CH05. Network Maintenance and Troubleshooting

- Backups

- In might not happen today or tomorrow, but Someday you will lose a hard drive containing essential network data.

- The drive might be stolen along with the computer, destroyed in a fire or other catastrophe or simply fail.

- Whatever happens, the data is gone and it's up to you, as the network administrator, to get it back.

- Backups are simply copies your data that you make on a regular basis, so that if a storage device fails or is damaged and data stored there is lost, you can restore it in a timely manner.

- A backup is the ultimate fault-tolerance measure.

Backup Hardware
1) Magnetic Tape drives
2) CD- ROM drives
3) Cartridge drives
4) Autochangers

1) Magnetic tape drives

- Magnetic tape drives are storage devices used to backup large amount of data. They rely on magnetic tape as the storage medium, similar to Older cassette tapes but with high capacity and storage

- How Magnetic Tape drive work
1. Storage medium : Magnetic tapes are long, thin strips coated with a magnetic material that stores data when the drive applies a magnetic field.

2. Sequential access : Unlike disk drive that offer random access, tape drives access data sequentially. This means they read or write data in the order it appear on the tape.

3. High capacity and durability : Modern tapes can store terabytes of data on single cartridge, with excellent longevity -often lasting 30 year or more if properly stored.

4. Cost efficiency : Magnetic tapes offer a lower cost per gigabyte compared to hard drives and SDDs.

Advantages :

1) Low cost storage for large volumes of data
2) High durability and reliability for long-term storage
3) Energy-efficient since tapes can be stored without active power.

disadvantages :

1)
1) Slower access time due to sequential access
2) Required specialized tape drives and management system.
3) Physical storage and handling logistics.

2) CD-ROM drives

1) Earlier use in Backup : CD-ROM drives were once used for data storage and backup but are rarely chosen today

2) Storage Limitation : A typically CD-ROM holds only around 700 MB, which limits its effectiveness for large backup

3) Slow Read/Write speeds : Compared to modern storage, CD-ROMs are much slower for reading and writing data.

4) Replaced by modern options : External hard drives, SSDs, USB flash drives, and cloud storage have replaced CD-ROMs for backup due to higher capacities and speed

5) Occasional use in Archiving : CD-ROMs may still be used for archiving specific files or distributing software.

6) Durability : CDs are relatively durable but can be scratched, and their data can degrade over time, especially with heavy use.

7) Obsolescense : Many newer computer don't include CD drives, making them less practical as backup H/W.

3) Cartridge drives

-Cartridge drives, once popular for data storage and backup, are specialized removable storage devices that offer unique benefits and limitation

-1) Removable storage : Cartridge drives use cartridge to store data, making it easy to remove and replace cartridge as needed

2) used for Backup : Cartridge drives commonly used for data Backup and archival storage, especially in professional settings requiring physical, offline data protection

3) Higher Capacity than CDs: Catridge drives often held more data than CDs or floppy disks. with zip disks ranging from 100 MB to 750 MB

4) Durability and reliability : Cartridge are typically durable and reliable, with a protective casing around the media that helps protect it form dust and physical damage.

5) Compatibility Issues : with advancement in technology, many newer computer don't Support Catridge drives, limiting their usability

4) Autochangers

-Autochangers, also known as tape libraries or Jukeboxes, are dutomated data storage devices designed to manage and retrieve multiple tapes or cartridge without manual intervention.

- Automated storage solution :- Autochanger are automated systems used to store and retrieve data tapes or caltridge, making data management efficient.

2) High capacity for data Backup: They provide high capacity storage, making them ideal for large-scale backups, archiving and disaster recovery in data centers.

3) Reduced human labor: Autochangers reduce manual handling of tapes, minimizing errors, wear and potential damage from human intervention.

4) Autochanger work with backup software to Schedule, manage and automate data backup processes, Streamlining storage management.

- ~~So~~Backup software functions

-Apart from the HW, the other primary component is network backup solution is the software that you use to perform the backup.

The primary function of a good backup SW product are examined in the following section.

1) Target selection and filtering
2) Incremental and differential Backup
3) Drive Manipulation
4) Scheduling
5) Logging and cataloging
6) Media rotation
7) Restoring 8) Disaster recovery
9) Network Backup functions

Backup software provides essential functions to help protect and manage data. Here are the key functions of backup SIW:

1) Data Backup: Creates copies of files, application, database, or entire system to restore in case of data loss or corruption

2) Scheduling Backup: Allows user to set automated backup Schedule to ensure regular, consistent backup without manual intervention

3) Data compression: Compress backup data to reduce the storage space required, making backups faster and more storage-efficient.

4) Encryption - provides encryption option to protect data from unauthorized access, enhancing data security.

5) Data deduplication: Removes duplicate data within the backup to reduce storage needs, making backups more efficient.

6) Restore and recovery: facilitates easy restoration of files, folders, applications or entire systems to their previous state after data loss or corruption

7) Versioning - Maintains multiple versions of files, allowing users to recover specific version or earlier states of files as needed.

8) Cloud Backup integration : offers options to backup data to cloud storage services, providing off-site storage and easy accessibity

9) Disaster recovery - support complete system recovery after critical failure, enabling businesses to quickly restore operation.

10) Backup validation : Verifies the integrity reports ~~on~~ of backup files to ensure data can be restored correctly without errors.

- Virus and its types

-A virus is a fragment of code embedded in a legitimate program

- Viruses are self-replicating and are designed to infect other programs.

