Module-5

Wireless and Cellular networks:

- IEEE 802.11 Wi-Fi, Bluetooth, and cellular networks;
- Threats and attacks.
- Network Address Translation.
- Firewalls, VPNs.
- Introduction to network management, SNMP.

IEEE 802.11 WIFI

WIRELESS LANs

- Connecting devices without the use of cables.
- *Architectural Comparison:*
- Medium
  - Wired LAN- use wires to connect hosts.
  - In a switched LAN, with a link-layer switch, the communication between the hosts is point to- point and full-duplex (bidirectional).
  - Wireless LAN, the medium is air, the signal is generally broadcast
- Hosts
  - Wired LAN- A host is always physically connected to its network at a point with a fixed linklayer address related to its network interface card (NIC).
  - A host is not physically connected to the network; it can move freely and can use the services provided by the network.

Isolated LANs

i. A wired isolated LAN is a set of hosts connected via a link-layer switch.

ii. A wireless isolated LAN, called an ad hoc network in wireless LAN terminology, is a set of hosts that communicate freely with each other.

Connection to Other Networks

- A wired LAN can be connected to another network or an internetwork such as the Internet using a router.
- A wireless LAN may be connected to a wired infrastructure network, to a wireless infrastructure network, or to another wireless LAN

Figure 6.1 *Isolated LANs: wired versus wireless*

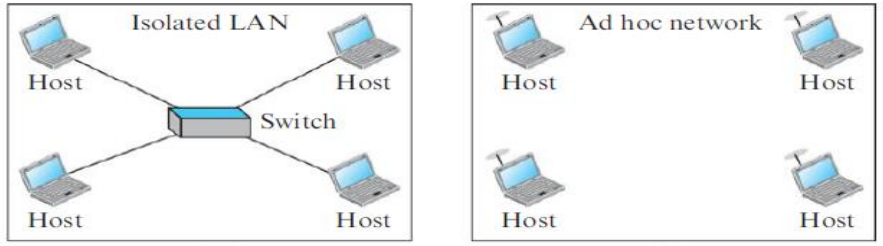


Figure 6.1 *Isolated LANs: wired versus wireless*

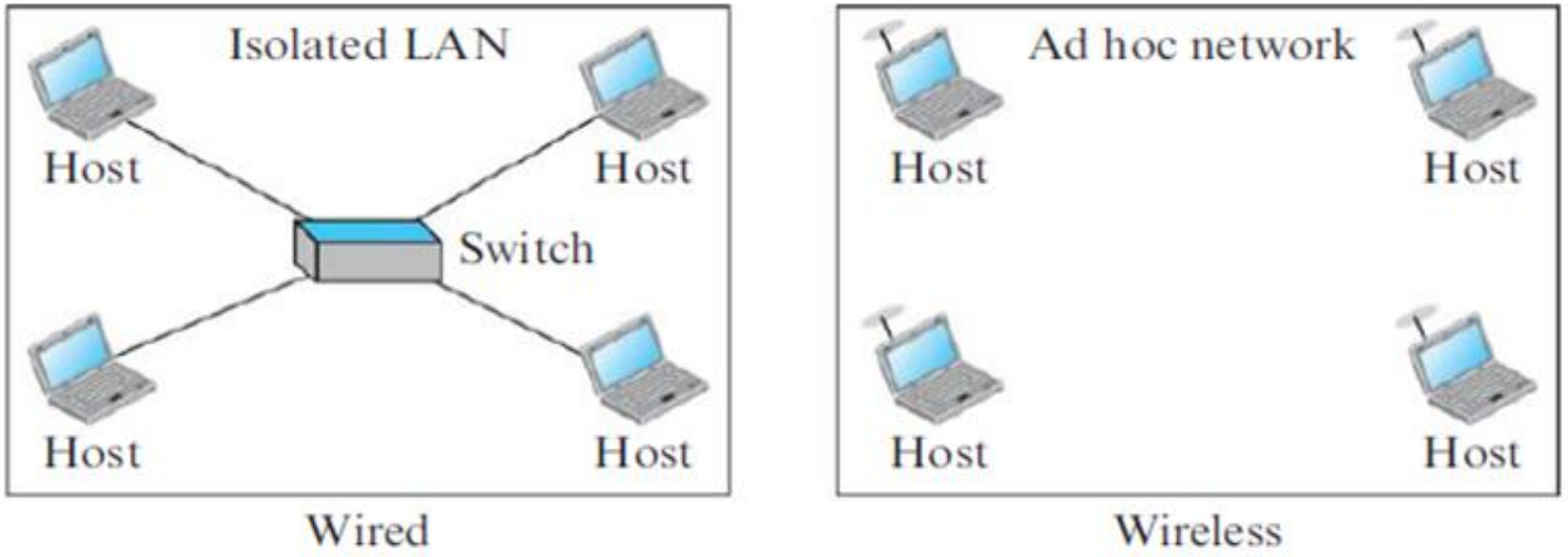
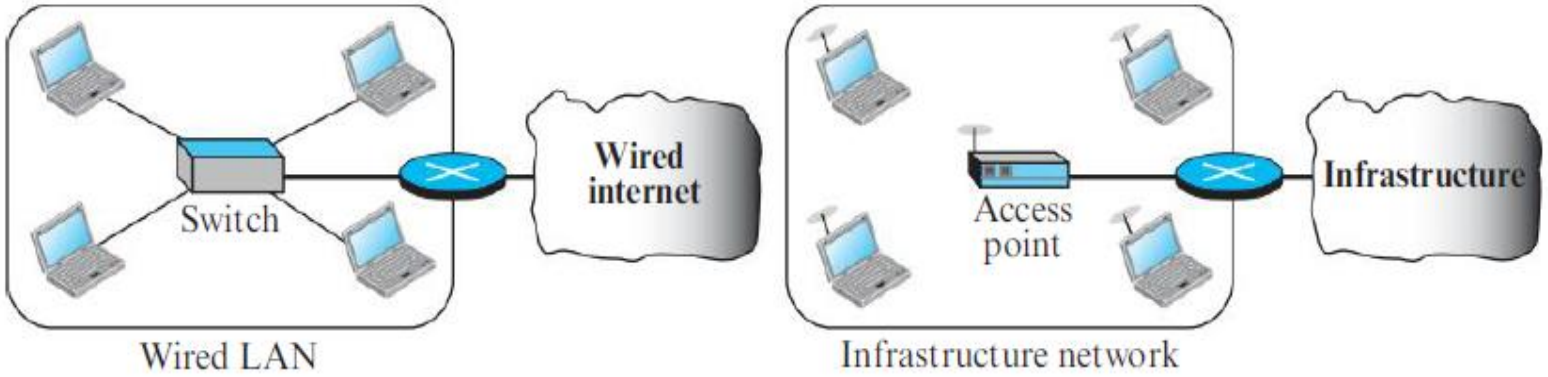


Figure 6.2 *Connection of a wired LAN and a wireless LAN to other networks*



In this case, the wireless LAN is referred to as an infrastructure network, and the connection to the wired infrastructure, such as the Internet, is done via a device called an access point (AP).

Characteristics

Attenuation

- The strength of electromagnetic signals decreases rapidly because the signal disperses in all directions; only a small portion of it reaches the receiver.

Interference:

- Another issue is that a receiver may receive signals not only from the intended sender, but also from other senders if they are using the same frequency band.

Multipath Propagation

- A receiver may receive more than one signal from the same sender because electromagnetic waves can be reflected back from obstacles such as walls, the ground, or objects.
- The result is that the receiver receives some different signals at different phases.

Signal to Noise ratio

- If SNR is high, it means that the signal is stronger than the noise (unwanted signal), so we may be able to convert the signal to actual data.
- When SNR is low, it means that the signal is corrupted by the noise and the data cannot be recovered.

Access Control

The CSMA/CD algorithm does not work in wireless LAN for three reasons:

1. To detect a collision, a host needs to do work in a duplex mode. Wireless hosts do not have enough power to do so.

2. A station may not be aware of another station's transmission due to some obstacles or range problems, collision may occur but not be detected.

3. Signal fading could prevent a station at one end from hearing a collision at the other end.

To overcome the above three problems Carrier Sense Multiple Access with Collision Avoidance (CSMA/CA) was invented for wireless LAN

IEEE 802.11 Project

- IEEE has defined the specifications for a wireless LAN, called IEEE 802.11,
- The public uses the term WiFi (wireless fidelity) as a synonym for wireless LAN

Architecture

The standard defines two kinds of services: the basic service set (BSS) and the extended service set (ESS).

- **Basic Service Set (BSS)**
- Wireless LAN is established using a central device called an Access Point that centralizes access and control over a group of wireless devices.
- All wireless devices do not communicate directly with each other but instead they communicate with the AP, and the AP forwards the frames to the destination stations.

- Extended Service Set (ESS) is created by connecting multiple Basic Service Set (BSS) via a distribution system.

- Two or more Access Points are connected to the same Local Area Network to provide a larger coverage area which allows the client to move from one AP to another AP and still be the part of the LAN.

- The wireless coverage area created by joining two or more Access Points via distribution system is called an Extended Service Area (ESA).

Figure below show a Basic Service Set on left side and an Extended Service Set on the right side.

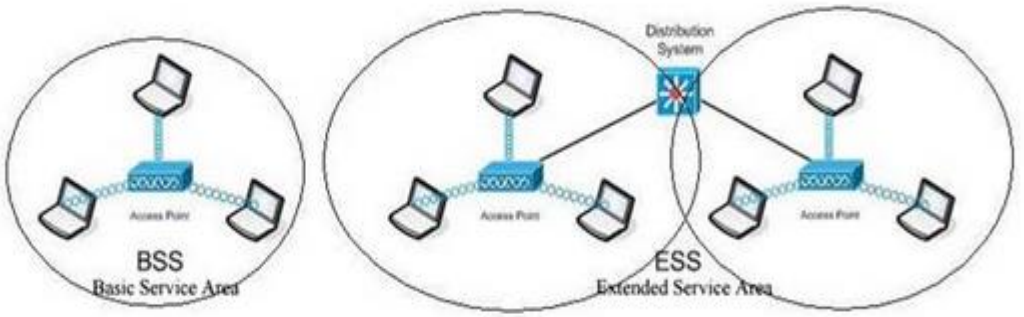


Figure 6.4 *Basic service sets (BSSs)*

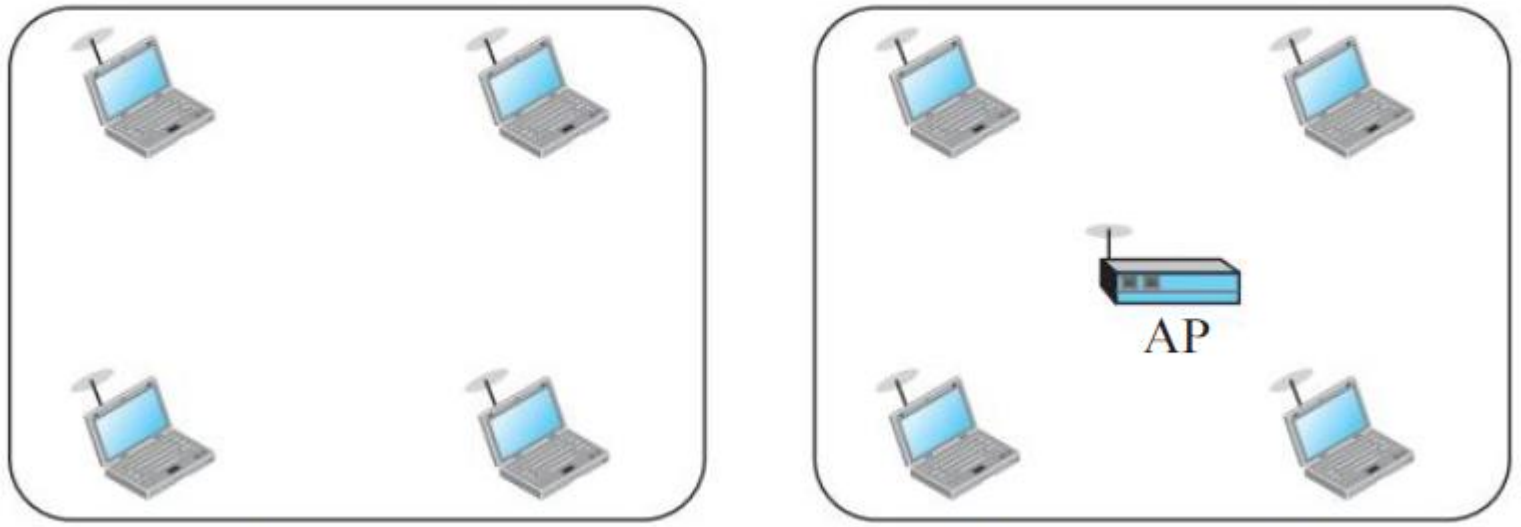
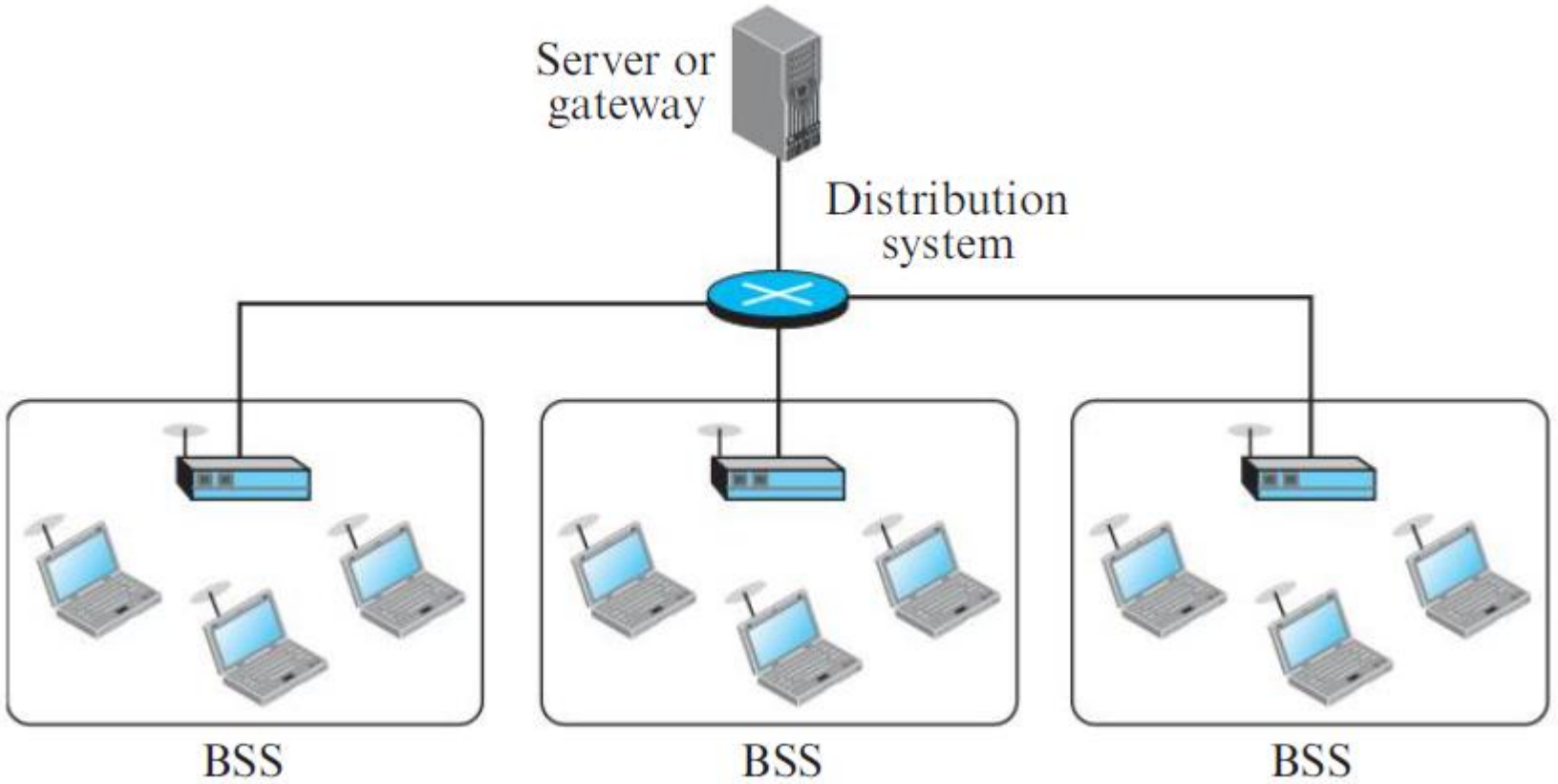
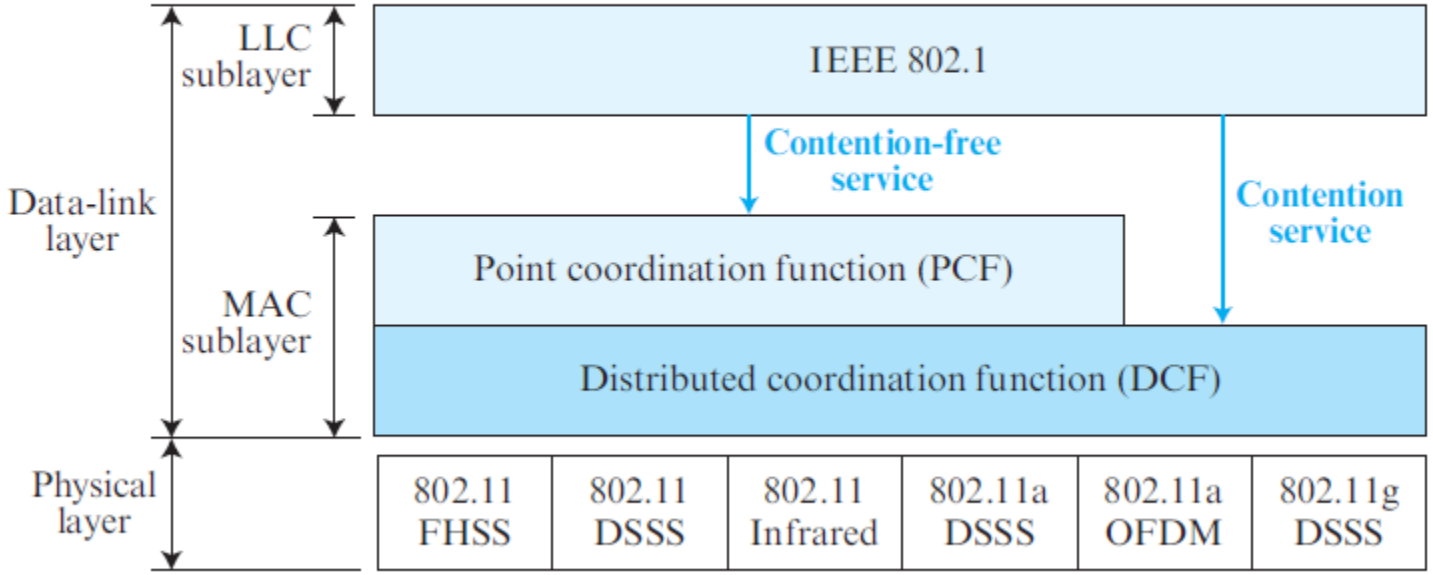


Figure 6.5 *Extended service set (ESS)*



MAC Sublayer

Figure 6.6 *MAC layers in IEEE 802.11 standard*



MAC Sublayer

- IEEE 802.11 defines two MAC sublayers:
  i. Distributed Coordination Function (DCF) and
  ii. Point Coordination Function (PCF).

