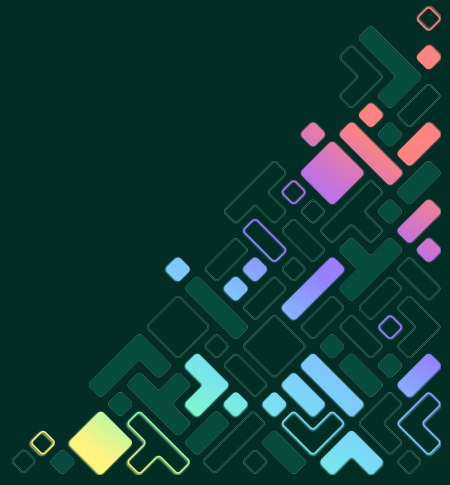
Zephyr® Project
Developer Summit

Connecting Zephyr Devices at Scale Using Open Source Solutions

Julien Vermillard, *Tado*



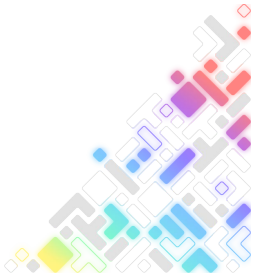
Agenda

Overview of CoAP the Constrained Application Protocol

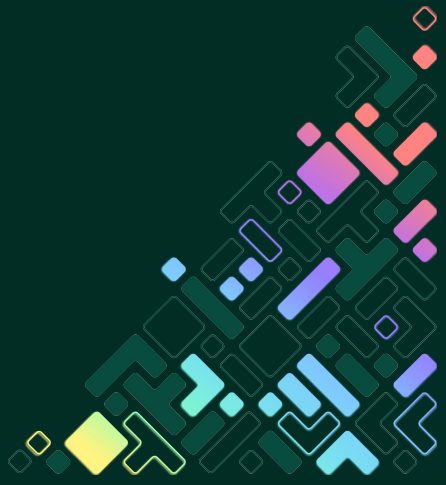
- CoAP in a nutshell
- Large payload transfer
- Security of CoAP
- NAT 😱
- Lightweight M2M

CoAP at scale, feedback from the trenches

- To use CoAP or LWM2M-or-not?
- System architecture and Open Source bricks

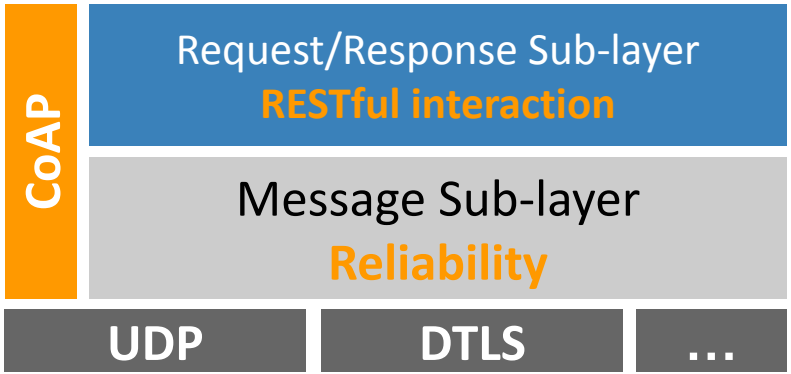


CoAP in a nutshell



CoAP, a protocol from the Web of sensors, Smart dust, 6LOWPAN era

Target: Smart energy and home automation using constrained networks and nodes



GET, **POST**, **PUT**, **DELETE**
URIs and Internet Media Types

Deduplication
Optional retransmissions
(Confirmables “CON”)

Not a generalist protocol, but flexible enough to adapt to every monstrosity :)

A very simple encoding Binary & compact, but complex semantics!

