T2TRG: Thing-to-Thing Research Group

T2TRG/OCF meeting
November 10, 2017, Singapore, SG

Chairs: Carsten Bormann & Ari Keränen

Note Well

- You may be recorded

- The IPR guidelines of the IETF apply:
  see **http://irtf.org/ipr** for details.

Administrivia (I)

- Pink Sheet
- Note-Takers
- Off-site (Jabber, Hangout?)
  - **xmpp:t2trg@jabber.ietf.org?join**
- Mailing List: **t2trg@irtf.org** — subscribe at: **https://www.ietf.org/mailman/listinfo/t2trg**
- Repo: **https://github.com/t2trg/2017-11-ocf**

Agenda (1)

Time	Topic	Who
8:00	Welcome and intro	Chairs
8:10	IoT at IETF/IRTF; status update and direction	Chairs
8:35	OCF status update and direction	Mark Trayer
9:00	Security	Chairs/Phil Hawkes
	— Object Security (OSCON, OSCOAP, OSCORE)	Francesca Palombini
	— Enabling end-to-end security	FP, Dave Thaler
	— Protecting the network, MUD	Eliot Lear
	— Using IETF ACE components in OCF?	Hannes Tschofenig
9:40	RESTful Interaction, links, forms	Chairs / Mark Trayer
	— synergy with IETF CoRE links work	Michael Koster
	— atomic measurements, batch interfaces	Herve Jourdain
	— CORAL and HSML	TBD/Chairs
10:15	Break	

Agenda (2)

10:35	Ubiquitous Discovery and Connectivity	
	— Use of RD to discover devices in a mesh (across a Border Router)	Mark Trayer
	— Cloud Strategy (IETF view), edge computing, big Internet	Chairs / Jieun Keum
	— IETF view on use of CoAP Native to Cloud etc	Chairs / Jieun Keum
	— IoT NAT traversal	Christer Holmberg
11:15	Progress of dependent work in the IETF	Chairs / Richard Bardini
	— CoAP over TCP	Carsten Bormann
	— CoAP URIs, coap-at://, protocol negotiation?	Jaime Jimenez
	— CoAP Pub-Sub, YANG Push/telemetry in COMI	Michael Koster/Henk Birkholz
	— Resource directory, links	TBD/Chairs
	— Review pipeline from OneIOTA.org to IETF IoT reviewers	Clarke Stevens
11:45	Closing recap and summary of next steps	(All)
12:05	Meeting ends. Lunch(*).	

16 agenda items in 160 min?

- Tasting menu!
  - We can spend more time where we find interest, less time on where things seem to be clear
- Some items are mostly reminders that we may need to be mutually aware about plans and objectives
- Can go into more detailed discussion offline once we know who the right people are for that

T2TRG scope & goals

- Open research issues in turning a true "Internet of Things" into reality
  - Internet where low-resource nodes ("things", "constrained nodes") can communicate among themselves and with the wider Internet
- Focus on issues with opportunities for IETF standardization
  - Start at the IP adaptation layer
  - End at the application layer with architectures and APIs for communicating and making data and management functions, including security

