VOLUME 13, ISSUE 2 • NOVEMBER 2017

IETF® Journal

A report from IETF 99, July 2017, Prague, Czech Republic. Published by the Internet Society in cooperation with the Internet Engineering Task Force.*

INSIDE THIS ISSUE

CORRECTION

The authors of "Segment Routing: Cutting Through the Hype and Finding the IETF's Innovative Nugget of Gold" (Issue 13, Vol. 1) are Adrian Farrel and Ron Bonica. The editor apologizes for the error.

FROM THE EDITOR'S DESK

By Mat Ford

THIS ISSUE MARKS THE FINAL HARDCOPY VERSION OF THE *IETF JOURNAL.* SINCE 2005, the *Journal* has been printed three times a year, and distributed at IETF meetings and by postal mail. As we explain in "We're Going Digital!" (this page), starting in 2018 we'll be shifting our focus to ietfjournal.org. Follow us on Twitter (@ietfjournal) and Facebook (facebook.com/IETFJournal) to stay current with our future *IETF Journal* activities.

The IETF returned to the beautiful European city of Prague for its 99th meeting. It was a busy meeting with lots of interesting work; we share here only a snapshot of the events and discussions that made this meeting so memorable.

In this issue, you'll learn about implementation work taking place in the Human Rights Protocol Considerations Research Group, the latest security updates to the Network Time Protocol, new email-related Working Groups JMAP and EXTRA, as well as the important coding work that took place as part of the IETF Hackathon.

Our regular columns from the chairs and coverage of the Birds-of-a-Feather meetings and presentations from the Applied Networking Research Prize winners wrap up the issue.

We are hugely grateful to all of our contributors. Please send comments and suggestions for contributions to ietfjournal@isoc.org or tweet us @ietfjournal.

WE'RE GOING DIGITAL!

By Megan Kruse

MUCH HAS CHANGED SINCE THE FIRST *IETF JOURNAL* WAS PUBLISHED IN 2005: exponentially more people are online in general, and more people are reading *Journal* articles online and via social media. The IETF Blog covers many of the organization's day-to-day updates and Chair reports, items we once relied on the *Journal* to share. And since the launch of our new website last year, more readers than ever are clicking through to our online version.

Continued on page 4

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

MESSAGE FROM THE IETF CHAIR

By Alissa Cooper

Alissa Cooper, IETF Chair

THE MORE THAN 1,000 YEAR OLD CITY OF PRAGUE, CZECH REPUBLIC, WAS HOST TO the 99th IETF meeting 16-21 July 2017. Exciting work went on across more than 100 Working Groups, plus Birds-of-a-Feather (BoF) sessions, plenary talks, and the kind of impromptu hallway and other meetings that make this event a thrice-yearly draw for Internet technologists around the globe. Following are just a few highlights from the meeting.

Premeeting Events

Nearly 200 people participated in the 8th Hackathon on 15-16 July. In about two dozen teams, participants collaborated on more than 25 code projects spanning the breadth of IETF protocols, including security, DNS, transports, and the Internet of Things. (See page 12.)

As usual, folks were also invited to join the Code Sprint[1] on 15 July to work on tools for the IETF community.

While not an IETF event, the Applied Networking Research Workshop[2], sponsored by the Association for Computing Machinery (ACM), the Internet Research Task Force, and the Internet Society, also took place on 15 July. The workshop provided a venue for discussing emerging results in applied networking research related to measurements, transport, implementation and operational issues, and Internet health metrics.

> **Exciting work went on across more than 100 Working Groups, plus Birds-of-a-Feather (BoF) sessions, plenary talks, and the kind of impromptu hallway and other meetings that make this event a thrice-yearly draw for Internet technologists around the globe.**

Meeting Events

Those interested in 5G attended the netslicing BoF, which looked at isolation of resources and virtual network functions to support a variety of services. There was also a plenary lunch panel about 3GPP and IETF collaboration on 5G.

Other BoFs included banana, which focused on developing solutions to support dynamic path selection on a per-packet basis in networks with more than one point of attachment to the Internet; ideas, which aimed to standardize a framework to provide identity-based services for use by any identifier-location separation protocol; and iasa 2.0, which continued the community discussion about administrative rearrangements for the IETF. Also in the realm of new work proposals, the IPPM Working Group discussed a charter update that allows the WG to take on work related to in-situ operations, maintenance, and administration (OAM).

Continued on page 4

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

Recent IESG Document and Protocol Actions

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

WORDS FROM THE IAB CHAIR

By Ted Hardie

Ted Hardie, IAB Chair

AS PART OF ITS ARCHITECTURAL OVERSIGHT, THE IAB PERIODICALLY CONVENES workshops to "perform in-depth reviews of particular architectural issues". While the results of the workshop are typically presented in a formal report, I'm happy to share some early reflections on our most recent workshop.

ENAME Workshop

The IAB held a workshop on Explicit Internet Naming Systems on 10-11 October in Vancouver, B.C., and there are a couple of interesting early conclusions to draw. The first conclusion is actually about the form of the workshop, which was an experiment by the IAB. While many of our workshops run like mini conferences, with paper presentations and follow-on questions, this workshop was structured as a retreat. There was a relatively small number of participants gathered around a common table space with sessions organized as joint discussions around specific topics. Moderators kept the conversations on topic, and discussants kept it moving forward if it lagged.

One clear conclusion from this workshop was that the choice of identifier structure and protocol mechanics will constrain the set of possible human interfaces. When those constraints don't match the needs of the human users, the resulting friction generates a lot of heat (and not much light).

The result was one of the most interactive workshops I've attended. While we did have to run a queue in most sessions (and the queues could get a bit long), the conversations had real give-and-take, more like an IETF hallway discussion than a series of mic-line comments.

While I don't expect that this style would be appropriate for all our workshops, it's useful to know that this retreat style can work. I suspect we would use it again in other situations where the IAB is trying to step back from the current framing of an issue and synthesize a set of new approaches.

A second early conclusion is that the IAB was right in suspecting that its previous framing of the issues around Internet naming and internationalization wasn't quite right. Among other things, that framing had us trying to push human interface considerations up the stack and away from the protocol mechanics that worked on what we saw as identifiers. One clear conclusion from this workshop was that the choice of identifier structure and protocol mechanics will constrain the set of possible human interfaces. When those constraints don't match the needs of the human users,

Continued on page 5

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

Message from the IETF Chair, continued from page 2

We continued to see high interest in ongoing work related to data modeling, QUIC, and security. Among other sessions, the OPSAWG session offered discussion about managing the development and use of YANG models, and the joint CCAMP/MPLS/PCE/TEAS session focused exclusively on YANG models. The QUIC WG met jointly with the HTTPBIS WG to discuss interaction between QUIC and HTTP. And in the security area, both the TLS and ACME WGs shared where they were in terms of finalizing several core deliverables, and the SAAG session featured a talk on post-quantum crypto.

Thank You

Of course we couldn't offer IETF meetings without the support of our sponsors. Big thanks to IETF 99 hosts Comcast, NBC-Universal, and CZ.NIC, and to all of our sponsors.

