NETWORK FUNDAMENTALS TRAINING

June 2026

DAY 2

The OSI Model & TCP/IP Suite

OSI • DOD - Network • Protocols

09:00 – 16:00 | 8 × 45-minute lessons | 1-hour lunch break

DAY 2

The OSI Model & TCP/IP Suite

09:00 – 16:00 | 8 × 45-minute lessons | 1-hour lunch break

09:00 – 09:45	**Lesson 1 The Physical Layer — Signals, Bandwidth & Media Overview**

1. Why Do We Need a Network Model?

Imagine two people trying to have a conversation — one

speaks only Kinyarwanda and the other speaks only Arabic. Even if they both want to communicate, they cannot, because they have no shared framework for language.

The same problem existed in early networking. Different manufacturers built networking equipment with their own proprietary rules. A router from Company A could not talk to a switch from Company B. A global network — like the internet — would have been impossible.

Network reference models were developed to solve this. A reference model is a blueprint that defines how communication between network devices should work. When all manufacturers follow the same blueprint, products from different companies can work together seamlessly.

The two most important reference models are:

Model	Full Name	Created By
OSI Model	Open Systems Interconnection	ISO (International Organization for Standardization)
DoD / TCP/IP Model	Department of Defense Model	US Government / DARPA

Key Takeaway

A network model is not a physical device — you cannot buy one. It is a set of agreed standards that manufacturers follow so that their products work together.

2. The OSI Model — Overview

The **OSI Model** was formalized by the ISO in **1984**. It divides networking functions into **7 layers**, each responsible for a specific task. The layers are numbered from the bottom up:

```
Layer 7 — APPLICATION
Layer 6 — PRESENTATION
Layer 5 — SESSION
Layer 4 — TRANSPORT
Layer 3 — NETWORK
Layer 2 — DATA LINK
Layer 1 — PHYSICAL
```

Think of the layers like a production line in a factory. Each station (layer) does one specific job and then passes the product to the next station. When data is sent, it travels **top-to-bottom** through the layers. When data is received, it travels **bottom-to-top**.

How to Remember the Layer Order

Bottom to top (Layer 1 → 7):
Please Do Not Throw Sausage Pizza Away
(Physical → Data Link → Network → Transport → Session → Presentation → Application)

Top to bottom (Layer 7 → 1):
All People Seem To Need Data Processing

Key Takeaway

OSI has 7 layers. Data flows **down** the layers on the sending device, and back **up** the layers on the receiving device.

3. The Upper Layers (Layers 5–7)

The top three layers are called the **upper layers**. They handle application-level functions and are mostly implemented in **software**. In practice, network engineers rarely troubleshoot these layers — that is the job of software developers. However, you still need to understand what each one does.

Layer 7 — Application

The **Application layer** is the one closest to the user. It provides the **interface between the user's software and the network**.

Important point: the user application itself (for example, your web browser) does not sit at this layer. The **protocol** that the application uses does. Your browser invokes HTTP; HTTP is the Layer 7 protocol.

Examples of Layer 7 protocols:

Protocol	Full Name	What it Does
HTTP / HTTPS	HyperText Transfer Protocol	Loads web pages
FTP	File Transfer Protocol	Transfers files between computers
SMTP	Simple Mail Transfer Protocol	Sends email

Protocol	Full Name	What it Does
POP3 / IMAP	Post Office Protocol / Internet Message Access	Receives email
Telnet / SSH	—	Remote access to a device's command line
DNS	Domain Name System	Translates names (google.com) to IP addresses

What Layer 7 does:

- Identifies communication partners (who is the other device?)
- Checks if resources are available
- Synchronizes communication

Layer 6 — Presentation

The **Presentation layer** is responsible for **formatting data** so that the sending and receiving applications can understand each other. Think of it as a translator.

If the sending device uses one data format and the receiving device uses another, the Presentation layer converts between them.

Examples of data formats handled here:

Type	Examples
Text	ASCII, RTF, EBCDIC
Images	GIF, JPG, PNG, TIF
Audio	MP3, WAV, MIDI
Video	MPEG, AVI, MOV

The Presentation layer also handles **encryption** (scrambling data for security) and **compression** (reducing the size of data).

💭 Think About It

When you open a website and see a JPEG photo — which layer ensures your computer knows how to decode and display that JPEG? (Answer: Layer 6 — Presentation)

Layer 5 — Session

The **Session layer** establishes, manages, and terminates **sessions** — the ongoing conversations between two applications.

