Internet of Things: 802.15.4, 6LoWPAN, RPL, COAP

IEEE 802.15.4

IEEE 802.15.4

The IEEE standard 802.15.4 offers physical and media access control layers for low-cost, low-speed, low-power wireless personal area networks (WPANs)

Application Scenarios

- Home Networking
- Automotive Networks
- Industrial Networks
- Interactive Toys
- Remote Metering
- ...

IEEE 802.15.4 Standard Versions

802.15.4-2003

Original version using Direct Sequence Spread Spectrum (DSSS) with data transfer rates of 20 and 40 kbit/s

802.15.4-2006

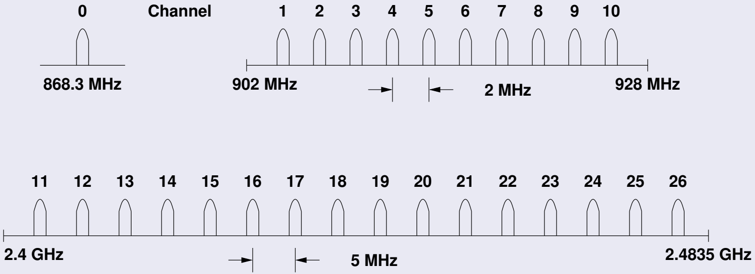
Revised version using Direct Sequence Spread Spectrum (DSSS) with higher data rates and adding Parallel Sequence Spread Spectrum (PSSS)

802.15.4a-2007

Adding Direct Sequence Ultra-wideband (UWB) and Chirp Spread Spectrum (CSS) physical layers to the 2006 version of the standard (ranging support)

Radio Characteristics (802.15.4-2003)

Frequencies and Data Rates



Frequency	Channels	Region	Data Rate	Baud Rate
868-868.6 MHz	0	Europe	20 kbit/s	20 kBaud
902-928 MHz	1-10	USA	40 kbit/s	40 kBaud
2400-2483.5 MHz	11-26	global	250 kbit/s	62.5 kBaud

IEEE 802.15.4 Device Classes

Full Function Device (FFD)

- Any topology
- PAN coordinator capable
- Talks to any other device
- Implements complete protocol set

Reduced Function Device (RFD)

- Reduced protocol set
- Very simple implementation
- Cannot become a PAN coordinator
- Limited to leafs in more complex topologies

IEEE 802.15.4 Definitions

Network Device

An RFD or FFD implementation containing an IEEE 802.15.4 medium access control and physical interface to the wireless medium.

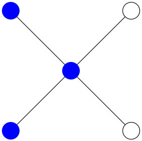
Coordinator

An FFD with network device functionality that provides coordination and other services to the network.

PAN Coordinator

A coordinator that is the principal controller of the PAN. A network has exactly one PAN coordinator.

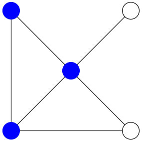
IEEE 802.15.4 Star Topology



Star Topology

- All nodes communicate via the central PAN coordinator
- Leafs may be any combination of FFD and RFD devices
- PAN coordinator is usually having a reliable power source

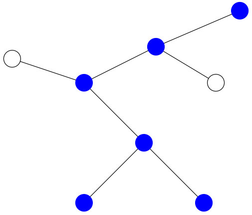
IEEE 802.15.4 Peer-to-Peer Topology



Peer-to-Peer Topology

- Nodes can communicate via the centeral PAN coordinator and via additional point-to-point links
- Extension of the pure star topology

IEEE 802.15.4 Cluster Tree Topology



Cluster Tree Topology

- Leafs connect to a network of coordinators (FFDs)
- One of the coordinators serves as the PAN coordinator
- Clustered star topologies are an important case (e.g., each hotel room forms a star in a HVAC system)

IEEE 802.15.4 Frame Formats

General Frame Format

octets: 2	1	0/2	0/2/8	0/2	0/2/8	variable	2
Frame control	Sequence number	Destination PAN identifier	Destination address	Source PAN identifier	Source address	Frame payload	Frame sequence check

bits: 0–2	3	4	5	6	7–9	10–11	12–13	14–15
Frame type	Security enabled	Frame pending	Ack. requested	Intra PAN	Reserved	Dst addr mode	Reserved	Src addr mode

- IEEE 64-bit extended addresses (globally unique)
- 16-bit “short” addresses (unique within a PAN)
- Optional 16-bit source / destination PAN identifiers
- max. frame size 127 octets; max. frame header 25 octets

IEEE 802.15.4 Frame Formats

Beacon Frames

- Broadcasted by the coordinator to organize the network

Command Frames

- Used for association, disassociation, data and beacon requests, conflict notification, ...