1) File virus - This type of virus infects the system by appending itself to the end of a file. It changes the start of a program so that the control jumps to its code. After the execution of its code, the control returns back to the main program.

Its execution is not even noticed. It is also called as a Parasistic virus.

2) Boot Sector virus:
- It infects the boot sector of the system, executing every time system is booted and before the operating system is loaded.
- It infects other bootable media like floppy disks.

3) Macro virus:
- Unlike most viruses which are written in low-level language, these are written in high-level language like visual Basic.
- These viruses are triggered when a program capable of executing a macro is run.

4) Polymorphic virus:
- A virus signature is a pattern that can identify a virus. So in order to avoid detection by antivirus a polymorphic virus changes each time it is installed.
- The functionality of the virus remains the same but its signature is changed.

5) Encrypted virus -
In order to avoid detection by antivirus, this type of virus exists in encrypted form. It carries a decryption algorithm along with it. So the virus first decrypts and then executes

6) Overwritting virus.
- This type of ~~co~~ virus overwrites the code with its own code.

7) Non-resident virus
This type of virus execute itself and terminate after some time

8) Stealth virus
It is the virus which hides the modification it has mode in the file or boot record.

- Preventing virus infections :-
1) use Antivirus software
- Install reputable antivirus s/w & keep it updated to detect and eliminate malicious s/w

2) Enable firewall

3) Use strong passwords and enable multi-factor Authentication.

4) Backup Important data

	Driver updates	software upgrades.
1)	Enhance compatibility between hardware & operating system or other software	Add new feature, improve performance, and Sometimes redesign the user interface
2)	affect hardware Components like graphics cards, etc.	affect applications or entire operating system.
3)	Smaller in size	larger in size
4)	ensure smooth operation between H/W and OS	focus on improving the application itself
5)	usually provided by h/w manufactures	Released by the SlW developers
6)	Quicker process	take longer time.
7)	It can be automatic	—
8)	more security	less security
9)	smaller size files	

11 Nov 2024.

Operating System utilities for network Troubleshoot

1) NET config
2) NET DIAG
3) NET START
4) NET STOP
5) NET SESSION
6) NET WATCHER.

1) NET config
- The NET CONFIG command is used to manage network resources.
- used on windows to display or configure setting for the server or workstation services.
- This command is commonly used in networked environments and can be useful for managing and checking network configuration on a computer
- Syntax:
NET CONEIG [server | workstation]

2] NET DIAG
- The NET DIAG command was historically used in windows to diagnose network issues, but it has been largely deprecated in newer version of Windows.
- In older versions, NET DIAG helped to run diagnostic test on network connection

Syntax
NET DIAG [options]

3) NET START
-The NET START command in window is used to start services on a local computer.
-It's particularly helpful for managing background service that may be required by application and system functions
-Syntax :-
NET START [server_name]

4) NET STOP
- The NET STOP command in windows is used to stop services running on local computer
- This command is helpful for managing system Service, especially when you need to restart a service or stop one that's causing issues
-syntax
NET STOP [service_name]

5) NET SESSION
-NET SESSION command in window is used to display or manage information about active Session on a computer.
- This command is especially useful in networked environments where you want to view users connected to shared resources or manage those session
-Syntax
NET SESSION [\\computername] [/DELETE]

6) NET WATCHER

- The term NET WATCHER is not an actual command in windows, but it refers to a tool or utility concept for monitoring network activity and active session.
- In older version of windows, there was a tool called Net watcher that allowed administrator to view and control connection to shared file and folder on a network

- TCP/IP utilities for N/W troubleshooting

1) Ping
2) traceroute
3) Route
4) Netstat
5) Nslookup
6) Ipconfig

1) Ping

- The ping command is TCP/IP command used to troubleshoot network connectivity, ~~reabh~~ reachability, and name solution
- The ping command sends one datagram per second and print one line of output for every response received
- Sends ICMP echo request message to target host
- Syntax

ping [hostname or IP address]

l command
utility
y and

was a
dministrator
ed file

sed to
eachabil

per
or

2) Traceroute
- Traceroute is network diagnostic tool used to track the path that packets take from one computer to another over a network.
- It helps identify the route and measure the transit delays of packets across the N/W
- tracert [hostname or IP address] - windows
- traceroute [hostname or IP] - macos

3) Route
- The route command is a networking utility used to view and modify the IP routing table on a computer
- This command allows users to manage how network traffic is directed on a local machine
- Syntax
  route print
  route delete [destination]
  route add [destination] mask [subnet mask]

4) NETSTAT
- NETSTAT is stands for Network statistics
- Netstat is a command-line network utility that display various network connection, routing tables, and other network-related information on a computer
- It is commonly used for network troubleshooting and monitoring
- Syntax
  netstat [options]

5) Nslookup:
- Nslookup stands for Name Server Lookup.
- Nslookup is a command-line tool used for querying the domain Name System to obtain information about domain names, IP addresses.
- It commonly used for troubleshooting DNS issue and verifying DNS configuration
- Syntax.
Nslookup [hostname]

6) IPconfig
- ipconfig is a command-line utility used in windows operating systems to display and manage the IP configuration of computers network interface.
- It provides information about N/W setting
- IPconfig [options]

