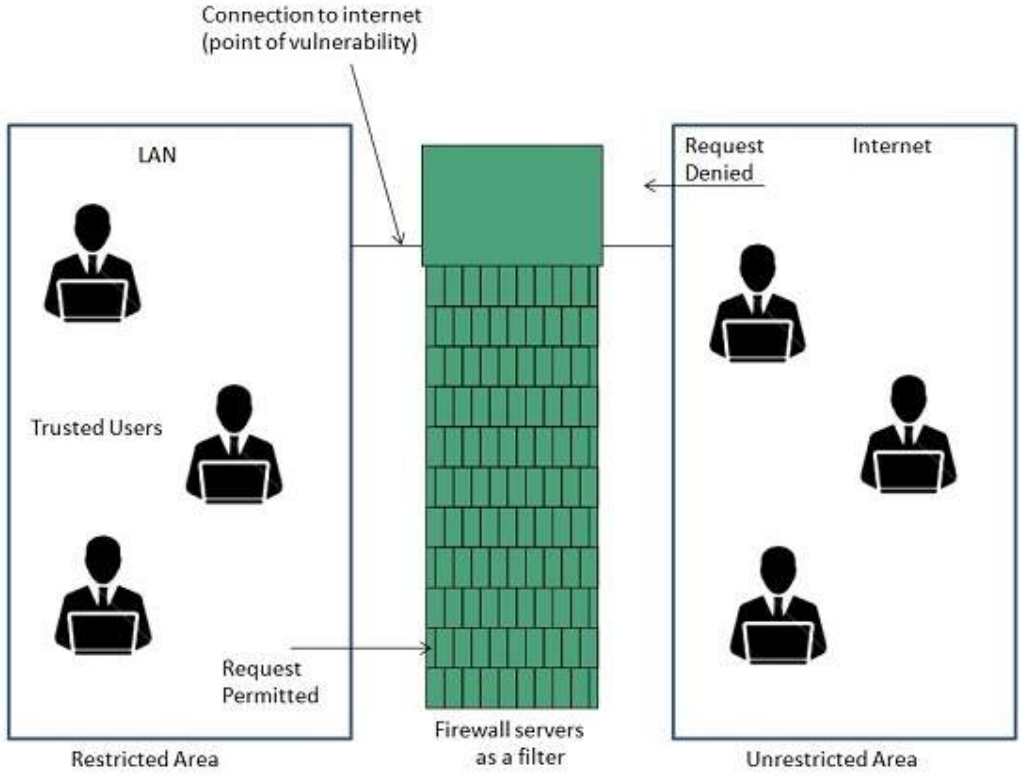
UNIT - 5

FIREWALL

Firewall is a barrier between Local Area Network (LAN) and the Internet. It allows keeping private resources confidential and minimizes the security risks. It controls network traffic, in both directions.

The following diagram depicts a sample firewall between LAN and the internet. The connection between the two is the point of vulnerability. Both hardware and the software can be used at this point to filter network traffic.



There are two types of Firewall system: One works by using filters at the network layer and the other works by using proxy servers at the user, application, or network layer.

Key Points

- Firewall management must be addressed by both system managers and the network managers.
- The amount of filtering a firewall varies. For the same firewall, the amount of filtering may be different in different directions.

PACKET FILTERING FIREWALL

Packet-filtering firewalls operate at the network layer (Layer 3) of the OSI model. Packet-filtering firewalls make processing decisions based on network addresses, ports, or protocols.

Packet-filtering firewalls are very fast because there is not much logic going behind the decisions they make. They do not do any internal inspection of the traffic. They also do not store any state information. You have to manually open ports for all traffic that will flow through the firewall.

Packet-filtering firewalls are considered not to be very secure. This is because they will forward any traffic that is flowing on an approved port. So there could be malicious traffic being sent, but as long as it's on an acceptable port, it will not be blocked.

Packet-filtering firewalls

Packet-filtering firewalls provide a way to filter IP addresses by either of two basic methods:

1.Allowing access to known IP addresses

2.Denying access to IP addresses and ports

By allowing access to known IP addresses, for example, you could allow access only to recognized, established IP addresses, or, you could deny access to all unknown or unrecognized IP addresses.

By denying access to IP addresses or ports, for example, you could deny access to port 80 to outsiders. Since most HTTP servers run on port 80, this would in effect block off all outside access to the HTTP server.

According to a report by CERT, it is most beneficial to utilize packet filtering techniques to permit only approved and known network traffic to the utmost degree possible. The use of packet filtering can be a very cost-effective means to add traffic control to an already existing router infrastructure.

IP packet filtering is accomplished by all firewalls in some fashion. This is normally done through a packet-filtering router. The router will filter or screen packets traveling through the router's interfaces that are operating under the firewall policy established by the enterprise. A packet is a piece of information that is being transmitted over the network. The packet filtering router will examine the path the packet is taking and the type of information contained in the packet. If the packet passes the firewall policy's tests, it is permitted to continue on its path. The information the packet filtering router looks for includes (1) the packet source IP address and source TCP/UDP port, and (2) the destination IP address and destination TCP/UDP port of the packet.

Packet filter firewalls have several advantages that explain why they are commonly used:

- **Packet filters are very efficient.** They hold up each inbound and outbound packet for only a few milliseconds while they look inside the packet to determine the destination and source ports and addresses. After these addresses and ports are determined, the packet filter quickly applies its rules and either sends the packet along or rejects it. In contrast, other firewall techniques have a more noticeable performance overhead.
- **Packet filters are almost completely transparent to users.** The only time a user will be aware that a packet filter firewall is being used is when the firewall rejects packets. Other firewall techniques require that clients and/or servers be specially configured to work with the firewall.
- **Packet filters are inexpensive.** Most routers include built-in packet filtering.

BASIC SECURITY PROBLEMS

Most businesses are aware that a spam filter and antivirus program are not all they need to protect themselves from the constantly evolving landscape of cybersecurity threats. Knowing just what a comprehensive security stance entails, however, is far less obvious. Comprehensive web security includes a full suite of tools to protect against malware infections, data breaches, and service disruptions. It protects the server, network, and email system. It includes advanced technologies like a web application firewall and involves proactive steps like vulnerability scanning.

But what do you do when something goes wrong? A click on the wrong email that leads to malware or a plug-in vulnerability that leads to a hacked webpage means that preventative measures are not enough, in that particular case. In order to minimize the damage caused by a security breach, a proactive web security stance has to be adopted ahead of time, including services and tools for mitigation, and a disaster recovery plan.

A major but often overlooked part of comprehensive cybersecurity protection is a remediation service. There is never time during a cybersecurity incident to search out an effective malware removal tool, for instance.

Organizational preparation is another important part of a complete, proactive cybersecurity posture. That means having the right tools, but also maintaining a minimum threshold of threat awareness. To assist with that awareness, consider the list below of the top five most common web security problems faced by businesses, and how to fix them.

1. Code Injection

Hackers are sometimes able to exploit vulnerabilities in applications to insert malicious code. Often the vulnerability is found in a text input field for users, such as for a username, where an SQL statement is entered, which runs on the database, in what is known as an SQL Injection attack. Other kinds of code injection attacks include shell injection, operating system command attacks, script injection, and dynamic evaluation attacks.

Attacks of this type can lead to stolen credentials, destroyed data, or even loss of control over the server. They are also surprisingly common, as the OWASP (Open Web Application Security Project) Foundation ranks code injection first in its Top 10 Application Security Risks.

There are two ways to prevent code injection: avoiding vulnerable code and filtering input. Applications can guard against vulnerable code by keeping data separate from commands and queries, such as by using a safe API with parameterized queries. Businesses should also use input validation, and observe the principle of least privilege, applying controls like the SQL LIMIT function to reduce the damage from a successful attack. A Web Application Firewall (WAF) which updates a threat database in real-time is the only effective way to filter application input to protect against code injection.

2. Data Breach

The cost of data breaches is well documented. They are often caused by compromised credentials, but the range of other common causes include software misconfiguration, lost hardware, or malware (more on that below). The Breach Level Index indicates there were 944 known data breaches in the first half of 2018 and nearly 2,000 in 2017.

Data breach prevention requires a range of good practices. Site traffic and transactions should be encrypted with SSL, permissions should be carefully set for each group of users, and servers should be scanned. Employees should be trained in how to avoid being caught by phishing attacks, and how to practice good password hygiene. The principle of least privilege is worth noting here, as well.

In the event that your business discovers a potential data breach, you may face legal or compliance requirements for notifying customers or regulatory authorities. Disclosure requirements and strategies should be determined ahead of time so that the maximum amount of organizational resources can be dedicated to making sure that no more data is stolen as well as repairing the damage caused. Once the attack vector has been blocked, a comprehensive incident investigation should be conducted, and the network scanned to make sure all vulnerabilities have been identified and closed off.

3. Malware Infection

Most businesses are aware on some level of the security threat posed by malware, yet many people are unaware that email spam is still the main vector of malware attack.

