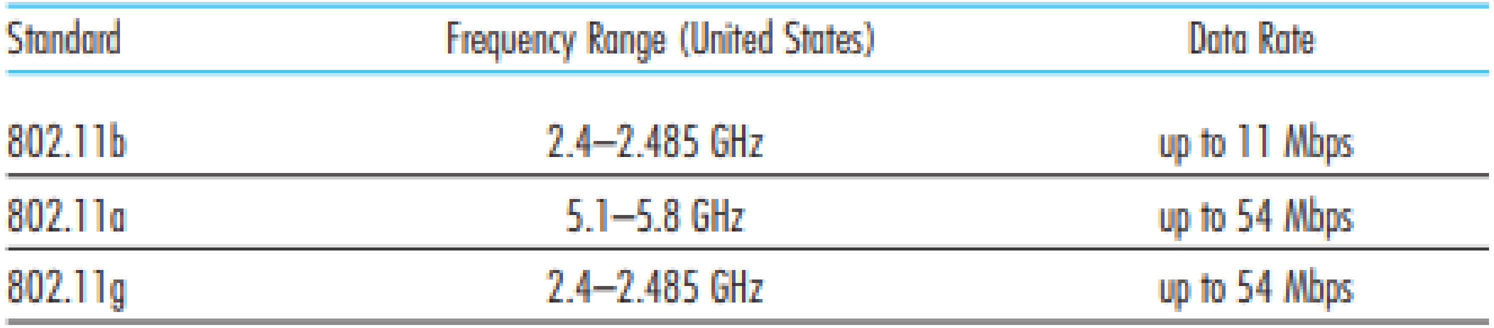
Module 5

WiFi: 802.11 Wireless LANs

WiFi: 802.11 Wireless LANs

- There are several 802.11 standards for wireless LAN technology, including 802.11b, 802.11a, and 802.11g.



Standard	Frequency Range (United States)	Data Rate
802.11b	2.4–2.485 GHz	up to 11 Mbps
802.11a	5.1–5.8 GHz	up to 54 Mbps
802.11g	2.4–2.485 GHz	up to 54 Mbps

Table 6.1 • Summary of IEEE 802.11 standards

James F Kurose and Keith W Ross, “Computer Networking: A Top - Down Approach”, Pearson Education; 6 th Edition (2017)

The 802.11 Architecture

- The fundamental building block of the 802.11 architecture is the basic service set (BSS).
- A BSS contains one or more wireless stations and a central base station, known as an access point (AP)
- Each 802.11 wireless station has a 6-byte MAC address that is stored in the firmware of the station’s adapter (that is, 802.11 network interface card).
- Each AP also has a MAC address for its wireless interface.

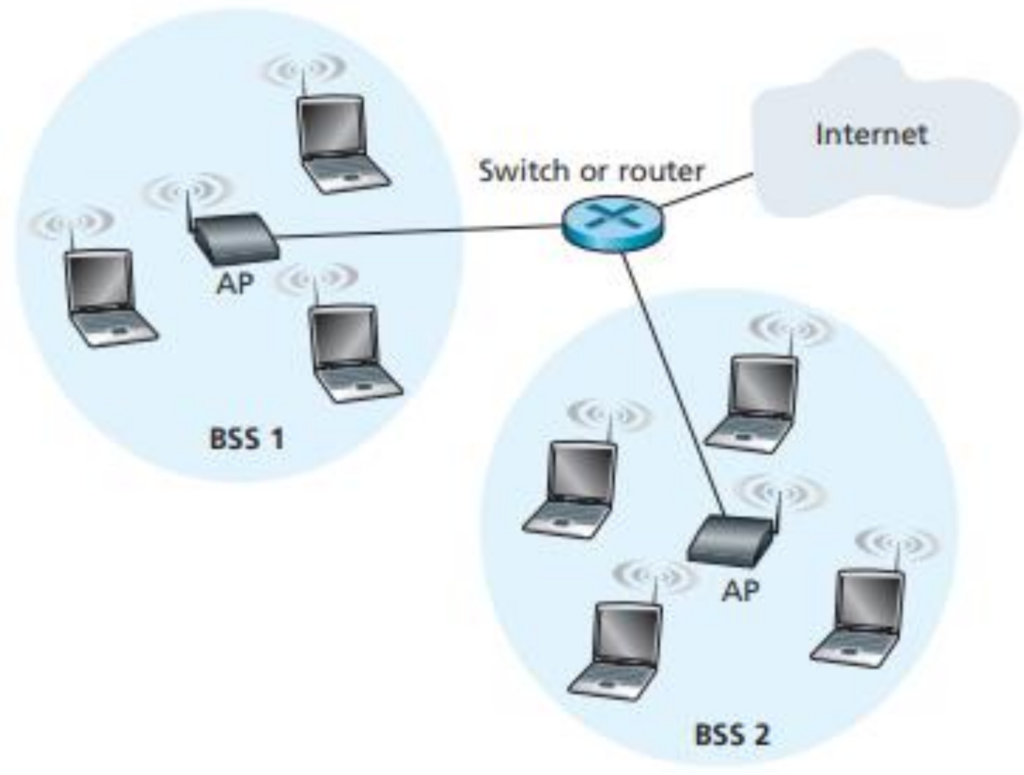


Figure 6.7 ♦ IEEE 802.11 LAN architecture

James F Kurose and Keith W Ross, “Computer Networking: A Top - Down Approach”, Pearson Education; 6 th Edition (2017)

The 802.11 Architecture

- IEEE 802.11 stations can also group themselves together to form an ad hoc network—a network with no central control and with no connections to the "outside world."

A BSS without an AP is called an ad hoc network;
a BSS with an AP is called an infrastructure network.

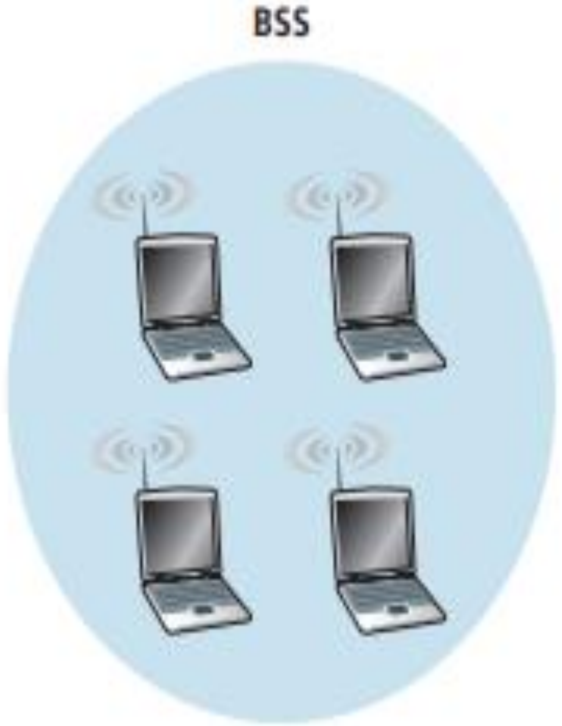
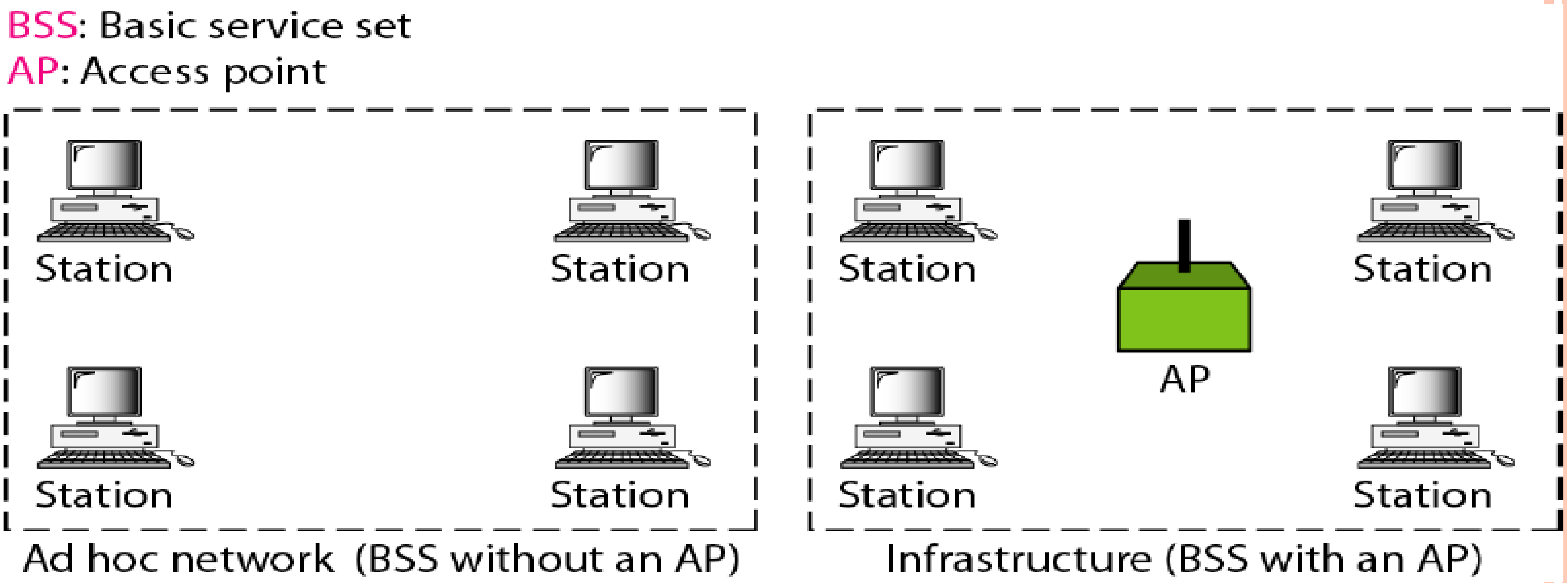


Figure 6.8 ♦ An IEEE 802.11 ad hoc network

James F Kurose and Keith W Ross, "Computer Networking: A Top - Down Approach", Pearson Education; 6 th Edition (2017)

The 802.11 Architecture

Basic service sets (BSSs)



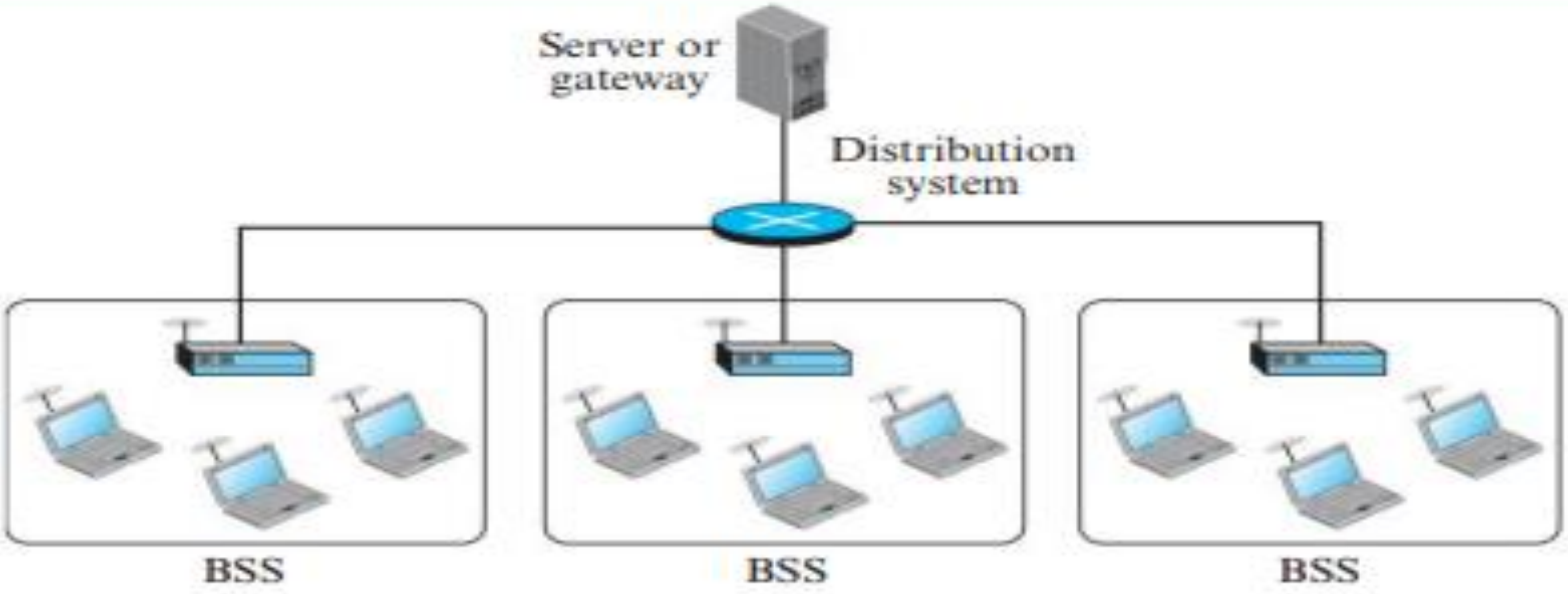
James F Kurose and Keith W Ross, “Computer Networking: A Top - Down Approach”, Pearson Education; 6 th Edition (2017)

The 802.11 Architecture

Extended Service Set

An extended service set (ESS) is made up of two or more BSSs with APs.

Figure 6.5 *Extended service set (ESS)*



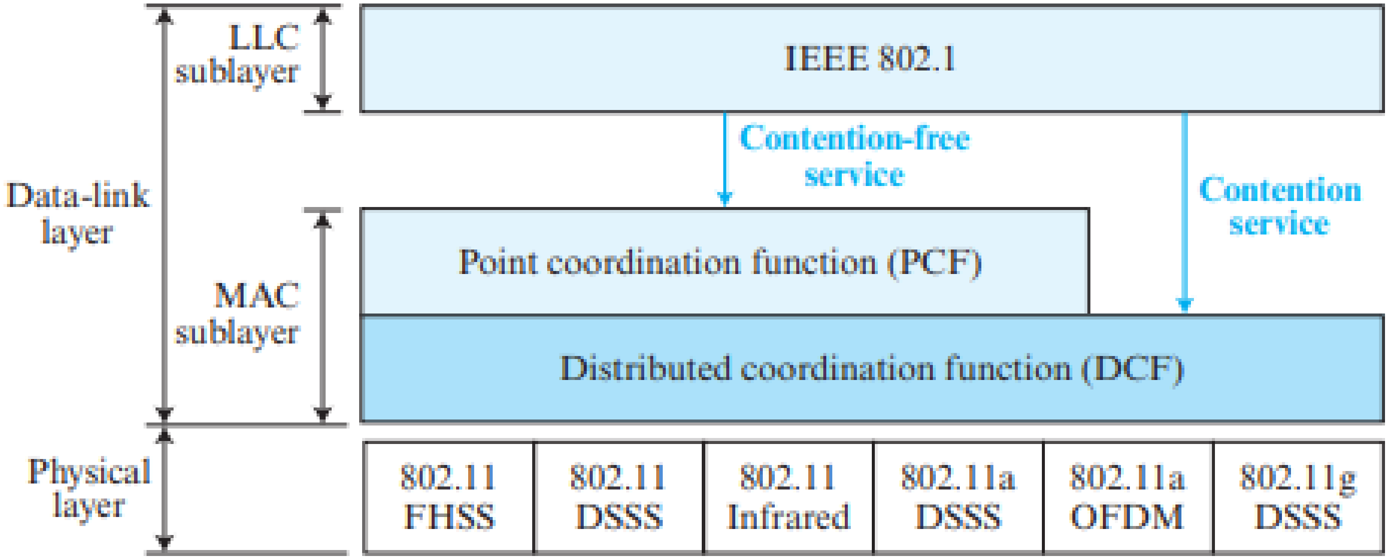
[Behrouz A Forouzan, Firouz Mosharraf, “Computer Networks: A top down Approach”, McGraw Hill Education]

The 802.11 Architecture

MAC Sublayer

IEEE 802.11 defines two MAC sublayers: the distributed coordination function (DCF) and point coordination function (PCF)

Figure 6.6 *MAC layers in IEEE 802.11 standard*



[Behrouz A Forouzan, Firouz Mosharraf, "Computer Networks: A top down Approach", McGraw Hill Education]

The 802.11 Architecture

MAC Sublayer

- Distributed Coordination Function: One of the two protocols defined by IEEE at the MAC sublayer is called the distributed coordination function (DCF). DCF uses CSMA/CA as the access method.
- Point Coordination Function (PCF): The point coordination function (PCF) is an optional access method that can be implemented in an infrastructure network (not in an ad hoc network). It is implemented on top of the DCF and is used mostly for time-sensitive transmission

The 802.11 Architecture

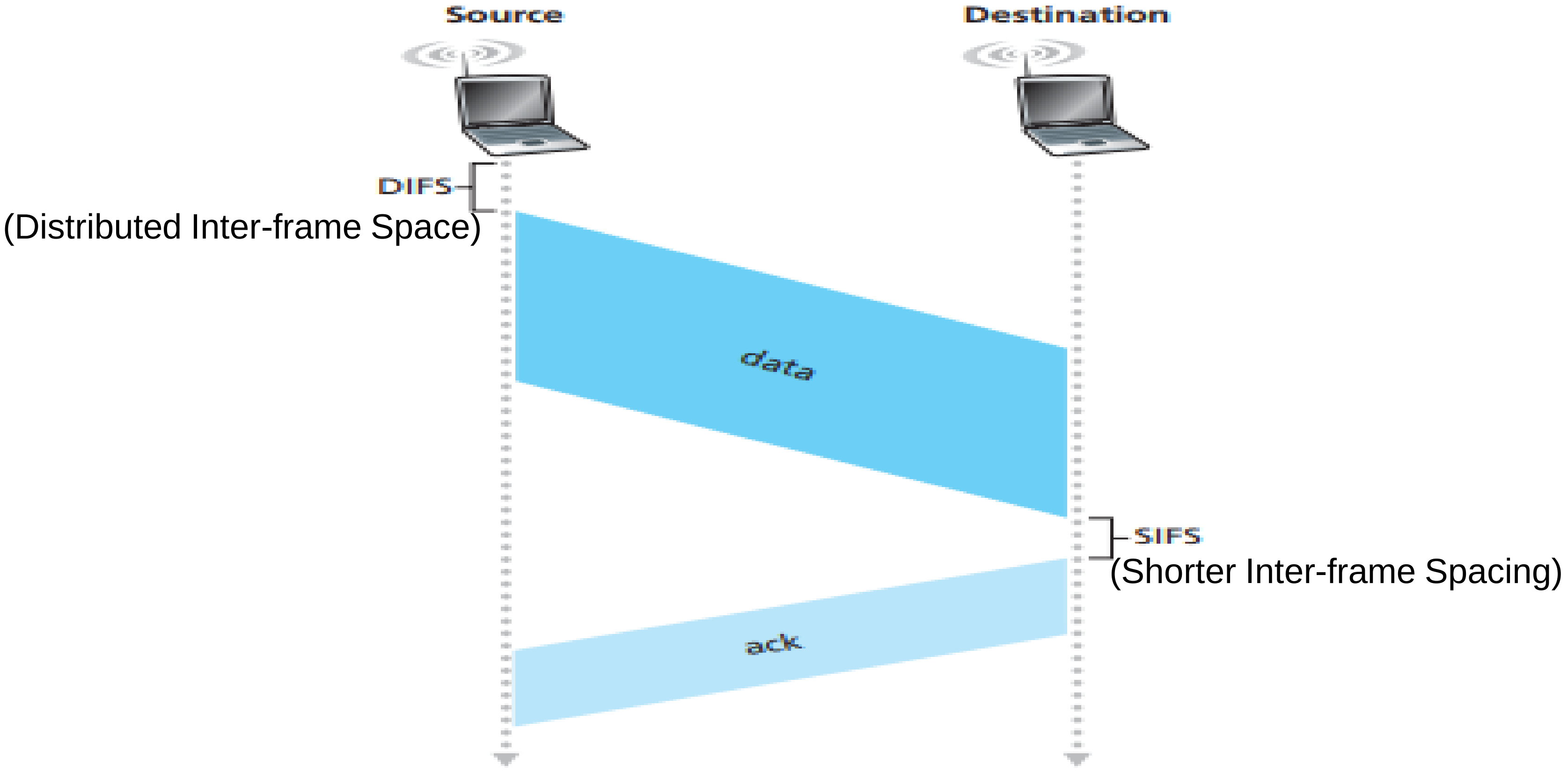

Source
Destination
DIFS
(Distributed Inter-frame Space)
data
SIFS
(Shorter Inter-frame Spacing)
ack

Figure 6.10 ♦ 802.11 uses link-layer acknowledgments

James F Kurose and Keith W Ross, “Computer Networking: A Top - Down Approach”, Pearson Education; 6 th Edition (2017)

- If the transmitting station does not receive an acknowledgment within a given amount of time, it assumes that an error has occurred and retransmits the frame, using the CSMA/CA protocol to access the channel.

