1. INTRODUCTION

Ethical Hacking Overview - Role of Security and Penetration Testers - Penetration - Testing Methodologies - Laws of the Land - Overview of TCP / IP - The Application Layer - The Transport Layer - The Internet Layer - IP Addressing - Network and Computer Attacks - Malware - Protecting against Malware Attacks - Intruder Attacks - Addressing Physical Security.

ETHICAL HACKING OVERVIEW:

Hacking is the act of finding the possible entry points that exist in a computer system or a computer network and finally entering into them. Hacking is usually done to gain unauthorized access to a computer system or a computer network, either to harm the systems or to steal sensitive information available on the computer.

Hacking is usually legal as long as it is being done to find weaknesses in a computer or network system for testing purpose. This sort of hacking is called **Ethical Hacking**.

A computer expert who does the act of hacking is called a "**Hacker**". Hackers are those who seek knowledge, to understand how systems operate, how they are designed, and then attempt to play with these systems. They are also called as **Black hat hackers**.

Types of Hacking:

Hacking can be segregated into different categories, based on what is being hacked.

- **Website Hacking** - Hacking a website means taking unauthorized control over a web server and its associated software such as databases and other interfaces.
- **Network Hacking** - Hacking a network means gathering information about a network by using tools like Telnet, NS lookup, Ping, Tracert, Netstat, etc. with the intent to harm the network system and hamper its operation.
- **Email Hacking** - It includes getting unauthorized access on an Email account and using it without taking the consent of its owner.
- **Ethical Hacking** - Ethical hacking involves finding weaknesses in a computer or network system for testing purpose and finally getting them fixed.

- **Password Hacking** - This is the process of recovering secret passwords from data that has been stored in or transmitted by a computer system.
- **Computer Hacking** - This is the process of stealing computer ID and password by applying hacking methods and getting unauthorized access to a computer system.

Advantages of Hacking:

Hacking is quite useful in the following scenarios,

- To recover lost information, especially in case you lost your password.
- To perform penetration testing to strengthen computer and network security.
- To put adequate preventative measures in place to prevent security breaches.
- To have a computer system that prevents malicious hackers from gaining access.

Disadvantages of Hacking:

Hacking is quite dangerous if it is done with harmful intent. It can cause

- Massive security breach.
- Unauthorized system access on private information.
- Privacy violation.
- Hampering system operation.
- Denial of service attacks.
- Malicious attack on the system.

Types of hackers:

Hackers can be classified into 3 categories. They are:

1. White Hat Hackers
2. Black Hat Hackers
3. Grey Hat Hackers

1. White Hat Hackers:

White hat hackers are the one who is **authorized or the certified hackers** who work for the government and organizations by performing penetration testing and identifying loopholes in their cybersecurity. They also ensure the protection from the malicious cyber crimes. They work under the rules and regulations provided by the government, that's why they are called **Ethical hackers or Cybersecurity experts.**

2. Black Hat Hackers:

They are often called **Crackers.** Black Hat Hackers can gain the unauthorized access of your system and destroy your vital data. The method of attacking they use common hacking practices they have learned earlier. They are considered to be as criminals and can be easily identified because of their malicious actions.

3. Gray Hat Hackers:

Gray hat hackers fall in the category between white hat and black hat hackers. They can hack any system even if they don't have permission to test the security of the system but they will never steal money or damage the system. Gray hat hacking is sometimes acted legally and sometimes not.

Difference between Hacking and Ethical hacking:

Table 1.1 Disfference between Hacking and Ethical hacking

Hacking	Ethical Hacking
Steal valuable information of company and individual for illegal activity.	Hack system to reduce vulnerabilities of company's system.
Illegal practice and considered a crime.	Legal practice authorized by the company or individual.
They are called as black hat hackers.	They are called as white hat hackers.
They work for themselves for dirty money.	They work with different government agencies and big tech companies.
Try to access the restricted network through illegal practices and reduce the security of data.	They create firewalls and security protocols.

Similarities between Hacking and Ethical hacking:

- Whether it be a white hat hacker, black hat or grey hat hackers, they use the same tools for hacking.
- All the hackers have in-depth and strong knowledge of networks, OS and computer fundamentals.

Introduction to Ethical Hacking:

Ethical hacking is an authorized practice of detecting vulnerabilities in an application, system, or organization's infrastructure and bypassing system security to identify potential data breaches and threats in a network. **Ethical hackers** are employed or contracted by a company to do what illegal hackers do. Ethical Hackers are also called as **security testers** or **penetration testers**. They are also termed as **White hat hackers**.

Companies sometimes hire ethical hackers to conduct penetration tests. In a **penetration test**, an ethical hacker attempts to break into a company's network to find the weakest link in the network or a network system. In a **security test**, testers do more than attempt to break in; they also analyzes a company's security policy and procedures and report any vulnerabilities to management. Security testing, in other words, takes penetration testing to a higher level. Security testing relies on a combination of creativeness, expansion of knowledge bases of best practices, legal issues, and client industry regulations as well as known threats and the breadth of the target organization's security presence (or point of risk).

A **penetration tester**, can simply report their findings to the company. Then it's up to the company to make the final decision on how to use the information they have supplied. However, a **security tester**, might also be required to offer solutions for securing or protecting the network. A security tester's job is to document all vulnerabilities and alert management and IT staff of areas that need special attention.

ROLE OF SECURITY AND PENETRATION TESTERS:

A **hacker** accesses a computer system or network without the authorization of the system's owner. By doing so, a hacker is breaking the law and can go to prison. Those who break into systems to steal or destroy data are often referred to as **crackers**; hackers might simply want to prove how vulnerable a system is by accessing the computer or network without destroying any data.

An **ethical hacker** is a person who performs most of the same activities a hacker does but with the owner or company's permission. Ethical hackers are usually contracted to perform penetration tests or security tests. Companies realize that intruders might attempt to access their network resources, and are willing to pay for someone to discover these vulnerabilities first. Companies would rather pay a "good hacker" to discover problems in their current network configuration than have a "bad hacker" discover these vulnerabilities. Bad hackers spend many hours scanning systems over the Internet, looking for openings or vulnerable systems.

Some hackers are skillful computer experts, but others are younger, inexperienced people who experienced hackers refer to as **script kiddies** or **packet monkeys**. These derogatory terms refer to people who copy code from knowledgeable programmers instead of creating the code themselves. Many experienced penetration testers can write computer programs or scripts in Perl (Practical Extraction and Report Language) or the C language to carry out network attacks. (A script is a set of instructions that run in sequence to perform tasks on a computer system.)

A penetration tester might include the following requirements:

- Perform vulnerability, attack, and penetration assessments in Internet, intranet, and wireless environments.
- Perform discovery and scanning for open ports and services.
- Apply appropriate exploits to gain access and expand access as necessary.
- Participate in activities involving application penetration testing and application source code review.
- Interact with the client as required throughout the engagement.
- Produce reports documenting discoveries during the engagement.
- Debrief with the client at the conclusion of each engagement.
- Participate in research and provide recommendations for continuous improvement.
- Participate in knowledge sharing.

Penetration testers and security testers usually have a laptop computer configured with multiple OSs and hacking tools. This collection of tools for conducting vulnerability assessments and attacks is sometimes referred to as a “**tiger box**”.

PENETRATION TESTING METHODOLOGIES:

Penetration testing can be defined as a legal and authorized attempt to locate and successfully exploit computer systems for the purpose of making those systems more secure. It is also termed as **Pen testing**. The process includes probing for vulnerabilities as well as providing proof of concept attacks to demonstrate the vulnerabilities are real. Proper penetration testing always ends with specific recommendations for addressing and fixing the issues that were discovered during the test. On the whole, this process is used to help secure computers and networks against future attacks. The general idea is to find security issues by using the same tools and techniques as an attacker. These findings can then be mitigated before a real hacker exploits them.

Ethical hackers who perform penetration tests use one of these models:

- White box model
- Black box model
- Gray box model

In the **white box model**, the tester is told what network topology and technology the company is using and is given permission to interview IT personnel and company employees. For example, the company might print a network diagram showing all the company's routers, switches, firewalls, and intrusion detection systems (IDSs) or give the tester a floor plan detailing the location of computer systems and the OSs running on these systems. This background information makes the penetration tester's job a little easier than it is with the black box model.

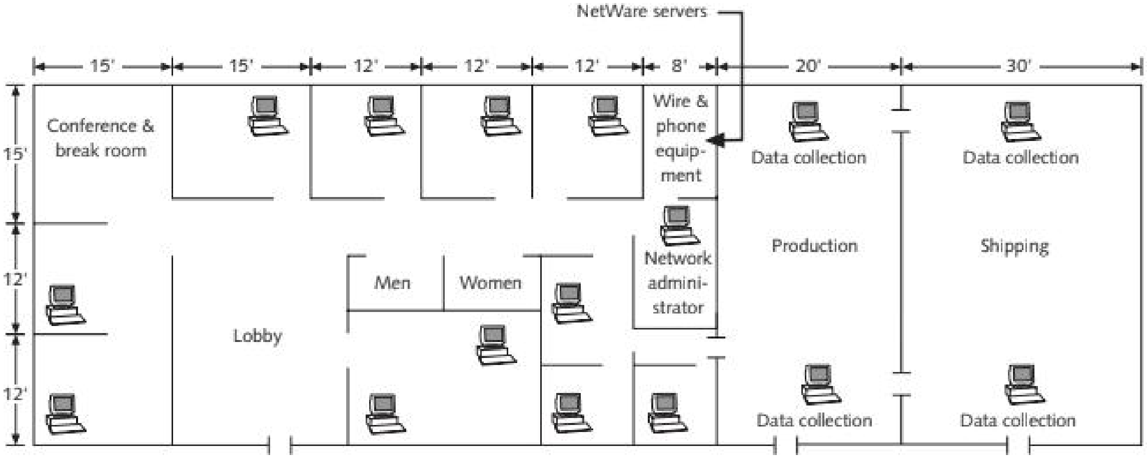

Fig 1.1 A sample floor plan

In the **black box model**, management doesn't divulge to staff that penetration testing is being conducted, nor does it give the tester any diagrams or describe what technologies the company is using. This model puts the burden on the tester to find this information by using certain techniques. This model also helps management see whether the company's security personnel can detect an attack.

The **gray box model** is a hybrid of the white and black box models. In this model, the company gives the tester only partial information. For example, the tester might get information about which OSs are used but not get any network diagrams.

The penetration test team is called a **red team** in the industry, which is composed of people with varied skills who perform the tests. For example, a red team might include a programming expert who can perform SQL injections or other programming vulnerability testing. The team might also include a network expert who's familiar with port vulnerabilities and IDS, router, or firewall vulnerabilities. It's unlikely that one person will perform all tests.