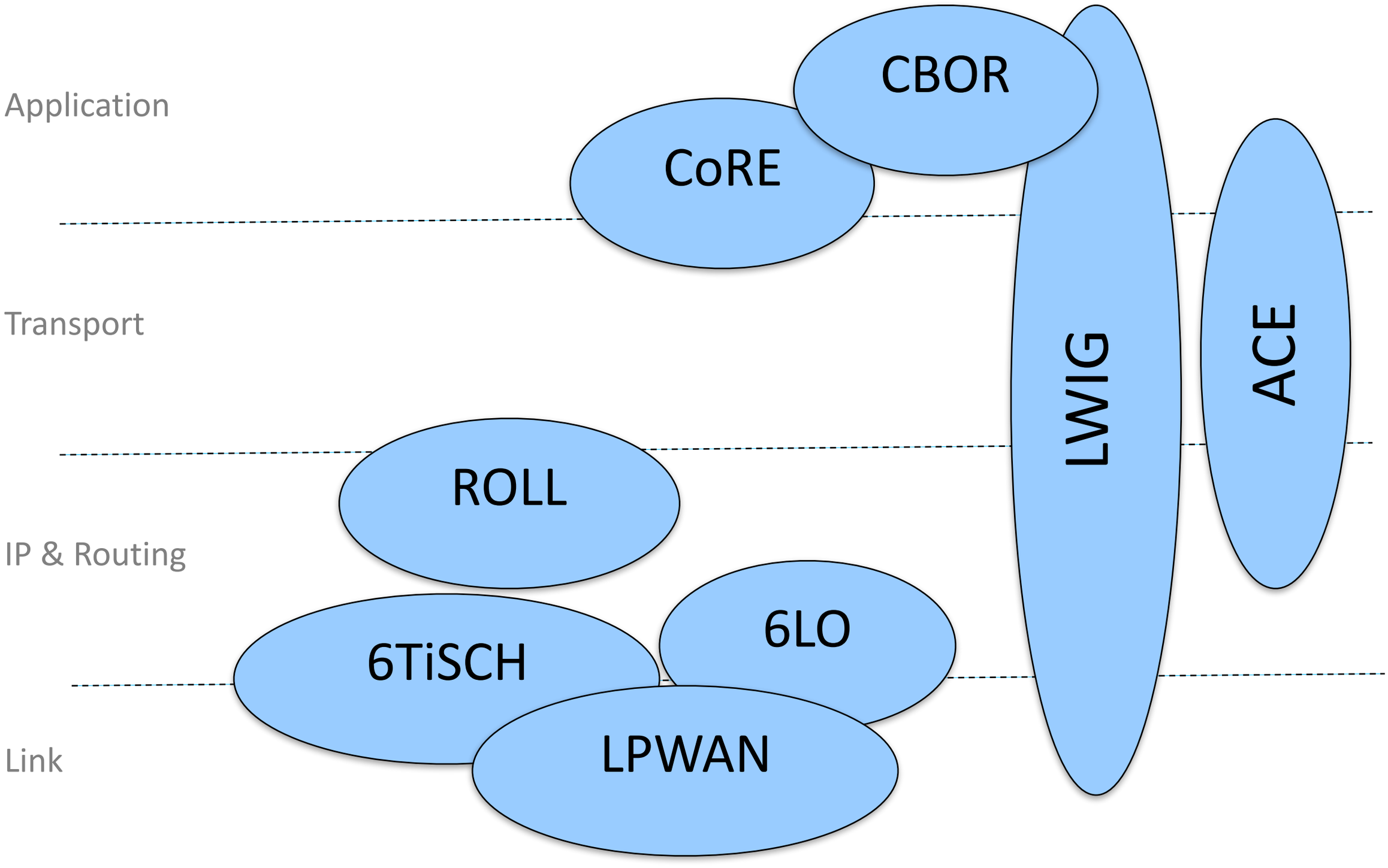
IoT @ IETF/IRTF

Status update and directions

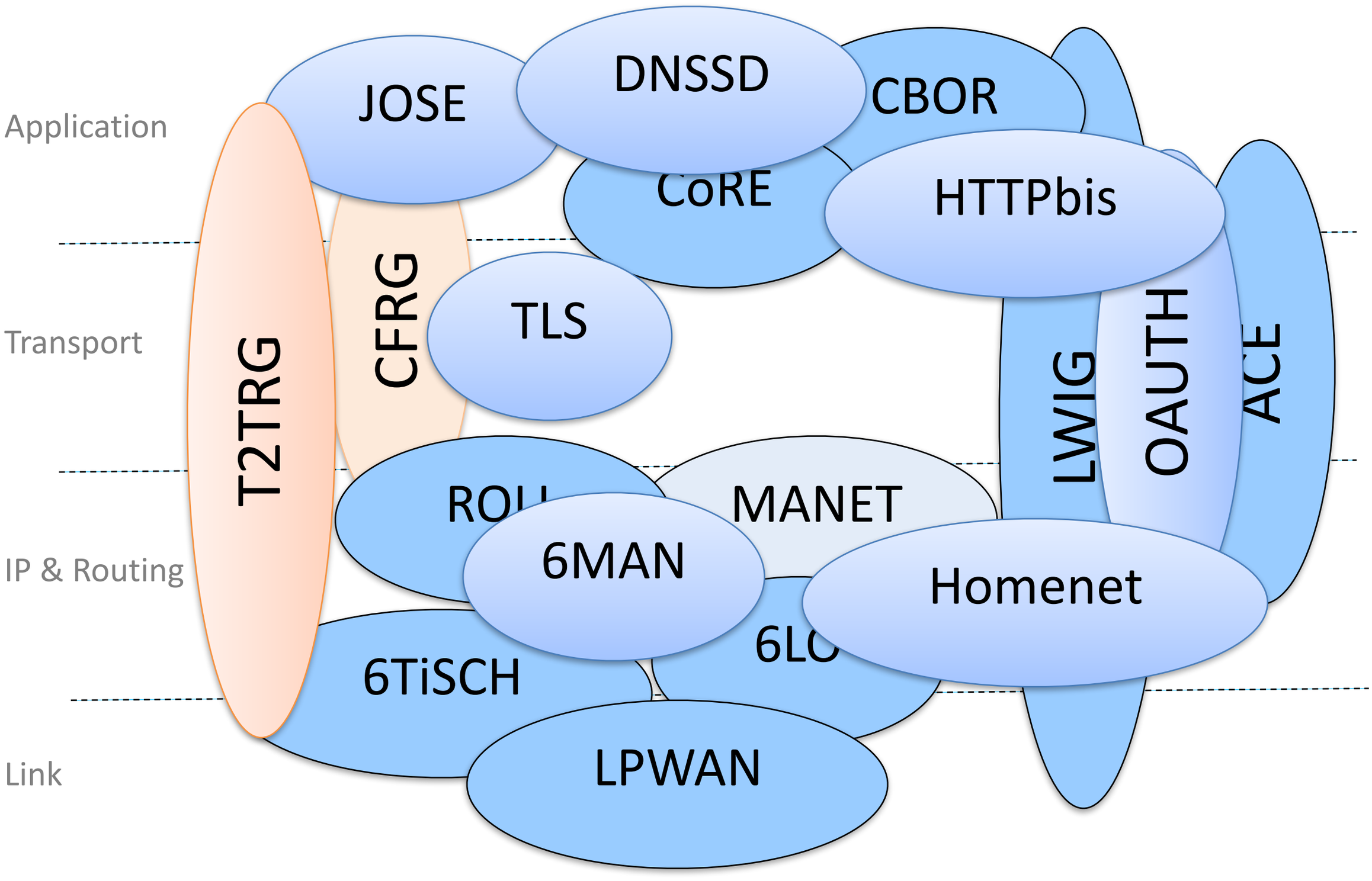
Recent Highlights

- Active work in semantic interoperability, data formats, and other “upper layer technologies”
  - T2TRG WISHI: Work(shop) on IoT Semantic/ Hypermedia Interoperability
- New IoT security related groups
  - Software Updates for Internet of Things (SUIT)
  - Trusted Execution Environment Provisioning (TEEP)

Primary Working Groups



Supporting Working/Research Groups



Constrained RESTful Environments

- CoRE WG is "providing a framework for resource-oriented applications intended to run on constrained IP networks"
- CoAP over TCP/TLS in final stages of IESG review
- SenML ready to publish
- OSCORE (OSCOAP) going for WG last call
- Finalizing Resource Directory
- CoAP pub/sub broker maturing
- CoMI work maturing
- New work on echo/request tag for attack mitigation
- Many drafts in the pipeline…

IPv6 over Networks of Resource-constrained Nodes

- 6lo WG is focusing on running IPv6 in IoT networks
- 6lo Neighbor Discovery (ND) improvements
  - 6LoWPAN ND update in WG last call
  - Securing ownership draft
  - Backbone router usage draft
- Bluetooth mesh, NFC, and WBAN work

IPv6 over the TSCH mode of IEEE 802.15.4e

- 6TiSCH WG is working on enabling IPv6 for the Timeslotted Channel Hopping (TSCH) mode of 802.15.4
- 6top protocol (enabling distributed scheduling in 6TiSCH networks) to IESG review
- Work on security framework and ACE use
- Architecture/terminology work ongoing

IPv6 Over Low-Power Wide Area Networks

- Enabling IPv6 connectivity for LPWANs and technologies to secure the operations and manage the devices and their gateways
- Overview document submitted to IESG
- Getting ready to ship IPv6 UDP compression and fragmentation (SCHC)
  - Relevant beyond LPWANs
- Working on CoAP compression