Mix HTTP like semantics with reliability and streaming

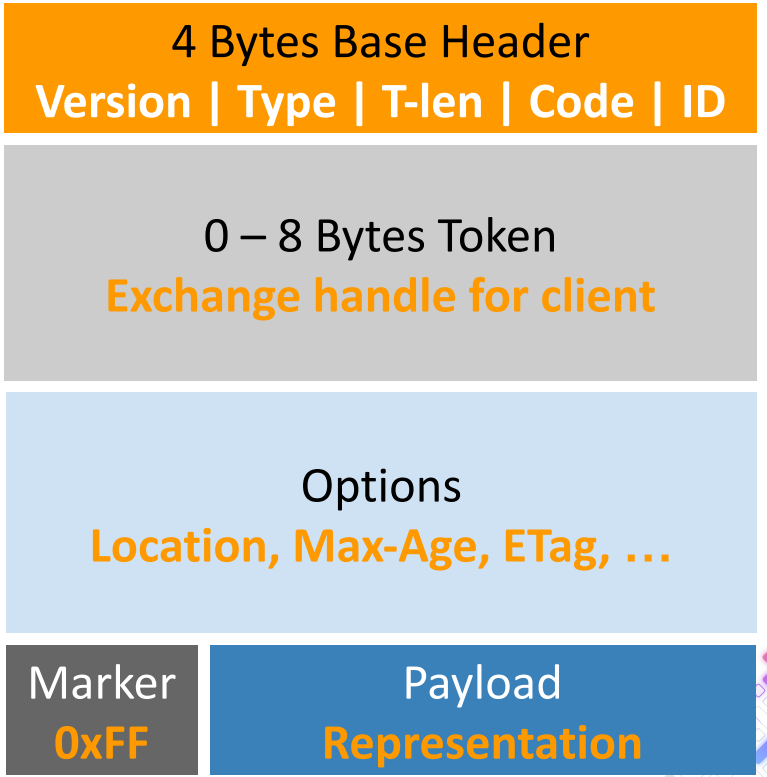
Type:

Confirmable, Non-confirmable, Acknowledgement, Reset

Code:

