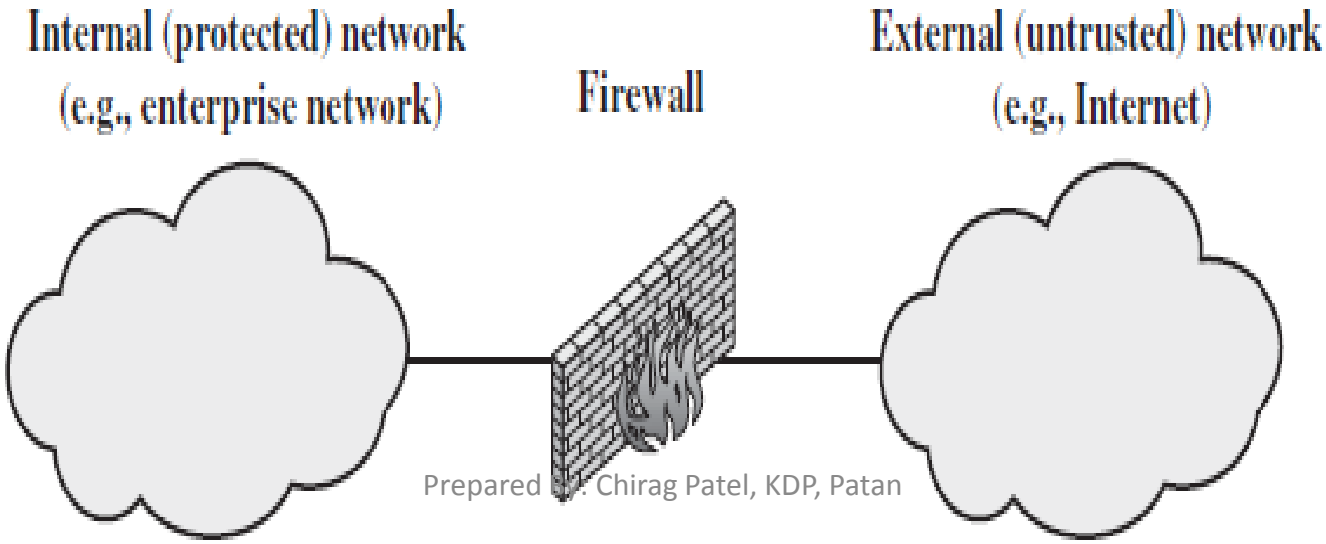
Chapter 4

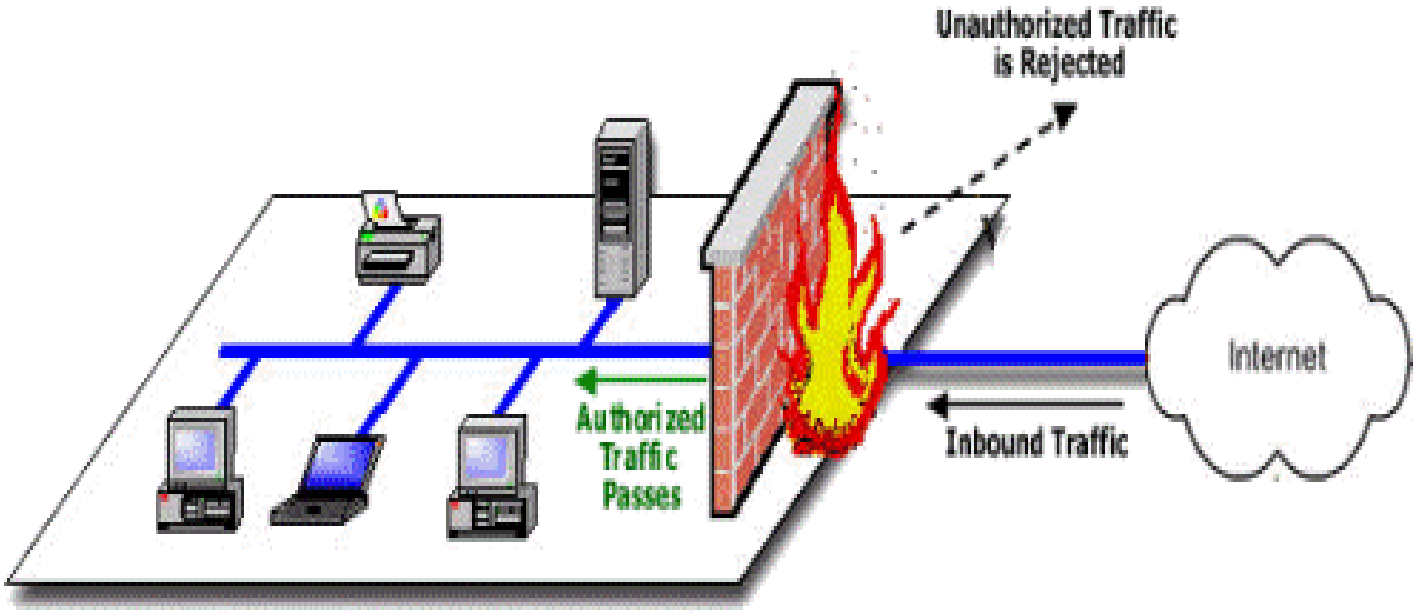
Network Security

Firewalls

- A firewall is a system designed to prevent unauthorized access to or from a private network which is connected to the internet.
- A firewall can be implemented in both hardware and software or combination of both.
- It is generally located between internal and external networks.
- A Firewall is software or hardware based network security system that controls the incoming and outgoing network traffic based on some rules.
- All messages entering or leaving the internet pass through the firewall, Which examines each message and blocks those that do not meet the specified security criteria.



- Some of the limitations of the firewall are listed below;
    1. The firewall cannot protect against attacks that bypass the firewall.
    2. The firewall does not protect against internal threats.
    3. The firewall cannot protect against the transfer of virus-infected programs or files.
    4. It is costly.



Characteristics of Firewall

1. All traffic from or to the internal network must pass through the firewall. This is achieved by physically blocking all access to the local network except via the firewall.

2. Only authorized traffic, as defined by the local security policy, will be allowed to pass. This can be achieved by using the suitable firewall type.

3. Firewall can filter packets based on their source and destination address and port numbers. This is known as packet filtering.

Access Control of Firewall (Design Goals of Firewall)

- **Service control**
  - Determines the types of Internet services that can be accessed, inbound or outbound
- **Direction control**
  - Determines the direction in which particular service requests are allowed to flow through the firewall.
- **User control**
  - Controls access to a service according to which user is attempting to access it.
  - This feature is usually applied for local users inside the firewall.
- **Behavior control**
  - Controls how particular services are used.
  - For example, the firewall may filter e-mail to eliminate spam.

Types of Firewalls

1. Types depending upon Firewalls methodology;
   - Packet-filtering
   - Circuit-level gateways
   - Application-level gateways

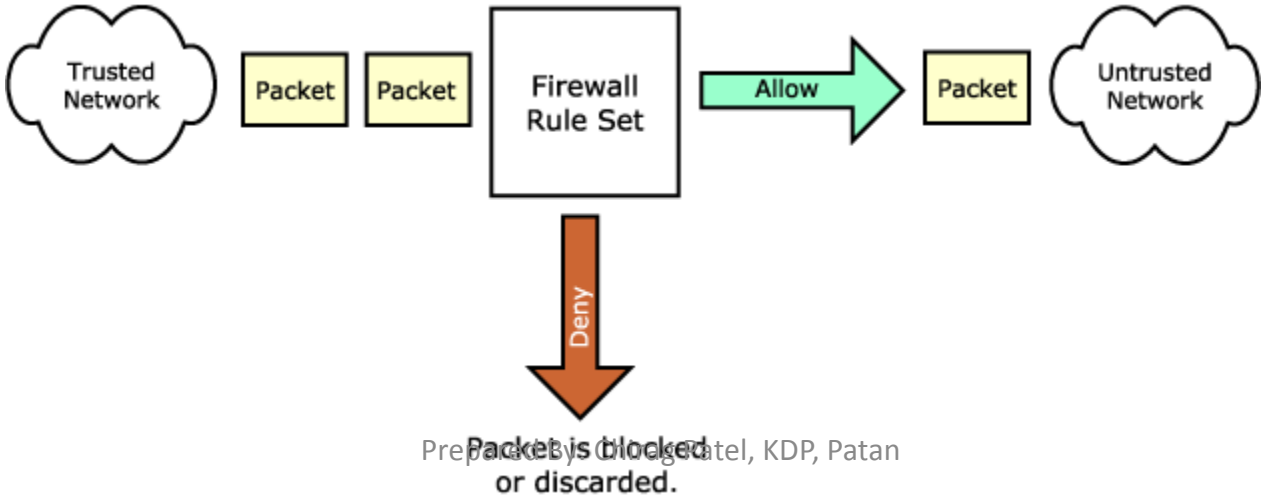
2. With regard to the scope of filtered communications done between a single node and the network, or between two or more networks there exist The firewall can be classified as;
   - Personal firewall
   - Network firewall

3. Types depending on whether the firewalls keeps track of the state of network connections;
   - Stateful firewall
   - Stateless firewall

