Ethernet Networking Basics

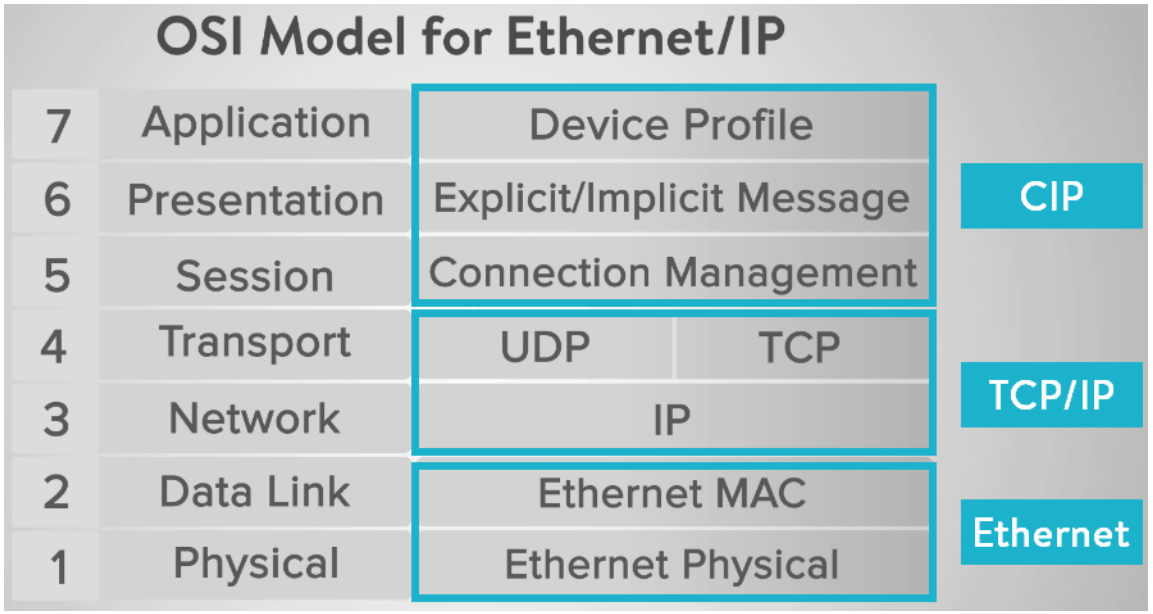
What Is the OSI Model?

- The **OSI Model** (Open Systems Interconnection) is a **7-layer framework** that describes how data moves through a network.
- Each layer has a specific role and only talks to the layers directly above or below it.
- Think of it like a **postal system** or a **relay team** — each person (layer) does their part and passes the data along.

Communication Layers

For the physical layer, Ethernet will be the primary item discussed in this document

Most industrial applications do not use TCP/UDP/IP directly but are built on top of those layers



Layer	Name	What It Does	Example	Who Uses It
7	**Application**	User-level interaction, interfaces for data exchange	Web browsers, HMIs, PLC programs	**You, PLC engineers, SCADA operators**
6	**Presentation**	Translates/encodes data formats, compression, encryption	JSON, XML, JPEG, ASCII, SSL	**Software developers, protocol stacks**
5	**Session**	Starts/stops communication sessions	Logging in, opening secure sessions	**Operating system, protocol libraries**
4	**Transport**	Breaks data into chunks, manages reliable delivery (TCP/UDP)	TCP, UDP	**OS kernel, networking code**
3	**Network**	Routes data across networks using logical addressing	Routers, IP addresses	**Routers, firewalls, IT staff**
2	**Data Link**	Transfers data between devices on the same network segment	Ethernet frames, MAC addresses	**NICs**(network interface card), **switches**
1	**Physical**	Sends raw bits via physical medium	Ethernet cables, voltage, fiber optics	**Electricians, hardware techs**

What Are EtherNet/IP, PROFINET, and Modbus TCP?

These are all **industrial communication protocols** that run over **Ethernet**, used to connect **PLCs**, **robots**, **sensors**, and other automation devices.

Think of them as **different "languages" industrial devices speak over the same Ethernet "wires."**

1. EtherNet/IP (Ethernet Industrial Protocol)

•**What it is:** An industrial protocol built on **standard Ethernet + TCP/IP**, using **CIP (Common Industrial Protocol)**.

