VOLUME 11, ISSUE 3 • APRIL 2016

IETF® Journal

A report from IETF 94, November 2015, Yokohama, Japan. Published by the Internet Society in cooperation with the Internet Engineering Task Force.*

INSIDE THIS ISSUE

Internet Society™

FROM THE EDITOR'S DESK

By Mat Ford

THE 94TH MEETING OF THE INTERNET ENGINEERING TASK FORCE (IETF) WAS HELD IN Yokohama, Japan, and was hosted by the WIDE Project. In this issue of the *IETF Journal* we present some of the highlights of the week and offer a peek at the many interesting people and discussions that comprised the meeting.

Our cover article celebrates the upcoming IETF meeting in Buenos Aires and shares the opportunities it brings for both the IETF and the region. Other articles explore IETF work on the Internet of Things, special-use domain names, the benefits of a data definition language for JSON, the pre-IETF Hackathon, the Simplified Use of Policy Abstractions (SUPA) working group, and some impressions from a newcomer to the IETF. You'll also find our regular columns from the IETF, IAB, and IRTF chairs, as well as coverage of hot topics discussed during the plenary meeting.

Finally, as 2016 marks the 30th anniversary of the IETF, I'd like to take this opportunity to wish the IETF a long and prosperous future making the Internet work better.

We are hugely grateful to all of our contributors. Please send your comments and suggestions for contributions to ietfjournal@isoc.org. Subscribe to hardcopy or email editions by visiting https://www.internetsociety.org/publications/ietf-journal/ietf-journal-subscription.

THE IETF FLIES TO SOUTH AMERICA

By Carlos Martinez

For only the second time in its history and on the event of its 30th anniversary, the IETF's next meeting will be held south of the equator in Buenos Aires, Argentina.

For the technical community in Latin America this is an important milestone: the Buenos Aires meeting will provide visibility to the technical work in the region that keeps the Internet humming. Many also anticipate that a meeting in the region will motivate a new generation of Latin American engineers to take up protocol engineering.

Continued on page 4

The articles published in the IETF Journal are not intended to reflect the opinions or the position of the IETF or the Internet Society. See http://www.ietf.org.

MESSAGE FROM THE IETF CHAIR

By Jari Arkko

Jari Arkko, IETF Chair

PERHAPS THE UPPERMOST THING ON MY MIND IS HOW FRIENDLY AND WELCOMING Japan was. I thoroughly enjoyed the incredibly well-working network, the wireless that covered all the way to the Ferris wheel, the ceremonies, the food, the modern facilities, and the long list of supporters for our meeting. Thank you!

We had a very good turnout in terms of participation: more than 1,300 participants on site at the end of the week.

Hackathon

Our third IETF Hackathon had 70–95 participants (depending on whether you count official registrations or the number of t-shirts handed out). It drew new participants to the IETF and a coder who was only 16 years old. That said, as with the overall meeting, the number of participants is not the key metric of success. What matters is the work that gets done and whether that work brings improvements to the Internet. This year's Hackathon focused largely on key Internet issues, including the privacy of metadata and ability to easily build networks. I also was impressed with how people learned. For example, although one team failed to do what they wanted, that failure had a lesson in it and later in the week the working group in question realized that they have to change their approach. Well done!

[A]s with the overall meeting, the number of participants is not the key metric of success. What matters is the work that gets done and whether that work brings improvements to the Internet.

Each of the ten teams made a significant contribution. Notable examples are the DNS security and privacy team (DPRIVE), which led a professional and systematic approach to securing the DNS infrastructure and eliminating metadata leakage, and the HOMENET team, which had an impressive demo involving multiple platforms ranging from routers to iPhones.

Birds of a Feather Sessions

Our one Birds of a Feather (BoF) this meeting, Internet Storage Sync (ISS), focused on synchronization protocols for Internet-based storage services. The origins of this topic are in academic research on optimized synchronization mechanisms, protocols that can improve the efficiency of other, widely used protocols. The BoF itself emphasized the prospect of broader synchronization protocol interoperability. I believe that this is of key interest and potentially very useful, particularly for enterprise customers and third-party application developers who would benefit from the ability

Continued on page 5

Recent IESG Document and Protocol Actions

A full list of recent IESG Document and Protocol Actions can be found at https://datatracker.ietf.org/iesg/ann/new/

WORDS FROM THE IAB CHAIR

By Andrew Sullivan

Andrew Sullivan, IAB Chair

IETF 94 WAS IN YOKOHAMA, JAPAN, AND AS USUAL, THE INTERNET ARCHITECTURE BOARD (IAB) had some things to report. But this time, instead of using plenary time for it, we sent a report in advance to the community (see https://www.iab.org/2015/11/02/report-from-the-iab/). This was inspired by a change to the way the meeting worked, and the IAB has concluded that it is a positive approach for our reports. Expect to see this kind of advance report again before Buenos Aires.

No News Is Good News?

One of the things that the IAB does is pay attention to new work coming to the IETF. The IAB tries very hard to make sure that at least one IAB member covers every Birds of a Feather (BoF) at an IETF meeting. We report back to the Internet Engineering Steering Group (IESG) about what we saw, how we think it fits into other work we know about, whether we think the effort is likely to produce a successful working group, and so on. So, it was with some discomfort that I contemplated the Yokohama meeting, since there was only one BoF.

In some ways, that shouldn't be too surprising. There were lots of working groups chartered last year, and previous meetings had record numbers of BoFs (more requests than were accommodated). Also, some areas have become good at chartering working groups without holding BoFs. Nevertheless, it was an unusual occurrence, and so it did not surprise me that it came up as a major topic at the plenary.

> **Scores of working groups were chartered last year, and previous meetings had record numbers of BoFs (more requests than were accommodated).**

An important part of that discussion was about process. How does new work get started? How do people meet informally to start working on a problem? Many people talked about reducing formal barriers. Yet it seems that the formal barriers are mostly a figment of our collective imagination. A significant reason for the IETF holding its meetings is exactly so that people can get together informally and explore topics collaboratively. At the IETF, you don't need permission to get started. You don't even need forgiveness. If you think a topic is interesting and you can convince a few other people to talk about it, then you have all you need to get a conversation going. Discuss, improve the idea, and so on. The barriers are low.

But to make the more formal parts of the process easier, the IAB is happy to help. If you are struggling with how an idea fits together or need help with how to approach your topic (or, perhaps, how it relates to the Internet), feel free to contact iab@iab.org. Talking about these issues is part of our job.

Collaboration and Meetings

The Yokohama meeting coincided with several other meetings in the region. The World Wide Web Consortium (W3C) held its meeting in Sapporo the week prior to the IETF meeting. The Internet Measurement Conference (IMC) was

Continued on page 6

The Internet Architecture Board is chartered both as a committee of the IETF and as an advisory body of the Internet Society. Its responsibilities include architectural oversight of IETF activities, Internet Standards Process oversight and appeal, and the appointment of the RFC Editor. See http://www.iab.org.

The IETF Flies to South America, continued from page 1

Development asymmetries are abundant in Latin America. While the region as a whole is classified as developing, some of its countries are nearing developed status by having been accepted in or applying for membership at the Organisation for Economic Co-operation and Development; others are lagging behind.

These asymmetries also manifest in Internet access. The region has countries with Internet penetration percentage rates in the low 20s or even less, while other countries have rates of 75–80%.

In terms of infrastructure, the availability of fixed copper or fiber plant can vary widely. Some countries are focusing their efforts on growing mobile networks as a means to bridge the Internet penetration gap and deliver services to their populations.

Geography and population density also play roles. Although Latin America is home to some of the largest cities in the world (e.g., Sao Paulo and Mexico City), the overall population density of the region is low, with many small communities scattered throughout the continent. Distances can be long and natural barriers like the Andes mountains and the Amazon rainforest make traditional communications difficult.

Internet access in the region not only offers access to entertainment and social networking, it is routinely leveraged to deliver eMedicine, education, eGovernment, and disaster warning and relief services. Examples include electronic textbook delivery in the Peruvian Andes and videoconferenced medical appointments in Central America. Information and communications technology (ICT)-related and knowledge-related industries are booming in several countries, in some cases quickly catching up with the primary, commodities-based sectors of the economy.

What It Means for the IETF

Protocol engineering is critical to ensuring that the Internet remains a useful tool that developing regions can use to cope with the many challenges imposed by geography, population distribution, and asymmetric economic development.

In technical terms, this means taking into consideration the following factors and challenging the following assumptions:

- Power efficiency can be critical. Some communities might have access to power during certain hours during the day or could suffer power outages due to weather or other natural events.
- Permanent, "always-on" connectivity is not always present, particularly in rural areas.
- Error rates do not always go down over time. Radio links spanning long distances can be part of any path.
- Bandwidth goes up over time, but not as quickly as in other regions. Efficiency in the wire should be considered in new protocol work.
- Efficient spectrum usage is critical. Many countries deploy mobile networks as a faster method for bridging the connectivity divide.
- Security is a priority for all protocol work. However, in regions where the Internet is still making its first inroads, it is critical to get security right and to build trust among users and applications in order to avoid the victimization of users.
- Pure client/server applications could behave poorly in mobile, radio, high-delay, or intermittent communication environments, and natural events could render large territories disconnected. Peer-to-peer protocols could provide solutions for certain niche problems.
- Operational practices can be very different than those in other regions, particularly in routing, peering, and ISP interconnection.
- IPv6 adoption is a must in a region that still needs to connect a significant portion of its population.

This is by no means an exhaustive list and the IETF has been working on several related topics, including whitespaces, Global Access to the Internet for All (GAIA), low-power protocols, and constrained environments. This work also will benefit from increased involvement by the local technical communities in the developing regions themselves, which could make the Buenos Aires meeting a very pivotal moment.