A **Certified Ethical Hacker (CEH)** must have a general knowledge about the following domains:

- Ethics and legal issues
- Foot-printing
- Scanning
- Enumeration
- System hacking
- Trojans and backdoors
- Sniffers
- Denial of service
- Social engineering
- Session hijacking
- Hacking Web servers
- Web application vulnerabilities
- Web-based password-cracking techniques
- Structured Query Language (SQL) injection
- Hacking wireless networks
- Viruses and worms
- Physical security
- Hacking Linux
- Intrusion detection systems (IDSs), firewalls, and honeypots
- Buffer overflows
- Cryptography
- Penetration testing methodologies

Phases of Penetration testing:

Penetration testing consists of 5 phases. They are:

- Reconnaissance
- Scanning
- Vulnerability Assessment
- Exploitation
- Reporting

1. Reconnaissance (Information Gathering):

In this phase, the tester gathers as much information about the target system as they can, including information about the network topology, operating systems and applications, user accounts, and other relevant information. The goal is to gather as much data as possible so that the tester can plan an effective attack strategy. Reconnaissance can be categorized into two, depending on what methods are used to gather information.

- Active reconnaissance - Gathers information by directly interacting with the target system.
- Passive reconnaissance - Gathers information from resources that are already publicly available.

2. Scanning:

The tester uses various tools to **identify open ports and check network traffic** on the target system. Because open ports are potential entry points for attackers, penetration testers need to identify as many open ports as possible for the next penetration testing phase.

3. Vulnerability Assessment:

The tester uses all the data gathered in the reconnaissance and scanning phases to identify **potential vulnerabilities** and determine whether they can be exploited. Much like scanning, vulnerability assessment is a useful tool on its own but is more powerful when combined with the other penetration testing phases.

4. Exploitation:

In this penetration testing phase, the penetration tester attempts to access the target system and exploit the identified vulnerabilities, typically by using a tool like Metasploit to simulate real-world attacks. This is perhaps the most delicate penetration testing phase because accessing the target system requires bypassing security restrictions.

5. Reporting:

Once the exploitation phase is complete, the tester prepares a report documenting the penetration test's findings. The report generated in this final penetration testing phase can be used to fix any vulnerabilities found in the system and improve the organization's security posture. The report serves as a roadmap to guide the organization towards a more secure organization infrastructure.

LAWS OF THE LAND:

As a security tester, one must be aware of what they're allowed to do and what they should not or cannot do. For example, some security testers know how to pick a deadbolt lock, so a locked door wouldn't deter them from getting physical access to a server. However, testers must be knowledgeable about the laws for possessing lock-picks before venturing out to a corporate site with tools in hand. In fact, laws vary from state to state and country to country. In some states, the mere possession of lock-picking tools constitutes a crime, whereas other states allow possession as long as a crime hasn't been committed. In one state, they might be charged with a misdemeanor for possessing these tools; in another state, they might be charged with a felony.

As with lock-picking tools, having some hacking tools on a computer might be illegal. One should contact local law enforcement agencies and ask about the laws for their state or country before installing hacking tools on your computer.

Laws are written to protect society. Laws for having hacking tools that allow one to view a company's network infrastructure aren't as clearly defined as laws for possession of lock-picking tools because laws haven't been able to keep up with the speed of technological advances. In some states, running a program that gives an attacker an overview and a detailed description of a company's network infrastructure isn't seen as a threat. Some hackers use software to crack passwords of logon accounts. This act, performed by many security professionals when given permission to do so by a network's owner, is a federal offense when done without permission and can add substantial prison time to a hacker's sentence.

Table 1.2 An overview of recent hacking cases

State and Year	Description
California, 2008	Jon Paul Oson, a former IT network engineer and technical services manager for San Diego's Council of Community Health Clinics, was sentenced to 63 months in prison on federal hacking charges. He was convicted of intentionally damaging protected computers by disabling the backup database of patient information and deleting data and software on several servers.
California, 2009	Mario Azar, 28, an IT consultant for Pacific Energy Resources (PER), was indicted on federal charges of damaging the company's computer systems after it declined to offer him permanent employment. He was charged with unauthorized impairment of a protected computer, which carries a maximum penalty of 10 years in federal prison. Azar accessed PER computer systems illegally and caused thousands of dollars of damage to data.
Pennsylvania, 2009	University of Pennsylvania student Ryan Goldstein, 22, was sentenced to 3 months in prison and 5 years of probation for a hacking scheme that crashed an engineering school server. He helped a New Zealand hacker launch a 50,000 computer attack against online chat networks by using a botnet. With this attack, Goldstein was able to access the university's server illegally, which was used by more than 4000 students, faculty, and staff.

Table 1.3 Federal computer crime laws

Federal law	Description
The Computer Fraud and Abuse Act. Title 18, Crimes and Criminal Procedure. Part I: Crimes, Chapter 47, Fraud and False Statements, Sec. 1030: Fraud and related activity in connection with computers	This law makes it a federal crime to access classified information or financial information without authorization.
Electronic Communication Privacy Act. Title 18, Crimes and Criminal Procedure. Part I: Crimes, Chapter 119, Wire and	These laws make it illegal to intercept any communication, regardless of how it

Electronic Communications Interception and Interception of Oral Communications, Sec. 2510: Definitions and Sec. 2511: Interception and disclosure of wire, oral, or electronic communications prohibited	was transmitted.
Homeland Security Act of 2002, H.R. 5710, Sec. 225: Cyber Security Enhancement Act of 2002	This amendment to the Homeland Security Act of 2002 specifies sentencing guidelines for certain types of computer crimes.
The Computer Fraud and Abuse Act. Title 18, Crimes and Criminal Procedure, Sec. 1029: Fraud and related activity in connection with access devices	This law makes it a federal offense to manufacture, program, use, or possess any device or software that can be used for unauthorized use of telecommunications services.

As a security tester, you must be careful that your actions don't prevent the client's employees from doing their jobs. If you run a program that uses network resources to the extent that a user is denied access to them, you have violated federal law. For example, denial-of-service (DoS) attacks, should not be initiated on your client's networks.

Skills of a Security tester:

- **Knowledge of network and computer technology** - As a security tester, one must have a good understanding of networking concepts. They should spend time learning and reviewing TCP/IP and routing concepts and be able to read network diagrams. Being a security tester is impossible without a high level of expertise in this area. They should also have a good understanding of computer technologies and OSs.
- **Ability to communicate with management and IT personnel** - Security testers need to be good listeners and must be able to communicate verbally and in writing with members of management and IT personnel. Explaining the findings to CEOs might be difficult, especially if they don't have a technical background. Their reports should be clear and succinct and offer constructive feedback and recommendations.
- **An understanding of the laws that apply to their location** - As a security tester, one must be aware of what they can and can't do legally. Gathering this information can be difficult when working with global companies, as laws can vary widely in other countries.

- **Ability to apply the necessary tools to perform their tasks** - Security testers must have a good understanding of tools for conducting security tests. More important, they must be able to think outside the box by discovering, creating, or modifying tools when current tools don't meet their needs.

OVERVIEW OF TCP / IP:

TCP/IP stands for Transmission Control Protocol/Internet Protocol and is a suite of communication protocols used to interconnect network devices on the internet. TCP/IP is also used as a communications protocol in a private computer. The entire IP suite is a set of rules and procedures which is commonly referred to as TCP/IP. TCP and IP are the two main protocols, though others are included in the suite. The TCP/IP protocol suite functions as an abstraction layer between internet applications and the routing and switching fabric.

TCP/IP specifies how data is exchanged over the internet by providing end-to-end communications that identify how it should be broken into packets, addressed, transmitted, routed and received at the destination. TCP/IP requires little central management and is designed to make networks reliable with the ability to recover automatically from the failure of any device on the network.

The two main protocols in the IP suite serve specific functions. TCP defines how applications can create channels of communication across a network. It also manages how a message is assembled into smaller packets before they are then transmitted over the internet and reassembled in the right order at the destination address. IP defines how to address and route each packet to make sure it reaches the right destination. Each gateway computer on the network checks this IP address to determine where to forward the message.

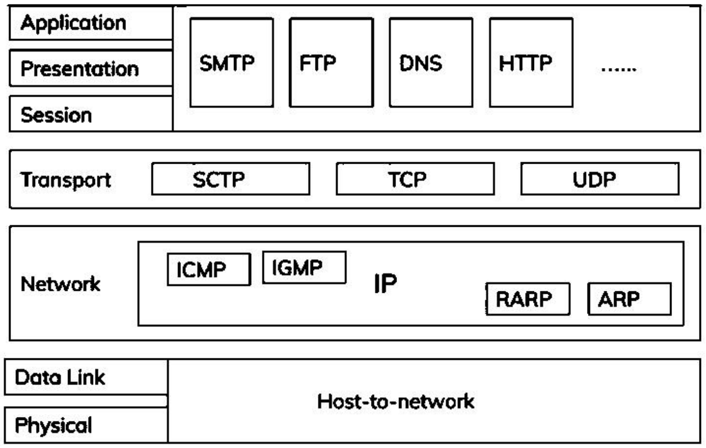

Fig 1.2 Overview of TCP / IP model

Common TCP/IP protocols include the following:

- **Hypertext Transfer Protocol (HTTP)** handles the communication between a web server and a web browser.
- **HTTP Secure** handles secure communication between a web server and a web browser.
- **File Transfer Protocol** handles transmission of files between computers.

TCP/IP uses the client-server model of communication in which a user or machine (a client) is provided a service, like sending a webpage, by another computer (a server) in the network. It is compatible with all operating systems (OSs), so it can communicate with any other system. The IP suite is also compatible with all types of computer hardware and networks. It is highly scalable and, as a routable protocol, can determine the most efficient path through the network.

TCP / IP model:

TCP/IP functionality is divided into four layers, each of which includes specific protocols:

1. The **application layer** provides applications with standardized data exchange. Its protocols include HTTP, FTP, Simple Mail Transfer Protocol (SMTP) and Simple Network Management Protocol (SNMP). At the application layer, the **payload** is the actual application data.

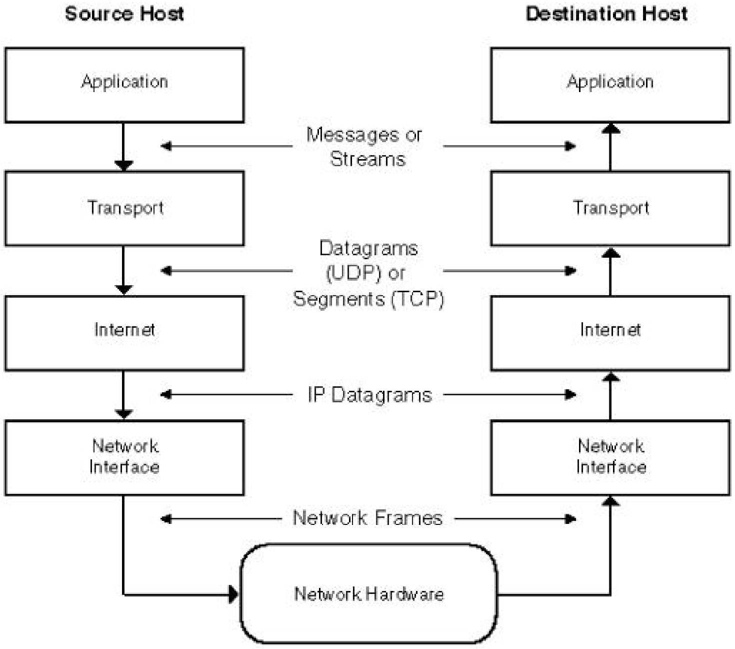

Fig 1.3 TCP / IP model

2. The **transport layer** is responsible for maintaining end-to-end communications across the network. TCP handles communications between hosts and provides flow control, multiplexing and reliability. The transport protocols include TCP and User Datagram Protocol (UDP), which is sometimes used instead of TCP for special purposes.

