The ZigBee IP Stack

IPv6-based stack for 802.15.4 networks

Robert Cragie

Pacific Gas and Electric Company

Chair, ZigBee Security Task Group
Co-chair, ZigBee IP Stack Group
Co-chair, IETF LWIG Working Group

ZigBee®
Control your world

ZigBee stack introduction

ZigBee Stack Evolution

- The ZigBee stack specification is defined in a document with ZigBee reference base 053474
- ZigBee 2004
  - 053474r06
- ZigBee 2006
  - 053474r13
- ZigBee PRO
  - Released 2007
  - 053474r18
  - Basis for ZigBee SE 1.0
- ZigBee IP
  - … a completely different stack

Why a new, different stack?

- ZigBee SE 1.0/PRO gaining momentum in the US (esp. Texas), Australia and the UK
- In the US, NIST SGIP was given a mandate to assist development of US-wide standards for the Smart Grid
- The main edict is that standards must be open
  - Based on IETF and IEEE standards at the lower layers
- The ZigBee Alliance wanted to propel the momentum achieved with ZigBee SE 1.0/PRO going forward
- Initiated development of ZigBee SE 2.0 and ZigBee IP stack specifications with supporting test documentation

ZigBee®
Control your world

Other MAC/PHYs

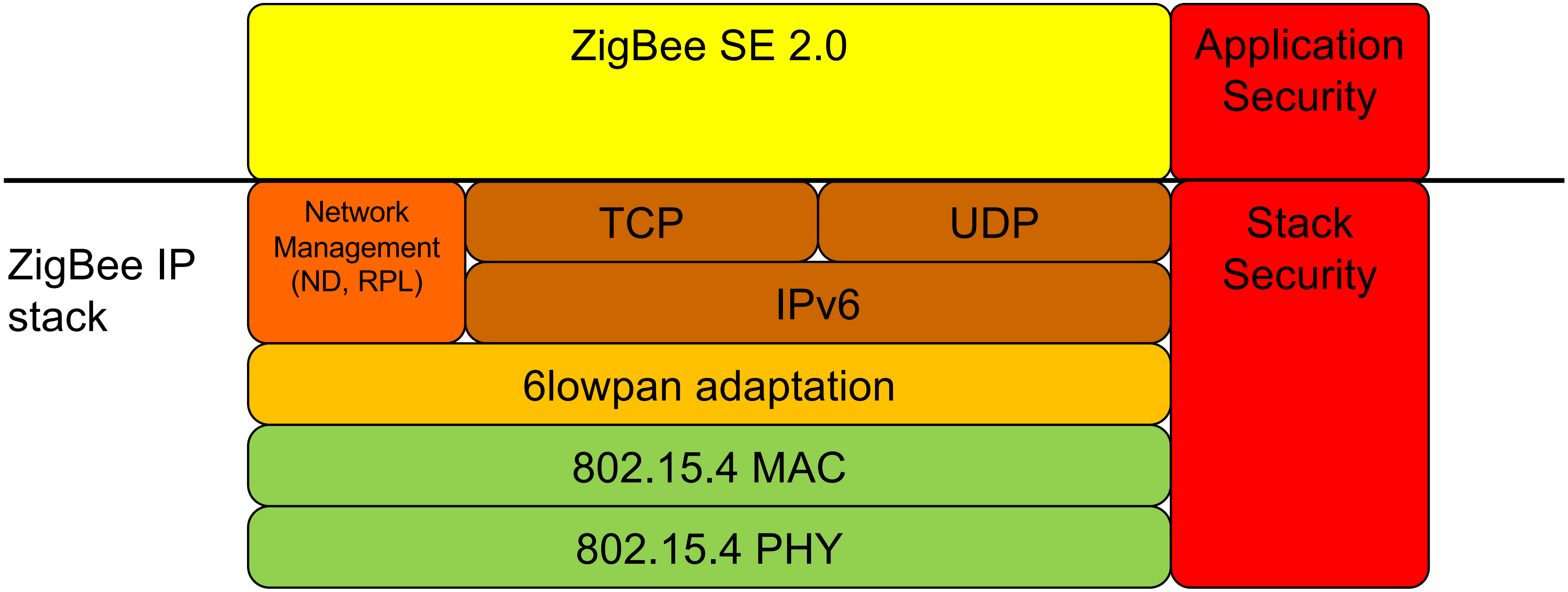
- It is clear that being able to use multiple MAC/PHYs gives maximum flexibility in premises
- The ZigBee and HomePlug Alliances therefore jointly developed the marketing and technical requirements for SE 2.0
- Split into SE 2.0 application layer and underlying stack
- SE 2.0 application layer is stack agnostic as it is based on TCP
- The ZigBee IP stack is aimed at 802.15.4 networks
- ZigBee is also developing guidelines for interfacing SE2.0 to HomePlug powerline and other IEEE-based stacks (Ethernet, 802.11)

