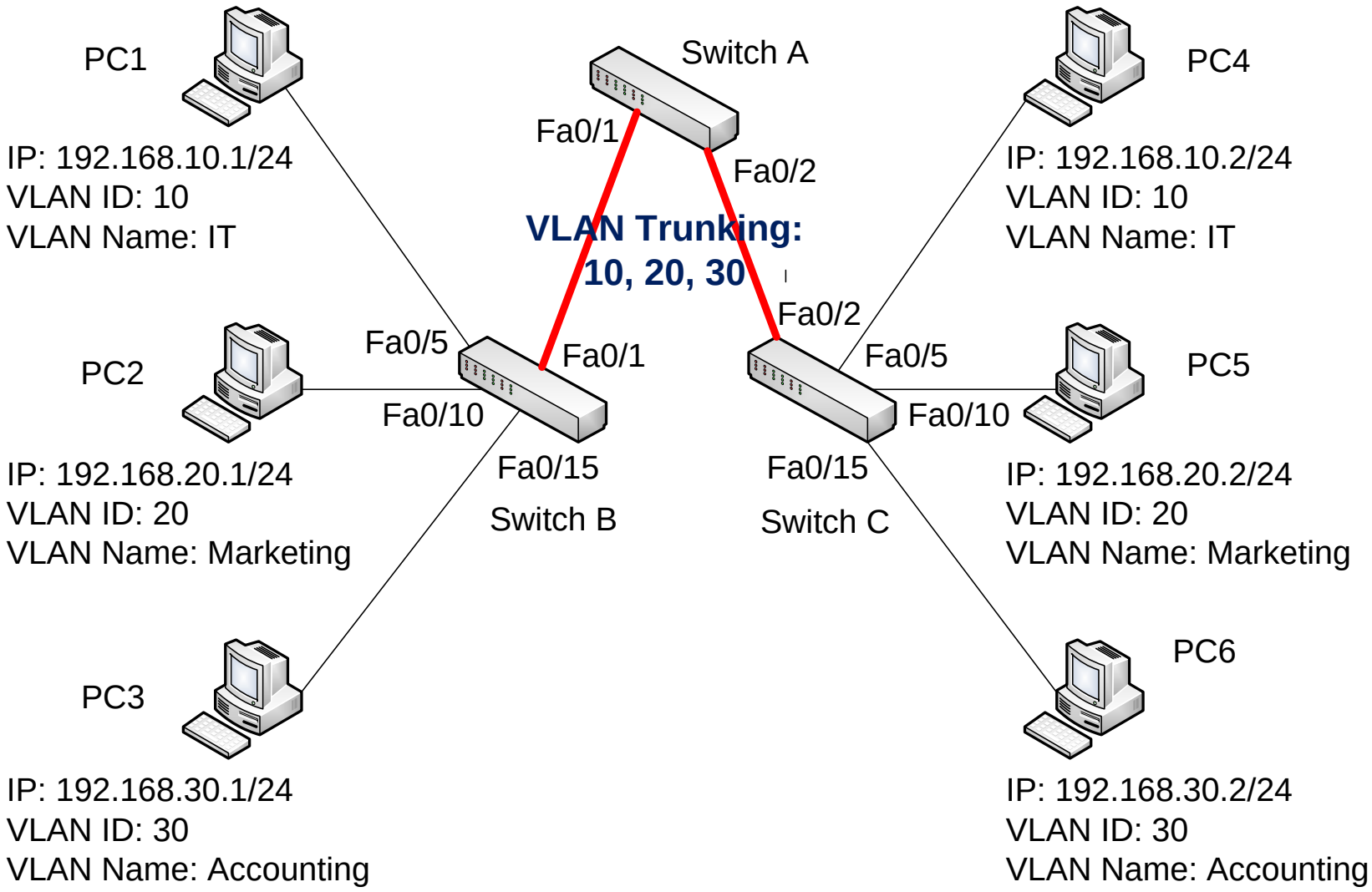


Figure 7.16 VLAN trunking

7.9.2 VLAN Tagging

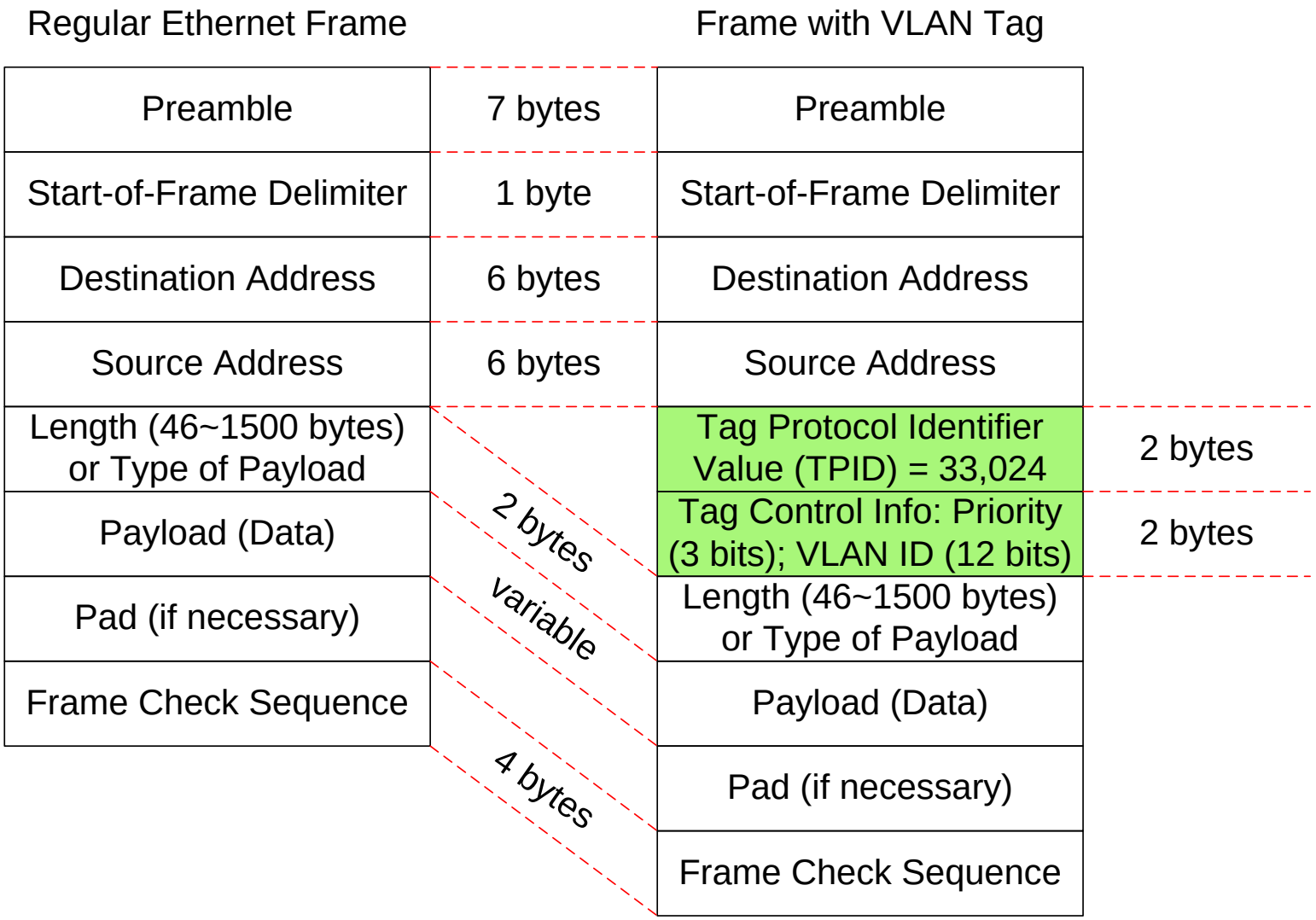


Figure 7.17 Ethernet frames: regular vs. VLAN tagged

7.9.3 VLAN Tagging/Untagging Process

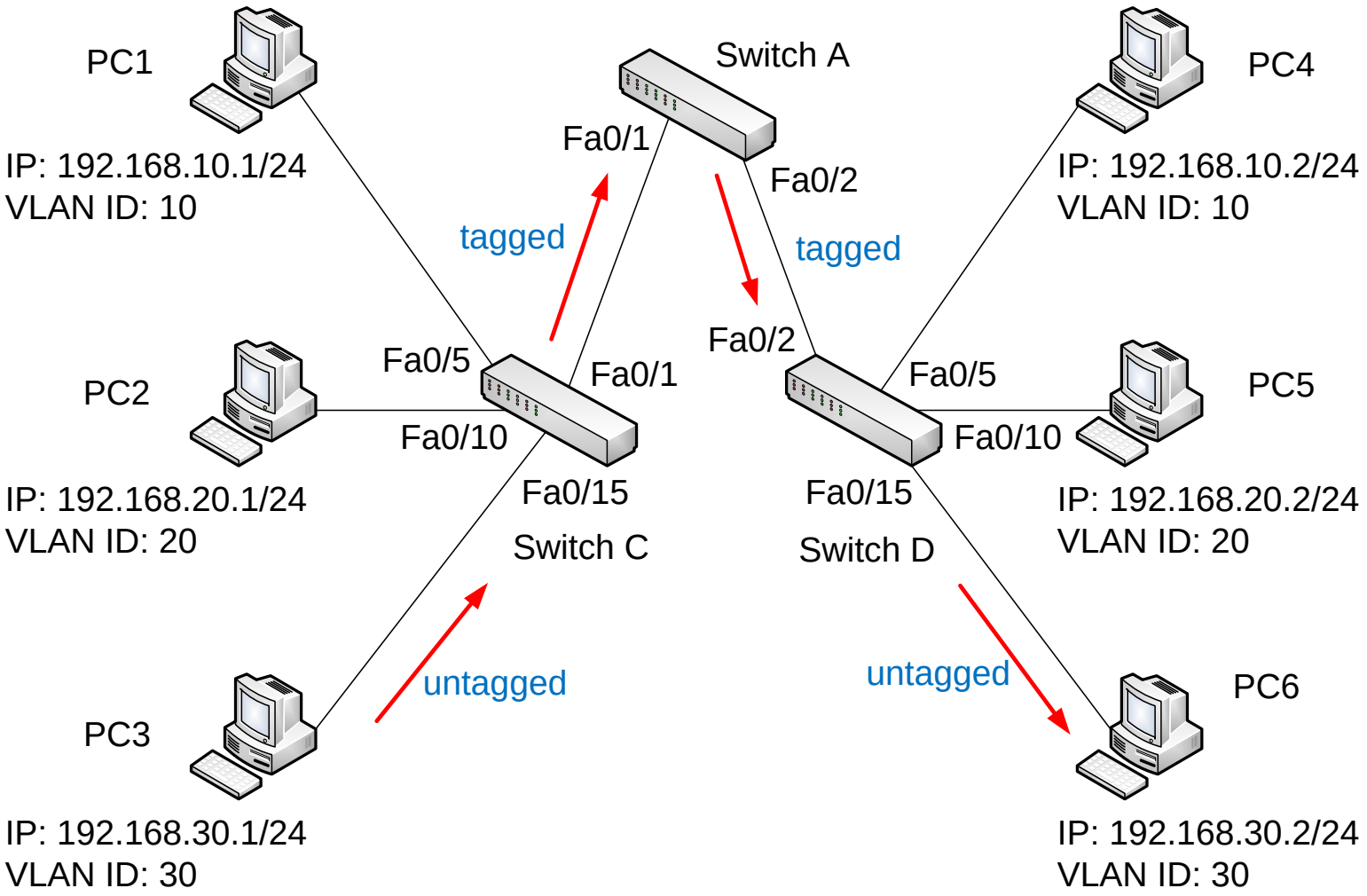


Figure 7.18 VLAN tagging and untagging

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

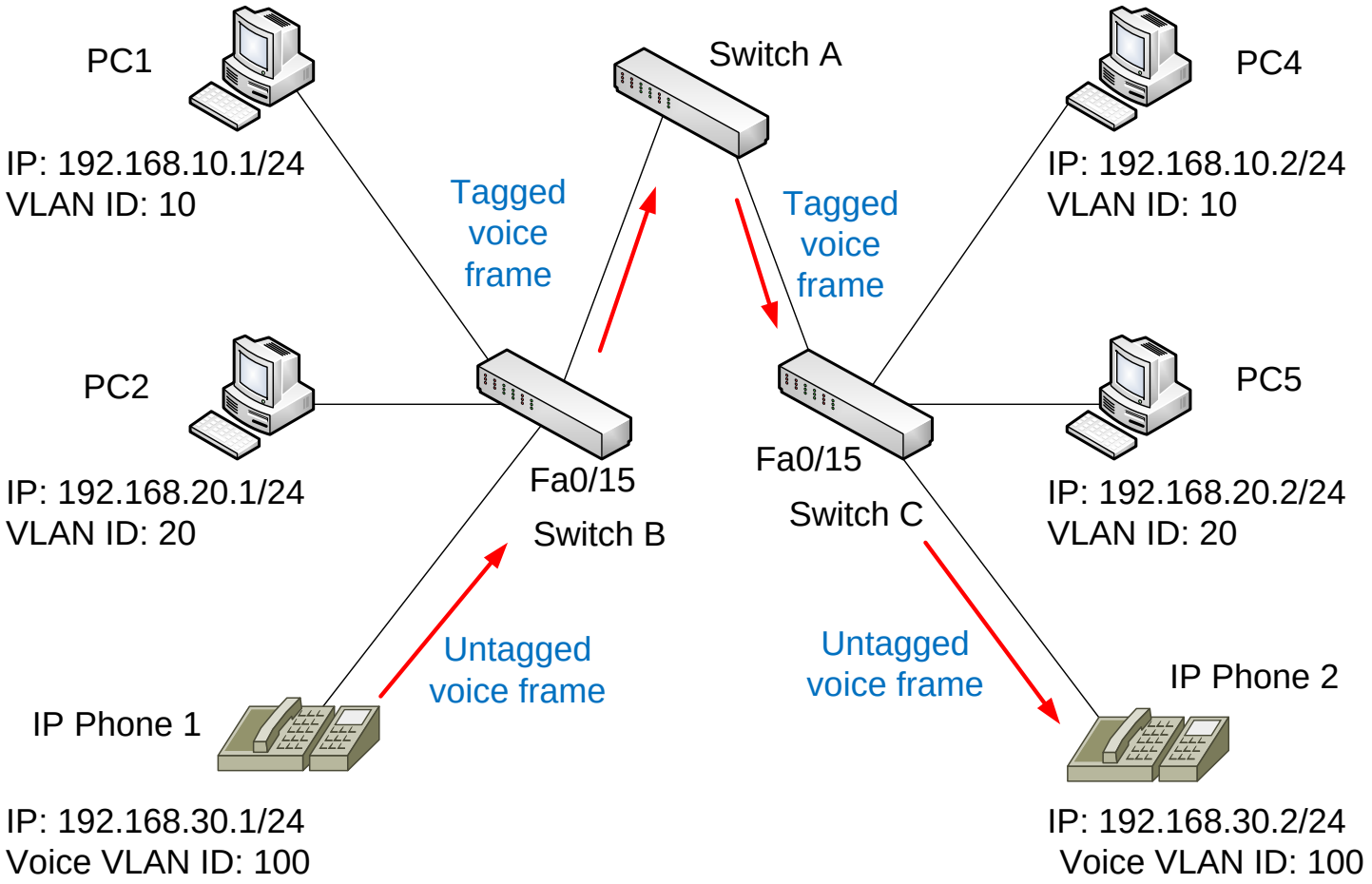
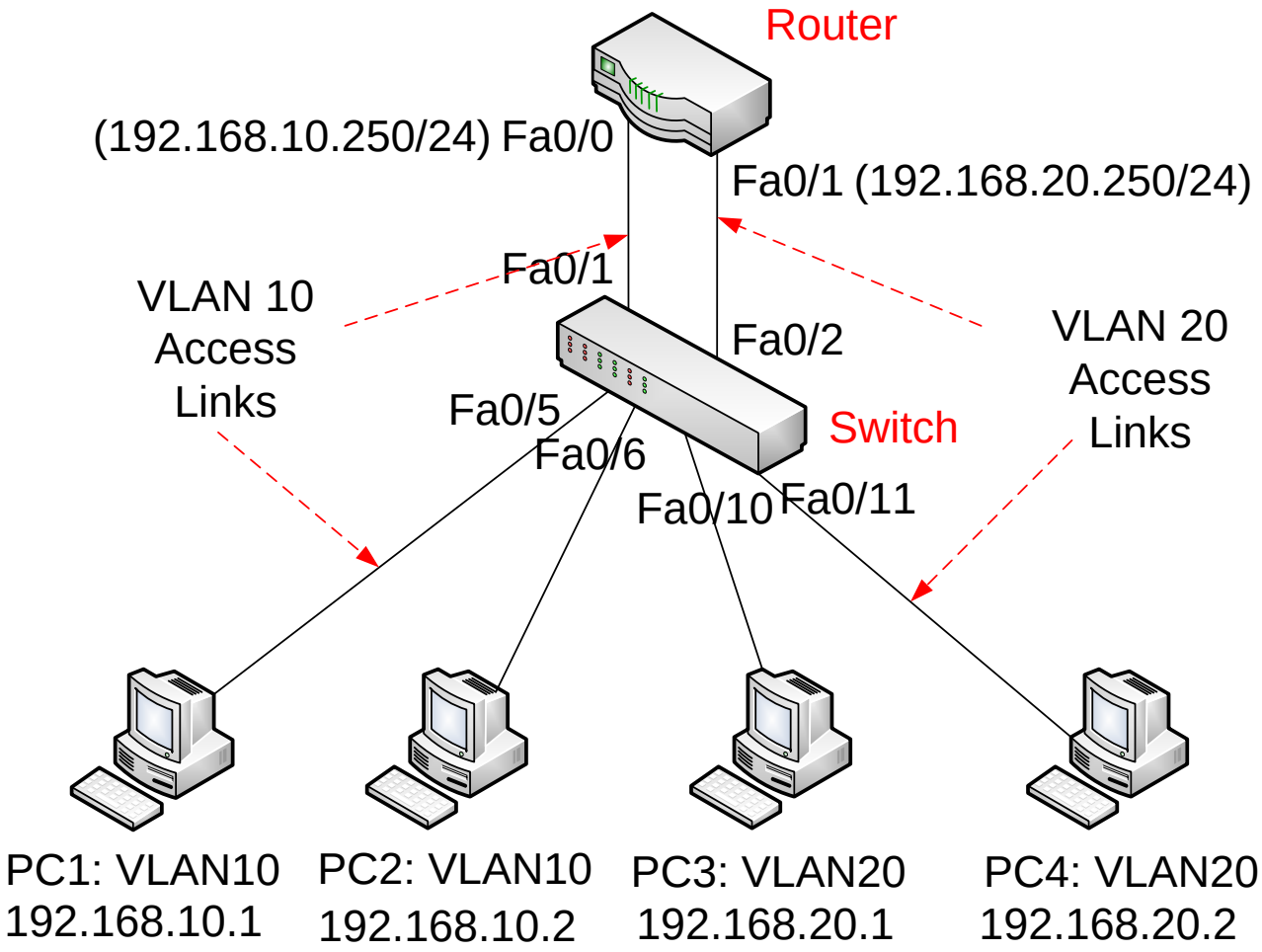


Figure 7.21 Demonstration of Voice VLAN

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

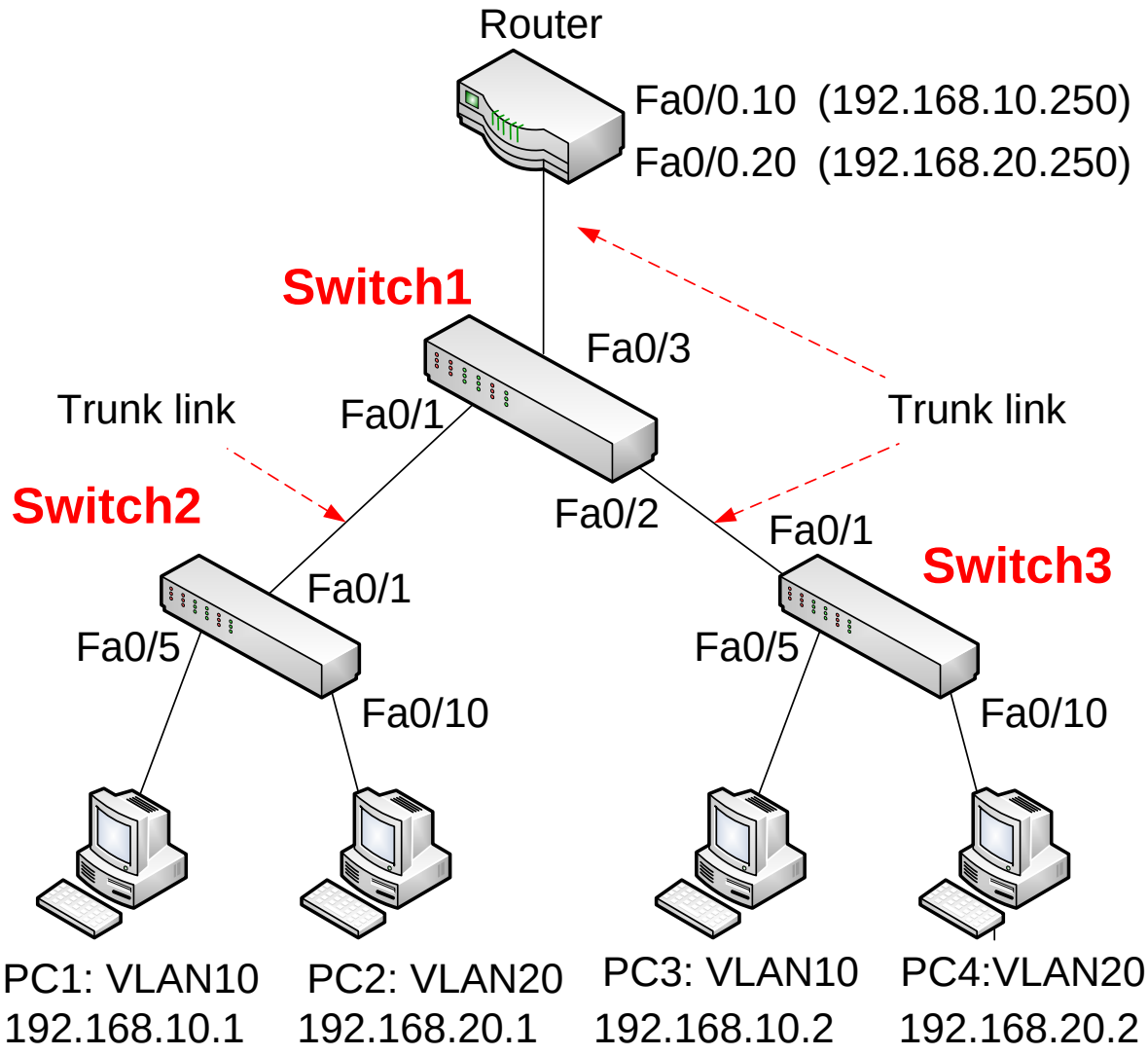


Figure 7.25
Inter-VLAN routing with sub-interfaces

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

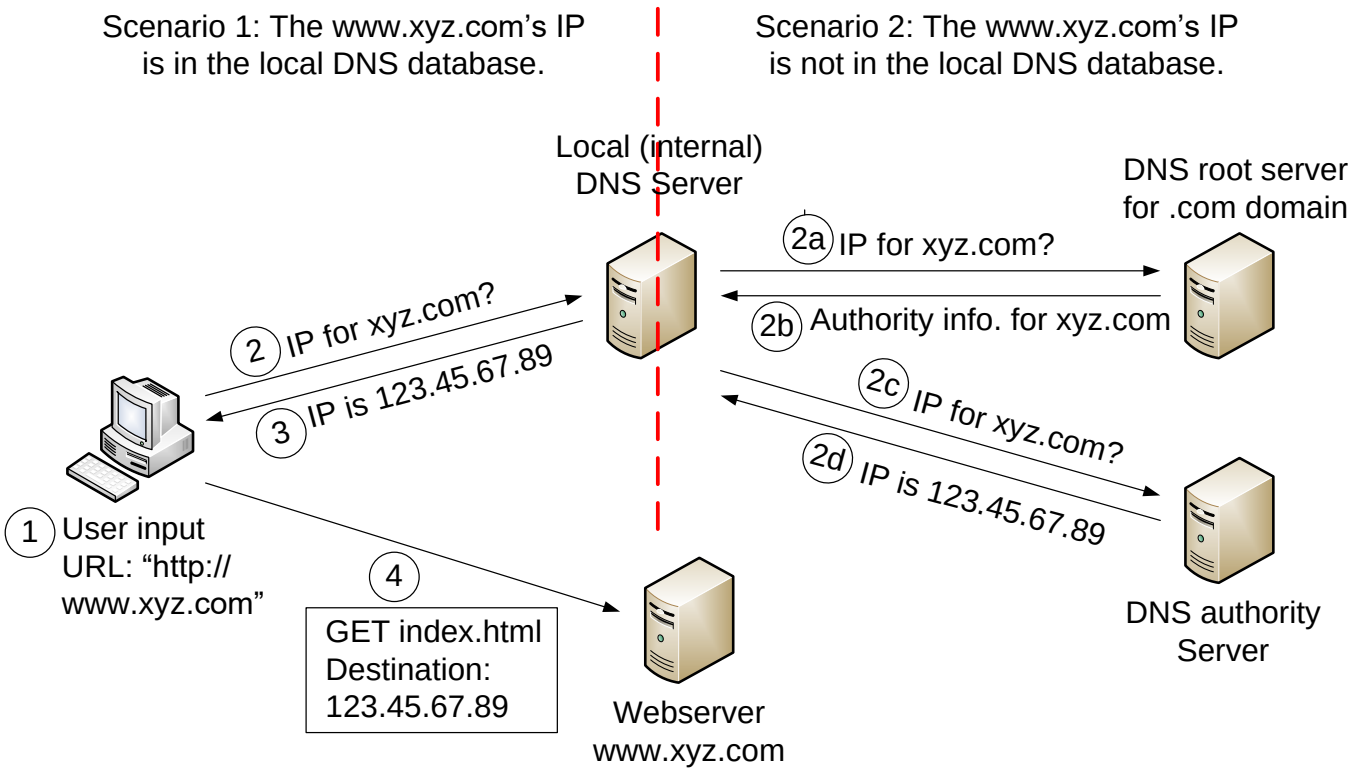


Figure 10.18

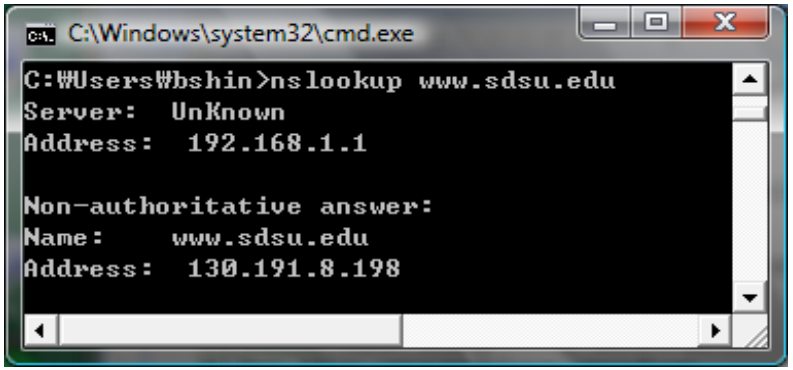


Figure 10.19 Sample *nslookup* inquiry

10.5 Client-Server Model

10.5.3 DHCP (Dynamic Host Configuration Protocol)

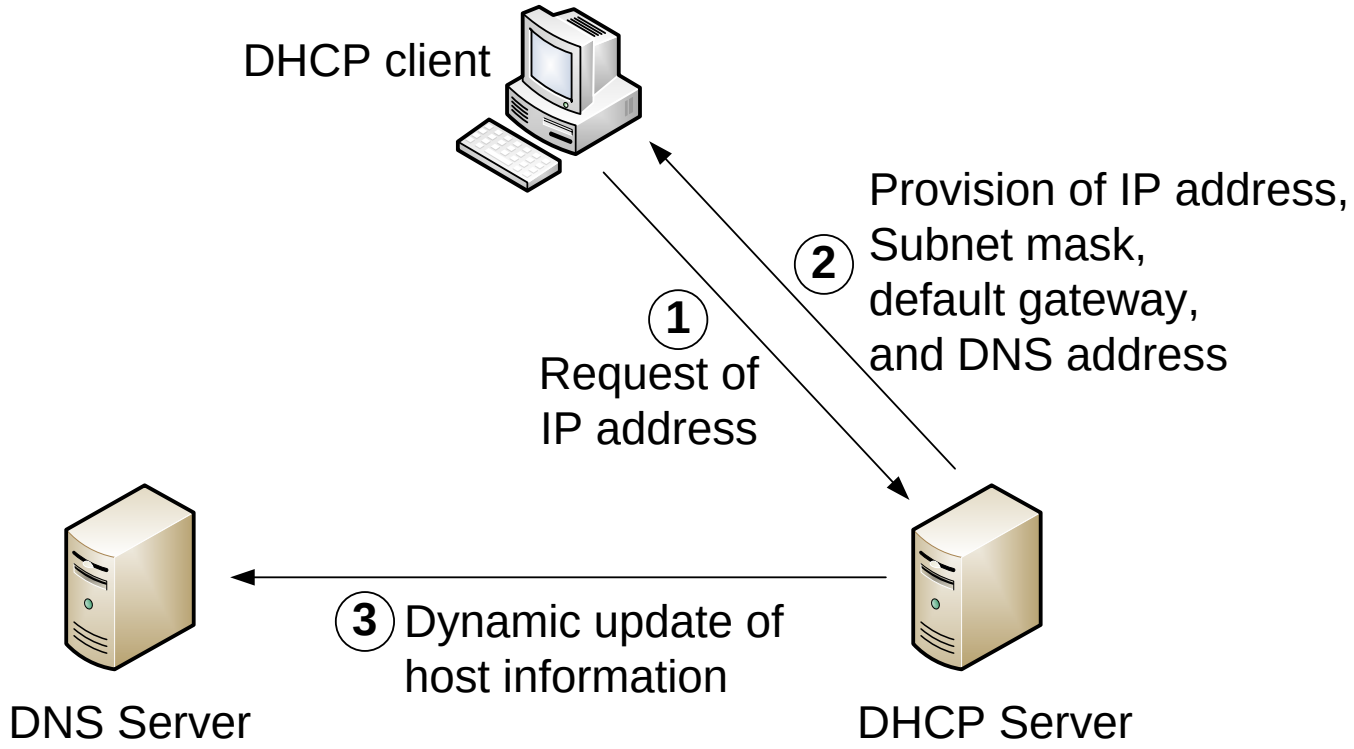


Figure 10.23 DHCP and dynamic IP assignment

CECS 303 Networks and Networks Security

IP Address Planning and Management Chapter 5

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

5.2 GOVERNANCE OF IP ADDRESS SPACE

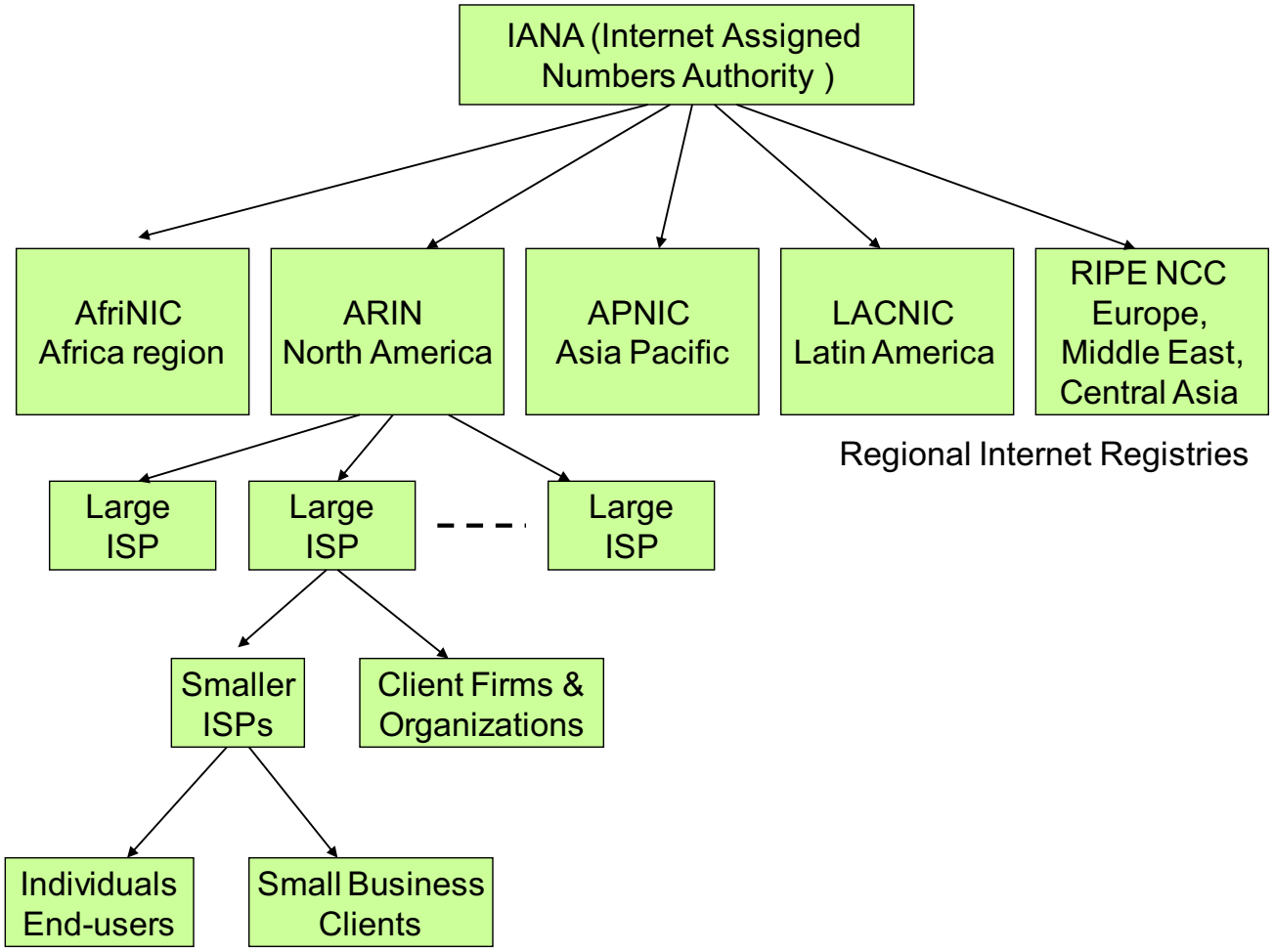


Figure 5.1 Delegation of IP address space

5.3 STRUCTURE OF THE IP ADDRESS

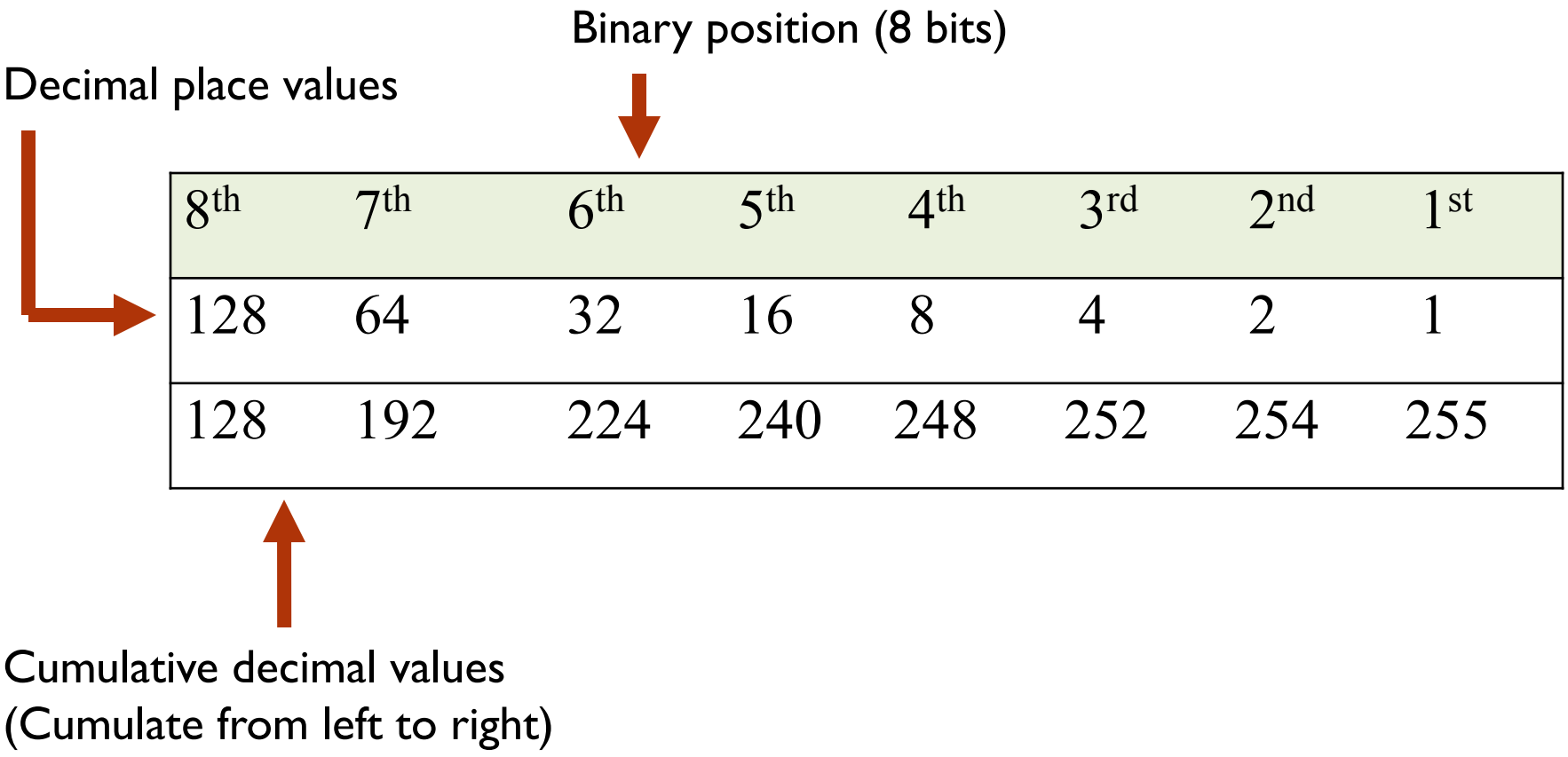


Table 5.1 Binary vs. decimal value conversion table

5.3 STRUCTURE OF THE IP ADDRESS

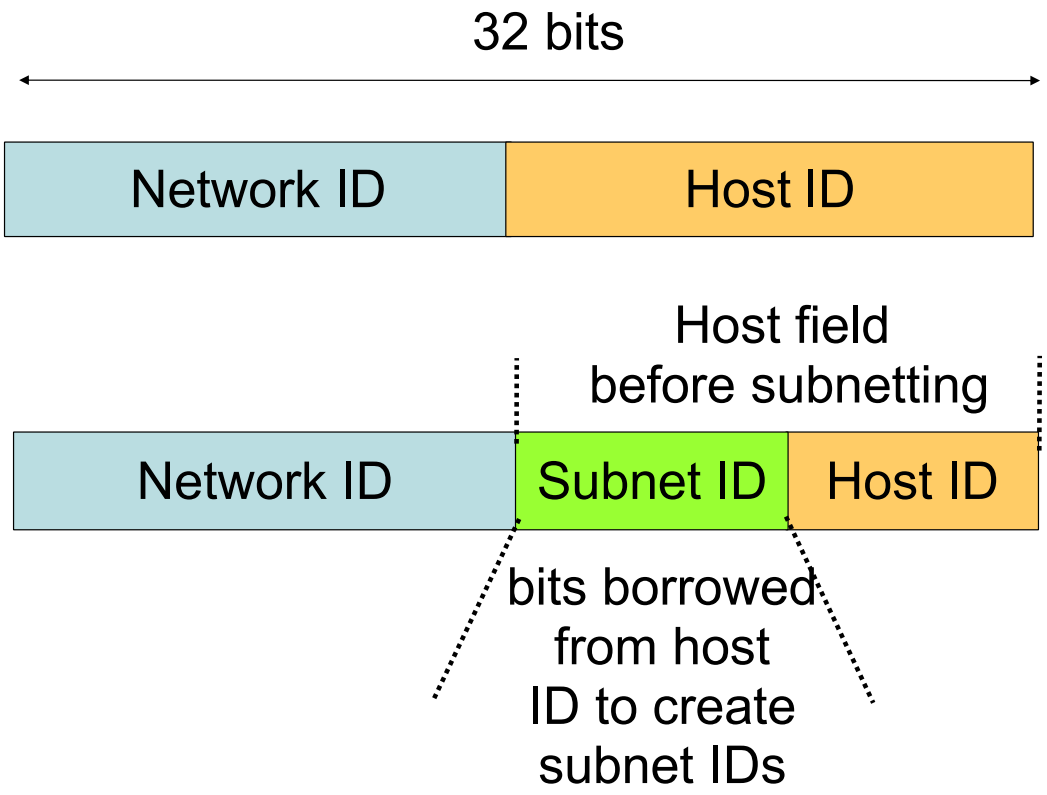


Figure 5.2 IPv4 address (without and with subnet ID)

