# Networking 101

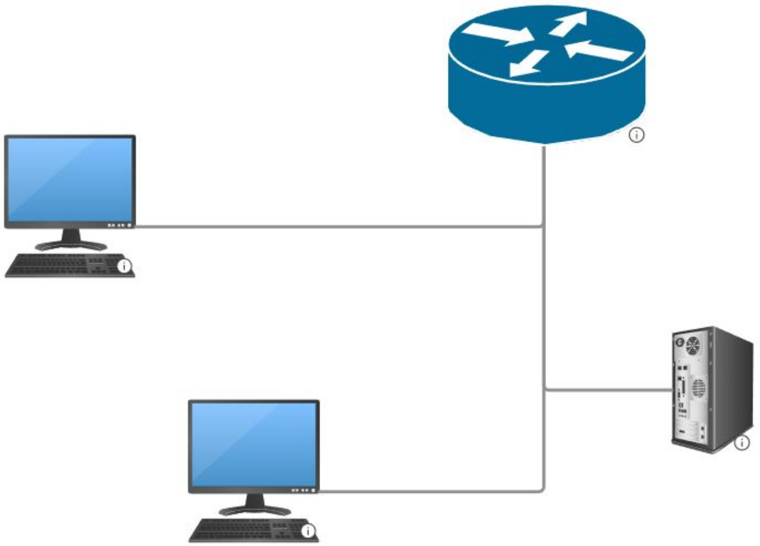
Cybersecurity Club

# Why do we care about network traffic?

Without basic networking knowledge, cybersecurity professionals are like soldiers navigating a battlefield without a map

