There and Back Again: Detecting OT Devices Across Protocol Gateways

ROB KING,
Director of Applied Research, runZero

runZero

Part I

How did we get here?

OT, ICS, and SCADA oh my!

- ***Operational technology*** - an umbrella term describing technology that affects or monitors things in the real world…Includes things like ***Programmable Logic Controllers*** (PLCs), ***Computer Numerical Control*** (CNC) systems, etc.
- ***Industrial control systems (ICS)*** - systems that actual do the controlling of the hardware and sensors
- ***Supervisory Control and Data Acquisition (SCADA)*** - computers, networks, user interfaces, and other high-tech things to control machines and processes.

Mission Control

Image credit: Steag

Ground Truth

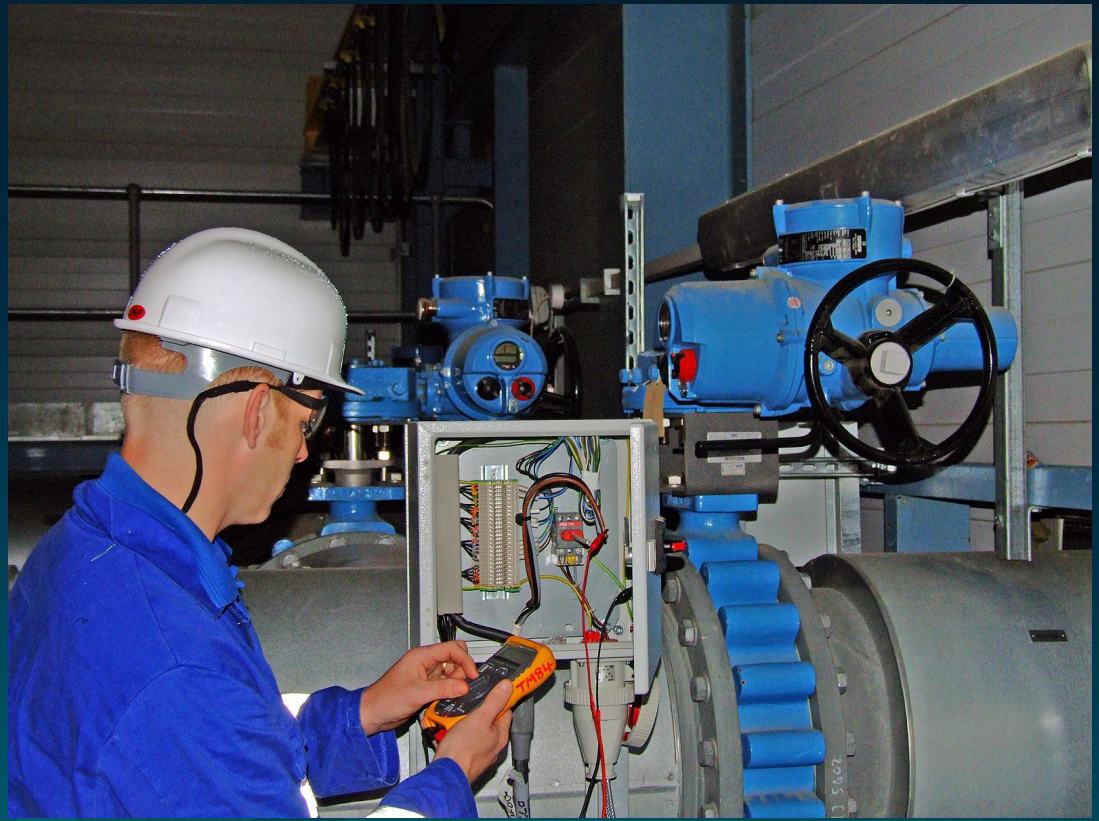


Image credit Wikimedia Commons

Industrial Control Technology

Image credit Wikimedia Commons

Programmable Logic Controllers

Image credit Wikimedia Commons

Backplanes, Modules, and Protocol Adaptation

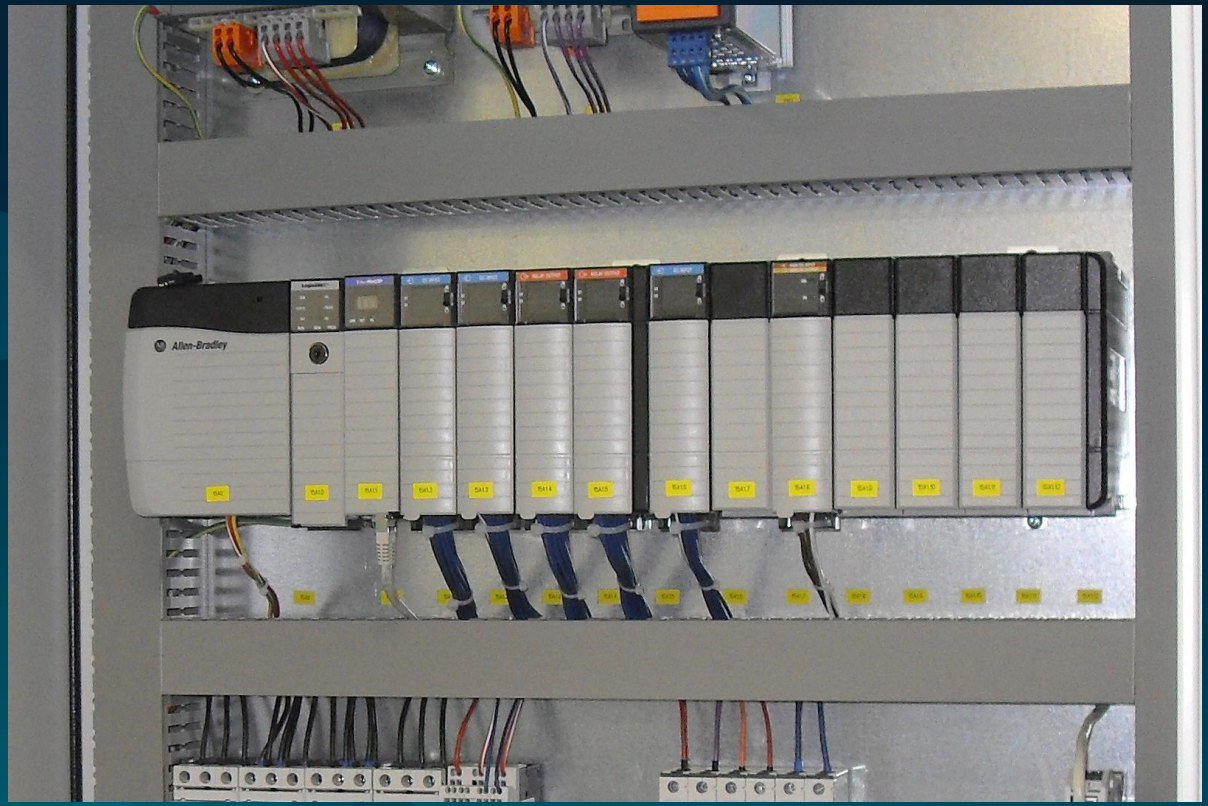


Image credit Wikimedia Commons

Part II

Convergence!

Industrial Ethernet

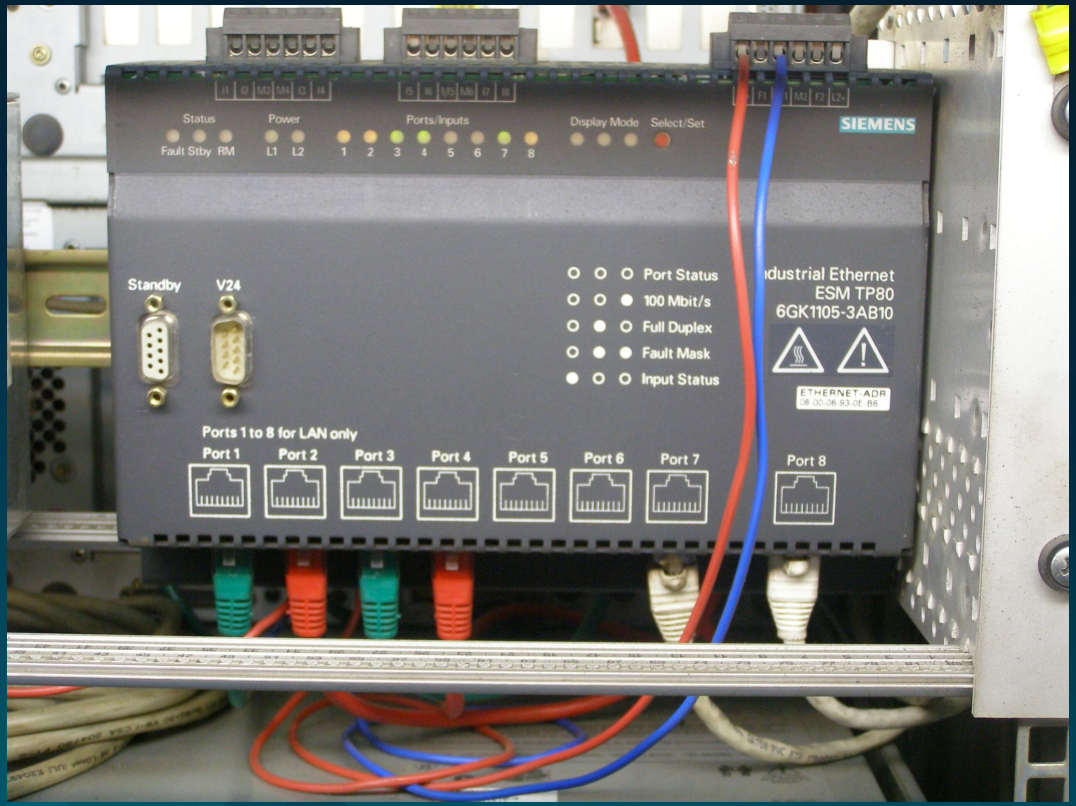
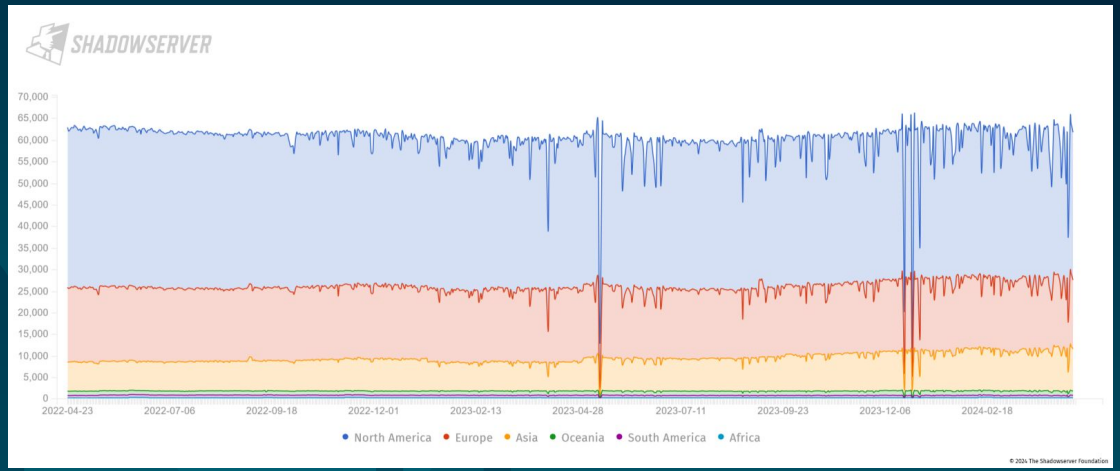