ZigBee®
Control your world

The ZigBee IP stack

ZigBee
Control your world

ZigBee IP stack diagram



ZigBee IP specification

- A collection of independent standard specifications (e.g. RFCs) does not produce a standards-based stack which is interoperable across products from different manufacturers
- ZigBee IP specification is a “super-specification”
  - A specification of other standard specifications
- Identifies required standard specifications
- Clarifies modes of operation
  - Interoperability
  - Streamlining

ZigBee IP stack highlights

- IEEE 802.15.4-2006 MAC/PHY
- IETF 6lowpan-hc adaptation layer
- IETF 6lowpan-nd neighbor discovery
- IPv6 network layer
  - RH4 routing header
  - Hop-by-hop header RPL option
- TCP/UDP transport layer
- IETF ROLL RPL routing
  - Non-storing mode
- PANA/EAP/EAP-TTLSv0/TLS security
  - Public key (ECC and RSA) and PSK cipher suites
- mDNS/DNS-SD service discovery support

IEEE 802.15.4-2006 MAC/PHY

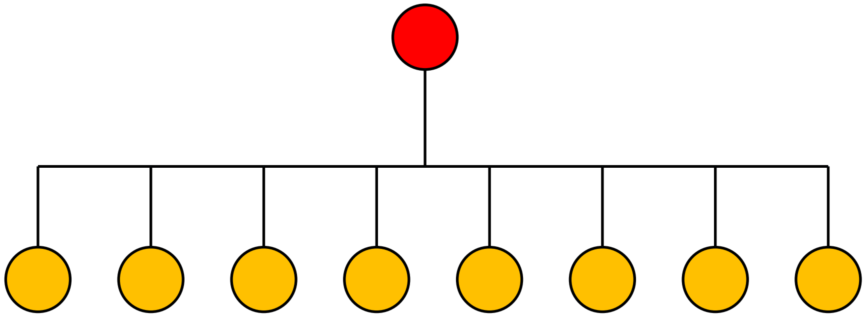
- 802.15.4-2006 standard established for over four years
- Many chipset vendors
- Cheap, low power radios
- Basis for earlier ZigBee devices
  - Potential to upgrade over-the-air
- RFD (reduced function device) aimed at ‘sleepy’, battery-operated devices
  - Sleepy device wakes up infrequently, sends data then goes back to sleep

IETF 6lowpan-hc adaptation layer

- 802.15.4 has small PDUs
  - Maximum PHY PDU is 127 bytes
- IP datagrams have a typical MTU of 1280 bytes
- IETF 6lowpan-hc
  - Header compression to optimize limited bandwidth
    - 40 octets to 3 octets
  - Fragmentation
    - Accommodate IPv6 datagram
- Autoconfiguration of IPv6 addresses based on MAC addresses
- Internet draft
  - draft-ietf-6lowpan-hc-15