3. The **network layer**, also called the **internet layer**, deals with packets and connects independent networks to transport the packets across network boundaries. The network layer protocols are IP and Internet Control Message Protocol (ICMP), which is used for error reporting.

4. The **physical layer**, also known as the **network interface layer** or **data link layer**, consists of protocols that operate only on a link which is the network component that interconnects nodes or hosts in the network. The protocols in this lowest layer include Ethernet for local area networks and Address Resolution Protocol (ARP).

Pros of TCP / IP:

The advantages of using the TCP/IP model include the following:

- helps establish a connection between different types of computers
- works independently of the OS
- supports many routing protocols
- uses client-server architecture that is highly scalable

Cons of TCP / IP:

The disadvantages of TCP/IP include the following:

- is complicated to set up and manage
- transport layer does not guarantee delivery of packets
- is not easy to replace protocols in TCP/IP

THE APPLICATION LAYER:

The application layer is the highest abstraction layer of the TCP/IP model that provides the interfaces and protocols needed by the users. It combines the functionalities of the session layer, the presentation layer and the application layer of the OSI model. This layer interacts with user and user applications. Because this layer is on the top of the layer stack, it does not serve any other layers. Application layer takes the help of

Transport and all layers below it to communicate or transfer its data to the remote host. When an application layer protocol wants to communicate with its peer application layer protocol on remote host, it hands over the data or information to the Transport layer.

Functions of the Application layer:

- It facilitates the user to use the services of the network.
- It is used to develop network-based applications.
- It provides user services like user login, naming network devices, formatting messages, and e-mails, transfer of files etc.
- It is also concerned with error handling and recovery of the message as a whole.

Protocols used in Application layer:

- **Hyper Text Transfer Protocol, HTTP** - It is the underlying protocol for World Wide Web (WWW). It defines how hypermedia messages are formatted and transmitted.
- **File Transfer Protocol, FTP** - It is a client-server based protocol for transfer of files between client and server over the network.
- **Simple Mail Transfer Protocol, SMTP** - It lays down the rules and semantics for sending and receiving electronic mails (e-mails).
- **Domain Name System, DNS** - It is a naming system for devices in networks. It provides services for translating domain names to IP addresses.
- **TELNET** - It provides bi-directional text-oriented services for remote login to the hosts over the network.
- **Simple Network Management Protocol, SNMP** - It is for managing, monitoring the network and for organizing information about the networked devices.

Application layer protocols:

There are several protocols which work for users in Application Layer. Application layer protocols can be broadly divided into two categories:

- Protocols which are used by users. For example, Email.
- Protocols which help and support protocols used by users. For example DNS.

(i) Domain Name System (DNS):

The Domain Name System (DNS) works on Client Server model. It uses UDP protocol for transport layer communication. DNS uses hierarchical domain based naming scheme. The DNS server is configured with **Fully Qualified Domain Names (FQDN)** and email addresses mapped with their respective Internet Protocol addresses. A DNS server is requested with FQDN and it responds back with the IP address mapped with it.

(ii) Simple Mail Transfer Protocol (SMTP):

The Simple Mail Transfer Protocol (SMTP) is used to transfer electronic mail from one user to another. This task is done by means of **email client software (User Agents)** the user is using. User Agents help the user to type and format the email and store it until internet is available. When an email is submitted to send, the sending process is handled by **Message Transfer Agent** which is normally comes inbuilt in email client software.

Message Transfer Agent uses SMTP to forward the email to another Message Transfer Agent (Server side). While SMTP is used by end user to only send the emails, the Servers normally use SMTP to send as well as receive emails.

(iii) File Tranfer Protocol (FTP):

The File Transfer Protocol (FTP) is the most widely used protocol for file transfer over the network. FTP uses TCP/IP for communication. FTP works on Client/Server Model where a client requests file from Server and server sends requested resource back to the client. The client requests the server for a file. When the server receives a request for a file, it opens a TCP connection for the client and transfers the file. After the transfer is complete, the server closes the connection. For a second file, client requests again and the server reopens a new TCP connection.

(iv) Post Office Protocol (POP):

The Post Office Protocol version 3 (POP 3) is a simple mail retrieval protocol used by User Agents (client email software) to retrieve mails from mail server. When a client needs to retrieve mails from server, it opens a connection with the server. User can then access the mails and download them to the local computer. POP3 works in two modes. The most common mode is the **delete mode**, which is to delete the emails from remote server after they are downloaded to local machines. The second mode is the **keep mode**, which does not delete the email from mail server and gives the user an option to access the mails later on mail server.

(v) Hyper Text Transfer Protocol (HTTP):

The Hyper Text Transfer Protocol (HTTP) is the foundation of World Wide Web. Hypertext is well organized documentation system which uses hyperlinks to link the pages in the text documents. HTTP works on client server model. When a user wants to access any HTTP page on the internet, the client machine at user end initiates a TCP connection to server. When the server accepts the client request, the client is authorized to access web pages.

To access the web pages, a client normally uses web browsers, who are responsible for initiating, maintaining, and closing TCP connections. HTTP is a stateless protocol, which means the Server maintains no information about earlier requests by clients.

THE TRANSPORT LAYER:

The transport layer is responsible for error-free, end-to-end delivery of data from the source host to the destination host. It ensures that packets arrive in sequence and without error, by swapping acknowledgments of data reception, and retransmitting lost packets. This type of communication is known as **end-to-end**. It is responsible for the reliability, flow control, and correction of data which is being sent over the network.

Functions of Transport layer:

- It facilitates the communicating hosts to carry on a conversation.
- It provides an interface for the users to the underlying network.
- It can provide for a reliable connection. It can also carry out error checking, flow control, and verification.

Protocols used in Transport layer:

- **Transmission Control Protocol, TCP**- It is a reliable **connection-oriented protocol** that transmits data from the source to the destination machine without any error. A connection is established between the peer entities prior to transmission. At the sending host, TCP divides an incoming byte stream into segments and assigns a separate sequence number to each segment. At the receiving host, TCP reorders the segments and sends an acknowledgment to the sender for correct receipt of segments. TCP also manages flow control so that a fast sender does not overwhelm a slow receiver.
- **User Datagram Protocol, UDP** - It is a **message-oriented protocol** that provides a simple unreliable, connectionless, unacknowledged service. It is suitable for applications that do not require TCP's

sequencing, error control or flow control. It is used for transmitting a small amount of data where the speed of delivery is more important than the accuracy of delivery.

- **Stream Control Transmission Protocol, SCTP** - It combines the features of both TCP and UDP. It is message oriented like the UDP, which providing the reliable, connection-oriented service like TCP. It is used for telephony over the Internet.

(i) Transmission Control Protocol:

The transmission Control Protocol (TCP) is one of the most important protocols of Internet Protocols suite. It is most widely used protocol for data transmission in communication network such as internet.

Features of TCP:

- TCP is reliable protocol. That is, the receiver always sends either positive or negative acknowledgement about the data packet to the sender, so that the sender always has bright clue about whether the data packet is reached the destination or it needs to resend it.
- TCP ensures that the data reaches intended destination in the same order it was sent.
- TCP is connection oriented. TCP requires that connection between two remote points be established before sending actual data.
- TCP provides error-checking and recovery mechanism.
- TCP provides end-to-end communication.
- TCP provides flow control and quality of service.
- TCP operates in Client/Server point-to-point mode.

TCP header:

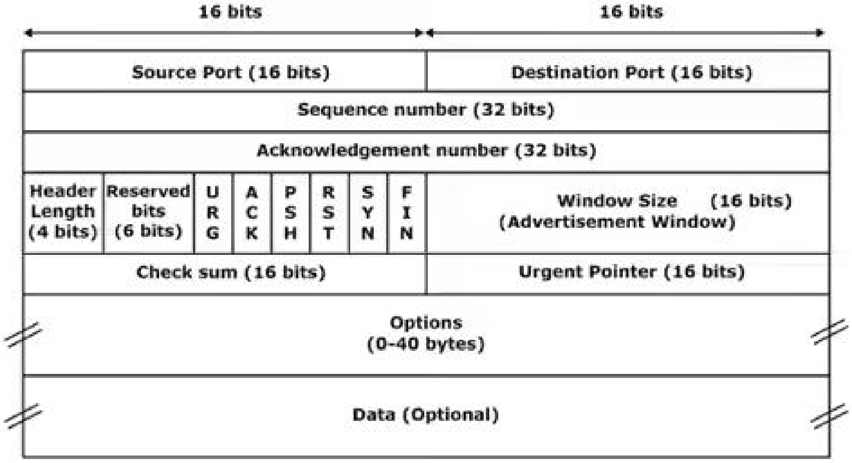

Fig 1.4 TCP header

- **Source Port (16-bits) -** It identifies source port of the application process on the sending device.
- **Destination Port (16-bits) -** It identifies destination port of the application process on the receiving device.
- **Sequence Number (32-bits) -** Sequence number of data bytes of a segment in a session.
- **Acknowledgement Number (32-bits) -** When ACK flag is set, this number contains the next sequence number of the data byte expected and works as acknowledgement of the previous data received.
- **Header length (4-bits) -** This field implies both, the size of TCP header and the offset of data in current packet in the whole TCP segment.
- **Reserved (3-bits) -** Reserved for future use and all are set zero by default.
- **Flags (1-bit each)**
    - ✓ **URG -** It indicates that **Urgent Pointer** field has significant data and should be processed.
    - ✓ **ACK -** It indicates that **Acknowledgement** field has significance. If ACK is cleared to 0, it indicates that packet does not contain any acknowledgement.
    - ✓ **PSH -** When set, it is a request to the receiving station to **PUSH** data (as soon as it comes) to the receiving application without buffering it.
    - ✓ **RST -Reset** flag has the following features:
        - o It is used to refuse an incoming connection.
        - o It is used to reject a segment.
        - o It is used to restart a connection.
    - ✓ **SYN -** This flag is used to set up a connection between hosts.
    - ✓ **FIN -** This flag is used to release a connection and no more data is exchanged thereafter. Because packets with SYN and FIN flags have sequence numbers, they are processed in correct order.
- **Windows Size -** This field is used for flow control between two stations and indicates the amount of buffer (in bytes) the receiver has allocated for a segment, i.e. how much data is the receiver expecting.
- **Checksum -** This field contains the checksum of Header, Data and Pseudo Headers.
- **Urgent Pointer -** It points to the urgent data byte if URG flag is set to 1.
- **Options -** It facilitates additional options which are not covered by the regular header. Option field is always described in 32-bit words. If this field contains data less than 32-bit, padding is used to cover the remaining bits to reach 32-bit boundary.

