CoRE Monday 13:00-15:00

Chairs: Carsten Bormann, Cullen Jennings

Jabber scribe: Linyi Tian

Note taker: Robert Cragie

Name abbreviations:

- CB: Carsten Bormann
- AC: Angelo Castellani
- RC: Robert Cragie
- LE: Lars Eggert
- KL: Kepeng Li
- BM: Bob Moskowitz
- MN: Mark Nottingham
- EKR: Eric Rescorla
- ZS: Zach Shelby
- LT: Linyi Tian
- JT: Joe Touch
- HT: Hannes Tschoefenig

13:00 Admin (10 min)

Intro from Carsten. Solve remaining few issues of the first set of deliverables.

IPR principles reminder

IAB meeting Friday and Sat. 70+ position papers plus tutorial slides available. IAB report will be coming out to report from the workshop

10/100 and 50/250

Not just a single class of constrained node

Three classes:

- Class 0: too constrained to run securely on Internet
- Class 1: ~10KiB data, ~100KiB code “quite constrained”, “10/100” may need binary protocols etc.
- Class 2: ~50KiB data, ~250KiB code “not so constrained”, “50/250” – can run HTTP, XML etc.

Two milestones met, constrained security spec not so good (due Dec 2010).

Jan 2011 recharter to add things reduced out of initial scope

WG drafts discussed today

13:10 Link format

draft-ietf-core-link-format-03 (Shelby 5 minutes)

Short update. Adaptation of web linking content. Main use in CoRE, want to be able to list resources available on CoRE server. Use GET on /.well-known/core URI. Server will return a payload containing links.

WGLC e/o year, ended at end of January. 9 tickets to be closed from the call. Mostly editorial. More text re. alternative link formats (atom, html). Added three use case Discovery, Resource Collections and Resource Directory.

Diff to RFC 5988. This is a payload, not in a link header is the main difference

draft-vial-core-link-format-wadl-00 worth reading

RFC 5988 done, basing work on that

Tested in two plugfests. Only trivial issues found, fixed in -03

Discussion

LT: Not mandatory to use WADL?

ZS: No, just one way of doing it

MN: Changing WADL?

ZS: No using as specified.

MN: Still uncomfortable with changing the attribute names. Linking but not linking, will create some subtle interop issues.

ZS: No changes – used 'title' as specified. Added new attributes appropriate for M2M.

MN: Inventing something new like weblinking but separate. Nice if it can be within 5988.

ZS: Big re-write after Maastricht. Using more weblinking relations.

MN: Still defining content-type for list of links?

ZS: Yes application/link-format.

MN: Bring it up in apps area list, others may find it useful.

Jabber: Procedure to define new attributes?

ZS: AD says we need a registry for adding more attributes. Normal IANA procedure for requesting new entry, e.g. Observe needs its own flag OBS

13:19 Core CoAP

draft-ietf-core-coap-05 (Shelby 25 minutes)

A lot of feedback after Beijing, 04-05. Focus on what still needs to be done. Plugfest in Beijing on -04, focused on optional features, Observe and Block work. -> -05 – closed 13 tickets and did a re-org of the document.

(slides detail changes)

Tech changes

Added content response code in addition to 2.00. Drafts now all use 2.05

- Allow 2.02 in response to POST
- Improve message deduplication rules
- Max-Age removed from requests
- Location-Query Option added
- ETag length set to 1-8 bytes

(for tickets see slides)

Don't really affect implementations

Issues

How to respond to a NON request?

NON means not just no ack but no response, But that doesn't work.

NON POST is meaningless in that sense – you have to get some response

NON does not have an ACK. but you will get a response on a new message exchange. Multicast requests could have an If-Success option, i.e. if the receiver didn't process, would not send any back. Need a ticket.

UTF8 URI matching needs clarification

URIs are specified as UTF-8. (RFC 5198). Why – for HTTP mapping

Difficult for constrained devices. Should do a simple binary comparison of URIs. Section 6.2 needs to explain this. Need a ticket

HTTP mapping section

Need to revamp HTTP mapping section a bit. Current description goes into too much detail. Klaus wrote a draft suggesting simple standard text to put into section 2. and add implementation considerations. Need a ticket: Adopt simple standard text and create a new mapping guide with considerations plus examples

Also fair to other protocols, e.g. XMPP/SIP

AC: We are working on document, please help us

Security updates

Unclear what is being specified. Clarify that DTLS is going to be the must-implement security mechanism.

SharedKey, MultiKey and Certificate modes are all related to DTLS.

PSK is must to implement

NoSec mode (not DTLS) may be used in combination with IPSec, L2 enc. or really no sec. needed

Ticket: Must implement cipher suites and align with ZigBee IP

PSK must use TLS_PSK_WITH_AES_128_CCM_8

Certificate mode TLS_ECHDE_ECDSA_AES_128_CCM_8

Ticket: IPSec could reference kivinen draft

Ticket: Clarify interaction of DTLS auth. and resource access control

Next steps

20+ implementations out there

A few minor updates identified

AC: First question: Deferred response. What can happen if the empty ack. is lost but not the code response? Probably the client should rexmit even if it has already received the response.