# What is a Network

2 or more devices connected together in order to sharing information



# Network Types

LAN - Local Area Network

WAN - Wide Area Network

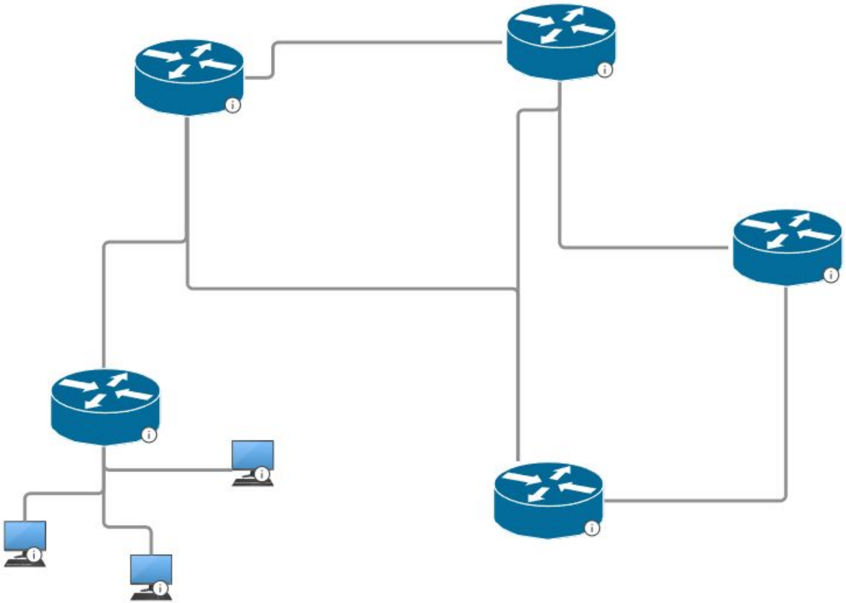
WLAN - Wireless Local Area Network

There are others like CAM or MAN, but they aren’t commonly mentioned

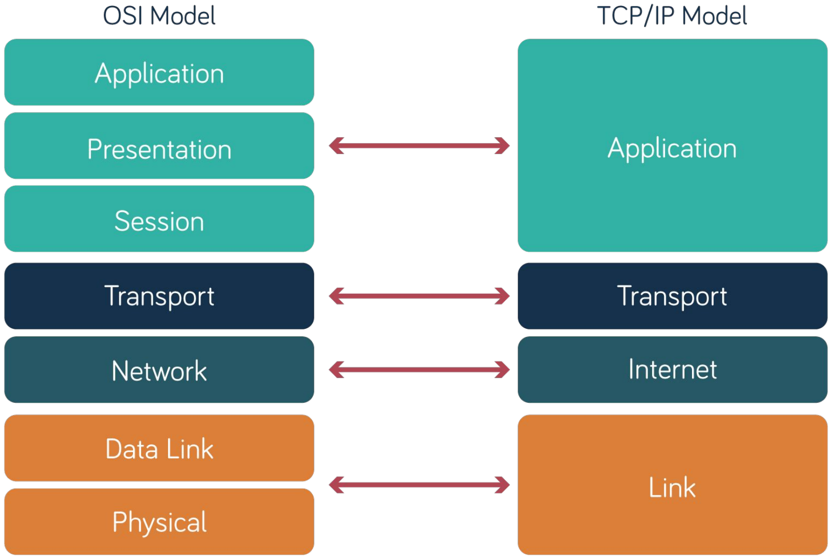
# What is the internet

Globally interconnected network

They all use TCP/IP to ensure common communication between all devices



# OSI Model vs TCP/IP Model

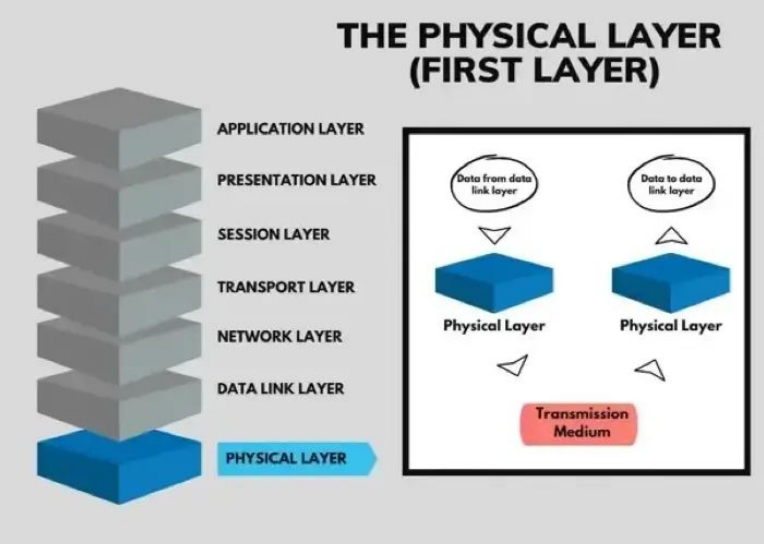


# Layer 1- Physical

Handles the actual physical transmission of raw binary data

It includes hardware like cables, fibre optic equipment and wireless transmitters or antennas

Ethernet and IEEE 802.11 (Wi-Fi)

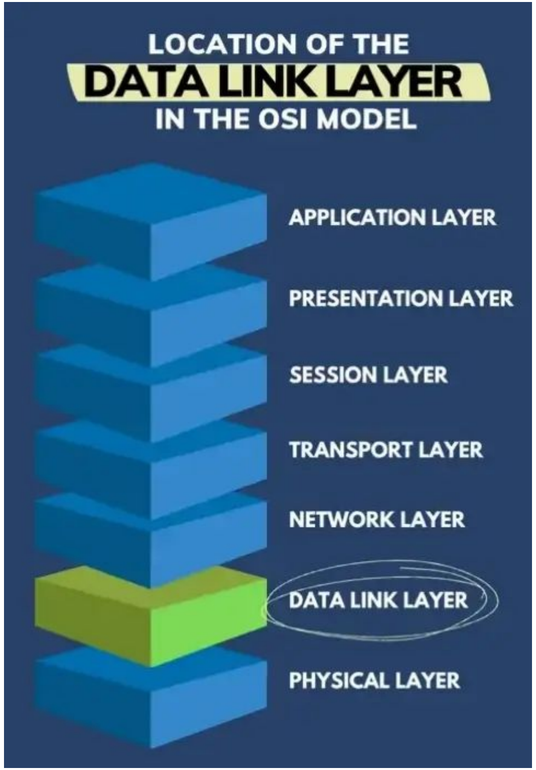


# Layer 2 - Data Link

node-to-node data transfer

packages data into frames and ensures reliable transfer between devices over the physical medium

