FROM THE EDITOR’S DESK

By Mat Ford

THE 98TH MEETING OF THE IETF TOOK PLACE IN RAINY DOWNTOWN CHICAGO, ILLINOIS, USA. As usual, it was a busy meeting with lots of interesting work to report on. This IETF Journal provides merely a snapshot of the events and discussions that made this meeting so memorable.

Our cover article is a deep dive into Segment Routing, a new traffic-engineering technology being developed by the SPRING Working Group.

Also in this issue, you’ll learn about the many activities of the new Education and Mentoring Directorate, which aims to enhance the productivity, diversity, and inclusiveness of the IETF (page 16).

We also present an update from the Security Automation and Continuous Monitoring WG (page 13), BoF updates (page 24), a readout from the pre-IETF Hackathon (page 18), a list of the tech demonstrations at the Bits-N-Bites event (page 8), and an article about the Internet Society’s IETF Policy Programme (page 17). Our regular columns from the chairs and coverage of the IETF plenary wrap up the issue.

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

SEGMENT ROUTING: CUTTING THROUGH THE HYPE AND FINDING THE IETF’S INNOVATIVE NUGGET OF GOLD

By Adrian Farrel and Ron Bonica

SEGMENT ROUTING (SR) IS A NEW TRAFFIC-ENGINEERING TECHNOLOGY BEING DEVELOPED BY THE IETF’S SPRING Working Group. Two forwarding plane encapsulations are being defined for SR: Multiprotocol Label Switching (MPLS) and IPv6 with a Segment Routing Extension Header. This article provides some historical context by describing the MPLS forwarding plane and

Continued on page 5
MESSAGE FROM THE IETF CHAIR

By Alissa Cooper

In March I officially took on the role of IETF Chair. My predecessor Jari Arkko noted upon beginning his term just how much can change from one term to the next. While settling into my new role these past months, I’ve been thinking about his comment, about both what is changing in the IETF and what is staying the same.

When I first started participating in the IETF, I soon realized its importance as a venue for creating the building blocks of the Internet. The significance of the IETF derives from a combination of what we choose to work on and how we carry out that work. Producing core standardized protocols wouldn’t have nearly the same impact on the Internet if it were done behind closed doors, if a single constituency could dictate the outcome, or if broad interoperability were not the main objective. The core principles of the IETF process—open participation, cross-area review, and consensus—contribute to the success of IETF protocols in tandem with the design choices and technical trade-offs inherent in protocol design.

Our nearest challenge is to preserve the benefits of the core IETF model while adapting to changes in the industry and the environment. With collaborative styles of engagement flourishing across both open source and standards development, there is a lot of opportunity for synergy.

Of course, those process features are also often cited as drawbacks of IETF participation. “The IETF moves too slowly,” some people say. “They’re not adaptable,” “they can’t compete with open source,” “the biggest players aren’t interested in consensus.” Sound familiar? Sure, it’s generally true that finding agreement among a large, heterogeneous pool of people requires different time and work investments than deciding things among a close group of friends or hacking something together on your own. A pressing challenge for us is to preserve the benefits of the core IETF model while adapting to changes in the industry and the environment. With collaborative styles of engagement flourishing across both open source and standards development, there is a lot of opportunity for synergy.

How can we do a better job of integrating our work with open source development efforts? How can we evolve our tools and processes to align with how software is being developed and deployed today? How might we apply the model of cross-area review and consensus more broadly than to static text specifications? How can we evolve the administration of the IETF to give the community more flexibility and room to experiment? I have my own thoughts about these questions, but far more important are the ideas and efforts of the IETF community.

Continued on page 4

Recent IESG Document and Protocol Actions

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

By Ted Hardie

During the Joint Internet Engineering Steering Group (IESG) and Internet Architecture Board (IAB) retreat on 15-17 May 2017, the group discussed a number of topics related to network operator activities for encrypted flows. As part of that conversation, the group looked at RFC 4084 (May 2005), which tackled the question, what does Internet access mean? A dozen years after its publication, the subject probably deserves a new look, and several of the folks at the retreat agreed to draft a new version for community review.

As one of those volunteers, I’d like to dive into RFC 4084, and share what may have changed since it was written. After walking through the need to avoid pejorative terms, the RFC sets out the following types of connectivity: web connectivity, client connectivity only with no public address, client connectivity only with a public address, firewalled Internet connectivity, and full Internet connectivity.

For those who have bought enterprise connectivity recently, it’s obvious that several common categories are missing, including dark fiber, lit service connectivity to a home office, and managed MPLS tunnels, to name a few. More important, however, the RFC doesn’t really touch on cellular wireless connectivity, which is now one of the most common ways people connect to the Internet. This means that it also doesn’t touch on topics like data caps, roaming for data services, zero rating, and data compression proxies. For cellular connectivity, these topics can be the key to understanding the trade-offs in connectivity, privacy, and costs for a particular service offering.

Beyond the proliferation in available offerings, there has been another major change: the ubiquity of filtering. RFC 4084 describes filtering at the ISP level in Section 3, where it notes: “the effort to control or limit objectionable network traffic has led to additional restrictions on the behavior and capabilities of internet services”. RFC 7754 (March 2016) provides a much more detailed description of blocking and filtering, and highlights restricting objectionable content as a category beyond blocking objectionable traffic that may be a requirement imposed by state regulators. In such jurisdictions, what RFC 4084 described as “full Internet connectivity” has disappeared, because service providers are required to prevent their customers from reaching specific Internet resources, services, or destinations. Even where blocks are not in place, regulatory increases in the amount of Internet tracking data retained and the length of time it is kept have become common. These may contribute to self-censorship in the use of some content. Simply put, firewalled Internet connectivity has become the default offering required of service providers within those territories.

In addition, RFC 4084 describes Internet connectivity in terms that apply to the services that are consumed by a human user and, although some social networking and streaming services are absent, it remains generally useful in that regard. As we move into an era in which devices talk to other devices, we need to examine what a service provides for traffic among devices or between devices and back-end services. Is the implication of a web-only service that the Internet of Things is not supported, or is the implication that it must be reached by a web-based gateway or proxy? The difference between those two scenarios is a topic of serious contemplation today, and the architecture of a number of future services may depend on it.

In many cases, the architecture of the Internet has developed in the course of a commercial dialog between network operators’ offerings and consumers’ use. Many efforts to make cellular systems walled gardens failed, for example, because users simply weren’t willing to use them that way and wanted the broader connectivity of the Internet. As we look at this new tension among users’ desires for confidential communication, network operators’ management practices, and regulatory frameworks, a common vocabulary for the services available to users may help us understand what architectures we can build. If you’d like to contribute to the early discussion, architecture-discuss@iab.org is one place to start.
Recent IETF standards development work, as well as ongoing community conversations and activities, offer many reasons to be optimistic about tackling these questions. Over the last several years we’ve seen protocol development efforts deeply intertwined with and informed by running code, with the concurrent development of 10 or more independent implementations in cases such as HTTP/2 and TLS 1.3. We’ve seen broad interest across the industry in the kind of security expertise that has become a hallmark of the IETF, and resulting security and privacy improvements being developed for Web, email, DNS, DHCP, real-time, and other kinds of traffic. We’ve seen tremendous energy behind the specification of YANG data models and their integration across the industry into standards processes. And community discussion and activity continues to grow around IETF Hackathons, use of Github, remote participation, and IASA 2.0.

I’m excited to work with the IETF community to tackle these coming changes. In addition to the existing discussion venues, please feel free to send your thoughts directly to me (chair@ietf.org) or post them to the IETF discussion list (ietf@ietf.org).