The 802.11 Architecture

- IEEE 802.11 protocol allows a station to use a short Request to Send (RTS) control frame and a short Clear to Send (CTS) control frame to reserve access to the channel.

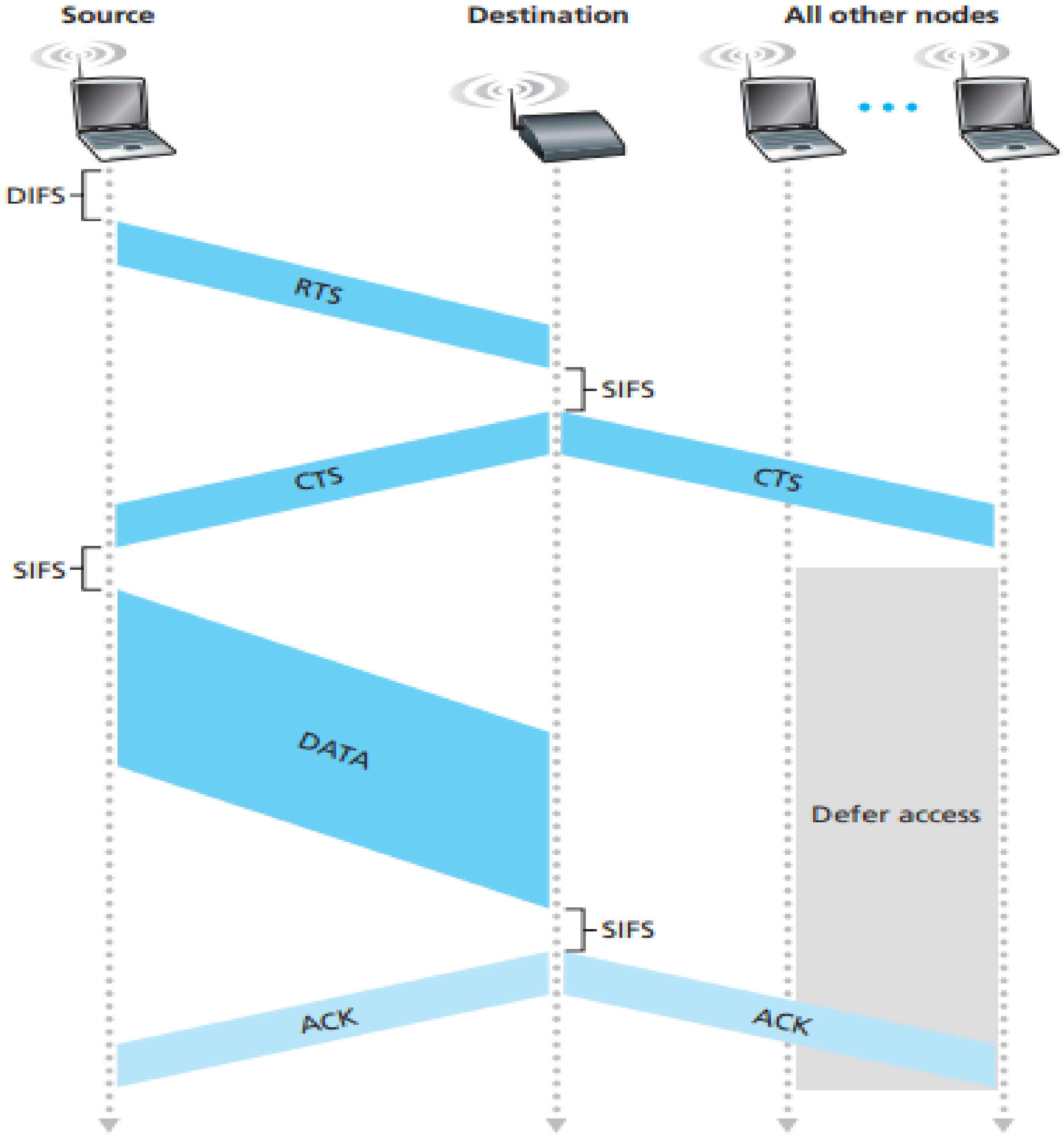
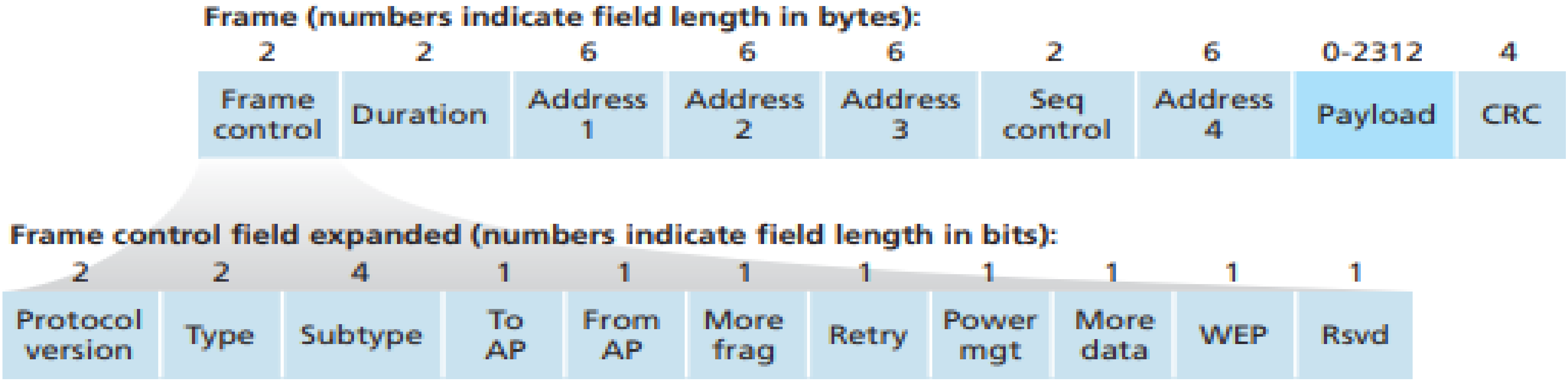


Figure 6.12 ♦ Collision avoidance using the RTS and CTS frames

James F Kurose and Keith W Ross, “Computer Networking: A Top - Down Approach”, Pearson Education; 6 th Edition (2017)

The IEEE 802.11 Frame



Frame (numbers indicate field length in bytes):

2	2	6	6	6	2	6	0-2312	4
Frame control	Duration	Address 1	Address 2	Address 3	Seq control	Address 4	Payload	CRC

Frame control field expanded (numbers indicate field length in bits):

2	2	4	1	1	1	1	1	1	1	1
Protocol version	Type	Subtype	To AP	From AP	More frag	Retry	Power mgt	More data	WEP	Rsvd

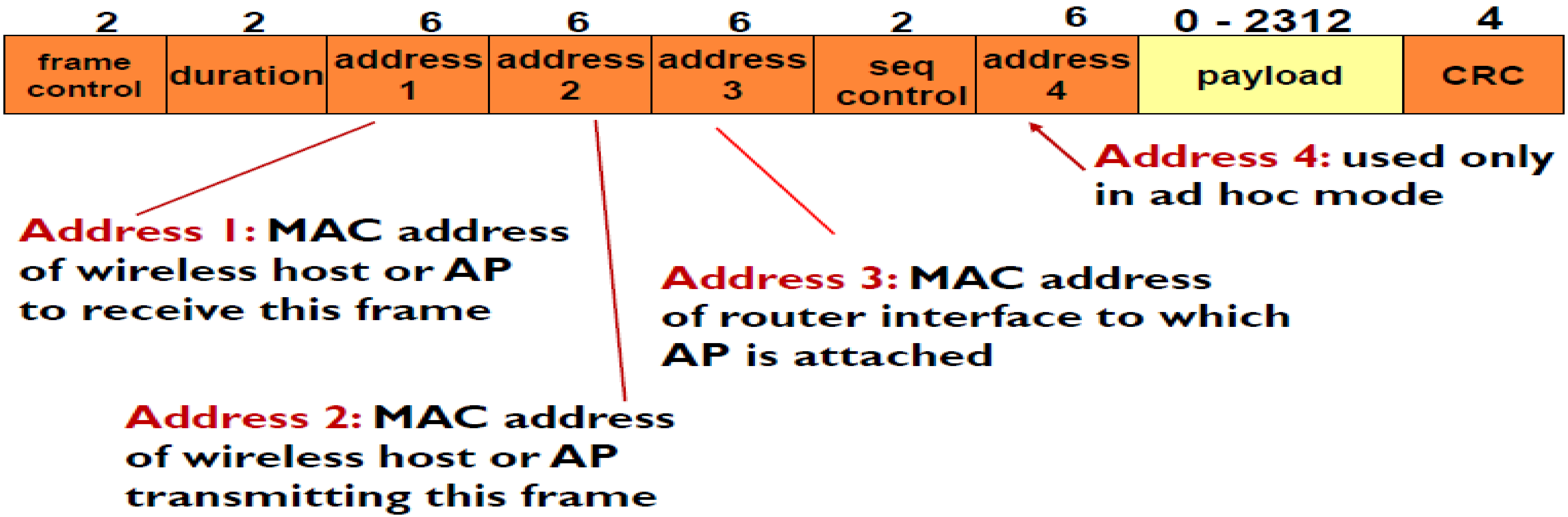
WEP field indicates whether encryption is being used or not

Figure 6.13 ♦ The 802.11 frame

- At the heart of the frame is the payload, which typically consists of an IP datagram or an ARP packet.

James F Kurose and Keith W Ross, “Computer Networking: A Top - Down Approach”, Pearson Education; 6 th Edition (2017)

The IEEE 802.11 Frame



2	2	6	6	6	2	6	0 - 2312	4
frame control	duration	address 1	address 2	address 3	seq control	address 4	payload	CRC

Address 1: MAC address of wireless host or AP to receive this frame

Address 2: MAC address of wireless host or AP transmitting this frame

Address 3: MAC address of router interface to which AP is attached

Address 4: used only in ad hoc mode

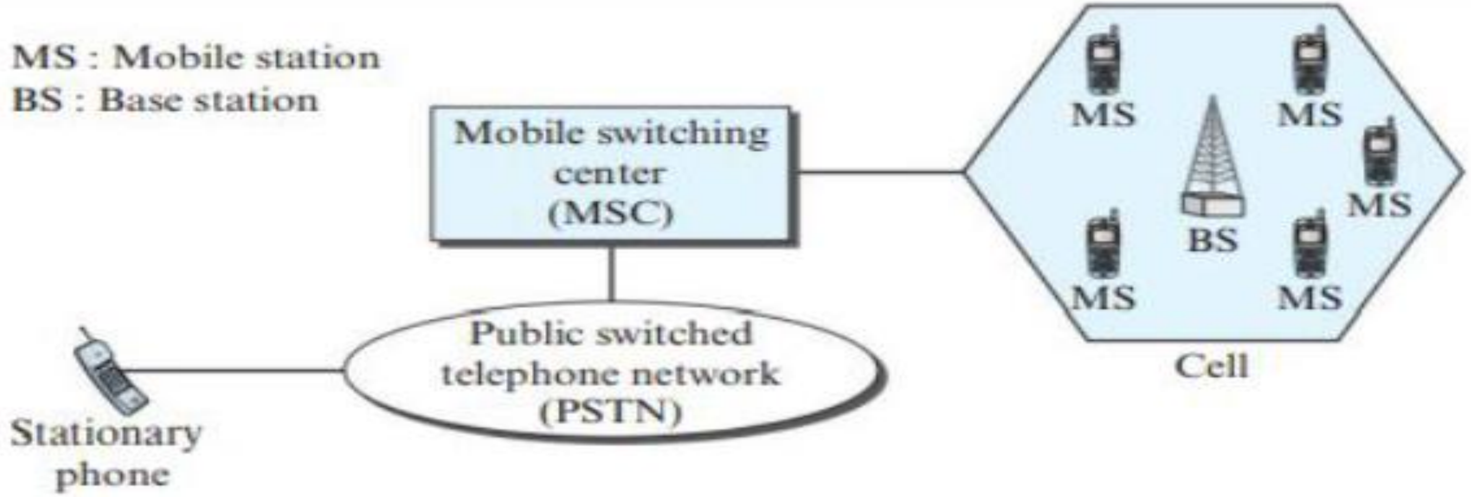
James F Kurose and Keith W Ross, “Computer Networking: A Top - Down Approach”, Pearson Education; 6 th Edition (2017)

CELLULAR NETWORKS

CELLULAR NETWORKS

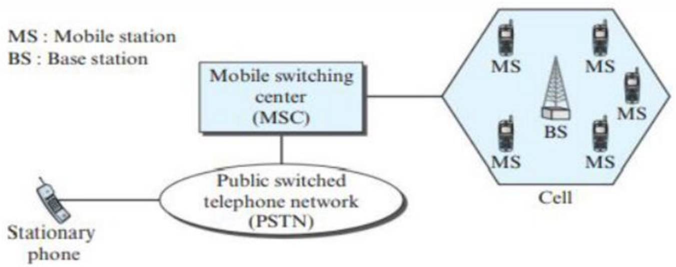
Cellular Telephony

Figure *Cellular system*


MS : Mobile station
BS : Base station
Mobile switching center (MSC)
Public switched telephone network (PSTN)
Stationary phone
MS
MS
MS
MS
MS
BS
Cell

James F Kurose and Keith W Ross, “Computer Networking: A Top - Down Approach”, Pearson Education; 6 th Edition (2017)

CELLULAR NETWORKS


MS : Mobile station
BS : Base station
Mobile switching center (MSC)
MS
MS
MS
BS
MS
MS
Cell
Public switched telephone network (PSTN)
Stationary phone

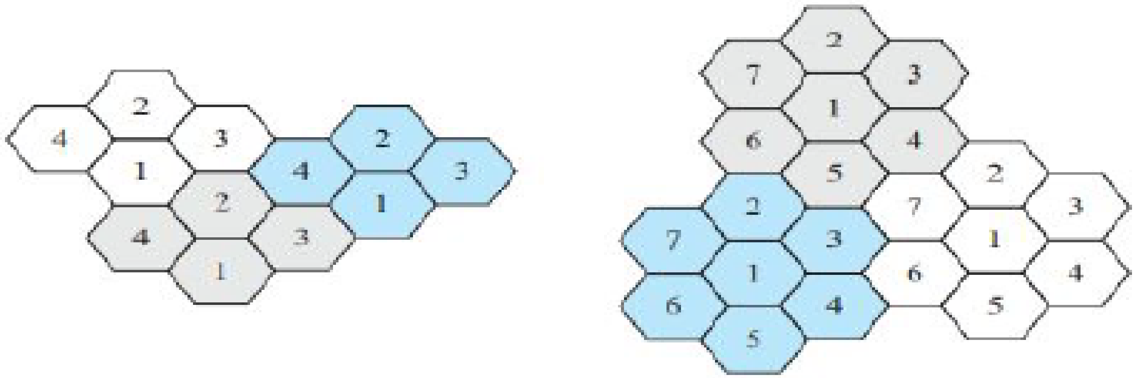
- Cellular telephony is designed to provide communications between two moving units, called mobile stations (MSs), or between one mobile unit and one stationary unit, often called a land unit.
- A service provider must be able to locate and track a caller, assign a channel to the call, and transfer the channel from base station to base station as the caller moves out of range.
- Each cellular service area is divided into small regions called cells.
- Each cell contains an antenna and is controlled by a solar- or AC powered network station, called the base station (BS).
- Each base station, in turn, is controlled by a switching office, called a mobile switching center (MSC).
- The MSC coordinates communication between all the base stations and the telephone central office. It is a computerized center that is responsible for connecting calls, recording call information, and billing.
- Cell size is not fixed(radius from 1 to 30 kms).
- High-density areas require more, geographically smaller cells to meet traffic demands than do low-density areas.

CELLULAR NETWORKS

Frequency-Reuse Principle:

- The frequency reuse factor is the rate at which the same frequency can be used in the
- network.
- Neighboring cells cannot use the same set of frequencies for communication because it may create interference for the users located near the cell boundaries.
- However, the set of frequencies available is limited, and frequencies need to be reused.
- A frequency reuse pattern is a configuration of N cells, N being the reuse factor, in which each cell uses a unique set of frequencies.
- When the pattern is repeated, the frequencies can be reused.
-

Figure *Frequency reuse patterns*

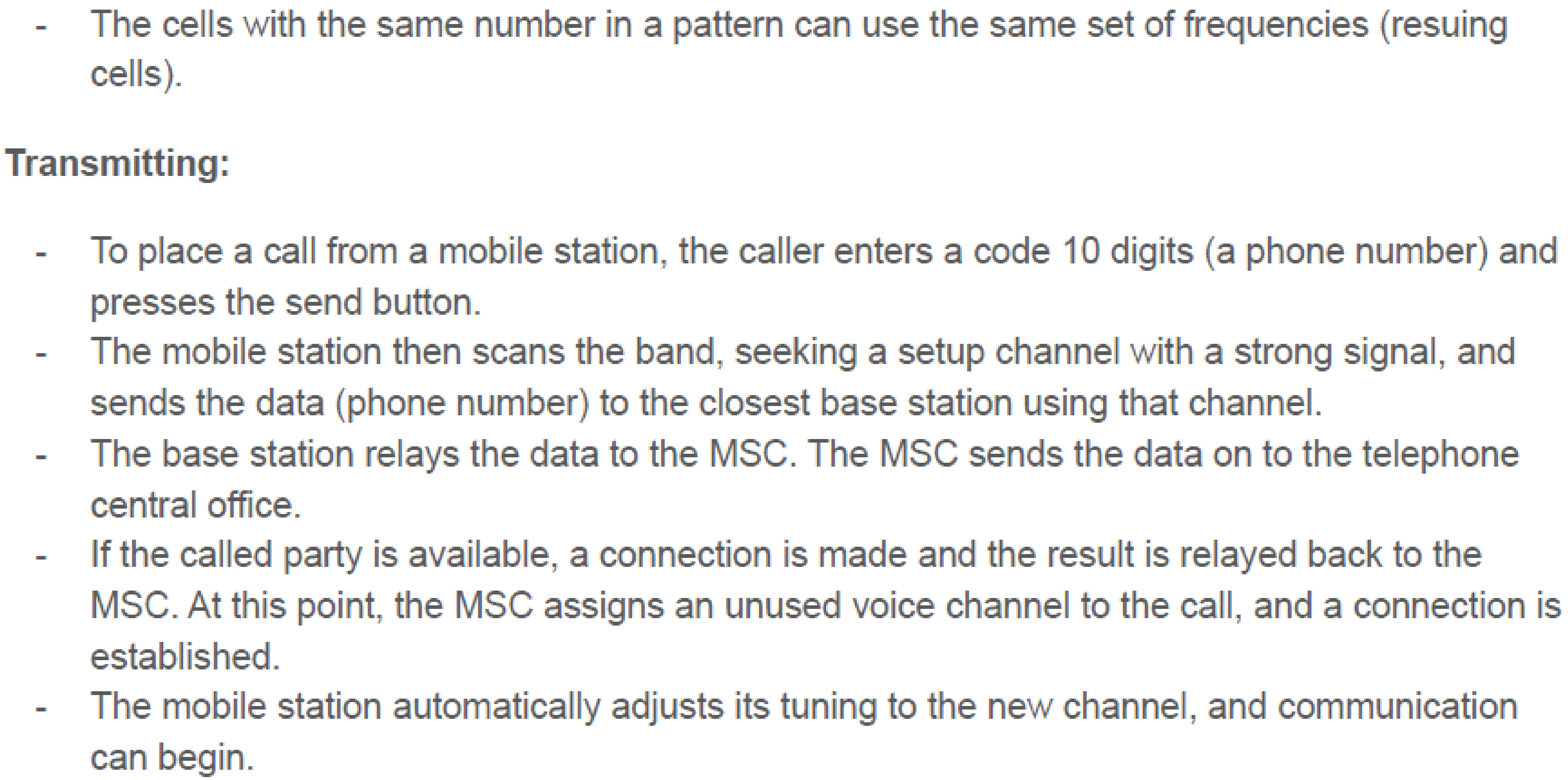


a. Reuse factor of 4

b. Reuse factor of 7

James F Kurose and Keith W Ross, “Computer Networking: A Top - Down Approach”, Pearson Education; 6 th Edition (2017)

