

IETF[®] Journal



A report from IETF 97, November 2016, Seoul, South Korea. Published by the Internet Society in cooperation with the Internet Engineering Task Force.*

INSIDE THIS ISSUE

From the Editor's Desk.....	1
Nothing to Hide, Everything to Gain.....	1
Message from the IETF Chair ...	2
Words from the IAB Chair.....	3
Internet Society Panel: The I in IoT—Implications for a Global Open Internet.....	7
CodeStand: Connect, Network, and Support in One Location....	9
IAB Panel Explores Causes, Potential Remedies for Massive DDoS Attack.....	10
Working Group Update: Microwave Modelling at CCAMP.....	13
Working Group Update: Light-Weight Implementation Guidance.....	15
Working Group Update: Dynamic Host Configuration....	17
Grass-Roots Collaboration: Enterprise Data Center Operators Group.....	18
Today's IETF Leaders: Jari Arkko.....	20
Today's IETF Leaders: Alissa Cooper	21
IETF 97 Hackathon: Improving Open Standards Through Open Source.....	22
Internet Society Fellowship to the IETF Programme.....	25
ANRP Winners Announced	27
IRTF Update	28
IETF Ornithology: Recent Sightings	29
IETF 97 At-A-Glance	30
Calendar	31

FROM THE EDITOR'S DESK


By Mat Ford

THE IETF COMMUNITY MET FACE-TO-FACE FOR THEIR 97TH MEETING IN THE BUSTLING city of Seoul, South Korea. In this issue of the *IETF Journal* we provide a snapshot of some of the proceedings that made this another great meeting.

Our cover article is a manifesto of why Internet-enabled businesses should care about the open standards and open source communities. We present the first two of a series of interviews with IETF leadership: outgoing IETF chair Jari Arkko (page 20) and his successor Alissa Cooper (page 21).

Also in this issue, you'll learn about CodeStand, a new initiative that matches developers with coding projects related to IETF activity (page 9).

We have several Working Group and BoF updates, a summary of the pre-IETF Hackathon (page 22), and an article about the Internet Society briefing panel, "The I in IoT: Implications for a Global Open Internet" (page 7). Our regular columns from the IETF, IAB, and IRTF chairs, and coverage of the IAB technical plenary wrap up the issue.

We are hugely grateful to all of our contributors. Please send your comments and suggestions for contributions to ietfjournal@isoc.org. You can subscribe to hardcopy or email editions at <https://www.internetsociety.org/form/ietfj>. 

NOTHING TO HIDE, EVERYTHING TO GAIN

By Russ White and Shawn Zandi

WHY SHOULD A PROVIDER—PARTICULARLY A CONTENT PROVIDER—CARE ABOUT the open standards and open source communities? There is certainly a large set of reasons why edge-focused content providers shouldn't care about the open communities. A common objection to working in the open communities often voiced by providers runs something like this: Isn't the entire point of building a company around data—which ultimately means around a set of processing capabilities, including the network—to hide your path to success and ultimately to prevent others from treading the

Continued on page 4

MESSAGE FROM THE IETF CHAIR

By Jari Arkko

I WANTED TO SUMMARIZE MY THOUGHTS OF THE DISCUSSIONS AT IETF 97. WE HAD 1,042 people from 52 countries on-site in Seoul, very active development on a number of fronts, and overall a successful meeting!

The meeting was supported by our host Huawei, cohosts the China Internet Network Information Center (CNNIC) and the Korean Internet & Security Agency (KISA), and a long list of sponsors. Thank you for your support!

The topic of the meeting was, of course, Internet tech and its evolution. The two most active discussion topics were (1) the increasingly serious denial-of-service attacks that we are seeing, and (2) the development of a new transport protocol, QUIC, as an alternative to TCP and TLS and especially being more optimized for HTTP/2 usage.

The most recent denial-of-service attacks involved a number of compromised Internet of Things devices attacking DNS infrastructure. The Internet Architecture Board (IAB) organized a discussion of these attacks as an example of a more general concern: the addition of millions of new hosts has the capability to overwhelm the Internet infrastructure when those hosts misbehave. There are ways to mitigate the attacks, but not without impacts in other ways, such as finding it necessary to deploy your services on large providers.



Jari Arkko, IETF Chair

The most recent denial-of-service attacks involved a number of compromised Internet of Things devices attacking DNS infrastructure.

At the very least, I think it would be beneficial for the IETF community to continue to call attention to folks that the minimum bar, when introducing a large number of devices (or any device) to the Internet, includes things like automatic software updates and avoiding default passwords. I used to think this was so obvious that it needn't be said, but I'm not so sure anymore. Nevertheless, the area for us to have an impact is improving defense and mitigation mechanisms. See page 10 for a summary of the IAB plenary session or watch a video of the session at https://www.youtube.com/watch?time_continue=3715&v=qPaaRaNxIY4.

The IETF recently chartered a Working Group to specify QUIC (Quick UDP Internet Connections). This new protocol combines the TCP and TLS layers, is typically implemented in user space rather than kernel space, and aims for faster connection setups using resumption, integrated security, and capabilities to evolve the protocol faster (not being in the kernel).

A previous version of the protocol, already in use at Google, was taken as a starting point for discussion in the Working Group. I'm quite excited about this development, and eager to see where it takes us, and it seems that I'm not alone—the QUIC room was completely full.

Continued on page 6

The mission of the Internet Engineering Task Force is to make the Internet work better by producing high-quality and relevant technical documents that influence the way people design, use, and manage the Internet. See <https://www.ietf.org>.

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

IETF 97 WAS MY LAST MEETING AS INTERNET ARCHITECTURE BOARD (IAB) CHAIR AND IETF 98 will mark the end of my time on the IAB. From the start of my appointment, I hoped to achieve three things. The first was to strengthen the IAB's programs in relation to Internet architecture. The second was to sort out the IAB's role in the IETF's relationship with other organizations—what I sometimes describe as being the “foreign office” of the IETF. The third was to try to root out traces of the “great person” theory of IETF leadership. Now is a chance to reflect on how well that all worked.



Andrew Sullivan, IAB Chair

Architectural Oversight and Programs

The IAB organizes its long-term work into programs. Since the IAB is unlikely to have experts on everything, programs give the IAB a way to call on outside expertise when the organization needs it. In addition, programs enable an IAB member to engage with work that the IAB starts, even if that work might extend past the end of the member's term. While not every program is about architecture, the IAB should organize its architectural efforts into programs.

Perhaps inevitably, architectural programs have sometimes worked better in theory than in practice. In my view, they work well when there is at least one and preferably more than one IAB member highly engaged with the work of the program. In that case, it can be an effective amplifier of that interest and a way to get the IAB to contribute something useful to architectural discussion. But the IAB can sometimes keep alive a program that is not really working. Often, this is because the IAB recognizes that the topic is one that has big implications for the IETF, but either does not have any members with an abiding interest in the topic or does not have enough participants with enough time to engage with the program's needs.

We managed to close or reconstitute some programs that were no longer producing results. We increased the frequency of program reviews, and attempted to ensure that program leads were fully engaged by asking them to produce topics for the IETF technical plenary or Birds-of-a-Feathers (BoFs).

Over the course of my tenure, we did make some improvements in this area. We managed to close or reconstitute some programs that were no longer producing results. We increased the frequency of program reviews, and attempted to ensure that program leads were fully engaged by asking them to produce topics for the IETF technical plenary or Birds-of-a-Feathers (BoFs). But some programs floundered, and the floundering ones appear to be the ones least likely to schedule themselves for review.

Setting up a new program if there is energy is not hard. And, unlike IETF Working Groups, there is no particular procedural advantage to keeping a program around to “tidy up”. This suggests that the IAB might be better served by aggressive closing of programs on the principle that it is bad for the IETF to offer to do work and not complete it.

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 <https://www.iab.org>.

Nothing to Hide, Everything to Gain, continued from page 1

Isn't pushing modifications to an open source project or your ideas to the open standards community ultimately assisting potential competitors (new or established) in their efforts to build a bigger, better, faster network?

same path you've tread? Shouldn't providers defend their intellectual property for all the same reasons as equipment vendors?

To form an answer, it's important to begin by differentiating between *ownership* and *secrecy*. For any technology or innovation, there are two questions that need to be asked:

- Should we own this?
- Should we keep this a secret?

The questions are interrelated, but not identical. Ownership is generally related to controlling your own future. Specifically, owning your architecture means the ability to intertwine your network and your business in a way that leads to competitive advantage. In contrast, handing your architecture to a vendor (almost always) means sharing their business goals with yours in some (not always obvious) way.

On the other hand, secrecy is generally related to controlling the ability of others to use your innovations to compete with you. To rephrase the second question for the open communities: Isn't pushing modifications to an open source project or your ideas to the open standards community ultimately assisting potential competitors

(new or established) in their efforts to build a bigger, better, faster network?

With the questions clarified, there are two lines of argument for active participation in the open communities—for providers, vendors, and individual engineers. The first line of argument might be called *altruistic*, the second might be called *opportunistic*. And they are more closely intertwined than they might first appear.

First, every network engineer in the world should recognize that we are all “standing on the shoulders of giants.” The folks who did the initial work of defining the protocols that run the Internet and all of our networks, today, didn't just live off government funding. They built the companies that put their inventions into practice. From optics to protocols, these people didn't just invent things, and they didn't just build them—they built companies that capitalized on those inventions. In other words, they not only made themselves wealthier, they made the world wealthier, as well. At both a personal and corporate level, then, we need to offer our shoulders to future generations just as past generations have offered theirs to us. This means, in part at least, supporting open standards and open source as a natural part of building the products and companies we build now.

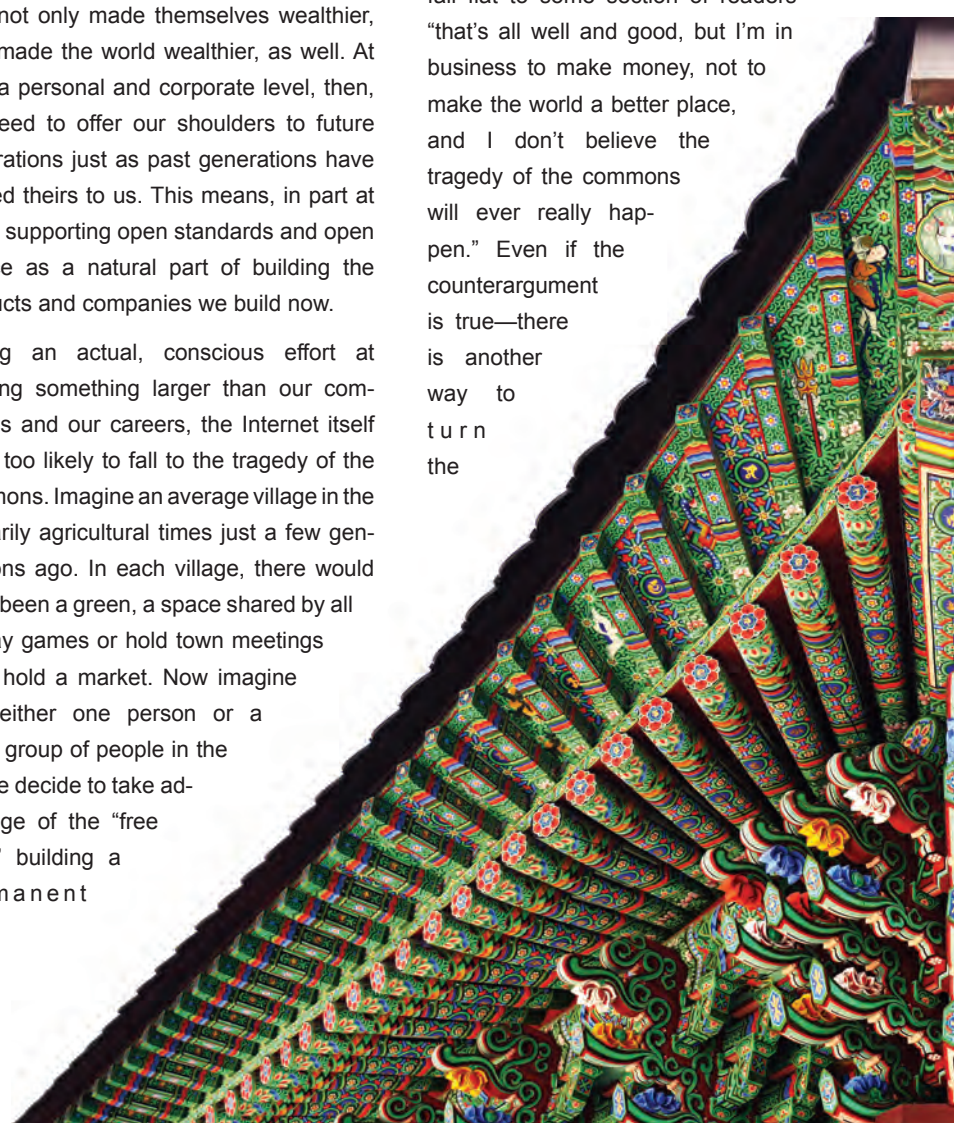
Failing an actual, conscious effort at building something larger than our companies and our careers, the Internet itself is far too likely to fall to the tragedy of the commons. Imagine an average village in the primarily agricultural times just a few generations ago. In each village, there would have been a green, a space shared by all to play games or hold town meetings or to hold a market. Now imagine that either one person or a small group of people in the village decide to take advantage of the “free land,” building a permanent

market in the space. The entire village has lost much to the gain of a few, but there's little that can be done. The commons are there to be used by anyone, after all.

