IETF protocol suite for the Internet of Things: Overview and Recent Advancements

Roberto Morabito∗†, Jaime Jiménez∗
∗Ericsson Research, Finland
†Princeton University, USA
{roberto.morabito, jaime.jimenez}@ericsson.com

Abstract—Internet of Things (IoT) is a rapidly growing technological domain and the effort that many Standards Developing Organizations (SDOs) and alliances are dedicating to it is constantly increasing. The Internet Engineering Task Force (IETF) is certainly one of the most active SDOs operating in this broad domain. With the aim of building a comprehensive, interoperable and streamlined IoT stack, several IETF working groups are developing protocols, in multiple technological domains, which are already nowadays very relevant to the IoT. This article gives a concise but comprehensive survey of the IETF efforts in the IoT. We discuss mainstream standardization and research activities, as well as other IETF-connected supporting initiatives provided still in the context of IoT.

I. INTRODUCTION

In the last two decades, the Internet of Things (IoT) became a significant research and development opportunity for industry, academia, and SDOs [1]. Simplifying its definition in non-rigorous terms, IoT refers to the usage of Internet protocols for enabling communication from "things" towards humans, between "things" or more complex Internet-based infrastructures. A key aspect of the IoT is the possibility of using Internet protocol technologies on constrained devices such as sensors and actuators. Namely, devices characterized by very limited computational capabilities and that e.g. are featuring between 100 and 250 KiB in terms of max code complexity, or between 10 and 50 KiB in RAM, as well as limited resources in battery, bandwidth or connectivity [2].

However, the integration of the well-known TCP/IP Internet protocol suite [3] on top of constrained devices generates several challenges, since such protocols were not originally designed to operate with this type of nodes. For example, the design guidelines followed for such protocols – originally defined for the Web – may not always be suitable for constrained network environments, in which nodes are limited in CPU, memory, and the networks are often characterized by high packet loss, low throughput, frequent topology changes and small useful payload sizes [4].

The Internet Engineering Task Force (IETF) has been since long on the front line to allow overcoming such challenges, by leading the standardization of Internet communication protocols suitable for resource constrained devices and networks. Where possible, the IETF aims to make existing Internet protocols suitable for IoT scenarios, by providing minor tweaking on their original characterization and by taking into account the different requirements. In other cases, significant gains can only be achieved by defining new protocols.

The authors would like to thank the Ericsson colleagues, Carsten Bormann, and Emmanuel Baccelli who provided helpful feedback and insightful comments on the paper.

Another key guideline followed by IETF in IoT-oriented standardization activities is the possibility of enabling a wide range of things to use interoperable technologies for communicating with each other – in this regard, "things" can range from embedded sensors to complex machinery (e.g., a car) or even large infrastructure (e.g. a bridge). As evidence of this demanded IoT interoperability, Figure 1 shows how an IoT stack deployable nowadays on constrained devices can include several IETF standards (defined for the IoT context and beyond), as well as Non-IETF standards.

![Fig. 1: An example of IoT device stack comprising a mix of IETF and Non-IETF standards.](image-url)

The above-depicted IoT stack represents just one possible example of an IoT device stack. It could easily comprise many other additional protocols, including the ones that were not originally designed for IoT or in IETF, which are now widely used in this context – e.g., the ISO standard Message Queue Telemetry Transport (MQTT) or the IETF standard HTTP. This is mainly caused by the fact that the IoT lends itself to a significant and varied number of definitions, design visions, and deployments [5].

However, since we focus on IETF and on its activities in the constrained IoT area, we rely on the vision and definition that IETF itself provides about IoT in [6]:

"The Internet of Things (IoT) refers to devices, that are often constrained in communication and computation capabilities, now becoming more commonly connected to the Internet, and to various services that are built on top of the capabilities these devices jointly provide. It is expected that this development will usher in more machine-to-machine communication using the Internet with no human user actively involved".

IETF activities are also supplemented by the Internet Re-
search Task Force (IRTF). While the first one focuses on the shorter term matters of the Internet engineering and standards making, the second one works on longer term subjects with a clear research-oriented approach.

