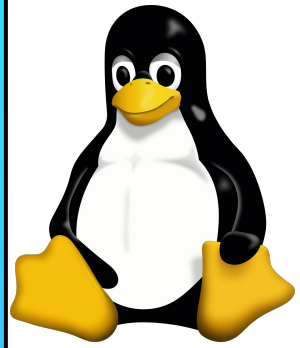
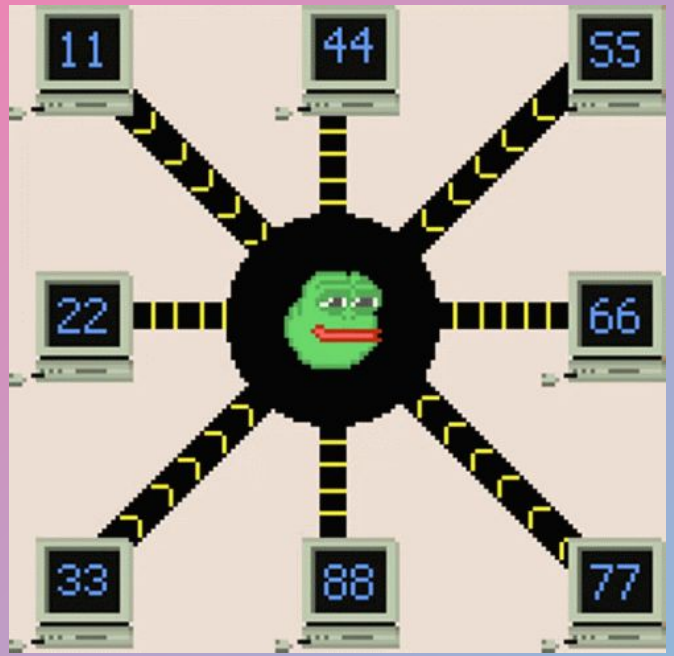


The Linux Week

Introduction to Linux



Welcome to Day 7

Day 7

- ★ Introduction to Networking
- ★ Network Concepts and Components
- ★ Protocols and Ports
- ★ Introduction to Linux Networking
- ★ Firewall Configurations
- ★ Network Troubleshooting
- ★ Network Security Best Practices


01
Introduction
What is Networking

Networking

The practice of connecting computers and other devices to share resources.

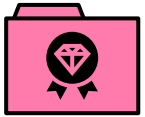
Importance: Facilitates communication, resource sharing, data exchange, etc

02

Network

Concepts and Components

Network Concepts - Types



LAN

Local Area Network

WAN

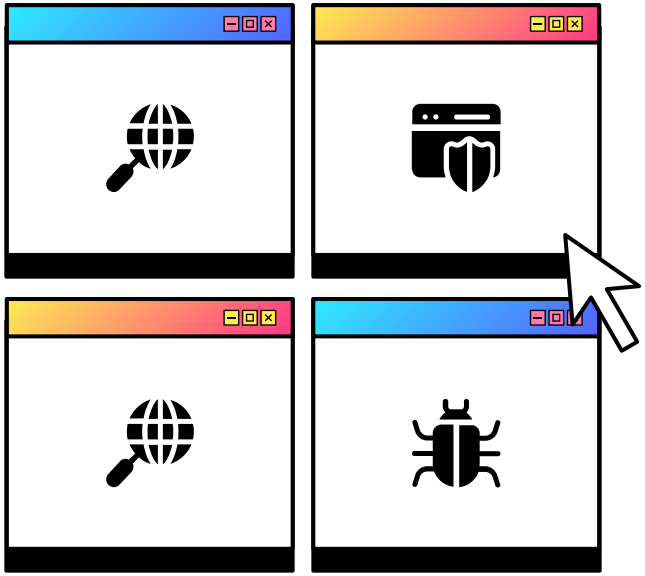
Wide Area Network

PAN

Personal Area Network

Network Component - Hardware

Routers



NICS

Switches

Hubs

Network Components – Software

Network OS

Microsoft Windows Server
Linux-based NOS

Network Protocols

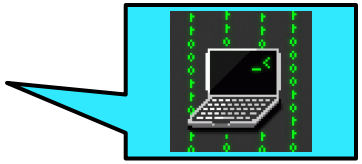
TCP/IP, HTTP, FTP, etc


03
IPs
IP Addresses

Definition

An IP (Internet Protocol) address is a unique identifier assigned to each device connected to a network, allowing them to communicate with each other