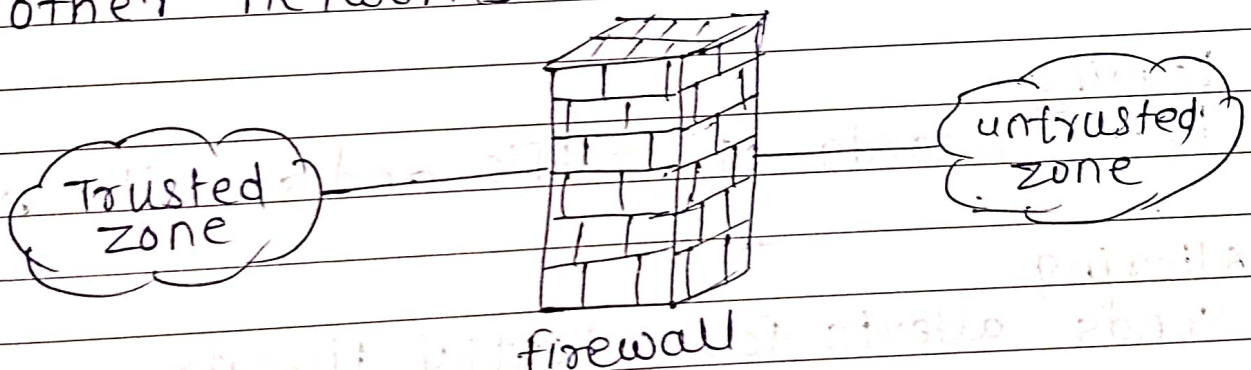
CH06. Network Security

- Firewall

-A firewall is defined as any device (or s/w) used to filter or control the flow of traffic

-firewall are typically implemented on the network perimeter, and function by defining trusted and untrusted zones.

- The firewall implement hardware or s/w solution based on the control of network connections between local network and other networks



- characteristics

1) Traffic Monitoring
observes incoming and outgoing network traf

2) Access control
Sets rules to allow or block traffic

3) Packet filtering
Inspects packs for security

4) NAT (Network Address Translation)
Hides internal IPs from external networks

5) Stateful Inspection
Tracks active connections

6) Logging
keeps records of traffic and security events

7) Altering
Sends alerts for potential threats

8) VPN support
Allows secure remote access

9) Application Awareness
Control traffic for specific apps

10) Intrusion Prevention
Blocks known threats.

- Types of control used by firewalls

1) Service control
determines what types of service can be accessed.

2) Direction control
determines in which direction particular service request may be initiated.

3) User control
determines access to a service according to a user

4) Behaviour control
Controls how particular services are used.

Limitations of the firewalls

- Cannot protect against attacks that bypass the firewall.

- Does not protect against internal threats

- Cannot protect, in general, against transfer of virus-infected programs or files

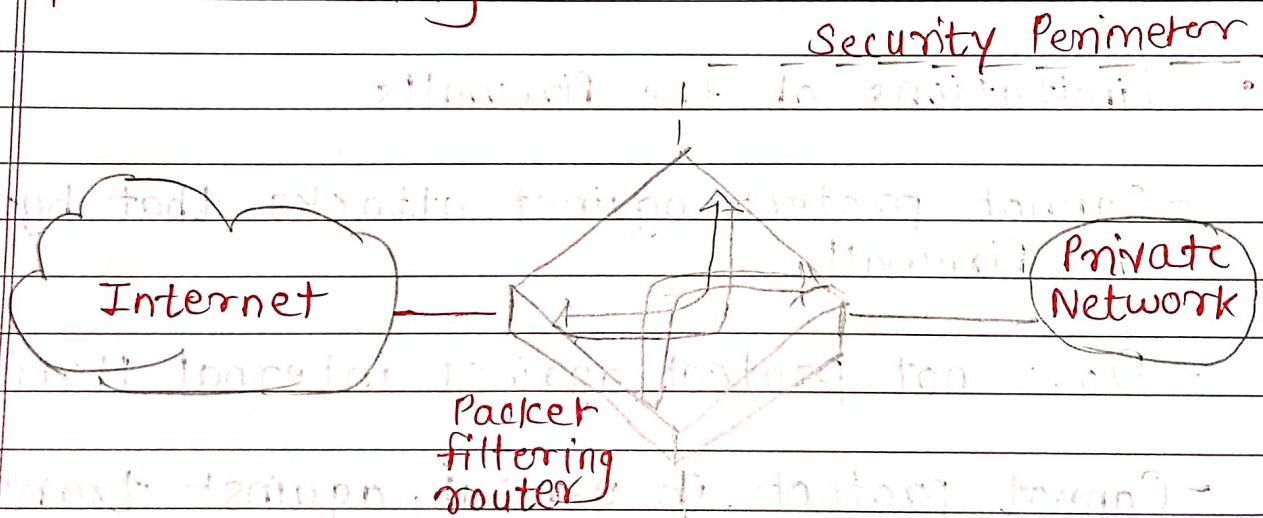
- Firewall cannot protect physical devices which may still be vulnerable to theft or loss

- Firewall do not encrypt data
- firewall can slow down network Performance, especially with advanced filtering
- Basic firewall may not detect threats in app

- Types of firewalls

- Packet filtering router
- Circuit level gateway
- Application level gateway

1) Packet filtering router



- Advantages

1) simple
2) Transpert for user
3) very fast

- A packet-filtering router applies a set of rules to each incoming IP packet and then forwards or discards the packet