Because malware comes from a range of sources, several different tools are needed for preventing infection. A robust email scanning and filtering system is necessary, as are malware and vulnerability scans. Like breaches, which are often caused by malware infection, employee education is vital to keep businesses safe from malware.

Any device or system infected with malware must be thoroughly scrubbed, which means identifying the hidden portions of code and deleting all infected files before they replicate. This is practically impossible by hand, so requires an effective automated tool.

4. Distributed Denial of Service Attack

A Distributed Denial of Service (DDoS) attack generally involves a group of computers being harnessed together by a hacker to flood the target with traffic.

A NETSCAPE Arbor report suggested there were 7.5 million DDoS attacks in 2017, so while many target IT service providers, they are still more prevalent than many people realize. One of the most worrying aspects of DDoS attacks for businesses is that without even being targeted, the business can be affected just by using the same server, service provider, or even network infrastructure.

If your business is caught up in a DDoS attack, put your disaster recovery plan into effect, and communicate with employees and customers about the disruption. A security tool such as a WAF is used to close off the port or protocol being saturated, in a process which will likely have to be repeated as attackers adjust their tactics.

Ultimately, service is best restored with a content distribution network (CDN) like CloudFlare, which can absorb an enormous impact while identifying and then filtering out malicious traffic. Make sure to also look for DDoS protection with real-time monitoring for comprehensive mitigation of attacks.

Preventing damage from insider attacks is largely about limiting the amount of access a malicious insider has. This means setting logical access control policies to implement the principle of least privilege (but you have that covered by now, right?), and monitoring the network with audit and transaction logs. A solution like Liquid Web's custom Malicious Activity Detector (MAD) will also guard against threats both from within and outside the organization.

If a malicious insider attack is detected, the insider's access privileges should immediately be revoked. That done, the police should be contacted to prevent that person from carrying out further actions that could damage the business, such as selling stolen data.

5. Malicious Insiders

This last threat is uncomfortable to think about, but common enough to require serious consideration, as the 2017 U.S. State of Cybercrime Highlights report from CERT shows that one in five attacks are committed by insiders.

ROUTING

Routing is the process of selecting a path for traffic in a network or between or across multiple networks. Broadly, routing is performed in many types of networks, including circuit-switched networks, such as the public switched telephone network (PSTN), and computer networks, such as the Internet.

In packet switching networks, routing is the higher-level decision making that directs network packets from their source toward their destination through intermediate network nodes by specific packet forwarding mechanisms. Packet forwarding is the transit of network packets from one network interface to another. Intermediate nodes are typically network hardware devices such as routers, gateways, firewalls, or switches.

General-purpose computers also forward packets and perform routing, although they have no specially optimized hardware for the task.

The routing process usually directs forwarding on the basis of routing tables. Routing tables maintain a record of the routes to various network destinations. Routing tables may be specified by an administrator, learned by observing network traffic or built with the assistance of routing protocols.

Routing, in a narrower sense of the term, often refers to IP routing and is contrasted with bridging. IP routing assumes that network addresses are structured and that similar addresses imply proximity within the network. Structured addresses allow a single routing table entry to represent the route to a group of devices. In large networks, structured addressing (routing, in the narrow sense) outperforms unstructured addressing (bridging). Routing has become the dominant form of addressing on the Internet. Bridging is still widely used within local area networks.

Types of Routing

Routing is a process which is performed by layer 3 (or network layer) devices in order to deliver the packet by choosing an optimal path from one network to another.

There are 3 types of routing:

1. Static routing –

Static routing is a process in which we have to manually add routes in routing table.

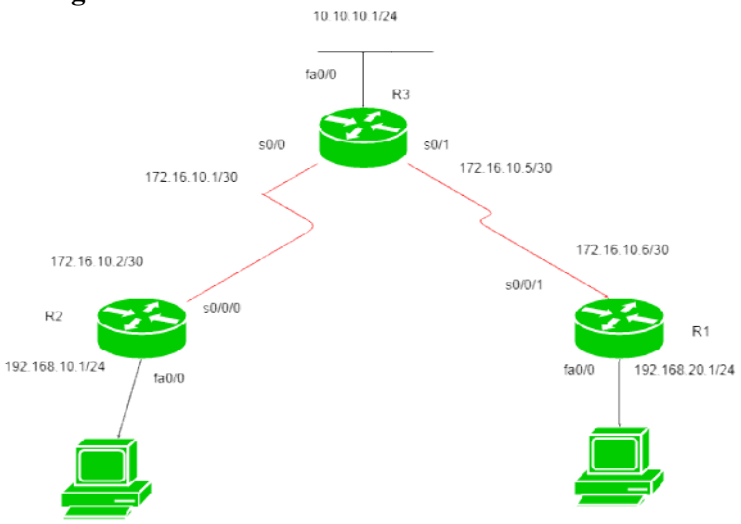
Advantages –

- No routing overhead for router CPU which means a cheaper router can be used to do routing.
- It adds security because only administrator can allow routing to particular networks only.
- No bandwidth usage between routers.

Disadvantage –

- For a large network, it is a hectic task for administrator to manually add each route for the network in the routing table on each router.
- The administrator should have good knowledge of the topology. If a new administrator comes, then he has to manually add each route so he should have very good knowledge of the routes of the topology.

Configuration –



R1 having IP address 172.16.10.6/30 on s0/0/1, 192.168.10.1/24 on fa0/0.
R2 having IP address 172.16.10.2/30 on s0/0/0, 192.168.20.1/24 on fa0/0.
R3 having IP address 172.16.10.5/30 on s0/1, 172.16.10.1/30 on s0/0, 10.10.10.1/24 on fa0/0.

Now configuring static routes for router R3:

```
R3(config)#ip route 192.168.10.0 255.255.255.0 172.16.10.2
R3(config)#ip route 192.168.20.0 255.255.255.0 172.16.10.6
```

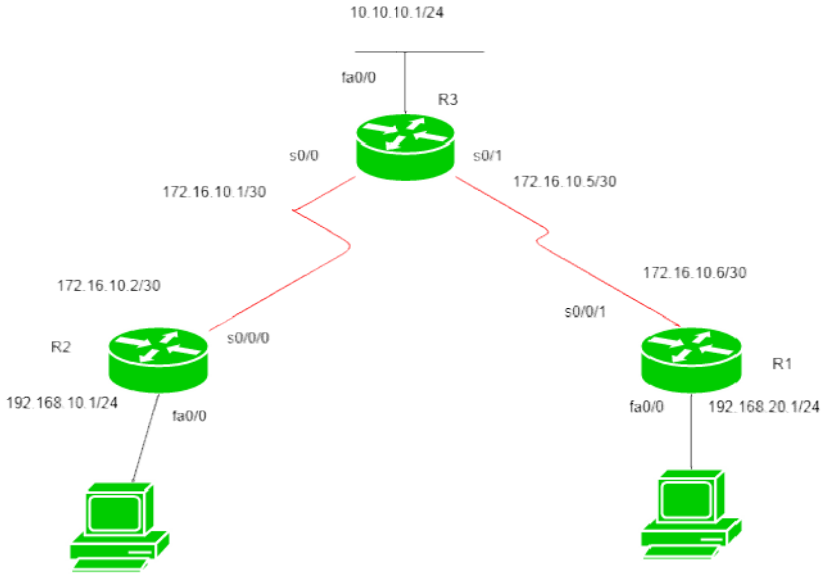
Here, provided the route for 192.168.10.0 network where 192.168.10.0 is its network I'd and 172.16.10.2 and 172.16.10.6 are the next hop address.
Now, configuring for R2:

```
R2(config)#ip route 192.168.20.0 255.255.255.0 172.16.10.1
R2(config)#ip route 10.10.10.0 255.255.255.0 172.16.10.1
R2(config)#ip route 172.16.10.4 255.255.255.0 172.16.10.1
```

Similarly for R1:

```
R1(config)#ip route 192.168.10.0 255.255.255.0 172.16.10.5
R1(config)#ip route 10.10.10.0 255.255.255.0 172.16.10.5
R1(config)#ip route 172.16.10.0 255.255.255.0 172.16.10.5
```

2. Default Routing –
This is the method where the router is configured to send all packets towards a single router (next hop). It doesn't matter to which network the packet belongs, it is forwarded out to router which is configured for default routing. It is generally used with stub routers. A stub router is a router which has only one route to reach all other networks.
Configuration –
Using the same topology which we have used for the static routing before.



In this topology, R1 and R2 are stub routers so we can configure default routing for both these routers.
Configuring default routing for R1:

```
R1(config)#ip route 0.0.0.0 0.0.0.0  172.16.10.5
```

Now configuring default routing for R2:

```
R2(config)#ip route 0.0.0.0 0.0.0.0  172.16.10.1
```

3. Dynamic Routing –
Dynamic routing makes automatic adjustment of the routes according to the current state of the route in the routing table. Dynamic routing uses protocols to discover network destinations and the routes to reach it. RIP and OSPF are the best examples of dynamic routing protocol. Automatic adjustment will be made to reach the network destination if one route goes down.
A dynamic protocol have following features:

1. The routers should have the same dynamic protocol running in order to exchange routes.
2. When a router finds a change in the topology then router advertises it to all other routers.