If a session is interrupted (for example, a network glitch), the Session layer attempts to recover it.

Sessions can be one of three types:

Type	Description	Example
Full-Duplex	Both devices transmit simultaneously	A phone call
Half-Duplex	Both devices can transmit, but not at the same time	A walkie-talkie
Simplex	Only one direction — one device transmits, the other only receives	A radio broadcast

Important Note

In practice, modern TCP/IP does not have a true Session layer protocol. Connection management is handled by lower layers — mainly by the Transport layer (TCP). The Session layer is important for understanding the OSI model, but you will not configure Session layer protocols on a Cisco router.

4. The Lower Layers (Layers 1–4)

The bottom four layers are called the **lower layers**. These are where the actual movement of data across a network happens. Network engineers work with these layers every day.

Layer 4 — Transport

The **Transport layer** is responsible for **reliable, end-to-end data delivery** between hosts.

Note the name carefully: it does not actually transmit data — the Physical layer does that. The Transport layer *prepares* data for transmission and ensures it arrives correctly.

Key functions of Layer 4:

- **Segmentation** — takes large pieces of data from the upper layers and breaks them into smaller chunks called **segments**. Large data is less likely to be lost or cause errors when broken into smaller pieces.
- **Sequencing** — each segment is given a sequence number, so the receiving device can reassemble them in the correct order even if they arrive out of sequence.
- **Acknowledgments** — the receiving device confirms receipt of data. If a segment is lost, the sender retransmits it.
- **Flow Control (Windowing)** — the two devices negotiate a data transfer rate so that a fast sender does not overwhelm a slow receiver.

Two Transport layer protocols in TCP/IP:

Protocol	Type	Description
TCP (Transmission Control Protocol)	Connection-oriented	Reliable — uses acknowledgments, sequencing, flow control
UDP (User Datagram Protocol)	Connectionless	Fast but unreliable — no acknowledgments, no guarantees

Connection-oriented vs. Connectionless:

- **Connection-oriented (TCP):** Before any data is sent, the two devices must first establish a connection and agree on parameters. Think of this like making a phone call — you must establish the call before speaking.
- **Connectionless (UDP):** Data is sent immediately with no prior setup. No guarantee of delivery. Think of this like sending a letter — you drop it in a mailbox and hope it arrives.

When is each used?

- **TCP** is used when reliability matters: loading a web page, downloading a file, sending email.
- **UDP** is used when speed matters more than reliability: live video calls, online gaming, DNS queries.

Key Takeaway

TCP = reliable but slower. UDP = fast but no guarantees. Layer 4 adds a **header** to data; the result is called a **Segment**.

Layer 3 — Network

The **Network layer** controls communication **between different networks** (internetwork communication). This is the layer that makes the internet possible.

Two key responsibilities:

- **Logical Addressing** — assigns unique IP addresses to devices. An IP address identifies both the host AND the network it belongs to.
- **Routing** — determines the best path from source to destination across multiple networks, then forwards the data along that path.

Key Layer 3 protocol:

- **IP (Internet Protocol)** — used in all modern networks (IPv4 and IPv6)

Key Layer 3 device:

- **Router** — reads IP addresses in the Layer 3 header and makes forwarding decisions

Key Takeaway

Layer 3 adds an IP header to the segment; the result is called a **Packet**. Routers operate at Layer 3.

Layer 2 — Data Link

The **Data Link layer** is responsible for transporting data **within a single network** — node to node. While Layer 3 moves data between networks, Layer 2 moves data between two directly connected devices.

The Data Link layer has two sublayers:

Sublayer	Full Name	Function
LLC	Logical Link Control	Acts as the bridge between physical hardware and higher layers; handles flow control and error checking
MAC	Media Access Control	Controls which device gets to use the physical medium and when; uses hardware (MAC) addresses

What Layer 2 adds:

Layer 2 wraps the Layer 3 packet in a **frame** by adding:

- A **Layer 2 Header** (containing source and destination MAC addresses)
- A **Layer 2 Trailer** (containing error-checking information — the FCS, Frame Check Sequence)

Common Layer 2 technologies:

Technology	Usage
Ethernet	Most common LAN technology
802.11 Wi-Fi	Wireless LAN
Frame-Relay / ATM	Older WAN technologies

Key Layer 2 device:

- **Switch** — reads MAC addresses in the Layer 2 header and forwards frames to the correct port

Key Takeaway

Layer 2 adds a header AND a trailer to the packet; the result is called a **Frame**. Switches operate at Layer 2.