Data Frames

- Carrying user data — this is what we are interested in

Acknowledgement Frames

- Acknowledges successful data transmission (if requested)

IEEE 802.15.4 Media Access Control

Carrier Sense Multiple Access / Collision Avoidance

Basic idea of the CSMA/CA algorithm:

- First wait until the channel is idle.
- Once the channel is free, start sending the data frame after some random backoff interval.
- Receiver acknowledges the correct reception of a data frame.
- If the sender does not receive an acknowledgement, retry the data transmission.

IEEE 802.15.4 Unslotted Mode

Node $\longrightarrow$ PAN, Node $\longrightarrow$ Node

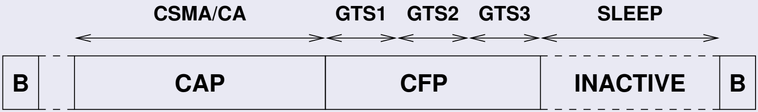
- The sender uses CSMA/CA and the receiver sends an ACK if requested by the sender.
- Receiver needs to listen continuously and can't sleep.

PAN $\longrightarrow$ Node

- The receiver polls the PAN whether data is available.
- The PAN sends an ACK followed by a data frame.
- Receiving node sends an ACK if requested by the sender.
- Coordinator needs to listen continuously and can't sleep.

IEEE 802.15.4 Slotted Mode

Superframes



- A superframe consists of three periods:
  1. During the Contention-Access-Period (CAP), the channel can be accessed using normal CSMA/CA.
  2. The Contention-Free-Period (CFP) has Guaranteed Time Slots (GTS) assigned by the PAN to each node.
  3. During the Inactive-Period (IP), the channel is not used and all nodes including the coordinator can sleep.
- The PAN delimits superframes using beacons.

IEEE 802.15.4 Security

Security Services

Security Suite	Description
Null	No security (default)
AES-CTR	Encryption only, CTR Mode
AES-CBC-MAC-128 AES-CBC-MAC-64 AES-CBC-MAC-32	128 bit MAC 64 bit MAC 32 bit MAC
AES-CCM-128 AES-CCM-64 AES-CCM-32	Encryption and 128 bit MAC Encryption and 64 bit MAC Encryption and 32 bit MAC

- Key management must be provided by higher layers
- Implementations must support AES-CCM-64 and Null

Reading Material I

IEEE.
IEEE Std 802.15.4-2003.
Technical Report 802.15.4-2003, IEEE, October 2003.

IEEE.
IEEE Std 802.15.4-2006.
Technical Report 802.15.4-2006, IEEE, September 2006.

IEEE.
IEEE Std 802.15.4a-2007.
Technical Report 802.15.4a-2007, IEEE, August 2007.

Y. Xiao, H.-H. Chen, B. Sun, R. Wang, and S. Sethi.
MAC Security and Security Overhead Analysis in the IEEE 802.15.4 Wireless Sensor Networks.
Journal on Wireless Communications and Networking, 2006:1–12, 2006.

E. Callaway, P. Gorday, L. Hester, J. A. Gutierrez, M. Naeve, B. Heile, and V. Bahl.
Home Networking with IEEE 802.15.4: A Developing Standard for Low-Rate Wireless Personal Area Networks.
IEEE Communications Magazine, 40(8):70–77, August 2002.

L. D. Nardis and M.-G. Di Benedetto.
Overview of the IEEE 802.15.4/4a standards for low data rate Wireless Personal Data Networks.
In *Proc. of the 4th IEEE Workshop on Positioning, Navigation and Communication 2007 (WPNC'07)*, Hannover, March 2007. IEEE.

S. Labella M. Petrova, J. Riihijarvi, P. Mahonen.
Performance Study of IEEE 802.15.4 Using Measurements and Simulations.
In *Proc. IEEE Wireless Communications and Networking Conference (WCNC 2006)*, pages 487–492, 2006.