Image credit Wikimedia Commons

IT and OT are Converging

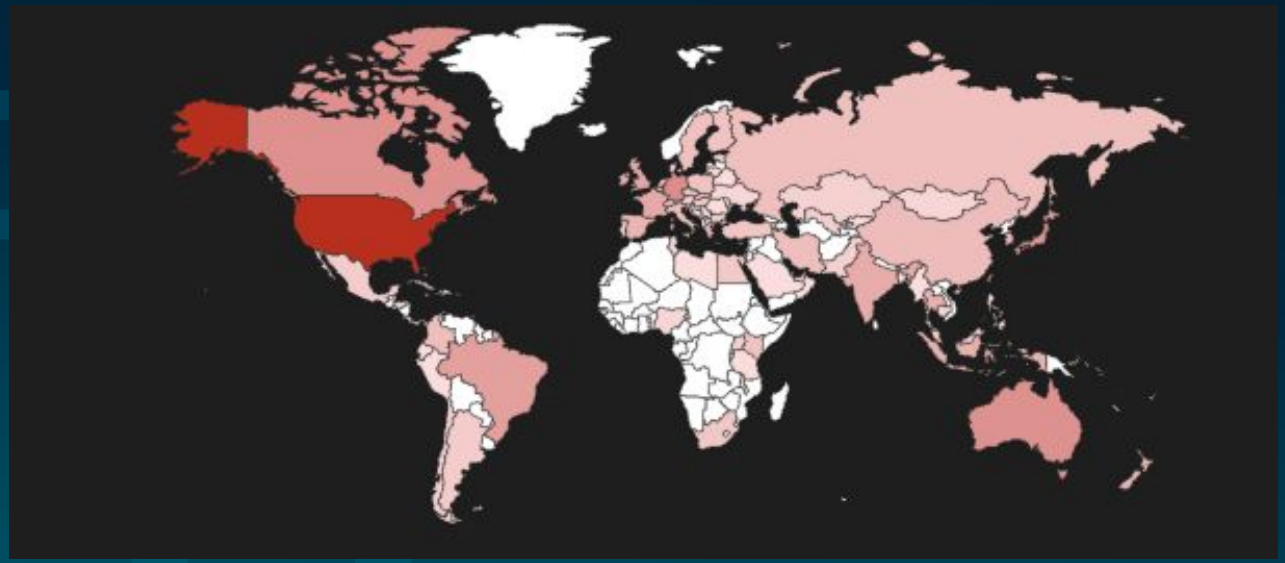
"IT/OT convergence will be the end state"

- CISOs are increasingly taking responsibility for OT
- OT continues to be internet-exposed (7%)



https://isc.sans.edu/diary/It+appears+that+the+number+of+industrial+devices+accessible+from+the+internet+has+risen+by+30+thousand+over+the+past+three+years/30860