Figure 2 illustrates different Internet-related technological meta-domains, whose development is extensively enhanced by IETF and IRTF. In the map, we identify four main areas (i.e. Connectivity, Routing, Application, Security) with which can be mapped a substantial number of IETF working groups characterized by a clear IoT scope. Additionally, several other working and research groups can somehow be classified as IoT-related, although characterized by a different general purpose. We map these additional working groups to two specific categories – Experimental & Use Cases and Infrastructures.

Fig. 2: IETF Working groups operating in the IoT classified in meta-domains.

The remainder of this article focuses on analyzing what are the leading IETF and IRTF activities currently oriented towards the IoT in the technical domains introduced above, and it is organized as follows. We first focus on the connectivity and routing aspects. Afterwards, application and security areas are reviewed and discussed, respectively. Following, we overview ongoing standardization efforts relating to experimental activities, use cases, and infrastructures. Before the conclusion are given, we also introduce what are the other committees and organizations established to work along the conclusion are given, we also introduce what are the other committees and organizations established to work along the meta-domains.

II. CONNECTIVITY & ROUTING

The IETF’s work on IoT has started by bringing connectivity to the constrained space, already at the turning of this century. At that time, there were already different Wireless Sensor Networks (WSNs) proposals that were not making use of standard IETF network protocols. However, the work for connecting constrained devices to the Internet by enabling IPv6 addressing on them has represented one of the first step towards the IoT.

A. CONNECTIVITY

**6LoWPAN** — The IPv6 over Low power WPAN (6LoWPAN) WG has operated from March 2005 to January 2014. The group produced several RFCs covering application scenarios and use cases for Low-power Wireless Personal Area Networks (LoWPANs). At that time, most of the LoWPANs were usually characterized by proprietary networking mechanisms. Thus, the group purpose was to bring IP (IPv6 in particular) to the short range, low bit rate, low power radios – specifically, IEEE 802.15.4 [8]. Along with header compression, one of the big hurdles existing for enabling such integration was due to the mismatch between the maximum frame size of 127 bytes and the Maximum Transmission Unit (MTU) of IPv6. This has led to the specification of an adaptation layer that provides fragmentation and reassembly, and allows to overcome the above mentioned problem. Table I shows three among the most representative RFCs produced in 6LoWPAN.

**6TiSCH** — The WG started in 2013 and still continues. It focuses on enabling IPv6 over the Time-Slotted Channel Hopping (TSCH) MAC mode of the IEEE802.15.4 standard. The TSCH WG brings to the IoT the possibility of time
TABLE I: Selection of relevant RFCs and I-Ds in the connectivity and routing domain.

| RFC/number and title | Description                  |
|----------------------|------------------------------|
| IPv6-6tisch          | Describes the minimal requirements for a device to join the aforementioned 6tISCH network securely. In this regard, it has prioritized the use of two CoRE WG’s specification: Constrained Application Protocol (CoAP) for the messaging and Object Security (OSCORE) to secure the communication. |
| 6LoWPAN              | Provides an overview of the latest low power wireless technologies, put together all the efforts made to compress protocol headers and extension headers. 6LoWPAN has produced guidelines for IPv6 over various constrained networks such as Bluetooth Low Energy (BLE), DUFT-T G.9959 networks, Digital Enhanced Cordless Telecommunications (DECT) Ultra Low Energy (ULE) or even over Master-Slave/Token-Passing (MS/TP) wired networks. The WG has also produced specifications and information for data models (e.g., MIBs for managing 6LoWPANs), adaptation layer extensions (e.g., Generic Header Compression for IPv6 over 6LoWPANs), as well as other maintenance documents such as new IEEE Ethertype assignments, RFC updates or informational RFCs on privacy considerations. The group is still active, working on bringing IPv6 to other networks such as Near Field Communication (NFC). |
| LPWAN                | The WG focuses on enabling IPv6 connectivity over multiple Low Power Wide-Area Network (LPWAN). LPWANs devices possess large coverage at the cost of substantially lower bandwidth (e.g., order of hundreds of millibits per second [9]) and reduced duty cycle. The group has selected four LPWANs to work on: Long Range (LoRa), Wireless Smart Utility Networks (Wi-SUN), Narrowband IoT (NB-IoT), and Sigfox. The WG started its work in 2016 and has completed an overview document specification of their selected LPWAN technologies. LPWAN current main focus is on LPWAN Static Context Header Compression (SCHC) for CoAP and for UDP (Table I). |
| B. Routing           | The Routing Over Low-power and Lossy networks (ROLL) WG focuses on routing solutions, targeting specific deployment environments such as connected home, building, and urban sensor networks. The scope of ROLL has been re-defined several times. The main outcome of its earlier activities is the specifications of the IPv6 Routing Protocol for Low-Power and Lossy Networks (RPL) protocol (RFC 6550, described in Table I), an IPv6 Routing Protocol for Low-Power and Lossy Networks (LLNs) that takes into consideration various aspects including high reliability and connectivity while ensuring low resource utilization into the devices. More recently, the WG has kept maintaining and improving already developed protocols (e.g., RPL), as well as defining related extensions for routing metrics, objective functions, and multicast. Finally, the WG has also produced several documents concerning requirements and applicability statements for routing in LLNs, terminology, and security threat analysis. |