Reading Material II

Z. Sahinoglu and S. Gezici.
Ranging in the IEEE 802.15.4a Standard.
In *Proc. IEEE Wireless and Microwave Technology Conference (WAMICON 2006)*, December 2006.

IPv6 over IEEE 802.15.4 (6LoWPAN)

6LowPAN Motivation

Benefits of IP over 802.15.4 (RFC 4919)

1. The pervasive nature of IP networks allows use of existing infrastructure.
2. IP-based technologies already exist, are well-known, and proven to be working.
3. Open and freely available specifications vs. closed proprietary solutions.
4. Tools for diagnostics, management, and commissioning of IP networks already exist.
5. IP-based devices can be connected readily to other IP-based networks, without the need for intermediate entities like translation gateways or proxies.

6LowPAN Challenge

Header Size Calculation...

- IPv6 header is 40 octets, UDP header is 8 octets
- 802.15.4 MAC header can be up to 25 octets (null security) or 25+21=46 octets (AES-CCM-128)
- With the 802.15.4 frame size of 127 octets, we have
  - 127-25-40-8 = 54 octets (null security)
  - 127-46-40-8 = 33 octets (AES-CCM-128)

  of space left for application data!

IPv6 MTU Requirements

- IPv6 requires that links support an MTU of 1280 octets
- Link-layer fragmentation / reassembly is needed

6LowPAN Overview (RFC 4944)

Overview

- The 6LowPAN protocol is an adaptation layer allowing to transport IPv6 packets over 802.15.4 links
- Uses 802.15.4 in unslotted CSMA/CA mode (strongly suggests beacons for link-layer device discovery)
- Based on IEEE standard 802.15.4-2003
- Fragmentation / reassembly of IPv6 packets
- Compression of IPv6 and UDP/ICMP headers
- Mesh routing support (mesh under)
- Low processing / storage costs

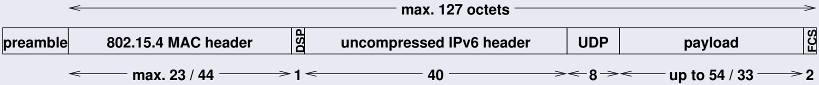
6LowPAN Dispatch Codes

- All LoWPAN encapsulated datagrams are prefixed by an encapsulation header stack.
- Each header in the stack starts with a header type field followed by zero or more header fields.

Bit Pattern	Short Code	Description
00 xxxxxx	NALP	Not A LoWPAN Packet
01 000001	IPv6	uncompressed IPv6 addresses
01 000010	LOWPAN_HC1	HC1 Compressed IPv6 header
01 010000	LOWPAN_BC0	BC0 Broadcast header
01 111111	ESC	Additional Dispatch octet follows
10 xxxxxx	MESH	Mesh routing header
11 000xxx	FRAG1	Fragmentation header (first)
11 100xxx	FRAGN	Fragmentation header (subsequent)

6LowPAN Frame Formats

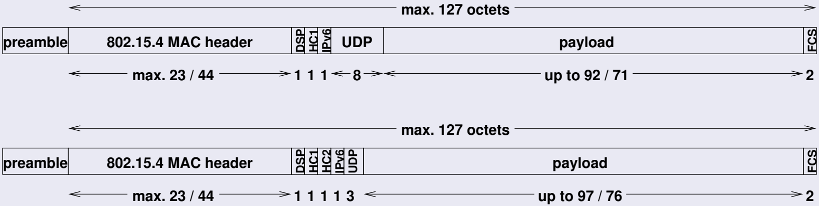
Uncompressed IPv6/UDP (worst case scenario)



- Dispatch code (01000001_2) indicates no compression
- Up to 54 / 33 octets left for payload with a max. size MAC header with null / AES-CCM-128 security
- The relationship of header information to application payload is obviously really bad

6LowPAN Frame Formats

Compressed Link-local IPv6/UDP (best case scenario)



- Dispatch code (01000010_2) indicates HC1 compression
- HC1 compression may indicate HC2 compression follows
- This shows the maximum compression achievable for link-local addresses (does not work for global addresses)
- Any non-compressable header fields are carried after the HC1 or HC1/HC2 tags (partial compression)

Header Compression

Compression Principles (RFC 4944)

- Omit any header fields that can be calculated from the context, send the remaining fields unmodified
- Nodes do not have to maintain compression state (stateless compression)
- Support (almost) arbitrary combinations of compressed / uncompressed header fields