We, as individuals and companies, want to make use of the commons—but we also need to expand the commons, lest they become ruined and the economic good they do for all, including ourselves, is removed to history. The commons of the digital world are not just the media we all share, but also the standards, source code, processes, and knowledge we have developed around building networked systems to solve problems at scale.

There is another point: where and how are the next generation of engineers going to learn to build networks at scale? If we abandon the commons the open communities represent, how will we build the engineers we need to expand the scope and scale of our companies and the Internet?

Perhaps these altruistic arguments will fall flat to some section of readers—“that's all well and good, but I'm in business to make money, not to make the world a better place, and I don't believe the tragedy of the commons will ever really happen.” Even if the counterargument is true—there is another way to turn the



argument. Participating helps the community, and it supports the creation of the products on which your company relies.

Consider the automotive market. What would have happened if there had never been, if there weren't today, people who take their cars out on their driveways and tinker with them? How many inventions would not have been invented, how many improvements left to the wayside? Would we still be able to buy a car in any color we want, so long as it is black?

The point is this: open communities are not only a place for creating, but also grounds for competing. The existence of the commons provides a basis for the competition that makes every piece of networking gear we buy better designed, better supported, and less expensive. When a market becomes fragmented enough that you either buy a single vendor or walk away, the market will no longer be useful for building the large-scale networks we use to build businesses. In the end, supporting open source and open standards

reduces operator's costs by increasing choice. Of course, the numbers here are impossible to quantify; perhaps something more concrete is needed to convince providers to participate.

For those
who are
still
not

convinced of the value of the open community, let me provide one more line of argument. Returning to the automotive market, suppose you were in the business of building a large delivery company. To build such a business, you need delivery vehicles. So you examine every delivery vehicle available and finally conclude that what you need to make your operations efficient doesn't yet exist. What are your options at this point?

One way might be to wave millions of dollars of contracts in front of a manufacturer. This would only get you so far, however, for there are competing customers, perhaps even regulatory agencies, that must be persuaded to allow the vehicle you're convinced you need to be built. But what if you were to work with other customers to develop a common core of features to which each of you could add, and around which you could all work with manufacturers and regulatory agencies to build the vehicle you need to build your business?

This common effort is precisely the open communities in the networking industry. Providers who participate in shaping open standards and open source not only help sway the market in their direction, they help build the foundations on which their businesses can be built. Further, the existence of the open community helps reduce dependence on any single vendor, thereby encouraging independence, which then feeds back into owning your own architecture.

To return to the initial question, of course there are things any provider will want to "hold back," to not share with the larger community. There is no definite line to be drawn in deciding what to hold back for business reasons, and what to share; any such line is likely to shift over time and space in ways that are hard to define. But "difficult to define" does not mean

"does not exist." Several questions might be helpful in this realm, including:

- Does this technology represent my core business?
- Is there the chance that sharing this technology will lead to enhancements that will accelerate my ability to build a great product? This is difficult to judge, because there is no way to know what sort of community might form in any specific case or what gains might be made.

Providers who participate in shaping open standards and open source not only help sway the market in their direction, they help build the foundations on which their businesses can be built.

While the answers to these questions may not be simple, we suggest tilting them in favor of the open communities rather than against. For instance, in the content provider space, the algorithms used to process data to produce the experience and information customers want would seem to be closer to the core of the business than how to build a network.

The long-standing ability of the open communities to improve on—and even revolutionize—ideas, adding value far above the investment, should convince every engineer and every company that relies on large scale networks of the open path.




Message from the IETF Chair, continued from page 2

Once again, the IETF Hackathon was running the weekend before the IETF. It was outstanding to see large student groups among the participants. A student team from SungKyunKwan University worked on the Interface to Network Security Functions (I2NSF) framework, for instance. They even had jackets made for the event! There was also a second large student team—on the other side of the world! The team from Université Catholique de Louvain worked on Multipath TCP, but much of their team did their work from back home in Belgium. See page 22 for more on the Hackathon.

Videos from IETF 97 sessions, interviews, and so forth are available as a YouTube playlist at https://www.youtube.com/playlist?list=PLC86T-6ZTP5gtLuoSjpTGO_mS5Ly2pflS. The official proceedings with slides, minutes, and everything else can be found at <https://datatracker.ietf.org/meeting/97/proceedings>. See also the blog post on routing area outcomes from IETF 97 at <https://www.ietf.org/blog/2016/12/reflections-on-the-routing-area-after-ietf-97/>, and the blog post from Srimal Andrahennadi from his experiences in participating as an Internet Society Fellow at the IETF at <https://blog.apnic.net/2016/12/14/ietf-97-fellowship-experience/>.

In addition to the Internet Society Fellows (page 25), a number of other gatherings happen during the week. The Internet Society also runs a Policy Fellows programme, with participants from regulators, governments, and other policy makers who do not usually attend technical conferences. Contact Konstantinos Komaitis at the Internet Society if you want to participate in this programme. The IEPG meeting on Sundays is a discussion among network operators. And the Systems Lunch gathers the women participants. Contact Allison Mankin at allison.mankin@gmail.com if you'd like to join them.

See you at IETF 98 in Chicago! 

Words from the IAB Chair, continued from page 3

The IETF Foreign Office

When I was appointed to the IAB, I thought we needed to tease apart the roles of the IAB and the Internet Engineering Steering Group (IESG). I believed the increasing external profile of the IESG and the IETF chair was risky for the IETF because of the role of the IESG in declaring IETF consensus. We have a hard time explaining rough consensus anyway, and there is some danger that people will mistake “IETF leadership” for people who are in control.

It is important that our leadership does not misunderstand itself as having control.

For better or worse, the Internet Assigned Numbers Authority (IANA) stewardship transition that happened during my IAB tenure gave me immediate exposure to the relationship between outside organizations and the IETF. It changed my mind about the “foreign office” approach. However we might like to organize ourselves and our work, most organizations are used to dealing with one another through the leadership. So, they want to talk to our leadership, even though our leaders are not really in control. We can either spend a lot of energy trying to change the way others understand us, or we can ignore the mismatch and try to achieve our more important goals. I have come around to the view that the second is more valuable.

The Community Is the Leadership


If our relationship to other organizations needs to conform to convention, then we must ourselves ensure that we do not allow that conventional mode of thinking to

undermine our own ways of working. It is important that our leadership does not misunderstand itself as having control.

One way of promoting that kind of thinking is to try to reduce the importance of the IAB chair and instead spread that work around. We have tried to do that. Communications from the IAB do not always come from the chair, but instead are sent by whichever IAB member leads the work in question. We separated from the chair some tasks that had previously come with the job, such as that of stream manager for the IAB's RFC stream. And, of course, the continued emphasis on programs means that there are more opportunities for the IAB to reflect views from outside itself.

There is still more to do here, however. Most worrisome to me is the linking of membership in the IETF Administrative Oversight Committee (IAOC) and the IETF Trust with the position of IAB chair. Not everyone who is chosen for IAB chair is likely to be the best candidate to work on issues for the IAOC or the IETF Trust. Because of the IANA stewardship transition, the Trust is more important than it used to be, and has a greater outward role than it originally had. I hope and trust that the “IASA 2.0” effort that the IETF has started will, among other things, permit greater flexibility in how those roles are filled.

Gratitude

In closing, I thank those who have been my colleagues on the IAB, and especially those who put their confidence in me by selecting me as their chair. I also thank my employer, Dyn, particularly for its steadfast support during the period when the IANA stewardship transition took much more time and work than forecast. And I thank the community for recommending me to the Nomcom for appointment and for the good counsel I received so often during my tenure. I am honoured to have served; I hope I have served you well. 

INTERNET SOCIETY PANEL: THE I IN IOT—IMPLICATIONS FOR A GLOBAL OPEN INTERNET

By Carolyn Duffy Marsan

WILL DEPLOYMENT OF INTERNET of Things (IoT) systems affect the open, global nature of the Internet? That was the topic of a panel discussion sponsored by the Internet Society and held in conjunction with IETF 97 in Seoul, South Korea.

Moderated by Olaf Kolkman, chief Internet technology officer for Internet Society, the panel explored the implications of IoT systems on the Internet itself. Panelists included Hannes Tschofenig of ARM Ltd., Carsten Bormann of Karlsruhe Institute of Technology, Erica Johnson of the University of New Hampshire's InterOperability Lab, Juan Carlos Zuniga of SIGFOX, and Michael Koster of the IoT Council.

Kolkman introduced the discussion by pointing out that the Internet is a global, general-purpose network that is accessible to all. He noted that the Internet is unique because it features permissionless innovation, which means anyone can deploy a new application. Further,

Panelists expressed concern that weak IoT deployments would denigrate the Internet's overall interoperability and accessibility.

it is based on interoperability, mutual agreement, and collaboration. Two other important aspects of the Internet are that it has reusable building blocks as its foundation and that it is constantly evolving, with no permanent favorites in terms of technology and business. Kolkman called these features "Internet invariants".

Kolkman asked the five panelists the following question: "What are the implications

of autonomous, always-on, connected, and often constrained devices on the global Internet from the perspective of the Internet invariants?"

Overall, panelists expressed concern that weak IoT deployments would denigrate the Internet's overall interoperability and accessibility. Further, they worried that problems with the performance or security of IoT devices could lead to additional government regulation, which would likely change the Internet's spirit of mutual agreement and collaboration.

"I think what we're looking at is a lack of confidence in IoT," Koster said. "The failures in confidence are the failures of integrity. What this requires is a clear notion of data ownership and a clear notion of where the policy control comes from."

Koster added that IoT represents a new paradigm for the Internet. Previously, the Internet depended on the deployment of a few extremely large websites. "Connected things are not going to get that much benefit from connecting to a massive website," he said. "Instead, connected things are going to drive scale at the edge of the networks."

Zuniga explained that IoT applications have been deployed successfully in industrial environments for years, but what's new is the range of consumer devices being connected to the Internet. "These are super-constrained, low-complexity devices," he said. "We need to be able to run generic IP services. I think this is key."

Bormann pointed out that IoT may result in government regulation of Internet-connected devices, which could affect the permissionless innovation aspect of the Internet. "Users may have a responsibility to run the Internet things responsibly," he said. "If I have a car, I have a responsibility to get the brakes fixed. That may be the kind of economic change that is coming."

The regulations may not be all bad, he added. "When I go to a restaurant, I like



Olaf Kolkman moderates the Internet Society's IETF 97 panel discussion.