**Highlights from IETF 98**

The 98th IETF meeting was a typically busy work week for IETF participants, but also a special week, as a number of changes in our leadership became official. We welcomed newly elected individuals into the leadership and gave our thanks to outgoing members of the Internet Engineering Steering Group (IESG), Internet Architecture Board (IAB), and IETF Administrative Oversight Committee (IAOC), including the outgoing IETF chair, Jari Arkko.

Amidst all the Working Group action and leadership transition activities, a few highlights stood out for me. Among more than 1,000 attendees, nearly 17% were attending their very first IETF meeting. We’re constantly evaluating what we can do to attract cutting-edge standardization work and new participants to the IETF, so it was nice to see many new faces.

Meetings at IETF 98 demonstrated that a number of core security and Web application standards are on a path towards high levels of maturity and industry adoption. These include the following:

- Transport Layer Security (TLS) version 1.3, a significant performance and security upgrade to the current version of TLS.
- The Automated Certificate Management Environment (ACME) protocol specification, which has provided the foundation for certificate management automation for the Web.
- The core Real-Time Communication in Web Browsers (RTCWEB) specifications, which together allow for standardized interactive communication using audio, video, and data connections between Web browsers.

Work on all of these standards is heading towards conclusion within their respective Working Groups. There was also a large TLS team at the IETF Hackathon representing 18 independent implementations, and they were named the overall Hackathon winners by the judges.

IETF 98 was also very busy for those working on YANG data models related to both network management and routing. While participants continue to press forward with the standardization of hundreds of different YANG modules in the IETF, they’ve also been focusing on guidelines and tooling (e.g., yangcatalog.org) to help streamline the model development process and aid interoperability.

Our technical plenary speakers, Niels ten Oever and David Clark, addressed questions about the relationship between Internet protocols and human rights. Clark encouraged us to think of standardization activities as “designing the playing field” and to contemplate how we “tilt the playing field” based on the design choices we make. As expected, the topic yielded a provocative community discussion session.

We owe deep thanks to our meeting host, Ericsson. As an IETF Global Host, Ericsson has committed to host three IETF meetings in a 10-year period and affirmed its long-standing support for the work of the IETF. We heard at the plenary session just how important IETF work is to Ericsson’s industry and technology goals, particularly as the coming shift towards 5G inspires potential new requirements around packet transport, network and service management, and virtualization.

Until we gather again in July for IETF 99, work will continue on mailing lists, at interim meetings, and on Github¹. See you in all of those places... ☺️

**Footnote**

control plane protocols, explains how Segment Routing works, introduces the MPLS-SR forwarding plane, and shows how the SR control plane is used. Finally, the article compares SR with legacy MPLS systems, and identifies its unique merits.

**MPLS Forwarding**

MPLS is a nearly 20-year-old technology. An MPLS domain is a contiguous set of Label Switching Routers (LSRs). Packets enter the MPLS domain through an ingress LSR and exit the MPLS domain through an egress LSR. A single LSR can serve as ingress for some packets and egress for others.

A Label Switched Path (LSP) provides connectivity between an ingress LSR and an egress LSR. An LSP can traverse the least-cost path or it can traverse a traffic-engineered path.

When an ingress LSR receives a packet, it assigns the packet to a Forwarding Equivalence Class (FEC) and encapsulates the packet with an MPLS label stack. It then forwards the packet to the next-hop associated with the FEC.

The MPLS label stack contains one or more label stack entries. Each label stack entry contains a label, a time-to-live (TTL) indicator, a Traffic Class (TC) indicator, and a bottom of stack indicator. These data items determine how a transit LSR will process the packet. In that way, each label stack entry is an instruction to an LSR.

When an LSR receives a packet it examines the top entry in the label stack and decrements the TTL. If the TTL has not expired, the LSR searches its Forwarding Information Base (FIB) looking for an entry that matches the incoming label.

If the LSR finds a FIB entry that matches the incoming label, the FIB entry will contain the following information:

- **Label action**
- **Next-hop interface**

Label actions are the following:

- Push one or more new entries onto the label stack.
- Pop the top entry from the label stack.
- Swap the label in the top entry.

Having found a matching FIB entry, the LSR executes the label action and forwards the packet through the next-hop interface. The next-hop interface can be an internal interface or an external interface. If the next-hop interface is an internal interface, the LSR forwards the packet to itself and processes the packet as it had just been received, examining other protocol headers. If the next-hop interface is an external interface, the LSR forwards the packet appropriately.

When a packet reaches the penultimate hop on an LSP, the LSR may pop the final label stack entry and forward the payload packet without any encapsulation.

**MPLS Control Plane**

**Routing Protocols**

An MPLS network makes heavy use of the Interior Gateway Protocols (IGPs)—Open Shortest Path First (OSPF) or Intermediate System-to-Intermediate System (IS-IS)—to learn the network topology, establish the least cost paths, and provide information for computing traffic engineering paths. Normal IGP advertisements are used to distribute the connectivity and metrics for the network links, and those messages are enhanced with additional information describing the links (such as bandwidth).

**Label Distribution Protocol (LDP)**

LDP is a TCP-based protocol that can be run between adjacent LSRs in an MPLS network. Each LSR uses the protocol to advertise the label to use when MPLS encapsulated packets are sent to it for final delivery to an IP prefix. As each LSR receives advertisements from other LSRs it is able to install entries in its FIB showing how to map from the label in a packet it receives (a label it has advertised) to a label in a packet it forwards (a label it has received in an advertisement).

LDP results in traffic being forwarded along the least cost path and does not support traffic engineering.

**Resource Reservation Protocol with TE Extensions (RSVP-TE)**

In RSVP-TE, network operators administratively assign TE attributes to interfaces. TE attributes include, but are not limited to, available bandwidth, reserved bandwidth and administrative color. These TE attributes are flooded by the IGP so that each node within the IGP domain maintains an identical copy of a Link State Database (LSDB) and a Traffic Engineering Database (TED). The LSDB describes the IGP topology, while the TED augments the LSDB with TE link attributes.

A Label Switched Path (LSP) provides connectivity between an ingress LSR and an egress LSR.
Network operators request LSPs that meet specific constraints. For example, a network operator could request an LSP that originates at Node A, terminates at Node Z, reserves 100 megabits per second, and traverses blue interfaces only. A path computation module, located on a central controller—such as the Path Computation Element (PCE)—or on the ingress LSR, computes a path that satisfies all of the constraints. In order to construct this SR-path, the path computation function consults the LSDB and TED.

RSVP-TE requires that state is maintained in the network for each LSP and that the protocol is a “soft state protocol”, meaning that Path and Resv messages must be exchanged periodically to keep the LSP active.

Each LSR selects a label that it will use to receive traffic on the LSP. It includes this label in the Resv message it sends. Thus, each LSR can build a FIB entry for the LSP mapping the label it has advertised to the label it has received.

RSVP-TE requires that state is maintained in the network for each LSP, and the protocol is a “soft state protocol”, meaning that Path and Resv messages must be exchanged periodically to keep the LSP active.

Segment Routing

Terminology
An SR domain is a contiguous set of SR-capable routers. An SR-Path (i.e., an SR-signaled LSP) provides connectivity through the SR domain. An SR-path can traverse the IGP least cost path between its endpoints. It can also traverse a traffic-engineered path.

