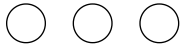


# OSI Model

1.4m views

Cybersecurity 101



## What Is the OSI Model?

The Open Systems Interconnection (OSI) model describes seven layers that computer systems use to communicate over a network. The OSI model is divided into seven distinct layers, each with specific responsibilities, ranging from physical hardware connections to high-level application interactions.

Each layer of the OSI model interacts with the layer directly above and below it, encapsulating and transmitting data in a structured manner. This approach helps network professionals troubleshoot issues, as problems can be isolated to a specific layer. The OSI model serves as a universal language for networking, providing a common ground for different systems to communicate effectively.

The OSI model was the first standard model for network communications, adopted by all major computer and telecommunication companies in the early 1980s. It was introduced in 1983 by representatives of the major computer and telecom companies, and was adopted by ISO as an international standard in 1984.

The modern Internet is not based on OSI, but on the simpler TCP/IP model. However, the OSI 7-layer model is still widely used, as it helps visualize and communicate how networks operate.

## Why Is the OSI Model Important?

The OSI model provides several advantages for organizations managing networks and communications:

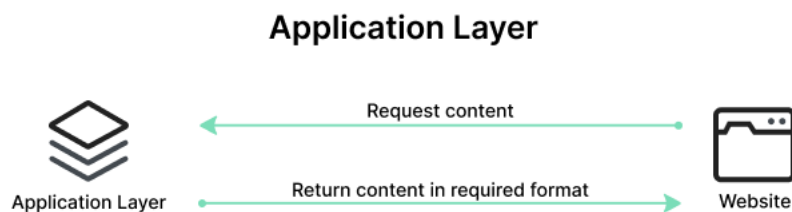
- **Shared understanding of complex systems:** OSI offers a universal language for networking, enabling different network devices and software to communicate. By dividing communication into seven distinct layers, it allows network professionals to isolate and troubleshoot problems effectively.
- **Faster research and development:** Developers can focus on improving specific layers without affecting others, leading to more rapid innovations. This modular approach enables specialization and enables different teams to work on various aspects of network communication simultaneously.
- **Flexible standardization:** The model's layered approach allows for the integration of new technologies at any layer without disrupting the overall network structure. This ensures compatibility across different devices and protocols, ensuring long-term viability and scalability of network infrastructure.

## OSI Model Explained: The OSI 7 Layers

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

We'll describe OSI layers "top down" from the application layer that directly serves the end user, down to the physical layer.

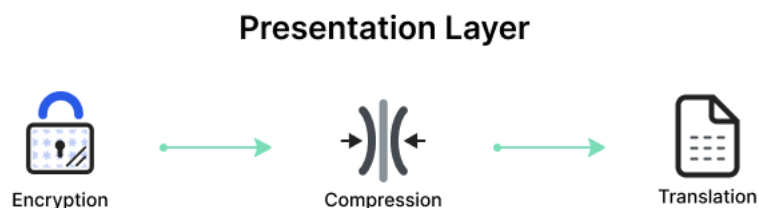
## 7. Application Layer



The Application Layer serves as the interface between the end-user applications and the underlying network services. This layer provides protocols and services that are directly utilized by end-user applications to communicate across the network. Key functionalities of the Application Layer include resource sharing, remote file access, and network management.

Examples of protocols operating at the Application Layer include [Hypertext Transfer Protocol \(HTTP\)](#) for web browsing, [File Transfer Protocol \(FTP\)](#) for file transfers, [Simple Mail Transfer Protocol \(SMTP\)](#) for email services, and [Domain Name System \(DNS\)](#) for resolving domain names to IP addresses. These protocols ensure that user applications can effectively communicate with each other and with servers over a network.

## 6. Presentation Layer



The Presentation Layer, also known as the syntax layer, is responsible for translating data between the application layer and the network format. It ensures that data sent from the application layer of one system is readable by the application layer of another system. This layer handles data formatting, [encryption](#), and compression, facilitating interoperability between different systems.

One of the key roles of the Presentation Layer is data translation and code conversion. It transforms data into a format that the application layer can understand. For example, it may convert data from ASCII to EBCDIC. It also includes encryption protocols to ensure [data security](#) during transmission and compression protocols to reduce the amount of data for efficient transmission.

## 5. Session Layer

### Session Layer



Session of communication

The Session Layer manages and controls the connections between computers. It establishes, maintains, and terminates connections, ensuring that data exchanges occur efficiently and in an organized manner. The layer is responsible for session checkpointing and recovery, which allows sessions to resume after interruptions.

Protocols operating at the Session Layer include Remote Procedure Call (RPC), which enables a program to execute a procedure on a remote host as if it were local, and the session establishment phase in protocols like NetBIOS and SQL. These services enable reliable communication, especially in complex network environments.

