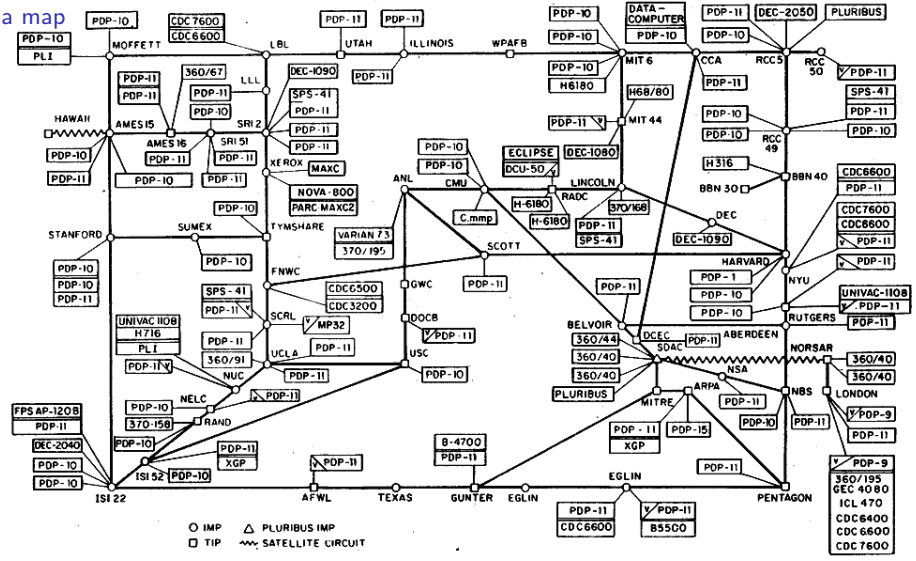
CoAP proxies
Gateway features without gateway requirements