CELLULAR NETWORKS

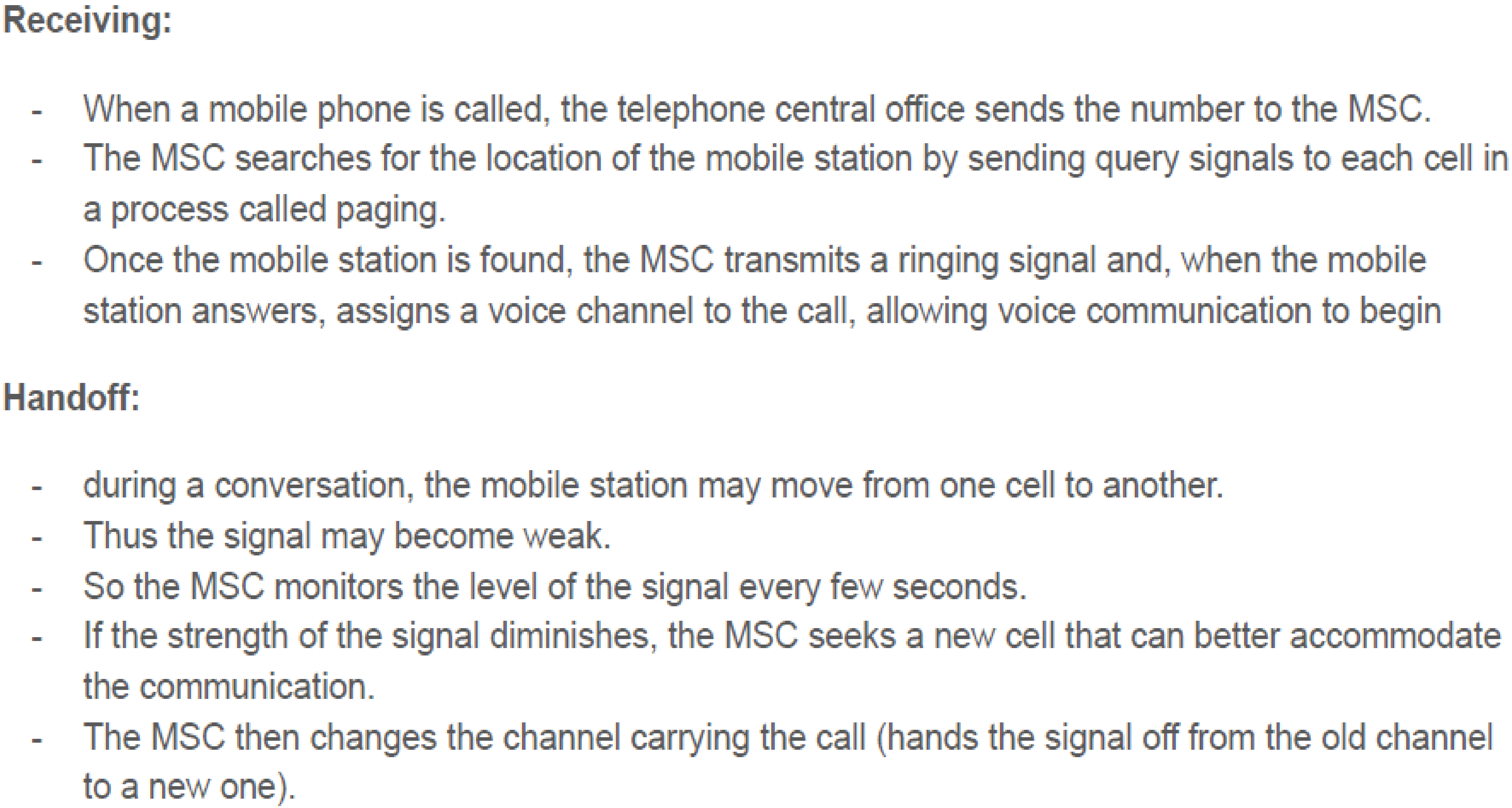


- The cells with the same number in a pattern can use the same set of frequencies (resuing cells).

Transmitting:

- To place a call from a mobile station, the caller enters a code 10 digits (a phone number) and presses the send button.
- The mobile station then scans the band, seeking a setup channel with a strong signal, and sends the data (phone number) to the closest base station using that channel.
- The base station relays the data to the MSC. The MSC sends the data on to the telephone central office.
- If the called party is available, a connection is made and the result is relayed back to the MSC. At this point, the MSC assigns an unused voice channel to the call, and a connection is established.
- The mobile station automatically adjusts its tuning to the new channel, and communication can begin.

CELLULAR NETWORKS



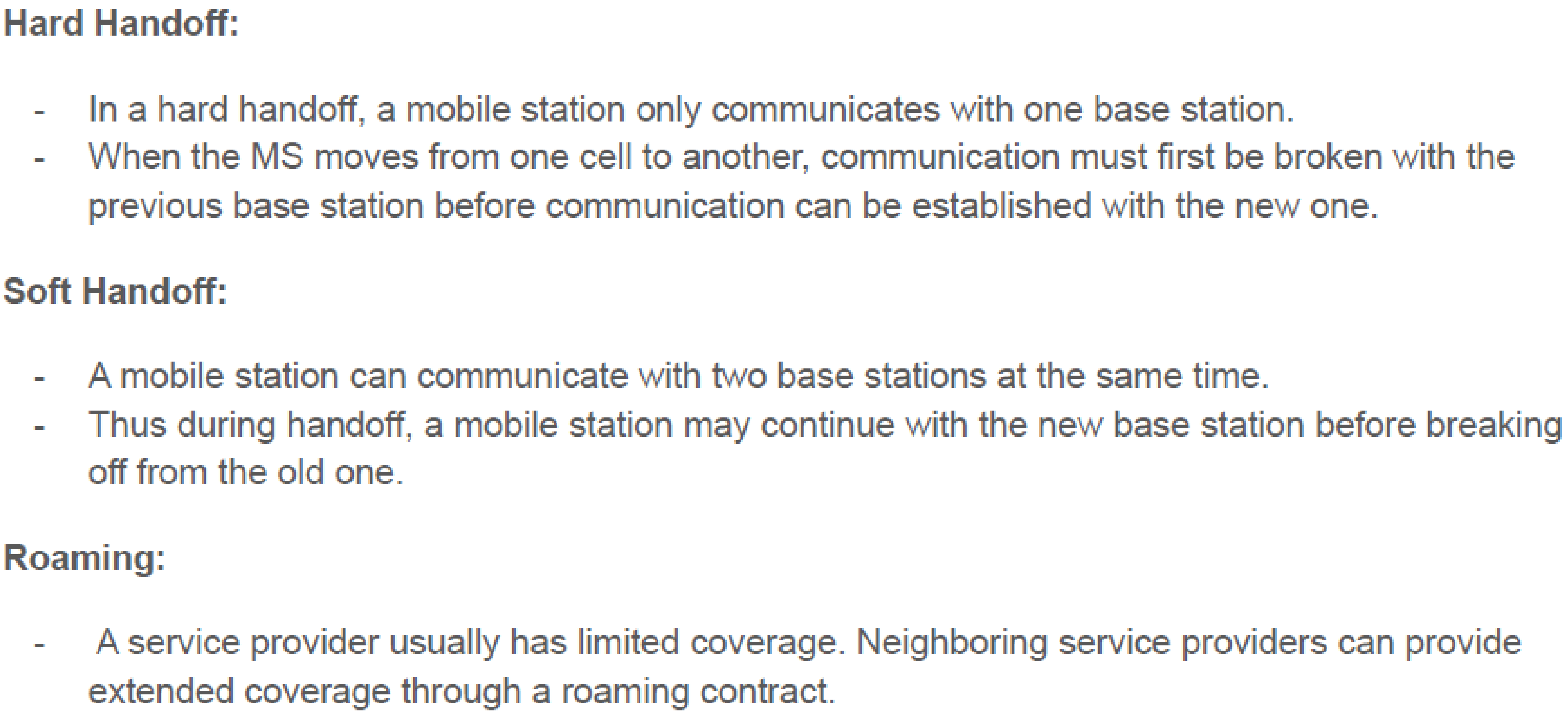
Receiving:

- When a mobile phone is called, the telephone central office sends the number to the MSC.
- The MSC searches for the location of the mobile station by sending query signals to each cell in a process called paging.
- Once the mobile station is found, the MSC transmits a ringing signal and, when the mobile station answers, assigns a voice channel to the call, allowing voice communication to begin

Handoff:

- during a conversation, the mobile station may move from one cell to another.
- Thus the signal may become weak.
- So the MSC monitors the level of the signal every few seconds.
- If the strength of the signal diminishes, the MSC seeks a new cell that can better accommodate the communication.
- The MSC then changes the channel carrying the call (hands the signal off from the old channel to a new one).

CELLULAR NETWORKS



Hard Handoff:

- In a hard handoff, a mobile station only communicates with one base station.
- When the MS moves from one cell to another, communication must first be broken with the previous base station before communication can be established with the new one.

Soft Handoff:

- A mobile station can communicate with two base stations at the same time.
- Thus during handoff, a mobile station may continue with the new base station before breaking off from the old one.

Roaming:

- A service provider usually has limited coverage. Neighboring service providers can provide extended coverage through a roaming contract.

BLUETOOTH (IEEE 802.15 std)

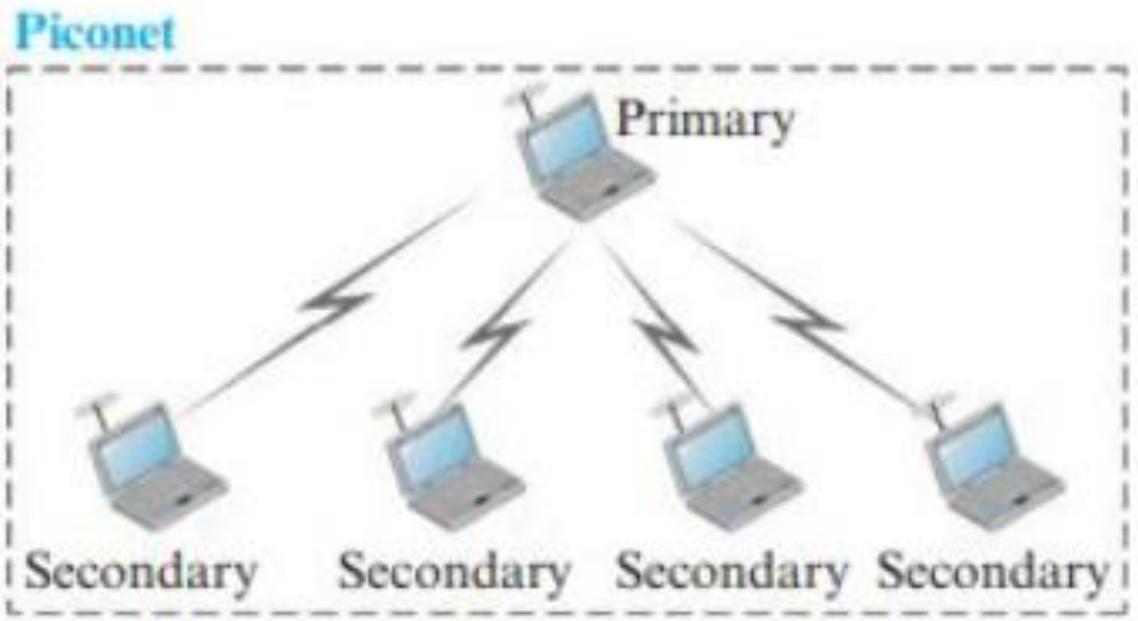
BLUETOOTH (IEEE 802.15 std)

- It is a wireless LAN technology designed to connect different types of devices which are at a shorter distance.
- It is a wireless personal-area network (PAN)
- It is an adhoc network, which means that the network is formed spontaneously.
- Two types of bluetooth networks: piconet, scatternet

Piconets:

- It is a bluetooth network
- A piconet can have up to eight stations, one of which is called the primary; the rest are called secondaries.
- The communication between the primary and the secondary can be one-to-one or one-to-many.
- Secondary stations cannot communicate with each other directly.
- It also have 255 parked nodes, these are secondary nodes and cannot take participation in communication unless it get converted to the active state.

Figure *Piconet*

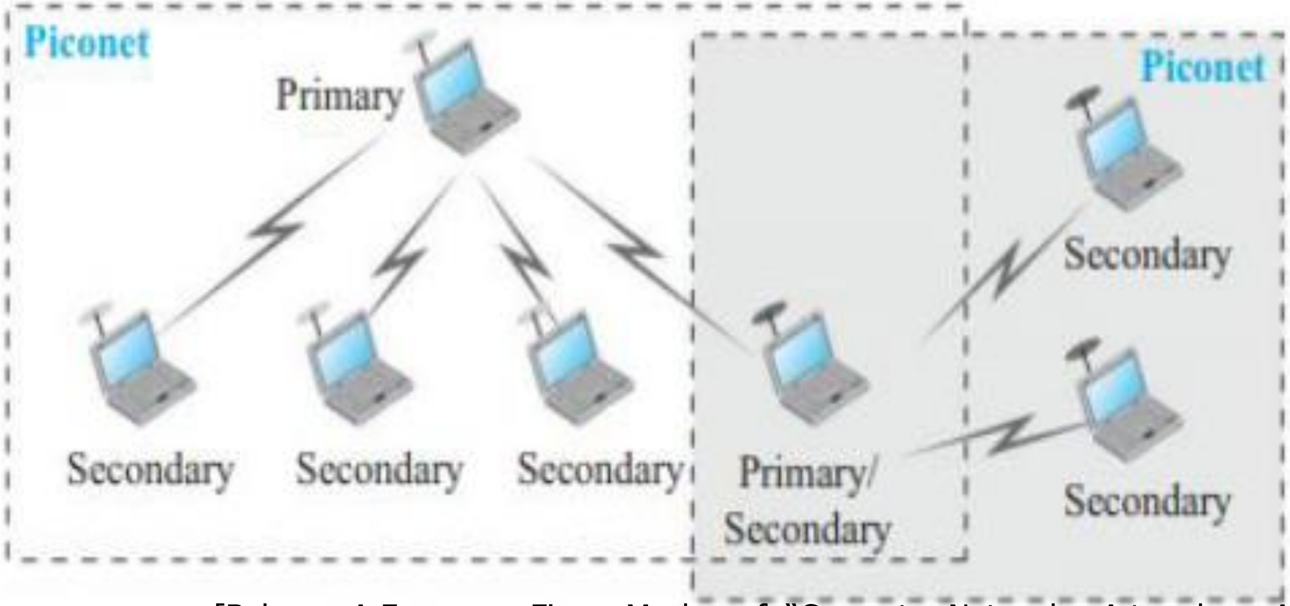


[Behrouz A Forouzan, Firouz Mosharraf, “Computer Networks: A top down Approach”, McGraw Hill Education]

Scatternet:

- It is a combination of piconets.
- A secondary station in one piconet can be the primary in another piconet.
- This station can receive messages from the primary in the first piconet (as a secondary) and, acting as a primary, deliver them to secondaries in the second piconet.

Figure *Scatternet*

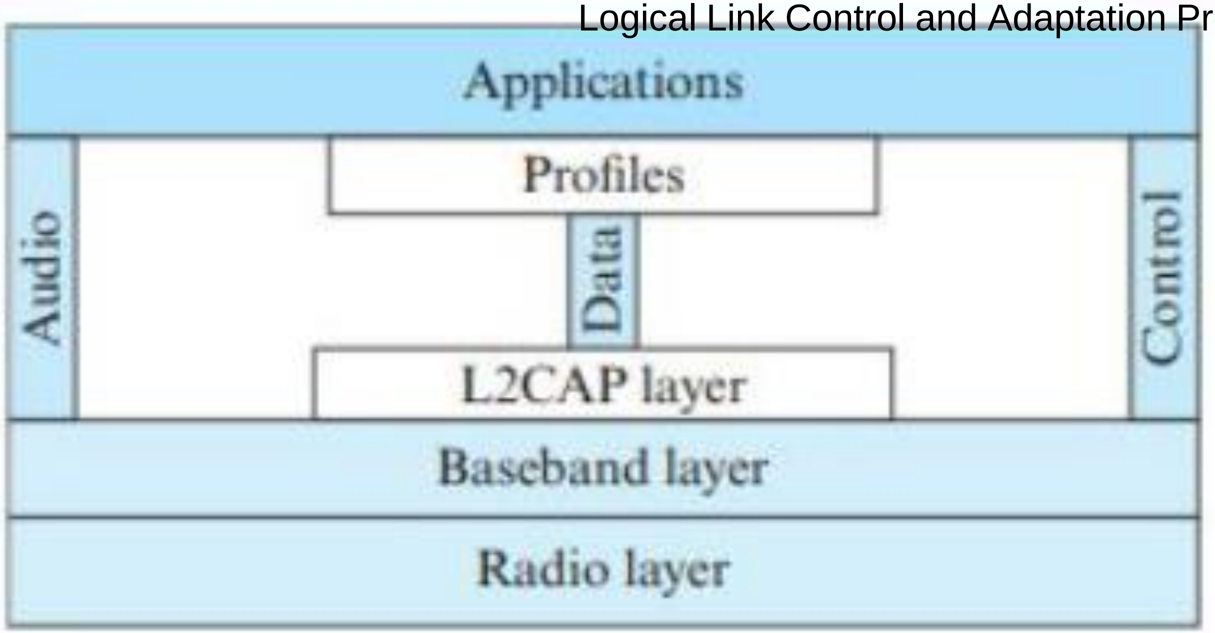


[Behrouz A Forouzan, Firouz Mosharraf, “Computer Networks: A top down Approach”, McGraw Hill Education]