•**Who uses it:** Rockwell/Allen-Bradley PLCs (CompactLogix, ControlLogix), Omron, etc.

•**Strengths:**

- •Real-time I/O and reliable messaging.
- •Supports both **explicit (TCP)** and **implicit (UDP)** communication.
- •Object-oriented – each device has "objects" with attributes and services.

Example use: A CompactLogix PLC sends high-speed sensor data to a robot over EtherNet/IP.

OSI Layer	EtherNet/IP Implementation
Layer 7: Application	CIP (Common Industrial Protocol) – objects, services, attributes
Layer 6: Presentation	Managed by CIP (data formatting, encoding/decoding)
Layer 5: Session	Managed by CIP (establishing/maintaining object communications)
Layer 4: Transport	TCP (for Class 3 explicit messaging) UDP (for Class 1 implicit I/O)
Layer 3: Network	IP (Internet Protocol)
Layer 2: Data Link	Ethernet (IEEE 802.3 – MAC addressing, frame formatting)
Layer 1: Physical	Ethernet cabling (Cat5e, Cat6, etc.), electrical signaling

1. EtherNet/IP (Ethernet Industrial Protocol)

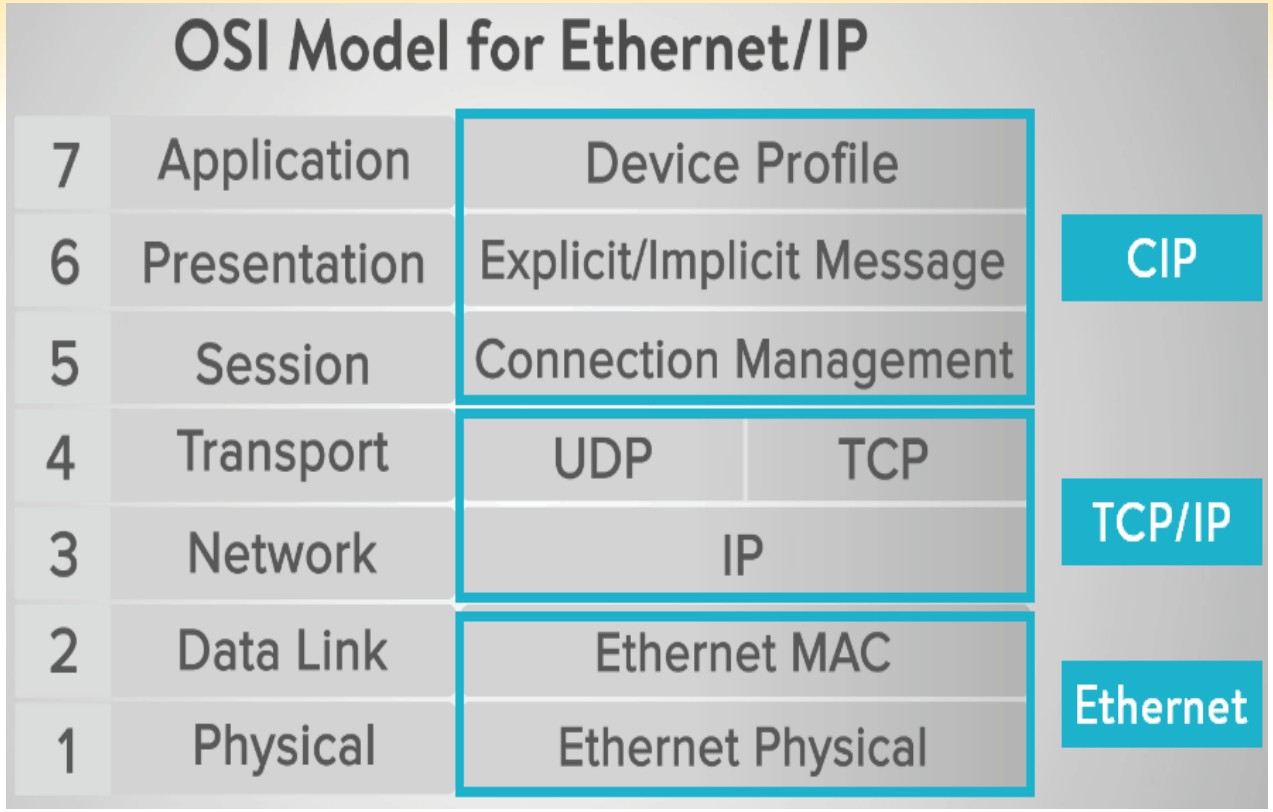
•**What it is:** An industrial protocol built on **standard Ethernet + TCP/IP**, using **CIP (Common Industrial Protocol)**.