<u>Connection management</u>:

TCP communication works in Server/Client model. The client initiates the connection and the server either accepts or rejects it. Three-way handshaking is used for connection management.

- **Connection establishment** - Client initiates the connection and sends the segment with a Sequence number. Server acknowledges it back with its own Sequence number and ACK of client's segment which is one more than client's Sequence number. Client after receiving ACK of its segment sends an acknowledgement of Server's response.

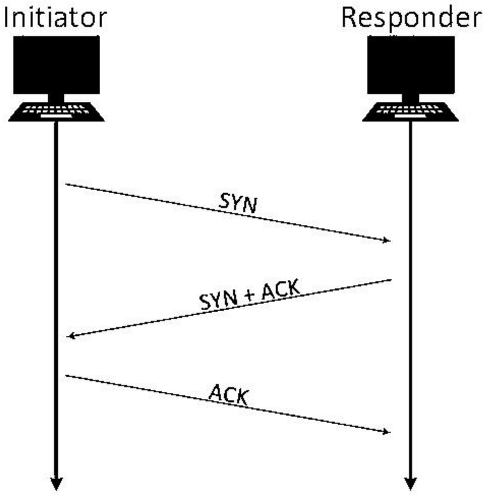

Fig 1.5 Connection establishment

- **Connection release** -Either of server and client can send TCP segment with FIN flag set to 1. When the receiving end responds it back by acknowledging FIN, that direction of TCP communication is closed and connection is released.

<u>Bandwidth Management</u>:

TCP uses the concept of window size to accommodate the need of Bandwidth management. Window size tells the sender at the remote end, the number of data byte segments the receiver at this end can receive. TCP uses **slow start phase** by using window size 1 and increases the window size exponentially after each successful communication.

If an acknowledgement is missed, i.e. data lost in transit network or it received NACK (Negative Acknowledgement), then the window size is reduced to half and slow start phase starts again.

Error control and Flow control:

TCP uses port numbers to know what application process it needs to handover the data segment. Along with that, it uses sequence numbers to synchronize itself with the remote host. All data segments are sent and received with sequence numbers. The Sender knows which last data segment was received by the Receiver when it gets ACK. The Receiver knows about the last segment sent by the Sender by referring to the sequence number of recently received packet.

If the sequence number of a segment recently received does not match with the sequence number the receiver was expecting, then it is discarded and NACK is sent back. If two segments arrive with the same sequence number, the TCP timestamp value is compared to make a decision.

Congestion Control:

When large amount of data is fed to system which is not capable of handling it, congestion occurs. TCP controls congestion by means of Window mechanism. TCP sets a window size telling the other end how much data segment to send. TCP may use three algorithms for congestion control:

- Additive increase, Multiplicative Decrease
- Slow Start
- Timeout React

Timer Management:

TCP uses different types of timer to control and management various tasks:

i. **Keep-alive timer:**
   - This timer is used to check the integrity and validity of a connection.
   - When keep-alive time expires, the host sends a probe to check if the connection still exists.

ii. **Retransmission timer:**
   - This timer maintains stateful session of data sent.
   - If the acknowledgement of sent data does not receive within the Retransmission time, the data segment is sent again.

iii. **Persist timer:**
   - TCP session can be paused by either host by sending Window Size 0.
   - To resume the session a host needs to send Window Size with some larger value.
   - If this segment never reaches the other end, both ends may wait for each other for infinite time.

- When the Persist timer expires, the host re-sends its window size to let the other end know.
- Persist Timer helps avoid deadlocks in communication.

iv. Timed-Wait:

- After releasing a connection, either of the hosts waits for a Timed-Wait time to terminate the connection completely.
- This is in order to make sure that the other end has received the acknowledgement of its connection termination request.
- Timed-out can be a maximum of 240 seconds (4 minutes).

Crash Recovery:

TCP is very reliable protocol. It provides sequence number to each of byte sent in segment. It provides the feedback mechanism i.e. when a host receives a packet, it is bound to ACK that packet having the next sequence number expected (if it is not the last segment).

When a TCP Server crashes mid-way communication and re-starts its process it sends **TPDU (Transport Protocol Data Unit)** broadcast to all its hosts. The hosts can then send the last data segment which was never unacknowledged and carry onwards.

(ii) User Datagram Protocol (UDP):

The User Datagram Protocol (UDP) is simplest Transport Layer communication protocol available of the TCP/IP protocol suite. It involves minimum amount of communication mechanism. UDP is said to be an unreliable transport protocol but it uses IP services which provides best effort delivery mechanism.

In UDP, the receiver does not generate an acknowledgement of packet received and in turn, the sender does not wait for any acknowledgement of packet sent. This shortcoming makes this protocol unreliable as well as easier on processing.

Requirement of UDP:

The UDP is deployed where the acknowledgement packets share significant amount of bandwidth along with the actual data. For example, in case of video streaming, thousands of packets are forwarded towards its users. Acknowledging all the packets is troublesome and may contain huge amount of bandwidth wastage. The best delivery mechanism of underlying IP protocol ensures best efforts to deliver its packets, but even if some packets in video streaming get lost, the impact is not calamitous and can be ignored easily. Loss of few packets in video and voice traffic sometimes goes unnoticed.

Features of UDP:

- UDP is used when acknowledgement of data does not hold any significance.
- UDP is good protocol for data flowing in one direction.
- UDP is not connection oriented.
- UDP does not provide congestion control mechanism.
- UDP does not guarantee ordered delivery of data.
- UDP is stateless.
- UDP is suitable protocol for streaming applications such as VoIP, multimedia streaming.

UDP Header:

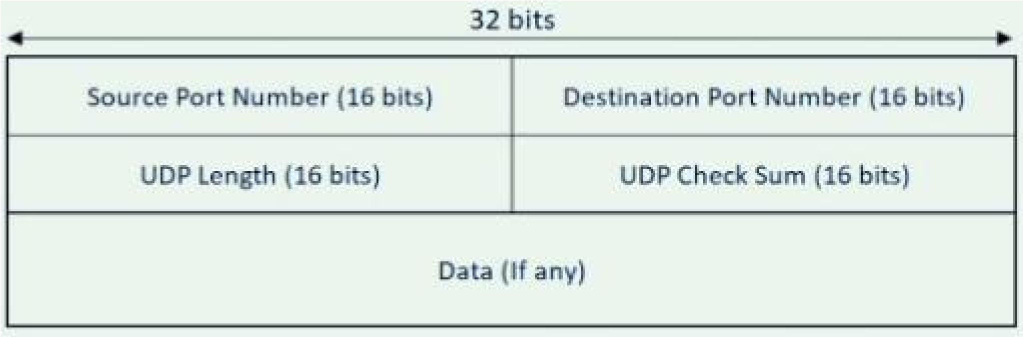

Fig 1.6 UDP header

UDP header contains four main parameters:

- **Source Port** - This 16 bits information is used to identify the source port of the packet.
- **Destination Port** - This 16 bits information, is used identify application level service on destination machine.
- **Length** - Length field specifies the entire length of UDP packet (including header). It is 16-bits field and minimum value is 8-byte, i.e. the size of UDP header itself.
- **Checksum** - This field stores the checksum value generated by the sender before sending. IPv4 has this field as optional so when checksum field does not contain any value it is made 0 and all its bits are set to zero.

UDP applications:

- Domain Name Services
- Simple Network Management Protocol

- Trivial File Transfer Protocol
- Routing Information Protocol

THE INTERNET LAYER:

The Internet layer, also known as the network layer or IP layer, accepts and delivers packets for the network. This layer includes the powerful Internet Protocol (IP), the Address Resolution Protocol (ARP), and the Internet Control Message Protocol (ICMP). It is responsible for logical transmission of data packets over the internet.

Functions of Internet layer:

- It transmits data packets to the link layer.
- It routes each of the data packets independently from the source to the destination, using the optimal route.
- It reassembles the out-of-order packets when they reach the destination.
- It handles the error in transmission of data packets and fragmentation of data packets.

Protocols used in Internet layer:

- **Internet Protocol, IP -** It is a connectionless and unreliable protocol that provides a best effort delivery service. It transports data packets called **datagrams** that travel over different routes across multiple nodes.
- **Address Resolution Protocol, ARP -** This protocol maps the logical address or the Internet address of a host to its physical address, as printed in the network interface card.
- **Reverse Address Resolution Protocol, RARP -** This is to find the Internet address of a host when its physical address is known.
- **Internet Control Message Protocol, ICMP -** It monitors sending the queries as well as the error messages.
- **Internet Group Message Protocol, IGMP -** It allows the transmission of a message to a group of recipients simultaneously.

Network layer protocols:

Every computer in a network has an IP address by which it can be uniquely identified and addressed. An IP address is Layer-3 (Network Layer) logical address. This address may change every time a computer restarts. A computer can have one IP at one instance of time.

(i) Address Resolution Protocol (ARP):

While communicating, a host needs Layer-2 (MAC) address of the destination machine which belongs to the same broadcast domain or network. A MAC address is physically burnt into the Network Interface Card (NIC) of a machine and it never changes.

On the other hand, IP address on the public domain is rarely changed. If the NIC is changed in case of some fault, the MAC address also changes. Thus, for Layer-2 communication to take place, a mapping between the two is required.

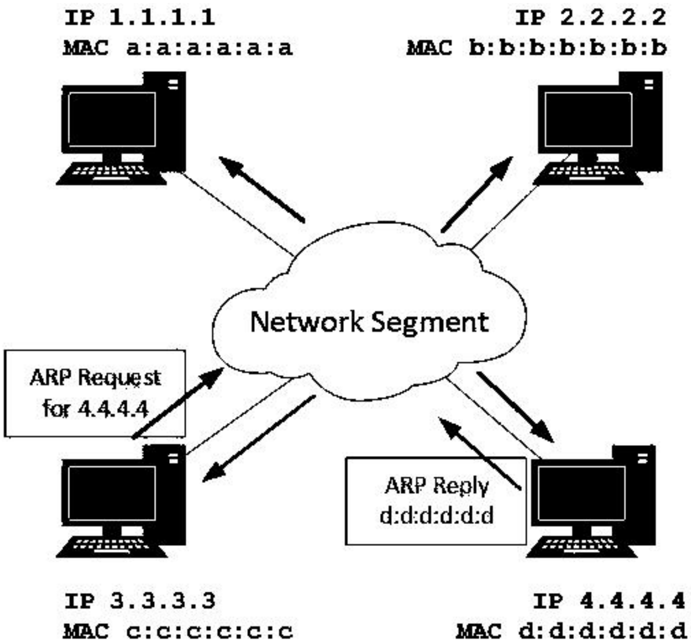

Fig 1.7 Address Resolution Network

To know the MAC address of remote host on a broadcast domain, a computer wishing to initiate communication sends out an ARP broadcast message asking, "Who has this IP address?" Because it is a broadcast, all hosts on the network segment (broadcast domain) receive this packet and process it. ARP packet contains the IP address of destination host, the sending host wishes to talk to. When a host receives an ARP packet destined to it, it replies back with its own MAC address.