4. Other
   - Hardware firewall
   - Software firewall

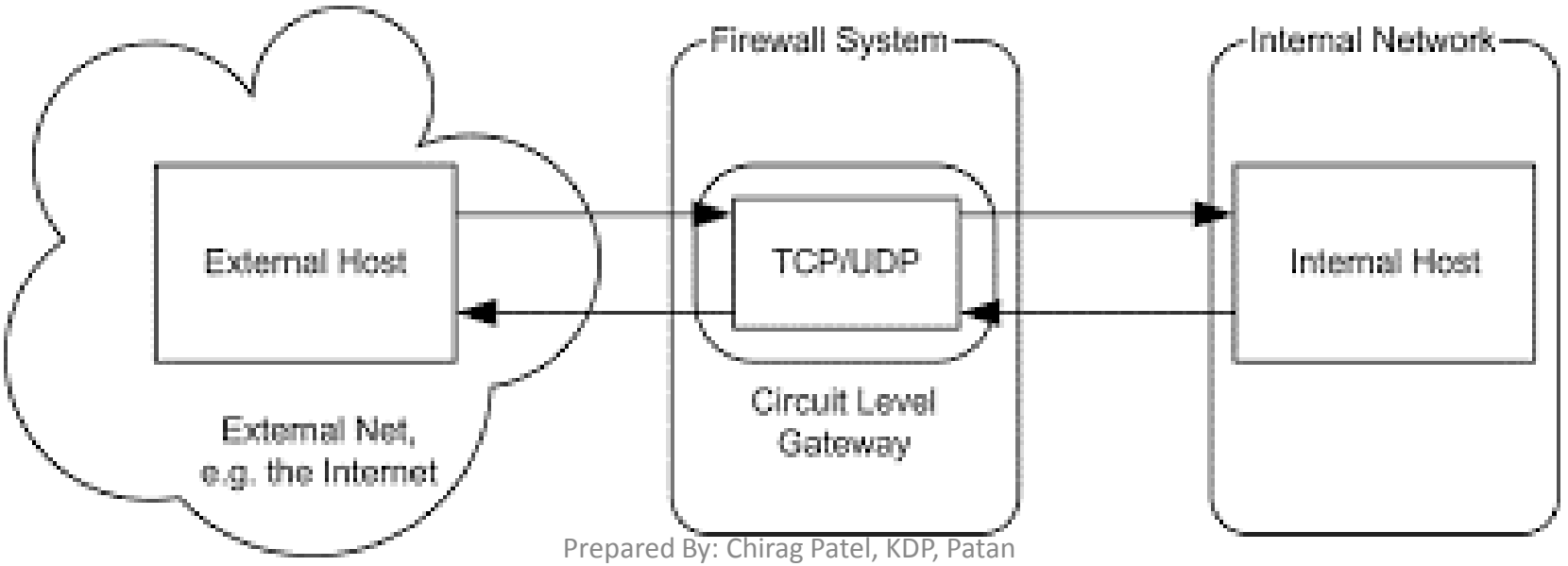
1.1 Packet Filtering Firewall

- **A packet-filtering router applies a set of rules to each incoming and outgoing IP packet and then forwards or discards the packet.**
- The router is typically configured to filter packets going in both directions.
- Filtering rules are based on information contained in a network packet like Source IP address**,** Destination IP address, Source port, Destination port etc.
- As each packet passes through the firewall, it is examined and information contained in the header is compared to a pre-configured set of rules or filters. An allow or deny decision is made based on the results of the comparison.



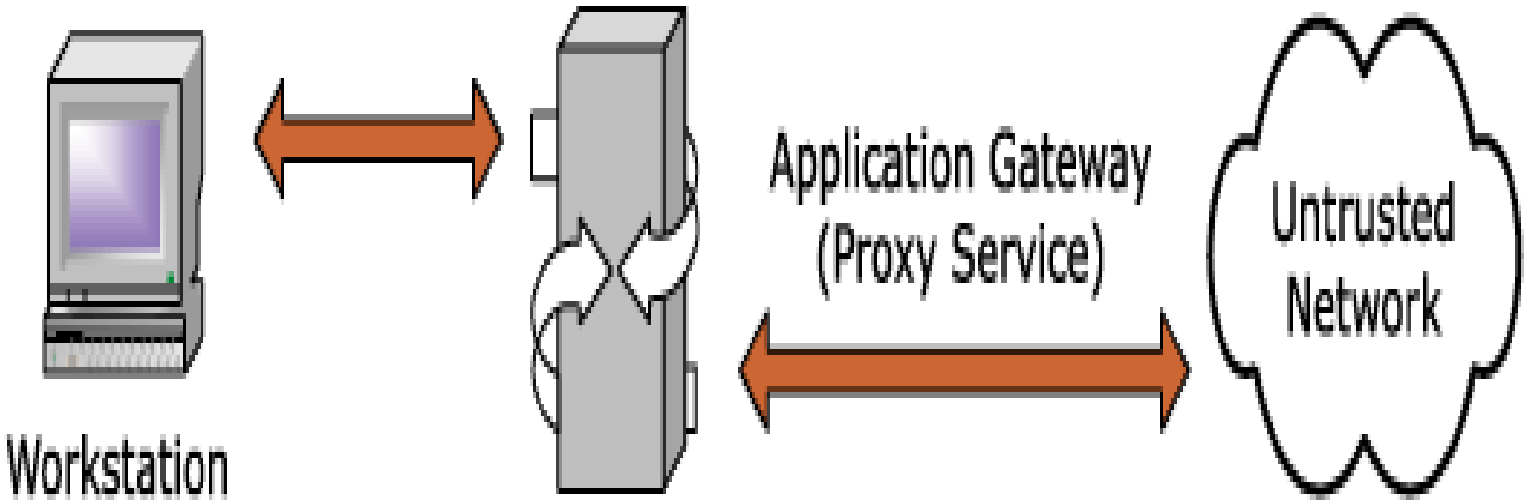
1.2 Circuit-Level Gateway

- It works at session layer of the OSI model or the TCP layer TCP/IP model.
- Unlike a packet filtering firewall, a circuit-level gateway does not examine individual packets. Instead, circuit-level gateways monitor TCP or UDP sessions.
- It monitors TCP handshaking between packets.
- It hides information about the private network.



1.3 Application-Level Gateway

- An application-level gateway, also called **a proxy server, acts as a relay** (**data transmitter**) of application-level.
- It **works at application layer** in both OSI and TCP/IP model.
- Application layer firewall provide all the circuit level firewall features and also provide extensive packet analysis.

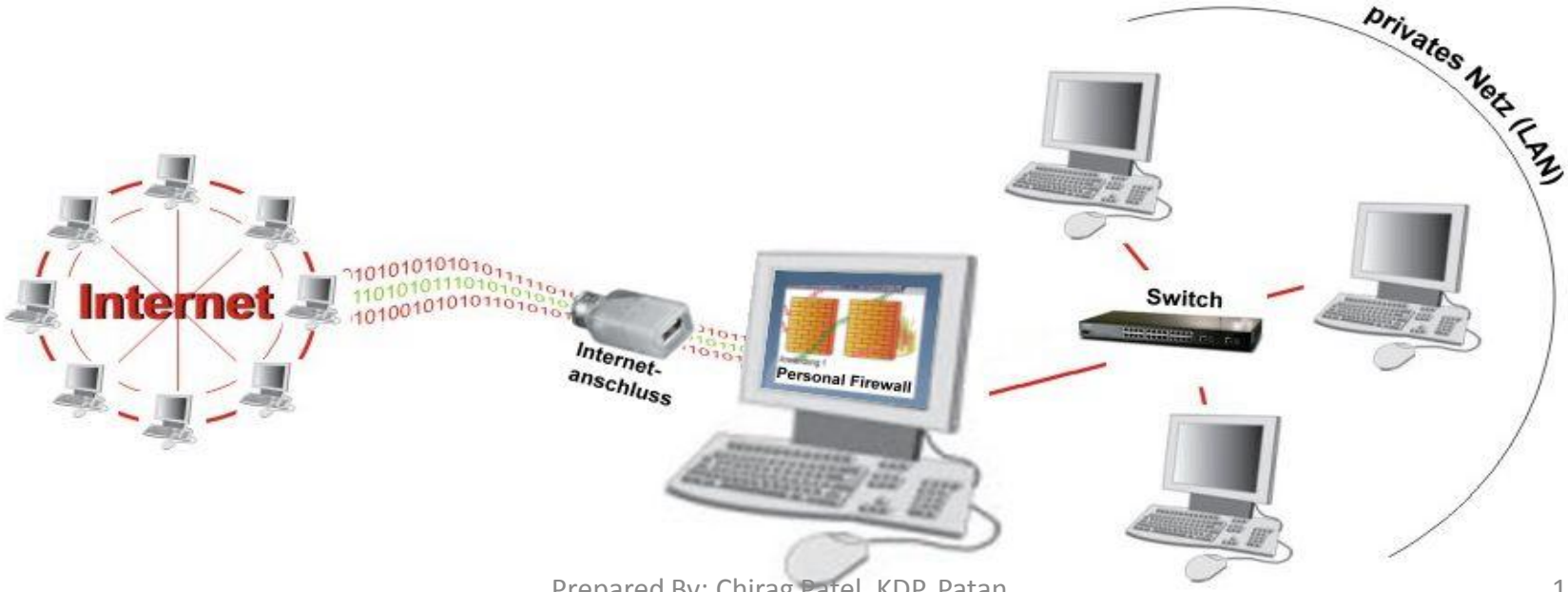


1.3 Application-Level Gateway

- This firewall **not only checks IP addresses, but also decides whether to drop a packet or send them.**
- The major benefit of deploying these firewall is -> they are able to hide the internal network information or structure.
- Even more, it is able to look at more detailed information inside the packets. That enables better monitoring and control of traffic flow.

