Deep Dive into IPv4 Addressing

Foundation of Modern Network Communication

Understanding the architecture that powers billions of daily connections

Instructor-
Summary
Sharaf A. Roble

•***Cisco ,Juniper,AWS, and lead auditor*** *Certified.*

Founder *of* ***SONAK ACADEMY*** *(in person, and online session classes)*

•*Extensive experience in teaching and mentoring students, both* ***in-person and online***

•*Specializes in* ***Network Administration, Network Security, and troubleshooting Juniper, Cisco, HPE, and DELL*** *products*

•*Passionate about helping others learn about networking*

•*Committed to creating a positive and supportive learning environment*

Chapter Agenda

01

What is IPv4?

Core concepts and historical context

02

Why IPv4 Still Matters

Current relevance in modern networks

03

Address Structure

Breaking down 32-bit architecture

04

Address Classes

A, B, C, D, and E classifications

05

Address Types

Public, private, loopback, and more

06

Reserved Ranges

Special purpose address blocks

07

Subnetting & CIDR

Efficient network segmentation

What is IPv4?

Logical Addressing System

IPv4 enables devices to identify and communicate across interconnected networks using unique identifiers

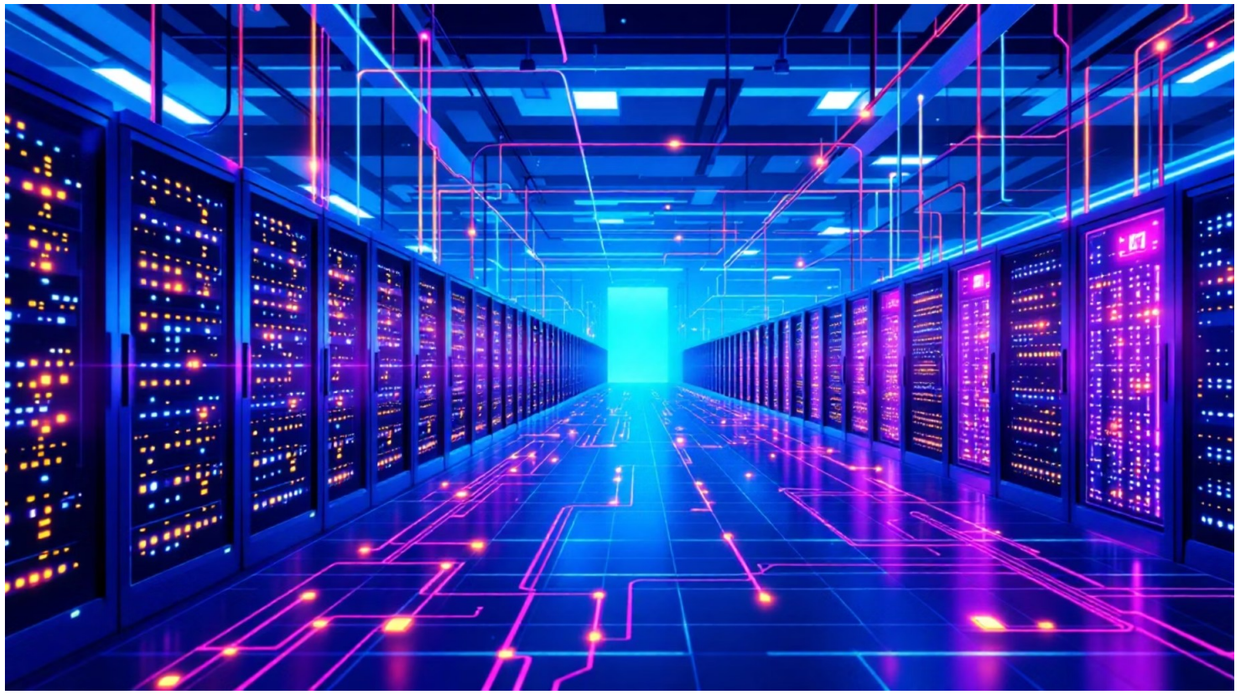
Historical Foundation

Introduced in 1981 as the fourth version of the Internet Protocol, establishing the basis for modern networking

32-Bit Architecture

Uses 32-bit addresses written in dotted decimal format, such as 192.168.1.1, supporting approximately 4.3 billion unique addresses

Why IPv4 Still Matters?