Advantages –

- Easy to configure.
- More effective at selecting the best route to a destination remote network and also for discovering remote network.

Disadvantage –

- Consumes more bandwidth for communicating with other neighbors.
- Less secure than static routing.

ROUTING SECURITY

Routing security has received varying levels of attention over the past several years and has recently begun to attract more attention specifically around Border Gateway Protocol (BGP) on the public Internet. Despite this new attention, however, the area most open to attack is often not the Internet's BGP tables but the routing systems within your own enterprise network. Because of some of the sniffing-based attacks, an enterprise routing infrastructure can easily be attacked with man-in-the-middle and other attacks designed to corrupt or change the routing tables with the following results:

- **Traffic redirection**—In this attack, the adversary is able to redirect traffic, enabling the attacker to modify traffic in transit or simply sniff packets.
- **Traffic sent to a routing black hole**—Here the attacker is able to send specific routes to null0, effectively kicking IP addresses off of the network.
- **Router denial-of-service (DoS)**—Attacking the routing process can result in a crash of the router or a severe degradation of service.

- **Routing protocol DoS**—Similar to the attack previously described against a whole router, a routing protocol attack could be launched to stop the routing process from functioning properly.
- **Unauthorized route prefix origination**—This attack aims to introduce a new prefix into the route table that shouldn't be there. The attacker might do this to get a covert attack network to be routable throughout the victim network.

WEAKNESS OF INTERNET SECURITY

Internet users should identify weaknesses of internet security in their information system security and outlined areas where they are most prone to be hacked. Weaknesses of internet security can be classified as internal factors that affect the security of the internet. Mostly weakness of internet security originates from the violations of security information system by employees. For the past twenty years, information system theft by the employee has been evidenced in many companies, and institution others have been able to transfer faulty information protocols.

This has been achieved since most employees are trusted and able to access most of the firm credentials logins whom whoever turns to be opposite. Furthermore, inadequate capital to fund internet security system has become a significant weakness of internet security.

For example, most corporations are unable to purchase privacy and security tools which offers maximum protection security while connected to the internet.

Despite this, they usually opt to buy relatively cheap and mostly free security tools, i.e., antivirus software such as Kaspersky internet antivirus that is expensive. Besides, with inadequate capital corporations are unable to hire skilled technicians to monitor and ensure maximum security of the internet and properly fix any attack discovered.

1.Internet security opportunities

2.Internet security threats

3.Evaluation of the current ethical and legal concerns surrounding internet security

4.Improvements of internet security over the last two years

5.Suggestion for improvement of internet security based on the current internet security issues.

6.Future prediction of internet security

INTRUSION DETECTION SYSTEM

- Process of tracking the activities that are being performed in the network. This tack of monitoring the activities on the network can be assigned to single or multiple

computers present inside the network (computer that is monitoring must always be kept on and backups)
- IDS used for tracking the user's activities (site visiting, time of visiting, URL and etc.)

Types of IDS:

a. Network Based IDS
- It captures the network traffic to perform Intrusion detection operation
- NIDS scans the network packets. Inspects the packet information and finds any unexpected packets.

Some of the threats and activities that can be controlled by using an NIDS are:

- IP Spoofing
- Dos Attack
- Man in the Middle attack

Control Mechanisms in the NIDS:

There are two types of control Mechanisms: Distributed and Centralized

a. Distributed: Information about the attack stored inside the database is being distributed to every node present in the network.
b. Centralized: the information about the attack present in the various IDSs is analyzed and processed by a central entity.

location of NIDS

If it is located In front of the firewall, it monitors all the data going into the network , resulting in processing of large amount of data and becomes bottleneck. However, if it is located behind the firewall, it only allows NIDS to process the data that penetrates the firewall.

Types of Responses: Active and Passive

Passive: Notifies the administrator about the threat using passive strategies which are:

- **Logging:** Records an event and the circumstances of its occurrence. It provides sufficient information about the nature of the attack.
- **Notification:** Communicate attack related information to the appropriate personal, when an event takes place.
- **Shunning:** Activity of avoiding the attack.

Active: When a System is threatened by some potential attack, the active response takes the immediate possible action required to decrease the impact of the attack. some examples are shown below:

- **Terminating processes or sessions:** Terminates all the unauthorized processes and sessions that are trying to gain the access to the system.
- **Network configuration changes:** Instructs the firewall or router to reject any request or traffic coming from a particular port that is being attacked.

- **Deception:** fools the attacker and redirects them to a system that is designed to be broken. it helps in gathering data about how the attack is planned and what techniques are used in the attack.

Advantages of using NIDS

a. Lower cost of ownership
b. Detects the malicious packets missed by the firewall
c. Analyze the payload of the packet
d. Real-time detection and response

b. Host - Based IDS:

- It is designed to monitor, detect and respond to activities and attacks on a given host. In other words, it is used to monitor the packets (incoming as well as outgoing traffic) from the device and alerts the user or administrator of any unexpected activity.
- HIDS performs various functions such as filtering, analyzing records
- Data integrity of the important files can be verified by HIDS.
- Provides an effective mechanism for detecting outside attacks
- Monitors users actions

HIDS can detects the attacks through: Signature based IDS or Statistical anomaly based IDS

1. Signature based IDS/ Knowledge based IDS:

- Contains a database of recognized attacks.
- Activity is compared with the data present inside the database
- Sounds an alarm for suspicious activity.

Advantages:

- Easy to implement, update and deploy
- Usage time is short as there is no need to learn network behavior

Disadvantage:

- Static in nature
- Signature Based IDS may sound alarms for normal activities that just might look unexpected
- If it is a new attack that is not present inside the database, that attack may very well totally ignored and not even care about it.

2. Statistical anomaly based IDS/ Observation based IDS:

- It has to sample normal activity and keep a record or an idea of what a normal activity looks like. Anything systems finds outside the record it triggers on an alarm.
- Dynamically detects deviations arising from the behavior of the user and accordingly triggers an alarm.
- sometimes called Expert system because the more it runs, the more it learns.

Advantages:

- Dynamic in Nature
- less dependent on OS

Disadvantages:

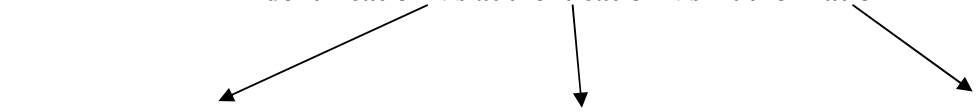
- It generates high false alarm rates
- it might incorrectly detect a non-attack event that caused a movementary action in the system.

UNDERSTANDING ACCESS CONTROL

Access Control is a security feature through which the system permits or deny the right to access the data and resource in a system. it includes:

- **File Permissions:** refers to the access control in which the user can create, read, edit or delete on a file server.
- **Program permissions:** refers to the access control in which the user can execute a program on an application. Example: Running a Whatapp application
- **Data rights permissions:** refers to the access control in which the user can retrieve or update information in a database.

Identification Vs authentication Vs Authorization



process of recognizing a user access

process of verifying whether the user is a valid user or not

the permission to a resource

for to access network resources and information, the user needs to provide his/her credentials(details) to a network. which identifies the user. if the user credentials(details) are correct, the user gains the access to the network resources else rejected.

Single Rule- Based factor (SFA) authentication

SFA implements authentication by using the combination of username & password. In the login process, the username and passwords are used as a unique identifier.

- the information (username & password) is passed to server either as a plain text form or in an encrypted form
- the client needs to prove its identity to a server, and the server needs to prove its identity to the client before any data communication on the client-server connection. it is called mutual authentication.

Multi factor authentication (MFA)

- Authentication process that contains 2 or more access methods is called MFA.
  Example: for to do online transaction using net banking there is a need of account password and OTP number.
- A system that uses smart card and password as authentication is called two-factor authentication system.

Discretionary Access Control (DAC)

DAC offers flexibility related to the exchange of information to the network users. Even though DAC offering flexible environment, unauthorized information leakage is always the likely possibility. Administrators struggle in the face of ensuring control over information access and grant of access rights. The permission set in the Unix/Linux environment has been classified into 3 groups of user, i.e., Owner, group, and others. Role plays an important role in accessing the information.

Role-Based Access Control (RBAC)
RBAC models put control over the information access from the viewpoint of organizational roles. Access to a specific information totally depends on the role of that particular user inside the organization.

Rule-Based Access Control
The Decision making is dependent on the rules that have been saved into security policies. These rules allow access to some people appearing in a allowing list while deny the people not appearing. Example: Username and Password.

DOMAIN NAME SYSTEM

The Domain Name System (DNS) is the phonebook of the Internet. Humans access information online through domain names, like nytimes.com or espn.com. Web browsers interact through Internet Protocol (IP) addresses. DNS translates domain names to IP addresses so browsers can load Internet resources.

Each device connected to the Internet has a unique IP address which other machines use to find the device. DNS servers eliminate the need for humans to memorize IP addresses such as 192.168.1.1 (in IPv4), or more complex newer alphanumeric IP addresses such as 2400:cb00:2048:1::c629:d7a2 (in IPv6).