IETF 6lowpan-nd neighbor discovery

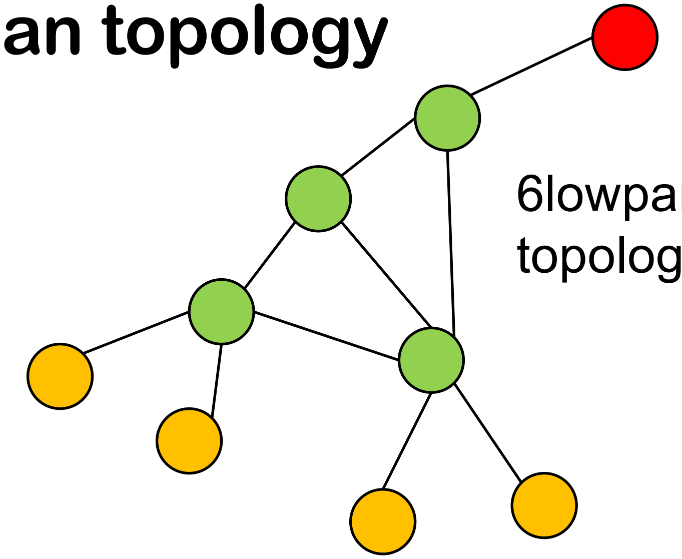
- RFC 4861 neighbor discovery aimed at hosts where router is always on-link
- 6lowpan topology is quite different
- A ZigBee IP network is 6lowpan topology



RFC 4861 topology

🟡 Host

🔴 Router



6lowpan topology

🟡 6lowpan host (6LH)

🟢 6lowpan router (6LR)

🔴 6lowpan border router (6LBR)

IETF 6lowpan-nd neighbor discovery (2)

- 6lowpan-nd produced to specify neighbor discovery for 6lowpan devices
- Uses host-initiated and unicast transactions where possible to help sleepy devices
- No redirects
- Options for disseminating 6lowpan-wide data
  - Prefix information
  - Context information for header compression
  - Border router information
- Address registration mechanism
  - Multihop DAD
  - Neighbor lifetime
- Internet draft
  - draft-ietf-6lowpan-nd-15

IPv6 network layer

- The use of IPv4 is deprecated
  - Running out of addresses
- 6lowpan designed for IPv6 to produce efficient MAC PDUs based on autoconfigured IPv6 addresses
- The Internet of Things can only be truly realized using IPv6
- One additional IPv6 header defined
  - RH4 routing header
- One additional option for hop-by-hop header
  - RPL option

RH4 routing header

- Similar to deprecated RH0
  - Header does not have to contain IP addresses
- Used for source routing within a 6lowpan
  - RPL non-storing mode
- Must not be used in the general Internet
- Internet draft
  - draft-ietf-6man-rpl-routing-header-02

Hop-by-hop header RPL option

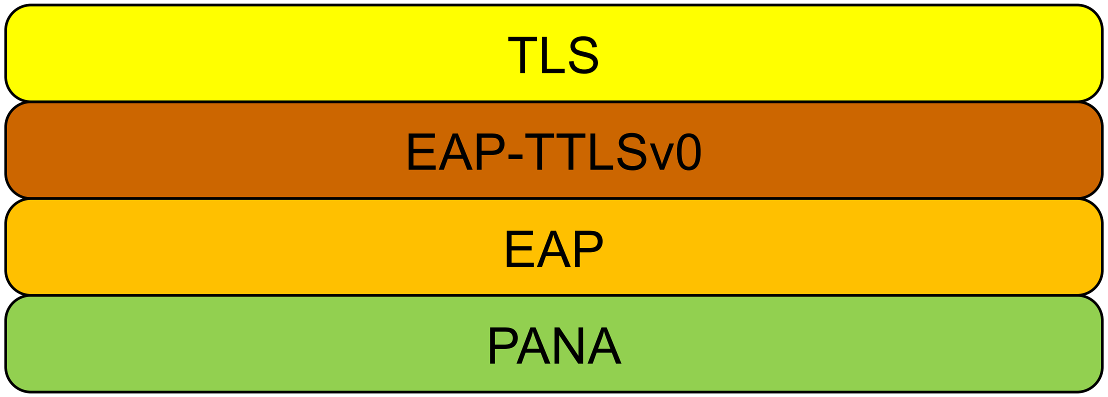
- Data plane ancillary information for RPL DODAG
  - Carried alongside data
  - Control plane information relatively infrequent
  - Limited ability to use control plane information for route repair
- Used for RPL instance selection and route repair
- Not to be used in the general Internet
- Internet draft
  - draft-ietf-6man-rpl-option-02