Internet Infrastructure Backbone

Despite IPv6 adoption, most networks and systems continue operating on IPv4 due to extensive infrastructure investment and compatibility requirements

Universal Support

Widely supported by routers, firewalls, applications, and legacy systems that form the backbone of enterprise and service provider networks

Fundamental Knowledge

Critical for understanding networking basics, troubleshooting connectivity issues, and planning efficient address allocation strategies

Structure of an IPv4 Address

Four Octets

Consists of four octets (8 bits each), totaling 32 bits of address space

Value Range

Each octet ranges from 0 to 255 in decimal notation

Binary Format

Example: 11000000.10101000.00000001.00000001 converts to 192.168.1.1

Address Components

Network ID

Identifies the specific network segment or subnet within the larger internetwork

Host ID

Identifies the individual device or host on that particular network segment

Classes of IPv4 Addresses

Class	*Range*	*Default Subnet Mask*	*Hosts/Network*	*Use Case*
Class A	*1.0.0.0 – 126.0.0.0*	*255.0.0.0 (/8)*	*~16 million*	*Very large organizations*
Class B	*128.0.0.0 – 191.255.0.0*	*255.255.0.0 (/12)*	*~65,000*	*Medium networks*
Class C	*192.0.0.0 – 223.255.255.0*	*255.255.255.0 (/16)*	*256*	*Small networks*
Class D	*224.0.0.0 – 239.255.255.255*	-	-	*Multicast*
Class E	*240.0.0.0 – 255.255.255.255*	-	-	*Reserved*

“Classful addressing is deprecated —
CIDR is what we use in real networks”

CIDR Notation (How & When)

Classless Inter-Domain Routing

Replaces class-based addressing system for more flexible and efficient IP allocation

CIDR Format

Example: 192.168.10.0/24 where /24 indicates first 24 bits are network bits

Advanced Features

Enables supernetting and Variable Length Subnet Masking (VLSM) for optimal address utilization

Before CIDR

Fixed class-based system (A, B, C) led to inefficient address allocation and wasted IP space

After CIDR

Flexible, variable-length subnet masks allow precise allocation matching actual network requirements

Types of IPv4 Addresses

Public Addresses

Routable on the internet and globally unique, assigned by IANA and regional internet registries

Private Addresses

Used exclusively in internal networks: Class A (10.0.0.0/8), Class B (172.16.0.0/12), Class C (192.168.0.0/16)

