the IETF® Journal

Volume 9, Issue 3 • March 2014

Inside this Issue

*A report from IETF 88, November 2013, Vancouver, Canada. Published by the Internet Society in cooperation with the Internet Engineering Task Force**

Hyatt photo: Franck Martin

From the Editor's Desk

By Mat Ford

The 88th meeting of the Internet Engineering Task Force was hosted by Huawei in Vancouver, Canada, a very popular location for IETF meetings over the years.

Our cover article in this issue is "An IETF View of IANA," and explains the relationships among the IETF, IANA, and ICANN, and how they all work together. We also have articles about the proceedings of the GeoNet and IGOVUPDATE BoF meetings, plus the BoF meetings that are covered in our regular IETF Ornithology column.

We celebrate the most recent winner of the Applied Networking Research Prize in "Cloud Storage Dissected: A View Inside Dropbox," and document the Internet Society panel event that debated the question of what success looks like for IPv6 deployment.

As usual, you'll find our regular columns from the IETF, IAB, and IRTF chairs, as well as coverage of hot topics discussed during the plenary meetings. For more details of the Internet Area of the IETF in particular, a Working Group summary report is available at http://wiki.tools.ietf.org/area/int/trac/wiki/IETF88.

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

An IETF View of IANA

By Thomas Narten

The Internet Engineering Task Force (IETF) currently outsources its supporting functions: Request for Comments (RFC) publication, secretarial support, and the registration and publication of Internet Protocol Parameters. The IETF protocol parameters function, widely known within the IETF as the Internet Assigned Numbers Authority (IANA), the RFC Editor, and IETF Secretariat all perform functions that are critical to the operation of the IETF.

Continued on page 4

Message from the IETF Chair

By Jari Arkko


Jari Arkko, IETF Chair

The year 2013 was very active for the Internet Engineering Task Force (IETF). Much of what we worked on during the year is having a significant impact on the evolution of Internet technology, including surveillance revelations, the revision of hypertext transfer protocol (HTTP) and transport layer security (TLS), new browser-based voice over Internet protocol (VoIP) and video platforms, and software-defined networking. Our discussions also covered diversifying the IETF, the role of the Area Directors and the IESG, and participation in Internet governance discussions.

Pervasive monitoring was perhaps the biggest worldwide Internet topic this year. Our role at the IETF dictates that we not involve ourselves in the politics of such activities, but that we strive to understand what threats exist in the Internet. At our Vancouver meeting we addressed these issues as we would any other vulnerability or threat in the Internet—we considered them as threats to defend against.

Pervasive monitoring was perhaps the biggest worldwide Internet topic this year.

While communications security alone is not a solution to pervasive monitoring, there are improvements in technology that could reduce opportunities for wholesale data collection. As part of the IETF's ongoing commitment to confronting security vulnerabilities and improving the security of the Internet, we are actively working on some of these improvements (e.g., protocol updates, applications, better use of TLS) and have created the Using TLS for Applications (UTA) working group to drive this work.

As I speak with people around the world about this topic, it becomes clear how very highly appreciated our work on improving the security against pervasive monitoring is. Of course, a lot of hard work remains. We will continue to place our attention on this topic, in our working group lists, interim meetings, at the London IETF meeting, at the IAB workshop (see Words from the IAB Chair on the facing page for more information about this event), and so on.

TLS and HTTP protocols are cornerstones of the Web protocol stack, and their revisions (TLS 1.3 and HTTP 2.0) make them more secure and faster to use—important improvements in light of the pervasive monitoring discussion.

Outside of the security concerns, we have been working with the W3C, other developers, and the WebRTC on a plugin-free mechanism that allows browsers to make voice and video calls—this is an exciting and much needed functionality that's drawn so much attention that some of the technical choices (e.g., video codec selection) have sparked intense debate.

Software-defined networking (SDN) and network virtualisation also have been hot topics in the industry. IETF efforts on these topics include the I2RS, SFC, FORCES, NVO3, and SPRING working groups and the SDN research group. Expect to see even more activity in this space in 2014.

Continued on page 4

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


Russ Housley, IAB Chair

By Russ Housley

This is my second contribution to *The IETF Journal* as chair of the Internet Architecture Board (IAB). It comes at a very eventful time. The news about pervasive surveillance of the Internet by several collaborating governments dominated the discussion at IETF 88 in Vancouver, and it has dominated mail list discussion since the meeting.

The Technical Plenary at IETF 88 was held in a very full room—I can't recall a better-attended plenary session. Presentations focused on reports of large-scale Internet traffic monitoring, summary of previous policy debates in the IETF, and potential actions that could be taken by the IETF. We're all aware that targeted interception takes place, but the scope and scale disclosed in recent news reports surprised the community. The threat is quite different than previously understood, and the community is considering a variety of responses. From my position in the front of the room, it was clear that the community considers pervasive surveillance an attack, and the community will adjust its threat model to consider countermeasures to pervasive surveillance when developing future specifications and updating old ones. Many felt that specifications should include encryption—even without authentication—where practical.

From my position in the front of the room, it was clear that the community considers pervasive surveillance an attack, and the community will adjust its threat model to consider countermeasures to pervasive surveillance when developing future specifications and updating old ones.

Two Statements

The IAB, alongside the Internet Society, the Institute of Electrical and Electronics Engineers (IEEE), and the World Wide Web Consortium (W3C), affirmed the OpenStand principles for the development of global, open standards:

> *While the OpenStand principles cannot ensure that all participants are acting in good faith, following the principles is the best way we know to decrease the risk that any participant can inappropriately manipulate the standards development process. We believe organizations that operate according to the OpenStand principles create the most robust basis for trustworthy standards in all fields of technology, including security and privacy.*[1]

A second statement has become known as the "Montevideo Statement." The IAB chair and leaders of nine other Internet organizations signed a statement regarding the Internet Assigned Numbers Authority (IANA) that is consistent with RFC 6220 and previous IAB statements.[2]

Continued on page 4

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

Message from the IETF Chair, continued

Internet governance discussions in 2013 occurred in both existing and new forums and were largely fueled by surveillance discussions. This will continue in 2014. Our role at the IETF is to be a part of the growing Internet community who cares that the Internet can continue to be managed in appropriate ways, consistent with its long evolution.

We have often discussed the central role of the Internet Engineering Steering Group (IESG) in the IETF, but the problems in finding a candidate to fulfill the position of the transport area director (AD) last spring drove the point home. Our organisation is too centralised, which in turn puts a high load on the ADs and disempowers the working groups. To alleviate this issue, so far we've implemented early directorate reviews and invited document shepherds on IESG calls. I believe this isn't nearly enough, but it's a start. More effort in this direction will come.

None of the aforementioned accomplishments would be possible without a strong and growing organisation. To that end, we're improving inclusiveness at all levels: in March 2013, we started a conversation around improving the diversity of IETF participants and leadership, and ensuring that all voices are heard. I'm proud of the programmes and initiatives that we have that make diverse participation easier, including the Internet Society policy and Fellow programmes, the mentoring programme, our antiharassment policy, the update of the IETF code of conduct, and the decision to hold a meeting in South America. The discussion itself may be the most important result, as it will remind all of us how important this issue is and enable us to actively take these considerations into account. Know that our work on this front to date is just the first step, and part of the kind of long-term process that helped the IETF evolve into the respected international organisation it is today.

Words from the IAB Chair, continued

Highlights since IETF 87

The IAB appointed Russ Mundy to the Internet Corporation for Assigned Names and Numbers (ICANN) NomCom for 2014. Many thanks to Ole Jacobsen for his contributions to the ICANN NomCom over the last two years.

The IAB published RFC 6950 on "Architectural Considerations on Application Features in the DNS."[3]

The IAB sent comments[4] to the US National Institute of Standards and Technology (NIST) supporting the reopening of the comment period on NIST SP 800-90A and recommending changes to the review process for cybersecurity and cryptographic standards to enhance transparency and openness.

Upcoming IAB Workshop

The IAB and W3C are hosting a workshop entitled, "Strengthening the Internet Against Pervasive Monitoring (STRINT)"[5] on 28 February 2014. The workshop will take place in London with support from the European Union FP7 Strategic Research Roadmap for European Web Security (EU FP7 STREWS) programme.[6] Participants are required to submit short position papers or Internet-Drafts.

References

1. http://open-stand.org/statement-from-openstand-on-the-strengths-of-the-openstand-principles/
2. http://www.iab.org/documents/correspondence-reports-documents/2013-2/montevideo-statement-on-the-future-of-internet-cooperation/
3. http://www.rfc-editor.org/rfc/rfc6950.txt
4. http://www.iab.org/wp-content/IAB-uploads/2013/10/IAB-NIST-FINAL.pdf
5. https://www.w3.org/2014/strint/
6. http://www.strews.eu/

An IETF View of IANA, continued

This article describes the protocol parameters function as administered by IANA from the perspective of the IETF community: how the IETF uses IANA services and how a smoothly running protocol parameters registry service is critical to the IETF's day-to-day functioning. It also indicates where IANA fits in the larger Internet governance arena and how its discussions can impact the IETF.

IANA is more properly thought of as a set of functions covering the operation and management of a number of key Internet registries ... Much like a register of deeds, IANA ensures that registrations are made only via authorized procedures, are documented clearly (e.g., purpose, contact information, etc.), and have followed appropriate policies.

Background

The IETF community has long thought of IANA as an entity that exists by itself. In fact, IANA is more properly thought of as a set of functions covering the operation and management of a number of key Internet registries, which are places for officially recording values and ensuring that they are assigned properly and uniquely. Much like a register of deeds, IANA ensures that registrations are made only via authorized procedures, are documented clearly (e.g., purpose, contact information, etc.), and have followed appropriate policies.

At the highest level, IANA coordinates three classes of registries: domain names, number resources (e.g., IP

The IETF has long thought of IANA as an entity that exists by itself. In fact, IANA is more properly thought of as a set of functions, operated by the Internet Corporation for Assigned Names and Numbers (ICANN) under a no-cost contract with the U.S. Government.

addresses), and protocol assignments. It is important to note that there are (at least) two different views of who and what IANA is. To the IETF community, IANA is thought of mostly within the context of protocol assignments. This is not surprising, because for most IETFers, the only interaction they have with IANA involves protocol assignments. To the larger Internet community, the term IANA generally refers to all three functions, or possibly just domain names, since there has been so much new and highly visible activity in the domain name arena in the last decade.