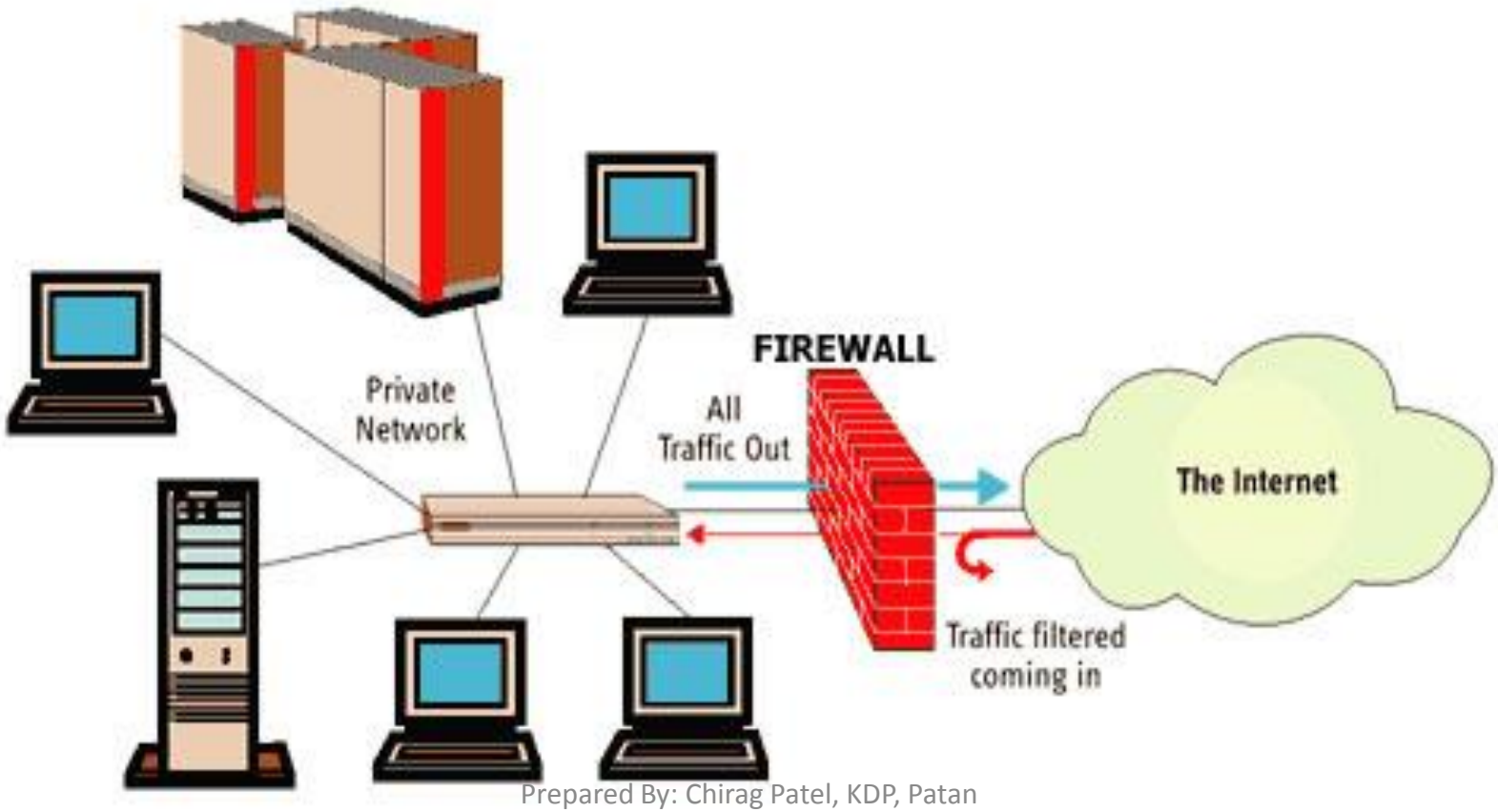
2.1 Personal Firewall

- A **personal firewall** is an application which controls network traffic **to and from a computer**, permitting or denying communications based on a security policy.
- Its primary role is to deny unauthorized remote access to the computer and monitor outgoing activity.
- The figure is shown below;



2.2 Network Firewall

- **A Network firewall is a hardware or software package which controls the flow of packet into and out of network.**
- The figure is shown below;



3 Stateful & Stateless Firewall

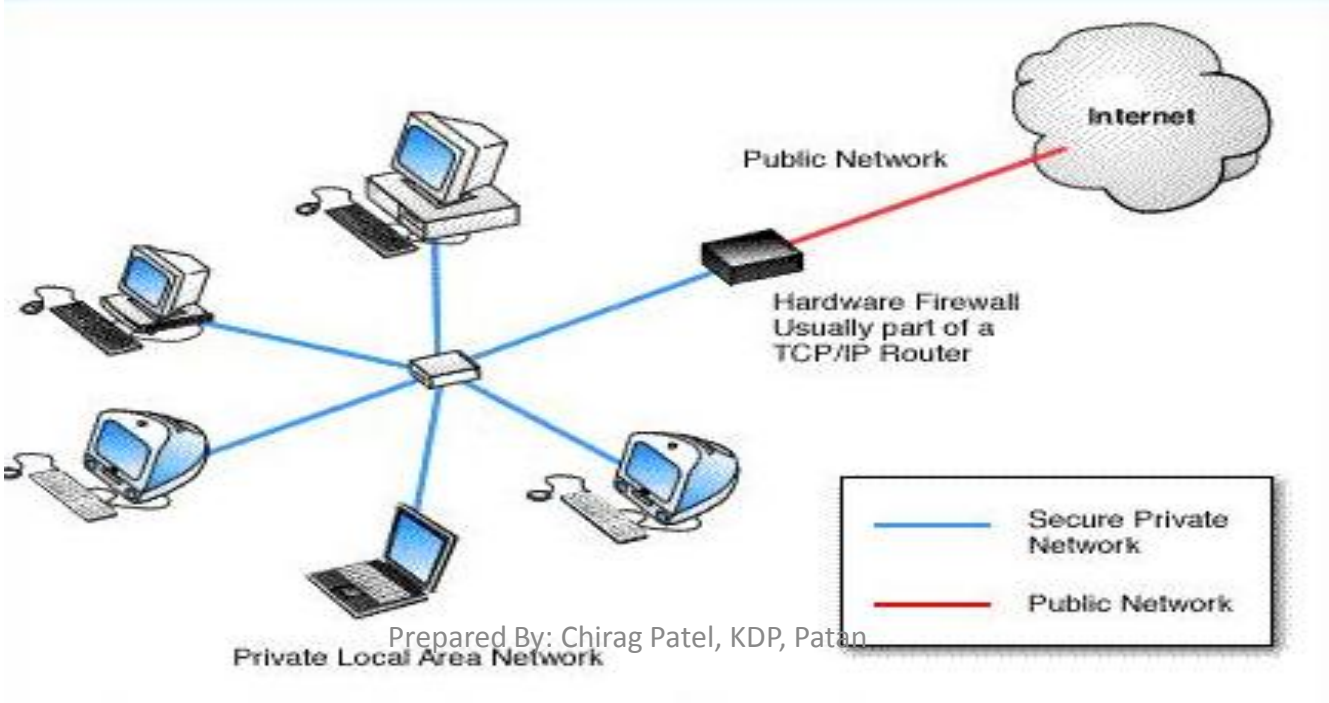
- **Stateless:**
- Stateless firewalls **watch network traffic**, and **restrict or block packets based on source and destination addresses** or other static values.
- They are **not 'aware' of traffic patterns or data flows.**
- Treats each network frame (Packet) individually.
- **Such a firewall has no way of knowing if any given packet is part of an existing connection, is trying to establish a new connection, or is just a dishonest packet.**
- **Stateful**:
- Stateful firewalls **can watch traffic streams from end to end.**

3 Stateful & Stateless Firewall

- They are **aware of communication paths and can implement various IP Security (IPSec) functions** such as tunnels and encryption.
- In technical terms, this means that **stateful firewalls can tell what stage a TCP connection is in** (open, open sent, synchronized, synchronization acknowledge or established).

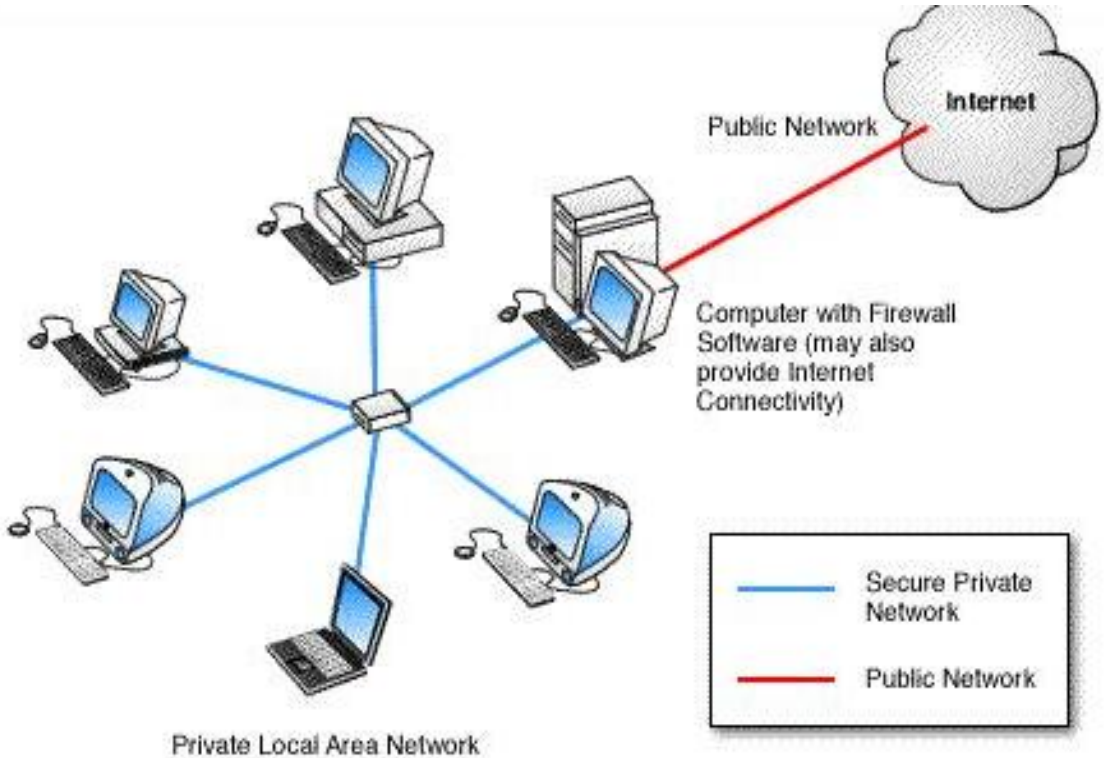
Hardware Firewall

- Hardware firewalls is a stand-alone product generally with Router, Which uses packet filtering to examine the header of a packet to determine its source and destination.
- This information is compared to a set of predefined or user-created rules that determine whether the packet is to be forwarded or dropped.
- Figure is depicted below;



Software Firewall

- Software firewalls are installed on your computer (like any software) which protect your computer from outside attempts to control or gain access your computer, it could also provide protection against the most common Trojan programs or e-mail worms.
- Figure is depicted below;



Security Zones

- **A security zone is a group of interface to which a security policies can be applied.**
- Security policies are **applied to control traffic between different areas**.
- Security Zones, allow you to effectively manage a secure environment by choosing the level of security for different zones of Internet, Organizations.
- **often create security zones by placing firewalls between internal and external networks.**
- Security zones **help organizations to classify, prioritize, and focus on security issues** based on the services that are required in each zone.

