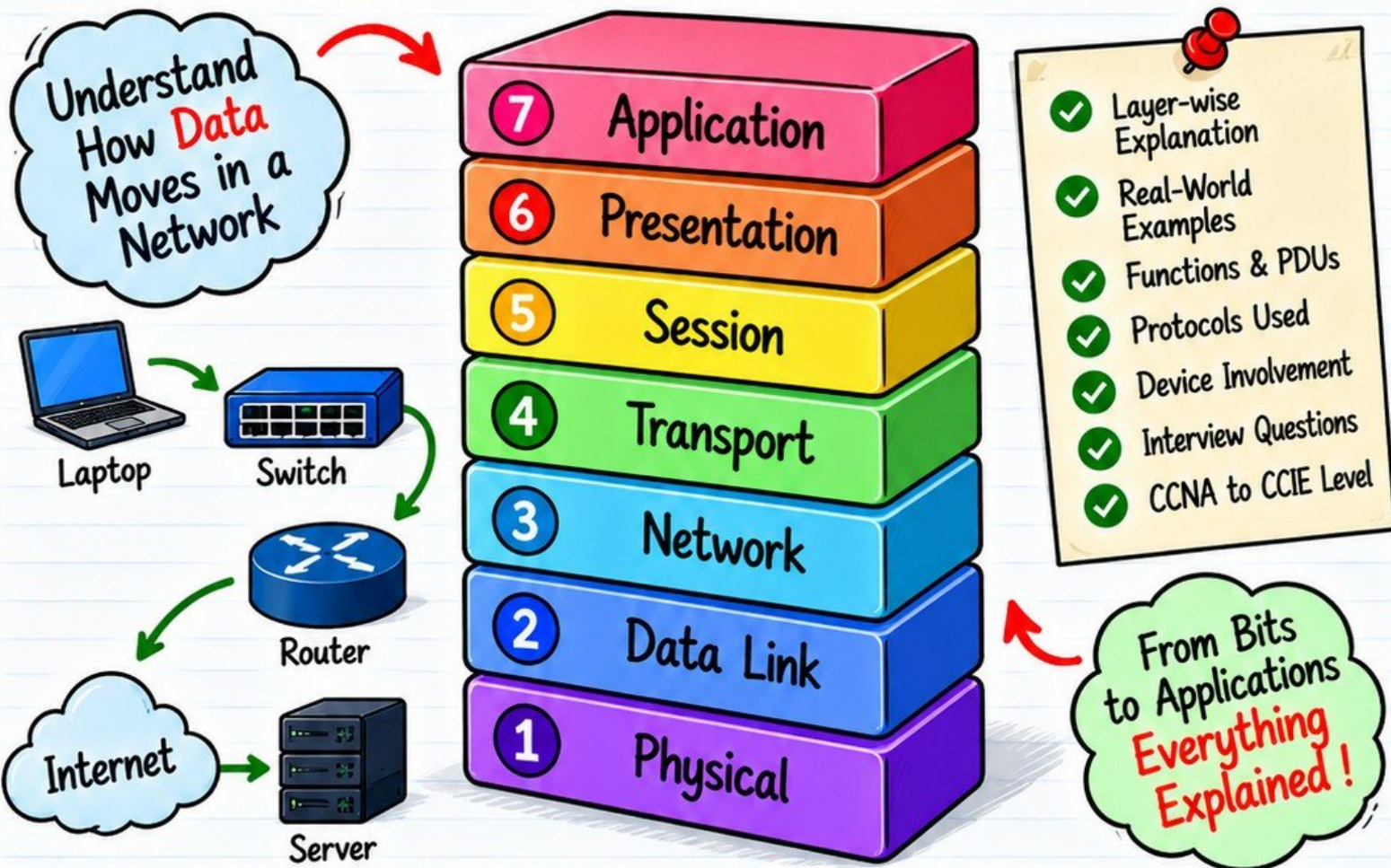


OSI MODEL

In Detailed Explanation

Concepts | Functions | Protocols | PDUs | Real-World Examples
Commands | Troubleshooting | Interview Questions