Automatic Tank Gauges – Worldwide Exposure



Up	Type	Hardware	Outlier	Attack surfaces
●	PLC	Siemens LOGO! PLC	1	External
●	Ethernet Gateway	Wiesemann & Theis Com-Server Highs...	2	External
●	Data Logger	Schneider Electric ComX	1	External
●	PLC	Allen-Bradley 1766-L32BXBA	2	External
●	Ethernet Gateway	Schneider Electric PowerLogic EGX1...	1	External
●	Power Device	SMA Solar Technology AG Sunny WebB...	1	External
●	PLC	Rockwell Automation PLC	1	External

Part III

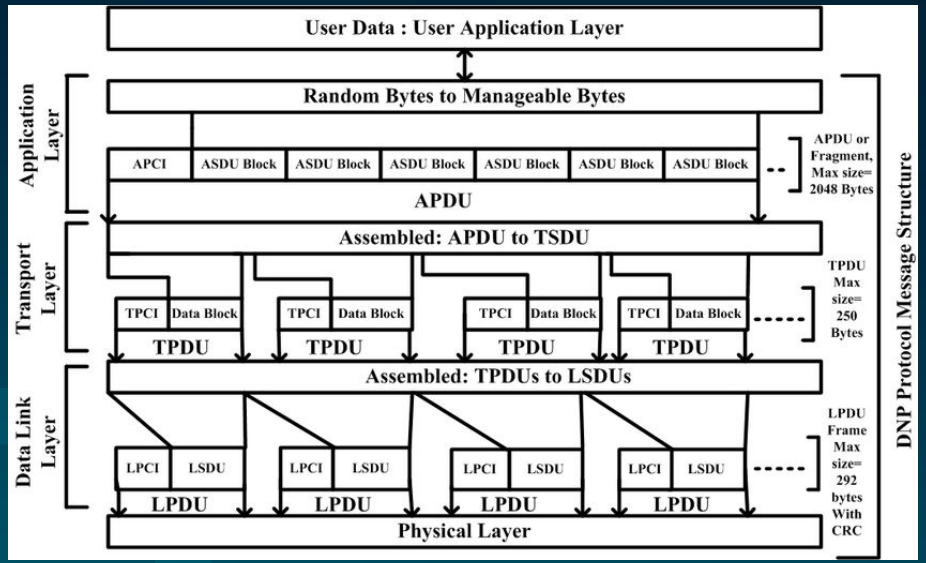
Discovery!

Discovery - Modbus Style

modbus.modelName	PX2-2146R
modbus.productCode	iPDU
modbus.productName	iPDU
modbus.revision	3.0.2.5-41550
modbus.vendor	Raritan
modbus.vendorURL	http://www.raritan.com
protocol	modbus

Distributed Network Protocol 3 (DNP3)

- Includes its own network and transport layers to be medium-agnostic
- Has its own complex checksumming/validation mechanisms



Shahzad, Aamir & Lee, Malrey & Kim, Hyung & Woo, Seon-mi & Xiong, Naixue. (2015). New Security Development and Trends to Secure the SCADA Sensors Automated Transmission during Critical Sessions. Symmetry. 7. 1945–1980. 10.3390/sym7041945.

Distributed Network Protocol 3 (DNP3)

dnp3.destination	0x0001
dnp3.deviceID	ID_CODE
dnp3.deviceName	RZHQ-OT-914
dnp3.hardwareVersion	DNP3 Outstation
dnp3.location	India
dnp3.manufacturer	FreyrSCADA Embedded Solution
dnp3.model	DNP3 Protocol Library
dnp3.serialNumber	21.05.025
dnp3.softwareVersion	21.05.026
dnp3.source	0x0002

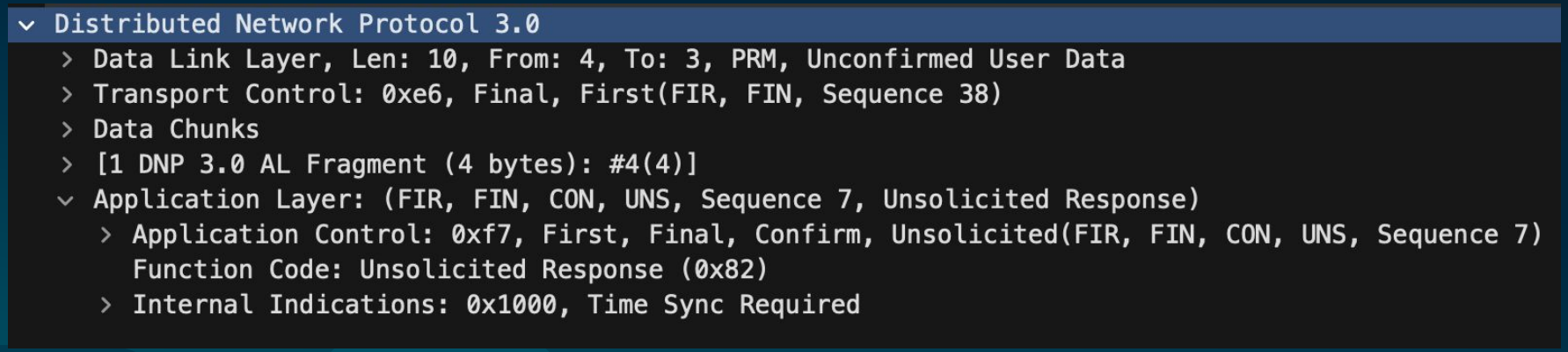
DNP3 Dual-Layer Addressing

- 16-bit address, with some reserved, leaving 65531 possible addresses.
- A designated *primary* device and multiple *secondary devices*.
- Secondary devices only talk to their preconfigured primary.
- You might have to guess the primary *and* secondary addresses!