Message from the IETF Chair, continued from page 2

to more easily switch between providers. It is also necessary to obtain interest from service providers, perhaps initially from the smaller players. ISS BoF members will search for that interest, especially from the industry. Join the mailing list at https://www.ietf.org/mailman/listinfo/storagesync.

Working Groups

The Domain Name System Operations (DNSOP) Working Group (WG) meeting covered the impacts of the recent .onion allocation and issues in the RFC 6761 process that specifies that such allocations can be made, but not when those allocations are appropriate. The discussion will continue, hopefully with appropriate interest from other parts of the IETF. The first goal is to define exactly what the problem is with RFC 6761. It is unlikely that many other allocations will be made before that process is reevaluated and redesigned.

The increase in YANG data models continued; the current count is 160 drafts. Benoit Claise and his colleague Jan Medved have produced a dependency graph tool that shows the dependencies between the drafts (see http://www.claise.be/modules.png).

The security area (SAAG) WG had several local presenters. I particularly enjoyed the presentation on the security analysis of IPv6 transition technologies and the report from the workshop on impacts of encryption in mobile networks.

The DISPATCH WG talked about opportunistic security for RTP flows.

Plenary

We had one combined plenary instead of separate technical and administrative ones. It appears to be a reasonable starting point for future arrangements, although there's a lot to improve still, such as shortening the presentations part even more.

Before the plenary, we were fortunate to preview of "A Net of Rights," a short film produced by members of the proposed Internet Research Task Force research group on human rights protocol considerations (HRPC).

Photo by Charles Eckel

Because both the W3C TPAC meeting and the OpenStack Summit were in Japan the previous week, we were able to visit and be visited by key individuals from these organizations.

Collaboration

Because both the W3C TPAC meeting and the OpenStack Summit were in Japan the previous week, we were able to visit and be visited by key individuals from these organizations. Having the IETF meeting in a similar area and time frame as other meetings may be useful in the future.

Once again, we saw many new participants—nearly three hundred! We also had visitors from the Internet Society Policy and Fellowship to the IETF programmes, underscoring that participation at the IETF is a collaborative project, a working group that you care for and contribute to. I'm hoping to see these new participants involved in projects that are important to them.

There were many remote participants, including presenters. For example, Jürgen Schönwälder held an hour-long discussion in the LMAP WG via Meetecho. We also learned from remote connection issues. For example, I didn't set up backup jabber channels to be monitored appropriately during the plenary. I apologize for the inconvenience this may have caused.

What's Next?

We will continue work over the Internet in the coming months, and then meet in person 3-8 April in Buenos Aires, where our host will be LACNIC. This will be the first meeting in South America and only the second meeting held south of the equator.

Finally, the Buenos Aires IETF Hackathon is 2-3 April, so be sure to be on site early!

For More Information

For more detailed information, see https://datatracker.ietf.org/meeting/94/materials.html. The information page for the Buenos Aires meeting can be found at http://www.ietf.org/meeting/95/index.html.

THE IETF IS 30!

By Jari Arkko

On 16–17 January 1986, in San Diego, California, 21 people attended what is now known as IETF 1. Several participants of that meeting are still active contributors, and some of the topics mentioned in the proceedings from that meeting still surface at IETF meetings. And although the IETF has evolved over the past 30 years, its goal of addressing challenges to improve the network via meetings and other means has remained.

The Internet also has evolved over the past three decades. In 1986, there were a few thousand hosts on the Internet; today there are more than 3 billion users. Many of today's users access the Internet via mobile devices, and the Internet of Things is gathering an increasing amount of attention.

The Internet's technical development community has expanded, too. Starting about 15 years ago, IETF meetings were held exclusively in Europe and Asia. Today, IETF meetings draw participants from all over the world, and this year marks the first IETF meeting to be held in South America.

While it may be impossible to predict what the Internet will look like 30 years from now, it is safe to say that literally billions more devices will be connected and that security and privacy will be increasingly important. Until then, our community will continue to work tirelessly on the standards that enable that growth.

Words from the IAB Chair, continued from page 3

in Tokyo just before the IETF meeting, as was the OpenStack Summit. And the Internet Research Task Force (IRTF) organized a workshop around the IMC.

One of the IAB's responsibilities is to serve as the IETF's formal interface to other organizations. When the happy coincidence of all these meetings came up in the plenary, it got me thinking about how we build our connections to other groups. There are lots of people participating in the IETF and other organizations, and they represent a large store of knowledge about what is going on there. This is, I suspect, a part of what people found great about having so many meetings close to each other. It isn't just the saved travel costs, but also the opportunity to experience work modes and hear views you otherwise might not.

Would it be useful to identify some groups with whom we have significant overlap and try to do some recruiting there?

I have been wondering whether there might be a way to make more links of this sort across the IETF without the happy accident of having a lot of meetings in physical proximity. Given the existing constraints on IETF meetings (and others' meetings), it will be hard to arrange this sort of schedule often. Would it be useful to identify some groups with whom we have significant overlap and try to do some recruiting there? Or is this better left to the natural processes of people working on these problems to pick the right venue for their work? If you have thoughts, the IAB is interested.

Not Just IETF Meetings

Of course, the IAB doesn't only do work at IETF meetings. Since the Yokohama meeting, the IAB has sent comments to the ICANN CCWG-Accountability survey and also to the ICANN call for comments on the Registration Data Access Protocol (RADP) Operational Profile proposals. You can see what the IAB sends to other organizations at https://www.iab.org/documents/correspondence-reports-documents/.

The IAB is responsible for a number of appointments both inside and outside the IETF community. The appointments are tracked at https://www.iab.org/activities/iab-appointments-and-confirmations/. An important ongoing appointment process is that of the IRTF chair. The current IRTF chair, Lars Eggert, has announced that he will not seek reappointment, and the IAB is looking for his replacement. Lars leaves some big shoes to fill, so we have our work cut out for us. By the time you read this, the IAB will also have made decisions about the appointments to the Internet Society Board of Trustees and the RFC Oversight Committee.

The IAB also convenes workshops on topics relevant to Internet architecture. By IETF 95, the IAB will have held the Internet of Things Semantic Interoperability Workshop. Interoperability is the core value of internetworking, and we anticipate that the workshop will make a positive contribution to it. For more about our workshops, see https://www.iab.org/activities/workshops/iotsi/.

Our next IETF meeting will be in April 2016, when new Nomcom appointments are seated. The IAB will both welcome new members and miss those who are departing. I have been grateful to serve on the IAB with the group this year and I look forward to next year with my IAB colleagues both new and returning.

HOW INTERNET TRAFFIC MEASUREMENTS CAN BOLSTER PROTOCOL ENGINEERING

By Carolyn Duffy Marsan

CAN THE IETF ADOPT MEASUREMENT-DRIVEN ENGINEERING IN THE DESIGN of Internet protocols? That was the technical topic at the IETF meeting held in Yokohama, with presenters Brian Trammell, who leads the Internet Architecture Board's (IAB's) IP Stack Evolution Program, and Alberto Dainotti, a research scientist with the Center for Applied Internet Data Analysis (CAIDA).

Trammell introduced the topic by saying that measurement-driven engineering would allow protocols to be designed for common occurrences, while taking into account the risks of uncommon occurrences.

"We'd like to apply measurement wherever we can to know the difference" between these two situations, he explained, adding that it might even be possible to take measurements at runtime.

Trammell focused his talk on the role that measurement can play in writing protocols related to IP stack evolution and path impairment. He noted that many solutions assume that the Internet can be run over User Datagram Protocol (UDP), but said "we need more data" before making that decision.

Trammell showed a picture of the evolving IP stack, which resembles a two-stem martini glass, and noted that we now have two layer threes, with IPv4 and IPv6 co-existing "more or less well."

However, he said that we have problems with fuzzy boundaries between layers three and four, with Transmission Control Protocol (TCP), Transport Layer Security (TLS), and Hypertext Transfer Protocol (HTTP) on top of IPv4, while UDP and new transports will be layered on top of IPv6.

"We'd like to fix this problem by putting in new transport layers and by rethinking the layer boundary with UDP encapsulation, crypto to reinforce the boundary between endpoint and path visible headers… and add explicit cooperation to give back transport and application semantics the path they actually need," he explained.

Trammell said the IETF has taken the assumption that all of this explicit relayering can be done with UDP encapsulation. "We assume that UDP works. Does it?" he asked.

Trammell said the IETF needs to engineer protocols that work for path impairments that are common.

Trammell explained that it's important to measure path impairment, which shows the likelihood that traffic with given characteristics will experience problems on a given path. These problems might include increased latency, reordering, connectivity failure, or selective disablement of features. The goal of measuring path impairment is to discover how and how often a proposed feature would break.

"Basically, the way we measure this is we put a bunch of packets on the Internet, and we see what happens," Trammell said.

He provided results from two testbeds, PlanetLab and Ark, which cover about 10,000 paths and have widely different results in measuring the percentage of paths modifying a selected packet feature. For example, with a TCP Initial Sequence Number (ISN), PlanetLab measures an error rate of 10.7% and Ark measures a rate of 1.8%.

Trammell pointed out that these two testbeds represent "a really tiny fraction of the Internet, which has billions and billions of paths," Trammell noted. "So the results are highly dependent on the vantage point."

Further, these testbeds have the same bias because they are deployed by people who are knowledgeable about networking. Yet they have widely different results.

"We need more data here and more diversity," Trammell added.

Trammell said the IETF needs to engineer protocols that work for path impairments that are common, such as Network Address Translators (NATs), but that they shouldn't create a lot of excess code to deal with rare problems.

"We need information about the prevalence of these [situations] in order to make informed decisions," he said.

Trammell pointed out several challenges for measurement-driven protocol

Continued on next page

Andrew Sullivan, IAB Chair and Presenter at the IETF 94 Technical and Administrative Plenary

How Internet Traffic Measurements Can Bolster Protocol Engineering, continued

engineering. First, measuring the Internet is hard, and measurements don't always measure what you want. Further, the Internet is not homogenous, so it is difficult to extrapolate from measurements on any given link. Further, researchers face the problem of having not enough data and too much data at the same time.

