Task 1

Linux cmnds:

1. pwd - Print Working Directory
   What it does: Shows you where the heck you are in the filesystem
   Eg: Lost in the terminal? pwd is like asking "Mom, where am I?" and actually getting a straight answer.
2. ls - List Directory Contents
   What it does: Shows you what files and folders are in your current location
   Eg: ls is like opening your cubboard to see how messy it really is

   Important variations: •
   ls -l : Long format (detailed info)
   • ls -a : Shows hidden files (the stuff you didn't want to see)
   • ls -lh : Human-readable file sizes
   • ls -lt : Sort by modification time
   • ls -R : Recursive (shows everything, EVERYTHING!)
3. cd - Change Directory
   What it does: Moves you from one folder to another
   Eg: cd is your magical wardrobe to Narnia, except Narnia is just another folder with more files.
4. mkdir - Make Directory
   What it does: Creates a new folder
   Eg: mkdir is like Marie Kondo telling you to create a place for everything. Now you have no excuse for messy files!

   Useful flags:
   • mkdir -p path/to/nested/dirs : Creates parent directories as needed (lazy mode activated)
5. 5. touch - Create Empty File
   What it does: Creates a new empty file or updates timestamp of existing file
   Eg: touch is like high-fiving a file into reality. No file? BOOM, now there is one!
6. 6. cat - Concatenate and Display Files
   What it does: Shows file contents in terminal
   Think of it as: Opening a book and reading it super fast
   Eg: Named after cats because it just dumps everything on your screen like a cat knocking stuff off a table.
7. 7. cp - Copy Files/Directories
   What it does: Makes a copy of files or folders
   Think of it as: Ctrl+C and Ctrl+V,
8. 8. mv - Move/Rename Files
   What it does: Moves files to new location OR renames them
9. rm - Remove Files/Directories
   What it does: Deletes files FOREVER (no recycle bin!)

   DANGER FLAGS:

   • rm -r : Remove directories recursively

   • rm -f : Force (no questions asked)

   • rm -rf : MAXIMUM DANGER - removes everything without asking

10. echo - Display Text
    What it does: Prints text to the terminal
11. grep - Search Text Patterns

What it does: Searches for text patterns in files
Useful flags:
• grep -i : Case insensitive
• grep -r : Recursive search
• grep -n : Show line numbers
• grep -v : Invert match (show lines that DON'T match)
• grep -c : Count matches

12. find - Search for Files
What it does: Finds files and directories based on criteria
Common patterns:
• find . -name "filename" : Find by name
• find . -type f : Find only files
• find . -type d : Find only directories
• find . -size +10M : Find files bigger than 10MB
• find . -mtime -7 : Files modified in last 7 days

13. chmod - Change File Permissions
What it does: Changes who can read, write, or execute files
Permission basics:
• r = read (4)
• w = write (2)
• x = execute (1)
• Common: 755 (rwxr-xr-x), 644 (rw-r--r--), 777 (rwxrwxrwx - danger!)

14. chown - Change File Owner
What it does: Changes the owner of files/directories
Syntax: chown user: group filename

15. 15. ps - Process Status
What it does: Shows running processes
Useful variations:
• ps aux : Show all processes (the full monty)
• ps aux | grep processname : Find specific process

16. kill - Terminate Processes
What it does: Stops running processes
Signal levels:
• kill PID : Polite termination (SIGTERM)
• kill -9 PID : Force kill (SIGKILL - the nuclear option)

17. top / htop - Interactive Process Viewer
What it does: Real-time view of system processes
Navigation in top:
• Press 'q' to quit
• Press 'k' to kill a process
• Press 'M' to sort by memory
• Press 'P' to sort by CPU

18. df - Disk Free
What it does: Shows disk space usage
df -h : Human readable (GB instead of bytes)

19. du - Disk Usage
What it does: Shows how much space files/directories use
Useful flags:
• du -h : Human readable
• du -s : Summary only
• du -sh * : Summary of each item in current directory

20. tar - Archive Files

What it does: Creates and extracts compressed archives

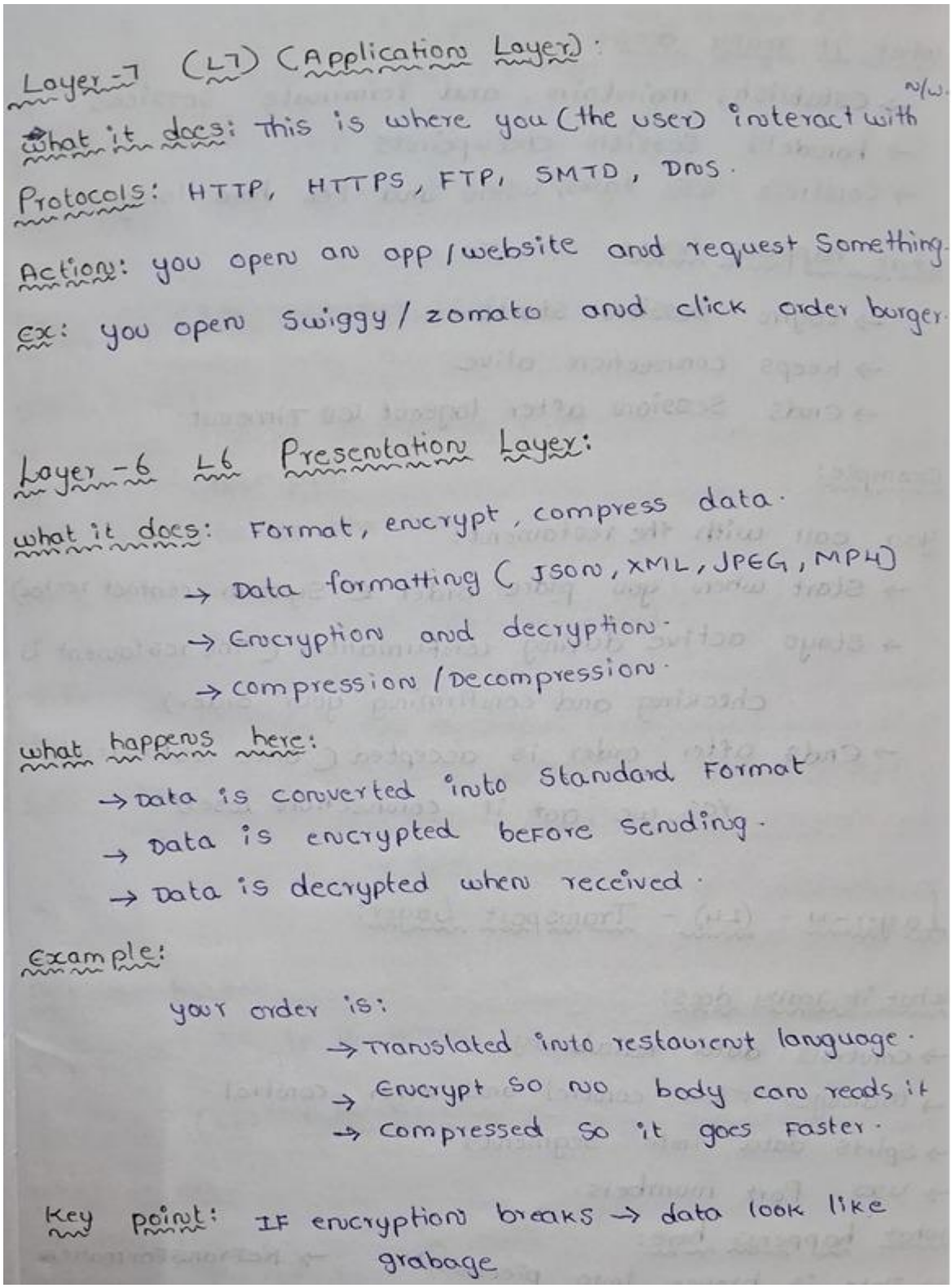
Common patterns:

- tar -czf archive.tar.gz directory/ : Create compressed archive
- tar -xzf archive.tar.gz : Extract archive
- tar -tzf archive.tar.gz : List contents

Flags meaning:

- c = create, x = extract, t = list • z = gzip, v = verbose, f = file

1. OSI MODEL :



Layer 5 - L5 - Session Layer

what it really does:

→ Establish, maintain, and Terminate Sessions.
→ handels Session checkpoints.
→ controls who talks, when and For how long.

what happens here:

→ Login Session starts
→ Keeps connection alive
→ Ends Session after logeout (or) Timeout.

Example:

your call with the restaurent:

→ Start when you place order & System contact restau)
→ Stays active during confirmation (the restaurent is checking and confirming your order)
→ Ends after order is accepted (once restaurent yes, we got it connection loses).

Layer-4 - (L4) - Transport Layer:

what it really does:

→ controls data reliability.
→ manages Flow control and error control.
→ Splits data into Segments.
→ uses Port numbers.

what happens here:

→ Data is broken into pieces.
→ ACKnowledgement is checked (TCP)
→ ReTransFormation If data is Lost

Ex: Your big order is split into packets:

TCP : "Did you receive the burger" 😊

UDP : I sent it, hope you get it.

Protocols: TCP, UDP

Key point: most cyber attack target open ports here.

Layer-3 (L3) network Layer:

what it does:

→ handels logical addressing (IP)

→ Decides best path

→ Routes packets blw n/w

what happens here:

→ Source ip and destination ip added.

→ Routing decision made.

→ Packets forwaded hop by hop.

Ex: Google map uses:

→ shorter route.

→ Less TRAFFIC route

→ alternative route if road blocked.

Devices: Router

Key point: IF ip is wrong → Packet is Lost forever.

Layer 2 (L2) Data link Layer:

what it does:

→ Handles mac address

→ convert Packet into Frames

→ Error detection using CRC

→ control acces to physical media.

what happens here:

→ IP → mac mapping (ARP)
→ Frames created
→ Delivered inside Local n/w

Ex:

Inside your apartment:

→ Delivery guy Find exact Flat numb
→ Ensure correct door delivary.

Device: Switch

Key Point: MAC works inside Local n/w.

Layer 1 (L1) Physical Layer:

what it does:

→ Transmit raw bits (0s and 1s)
→ Deals with cables, Fiber, wifi

what happens here:

→ Electric Signals
→ Light puleses

Ex: The road, bike, signal, cable - actual movement.

Key point:

no intellegence here - Just Send bits.

2. Difference Between TCP and UDP

Feature	TCP (Transmission Control Protocol)	UDP (User Datagram Protocol)
Connection Type	Connection-oriented	Connectionless
Reliability	Reliable (guarantees delivery)	Unreliable (no guarantee)
Data Ordering	Packets arrive in order	Packets may arrive out of order
Error Handling	Error detection & recovery	Basic error detection only
Acknowledgements	Uses ACKs	No acknowledgements
Retransmission	Yes (lost packets resent)	No retransmission
Flow Control	Yes	No
Congestion Control	Yes	No
Speed	Slower	Faster
Header Size	Larger (20+ bytes)	Smaller (8 bytes)
Overhead	High	Low
Latency	Higher	Lower
Use Case Priority	Accuracy & reliability	Speed & low delay
Typical Applications	HTTP, HTTPS, FTP, Email	Streaming, Gaming, VoIP, DNS

1)TCP

TCP is a **connection-oriented protocol**, meaning a connection must be established before data is sent.

Key characteristics:

- Reliable communication
- Guaranteed delivery of data
- Data arrives **in correct order**
- Lost packets are retransmitted

In simple terms: **Accuracy and reliability are prioritized over speed.**

2) TCP Three-Way Handshake

Before communication begins, TCP performs a connection setup:

1. **SYN** → Client requests connection
2. **SYN-ACK** → Server acknowledges
3. **ACK** → Client confirms

Only after this process does data transfer start.

Purpose:

- Ensures both sides are ready

- Synchronizes sequence numbers
- Prevents invalid connections

3) Key Features of TCP

- **Error Checking** → Detects corrupted data
- **Flow Control** → Prevents receiver overload
- **Congestion Control** → Avoids network congestion
- **Acknowledgements (ACKs)** → Confirms delivery
- **Retransmission** → Sends lost packets again
- **Larger Header Size** (20+ bytes)
- **Slower** due to overhead
  Reason for slower speed:
  Extra mechanisms = more processing = higher reliability.