Christian Amsüss <christian@amsuess.com>

2022-06-02, IT-S NOW, Vienna

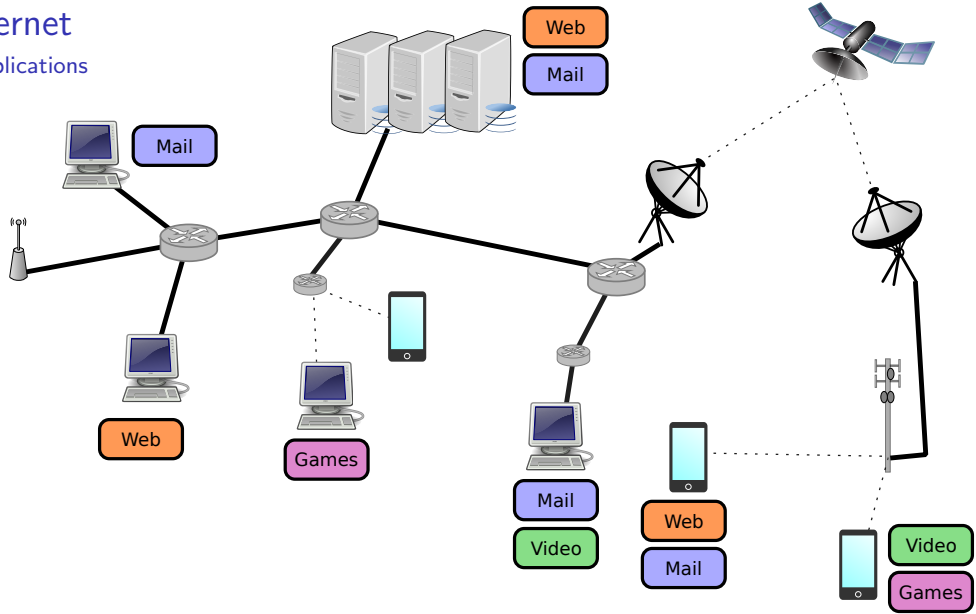
The Internet

when it still fit on a map



The Internet

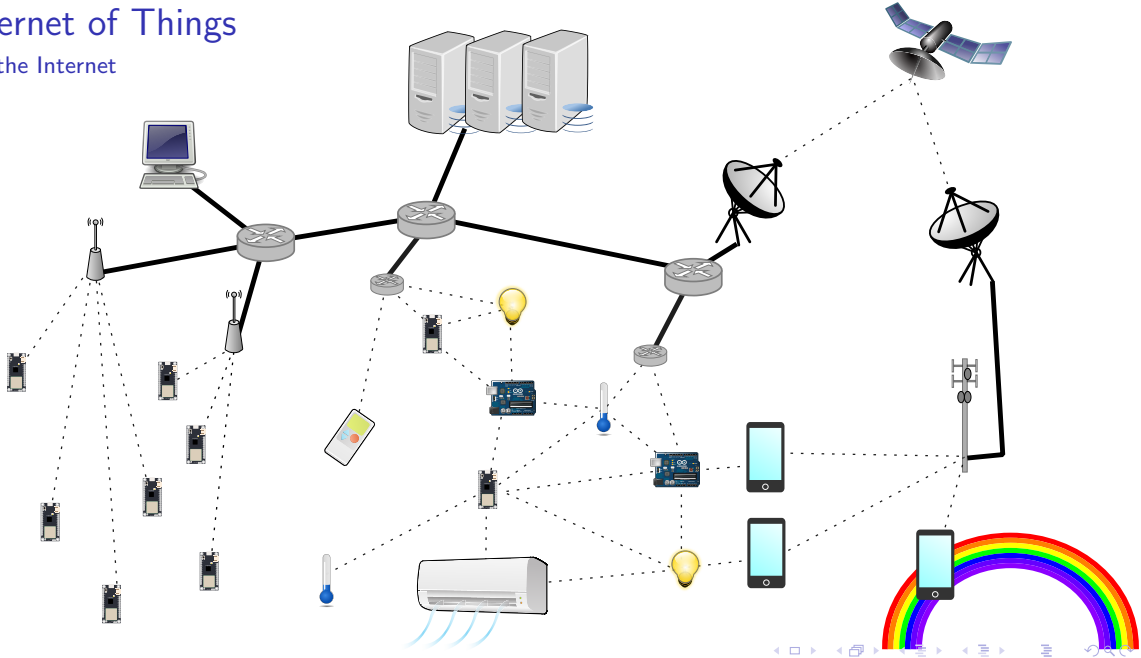
multiple applications



Outline

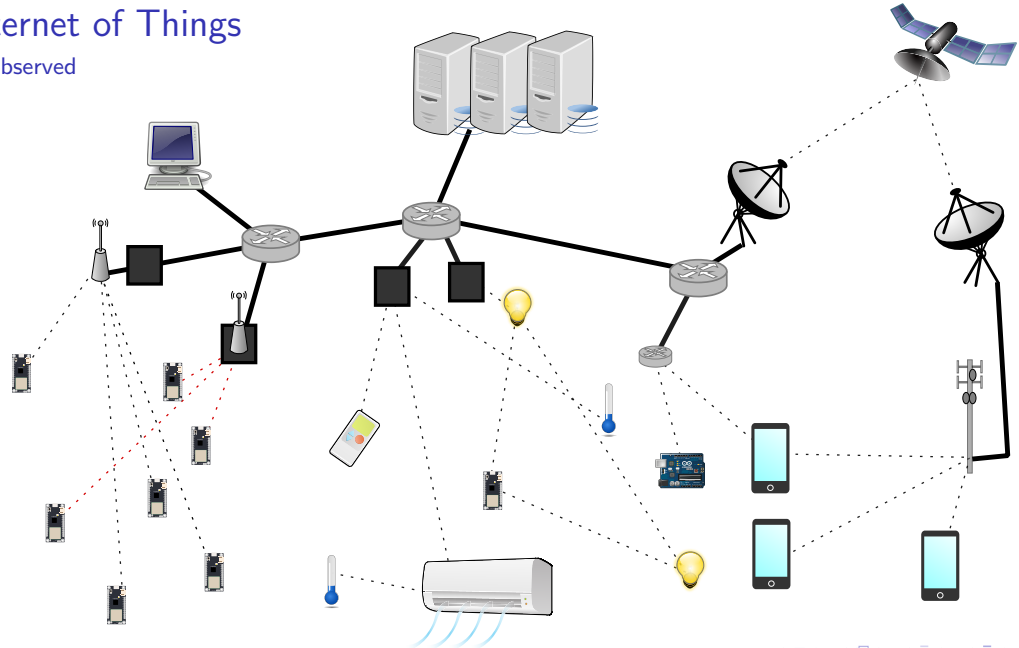
Internet of Things

like the Internet



Internet of Things

as observed



Things of the Internet

Definition and scope

Constrained Device Limited code ($\leq 100\,\text{KiB}$) and RAM ($\leq 1\,\text{MiB}$), power constrained (e. g. battery or solar powered)

