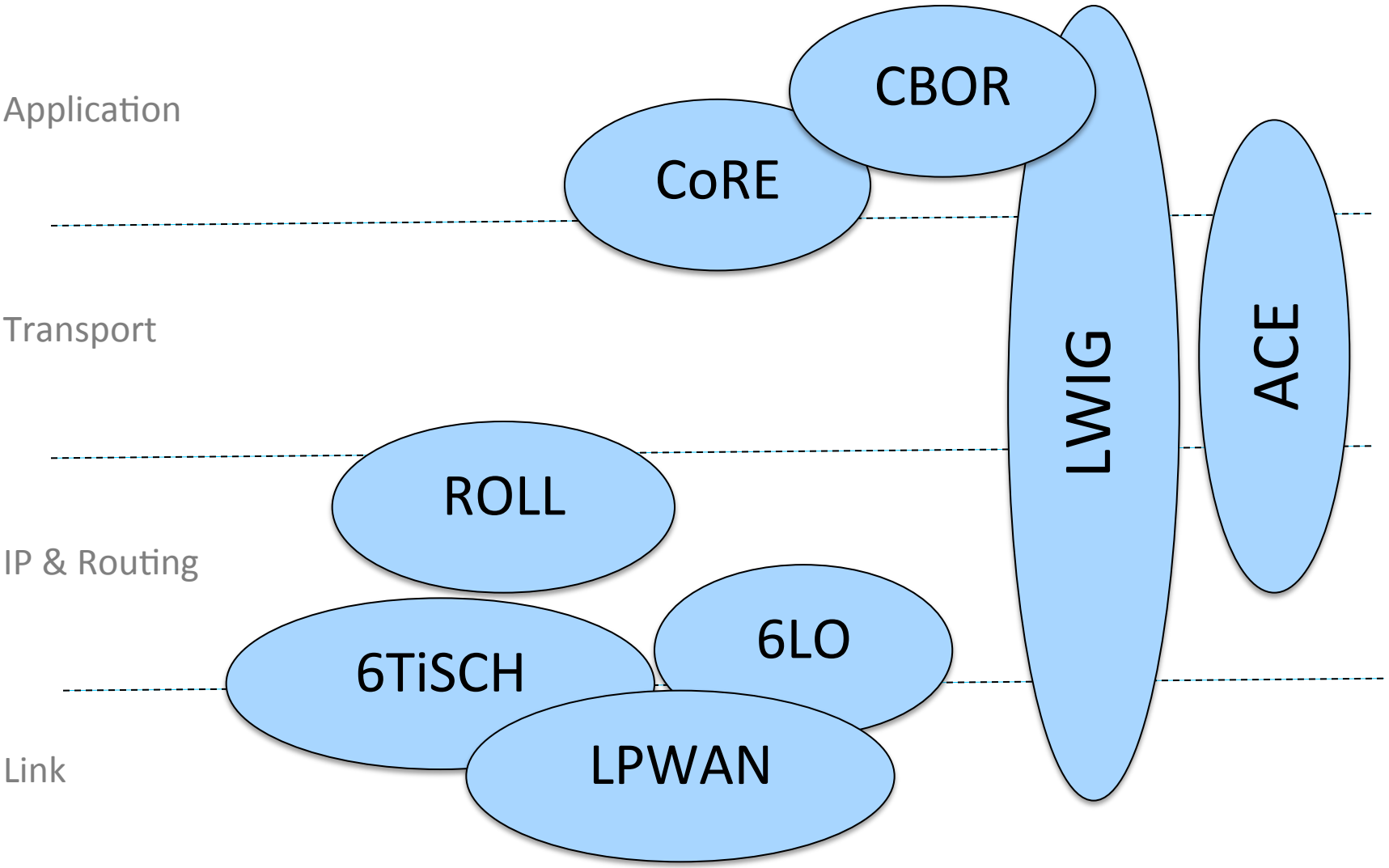
IoT @ IETF

Ari Keränen
ari.keranen@ericsson.com
10.3.2017

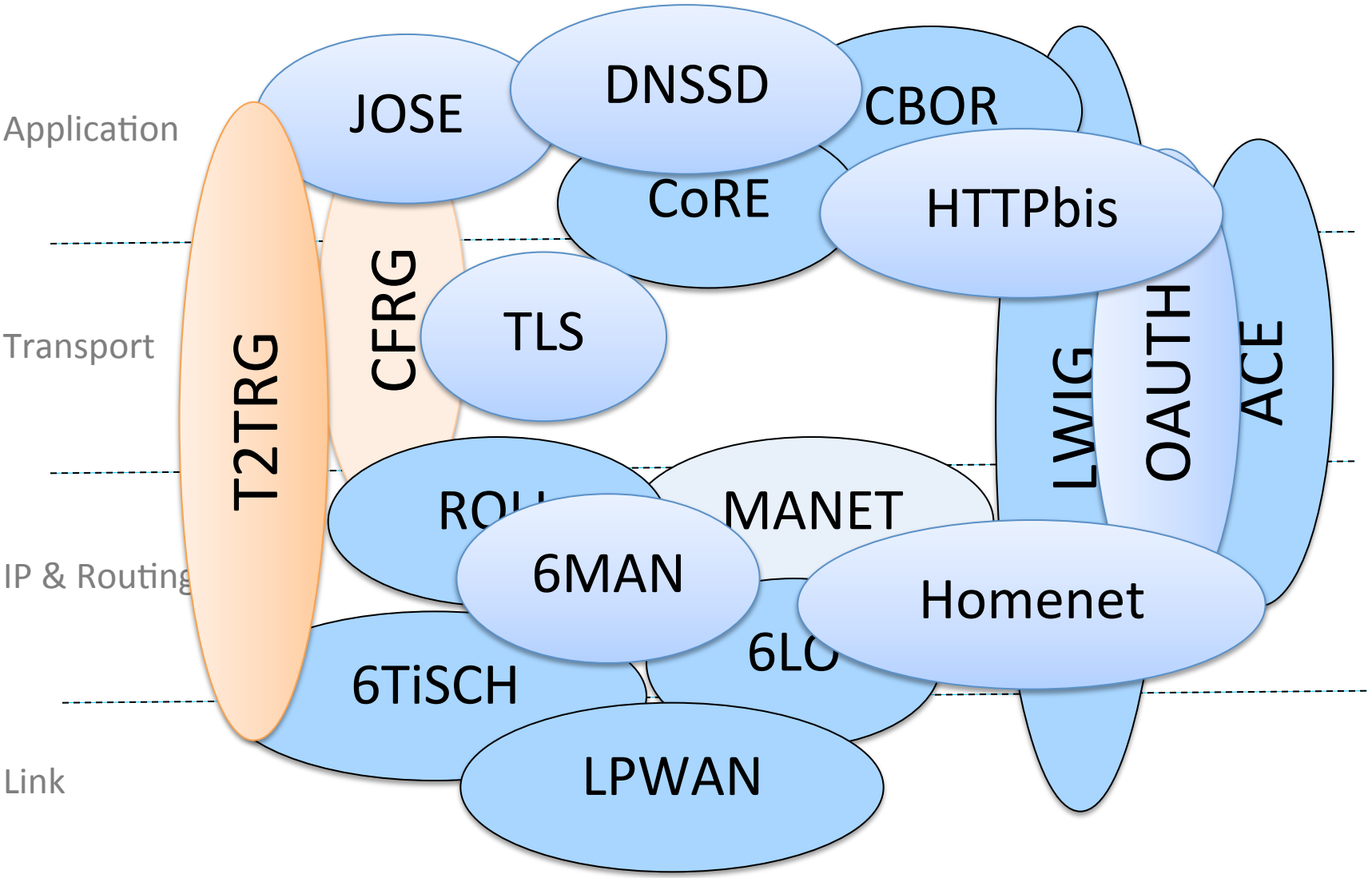
Recent Highlights

- Web protocol stack evolution. Improvements likely to be broadly used in IoT space
- Increased/recent interest
  - Advanced security
  - 6LowPAN on various link types
  - Data formats
  - Semantic interoperability
- IETF IoT Directorate for coordination
- Thing-to-Thing Research Group (T2TRG) for long-term search topics
- New Low-Power Wide Area Networks (LPWAN) and CBOR working groups

Primary Working Groups



Supporting Working/Research Groups



Constrained RESTful Environments

- Framework for resource-oriented applications intended to run on constrained IP networks
- "CoRE Link Format" (RFC 6690)
- "Constrained Application Protocol (CoAP)" (RFC 7252)
- "Observing Resources in CoAP" (RFC 7641)
- "Block-Wise Transfers in CoAP" (RFC 7959)
- "Guidelines for HTTP-CoAP mapping" (RFC 8075)
- "Patch and Fetch Methods for CoAP" (to be published)
- Working on finalizing Resource Directory, CoRE interfaces, CoAP over TLS/TCP, JSON/CBOR web links, Management over CoAP, SenML, Object Security, …

Constrained RESTful Environments

- Re-chartered April 2016; including new topics
  - RESTCONF style management
  - Sensor Measurement Lists (SenML)
  - Publish-Subscribe Broker for CoAP
  - Object Security for CoAP
- Many additional Internet Drafts for proposals of new work in various topics
  - Congestion control
  - Security
  - Management
  - CoAP over different transports
  - …

