Get to Know the Opus Codec

By Jean-Marc Valin and Timothy B. Terriberry

As more and more communications moved to IP (Internet Protocol), new applications like WebRTC (Web real-time communications) expanded the capabilities of traditional VoIP (Voice over Internet Protocol), and Plain Old Telephone Service (POTS) began to go the way of...
Message from the IETF Chair

By Jari Arkko

IETF 87 was a very successful meeting. We had 1,426 on-site participants from 62 countries—more attendees than we’ve seen in a long time from more countries than we’ve ever had. There were 12 new working-group proposals, and although many were taken to the discussion stage quite early, many of those seem to have experienced positive results. I anticipate that about two-thirds of the proposals will soon be up for approval as working groups.

In addition to new work, IETF 87 attracted a record 316 first-timers. This is great news—new people are vital to ensuring we understand the myriad challenges of Internet technology.

IETF 87 also saw the debut of our new mentoring system. Approximately 50 IETF attendees volunteered to mentor new attendees: help them navigate the meeting and, most important, establish connections with others. For me, an important aspect of each meeting is the interaction I have with people who are building devices on the Internet. Specifics aside, this kind of like-minded networking is a crucial part of setting up new, interoperable Internet technology and a vital part of each new attendee’s IETF experience.

In addition to new work, IETF 87 attracted a record 316 first-timers. This is great news—new people are vital to ensuring we understand the myriad challenges of Internet technology.

We had a great social event, thanks to DENIC, our platinum sponsor. I’ve yet to meet an engineer who doesn’t love trains. Everyone in attendance had a wonderful time. Thank you, DENIC! And this meeting’s Bits-n-Bites was so well attended that at times it was difficult to get to the demo tables. Many thanks to all of our event sponsors: A10 Networks, ADVA Optical Networking, Comcast, Deutsche Telekom, Dyn, ECO, EURid, Huawei, ICANN, the Internet Society, IPSO Alliance, and Nominum. We couldn’t do it without you.

The practical meeting organisation worked well. In fact, participants liked the hotel and the facilities so much that many suggested we return to Berlin soon.

From a personal perspective, some of the most interesting work that occurred this meeting included work related to the Internet of Things (many of the new work proposals were in this space), home networking (also some new proposals and a lot of running code), and multimedia communications from browsers (WebRTC). I also liked the new Advanced Queue Management (AQM) work proposal, which attempts to keep bad router buffering practices from wasting capacity. This group has a real chance of improving how responsive the Internet feels to individual users without requiring an increased broadband connection speed.

During the meeting, we continued our discussion of technical and organisational issues. In our administrative plenary, Kathleen Moriarty and Suresh Krishnan updated us on the Diversity Design team’s activities (page 9). These discussions are on a productive path. I’m looking forward to the improvements we’ll make in this space.

Continued on page 4
Words from the IAB Chair

By Russ Housley

This is my first contribution to The IETF Journal as chair of the Internet Architecture Board (IAB). Olaf Kolkman and Bernard Aboba left large shoes to fill—over the past few years, they restructured the way the IAB works by introducing the new program model that greatly improved the ability of the IAB to simultaneously handle administrative, liaison, and technical responsibilities. I greatly appreciate the support of the IAB and the entire Internet community.

Appointments

In July, the NomCom announced the appointment of Erik Nordmark to the IAB, filling the seat vacated by Spencer Dawkins, who accepted the Transport Area Director position. The IAB thanks Spencer for his service.

The IAB appointed Bob Hinden to another term on the Internet Society Board of Trustees. During the Board meeting in Berlin the day after IETF 87, Bob was elected chair of the ISOC Board. Congratulations Bob!

Two liaison manager positions closed. The IAB thanks Fred Baker for serving as liaison manager to the Smart Grid Interoperability Panel (SGIP) and Richard Barnes for serving as liaison manager to IEEE 802.23.

There has been turnover in three liaison manager positions: the IAB appointed Scott Mansfield as the IETF Liaison Manager to the ITU-T, replacing Eliot Lear; it appointed Deborah Brungard as the IETF Liaison Manager to the ITU-T for Multiprotocol Label Switching (MPLS), replacing Scott Mansfield; and it appointed Jonne Soininen as liaison to the Internet Corporation for Assigned Names and Numbers (ICANN) Board, replacing Thomas Narten. The IAB thanks Eliot and Thomas for their service as liaison managers.

Highlights since IETF 86

The IAB sent letters on open standards in the Transatlantic Trade and Investment Partnership (TTIP) to both the U.S. government and the European Commission. You can find these letters on the IAB website.1,2

The IAB published a statement entitled, “Dotless Domains Considered Harmful.” You can find the statement on the IAB website.3

The IAB responded to the ICANN Consultation on the Source of Policies and User Instructions for Internet Number Resource Requests. You can find the response on the IAB website.4

Appeal to the IAB

The IAB received an appeal from JFC Morfin regarding RFC 6852 on 8 July 2013 and answered the appeal on 17 July 2013.5

Upcoming IAB Workshop

The IAB is sponsoring a workshop on Internet Technology Adoption and Transition (ITAT). The workshop will be held on 4–6 December 2013 in Cambridge, UK. Participants were required to submit 3–10 page interest statements by 29 August 2013.

References


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

But the IETF is about more than specifications and papers—it’s about running code. I was pleased to see so many instances of running code both during the meeting itself and around it, including an interop event on 6LowPAN technology, an XMPP hackfest, NAT64 live testing on the IETF network, using the Opus audio codec for remote attendees (p. 1), home networking demos, a distributed mobility demo, Code Sprint working on IETF tools, the Bits-n-Bites demos, and probably a host of other places that I’m not aware of. I’d like to see even more code at the next meeting. If you have a test or demo in mind, let’s talk.

As usual, much collaboration occurred outside the open meetings: engineers talked to each other, implementers shared experiences, operators explained their needs, and so forth. It was also a pleasure to note so many attendees from outside our traditional demographic, such as root server operators, network operators from developing countries, regulators and policy makers, ICANN specialists, and students. Participants of all types were engaged in discussions that certainly appeared to be useful, particularly those meetings between the IAB and meeting attendees.

How did you find IETF 87? Your thoughts are welcome.

Get to Know the Opus Codec, continued

The creation of an audio codec working group within the IETF was subject to much controversy. Although Opus is not the first codec to be stamped by the IETF, it is the first to be developed within a dedicated IETF working group and published on the standards track. The two complementary technologies were combined in 2010 as part of the IETF audio codec effort started one year earlier.

The creation of an audio codec working group within the IETF was subject to much controversy. Although Opus is not the first codec to be stamped by the IETF, it is the first to be developed within a dedicated IETF working group and published on the standards track. Described as “one of (if not the) most technically complex pieces of work that has been presented to the IETF” by its Gen-Art reviewer, the effort also raised new issues within the IETF, such as how to specify a standard as C code.

Overview
To cover a wide range of network conditions, Opus supports a wide array of quality and bitrate options:

- Bitrates from 6 kbit/s to 510 kbit/s
- Narrowband (8 kHz) to fullband (48 kHz) audio
- Frame sizes from 2.5 ms to 60 ms
- Speech and music support
- Mono and stereo
- Flexible rate control

As network conditions change, all of the abovementioned settings may be dynamically changed in real time without causing audible artifacts or other glitches. Its rate control can generate constant bitrate (CBR) streams, such that each packet is exactly the size requested, or variable bitrate (VBR) streams, which target a specific quality, optionally constrained to impose a bound on required buffering or to respect an absolute maximum rate. All of this makes Opus suitable for almost all audio applications, including:

- VoIP and videoconferencing (e.g., WebRTC)
- Music streaming
Music files and audiobooks
Low-delay broadcast reporting
Wireless audio equipment
Network music performance

In addition to making things easier for implementers—one codec can deliver best-in-class performance where five or six different codecs would have been required before—Opus’s wide range of applications also helps reduce transcoding when linking different applications (e.g., streaming a videoconference).

Testing
To justify these claims and verify that Opus met its requirements, independent testers compared it to other speech and music codecs. Among these tests, a wideband/fullband speech test conducted by Google found that Opus provided better quality at equal rate than G.719, Speex, G.722.1, and AMR-WB (Adaptive Multi-Rate Wideband). See figure 1.

In a test by HydrogenAudio, Opus outperformed Vorbis and both the Nero and Apple HE-AAC encoders on 64 kbit/s music. See figure 2.

The results of these tests prove that Opus delivers better quality than previous state-of-the-art music codecs while maintaining the low delay of communications codecs.

Adoption
Despite being standardized only last year, Opus is already being adopted in many VoIP and videoconferencing clients. Along with G.711, it is mandatory to implement for the new WebRTC standard, which was used to broadcast the technical plenary (on Opus) at IETF 87 (using Opus). Tieline and vLine use Opus to deliver broadcast contributions. Real-time communications clients, including Jitsi, Meetecho, CounterPath, SFLphone, Mumble, Teamspeak, and many others support Opus.

Opus is also being adopted as a music-streaming and music-storage format. It can be used with the HTML5 <audio> tag in Firefox and, with a flag, on Chrome and Opera. Popular players such as VLC, foobar2000, Winamp (via a plugin), xmms2, and Amarok have added support; as have media frameworks like gstreamer and FFmpeg. Magnatune recently converted their entire collection to Opus, and a number of Internet radio stations are streaming in it. Even the StreamGuys CDN has added support.

Ongoing Work
Opus developers are currently focused on releasing version 1.1 of the Opus implementation. This will be the first

The results of these tests prove that Opus delivers better quality than previous state-of-the-art music codecs while maintaining the low delay of communications codecs.
major release since version 1.0 was published alongside the RFC. Version 1.1 will include quality improvements that are possible because RFC 6716 only specifies the Opus decoder, thereby allowing smarter encoders in the future. These improvements include much-improved support for surround audio, and bitrate allocation tuning to enable more-uniform audio quality and to lower the average rate required to avoid noticeable artifacts.

