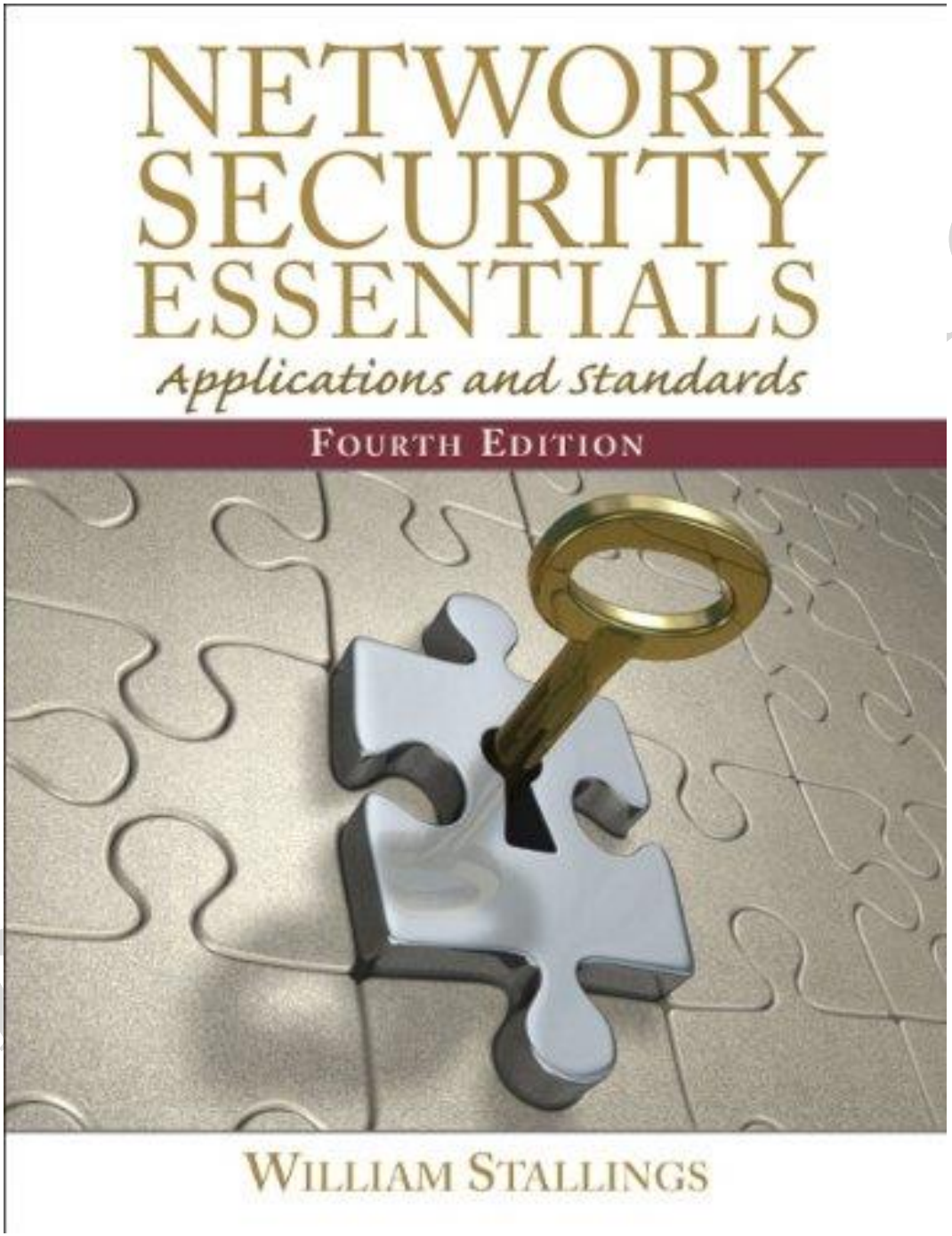
Network Security

Unit-1

Dr. Vijeta Khare

Syllabus

- ISO/OSI,
- TCP-IP,
- Networking devices: Host, Hub, Bridge, Switch, Router and its functioning,
- Perimeter devices: IDS, IPS, Firewall and its functioning.
- NOC, SOC, SIEM,
- Servers: DNS, DHCP, Proxy, Mail and Application servers.
- Threat, vulnerability, attack surface, attack vector, exploit.
- Common attacks and countermeasures: Phishing attack, ARP poising, MAC flooding, DoS and DDoS.


NETWORK SECURITY ESSENTIALS
Applications and Standards
FOURTH EDITION
WILLIAM STALLINGS

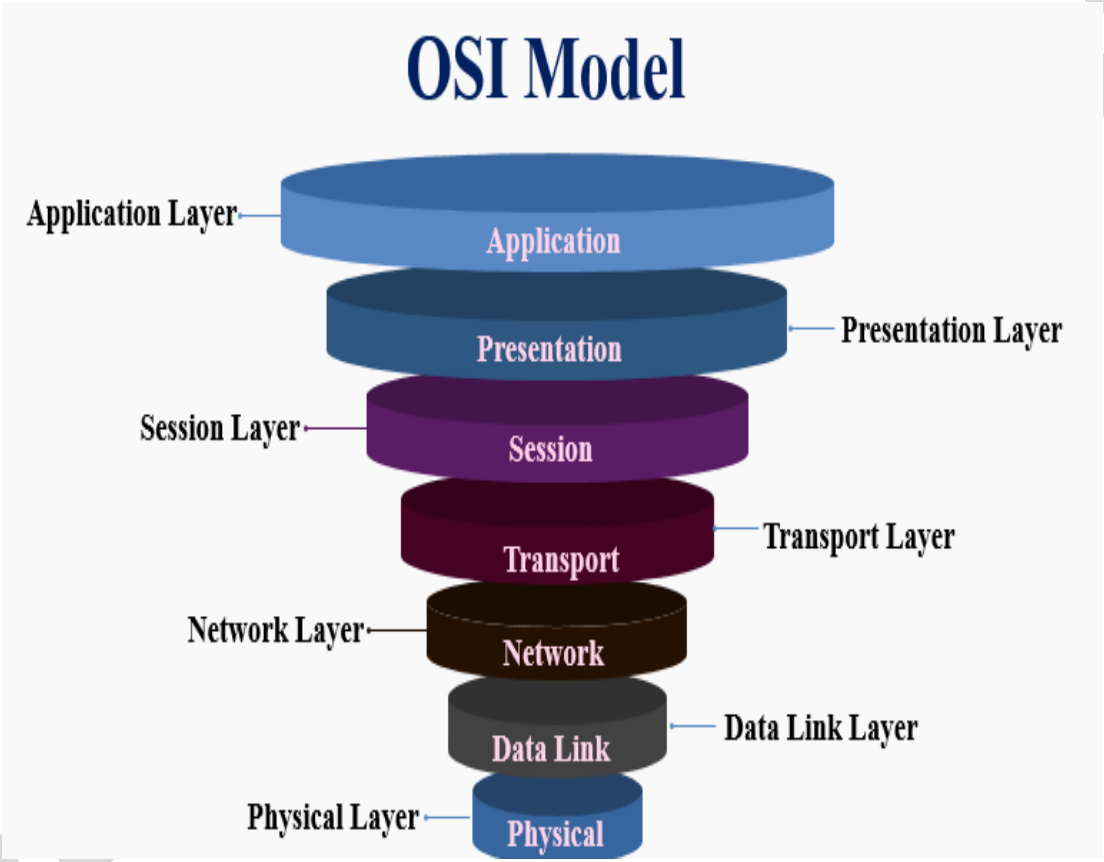
OSI REFRENCE MODEL

OPEN SYSTEM INTERCONNECTION REFERENCE MODEL (OSI REFERENCE MODEL OR OSI MODEL)

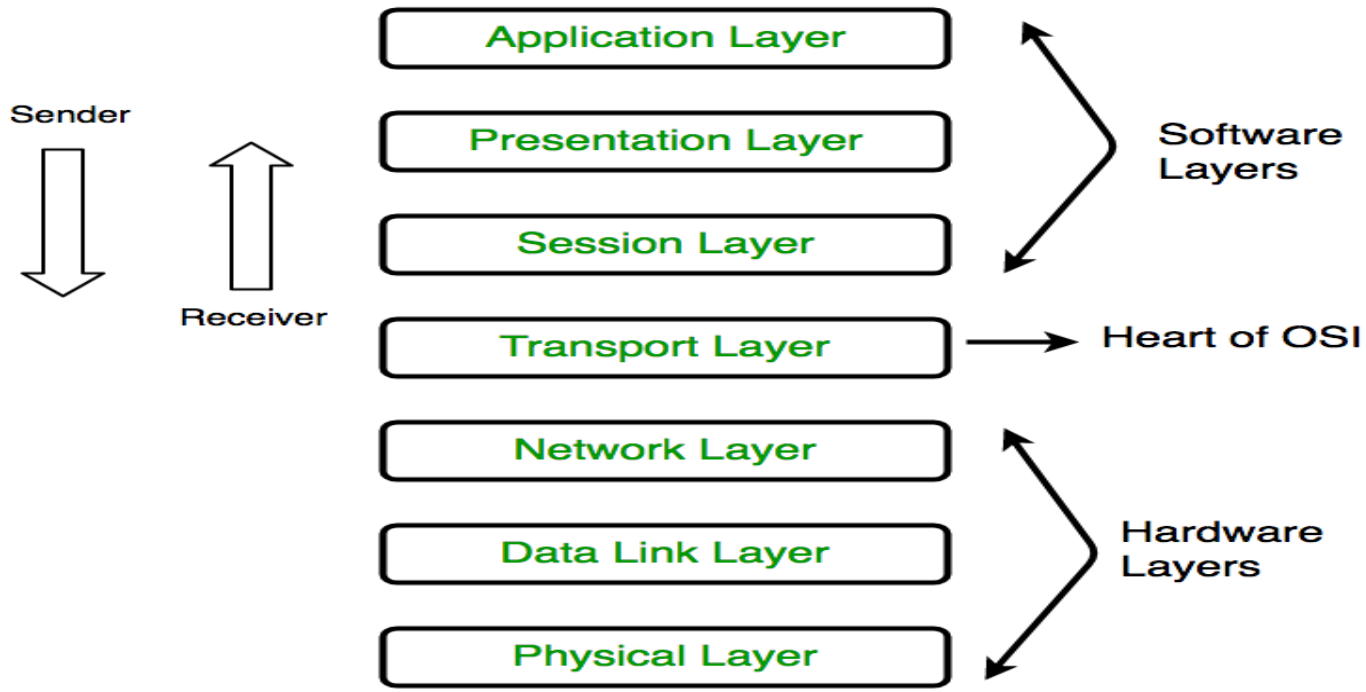
- ✓ The **Open System Interconnection Reference Model** (OSI Reference Model or **OSI Model**) is a description for layered communications and computer network protocol & transmission design.
- ✓ It divides data movement into seven layers which, from top to bottom, are the Application, Presentation, Session, Transport, Network, Data Link, and Physical Layers.
- ✓ It is therefore often referred to as the **OSI Seven Layer Model**.
- ✓ In 1978, the International Standards Organization (ISO) began to develop its OSI framework architecture.
- ✓ The concept of a 7 layer model was provided by the work of Charles Bachman, then of Honeywell.
- ✓ Various aspects of OSI design evolved from experiences with the Advanced Research Projects Agency Network (ARPANET) and the fledgling Internet.

OSI- OPEN SYSTEMS INTERCONNECTION

- ✓Conceptual model.
- ✓It characterises and standardises the communication function of a telecommunication or computing system.
- ✓The rules of communication.
- ✓A blue print of network.
- ✓ISO(International Organisation for Standardisation)- 1984.
- ✓Seven layer model.
- ✓Each layer is a package of protocol.
- ✓Specified in ISO 7498.


OSI Model
Application Layer
Application
Presentation
Presentation Layer
Session Layer
Session
Transport
Transport Layer
Network Layer
Network
Data Link
Data Link Layer
Physical Layer
Physical

OSI MODEL


Application Layer
Presentation Layer
Session Layer
Transport Layer
Network Layer
Data Link Layer
Physical Layer
Sender
Receiver
Software Layers
Heart of OSI
Hardware Layers

OSI LAYERS

OSI Model			
	Data unit	Layer	Function
Host layers	Data	7. Application	Network process to application
		6. Presentation	Data representation, encryption and decryption
		5. Session	Interhost communication
	Segments	4. Transport	End-to-end connections and reliability, Flow control
Media layers	Packet	3. Network	Path determination and logical addressing
	Frame	2. Data Link	Physical addressing
	Bit	1. Physical	Media, signal and binary transmission

APPLICATION LAYER

- ✓ Used by Network Applications.
- ✓ Web browsers, Skype, Outlook etc.
- ✓ All network Applications and network services.
- ✓ Protocols:-
  - ✓ HTTP(Hypertext Transfer Protocol)
  - ✓ HTTPS (Hypertext Transfer Protocol secure)
  - ✓ FTP (File Transfer Protocol)
  - ✓ NFS (Network File System- to access remote data)
  - ✓ DHCP(Dynamic Host Configuration Protocol)
  - ✓ SMTP(Simple Mail Transfer Application)
  - ✓ TELNET(Teletype Network Protocol- NW virtual telecom protocol)
  - ✓ POP3(Post Office Protocol ver 3- mail protocol for Rx mail)
  - ✓ IMAP(Internet Message Access Protocol- mail protocol for Rx mail)
  - ✓ IRC(Internet Relay Chat protocol)
  - ✓ NNTP(Network News Transfer Protocol- distributed, inquiry, retrieval & posting of new article.

PRESENTATION LAYER

- ✓Performs three functions(Translation, Compression & Encryption/Decryption).
- ✓Translation.
  - ✓Characters/Nos to machine understandable binary format).
  - ✓ASCII(American Standard Code for Information Interchange) to EBCDIC(Extended Binary Coded Decimal Interchange Code)
- ✓Data Compression.
  - ✓Technique for bit reduction.
  - ✓Two methods- Lossy & Lossless.
  - ✓Data txn can be done faster.
- ✓Encryption.
  - ✓SSL(Secure Socket layer- NW protocol for securing comn between web client and web server).

SESSION LAYER

- ✓ Helps in setting up & managing connection or session and termination.
- ✓ APIs setup sessions(eg NetBIOS).
- ✓ Session Establishment- Authentication & Authorisation.
  - ✓ Authentication(who are you?- User name & Password).
  - ✓ Authorisation(to access file).
- ✓ Session Management.
  - ✓ Page management is done by session management(Server stores image and text contents separately- which data packet belongs to text & image and put it together on client side).
- ✓ Summary- Session layer helps in:-
  - ✓ Session management.
  - ✓ Authentication.
  - ✓ Authorisation.
- ✓ Web browser performs all functions of Application, Presentation & session layer.

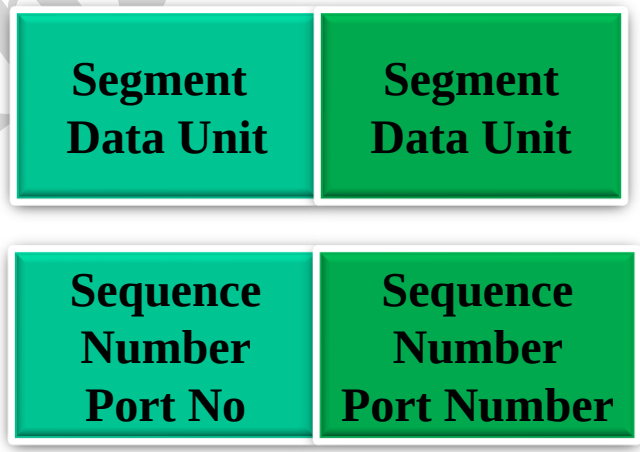
TRANSPORT LAYER

- ✓ Maintains reliability of comn (through segmentation, flow control and error control).
- ✓ Data received from session layer is divided into segments- small data units are called segments.
  - ✓ Each segment contains source & destination port number.
  - ✓ Port No. helps to direct each segment to correct Appl.
  - ✓ Sequence No. helps to reassemble the segment in correct order to form correct message at Rxr.
- ✓ Flow Control.
  - ✓ Controls amount of data being transmitted.
  - ✓ Data txn rate can incr/decrease based on the request of Rxr.
- ✓ Error Control.
  - ✓ If some data doesn't arrive at destination, Automatic repeat request to retransmit the loss or corrupted data.
  - ✓ A group of bit called checksum is added to each segment to find out the Rxd corrupted segment.

TRANSPORT LAYER

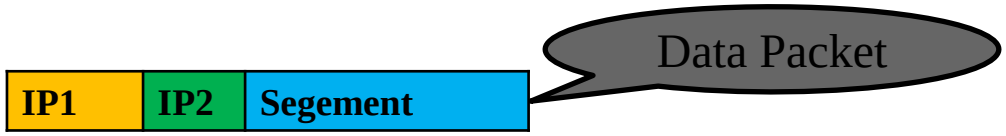
- ✓ Services
  - ✓ Connection oriented Transmission(TCP).
    - ✓ Feedback.
    - ✓ www, email, FTP protocol etc.
  - ✓ Connectionless Transmission(UDP).
    - ✓ No feedback.
    - ✓ Video, games, VOIP, DNS protocols etc.
- ✓ Summary- Transport layer is involved in:-
  - ✓ Segmentation.
  - ✓ Flow control.
  - ✓ Error control.
  - ✓ Connection oriented/Connectionless Txn.

  * Transport layer passes on segment to Network layer.



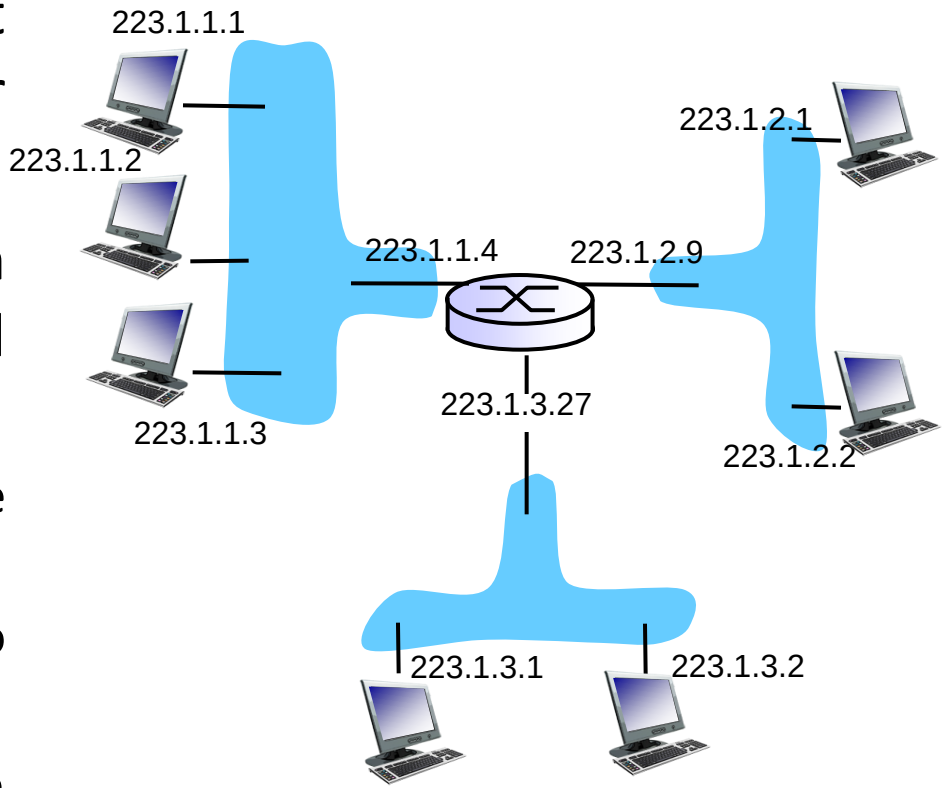
NETWORK LAYER

- ✓ Works for transmission of data segment from one computer to another computer located in another NW group or different NW.
- ✓ Data units in a network are called packets.
- ✓ It is the layer where Router resides.
- ✓ NW layer performs three important functions:-
  - ✓ Logical Addressing.
  - ✓ Routing.
- ✓ Logical Addressing.
  - ✓ IP addressing done at NW layer is called logical addressing(Ipv 4 or Ipv 6).
  - ✓ Every computer in Network has unique IP address.
  - ✓ NW layer assigns sender & reciever IP Add to each segment to home an IP packet.
  - ✓ IP Addresses are assigned to ensure that each data packet reaches correct destination.



IP Addressing - Example

- **IP address:** It is 32-bit identifier for host, router interface
- **Interface:** It is a connection between host/router and physical link.
  - ✓ A router's typically have multiple interfaces
  - ✓ A host typically has one or two interfaces
- IP addresses associated with each interface.



223.1.1.1 = 11011111 00000001 00000001 00000001

223 1 1 1

IP Address

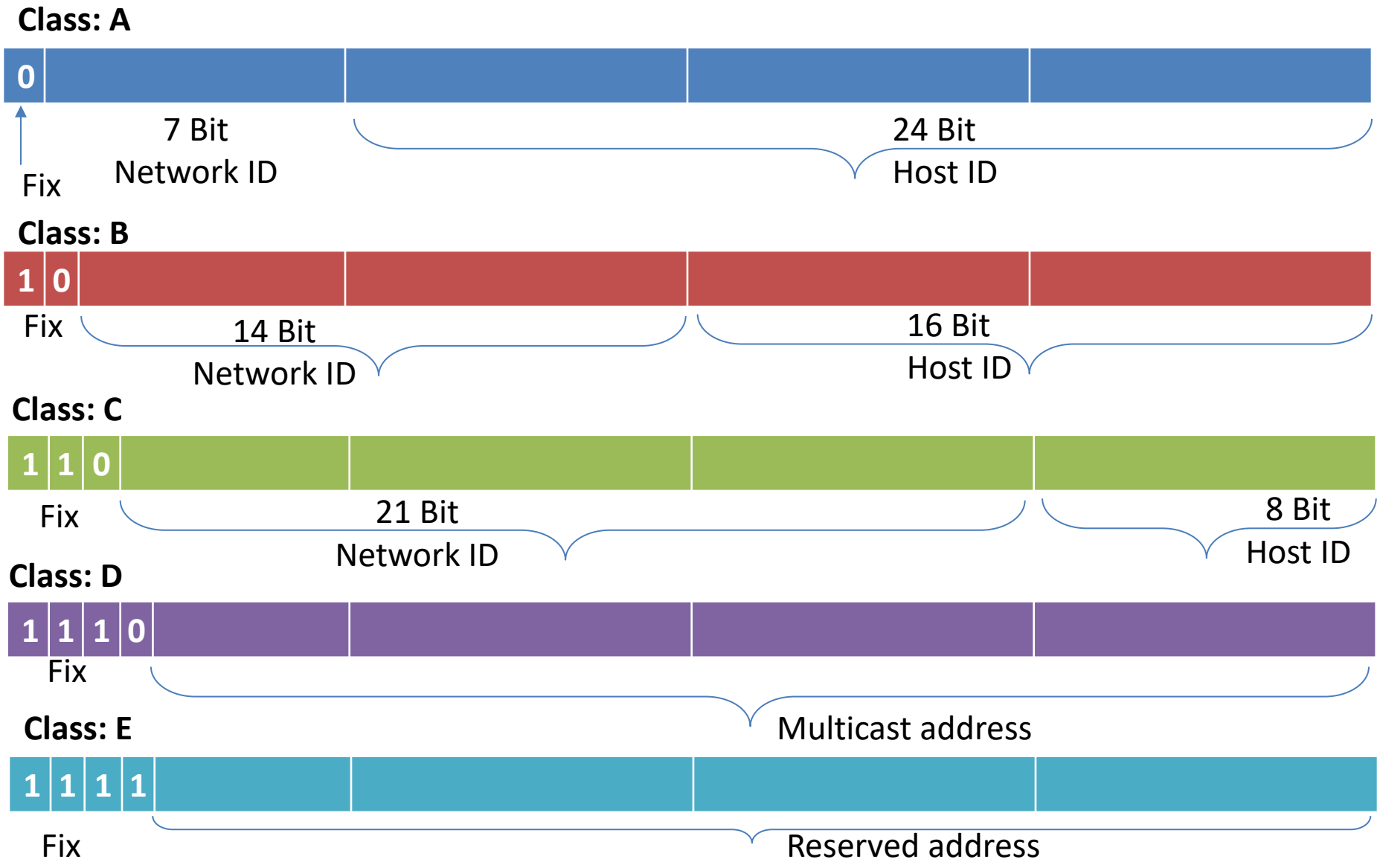
- IP addresses are useful in identifying a specific host in a network.
- IP addresses are 32 bit numbers which are divided into 4 octets. Each octet represents 8 bit binary number.
- Below is an example of an IP address:

10101100	00010000	11111110	00000001
172	**16**	**254**	**1**

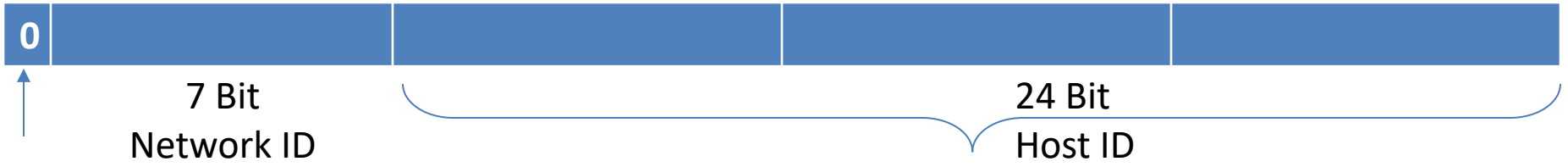
IP addresses are divided into 2 parts:
Network ID & Host ID

<NID> <HID> = IP Address

Classification of IP Addresses (Classful Addressing)



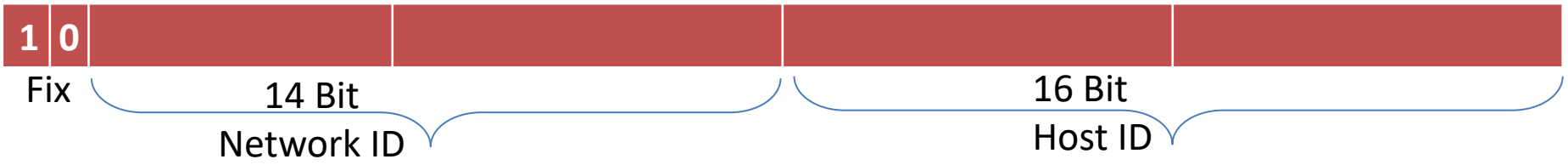
Class A: Range(0.0.0.0 to 127.255.255.255) Dotted decimal notation



- Only 126 addresses are used for network address.
- All 0's and 1's in Network-ID are dedicated for special IP address.
  So, total number of IP address in class A can be represented:

0.0.0.0	Special IP Address
00000001.0.0.1 1.0.0.2 1.0.0.3 . . . 126.255.255.254	$2^{24} - 2$ are Host IP
127.255.255.255	Special IP Address – Loopback

Class B: Range (128.0.0.0 to 191.255.255.255)



128.0.0.0	Special IP Address
10000001.0.0.1 130.0.0.2 130.0.0.3 . . . 190.255.255.254	2^{16} – 2 are Host IP
10111111.255.255.255	Special IP Address – Loopback

Class C: Range(192.0.0.0 to 223.255.255.255)

192.0.0.0	Special IP Address
11000001.0.0.1 194.0.0.2 194.0.0.3 . . . 222.255.255.254	2^8 – 2 are Host IP
11011111.255.255.255	Special IP Address – Loopback

Class D: Range (224.0.0.0 to 239.255.255.255)

- Very first four bits of the first octet in Class D IP addresses are set to 1110, giving a range of:

11100000 – **1110**1111
224 – 239

- Class D has IP address rage from 224.0.0.0 to 239.255.255.255.
- Class D is reserved for Multicasting.
- In multicasting data is not destined for a particular host, that is why there is no need to extract host address from the IP address, and Class D does not have any subnet mask.