5.4 CLASSFUL IP – LEGACY

Class	Initial bit(s)	Network ID	Host ID	Possible number of nodes
A	0.....	8 bits	24 bits	2^{24}-2 = about 16.7 million
B	10.....	16 bits	16 bits	2^{16}-2 = 65,534
C	110.....	24 bits	8 bits	2^{8}-2 = 254
D (Multicast)	1110.....	N/A	N/A	N/A

Table 5.2 Classful allocation of IP space

5.5 CLASSLESS IP - TODAY

- The network ID is not a multiple of an octet (i.e., 8 bits, 16 bits, or 24 bits)
- Search network ID at *www.arin.com*
- Some organizations have returned their allocated 'class A' IP to Internet registries.
  - Ex. Stanford University: formerly 36.0.0.0/8

5.6 SPECIAL IP ADDRESS RANGES

- Loopback:
  - 127.0.0.0 ~ 127.255.255.255
  - To send packets addressed to itself
- Broadcasting & multicasting
- Private IP:
  - For internal usage
  - Packets with private IPs are not routable over the Internet

5.6.1 Loopback (127.0.0.0 ~ 127.255.255.255)

- Internal testing of TCP/IP stack
- Offline application testing
- Corresponding domain name is Localhost

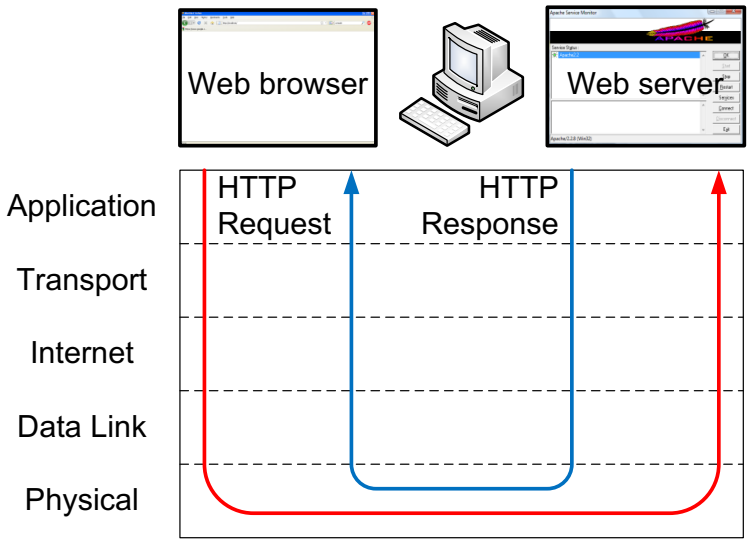


Figure 5.4 Internal client-server communication with a loopback IP

5.6.2 Broadcasting

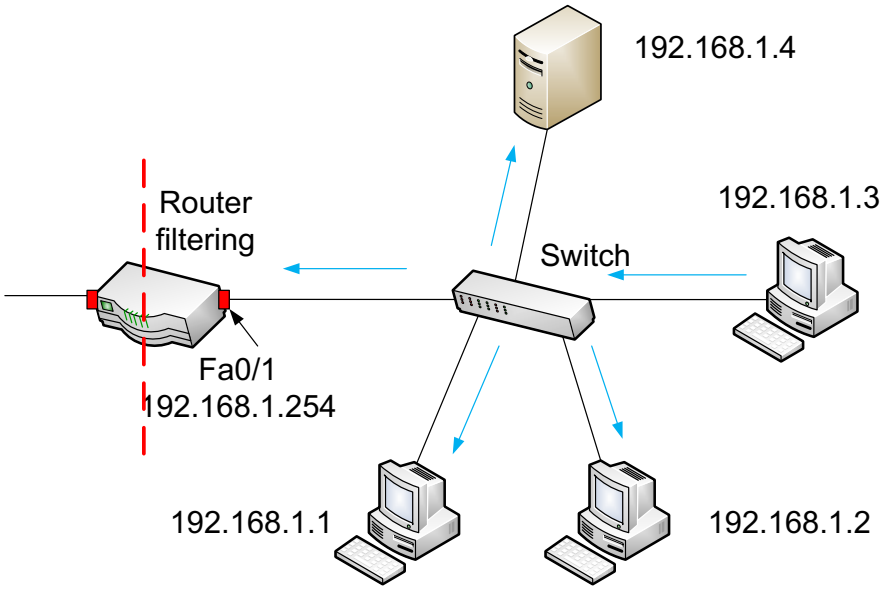
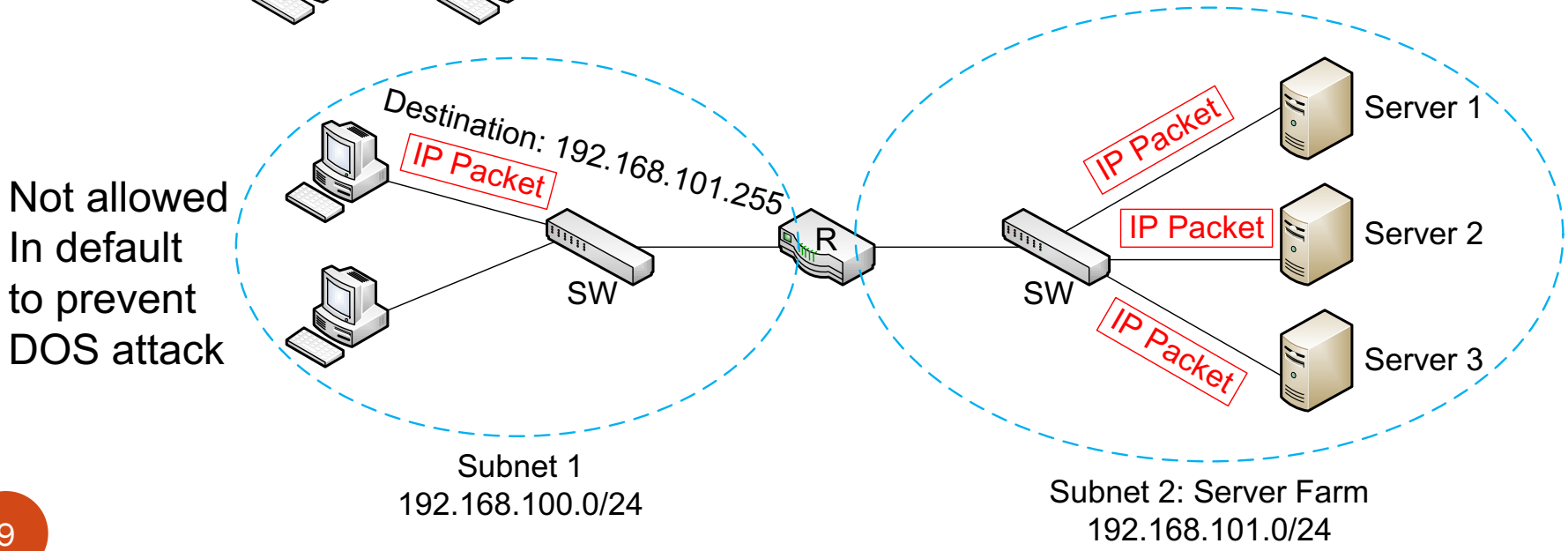


Figure 5.5 Limited broadcasting

Destination addresses
of limited broadcasting:
IP: 255.255.255.255
MAC: FFFF.FFFF.FFFF

Figure 5.6 Directed broadcasting



5.6.3 Multicasting (224.0.0.0~239.255.255.255)

- Multicast group (e.g., video conferencing)
- Both multicast IP and unicast IP
- IGMP (Internet Group Management Protocol)
- Relies on UDP

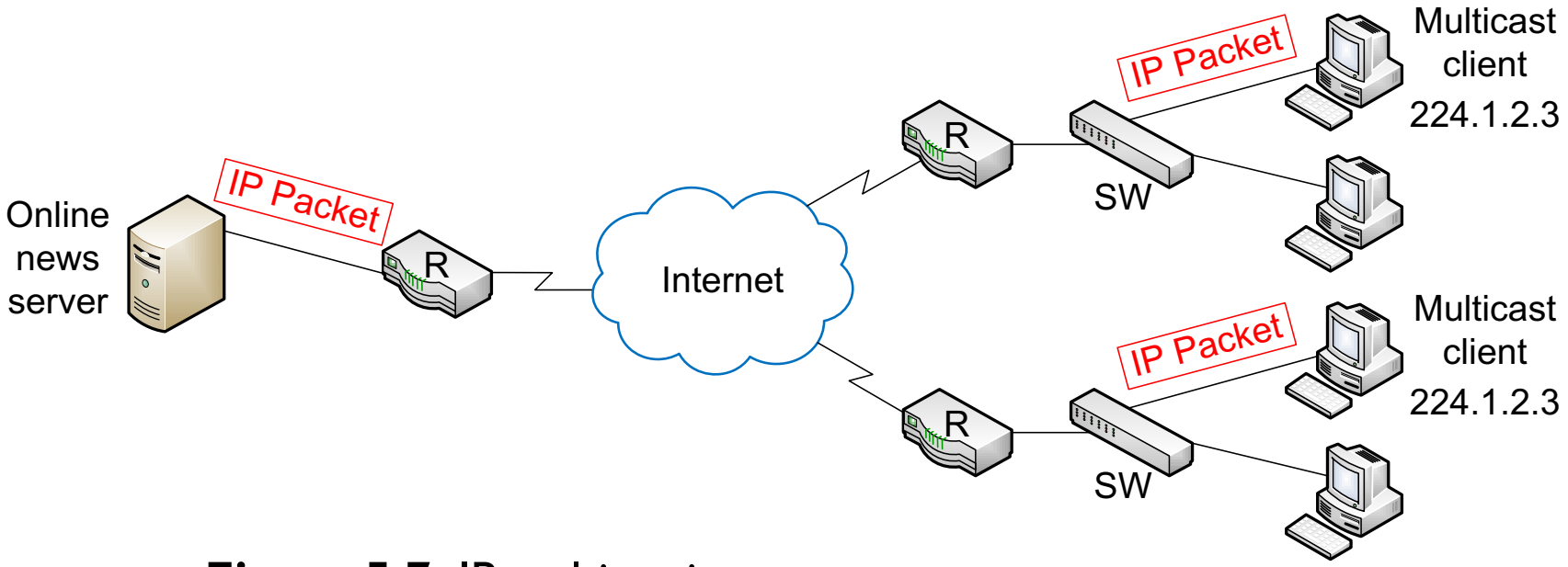


Figure 5.7 IP multicasting

5.6.4 Private IP & NAT

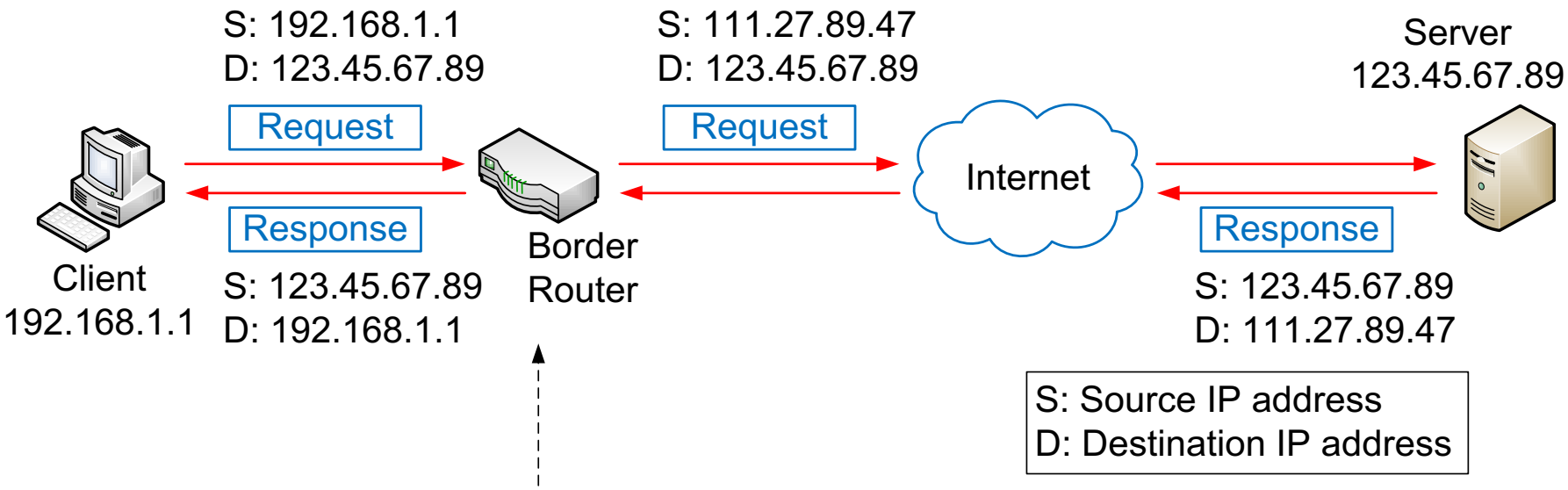
Three private IP address ranges in use

- 10.0.0.0 ~ 10.255.255.255
- 172.16.0.0 ~ 172.31.255.255
- 192.168.0.0 ~ 192.168.255.255

Network address translation (NAT): IP masquerading

- NAT: one-to-one IP mapping
- NAT: many-to-one IP mapping

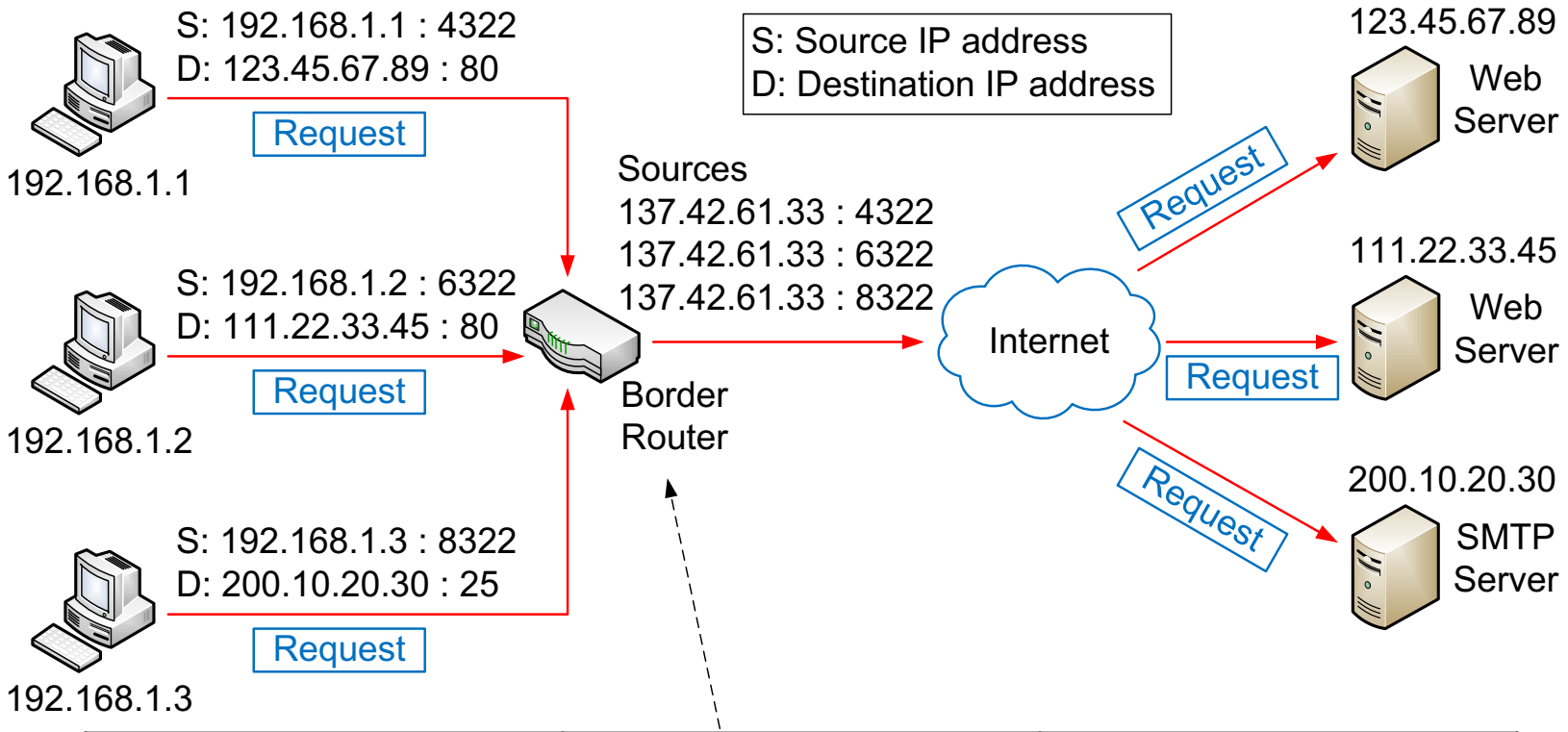
NAT: one-to-one IP mapping



Interface	Internal Source IP	External Source IP
S0/0/0	192.168.1.1	111.27.89.47

Figure 5.8 Router's one-to-one IP mapping and address conversion table

NAT: many-to-one IP mapping



Interface	Internal Source IP	External Source IP
S0/0/0	192.168.1.1:4322	137.42.61.33:4322
S0/0/0	192.168.1.2:6322	137.42.61.33:6322
S0/0/0	192.168.1.3:8322	137.42.61.33:8322

Figure 5.9 Router's many-to-one IP mapping and address conversion table

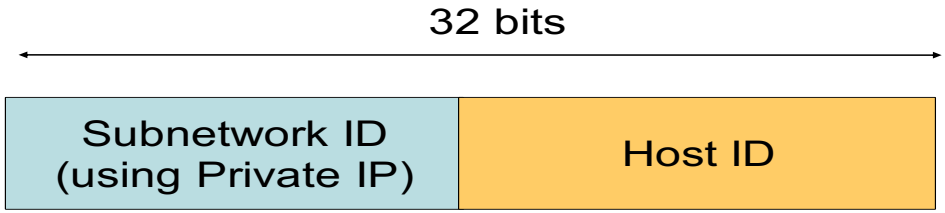
Pros and Cons of NAT

Pros

- Flexibility in internal IP allocation
  - No need for designated network ID
- Consistency in internal IP allocation

Cons

- Potential performance degradation
- Possible conflicts with some network applications



5.7 SUBNETTING

- **5.7.1 Defining Subnet Boundaries: Review**
  - Better security management
  - Customization of network segments
  - Limit broadcasting effects

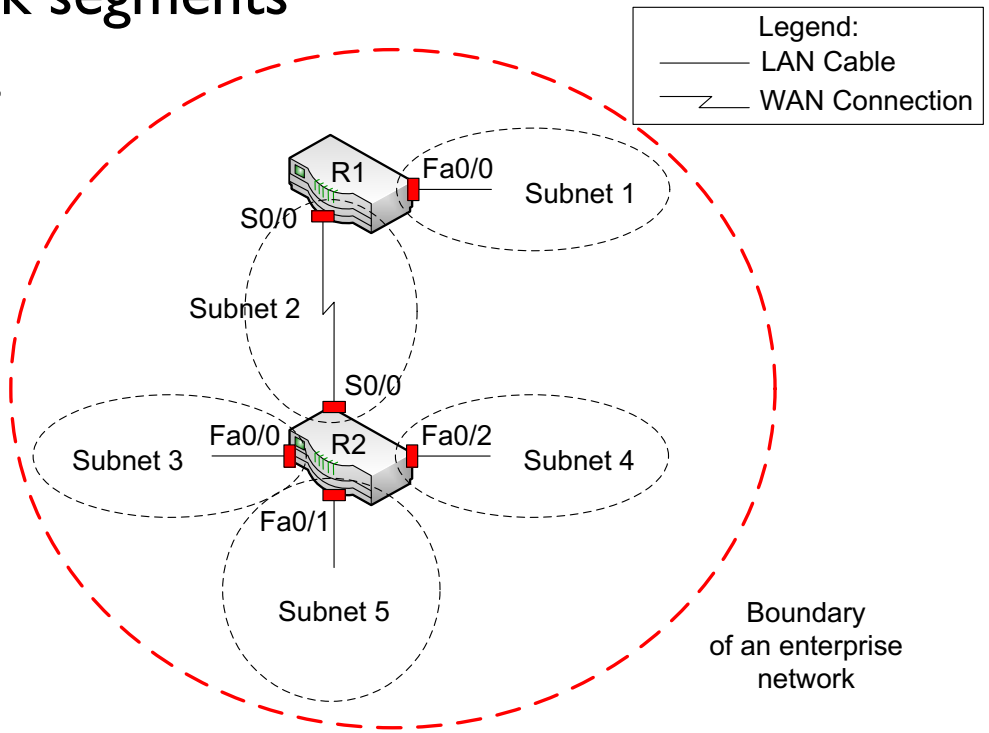


Figure 5.10 Subnets defined by router ports

5.7.2 IP Assignment of a Subnetwork

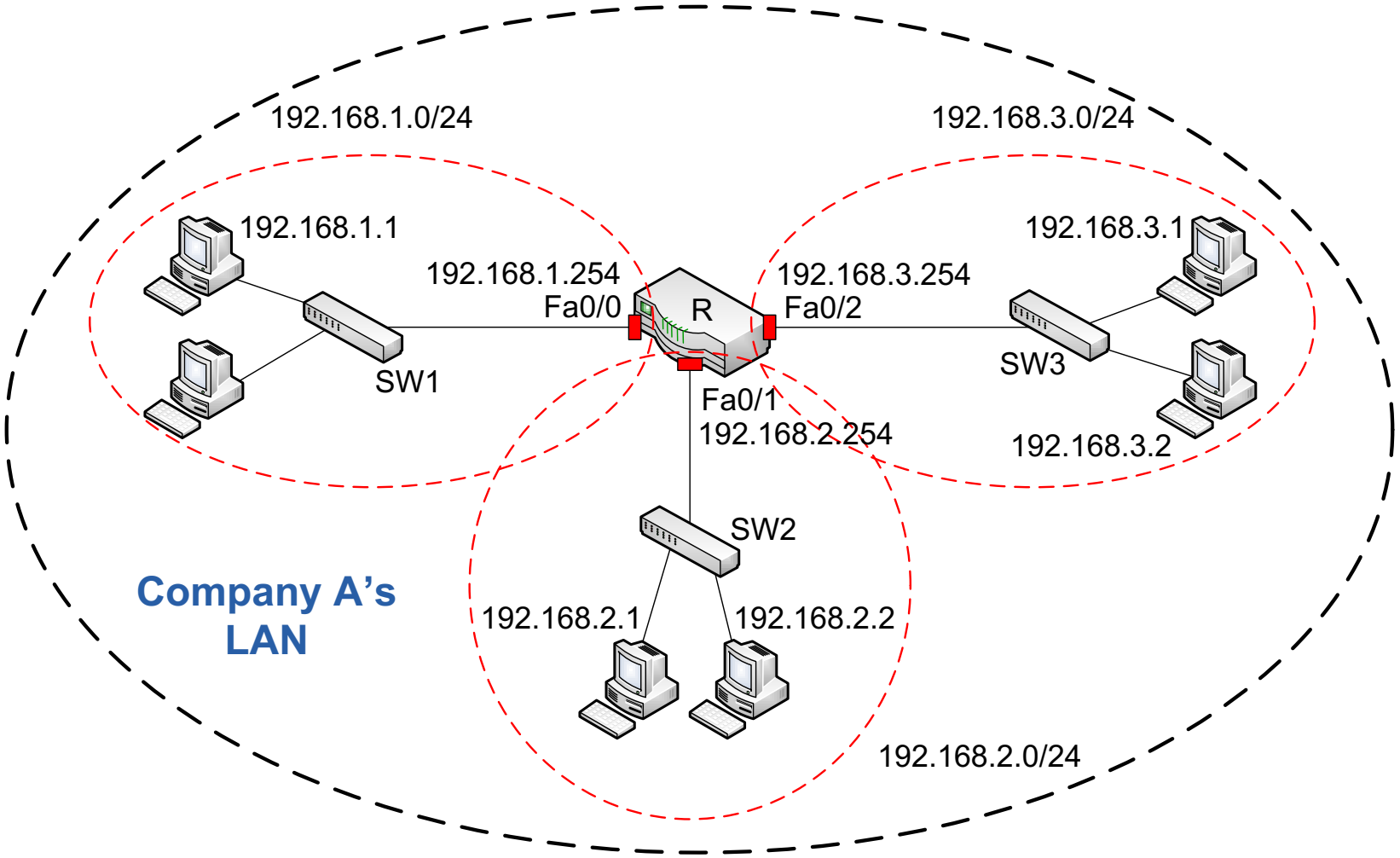


Figure 5.13 A firm's LAN with three subnetworks

5.7.2 IP Assignment of a Subnetwork

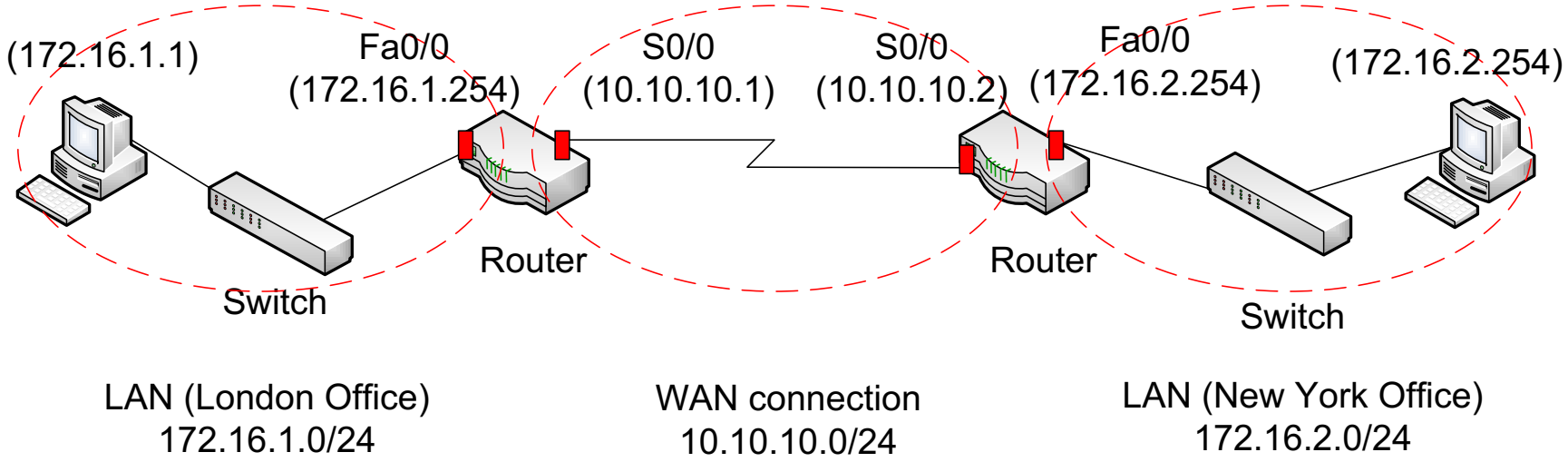


Figure 5.14 An organization's network with 3 subnetworks

5.8 SUBNET MASK

- Indicate the subnet address of an IP address
- Either prefix or a combination of continuous 1s and 0s (Continuous 1s indicate subnet address.)
- Configured on hosts and routers

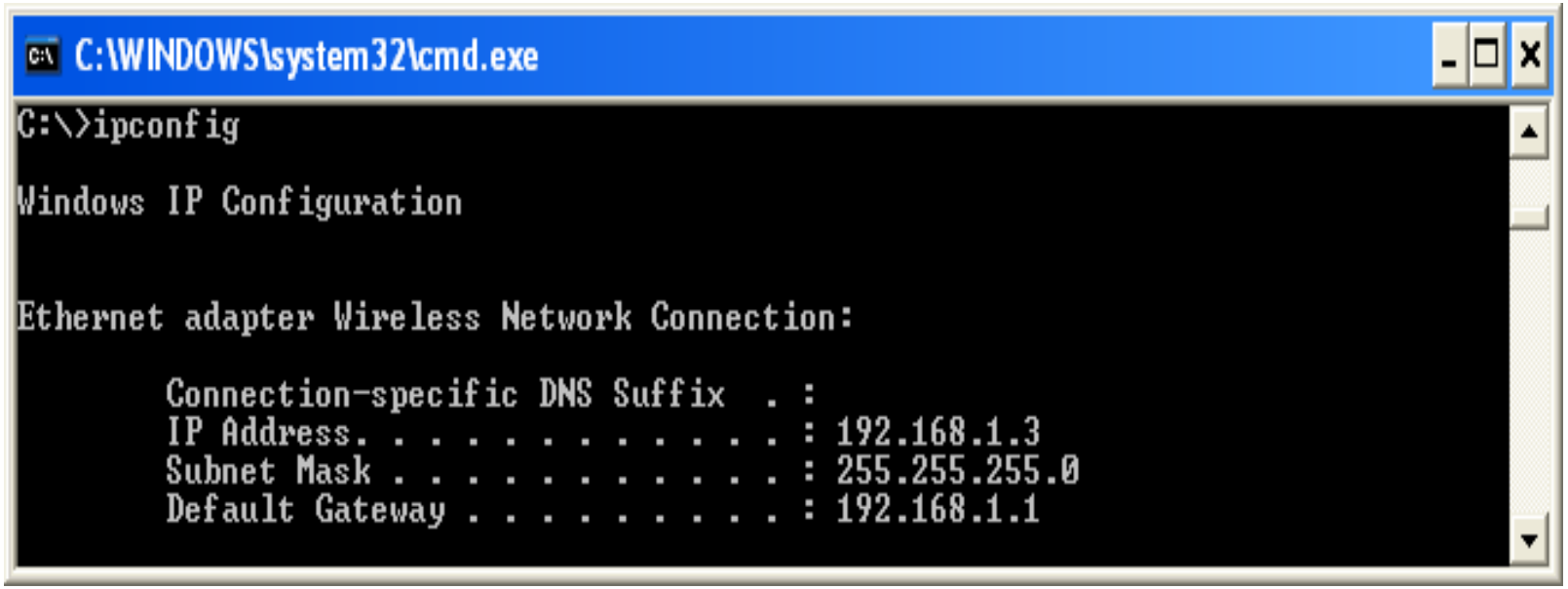


Figure 5.15 IP configuration of a host station

5.8.1 Subnet Mask

Example 1: Host address: 176.20.38.4
Network ID : 176.20
Subnet ID: 38
Host ID: 4

Items	Decimal	Binary
Host address	176.20.38.4	10110000.00010100.00100110.00000100
Network address	176.20.0.0	10110000.00010100.00000000.00000000
Subnet address	176.20.38.0	10110000.00010100.00100110.00000000
Subnet mask	255.255.255.0 or "/24" (prefix)	11111111.11111111.11111111.00000000
Host address with subnet mask	176.20.38.4/24	
Subnet address with subnet mask	176.20.38.0/24	

5.8.1 Subnet Mask

- **Example 2:** Host address: 192.168.1.51
  Network ID: 192
  Subnet ID: 168
  Host ID: 1.51

Items	Decimal	Binary
Host address	192.168.1.51	11000000.10101000.00000001.00110011
Network address	192.0.0.0	11000000.00000000.00000000.00000000
Subnet address	192.168.0.0	11000000.10101000.00000000.00000000
Subnet mask (network ID + subnet ID part)	255.255.0.0 or "/16" (prefix)	11111111.11111111.00000000.00000000
Host address with subnet mask	192.168.1.51/16	
Subnet add. with subnet mask	192.168.0.0/16	

5.8.1 Subnet Mask

Example 3 (Challenge)

Host address: 192.168.1.51
Network ID: 192
Subnet ID: 160
Host ID: 8.1.51

Items	Decimal	Binary
Host address	192.168.1.51	11000000.10101000.00000001.00110011
Network address	192.0.0.0	11000000.00000000.00000000.00000000
Subnet address	192.160.0.0	11000000.10100000.00000000.00000000
Subnet mask (network ID + subnet ID)	255.224.0.0 or "/11" (prefix)	11111111.11100000.00000000.00000000
Host address with subnet mask	192.168.1.51/11	
Subnet address with subnet mask	192.160.0.0/11	

5.8.2 Subnetting Address Space

#	Subnet address (binary)	Subnet address (decimal)	Subnet mask
1	10000010.10111111.00000000.00000000	130.191.0.0	255.255.192.0
2	10000010.10111111.01000000.00000000	130.191.64.0	255.255.192.0
3	10000010.10111111.10000000.00000000	130.191.128.0	255.255.192.0
4	10000010.10111111.11000000.00000000	130.191.192.0	255.255.192.0

The first subnet (130.191.0.0) has a usable host address range of:
10000010.10111111.00000000.00000001 ~
10000010.10111111.00111111.11111110
= 130.191.0.1 ~ 130.191.63.254

5.9 SUPERNETTING

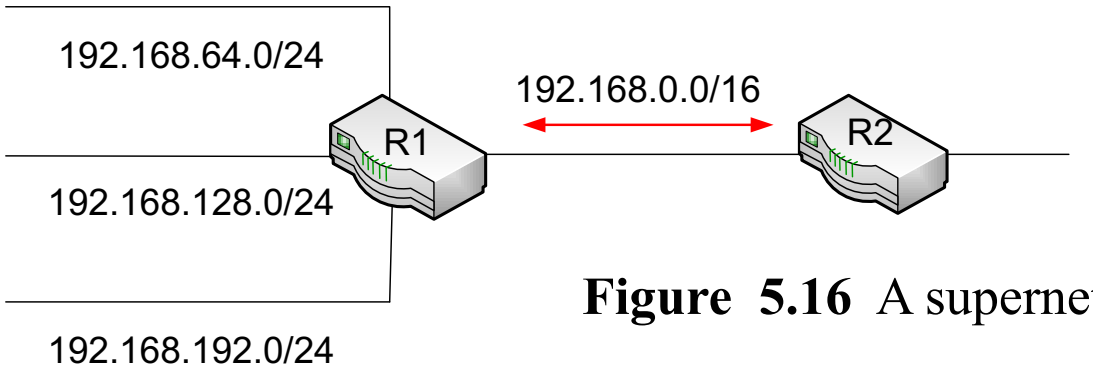


Figure 5.16 A supernet that summarizes 3 subnets

Subnet address & mask (decimal)	Subnet address (binary)
192.168.64.0/24	11000000. 10101000.01000000.00000000
192.168.128.0/24	11000000. 10101000.10000000.00000000
192.168.192.0/24	11000000. 10101000.11000000.00000000

Supernet address: 11000000. 10101000.00000000.00000000 = 192.168.0.0

Supernet's subnet mask: 11111111. 11111111.00000000.00000000 =

255.255.0.0 = '/16'

5.10.1 Determining Number of Nodes

Node Categorization	Nodes	Preferred IP addressing
Resource consumers	End user stations (e.g., workstations, productivity tools)	Dynamic IPs
Resource or service providers	• Dedicated servers • Peripherals including printers, fax, and backup devices • Specialty devices including surveillance cameras, AC sensors, and alarms	Permanent IPs
Intermediary devices	• Router LAN and WAN ports (interfaces) • Firewall • Managed switch (An IP address is assigned to remotely access its OS over the network) • Managed wireless access point (An IP address is assigned to remotely access its OS over the network)	Permanent IPs