Another important feature in version 1.1 is the ability to automatically detect whether an input signal is speech or music and adapt the encoding process accordingly. Although the reference implementation could switch between modes, it relied on the user to identify whether the input was speech or music.

At the IETF, the focus is now on encapsulating Opus in both RTP and Ogg with two active working group drafts. Encapsulating Opus is straightforward because it signals all mode changes in-band—no out-of-band signaling is required. The SDP (Session Description Protocol) codec parameters carry only informative parameters, which almost completely eliminates the possibility of negotiation failure. In fact, an RTP receiver can correctly decode an Opus stream without ever seeing the SDP.

Next Steps: Video
Watch for the Daala project, a competitive, royalty-free video codec, based on "new" (for video codecs) technology, including lapped transform, frequency-domain intraprediction, and vector quantization.

References
12. http://dir.xiph.org/by_format/Opus
17. http://xiph.org/daala/
Opus Is a Model for Future IETF Standards Work

By Carolyn Duffy Marsan

The Internet Architecture Board (IAB) showcased the Opus codec at its technical plenary in Berlin as a recent example of how Internet Engineering Task Force (IETF) working groups can produce a high-quality standard, avoid intellectual property minefields, and meet a market need.

Opus is a versatile audio codec that can support both interactive speech and streaming music over the Internet. It was defined in RFC 6717, which was published in September 2012. Opus applications include voice-over-IP (VoIP), video conferencing, streaming music, broadcast, and network music performances.

“Opus was designed to work for the vast majority of audio applications,” said Jean-Marc Valin, a Mozilla engineer who coauthored the Opus specification. Valin said the market needed an open standard for a codec that could provide high-quality audio for real-time applications.

Until now, two types of codecs existed: (1) speech codecs that provide the same level of quality as analog telephone service and (2) general-purpose codecs designed for more demanding music streaming applications.

“What we were trying to achieve here is to get the best of both types of codecs—something that works for voice and music, something that works in real-time environments, and something that can still have high quality,” said Valin.

Opus is highly flexible, supporting bit rates that range from 6 to 150 kilobits/sec. It can support narrowband to fullband as well as frame sizes from 2.5 to 60 milliseconds. Even better, Opus can dynamically adjust bitrate, bandwidth, and frame size on the fly. And it is optimized for the Internet, meaning that it has packet-loss concealment and can handle discontinuous transmission.

To achieve this level of flexibility, the Opus design team merged the SILK codec designed by Skype for speech applications and the constrained energy lapped transform (CELT) codec used in streaming music applications. “The result is better than the sum of its parts,” said Valin. “We have a hybrid mode that combines the best of SILK and CELT, and we can switch between modes in real-time without a glitch.”

Adoption of Opus appears solid. Opus is supported in Firefox and Chrome because it was accepted as one of two mandatory-to-implement codecs for the Web real-time communication (WebRTC) application programming interface (API) for browser-to-browser applications. It has been adopted by several VoIP clients and the real-time chat component of gaming applications. And it’s in use by applications like IceCast for music streaming and for standalone music players like Rockbox.

Because Opus is so flexible—it has more than 4,000 possible configurations—it was difficult to test. Greg Maxwell from the Xiph.org Foundation described a series of subjective and objective testing protocols that were used during the creation of Opus. Maxwell said that continuous listening tests “showed Opus doing significantly better than other codecs.”

Cisco engineer Peter Saint-Andre said the Opus working group had to get past skepticism on the part of many IETF contributors, who doubted that the standards body had the expertise to create a codec specification. The working group also had to deal with several intellectual-property-rights disclosures. But engineers who wanted to develop an innovative codec got to work figuring out how to meld SILK and CELT.

“There was a great sense of shared purpose in the work,” Saint-Andre said. “That was really key to making this effort a success.”

Saint-Andre admits that the group didn’t have a testing plan in place ahead of time, nor did it have a plan for outreach to other interested standards bodies or a plan for dealing with patent issues.
“The working group succeeded despite itself,” Saint-Andre says. “We had a core group of people who were really committed to making it happen. They were really smart and well informed and knew a lot about codecs. And that is why we were able to succeed... Opus sounds great, and it is being built into a lot of products. But it wasn’t clear that we would reach that goal right from the start.”

In related news, the IAB’s Open Mic session prompted a discussion about the IETF’s use of the term Proposed Standard to describe a specification that is ready for deployment, rather than the term Internet Standard, which implies that it is done.

Former IAB Chair Olaf Kolkman said the term Proposed Standard is causing confusion for the group that sets technical standards for European government procurements. The government group is only allowed to choose formal standards, but the IETF’s own description of a Proposed Standard implies that it is immature. Kolkman said the EU group wanted to specify IPv6, but all the RFCs are at the Proposed Standard level rather than the Internet Standard level.

“This puts the IETF at a disadvantage when compared to other standards organizations,” added Thomas Narten, a former IETF liaison to ICANN and an IBM engineer. “That may not be a big deal from an engineering perspective, but it is a big deal in other circles.”

Eliot Lear, a former IETF liaison to the ITU-T and Cisco engineer, agreed. “If people in other standards bodies feel there isn’t a standard, then they get into the pool. Then we get into having market confusion as a result and multiple standards,” he said.
IETF Hosts Diversity Debate

By Carolyn Duffy Marsan

The highlight of the Internet Engineering Task Force (IETF) Administrative Plenary in Berlin was a report by the Diversity Design Team on its ongoing efforts to make the standards body more inclusive.

IETF Chair Jari Arkko said that although the Berlin meeting attracted attendees from 62 countries, there was still room to improve.

“I think we could be more diverse in terms of vendors and operators and in gender diversity,” he said. “We don’t reach all the ends of the world, and it is very important to understand all the kinds of conditions where the Internet operates.”

Arkko said that cultural differences are an issue for the IETF, in particular the direct manner in which contributors comment online and at meetings about the work of others. Some view the IETF’s technical discussions as being too aggressive, which prevents them from participating in the group.

“We have to compete for talent. We can’t exclude anyone,” Arkko said. “We have to be a global, inclusive organization.”

Kathleen Moriarty, one of the leaders of the IETF’s Diversity Design Team, said increasing the IETF’s inclusivity is important.

“It’s very important to attract and maintain new talent in the IETF,” she said. “A diverse organization is better at adapting to external changes. Diverse and inclusive teams can perform better.”

Moriarty said the team is developing initiatives aimed at increasing inclusivity and addressing the group’s aggressive culture.

“The word aggressive came up many times,” Moriarty said. “It’s absolutely essential to have good technical debates…but there are many ways to be heard without being too aggressive.”

Moriarty said the IETF needs to boost participation by network operators, representatives of small companies, and academia. To do this the group is considering various ways of fostering collaboration, engaging and attracting newcomers, and expanding the IETF community.

“We would like to reduce the number of situations that are perceived as hostile by members of specific groups,” Moriarty said. “One option is a code of conduct. Another is communication guidance materials, and the reduction of culture-specific references. There also was a recommendation of an ombuds-person.”

Audience members expressed support for the IETF’s diversity effort.

“Diversity leads to better results. As engineers that should really appeal to us,” said Thomas Narten, a long-time IETF participant and IBM engineer. “It isn’t necessarily what you say, but how you say it. That’s one of the things we should work on.”
IETF Privacy Update

By Hannes Tschofenig

Online privacy and security concerns took centre stage in the global news recently, with much publicity surrounding both the proposed data protection regulation in Europe and the growing allegations of state-sponsored pervasive Internet surveillance. Between the lines, members of the IETF community can see their ongoing privacy and security efforts at work. It’s heartening to see the renewed interest in these important topics and the fresh look they’re receiving in light of a greater understanding of pervasive monitoring. Below you’ll find a brief summary of IETF 87 activities related to privacy and security.

HTTP 2.0 and Encryption by-default

The HTTPbis working group (WG) is working on a new version of HTTP (Hypertext Transfer Protocol), called HTTP 2.0. The working draft introduces major changes to HTTP 1. At the March 2012 IETF meeting (IETF 83), the group decided against an HTTP 2.0 design using a secure-only version with mandatory-to-use TLS (Transport Layer Security). Recent debates about state-sponsored Internet surveillance, including an inspiring presentation from the WG chair, Mark Nottingham, motivated the group to revisit the decision.

The importance of these developments has prompted mainstream media reports and we expect the ongoing debate to be an interesting one. A solution that enables encryption by default is a privacy feature that many experts have been seeking for some time. It does, however, create a dilemma for firewall manufacturers, who struggle to intercept TLS communication in enterprise networks, particularly with the increase of bring-your-own-device (BYOD) deployments. Today, many enterprise-controlled devices, like laptops, come with a fake trust anchor installed to transparently terminate TLS connections at the company firewall. With BYOD this “trick” does not work anymore. Ideas, such as the TLS proxy, that would have allowed intermediaries to look into the traffic were quickly dismissed by IETF meeting participants.

RTCWeb and E2E Media Security

The IETF has a long history of developing real-time communication protocols, including the Session Initiation Protocol (SIP), the Extensible Messaging and Presence Protocol (XMPP), and most recently, the RTCWeb (Real-time Communication in Web Browsers) protocol, which builds on the Web infrastructure and JavaScript.

The core specifications of RTCWeb were developed in the RTCWeb WG and in the W3C. In addition to functional aspects, last meeting’s agenda included an item to discuss the key management protocol for establishing the necessary keying material and parameters for use with the Secure Real-Time Transport Protocol (SRTP), which is used to protect voice and video communication on an end-to-end basis. Two proposals were put forward: SDES (Session Description Protocol Security Descriptions) and DTLS-SRTP (Datagram Transport Layer Security–Secure Real-time Transport Protocol).

SDES carries keying material along a signalling path such that signalling intermediaries can see the keying material. It’s simple to implement and convenient for those seeking lawful intercept functionality (or other forms of inspection) for end-to-end voice communication. DTLS-SRTP, on the other hand, uses DTLS to distribute the necessary keying material and provides increased protection against intermediaries and eavesdroppers.