> **We continued to see high interest in ongoing work related to data modeling, QUIC, and security.**

Footnotes

1. https://trac.tools.ietf.org/tools/ietfdb/wiki/IETF99Sprint.
2. https://irtf.org/anrw/2017/.

We're Going Digital!, continued from page 1

> **We look forward to closing our print version and launching ourselves fully into the digital world in 2018.**

Like innumerable print publications before us, we took a hard look at the economics of printing and shipping issues around the world. And between greater access and less expense, the decision was simple. We look forward to closing our print version and launching ourselves fully into the digital world in 2018.

Our new format will focus on long-form articles—the detailed technical pieces that share the most current work of IETF Working Groups and BoFs. And keeping up with us will be easy. Join us online at www.ietfjournal.org and on social media at www.twitter.com/IETFJournal and www.facebook.com/IETFJournal.

One thing hasn't changed... we're still looking for your contributions from the field! This is still your publication. If you're interested in writing about your work at the IETF, please contact us at ietfjournal@isoc.org.

Words from the IAB Chair, continued from page 3

the resulting friction generates a lot of heat (and not much light). One suggestion for follow-on work from the workshop will be to document the user-interface considerations that arise from using different types of identifiers, so that new systems can more easily recognize the consequences of the identifier types they choose.

Another point that came up multiple times was the role of implicit context in transforming references in speech or writing into identifiers that drive specific protocol mechanics. While the shorthand for this is “the side of the bus” problem, the space is much larger and includes heuristic search systems ranging from the educated guess to highly personalized algorithmic responses. The participants saw a couple of possible ways in which standards developed in this area might advance how these tuples of context elements and references can be safely used to mint or manage identifiers. A first step in that will be to suggest that the IAB look at language tags, network provider identifiers, and similar common representations of context to see how they function across protocols. Follow-on work from that might include developing common vocabularies, serialization formats, and privacy models.

Like many others, I came away from the workshop with the realization that there is a dauntingly large amount of work to be done in this space. The workshop will be recommending more than a half dozen follow-on pieces of work to the IAB, as well as a potential Research Group and some individual drafts. Despite the amount of work facing us, I and many other participants left the room more hopeful than we came in, both that we can make progress and that some of the tools we need are already available.

To join the conversation, please share your comments on Internet naming by email to architecture-discuss@ietf.org or directly with the IAB at iab@iab.org.

WORKING GROUP UPDATE

EXTRA AND JMAP: IMPROVING MAILSTORE ACCESS

By Bron Gondwana

THERE ARE PRESENTLY TWO IETF WORKING GROUPS LOOKING AT EMAIL mailstore client protocols.

Chartered in late 2017, Email mailstore and eXtensions To Revise or Amend (EXTRA) is tasked with maintaining existing standards related to email stores. This includes both creating new extensions and correcting and clarifying existing standards and extensions where needed.

Email mailstore and eXtensions To Revise or Amend (EXTRA) is tasked with maintaining existing standards related to email stores.

To begin, we are processing the backlog of proposed extensions to the Internet Message Access Protocol (IMAP) that have already been written. Once that is complete, we will look for existing vendor-specific behaviour that can be generalised, and coordinate with the JSON Mail Access Protocol (JMAP) WG on common data-model needs. EXTRA will hold our first meeting at IETF 100 in Singapore.

JMAP is a new JSON-based protocol for interactions with a mailstore. The charter aims to retain data-model compatibility with IMAP, so a server can provide both JMAP and IMAP access to the same mail. JMAP specifically focuses on simplicity for client authors and efficient synchronisation primitives, including over constrained channels.

The JMAP WG held meetings at IETF 98 in Chicago and IETF 99 in Prague, and has an active mailing list. Both the core protocol and the mail-specific drafts have undergone significant revisions, and new drafts are expected to be presented before IETF 100 in Singapore. Many of the significant areas of debate have been resolved, however some ongoing churn is expected before we reach consensus.

Both groups look forward to new members and more feedback, particularly from client or server implementers, who are willing to share how their own data models could implement proposed drafts. Please come by our sessions in Singapore (in person or remotely) and join our mailing lists[1].

JMAP is a new JSON-based protocol for interactions with a mailstore. The charter aims to retain data-model compatibility with IMAP, so a server can provide both JMAP and IMAP access to the same mail.

Footnote

1. https://datatracker.ietf.org/wg/extra/about/, https://datatracker.ietf.org/wg/jmap/about/.

HUMAN RIGHTS PROTOCOL CONSIDERATIONS: BRIDGING THE IMPLEMENTATION GAP

By Alp Toker

A GROUP OF TECHNOLOGISTS REPRESENTING CIVIL SOCIETY MET AT IETF 99 to answer long-running questions regarding the human rights impact of protocol design with running code. This effort builds on work done by the Internet Research Task Force's Human Rights Protocol Considerations (HRPC) Research Group over the last two years, and explores how Internet protocols affect human rights, such as freedom of expression and freedom of assembly.

The HRPC mission was well-received at a technical plenary session at IETF 98 in Chicago, however concerns were voiced about open-ended ethical debates that risk sidetracking core IETF engineering goals. The shift from conversation to implementation marks a milestone as the human rights community steps up to demonstrate its capacity to bolster research and policy work with visible, hands-on participation in the standardisation and implementation lifecycle of Internet protocols.

In Prague, the group focused on validation of RFC 7725 that specifies the new HTTP status code 451 for use when resource access is denied as a consequence of legal demands. The number references novelist Ray Bradbury's dystopian novel, *Fahrenheit 451,* in which books are outlawed and burned. The specification is intended to increase transparency around withheld content by offering a semantic alternative to the 404 "Not Found" and 403 "Forbidden" codes that carry no indication as to the underlying cause of the restriction.

Over the course of the IETF 99 Hackathon, the group spent more than 48 hours developing the following three technology components to validate and showcase different aspects of RFC 7725:

- A crawling tool that tests online resources to identify legally withheld web content "in the wild" as part of the NetBlocks Open Source Internet observatory project
- A web-browser extension that enables users to self-report legally withheld content
- A plug-in for the WordPress content-management system designed to withhold pages according to criteria, such as the user's geographic origin

> **The shift from conversation to implementation marks a milestone as the human rights community steps up to demonstrate its capacity to bolster research and policy work with visible, hands-on participation in the standardisation and implementation lifecycle of Internet protocols.**

At the conclusion of the Hackathon, a panel of judges for the competition recognised the group's work as "Best New Work".

Olga Khrustaleva and I presented our implementation report at the HRPC Research Group session; our findings were a mixed verdict for RFC 7725 as it stands today. We found that existing usage of 451 codes on the public Internet is often technically invalid or misapplied; moreover, we noted that the specification does not significantly enhance transparency surrounding online censorship because of prevalent geographic restriction (or geoblocking) that continues to make state-sponsored censorship difficult to remotely discover using technical means.

> **We found that existing usage of 451 codes on the public Internet is often technically invalid or misapplied.**

Instances of 451-marked content identified by our tools included material related to gender, sexual health, and democracy that were blocked by two major Western content platforms, when served to people living in the Middle East. Most important, we found that governmental authorities in the countries in question had not taken technical measures to block the material. Rather, media platforms had proactively restricted those pages on their own servers.