How does DNS work?

The process of DNS resolution involves converting a hostname (such as www.example.com) into a computer-friendly IP address (such as 192.168.1.1). An IP address is given to each device on the Internet, and that address is necessary to find the appropriate Internet device - like a street address is used to find a particular home. When a user wants to load a webpage, a translation must occur between what a user types into their web browser (example.com) and the machine-friendly address necessary to locate the example.com webpage.

In order to understand the process behind the DNS resolution, it's important to learn about the different hardware components a DNS query must pass between. For the web browser, the DNS lookup occurs " behind the scenes" and requires no interaction from the user's computer apart from the initial request.

There are 4 DNS servers involved in loading a webpage:

- *DNS recursor* - The recursor can be thought of as a librarian who is asked to go find a particular book somewhere in a library. The DNS recursor is a server designed to receive queries from client machines through applications such as web browsers. Typically the recursor is then responsible for making additional requests in order to satisfy the client's DNS query.
- *Root nameserver* - The root server is the first step in translating (resolving) human readable host names into IP addresses. It can be thought of like an index in a library

that points to different racks of books - typically it serves as a reference to other more specific locations.

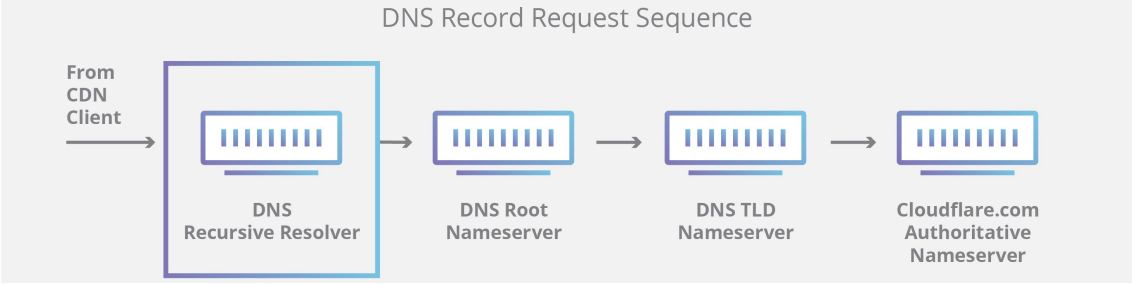
- *TLD nameserver* - The top level domain server (TLD) can be thought of as a specific rack of books in a library. This nameserver is the next step in the search for a specific IP address, and it hosts the last portion of a hostname (In example.com, the TLD server is “com”).
- *Authoritative nameserver* - This final nameserver can be thought of as a dictionary on a rack of books, in which a specific name can be translated into its definition. The authoritative nameserver is the last stop in the nameserver query. If the authoritative name server has access to the requested record, it will return the IP address for the requested hostname back to the DNS Recursor (the librarian) that made the initial request.

What's the difference between an authoritative DNS server and a recursive DNS resolver?

Both concepts refer to servers (groups of servers) that are integral to the DNS infrastructure, but each performs a different role and lives in different locations inside the pipeline of a DNS query. One way to think about the difference is the recursive resolver is at the beginning of the DNS query and the authoritative nameserver is at the end.

Recursive DNS resolver

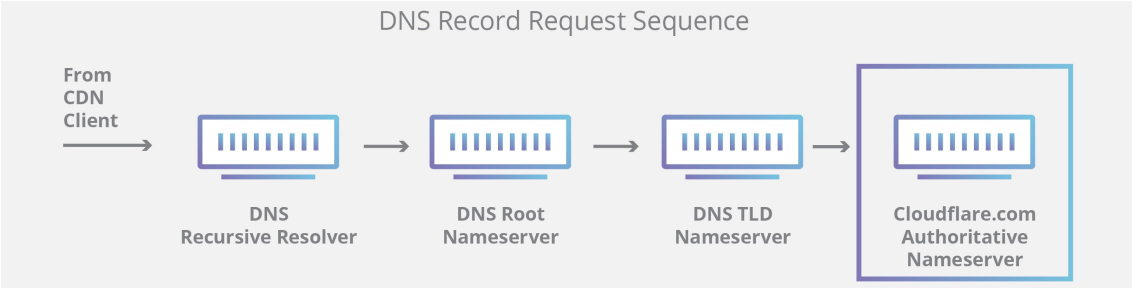
The recursive resolver is the computer that responds to a recursive request from a client and takes the time to track down the DNS record. It does this by making a series of requests until it reaches the authoritative DNS nameserver for the requested record (or times out or returns an error if no record is found). Luckily, recursive DNS resolvers do not always need to make multiple requests in order to track down the records needed to respond to a client; caching is a data persistence process that helps short-circuit the necessary requests by serving the requested resource record earlier in the DNS lookup.



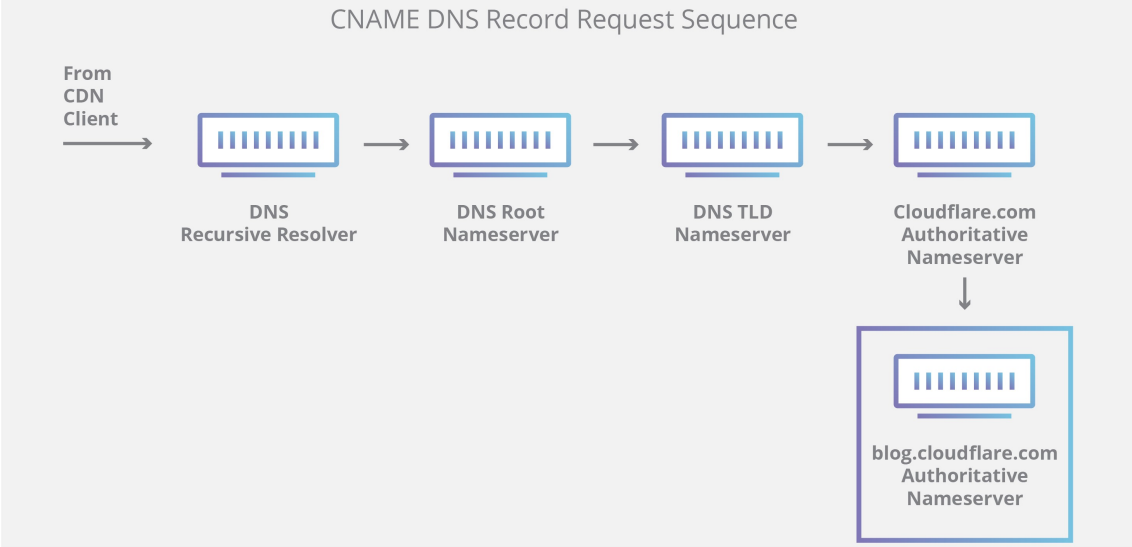
Authoritative DNS server

Put simply, an authoritative DNS server is a server that actually holds, and is responsible for, DNS resource records. This is the server at the bottom of the DNS lookup chain that will respond with the queried resource record, ultimately allowing the web browser making the request to reach the IP address needed to access a website or other web resources. An

authoritative nameserver can satisfy queries from its own data without needing to query another source, as it is the final source of truth for certain DNS records.



It's worth mentioning that in instances where the query is for a subdomain such as foo.example.com or blog.cloudflare.com, an additional nameserver will be added to the sequence after the authoritative nameserver, which is responsible for storing the subdomain's CNAME record.



What are the steps in a DNS lookup?

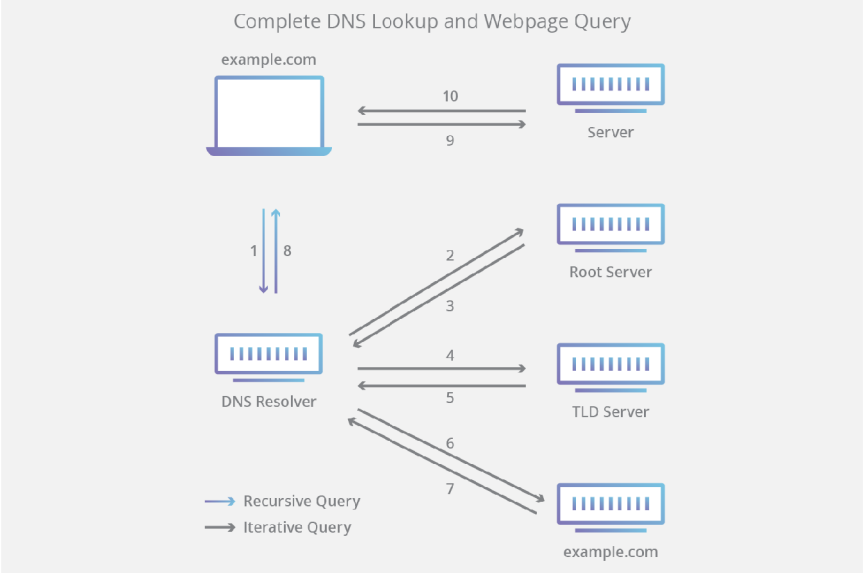
For most situations, DNS is concerned with a domain name being translated into the appropriate IP address. To learn how this process works, it helps to follow the path of a DNS lookup as it travels from a web browser, through the DNS lookup process, and back again. Let's take a look at the steps.