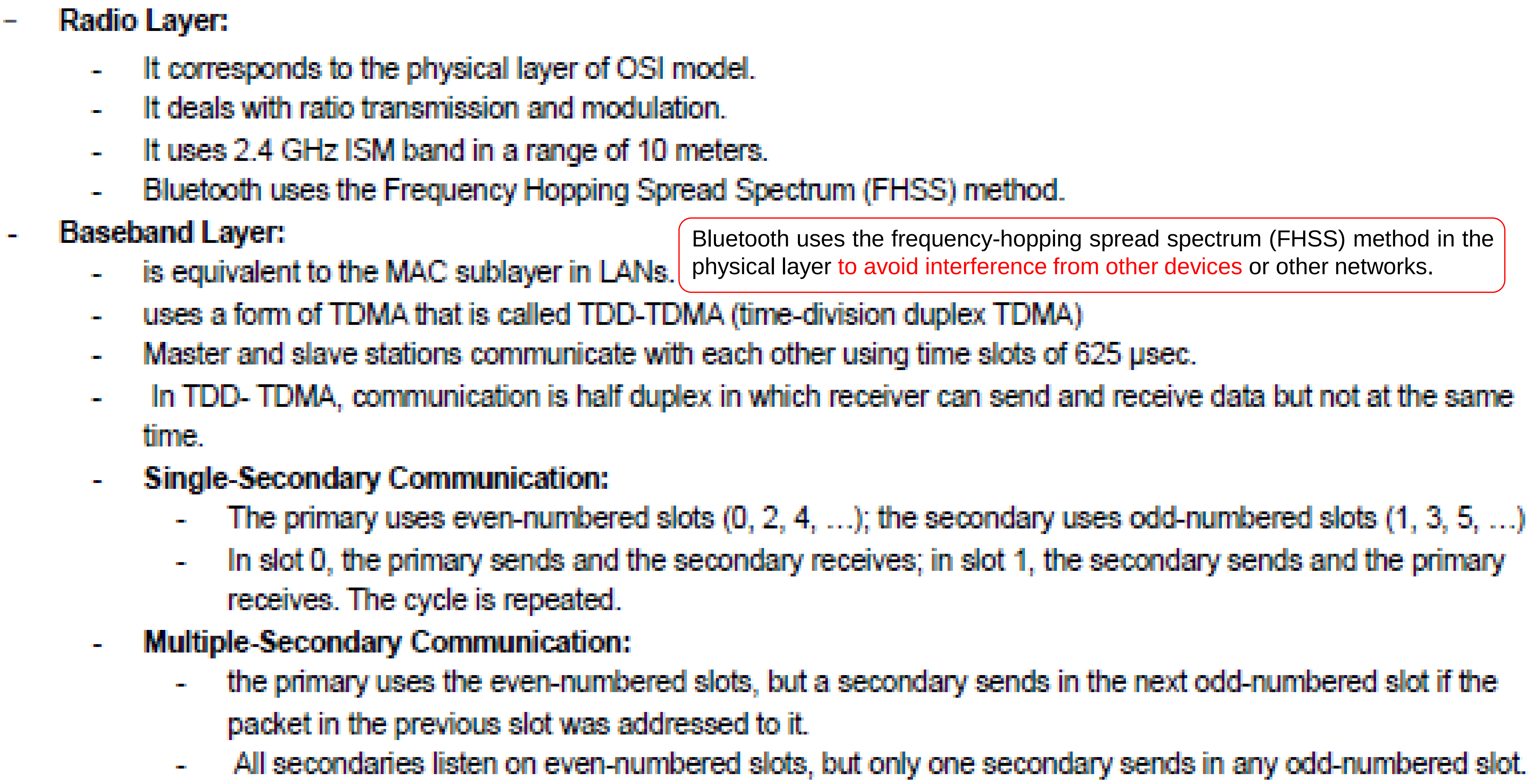
Bluetooth Protocol Architecture:

Figure *Bluetooth layers*

Logical Link Control and Adaptation Protocol, or L2CAP



[Behrouz A Forouzan, Firouz Mosharraf, “Computer Networks: A top down Approach”, McGraw Hill Education]



- **Radio Layer:**
  - It corresponds to the physical layer of OSI model.
  - It deals with ratio transmission and modulation.
  - It uses 2.4 GHz ISM band in a range of 10 meters.
  - Bluetooth uses the Frequency Hopping Spread Spectrum (FHSS) method.
- **Baseband Layer:**
  - is equivalent to the MAC sublayer in LANs.
  - uses a form of TDMA that is called TDD-TDMA (time-division duplex TDMA)
  - Master and slave stations communicate with each other using time slots of 625 µsec.
  - In TDD- TDMA, communication is half duplex in which receiver can send and receive data but not at the same time.
  - **Single-Secondary Communication:**
    - The primary uses even-numbered slots (0, 2, 4, ...); the secondary uses odd-numbered slots (1, 3, 5, ...)
    - In slot 0, the primary sends and the secondary receives; in slot 1, the secondary sends and the primary receives. The cycle is repeated.
  - **Multiple-Secondary Communication:**
    - the primary uses the even-numbered slots, but a secondary sends in the next odd-numbered slot if the packet in the previous slot was addressed to it.
    - All secondaries listen on even-numbered slots, but only one secondary sends in any odd-numbered slot.

Bluetooth uses the frequency-hopping spread spectrum (FHSS) method in the physical layer to avoid interference from other devices or other networks.

- In Baseband layer, two types of links can be created between a primary and a secondary. These are:
    - **Asynchronous Connection-less (ACL):**
        - is used when data integrity is more important than avoiding latency
        - If the data gets corrupted, it will be retransmitted.
    - **Synchronous Connection-Oriented (SCO):**
        - It is used when fast delivery is needed.
        - No retransmissions even if data gets corrupted
        - used for real-time audio where avoiding delay is all-important

- **Logical Link, Control Adaptation Protocol Layer (L2CAP):**
    - is equivalent to logical link control sub-layer of LAN.
    - The ACL link uses L2CAP for data exchange but sco channel does not use it.
    - The various functions of L2CAP are:

    i) Segmentation and reassembly:

        - L2CAP receives the packets of up to 64 KB from upper layers and divides them into frames for transmission.
        - It adds extra information to define the location of frame in the original packet.
        - The L2CAP reassembles the frame into packets again at the destination.

    ii) Multiplexing:

        - L2CAP perfoms multiplexing at sender side and de-multiplexing at receiver side.

- At the sender site, it accepts data from one of the upper layer protocols, frames them and deliver them to the Baseband layer.
- At the receiver site, it accepts a frame from the baseband layer, extracts the data, and delivers them to the appropriate protocol 1ayer.

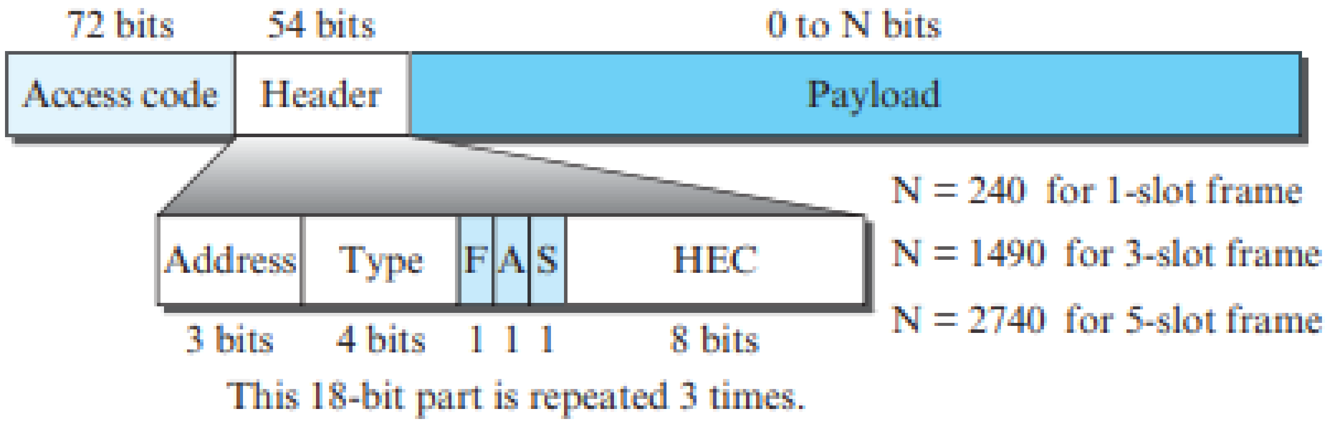
iii) Quality of Service (QOS):

- L2CAP handles quality of service requirements, both when links are established and during normal operation.

iv) Group Management

Bluetooth Frame Format:

Figure 6.25 *Frame format types*



[Behrouz A Forouzan, Firouz Mosharraf, “Computer Networks: A top down Approach”, McGraw Hill Education]

- **Access Code**: It is 72 bit field that contains synchronization bits. It identifies the master.
- **Header**: This is 54-bit field. It contain 18 bit pattern that is repeated for 3 times.

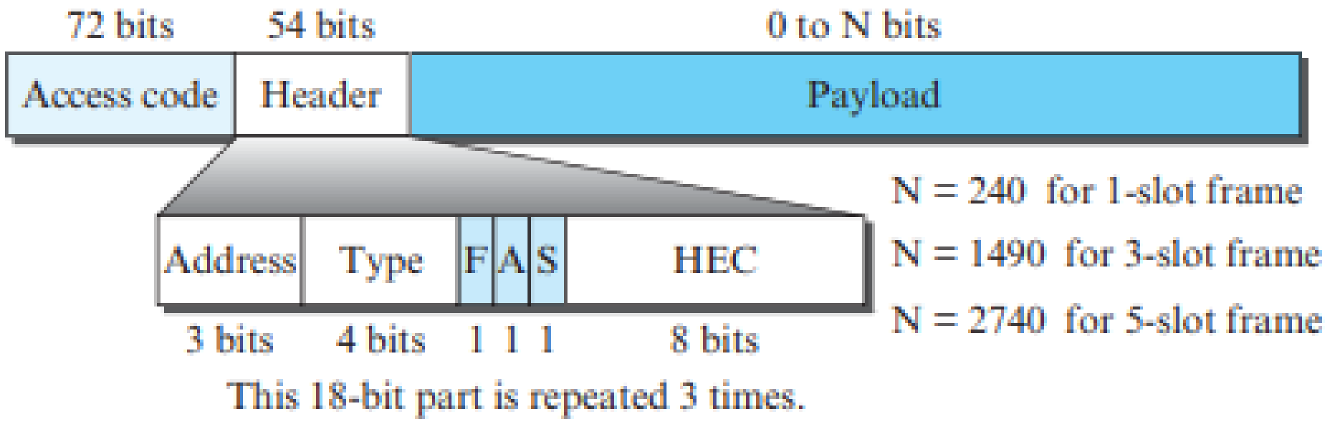
The header field contains following sub-fields:

(i) **Address**: This 3 bit field can define up to seven slaves (1 to 7). If the address is zero, it is used for broadcast communication from primary to all secondaries.

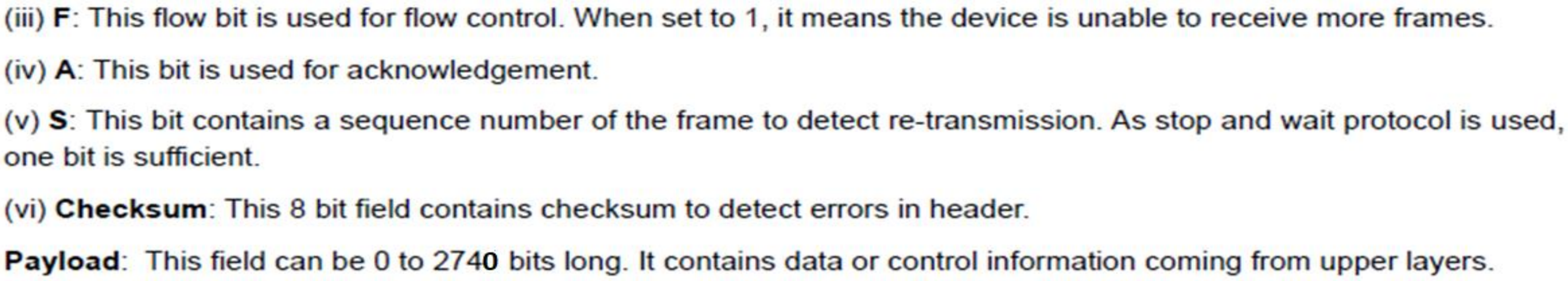
(ii)Type: This 4 bit field identifies the type of data coming from upper layers.

Bluetooth Frame Format:

Figure 6.25 *Frame format types*



[Behrouz A Forouzan, Firouz Mosharraf, “Computer Networks: A top down Approach”, McGraw Hill Education]



(iii) **F**: This flow bit is used for flow control. When set to 1, it means the device is unable to receive more frames.

(iv) **A**: This bit is used for acknowledgement.

(v) **S**: This bit contains a sequence number of the frame to detect re-transmission. As stop and wait protocol is used, one bit is sufficient.

(vi) **Checksum**: This 8 bit field contains checksum to detect errors in header.

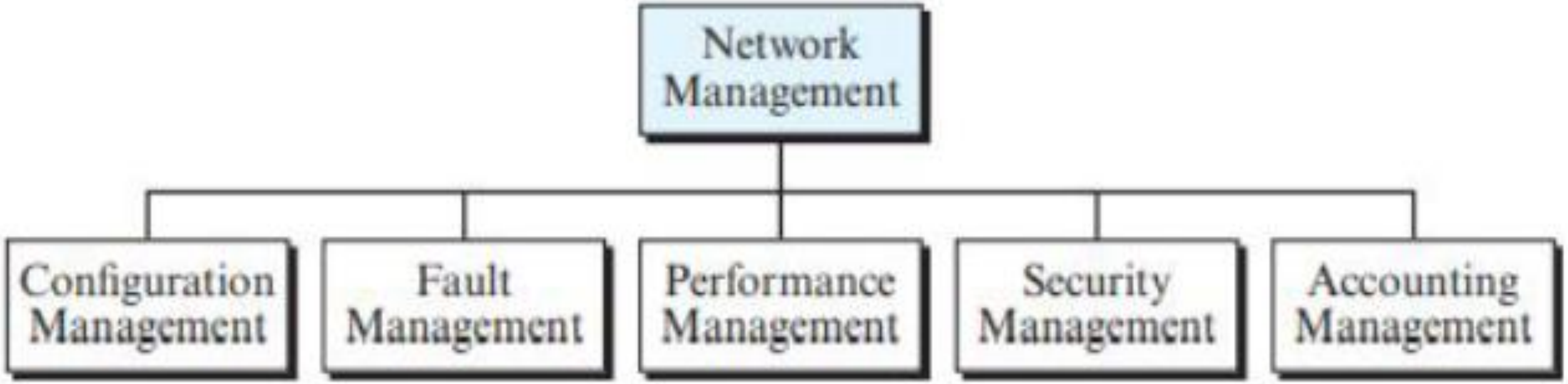
Payload: This field can be 0 to 2740 bits long. It contains data or control information coming from upper layers.

HEC: The 8-bit header error correction subfield is a checksum to detect errors in each 18-bit header section.

Introduction to Network Management

- Network management includes the deployment, integration, and coordination of the hardware, software, and human elements to monitor, test, poll, configure, analyze, evaluate, and control the network and element resources to meet the real-time, operational performance, and Quality of Service requirements at a reasonable cost.

Figure ' *Areas of network management*



[Behrouz A Forouzan, Firouz Mosharraf, "Computer Networks: A top down Approach", McGraw Hill Education]

i) Configuration Management:

- Monitors the different devices in the managed network and their hardware and software configurations.
- **Reconfiguration:**
  - a daily occurrence in a large network.
  - **Hardware Reconfiguration:**
    - covers all changes to the hardware.
  - **Software Reconfiguration:**
    - covers all changes to the software.
  - **User-Account Reconfiguration:**
    - adding/removing users, creating groups, setting user-privileges etc
- **Documentation**:
  - The original network configuration and each subsequent change must be recorded.
  - **Hardware Documentation**
  - **Software Documentation**
  - **User-Account Documentation**

ii) Fault Management:

- It continuously monitors the status of each component individually and in relation to each other.
    - **Reactive Fault Management:**
        - It is responsible for detecting, isolating, correcting, and recording faults.
        - It handles short-term solutions to faults.
    - **Proactive Fault Management:**
        - It tries to prevent faults from occurring.

iii) Performance Management:

- It continuously monitors the performance of each device of the network.
- Capacity, Traffic, Throughput, Response Time

iv) Security Management:

- It is responsible for controlling access to the network based on predefined policy.

v) Accounting Management:

- is the controlling of users' access to network resources through charges.

- There are three principal components of a network management architecture: a managing entity (the boss in our analogy above—you), the managed devices (the branch office), and a network management protocol.

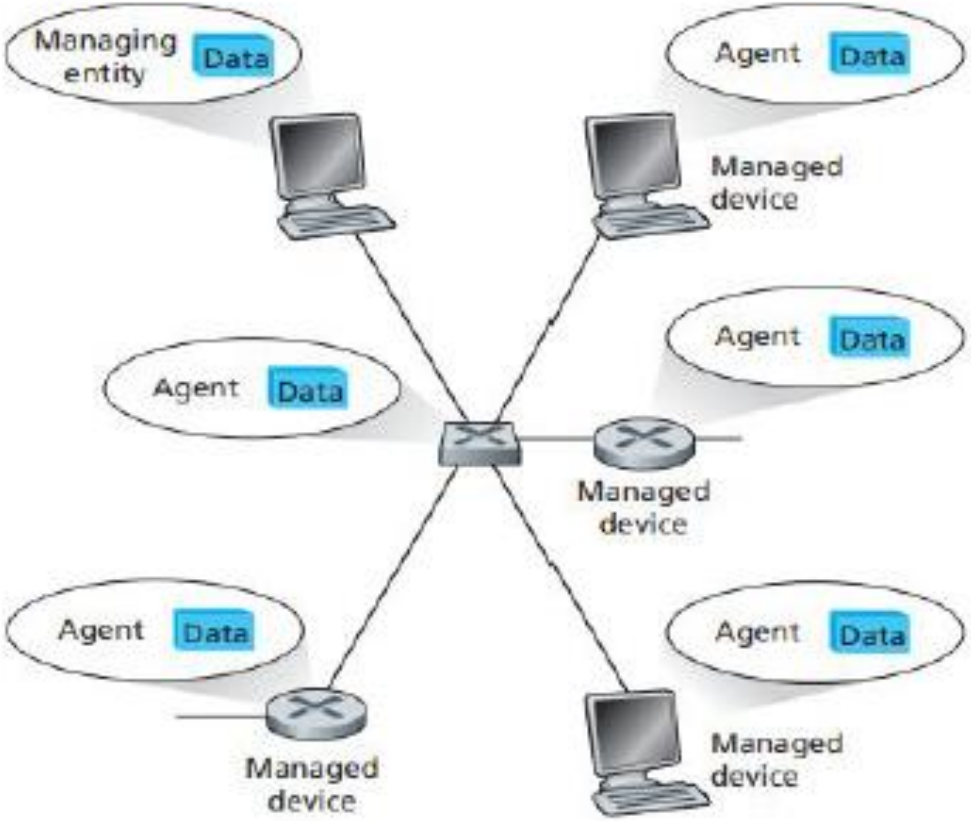
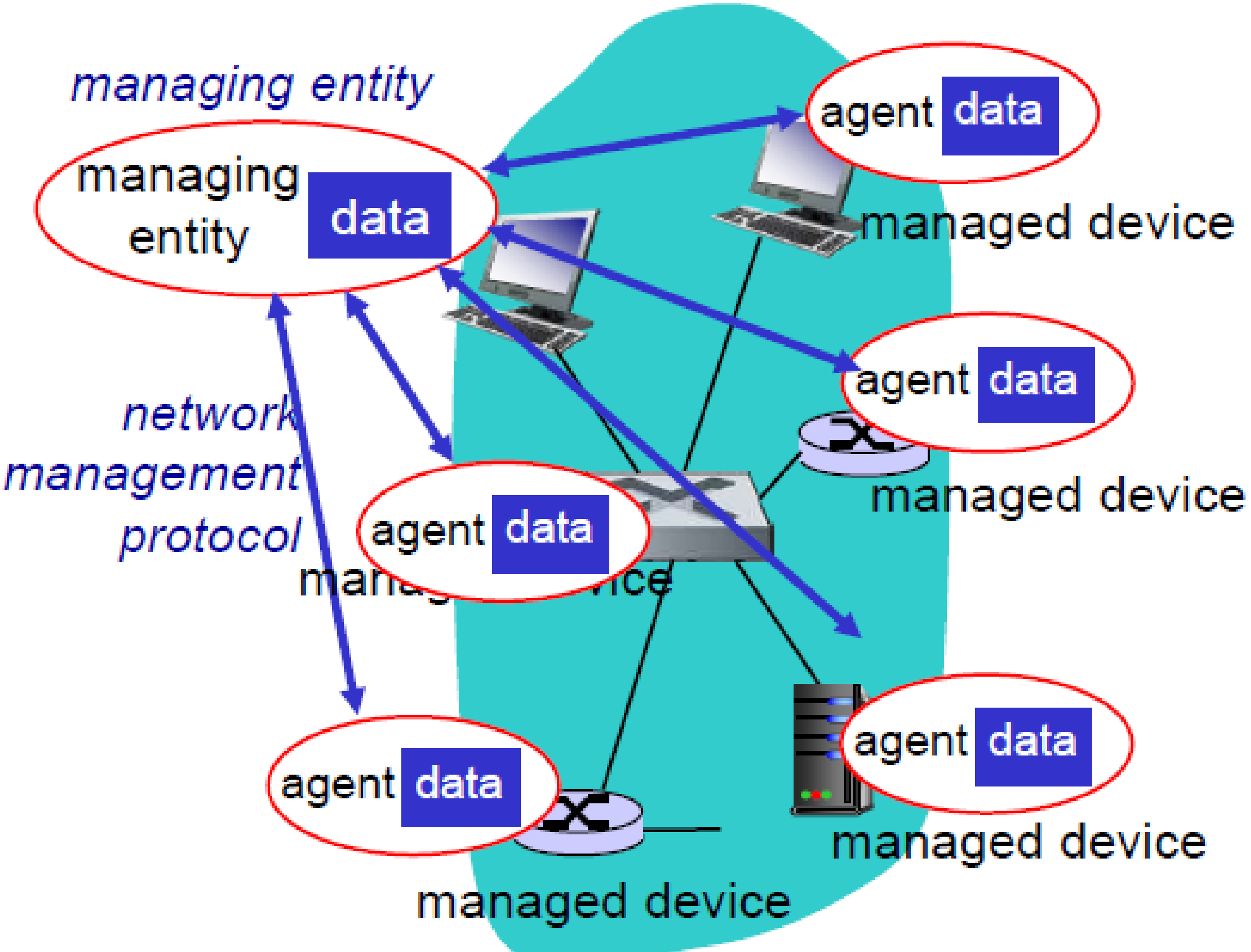