Hadriel Kaplan and Martin Thomson presented arguments in favour of SDES. Eric Rescorla presented arguments for DTLS-SRTP.

For many meeting participants this was a critical decision and a number of security experts were in attendance to weigh in. By meeting’s end, participants were in favour of DTLS-SRTP.

TLS 1.3: The Next Generation of Transport Layer Security

A side benefit of the design of HTTP 2.0, the work on RTCWeb, and the overall attempt to make the Web more secure (particularly for the mobile environment) is a renewed interest in the TLS WG.

We’re seeing today a desire for both more security protection and lower communications latency, but cryptographic computations and the latency of the security handshake come at a cost. In response, major Web companies, most notably Google, are looking at ways to optimize TLS.

New developments include application layer protocol negotiation to allow the demultiplexing of HTTP 1.1 and HTTP 2.0 payloads, OCSP stapling and multiple OCSP stapling to avoid requiring separate protocol exchanges to check the status of certificates, TLS channel IDs to develop a “cryptographic cookie” at the TLS layer, and mostly recently, TLS 1.3.

Eric Rescorla, TLS WG cochair and TLS author, offered an overview of some of the TLS 1.3 design characteristics, and although he describes the changes as minor, compared to earlier TLS versions they include major improvements (e.g., the addition of a Diffie-Hellman exchange to avoid passive eavesdropping on the TLS exchange, a privacy increasing functionality).
Privacy concerns came up in a number of TLS WG discussions. There appears now to be a better understanding of the need to consider privacy issues when designing TLS protocol extensions.

**IAB Privacy Considerations**

The IAB (Internet Architecture Board) privacy considerations document was published as RFC 6973. To inform the IETF community about the new guidelines, the IAB privacy program devised a tutorial, which they piloted at IETF 87 in order to solicit feedback. A revised tutorial for a much larger audience is planned for IETF 88 in Vancouver (November 2013).

The IETF security area directors published a document that requires IETF document authors to address privacy in their protocols. The IAB document is currently used for guidance, but the Internet Engineering Steering Group (IESG) is in a much better position to encourage document authors to consider privacy. This approach will be similar to the approach taken with security in BCP (Best Current Practice) 107 and BCP 61.

**Tor and the IETF**

Members of the Tor project, including Jacob Appelbaum and Linus Nordberg, attended the IETF 87 to discuss the PRISM revelations, share information about their work, and determine what collaboration with the IETF might look like. In addition to side meetings, a presentation at the Security Area Advisory Group was made and a mailing list (perpass@ietf.org) created to foster continued conversation.

Cooperation with the Tor community could provide the IETF with additional insight into fingerprinting prevention and the state of middleboxes throughout networks (see Tor’s Open Observatory of Network Interference project). The Tor community could benefit from additional reviews and involvement of

---

**ATTENTION ALL SUBSCRIBERS**

**Let’s Talk**

**SURVEY**


**HARDCOPY SUBSCRIPTION RENEWALS**

Do you receive a hardcopy *Journal*? If so, your subscription is about to expire. To continue receiving it, you **MUST** visit [https://portal.isoc.org](https://portal.isoc.org) and confirm your postal address to receive the next issue.

Thank you.

*Continued on next page*
the IETF community in their ongoing projects.

Security Incident Information Sharing

High-profile data breaches and security incidents on the Internet are gaining more and more attention from the Internet community, the public, and governments around the globe. A variety of cybersecurity activities have recently been launched, including the European Union’s CyberSecurity strategy, the European Commission-created Network and Information Security Platform, and the NIST (National Institute for Standards and Technology) Cyber-Security Framework. Sharing security incident information is critical to improving awareness of and ensuring a quicker response to security incidents.

Just prior to IETF 87, the IETF held a workshop on its ongoing standardization efforts in the areas of incident and abuse information sharing. The workshop page contains slides from the presenters, including presentations about privacy and other legal aspects. A workshop report is in progress.

Workshop discussions underscored the fact that privacy issues are not well understood. For example, what information about the communication interactions is allowed to be collected? What can be shared with third parties and under what conditions? While some techniques have been deployed for some time already (e.g., spam filtering), it was not obvious from the discussions at the workshop how well these issues have been considered vis-à-vis data-protection frameworks. Further discussion is needed and recommendations will be developed as more sharing occurs and as IETF efforts progress, specifically in the Security Automation and Continuous Monitoring (sacm) WG and in the Managed Incident Light-weight Exchange (mile) WG.

Improving the Web Public Key Infrastructure (WebPKI)

Problems with the WebPKI received attention by the Internet security community when DigiNotar, a Dutch certificate authority, had a security breach, and then again in the same year when a Comodo affiliate was compromised. Both involved the fraudulent issue of certificates and raised questions regarding the strength of the PKI in use today.

A compromise of the PKI leads to privacy violations as it allows an attacker to intercept encrypted communication. Almost two years have passed since the aforementioned incidents and new technical mechanisms have been developed—including DANE (DNS-based Authentication of Named Entities), key pinning, and certificate transparency. But very little has happened in terms of actual deployment and similar attacks could still occur.

In April 2013, NIST held a workshop on “Improving Trust in the Online Marketplace” and invited stakeholders to discuss technical options for improving the state-of-the-art. It became clear that there exist very few organizations with the technical expertise, appropriate membership model, and independence required to lead the follow-up discussions.

The IAB will work with the Internet Society on how to proceed. A meeting is planned for IETF 88 and a workshop will be organized in 2014.

Looking Ahead to IETF 88 in Vancouver

Just prior to publication of this article, Bruce Schneier published an article suggesting that IETF 88 be dedicated to discussing how to make surveillance more expensive. In response, Jari Arkko, IETF chair, and Stephen Farrell, IETF security area director, shared their views about pervasive surveillance in a blog post. Discussions continue on the IETF mailing list and on the perpass mailing list, about specific steps the IETF can take as a standardization body and steps the wider Internet community can take. Lots of ideas are being bounced around and the open nature of the IETF is, as expected, facilitating a fruitful exchange. I encourage you to contribute your views to the discussion.

References

17. http://datatracker.ietf.org/wg/mile/charter/
Internet Society Fellow Sets RFC Milestone

By Carolyn Duffy Marsan

IETF participant Sandra Céspedes reached an important milestone this summer, when she became the first ISOC Fellowship Programme alumni from Colombia to coauthor an RFC (Request for Comments).

Céspedes is coauthor of RFC 6971, Depth-First Forwarding in Unreliable Networks, which was published as an Experimental RFC in June 2013.

Céspedes is an assistant professor with the Department of Information and Communications Technology at Icesi University in Cali, Colombia. She directs the university’s telematics engineering undergraduate programme, and she is a member of the Informatics and Telecommunications Research Group.

“Anyone professional in this area can contribute to make a better Internet, even if you only start by asking questions to a working group or by proposing an experimental protocol.”

Céspedes was awarded a fellowship from the Internet Society that covered the cost of travel, accommodations, and meeting fees to attend IETF 69 in July 2007. With the Internet Society’s support, she came back as a Returning Fellow at IETF 76, IETF 79, IETF 83, and IETF 87. She was able to attend one IETF meeting without ISOC funding, which was IETF 81 (in Quebec) because she was studying in Waterloo, Ontario, at the time.

Over the years, Céspedes has participated in a variety of IETF working groups: Mobility Extensions for IPv6 (Mext); Network Based Mobility Extensions (Netext); Distributed Mobility Management (DMM); and the Internet Research Task Force’s IP Mobility Optimizations Research (MOBOPTS). She also was involved in the Intelligent Transport Systems BoF.

Céspedes spent two years working on the research that became RFC 6971. She met one of the coauthors, Álvaro Cárdenas, at IETF 79 and started working with him a few months later to improve a forwarding mechanism that she discovered while conducting a research internship at Fujitsu Laboratories in California. Céspedes and Cárdenas did some experimental research and simulations on the mechanism, and together wrote the first version of the draft in March 2011. Fujitsu engineer Ulrich Herberg served as editor for the RFC and presented it at IETF 84.

“We couldn’t convince a working group to adopt the document,” Céspedes said. “We continued as an independent submission, and Ulrich found reviewers who were interested.”

Céspedes says the publication of RFC 6971 represents “a big accomplishment in my professional career. It’s been recognized as a big success by the university where I work, not only because I’m a professor there but also because I’m an alumni of the telematics engineering programme there.”

Céspedes is among a handful of Colombians who are active in the IETF and have published RFCs.

“What the publication demonstrates is that any professional in this area can contribute to make a better Internet, even if you only start by asking questions to a working group or by proposing an experimental protocol,” she said. “That’s what I share with my colleagues and students in my home country.”

Céspedes says she wouldn’t have been able to get involved with the IETF without the support of the Internet Society Fellowship Programme.

“Nothing would have happened if I hadn’t received the continuous support from the Internet Society,” she said. “Even though at most I’ve attended one meeting per year over the last five years, it’s definitely helped keep things rolling.”

Céspedes says the Internet Society Fellowship Programme is key to expanding participation at the IETF meetings among network engineers from Latin American countries.

“Every time I attend an IETF meeting, I find people attending from Venezuela, Brazil, and Argentina—it’s clear that Latin American countries are getting more involved,” she said. “The hardest part is maintaining the interest and will to work after the initial meeting when companies and universities from our region don’t allow time to be dedicated to the standardization process.”

Steve Conte (left) and Toral Cowieson (right) present Sandra Céspedes (middle) with a copy of the RFC she coauthored.
It’s Time to Give Online Games Serious Consideration

By Jose Saldana and Mirko Suznjevic

I attended my first IETF meeting in Paris (IETF 83) in order to present the preliminary idea for a traffic optimization proposal in the Transport Area. The idea emerged when I tried to adapt a VoIP (voice-over-Internet protocol) optimization technique to online game traffic. One of my research interests is the characterization of online game traffic so when several people mentioned that it might be interesting to have an informal session about the topic, we requested a room and organized an online games session on the fly (see The IETF Journal June 2012, Vol. 8, Issue 1).