Once the host gets destination MAC address, it can communicate with remote host using Layer-2 link protocol. This MAC to IP mapping is saved into ARP cache of both sending and receiving hosts. Next time, if they need to communicate, they can directly refer to their respective **ARP cache**.

Reverse ARP is a mechanism where host knows the MAC address of remote host but requires to know IP address to communicate.

(ii) Internet Control Message Protocol (ICMP):

ICMP is network diagnostic and error reporting protocol. ICMP belongs to IP protocol suite and uses IP as carrier protocol. After constructing ICMP packet, it is encapsulated in IP packet. Because IP itself is a best-effort non-reliable protocol, so is ICMP.

Any feedback about network is sent back to the originating host. If some error in the network occurs, it is reported by means of ICMP. ICMP contains dozens of diagnostic and error reporting messages.

ICMP-echo and **ICMP-echo-reply** are the most commonly used ICMP messages to check the reachability of end-to-end hosts. When a host receives an ICMP-echo request, it is bound to send back an ICMP-echo-reply. If there is any problem in the transit network, the ICMP will report that problem.

(iii) Internet Protocol Version 4 (IPv4):

IPv4 is 32-bit addressing scheme used as TCP/IP host addressing mechanism. IP addressing enables every host on the TCP/IP network to be uniquely identifiable.

IPv4 provides hierarchical addressing scheme which enables it to divide the network into sub-networks, each with well-defined number of hosts. IP addresses are divided into many categories:

- **Class A** - it uses first octet for network addresses and last three octets for host addressing
- **Class B** - it uses first two octets for network addresses and last two for host addressing
- **Class C** - it uses first three octets for network addresses and last one for host addressing
- **Class D** - it provides flat IP addressing scheme in contrast to hierarchical structure for above three.
- **Class E** - It is used as experimental.

IPv4 also has well-defined address spaces to be used as private addresses (not routable on internet), and public addresses (provided by ISPs and are routable on internet).

Though IP is not reliable one; it provides '**Best-Effort-Delivery**' mechanism.

(iv) Internet Protocol Version 6 (IPv6):

Exhaustion of IPv4 addresses gave birth to a next generation Internet Protocol version 6. IPv6 addresses its nodes with 128-bit wide address providing plenty of address space for future to be used on entire planet or beyond.

IPv6 has introduced **Anycast addressing** but has removed the concept of broadcasting. IPv6 enables devices to self-acquire an IPv6 address and communicate within that subnet. This auto-configuration removes the dependability of **Dynamic Host Configuration Protocol (DHCP)** servers. This way, even if the DHCP server on that subnet is down, the hosts can communicate with each other.

IPv6 provides new feature of IPv6 mobility. Mobile IPv6 equipped machines can roam around without the need of changing their IP addresses.

Network layer routing:

When a device has multiple paths to reach a destination, it always selects one path by preferring it over others. This selection process is termed as Routing. Routing is done by special network devices called routers or it can be done by means of software processes.The software based routers have limited functionality and limited scope.

A router is always configured with some default route. A default route tells the router where to forward a packet if there is no route found for specific destination. In case there are multiple path existing to reach the same destination, router can make decision based on the following information:

- Hop Count
- Bandwidth
- Metric
- Prefix-length
- Delay

i. Unicast routing:

Most of the traffic on the internet and intranets known as **unicast data** or **unicast traffic** is sent with specified destination. Routing unicast data over the internet is called unicast routing. It is the simplest form of routing because the destination is already known. Hence the router just has to look up the routing table and forward the packet to next hop.

Unicast routing algorithms:

There are two kinds of routing protocols available to route unicast packets:

a) Distance Vector Routing Protocol:

Distance Vector is simple routing protocol which takes routing decision on the **number of hops** between source and destination. A route with less number of hops is considered as the best route. Every router advertises its set best routes to other routers. Ultimately, all routers build up their network topology based on the advertisements of their peer routers. For example, Routing Information Protocol (RIP).

b) Link State Routing Protocol:

Link State protocol is slightly complicated protocol than Distance Vector. It takes into account the **states of links** of all the routers in a network. This technique helps routers build a common graph of the entire network. All routers then calculate their best path for routing purposes. For example, Open Shortest Path First (OSPF) and Intermediate System to Intermediate System (ISIS).

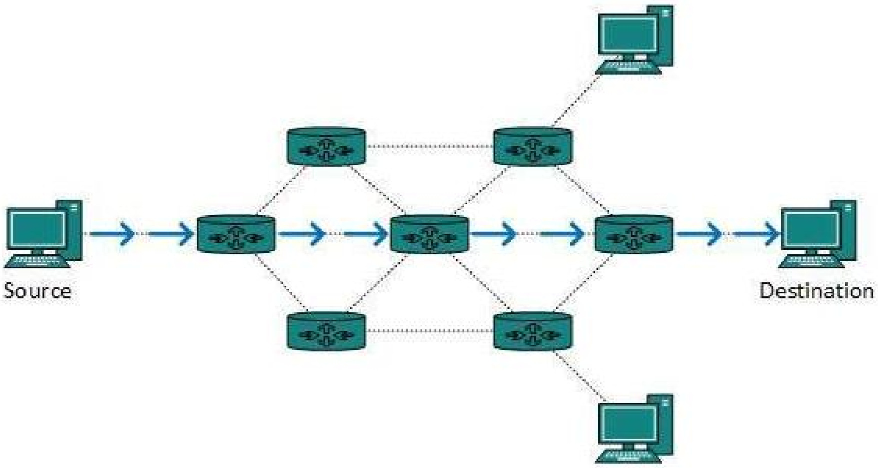

Fig 1.8 Unicast routing

ii. Broadcast routing:

By default, the broadcast packets are not routed and forwarded by the routers on any network. Routers create broadcast domains. But it can be configured to forward broadcasts in some special cases. A broadcast message is destined to all network devices.

Broadcast routing can be done in two ways (algorithm):

- A router creates a data packet and then sends it to each host one by one. In this case, the router creates multiple copies of single data packet with different destination addresses. All packets are sent as unicast but because they are sent to all, it simulates as if router is broadcasting. This method consumes lots of bandwidth and router must know the destination address of each node.

- Secondly, when router receives a packet that is to be broadcasted, it simply floods those packets out of all interfaces. All routers are configured in the same way.
- Broadcast routing uses **reverse path Forwarding technique**, to detect and discard duplicates.

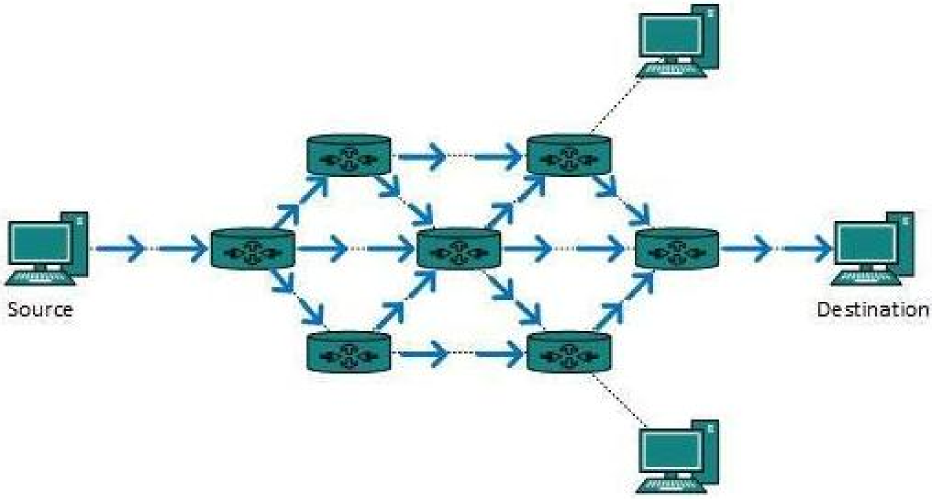

Fig 1.9 Broadcast routing

iii. <u>Multicast routing</u>:

Multicast routing is special case of broadcast routing with significant difference and challenges. In broadcast routing, packets are sent to all nodes even if they do not want it. But in Multicast routing, the data is sent to only nodes which wants to receive the packets. The router must know that there are nodes, which wish to receive multicast packets (or stream) then only it should forward. Multicast routing uses **spanning tree protocol** to avoid looping. It also uses **reverse path Forwarding technique**, to detect and discard duplicates and loops.

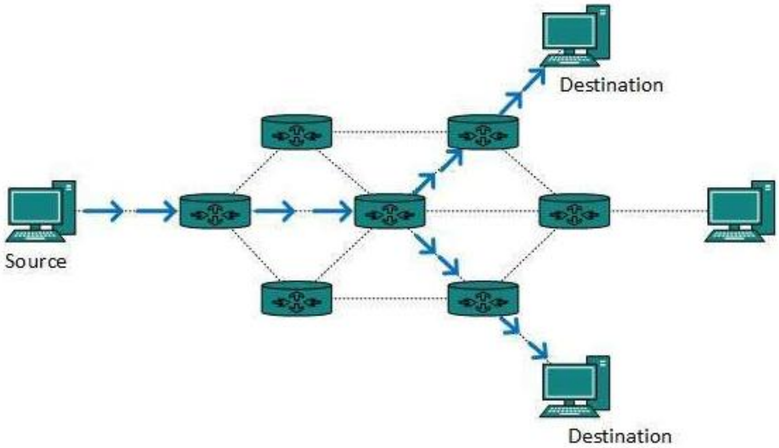

Fig 1.10 Multicast routing

Multicast routing algorithms:

Unicast routing protocols use graphs while Multicast routing protocols use trees, i.e. spanning tree to avoid loops. The optimal tree is called shortest path spanning tree.

- **DVMRP** - Distance Vector Multicast Routing Protocol
- **MOSPF** - Multicast Open Shortest Path First

iv. Anycast routing:

Anycast packet forwarding is a mechanism where multiple hosts can have same logical address. When a packet destined to this logical address is received, it is sent to the host which is nearest in routing topology. Anycast routing is done with help of DNS server. Whenever an Anycast packet is received it is enquired with DNS to where to send it. DNS provides the IP address which is the nearest IP configured on it.

