CS-040 · Network

The OSI Model

A seven-layer map for understanding how data moves across a network.

Executive Summary

The OSI model is a conceptual framework that breaks network communication into seven stacked layers, each with a defined job. It gives engineers a shared vocabulary for describing where a problem, a protocol, or an attack lives. Although real networks run on the TCP/IP model, the OSI model remains the standard teaching and troubleshooting reference.

What It Is

The Open Systems Interconnection (OSI) model is a reference framework standardized by the International Organization for Standardization that divides the work of moving data between two systems into seven distinct layers. From the bottom up they are: Physical, Data Link, Network, Transport, Session, Presentation, and Application. Each layer performs a specific function and communicates only with the layers directly above and below it, passing data through well-defined boundaries. As data is sent, it moves down the stack and each layer wraps it with its own control information, a process called encapsulation. On the receiving side the data moves back up the stack and each layer strips off the information meant for it.

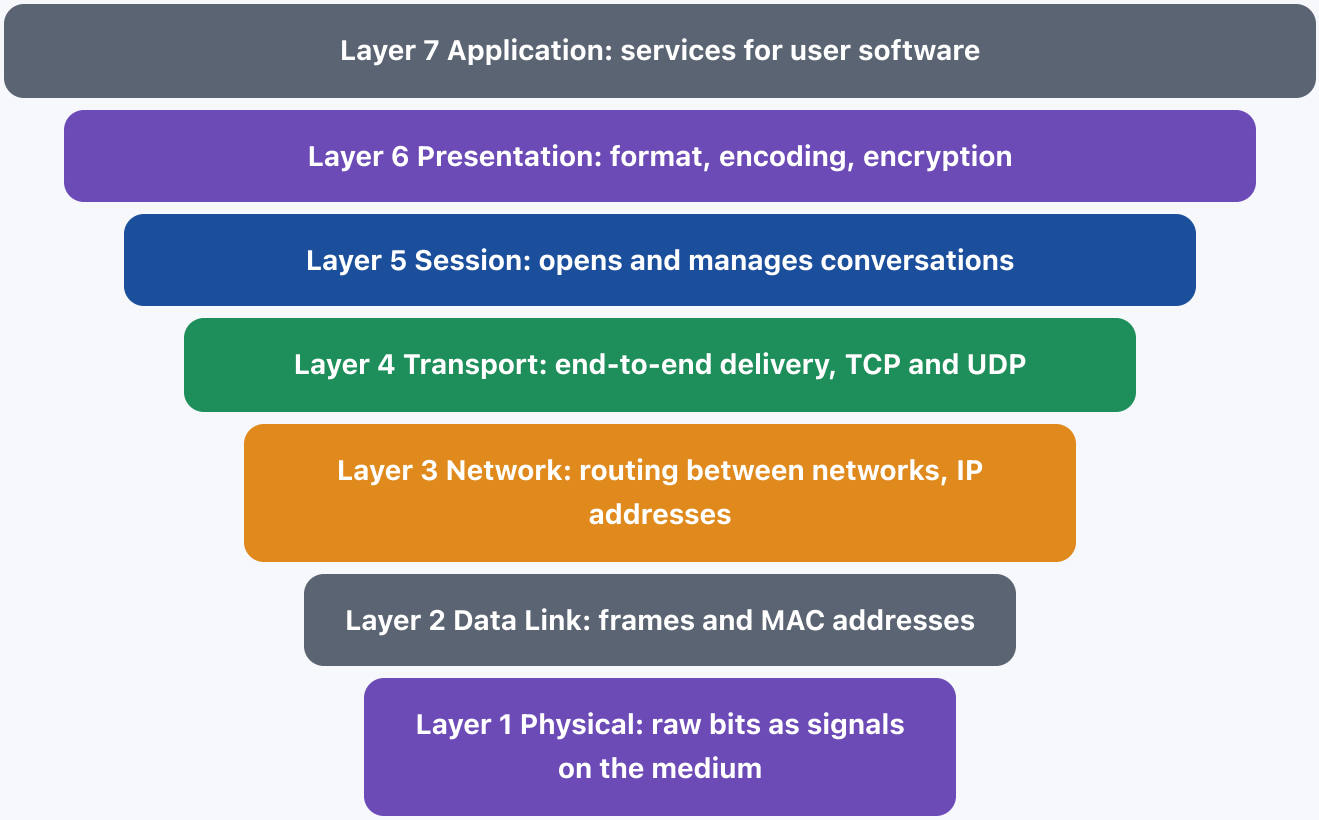
Why It Matters