Trammell recommends that the IETF consider using measurements that are inadvertently gathered by protocols, such as how TCP measures its round-trip time. Further, he suggests that the IETF design protocols with built-in measurements in mind, thereby making instrumentation accessible and operational at runtime.

He also suggested that the IETF enhance the testbeds that are available, such as PlanetLab and Ark, as well as existing measurement tools like the Large Scale Measurement of Broadband Performance (LMAP). The IETF should use these testbeds and tools to create a framework to bring comparability and repeatability to observations.

"The goal would be to combine measurements from different vantage points and data sources for wider and deeper insight," he explained. "Here are two things we can do: develop common information models and query sources, and develop common coordination and control protocols."

Next, Dainotti considered the role that Internet traffic measurement can play in the development of protocols related to the Border Gateway Protocol (BGP).

"BGP is the central nervous system of the Internet," Dainotti said. "BGP design is known to contribute to issues in availability, performance, and security. So we know that we need to engineer protocol evolution. However, it's difficult to make protocol engineering decisions because we know very little about the structure and dynamics of the BGP ecosystem."

Dainotti said researchers need more and better data about BGP operations, including more information from routers, more data collectors, and more experimental testbeds. Further, the Internet engineering community needs better tools to learn from the data, so that data analysis is easier, faster, and better able to cope with larger data sets. Researchers would like to monitor BGP in near real-time and tighten data collection, processing, and visualization.

Researchers would like to monitor BGP in near real-time and tighten data collection, processing, and visualization.

Dainotti shared research related to BGP outages, like those caused by country-level Internet blackouts and natural disasters. Before his Internet Outage Detection and Analysis (IODA) project, it took four months to analyze an Internet shut-down, such as the 2011 Arab Spring. With IODA's live Internet monitoring, he can detect Internet outages, such as a 20-minute outage experienced by Time Warner Cable in September 2015, in near real-time.

"We built some complex software and hardware to track outages in near real-time and to perform additional measurements while the event is actually happening," Dainotti explained. "Christmas last year, we were able to follow the outages in North Korea in almost real-time—just a 30-minute delay. This was thanks to the infrastructure we built."

Now CAIDA is making these tools more generally available. For example, it has a new tool called BGPstream that provides a software framework for historical and live BGP data analysis. This tool is available open source at bgpstream.caida.org.

BGPsteam is "used mostly by the scientific and operational community," Dainotti said. "It efficiently deals with large amounts of distributed BGP data from multiple BGP collectors. The main library offers a time-ordered data stream from heterogeneous sources. It supports near real-time data

Attendees at the combined IETF 94 Technical and Administrative Plenary.

processing and targets a broad range of applications and users."

CAIDA has built several tools including PyBGPstream, which can be used to study AS path inflation, and BGPcorsaro for monitoring address space. Another project tracks BGP hijacking attacks.

In conclusion, Dainotti described a BGP Hackathon that CAIDA hosted in February focused on live BGP measurements and monitoring. To learn more about this event, contact bgp-hackathon-info@caida.org.

"How you can contribute is to… propose problems that are worth addressing and things you would like to see in tools used to study BGP," he concluded.

To start the Q&A discussion, Trammell returned to the question of why the IETF doesn't have enough data to support the idea of running the Internet over UDP.

"This is a question I'm spending a fair amount of time working on," he said. "Lots of firewalls block or limit or impair UDP for security reasons, particularly DDoS attacks. So they turn it off… Depending on which of the commonly available testbeds we consider, we see 2% to 6% of access networks are actually blocking UDP. That's kind of a high number. We'd like to understand the shape of that impairment before we talk about UDP encapsulation."

Audience members questioned the overhead costs and privacy risks associated with having protocols take live measurements, essentially those monitoring user behavior.

"There is a huge cost in data, not just in storage of it but in privacy," Dainotti admitted, adding that the research community has many ways to anonymize data and doesn't need to retain the data forever.

In response to another question, Trammell said two protocols that could benefit from additional measurement are DNS and DNSSEC. "We should be measuring the tradeoffs of assurance versus the ability to use it for attacks," he said.

THE BENEFITS OF A JSON DATA DEFINITION LANGUAGE

By Andy Newton

JAVASCRIPT OBJECT NOTATION (JSON) [RFC 4627, RFC 7159] IS A VERY POPULAR method for exchanging data in protocols. Where Extensible Markup Language (XML) was once considered the go-to choice for data serialization, now JSON is the preferred format. As with XML, there are a number of JSON-centric building blocks, standards, and conventions and tools for using JSON to create applications and protocols. But where XML has a handful of data definition languages, JSON has none (that have been standardized).

The Wikipedia entry for *data definition language* is: "A data definition language or data description language (DDL) is a syntax similar to a computer programming language for defining data structures, especially database schemas." They are also referred to as *schema languages*.

The IETF's JSON Working Group has discussed a JSON DDL in the past. Understandably, the discussions often invoked the scars of experience with XML's most widely used DDL, XML Schema. The influence of XML Schema on the XML ecosystem is extensive; shortcomings of XML Schema almost always have a negative cascading impact with any XML work. But XML is not JSON, and although the complexities of XML are by-necessity present in an XML DDL, such entanglements can be avoided in a JSON DDL. I posit that a JSON DDL can be more powerful and flexible than an XML DDL because JSON's scope is narrowed to data serialization (a markup language is much more than data serialization, as commonly used).

XML is not JSON, and although the complexities of XML are by-necessity present in an XML DDL, such entanglements can be avoided in a JSON DDL.

Are Prose and Examples Good Enough?

Some reasoning against the need for a JSON DDL, or a DDL for any data format, is that descriptive text accompanied by examples should be all that is necessary for a programmer to implement a specification, and that the overhead of a DDL complicates matters. I agree that for most simple cases this is true. But I have first-hand knowledge that not every case is simple.

RFC 7483 describes the JSON used by Registration Data Access Protocol (RDAP), by far the largest of the documents produced by the Web Extensible Internet Registration Data Service (WEIRDS) Working Group. As part of an area review, Tim Bray wrote this of RFC 7483:

"Speaking as a person who's been skeptical of JSON schema efforts, it pains me to say this, but the information about large-scale message structure is scattered through this document in a diffuse way and it'd make me nervous as an implementer whether or not I was getting it right. I think it might be helpful to have a "large-scale message structure" section that quickly

Continued on next page

The Benefits of a JSON Data Definition Language, continued

runs through the allowable top-level shapes of messages, and exactly what can be nested inside what."

Despite RFC 7483's extensive prose describing JSON and its copious, multi-page examples, a DDL would have really been helpful. (For the curious, https://datatracker.ietf.org/doc/draft-newton-rdap-jcr/ shows what a DDL can do for RFC 7483).

In my opinion, Tim Bray's precognition was borne out during the several interoperability sessions held for RDAP at the IETF. Some implementers made assumptions about the data structures that were incorrect. And in a few cases, we found that the examples were incorrect.

In addition, I drew another conclusion from my experiences with the RDAP interoperability tests: textual descriptions are not as easy to read for the many programmers who are not native English speakers. Even I often succumb to the TL;DR ("too long; didn't read") nature of specifications. The tediousness of prose could be worse for them, and the preciseness and conciseness of a DDL might be more helpful.

I drew another conclusion from my experiences with the RDAP interoperability tests: textual descriptions are not as easy to read for the many programmers who are not native English speakers.

```
{
     "Image": {
         "Width":  800,
         "Height": 600,
         "Title":  "View from 15th Floor",
         "Thumbnail": {
             "Url":    "http://www.example.com/image/481989943",
             "Height": 125,
             "Width":  "100"
         },
         "IDs": [116, 943, 234, 38793]
      }
}
```

Figure 1. JSON Used as an Example in RFC 4627

```
{
       "Image" {
           width, height,
           "Title" :string,
           "thumbnail"
           {
               width,
               height,
               "Url" :uri
           },
           "IDs" [ *:integer ]
       }
}
width "width" : 0..1280
height "height" : 0..1024
```

Figure 2. JCR Schema

Testing and Test Software

Bad experiences with XML Schema have led some to believe that DDLs often focus implementers on correctness of the XML document to the detriment of other aspects of interoperability. "Just hand me the XSD (XML Schema Document). I don't need to read the specification." Indeed, this is one of several reasons I personally switched to Relax NG for all my XML work.

But this aspect of XML Schema is not a universal constant with all DDLs, not even all XML DDLs. It is not even a function of XML Schema, but rather a so-called feature of the tooling and the push-button, code-generation development frameworks that abstracted away all protocol aspects from the programmer (environments popular with XML technologies such as Simple Object Access Protocol).

Negative experiences aside, DDLs can be an important part of interoperability testing. DDL validators aid the creation of test

```
{
        "type" : "object",
        "properties" : {
            "Image": {
                "type" : "object",
                "properties" : {
                    "Width" : {
                        "type" : "integer",
                        "minimum" : 0,
                        "maximum" : 1280,
                        "required" : "true"
                    }
                    "Height" : {
                        "type" : "integer",
                        "minimum" : 0,
                        "maximum" : 1024,
                        "required" : "true"
                    }
                    "Title" : { "type": "string" },
                    "Thumbnail" : {
                        "type" : "object",
                        "properties" : {
                            "Url" : {
                                "type" : "string",
                                "format" : "uri",
                                "required" : "true"
                            },
                            "Width" : {
                                "type" : "integer",
                                "minimum" : 0,
                                "maximum" : 1280,
                                "required" : "true"
                            },
                            "Height" : {
                                "type" : "integer",
                                "minimum" : 0,
                                "maximum" : 1280,
                                "required" : "true"
                            }
                        }
                    },
                    "IDs" : {
                        "type":"array",
                        "items":[ { "type": "integer" } ],
                        "required" : "true"
                    }
                }
            }
        }
}
```

Figure 3. JSON Schema

suites, knocking out the low-hanging fruit with regards to syntax.