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.
- CSMA/CA
- Since we need to avoid collisions on wireless networks because they cannot be detected, carrier sense multiple access with collision avoidance (CSMA/CA) was invented for this network.
- Collisions are avoided through the use of CSMA/CA's three strategies:
  i. the interframe space,
  ii. the contention window, and
  iii. acknowledgments

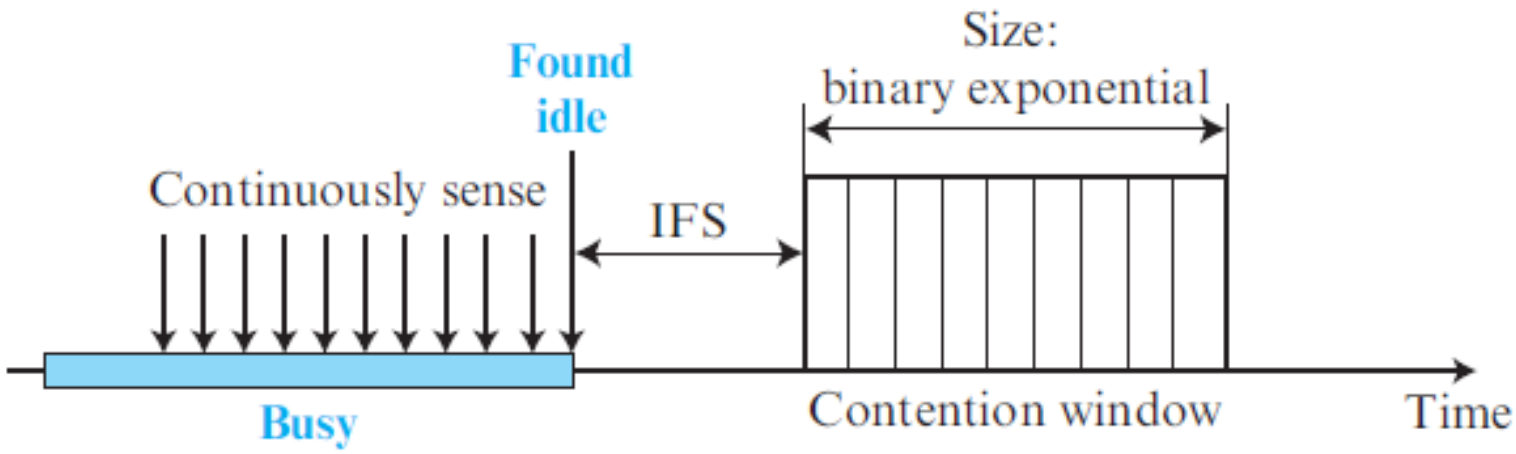
Interframe Space (IFS).

- First, collisions are avoided by deferring transmission even if the channel is found idle. When an idle channel is found, the station does not send immediately. It waits for a period of time called the interframe space or IFS.
- Even though the channel may appear idle when it is sensed, a distant station may have already started transmitting.
- The distant station's signal has not yet reached this station.
- The IFS time allows the front of the transmitted signal by the distant station to reach this station. After waiting an IFS time, if the channel is still idle, the station can send, but it still needs to wait a time equal to the contention time.

Contention Window.

- The contention window is an amount of time divided into slots.
- A station that is ready to send chooses a random number of slots as its waittime.
- The number of slots in the window changes according to the binary exponential back-off strategy.
- This means that it is set to one slot the first time and then doubles each time the station cannot detect an idle channel after the IFS time
- One interesting point about the contention window is that the station needs to sense the channel after each time slot.
- However, if the station finds the channel busy, it does not restart the process; it just stops the timer and restarts it when the channel is sensed as idle. This gives priority to the station with the longest waiting time.

Figure 6.8 *Contention window*



Acknowledgment.

- The positive acknowledgment and the time-out timer can help guarantee that the receiver has received the frame.

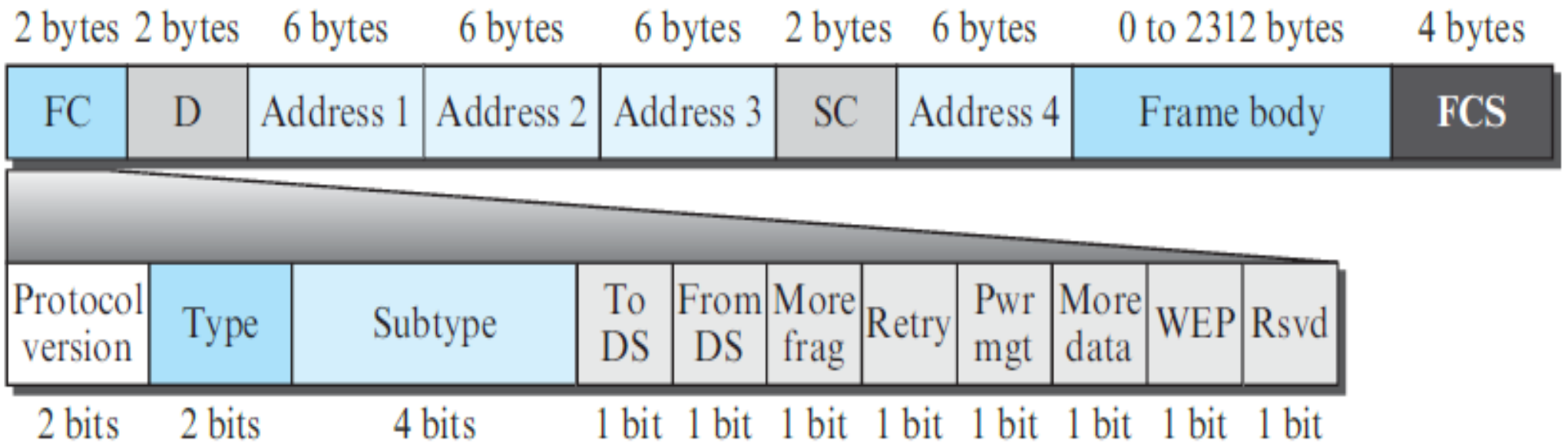
Point Coordination Function (PCF)

- 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.
- PCF has a centralized, contention-free polling access method.
- The AP performs polling for stations that are capable of being polled.
- The stations are polled one after another, sending any data they have to the AP.

MAC Frame: IEEE 802.11 FRAME FORMAT

The MAC layer frame consists of 9 fields.

Figure 6.11 *Frame format*



- **Frame Control(FC):**
- It is 2 bytes long field which defines type of frame and some control information. Various fields present in FC are:

i. **Version:**It is a 2 bit long field which indicates the current protocol version which is fixed to be 0 for now.

ii. **Type:** It is a 2 bit long field which determines the function of frame;
   - i.e management(00), control(01) or data(10). The value 11 is reserved.

iii. **Subtype:** It is a 4 bit long field which indicates sub-type of the frame ;
   - like 0000 → association request, 1000 → beacon.

iv. **To DS:** It is a 1 bit long field which when set indicates that destination frame is for DS(distribution system).

v. From DS: It is a 1 bit long field which when set indicates frame coming from DS.

vi. More frag (More fragments): It is 1 bit long field which when set to 1 means frame is followed by other fragments.

vii. Retry: It is 1-bit long field, if the current frame is a retransmission of an earlier frame, this bit is set to 1.

viii. Power Mgmt (Power management): It is 1-bit long field that indicates the mode of a station after successful transmission of a frame.

- Set to 1 the field indicates that the station goes into power-save mode.
- If the field is set to 0, the station stays active.

ix. More data: It is 1-bit long field that is used to indicate receiver that a sender has more data to send than the current frame. This can be used by an access point to indicate to a station in power-save mode that more packets are buffered or it can be used by a station to indicate to an access point after being polled that more polling is necessary as the station has more data ready to transmit.

x. WEP: It is 1 bit long field which indicates that the standard security mechanism of 802.11 is applied.

xi. Rsvd: Reserved bit

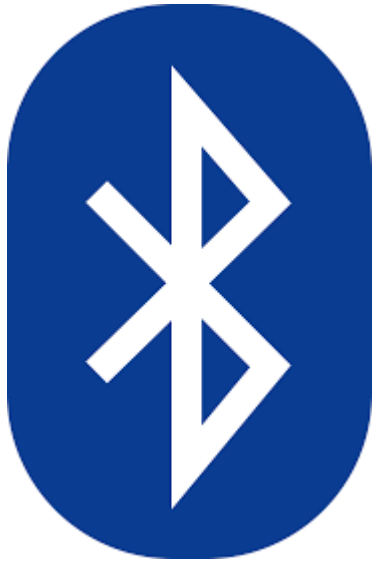
IEEE 802.11 FRAME FORMAT

- Duration/ID – It is 4 bytes long field which contains the value indicating the period of time in which the medium is occupied(in µs).
- Address 1 to 4 – These are 6 bytes long fields which contain standard IEEE 802 MAC addresses (48 bit each). The meaning of each address depends on the DS bits in the frame control field.
- SC (Sequence control) – It is 16 bits long field which consists of 2 sub-fields, i.e., Sequence number (12 bits) and Fragment number (4 bits). Since acknowledgement mechanism frames may be duplicated hence, a sequence number is used to filter duplicate frames.
- Data – It is a variable length field which contain information specific to individual frames which is transferred transparently from a sender to the receiver(s).
- **FCS-CRC (Cyclic redundancy check):** It is 4 bytes long field which contains a 32 bit CRC error detection sequence to ensure error free frame.

Table 6.3 *Addresses*

To DS	*From DS*	*Address 1*	*Address 2*	*Address 3*	*Address 4*
0	0	Destination	Source	BSS ID	N/A
0	1	Destination	Sending AP	Source	N/A
1	0	Receiving AP	Source	Destination	N/A
1	1	Receiving AP	Sending AP	Destination	Source

Bluetooth



Bluetooth

- Bluetooth is a short-range wireless technology standard that is used for exchanging data between fixed and mobile devices over short distances using UHF radio waves in the ISM bands, from **2.402 GHz to 2.480 GHz**, and building personal area networks (PANs).
- It was originally conceived as a wireless alternative to RS-232 data cables. It is mainly used as an alternative to wire connections, to exchange files between nearby portable devices and connect cell phones and music players with wireless headphones.
- In the most widely used mode, transmission power is limited to 2.5 milliwatts, giving it a very short range of up to 10 meters (30 feet).
- Today, Bluetooth technology is the implementation of a protocol defined by the **IEEE 802.15** standard.
- The standard defines a wireless personal-area network (PAN) operable in an area the size of a room or a hall.

Bluetooth-History

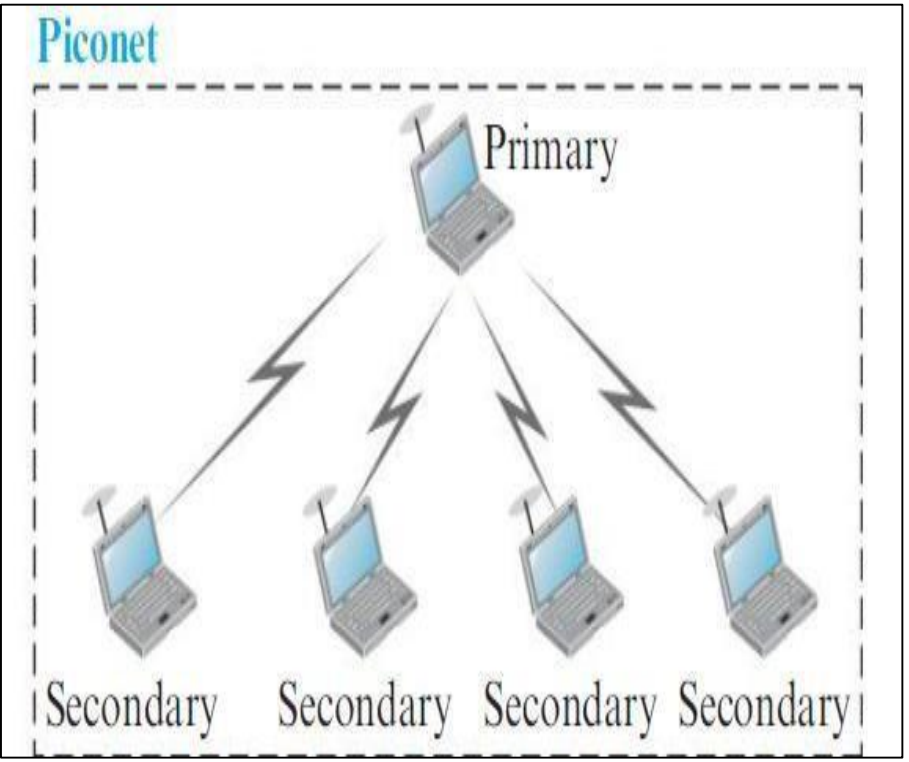
- Bluetooth was originally started as a project by the Ericsson Company.
- It is named for **Harald Blaatand,** the king of Denmark (940-981) who united Denmark and Norway.
- Blaatand translates to Bluetooth in English.
- Today, Bluetooth technology is the implementation of a protocol defined by the IEEE 802.15 standard.
- The standard defines a wireless personal-area network (PAN) operable in an area the size of a room or a hall.

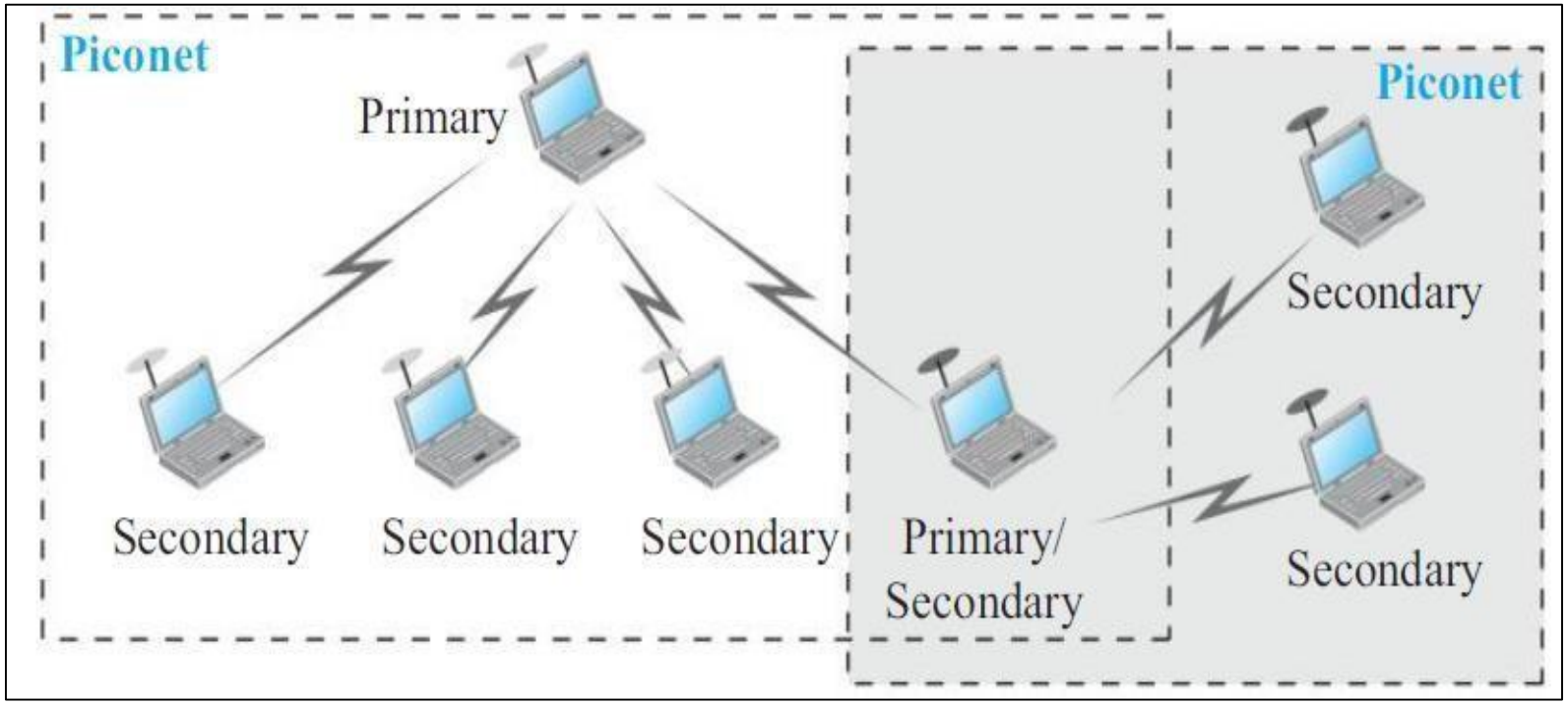
Bluetooth:

Architecture

- Bluetooth defines two types of networks:
  - **Piconet &**
  - **Scatternet.**
- **Piconets**: A Bluetooth network is called a piconet, or a small net. A piconet can have up to eight stations, one of which is called the primary;
- the rest are called secondaries.
- All the secondary stations synchronize their clocks and hopping sequence with the primary.
- A piconet can have **only one primary station**. The communication between the primary and secondary stations can be **one-to-one** or **one-to-many**
- A piconet can have a maximum of seven secondaries, additional secondaries can be in the **parked state.** A secondary in a parked state is synchronized with the primary, but cannot take part in communication until it is moved from the **parked state to the active state.** Because only eight stations can be active in a piconet, activating a station from the parked state means that an active station must go to the parked state.

Bluetooth:





Scatternet: Piconets can be combined to form what is called a scatternet. 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. A station can be a member of two piconets.

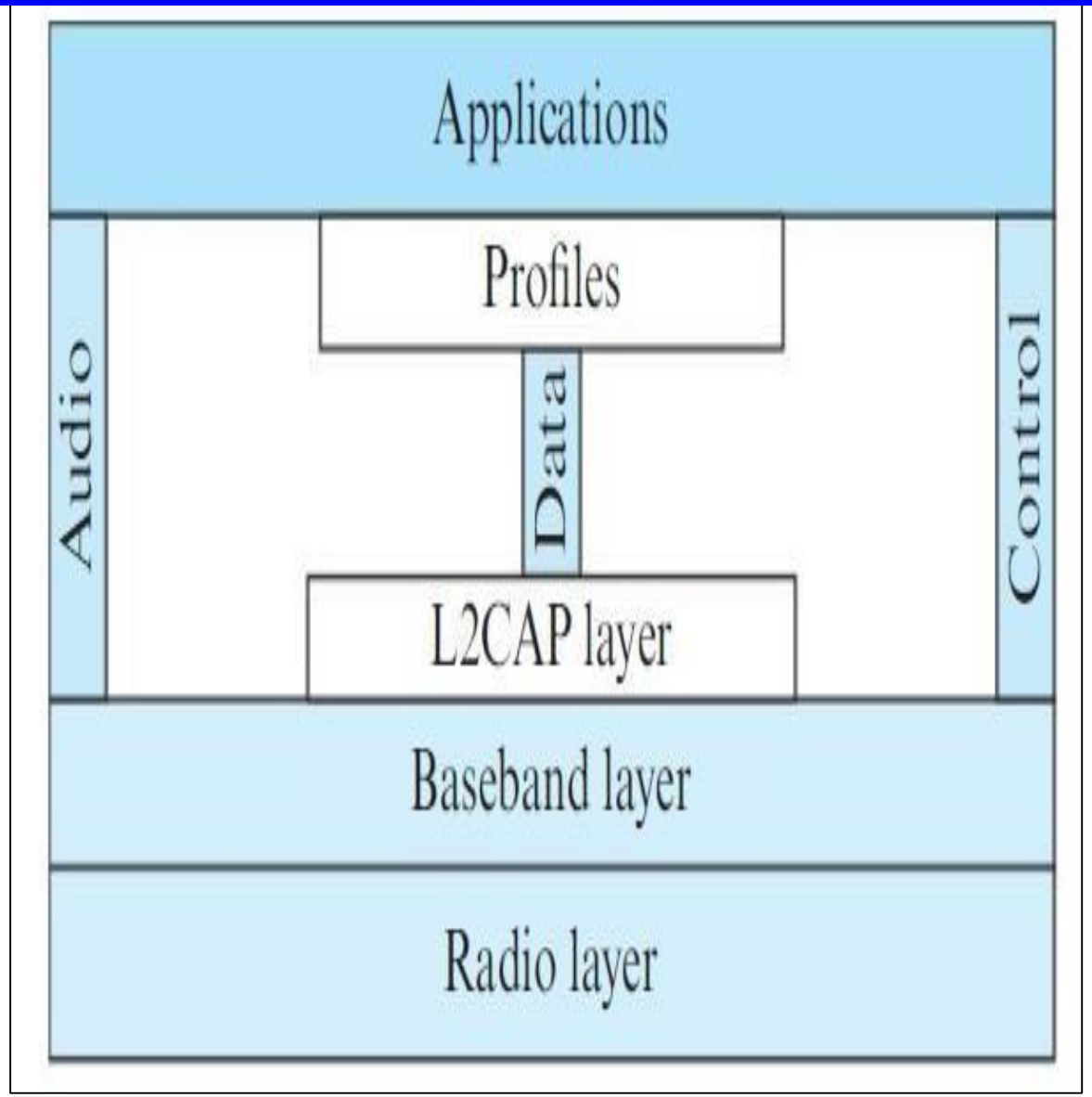
Bluetooth Layers

L2CAP: The Logical Link Control and Adaptation Protocol, or L2CAP (L2 here means LL), is roughly equivalent to the LLC sublayer in LANs. It is used for data exchange on an ACL link

The L2CAP has specific **duties:**

- multiplexing,
- segmentation
- reassembly,
- quality of service (QoS), &
- group management.