An SR-path contains one or more segments and a segment contains one or more router hops. The SPRING WG has proposed many segment types. However, the following segment types are most common:

- Adjacency
- Prefix
- Acast
- Binding

Adjacency segments represent an IGP adjacency between two routers. They typically contain one router hop, but can contain more. Prefix segments represent the IGP least cost path between any router and a specified prefix. Prefix segments contain one or more router hops. Anycast segments are like prefix segments in that they represent the IGP least cost path between any router and a specified prefix. However, the specified prefix can be advertised from multiple points in the network. Binding prefixes represent tunnels through the SR domain. The tunnel can be another SR-Path, an LDP-signaled LSP, an RSVP-TE signaled LSP, or any other encapsulation.

A Segment Identifier (SID) identifies each segment. SIDs that represent prefix and anycast segments have domain-wide significance. Therefore, network operators allocate them using procedures that are similar to those used to allocate private IP (i.e., RFC 1918) addresses. Conversely, SIDs that represent adjacency and binding segments have local significance only. SR-capable routers allocate these SIDs automatically, without concern for domain-wide coordination.

Every SID maps to an MPLS label. As stated, MPLS labels have local significance only. Therefore, SIDs that have local significance can only map directly to MPLS labels. However, SIDs that have domain-wide significance require special treatment.

Each SR-capable router reserves a range of MPLS labels, called the SR Global Block (SRGB). For example, Router A might reserve labels 10,000 through 20,000, while Router B reserves labels 20,000 through 40,000. Both routers map SIDs to MPLS labels by adding the SID to the lowest SRGB value. Therefore, Router A maps SID 1 to MPLS label 10,001, while Router B maps the same SID to MPLS label 20,001.

SR Forwarding
When an SR ingress router receives a packet, it assigns the packet to FEC and encapsulates it in an MPLS label stack. Finally, it forwards the packet to the next-hop associated with the FEC.
The MPLS label stack represents an SR-path that is associated with the FEC. Each entry in the label stack represents a segment in the SR-path.

In Figure 1, R1 maintains an SR-path to R4. The SR-path contains five adjacency segments, originating at R2, R3, R7, R6, and R5. The ingress LSR (R1) imposes a label stack with one entry for each adjacency segment. Finally, R1 forwards the packet to R2, where the first adjacency segment begins. R2 processes the outer label stack entry, popping it and forwarding the packet to R3. Each downstream LSR repeats the process until the packet arrives at R4.

In Figure 2, R1 through R6 all maintain an SR-path to R7. The SR-path contains a single prefix segment, represented by SID 7. We will examine the path from R4 to R7.

The ingress router (R4) imposes a label stack that contains exactly one entry, representing the prefix segment (i.e., the IGP least cost path) between R4 and R7. This label stack entry carries a label that corresponds to SID 7. In order to calculate that label, R4 adds the SID (7) to the SRGB base advertised by the next-hop, R5 (i.e., 200). The result is 207. Finally, R4 forwards the packet to R5.

R5 processes the label. In order to do so, it identifies the router on the IGP least cost path to R7 (i.e., R6). Then R5 swaps the label, replacing it with the value that R6 maps to SID 7 (i.e., 307). Finally, it forwards the packet to R6. R6 repeats this process and the packet arrives at R7.

In Figure 3, R1 maintains a traffic-engineered SR-path to R4 via R7. The SR-path contains two prefix segments. One prefix segment represents the IGP least cost path from R1 to R7, the other represents the IGP least cost path from R7 to R4.

The ingress LSR (R1) imposes a label stack with one entry representing each...
Segment Routing, continued

prefix segment. It calculates the inner label value by adding R4’s SID (4) to R7’s SRGB base (300). It calculates the outer label by adding R7’s SID (7) to R2’s SRGB base. Finally, R1 forwards the packet to R2. All downstream routers process the packet as described in the previous example and the packet arrives at R4.

IGP Extensions for Segment Routing
Each SR-capable router allocates a SID and a label for the following:

• Each prefix or anycast segment that it terminates
• Each adjacency or binding segment that it originates

Having done so, it creates a RIB entry for each of the above and installs the RIB entries into the FIB.

Next, the SR-capable router advertises the following into its IGP:

• Its SRGB characteristics
• Each prefix or anycast segment that it terminates
• Each adjacency or binding segment that it originates

The IGP floods this data, in addition to the TE link attributes, throughout the IGP domain. Therefore, each node within the IGP domain maintains an identical copy of a Link State Database (LSDB) and a Traffic Engineering Data-base (TED). The LSDB describes the IGP topology, including SIDs and SRGB data, while the TED augments the LSDB with TE link attributes.

When flooding is complete, every node within the IGP domain constructs two RIB entries for each prefix or anycast segment that it does not terminate. The first RIB entry instructs the local device to process all incoming IP traffic bound for the prefix as follows:

• Push an MPLS label stack entry whose label maps to the SID.
• Forward the packet to the next-hop on the IGP least cost path to the segment endpoint.

The second RIB entry instructs the local device to process all incoming MPLS traffic whose outermost label maps to the segment as follows:

• Swap the outermost label, accounting for the next-hop’s SRGB.
• Forward the packet to the next-hop on the IGP least cost path to the segment endpoint.

Path Computation
A path computation function calculates SR-paths. Given a set of TE constraints, the path computation function yields an MPLS label stack representing an SR-path that satisfies the constraints. In order to construct this SR-path, the path computation function consults the LSDB and TED.

The path computation function can reside on a central controller. Conversely, the path computation function can be distributed among ingress LSRs.

Analysis
LDP and RSVP-TE are end-to-end signaling protocols that establish per-LSP forwarding state in LSRs. Because LDP and RSVP-TE maintain all required forwarding state in LSRs, an LDP, or RSVP-TE signaled LSP can be represented by a single MPLS label stack entry.

By contrast, SR moves some, but not all, forwarding state from the network to the packet. An SR-path is represented by a label stack, with one label stack entry representing each segment in the SR-path. Therefore, the network maintains enough state to route the packet from segment ingress to segment egress, while the packet maintains enough state to route the packet from segment to segment.

By moving state from the network to the packet, SR reduces the amount of memory that LSRs require and the amount of processing needed to maintain state.
A more-significant benefit of moving state from the network to the packet is that it eliminates the need for an end-to-end signaling protocol.

Recent increases in CPU and memory within routers, and improvements to the RSVP-TE protocol and to implementations have reduced this issue, but it remains an important concern.

A more-significant benefit of moving state from the network to the packet is that it eliminates the need for an end-to-end signaling protocol. While SR requires an IGP and a path computation module, it does not require a signaling protocol like LDP or RSVP-TE.

However, some advanced functions offered by RSVP-TE rely on end-to-end signaling and per-LSP state in the network. Among these are bandwidth reservation, failure detection, and fast-reroute.

In RSVP-TE, the path computation function can be distributed among ingress LSRs, even when TE constraints include bandwidth reservations. This is possible because in RSVP-TE, each LSR maintains state for each LSP that it supports. Having this state, it can compute the remaining bandwidth on each RSVP-enabled interface and flood that information into the IGP. Therefore, every node in the IGP maintains an LSDB and TED with sufficient information to support the path computation function.

In SR, no such mechanism exists. When TE constraints include bandwidth reservations, the path computation function must be centralized in a controller where a global view of bandwidth allocation is available.

In RSVP-TE, the end-to-end signaling mechanisms also provides OAM functionality. When an RSVP-TE neighboring session fails, the LSR upstream of the failure signals the ingress LSR, causing it to invoke head-end restoration procedures. If configured to do so, the LSR upstream of the failure can also invoke local restoration procedures.