Continued on next page

Internet Society Panel: The I in IoT—Implications for a Global Open Internet, continued



Erica Johnson, Internet Society panelist and director of University of New Hampshire's InterOperability Lab

that regulations mean that I'm not going to be poisoned," he said. "Things like UL Certification in the United States is something that will have to happen so that we have an understanding of what we would like these devices to do. As engineers, our end product is not technology; it is confidence."

Johnson said her lab has been conducting interoperability testing for several IoT providers, who are struggling with interoperability through home gateways and various access technologies. "They want to give their customers the user confidence and assurance about interoperability," she said.

One concern Johnson noted is that these IoT vendors don't seem to care about IPv6, the next-generation Internet Protocol that is critical to maintaining the open, end-to-end nature of the Internet.

"We have an opportunity to help educate the companies that are producing these products," she said. "By expanding IPv6 forums to include an IoT logo, we might be able to help give them that user confidence and assurance. We would include the most basic RFPs including 6LoWPAN. We would provide the tools and test specifications... to make it readily available and cost-effective to ensure interoperability."

Tschofenig agreed that the IETF has an opportunity to provide open source

protocol stacks to IoT developers to ensure that they meet the standards-based interoperability feature of the Internet.

"At ARM, we have an operating system, protocol stacks and security stacks. Hopefully IoT developers will be encouraged to use them, rather than write their own and introduce lots of security vulnerabilities into the architecture," he said.

The panelists agreed that the IETF and other standards bodies have been working on interoperable building blocks for IoT deployments, but that incompatibility remains a problem.

One concern Johnson noted is that these IoT vendors don't seem to care about IPv6, the next-generation Internet Protocol that is critical to maintaining the open, end-to-end nature of the Internet.

"The challenge has been to get [the standards] into the hands of the developers and have the developers implement them. The developers don't know how to use them," Tschofenig said.

Koster pointed out that there is a lot of fragmentation in the IoT standards space. "Lots of bodies are working on essentially overlapping and competing standards, and that has moved up to the data model

space," he said, adding that it is important for the IETF to work with other standards bodies to converge on a single set of IoT standards.

Bormann noted that both small and large companies are struggling with deploying IoT standards, but for different reasons. He says small companies often aren't educated about the importance or availability of interoperability standards. "We need to show people what's out there so they don't start building products with extremely shoddy protocols that are going to hurt them in the long run," he said. "At the other end of the spectrum, very large companies are seeing a way to build little monopolies and are not that interested in building a common substrate."

Bormann said he would like to see more open source offerings for developers that are essentially "IoT in a box".

Tschofenig added that what's needed are not only open source operating systems, IP stacks, and security, but also device management solutions. This will make it easier for IoT startups to create new products with solid IP deployments.

One outstanding issue is who will maintain IoT devices in the field. Panelists said that standards would allow third-party vendors to enter this market.

"If I hire someone to fix my car, they have to know how to handle my tires. There are standards in that space that make it relatively straightforward to handle different kinds of tires," Bormann explained. "So standard device management solutions and the security concepts required to make this work are really important to allow these companies to exist."

At the end of the discussion, Kolkman summarized that it appears the Internet invariants continue to matter in IoT deployments and that it is the responsibility of Internet stakeholders, including the IETF, to support these features as IoT evolves.



CODESTAND: CONNECT, NETWORK, AND SUPPORT IN ONE LOCATION

By Kathleen Moriarty, Lisandro Zambenedetti Granville, Charles Eckel, Jéferson Campos Nobre, and Christian O'Flaherty

THE IETF HAS RECOGNIZED THE NEED TO WORK CLOSELY WITH THE open source software movement. For an editor, running code is a requirement to move documents along the standards track. At the same time, open source repositories, such as github, have plenty of references to Request for Comments (RFC) and Internet-Drafts (I-Ds). Many of the coding efforts hosted in these open source repositories are carried out without support, test, or review from the IETF.

CodeStand provides the missing link that connects IETF documents and software implementations, both open source and proprietary. Authors of IETF documents can benefit from knowing about implementations of their proposals, and developers can receive support from experienced Working and Research Group participants (including authors), while they are creating code based on IETF proposals.

CodeStand acts as a marketplace, where authors and software developers—including industry professionals, students, researchers, and professors—can connect. It can showcase opportunities to develop running code for IETF protocols that can aid, for example, students in a class or researchers in projects, thereby lowering the entry barrier for IETF participation. When developers have questions about the protocol's operation, they may suggest changes that could be used to update documents to improve accuracy and interoperability for future implementations. Discussions to update a standard would still occur on the appropriate IETF mailing list, but CodeStand offers a way for those new to the IETF to more easily engage with other members.

CodeStand also can enable the promotion of opportunities sponsored by industry and support working with undergraduate and graduate-level students. Its unique structure introduces students to software engineering practices used in industry, while providing a networking opportunity for both students and industry participants.

In addition, it can help companies to identify talented resources via networking profiles.

How It Works

The tool (<https://CodeStand.ietf.org>) is linked with Datatracker. Opportunities to develop code for drafts or standards are

CodeStand provides the missing link that connects IETF documents and software implementations, both open source and proprietary.

listed as CodeRequests, which are established by a sponsor or mentor. Software developers can create projects and link them to a CodeRequest that already exists or, if no CodeRequest is available for those documents, developers can create a new project referencing the appropriate IETF standard(s) or I-Ds in development.

Software projects themselves are maintained externally to the IETF CodeStand site, either in code repositories (e.g., GitHub, SourceForge) or the tool of choice for that organization. CodeStand will provide a link to the project descriptions for proprietary implementations or the code repository for open source projects. Licensing and intellectual property rights




related to the code are provided by the project owner in their external code repository or description page.

How to Contribute

If you are an active IETF participant and are willing to mentor a software developer (as an author or supporting an existing document), create a CodeRequest volunteering yourself as the mentor. With your Datatracker user and password, log into CodeStand, and select "New Code Request" at the bottom of the CodeRequests list.

If you're a software developer and not yet a Datatracker user, create an account in Datatracker (<https://datatracker.ietf.org/>), log into CodeStand, and look for an appropriate CodeRequest. If there is no CodeRequest available to link your project, list all projects and select "New Project" at the bottom.

Give CodeStand a spin! See how its combination of IETF standards and open source software development can help you. 

Championing a project in an IETF Hackathon? Consider creating a CodeRequest to both get the word out and provide a home for the developed code beyond the single Hackathon. If you already have a CodeRequest in CodeStand, why not champion a project for it in the next IETF Hackathon?

IAB PANEL EXPLORES CAUSES, POTENTIAL REMEDIES FOR MASSIVE DDOS ATTACK

By Carolyn Duffy Marsan

JUST WEEKS AFTER A HEADLINE-GRABBING INTERNET INFRASTRUCTURE attack, the Internet Architecture Board (IAB) presented a timely and engaging technical talk to IETF 97 participants aimed at sharing the vulnerabilities associated with the massive cyberattack, as well as potential fixes that the standards body can pursue.

The IAB was preparing a different technical talk for IETF 97, but scrapped its plans after a large-scale Distributed Denial of Service (DDoS) attack harmed managed DNS infrastructure provider Dyn on 21 October 2016. Two aspects of the Dyn attack were unusual: first, the attack came from a botnet comprising Internet of Things (IoT) devices; and second, it was the largest attack of its kind in history.

The Dyn DDoS attack came in three waves over a six-hour period. Although Dyn says it never suffered a network-wide outage, the company's managed DNS infrastructure was slowed to the point where many of its customers—including marquee Internet brands such as Twitter, CNN, and Netflix—were unreachable.

In addition to creating a massive Internet disruption for customers, what made the Dyn DDoS attack newsworthy is that it involved tens of thousands of discrete IP addresses from the Mirai botnet, which comprises IoT devices. This foreshadows a future where more attacks are derived from IoT devices that are typically neither secured nor regularly upgraded.

"We are here to talk about a new class of attacks on the Internet architecture—or perhaps just some insights we hope are new," said IAB member Suzanne Woolf, who introduced the technical plenary. She said the Dyn DDoS attack "caused an explosion of attention on DNS, Internet of Things, mass compromise of Internet-connected devices, and the business and operational models underlying the provisioning of content at Internet scale."

The first speaker was Nick Sullivan, head of cryptography at Cloudflare and an active participant in the IETF's work related to

In addition to creating a massive Internet disruption for customers, what made the Dyn DDoS attack newsworthy is that it involved tens of thousands of discrete IP addresses from the Mirai botnet, which comprises IoT devices.

Transport Layer Security (TLS). He said what was unique about the Dyn DDoS attack was its magnitude.

"This is not something particularly new. Botnets exist and have existed for a long time," Nick said. "But this is an example of botnets at a larger scale, and they sent a mix of attacks."

Nick said the majority of DDoS attacks seen on the Internet in 2016 were known attacks—DNS floods, Syn floods and HTTPS floods—but that these attacks are now coming at a larger scale.

DNS attacks fall into two camps: direct attacks on the authoritative DNS server from a botnet or botnet attacks that go through valid recursors before they move to the authoritative DNS server.

For direct attacks, Nick recommended that DNS operators treat every request from an unknown resolver with suspicion and assume that a flood of requests from non-resolvers to an authoritative server is an attack. "Just drop the packets," he advised.

Nick said these floods are typically requests for an Apex Domain or random subdomains. He added that sometimes these floods come with spoofed source addresses, which are harder to handle.

"The Mirai botnets often are not spoofed addresses, which makes them slightly easier to deal with," he said.



Andrew Sullivan, IAB chair, addresses the IAB technical plenary at IETF 97 in Seoul.



Nick Sullivan, panelist and head of cryptography at Cloudflare, takes the podium at the IAB technical plenary.

When experiencing a DNS flood, you shouldn't advertise the IPs that are under attack as what's called "null-routing IPs," because it would cause them to fall off the Internet, Nick said. "This is a pretty dangerous thing to do, and it has lots of repercussions," he said. "Lately, attacks have been attacking entire subnets and that makes this entirely unreasonable as a defense mechanism."

Instead, Nick suggested spreading the load of the attack geographically with the Anycast protocol and across data centers with the equal-cost multipath (ECMP) routing protocol. He also recommended filtering packets as early as possible. "The main way to handle a large flood is to make sure that only legitimate applications get to your application," he said.

Nick recommended filtering traffic through iptables Berkeley Packet Filter (BPF) rules, which are powerful techniques for matching and blocking packets inside the kernel and can be automated. He admitted that the iptables BPF rules must be dynamic and use machine learning and heuristics to keep up with ever-changing attack profiles. "The attacks you see from one botnet are not what you're going to see from another, so this has to be very dynamic," he said. "If you have static rules, you are probably going to go down. If possible, move the rules outside of your server and into the Network Interface Card. This can help relieve the load."

Nick said that DNS floods that go through recursive servers are different types of attacks, and that network operators should answer these attacks rather than try to block and drop the traffic. That's because recursive DNS is making requests for legitimate customers at the same time as attackers. "If it's possible to whitelist known recursive DNS servers, do so," he recommended. "This is very helpful and the right thing to do."

He advised against rate limiting this traffic as it can cause negative effects including amplifying the attack. "Rate limiting is not a very effective method for this. Really, you have to handle the packets," he said.

Nick [Sullivan] suggested spreading the load of the attack geographically with the Anycast protocol and across data centers with the equal-cost multipath (ECMP) routing protocol.

One suggestion is taking advantage of NSEC, which is a feature of the DNS Security Extensions (DNSSEC) protocol that is used to prove a name doesn't exist. "Potentially caching this for nonsigned ranges might help," Nick suggested. "It's one of the many different options for keeping the traffic from going all the way through to the authoritative server."

With regard to battling Syn flood attacks, he said using BGP Anycast for TCP and establishing dynamic IPtables BPF rules can be effective.

For HTTPS floods, you can use the protocol's rate limiting features, which include

rate limiting by request or volume. He added that "a simple TCP reset will get you a long way."

