Stories around ModBus

Why Modbus Is Even Worse than SNMP

Richard Hartmann,
RichiH@{freenode,OFTC,IRCnet},
richih@{debian,fosdem,richih}.org,
@TwitchiH

2020-02-02

Show of hands

- Who is running directly on or dealing with hardware?
- Who has heard of SNMP?
- Who has heard of Modbus?

Show of hands

- Who likes SNMP?

Modbus

Modbus is worse

Relation

- SNMPv1: 1988
- Modbus release: 1979 (!)

SNMP

Without SNMP, the Internet would break down within hours

Modbus

Without Modbus, society would break down within hours

Modbus

- Without Modbus, you would have no power
- Without Modbus, you would have no water
- Without Modbus, you would have no ports
- Without Modbus, you would have no medicine
- Without Modbus, you would have no processed food
- Without Modbus, you would have no clothes

Modbus

So, of course, Modbus has zero security built in

Flavours of Modbus

- Modbus RTU: Serial bus with binary data, most common. Hard real-time
- Modbus ASCII: Serial bus with ASCII. Just don't. Hard real-time
- Modbus TCP: Binary over TCP/IP. Not even soft real-time ensured
- Modbus over TCP: Slight differences to Modbus TCP, not commonly used
- Modbus UDP: Not commonly used
- Modbus Plus: Not commonly used
- Pemex Modbus: Not commonly used
- Enron Modbus: Not commonly used

Which to use?

You want to use Modbus TCP

What if I can't?

If you have hard real-time requirements, you need to use Modbus RTU

Create local islands of Modbus RTU where you need them

Bridging into Modbus TCP is common and you can buy ”master” units off the shelf

Master & slave

References to master & slave in modbus_exporter have been removed even though they are still part of the official standard

Addressing scheme

- 00001-09999: Read-Write, Discrete Output Coils
- 10001-19999: Read-Only, Discrete Input Contacts
- 30001-39999: Read-Only, Analog Input Registers
- 40001-49999: Read-Write, Analog Output Holding Registers

Addressing scheme

- 00001-19999: Bit-wise addressing into a 2-byte block. So you need sub-addressing
- 30001-49999: 2-byte block. Unless you need 16 bits, you need suba-ddressing or combination
- You always get 2-byte blocks back so you need to do subadressing

Wat?

- No other data types defined
- Four ways to clobber a Float32 together:
  - Big endian (1 2 3 4)
  - Little endian (4 3 2 1)
  - Mixed endian (2 1 4 3)
  - YOLO endian (3 4 1 2)

Waat?

In Nomver 2019, I stated that at least I had not seen YOLO endian yet

Waaat?

I got email stating people had seen YOLO endian in the wild

Waaaat?

- Yes, ”Input” and ”Output” are from the perspective of the sender, not the actual device
- Yes, 50000+ is skipped in that spec; but you can use it
- Yes, the binary 0x0000 maps to decimal 00001
- No, there’s no rule if you start counting with 0 or 1, it’s free for all
- Addresses up to 65536, or 105536, are the ”extended range”. Not a problem as everyone is doing what they want, anyway.

Waaaaat?

This standard is enforced by devices simply stopping to work

Easy, reliable, horrible

Reminder

- Without Modbus, you would have no power
- Without Modbus, you would have no water
- Without Modbus, you would have no ports
- Without Modbus, you would have no medicine
- Without Modbus, you would have no processed food
- Without Modbus, you would have no clothes

Maps

Modbus maps are roughly what SNMP MIBs are

Maps

Only you can't unit test them and your production might stop working if you do something wrong

Maps

I have seen maps which are scans of photocopied paper

How do you work with that?

Industry standard is to have a hex viewer, a map, an Excel sheet, and strong nerves

What do I use this in datacenters for?

Everything

What do I use this in datacenters for?

Everything, except the cameras

What do I use this in datacenters for?

Access control, intruder detection, glass breakage, fire detection, fire suppression, cooling set points, groundwater pump, groundwater filters, ion exchange pump, reverse osmosis system, water leakage, fan speed, doors opening and closing, fence gates, lighting, MCCB & status, diesel engine status, diesel fuel tank levels, battery runtime, battery health, elevator access, elevator position, movement in secure areas, potential to ground, lightning strikes, microsecond events on power distribution, medium voltage, transformer load, transformer heat, floodlights, pressure release valves, airflow in office, temperature in office, temperature/humidity/pressure in data halls, smoke extraction fans, emergency exit status, LASER fence scanners, conductivity of cooling water

Bullet-proof glass being shot at

What do I use this in datacenters for?

Not a complete list

Why?

Why am I doing this?

Why?

I like pain

Why?

Modbus is the one standard supported by ALL industrial equipment

Why?

Modbus is horrible, but it's also extremely reliable within the constraints of its use

Why?

Because countless people would die if it wasn't

How?

`https://github.com/RichiH/modbus_exporter`

Max Inden did tons of work during a one-month networking & Modbus stint at SpaceNet

Needs more love, PRs and docs welcome

Caveats

If you have Modbus RTU, use a PLC as a gateway to expose Modbus TCP

Caveats

Reading out Modbus registers takes several seconds

Future work

Currently having my PLCs reprogrammed to expose seconds spent and might adapt exporter to calculate correct time

Future work

There is a semi-standard way to write a Modbus map and I want to have a generator like snmp_exporter's

Reminder

- Without Modbus, you would have no power
- Without Modbus, you would have no water
- Without Modbus, you would have no ports
- Without Modbus, you would have no medicine
- Without Modbus, you would have no processed food
- Without Modbus, you would have no clothes

Modbus

Without Modbus, society would break down within hours

Thanks!

Thanks for listening!

Questions?

Twitter: @TwitchiH