After the informal session in Paris, Wes Eddy suggested that I organize a more-formal tutorial and announce it in advance to get more people interested. Although online games have become increasingly popular, we wondered if the IETF community was interested in learning more about them. I enlisted the help of Mirko Suznjevic of the University of Zagreb, who’d just received a fellowship for attending the IETF meeting in Berlin. We’d previously collaborated on some research articles, mainly about the traffic of massively multiplayer online role-playing games (MMORPGs), one of today’s most popular game genres.

We talked with the Transport Area directors, and they encouraged us to prepare the tutorial. They also granted us a slot in the Transport Area Open Meeting at IETF 87. The main objectives of the presentation, after a succinct overview of the online games market, were to inform the IETF crowd about the traffic characteristics of online games and to play a variety of game genres to illustrate in real time the impact of network impairments on a player’s quality of experience (QoE).

Those who think gaming is only for a minority of the population are mistaken. The current number of players worldwide is estimated to be 1.2 billion... Facebook has confirmed that it has more than 250 million unique players a month.

We also summarized different game architectures. Today, there is a strong predominance of client-server schemes. The biggest reason is that they permit better control of the server, which translates into good synchronization between players. Other reasons include the deterrence of cheating (some players modify the packets in order to gain an advantage over others) and easier billing.

In recent years, a trend has arisen in gaming business models: pay-to-play models (e.g., game client purchase, subscription-based games) are being replaced by free-to-play models in which the game is free, but additional content or cosmetic and usability improvements are offered for microtransactions. In this model, a player can either spend a week trying to get a new item (e.g., a sword, a car, camouflage paint) or buy it immediately for a small sum.

The Internet is the part of the problem that the gaming company does not control—upon installation of the application, all 3D information about the game’s virtual world is stored in the user’s hard disk. We showed a World of Warcraft folder that comprised 25GB of data as an example. This model enables games to function with very low bandwidth requirements: they need only send information containing the

Jose Saldana copresents an online game tutorial during the Transport Area Open Meeting
Mirko Suznjevic copresents an online game tutorial during the Transport Area Open Meeting.

player’s commands and inputs, in addition to chat and built-in voice systems. All textures, characters, and landscape meshes reside on the hard disk—they need not be transmitted during play.

As a result, the main characteristic of gaming traffic is very small packets (a few tens of bytes) sent at a fast pace. Similar to VoIP, interactivity is critical. The bandwidth sent is low—in some cases tens of kilobits-per-second, and a player’s actions are transmitted to the server in milliseconds. This ensures that the competition between players is realistic and not a case of the gamer with the highest delay being penalized.

We also presented an approach used by cloud-based games in which clients are “thin,” and servers calculate the virtual-world state and send a high-quality video stream to the player’s client. The client then sends the player’s commands to the server. This results in different traffic characteristics, including significantly higher bandwidth usage.

The effect of network delay and packet loss on playability is a critical concern of online game developers, network operators, and Internet service providers. Players are difficult customers to deal with—if a game does not work properly, they may leave the game and never return. For this reason, gaming companies tend to simplify the problem with a goal of 24/7 workability and very low network delay.

In order to show the audience the effect of network impairments on playability, we had two volunteers play three rounds of a first-person shooter (FPS) game on a dedicated server. They played the first round as normal. During the second round, we added 300ms (round trip) of latency to one of the players via a network emulator. During the third round, we added 10 percent packet loss.

Although the FPS game was resilient to our imposed impairments, particularly the loss, some negative impact was observed: the video was not continuous and it went back in moments. Since manageability was reduced, the player with the impairments had a higher probability of being shot. Even so, the impairments did not significantly affect performance and both players reported that their quality of experience (QoE) was not significantly degraded.

In another demonstration, we had two different volunteers play three duels on the public server of a MMORPG. The same scenarios were executed: normal network conditions, 300ms of latency, and 10 percent of loss. Due to the MMORPG using TCP (transmission control protocol), a much more significant impairment was reported by the player with the high loss rate.

In summary, our tutorial presented some important high-level information about the game industry, gaming traffic characteristics, and game QoE issues. As online games become an increasingly significant market, we believe that the IETF should consider game characteristics and requirements during the standardization process.

A NEWCOMER’S EXPERIENCE

I attended IETF 87 primarily to participate in the birds-of-a-feather (BoF) for Tunneling Compressed Multiplexed Traffic Flows—a mailing list on which I’m active. I was nervous prior to the meeting. It was both my first IETF meeting and I was giving two presentations: one at the BoF and another on online gaming traffic.

The Internet Society’s morning meetings eased my nervousness by breaking the ice with other fellows and Fellowship program staff. That first contact was very warm and helped calm me. I specifically thank Steve Conte for his advice and guidance. I didn’t expect the people in the IETF to be so approachable, but everyone—from students to highly ranked members from corporations like Cisco—is polite, kind, and willing spare a few moments to answer questions. I talked with a lot of people and received a lot of very good advice regarding my current research and further activities in the IETF. Conversations and the ability to meet with a variety of people were probably the greatest benefits of attending the meeting.

I’m very pleased with the meeting’s outcome: the tutorial was very well received. Although the BoF did not result in creation of a working group, we received a lot of constructive criticism, and we were able to identify issues that need to be addressed in order to advance our work. I also realized what a great opportunity IETF meetings are to meet and talk with people from different parts of the world. Gaining these vastly different perspectives is valuable for researchers like myself and I’m grateful to ISOC’s Fellowship program for enabling my attendance.

— Mirko Suznjevic
Internet Society Panel Tackles Transient Congestion

By Carolyn Duffy Marsan

Alongside the IETF meeting, the Internet Society hosted a panel discussion about the impact of transient congestion on the end-user experience and whether or not the IETF could develop transport-layer strategies to improve overall network performance.

Leslie Daigle, chief Internet technology officer for the Internet Society, moderated the discussion, “Improving Internet Experience: All Together, Now.” Participants considered how to improve overall network performance by addressing latency, throughput, jitter, and other issues that affect application performance.

Daigle explained that alleviating congestion problems requires attention from a variety of people: application software developers, operating system developers, access network hardware vendors, access network operators, transit network operators, and other infrastructure providers. Each person optimizes systems for their own needs, which may not lead to overall network optimization, she said.

“It can lead to brittleness,” Daigle said. “People are making assumptions that may not play well together... And there is the very real fact that the existing model of the Internet may not fit with today’s reality of mobile handsets as the primary mode of access of the Internet.”

Panelist Patrick McManus, who is responsible for the networking module for Mozilla Firefox, said he considers application responsiveness to be one of the key areas needing improvement in order for the Internet to continue to grow and innovate.

McManus gave an example of downloading a 1-kilobyte image to explain the amount of excess communications required by the various protocols—SSL, DNS, DNSSEC, TCP, and HTTP—involving in this simple user request.

“By the time you’re done, that’s about one second to get your 1-kilobyte image,” McManus says. “It doesn’t matter if you upgrade your home from 2 megabits/second access to 50 megabits/second because of the many protocol interactions involved. The issue is: How do I get reliable congestion control? I’m just moving 1 kilobyte of data. Why does it take me one second to do that? How do I deploy this application so it can work faster with all the middle boxes and firewalls of the Internet?”

McManus said that developers increasingly are creating new transport protocols to reduce the overhead associated with TCP and SSL and tunneling them over UDP, such as Google’s QUIC.

“The question for us as an Internet community is... How do we design more robust building blocks where we don’t reinvent the entire wheel?” he said.

“The question for us as an Internet community is... How do we design more robust building blocks where we don’t reinvent the entire wheel?”
—Patrick McManus, panelist

Jason Livingood, vice president of Internet and communications engineering at Comcast Cable, said he is intrigued by efforts to measure the end user’s experience on the Internet. He pointed to the IETF’s Large-Scale Measurement of Broadband Performance (LMAP) working group, which is looking at aspects of Internet performance including throughput, latency, and jitter.

—Patrick McManus, panelist
“In the past, people mostly focused on throughput: speed, speed, speed, and that’s all,” Livingood said. “There’s a lot more to your Internet experience than that. One of the big issues is latency.”

He added that the excess buffering of packets can have a big impact on end-user performance as can protocols used by Content Delivery Networks. “Optimizations to your part of it can have unexpected effects on other parts of the Internet,” he said.

“Building everything in UDP (user datagram protocol) is not a panacea. The issue is whether we carry on down the path of trying to use TCP (transmission control protocol) or we give up on it completely.”

—Stuart Cheshire, panelist

Stuart Cheshire, distinguished engineer at Apple, said it is important to reduce the number of round trips that Internet protocols require for particular applications in order to improve responsiveness. However, he warned that “coordinating all these different improvements that are going on so they don’t conflict with each other is really challenging.”

Daigle asked the panelists to identify one change that they wish they could make to improve Internet performance.

McManus said he’d address the lack of transport security. “In Firefox, we see 20 percent of our traffic in some form of SSL (secure sockets layer). That’s just appalling,” he said. “That’s largely a technological failure, and it’s a process failure.”

Cheshire said he’d find a way to improve performance through middle boxes. “Everything is really centered on the Web: stock quotes, weather forecasts, maps. Everything is an HTTP GET,” he said. “If you’re on a network that requires you to use HTTP proxies, you can only use HTTP-based applications. That’s fairly depressing because everything is getting forced into a very narrow pipe.”

To illustrate the point, Cheshire cited new IETF transport protocols such as WebSockets, which maintains a two-way connection between a Web server and browser over TCP to facilitate live content, and WebRTC, which supports browser-to-browser applications.

Livingood said he would tackle Wi-Fi network performance. “There are millions of consumer electronic devices in people’s houses that will take years to get upgraded,” he said. “There’s a big tail on what end users think of as Internet performance.”