Nick said that DDoS attacks are sent by botnets consisting of compromised endpoints, which are increasingly IoT devices. "We are in the early days of this new set of devices that are running software, and the software is getting old on a lot of these devices," he said, warning that the IoT-based botnet attacks are likely to get worse.

He explained that IoT devices are low-cost, low-margin devices and that manufacturers are not incentivized to build in security or even a method to upgrade the devices later in response to newfound vulnerabilities.

"Nothing about these attacks should be new to you," Nick told the audience. "We're dealing with the same problems, but now at a much larger scale, and it's exposing certain things about the Internet of Things that we've known."

The best advice that Nick offered was for network operators to stop bad traffic as close as possible to the entry point and to use Anycast. "Distribute the load and filter early," he advised.

He also noted that being able to stay online while experiencing a DDoS attack requires scale.

"You have to be big, you have to be smart, and you have to have the tools and to work together with other people to stop the attacks as close as possible to the edge," he concluded.

The second speaker at the technical plenary session was IAB chair Andrew Sullivan, Fellow at Dyn. Andrew said that the attack against Dyn's infrastructure was large in scale and that even the company's well-built Anycast-based DNS system couldn't withstand it without long latency and resolution failures.

Continued on next page

IAB Panel Explores Causes, Potential Remedies for Massive DDoS Attack, continued



Andrew Sullivan, panelist, IAB chair, and director of DNS engineering at Dyn, addresses the audience at the IAB technical plenary.

“We’ve seen lots of standard amplification attacks,” Andrew said. “This particular attack had a high proportion of TCP—we don’t normally see this. This was comparatively low spoofing. We have definitely confirmed 40,000 addresses involved in the botnet, although it may be up to 100,000.”

Andrew said he doesn’t believe that the Dyn DDoS attack was a one-time occurrence.

“There was a previous attack just a couple weeks before this that was very, very large,” he warned. “We know the Mirai botnet code is out there and is being improved upon by various people.”

Andrew said attacks of this type are ironic because they use the strengths of the Internet—its distributed nature, ease of attaching endpoints, and lack of intelligence in the network itself—to attack the Internet architecture. He said that the endpoints are supposed to be more intelligent than the network itself, but that this design philosophy isn’t true with IoT systems.

“It’s obvious that Internet of Things is going to continue to create these types of problems,” Andrew said. “It creates ubiquitous connectivity and very, very

Andrew [Sullivan] fears that attacks like the recent Dyn DDoS attacks could result in government regulations aimed at preventing compromised hosts from connecting to the Internet, which would reduce the openness of the Internet.

lightweight systems... If you have millions and millions of these devices all over the place, you will have lots of compromised hosts.”

Andrew fears that attacks like the recent Dyn DDoS attacks could result in government regulations aimed at preventing

compromised hosts from connecting to the Internet, which would reduce the openness of the Internet.

“We are the people who ought to tackle this problem because we understand the technology, we understand the incentives, and we understand the nature of the underlying architecture,” Andrew concluded. “I don’t have a magic solution, but I hope we can have an interesting and useful discussion.”

This technical talk was followed by a lively question-and-answer period that raised such suggestions as creating lightweight security protocols for IoT devices and otherwise advising endpoint manufacturers on how to build in security at a lower cost. The goal of these suggestions was for the IETF to find ways to make it easier and cheaper for people building IoT devices to have security by default.

At the panel’s conclusion, Suzanne said the IAB would continue this discussion online.

In other news, the Internet Society at this plenary session presented its Jonathan B. Postel Service Award to Kanchana Kanchanasut for her pioneering work in establishing Internet services in her native Thailand and across Southeast Asia. Kanchanasut receives a crystal trophy and US\$20,000. She is the 19th recipient of the award, which has been given since 1999.



2017 Jonathon B. Postel Award winner Kanchana Kanchanasut

WORKING GROUP UPDATE: MICROWAVE MODELLING AT CCAMP

By Jonas Ahlberg, Daniele Ceccarelli, and Fatai Zhang

MICROWAVE AND MILLIMETER WAVE (HEREAFTER COLLECTIVELY REFERRED to as *microwave*) technologies are becoming critical for radio access networks. These technologies are able to support cost-efficient delivery with the best possible network performance and quality of experience.

The main application for microwave is backhaul for mobile broadband. Today's microwave can fully support the capacity needs of backhaul in a radio access network. It is expected to evolve to support multiple gigabits in traditional frequency bands and beyond 10 Gbps in the millimeter wave. Layer 2 (L2) packet features are normally an integrated part of microwave nodes and more advanced L2 and L3 features will be introduced over time to support the evolution of transport services that will be provided by a backhaul/transport network.

In order to achieve operational support of seamless multilayer networking and automated network-wide provisioning and operation, there is the need for the unification of the control and management of microwave and millimeter wave radio link interfaces with the control and management of L2 and L3 capabilities.

To that end, the Common Control and Measurement Plane (CCAMP) Working Group (WG) established a Microwave Design team and challenged it with defining a unified YANG data model for microwave and millimeter wave radio links. The team aims to provide a standardized management model that:

- aligns with how other packet technology interfaces in a microwave/millimeter wave node are modeled,
- supports core parameters, and
- allows for optional product/feature-specific parameters that support new, innovative features until they are mature enough to be included in a standardized model.

The CCAMP Working Group established a Microwave Design team and challenged it with defining a unified YANG data model for microwave and millimeter wave radio links.

Currently, numerous IETF data models, Request for Comments (RFCs) and Internet-Drafts (I-Ds) comprise technology-specific extensions that cover a large part of the packet domain. Examples include IP Management [RFC 7277] and Routing Management [RFC 8022], which are based on RFC 7223, the IETF YANG model for interface management and an evolution of the SNMP IF-MIB [RFC 2863].

Since microwave nodes will contain more and more packet functionality that will then be managed using those models, advantages exist if radio link interfaces can be modeled and managed using the same structure and the same approach. This is particularly true for use cases in which a microwave node is managed as one common entity, which includes both the radio link and the packet functionality. All interfaces in a node, irrespective of technology, are then accessed from the same core model (RFC 7223) and can

be extended with technology-specific parameters in models that augment the core model.

There will always be certain implementations that differ among products. So it is important to focus on those parameters required to support the applicable use cases for centralized, unified, multivendor management, and to allow other parameters to be optional or to be covered by extensions to the standardized model.

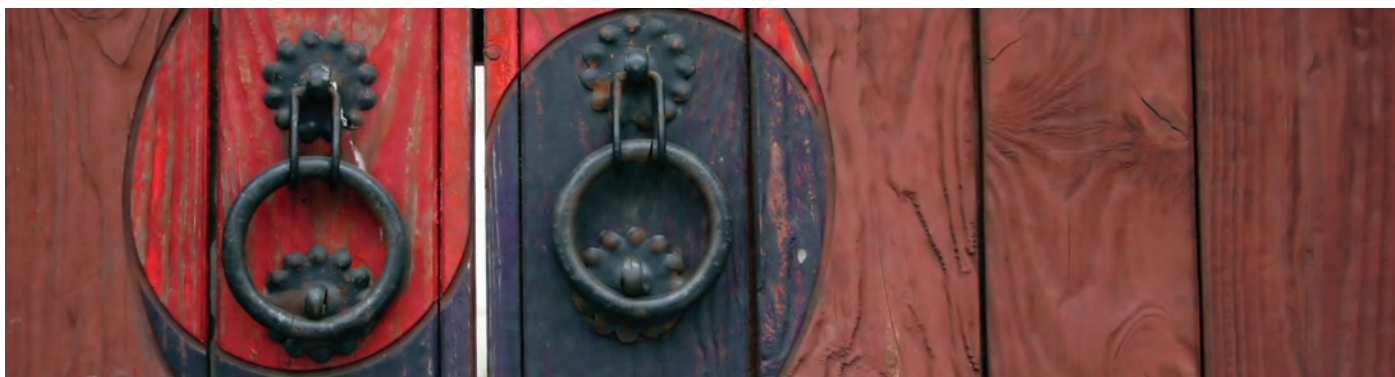
The Microwave Design team seeks consensus both within the industry and with other standards development organizations (SDOs) around one common YANG model, with respect to the use cases and requirements to be supported, the type and structure of the model, and the resulting attributes to be included.

Characteristics of the Model

Definition of the YANG model has begun and a second version of the draft was published on 23 December 2016. The model uses the structure of the IETF's Radio Link Model as its starting point, as that model provides the desired alignment with RFC 7223. For the definition of the detailed leafs/parameters, the model uses both the Radio Link Model and the Open Network Foundation's (ONF's) Microwave Model as its basis, plus includes new ones to cover identified gaps. The parameters in those models have been defined by both operators and vendors within the industry, and implementations of the ONF Model have been tested in proof-of-concept events in multivendor environments, thereby demonstrating the validity of the approach used. The model also includes data nodes to describe the interface layering for the capacity provided by a radio link, as well as the associated Ethernet and time-division multiplexing (TDM) interfaces in microwave nodes.

The model includes support for configuration of microwave specific alarms, but relies on generic models for notifications

Continued on next page



Working Group Update: Microwave Modelling at CCAMP, continued


and alarm synchronization. The same approach is chosen for the general functionality for physical/equipment inventory, which is not supported by the microwave model and instead relies on generic models.

Key Concepts of the Model

Carrier termination is an interface for the capacity provided over the air by a single carrier. It is typically defined by its transmitting and receiving frequencies. Radio link terminal is an interface providing packet capacity and/or TDM capacity to associated Ethernet and/or TDM interfaces in a node. It also is used for setting up a transport service over a microwave/millimeter wave link. Figure 1 illustrates these carrier termination and radio link terminal concepts.

Figure 2 shows the overall structure of the model with radio-link-terminal and carrier-termination, plus three new containers that describe the relationship and interaction between the carrier terminations in more detail: radio-link-protection-groups, xpic-pairs, and mimo-groups.

Next Steps

The Microwave Design team created a draft of the unified YANG Data Model for microwave and millimeter radio link, draft-mwdt-ccamp-mw-yang, and it now seeks feedback from and anchoring with a broader industry audience. 

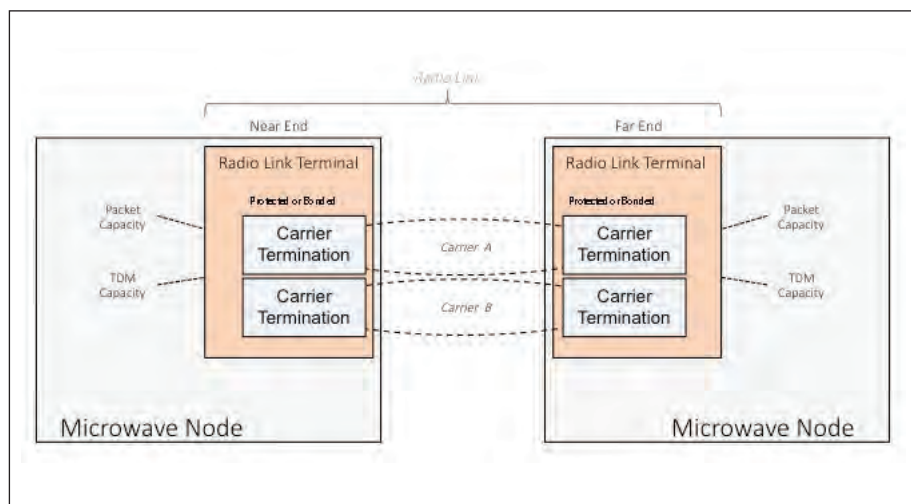


Figure 1. Radio Link Terminal and Carrier Termination

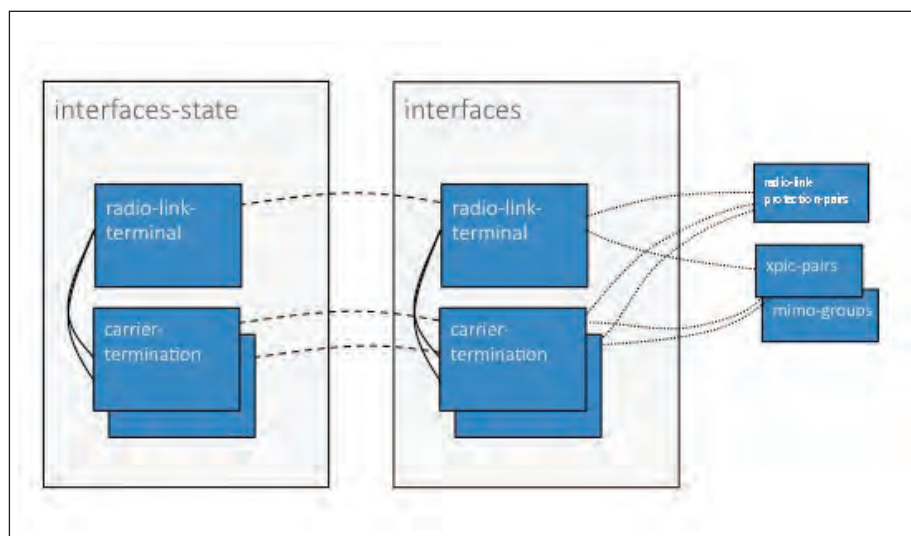


Figure 2. Overall Structure of the Model

WORKING GROUP UPDATE: LIGHT-WEIGHT IMPLEMENTATION GUIDANCE

Building Minimal yet Interoperable IP Stacks on Tiny Devices

By Zhen Cao

BUILDING MINIMAL YET INTEROPERABLE IP-CAPABLE DEVICES FOR THE most constrained environments isn't easy. The IETF, as the home community for sharing engineering experiences, observed this issue and, in response, chartered the LWIG (Light-weight Implementation Guidance) Working Group (WG) to collect the implementation experiences of IP stacks in constrained environments.