Further still, some DDLs such as JSON Content Rules (JCR) contain features to aid the creation of specific test cases: is a value Y under condition X. The nature of JCR accommodates locally overriding rules to a narrower definition (e.g., specific constants or ranges). Writing a test can involve a simple rule change instead of tediously traversing nested data structures to access the value to be inspected. (Bias warning, I am one of the coauthors of JCR).

DDL validators, or schema validators as they are sometimes known, also have the benefit of helping implementers develop software as specifications progress through the standards process. For example, during the standardization of RFC 7484, I was able to provide valuable feedback to the specification authors—feedback that was vital to the performance of software using the specification. At some point during the standardization process, however, a small, unsubstantial change was made to the JSON that I had not noticed. The result was that my software would not interoperate despite the many, many unit tests I had written. Had RFC 7484

For the purposes of the IETF, some DDLs are more practical than others. When writing a specification, one aspect of a DDL that is a benefit is conciseness.

Continued on next page

The Benefits of a JSON Data Definition Language, continued

used JCR or JSON Schema, I could have easily dropped in the final DDL and quickly discovered the problem.

Desired Features of DDLs

For the purposes of the IETF, some DDLs are more practical than others. When writing a specification, one aspect of a DDL that is a benefit is conciseness. Internet Drafts have many sections and seldom pass muster without explanatory text. Therefore a DDL that does not add bloat is appreciated. While conciseness can sometimes reduce readability, for complex uses “TL;DR” is much more of an issue. As a specification writer, if you feel writing a computer language can be tedious, the same is probably true for the many readers of the document.

Figure 1 shows JSON used as an example in RFC 4627.

And now let’s examine two different JSON DDLs describing the aforementioned example: JCR and JSON Schema. Figure 2 is the JCR example, which has a more concise syntax .

By contrast, in Figure 3, the JSON Schema is more verbose.

DDLs, such as XML Schema and JSON Schema, use the syntax of their respective formats to construct rules. This has the benefit of easing implementation of their DDL validators but jettisons conciseness. These forms also make it difficult to interleave instructive prose as normal draft text between the DDL rules, a habit of IETF authors familiar with notations, such as Augmented Backus–Naur Form (ABNF).

Figure 4 is an excerpt from RFC 4287 (The ATOM Format). ATOM is an XML format, and RFC 4287 uses the Relax NG Compact Syntax to define it. RFC 4287 is well written and makes good use of mixing explanatory text with formal syntax rules.

```
The “atom:author” element is a Person construct that indicates
   the author of the entry or feed.

   atomAuthor = element atom:author { atomPersonConstruct }

  If an atom:entry element does not contain atom:author elements,
  then the atom:author elements of the contained atom:source element
  are considered to apply.  In an Atom Feed Document, the atom:author
  elements of the containing atom:feed element are considered to
  apply to the entry if there are no atom:author elements in the
  locations described above.
```

Figure 4. Excerpt from RFC 4287 (The ATOM Format)

Another common usage with ABNF is to reference rules across documents. This promotes reuse and reduces error. Figure 5 is an excerpt from RFC 6270 (the tn3270 URI scheme). It references back to RFC 3986 for a normative definition of the ABNF rule for authority.

```
The normative syntax of the ‘tn3270’ URI is defined in <tn3270-uri>
   ABNF [RFC5234] rule:

     tn3270-uri = “tn3270:” “//” authority [“/”]

   where the <authority> rule is specified in RFC 3986 [RFC3986].
```

Figure 5. Excerpt from RFC 6270 (the tn3270 URI Scheme)

As of this writing, there is no standard for a JSON DDL. Having one ... would benefit software developers when they write test suites.

A DDL with this feature provides the same benefit as we see with ABNF. And while this is also possible with prose, it is much more precise and concise when referencing specific rules.

Conclusion

As of this writing, there is no standard for a JSON DDL. Having one (or more—there is no harm in giving specification authors a choice) would benefit software developers when they write test suites. It would also make for better RFCs, as definitions would be more precise. On top of this, I believe JCR has many properties that flow more naturally with the style in which RFCs are written.

If you are writing or plan to write a specification using JSON, I invite you to take a look at both JCR and JSON Schema.

HOW THE IETF HELPS EMERGENCY CALLS SAVE LIVES

By Brian Rosen

IN LATE 2004, MEMBERS OF THE SESSION INITIATION PROTOCOL (SIP) WORKING group (WG) gathered to discuss how SIP-based devices could place emergency calls (e.g., 1-1-2, 9-1-1). Around the same time, SIP-based phones started making such calls. In the case of North America, the calls were received with concern at public safety answering points (PSAPs, the call centers where emergency calls are answered). The concern stemmed from the fact that neither the devices nor the back-end systems that supported them were capable of adequately placing the calls or sending the information needed to correctly route them. North American PSAPs had recently settled a related issue with mobile operators: while no one anticipated that mobile phones would be used for emergency calls, users found their mobile phones were perfect for them. And because mobile phones and their systems were unprepared to handle such calls, when they were made problems ensued. Ultimately, regulation prompted the ability of mobile phones to support emergency calls. The SIP members realized that handling emergency calls properly would be a critical step in order for SIP to succeed as a multimedia session-initiation protocol.

Many of the standards that governed how emergency calls are handled in the United States and Canada come from the North American Emergency Number Association (NENA). In spring 2005, the SIP members met with NENA's technical people to discuss how the existing emergency call system worked. They were surprised to learn that in addition to seeking a way to correctly handle VoIP calls in the current E9-1-1 system, NENA sought a redesign of the entire emergency call system based on modern IP protocols and mechanisms. The result of that meeting was a three-pronged plan:

1. NENA would document several ad hoc mechanisms that VoIP providers had implemented, and detail the strengths and weaknesses of the ideas.
2. NENA would standardize a method for SIP-based VoIP phones to place emergency calls using the current telephone network-based system. The IETF would assist with any needed SIP standards.
3. The IETF would work with NENA to create a new IP-based emergency calling system for North America with IETF standards as the base and NENA standards built on top of the IETF standards.

While no one had anticipated that mobile phones would be used for emergency calls, users found their mobile phones were perfect for them.

Their efforts have been largely successful. NENA i2 standards now largely govern VoIP emergency calls on the existing E9-1-1 network. No significant work in the IETF was required to achieve this goal. NENA i3 standards, based on several IETF standards in the now concluded GEOPRIV WG and the still active ECRIT WG, form the technical base for the Next Generation 9-1-1. And the European Union Emergency Number Association (EENA) has developed its standards based on NENA and IETF standards for new pan- European Union 1-1-2 IP-based emergency calling.

One of the core standards that underpin these developments is RFC 5222, the "Location to Service Translation (LoST)"

Continued on next page

Photo by Olaf Kolkman

How the IETF Helps Emergency Calls Save Lives, continued

protocol. LoST accepts location information typically extracted from a Presence Information Data Format-Location Object (PIDF-LO), RFC 4119, which may be a civic (street) address or a latitude/longitude/altitude. LoST then maps that location information into a route the emergency call should take towards a PSAP. LoST is also used to validate a civic location prior to it being loaded into a Location Information Server (LIS). In this way, if an emergency call is subsequently placed by a SIP-based phone using the location associated with the phone stored in the LIS, that location will be recognized by emergency authorities, the call will route correctly, and responders can be directed to the location of the caller.

The entire NG9-1-1 system is based on emergency calls being routed by LoST and calls accepted by the PSAP being SIP-signaled. Calls that originate in legacy wireline or wireless networks are passed through a Legacy Network Gateway to translate the legacy signaling and routing information to SIP signaling and LoST-based routing.

The [LoST] protocol is an unheralded IETF success.

The framework for how multimedia emergency calls are handled on the Internet is described in RFC 4883. RFC 6881 describes the best current practice for originating devices and networks to obtain the location of a caller, access a LoST server to get a route, and send a call using SIP signaling towards the PSAP.

Next Generation 9-1-1 is being deployed, albeit slowly. In a small number of U.S. states, emergency calls are being routed by LoST. The protocol is an unheralded IETF success—there are dozens of interoperable implementations, it's deployed, and thousands of emergency calls are routed every day using the LoST protocol.

Emergency authorities, organizations like NENA and EENA, and callers who need help rely on IETF protocols, frameworks, and data structures to save lives. And we can trace the entire effort to a single meeting between a dedicated cohort of IETF members and NENA participants, who had a vision of what could be done and then did it.

SPECIAL-USE DOMAIN NAMES: A REGISTRY UNDER REVIEW

By Peter Koch

IN OCTOBER 2015, JUST PRIOR TO IETF 94, PUBLICATION OF "THE .ONION Special-Use Domain Name" (RFC 7686) put an end to intense debate within the Domain Name System Operations (DNSOP) working group (WG) and the wider IETF community. RFC 7686 added the "onion" label to the Special-Use Domain Names registry[1] maintained by the Internet Assigned Numbers Authority (IANA). This was the second addition to that registry after RFC 6762 to reserve "local" for the Multicast DNS protocol.

A blog post[2] by IETF Chair Jari Arkko explained the details and external dependencies of the Certificate Authority system that led to the approval, while also suggesting that the registration procedure laid out in RFC 6761 needed review and action.

The first and last time that the IETF reserved top-level domain names under its formal standardization process was in 1999, when RFC 2606 reserved "test", "example", and "invalid", for test and documentation purposes and "localhost" to document operational practices. This was done in light of the recently founded Internet Corporation for Assigned Names and Numbers (ICANN) opening the first round of top-level domains.