## 4. Transport Layer

### Transport Layer



The Transport Layer provides end-to-end communication services for applications. It ensures complete data transfer, error recovery, and flow control between hosts. This layer segments and reassembles data for efficient transmission and provides reliability with error detection and correction mechanisms.

Protocols at this layer include [Transmission Control Protocol](#) (TCP) and [User Datagram Protocol](#) (UDP). TCP is connection-oriented and ensures reliable data transfer with error checking and flow control, making it suitable for applications like web browsing and email. UDP is connectionless, offering faster, though less reliable, transmission, suitable for applications like video streaming and online gaming.

## 3. Network Layer

### Network Layer



The Network Layer is responsible for data routing, forwarding, and addressing. It determines the best physical path for data to reach its destination based on network conditions, the priority of service, and other factors. This layer manages logical addressing through IP addresses and handles packet forwarding.

Key protocols at this layer include the Internet Protocol (IP), which is important for routing and addressing, Internet Control Message Protocol (ICMP) for diagnostic and error-reporting purposes, and routing protocols like Routing Information Protocol (RIP) that manage the routing of data across networks.

## 2. Data Link Layer

The Data Link Layer is responsible for node-to-node data transfer and error detection and correction. It ensures that data is transmitted to the correct device on a local network segment. This layer manages [MAC \(Media Access Control\)](#) addresses and is divided into two sublayers: Logical Link Control (LLC) and Media Access Control (MAC).

Protocols and technologies at this layer include Ethernet, which defines the rules for data transmission over local area networks (LANs), and Point-to-Point Protocol (PPP) for direct connections between two network nodes. It also includes mechanisms for detecting and possibly correcting errors that may occur in the Physical Layer.

## 1. Physical Layer

The Physical Layer is responsible for the physical connection between devices. It defines the hardware elements involved in the network, including cables, switches, and other physical components. This layer also specifies the electrical, optical, and radio characteristics of the network.

Functions of the Physical Layer include the modulation, bit synchronization, and transmission of raw binary data over the physical medium. Technologies such as Fiber Optics and Wi-Fi operate at this layer, ensuring that the data physically moves from one device to another in the network.

## How Does Communication Happen in the OSI Model? A Practical Example

Let's consider how OSI layers play a role in an everyday activity like sending an email to a person overseas:

- When a user in New York sends an email to a colleague in London, the process starts at the Application Layer (Layer 7). The user's email client, such as Outlook, uses SMTP (Simple Mail Transfer Protocol) to handle the email message.
- The email is then passed to the Presentation Layer (Layer 6), where it is formatted and encrypted to ensure proper transmission.
- Next, the email moves to the Session Layer (Layer 5), where a session is established between the sender's email server in New York and the receiver's email server in London. This layer manages the session, keeping the connection open long

enough to send the email.

- The email data then reaches the Transport Layer (Layer 4), where it is divided into smaller packets. TCP ensures these packets are sent reliably and in the correct order.
- At the Network Layer (Layer 3), each packet is assigned source and destination IP addresses, allowing it to be routed through multiple networks, including routers and switches, to reach the recipient in London.
- The Data Link Layer (Layer 2) then uses MAC addresses to handle the packets' journey across local networks and correcting any errors that occur.
- Finally, the Physical Layer (Layer 1) converts the data into electrical signals, which are transmitted over fiber-optic cables under the Atlantic Ocean.

Upon reaching the recipient's server in London, the process is reversed:

- The Physical Layer converts the signals back into data packets, which are reassembled at the Data Link Layer.
- The Network Layer ensures the packets have arrived correctly, and the Transport Layer reorders them if necessary.
- The Session Layer maintains the session until the email is fully received.
- The Presentation Layer decrypts and formats the email, and the Application Layer delivers the email to the client, where it appears in their inbox.

## Advantages of OSI Model

The OSI model helps users and operators of computer networks:

- Determine the required hardware and software to build their network.
- Understand and communicate the process followed by components communicating across a network.
- Perform troubleshooting, by identifying which network layer is causing an issue and focusing efforts on that layer.

The OSI model helps network device manufacturers and networking software vendors:

- Create devices and software that can communicate with products from any other vendor, allowing open interoperability
- Define which parts of the network their products should work with.
- Communicate to users at which network layers their product operates – for example, only at the application layer, or across the stack.

## OSI vs. TCP/IP Model

The [Transfer Control Protocol/Internet Protocol](#) (TCP/IP) is older than the OSI model and was created by the US Department of Defense (DoD). A key difference between the models is that TCP/IP is simpler, collapsing several OSI layers into one:

- OSI layers 5, 6, 7 are combined into one Application Layer in TCP/IP
- OSI layers 1, 2 are combined into one Network Access Layer in TCP/IP – however TCP/IP does not take responsibility for sequencing and acknowledgement functions, leaving these to the underlying transport layer.