Address Guessing

- Addresses range from 0 to 65k
- *Usually* addresses are assigned sequentially starting at 1
- *Usually* addresses are in the first part of the address space, say no more than 512
- ...this still means potentially guessing 262,144 address pairs 😐

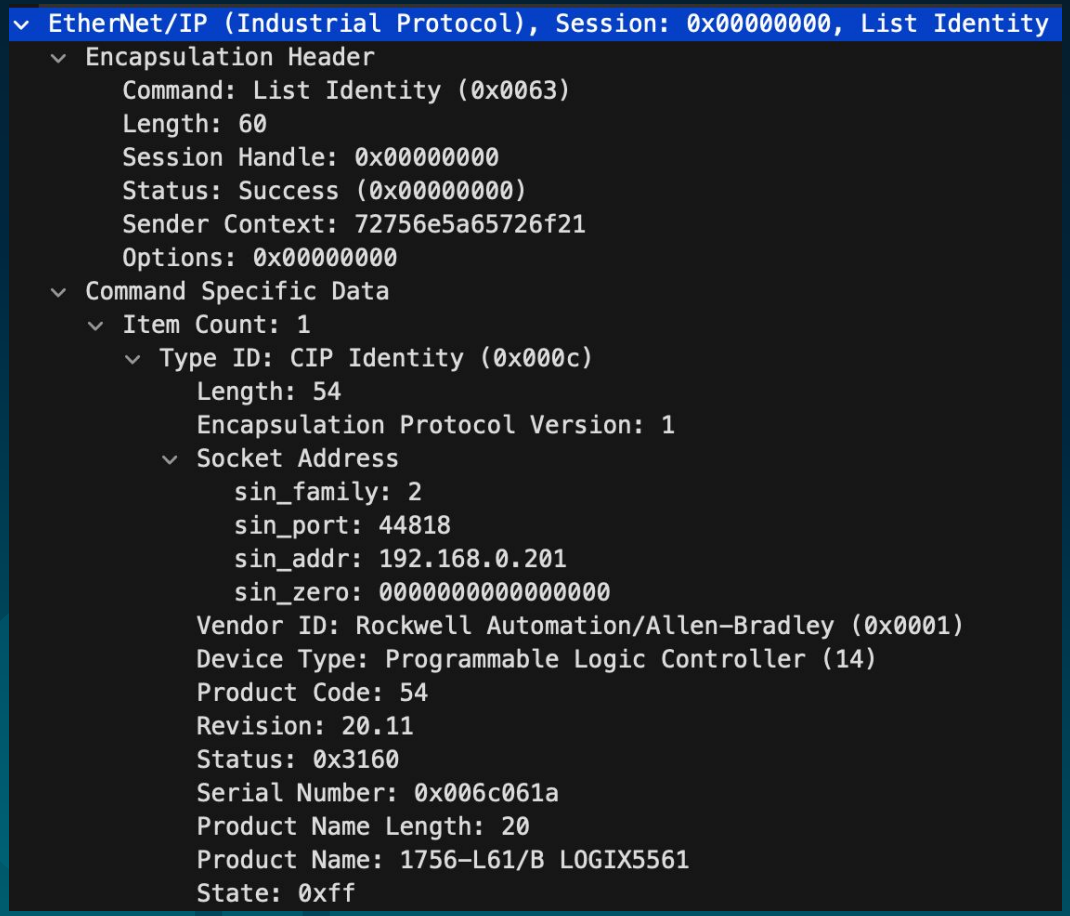
The Good News: Banner Sniffing!