TCP/UDP transport

- TCP to support HTTP
  - Web technology-based M2M
  - Universal
  - Some challenges for lossy and low-power networks
- UDP to support CoAP
  - Development in IETF CoRE WG
  - RESTful protocol for constrained devices
- RESTful HTTP/XML proposed for ZigBee SE 2.0
  - Data model based on Common Information Model (CIM)
  - XML schema to describe presentation layer
  - Content compression being considered
    - gzip/deflate
    - EXI (efficient XML interchange)

PANA/EAP/EAP-TTLSv0/TLS security

- Follows conventional network access model
  - “If it ain’t broke, don’t fix it!”
- EAP and TLS are already widely used
- PANA is appropriate transport mechanism for 6lowpan



TLS

EAP-TTLSv0

EAP

PANA

Security stack diagram

PANA

- PANA (Protocol for Authentication and Network Access) (RFC 5191) specified
- EAP lower layer
- Transport over UDP
- Similar concept to EAPOL (802.1X)
- Why not use EAPOL?
    - More complex topology than 802.3/802.11
    - No guaranteed direct access to authenticator
    - UDP transport efficiently optimized in 6lowpan-hc
- PANA relay extension developed for 6lowpan networks
    - draft-ohba-pana-relay-03

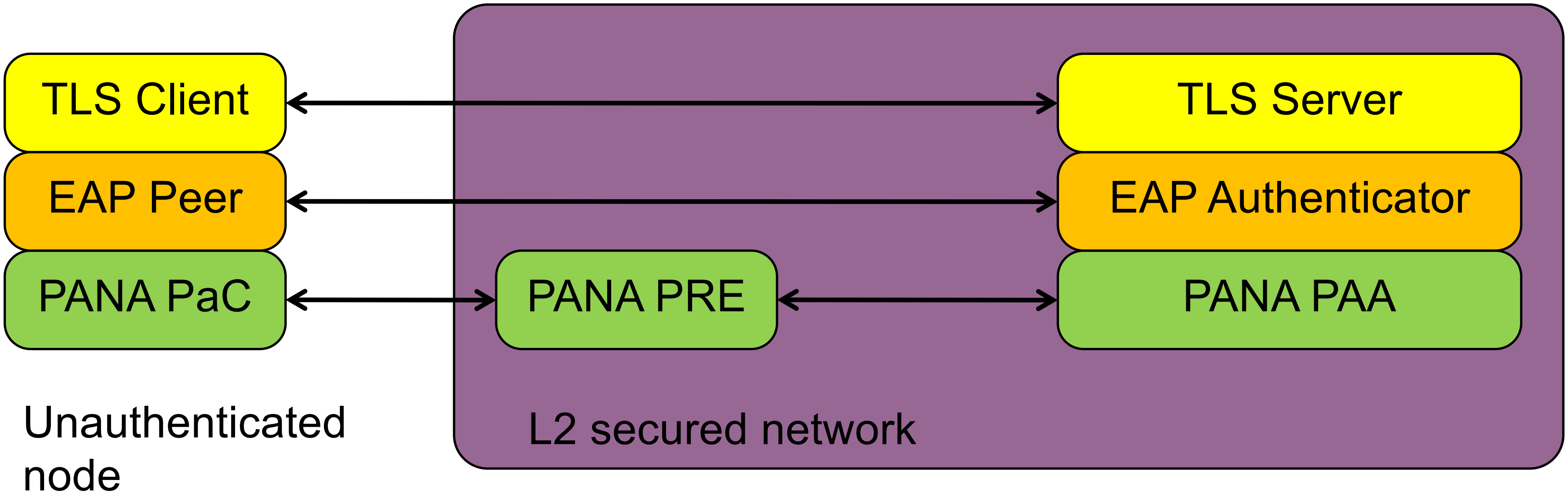
EAP and EAP-TTLSv0

- EAP (RFC 3748): Extensible Authentication Protocol
- Extensible packet format for carrying multiple authentication methods (EAP method)
- Specifies derived key hierarchy (MSK, EMSK)
- EAP-TTLSv0 (RFC 5281) is an EAP method for Transport Layer Security (TLS)
    - Simple extension to EAP-TLS (RFC 5216) to provide a phase for securely transporting additional data
