WHAT IS THE OSI MODEL? THE 7 LAYERS EXPLAINED

Understanding the OSI Model

The Open Systems Interconnection (OSI) model is a conceptual framework that divides network communication into seven abstract layers, providing a standardized approach for different computer systems, applications and network devices to communicate across networks.

Developed by the International Organization for Standardization (ISO), the OSI model emerged as a solution to communication incompatibilities between diverse networking protocols. It gives developers and engineers a categorical approach to building interoperable hardware and software for computer networking.
At each layer of the stack, the model provides guidelines for network components and their computing functions, defining how data flows from physical transmission to application interfaces.

The seven layers of the OSI model

- Layer 1: Physical Layer

The OSI model provides tasks for engineers to complete in building each layer of network architecture. This theoretical approach enables developers to visualize and build complex networks even without prior knowledge of networking systems. Although not the direct basis for modern networking technologies, it profoundly impacted computing standards development and shaped contemporary understanding of how networks function.

Why ISO developed the OSI model

In the late 1970s, computer systems were increasingly interconnected, but manufacturers developed proprietary networking solutions, creating non-interoperable systems that locked organizations into single-vendor ecosystems.

Early efforts like ARPANET and the TCP/IP protocol suite made progress but highlighted the need for a universal framework. In 1984, ISO published the OSI model. Its layered configuration enables disparate systems to communicate despite differences in underlying architectures and protocols.

The OSI model remains integral to understanding network architecture. Whether designing a local area network (LAN) or managing complex global networks, it provides a clear, structured approach.

The three categories of OSI layers

Data moves bidirectionally through these layers, with each layer communicating with the layers above and below it.

- **Software layers** (Layers 5-7): Application, presentation and session layers handle software-level transmissions.
- **Transport layer** (Layer 4): Bridges software and hardware, managing end-to-end data delivery.
- **Hardware layers** (Layers 1-3): Network, data link and physical layers handle transmission through physical network components.

Data flow example

Email transmission example: When you send an email, data traverses all seven layers:

- **Layer 7 (Application):** Email client uses SMTP to prepare the message.
- **Layer 6 (Presentation):** Compresses and encrypts the data for secure transmission.
- **Layer 5 (Session):** Establishes and maintains the connection between your device and mail server.
- **Layer 4 (Transport):** TCP breaks the email into segments with sequence numbers, manages flow control and ensures reliable delivery.
- **Layer 3 (Network):** Adds IP addresses and routes packets across different networks through nodes.
- **Layer 2 (Data link):** Creates frames with MAC addresses for local network segment transmission with error detection.
- **Layer 1 (Physical):** Converts frames to bits—electrical signals, light pulses, or radio waves—for physical transmission.

At the receiving end, the process reverses: the physical layer receives bits, layers process them

upward, and the email arrives in the recipient's inbox.

The seven layers of the OSI model

Layer 7: The application layer

The application layer is the OSI layer closest to end users. It provides network services directly to user applications and facilitates communication between software and lower layers. The application layer enables applications like web browsers, email clients and file transfer programs to initiate network communication.

Applications themselves aren't part of this layer. Rather, the application layer provides the protocols that enable software to send and receive data.

Key protocols:

- **HTTP** and **HTTPS** for web communication and secure connections
- **FTP** and **SFTP** for file transfers between networked computers
- **SMTP** for email transmission between mail servers
- **DNS** for translating domain names into IP addresses
- **POP3** and **IMAP** for retrieving email
- **SNMP** for network management and monitoring
- **SSH** and **Telnet** for remote access to network devices

Key functions

- **Resource identification:** The application layer determines resource availability before initiating communication.
- **Directory services:** Provides shared databases of information about network devices and users to facilitate resource management.
- **Communication synchronization:** Manages timing and coordination between applications for data transfer.

Layer 6: The Presentation Layer

The presentation layer transforms data into formats the application layer can process, acting as the data translator between systems with different data representation methods. It's sometimes called the "syntax layer" for converting data and graphics into displayable formats.

Key functions

- **Data translation**: Converts data between different encoding systems (EBCDIC to ASCII, for instance) during encapsulation as outgoing messages move down the protocol stack. During de-encapsulation, incoming messages undergo reverse conversion.
- **Data compression**: Reduces data stream size for efficient transmission and decompresses for use at the destination.
- **Encryption and decryption**: Uses SSL/TLS protocols to secure transmission, protecting data during network communications.

- **Format handling**: Manages image compression (JPEG, GIF) and video compression (MPEG, H.264) for multimedia data transfer.

The presentation layer ensures seamless data transfer across systems with different architectures by handling all format conversions transparently.