Table 5.3 Classification of network nodes

5.10.3 Managing Security with DMZ Subnet

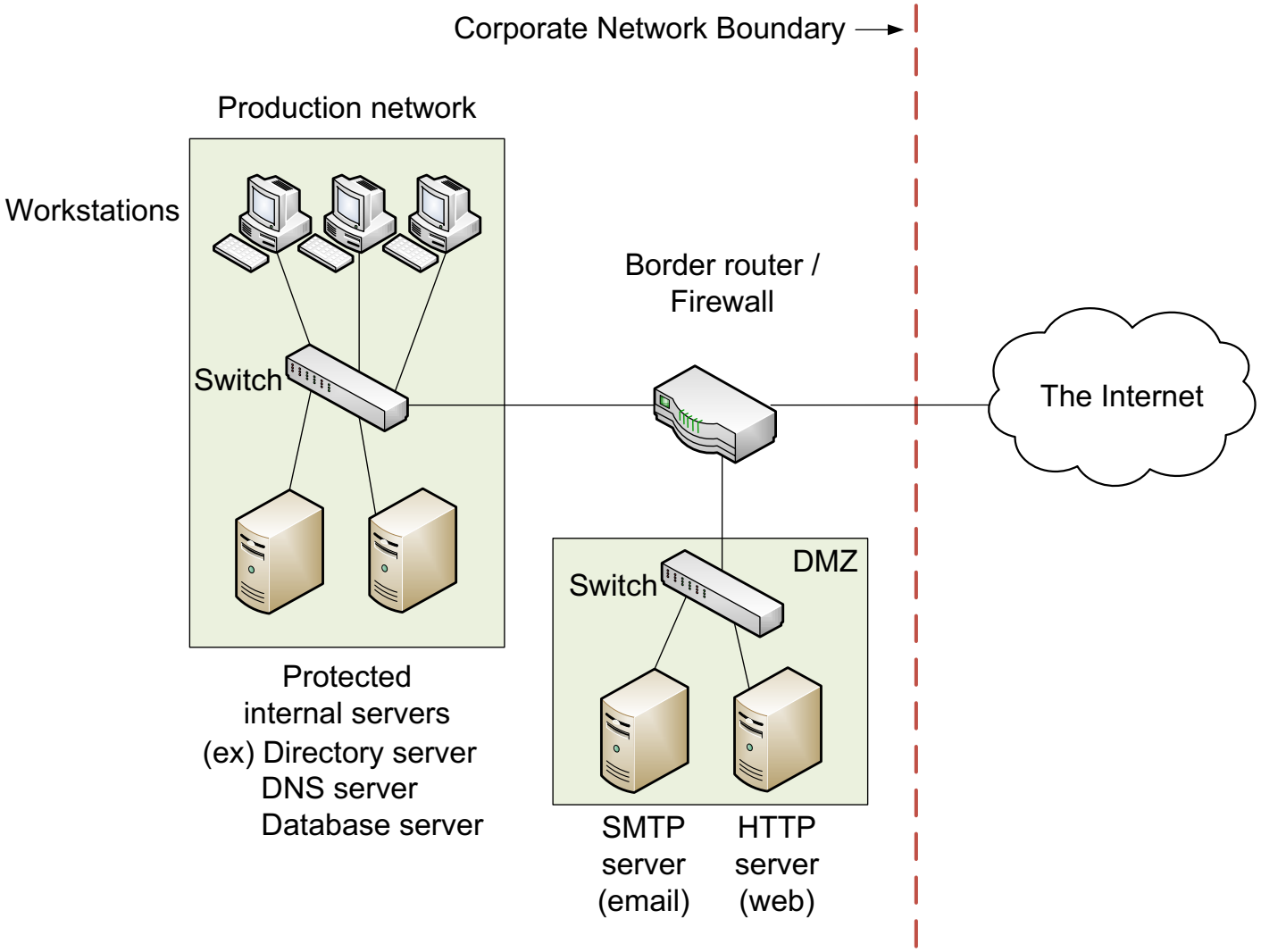


Figure 5.18 General setup of DMZ as a subnet

IP Range	Assignment
• Network address: 192.168.0.0	
• Subnet mask: 255.255.255.0 (/24)	
• Subnet range (third octet)	
192.168.1.0	DMZ (accessible from the Internet)
192.168.2.0 ~ 192.168.7.0	University administration
192.168.8.0 ~ 192.168.40.0	Academics (colleges & departments)
192.168.41.0 ~ 192.168.43.0	Library
192.168.44.0 ~ 192.168.50.0	Student labs
192.168.51.0	Campus storage area network
192.168.52.0	Campus operation and maintenance
192.168.53.0	Campus safety and security
192.168.54.0 ~ 192.168.55.0	Athletics
192.168.56.0 ~ 192.168.60.0	WAN links
192.168.61.0 ~ 192.168.62.0	Internet links
• Host range within a subnet (fourth octet)	
x.x.x.1 ~ x.x.x.2:	Router (gateway) & firewall interface(s)
x.x.x.3 ~ x.x.x.10:	Managed switches (core & workgroup switches)
x.x.x.11 ~ x.x.x.15:	Managed wireless devices (ex. access points)
x.x.x.16 ~ x.x.x.25:	Servers
x.x.x.26 ~ x.x.x.40:	Peripherals (ex. printers, fax, back-up devices)
x.x.x.41 ~ x.x.x.250:	General user stations
x.x.x.251 ~ x.x.x.254:	Network technician/administrator stations

Table 5.4 A hypothetical policy for IP address allocation

Recap

- IP Governance
- IP address structure
- Classful vs classless IPs
- Special IP ranges: loopback, private IPs, broadcasting & multicasting
- Network address translation
- Subnetting & subnet mask
- Supernetting
- Planning IP address allocation

End
Chapter 5

CECS 303 Networks and Networks Security

Fundamentals of Packet Routing
Chapter 6

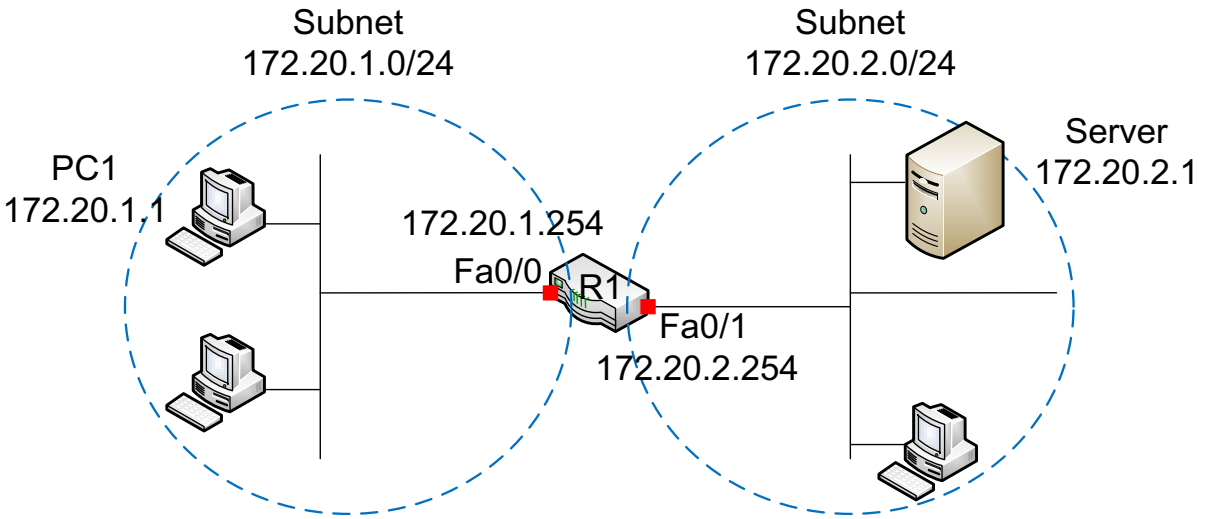
Jose Tamayo, M.S.
Computer Engineering & Computer Science
California State University, Long Beach

6.1 Introduction

- Routers
  - Intra-domain routing: Within an autonomous system
  - Inter-domain routing: Between autonomous systems
  - Heads up on autonomous systems (Refer to section 10.2.3 for more details)
    - An ISP or organization (e.g., enterprise, university) that defines its own internal routing policy (e.g., UCSD, IBM, Google, MIT)
    - Autonomous system number (ASN): a unique identifier of an AS.
    - IANA (Internet Assigned Numbers Authority) allocates ASNs to RIR (Regional Internet Registries) just like the allocation of IP blocks
    - 54000 ASNs in 2016

- Chapter Focus: internal (or intra-domain) routing

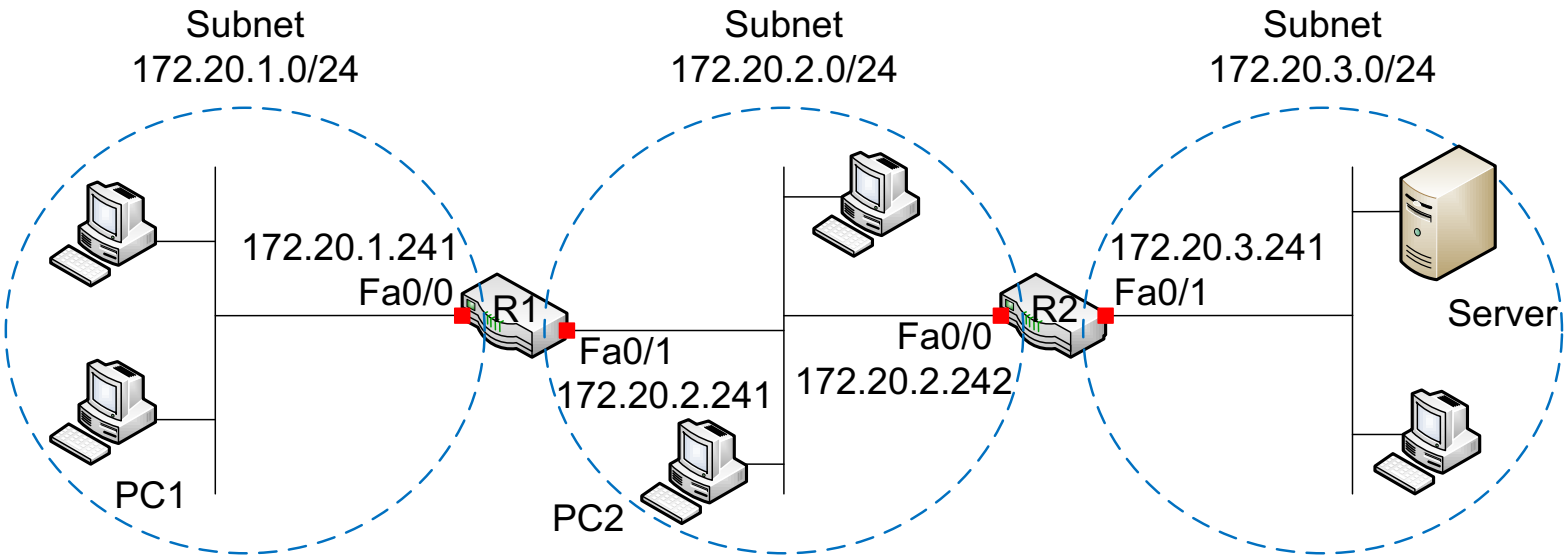
6.2 Routing Mechanism



Destination Subnetwork/ Subnet Mask	Exit Port/ Interface	Next hop IP	Metric
172.20.1.0/24	FastEthernet0/0	N/A	0
172.20.2.0/24	FastEthernet0/1	N/A	0

Figure 6.1 A case of two subnetworks and a router

6.2 Routing Mechanism



Destination Subetwork/ Subnet Mask	Exit Port/ Interface	Next hop IP	Metric
172.20.1.0/24	FastEthernet0/0	N/A	0
172.20.2.0/24	FastEthernet0/1	N/A	0
172.20.3.0/24	FastEthernet0/1	172.20.2.242	1

Figure 6.2 A case of three subnets and R1's routing table

6.3 Routing Table

- Background: routing protocol (ex. RIP) vs. routed protocol (ex. IP)

- Routing Table Elements
  - Destination subnet addresses and subnet masks
  - Exit ports/interfaces
  - Next-hop IP address
  - Metric value

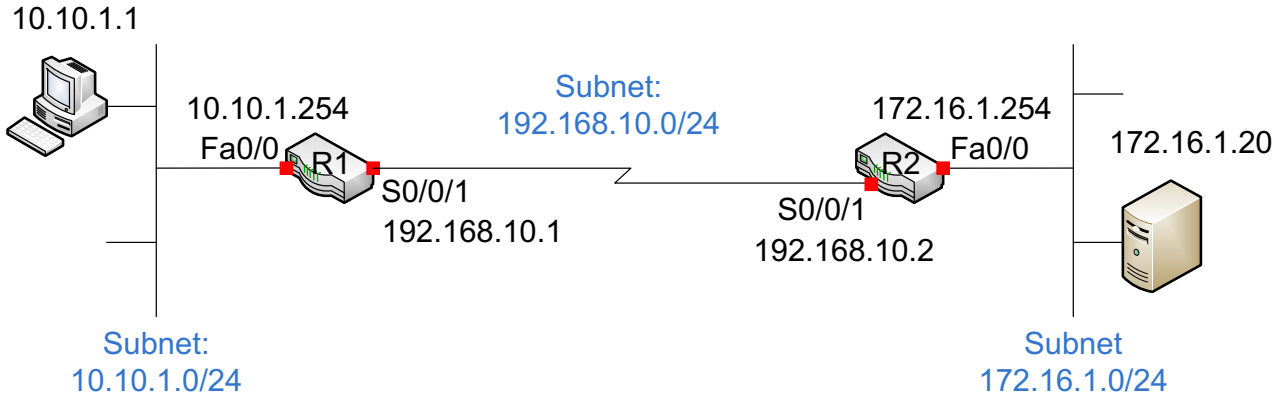


Figure 6.3 Exit port (interface) & next-hop IP address

6.3 Routing Table

- Metric: cost factors – breaking a tie
  - Hop count
  - Bandwidth
  - Delay: type of link to a router port (ex. T-1)
  - Reliability: probability of link failure (ex. 80%)
  - Load: utilization rate of a link (ex. 80%)

Destination Subnetwork/ Subnet Mask	Exit Port/ Interface	Next hop IP	Metric
172.20.1.0/24	FastEthernet0/0	N/A	0
172.20.2.0/24	FastEthernet0/1	N/A	0
172.20.3.0/24	FastEthernet0/1	172.20.2.242	1

6.4 Packet Forwarding Decision

1. Finding matching entries of a routing table:

   (ex) Destination IP of a packet 192.168.20.32

   192.168.20.0/24; 192.168.0.0/16; 192.0.0.0/8; 0.0.0.0/0

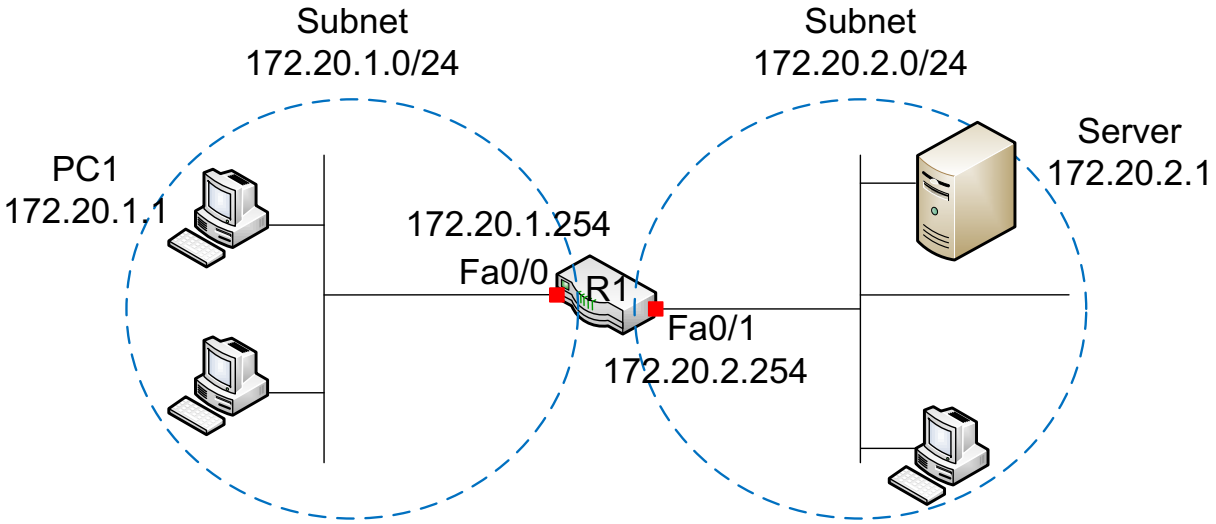
   192.168.10.0/24; 192.0.0.0/16; 192.168.20.196/27

2. General decision rules

   a) A single match: forward the packet to the matching exit interface.
   b) Multiple matches: choose the path that has the most explicit (longest) match
   c) No matching entry: forward the packet to the *default route* (0.0.0.0/0)
   d) If there is more than one best path, metric values are used to break the tie.

6.5 Entry Types Of Routing Table

6.5.1 Directly Connected Routes



Cisco OS Example:

R1(config)# ***interface Fastethernet0/0***

R1(config-if)# ***ip address 172.20.1.254 255.255.255.0***

R1(config-if)# ***no shutdown***

6.5 Entry Types of Routing Table

6.5.2 Static Routes

Destination Network/Subnet Mask	Exit Port/ Interface	Next hop IP	Metric
172.20.1.0/24	FastEthernet0/0	N/A	0
172.20.2.0/24	FastEthernet0/1	N/A	0
0.0.0.0/0	FastEthernet0/0	N/A	1

Table 6.1 Default route as a static route entry

Cisco Example:
R1(config)# ***ip route 0.0.0.0 0.0.0.0 Fa0/0***

6.5 Entry Types of Routing Table

- Static routing table of a host station

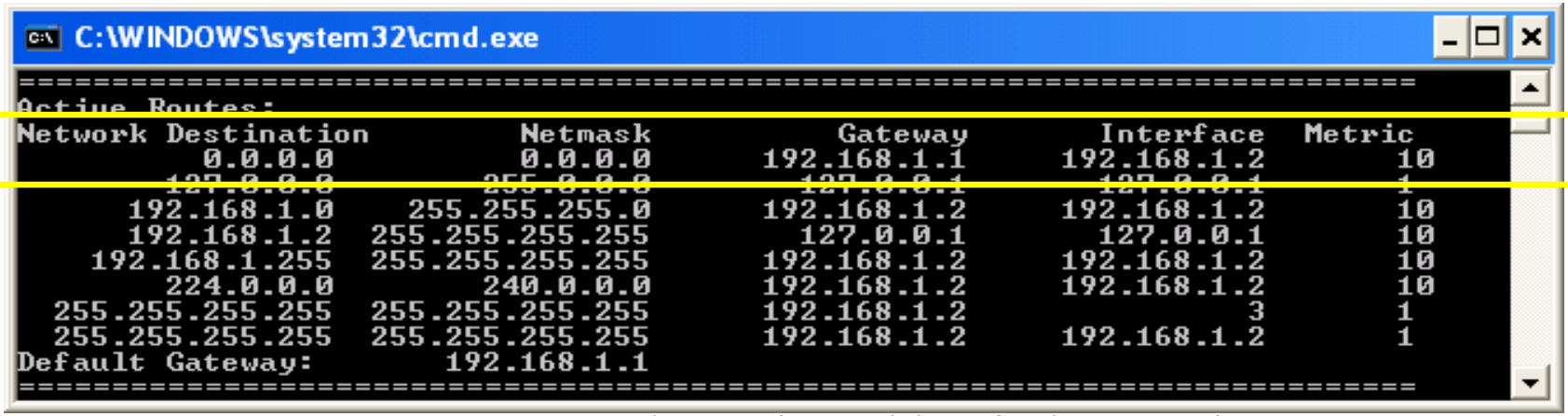


Figure 6.6 A sample routing table of a host station

Modification of PC routing table

C:\>route **PRINT**

C:\>route **DELETE** *network*

C:\>route **ADD** *network* **MASK** *mask gateway-IP address*

6.5 Entry Types of Routing Table

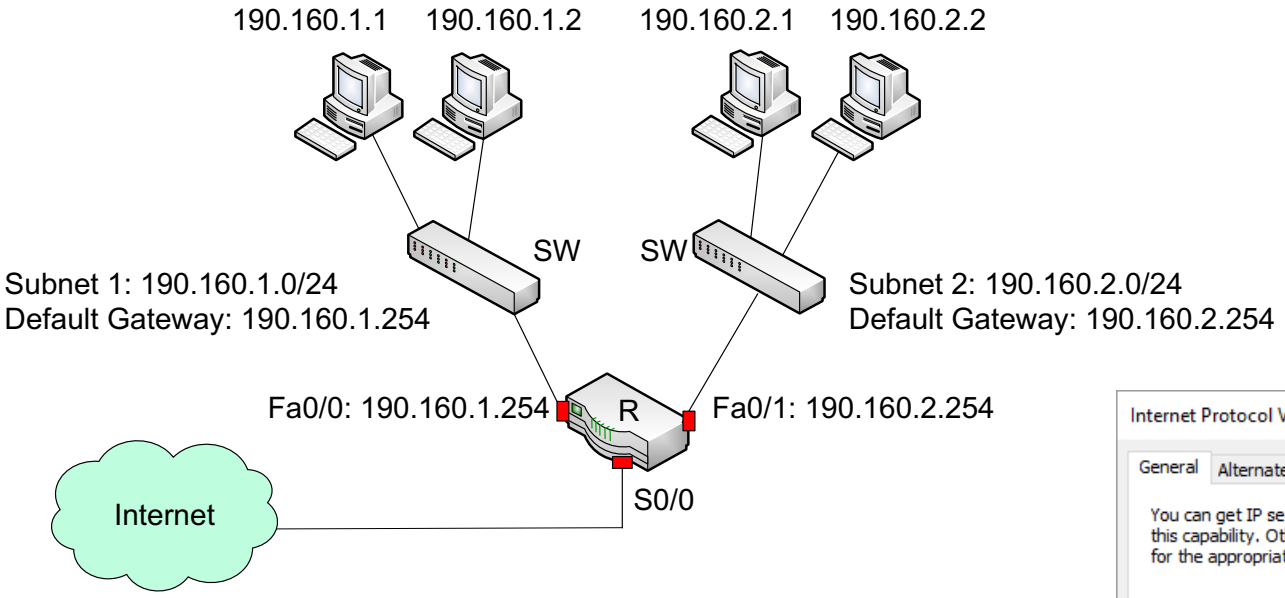
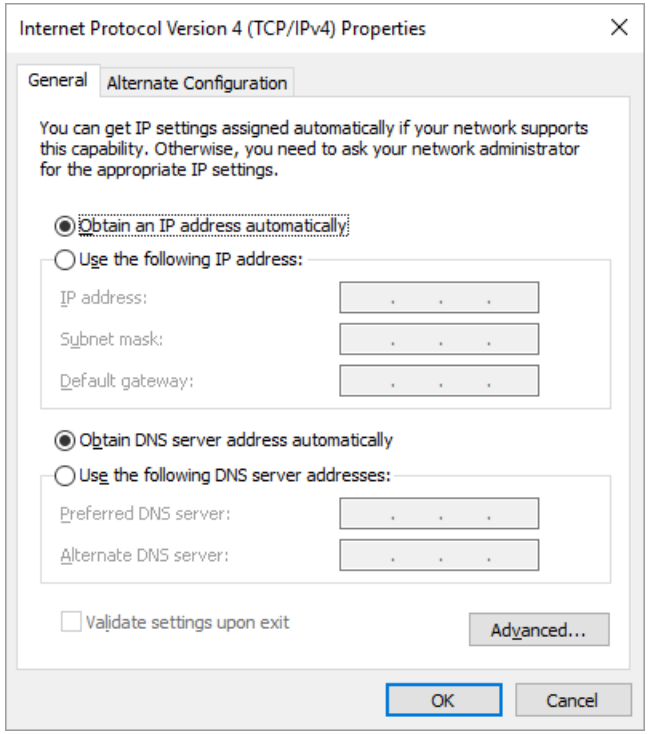


Figure 6.7 Demonstration of default gateway



6.5 Entry Types of Routing Table

6.5.3 Dynamic Routes

Type	Destination Subnetwork/Mask	Exit Port/ Interface	Next hop IP	Metric
C	192.168.10.0/24	FastEthernet0/1	N/A	0
C	172.20.1.0/24	FastEthernet0/0	N/A	0
O	10.10.1.0/24	FastEthernet0/1	192.168.10.254	120
O	192.168.1.0/24	Serial0/1	172.16.10.254	120
S	0.0.0.0/0	Serial0/1	172.16.10.254	1

Table 6.2 Routing table with entry *Type* information

6.6 Dynamic Routing Protocols

6.6.1 Protocol Types

- **Interior Gateway Protocols:** intra-domain routing
  - RIP (Routing Information Protocol)
  - EIGRP (Enhanced Interior Gateway Routing Protocol)
  - OSPF (Open Shortest Path First)
  - IS-IS (Intermediate System to Intermediate System)

- **Exterior Gateway Protocols:** inter-domain routing
  - Border Gateway Protocol (BGP)

6.6 Dynamic Routing Protocols

6.6.2 Delivery of Advertisement

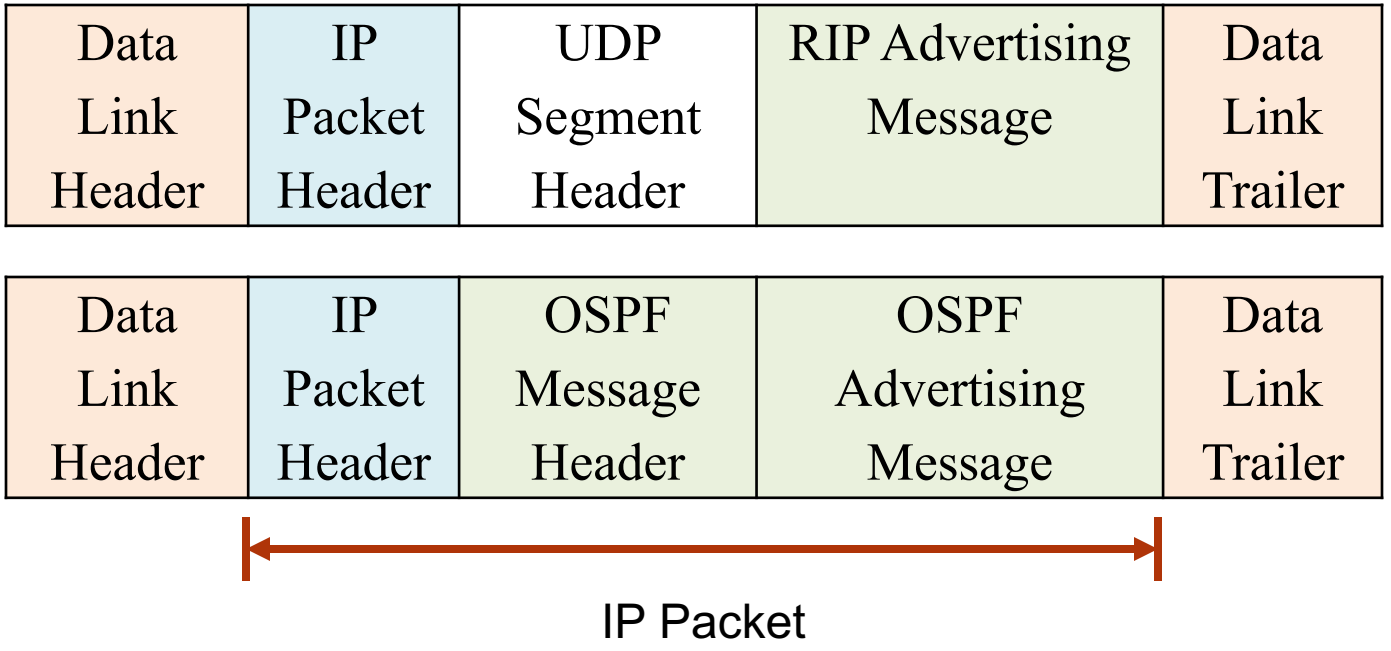


Figure 6.9 Encapsulation of routing protocol advertisement

6.6 Dynamic Routing Protocols

6.6.3 Determination of Dynamic Routes

a) Learn directly connected links: inputs from IP configuration of LAN/WAN ports

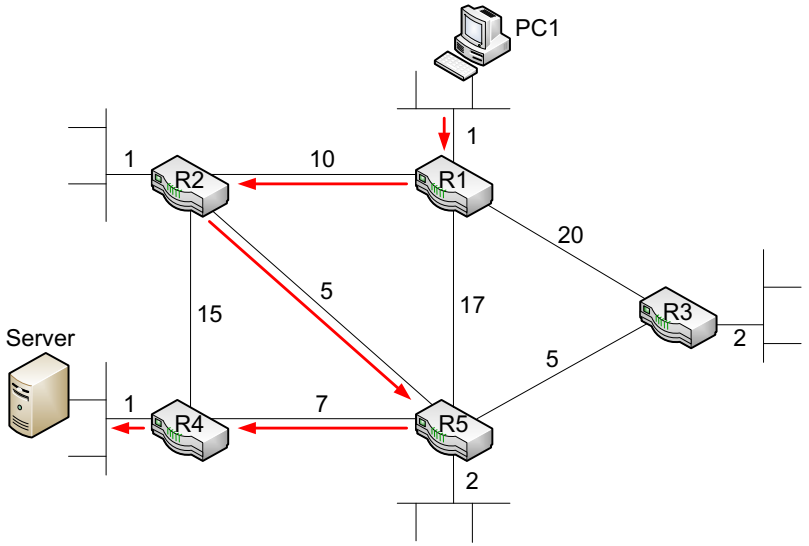
b) Form adjacency: exchange of 'hello'

c) Build link-state information: see Figure 6.10

d) Advertise link-state information: multicasting

e) Each router constructs a map using link-state database: see Figure 6.11

f) Update routing table: shortest path first



6.6 Dynamic Routing Protocols

6.6.3 Determination of Dynamic Routes

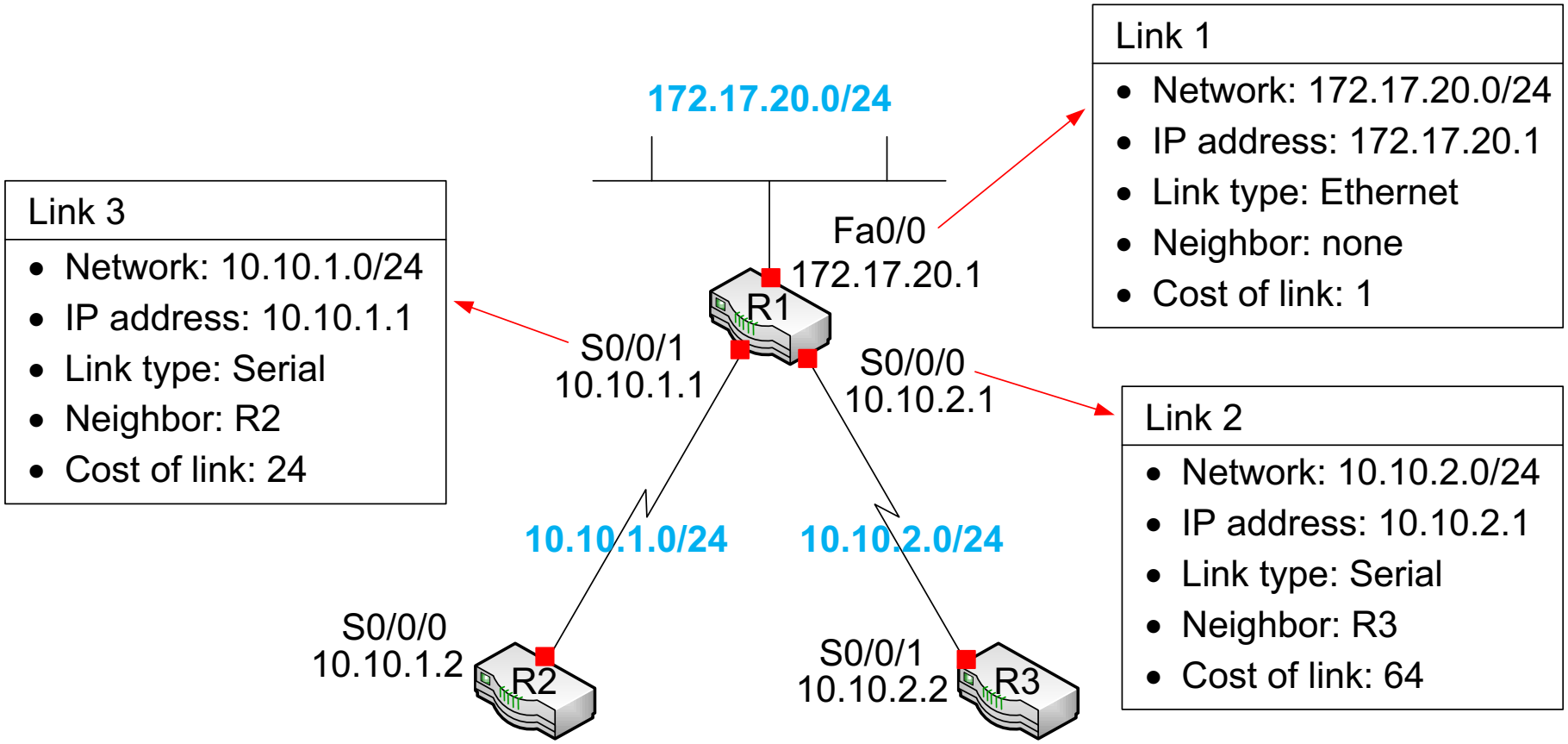


Figure 6.10 Link-state information of R1

6.6 Dynamic Routing Protocols

6.6.3 Determination of Dynamic Routes

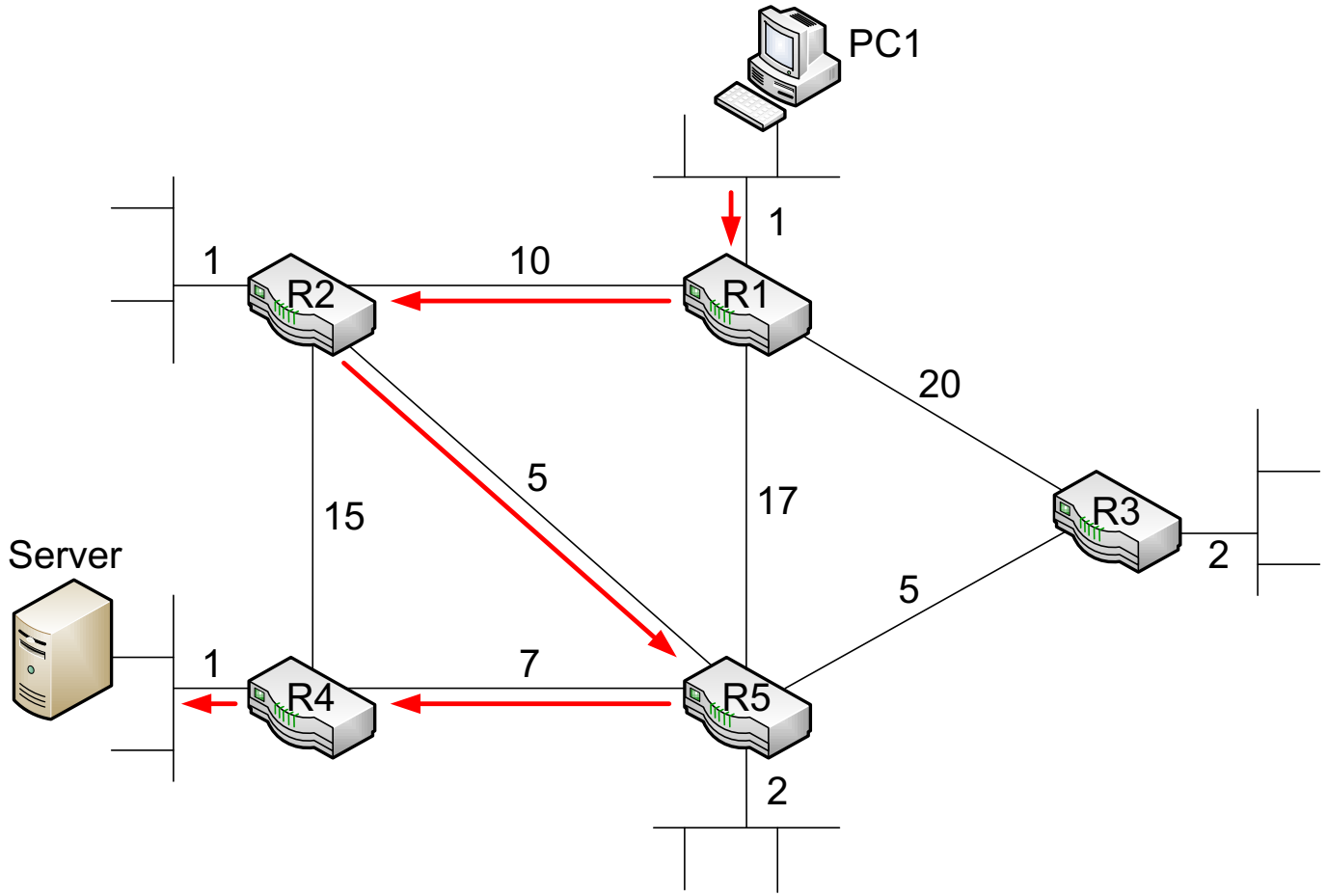


Figure 6.11 A sample router map

6.6.4 Security Management

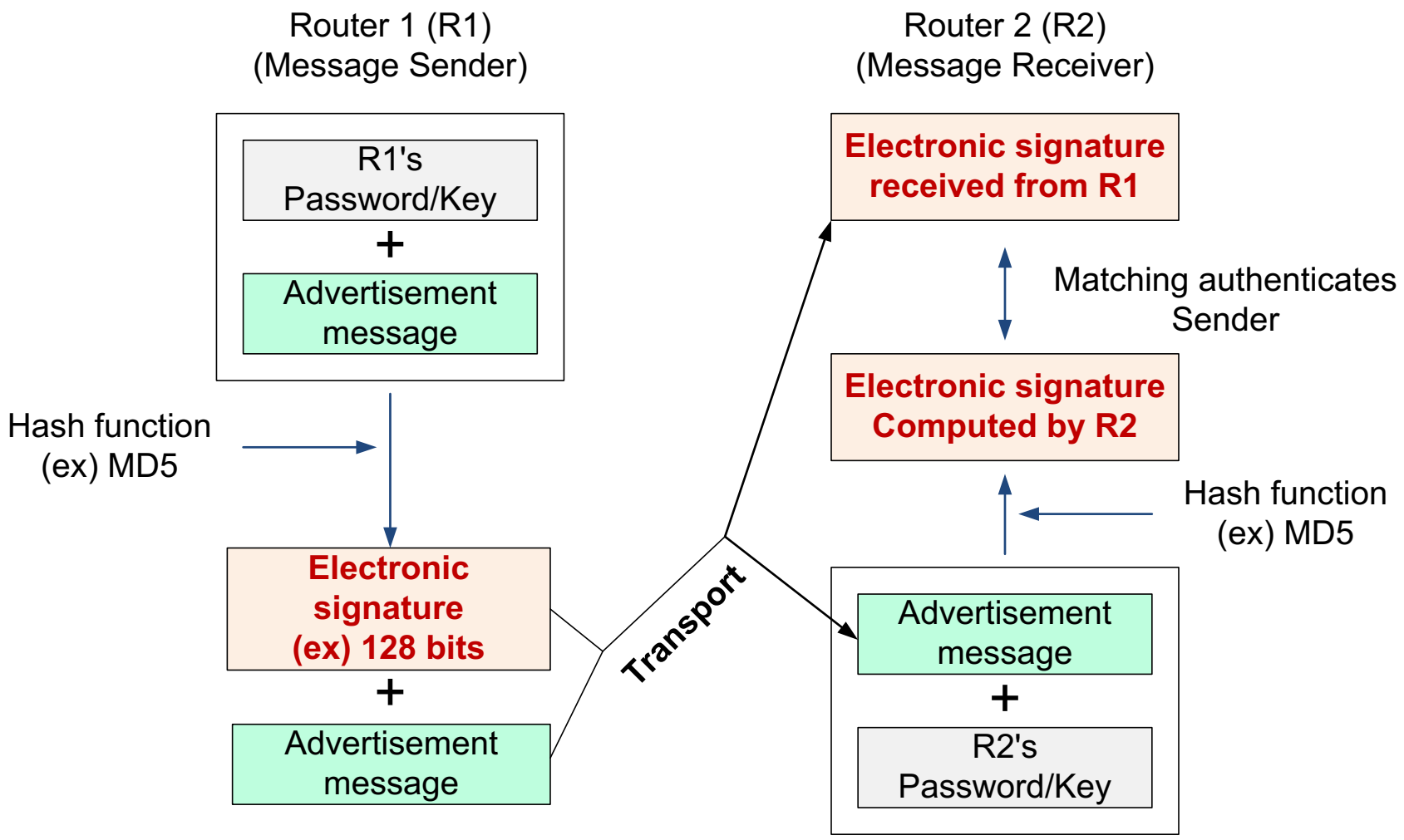


Figure 6.12 Authentication of advertisement

Example: Activating RIP on a Cisco router

- R1(config) #***router rip*** :
- R1(config-router) #***network 172.20.1.0***
- R1(config-router) #***network 172.20.2.0***
- R1(config-router) #***end***