    - Used to transport network key for frame security at the MAC layer
- Uses TLS handshake to provide mutual authentication

TLS

- TLS 1.2 (RFC 5246) specified
- Two mandatory cipher suites
  - TLS_PSK_WITH_AES_128_CCM_8
  - TLS_ECDHE_ECDSA_WITH_AES_128_CCM_8
- Optional cipher suite
  - TLS_DHE_RSA_WITH_AES_128_CCM_8
- AES-128-CCM used for AEAD cipher
  - Implemented in many 802.15.4 chipsets
- Cipher suites in internet drafts
  - draft-mcgrew-tls-aes-ccm-00
  - draft-mcgrew-tls-aes-ccm-ecc-01

Typical security model



IETF ROLL RPL routing

- ROLL: Routing Over Low power and Lossy networks
- 802.15.4 networks are characterized as low power and lossy
- Builds a DODAG (Destination-Oriented Directed Acyclic Graph) comprised of 6lowpan routers to a border router (DODAG root)
- Data flow implicitly to root
- Non-storing mode means source routes have to be stored at root to communicate from root
- Internet draft
    - draft-ietf-roll-rpl-19

mDNS and DNS-SD

- mDNS: draft-cheshire-dnsext-multicastdns-14
  - Method of hosting a DNS server on every device and using multicast to send a request within a local domain
  - Current draft applies to link-local domain only
  - Some additional considerations needed for site local domain and group addressing
- DNS-SD: draft-cheshire-dnsext-dns-sd-10
  - Use of DNS records in service discovery
  - Namespacing and mechanisms appropriate to service discovery above name resolution
  - ZigBee SE 2.0 defines additional service '_smartenergy'