4) Real-World Examples of TCP
Used where correctness is critical:

- **HTTP / HTTPS** (Web browsing)
- **FTP** (File transfer)
- **SMTP / IMAP** (Email)
- Database communication

UDP (User Datagram Protocol)
Type: Connectionless & Fast (but Unreliable)

1) UDP
UDP is a **connectionless protocol**, meaning:

- No connection setup
- No guarantee of delivery
- No ordering of packets
- Faster transmission
  In simple terms: **Speed is prioritized over reliability.**

2) UDP Communication Behavior
UDP sends data directly:

- No handshake
- No acknowledgements
- No retransmission
  Packets are sent using **best-effort delivery**.
  Possible outcomes:
- Packets may be lost
- Packets may arrive out of order

3) Key Features of UDP

- No connection establishment
- No flow control
- No congestion control
- No ACK mechanism
- **Very small header** (8 bytes)
- **Low latency**
- **High speed**
  Why faster?

Minimal protocol overhead.

4) Real-World Examples of UDP
Used where real-time performance matters:

- **Video / Audio streaming**
- **Online gaming**
- **VoIP calls**
- **DNS queries**

3. Ports and Protocols

Secure Ports & Protocols

SFTP – Port 22

- SFTP (SSH File Transfer Protocol) is used for secure file transfers.
- Operates over SSH and uses strong encryption.
- Protects both credentials and transferred data.

Security Advantage: Data is encrypted during transmission.

SSH (Secure Shell) – Port 22

- SSH provides secure remote login and command execution.
- Encrypts all communication between client and server.
- Secure replacement for Telnet.

Security Advantage: Prevents credential interception and session hijacking.

SMTP with TLS – Port 587

- Port 587 is used for secure email submission.
- Uses TLS (Transport Layer Security) to encrypt email traffic.
- Protects email contents and authentication details.

Security Advantage: Ensures confidentiality of email data.

NTP – Port 123

- Network Time Protocol synchronizes system clocks.
- More reliable and robust than legacy time protocols.
- Includes better error-handling mechanisms.

Security Advantage: Improved reliability and reduced protocol weaknesses.

DoT (DNS over TLS) – Port 853

- Encrypts DNS queries using TLS.
- Prevents eavesdropping and manipulation of DNS requests.

Security Advantage: Protects privacy and data integrity.

HTTPS – Port 443

- HTTPS (HTTP Secure) is used for secure web communication.
- Uses TLS/SSL encryption.
- Protects data exchanged between browser and server.

Security Advantage: Prevents sniffing and man-in-the-middle attacks.

Insecure Ports & Protocols

FTP – Port 21

- FTP (File Transfer Protocol) sends data in plaintext.
- Usernames and passwords are not encrypted.
  Security Risk: Credentials can be intercepted.

  Telnet – Port 23
- Telnet allows remote login but transmits unencrypted data.
- All session information is visible on the network.
  Security Risk: Highly vulnerable to attacks.

  SMTP – Port 25 (Traditional)
- Default SMTP traffic is typically not encrypted.
- Email contents may be exposed.
  Security Risk: Susceptible to interception and spoofing.

  Time Protocol – Port 37
- Legacy protocol for time synchronization.
- Lacks modern reliability and security features.
  Security Risk: Obsolete and rarely used.

  DNS – Port 53 (Traditional)
- Standard DNS queries are not encrypted.
- Queries can be monitored or altered.
  Security Risk: Privacy and integrity concerns.

  HTTP – Port 80
- HTTP transmits web data without encryption.
- Data visible to attackers.
  Security Risk: Vulnerable to sniffing and tampering.

4. Private vs Public IP Addresses

Private IP Addresses

Private IP addresses are used inside local networks (LANs) such as:
- Home networks
- Office networks
- Internal enterprise networks

Key properties:
- Defined by RFC 1918 address space
- Not routable on the Internet
- Can be reused across different networks
- Free to use
- Assigned by:
  - Network administrator
  - DHCP server

Purpose:
- Internal communication
- Conserves public IPv4 addresses
  Reserved Private IPv4 Ranges (RFC 1918)

Range	Description
10.0.0.0/8	Large private networks
172.16.0.0/12	Medium private networks
192.168.0.0/16	Home & small networks

These addresses never appear directly on the Internet.

Public IP Addresses

Public IP addresses are used on **global networks / Internet**.
Key properties:

- **Routable on the Internet**
- Must be globally unique
- Limited in number (IPv4 scarcity)
- Allocated by:
  - ISPs
  - Regional Internet Registries (RIRs)

Usage characteristics:

- May be **static** (often paid)
- May be **shared using NAT**

Purpose:

- Internet communication
- Accessible from anywhere

Other Important Reserved IPv4 Ranges

Loopback Addresses – 127.0.0.0/8

- Used for **self-communication**
- Example: **127.0.0.1 (localhost)**
- Used for testing & diagnostics

Link-Local Addresses – 169.254.0.0/16

- Automatically assigned when DHCP fails
- Used for local communication only
- Not Internet routable

Multicast Addresses – 224.0.0.0 to 239.255.255.255

- Used for **one-to-many communication**
- Common in streaming & routing protocols

Reserved / Experimental – 240.0.0.0 to 255.255.255.255

- Reserved for future use
- Not used for normal hosts

Comparison

Feature	Private IP	Public IP
Usage Scope	Local networks	Internet / Global
Routability	Not routable on Internet	Routable
Uniqueness	Not globally unique	Globally unique
Cost	Free	Often paid
Assignment	Admin / DHCP	ISP / RIR
Reusability	Yes	No

5. Static vs Dynamic IP Addresses

Static IP Address
A static IP address is an IP that does not change.

Key properties:
- Manually configured by administrator
- Remains constant over time
- Predictable & fixed
- Commonly used for servers & infrastructure devices

Advantages:
- Stable communication
- Easy to locate devices
- Required for hosting services (web, mail, DB)

Disadvantages:
- Manual setup required
- Poor scalability for large networks
- Risk of misconfiguration

Dynamic IP Address

A dynamic IP address is an IP that is automatically assigned and can change.

