UFSM00741

Fundamentals of Networks and Protocols for OT-ICS

Prof. Dr. Luiz F. Freitas-Gutierres
luiz.gutierres@ufsm.br
linkedin.com/in/lffreitas-gutierres

[Introduction #1]. Basic Knowledge of Information Technology

UFSM

CT
CENTRO DE TECNOLOGIA - UFSM

LAPES
LABORATÓRIO DE ANÁLISE E PROTEÇÃO DE SISTEMAS ELÉTRICOS

[#0]. Luiz F. Freitas-Gutierres

(LinkedIn)

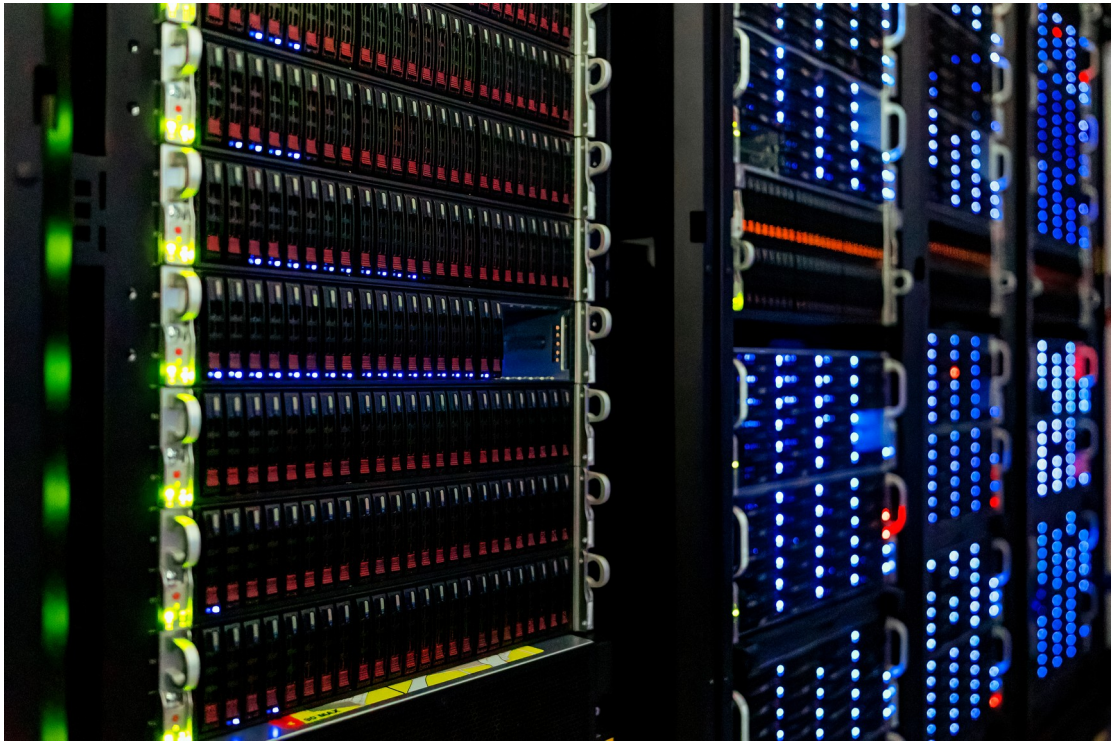
- **Professor** (UFSM-CT-DESP).
    - Bachelor's degree (2010), master's degree (2013), teaching license (2013), and doctoral degree (2018), all in electrical engineering from UFSM.
- **Researcher** (CEESP & LAPES).
- Author of ***Ind.Cyber.Sec Letters***.
    - `https://github.com/substationworm/IndCyberSecLetters`

Areas of Interest:

- 🕵️ Industrial cybersecurity.
- 🕵️ Cyber threat hunting.
- ⚡ Automation of electrical power systems.

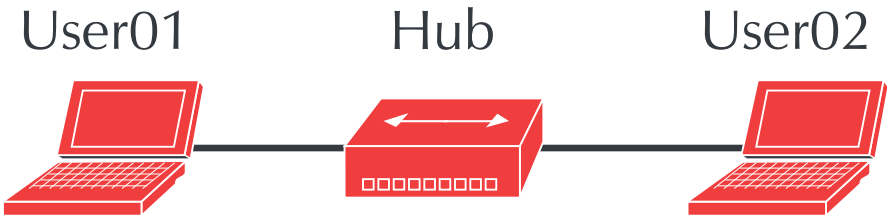
[#1]. Summary

- Internetworking Basics.
  - 👉 Hub.
  - 👉 Switch.
  - 👉 Router.
- The OSI Model.
  - 👉 Ethernet Networking.
  - 👉 Data Encapsulation.
- Introduction to TCP/IP.
  - 👉 TPC/IP Model.
  - 👉 IP Addressing.