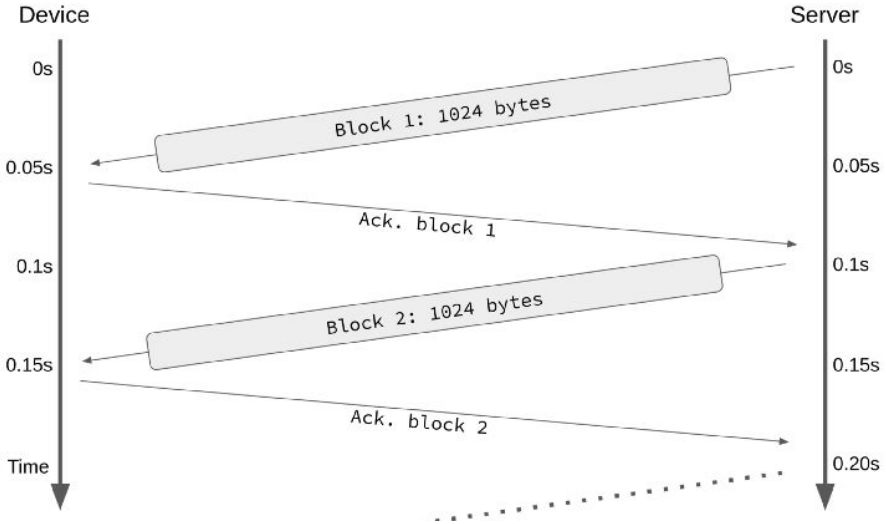
GET, POST, PUT, DELETE

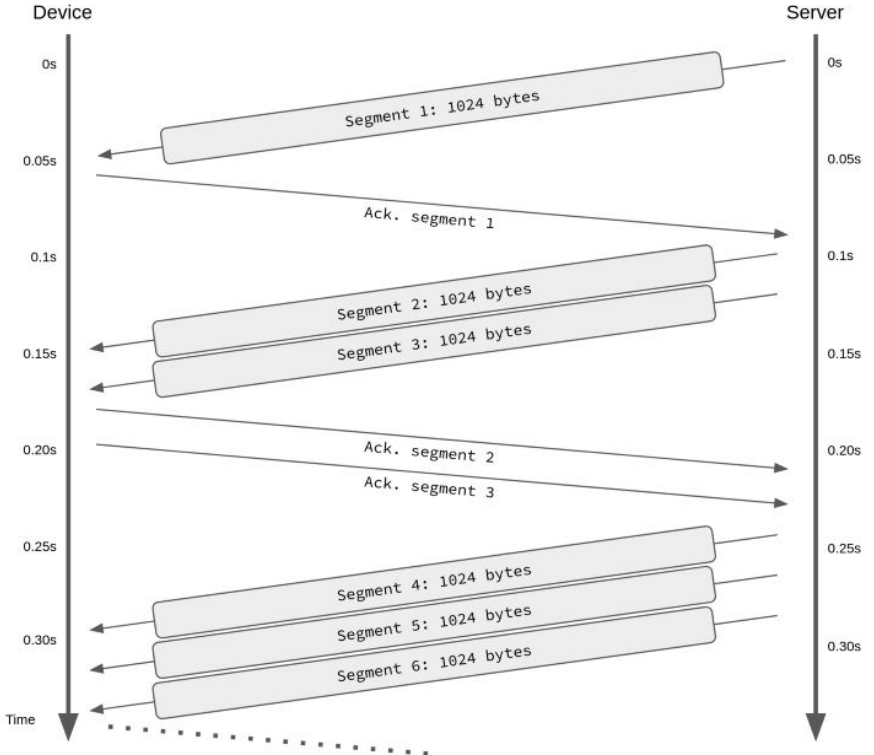
2.xx, 3.xx, 4.xx, 5.xx



Large payload with CoAP (blockwise transfer)

CoAP blockwise vs TCP





Security of CoAP: DTLS

Pre-Shared-Key: 830 bytes

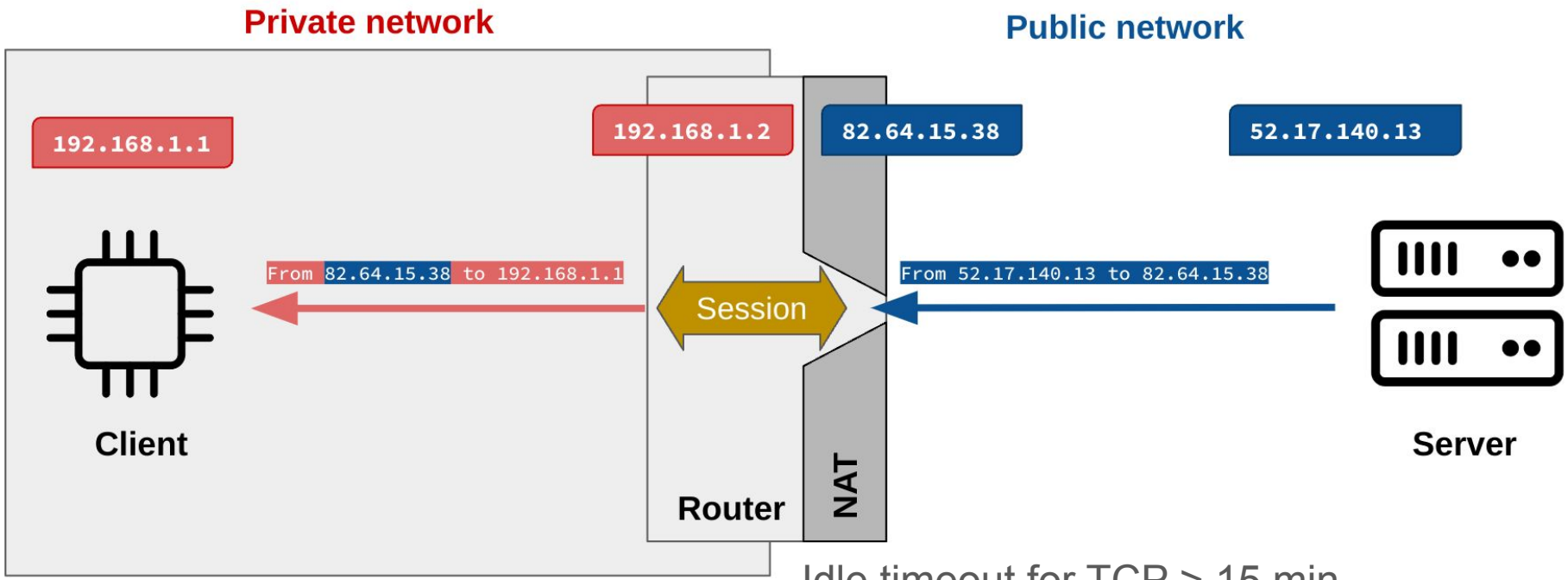
Length	Info
137	Client Hello
102	Hello Verify Request
169	Client Hello
162	Server Hello, Server Hello Done
151	Client Key Exchange, Change Cipher Spec, Encrypted Handshake Message
109	Change Cipher Spec, Encrypted Handshake Message