MAC Addresses and ARP



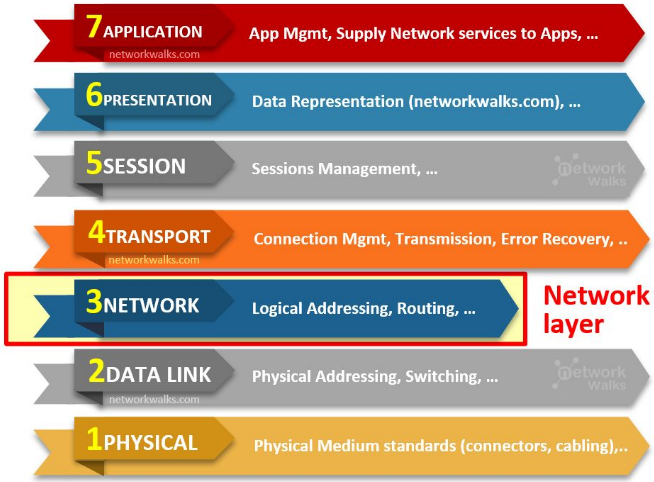
# Layer 3 - Network

Handles routing: moving packets from source to destination across multiple networks

Uses logical addressing

IP (Internet Protocol)

OSI Model



7 APPLICATION — App Mgmt, Supply Network services to Apps, ...

6 PRESENTATION — Data Representation (networkwalks.com), ...

5 SESSION — Sessions Management, ...

4 TRANSPORT — Connection Mgmt, Transmission, Error Recovery, ..

3 NETWORK — Logical Addressing, Routing, ...

2 DATA LINK — Physical Addressing, Switching, ...

1 PHYSICAL — Physical Medium standards (connectors, cabling),..

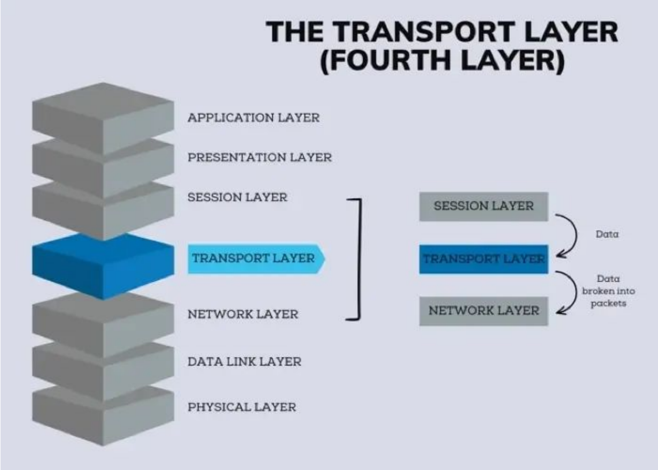
Network layer

# Layer 4 - Transport

Manages segmentation, flow control, and error handling

TCP (Transmission Control Protocol) – reliable, connection-based

UDP (User Datagram Protocol) – fast, connectionless