Consequently, the specification may not only be failing to increase transparency, but may inadvertently be serving as an RFC stamp of approval that legitimises

While the group's work to assess RFC 7725 is ongoing, our experience already demonstrates how implementation and data on human rights can inform protocol design.

corporate compliance with overbearing censorship. Even when the content violates no platform rules and falls well within generally understood norms of acceptable speech, the 451 code provides an easy way out of difficult discussions with authorities. If this is the case, RFC 7725 serves as an example of the law of unintended consequences in protocol specification and design: an extension that sought to shed light on cases of censorship that may now be in use to rubber-stamp systematic violations of Article 19 of the Universal Declaration of Human Rights and other international conventions and commitments to which we are duty-bound.

While the group's work to assess RFC 7725 is ongoing, our experience already demonstrates how implementation and data on human rights can inform protocol design. Future threads of the work planned for IETF 100 in Singapore include an examination of web surveillance and privacy in real-time communication protocols—key topics that are currently receiving mainstream news coverage. These issues, which often pit the interests of large corporations against those of the general public, can be difficult to approach in a space where vendors and their representatives often take a leadership role. It is in this light that we hope our active participation will lend a new voice to civil society, when bridging concerns arising from the IRTF with the broader spectrum of day-to-day activities at the IETF.

Participants at the IETF 99 human rights discussion comprised a diverse group of civil society and nonprofit human rights organizations from around the world.

Internet pioneer John Gilmore once said, "the Net interprets censorship as damage and routes around it."

Internet pioneer John Gilmore once said, "the Net interprets censorship as damage and routes around it." Even as the conversation around digital rights has grown infinitely more nuanced, there is no doubt that the collective work of the IETF on core Internet protocols will play a central role in the way society protects its most vulnerable members. The way we adapt will determine to what extent we are able to preserve and enhance those universal values and protections in the years and decades to come.

Links

- Implementation Report draft, https://www.ietf.org/archive/id/draft-451-imp-report-00.txt.
- RFC 7725, https://tools.ietf.org/html/rfc7725.
- GitHub repository for Hackathon, https://github.com/451hackathon/.
- Live demonstration and dashboard, https://netblocks.org/dashboard/.

A NEW SECURITY MECHANISM FOR THE NETWORK TIME PROTOCOL

By Karen O'Donoghue

NETWORK TIME SYNCHRONIZATION PROTOCOLS HAVE BEEN EVOLVING FOR more than 30 years. Initially, security was not a priority because the security of timestamps was not seen as a critical need. After all, the time of day is not a secret, and any attempts to hide or authenticate the source of timestamps add additional latency. This additional latency had a negative impact on the overall objective of time synchronization between two devices. The protocols were lightweight and not deemed to put a burden onto the infrastructure. The perceived risk of attacks targeting clocks was quite low. This environment resulted in time synchronization protocols that did not include robust security functionality in the initial designs. Since then, synchronized time has become an important requirement in applications, as well as in general security mechanisms. As a result, as with other protocols and applications, security functionality is now identified as a necessary and integral part of network time synchronization.

Because of the shortcomings of preshared key and Autokey mechanisms, there has been an ongoing effort in the IETF to provide updated security mechanisms for NTP.

The Network Time Protocol (NTP) was initially published as RFC 958[1] in 1985. The current version, RFC 5905[2], was published as a standards track in 2010. These versions of NTP provided a basic preshared key scheme for authentication of time servers by clients. However, the preshared key approach does not scale sufficiently for large-scale network deployments or the global Internet. As a result, the Autokey Authentication Protocol, RFC 5906[3] was published as an Informational RFC in 2010 to address the scaling issue. With Autokey, clients authenticate time servers using Public Key Infrastructure (PKI) mechanisms. Security analysis, however, has demonstrated a number of security issues with Autokey. Because of the shortcomings of preshared key and Autokey mechanisms, there has been an ongoing effort in the IETF to provide updated security mechanisms for NTP.

Deployment Examples

Security for time synchronization is increasingly important, as several applications in the critical infrastructure domain depend on timing information. Possible examples for domain specific applications include:

- Synchronization of Phasor Measurement Units in the energy transmission and/or distribution network. These devices provide information about voltage, current, and phase angle used to derive the current state of the electricity network. Security for the synchronization between these units is a cornerstone in the reliable operation of the transmission/distribution networks.
- Synchronization in substation automation networks to ensure the correct operation of protection devices (in conjunction with protocols like GOOSE (Generic Object Oriented Substation Event) or SV (Sampled Values).
- Synchronization of machine parts in motion control in the process industry, for instance in a rolling mill or for printing presses.
- Synchronization of logging information in distributed systems to enable error tracking and thereby contribute to system stability and system integrity.
- New regulations of the finance sector raise high demands on the time synchronization of business clocks in trading systems. This is especially true in high-frequency trading, where a new EU legislation called Markets in Financial Instruments Directive (MiFID II) requires a timestamping granularity of 1 µs and a maximal divergence to UTC from 100 µs. Similar requirements are formulated by the US Securities and Exchange Commission (SEC Rule 613).
- Many national metrology institutes in Europe and in the US apply NTP for the dissemination of UTC.
- Security management, specifically the increasing usage of X.509 certificates, relies on time for validity checks. As this builds the base for many applications, security is a necessary prerequisite.

Requirements Analysis

In advance of the IETF NTP security efforts, the IETF TICTOC Working Group assessed the security requirements for network time synchronization protocols. RFC 7384[4] documents the results of that analysis. It distinguishes the threat model in terms of an internal versus an external attacker, and in terms of man-in-the-midde (MITM) versus packet injection types of attacks. RFC 7384 then identifies several potential threats to network time synchronization protocols including:

- Manipulation of time synchronization packets,
- Masquerading as a legitimate participant in the time synchronization protocol,

- Replay of legitimate packets,
- Tricking nodes into believing time from the wrong master,
- Intercepting and removing valid synchronization packets,
- Delaying legitimate time synchronization packets on the network,
- Denial of service attacks on the network at layer 2 and layer 3,
- Denial of service by overloading the cryptographic processing components,
- Denial of service by overloading the time synchronization protocol,
- Corruption of the time source used by the grand master,
- Protocol design and implementation vulnerabilities, and
- Using the time synchronization protocol for broader network surveillance and fingerprinting types of activities.