Background

Lower-power and constrained devices connected with lossy links are increasingly seen in today's Internet. Ensuring that these devices are IP-capable is critical to avoiding a fragmented Internet. Before the LWIG WG, the IETF was working on light-weight IPv6 (6Lowpan WG, now continued by 6Lo), routing protocols (ROLL WG) and constrained application protocols (Core WG). This work has helped move constrained networks toward global interconnectivity (Figure 1).

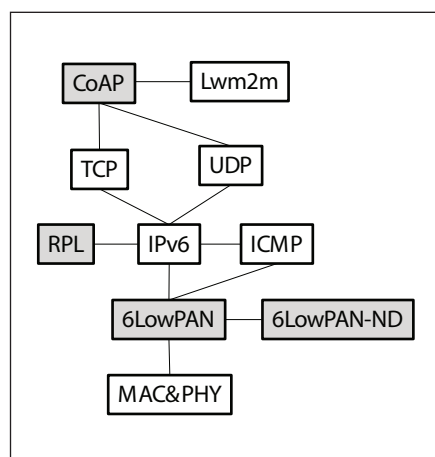


Figure 1. Light-weight Protocol Suite

In addition to protocol design, there are various implementation challenges stemming from limited computational space, cost-efficient discovery and security, and low-power operation mode when building

a minimal but compliant protocol stack. Sharing these implementation experiences can support interoperation, as well as the avoidance of engineering pitfalls.

LWIG Activities

LWIG started by classifying constrained devices by various aspects, including computing and power efficiency. This work has been summarized into the constrained network terminology document RFC 7228¹, where the device capabilities are roughly classified into three categories: Class 0/1/2 respectively. Categories represent data/code size and range from very constrained (Class 0, <10 KB Data, <100 KB code size), constrained (Class 1, around 10 KB data and 100 KB code), and less constrained (Class 2, 50 KB data and 250 KB code size). While this consensus was finalized three years ago, most terms are still useful in related WG conversations. An updated version of this document² is also available and under discussion within the group, which plans to include recent insights from the community on topics such as MTU size implications and lower-power WAN devices.

When designing and implementing the stack on nonconstrained Internet devices, it is generally assumed that they are reachable (at least as the server role) and that the maintenance of the always-on connection by sending periodic keep-alive

beacons are not too costly to be employed. But these assumptions cannot be taken for granted in a constrained environment, as tiny devices have been built duty-cycled and may switch to sleeping mode for the sake of power efficiency. The draft by Arkko et al. on building power-efficient CoAP devices for cellular networks³ examines this issue and makes a number of recommendations. The key to enabling network applications on top of sleepy nodes is to inform the other participating nodes of the existence of the sleepy devices and the locations of their data through a discoverable delegator. While data delegation infrastructure has been specified by the CoRE-RD⁴, limited support is available for the discovery of the resource directory or other registration services. Arkko et al. point out that multicast discovery over cellular alike point-to-point link is not feasible, and they suggest a number of ways for such initial discovery, including manual configuration, manufacturer server hardwiring, delegated manufacturer server hardwiring, and common global resolution infrastructure. For those implementing their services over cellular devices, Arkko et al.'s draft is a must read.

CoAP is an important component for constrained applications. Many open source projects are available, but seldom do they consider how to implement CoAP service in a cost-efficient way. Kovatsch et al.⁵ provide lessons learned from implementing CoAP for tiny devices. This document covers many details of CoAP implementation that engineers usually encounter repeatedly but have not been covered by the specification. There are many insights shared, and the authors provide detailed recommendations on Message ID Usage, Duplication Detection/Rejection, Token Usage, (re)transmission state management, and foreseen optimization. One concrete example is about an insight and clever finding on the Token Usage in CoAP observation model. Instead of

Continued on next page

Working Group Update: Light-weight Implementation Guidance, continued

constantly polling the sensor device to fetch most updated information, CoAP enables an observer to register its interest in a certain resource and subsequently be notified with the most recent data representation, which is called observation model. The observation relationship, represented by URI, IP, Port and Token value (of the observer), is usually kept on the tiny sensors. However, CoAP supports duplicate registrations from one endpoint on the same URI with different Token values, which may add additional cost. Kovatsch et al. instead recommend to assign and reuse a dedicated token value space (8-byte) for each observe relationship, by keeping four bytes constant and iterating the rest four byte space to avoid replay and spoofing attacks. This method not only saves resources to support CoAP observation, but also is protocol compliant. It is also recommended that retransmission buffers are assigned per observable resource instead of per observer (Section 3.3), which consequently saves additional state.

Specific guidelines of power-efficient protocol design are discussed by Gomez et al.⁶, who offer insights about broadcast and nonsynchronized transmissions consuming more than other Tx/Rx operations. If protocols must use these ways to collect information, reducing their usage by aggregating similar messages will help save power. What's more, operations, such as retransmission management, duplicate detection, and observable conversation turn out to be both memory consuming and power inefficient. Reduction of such states in protocol design is a recommended way to be energy efficient.

Security components are generally considered costly, but their absence is a huge risk. Valuable practical considerations and experiences are provided by Sethi et al.⁷, who detail the available cryptography libraries and evaluate their performance in terms of execution time and memory

footprint. This is an interesting document for implementers to reference before evaluating the computational cost of a relevant security solution. Most important, the authors positively conclude that with the help of an informed selection of algorithms and security protocol exchange, the additional cost (e.g., execution time and memory consumption) can be controlled so as to fit most application scenarios.

In addition, Kivinen shares a very small IKEv2 initiator implementation in RFC 7815⁸. The thinking is that a typical IoT device is deployed to communicate with only one server endpoint, so certain portions of the payload contained in the protocol exchange will be static and duplicate validations will be avoided by the minimal implementation. Kivinen also offers a list of optional payloads (e.g., multiple status notifications) that are only useful for multiple peer cases and can be ignored by such minimal implementation. The minimal initiator protocol described is interoperable with a full backend IKEv2 implementation and, therefore, is quite useful on tiny end points.

Conclusion

This article listed just some of the activities of the LWIG WG. Topics that were not covered here, but are taking place in the WG day to day, include minimal TCP,

TLS and DTLS, ESP, and neighbor management implementation. Please drop by the group page at <https://tools.ietf.org/wg/lwig> to learn more. We are grateful to all contributors who are willing to share their experiences of crafting minimal implementations.

References

1. Bormann, C., Ersue, M., and A. Keranen, "Terminology for Constrained-Node Networks", RFC 7228, May 2014.
2. Bormann, C., Gomez, C., "Terminology for Constrained-Node Networks", draft-bormann-lwig-7228bis-00 (work in progress), 2017.
3. Arkko, J., Eriksson, A., Keranen, A., "Building Power-Efficient CoAP Devices for Cellular Networks", draft-ietf-lwig-cellular-06(work in progress), 2016
4. Shelby, Z., Koster, M., Bormann, C., and P. Stok, "CoRE Resource Directory", draft-ietf-core-resource-directory-09(work in progress), 2016.
5. Kovatsch, M., Bergmann, O., and Bormann, C., "CoAP Implementation Guidance", draft-ietf-lwig-coap-03 (work in progress), 2015.
6. Gomez, C., Kovatsch, M., Tian, H., and Cao, Z., "Energy-Efficient Features of Internet of Things Protocols", draft-ietf-lwig-energy-efficient-06 (work in progress), 2017.
7. Sethi, M., Arkko, J., Keranen, A., Back, H., "Practical Considerations and Implementation Experiences in Securing Smart Object Networks," draft-ietf-lwig-crypto-sensors-02 (work in progress), 2017.
8. T. Kivinen, "Minimal Internet Key Exchange Version 2 (IKEv2) Initiator Implementation", RFC 7815, 2016.



WORKING GROUP UPDATE: DYNAMIC HOST CONFIGURATION

By Tomek Mrugalski and Bernie Volz

IT IS COMMON KNOWLEDGE AMONG SEASONED IETFERS THAT THE DYNAMIC Host Configuration (DHC) Working Group (WG) is old. But identifying exactly how old has proven to be a challenge. According to WG archives, its first email was posted¹ on 12 July 2001. But that can't be the right date, as its first Request for Comments (RFC) is RFC 1531 from October 1993. Datatracker history for DHC² provides some clues, but the data appears incomplete: milestone updates go back to 2003, followed by a 13-year gap and two entries indicating that the WG was proposed and formed on 1 January 1991. If this is correct, it gives the WG an impressive 26 years of age—at least as old as the Web, whose creation is typically cited as either January (first public server available) or August (Sir Tim Berners-Lee announces the project to alt.hypertext newsgroup) 1991. However, there exists yet another clue that DHC is even older: the Active Working Group list on the IETF website³. While the page itself is a bit basic, the dates next to each WG name look like creation dates. And this page lists DHC's creation as "1989-Apr-13"—almost 28 years ago.

So what has the DHC WG been doing all this time? Its original goal hasn't changed. It was created to configure hosts in a dynamic way and that's what it has done. If you think about it for a moment, modern networks look completely different than when the work was started. A so-called large network in the late 80s would likely comprise approximately 100 desktop computers. There was no concept of mobility and work on IPv6 hadn't really started. Much has changed and DHC has done its best to stay on top of the changing reality. In the process, the WG published 96 RFCs that defined, clarified, and improved various aspects of devices' auto-configuration. Devices, because it's much more than just hosts nowadays. And that raises the question: is there anything else that DHC still needs to do?

DHCPv6bis

Like most IETF Working Groups, DHC prefers not to spend time on legacy technologies, such as IPv4, except in cases when it's helpful with IPv6 transition. In DHC terms, this means that the WG is almost exclusively focused on DHCPv6. This core protocol (RFC 3315) was published in 2003. A lot has changed since then. Most notably, the ability for routers, not just

With recent changes in how networks are organized, the original assumptions no longer hold. The distinction between hosts and routers is blurred (if you use your phone as a hotspot or run virtual machines on your phone, is the phone still a host?).

hosts, to participate. Routers usually use prefix delegation (PD) mechanism (RFC 3633). Also, with recent changes in how networks are organized, the original assumptions no longer hold. The distinction between hosts and routers is blurred (if you use your phone as a hotspot or run virtual machines on your phone, is the

phone still a host?), the perceptions of trust have changed (do you trust the hotspot in the coffee shop you visit to be legitimate?), and so have our expectations (wait a whole second when logging into a network?).