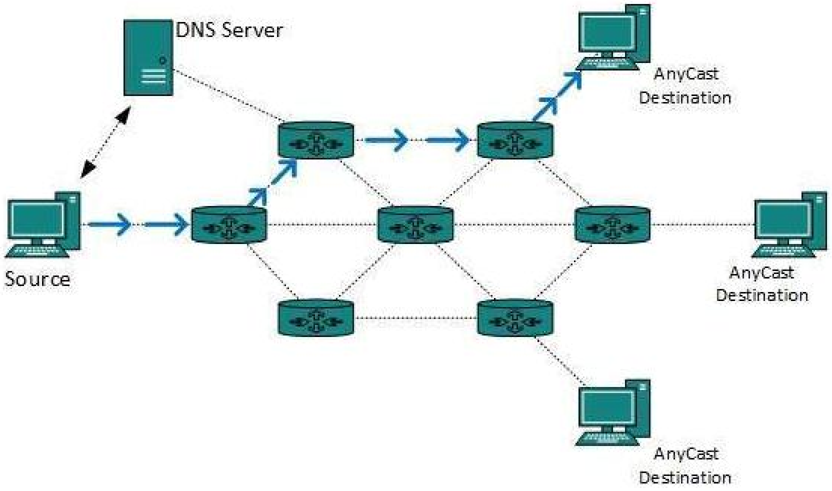

Fig 1.11 Anycast routing

IP ADDRESSING:

An IP address is an address having information about how to reach a specific host, especially outside the LAN (Local Area Network). An IP address is a 32-bit unique address having an address space of 2^{32}.Generally, there are two notations in which the IP address is written, dotted decimal notation and hexadecimal notation.

i. Dotted Decimal Notation:

A dotted decimal notation should have the following:

1. The value of any segment (byte) is between 0 and 255 (both included).

2. No zeroes are preceding the value in any segment (054 is wrong, 54 is correct).

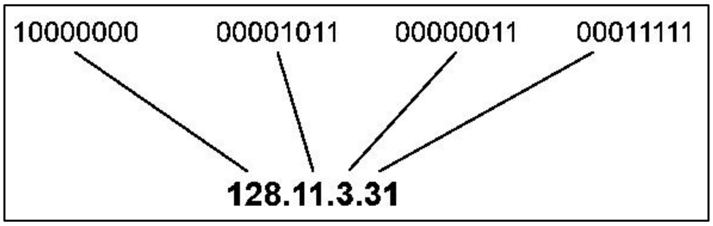

Fig 1.12 Dotted decimal notation

ii. <u>Hexadecimal Notation</u>:

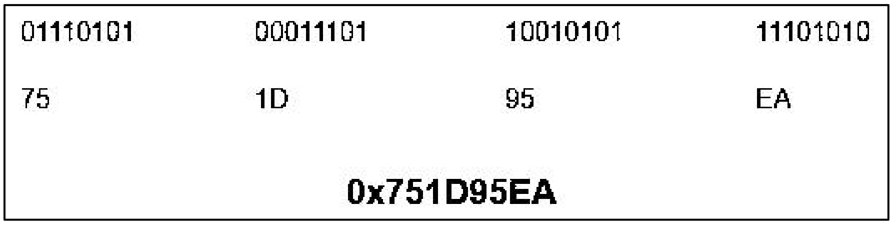

Fig 1.13 Hexadecimal notation

(i) <u>Classful addressing</u>:

The 32 - bit IP address is divided into five sub-classes. These are:

- Class A
- Class B
- Class C
- Class D
- Class E

Each of these classes has a valid range of IP addresses. **Classes D and E** are reserved for **multicast and experimental purposes** respectively. The order of bits in the first octet determines the classes of the IP address. The IPv4 address is divided into two parts:

- Network ID
- Host ID

The class of IP address is used to determine the bits used for network ID and host ID and the number of total networks and hosts possible in that particular class. Each network administrator assigns an IP address to each device that is connected to its network.

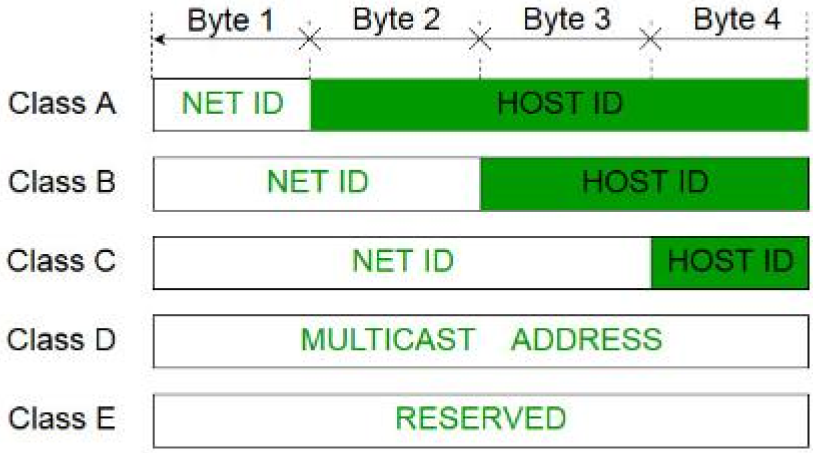

Fig 1.14 Classful addressing

<u>Class A</u>:

IP addresses belonging to class A are assigned to the networks that contain a large number of hosts.

- The network ID is 8 bits long.
- The host ID is 24 bits long.

The higher-order bit of the first octet in class A is always set to **0**. The remaining 7 bits in the first octet are used to determine network ID. The 24 bits of host ID are used to determine the host in any network. The default subnet mask for Class A is 255.x.x.x. Therefore, class A has a total of:

- 2 ^ 7 - 2 = 126 network ID (Here 2 address is subtracted because 0.0.0.0 and 127.x.y.z are special address.)
- 2 ^ 24 - 2 = 16,777,214 host ID

IP addresses belonging to class A ranges from 1.x.x.x - 126.x.x.x

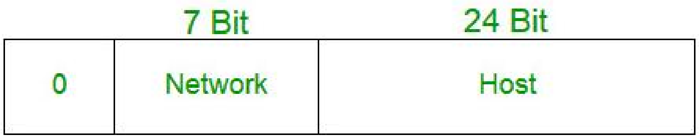

Fig 1.15 Class A

<u>Class B</u>:

IP address belonging to class B is assigned to networks that range from medium-sized to large-sized networks.

- The network ID is 16 bits long.
- The host ID is 16 bits long.

The higher-order bits of the first octet of IP addresses of class B are always set to **10**. The remaining 14 bits are used to determine the network ID. The 16 bits of host ID are used to determine the host in any network. The default subnet mask for class B is 255.255.x.x. Class B has a total of:

- 2^14 = 16384 network address
- 2^16 – 2 = 65534 host address

IP addresses belonging to class B ranges from 128.0.x.x - 191.255.x.x.

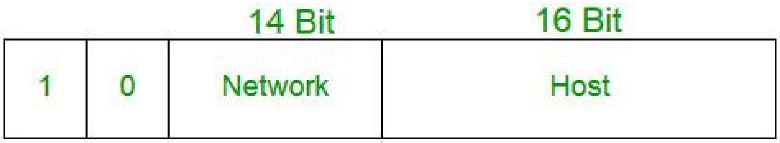

Fig 1.16 Class B

<u>Class C</u>:

IP addresses belonging to class C are assigned to small-sized networks.

- The network ID is 24 bits long.
- The host ID is 8 bits long.

The higher-order bits of the first octet of IP addresses of class C is always set to **110**. The remaining 21 bits are used to determine the network ID. The 8 bits of host ID are used to determine the host in any network. The default subnet mask for class C is 255.255.255.x. Class C has a total of:

- 2^21 = 2097152 network address
- 2^8 – 2 = 254 host address

IP addresses belonging to class C range from 192.0.0.x - 223.255.255.x.

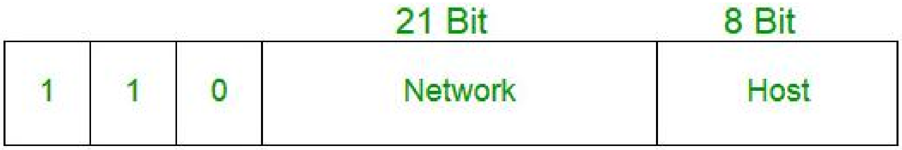

Fig 1.17 Class C

<u>Class D</u>:

IP address belonging to class D is reserved for **multi-casting**. The higher-order bits of the first octet of IP addresses belonging to class D is always set to **1110**. The remaining bits are for the address that interested hosts recognize.

Class D does not possess any subnet mask. IP addresses belonging to class D range from 224.0.0.0 - 239.255.255.255.

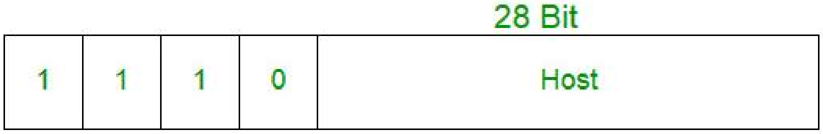

Fig 1.18 Class D

Class E:

IP addresses belonging to class E are reserved for **experimental and research purposes**. IP addresses of class E range from 240.0.0.0 - 255.255.255.254. This class doesn't have any subnet mask. The higher-order bits of the first octet of class E are always set to **1111**.

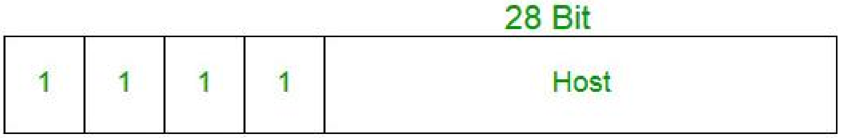

Fig 1.19 Class E

(ii) Classless addressing:

The problem with the classful addressing method is that millions of class A addresses are wasted, many of the class B addresses are wasted, whereas, the number of addresses available in class C is so small that it cannot cater to the needs of organizations. Class D addresses are used for multicast routing and are therefore available as a single block only. Class E addresses are reserved. Since there are these problems, Classful networking was replaced by **Classless Inter-Domain Routing (CIDR)**.

To reduce the wastage of IP addresses in a block, **sub-netting** is used. The IP address will be given and the number of bits for mask are defined along with it, like, 192.168.1.1/28. Here, **subnet mask** is found by putting the given **number of bits out of 32 as 1**, like, in the given address, **28 out of 32 bits** need to be set as 1 and the rest as 0, and so, the **subnet mask** would be **255.255.255.240**.

Network address:

It identifies a network on internet. Using this, the range of addresses in the network and total possible number of hosts in the network can be found.

Mask:

It is a 32-bit binary number that gives the network address in the address block when AND operation is bitwise applied on the mask and any IP address of the block.

The default mask in different classes are :

Class A	Class B	Class C
255.0.0.0	255.255.0.0	255.255.255.0

Problem: If the IP address is 132.6.17.85, then find the network address.

Solution: The default mask is 255.255.0.0, which means that only the first 2 bytes are preserved and the other 2 bytes are set to 0. Therefore, the network address is **132.6.0.0**.

Subnetting:

Dividing a large block of addresses into several contiguous sub-blocks and assigning these sub - blocks to different smaller networks is called subnetting. It is a practice that is widely used when classless addressing is done.