EASY
EXPLANATION



REAL-WORLD
EXAMPLES



PRACTICAL
COMMANDS



INTERVIEW
QUESTIONS

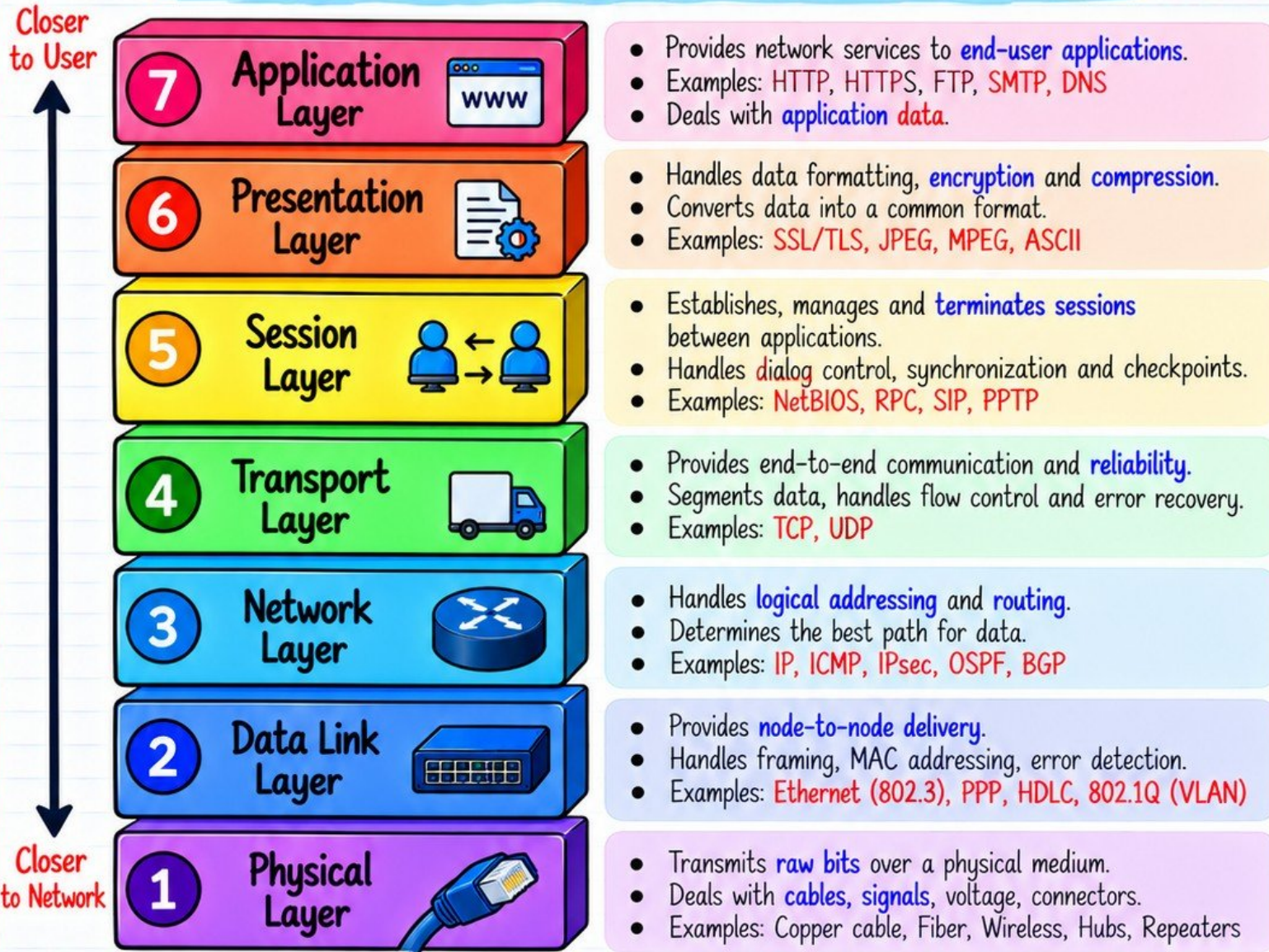


CCNA TO CCIE
LEVEL

Swipe Next

A 7-Layer Model to Understand How Networks Work

The **OSI (Open Systems Interconnection) Model** is a conceptual framework created by **ISO (International Organization for Standardization)** to understand how data communicates between two devices over a network.



Key Points:

- ✓ OSI Model has 7 layers.
- ✓ Each layer has a specific function.
- ✓ Data moves from Layer 7 → Layer 1 (Sender) and Layer 1 → Layer 7 (Receiver).
- ✓ Helps in troubleshooting, understanding protocols and network communication.



Why is OSI Model Important?

- ✓ Helps to understand how networking works.
- ✓ Easy to identify where a problem is occurring.
- ✓ Useful for CCNA to CCIE level troubleshooting.
- ✓ Foundation for many networking protocols.
- ✓ Used as a standard model across industries.



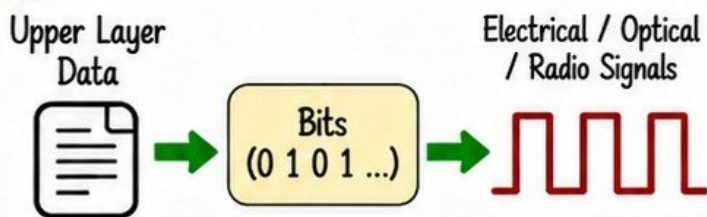
Deals with Raw Bits, Signals and Physical Transmission

The Physical Layer is the first layer of the OSI model. It is responsible for transmitting raw bits over a physical medium in the form of electrical, optical or radio signals.

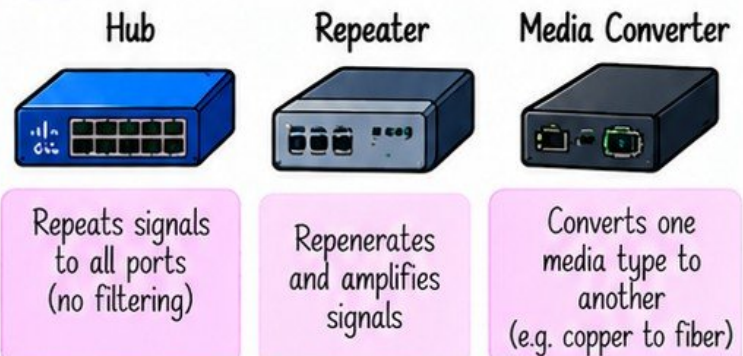
1 Key Functions

- ✓ Converts bits (0 and 1) into signals.
- ✓ Defines electrical, optical and mechanical specifications.
- ✓ Handles data transmission over physical media.
- ✓ Defines data rate, signal encoding and modulation.
- ✓ Manages physical topology and connectors.
- ✓ Does not perform error correction (handled at upper layers).