Key properties:
- Assigned by DHCP (Dynamic Host Configuration Protocol)
- Temporary lease-based allocation
- Changes when lease expires or reconnecting
- Common for client devices

Advantages:
- Automatic configuration
- Scalable & efficient
- Minimal admin effort
- Reduces IP conflicts

Disadvantages:

- Address may change
- Not ideal for hosting services
- Harder to track specific devices

Differentiation Table

Feature	Static IP Address	Dynamic IP Address
Assignment	Manual configuration	Assigned by DHCP
Address Change	Does not change	May change
Management Effort	Higher	Lower
Scalability	Limited	Highly scalable
Stability	Very stable	Less predictable
Typical Use	Servers, printers, routers	User devices
Cost (ISP context)	Often paid	Usually default/free
Risk of Conflict	Possible if misconfigured	Rare (DHCP managed)

6. NAT

In real-world incidents, attackers never show up with internal IP addresses.
What SOC analysts actually see are public IPs, translated ports, and firewall decisions.

This is where NAT becomes critical.

NAT:- Network Address Translation.

DNAT:- Dynamic Network Address Translation.
PAT (NAT Overload):- Port Address Translation.
SNAT:- Source Network Address Translation.
DNAT:- Destination Network Address Translation.

Understanding Static NAT, Dynamic NAT, PAT (NAT Overload), SNAT, and DNAT directly impacts:
• Firewall log analysis
• SIEM correlation
• Incident attribution
• Threat hunting accuracy
• Root cause analysis

Without NAT visibility:
IP ownership becomes unclear
Investigations lose accuracy
Alerts tell an incomplete story

NAT is the invisible bridge between private networks and public threats.
If you can't trace NAT mappings, you can't confidently trace attackers.

Types :

1. Static NAT (One-to-One Mapping)
Definition:
Each private IP is permanently mapped to one fixed public IP.
Example:
Private IP: 192.168.1.10 ↔ Public IP: 49.205.12.5
Meaning:

- Same public IP always used
- Mapping never changes

Used For: Servers , Devices needing fixed identity
Advantage: Predictable & stable
Disadvantage: Wastes public IPs

2. Dynamic NAT (Many-to-Many Mapping)
Definition:
Private IPs are mapped to a pool of public IPs.
Example:

- Public IP Pool → 49.205.12.5 – 49.205.12.10

When devices connect:

- Router picks any available public IP
- Mapping is temporary

Meaning: No fixed public IP for a device
Used For:Medium-sized networks
Advantage: Efficient public IP usage
Disadvantage: Still limited by pool size

3. PAT (Port Address Translation) / NAT Overload (Most Important)
Definition:
Many private IPs share one single public IP using port numbers.
Example:
192.168.1.10 → 49.205.12.5:5001
192.168.1.11 → 49.205.12.5:5002
192.168.1.12 → 49.205.12.5:5003
Meaning:

- Same public IP
- Different port numbers identify devices

Used For: Home networks , Almost all modern routers
Advantage: Saves huge number of public IPs
Disadvantage: Slight processing overhead

NAT in IPv4?
NAT (Network Address Translation) in IPv4 is a process used by a router to translate private IP addresses into a public IP address so devices inside a local network can access the internet.
Because IPv4 has limited addresses (~4.3 billion), NAT helps save public IPs.

NAT in IPv6?

NAT (Network Address Translation) in IPv6 is generally not required because IPv6 provides a vast address space, allowing every device to have its own globally unique IP address.
Unlike IPv4, IPv6 was designed to eliminate the need for address conservation techniques like NAT.

Types of NAT in IPv6 :

1. **NAT66 (IPv6 ↔ IPv6) :** Translates IPv6 to IPv6
2. **NPTv6 (Network Prefix Translation):**Translates only network prefix
3. **NAT64 (IPv6 ↔ IPv4):** Allows IPv6 devices to talk to IPv4 servers

Processs:

Step 1 – Device Sends Request
Your laptop inside the network wants to open Google.

- Laptop Private IP → 192.168.1.10
- Google Server IP → Public Internet address

Laptop sends: "Hello Google, send me data"
At this point:
Packet uses **private IP**

Step 2 – Router Changes Address (NAT Happens)
The router acts like a translator.
It:

- Removes laptop's private IP
- Replaces it with **public IP** of router
- Adds a **port number** to remember the device

Example:
192.168.1.10 → 49.205.12.5:5001
Meaning:Router says: "Use my public identity"

Step 3 – Internet Server Replies
Google sends response to:
49.205.12.5:5001
Google does **NOT know your private IP**.

Step 4 – Router Remembers Device
Router checks its **NAT table**:
"Who used port 5001?"
Finds:
5001 → 192.168.1.10

Step 5 – Data Sent Back to Laptop
Router forwards response to your laptop.
Laptop thinks: "Google replied to me directly"

NAT Address Terminology

Inside = Internal network
Outside = External network (Internet)
Global = Real, routable address
Local = Seen within local network

1. Inside Local Address: Private IP of internal device

- Assigned inside LAN
- Not Internet routable

Example:
192.168.1.10

2. Inside Global Address: Public IP representing inside device on Internet

- Assigned by router during NAT

Example:
49.205.12.5
Meaning: How outside world sees the inside device

3. Outside Global Address: Actual public IP of external server
Example:
142.250.183.206 (Google Server)
Real Internet address

4. Outside Local Address: How inside network views outside device
Often same as outside global, but conceptually:
Address of external host as seen internally

7. Firewall

What is a Firewall?
A firewall is a security system that monitors, filters, and controls network traffic based on predefined security rules.
Think of a firewall as: A security gate between networks
It decides:
Which traffic is allowed
Which traffic is blocked

- Purpose of a Firewall

Firewalls exist to protect systems and networks from unauthorized access and malicious traffic.
Main goals:
Prevent attacks
Enforce security policies
Control inbound & outbound traffic
Reduce attack surface

- Core Functions of a Firewall

A firewall mainly performs:
1. Traffic Filtering

- Inspects packets
- Applies allow / deny rules
- Based on IP, port, protocol

Example: Allow HTTPS (443)
Block Telnet (23)

2. Access Control
Controls:

- Who can talk to whom
- Which services are accessible

3. Threat Prevention (Advanced Firewalls)
Modern firewalls detect:
- Malware
- Intrusion attempts
- Suspicious behavior

4. Logging & Monitoring
Records:
- Connections
- Blocked traffic
- Security events

Useful for audits & forensics.