The DHC WG is addressing some of these changing conditions via an initiative to republish the DHCPv6 specification. Today, this initiative represents the WG's primary focus. A design team formed in 2013 took the original RFC (fun fact: it was in nroff format); cleaned it up; took all the erratas, corrections, and changes that had been introduced (e.g., RFC 7550, which improved several stateful issues); and published updated versions⁴. The work is organized around a dedicated issue tracker⁵. The document went through a very successful WG Last Call (WGLC) in 2016, in which nearly 300 independent comments were received. The design team holds biweekly meetings with a public spreadsheet on Google docs and an intermediate draft text in a public github repository. Remaining comments are expected to be addressed and presented during IETF 98 in Chicago. The intention is to publish the document as a Draft Standard RFC and advance it to Full Standard some time later.

Privacy and Security

The notion of security has also radically changed over the years. Both Edward Snowden's revelations and RFC 7258 prompted many Working Groups to reevaluate certain mechanisms that can be used for pervasive monitoring and other attacks on privacy. In addition, the way people use modern networks has changed. Visiting a coffee shop that you know nothing about seems to be a more common use case nowadays than having your device plugged into a wired network, of which you personally know the admin. DHC spent a considerable amount of time going through mechanisms and options of both DHCPv4 and DHCPv6 with the goal

Continued on next page

Working Group Update: Dynamic Host Configuration, continued

of finding out which of them can be used to track devices and users. As a result, a recommendation called *anonymity profile* has been published in RFC 7844, which recommends certain changes for clients who want to protect their privacy. Clients who implement that recommendation do not reveal anything of use about themselves and don't use any long-lived identifiers that could be used to track them.

At the same time, there are deployment models where almost the opposite is true: in certain deployments clients want to prove their identity to the network and verify that the network is really what it claims to be. Security and preventing pervasive monitoring is of great concern to all, and the lack of security (encryption and authentication) has been a long-standing issue with DHCP as it is used to connect to many networks. This work⁶ started in late 2013 and has had several restarts after review by the Internet Engineering Steering Group (IESG). The current document provides for encrypting client/server interactions. The work is expected to undergo WGLC in the near future, and hopefully it will have another attempt at IESG approval.

The current document provides for encrypting client/server interactions. The work is expected to undergo WGLC in the near future, and hopefully it will have another attempt at IESG approval.

Going Forward

DHCPv6 is an extensible protocol with roughly 10 new options being defined every year. Most of those options convey new parameters that the server is expected to deliver to the clients—they do not change how the protocol operates. As such, more and more option definitions work is being conducted outside of DHC in dedicated groups that comprise subject matter experts, who can better verify the actual content of those parameters. In May 2014, DHC published RFC 7227, which provides

guidelines for authors who work on new options. Nevertheless, there are several extension mechanisms being discussed that are specific to the protocol, so they belong to DHC. Defining YANG models, providing DHCPv6 failover, and tweaking how relay agents are operating are just some of the examples currently being worked on⁷.

You might ask: is the DHC going to wrap up anytime soon? When current chairs Bernie Volz and Tomek Mrugalski took over from Ted Lemon, Lemon made a comment that the group had maybe five years of work left. He then promptly added that when he stepped in, the outgoing chair made the same comment. And who knows? Perhaps Volz and Mrugalski will pass that same prediction to their successors. 🍷

Footnotes

1. <https://www.ietf.org/mail-archive/web/dhcwg/current/mail402.html>.
2. <https://datatracker.ietf.org/wg/dhc/history/>.
3. <https://tools.ietf.org/wg/>.
4. <https://tools.ietf.org/html/draft-ietf-dhc-rfc3315bis>.
5. <http://tools.ietf.org/group/dhcpv6bis/>.
6. <https://tools.ietf.org/html/draft-ietf-dhc-sedhcpv6-20>.
7. <https://datatracker.ietf.org/wg/dhc/documents> and <https://datatracker.ietf.org/wg/dhc/charter/>.

GRASS-ROOTS COLLABORATION: ENTERPRISE DATA CENTER OPERATORS GROUP

By Nalini Elkins and Darin Pettis

THE ENTERPRISE DATA CENTER OPERATORS (EDCO) GROUP WAS FORMED TO monitor the impact of protocol changes on large, sophisticated data centers. The group represents a grass-roots effort organized and led completely by volunteers. Although we will meet in conjunction with IETF meetings, the group is not an official part of the IETF.

Enterprises and large organizations use IETF protocols both on the Internet and inside data centers. A small change to a

crucial protocol can mean a significant shift in the operations and diagnostics for an organization that, in turn, may result

in higher costs or even preclude how a crucial function, such as fraud monitoring, is completed.

For example, the change in TLS1.3 to eliminate the static RSA key exchange, while justified for enhanced security and privacy, also leads to major changes in critical functions, including diagnostics, fraud monitoring, and leak detection for banks, payment processors, retail organizations, health care, and other large organizations that comprise both early adopters of encryption and regulated industries.

Changes to fraud monitoring can be costly and time consuming, but if not acted upon can lead to compromised security, as applications designed for consumer protection may not work properly. EDCO is in the process of working with both TLS group members and implementers to engineer the best solution to these conflicting priorities.

We learned from the experience with TLS1.3 that enterprises are frequently not aware of the protocol changes that impact them until quite late in the process. So, now, we aim to be involved as early as possible in the work of as many Working Groups (WGs) as possible, so that we can provide timely feedback and help them craft effective solutions.

To that end, individual EDCO members plan to review the IETF WG drafts under discussion for changes that could impact large data centers. The IETF has more than 100 Working Groups—it would be impossible for any organization to monitor that many by itself, and if each enterprise sought to do the work, it would need to dedicate up to 40 or 50 people. Our solution is to work together.

Activities at IETF 98

The first meeting of EDCO will be at IETF 98 in Chicago. We intend to have a Boot Camp on Saturday for our members (the Boot Camp is organized completely by volunteers and is not an official part of the IETF). We will provide members an overview of the IETF, discuss IETF terminology, the mentoring programme, the IETF application, as well as several drafts underway by EDCO members. We have designed the Boot Camp to be a space where people can come together as a cohesive group and learn about the IETF from our unique perspective.

To promote networking and integration with IETF members, our members are invited to attend the Sunday newcomers' sessions, if appropriate, as well as the educational sessions organized by the

IETF EDU team and social events. We are coordinating with mentors from the IETF, as well as participating in the IETF Speed Mentoring programme so our members can meet as many experienced IETFers as possible.

We will provide EDCO members with a schedule of WG sessions that they are invited to attend, as well as overviews of the WGs, drafts, and terminology for selected WGs. At the last coffee break of each day, we will offer a daily check-in. We believe that conversations among ourselves about how protocol changes will affect us and conversations with IETFers about activities going on in other parts of the world will prove valuable for the EDCO. Some call this the "hallway track". In our experience, nothing can replace it. We want as many EDCO members as possible to physically attend IETF meetings.

Next Steps

In the future, as the membership of EDCO grows, we may form a trade organization. Ideally, we will work with experts to monitor the Working Groups and upcoming drafts and to provide an assessment of their impacts. In that scenario, members of EDCO will pay for a subscription to those reviews and to webcasts. We may also provide lab facilities so members can get hands-on experience with new protocols. All of this will take money. We want our group to grow organically. If, as our membership grows, members feel that expert reviews and labs are valuable, then we will take that direction. Alternatively, we could also stay a volunteer organization.



Benefits to the IETF

Having sophisticated users of the protocols from large enterprises is a benefit to the IETF. Enterprises are not the only users of the Internet protocols, but they are important ones. The business and government sector organizations, who are members of EDCO, keep the governments and economies of the world running—and Internet protocols are critical to their functioning. Timely feedback from such users will only make IETF standards stronger.

Some cite investments as high as \$1 million per standard created. It may be impossible to calculate the real costs of creating an RFC, but one thing is certain: requirements from the people who will use the protocols in their business functions are priceless.

For more information on EDCO, please contact Nalini Elkins at Nalini.elkins@insidesthestack.com or Darin Pettis at dpp.edco@gmail.com. 

Changes to fraud monitoring can be costly and time consuming, but if not acted upon can lead to compromised security, as applications designed for consumer protection may not work properly.

TODAY'S IETF LEADERS : JARI ARKKO

By Carolyn Duffy Marsan

Began IETF participation	1996
Current role	Outgoing IETF chair
Previous roles	Internet area director, IAB; cochair of Working Groups for the Extensible Authentication Protocol (EAP), EAP Method Update, and IKEv2 Mobility and Multi-Homing Protocol (MOBIKE)
Day job	Senior expert at Ericsson Research
Favorite aspect of leadership	Observing Internet developments



I had my first contact with the IETF in 1996. I was working at Ericsson on modem pools and access services. Some of what we wanted to build for our products needed standards so they could interoperate. I started working with AAA protocols and extensions, and later became chair of the EAP, EMU, and MOBIKE Working Groups. These were long-term efforts that I was heavily involved in.

When I was first approached about the area director (AD) role, it didn't sound like a feasible goal—but it grew on me. A few years later, I applied for the role and it turned out to be a perfect fit. I got to work on topics I really cared about, such as IPv6 transition techniques. And it was good for Ericsson because this is the layer where our products mostly were.

I was an AD from 2006 to 2012—a little on the long side for the position. We say that four years is optimal because it takes about two years to learn the job. During that period, the IETF took up 50–100% of my time. Meanwhile, Ericsson benefitted from my advising them on where the technical pieces that we cared for were heading.

I spent the year after my AD term on the IAB [Internet Architecture Board] and already wondering if I wanted to be the IETF chair. I knew it would be a growing experience, perhaps even a scary challenge. I thought about it for a long time, and decided to go for it.

“ **Being a leader in the IETF has shown me that we *can* make a difference. We *can* make significant technical changes in the Internet and influence how it is administered.** ”

I was IETF chair from 2013 to 2017. And this year things are changing again: I will remain at the IETF and contribute to it, and also again be on the IAB.


I have benefitted tremendously from my role in the IETF—it's been a privilege to witness Internet technology in the making. Plus, the nature of a leadership role in the IETF demanded that I see things in a broader way, talk with other companies, talk with lots of people with new ideas. It forced me to understand the bigger picture. I've also become personal friends with lots of people in the industry, a perk I've enjoyed a great deal.

In a leadership role, you get the feeling that you are in the middle of important issues. As chair of one of the more active or high-profile working groups, you are doing things that are broadly visible and have an impact on the Internet. As IETF chair, I was witness to many interesting things. I am an engineer and have no interest in going into political matters. Yet observing the IANA [Internet Assigned Numbers Authority]

transition was a wonderful experience, and I was glad to see how that played out.

Being an IETF chair represents almost 100% of my efforts; although I spend a fair bit of time at Ericsson, too, where I share what is changing in the Internet and make sure the company considers that information. There have been many cases, including encryption changes, HTTP, and IoT technology, where Ericsson's business was affected by what occurred at the IETF. The company appreciates the IETF team's involvement and expertise on these topics.

Are you thinking about applying for an IETF leadership position? Take the challenge! Expose yourself to new things. You'll learn so much more—a benefit to both you as a person and your employer.

Being a leader in the IETF has shown me that we *can* make a difference. We *can* make significant technical changes in the Internet and influence how it is administered. Yes, sometimes it is hard and takes a lot of effort, but isn't that the exciting part? 

TODAY'S IETF LEADERS : ALISSA COOPER

By Carolyn Duffy Marsan

Began IETF participation	2008
Current role	Incoming IETF chair
Previous roles	Applications and Real-Time area director, IAB member
Day job	Fellow at Cisco Systems
Favorite aspect of leadership	Influencing the future of the Internet



I started participating in the IETF in 2008 and went to my first meeting at IETF 72 in Dublin. I was working at the nonprofit Center for Democracy and Technology (CDT) in Washington, DC, where my role was to explore and articulate the technical implications of policy. I worked on a number of issues, including online privacy.