1.Intranet

- **The security zone closest to the company is called the intranet.**
- **Intranet is a local communication network, especially a private network which not available to the outside world.**
- This is also known as the **internal network, private network, local area network (LAN), trusted network, protected network, and company or organizational network.**

1.Intranet

- **Generally company and organizations have their own intranet network and members of that company can access that network.**
- The intranet is typically the network (or networks) that contains most of the organization's private resources, including computers, users, data, printers, and other network infrastructure equipment.
- An intranet uses TCP/IP, HTTP and other internet protocols and in general looks like a private version of the internet.

2.Internet (Extranet)

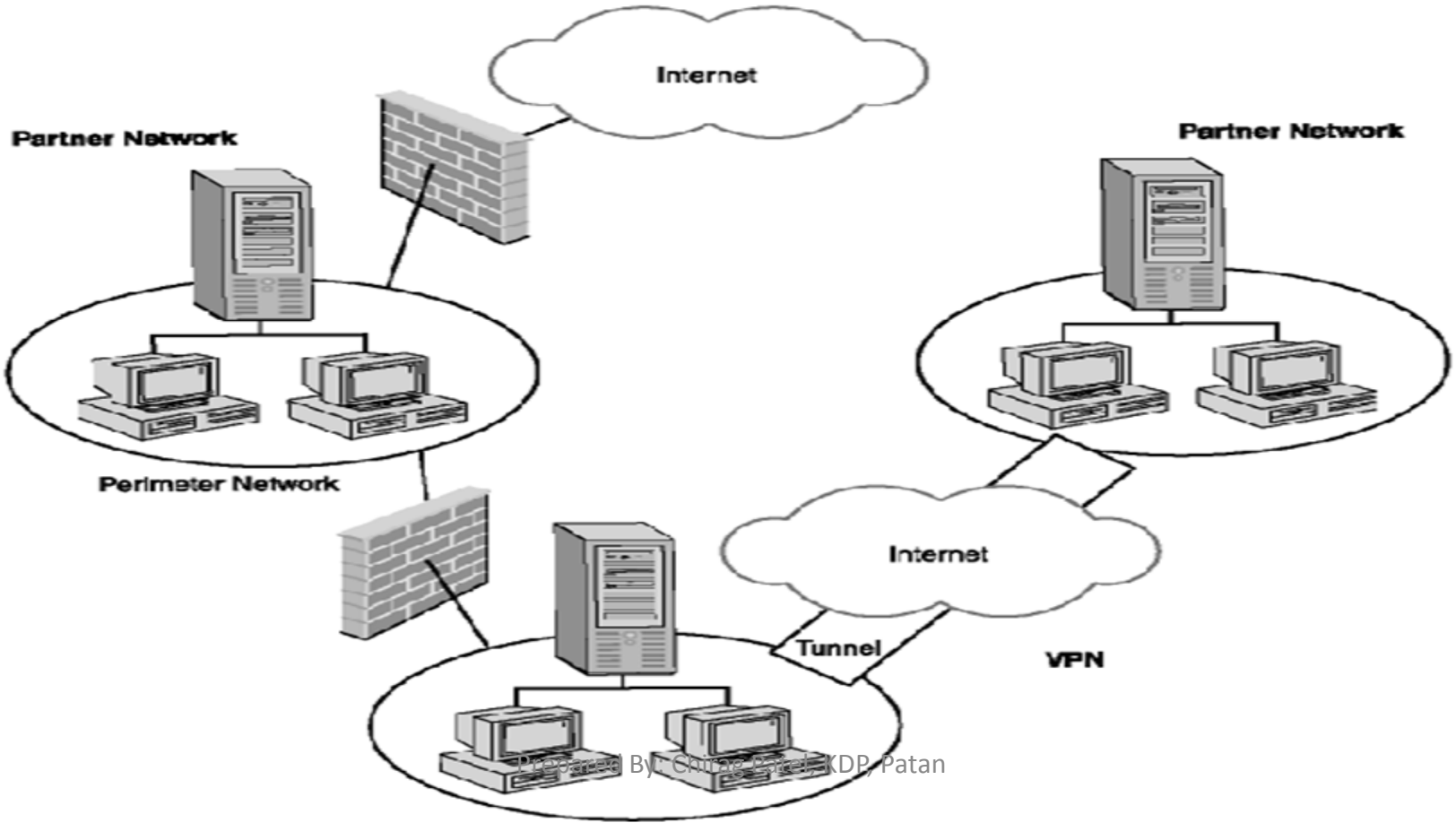
- **INTER connected NETwork -> means of connecting a computer to any other computer or device anywhere in the world via dedicated routers and servers.**
- **Internet is a worldwide / global system of interconnected computer networks.**
- **It uses the standard internet protocol (TCP/IP).**
- **The purpose of an extranet is to share information and technology between members of multiple organizations.**
- Extranets are typically created using VPN connections, which are encrypted connections that can be used on a private or public network.

2.Internet (Extranet)

- **INTERNET DESIGN PRINCIPLES:**
- **Interoperability:** Systems can be assembled using client and server computers and software from different vendors.
- **Layering:** Internet protocol are designed to work in layers.
- **Simplicity:** internet is provided by IP which is very simple, providing only addressing and formatting of packets.
- **It provides uniform naming and addressing.**
- **Internet is designed to deliver packets end to end.**
- **Protocols used for internet are: FTP(File Transfer Protocol), TCP/IP (Transmission Control Protocol and Internet Protocol), SMTP (Simple Mail Transfer Protocol) and telnet.**

- **Main three applications of internet are:**

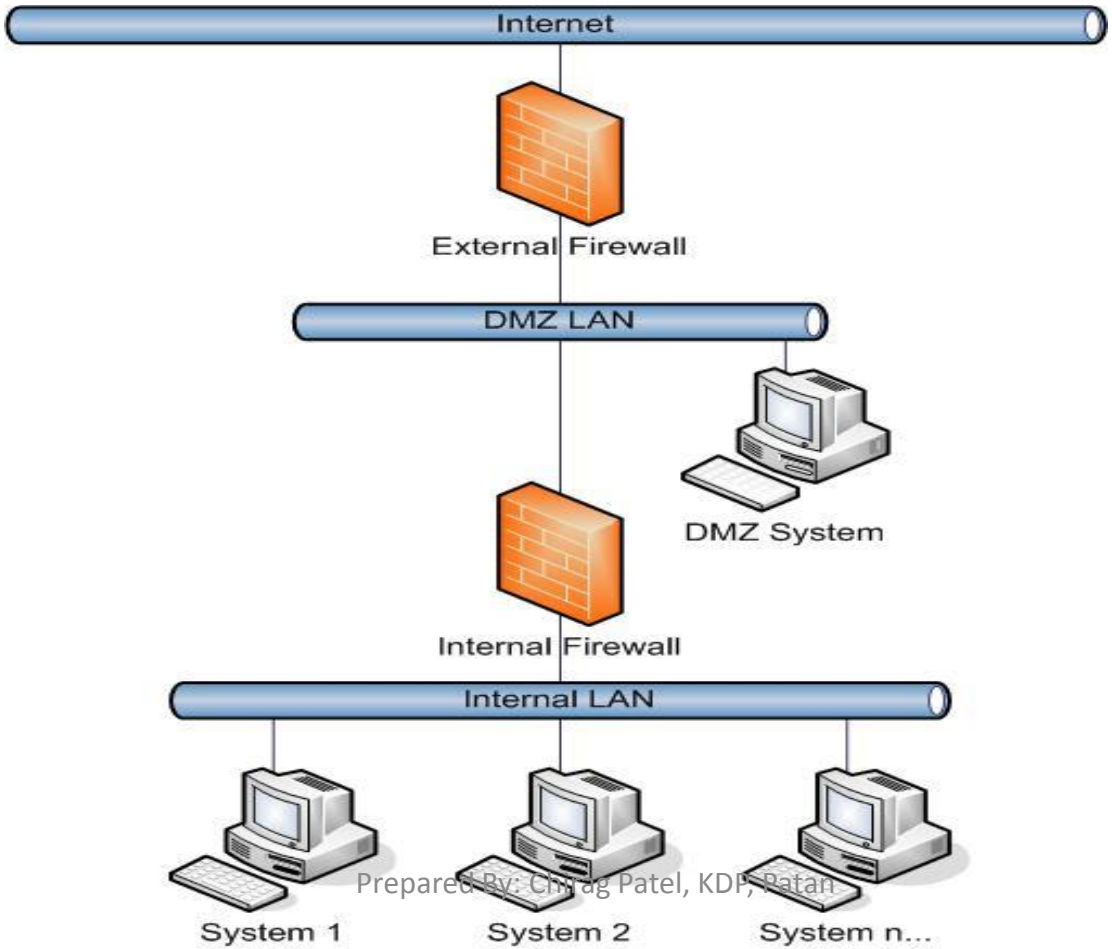
1. **Communication**
2. **Buying or Selling**
3. **Searching information**