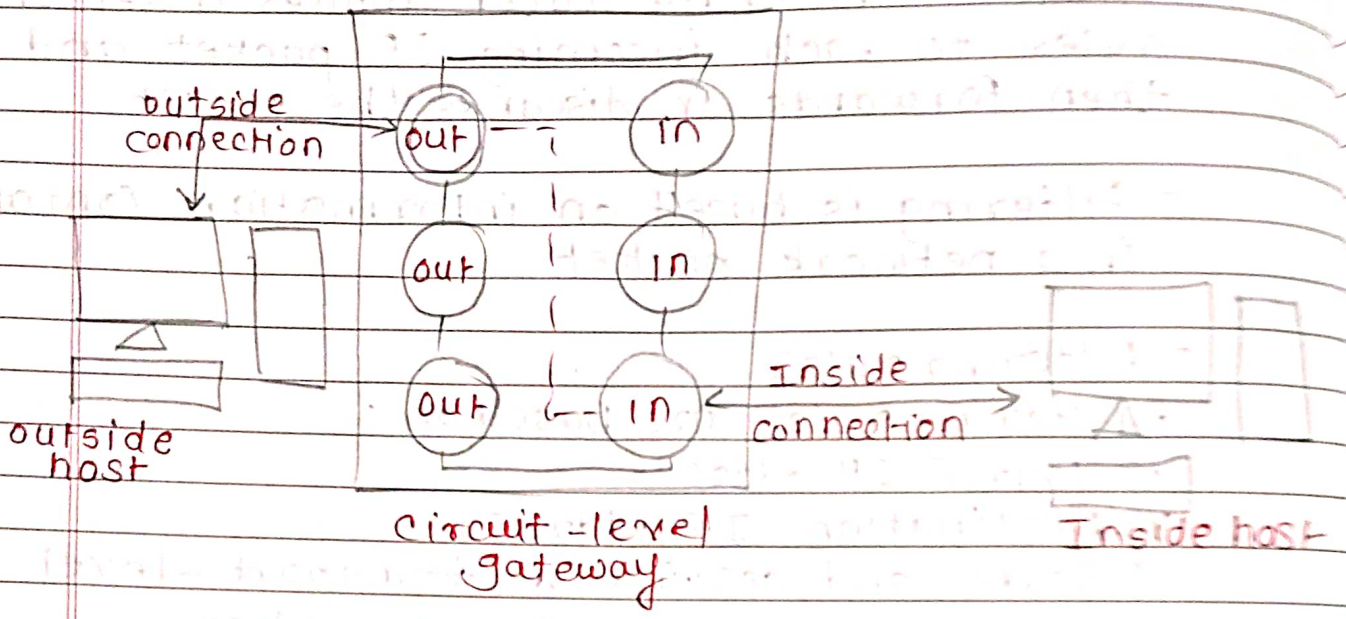
- Filtering is based on information contained in a network packet

- Filtering rules
  - Filtering rules are based on:
    1) Source IP address
    2) Destination IP address
    3) Source and destination transport-level address: transport level port number
    4) IP protocol field: defines the transport protocol

- One may apply rules following two different default policies.
  1) Discard: When packet is discarded, it is blocked or droped by the router or firewall.
  2) Forward: When a packet is forwarded, it is allowed to pass through the router or firewall to reach its destination.

disadvantage
1) lack of upper layer functionality
2) do not support advanced user authentication schemes.
3) Cant identify individual user or session
4) difficult to configure.

2) Circuit level gateway:



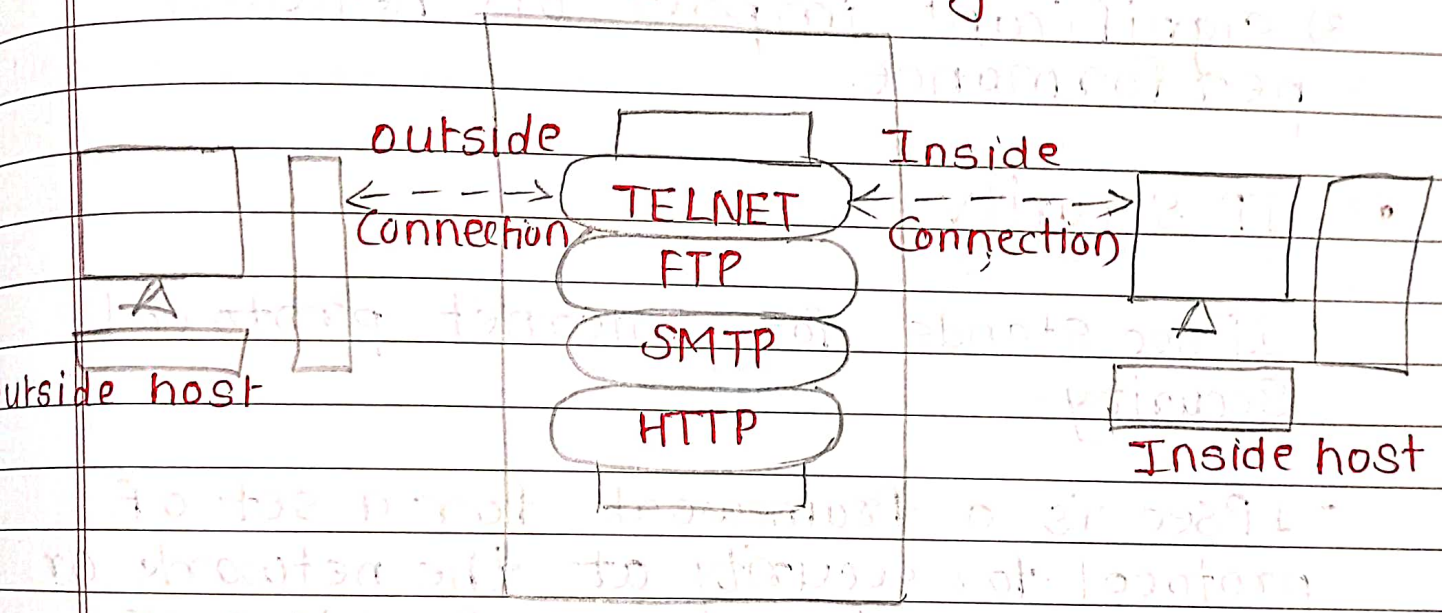
- Traffic is filtered based on specified session rules, like:
  a session is initiated by a recognized computer
- A circuit-level gateway sets up two connections:-
  1) one between itself and a TCP user on the inner host.
  2) one between itself and a TCP user on the outer host.