III. Application
In the application domain, there are currently three groups targeting the IoT context.

The Constrained RESTful Environments (CoRE) is one of the key WGs, also in view of its well-established activities started already in 2010. More recently, two additional groups have been chartered in the IoT application domain, namely the Thing-to-Thing (T2TRG) RG in 2015 and the Converse Binary Object Representation Maintenance and Extensions (CBOR) WG in 2017.

CoRE — The main goal of CoRE is to define mechanisms and frameworks that are suitable for resource-oriented applications, intended to run on constrained IP networks—i.e. networks characterized by operating constraints like those defined in ROLL and 6Lo. The Constrained Application Protocol
CoAP (which has been defined in RFC 7252), represents the foundation around which most of CoRE activities are developed [10]. CoAP is a UDP-based protocol that enables manipulation of resources hosted by devices and it is considered analogous to HTTP for constrained environments (although CoAP is designed for being used also in non-constrained IP networks). Based on CoAP specification, CoRE explores several additional areas (e.g., security, interoperability, data sensors representation, etc.), with the purpose of building a comprehensive and standard-compliant ecosystem around it. Table II summarizes some among the most relevant RFCs and I-Ds produced by the WG. Although CoAP was originally designed in order to operate over UDP and Datagram Transport Layer Security (DTLS), CoRE is committing to ensure a functional mapping of CoAP towards additional transport protocols and security mechanisms (e.g., TCP and TLS in RFC 8323), application protocols (e.g., HTTP in RFC 8075). Interoperability with non-IP networks and non-IETF standards and implementations also represents a key requirement. CoRE standards are used by other SDOs like OMA SpecWorks [11] which uses CoAP on its Lightweight M2M (LWM2M) IoT device management protocol.

CBOR — The WG has as its primary objective the maintenance of RFC 7049, which defines the Concise Binary Object Representation (CBOR) data format. Originally, CBOR was defined to make available the benefits that JavaScript Object Notation (JSON, RFC 7159) brings to the Web towards the constrained devices and today there is available a CBOR library in almost any programming language. CBOR includes binary data as well as an extensibility model, using a binary representation format that is easy to generate and parse.

However, in view of an increasing usage as a message format in other WGs (e.g., CORE, ANIMA GRASP), the group is aiming to revise its definition by taking into account the related security matters. The new CBOR definition will ensure backward compatibility, and it will be designed in such a way that a specific data definition language (CDDL, see Table II) provides a single description format to express CBOR and JSON encoded messages.

T2TRG — The WG investigates open research questions stemming from the use of well-established standards already defined in the scope of IoT-oriented IETF WGs. It additionally explores emerging opportunities and issues arising by new requirements of IoT infrastructures, which consequently exhibit standardization potential at the IETF. Although in this context the term "thing" often refers to constrained nodes, this RG targets IoT architectures where not all things are highly constrained. Leaving aside the nodes’ computational capabilities, it is assumed that devices can communicate among themselves and with the rest of the Internet.

T2TRG is a research-oriented group in which the topics explored vary considerably, ranging from the management and operation of constrained-node networks, security and lifecycle management, methods to use the REST paradigm in IoT scenarios, and semantic interoperability – to this extent, although we categorized this WG in the application meta-domain, a relevant part of the WG’s activities belong also to other domains. Table II describes a very limited part of the considerable documentation produced within the T2TRG.

