Low-power Networks, High-capacity Cables, and the DNS after DNSSEC

From the Editor’s Desk, by Arno Meulenkamp

In the early days of the Internet it was a marvel to see a message sent from someone in another part of the world. We learned that we could communicate with people anywhere, even if they were not at their desks. Today, we have more diverse devices connecting to the Internet and in sensor networks, and we have devices communicating with other devices.

In this issue of the IETF Journal, Carsten Bormann, JP Vasseur, and Zack Shelby describe the aspects of this phenomenon that are being worked on in their article, “The Internet of Things” (this page). Samita Chakrabarti goes into a bit more detail on how IPv6 Neighbor Discovery can be optimized in these types of low-power networks in her article on page 12.

Even as we look at new types of networking activities, we should not lose sight of the need to maintain and expand basic network infrastructure. Kevin Chege illustrates how extra capacity can change the way people can use the Internet in his article, “Impact of New Undersea Capacity on KENET and East Africa” (page 16).

There is, however, a lot more work in different parts of the stack. At IETF 78, not only was there a celebration of the DNSSEC signing of the DNS root zone, an Internet Society-organized panel explored how the DNS is likely to evolve now that DNSSEC is here (see page 8).

To round out this issue we take a look at how to best streamline the standards process (page 7), we get introduced to the Internet Society Fellows who attended IETF 78 (page 10), and we honor Jianping Wu, recipient of the 2010 Jonathan B. Postel Service Award (page 9).

Many thanks to all of our contributors. We invite you to send comments and suggestions for future issues to ietfjournal@isoc.org.

The Internet of Things

By Carsten Bormann, JP Vasseur, and Zack Shelby

Over the past decade, we’ve come to think of personal computers, laptops, and mobile phones not just as computing devices but as communications systems as well. The next frontier in the evolution of the Internet will be the ability to connect more than just computers and communications devices; that next step will involve connecting smart objects.

Imagine the energy savings that could be realized by connecting energy-consuming objects such as dishwashers and washing machines to an energy-producing smart grid. Imagine further the energy-consumption savings and the cost benefits if HVAC (heating, ventilating, and air-conditioning)
Message from the IETF Chair

By Russ Housley

The work of the IETF remains relevant and energetic!

IETF 78 was held in Maastricht, Netherlands. It was a very successful meeting, attended by 1,153 people from 53 different countries. While many attendees experienced travel difficulties, once they arrived everyone worked enthusiastically on their IETF activities. Significant progress was made by many working groups (WGs), and it was a genuine pleasure to see so many talented and engaged people collaborating.

SIDN, which served as a very accommodating host, coordinated with eight sponsors to provide an effective meeting venue. In addition, Gemeente Maastricht, the Ministry of Economic Affairs, and Provincie Limburg worked with SIDN to create a wonderful social event on the waterfront, and SURFnet sponsored the network connectivity.

Since IETF 77, six new WGs have been chartered and three WGs were closed. There are 122 chartered WGs. Between meetings, the WGs and their individual contributors produced 467 new Internet-Drafts and updated 1,069 existing Internet-Drafts, some of the drafts more than once. The Internet Engineering Steering Group (IESG) approved 106 Internet-Drafts for publication as RFCs. The RFC Editor published 120 new RFCs.

During the plenary session on Wednesday evening, the IETF celebrated the signing of the Domain Name System Security Extensions (DNSSEC) root. The root zone is signed, as are the .org, the ietf.org, and the iab.org domains. While the names of all of the people who contributed to the DNSSEC effort scrolled on the screen, wine was passed around at the plenary session, and we toasted the universal deployment of DNSSEC.

Let’s all work toward the same milestone for IPv6 deployment soon. I’m looking forward to a similar toast at a future plenary.

A new nominations committee (NomCom) has been seated, and the members are working to select the leaders who will begin their terms at the March 2011 IETF meeting. Please help the NomCom identify great leaders for the community.