EtherNet/IP and CIP

Image credit ODVA

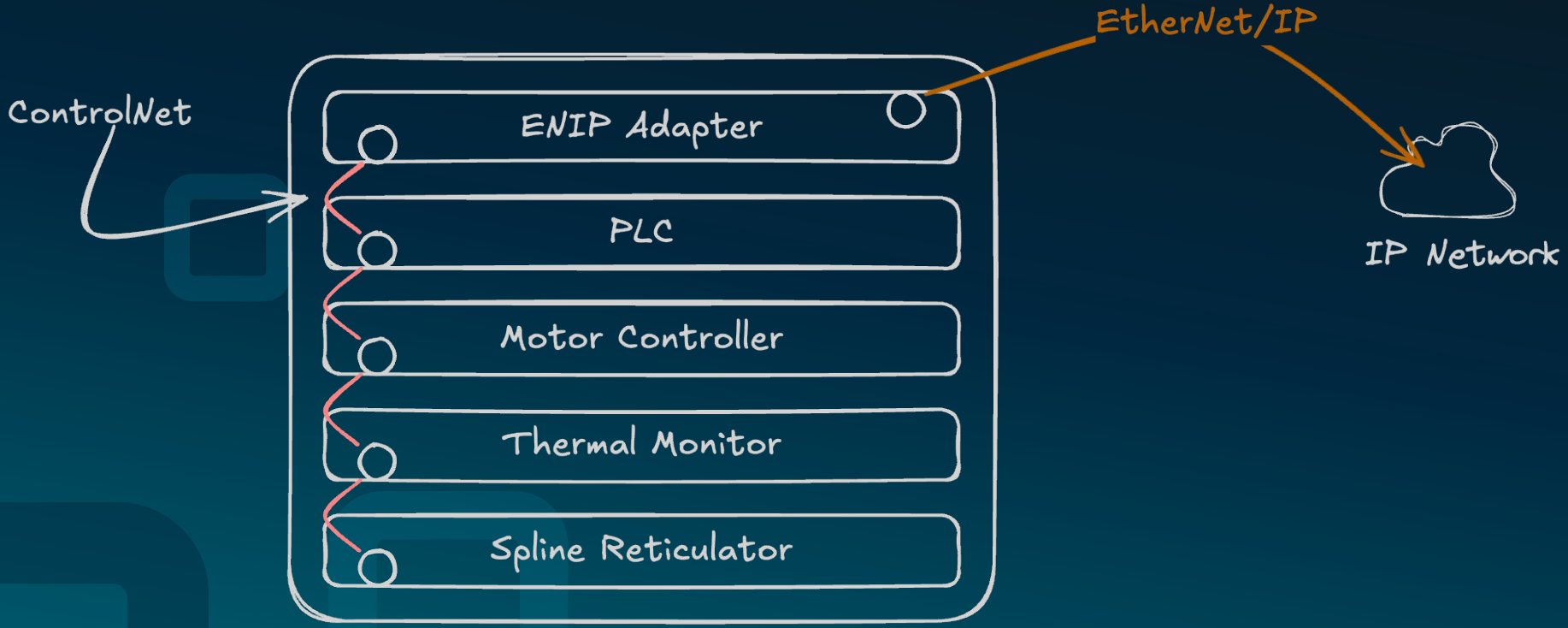
EthetNet/IP Connected Device Discovery



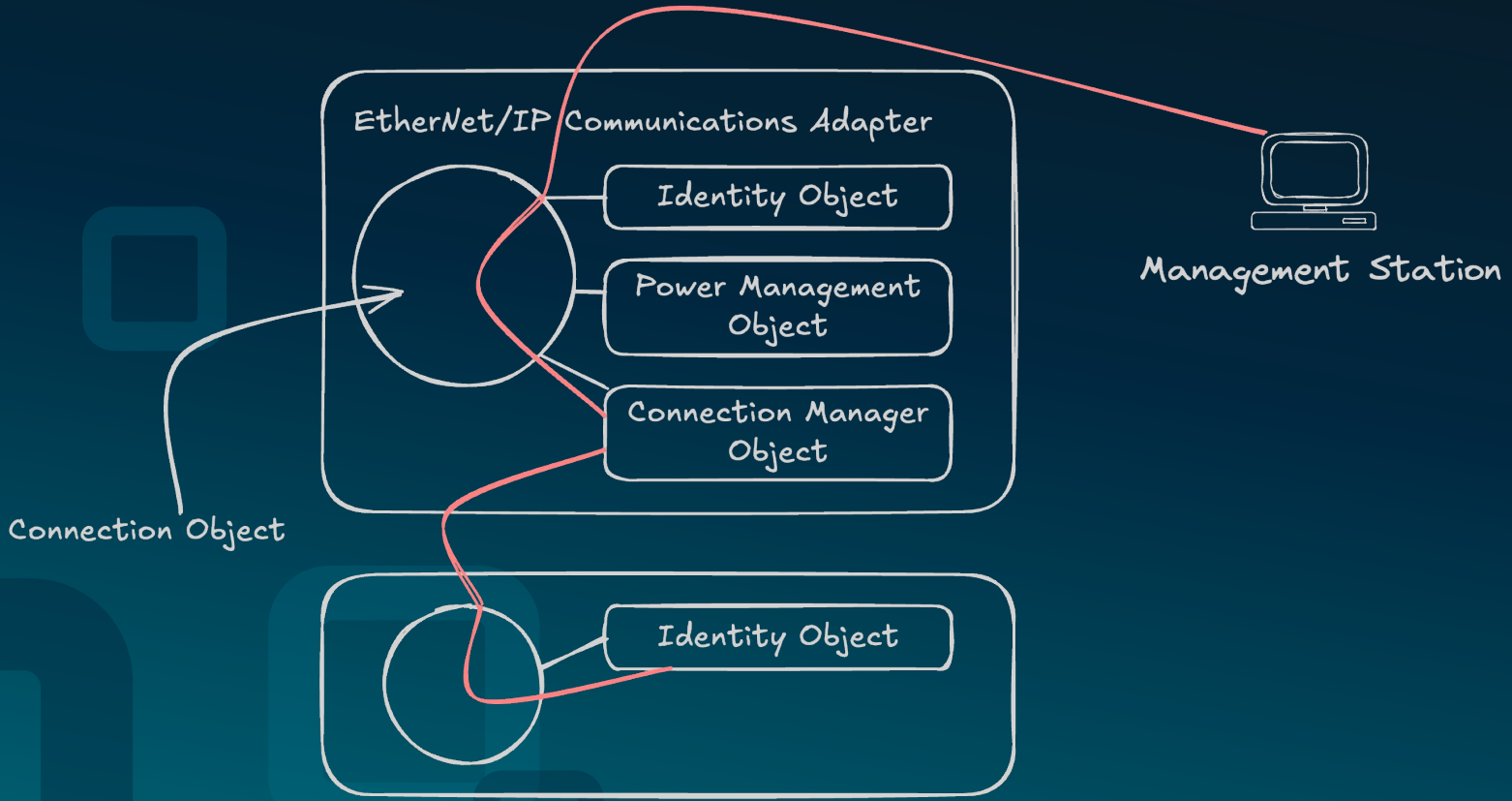
EtherNet/IP List Identity

192.168.40.9 - 44818/udp	
ethernetip.address	192.168.40.9
ethernetip.deviceType	Generic Device (keyable)
ethernetip.port	44818
ethernetip.product	IO-Link master EIP 8P IP20
ethernetip.productID	1030
ethernetip.revision	1.4
ethernetip.serialNumber	2516058524
ethernetip.vendor	ifm efector, inc.
fp.hw.device	Generic Device (keyable)
fp.hw.match	runzero-ethernetip
fp.hw.product	IO-Link master EIP 8P IP20
fp.hw.serialNumber	2516058524
fp.hw.vendor	ifm efector, inc.
fp.hw.version	1.4
protocol	ethernetip
ts	Oct 29 2024 4:48PM [UTC-5] (Tue)