Layer 5: The Session Layer

The session layer manages communication sessions between nodes, handling establishment, maintenance and termination of connections. The session layer keeps connections open long enough to transmit necessary data, then closes them to preserve network resources.

Key functions

- **Session establishment**: Initiates connections between local and remote applications, managing user logon and authentication protocols.
- **Session maintenance**: Manages connection state during active data transfer, coordinating communication between devices.
- **Synchronization**: Implements checkpoints in data streams, enabling recovery if network communications are interrupted.
- **Session termination**: Closes connections when complete, managing user logoff procedures.
- **Session recovery**: Manages session failures and re-establishes connections when network problems occur.

The session layer is explicitly implemented in network environments utilizing remote procedure calls and is critical for applications requiring persistent connections like web conferencing, where it establishes protocols for connecting audio and video streams.

Common protocols

- Remote Procedure Call Protocol (RPC)
- Point-to-Point Tunneling Protocol (PPTP)
- Session Control Protocol (SCP)
- Session Description Protocol (SDP).

Layer 4: The transport layer

The transport layer ensures reliable end-to-end data delivery between hosts across networks. As the heart of the OSI Model, it receives data from the session layer, breaks it into segments or datagrams, and manages reliable delivery to destination nodes.

Key functions

- **Segmentation and reassembly**: Divides messages into smaller segments for efficient data transfer, adds sequence numbers for proper ordering, then reassembles segments at the receiving device.
- **Flow control**: Regulates transmission rates to prevent buffer overflow at the receiver, ensuring smooth data transfer without overwhelming network resources.
- **Error control**: Checks segments for errors using checksums and manages retransmission of

corrupted segments to ensure data integrity.
- **Service-point addressing**: Uses port numbers to enable multiplexing, allowing multiple applications to use the same network connection simultaneously.
- **Congestion control**: Manages bandwidth allocation and prevents network bottlenecks by adjusting transmission rates based on network conditions.
- **Connection management**: Establishes, maintains and terminates connections between communicating nodes.

The transport layer provides two types of service:

- **Connection-oriented service (TCP)**: Transmission Control Protocol provides reliable delivery with three-way handshake. TCP divides data into numbered segments that are acknowledged and reassembled at the destination, with retransmission for lost or corrupted segments. Used for web browsing, email and file transfers where accuracy is critical.
- **Connectionless service (UDP)**: User Datagram Protocol offers faster transmission without acknowledgment, reducing overhead and latency. Ideal for real-time applications like video streaming, online gaming, VoIP and DNS queries where speed matters more than accuracy.

Layer 3: The network layer

The network layer manages data transmission between multiple networks, enabling internetworking. It uses routers and layer 3 switches with IPv4 (32-bit addresses) and IPv6 (128-bit addresses) protocols to route data across different networks.

The network layer allows nodes with unique IP addresses to send messages to nodes on different networks, determining the best path through intermediate networks and nodes.

Key functions:

- **Logical addressing**: Uses IP addresses to identify and locate nodes across different networks, enabling internetwork communication.
- **Routing**: Determines the best path for data transmission across intermediate networks, considering factors like congestion, network topology and routing metrics.
- **Packet fragmentation and reassembly**: Splits packets exceeding maximum transmission unit (MTU) limits into smaller units for transmission through network segments with different capacity constraints, then reassembles them at the destination.
- **Traffic management**: Implements quality of service (QoS) policies for different traffic types, prioritizing time-sensitive data.
- **Internetwork communication**: Connects LANs to WANs across heterogeneous networks, enabling global data transfer.

The network layer uses IP addresses to route data between nodes on different networks. Supporting protocols include ICMP (Internet Control Message Protocol) for error reporting and network diagnostics, and IGMP (Internet Group Management Protocol) for multicast communication.

Reliability isn't guaranteed at the network layer—while many protocols offer reliable message delivery, error reporting isn't mandatory, so senders may not receive delivery confirmation.

Layer 2: The data link layer

The data link layer manages error-free data transfer between devices on the same local network segment. This layer receives packets from the network layer and organizes them into frames for transmission across the physical medium.

Two sublayers

- **Logical Link Control (LLC)**: Serves as interface between MAC and network layer, handling flow control, synchronization, error controls and protocol multiplexing where multiple data streams share a single connection.
- **Media Access Control (MAC)**: Controls how devices access network media and transmit data. Uses MAC addresses (hardware addresses on network interface cards) to identify devices on the local network segment.