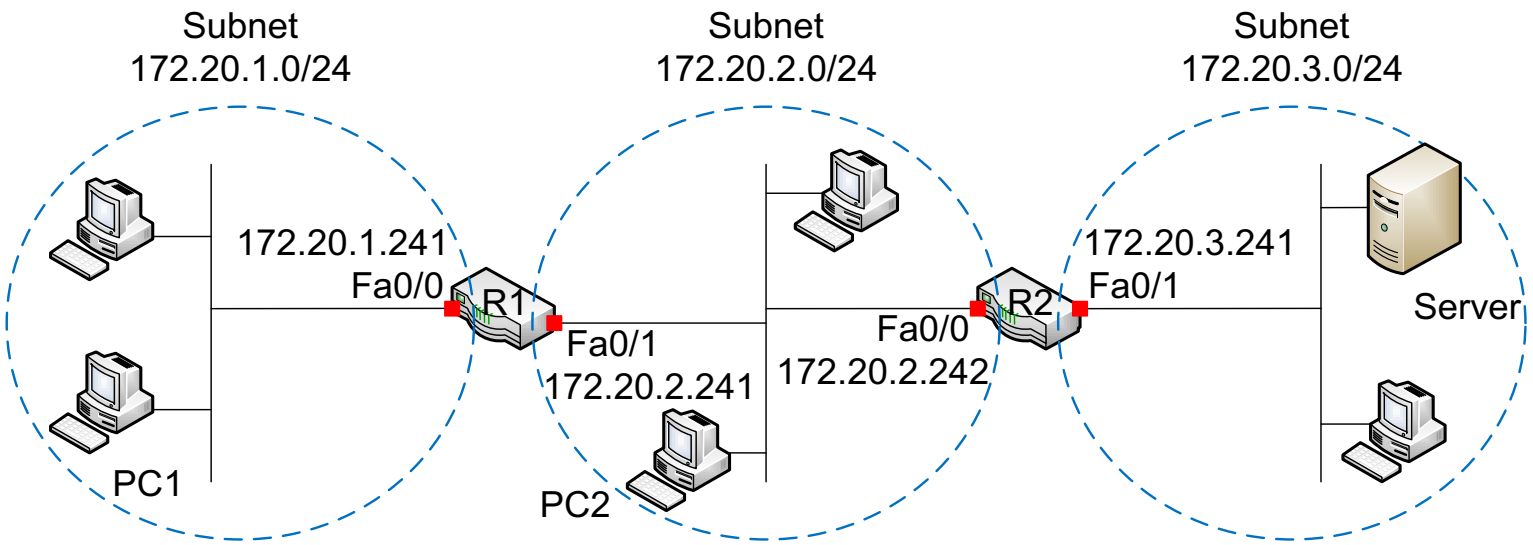


Figure 6.13 A hypothetical network

6.6.5 Static Routing vs. Dynamic Routing

Compared aspects	Comparison	
	Static approach	Dynamic approach
Difficulty in configuration	More difficult	
Chance of configuration errors	Higher chance	
Security of routing table entries	More secure	
Responsiveness to changes in network topology		More responsive
Burden (overhead) on network		Higher burden
Burden on router (e.g., CPU, memory)		Higher burden

Table 6.3 Static vs. dynamic update of the routing table

6.7 Border Gateway Protocol

- For Inter-domain routing: Between autonomous systems

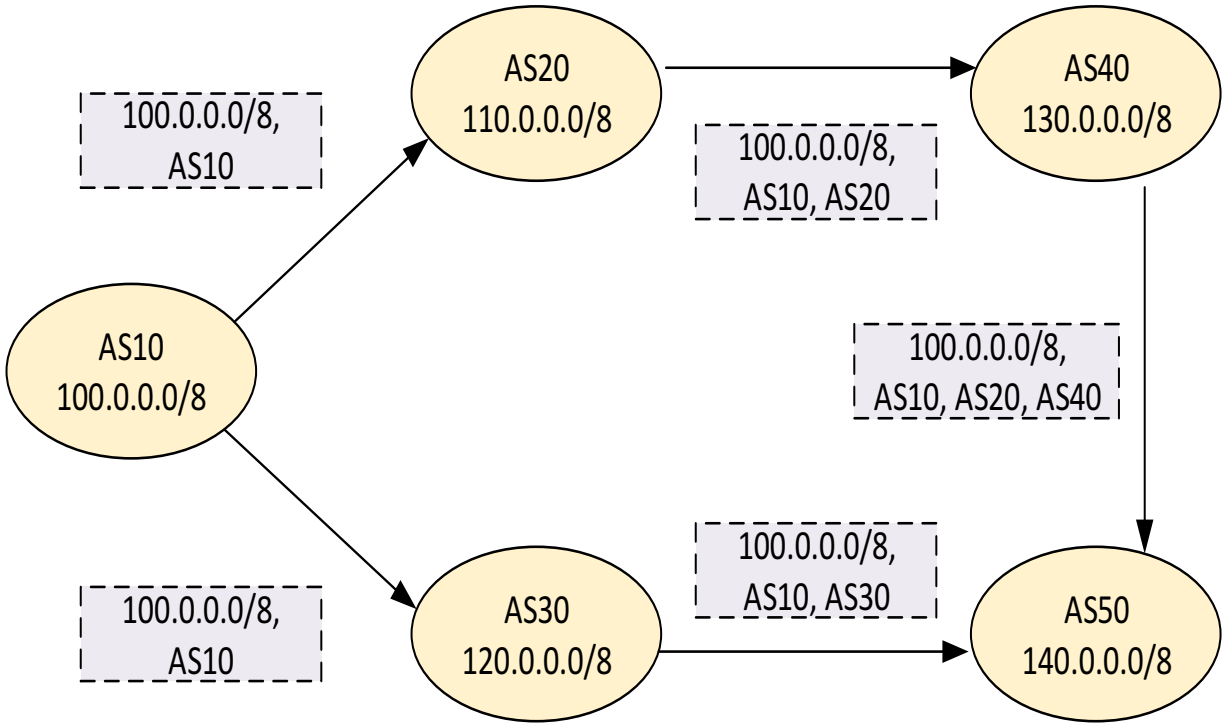


Figure 6.14 A demonstration of BGP mechanism

Recap

- Intra vs Inter-domain routing
- Routing table and elements
- Packet forwarding decision
- Entry types of a routing table
- Routing protocol & dynamic routing protocols
- Determination of dynamic routes
- Static vs dynamic routing
- Border gateway protocol

End
Chapter 6

Wireless LAN
Chapter 8

8.1 Introduction

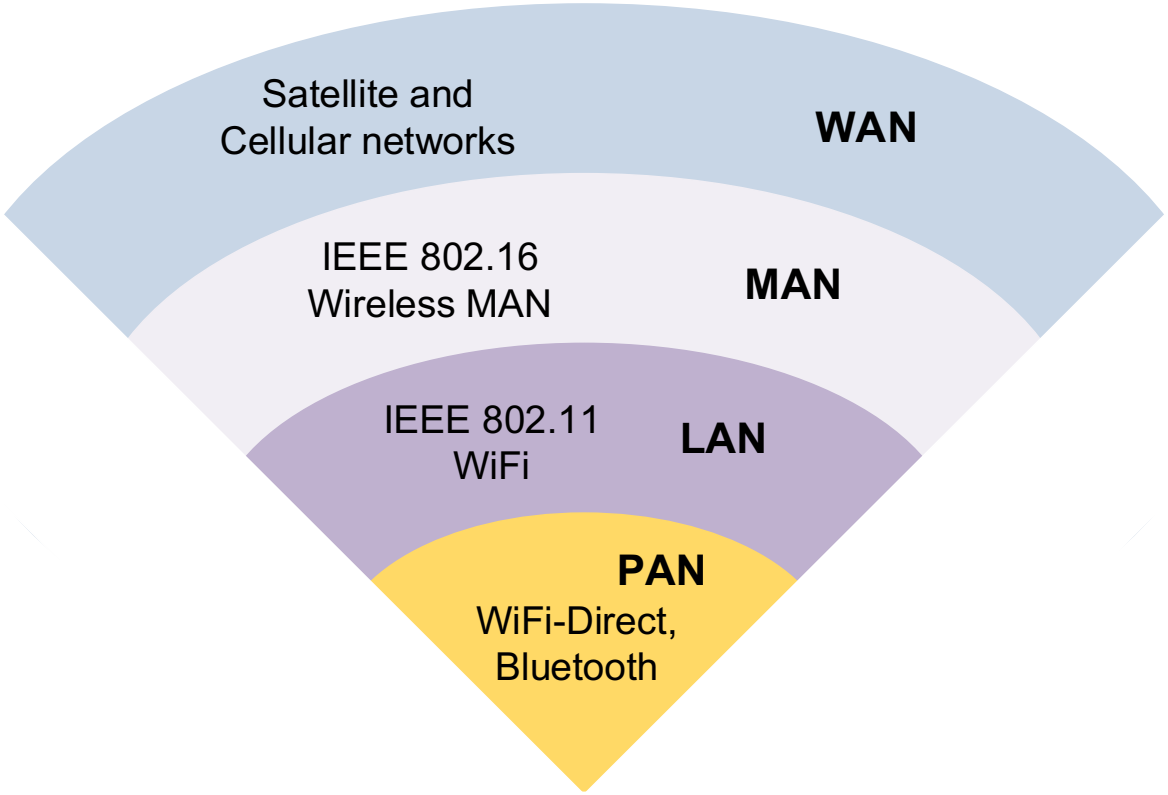


Figure 8.1 Select wireless networking technologies

8.2.1 Layers of WiFi Technology

Data link layer functions:

- Creation of WiFi frames
- Implementation of reliable data transmission service
- Authentication and association between nodes
- Protection of transmitted data with encryptions
- Media access control

8.2.2 Setup Modes & Access Points

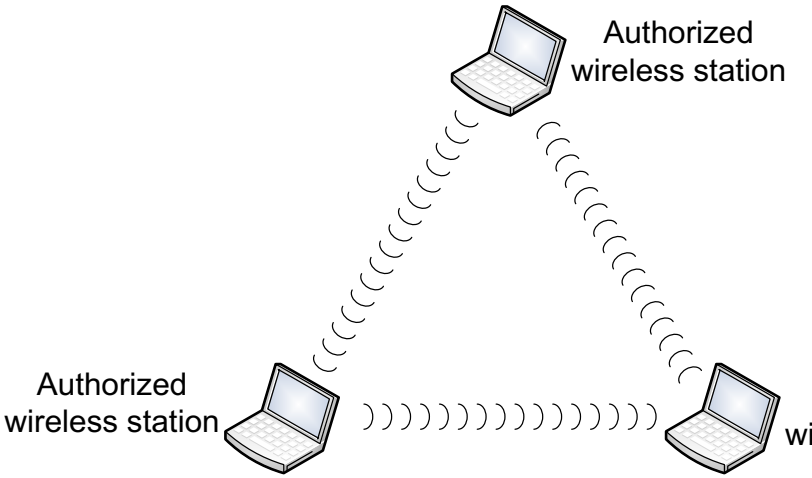


Figure 8.2 WiFi in ad-hoc mode

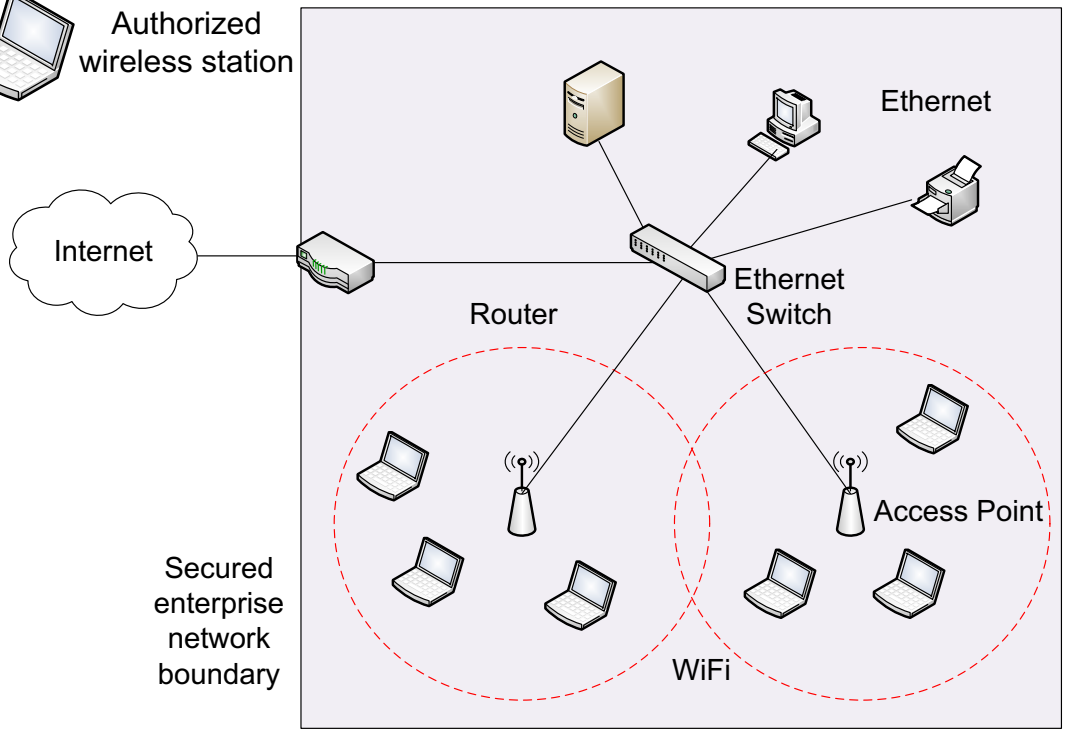


Figure 8.3 WiFi in infrastructure mode

8.2.2 Setup Modes & Access Point

- Access Point (Hotspot): Key functions
  - *Bridging*
  - *Authentication*
  - *Media access control*
  - *Data security*
  - *Frame routing*

8.2.2 Setup Modes & Access Point

Access Point: Association Table

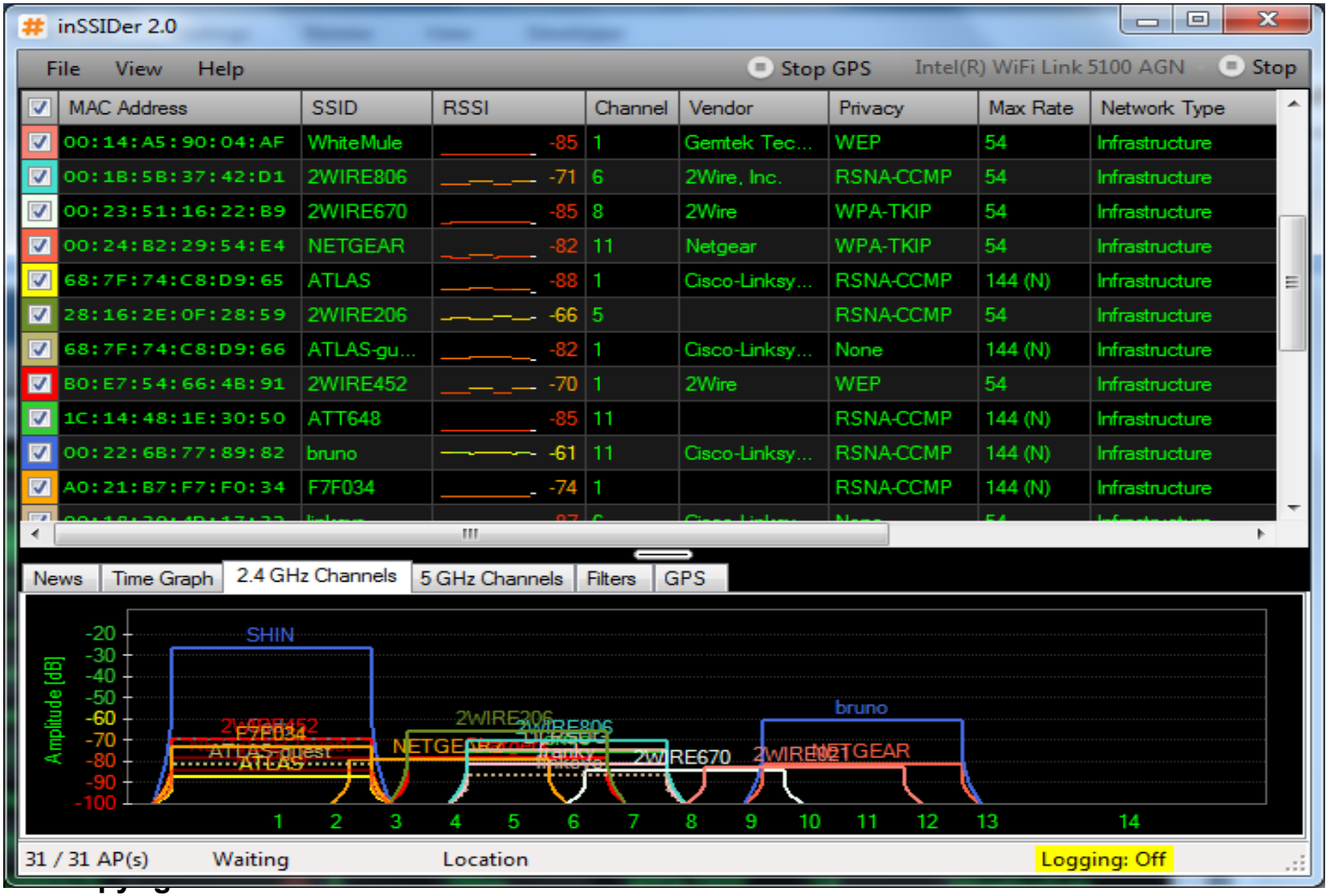
Host name	IP address	MAC address	State
Shin09	172.26.10.1	0203.23AB.D051	Associated
Jmon	172.26.10.12	0203.23A3.D591	Authenticated
Glan7	172.26.10.14	0203.236B.A031	Associated

Figure 8.5 Sample association table

- Thin vs thick access point
- Master AP controller

Cisco Wireless LAN controller
Source: itechdevice.com

8.2.3 Service Set Identifier (SSID)



8.2.4 Service Set (BSS vs. ESS)

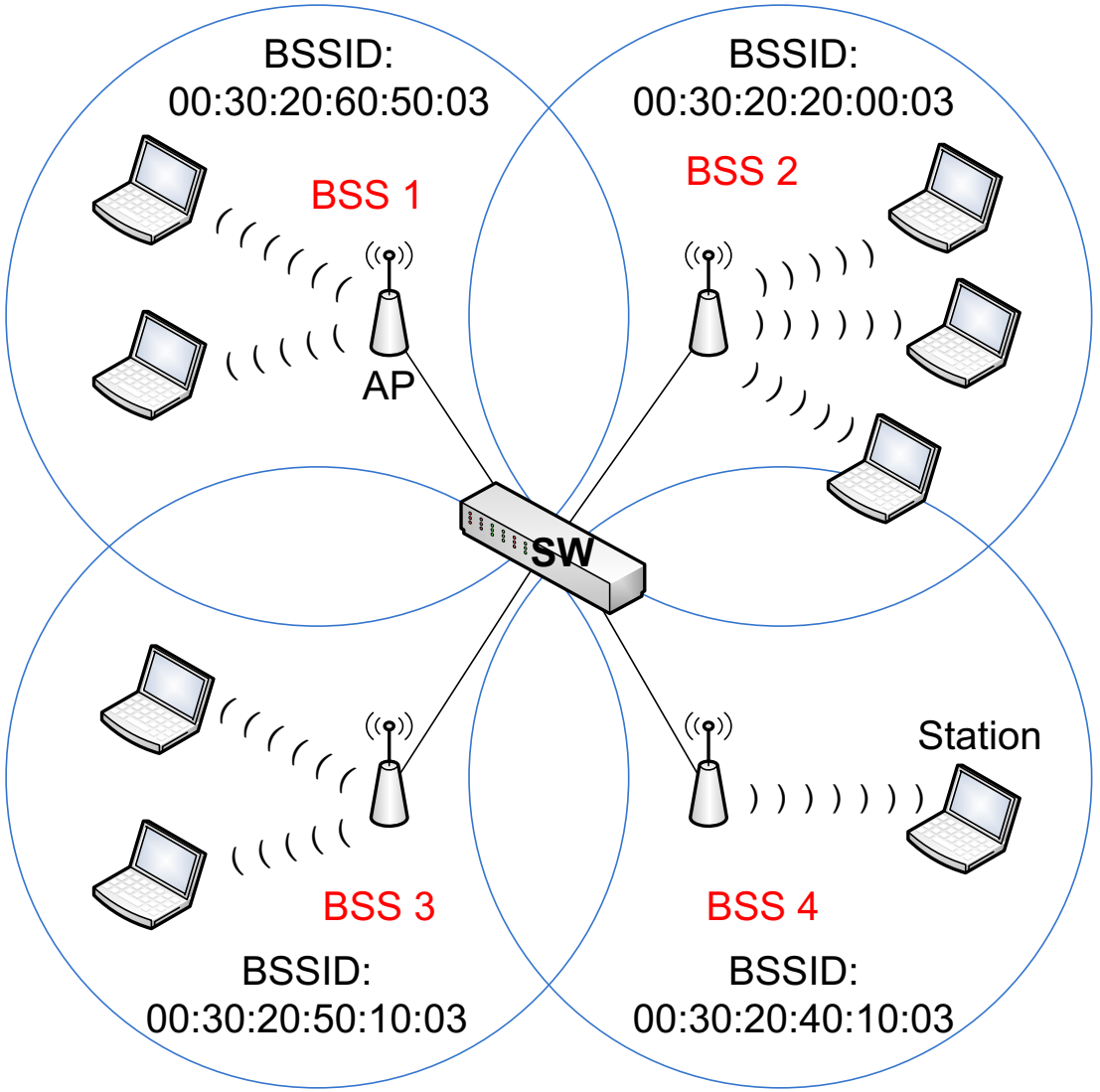
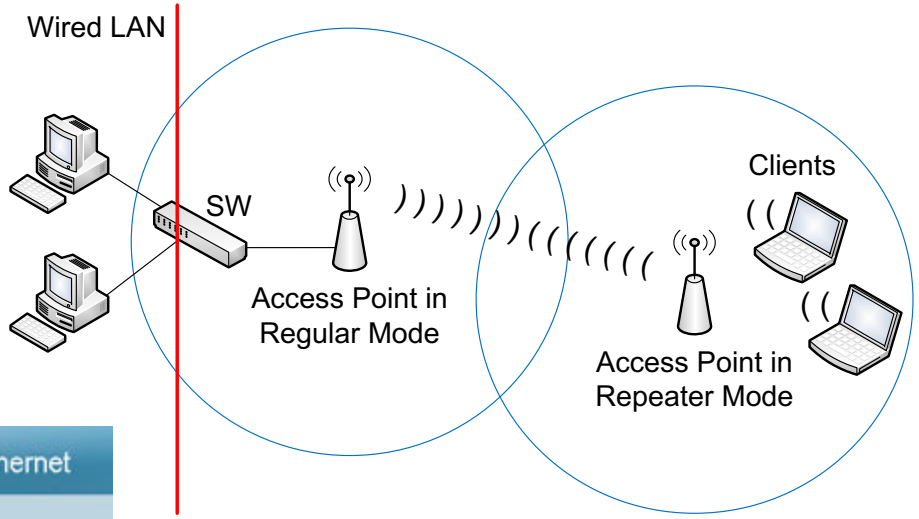


Figure 8.7
Basic service set (BSS) vs. extended service set (ESS)

Extended Service Set (ESS) = BSS1 + BSS2 + BSS3 + BSS4

8.2.5 AP vs. Repeater Mode



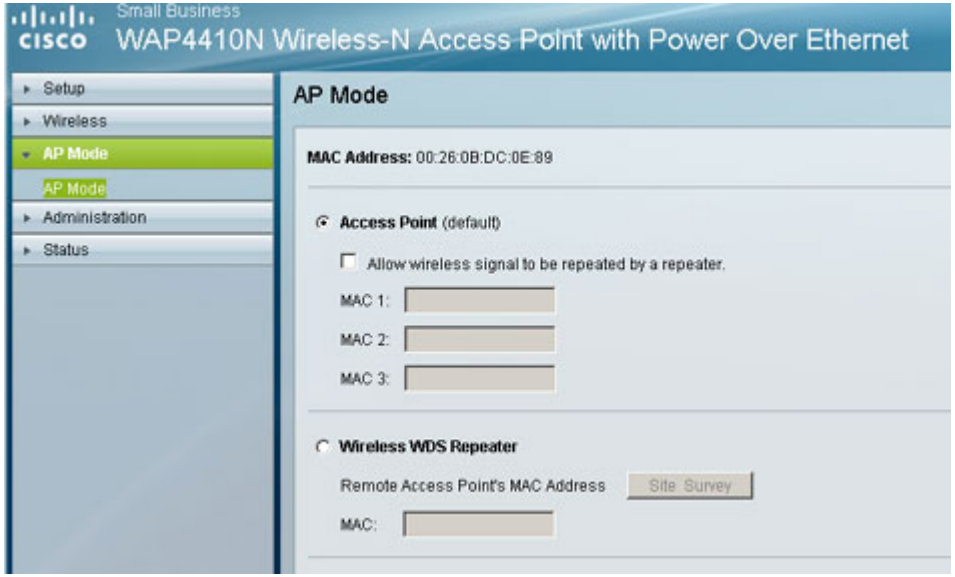
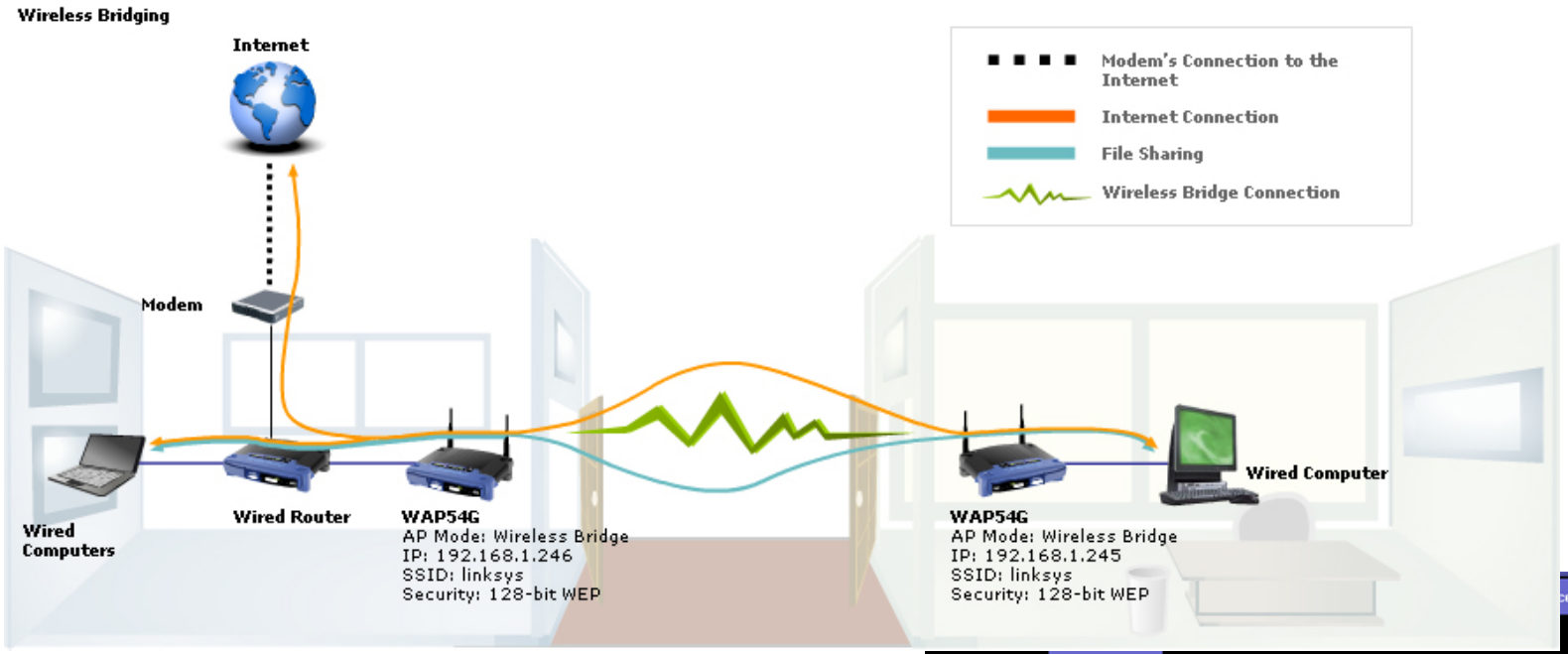
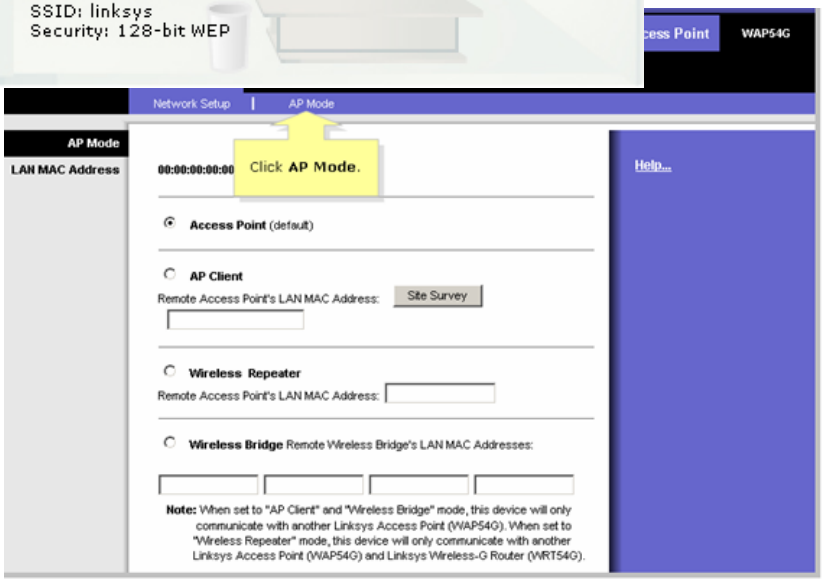


Figure 8.8 Access point in repeater mode

AP vs. Bridge Mode (Extra)





Source: http://www.linksys.com

8.3 Media Access Control

- 8.3.1 CSMA/CA: Carrier Sense Multiple Access/Collision Avoidance
- 8.3.2 RTS/CTS: Request to Send/Clear to Send

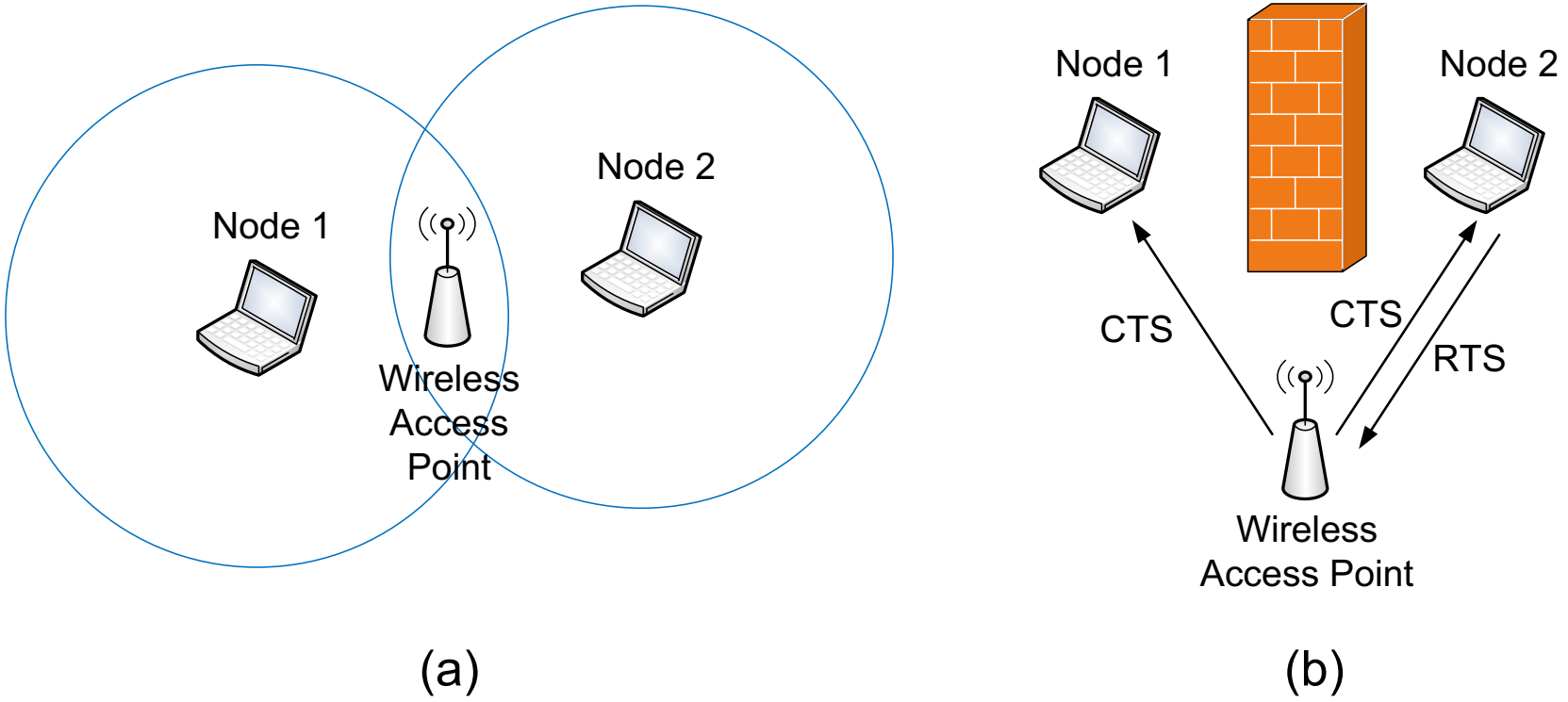


Figure 8.9 Hidden node problems

8.3 Media Access Control

RTS/CTS: Request to Send/Clear to Send

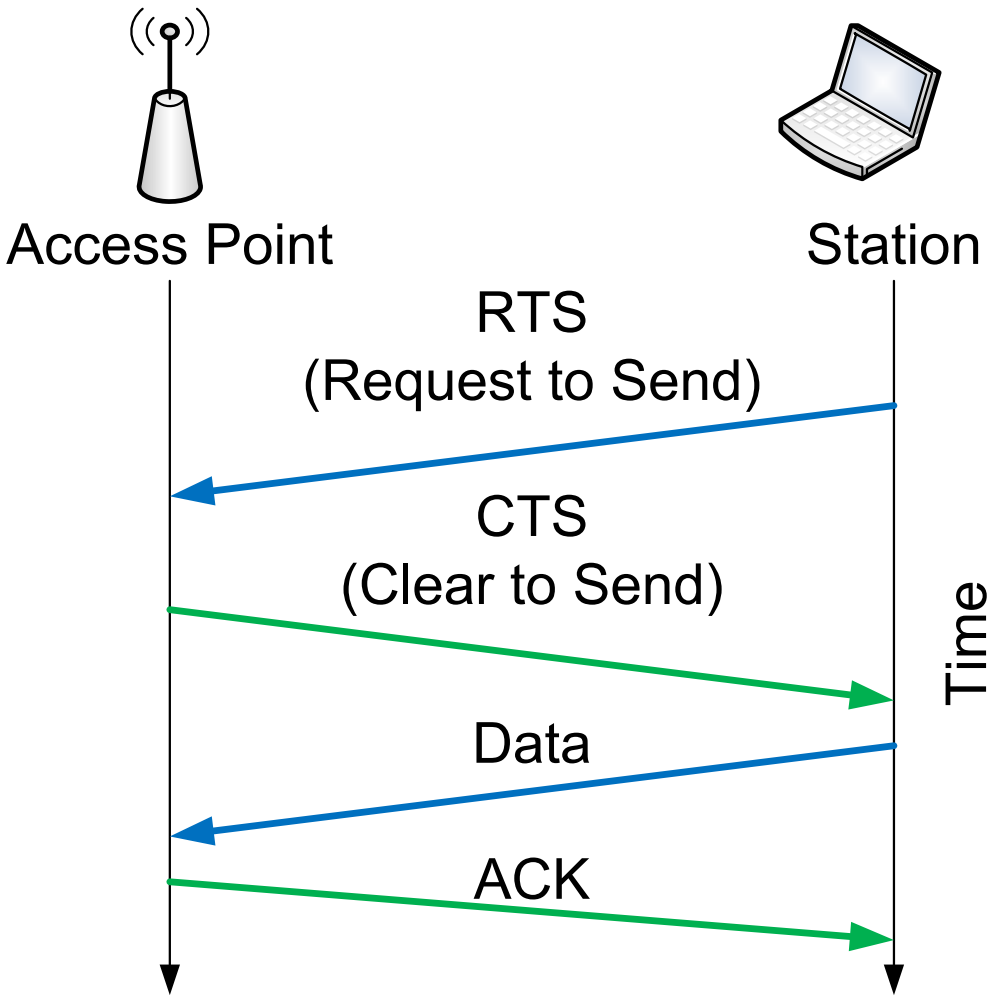
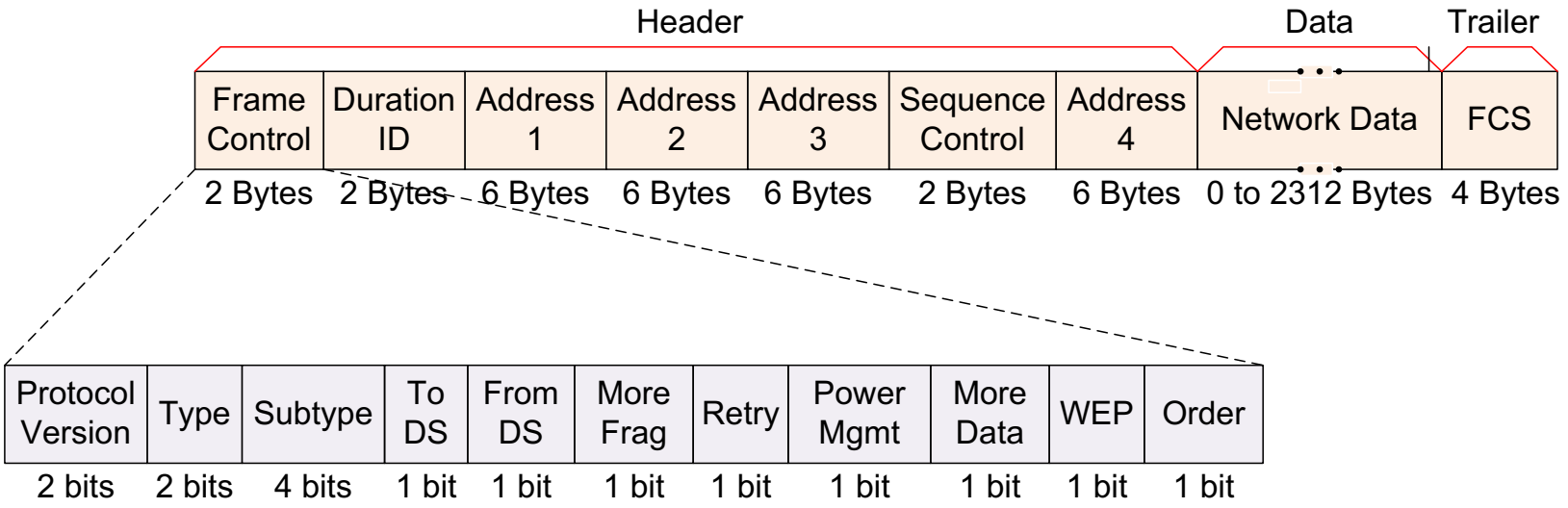