Types of IPs



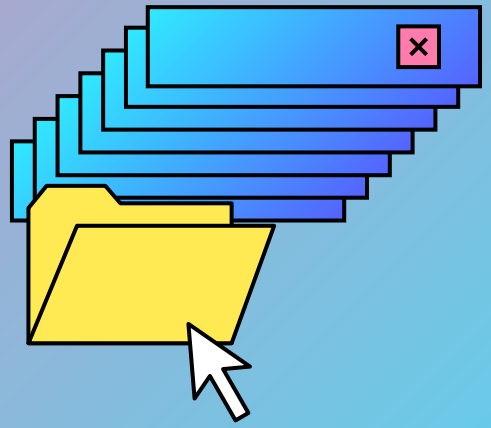
IPv4

Consists of four octets (32 bits), typically written as four decimal numbers separated by dots (e.g., 192.168.1.1).

IPv6

Consists of eight groups of four hexadecimal digits (128 bits), separated by colons (e.g., 2001:0db8:85a3:0000:0000:8a2e :0370:7334).

IPv4



Definitions and Examples

IP Address Classes

Class A

1. Range: 0.0.0.0 to 127.255.255.255
2. Default Subnet Mask: 255.0.0.0
3. Number of Networks: 128

Class B

1. Range: 128.0.0.0 to 191.255.255.255
2. Default Subnet Mask: 255.255.0.0
   Number of Networks: 16,384

Class C

1. Range: 192.0.0.0 to 223.255.255.255
2. Default Subnet Mask: 255.255.255.0
3. Number of Networks: 2,097,152 (2^21)

Class D

1. Range: 224.0.0.0 to 239.255.255.255
2. Purpose: Reserved for multicast groups.

Class E

Reserved For Experimental Uses

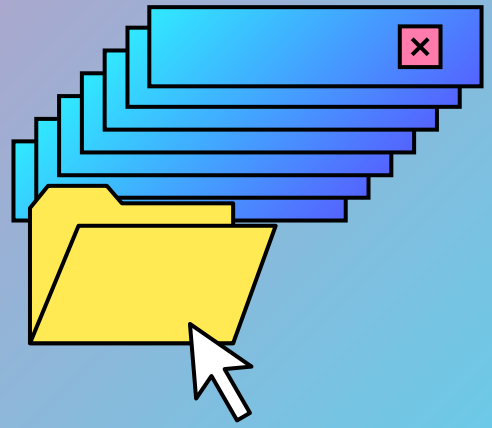
Private IP Addresses

Private IP Addresses: Used within private networks and not routable on the internet.
Class A: 10.0.0.0 to 10.255.255.255
Class B: 172.16.0.0 to 172.31.255.255
Class C: 192.168.0.0 to 192.168.255.255

Loopback Address: 127.0.0.1, used for testing and diagnostics on the local machine.

APIPA (Automatic Private IP Addressing): 169.254.0.0 to 169.254.255.255, used when a device fails to obtain an IP address from a DHCP server.

IPv6



Definitions and Examples

IPv6 Definition

Structure

Consists of 128 bits, written in eight groups of four hexadecimal digits

Example

2001:0db8:85a3:0000:0000:8a2e
:0370:7334

4x4x8 =16x8 = 128

Features of IPv6

Larger Address Space

Simplified Headers

Auto-configuration

Enhanced Security

Subnet & CIDR

Definitions and Examples

Subnet

The process of dividing a network into smaller subnetworks (subnets) to improve manageability and security.