ZS: Need to look through message exchange diagrams. Need to be able to ignore dups, but get the response,

AC: State of devices – some text in my document. Second question: Define a timeout for receiving deferred response.

ZS: Threw idea out on mailing list- doesn't seem to make much sense. HTTP on TCP so you will know. Not intended to take days to get it back. Up to the client to decide how long.

AC Third question: Handle token option – when deferred (piggy back), complex to check the msg id and token. Token is optional – may be some text why you don't need to implement token?

ZS: Some text why you want to use default token, and some text on uniqueness

LE. Do timers need to be jittered, or is it possible to do this? To help synchronisation issues?

ZS: Need to look at text. We only have rexmit timeout in document.

Jabber: Anyone implement DTLS yet?

ZS: TLS has been done on 6lp and in ZigBee IP.

CB: libcoap is being linked but difficult to link to OpenSSL.

KL: Response mode on timer. Two suggestions. Response code 4.08 can merge - inconsistent use. MaxAge – no decision, need to clarify in CoAp-05. Server sends response to proxy with MaxAge 60 secs. then response needs to be sent to client. This is not defined.

ZS: Look at caching section – should cover this case

CB: 4.08 is done in Block, not core

13:46 Block

draft-ietf-core-block-02 (Bormann 15 minutes)

Needed to work with resource reps. larger than MTU. Base said should not send larger than 1K plus a few options. Block splits into multiple blocks.

(frame descrs. from slide)

16 <= x = 2048 blocks

2048 an accident not compatible with MTU 1152 – maybe relegate szx = 7 to reserved

Use ETag to synchronise block access. Also works with async rsp. (initiative w/ rsp)

Can do parallel operations. Can put block and replace parts of resource. Not allowed in HTTP.

Block can be used on either PUT/POST or GET. Currently no response bodies to PUT/POST. Want it on both. Enable payloads with 2.05 only now but also allow 2.04, 2.01 and a generic 2.00 OK for generic rsp.

Clean up block options – make block option 1 and block option 2. New numbers for B1 and B2, retire old block option.

LT: Didn't see strong use case for large response to put and post.

CB: Use cases come in from POST. General catch-all method used in many applications. SOAP on COAP e.g.

LT: Is it possible it has to wait for all blocks and then send all blocks, or could it be pipelined?

CB: See it as a clean up.

LT: Clean-up means we have two options?

CB: Yes

AC: In current understanding, request can be pipelines?

CB: Yes can have multiple outstanding requests. When request block, in response can understand in the same resource? Is it therefore not possible to pipeline requests before receiving the whole response?

ZS: If 4k in size, could ask for partial representation.

CB: If you read beyond, will get an error. Block 1 for request, Block 2 for response

14:02 Observe

draft-ietf-core-observe-02 (Hartke 25 minutes)

(CB presents)

Discussion needed re. server-side state needed. Per-observation relationship IP address + port, Token and Lifetime running down.

So one client may have a large no. of relationships with one server. Can we get rid of some of this state? Ensure state doesn't last forever, which is why there is a lifetime. But not many use cases for this.

Node can terminate when a CON to client gets a RST, node unreachable, error on server side (no more events), re-install or remove observe relationship

Change lifetime to observer. Simplifying the protocol. Lifetime was used to detect reordering, so timer used as a sequence number. Can we do a single per-server counter? Yes, roughly seconds. Sequence number arithmetic. No potential for reordering between wraps. No need to compare

JT. What happens if the server reboots? If it has a wallclock and loses all state it could look odd from ordering.

CB: Would also lose the observation relationship. Client would have to install a new relationship with new token. Keep alive mechanism – well known problem. Used to ensure that TCP connections can be assumed to be dead. Would be nice for server to know a client is not there. Client is also interested to ensure server is still there, so both ends. Removing lifetimes has removed frame of reference for keep-alives. When does a server start sending GC messages? Would a day be about right?

Jabber: How does the client determine a relationship has ended?

CB: A client does have to talk to the server – and a keep alive would do this.

AC: If server is sending notification in NON messages, if a client has rebooted, can I drop observation as I can't respond to a NON?

CB: No, we can't do this. Would have to wait for a CON. A little bit strange

KL: Can we simplify the counters. Milliseconds could be better.

CB: What's complex is the amount of explanation. Code is easy – subtract two 16 bit numbers. Point to seq. no. arithmetic RFC.

14:15: CoAP Security (Shelby, Garcia 20 min)

How will draft-ietf-core-coap satisfy BCP 61?

Good background in draft-garcia-core-security-01

'Thing' lifecycle

Important to think about bootstrapping

Configuration entity for bootstrapping. Section 6 has a number of considerations

BCP 61 must be satisfied

Assume we put all the DTLS must-implement in.

What's missing? Key management in PSK mode. How do we get the keys there? Must work on 10/100 devices

Must be interoperable – must implement must work

One or more keys to use with DTLS.

Mother-duckling – imprint the key in close proximity (key in the clear)

Need security manager

Imprint on two devices by TC sending keys to both devices

HT: Network Access is different but then mentioning security bootstrapping mechanism. They don't talk about imprint PSKs but instead using certificates. How does it work?