Layer 1 — Physical

The **Physical layer** is the bottom of the stack — it handles the actual transmission of **raw bits (0s and 1s)** across the physical medium.

This layer converts digital bits into signals:

- **Electrical signals** for copper cables
- **Light pulses** for fiber optic cables
- **Radio waves** for wireless connections

What the Physical layer defines:

- Voltage levels and timing for electrical signals
- Physical connectors (RJ45, fiber connectors)
- Cable specifications (Cat5e, Cat6, multimode fiber)
- Maximum cable distances
- Wireless frequencies and transmission power

Key Layer 1 devices:

Cables, connectors, hubs, repeaters, network interface cards (NICs), wireless radios

Key Takeaway

Layer 1 transmits raw **Bits** across the physical medium. No header is added here — bits are just the electrical or optical signals on the wire.

5. Protocol Data Units (PDUs)

As data moves down the OSI stack, each layer **wraps the data** from the layer above it with its own header (and sometimes a trailer). This wrapping process is called **encapsulation**. The name for the "package" at each layer is the **PDU (Protocol Data Unit)**.

OSI Layer	PDU Name	What Is Added
7 — Application	**Data**	User data
6 — Presentation	**Data**	Formatting / encryption
5 — Session	**Data**	Session info
4 — Transport	**Segment**	Layer 4 Header (ports, sequencing, flow control)
3 — Network	**Packet**	Layer 3 Header (IP addresses)
2 — Data Link	**Frame**	Layer 2 Header (MAC addresses) + Layer 2 Trailer (FCS)
1 — Physical	**Bit**	Raw electrical / optical / radio signals

Visually, as data travels down the layers:

```
                 [ DATA ]                           ← Layers 7-5
   [ L4 Header ][ DATA ]                            ← Segment (Layer 4)
[ L3 Header ][ L4 Header ][ DATA ]                  ← Packet (Layer 3)
[ L2 Hdr ][ L3 Hdr ][ L4 Hdr ][ DATA ][ L2 Trl ]   ← Frame (Layer 2)
              010110010101101...                     ← Bits (Layer 1)
```

Key Takeaway

Segment = Transport layer PDU **Packet** = Network layer PDU **Frame** = Data Link layer PDU **Bit** = Physical layer PDU

6. Encapsulation & De-encapsulation

Encapsulation is the process of adding headers as data travels **down** the OSI model (from Application toward Physical) on the **sending** device.

De-encapsulation is the reverse — stripping headers as data travels **up** the OSI model (from Physical toward Application) on the **receiving** device.

Step-by-step: Sending a file

1. Your file application hands data to the **Transport layer** → a L4 header is added → creates a **Segment**
2. The Segment is handed to the **Network layer** → a L3 header (IP addresses) is added → creates a **Packet**
3. The Packet is handed to the **Data Link layer** → a L2 header (MAC addresses) and L2 trailer (FCS) are added → creates a **Frame**
4. The Frame is handed to the **Physical layer** → converted into **Bits** and transmitted on the wire

Step-by-step: Receiving a file

1. Physical layer receives bits from the wire → assembles them into a **Frame** → passes it up
2. Data Link layer checks the MAC addresses, validates the FCS, strips the L2 header and trailer → passes the **Packet** up
3. Network layer checks the IP address, strips the L3 header → passes the **Segment** up
4. Transport layer checks sequencing, reassembles data, strips the L4 header → passes the **Data** up to the application

Think About It

When a switch receives a frame, at which OSI layer does it process the information? And when a router receives a packet, at which layer does it operate? (Answer: Switch = Layer 2, Router = Layer 3)

7. Same-Layer vs. Adjacent-Layer Interaction

Two important concepts explain how layers communicate:

Adjacent-Layer Interaction

Interaction between **different layers on the same device**.

Example: The Transport layer receives data from the Session layer above it, adds a header, and passes the segment to the Network layer below it.

Same-Layer Interaction

Interaction between the **same layer on two different devices**.

Example: The Transport layer on your laptop (Layer 4) communicates with the Transport layer on the web server (Layer 4). They speak the same "language" and understand each other's headers — even though all the other layers are involved in actually moving the data between them.

This is a powerful concept: you can think about what Layer 4 is doing without worrying about what Layers 1, 2, and 3 are doing underneath. The layers are **independent**.