In 2008, real-time applications were the focus of many of the consumer privacy issues of most interest to CDT. Initially, I focused on the GEOPRIV Working Group. I became a document author and then a cochair of the group. It was a busy time in GEOPRIV—many battles had already been fought about the design of the technology, but finishing the protocol suite required substantial effort. Over time, IETF work became a larger portion of my responsibilities, as it aligned with my CDT work.

In 2011, I was appointed to the Internet Architecture Board (IAB) and soon became the lead of the IAB's Privacy Program. CDT was thrilled—they saw it as an honor that one of their own was selected to serve.

In 2013, I joined Cisco, and in 2014, I joined the Internet Engineering Steering Group (IESG) as Applications and Real-Time area director (AD). I've tried to do my area director work approximately half-time and my day job half-time. I'm leaving the post now because I've been appointed IETF chair beginning in March 2017—my new full-time role for the next two years.

Leadership in the IETF offers exposure to a broad swath of Internet technology that most of us otherwise wouldn't be able to justify spending our time learning and influencing. This is particularly true on the IESG, but also on the IAB. It's incredibly enriching because you're able to make connections between your day job and things going on across the whole industry.


IETF leadership requires management skills of many kinds—you have to manage authors, your time, community processes. It requires a lot of strategy and work in the background to achieve good outcomes. **Many people do not realize the depth of the management education you get while serving in the IETF leadership.**

Lastly, you get to (try to) promote your vision of what the future of the Internet should look like. **Everybody might not agree with you, but leadership gives you a platform to steer and influence.**

Cisco has been a big supporter of the IETF because it is deeply invested in the growth and stability of the Internet. Its customers like that the products they buy

from different vendors interoperate. **Cisco enjoys having people in leadership positions dedicating a portion of their time to furthering interoperability and making sure that standards are keeping pace with technological developments.**

Some IETF participants have difficulty convincing their employers of the value of the time commitment associated with IETF leadership positions. **In reality, it is possible to balance your day job with an IETF leadership role—you set the parameters for how you manage your time.** Lots of positions require a half-time commitment or less.

Having a well-functioning IETF and an Internet that runs on secure, interoperable standards should be important to any large tech company. If that model goes away, the options for how we replace it are all inferior. I hope that the benefits of supporting IETF leaders are obvious; if not, current and past IETF leaders are available to explain them. We have a big incentive to expand the population of people willing to take on leadership roles. 

“ Leadership in the IETF offers exposure to a broad swath of Internet technology that most of us otherwise wouldn't be able to justify spending our time learning and influencing. ”

IETF 97 HACKATHON: IMPROVING OPEN STANDARDS THROUGH OPEN SOURCE

Originally posted by Charles Eckel in the DevNet Open Source Community on 17 November 2016.

IETF 97 MET IN SEOUL AND GOT OFF TO A GREAT START WITH THE IETF Hackathon, 12–13 November. This sixth Hackathon event drew approximately 120 participants on site, plus more than 20 remotely. Work covered a broad range of IETF topics, and the results were both valuable and inspiring.

The IETF Hackathon series started in March 2015 at IETF 92 with the following goals:

1. Advance the pace and relevance of IETF work.
2. Attract young people and developers to the IETF.

Confirmation of the second goal was evident from the start of this Hackathon, as a show of hands indicated this was the first IETF experience for a few dozen participants and the first IETF Hackathon for many more. Evidence of achieving the first goal would need to wait until the results presentations at the end of the Hackathon.

Not Your Typical Hackathon

The IETF Hackathon is not a typical hackathon. Participants are motivated by

a desire to improve the Internet rather than prize money. The spirit is collaborative rather than competitive. Participation is free and attending the IETF meeting that follows is not required. Individuals volunteer to “champion” projects related to IETF work, and teams form around these champions. The list of projects for this Hackathon were as follows:

- ACTN
- Capturing and analyzing network data features – Joy
- COSE/JOSE
- DNS/DPRIVE/DNSSEC/DANE
- Interface to Network Security Functions (I2NSF) Framework
- Interface to the Routing System (I2RS)

- LoRaWAN Wireshark dissector
- Multipath TCP
- PCE
- Service Function DevKit
- SFC
- TLS 1.3
- YANG/NETCONF/RESTCONF

A show of hands indicated this was the first IETF experience for a few dozen participants and the first IETF Hackathon for many more.

One of the ways the Hackathon increases the pace and relevance of IETF work is via running code. Implementing evolving standards and producing running code validates the standards and highlights things that may be missing, wrong, or ambiguous in draft versions of these standards. Better



One of more than 120 Hackathon participants



The Hackathon spirit is collaborative rather than competitive.

Implementing evolving standards and producing running code validates the standards and highlights things that may be missing, wrong, or ambiguous in draft versions of these standards.

still, if the code is open source, viewing and sharing the source code aids in understanding of a standard, makes it easier to use, and promotes its adoption. Open source projects that featured prominently this Hackathon included OpenDaylight, ONOS, VPP, and Joy. For a list and brief description of the Hackathon projects, see the wiki at <https://www.ietf.org/registration/MeetingWiki/wiki/97hackathon>.

Winners and Winners

Despite a lack of big prize money, participants engage in friendly competition

for bragging rights and first shot at a set of gadgets donated by sponsors. Teams present their results to a panel of judges, who have the difficult job of choosing winners. The winners and categories this round were as follows:

- Best Overall: Multipath TCP team**
 This team was composed of a set of professors and students from Ecole Polytechnique de Louvain in Belgium. Since some team members travelled to Seoul and others participated remotely from Belgium, the team had the benefit of working in shifts around the clock.
- Best Input to a Working Group: ACTN team**
 The Abstraction and Control of Transport Networks (ACTN) team produced important feedback for both the Traffic Engineering Architecture and Signaling (TEAS) and Interface to Routing System (I2RS) Working Groups, and their code will become an upstream contribution to the ONOS project.
- Best Group Work: I2NSF team**
 The Interface to Network Security Function (I2NSF) team, powered by energetic professors and students

Continued on next page

Seoul by the Numbers*

[25.5 million]

Population of the Seoul capital area, the fifth largest metropolitan area in the world.

[13.2 million]

Foreign visitors to Seoul in 2015

[1]

Seoul's world ranking in fiber-optic broadband penetration and Internet connection speed

[1988]

Year Seoul hosted the Summer Olympic Games

[2.64 billion]

Times Psy's "Gangnam Style" has been viewed on YouTube, the most for a video on the site.

[40]

Pounds of kimchi the average Korean consumes each year

[20]

Korean players who have made it to Major League Baseball in the United States

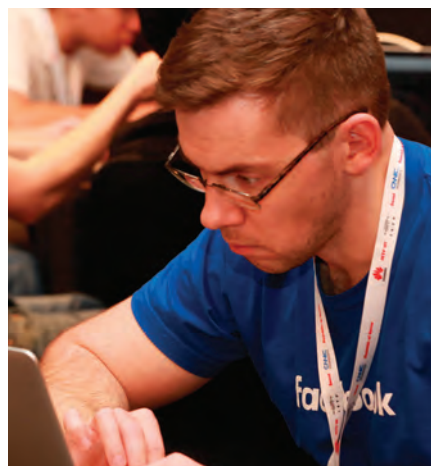
[160]

Length in miles of the demilitarized zone that separates North and South Korea

*Hemispheres, magazine of United Airlines, Nov. 2016.



One of the many who championed an IETF project



One of more than 120 Hackathon participants

IETF 97 Hackathon: Improving Open Standards Through Open Source, continued

from Sungkyunkwan University in South Korea, used RESTCONF and NETCONF together with YANG data models to implement network security services using OpenDaylight and mininet. In doing so, they validated the approach defined by the I2NSF Working Group.

• **Best New Work to IETF: Service Function Dev Kit team and SFC team**

The award was given to two separate teams that both did work related to Service Function Chaining (SFC).

The first added support for Network Service Headers (NSH) to VPP and the Service Function Dev Kit, making it easier for developers to integrate with service function classifiers and forwarders. The second demonstrated hierarchical SFC with flow stateful classifier using OpenDaylight and intent based SFC with ONOS.


Other teams had fantastic achievements, as well. All project presentations have been uploaded to <https://datatracker.ietf.org/meeting/97/session/hackathon>. One pervasive theme was the continued

work involving YANG, NETCONF, and RESTCONF aimed at improving operations through automation. Benoit Claise, one of the operations and management area directors, posted a summary here: <https://www.ietf.org/blog/2016/11/yang-quick-status-update-before-this-ietf-97/>.

Join the Next IETF Hackathon

The next IETF Hackathon will be at IETF 98 in Chicago, 25-26 March 2017. As always, participation is free and open

to everyone. It is a great way to experience firsthand the far reaching work the IETF does and the people that make it happen. It invites open source communities to join the IETF and other standards organizations to improve the functionality, security, and operation of the Internet we all know and love.

To stay up-to-date with all things related to past, present, and future Hackathons—including the opening of registration for the IETF 98 Hackathon—subscribe to hackathon@ietf.org. 



One of many dedicated teams at the pre-IETF 97 Hackathon

VLADIMIR VASSILEV, FROM TRANSPACKET, TRAVELLED FROM OSLO TO SEOUL TO PARTICIPATE IN THE HACKATHON. WHEN ASKED WHY, HE REPLIED:

"You get all these people with passion for what they are doing trying to accomplish something in these two days that will make the world better in a very practical way. It creates a unique atmosphere for creativity. Free to participate, getting the chance to interact with all the great minds there and share ideas makes the Hackathon a unique event. Those are the same principles the IETF is built on.

"I have participated twice and both have proven to be very successful. I intend to continue. On the practical side the event is held during the weekend which allows engineers from smaller companies that do not have dedicated standardization work focus to participate.

"TransPacket has taken some bold decisions that have brought benefit to the company and in the same time to the open source community and the IETF. We are one of the fastest implementers of YANG/NETCONF drafts and standards... I think the importance of the Hackathon event will grow with the tendency of increased adoption of YANG/NETCONF by more smaller companies."

INTERNET SOCIETY FELLOWSHIP TO THE IETF PROGRAMME

More than Observers, Fellows Present and Participate at IETF 97 in Seoul

By Niel Harper

THE INTERNET SOCIETY FELLOWSHIP TO THE IETF PROGRAMME SUPPORTS Internet Society members from emerging or developing economies who have the technical skills and experience to contribute to the work of the IETF. At IETF 97 in Seoul, there were 12 Fellows from 10 countries: Brazil, China, Colombia, Ecuador, Ethiopia, Georgia, India, Tunisia, Uganda, and Zimbabwe. The in-person experience of IETF meetings can help promote a stronger understanding of the standardization process, encourage active involvement in IETF work, and facilitate personal networking with others who have similar technical interests.

In Seoul, several Fellows took attendance a step further and demonstrated the value of both the programme and its participants by presenting or participating in Working Groups or other activities.

- **Harish Chowdhary (India)** presented at two Birds of a Feather (BoF) sessions: DNSBUNDLED and another on implementation issues associated with internationalized domain names (IDNs). He also addressed the Internet Engineering Steering Group (IESG) on progress in India regarding IETF-related activities.

- **Srimal Andrahennadi (Sri Lanka)** entered into an agreement for partnership between Sri Lanka and India to develop an Internet of Things (IoT) research programme and deliver training for young IoT engineers.
- **Eduardo Morales (Brazil)** collaborated with Lee Howard, who provided input into updating his IPv6 teaching materials for NIC.br.
- **Tariq Saraj (Pakistan)** participated in discussions in the DPRIVE Working Group regarding the inclusion of authoritative name



Internet Society Fellows at IETF 97 in Seoul: (top row from left) Habtom Tesfaye (Ethiopia), Eduardo Morales (Brazil), Harish Chowdhary (India), Konstantin Karosanidze (Georgia), Raphael Rosa (Brazil), Ricardo Peláez-Negro (Colombia); (bottom row from left) Niel Harper (Senior Manager, Internet Society), Anissa Bhar (Tunisia), Cristhy Jimenez (Ecuador), Nomsa Mwayenga (Zimbabwe), Xiaohong Deng (China), David Gaamuwa (Uganda). Not pictured: Srimal Andrahennadi (Sri Lanka).