- Once connection are established and security criteria are met, both connections are linked by the gateway.

Advantages
1) inexpensive
2) faster
3) Hides internal network details

disadvantage
1) limited security
2) do not filter individual packet.

3) Application - level gateway



Application-level gateway

- They can filter packets at the application layer of the OSI model.
- Incoming or outgoing packet cannot access services for which there is no proxy.
- They can filter application specific commands such as http: post and get etc.

Pros:

1) High security
2) Application specific protection
3)

Disadvantages

1) Not transpernt to user
2) require manual configuration of each client computer
3) Significant impact on network performance.

- IP Security

- IPsec stands for Internet protocol Security

- IPsec is a framework for a set of protocol for security at the network or packet processing layer of network communication.

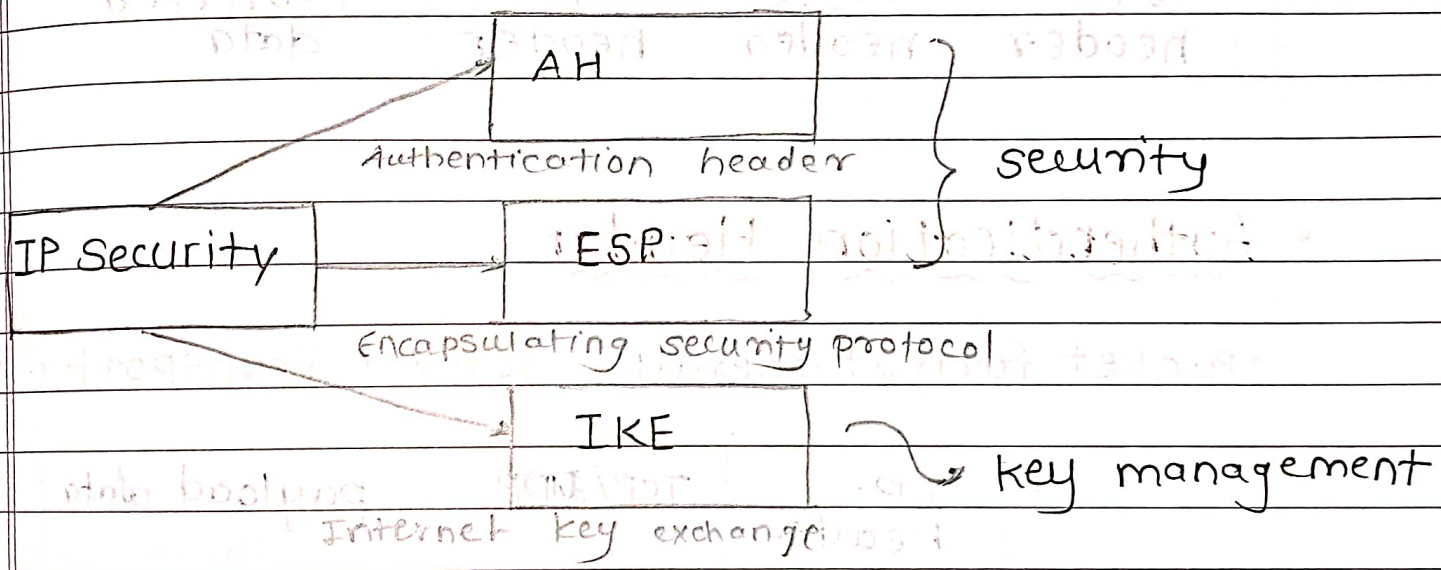
- IPsec is said to be especially useful for implementing virtual private networks and for remote control access through dial-up connection to private network

- IPsec is a protocol suite for securing Internet protocol IP communication by authenticating & encrypting each IP packet of a commun session

- IPsec can be used in protecting data flow between host to host, network to network and network to host.

- Benefits / service by IPsec
  1) confidentiality
  2) Integrity
  3) Authentication
  4) Protection
  5) key & session management.

- IPsec Architecture



- Modes of IPsec Operation

- In transport mode, only the payload of the IP packet is usually encrypted and authenticated. The routing is intact because the IP header is neither modified nor encrypted.

- In Tunnel mode the entire IP packet is encrypted and authenticated. It is then encapsulated into a new IP packet with a new IP header.

1) Transport mode - only payload encrypted.

IP header	IPsec header	Protected data

2) Tunnel Modes - Entire IP packet encrypted.

IP header	IPsec header	IP header	Protected data

- **Authentication Header**

- Packet format alteration for AH Transport mode.