Some values calculated in subnetting:

1. Number of subnets : $2^{(\text{Given bits for mask - No. of bits in default mask})}$

2. Subnet address : AND result of subnet mask and the given IP address

3. Broadcast address : By putting the host bits as 1 and retaining the network bits as in the IP address

4. Number of hosts per subnet : $2^{(32 - \text{Given bits for mask})} - 2$

5. First Host ID : Subnet address + 1 (adding one to the binary representation of the subnet address)

6. Last Host ID : Subnet address + Number of Hosts

Problem: If the IP Address is 172.16.0.0/25, then find the number of subnets and the number of hosts per subnet. Also, for the first subnet block, find the subnet address, first host ID, last host ID, and broadcast address.

Solution: This is a class B address. So, no. of subnets = $2^{(25-16)} = 2^9 = 512$.

No. of hosts per subnet = $2^{(32-25)} - 2 = 2^7 - 2 = 128 - 2 = 126$.

For the first subnet block, we have subnet address = 172.16.0.0.

First host id = 172.16.0.1.

Last host id = 172.16.0.126.

and Broadcast address = 172.16.0.127.

NETWORK AND COMPUTER ATTACKS:

Network attack:

A **network attack** is an attempt to gain unauthorized access to an organization's network, with the objective of stealing data or perform other malicious activity. There are two main types of network attacks:

- **Passive:** Attackers gain access to a network and can monitor or steal sensitive information, but without making any change to the data, leaving it intact.
- **Active:** Attackers not only gain unauthorized access but also modify data, either deleting, encrypting or otherwise harming it.

Computer attack:

A **cyber attack** or **computer attack** is any attempt to gain unauthorized access to a computer, computing system or computer network with the intent to cause damage. Cyber attacks aim to disable, disrupt, destroy or control computer systems or to alter, block, delete, manipulate or steal the data held within these systems.

Network security:

Network Security protects data and systems from unauthorized access, unwanted modification, intrusions, and other threats because unauthorized persons or attackers can penetrate the data, expose personal information, or steal money. It defends network traffic and protects the infrastructure from numerous threats, including trojan horses, malware, etc.

Types of Network Security Attacks:

There are different types of attacks on Network Security. Some of the most common types are discussed:

1. Malware:

Malware is the fastest type of malicious software that a hacker designs specifically for his use to disrupt and damage systems and networks of systems and acquire authorized access to steal data or personal information. Malware is automatically installed via the internet and quickly infects all computers linked to the network.

2. Virus:

A virus is also malicious software but requires user interaction to harm the system. The virus cannot replicate itself; it requires human involvement by using malicious links, such as email attachments that contain malicious code. The files can be corrupted when one click on malicious links, and the personal information is stolen.

3. Worm:

The most common standalone computer malware program is the worm, which replicates itself without human involvement and spreads via a network from one infected system to another by exploiting system flaws and transmitting "payloads" that harm host computers. Worms don't need a host file to get started; they use the same host as the system they are in, and the number of worms grows over time. It penetrates the system via an application and consumes its processing power bandwidth, causing the system to become unresponsive.

4. Man-in-the-middle:

A Man-in-the-middle (MITM) attack occurs when an attacker stands between two devices or between a client and a server, intercepts, monitors, and steals confidential data, or modifies it and sends it back to the original receiver.

5. Distributed Denial of Service (DDoS):

DDoS (Distributed Denial of Service) is a more sophisticated type of DoS attack. In this attack, the attacker uses numerous systems to bombard the victim's server with traffic, causing the server or network to malfunction and the victim to be unable to access it. It is challenging to detect DDoS threats since they are launched from several infected systems. Most black hat hackers use this attack to blackmail or retaliate against the victim. There are three types of denial-of-service attacks:

- Connection flooding
- Vulnerability attacks
- Bandwidth flooding

6. Phishing:

A phishing attack is a social engineering attack. An attacker manipulates the victim's thoughts to get personal information like credit and debit cards, online banking details, username and password, social networking information, and other digital account information. Phishing is the term used nowadays when a hacker or attacker tries to deceive individuals by threatening, frightening, or seducing them. Attackers send malicious attachments and links to users via email, posing as trusted sources such as company owners, managers, or bankers. When users open the email with interest, they allow access to the attackers.

7. IP Spoofing:

IP (Internet Protocol) Spoofing is a form of malicious attack. Spoofing is a DDoS and Man-in-the-Middle attack technique used by attackers on target devices. The attacker keeps track of the system's packet header information, such as IP address and Mac address, and then replaces the source IP address with a spoofed IP address to impersonate the sender's true identity. The receiver will believe it interacts with a trusted source and provides access to the attacker. Hackers take advantage of spoofed IP packets because they know these are the primary way of transmitting data between sender and recipient.

8. Botnet:

Botnets are a group of computers and networks, including PCs, servers, and mobile devices, infected with malware and controlled by hackers. A hacker uses malicious software to connect with multiple computers via a private network to perform attacks. Because it attacks various systems at once and corrupts them, this attack is also known as the **zombie army attack**. Without the owner's awareness, the attacker gains access to and manages all of the systems on that network, manipulates bots to transmit spam, steal data, and gain unwanted access.

9. Trojan horse:

A Trojan horse is a malicious application that seems useful due to its harmless appearance, but it is harmful when installed and downloaded on a computer. This is a malicious program that can alter computer settings and perform unusual tasks like deleting file allocation tables and causing the system to hang. It is usually embedded in games and spreads via social engineering methods like emails. It could give attackers access to personal information such as financial information, usernames, passwords, etc.

10. Packet Sniffer:

Packet sniffers capture or save copies of each transmission packet when packets flow over a network in a wireless transmission zone. A sniffer is a tool attackers use to gather sensitive information such as social information, financial data, trade secrets, user IDs, passwords, etc. Sniffing is a data theft technique that involves capturing, decoding, inspecting, and interpreting the information contained within a network packet on a TCP/IP connection using a packet sniffer.

MALWARE:

Malware, short for malicious software, refers to any intrusive software developed by cybercriminalas (hackers) to steal data and damage or destroy computers and computer systems. It is a software that is specifically designed to disrupt, damage, or gain unauthorized access to a computer system. Example of common malware include viruses, worms, trojan horses, spyware, adware and ransomeware.

Malware attack:

A malware attack is a common cyberattack where malware executes unauthorized actions on the victim’s system. The malicious software encompasses many specific types of attacks such as ransomware, spyware, command and control, and more. Criminal organizations, state actors, and even well-known businesses have been accused of deploying malware. Like other types of cyber attacks, some malware attacks end up with mainstream news coverage due to their severe impact. An example of a famous malware attack is the **WannaCry ransomeware attack**.

Examination of malware attacks:

Malware attack discussion typically encompasses three main aspects:

- **Objective**: What the malware is designed to achieve
- **Delivery**: How the malware is delivered to the target
- **Concealment**: How the malware avoids detection

Objectives:

Malware is created with an objective in mind. While it could be said that the objective is “limited only to the imagination of its creator,” this will focus on some of the most common objectives observed in malware.

(i) Exfiltrate Information:

Stealing data, credentials, payment information, etc. is a recurring theme in the realm of cybercrime. Malware focused on this type of theft can be extremely costly to a person, company, or government target that falls victim.

(ii) Disrupt Operations:

Actively working to "cause problems" for a target's operation is another objective seen in malware. From a virus on a single computer corrupting critical OS files (making that one system unusable) to an orchestrated, physical self-destruction of many systems in an installation, the level of "disruption" can vary. And there's also the scenario where infected systems are directed to carry out large-scale distributed denial of service (DDOS) attacks.

(iii) Demand Payment:

Some malware is focused on directly extorting money from the target. **Scareware** uses empty threats to "scare" the target into paying some money. **Ransomware** is a type of malware that attempts to prevent a target from accessing their data (usually by encrypting files on the target) until the target "pays up." While there is debate over whether victims of ransomware should or should not pay, it has become enough of a threat that some companies have preemptively purchased Bitcoin just in case they get hit with ransomware and decide to pay the ransom.

Types of Malware Attack Vectors:

There are three main types of malware attack vectors:

(i) Trojan Horse:

This is a program which appears to be one thing (e.g. a game, a useful application, etc.) but is really a delivery mechanism for malware. A trojan horse relies on the user to download it (usually from the internet or via email attachment) and run it on the target.

(ii) Virus:

A virus is a type of self-propagating malware which infects other programs / files (or even parts of the operating system and/or hard drive) of a target via **code injection**. This behavior of malware propagation through injecting itself into existing software/data is a differentiator between a virus and a trojan horse (which has purposely built malware into one specific application and does not make attempts to infect others).

(iii) Worm:

Malware designed to propagate itself into other systems is a worm. While virus and trojan horse malware are localized to one infected target system, a worm actively works to infect other targets (sometimes without any interaction on the user's behalf).

Over the years, malware has been observed to use a variety of different delivery mechanisms, or attack vectors. While a few are admittedly academic, many attack vectors are effective at compromising their targets. These attack vectors generally occur over electronic communications such as email, text, vulnerable network service, or compromised website, malware delivery can also be achieved via physical media (e.g. USB thumb drive, CD/DVD, etc.).

PROTECTION AGAINST MALWARE ATTACKS:

The following best practices can help prevent a malware attack from succeeding and/or mitigate the damage done by a malware attack.

Continuous User Education:

Training users on best practices for avoiding malware (i.e. don't download and run unknown software, don't blindly insert "found media" into your computer), as well as how to identify potential malware (i.e. phishing emails, unexpected applications/processes running on a system) can go a long way in protecting an organization. Periodic, unannounced exercises, such as intentional phishing campaigns, can help keep users aware and observant.

Use Reputable A/V Software:

When installed, a suitable A/V (Anti-Virus) solution will detect (and remove) any existing malware on a system, as well as monitor for and mitigate potential malware installation or activity while the system is running. It'll be important to keep it up-to-date with the vendor's latest definitions/signatures.

Ensure Your Network is Secure:

Controlling access to systems on the organization's network is a great idea for many reasons. Use of proven technology and methodologies - such as using a **firewall, IPS** (Intrusion Prevention System), **IDS** (Intrusion Detection System), and remote access only through **VPN** (Virtual Private Network) will help minimize the attack "surface" the organization exposes. **Physical system isolation** is usually considered an extreme measure for most organizations, and is still vulnerable to some attack vectors.

<u>Perform Regular Website Security Audits</u>:

Scanning an organization's websites regularly for vulnerabilities (i.e. software with known bugs, server/service/application misconfiguration) and to detect if known malware has been installed can keep the organization secure, protect the users, and protect customers and visitors for public-facing sites.

<u>Create Regular, Verified Backups</u>:

Having a regular (i.e. current and automated) offline backup can be the difference between smoothly recovering from a destructive virus or ransomware attack and stressful, frantic scrambling with costly downtime/data-loss. The key here is to actually have regular backups that are verified to be happening on the expected regular basis and are usable for restore operations. Old, outdated backups are less valuable than recent ones, and backups that don't restore properly are of no value.