RFC 7384 analyzes these threats in the context of the threat model above to determine the likelihood of occurrence and the potential impact. Based on this analysis, a set of requirements were identified for time synchronization protocols and mapped to the threats that they address. These requirements include:

- Authentication and authorization of a clock's identity,
- Integrity of the time synchronization protocol messages,
- Prevention of various spoofing techniques,
- Protection against Denial of Service (availability),
- Protection against packet replay,
- Timely refreshing of cryptographic keys,
- Support for both unicast and multicast security associations,

Continued on next page

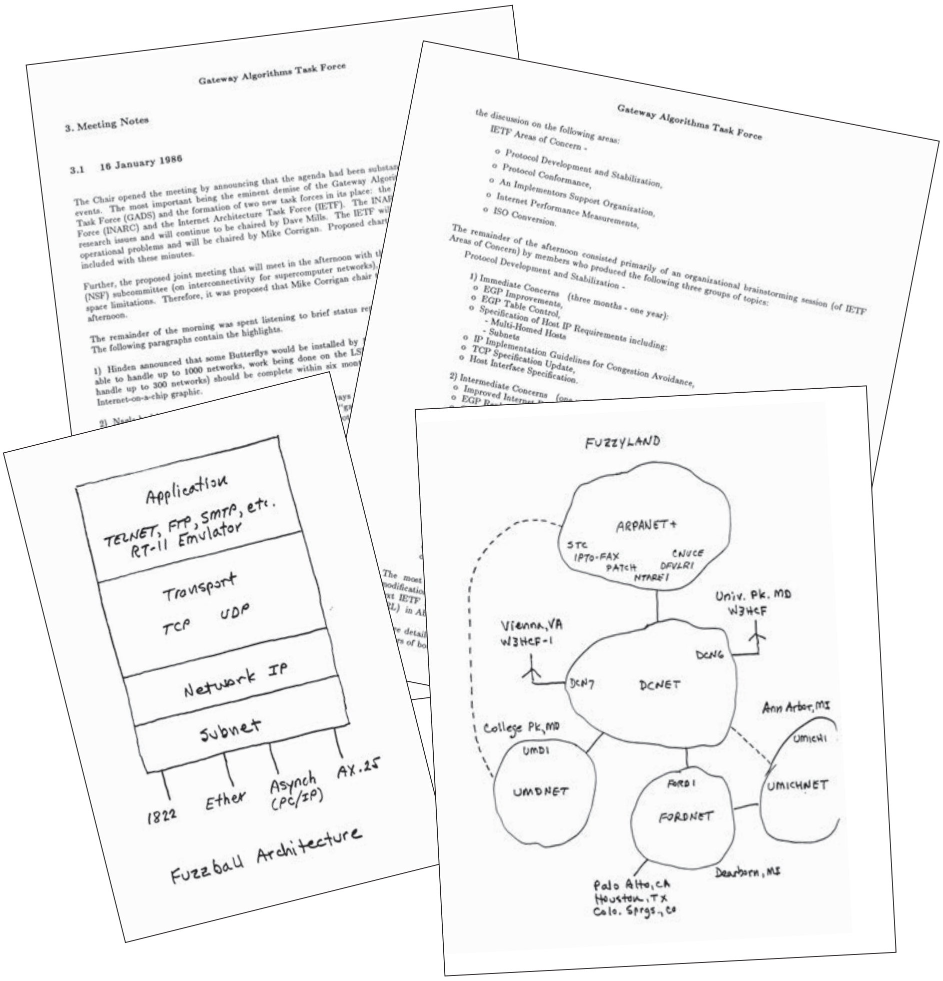
CELEBRATING 100 MEETINGS

THE FIRST IETF MEETING, 16-17 JANUARY 1986, IN SAN DIEGO, CALIFORNIA, had 21 attendees. That same year, IBM unveiled the PC Convertible (the first laptop computer), the 386 series of microprocessor was introduced by Intel, and the Internet Mail Access Protocol (IMAP) was defined for email transfer. How times have changed! This week's meeting in Singapore—IETF 100—is expected to draw more than 1,000 people from around the world to discuss the very latest in Internet standards and protocols.

But the IETF is about more than meetings. We're a robust online community of network designers, operators, vendors, and researchers concerned with the evolution of Internet architecture and the smooth operation of the Internet. Our efforts help move the Internet forward, provide "rough consensus and running code" to produce high-quality, relevant technical documents that influence the way people design, use, and manage the Internet.

The proceedings from that first meeting show threads that continue today. And we can anticipate that the next 100 meetings will further our current work on IPv6, the Internet of Things, video codecs, security solutions, and more… in addition to emerging technologies we haven't even thought of yet.

Please join us in Singapore as we celebrate the successes we've had so far and look forward to continuing our mission to make the Internet work better.



Gateway Algorithms Task Force

3. Meeting Notes

3.1 16 January 1986

The Chair opened the meeting by announcing that the agenda had been substan
events. The most important being the eminent demise of the Gateway Algori
Task Force (GADS) and the formation of two new task forces in its place: the
Force (INARC) and the Internet Architecture Task Force (IETF). The INAR
research issues and will continue to be chaired by Dave Mills. The IETF wil
operational problems and will be chaired by Mike Corrigan. Proposed chart
included with these minutes.

Further, the proposed joint meeting that will meet in the afternoon with th
(NSF) subcommittee (on interconnectivity for supercomputer networks),
space limitations. Therefore, it was proposed that Mike Corrigan chair t
afternoon.

The remainder of the morning was spent listening to brief status rep
The following paragraphs contain the highlights.

1) Hinden announced that some Butterflys would be installed by
able to handle up to 1000 networks, work being done on the LS
handle up to 300 networks) should be complete within six mont
Internet-on-a-chip graphic.

Gateway Algorithms Task Force

the discussion on the following areas:
IETF Areas of Concern -
o Protocol Development and Stabilization,
o Protocol Conformance,
o An Implementors Support Organization,
o Internet Performance Measurements,
o ISO Conversion.

The remainder of the afternoon consisted primarily of an organizational brainstorming session (of IETF Areas of Concern) by members who produced the following three groups of topics:
Protocol Development and Stabilization -
1) Immediate Concerns (three months - one year):
o EGP Improvements,
o EGP Table Control,
o Specification of Host IP Requirements including:
- Multi-Homed Hosts
- Subnets
o IP Implementation Guidelines for Congestion Avoidance,
o TCP Specification Update,
o Host Interface Specification.
2) Intermediate Concerns (one
o Improved Internet
o EGP R

From the proceedings of the first IETF, https://www.ietf.org/proceedings/01.pdf.

A New Security Mechanism for the Network Time Protocol, continued

- Minimal impact on synchronization performance,
- Confidentiality of the data in the time synchronization messages,
- Protection against packet delay and interception, and
- Operation in a mixed secure and nonsecure environment.

The requirements are analyzed in terms of being required and being recommended/optional depending on the needs of the application. This analysis informed the objectives of the NTP Working Group effort on Network Time Security (NTS).

NTP Security

The IETF NTP Working Group is focused on the development of a set of security mechanisms for NTP that are specified in the Internet Draft “Network Time Security for the Network Time Protocol”[5]. The main objectives of the NTS measures are to enable NTP entities to cryptographically identify their communication partner, to ensure authenticity and integrity of exchanged time synchronization packets, and to provide replay protection. A relatively new goal of NTS is to provide unlinkability, which ensures that NTS does not leak any data that would allow an attacker to track mobile NTP clients when they move between different networks. Although NTS can provide confidentiality for specific NTP extension fields, the NTP header itself will not be encrypted.