Other considerations

- Missing parts
- Multiple subnet behavior

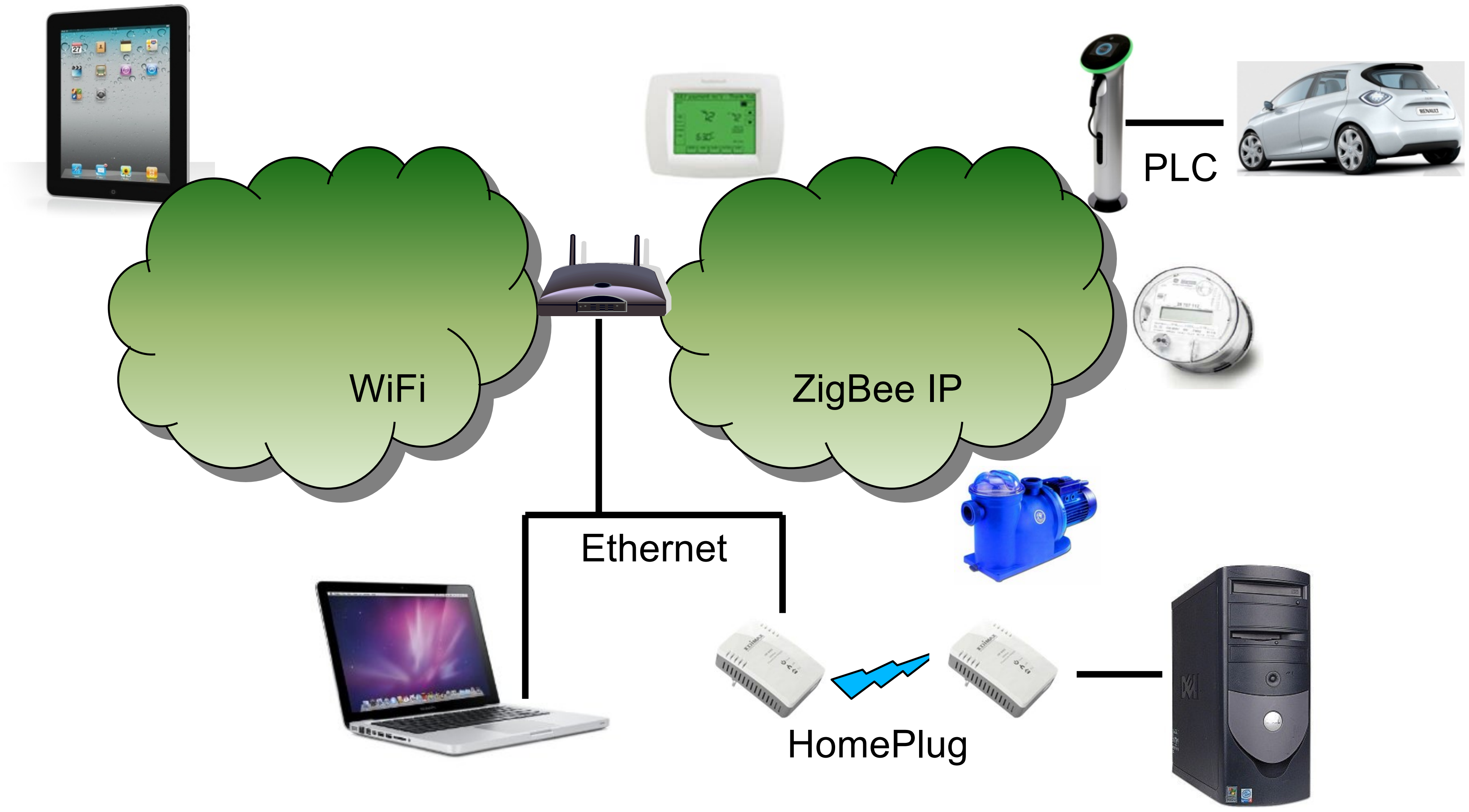
Missing parts

- Protocols specified do not fit perfectly together
- There are overlaps and gaps
- Gaps have to be filled somehow
- PANA relay is a good example of further work undertaken to fill in a gap
- Other work is needed
    - Neighbor exchange protocol for link status and alternative L2 address
        - Link status needed for routing
        - Alternative L2 address (IEEE address in 802.15.4) needed for frame security processing