A few months later and within the same historic context, the Internet Architecture Board (IAB) published "IAB Technical Comment on the Unique DNS Root" (RFC 2826) and the "Memorandum of Understanding Concerning the Technical Work of the Internet Assigned Numbers Authority" (RFC 2860) was achieved between the IETF and ICANN. The following excerpt from the Memorandum clearly separates the roles regarding domain names:

> 4.3. Two particular assigned spaces present policy issues in addition to the technical considerations specified by the IETF: the assignment of domain names, and the assignment of IP address blocks. These policy issues are outside the scope of this MoU.
>
> Note that (a) assignments of domain names for technical uses (such as domain names for inverse DNS lookup), (b) assignments of specialized address blocks (such as multicast or anycast blocks), and (c) experimental assignments are not considered to be policy issues, and shall remain subject to the provisions of this Section 4. (For the purposes of this MoU, the term "assignments" includes allocations.)

> In the event ICANN adopts a policy that prevents it from complying with the provisions of this Section 4 with respect to the assignments described in (a) – (c) above, ICANN will notify the IETF, which may then exercise its ability to cancel this MoU under Section 2 above.

Another year later, in September 2001, the ARPA top-level domain, initially named after the Advanced Research Projects Agency (ARPA) was renamed the Address and Routing Parameter Area Domain and the IAB took responsibility and published a registration policy in RFC 3172.

In 2011, the DNSOP working group published "Locally Served DNS Zones" (RFC 6303) to establish an IANA registry of DNS zones that every recursive resolver should serve from local knowledge, instead of following the normal DNS delegation path. The registry was seeded with various domains in the IN-ADDR.ARPA and IP6.ARPA reverse mapping space, particularly for private addresses of RFC 1918, where there cannot exist a globally unique mapping due to multiple independent instances of the same IP address. This was done primarily to reduce the DNS load on the sacrificial servers of the so-called AS112 project. The domains reserved in RFC 2606 deliberately were not imported into the new registry.

In early 2013, the IETF published "Special-Use Domain Names" (RFC 6761), which established a new registry quite similar to that initiated by RFC 6303. Names (and their descendants) in the new Special-Use Domain Names registry would be considered non-DNS names and their resolution would be redirected to other mechanisms before they were fed into the local DNS resolver:

> [...] Hence, the act of defining such a special name creates a higher-level protocol rule, above ICANN's manage-ment of allocable names on the public Internet.

In other words, these names would be greyed out of the Domain Name System and thus any registration within the DNS would not make sense, since compliant resolvers would never even try to resolve them the generic way.

[N]either "local" nor any other TLD will be subject to a DNS delegation in the public DNS tree.

RFC 6762, specifying Multicast DNS, then added the "local" TLD to the new registry that had been seeded with domains from RFC 2606. It should be noted that neither "local" nor any other TLD will be subject to a DNS delegation in the public DNS tree. Quite the opposite: it is expected that presence in the Special-Use Domain Names registry will prevent any such delegation.

Several questions arose around the procedure in RFC 6761, some of which will require wider community discussion:

- **Is the registration available for protocols not under IETF change control?** RFC 6761 specifies *Standards Action* or *IESG Approval* as the registration policy for Special-Use Domain Names, where RFC 5226 states that the latter should be a rare exception to the former only. How should the eligibility criteria for non-IETF protocols be defined?
- **Are the seven questions meant as criteria or as directions?** RFC 6761 gives seven different entities that may need to implement special treatment of a Special-Use Domain Name, including application software, stub and recursive resolvers, and authoritative DNS servers. It also suggests that if there is no special handling by any of the seven, the registration might not be useful. However, no guidance is given to assess treatment of how many of the entities ought to be necessary or sufficient for registration and what alternate approaches might be chosen.
- **Can the Special-Use Domain Names registry keep its promise?** Following from the previous question, how would software compliant with RFC 6761 learn the existence of a future Special-Use Domain Name and the special handling required? This is even more important if leaking DNS queries into the Internet is to be avoided for security reasons, as in the case of "onion".
- **How will consistency with RFC 2826 and RFC 2860 be maintained?** Can the emerging view of the existence of domain names that are not DNS names be made consistent with the uniqueness postulate expressed in RFC 2826? What mechanisms exist or need to exist to avoid conflicts between registrations under RFC 6761 and (future) ICANN TLD application rounds?

Since names have a tendency towards controversy, there are also the questions of who is going to determine the exact name at what stage in the process and whether a whole subtree of the DNS could be safely set aside for the intended purpose. The risk for the IETF is that it might find itself entangled in a mesh of legal and economic challenges without access to the resources necessary to inform or defend its decisions.

A detailed discussion will take place in the DNSOP WG. In addition, the ARCING BoF will address the question of signaling other resolution contexts beyond the Internet's Domain Name System.

Footnotes

1. http://www.iana.org/assignments/special-use-domain-names/special-use-domain-names.xhtml#special-use-domain.
2. https://www.ietf.org/blog/2015/09/onion/.

IETF 94 HACKATHON: OPEN SOURCE AND OPEN STANDARDS

Originally posted by Charles Eckel in the DevNet Open Source Community on 12 November 2015.

YOKOHAMA, JAPAN, WAS THE HOST CITY FOR IETF 94. THE IETF HACKATHON, sponsored by Cisco DevNet, got things started the weekend prior: 31 October–1 November. The Hackathon was the third in a continuing series designed to advance the pace and relevance of IETF standards activities by bringing the speed and collaborative spirit of open source software into the IETF.

More than 70 developers came together to test experimental protocols, produce reference implementations, create useful utilities, and so forth. Many participants were long-time IETF contributors; there also were several first-time attendees and young developers with new ideas, including our youngest coder at 16 years of age.

Hackathon participant Mahesh Jethanandani, Cisco Systems, reports for his team.

Participants formed into roughly a dozen teams working across a wide range of technologies. These included many IETF working groups (e.g., DANE, DHC, DNSOP, DPRIVE, HOMENET, I2RS, IPTUBE, NETCONF, NETVC, and SFC) and corresponding open source projects (e.g., Dalla, GETDNS, Kea, OpenDaylight, OPNFV, RIOT, and Thor). Each team produced significant results, including the DNS privacy and security team that extended and demonstrated use of getdns APIs to eliminate metadata leakage; and the Homenet team, which prototyped and demonstrated a provider-aware selection of IPv6 prefixes for home routers, PCs, and mobile devices.

Sunday afternoon, each team shared accomplishments and lessons learned with peers and a panel of esteemed judges.

How an IETF Hackathon Works

The Hackathon started Saturday at 09:00. Technology "champions" introduced each technology and proposed projects. Next, champions and participants formed teams and started hacking. Several teams included members from more than one IETF working group and/or open source community. The ensuing collaboration, mix of cultures and ideas, and new friendships all point to the long-term benefits that extend beyond the Hackathon itself.

Motivated, caffeinated, and energized, participants worked tirelessly, advancing the standards that provide the Internet's foundation and creating open source implementations that validate these standards and make them easier for others to consume. Not everything worked according to design and there were frustrating moments, but course correction and eventual success ruled the day.

Sunday afternoon, each team shared accomplishments and lessons learned with peers and a panel of esteemed judges: Jari Arkko (IETF chair), Ray Pelletier (IETF administrative director), and Adam Roach (NETVC chair). The judges recognized teams based on various criteria established for the Hackathon:

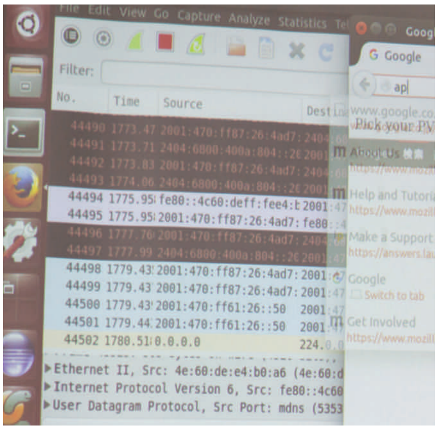
- Advance pace and relevance of IETF standards
- Bring speed and collaborative spirit of open source software into the IETF
- Expand upon ideas, feed into Working Group sessions
- Produce sample code/reference implementations
- Create useful utilities
- Attract developers, young people to IETF

There were techie prizes compliments of Cisco DevNet and tickets to the IETF social event donated by WIDE, but the real winner was the IETF community. The hackers' efforts were shared in corresponding working group meetings the following week and a number of teams demonstrated their work at Bits-N-Bites on Thursday night.

A complete list of this and archived Hackathon technologies and projects are available on the event Wiki (https://www.ietf.org/registration/MeetingWiki/

Hackathon participant Allison Mankin, Verisign, reports for her team.

Photos by Charles Eckel



wiki/94hackathon), which is accessed from the main Hackathon page (https://www.ietf.org/hackathon/). The IETF and open source communities are encouraged to bookmark and reference these sites to help with their ongoing work.

Next Steps

For the first time ever, the IETF is going to South America! IETF 95 will be held in Buenos Aires, and the Hackathon will kick things off the weekend prior: 2–3 April. Mark your calendars and join us as we accelerate the pace and relevance of the IETF's tireless work of extending and improving the Internet we all know, love, and use every day.

Stay informed

To keep up to date with all things related to past and future Hackathons, subscribe to hackathon@ietf.org.

> **The hackers' efforts were shared in corresponding working group meetings the following week and a number of teams demonstrated their work at Bits-N-Bites.**

> **[C]hampions and participants formed teams and started hacking. Several teams included members from more than one IETF working group and/or open source community. The ensuing collaboration, mixing of cultures and ideas, and new friendships all point to the long-term benefits that extend beyond the Hackathon itself.**

Participants at the third IETF Hackathon working together.