Another relevant aspect characterizing T2TRG is interaction with other standardization bodies and consortia active in the IoT area. For example, with the W3C Web of Things (WoT) interest group [12] is explored how Web technologies can be harnessed in the future of IoT.

### IV. Security

**DICE** — Initiated in 2013, the DTLS In Constrained Environments (DICE) WG completed in 2016. DICE has been focusing on defining guidelines and mechanisms for the support of DTLS (RFC 6347) in the context of constrained environments (i.e. including constrained devices and constrained networks). Essentially, DICE provided a dedicated DTLS profile suitable for IoT applications (RFC 7925, Table III), where CoAP is assumed to be the main protocol used to manage such resources.

**ACE** — The main objective of the WG is the definition of authentication and authorization mechanisms suitable for resource access in constrained environments. Three-party authentication and authorization protocols previously defined in IETF (e.g., Public Key Infrastructure – PKI, Web Authorization Protocol – OAuth) are mostly suitable for non-constrained environments and do not consider additional requirements and limitations of typical IoT scenarios (for example, intermittent connectivity may reduce the possibility to contact an authorization server in real-time). Assuming that CoAP over DTLS is used to access resource-constrained servers, ACE seeks to assess the suitability of already existing protocols as baseline for the definition of its analogues in constrained environments.

### Table II: Selection of relevant RFCs and I-Ds in the application domain.

| RFC Number and Title | Description |
|----------------------|-------------|
| RFC 7252 CoAP        | Defines a protocol for transferring messages between CoAP nodes. The protocol is designed to operate over UDP and Datagram Transport Layer Security (DTLS). CoAP is intended to be used as a lightweight alternative to the Internet Protocol (IP). |
| RFC 6080 CoRE        | Defines the Concise Binary Object Representation (CBOR) data format, which allows for efficient transmission of data in a variety of environments, including constrained networking protocols. CBOR is designed to be compact and efficient, with a focus on binary data representation. |
| RFC 8323 CoAP        | Defines an abstract CoAP security framework that can be used by CoAP implementations to implement security mechanisms such as authentication and encryption. The security framework is designed to be flexible and extensible, allowing for the addition of new security protocols and mechanisms. |
| RFC 8428 CoAP        | Specifies the COSE (Constrained Object Signing and Encryption) algorithm suite, which is used for securing CoAP messages. COSE is designed to be lightweight and efficient, with a focus on providing security for CoAP messages in constrained environments. |

**CBOR** — The WG has as its primary objective the maintenance of RFC 7049, which defines the Concise Binary Object Representation (CBOR) data format. Originally, CBOR was defined to make available the benefits that JavaScript Object Notation (JSON, RFC 7159) brings to the Web towards the constrained devices and today there is available a CBOR library in almost any programming language. CBOR includes binary data as well as an extensibility model, using a binary representation format that is easy to generate and parse.

---

**Notes:**
- CBOR is designed for being used in constrained environments, and it is considered analogous to JSON.
- CoAP is used as a transport protocol for CoRE activities, allowing CoAP clients to be kept updated about the representation of a resource over a network.
- CBOR is designed for constrained environments and provides end-to-end security.
- CoRE is aimed at supporting the Internet of Things (IoT) by defining a comprehensive and standard-compliant ecosystem around it.
allowing however to understand which kind of contribution is produced by this WG. At the moment an OAuth-based framework with profiles for DTLS and OSCORE is nearing completion, while several related individual-submission I-Ds that address group communication are in the process of WG adoption.

**SUIT** — The Software Updates for Internet of Things (SUIT) WG was chartered at the end of 2017 with the goal to strengthen, from security perspective, software update mechanisms so as to mitigate potential attacks (e.g., Mirai DDOS attack in 2017). Specifically, the group aims to define a firmware update solution to be used even with Class 1 type of devices [2], i.e., devices with 10 KiB RAM and 10 KiB flash. The design of a manifest format that provides metadata about the firmware image is currently under development. The manifest also specifies pre- and post-conditions for the installation of the firmware as well as other parameters that need to be validated (e.g., hardware conditions, processor information, firmware makers, etc.).