Note. *Server racks*, NOIRLab/NSF/AURA/T. Slovinský, 2022, Wikimedia Commons. CC-BY 4.0.

[#2]. Internetworking Basics



Note. *A basic network*, Luiz F. Freitas-Gutierres, 2025. CC-BY 4.0.

🌐 Basic **local area network (LAN)** connected using a **hub**.

- One collision domain & one broadcast domain.

- A hub serves as an exchange point at the logical center of the network, with cables plugged into its ports.

🧟 A hub relays incoming packets to all ports and forwards them to the nodes connected to those ports. **There is no information management**.

🧟 Only one packet can travel through the network at a time (Ethernet's collision detection). In a 10/100 Mbps network, a hub would be forced to operate at 10 Mbps.

[#2]. Internetworking Basics

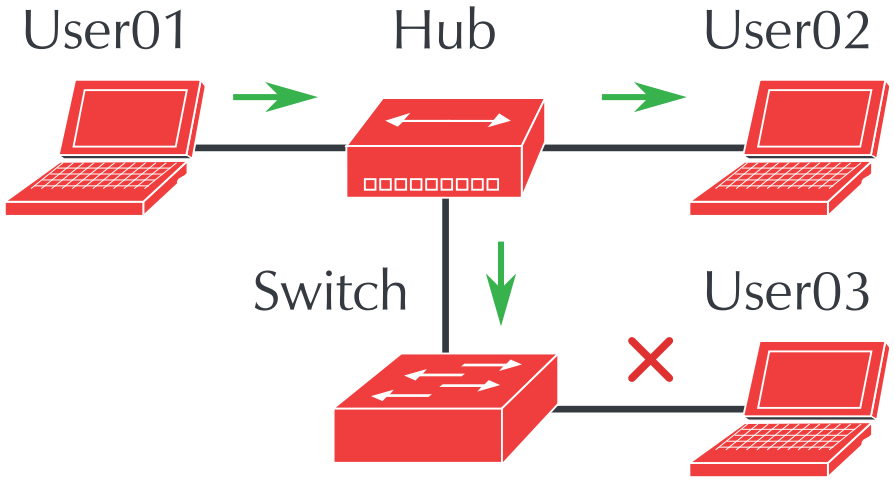
🌐 Basic LAN with a hub and a **switch**.

- Two collision domains.
- One broadcast domain.

🌐 Switches read the address section of each incoming packet to determine its destination.

👍 Switches can handle multiple connections simultaneously. Each switch port functions as a separate segment (**multiple segments**).

👍 Devices can transmit and receive data simultaneously (**full-duplex mode**).



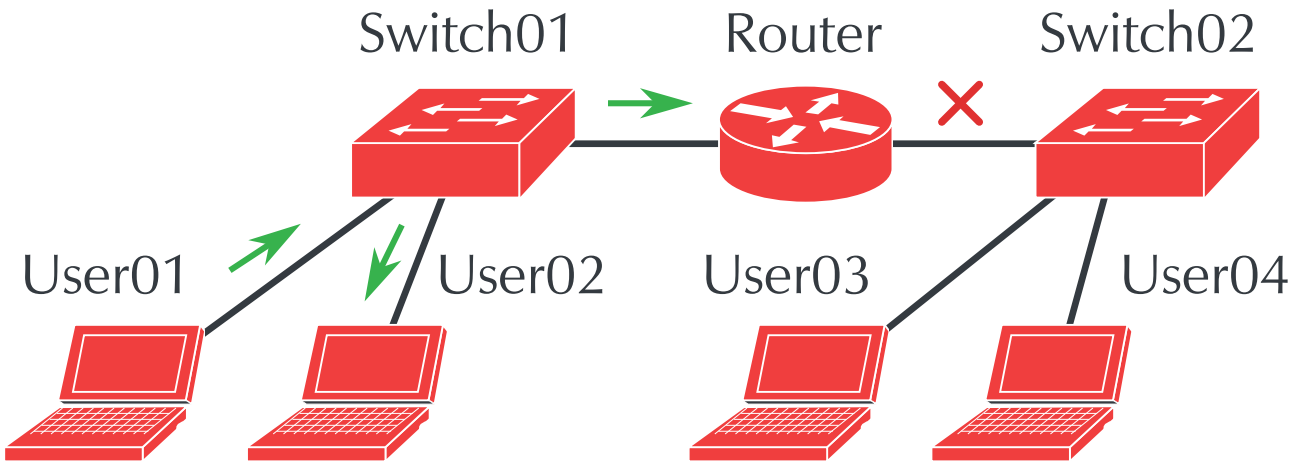
Note. A basic network with a switch (source = User01, destination: User02), Luiz F. Freitas-Gutierres, 2025. CC-BY 4.0.