We are looking for mentors to help the Fellows, most of whom are first-time attendees! The amount of time needed to be a mentor is low, but the satisfaction is very high. Mentoring a Fellow means helping him or her navigate that critical first IETF meeting (remember yours?), as well as helping your Fellow build the contacts and relationships that will support his or her being an active contributor to the IETF process and the continued development of open Internet standards.

For more information about mentorship, visit <https://www.internetsociety.org/what-we-do/education-and-leadership-programmes/ietf-and-ois-programmes/internet-society-fellowship-1>.

To apply, send your contact details and a brief statement of interest to ietfmentors@isoc.org.

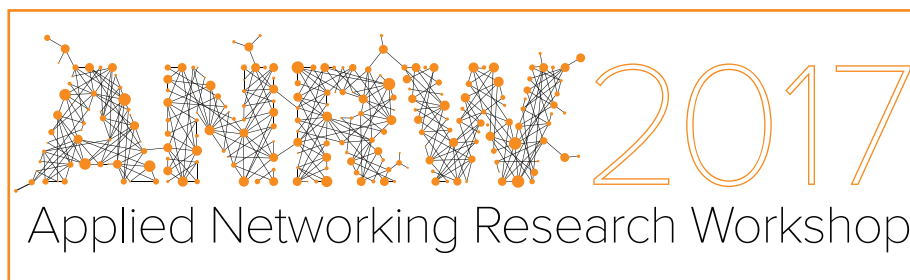
servers in future drafts. He also presented his thesis to the Working Group chair.

- **Konstantine Karosanidze (Georgia)** received assistance from IETF attendees to deploy the first root DNS server (K root by RIPE-NCC) in Georgia. He also built relationships with Working Group chairs and other individuals who are supporting him with an IXP deployment in Georgia.

Please share this Fellowship opportunity with anyone you think is eligible. Applications open for the next three meetings as follows: IETF 99 (Prague, Czech Republic): open now; IETF 100 (Singapore): 10 July; IETF 101 (London, UK): 30 October.



CALL FOR PAPERS



For more information: <https://irtf.org/anrw/2017/cfp.html>

SATURDAY, 15 JULY 2017 • PRAGUE, CZECH REPUBLIC THE IETF 99 MEETING VENUE

The Association for Computing Machinery (ACM), Internet Research Task Force (IRTF), and Internet Society (ISOC) Applied Networking Research Workshop 2017 is a forum for researchers, vendors, network operators, and the Internet standards community to present and discuss emerging results in applied networking research.

Researchers should consider submitting early emerging results that do one of more of the following:

- **Illustrate** the scientific and engineering principles underlying the Internet architecture, protocols and applications
- **Demonstrate** new capabilities, features, or extensions to the Internet protocol layers
- **Enhance** our understanding of how Internet protocols work in real-world deployments or realistic testbeds
- **Improve** Internet security and privacy, scalability, performance, and robustness

Important Dates

Paper submission deadline: 3 April

Acceptance notification: 2 June

Camera-ready paper deadline: 23 June



APPLIED NETWORKING RESEARCH PRIZE WINNERS ANNOUNCED

By Mat Ford

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 97 went to the following two individuals:

- **Benjamin Hesmans** for enabling applications to control how Multipath TCP transfers data. See the full paper at <http://conferences2.sigcomm.org/co-next/2015/img/papers/conext15-final169.pdf>.
- **Olivier Tilmans** for the Fibbing architecture that enables central control over distributed routing. See the full paper at <http://conferences.sigcomm.org/sigcomm/2015/pdf/papers/p43.pdf>.

Hesmans and Tilmans presented their findings to the Internet Research Task Force open meeting during IETF 97. Their slides are available at <https://www.ietf.org/proceedings/97/slides/slides-97-irtfopen-fibbing-central-control-over-distributed-routing-00.pdf> and <https://www.ietf.org/proceedings/97/slides/slides-97-irtfopen-towards-smart-multipath-tcp-enabled-applications-00.pdf>. Thanks to Meetecho, audio and video from the presentations is also available at www.youtube.com/watch?v=mNL8bwotLMg (from 00:13:50).

ANRP winners have been selected for all of the IETF meetings in 2017. The following winners will present their work at the IETF 98 meeting in Chicago:

- **Yossi Gilad**, a postdoctoral researcher at Boston University and the Massachusetts Institute of Technology. Gilad will present improvements to routing security using the “path-end validation” extension to the RPKI.
- **Alistair King**, an Internet Data Scientist at the Center for Applied Internet Data Analysis (CAIDA), SDSC, UC San Diego. King will present a framework to enable efficient processing of large amounts of distributed and/or live BGP data. 🌐



ANRP winners Olivier Tilmans (left) and Benjamin Hesmans (right) at the IRTF open meeting in Seoul.

The call for nominations for the 2018 ANRP award cycle will open in mid-2017. Join the irtf-announce@irtf.org mailing list for all ANRP-related notifications.

IRTF UPDATE

By Mat Ford



Benjamin Hesmans shared his presentation for enabling applications to control how Multipath TCP transfers data.

To stay informed about these and other happenings, join the IRTF discussion list at <https://www.irtf.org/mailman/listinfo/irtf-discuss>.

HAVING SERVED AS IRTF CHAIR SINCE 2011, LARS EGGERT WILL STEP DOWN as Internet Research Task Force (IRTF) chair during IETF 98 in March 2017. The IAB has appointed Allison Mankin as his successor. Thank you for your service, Lars, and welcome, Allison!

Mankin, an Internet protocol lead and researcher based in the Washington, DC, area, is currently senior director, Public DNS, at Salesforce. She has a long history in and around the IETF and IRTF, including serving as Nomcom chair, Transport area director (most recently stepping down in 2006), and IPng AD. In the IRTF, she chaired the Reliable Multicast Research Group (RG) and then moved it to the IETF as the RMT Working Group (WG). She has worked in a diverse set of industry, academic, and government settings. Some of her positions prior to Salesforce were at Verisign, JHU Applied Physics Lab, the US National Science Foundation (NSF), Bell Labs, and USC/ISI. As a program director at the US NSF, Allison was a leader of the Future Internet Design programme, which initiated the funding of infocentric networking and also played an early role in software-defined networking.


During IETF 97 in Seoul, ten chartered IRTF RGs held meetings:

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

- Thing-to-Thing (T2TRG)
- Human Rights Protocol Considerations (HRPCRG)
- Measurement and Analysis for Protocols (MAPRG)
- Internet Congestion Control (ICCRG)

In addition to the meetings of those already chartered RGs, the proposed Network Machine Learning Research Group (NMLRG) met. Since IETF 97, the SDNRG has closed.

The IRTF Open Meeting received Applied Networking Research Prize presentations from Olivier Tilmans on the Fibbing architecture that enables central control over distributed routing, and Benjamin Hesmans for enabling applications to control how Multipath TCP transfers data.

See the Applied Networking Research Workshop 2017 call for papers at <https://irtf.org/anrw/2017/cfp.html>. The paper submission deadline is 3 April 2017. The ANRW'17 is an academic workshop that provides a forum for researchers, vendors, network operators, and the Internet standards community to present and discuss emerging results in applied networking research. Sponsored by ACM SIGCOMM, the Internet Research Task Force (IRTF) and the Internet Society (ISOC), the workshop will take place Saturday, 15 July 2017, in Prague, Czech Republic, the venue of IETF 99. 

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 BoFs that took place during IETF 97, including their 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".

Bundled Domains (dnsbundled)

Description: This BoF focussed on the challenges of fully mapping one domain name to another domain name. With the emergence of internationalized domain names and new TLDs, it is often useful to redirect one domain name tree fully to another domain name tree. Current DNS protocols do not provide good tools to satisfy these requirements.

Proceedings: N/A

Outcome: The proponents were unable to demonstrate a coherent set of problems or use cases. Several participants felt that this was work that had been proposed and failed before, due to lack of clarity and lack of due consideration to collateral damage caused by proposed solutions.

With the emergence of internationalized domain names and new TLDs, it is often useful to redirect one domain name tree fully to another domain name tree.

Bandwidth Aggregation for Internet Access (banana)

Description: This BoF discussed ways to take advantage of multiple access links provided by one or more access providers in cases where end nodes and applications may not be multi-access-aware. Use of multiple access links could provide bandwidth aggregation when multiple links are available (i.e., improved performance), and session continuation when a link becomes unavailable (i.e., increased reliability).

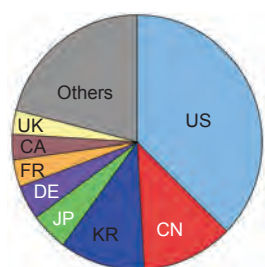
Proceedings: <https://www.ietf.org/proceedings/97/minutes/minutes-97-banana-00.txt>

Outcome: This was a non-WG forming BoF and, as such, provided an opportunity for participants to explore the problem space, identify and share requirements and challenges, and try to scope the work to something that isn't already being done elsewhere and that is relevant to the IETF community. There was clearly energy and interest to continue working on some aspects of this problem space and discussion will continue on the mailing list to try to better scope the problem (or problems) that people want to work on. 🍌

Grey heron
(*Ardea cinerea*)



IETF 97 AT-A-GLANCE



Onsite participants: 1042
 Remote participants: 238
 Newcomers: 154
 Number of countries: 52
 Hackathon participants: 140+

IETF Activity since IETF 96 (17 July–13 November 2016)

New WGs: 6

WGs closed: 4

WGs currently chartered: 146

New and revised Internet-Drafts (I-Ds): 1419

RFCs published: 88

- 53 Standards Track, 3 BCP, 3 Experimental, 29 Informational

IANA Activity since IETF 96 (July–October 2016)

Processed 1281+ IETF-related requests, including:

- Reviewed 95 I-Ds in Last Call and 91 I-Ds in Evaluation
- Reviewed 94 I-Ds prior to becoming RFCs, 51 of the 94 contained actions for IANA

Added two new stand-alone registries since IETF 96 (July–October 2016): iodef2, clue

SLA Performance (May–October 2016)

- Processing goal average for IETF-related requests: 99.6%
- The 2017 SLA between ICANN and IAOC for the protocol parameter work is being drafted for review and approval.

IANA and DNSSEC

- As of 9 October 2016, 1351 TLDs have a full chain of trust from the root. http://stats.research.icann.org/dns/tld_report/.
- Ceremony 26 was executed successfully on 11 August 2016. Ceremony 27 was executed successfully on 27 October 2016.
- Ceremony 28 is planned for 2 February 2017. <https://www.iana.org/dnssec/ceremonies/28>.

RFC Editor Activity since IETF 96 (July–October 2016)

Published RFCs: 91

- 71 IETF (8 IETF non-WG), 2 IAB, 4 IRTF, 6 Independent
- Improvements to the website based on community feedback; expect launch of live version prior to IETF 98.

Website to document coding projects based on IETF specifications has been renamed CodeStand.
 (See page 9 for more information about CodeStand.)

Be the First Host on Your LAN to Receive the *IETF Journal*!



Receive the latest edition of the *IETF Journal* as soon as it is available—in hardcopy or via email. Subscribe today at:

www.ietfjournal.org/subscribe

Want it faster? Follow the [@ietfjournal](https://twitter.com/ietfjournal) Twitter stream to read the articles as they are published.

IETF MEETING CALENDAR

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

IETF 99 **Date** 16–21 July 2017
Hosts Comcast–NBCUniversal
 CZ.NIC
Location Prague, Czech Republic

IETF 100 **Date** 12–17 November 2017
Host Cisco Systems
Location Singapore

IETF 101 **Date** 18–23 March 2018
Host TBD
Location London, UK

IETF 102 **Date** 22–27 July 2018
Host Juniper Networks
Location San Francisco, CA, USA

Special thanks for hosting IETF 97



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



IETF 97 was cohosted by



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