3.DMZ

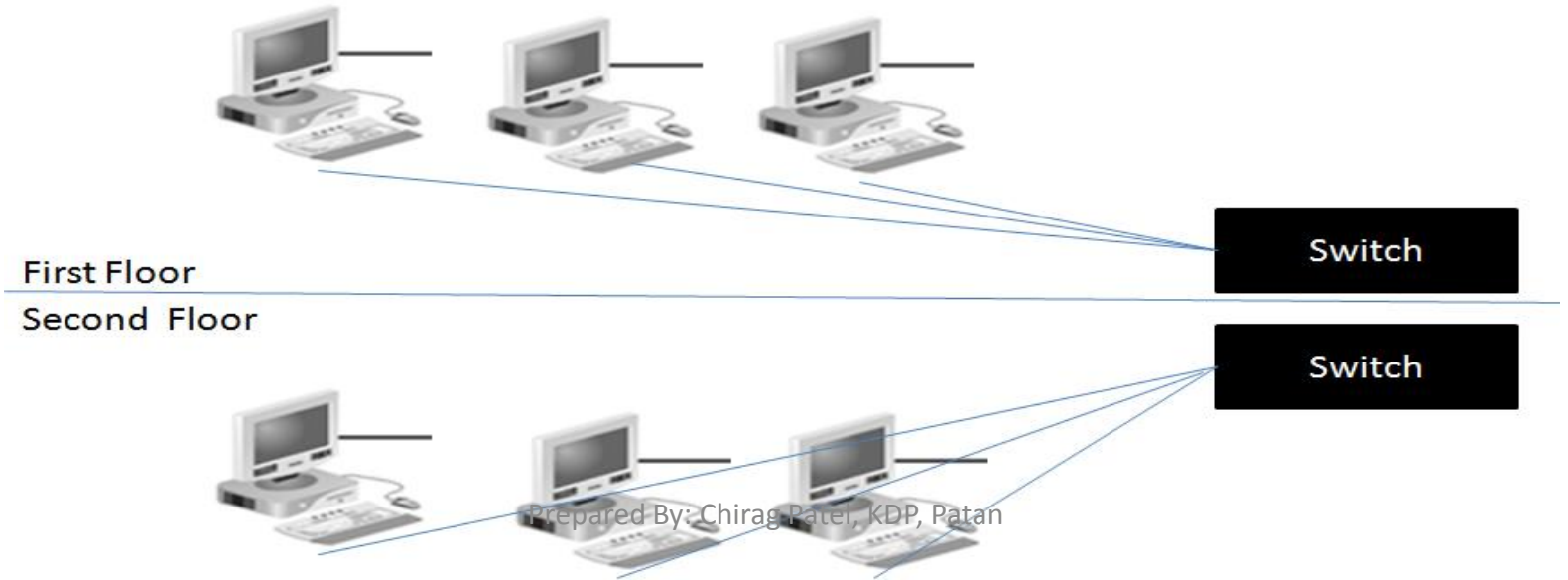
- A **demilitarized zone (DMZ) is a buffer zone between the internet and the intranet**, generally located between an internal and an external firewall.
- **Actually DMZ is a small network or computer host inserted as a "neutral zone"** between company's private network and outside public network.
- **It prevents outside users from getting direct access to a server of a company that has secure data.**
- **DMZ is optional and more secure approach to a firewall and effectively act as a proxy server.**
- **To configure DMZ, A firewall has at least three network interfaces**.
- **One connects to internal private network, second connect to external public network and the third connects to the public server (which form the DMZ network).**
- The users of the public network outside the company can access only to the DMZ host.

- Design Goal of Firewall are,
  1. **Minimize scope of damage**
  2. **Protect sensitive data on the server**
  3. **Minimize effect of on other organizations**
- The basic figure of DMZ are shown below,



4.Virtual LAN (VLAN)

- VLAN stands for **Virtual Local Area Network.**
- It is a **logical implementation of a LAN.**
- **It allows computer connected to different physical networks to act and communicate as if they are on the same physical network.**
- **It is implemented using software and switches, diagram is shown below,**

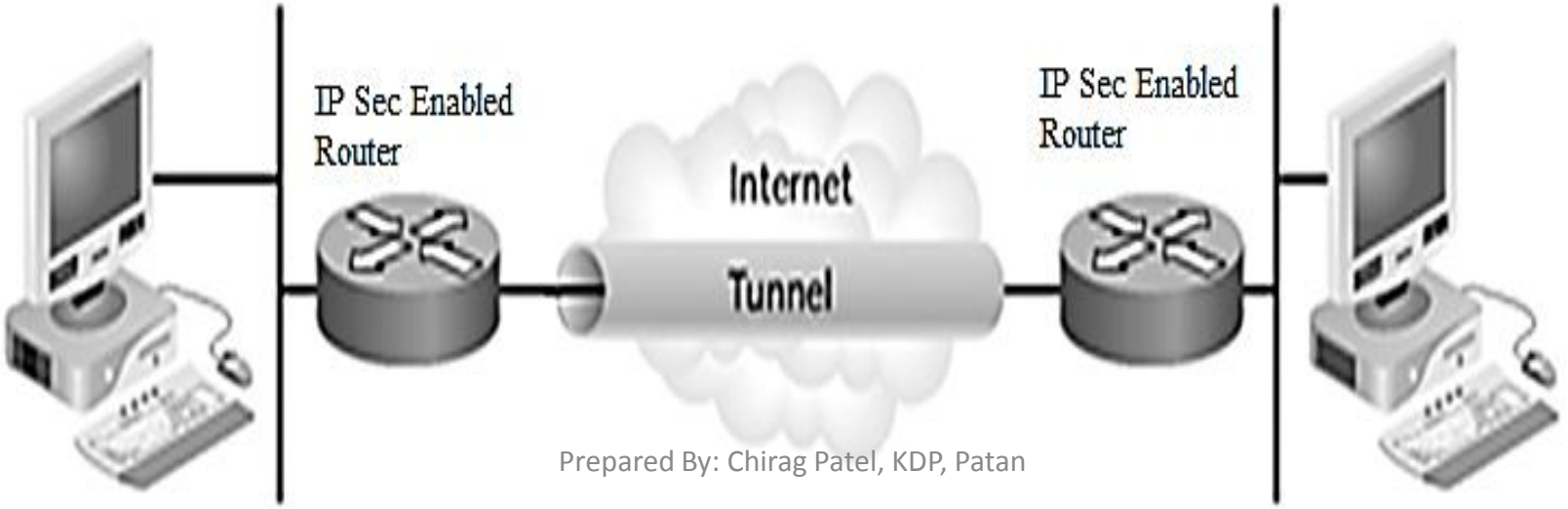


4.Virtual LAN (VLAN)

- It is **logically separated IP sub network.**
- It is implemented using switches and software. It has same characteristics like LAN.
- It **allows multiple IP networks** and **subnets to exist on the same network**.
- It allows **administrator to implement access and security policies to particular group of users.**
- VLAN can be configured like **Static VLAN and Dynamic VLAN.**
- Types of VLAN are, **Port based VLAN, MAC based VLAN, IP based VLAN.**

5.Tunneling

- It also known as **port forwarding.**
- It allows **secure movement of data from one network to another.**
- **It allows private network communication to be sent over a public network, such as internet, using process called encapsulation.**
- It involves **encapsulating packets within packets**, **enabling different protocols to live in a single communication stream.**



5.Tunneling

- The encapsulation process **allows private packets to behave like public packets** and **allow them to pass unnoticed**.
- In tunneling data are broken into packets. They are encapsulated and encrypted. Encrypted packets moves in to tunnel.
- At destination end, encapsulation removed and decryption is done.
- Tunneling supports various protocols like **PPTP(Point To Point Tunneling protocol) and L2TP (Layer Two Tunneling Protocol).**
- **Why Needed?**
  - Assume that a company has a multiple branches and decides to use public internet to connect various branches.
  - Then to make these connections secure from outside unauthorized use, The company use a VPN connection between different branches.

Kerberos

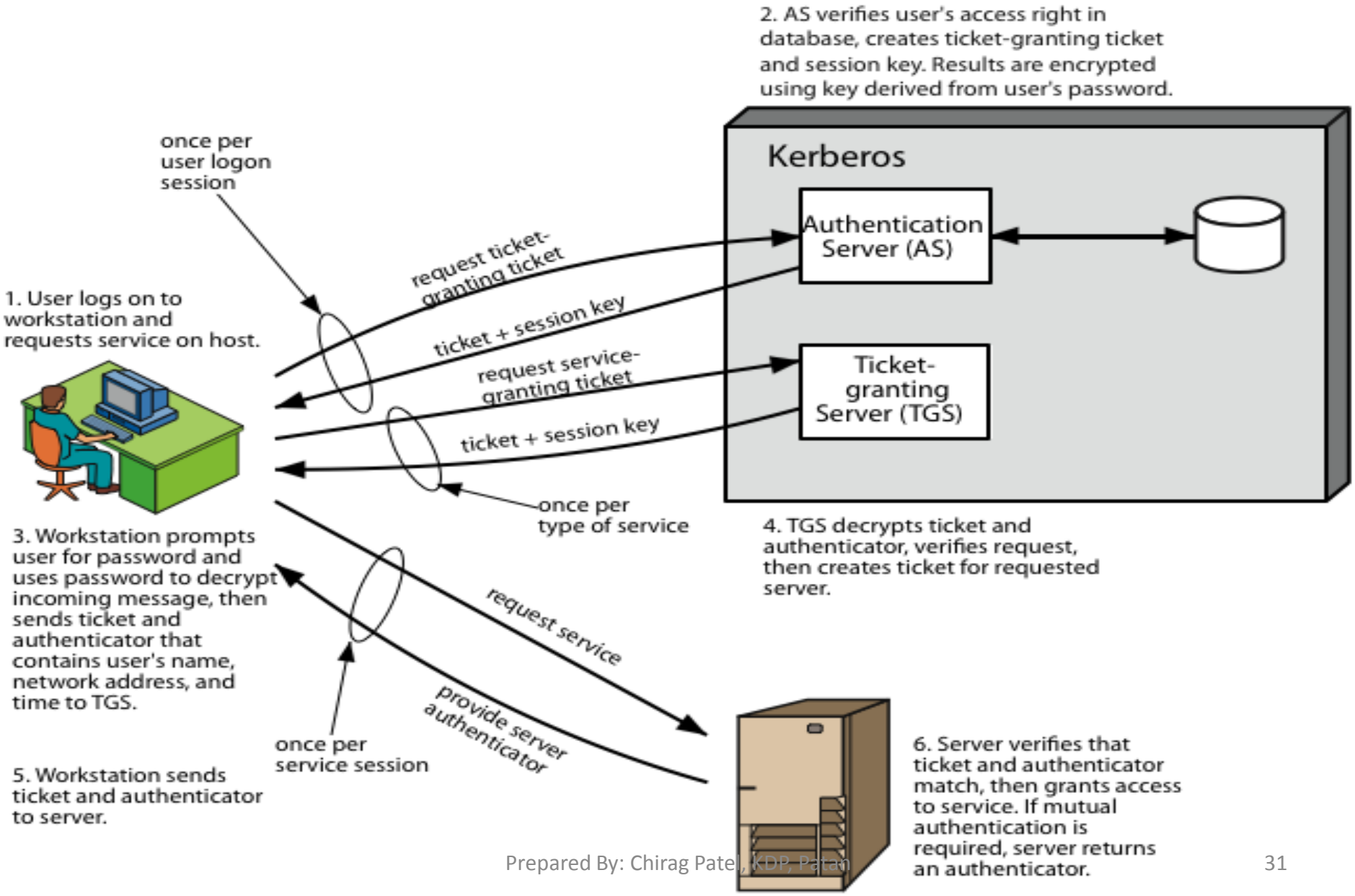
- Kerberos is a **network authentication protocol.**
- It is designed to provide **strong authentication for client/server applications** by using secret-key cryptography.
- Kerberos uses the **Data Encryption Std. (DES)** to implement encryption.
- Characteristic are,
  1. **It is secure:** it never sends a password unless it is encrypted.
  2. **Only a single login is required per session.**
  3. **The concept depends on a trusted third party** – a **Key Distribution Center (KDC).** The KDC is aware of all systems in the network and is trusted by all of them.