Class E: (240.0.0.0 to 255.255.255.255)

- This IP Class is reserved for experimental purposes only for R&D or Study.
- IP addresses in this class ranges from 240.0.0.0 to 255.255.255.254.
- Like Class D, this class too is not equipped with any subnet mask.

Type of addresses in IPv4 Network

- **Network address** - The address by which we refer to the network.
  - ✓ E.g.: 10.0.0.0
- **Broadcast address** - A special address used to send data to all hosts in the network.
  - ✓ The broadcast address uses the highest address in the network range.
  - ✓ E.g.: 10.0.0.255
- **Host addresses** - The addresses assigned to the end devices in the network.
  - ✓ E.g.: 10.0.0.1

Subnets

- Problem: need to break up large A and B classes
- Solution: add another layer to the hierarchy
  - ✓ From the outside, appears to be a single network
    - Only 1 entry in routing tables
  - ✓ Internally, manage multiple subnetworks
    - Split the address range using a subnet mask

Subnet Mask: 11111111 11111111 11000000 00000000

Subnet Example

- Extract network:

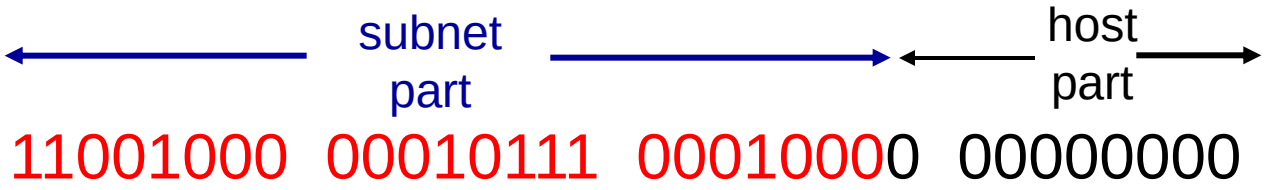
```
   IP Address:  10110101 11011101 01010100 01110010
Subnet Mask:  & 11111111 11111111 11000000 00000000
-------------------------------------------------------
      Result:  10110101 11011101 01000000 00000000
```

- Extract host:

```
   IP Address:  10110101 11011101 01010100 01110010
Subnet Mask: & ~(11111111 11111111 11000000 00000000)
-------------------------------------------------------
      Result:  00000000 00000000 00010100 01110010
```

Classless Inter-Domain Routing(CIDR)

- CIDR is a slash notation of subnet mask. CIDR tells us number of on bits in a network address.



200.23.16.0/23

- A single IP address can be used to designate many unique IP addresses with CIDR.
- A CIDR IP address looks like a normal IP address except that it ends with a slash followed by a number, called the IP network prefix.
- CIDR addresses reduce the size of routing tables and make more IP addresses available within organizations.

Data Link Layer

- Data link layer is concerned with:
  - Framing – divide bits stream into data unit (frame)
  - Physical addressing
  - Flow control – avoid over overwhelming
  - Error control – bit loses, retransmission
  - Access control

  - Data link layer attempts to provide reliable communication over the physical layer interface.
  - Breaks the outgoing data into frames and reassemble the received frames.
  - Create and detect frame boundaries.
  - Handle errors by implementing an acknowledgement and retransmission scheme.
  - Implement flow control.
  - Supports points-to-point as well as broadcast communication.
  - Supports simplex, half-duplex or full-duplex communication.

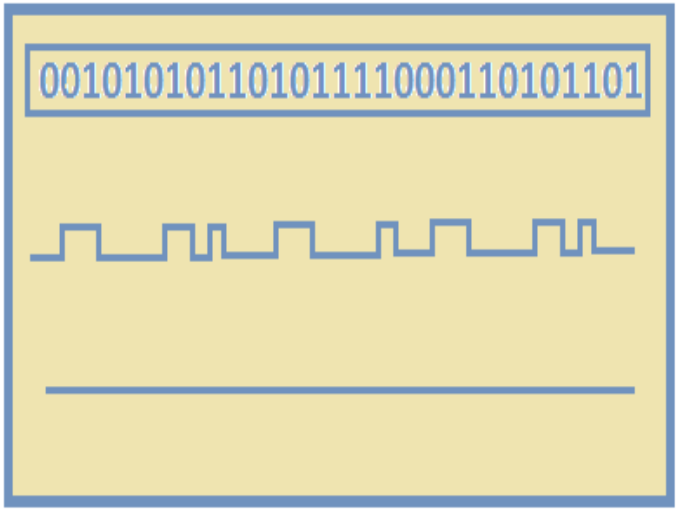
Physical Layer

- Carries the bit stream over a physical media.
- Physical Layer is concerned with:
  - Interface and Medium like guided cables
  - Representation of bits
  - Data rate
  - Synchronization of bits
  - Line configuration
  - Physical topology
  - Transmission mode

  - Provides physical interface for transmission of information.
  - Defines rules by which bits are passed from one system to another on a physical communication medium.
  - Covers all - mechanical, electrical, functional and procedural - aspects for physical communication.
  - Such characteristics as voltage levels, timing of voltage changes, physical data rates, maximum transmission distances, physical connectors, and other similar attributes are defined by physical layer specifications.

PHYSICAL LAYER

Physical layer process: encoding and signaling



Encoding

Signaling

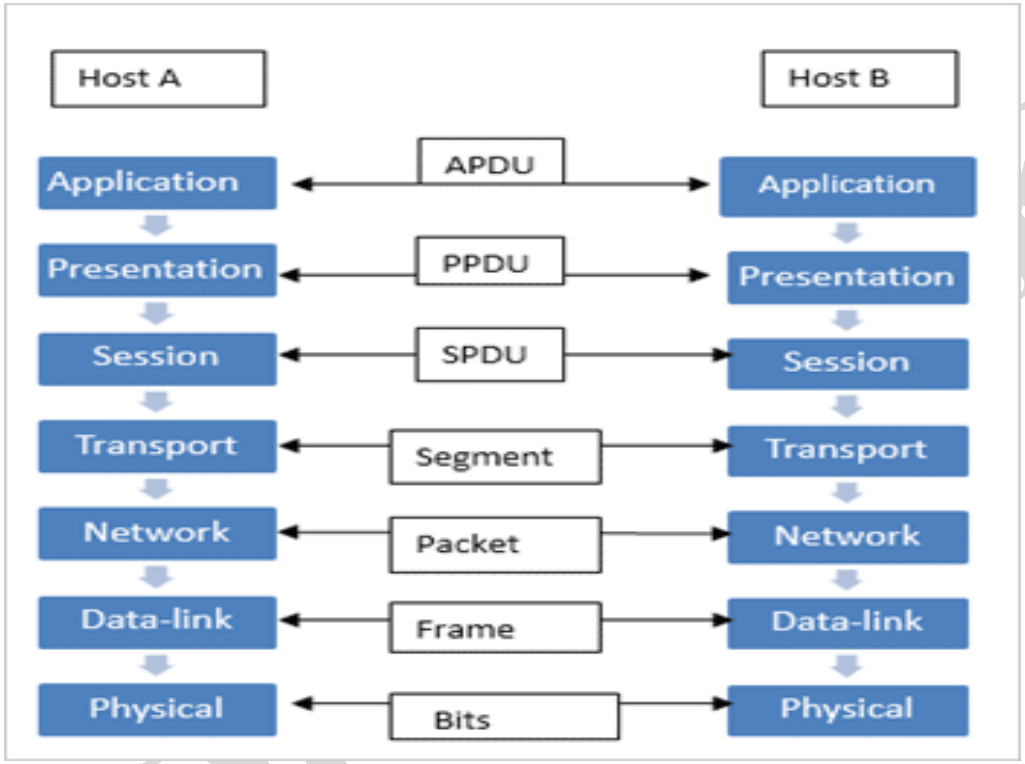
Media

1. Frames are
2. encoded
3. signaled

then trasmitted through media e.g. cables (copper, fiber optics, coaxial)

- ✓ Physical Layer converts binary segment into signal and transmit over media.

RELATIONSHIP BETWEEN EACH LAYER

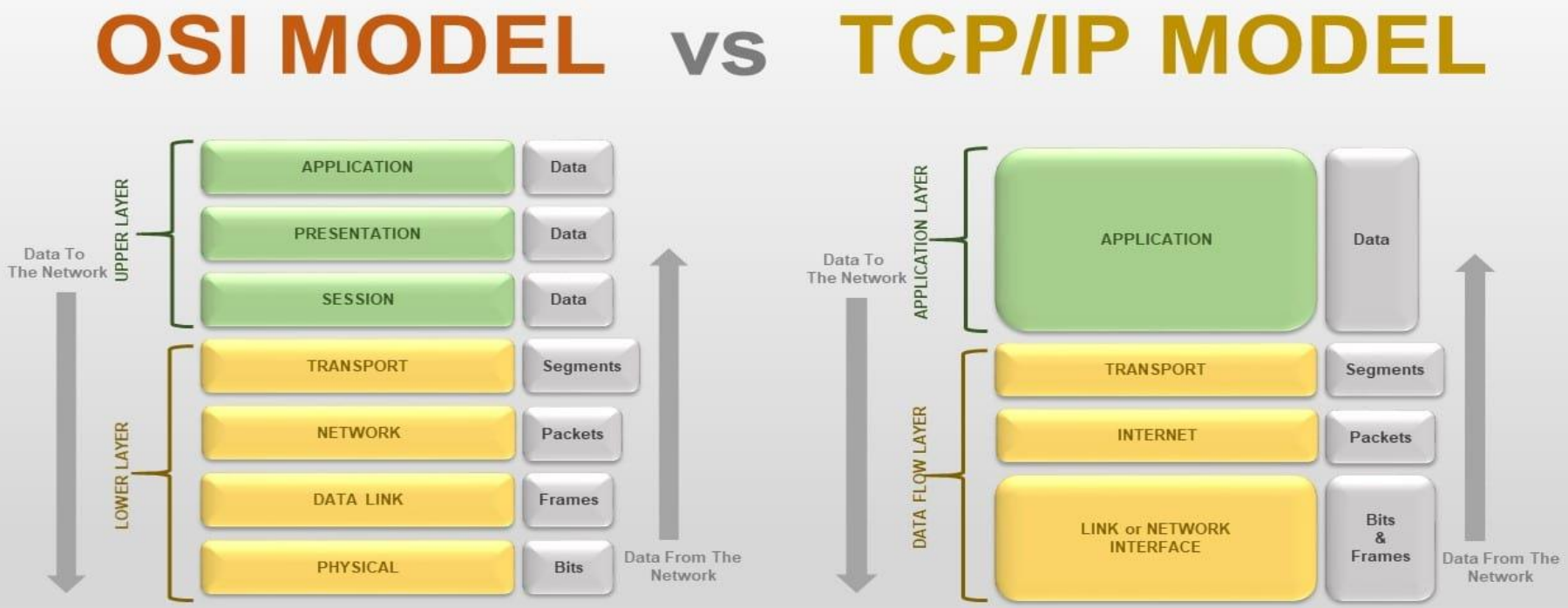


Protocol Unit exchanged between the Layers

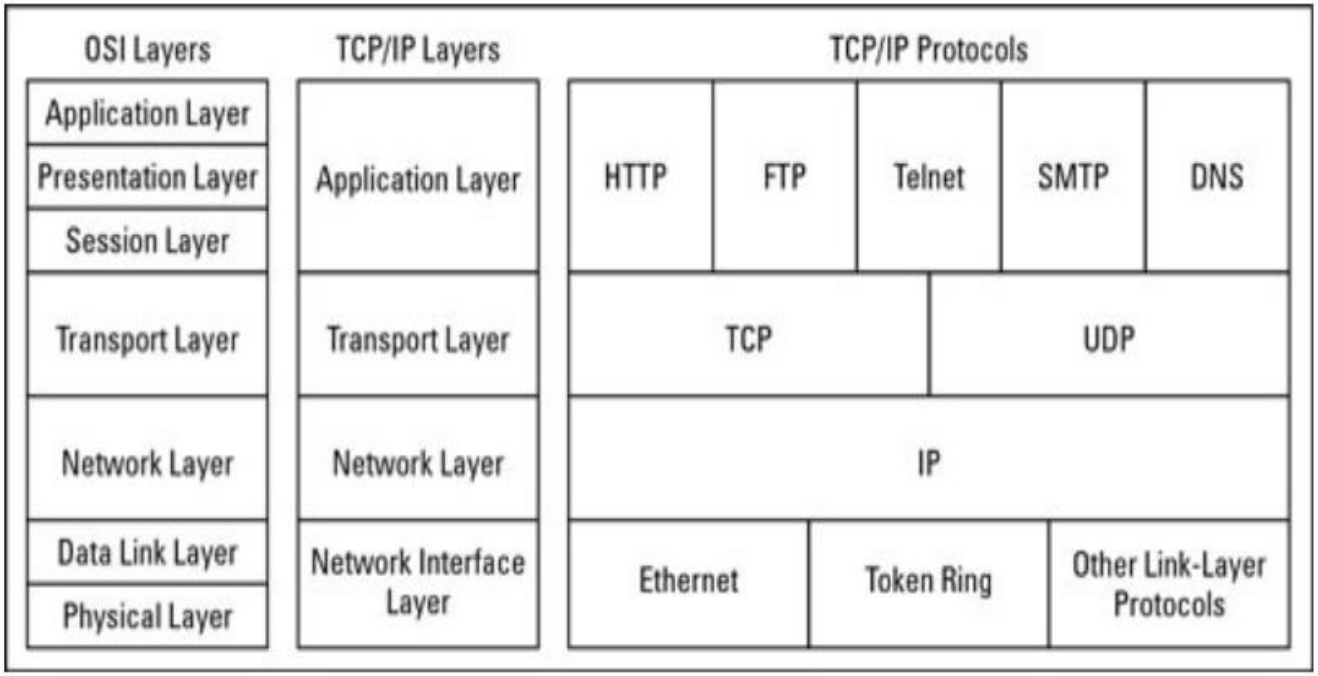
APDU– Application protocol data unit.
PPDU– Presentation protocol data unit.
SPDU– Session protocol data unit.
TPDU– Transport protocol data unit (Segment).
Packet– Network layer host-router protocol.
Frame– Data-link layer host-router protocol.
Bits– Physical layer host-router protocol.

* Encapsulation- process of adding header or trailer at each layer of OSI
* PDU- consists of layer n control info & layer n+1 encapsulated data for each layer