[#2]. Internetworking Basics

🌐 **Routers** divide a broadcast domain.

- Six collision domains.
- Two broadcast domains.

🌐 Routers examine the address contained in each packet and forward it to its ultimate destination.



Note. A internetwork (source = User01 [broadcast]), Luiz F. Freitas-Gutierres, 2025. CC-BY 4.0.

🚨 A **collision domain** is a scenario in which a device transmits a packet within a network segment, and all other devices connected to that same segment are forced to process it. If another device attempts to transmit at the same time, a collision will occur.

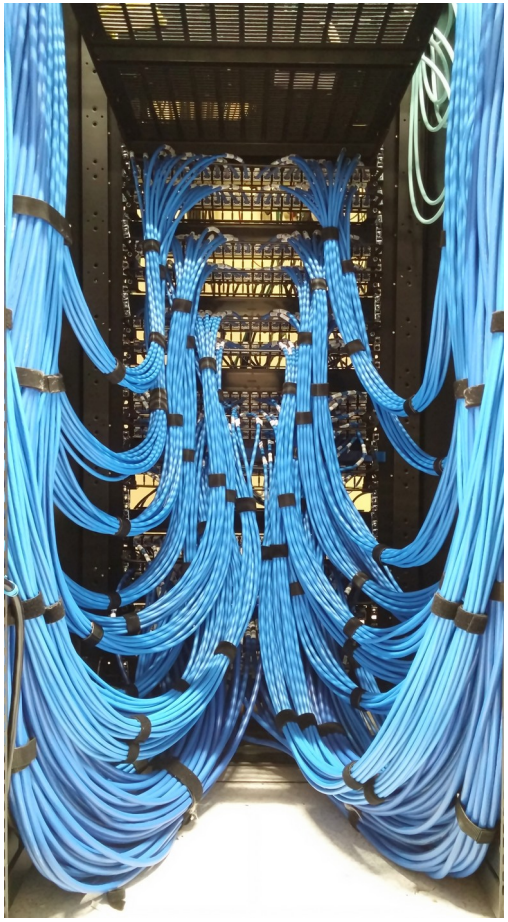
[#2]. Internetworking Basics

🚨 A **broadcast domain** is a section of the network where any device can send broadcast messages, and all other devices within the same domain will receive them.

1️⃣ Switches keep all devices within the same broadcast domain.

2️⃣ Routers separate broadcast domains, preventing broadcast packets from crossing between networks.

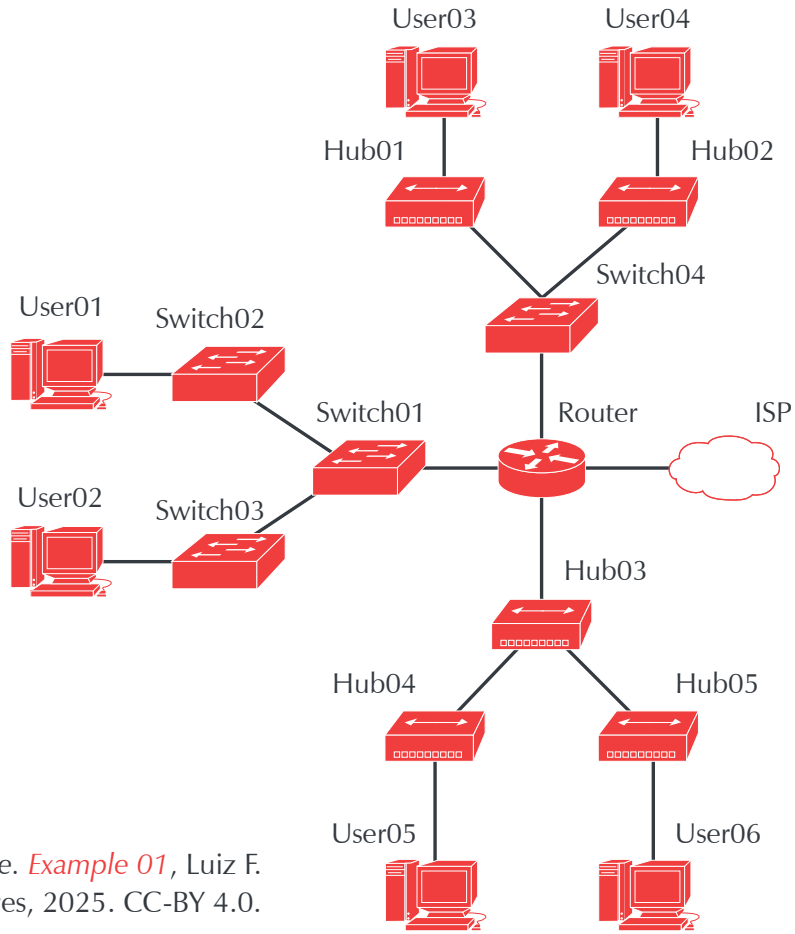
3️⃣ Switches increase the number of collision domains in a network, providing more bandwidth to users.