**TEEP** — The Trusted Execution Environment Protocol (TEEP) WG was chartered in 2018. The WG operates in the context of a specific and highly secure area of modern devices’ processor, as well as all the Trusted Application (TA) components executed in it. In the TEEP WG are currently developed two drafts that provide an overview of the architecture and protocol specifics. Its architecture document presents the need for an interoperable protocol for managing TAs that run in different TEEs of various devices. The document also contains definitions of the parties involved in the protocol and the requirements when it comes to TEE attestation. The group may document several attestation technologies considering different hardware capabilities, performance, privacy, and operational properties.

**COSE** — The CBOR Object Signing and Encryption (COSE) WG was chartered in 2015, concluded in 2016, and re-chartered in 2019. The group makes use of CBOR for object signing and encryption formats. One motivation is to reuse the cryptographic keys, message authentication (MACs), encryption, and digital signatures that were done for JSON in the now concluded JOSE WG but this time in CBOR. CBOR has new capabilities that are not present in JSON, thus the intention was not to do a direct mapping from JSON to CBOR. For example as RFC 8152 mentions, COSE uses binary encoding for binary data rather than base64url, it also redefines the message structure for better identification and consistency. The group finalized the work, being that RFC 8152 the target set.

**LAKE** — The Lightweight Authenticated Key Exchange (LAKE) WG was chartered at the end of 2019, with the sole purpose of designing the requirements and a LAKE solution for OSCORE—which can be suitable for constrained environment as well. Once achieved such milestone the WG will be closed. The LAKE WG must necessarily coordinate with other IoT-related IETF WGs such as ACE, CORE, 6TISCH, LPWAN, and LWIG in order understand and validate the requirements and the solution.

**RATS** — The Remote ATtestation ProcedureS (RATS) WG has recently been chartered in order to create an architecture, protocols and data models that allow various parties to assess the trustworthiness of remote system components. The group has already produced a draft architecture document and compressed token with signed claims about an IoT device.

The IETF standardization efforts in the IoT rely on the activities of additional WGs and other IETF-related organizations. In the next section, we shed light on other IETF WGs and RGs whose activities, by extension, consider the IoT landscape as well. Then, we introduce how additional IETF committees and organizations are promoting network and infrastructure convergence in the IoT domain.

V. EXPERIMENTAL, USE CASES, AND INFRASTRUCTURES

In the experimental and use cases domains, there are at least three WGs whose interests are closely linked to IoT.

**IPWAVE** — In the context of modern vehicular systems, the IP Wireless Access in Vehicular Environments (IPWAVE) WG (established in 2016) concentrates its focus on Vehicle-to-Vehicle Communications (V2V) and Vehicle-to-Infrastructure (V2I) use-cases. The main scope of the WG is to develop an IPv6 based solution to establish efficient and secure connectivity between vehicles and other infrastructure components. V2V and V2I communications may encompass the use of different link layer technologies including 802.11-OCB (Outside the Context of a Basic Service Set), 802.15.4 with 6LoWPAN, LTE-D, LPWAN, etc. Many of these link-layers already provide full support for IPv6 unlike 802.11-OCB, despite representing one of the most promising link layer in this context. In this regard, IPWAVE aims to activate coordination with IEEE 802.11 for fully enabling transmission of IPv6 datagrams over IEEE 802.11-OCB mode. The WG also aims to document state of the art and use cases of IPv6-
based vehicular networks, by taking also into account the IoT protocol suite being developed in other IETF and IRTF groups. Table IV summarizes two I-DS in the IPWAVE WG.

**HOMENET** — The Home Networking (HOMENET) WG mainly focuses on automatic configuration of IPv6 within and among home networks, as well as investigating home networks setup issues caused by the use of different networking technologies and heterogeneous devices. Two relevant aspects are considered. The first relates to the complexity of managing multiple home network segments, including scenarios in which the subnets are physically deployed in different places. These issues are generated, for example, by the concurrent use of different link layers (e.g., Ethernet technology and others designed for low-powered sensors) that require different routing and security policies. The second aspect regards the IPv6 support in home network devices (e.g., gateways and routers), as the use of IPv6 implies the re-definition of specific requirements and mechanisms (e.g., prefix configuration for routers, managing routing, name resolution, service discovery, network security). HOMENET has already produced several informational and proposed standard RFCs. Table IV summarizes two of the most relevant ones (RFC 7368 and RFC 7788).