The IANA functions are operated by the Internet Corporation for Assigned Names and Numbers (ICANN) under a no-cost contract with the U.S. Government. While ICANN has played a very prominent role in domain names, almost all protocol assignment discussions have been between the IETF and the IANA part of ICANN, outside of the ICANN spotlight.

The Need for Protocol Parameter Registries

Using protocol constants is basic to all protocols. For example, browsers access Web pages via the hypertext transfer protocol (HTTP) protocol. Packets carrying HTTP contain such protocol fields as the transmission control protocol (TCP) port numbers and Internet protocol (IP) addresses that identify the client and the HTTP server, protocol-type fields that show the packet carries IP (whether IPv4 or IPv6) and TCP (as opposed to user datagram protocol or UDP), etc. Many of these protocol fields have associated registries.

Individual protocols use their own registries. TCP, for example, has a registry for recording well-known port numbers. Registering port numbers makes it possible for all software to understand that HTTP servers can usually be found on servers at TCP port 80, whereas secure Internet message access protocol (IMAP) servers are found at port 993.

Most standards organizations make use of protocol registries, since they are so intimately tied to protocols. The Institute of Electrical and Electronics Engineers (IEEE), for instance, operates a registration authority for recording organizationally unique identifiers (OUIs) used in ethernet addresses.[1]

While the IETF could operate its own protocol parameters registry, it uses a separate organization—the IANA function operated by ICANN—for this purpose.

Although DHCP is an "old" protocol (it dates back to the early 1990s), it continues to evolve and new options continue to be defined. Hence, it demonstrates the importance of protocol parameter registries.

Example Protocol Usage

Dynamic host configuration protocol (DHCP) (RFC 2131 *Dynamic Host Configuration Protocol*) is a core IETF protocol used almost everywhere. When a device connects to the Internet, it uses DHCP to obtain an IP address and other such parameters as a default router and domain name system (DNS) server. The parameters exchanged via DHCP are encoded in DHCP options. Each option has its own assigned unique value, so that the option for a DNS server isn't confused with the option denoting a default router. As with other IETF protocols, DHCP parameters are recorded in protocol parameter registries administered by IANA.[2] DHCP defines a number of individual registries in addition to option numbers; there are DHCP registries for message types (to distinguish different kinds of messages), status codes (for signaling different types of errors), etc.

Although DHCP is an "old" protocol (it dates back to the early 1990s), it continues to evolve and new options continue to be defined. Hence, it demonstrates the importance of protocol parameter registries. When someone proposes a new DHCP option, they write it up in an Internet Draft and (most likely) bring it to the IETF DHCP Working Group (WG) for

Continued on next page

discussion. If the proposal is accepted, it is refined in the WG and eventually sent to the IESG for approval and RFC publication.

At some point during the process, the proposed option needs a DHCP option code assigned to it. That is where IANA comes in. The IETF has defined a formal process for requesting protocol parameter assignments from IANA, a process that is intimately tied to the IETF standards process. In most cases, protocols and extensions are published in IETF RFCs. As a document is being finalized, it goes to the IETF for Last Call processing and to the IESG for formal approval. Any requests for IANA actions (e.g., to request a code point assignment) are usually made within an "IANA Considerations Section" of the document under review. As part of the IETF Last Call process, IANA reviews the document for actions, and verifies that any requests can be carried out. Once approved by the IESG, IANA carries out its actions and coordinates with the RFC Editor to make sure that any assigned option values appear in the published RFC.

The Details

New registries are typically created by protocol documents. Protocols define the fields in packet headers and the allowed values for those fields. Some fields contain enumerated types, in which specific values have well-defined meanings that will never change once defined and that all implementations will interpret the same way forever. For example, a security protocol might have a field denoting a specific encryption transform, with one value defined for Triple-DES. Once assigned, the value denoting the triple data encryption algorithm (Triple-DES) transform would always have the same meaning. Later, a new or otherwise different algorithm could be added (e.g., one based on the advanced encryption standard, or AES).

> The IANA functions for managing the Internet protocol parameter registries have existed since the dawn of the Internet.

It would be given its own distinct value. That way both could be supported simultaneously in an interoperable manner.

Once a registry has been created, future additions to it can be expected. To properly evaluate such future requests, governing policies are needed to define the criteria under which requests are to be granted. The IETF defines these policies for the protocol parameter registries.

The details of what policies make sense almost always depend on the specifics of the actual protocols using the registry. For example, some registries have a limited number of possible values (e.g., the 4-bit IP version field can represent only 16 distinct values), so assigning additional values must be done prudently. Other registries may be essentially unlimited in size (e.g., long text strings) and can be done with much less review. Also, some types of registries record values that can have a big impact on how a protocol works (e.g., defining a new message type). Such requests may warrant a more in-depth review, perhaps involving consultation with the IETF working group responsible for maintaining the protocol of interest.

The IANA functions for managing the Internet protocol parameter registries have existed since the dawn of the Internet. The formal processes for creating and managing registries were first documented in 1998 in RFC 2434's *Guidelines for Writing an IANA Considerations Section* (later obsoleted by [RFC 5226] *Guidelines for Writing an IANA Considerations Section in RFCs*), and the IETF now has more than 15 years of operational experience in creating, using, and updating registries via the IANA Considerations Section framework.

RFC 5226 provides guidelines on how to create registries, how to populate those registries with initial values, etc. RFC 5226 also provides best practices on defining policies for governing future assignments to a registry. A number of predefined, "cookie-cutter" policies have been defined that handle many of the common cases. For example, the policy of "Standards Action" indicates that an assignment only happens via approval of a Standards Track document, whereas "First Come, First Served" denotes registries in which assignments are given out with little or no review.

> Any change to the current overall IANA functions could potentially impact the protocol parameters portion of IANA. Since the IETF depends on its smooth operation, it is critical that the IETF be engaged in any such discussion.

Bottom Line

Having the protocol parameters function separate from the IETF has worked well in practice and works well today with ICANN executing that function.

Many details have been formalized, beginning with the *Memorandum of Understanding Concerning the Technical Work of IANA* [RFC 2860] and *Defining the Role and Function of IETF Protocol Parameter Registry Operators* [RFC 6220], as well as yearly service-level agreements (SLAs) since 2006.[3] Performance reports called for in the SLAs can be found at http://www.iana.org/performance/ietf-statistics.

The IETF and IANA worked closely together for years to develop the current system. In it, IANA performs an administrative function—fielding requests, processing them, and publishing the results. Matters of policy, including matters requiring technical evaluation of a specific request or what policies should govern assignments, reside squarely within the IETF. The close, day-to-day working relationship between IANA and the IETF has in practice resulted in a shared understanding of the respective roles of each entity. The current IETF/IANA relationship is strong and its maintenance will continue to require diligence going forward.

Where does the IETF fit into the Internet governance discussion? Any change to the current overall IANA functions could potentially impact the protocol parameters portion of IANA. Since the IETF depends on its smooth operation, it is critical that the IETF be engaged in any such discussion. The IETF has a unique need for the protocol parameters function and a unique view of IANA, and that view needs to be understood by the broader community in any Internet governance discussions related to IANA. This is particularly true when discussion of IANA (or ICANN) is really specific, for example, to DNS names, and does not apply to the protocol parameters function.

Conclusion

A properly operating protocol parameters function is critical to the IETF. The current relationship, in which ICANN operates IANA, has worked well for a number of years and continues to work well today. But given that IANA inevitably seems to come up in Internet governance discussions, the IETF must engage in such discussions so that its interests are not marginalized and the broader community fully appreciates the IETF/IANA relationship.

References

1. http://standards.ieee.org/develop/reg1. http://standards.ieee.org/develop/regauth/oui/public.html
2. http://www.iana.org/assignments/bootp-dhcp-parameters/bootp-dhcp-parameters.xhtml
3. http://iaoc.ietf.org/documents/ICANN-IETF-Agreement-2012-Executed.pdf

Internet Society Panel Explores Measuring IPv6 Momentum

By Carolyn Duffy Marsan

As more service and content providers deploy IPv6, the Internet engineering community is grappling with how to establish milestones and metrics to measure progress in the rollout of next-generation Internet services.

To reflect on the headway that's been made in IPv6 deployment and to consider what steps need to be taken next, the Internet Society hosted a panel discussion entitled "IPv6: What Does Success Look Like?" in conjunction with IETF 88.

Leslie Daigle, the Internet Society's chief Internet technology officer, moderated the panel, which included John Brzozowski, fellow and chief IPv6 architect at Comcast Cable Communications; Erik Nordmark, an Internet Architecture Board member and software developer for Arista Networks; and Chris Palmer, program manager for IPv6 at Microsoft.

Daigle kicked off the discussion with a recap of the significant progress that's been made in IPv6 deployment during the past year. For example, Google reports that the percentage of its users accessing its sites over IPv6 doubled between August 2012 and November 2013 from 1 percent to 2 percent.

"In June of 2012, we had World IPv6 Launch, which was an opportunity for access providers, content providers and CPE vendors to step up to deploy IPv6," Daigle said. "A lot of major ISPs stepped up to that particular challenge. Sixty-nine networks achieved a measurable amount of IPv6 traffic—at least 0.1 percent—in June of 2012, and now that number is up to 197 networks in October of 2013."

Leslie Daigle, moderator and the Internet Society's chief Internet technology officer

Daigle said that for these ISPs, IPv6 is "a regular part of their business now,

Continued on next page

Internet Society Panel Explores Measuring IPv6 Momentum, continued

with new subscribers getting IPv6 by default without user configuration." She added that the deployment of IPv6 by Google, Facebook, and Yahoo is driving most of the IPv6 traffic.

The major ISPs that are deploying IPv6 for their users are finding a significant amount of their traffic immediately migrates from IPv4 to IPv6, Daigle added. "Verizon Wireless sends 40 percent of their traffic to Google, Facebook, and Yahoo over IPv6," she said. "When IPv6 gets turned on, pretty serious things happen."