Figure 8.10 4-Way handshake with RTS/CTS

8.4 WiFi Frames

- Data frames

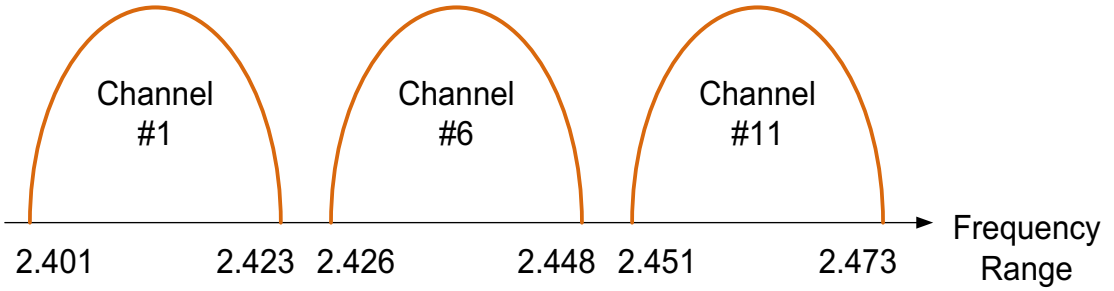


- Management frames: authentication/association frames, beacon frames
- Control frames: ACK frames, RTS/CTS frames

8.5.2 WiFi Channels

Figure 8.12 2.4 Ghz Non-Overlapping Channels (In the US and Canada)

Channel	Lower Frequency	Upper Frequency
1	2.401	2.423
2	2.406	2.428
3	2.411	2.433
4	2.416	2.438
5	2.421	2.443
6	2.426	2.448
7	2.431	2.453
8	2.436	2.458
9	2.441	2.463
10	2.446	2.468
11	2.451	2.473



8.5.3 Planning Basic Service Sets (BSS)

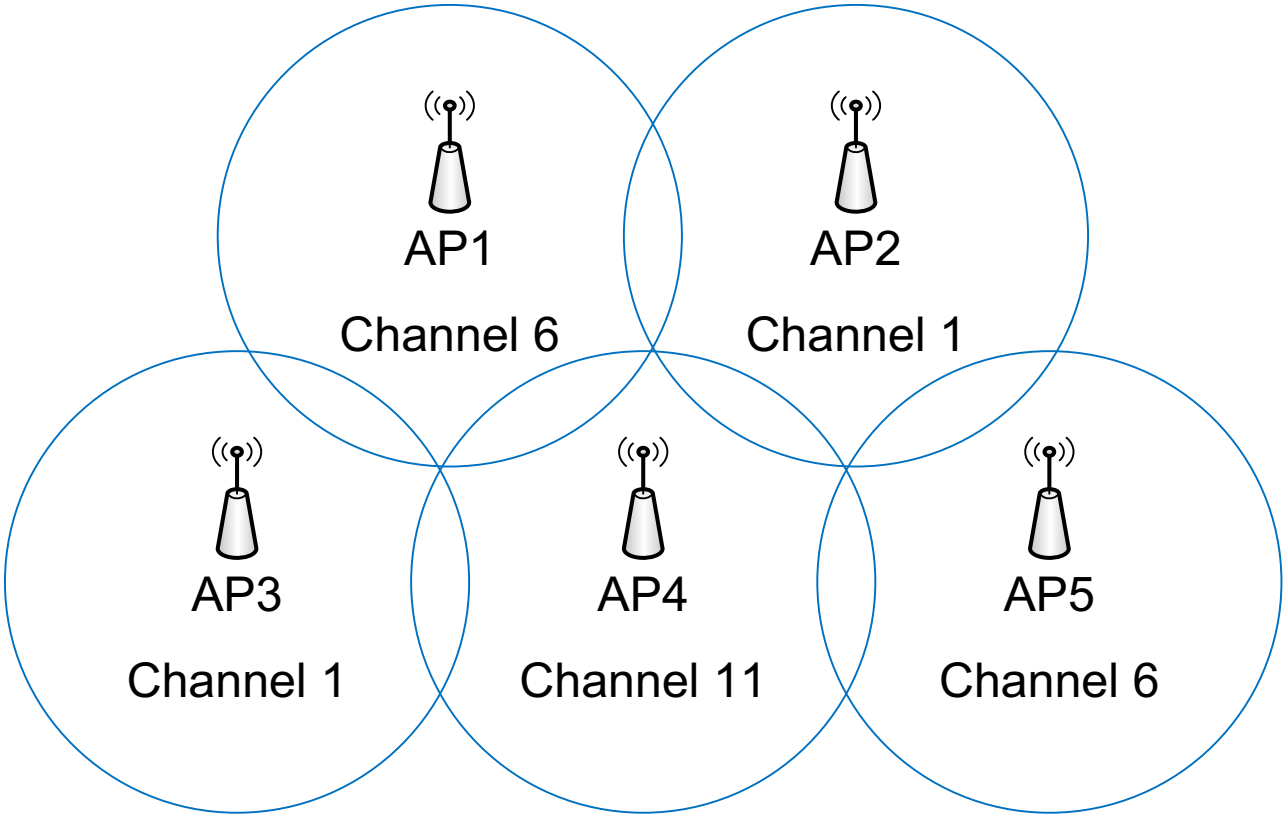


Figure 8.13 WiFi channel selection in an area

8.6 Authentication & Association

8.6.1 Three Stage Process

	State	Description
1	Unauthenticated/ Unassociated	No relationship between a station and an AP
2	Authenticated/ Unassociated	• The client is authenticated by the AP. • For this, the client submits an authentication frame to the AP. • At an enterprise, there is generally a designated authentication server.
3	Authenticated/ Associated	• Upon successful authentication, the client sends an association request frame to the AP. • The AP's association response completes the binding. • At this stage, other options including security and data transmission rate are finalized.

8.6.2 Authentication Methods of a Station

- Open authentication

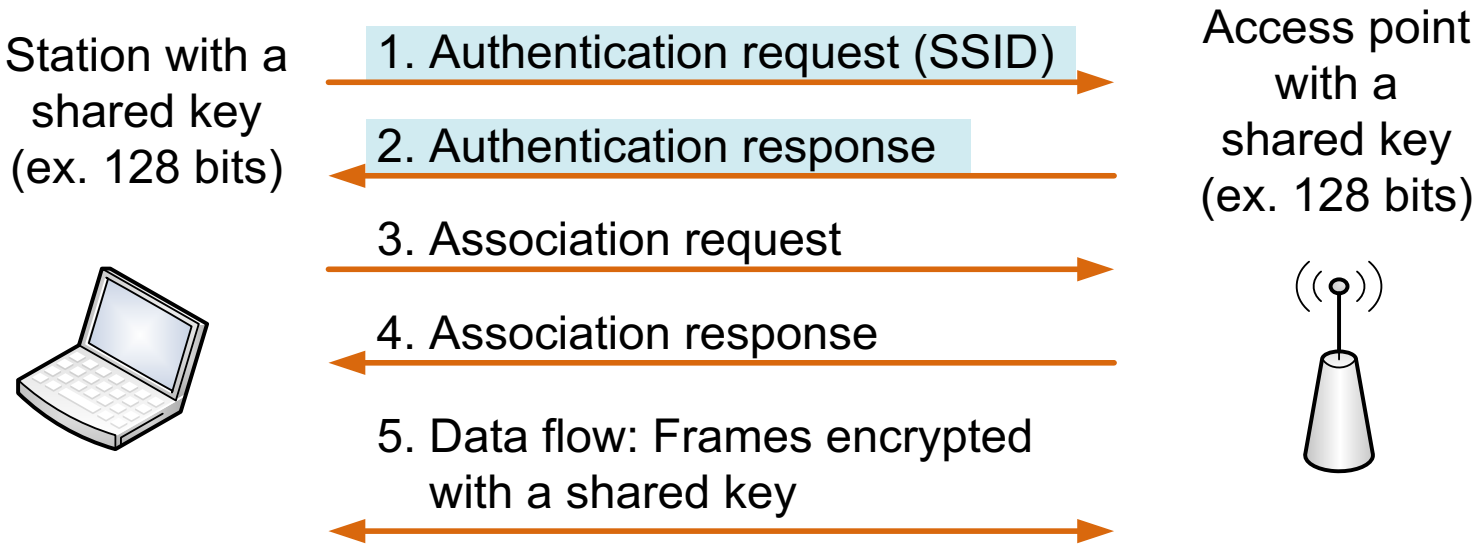


Figure 8.15 Two-way open authentication (step 1 and 2)

8.6.2 Authentication Methods of a Station

- Pre-shared key authentication

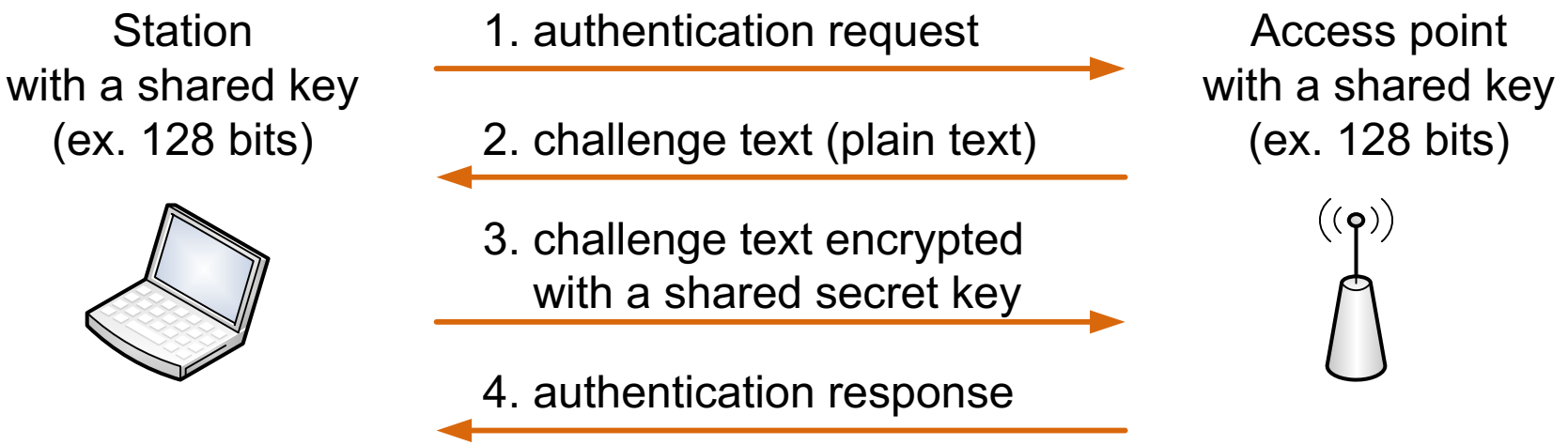


Figure 8.16 Four-way shared-key authentication

8.6.2 Authentication Methods of a Station

- Authentication server

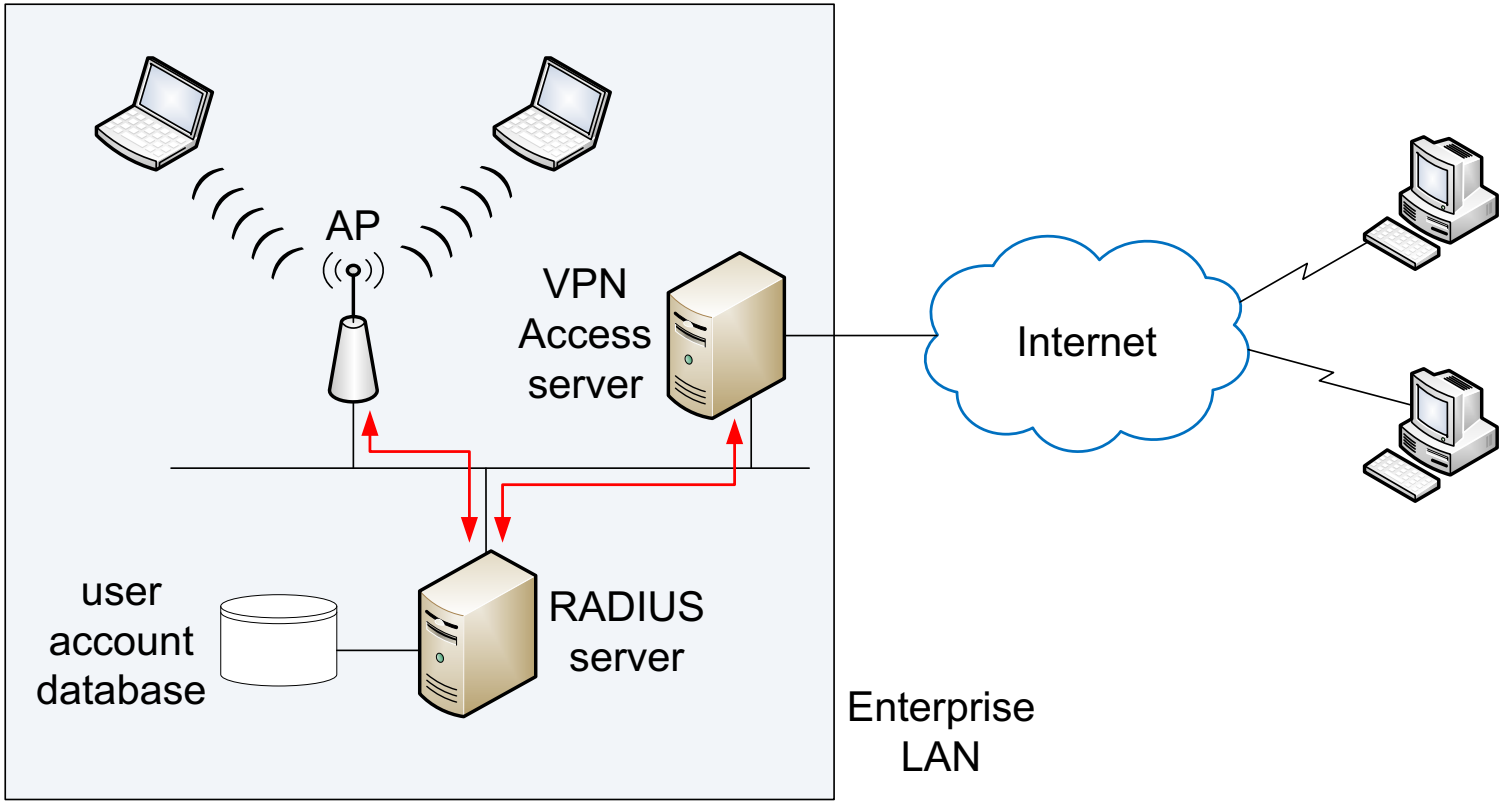


Figure 8.17 Authentication of WiFi stations with RADIUS

8.7 WIFI STANDARDS

Status	IEEE WiFi Standards	Rated Speed
Legacy	802.11b	11Mbps
	802.11a	54 Mbps
On the path to legacy	802.11g	54 Mbps
Current and Emerging	802.11n	100-600 Mbps
	802.11ac	Up to 1.3 Gbps

Table 8.5 WiFi standards

8.7.1 802.11n

- Throughput Modes
  - 20MHz and 40MHz
  - *channel bonding*
- 2.4/5.0 GHz Bands
  - *concurrent dual-band transmission*
  - *non-concurrent dual-band transmission*
- Multiple antennas: multi-path propagations
- Support both SISO and MIMO
- Single-user MIMO: Up to 4 data streams (or spatial streams)
- QoS Support (IEEE 802.11e)

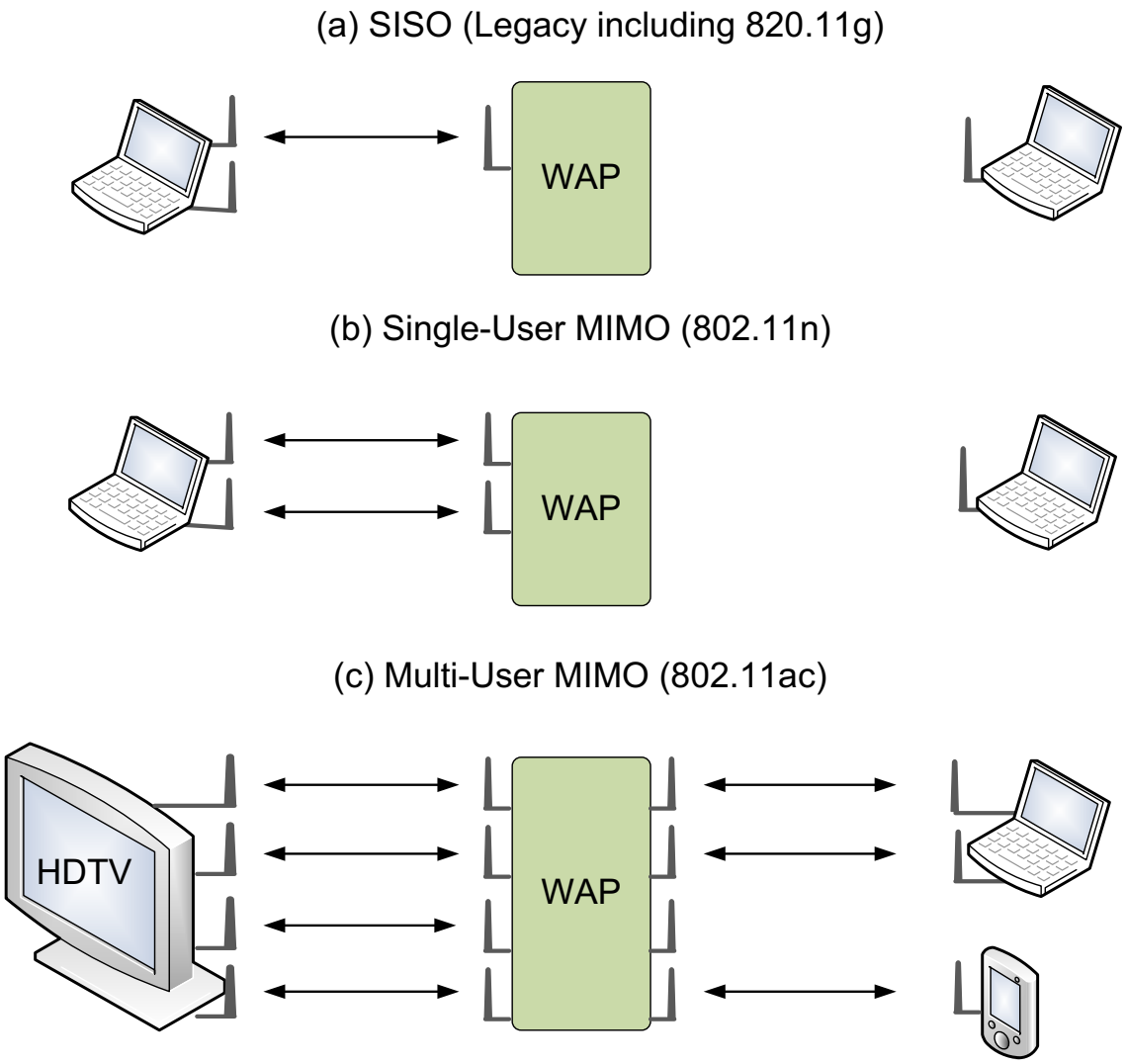
8.7.2 802.11ac

- 5.0 GHz Band

- Throughput Modes
  - 20MHz and 40MHz for backwards compatibility
  - 80MHz and 160MHz for faster throughputs.
  - Up to 8 data streams (or spatial streams)

- Support both
  - Single-user environment
  - Multi-User MIMO (MU-MIMO)

Figure 8.18 SISO, single-user MIMO, and multi-user MIMO



8.7 WiFi Standards

Features	802.11g	802.11n	802.11ac
Frequency bands (unlicensed)	2.4 GHz	2.4 / 5.0 GHz	5.0 GHz
Channel bandwidth options (in MHz)	20	20 (mandatory) 40 (optional)	20, 40, and 80 (mandatory) 160 (optional)
No. of concurrent data streams supported	1	up to 4	up to 8
MIMO-support	N/A (SISO)	Single-user MIMO	Multi-user MIMO
No. of clients concurrently supported by an AP	1	1	up to 4

Table 8.6 Comparison of WiFi standards

8.9 WiFi Home Networking

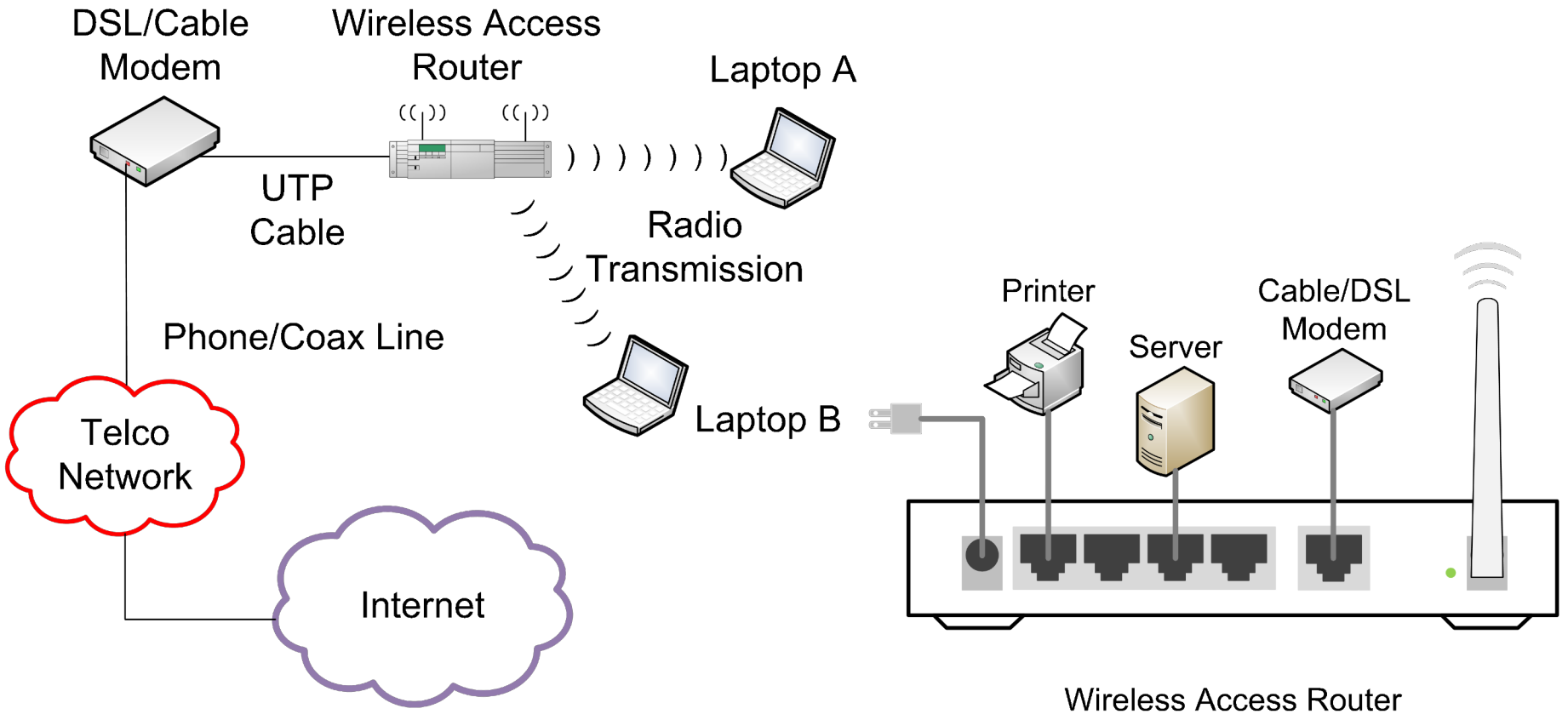


Figure 8.20 WiFi home networking and wireless access router

8.9 WiFi Home Networking

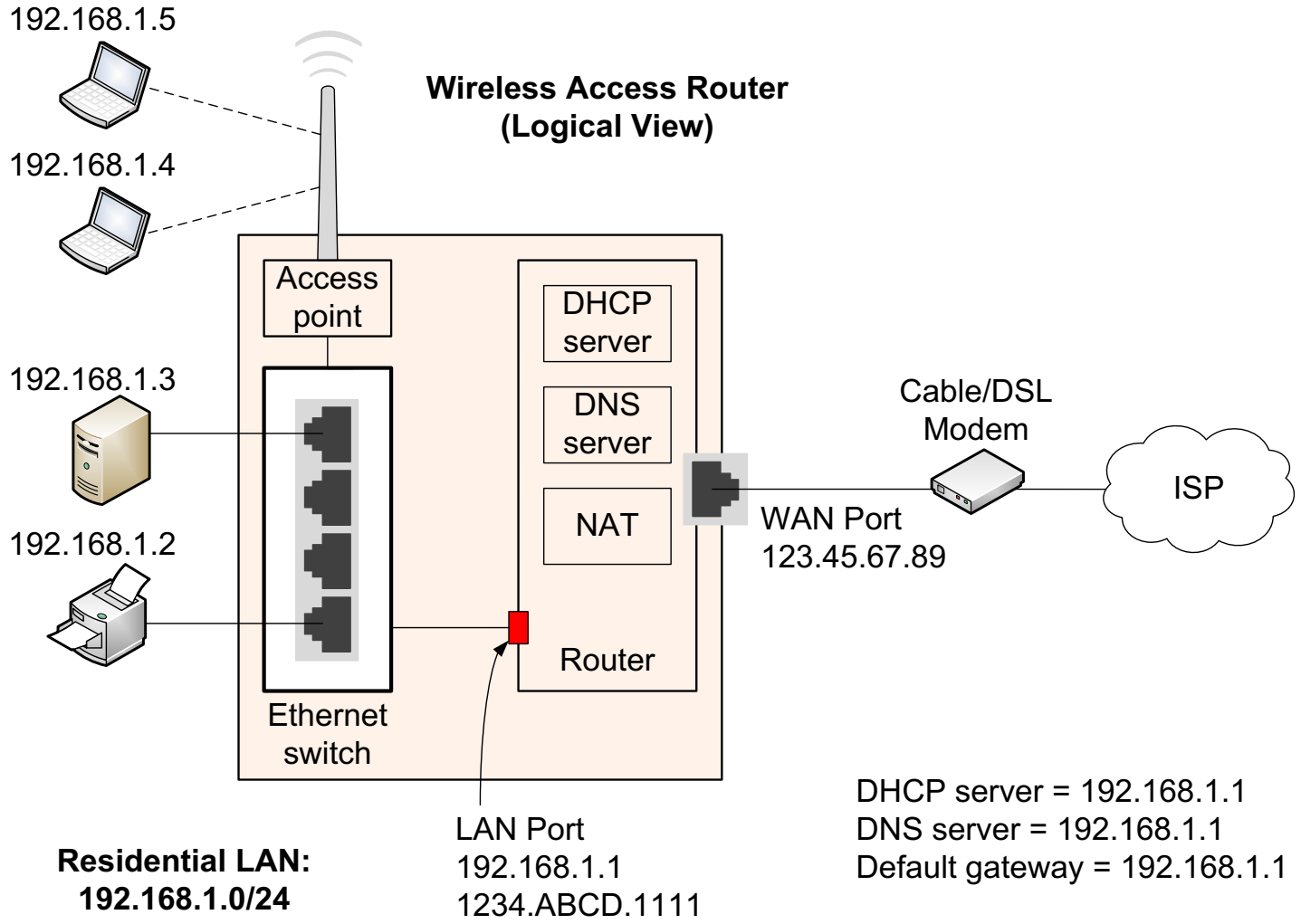


Figure 8.21 Wireless Access Router – Logical View

End
Chapter 8

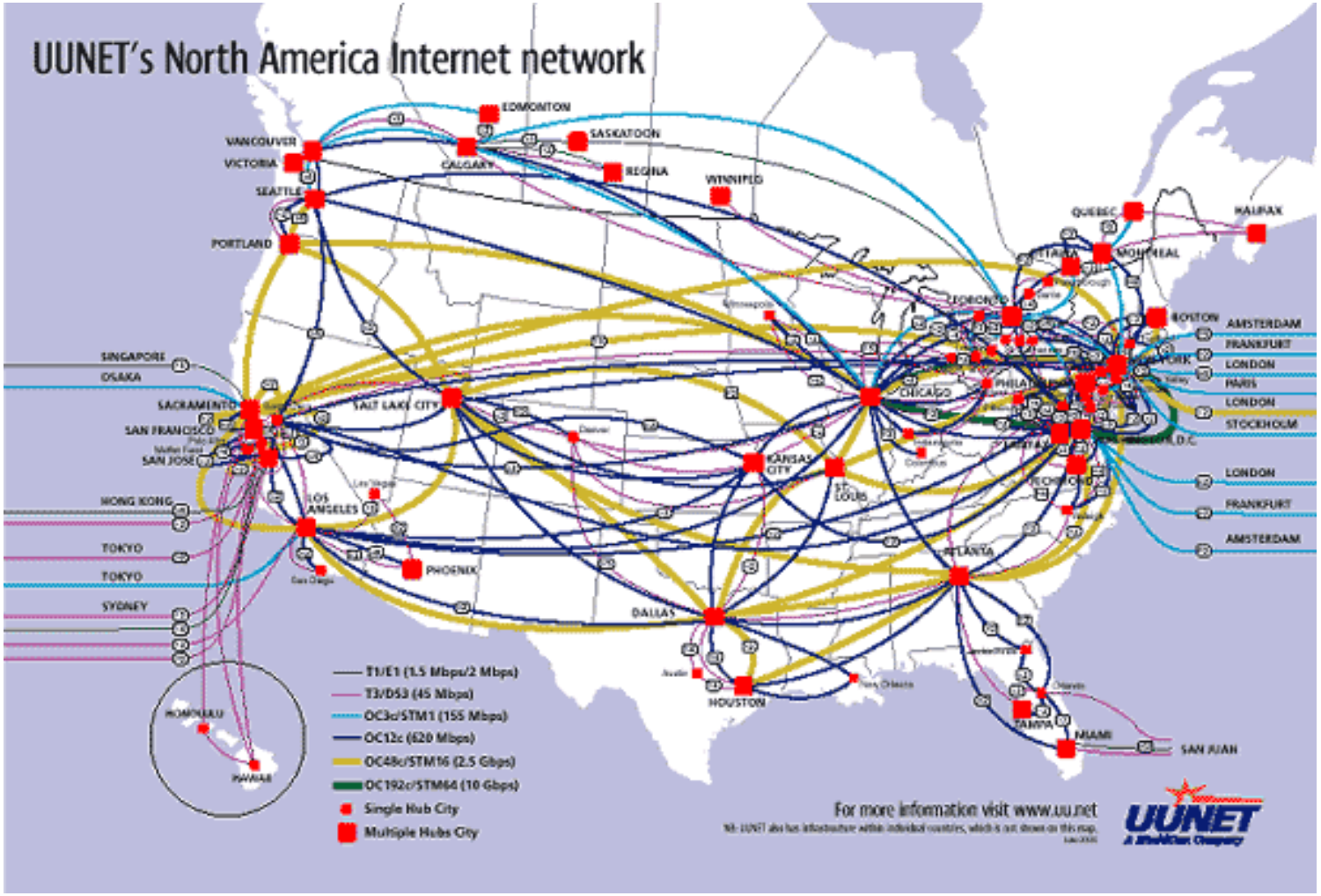
CECS 303 Networks and Networks Security

The Internet & Client-Server System
Chapter 10

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

10.2 Internet Architecture

10.2.1 Internet Service Provider (ISP)



Source http://www.serverprofessionals.com

10.2 Internet Architecture

10.2.1 Internet Service Provider (ISP)

- National ISPs (or Tier 1 ISPs)
- Regional/local ISPs (Tier 2/Tier 3 ISPs)

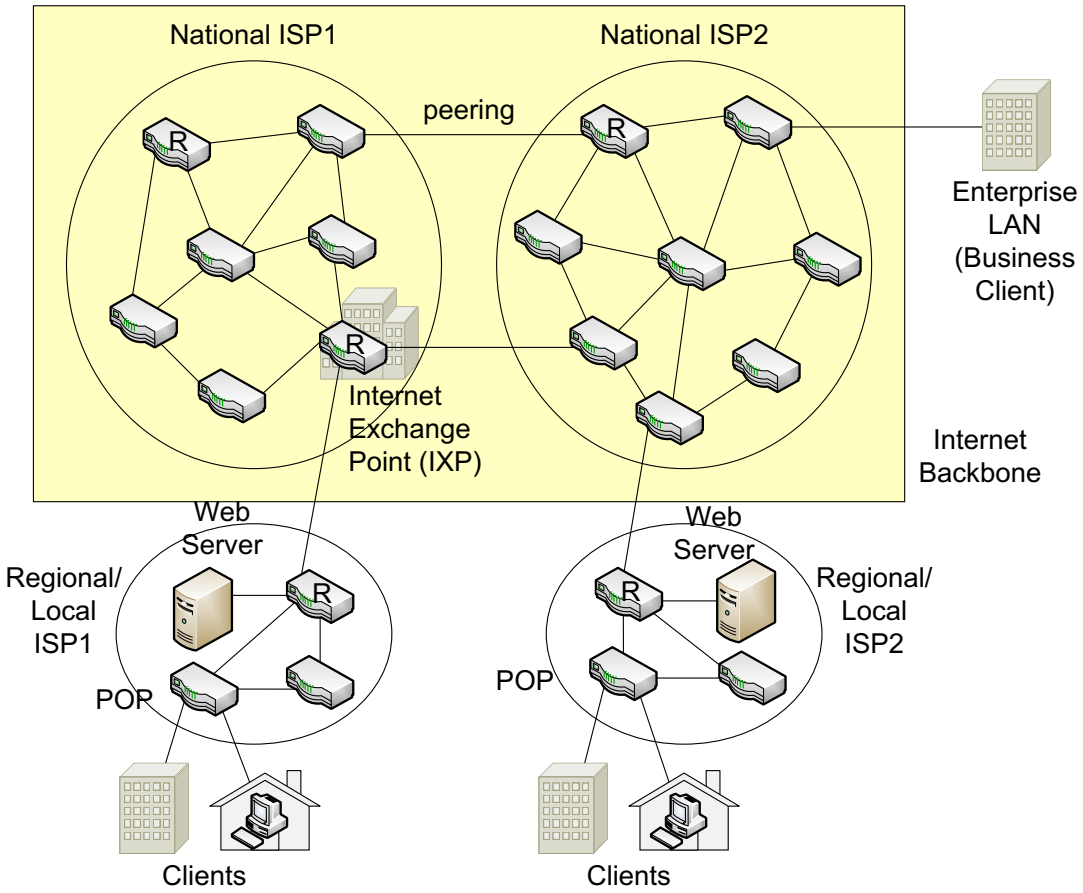


Figure 10.2 Internet architecture and ISPs

10.2 Internet Architecture

10.2.2 Internet Exchange Point (IXP)

Internet Exchange Point (IXP) = Network Access Point (NAP)

Figure 10.3 Select IXP locations on the planet (Go Green!)

