Sailing the (Standards) Sea of I-oh-T.

Presenter: Michael Richardson
mcr@sandelman.ca
http://www.sandelman.ca/mcr/

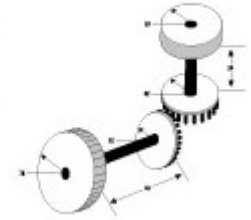http://www.sandelman.ca/SSW/talks/iotottawa2014/sailingseaofiot.html

Who am I?

Xelerance Corp 2003-2007,2014-

xelerance

Internet technologist, doing IP since 1988. "Garage Entrepreneur"
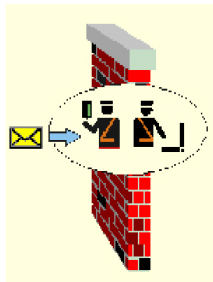
SANDELMAN SOFTWARE WORKS

1996-

SOLIDUM

(1998-2001)

FreeS/WAN (2001-2004)

Linux FreeS/WAN

CENTRE DE RECHERCHE ET DÉVELOPPEMENT EXPÉRIMENTAL EN INFORMATIQUE LIBRE
}{ CREDIL
CENTRE FOR RESEARCH AND EXPERIMENTAL DEVELOPMENT IN INFORMATICS LIBRE

RFC4322
RFC4025
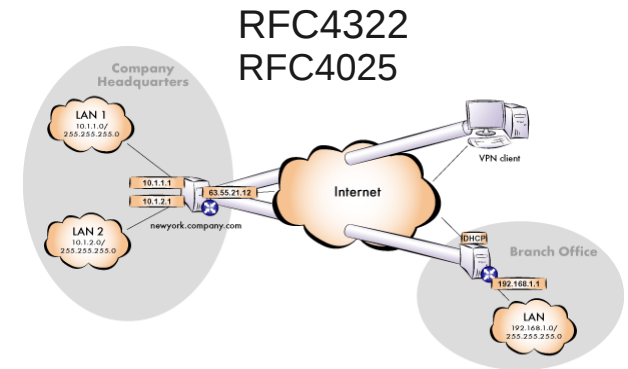
#4 at Milkyway Networks (1994)

ROLL – RFC6550
2012-

6TiSCH

IETF standard security:IPsec/VPN

What is this talk?

1. Gentle Introduction to network part of Internet of Things.

2. Overview of standards that we have, and those that are still coming.

3. IPv6 MESH, RPL, 6tisch and security are my interests

4. Please interrupt and ask questions.

Internet of Things

- INTER / NETWORK part.

- Implies there is a network, connected to another network, possibly many.

Residential Network and Home Area Network Interaction

- Imagine a high end home network:
  - Audio/Video
  - Wireless
  - Telecommuting
  - Home Area Network
- What is the HAN?
  - Network connecting sensors in the home
  - Communications with utilities
  - Services to residents

"Home Area Network"

His Office

Her Office

Home Wireless

A/V LAN

ISP
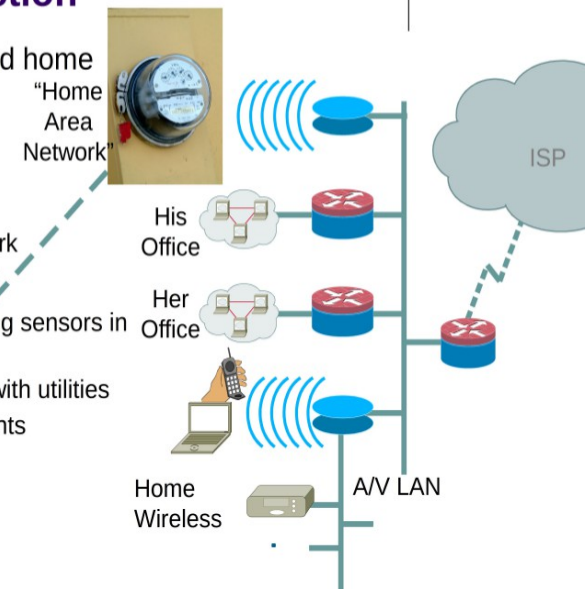
I E T F

Standards

- IETF

  -
  -
  -
  -

| CoAP	Session Layer	DTLS?
UDP	Transport Layer	
IPv6 / RPL	Network Layer	
6lowpan	Network adapter	PANA? 6tisch?
802.15.4	Physical layer	