Daigle posed a series of questions to the panelists about progress being made in IPv6 deployments. In particular, she wondered how the IETF community will know if it is progressing both in the right direction and quickly enough. "As a community, what are the metrics and milestones of importance?" she asked.

Brzozowski argued that the best metrics are IPv6 traffic volumes and the numbers of users with IPv6 access to the Internet. He said that Comcast has IPv6 deployed across 75 percent of its broadband network, with 25 percent of its customers currently using IPv6. He said Comcast will complete its deployment of IPv6 across its broadband network in early 2014.

"By this time next year, we expect double the penetration," Brzozowski said. "We hope to have 50 to 60 percent of our customers using IPv6."

The biggest hurdle to IPv6 deployment is the lack of support from consumer electronics vendors and content providers, Brzozowski said. "Our statistic when we light up a house with IPv6 is that 20 percent of the traffic almost immediately happens over IPv6," he said. "That's not bad, but that's not great either."

Brzozowski said one milestone that will indicate successful deployment of IPv6 is when it's possible for users to operate in an IPv6-only fashion. "We hope to announce IPv6-only trials and, of course, they will be opt-in," he said. "We really want to go down that path so we can better assess what the IPv6-only experience is and is not."

Nordmark pointed out that IPv6 is not making inroads in enterprise networks, which he says will hamper interoperability if it is a long-term trend. However, one possibility is that the Bring Your Own Device (BYOD) shift in corporate IT environments will prompt companies to adopt IPv6.

"The trend that people want to bring their smart phone or tablet to work and have the same type of services when they use the Wi-Fi of the enterprise as they have at home means that there will be some pressure on the enterprise to adopt IPv6," Nordmark said. "Also, companies are using more virtual networks, and for some virtual networks done at very large scales, IPv6 might be a natural fit for simplicity and flexibility reasons."

John Brzozowski, panelist and chief IPv6 architect at Comcast Cable Communications

A milestone that Nordmark says would indicate continued progress for IPv6 is when software developers automatically support both IPv4 and IPv6. "Something that we can collectively work towards is IPv6 version agnostic software development, which will help over a very long time period," he added. "But I think to get rid of IPv4 legacy software will take about 20 years."

Erik Nordmark, panelist, Internet Architecture Board member, and software developer for Arista Networks

"The trend that people want to bring their smart phone or tablet to work and have the same type of services when they use the Wi-Fi of the enterprise as they have at home means that there will be some pressure on the enterprise to adopt IPv6."

—Erik Nordmark, Panelist

Palmer pointed out that IPv6 has picked up momentum in three categories: in-home hardware and operating systems, in-home routing infrastructure, and network access. "In all three of those dimensions, there has been significant qualitative and quantitative improvement and forward velocity when it comes to IPv6 transition. So that's good news," he said.

Palmer prefers a simple metric for measuring the success of IPv6 deployment between now and 2020: a working Internet.

Palmer pointed out that IPv6 has picked up momentum in three categories: in-home hardware and operating systems, in-home routing infrastructure, and network access.

"The simplest thing that I would like to have is the Internet continue to work and work well for the purposes of using it every day, despite the fact that the number of devices is going to increase by 30 times between now and 2020," Palmer said. "We need to be ready."

When discussing specific metrics of IPv6 progress, Brzozowski said Comcast will reach an important milestone when its Internet-facing traffic is 51 percent running on IPv6. Nordmark would like to see corporations running VPNs over an IPv6 backbone. Palmer said he would like to see less reliance on transition mechanisms that allow IPv6-only devices to reach IPv4 sites.

"Now that we're getting close enough to IPv6 being operational by default, how do we avoid or sunset the transition technologies… that leave one foot left in the IPv4 doorway because they make applications and services that are not on IPv6 very fragile," Palmer asked.

One concern for Daigle is that ISPs in North America are making great strides in IPv6 deployment, but that their rivals in Asia are lagging.

"Asia Pacific ran out of IPv4 addresses a couple of years ago," Daigle said. "There are no network build-outs with IPv4, but they are not deploying IPv6. Instead, they are exploring vast workarounds of large-scale network address translation (NAT). Can we have a path for success of IPv6 if it's not uniformly deployed across the globe?"

Audience members queue up to ask questions and offer comments.

Brzozowski admitted that the user's Internet experience may vary around the globe, with better and faster service in countries where ISPs deploy native IPv6 and slower service in countries where ISPs adopt NATs.

"It will be hard for [Asia] to avoid the tidal wave that is IPv6 transition without creating some definition between the Internet here and the Internet there because a plethora of services work in a degraded or broken state there," Palmer said.

During the Q&A session, Erik Kline, an IPv6 software engineer with Google, pointed out that some Asian countries such as Singapore are making inroads in IPv6 deployment because regulators require ISPs to adopt it.

"The Singapore regulator put together a policy called 'no islanding' and used this to get IPv6 going," Kline said. "This has not been without issue, but Singapore is in the top 12 countries for IPv6 deployment because of that regulatory foresight."

Another audience question prompted a discussion among the panelists about whether or not it makes sense to market IPv6 directly to end users so they can ask for it from their ISPs and hardware vendors. Panelists disagreed about whether that was a good idea.

"If we waited for people to ask for IPv6, people's dream of deploying it by 2020 would be 3020," Brzozowski said. "Early on, we said we must have IPv6 on by default."

However, Palmer pointed out that IPv6 offers bottom-line benefits for gamers due to reduced latency. "There are a couple benefits of IPv6 because the complexity and fragility of STUN [Simple Traversal of UDP through NAT] is a real thing," he said. "UDP is not universally implemented and it's not implemented well. The complications of STUN have a real impact on people's experience."

Cisco Fellow Mark Townsley suggested that instead of marketing IPv6 to end users, it might be more appealing to market the idea of globally unique addresses to both end users and regulators.

Internet Society Programme Builds Bridge Between IETF and Regulators

By Carolyn Duffy Marsan

At IETF 88, as part of an ongoing effort to foster better understanding between the Internet's technical and regulatory communities, the Internet Society (ISOC) hosted ten policymakers from South America, Africa, and Asia.

ISOC's Policymakers Programme to the IETF facilitates exchange between government policymakers and IETF leaders by providing visiting policymakers with an overview of how the IETF works and key issues affecting the Internet's continued growth. Via this programme since 2012, ISOC has hosted more than 50 individuals from 40 governments to attend IETF meetings.

"The goal is to offer a bridge between the IETF community and the policy realm and to help demystify the IETF," said Sally Wentworth, senior director of Strategic Public Policy for the Internet Society. "The response from policymakers has been overwhelmingly positive, and the IETF community's welcome to policymakers has been tremendous. We are going into a very important period for Internet governance, and more focused engagement like this is needed."

All of the policymakers who attended IETF 88 work for government agencies that oversee the telecommunications and/or ICT sectors in countries including Brazil, Kenya, and Vietnam.

At IETF 88, these policymakers were given presentations about the IETF, including its mission and how it develops open standards through an ethos of rough consensus and running code. Leaders from across the IETF community explained working groups and leadership committees and how documents such as Request for Comments and best current practices are produced.

Experts from the IETF community gave policymakers an overview of the big-picture challenges that the Internet faces, including mobility, bandwidth constraints and the emergence of new applications. This programme is also an opportunity for the IETF community to listen and learn about the priorities of policymakers.

> "Policymakers gained a greater understanding of how the Internet and Internet standards work, something that had never been explained to them in such depth before."
>
> —Sally Wentworth
> Internet Society

"Our policy guests saw that the IETF is focused on its technical role and work, but felt that the community also handled the policy-related issues well and appropriately," Wentworth said. "The IETF's passion and enthusiasm for the Internet model and open debate was evident and inspiring to the policymakers. They were impressed that anyone who comes to an IETF meeting is allowed to participate and be heard."

The government representatives heard a series of presentations from IETF leaders on critical aspects of the Internet:

- Fred Baker, Cisco Fellow and former IETF chair, gave presentations about BGP (border gateway protocol) routing and the history of the Internet.
- Mark Kosters, chief technology officer of the American Registry for Internet Numbers, provided a deep dive into Internet protocol (IP) addressing, with an explanation of the differences between IPv4 and IPv6.
- Former Internet Architecture Board Chair Olaf Kolkman, director of NLnet Labs, gave a talk about the domain name system (DNS) and the need to secure it with DNS security extensions.

The Internet Society's IETF Policy Programme Fellows

- Geoff Huston, chief scientist at Asia-Pacific Network Information Centre, spoke about the concept of quality of service in the Internet in comparison to predecessor voice-only networks.
- Alvaro Retana, a Cisco distinguished engineer, spoke about the impact of the IETF on Internet development, including the group's new efforts to harden the Internet against pervasive monitoring attacks and to improve the diversity of its membership.
- Milton Kaoru Kashiwakura, director of the Brazilian NIC, gave a talk about regional interconnection from Latin America.

They also attended the Internet Governance Update (IGOVUPDATE) Birds of a Feather session, which all of the policymakers noted was a highlight of the week. This session was sponsored by the Internet Architecture Board to discuss IANA matters.

"Policymakers gained a greater understanding of how the Internet and Internet standards work, something that had never been explained to them in such depth before," Wentworth said. "Giving policymakers a chance to attend the IETF helps build trust among organizations, and this trust is key for the future of the Internet."

The Internet Society will provide a similar set of presentations for a new group of policymakers at IETF 89 in London that include senior policy leaders from Africa, Europe, and the Middle East.

"Past participants of the ISOC's IETF Policy Programme want to get more experts from their countries involved in the IETF," Wentworth said, noting that it is always difficult to get academic and industry participation in standards work because it is a voluntary effort. "This programme is helping build awareness of the IETF in developing countries, which is needed."

Packed IAB Plenary Debates Pervasive Monitoring Attacks

By Carolyn Duffy Marsan

The Internet engineering community debated the steps it can take to harden the Internet against pervasive surveillance from well-funded governments and other adversaries in a packed technical plenary session held during IETF 88 in Vancouver.