IETF 79 will take place Beijing on 7–12 November 2010 and will be hosted by Tsinghua University. Scheduling information for upcoming IETF meetings can be found, as always, at http://www.ietf.org/meetings/meetings.html. I look forward to seeing you in Beijing.

Russ Housley, IETF Chair

Recent IESG Document and Protocol Actions

A full list of recent IESG Document and Protocol Actions can be found at http://www.isoc.org/ietfjournal/DocProtoActions0602.shtml
Words from the IAB Chair

By Olaf Kolkman

In the last issue of The IETF Journal, I told you that the Internet Architecture Board (IAB) would have its retreat in June 2010, and so it did. We met on the campus of Harvard University in Cambridge, Massachusetts, where we enjoyed the facilities made available to us by Scott Bradner.

At this year’s retreat, our focus was on establishing methods that would enable us to identify and organize work items in ways that will lead to greater effectiveness in terms of prioritization, communication, and delivery.

IAB work items can be divided roughly into four major categories:

- Long-term interests
- Short-term working items (initiatives)
- Long-term working items (programmes)
- Activity plan

Long-Term Interests

Traditionally, the IAB has taken an interest in a number of architectural areas. Among them, in no particular order, are:

- IPv6 and its adoption and transitional coexistence with IPv4 given the realities of an IPv4-dominated Internet
- Domain Name System health and security
- Web security
- The realities of maintaining the end-to-end and layered architectures
- Prevention of unwanted traffic
- The security and stability of the routing system
- Internationalization of the Internet and balance with localization and retention of a global network

Short-Term Working Items (initiatives)

To some of those items the IAB may consider committing short-term efforts—ones in which an activity is expected to be completed in less than one tenure of an IAB member. We call such activities initiatives. The outcomes of initiatives usually are the results of guidance provided in the form of IAB Stream RFCs, statements, or working group/plenary presentations.

Long-Term Working Items (programmes)

Other items may require longer-term perspective, and the results may involve a variety of activities and deliverables. They may also involve separate activities, such as scoping the work (in the form of birds of a feather, presentations, and position papers), advancing the work, or stimulating the charter development of new work within the IETF. In some cases, work in these areas may involve some form of collaboration with other organizations.

Continued on page 6
systems, lights, windows and window shades and blinds, doors, and locks could talk both to each other and to controller systems as a matter of routine.

What is the Internet of Things? While much has been written that describes IP (Internet Protocol) smart-object networks in great detail, simply put, the Internet of Things refers to the interconnection of IP smart objects, such as sensors and actuators. Such devices have been used in the industry for decades, usually in the form of non-IP/proprietary protocols that are connected to IP networks by way of protocol translation gateways. With the emergence of a myriad of applications, such as Smart Grid, Smart Cities, building and industrial automation, as the smart grid, smart cities, and building and industrial automation, and cars that interconnect millions of objects for sensing things like power quality, tire pressure, and temperature and that can actuate engines and lights, it quickly became of the utmost importance to extend the IP protocol suite for these networks.

To that end, the IETF has formed (as of this writing) three working groups (WGs) that define an adaptation layer (6LoWPAN), routing (ROLL), and a resource-oriented application protocol (CoRE). The activities of these WGs are described briefly in this article.

**IP Smart-Object Networks (the Internet of Things) and the IETF**

**The 6LoWPAN Working Group**

One particular IP smart-object network has been standardized as IEEE 802.15.4. It was initially popularized by the Zigbee family of vertical specifications. This low-power radio is designed to deliver 20 to 256 kilobits per second (less on 900 megahertz [MHz], more on 2.4 gigahertz) with about a milliwatt of transmission power.

The MAC (medium access control) layer provides only a small packet size of 127 bytes, which requires an adaptation layer with fragmentation and reassembly to enable Internet-style maximum transmission units. As a result, the so-called IP over foo specification (RFC 4944) is more complicated than, for example, that for Ethernet. The 6LoWPAN (IPv6 over Low-Power Wireless Personal Area Networks [WPANs]) WG, initially chartered to create that specification, went on to provide two critical performance improvements: 6LoWPAN-HC and 6LoWPAN-ND.