Note. *Ethernet patch panel*, Kbh3rd, 2017, Wikimedia Commons. CC-BY 4.0.

[#2]. Internetworking Basics (*Example 01*)

- 📝 Identify the number of collision domains.
- 📝 Quantify the number of broadcast domains.
- 📝 Assess which is the "best" network connected to the router.



Note. *Example 01*, Luiz F. Freitas-Gutierres, 2025. CC-BY 4.0.

[#2]. Internetworking Basics (*Example 01*)

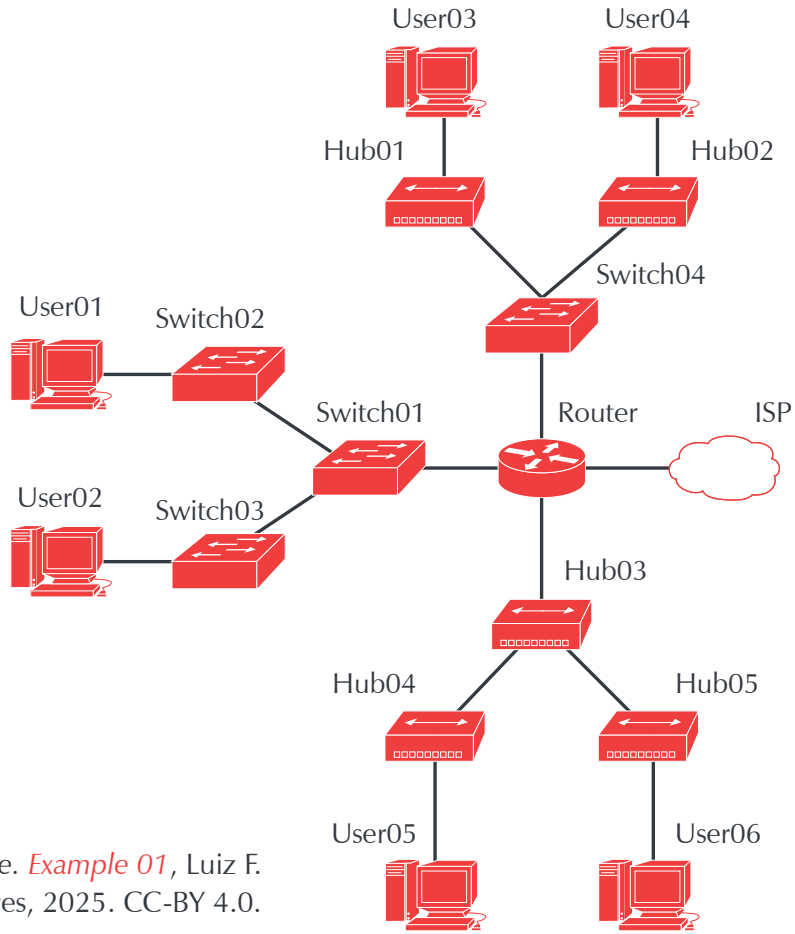
📝 Identify the number of collision domains.
📝 Quantify the number of broadcast domains.
📝 Assess which is the "best" network connected to the router.

Answers:

- Nine collision domains.

- Three broadcast domains.