The discussion was prompted by recent revelations that the US National Security Agency (NSA) was involved in a wide-scale global Internet and telephone surveillance program in conjunction with other governments and commercial vendors. The Internet Architecture Board (IAB) focused its discussion on what can be done in terms of protocol design and development to protect the Internet and its users from pervasive monitoring attacks.

"We'd like to focus on who needs to be doing work in the technical community both here in the IETF and elsewhere," said IAB member Alissa Cooper, distinguished engineer at Cisco. "We in the IAB need to be thinking about longer-term architecture issues, opportunities for stronger security, and potential barriers to stronger security."

Cybersecurity expert Bruce Schneier, chief technology officer of Co3 Systems, set the stage for the discussion by explaining the scope of Internet traffic monitoring being conducted by the NSA and other government agencies.

> "The NSA has turned the Internet into a giant surveillance platform. This is robust. It is robust politically, it is robust legally, and it is robust technically."
>
> —Bruce Schneier, Panelist

"The NSA has turned the Internet into a giant surveillance platform," Schneier said. "This is robust. It is robust politically, it is robust legally, and it is robust technically."

Schneier pointed out that it isn't only the NSA that is involved in extensive Internet traffic monitoring.

"This is what any well-funded nation state or adversary would do," he said. "The United States has a privileged position on the Internet that allows it to do more, and it has an enormous budget. But we know other countries do the same thing."

Continued on next page

Alissa Cooper, panelist and distinguished engineer, Cisco

Packed IAB Plenary Debates Pervasive Monitoring Attacks, continued

Bruce Schneier, panelist and chief technology officer, Co3 Systems

Schneier said the choice facing network engineers is whether they will continue to support an Internet that is vulnerable to all attackers, or whether they will make the Internet secure for all users.

"We have made surveillance too cheap, and we need to make it more expensive," he said. The goal is to make eavesdropping expensive to force NSA to abandon wholesale collection in favor of targeted collection.

Schneier gave the IETF community three recommendations for hardening the Internet: (1) deploy encryption ubiquitously on the Internet backbone, (2) encourage dispersal of Internet traffic targets rather than centralization in the hands of a few companies, and (3) develop user-friendly application-layer encryption.

[Stephen] Farrell said the IETF should focus on driving up the cost of pervasive monitoring through such actions as encouraging the use of encryption.

"We need more open standards and open source tools because these are harder to convert to attacks," he said. "We need better integrated anonymity tools and real assurance… Long term, we need to get everyone to understand that a secure Internet is in everyone's best interest."

Brian Carpenter, a former IETF chair and now a computer science professor at the University of Auckland, gave a historical talk focused on how the Internet engineering community has handled similar cybersecurity issues in the past.

Carpenter acknowledged that the IETF didn't take security seriously before 1998. "There was a general tendency to ignore security issues, including confidentiality and privacy, until the late 1990s. That's a fact," he told the audience.

However, he pointed out that the Internet engineering community has twice confronted security-related public policy issues similar to the recent NSA revelations.

"Surveillance is not a new phenomenon," Carpenter said. "Don't have the impression that this is just the NSA or just the US government."

The first of these IETF debates, held in 1996, dealt with a movement by many governments to restrict the use and sale of strong cryptography, which is a foundational technology for e-commerce. The result of this debate was RFC 1984, signed by both the IAB and the Internet Engineering Steering Group (IESG), which encouraged policies that allow ready access to strong cryptographic technology for all Internet users.

In 1999, the IETF had a similar debate about Internet wiretapping. The result of that debate was RFC 2804, also signed by both the IAB and the IESG, which stated that the IETF would not consider wiretapping as a requirement for creating or maintaining IETF standards.

Carpenter said the underlying principal of these two previous IETF debates is that "IETF technology should be able to make the Internet secure, including the ability to provide privacy, but it should be neutral with respect to varying cultural views of legality and privacy."

The final speaker at the technical plenary was Stephen Farrell, an IETF security area director and a research fellow in the School of Computer Science and Statistics at Trinity College Dublin. Farrell urged IETF participants to view the NSA activities as an attack and try to mitigate it.

"Forget the motives. Forget the political stuff. Look at the actions of the NSA and its partners—whether coerced or not—as a multifaceted form of attack," Farrell said. "It's not unique. The NSA and its partners are doing it, but others are doing the same though perhaps on a smaller scale."

Farrell said the IETF should focus on driving up the cost of pervasive monitoring through such actions as encouraging the use of encryption.

"What would be the impact if we turned on Transport Layer Security (TLS) more ubiquitously?" he asked. He also suggested TCPcrypt and IPSec as ripe for additional deployments. "What about Secure/Multipurpose Internet Mail Extensions (S/MIME) and Pretty Good Privacy (PGP)? We need to do the same for Session Initiation Protocol (SIP). We need end-to-end security for e-mail, instant messaging and Voice over Internet Protocol (VOIP)."

Farrell said it will be harder to secure real-time Web communications and

sensors deployed in Internet of Things applications. Another hard problem is how to prevent the extraction of metadata through Internet traffic analysis.

"We need to take steps, do them openly, and start now," Farrell said. "It's not just about us taking action through the IETF. We also need to go back to our companies and try to get them to take action. Lots of companies are looking at their source code. Operators are looking at their networks."

Brian Carpenter, panelist, former IETF chair, and computer science professor at the University of Auckland

"IETF technology should be able to make the Internet secure, including the ability to provide privacy, but it should be neutral with respect to varying cultural views of legality and privacy."

—Brian Carpenter, Panelist

Farrell concluded that the NSA revelations don't represent a new attack on the Internet, but an attack at a larger scale.

"The right response for us is, as usual, to develop technical mitigations not to solve the problem but to make it harder to do widely pervasive monitoring," he said. "The goal is to make it significantly more expensive for a bad actor."

The technical plenary speakers generated vigorous debate about what the IETF should do to improve Internet security and privacy during the open mic session. More than two dozen attendees asked follow-up questions or made suggestions to IAB members about how best to harden the Internet.

"My little box here is running IPsec, TLS and Domain Name System Security Extensions (DNSSEC)," said Russ Mundy, an engineer with security firm Parsons, pointing to his laptop. "I urge everybody in this room to have some amount of this security capability themselves on their own machines. Turn it on, and start using it right now… Work within your own organizations to deploy it, and push your providers to give it to you."

Google engineer Erik Kline suggested the IETF community consider the economics of deploying cybersecurity solutions. "SSL certificates are still not the default," he said. "Most of the vendors charge more for SSL. There are economic incentives stacked against people who want to do security."

Michael Abramson of Advanced Systems Management Group worried aloud about the usability of Internet security protocols such as DNSSEC. "How do we expose failure modes to users, and how do they interact with all this cryptography?" he asked. "I don't know if there are any usability experts active in the IETF, but I think we need some."

Terry Davis, who develops aviation networks, pointed out that within a decade aircraft will be communicating to ground control via the Internet, heightening the need for security. "We first spoke about Internet hardening back in 1998 for [industrial control and aviation] networks. We really don't provide any good guidance to build these type of networks," he said. "I encourage the IESG to form a working group on critical networking infrastructure."

At the end of the discussion, IAB Chair Russ Housley tried to gauge interest in taking action on pervasive monitoring by asking attendees to hum in response to particular questions. The audience overwhelmingly responded in favor to questions about the IETF's willingness to respond to pervasive surveillance attacks, whether or not the IETF should consider the threat of pervasive surveillance attacks when approving standards track specifications; and whether or not the IETF should include encryption where practical.

At the IETF administrative plenary later the same day, IETF Chair Jari Arkko called pervasive monitoring a very important topic with high impact on all Internet users.

"From my perspective, it's not that sensible to react to specific incidents [rather than] take them as a sign that our Internet is not as secure as it should be," Arkko said. "There's so much interest by regular Internet users, politicians, vendors, service providers and even some governments. It is an opportunity for us to actually make a change—perhaps a unique opportunity—so let's use this moment to make a fundamental improvement to Internet security."

In sum, there appeared to be consensus among IETF participants and leaders to improve the technical standards of the Internet in order to improve the privacy and security of the Internet and thereby make large-scale surveillance efforts more difficult.

The IAB Plenary drew a packed room.

Meetecho: How We Turned an IETF Experiment into an IETF Tool

By Alessandro Amirante, Tobia Castaldi, Lorenzo Miniero, and Simon Pietro Romano

Remote participation is a hot topic in the Internet Engineering Task Force (IETF). Many participants attend IETF meetings remotely if the venue is either too far away or too expensive for them to attend in person. Many regularly only attend remotely in the first place.

To make remote attendance possible, the IETF makes available the following solutions:

- A Jabber chatroom associated with each session, in which participants, both local and remote, can join using any compliant client in order to discuss the presentations
- An MP3 audio feed to listen to what is being discussed in the physical rooms

In addition, the Jabber room typically is used to give remote participants hints about ongoing presentations, e.g., the name of the slide deck being projected, slide numbers, and so on. It is expected that remote participants download the slides and open them in a compliant viewer to follow the presentation.

While this is an easy and often effective means for remote participation, it does not afford an optimal user experience. Users must download and install various applications (e.g., an extensible messaging and presence protocol (XMPP) client, a multimedia player, a slide viewer/editor), and use them at the same time. While the audio feed has a good quality, it also can have up to a 10-second delay, making seamless interaction (e.g., questions and answers) harder to achieve.

A Brief History

A few years ago, while considering our efforts to build a standards-compliant conferencing architecture, mostly based on IETF protocols, and our regular attendance at IETF meetings as active contributors, we asked ourselves: why can't we eat our own dog food? The IETF had already devised several protocols and architectures that could be leveraged for a better remote participation experience. We'd already tested some remote participation using Meetecho at IETF 76 in Hiroshima, where Lorenzo Miniero had a presentation scheduled at the MEDIACTRL session but couldn't make it to Japan. A desktop application implementing XMPP, session initiation protocol (SIP), and real-time transport protocol (RTP), and providing slide-sharing functionality was used for a bidirectional interaction between Lorenzo and local attendees.