ACL→Asynchronous Connection Less Link



Bluetooth Layers

Bluetooth:

- **Multiplexing:** At the **sender site,** it accepts data from one of the upper-layer protocols, frames them, and delivers 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 layer. It creates a **kind of virtual channel.**
- **Segmentation and Reassembly:** The maximum size of the payload field in the baseband layer is 2774 bits or 343 bytes. This includes 4 bytes to define the packet and packet length. Therefore, the size of the packet that can arrive from an upper layer can only be 339 bytes. However, application layers sometimes need to send a data packet that can be up to 65,535 bytes. The **L2CAP divides these large packets into segments** and adds extra information to define the location of the segments in the original packet. The **L2CAP segments the packet at the source and reassembles them at the destination.**
- **QoS:** Bluetooth allows the stations to define a quality-of-service level.
- **Group Management:** Another functionality of L2CAP is to allow devices to create a type of logical addressing between themselves. This is similar to multicasting.

- **Baseband Layer:** The baseband layer is roughly equivalent to the MAC sublayer in LANs.
- The access method is TDMA(Time Division Multiple Access) .
- The primary and secondary stations communicate with each other using time slots. The length of a time slot is exactly the same as the dwell time, 625 µs.
  - This means that during the time that one frequency is used, a primary sends a frame to a secondary, or a secondary sends a frame to the primary.
- The communication is only between the primary and a secondary; secondaries cannot communicate directly with one another.
- In Baseband layer two types of links created between primary and secondary:
  - **SCO**
  - **ACL**

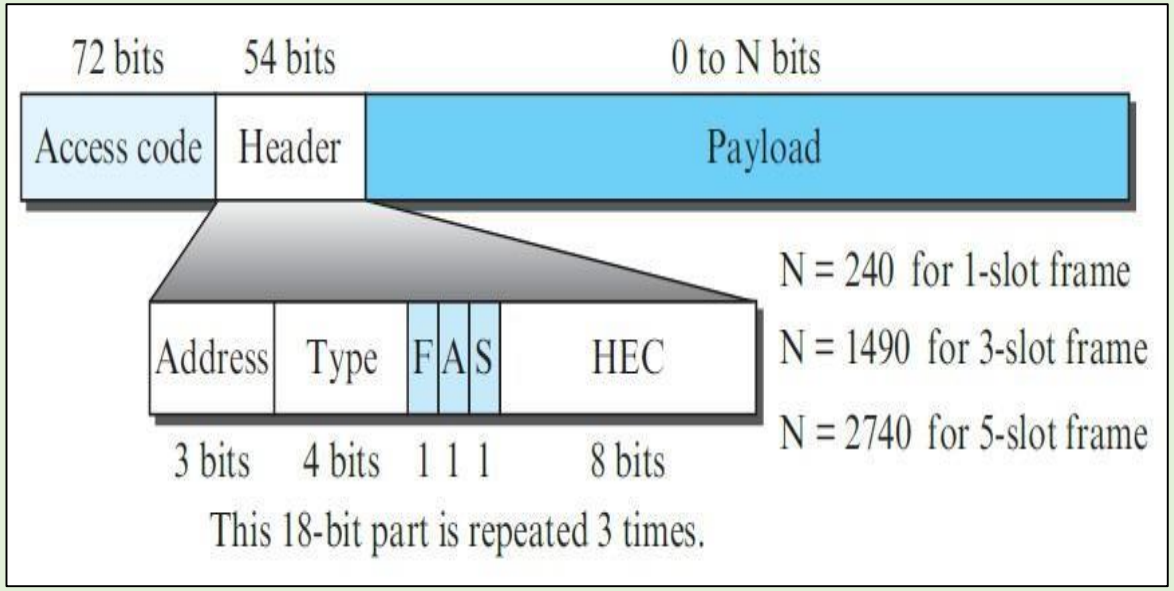
- **SCO:** A synchronous connection-oriented (SCO) link is used when avoiding latency (delay in data delivery) is more important than integrity (error-free delivery). In an SCO link, a physical link is created between the primary and a secondary by reserving specific slots at regular intervals. The basic unit of connection is two slots, one for each direction. If a packet is damaged, it is never retransmitted. SCO is used for real- time audio where avoiding delay is all-important.

- **ACL:** An asynchronous connectionless link (ACL) is used when data integrity is more important than avoiding latency. In this type of link, if a payload encapsulated in the frame is corrupted, it is retransmitted. A secondary returns an ACL frame in the available odd-numbered slot if the previous slot has been addressed to it. ACL can use one, three, or more slots and can achieve a maximum data rate of 721 kbps.

Bluetooth:

- **Radio Layer**: The radio layer is roughly equivalent to the physical layer of the Internet model. Bluetooth devices are low-power and have a range of 10 m.
- Band : Bluetooth uses a 2.4-GHz ISM band divided into 79 channels of 1 MHz each.
- **FHSS:** Bluetooth uses the frequency-hopping spread spectrum (FHSS) method in the physical layer to avoid interference from other devices or other networks. Bluetooth hops 1600 times per second, which means that each device changes its modulation frequency 1600 times per second.
- **Modulation:** To transform bits to a signal, Bluetooth uses a sophisticated version of FSK, called GFSK (FSK with Gaussian bandwidth filtering).
- GFSK has a carrier frequency. Bit 1 is represented by a frequency deviation above the carrier; bit 0 is represented by a frequency deviation below the carrier.

Frame Format of Bluetooth

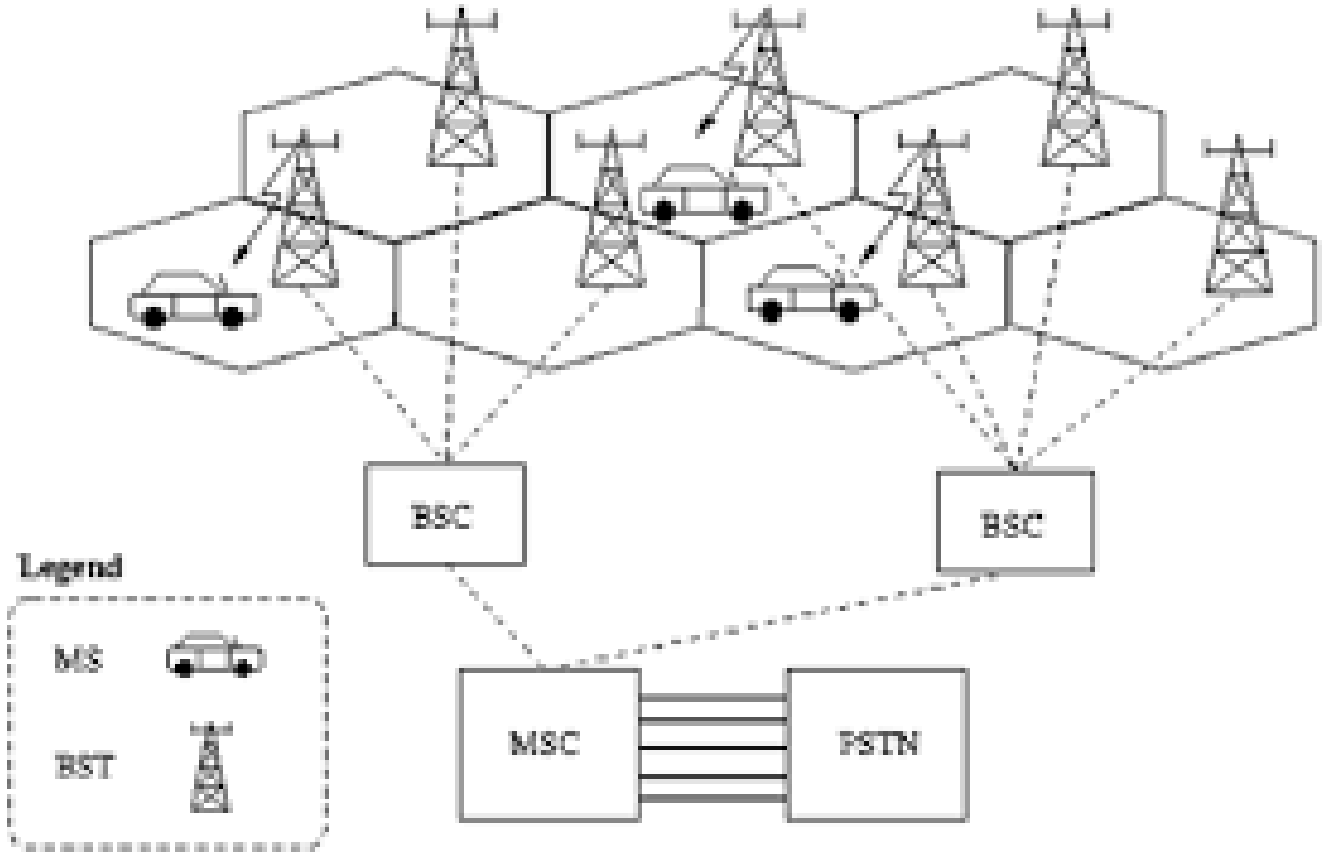


- **Access code.** This 72-bit field normally contains synchronization bits and the identifier of the primary to distinguish the frame of one piconet from another.
- **Header.** This 54-bit field is a repeated 18-bit pattern. Each pattern has the following subfields:
- **Address.** The 3-bit address subfield can define up to seven secondaries (1 to 7). If the address is zero, it is used for broadcast communication from the primary to all secondaries.
- **Type.** The 4-bit type subfield defines the type of data coming from the upper layers.
- **F.** This 1-bit subfield is for flow control. When set (1), it indicates that the device is unable to receive more frames (F = 1 → buffer is **full**).

Bluetooth – Frame Format:

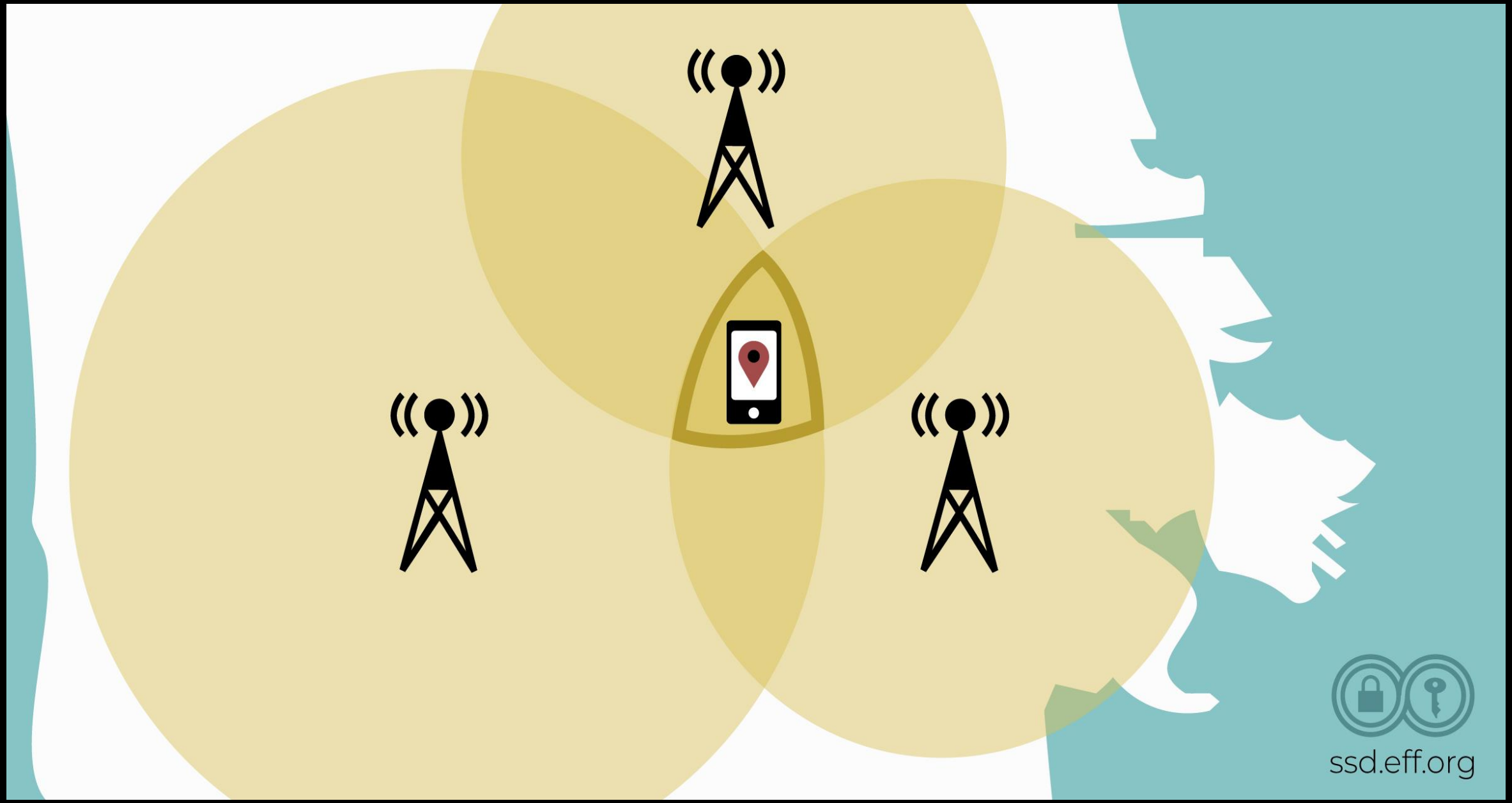
- **A**. This 1-bit subfield is for acknowledgment. Bluetooth uses Stop-and-Wait ARQ; 1 bit is sufficient for acknowledgment.
- **S.** This 1-bit subfield holds a sequence number. Bluetooth uses Stop-and-Wait ARQ; 1 bit is sufficient for sequence numbering.
- **HEC.** The 8-bit **Header Error Correction** subfield is a checksum to detect errors in each 18-bit header section.
- **Payload**. This subfield can be 0 to 2740 bits long. It contains data or control information coming from the upper layers.

Cellular Telephony

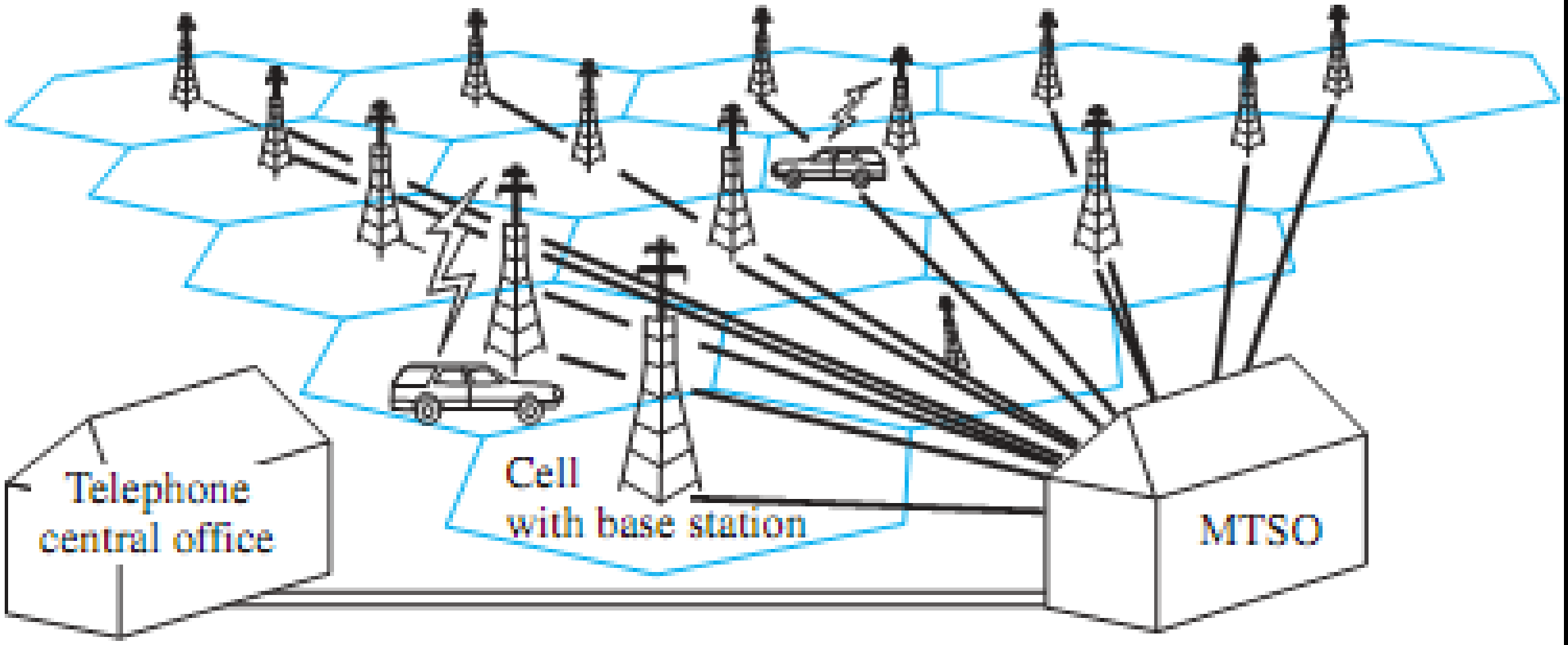


Cellular Telephony

Cellular Telephony


ssd.eff.org

Cellular Telephony



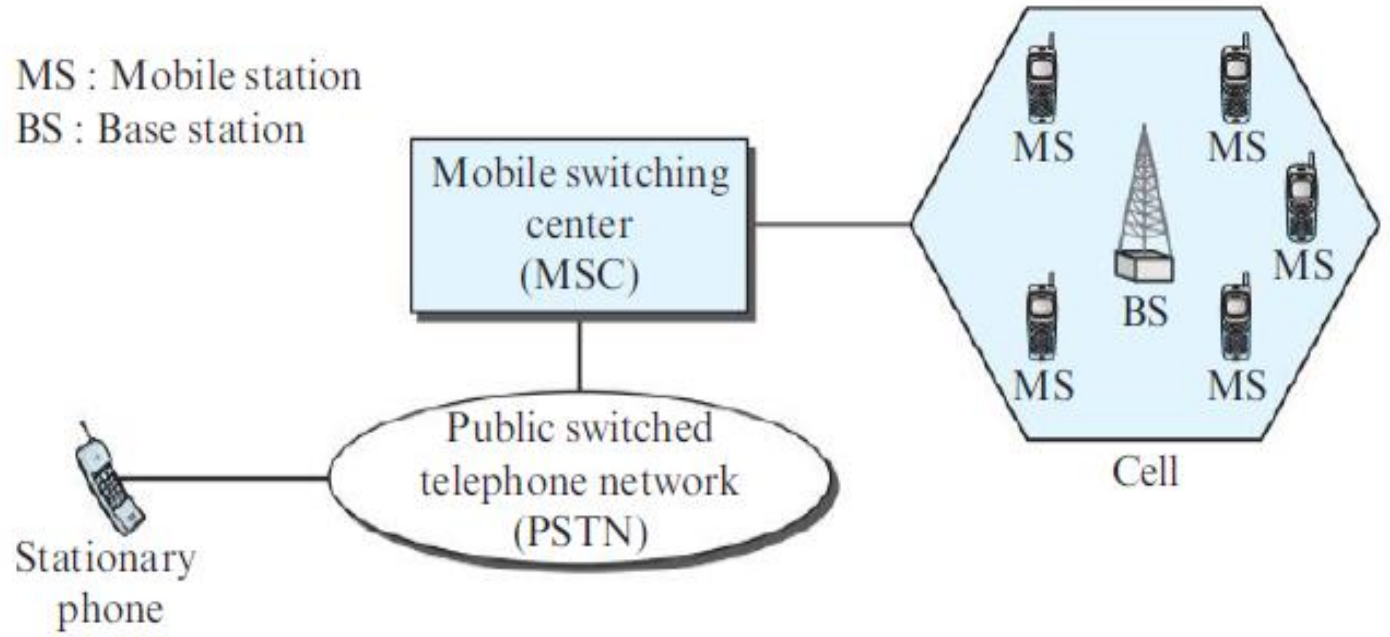
Cellular telephone concept in mobile radio system.