•**Who uses it:** Rockwell/Allen-Bradley PLCs (CompactLogix, ControlLogix), Omron, etc.

•**Strengths:**

- •Real-time I/O and reliable messaging.
- •Supports both **explicit (TCP)** and **implicit (UDP)** communication.
- •Object-oriented – each device has “objects” with attributes and services.

Example use: A CompactLogix PLC sends high-speed sensor data to a robot over EtherNet/IP.



2. PROFINET (Process Field Network over Ethernet)

•**What it is:** Siemens' industrial Ethernet protocol, built on standard Ethernet but with additional support for **real-time** and **isochronous** (precise timing) communication.

•**Who uses it:** Siemens S7-1200/S7-1500 PLCs, industrial drives, HMIs.

•**Strengths:**

- •Supports **Real-Time (RT)** and **Isochronous Real-Time (IRT)** for motion control.
- •Integrated with TIA Portal for configuration.
- •Uses **GSDML** files to describe device capabilities.

Example use: A Siemens PLC controls multiple VFDs and IO blocks on a high-speed packaging line using PROFINET.

3. Modbus TCP (Modbus over Ethernet)

- **What it is:** A **simplified, open protocol** originally designed for serial devices, now adapted to Ethernet.

- **Who uses it:** Schneider Electric, Wago, AutomationDirect, many low-cost devices.
  - Note: modbus RTU used to be common for rockwell VFDs is different from modbus TCP

- **Strengths:**
  - Very simple and easy to implement.
  - Master/slave (client/server) model — one device polls others for data.
  - Works well for basic data exchange (no object model or device discovery).

Example use: A Raspberry Pi reads temperature data from a Modbus TCP sensor on a lab bench.

Modbus 2-Wire (RS-485) vs Modbus TCP – Key Differences

Feature	**Modbus RTU (RS-485, 2-wire)**	**Modbus TCP (Ethernet)**
Physical Layer	RS-485 (2-wire twisted pair)	Ethernet (Cat5/6 cables)
Data Link	Serial bytes over voltage differential	Ethernet frames over TCP/IP
Speed	Slower (typically 9600–115200 baud)	Faster (10/100 Mbps or more)
Distance	Long (up to 1,200 meters)	Shorter (300ft standard per switch/hop)
Wiring	2 wires (plus optional ground/shield)	4/8-wire Cat5e/Cat6
Topology	Bus (daisy chain, one master, many slaves)	Star (via switch/router), client-server model
Addressing	Slave IDs (1–247)	IP addresses + Unit ID (usually 0 or 1)
Protocol Format	Binary or ASCII framed by start/stop/parity bits	Uses TCP/IP headers
Reliability	Susceptible to EMI without shielding	More robust if network is managed
Setup Complexity	Simple – minimal config, but manual addressing	Easier to integrate with modern systems
Use Case	Legacy PLCs, simple sensor networks, long runs	SCADA systems, modern PLCs, faster IO

⚠️ **Important Note:**

- Both protocols **use the same data structure** (function codes, registers), but the **wrapping and transmission methods** are different.
- Some devices (like gateways or dual-protocol sensors) can **convert between them**.