CB: Try to bootstrap – no security, no keying material to a situation where we have some. There has to be a phase. Something else that there is some clear trust between the new node and the system you are trying to get into. Then use this as the imprint key. This can be used as shared secret.

CJ: Picture is too vague – we need help

BM – use DH in a closed environment. Can use that to establish keys. A HIP mode assumes use of this. OK if no MitM.

EKR: A Device is stupid – how do you get from pt A to pt B. As new devices come on, need to add keys. Mesh needs sharing. Mentioned

RC: app layer security and network access are distinct

HT: Key distribution model may be simplistic. Prior constraints need to be considered. Can't just use a random node on the internet as it doesn't scale. Use OAuth and shared secret for sensor talking to Facebook.

BM: Two basic modes. Third party, cert. based or Kerberos or private. Always a third party, even if that is the person doing it. Over simplifying it.

CB: Trying to install a node without a hammer.

RC: could use certificates

CB: That's a hammer

RC: A third party distributing keys could be a hammer

14:50 Discovery (Bormann/Brandt 20 min)

draft-bormann-core-simple-server-discovery-00

draft-brandt-coap-subnet-discovery-00

(Carsten Bormann presents)

CoAP server discovery process. CSDS on a server. How to find a CSDS – use ABRO. Could use additional ND options. Could use DHCP options

(Anders Brandt presents)

May end up with MAC/PHYs in different subnets. CoAP assumes single subnet. How to get across multiple subnets.

Adding a second router – it must happen magically! Remote control in one subnet must be able to control nodes in another subnet. Client may be anywhere, therefore disc. may traverse several subnets. Zeroconfig LLN subnet prefix (ULA).

Avoid LLN multicast, support sleeping nodes and limiting LLN traffic

Use CoAP Link formats

Filtered requests

No aggregation in a single gateway

Build up picture distributed over several units

Backdoor for gateways for legacy devices

IETF-80 CoRE WG Session 2

rahman-core-groupcomm-04 (Akbar Rahman)

Akbar: Added security considerations after Beijing
- IETF MSEC use discussion
- IRTF SAMRG
- Presented new security requirements

Don Sturek: Asked about REQ2/3 and group authentication.
Akbar: This is covered by REQ3.

Akbar: Not necessarily all requirements are needed for all deployments.

Bob: Take a look at 802.1ae, it has a good architectural model for group key management

Dirk: Are you doing single-source multicast? Should this be mentioned in the draft.
Akbar: Presented the figure on slide 135

Zach: Draft currently concentrates on HTTP-CoAP multicast mapping, would be good to concentrate on
normal CoAP multicast interaction.
Akbar: OK, will do that in the next version.

Akbar: How should we collaborate with other work in the WG.
Carsten: Would be a good idea to synchronize with the HTTP mapping work.

draft-vanderstok-core-bc-03 (Peter Van der Stok)

Peter: Group and multicast issues.

Peter: How to access legacy requirements.
- Gateway provides URIs for accessing legacy protocols

Peter: Use of DNS-SD in building automation
- Centralized

Zach: I don't understand the use of schema== in the TXT record, shouldn't that be path?
Peter: This is meant to indicate the type of legacy service.
Zach: That should probably be path= and rt= for example.

Don: Why did you put __coap in the sub-type?
Peter: To be conformant with DNS-SD...

Zach: We should work together to synchronize this with link-format.
Peter: OK

Carsten presents slide about CoAP-HTTP mapping

Carsten: Charter says we will define a mapping from CoAP to an HTTP REST API.
- Not clear what direction that is, probably we should do both.
- This should be generic, not for a specific application or non-rest, but for REST use.

Salvatore: We need more detail about the mapping as well.
Carsten: Yes, we need the minimal standards text in coap and a separate informational document.

Peter: Not sure if "mapping to an HTTP API" requires us to do a protocol interworking mapping.
Salvatore: We could consider it a CoAP to RESTful HTTP mapping.

Carsten: Now let's have presentations from Klaus and Angelo and get back to the discussion.

draft-hartke-core-coap-http-00 (Klaus)
draft-castellani-core-http-coap-mapping-01 (Angelo)

Klaus first presented his slides:

Kerry: In a forward mapping how do you know where the proxy is?
Carsten: The client must be specified to use the proxy.

Don: How does the HTTP client know how to handle a coap:// scheme.
Carsten: That is how a forward proxy works.

Robby: Noticed that CoAP doesn't support HEAD function. How does that work in a proxy?
Carsten: There are trivial solutions to that in the proxy [missed the solution].

[missed a bunch of discussion while in the mic queue]

Angelo presented his draft:

Angelo: There is a third type of proxy, a transparent proxy.

Akbar: Have you looked at possible NAT issues affecting the proxy.
Angelo: Good idea, we will take a look at it.

Salvatore: Could the chair ask for a show of support for this draft.
Carsten: We have a good seeds for the parts of an informational draft that we could eventually
make into a WG document. Who has written or is planning to write a document on this?

Hands raised - Esko, Dorothy, Angelo, Klaus, Akbar, Angelo, Salvatore