Due to the number of nodes that will be on constrained node/networks, only IPv6 provides enough addresses, but IPv6's large headers would fill almost half of a MAC layer packet and therefore require good header compression (HC). RFC 4944 provides a simple, stateless form of header compression, but it does not compress globally prefixed addresses well. Unfortunately, the existing HC family of specifications created in the Robust Header Compression (ROHC) working group is too expensive for 6LoWPAN, as it is based on per-flow state, which would be prohibitive for a constrained node.

The solution in 6LoWPAN-HC [draft-ietf-6lowpan-hc] is simple (mostly static) networkwide state in the form of /context/, which can be distributed, for example, via IPv6’s neighbour discovery (ND) protocol.

6LoWPAN-ND [draft-ietf-6lowpan-nd] uses the RFC 5889 IP addressing model with off-link hosts, thereby limiting the need for multicast to inexpensive radio-range transmissions. Hosts can /register/ to their routers, allowing these to redistribute host addresses in the routing protocol. 6LoWPAN-ND also contains support for distributing 6LoWPAN-HC’s context. As of this writing, 6LoWPAN-ND is in WG last-call.

**The Routing Over Low power and Lossy networks (ROLL) Working Group**

The IETF has considerable experience in routing in IP networks and it has specified a number of routing protocols over the past two decades (such as RIP, OSPF, BGP, and IP for IS-IS), but routing in networks made of IP smart objects has unique characteristics. Indeed, not only are the devices constrained in terms of resources (such as process power, memory, and, potentially, energy); they also are usually...
interconnected by low-speed lossy links where the packet drop ratio may be quite high. Furthermore, some of those networks may be made of hundreds of thousands of nodes. This unique set of characteristics led to the formation in 2008 of a new working group called ROSS, whose objective is to specify an IPv6 routing solution for such IP smart-object networks.

After one year of detailed requirements analysis and a survey of the existing IP routing protocols specified at IETF 78, the WG concluded that none of the existing protocols would meet the set of requirements. Thus, the ROLL WG was rechartered to specify a new routing protocol, called RPL (Routing Protocol for LLNs). RPL is a distance-vector routing protocol that supports the formation of directed acyclic graphs (DAGs) according to a user-defined objective function using a set of link/node routing metrics/constraints. RPL supports the notion of multitopology routing (where the DAG is specified in a newly defined IPv6 hop-by-hop header) and has been designed to make efficient use of limited resources in the network (such as using Trickle timer and supporting local repair complemented with global repairs).

RPL supports two modes of operation known as storing and nonstoring. In storing mode, each node in the network stores a routing table. Traffic between two nodes travels along the DAG in an upward direction to a common ancestor, at which point packets are redirected to their destination. In the nonstoring mode, no routing tables are stored; packets always travel up to the DAG root, where routes are stored and the root redirects the traffic to its destination by using source routing.

RPL has currently passed WG and IETF Last Call and is under IESG review. More than a dozen implementations exist as of this writing, and two interoperability tests have been performed by the IPSO (www.ipso-alliance.org) and Zigbee-IP alliances.

**Constrained RESTful Environments**

In spring 2010, the IETF started a new working group called Constrained RESTful Environments (CoRE). The aim of this WG is to extend the Web architecture to even the most constrained networks and embedded devices. Machine-to-machine applications—such as smart energy, building automation, and asset management—will benefit tremendously from the use of Internet technology and from integration with the Internet of Things. In particular, the Web architecture will be important in scaling large-scale, machine-to-machine applications. Today’s Web protocols work well between Web servers and Web clients running on PCs and handheld computing devices. However, constrained Low-power and Lossy networks often mean high packet loss (5 to 10 percent is common), frequent topology changes, low throughput (10–20 kilobits per second is common), and useful payload sizes that are often less than 100 bytes. Embedded devices typically depend on cheap embedded microcontrollers with processors running at several MHz and limited RAM and ROM. In addition, the interaction patterns in machine-to-machine applications are different, often requiring multicast support, asynchronous transactions, and push rather than pull. The CoRE WG has been chartered to develop a new Web transfer protocol and appropriate security setups for these machine-to-machine applications over constrained networks and nodes.