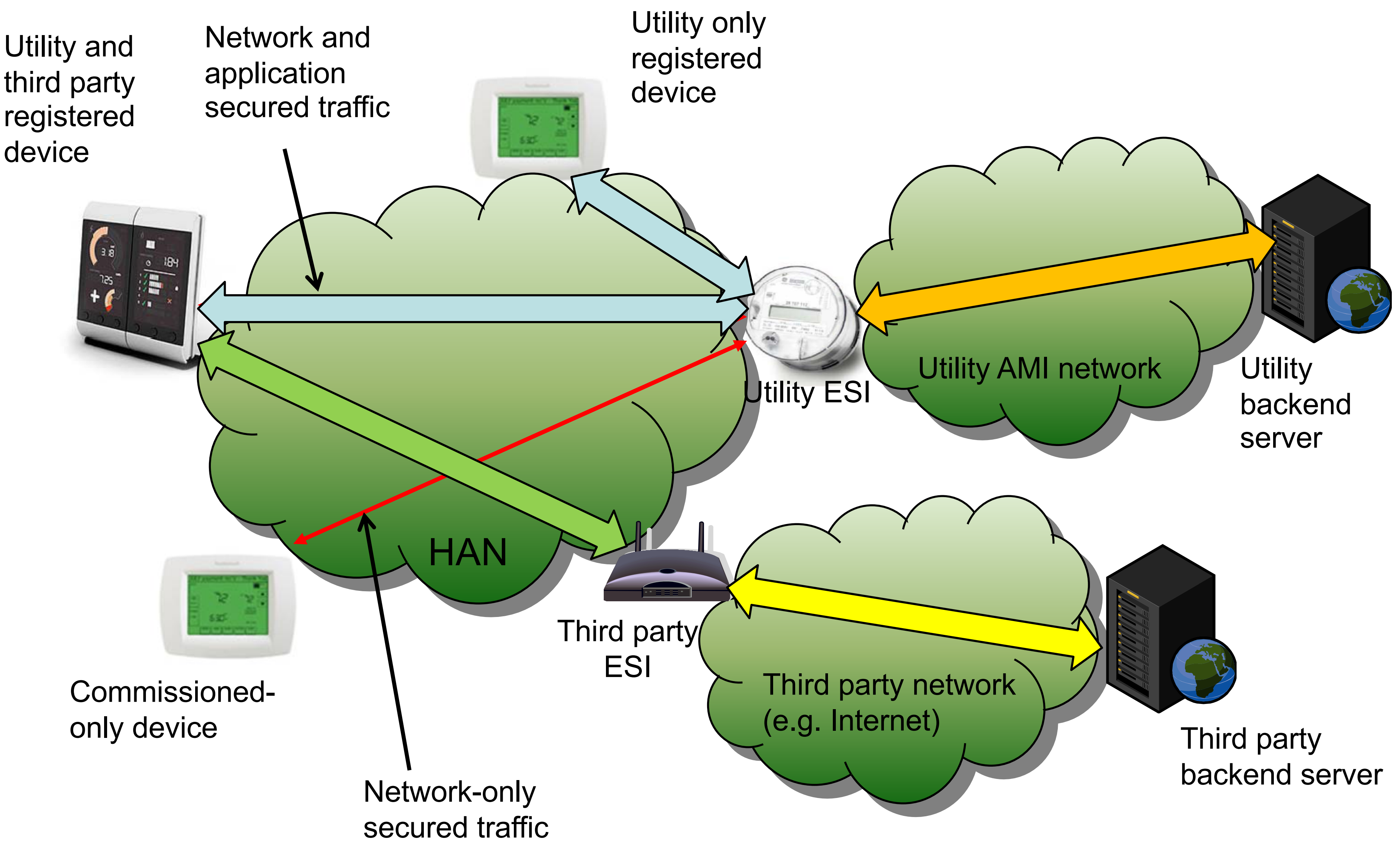
Multiple subnet behavior

- Not specifically a ZigBee IP issue
- ZigBee SE 2.0 needs to work over multiple subnets in the premises
- Some work needed to rationalize prefixes within subnets
- Work being done in v6ops
    - draft-herbst-v6ops-cpeenhancements-00

Example of multiple subnets



Example ZigBee SE 2.0 deployment


Utility and third party registered device
Network and application secured traffic
Utility only registered device
Utility ESI
Utility AMI network
Utility backend server
HAN
Third party ESI
Third party network (e.g. Internet)
Third party backend server
Commissioned-only device
Network-only secured traffic

ZigBee®
Control your world

Progress

ZigBee®
Control your world

Stack support

- Numerous vendors
  - Chipset vendors
  - OEM product
  - Stack suppliers
- Aimed at resource constrained devices
- IP-based open source can be adapted
  - Contiki/uIP
    - Already supports 6lowpan
  - lwIP
    - Limited IPv6 support
  - TinyOS
- Code size
  - Not yet fully known as stacks still experimental

Test events and timeline

- 10 test events held so far in the US and the UK
- Gating test event in August 2010
- 10 implementers past gating event
- Aim to have specification ready for members to start certification at the end of May 2011

Thank you!

robert.cragie@gridmerge.com