Other important differences:

- TCP/IP is a functional model designed to solve specific communication problems, and which is based on specific, standard protocols. OSI is a generic, protocol-independent model intended to describe all forms of network communication.
- In TCP/IP, most applications use all the layers, while in OSI simple applications do not use all seven layers. Only layers 1, 2 and 3 are mandatory to enable any data communication.

**See how Imperva [Web Application Firewall](#) can help you with application security.**

[Request demo](#)

[Learn more](#)


## Imperva Application Security

Imperva security solutions [secure](#) your applications across multiple layers of the OSI model, from the network layer, protected by Imperva DDoS mitigation, to Imperva's web application firewall (WAF), bot management and API [security technology](#) that safeguards the application layer.

To secure applications and networks across the OSI stack, Imperva provides multi-layered protection to make sure websites and applications are available, easily accessible and safe. The Imperva application security solution includes:

- **DDoS Protection**—maintain uptime in all situations. Prevent any type of DDoS attack, of any size, from preventing access to your website and network infrastructure.
- **CDN**—enhance website performance and reduce bandwidth costs with a CDN designed for developers. Cache static resources at the edge while accelerating APIs and dynamic websites.
- **WAF**—cloud-based solution permits legitimate traffic and prevents bad traffic, safeguarding applications at the edge. Gateway WAF keeps applications and APIs inside your network safe.
- **Bot protection**—analyzes your bot traffic to pinpoint anomalies, identifies bad bot behavior and validates it via challenge mechanisms that do not impact user traffic.
- **API security**—protects APIs by ensuring only desired traffic can access your API endpoint, as well as detecting and blocking exploits of vulnerabilities.
- **Account takeover protection**—uses an intent-based detection process to identify and defends against attempts to take over users' accounts for malicious purposes.
- **RASP**—keep your applications safe from within against known and zero-day attacks. Fast and accurate protection with no signature or learning mode.
- **Attack analytics**—mitigate and respond to real **cyber security** threats efficiently and accurately with actionable intelligence across all your layers of defense.


## Latest Blogs



**Imperva Threat Research**

### ShadyShader: Crashing Apple Devices with a Single Click


**Ron Masas**  
Oct 22, 2024 | 4 min read



**Imperva Threat Research**

### Imperva Defends Against Targeted Exploits Used By APT29 Hackers


**Gabi Sharadin**  
Oct 14, 2024 | 2 min read



**Imperva Threat Research**

### Trouble in Da Hood: Malicious Actors Use Infected PyPI Packages to Target Roblox[...]

**Sarit, Omri, Daniel**  
Sep 30, 2024 | 4 min read



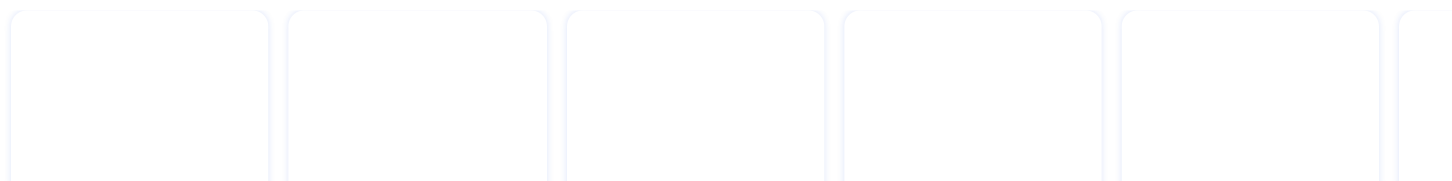
**Imper**

### Cursor a Catc You're

**I**  
!



## Latest Articles



<div>Data Security</div> <div>Information Security: The Ultimate Guide</div> <div>216.9k Views</div>	<div>App Security</div> <div>Cybersecurity Threats</div> <div>149.9k Views</div>	<div>App Security</div> <div>Security information and event management (SIEM)</div> <div>134.2k Views</div>	<div>App Security</div> <div>Defense-in-Depth</div> <div>128.7k Views</div>	<div>App Security</div> <div>Honeypot</div> <div>110.9k Views</div>	
<	>				



+1 866 926 4678

Partners

- Imperva Partner Ecosystem
- Channel Partners
- Technology Alliances
- Find a Partner
- Partner Portal Login

About Us

- Why Imperva
- Who We Are
- Events
- Careers
- Press & Awards
- Contact Information

Support

- Emergency DDoS Protection
- Support Portal
- Imperva Community
- Documentation Portal
- API Integration
- Trust Center

Resources

- Imperva Blog
- Resource Library
- Case Studies
- Learning Center

Network

- Network Map
- System Status

English



Trust Center

Modern Slavery Statement

Privacy



Legal

Copyright © 2024 Imperva. All rights reserved