Internet Exchange Point (IXP)
Source: http://en.wikipedia.org

Inside of an Internet Exchange Point
Source, http://cajnewsafrica.com/

10.2 Internet Architecture

10.2.3 Autonomous System (AS)

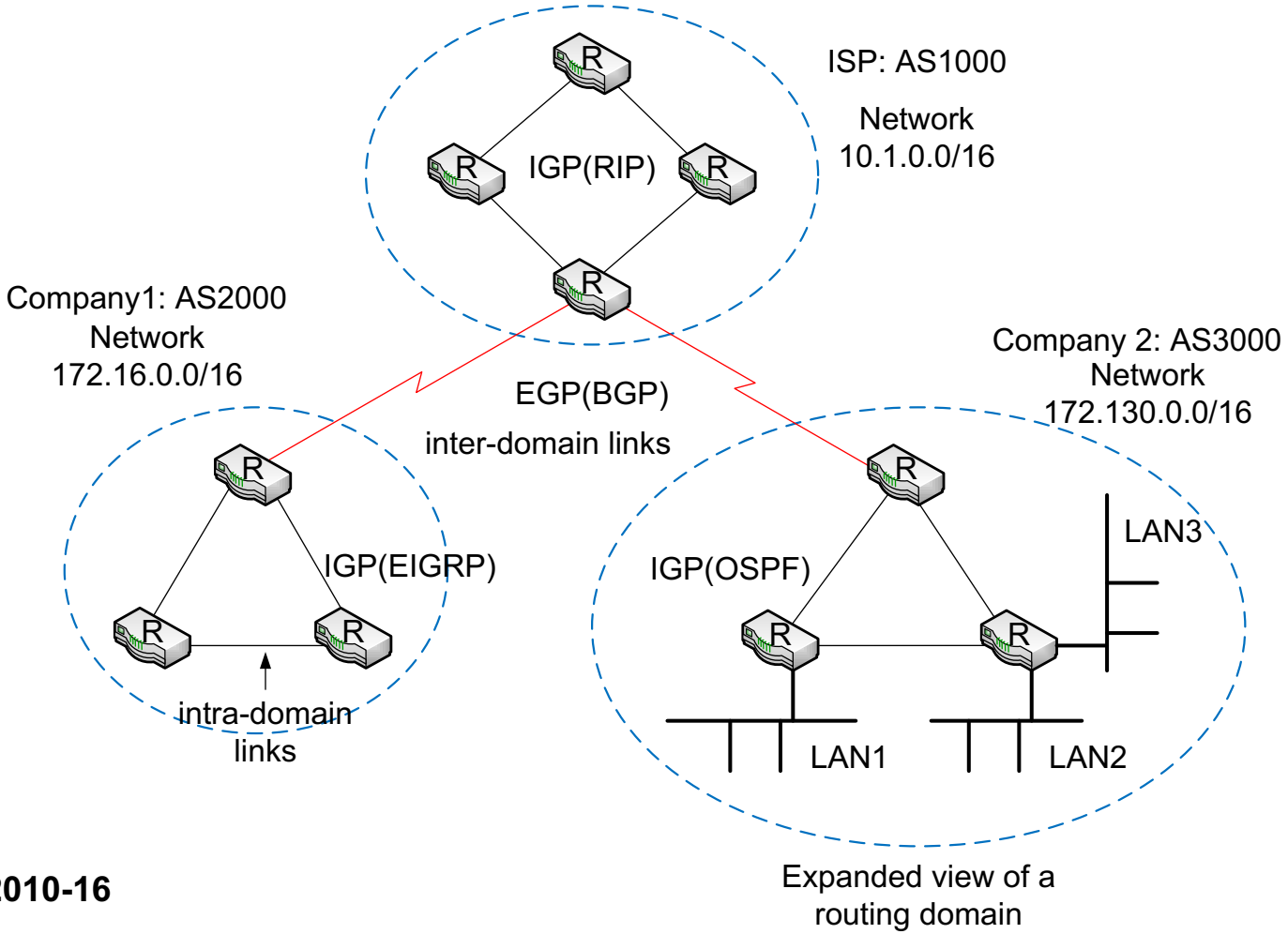


Figure 10.4
An Illustration of Autonomous Systems

10.3 Virtual Private Network (VPN)

10.3.1 Technology

- WAN connections over the Internet
- Use of tunnelling technology

10.3.2 Benefits of VPN

- Cost effectiveness
- Network accessibility and scalability
- Flexibility

10.3.3 Risks of VPN

- Reliability: Difficulty in maintaining QoS
- Security

10.3.4 Types of VPN

- Remote access VPN
- Site-to-site VPN

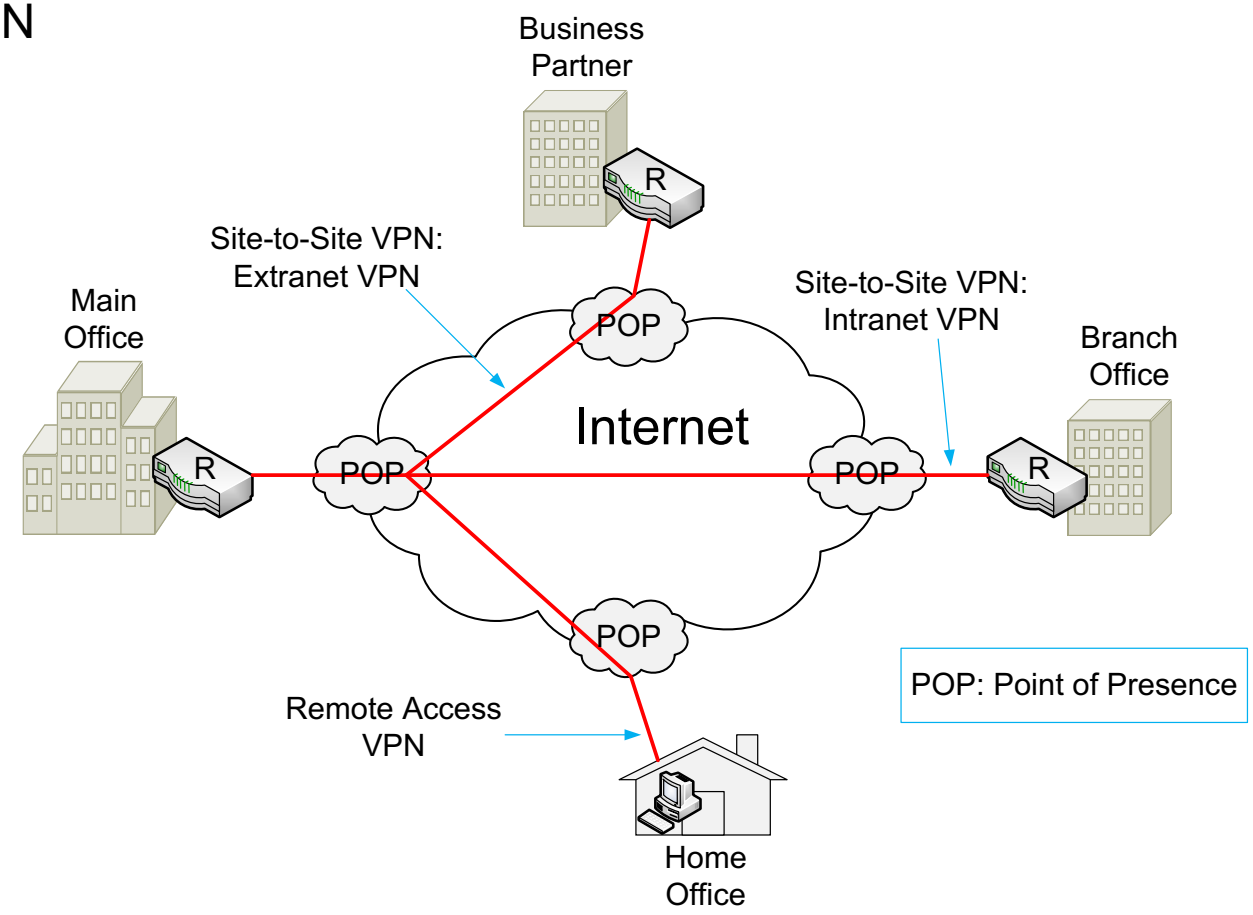


Figure 10.6 VPN Types

10.3.5 VPN Standards

Layer	Protocols
Transport	SSL/TLS (Secure Socket layer/Transport Layer Security)
Internet	IPsec (IP Security)
Data Link	PPTP (Point-to-Point Tunneling Protocol)
	L2TP (Layer 2 Tunnelling Protocol)

Table 10.1 Popular VPN protocols

10.3.6 IPSec (IP Security)

- *Authentication*
- *Data integrity*
- *Data confidentiality*
- Anti-Replay

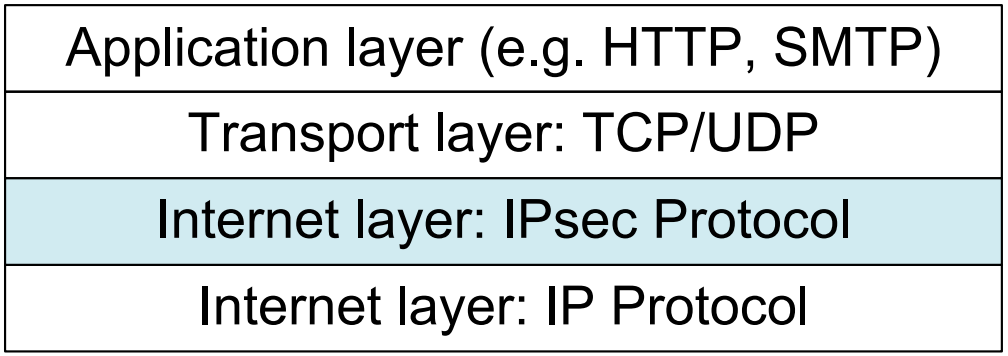


Figure 10.7 The IPSec layer

10.3.6 IPSec (IP Security): Modes

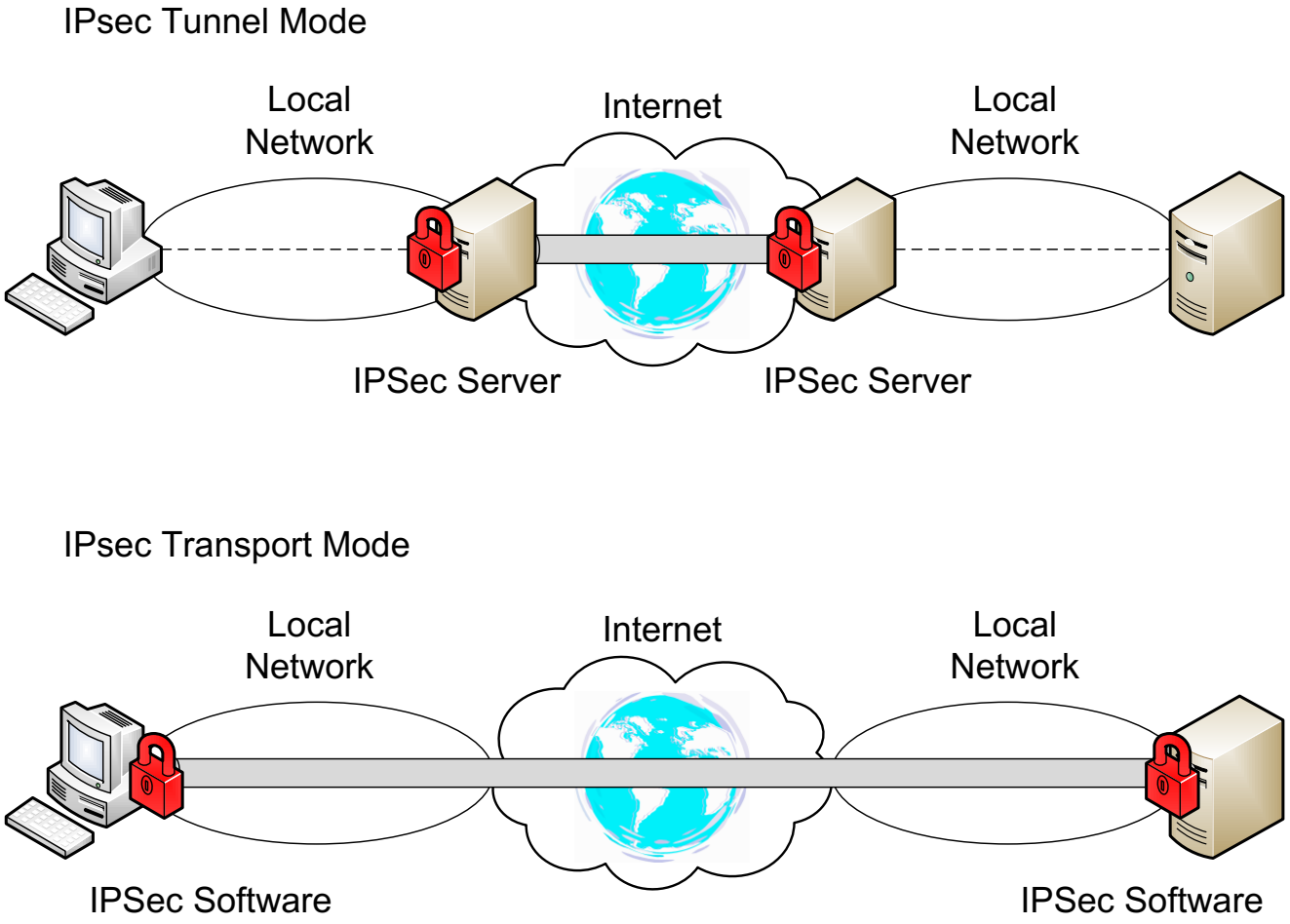


Figure 10.8 IPsec tunnel mode vs. transport mode

10.3.6 IPSec: Modes

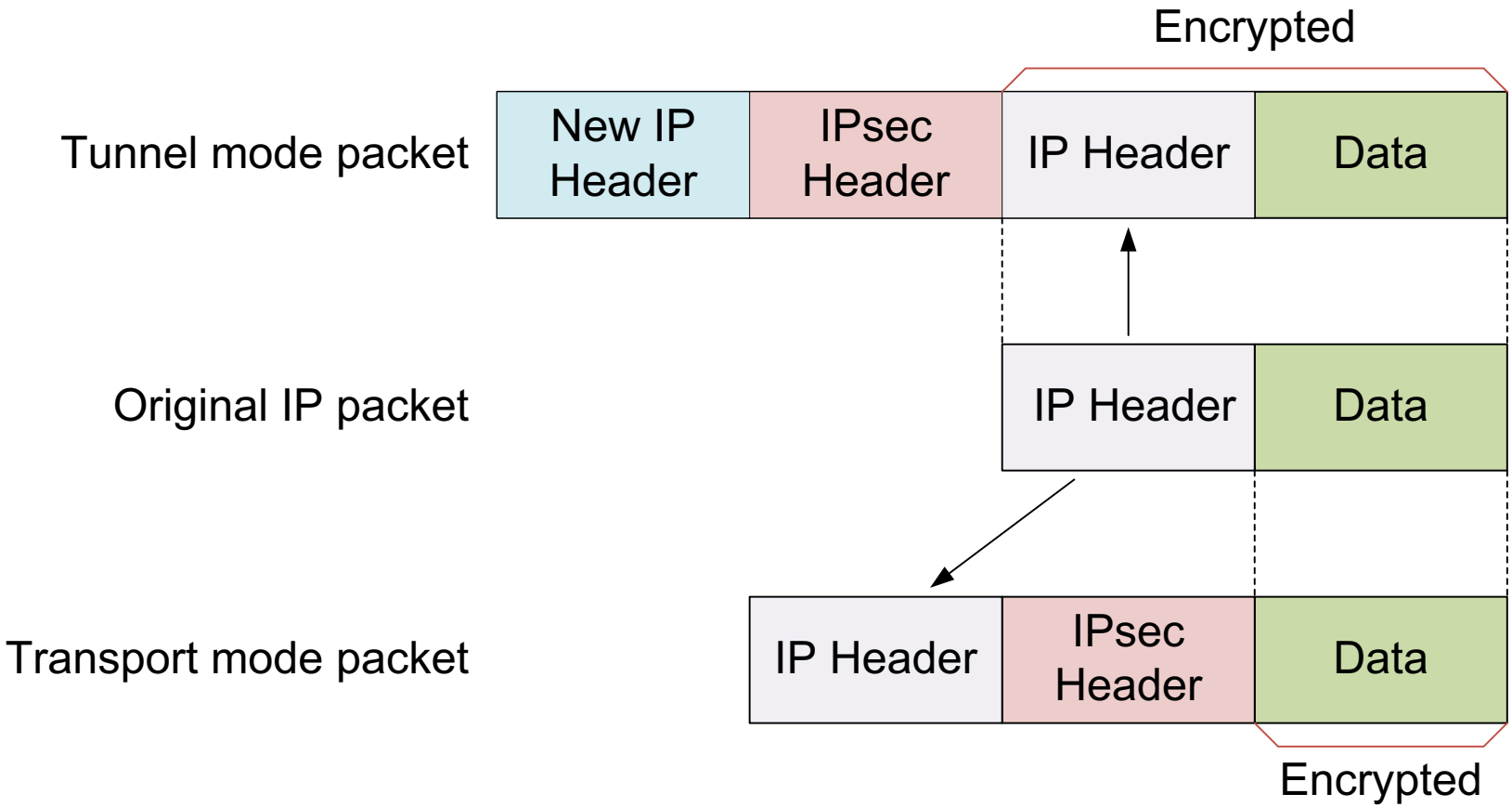
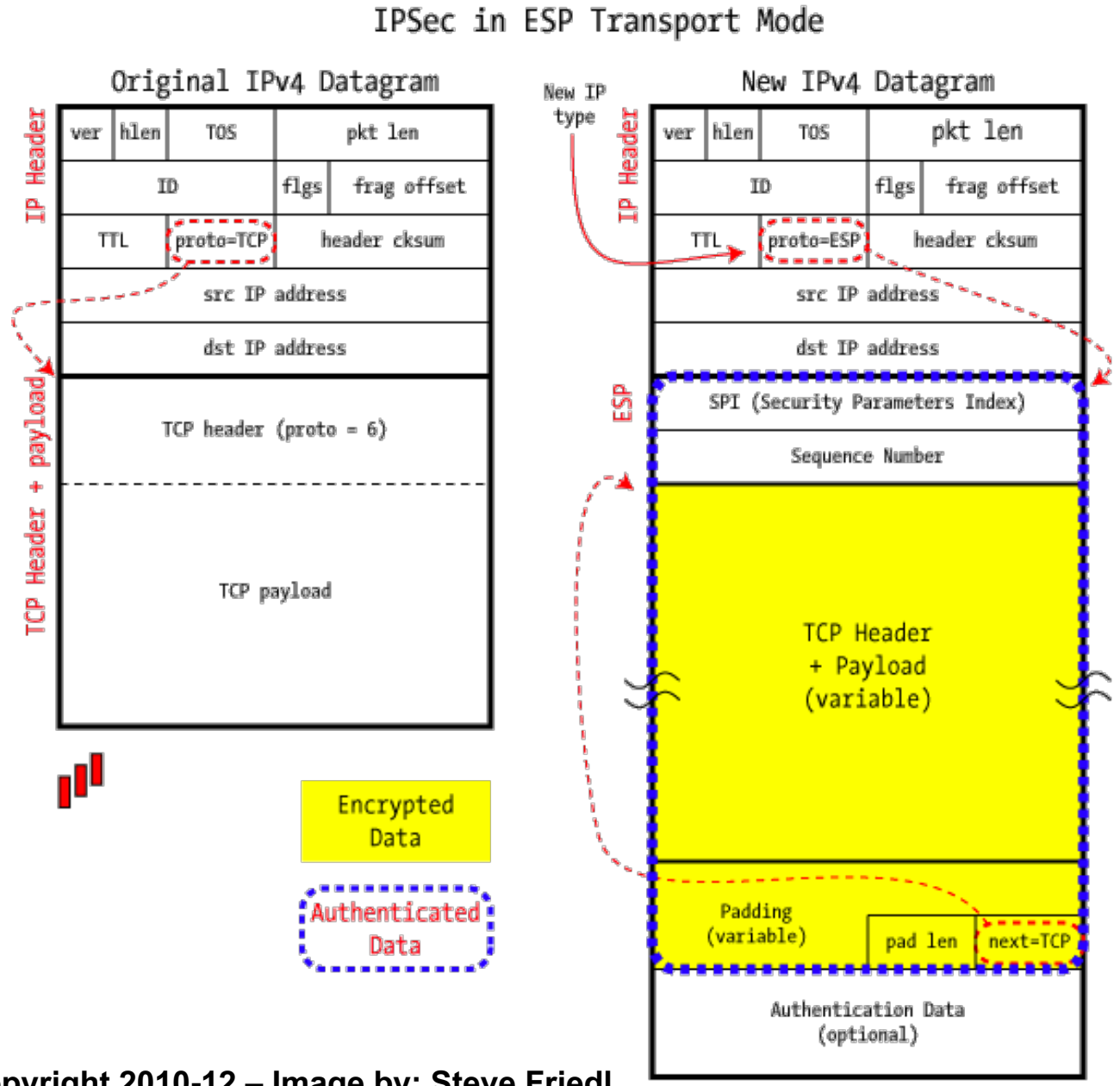
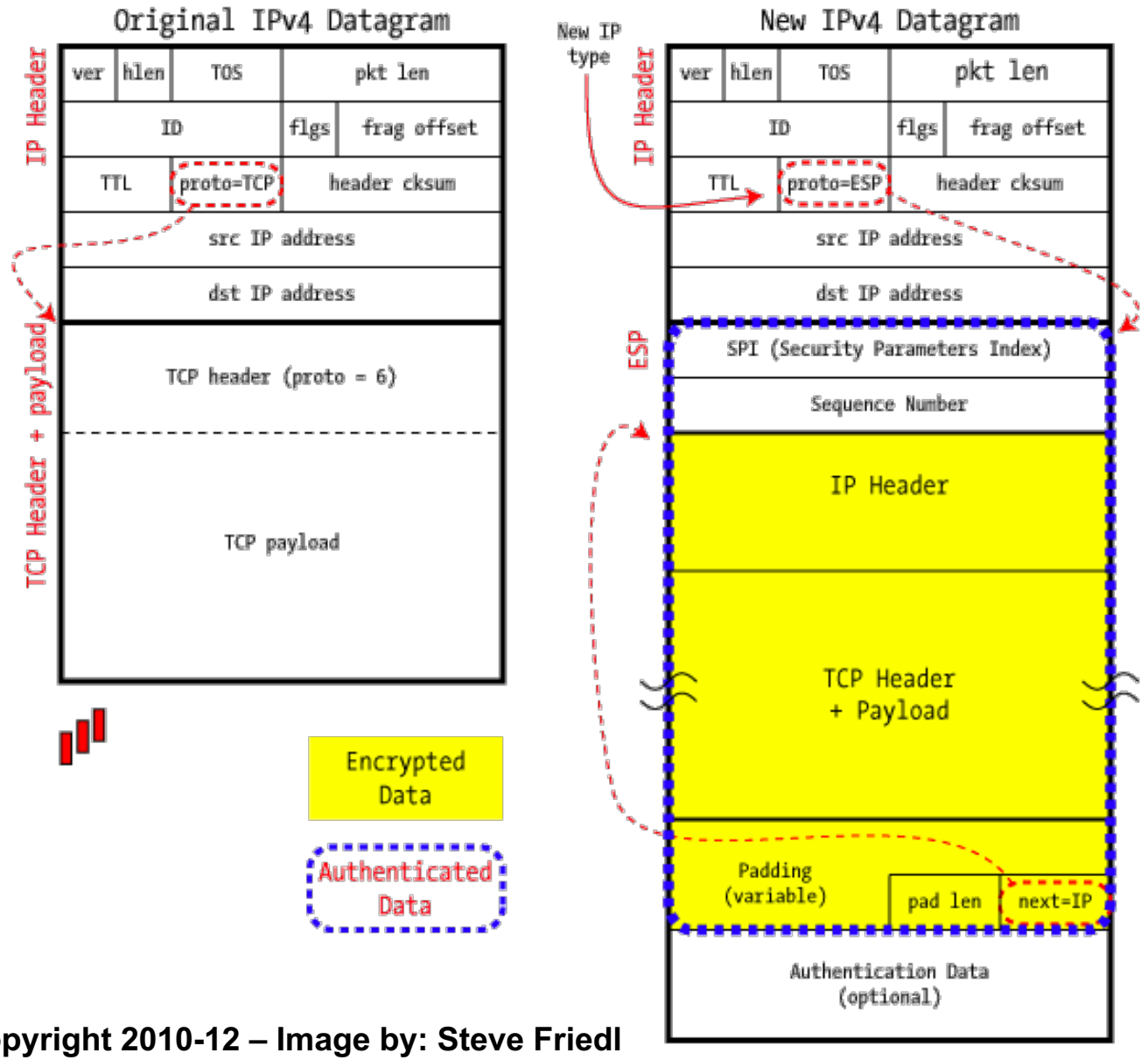


Figure 10.9 IP packet encapsulation: tunnel vs. transport mode



IPSec in ESP Tunnel Mode



Building a Site-to-Site VPN with IPSec

Phase I

- ISAKMP Security Association
- Uses port UDP 500
- Manages the initial connection
- Agrees in the use of encryption and hashing algos
- Key negotiation and lifetime
- Tunnel turn on when interesting traffic is present
- Policy set parameters

Building a Site-to-Site VPN with IPSec

Phase 2

- IPSec security association
- Transform set parameters
- Protects and encrypts the users data before traversing the tunnel
- Two SA are built: one for inbound and one for outbound traffic

Both phase 1 and 2 are activated at the time of the device detecting interesting traffic

10.3.7 SSL (Secure Socket Layer)

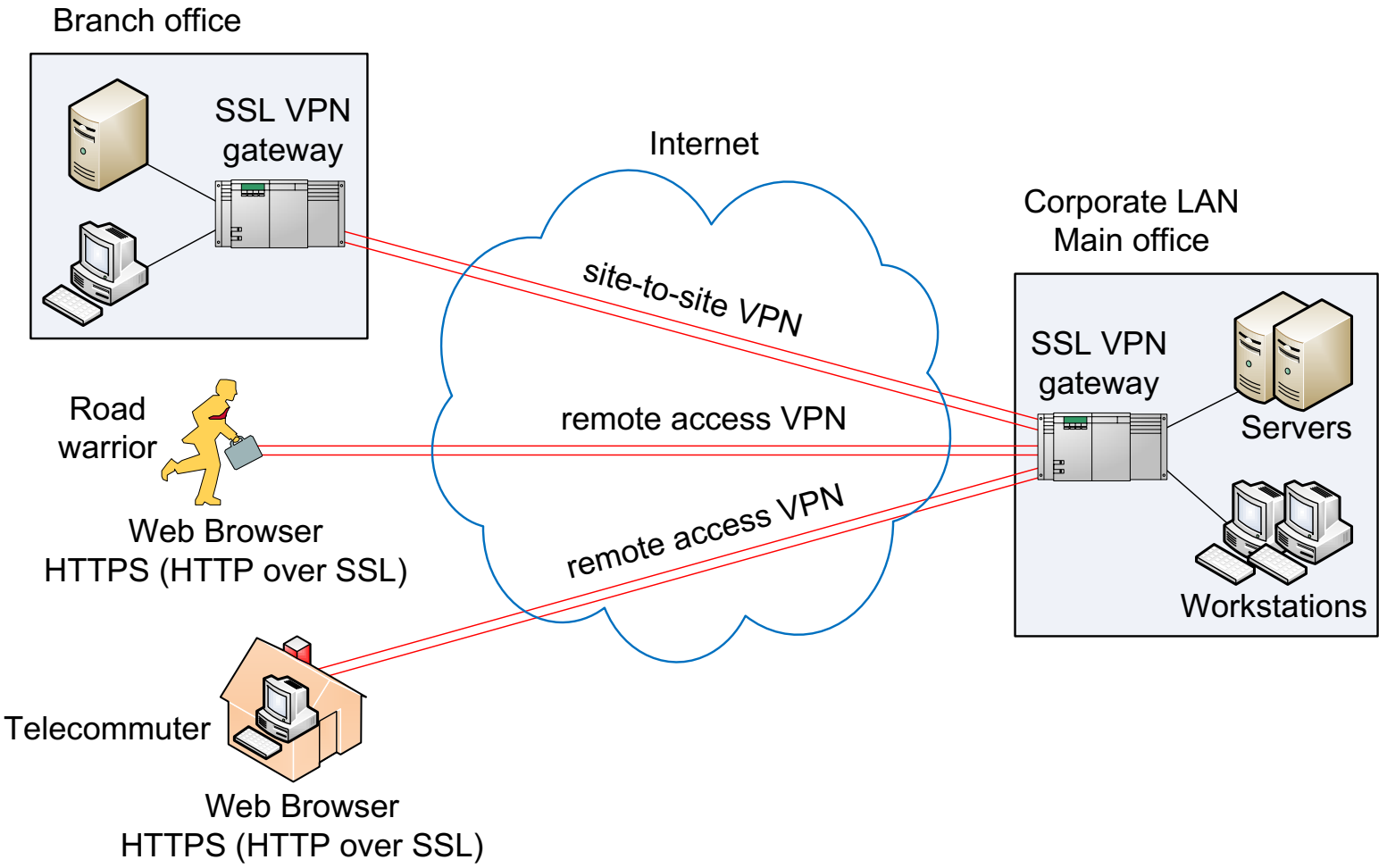


Figure 10.10 VPN implementation with SSL/TLS

10.3.7 SSL (Secure Socket Layer)

SSL and Internet Commerce

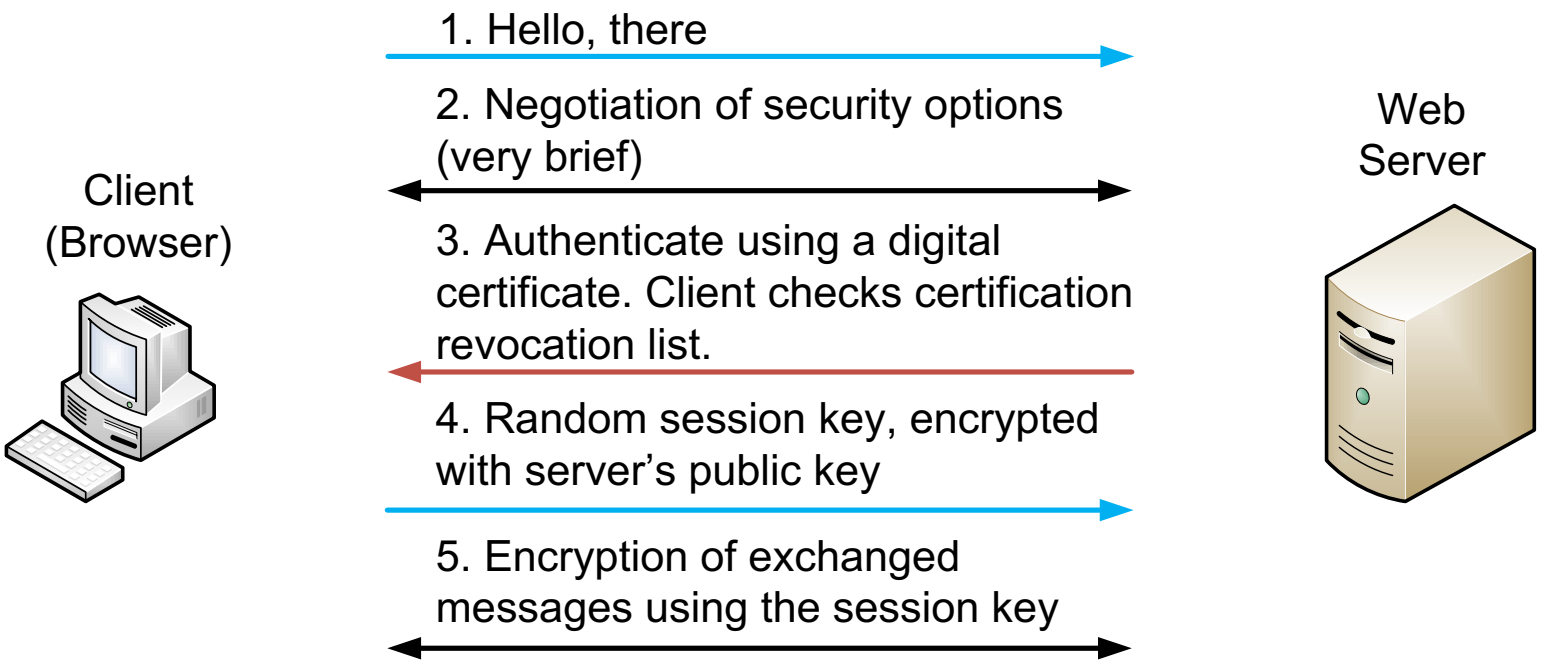


Figure 10.11 Server authentication with SSL in e-commerce

10.3.8 IPSec vs. SSL

	IPSec (IP Security)	SSL/TLS
Layer	Internetwork layer	Transport layer
Software	Should be installed and maintained for each user station.	Built into the web browser
Setup and maintenance Cost	High setup, maintenance and update burden with a large installation base.	Low maintenance and update costs.
Ease of use	End-user training is necessary.	No need for end-user training.
Overall security	Generally provides a higher level of security than SSL.	Considered less secure than IPSec
VPN implementation	Complicated as security configuration in each station requires expertise.	On the client-side it works more like plug-and-play.

End
Chapter 10

CECS 303 Networks and Networks Security

Network Security: Threats
Chapter 11

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

11.2 Malicious Codes: Malware

Many different types of malware

Source: http://fullonn.blogspot.com/

11.2 Malicious Codes: Malware

11.2.1 Virus:

- Executable program with many different types of damage if infected
- Spread by attaching to a benign program
- e.g., ransomware

11.2.2 Worm:

- A program to be able to self-replicate without human intervention
- Not necessarily attached to another program for spreading
- Spreading methods: social engineering, vulnerabilities of OS

11.2.3 Trojan:

- Not designed for infecting files or cause damages
- Not intended for self-replication
- Mainly intended to create backdoors

11.2.4 Bot

- Bot: a remotely controllable program
- Botnet: A collection of such infected computers
- C&C server
- Protocol: IRC, HTTP, P2P
- Conduct evil doing: spamming, stealing personal information, DDOS attacks, phishing, spreading new malware, …..