Ongoing Work

- Compression for globally routable addresses (HC1G)
- Stateful compression (IPHC, NHC)

Fragmentation and Reassembly

Fragmentation Principles (RFC 4944)

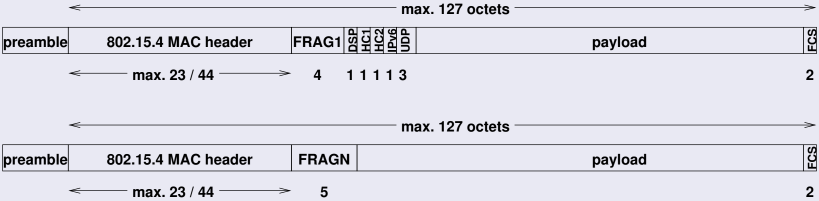
- IPv6 packets to large to fit into a single 802.15.4 frame are fragmented.
- A first fragment carries a header that includes the datagram size (11 bits) and a datagram tag (16 bits).
- Subsequent fragments carry a header that includes the datagram size, the datagram tag, and the offset (8 bits).
- Time limit for reassembly is 60 seconds.

Ongoing Work

- Recovery protocol for lost fragments (RFC 4944 requires to resend the whole set of fragments)

Fragmentation and Reassembly

Fragmentation Example (compressed link-local IPv6/UDP)



Homework Question (consult RFC 4944 first)

- How many fragments are created for an 1280 octet IPv6 packet with no / maximum compression and none / AES-CCM-128 link-layer security?
- How many fragmented datagrams can be in transit concurrently for a 802.14.5 source / destination pair?

Interoperability Evaluation (2009)

6LowPAN Implementations

Name	OS / License	Hardware	Maintained
Jacobs	TinyOS / 3BSD	Telos B, ...	no
Berkley IP	TinyOS / 3BSD	Telos B, ...	active
Arch Rock	TinyOS / EULA	Raven, ...	active
SICSlowpan	Contiki / 3BSD	Raven, ...	active
Sensinode	Own / EULA	Sensinode	active
Hitachi	Own / EULA	Renesas	unknown

Unfortunately...

- The Jacobs implementation uses the TinyOS Active Message framing format and thus does not interoperate

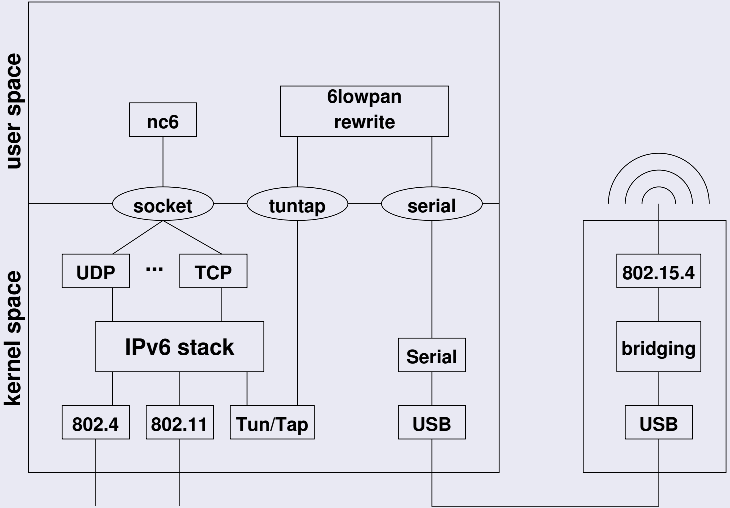
Interoperability Evaluation (2009)