Cellular Telephony

- 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.
- To make this tracking possible, **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.
- Eg: MSC vendors→ Nokia , Cisco,…

Cellular Telephony:

Figure 6.35 *Cellular system*



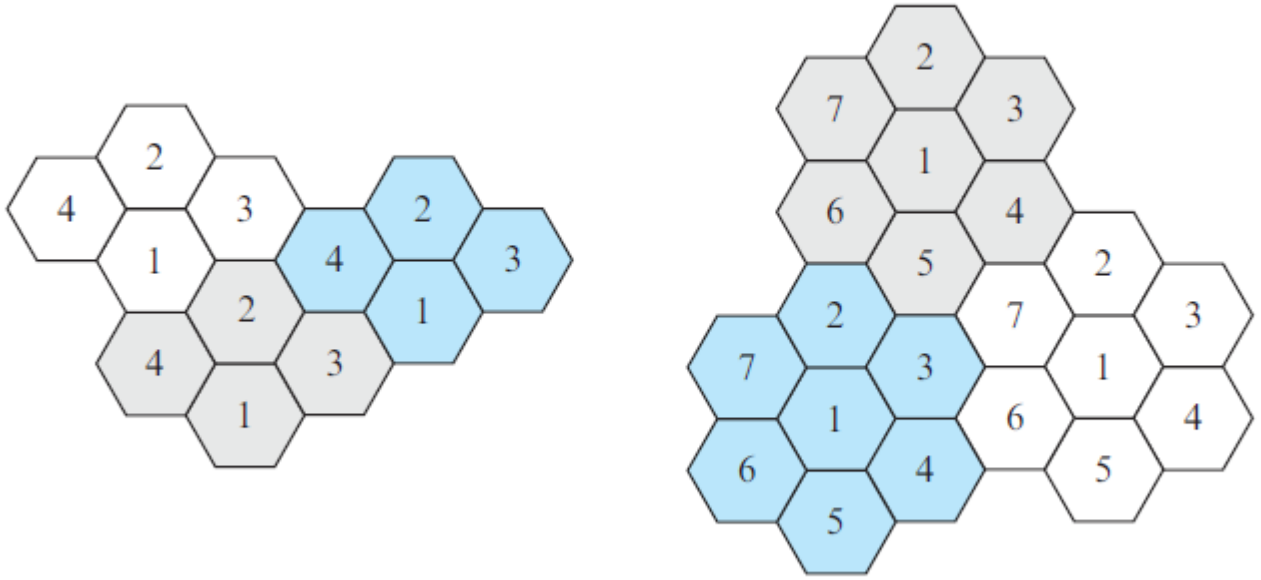
- Cell size is not fixed and can be increased or decreased depending on the population
- Cell size is optimized to prevent the interference of adjacent cell signals.
- The transmission power of each cell is kept low to prevent its signal from interfering with those of other cells of the area.

Frequency-Reuse Principle

- In general, 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.

Cellular Telephony:

Figure 6.36 *Frequency reuse patterns*



a. Reuse factor of 4

b. Reuse factor of 7

- **The numbers in the cells define the pattern. The cells with the same number in a pattern can use the same set of frequencies. We call these cells the reusing cells.**

Transmitting:

- To place a call from a mobile station, the caller enters a code of 7 or 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.

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

- It may happen that, during a conversation, the mobile station moves from one cell to another.
- When it does, the signal may become weak.
- To solve this problem, 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).

Hard Handoff

- Early systems used a 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. This **may create a rough transition.**

Soft Handoff

- New systems use a soft handoff. In this case, a **mobile station can communicate with two base stations at the same time.**
- This means that, during handoff, a **mobile station may continue with the new base station before breaking off** from the old one.

Roaming

- One feature of cellular telephony is called roaming.
- Roaming means, in principle, that a user can have access to communication or can be reached where there is coverage.
- A **service provider** usually has **limited coverage**.
- **Neighboring service providers** can **provide extended coverage** through a **roaming contract.**

Threats and Attacks

- Information needs to be secured from attacks. To be secured, information needs to be hidden from unauthorized access (confidentiality), protected from unauthorized change (integrity), and available to an authorized entity when it is needed (availability).
- **Security Goals: confidentiality, integrity, and availability.**
- **Confidentiality:** Confidentiality is probably the most common aspect of information security. We need to protect our confidential information. An organization needs to guard against those malicious actions that endanger the confidentiality of its information. Confidentiality not only applies to the storage of information, it also applies to the transmission of information. When we send a piece of information to be stored in a remote computer or when we retrieve a piece of information from a remote computer, we need to conceal it during transmission.
- **Integrity:** Information needs to be changed constantly. In a bank, when a customer deposits or withdraws money, the balance of her account needs to be changed. Integrity means that changes need to be done only by authorized entities and through authorized mechanisms. Integrity violation is not necessarily the result of a malicious act; an interruption in the system, such as a power surge, may also create unwanted changes in some information.

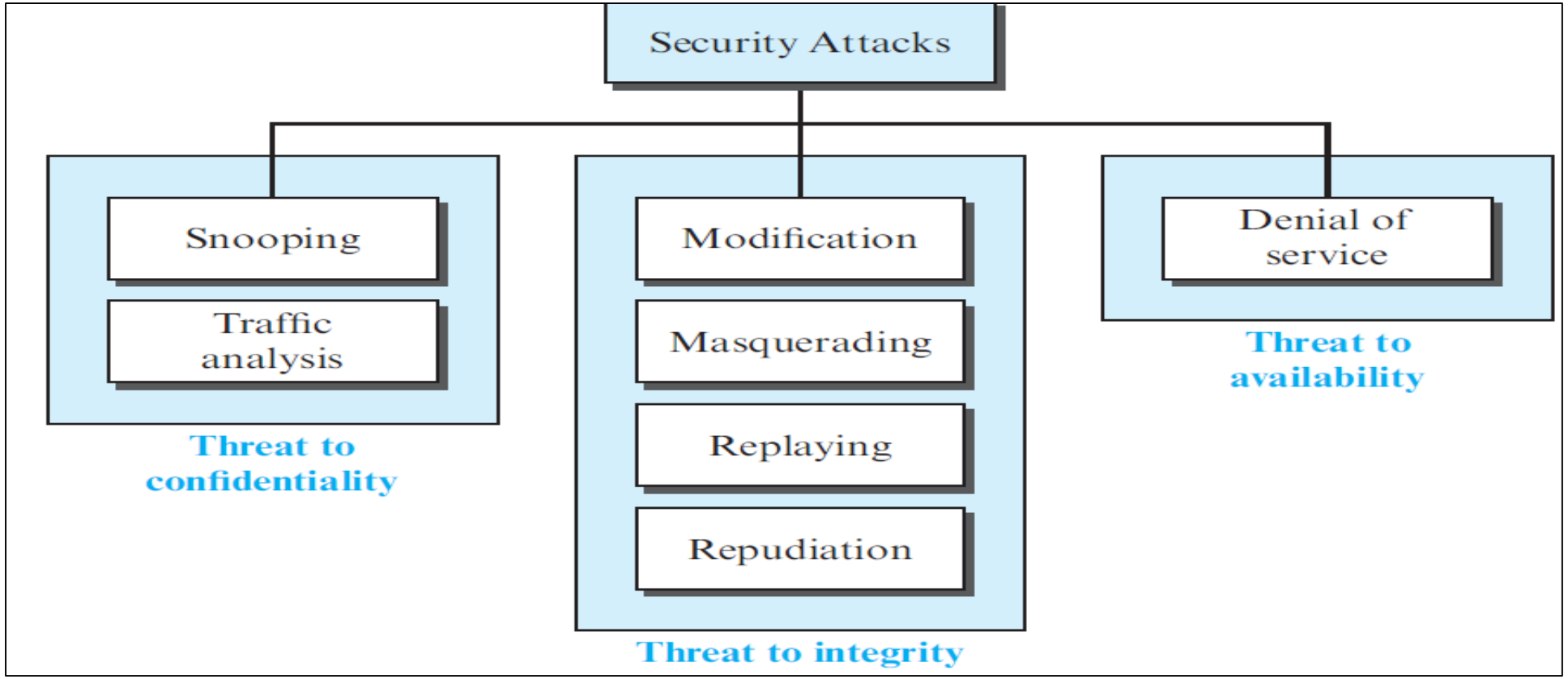
Threats and Attacks

- **Availability:** The third component of information security is availability. The information created and stored by an organization needs to be available to authorized entities. Information is useless if it is not available. Information needs to be constantly changed, which means it must be accessible to authorized entities. The **unavailability** of information is just as **harmful for an organization** as the lack of confidentiality or integrity.
- *Eg:- Imagine what would happen to a bank if the customers could not access their accounts for transactions.*

Attacks

- These three goals of security: confidentiality, integrity, and availability can be threatened by security attacks. These three goals of security: confidentiality, integrity, and availability can be threatened by security attacks.
- **Attacks Threatening Confidentiality:**
- Two types of attacks threaten the confidentiality of information: snooping and traffic analysis.

1. **Snooping:** Snooping refers to unauthorized access to or interception of data.
   - Eg:- a file transferred through the Internet may contain confidential information.
   - An unauthorized entity may intercept the transmission and use the contents for her own benefit.
   - To prevent snooping, the data can be made non intelligible to the interceptor by using encipherment techniques.



2. Traffic Analysis: Although encipherment of data may make it non intelligible for the intercepter, she can obtain some other type of information by monitoring online traffic.

- Eg:- she can find the electronic address (e-mail address) of the sender or the receiver.
- She can collect pairs of requests and responses to help her guess the nature of the transaction.

Attacks Threatening Integrity

The integrity of data can be threatened by attacks such as modification, masquerading, replaying, and repudiation.

1. **Modification:** After intercepting or accessing information, the attacker modifies the information to make it beneficial to herself.
   - For example, a customer sends a message to a bank to initiate a transaction. The attacker intercepts the message and changes the type of transaction to benefit herself. Sometimes the attacker simply deletes or delays the message to harm the system or to benefit from it.
2. **Masquerading:** Masquerading, or spoofing, happens when the attacker impersonates somebody else.

- Eg:- an attacker might steal the bank card and PIN of a bank customer and pretend that he is that customer. Sometimes the attacker pretends instead to be the receiver entity.
- Eg:- a user tries to contact a bank, but another site pretends that it is the bank and obtains some information from the user.

Replaying: Replaying is another attack. The attacker obtains a copy of a message sent by a user and later tries to replay it.

- For example, a person sends a request to her bank to ask for payment to the attacker, who has done a job for her. The attacker intercepts the message and sends it again to receive another payment from the bank.

Repudiation: This type of attack is different from others because it 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. An example of denial by the sender would be a bank customer asking her bank to send some money to a third party but later denying that she has made such a request.
- An example of denial by the receiver could occur when a person buys a product from a manufacturer and pays for it electronically, but the manufacturer later denies having received the payment and asks to be paid.

Attacks Threatening Availability

Attack threatening availability: denial of service.

Denial of Service: Denial of service (DoS) is a very common attack. It may slow down or totally interrupt the service of a system.

- The attacker can use several strategies to achieve this. She might send so many bogus requests to a server that the server crashes because of the heavy load. The attacker might intercept and delete a server's response to a client, making the client believe that the server is not responding.
- The attacker may also intercept requests from the clients, causing the clients to send requests many times and overload the system.

Security Services to Prevent Attacks

ITU-T defines some security services to achieve security goals and prevent attacks. Two techniques are prevalent today: one is very general (cryptography) and one is specific (steganography).

1. **Cryptography:** Some security services can be implemented using cryptography. Cryptography means "secret writing." The term is used to refer as, the science and art of transforming messages to make them secure and immune to attacks. In the past cryptography referred only to the encryption and decryption of messages using secret keys, today it is defined as involving three distinct mechanisms: symmetric-key encipherment, asymmetric-key encipherment, and hashing.
2. **Steganography:** The technique used for secret communication in the past is being revived at the present time: steganography. The word steganography, means "covered writing," in contrast with cryptography, which means "secret writing."

- ***Cryptography*** *means concealing the contents of a message by enciphering;*
- ***Steganography*** *means concealing the message itself by covering it with something else.*

Network Address Translation. (NAT)

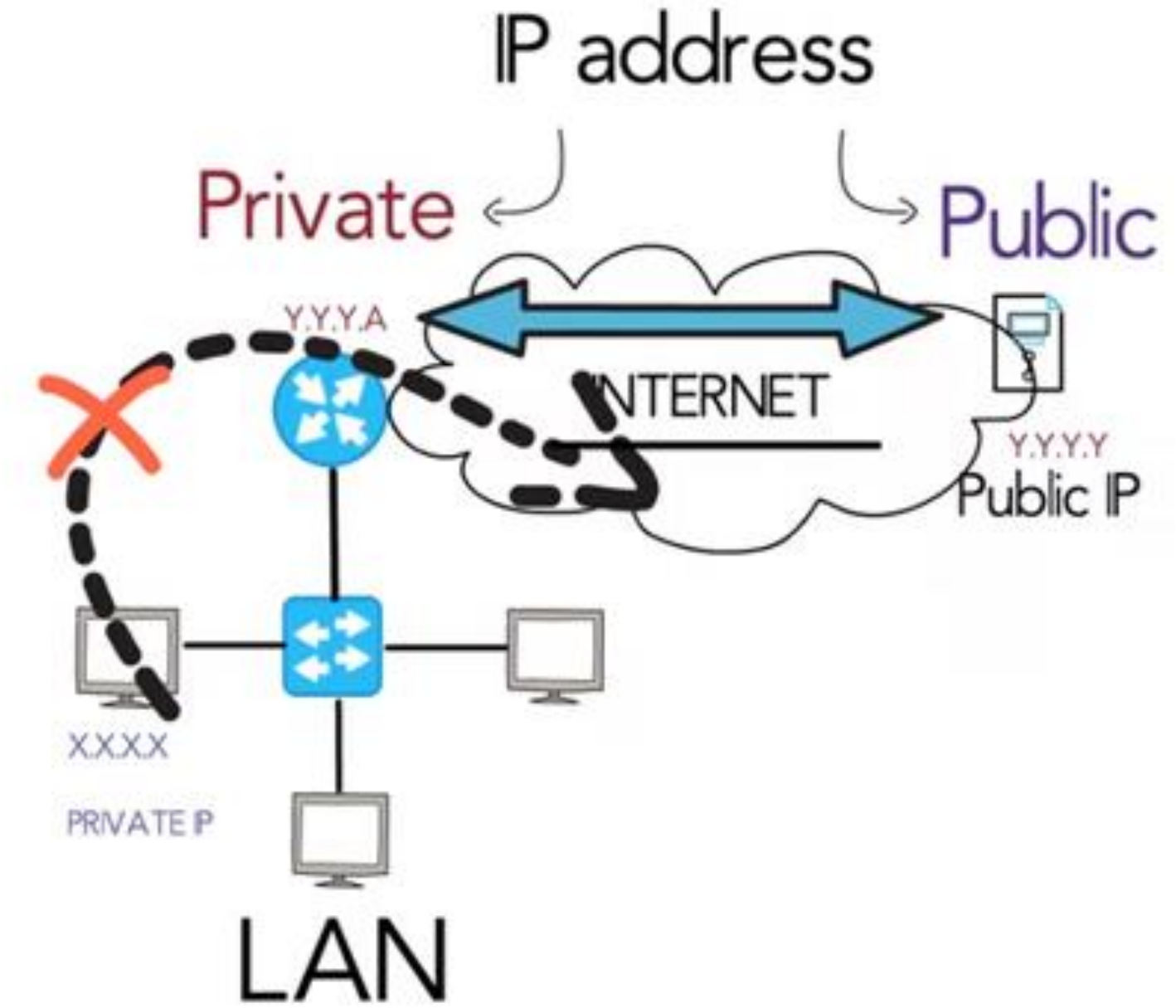
Network Address Translation: (NAT)

Network Address Translation

NAT Translate Private IP to Public IP and Public IP to Private IP

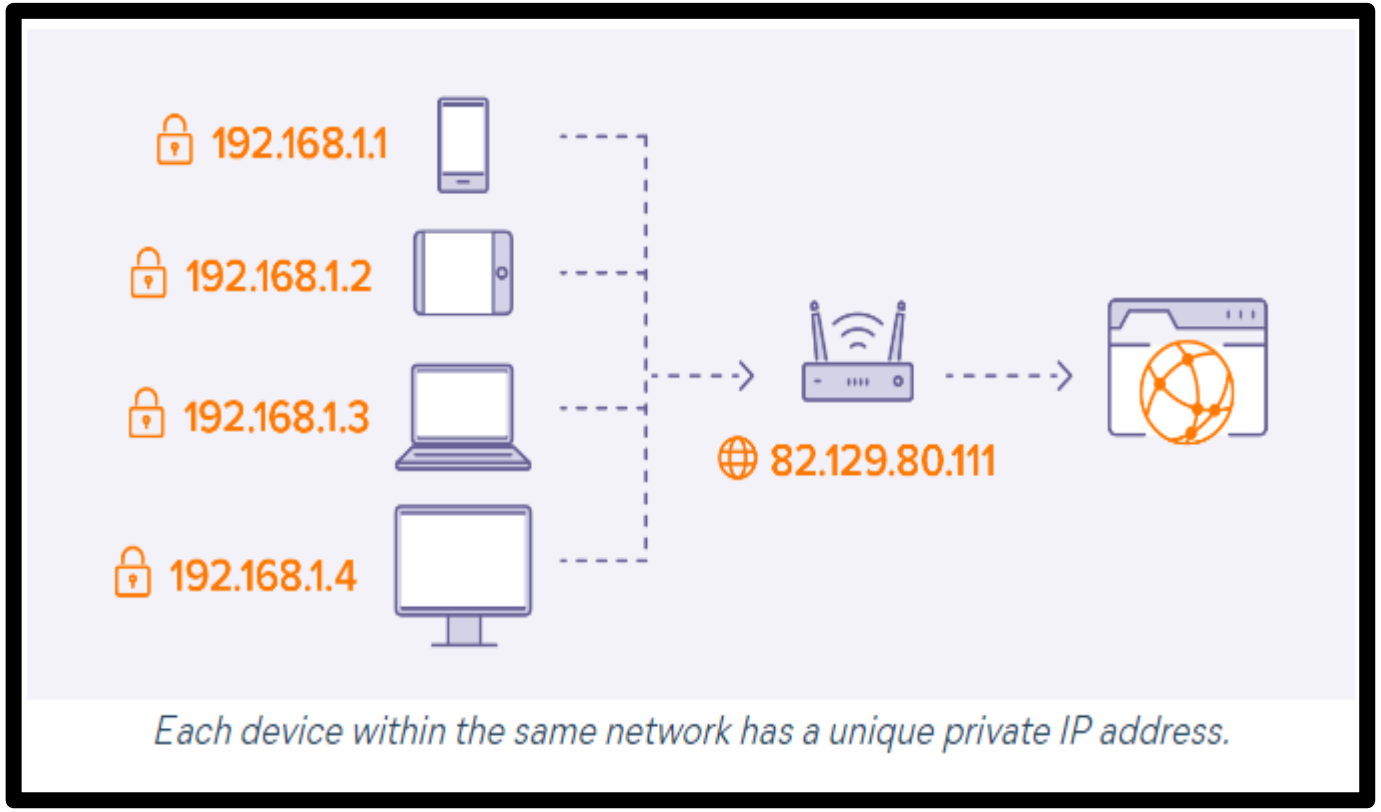
- **Private IP:**
- A private IP address is the address your network router assigns to your device. **Each device within the same network is assigned a unique private IP address** (sometimes called a private network address) — this is how devices on the same internal network talk to each other.
- **Public IP:**
- A *public* IP address is an IP address that can be accessed directly over the internet and is assigned to your network router by your internet service provider (ISP). Your personal device also has a *private* IP that remains hidden when you connect to the internet through your router's public IP.
- Using a public IP address to connect to the internet is like using a P.O. box for your snail mail, rather than giving out your home address. It's a little bit safer, but a lot more visible.