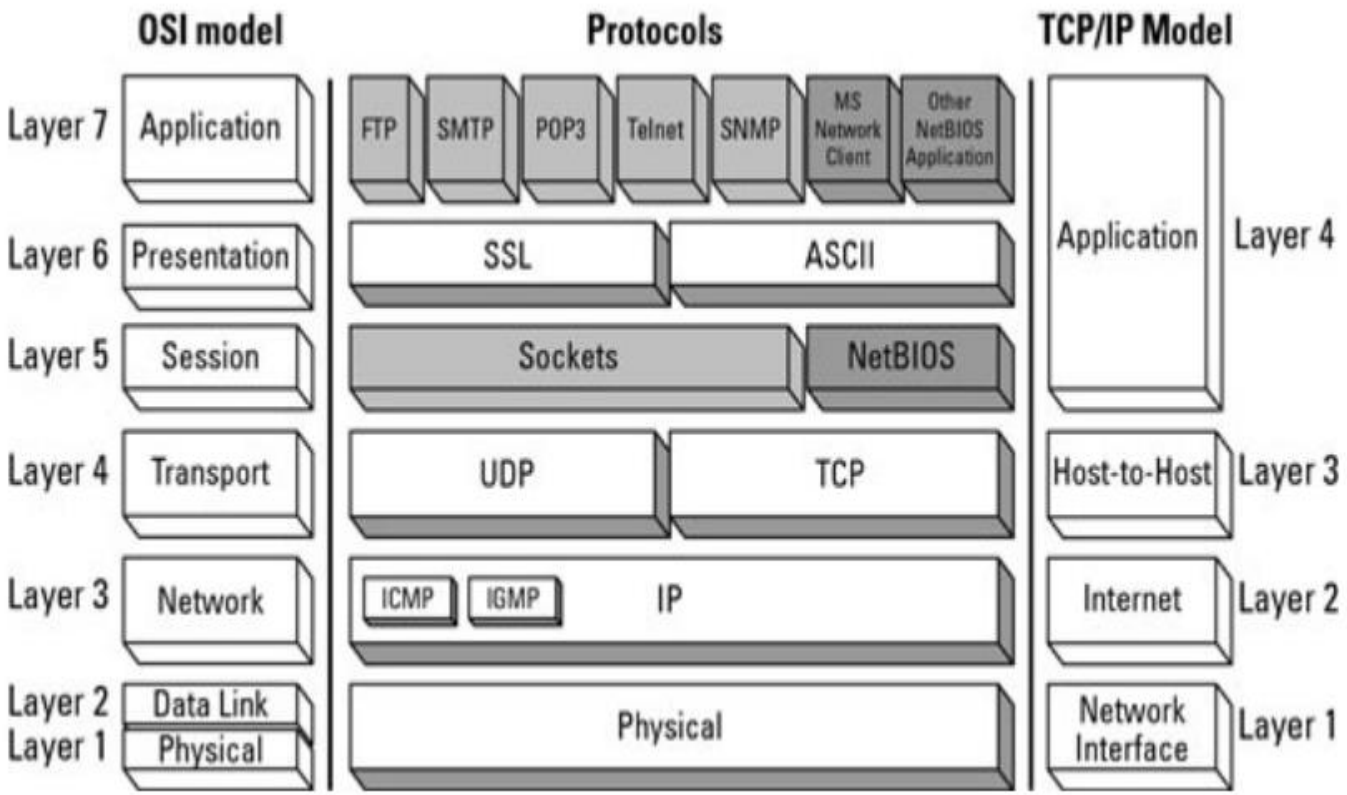
OSI VS TCP IP MODEL



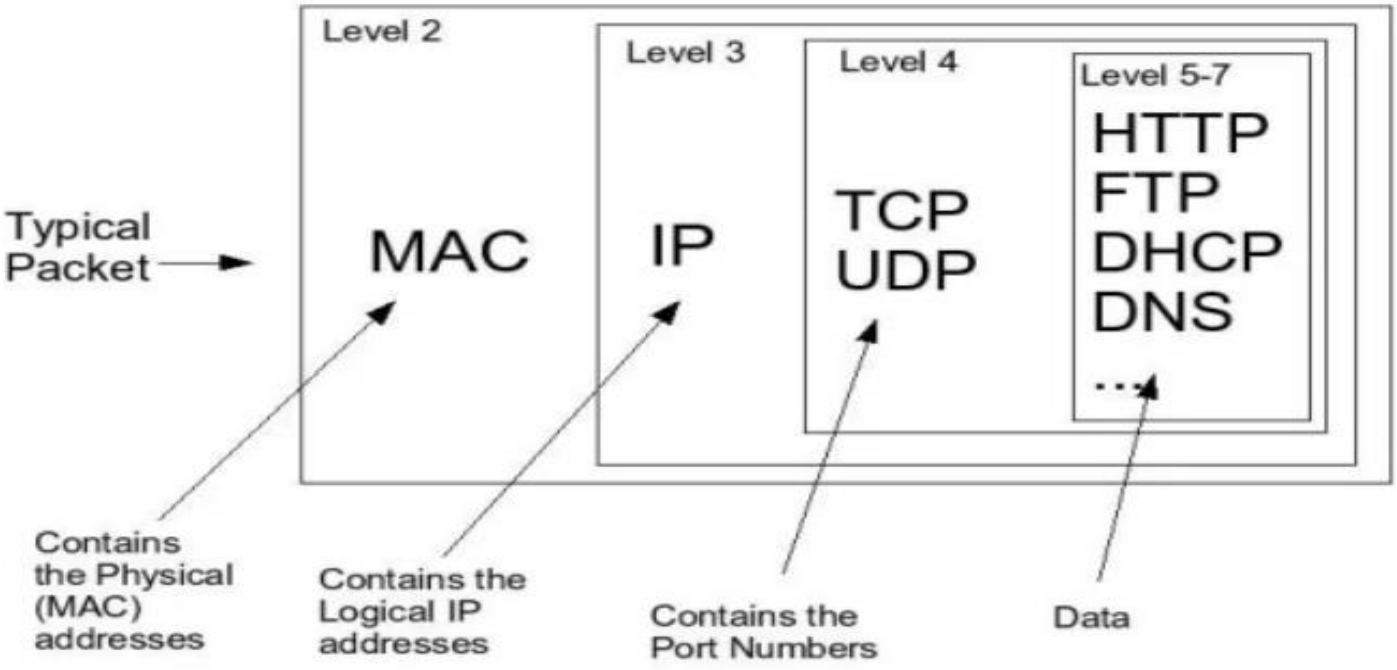
OSI Vs TCP/IP



RELATIONSHIP BETWEEN THE OSI MODEL AND THE TCP/IP MODEL



Basics of TCP/IP Network Packet



Information Security

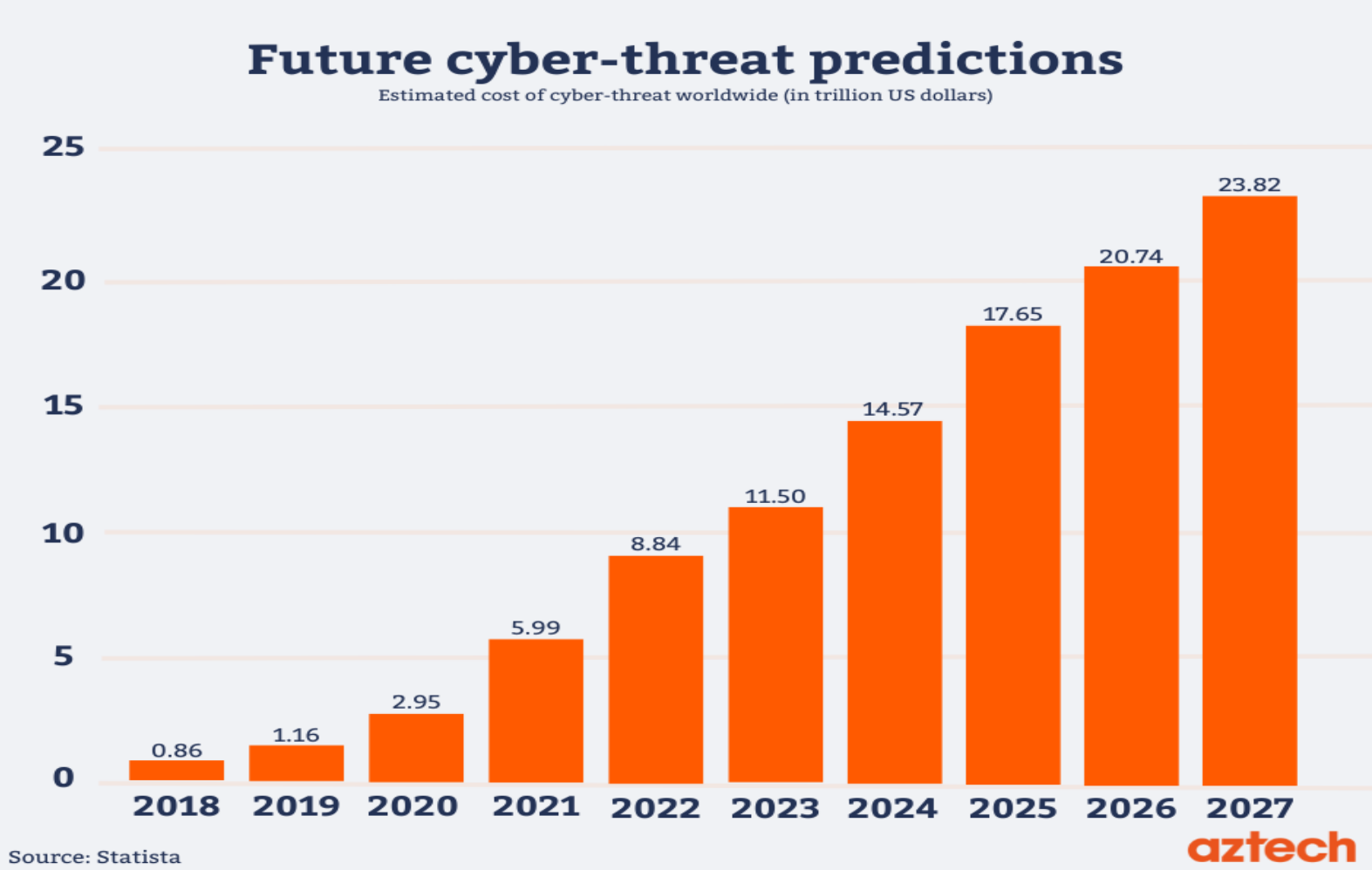
Background

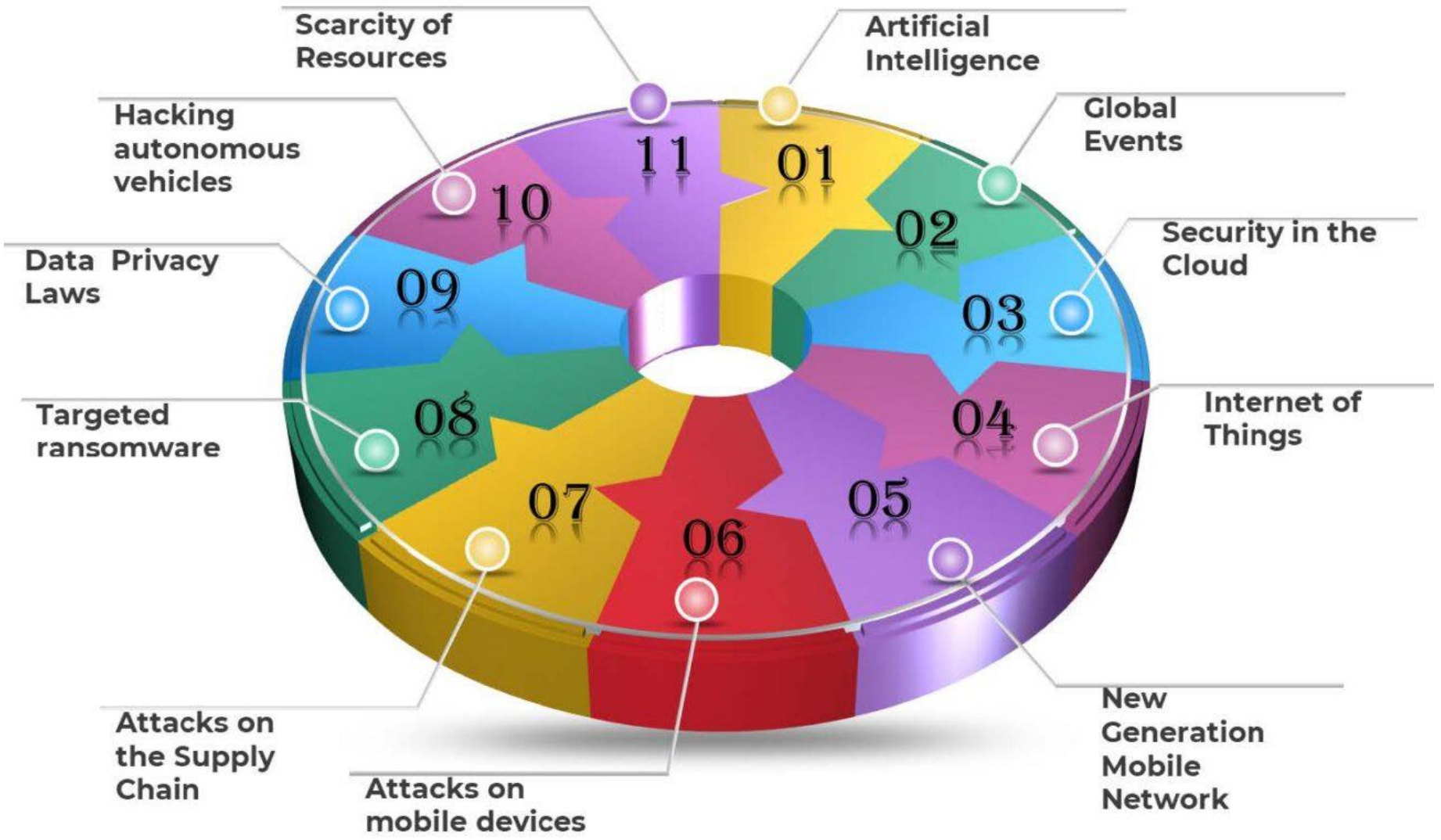
- Information Security requirements have changed in recent times
  - Traditionally provided by physical and administrative mechanisms
  - Many daily activities have been shifted from physical world to cyber space
    - Use of computers
      - Protect files and other stored information
    - Use of networks and communications links
      - Protect data during transmission

Definitions

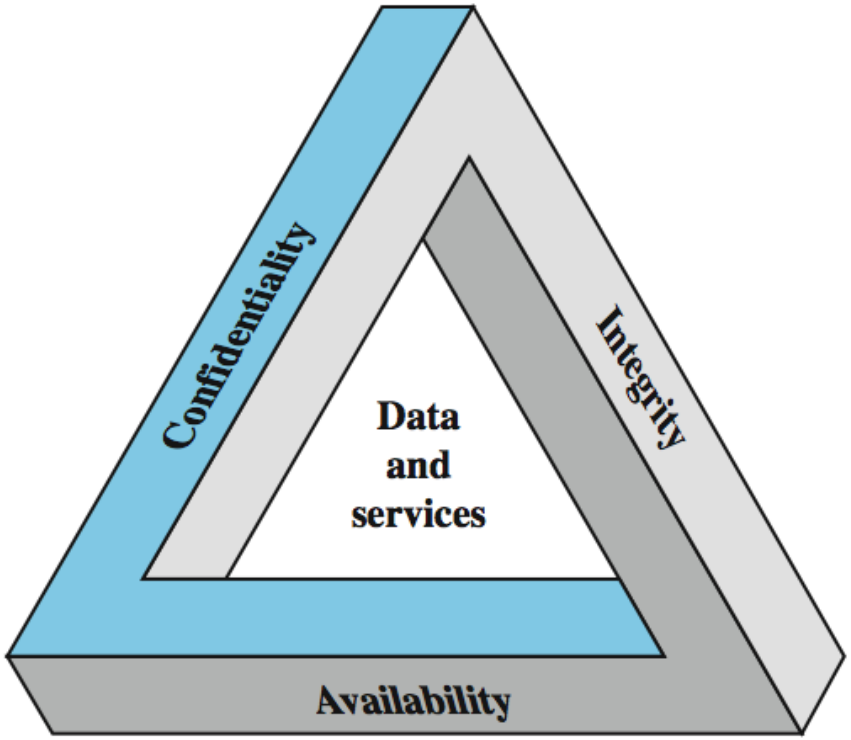
- Computer Security
  - Generic name for the collection of tools designed to protect data and to thwart hackers
- Network Security
  - Measures to protect data during their transmission
- Internet Security
  - Measures to protect data during their transmission over a collection of interconnected networks

Security Trends




Scarcity of Resources
Artificial Intelligence
Hacking autonomous vehicles
Global Events
Data Privacy Laws
Security in the Cloud
Targeted ransomware
Internet of Things
Attacks on the Supply Chain
Attacks on mobile devices
New Generation Mobile Network
11
01
10
02
09
03
08
04
07
06
05

3 Primary Security Goals



Fundamental security objectives for both data and information/computing services

SANGFOR

What is the CIA Triad?

CONFIDENTIALITY

The protection of sensitive information from being accessed or disclosed by unauthorized individuals.

INTEGRITY

The protection of data from unauthorized modification or destruction.

AVAILABILITY

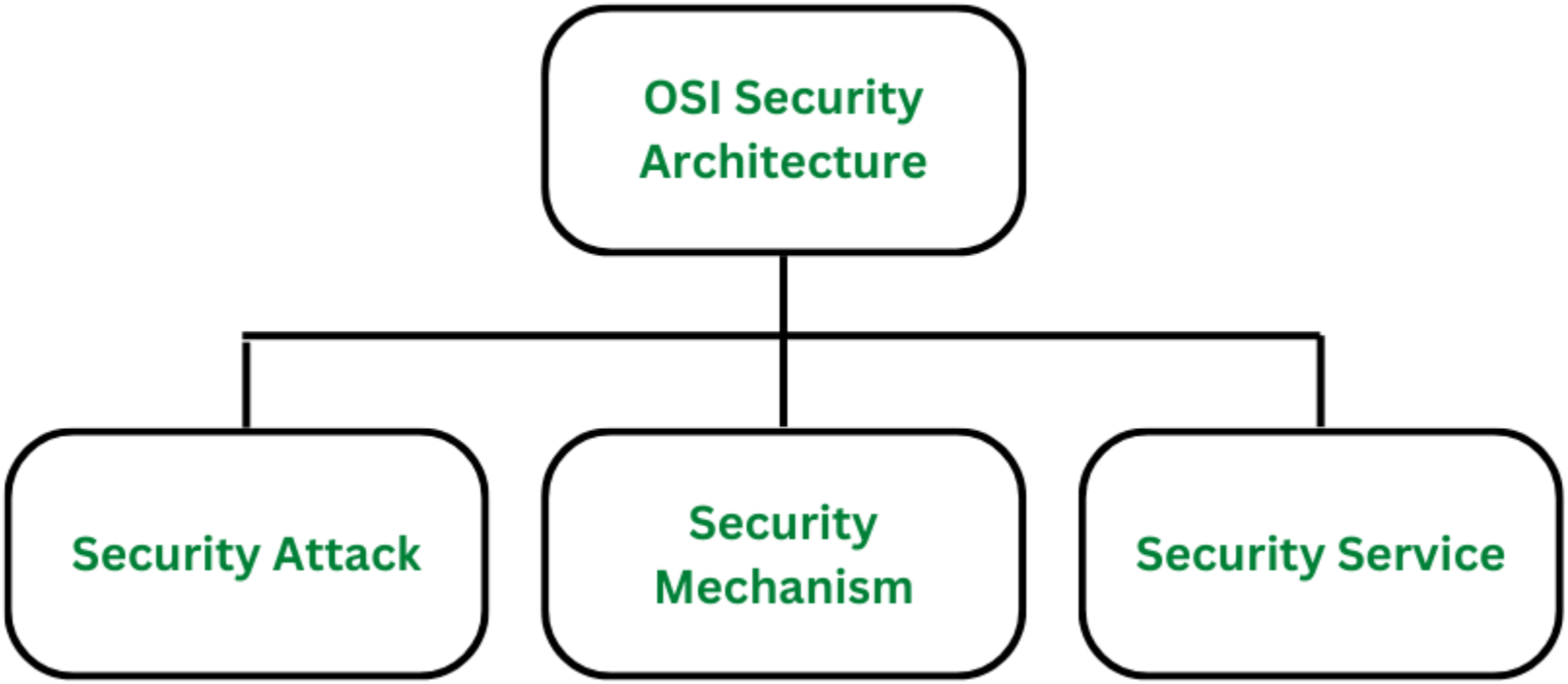
The assurance of timely and reliable access to data and systems by authorized users.

OSI Security Architecture

- ITU-T X.800 “Security Architecture for OSI”
  - A systematic way of defining and providing security requirements at each layer
  - These security services and mechanisms help to ensure the confidentiality, integrity, and availability of the data

ITU-T: International Telecommunication Union Telecommunication Standardization Sector

OSI: Open Systems Interconnection

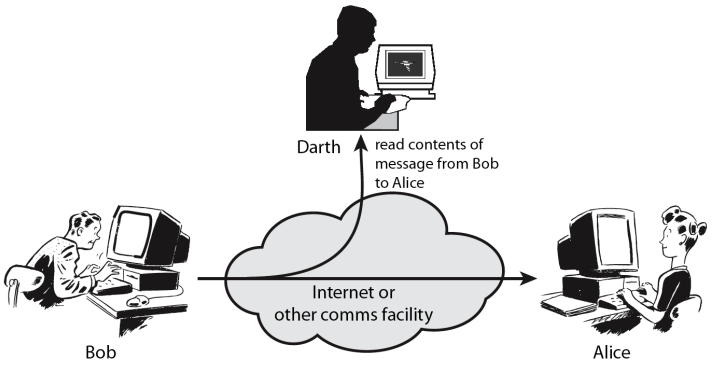

OSI Security Architecture
Security Attack
Security Mechanism
Security Service

OSI Security Architecture

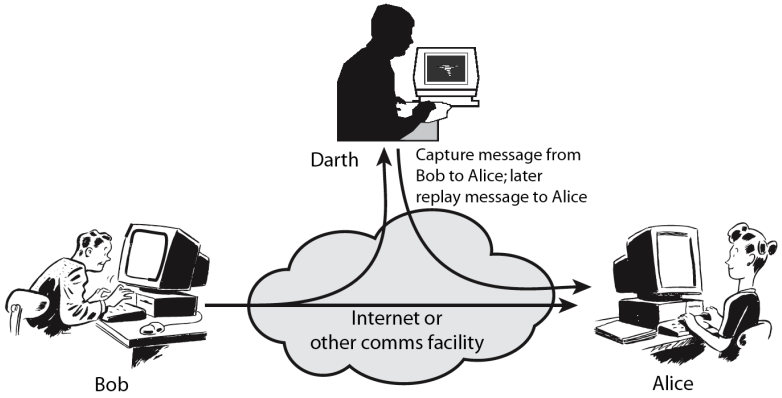
- **Security Attack**
  - Any action that compromises the security of information.
- **Security Mechanism**
  - A mechanism that is designed to detect, prevent, or recover from a security attack.
- **Security Service**
  - A service that enhances the security of data processing systems and information transfers.
    - Makes use of one or more security mechanisms.

Security Attacks

- Threat & attack
  - Often used equivalently
- There are a wide range of attacks
  - Two generic types
    - Passive



    - Active



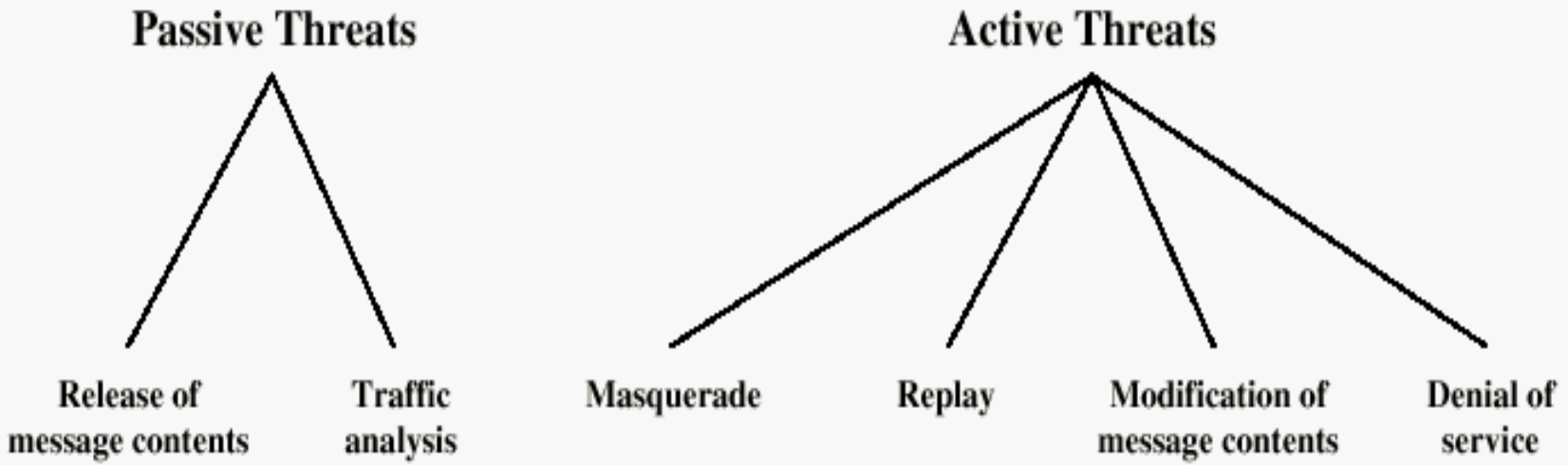


Figure 1.2 Active and Passive Security Threats

- **Passive Attacks:**
- **Eavesdropping:** Eavesdropping involves the attacker intercepting and listening to communications between two or more parties without their knowledge or consent. Eavesdropping can be performed using a variety of techniques, such as **packet sniffing, or man-in-the-middle attacks.**
- **Traffic analysis:** This involves the attacker analyzing network traffic patterns and metadata to gather information about the system, network, or device. Here the intruder can't read the message but only understand the pattern and length of encryption. Traffic analysis can be performed using a variety of techniques, such as **network flow analysis, or protocol analysis**.
- **Active attacks :**
- **Masquerade:** Masquerade is a type of attack in which the attacker pretends to be an authentic sender in order to gain unauthorized access to a system.
- **Replay:** Replay is a type of active attack in which the attacker intercepts a transmitted message through a passive channel and then maliciously or fraudulently replays or delays it at a later time.
- **Modification of Message:** Modification of Message involves the attacker modifying the transmitted message and making the final message received by the receiver look like it's not safe or non-meaningful. This type of attack can be used to manipulate the content of the message or to disrupt the communication process.
- **Denial of service (DoS): Denial of Service** attacks involve the attacker sending a large volume of traffic to a system, network, or device in an attempt to overwhelm it and make it unavailable to users.