The OSI model matters because it turns a messy, invisible process into a structured map that people can reason about together. When something breaks, an engineer can ask which layer is failing: is it a cable and signal issue at Layer 1, an addressing issue at Layer 3, or an application response issue at Layer 7. Security professionals use the same map to place controls and attacks precisely. Firewalls, encryption, and monitoring all operate at particular layers, and knowing which is which prevents wasted effort. For anyone building a networking or security career, fluency in the seven layers is expected in interviews and daily work.

How It Works

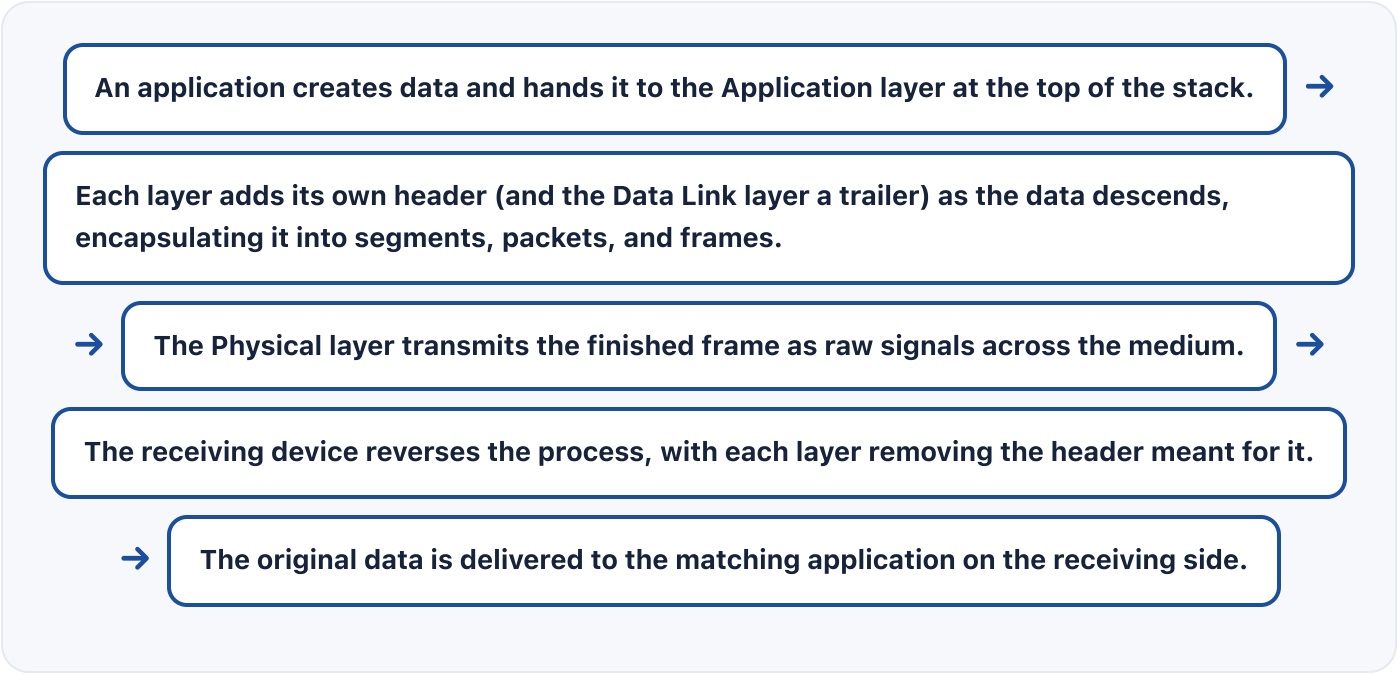
Communication flows down the stack on the sending device and up the stack on the receiving device. The Physical layer moves raw bits as electrical, optical, or radio signals. The Data Link layer packages bits into frames and handles local delivery using hardware (MAC) addresses. The Network layer routes packets between networks using logical (IP) addresses. The Transport layer provides end-to-end delivery, ordering, and reliability, and this is where TCP and UDP live. The Session layer manages the dialogue between applications, opening and closing conversations. The Presentation layer handles data format, encoding, and encryption so both sides interpret data the same way. The Application layer is closest to the user and provides network services to software, such as web browsing and email. A common memory aid reads the layers from Layer 1 to Layer 7 as Please Do Not Throw Sausage Pizza Away.