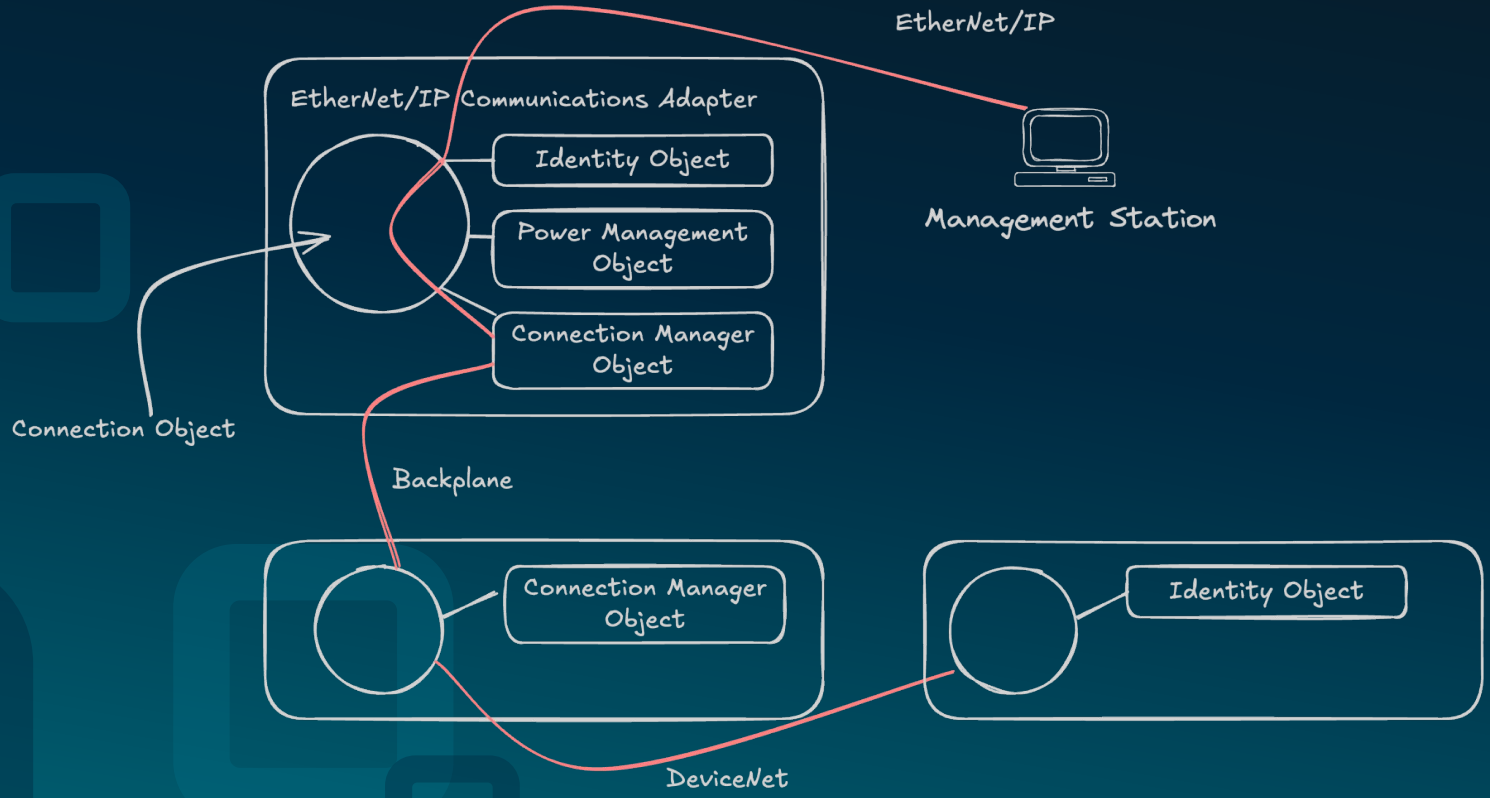
Example Rack



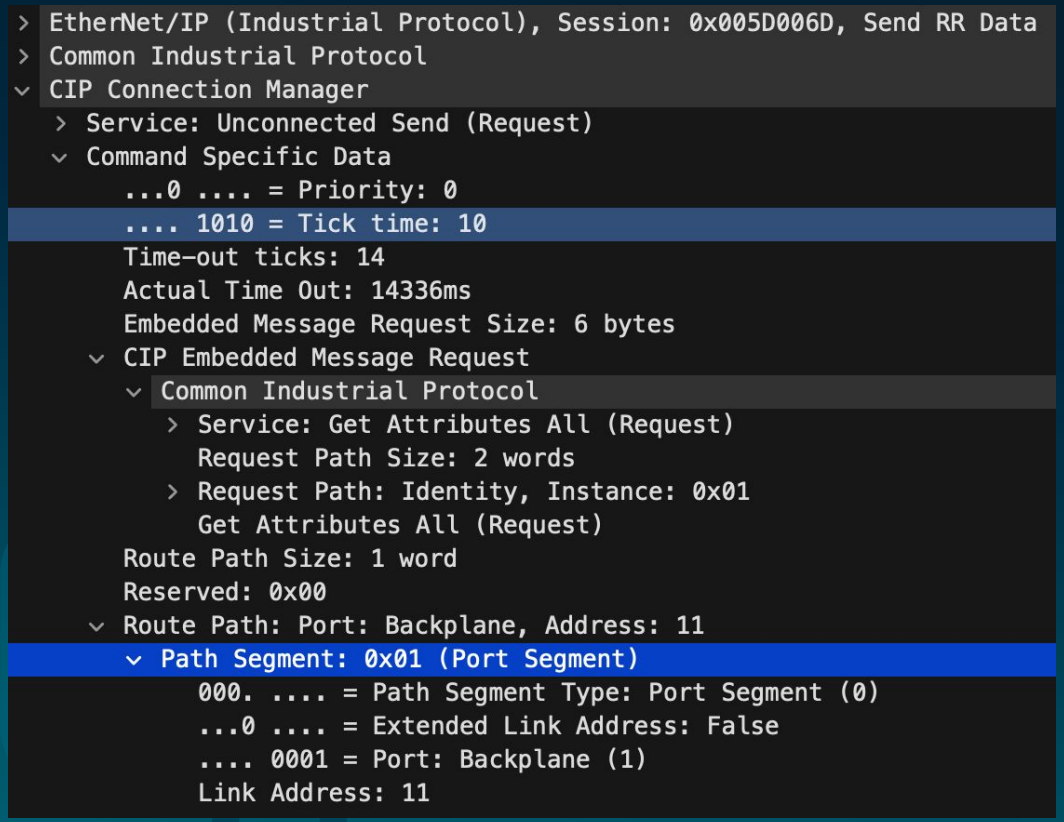
CIP Forwarded Messages



CIP Forwarded Messages



Source Routing and Path Construction



Walking the Backplane


```
[
  "1": {
    "identification": {
      "vendor": "Rockwell Automation/Allen-Bradley",
      "type": "General Purpose Discrete I/O",
      "product": 1140,
      "revision": [
        30,
        14
      ],
      "status": 97,
      "serialNumber": 0
    },
    "name": "24VDC 16PT INPUT & 16PT OUTPUT",
    "slotNumber": 1
  },
  "2": {
    "identification": {
      "vendor": "Rockwell Automation/Allen-Bradley",
      "type": "Unknown (115)",
      "product": 110,
      "revision": [
        4,
        3
      ],
      "status": 97,
      "serialNumber": 0
    },
    "name": "1734-232ASC/C RS-232 ASCII",
    "slotNumber": 2
  },
```

Thank you!

ROB KING
rob@runzero.com

runZero