The Internet of Things within the IETF

What IoT-related activities are taking place?

Date
10 October 2018

Author(s)
Marco Davids

Page
1/5

Classification
Public

Contact
sidnlabs@sidn.nl

Contact
T +31 (0)26 352 5500
support@sidn.nl
www.sidn.nl

Offices
Meander 501
6825 MD Arnhem
The Netherlands

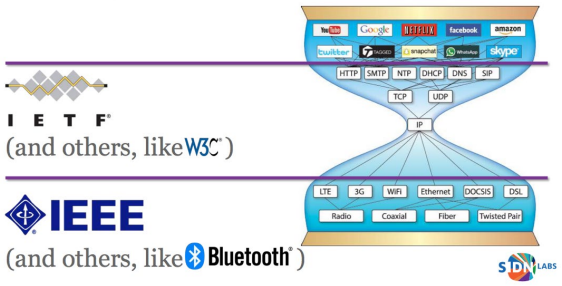
Mailing address
PO Box 5022
6802 EA Arnhem
The Netherlands

The 102nd IETF meeting took place between 14 and 20 July 2018. This report looks at the IoT-related activities and working groups currently grabbing attention within the IETF.

Introduction

The Internet of Things (IoT) is a broad concept, which can be viewed from a variety of perspectives. Many people and organisations are working on the IoT, each approaching it from their own angle. Manufacturers are looking to bring new IoT products to market. Cybersecurity organisations such as ENISA and NCSC are concerned with certain IoT security issues, while various standardisation bodies are striving to develop and refine protocols with a view to promoting interoperability. In political circles, the privacy implications are a particular focus, and the academic community is also interested in the IoT's many facets.

Against that complex background, the IETF (Internet Engineering Task Force) has its own particular role. That role is best explained by reference to the familiar 'hourglass model' of the internet's various abstraction layers, even if the demarcation lines are not as clear in practice as the model suggests.



Applications

At the top of the hour glass, we have the applications developed by companies such as Facebook, Google and all the others. Relatively speaking, the top part of the hourglass is highly dynamic. The applications make use of the standardised protocols beneath them.

Protocols

At the bottom of the hourglass, we have the so-called 'link layer' and 'physical layer'. They are the abstraction layers at which communication standards such as Zigbee and other IEEE 802.15.4-based protocols are realised. Like the top of the hourglass, the bottom is changing all the time. For anyone who isn't aware: Zigbee is already widely used in IoT products.

Core of the internet

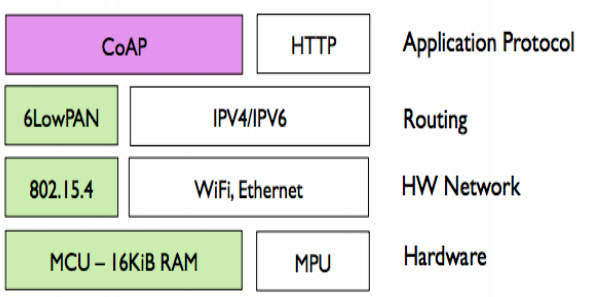
In the middle of the hourglass is the 'transport layer' and the 'internet layer' or 'network layer', otherwise known as 'the core of the internet'. The core is the abstraction layer that changes least, if for no other reason than that

realising changes to the global internet is operationally very challenging. The core is typically the domain of the IETF (albeit not exclusively) and also the scope of this report.

IETF and the IoT: a brief history

Having established itself on the IETF agenda gradually, the IoT is now a key topic of interest and the subject of more fundamental debates, such as that regarding the 'Architectural Considerations in Smart Object Networking' (RFC7452)

The topic's rise to prominence within the IETF may be seen as starting with development of the IPv6 addressing protocol, since the IoT depends on IPv6. Also, although IPv6 has been in existence for some time, it remains a topical and relevant theme within the IETF, especially the **6Man** WG (Working Group).



Following the arrival of IPv6, several 'waves' of IoT development can be discerned. First, there was the standardisation work in the lower abstraction layers of the hourglass model. That work included the **6LoWPAN** initiative, for example, which is now being carried forward by the **6Lo** WG. And, in 2015, RFC7668 came out, standardising IPv6 over Bluetooth Low Energy (BLE).

Both of those developments took place very close to the bottom of the hourglass. That is also where the **6TiSCH** WG operates, defining IPv6 over TSCH (Timeslotted Channel Hopping, an extension to IEEE 802.15.4). Other standards to emerge at the base of the hourglass included **ROLL** (Routing Over Low power and Lossy networks), **LWIG** (Light-Weight Implementation Guidance) and **IPWAVE** (IP Wireless Access in Vehicular Environments).

Higher in the stack

Over time, the IETF's IoT activities shifted to higher levels of the hourglass. The emphasis moved towards 'the Web of Things', exemplified by the **CoRE** WG (Constrained RESTful Environments), which is best known for CoAP (the Constrained Application Protocol), RFC7252.