Note: Often DNS lookup information will be cached either locally inside the querying computer or remotely in the DNS infrastructure. There are typically 8 steps in a DNS lookup. When DNS information is cached, steps are skipped from the DNS lookup process which makes it quicker. The example below outlines all 8 steps when nothing is cached.

The 8 steps in a DNS lookup:

1. A user types ‘example.com’ into a web browser and the query travels into the Internet and is received by a DNS recursive resolver.
2. The resolver then queries a DNS root nameserver (.).
3. The root server then responds to the resolver with the address of a Top Level Domain (TLD) DNS server (such as .com or .net), which stores the information for its domains. When searching for example.com, our request is pointed toward the .com TLD.
4. The resolver then makes a request to the .com TLD.
5. The TLD server then responds with the IP address of the domain’s nameserver, example.com.
6. Lastly, the recursive resolver sends a query to the domain’s nameserver.
7. The IP address for example.com is then returned to the resolver from the nameserver.
8. The DNS resolver then responds to the web browser with the IP address of the domain requested initially.

   Once the 8 steps of the DNS lookup have returned the IP address for example.com, the browser is able to make the request for the web page:
9. The browser makes a HTTP request to the IP address.
10. The server at that IP returns the webpage to be rendered in the browser (step 10).



WHAT IS DNS CACHE POISONING?

Imagine that, as a senior-year prank, high school seniors change out all the room numbers on their high school campus, so that the new students who don't know the campus layout yet will spend the next day getting lost and showing up in the wrong classrooms. Now imagine that

the mismatched room numbers get recorded in a campus directory, and students keep heading to the wrong rooms until someone finally notices and corrects the directory.

DNS cache poisoning is the act of entering false information into a DNS cache, so that DNS queries return an incorrect response and users are directed to the wrong websites. DNS cache poisoning is also known as 'DNS spoofing.' IP addresses are the 'room numbers' of the Internet, enabling web traffic to arrive in the right places. DNS resolver caches are the 'campus directory,' and when they store faulty information, traffic goes to the wrong places until the cached information is corrected. (Note that this does not actually disconnect the real websites from their real IP addresses.)

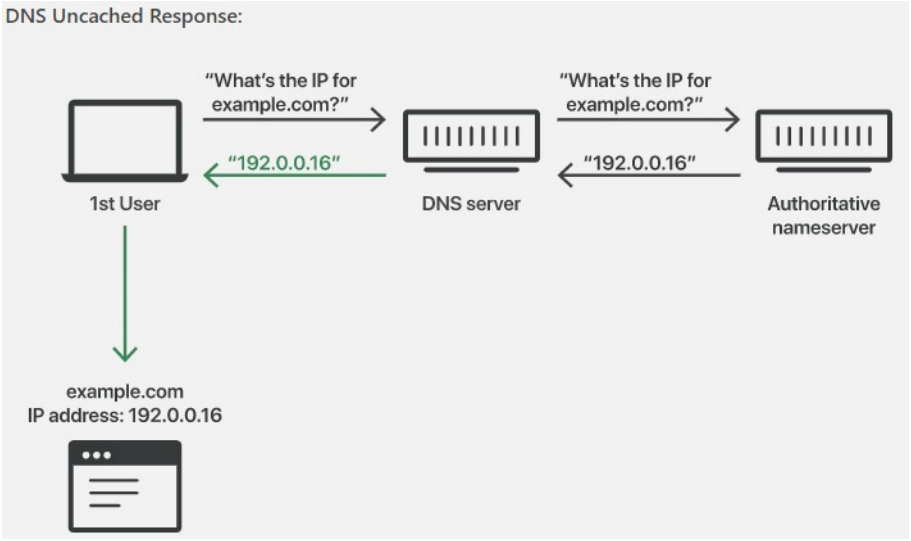
Because there is typically no way for DNS resolvers to verify the data in their caches, incorrect DNS information remains in the cache until the time to live (TTL) expires, or until it is removed manually. A number of vulnerabilities make DNS poisoning possible, but the chief problem is that DNS was built for a much smaller Internet and based on a principle of trust (much like BGP). A more secure DNS protocol called DNSSEC aims to solve some of these problems, but it has not been widely adopted yet.

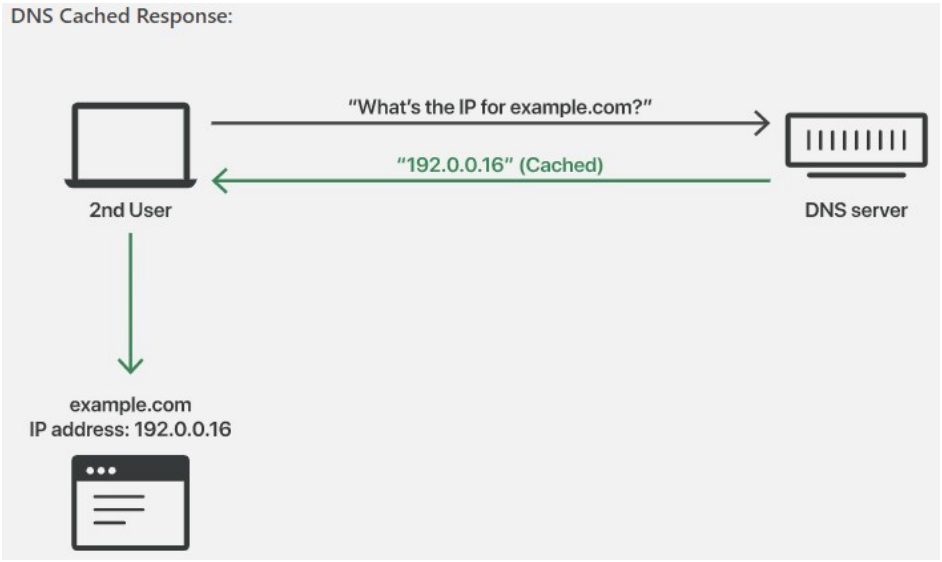
What do DNS resolvers do?

DNS resolvers provide clients with the IP address that is associated with a domain name. In other words, they take human-readable website addresses like 'cloudflare.com' and translate them into machine-readable IP addresses. When a user attempts to navigate to a website, their operating system sends a request to a DNS resolver. The DNS resolver responds with the IP address, and the web browser takes this address and initiates loading the website.

How does DNS caching work?

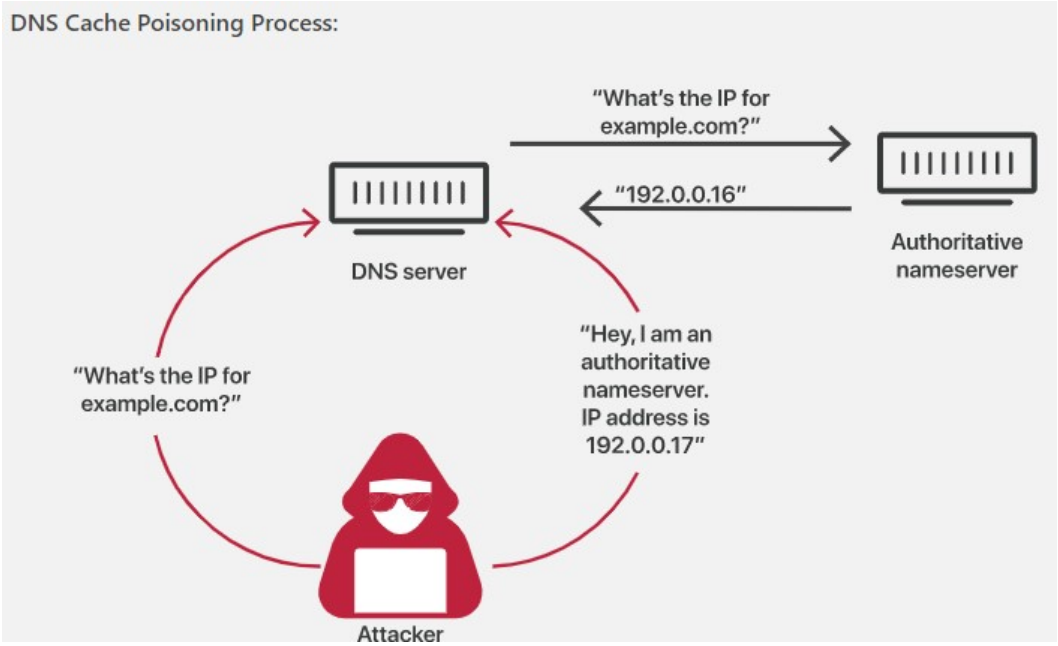
A DNS resolver will save responses to IP address queries for a certain amount of time. In this way, the resolver can respond to future queries much more quickly, without needing to communicate with the many servers involved in the typical DNS resolution process. DNS resolvers save responses in their cache for as long as the designated time to live (TTL) associated with that IP address allows them to.