Figure ♦ Principal components of a network management architecture

Infrastructure for network management

definitions:



managed devices contain *managed objects* whose data is gathered into a *Management Information Base (MIB)*

SNMP overview: 4 key parts

- Management information base (MIB):
  distributed information store of network management data
- Structure of Management Information (SMI):
  data definition language for MIB objects
- SNMP protocol
  protocol for network management
- Security, administration capabilities
  major addition in SNMPv3

Management information base (MIB):

- Definitions of network management objects, known as MIB objects.
- An MIB object might be a counter, such as the number of IP datagrams discarded at a router due to errors in an IP datagram header or the number of carrier sense errors in an Ethernet interface card;
- descriptive information such as the version of the software running on a DNS server;
- status information such as whether a particular device is functioning correctly;
- or protocol-specific information such as a routing path to a destination.
- MIB objects thus define the management information maintained by a managed device.
- Related MIB objects are gathered into MIB modules.

Structure of Management Information: SMI

- The language used to define the management information residing in a managed network entity.
- Such a definition language is needed to ensure that the syntax and semantics of the network management data are well defined and unambiguous.

SNMP protocol

- The Simple Network Management Protocol is used to convey MIB information among managing entities and agents executing on behalf of managing entities.
- The most common usage of SNMP is in a request-response mode in which an SNMP managing entity sends a request to an SNMP agent, who receives the request, performs some action, and sends a reply to the request
- Typically, a request will be used to query (retrieve) or modify (set) MIB object values associated with a managed device.

SNMP protocol

- A second common usage of SNMP is for an agent to send an unsolicited message, known as a trap message, to a managing entity.
- Trap messages are used to notify a managing entity of an exceptional situation that has resulted in changes to MIB object values.

SNMP protocol: message formats

SNMPv2 defines seven types of messages, known generically as protocol data units—PDUs—

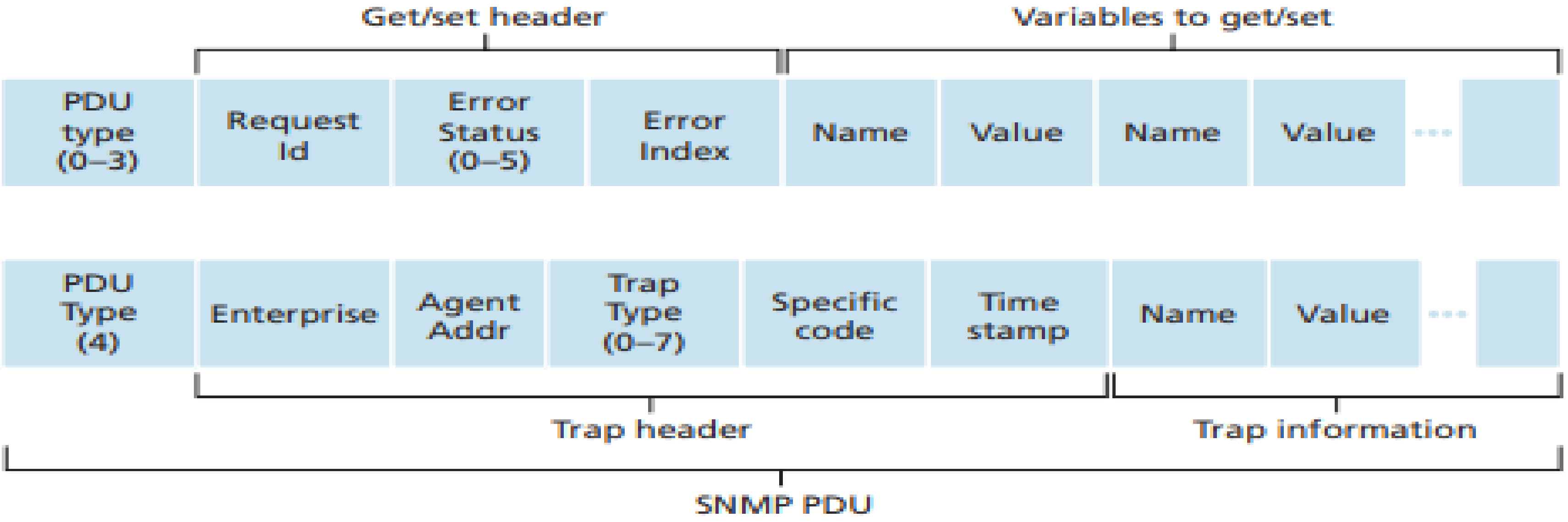
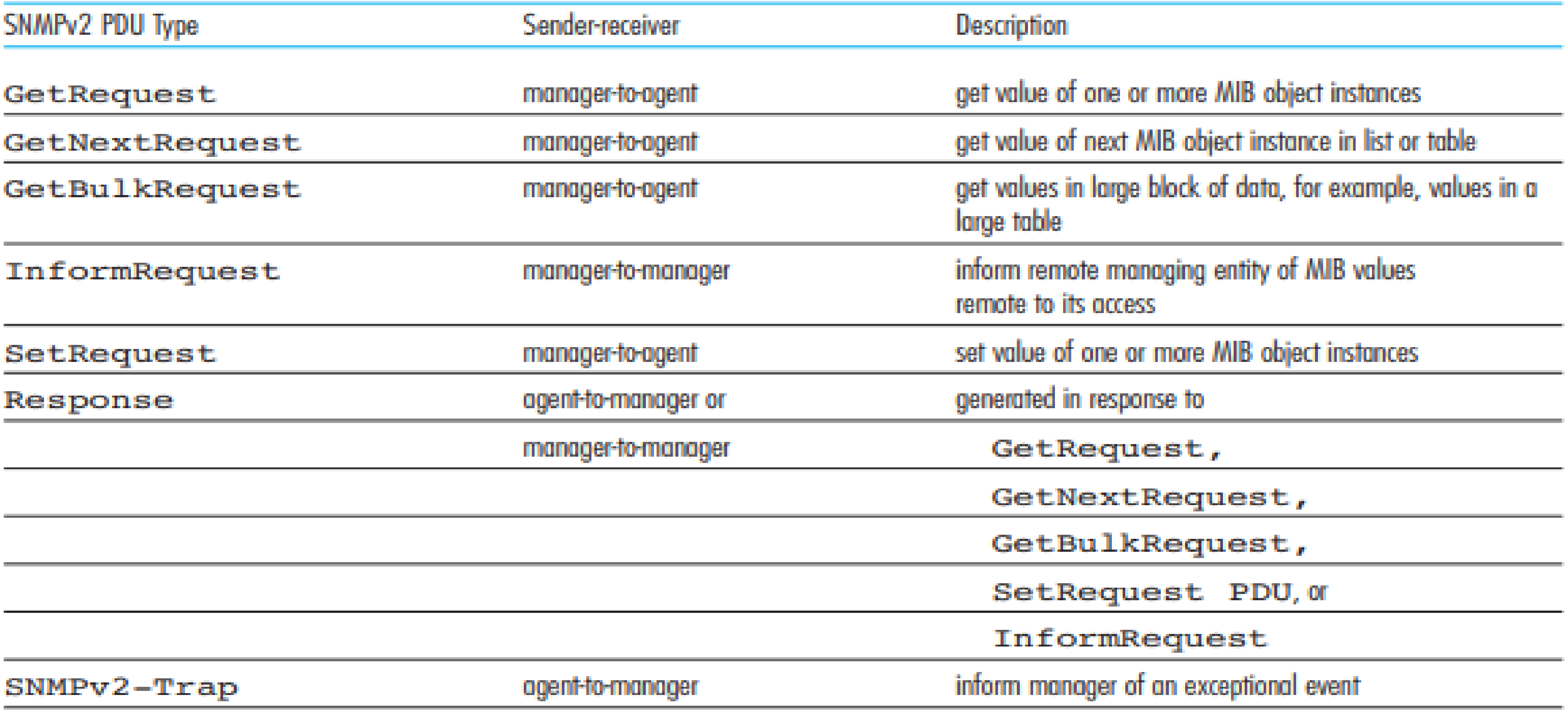


Figure 9.4 ♦ SNMP PDU format

James F Kurose and Keith W Ross, “Computer Networking: A Top - Down Approach”, Pearson Education; 6 th Edition (2017)



SNMPv2 PDU Type	Sender-receiver	Description
GetRequest	manager-to-agent	get value of one or more MIB object instances
GetNextRequest	manager-to-agent	get value of next MIB object instance in list or table
GetBulkRequest	manager-to-agent	get values in large block of data, for example, values in a large table
InformRequest	manager-to-manager	inform remote managing entity of MIB values remote to its access
SetRequest	manager-to-agent	set value of one or more MIB object instances
Response	agent-to-manager or	generated in response to
	manager-to-manager	GetRequest,
		GetNextRequest,
		GetBulkRequest,
		SetRequest PDU, or
		InformRequest
SNMPv2-Trap	agent-to-manager	inform manager of an exceptional event

Table 9.4 ◆ SNMPv2 PDU types

James F Kurose and Keith W Ross, “Computer Networking: A Top - Down Approach”, Pearson Education; 6 th Edition (2017)

Security and Administration

- The designers of SNMPv3 have said that “SNMPv3 can be thought of as SNMPv2 with additional security and administration capabilities”
- SNMPv3 provides for encryption, authentication,protection against playback attacks and access control.

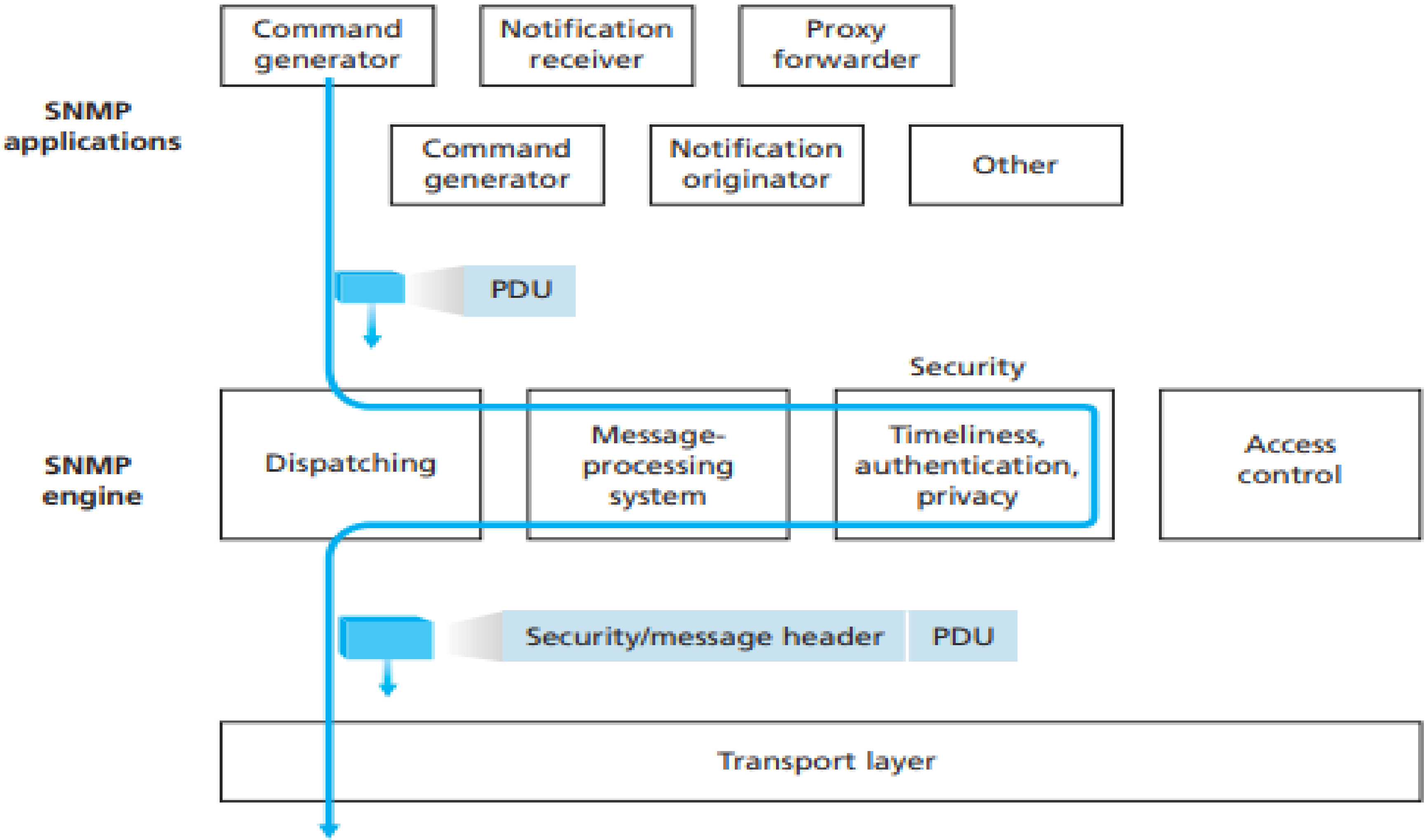


Figure 9.5 ♦ SNMPv3 engine and applications

James F Kurose and Keith W Ross, “Computer Networking: A Top - Down Approach”, Pearson Education; 6 th Edition (2017)

- Encryption

SNMP PDUs can be encrypted using the Data Encryption Standard (DES) in Cipher Block Chaining (CBC) mode.

- Authentication

SNMP uses the Message Authentication Code (MAC) technique

- Protection against playback

Nonces can be used to guard against playback attacks.

- Access control

SNMPv3 provides a view-based access control that controls which network management information can be queried and/or set by which users.

Network-Layer Security: IPsec and Virtual Private Networks

IPsec and Virtual Private Networks

- The IP security protocol, more commonly known as IPsec, provides security at the network layer.
- IPsec secures IP datagrams between any two network-layer entities, including hosts and routers.
- Institutions (corporations, government branches, non-profit organizations, and so on) use IPsec to create virtual private networks (VPNs) that run over the public Internet.

Virtual Private Networks (VPNs)

- An institution that extends over multiple geographical regions often desires its own IP network, so that its hosts and servers can send data to each other in a secure and confidential manner.
- To achieve this goal, the institution could actually deploy a stand-alone physical network—including routers, links, and a DNS infrastructure—that is completely separate from the public Internet.
- Such a disjoint network, dedicated to a particular institution, is called a private network.
- A private network can be very costly, as the institution needs to purchase, install, and maintain its own physical network infrastructure.
- Instead of deploying and maintaining a private network, many institutions today create VPNs over the existing public Internet.
- With a VPN, the institution's interoffice traffic is sent over the public Internet rather than over a physically independent network.
- But to provide confidentiality, the inter-office traffic is encrypted before it enters the public Internet

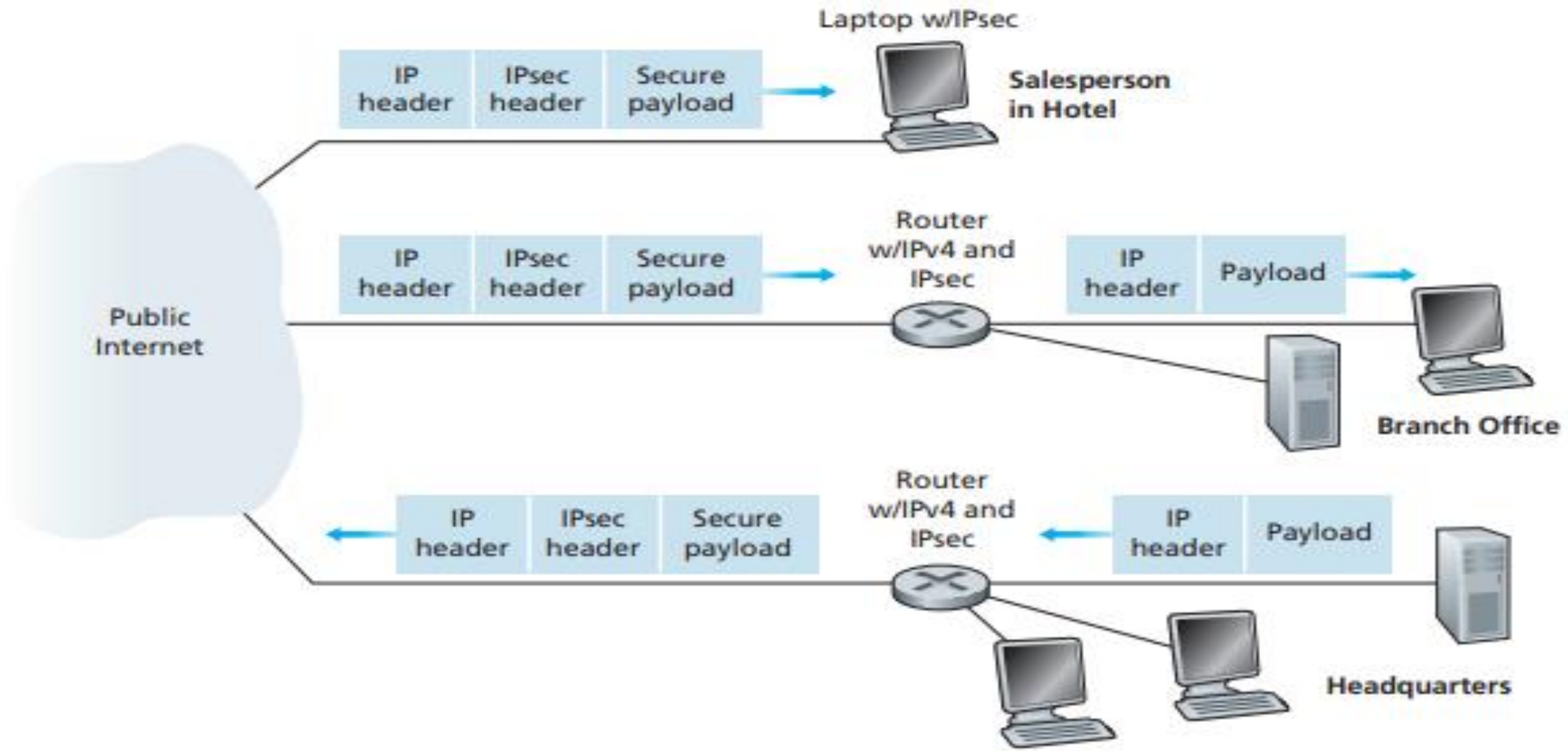


Figure 8.27 ♦ Virtual Private Network (VPN)