Loopback

127.0.0.1 reserved for testing and referring to the local machine itself

Broadcast

192.168.1.255 sends data to all hosts within a subnet simultaneously

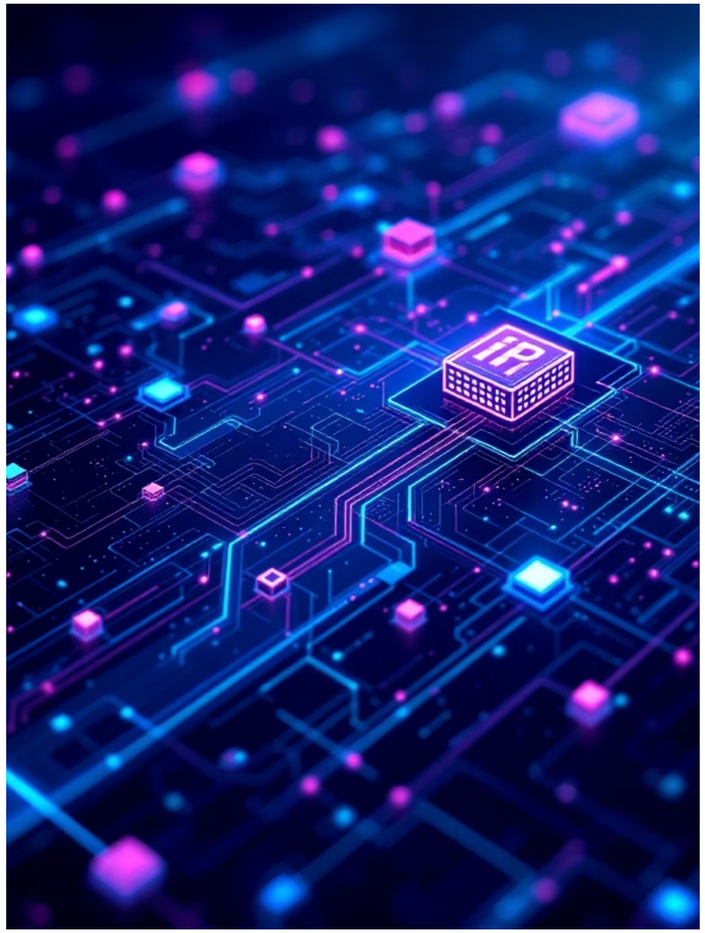
Network Address

Identifies the subnet itself, such as 192.168.1.0, cannot be assigned to hosts

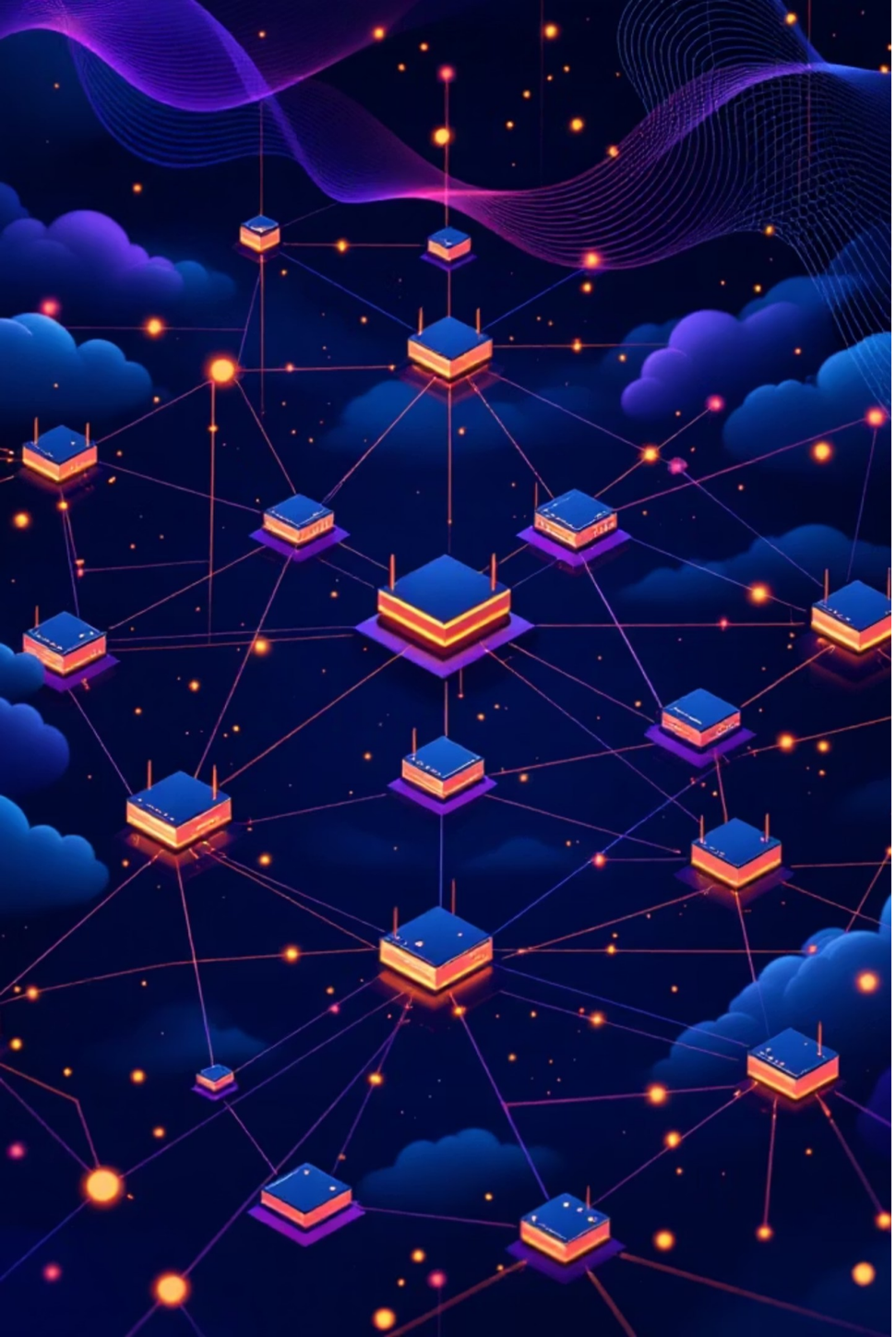
Link-Local (APIPA)