**LWIG** — The main scope of the Lightweight Implementation Guidance (LWIG) WG is to provide guidelines for efficient implementation techniques and practical considerations about the usage of Internet protocols in low-capabilities devices operating in constrained environments. Defining this type of good practices becomes crucial if we consider the limited computing power, battery capacity, available memory, or communications bandwidth of constrained (IP-capable) devices. In fact, a minimal optimization in the software implementation and execution (even in the order of few kilobytes of code) can result in tangible benefits in terms of reduced complexity, memory footprint, or power usage. The WG was with the purpose of scrutinizing IoT-related IETF protocols, such as IPv6, 6LoWPAN, CoAP, and RPL. LWIG seeks to provide recommendations for the optimization of already existing and stable protocols implementations, ensuring the critical requirement of interoperability with other devices. Table IV summarizes an RFC defining common terminology for constrained-node networks, as well as drafts outlining guidance for CoAP implementation or TCP usage guidance in IoT contexts.

Two additional IRTF groups shows interest on exploring the applicability of specific network infrastructure also to IoT scenarios: ICNRG (Information-Centric Networking RG) and DINRG (Decentralized Internet Infrastructure RG).

**ICN RG —** ICN RG considers also the IoT, as domain in which to take advantage of ICN. RFC 7476 outlines what ICN characteristics can be exploited in IoT (e.g., naming, data discovery, caching), while RFC 7927 what are the research challenges deriving from such integration. Both RFCs provide a comprehensive literature review and analysis of ongoing research efforts that are aiming to enable the ICN-based IoT paradigm. It is also emphasized how IoT exposes ICN abstractions to an even more strict set of requirements due to the large quantity of nodes, as well as type and volume of information to be processed. Table IV mentions also two I-DSs, which are characterized by a clear IoT focus. One describes architecture design guidelines for leveraging ICN to IoT, while the other specifies dedicated mechanisms for adapting ICN to LoWPAN networks.

**DINRG** — DINRG is one of the latest RG established in IRTF. The group’s charter identifies the WG scope in investigating infrastructure services that benefit from decentralization or that are difficult to realize in connectivity-constrained networks. Both aspects can relate to IoT, since centralized deployments can represent a limitation to many IoT use cases as well as well-known connectivity limitation of IoT networks. Infrastructure services decentralization brings additional research challenges (e.g., trust management, name resolution, resource discovery), which are investigated by DINRG.

**VI. SUPPORTING ORGANIZATIONS**

**IoT Directorate** — Beyond the activities of the WGs focusing on IoT scenarios, the entire protocol stack is evolving and many of the new technologies developed in other IETF WGs can find applicability also in IoT contexts. With a view to strengthening an effective coordination between WGs and external IoT standard organizations and alliances, IETF has established the IoT Directorate, an advisory group of technical experts the primary purpose of which is "coordination within IETF on IoT-related work and increasing the visibility of IETF IoT standards visibility to other SDOs, industry alliances, and other organization" [6].

**Internet Architecture Board (IAB)** — The IAB is a committee established to serve and support the IETF activities, in order to facilitate the standardization process. In the

---

### TABLE IV: Selection of relevant RFCs and I-Ds in the experimental and use cases and infrastructures.

| RFC Number | Title | Description |
|------------|-------|-------------|
| RFC 7368   | IPv6 Home Networking Devices and the Home Networking Control Protocol (HNCP) | Defines requirements for home network devices and the Home Networking Control Protocol (HNCP). HNCP provides multiple functions such as, e.g., redefined configuration of addresses, name resolution, service discovery, etc. |
| RFC 7788   | IPv6 Wireless Access in Home Networks - IPv6 Devices | Describes the definition of key parameters for enabling an efficient transmission of IPv6 packets over IPv6 networks. Among these parameters the expected Transmission Medium (ETM) size, the header format providing the IPv6 header, IPv6 address format, source address extension, etc. |
| RFC 8691   | Basic Support for IPv6 Networks Operating Outside the Context of a LAND Service | Describes principles and requirements for enabling an efficient transmission of IPv6 packets over LAND networks. It provides a solution that is able to operate outside the context of a LAND service. |
| RFC 8690   | IPv6 Device Networking Architecture Principles | Describes principles and requirements for enabling an efficient transmission of IPv6 packets over IPv6 networks. It provides a solution that is able to operate outside the context of a LAND service. |
| RFC 8689   | IPv6 Routing Protocol | Defines requirements for IP-based routing protocols over IPv6 networks. It specifies how routing information can be exchanged in an IPv6 network. |
| RFC 8688   | IPv6 Home Networking | Defines requirements for home network devices and the Home Networking Control Protocol (HNCP). HNCP provides multiple functions such as, e.g., redefined configuration of addresses, name resolution, service discovery, etc. |
| RFC 7927   | IPv6 EUI-64 OOB CoAP Context | Defines the CoAP context in which IPv6 EUI-64 addresses are used. The CoAP context is defined and described, and a CoAP context object is provided to facilitate the standardization process. |
| RFC 7476   | IPv6 EUI-64 OOB CoAP Context | Defines the CoAP context in which IPv6 EUI-64 addresses are used. The CoAP context is defined and described, and a CoAP context object is provided to facilitate the standardization process. |