NTP provides different modes of operation. Besides the most utilized client-server mode, it also provides a mode for synchronization of symmetric peers, a mode for exchanging control messages, and a broadcast mode. These modes have different security and performance requirements. The symmetric and control modes have more-rigorous security requirements when compared to the client-server mode. However, the client-server mode requires more attention to resource utilization, since NTP servers may be contacted by a high number of clients and may not able to maintain state information for each client. NTS provides different mechanisms to meet these different requirements.

> **A relatively new goal of NTS is to provide unlinkability, which ensures that NTS does not leak any data that would allow an attacker to track mobile NTP clients when they move between different networks.**

Symmetric and Control Mode

NTP’s symmetric and control modes are protected by encapsulating the corresponding packets as DTLS Applications Data, respectively. This provides mutual authentication and replay protection. It also provides confidentiality, which is required by certain NTP control messages. This solution is somewhat controversial and is being considered for publication as an Experimental RFC.

Client-Server Mode

There are two security related phases for client-server mode. In the first phase, an NTP client verifies the authenticity of its time server and performs the key exchange. In the second phase, the client and server exchange NTP messages. The first phase is performed once during the establishment of an NTP association. The second phase is repeated for as long as the NTP association is active.

First Phase: Authentication and Key Exchange

The current draft defines an NTS key exchange protocol that uses the TLS protocol to provide a secure and robust means for the initial authentication of the server and the subsequent exchange of the keying material. Since TLS requires a TCP connection between client and server, an NTS enabled NTP server must not only listen to port 123/UDP, but also to a TCP port that will be assigned by IANA.

Note that earlier versions of this draft (up to version 6) defined a custom key exchange protocol in which the authentication and key exchange messages were encapsulated into NTP extension fields that were piggy-backed onto NTP packets. This key exchange protocol has been discarded because of potential security issues related to IP fragmentation.

Second Phase: Protection of the Time Synchronization

During the second phase, NTS introduces four new Extension Fields (EF) to satisfy the security objectives. The latencies introduced by cryptographic algorithms may impede the time synchronization performance. It is therefore imperative that the applied cryptographic primitives be fast to calculate. This requirement is met by applying only symmetric cryptography. The four new extension fields are:

1. The NTS Unique-Identifier extension. This EF contains a 32-octet random value that serves as nonce and protects the client against replay attacks.
2. The NTS Cookie extension. This EF contains information that enables the server to recalculate keys upon receipt. The server does not have to keep per-client state. It is opaque to the client.
3. The NTS Cookie Placeholder extension. This EF is sent when the client wishes to receive a new cookie. The server sends an NTS Cookie extension for

Suresh Krishnan opens the Technical Plenary

Systers Group Portrait, IETF 99

each received NTS Cookie Placeholder extension. It enables NTS to fulfill the unlinkability requirement.

4. The NTS Authenticator and Encrypted Extensions extension. This EF contains the ICV, which is computed over the NTP header and any preceding EF. It is calculated by applying the Authenticated Encryption with Associated Data approach.

Broadcast Mode

The current draft does not provide any cryptographic security measures to protect NTP's broadcast mode. This is due to the difficulty of specifying an appropriate mechanism that is resistant to packet-delay attacks. A TESLA-like mechanism is being considered, but because NTP does not provide periodical two-way packet delay measurements, it is especially vulnerable against tailored delay attacks. Further countermeasures have been discussed, but additional study is required in order to specify additional security measures for NTP's broadcast mode.

Best Current Practice

Beyond the specification of NTS, the NTP community is addressing security concerns via corrections to the specification, improvements to the implementation, and the issuance of an NTP BCP[6].

Related Activity

In addition to the NTP security work, there is work on time synchronization security for the Precision Time Protocol (PTP, IEEE 1588). PTP was originally published in 2002 with a focus on precision synchronization for instrumentation, industrial automation, and military applications. The second version was finalized in 2008, and includes more application use cases, such as telecom and enterprise environments. While the first version of PTP contained no security mechanisms, the second version was published with an Experimental Annex (Annex K). Annex K specified a security solution that provided group source authentication, message integrity, and replay attack protection. However, Annex K was not well adopted and implemented, and a number of studies were published regarding its weaknesses. Therefore, the ongoing effort to revise IEEE 1588 includes a plan to provide updated security mechanisms for PTP. These efforts are being coordinated.

Next Steps

As of the completion of this article, the work in the IETF NTP Working Group has not been finalized. However, while it is true that the efforts are still evolving, they do appear to be converging towards some consensus. As of this date, it appears that the NTS mechanism for client/server described here is progressing towards a standards track RFC, and the DTLS mapping suggested for symmetric and control modes may be published as an Experimental RFC. It is hoped that there will be new stable, published security mechanisms for NTP in 2018.

A preliminary implementation of NTS is underway, and additional implementations have been indicated. Interoperability testing, vulnerability research and analysis, and operational testing will be needed to ensure that the proposed solutions are robust and secure. While there is still much work to do, significant progress has been made.

Acknowledgement

K. O'Donoghue, D. Sibold, S. Fries, "New Security Mechanisms for Network Time Synchronization Protocols", presented at International IEEE Symposium on Precision Clock Synchronization for Measurement, Control, and Communication (ISPCS 2017), Monterey, California, USA, 2017, https://www.internetsociety.org/wp-content/uploads/2017/10/ispcs-2017-time-security-final-copyright.pdf.

References

1. https://www.rfc-editor.org/info/rfc0958.
2. https://www.rfc-editor.org/info/rfc5905.
3. https://www.rfc-editor.org/info/rfc5906.
4. http://www.rfc-editor.org/info/rfc7384.
5. https://datatracker.ietf.org/doc/draft-ietf-ntp-using-nts-for-ntp.
6. https://datatracker.ietf.org/doc/draft-ietf-ntp-bcp.

RUNNING CODE IS KING AT IETF 99 IN PRAGUE

Originally posted by Charles Eckel in the DevNet Open Source Community on 23 July 2017.

WHERE ARE THE NEW KINGMAKERS[1]? THEY ARE AT THE IETF HACKATHON—at least they were 15–16 July, when the best and brightest Internet technologists from around the planet gathered in Prague for IETF 99. And their first order of business was the IETF Hackathon, aimed at invigorating the standards process, enhancing the speed and relevance of emerging standards, and growing the community of people working with and contributing to the IETF.

Prague is a beautiful city with fantastic architecture, picturesque bridges and canals, and terrific food and beer at very affordable prices. Despite these enticements, a record 199 Hackathon participants opted to spend the weekend in a crowded room collaborating with fellow subject-matter experts and developers working on the latest algorithms and ideas around Internet protocols, transports, and security. For nearly half of the participants, this was their first IETF Hackathon; for 45 participants, it was their first time at any IETF event. The Hackathon's collaborative and constructive atmosphere is a great way to get started with the IETF, its community, and its work items. With more than 25 different projects from which to choose, newcomers and seasoned IETF veterans alike found areas of common interest and expertise on which to contribute.