- How a Firewall Actually Works (Simple Flow)

When traffic arrives:
1. Packet enters firewall
2. Firewall checks rule set
3. Compares:
    - Source IP
    - Destination IP
    - Port
    - Protocol
4. Decision:
   Permit → Forward packet
   Deny → Drop packet

- Firewall Placement & Network Segmentation

Firewalls can be positioned at different layers of network architecture.

1. Perimeter Firewall (Edge Firewall)
Position: Between internal network & Internet
Purpose:
- First line of defense
- Blocks external threats

Benefits:
Stops internet-based attacks
Controls external access

2. Internal / Core Firewall
Position: Inside the organization network
Purpose:
- Separates departments / zones
- Prevents lateral movement

Benefits:
Limits internal breaches
Segments sensitive systems
Example:

User VLAN ↔ Server VLAN

3. Distributed Firewall
Position: Implemented at host / workload level
Used in:

- Virtualized environments
- Cloud / SDN networks

Benefits:
Fine-grained control
Protects east-west traffic

- **Micro-Segmentation**

Micro-segmentation = Dividing network into very small security zones.
Instead of protecting entire network: Protect individual workloads / apps
Benefits:
Stops attacker movement
Limits breach impact
Granular security policies

Common in:

- Cloud
- Data centers
- Zero Trust models

- Types of Firewalls

1. Packet Filtering Firewall

- Basic type
- Checks IP, port, protocol
- No session awareness

Fast but limited security

2. Stateful Inspection Firewall

- Tracks active connections
- Remembers session state

Much more secure than packet filtering

3. Circuit-Level Gateway

- Validates TCP handshakes
- Does not inspect payload

Hides internal network structure

4. Application-Level Gateway (Proxy Firewall)

- Acts as intermediary
- Inspects application data

Deep inspection
Higher latency

5. Next-Generation Firewall (NGFW)
Modern & most important.
Features:

Deep Packet Inspection (DPI)
Intrusion Prevention (IPS)
Application awareness
Malware detection

6. Web Application Firewall (WAF)
Specialized firewall.
Protects:

- Web applications
- HTTP/HTTPS traffic

Stops:
SQL Injection
XSS attacks

7. Network-Based Firewall

- Hardware appliance
- Protects entire network

Used at:Perimeter / Core

8. Host-Based Firewall

- Installed on individual machines
- Controls local traffic

Example:
Windows Defender Firewall

- Types of Firewall Deployment

Firewalls can be deployed in multiple ways.

1. Hardware Firewall

- Physical device
- High performance
- Used in enterprises

2. Software Firewall

- Installed on OS / server
- Flexible & low cost

3. Cloud Firewall (FWaaS)

- Firewall as a Service
- Used in cloud environments

Benefits:
Scalable
Centralized security

4. Virtual Firewall

- Runs inside VMs / hypervisors
- Common in data centers

8. SUBNET

Subnetting
• Subnetting means dividing one large IP network into multiple smaller networks called subnets
• It helps organize and manage networks efficiently
• Subnetting is achieved by borrowing bits from the host portion of an IP address

Basic Concept
• Every IPv4 address has two parts: Network portion and Host portion
• The network portion identifies the subnet
• The host portion identifies devices inside that subnet

What is a Subnet
• A subnet is a smaller logical network inside a larger IP network
• Subnets reduce broadcast domains
• Subnets improve traffic management

Subnetting Benefits
• Efficient IP address usage
• Improved network performance
• Better security and isolation
• Easier management and scalability
• Control of broadcast traffic
• Simplified administration

Why Subnetting Improves Performance
• Broadcast traffic is limited within subnet
• Reduces unnecessary network load
• Prevents congestion

Why Subnetting Improves Security
• Allows network segmentation
• Restricts traffic between departments
• Limits lateral movement of attackers

Subnet Mask
• A subnet mask is a 32-bit number used with an IP address
• It defines which bits belong to the network and which belong to hosts
• It acts as a boundary between network and host portions

Purpose of Subnet Mask
• Helps devices determine whether a destination is local or remote
• Assists routers in forwarding decisions
• Enables subnet creation

Examples of Subnet Masks
• 255.0.0.0 → /8
• 255.255.0.0 → /16
• 255.255.255.0 → /24
• 255.255.255.128 → /25
• 255.255.255.252 → /30

CIDR Notation Meaning
• /8 → First 8 bits represent network
• /16 → First 16 bits represent network
• /24 → First 24 bits represent network

Hosts Per Subnet Formula
• Number of hosts = 2^n – 2
• n = Number of host bits
• Subtract 2 for network address and broadcast address
Example:
• /24 → 8 host bits → 2^8 – 2 = 254 hosts
• /25 → 7 host bits → 2^7 – 2 = 126 hosts

Subnetting Logic
• Borrowing bits from host portion increases subnets
• Borrowing bits reduces hosts per subnet
• More subnets → Fewer hosts per subnet
Example:
• /24 → One network, 254 hosts
• /25 → Two subnets, 126 hosts each

Subnetting Methods

1. FLSM (Fixed Length Subnet Mask)
   • All subnets have same size
   • Simple but less flexible
2. VLSM (Variable Length Subnet Mask)
   • Subnets have different sizes
   • Efficient IP usage
   • Used in modern networks

9. DNS and DHCP

DNS (Domain Name System)
• DNS is a system that converts human-readable domain names into IP addresses
• It acts like the phonebook of the Internet
• Without DNS, users would need to remember numeric IP addresses

Purpose of DNS
• Translate domain names to IP addresses
• Simplify Internet usage for humans
• Enable access to websites and services
Example
• User enters google.com in browser
• DNS resolves it to an IP address
• Browser connects to the server using that IP