Photos by Charles Eckel

SUPA HELPS TO SIMPLIFY SERVICE MANAGEMENT

By Yiyong Zha, Dan Romascanu, Nevil Brownlee, Daniel King, and Tina Tsou

SIMPLIFIED USE OF POLICY ABSTRACTIONS (SUPA), A NEW WORKING GROUP (WG) in the OPS Area, held its first meeting at IETF 94. The rapid growth of traffic flowing over service provider networks brings new challenges in network operations and management applications. Policy-based service management is one efficient approach that uses policy rules to manage the behavior of one or more managed entities. Unlike conventional policies, which are interpreted into devices as ACLs (Access Control Lists) and packet filters, SUPA introduces policies at the service-management level. More specifically, SUPA works on policy models, but not policy content. Operators can use the policy model to define their policies at a different abstraction level.

Introducing the SUPA Demo

Photo contributed by the authors

The SUPA WG's History and First Session

The first IETF activity to propose policy abstractions to help simplify service management, SUPA made its initial call for interest at IETF 91, where it held a bar-BoF, followed by BoFs at IETF 92 and 93. During the second BoF session, more than ten operators supported the work and were willing to use this mechanism with standardized policy models. After public and Internet Engineering Steering Group (IESG) reviews the WG was created before the 94th meeting and held its first session in Yokohama.

Chaired by Daniel King and Nevil Brownlee, the first meeting focused on four topics: SUPA's value, the policy-information model, the policy-data model, and applicability. There was also discussion about the possibility of using the SUPA policy model to guide specific policy design in routing systems. Finally, a SUPA policy engine demo was prepared for Bits-N-Bites.

During the WG meeting, Maxim Klyus introduced the value proposition of the SUPA work. For example, the Interface to the Routing System (I2RS) WG is considering whether the SUPA policy framework can be used to benefit I2RS. John Strassner presented a generic policy-information model that defines a common set of terms independent of protocol and technologies. A key point of the work is knowing how to use the information model to design data models. Michiaki Hayashi presented the current status of the event-condition-action policy-data model, the key component of deliverables in the current charter. Audience feedback indicated that one measure of success is whether operators can use the policy model to handle service management. The chair and Area Director encouraged more operators to get involved with the design of the policy-data model.

SUPA works on policy models, but not policy content.

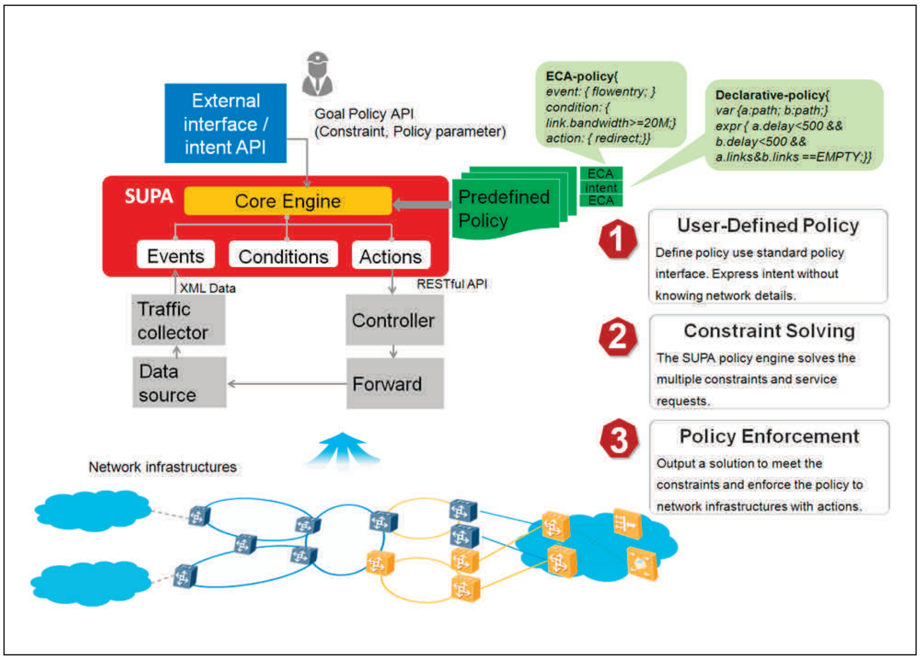


Figure 1. Setup of the SUPA Policy Engine Demo

Another interesting aspect of the SUPA WG is the implementation and possible contribution to the Open Source community. Yiyong Zha introduced a policy engine demo which focused on building

> **Another interesting aspect of the SUPA WG is the implementation and possible contribution to the Open Source community.**

a working system to take a policy and translate it into configuration changes.

SUPA's Bits-N-Bites Demo

A SUPA policy engine was demonstrated in Bits-N-Bites. The demo presented VPN service management in a packet transport network with a demo topology including 5000 nodes (Figure 1). In this schematic, the user of the external API selects the policy model and defines the policies, and the policy engine derives the policies using a constraint solver. Information from the network infrastructure devices is also needed to evaluate the policies and make the configuration changes. For a VPN service with connectivity from node A to node B, the user may want the connection to have two paths: a main path and a backup path. In reality, the user may want the two paths to be disjoint for resilience purposes. The user will express the policy of two disjoint paths using the given policy models and then the policy engine will find two disjoint paths and do the rest. Note that the user does not need to know the details of the path computation and network infrastructure, the user only expresses the policy using policy models. The policy models decide the level of abstraction to meet the user's needs.

Acknowledgements

This work has benefited from the reviews, suggestions, comments, and proposed text provided by the following individuals: Juergen Schoenwaelder, John Strassner, and Liya Zhang.

References

1 Maxim Klyus, John Strassner, SUPA Value Proposition, draft-klyus-supa-proposition-02 (work in progress), July 2015.

2 John Strassner, Generic Policy Information Model for Simplified Use of Policy Abstractions (SUPA), draft-strassner-supa-generic-policy-info- model-01 (work in progress), July 2015.

Q&A ON THE SUPA DEMO

Was the demo based on the SUPA drafts?

Yes, the demo was based on the SUPA framework as described in draft-klyus-supa-proposition[1]. The policy engine's role is to perform the policy translation. The policy model used here follows the style in the policy model draft[2].

Why was it called policy-based service management?

The user needs only to express its policy using the given policy model for the policy engine to generate the configuration change. There is no need to rewrite the code for different policy needs. For example, a user can set up a VPN connection with more than two pairs of disjoint paths by simply changing the policy.

Was it only used for path changes in VPN management?

Not really. The policy model is defined for one problem domain, but anything that can be expressed via the policy model is supported for more than only VPNs. However, we are working on more problem domains, such as inter-datacentre traffic optimization, load balancing for NFV (Network Functions Virtualisation), and network operations, administration, and management (OAM).

Photo contributed by the authors

The Implementation Team and Draft Author Noriyuki Arai

INTERNET OF THINGS: STANDARDS AND GUIDANCE FROM THE IETF

By Ari Keränen and Carsten Bormann

A TRUE INTERNET OF THINGS (IOT) REQUIRES "THINGS" TO BE ABLE TO USE Internet Protocols. Various "things" have always been on the Internet, and general-purpose computers at data centers and homes are usually capable of using the Internet protocols as they have been defined for them. However, there is considerable value in extending the Internet to more constrained devices that often need optimized versions or special use of these protocols.

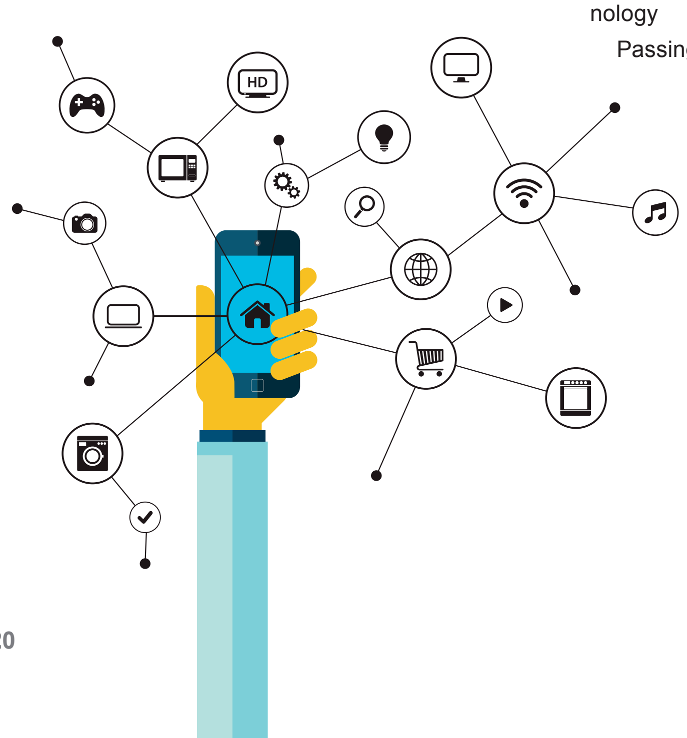
Background

During the past ten years there have been a variety of IETF activities initiated to enable a wide range of things to use interoperable technologies for communicating with each other—from quite small microcontroller-enabled sensors to large computers in datacenters.

When we wrote about IoT in the IETF Journal in 2010, there were three IETF working groups (WGs) focusing on IoT with constrained devices and networks: 6LoWPAN, which defined IPv6 adaption layer and header compression suitable for constrained radio links; ROLL, which focuses on routing protocols for constrained-node networks; and CoRE, which aims to extend the Web architecture to most constrained networks and embedded devices. The activity around IoT has increased since 2010 and today we have seven WGs actively looking into various aspects of IoT (an additional two are completed), as well as an Internet Research Task Force (IRTF) research group focusing on open IoT research issues.

IETF IoT Activities

The first IETF IoT WG, IPv6 over Low-power WPAN (6LoWPAN), was chartered in March 2005. It defined methods for adapting IPv6 to IEEE 802.15.4 (WPAN) networks that use very small packet sizes by means of header compression and optimizations for neighbor discovery. The 6LoWPAN WG concluded in 2014, and the 6Lo WG that replaced it applies similar adaption mechanisms to a wider range of radio technologies, including "Bluetooth Low Energy" (RFC 7668), ITU-T G.9959 (as used in Z-Wave, RFC 7428), and the Digital Enhanced Cordless Telecommunications (DECT) Ultra Low Energy (ULE) cordless phone standard and the low-cost wired networking technology Master-Slave/Token-Passing (MS/TP) that is widely used over RS-485 in building automation.