IETF 80, Prague

This motivated us to propose a wider remote participation experiment at IETF 80. Specifically, considering that a desktop application would have been more of an obstacle than an asset, we devised a web-based, front-end to our platform, thereby providing an integrated view of the Jabber room, the slides being projected, and an audio/video feed from the room. We focused on real-time delivery of the streams by extending our platform, which was already based on modified versions of open source components such as Asterisk, Openfire, and Tomcat, to better interact and seamlessly merge with the available IETF remote participation tools.

We discussed the possibility of exploiting this new interface with IETF management, particularly with respect to the interaction with local equipment (e.g., room mixers) and supported seven sessions. The experiment proved quite successful—remote participants tested our platform and we received useful feedback that we used to further develop and strengthen our prototype experiment. While the presence of a video feed (a webcam in the sessions) confused some of the local participants, it was a very welcome feature by remote participants, who praised the possibility of looking at the mic line queues. Not all feedback was positive, but it was constructive and helpful. For example, all the sessions were recorded and made available a few days later, initially by means of a Java playback application. Several users complained about relying on an untrusted Java application, despite the fact that the source code had been made available. During the week we developed a completely web-based HTML5 player for the same recordings. That Web application was the first version of the one we use today to provide all the IETF recordings.

> IETF 83 also represented a milestone with respect to realization of a system for the automated management of floor control and the moderation of both local and remote participants.

IETF 81, Quebec City

The success of the Prague experiment motivated us to improve the platform and user interface, and propose another round at IETF 81. The number of supported sessions increased to 12, including two plenaries, resulting in a couple of parallel sessions.

IETF 82, Taipei

The experience we gained in Prague led us to new improvements that we applied at IETF 82, an important meeting in terms of remote participation—28 sessions were supported with up to three

sessions in parallel; and for the first time, we used the tool for active remote participation.

IETF 83, Paris

By IETF 83, Meetecho wasn't news anymore. We prepared a tutorial on it, focusing on the Meetecho Scribe, a role that can be played by any local participant to help remote attendees. Nearly 30 sessions were supported.

IETF 83 also represented a milestone with respect to realization of a system for the automated management of floor control and the moderation of both local and remote participants (http://ietf83.conf.meetecho.com/index.php/UMPIRE_Project). This system is called UMPIRE (Universal Moderator for the Participation in IETF Remote Events) and is built around the Binary Floor Control Protocol (BFCP) that represents the IETF standard protocol for moderation. At the time of this writing, UMPIRE has not yet been used to moderate actual meeting sessions. Although at the 83, 84, and 85 meetings it was demonstrated in a tutorial. Today we are awaiting completion of the Remote Participation Services document in order to further fine-tune UMPIRE and propose it for official adoption within the IETF.

IETF 84, Vancouver

With regard to the main functionality of the platform, we started work on WEBRTC/RTCWEB, the joint standardization of the W3C and the IETF to enable native, real-time multimedia communications within browsers. We implemented the missing bricks and added a way to make use of WebRTC to join the audio/video conference. We made the completed feature available for the RTCWEB session at IETF 84 (a possibility that was praised by the active contributors in the same working group). Vancouver also saw our platform used, for the first time, to stream and record both meeting sessions and some of the tutorials, which were recorded and converted to video files now available on the IETF education pages.

IETF 85, Atlanta

Intrigued by the possibilities offered by WebRTC, we started working with the Opus codec. At IETF 85 we made available an additional stream for remote participants—an HTTP-based Opus stream, which could be played in either HTML5 or an external player. We also added a Flash-based video stream.

IETF 86, Orlando

A decisive improvement was made for IETF 86: we changed the audio backend of our platform and got rid of the narrowband audio constraint by moving to a higher quality, wideband audio mix. Participants were now able to get a real-time audio feed as good as the official MP3 stream. The improved audio quality was a welcome addition to recordings and enabled us to better integrate the Opus codec into our platform and to take advantage of its novel features.

IETF 87, Berlin

The Opus integration motivated us to organize a high-quality, remote participation experiment based on Opus for the technical plenary at IETF 87, whose topic was Opus itself. We envisioned a completely Web-based attendance to the plenary, involving a high-quality VP8 video feed and a 48kHz mixed audio feed based on Opus. Our efforts were briefly discussed during the plenary.

IETF 87 was also a training ground for experiments in recording tutorials, including a brief presentation of the MILE WG by Kathleen Moriarty. By that time, session recordings had become a fundamental asset for the IETF community. IETF chairs rely on them when editing meeting minutes. WG participants, in turn, count on such synchronized multimedia assets for ex-post fruition of one or more recorded sessions.

Next Steps

We recently obtained a formal agreement with IETF management for support of an increasing number of sessions at upcoming meetings. (We supported nearly 40 sessions at IETF 88.)

Future meetings will be both challenging and stimulating as we simultaneously cover more and more sessions. The plan is to cover all of them in Honolulu at IETF 91. With that goal in mind, we're working on new features, including ways to automate the scribe role (instead of relying on a local participant for videos and slides) and obtain detailed participation statistics. We're also seeking a more seamless integration with the community's tools (meeting agenda, materials page, meeting minutes, etc.).

We're proud to be working with and for the community—whether you attend in person or not, we look forward to seeing you in London.

The Meetecho team at IETF 83, (left to right) Lorenzo Miniero, Simon Romano, Tobia Castaldi, and Alessandro Amirante

An Overview of the GeoNet BoF

By Alexandru Petrescu, Melinda Shore, Georgios Karagiannis, Dino Farinacci, Dimitri Papadimitriou, Alison Chaiken, Bastiaan Wissingh, Duan Shihui, Rex Buddenberg, Carl Reed, and Brian Dickson

GeoNet stands for geographical networking. The concept relates to the intertwining of Internet Protocol (IP) networking with geographical addressing. As used today, IP routing and addressing operate outside of geographic parameters such as coordinates or postal addresses. Possible applications of future Internet-wide geo-networking mechanisms include, but are not limited to, dissemination of IP packets to particular geographical areas, and precise tracking of package positions during a shipping process. More use cases are under discussion.

The Birds-of-a-Feather (BoF) meeting at IETF 88 was the result of a multiyear effort initiated in 2012 in the context of IP communications in vehicular networks. The initial email list is still being used despite a change in the name—it is hosted at https://ietf.org/mailman/listinfo/its and includes approximately 250 subscribers. We held a bar BoF at IETF 87 with the participation of some key contributors, including the chair of ETSI ITS WG3 "Networking and Transport," and an IAB shepherd. After the publication of an initial set of Internet-Drafts, a request to meet as an official GeoNet BoF was approved by the IESG. More than 100 participants attended the Vancouver BoF meeting.

Current discussions target the development of a problem statement that will identify realistic goals for a potential working group. We also are refining a list of use cases around the topic of geographical dissemination of IP packets.

Current discussions target the development of a Charter and of a problem statement that will identify realistic goals for a potential working group. We also are refining a list of use cases around the topic of geographical dissemination of IP packets. While the first use case was related to vehicular communications (see below), more uses have been identified by partners at various organizations. The use case discussion is ongoing.

For the London meeting, the group is preparing a charter proposal that would briefly lay out the problem, list the use-cases, and develop a list of deliverables. See the current text at https://github.com/melindashore/geonet.

Older Activities

Earlier efforts in this area targeted vehicular communications with geo-networking as a potential side-product. Vehicular traffic efficiency and management improve traffic flow, traffic coordination, and traffic assistance, and provide up-to-date local information, maps, and relevant messages well-defined in space and time. This has obvious applications in ensuring traffic safety.

A fully functional mechanism for geographical dissemination of data to vehicles over IP networks would need the participation of many underlying mechanisms. Previous discussions revolved around the use of the DNS subsystem in the initial steps of resolving an IP address into a set of geocoordinates, and vice-versa. However, during the BoF meeting in Vancouver this was discarded based on certain drawbacks of a fully DNS-based architecture.

One aspect considered very early is related to IP-over-foo. In the context of vehicular communications several wireless link layers are used for exchanging data among vehicles—one is IEEE 802.11p, which makes use of spectrum in the 5.9GHz band. The particularly dynamic nature of vehicle movement leads to stringent requirements on the use of IP datagrams on these dynamic links, hence a potential activity of IP-over-foo, in which foo equals 802.11p, has been identified. However, at this time, this topic seems dedicated solely to vehicular communications, rather than the generic problem of geographical dissemination of data across paths that may traverse the Internet. In addition, several groups of external Standards Development Organizations (e.g., IEEE P1609.3, ETSI ITS TC WG3, and ISO TC204 WG16) have already developed stack models that are in near-deployment phases.

Other interest has been expressed in vehicle-to-vehicle IP networking, alarm distribution among vehicles, vehicles in smart cities, autonomous driving, and more.

Current Goals

Mechanisms and IETF protocols are needed for authorized source nodes anywhere in the Internet to disseminate packets to other nodes in areas described by geographic parameters, while respecting the privacy concerns of sender and receiver. Parameters such as geographical coordinates and other geo-locators, such as civic addresses, should be usable in order to specify the destination.

Other interest has been expressed in vehicle-to-vehicle IP networking, alarm distribution among vehicles, vehicles in smart cities, autonomous driving, and more.

Privacy concerns need to guarantee from the start that the new dissemination mechanism cannot be used to identify the geographical situation of computers issuing requests to resources or to prevent access based on such supposed identification.

The main use cases currently under discussion are listed below. We expect that some will be merged to others or simply disappear. We will be meeting in London to discuss this.