Things of the Internet

Definition and scope

Constrained Device Limited code ($\leq 100\,\text{KiB}$) and RAM ($\leq 1\,\text{MiB}$), power constrained (e. g. battery or solar powered)

Constrained Network Small messages, high packet loss, data rates down to $\sim 100\,\frac{\text{mBit}}{\text{s}}$

Details for both in RFC 7228

Things of the Internet

Definition and scope

Constrained Device Limited code ($\leq 100\,\text{KiB}$) and RAM ($\leq 1\,\text{MiB}$), power constrained (e. g. battery or solar powered)

Constrained Network Small messages, high packet loss, data rates down to $\sim 100\,\frac{\text{mBit}}{\text{s}}$

Details for both in RFC 7228

Development stage Devices originally designed for the Internet

Gateways: Why?

- Connectivity: Translate between lower layers

Gateways: Why?

- Connectivity: Translate between lower layers
- Augmenting access

Gateways: Why?

- Connectivity: Translate between lower layers
- Augmenting access
- Data preprocessing / aggregation

Gateways: Why?

- Connectivity: Translate between lower layers
- Augmenting access
- Data preprocessing / aggregation
- Assistance in provisioning

Gateways: Why?

- Connectivity: Translate between lower layers
- Augmenting access
- Data preprocessing / aggregation
- Assistance in provisioning
- Distribution of firmware updates

Gateways: Why?

- Connectivity: Translate between lower layers
- Augmenting access
- Data preprocessing / aggregation
- Assistance in provisioning
- Distribution of firmware updates
- Power saving

Gateways: Why?

- Connectivity: Translate between lower layers
- Augmenting access
- Data preprocessing / aggregation
- Assistance in provisioning
- Distribution of firmware updates
- Power saving
- Customer experience

Gateways: Why?

- Connectivity: Translate between lower layers
- Augmenting access
- Data preprocessing / aggregation
- Assistance in provisioning
- Distribution of firmware updates
- Power saving
- Customer experience
- Prevent a compromised device from reaching third parties

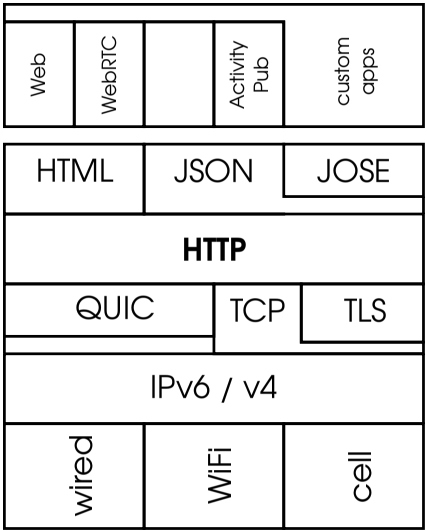
Gateways: Why?

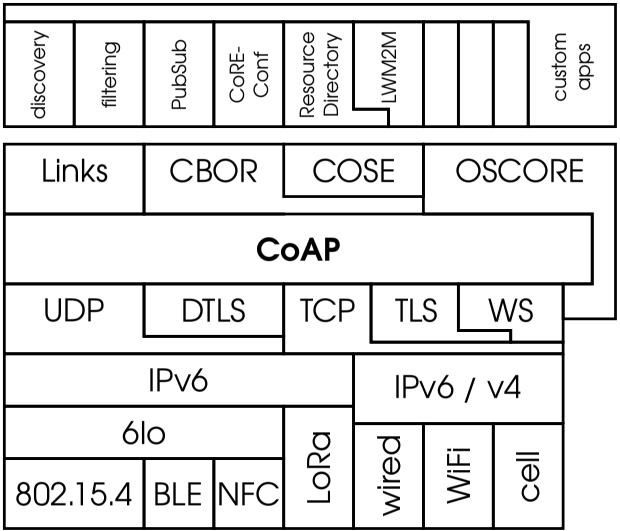
- Connectivity: Translate between lower layers
- Augmenting access
- Data preprocessing / aggregation
- Assistance in provisioning
- Distribution of firmware updates
- Power saving
- Customer experience
- Prevent a compromised device from reaching third parties
- Prevent unauthorized parties from accessing the device

Gateways: Why?