Feature Comparison

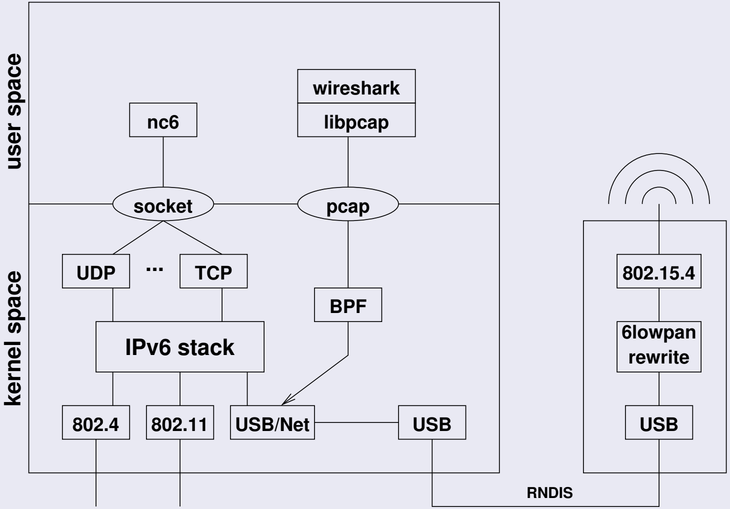
Feature	Jacobs	Berkley	Contiki	Arch Rock
Dispatch Header	+	+	+	+
Dispatch Type	+	+	+	+
Mesh Header	-	+	+	+
Mesh Routing	-	*	*	+
Multicasting Header	-	+	+	+
Multicasting	+	+	+	+
Fragmentation	*	*	*	*
HC1	+	+	+	+
HC2 for UDP	-	-	-	+
HC1g	-	-	o	o
ICMPv6 Echo	+	+	+	+

+ = supported and tested, o = supported but not tested,
- = not supported, * = see [?] for details

Implementation via USB Serial Interfaces



Implementation via USB Network Interfaces



Reading Material I

K.D. Korte, I. Tumar, and J. Schönwälder.
Evaluation of 6lowpan Implementations.
In *4th IEEE International Workshop on Practical Issues in Building Sensor Network Applications (SenseApp 2009)*. IEEE, October 2009.

N. Kushalnagar, G. Montenegro, and C. Schumacher.
IPv6 over Low-Power Wireless Personal Area Networks (6LoWPANs): Overview, Assumptions, Problem Statement, and Goals.
RFC 4919, Intel Corp, Microsoft Corporation, Danfoss A/S, August 2007.

G. Montenegro, N. Kushalnagar, J. Hui, and D. Culler.
Transmission of IPv6 Packets over IEEE 802.15.4 Networks.
RFC 4944, Microsoft Corporation, Intel Corp, Arch Rock Corp, September 2007.

M. Harvan and J. Schönwälder.
TinyOS Motes on the Internet: IPv6 over 802.15.4 (6lowpan).
Praxis der Informationsverarbeitung und Kommunikation, 31(4):244–251, December 2008.

RPL: IPv6 Routing Protocol for LLNs

Motivation and Requirements

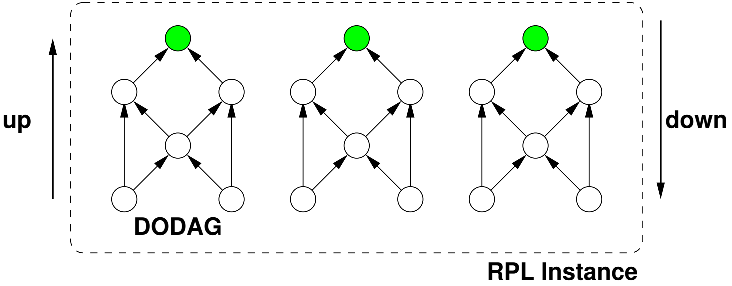
Routing Requirements

- Urban LLNs [RFC5548]
- Industrial LLNs [RFC5673]
- Home Automation LLNs [RFC5826]
- Building Automation LLNs [RFC5867]

Common Characteristics

- Low power and Lossy Networks (LLNs) consisting largely of constrained nodes.
- Lossy and unstable links, typically supporting low data rates, relatively low packet delivery rates.
- Traffic patterns are not simply point-to-point, but in many cases point-to-multipoint or multipoint-to-point.
- Potentially comprising up to thousands of nodes.

RPL Instance and DODAGs



Definition

An RPL Instance consists of multiple Destination Oriented Directed Acyclic Graphs (DODAGs). Traffic moves either up towards the DODAG root or down towards the DODAG leafs.