IP header	TCP/UDP	payload data

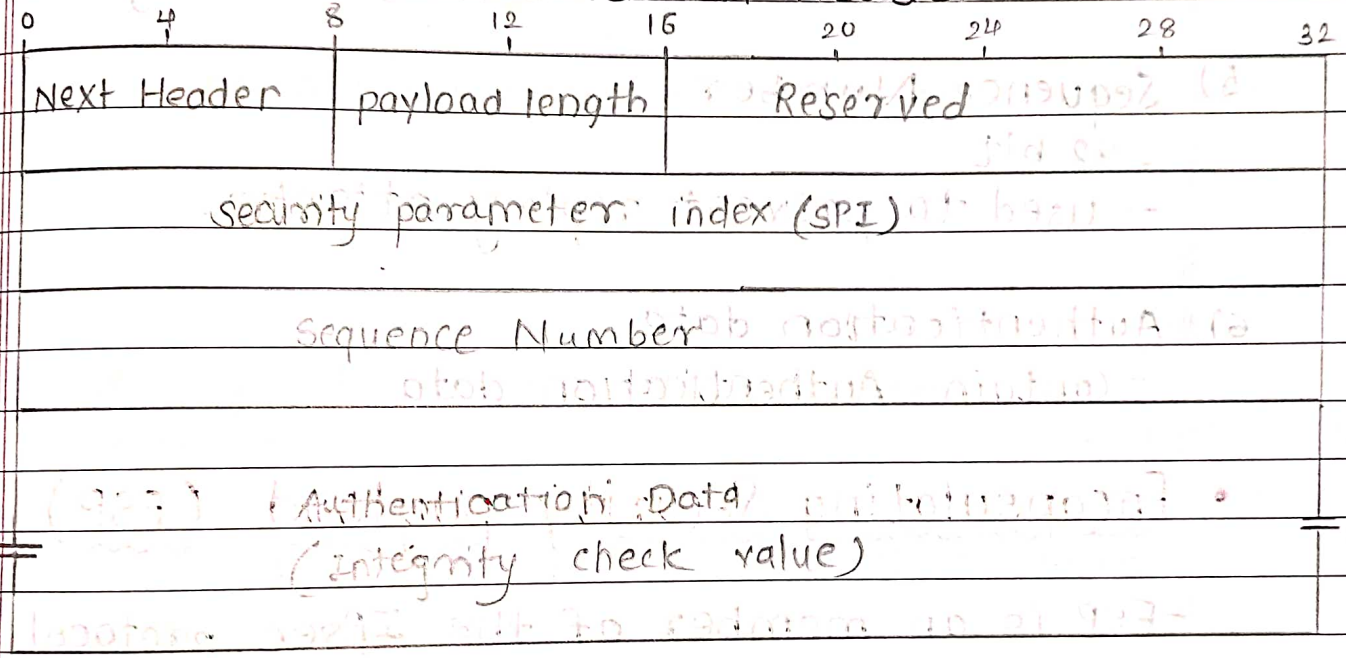
IP header	AH header	TCP/UDP	payload data

- Packet format Alteration for AH : Tunnel mode

IP header	TCP/UDP	Payload data

New IP header	AH header	original IP header	Payload data

- Format of Authentication Header



1) Next Header
   - 8 bit
   - Identifies the type of header
   - It is used to link headers together.

2) Payload length.
   - 8 bit
   - Length of Actual data.

3) Reserved
- 16 bit field
- reserved for future use

4) Security parameter index
- 32 bit
- It is an combination of source and destination address as well as IPsec protocol
- It used to uniquely identify Security Association

5) Sequence Number
- 32 bit
- used to prevent replay attacks.

6) Authentication data
- Contain Authentication data.

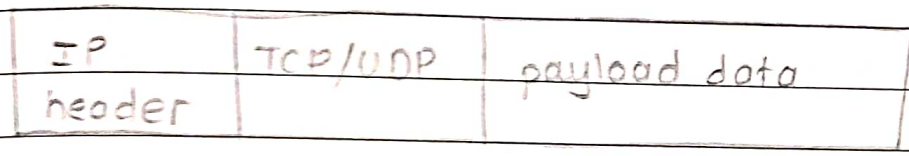
- **Encapsulating Security payload (ESP)**

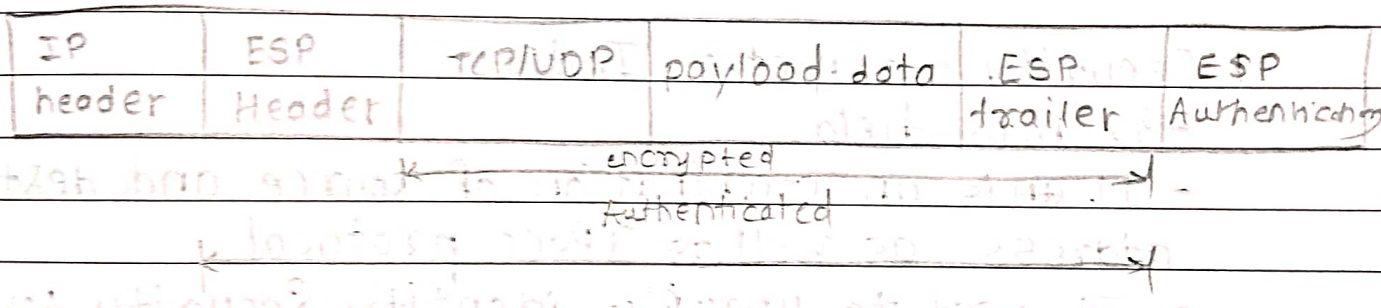
- ESP is an member of the IPsec protocol suite
- IPsec provide origin authenticity, integrity and confidentiality and protection of packets
- ESP operates directly on top of IP
- ESP can also be implemented in both transport and tunneling mode.