Network Address Translation: (NAT)



Network Address Translation: (NAT)

- A **public IP address** identifies you to the wider internet so that all the information you're searching for can find you.
- A **private IP address** is used within a private network to connect securely to other devices within that same network.



Each device within the same network has a unique private IP address.

Difference between Public & Private IP Address

Public IP address	Private IP address
External (global) reach	Internal (local) reach
Used for communicating outside your private network, over the internet	Used for communicating within your private network, with other devices in your home or office
A unique numeric code never reused by other devices	A non-unique numeric code that may be reused by other devices in other private networks
Found by Googling: "What is my IP address?"	Found via your device's internal settings
Assigned and controlled by your internet service provider	Assigned to your specific device within a private network
Not free	Free
Any number not included in the reserved private IP address range Example: 8.8.8.8.	10.0.0.0 — 10.255.255.255; 172.16.0.0 — 172.31.255.255; 192.168.0.0 — 192.168.255.255 Example: 10.11.12.13

Network Address Translation:

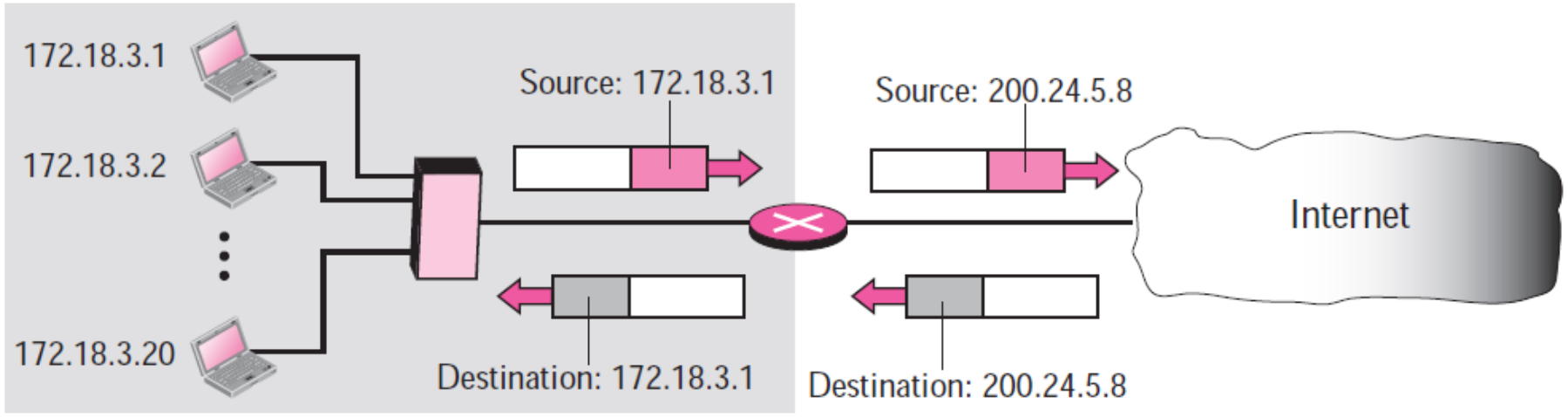
- To access the Internet, one public IP address is needed, but we can use a private IP address in our private network. The idea of NAT is to allow **multiple devices** to **access the Internet** through a **single public address**. To achieve this, the translation of a private IP address to a public IP address is required.
- **Network Address Translation (NAT)** is a process in which one or more local IP address is translated into one or more Global IP address and vice versa in order to provide Internet access to the local hosts.
- Also, it does the translation of port numbers i.e. masks the port number of the host with another port number, in the packet that will be routed to the destination. It then makes the corresponding entries of IP address and port number in the NAT table.
- NAT generally operates on a router or firewall.

https://www.myip.com/

Address Translation:

- All of the outgoing packets go through the NAT router, which replaces the *source address* in the packet with the global NAT address.
- All incoming packets also pass through the NAT router, which replaces the *destination address* in the packet (the NAT router global address) with the appropriate private address.

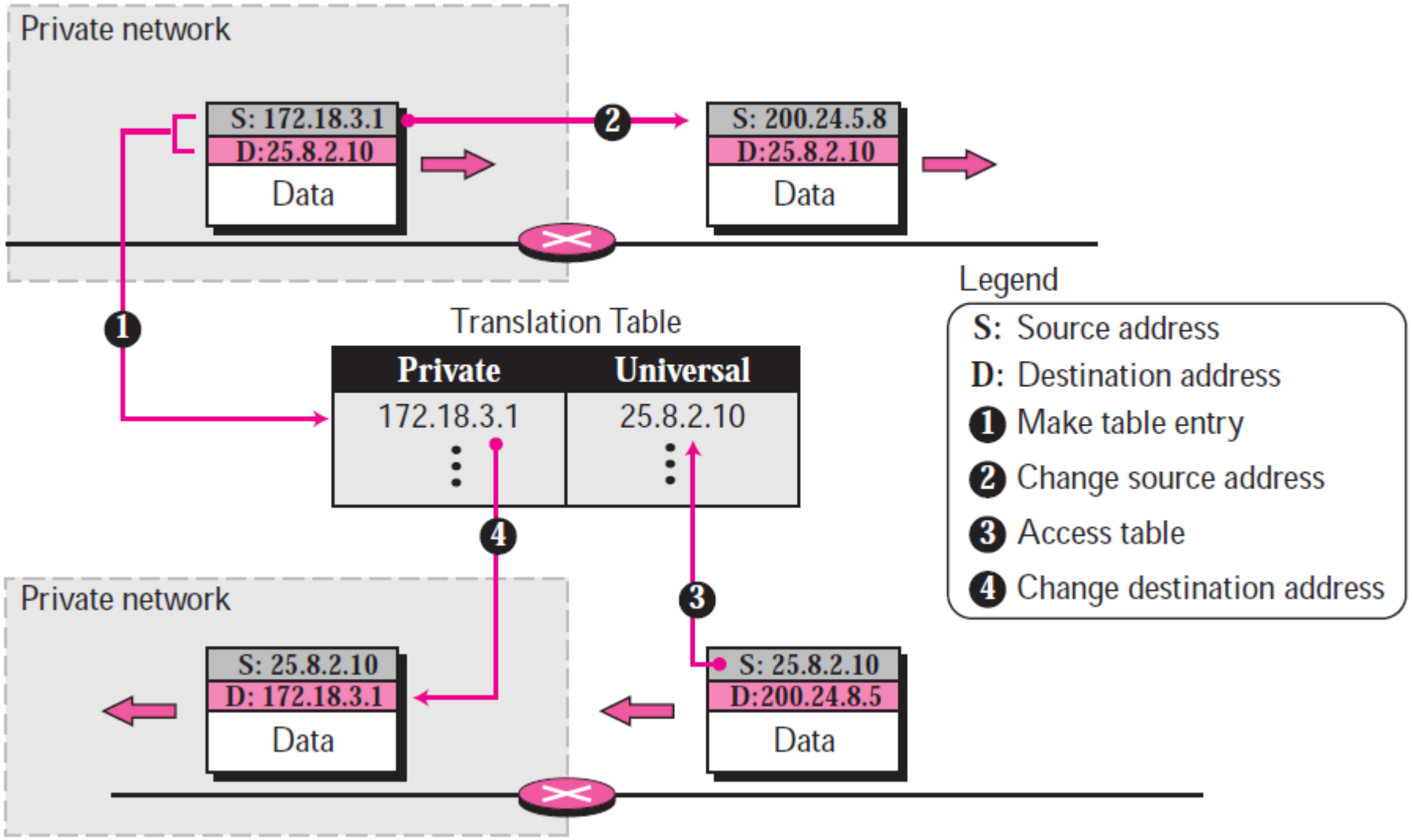
Figure 5.40 *Address translation*



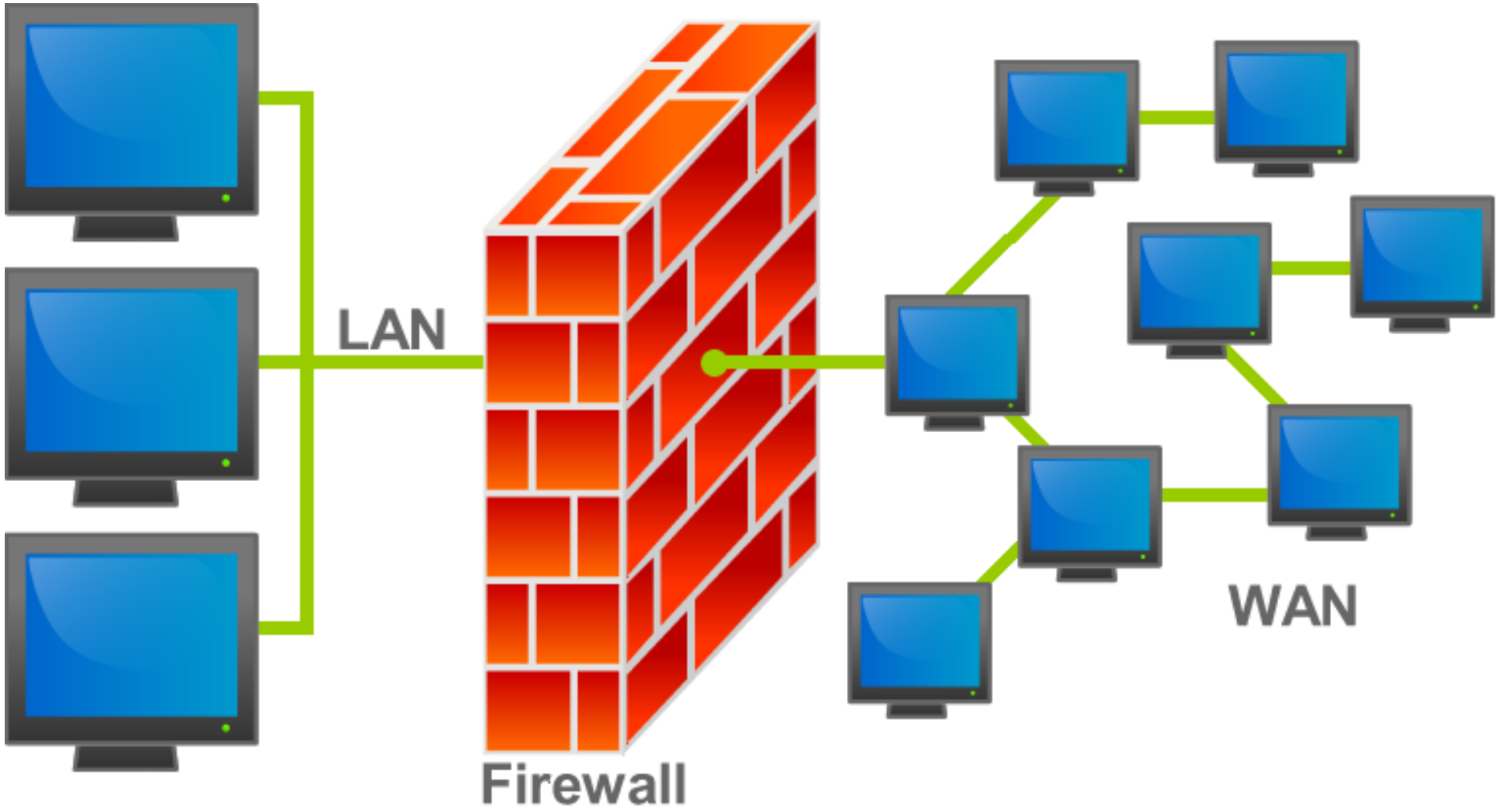
Translation Table

- Translating the source addresses for an outgoing packet is straightforward.
- But how does the NAT router know the destination address for a packet coming from the Internet? There may be tens or hundreds of private IP addresses, each belonging to one specific host. The problem is solved if the NAT router has a **translation table.**
- In its simplest form, a translation table has only two columns: the private address and the external address (destination address of the packet). When the router translates the source address of the outgoing packet, it also makes note of the destination address— where the packet is going. When the response comes back from the destination, the router uses the source address of the packet (as the external address) to find the private address of the packet.

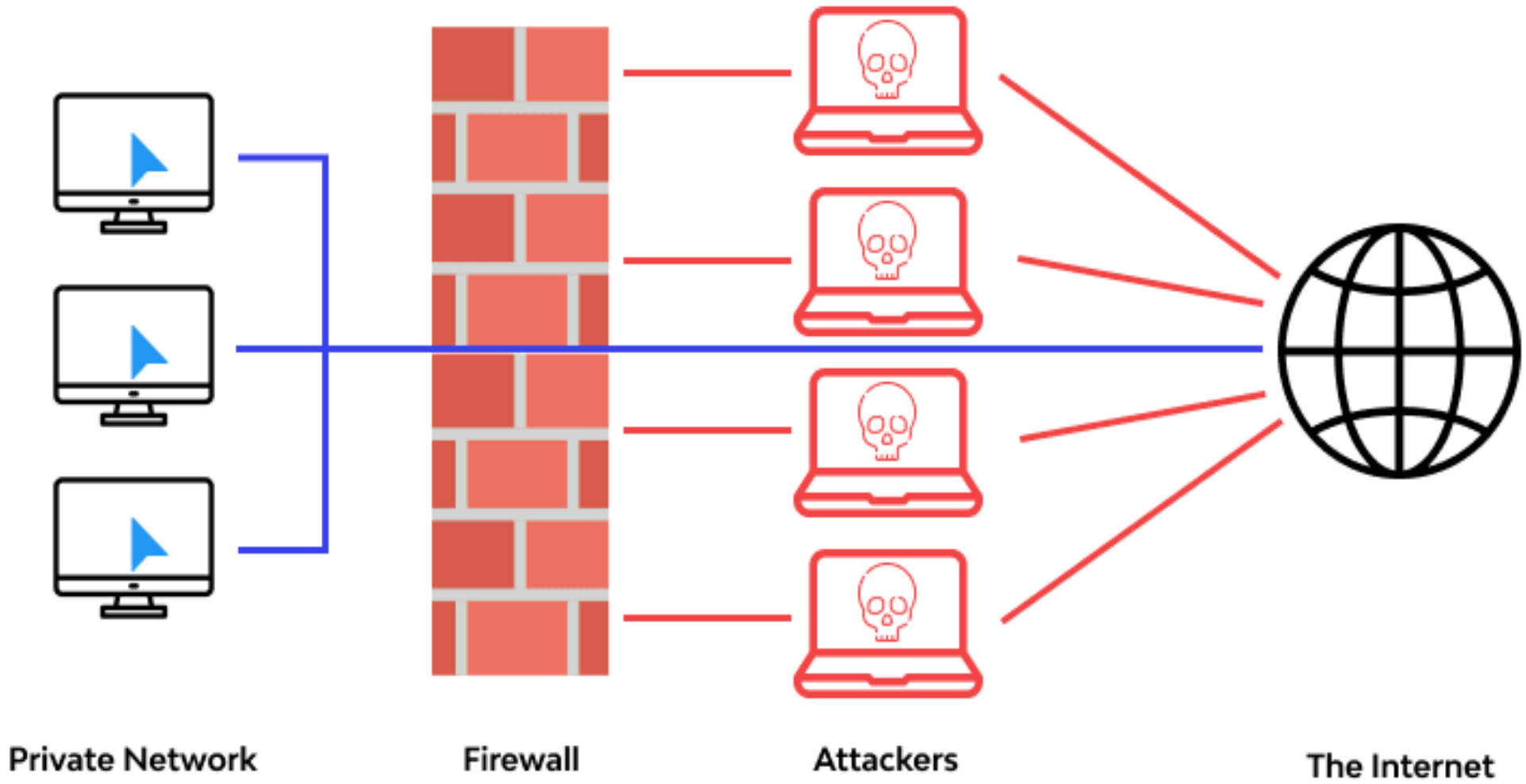
Translation

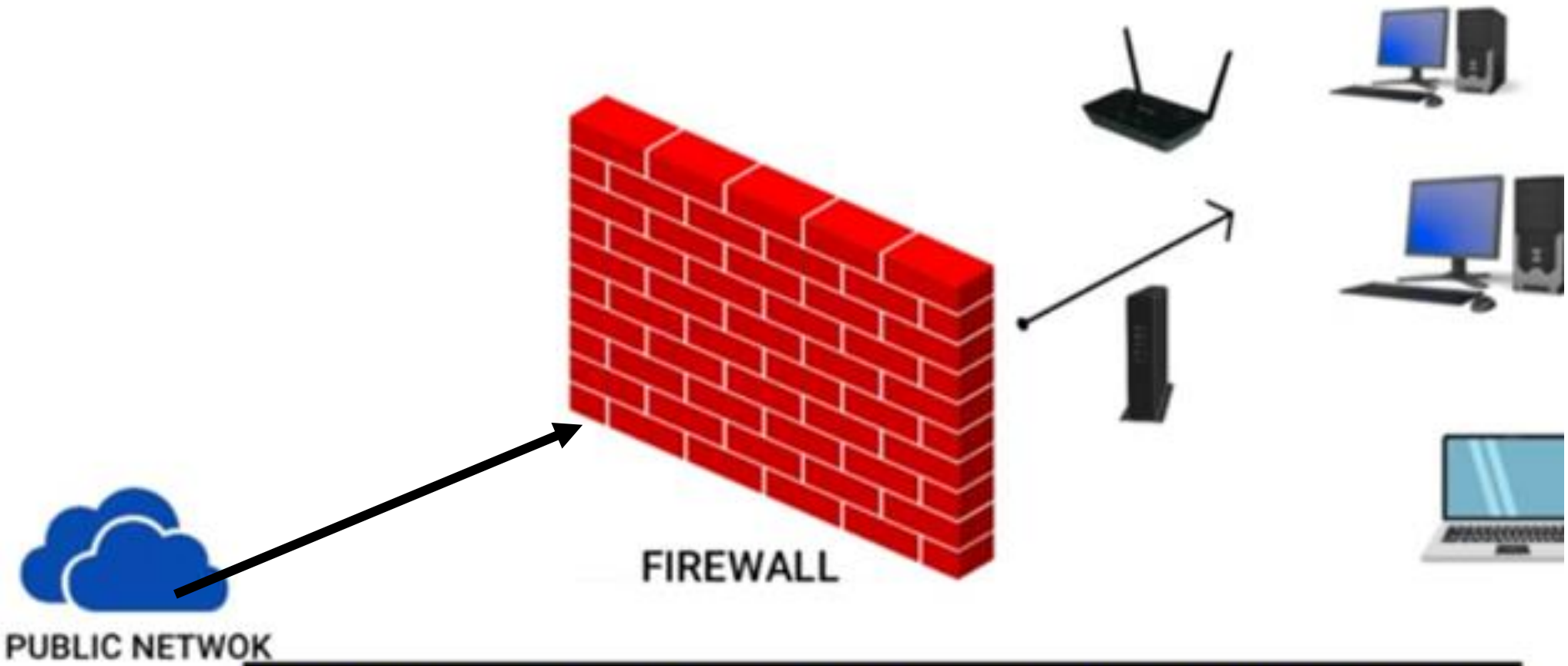


Firewalls



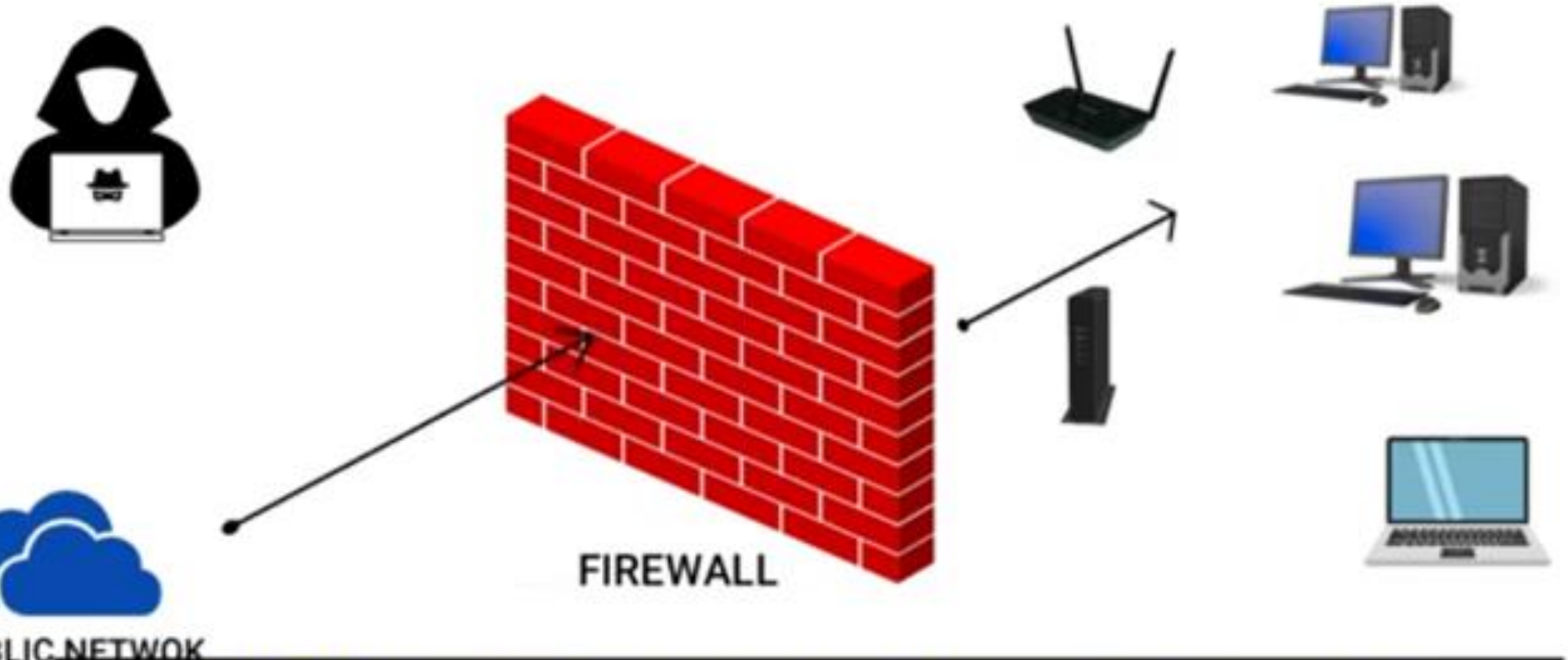
What is a Firewall





FIREWALL is a wall stands between public Network and our Private network. It protect our private network.