CIDR

(Classless Inter-Domain Routing) - A method for allocating IP addresses and routing that replaces the traditional class-based system.

Notation: Uses a suffix (e.g., /24) to indicate the number of bits in the subnet mask.

CIDR Calculations

Determine Network Prefix Length:

- Subtract the number of host bits from 32 (IPv4) or 128 (IPv6).
- **Example:**
  - For a network with 256 hosts, you need 8 bits for hosts (`2^8 = 256`).
  - Network prefix length is `32 - 8 = 24` (IPv4), hence `/24`.

Subnet Mask Calculation:

- Convert the prefix length to a subnet mask.
- **Example:** `/24` corresponds to `255.255.255.0`.

-

Example

Scenario: Allocating IP addresses for a company with different departments.

- **Network**: 192.168.0.0/22
  - /22 means: 22 bits are used for the network prefix, and 10 bits are used for host addresses.
  - Subnet Mask: 255.255.252.0

Example

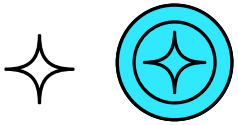
Subnets:

- **Marketing Department:** 192.168.0.0/24
  - Range: 192.168.0.1 to 192.168.0.254
  - Subnet Mask: 255.255.255.0
- **Sales Department:** 192.168.1.0/24
  - Range: 192.168.1.1 to 192.168.1.254
  - Subnet Mask: 255.255.255.0
- **IT Department**: 192.168.2.0/24
  - Range: 192.168.2.1 to 192.168.2.254
  - Subnet Mask: 255.255.255.0
- **Finance Department:** 192.168.3.0/24
  - Range: 192.168.3.1 to 192.168.3.254
  - Subnet Mask: 255.255.255.0


04
Protocols
Protocols and Ports

7	Application Layer	Human-computer interaction layer, where applications can access the network services
6	Presentation Layer	Ensures that data is in a usable format and is where data encryption occurs
5	Session Layer	Maintains connections and is responsible for controlling ports and sessions
4	Transport Layer	Transmits data using transmission protocols including TCP and UDP
3	Network Layer	Decides which physical path the data will take
2	Data Link Layer	Defines the format of data on the network
1	Physical Layer	Transmits raw bit stream over the physical medium

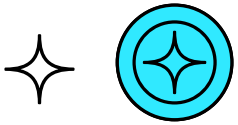
Ports



Application Layer

- HTTP
  - Port: 80
  - Usage: transferring web pages on the internet.
- HTTPS
  - Port: 443
  - Usage: Secure version of HTTP
- FTP
  - Port: 21 (control), 20 (data)
  - Usage: transferring files between a client and server

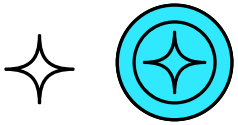
Ports



Application Layer

- SMTP
  - Port: 25
  - Usage: Used for sending emails.
- POP3
  - Port: 110
  - Usage: retrieving emails from a mail server.
- DNS
  - Port: 53
  - Usage: Translates domain names to IP addresses.

Ports



Transport Layer

UDP

Port: Multiple Ports

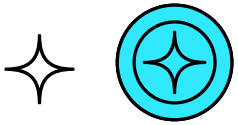
Usage: Provides a simpler, connectionless network communication model with minimal protocol mechanisms.

TCP

Port: Multiple Ports

Usage: Provides reliable, ordered, and error-checked delivery of a stream of data between applications.

Ports



Session Layer

SMB

Port: 445

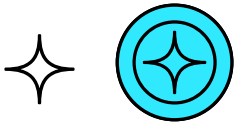
Usage: Provides shared access to files, printers, and serial ports between nodes on a network.

RDP

Port: 135

Usage: Allows a program to cause a procedure to execute on another address space.

Ports



Database Layer

MySQL

Port: 3306

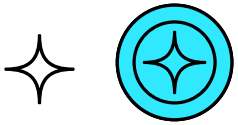
Usage: Protocol used by MySQL databases for database access.