- Service provided include:
  1) confidentiality
  2) Data origin authentication
  3) Connectionless integrity
  4) Anti-replay service

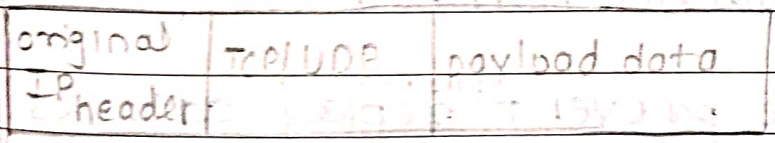
- Security service can be provided between
  1) A pair of communicating hosts
  2) A pair of security gateway
  3) A security gateway and a host.

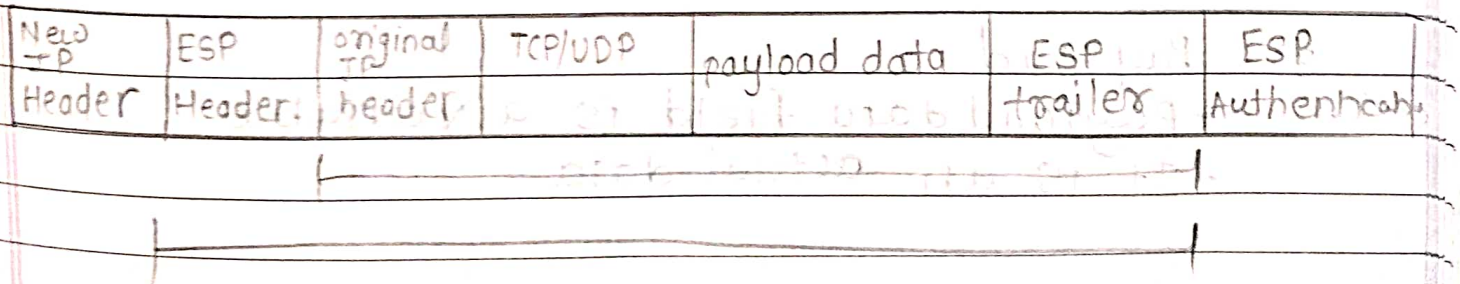
- Packet format Alteration for ESP : Transport Mode



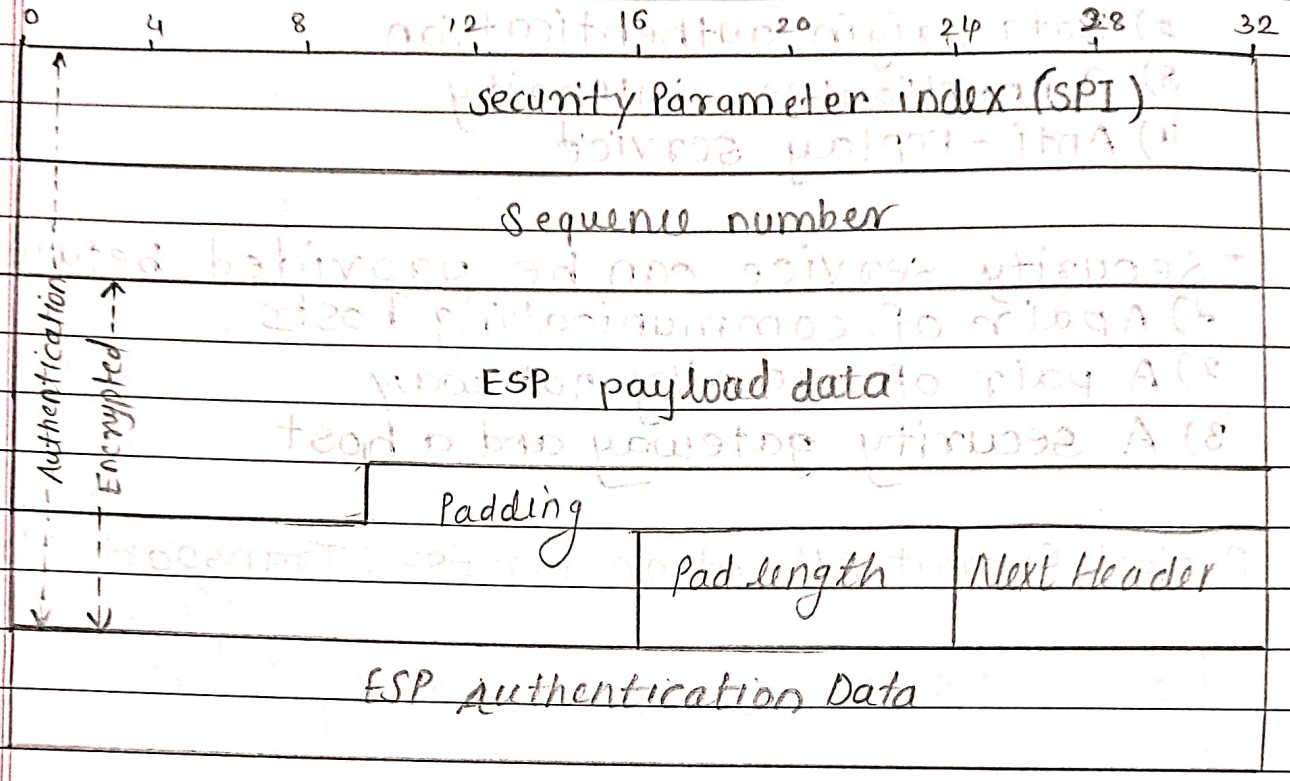


- Packet format alteration for ESP : Tunnel mode.