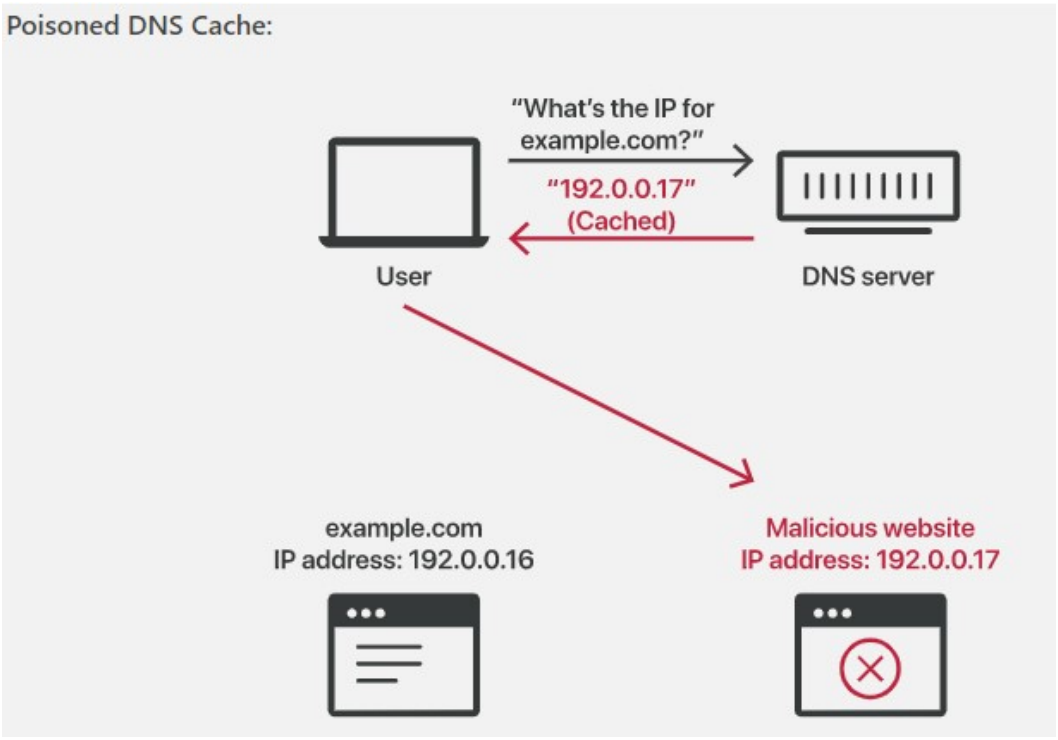




How do attackers poison DNS caches?

Attackers can poison DNS caches by impersonating DNS nameservers, making a request to a DNS resolver, and then forging the reply when the DNS resolver queries a nameserver. This is possible because DNS servers use UDP instead of TCP, and because currently there is no verification for DNS information.





Instead of using TCP, which requires both communicating parties to perform a 'handshake' to initiate communication and verify the identity of the devices, DNS requests and responses use UDP, or the User Datagram Protocol. With UDP, there is no guarantee that a connection is open, that the recipient is ready to receive, or that the sender is who they say they are. UDP is vulnerable to forging for this reason – an attacker can send a message via UDP and pretend it's a response from a legitimate server by forging the header data.

If a DNS resolver receives a forged response, it accepts and caches the data uncritically because there is no way to verify if the information is accurate and comes from a legitimate

source. DNS was created in the early days of the Internet, when the only parties connected to it were universities and research centers. There was no reason to expect that anyone would try to spread fake DNS information.

Despite these major points of vulnerability in the DNS caching process, DNS poisoning attacks are not easy. Because the DNS resolver does actually query the authoritative name server, attackers have only a few milliseconds to send the fake reply before the real reply from the authoritative name server arrives.

Attackers also have to either know or guess a number of factors to carry out DNS spoofing attacks:

- Which DNS queries are not cached by the targeted DNS resolver, so that the resolver will query the authoritative name server
- What port* the DNS resolver is using – they used to use the same port for every query, but now they use a different, random port each time
- The request ID number
- Which authoritative name server the query will go to

Attackers could also gain access to the DNS resolver in some other way. If a malicious party operates, hacks, or gains physical access to a DNS resolver, they can more easily alter cached data.

*In networking, a port is a virtual point of communication reception. Computers have multiple ports, each with their own number, and for computers to talk to each other, certain ports have to be designated for certain kinds of communication. For instance, HTTP communications always go to port 80, and HTTPS always uses port 443.

DNS spoofing and censorship

Several governments have intentionally poisoned DNS caches within their countries in order to deny access to certain websites or web resources.

LINK LAYER , NETWORK LAYER AND TCP/IP ARCHITECTURE

This lecture introduces the ISO-OSI layered architecture of Networks. According to the ISO standards, networks have been divided into 7 layers depending on the complexity of the fucntionality each of these layers provide. The detailed description of each of these layers is given in the notes below. We will first list the layers as defined by the standard in the increasing order of function complexity:

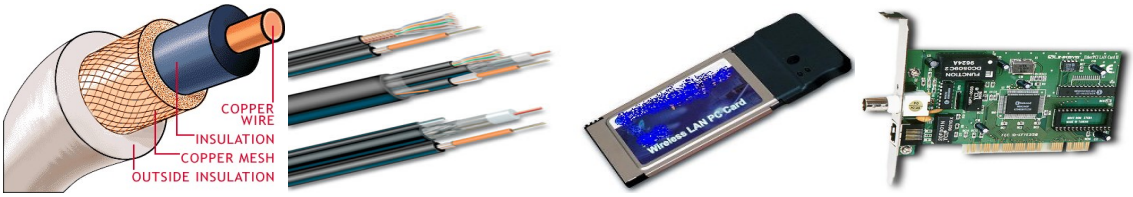
1. Physical Layer
2. Data Link Layer
3. Network Layer
4. Transport Layer
5. Session Layer
6. Presentation Layer
7. Application Layer

Physical Layer

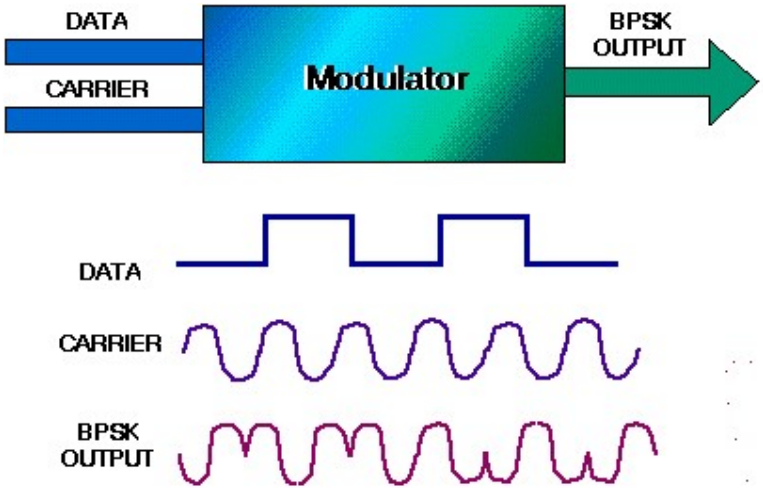
This layer is the lowest layer in the OSI model. It helps in the transmission of data between two machines that are communicating through a physical medium, which can be optical fibres,copper wire or wireless etc. The following are the main functions of the physical layer:

1. **Hardware Specification:** The details of the physical cables, network interface cards, wireless radios, etc are a part of this layer.

Coaxial Cable **Hybrid Cable** **Wireless Card** **Network Card**



2. **Encoding and Signalling:** How are the bits encoded in the medium is also decided by this layer. For example, on the coppar wire medium, we can use differnet voltage levels for a certain time interval to represent '0' and '1'. We may use +5mV for 1nsec to represent '1' and -5mV for 1nsec to represent '0'. All the issues of modulation is dealt with in this layer. eg, we may use Binary phase shift keying for the representation of '1' and '0' rather than using different volatage levels if we have to transfer in RF waves.



Binary Phase Shift Keying

3. **Data Transmission and Reception:** The transfer of each bit of data is the responsibility of this layer. This layer assures the transmissoin of each bit with a *high probability*. The transmission of the bits is not completely reliable as their is no error correction in this layer.
4. **Topology and Network Design:** The network design is the integral part of the physical layer. Which part of the network is the router going to be placed, where the switches will be used, where we will put the hubs, how many machines is each switch going to handle, what server is going to be placed where, and many such concerns are to be taken care of by the physical layer. The various kinds of topologies that we decide to use may be ring, bus, star or a hybrid of these topologies depending on our requirements.