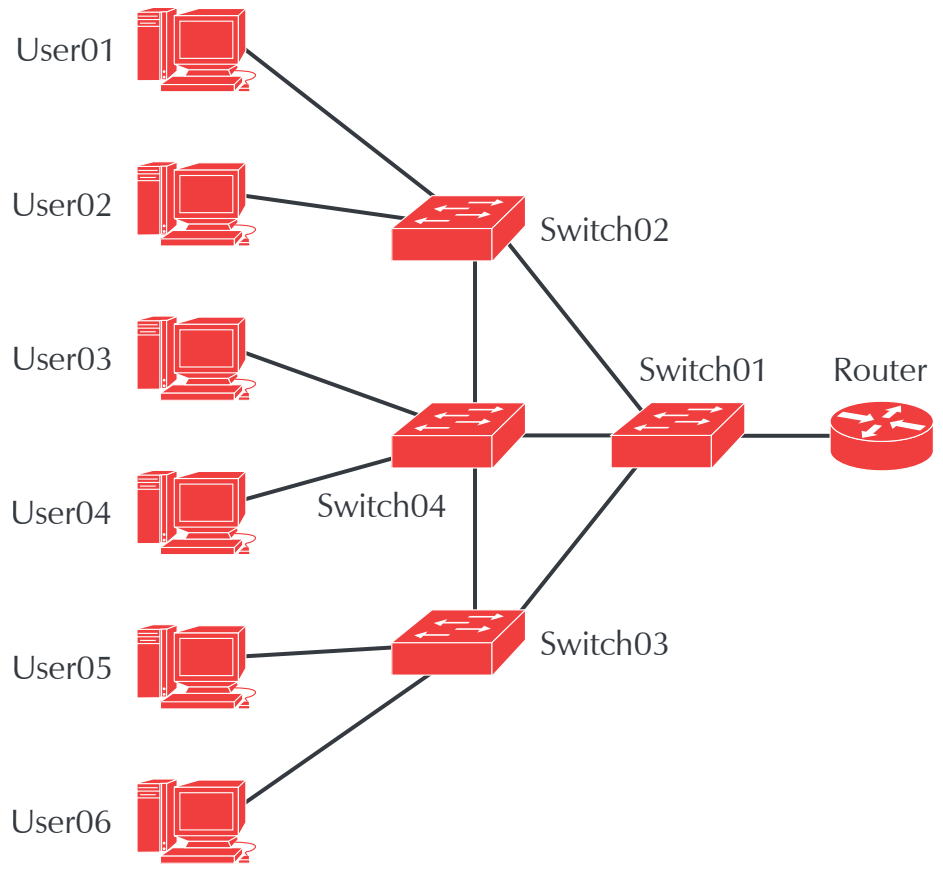
- The network of Switch01, despite all its devices still sharing the same broadcast domain.



Note. *Example 01*, Luiz F. Freitas-Gutierres, 2025. CC-BY 4.0.

[#2]. Internetworking Basics (*Example 02*)

- Identify the number of collision domains.
- Quantify the number of broadcast domains.



Note. *Example 02*, Luiz F. Freitas-Gutierres, 2025. CC-BY 4.0.

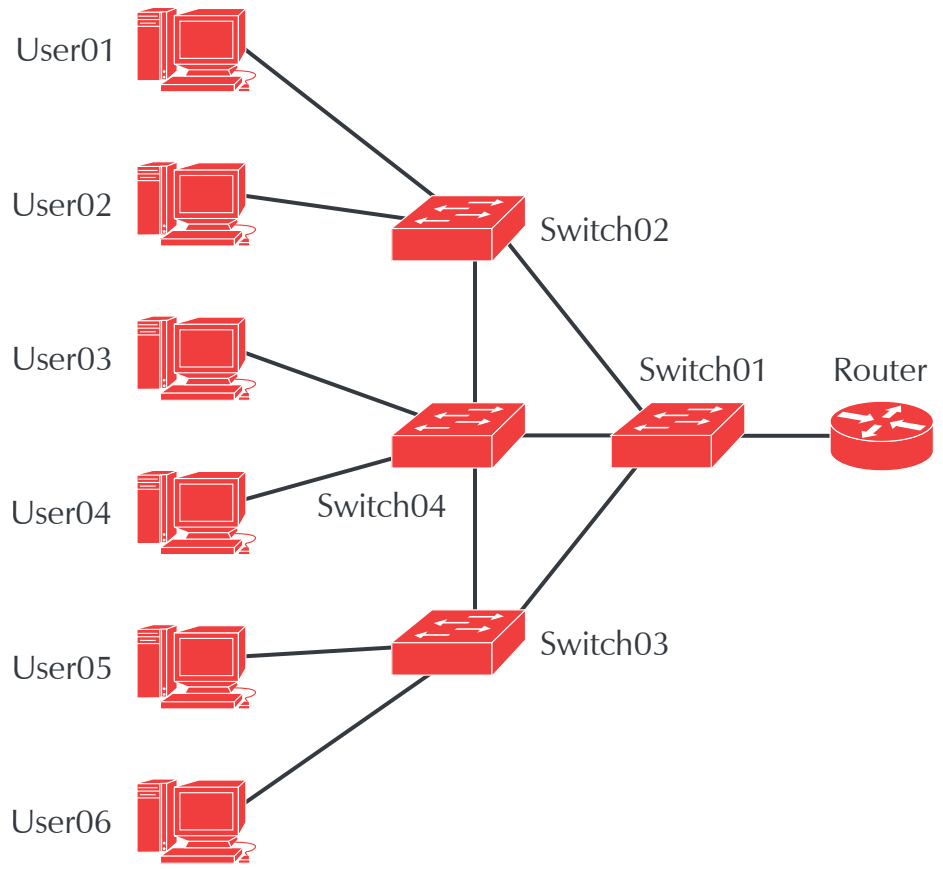
[#2]. Internetworking Basics (*Example 02*)