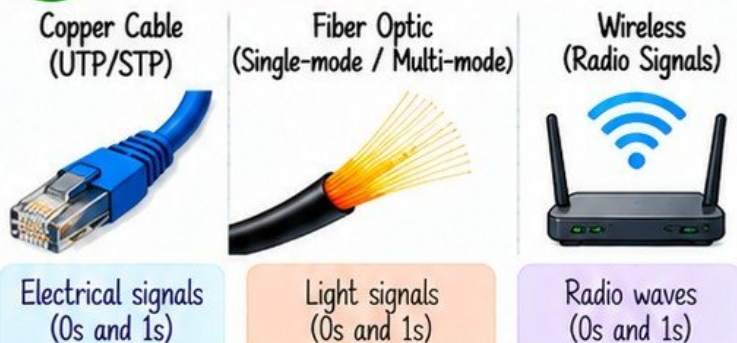
3 Physical Layer Encapsulation



2 Devices Working at Layer 1



4 Physical Media Types



5 Physical Layer Standards

Standard	Technology	Data Rate
10BASE-T	Ethernet (UTP)	10 Mbps
100BASE-TX	Fast Ethernet	100 Mbps
1000BASE-T	Gigabit Ethernet	1 Gbps
10GBASE-T	10 Gigabit Ethernet	10 Gbps
802.11 (Wi-Fi)	Wireless LAN	Up to several Gbps
SONET/SDH	Optical Transport	155 Mbps - 40 Gbps

6 Important Concepts

- ✓ **Bit** - Smallest unit of data (0 or 1).
- ✓ **Data Rate** - Speed at which bits are transmitted (e.g. 100 Mbps).
- ✓ **Bandwidth** - Maximum data rate of the medium.
- ✓ **Signal Encoding** - Converts bits to signals (e.g. NRZ, Manchester Encoding).
- ✓ **Modulation** - Used in wireless (e.g. AM, FM, QAM).
- ✓ **Attenuation** - Loss of signal strength over distance.
- ✓ **Impedance** - Must match for proper transmission.

Provides Node-to-Node Delivery & Framing

The Data Link Layer provides reliable node-to-node data delivery over a physical link. It takes the bits from Layer 1, groups them into frames, adds MAC addresses, performs error detection and controls access to the medium.

1 Key Functions

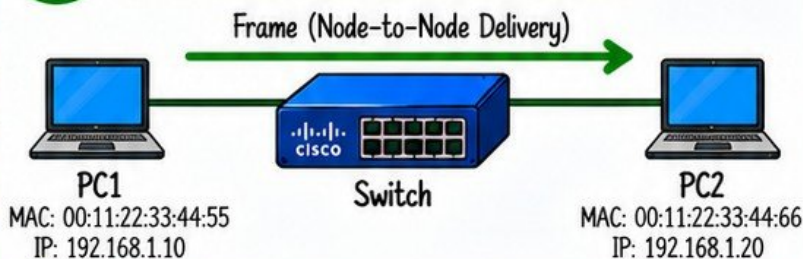
- ✓ **Framing** - groups bits into frames.
- ✓ **MAC Addressing** - identifies source and destination devices on the same network.
- ✓ **Error Detection** - uses FCS (CRC) to detect errors.
- ✓ **Flow Control** - prevents fast sender from overwhelming slower receiver.
- ✓ **Media Access Control (MAC)** - controls which device can use the medium.
- ✓ **Link Management** - establishes, maintains and terminates the link.

2 Frame Structure (Ethernet Frame)

Preamble (7 Bytes)	SFD (1 Byte)	Destination MAC (6 Bytes)	Source MAC (6 Bytes)	Type/Length (2 Bytes)	Data (46 - 1500 Bytes)	FCS (4 Bytes)
-----------------------	-----------------	---------------------------------	----------------------------	--------------------------	------------------------------	------------------

- **Preamble** - 7 bytes of alternating 1s and 0s for synchronization.
- **SFD (Start Frame Delimiter)** - 1 byte (10101011) marks the start of the frame.
- **Destination MAC** - MAC address of receiver.
- **Source MAC** - MAC address of sender.
- **Type/Length** - identifies the upper layer protocol (e.g. 0x0800 for IPv4).
- **Data** - actual payload (minimum 46 bytes, maximum 1500 bytes).
- **FCS (Frame Check Sequence)** - 4 bytes CRC for error detection.

3 How Layer 2 Works (Example)



- 1 PC1 sends data to PC2 (same network).
- 2 Layer 2 on PC1 encapsulates the data into an Ethernet frame.
- 3 Frame contains Source MAC (PC1) and Destination MAC (PC2).
- 4 Switch forwards the frame based on MAC address table.
- 5 PC2 receives the frame, checks FCS and passes data to Layer 3.