Another example of the IoT's migration up the stack is the Manufacturer Usage Description ('MUD') Specification drafted by the **OPSAWG** (Operations and Management Area Working Group). MUD has been a focal point within our SPIN project.

Research groups

There has been a lot of activity within the IRTF (Internet Research Task Force) as well. Of particular note in that regard is the **T2TRG** (Thing-to-Thing Research Group).

Overview

We have compiled an overview of the (active) IETF working groups whose work is relevant to the IoT. A few of each group's key activities are highlighted by reference to the most recent IETF meeting (IETF 102).

It is important to note, however, that a great deal of other work is being done within the IETF, which is indirectly relevant to the IoT. For example, CoAP works with DTLS (**TLS WG**), while MUD (**OPSAWG WG)** leans heavily on YANG (**NETCONF WG**). So, the working groups responsible for those supporting technologies are also contributing indirectly to IoT standardisation. Other working groups with indirect influence include **ACE** (Authentication and Authorization for Constrained Environments), **CBOR** (Concise Binary Object Representation), **ANIMA** (Autonomic Networking Integrated Model and Approach) and **Homenet** (Home Networking).

Although, with the exception of **Homenet**, the working groups in question are not included in the overview, they are influential in relation to the wider IoT landscape within the IETF.

6Man (IPv6 Maintenance)

The IPv6 protocol has traditionally thrown up a lot of

'detail issues'. That may be seen as a positive, insofar as it reflects the active way that the protocol is maintained. In the past, it has even been suggested that the IETF should stop maintaining IPv4 and focus exclusively on IPv6. However, that controversial proposal didn't secure support. The topics currently receiving attention within 6Man are highly technical and involve improvements to certain facets of the protocol. One such is the 'draft-ietf-6man-ipv6only-flag', which will enable operators to identify a network as IPv6-only. The purpose of that being to prevent certain problems, particularly as revealed by IPv6-only experiments undertaken at previous IETF meetings.

6Lo (IPv6 over Networks of Resource-constrained Nodes)

Refinements are still being made to the 6LoWPAN protocol, which enables IP(v6) on 'constrained' (i.e. limited-capability) devices that may be on line only a few times a day (see also RFC7228 for relevant terminology). Issues being addressed include: 'IPv6 over Constrained Node Networks (6lo) Applicability & Use cases' (draft-ietf-6lo-use-cases) and 'Transmission of IPv6 Packets over Near Field Communication' (draft-ietf-6lo-nfc), which are ambitious undertakings.

6TiSCH
(IPv6 over the TSCH mode of IEEE 802.15.4e)

This active working group too has numerous technical drafts on its agenda. For example, there's a draft protocol that would provide a basis for devices to join a 6TiSCH network on a secure basis ('draft-ietf-6tisch-minimal-security'). The issue of interoperability is being examined as well.

CoRE WG (Constrained RESTful Environments)

The CoRE Working Group's activities are more closely related to, for instance, our SPIN work and therefore our 'experience' of the IoT. That is undoubtedly linked to the fact that the group operates at a higher level of 'the stack' than some. It is concerned with, for example, standardised formats for the exchange of sensor data ('draft-ietf-core-senml') and the prevention of congestion within the CoAP protocol ('draft-ietf-core-cocoa'). Devices such as IKEA's TRÅDFRI (smart lighting) already use CoAP.

IPWAVE
(IP Wireless Access in Vehicular Environments)

This working group is concerned with the somewhat futuristic field of internet-connected vehicles. The belief is that such vehicles will ultimately become commonplace. The WG was therefore created to consider how vehicle-internet communication can best be realised, in the interests of both passenger convenience and operational data exchange. Communication between vehicles is also relevant, since it is seen as a way of enabling (self-driving) vehicles to travel very closely together on highways. Data exchange prior to manoeuvring would enable coordinated braking, for example. To a large extent, therefore, the WG is active in virgin research territory. The working group is currently still at the stage of defining problem statements and use cases, such as 'draft-ietf-ipwave-vehicular-networking'. However, it is also addressing more practical matters, such as the automatic naming of sensors and other in-vehicle devices using the DNS ('draft-jeong-ipwave-iot-dns-autoconf').

LWIG (Light-Weight Implementation Guidance)

This working group's goal is to enable minimalist, operational, interoperable TCP stacks even on the most 'constrained' IoT devices. The intention is to secure that goal using existing, proven technology.

The WG's field of interest interfaces directly with those of various other working groups, including 'Neighbor Management Policy for 6LoWPAN' (draft-ietf-lwig-nbr-mgmt-policy) and 'CoAP Implementation Guidance' (draft-ietf-lwig-coap). Other topics addressed include 'TCP Usage Guidance in the IoT' (draft-ietf-lwig-tcp-constrained-node-networks), which is about enabling lightweight TCP stacks to operate on very simple, low-capacity devices. Security and encryption are also on the WG's agenda.