- Dissemination to a geographical area (figure 1). A source node, which may be located anywhere, sends packets to a wireless access router through the Internet. Those wireless access routers are selected based on geographical location information, and traffic is routed to them using the IPv6 address of the router and conventional IP routing. Each of the destination access routers then copies and broadcasts the received packets to listeners within its radio coverage area.
- Goods tracking (figure 2). A good delivered by a shipping organization has a provider-independent IP address. This good is tracked in that its geographical position is known to end-users continuously throughout the entire delivery process. The IP address of the good is associated to the geographical coordinates of the router to which it connects. Using IP addresses enables very finely grained and precise tracking.
- Vehicular traffic safety, efficiency, management, and infotainment. The data disseminated to road side units (RSUs) is relevant for traffic management and on-board infotainment.
- Mobile roadside unit. Most RSUs are placed at a fixed geographical location that will most likely not be changed until the device -[p0eitherreachesitsendoflifeorisno longer needed at that location. But a mobile roadside unit, on the other hand, is portable and not switched off while moving, meaning that among other settings its geographical position adjusts as it moves. Such a mobile RSU allows more flexible use in multiple situations. For example, at a location along a road where there is ongoing road works, a road worker could take a Mobile RSU, position it somewhere at the road works site, and start sending warning messages to incoming vehicles. The next day it would position it elsewhere.
- Identification of originating area. In some IP network deployments in large cities, Internet Service Providers (ISPs) and Internet Content Providers (ICPs) need to identify which parts of the city originate the most IP traffic. When it has knowledge of the geographic location of an IP address, it can deduce the origin of the IP traffic and thus subsequently schedule its resources among the entire network to realize the best service for the Internet users.

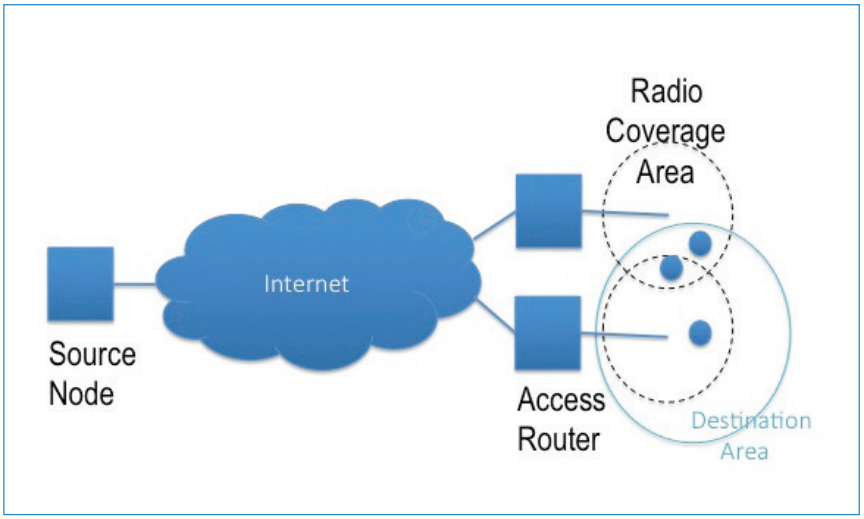


Figure 1. DIssemination to a Geographical Address

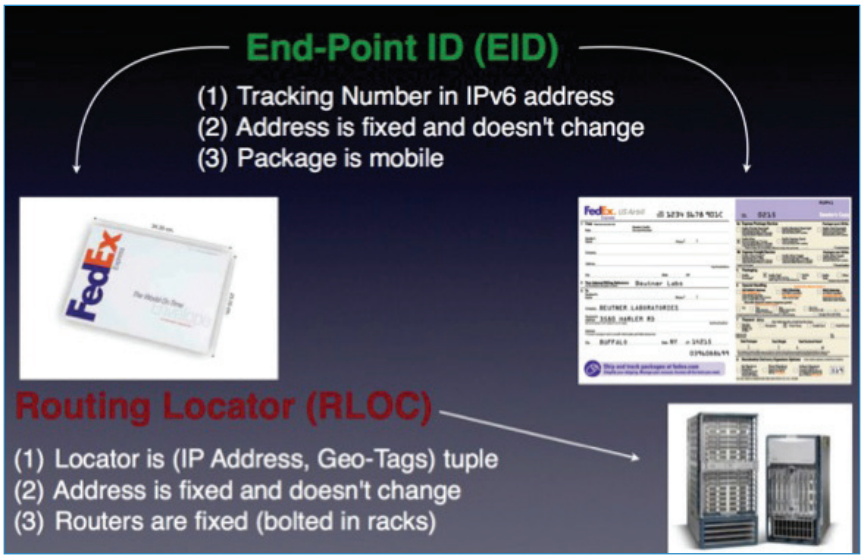


Figure 2. Goods Tracking

Continued on next page

- Geolocation of an instrumented ambulance. When an ambulance transports a casualty, the primary objectives are to get the medical data (e.g., vital signs) securely delivered to the hospital by telemetry through the Internet and to enable the Emergency Room doctor to remain connected to the emergency medical technicians in the ambulance. In addition, during this process the communication between the ambulance driver and the dispatcher, and the communication afforded by the ambulance hotspot to public authorities (Bring-Your-Own-Device, Bring-Your-Own-Communication), is critically qualified by geographical coordinates and geolocators such as civic addresses. This case should be further described because some of these functions are sometimes provided over radio by way of voice dispatching and by GPS trackers.

Relationships between GeoNet and other IETF Working Groups

Any new use cases GeoNet comes up with that require protocol changes for any overlay technology, such as LISP, can be done in the appropriate protocol working groups, such as the LISP WG.

The GEOPRIV working group concentrates on protocols that allow applications to represent location/geography objects and to allow users to express policies on how these representations are exposed and used. Moreover, GEOPRIV analyses the authorization, integrity, and privacy requirements that must be met when these representations of location/geography are created, stored, and used. GeoNet mainly focuses on how IP routing and addressing use such location/geography representations.

The LISP WG mainly focuses on network-layer-based protocol solutions that enable the separation of routing locators (where you are attached to the network) and identifiers (who you are) in one number space. GeoNet mainly focuses on how IP routing and addressing use geographic parameters to disseminate packets from a sender located anywhere in the Internet to nodes in the area specified by these geography parameters.

The most important next steps are to refine the set of use cases to a subset of achievable goals and agree on a charter. We will be meeting in London to progress both.

The ECRIT WG focuses on how location data and call routing information are used to enable communication between a user and a relevant emergency response center. The ECRIT WG has specified protocols to map emergency services identifiers and geodetic or civic location information to service contact URIs. GeoNet mainly focuses on how IP routing and addressing use location information to disseminate packets from a sender located anywhere in the Internet to nodes that are located in the area specified by this geodetic or civic location information.

Next Steps

The most important next steps are to refine the set of use cases to a subset of achievable goals and agree on a charter. We will be meeting in London to progress both.

The initial objectives of the group are focused on a common vocabulary for contexts using IP protocols and geography coordinates, on a data definition of geolocators, and on defining a bidirectional relationship—and not a mechanism—between geospatial locators and IP locators.

For a complete solution, many solutions at different layers would be needed for the items below:

- The accurate representation of geographic areas using coordinates such as geolocators/logical coordinates and geographical/physical coordinates, and for the naming of geographic areas.
- Ensuring that geographical area information (for example, geolocators, names, and physical geographic coordinates) is accurately mapped to an IP address or addresses.
- Databases associating locations with addresses may be maintained at the source, intermediate or edge nodes, and at specific IP locator nodes.
- Ensuring that an IP address can be accurately mapped to geographic area information (geolocators, names, and geographic physical coordinates). Note that this refers to the addresses of access routers, roadside units (RSUs), and so on, and not end nodes.
- Ensuring that data packets generated by source nodes placed arbitrarily in the Internet can be forwarded over multiple hops by using, where possible, geographic location representations of the destination node(s) and/or the intermediate nodes for the routing decisions, instead of using their IP addresses. Note that in order to solve the above challenge it is not mandated that all nodes located on the path from source to destination nodes are able to forward packets using the geocoordinates of the destination node(s) and/or the intermediate nodes for routing decisions. This is emphasized by using the words *where possible.*

Internet Governance for IETFers

By Andrew Sullivan

The Internet Governance Update (IGOVUPDATE) Birds of a Feather (BoF) session was held at IETF 88 in Vancouver, Canada. The topic was unusual in that it was not about a protocol, or even about discussion that might be needed for future technical developments. Instead, this was an effort to encourage understanding by the Internet Engineering Task Force (IETF) of what other actors are doing or planning to do with the standards that the IETF produces. As is normal, the minutes for the BoF are in the IETF meeting proceedings.

There were two main topics of focus for this meeting. In the Web Extensible Internet Registration Data Service (WEIRDS) working group, the IETF is working on a protocol intended to be used instead of WHOIS. The Internet Corporation for Assigned Names and Numbers (ICANN) is also investigating issues related to the data that is available in WHOIS, and how and to whom that data is available. It seemed useful to show how these two efforts affected one another, so half the BoF was devoted to that issue.

The second topic was an overview of what happened at the Internet Governance Forum (IGF) in Bali. This was important partly because the IETF sent some people to the IGF to talk about what the IETF does. In addition, during the IGF some proposals for new Internet governance initiatives emerged.

WEIRDS and WHOIS

Chris Disspain presented a description of the progress of the ICANN Expert Working Group (EWG) on gTLD Directory Services. Disspain is the ICANN Board liaison to the EWG. He observed that there are two kinds of issue. One has to do with the protocol itself: the WHOIS protocol has no structure to its data, and is badly designed for the international Internet we have today. The other kind has to do with policy questions such as accuracy, consistency, and privacy.

Next, Murray Kucherawy, WEIRDS Working Group cochair, outlined the progress of the WG in delivering a new Registry Data Access Protocol (RDAP) that uses hypertext transfer protocol (HTTP). The idea is to use the facilities that HTTP already offers in order to reduce the effort required to satisfy all the needs.

The goal of the discussion was to highlight the ways in which external needs of policy-making bodies can be satisfied by IETF work without the IETF work grinding to a halt while those needs are determined.

The goal of the discussion was to highlight the ways in which external needs of policy-making bodies can be satisfied by IETF work without the IETF work grinding to a halt while those needs are determined. As Olaf Kolkman (the other WEIRDS cochair) observed, the WG is depending on the extensibility of its design. The RDAP specification can proceed for number resources even while the exact problem description for name resources is not ready. Once the latter is ready, more extensions can be added to meet those needs. The result, it is hoped, will be able to satisfy even unknown policy requirements.

Some BoF participants expressed skepticism about this approach. But unless the IETF is prepared to do nothing until external parties establish all requirements, it may not be able to do any work. In the case of WHOIS, the policy disputes have been going on for more than 10 years. If we want to proceed with flexible protocols, this is our way forward.