In SR, restoration is more complex. If the failure occurs at a segment ingress, some OAM mechanism outside of SR detects the failure and informs the path computation module. The path computation module invokes head-end restoration procedures, recalculating the SR-path between the SR ingress and the SR egress. While local restoration procedures for SR are conceivable, none have been standardized to date.

If a failure occurs at some point other that the segment endpoint, SR relies on external recovery mechanisms. For example, if a failure occurs in the middle of a prefix segment, SR relies on an IGP to detect the failure, flood topology changes, and compute the new IGP least-cost path to the segment endpoint. In this example, TI-LFA can be deployed to reduce dependence upon IGP convergence.

Conclusion

SR supports traffic engineering while reducing the amount of state maintained by the network. In many cases, SR eliminates the need for MPLS signaling protocols (i.e., LDP and RSVP-TE). For these reasons, the IETF should continue to develop SR capabilities.

Specifically, IETF should continue to develop IGP extensions for SR, as well as BGP extensions that may be required to extend SR across IGP boundaries. Additional work is essential to develop key networking functions such as OAM and ways to carry entropy to resolve ECMP choices. Furthermore, network equipment vendors and network operators should work together to prototype and experiment with SR to provide operational feedback to the IETF, so that SR can be improved and made ready for wide-scale deployment.

It is likely that network operators will deploy SR incrementally over the next several years. As deployments proceed, the SR community will gain operational experience, SR standards will be refined to address unforeseen problems, and implementations will improve accordingly. Furthermore, network operators will identify use-cases for which SR is well suited, as well as use-cases for which LDP and RSVP-TE may be better suited.

For these reasons, as well as to support a massive installed base, the IETF and network equipment vendors should continue to refine and support LDP and RSVP-TE with the same intensity that they progress SR.
IETF DEBATES ITS ROLE IN SUPPORTING HUMAN RIGHTS VIA INTERNET PROTOCOL DEVELOPMENT

By Carolyn Duffy Marsan

At its technical plenary session at IETF 98 in Chicago, the Internet Architecture Board sponsored a lively debate about how best to handle human rights considerations in protocol development. The discussion revolved around a draft document that was developed during the last two years by the Internet Research Task Force’s Human Rights Protocol Consideration (HRPC) Research Group. The HRPC group is exploring how Internet protocol development can enable, strengthen, or weaken rights, such as freedom of expression and freedom of assembly as outlined in widely approved treaties such as the Universal Declaration of Human Rights and the International Covenant on Civil and Political Rights.

The HRPC group believes that as a global network-of-networks, the Internet should strive to provide continuous connectivity to all users for all content. As such, the group believes that the Internet’s promise of open, secure, and reliable connectivity makes it a key enabler of human rights. The group is exploring the relationship between human rights and protocols, and is working on guidelines for protocol developers to help them avoid situations where a new protocol would inhibit users’ ability to exercise their freedom. Ideally, these guidelines will be similar to the work done for Privacy Considerations in RFC 6973.

Niels ten Oever, cochair of the HRPC Research Group and head of digital for article 19, opened the discussion by conceding that the HRPC group’s effort to understand and demonstrate the human rights impact of Internet protocols is difficult. “We’ve all seen the Internet as this huge engine for freedom of expression, and it has indeed enabled us to create whole new opportunities for people to express themselves and gather information. But it doesn’t mean there aren’t downsides to our work as in the case of pervasive surveillance,” ten Oever explained.

Ten Oever pointed out that the Internet is playing an increasingly important role in such areas as freedom of expression, "We have, in the IETF, contributed greatly to the shaping of the Internet that we have today. But with great power, comes great responsibility. This is a call to assert that power.”—Niels ten Oever
association, and assembly, as well as in education, public debate, and even voting. He emphasized that despite the IETF’s efforts, access to the Internet is not equally distributed to the rest of the world.

“We have, in the IETF, contributed greatly to the shaping of the Internet that we have today,” ten Oever said. “But with great power, comes great responsibility. This is a call to assert that power.”

Ten Oever said that the IETF holds and propagates certain values, such as fairness, decentralization of control, and resource sharing. So considering ways to mitigate how its protocols might be used to limit human rights is not out of the standards body’s charter. In particular, he pointed to RFC 6973, which outlines privacy considerations for Internet protocols, and to BCP 72, which provides guidelines for security considerations for all protocols.

Ten Oever added that other standards bodies, including IEEE and ISO, are taking ethical concerns and social responsibility into consideration when creating Internet protocols.

“This is complex,” ten Oever admitted. “We need to understand our own role and take responsibility. This does not mean that our technology is bad nor that it is good, but it definitely means that our technology is not neutral.”

He encouraged all IETF participants to review the draft guidelines for human rights considerations that are published as an information document on the group’s website. “We need protocol developers to road test the guidelines,” he said.

David Clark, head of the Computer Science Artificial Intelligence Lab (CSAIL) at Massachusetts Institute of Technology (MIT), said that he has read the draft guidelines and found them both “fascinating” and in alignment with a movement he supports called “values in design”.

“Human rights are not absolute,” Clark said. “Designers of technology have a choice: to be in the conversation or not.”

As an example, he pointed to the Raven debate back in the year 2000, when the IETF declined to develop standards that would allow for lawful intercept of communications by law enforcement agencies.

“By declining, the IETF left the decision to others,” he said. “It doesn’t mean we didn’t get wiretap standards. It just meant they were made by someone else.”

Clark said the IETF has a choice: to continue designing protocols for a preferred outcome as it did in the Raven debate. Or it can incorporate into its protocol design a tolerance for a range of
outcomes that it might not prefer, such as the ability to wiretap.

“You are designing the playing field, not the outcome of the game,” Clark pointed out. “But if you are clever enough, you can tilt the playing field.”

Following remarks from ten Oever and Clark, the IAB’s Lee Howard moderated questions from the audience.

Longtime IETF member Scott Bradner provided some background on the Raven debate for audience members who hadn’t participated in those discussions. “It was not an easy discussion,” Bradner said. “There were people who said it is a moral sin that governments wiretap, and also people who said it is a government’s responsibility to do so. It was a political discussion masquerading as technology.”

The audience seemed split on the IETF’s role in human rights discussions. Some members questioned whether the IETF was the right standards body to tackle these types of issues and warned that its engineering goals could be sidetracked by ethical debates. Others, including Clark and ten Oever, encouraged the IETF to take a more active role in these controversial debates than it has in the past.

“There are people such as lawyers, judges, legislators, public opinion, and the market that are thinking about ethics. This does not mean that we should not,” ten Oever said. “We cannot outsource our ethics to others and hope that they take care of it. But it also means that we are not going to replace them. We should, just within our little realm, take our responsibility.”

Similarly, former IETF Chair Harald Alvestrand argued that the IETF has no choice but to get involved in human rights-related debates and try to “tilt the playing field in the direction that we want.”

Daniel Kahn Gillmor of the American Civil Liberties Union likewise argued for the IETF to get involved in these debates because it is building important tools that everyone in the world uses.

“It is critically important that engineers, like all of us in this room, think ethically all the time about what the consequences are,” Gillmor said. “I’m really happy to hear that we are having this discussion and acknowledging that we are playing a role about whether people can exercise the rights that they expect to have on the Internet today, tomorrow, and the day after tomorrow.”