Format of ESP



1) Security parameter Index -
- 32 bits field
- It ~~an~~ is an combination of source and destination address as well as IPsec protocol
- It used to unquely identify Security Association

2) ~~Security num~~ Sequence number
- 32 bits field
- It is used to prevent from replay attacks

3) Payload
- Payload data field is a variable
- It is an actual data.

4) Padding
- It is used as padding for encryption

5) Pad length
- Size of padding

6) Next header
- type of Header

• Key Management - IKE

- The primary support protocol used for this purpose in IPsec which is called Internet key exchange (IKE)

- The purpose of IKE is to allow devices to exchange information that's required for secure communication

- Cryptographic keys that are used for encoding authentication information and performing payload encryption. IKE works by allowing IPsec-capable device to exchange SAs.

Negotiation process :

1. IKE phase-1
   1) establish the initial tunnel.
   2) peers as authenticated, encryption and hashing algorithms are negotiated, and keys are exchanged based on the IKE policy sets
   3) Two modes can be used for phase-1 negotiation
      i) Main mode - slower but more secure
      ii) Aggressive mode - faster but less secure

2) IKE phase-2 [establish the IPSEC tunnel]
   1) AH or ESP parameter for securing data
   2) These parameters are contained in an IPSEC Transform set.

IKE phase 1 negotiates parameters for the tunnel itself while IKE phase-2 negotiates parameters for the data traversing that tunnel.

Feature of IKE

- An IPsec component used for performing mutual authentication and establishing and maintaining Security Associations
- typically used for establishing IPsec Sessions
- A key exchange mechanism
- Variation of an IKE negotiation :
  1) Two modes
  2) Three Authentication methods

3. Domain Name system

Q. what is the need for DNS ?

- DNS translate human-readable domain names into IP addresses required for communication over the internet
- It eliminates the need for users ~~for~~ to remember complex IP addresses
- DNS provides a structured, scalable, and efficient naming system for device and services on the internet.

Q. What flat name space ?

- A flat name space is system where every name must be unique and is not organized hierarchically
- It is suitable for small networks but lacks scalability and flexibility for longer system

Q. hierarchical name space

- In hierarchical name space, names are organized in a tree structure with levels of specificity
- For example, www.example.com is structured with .com at the top level, example as a subdomain, and www as a specific host.
- It allows scalability and simplifies domain management.

Q domain name space
- The domain name space is the hierarchical organization of domain names used on the internet.
- it include various levels like top level domains, second-level domains and subdomains.
- It is divided into zones managed by different DNS authorities.

Q what are the types of top-level domains?
1) Generic TLDs : includes .com, .org and .net, used for general purpose
2) Country code TLDs : includes .in (india), .us (USA), .uk (UK), representing specific countries

Q What are inverse domain?
- Inverse domain are used for reverse DNS lookup, mapping IP address to domain name.
- This commonly implemented using pointer records in DNS (PTR)

Q What is DNS registar
- A registar is an organization authorized to register domain names
- examples includes companies like GoDaddy and Namecheap
- Registars maintain domain records in the DNS registry

Q What is DNS resolver ?
- A DNS resolver is a client that sends queries to DNS servers to resolve domain names into IP addresses
- Resolvers can perform recursive or iterative queries based on the configuration

Q DNS record
- Question Record : Contains the domain name and Query type
- Resource Record : Contains the response details, such as IP addresses and TTL (Time to Live)

Q Root ~~server~~ name server
- Root name server are the top level DNS server that resolves queries for Top-level domain
- They direct the query to the authoritative server for the specific domain

Q explain following processes
a) Mapping names to addresses
b) mapping addresses to name

→ a) Mapping names to addresses

This process involves associating human-readable name with their corresponding machine-readable addresses. It is most commonly seen in the Domain Name System (DNS)

steps in the process:

1) Input Name : A user enters a domain name into a web browser

2) Query DNS : The system sends a request to a DNS resolver to find the corresponding IP address for the given domain name.

3) Resolve Address : The DNS resolver queries various DNS server to retrieve the IP address associated with the domain name.

4) Return Address : The resolved IP address is sent back to the user's system, enabling the browser to connect to the desired server.

- Name : www.example.com
- mapped Name : 93.183.216.34

b) mapping addresses to Names

This is the reverse of the above process, where a machine-redable address is mapped to its corresponding human-readable name. This is called Reverse DNS Lookup.

Steps in the process :

1) input address : An IP address is queried. (93.183.216.34)

2) Query DNS : A reverse DNS query is sent to a special DNS server that handle reverse mapping

3) Resolve Name : The reverse DNS server look up the name associated with the IP address in its database

4) Return Name : The human-readable domain name is sent back.

Q. Describe recursive resolution with diagram

Recursive resolution is the process where a DNS resolver takes complete responsibility for resolving a domain name into an IP address by querying other DNS servers until it gets the final answer.

steps of recursive resolution :

1) user Query : The client sends a DNS query to the recursive resolver.

2) Query to root server : The resolver asks the root DNS server for the IP address of the domain
   - The root server does not know the IP but provides the address of the top-level domain server.

3) Query to TLD server
The resolver then queries the TLD server for the domain
- The TLD server responds with the address of the authoritative DNS server for the domain

4) Query to Authoritative server
- The resolver queries the authoritative DNS server for the specific subdomain
- The authoritative server provide the IP.

5) Return Result : The resolver returns the IP address to the Client.