---

8. The TCP/IP (DoD) Model

The **TCP/IP model** (also called the **DoD model**) was developed by the US Department of Defense. This is the model that is actually used in modern networks — including the internet.

It is simpler than OSI, with only **4 layers**:

TCP/IP Layer	Equivalent OSI Layers	Example Protocols
Application	OSI Layers 7, 6, 5	HTTP, FTP, SMTP, DNS
Host-to-Host (Transport)	OSI Layer 4	TCP, UDP
Internet (Network)	OSI Layer 3	IP
Network Access (Link)	OSI Layers 2, 1	Ethernet, Wi-Fi

The TCP/IP model consolidates the OSI upper layers (Application, Presentation, Session) into a single **Application layer**, and the OSI lower layers (Data Link, Physical) into a single **Network Access layer**.

Key Takeaway

TCP/IP is the model the real internet runs on. OSI is the model we use to think and talk about networking. You need to know both.

Why does OSI still matter if TCP/IP is what's actually used? Because network engineers use OSI vocabulary every day. When someone says "Layer 2 problem" or "Layer 3 device," they are using OSI terminology. OSI is the shared language of networking.

---

9. Real-World Example — What Happens When You Browse a Website

Let's trace what happens at each OSI layer when you type `http://www.example.com` into your browser:

Layer	What Happens
7 — Application	Your browser invokes HTTP to send a request for the web page
6 — Presentation	The server knows how to encode the web page in HTML, JPEG images, etc. Encryption (HTTPS/TLS) may be applied here

Layer	What Happens
5 — Session	A session is established between your browser and the server (in TCP/IP, this is mostly handled by TCP)
4 — Transport	HTTP uses TCP. A connection is established. Data is broken into segments, each numbered for reliable delivery
3 — Network	IP determines the best path from your PC to the web server. Source and destination IP addresses are added
2 — Data Link	As the packet travels from device to device (PC → Switch → Router), MAC addresses are used to deliver the frame on each individual link
1 — Physical	Electrical signals or light pulses carry the bits across the cable (or radio waves carry them wirelessly)

💭 Think About It

Your web page loads, but some images are missing. Which layer is most likely responsible for the missing images? (Answer: Layer 6 — Presentation, which handles image formats like JPEG and GIF)

Day 2 Summary

Concept	What to Remember
OSI Model	7 layers: Physical, Data Link, Network, Transport, Session, Presentation, Application
TCP/IP Model	4 layers: Network Access, Internet, Host-to-Host, Application — this is what the real internet uses
Encapsulation	Adding headers as data travels DOWN the layers (sending)
De-encapsulation	Stripping headers as data travels UP the layers (receiving)
PDU — Segment	Layer 4 (Transport) PDU
PDU — Packet	Layer 3 (Network) PDU
PDU — Frame	Layer 2 (Data Link) PDU
PDU — Bit	Layer 1 (Physical) PDU
Layer 1 — Physical	Raw bit transmission; cables, connectors, NICs
Layer 2 — Data Link	Node-to-node; MAC addresses; Switch
Layer 3 — Network	Network-to-network; IP addresses; Router
Layer 4 — Transport	End-to-end; TCP (reliable) and UDP (fast)
Layer 5 — Session	Establishes / manages / terminates sessions
Layer 6 — Presentation	Data formatting, encryption, compression
Layer 7 — Application	Interface between user software and the network; HTTP, FTP, SMTP
Same-layer interaction	Layer N on Device A communicates with Layer N on Device B

Concept	What to Remember
Adjacent-layer interaction	One layer passes data to the layer directly above or below it on the same device

Review Questions

Test yourself before the next session:

1. How many layers does the OSI model have? List them in order from Layer 1 to Layer 7.
2. What is the PDU name at Layer 3? What header information is added at that layer?
3. What is the difference between TCP and UDP? Give one example of when you would use each.
4. A switch reads the destination MAC address and forwards a frame to the correct port. At which OSI layer is it operating?
5. What is encapsulation? What is de-encapsulation?
6. Data travels from Layer 7 down to Layer 1 on the sending device. What is this process called?
7. At which layer does a router operate? What address does it use to make forwarding decisions?
8. What are the four layers of the TCP/IP (DoD) model?
9. The Presentation layer can perform two security/efficiency functions. What are they?
10. What is "same-layer interaction"? Give an example.