ZigBee IP update
IETF 85 Atlanta

Robert Cragie
robert.cragie@gridmerge.com
Introduction

- ZigBee IP is a “super” specification for an IPv6 stack
  - Umbrella specification for a set of IETF RFCs
- Aimed at 802.15.4 MAC/PHY devices
- Mesh network (multi-hop)
- Developed primarily for SEP 2.0 (Smart Energy Profile) application layer traffic to aid migration from SEP 1.0
- Certifiable platform
  - PICS and Test Plan
Transport layer

- TCP
  - Data plane
    - HTTP
    - HTTPS
- UDP
  - Control plane
    - PANA, MLE
  - Data plane
    - CoAP
      - Not currently proposed for SEP 2.0
      - Maybe used in other application profiles
Network Layer

• IPv6
  – RFC 2460
  – Not using IPv4
• 6LoWPAN adaptation layer
  – RFC 4944 (IPv6 over 802.15.4)
  – RFC 6282 (header compression)
• Stateless address autoconfiguration (SLAAC)
  – RFC 4862
  – Maps IPv6 addresses to link layer addresses
  – 16 and 64 bit MAC addresses
• 6LoWPAN contexts
  – ULA and/or global prefixes
Neighbor discovery

• “Classic” ND
  – RFC 4861
  – Not all features used

• 6LoWPAN ND
  – draft-ietf-6lowpan-nd
  – Extends “classic” ND for LLNs and multi-link subnets
Routing

• RPL
  – RFC 6550
  – Route-over
  – Intermediate routers as well as border router
  – Based on Directed Acyclic Graph (DAG)

• MRHOF objective function
  – RFC 6719

• Trickle multicast
  – draft-ietf-roll-trickle-mcast
Security (1)

• Link layer security
  – 802.15.4 frame security (AES-CCM)
  – Global network key

• PANA (EAP transport)
  – RFC 5191 (PANA)
  – RFC 6345 (PANA relay)
  – draft-yegin-pana-encr-avp (encryption AVP)
  – Carries EAP in UDP datagrams
  – Convenient for 6LoWPAN header compression
Security (2)

- **EAP-TLS (EAP method)**
  - RFC 5216
  - Carries TLS records for authentication and key establishment

- **TLS cipher suites**
  - Pre-shared key with AES-CCM
    - c/w Wi-Fi WPA/WPA2 PSK passphrase
  - Elliptic curve DH and ECDSA with AES-CCM
    - In conjunction with device certificate
Additional IETF protocols developed

• MLE (Mesh Link Establishment)
  – Transfer of link costs between neighbors
    • Improved link costs for RPL metrics
  – Transfer of frame counters between neighbors
    • Freshness checking and nonce consistency
  – Dissemination of network-wide information, e.g. beacon payload, PAN ID, channel

• PANA relay
  – Enables PANA for multihop networks

• PANA encryption extensions
  – Secure delivery of configuration parameters
Implementation

• Can’t give details for commercial reasons
  – 7 independent developers
• Aimed at LWIG class 2 devices
  – ~50 kiB data (RAM), ~250 kiB code (Flash)
  – draft-ietf-lwig-guidance
  – Class 1 devices may be able to act as hosts
  – Some devices have more resources and processing power (e.g. ARM9 core, MiBs RAM/Flash)
• Home-grown OS, embedded Linux
Restrictions to meet resource constraints

- **6LoWPAN** – 4 contexts plus stateless (64-bit and 16-bit address)
- **RPL** – non-storing mode
  - Resources required mainly at DAG root
  - Source routing down the DAG
- **TLS** – only two cipher suites
  - Pre-shared key
  - Elliptic curve for processing speed up and memory saving
- **Buffer restrictions for pending data to sleeping hosts**
Other implementation efficiencies

• Holistic approach to combining protocols
• AES-CCM used universally at many layers
• RPL, ND, MAC all have concepts of neighbors and stored addresses
• Limit the storage by linking tables from different protocols together
• Cross-layer management – more complex API whereby all protocols have access to other data and can use it accordingly
Status December 2012

• Specification virtually complete
  – One or two remaining IDs in the process of becoming RFCs
  – Multicast is last remaining item to finalize
• PICS and Test plan almost complete
  – Additional test cases being developed
• Specification Validation Event (SVE) in January 2013
  – Take all specifications to version 1.0
Next steps for LWIG

• Produce more detailed ID or incorporate in guidance document
  – Aim to start ID or text on completion of SVE