DODAG and RPL Instance Properties

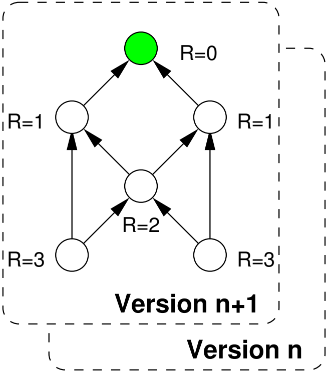
DODAG Properties

- Many-to-one communication: upwards
- One-to-many communication: downwards
- Point-to-point communication: upwards-downwards

RPL Instance Properties

- DODAGS are disjoint (no shared nodes)
- Link properties: (reliability, latency, . . .)
- Node properties: (powered or not, . . .)
- RPL Instance has an optimization objective
- Multiple RPL Instances with different optimization objectives can coexist

Version Numbers and Ranks



Definition

A node's Rank defines the node's individual position relative to other nodes with respect to a DODAG root. The scope of Rank is a DODAG Version.

Route Construction and Forwarding Rules

Route Construction

- Up routes towards nodes of decreasing rank (parents)
- Down routes towards nodes of increasing rank
  - Nodes inform parents of their presence and reachability to descendants
  - Source route for nodes that cannot maintain down routes

Forwarding Rules

- All routes go upwards and/or downwards along a DODAG
- When going up, always forward to lower rank when possible, may forward to sibling if no lower rank exists
- When going down, forward based on down routes

RPL Control Messages

DAG Information Object (DIO)

- A DIO carries information that allows a node to discover an RPL Instance, learn its configuration parameters and select DODAG parents

DAG Information Solicitation (DIS)

- A DIS solicits a DODAG Information Object from an RPL node

Destination Advertisement Object (DAO)

- A DAO propagates destination information upwards along the DODAG

DODAG Construction

Construction

- Nodes periodically send link-local multicast DIO messages
- Stability or detection of routing inconsistencies influence the rate of DIO messages
- Nodes listen for DIOs and use their information to join a new DODAG, or to maintain an existing DODAG
- Nodes may use a DIS message to solicit a DIO
- Based on information in the DIOs the node chooses parents that minimize path cost to the DODAG root

Comment

- Essentially a distance vector routing protocol with ranks to prevent count-to-infinity problems.

Reading Material I

T. Winter, P. Thubert, A. Brandt, T. Clausen, J. Hui, R. Kelsey, P. Levis, K. Pister, R. Struik, and JP. Vasseur.
RPL: IPv6 Routing Protocol for Low power and Lossy Networks.
Internet-Draft (work in progress) <draft-ietf-roll-rpl-12>, Cisco Systems, Sigma Designs, LIX, Arch Rock Corporation, Ember Corporation, Stanford University, Dust Networks, October 2010.

M. Dohler, T. Watteyne, T. Winter, and D. Barthel.
Routing Requirements for Urban Low-Power and Lossy Networks.
RFC 5548, CTTC, UC Berkeley, Eka Systems, France Telecom R&D, May 2009.

K. Pister, P. Thubert, S. Dwars, and T. Phinney.
Industrial Routing Requirements in Low-Power and Lossy Networks.
RFC 5673, Dust Networks, Cisco Systems, Shell, October 2009.

A. Brandt, J. Buron, and G. Porcu.
Home Automation Routing Requirements in Low-Power and Lossy Networks.
RFC 5826, Sigma Designs, Telecom Italia, April 2010.

J. Martocci, P. De Mil, N. Riou, and W. Vermeylen.
Building Automation Routing Requirements in Low-Power and Lossy Networks.
RFC 5867, Johnson Controls Inc, Ghent University, Schneider Electric, Arts Centre Vooruit, June 2010.

Constrained Application Protocol (CoAP)

1. IEEE 802.15.4
   - Radio Characteristics and Topologies
   - Frame Formats, Media Access Control, Security
2. IPv6 over IEEE 802.15.4 (6LoWPAN)
   - Header Compression
   - Fragmentation and Reassembly
3. RPL: IPv6 Routing Protocol for LLNs
   - Instances, DODAGs, Versions, Ranks
   - DODAG Construction and RPL ICMPv6 Messages
4. Constrained Application Protocol (CoAP)
   - Transactions and Methods
   - Message Formats

CoAP Overview

Characteristics

- Constrained machine-to-machine web protocol
- Representational State Transfer (REST) architecture
- Simple proxy and caching capabilities
- Asynchronous transaction support
- Low header overhead and parsing complexity
- URI and content-type support
- UDP binding (may use IPsec or DTLS)
- Reliable unicast and best-effort multicast support
- Built-in resource discovery