169.254.0.0/16 auto-assigned when no DHCP server is available for temporary connectivity

Reserved & Special IPv4 Ranges



Purpose	*Address Ranges*
Loopback	*127.0.0.0/8*
Private	*10.0.0.0/8, 172.16.0.0/12, 192.168.0.0/16*
Link-local (APIPA)	*169.254.0.0/16*
Multicast	*224.0.0.0 – 239.255.255.255*
Broadcast	*Last address in subnet*



Subnetting Explained (What & Why)

Network Segmentation

Breaks a large network into smaller, manageable segments called subnets

Performance Optimization

Reduces broadcast domain size and optimizes use of IP addresses

Security & Management

Enables better network management, security policies, and traffic control

Subnet Masks in Action

Example

IP Address: 192.168.10.5

Subnet Mask: 255.255.255.0

Notation: /24

Result

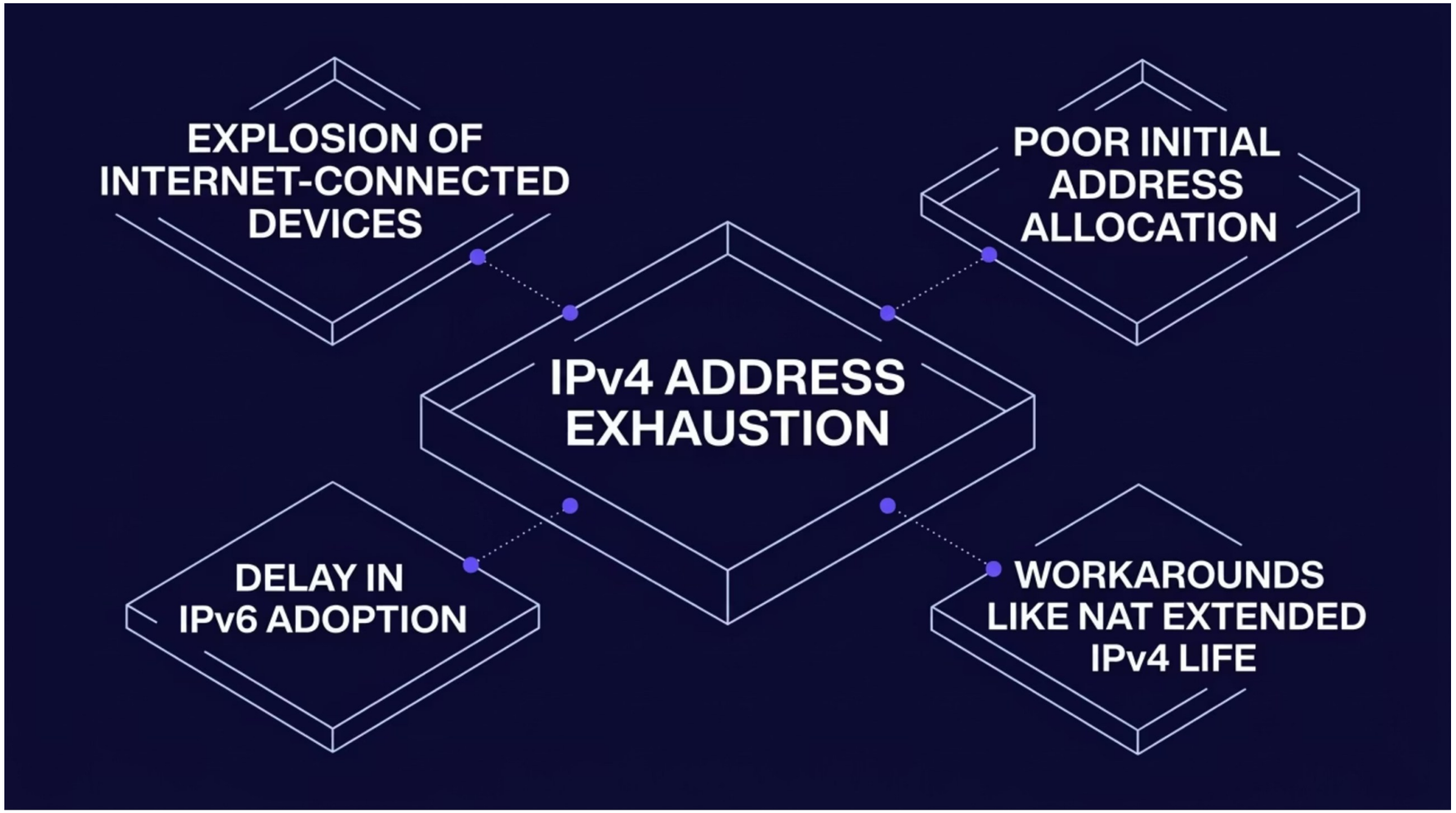
Network: 192.168.10.0

Broadcast: 192.168.10.255

Usable Hosts: 192.168.10.1–254

Why IPv4 Exhaustion Happened

Understanding the factors that led to the depletion of IPv4 addresses is crucial for grasping modern network challenges.



Who Manages the Internet?

Internet governance is a multi-stakeholder model involving various organizations, not a single central entity. It's a collaborative effort to maintain a stable, secure, and accessible global network.

ICANN

Coordinates global internet identifiers, including IP addresses and domain names, ensuring unique and consistent allocation.

IETF

Develops and promotes internet standards (e.g., TCP/IP, HTTP) through open, collaborative processes.

RIRs

Regional Internet Registries allocate IP addresses and autonomous system numbers within specific geographic regions.

How Regional Internet Registries (RIRs) Work

RIRs play a critical role in the organized distribution and management of IP addresses, ensuring that every device connected to the internet has a unique identifier.

Receive from IANA

RIRs receive large blocks of IP addresses from the Internet Assigned Numbers Authority (IANA), which oversees global IP address space.

Allocate to LIRs