- Identify the number of collision domains.
- Quantify the number of broadcast domains.

Answers:

- Twelve collision domains.

- One broadcast domains.



Note. *Example 02*, Luiz F. Freitas-Gutierres, 2025. CC-BY 4.0.

[#3]. The OSI Model

Layer 07	**Application**
Layer 06	**Presentation**
Layer 05	**Session**
Layer 04	**Transport**
Layer 03	**Network**
Layer 02	**Data Link**
Layer 01	**Physical**

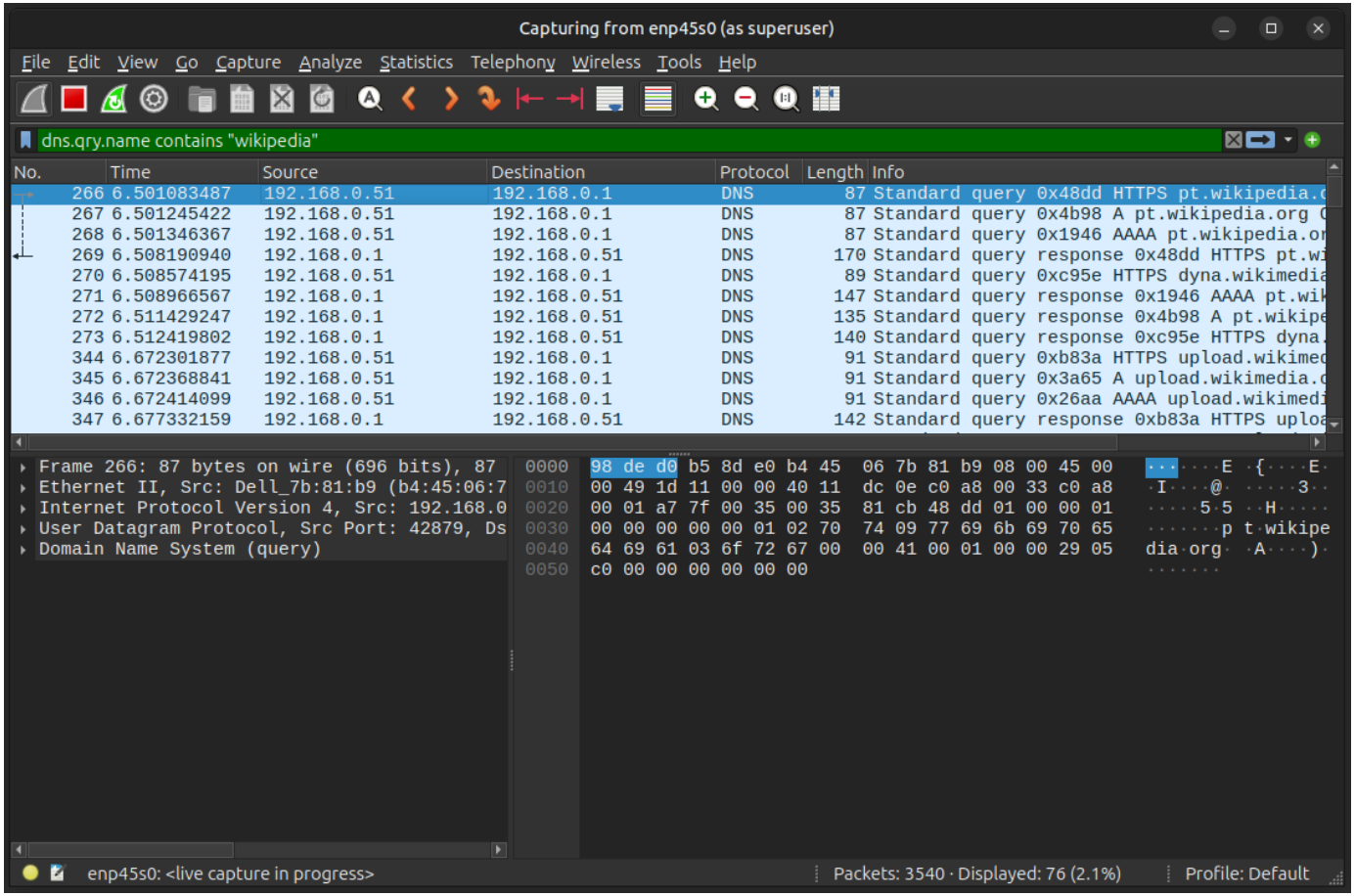
Note. *The OSI model (Fig. 01)*, Luiz F. Freitas-Gutierres, 2025. CC-BY 4.0.