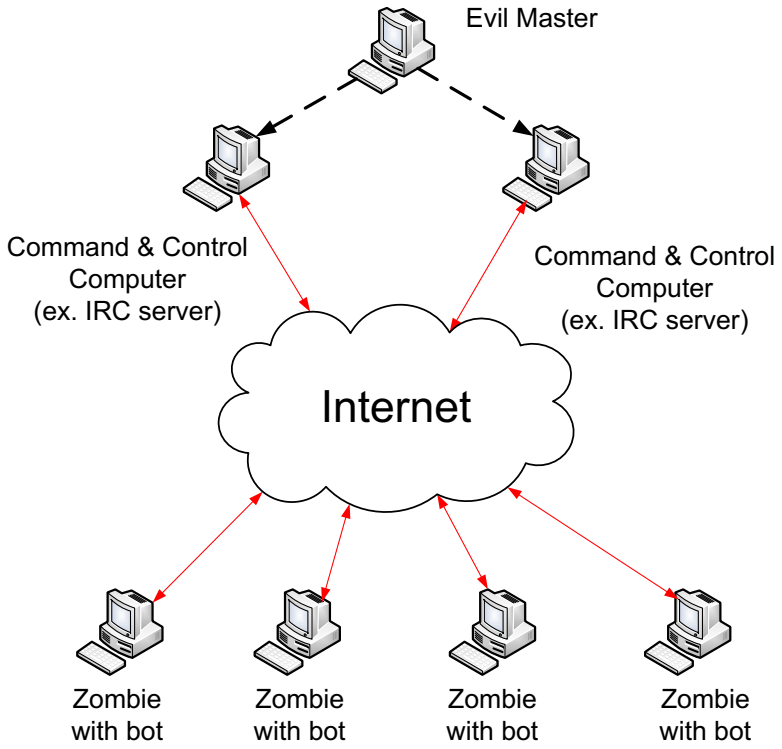


Figure 11.1 Bots and botnet creation

11.3 Password Cracking

- **Hash Function**
  - Popular Hash Algorithms: MD5 and SHA-1
  - One way function
  - Message digest (hash value)
  - Digital fingerprinting: checking the integrity of software

Inputs (ex. passwords)	Outputs (hash values in hexadecimal)
Stealth	→ 899db408cba5858a0f1701a2caef2628
She	→ 1a699ad5e06aa8a6db3bcf9cfb2f00f2
I am a student.	→ 2f1f75e8bb00643cb05aed57f7bdb4a8

11.3 Password Cracking

- **Brute Force Method**

	Password length		
Available characters	6 characters (48 bits)	7 characters (56 bits)	9 characters (72 bits)
Lowercase letters only	10 minutes	4 hours	4 months
Lower & uppercase letters combined	10 hours	23 days	178 years
All ASCII characters that include letters, numbers, and special characters	18 days	4 years	44,530 years

Table 11.2 Password cracking with brute force (source: businessweek.com)

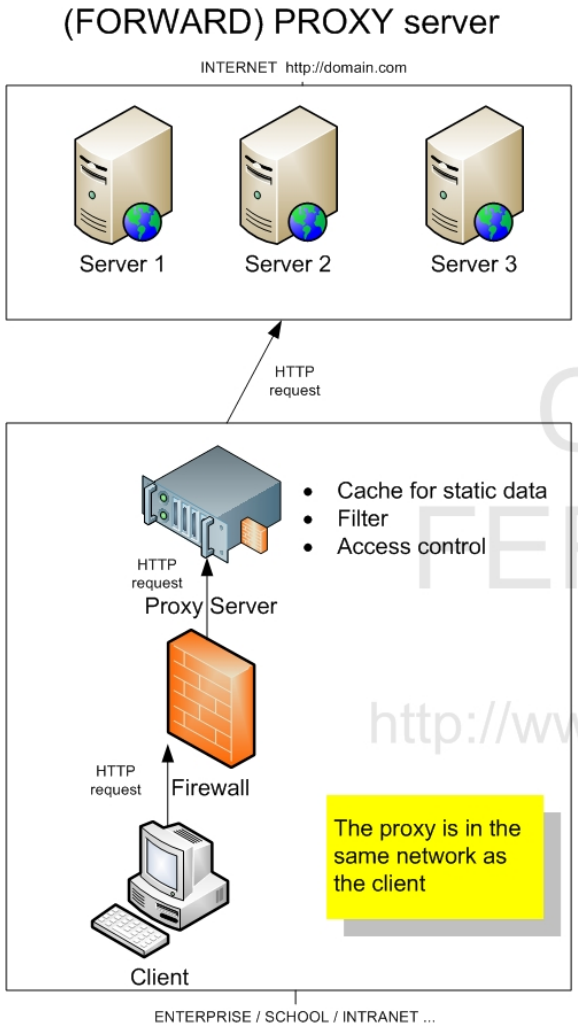
- **Dictionary Method**
- **Many software tools: (e.g., Cain & Abel)**

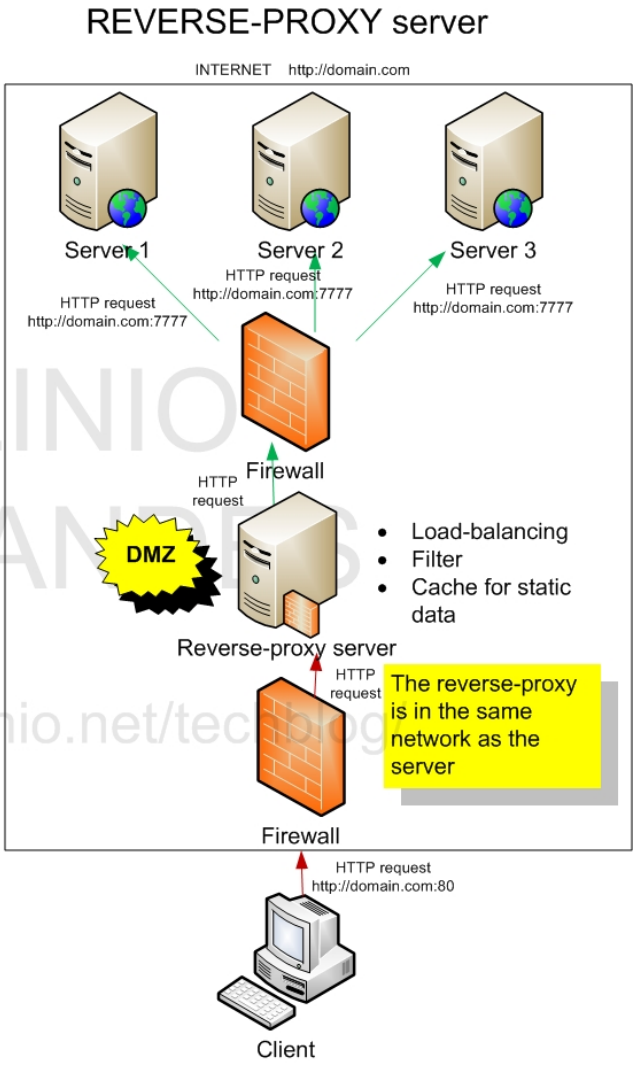
11.4 Spoofing (or Masquerading)

- Pretending (or faking) to be someone or something
- Among them are:
  - IP Address Spoofing
    - IP spoofing software
    - IP proxy server
    - Online proxy sites (e.g., https://zend2.com)
  - MAC Address Spoofing
  - Email Address Spoofing
  - Web (or HTTP) Spoofing
  - MITM – DHCP Spoofing

Source: http://michellgroup.com/

Extra on Proxy: Forward proxy vs reverse proxy

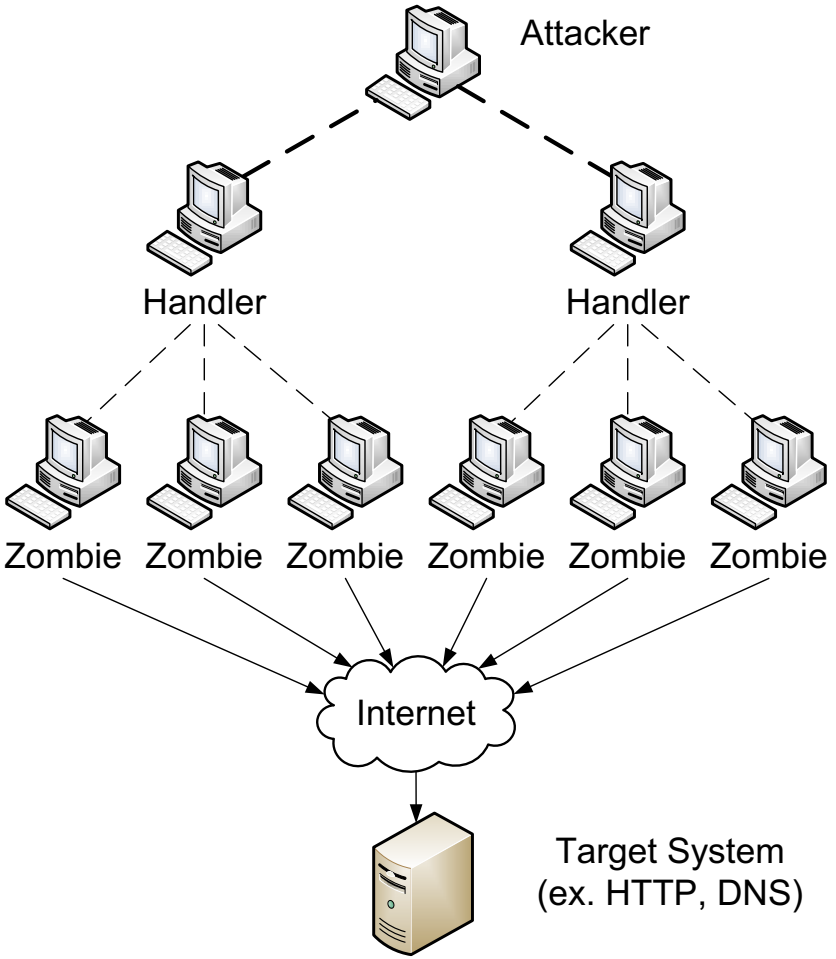




Source: http://www.celinio.net/

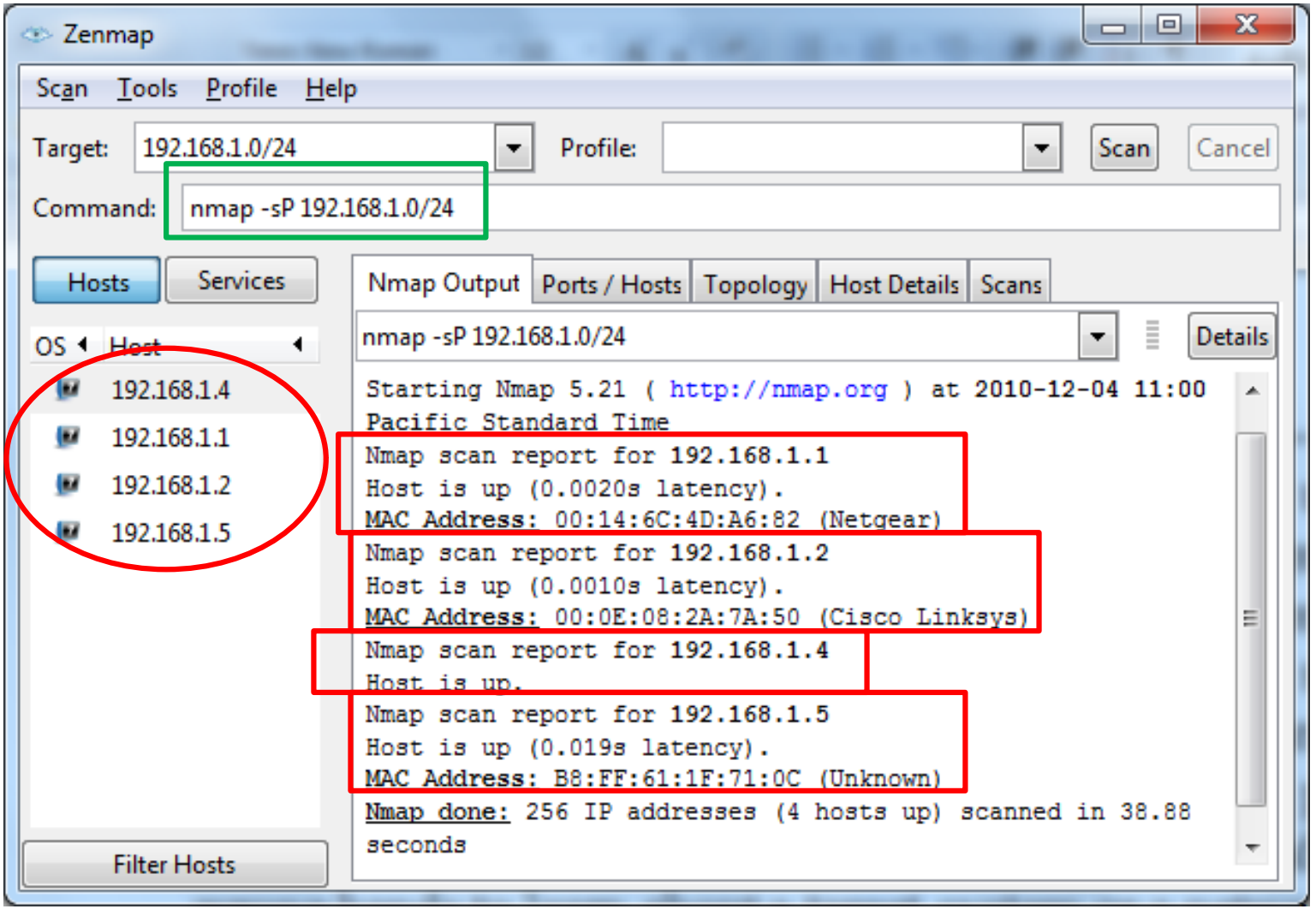
11.5 Denial Of Service

- ICMP-based Pinging
- *SYN* requests
- DDOS (Distributed DOS)
- MAC Address Flooding

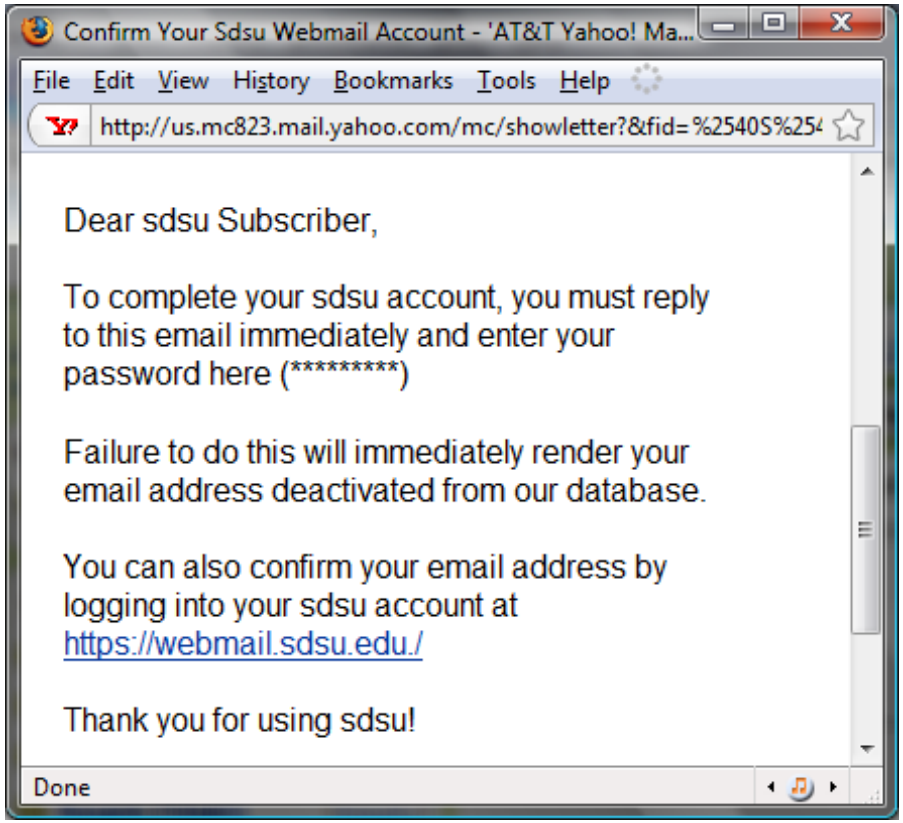


11.7 Port Scanning

Port Scanning with Zenmap



11.8 Social Engineering



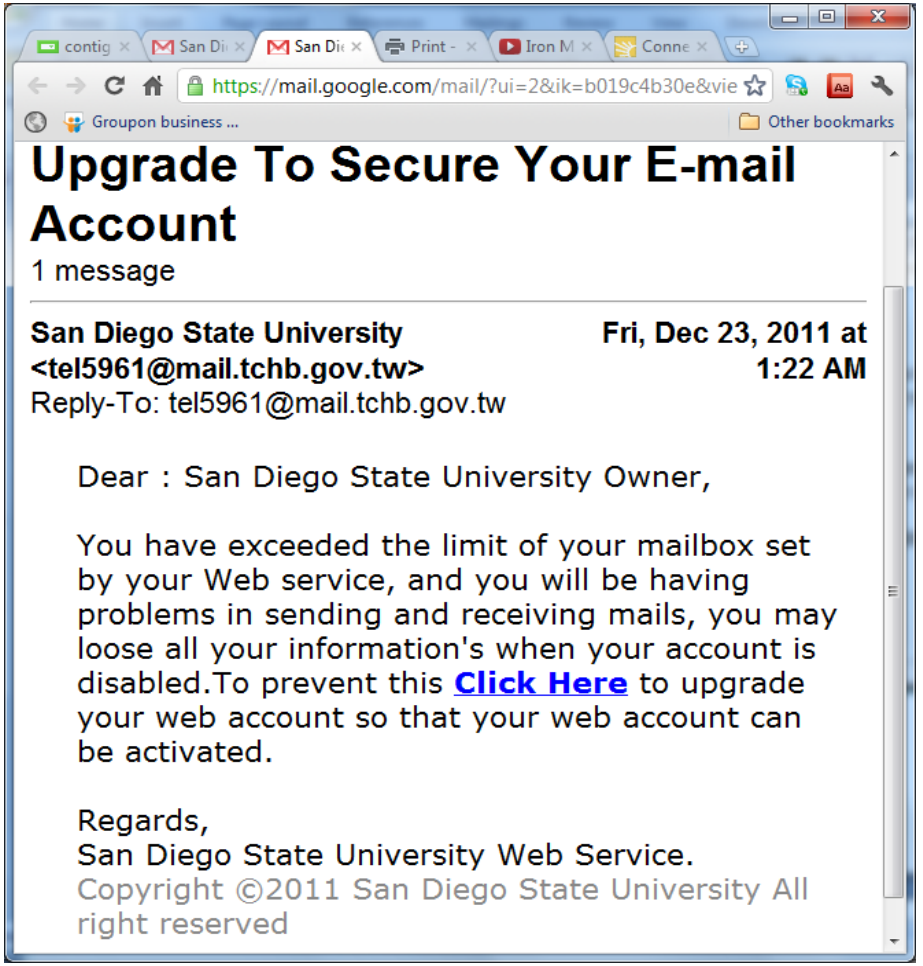


Figure 11.4 Sample phishing emails

11.9 Man-in-the-middle (MITM)

Definition: An attacker intercepts packets and relay (or substitute) them as a middle man.

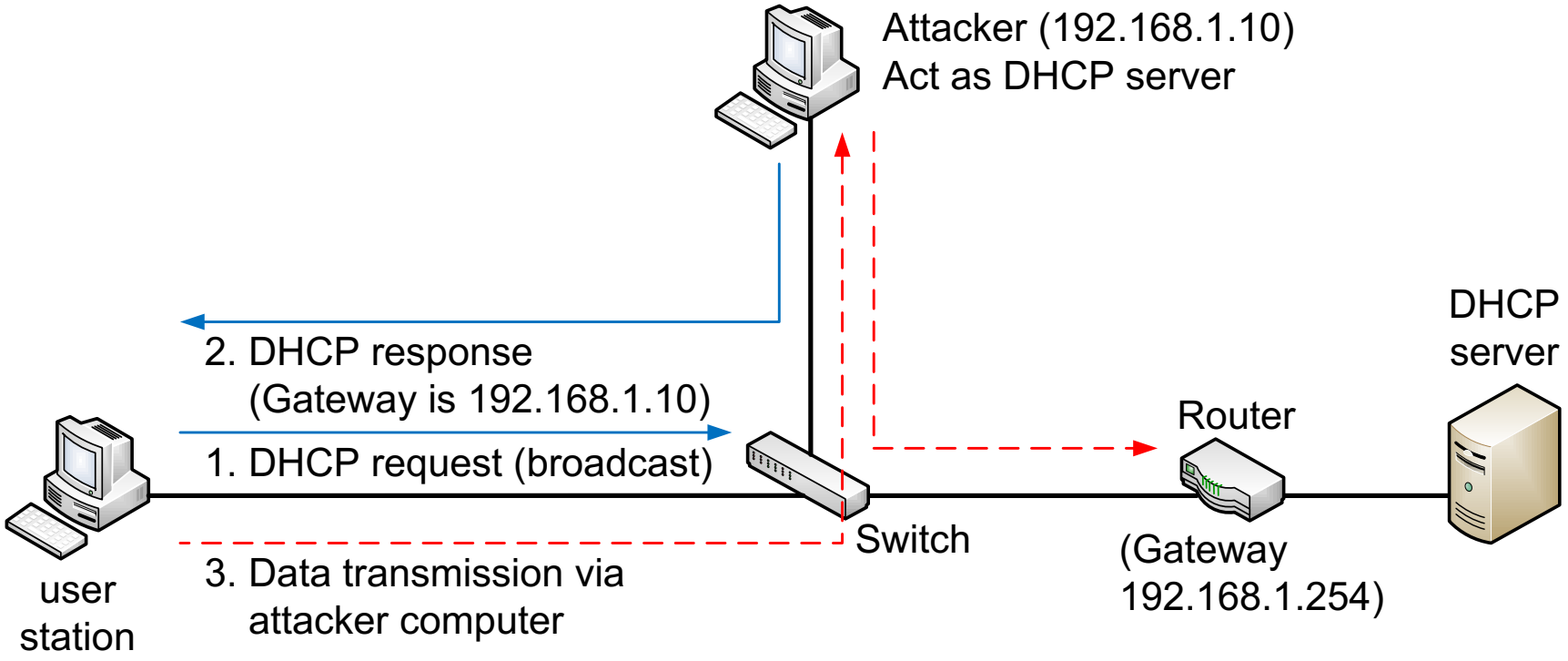


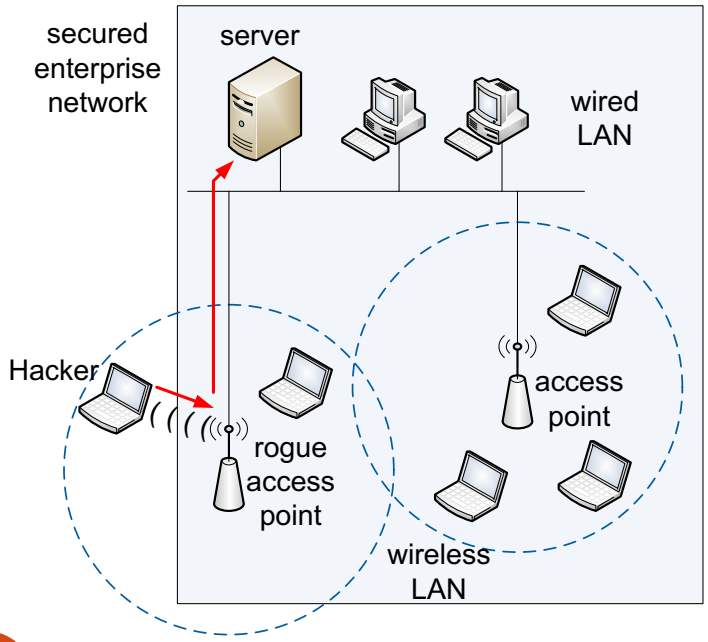
Figure 11.5 DHCP Spoofing and MITM

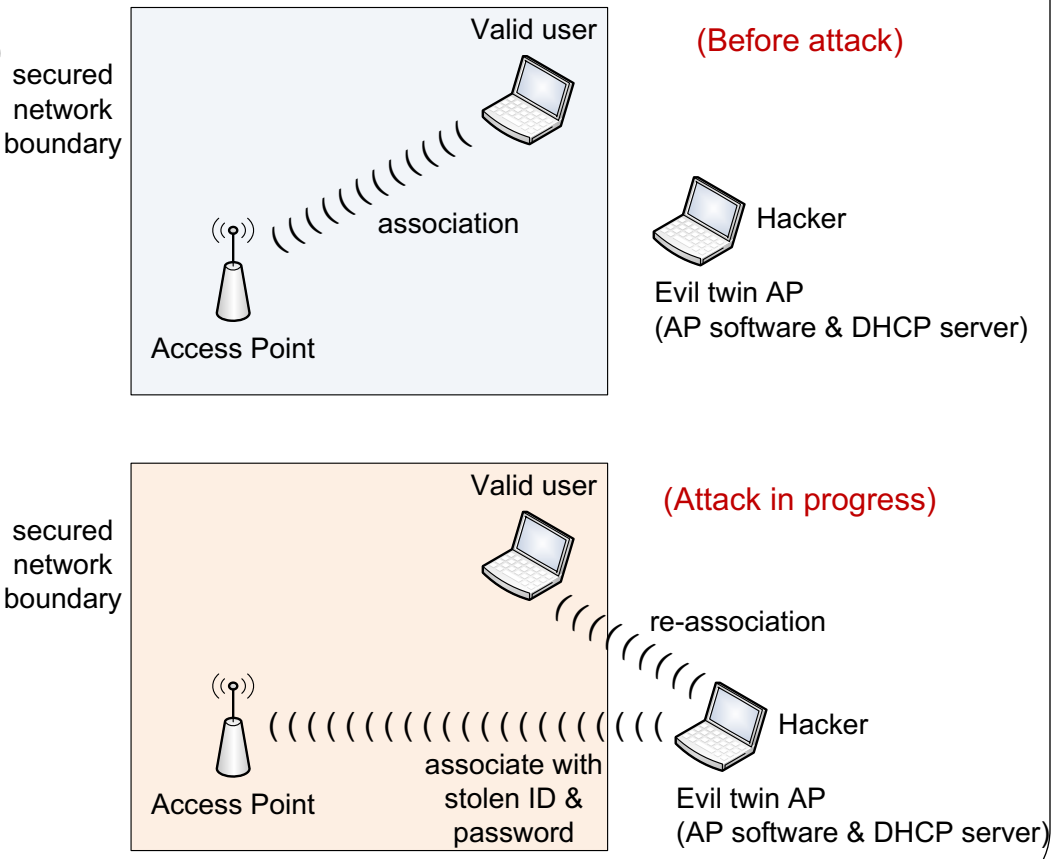
11.11 Zero-Day Attack

- Software programs including OS have vulnerabilities
- Vendors are simply unaware of their existence.
- Some are found after years.
- It is an act of exploiting such software flaws.

11.12 WiFi Threats

- Wardriving
- Denial of service
- Rogue wireless access point
- Man-in-the-middle (MITM)





Recap

- Malware: virus, worm, Trojan, & bot
- Password cracking
- Spoofing
- Denial of service
- Packet sniffing
- Port scanning
- Social engineering
- Man-in-the-middle (MITM)
- Zero-day attack
- WiFi threats

End
Chapter 11

CECS 303 Networks and Networks Security

Network Security: Defenses
Chapter 12

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

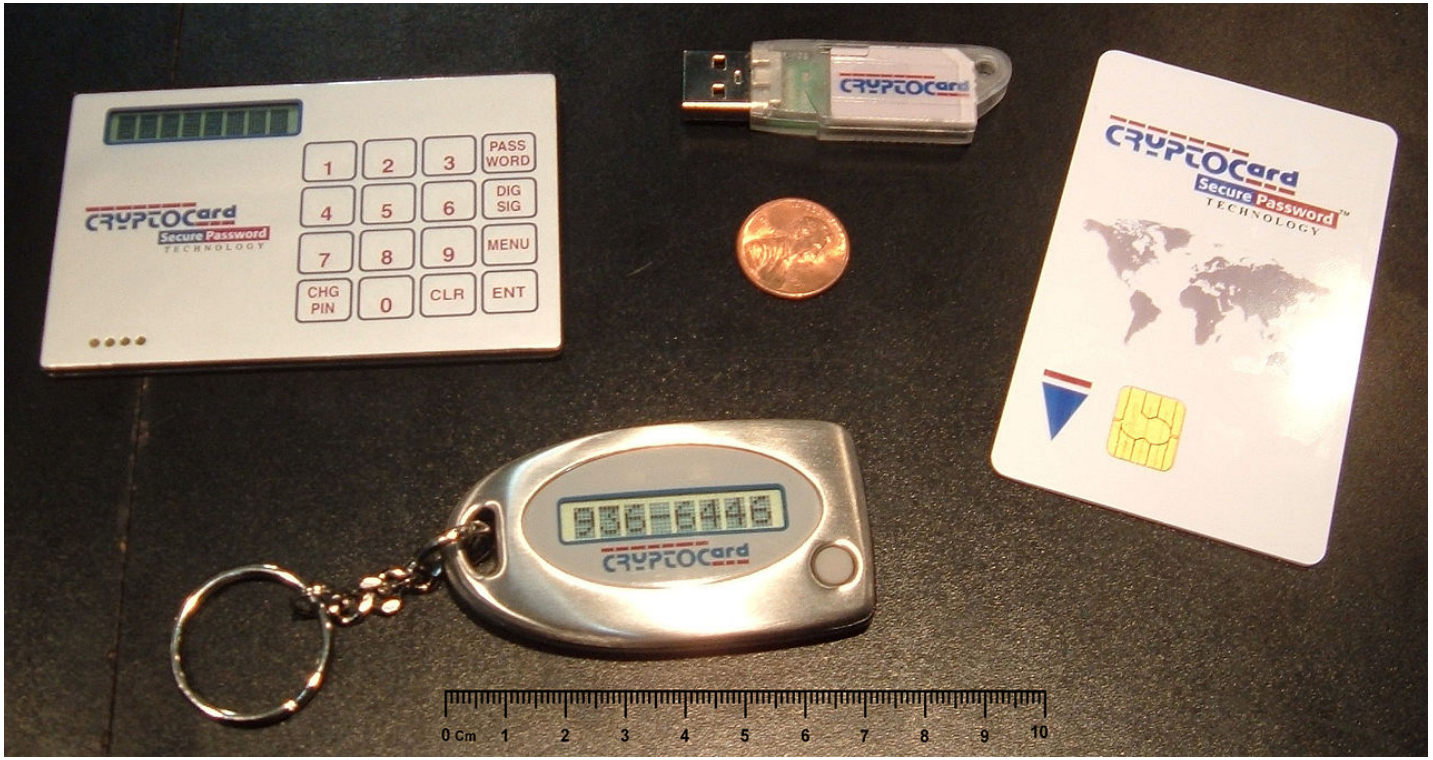
12.2 Defense Requirements and Solutions

Security requirements	Popular Technologies
Message confidentiality	• Cryptography
Message integrity	• Checksum/frame check sequence (FCS) • Digital signature
Access control/ Authorization	• Access Control List (ACL) • Firewall • Anti-virus and anti-spyware • Intrusion detection and prevention • Directory service
Authentication	• Password and passphrase • Digital signature and digital certificate • Biometric solutions (e.g., face recognition). • Security token

Table 12.1 Security requirements and technology solutions

Security Tokens for Authentication

Source: http://en.wikipedia.org/



For one time password (OTP)

12.3.1 Firewall and DMZ

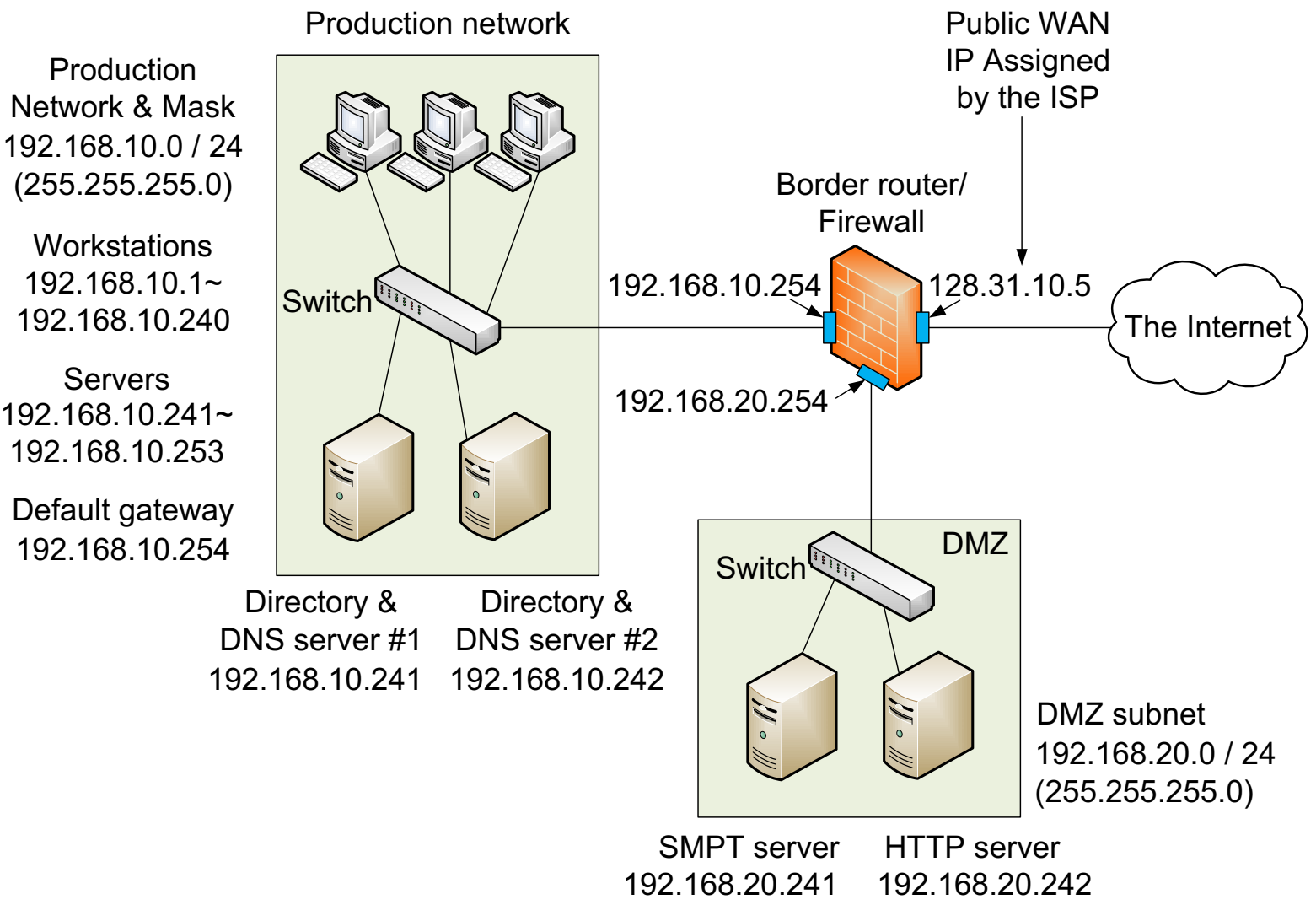


Figure 12.1 Border router firewall and DMZ

12.3.1 Firewall and DMZ

- A corporate network is large and needs a dedicated firewall.
- A firewall may not support the connectivity (e.g., serial port) or a protocol for external packet routing.

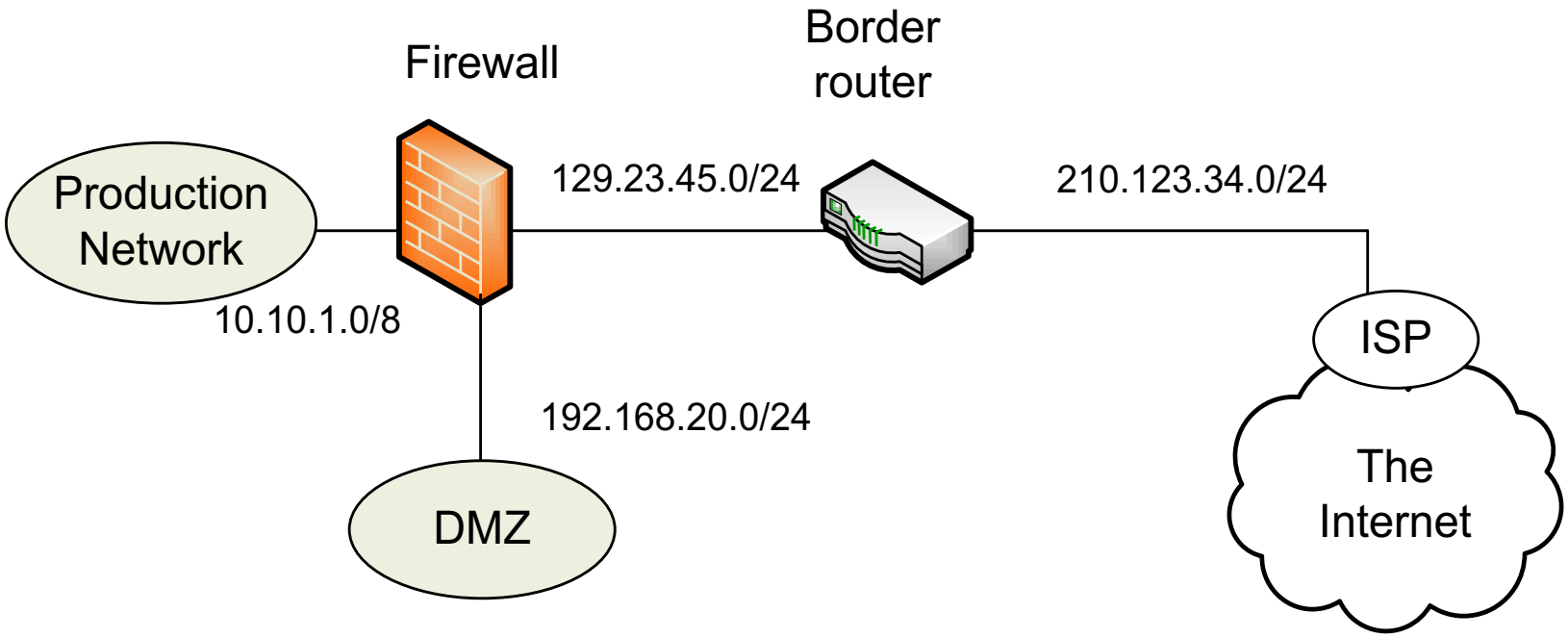
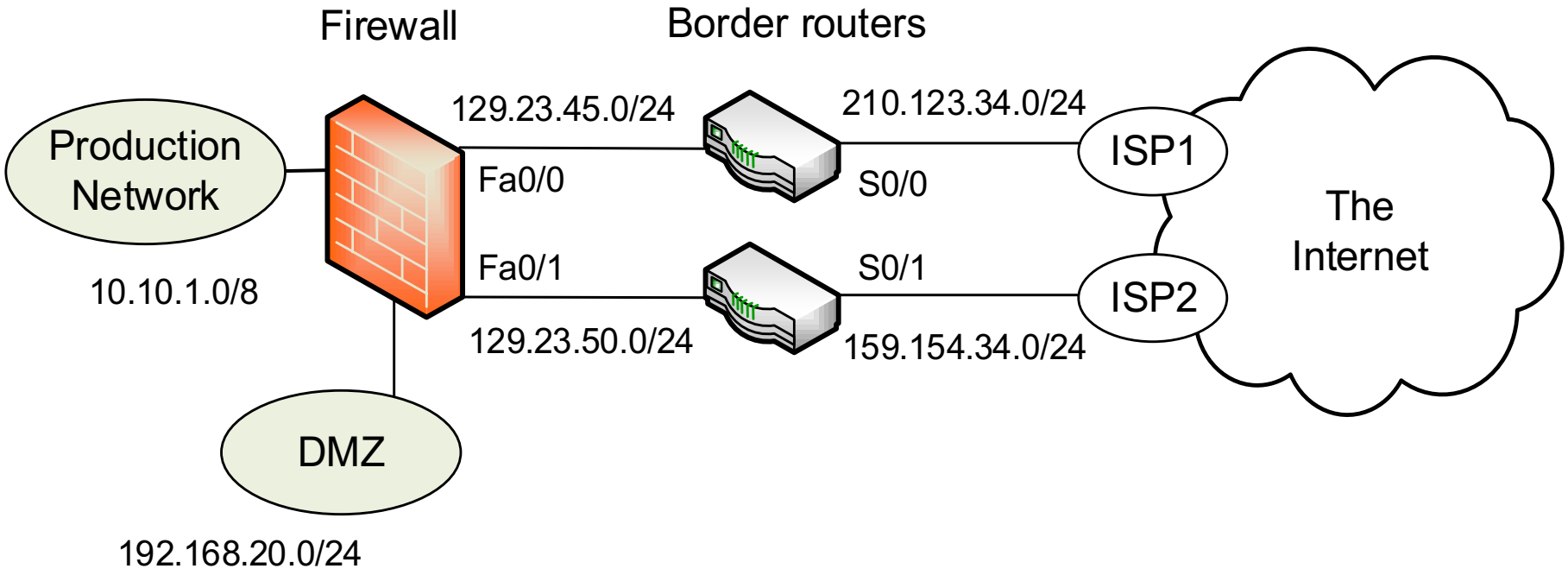


Figure 12.2 Separating firewall and border router

12.3.1 Firewall and DMZ



Another Scenario: Separating firewall and border routers

12.3.2 Firewall Functions & Management

Select key functions

- Packet inspections to examine IP, TCP, UDP, and ICMP PDUs – intrusion prevention
- Inspection of application layer PDUs for email and web content filtering, URL filtering, anti-virus and anti-spyware enabled filtering – intrusion prevention
- Intrusion detection to uncover potential or on-going attacks (e.g., denial-of-service).
- Network address translation (NAT) to hide internal IP addresses
- VPN gateway that provides secure tunnelling for remote connections over the Internet

12.3.2 Firewall Functions & Management

Managing Firewall

- Corporate security policy and any other regulations
- Synchronize packet filtering rules with business requirements
- Conduct security audit on a regular basis
- Conform to general principles of security management

  (ex) OS security patches, TCP/UDP ports
- Separate filtering rules for ingress and egress traffic
- Egress filtering:
  - Protect internal resources and data from theft
  - Stop viruses and worms from spreading to outside.
  - Guard internal systems from being appropriated (ex. DDOS attack) by Trojans.