While some of these issues such as eliminating middle boxes are seemingly impossible, Daigle asked the panelists to identify actions that the IETF can take to reduce congestion.

Cheshire pointed to Minion, a new TCP-based service model and conceptual API (application programming interface) being developed jointly with Janardhan Iyengar at Google, as a way of improving Internet application performance through middle boxes. “Building everything in UDP (user datagram protocol) is not a panacea,” he warned. “The issue is whether we carry on down the path of trying to use TCP (transmission control protocol) or we give up on it completely.”

McManus said he likes Minion because it offers connection management and congestion control. “With today’s protocols, developers have to choose: Do you want to use TCP and pick up latency delays? Or do you want to roll your own on top of UDP? That’s never a satisfying choice,” he said. “Minion is a great example of ways we can go forward.”

Another suggestion made by McManus is to look for ways to create a single building block that combines the...
behavior of more than one protocol, such as stream control transmission protocol (SCTP) and datagram transport layer security (DTLS). “SCTP and DTLS are really made for each other, and yet you establish one before the other and you get this strip of serial things going on,” he explained. “You could establish one building block that is those two things mushed together.”

Livingood pointed out that for any of these new transport protocols that address congestion issues, such as Minion, it will be difficult to adequately test end-to-end performance across the Internet given the diversity of access capabilities.

“One of the benefits we get in this community of the IETF is that the people who participate here have a good understanding of how varied the network is,” Cheshire argued. “One of our responsibilities at the transport area is to improve TCP, to cut out some of the round trips, and to make it more responsive and make it better for low-latency, real-time data. The longer we fail to do that, the more developers are pushed towards doing their own thing with UDP.”

The audience responded positively to the panelists and their suggestions for new transport area work to relieve the risk of excessive congestion caused by badly designed UDP-based transport protocols that lack TCP’s congestion control protections.

“These are really hard questions that are largely being ignored,” said longtime IETF participant Dave Crocker during the Q&A. “The IETF is not attending to these issues, and it would be great if this panel triggers something.”

Crocker suggested that the IETF leadership consider the issue of latency-related round trips when it charters working groups much as it asks about security and privacy concerns. “It could get interesting if we try to press for charters to make some assertions… along a set of parameters such as latency or jitter,” he said.

Latin American Participation in the IETF

IETF LAC Task Force Begins Long-term Mission

By Alvaro Retana

During the past 20 years, use of the Internet has spread across the globe at an unimaginable rate. However, participation in the development of Internet standards has not grown in all regions at the same rapid pace. This disparity matters—global standards growth serves to both increase the talent pool and ensure that all issues are brought to light and properly addressed.

Holding IETF meetings in regions with high growth rates has spread the word about the organization and attracted new participants. China is a great example: IETF 79 was held in Beijing in 2010, where authorship and participation has been growing rapidly for almost 10 years.

Earlier this year when the IETF Administrative Oversight Committee (IAOC) announced its intent to have a meeting in Buenos Aires, all kinds of discussions arose around the venue, cost, security, language, politics, and even objectives and value of holding a meeting where local participation is still relatively low. But results from a survey conducted by the IAOC indicated that a significant number of people would attend an IETF meeting in South America.

What does this mean to the region? Is it an indication of the impending explosive growth in participation from Latin America? Hardly. While having a meeting in the region may help in raising awareness, there’s no clear correlation between it and increased participation or the quality of the work.

Discussions were also held at the regional level. We talked about the potential impact and expectations of having the IETF meet locally and about the barriers of entry. Most important, we talked about what should be done. In true Latin fashion, we put perceived limitations aside and focused on the long term.

Before the end of May 2013, less than a week after the original IAOC message, the Latin American and the Caribbean Network Operators Group (LACNOG) chartered the IETF
LAC Task Force with the objective of encouraging the participation of people from the region in IETF processes and discussions. Some of the goals include:

- Being a mechanism for introducing new people to the IETF
- Provide a place where people can discuss drafts in their own language (Spanish, Portuguese, English)
- Provide a place where Latin authors can send their drafts and get feedback from their peers

Note that the intent of the task force is not to create a parallel organization, but to ease new participants into the IETF process by facilitating discussions in their local languages.

It is an honor to have been nominated and confirmed as the first chair of the IETF-LAC Task Force. I was born and raised in Costa Rica and have spent the past 18 years working and living in the United States—taking every opportunity to support Latin America’s technological growth. With the strong support from LACNOG, LACNIC, the Internet Society and the whole LAC community, we’re building robust momentum.

Our first order of business is to increase awareness of the IETF standardization process and the work done in it. To that extent, a grassroots effort out of Brazil kicked off to create a bound version of the ‘Tao of IETF’ in Spanish, Portuguese, and English to be available soon so that new participants have a lasting memory of their initial encounter with the IETF. Another local effort is brewing in Mexico to reach out more to both academia and local communication companies.

Note that the intent of the task force is not to create a parallel organization, but to ease new participants into the IETF process by facilitating discussions in their local languages.

On the technical side, the group hasn’t been focusing on finding regional problems to be solved; we believe that most of the issues facing the Internet are global in nature. Interesting discussions, which have already resulted in the publication of at least two Internet-Drafts, have been held around topics as varied as peer-to-peer, RDAP bootstrapping, net neutrality, SDN, IPv6 measurement, monitoring, security and address reservation, certificate transparency, and geolocalization. The technical depth and breadth of the region is impressive!

It’s been a very exciting few months. We’ve been able to tap into an active and very diverse group of people in the region. Our plans are ongoing, extensive and include a partnership with the Internet Society. We look forward to expanding the reach of the IETF.

An IETF Tutorial was first presented at LACNOG 2012 in Uruguay. We are currently refining it for presentation in October at the LACNOG 2013 meeting in Curacao. In addition, it has become a constant on the agenda to talk about current “Hot Topics” being discussed in the IETF. A pre-IETF meeting was created to share interesting topics to be discussed (guided by the authors and leaders from the region). The first such meeting was held a couple of weeks before IETF 87; another is planned for just before IETF 88.

On the technical side, the group hasn’t been focusing on finding regional problems to be solved; we believe that most of the issues facing the Internet are global in nature.

References

4. IETF-LAC mailing list, https://mail.lacnic.net/mailman/listinfo/ietf-lac

The Punta side of Willemstad city, Curacao
Protecting Consumers from Fraud
A Story of Industry, the IETF, and DMARC

By J. Trent Adams

This is a story about how to prevent crime. It’s about experimentation and empirical evidence that shows real world results. It’s about industry working with the open standards community. It’s also about rough consensus and running code. Most important, though, it’s about preventing people from becoming victims of fraud.

The story begins with a loose series of conversations that started about five years ago. A few prominent email senders, service providers, and large mailbox providers started to talk about how to handle the problem of email fraud. While the email community was grappling with the broader difficulties associated with generic spam, these senders were particularly mired in the battle to defend their domains from being spoofed. Attackers were preying on their customers as part of protracted phishing campaigns—attacks designed to extract customer access credentials in order to break into their accounts and do real harm.

To be clear, phishing isn’t just unsolicited email attempting to convince unwary consumers into purchasing something they don’t need. It is outright theft and an undeniably illegal activity. Unfortunately, due to the patchwork of legal regimes in play around the world and the complexity of identifying the criminals, prosecuting those responsible isn’t a straightforward process (even when it’s possible).

By 2011 it was determined that the right mix was to use Sender Policy Framework (see http://tools.ietf.org/html/rfc4408) in combination with DomainKeys for Internet Mail (see http://tools.ietf.org/html/rfc6376), both of which are specifications being worked through the IETF. To learn how well the scheme was performing, the participants in the experiment instituted a method for the mailbox providers to send email authentication reports back to the senders. Once that was in place, the effectiveness of the model was obvious: for the first time, senders were able to see that in some cases up to 60 percent of email received was fraudulent.

Given that the number of spoofed messages was staggering, this new stream of data was rigorously analyzed to ensure it was accurate. In the end, it was clear that email spoofing a particular domain could be entirely blocked using this new scheme. Unfortunately, it wasn’t a silver bullet against phishing, but it significantly degraded the unfettered attacks. However, companies still needed to figure out how to handle look-alike or cousin-domain attacks that try to masquerade as a sender, as well as common attacks that try to play with how From addresses are displayed in various mail clients. Further, questions remained about how to handle redistributed mail sent via discussion lists and automated forwarding services.

Nevertheless, the success of the experiment was too important to ignore. The next step was to document the experiment as a specification describing the methodology and submit it to the IETF, the same standards body that nurtured the underlying technologies of SPF (Sender Policy Framework) and DKIM (DomainKeys Identified Mail). As part of that exercise, the experiment was expanded to test the existing running code at Internet scale. In January of 2012 the group published the draft specification that became known as Domain-based Message Authentication, Reporting, and Conformance (DMARC).

The effectiveness of the model was obvious: for the first time, senders were able to see that in some cases up to 60 percent of email received was fraudulent.
What happened next was unprecedented: within one year of the specification being made public, an estimated 60 percent of the world’s email boxes were protected by DMARC—that’s 1.976 billion email accounts.

It’s been nearly five years since DMARC started its journey and it is now nearing the point where it is recognized as a strong foundational technology on which the email community can rely. But, it’s incredibly important not to lose sight of the true goal of this work: protecting people from crime.
Secure Telephone Identity Revisited
BoF Results in Motivated Working Group

By Alan Johnston

The Secure Telephone Identity Revisited (STIR) BoF was one of the most anticipated sessions of IETF 87—the BoF mailing list had more than 500 messages sent in the month prior to the meeting and because of similarities between the source identification in the telephone network and the source identification techniques for managing spam, the BoF drew interested parties from both the telephony and email worlds.

Background

Today, much of the Public Switched Telephone Network (PSTN) has moved to a Voice over IP (VoIP) core, using IETF standards such as Session Initiation Protocol (RFC 3261) for signaling and Real-time Transport Protocol (RFC 3550) for media transport.