James F Kurose and Keith W Ross, "Computer Networking: A Top - Down Approach", Pearson Education; 6 th Edition (2017)

IPsec Protocol

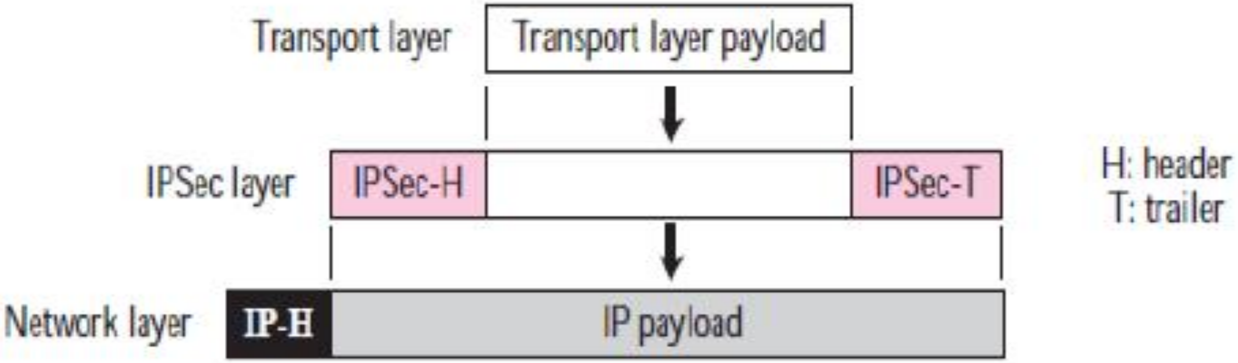
Two Modes

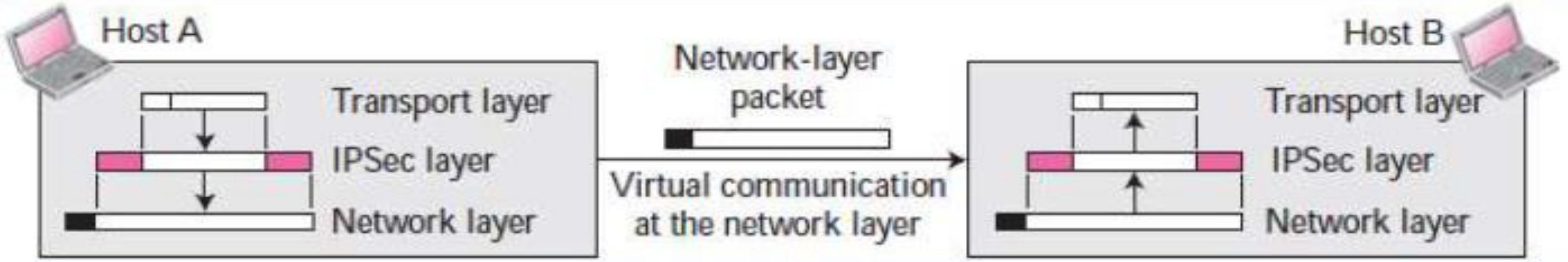
- **IPSec operates in one of two different modes: transport mode or tunnel mode.**

Transport Mode **-** In **transport mode, IPSec protects what is delivered from the transport layer to the network** layer.

- In other words, transport mode protects the payload to be encapsulated in the network layer.
- Transport mode is normally used when we need host-to-host (end-to-end) protection of data.
- The sending host uses IPSec to authenticate and/or encrypt the payload delivered from the transport layer.

IPSec in transport mode

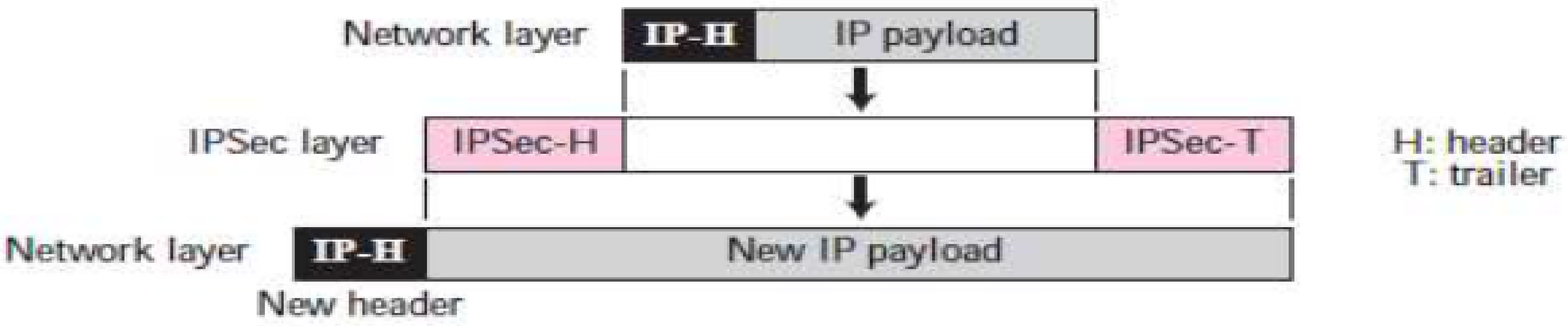




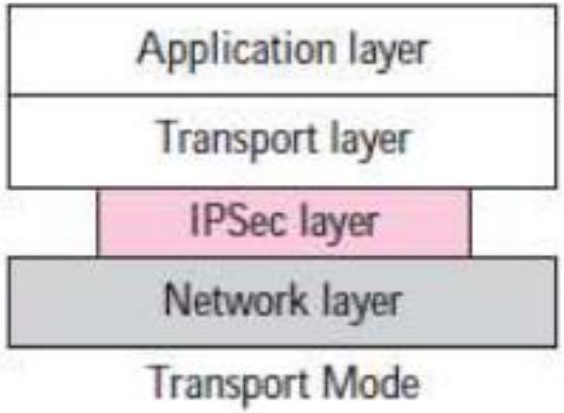
IPSec in Tunnel mode

Tunnel Mode

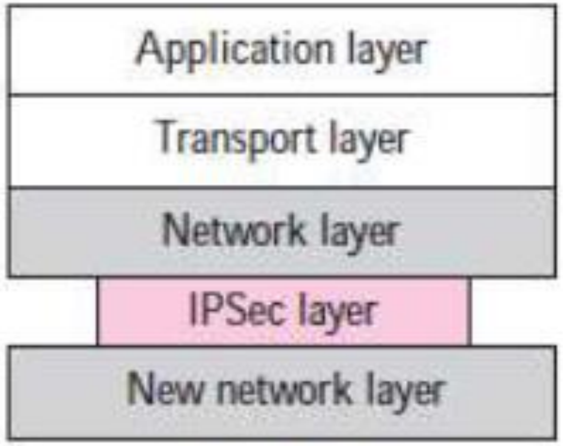
- In **tunnel mode, IPSec protects the entire IP packet.**
- **It takes an IP packet, including the** header, applies IPSec security methods to the entire packet, and then adds a new IP header.



Transport mode versus tunnel mode



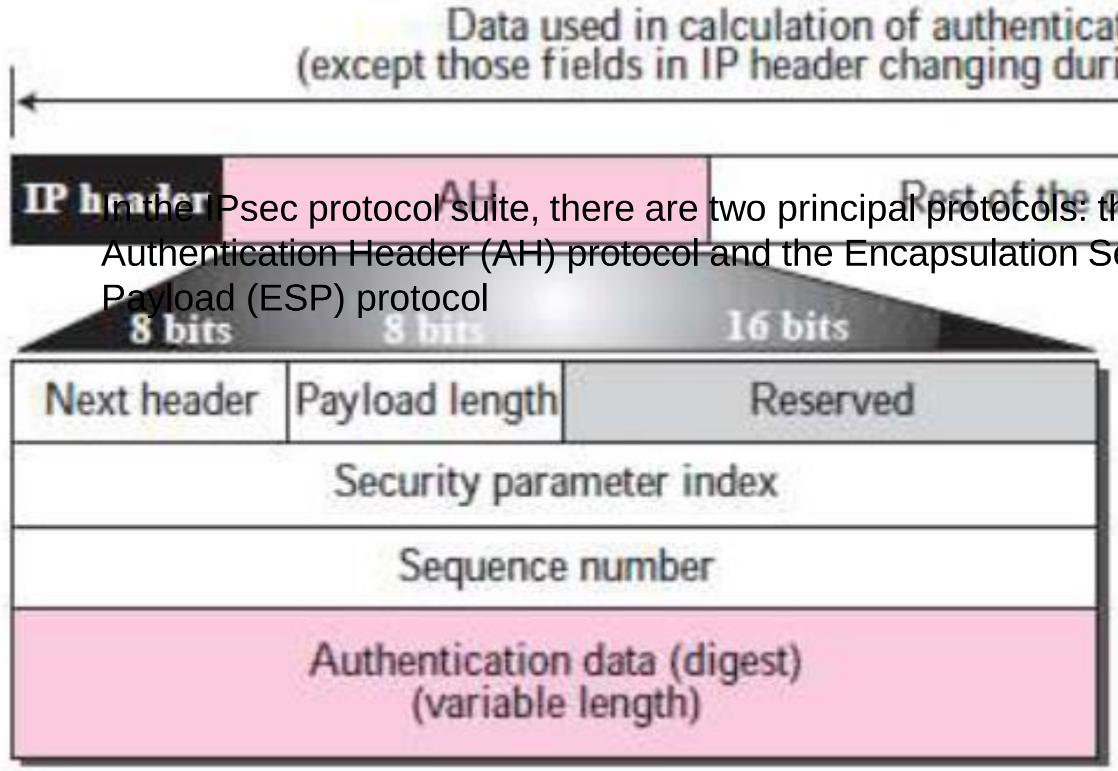
Transport Mode



Tunnel Mode

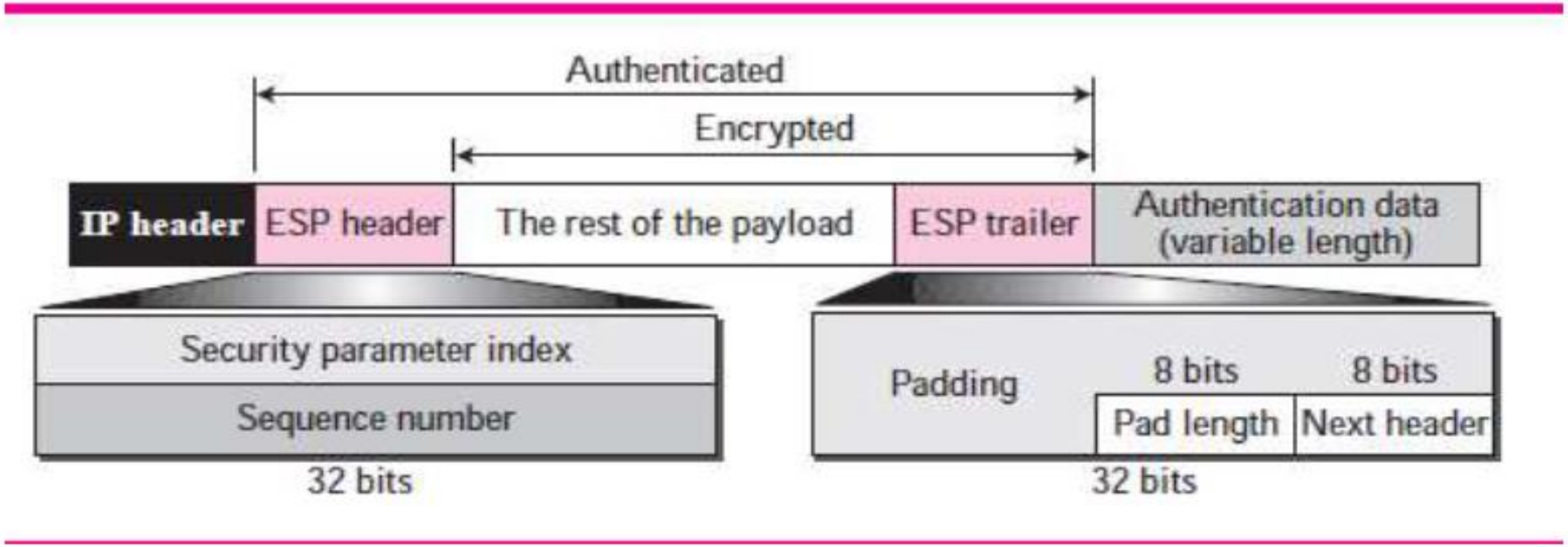
In the IPsec protocol suite, there are two principal protocols: the Authentication Header (AH) protocol and the Encapsulation Security Payload (ESP) protocol

Authentication header protocol


Data used in calculation of authentication data
(except those fields in IP header changing during transmission)
IP header
AH
Rest of the original packet
Padding
8 bits
8 bits
16 bits
Next header
Payload length
Reserved
Security parameter index
Sequence number
Authentication data (digest)
(variable length)

In the IPsec protocol suite, there are two principal protocols: the Authentication Header (AH) protocol and the Encapsulation Security Payload (ESP) protocol

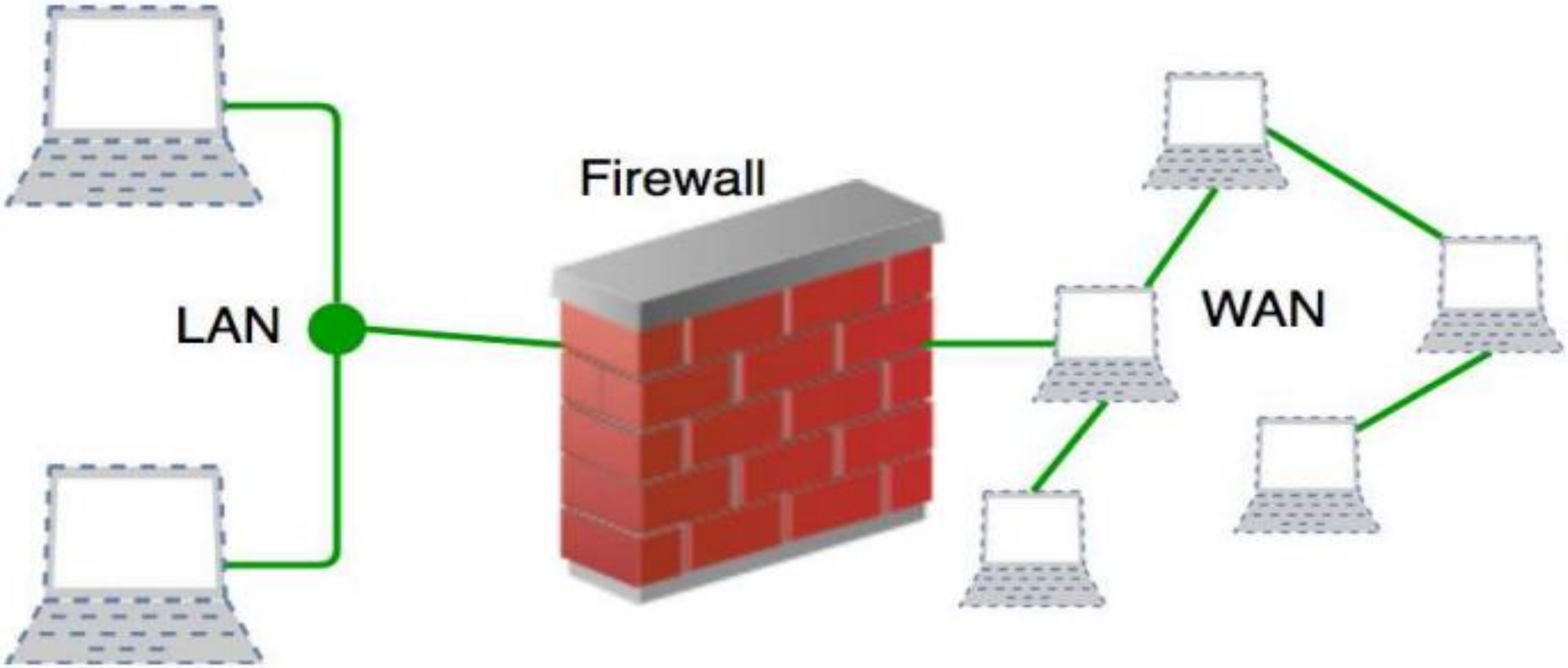
ESP


Authenticated
Encrypted
IP header
ESP header
The rest of the payload
ESP trailer
Authentication data
(variable length)
Security parameter index
Sequence number
32 bits
Padding
8 bits
8 bits
Pad length
Next header
32 bits

FIREWALLS

Overview of Firewalls

- As the name implies, a firewall acts to provide secured access between two networks
- A firewall may be implemented as a standalone hardware device or in the form of a software on a client computer or a proxy server
  - The two types of firewall are generally known as the hardware firewall and the software firewall