Why DNS is Needed
• Humans prefer names, not numbers
• IP addresses are difficult to remember
• DNS automates the mapping process

How DNS Works (Simple Flow)
• Client sends DNS query to resolver
• Resolver checks cache
• If not found, queries DNS hierarchy
• IP address returned to client
DNS Resolution Process
• Recursive resolution → DNS server does full lookup
• Iterative resolution → DNS server refers client to other servers

DNS Hierarchy (Conceptual)
• Root servers
• Top Level Domain (TLD) servers (.com, .org, .net)
• Authoritative name servers

Common DNS Record Types
• A record → Domain to IPv4 address
• AAAA record → Domain to IPv6 address
• MX record → Mail server information
• CNAME record → Alias for domain
• NS record → Name server details

DNS Port
• Uses Port 53
• Operates over UDP and TCP

Why UDP and TCP Both Used
• UDP → Faster queries
• TCP → Large responses / zone transfers

DNS Caching
• Stores previous query results
• Reduces lookup time
• Improves performance

DNS Security Issues
• DNS queries traditionally unencrypted
• Vulnerable to spoofing and poisoning

Secure DNS Alternatives
• DoT (DNS over TLS)
• DoH (DNS over HTTPS)

DHCP (Dynamic Host Configuration Protocol)
• DHCP automatically assigns IP configuration to devices
• Eliminates manual IP setup
• Commonly used in modern networks

Purpose of DHCP
• Assign IP address
• Assign subnet mask

• Assign default gateway
• Assign DNS server

Why DHCP is Needed
• Manual configuration is inefficient
• Prevents IP conflicts
• Simplifies network management

How DHCP Works (DORA Process)
• Discover → Client searches for DHCP server
• Offer → Server offers IP configuration
• Request → Client accepts offer
• Acknowledge → Server confirms assignment

Important DHCP Behavior
• Uses broadcast communication initially
• Client has no IP at start

DHCP Ports
• Port 67 → DHCP Server
• Port 68 → DHCP Client

DHCP Lease Concept
• IP assigned temporarily
• Lease has expiration time
• Client may renew lease

Advantages of DHCP
• Automatic configuration
• Scalable for large networks
• Reduces admin workload
• Minimizes IP conflicts

Disadvantages of DHCP
• IP addresses may change
• Dependency on DHCP server availability

What Happens if DHCP Fails
• Device cannot obtain IP
• May assign link-local address (169.254.x.x)
• Network connectivity issues

DHCP vs Static Addressing
• DHCP → Automatic, dynamic
• Static → Manual, fixed

Cmnds :

1. Ping : Ping is a network troubleshooting tool used to test reachability between two devices. It measures response time and packet loss.

Protocols Involved in Ping

ICMP (Internet Control Message Protocol)
Ping mainly uses ICMP. It sends an Echo Request to the destination and waits for an Echo Reply. This helps verify whether the remote device is reachable.

ARP (Address Resolution Protocol)
Before sending packets inside a local network, the device must know the destination MAC address. ARP resolves the IP address into a MAC address.

IP Protocol (Layer 3)
IP handles logical addressing and routing. The packet carries source and destination IP addresses so routers know where to forward it.

DNS Eg: If you ping a domain name like **google.com**, DNS first translates the domain into an IP address.

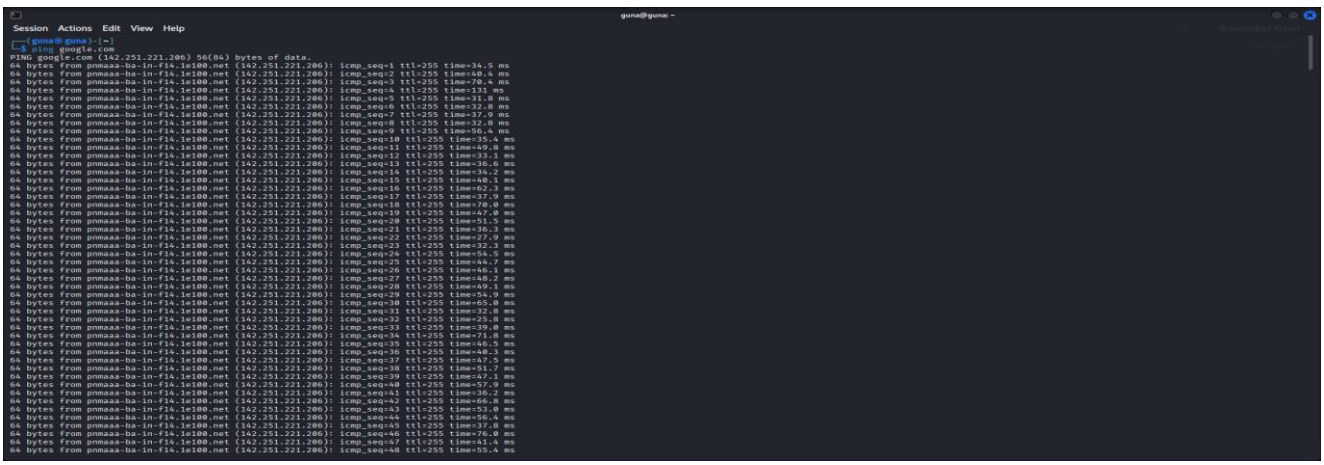
Step-by-Step Flow

1. User types: "ping **google.com**"
2. DNS resolves the domain into an IP address
3. ARP finds the MAC address (inside LAN)
4. ICMP Echo Request is sent
5. Destination replies with ICMP Echo Reply
6. You see time, TTL, and packet statistics

Why Ping is Important?
Tests connectivity
Helps identify network latency
Useful for basic troubleshooting in TCP/IP networks