[#3]. The '*open systems interconnection*' (OSI) Model

Layer 07	**Application:** The point where users communicate with the computer (e.g., HTML).
Layer 06	**Presentation:** Presents data to the application layer (data translation, code formatting, and application encryption [e.g., SSL, TLS]).
Layer 05	**Session:** Manages communication between devices.
Layer 04	**Transport:** TCP/UDP, HTTP (port 80), HTTPS (port 443), segments, etc.
Layer 03	**Network:** Routers, IP addresses (e.g. 192.168.1.100), and packets.
Layer 02	**Data Link:** Switches, MAC addresses (e.g., 3A:5F:BC:92:AD:17), and frames.
Layer 01	**Physical:** Electrical signals, cables, connectors, etc.

Note. *The OSI model (Fig. 02)*, Luiz F. Freitas-Gutierres, 2025. CC-BY 4.0.

[#3]. The OSI Model (*Example 03*)



Note. *Example 03*, Luiz F. Freitas-Gutierres, 2025. CC-BY 4.0.

[#3]. The OSI Model

🚨 **Data encapsulation:** 7 ➡️ 6 ➡️ 5 ➡️ 4 ➡️ 3 ➡️ 2 ➡️ 1.

🚨 **Data decapsulation:** 7 ⬅️ 6 ⬅️ 5 ⬅️ 4 ⬅️ 3 ⬅️ 2 ⬅️ 1.

🪜 Layers 7-6-5 produce the protocol data unit (PDU), referred to here as "**data**" (`0101011...`), which is then delivered to Layer 4 (Transport).

📍 Application (7): HTTP + DNS (browser).

📍 Presentation (6): Enconding (ASCII), encrypting (SSL/TSL), compression (gzip).

📍 Session (5): Dialog management.

🪜 Layer 4 identifies (via port address) which **application/client** is making the request (**source, `Src`**) and which **service/server** will receive the request (**destination, `Des`**).

🔨 PDU = Segments (data broken into smaller pieces for performance, security, and multiplexing).

👉 HTTP: `Src` = Randomly assigned by the client, `Des` = Port 80.

[#3]. The OSI Model

❗ TCP: Reliability > Speed.

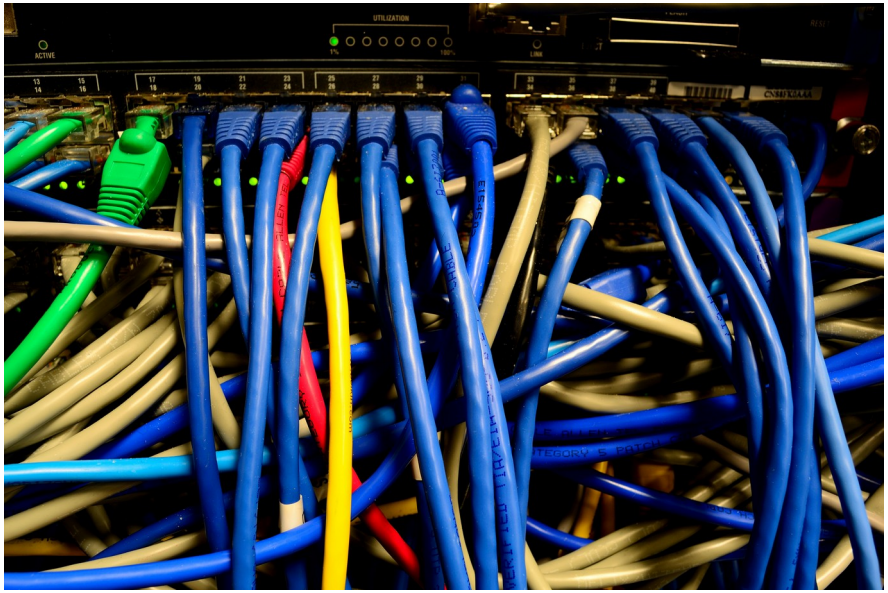
❗ UDP: Speed > Reliability.