They then distribute these address blocks to Local Internet Registries (LIRs), primarily Internet Service Providers (ISPs) and large end-user organizations within their designated geographic region.

Maintain Registration

Each RIR maintains public databases, such as WHOIS, to accurately record and track IP address assignments, ensuring global uniqueness and assisting with network troubleshooting.

Develop Policies

RIRs facilitate policy development through a bottom-up process, allowing their community members (ISPs, governments, academia, technical experts) to collaboratively define rules for IP address allocation.

IP Geolocation & Privacy: A Double-Edged Sword

IP addresses are essential for internet communication, but they can also reveal an approximate location, ISP, and browsing patterns — creating real privacy tradeoffs.

The Threat

Tracking & Profiling

Used by websites and advertisers to build user profiles and target ads.

Censorship & Surveillance

Can be used to monitor activity or restrict access by region.

Cybersecurity Risks

Location data can help power social engineering and other attacks.

The Shield

VPNs & Proxies

Hide your real IP by routing traffic through another server.

Tor Network

Routes traffic through multiple relays to make tracing difficult.

Browser Privacy

Adjust settings and use extensions to reduce IP-based tracking.

GDPR and similar laws limit how IP data can be collected and used, requiring consent and stronger data rights.

IP Spoofing & IPv4 Security

IP spoofing is a technique where an attacker disguises their identity by falsifying the source IP address in network packets, making it appear as if the packets originate from a legitimate source.

Falsified Source IP

Attackers send packets with a forged source IP address to conceal their true origin and impersonate trusted entities.

IPv4 Vulnerability

IPv4 lacks inherent mechanisms to verify the source IP address, making it susceptible to spoofing without additional security measures.