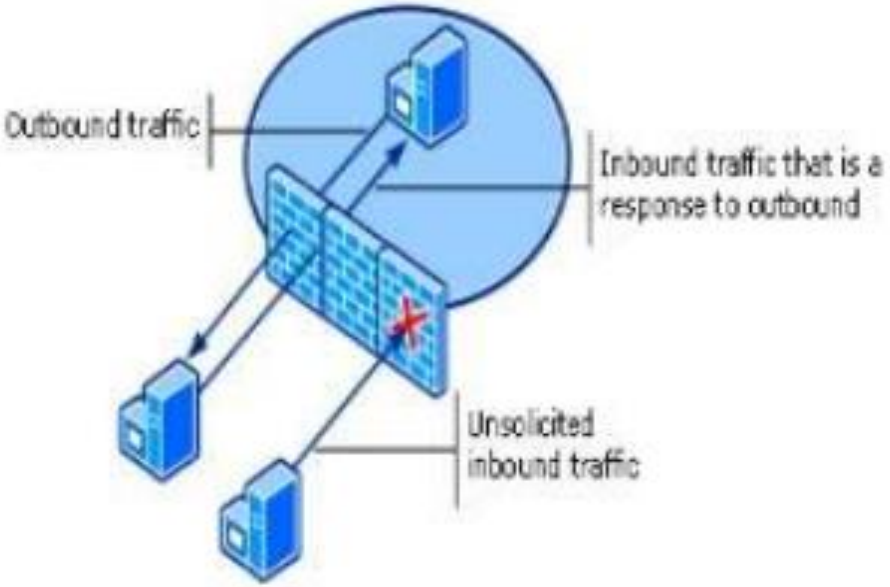

Firewall
LAN
WAN

Firewalls in Practice

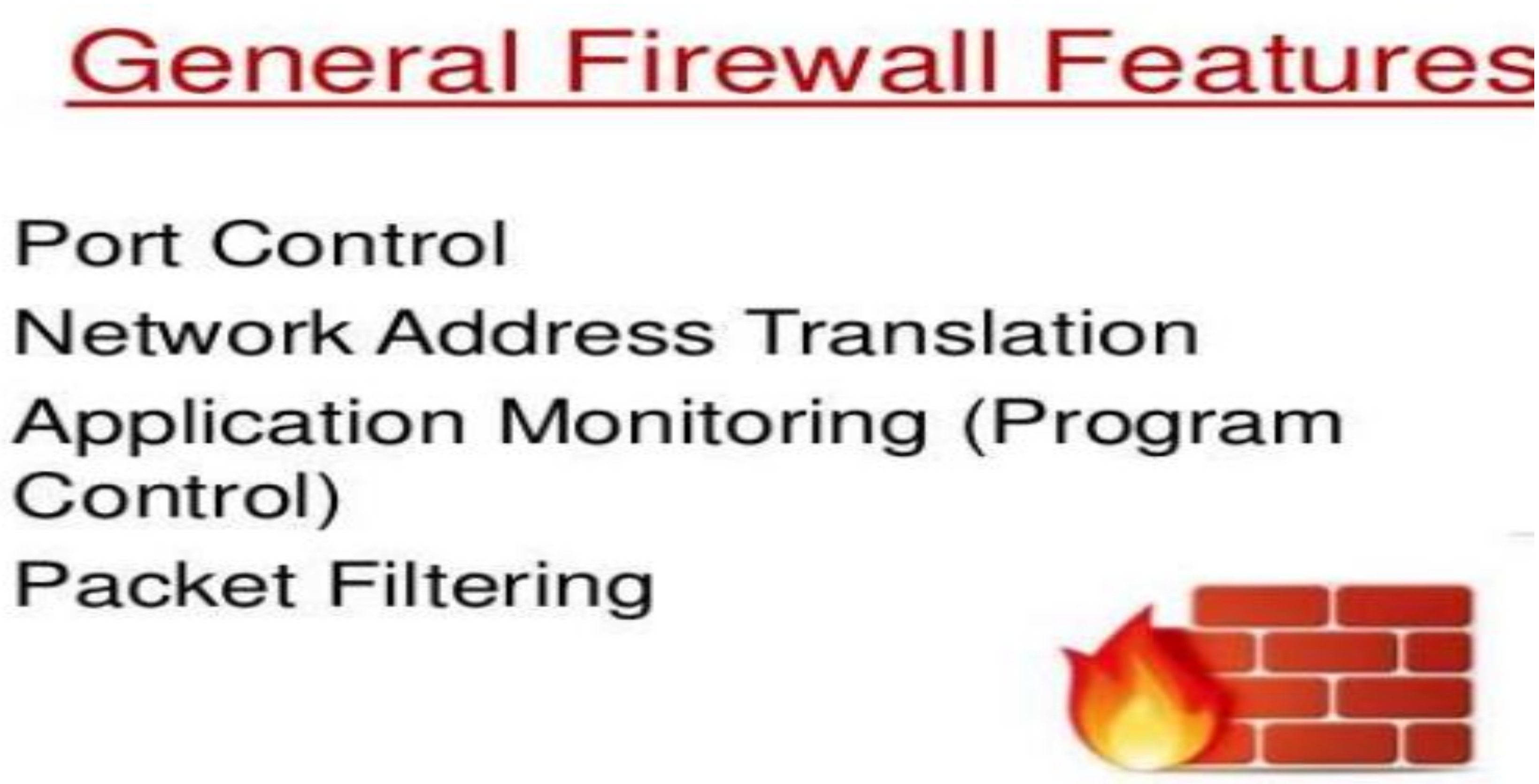
A computer may be protected by both a hardware and a software firewall.

Mode of Operation

A firewall that stands in between two networks will inspect a packet that is ready to pass between the networks and allow or block the packet based on the rules set for the firewall to operate.



Outbound traffic
Inbound traffic that is a response to outbound
Unsolicited inbound traffic



General Firewall Features

- Port Control
- Network Address Translation
- Application Monitoring (Program Control)
- Packet Filtering

Additional Firewall Features

- Data encryption
- Hiding presence
- Reporting/logging
- e-mail virus protection
- Pop-up ad blocking
- Cookie digestion
- Spy ware protection etc.

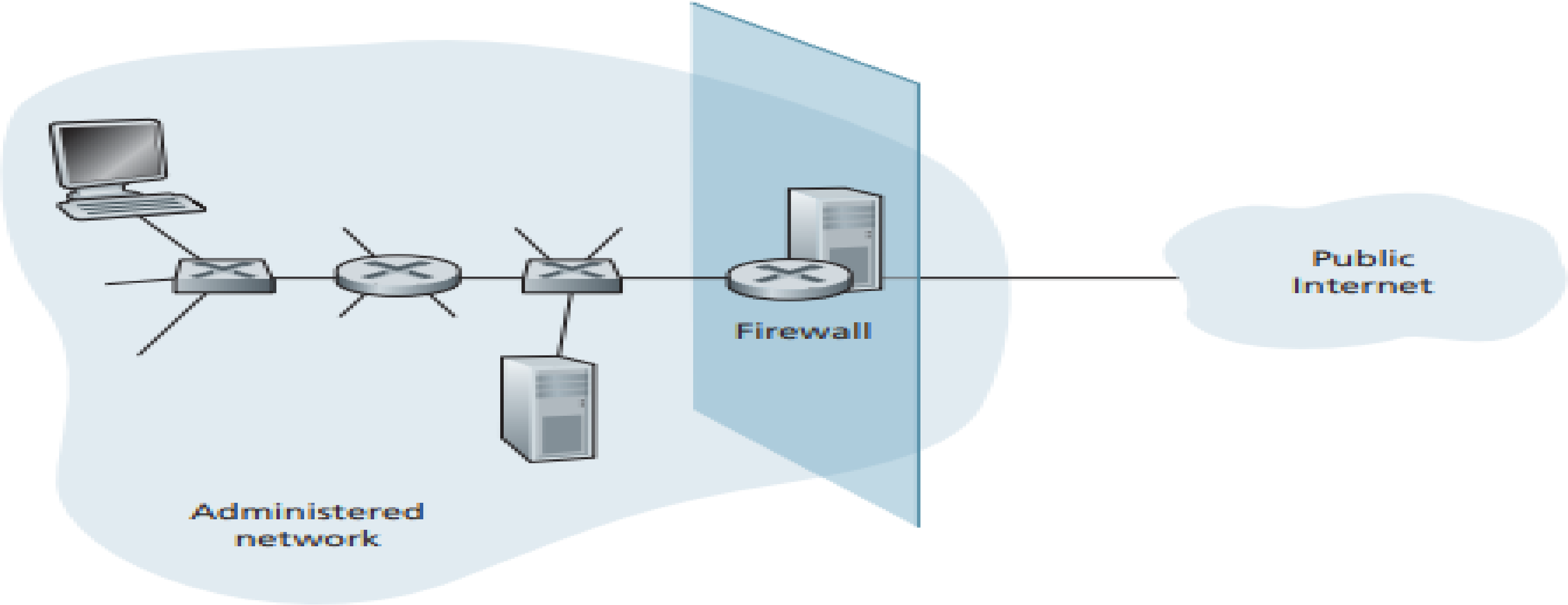


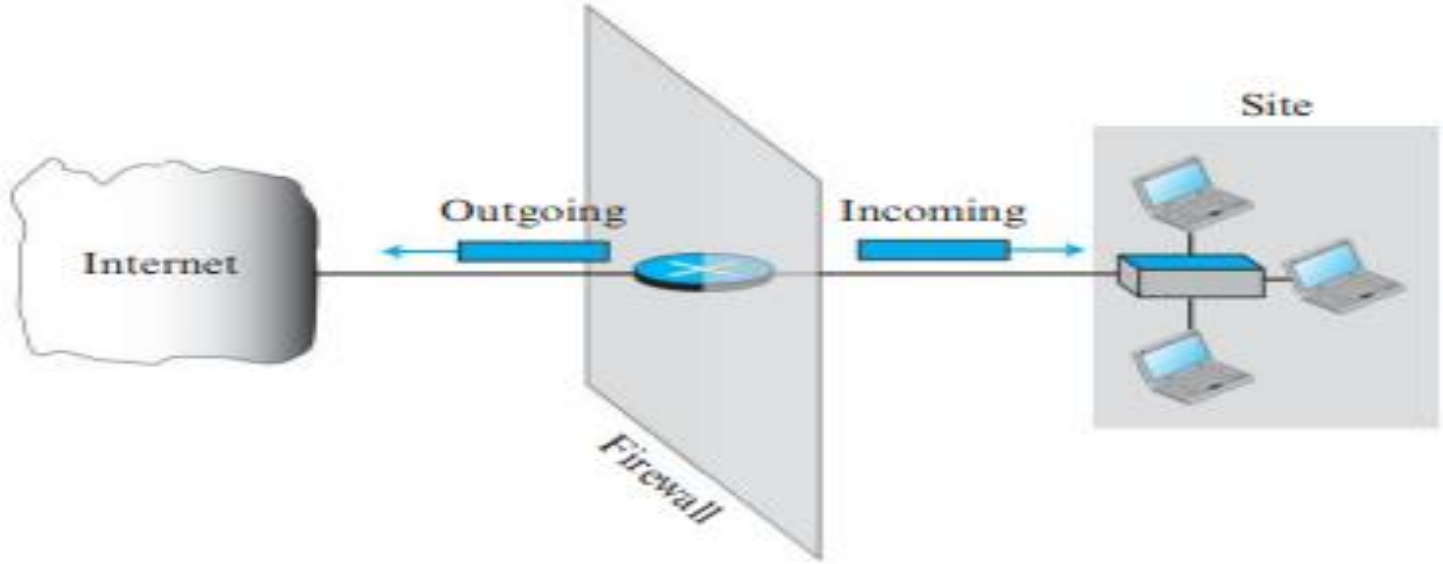
Figure 8.33 ♦ Firewall placement between the administered network and the outside world

James F Kurose and Keith W Ross, “Computer Networking: A Top - Down Approach”, Pearson Education; 6 th Edition (2017)

FIREWALLS

- A firewall is a device (usually a router or a computer) installed between the internal network of an organization and the rest of the Internet.
- It is designed to forward some packets and filter (not forward) others.

Figure 10.60 *Firewall*

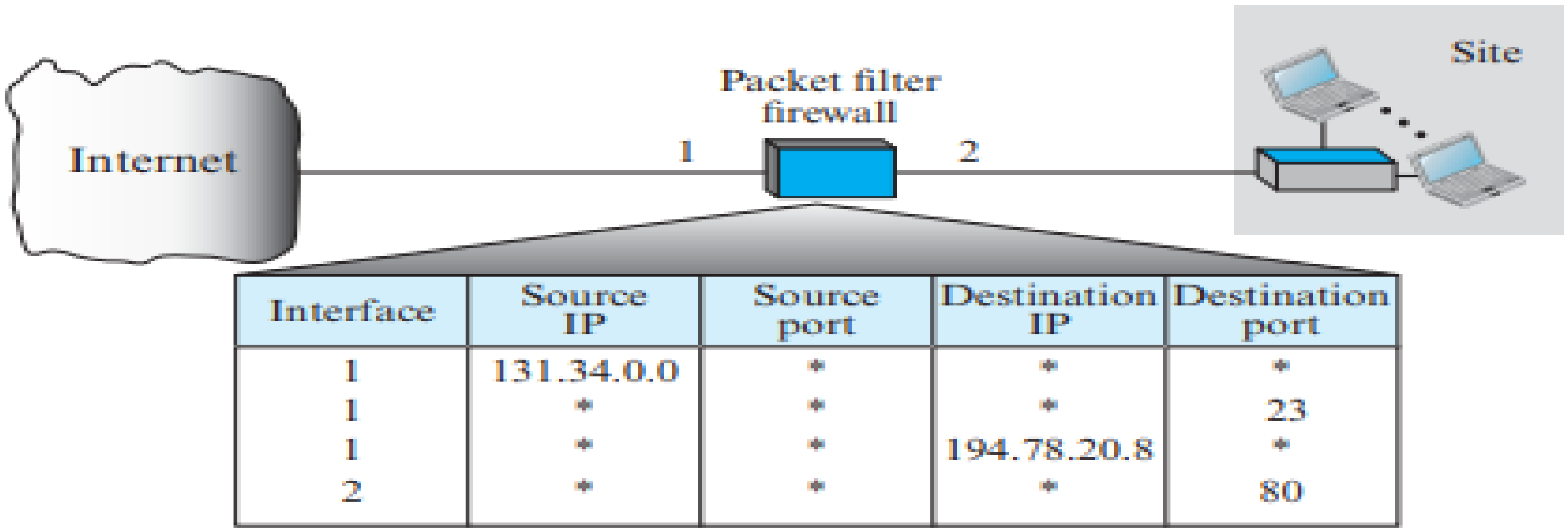


[Behrouz A Forouzan, Firouz Mosharraf, “Computer Networks: A top down Approach”, McGraw Hill Education]

FIREWALLS

- A firewall is usually classified as a packet-filter firewall or a proxy-based firewall
- Packet-Filter Firewall
- A packet-filter firewall is a router that uses a filtering table to decide which packets must be discarded (not forwarded).

Figure 10.61 *Packet-filter firewall*



Interface	Source IP	Source port	Destination IP	Destination port
1	131.34.0.0	*	*	*
1	*	*	*	23
1	*	*	194.78.20.8	*
2	*	*	*	80

[Behrouz A Forouzan, Firouz Mosharraf, "Computer Networks: A top down Approach", McGraw Hill Education]

FIREWALLS

- Packet-Filter Firewall

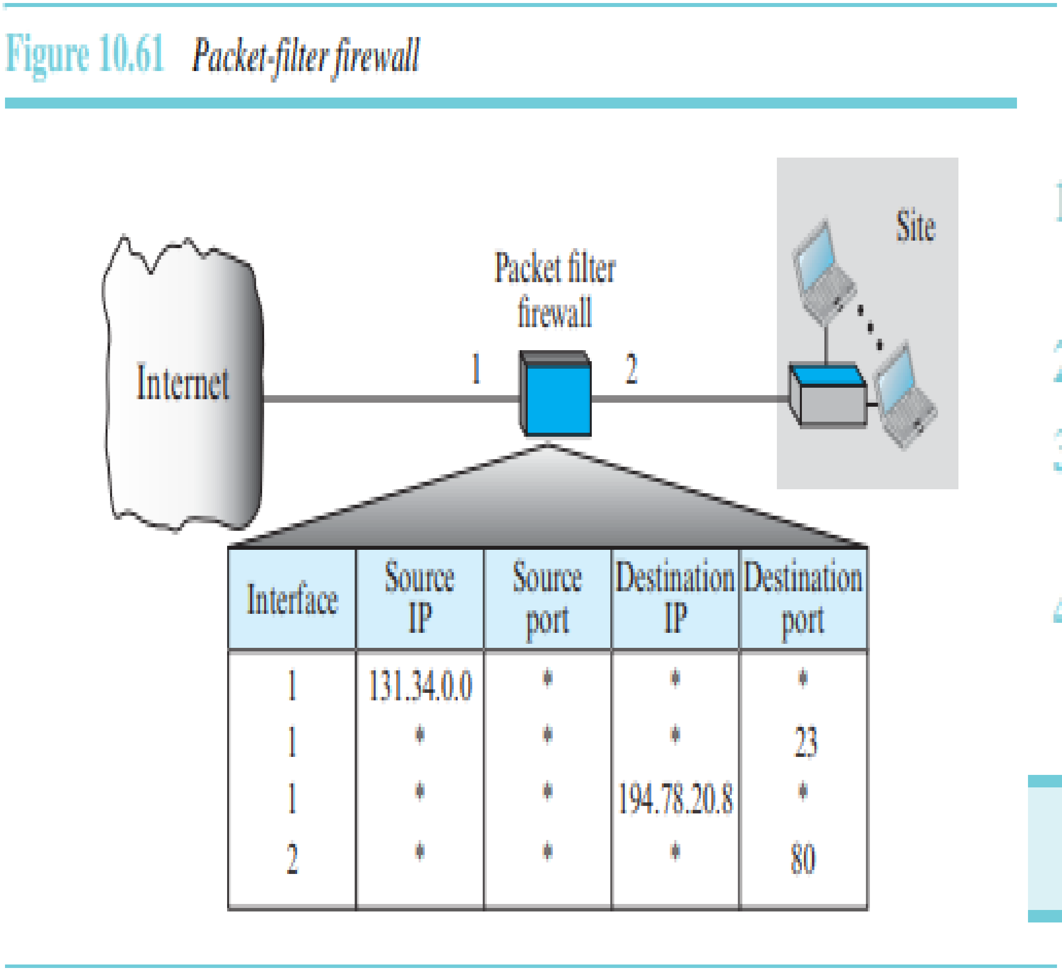
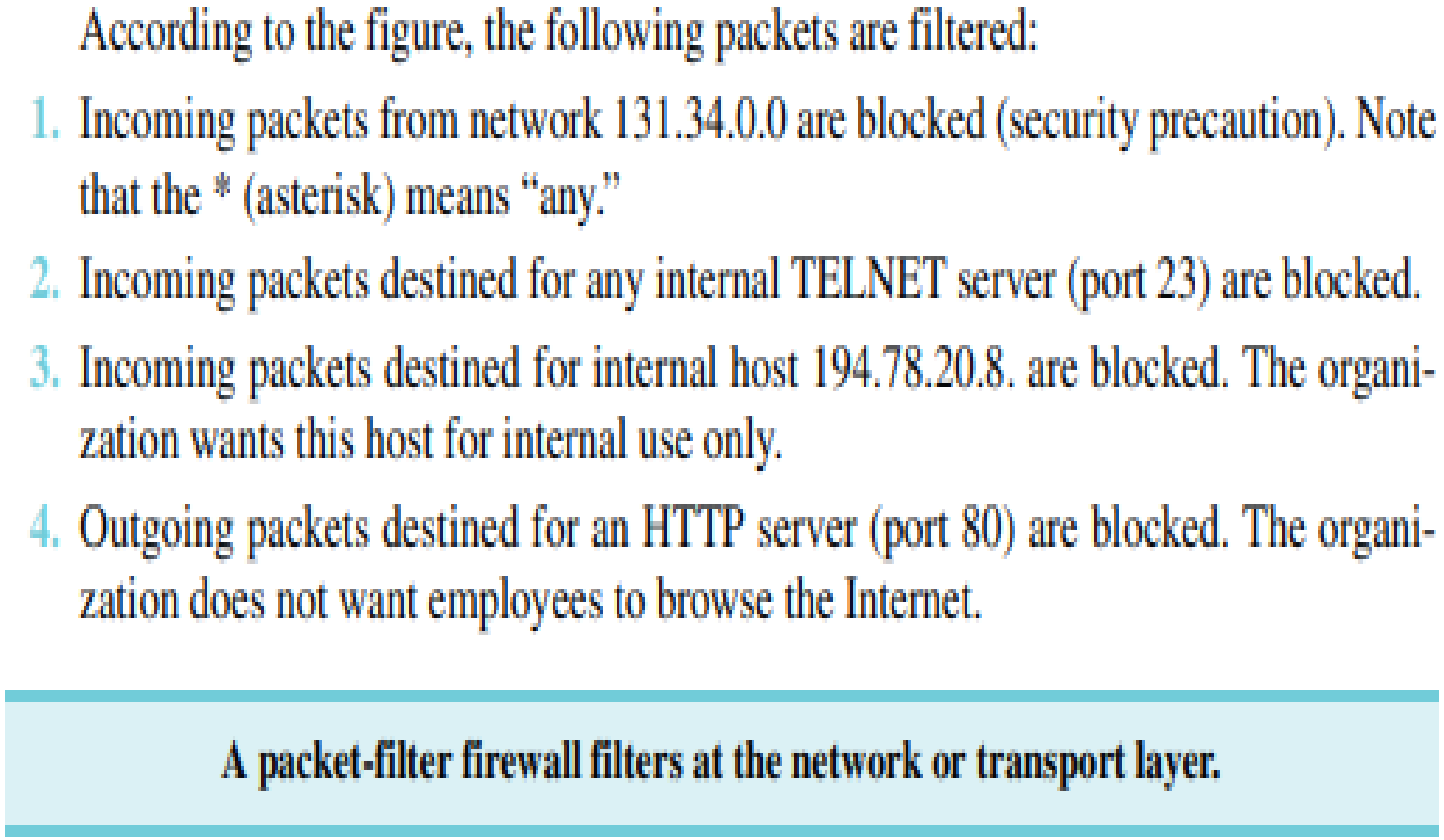


Figure 10.61 *Packet-filter firewall*

Interface	Source IP	Source port	Destination IP	Destination port
1	131.34.0.0	*	*	*
1	*	*	*	23
1	*	*	194.78.20.8	*
2	*	*	*	80



According to the figure, the following packets are filtered:

1. Incoming packets from network 131.34.0.0 are blocked (security precaution). Note that the * (asterisk) means "any."
2. Incoming packets destined for any internal TELNET server (port 23) are blocked.
3. Incoming packets destined for internal host 194.78.20.8. are blocked. The organization wants this host for internal use only.
4. Outgoing packets destined for an HTTP server (port 80) are blocked. The organization does not want employees to browse the Internet.