Not Your Typical Hackathon

The IETF Hackathon is not a typical competition. Participants are motivated by a desire to improve the Internet, rather than prize money. The spirit is collaborative, rather than competitive. Participation is free, and attending the IETF meeting that follows is not required. Individuals volunteer to champion projects related to IETF work, and teams form around these champions. For descriptions of this Hackathon's projects, see the Hackathon wiki.[2]

One of the ways the Hackathon increases the pace and relevance of IETF work is via running code. Implementing evolving standards and producing running code validates the standards and highlights things that may be missing, wrong, or ambiguous in the drafts. Better still is if the code is open source, in which case viewing and sharing the source code aids in understanding the standards, makes them easier to use, and promotes adoption.

The doors to the Hackathon opened at 8am Saturday so project champions could set up their tables and development environments. By 9am, the room was nearly full with eager participants exploring options and opportunities with champions.

At 9:30am, we had an official kickoff to welcome everyone, review logistics, and answer questions. Then the real work began. Teams dug in and worked past the official closing time of 9pm. We had fun throughout, took time to get to know each other, and in many cases, helped or were helped by people from other teams. Having people from various standards organizations, open source communities, and universities exchange contact info and ideas provides benefits that reach far beyond the course of the weekend. By 9:30pm, the last remaining participants grudgingly packed up for the night.

Although the doors officially reopened Sunday at 9am, the room was half full by 8:30am. Work continued until early afternoon, when teams prepared and delivered presentations summarizing what they achieved, lessons learned, and what would be introduced into IETF Working Groups (WG). Finally, presentations were delivered to a panel of judges from the IETF community.

Winners were selected based on the following criteria:

- Advance pace and relevance of IETF standards
  - Bring speed and collaborative spirit of open source software into the IETF
  - Flush out ideas, feed into WG session
  - Produce sample code/reference implementations, utilities
- Attract developers, young people to the IETF

- Match young, skillful developers with IETF veterans
- University engagement around Hackathon projects

The award categories and winners from this Hackathon were as follows:

- Best New Work–HTTP error code 451
- Best University Work–Interface to Network Security Functions (I2NSF) Framework
- "NEAT"est Work–NEAT/TAPS
- Best Interop Work–QUIC
- Best Continuing Work–SCHC implementation and test SCTP
- Best Name–Waiting for go-dots
- Best Overall–SDN Apps for management of microwave radio link via IETF YANG Data Model

Other teams had fantastic achievements, as well. All project presentations are available on Github[3].

This Hackathon, collaboration across standards efforts and open source communities emerged as a theme. A particularly good example of this was the work done by the team working on RIOT.

"RIOT[4,5] powers the Internet of Things (IoT) like Linux powers the Internet," said Cenk Gündoğan, RIOT maintainer. "RIOT is a free, open source operating system developed by a grassroots community gathering companies, academia, and hobbyists, distributed all around the world. It supports most low-power IoT devices and microcontroller architectures (32-bit, 16-bit and 8-bit) and implements all relevant open standards supporting an Internet of Things that is connected, secure, durable, and privacy-friendly."

Efforts and Benefits Continue

The Hackathon ended Sunday afternoon, when the general IETF meeting began. Fortunately, the kind of collaboration on running code that progresses IETF standards continued during the week. To support this, a portion of the IETF Lounge was designated as Hackathon Corner, where people conveniently met, collaborated, and coded.

New to this meeting was the Hacklab, a rack of servers and network gear, including a full DOCSIS network with six simulated home networks accessible via a cable modem and built-in WiFi.

Demos to the IETF Community

One of the perks of participating in the Hackathon is showing off what you did at the Thursday night social, Bits-N-Bites. This meeting, a record number of teams took advantage of this, and more would have if we'd had the space to accommodate them! Hackathon teams polished and enhanced their projects throughout the week, then put them on display for the largest-ever turn out at an IETF meeting. As usual, great local food and beverages also helped attract crowds.

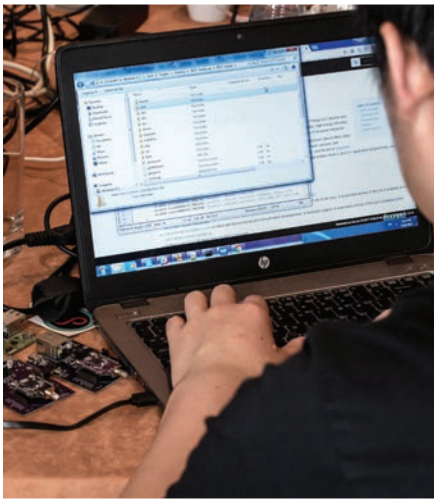
Next Steps

The next IETF Hackathon is at IETF 100 in Singapore, 11-12 November. As always, participation is free and open to everyone. It's an excellent opportunity to experience firsthand the work that the IETF does and the people who make it happen.

For more information on past, present, and future Hackathons, including how to register for the IETF 100 Hackathon, visit https://www.ietf.org/hackathon/. You are also encouraged to subscribe to hackathon@ietf.org to receive the latest event news and announcements.

Footnotes

1. From The New Kingmakers: How Developers Conquered the World by Stephen O'Grady (2013).
2. https://www.ietf.org/registration/MeetingWiki/wiki/99hackathon.
3. https://github.com/IETF-Hackathon/ietf99-project-presentations.
4. https://github.com/RIOT-OS/RIOT.
5. https://riot-os.org/.



A record 199 people attended the Hackathon.

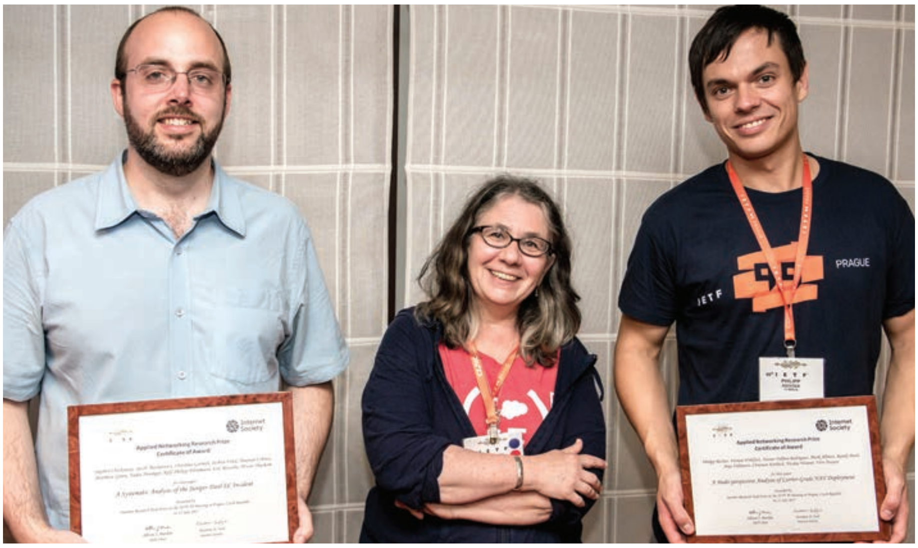
The team working on RIOT collaborated across standards efforts and open source communities.