Kerberos

4. It performs mutual authentication, where a client proves its identity to a server and a server proves its identity to the client.

- Kerberos introduces the concept of a Ticket-Granting Server (TGS), A client that wishes to use a service has to receive a ticket
- Kerberos also requires an Authentication Server (AS) to verify clients.

Kerberos Authentication



- **Step 1:** The **user logs on to the workstation** and **requests service** on the host.
- The workstation **sends a message to the Authorization Server requesting a ticket granting ticket (TGT).**
- **Step 2:** The **Authorization Server verifies the user's access rights** in the user database and **creates a TGT and session key.**
- The Authorization Sever **encrypts the results using a key derived from the user's password** and sends a message back to the user workstation.
- **The workstation prompts the user for a password and uses the password to decrypt the incoming message.**
- When decryption succeeds, the user will be able to **use the TGT to request a service ticket.**

- **Step 3: The user sends request for the ticket to the TGS.** User proves his identity to the TGS using encrypted message.
- **Step 4:** The TGT decrypt message, **verifies the user request and creates the ticket for client.**
- **The client can access service using single ticket for specific time period without having to be re-authenticated.**
- **Step 5: Now client sends a service request to the server using the ticket given by TGS**.
- The server verifies the client and ticket then grant access to the service.

- **Drawbacks:**
- It is single point failure system as it requires continuous availability of a central server.
- If TGT is stolen, it can be used to access network services.
- It is very bad if authentication server compromised. The server knows all the data of client and server.
- Doesn’t work well in time sharing system.
- **Application of Kerberos:**
- Authentication
- Confidentiality
- Generally used within network.

Trusted System

- **Trusted systems are used to enhance the ability to defend against intruders and malicious programs.**
- **It is protection of data and resources on the basis of level of security.**
- Trusted System is a computer system that can be trusted to a specified level to apply specified security.
- It is **mostly needed in the areas where the data are very crucial and confidential** like military, banking or financial community.
- **Users can be granted to access certain category of data**. It provides high level of security.
- When multiple categories or levels of data are defined, the requirement is referred to as **multilevel security**.

Trusted System

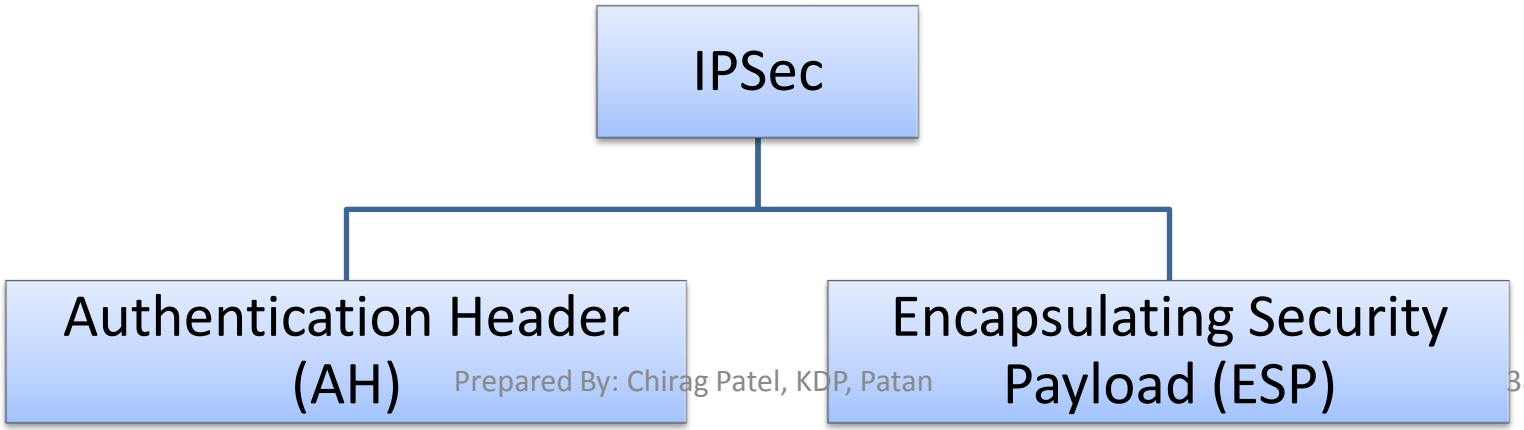
- For implementation that, a multilevel secure system must enforce the following:
  - **No read-up**: A subject can only read an object of less or equal security level.
  - **No write-down**: A subject can write into an object of greater or equal security level.

IPSec

- IPSec provides security at the IP level.
- The IP packets contains data in plain text, so anyone can access the IP packets and forge or modify it.
- So there is a need of security to the IP packet itself. And IPSec provides that solution for that.
- The main idea behind the IPSec is to encrypt and seal the transport and application layer data while transmission.
- IP packet are made by IP header and actual data.
- IPSec features are implemented in the form of additional IP headers also known as extension header.
- IPSec offers two main services: Authentication and confidentiality.

IPSec

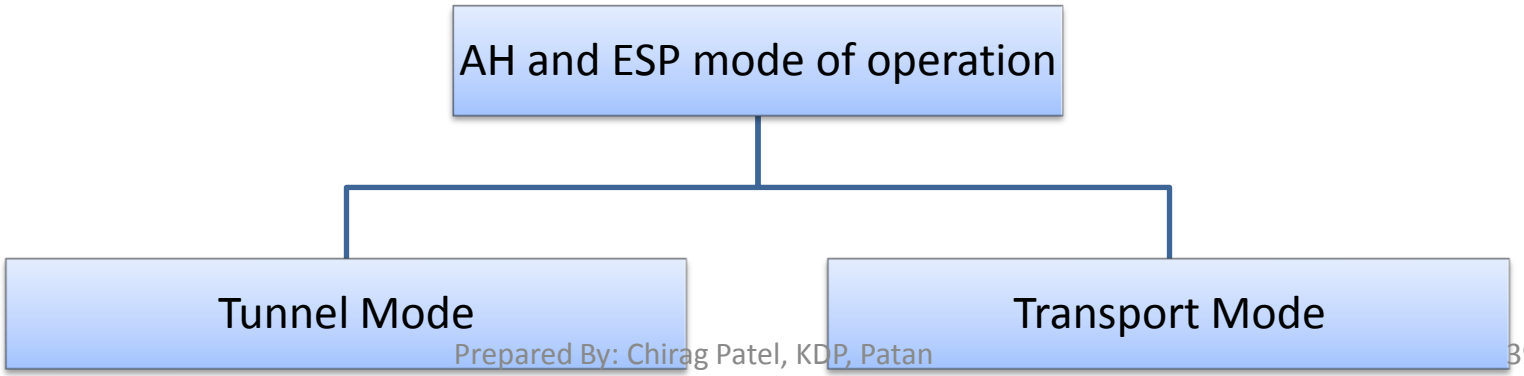
- **Two main protocols are required for these purposes.**
- **The Authentication Header (AH) protocol:** It provides authentication and integrity.
- **The Encapsulating Security Payload (ESP) protocol:** It provides data confidentiality.
- It defines new header with encryption to protect the data.



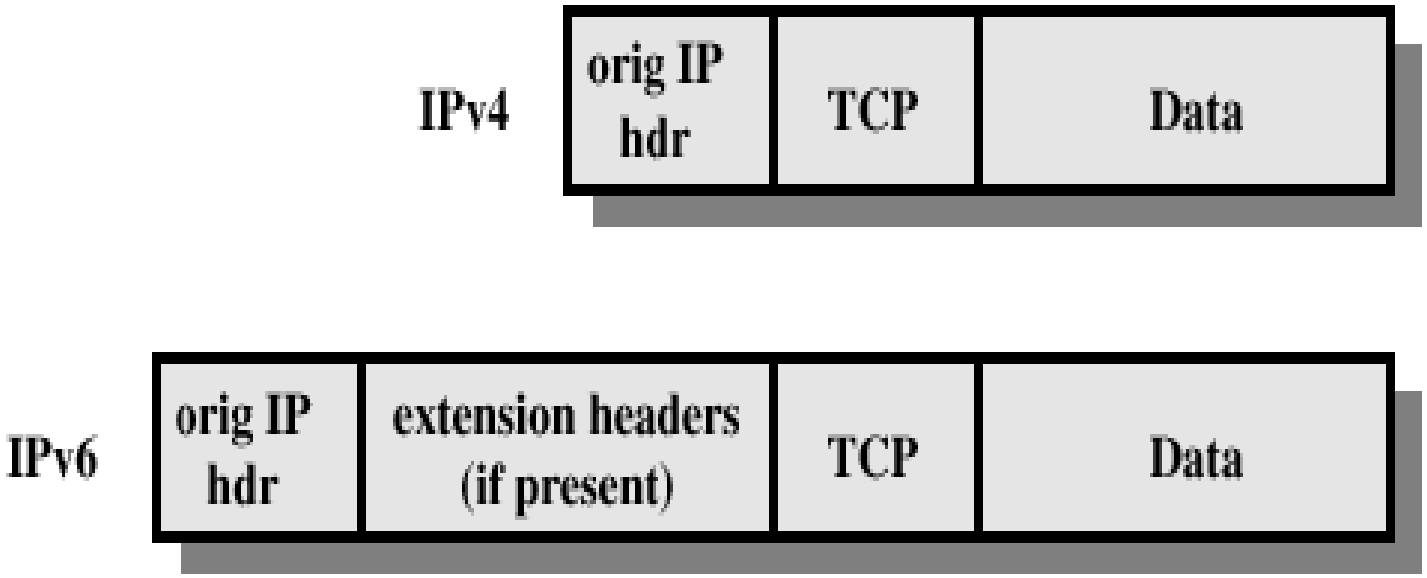
IPSec

- **Both AH and ESP can be used in one of the two modes: Tunnel Mode or Transport Mode.**