---

**Notes:**

1. **ICN** stands for *Information-Centric Networking*.
2. **IoT** stands for *Internet of Things*.
3. **SDOs** stands for *Standard Development Organizations*.
4. **ETM** stands for *Expected Transmission Medium*.
5. **CoAP** stands for *Constrained Application Protocol*.
6. **TCP** stands for *Transmission Control Protocol*.
7. **IPv6** stands for *Internet Protocol Version 6*.
8. **6LoWPAN** stands for *IPv6 over Low-Power Wireless Personal Area Network*.
9. **RPL** stands for *Rendezvous Point Locator*.
10. **ICN** stands for *Information-Centric Networking*.
11. **IETF** stands for *Internet Engineering Task Force*.
12. **HOMENET** stands for *Home Networking*.
13. **LWIG** stands for *Lightweight Implementation Guidance*.
14. **ICNRG** stands for *Information-Centric Networking Research Group*.
15. **DINRG** stands for *Decentralized Internet Infrastructure Research Group*.
16. **IoT Directorate** stands for *Internet of Things*.
17. **IAB** stands for *Internet Architecture Board*.
18. **EtC** stands for *Effective Traffic Control*.
19. **NSP** stands for *Network Service Provider*.
20. **IETF** stands for *Internet Engineering Task Force*.
21. **ICNRG** stands for *Information-Centric Networking Research Group*.
22. **ICN** stands for *Information-Centric Networking*.
23. **RFC** stands for *Request for Comments*.
24. **I-D** stands for *Internet-Draft*.
25. **TCP** stands for *Transmission Control Protocol*.
26. **IPv6** stands for *Internet Protocol Version 6*.
27. **6LoWPAN** stands for *IPv6 over Low-Power Wireless Personal Area Network*.
28. **CoAP** stands for *Constrained Application Protocol*.
29. **RPL** stands for *Rendezvous Point Locator*.
30. **ICN** stands for *Information-Centric Networking*.
31. **IETF** stands for *Internet Engineering Task Force*.
32. **HOMENET** stands for *Home Networking*.
33. **LWIG** stands for *Lightweight Implementation Guidance*.
34. **ICNRG** stands for *Information-Centric Networking Research Group*.
35. **DINRG** stands for *Decentralized Internet Infrastructure Research Group*.
36. **IoT Directorate** stands for *Internet of Things*.
37. **IAB** stands for *Internet Architecture Board*.
38. **EtC** stands for *Effective Traffic Control*.
39. **NSP** stands for *Network Service Provider*.
40. **IETF** stands for *Internet Engineering Task Force*.
specific context of IoT, IAB has organized multiple workshops (e.g., about security, architecture, and semantic interoperability [13]), with the intention of promoting IoT-related IETF activities and receiving active engagement of external parties for the development of a better IoT. Furthermore, it has also drawn up an informational document that offers guidance for designing Internet-connected smart objects networks [14].

Internet Assigned Numbers Authority (IANA) — It is an organization that coordinates and manages domain names (e.g., through DNS Root), IP addressing, as well as maintaining the Internet protocols’ numbering systems where e.g. protocols parameters specified in RFCs are defined. IANA is responsible of assigning and registering the static fields defined in the different protocols. In the case of IoT, several protocol constants require a well-kept registry (e.g., CoAP Content-Formats, COSE Algorithms, 6LoWPAN Capability Bits, or CBOR Tags), which is regularly defined during the publication of new RFCs [15].