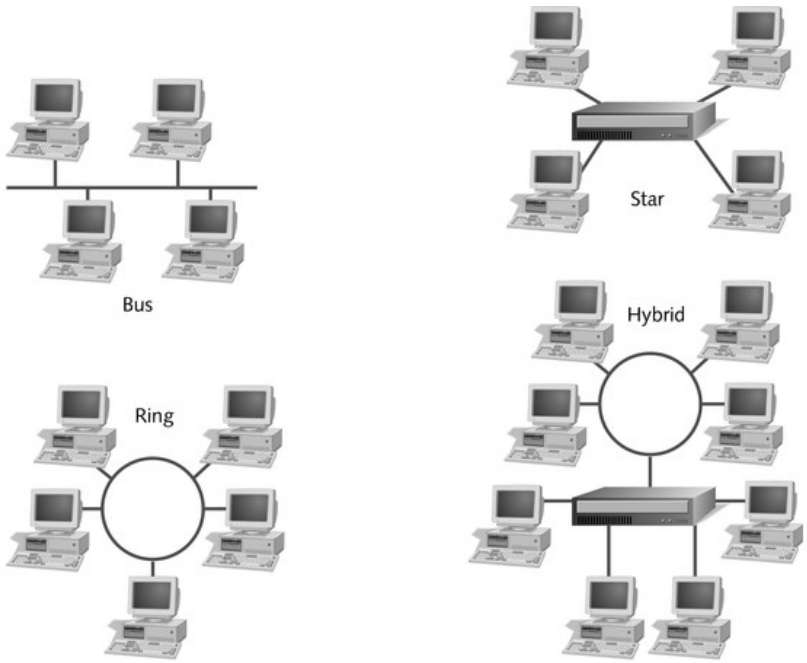


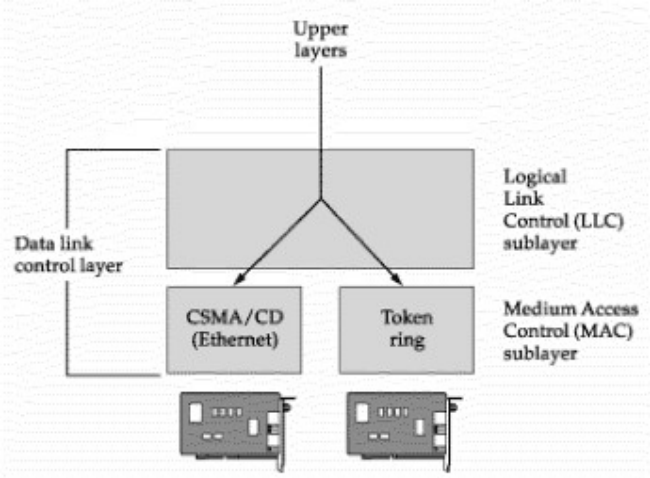
Figure 1-7 Commonly used network topologies

Data Link Layer

This layer provides reliable transmission of a packet by using the services of the physical layer which transmits bits over the medium in an unreliable fashion. This layer is concerned with :

1. Framing : Breaking input data into frames (typically a few hundred bytes) and caring about the frame boundaries and the size of each frame.
2. Acknowledgment : Sent by the receiving end to inform the source that the frame was received without any error.
3. Sequence Numbering : To acknowledge which frame was received.
4. Error Detection : The frames may be damaged, lost or duplicated leading to errors.The error control is on **link to link** basis.

5. Retransmission : The packet is retransmitted if the source fails to receive acknowledgment.
6. Flow Control : Necessary for a fast transmitter to keep pace with a slow receiver.

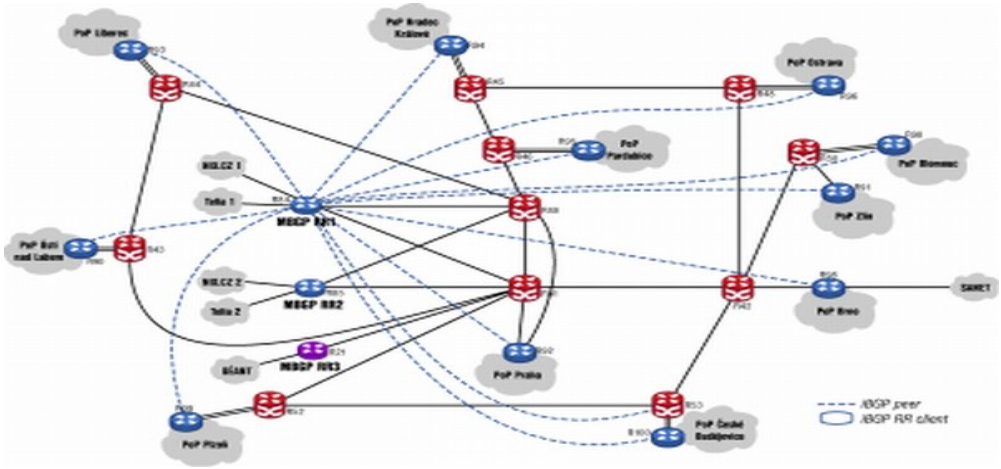


Data Link Layer

Network Layer

Its basic functions are routing and congestion control. **Routing:** This deals with determining how packets will be routed (transferred) from source to destination. It can be of three types :

- Static : Routes are based on static tables that are "wired into" the network and are rarely changed.
- Dynamic : All packets of one application can follow different routes depending upon the topology of the network, the shortest path and the current network load.
- Semi-Dynamic : A route is chosen at the start of each conversation and then all the packets of the application follow the same route.



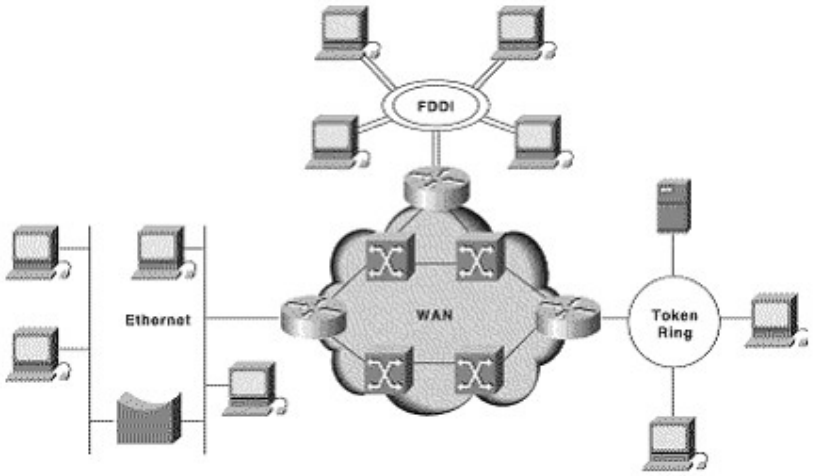
Routing

The services provided by the network can be of two types :

- **Connection less service:** Each packet of an application is treated as an independent entity. On each packet of the application the destination address is provided and the packet is routed.
- **Connection oriented service:** Here, first a connection is established and then all packets of the application follow the same route. To understand the above concept, we can also draw an analogy from the real life. Connection oriented service is modeled after the telephone system. All voice packets go on the same path after the connection is established till the connection is hung up. It acts like a tube ; the sender pushes the objects in at one end and the receiver takes them out in the same order at the other end. Connection less service is modeled after the postal system. Each letter carries the destination address and is routed independent of all the others. Here, it is possible that the letter sent first is delayed so that the second letter reaches the destination before the first letter.

Congestion Control: A router can be connected to 4-5 networks. If all the networks send packet at the same time with maximum rate possible then the router may not be able to handle all the packets and may drop some/all packets. In this context the dropping of the packets should be minimized and the source whose packet was dropped should be informed. The control of such congestion is also a function of the network layer. Other issues related with this layer are transmitting time, delays, jittering.

Internetworking: Internetworks are multiple networks that are connected in such a way that they act as one large network, connecting multiple office or department networks. Internetworks are connected by networking hardware such as routers, switches, and bridges.Internetworking is a solution born of three networking problems: isolated LANs, duplication of resources, and the lack of a centralized network management system. With connected LANs, companies no longer have to duplicate programs or resources on each network. This in turn gives way to managing the network from one central location instead of trying to manage each separate LAN. We should be able to transmit any packet from one network to any other network even if they follow different protocols or use different addressing modes.