Before VoIP, there were only a few levels of carriers—typically two local carriers and one transit (long distance) carrier per call. Today, a PSTN VoIP call can traverse multiple levels of VoIP wholesalers and resellers, making it extremely difficult to identify the source of the caller ID.

However, nonInternet E.164 telephone numbers remain the dominant form of identity used over these VoIP networks. The problem of caller-ID spoofing and anonymization didn’t begin with VoIP, but VoIP has exacerbated it. Widespread VoIP/PSTN interconnection has expanded the number of telephony carriers from dozens to tens of thousands. Before VoIP, there were only a few levels of carriers—typically two local carriers and one transit (long distance) carrier per call. Today, a PSTN VoIP call can traverse multiple levels of VoIP wholesalers and resellers, making it extremely difficult to identify the source of the caller ID.

Secure Telephone Identity Revisited

BoF Results in Motivated Working Group

By Alan Johnston

The Secure Telephone Identity Revisited (STIR) BoF was one of the most anticipated sessions of IETF 87—the BoF mailing list had more than 500 messages sent in the month prior to the meeting and because of similarities between the source identification in the telephone network and the source identification techniques for managing spam, the BoF drew interested parties from both the telephony and email worlds.

Background

Today, much of the Public Switched Telephone Network (PSTN) has moved to a Voice over IP (VoIP) core, using IETF standards such as Session Initiation Protocol (RFC 3261) for signaling and Real-time Transport Protocol (RFC 3550) for media transport.

Before VoIP, there were only a few levels of carriers—typically two local carriers and one transit (long distance) carrier per call. Today, a PSTN VoIP call can traverse multiple levels of VoIP wholesalers and resellers, making it extremely difficult to identify the source of the caller ID.

Schulzrinne concluded by arguing that telephone-number spoofing is the root of almost all telephone network evil, and that a solution was needed or the role of the PSTN as a universal way for personal and commercial communication could be compromised.
Verification Involving PSTN Reachability (VIPR) working group (WG) were presented, as well. Schulzrinne concluded by arguing that telephone-number spoofing is the root of almost all telephone network evil, and that a solution was needed or the role of the PSTN as a universal way for personal and commercial communication could be compromised.

Next, Jon Peterson presented an “in-band” solution. This approach can be used in trunking connections between service providers or between a service provider and an enterprise. In this approach, information about who made the telephone number assertion in the From header field is carried in SIP Identity and Identity-Info header fields that can be cryptographically verified.

No changes to any PSTN protocols are involved in this approach, which has some similarities to the techniques used to authenticate the source identity of SMTP email messages developed by the Domain Keys Identified Mail (DKIM) working group. Peterson argued that the Enhanced SIP Identity defined in RFC 4474 with some modification could provide a way for service providers to begin to require authenticated caller ID in intercarrier trunking. Service providers would need credentials so that only the correct service provider could assert particular E.164 telephone identities. With wide deployment and a regulatory mandate, this could eventually result in more-accurate caller ID and make robocalling and TDoS easier to prevent and block.

Eric Rescorla presented an alternative solution known as the “out-of-band” solution. This approach attempts to provide a verification of caller ID asserted by the PSTN without making any changes to the PSTN or VoIP infrastructure. The verification is done over the Internet using a third party known as a Call Placement Service (CPS), which stores and validates Call Placement Records (CPRs), records stored in real-time about who is calling whom. A very similar architecture is used today by Apple’s iMessage service in which E.164 identities are used to route text messages over the Internet. For such a service to work, users need credentials that prove that they “own” or “control” a telephone number. With this service, users would immediately begin seeing authenticated caller ID improvements, assuming that the Call Placement Services and the necessary credentials were deployed.

The resulting discussion focused on the threats and their outlined solutions. An important challenge for both methods is the allocation and validation of credentials for the service providers and users who are entitled to assert a particular E.164 telephone number as an identity. There was also some concern that although the in-band and out-of-band solutions are orthogonal, the out-of-band solution could distract from the in-band solution. Consensus calls taken by chairs Brian Rosen and Russ Housley established a strong interest in solving this problem in the IETF. Subsequent consensus calls showed interest in working on both the in-band and out-of-band solution.

Taking Action

Less than a month after this successful BoF, the STIR WG was chartered, with Robert Sparks and Russ Housley as cochairs. The charter language for the working group is to work on the in-band approach first, then work on the out-of-band approach. An overview Internet-Draft was submitted by Hadriel Kaplan called draft-kaplan-stir-fried. The STIR WG will meet for the first time at IETF 88. They’ve chosen a very aggressive timeline in which protocols are published by the middle of 2014.

Telephone users around the world can look forward to more-accurate caller ID and less telephone crime in the future once this working group completes its chartered items.

With wide deployment and a regulatory mandate, this [in-band solution] could eventually result in more-accurate caller ID and make robocalling and TDoS easier to prevent and block.

With this [out-of-band] service, users would immediately begin seeing authenticated caller ID improvements, assuming that the Call Placement Services and the necessary credentials were deployed.

With the active participation of PSTN regulators, the protocol work of STIR will likely be referenced by new regulations and laws. Telephone users around the world can look forward to more-accurate caller ID and less telephone crime in the future once this working group completes its chartered items.

For more information

Visit the STIR Working Group page at https://datatracker.ietf.org/wg/stir/charter/.
To participate in the work, subscribe to the mailing list at https://www.ietf.org/mailman/listinfo/stir.
During IETF 87 in Berlin, Germany, seven of the nine currently chartered Internet Research Task Force (IRTF) research groups (RGs) held meetings:

- Crypto Forum (CFRG)
- Delay-Tolerant networking (DTNRG)
- Internet Congestion Control (ICCRG)
- Information-Centric Networking (ICNRG)
- Network Complexity (NCRG)
- Network Management (NMRG)
- Software-Defined Networking (SDNRG)

In addition to the meetings of those already-chartered research groups, a new proposed research group on Network Coding held a second side meeting. The discussion was again positive, and the proponents are planning a third discussion during IETF 88 in Vancouver, Canada, in November.

Since IETF 86, no new RFCs were published on the IRTF RFC Stream. This is not uncommon, given the low average publication numbers on the stream. A few RFCs are expected to be published on the stream before the next meeting.

The large number of meetings in Berlin demonstrates that most RGs are active. One exception is the Routing RG, which has been dormant for a few meeting cycles. I would like to discuss with routing researchers how the group could be revitalized—please feel free to send me email or talk to me in Vancouver.

The IRTF Open Meeting at IETF 87 was the venue for two Applied Networking Research Prize (ANRP) winners of 2013 to present their research. Te-Yuan Huang presented insights into the difficulties of rate adaptation for streaming video and Laurent Vanbever proposed a framework to facilitate seamless BGP reconfigurations. The final ANRP winner of 2013 will present at IETF 88. Visit the ANRP home page at http://irtf.org/anrp to find out who it will be! For more information about the ANRP awards, see the article on page 25.

The 2014 nomination cycle of the ANRP is in full swing! Please nominate outstanding research papers. See http://irtf.org/anrp for details of the 2014 call for nominations and information about past winners.

Please join the IRTF discussion list to stay informed about these and other happenings. The website is http://www.irtf.org/mailman/listinfo/irtf-discuss.
The Internet Research Task Force (IRTF) played host to two excellent talks from the latest crop of Applied Networking Research Prize winners at their recent meeting in Berlin during IETF 87. First up was Te-Yuan (TY) Huang, a PhD student from Stanford University who presented her work on the behaviour of video streaming codecs in the presence of competing flows. For full details, see the paper for which Te-Yuan won her award: Te-Yuan Huang, Nikhil Handigol, Brandon Heller, Nick McKeown and Ramesh Johari. Confused, Timid, and Unstable: Picking a Video Streaming Rate is Hard. Proc. ACM Internet Measurement Conference, November 2012, Boston, MA, USA.

The quality of Te-Yuan’s work is amply demonstrated by the fact that her results have already influenced changes in the way major online video streaming services operate. Slides from TY’s presentation are available online at http://www.ietf.org/proceedings/87/slides/slides-87-irtfopen-0.pptx. At the ACM Sigcomm 2013 workshop on future human-centric multimedia networking, some follow-on work was also presented (http://conferences.sigcomm.org/sigcomm/2013/papers/fhmn/p9.pdf).

TY’s talk was followed by Laurent Vanbever, a post-doctoral research associate at Princeton University. Laurent presented a novel framework to deal with the difficulties of performing reconfiguration of the routing fabric of a network without causing transient instabilities. He presented results showing that the proposed framework achieves a lossless reconfiguration of a European-wide network. For full details, see the paper for which Laurent won the award: Stefano Vissicchio, Laurent Vanbever, Cristel Pelsser, Luca Cittadini, Pierre Francois and Olivier Bonaventure. Improving Network Agility with Seamless BGP Reconfigurations. Proc. IEEE/ACM Transactions on Networking, To Appear. Laurent’s slides are available at http://www.ietf.org/proceedings/87/slides/slides-87-irtfopen-2.pdf.

The final ANRP awards for 2013 will be presented during the IETF 88 meeting later this year, and the call for nominations for the 2014 award cycle is now open. Nominations can be submitted until the deadline of November 30, 2013, at http://irtf.org/anrp/2014.
Record Number of Students Attend IETF 87

By Carolyn Duffy Marsan

The Internet Society ran a successful new program this summer aimed at increasing the participation of computer science and engineering students at the IETF meeting in Berlin.

Dubbed the IETF University Outreach Pilot Programme, the effort included outreach to German and Austrian faculty, the creation of materials to help students prepare for the meeting, and daily student-focused events at the meeting.

The number of paid student registrations at IETF 87 reached 144, more than triple the number at previous meetings.

To attract these students, an ISOC team contacted 15 German and Austrian universities and asked them to share information about the IETF 87 meeting in Berlin. Two professors—Matthias Wählsch of Freie Universität Berlin and Thomas Schmidt of Hamburg University of Applied Sciences—were particularly supportive of the effort, having both attended IETF meetings in the past.