The Internet Governance Forum

The purpose of the discussion of the IGF was partly to make IETF participants aware of the way in which others in the world view "the technical community," and partly to begin a discussion of how we might respond to those views. Some of these issues have come to the fore as a result of political developments having little to do with the IETF. Nevertheless, they make the IETF's job more challenging.

One of the things that came out of the IGF meeting was a plan for a spring 2014 meeting in Brazil on the topic of Internet governance. It is unclear the extent to which this meeting, or others, will continue to favour the multistakeholder approach with which many of us are familiar. A competing model is a more traditional, multilateral approach in which governments negotiate exclusively with one another. Such an

Continued on next page

It is unclear the extent to which [the spring 2014 Bali] meeting, or others, will continue to favour the multistakeholder approach with which many of us are familiar. A competing model is a more traditional, multilateral approach in which governments negotiate exclusively with one another.

Internet Governance for IETFers, continued

approach could be bad for the IETF traditions of standards development.

One of the central issues here is a mismatch of expectations. Organizations that work primarily through or extensively with governments often try to divide issues by representative groups. The IETF does not work that way: we officially take input from individuals, individuals act within working groups, and so on. This can be an awkward interface for government employees, who often are not allowed to deviate from an official government position. As a community we may have been loathe to engage in governance topics because we do not have a representative model, and cannot appoint a representative to interact with other bodies.

There was a great deal of feedback after the IGF about how useful it was to have Jari Arkko (as IETF chair) at the meeting, and it seems important to continue this work. In an effort to continue toward a resolution, BoF participants were invited to discuss issues on the internetgovtech@iab.org list.

As the importance of the Internet grows, and especially in light of changing political circumstances, the IETF needs to establish how best to address policy demands.

Conclusion

While the two topics for this meeting may appear to be quite different, they have at their cores the fundamental question of how the IETF can deal with groups involved with policy rather than protocol. The policy/protocol distinction, while often relied upon, is not really as clear as one might wish. As the importance of the Internet grows, and especially in light of changing political circumstances, the IETF needs to establish how best to address policy demands. Advancing that work is what IGOVUPDATE at IETF 88 was all about. There will surely be more of this kind of work at future meetings.

ONLINE EXCLUSIVE ARTICLE: Bits-N-Bytes–Running Code at IETF

Don't miss this special feature to *The IETF Journal* by John Jason Brzozowski, Comcast; Tina Tsou, Huawei; David Fang, Huawei; Diego Lopez, Telefónica I+D; and Glen Turner, A10

The first IETF Bits-N-Bytes took place in the summer of 2012. While today's Bits-N-Bytes concept is evolving and maturing rapidly, it has deep roots in the technical and operational communities. See this exclusive online feature for behind-the-scenes details about some of the event's key exhibits over the past two years. http://www.internetsociety.org/fr/publications/ietf-journal

IRTF Update

By Lars Eggert

During IETF 88 in Vancouver, Canada, five out of the nine then-chartered Internet Research Task Force (IRTF) research groups (RGs) held meetings:

- Internet Congestion Control Research Group (iccrg)
- Information-Centric Networking (icnrg)
- Network Complexity Research Group (ncrg)
- Network Management Research Group (nmrg)
- Software Defined Networking Research Group (sdnrg)

In addition to the meetings of the already-chartered research groups, a new proposed research group on Network Coding held a third side meeting. The discussion was positive, and the Network Coding Research Group (nwcrg) was formally chartered on 13 November 2013.

Since IETF 87, one new RFC (Request for Comment) has been published on the IRTF RFC Stream by the Scalable Active Multicast Research Group (samrg): RFC 7019 on "Application-Layer Multicast Extensions to REsource LOcation And Discovery (RELOAD)."

The IRTF Open Meeting at IETF 88 was the venue for the final Applied Networking Research Prize (ANRP) winner of 2013 to present his research. Idilio Drago presented insights into characterizing the traffic and workloads of the Dropbox cloud storage system. Read more about Drago's work on page 23.

The 2014 nomination cycle of the ANRP concluded after IETF 88 with 46 nominations. The selection committee selected six award winners for 2014, with each of the three IETF meetings in 2014 scheduled to see two award talks, which will be announced shortly before each meeting.

Join the IRTF discussion list to stay informed about these and other happenings! The website is http://www.irtf.org/mailman/listinfo/irtf-discuss.

Idilio Drago (left), final ANRP winner of 2013, and Lars Eggert, IRTF chair

CodeMatch Programme Aims to Attract Computer Science Students to the IETF

By Carolyn Duffy Marsan

In an effort to boost its inclusivity, the Internet Engineering Task Force (IETF) is considering a programme aimed at encouraging university students to engage in working groups.

The goal of the effort—dubbed CodeMatch—is to market the IETF to budding computer scientists as a community that can help deepen their skills. University students would be encouraged to help develop new Internet protocols, draft Request for Comments (RFCs), and participate in interoperability testing with vendors—all activities that they can highlight on their resumes. In return, the IETF would gain access to a pipeline of fresh participants.

> "This is an opportunity to expose university students to the IETF at an early stage and show them that the IETF is something they can use to get ahead in the workplace."
>
> —Kathleen Moriarty
> Global Lead Security Architect, EMC

"This is an opportunity to expose university students to the IETF at an early stage and show them that the IETF is something they can use to get ahead in the workplace," said Kathleen Moriarty, cochair of the IETF's Diversity Design Team, which proposed CodeMatch. "The students would have the opportunity to dive into and understand really deep levels of Internet protocols. Letting them know that this experience could be an advantage to them is really important."

Moriarity, global lead security architect at EMC, said CodeMatch would provide an online repository in which IETF working groups could post code they need written. Students would participate in bake-off style competitions to write the code, which would be widely available as open source.

"CodeMatch is an online matching service where IETF working groups could post needs for code, and where computer science students and researchers could find opportunities to write open source coding projects to burnish their resumes," Moriarty explained. "It gives us an opportunity to make connections with the open source community… Creating relationships between the IETF and the open source community is probably the strongest reason to go ahead with this."

Although the idea for CodeMatch originated as a way to attract women computer science majors to the IETF community, it would be open to male university students, too.

"We need to improve our regional diversity, too, with additional exposure and connections to the open source community," Moriarty said. "Hopefully we would attract developers and students in other countries. I talked to a computer science professor from Chile, and she was interested in assigning projects to her students via CodeMatch."

Moriarty proposed CodeMatch after she spoke about the IETF at the Grace Hopper Celebration of Women in Computing Conference, the world's largest technical c onference for women in computing. Run by the Anita Borg Institute, the conference was held in Minneapolis in October 2013. The Internet Society is a sponsor of the three-day event and provides scholarships for international attendees.

"We are delighted that [Moriarity] was part of the Internet Society's 2013 contingent to the Grace Hopper Celebration meeting. CodeMatch is an ideal bridge for increasing the awareness of the value of IETF and open standards to a new community of emerging professionals while also bringing different and important voices to the IETF and the standards development process," said Toral Cowieson, senior director of Internet leadership at the Internet Society.

Although the idea for CodeMatch originated as a way to attract women computer science majors to the IETF community, it would be open to male university students, too.

Moriarty hopes CodeMatch will attract both women computer scientists and other university students from around the globe to participate in the IETF.

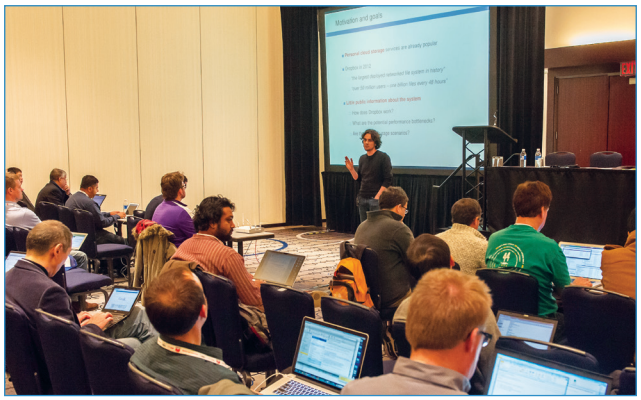
Cloud Storage Dissected: A View Inside Dropbox

Applied Networking Research Prize winner presentation

By Mat Ford

Idilio Drago, the latest recipient of the Applied Networking Research Prize (ANRP) was in Vancouver to receive his award and present the research work for which he was selected. Idilio received his award for characterizing the traffic and workloads of the Dropbox cloud storage system (Idilio Drago, Marco Mellia, Maurizio M. Munafo, Anna Sperotto, Ramin Sadre, and Aiko Pras. Inside Dropbox: Understanding Personal Cloud Storage Services. Proc. ACM Internet Measurement Conference, November 2012, Boston, MA, USA.).

Presenting to the Internet Research Task Force open meeting, Drago gave a master class in reverse engineering in his talk titled, "Inside Dropbox: Understanding Personal Cloud Storage Services." Drago recently received his PhD from the University of Twente in the Netherlands, and he was the fourth and final ANRP winner for 2013.



Idilio Drago, ANRP winner, presents his work on characterizing the traffic and workloads of the Dropbox cloud storage stystem.

Drago and his coauthors' analysis illustrates the considerable volume of traffic that cloud storage services now represent by total volume of traffic on a campus network—up to a third of YouTube traffic in one case. Their work also identified scalability problems resulting from system design choices. and they were able to observe these inefficiencies being resolved by the developers during the course of their study. Downloads of their final paper are available online on the IRTF Web site at http://irtf.org/anrp.

The selection committee for the 2014 ANRP awards has concluded sifting through the highest number of nominations to date. The call for nominations for the 2015 award cycle will open in autumn 2014. Put it in your calendar now and submit your nominations when the time comes!

ABOUT THE APPLIED NETWORKING RESEARCH PRIZE

The ANRP is awarded for recent results in applied networking research that are relevant for transitioning into shipping Internet products and related standardization efforts. The goal of the prize is to recognize the best new ideas in networking, and bring them to the Internet Engineering Task Force (IETF) and its research arm, the Internet Research Task Force (IRTF), especially in cases where they would not otherwise see much exposure or discussion.