🪜 Layer 3 operates with **packets** (PDU), which include a `Src` and a `Des` based on **IP addresses**.

👉 The sender and receiver are devices.

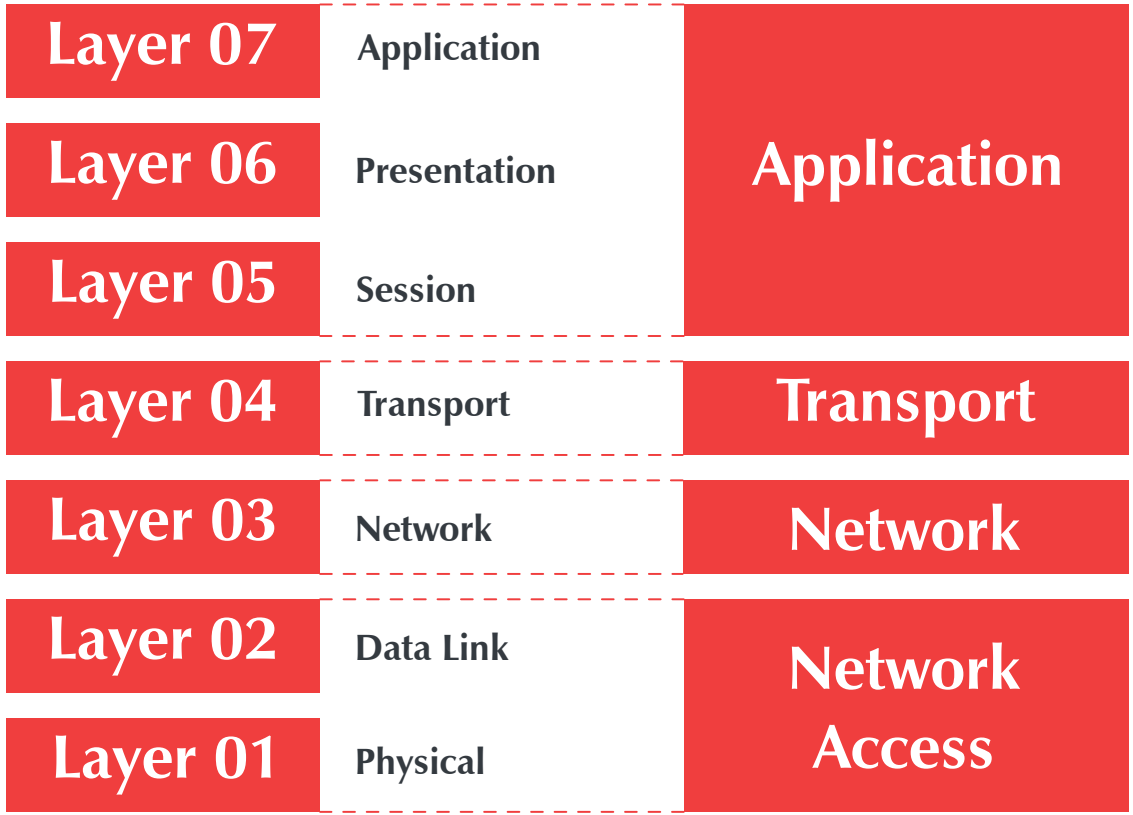
🪜 Layer 2 generates **frames** (PDU) for communication, with `Scr` and `Des` at the physical level (**MAC addresses**).

🪜 Layer 1 ultimately converts data into **electrical signals**, which are transmitted through cables and connectors.



Note. *Ethernet switch*, Raysonho @ Open Grid Scheduler / Grid Engine, 2011, Wikimedia Commons. CC0 1.0 Universal.

[#4]. The TCP/IP Model



🚨 **TCP** = Transmission Control Protocol.

🚨 **IP** = Internet Protocol.

Note. *The TCP/IP*, Luiz F. Freitas-Gutierres, 2025. CC-BY 4.0.

UFSM00741

Fundamentals of Networks and Protocols for OT-ICS

Prof. Dr. Luiz F. Freitas-Gutierres
luiz.gutierres@ufsm.br
linkedin.com/in/lffreitas-gutierres

[Introduction #1]. Basic Knowledge of Information Technology

UFSM

CT
CENTRO DE TECNOLOGIA - UFSM

LAPES
LABORATÓRIO DE ANÁLISE E PROTEÇÃO DE SISTEMAS ELÉTRICOS