Howard ended the discussion by encouraging IETF participants to continue the conversation in the HRPC Research Group.
WORKING GROUP UPDATE: SECURITY AUTOMATION AND CONTINUOUS MONITORING

By Jessica Fitzgerald-McKay

In light of recent network attacks, security automation and continuous monitoring of your network is a must. Up-to-date knowledge about the state of the network and the endpoints that comprise it is more critical than ever. Network posture information provides network defenders with the information they need to properly secure critical data, remediate vulnerabilities before they are exploited, and deflect attacks by malicious actors. The same network posture information underpins network resiliency, enabling operators to fight through and recover from network attacks when deflection fails. Automating the processes to collect this data, leverage it against network attacks, and support resilient network operation saves time and resources, thereby offering both security benefits to the network and economic benefits to network owners.

Why, then, is security automation not ubiquitous? Because proper security automation requires interoperability from a diverse set of products. Each tool or analytic process on the network must work in concert—from orchestrators that direct network security actions to the collectors that feed them data, from Security Information and Event Management tools (SIEMs) that detect attacks to the firewalls that perform commands to block malicious activity, from the routers and switches that form the backbone of the network to the boundary devices that protect them. Each endpoint needs to be a part of a fully automated solution. And the scope of the desired solution—automating network security functions to the fullest extent feasible—is enormous. Currently, network endpoints, tools, and analytics do not interoperate sufficiently within available security automation solutions to truly automate network security functions.

Interoperable solutions for this broad problem space can be achieved only via standards. Interoperable solutions for this broad problem space can be achieved only via standards. The IETF Security Automation and Continuous Monitoring (SACM) Working Group has been working to properly scope the security automation problem. This includes identifying what posture information is critical to network security and standardizing how to collect and share that data with the evaluation tools and analytics that can use it to improve their ability to detect and respond to attacks. To make the broad scope of security automation standardization more manageable, it must be broken into a prioritized set of functional security automation tasks.

SACM has chosen vulnerability assessment as the first network security task to automate. The SACM Vulnerability Assessment Scenario2 describes how an enterprise can evaluate its susceptibility to an announced vulnerability. There are many reasons why vulnerability assessment is a good first choice for a security automation use case.

- It is a critical network security task— the rise of “named vulnerabilities”, such as Heartbleed and Shellshock, is indicative of that.
- Pursuing vulnerability assessment as the first automation use case has the added benefit that it forces us to address the fundamental problem of knowing what is on our network. It is impossible to assess a network’s vulnerability without knowing the composition of the network. Specifically, the evaluator needs to know what endpoints are on the network and what software they are running—knowledge supported by sound hardware and software asset management practices. Hardware and software asset management underpin vulnerability assessment, as well as configuration management, threat detection, malware analysis, and a host of other automatable network security functions.

Continued on next page
While it is obvious that network operators must continuously monitor hardware and software assets on the network, how this monitoring is architected is vitally important. To get this data to the evaluators that need it, it must be collected in a well-known, structured format. For the security of the endpoints that network operators are monitoring, the solution requires authenticated and encrypted protocols. Data must be provided as timely as possible when monitored information changes in order to eliminate periodic network scans that could be leveraged for an attack. For scalability, the solution must be flexible and lightweight. And, to support future security automation use cases, the solution must be extensible.

The IETF has standardized the Network Endpoint Assessment (NEA) architecture\(^2\), so a solution that meets these requirements already exists for client machines. Using the PT-TLS protocol\(^3\), any endpoint connected to the network can communicate posture information to a compliance server, including endpoint identity. SACM, building upon work from the Trusted Computing Working Group, has added to these protocols, and specified how to communicate software identification data over NEA in the Software Inventory Message and Attributes for PA-TNC (SWIMA) draft specification\(^4\).

SWIMA is an instantiation of an NEA collector that can monitor endpoint software inventory and push reports to a compliance server. Using SWIMA over PT-TLS enables collection of endpoint identity and software inventory in advance of a vulnerability being announced. It uses software identity (SWID) tags, an ISO/IEC standard, as a data model, enabling software vendors and owners to develop unique XML representations of a software’s identity. The compliance server can store this data for future reference in a data repository (Figure 1).

Some types of endpoints will not be able to support the client software required by NEA. Others, particularly network devices, already support endpoint type-specific protocols that are designed specifically for generating posture reports. It is impossible to have good network hygiene without posture reports from network devices. An IETF Mailing List, Posture Assessment through Network Information Collection (PANIC)\(^5\) is exploring solutions for network device posture collection, particularly YANG models that could provide the right information to network defenders about the posture of their network devices. These models, communicated over NETCONF and leveraging the draft YANG Push specification\(^6\), may help maintain an up-to-date view of the state of the network (Figure 2).

With a robust collection of endpoint software inventory data now available at the data repository, enterprise security tools with appropriate authorization can access and make use of this data. While the vulnerability assessment scenario focuses on using software inventory data for a very specific use case, it is easy to envision this data being valuable to any number of network security tools—asset management tools, behavioral analytics, and even threat detection tools can improve their outputs with access to accurate, up-to-date software inventory information.

Each of these evaluators will query the data repository for the data they require. To extend our vulnerability assessment example, a vulnerability evaluator will query the data repository for endpoints

![Figure 1. Precollection of Endpoint Software Inventory Information](image1)

![Figure 2. Precollection of Network Device Software Inventory](image2)
With a robust collection of endpoint software inventory data now available at the data repository, enterprise security tools with appropriate authorization can access and make use of this data.

![Figure 3. Evaluators Query the Data Store](image)

that have the vulnerable software installed, leveraging the hardware and software asset management data collected from the network endpoints. This data can be leveraged by other network evaluators, creating shared situational awareness of the network’s posture (Figure 3).

In addition to understanding network posture, enterprises need a shared situational awareness of current threats to the network. Situational awareness may take many forms, depending on the use case being addressed. For vulnerability assessment, the vulnerability evaluation tool must know what vulnerabilities it is searching for. The SACM Vulnerability Assessment draft defines a vulnerability data repository that can provide information on weaknesses that could compromise network security. This is a content repository that should be accessed by evaluators to help define the criteria against which they perform their evaluation. Such a content repository could be implemented using the IETF Managed Incident Lightweight Exchange (MILE) Resource Oriented Lightweight Information Exchange (ROLIE) draft specification. ROLIE builds off of ATOM Publishing Protocol to share software, vulnerability, cyber threat intelligence, configuration checklist, and other security automation information in a scalable way. Vendors, security researchers, and network management personnel can stand up ROLIE repositories to ensure that their evaluators have the most up-to-date security information possible (Figure 4).

The SACM Working Group will demonstrate how the SWIMA, NEA, and ROLIE standards can meet the Vulnerability Assessment Scenario requirements at the Hackathon prior to IETF 99. We invite interested parties to join us on the SACM mailing list. Those interested in security automation for network equipment are welcome on the PANIC mailing list, and those interested in content repository work are welcome on the MILE mailing list.

**Footnotes**

EDUCATION AND MENTORING DIRECTORATE ESTABLISHED

By Karen O’Donoghue

The IETF is a large, diverse organization with an extensive body of technical work, a unique culture, and an amazing collection of tools and information designed to support a globally distributed community that connects both in-person and, increasingly, remotely. Our broad base of membership and vast content areas present a variety of challenges, including disseminating the right information to the right people at the right time, and, specifically for newcomers, obtaining the information they need to comfortably and effectively enter and contribute to the community. To help address these challenges and create better coordination across the organization’s many ongoing activities, we formed the Education and Mentoring Directorate. This article shares an overview of current directorate activities and includes a call for volunteers to help with its projects.

Introduction to the Directorate

The Education and Mentoring Directorate was created with the following three primary goals:

- Enhance the productivity of IETF work.
- Expand diversity and inclusiveness of the IETF.
- Enable the IETF to facilitate technical development and innovation in the Internet.