Routing Over Low power and Lossy networks

- The ROLL WG is focusing on routing issues with Low power and Lossy Networks
- “AODV-RPL use” and “updated use cases” in last call

Authentication and Authorization for Constrained Environments

- ACE WG is defining solutions for authentication and authorization to enable authorized access to resources hosted on resource servers in constrained environments
- Authentication/authorization framework
  - Profiles: OSCOAP, DTLS, (IPsec), …
- CBOR Web Tokens in second WGLC
- CWT proof of possession

Light-Weight Implementation Guidance

- LWIG WG is providing guidance on how to implement Internet technologies on the constrained devices
  - CoAP and TCP implementation guidance
  - Neighbor management policy
  - Updated version of “Terminology for Constrained-Node Networks”

Thing-to-Thing Research Group

- IRTF group investigating open research issues at IoT
- “State-of-the-Art and Challenges for the IoT Security” getting ready to publish
- “RESTful Design for IoT” adopted
- Work(shop) on IoT Semantic/Hypermedia Interoperability
- Edge computing for IoT on agenda

Object Security, OSCORE, e2e sec

Protecting the network, MUD

Security Workflows

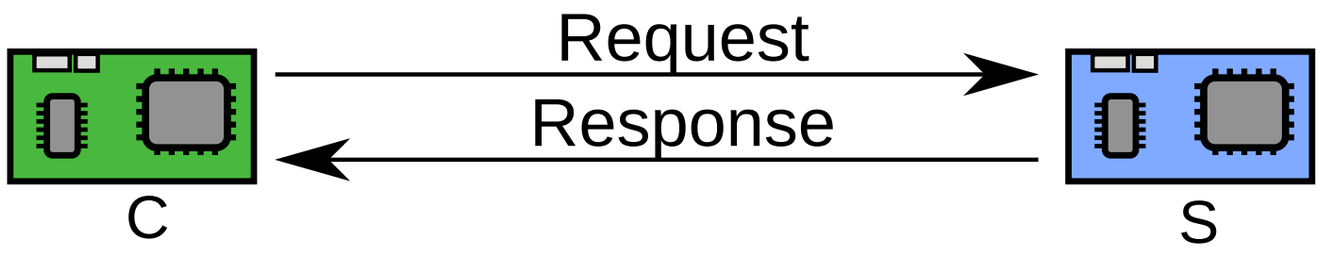
Using ACE in OCF?