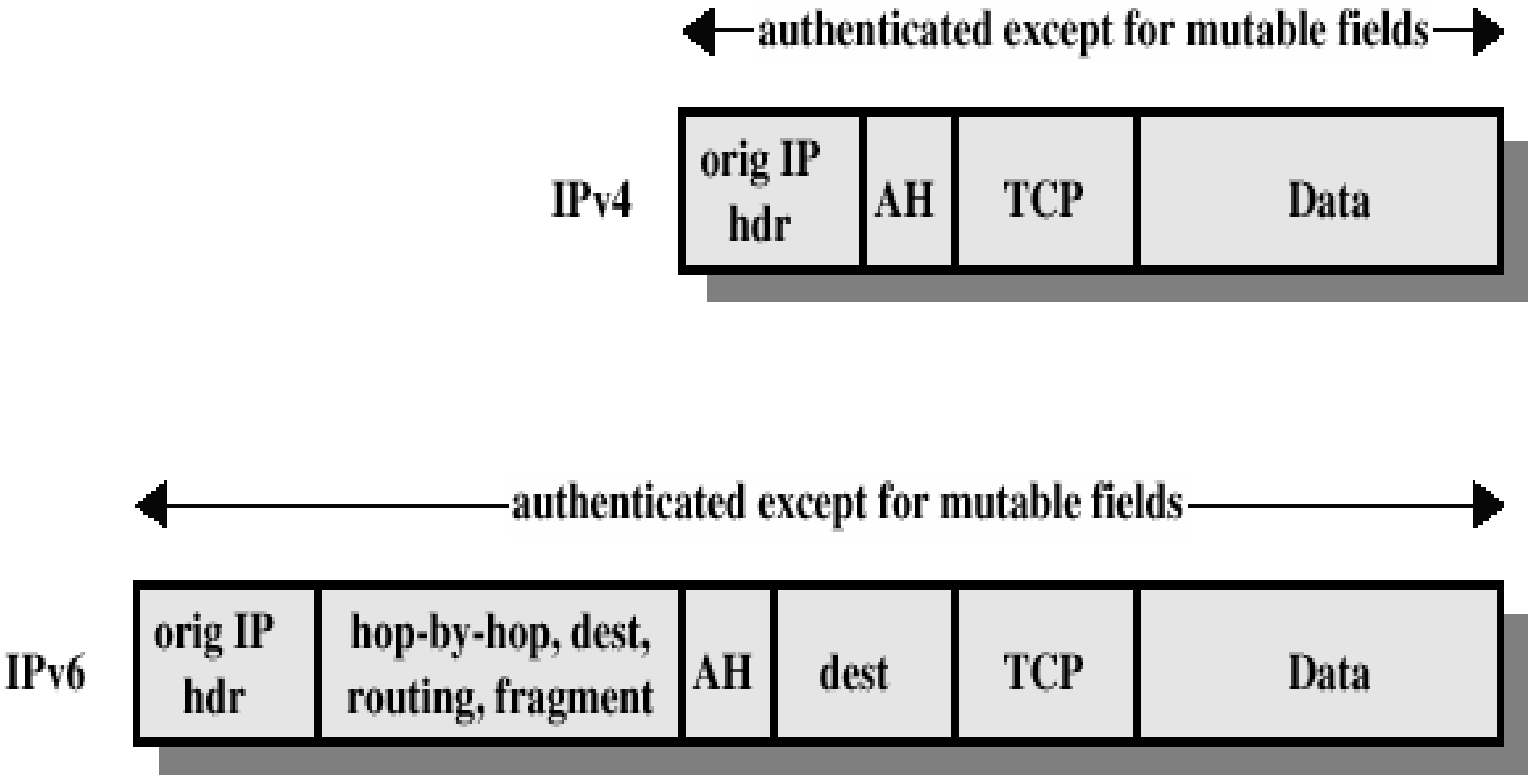
1. **The transport method**
   - It encrypts only data portion of packet.
   - It does not hide the actual source and destination address.
2. **The tunneling method**
   - It provides protection to data portion as well as source and destination IP address.
   - In this encrypted tunnel is established between two hosts.
   - This mode is used to create Virtual Private Network (VPN).