Security Attack Classification

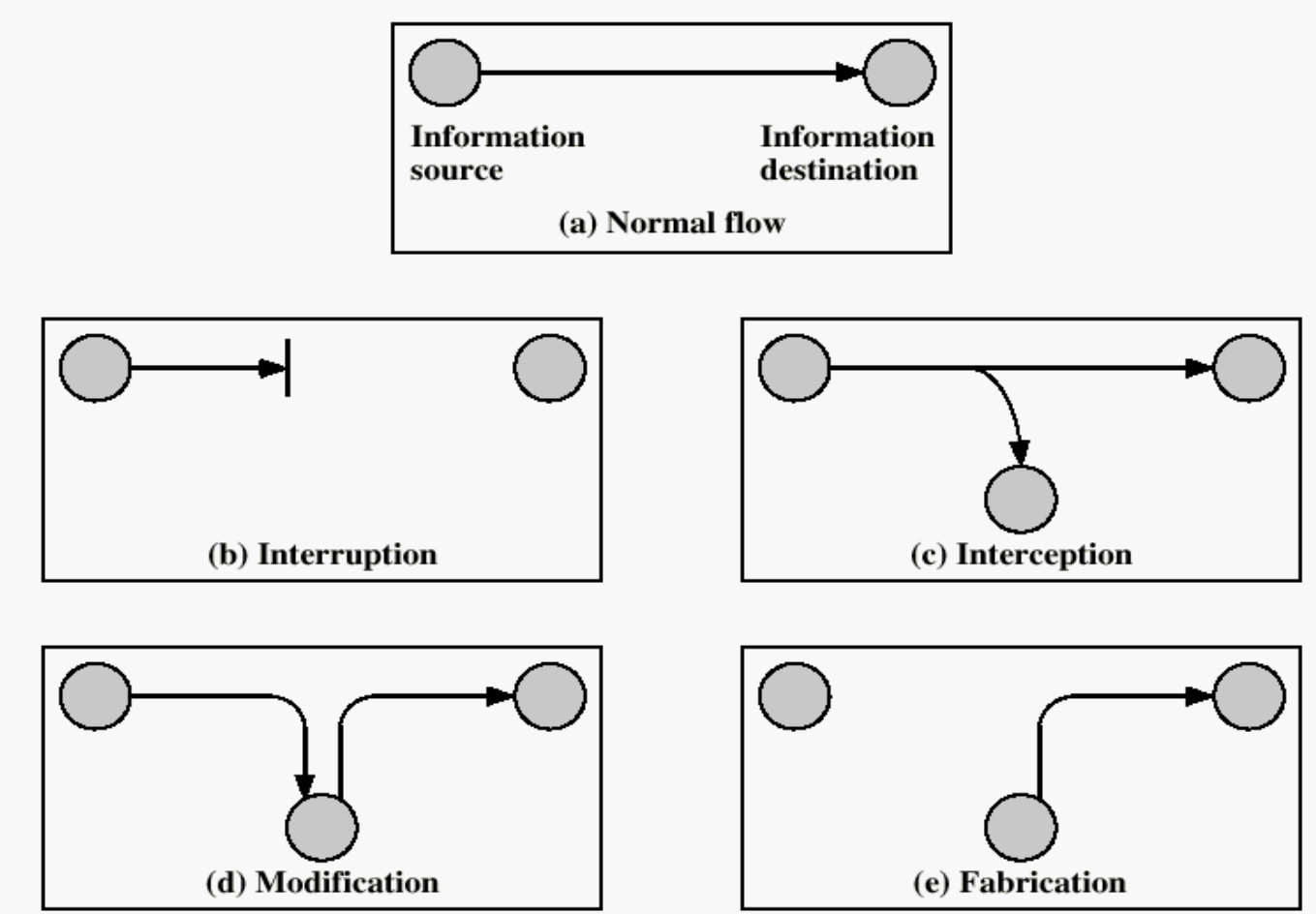


Figure 1.1 Security Threats

Security Attacks

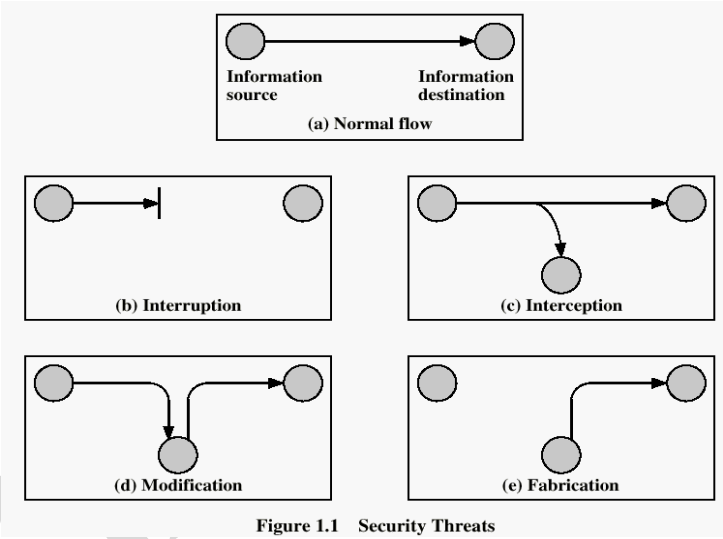


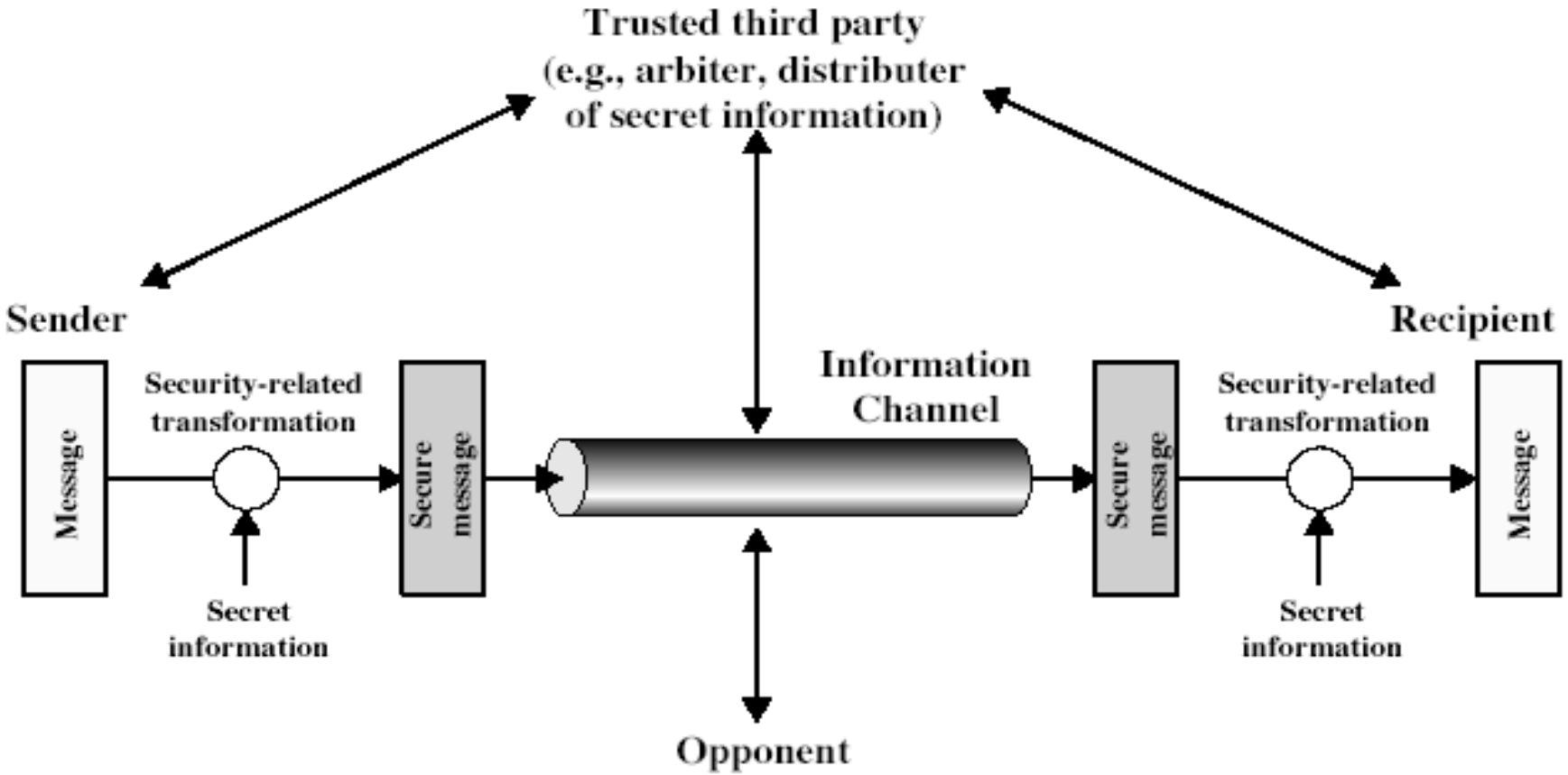
Figure 1.1 Security Threats

- **Interruption:** This is an attack on availability
- **Interception:** This is an attack on confidentiality
- **Modification:** This is an attack on integrity
- **Fabrication:** This is an attack on authenticity

Security Mechanism

- The mechanism that is built to identify any breach of security or attack on the organization, is called a security mechanism.
- Security Mechanisms are also responsible for protecting a system, network, or device against unauthorized access, tampering, or other security threats.
- **Encipherment (Encryption): Encryption** involves the use of algorithms to transform data into a form that can only be read by someone with the appropriate decryption key. Encryption can be used to protect data it is transmitted over a network, or to protect data when it is stored on a device.
- **Digital signature: Digital Signature** is a security mechanism that involves the use of cryptographic techniques to create a unique, verifiable identifier for a digital document or message, which can be used to ensure the authenticity and integrity of the document or message.
- **Traffic padding:** Traffic Padding is a technique used to add extra data to a network traffic stream in an attempt to obscure the true content of the traffic and make it more difficult to analyze.
- **Routing control:** Routing Control allows the selection of specific physically secure routes for specific data transmission and enables routing changes, particularly when a gap in security is suspected.

Model for Network Security

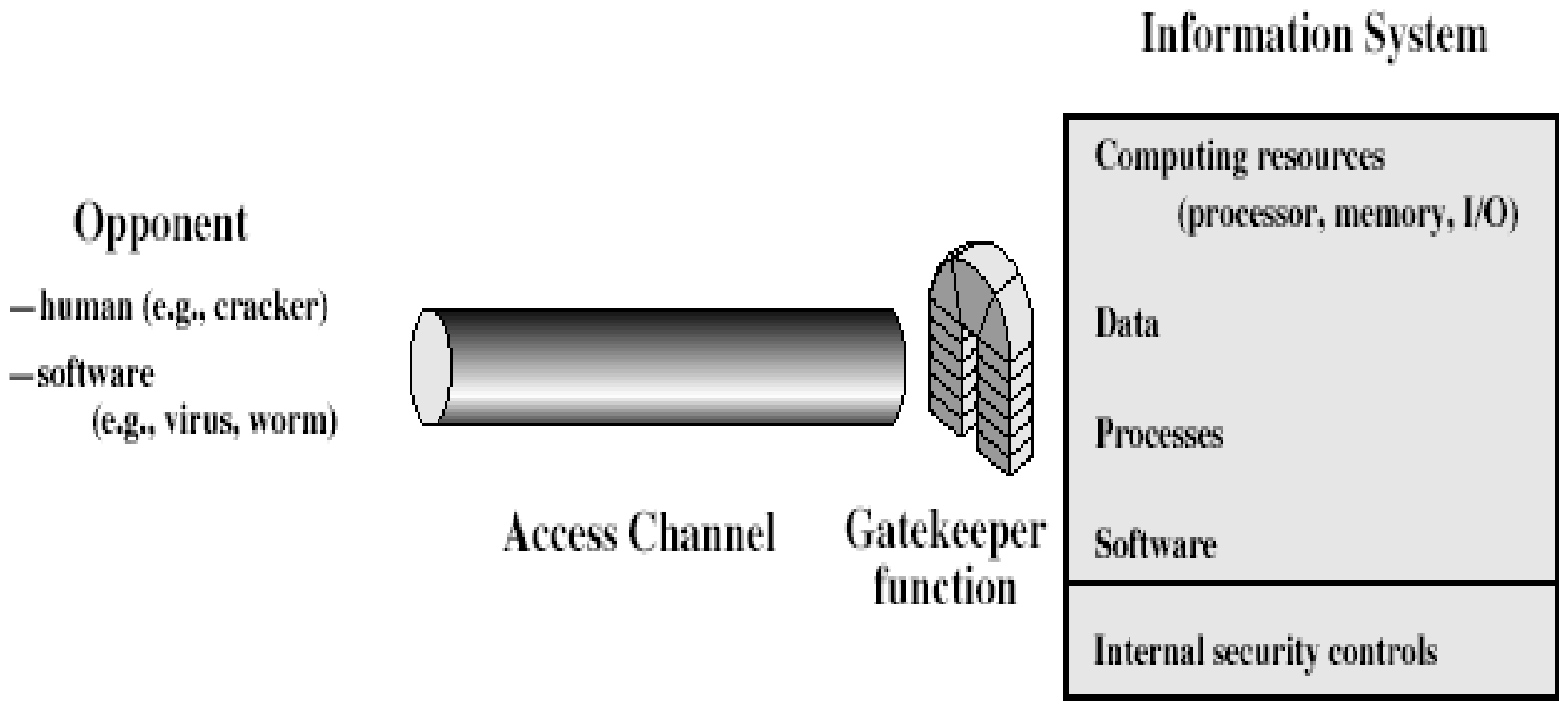


Model for Network Security

Using this model requires us to:

1. design a suitable algorithm for the security transformation (message de/encryption)
2. generate the secret information (keys) used by the algorithm
3. develop methods to distribute and share the secret information (keys)
4. specify a protocol enabling the principals to use the transformation and secret information for a security service (e.g. ssh)

Model for Network Access Security



Model for Network Access Security

Using this model requires us to implement:

1. Authentication
   - select appropriate gatekeeper functions to identify users
2. Authorization
   - implement security controls to ensure only authorized users access designated information or resources

Trusted computer systems may be useful to help implement this model

Methods of Defense

- Encryption
- Software Controls
  - Limit access in a database or in operating systems
  - Protect each user from other users
- Hardware Controls
  - Smartcard (ICC, used for digital signature and secure identification)
- Policies
  - Frequent changes of passwords
- Physical Controls

Security Services

X.800

- A service provided by a protocol layer of communicating open systems, which ensures adequate security of the systems or of data transfers

- Confidentiality (privacy)
- Authentication (who created or sent the data)
- Integrity (has not been altered)
- Non-repudiation (the order is final)
- Access control (prevent misuse of resources)
- Availability (permanence, non-erasure)
  - Denial of Service Attacks
  - Virus that deletes files

Networking devices

- Host:
  - Host are devices (laptops, smartphones, workstations, etc.) on the network must always be protected and in case of a penetration or an attack should be analyzed correctly to calculate damage and implement appropriate incident response.
  - A host inside a network is a network element which can be assigned an IP address and can communicate to other hosts using IP address which is a unique identifier of a host inside a particular network.

Hub

- Hub is a hardware multiport device used at the physical layer to connect multiple devices in the network.
- Hubs are widely used to connect LANs.
- A hub has multiple ports and it is a non-intelligent device.
- A hub acts as a dumb switch that does not know, which data needs to be forwarded where so it broadcasts or sends the data to each port.
- The transmission mode is half-duplex.
- It performs frame flooding, which includes broadcast, multicast and unicast as well.

Advantages of Network Hubs:

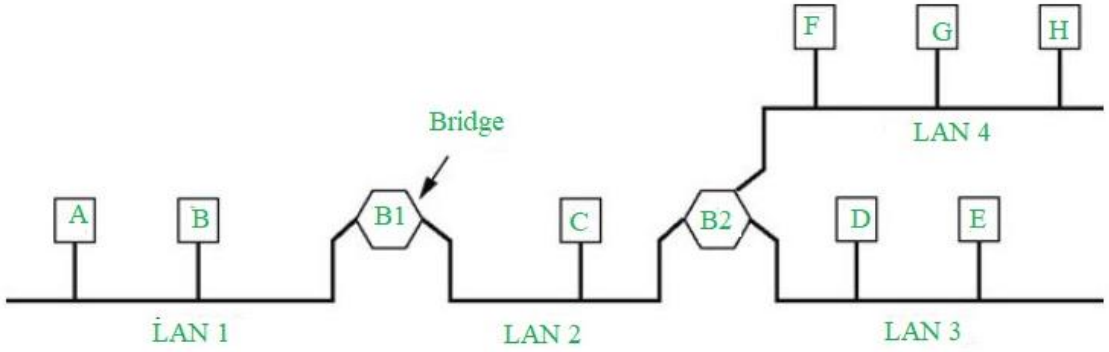
- Less expensive.
- Does not impact network performance.
- Support different network media.
- Easily connects with different media.

Disadvantages of Network Hubs:

- **Not intelligent**
- **Hub is everything**
- **No filtering:** Hubs do not allow packet filtering. This means that any data that is being forwarded to one device will also be forwarded to all connected devices. It, however, does not forward the frame to the port of entry. Since the hub is purely hardware, it does not have a MAC address for locating the target device.
- **No security:** Since the hub broadcasts messages to every port, it is not possible to send any private frame. This allows other connected ports to access your data.
- **Network Traffic is high**
- **Does not use full duplex transmission mode**
- **Cannot connect to different network architectures**

Bridge

- The bridge is a networking device that connects the larger LAN networks with the group of smaller LAN networks.
- The bridge is a physical or hardware device but operates at the OSI model's data link layer and is also known as a layer of two switches.



Advantages:

- Bridges can be used as a network extension like they can connect two network topologies together.
- It has a separate collision domain, which results in increased bandwidth.
- Highly reliable and maintainable. The network can be divided into multiple LAN segments.
- Simple installation, no requirement of any extra hardware or software except the bridge itself.

Disadvantages:

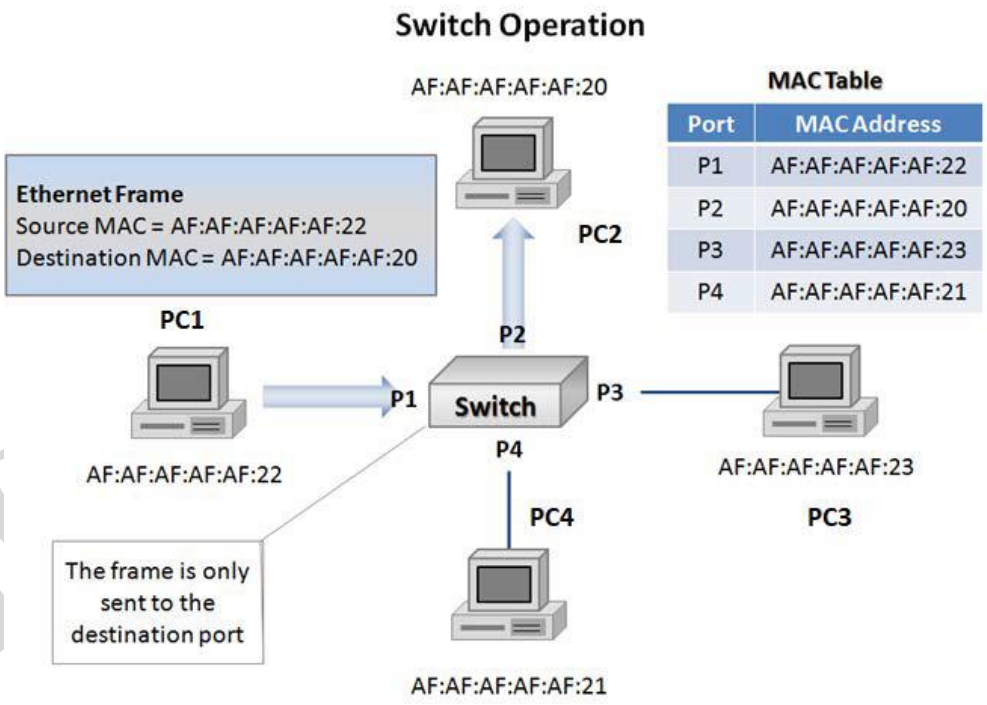
- Expensive as compared to hubs and repeaters.
- Slow in speed.
- Poor performance as additional processing is required to view the MAC address of the device on the network.

Switches

- L2 Switch works at layer 2(DLL) of OSI model.
- Sends packet to destination port using MAC address table which stores the MAC address of a device associated with that port.
- Switch learns, by flooding network to fill MAC- address table, on which port a particular device is connected. After learning it sends packets to that particular host only.
- There are two types of switches (Static & Dynamic).
- Other types are Unmanaged, Managed and PoE Switches.

- **Unmanaged Switch** − These are inexpensive switches commonly used in home networks and small businesses. **They can be set up by simply plugging in to the network, after which they instantly start operating**. When more devices needs to be added, more switches are simply added by this plug and play method. They are referred to as u managed since they do not require to be configured or monitored.
- **Managed Switch** − These are costly switches that are used in organizations with large and complex networks, since **they can be customized to augment the functionalities of a standard switch**. The augmented features may be QoS (Quality of Service) like higher security levels, better precision control and complete network management. Despite their cost, they are preferred in growing organizations due to their scalability and flexibility. Simple Network Management Protocol (SNMP) is used for configuring managed switches.
- **LAN Switch** − Local Area Network (LAN) switches connects devices in the **internal LAN of an organization**. They are also referred as Ethernet switches or data switches. These switches are particularly helpful in reducing network congestion or bottlenecks.
- **PoE Switch** − Power over Ethernet (PoE) switches are used in PoE Gigabit Ethernets. **PoE technology combine data and power transmission over the same cable so that devices connected to it can receive both electricity as well as data over the same line.** PoE switches offer greater flexibility and simplifies the cabling connections

- If PC1 sends a frame to PC2, the switch will receive it at port P1 and forwards the received frame to port P2 according to the MAC table of the switch.
- The switch learns the MAC table automatically.



- Switches connect the devices in the network together.
- **They are usually not a target of an attack, but would be used to do so and might contain some information that might help with the analysis.**
- Switches create an efficient network by isolating the traffic on different switch ports so that each switch port is a separate collision domain.

What Are the Security Risks of Network Switches?

Network switches are essential components of modern computer networks, but they are not immune to security risks. Understanding these risks is crucial for network administrators and organizations to implement appropriate security measures.

1. **Unauthorized Access:** If an attacker gains physical access to a network switch, they may be able to connect to the console port or reset the switch to factory defaults, potentially giving them control over the device. Weak or default login credentials can be exploited by attackers to gain unauthorized access to the switch's management interface.
2. **VLAN Hopping:** VLAN hopping is a technique where an attacker gains access to traffic on multiple VLANs by exploiting vulnerabilities in the switch's configuration or protocols. This can lead to unauthorized access to sensitive information.
3. **MAC Address Spoofing:** Attackers can spoof MAC (Media Access Control) addresses to gain unauthorized access to the network or launch man-in-the-middle attacks, intercepting and manipulating network traffic.
4. **Denial of Service (DoS) Attacks**

5. Security Misconfigurations: Misconfigurations in switch settings, such as incorrect access control lists (ACLs), can lead to security vulnerabilities.

6. Port Security: Failing to implement port security features can allow unauthorized devices to connect to the network. Port security mechanisms can restrict access based on MAC addresses or the number of devices per port.

7. SNMP Vulnerabilities: Simple Network Management Protocol (SNMP) is often used for remote management of switches. If SNMP is not configured securely, attackers can exploit it to gain access or gather information about the switch.

8. Firmware and Software Vulnerabilities

9. Insider Threats

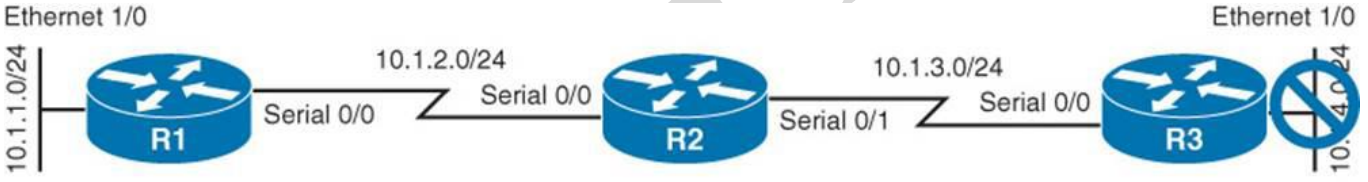
10. Physical Security

11. Lack of Logging and Monitoring

Router

- (Network **layer)**
- Routers are a core component of any network. A router connects the local network to other networks and the internet.
- Because of this, routers are sometimes the target of an attack or are used to gain access to a network. Thus, it is very important to protect routers in the first instance.
- In case of an attack or penetration, routers should be able to provide any information that can help in investigating the event .
- Routers contain routing tables rules and configuration parameters such as bandwidth, QoS, delay, distance, load and other important information.

- The purpose of the router device is to allow route selection from source to destination based on the IP address of the destination.
- The router accomplishes this task by using its routing table.
- The routing table can be built dynamically using dynamic routing protocols such as RIP, OSPF, BGP, etc.
- Also, the routing table can be defined statically using manually entered routes.



Router R2's Routing Table

Network	Interface	Metric
10.1.1.0/24	S0/0	1
10.1.2.0/24	S0/0	0
10.1.3.0/24	S0/1	0
10.1.4.0/24	S0/1	1

10.1.4.0/24
Hop Count 1

Router R3's Routing Table

Network	Interface	Metric
10.1.1.0/24	S0/0	2
10.1.2.0/24	S0/0	1
10.1.3.0/24	S0/0	0
~~10.1.4.0/24~~	~~E1/0~~	~~0~~
10.1.4.0/24	S0/0	2

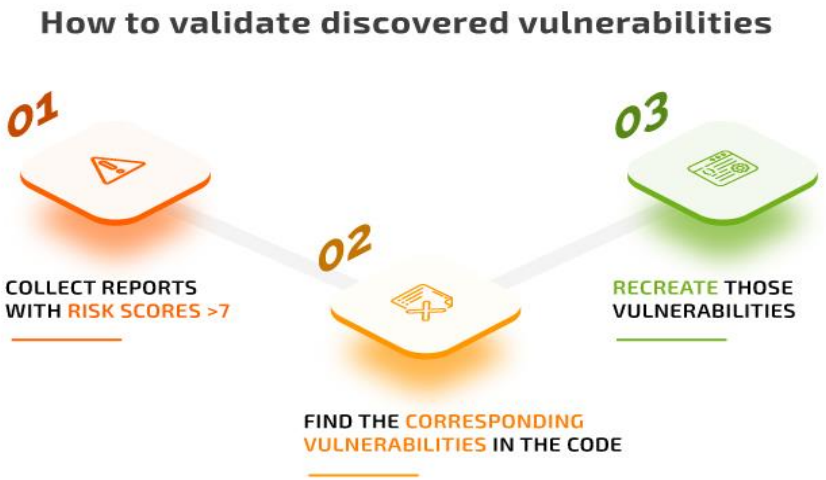
- **Routers**
  - Routing table often specifies a default route, which it uses whenever it fails to find a better forwarding option for a given packet (eg home router directs all traffic to ISP router).
  - Routing table can be Static (manually configured) or Dynamic (updates on Network activity, exchanging information with other devices via Routing protocol).
  - Performs NAT function by shielding private IP Address.
  - Types- Core Router(used by ISP's- forwards information along main fibre optic), Backbone Routers(Connects large enterprise Network to Core Router), Edge Router (also known as Access Router- low capacity, resides at boundary LAN and connects to public internet, private WAN or external LAN.
  - Routers are specialised computer with CPU, RAM, Network interface.
  - In addition to studying the overall statistics generated from a router device, the router table provides **important information about the paths followed by the network traffic**.
  - The interfaces and the connections of the routers help figure out the network topology.

How can routers get compromised?

1. Firmware vulnerabilities
2. Credential hacking
3. Abuse of device misconfiguration
4. Vulnerabilities of outdated technologies
5. Insider threats

How to discover firmware vulnerabilities

- When talking about searching for vulnerabilities, we usually mean discovering **first-day vulnerabilities** — security issues that were already discovered and reported. The details of a reported first-day vulnerability help both for manufacturers to release a patch for their product and for malicious actors hack the affected software.
- Though you often hear about zero-day vulnerabilities, searching for them is a challenging process of trial and error, as the weaknesses are still unknown.
- **The search for first-day vulnerabilities starts with discovering libraries inside the router firmware. You need to gather library names and versions, then look for vulnerability reports on these libraries in vulnerability databases.**
-



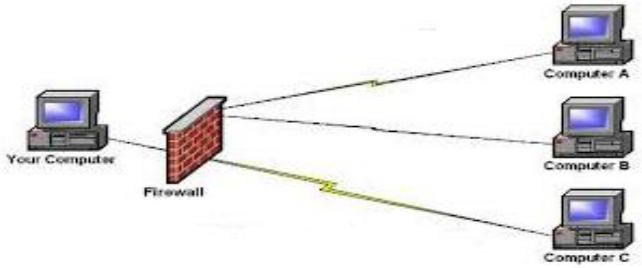
FIREWALL

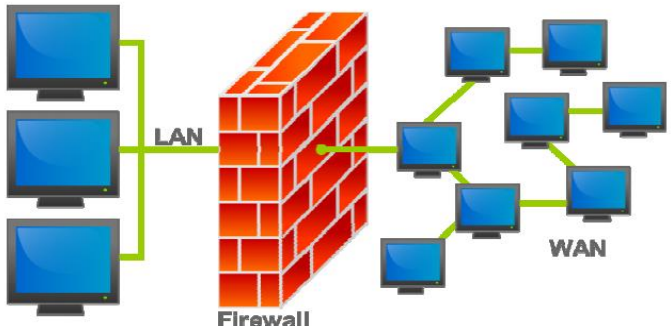
- ✓ Network security device.
- ✓ It may be Hardware or Software based.
- ✓ Monitors all incoming and outgoing traffic.
- ✓ Based on defined set of security rules it accepts, rejects or drops that specific traffic.
  - ✓ **Accept :** allow the traffic
  - ✓ **Reject :** block the traffic but reply with an "unreachable error"
  - ✓ **Drop : block the traffic with no reply**
- ✓ Establishes a barrier between secured internal networks and outside untrusted network, such as Internet.