- IEEE

  - 802.15.4, 802.11,

  - P1920, STD 1547, etc

- Zigbee Alliance

  - Zwave,

IETF Working Groups

- 6man (Internet Area)– generic IPv6 stuff

- 6lowpan (Internet Area) (concluded)

  - 6lo (Internet Area)

- ROLL (Routing Area)

- DICE (Security Area)

- ACE (Security Area)

- CORE (Applications Area)

- HOMENET (Internet Area)

- LWIG (Internet Area)

- OAUTH/JOSE (Security Area)
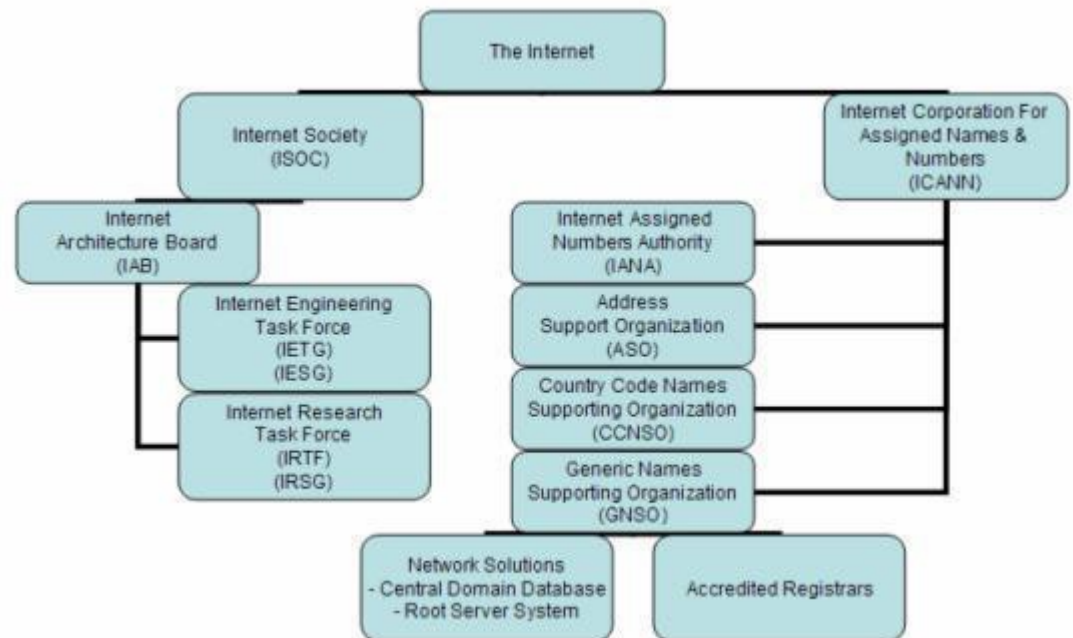
Who does what for the Internet

Zigbee IP Smart Energy Version 2

- http://www.zigbee.org/Standards/ZigBeeSmartEner
- 802.15.4, 6lowPAN
- PANA + EAP-TLS for network security/join control
- ROLL RPL for mesh-over routing
- Tends to use HTTP for control, but this layer not fully standard.

802.15.4 slide 1

- Used by ZigBee, ISA100.11a, WirelessHART, MiWi, 6tisch, …

- 10-meter range, 250 kbit/s typical rate

- 868.0–868.6 MHz (Europe)

- 902–928 MHz (NA, ten channels)

- 2400–2483.5 MHz: (world, 16 channels)

Octets: 1/2	0/1	0/2	0/1/2/8	0/2	0/1/2/8	0/1/5/6/1 0/14	variable		variable	2
Frame Control	Sequence Number	Destination PAN Identifier	Destination Address	Source PAN Identifier	Source Address	Auxiliary Security Header	Information Elements		Frame Payload	FCS
							Header IEs	Payload IEs		
		Addressing fields								
MHR								MAC Payload		MFR

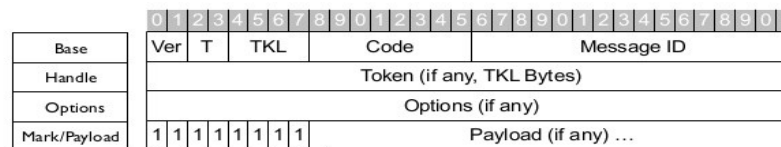**Figure 35—General MAC frame format**

802.15.4 challenges

- Maximum packet size is 128.