Larger Picture

CoAP Layers in the Protocol Stack

- CoAP transactions provide reliable UDP messaging
- CoAP methods resemble HTTP method requests and responses
- CoAP method calls may involve multiple CoAP transactions
- Roles at the transaction layer may change during a method request / response execution

Application
CoAP Methods
CoAP Transactions
UDP
IPv6 / RPL
6LoWPAN
802.15.4

CoAP Transactions

Messages

Message	Description
CON	Confirmable requests that the receiving peer sends an acknowledgement or a reset
NON	Non-confirmable messages do not request any message being sent by the receiving peer
ACK	Acknowledges that a CON has been received, may carry payload
RST	Indicates that a CON has been received but some context is missing to process it

- Transactions are invoked peer to peer (not client/server)
- Transactions are identified by a Transaction ID (TID)

CoAP Methods

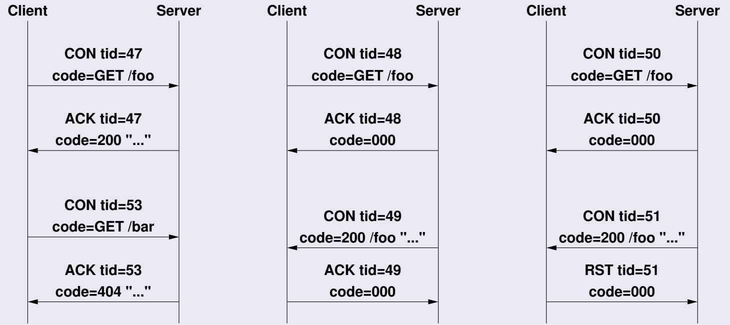
Methods

Method	Description
GET	Retrieves information of an identified resource
POST	Creates a new resource under the requested URI
PUT	Updates the resource identified by an URI
DELETE	Deletes the resource identified by an URI

- Resources are identified by URIs
- Methods are very similar to HTTP methods
- Response codes are a subset of HTTP response codes
- Options carry additional information (similar to HTTP header lines, but using a more compact encoding)

CoAP Message Exchanges

Examples



- Synchronous transaction (left)
- Asynchronous transaction (middle)
- Orphaned transaction (right)

CoAP Message Format

CoAP Header

```
 0                   1                   2                   3
 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
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
|Ver| T |  OC   |      Code     |         Transaction ID        |
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
|   Options (if any) ...
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
|   Payload (if any) ...
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
```

- The `Ver` field contains the version number, the `T` field the message type, and the `OC` field the number of options.
- The `Code` field carries the method code / response code (methods are numbers not strings).
- The unique `Transaction ID` is changed for every new request but not during retransmissions.

CoAP Message Format

CoAP Option Format

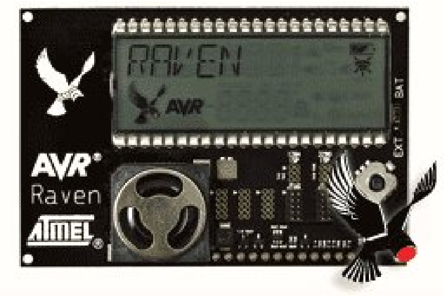
```
  0   1   2   3   4   5   6   7
+---+---+---+---+---+---+---+---+
| option delta  |    length     | for 0..14
+---+---+---+---+---+---+---+---+
                                                   for 15..270:
+---+---+---+---+---+---+---+---+---+---+---+---+---+---+---+---+
| option delta  | 1   1   1   1 |          length - 15          |
+---+---+---+---+---+---+---+---+---+---+---+---+---+---+---+---+
```

- The option delta identifies the option type, encoded as the delta (difference) to the previous option code.
- The option code implies the type of the encoded data.
- URI parameters are carried in options.
- The content-type defaults to text/plain.

Reading Material I

Z. Shelby, B. Frank, and D. Sturek.
Constrained Application Protocol (CoAP).
Internet-Draft (work in progress) <draft-ietf-core-coap-02>, Sensinode, SkyFoundry, Pacific Gas and Electric, September 2010.

Demo: ATMEL Raven / Contiki



Description

- ATmega1284PV: 8 bit, 20 MHz, 16K RAM, 128K Flash
- Contiki 2.4 (6LoWPAN, UDP, TCP, HTTP, ...)