APPLIED NETWORKING RESEARCH PRIZE WINNERS ANNOUNCED

By Mat Ford

THE APPLIED NETWORKING RESEARCH PRIZE (ANRP) IS AWARDED FOR recent results in applied networking research that are relevant for transitioning into shipping Internet products and related standardization efforts. The ANRP awards presented during IETF 99 went to the following two individuals:

- **Stephen Checkoway** for a systematic analysis of the Juniper Dual EC incident. See the full paper at https://www.cs.uic.edu/~s/papers/juniper2016/juniper2016.pdf.
- **Philipp Richter** for a multiperspective analysis of carrier-grade NAT deployment. See the full paper at https://net.t-labs.tu-berlin.de/~prichter/imc176-richterA.pdf.



2017 ANRP winners Stephen Checkoway (left) and Philipp Richter (right) with IRTF Chair Allison Mankin.

Checkoway and Richter presented their findings to the Internet Research Task Force open meeting during IETF 99. Slides are available at https://datatracker.ietf.org/meeting/99/materials/slides-99-irtfopen-anrp-stephen-checkoway-a-systematic-analysis-of-the-juniper-dual-ec-incident/ and https://datatracker.ietf.org/meeting/99/materials/slides-99-irtfopen-anrp-philipp-richter-a-multi-perspective-analysis-of-carrier-grade-nat-deployment/. ThankstoMeetecho, audio and video from the presentations is also available at https://www.youtube.com/watch?v=JRneMj7LX8U&list=PLC86T-6ZTP5jdbiwi5ggLNnwLn1-r0M4h (from 00:11:20).

ANRP winners have been selected for all of the IETF meetings in 2017. The following winners will be next to present their work at the IETF 100 meeting in Singapore:

- **Paul Emmerich,** a research associate at the Technical University of Munich. Emmerich will present his work to develop the high-speed packet generator, MoonGen.
- **Roland van Rijswijk-Deij,** a researcher at the Centre for Telematics and Information Technology (CTIT) at the University of Twente. Van Rijswijk-Deij will present his analysis of the impact of elliptic curve cryptography on DNSSEC validation performance.

The call for nominations for the 2018 ANRP award cycle is closed. Join the irtf-announce mailing list at https://www.irtf.org/mailman/listinfo/irtf-announce to receive all ANRP related notifications.

IRTF UPDATE

By Allison Mankin

YOU CAN TELL HOW BEAUTIFUL PRAGUE IS IN JULY! DURING IETF 99, ALL 10 chartered Internet Research Task Force (IRTF) Research Groups (RGs) held meetings:

- Crypto Forum (CFRG)
- Information-Centric Networking (ICNRG)
- Network Function Virtualization (NFVRG)
- Network Management (NMRG)
- Network Coding (NWCRG)
- Software Defined Networking (SDNRG)
- Thing-to-Thing (T2TRG)
- Human Rights Protocol Considerations (HRPCRG)
- Measurement and Analysis for Procols (MAPRG)
- Internet Congestion Control (ICCRG)

In addition to the meetings of those already chartered Research Groups, one proposed RG met:

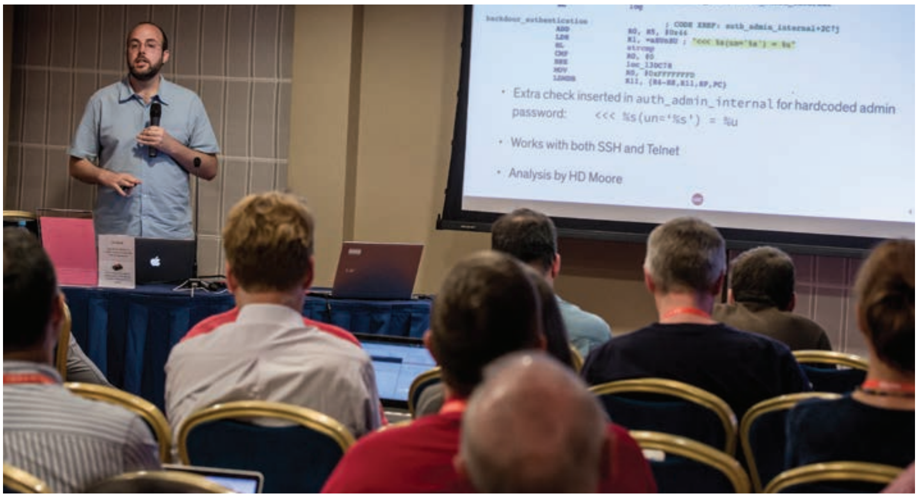
- Path Aware Networking Research Group (PANRG)

There has been a long of history of path-aware approaches at the IETF, and it may be that now is the time for researchers on this topic to make some progress. Since the IETF 99 meeting, PANRG has been chartered. You can read more about their work here at https://datatracker.ietf.org/rg/panrg/about/.

The IRTF Open Meeting received presentations from Stephen Checkoway on a systematic analysis of the Juniper Dual EC incident, and Philipp Richter on a multi-perspective analysis of carrier-grade NAT deployment.

The Applied Networking Research Workshop 2017 took place on Saturday, 15 July, prior to the IETF meeting. The ANRW'17 is an academic workshop that provides a forum for researchers, vendors, network operators, and the Internet standards community to present and discuss emerging results in applied networking research. The workshop is sponsored by ACM SIGCOMM, the Internet Research Task Force, and the Internet Society. You can find the workshop papers and Meetecho recordings at https://irtf.org/anrw/2017/program.html.

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


Extra check inserted in auth_admin_internal for hardcoded admin password: <<< %s(un='%s') = %u
Works with both SSH and Telnet
Analysis by HD Moore

ANRP winner Stephen Checkoway presents at the IRTF open meeting in Prague.

ANRP winner Philippe Richter presents at the IRTF open meeting in Prague.

IETF ORNITHOLOGY: RECENT SIGHTINGS

Compiled by Mat Ford

GETTING NEW WORK STARTED IN THE IETF USUALLY REQUIRES A BIRDS-of-a-feather (BoF) meeting to discuss goals for the work, the suitability of the IETF as a venue for pursuing the work, and the level of interest in and support for the work. In this article, we review the BoFs that took place during IETF 99, including their intentions and outcomes. If you're inspired to arrange a BoF meeting, please read RFC 5434, "Considerations for Having a Successful Birds-of-a-Feather (BoF) Session".

Network Slicing (netslicing)

Description: A network slice represents a logical network. It is a union of resources (connectivity, storage, computing), network functions, and service functions that were combined to provide a logical networking infrastructure in support of a variety of services.

The purpose of this discussion was to explore developing a set of protocols and/or protocol extensions that enable slicing within a network environment that assumes an IP and/or MPLS-based underlay.

Proceedings: Minutes are available at https://datatracker.ietf.org/meeting/99/materials/minutes-99-netslicing/. Slides, documents, and audio and video recordings are available at https://datatracker.ietf.org/meeting/99/proceedings (search for *netslicing*).

> **The presentations and discussion helped clarify where there is scope for input to the 3GPP process and where existing IETF work may be relevant to the network slicing use cases.**

Outcome: This was not intended to be a Working Group-forming meeting. The presentations and discussion helped clarify where there is scope for input to the 3GPP process and where existing IETF work may be relevant to the network slicing use cases. Further discussion and work is required to clarify whether additional work is required in existing or new WGs.