- Minimum packet size for IPv6 is 1280.

- THUS 6lowpan explains how to put it together.

- In Wifi (802.11) cost of TX is 10 to 100 times cost of RX.

- In 802.15.4, power is so low, that cost of TX == cost of RX.

- Typical 802.15.4 devices claim multiple year lifetime on single battery.

CoAP

- "CoRE is providing a framework for resource-oriented applications intended to run on constrained IP networks."

- CoAP is HTTP-like, RESTful verbs.

- Runs over UDP, binary format.

    – Supports subscribing to a resource!

CoAP Message

	0 1 2 3 4 5 6 7 8 9 0 1 2 3 4 5 6 7 8 9 0 1 2 3 4 5 6 7 8 9 0 1			
Base	Ver	T	TKL	Code	Message ID
Handle	Token (if any, TKL Bytes)
Options	Options (if any)
Mark/Payload	1 1 1 1 1 1 1 1	Payload (if any) …

Ver	Version
T	Transaction Type
TKL	Token Length
Code	Request Code
Message ID	Identifier

#oscon   OSCON

MESH network 1

- Community MESH network
  - http://goo.gl/aMf3HQ - CzFree Network
  - http://reseaulibre.ca - Montreal network

MESH network 2

- Here is a google search of diagrams of industrial things: http://goo.gl/Z4tb2h

- Lots of really cool animated diagrams out there.

    - TOO MANY are company confidential :-(

    - Really cool to see, wish I could show.

MESH fun

- Routing flaps caused by opening and closing of doors

- Battery operated nodes

- Solar-powered nodes

- Light switches powered by the motion of the lightswitch!
    - http://www.energyharvestingjournal.com/articles/kine
    - http://www.enocean.com/en/switch/
    -

MESH-under networks

- 802.11s: http://en.wikipedia.org/wiki/IEEE_802.11s
- What the XO / One Laptop Per Child (OLPC) used.
- Tries to replicate ethernet to layer-3+,
  - applications assume ethernet bandwidth
  - Ethernet latencies
  - Tended to result in congestion collapse
- B.A.T.M.A.N. - used by community mesh networks

MESH-over networks

- Routing Over Low-power Lossy Networks (ROLL) routing protocol "RPL" (Ripple)

- OLSR – now favoured by community mesh people

P2P RPL

DAG expires along DRO path
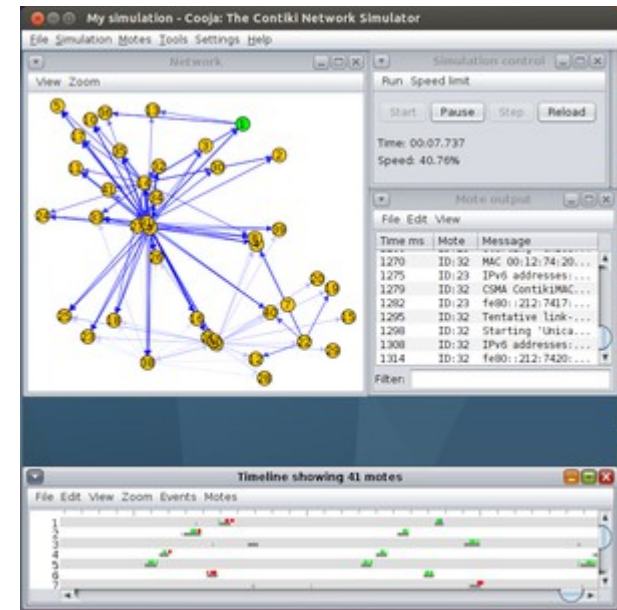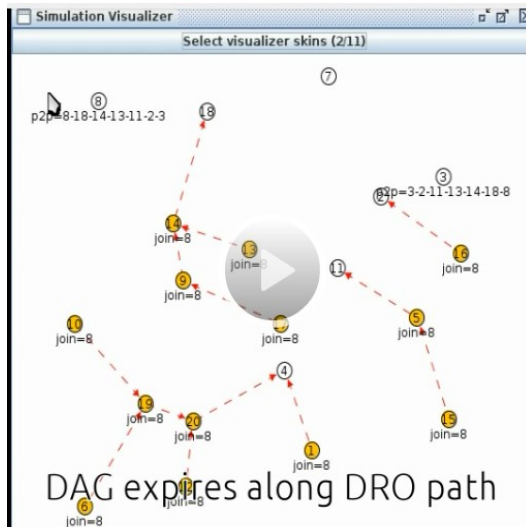
MESH-over