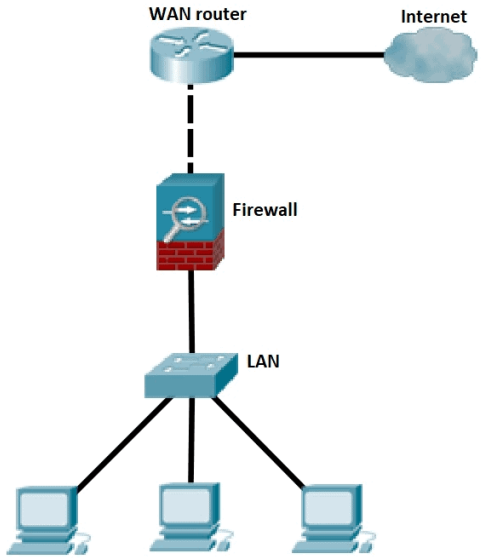
✓ It is designed to forward some packets and filter others.

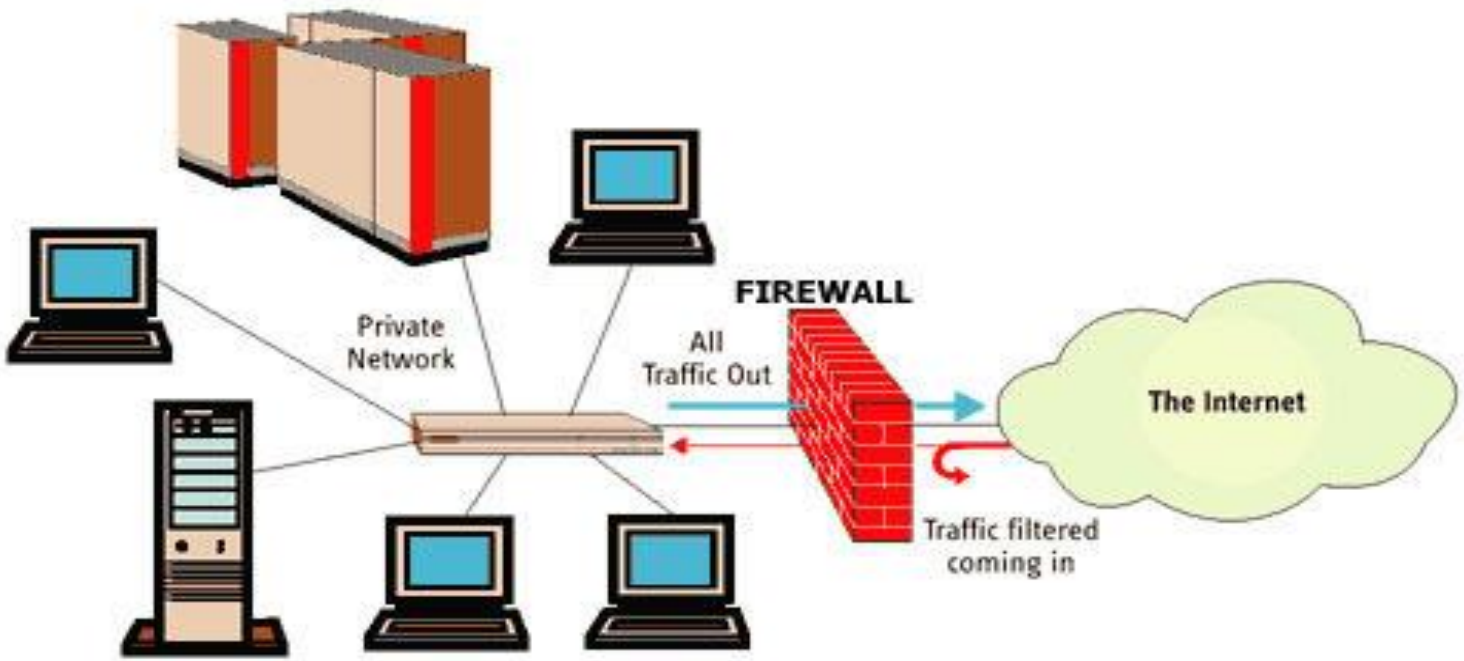
✓ A firewall is **hardware, software, or a combination of both** that is used to prevent unauthorized programs or Internet users from accessing a private network and/or a single computer.

✓ Acts as a security gateway between two networks.



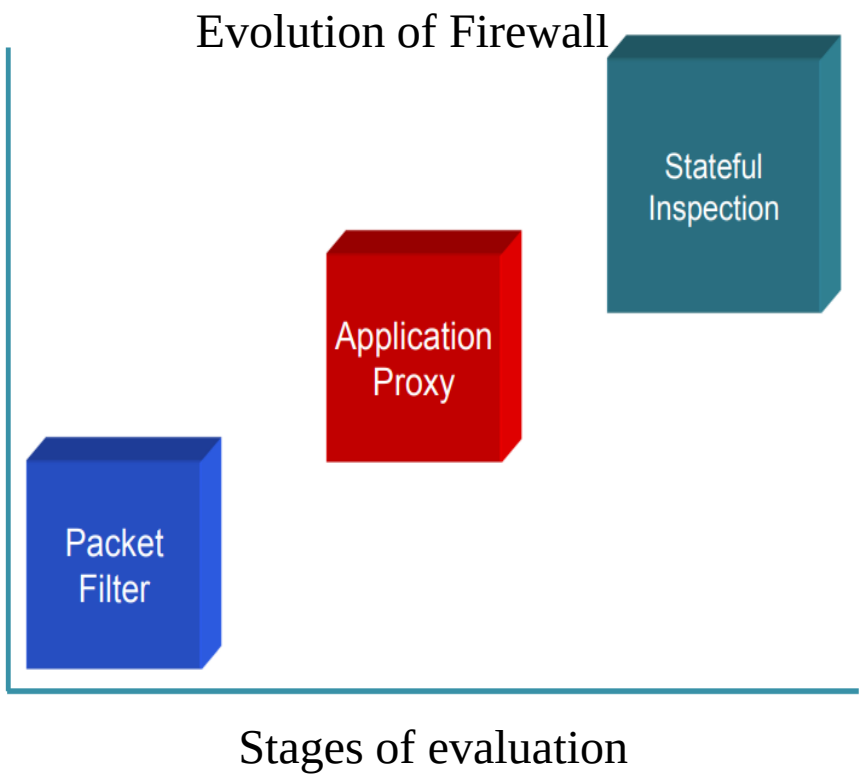





FIREWALL
Private
Network
All
Traffic Out
The Internet
Traffic filtered
coming in

FIREWALL CLASSIFICATION

- ✓Hardware firewall
- ✓Software firewall
- ✓Packet-filter firewall
- ✓Proxy firewall
- ✓Circuit-level gateways
- ✓Stateful packet inspection (SPI)
- ✓Next-generation firewall (NGFW)



HARDWARE VERSES SOFTWARE FIREWALLS

- ✓ Hardware Firewalls
  - ✓ A hardware firewall is preferred when a firewall is required on more than one machine.
  - ✓ A hardware firewall provides an additional layer of security to the physical network.
  - ✓ Protects an entire network.
  - ✓ Implemented on the router level Usually more expensive, harder to configure.
  - ✓ **The disadvantage of this approach is that if one firewall is compromised, all the machines that it serves are vulnerable.**

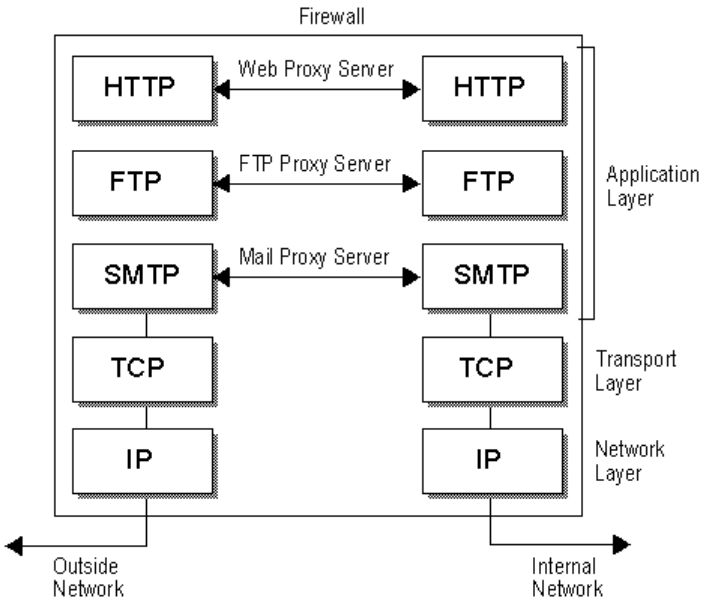
- ✓ Software Firewalls
  - ✓ A software firewall is a second layer of security and secures the network from malware, worms, viruses and email attachments.
  - ✓ It looks like any other program and can be customized based on network requirements.
  - ✓ Software firewalls can be customized to include antivirus programs and to block sites and images.
  - ✓ Protects a single computer.
  - ✓ **Usually less expensive, easier to configure.**

PACKET-FILTERING FIREWALL

- ✓ A packet-filtering firewall filters at the network or transport layer.
- ✓ **It provides network security by filtering network communications based on the information contained in the TCP/IP header of each packet**.
- ✓ The firewall examines these headers and uses the information to decide whether to accept and route the packets along to their destinations or deny the packet by dropping them.
- ✓ This firewall type is a router that uses a filtering table to decide which packets must be discarded.
- ✓ Packer filtering makes decisions based upon the following header information:
  - ✓ The source IP address.
  - ✓ The destination IP address.
  - ✓ The network protocol in use (TCP, ICMP or UDP).
  - ✓ The TCP or UDP source port.
  - ✓ The TCP or UDP destination port.
  - ✓ If the protocol is ICMP, then its message type.

Proxy firewall

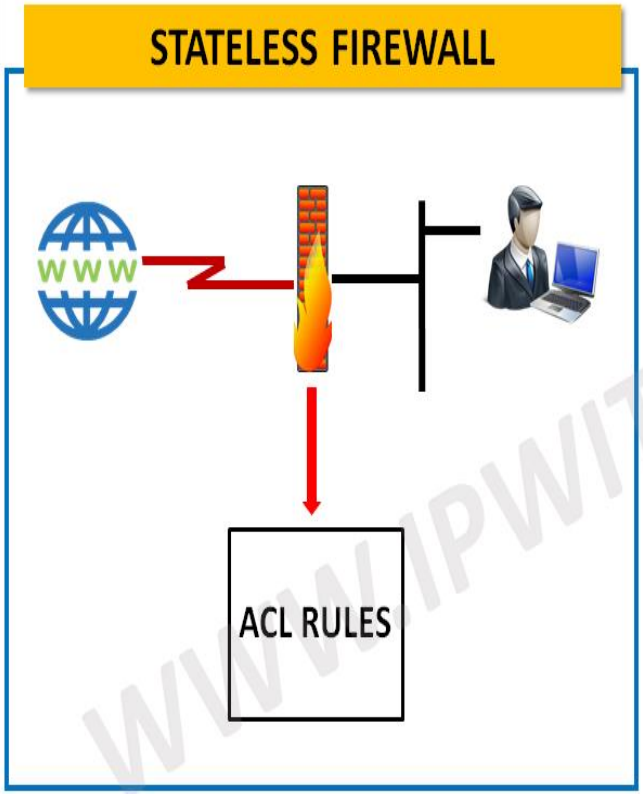
- ✓ The packet-filtering firewall is based on information available in the network and transport layer header. However, sometimes we need to filter a message based on the information available in the message itself (at the application layer).
- ✓ A proxy firewall is a network security system that protects network resources by filtering message at the application layer.
- ✓ A firewall proxy server is an application that act as an intermediate between two end systems.
- ✓ Firewall proxy servers operate at the application layer through the Proxy.
- ✓ They do this by creating and running a process on the firewall that mirrors a service as if it were running on the end host.
- ✓ A firewall proxy server essentially turns a two party session into a four party session with the middle process emulating the two real hosts.
- ✓ Because they operate at the application layer, proxy servers are also referred to as Application Layer Firewalls.
- ✓ Firewall proxy servers centralize all activity for an application into a single server.

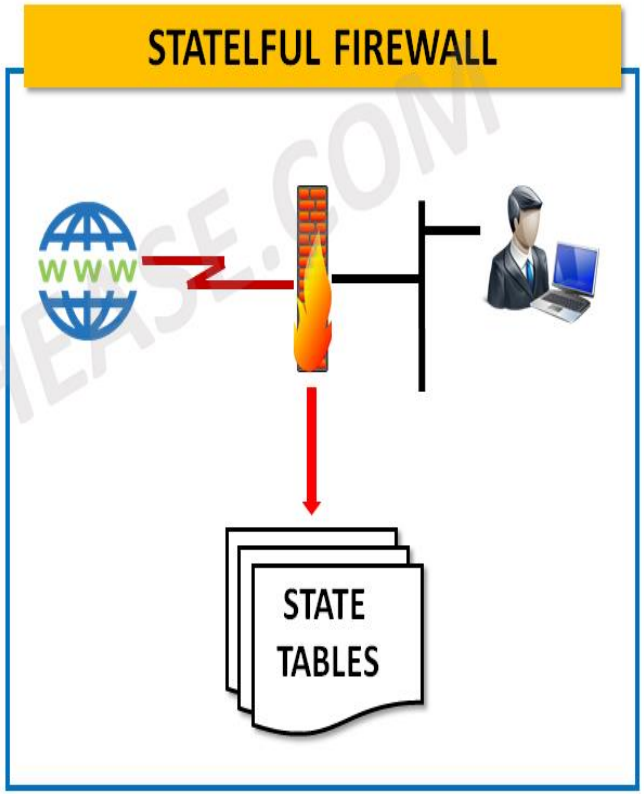


CIRCUIT-LEVEL FIREWALL

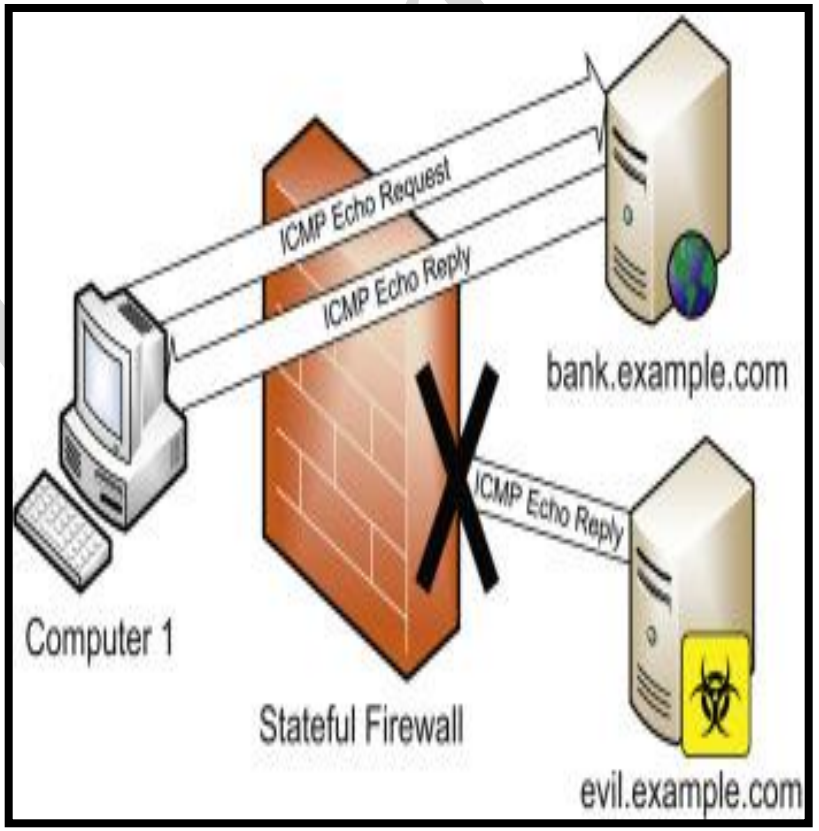
- ✓ Circuit-level *firewalls* are similar in operation to packet-filtering firewalls, but they operate at the transport and session layers of the OSI model.
- ✓ The biggest difference between a packet-filtering firewall and a circuit-level firewall is that a circuit-level firewall validates TCP and UDP sessions before opening a connection, or circuit, through the firewall.
- ✓ When the session is established, the firewall maintains a table of valid connections and lets data pass through when session information matches an entry in the table.
- ✓ The table entry is removed, and the circuit is closed when the session is terminated.

- ✓ **Firewall**
  - ✓ Other Two Types- Stateless & Stateful
    - ✓ Stateless Firewalls are basically ACLs (Access Control List). It contains rule about which traffic to allow/block depending on Source IP, Destination IP, Port Nos, Network Protocols (TCP, UDP, ICMP, DHCP) etc.
    - ✓ Stateful- associates each packet with a "connection"(maintains a record), so that it can decide if an arriving packet is related to a previous outgoing packet.





- ✓ *Stateful firewalls* have a state table that allows the firewall to compare current packets to previous ones.
- ✓ Computer 1 sends an ICMP Echo Request to bank.example.com.
- ✓ An Echo Reply is then received from bank.example.com to Computer 1, firewall checks to see, if it allows this traffic (it does), and then checks the state table for a matching echo request in the opposite direction.
- ✓ The firewall finds the matching entry, deletes it from the state table, and passes the traffic.
- ✓ Then evil.example.com sends an unsolicited ICMP Echo Reply. The stateful firewall, shown in Figure, sees no matching state table entry, and denies the traffic.



Advantages of Using Firewalls

Firewalls play an important role in the companies for security management. Below are some of the important advantages of using firewalls.

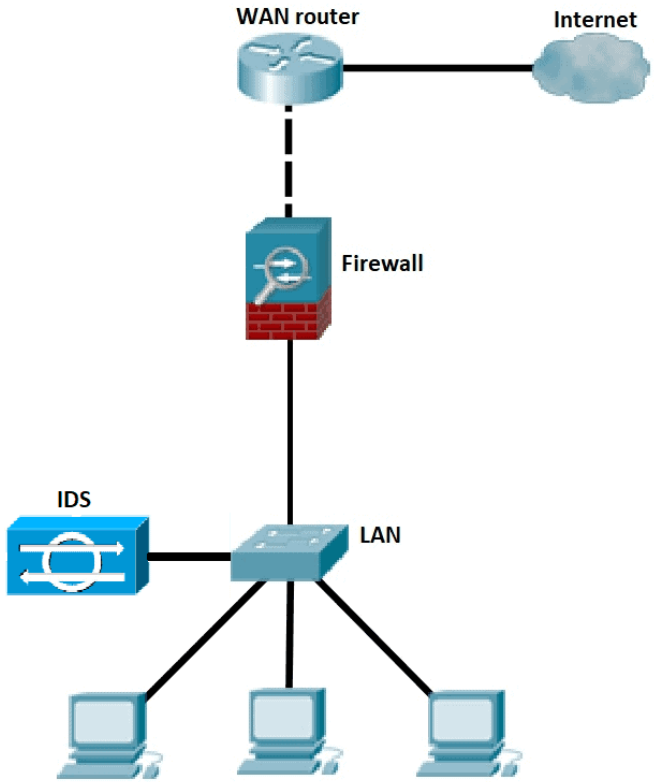
- It provides enhanced security and privacy from vulnerable services. It prevents unauthorized users from accessing a private network that is connected to the internet.
- Firewalls provide faster response time and can handle more traffic loads.
- A firewall allows you to easily handle and update the security protocols from a single authorized device.
- It safeguards your network from phishing attacks.

Limitations of a Firewall

- Firewalls are not able to stop the users from accessing the data or information from malicious websites, making them vulnerable to internal threats or attacks.
- It is not able to protect against the transfer of virus-infected files or software if security rules are misconfigured, against non-technical security risks (social engineering)
- It does not prevent misuse of passwords and attackers with modems from dialing in to or out of the internal network.
- Already infected systems are not secured by Firewalls.

Intrusion Detection System (IDS)

- ✓ A system called an intrusion detection system (IDS) **observes network traffic for malicious transactions** and **sends immediate alerts** when it is observed.
- ✓ It is software that checks a network or system for malicious activities or policy violations.
- ✓ **Each illegal activity** or violation is often recorded either centrally using a SIEM system or **notified to an administration.**
- ✓ IDS monitors a network or system for malicious activity and protects a computer network from unauthorized access from users, including perhaps insiders.



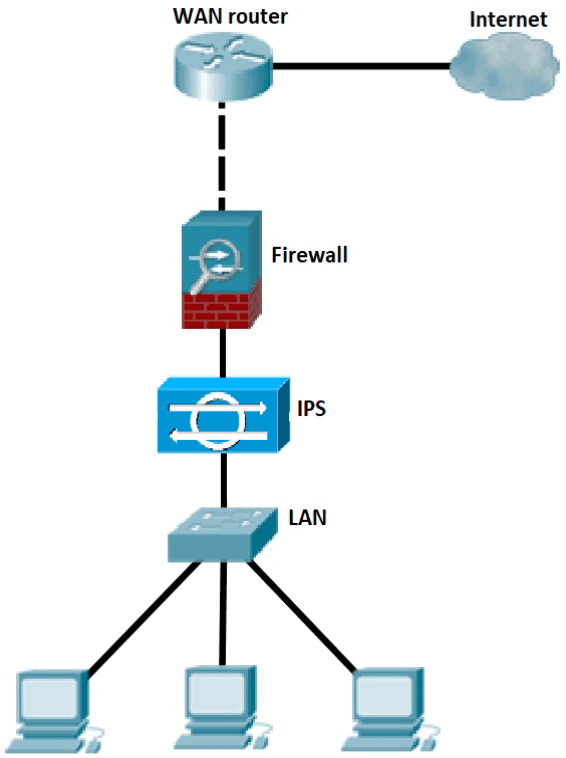
- ✓ IDS is basically classified into two types:-
  - ✓ **Network intrusion detection systems (NIDS)** - set up at a planned point (where Firewall is located) within the network to examine traffic from all devices on the network. It performs an observation of passing traffic and matches traffic that is passed on the subnets to the collection of known attacks.
  - ✓ **Host intrusion detection systems (HIDS)** - run on independent hosts or devices on the network. It monitors the incoming and outgoing packets from the device only, takes a snapshot of existing system files and compares it with the previous snapshot , if edited or deleted. HIDS seen on mission critical machines, which are not expected to change their layout.