Researchers with relevant, recent results are encouraged to apply for this prize, which offers them the opportunity to present and discuss their work with the engineers, network operators, policy makers, and scientists who participate in the IETF the IRTF. Third-party nominations for this prize are encouraged.

The Applied Networking Research Prize consists of:

- an invited talk at the IRTF Open Meeting
- a cash prize of $500 (USD)
- a travel grant to attend a week-long IETF meeting (including airfare, hotel, registration, and stipend)
- recognition at the IETF plenary
- an invitation to related social activities
- potential for additional travel grants to future IETF meetings, based on community feedback

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'll review the BoFs that took place during IETF 88, including their intentions and outcomes. If you're inspired to arrange a BoF meeting, please be sure to read RFC 5434: Considerations for Having a Successful Birds-of-a-Feather (BoF) Session.

Internet Governance Update (igovupdate)

Description: This meeting provided the IETF community with an opportunity to hear about and discuss some Internet governance developments, especially as they relate to protocol development in the WEIRDS working group (WG). There was also an update on proceedings at the Internet Governance Forum.

Proceedings: http://www.ietf.org/proceedings/88/minutes/minutes-88-igovupdate

Outcome: The meeting generated a lively discussion about the evolving Internet governance landscape, the issues that people believe need to addressed, and where those issues have touch points with the IETF.

RFC Format Design Team Update (rfcform)

Description: This will serve as a report out to the community and opportunity for discussion on the requirements for tool specifications for a revised RFC Format.

Proceedings: http://www.ietf.org/proceedings/88/minutes/minutes-88-rfcform

Outcome: The RFC Editor provided an update on the progress of the RFC Format Design Team. The community engaged in a detailed discussion of various open and ongoing issues.

Internet-wide Geo-Networking (geonet)

Description: Internet-wide geo-networking concerns IP-layer extensions that allow source nodes anywhere in the Internet to disseminate packets to all/any node(s) with geographic location awareness within a specified destination area. Use cases include environmental monitoring and vehicular networking.

Proceedings: http://www.ietf.org/proceedings/88/minutes/minutes-88-geonet

Outcome: More work is required to narrow the scope of this proposed activity so that it more closely aligns with IETF work. Another BoF meeting seems necessary to achieve that. Approximately 20 attendees expressed interest in working on documents on this subject.

Handling Pervasive Monitoring in the IETF (perpass)

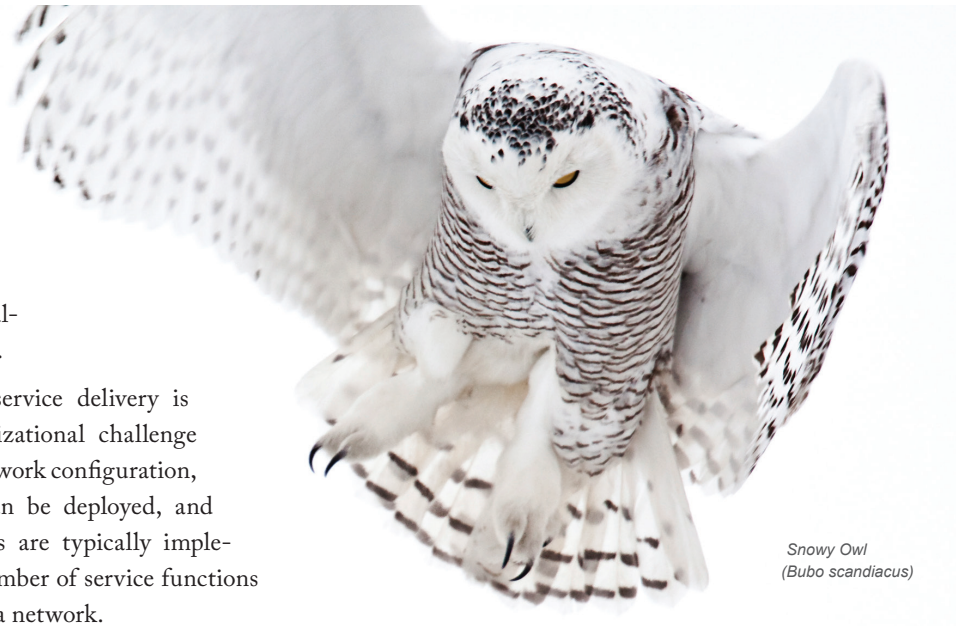
Description: The perpass BoF was for discussion of the privacy properties of IETF protocols and concrete ways in which those properties could be improved. The meeting was not intended to be a precursor to formation of a WG, but rather to, for example, discuss ways in which IETF protocols at any layer can be made more robust against pervasive passive monitoring. If subsequent protocol work is to be done in the IETF, it will likely happen in existing or new protocol-specific WGs.

Proceedings: http://www.ietf.org/proceedings/88/minutes/minutes-88-perpass

Outcome: A lot of good discussion including identification of many potential work items for IETF, IAB, and others. The threat model is fairly mature. Discussion will continue on the perpass mailing list (https://www.ietf.org/mailman/listinfo/perpass).

Starling (Sturnus vulgarus)

Service Function Chaining (sfc)



Snowy Owl (Bubo scandiacus)

Description: Network operators often utilize service functions such as packet filtering at firewalls, load-balancing, and transactional proxies (e.g., spam filters) in the delivery of services to end users. Delivery of these types of services is undergoing significant change with the introduction of virtualization, network overlays, and orchestration.

Deploying service functions to support service delivery is currently both a technical and an organizational challenge involving significant modification to the network configuration, impacting the speed at which services can be deployed, and increasing operational costs. Such services are typically implemented by the ordered combination of a number of service functions that are deployed at different points within a network.

Today, common deployment models have service functions inserted on the data-forwarding path between communicating peers. Going forward, however, there is a need to move to a model in which service functions—physical or virtualized—are not required to reside on the direct data path and traffic is instead steered through required service functions wherever they are deployed.

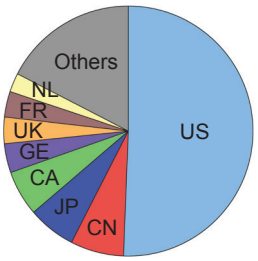
Deploying service functions to support service delivery is currently both a technical and an organizational challenge involving significant modification to the network configuration, impacting the speed at which services can be deployed, and increasing operational costs.

For a given service, the abstracted view of the required service functions and the order in which they are to be applied is called a Service Function Chain (SFC). An SFC is instantiated through selection of specific service function instances on specific network nodes to form a service graph: this is called a Service Function Path (SFP). The service functions may be applied at any layer within the network protocol stack (network layer, transport layer, application layer, etc.).

Proceedings: http://www.ietf.org/proceedings/88/minutes/minutes-88-sfc

Outcome: This meeting was very well attended. The group of active participants have made considerable progress since their last meeting in Berlin (where they had a non-WG forming BoF). Lots of attendees volunteered to work on this topic and write documents. More work is required to define key terminology and more discussion will be required on the mailing list. (Editorial note: The Service Function Chaining working group was chartered on 20 December 2013).

IETF 88 At–A–Glance



On-site attendees: 1,142

Newcomers: 123

Number of countries: 54

IETF Activity since IETF 87 (July 2013–November 2013)

New WGs: 7

WGs closed: 0

WG currently chartered: 115

New or revised Internet-Drafts (I-Ds): 1547

IETF Last Calls: 105

Internet-Drafts approved for publication: 101

RFCs published: 55

- 46 IETF (42 WG, 7 Individual/AD Sponsored), 1 IAB, 1 IRTF, 4 Independent

Live and Social Media During the Technical Plenary

- YouTube: 276 max concurrent viewers, 748 total views by 3:30pm
- Twitter: 837 tweets on #IETF88, exposure via @IETF= 217,466, exposure via #IETF88=1,658,351, 40 new followers to @IETF
- Facebook: 327 Likes

Antiharassment Policy (www.ietf.org/iesg/statement/ietf-anti-harassment-policy.html)

- Specifies "IETF participants should not engage in harassment," and establishes an ombudsperson.

Mentoring Programme now has 58 participants

IANA Activity since IETF 87 (July 2013–September 2013)

Processed 946+ IETF-related requests, including:

- Reviewed 79 I-Ds in Last Call and reviewed 64 I-Ds in Evaluation
- Reviewed 66 I-Ds prior to becoming RFCs, 35 of the 66 contained actions for IANA

SLA Performance

- Processing goal average for IETF-related requests: 99%
- Currently drafting the 2014 SLA

IANA and DNSSEC

- 119 TLDs have a full chain of trust in the root, see http://stats.research.icann.org/dns/tld_report/

RFC Editor Activity since IETF 87 (July 2013–November 2013)

Published RFCs: 62

- 26 Standards Track, 3 BCP, 6 Experimental, 27 Informational

IETF Meeting Calendar

IETF 89
2–7 March 2014
Host: ICANN
Location: London, England

IETF 90
20–25 July 2014
Host: Ericsson
Location: Toronto, ON, Canada

IETF 91
9–14 November 2014
Host: Cisco
Location: Honolulu, HI, USA

IETF 92
22–27 March 2015
Host: TBD
Location: Dallas, TX, USA

For more information about past and upcoming

IETF Meetings

http://www.ietf.org/meeting/

Special thanks to

HUAWEI

for hosting IETF 88

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

Afilias Google Microsoft NBCUniversal SIDN

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

Afilias ARIN American Registry for Internet Numbers CISCO comcast Juniper NETWORKS NBCUniversal RIPE NCC SIDN

pub-IETFJv9.3-201302l8-en

Published three times a year
by the Internet Society.

Galerie Jean-Malbuisson 15
1204 Geneva, Switzerland

Email
ietfjournal@isoc.org

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

Editor's Note

The IETF Journal adheres to the *Oxford English Dictionary*, 2nd Edition.

IETF Journal
IETF 88 • Volume 9, Issue 3 • March 2014

IETF Journal

Internet Society
Galerie Jean-Malbuisson 15
1204 Geneva, Switzerland