In support of these goals, the directorate will structure and guide the development of educational activities and associated materials to be more accessible, relevant, reusable, and broadly understandable. The directorate will also help the mentoring activities establish relationships among participants that enable productive participation in the IETF. The directorate will help coordinate IETF-related outreach activities and ensure that related activities are sufficiently aligned and have the necessary education and mentoring programme support. Finally, the directorate will work on improved metrics and measurements for assessing the effectiveness of directorate activities.

The directorate serves the General (GEN) area in IETF. Participants include the IESG liaison to educational activities, the IETF chair, the IETF executive director, liaisons to the Tools team and ISOC outreach programmes, and the project leaders of education, mentoring, and outreach coordination projects. The plan is that the directorate itself will focus on coordination and lightweight project management, and the individual projects will have larger teams of volunteers for the execution of the projects.

Directorate projects cover the three areas of education, mentoring, and outreach and include two cross-cutting initiatives: metrics and analysis, and improvement of the newcomer experience.

Directorate Projects

Directorate projects cover the three areas of education, mentoring, and outreach and include two cross-cutting initiatives: metrics and analysis, and improvement of the newcomer experience.

Education projects provide training materials for both newcomers and long-time IETF participants, including Sunday tutorials, online materials, and the Working Group Chairs Forum. In addition, this area includes projects that explore ways to enhance the online accessibility of education materials.

There are also a number of projects related to mentoring and newcomer outreach, all targeted at helping IETF newcomers quickly integrate into the community. For example, the IETF runs a full mentor programme that matches mentors with mentees based on desired outcomes and interests, plus speed mentoring and a newcomer’s dinner are offered.

There also are activities that support the building of physical communities beyond IETF meetings. Examples include individuals gathering together to remotely participate in an IETF meeting and local IETF participants gathering outside an IETF meeting for further collaboration.

Cross-cutting the three project areas are two efforts designed to help monitor and evaluate the efficiency and effectiveness of these projects. The first explores ways to improve the newcomer experience across the IETF, and includes the website, training, registration, interaction with Working Groups, and so forth. Primary questions that this project is addressing include: What do newcomers need to become effective contributors? and What can the IETF community do to meet these needs?

The second effort is tasked with identifying metrics and monitoring the effectiveness of all these programmes. Resources are valuable—we must focus first on those projects that offer the biggest benefit from the resources available.

For more information about the directorate projects, please see our wiki.

How You Can Help

There are many opportunities for IETF members to contribute to the directorate:
• Your expertise in technical training can be used to improve our online materials.
• Your expertise in metrics and survey design approaches can be used to help us evaluate the effectiveness of our programmes.
• If you are working on a new and exciting technology, you could share your work with a broader audience in a one-hour Sunday tutorial. Examples include the DNS Privacy tutorial2 and the QUIC tutorial3.
• If you are a relatively new participant to the IETF (in the last two years), you could provide feedback on how well the IETF programmes addressed your needs.
• If you are a remote participant, individually or via a remote hub, your feedback and collaboration could help us improve those experiences.
• If you are a seasoned IETF participant, you could offer guidance to newcomers via either the regular mentoring or speed mentoring programme.
• If you are frustrated by the difficulty of finding what you need on IETF platforms (e.g., website, datatracker, tools), you could help us review and reorganize these materials.

To offer comments or suggestions, or to volunteer, please send email to the directorate mailing list (emo-dir@ietf.org) or approach any of the directorate members in the hallway at IETF 99. More information on the directorate can be found on the IETF website4 and the directorate wiki.

Footnotes

THE INTERNET SOCIETY’S IETF POLICY PROGRAMME

By Ryan Polk

The Internet Society looks forward to hosting its 16th IETF Policy Programme at IETF 99 in Prague. The programme introduces Internet policymakers to the IETF and the Internet standards-making process. During an intensive week, policy guests attend Working Group meetings, as well as sessions led by IETF experts on technical topics such as routing, Internet Protocol (IP) addressing, and the Domain Name System (DNS).

In many ways, the programme acts as a “crash course” on how the Internet works, its history, and how it continues to evolve through the work of the IETF. Policymakers are exposed to comprehensive and interactive presentations from IETF experts, who can offer policymakers the kind of technical foundations they need to effectively make policy decisions.

Over the course of 15 meetings, the programme has brought to the IETF 189 policymakers from 93 countries and territories. In this way, the programme also aids in the diversification of our standards body—policy guests recognise the benefits of their region’s technical experts contributing their expertise and perspectives to the IETF. A common concern among participants by the end of the programme is how to get more engineers from their countries involved in the work of the IETF, whether by attending the in-person meetings or contributing on the mailing lists.

Promoting participation from a new generation of global technical experts is critical for the IETF’s long-term success. By garnering greater support from policymakers and helping drive greater participation around the world, the IETF Policy Programme is another way the Internet Society contributes to the continued success of the IETF.

[T]he programme has brought to the IETF 189 policymakers from 93 countries and territories.

Participants of the Internet Society’s IETF Policy Guest Programme at IETF 98.
IETF 98 HACKATHON IMPROVES THE INTERNET THROUGH RUNNING CODE


The Internet Engineering Task Force (IETF) Blew into Chicago for IETF 98 on 25-31 March. As has become customary, the week-long meeting kicked off the weekend prior with the IETF Hackathon, a key element of the IETF’s approach to combine running code and open source software with the specification of new and evolving Internet standards.

IETF Hackathons are free and open to everyone. Its stated goals are to:

• Advance the pace and relevance of IETF standards activities by bringing the speed and collaborative spirit of open source development into the IETF.
• Bring developers and young people into IETF and get them exposed to and interested in IETF.

Attending the IETF meeting the following week is encouraged, but optional. One of the ways the Hackathon meets its first goal is by encouraging participants to share what they gained during the Hackathon with the larger IETF community, both by presenting their results during Working Group sessions and by demonstrating their work at the Bits-N-Bites reception.

The Chicago Hackathon saw more than 115 people collaborate on code with colleagues from various companies, standards organizations, open source communities, and universities. For about a third of the participants, this was their first IETF Hackathon. For about a dozen, this was their first experience with the IETF.

We had roughly 15 projects, each led by volunteers called champions. Projects were shared in advance via the Hackathon wiki, and when the doors opened at 8am Saturday, champions posted signs by their tables to help potential contributors locate the teams they wished to join.

Despite jet lag from travel and the early start, teams worked late into the night Saturday, even after the last remnants of dinner were cleared and the last beer was consumed. On Sunday, folks again started early by ironing out bugs and coding up additional functionality until the project presentations started at 2pm. Each team had four minutes to share what they had done, what they had learned, and how they moved IETF work forward.

An esteemed set of judges from the IETF community listened and asked clarifying questions after each presentation. Winners were then announced in the spirit of friendly competition.

For about a third of the participants, this was their first IETF Hackathon. For about a dozen, this was their first experience with the IETF.

An esteemed set of judges from the IETF community listened and asked clarifying questions after each presentation. Winners were then announced in the spirit of friendly competition.
The (D)TLS team won Best Overall for their work on TLS 1.3 and the corresponding version of DTLS.

- **(D)TLS: Best Overall**, for their work on TLS 1.3 and the corresponding version of DTLS.
- **NETVC: Measure Twice Cut Once**, for a proof of concept that will guide future specifications.
- **CAPPORT: Best Kickstart**, for a project that kicked new energy into a Working Group that had stalled.
- **WebRTC PSAP: Best Students**, for a new project from professors and students at the Illinois Institute of Technology.
- **LoRaWAN: Best Newcomers**, for a project that benefited from significant contribution from first-time IETFers.
- **AMT-Multicast: Most Remote Participant**, with a team member participating remotely from Mauritius.