Ping specific IP : ping 8.8.8.8

Send limited packets (very useful): ping -c 4 google.com



2. Traceroute

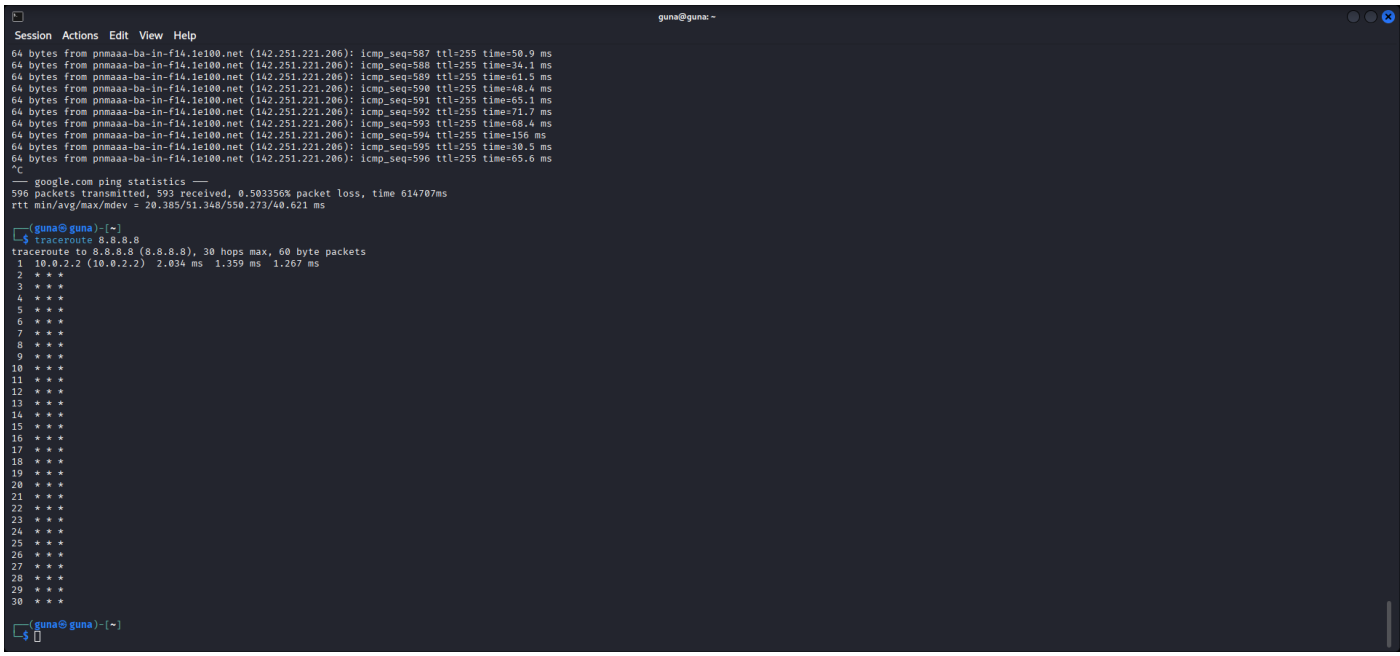
• traceroute identifies the path packets take to reach a destination
• Displays intermediate routers (hops)
• Helps diagnose delays and routing problems

- Purpose of traceroute

• Detect network bottlenecks
• Identify failing hop
• Understand routing path

- What traceroute Actually Does

• Sends packets with increasing TTL values
• Each router decrements TTL
• Router returns ICMP Time Exceeded



3. Netstat Command

netstat displays active network connections and listening ports
• Shows protocol statistics
• Useful for network monitoring

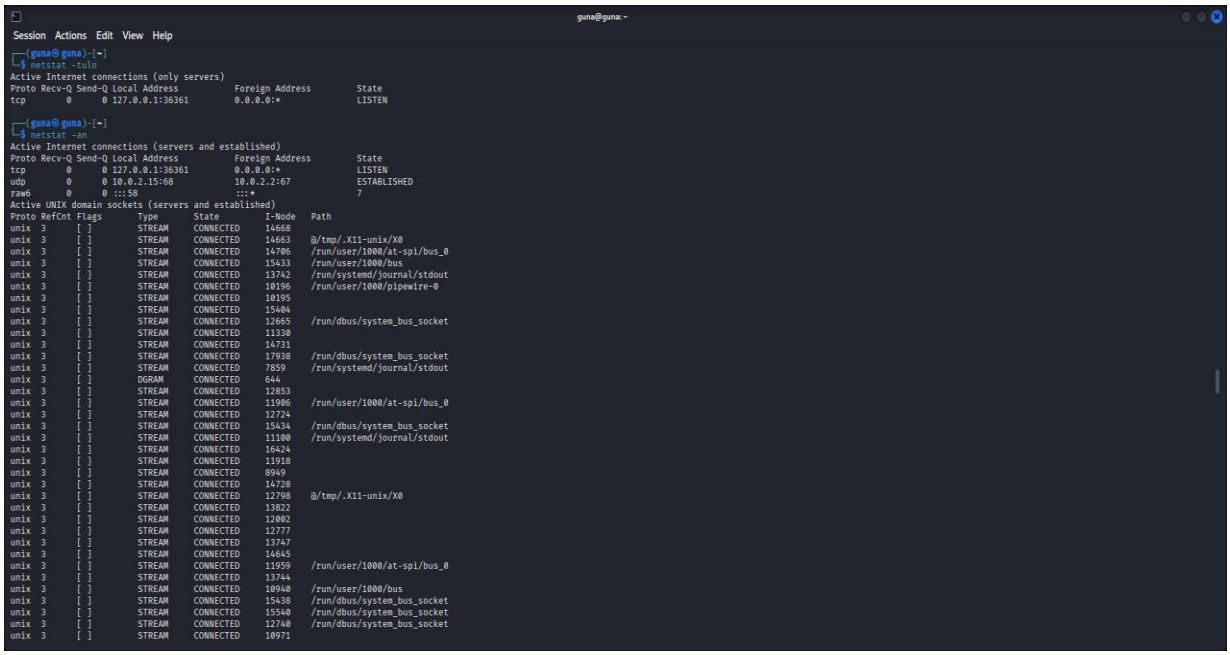
- Purpose of netstat

• View open connections
• Identify listening services
• Troubleshoot port issues

- Common Usage : netstat -tuln
- Meaning of Flags

  • t → TCP
  • u → UDP
  • l → Listening
  • n → Numeric format

- Practical Use: Check if service is running
  • Detect suspicious connections
  • Verify port bindings