5 MAC Address Format

00 : 1A : 2B : 3C : 4D : 5E

OUI
(First 24 bits)
Identifies the Vendor
(e.g. Cisco, HP, Dell)

Device ID
(Last 24 bits)
Unique to the device
(assigned by vendor)



Important:

- MAC address is 48-bit (6 bytes).
- Written in hexadecimal format.
- Example: 00:1A:2B:3C:4D:5E

4 Sub-Layers of Data Link Layer

LLC (Logical Link Control)

- Interface between Layer 2 and Layer 3.
- Identifies and multiplexes network layer protocols using SAP (Service Access Point).
- Provides flow control and error control.

MAC (Media Access Control)

- Controls access to the shared medium.
- Uses MAC addressing (48-bit).
- Defines how devices place frames on the medium (e.g. CSMA/CD in Ethernet).
- Handles frame formatting and FCS.

6 Layer 2 Protocols

Protocol	Purpose
Ethernet (802.3)	LAN technology, most widely used
802.11 (Wi-Fi)	Wireless LAN
PPP	Point-to-Point communication
HDLC	Synchronous data link protocol
Frame Relay	WAN technology (legacy)
ATM	Cell-based data link layer (legacy)



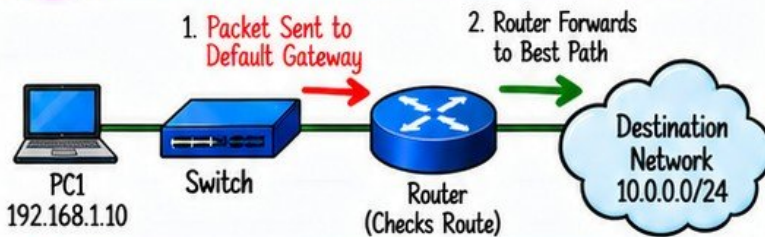
Provides Logical Addressing, Routing & Path Selection

The Network Layer is responsible for logical addressing, routing, and delivering data from the source to the destination across multiple networks. It determines the best path and handles packet forwarding.

1 Key Functions

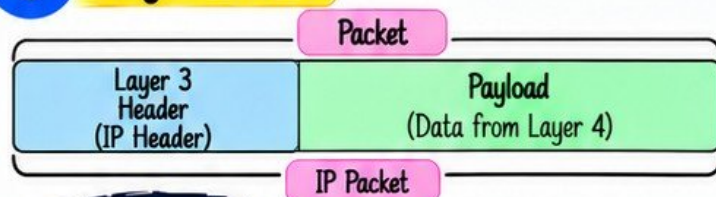
- ✓ Provides **logical addressing** (IP address).
- ✓ Determines the best path for data (routing).
- ✓ Forwards packets between **different networks**.
- ✓ Handles **fragmentation and reassembly** of packets.
- ✓ Manages **congestion** and Quality of Service (QoS).
- ✓ Supports internetworking (connecting multiple networks).
- ✓ Uses protocols like **IP, ICMP, OSPF, EIGRP, BGP** etc.
- ✓ Works with routers and Layer 3 switches.

3 Routing Process (How It Works?)



- 1 PC1 sends packet to a remote network (e.g. 10.0.0.0/24).
- 2 Router checks its routing table for the best path.
- 3 If route is found, it forwards the packet to the next hop.
- 4 If no route is found, it can use a default route.
- 5 Packet continues to travel through multiple routers until it reaches the destination network.

6 Layer 3 PDU



2 Logical Addressing (IP Address)

The Network Layer uses **IP addresses** to identify source and destination networks.

IPv4 Address (32-bit)

192 . 168 . 1 . 10

Network Portion

Host Portion

IPv6 Address (128-bit)

2001 : 0db8 : 85a3 : 0000 :
0000 : 8a2e : 0370 : 7334

- IP address helps in routing packets to the correct network.
- Routers read the destination IP address to forward the packet.

4 Common Layer 3 Devices



Router

- Forwards packets between networks
- Uses routing table



Layer 3 Switch

- Performs routing at hardware speed
- Used in enterprise networks



Firewall

- Performs Layer 3 filtering (IP based)
- Controls traffic between networks

5 Common Protocols at Layer 3

Protocol	Purpose
IP (IPv4/IPv6)	Logical addressing and packet delivery
ICMP	Error reporting and diagnostics (e.g. ping)
IGMP	Multicast group management
OSPF	Dynamic routing protocol (Link State)
EIGRP	Dynamic routing protocol (Cisco)
BGP	Routing between autonomous systems (Internet)
RIP	Simple distance vector routing (legacy)

7 Important Points



- ✓ Layer 3 works with logical addressing (IP).
- ✓ Routers operate at Layer 3.
- ✓ Fragmentation happens at Layer 3 (IPv4).
- ✓ Layer 3 is responsible for end-to-end delivery across networks.
- ✓ Key for CCNA to CCIE: Understand IP addressing, routing, subnetting and routing protocols in depth.

Provides End-to-End Communication, Port Numbering & Reliability

The Transport Layer is responsible for end-to-end communication between applications. It provides segmentation, reliability, flow control and multiplexing using port numbers.