Another noteworthy team was the I2NSF team, which [...] traveled to Chicago to continue its award-winning project from last year’s IETF 97 Hackathon in Seoul.

Four teams took advantage of the opportunity to share their work at Bits-N-Bites: AMT/Multicast, CAPPORT, (D)TLS, and WebRTC PSAP.

Special thanks to Hackathon sponsors, Ericsson and Mozilla; and thanks to my employer, Cisco DevNet, for supporting my efforts to organize the Hackathons and providing t-shirts for all participants—including for the first time ever, women’s sizes!

Last, but certainly not least, thanks to Alissa Cooper and Jari Arkko, the incoming and outgoing IETF chairs, who are both big supporters of the Hackathon and who have been instrumental in bringing it to the IETF.
WORKING TOGETHER:
THE IETF AND 3GPP ON 5G

Adapted from a post by Alissa Cooper in the IETF Blog on 12 June 2017.

In June 2017, IETF CHAIR ALISSA COOPER PARTICIPATED AT THE 3GPP PLENARY meeting in West Palm Beach, Florida, USA. At the invitation of Georg Mayer, the 3GPP liaison to the IETF, she both attended meetings of 3GPP’s radio access network and system architecture groups, and kicked off the organization’s new Wednesday Speaker Club series with a discussion of how 3GPP and the IETF can cooperate on 5G standardization.

The push towards the next generation of wireless networking technology has been gaining attention and spurring new work across the industry, standards developing organizations (SDOs), and open source projects. 3GPP participants are investing tremendous effort to define and prioritize 5G requirements to help bring this technology to fruition. They are also working against very tight timelines—the initial set of 5G standards is due to be completed by June 2018. It is therefore both timely and important to identify whether dependencies between 5G and IETF work exist, as well as to identify mechanisms to ensure smooth collaboration.

The IETF and 3GPP have a long history of working together and many successes to build on, including experiences with SIP/IMS, EAP-AKA, and Diameter. Because 5G encompasses a broader swath of individuals than those who have been involved in previous joint efforts, Cooper spent part of her time at the meeting sharing how the IETF works, examples of the IETF’s focus on broadly deployable Internet technology, and what the organization works on. She highlighted areas of existing IETF work that may be relevant in the 5G context, including work on data models, service chaining, deterministic networking, and QUIC. She also engaged with 3GPP participants around specific strategies to help the two organizations collaborate.

The Speaker Club Q&A focused on the potential and practicalities of improving collaboration. Topics included the following:

- The need for technical experts from each group to engage directly with each other (in addition to the existing liaison managers working in both directions).
- Opportunities to provide more introductory presentations in both directions, so people not familiar with 5G or specific IETF work can learn more.
- Ways to identify potential 5G requirements that may yield IETF protocol dependencies early on, even if later analysis in 3GPP reduces the urgency of the need for IETF protocol work.

IETF 99 is an opportunity to gain more clarity about specific dependencies that the IETF can expect between the 5G plans and IETF work—there is a slot on the agenda to discuss some of the network slicing work motivated by 5G, in addition to potential hallway conversations and ad hoc discussions. If you’re working on aspects of 5G not covered in the BoF proposals and looking for guidance or input about overlaps with IETF work, please contact the IETF liaison to 3GPP, Gonzalo Camarillo (gonzalo.camarillo@ericsson.com).

Footnote

1. See slides from Cooper’s presentation at https://www.ietf.org/blog/2017/06/working-together-with-3gpp-on-5g/.
APPLIED NETWORKING RESEARCH PRIZE WINNERS ANNOUNCED

By Mat Ford

The Applied Networking Research Prize (ANRP) is awarded for recent results in applied networking research that are relevant for transitioning into shipping Internet products and related standardization efforts. The ANRP awards presented during IETF 98 went to the following two individuals:

- **Yossi Gilad** for the path-end validation extension to the Resource Public Key Infrastructure (RPKI). See the full paper at https://dl.acm.org/ft_gateway.cfm?id=2934883.
- **Alistair King** for a framework to enable efficient processing of large amounts of distributed and/or live Border Gateway Protocol (BGP) data. See the full paper at https://dl.acm.org/citation.cfm?id=2987482.


ANRP winners have been selected for all of the IETF meetings in 2017. The following winners will be next to present their work at the IETF 99 meeting in Prague:

- **Stephen Checkoway**, an assistant professor in the department of computer science at the University of Illinois, Chicago. Checkoway will present a systematic analysis of the Juniper dual elliptic curve (EC) incident.
- **Philipp Richter**, a doctoral student in the INET group at the Technical University of Berlin. Richter will present a multiperspective analysis of carrier-grade network address translator (NAT) deployment.

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

From the IRTF Report presented 27 March, 2017 at the IETF 98 Plenary

IETF 98 IN CHICAGO MARKED THE FIRST MEETING WITH NEWLY APPOINTED Chair Allison Mankin. During the meeting, seven chartered IRTF RGs held meetings:

- Human Rights Protocol Considerations (HRPC)
- Internet Congestion Control (ICCRG)
- Information-Centric Networking (ICN RG)
- Measurement and Analysis for Protocols (MAPRG)
- Network Function Virtualization (NFVRG)
- Network Management (NMRG)
- Thing-to-Thing (T2TRG)

The following two RGs recently concluded: Software-Defined Networking (SDNRG) and the Network Machine Learning (NMLRG) provisional group.

The IRTF Open Meeting received Applied Networking Research Prize presentations from Yossi Gilad for the path-end validation extension to the Resource Public Key Infrastructure (RPKI), and Alistair King for a framework to enable efficient processing of large amounts of distributed and/or live Border Gateway Protocol (BGP) data.

The Applied Networking Research Workshop 2017 call for papers has closed. The ANRW’17 is an academic workshop that provides a forum for researchers, vendors, network operators, and the Internet standards community to present and discuss emerging results in applied networking research. Sponsored by ACM SIGCOMM, the Internet Research Task Force (IRTF) and the Internet Society (ISOC), the workshop will take place Saturday, 15 July 2017, in Prague, Czech Republic, the venue of IETF 99.
I first got involved with the IETF when I started my PhD. A colleague, who was already involved with the organization, pointed out that it was starting work closely related to my own interests. I attended my first IETF meeting in 2010, when the CONEX [Congestion Exposure] Working Group (WG) held a BoF meeting. From then on, my own initiative kept me working with the IETF—I had support from my group, and they usually had enough travel budget for me to attend the meetings.

Three years ago, I became chair of the RMCAT [RTP Media Congestion Avoidance Techniques] Working Group. I gave that up when I became Transport area director (AD). I also was chair of the TCPINt Working Group for half a year. So I became an AD just six years after joining the IETF.

A limited number of people are involved in the Transport area. When I became more active, I was encouraged to take the role of a Working Group chair. Transport AD wasn’t an option until I finished my PhD. Ultimately, it worked out nicely because I got stable funding for a project for a little more than two years, which freed me up to consider the job. The project is funded by Switzerland and includes proposed work that we plan to bring into the IETF. So it helped me justify spending so much time on IETF work. My two-year term as Transport AD began in March 2016.

I hope that my experience as AD can count as management experience and that people value it. It’s a good way to improve your skills because you are in a management position where you don’t have any power, but you need to motivate people. For me, it is about how well I manage Working Groups and how well I manage my time. I spend 40% of my time on my AD work and 60% on my research project. It can be a challenge to balance them.