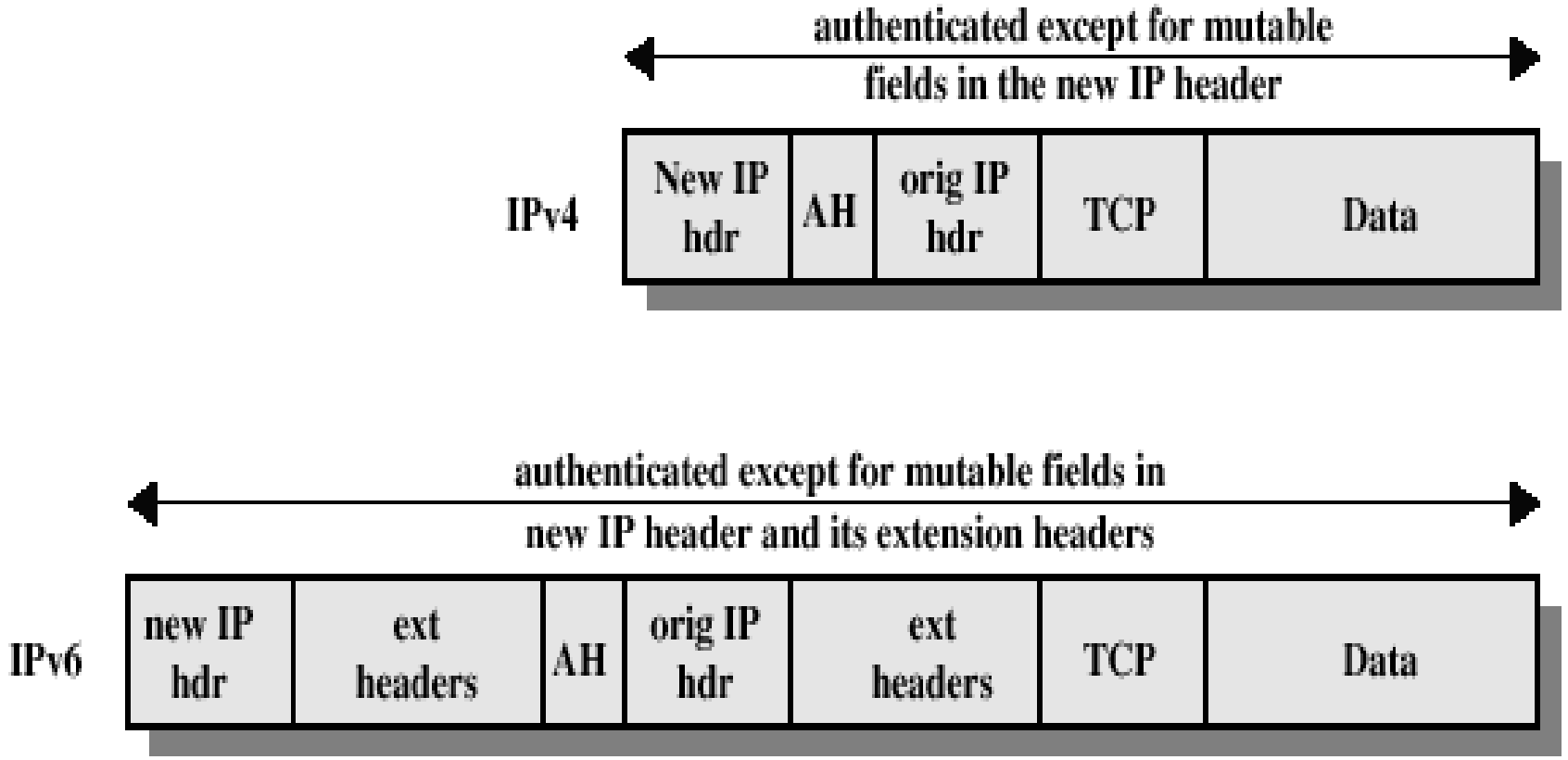
Before applying AH



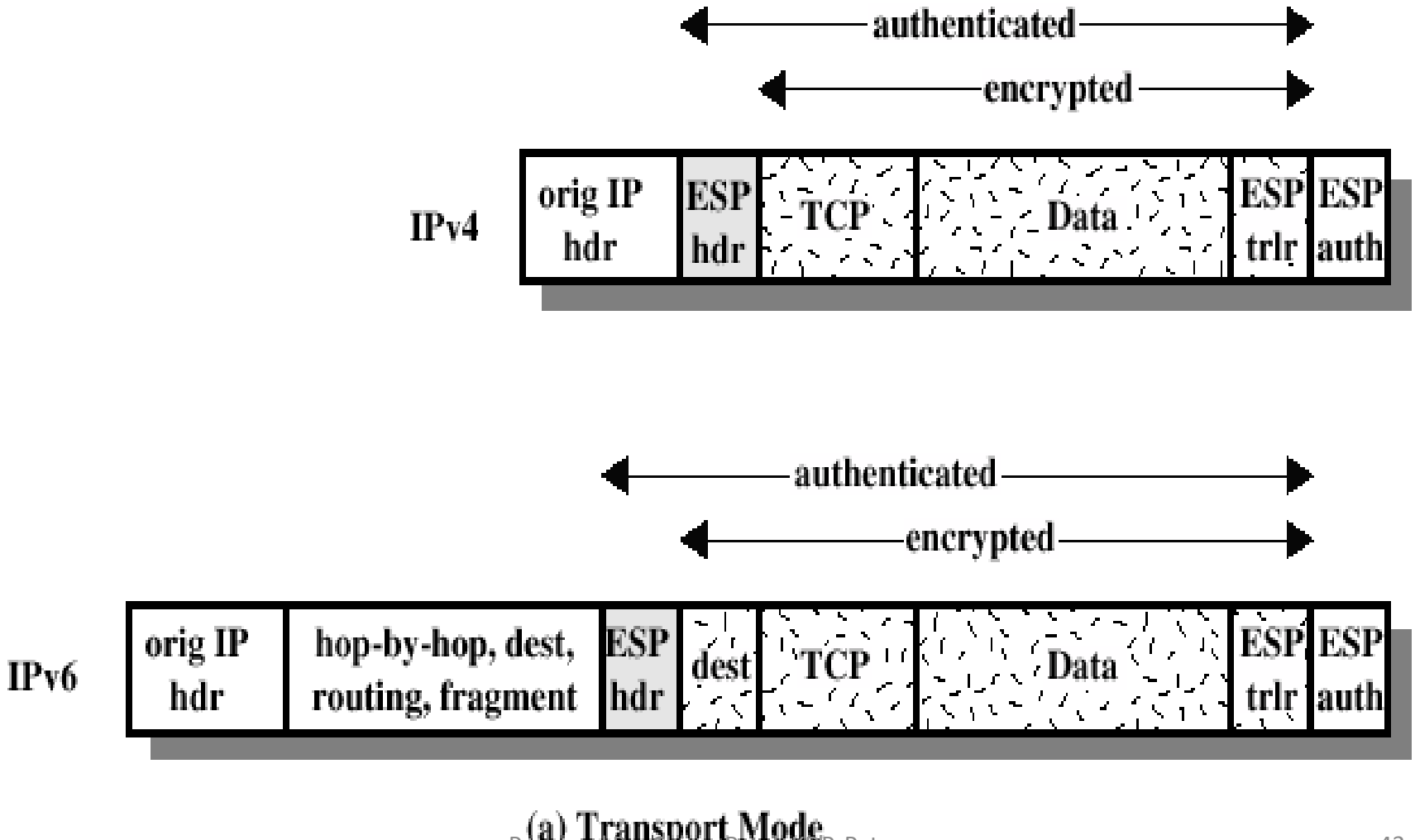
Transport Mode (AH Authentication)



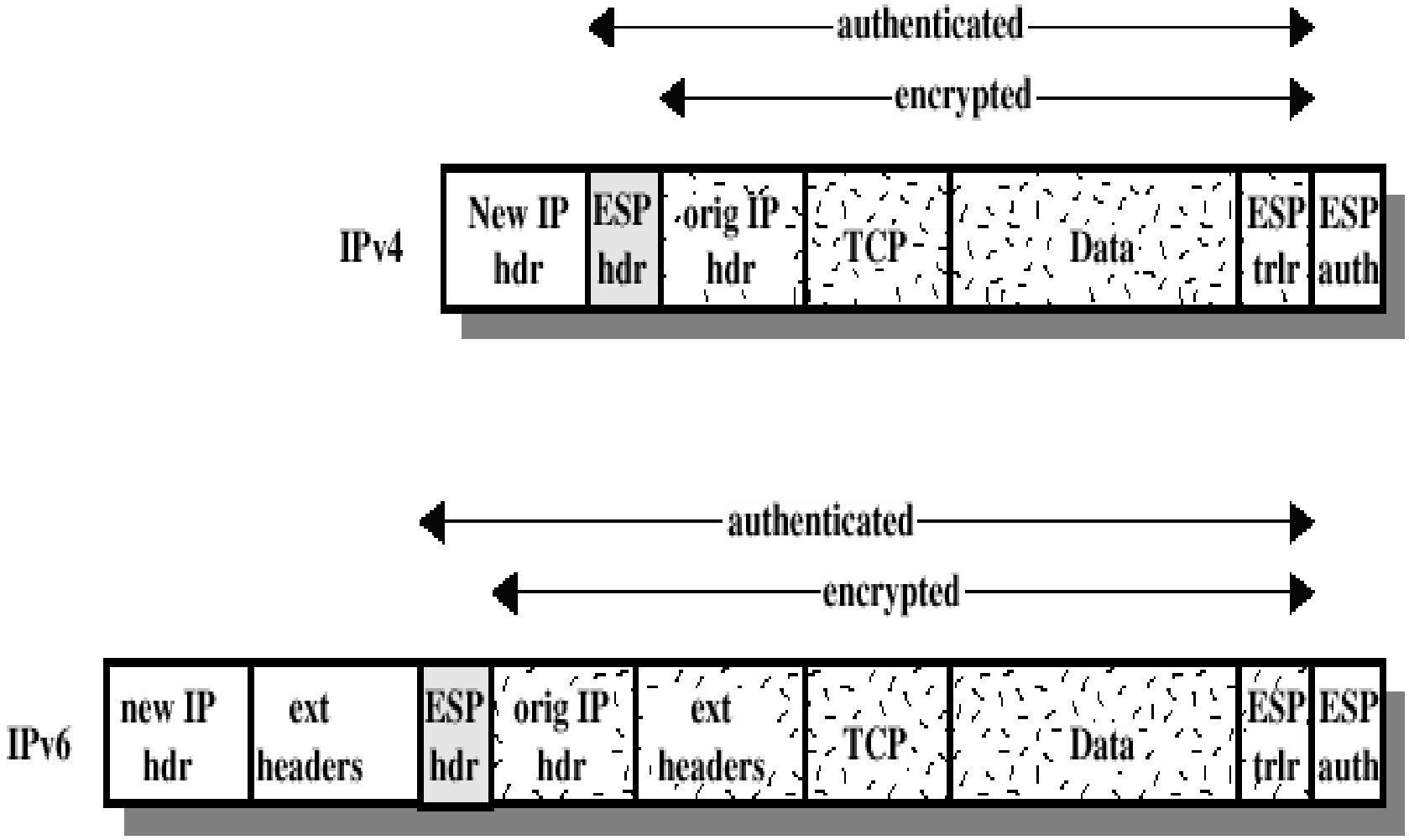
Tunnel Mode (AH Authentication)



ESP Encryption and Authentication



(a) Transport Mode



(b) Tunnel Mode

IPSec Security Services

- **Connectionless integrity**
- **Data origin authentication**
- **Confidentiality (encryption)**
- **Access control**

IPSec Application

- Secure branch office connectivity over the Internet
- Secure remote access over the Internet
- Establishing extranet and intranet connectivity with partners
- Enhancing electronic commerce security
- IPSec enables varied applications to support services like encrypt and/or authenticate all traffic at the IP level.
- All distributed applications, including remote logon, client/server, e-mail, file transfer, Web access, and so on, can be secured.

Email Security

- **The protection of email from unauthorized access & inspection is known as email security.**
- Email is the most widely used application on the internet. Users can send data sound, videos, photos etc. to other user using Email.
- For better email security, encryption software is used to encode message.
- **There are three main email security protocols:**

1. **Privacy Enhanced Mail (PEM)**
2. **Pretty Good Privacy (PGP)**
3. **Secure Multipurpose Internet Mail Extensions (S/MIME)**

1. Privacy Enhanced Email (PEM)

- It is an email security standard adopted by Internet Architecture Board (IAB).
- Basically PEM provides Three Services,
  1. Encryption
  2. Non-repudiation
  3. Message integrity

2.Pretty Good Privacy (PGP)

- The Pretty Good Privacy (PGP) is a general purpose application to protect files or to protect email messages.
- It is simple and easy to use.
- It supports basic cryptographic requirements. It is free software.
- Basically PGP provides Three Services,
  1. Authentication
  2. Confidentiality
  3. Confidentiality & Authentication

3. S/MIME (Secure/Multipurpose Internet Mail Extensions)

- S/MIME is a secure method to sending email and it is based on RSA security.
- Secure/Multipurpose Internet Mail Extension (S/MIME) is a security enhancement to the MIME Internet e-mail format standard.
- S/MIME is very similar to PGP. Both offer the ability to sign and/or encrypt messages, it is used in several mail agents like MS Outlook, Mozilla, MAC Mail etc.

NO.	QUESTIONS	MARKS	YEAR				
1	Define Firewall.	2		2015			
2	List out Type of Firewall.	2		2015			
3	What is necessity of firewall in network?	2				2017	
4	Write a limitation of firewall or Define: Firewall and Write down Limitations of firewall or Define firewall. List out types of firewall. Write its merits and de-merits.	4	2014				
		3			2016		2018
5	List the types of firewall and explain any two. Or List out type of firewall and explain any one.	4	2014		2016		
		3		2015			
6	Write short note on : Kerberos or Explain Kerberos Authentication algorithm.	4		2015	2016	2017	
7	Explain Kerberos authentication. Or Explain Kerberos Authentication.	7	2014				2018
8	List out various security topologies and explain any one in detail.	4					2018

9	Explain DMZ . Or Write note on DMZ. Or Write a short note on DMZ.	4		2015	2016		
	Describe DMZ	3					2018
10	Explain Tunneling. Or Explain Tunneling in detail. Or Discuss tunneling.	4		2015	2016	2017	
11	Write a short note on VLAN.	3			2016		
	Explain VLAN in detail.	4		2015			
12	Differentiate between internet and intranet.	2			2016		
13	Define: Internet, Intranet	2			2016		2018
14	Write Short note on Internet.	3		2015			
15	Why is email security important?	4				2017	
16	Explain Email Security. Or Explain E-Mail Security.	3			2016		2018
	Explain E-Mail Security.	4		2015			
17	Explain IP Security architecture. Or Explain architecture of IP Security. Or Explain the IP security architecture using neat diagram.	4	2014	2015	2016	2017	2018