X.509 certificate: 3849 bytes (signed cert + ECDH)

Length	Info
145	Client Hello
102	Hello Verify Request
177	Client Hello
1851	Server Hello, Certificate, Server Key Exchange, Certificate Request, Server Hello Done
1465	Certificate, Client Key Exchange, Certificate Verify, Change Cipher Spec, Encrypted Handshake Message
109	Change Cipher Spec, Encrypted Handshake Message

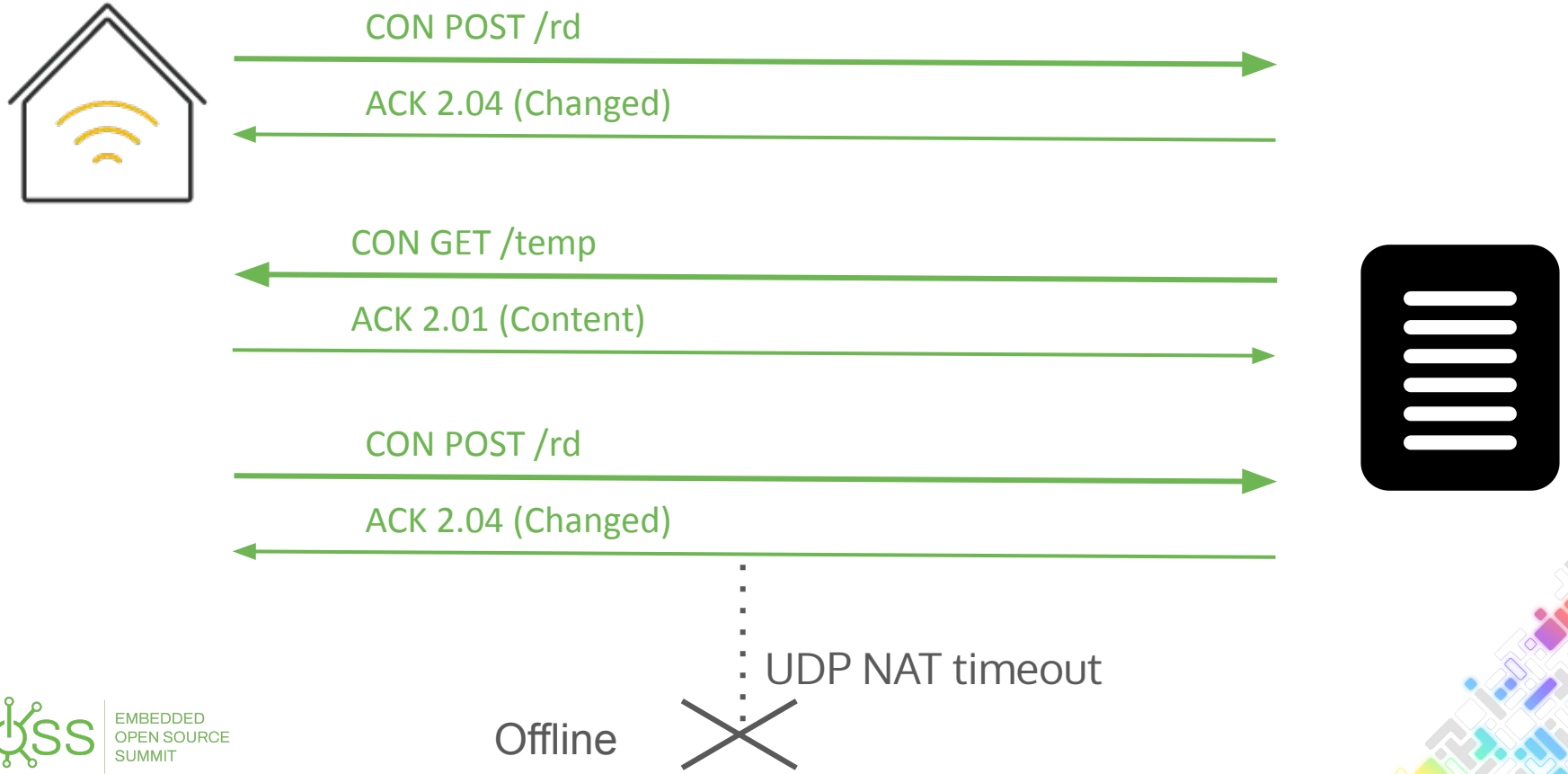
For reference: HTTPS TLS 1.2 handshake ~6k