At the meeting, students attended a German-language orientation delivered by ISOC Germany chapter leader and long-time IETF participant Hans Peter Dittler and briefings with guest speakers including Axel Clauberg and Steve Conte.

The Internet Society more than tripled its goal of 50–75 student registrations—there were 144 paid student registrations at IETF 87. In comparison, the percentage of paid students among all registrants rose from 3 percent at previous meetings to more than 10 percent at IETF 87.

A post-meeting survey of the Freie Universität Berlin and Hamburg University students showed promise for the students’ continued engagement in IETF work. Nearly 100 percent of survey respondents subscribed to working group elists prior to the meeting and planned to continue tracking Internet-Drafts after the meeting. In addition, 85 percent said they had a better understanding of the Internet standards development process after attending the meeting.

Hamburg University sent 10 students to the IETF meeting in Berlin, and half of them plan to continue their involvement with particular working groups, Prof. Schmidt said.

“Having first-hand discussions with those who lead protocol design processes offered valuable insight in the thinking behind the documents, Prof. Schmidt said. He added that “the review process offered a unique chance to see how critical feedback can happen in a constructive way.”

Freie Universität Berlin also had 10 students attend the meeting, including bachelor’s, master’s and PhD candidates.

“Following the IETF process is a perfect exercise to deepen your understanding of protocol engineering,” Prof. Wählsch said. “Students see that you can start with a good idea, but that most good ideas need refinement.”

The Internet Society’s Toral Cowieson and her team will fine-tune the University Outreach Programme and roll it out again in conjunction with upcoming IETF meetings held in cities with sufficient computer science and engineering student populations.

London, Toronto, and Honolulu Area Faculty Sought for IETF University Outreach in 2014

The Internet Society is seeking computer science and engineering faculty to participate in University Outreach Programmes at IETF 89, 90 and 91. If you teach at a college or university in or near one of next year’s host cities and you wish to provide your students with exposure to the standards development process, please contact Kevin Craemer at craemer@isoc.org.
The MANIAC Challenge at IETF 87
Student competition makes network problem solving fun

By Emmanuel Baccelli, Felix Juraschek, Oliver Hahm, Thomas C. Schmidt, Heiko Will, and Matthias Wahlisch

The 87th IETF meeting was populated by MANIACs—students participating in an algorithmic communication and programming contest. The MANIAC (Mobile Ad Hoc Networking Interoperability And Cooperation) Challenge is a competition to better understand cooperation and interoperability in ad hoc networks. The third edition was held 27–28 July 2013 in Berlin, Germany. It was the first time that the MANIAC Challenge was colocated with an IETF meeting, and it was a big success.

About the MANIAC Challenge
During the MANIAC Challenge, competing teams form a wireless ad hoc network. Participants’ end devices are not only connected among each other, but also simultaneously connected to an infrastructure backbone. Teams are judged based on how much of their relayed traffic reaches its destination. A fine must be paid in the case of unsuccessful packet delivery (e.g., packet loss or exceeding the packet delivery time).

Basic Setup
All devices (i.e., WiFi access points and tablets) operated in ad hoc mode. Tablets ran Android, OLSR (Optimized Link State Routing), and the MANIAC framework. The MANIAC framework included an API (application programming interface), which provided function calls for bidding and auction and for sending and receiving data, as well as full network topology information through OLSR, which teams leveraged for their forwarding strategies.

Before the competition started, participants implemented a first version of their concept. Each team was free to design its own forwarding and bidding strategy, but it needed to comply with a detailed rule set. Challenge organizers monitored packets and collected statistical data to analyze the contest and identify incorrectly behaving nodes.

Global Participation
Five teams from North America, South America, and Europe participated in the MANIAC Challenge 2013. Isaac Supeene (University of Alberta), René Steinrücken (Hamburg University of Technology), and Asanga Udugama (University of Bremen) implemented selfishness as a virtue in MANETs (Mobile Ad-hoc Networks). The mobile offloading strategy from Alan Ferrari and Dario Gallucci (University of Applied Sciences of Southern Switzerland) was based on a Bayesian MANIAC Challenge team member at the Freie Universität Berlin

A fine must be paid in the case of unsuccessful packet delivery (e.g., packet loss or exceeding the packet delivery time).

Continued on next page

Five teams from North America, South America, and Europe participated in the MANIAC Challenge 2013.

The focus of this year’s MANIAC Challenge was on developing and comparatively evaluating strategies to offload traffic usually carried by infrastructure access points (e.g., providers) via ad hoc forwarding using handhelds (e.g., customers). The incentive for customers is discounted monthly fees, the incentive for operators is decreased infrastructure costs. The idea was to demonstrate forwarding strategies that don’t degrade user experience while offering significant mobile offloading on the infrastructure.

The competition had multiple rounds, each round comprised multiple games. After each round, teams could refine their strategies. Each game started with a bidding request of a randomly selected access point (AP) to deliver a data packet to another randomly selected AP. The AP indicated the maximum budget available for this data packet, a fine, and a maximum packet delivery time. Based on the lowest offer, the AP selected a tablet for forwarding. Each handheld should deliver the packet to the destination, either via the ad hoc network or the backbone based on independent bidding.
network. Di Li and Asya Mitseva (RWTH Aachen) tried a no-regret learning strategy. Cristian Chilipirea, Andreea-Cristina Petre, and Ciprian Dobre (University Politehnica of Bucharest) presented a wolf-pack strategy, in which rich nodes were taxed. Gabriel B. T. Kalejaiye, Joao A. S. R. Rondina, Leonardo V. V. L. Albuquerque, Tais L. Pereira, Luiz F. O. Campos, Raphael A. S. Melo, Daniel S. Mascarenhas, Marcelo M. Carvalho (University of Brasilia) followed a path-tightness strategy by analyzing the corresponding routing graph.

One goal of the MANIAC Challenge was to involve young people in IETF/IRTF activities. For most of the participants, IETF 87 was their first IETF experience. The Internet Society sponsored the students’ registration fees, which enabled the teams to attend the whole week.

On-site Event

The MANIAC Challenge continued for two days. On the first day, students met at the Freie Universität Berlin, which provided the wireless setup to perform the on-site competition. Participants tested and refined their strategies during multiple rounds. The second day took place at the IETF venue and allowed MANIAC and IETF folks to discuss practical experiences. This half-day workshop included an overview about the MANIAC Challenge, presentations of the different offloading concepts, and talks from Stan Ratliff about the current state in the MANET working group and Henning Rogge about Freifunk and OLSR.

One goal of the MANIAC Challenge was to involve young people in IETF/IRTF (Internet Research Task Force) activities. For most of the participants, IETF 87 was their first IETF experience. The Internet Society sponsored the students’ registration fees, which enabled the teams to attend the whole week. They enjoyed open-minded exchange in the different working and research groups.

Key Findings

A major problem was incompatible WiFi drivers that led to incorrect behavior between end devices. In contrast to the commonly applied infrastructure setting, nodes were operated in ad hoc mode. Our experiences showed much worse performance compared to the infrastructure mode. On the networking layer, the Android port of OLSR raised some problems. Heterogeneous bidding strategies occasionally
The winners of the MANIAC Challenge were announced during the IRTF Open Meeting on Tuesday. Two prizes have been awarded: the Performance and the Strategy Awards. The Performance Award went to the team with the maximum budget after all the rounds. The Strategy Award considered the most compelling concept.

caused negative resonance due to the convergence of different training phases.

But most important, we learned that experimenting with ad hoc networks and interesting offloading strategies can be fun!

And the Winners Are ...

The winners of the MANIAC Challenge were announced during the IRTF Open Meeting on Tuesday. Two prizes have been awarded: the Performance and the Strategy Awards. The Performance Award went to the team with the maximum budget after all the rounds. The Strategy Award considered the most compelling concept.

Lars Eggert presented the Performance Award to Isaac Supeene, René Steinrücken, and Asanga Udugama for a predictive-greedy strategy based on fine-grained, neighbor-node profiling.


Acknowledgements

The organizers of the MANIAC Challenge thank all its sponsors, in particular IETF, IRTF, and the Internet Society, which provided the appropriate setting in which to discuss the competition’s challenges and results. We thank Fabian Brandt, Lennart Dührsen, Andreas Reuter, Tim Scheuermann, and Lotte Steenbrink from Freie Universität Berlin, who implemented the MANIAC API and took care of the on-site experiments (meaning, straightened all the wireless pain).

Further Information

• MANIAC website, http://2013.maniacchallenge.org
• Code Repository, https://github.com/maniacchallenge
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 87, 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.

Stacked Tunnels for Source Routing (status)

Description: The ability of a router to influence or control the forwarding path of an individual packet or all the packets of a given Forwarding Equivalence Class (FEC) is a desirable feature for a number of reasons, including Label Switched Path stitching, egress protection, explicit routing, egress ASBR (Autonomous System Boundary Router) link selection, and backup (bypass tunnels, Remote Loop-Free Alternates) routing. This can be achieved by facilitating source-initiated selection of routes to complement the route selection provided by existing routing protocols for both interdomain and intradomain routes.

This BoF was intended to discuss the practicalities of various use cases and to establish a consensus regarding the problem space and desirability of developing solutions in this area.

Proceedings: http://www.ietf.org/proceedings/87/minutes/minutes-87-status

Outcome: A packed meeting demonstrated a clear demand to work on this. The overwhelming majority want to work on MPLS (Multiprotocol Label Switching), with some support for an IPv6 variant using extension headers. There was clear consensus to charter work on architecture, use cases, and requirements.

Network Service Chaining (nsc)

Description: Service chaining is a broad term used to describe a common model for delivering multiple services in a specific order. Service chaining decouples service delivery from the underlying network topology and creates a dynamic services plane that addresses the requirements of cloud- and virtual-application delivery. Packets and/or flows that require service chaining are classified and redirected to the appropriate, available services. Additionally, context can be shared between the network and the services.