5. ss cmd :

Show listening ports : `ss -tuln`

Show active connections: `ss -an`

Filter TCP only: `ss -t`

ss provides socket statistics
• Faster and more detailed than netstat
• Commonly used in modern Linux systems

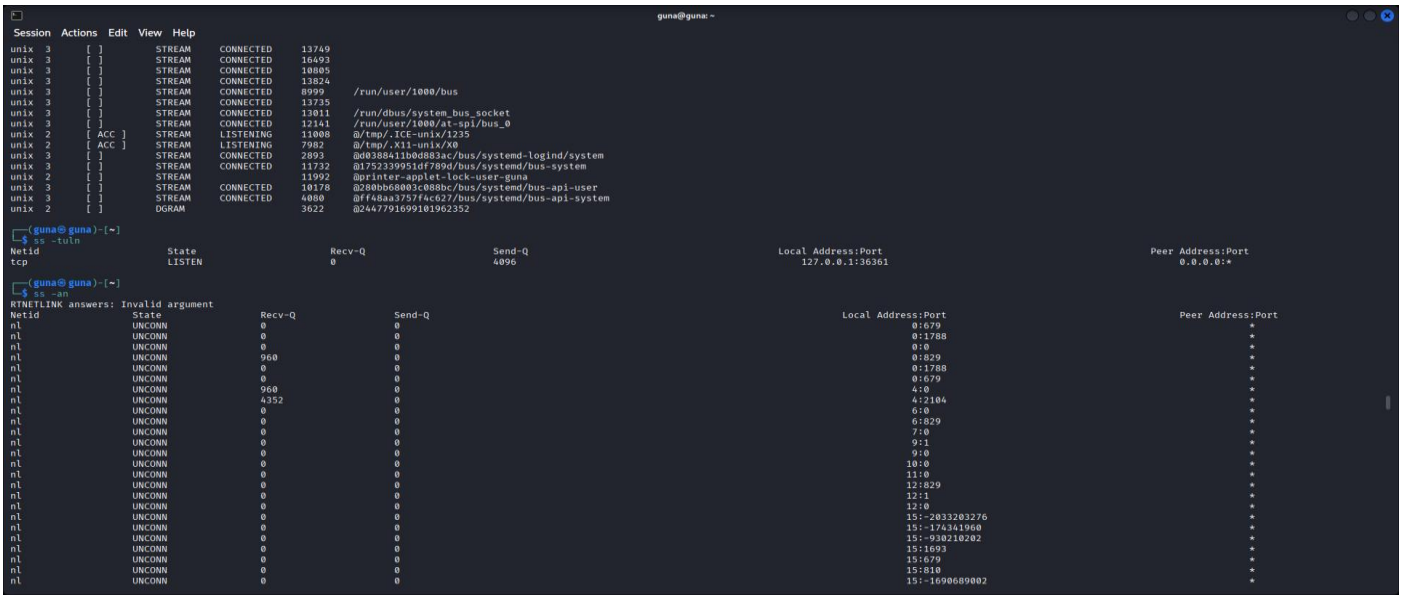
Purpose of ss

• Display active sockets
• View listening ports
• Analyze network connections

Example: ss -tuln

Practical Use

• Same use cases as netstat
• Preferred in newer systems



6. ip a Command (IP Address Command)

   • ip a displays network interfaces and IP addresses
   • Shows interface state and configuration

Purpose of ip a : • View assigned IP addresses
• Check interface status
• Verify MAC addresses

Example: • ip a

Practical Use: • Confirm IP assignment
• Troubleshoot interface issues
• Check DHCP results

7. ip route Command (Check Gateway & Routes)

ip route displays routing table
• Shows how packets are forwarded

Purpose of ip route

• Identify default gateway
• Check routing paths
• Diagnose routing problems

Example: ip route

Important Output Entry

• default via <gateway IP>

Practical Use

• Troubleshoot Internet issues
• Detect wrong gateway
• Verify network configuration

8. telnet Command (IP Port Testing)

Test SSH port : telnet google.com 80

Test local machine port: telnet 127.0.0.1 22

• telnet can test connectivity to a specific IP and port
• Used as a simple port testing tool

Purpose of telnet

- Check if port is open
- Verify service availability
- Test firewall rules

Basic Syntax: telnet <IP address> <port>

Example: telnet 192.168.1.10 22

Result Interpretation

- Connected → Port open
- Connection refused → Port closed / blocked

Practical Use

- Service troubleshooting
- Firewall verification
- Port accessibility testing

- Check DNS resolution: nslookup google.com
- Check open ports on system: sudo ss -lntp
- Check default gateway quickly: ip route | grep default

File Viewing Commands in Linux

1. cat command

• Displays entire contents of a file
• Suitable for small files
• Outputs file directly to terminal

Example

cat filename
cat notes.txt

2. less command

• Displays file content page by page
• Allows scrolling up and down
• Best for large files

Example

less filename
less notes.txt

3. more command

• Displays file content one screen at a time
• Limited navigation compared to less
• Used for basic viewing

Example: more filename
more notes.txt

4. head command

- Displays beginning of a file
- Default shows first 10 lines
- Useful for previewing files

Example

head filename
head notes.txt

Custom lines: head -n 5 notes.txt

5. tail command

- Displays end of a file
- Default shows last 10 lines
- Commonly used for log inspection

Example

tail filename
tail notes.txt

Custom lines: tail -n 5 notes.txt

6. tail -f command

- Displays file updates in real time
- Used for monitoring logs
- Runs continuously until stopped

Example

tail -f filename
tail -f /var/log/syslog

7. grep command

- Searches for specific text inside file
- Displays matching lines only
- Very useful for troubleshooting

Example: grep "word" filename
grep error syslog

8. file command

- Identifies file type
- Shows whether file is text, binary, etc.

Example: file filename
file notes.txt

• cat → Show full file
• less → Scrollable viewer
• more → Basic page viewer
• head → First lines
• tail → Last lines
• tail -f → Live updates
• grep → Search text
• file → File type info