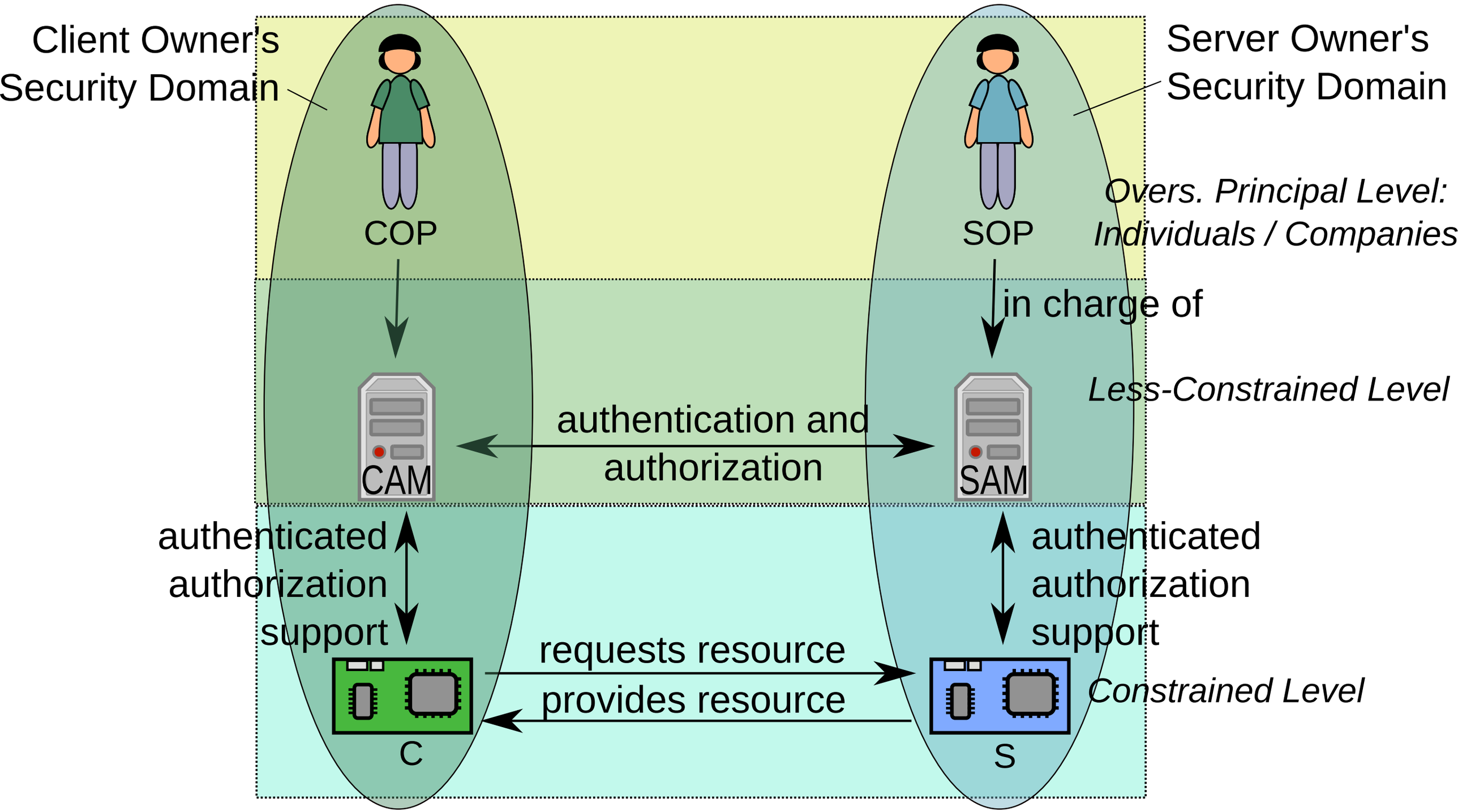
Protect the objectives right ✔

vs.

Protect the right objectives 

Now let's apply all this to constrained devices




Client Owner's
Security Domain
Server Owner's
Security Domain
COP
SOP
Overs. Principal Level:
Individuals / Companies
in charge of
Less-Constrained Level
CAM
authentication and
authorization
SAM
authenticated
authorization
support
authenticated
authorization
support
requests resource
provides resource
Constrained Level
C
S

Shaping the Security Workflows

- Stakeholders, Principals
- Less-constrained nodes
- Constrained nodes
- Device Lifecycle
- Authorized, authenticated delegation

2014-05-05: ACE

- “Authentication and Authorization for Constrained Environments”

  - currently applying OAuth framework to IoT

RESTful Interaction, links, forms

Cloud strategy, Edge Computing, DINRG

CoAP native to cloud?

Types of access

- Regular “Telemetry” (cf. pubsub/telemetry slot)
  - CoAP has observe
    - Build on that?
- Configuration settings; special state requests
  - REST fits perfectly

Call-home vs. Client-Server

- CoAP generally assumes connectivity
  - Problems that can be solved at the IP layer are also solved there
- Great for IoT-focused networks, not so great for IoT add-ons to brownfield
  - Middleboxes ➔ traversal issues
  - CoAP-over-TCP, Thin ICE, …

Rendezvous problem

- How do parties that want to talk, find each other
- Classical solution: DNS (dynamic DNS)
  - Often not acceptable for privacy reasons
- Resource directory is another way
- “finding” now also includes finding and setting up information about and for authorization
- Do we need to do more in this space?

Who has the onus to re-rendezvous?

- Observe: Client!
  - No way for server to act on known connectivity changes
- Pubsub: Both publisher (server) and subscriber (client), but not broker
  - Assumption: broker is a rock in the surf

CoAP over TCP

Draft-ietf-core-tcp-tls-10

- Should now cover all IESG comments
  - Waiting for DISCUSS to clear
- Now implemented in libcoap master:
  - https://github.com/obgm/libcoap/pull/113
  - Possibly get some interop testing going tomorrow

Closing recap and summary of next steps