Key functions

- **Framing**: Encapsulates packets with headers and trailers containing MAC addresses and error-checking codes. Attaches special bit patterns to mark frame boundaries, making transmissions meaningful to the receiving device.
- **Physical addressing**: Uses MAC addresses for local network identification, enabling devices to communicate on the same network segment.
- **Error detection**: Implements cyclic redundancy check (CRC) to detect damaged or lost frames and manages retransmission to ensure data integrity during network communications.
- **Access control**: When multiple devices share a communication channel, the MAC sublayer determines which device has control at any given moment using protocols like CSMA/CD (Carrier Sense Multiple Access with Collision Detection) for Ethernet and CSMA/CA (Collision Avoidance) for Wi-Fi.
- **Flow control**: Regulates transmission rates between devices to prevent receiver buffer overflow.

The data link layer ensures reliable frame delivery between directly connected nodes on the same network segment. Technologies include Ethernet (IEEE 802.3), Wi-Fi (IEEE 802.11), Point-to-Point Protocol (PPP), HDLC (High-Level Data Link Control), and ARP (Address Resolution Protocol) for mapping IP addresses to MAC addresses.

Layer 1: The physical layer

The physical layer comprises the physical network components that transmit raw data as bits between devices across physical media—using electrical signals, optical signals or electromagnetic signals through physical infrastructure.

This is where troubleshooting often begins. The physical layer includes hardware for data transmission: copper cables (twisted pair, coaxial), fiber optic cables, radio frequencies for wireless, network interface cards, routers, repeaters and hubs.

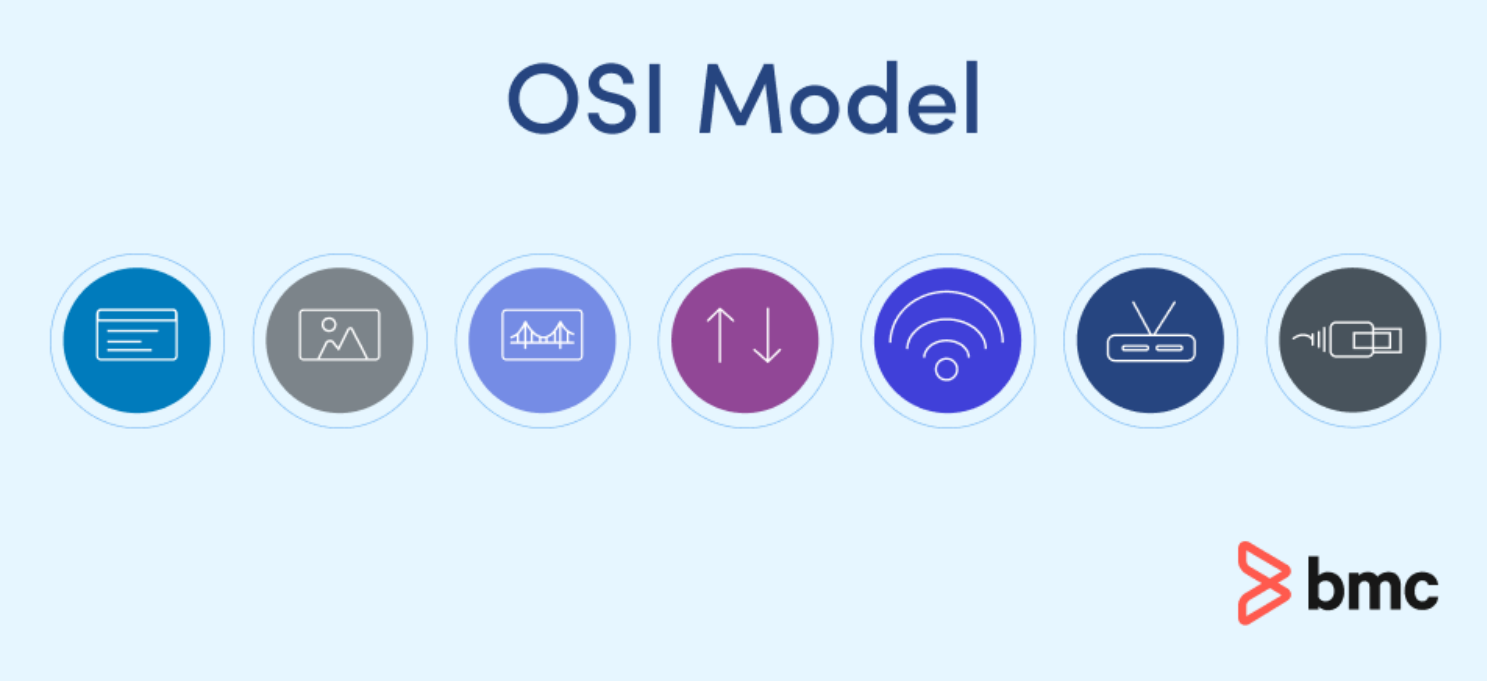
Key functions

- **Bit transmission**: Converts data frames into bits for transmission across physical media and

converts received bits back to frames.