12.3.3 Stateless vs. stateful filtering

Stateless Filtering

- If TCP destination port = 21 (FTP connection attempt), then drop.
- If destination IP = 161.154.23.59 and TCP port = 80 (Web server connection), then pass
- If destination IP = 161.154.23.59 and TCP port = 25 (Email server connection), then pass

Stateful Filtering

- If a packet's source and destination sockets are in the state table, *pass*.
- If a packet's source and destination sockets are not in the state table and the packet is not a connection-opening attempt, *drop*.

12.4 Access Control List

- Built into routers: ACL-based filtering primarily relies on
  - Source and destination IP addresses
  - Source and destination TCP/UDP ports
  - Protocol of a packet (e.g., IP, ICMP)
  - ICMP message types (e.g., pinging, traceroute)

- How many ACLs? : (e.g.,) two ports (S0/0/0 and Fa0/1)
  A. ACLs for Interface S0/0/0
     1. ACL for Inbound traffic; 2. ACL for Outbound traffic
  B. ACLs for Interface Fa0/1
     3. ACL for Inbound traffic; 4. ACL for Outbound traffic

12.5 Cryptography

12.5.1 A cryptography system

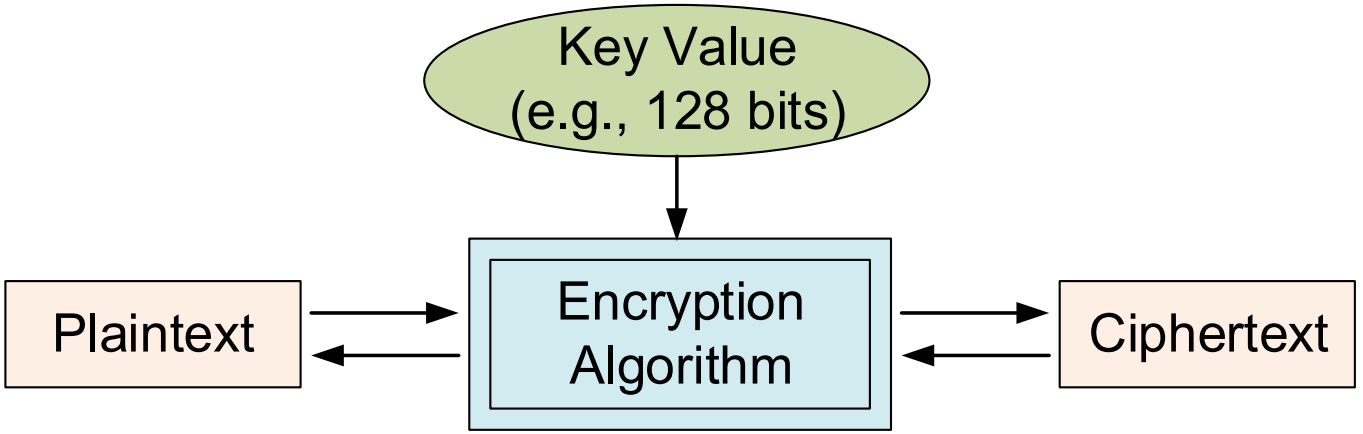


Figure 12.4 Components of cryptography

12.5 Cryptography

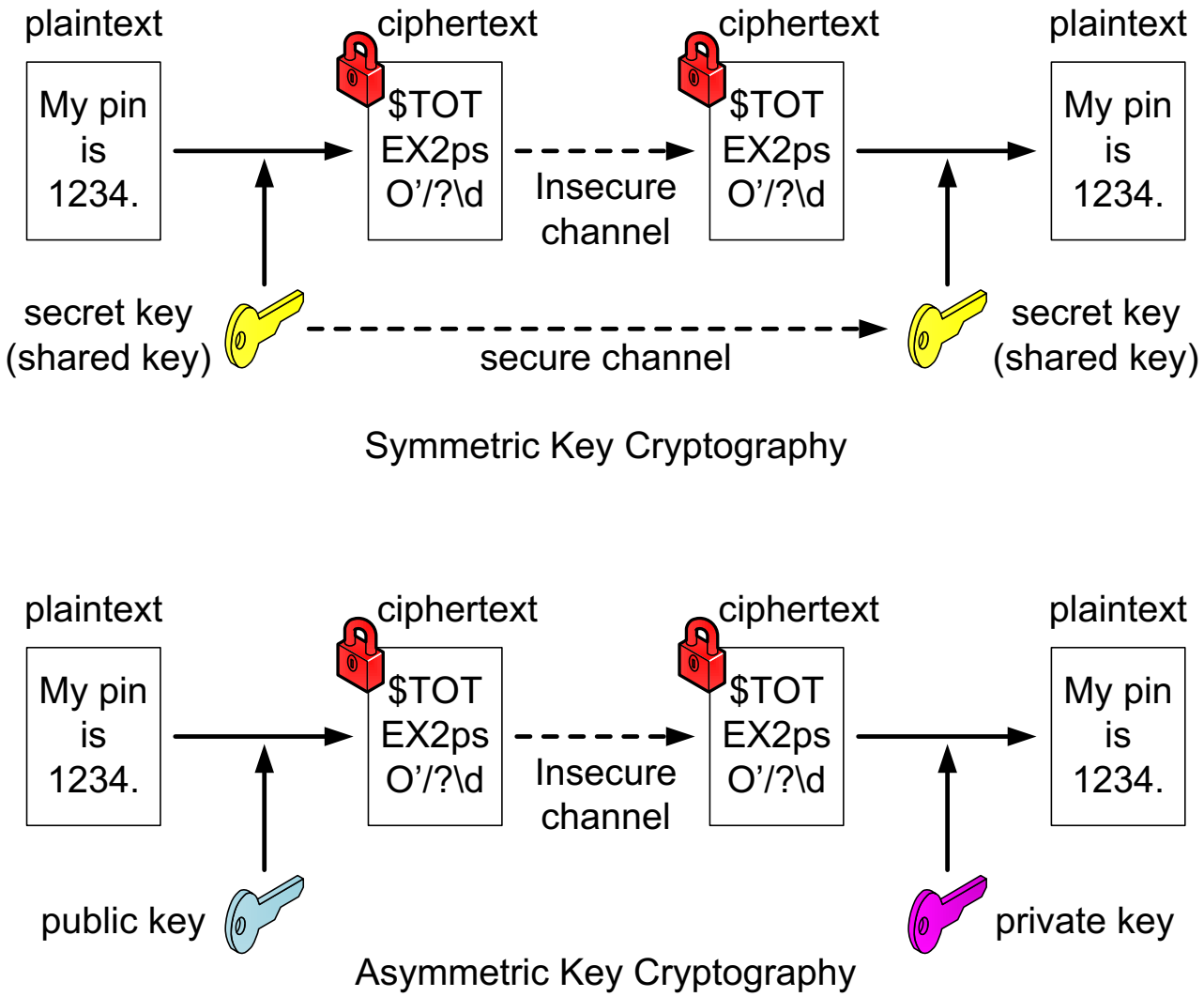


Figure 12.5 Symmetric-key vs. asymmetric-key cryptography

12.5 Cryptography

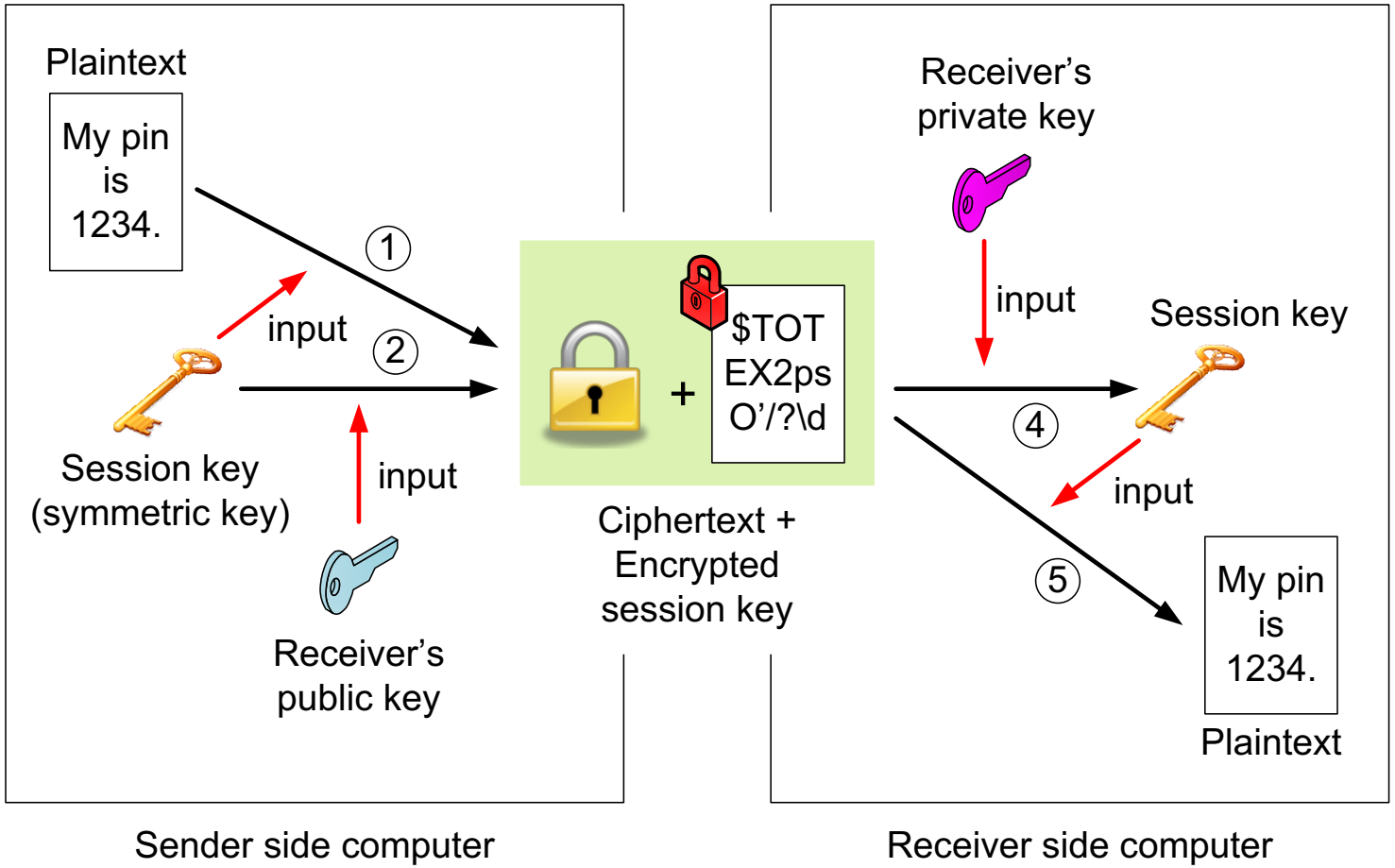


Figure 12.6 Hybrid usage of symmetric and asymmetric cryptography

12.6 Digital Signature

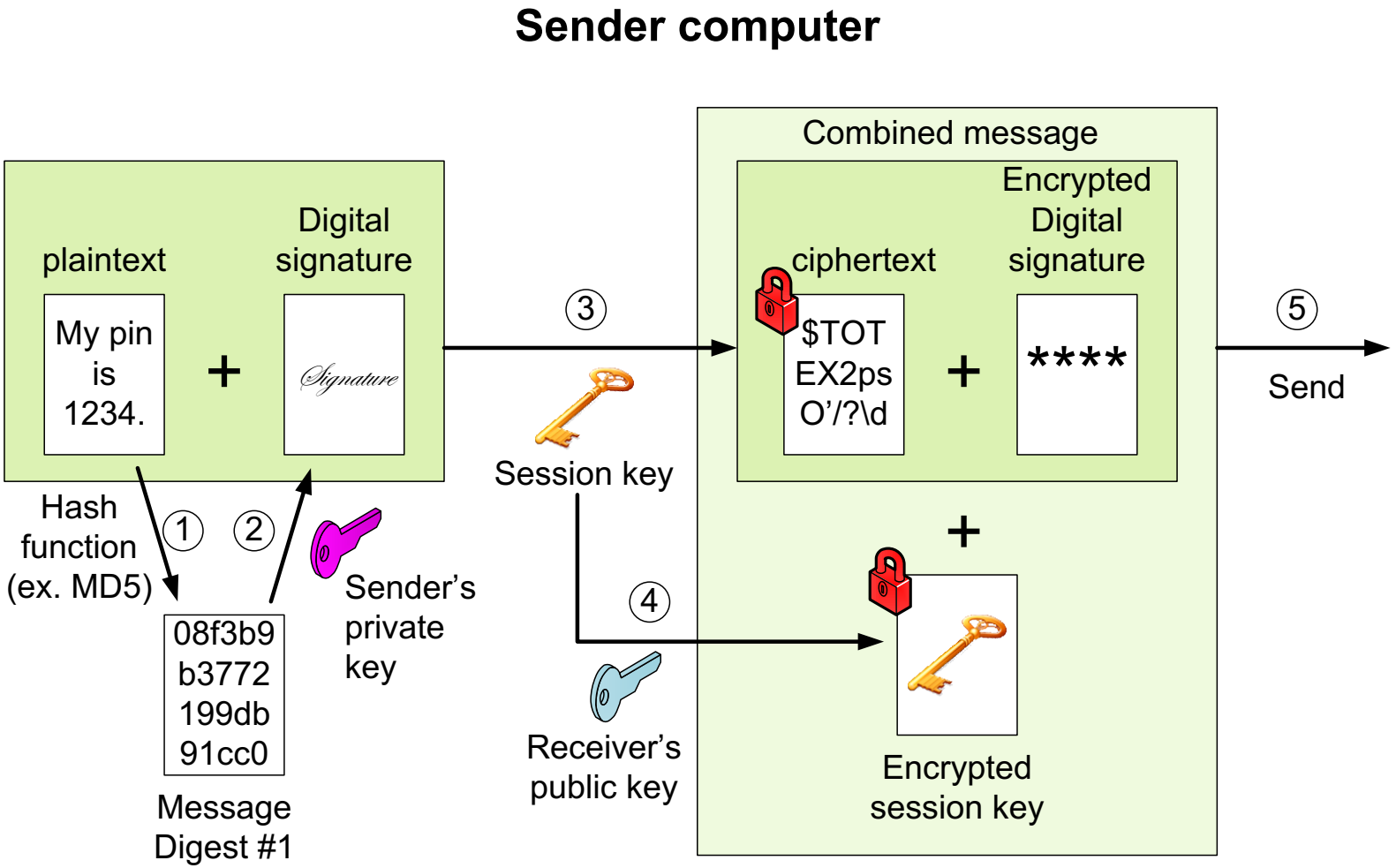


Figure 12.7 Usage of a digital signature

12.6 Digital Signatures

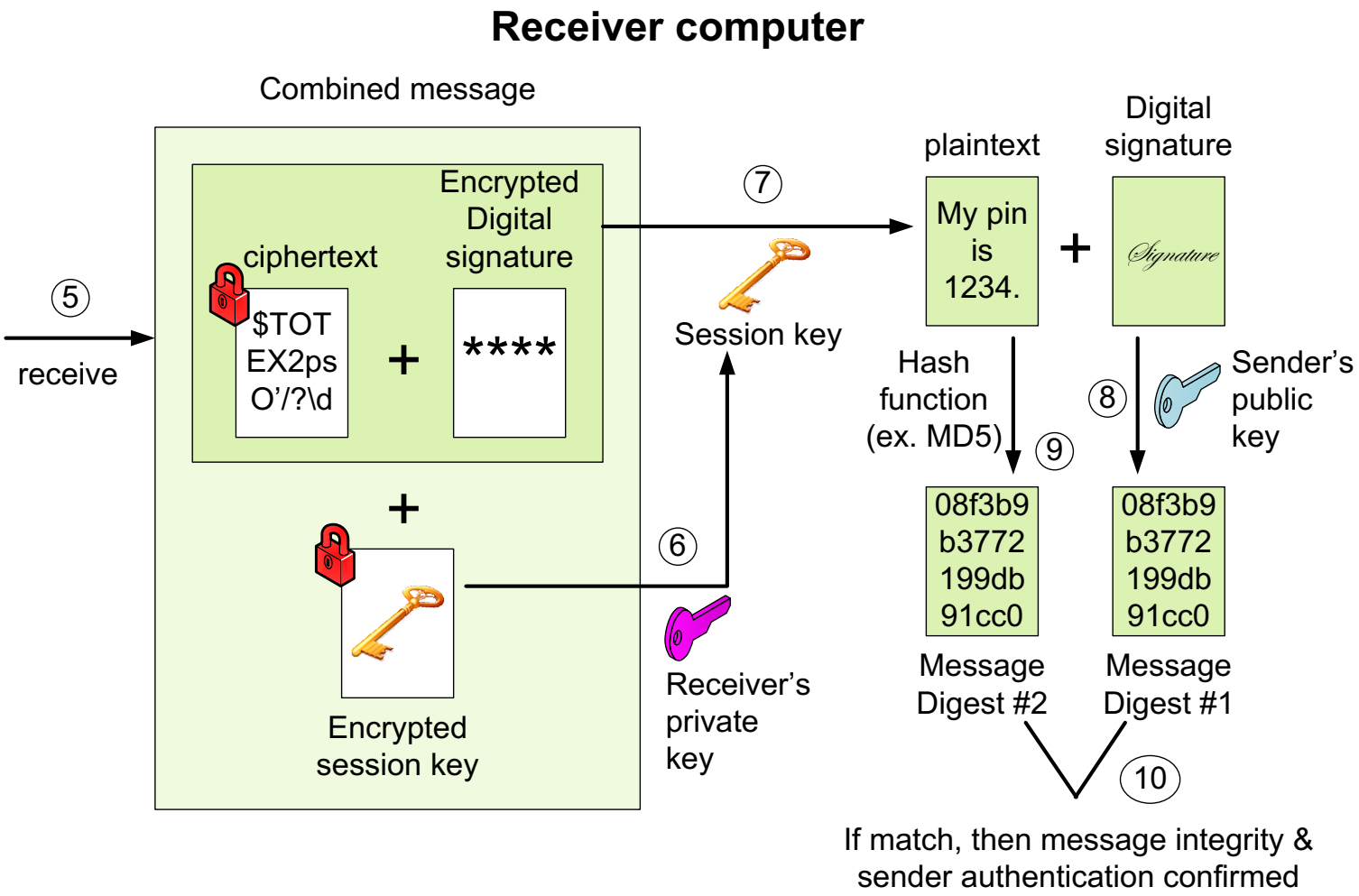


Figure 12.7 Usage of a digital signature

12.7 Digital Certificates

Version: 3
Serial number: 123456
Algorithm: RSA
Issuer name: VeriSign
Validity period: start / expiration dates
Subject name: John Doe
Subject public key: XXXXXXXXXXX
CA digital signature: XXXXXXXX

- certificate authorities (CAs)
- PKI (public key infrastructure)
- X.509 ITU standard

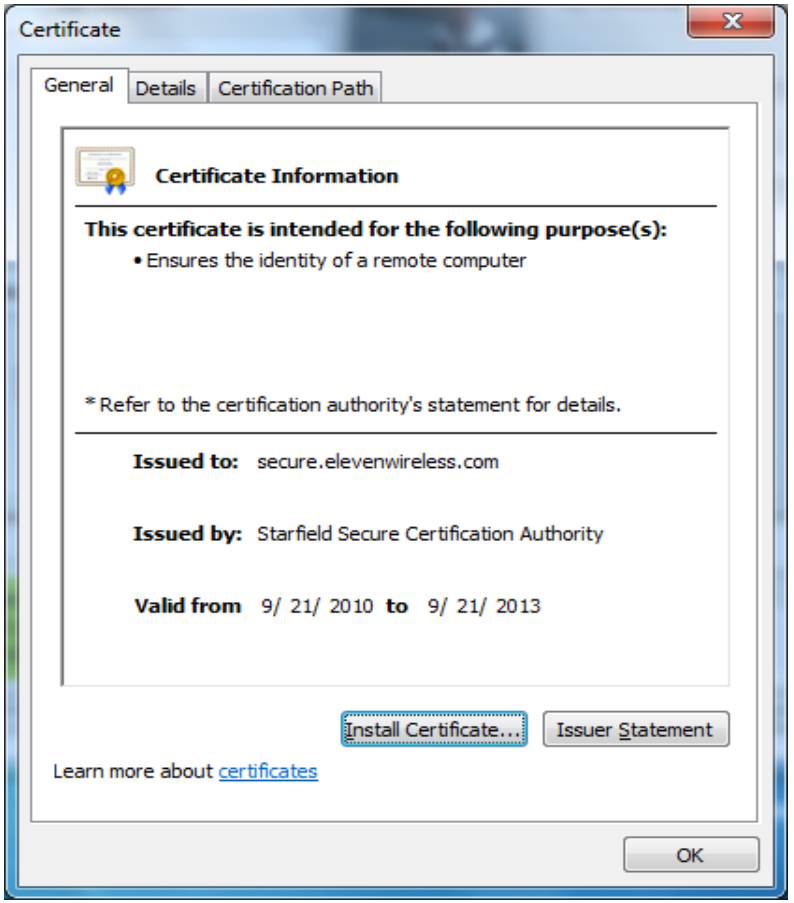


Figure 12.8 Information items of X.509 and its simplified view (Chrome)

12.7 Digital Certificates

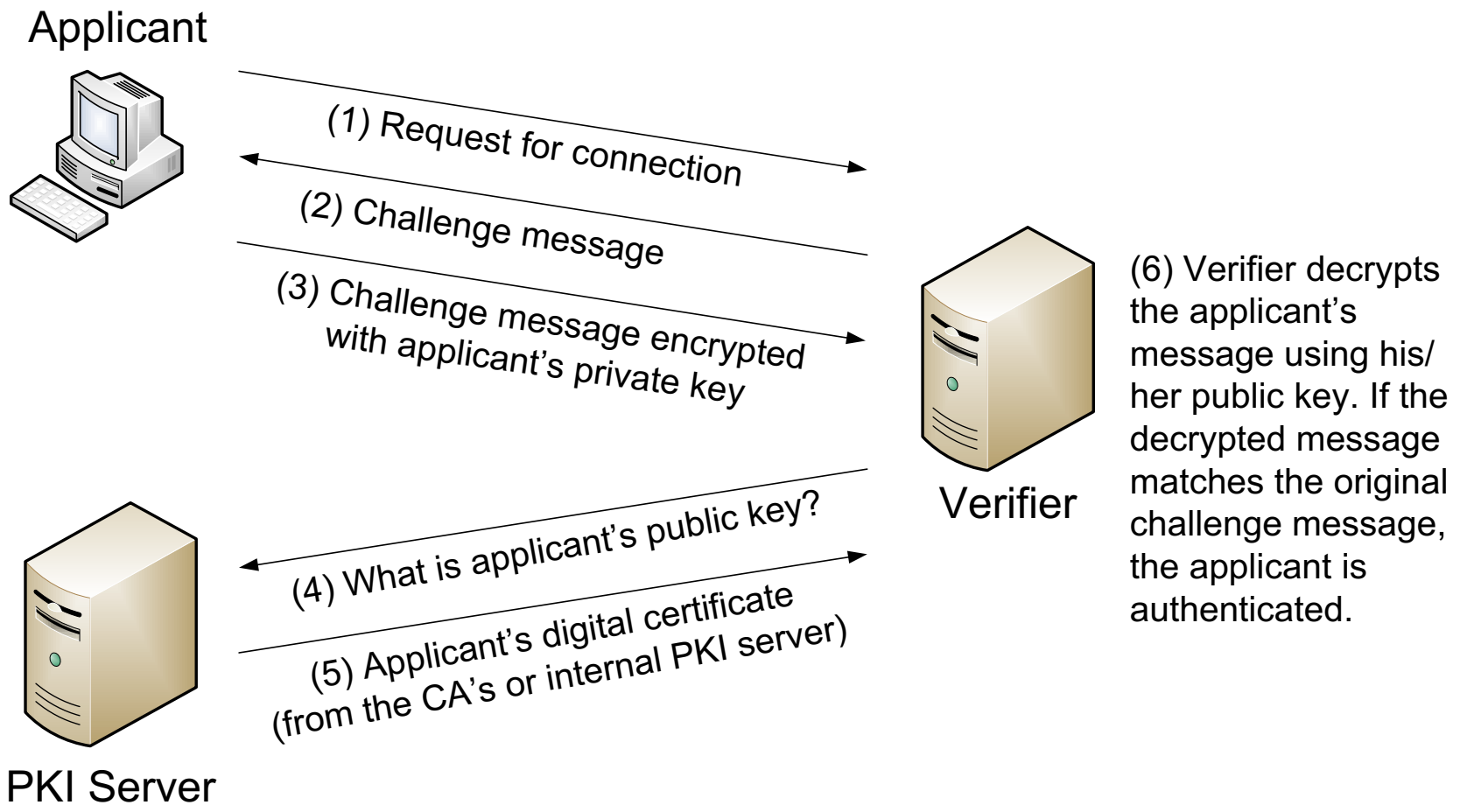


Figure 12.9 Scenario: digital certificate-based authentication

12.7 Digital Certificates

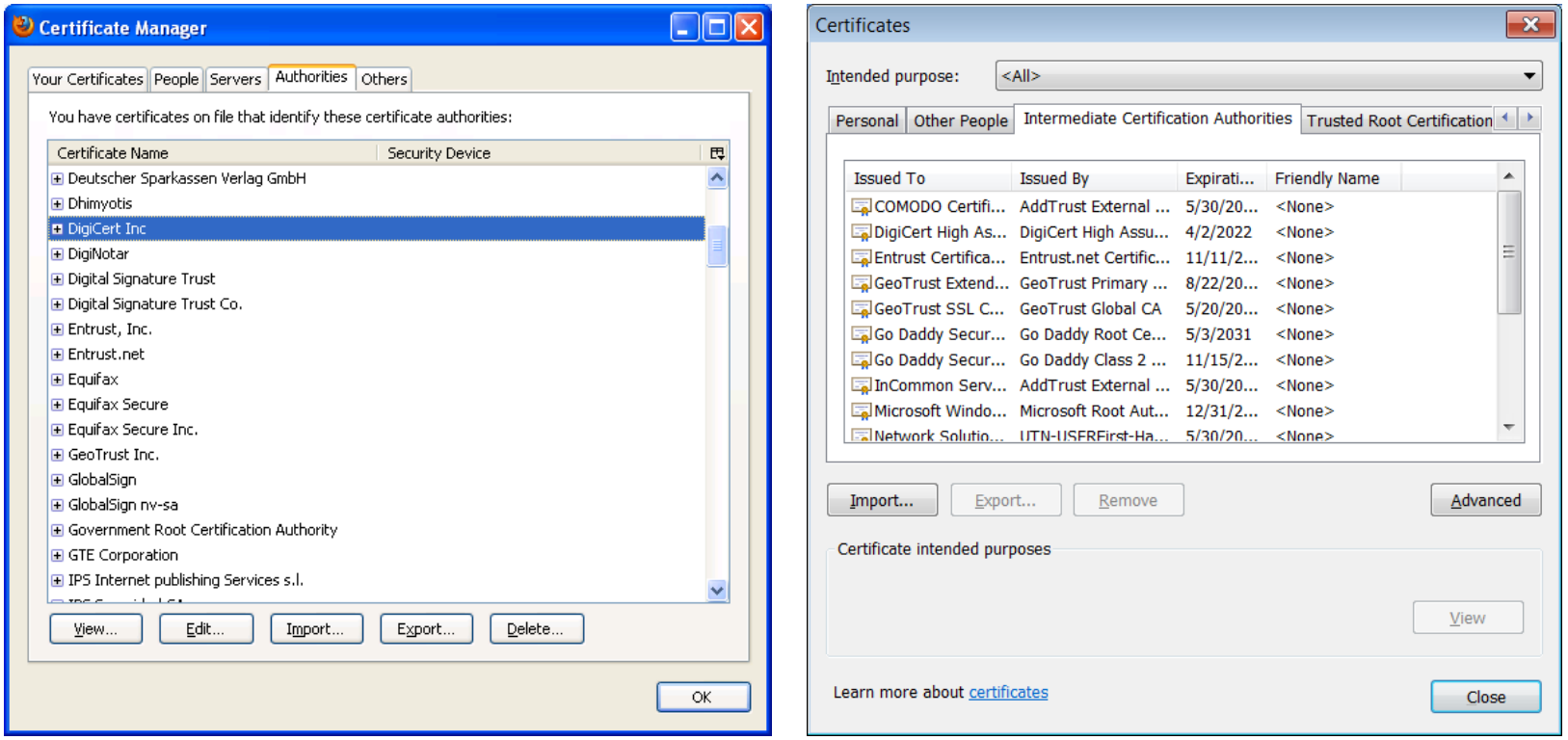
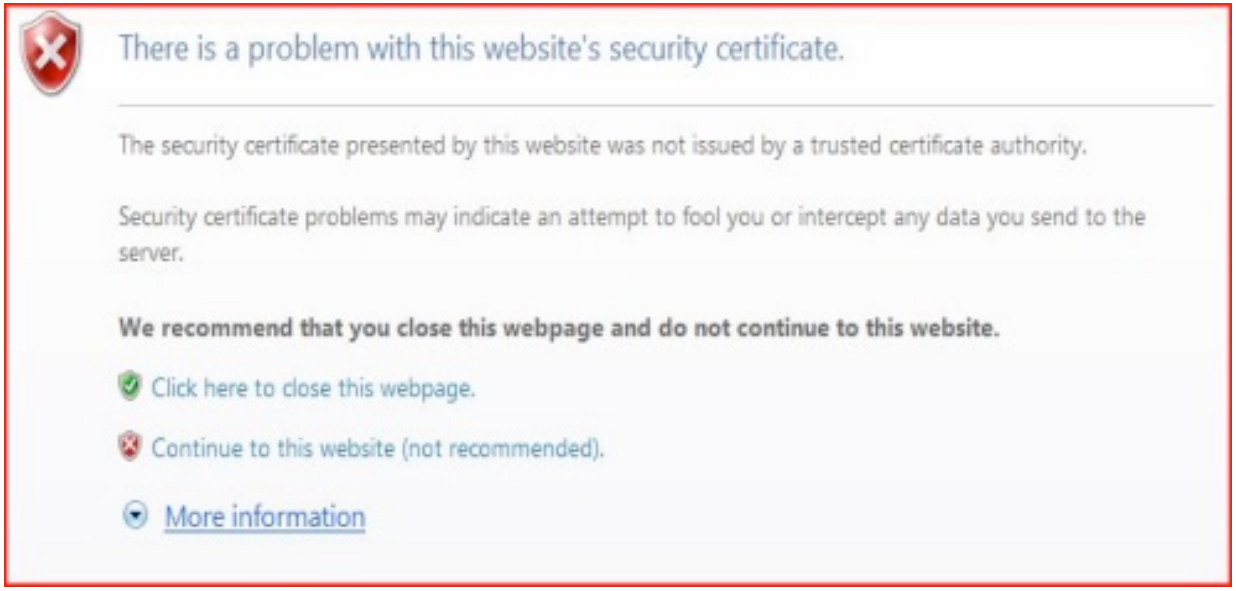
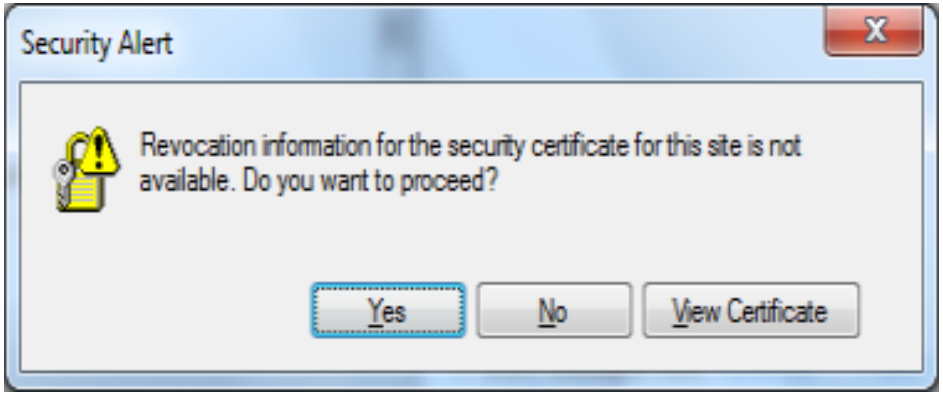


Figure 12.10 Trusted CAs: Firefox (left) and Chrome browsers

Figure 12.11 Sample warnings associated with digital certificates



(a) Warning for a digital certificate (Internet Explorer)



(b) Warning for inaccessibility of certificate revocation list (Google Chrome)

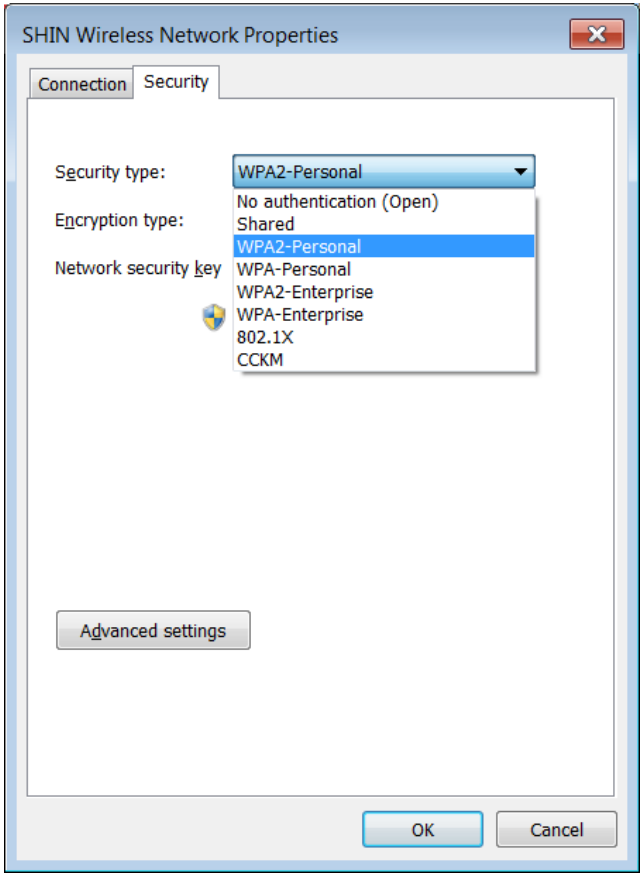
12.8 Security Protocols

- Application layer: S/MIME, PGP (Pretty Good Privacy)
- Transport layer: SSL/TLS
- Internet layer: IPSec
- Data link layer: WPA, WPA2

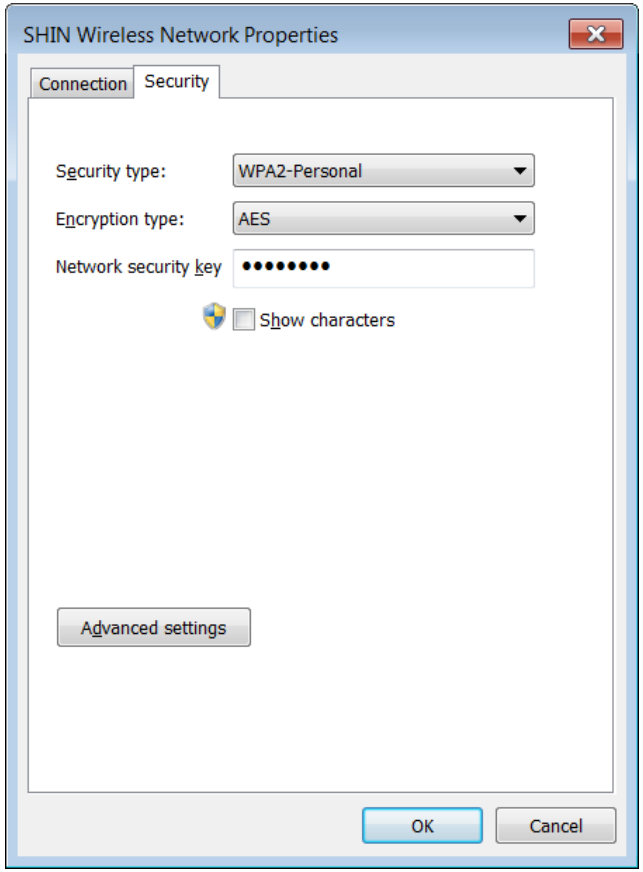
12.8.1 WLAN Security Standards

- Types
  - Wired Equivalent Privacy (WEP)
  - Wi-Fi Protected Access (WPA)
  - IEEE 802.11i (also called WPA2) : For "robust security network"
- Personal mode (Pre-shared Key or PSK Mode)
  - For homes and small offices
  - Supports *WPA-Personal* and *WPA2-Personal*
  - APs responsible for user authentication and key management.
- Enterprise mode
  - To offer WiFi security for an enterprise
  - Supports *WPA enterprise* and *WPA2 enterprise*
  - Uses a *central server* for authentication and key management

12.8.1 WLAN Security Standards



(a) Security standards



(b) Network key (i.e., password)

Figure 12.12 WiFi security standards (Windows)

Recap

- Defense requirements and solutions
- Firewall and DMZ
- Firewall functions & management
- Firewall: stateful vs stateless
- Access control list
- Cryptography
- Digital signature
- Digital certificate
- Security protocols
- WLAN security standards

End
Chapter 12