The Routing Over Low-power and Lossy networks (ROLL) WG produced specifications for both the RPL protocol "IPv6 Routing Protocol for Low-Power and Lossy Networks" (RFC 6550) and a set of related extensions for various routing metrics, objective functions, and multicast. Another output of ROLL was a number of requirements documents and applicability statements, a terminology document, and a security threat analysis.

The Constrained RESTful Environments (CoRE) WG is still one of the most active IoT groups. Its main output centers around the "Constrained Application Protocol" (CoAP, RFC 7252), a radically simplified UDP-based analog to HTTP. Extensions to CoAP enable group communications (RFC 7390) and low-complexity server-push for the observation of resources (RFC 7641). This is complemented by a discovery and self-description mechanism based on a weblink format suitable for constrained devices (RFC 6690). Current WG activities focus on extensions that enable transfer of large resources, use of resource directories for coordinating discovery, reusable interface descriptions, and the transport of CoAP over TCP and TLS. The CoRE WG is being rechartered to include RESTCONF-style management functions and publish-subscribe style communication over CoAP. CoRE is also looking at a data format to represent sensor measurements, which will benefit from the "Concise Binary Object Representation" (CBOR) (RFC 7049), a JSON analog optimized for binary data and low-resource implementations.

Since 2010, it has become clear that IoT will not work without good security. Accordingly, most new IoT WGs have been added in the Security Area. The DTLS In Constrained Environments (DICE) WG (already completed) produced a TLS/DTLS profile that is suitable for constrained IoT devices. The Authentica-

Since 2010, it has become clear that IoT will not work without good security.

tion and Authorization for Constrained Environments (ACE) WG is working on authenticated authorization mechanisms for accessing resources hosted on servers in constrained environments and a comprehensive use case document (RFC 7744) was recently completed. This work is supported by the recently chartered COSE WG that is building simplified CBOR analogs for the JSON object signing and encryption methods that were developed in the JOSE WG.

As a special development somewhat beyond the usual 6Lo work, the 6TiSCH WG (IPv6 over the TSCH mode of IEEE 802.15.4e) was chartered in 2014 to enable IPv6 for the Time-Slotted Channel Hopping (TSCH) mode that was recently added to IEEE 802.15.4 networks. This work aims to capitalize on the deterministic, real-time oriented features of TSCH, and includes architecture, information model, and configuration aspects. The 6TiSCH overview and problem statement document (RFC 7554) was published in 2015; a specification for a minimal configuration interface is next in line.

In addition to the new protocols and other mechanisms developed by IETF working groups, Internet protocols for constrained environments often benefit from additional guidance for efficient implementation techniques and other considerations. The Lightweight Implementation Guidance (LWIG) WG is working on such documents, including ones for CoAP and IKEv2 protocols, asymmetric cryptography, and CoAP in cellular networks. The LWIG WG published RFC 7228, which defines common terminology for constrained-node networks.

Beyond the IETF work specifically focusing on IoT scenarios, the whole Web protocol stack is evolving fast and many of the new technologies developed in other IETF working groups will likely end up being used also for IoT. The HTTPbis WG recently finalized the specification for the HTTP/2 protocol that is more suitable for IoT scenarios than earlier versions of HTTP, thanks to a more-compact wire format and simplified processing rules. The TLS WG is defining TLS version 1.3, including DTLS 1.3, which can establish secure transport sessions more efficiently and will therefore be better suited for IoT. The Homenet WG is working on enabling automatic configuration of IPv6 networks in homes and beyond. In parallel to IETF's standardization work, two IRTF research groups are of special interest: ICNRG (Information-Centric Networking) that explores the applicability of their technologies for IoT scenarios, and CFRG (Crypto Forum) that progresses advanced cryptographical foundations, such as new elliptic curve cryptography (ECC) curves that will be more appropriate for IoT use cases. Finally, the Internet Architecture Board (IAB) is organizing multiple related workshops (e.g., about security, architecture, and semantic interoperability) and has published informational documents such as "Architectural Considerations in Smart Object Networking" (RFC 7452).

While the IoT-oriented IETF working groups have already produced the first wave of mature standards for IoT, new research questions are emerging based on the use of those standards. The IRTF Thing-to-Thing Research Group (T2TRG) was chartered in 2015 to investigate open research issues in IoT, focusing on issues that exhibit standardization potential at the IETF. Topics being explored include the management and operation of constrained-node networks, security and lifecycle management, ways to use the REST paradigm in IoT scenarios, and semantic interoperability. There is also a strong interest in following and contributing to other groups that are active in the IoT area. For example, the W3C Web of Things (WoT) interest group recently began activities and the two groups have been working together to explore the future of IoT and Web technologies.

Conclusion

The IETF already has a decade of history specifying and documenting key IoT standards and guidance, and today there is more activity than ever around IoT. Other organizations and consortia working on IoT have adopted the Internet protocol stack as the basis of their solutions. IP and specifically IPv6 are the obvious choice for networking, but the rest of the IETF IoT stack, including CoAP and DTLS, are also widely used. The base IETF IoT protocol stack as published in RFCs today is mature and suitable for deployment. Additional needs are emerging for standardization, and the active groups at the IETF and the IRTF are working hard to ensure that they are identified and addressed.

While the IoT-oriented IETF working groups have already produced the first wave of mature standards for IoT, new research questions are emerging based on the use of those standards.

REFLECTIONS ON THE IETF 94 PUBLIC POLICY PROGRAMME

By Rinalia Abdul Rahim

IETF 94 IN YOKOHAMA WAS MY FIRST IETF MEETING. WHILE SUBSCRIBING TO specific Working Group lists offers exposure to the IETF's work, to obtain a true overview of how the organization works you must attend one of its meetings. The Yokohama meeting was my first such opportunity.

Quite a few people were curious about why I was there. As a relatively new Internet Corporation for Assigned Names and Numbers (ICANN) Board Member, I felt it was important to have a better understanding of the IETF, a key client of the Internet Assigned Numbers Authority (IANA) functions. I sought a better sense of the scope of the IETF's work, its priorities, community, and norms. The meeting in Japan was opportune in terms of timing and location.

Once at the meeting, I joined the Internet Society Public Policy Programme, for which I am extremely grateful. This programme provided crucial introduction and context for nontechnical participants who focus on policy matters. The Policy Fellows who convened in Yokohama came from Australia, Bhutan, Fiji, Japan, Kenya, Philippines, and Vanuatu. My participation brought Malaysia into the mix. It was a small group, designed for high interaction under the skilled guidance of Sally Wentworth, vice president of Global Policy Development.

Policy Fellows were introduced to both ISOC and IETF members and projects. Briefings covered topics such as IP addressing, DNS, IANA, routing, encryption, IXPs, interconnection, CSIRTs, as well as key programmes like Deploy360. IETF 94 hot topics were highlighted for our attention. I found the prominence of YANG modeling puzzling, but the rest of the hot topics fell within the range of my expectations. I was pleased to see the IETF continue its work on hardening the Internet and address issues of trust, identity, and privacy, while enhancing infrastructure resilience and security. New areas of work based on recent Birds of a Feather meetings (BoFs) also were flagged, including ISS, HOPSRG, NMLRG, HRPC, and T2TRG.

> **[T]he value of attending an IETF Working Group session was primarily in observing the interaction, dynamics, and norms.**

Policy Fellows had structured opportunities to interact with a select group of Working Group chairs and subject matter experts. Chairs of the IETF and the Internet Architecture Board (IAB) also popped by and discussions were lively and interesting. How the IETF deals with conflicts of interest, how it collaborates with other standards development bodies, and what progress has been achieved in enhancing the diversity of IETF participation were topics of interest to we Policy Fellows.

The IETF meeting schedule was woven into the Policy programme. Time slots were allocated for Policy Fellows to attend Working Group sessions. Before I arrived in Yokohama, I drew up a schedule of sessions I wanted to attend based on personal interest and suggestions from friends who are veterans of the IETF. The Policy programme made the following additional schedule-enhancing suggestions: RMCAT, NETVC, DPRIVE, V6OPS, ISS, HRPC, MODERN, IRTFOPEN and SIDR. Among the Working Group sessions that I attended, DNSOP distinguished itself in being the one with the most number of consensus-seeking hums.

The Policy Fellows were asked how we found the Working Group sessions. To my mind, the Policy Fellows were equally fascinated and frustrated by what they encountered. Without a technical background, it was extremely hard to understand the substance of Working Group discussions and to pinpoint the policy implications. The primary barrier was the technical vernacular. It did not matter how much one prepared ahead of time or how much material was read or whether one had followed the work in other spaces.

For us, the value of attending an IETF Working Group session was primarily in observing the interaction, dynamics, and norms. Understanding the policy implications and interacting effectively on those points require a dedicated forum where policy specialists can engage with technical people who can bridge the technical/policy language barrier. The Public Policy Programme was invaluable precisely for this reason: It provided a structured introduction to the IETF and its work, and it framed that introduction through a specialized lens for a policy audience. The programme could add further value by extending itself to provide a policy engagement platform on topics of interest beyond the meeting.

At the start of the meeting, it was impressed upon the Policy Fellows that at the IETF no one is in charge, anyone can contribute, and that everyone can benefit in the effort to make the Internet work better. I came away from the meeting thinking that there is truth to this, but to engage and contribute meaningfully there is a certain level of technical knowledge and language that is required. I also came away from the meeting with a deeper appreciation for the IETF and what it does. The breadth and depth of its work is challenging to absorb in one go, but it was clear that the work is essential to improving the Internet.