1 Key Functions

- Provides **end-to-end communication** between applications.
- Segments** data from upper layers into smaller pieces (segments).
- Reassembles** segments at the destination.
- Uses **port numbers** to identify applications.
- Provides **reliability, flow control** and **error recovery** (TCP).
- Supports **multiplexing** and **demultiplexing**.
- Controls the rate of data transmission.

2 Transport Layer Protocols

TCP (Transmission Control Protocol)

- Connection-oriented protocol
- Reliable data delivery
- Uses 3-way handshake
- Provides flow control & congestion control
- Guaranteed delivery (acknowledgment)
- Used for web, email, file transfer etc.
- Examples: HTTP, HTTPS, FTP, SMTP, POP3, IMAP

UDP (User Datagram Protocol)

- Connectionless protocol
- No guarantee of delivery
- No handshake (faster)
- No flow control or congestion control
- Lower overhead
- Used for real-time applications
- Examples: DNS, DHCP, VoIP, Streaming, Online Gaming

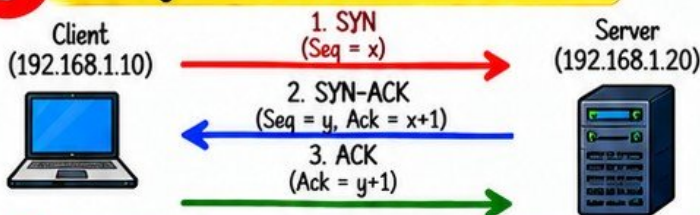
3 TCP vs UDP Comparison

Feature	TCP	UDP
Connection	Connection-oriented	Connectionless
Reliability	Reliable (ACK)	Not reliable
Speed	Slower	Faster
Handshake	Yes (3-way)	Not required
Flow Control	Yes	No
Congestion Control	Yes	No
Header Size	20-60 bytes	8 bytes
Use Case	Web, Email, File Transfer	DNS, VoIP, Streaming
Data Delivery	Guaranteed	Best effort

4 Segment Structure (TCP Header)

0	4	10	16	24	31
Source Port (16 bits)			Destination Port (16 bits)		
Sequence Number (32 bits)					
Acknowledgment Number (32 bits)					
Data Offset (4 bits)	Reserved (3 bits)	Flags (9 bits)	Window Size (16 bits)		
Checksum (16 bits)			Urgent Pointer (16 bits)		
Options (0 - 40 bytes)					
Data (Variable)					

5 3-Way Handshake (TCP Connection)



- Client sends **SYN** to start the connection.
- Server responds with **SYN-ACK**.
- Client sends **ACK** to complete the connection.

7 Important Points

- Transport Layer works at the host level (end-to-end).
- Uses port numbers to identify applications.
- TCP ensures reliable delivery, UDP provides faster delivery.
- Commonly used in troubleshooting to check port reachability (e.g. TCP 80, 443).
- Essential for application communication and session management.

6 Port Numbers (Examples)

Port	Protocol	Application / Service
20, 21	TCP	FTP (File Transfer)
22	TCP	SSH (Secure Shell)
23	TCP	Telnet
25	TCP	SMTP (Email)
53	UDP/TCP	DNS (Domain Name System)
67, 68	UDP	DHCP (IP Address)
80	TCP	HTTP (Web)
443	TCP	HTTPS (Secure Web)
3389	TCP	RDP (Remote Desktop)

8 Real-World Examples

Web Browsing (HTTP/HTTPS) TCP 80/443	Email (SMTP) TCP 25	File Transfer (FTP) TCP 20/21	DNS Queries (DNS) UDP 53	VoIP Calls (SIP/RTP) UDP
---	------------------------	----------------------------------	-----------------------------	-----------------------------

Establishes, Manages and Terminates Sessions

The Session Layer is responsible for establishing, managing and terminating sessions between applications. It provides dialog control, synchronization and checkpointing to ensure reliable communication between devices.

1 Key Functions

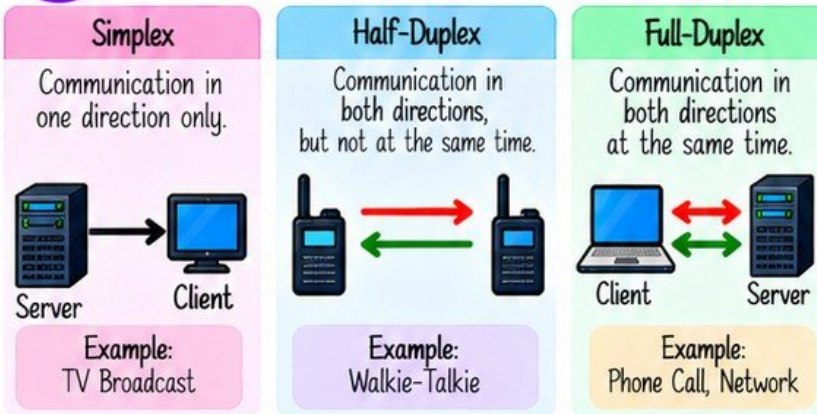
- Establishes, manages and terminates sessions between applications.
- Provides **dialog control** (who can send data and when).
- Handles **synchronization** (keeps both sides in sync).
- Uses **checkpointing** (saves the state of the session to recover in case of failure).
- Manages **session tokens** and **session IDs**.
- Supports **full-duplex** and **half-duplex** communication.