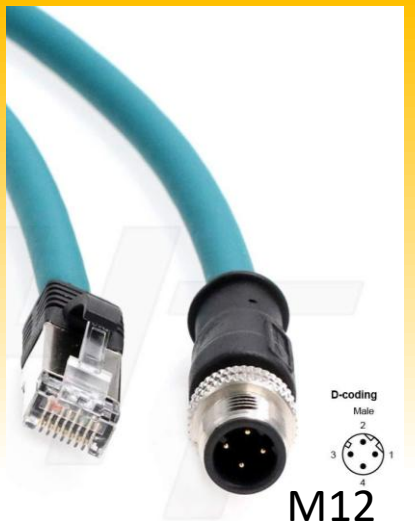
Physical Layer

Ethernet comes with a variety of connectors

- RJ45
- M12 4 pin D-coded
- M12 8 pin X-coded
- M12 8 pin
- Sfp connectors

Just because the system you are using has the correct connector does not mean it actually uses ethernet communication

RJ 45



M12
D-Coded

M12
X-Coded

SFP

M12
8 pin

Physical layer

The most common connectors are RJ 45 and M12 D-coded cables

M12 D-Coded cables are limited to 4 conductors while RJ 45 can have up to 8

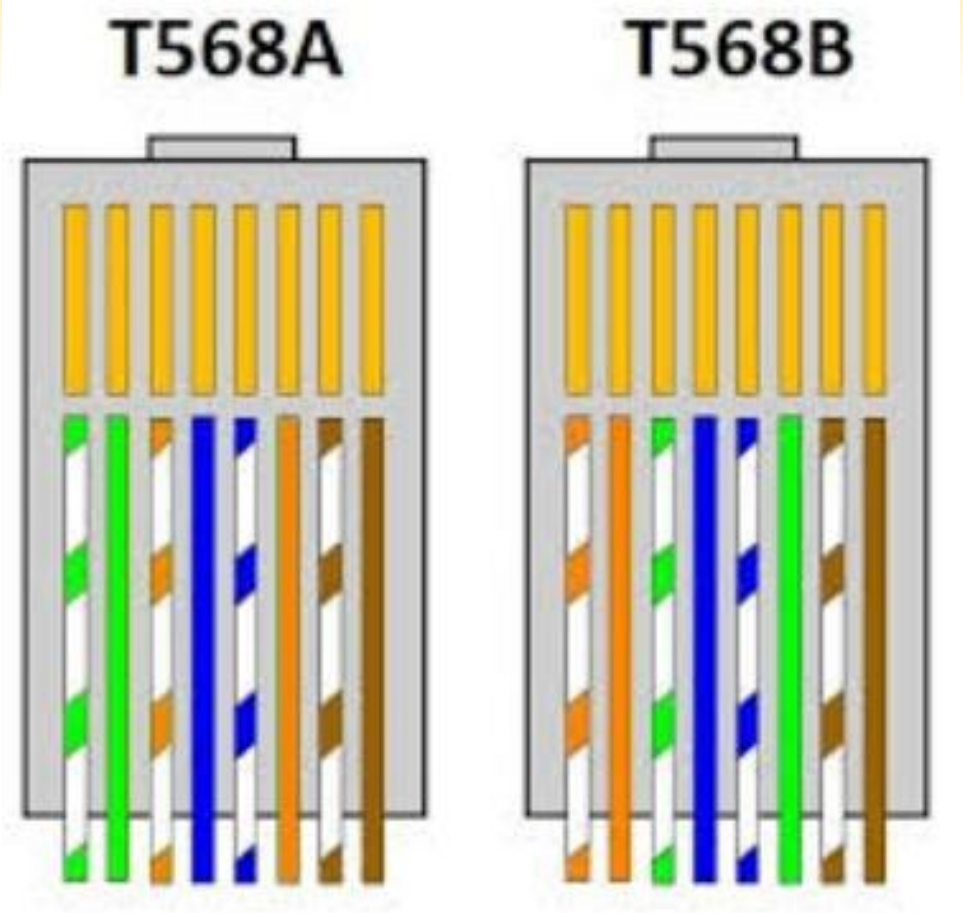
- 4 and 8 conductors are the only options for standard ethernet communication
- When using 4 pins, communication is limited to 100 Mbps some 8 pin connectors are capable of 40 Gbps
- For industrial applications, 100 Mbps is often all that is needed

Some cables exist that are called cross over cables, this is not common now, but can create problems in old networks

- The receiving pair is attached to the sending pair on the other end, this is auto negotiated in most systems now

RJ-45

- RJ-45s are the connectors commonly used to terminate ethernet cables
- They can be wired A standard or B standard
- B standard at both ends is typical
- B to A is what is referred to as a crossover cable