- Connectivity: Translate between lower layers
- Augmenting access
- Data preprocessing / aggregation
- Assistance in provisioning
- Distribution of firmware updates
- Power saving
- Customer experience
- Prevent a compromised device from reaching third parties
- Prevent unauthorized parties from accessing the device
- Avoiding the need for in-device cryptography

Stacks, side by side





CoAP by example

A request in a UDP datagram

```
POST coap://[2001:db8::1]/a/5/
If-Match: 123abc
Content-Format: application/senml+cbor

[{"bpi": 3, "n": "x", "d": 255},
{"n": "y", "d": 128}]
```

```
4002303a161013
5913123abc
1170

ff82a3636270690300617802 18ff
a2006179021880
```

Hex dump slightly rearranged to match HTTP-style option list.

CoAP and transports

. . . and how they meet at proxies

- over UDP/DTLS: General use

CoAP and transports

. . . and how they meet at proxies

- over UDP/DTLS: General use
- over TCP/TLS (RFC 8323): between unconstrained devices
- over WebSockets (RFC 8323): CoAP implementations in browsers

CoAP and transports

. . . and how they meet at proxies

- over UDP/DTLS: General use
- over TCP/TLS (RFC 8323): between unconstrained devices
- over WebSockets (RFC 8323): CoAP implementations in browsers
- over 3GPP NIDD (Open Mobile Alliance): some cellular devices
- more transports in progress

CoAP and transports

. . . and how they meet at proxies

- over UDP/DTLS: General use
- over TCP/TLS (RFC 8323): between unconstrained devices
- over WebSockets (RFC 8323): CoAP implementations in browsers
- over 3GPP NIDD (Open Mobile Alliance): some cellular devices
- more transports in progress

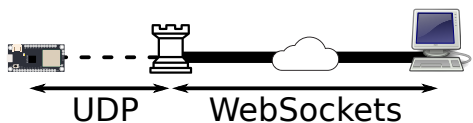
Shared infrastructure?

CoAP and transports

. . . and how they meet at proxies

- over UDP/DTLS: General use
- over TCP/TLS (RFC 8323): between unconstrained devices
- over WebSockets (RFC 8323): CoAP implementations in browsers
- over 3GPP NIDD (Open Mobile Alliance): some cellular devices
- more transports in progress

Shared infrastructure?



OSCORE and EDHOC: above and below CoAP

`GET /path, Observe: 0` $\rightarrow$ `POST Observe: 0, enc(GET /path)`

Data necessary for forwarding stays unencrypted.

OSCORE and EDHOC: above and below CoAP

`GET /path, Observe: 0` → `POST Observe: 0, enc(GET /path)`

Data necessary for forwarding stays unencrypted.

EDHOC	Asymmetric mutually authenticated key exchange
OSCORE	Symmetric encryption (with asymmetric group communication)
ACE	Third party key provisioning (think OAuth)

OSCORE and EDHOC: above and below CoAP

`GET /path, Observe: 0` → `POST Observe: 0, enc(GET /path)`

Data necessary for forwarding stays unencrypted.

EDHOC	Asymmetric mutually authenticated key exchange
OSCORE	Symmetric encryption (with asymmetric group communication)
ACE	Third party key provisioning (think OAuth)

Minimal overhead of encryption

OSCORE: few bytes per message, EDHOC: one round-trip, < 50 byte each

Half-time questions?

Gateway features without gateways: Base setup

- 6LoWPAN network (6TiSCH, RFC 9030)
- border router has MUD configured firewall
- border router runs and announces a CoAP proxy
- no application specific software

Connectivity: Translate between lower layers

Connectivity: Translate between lower layers

That's a router.

Connectivity: Translate between lower layers

That's a router.

6LoWPAN: same hardware as Zigbee, IPv6 address overhead minimized
IPSP: Bluetooth Low Energy network, same compressions

Connectivity: Translate between lower layers

That's a router.