2 How Session Layer Works?



- Creates a session between applications.
- Maintains the session throughout the communication.
- Uses session IDs to keep track of the session.
- Terminates the session when communication is complete.

3 Dialog Control (Communication Modes)



4 Synchronization & Checkpointing

Synchronization

- Adds synchronization points in data streams.
- Ensures both sides remain in sync.
- If connection is interrupted, communication can resume from the last sync point.



Checkpointing

- Saves the state of an ongoing session.
- Helps in recovery if the connection fails.
- Allows resuming the session from the last checkpoint instead of starting again.



5 Common Protocols at Layer 5

Protocol	Description
NetBIOS	Session management for Windows networking
RPC (Remote Procedure Call)	Manages sessions for remote services
SIP (Session Initiation Protocol)	Used in VoIP to establish, manage and terminate calls
PPTP (Point-to-Point Tunneling)	Manages VPN sessions
SMB (Session Management Block)	Manages file sharing sessions

6 Real-World Examples



7 Important Points

- Session Layer is responsible for dialog control, synchronization and checkpointing.
- It provides session IDs to identify sessions.
- It helps in error recovery if the connection breaks.

- Works closely with the Presentation Layer (data format).
- Essential for reliable and continuous communication.
- Widely used in VoIP, file sharing and remote access.

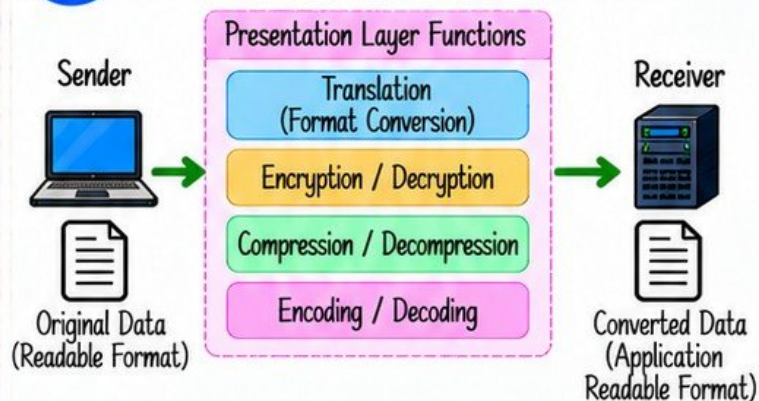
Handles Data Format, Encryption, Compression and Translation

The Presentation Layer is responsible for converting data into a format that the application layer can understand. It performs data translation, encryption, decryption, compression and encoding to ensure secure and efficient communication.

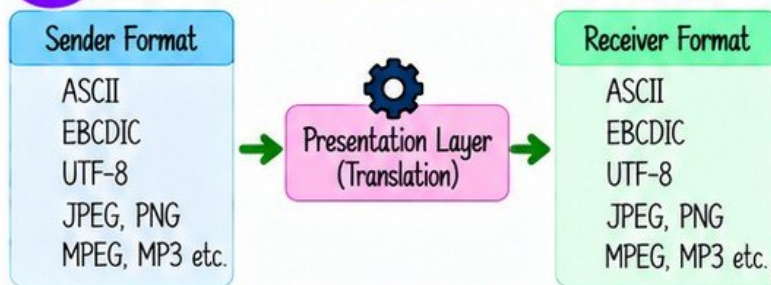
1 Key Functions

- ✓ **Data Translation** - converts data between different formats (e.g. ASCII, EBCDIC).
- ✓ **Encryption** - encrypts data for secure transmission.
- ✓ **Decryption** - decrypts data at the destination.
- ✓ **Compression** - reduces the size of data to save bandwidth.
- ✓ **Encoding** - converts data into a standard format (e.g. ASCII, UTF-8).
- ✓ **Format Conversion** - handles differences in data representation (text, images, audio, video).

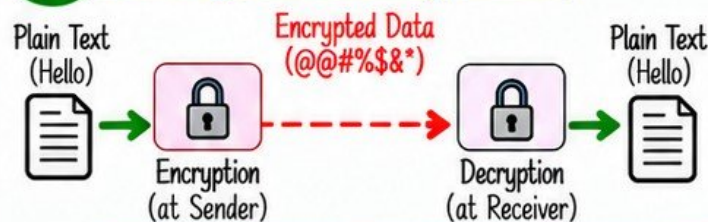
2 How Presentation Layer Works?



3 Data Translation (Format Conversion)

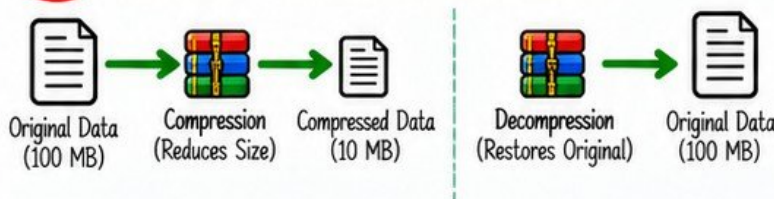


4 Encryption & Decryption



Common Algorithms: SSL/TLS, AES, DES, RSA

5 Compression & Decompression



6 Encoding (Text Representation)

Encoding Type	Description	Example (Character 'A')
ASCII	7-bit character encoding	01000001
UTF-8	Variable-length encoding	01000001
UTF-16	16-bit encoding	00000000 01000001
EBCDIC	Used in IBM systems	C1
Base64	Encodes binary data to text	SGVsbG8=

Encoding is used to ensure data can be properly interpreted by the application.