Mitigation Strategies

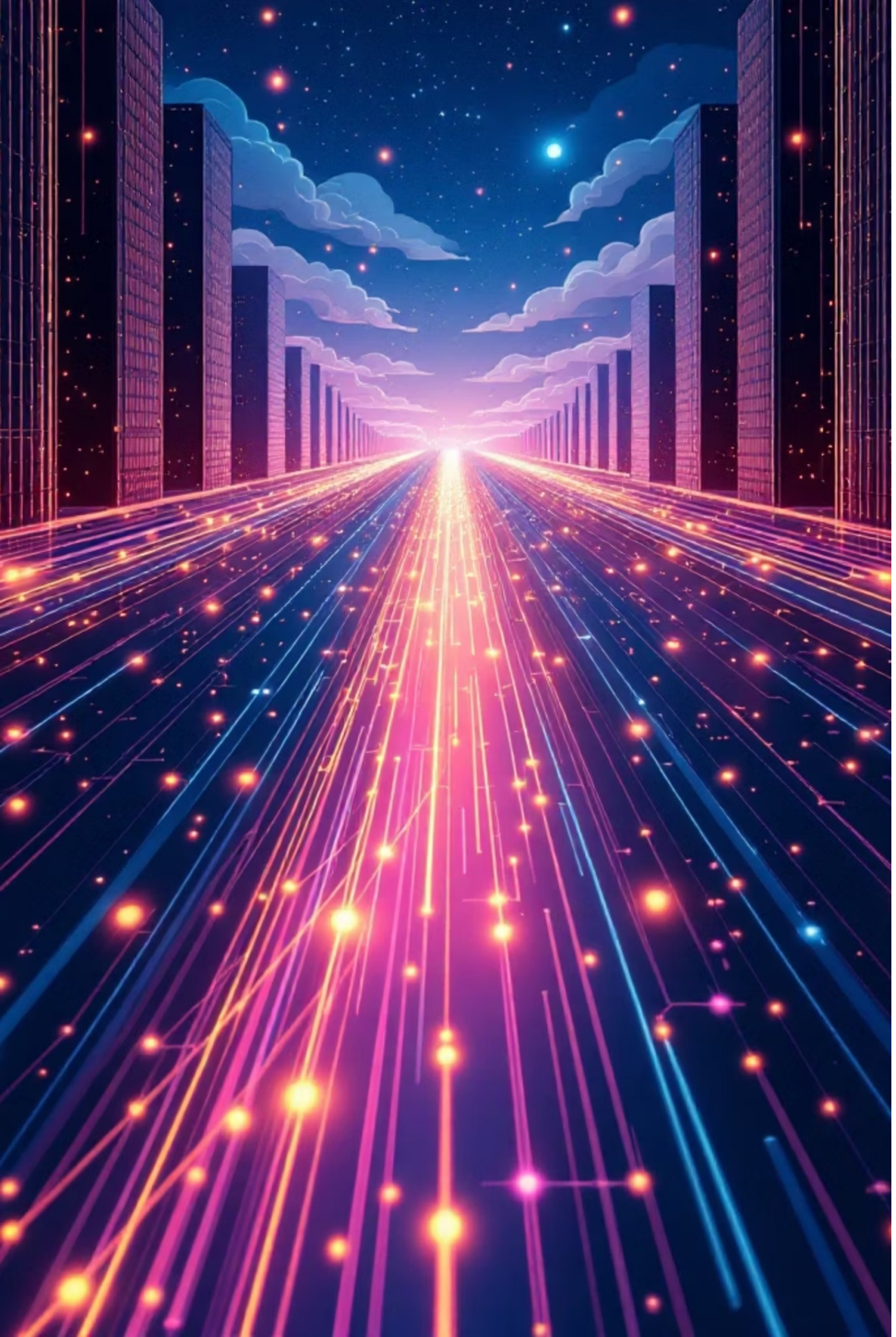
Implement firewalls, ingress filtering, and robust authentication protocols to validate packet origins and prevent spoofing.

Common Attack Types

Often used in Distributed Denial-of-Service (DDoS) attacks, some phishing attempts, and man-in-the-middle scenarios.