PostgreSQL

Port: 5432

Usage: Protocol used by PostgreSQL databases for database access.

Ports



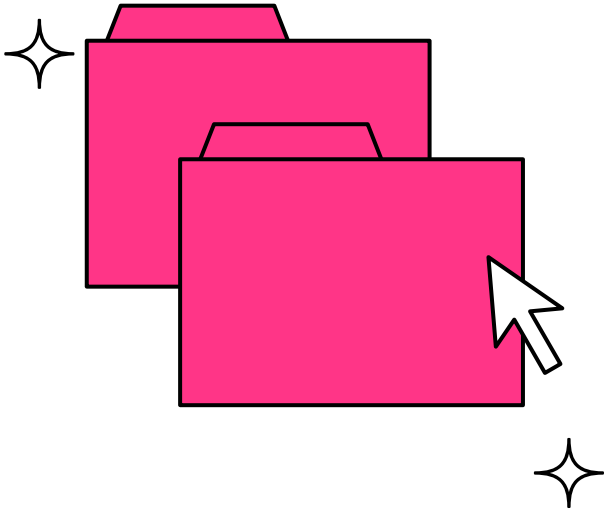
Security Layer

- SSH
  - Port: 22
  - Usage: Provides a secure channel over an unsecured network.
- Telnet
  - Port: 23
  - Usage: Provides a bidirectional interactive text-oriented communication facility using a virtual terminal connection.

10 Minute Break


05
Network
Linux Networking

Why Use Linux for Networking



Stable

can run for long periods without needing a reboot, andless prone to crashes and system failures

Secure

Built-in security, user permission, regular updates

Protocols

Linux supports a wide range of networking protocols (TCP/IP, UDP, HTTP, FTP, etc.)


06
Commands
In Linux Networking

Linux Commands

Ifconfig

View and configure IP addresses, netmasks, and broadcast addresses

ip

Similar to ifconfig but with additional capabilities

ping

Sends ICMP Echo Request packets to the target host and waits for an ICMP Echo Reply.

netstat

Useful for monitoring and troubleshooting network issues.

syslog

tail -f /var/log/messages

Wireshark

sudo apt-get install wireshark

Capture Network Traffic:

Open Wireshark and select the network interface to capture traffic from.
Click "Start" to begin capturing packets.
Use filters to narrow down the captured traffic, e.g., ip.addr == 192.168.1.1.

Analyze Captured Data:

Inspect packet details and headers.
Use protocol-specific dissectors to analyze data.

iftop

sudo apt-get install iftop

sudo iftop

Key Options:

-i [interface]: Specify the network interface to monitor, e.g., sudo iftop -i eth0.
-n: Disable DNS hostname resolution for faster performance.
-P: Show ports as well as IP addresses.

sudo iftop -i eth0 -n -P

nmap

sudo apt install nmap

nmap <hostname_or_IP>

Example:
nmap 192.168.1.1

nmap <ip>: Basic port scan.
nmap -sV <ip>: Service version detection.
sudo nmap -O <ip>: Operating system detection.
sudo nmap -A <ip>: Aggressive scan.
nmap -sn <ip>: Ping scan.

sudo ufw enable
sudo ufw disable

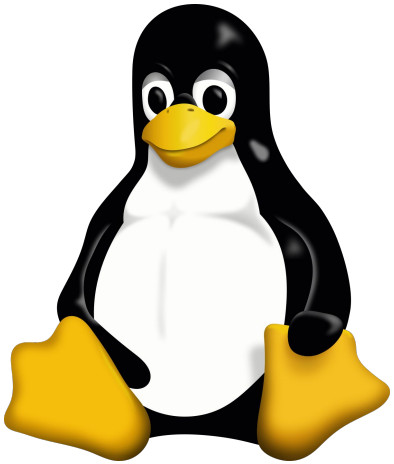
sudo ufw allow ssh
sudo ufw deny http

sudo ufw status

Firewall

Q/A Session

Thank you !



End of Day 7!

By Maya Mnaizel