CS-041 · Network

TCP/IP

The four-layer protocol suite that actually runs the internet.

Executive Summary

TCP/IP is the protocol suite that powers the internet and virtually every modern network. It is organized into four layers and pairs the Internet Protocol, which addresses and routes packets, with transport protocols like TCP for reliable delivery and UDP for fast, connectionless delivery. Understanding it is essential for anyone who defends or builds networked systems.

What It Is

TCP/IP stands for Transmission Control Protocol and Internet Protocol, the two most important members of a larger family of protocols that carry data across the internet. The model is usually described in four layers: the Link layer handles the local physical network, the Internet layer addresses and routes packets between networks using IP, the Transport layer manages end-to-end delivery using TCP or UDP, and the Application layer provides services to software such as web, email, and file transfer. Unlike the seven-layer OSI reference model, TCP/IP is the practical stack that real devices implement and run.

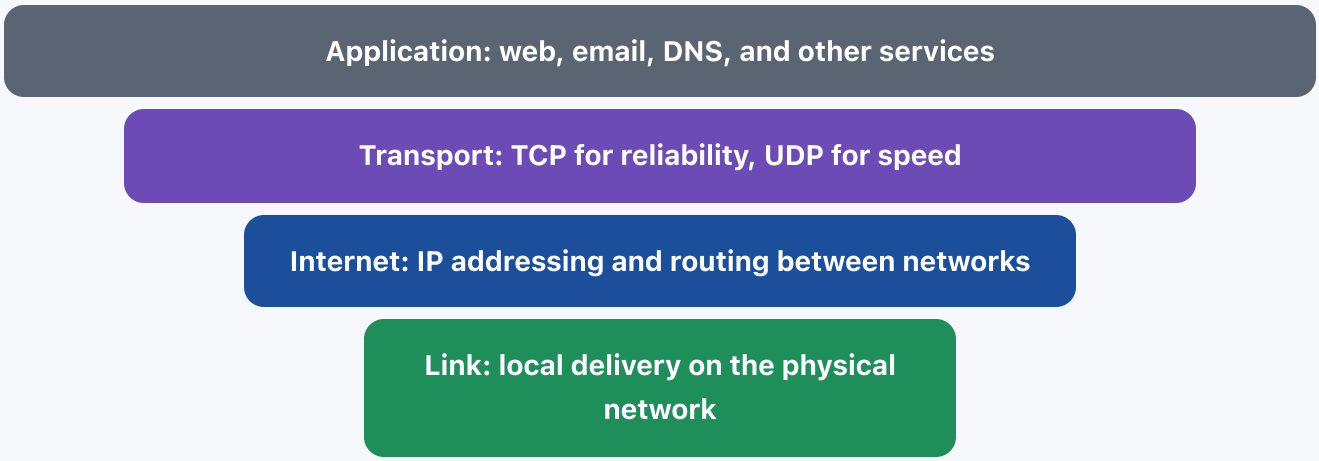
Why It Matters

Almost all business and consumer communication depends on TCP/IP, so every security professional needs to understand it. Attackers exploit its behaviors, such as flooding the connection setup process or spoofing IP addresses, and defenders build firewalls, intrusion detection, and monitoring around its packets and ports. Knowing how addressing, routing, and reliable delivery work lets a professional read traffic, spot anomalies, and design controls that actually match how data moves. For career growth, TCP/IP fluency separates people who can only follow runbooks from those who can diagnose and reason about a network.

How It Works

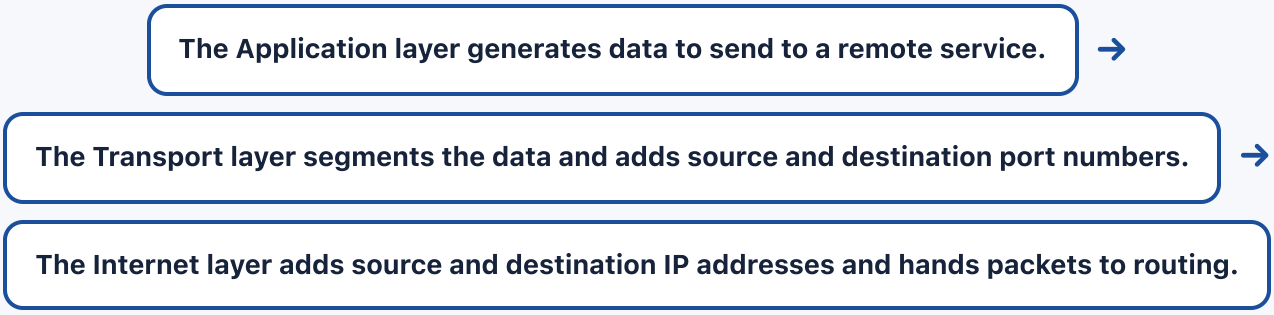
When one device sends data to another, the Application layer produces the data, the Transport layer breaks it into segments and adds port numbers, the Internet layer wraps each segment in a packet with source and destination IP addresses, and the Link layer frames it for the local medium. TCP provides reliable, ordered delivery by establishing a connection with a three-way handshake (SYN, SYN-ACK, ACK), numbering bytes, acknowledging receipt, and retransmitting lost data. UDP skips the handshake and delivery guarantees, trading reliability for speed and low overhead, which suits streaming, voice, and DNS lookups. IP addresses identify hosts, ports identify the specific service on a host, and routers forward packets toward their destination one hop at a time.