7 Real-World Examples (Layer 6 in Action)

HTTPS
Uses SSL/TLS encryption

File Compression
Zip, RAR reduces file size

Media Streaming
Video/Audio encoding (MPEG, H.264, MP3)

Data Translation
ASCII ↔ EBCDIC (used in mainframe environments)

8 Important Points

- ✓ Works closely with Application Layer (Layer 7).
- ✓ Handles data format, encryption, compression and encoding.
- ✓ **Examples:** SSL/TLS, JPEG, MPEG, ASCII, UTF-8.
- ✓ Improves security and reduces bandwidth usage.
- ✓ Essential for applications that handle different data formats across platforms.
- ✓ Important for CCNA to CCIE level in troubleshooting application and encryption related issues.

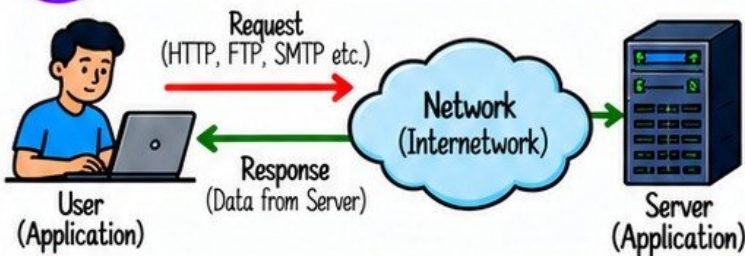
Provides Network Services to End-User Applications

The Application Layer is the top layer of the OSI model. It provides network services directly to end users and applications. It acts as an interface between user applications and the network. This layer includes protocols such as HTTP, HTTPS, FTP, SMTP, DNS, DHCP, SNMP etc.

1 Key Functions

- ✓ Provides services directly to **user applications**.
- ✓ Enables **communication** between applications on different devices.
- ✓ Handles user **authentication, authorization** and access control (in some protocols).
- ✓ Provides **network services** like web, email, file transfer, name resolution etc.

3 How Application Layer Works?



- 1 User opens an application (e.g. web browser).
- 2 Application uses protocols like HTTP, FTP, SMTP etc.
- 3 Data is processed and sent over the network.
- 4 Server responds with the requested data.
- 5 Application layer provides the data to the end user.

5 Application Layer vs Other Layers

Layer	Focus	Example
Application (L7)	User applications and services	HTTP, FTP, SMTP, DNS
Presentation (L6)	Data format, encryption, compression	SSL/TLS, JPEG, MPEG
Session (L5)	Session management	Session IDs, Dialog Control
Transport (L4)	End-to-end delivery, reliability	TCP, UDP
Network (L3)	Logical addressing and routing	IP, ICMP, OSPF, BGP
Data Link (L2)	Framing and MAC addressing	Ethernet, Switch
Physical (L1)	Bits transmission over medium	Cables, Signals

7 Important Points

- ✓ Application layer provides services to end-user applications.
- ✓ Works closely with Presentation layer for data formatting and encryption.
- ✓ Uses well-known port numbers to identify services.
- ✓ Common in daily life applications like web, email, file transfer, DNS etc.
- ✓ Essential for CCNA to CCIE level troubleshooting and network analysis.

2 Common Application Layer Protocols

Protocol	Purpose	Port No.	Transport
HTTP	Web browsing	80	TCP
HTTPS	Secure web browsing	443	TCP
FTP	File transfer	20, 21	TCP
SFTP	Secure file transfer	22	TCP
SMTP	Send email	25	TCP
POP3	Receive email (download)	110	TCP
IMAP	Receive email (sync)	143	TCP
DNS	Name resolution	53	UDP/TCP
DHCP	IP address assignment	67, 68	UDP
SNMP	Network monitoring	161, 162	UDP
SSH	Secure remote access	22	TCP
Telnet	Remote access (insecure)	23	TCP
NTP	Time synchronization	123	UDP

4 Real-World Examples

Web Browsing (HTTP/HTTPS) Port 80/443	Email (SMTP/IMAP/POP3) Port 25/143/110	File Transfer (FTP/SFTP) Port 20/21/22	Name Resolution (DNS) Port 53
IP Address Assignment (DHCP) Port 67/68	Network Monitoring (SNMP) Port 161/162	Time Sync (NTP) Port 123	Remote Access (SSH/Telnet) Port 22/23

6 Application Layer in Packet (Example: HTTP)

Layer 2 Ethernet Header	Layer 3 IP Header	Layer 4 TCP Header	Layer 7 HTTP Data (GET /index.html)	Layer 2 FCS
----------------------------	----------------------	-----------------------	---	----------------

- Application layer data is encapsulated by Transport, Network, Data Link and Physical layers.
- Example: HTTP GET request "GET /index.html" is application layer data.
- When received, each layer removes its header until the data reaches the application layer.