The WG is now completing work on the Constrained Application Protocol (CoAP) [draft-ietf-core-coap-02], which is on schedule for completion at the end of 2010. At IETF 78, a successful PlugFest of CoAP was held with more than 10 implementations of the protocol. Security is another important subject for CoRE, which is also working on security bootstrapping techniques for these environments.

**Perspectives**

Enormous progress has been made at the IETF over the past few years in specifying new IPv6 protocols that connect IP smart objects to private IP networks or the public Internet, thus facilitating a myriad of new applications. Still, there’s no doubt that new work will further enrich the IPv6 protocol suites for these devices—and transport, security, and management for this new wave of the Internet: the Internet of Things.

**References**

These types of work are organized in the form of programmes. They can be thought of as IAB directorates, small task forces, or ad hoc bodies of (independent) technical experts (see RFC 2850 Section 2.1). Programmes are managed by the IAB, but the actual work may require the IAB to form a team with specific expertise that may not be available within the IAB.

The structuring of the work in this way has several objectives:

- To minimize dependency on the current IAB composition and the specific expertises and competencies of the IAB’s members
- To minimize dependency on the tenure of IAB members;
- To increase bandwidth by shifting IAB members’ responsibilities from doing the actual work to organizing and delegating work and providing guidance
- To shift the IAB’s focus from the specifics of an activity to the development of a vision of the Big Picture and the maintenance of that Big Picture
- To advance an IAB whose focus is on identifying areas of priority and carrying out respective efforts
- To improve visibility of the IAB’s activities and create opportunities for the community to offer feedback on content and priorities

In most cases, programme leaders will be IAB members. A leader’s objective will be to facilitate activities within the programme, provide oversight, and ensure continuity. The leader is not required to have specific expertise in the area but must possess a good general understanding of the issues from technical, business, and/or policy perspectives. Generally speaking, the programme leader is expected to bring the IAB perspective to the work. The IAB as a whole will periodically review the state of a programme, monitor its progress, make necessary adjustments, and set prioritizations.

Responsibilities

The IAB has a number of regular responsibilities that fall under the umbrella of periodic and recurring responsibilities. For example, in 2010-2011, the IAB will need to:

- Confirm the Internet Engineering Steering Group candidates (RFC 3777)
- Appoint a member of the ISOC Board of Trustees (RFC 3677)
- Appoint the Internet Research Task Force chair (RFC 2850)
- Appoint the Internet Corporation for Assigned Names and Numbers board liaison [ICANN Bylaws, Article VI, section 9, par. 1(f)]
- Handle any appeals

Activity Plan

Subject areas and related programmes are periodically reviewed by the IAB. Selected programmes and initiatives form an activity plan. We have published an overview of the 2010-2011 activity plan at [http://www.ietf.org/mail-archive/web/ietf/current/msg62743.html](http://www.ietf.org/mail-archive/web/ietf/current/msg62743.html) and will make the information available in a more comprehensive fashion on our website.
IETF Debates Streamlined Standards Process

By Carolyn Marsan

IETF chair Russ Housley’s proposal to streamline the Internet standards process dominated the discussion at the IETF 78 plenary session on Wednesday night. Russ proposed replacing the current three-step process—which includes Draft Standard, Proposed Standard, and Internet Standard—with a two-step process that includes only Proposed Standard and Internet Standard.

