EtherNet/IP Protocol

Industrial Ethernet protocol for Rockwell and Allen-Bradley systems

OT Security Learning Series

Document 203 | January 2026

Contributors: Matthias Niedermaier

Created with AI assistance

LEARNING RESOURCE

Contents

1 Introduction

Information

EtherNet/IP (Ethernet Industrial Protocol) is one of the most widely deployed industrial Ethernet protocols, particularly dominant in North American manufacturing. It is the primary protocol for Rockwell Automation and Allen-Bradley control systems.

Key characteristics:

- Uses standard Ethernet and TCP/IP infrastructure
- Built on Common Industrial Protocol (CIP)
- Supports both discrete and process control
- Real-time I/O and messaging capabilities
- Managed by ODVA (Open DeviceNet Vendors Association)

2 Protocol Architecture

2.1 Protocol Stack

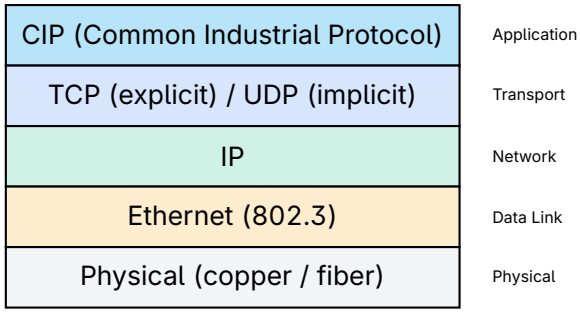

Figure 1: EtherNet/IP Protocol Stack

2.2 Common Industrial Protocol (CIP)

CIP - The Foundation

CIP is an application layer protocol shared by EtherNet/IP, DeviceNet, and ControlNet. It provides:

- Object-oriented device modeling
- Standardized device profiles
- Common services across networks
- Producer/consumer communication model

2.3 Communication Types

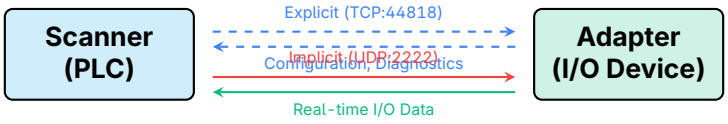

Figure 2: EtherNet/IP Communication Types

- **Explicit Messaging** – TCP-based, connection-oriented, for configuration and diagnostics
- **Implicit Messaging** – UDP-based, for real-time I/O data exchange
- **Unconnected** – Single request/response transactions
- **Connected** – Established sessions for ongoing communication

3 Network Ports and Services

Port	Protocol	Purpose
TCP/44818	CIP Explicit	Configuration, diagnostics
UDP/44818	CIP Explicit	Unconnected messages
UDP/2222	CIP Implicit	Real-time I/O data
TCP/80	HTTP	Web interface (if enabled)
UDP/67-68	DHCP/BootP	Address assignment

Table 1: EtherNet/IP Network Ports

4 CIP Objects and Services

4.1 Object Model

EtherNet/IP devices are modeled as collections of objects:

- **Identity Object (0x01)** – Device information, serial number, vendor
- **Message Router (0x02)** – Routes requests to appropriate objects
- **Assembly Object (0x04)** – Groups I/O data for transmission
- **Connection Manager (0x06)** – Manages connections
- **TCP/IP Interface (0xF5)** – Network configuration
- **Ethernet Link (0xF6)** – Ethernet statistics

Code	Service	Purpose
0x01	Get_Attribute_All	Read all object attributes
0x0E	Get_Attribute_Single	Read single attribute
0x10	Set_Attribute_Single	Write single attribute
0x4C	Forward_Open	Establish connection
0x4E	Forward_Close	Terminate connection
0x52	Unconnected_Send	Send without connection

Table 2: Common CIP Services

4.2 Common Services

5 Security Vulnerabilities

Critical

EtherNet/IP was designed for reliability and interoperability, not security. Like most industrial protocols, it lacks built-in authentication and encryption.

5.1 Protocol Weaknesses

- **No authentication** – Any device can send commands
- **No encryption** – All traffic is plaintext
- **No integrity protection** – Messages can be modified
- **Predictable ports** – Easy to identify on network
- **Information disclosure** – Identity object reveals device details

5.2 Known Attack Vectors

- **Device enumeration** – Query Identity objects to map network
- **Unauthorized configuration** – Change device settings via Set_Attribute
- **I/O manipulation** – Inject or modify implicit messages
- **Connection hijacking** – Take over established connections
- **Denial of service** – Flood with connection requests
- **Firmware manipulation** – Upload malicious firmware

6 Security Mitigations

6.1 Network-Level Controls

Key Point

Since EtherNet/IP lacks native security, protection must come from network architecture and external controls.

- **Network segmentation** – Isolate EtherNet/IP traffic in dedicated VLANs
- **Firewall rules** – Restrict access to ports 44818 and 2222
- **Industrial firewalls** – Deep packet inspection for CIP
- **Access control lists** – Limit which devices can communicate

6.2 CIP Security (Recent Addition)

ODVA has developed CIP Security extensions:

- TLS/DTLS for encrypted communications
- X.509 certificates for device authentication
- Integrity protection for messages
- Requires newer devices with CIP Security support

Warning

CIP Security adoption is still limited. Most installed devices do not support it, requiring network-based protection.

6.3 Monitoring and Detection

- Monitor for unauthorized CIP service requests
- Alert on Identity object queries (reconnaissance)
- Detect configuration changes via Set_Attribute services
- Baseline normal I/O patterns, alert on anomalies
- Watch for connections from unauthorized IP addresses

7 Common Implementations

- **Rockwell/Allen-Bradley** – ControlLogix, CompactLogix PLCs
- **Drives** – PowerFlex variable frequency drives
- **I/O** – POINT I/O, FLEX I/O modules
- **HMI** – PanelView terminals

- **Third-party** – Many vendors support EtherNet/IP

8 Summary

Key Takeaways

- **Dominant protocol** – Primary for Rockwell/Allen-Bradley systems
- **CIP-based** – Shares application layer with DeviceNet, ControlNet
- **Standard Ethernet** – Uses TCP/UDP on ports 44818, 2222
- **No native security** – Authentication and encryption absent
- **CIP Security** – New extension, limited adoption
- **Network protection** – Segmentation and firewalls essential

9 Further Reading

Standards

- **ODVA – EtherNet/IP Specification**
  https://www.odva.org/
- **IEC 61158** – Industrial communication networks
  https://webstore.iec.ch/

Resources

- **CISA – ICS Advisories**
  https://www.cisa.gov/topics/industrial-control-systems
- **Rockwell Automation Security**
  https://www.rockwellautomation.com/en-us/capabilities/industrial-cybersecurity.html

Part of the OT Security Learning Series