OPSAWG (Operations and Management Area Working Group)

OPSAWG is the working group that produced the MUD draft referred to above and therefore very important in relation to the IoT. However, the MUD draft (draft-ietf-opsawg-mud), now in its 25th iteration, was not on the agenda at IETF 102. The reason being that it is currently

undergoing IESG review, one of the final stages en route to RFC status.

ROLL
(Routing Over Low power and Lossy networks)

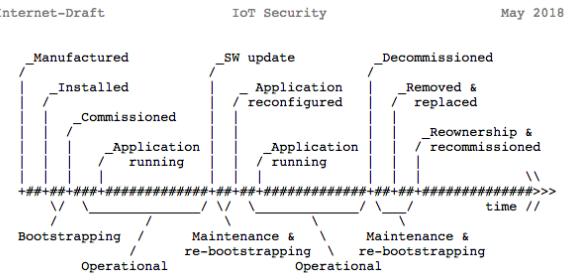
This working group focuses on routing issues and solutions in home networks and in sensor networks within buildings and smart cities. To that end, an (IPv6-only) framework is under development. The type of system addressed includes networks based on IEEE 802.15.4, Bluetooth and other protocols. The WG's most important early products include RFC6550 (RPL: IPv6 Routing Protocol for Low-Power and Lossy Networks) and RFC5826 (Home Automation Routing Requirements in Low-Power and Lossy Networks). RFC7102, which defines related terminology, is also relevant to the ROLL working group. ROLL has various draft documents in production, several of which were discussed at IETF 102.

Homenet

Finally, the Homenet working group should not be overlooked. Although it isn't directly concerned with the IoT, the Homenet WG's remit is the home networks of the future, which are expected to include all sorts of IoT devices. Future home networks may therefore feature far more subnets than we are currently used to. And it is the associated challenges that occupy the working group. Against that background, RFC7368 (IPv6 Home Networking Architecture Principles) is worth reading. The working group has also proposed that a domain ('home.arpa') should be reserved for home applications (RFC8376). Subjects discussed by the WG at IETF 102 included 'draft-ietf-homenet-front-end-naming-delegation' (Outsourcing Home Network Authoritative Naming Service) and other naming proposals, as well as proposed 'service discovery' solutions and the Babel routing protocol (draft-ietf-homenet-babel-profile).

T2TRG (Thing-to-Thing Research Group)

As indicated, T2TRG isn't a working group, but a research group that is currently working on various documents. One being 'draft-irtf-t2trg-iot-seccons' (State-of-the-Art and Challenges for the Internet of Things Security), which covers issues such as the lifecycle of IoT devices and the associated security issues. Such issues differ from those presented by general purpose devices, such as laptops. IoT devices may be hidden deep within buildings or machines and, as a result, they'll probably have much longer lifecycles than the average laptop. They may be operating for many years and are consequently liable to be forgotten. All those characteristics have implications for cybersecurity. For additional information on this, read RFC7744 (Use Cases for Authentication and Authorization in Constrained Environments).



The security benefits of automation are set out in 'draft-garciamorchon-t2trg-automated-iot-security'.
T2TRG is also considering the value of RESTful interfaces in relation to the IoT (draft-irtf-t2trg-rest-iot). All three of those drafts received further consideration at IETF 102.

Conclusions

From the picture presented above, it will be apparent that the IoT now has a high profile within the IETF, just as it does in many other spheres. The IETF's involvement began with the development of solutions close to the link layer. Where those solutions involve IP technology, it is almost exclusively IPv6.

Later, there were developments higher in the stack, closer to the Web of Things. CoAP is a good example of that, as is the interest in RESTful communication using IoT devices.

Attention has also turned to more fundamental issues, particularly from a research perspective. How should small IoT devices be secured, given that many will have long life cycles, hidden away within buildings and installations? How can we ensure that they can easily be

added to home or business networks in large numbers? For example: how can thousands of lamps in a large office complex be connected, monitored and managed? And what should be done to align development of the IoT with other developments? What is needed for the home network of the future?

In this article, we have sought to summarise the extensive and complex IoT-related activities taking place within the IETF. It was not our intention to present a comprehensive survey of relevant working groups or their activities. In many cases, IoT developments make use of or are based on other technologies, such as YANG, TLS, HTTP or DNS, which are the province of further IETF working groups. Consequently, those groups have an indirect influence on the bigger picture. Nevertheless, we hope and believe that our summary is a useful general overview of key IoT initiatives.

It will be apparent that, as a body to which everyone is free to contribute, the IETF remains highly relevant to the further development of the internet.

It organises conferences three times a year, which generally attract between a thousand and fifteen hundred experts. The next one, IETF 103, takes place in November 2018.