8 Key Takeaways

- ✓ Application layer = user services and network applications.
- ✓ Uses protocols like HTTP, HTTPS, FTP, SMTP, DNS, DHCP, SNMP.
- ✓ Identified by port numbers.
- ✓ Provides real-world services used daily.
- ✓ Important for security, monitoring and troubleshooting.

Complete OSI Model in One Page (CCNA to CCIE)

The OSI model helps us understand how data travels from one device to another.

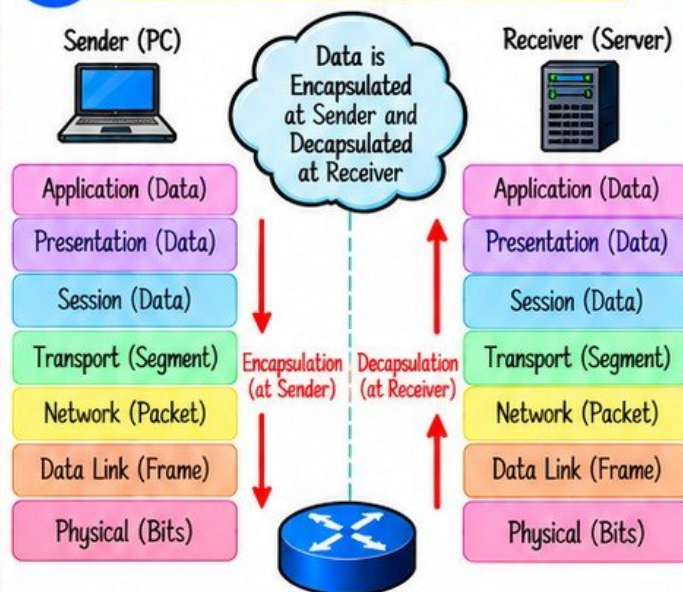
Each layer has a specific function and works with the layer above and below it.

This summary will help you quickly revise all 7 layers with examples, protocols and PDUs.

1 Complete OSI Model Summary

Layer	Name	Main Function	Examples / Protocols	PDU
7	Application	Provides network services to user applications	HTTP, HTTPS, FTP, SMTP, DNS, DHCP, SNMP, SSH	Data
6	Presentation	Data format, encryption, compression, translation	SSL/TLS, JPEG, MPEG, ASCII, EBCDIC, UTF-8	Data
5	Session	Establishes, manages and terminates sessions	NetBIOS, RPC, SIP, SMB, PPTP	Data
4	Transport	End-to-end communication, reliability, port numbers	TCP, UDP	Segment
3	Network	Logical addressing, routing and path selection	IP, ICMP, OSPF, EIGRP, BGP, RIP	Packet
2	Data Link	Framing, MAC addressing, error detection	Ethernet, PPP, HDLC, VLAN (802.1Q)	Frame
1	Physical	Transmits raw bits over physical medium	Cables, Fiber, Signals, Hubs, Repeaters	Bits

2 Data Flow Through OSI Model



3 Real-World Scenario

Example: You open a website (<https://www.google.com>)



- 1 Application: You enter www.google.com in browser (HTTP/HTTPS).
- 2 Presentation: Data is encrypted using SSL/TLS.
- 3 Session: Session is established between your PC and server.
- 4 Transport: TCP ensures reliable delivery (Port 443).
- 5 Network: IP routes the packet to the destination network.
- 6 Data Link: MAC addresses are used to deliver the frame in local network.
- 7 Physical: Data is sent as electrical/optical signals over the cable.

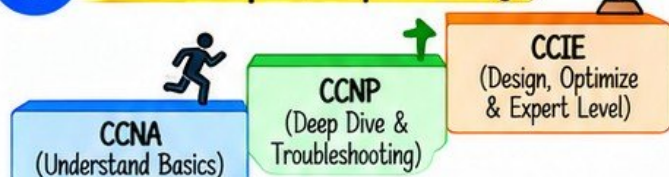
4 Key Points to Remember

- ✓ Each layer has a **specific function** and works with the layer above and below.
- ✓ Data is **encapsulated** at the sender and **decapsulated** at the receiver.
- ✓ **Application** layer provides services to end users.
- ✓ **Transport** layer uses **port numbers** and ensures **reliability** (TCP).
- ✓ **Network** layer uses **IP addressing** and routing.
- ✓ **Data Link** layer uses **MAC addresses** and creates frames.
- ✓ **Physical** layer transmits **bits** over the medium.
- ✓ **Common protocols**: HTTP, HTTPS, FTP, SMTP, DNS, DHCP, SNMP.
- ✓ **Important for CCNA to CCIE** in troubleshooting and network design.

5 Interview Questions (Quick Revision)

- Q Which layer provides IP addressing? → **Network Layer (L3)**
- Q Which layer uses port numbers? → **Transport Layer (L4)**
- Q Which layer handles encryption? → **Presentation Layer (L6)**
- Q What is the PDU at Layer 3? → **Packet**
- Q Which protocol is used for reliable delivery? → **TCP**
- Q Which layer creates frames? → **Data Link Layer (L2)**

6 Next Steps (Keep Learning)



7 Follow for More

If you found this helpful,
Follow @Technetworkk
for more Networking & Cybersecurity
Visual Notes