Detection Method of IDS

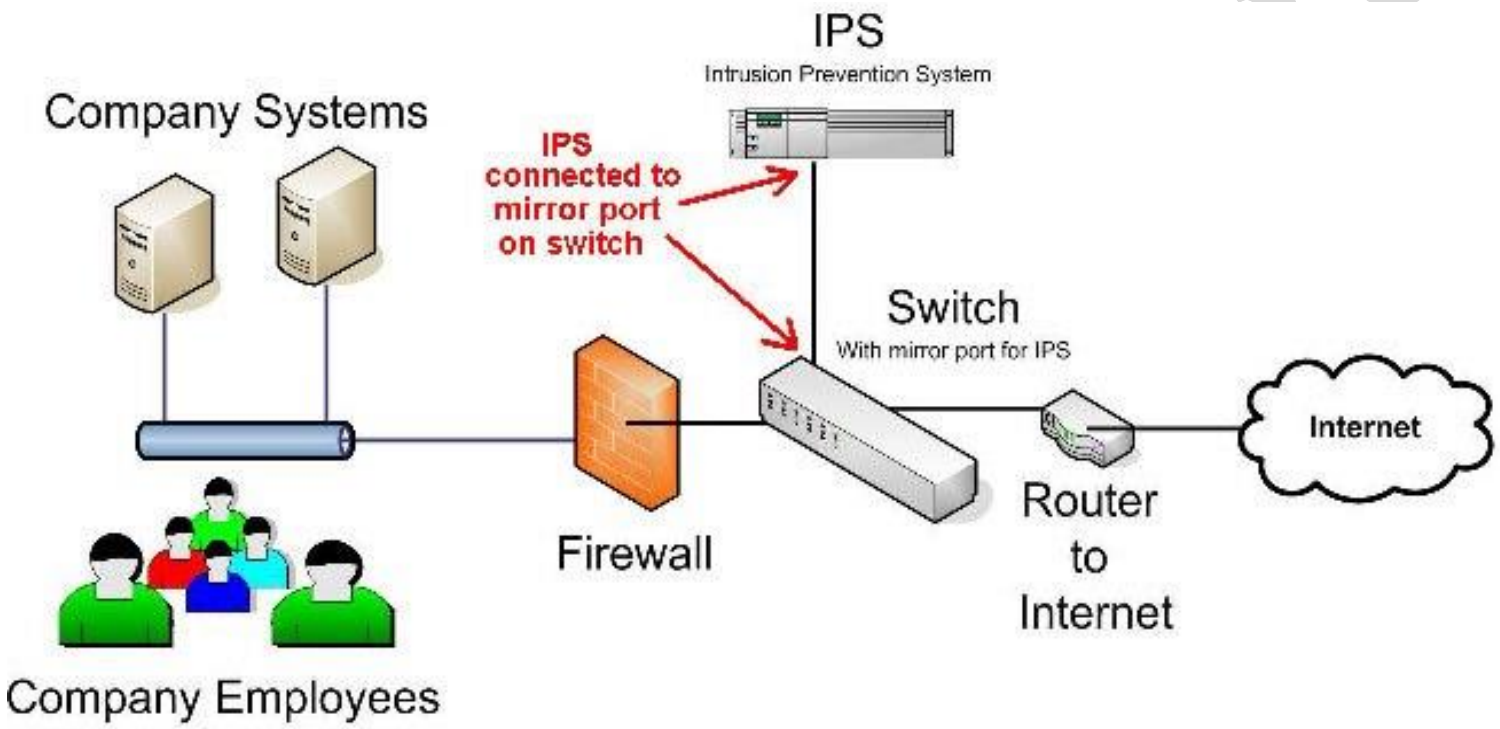
- ✓ **Signature-based Method.**
  - ✓ Detects on the basis of the already known malicious instruction sequence.
  - ✓ The detected patterns are known as signatures.
  - ✓ Signature-based IDS detects attacks whose pattern (signature) already exists in system.
- ✓ **Anomaly-based IDS**
  - ✓ Introduced to detect the unknown malware attacks as new malware are developed rapidly.
  - ✓ Anomaly-based IDS uses Machine Learning to create a trustful activity model.
  - ✓ Anything coming is compared with that model and it is declared suspicious if it is not found in model.
- ✓ Machine Learning based method has a better generalized property in comparison to signature-based IDS as these models can be trained according to the Applications and Hardware configurations.

Intrusion Prevention System (IPS)

- ✓ Network security/threat prevention technology that examines network traffic flows to detect and prevent vulnerability exploits.
- ✓ Unlike IDS—which is a passive system that scans traffic and reports back on threats, **IPS is placed inline** (in the direct communication path between source and destination), actively analysing and taking automated actions on all traffic flows that enter the network.
  - ✓ Sending an alarm.
  - ✓ Dropping malicious packets.
  - ✓ Blocking traffic from the source address.
  - ✓ Resetting the connection.

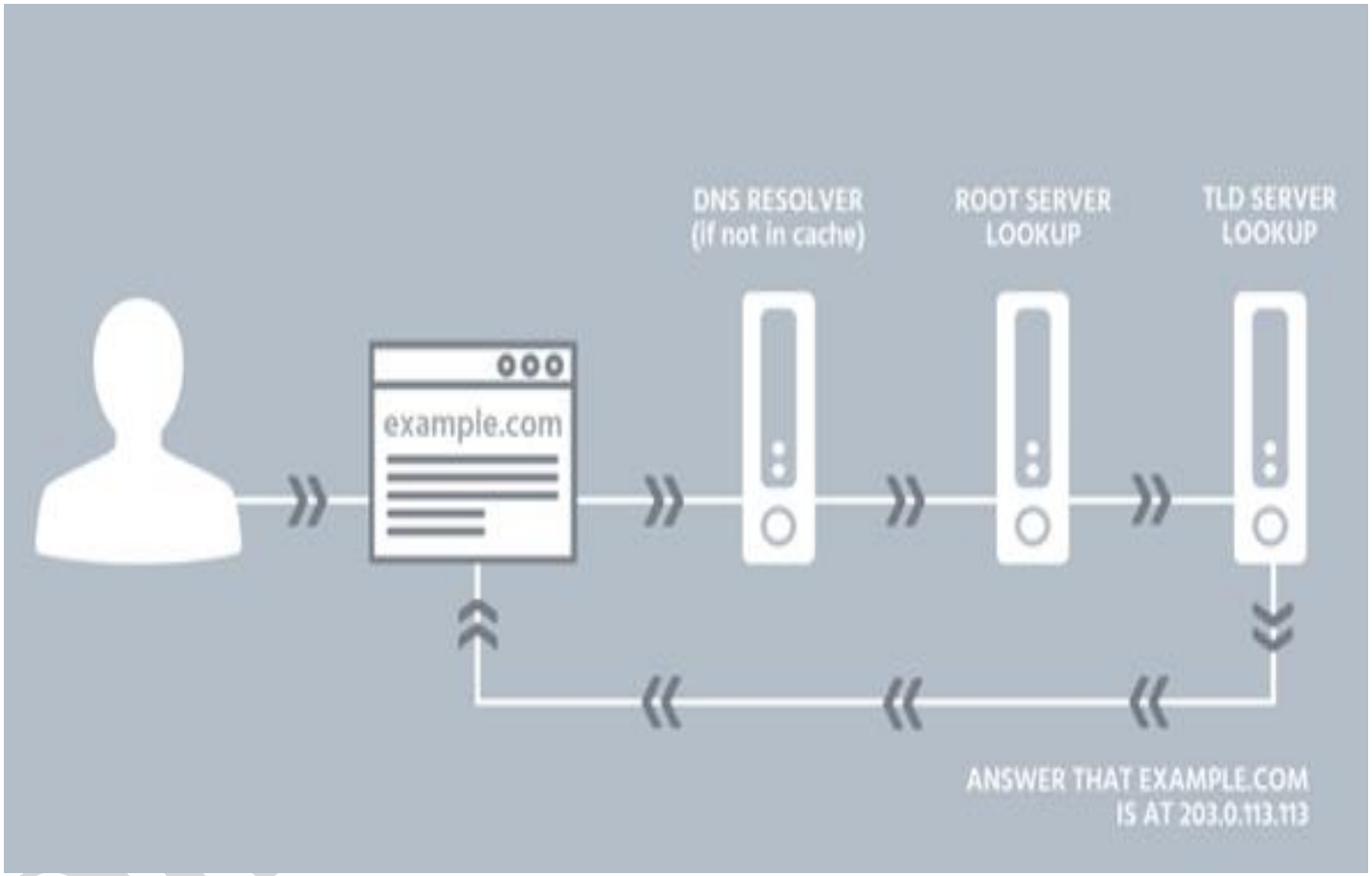


- ✓ Classified into two types:-
  - ✓ **Signature-based detection- it** is based on a dictionary of uniquely identifiable patterns (or signatures) in the code of each exploit.
- ✓ **Statistical Anomaly Detection**
  - ✓ Takes samples of network traffic at random and compares them to a pre-calculated baseline performance level.
  - ✓ If the sample of network traffic activity is outside the parameters of baseline performance, the IPS takes action to handle the situation.

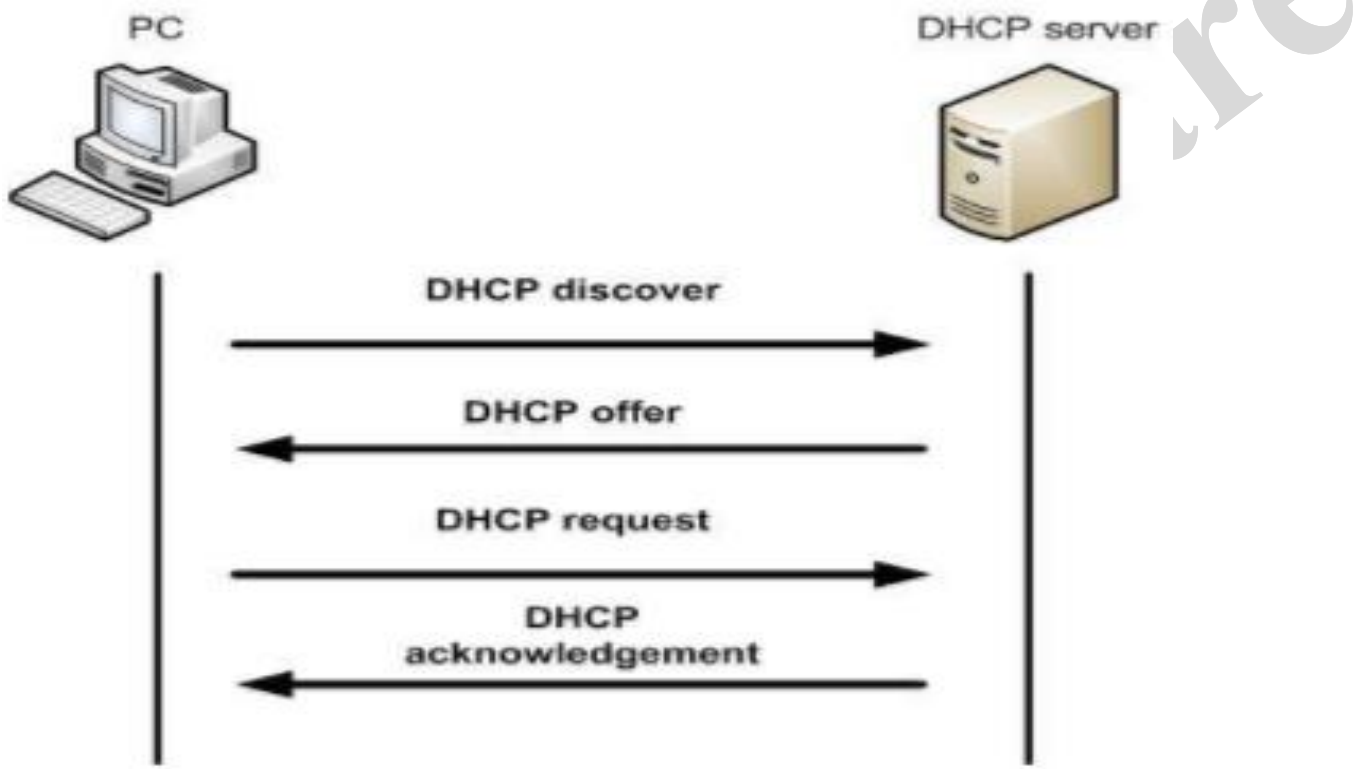

IPS
Intrusion Prevention System
Company Systems
IPS
connected to
mirror port
on switch
Switch
With mirror port for IPS
Internet
Firewall
Router
to
Internet
Company Employees

PARAMETER	FIREWALL	IPS	IDS
Abbreviation for	-	Intrusion Prevention System	Intrusion Detection System
Philosophy	Firewall is a network security device that filters incoming and outgoing network traffic based on predetermined rules	IPS is a device that inspects traffic, detects it, classifies and then proactively stops malicious traffic from attack.	An intrusion detection system (IDS) is a device or software application that monitors a traffic for malicious activity or policy violations and sends alert on detection.
Principle of working	Filters traffic based on IP address and port numbers	inspects real time traffic and looks for traffic patterns or signatures of attack and then prevents the attacks on detection	Detects real time traffic and looks for traffic patterns or signatures of attack and them generates alerts
Configuration mode	Layer 3 mode or transparent mode	Inline mode , generally being in layer 2	Inline or as end host (via span) for monitoring and detection
Placement	Inline at the Perimeter of Network	Inline generally after Firewall	Non-Inline through port span (or via tap)
Traffic patterns	Not analyzed	Analyzed	Analyzed
Placement wrt each other	Should be 1st Line of defense	Should be placed after the Firewall device in network	Should be placed after firewall
Action on unauthorized traffic detection	Block the traffic	Preventing the traffic on Detection of anomaly	Alerts/alarms on detection of anomaly
Related terminologies	• Stateful packet filtering • permits and blocks traffic by port/protocol rules	• Anomaly based detection • Signature detection • Zero day attacks • Blocking the attack	• Anomaly based detection • Signature detection • Zero day attacks • Monitoring • Alarm

- ✓ **DNS(Domain Name System)**
  - ✓ Phone book of the internet.
  - ✓ DNS translates domain names to IP Address so browsers can load Internet resources.
  - ✓ DNS servers eliminate the need for humans to memorize IP Address.
  - ✓ How it works?
    - ✓ Fully qualified domain name (FQDN) such as "www.example.com" typed by the user/client.
    - ✓ A client can sometimes answer a query locally using cached (stored) information obtained from a previous query.
    - ✓ DNS server can also query or contact other DNS servers on behalf of the requesting client to fully resolve the name, then send an answer back to the client. This process is known as *recursion (with ISP or 3rd party)*.
    - ✓ If DNS Resolver does not have the answer, so it has to go to the Root server.
    - ✓ Root server directs to the correct (Top Level Domain) TLD Server.


DNS RESOLVER
(if not in cache)
ROOT SERVER
LOOKUP
TLD SERVER
LOOKUP
example.com
ANSWER THAT EXAMPLE.COM
IS AT 203.0.113.113

- ✓ **DHCP(Dynamic Host Configuration Protocol)**
  - ✓ DHCP is part of "Application Layer," of OSI model.
  - ✓ DHCP server is one computer on the network that has a number of IP address at its disposal to assign to the computers/hosts on that network (ISP DHCP Server).
  - ✓ DHCP provides IP addresses that "expires. It actually leases that connection identifier (IP) to computer for a specific amount of time (default lease is 05 days).
  - ✓ How it works, when user go online?
    - ✓ User log go on to computer to connect to the Internet.
    - ✓ Network requests an IP address (this is actually referred to as a DHCP discover message).
    - ✓ On behalf of user computer's request, the DHCP server allocates (leases) to user computer an IP address. This is referred to as the DHCP offer message.
    - ✓ User computer (remember—user is DHCP client) takes the first IP address offer that comes along. It then responds with a DHCP request message that verifies the IP address that's been offered and accepted.
    - ✓ DHCP then updates the appropriate network servers with the IP address and other configuration information for user computer.
    - ✓ User computer accepts the IP address for the lease term.


PC
DHCP server
DHCP discover
DHCP offer
DHCP request
DHCP
acknowledgement

Mail Server

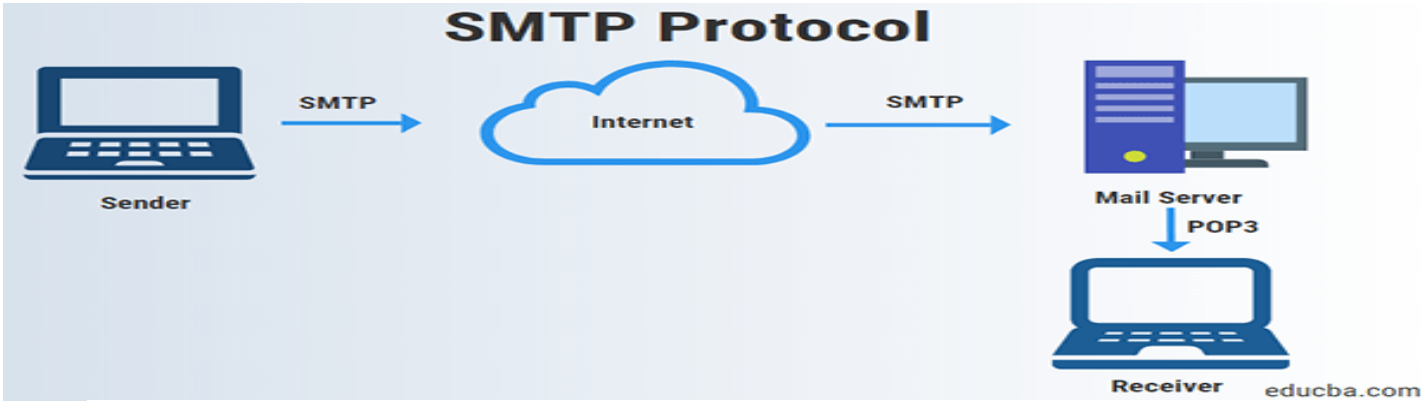
- ✓ **Email client is used to compose & send email**.
- ✓ **email client** connects to the **Outgoing SMTP server** and handovers the email in **MIME format.**
- ✓ Outgoing SMTP validates the **sender details** and processes the message for sending and places it in **Outgoing queue**.
- ✓ **SMTP server** based on the domain details in the recipient address, looks up the **DNS Server** of the domain and retrieves the **Recipient server information (MX records/ A Records** in case **no MX record** is found) of the recipient domain.
- ✓ **SMTP Server** connects with the **Recipient email server** and sends the email through SMTP protocol.
- ✓ **Recipient server** in turn validates the recipient account and delivers the email to the users mail account.
- ✓ User views the received email using his email client.

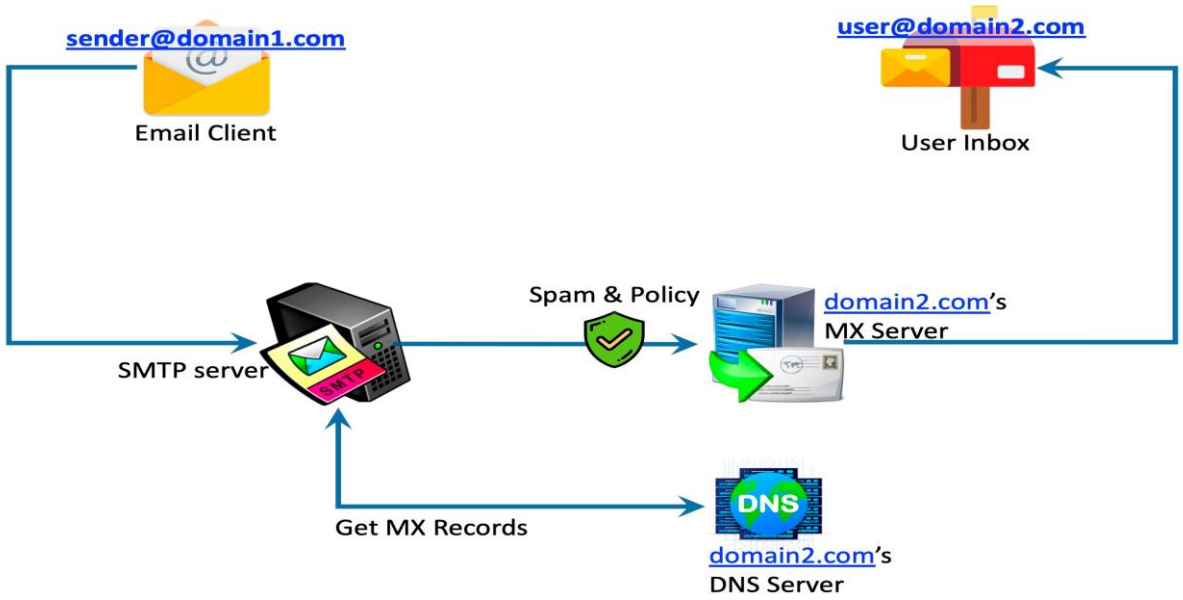
- **MX (Mail Exchange)** records are DNS records that are necessary for delivering email to your address.
- The A **record** simply points the host name to the IP address. MX record points to your mail domain name for e.g. company.com > mail.company.com, and an A record points to a mail server IP address.

*MIME(Multipurpose Internet Mail Extension) is an *add on or a supplementary protocol* which allows non-ASCII data to be sent through SMTP(audio, video images)

* POP v3(Post Office Protocol) and IMAP(Internet Message Access Protocol) are two protocols which are used for receiving mails in inbox.

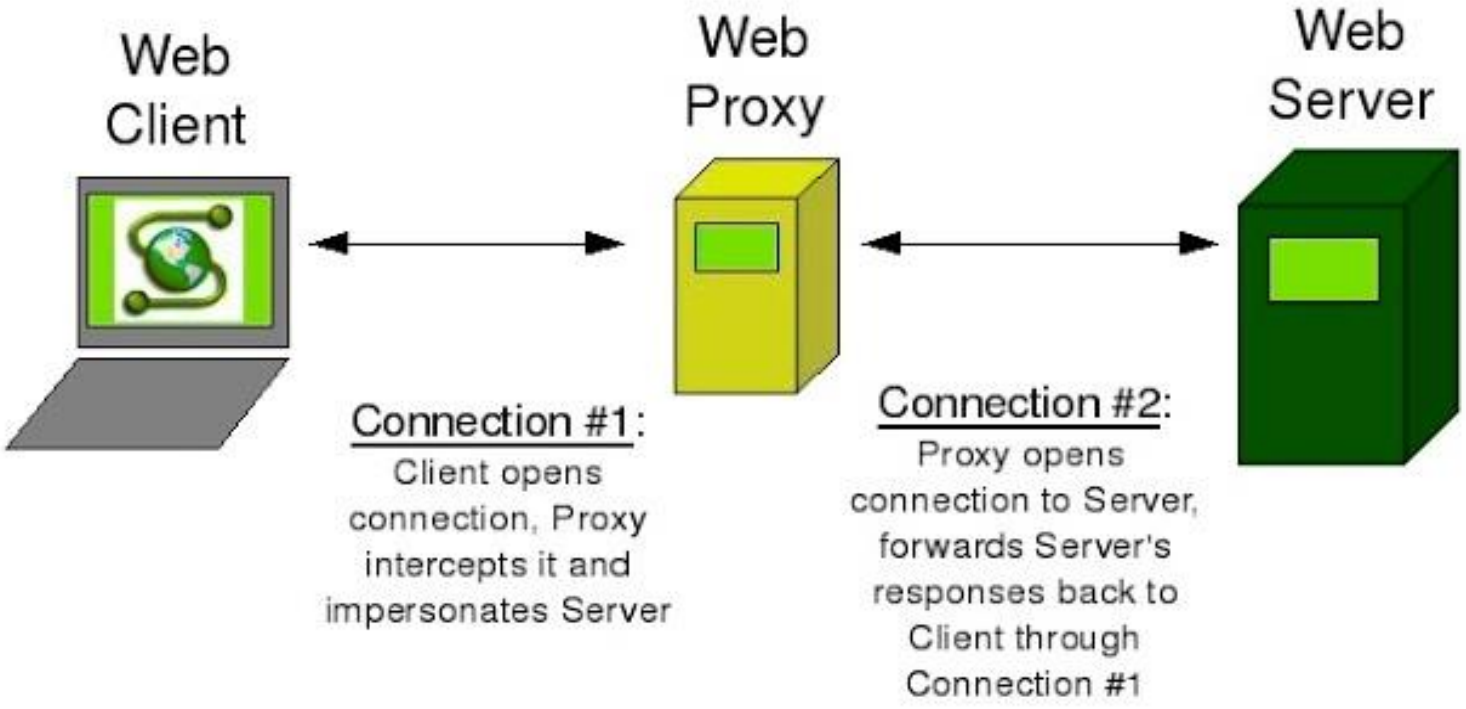
Mail Server


SMTP Protocol
SMTP
Internet
SMTP
Sender
Mail Server
POP3
Receiver
educba.com

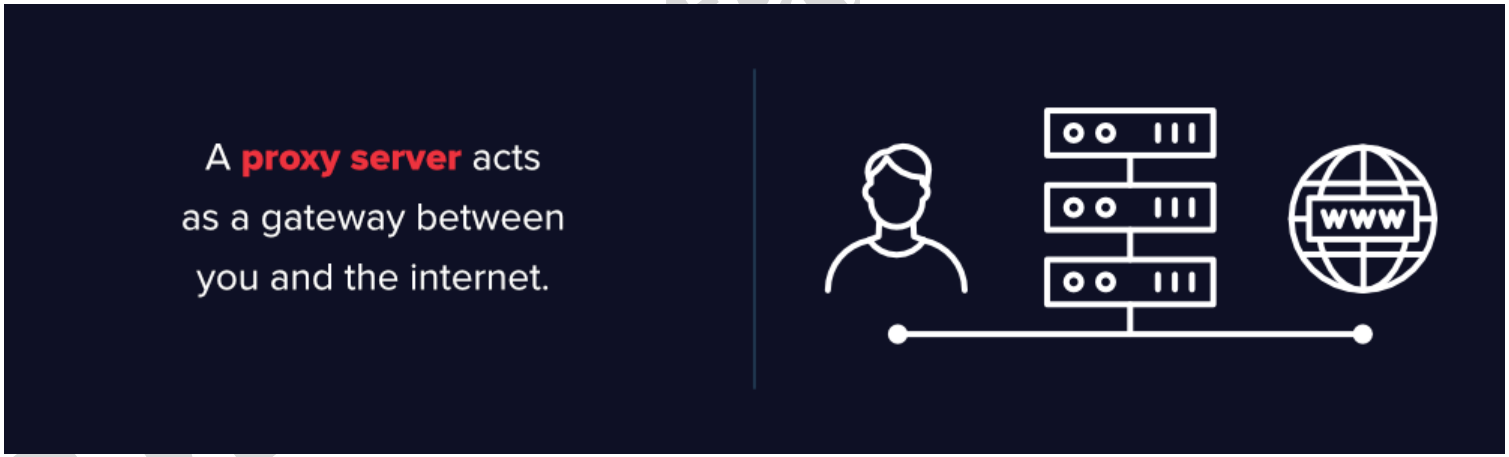

sender@domain1.com
Email Client
user@domain2.com
User Inbox
SMTP server
Spam & Policy
domain2.com's
MX Server
Get MX Records
DNS
domain2.com's
DNS Server

Web Proxies

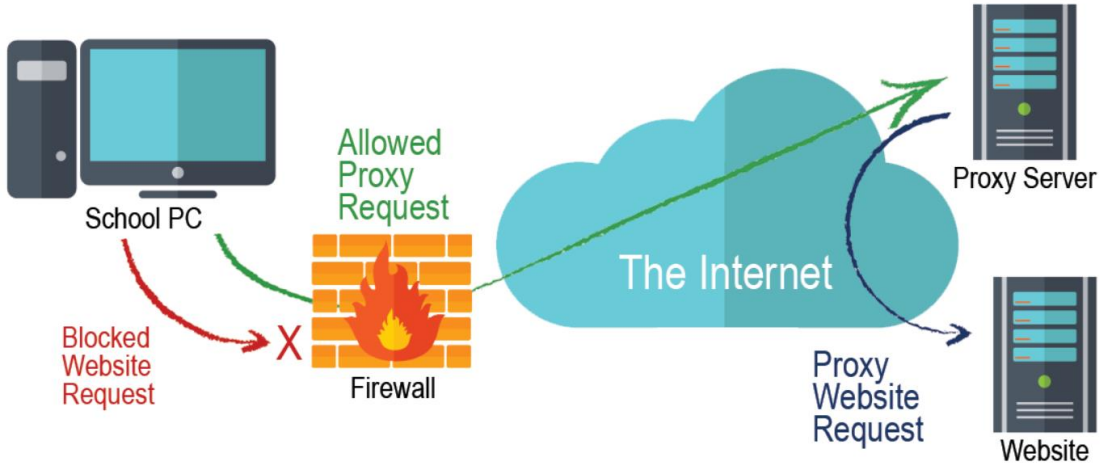
- ✓ A web proxy is one method for hiding clients IP Address from the visiting websites.
- ✓ Web proxies act as shield between the client and and the website being visited.
- ✓ When viewing a web page through a web proxy, the website sees that a specific IP Address is accessing its server, but the address doesn't belong to client because all of the web traffic between client computer and the web server is first passed through the Proxy Server.
- ✓ Web proxy works by camouflaging user identity (hiding user's IP address), acting as the middle man between user computer and the website client is accessing.
- ✓ This enables the user to privately surf the web making it difficult for malicious forces to infiltrate and acquire your browsing data information.
- ✓ Using a web proxy will also allow a user to access sites that are otherwise inaccessible.