Connect to the cloud? : UDP & NAT



Idle timeout for TCP > 15 min
For UDP can be 30 sec

Keep the route open



Can’t control the network?

Cloud CoAP server

Border router

Low power network Devices

Home router

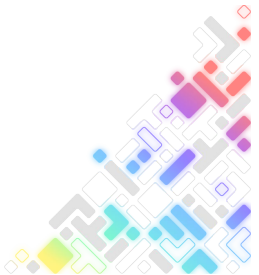
Internet Service Provider

Use “keep-alive” or buffer operations on the cloud side

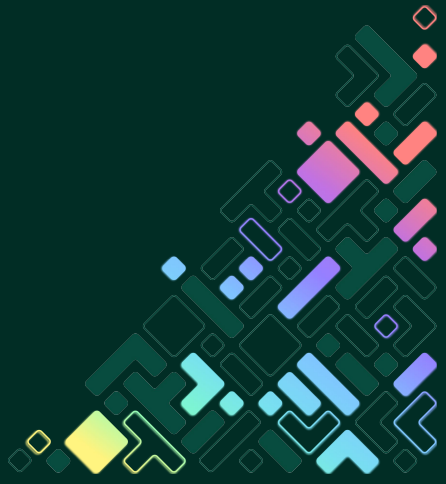
IPv6 one day 🥲

And for cellular based systems?

- Intermittent connections: queueing operations on the cloud side
- SMS for forcing reconnection
- Create your own private APN for cellular solutions, to remove NAT
- Use TCP/MQTT/Websockets, if you can cope with the performances
- IPv6?



OMA Lightweight M2M



OMA Lightweight M2M

A standard device management Protocol on top of CoAP

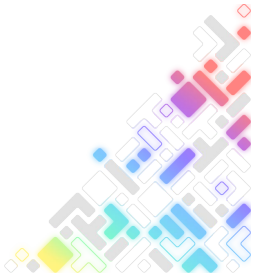
Strong focus on cellular wireless technologies

Keep-Alive system (registration)

Provisioning (bootstrap)

REST model for common management objects (FOTA, monitoring)

Popular in smart metering



Device /3

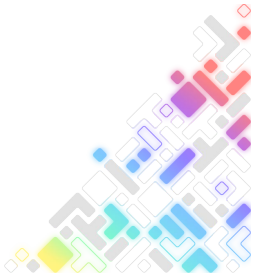
Instance 0	/3/0	Observe ▶ ■ Read Write Delete
Manufacturer	/3/0/0	Observe ▶ ■ Read
Model Number	/3/0/1	Observe ▶ ■ Read
Serial Number	/3/0/2	Observe ▶ ■ Read
Firmware Version	/3/0/3	Observe ▶ ■ Read
Reboot	/3/0/4	Exec ⚙
Factory Reset	/3/0/5	Exec ⚙
Available Power Sources	/3/0/6	Observe ▶ ■ Read
Power Source Voltage	/3/0/7	Observe ▶ ■ Read
Power Source Current	/3/0/8	Observe ▶ ■ Read
Battery Level	/3/0/9	Observe ▶ ■ Read
Memory Free	/3/0/10	Observe ▶ ■ Read
Error Code	/3/0/11	Observe ▶ ■ Read
Reset Error Code	/3/0/12	Exec ⚙

Feedback from the trenches

When to use CoAP?