I took a bit of time in Yokohama to observe the IANA Team at work during the IETF meeting and to listen to feedback about them. It was evident to me that the IANA service and team were highly regarded and appreciated by the IETF community.

Overall, I had a great time at IETF 94. I found the meeting intellectually stimulating and I enjoyed interacting with the IETF community. People were wonderfully warm, welcoming, and helpful. The out-of-meeting activities were equally memorable: the coffee runs, the musical event at Minato Mirai Hall, and the meals with IETF friends. And who could forget the Cosmo Clock 21, the gigantic Yokohama Ferris wheel that added color to the night?

Cosmo Clock 21, the Yokohama Ferris Wheel

IRTF UPDATE

By Lars Eggert

DURING IETF 94 IN YOKOHAMA, FIVE OF the nine chartered Internet Research Task Force (IRTF) research groups (RGs) held meetings:

- Crypto Forum (CFRG)
- Information-Centric Networking (ICNRG)
- Network Function Virtualization (NFVRG)
- Network Management (NMRG)
- Software Defined Networking (SDNRG)

In addition to the meetings of those already chartered research groups, the following four proposed research groups met:

- Human Rights Protocol Considerations Research Group (HRPCRG)
- Thing-to-Thing Research Group (T2TRG). Related to Internet-of-things networking, this proposed RG held a longer meeting on the weekend before the IETF with the W3C Interest Group on Internet of Things.
- Network Machine Learning Research Group (NMLRG)
- How Ossified is the Protocol Stack? Research Group (HOPSRG)

Since IETF 94, both HRPCRG and T2TRG have been formally chartered. HOPSRG has been renamed and is now the proposed Measurement and Analysis for Protocols Research Group (MAPRG).

Prior to the IETF 94 meeting, the IRTF and the Internet Society held a workshop on Research and Applications of Internet Measurements (RAIM) in cooperation with ACM SIGCOMM. This one-day workshop was very well attended and helped to increase collaboration between industry and academia in the field of networking. For more information on the RAIM workshop, visit https://irtf.org/raim-2015/.

The IRTF Open Meeting included presentations from Xiao Sophia Wang on a systematic study of Web page load times using SPDY and comparisons with HTTP, and from Roland van Rijswijk-Deij on a detailed measurement study using a large dataset of DNSSEC-signed domains.

The nominations period for the 2016 ANRP awards is now closed. The ANRP is awarded for recent results in applied networking research that are relevant for transitioning into shipping Internet products and related standardization efforts. Everyone is encouraged to nominate relevant scientific papers they have recently authored—or read—for consideration for the award. Nominations for the 2017 awards will be accepted later this year. Please see https://irtf.org/anrp for details.

Stay informed about these and other happenings by joining the IRTF discussion list at www.irtf.org/mailman/listinfo/irtf-discuss.

APPLIED NETWORKING RESEARCH PRIZE WINNERS ANNOUNCED

By Mat Ford

2015 ANRP winners Roland van Rijswijk-Deij and Xiao Sophia Wang

Photo by Olaf Kolkman

THE APPLIED NETWORKING RESEARCH PRIZE (ANRP) IS AWARDED FOR recent results in applied networking research that are relevant for transitioning into shipping Internet products and related standardization efforts. The ANRP awards presented during IETF 94 went to the following two individuals:

- **Xiao Sophia Wang.** For a systematic study of Web page load times using SPDY (an open networking protocol developed primarily at Google for transporting Web content) and comparisons with HTTP.

  Read the full paper at http://homes.cs.washington.edu/~arvind/papers/spdy.pdf.

- **Roland van Rijswijk-Deij.** For a detailed measurement study on a large dataset of Domain Name System Security Extensions (DNSSEC)-signed domains.

  Read the full paper at https://conferences2.sigcomm.org/imc/2014/papers/p449.pdf.

Xiao and Roland presented their findings to the Internet Research Task Force (IRTF) open meeting during IETF 94.

Slides are available at https://www.ietf.org/proceedings/94/slides/slides-94-irtfopen-1.pdf and https://www.ietf.org/proceedings/94/slides/slides-94-irtfopen-0.pdf.

Thanks to Meetecho, audio and video from the presentations is available at http://recs.conf.meetecho.com/Playout/watch.jsp?recording=IETF94_IRTFOPEN&chapter=chapter_1 (from 00:10:49).

ANRP winners for 2016 also have been selected. The following winners will be the first to present their work at an IRTF meeting:

- **Zakir Durumeric,** a Google Research Fellow and PhD candidate in computer science and engineering at the University of Michigan. Zakir will present an empirical analysis of email delivery security.
- **Roya Ensafi,** a postdoctoral researcher at Princeton University. Roya will present an examination of how the Great Firewall of China discovers hidden circumvention servers.

The call for nominations for the 2016 ANRP award cycle is now closed. ANRP winners for 2016 will be announced prior to each of the three IETF meetings scheduled in 2016. Join the irtf-announce@irtf.org mailing list for all ANRP related notifications. Nominations for 2017 ANRP awards will open later this year.

IETF ORNITHOLOGY: RECENT SIGHTINGS

Compiled by Mat Ford

GETTING NEW WORK STARTED IN THE IETF USUALLY REQUIRES A BIRDS-OF-A-FEATHER (BoF) meeting to discuss goals for the work, the suitability of the IETF as a venue for pursuing the work, and the level of interest in and support for the work. In this article, we review the BoF that took place during IETF 94, including its intentions and outcomes. If you're inspired to arrange a BoF meeting, please read RFC 5434, "Considerations for Having a Successful Birds-of-a-Feather (BoF) Session."

Internet Storage Sync (iss)

Description: Network-based storage services that allow users to sync local files with remote servers on the Internet are getting more and more popular. They attract huge numbers of users and produce a significant share of Internet traffic. However, most of them employ proprietary protocols to achieve data synchronization. Such proprietary formats create challenges for users when they want to use multiple services or wish to share local files with users from other services. These proprietary sync protocols are also often inefficient and lacking in important collaboration features. The goal of this BoF meeting was to explore whether there is sufficient interest to work on this topic, the possible scope of work, and a plan for doing the work identified.

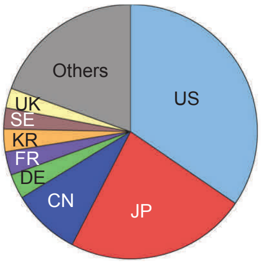
[Network-based storage services] attract huge numbers of users and produce a significant share of Internet traffic. However, most of them employ proprietary protocols to achieve data synchronization.

Proceedings: https://www.ietf.org/proceedings/94/minutes/minutes-94-iss

Outcome: The BoF meeting stimulated a wide-ranging discussion about the landscape of storage services, what could sensibly be standardized, and whether there were any incentives for storage providers to participate in a standardization effort. Further work is required to identify a clear use case for this work, and to narrow the scope to something that is both well understood and supported by a defined user community.

Japanese White-Eye (Zosterops japonicus)

IETF 94 AT–A–GLANCE



Participants: 1,320

Newcomers: 278

Number of countries: 52

IETF Activity since IETF 93 (19 July–1 November 2015)

New WGs: 6

WGs closed: 6

WG currently chartered: 146

New and revised Internet-Drafts (I-Ds): 1590

RFCs published: 88

- 55 Standards Track, 3 BCP, 4 Experimental, 26 Informational

IANA Activity since IETF 93 (July–September 2015)

Processed 978+ IETF-related requests, including:

- Reviewed 80 I-Ds in Last Call and 89 I-Ds in Evaluation
- Reviewed 79 I-Ds prior to becoming RFCs, 40 of the 79 contained actions for IANA

Added four new registries since IETF 93 (July–September 2015): tzdist-actions, tzdist-identifiers, ianastoragemediatype-mib, posh-service-names

SLA Performance (April–September 2015)

- Processing goal average for IETF-related requests: 98%

IANA and DNSSEC

- As of 30 October 2015, 920 TLDs have a full chain of trust from the root. http://stats.research.icann.org/dns/tld_report/.

RFC Editor Activity since IETF 93 (July–28 October 2015)

Published RFCs: 101

- 82 IETF (6 IETF non-WG), 3 IAB, 0 IRTF, 10 Independent

Revamped website

Responded to nine legal requests

RFC Format Project: The RFC Editor and the IESG are planning a staged approach to testing new features for RFCs.

- XML as the unchanging, underlying format
- TXT, PDF/A-3, HTML as the outputs
- SVG line art (black and white) allowed
- Non-ASCII characters allowed

Photos by Olaf Kolkman

IETF MEETING CALENDAR

For more information about past and upcoming IETF meetings visit **www.ietf.org/**.

IETF 96
Date 17–22 July 2016
Host Juniper Networks
Location Berlin, Germany

IETF 97
Date 13–18 November 2016
Host TBD
Location Seoul, South Korea

IETF 98
Date 26–31 March 2017
Host TBD
Location Chicago, IL, USA

IETF 99
Date 16–21 July 2017
Host TBD
Location Prague, Czech Republic

Special thanks for hosting IETF 94

WIDE PROJECT

The Internet Society Fellowship to the IETF, as part of the Internet Society Next Generation Leaders Programme, is sponsored by

Afilias Google Microsoft VERISIGN

This publication has been made possible through the support of the following Platinum Programme supporters of the Internet Society

Afilias CISCO Comcast ERICSSON Google ICANN IIJ Internet Initiative Japan Juniper Networks NBCUniversal NTT Communications RIPE NCC

IETF Journal
Internet Society
Galerie Jean-Malbuisson 15
1204 Geneva, Switzerland

Published three times a year
by the Internet Society.

Galerie Jean-Malbuisson 15
1204 Geneva, Switzerland

Email
ietfjournal@isoc.org

Find us on the Web
www.internetsociety.org/ietfjournal

Editor's Note
IETF Journal adheres to the *Oxford English Dictionary,* 2nd Edition.

pub-IETFJv11.3-20160310-en