Web Client
Web Proxy
Web Server
Connection #1:
Client opens connection, Proxy intercepts it and impersonates Server
Connection #2:
Proxy opens connection to Server, forwards Server's responses back to Client through Connection #1

- The risk of that is the looming danger of crimes such as identity theft and data security breaches. Different individuals use proxy servers or **(VPN)** to protect themselves. A proxy server is a web server that acts as a gateway between a client application, for example, a browser, and the real server. It makes requests to the real server on behalf of the client or sometimes fulfills the claim itself.
- Web proxy servers have two primary purposes, namely to filter requests and improve performances. Additionally, there are proxy servers that sit between web servers and web clients known as a reverse proxy. Reverse proxy servers pass on requests from web clients to web servers.



What are web proxy servers used for?



- **Control internet access**
- **Privacy benefits**
- **Access to blocked sites**
- **Improved security**

Why to investigate

- A web proxy can literally contain the web browsing history of an entire organization all in one place.
- Caching proxy—Stores previously used pages to speed up performance.
- Content filter—Inspects the content of web traffic and filters based on keywords, presence of malware, or other factors.
- TLS/SSL proxy—Intercepts web traffic at the session layer to inspect the content of TLS/SSL-encrypted web traffic.
- Anonymizing proxy—Acts as an intermediary to protect the identities of web surfers.
- Reverse proxy—Provides content inspection and filtering of inbound web requests from the Internet to the web server

- Caching—Locally storing web objects for limited amounts of time and serving them in response to client web requests to improve performance.
- URI Filtering—Filtering web requests from clients in real-time according to a blacklist, whitelist, keywords, or other methods.
- Content Filtering—Dynamically reconstructing and filtering content of web requests and responses based on keywords, antivirus scan results, or other methods.
- Distributed Caching—Caching web pages in a distributed hierarchy consisting of multiple caching web proxies in order to provide locally customized web content, serve advertisements, and improve performance.

Types of Evidence

- Persistent
- History of all HTTP or HTTPS traffic, including blogs, IM, web mail, etc. Volatility varies based on storage space, level of web activity, and configuration options.
- Web access logs tend to be stored on disk for significant periods of time. Often, system administrators do not realize the length of time or granularity of the data that is cached, and years' worth of web history can accumulate without notice.
- Blocked web traffic attempts
- Summarized user activity reports
- Web proxy configuration files

Obtaining Evidence

- Log files stored on the web proxy server or a logging server
- Web cache files stored on the web proxy server
- Reports from tools built into the web proxy server

Security Information and Event Management (SIEM)

A SIEM is a collection of cybersecurity components used to monitor network traffic and resources.

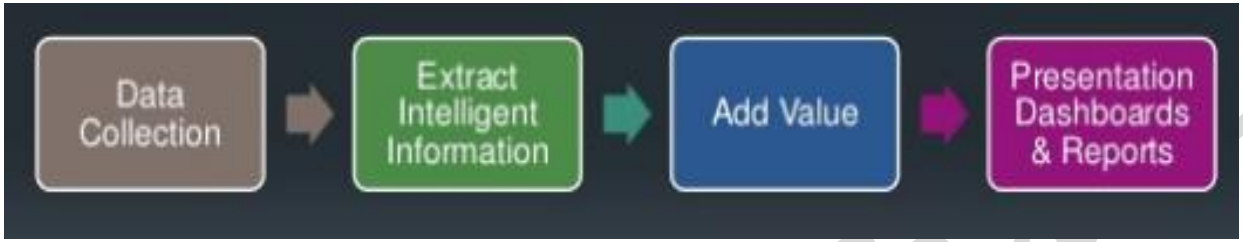
- From a user perspective, it's a centralized dashboard of security information used to display alerts and suspicious network activity to a security analyst. It's a platform containing:
- Log aggregation from multiple sources
- Threat intelligence
- Event correlation and organization for easier analysis
- Advanced analytics visualization
- Customizable dashboards for analytics
- Threat hunting features to find currently compromised resources
- Forensics tools for investigation after a cyber-incident

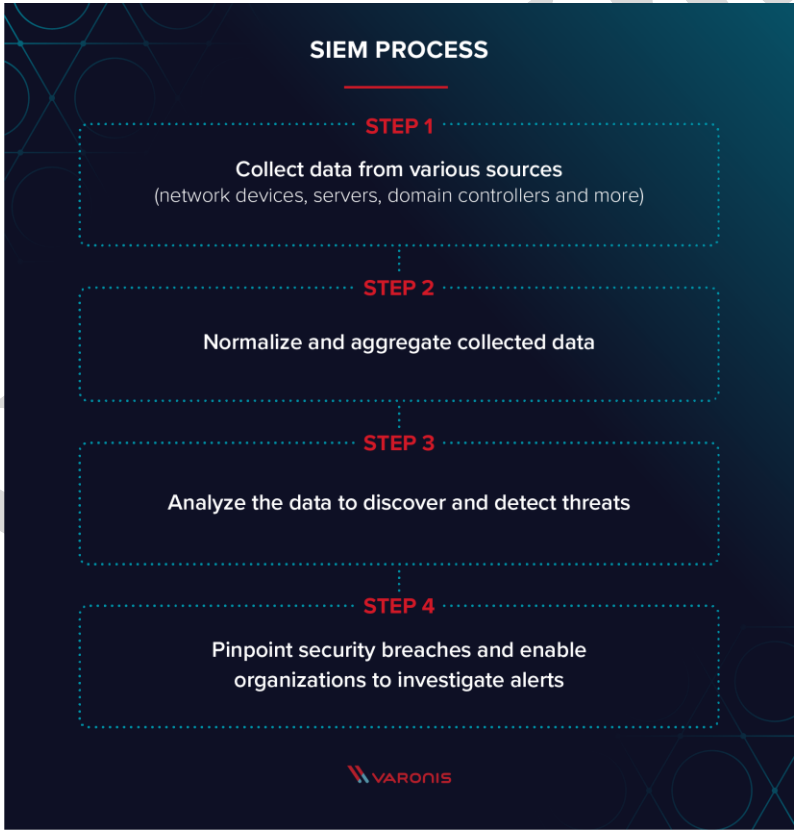
Security Information and Event Management (SIEM)

- ✓Set of tools and services offering a holistic view of an organization's information security.
- ✓SIEM tools provide:-
  - ✓Real-time visibility across an organization's information security systems.
  - ✓Event log management that consolidates data from numerous sources.
  - ✓Correlation of events gathered from different logs or security sources, using if-then that add intelligence to raw data.
  - ✓Automatic security event notifications.
  - ✓Most SIEM systems provide dashboards for security issues and other methods of direct notification.

FEATURES OF SIEM

SIEM PROCESS FLOW





How SIEM works?

- ✓ Combining two technologies (**SIM & SEM**):-
  - ✓ Security Information Management (SIM), which collects data from log files for analysis and reports on security threats and events.
  - ✓ Security Event Management (SEM), which conducts real-time system monitoring, notifies network admins about important issues and establishes correlations between security events.
- ✓ **Entire SIEM Process could be summarised as:-**
- ✓ **Data collection** – All sources of network security information (Servers, OS, FW, AV & IPS) are configured to feed event data into a SIEM tool, which are then processed, filtered and sent them to the SIEM.
- ✓ **Policies** – Profile is created by the SIEM administrator, which defines the behaviour of enterprise systems, both under normal conditions & during pre-defined security incidents.
- ✓ **Data consolidation and correlation** – SIEM solutions consolidate, parse and analyze log files. Events are then categorized based on the raw data and apply correlation rules that combine individual data events into meaningful security issues.

SIEM CAPABLITIES

MAIN FEATURES

- Threat detection
- Investigation
- Time to respond

ADDITIONAL FEATURES

- Basic security monitoring
- Advanced threat detection
- Forensics & incident response
- Log collection
- Normalization
- Notifications and alerts
- Security incident detection
- Threat response workflow

VARONIS

Top SIEM Tools

These are some of the top players in the SIEM space:

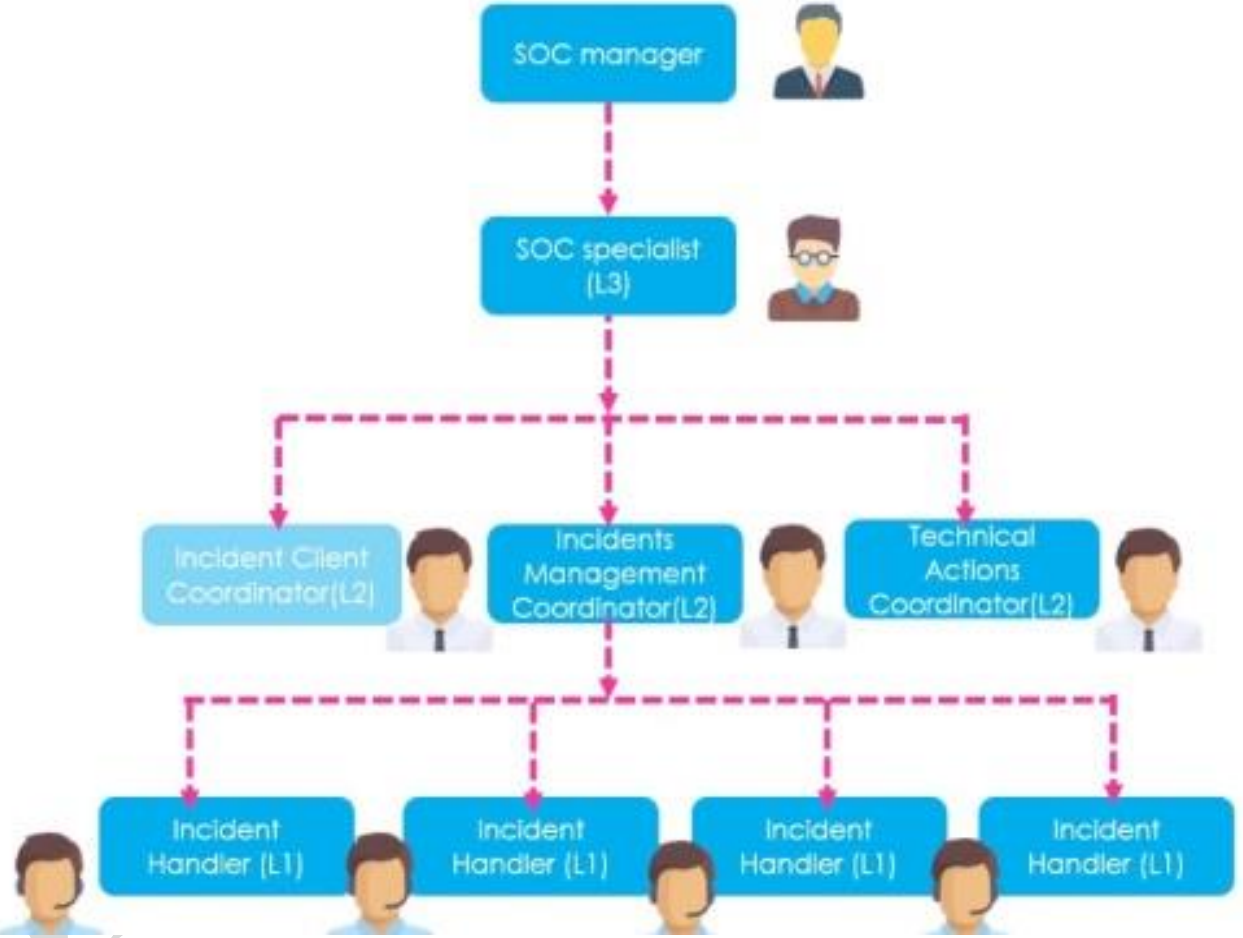
- **Splunk**
- Splunk is a full on-prem SIEM solution that Gartner rates as a leader in the space. Splunk supports security monitoring and can provide advanced threat detection capabilities.
- **IBM QRadar**
- QRadar is another popular SIEM that you can deploy as a hardware appliance, a virtual appliance, or a software appliance, depending on your organization's needs and capacity.
- **LogRhythm**
- LogRhythm is a good SIEM for smaller organizations. You can integrate LogRhythm with Varonis to get threat detection and response capabilities.

Some Open Source Tools:

- OpenSearch
- The ELK Stack
- OSSEC Host Intrusion Detection System (HIDS)
- Snort network intrusion detection system (NIDS)

Security Operation Centre

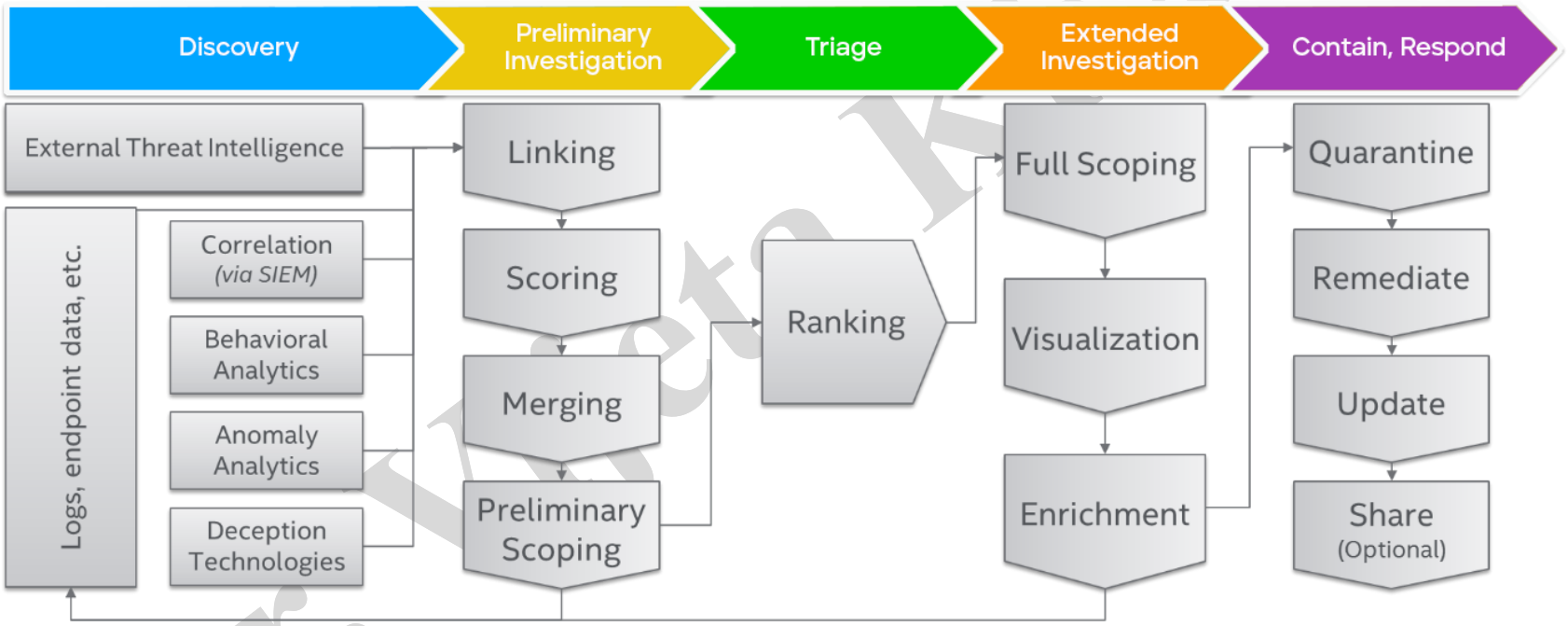
- ✓ Function of a SOC is to maintain situational awareness of events on the computer systems and networks that it monitors.
- ✓ Events occurring on computer systems are monitored by software, and transmitted to the SOC, for logging and review by an analyst team.
- ✓ Essentially, the SOC team are the 'virtual security guards' that protect your network, whereas the IT team build and maintain it.
- ✓ Network monitoring capability allows for the effective prevention, detection and response to any malicious attack.
- ✓ If suspicious event is detected, the SOC can investigate and respond accordingly to reduce both the impact and severity.
- ✓ Effective SOC is a combination of people (SOC management, analysts, response and maintenance staff), procedures (standardised, repeatable processes for defending and responding to incidents on systems) and technology (deployment of software and hardware on the network and Operations Centre to monitor, triage, display and respond to events).


SOC manager
SOC specialist (L3)
Incident Client Coordinator(L2)
Incidents Management Coordinator(L2)
Technical Actions Coordinator(L2)
Incident Handler (L1)
Incident Handler (L1)
Incident Handler (L1)
Incident Handler (L1)

What Does a SOC Do?

- Prevention and detection
- Investigation
- Response

Threat management plans integrate and structure many processes across security and IT operations.

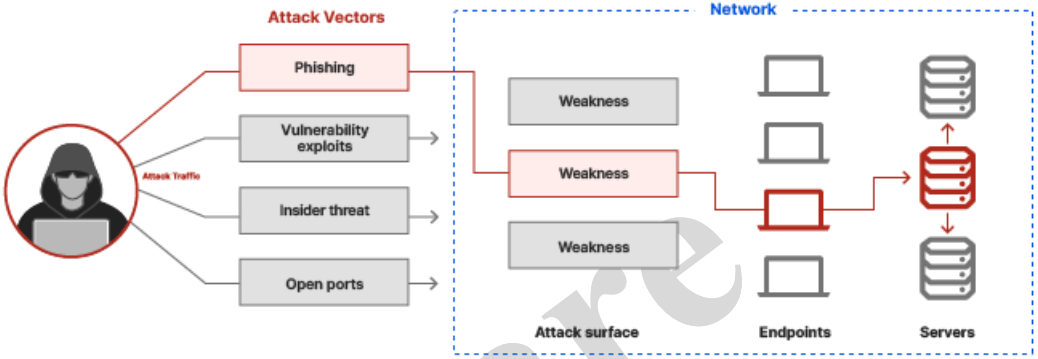


When a SOC is implemented correctly, it provides numerous benefits including the following:

- Continuous monitoring and analysis of system activity.
- Improved incident response.
- Decreased timeline between when a compromise occurs and when it is detected.
- Reduced downtime.
- Centralization of hardware and software assets leading to a more holistic, real time approach to infrastructure security.
- Effective collaboration and communication.
- Reduction in direct and indirect costs associated with the management of cyber security incidents.
- Employees and customers trust the organization and become more comfortable with sharing their confidential information.
- Greater control and transparency over security operations.
- Clear chain of control for systems and data, something that’s crucial for the successfully prosecution of cybercriminals.

SOC Challenges

- Shortage of cybersecurity skills
- Sophisticated Attackers
- Too many alerts
- Voluminous Data and Network Traffic
- Unknown Threats
- Security Tool Overload



Attack Vectors

- ✓Attack vector is a path or means by which one can gain access to a computer or network server in order to deliver a payload or malicious outcome.
- ✓Attack vectors enables exploitation of system vulnerabilities, including the human element.
- ✓Attack vectors include viruses, e-mail attachments, Web pages, pop-up windows, instant messages, chat rooms, and deception.
- ✓All of these methods involve programming (or, in a few cases, hardware), except deception, in which a human operator is fooled into removing or weakening system defences.
- ✓The most common malicious payloads are viruses, Trojan horses, worms, and spyware. If an attack vector is thought of as a guided missile, its payload can be compared to the warhead in the tip of the missile.

What are some of the most common attack vectors?

- Phishing: Phishing involves stealing data, such as a user's password, that an attacker can use to break into a network. Attackers gain access to this data by tricking the victim into revealing it.
- Email attachments
- Account takeover: via phishing attack, brute force attack, or purchasing them on the underground market.
- Lack of encryption
- Insider threats
- Vulnerability exploits
- Browser-based attacks: Attackers can inject malicious code into a website or direct users to a fake website, tricking the browser into executing code that downloads malware or otherwise compromises user devices.
- Application compromise
- Open ports: A port is a virtual entryway into a device. Ports help computers and servers associate network traffic with a given application or process.

How can an organization secure its attack vectors?

- Good security practices
- Encryption
- Browser isolation
- Patching vulnerabilities
- Secure access service edge (SASE): is a cloud-based IT model that bundles software-defined networking with network security functions and delivers them from a single service provider

Attack surface

- ✓Attack surface is the total sum of all the vulnerabilities in a given computing device or network that are accessible to the attackers.
- ✓Attack surface may be categorized into different areas:-
  - ✓Such as software attack surfaces (open ports on a server).
  - ✓Physical attack surfaces (USB ports on a laptop).
  - ✓Network attack surfaces (console ports on a router).
  - ✓Human/social engineering attack surfaces (employees with access to sensitive information).
- ✓This includes not only Software, OS, Network services and protocols but also domain names and SSL certificates.