VII. CONCLUSION

The IETF is a leading entity for specification and documentation of key IoT standards, as well as guidelines for their implementations. The IETF focus on IoT is constantly growing, besides strengthened by a larger adoption of its IoT protocol suite across other SDOs, organizations, and consortia. The main goal of this article was to provide a comprehensive and detailed overview on the current IETF activities in support of IoT deployments. We have inspected six meta-domains, presenting what is the main focus of distinct working (and research) groups operating in each single area. We have also presented a concise summary of the main outcomes produced by the WGs, as well as some of the most significant technical areas currently explored.

REFERENCES

[1] A. Al-Fuqaha, M. Guizani, M. Mohammadi, M. Aledhari, and M. Ayyash, “Internet of Things: A Survey on Enabling Technologies, Protocols, and Applications,” IEEE Communications Surveys & Tutorials, vol. 17, no. 4, pp. 2347–2376, 2015.
[2] C. Bormann, M. Ersue, and A. Keranen, “RFC7228 – Terminology for Constrained-Node Networks,” May 2014, Accessed: 2018-12-08. [Online]. Available: http://tools.ietf.org/rfc/rfc7228.txt
[3] B. A. Forouzan and S. C. Fegan, TCP/IP protocol suite. McGraw-Hill Higher Education, 2002.
[4] I. Ishaq, D. Carels, G. Teklemariam, J. Hoebeke, F. Abeele, E. Poorter, I. Moerman, and P. Demeester, “IETF Standardization in the Field of the Internet of Things (IoT): a Survey,” Journal of Sensor and Actuator Networks, vol. 2, no. 2, pp. 235–287, 2013.
[5] R. Minerva, A. Biru, and D. Rotondi, “Towards a Definition of the Internet of Things (IoT),” IEEE Internet Initiative, vol. 1, pp. 1–86, 2015.
[6] “IETF – Internet of Things,” Accessed: 2018-12-08. [Online]. Available: https://www.ietf.org/topics/iot/
[7] Z. Sheng, S. Yang, Y. Yu, A. Vasilakos, J. Mccann, and K. Leung, “A Survey on the IETF Protocol Suite for the Internet of Things: Standards, Challenges, and Opportunities,” IEEE Wireless Communications, vol. 20, no. 6, pp. 91–98, 2013.
[8] I. W. Group et al., “Wireless Medium Access Control and Physical Layer Specifications for Low-Rate Wireless Personal Area Networks,” IEEE Standard, vol. 802, no. 4, p. 2003, 2003.
[9] C. Gomez, J. Paradells, C. Bormann, and J. Crowcroft, “From 6lowpan to 6lo: Expanding the universe of ipv6-supported technologies for the internet of things,” IEEE Communications Magazine, vol. 55, no. 12, pp. 148–155, Dec 2017.
[10] C. Bormann, A. P. Castellani, and Z. Shelby, “Coap: An application protocol for billions of tiny internet nodes,” IEEE Internet Computing, vol. 16, no. 2, pp. 62–67, March 2012.
[11] “Lightweight M2M (LWM2M) – OMA Specworks,” Accessed: 2018-12-08. [Online]. Available: https://www.omaspecworks.org/what-is-oma-specworks/iot/lightweight-m2m-lwm2m/
[12] “Web of Things Interest Group,” Accessed: 2018-12-08. [Online]. Available: https://www.w3.org/WoT/IG/
[13] J. Jimenez, H. Tschofenig, and J. Arkko, “Report from the Internet of Things (IoT) Semantic Interoperability (IOTSI) Workshop,” 2016, Accessed: 2018-12-08. [Online]. Available: https://datatracker.ietf.org/doc/rfc8477/
[14] H. Tschofenig, J. Arkko, D. Thaler, and D. McPherson, “Architectural Considerations in Smart Object Networking,” 2015, Accessed: 2018-12-08. [Online]. Available: https://tools.ietf.org/html/rfc7452
[15] “IANA – Protocol Registries,” Accessed: 2018-12-08. [Online]. Available: https://www.iana.org/protocols/