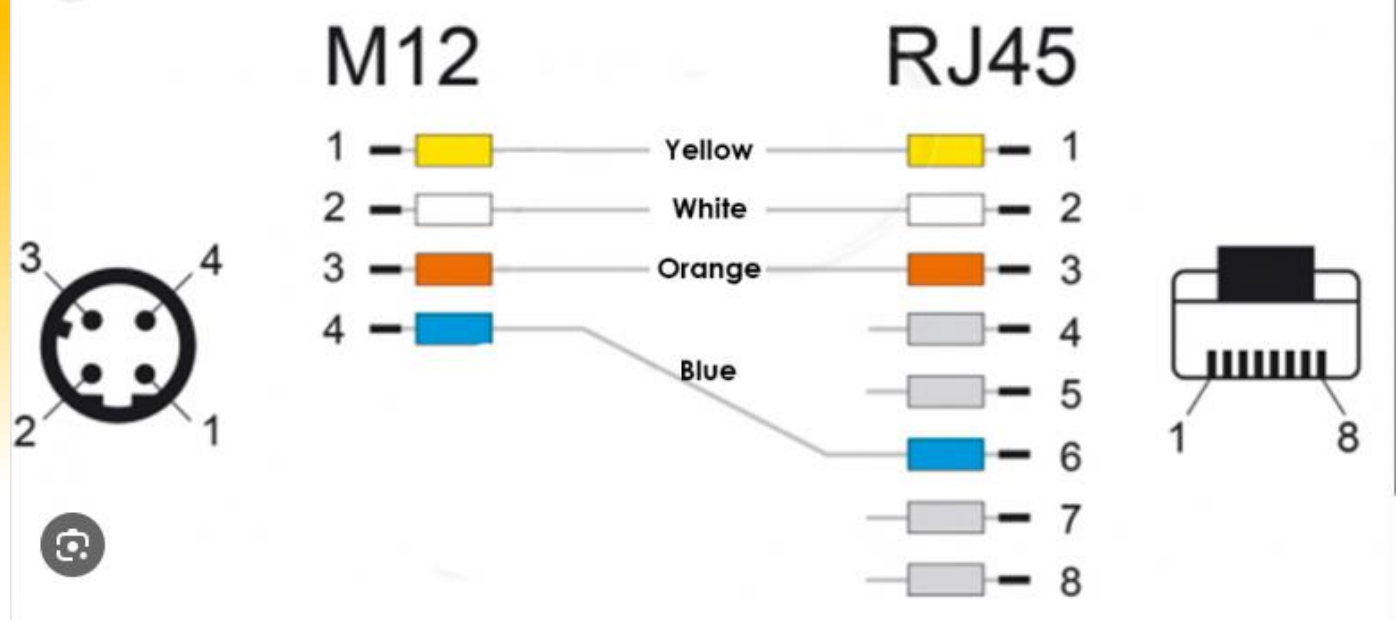


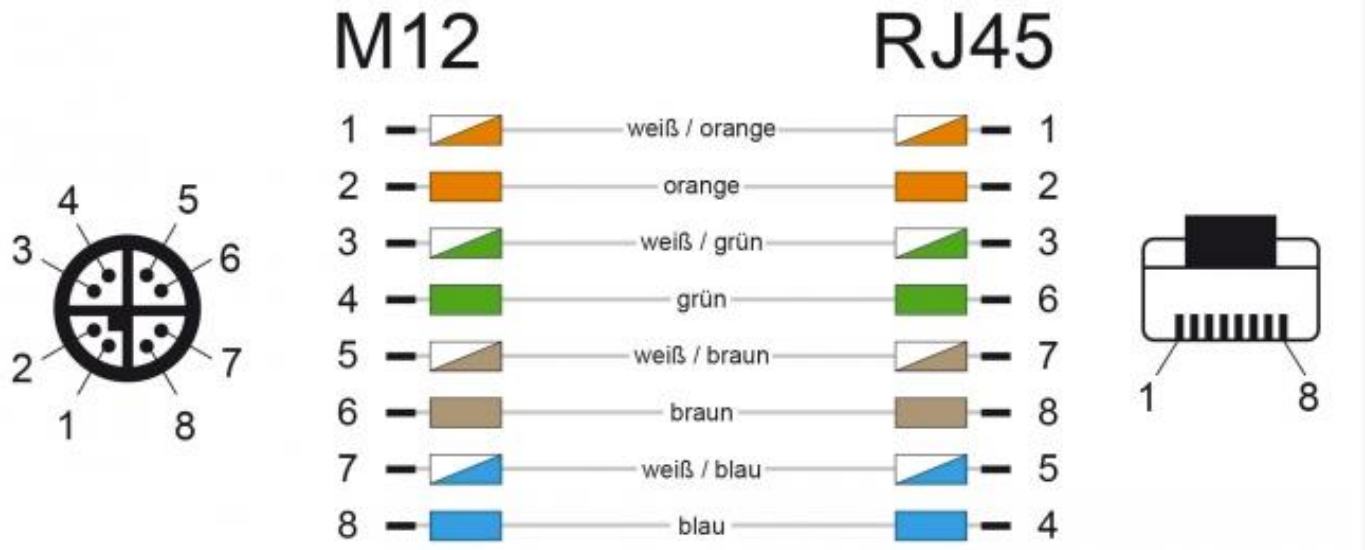
M12

M12 connectors are either

4-pin or 8-pin

They can be wired to another M12 or to an RJ-45 as shown





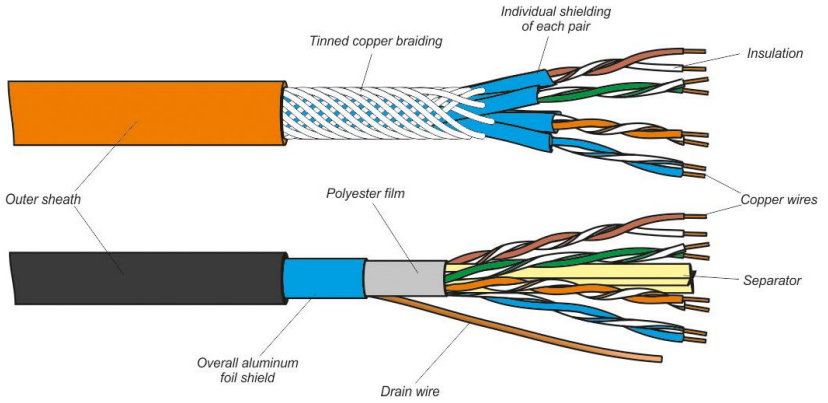
Physical layer

Almost all ethernet cables consist of twisted pairs

This is done to reduce the about of interference that each cable transmits and receives

Cables can sometimes function without a twisted pair, but this will reduce the speed of the cable as well as reduce reliability

Not applicable for fiber optic cables



Network Switch(data Link layer)

This provides a means of connecting devices in such a way that it is not one to one

Network switches will have different speed ratings, check your device speeds and match where necessary

- If all ten of your 100Mbps devices are talking to your PLC, you will need a 1 Gbps switch or have at least 1 Gbps port on your switch to get maximum speeds
- Max speeds are often not required

Switches require a physical cable and port for each item that needs to connect to the device, the more ports the more expensive

Router (network layer)

Routers direct network traffic between different devices

- These connections are typically to network switches or external resources

Routers work to direct traffic, assign IP addresses, and connect a network to the outside world

Often act as a DHCP server in networks

These often perform the same actions as a managed network switch

Wireless Access Point (network layer)

Wireless Access Points provide the ability to connect wirelessly to a network

Access points often have a built in network switch

Many wireless routers can be configured to be a wireless Access point

Combo Units (network layer)

Many devices are a combination of Access Points, Routers, and or Switches

Most Access Points include network ports on the back to act as a switch as well

Many routers are also wireless and enable computers to connect to the external internet network provided by an ISP

IP Address(network layer)

IP address are identifiers used on a network to control what device reads and writes information between devices.