BANdwidth Aggregation for interNet Access (banana)

Description: Bandwidth Aggregation consists of splitting local traffic across multiple Internet links on a per-packet basis, including the ability to split a single flow across multiple links when necessary.

The goal of this proposed WG is to produce a Bandwidth Aggregation solution that will provide the following:

- Higher per-flow bandwidth. Many of the Internet links available to homes and small offices (e.g., DSL, Cable, LTE, Satellite) have relatively low bandwidth. Commonly used applications, such as streaming video or content up/downloads require or could benefit from more bandwidth for a single traffic flow than is available on any of the local links. A Bandwidth Aggregation solution could supply the needed bandwidth by splitting a single traffic flow across multiple Internet links.
- Reduced cost. Traffic sharing on a per-packet basis allows the full bandwidth of the lowest-cost link to be used first. It only uses a higher-cost link once the lowest-cost link is full.
- Increased reliability. When one Internet link goes down, ongoing application flows can be moved to another link, preventing service disruption.

Proceedings: Minutes are available at https://datatracker.ietf.org/meeting/99/materials/minutes-99-banana/. Slides, documents, and audio and video recordings are available at https://datatracker.ietf.org/meeting/99/proceedings (search for *banana*).

Outcome: This was a WG-forming BoF meeting that spent a lot of time discussing the proposed charter for a WG. A straw poll of the room indicated that there is a small constituency of people interested in working on this topic. Further discussion will take place on the mailing list to refine the proposed WG charter with a view to Working Group formation in future.

IDentity Enabled Networks (ideas)

Description: The goal of this group is to standardize a framework that provides identity-based services usable by any identifier-location separation protocol. The new requirements driving this framework go beyond the traditional discovery service and mapping of identifier-to-location for packet delivery.

In addition, an IDEAS Working Group will identify gaps and make recommendations for changes needed for interface interactions between the framework and identifier-enabled protocols.

Proceedings: Minutes are available at https://datatracker.ietf.org/meeting/99/materials/minutes-99-ideas/. Slides and audio and video recordings are available at https://datatracker.ietf.org/meeting/99/proceedings (search for *ideas*).

Outcome: The discussion highlighted some confusion about the terminology and permanence of identifiers. More work is needed to clearly define the work to be undertaken by a new IETF WG and to allay concerns about identifier permanence and implications for privacy and online tracking.

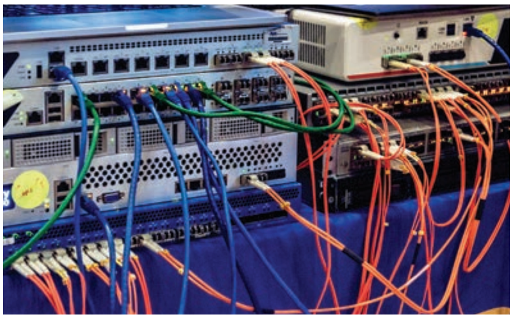
IASA 2.0 (iasa20)

Description: The IETF community has identified a need to review and possibly rework the administrative arrangements at the IETF, dubbed the IASA 2.0 project (https://www.ietf.org/blog/2016/11/proposed-project-ietf-administrative-support-2-0/). A series of virtual workshops were offered related to this effort. This BoF provided an opportunity to talk about the feedback that was received from the workshops and to solicit further feedback.

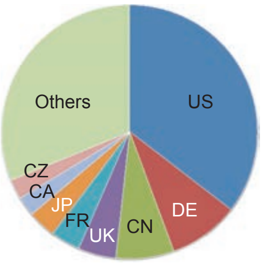
Proceedings: Minutes are available at https://www.ietf.org/proceedings/98/minutes/minutes-98-iasa20-00.txt. Slides, documents, audio and video recordings are available at https://datatracker.ietf.org/meeting/98/proceedings (search for *iasa20*).

Outcome: A robust discussion about the challenges facing the current administrative structure and arrangements, and an opportunity for those present to express their views and concerns vis-à-vis some of the alternative approaches to reform. Discussion will continue on the mailing list (https://www.ietf.org/mailman/listinfo/iasa20).

great cormorant
(Phalacrocorax carbo)



IETF 99 AT–A–GLANCE



Onsite participants: 1204

First-time participants: 199

Number of countries: 61

Hackathon participants: 199

IETF Activity since IETF 98 (26 March–16 July 2017)

New WGs

- DKIM Crypto Update (dcrup)

WGs closed

- Domain Boundaries (dbound)
- Geographic JSON (geojson)
- ART Area General Applications Working Group (appsawg)

WG currently chartered: 136

New and revised Internet-Drafts (I-Ds): 1388

IESG Protocol and Document Actions: 57

IESG Last Calls issued to the IETF: 70

RFCs published: 76

- 44 Standards Track, 5 BCP, 6 Experimental, 18 Informational

Notable process updates

- Published update to BCP 26, Guidelines for Writing an IANA Considerations Section in RFCs. https://tools.ietf.org/html/bcp26
- Published update to BCP 79, Intellectual Property Rights in IETF Technology. https://tools.ietf.org/html/bcp79
- Published update to RFC 2119, Ambiguity of Uppercase vs Lowercase in RFC 2119 Key Words. https://tools.ietf.org/html/rfc8174
- Beta website at https://beta.ietf.org. Send feedback via GitHub or webmaster@ietf.org.

RFC Editor Activity since IETF 98 (April–June 2017)

Published RFCs: 64 (1720 pages)

Stable and pretty URLs for errata

- http://www.rfc-editor.org/errata/rfc7991
- http://www.rfc-editor.org/errata/eid4906

Format-related updates

- Testing existing toolset with non-ASCII chars
- Testing id2xml (converts .txt to .xml v2)
- Reviewing required database and script updates related to non-ASCII chars and multiple file formats

Current and ongoing activities

- Publishing RFCs: keep the docs moving
- Continue testing and sending feedback to tools team regarding XMLv3-related tools
- Update tools to handle UTF-8 and multiple file formats
- Draft internal procedures for v3 era as tools become more stable
- Work with RSE on rfc7322bis (RFC Style Guide)

IETF MEETING CALENDAR

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

IETF 101
Date 17–23 March 2018
Hosts Google and ICANN
Location London, UK

IETF 102
Date 14–20 July 2018
Host Juniper Networks
Location Montreal, Quebec, Canada

IETF 103
Date 3–9 November 2018
Host TBD
Location TBD

IETF 104
Date 23–29 March 2019
Host TBD
Location Prague, Czech Republic

Special thanks for hosting IETF 99

COMCAST
CZ.NIC
NBCUniversal

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

APNIC
apTLD
ICANN
Google

This publication has been made possible through the support of the following Platinum organization members of the Internet Society

Afilias
CISCO
COMCAST
ICANN
JUNIPER NETWORKS
NBCUniversal
privateinternetaccess™ for safe browsing, always use protection.™
RIPE NCC RIPE NETWORK COORDINATION CENTRE