- Can run over any link-type. Can transition from ethernet, to wifi, to Bluetooth, to 802.15.4 (128 byte packets), 802.15.4g (1500 byte packets)

- Naturally supports repeaters and healing

- OLSR, RPL, AODV, many others

More about RPL

- My implementation: https://github.com/mcr/unstrung

- I am co-chair of the IETF working group.

    – Almost done, probably not meet again.

- RPL builds a Directed, Acyclic, Graph (DAG), no loops.

- Uses "Trickle" (rfc6206) to avoid unnecessary traffic

- Packets go up to the root, back down. Very useful for Point to Multi-Point (e.g. AMI)

- RPL P2P (RFC 6997) supports routing across DAG for lighting.

Recent Developments: 6tisch

- http://datatracker.ietf.org/wg/6tisch/charter/

  - "IPv6 over the TSCH mode of IEEE 802.15.4e".

  - TDM vesion of 15.4.

  - Coordinates receivers to be on when transmitters want to transmit. Everyone sleeps otherwise.

  - Makes communication deterministic, suitable for industrial controls.

Slotted Structure: Trade-Off

- Cells are assigned according to application requirements
- Tunable trade-off between
  - packets/second
  - latency
  - robustness

...and energy consumption

16 channel offsets

e.g. 31 time slots (310ms)
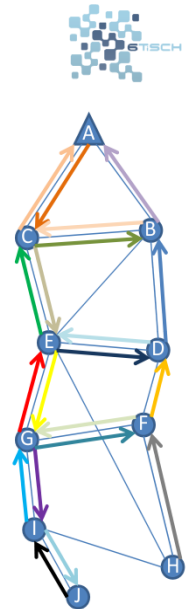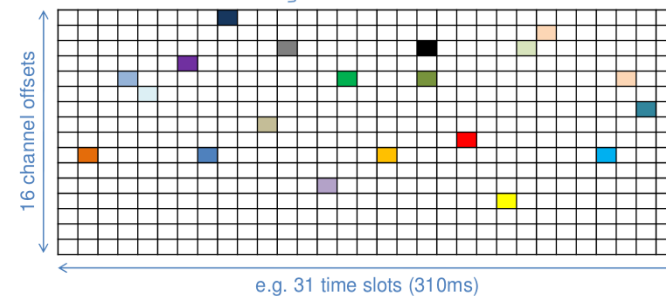
Authorization: ACE

- Alice: "Hi, Bob, I'm Alice, I'm a light switch. Please illuminate"

- Bob: "Hi, I see that you are a light switch, but are you really my light switch?"

- Charter: "produce a standardized solution for authentication and authorization to enable authorized access to resources identified by a URI and hosted on a resource server in constrained environments"

- http://datatracker.ietf.org/wg/ace/c

DTLS-In-Contrained-Environments (DICE)

- 802.15.4 to Security Hood: "My, that's a big DTLS packet you have there."

- (d)TLS: "Oh, the better to support 1000 different options"

- DICE Charter: "The first task of the working group is to define a DTLS profile that is suitable for Internet of Things applications and is reasonably implementable on many constrained devices.

- The second task of the working group is to define how DTLS record layer can be used to transmit multicast messages securely. "

-

- http://datatracker.ietf.org/wg/dice/charter/

Questions

More resources:
http://www.slideshare.net/vgholkar/io-t-protocolsoscon

- – THIS TALK is at:

- – http://www.sandelman.ca/SSW/talks/