Inter-Networking

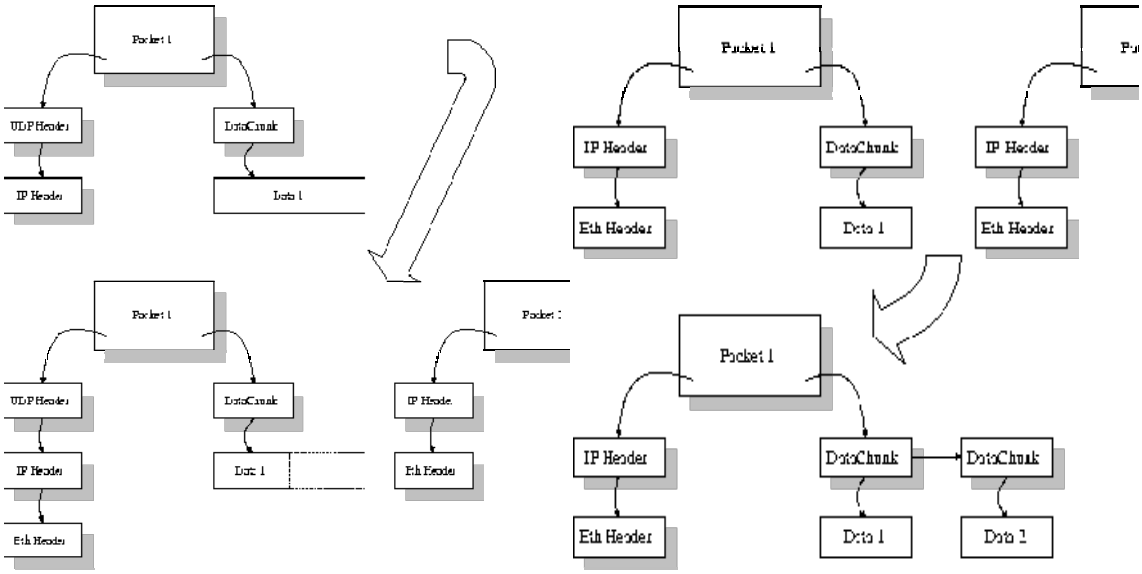
Network Layer **does not** guarantee that the packet will reach its intended destination. There are no reliability guarantees.

Transport Layer

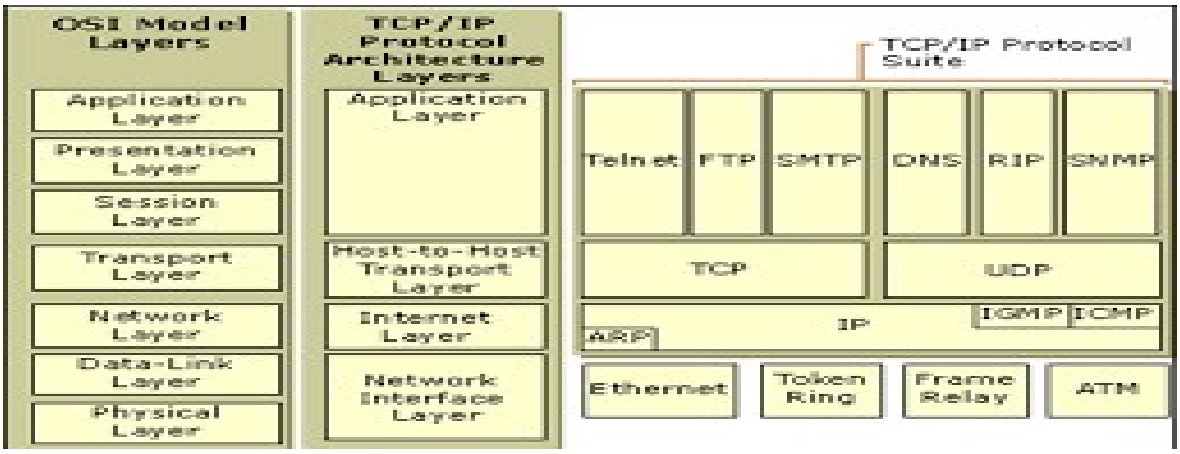
Its functions are :

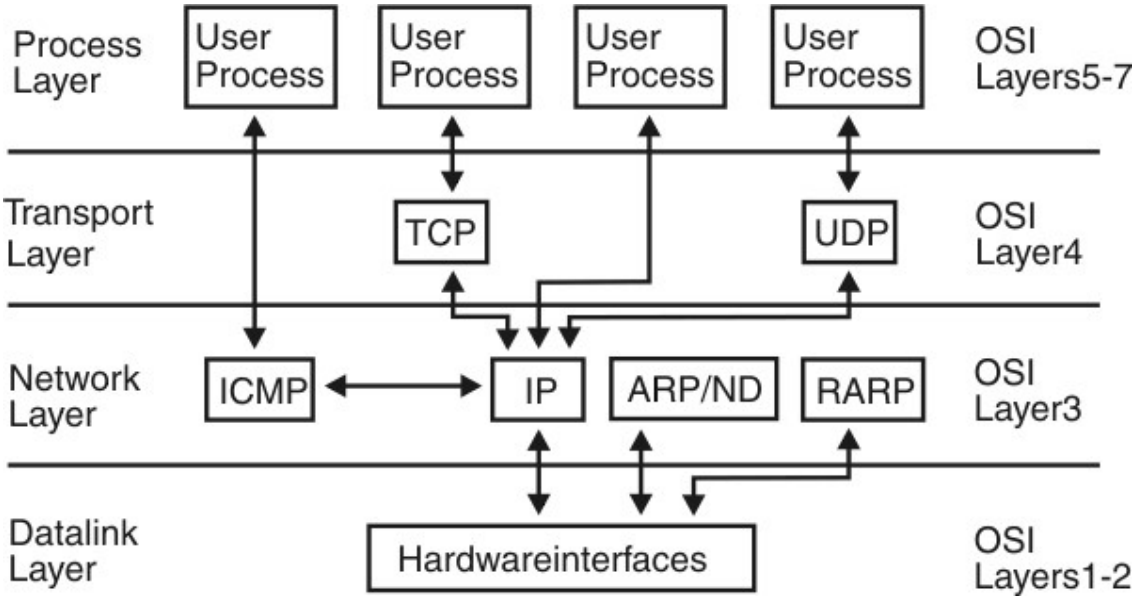
- **Multiplexing / Demultiplexing :** Normally the transport layer will create distinct network connection for each transport connection required by the session layer. The transport layer may either create multiple network connections (to improve throughput) or it may multiplex several transport connections onto the same network connection (because creating and maintaining networks may be expensive). In the latter case, demultiplexing will be required at the receiving end. A point to note here is that communication is always carried out between two processes and not between two machines. This is also known as process-to-process communication.
- **Fragmentation and Re-assembly :** The data accepted by the transport layer from the session layer is split up into smaller units (fragmentation) if needed and then passed to the network layer. Correspondingly, the data provided by the network layer to the transport layer on the receiving side is re-assembled.

Fragmentation **Reassembly**



- **Types of service :** The transport layer also decides the type of service that should be provided to the session layer. The service may be perfectly reliable, or may be reliable within certain tolerances or may not be reliable at all. The message may or may not be received in the order in which it was sent. The decision regarding the type of service to be provided is taken at the time when the connection is established.
- **Error Control :** If reliable service is provided then error detection and error recovery operations are also performed. It provides error control mechanism on **end to end** basis.
- **Flow Control :** A fast host cannot keep pace with a slow one. Hence, this is a mechanism to regulate the flow of information.
- **Connection Establishment / Release :** The transport layer also establishes and releases the connection across the network. This requires some sort of naming mechanism so that a process on one machine can indicate with whom it wants to communicate.


OSI Model Layers
Application Layer
Presentation Layer
Session Layer
Transport Layer
Network Layer
Data-Link Layer
Physical Layer
TCP/IP Protocol Architecture Layers
Application Layer
Host-to-Host Transport Layer
Internet Layer
Network Interface Layer
TCP/IP Protocol Suite
Telnet
FTP
SMTP
DNS
RIP
SNMP
TCP
UDP
IP
IGMP
ICMP
ARP
Ethernet
Token Ring
Frame Relay
ATM


Process Layer
User Process
User Process
User Process
User Process
OSI Layers5-7
Transport Layer
TCP
UDP
OSI Layer4
Network Layer
ICMP
IP
ARP/ND
RARP
OSI Layer3
Datalink Layer
Hardwareinterfaces
OSI Layers1-2

TCP/IP DoD Model			OSI Model
Application Layer (Services Layers 5,6,7) **PDU: Data**	HTTP: port **80** HTTPS/TLS/SSL: port **443** NNTP: port **119** FTP: port **21, 20** Telnet: port **23** SSH: port **22** POP3: port **110** IMAP4: port **143** SMTP: port **25**	DNS: port **53** TFTP: port **69** DHCP/BootP: port **67,68** SNMP: port **162, 161** NTP: port **123** Syslog: port **514**	Application Layer (7) **Scribe.** APIs, network services Serves the King/User
			Presentation Layer (6) **Translator.** Reformats, encrypts/de-crypts, compress/de-compress
			Session Layer (5) **Negotiator.** Establishes, manages and ends sessions.
Transport Layer (Host to Host Layer 4) **PDU: Segments**	TCP: protocol 6	UDP: protocol 17	Transport Layer (4) **Middle Manager.** Segment ID/Assembly
Internet Layer (Network Layer 3) **PDU: Packets**	IP	IP	Network Layer (3) **Mail Room Guy.** IP Addressing/Routing
Network Acces Layer 1 & 2 **PDU: Frame**	Ethernet, PPP Frame Relay MAC addresses, ARP	Ethernet, PPP Frame Relay MAC addresses, ARP	Data-Link Layer (2) **Envelope Stuffer.** Organizes bits into frames
Network Access Layer 1 & 2 **PDU: Bits or Data Stream**	Electrons, RF or Light	Electrons, RF or Light	Physical Layer (1) **The Truck.** Movement of bits.