Real-World Impact

Can lead to data breaches, service disruptions, and compromised systems, affecting businesses and individuals alike.



IPv4 to IPv6: The Great Transition

The internet's continuous evolution necessitates a transition from IPv4 to IPv6, a process marked by coexistence and strategic migration.

The Need for IPv6

IPv6 was developed to address IPv4's address exhaustion and introduce features like better security, auto-configuration, and improved routing efficiency.

Parallel Operation (Coexistence)

Today, both IPv4 and IPv6 protocols run in parallel on the internet, allowing devices to communicate regardless of their native IP version.

Dual-Stack Networks

Many organizations implement dual-stack networks, where devices are configured to support both IPv4 and IPv6 simultaneously to ensure seamless connectivity.

Tunneling & Translation

Mechanisms like 6to4 and Teredo enable IPv6 traffic to traverse IPv4 networks, acting as temporary bridges during the transition phase.

Gradual Migration & Challenges

The transition is a gradual process, not a hard cutover. Challenges include legacy system compatibility, training, and the ongoing dominance of IPv4, though IPv6 adoption is steadily growing.

Network Design Scenarios: From Small Office to Enterprise

Effective network design adapts to organizational scale, balancing connectivity, security, and manageability. Here's how IP addressing strategies evolve across different environments.

1

Small Office

IP Range: *Typically Class C private (e.g., 192.168.1.0/24).*

Subnets: *Often a single subnet for all devices.*

IP Allocation: *DHCP for most, static for printers/servers.*

Addresses: *Private IPs internally, NAT for internet access.*

Segmentation: *Basic, e.g., separate guest Wi-Fi.*

2

Medium Enterprise

IP Range: *Class B private (e.g., 172.16.0.0/16).*

Subnets: *Multiple subnets for departments (Sales, HR, IT).*

IP Allocation: *DHCP for user devices, static for critical infrastructure.*

Addresses: *Primarily private, public for external services.*

Segmentation: *VLANs for departmental separation and traffic control.*

3

Large Organization

IP Range: *Class A private (e.g., 10.0.0.0/8) or supernetting.*

Subnets: *Extensive VLSM across many locations and departments.*

IP Allocation: *Centralized DHCP, extensive static IPs for infrastructure.*

Addresses: *Public IPs for servers, private for internal hosts.*

Segmentation: *Advanced with firewalls, ACLs, and zero-trust principles.*

Key Design Considerations

Planning for Growth

- *Reserve address space for future expansion.*
- *Implement scalable subnetting schemes (VLSM).*
- *Document IP assignments and network topology thoroughly.*

Public vs. Private Addresses

- *Use private addresses for internal networks to conserve public IPs.*
- *Public IPs are needed for internet-facing services and direct external access.*
- *Utilize NAT (Network Address Translation) to bridge private networks to the internet.*

DHCP vs. Static IP

- *DHCP for dynamic assignment to end-user devices (laptops, phones) for ease of management.*
- *Static IPs for critical infrastructure (servers, routers, firewalls) requiring consistent addresses.*

Network Segmentation

- *Isolate different departments or types of devices (e.g., IoT, guest Wi-Fi) into separate subnets/VLANs.*
- *Enhances security by limiting the scope of breaches and controlling traffic flow.*
- *Improves performance by reducing broadcast traffic and localizing communication.*

IPv4 Troubleshooting & Diagnostic Tools

Diagnose and resolve common network issues using essential command-line utilities.

Ping

Checks basic connectivity and measures round-trip time to a network host. Use to confirm if a server is online and responding.

Traceroute / Tracert

Maps the network path (hops) that packets take to reach a destination. Useful for identifying where network congestion or failures occur.

Netstat

Shows active network connections, routing tables, and network interface statistics. Helps identify open ports and suspicious connections.

IPConfig / IfConfig

Displays your local machine's IP configuration (IP address, subnet mask, default gateway). Essential for checking your own network settings.

NSLookup / Dig

Queries DNS servers to resolve domain names to IP addresses, or vice-versa. Crucial for diagnosing DNS resolution problems.

ARP

Manages the Address Resolution Protocol cache, mapping IP addresses to physical (MAC) addresses on the local network segment.