Constrained networks:

- NBIoT: latency 1.6sec to 10sec
- Thread/Matter: 3sec border router buffering
- or you need reliability in harsh conditions (e.g. max LTE-M coverage)



When to use LWM2M?

If you need the interoperability or the standard compliance

Strong security requirement:

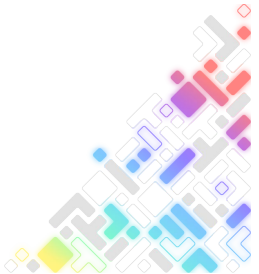
- provisioning certificate, key rotation, multi server with ACLs

When not to use LWM2M?

If you need very compact and very limited number of packet, use plain CoAP

Simple system, without interoperability concerns

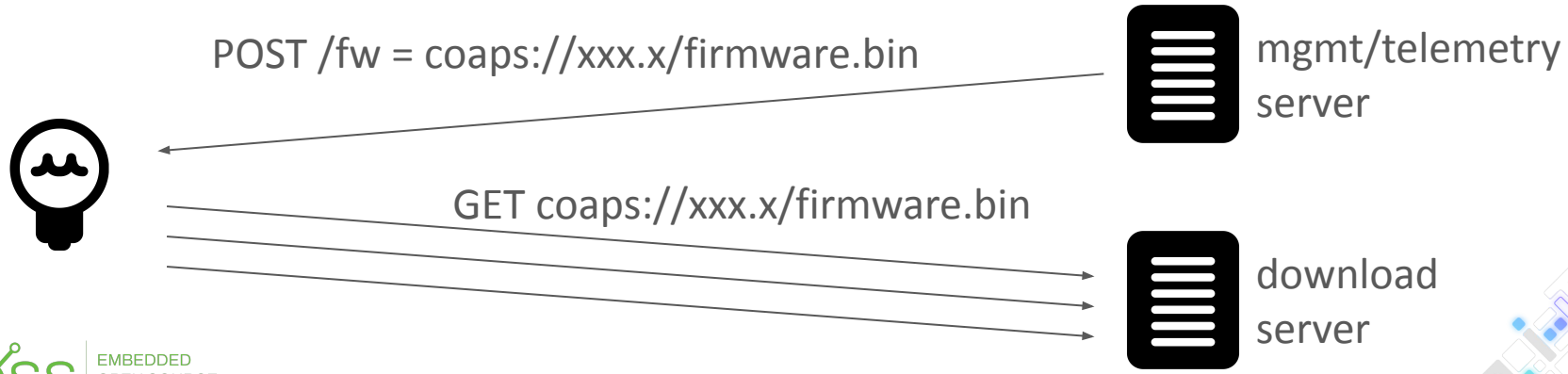
Picking some inspiration is good (avoid the bad parts)



FOTA and CoAP

Device initiated FW download to maximise resiliency:

- Control condition when to start (e.g.: battery status, not in user interaction)
- Can resume on disconnection or reboot

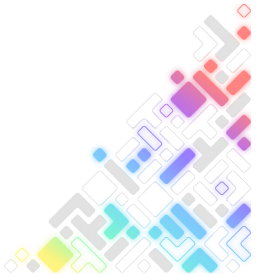


Low power IoT System TCO

Selling sub $100 hardware with or without recurring model

Firmware are always shipped with bugs, and need to be supported for 10 years+
So you'll need to have a lot of control on your software

Open-source blocks at the rescue!



CoAP stack?

Embedded:

Zephyr contains a good quality CoAP client/server and LWM2M client

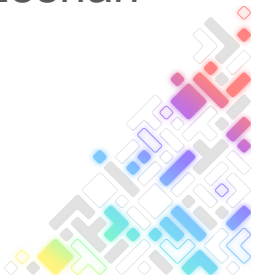
If you need Matter/Thread re-use OpenThread bundled CoAP

libCoAP is awesome if you need something complete on Linux

Server:

Java: Eclipse Californium, github.com/open-coap/java-coap, Eclipse Leshan

Go: plgd-dev/go-coap with pion/dtls



tado° is hiring!

https://apply.workable.com/tado/

Thanks!

julien@vermillard.com
https://www.linkedin.com/in/jvermillard/