Architecture Diagram



The seven OSI layers, from raw signal at the bottom to user-facing services at the top. Data is encapsulated on the way down and decapsulated on the way up.

Visual Workflow



Common Attacks

- Cable tapping and physical signal interception at Layer 1
- MAC address spoofing and ARP poisoning at Layer 2
- IP spoofing and routing manipulation at Layer 3
- SYN floods and other transport-layer denial-of-service at Layer 4
- Application-layer attacks such as injection and HTTP floods at Layer 7

Common Mistakes

- Confusing the OSI model with the real protocol stack, which follows the TCP/IP model
- Memorizing layer names without understanding what each layer actually does
- Assuming a problem is always at Layer 7 when it is often lower in the stack
- Placing a security control at the wrong layer for the threat it should stop
- Ignoring the Data Link and Physical layers when troubleshooting connectivity

Best Practices

- Troubleshoot from the bottom of the stack upward to isolate faults quickly
- Map each security control and monitoring tool to the layer it protects
- Use the layer model as a shared vocabulary in incident and design discussions

- Remember that encryption and application logic differ, and treat them separately
- Cross-reference OSI layers with their TCP/IP equivalents when reading real traffic

Quick Checklist

- [x] Can name all seven layers in order, top to bottom and bottom to top
- [x] Can state the primary job of each layer in one sentence
- [x] Can place TCP, UDP, IP, and MAC addresses at the correct layer
- [x] Can identify which layer a given attack or control operates at
- [x] Can map each OSI layer to the four-layer TCP/IP model

Recommended Tools

Packet analyzer
Shows how data is encapsulated across layers in captured traffic

Cable and link tester
Verifies Physical and Data Link layer connectivity

Ping and traceroute
Tests Network layer reachability and the path packets take

Protocol reference chart
Maps common protocols to their OSI layers

Industry Standards

ISO/IEC 7498-1
The formal standard that defines the OSI reference model

IEEE 802 family
Defines Data Link and Physical layer standards for LANs and wireless

IETF RFCs
Define the transport and network protocols mapped onto the model

Career Relevance

The OSI model is foundational knowledge for network engineers, network security engineers, SOC analysts, and security engineers, and it appears in nearly every entry-level networking and security interview. Cloud security engineers use it to reason about virtual networks and traffic flow. Understanding the layers lets professionals communicate precisely about where problems and defenses belong, which is a daily requirement across the roles that AI-Governance-Jobs.com serves.

Interview Questions

- Name the seven OSI layers in order and give the main function of each.
- At which layer do TCP and UDP operate, and how does that differ from IP?
- How does the OSI model map to the four-layer TCP/IP model?
- Which OSI layer would you investigate first for an ARP spoofing attack, and why?
- Explain encapsulation and what happens to data as it moves down the stack.

Related Certifications

CompTIA Network+ | CompTIA Security+ | Cisco CCNA

Further Reading

- NIST Computer Security Resource Center Glossary
- IETF: The Internet Standards Process
- CISA: Securing Network Infrastructure Devices

Key Takeaways

- The OSI model splits networking into seven layers, each with a defined job.
- Data is encapsulated as it moves down the stack and decapsulated on the way up.
- It is a teaching and troubleshooting reference, while real traffic uses TCP/IP.
- Security controls and attacks each live at specific layers, so placement matters.

- Fluency in the seven layers is expected across networking and security careers.

FAQ

Related Careers

RELATED ROLES

Network Security Engineer

Soc Analyst | 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: **The OSI Model**
3. Go deeper: TCP/IP
4. Go deeper: Ports & Protocols
5. Validate it: work toward **CompTIA Network+**

6. Find the role: browse current openings

RELATED SHEETS

CS-041 TCP/IP | CS-042 Ports & Protocols | CS-043 Firewalls | CS-047 Intrusion Detection Systems (IDS) | CS-001 Cybersecurity