Concise Binary Object Representation (CBOR) Maintenance and Extensions

- CBOR (RFC 7049) extends JSON to include binary data and extensibility model. Uses compact binary representation format.
- CBOR WG Chartered January 2017
- WG is updating RFC 7049, completing CBOR Data Definition Language (CDDL) spec, and exploring use of CBOR extension for tagging of Typed Arrays and OIDs/UUIDs

IPv6 over Networks of Resource-constrained Nodes

- IPv6 in IoT networks ("v6 over foo")
- "IPv6 over BLUETOOTH(R) Low Energy" (RFC 7668)
- "Transmission of IPv6 Packets over ITU-T G.9959 Networks" (RFC 7428)
- "Generic header compression" (RFC 7400)
- Active drafts for adaption layers for DECT ULE, MS/TP (Master-Slave/Token-Passing), NFC, and RFID
- Also privacy and security work, proposal for BLE Mesh

IPv6 over the TSCH mode of IEEE 802.15.4e

- IPv6 for the Timeslotted Channel Hopping (TSCH) mode of 802.15.4
- Overview and problem statement (RFC 7554)
- WG docs: architecture, terminology, configuration interface, CoAP bindings, security

IPv6 over Low-Power Wide Area Networks

- LPWAN WG chartered in October 2016
- Enabling IPv6 connectivity for LPWANs (SIGFOX, LoRa, WI-SUN, NB-IOT) and technologies to secure the operations and manage the devices and their gateways
- WG docs: overview and enabling compression of CoAP & UDP/IPv6 packets over LPWANs

Routing Over Low power and Lossy networks

- ROLL WG: routing issues with Low power and Lossy Networks
- 18 published RFCs since 2009
  - Requirements for various use cases
  - Routing protocol “RPL” and related extensions
  - Terminology
  - Security threat analysis
  - Multicast
  - Applicability statements
- Remaining work items on routing extensions

Authentication and Authorization for Constrained Environments

- Solutions for authentication and authorization to enable authorized access to resources hosted on resource servers in constrained environments
- "Use Cases for Authentication and Authorization in Constrained Environments" (RFC 7744) in 2016
- WG docs: Architecture, OAuth based authorization, compact web tokens

CBOR Object Signing and Encryption

- COSE WG: Object security for IoT (concluded)
- Based on **JOSE**: JSON Web Token, JWS, JWE, …
  - Data structures for signatures, integrity, encryption…
  - Derived from on OAuth JWT
  - Encoded in JSON, can encrypt/sign other data
- **COSE: use CBOR instead of JSON**
  - Can directly use binary encoding (no base64)
  - Optimized for constrained devices

CWT: CBOR Web Token

- Data Structure for "Claim Sets"
  - modeled after JWT (RFC 7519)
  - signed or MACed, encrypted using COSE
- Can replace unstructured misuse of certificates for claim sets
- Being completed in IETF ACE WG

Light-Weight Implementation Guidance

- How to implement Internet technologies on the constrained devices
- "Terminology for Constrained-Node Networks" (RFC 7228)
- "Minimal IKEv2 Implementation" (RFC 7815)
- WG docs: experiences in securing smart object networks, using CoAP with cellular networks, energy efficient protocol operations

Constrained Management work

- Two RFCs on "Management of Networks with Constrained Devices" published in May 2015 by Operations and Management Area Working Group
- OMA Light-weight M2M protocol (LWM2M) uses CoAP
- RESTCONF style management (CoMI) in CoRE

Thing-to-Thing Research Group

- IRTF group investigating IoT open research issues
  - Potential for future standardization work at the IETF
  - Scope: IP adaption layer to application layer with architectures and APIs that enable communication, data, management, and security functionality
  - Initial topics: security and RESTful system design
- Close collaboration with W3C WoT group
- Outreach to other organizations (OCF, Bluetooth SIG, open source communities, etc.)

IETF IoT Directorate

- Formed in 2014; re-chartered late 2016
- Coordination between working groups
- Reviews for IoT-related specifications
- Focal point for external organizations

Other

- "Architectural Considerations in Smart Object Networking" (RFC 7452) published by IAB in March 2015
- IoT actively discussed in IETF plenaries, various IETF/IAB workshops, and other working groups
  - JOSE WG: security for JSON (often used with CoAP)
  - OAuth: ACE adopted similar model for authentication
  - HTTPbis: HTTP/2 is more suitable for IoT than earlier versions
  - TLS: CoAP uses (D)TLS for security
  - Homenet: IoT devices are often part of a home network
  - ANIMA: self-managing networks are relevant for IoT
  - ICNRG: lots of discussion on how to apply ICN for IoT
  - ...
- Other already concluded groups (6LoWPAN, DICE)
- Recently security for IoT has got a lot of attention; visible across working groups and all discussions
- IoT Semantic Interoperability WS in March 2016
- IoT Software Update WS in June 2016