EXAMPLES OF ATTACK

Phishing

- ✓ Phishing is a attack often used to steal user data, including login credentials and credit card numbers.
- ✓Attacker, masquerading as a trusted entity, dupes a victim into opening an email, instant message, text message or
- ✓Tricked into clicking a malicious link, which can lead to the installation of malware, the freezing of the system as part of a ransomware attack or the revealing of sensitive information.
- ✓Well known phishing attacks are:-
  - ✓Blind phishing: Send link to many
  - ✓Spear phishing: Targeted
  - ✓Vishing (Voice + Phishing: Vishing)
  - ✓Smishing (SMS + Phishing: Smishing)

MAC FLOODING

- ✓ Switches maintain a table structure called MAC Table (MAC addresses & Port No).
- ✓ The aim of the MAC Flooding is to takedown this MAC Table.
- ✓ Attacker sends Ethernet Frames in a huge number to consume the memory of the switch that stores MAC address table.
- ✓ The MAC addresses of legitimate users will be pushed out of the MAC Table. Now the switch cannot deliver the incoming data to the destination system. So considerable number of incoming frames will be flooded at all ports.
- ✓ MAC Address Table is full and it is unable to save new MAC addresses. It will lead the switch to enter into a fail-open mode and the switch will now behave same as a network hub. It will forward the incoming data to all ports like a broadcasting.
- ✓ As the attacker is a part of the network, the attacker will also get the data packets intended for the victim machine. So that the attacker will be able to steal sensitive data from the communication.

DOS AND DDOS ATTACKS

- ✓A denial-of-service (**DoS**) is an **attack** where the attackers attempt to prevent legitimate users from accessing the service.
- ✓In a **DoS attack**, the attacker usually sends excessive messages asking the network or server to authenticate requests that have invalid return addresses.

DDoS

- ✓Denial of Service (**DoS**) **attack** is **different** from a **DDoS attack**.
- ✓**DoS attack** typically uses one computer and one Internet connection to flood a targeted system or resource.
- ✓**DDoS attack** uses multiple computers and Internet connections to flood the targeted resource.

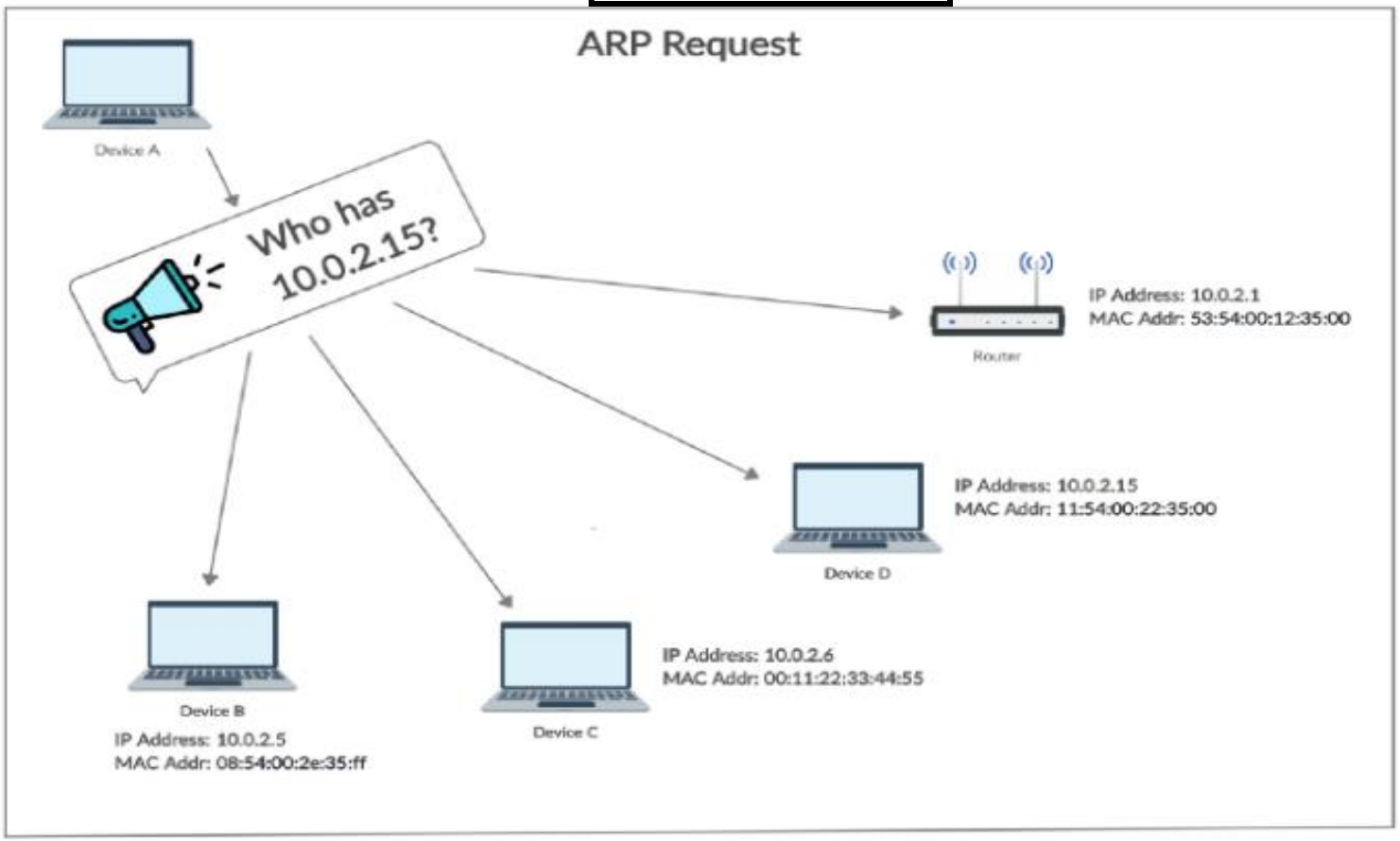
ARP Protocol

- ✓ Address Resolution Protocol (ARP) is a protocol that enables network communications to reach a specific device on the network.
- ✓ ARP translates Internet Protocol (IP) addresses to a Media Access Control (MAC) address, and vice versa.
- ✓ Most commonly, devices use ARP to contact the router or gateway that enables them to connect to the Internet.
- ✓ Hosts maintain an ARP cache, a mapping table between IP addresses and MAC addresses, and use it to connect to destinations on the network. If the host doesn't know the MAC address for a certain IP address, it sends out an ARP request packet, asking other machines on the network for the matching MAC address.
- ✓ The ARP protocol was not designed for security, so it does not verify that a response to an ARP request really comes from an authorized party. It also lets hosts accept ARP responses even if they never sent out a request.
- ✓ This is a weak point in the ARP protocol, which opens the door to ARP spoofing attacks.
- ✓ ARP only works with 32-bit IP addresses in the older IPv4 standard.
- ✓ The newer IPv6 protocol uses a different protocol, Neighbor Discovery Protocol (NDP), which is secure and uses cryptographic keys to verify host identities. However, since most of the Internet still uses the older IPv4 protocol, ARP remains in wide use.

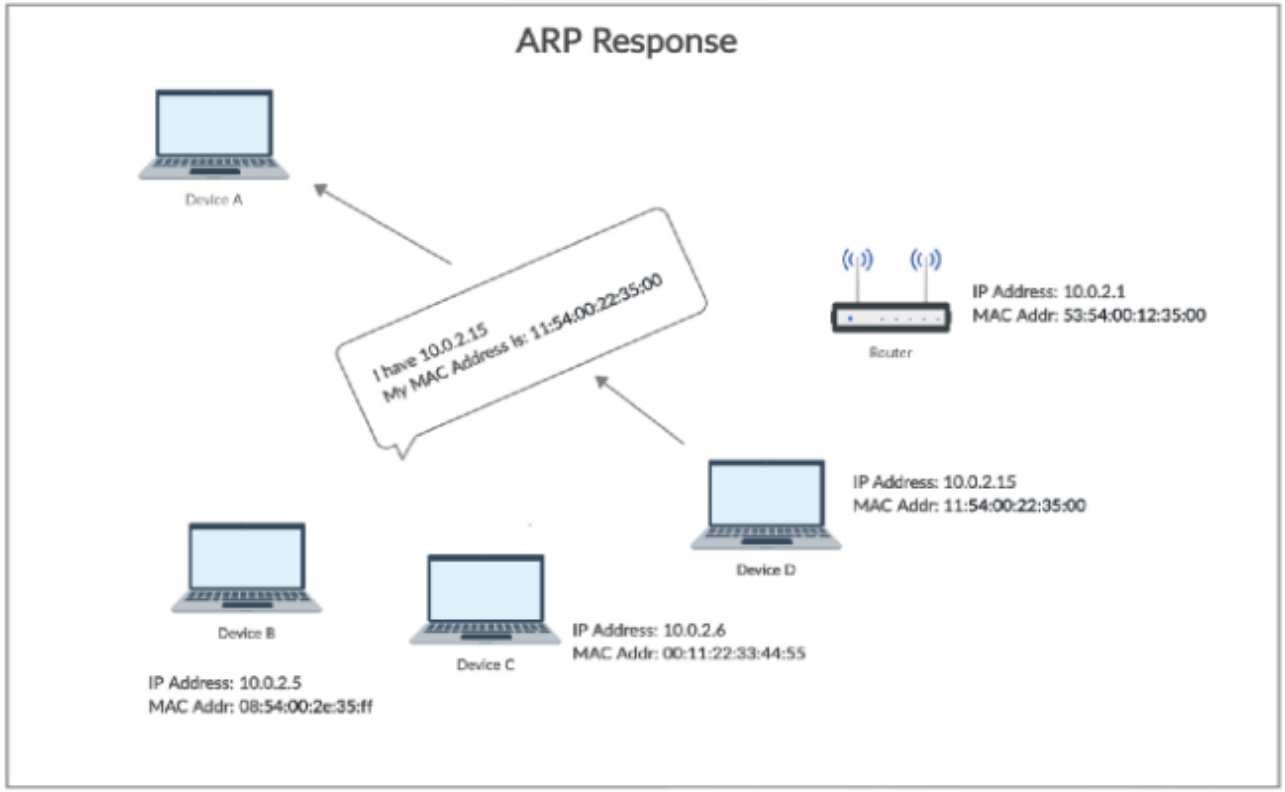
What Address Resolution Protocol (ARP) Works?

- ✓ In a network, computers use the **IP Address** to communicate with other devices, however, in reality, the communication happens over the **MAC Address.**
- ✓ **ARP is used to find out the MAC Address of a particular device whose IP address is known.**
- ✓ For instance, a device wants to communicate with the other device on the network, then the sending device uses ARP to find the MAC Address of the device that it wants to communicate with.
- ✓ ARP involves two steps to find the MAC address:
  - ✓ The sending device sends an **ARP Request** containing the IP Address of the device it wants to communicate with. This request is broadcasted meaning every device in the network will receive this but only the device with the intended IP address will respond.
  - ✓ After receiving the broadcast message, the device with the IP address equal to the IP address in the message will send an **ARP Response** containing its MAC Address to the sender.

ARP REQUEST


ARP Request
Device A
Who has 10.0.2.15?
IP Address: 10.0.2.1
MAC Addr: 53:54:00:12:35:00
Router
IP Address: 10.0.2.15
MAC Addr: 11:54:00:22:35:00
Device D
IP Address: 10.0.2.6
MAC Addr: 00:11:22:33:44:55
Device C
Device B
IP Address: 10.0.2.5
MAC Addr: 08:54:00:2e:35:ff

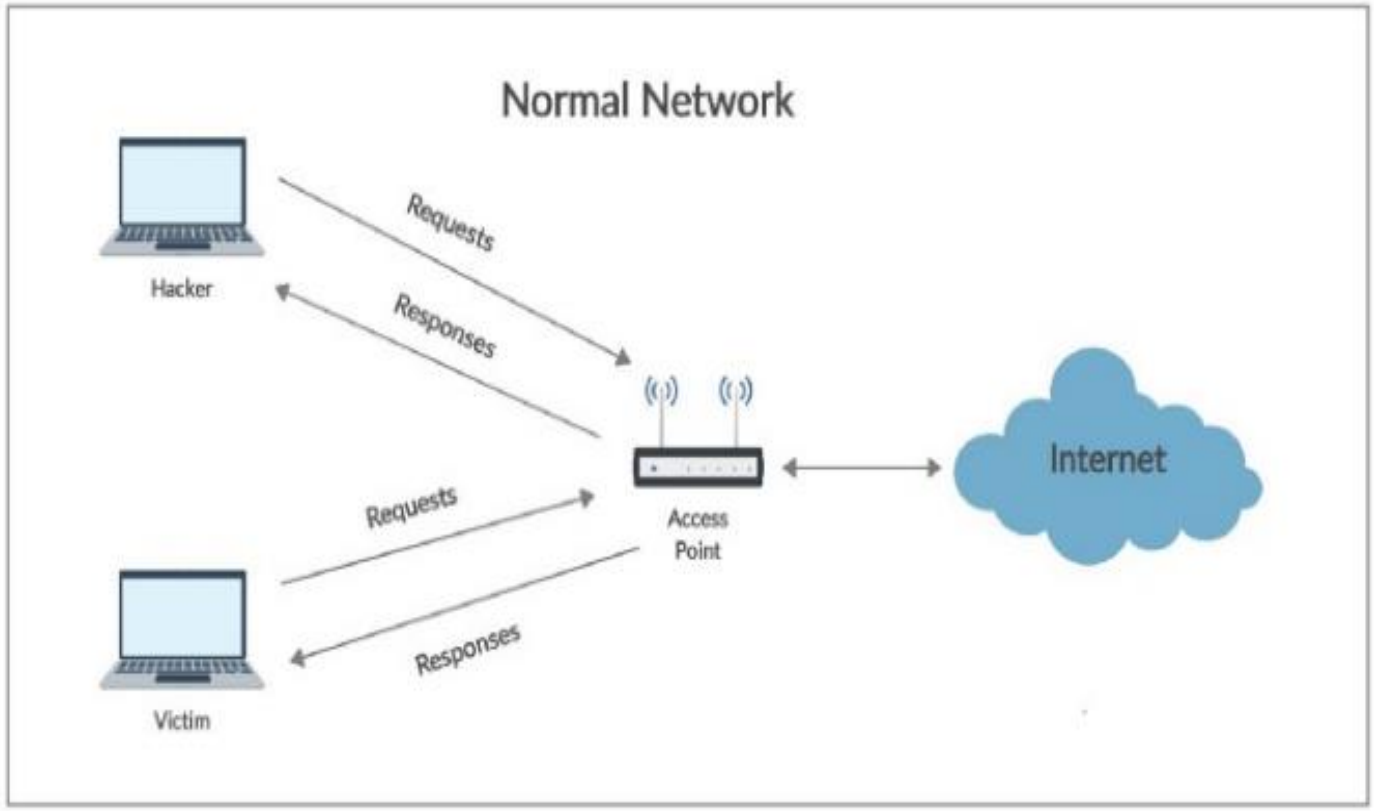
ARP RESPONSE



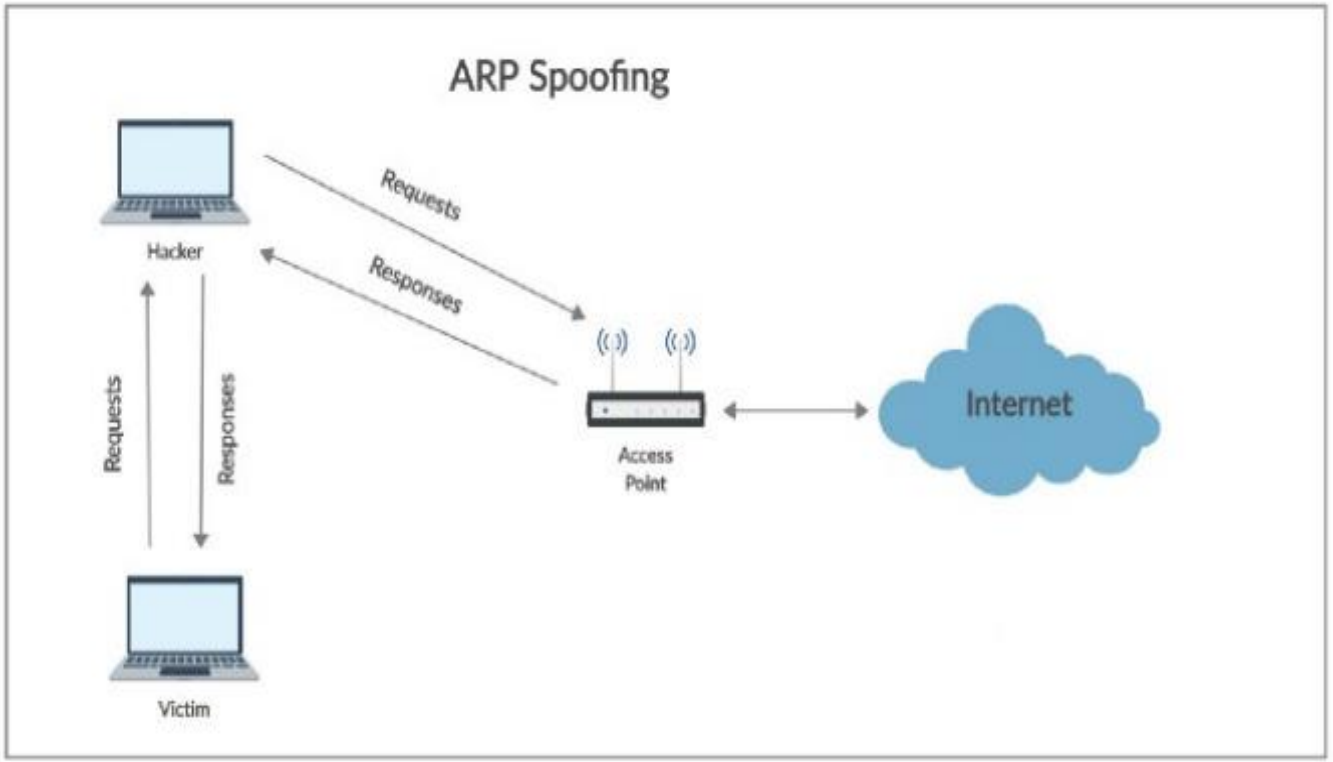
What is ARP Spoofing?

- ✓ ARP spoofing is a **Man In The Middle (MITM)** attack in which the attacker (hacker) sends forged ARP Messages.
- ✓ This allows the attacker to pretend as a legitimate user as it links the attacker machine's MAC Address to the legitimate IP Address of the victim machine.
- ✓ Once the MAC Address has been linked the attacker will now receive the messages intended for the legitimate IP Address(victim machine).
- ✓ Furthermore, ARP Spoofing allows the attacker can intercept, modify, and drop the incoming messages.

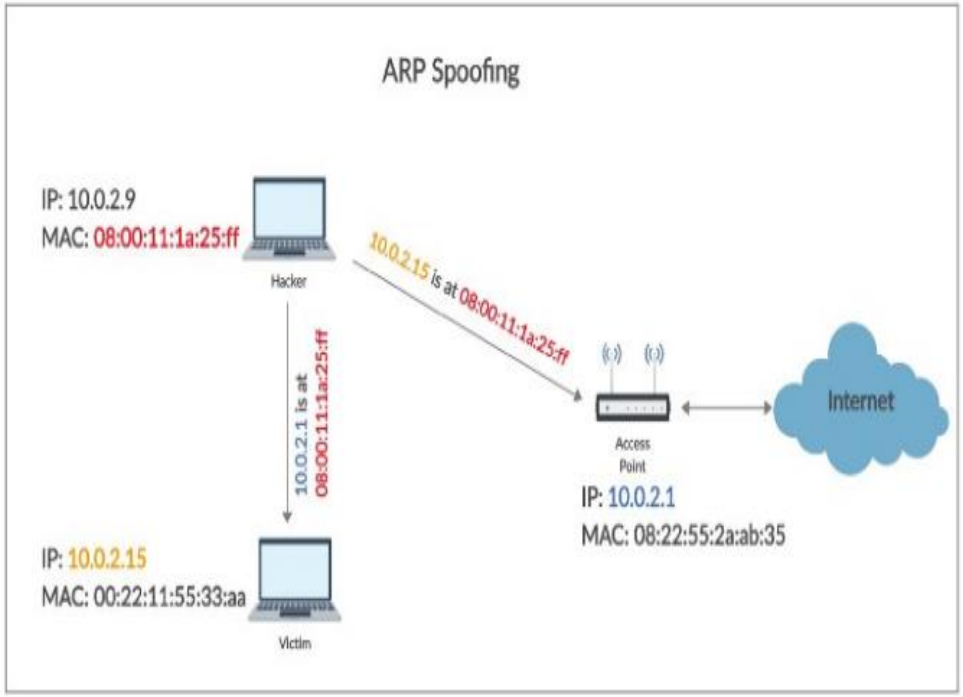
NORMAL NETWORK



ARP SPOOFING



ARP SPOOFING

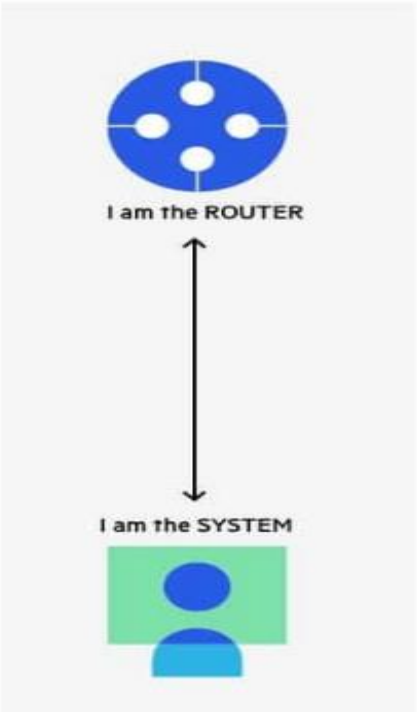


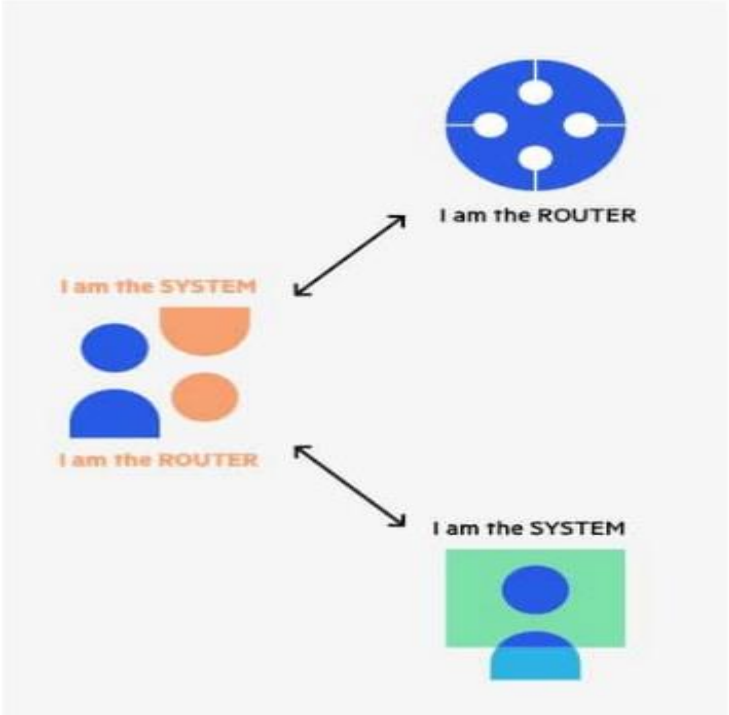
In ARP Spoofing, the hacker simply fools the **access point** and the **victim** by pretending as the **access point** in front of the **victim** and as the **victim** in front of the **access point**.

HOW TO EXECUTE ARP SPOOFING (ARP POISONING)

- ✓ An ARP spoofing, also known as ARP poisoning, is a Man in the Middle (MitM) attack that allows attackers to intercept communication between network devices.
- ✓ The attack works as follows:-
  - ✓ The attacker must have access to the network. They scan the network to determine the IP addresses of at least two devices—let's say these are a workstation and a router.
  - ✓ The attacker uses a spoofing tool, such as Ettercap, Arpspoof or Driftnet, to send out forged ARP responses.
  - ✓ The forged responses advertise that the correct MAC address for both IP addresses, belonging to the router and workstation, is the attacker's MAC address. This fools both router and workstation to connect to the attacker's machine, instead of to each other.
  - ✓ The two devices update their ARP cache entries and from that point onwards, communicate with the attacker instead of directly with each other.
  - ✓ The attacker is now secretly in the middle of all communications.

IP SPOOFING ATTACKER PRETENDS TO BE BOTH SIDES OF A NETWORK COMMUNICATION CHANNEL





Once the attacker succeeds in an ARP spoofing attack, they can:-

- ✓ Continue routing the communications as-is—the attacker can sniff the packets and steal data, except if it is transferred over an encrypted channel like HTTPS.
- ✓ Perform session hijacking—if the attacker obtains a session ID, they can gain access to accounts the user is currently logged into.
- ✓ Alter communication—for example pushing a malicious file or website to the workstation.
- ✓ Distributed Denial of Service (DDoS)—the attackers can provide the MAC address of a server they wish to attack with DDoS, instead of their own machine. If they do this for a large number of IPs, the target server will be bombarded with traffic.