FIREWALL



FIREWALL protect our private from Hacker attack, suspecious malware and virus pop ups.

FIREWALL

action	source address	dest address	protocol	source port	dest port	flag bit
allow	222.22/16	outside of 222.22/16	TCP	> 1023	80	any
allow	outside of 222.22/16	222.22/16	TCP	80	> 1023	ACK
allow	222.22/16	outside of 222.22/16	UDP	> 1023	53	---
allow	outside of 222.22/16	222.22/16	UDP	53	> 1023	----
deny	all	all	all	all	all	all

Access Control List

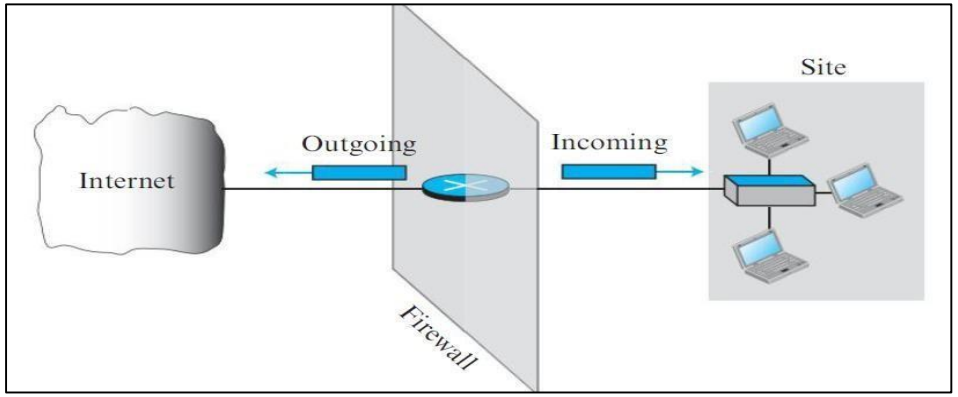
FIREWALL

action	source address	dest address	protocol	source port	dest port	flag bit
allow	222.22/16	outside of 222.22/16	TCP	> 1023	80	any
allow	outside of 222.22/16	222.22/16	TCP	80	> 1023	ACK
allow	222.22/16	outside of 222.22/16	UDP	> 1023	53	---
allow	outside of 222.22/16	222.22/16	UDP	53	> 1023	----
deny	all	all	all	all	all	all

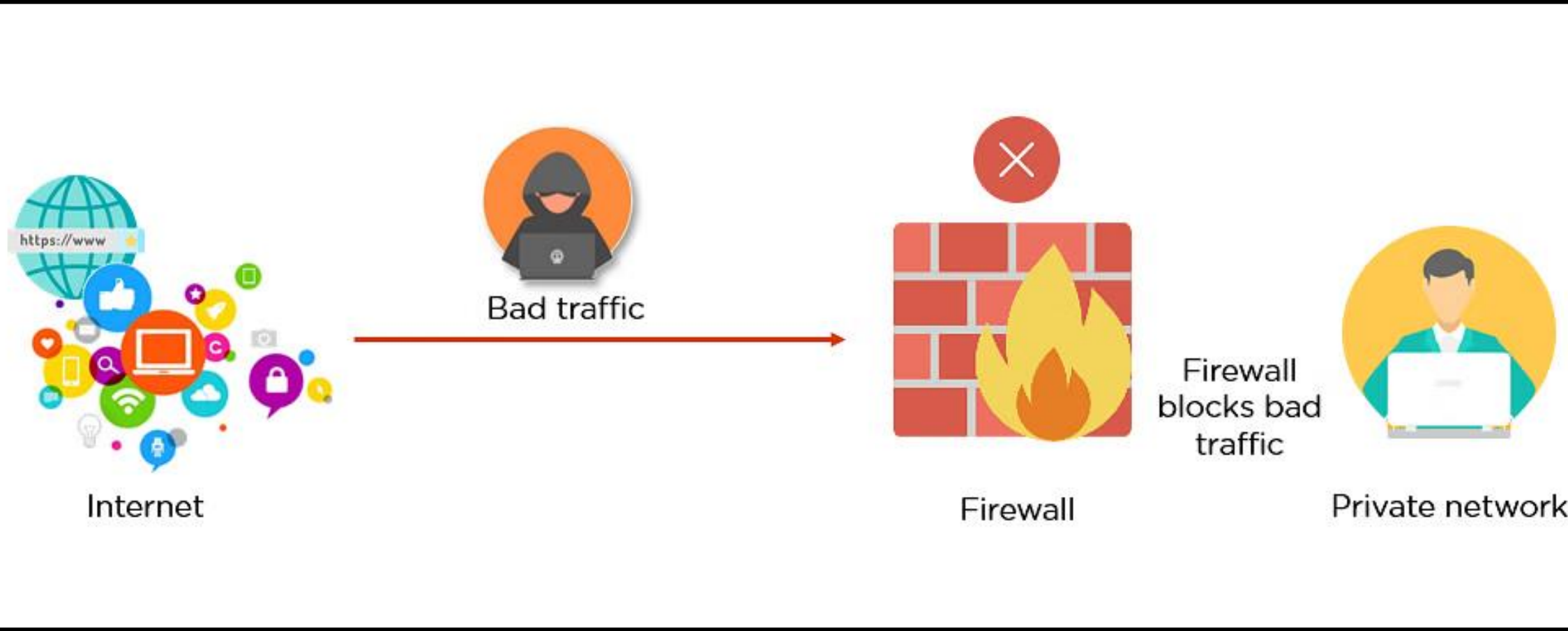
We can allow and deny any IP address and Ports etc.
Also we can also change it later if we require

FIREWALLS

- Security measure which prevent Eve from sending a harmful message to a system. To control access to a system we need firewalls.
- A firewall is a device (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.
  - *Eg:- a firewall may filter all incoming packets destined for a **specific host or a specific server** such as HTTP.*
  - *A firewall can be used to **deny access to a specific host** or a **specific service** in the organization*.
- A firewall is usually classified as:
  - ✓ **packet-filter firewall or**
  - ✓ **proxy-based firewall**.



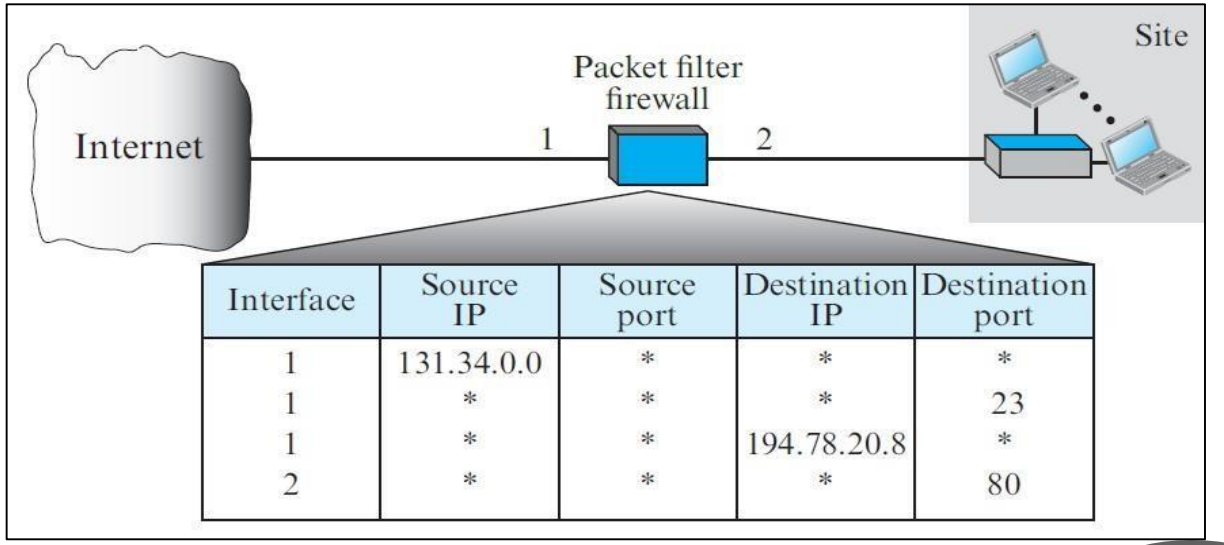
Firewalls:


https://www
Bad traffic
Internet
Firewall
Firewall blocks bad traffic
Private network

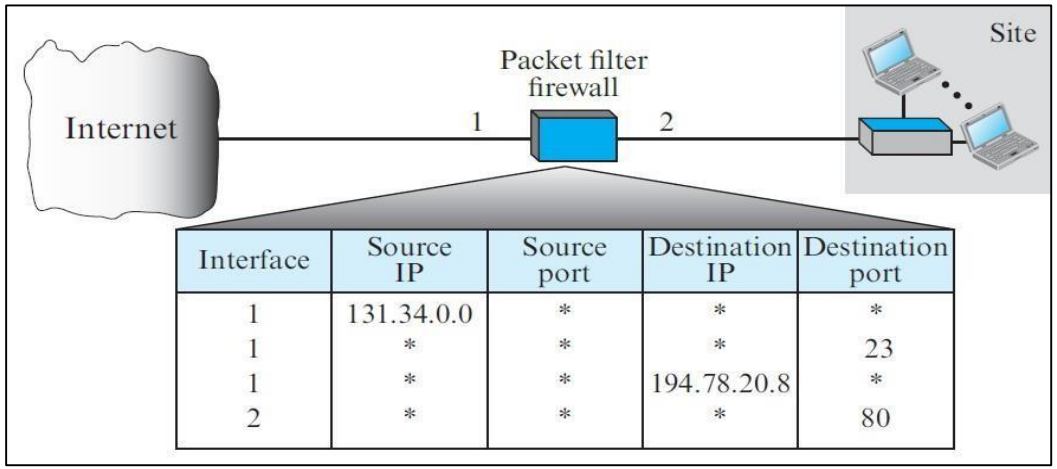
Packet-Filter Firewall

- A firewall can be used as a packet filter. It can forward or block packets based on the information in the network- layer and transport-layer headers: source and destination IP addresses, source and destination port addresses, and type of protocol (TCP or UDP).
- A packet-filter firewall is a **router** that uses a filtering table to decide which packets must be discarded (not forwarded).
- Figure shows an example of a filtering table for this kind of a firewall.

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



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



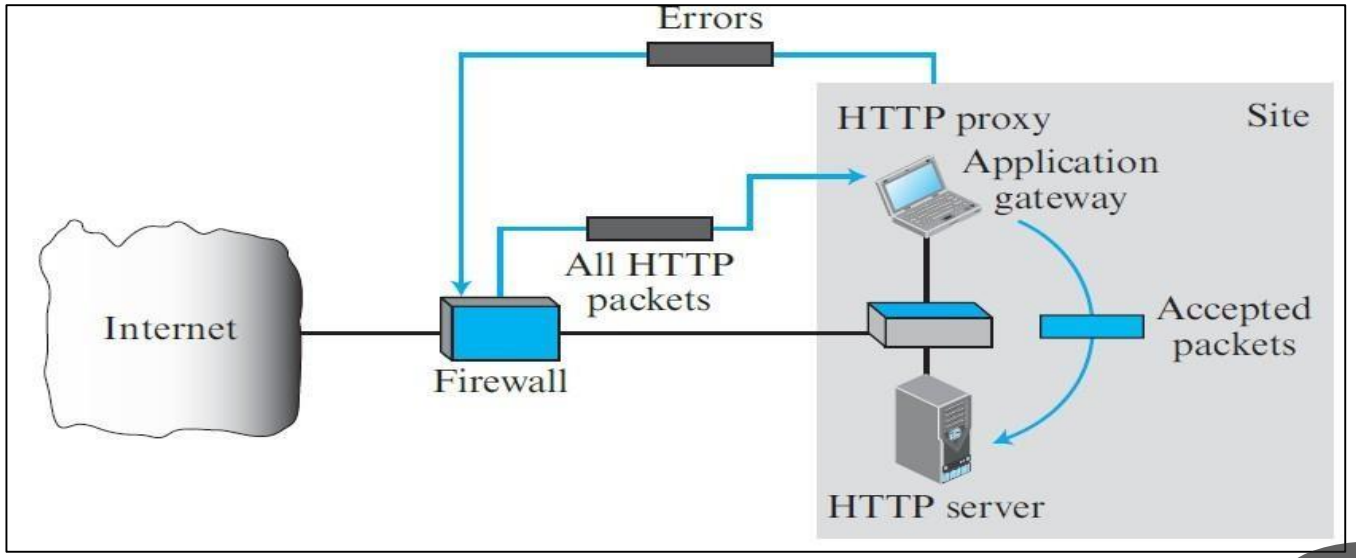
Interface	Source IP	Source port	Destination IP	Destination port
1	131.34.0.0	*	*	*
1	*	*	*	23
1	*	*	194.78.20.8	*
2	*	*	*	80

- **According to the figure, the following packets are filtered:**
- Incoming packets from network 131.34.0.0 are blocked (security precaution).
- The * (asterisk) means "any."
- Incoming packets destined for any internal TELNET server (port 23) are blocked.
- Incoming packets destined for internal host 194.78.20.8. are blocked. The organization wants this host for internal use only.
- Outgoing packets destined for an HTTP server (port 80) are blocked. The organization does not want employees to browsethe Internet.

Proxy Firewall

- The packet-filter firewall is based on the information available in the network layer and transport layer headers (IP and TCP/UDP).
- However, sometimes we need to filter a message based on the information available in the message itself (at the application layer).
- ***Example:*** *Assume that an organization wants to implement the following policies regarding its web pages: only those* ***Internet users*** *who have* ***previously established business relations*** *with the* ***company*** *can* ***have access****; access to* ***other users*** *must be* ***blocked.*** *In this case, a packet-filter firewall is not feasible because it cannot distinguish between different packets arriving at TCP port 80 (HTTP). Testing must be done at the application level (using URLs).*

Application gateway implementation for HTTP.



- One solution is to install a proxy computer (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.

Firewalls:

2-types:

1. Software Firewall

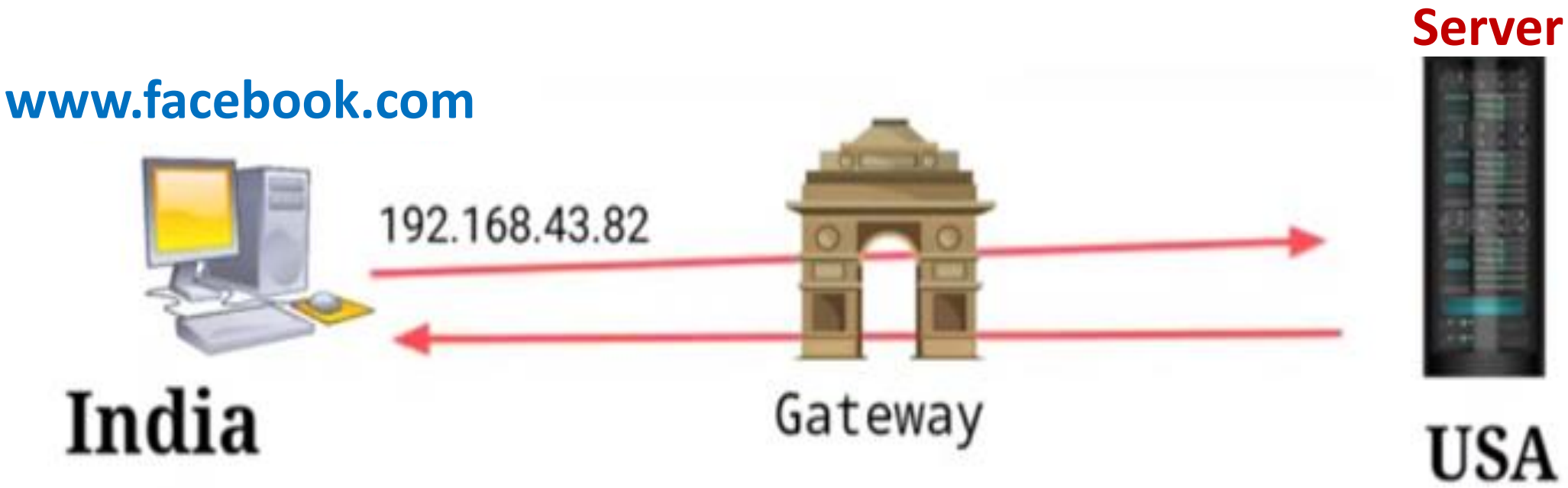
- Software firewall is a special type of computer software runs on a computer/server.
- It's main purpose is to protect your computer/server from outside attempts to control or gain access and depending on your choice of software firewall. Software firewall can also be configured for checking any suspicious outgoing requests.
- Sophos XG Firewall are an example of a software firewall.

2. Hardware Firewall

- It is physical piece of equipment planed to perform firewall duties.
- A hardware firewall can be a computer or a dedicated piece of equipment which serve as a firewall.
- Hardware firewall are incorporated into the router that is situated between the computer and the internet gateway.
- A hardware firewall is **a physical device much like a server that filters the traffic going to a computer**.
- The firewall sits between the external network and the server, providing an **antivirus solution** and a **hard barrier against intrusions**.
- **Linksys routers** are an example of a hardware firewall.