<u>INTRUSION ATTACKS</u>:

The most common threat to security is the attack by the intruder. Intruders are often referred to as hackers and are the most harmful factors contributing to the vulnerability of security. They have immense knowledge and an in-depth understanding of technology and security. Intruders breach the privacy of users and aim at stealing the confidential information of the users. The stolen information is then sold to third-party, which aim at misusing the information for their own personal or professional gains.

<u>Categories of intruders</u>:

(i) <u>Masquerader</u>:

The category of individuals that are **not authorized** to use the system but still exploit user's privacy and confidential information by possessing techniques that give them control over the system, such category of intruders is referred to as Masquerader. Masqueraders are **outsiders** and hence they **don't have direct access** to the system, their aim is to attack unethically to steal data/ information.

(ii) <u>Misfeasor</u>:

The category of individuals that are **authorized** to use the system, but misuse the granted access and privilege. These are individuals that take undue advantage of the permissions and access given to them, such category of intruders is referred to as Misfeasor. Misfeasors are **insiders** and they have **direct access** to the system, which they aim to attack unethically for stealing data/ information.

(iii) Clandestine User:

The category of individuals those have **supervision/administrative control** over the system and misuse the authoritative power given to them. The misconduct of power is often done by superlative authorities for financial gains, such a category of intruders is referred to as Clandestine User. A Clandestine User can be any of the two, **insiders or outsiders**, and accordingly, they can have **direct/ indirect access** to the system, which they aim to attack unethically by stealing data/ information.

Methods adopted by intruders for cracking passwords:

- Regressively try all **short passwords** that may open the system for them.
- Try unlocking the system with **default passwords**, which will open the system if the user has not made any change to the default password.
- Try unlocking the system by **personal information** of the user such as their name, family member names, address, phone number in different combinations.
- Making use of **Trojan horse** for getting access to the system of the user.
- Attacking the connection of the host and remote user and getting entry through their **connection gateway**.
- Trying all the **applicable information**, relevant to the user such as plate numbers, room numbers, locality info.

To prevent intruders from attacking the computer system, it is extremely important to be aware of the preventive measures which leads to strengthening of the security posture. Also, whenever there is potential detection of the system being attacked make sure to reach cyber security experts as soon as possible.

Burp Intruder:

Burp Intruder is a tool for **automating customized attacks** against web applications. It enables one to configure attacks that send the same HTTP request over and over again, inserting different payloads into predefined positions each time.

ADDRESSING PHYSICAL SECURITY:

Physical security is the protection of personnel, hardware, software, networks and data from physical actions and events that could cause serious loss or damage to an enterprise, agency or institution. This includes protection from fire, flood, natural disasters, burglary, theft, vandalism and terrorism. While most of these are covered by insurance, physical security's prioritization of damage prevention avoids the time, money and resources lost because of these events. In terms of cybersecurity, the purpose of physical security is to minimize this risk to information systems and information. Systems and devices can provide threat actors with additional attack vectors to connect to networks, infect other devices, and exfiltrate data; therefore, access to systems, equipment, and respective operating environments should be limited to only authorized individuals. Multiple layers of physical security can be implemented to protect the most critical assets and services. There are four categories of **physical access security zones: public, reception, operations, and restricted access**. Physical access controls can be implemented in accordance with these security zones, including barriers, security guards, security cameras, physical access devices, and identity and authorization controls. In addition, sensitive information, whether in paper or electronic form, must be protected from unauthorized access and disclosure.

Components of Physical security framework:

The success of an organization's physical security program can often be attributed to how well each of the below components is implemented, improved and maintained.

1. Access control
2. Surveillance
3. Testing

1. Access control:

The key to maximizing one's physical security measures is to limit and control what people have access to sites, facilities and materials. Access control encompasses the measures taken to limit exposure of certain assets to authorized personnel only. Examples of these corporate barriers often include ID badges, keypads and security guards. However, these obstacles can vary greatly in terms of method, approach and cost.

The building is often the first line of defense for most physical security systems. Items such as fences, gates, walls and doors all act as physical deterrents to criminal entry. Additional locks, barbed wire, visible security measures and signs all reduce the number of casual attempts carried out by cybercriminals. More sophisticated access controls involve a technology-supported approach. ID card scanners and near-field communication (NFC) ID cards are methods of physical authentication that security teams can use to verify the identities of individuals entering and exiting various facilities.

Using tactically placed obstacles, organizations can make it more difficult for attackers to access valuable assets and information. Similarly, these barriers increase the time it takes for threat actors to successfully carry out acts of thievery, vandalism or terrorism. The more obstacles that are in place, the more time organizations have to respond to physical security threats and contain them.

But criminals are not the only threat that access controls can minimize. Barriers such as walls and fences can also be used to harden buildings against environmental disasters, such as earthquakes, mudslides and floods. These risks are extremely location-dependent. Organizations that divert resources toward such hardening measures should balance the cost and benefit of their implementation prior to investment.

2. Surveillance:

This is one of the most important physical security components for both prevention and post-incident recovery. Surveillance refers to the technology, personnel and resources that organizations use to monitor the activity of different real-world locations and facilities. These examples can include **patrol guards, heat sensors and notification systems**.

The most common type of surveillance is **Closed Circuit Television (CCTV) cameras** that record the activity of a combination of areas. The benefit of these surveillance cameras is that they are as valuable in capturing criminal behavior as they are in preventing it. Threat actors who see a CCTV camera are less inclined to break in or vandalize a building out of fear of having their identity recorded. Similarly, if a particular asset or piece of equipment is stolen, surveillance can provide the visual evidence one needs to identify the culprit and their tactics.

3. Testing:

Physical security is a preventative measure and incident response tool. **Disaster recovery (DR) plans**, for example, center on the quality of one's physical security protocols - how well a company identifies, responds to and contains a threat. The only way to ensure that such DR policies and procedures will be effective when the time comes is to implement active testing.

Testing is increasingly important, especially when it comes to the unity of an organization. Fire drills are a necessary activity for schools and buildings because they help to coordinate large groups, as well as their method of response. These policy tests should be conducted on a regular basis to practice role assignments and responsibilities and minimize the likelihood of mistakes.

Importance of physiacl security:

As businesses become more dependent on the internet of things (IoT), so does the need for digital and physical security. IoT demands a significant amount of physical security to safeguard data, servers and networks. The rising interconnectedness of IoT has expanded the sphere of physical security. Virtual machines (VMs) and applications that run in the cloud, for example, are only as protected as their physical servers. Whether organizations invest in first-party or third-party cloud computing services, these data centers need to be sufficiently protected using physical security measures to avoid severe data losses.

Physical security examples:

Physical security can take many shapes and forms. The strategies, barriers and techniques that organizations use to support general physical information technology (IT) security are significantly different from those used to facilitate consistent physical network security. Here are a few physical security examples used to contain and control real-world threats.

1. Log and trail maintenance:

Keeping a record of what is accessed and what people attempt to access is a reliable way to not only discourage unauthorized users, but create a forensic-friendly data environment. Multiple failed login attempts and attempted access using a lost card are both physical security tools that organizations can use to reliably track their asset activity. In the case of a security breach, these records can prove incredibly valuable for identifying security weaknesses.

2. Risk - based approach:

One of the most effective ways to optimize a physical security investment is to use a risk-based approach. This is a data analysis technique used to evaluate scenarios based on one's risk profile. If a business is particularly risk-averse, it will opt to invest in a more expensive physical security system that is more equipped to mitigate risk. Therefore, the amount of resources a company dedicates to its physical security using a risk-based approach should be equivalent to the value it places on risk mitigation.

3. <u>Accountable access control</u>:

By tying access control to individuals, an organization can improve its visibility over personnel activity. For example, imagine if a particular room can only be accessed by a single key, and that key is given to two people. If an asset in that room goes missing, then only those two people are accountable for its disappearance.

<u>Recommendations to protect digital assets</u>:

The NJCCIC (New Jersey Cybersecurity & Communications Integration Cell) recommends users apply cybersecurity best practices to protect their digital assets and reduce the likelihood and impact of attack.

- **Lock screens -** When stepping away from the computer or device, the manual lock function helps to protect the information stored on or accessible from the computer. Also, check security settings or policies to automatically lock screens after inactivity.
- **Secure physical devices -** Safeguard devices and ensure a password / passcode or an additional authentication factor is enabled for all devices to prevent unauthorized access in the event a device is lost or stolen, or USB or external device is inserted.
- **Check privacy and security settings -** Checking these settings will help manage cyber risk and limit how and with whom one share information. This will help safeguard information or resources if an unauthorized user gains access.
- **Cover or disconnect camera when not in use.** Covering or disconnecting webcam and microphone when not in use prevents malware from taking control of the camera to spy on the person and his surroundings. Additionally, when the camera is in use, ensure no sensitive information is visible.
- **Backup devices -** Protect information from malware, hardware failure, damage, loss, or theft by making multiple copies and storing them offline.
- **Keep devices up to date -** Stay informed about publicly-disclosed vulnerabilities and update devices including firmware to the latest version to ensure they are patched against known vulnerabilities that could be exploited by threat actors to gain unauthorized access to your device and/or data. If a device is unable to receive updates from the vendor, consider not purchasing or discontinuing use of the device.

- **Implement protective technologies -** IT departments are advised to implement endpoint detection and response software, host-based firewalls, device and file encryption, and keep devices updated with latest security patches.
- **Remediate compromised and/or stolen devices -** It is important to monitor logs for signs of access and exfiltration. When practical, wipe and reimage hard drives. Also, utilize remote administration and data wiping solutions to regain control of devices if they cannot be physically accessed.
- **Use unique, complex passwords for all accounts -** Unique passwords for each account prevent password reuse attacks, in which threat actors obtain your password for one account and use it to compromise an additional account using the same credentials.
- **Enable multi-factor authentication (MFA) -** MFA is the use of two or more factors to authenticate to an account or service. This significantly reduces the risk of account compromise via credential theft in which your password has been exposed. Even if a cybercriminal obtains a user's username and password, they will be unable to access that user's account without their second factor.
- **Refrain from sharing login credentials or other sensitive information -** Login credentials and other sensitive information should not be shared with anyone, posted in plain view, or saved on your computer or other platforms.
- **Exercise caution with communications -** Before providing sensitive information, confirm the legitimacy of the message or request via a separate means of communication such as telephone obtained directly from official websites or welcome emails.
- **Navigate directly to websites -** Navigate directly to authentic or official websites by typing the legitimate URL into the browser instead of clicking on links in messages, and refrain from entering login credentials on websites visited via links delivered in messages.
- **Use secure websites -** When sharing personal or financial information, ensure you are using verified, secure, and encrypted websites.
- **Update passwords immediately following a data breach or potential compromise -** Often check, if your information, such as an account password, has been revealed in a public data breach. Change exposed passwords for every account that uses it to protect against account compromise.
- **Invest in security awareness training -** Invest the time, money, and resources to ensure users understand risks, the latest cyber threats, and best practices.
- **Implement strategies for emergency situations -** It is important to implement strategies for leaving workstations and IT infrastructure behind in the event of sudden evacuations or when human life is at risk. The strategy may include planning and tabletop exercises, preparation and training, and monitoring.