- **Bit rate control**: Defines data transmission rates, measured in bits per second (bps), megabits per second (Mbps) or gigabits per second (Gbps).
- **Bit synchronization**: Ensures sender and receiver are synchronized by providing timing signals for accurate bit interpretation.
- **Transmission mode**: Defines how data flows between connected devices—simplex (one direction only), half duplex (both directions but not simultaneously), or full duplex (both directions simultaneously).
- **Physical topology**: Defines network configuration including bus, star, ring and mesh topologies.
- **Signal encoding**: Determines how data encoding occurs over physical signals using electrical voltage through copper, light pulses through fiber optics, or radio waves through wireless media.
- **Electrical and mechanical specifications**: Defines cable types, connector specifications, signal frequency, voltage levels and pin configurations for physical connections.
- **Technologies**: Wi-Fi standards (IEEE 802.11), Ethernet specifications (10BASE-T, 100BASE-TX, 1000BASE-T, 10GBASE-T), network interface cards, structured cabling (Cat5e, Cat6, Cat7), fiber optic cables (single-mode, multi-mode), modems, repeaters, hubs, RS-232 serial communication.

The physical layer handles all network communications at the bit level. When troubleshooting connectivity issues, network technicians start here: check cables for damage, verify link lights on network devices, test signal strength, and verify power to equipment.



OSI model vs. TCP/IP model

The OSI Model provides theoretical underpinning for understanding network communication, while the TCP/IP (Transmission Control Protocol/Internet Protocol) model offers practical implementation with four layers instead of seven.

- **Network Access Layer (OSI Layers 1-2)**: Combines physical and data link layers, handling

physical transmission via Ethernet protocols for LANs and ARP (Address Resolution Protocol) for mapping IP addresses to MAC addresses.
- **Internet Layer (OSI Layer 3)**: Uses IP (IPv4 with 32-bit addresses, IPv6 with 128-bit addresses) for routing data between networks. Includes ICMP for error reporting and network diagnostics, plus IGMP for multicast group management.
- **Transport Layer (OSI Layer 4)**: Uses TCP for reliable connection-oriented communication with flow control and error checking, plus UDP for connectionless transmission in real-time applications.
- **Application Layer (OSI Layers 5-7)**: Combines session, presentation and application layers, providing HTTP, HTTPS, FTP, SMTP, DNS, SSH protocols directly to applications.

The TCP/IP model's practical focus made it the backbone of modern networking, accommodating billions of devices and massive data traffic. However, the OSI Model's layered approach enables modular protocol development where each layer can be developed independently, making it invaluable for understanding network architecture and troubleshooting network problems.

Why the OSI Model matters

Systematic troubleshooting

The OSI Model provides a methodical framework for diagnosing network problems. Network technicians check each layer—physical layer for connectivity, data link layer for frame errors, network layer for routing problems, transport layer for segment delivery, and upper layers for application errors—quickly identifying whether issues stem from hardware, configuration or software.

Modular protocol development

The layered network architecture enables engineers to create protocols for one layer without modifying others. Application developers don't need to understand physical transmission details; hardware engineers don't need to modify application protocols.

Standardized communication

The model provides common terminology across organizations. When engineers discuss "Layer 3 routing issues" or "Layer 7 application problems," everyone understands which networking stack component is involved.

Enhanced network security

OSI layers enable defense-in-depth security strategies. Firewalls filter at Layer 3 (packet filtering), Layer 4 (stateful inspection), and Layer 7 (application-aware filtering). Security teams map different threats to specific layers, applying targeted countermeasures—Layer 2 ARP spoofing attacks require different responses than Layer 7 SQL injection attacks.

Educational foundation

The OSI Model remains the cornerstone of networking education, taught in certifications like CompTIA Network+ and Cisco CCNA because its structure helps learners grasp complex networking concepts.

The OSI Model in modern network management

While the TCP/IP model dominates practical implementation, the OSI model's layered framework remains essential for designing, troubleshooting and securing modern networks. Understanding how data flows through each layer—from physical transmission to application delivery—enables network professionals to build more reliable, efficient and secure network infrastructure.

Optimize your network infrastructure with BMC

Ready to transform your network operations? Explore how BMC's IT operations management solutions apply OSI Model principles to improve network reliability, performance and efficiency across all seven layers of your infrastructure.

Learn more about BMC network management solutions