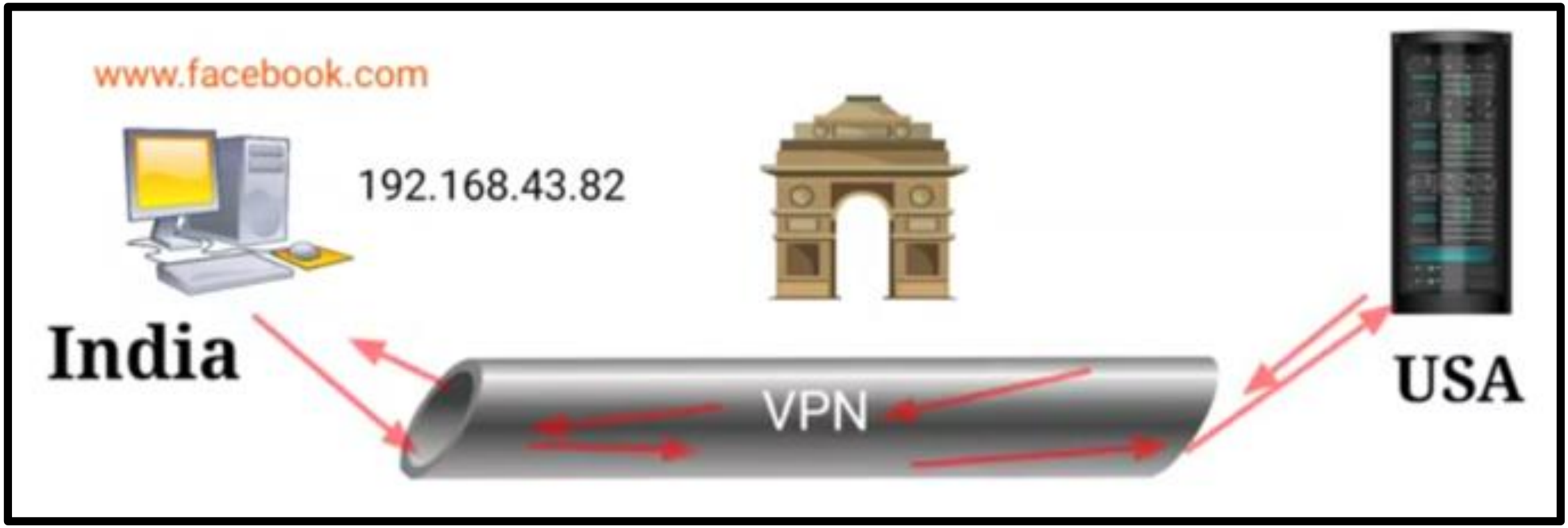
Virtual Private Network (VPN)

Virtual Private Network (VPN)

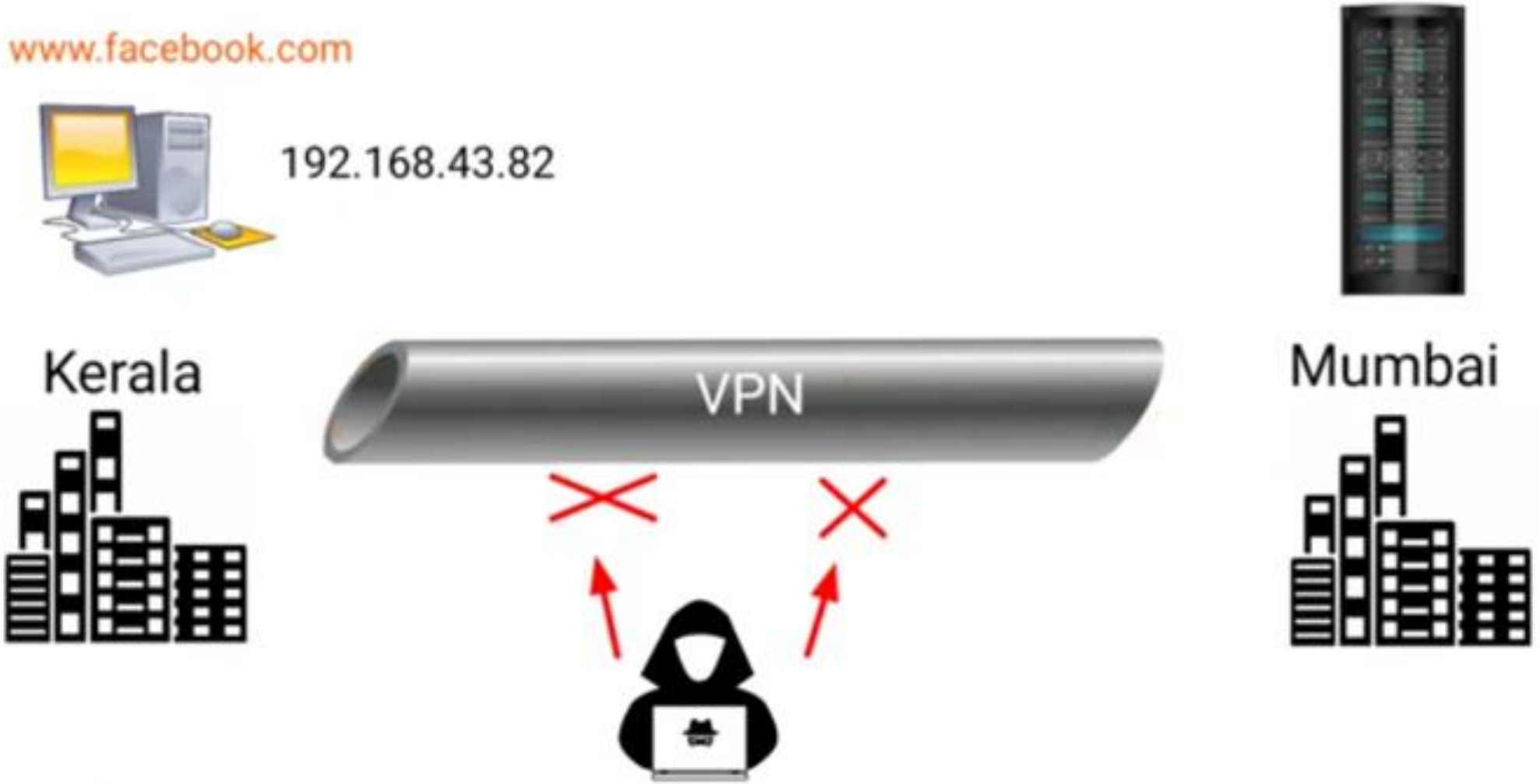


Government, Service Provider, Website

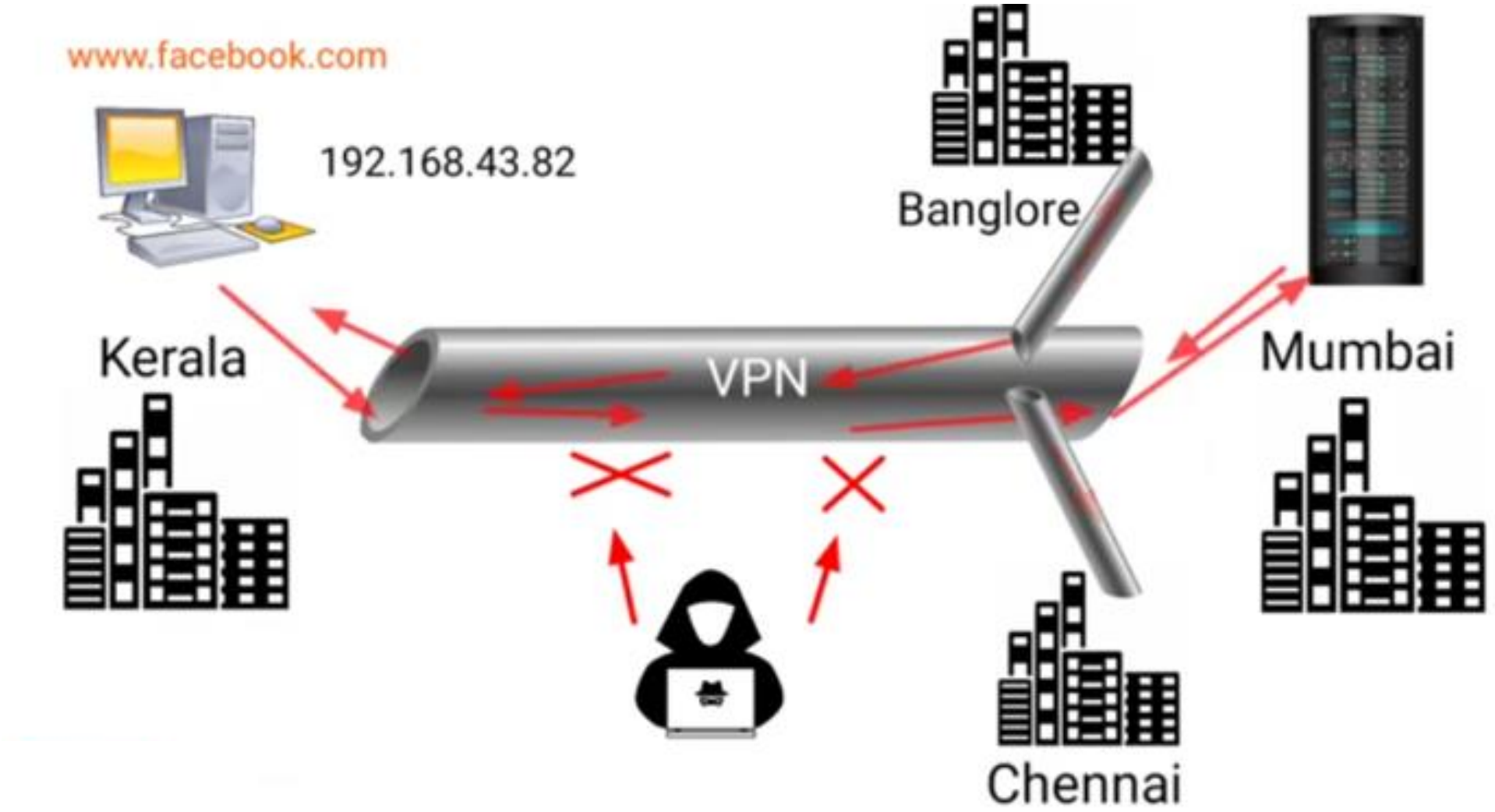
Virtual Private Network (VPN)



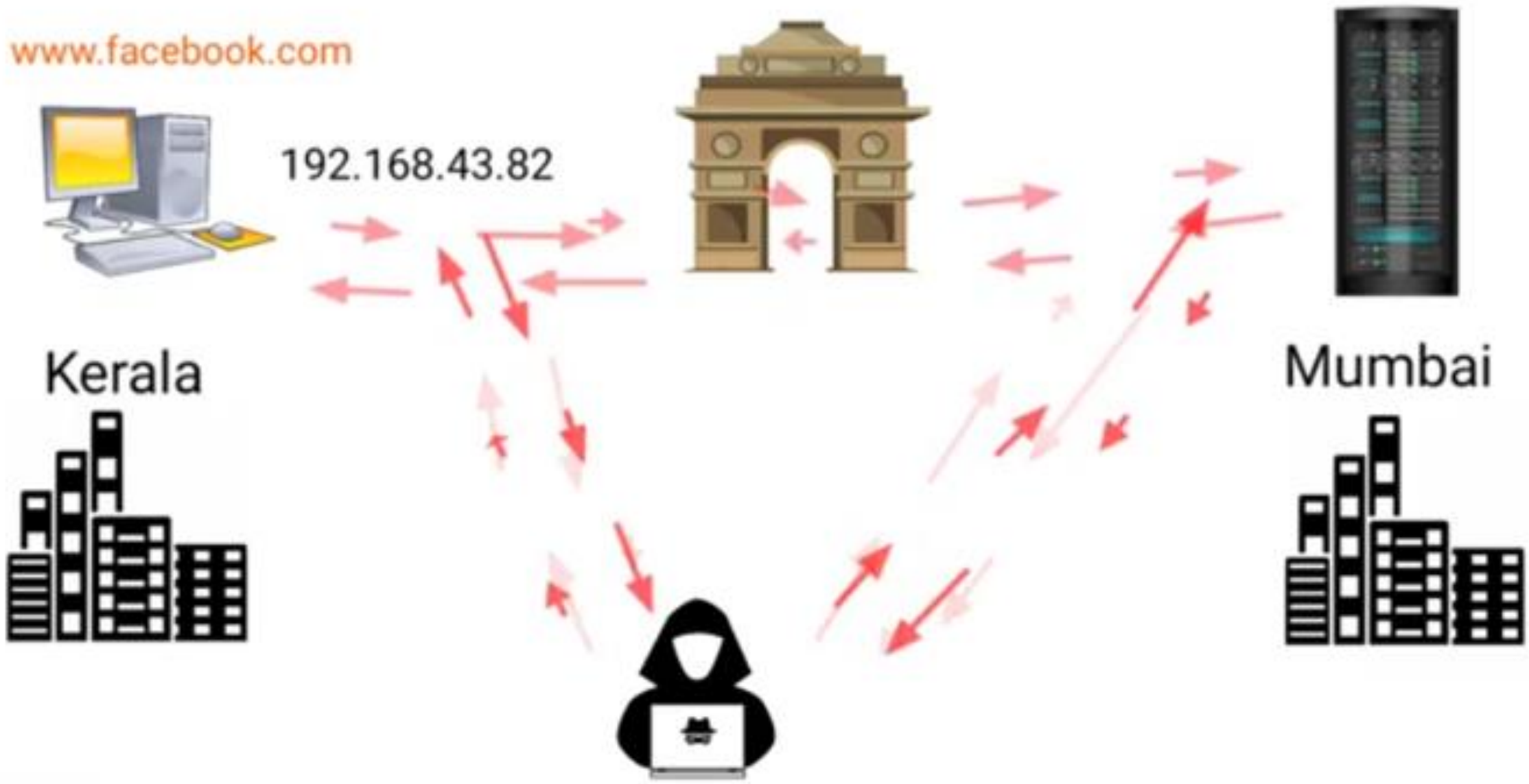
Virtual Private Network (VPN)



Virtual Private Network (VPN)

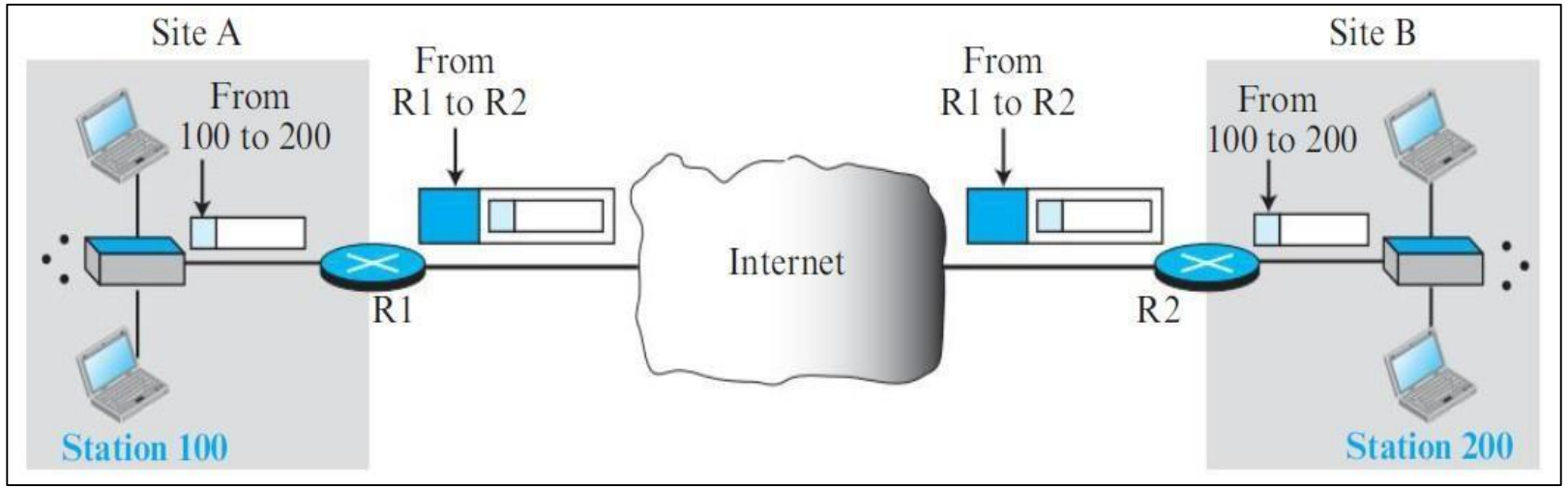


Virtual Private Network (VPN)



Virtual Private Network (VPN)

- One of the applications of IPSec is in virtual private networks.
- A virtual private network (VPN) is a technology that is gaining popularity among large organizations that use the global Internet for both intra- and interorganization communication, but **require privacy** in their intraorganization communication.
- **VPN is a network that is private but virtual.**
- It is **Private** because it guarantees privacy inside the organization.
- It is **Virtual** because it does not use real private WANs; the **network is physically public but virtually private.**



How does a VPN work?

- A VPN hides your IP address by letting the network redirect it through a specially configured remote server run by a VPN host.
- This means that if you surf online with a VPN, the **VPN server** becomes the **source** of your data.
- This means your **Internet Service Provider (ISP)** and **other third parties cannot see** which **websites you visit** or **what data you send** and **receive online.**
- A VPN **works like a filter** that turns all your data into unintelligible data.
- Even if someone were to get their hands on your data, it would be useless.

Benefits and Advantages of using a VPN

- Secure public Wi-Fi connections
- Stream regionally blocked websites and content
- Avoid censorship
- Prevent ISP tracking
- Prevent price discrimination
- Online banking security
- Online shopping security
- Unblock social media

Network Management:

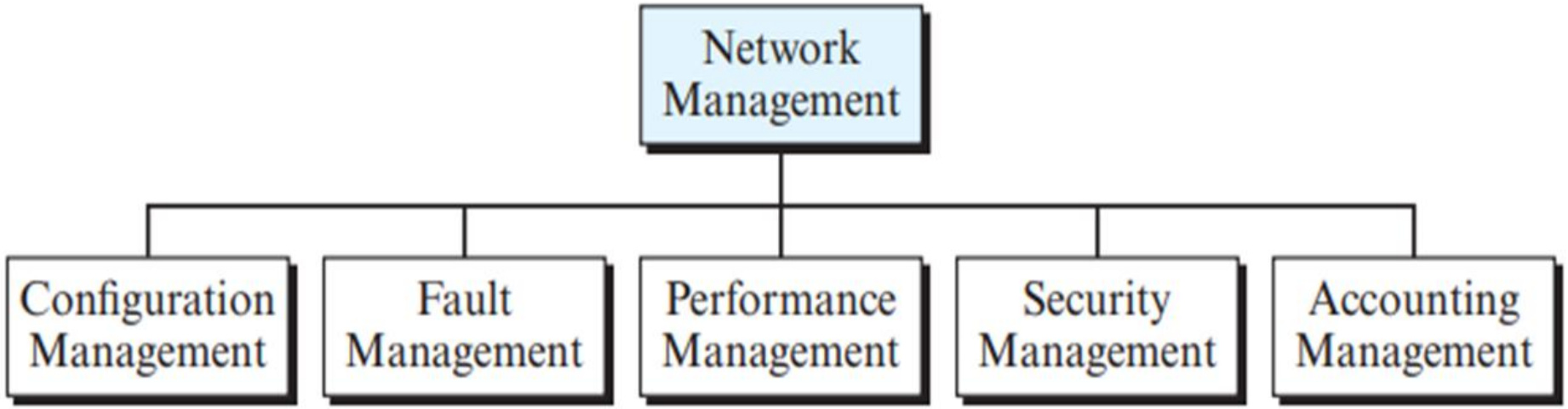
- SNMP

Virtual Private Network (VPN)

Network Management

- Network management as monitoring, testing, configuring, and troubleshooting network components to meet a set of requirements defined by an organization.
- To accomplish this task, a network management system uses hardware, software, and humans.
- The International Organization for Standardization (ISO) defines five areas of network management:
  1. Configuration management
  2. Fault management
  3. Performance management
  4. Security management, and
  5. Accounting management

Figure 9.1 *Areas of network management*



1. 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:
  i. Reconfiguration and
  ii. Documentation.
- **Reconfiguration** - Reconfiguration can be a daily occurrence in a large network. There are three types of reconfiguration:
  - Hardware reconfiguration
  - Software reconfiguration &
  - User account reconfiguration

1. Configuration Management(cntd.):

- **Hardware Reconfiguration**: covers all changes to the hardware.
  - Eg:- 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 case by case.

1. Configuration Management(cntd.):

- **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 on a system.
- We must also consider the , both as an individual and as a member of a group. adding or deleting users user privileges.
  - *Eg:- 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.
  - For example, in a college or university, at the beginning of each quarter or semester, new students are added to the system. The students are normally grouped according to the courses they take or the majors they pursue.
  - The members of each group have specific privileges;
    - computer science students may need to access a server providing different computer language facilities, while engineering students may need to access servers that provide computer assisted design (CAD) software.

1. Configuration Management(cntd.):

- **Documentation** The original network configuration and each subsequent change must be recorded meticulously.
- This means that there must be documentation for:
  i. hardware
  ii. software, and
  iii. user accounts.

1. Configuration Management(cntd.):

- 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.

i. 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. The maps use some kind of standardization to be easily read and understood by current and future personnel.

ii. Specifications Maps are not enough per se. Each piece of hardware also needs to be documented. 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.