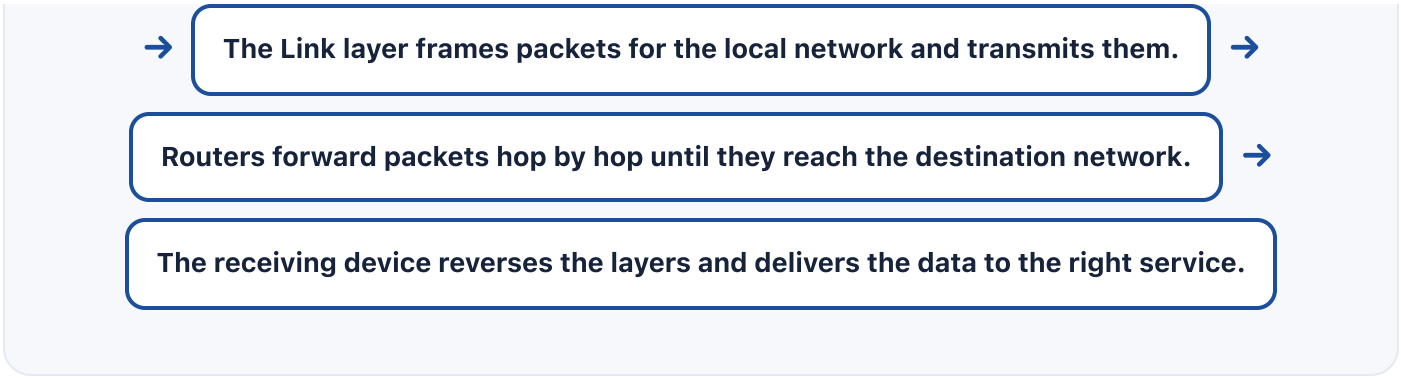
Architecture Diagram



The four TCP/IP layers. Data descends from application to link on send and ascends on receive, with TCP or UDP handling transport.

Visual Workflow





Common Attacks

- SYN flood attacks that exhaust a server by leaving handshakes half-open
- IP spoofing that forges source addresses to hide origin or bypass filters
- TCP session hijacking that takes over an established connection
- UDP-based amplification and reflection attacks that overwhelm targets
- Packet sniffing of unencrypted traffic to capture credentials and data

Common Mistakes

- Assuming TCP/IP traffic is private when it is unencrypted by default
- Confusing IP addresses (the host) with port numbers (the service)
- Treating UDP as unreliable and unimportant when many core services depend on it
- Overlooking the difference between the OSI reference model and the real TCP/IP stack
- Filtering only by IP and ignoring that source addresses can be spoofed

Best Practices

- Encrypt sensitive traffic in transit rather than trusting the network
- Filter and rate-limit traffic to blunt flooding and amplification attacks
- Use stateful firewalls that track connection state rather than only ports
- Baseline normal traffic so anomalies in flows and ports stand out
- Apply anti-spoofing filtering at network edges to reject forged source addresses

Quick Checklist

- [x] Can explain the four TCP/IP layers and their jobs
- [x] Can describe the TCP three-way handshake step by step
- [x] Can state when to use TCP versus UDP
- [x] Understands the difference between an IP address and a port number
- [x] Knows how anti-spoofing and stateful filtering reduce common attacks

Recommended Tools

Packet analyzer
Captures and inspects TCP/IP packets and connection state

Port scanner
Discovers which TCP and UDP services a host exposes

Ping and traceroute
Test reachability and trace the routed path to a host

netstat or ss
Lists active connections and listening ports on a system

Industry Standards

RFC 791 (IP)
Defines the Internet Protocol and packet structure

RFC 793 (TCP)
Defines the Transmission Control Protocol and its handshake

RFC 768 (UDP)
Defines the connectionless User Datagram Protocol

Career Relevance

TCP/IP is core knowledge for network security engineers, SOC analysts, security engineers, and cloud security engineers, and it is tested in almost every technical interview at every level. Analysts read packet captures and flow logs built on it, engineers design segmentation and

filtering around it, and incident responders trace attacks through it. It is one of the most durable skills in the roles that AI-Governance-Jobs.com serves.

Interview Questions

- Walk me through the TCP three-way handshake.
- When would you choose UDP over TCP, and what do you give up?
- How does the four-layer TCP/IP model differ from the seven-layer OSI model?
- What is a SYN flood, and how does it abuse TCP connection setup?
- How does a packet get from your laptop to a server across the internet?

Related Certifications

CompTIA Network+ | **CompTIA Security+** | **Cisco CCNA**

Further Reading

- IETF RFC 793: Transmission Control Protocol
- IETF RFC 791: Internet Protocol
- NIST Computer Security Resource Center Glossary

Key Takeaways

- TCP/IP is the practical four-layer stack that runs the internet.
- TCP gives reliable, ordered delivery; UDP gives fast, connectionless delivery.
- The three-way handshake establishes every TCP connection.
- IP addresses identify hosts and ports identify services on those hosts.
- TCP/IP fluency is foundational for defending and building networks.

FAQ

▶ **What is the difference between TCP and UDP?**

▶ **What is the three-way handshake?**

▶ **Is TCP/IP secure by itself?**

Related Careers

RELATED ROLES

Network Security Engineer

Soc Analyst | Cloud Security Engineer

RELATED CERTIFICATIONS

CompTIA Network+

CompTIA Security+ | Cisco CCNA

CURRENT OPENINGS

Live roles are on the job board.

Browse all jobs

GUIDES & SALARY

Career guides | Role roadmaps

Salary data | Career tools

SUGGESTED LEARNING PATH

1. Ground the basics with CS-001 Cybersecurity
2. Study this sheet: **TCP/IP**
3. Go deeper: The OSI Model
4. Go deeper: Ports & Protocols
5. Validate it: work toward **CompTIA Network+**
6. Find the role: browse current openings

RELATED SHEETS

CS-040 The OSI Model | CS-042 Ports & Protocols | CS-043 Firewalls | CS-046 NAT

CS-001 Cybersecurity