# Layer 5,6 and 7 - Session, Presentation, and Application

Provides network services to applications

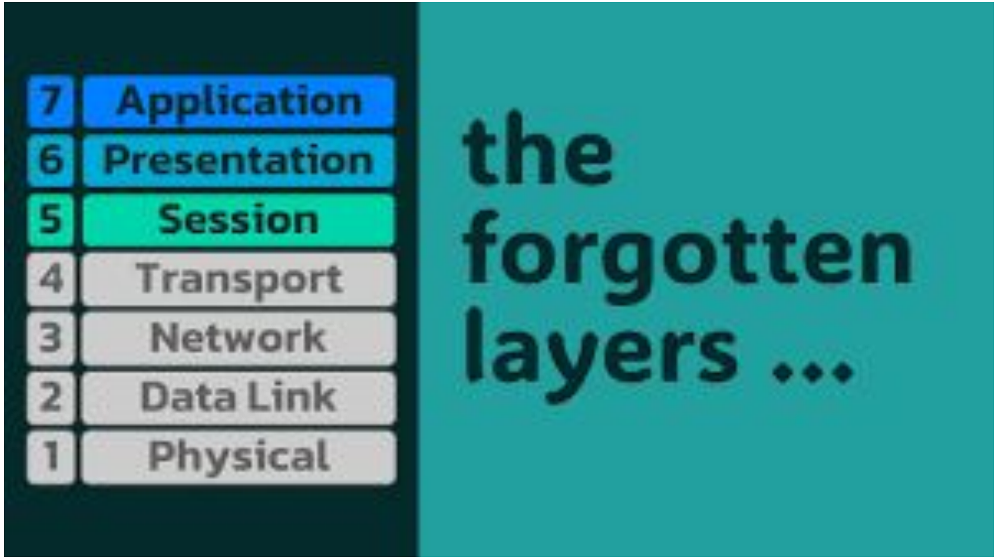
Deals with high-level protocols and user data.

Often obscured into each other

L5 - SMB

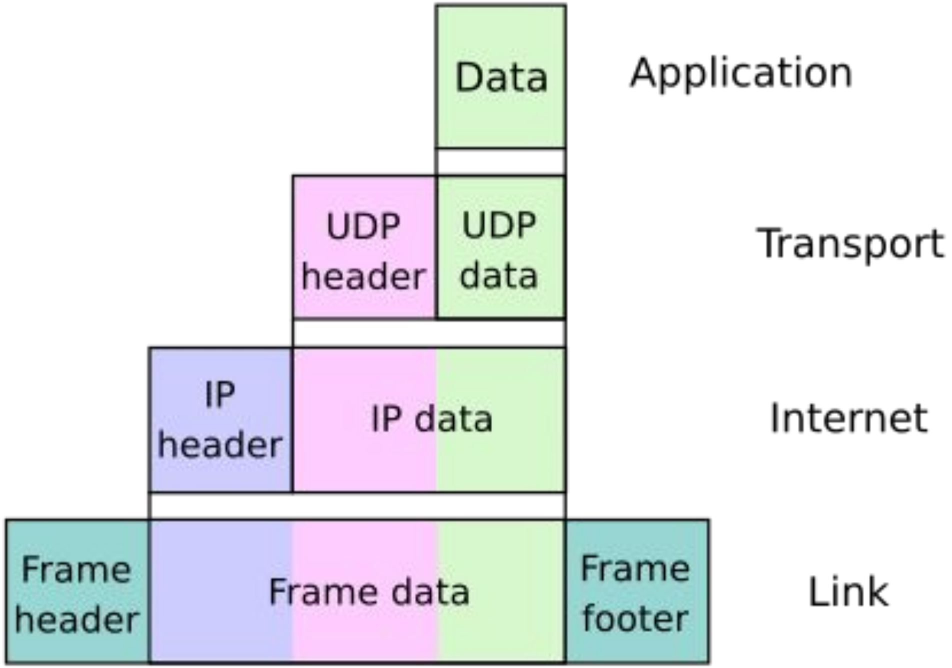
L6 - SSL/TLS

L7 - HTTP, DNS, SSH, Telent



# Encapsulation / Decapsulation

When data is prepared to be sent out by the user, it will be encapsulated by each layer down it touches.



# How do you connect to a service?

You send your packet to an IP addresses

Different services are host on commonly known ports

HTTP - 80

HTTPS - 443

SSH - 22

FTP - 20 and 21

# Wireshark Lab

Open your Vm of choice (kali is preferred)

Go to https://github.com/utica-cybersecurity-club

Download the files underneath the networking lab files

Open them with Wireshark