The goal of this BoF was to let service providers explain their NSC use cases and requirements so that the IETF is exposed to the problem space and can determine next steps.

Proceedings: http://www.ietf.org/proceedings/87/minutes/minutes-87-nsc

Outcome: This was not a working-group forming BoF and there remains quite some work to do to get to a WG. More clarity regarding the problem statement and the relevant IETF work is a top priority.
PKIX over Secure HTTP (posh)

**Description:** Channel encryption with TLS (Transport Layer Security) depends on proper checking of the server's identity, as specified in RFC 2818 or RFC 6125 for PKIX certificates. However, in multitenanted environments it is effectively impossible for a hosting service to offer the correct certificates on behalf of a hosted domain, since neither party wants the hosting service to hold the hosted domain’s private keys. As a result, typically the hosting service offers its own certificate (say, for hosting.example.net), which means that TLS clients and peer servers need to “just know” that the hosted domain (say, foo.example.com) is hosted at the service.

This situation is clearly insecure. POSH (PKIX Over Secure HTTP) solves the problem via two interconnected aspects: TLS clients and peer servers retrieve the material to be used in checking the TLS server’s identity by requesting it from a well-known HTTPS URI (uniform resource identifier). If a hosted domain securely delegates an application to a hosting service, it redirects requests for the well-known HTTPS URI to an HTTPS URI at the hosting service.

The goal is to form a working group to produce a specification for POSH, and informally provide advice about how to use the POSH technique for particular application protocols.

**Proceedings:** http://www.ietf.org/proceedings/87/minutes/minutes-87-posh

**Outcome:** A good meeting helped clarify the problem space and the strong potential for IETF work. Next steps is to fine-tune the proposed WG charter.

IPRbis (iprbis)

**Description:** Experience shows that BCP 79 (Best Current Practice 79) needs a few updates. A draft is available with the proposed updates, and this BoF meeting provided the community with an opportunity to discuss the proposed changes. It was not intended to form a WG.

**Proceedings:** http://www.ietf.org/proceedings/87/minutes/minutes-87-iprbis

**Outcome:** A good discussion and some consensus was reached on difficult issues. In order to maintain momentum, an updated document will be posted and consensus confirmed on the mailing list.

Deterministic IPv6 over IEEE802.15.4e Timeslotted Channel Hopping (6tsch)

**Description:** If formed, a WG on this topic would develop an architecture that supports centralized and distributed routing and resource allocation over a TSCH-based mesh. The group would resolve the impacts on existing protocols such as RPL (Routing Protocol for Low-Power and Lossy Networks) and 6LoWPAN (IPv6 over Low-power Wireless Personal Area Networks). It would define a component that provides the expected link functionality for IPv6 over the TSCH MAC and a G-MPLS switching sublayer, and standardize the protocols or protocol extensions to establish time slots between peers and reserve resources along a path.

**Proceedings:** http://www.ietf.org/proceedings/87/minutes/minutes-87-6tsch

**Outcome:** An excellent meeting that demonstrated strong support for doing the proposed work. Although many expressed willingness to contribute to the work, concerns were expressed about the potentially large scope. A refined charter with fewer work items is likely to be approved soon.
Domain-based Message Authentication, Reporting and Conformance (dmarc)

See page 20 for our article on this topic. See the proceedings at http://www.ietf.org/proceedings/87/minutes/minutes-87-dmarc.

Tunnelling Compressed Multiplexed Traffic Flows (tcmtf)

Description: The interactivity requirements of some emerging services (e.g., VoIP, videoconferencing, tele-medicine, video vigilance, and online gaming) make them send high rates of small packets in order to transmit frequent updates between the two extremes of the communication. They also demand small network delays. In addition, other services also use small packets, although they are not delay-sensitive (e.g., instant messaging, m2m packets sending collected data in sensor networks using wireless or satellite scenarios). For both the delay-sensitive and delay-insensitive applications, their small data payloads incur significant overhead.

When a number of small-packet flows share the same path, bandwidth can be saved by multiplexing packets belonging to different flows. If a transmission queue has not already been formed but multiplexing is desired, it is necessary to add a multiplexing delay that must be maintained under some threshold in order to grant the delay requirements.

The BoF aims for the creation of a WG in order to specify the protocol stack, signalling mechanisms, and maximum added delay recommendations for tunnelling, compressing, and multiplexing traffic flows (TCMTF).

Proceedings: http://www.ietf.org/proceedings/87/minutes/minutes-87-tcmtf

Outcome: Opinion was divided regarding the clarity and completeness of the problem statement and whether or not to create a working group to address this. More work is required to understand the potential side effects of using something like TCMTF beyond satellite links.

DNS-SD Extensions (dnssdext)

Description: The proposed WG will develop solutions to provide scalable DNS-SD (Domain Name System-Service Discovery) services in multilink, routed networks as found in academic, enterprise, home, and mesh radio networks. This was the second BoF on this topic, following the mdnsext BoF held during IETF 85.

Proceedings: http://www.ietf.org/proceedings/87/minutes/minutes-87-dnssdext

Outcome: A good meeting with strong support shown for IETF work on this topic and people willing to contribute. More work is required to refine the charter, but this is likely to proceed.
IPv6 over networks of resource-constrained nodes (6lo)

**Description:** This BoF discussed a proposed working group that would focus on adaptation layers for constrained node networks, working closely with the Internet Area working groups and other IETF WGs focused on constrained node networks.

**Proceedings:** http://www.ietf.org/proceedings/87/minutes/minutes-87-6lo

**Outcome:** Very strong support for IETF work on this topic and lots of people willing to review, edit, and implement documents. Further scoping discussions are required, but this is likely to proceed.

Active Queue Management (aqm)

**Description:** Internet routers, lower-layer switches, and other middleboxes include buffers or queues to hold packets when they are not immediately able to be forwarded to the next hop. These queues are intended to absorb bursts of traffic that may naturally occur, and to avoid unnecessary losses. However, queues also cause latency and jitter in the eventual arrival times of packets. This can cause issues and complications for interactive applications.

The Active Queue Management and Packet Scheduling working group (AQM) is intended to work on algorithms for proactively managing queues.

**Proceedings:** http://www.ietf.org/proceedings/87/minutes/minutes-87-aqm

**Outcome:** A very productive discussion with strong support shown to form an IETF WG on this topic. Lots of people are interested in contributing.

DTLS in Constrained Environments (dice)

**Description:** There is an increased use of wireless control networks in city infrastructure, environmental monitoring, industrial automation, and building management systems. These wireless control networks comprise many electronic devices, sensors, and actuators that are connected to each other, and in most cases Internet connected. The CoRE working group has defined a framework for resource-oriented applications intended to run on Constrained Node Networks (CNN) (see I-D-ietf-lwig-terminology). The Constrained Application Protocol (CoAP) can be used to manipulate resources on a device in a CNN.

Unsecured group communication for CNNs is enabled by using CoAP on top of IP-multicast. However, it must be secured as it is vulnerable to the usual attacks (e.g., eavesdropping, tampering, message forgery, and replay). Datagram Transport Layer Security (DTLS) has been chosen by CoRE to protect CoAP unicast communications, and it would be beneficial if the same security protocol can be used to protect CoAP group communication as well.

This WG combines expertise from both the IETF Application and Security areas in order to develop the appropriate security solutions.

**Proceedings:** http://www.ietf.org/proceedings/87/minutes/minutes-87-dice

**Outcome:** A well-organised meeting that detailed the problem statement, scope of the proposed work, and relationships with other Working Groups. Lots of enthusiasm for starting a WG on this topic and people with energy to contribute to doing the work.

Secure Telephony Identity Revisited (stir)

See page 22 for our article on this topic. See the proceedings at http://www.ietf.org/proceedings/87/minutes/minutes-87-stir.
IETF 87 At–A–Glance

Registered attendees: 1,426
Newcomers: 316
Number of countries: 62

IETF Activity since IETF 86
(March 2013–June 2013)
New WGs: 6

SLA Performance
• Processing goal average for IETF-related requests: 98%
• Currently drafting the 2014 SLA

Projects and Deliverables
• Phase 2 of integration completed!
• XMLization of registries 99% complete

IANA and DNSSec
• 107 TLDs have a full chain of trust in the root, see http://stats.research.icann.org/dns/tld_report/
• Ceremony 13 was executed successfully 2 May 2013
• Ceremony 14 took place 7 August 2013

RFC Editor Activity since IETF 86
(March 2013–June 2013)
Published RFCs: 98
• 48 Standards Track, 5 BCP, 7 Experimental, 33 Informational
citations@rfc-editor.org replaced webmaster@xml.resource.org
Datatracker extensions (RFC 6359): two phases
• 1. RFC Editor – Datatracker (complete)
• 2. Datatracker – RFC Editor (complete)

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

Receive the latest edition of the IETF Journal as soon as it is available—in hardcopy or via email. Subscribe today at:
http://www.internetsociety.org/ietfjournal

Want it faster? Follow the @ietfjournal Twitter stream to read the articles as they are published.
### IETF Meeting Calendar

<table>
<thead>
<tr>
<th>IETF 88</th>
<th>IETF 90</th>
</tr>
</thead>
<tbody>
<tr>
<td>3–8 November 2013</td>
<td>20–25 July 2014</td>
</tr>
<tr>
<td>Host: Huawei</td>
<td>Host: TBD</td>
</tr>
<tr>
<td>Location: Vancouver, BC, CA</td>
<td>Location: Toronto, ON, Canada</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>IETF 89</th>
<th>IETF 91</th>
</tr>
</thead>
<tbody>
<tr>
<td>2–7 March 2014</td>
<td>9–14 November 2014</td>
</tr>
<tr>
<td>Host: TBD</td>
<td>Host: TBD</td>
</tr>
<tr>
<td>Location: London, England</td>
<td>Location: Honolulu, HI, USA</td>
</tr>
</tbody>
</table>

For more information about past and upcoming IETF Meetings

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

---

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

[Platinum Programme supporters of the Internet Society]

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