

## EtherNet/IP

EtherNet/Industrial Protocol (EtherNet/IP) a member of the Common Industrial Protocol (CIP) provides the network tools to deploy standard Ethernet technology to enable industrial automation applications and enterprise connectivity for data and control. This protocol runs over TCP/IP or UDP/IP. TCP/IP uses the reserved port **0xAF12 (44818)** for transmitting explicit messages while UDP/IP uses the reserved port **0x08AE (2222)** for transmitting I/O messages. A typical Ethernet frame with the encapsulated EtherNet/IP data and the encapsulated packet format are shown in Figures 16 and 17, respectively (Schiffer, 2016).

Ethernet Header	IP Header	TCP or UDP Header	EtherNet/IP Encapsulation Header	EtherNet/IP Encapsulation Data	Ethernet Trailer
-----------------	-----------	-------------------	----------------------------------	--------------------------------	------------------

Figure 16. Ethernet Frame with Encapsulated EtherNet/IP

ENCAPSULATION HEADER						ENCAPSULATION DATA
Cmd 2 octets	Len 2 octets	Session Handle 4 octets	Status 4 octets	Sender Context 8 octets	Options 4 octets	Command Specific Data 0-65511 octets

Figure 17. Encapsulation Packet Format

The two-octet command (Cmd) field represents various types of commands such as broadcast, session opening and closing, and receiving and sending data for connected and unconnected messaging (Francia & Francia, 2013).

```

> Frame 2: 138 bytes on wire (1104 bits), 138 bytes captured (1104 bits) on interface 0
> Ethernet II, Src: Rockwell_96:63:b9 (08:00:bc:b5:63:b9), Dst: Rockwell_64:8c:bd (08:00:bc:c4:0c:bd)
> Internet Protocol Version 4, Src: 10.1.1.17, Dst: 10.1.1.10
> User Datagram Protocol, Src Port: 2222 (2222), Dst Port: 2222 (2222)
  Source Port: 2222
  Destination Port: 2222
  Length: 104
  Checksum: 0xb496 [validation disabled]
  [Stream index: 1]
  EtherNet/IP (Industrial Protocol)
    Item Count: 2
    > Type ID: Sequenced Address Item (0x0002)
    > Type ID: Connected Data Item (0x0001)

```

Figure 18. Packet Details of Ethernet/IP over UDP