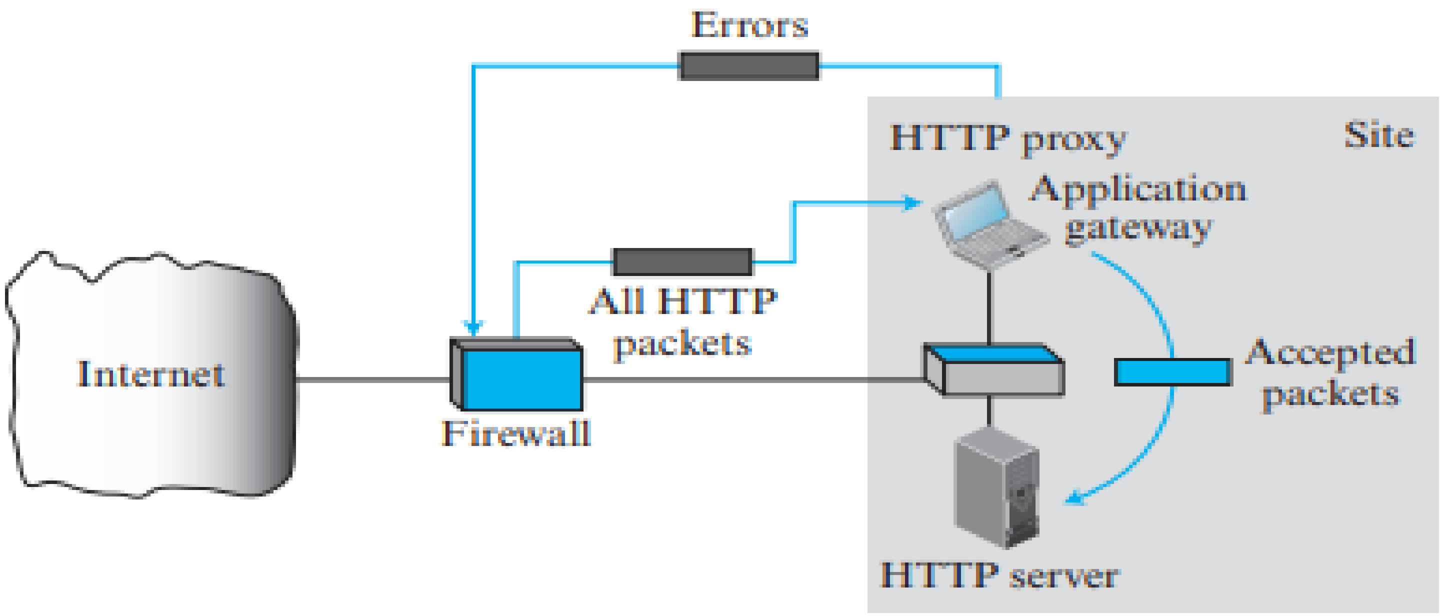
A packet-filter firewall filters at the network or transport layer.

[Behrouz A Forouzan, Firouz Mosharraf, "Computer Networks: A top down Approach", McGraw Hill Education]

FIREWALLS

- Proxy Firewall

Figure 10.62 *Proxy firewall*



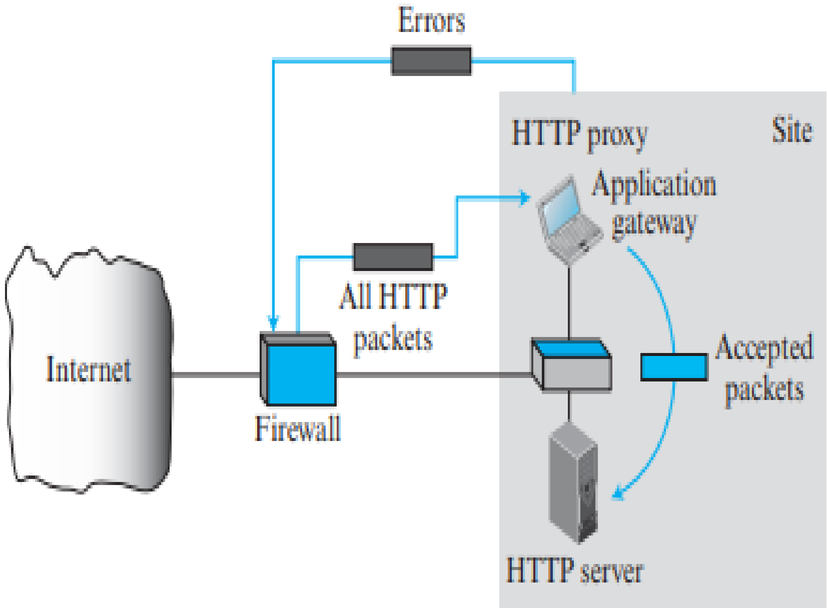
A proxy firewall filters at the application layer.

[Behrouz A Forouzan, Firouz Mosharraf, “Computer Networks: A top down Approach”, McGraw Hill Education]

FIREWALLS

- Proxy Firewall

Figure 10.62 *Proxy firewall*



A proxy firewall filters at the application layer.

- A proxy computer (sometimes called an application gateway), which stands between the customer computer and the corporation computer.
- When the user client process sends a message, the application gateway runs a server process to receive the request.
- The server opens the packet at the application level and finds out if the request is legitimate.
- If it is, the server acts as a client process and sends the message to the real server in the corporation.
- If it is not, the message is dropped and an error message is sent to the external user.
- In this way, the requests of the external users are filtered based on the contents at the application layer

[Behrouz A Forouzan, Firouz Mosharraf, "Computer Networks: A top down Approach", McGraw Hill Education]

THREATS AND ATTACKS

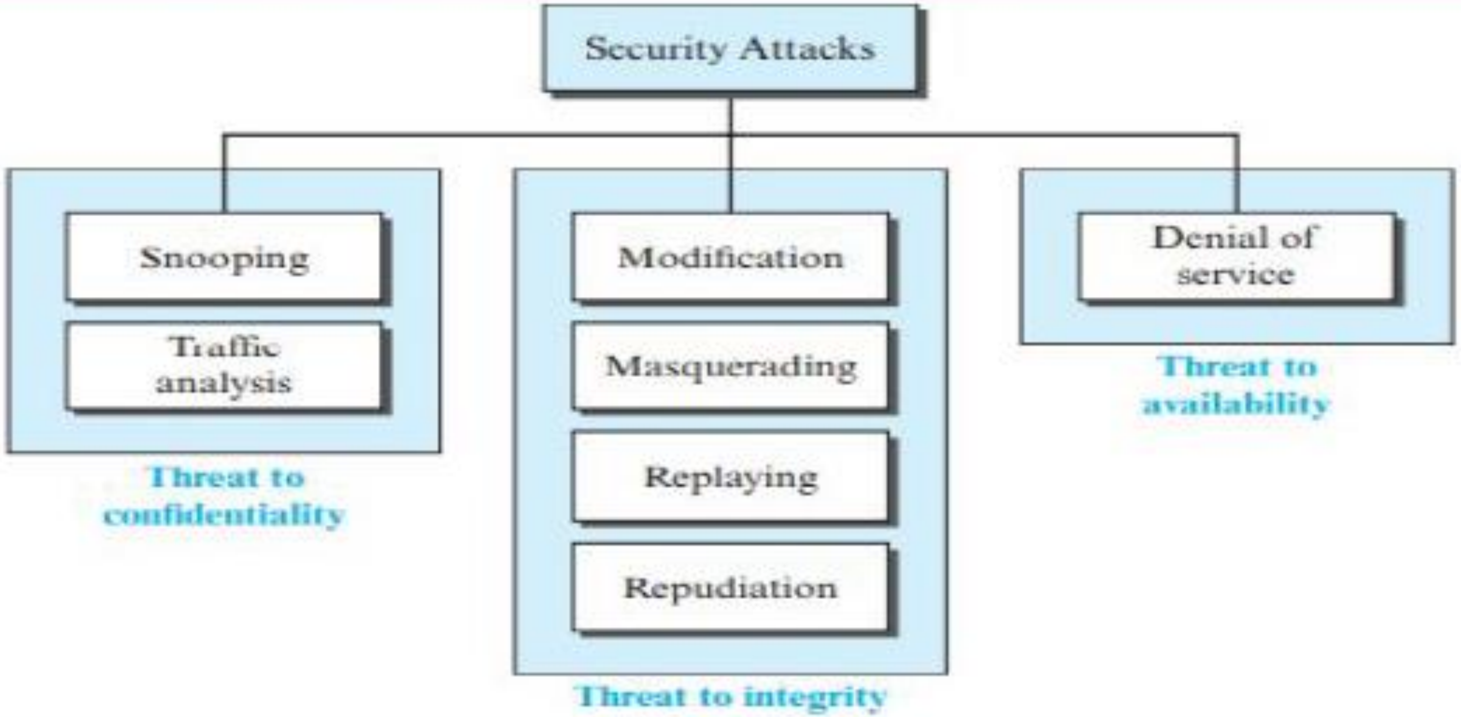
Network security

- Our three goals of security are
  - Confidentiality: for achieving this, we need to conceal it during transmission.
  - Integrity: changes need to be done only by authorized entities and through authorized mechanisms.
  - Availability: The information created and stored by an organization needs to be available to authorized entities

Attacks

- Our three goals of security —confidentiality, integrity, and availability —can be threatened by security attacks.

Figure *Taxonomy of attacks with relation to security goals*



[Behrouz A Forouzan, Firouz Mosharraf, “Computer Networks: A top down Approach”, McGraw Hill Education]

I) Attacks Threatening Confidentiality:

- the two types of attacks that threatens the confidentiality of information are snooping and traffic analysis.
- **Snooping:**
  - It refers to unauthorized access to or interception of data.
  - To prevent snooping, we can encrypt the data so that it is not understandable to the interceptor.
- **Traffic Analysis:**
  - by monitoring online traffic, the interceptor can find the e-mail address of the sender or the receiver. He can also collect pairs of requests and responses to help him guess the nature of the transaction.

ii) Attacks Threatening Integrity:

- The integrity of data can be threatened by several kinds of attacks: modification, masquerading replaying, and repudiation.
- **Modification:**
    - After accessing information, the attacker modifies the information like deleting or delaying the message to harm the system or to benefit from it.
- **Masquerading:**
    - Masquerading, or spoofing, happens when the attacker impersonates somebody else.
    - For example, a user tries to contact a bank, but another site pretends that it is the bank and obtains some information from the user.
- **Replaying:**
    - The attacker obtains a copy of a message sent by a user and later tries to replay it.
- **Repudiation:**
    - Such attack is performed by one of the two parties in the communication: the sender or the receiver. The sender of the message might later deny that she has sent the message; the receiver of the message might later deny that he has received the message.

iii) Attacks Threatening Availability:

- **Denial of Service:**
    - It may slow down or totally interrupt the service of a system.
    - The attacker might send so many bogus requests to a server that the server crashes because of the heavy load. Or
    - The attacker might intercept and delete a server’s response to a client, making the client believe that the server is not responding.

Overview of tools and troubleshooting

- Network troubleshooting tools are standalone or integrated solutions that help network administrators identify the root cause of a network issue in order to fix it.
- These network troubleshooting tools range from simple command line based troubleshooting utilities to more comprehensive and robust solutions that allows for a systematic, efficient and proactive approach to network troubleshooting.
- There are many programs and utilities available for Windows and UNIX operating systems that allow us to sniff, capture, trace, and analyze packets that are exchanged between our computer and the Internet.

- Sniffing is a process of monitoring and capturing all data packets passing through given network.
- Sniffers are used by network/system administrator to monitor and troubleshoot network traffic.
- Attackers use sniffers to capture data packets containing sensitive information such as password, account information etc.
- Some of these, such as Wireshark and Ping Plotter have graphical user interface (GUI); others, such as traceroute, nslookup, dig, ipconfig, and ifconfig, are network administration command-line utilities.
- Any of these programs and utilities can be a valuable debugging tool for network administrators.

Some of the basic network troubleshooting tools are as follows:

- Ping
- Tracert/ Trace Route
- Ipconfig/ ifconfig
- Netstat
- Nslookup
- Pathping/MTR
- Route
- PuTTY

- One of the tools that a host can use to test the liveliness of another host is the **ping** program. The **ping** program can also measure the reliability and congestion of the router. Ping can calculate the round-trip time.

- The **traceroute** program in UNIX or tracert in Windows can be used to trace the path of a packet from a source to the destination. It can find the IP addresses of all the routers that are visited along the path. The program is usually set to check for the maximum of 30 hops (routers) to be visited.

- **ipconfig** is a console application program of some computer operating systems that displays all current TCP/IP network configuration values. **ifconfig**(interface configuration) command is used to configure the kernel resident network interfaces. It is used at the boot time to set up the interfaces as necessary. Also, this command is used to assign the IP address and netmask to an interface or to enable or disable a given interface.

- The **network statistics (netstat)** command is a networking tool used for troubleshooting and configuration, that can also serve as a monitoring tool for connections over the network. Both incoming and outgoing connections, routing tables, port listening, and usage statistics are common uses for this command.

- **nslookup** is a network administration command-line tool available for many computer operating systems for querying the Domain Name System (DNS) to obtain domain name or IP address mapping.

- The **PathPing** command is a command-line network utility supplied in Windows 2000 and beyond that combines the functionality of ping with that of tracert. It is used to locate spots that have network latency and network loss.

- **Route** is a command used to view and manipulate the IP routing table.

- **PuTTY** is a free and open-source terminal emulator, serial console and network file transfer application. It supports several network protocols, including SCP, SSH, Telnet, rlogin, and raw socket connection.

- The **echo request and the echo reply** pair of messages are used by a host or a router to test the liveliness of another host or router.

- The **timestamp request and the timestamp reply** pair of messages are used to find the round-trip time between two devices or to check whether the clocks in two devices are synchronized.

Traffic Analysis

Network Analysis and Sniffing

-It is the process of capturing, decoding, and analyzing network traffic.

- Why is the network slow?
- What is the network traffic pattern?
- How is the traffic being shared between nodes?

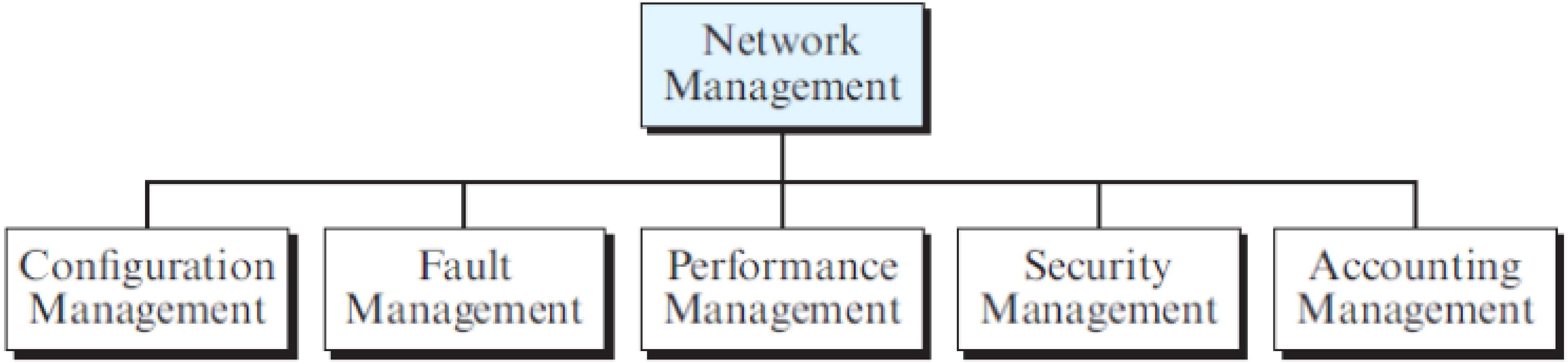
- Also known as traffic analysis, protocol analysis, sniffing, packet analysis etc.

Network Analyzer

- A combination of hardware and software tools that can detect, decode, and manipulate traffic on the network
- Available both free and commercially
- Mainly software-based (utilizing OS and NIC)
- Also known as sniffer
- A program that monitors the data traveling through the network passively

- Wireshark captures live packet data from a network interface and displays them with detailed protocol information.
- Wireshark, is a passive analyzer.
- It only "measures" things from the network without manipulating them; it does not send packets on the network or do other active operations.

Configuration Management



- A large network is usually made up of hundreds of entities that are physically or logically connected to each other.
- These entities have an initial configuration when the network is set up, but can change with time.
- Desktop computers may be replaced by others; application software may be updated to a newer version; and users may move from one group to another.
- The configuration management system must know, at any time, the status of each entity and its relation to other entities.
- Configuration management can be divided into two subsystems: reconfiguration and documentation.

Reconfiguration

- Reconfiguration can be a daily occurrence in a large network. There are three types of reconfiguration: hardware reconfiguration, software reconfiguration, and user-account reconfiguration.
- Hardware reconfiguration covers all changes to the hardware.
- For example, a desktop computer may need to be replaced. A router may need to be moved to another part of the network. A subnetwork may be added or removed from the network.
- All of these need the time and attention of network management.
- In a large network, there must be specialized personnel trained for quick and efficient hardware reconfiguration.
- Unfortunately, this type of reconfiguration cannot be automated and must be manually handled.

- Software reconfiguration covers all changes to the software. For example, new software may need to be installed on servers or clients. An operating system may need updating.
- Fortunately, most software reconfiguration can be automated. For example, an update for an application on some or all clients can be electronically downloaded from the server.
- User-account reconfiguration is not simply adding or deleting users on a system. We must also consider the user privileges, both as an individual and as a member of a group.
- For example, a user may have both read and write permission with regard to some files, but only read permission with regard to other files.
- User-account reconfiguration can be, to some extent, automated.

Documentation

- The original network configuration and each subsequent change must be recorded meticulously.
- This means that there must be documentation for hardware, software, and user accounts.
- Hardware documentation normally involves two sets of documents: maps and specifications.
- Maps track each piece of hardware and its connection to the network.
- There can be one general map that shows the logical relationships between subnetworks.
- There can also be a second general map that shows the physical location of each subnetwork.
- For each subnetwork, then, there is one or more maps that show all pieces of equipment.

- There must be a set of specifications for each piece of hardware connected to the network.
- These specifications must include information such as hardware type, serial number, vendor (address and phone number), time of purchase, and warranty information.
- All software must also be documented. Software documentation includes information such as the software type, the version, the time installed, and the license agreement.
- Most operating systems have a utility that allows user account documentation.
- The management must make sure that the files with this information are updated and secured.
- Some operating systems record access privileges in two documents; one shows all files and access types for each user; the other shows the list of users that have access to a particular file.