I don’t think that ETH directly benefits from me being Transport AD. But they did get external funding for our project, and that funding had a strong focus on making an impact on industry. So my standardization work may have helped to get the project funded. I don’t think I needed a leadership role for that. Being a Working Group chair was probably enough to show that I had IETF experience.

Everybody’s biggest concern about taking on an IETF leadership role is time management. I do it on a 40% basis. It’s a little stressful, yes, but it is possible. The other reason it’s hard to find people for the Transport AD role is that the right person not only needs support, money, and time for the IETF, but also must have an overview about what’s going on in Transport. I was in the unique position that I was following the same Working Groups that I now carry as AD—it’s no extra effort.

I don’t have a plan yet for when my term is over, but I know I’d like to stay involved in the IETF. When my ETH project is finished, I’ll be a four-year post doc. I’ll need to make a decision about whether to stay in academics or go into industry. If I apply for a job next year, I won’t stand as Transport AD—I can’t ask a new employer to let me spend 40% of my time on the IETF. Even as a professor, it would be hard for me to get 40% of my time off for the IETF.

It’s been an interesting experience, particularly because I’m just starting my career. I’ve learned a lot, and I’ve made a lot of industry contacts that I’ve gotten to know well. I’m grateful—the IETF as a community has provided me with networking opportunities and a source of ideas for research.

I’m grateful—the IETF as a community has provided me with networking opportunities and a source of ideas for research.
IETF ORNITHOLOGY: RECENT SIGHTINGS

Compiled by Mat Ford

GETTING NEW WORK STARTED IN THE IETF USUALLY REQUIRES A BIRDS-of-a-feather (BoF) meeting to discuss goals for the work, the suitability of the IETF as a venue for pursuing the work, and the level of interest in and support for the work. In this article, we review the BoFs that took place during IETF 98, including their intentions and outcomes. If you’re inspired to arrange a BoF meeting, please read RFC 5434, “Considerations for Having a Successful Birds-of-a-Feather (BoF) Session”.

Coordinated Address Space Management (casm)

Description: Organizations use IP address space management (IPAM) tools to manage their IP address space, often with proprietary databases and interfaces. This proposed work is intended to evolve IPAM into standardized interfaces for coordinated management of IP addresses, including software-defined networks and other forms of virtualization. Use cases include dynamic allocation and release of IP addresses and prefixes based on usage and/or user intent. The purpose of the BoF was to gather a common set of requirements from a larger set of operators and to better understand use cases.

Proceedings: Slides, documents, and audio and video recordings are available online (https://datatracker.ietf.org/meeting/98/proceedings, search for “casm”).

Outcome: There was discussion of IPAM services and use cases. The meeting concluded with discussion of whether the IETF should take on this work in the future. There was agreement that there was a problem for the IETF to solve and interest from diverse stakeholders in working on a solution. Further work to refine the problem and scope will take place on the mailing list (https://www.ietf.org/mailman/listinfo/casm).

WGs Using GitHub (wugh)

Description: GitHub is being used by more IETF Working Groups for proposing and tracking changes to WG Internet-Drafts. Using GitHub for normal WG processes requires some training, and edge cases in its usage abound. There are also questions of how to capture information that is created in GitHub into WG mailing lists so it can be both seen by all participants and properly archived. This BoF was also used to discuss the creation of IETF-wide documentation about how to use GitHub effectively in WG processes.

Using GitHub for normal WG processes requires some training, and edge cases in its usage abound. There are also questions of how to capture information that is created in GitHub into WG mailing lists so it can be both seen by all participants and properly archived.

Outcome: A good discussion of the ways in which GitHub is being used by various IETF Working Groups and IRTF Research Groups. Several issues were identified and more work will be required to document best practices and better integrate use of GitHub with IETF processes. The discussion will continue on the mailing list (https://www.ietf.org/mailman/listinfo/ietf-and-github).

A Protocol for Dynamic Trusted Execution Environment Enablement (teep)

Description: The goal of this group is to standardize a protocol for dynamic trusted execution environment enablement. The industry has been working on an application layer security protocol that allows configuration of security credentials and software running in a Trusted Execution Environment (TEE). Today, TEEs are found in home routers, set-top boxes, smart phones, tablets, wearable devices, and so forth. To date, mostly proprietary protocols are used in these environments. This BoF was an attempt to start work on standardizing such a protocol. A straw man proposal has been published at https://tools.ietf.org/html/draft-pei-opentrustprotocol-03.

The industry has been working on an application layer security protocol that allows configuration of security credentials and software running in a Trusted Execution Environment (TEE).


Outcome: There was an overview presentation on TEEs, presentations from ARM and Intel about their product offerings and presentations on use-cases and possible architectures. The meeting concluded by identifying a number of people willing to volunteer to continue participating in the work to better define the problem and proposed work items. Discussion will continue on the mailing list (https://www.ietf.org/mailman/listinfo/teep).

IASA 2.0 (iasa20)

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


Outcome: A robust discussion about the challenges facing the current administrative structure and arrangements, and an opportunity for those present to express their views and concerns vis-à-vis some of the alternative approaches to reform. Discussion will continue on the mailing list (https://www.ietf.org/mailman/listinfo/iasa20).
IETF 98 AT–A–GLANCE

Onsite participants: 1127
Remote participants: 315
Number of countries: 57
Hackathon participants: 115+

IETF Activity since IETF 97 (16 November–26 March 2017)

New WGs: 2
- Concise Binary Object Representation Maintenance and Extensions (cbor)
- JSON Mail Access Protocol (jmap)

WG closed: 10
WG currently chartered: 138

New and revised Internet-Drafts (I-Ds): 1,484
IESG Protocol and Document Actions: 124
IESG Last Calls issued to the IETF: 130

RFCs published: 116
- 66 Standards Track, 5 BCP, 9 Experimental, 36 Informational

Notable process updates

RFC Editor Activity since IETF 97 (November–March 2017)

Published RFCs: 126 (3,928 pages)
- 37% increase in page count since last reported
- 29% increase in document count since last reported

Cluster AUTH48 pages updates (full view of author approvals on one page)

Server upgrades

Current and ongoing activities:
- Stable URIs for errata
- xml2rfc v3: Continue to follow format developments and be ready to test tools and draft test procedures
- Improving cluster management and transparency

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

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

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

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

<table>
<thead>
<tr>
<th>IETF 100</th>
<th>Date</th>
<th>12–17 November 2017</th>
</tr>
</thead>
<tbody>
<tr>
<td>Host</td>
<td>Cisco Systems</td>
<td></td>
</tr>
<tr>
<td>Location</td>
<td>Singapore</td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>IETF 101</th>
<th>Date</th>
<th>18–23 March 2018</th>
</tr>
</thead>
<tbody>
<tr>
<td>Host</td>
<td>TBD</td>
<td></td>
</tr>
<tr>
<td>Location</td>
<td>London, UK</td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>IETF 102</th>
<th>Date</th>
<th>22–27 July 2018</th>
</tr>
</thead>
<tbody>
<tr>
<td>Host</td>
<td>Juniper Networks</td>
<td></td>
</tr>
<tr>
<td>Location</td>
<td>San Francisco, CA, USA</td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>IETF 103</th>
<th>Date</th>
<th>4–9 November 2018</th>
</tr>
</thead>
<tbody>
<tr>
<td>Host</td>
<td>TBD</td>
<td></td>
</tr>
<tr>
<td>Location</td>
<td>TBD</td>
<td></td>
</tr>
</tbody>
</table>

---

Special thanks for hosting IETF 98

---

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

[Logos of sponsors]

---

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

[Logos of sponsors]