1. Configuration Management(cntd.):

- Software Documentation: All software must also be documented. Software documentation includes information such as the software type, the version, the time installed, and the license agreement.
- User-Account Documentation: 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.

2. Fault Management:

- Complex networks today are made up of hundreds and sometimes thousands of components. Proper operation of the network depends on the proper operation of each component individually and in relation to each other.
- Fault management is the area of network management that handles this issue.
- An effective fault management system has two subsystems:
  i. Reactive Fault Management And
  ii. Proactive Fault Management.

1. Reactive Fault Management

- A reactive fault management system is responsible for detecting, isolating, correcting, and recording faults. It handles short-term solutions to faults.
- Detecting Fault
- The first step taken by a reactive fault management system is to find the exact location of the fault. A fault is defined as an abnormal condition in the system. When a fault occurs, either the system stops working properly or the system creates excessive errors.
- A good example of a fault is a damaged communication medium.

2. Fault Management(cntd..):

- Isolating Fault
- The next step taken by a reactive fault management system is isolating the fault. A fault, if isolated, usually affects only a few users. After isolation, the affected users are immediately notified and given an estimated time of correction.
- Correcting Fault
- The next step is correcting the fault. This may involve replacing or repairing the faulty components.
- Recording Fault
- After the fault is corrected, it must be documented. The record should show the exact location of the fault, the possible cause, the action or actions taken to correct the fault, the cost, and the time it took for each step

2. Fault Management(cntd..):

2. Proactive Fault Management :

- Proactive fault management tries to prevent faults from occurring.
- Although this is not always possible, some types of failures can be predicted and prevented.
- For example, if a manufacturer specifies a lifetime for a component or a part of a component, it is a good strategy to replace it before that time.
- As another example, if a fault happens frequently at one particular point of a network, it is wise to carefully reconfigure the network to prevent the fault from happening again.

3. Performance Management

- Performance management, which is closely related to fault management, tries to monitor and control the network to ensure that it is running as efficiently as possible. Performance management tries to quantify performance using some measurable quantity, such as capacity, traffic, throughput, or response time. Some protocols, such as SNMP can be used in performance management.
- Capacity
- One factor that must be monitored by a performance management system is the capacity of the network. Every network has a limited capacity and the performance management system must ensure that it is not used above this capacity.
- For example, if a LAN is designed for 100 stations at an average data rate of 2 Mbps, it will not operate properly if 200 stations are connected to the network. The data rate will decrease and blocking may occur.
- Traffic
- Traffic can be measured in two ways: internally and externally.
  i. Internal traffic is measured by the number of packets (or bytes) travelling inside the network.
  ii. External traffic is measured by the exchange of packets (or bytes) outside the network. During peak hours, when the system is heavily used, blocking may occur if there is excessive traffic.

3. Performance Management

- **Throughput**
- We can measure the throughput of an individual device (such as a router) or a part of the network. Performance management monitors the throughput to make sure that it is not reduced to unacceptable levels.
- **Response Time**
- Response time is normally measured from the time a user requests a service to the time the service is granted.
- Other factors such as capacity and traffic can affect the response time.
- Performance management monitors the average response time and the peak-hour response time. Any increase in response time is a very serious condition as it is an indication that the network is working above its capacity.

4. Security Management

- Security management is responsible for controlling access to the network based on predefined policy.
- Uses The security tools such as encryption and authentication .
- Encryption allows privacy for users;
- Authentication forces the users to identify themselves.

5. Account Management

- Accounting management is the controlling of users' access to network resources through charges.
- Under accounting management, individual users, departments, divisions, or even projects are charged for the services they receive from the network.
- Charging does not necessarily mean cash transfer;
- it may mean debiting the departments or divisions for budgeting purposes.
- Today, organizations use an accounting management system for the following ***Reasons:***

➢ It prevents users from monopolizing limited network resources.

➢ It prevents users from using the system inefficiently.

➢ Network managers can do short- and long-term planning based on the demand for network use.

SNMP (Simple Network Management Protocol)

- Several network management standards have been devised during the last few decades.
- The most important one is Simple Network Management Protocol (SNMP), used by the Internet.
- SNMP is a framework for managing devices in an internet using the TCP/IP protocol suite.
- It provides a set of fundamental operations for monitoring and maintaining an internet.
- SNMP uses the concept of manager and agent.
- A manager, usually a host, controls and monitors a set of agents, usually routers or servers.

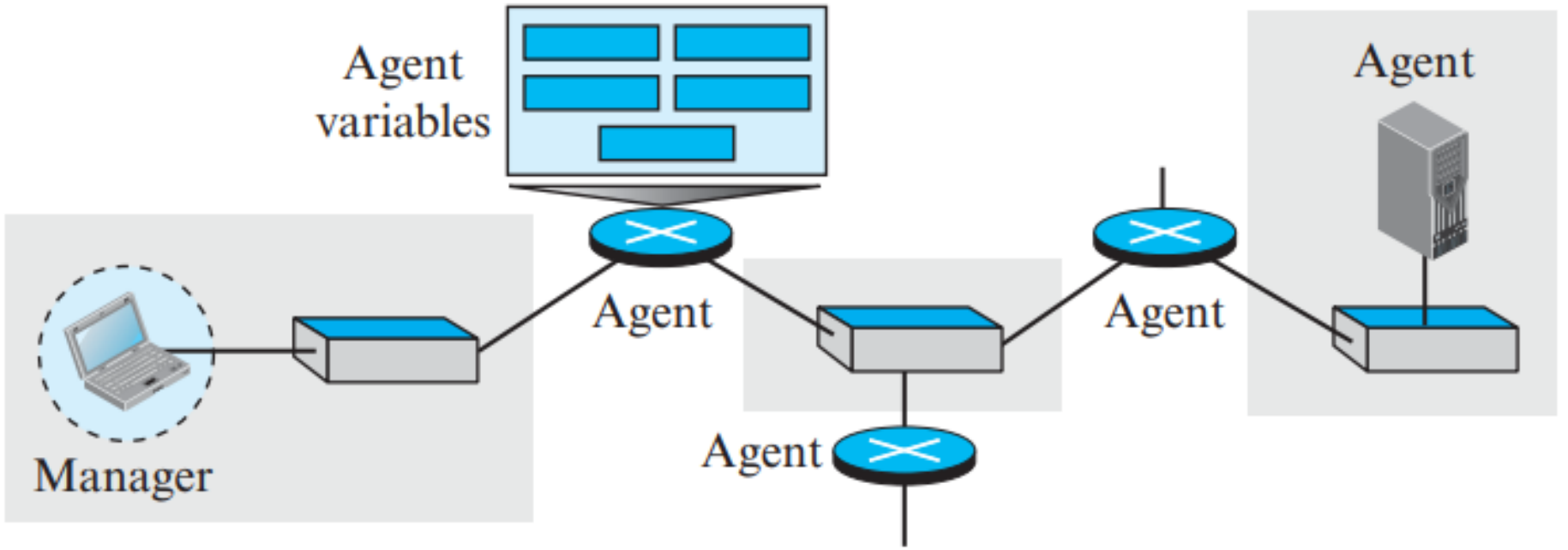
- SNMP is an application-level protocol in which a few manager stations control a set of agents.
- The protocol is designed at the application level so that it can monitor devices made by different manufacturers and installed on different physical networks.
- In other words, SNMP frees management tasks from both the physical characteristics of the managed devices and the underlying networking technology.
- It can be used in a heterogeneous internet made of different LANs and WANs connected by routers made by different manufacturers.

Simple Network Management Protocol (SNMP)

- Simple Network Management Protocol (SNMP) is an application-layer protocol for monitoring and managing network devices on a local area network (LAN) or wide area network (WAN).
- The purpose of SNMP is to provide network devices, such as routers, servers and printers, with a common language for sharing information with a network management system.
- SNMP's client-server architecture has the three following components:
  i. an SNMP Manager;
  ii. an SNMP Agent; and
  iii. a Management Information Base (MIB).

SNMP Concept

SNMP concept



- A management station, called a **Manager**, is a host that runs the SNMP client program.
  - (EG:- **Network Management Systems (NMS)**, Enterprise Monitoring Solutions: etc…)
- A managed station, called an **Agent,** is a router (or a host) that runs the SNMP server program.
- Management is achieved through simple interaction between a manager and an agent.
- The **agent** keeps **performance information** in a **database.**

- Agents can also contribute to the management process:
- The server program running on the agent can check the environment and, if it notices something unusual, it can send a warning message (called a trap) to the manager.
- Management with SNMP is based on three basic ideas:
  1. A manager checks an agent by requesting information that reflects the behavior of the agent.
  2. A manager forces an agent to perform a task by resetting values in the agent database.
  3. An agent contributes to the management process by warning the manager of an unusual situation.

SNMP components:

- There are 3 components of SNMP:

1. **SNMP Manager :**

- The SNMP manager is the central system used to monitor the SNMP network.
- Also known as a network management station (NMS), an SNMP manager is responsible for communicating with the SNMP-agent-implemented network devices.
- It runs on a host on the network.
- The manager queries the agents, gets responses, sets variables in them, and acknowledges events from them.

2. SNMP Agent:

- An SNMP agent is a software process that responds to SNMP queries to provide status and statistics about a network node.
- SNMP agents play the most important role in management.
- They are locally located and associated with SNMP network devices from which they collect, store, and transmit monitoring data.
- Data is transmitted to the designated SNMP manager when queried.
- **Managed devices** can be **network devices** like **PC, routers, switches, servers**, etc.

3. Management Information Base(MIB):

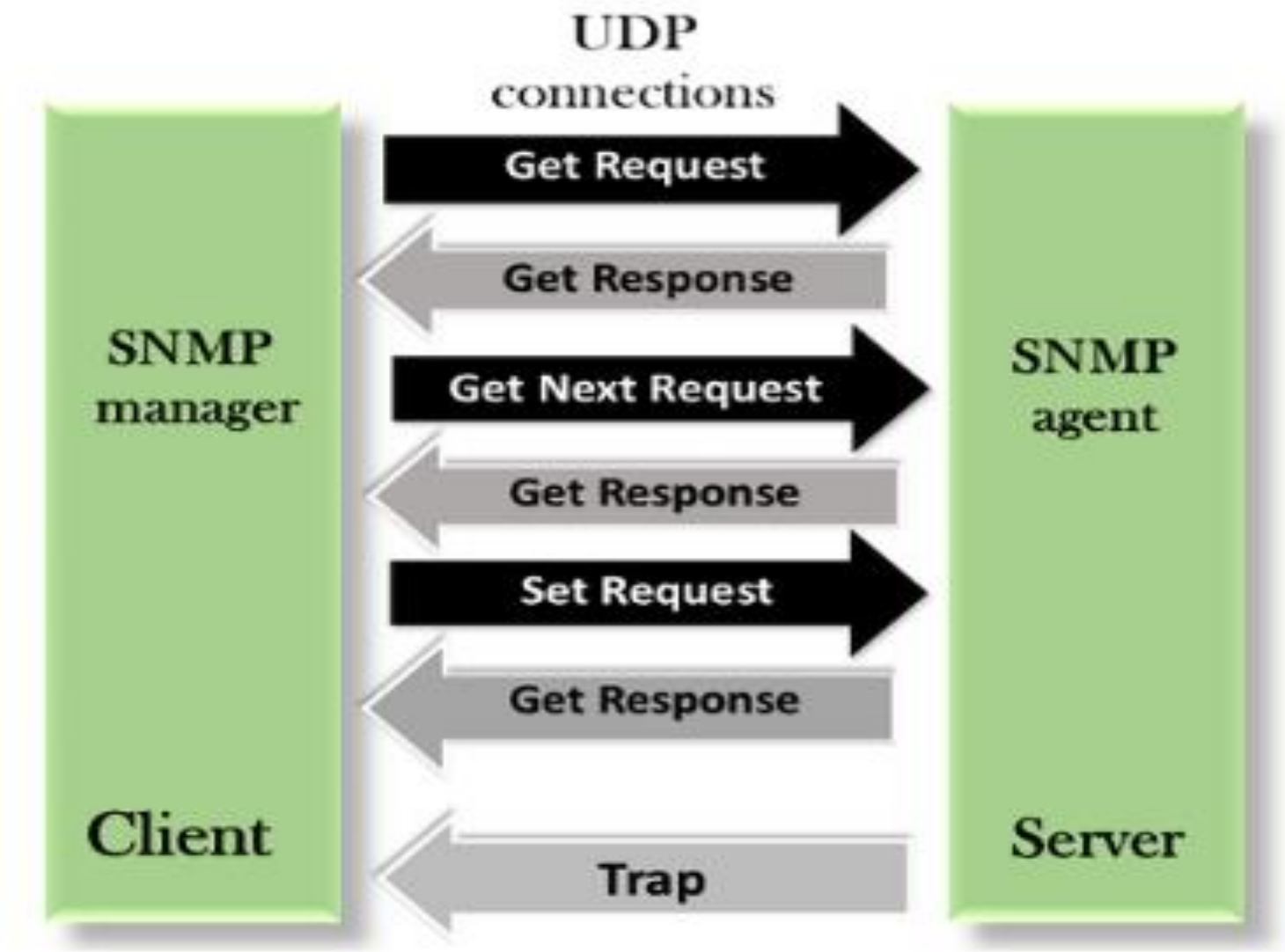
- A management information base (MIB) forms an integral part of network management models.
- An SNMP MIB is a structure that defines the format of information exchange in an SNMP system.
- Every SNMP agent maintains an information database describing the parameters of the device it manages.
- An SNMP manager is a software system that uses SNMP to collect data for fault management, performance management, and capacity planning.
- SNMP managers store collected data in a MIB as a commonly shared database between the agent and the manager.
- MIBs are saved as a text file in a specific format that MIB editors, SNMP agent builders, network management tools, and network simulation tools can understand, facilitating network building, testing, deployment, and operations.
- The managed objects in an MIB are called object identifiers (object IDs or OIDs).

Network Management - SNMP:

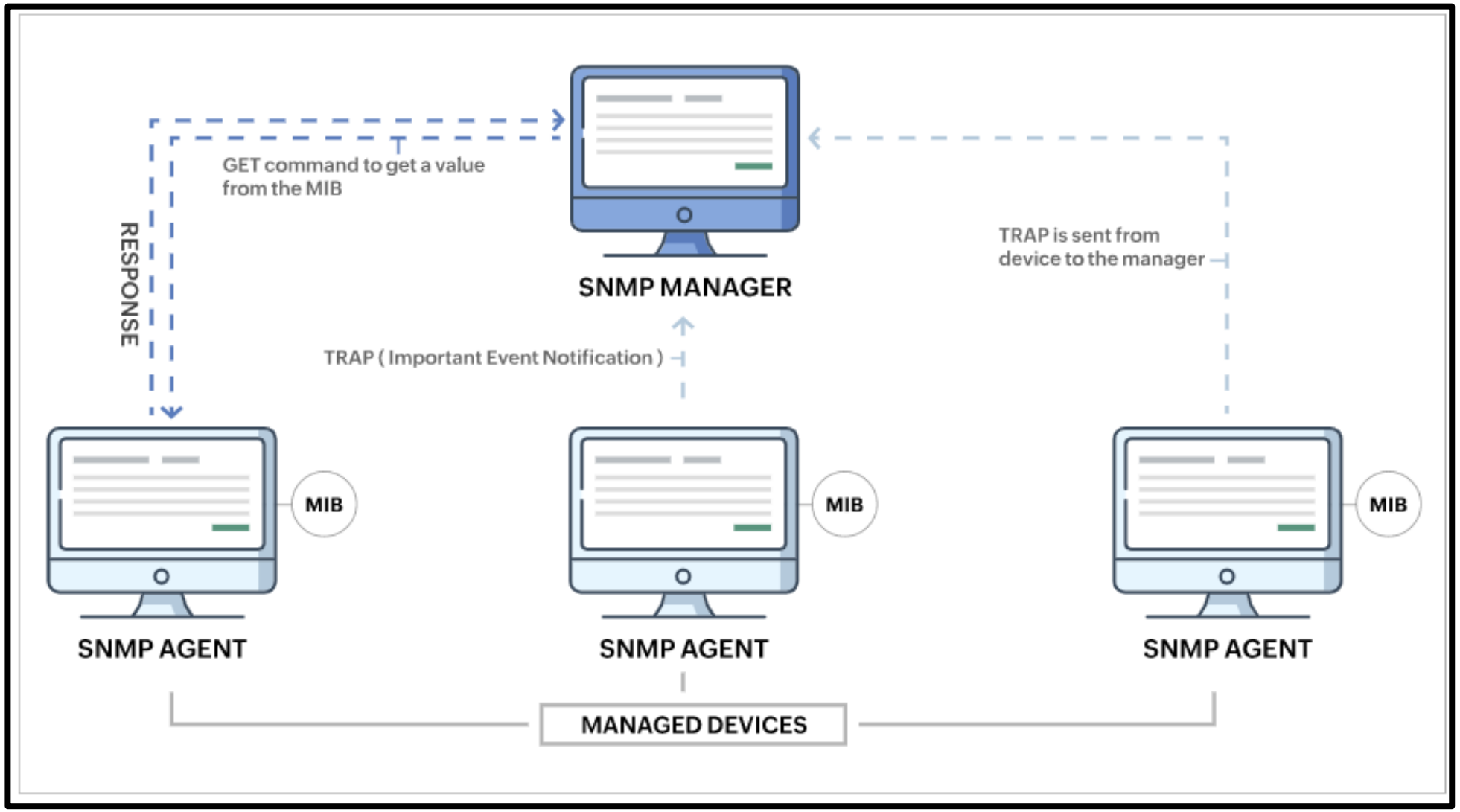
- SNMP manager acts as the client’
- SNMP agent acts as the server;
- MIB acts as the server's database.
- When the SNMP manager asks the agent a question, the agent uses the MIB to supply the answer.
- To make use of the protocol, network administrators must first change the default configuration settings of their network devices so SNMP agents can communicate with the network's management system.
- The agent is used to keep the information in a database while the manager is used to access the values in the database. For example, a router can store the appropriate variables such as a number of packets received and forwarded while the manager can compare these variables to determine whether the router is congested or not.
- Agents can also contribute to the management process. A server program on the agent checks the environment, if something goes wrong, the agent sends a warning message to the manager.

Network Management - SNMP:

- **Below are common SNMP commands:**
- **GET Request:** Generated by the SNMP manager and sent to an agent to obtain the value of a variable, identified by its OID, in an MIB.
- **GETBULK Request:** Sent by the SNMP manager to the agent to efficiently obtain a potentially large amount of data, especially large tables.
- **GETNEXT Request:** Sent by the SNMP manager to the agent to retrieve the values of the next OID in the MIB's hierarchy.
- **INFORM Request:** An asynchronous alert similar to a TRAP but requires confirmation of receipt by the SNMP manager. It was introduced in SNMPv2c, used to identify if the trap message has been received by the manager or not. The agents can be configured to send trap message continuously until it receives an Inform message. It is the same as a trap but adds an acknowledgement that the trap doesn't provide.
- **RESPONSE:** Sent by the agent to the SNMP manager, issued in reply to a GET Request, GETNEXT Request, GETBULK Request and a SET Request. Contains the values of the requested variables.
- **SET Request:** It is used by the SNMP manager to set the value of an object instance on the SNMP agent
- **TRAP:** An asynchronous alert sent by the agent to the SNMP manager to indicate a significant event, such as an error or failure, has occurred. These are the message sent by the agent without being requested by the manager. It is sent when a fault has occurred.


UDP
connections
SNMP
manager
Client
Get Request
Get Response
Get Next Request
Get Response
Set Request
Get Response
Trap
SNMP
agent
Server

SNMP - Components



Module-5: Important Questions

1. Explain Bluetooth with its architecture and layers.
2. What is a firewall? Explain.
3. Explain the piconet and scatternet architecture of Bluetooth.
4. What is the use of VPN are the techniques to guarantee privacy for organizations using VPN?
5. Explain SNMP framework for managing devices in the Internet.
6. Explain Network Address Translation.
7. What is VPN. List different types of LAN.
8. With neat diagram explain the architecture of IEEE 802.11 Wireless LAN.
9. Describe the format of IEEE 802.11. How does Multiple Access with Collision Avoidance solve the hidden node problem in Wireless LANs?
10. Explain about network threats and attacks.

Thank You