6LoWPAN: same hardware as Zigbee, IPv6 address overhead minimized
IPSP: Bluetooth Low Energy network, same compressions

CoAP proxies can assist to avoid fragmentation.

Augmenting access

Providing a browser accessible local interface

For web hosted UIs: CoAP-over-WebSockets to CoAP-over-UDP proxying

Augmenting access

Providing a browser accessible local interface

For web hosted UIs: CoAP-over-WebSockets to CoAP-over-UDP proxying

Locally hosted UIs: Could devices configure local HTTP reverse proxies?

Data preprocessing / aggregation

CoAP proxies can utilize advertised information to trigger additional behavior.

Data preprocessing / aggregation

CoAP proxies can utilize advertised information to trigger additional behavior.

Example (from draft ietf-core-conditional-attributes):
`GET /temp?c.gt=-4` filters values above -4°C

Assistance in provisioning

"Pairing the device with the network"

6LoWPAN is joined by per-device preshared keys (RFC 9031)

Zero-touch onboarding is work in progress as draft ietf-6tisch-dtsecurity-zerotouch-join.

Distribution of firmware images

SUIT (Software Updates for IoT, RFC 9019) manifests and binaries can be distributed over CoAP.

CoAP proxies can be caching.

Power saving

CoAP proxies adjust (re)transmission parameters to local network.

Resource Directory (RFC 9176) spools discovery information to reduce the need for multicast discovery.

Customer experience

"The Internet is broken!"

Least technical; industry certification like WiFi?

Technical approaches:

- Feature discovery: report missing components.
- Graceful degradation

Prevent a compromised device from reaching third parties

That's a firewall.

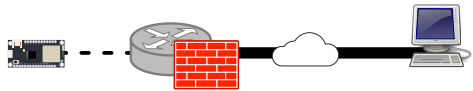
Prevent a compromised device from reaching third parties

That's a firewall.

In Manufacturer Usage Descriptions (MUDs, RFC 8520), manufacturers describe intended behavior; firewalls can then configure themselves accordingly.

Prevent unauthrized parties from accessing the device

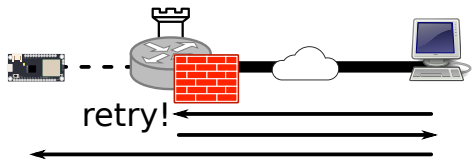
Same firewall argument.



Prevent unauthrized parties from accessing the device

Same firewall argument.

. . . but source IP addresses can be spoofed.
CoAP proxies can enforce reachability.
CoAP proxies can recognize whether encrypted traffic is accepted, and throttle offenders.

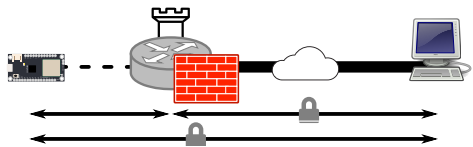


Prevent unauthrized parties from accessing the device

Same firewall argument.

. . . but source IP addresses can be spoofed.
CoAP proxies can enforce reachability.
CoAP proxies can recognize whether encrypted traffic is accepted, and throttle offenders.

. . . but that's not the same as only accepting authenticated peers.
Device could announce ACE server (e. g. per MUD policy), enforce authentication at proxy.



Avoiding the need for in-device cryptography

A proxy as before can be used without inner OSCORE...

...but do you really want to?

Summary: Feature comparison

Application specific gateway	All features; little reuse of code and hardware.
Firewalled IP network	Basic connectivity, fully generic router; security largely depending on device; no fancy features.
CoAP proxy at edge	Security properties on par with gateways, advanced features, some preprocessing possible; generic if feature set matches; some gaps in specifications.
CoAP proxy with loaded code	Feature parity with application specific gateways should be possible; research topic.

You don't use science to show that you're right, you use science to become right.

Mouseover of XKCD 701

The road ahead

- Full guard proxy security was a research paper in 2021, will need practical evaluation.
- Some gaps were surprising: Locally hosted UIs, provisioning, customer experience.

  Taking these to research groups.
- An 80% solution is three mails to IANA away from being specified.

  Want to play?

  Let's try your application and see whether we have the right 80%!

Thank you

Discussion, Questions

Slides and further links are available on the conference website.

Christian Amsüss
christian@amsuess.com

Image components from https://openclipart.org/