They are 4 numbers separated by “.” and each number is 0-255

IP addresses consist of

- IP Address – Computer identity
- Subnet Mask – limits the IP Addresses the computer can talk to
- Gateway-Provides access to other networks through this address(Optional)
- DNS-Domain Name System is used in internet applications primarly(Optional)

Subnet Mask (network layer)

The subnet mask will look something like the following

- 255.255.255.0

This will mark what sections of the IP address have to match between devices so that they can communicate

For example

- If the subnet mask is 255.255.255.0 and the IP addresses are set to 192.168.125.1 and 192.168.125.2 the two devices can communicate to one another
- Those two devices cannot communicate with the IP address of 192.168.10.1
- If the subnet mask is changed to 255.255.0.0, then they can all three communicate

Static vs DHCP

There are 2 general ways IP addresses are set

Static IP addresses are manually entered and require knowledge of other devices on the network to be able to correctly setup communication

When a devices is set to DHCP, it will receive an IP address from a server on the same network

If a DHCP server is not present on the network, the device will be disable the network or assign itself a dummy address

- The dummy address is often 169.168.xxx.xxx

Static vs DHCP

The IP address can be used as a means of identifying individual devices

- This is often how a system determines what device to talk to, if the IP address changes, the device can no longer be found
- With static IP addresses mistakes can be made, and two devices can be given the same IP Address, this will break communication with both devices
- DHCP can cause IP addresses to change. When this happens, it can make it difficult to establish communication
- DHCP verifies an IP address is open before it assigns it to a device, so duplicate IP address do not occur
- Devices on a network with a DHCP server can still be set as static IP addresses

Static vs DHCP

DHCP is often used on devices that are temporarily on the network

- The computer used to program a robot or on a wireless network

Static should be used on local networks that utilize industrial communications

Static may need to be used if the network you are on does not have a DHCP server on it

- Some robots include a DHCP server, others do not.

TCP(Transport Layer)

TCP stands for Transmission control protocol

Reliable connection- All information sent waits for an acknowledgement that the other end has received the correct information

Slow-This is a slower communication because it waits for a response before it will send the next part of data

This is great for data tracking when no data can be lost and the speed is not too great

UDP (Transport Layer)

UDP stands for User datagram protocol

Unreliable- No verification occurs between the sender and receiver to determine if the message arrived correctly at the other end

- Checks can be added by the programmer to account for this

Fast- Because no response is needed this is much faster.

This is great for real time controls where if a package fails to send, resending it would just put the system further behind. Instead it is best to send the most up to date information

TCP vs. UDP (the two main Transport Layer protocols)

Feature	**TCP** – Transmission Control Protocol	**UDP** – User Datagram Protocol
Connection	Connection-oriented (like a phone call)	Connectionless (like sending a letter)
Reliability	Reliable – guarantees delivery	Unreliable – no delivery guarantee
Order	Packets arrive in the correct order	Packets may arrive out of order
Speed	Slower (due to checks and confirmation)	Faster (no waiting, less overhead)
Use Case	Emails, web pages, file transfers	Video streaming, VoIP, sensor data
Acknowledgments	Yes – confirms receipt of each packet	No – just sends
Error Checking	Stronger (retransmits if corrupted/lost)	Basic (no retransmission)

Glossary of Key Terms

NIC – Network Interface Card: Hardware that connects a device to a network.

CIP – Common Industrial Protocol: Used by EtherNet/IP for data exchange.

GSDML – General Station Description Markup Language: XML-based file describing PROFINET devices.

TCP – Transmission Control Protocol: Reliable, connection-oriented communication.

UDP – User Datagram Protocol: Unreliable but fast, connectionless communication.

Static IP – Manually assigned IP address.

DHCP – Dynamic Host Configuration Protocol: Automatically assigns IP addresses on a network.

Subnet Mask – Defines which IP addresses a device can communicate with directly.

Switch – A device that connects multiple devices on a local network and sends data only to the intended recipient using MAC addresses.

IP Address – A unique number assigned to a device on a network, used to identify it and route data correctly (e.g., 192.168.1.10).

EtherNet/IP – An industrial protocol based on standard Ethernet and TCP/IP, using the Common Industrial Protocol (CIP) for communication between devices like PLCs and robots.

PROFINET – A real-time industrial Ethernet protocol developed by Siemens, used to connect PLCs, drives, and sensors, with support for precise timing and modular configuration via GSDML files.