Driving his proposal is his view that the initial publication of Internet-Drafts takes too long because the drafts receive too much scrutiny. Instead, Russ proposes an environment where good-enough documents are published as soon as rough consensus has been achieved—plus it’s easier to revise such documents.

Between Proposed Standard and Internet Standard, Russ suggests only one requirement: proof of interoperability. He would remove the requirement for a six-month waiting period between when a document can transition from a Proposed Standard to an Internet Standard. Indeed, he suggests that some documents can go straight to Internet Standard if they include documentation of interoperability. In another change, Internet Standards would be allowed to reference Proposed Standards.

Russ’s proposal includes no changes to Informational RFCs. However, it would abandon the STD numbering system.

Attendees at the plenary session were split on the proposal. Bob Hinden said he liked the idea of getting the group back to focusing on running code. Ross Callon said he thought the proposal would improve the standards process, especially with downward references allowed.

Olafur Gudmundsson said he’s worried about the rapid advancement of complicated drafts straight to Internet Standard. Several attendees—including Bernard Aboba, John Klensin, and Thomas Narten—questioned whether Russ’s proposal would actually speed up the process of publishing standards.

Most of the plenary attendees were in favor of eliminating one step in the current three-step standardization process, but they did not agree with the idea of documents’ being able to go straight to Internet Standard.

In other IETF news, the Jonathan B. Postel Service Award was given to Prof. Jianping Wu of CERNET at the Tsinghua University in recognition of his work as a champion of Internet development and deployment in China.

The IETF plenary concluded with a champagne toast in recognition of the significant progress being made in the deployment of the Domain Name System Security Extensions (DNSSEC). More than 200 IETF participants who have contributed to the development of this standard during the past 17 years were recognized.

DNSSEC is currently deployed on ietf.org, iab.org, isoc.org, and icann.org and will be deployed soon on iana.org and the .arpa domain.

IETF 78 At–A–Glance

- Registered attendees: 1153
- Newcomers: 267
- Number of countries: 53
- New WGs: 6
- WGs closed: 3
- WG currently chartered: 122
- New Internet-Drafts: 467
- Updated Internet-Drafts: 1069
- IETF Last Calls: 115
- Internet-Drafts approved for publication: 106
- RFC Editor Actions (March–June 2010)
  - RFCs published: 142
  - I-Ds submitted for publication: 129
    - 93 IETF WGs
    - 31 IETF individuals
    - 5 IRTF, IAB, and independent combined
  - RFC Online: 30+ documents were put online
  - RFC repository rsync: “everything–ftp” now available
- IANA Actions (March–June 2010)
  - 1580+ IETF-related requests processed
  - 760 private enterprise numbers
  - 72 port numbers
  - 82 TRIP ITAD numbers
  - 23 language subtag requests
  - 17 media-type requests
- In addition, IANA:
  - Reviewed 134 I–Ds in Last Call
  - Reviewed 129 I–Ds in IESG Evaluation
  - Reviewed 128 I–Ds prior to becoming RFC and 79 contained actions for IANA
DNSSEC Doesn’t Mitigate All DNS Threats

By Carolyn Marsan

Even as deployment of Domain Name System Security Extensions (DNSSEC) is gaining momentum across the Internet, many threats to the DNS remain, according to a panel discussion sponsored by the Internet Society in conjunction with the IETF meeting in Maastricht, Netherlands, in July 2010.

Among the most serious of the threats is the amount of additional information that new protocols such as DNSSEC are pushing through the DNS as well as add-on functionality that Internet engineers want to append to the DNS now that the system is more secure.

The panelists—all of them DNS experts—expressed their pleasure about the summer 2010 deployment of DNSSEC on the root servers: top-level domains, such as .org, and country-code top-level domains, such as Sweden’s .se.

“With DNSSEC, we changed the maintenance on the engine of a plane in flight—and with no noticeable disruption,” said Danny McPherson, who leads VeriSign Labs’ research in network security and availability. He pointed out what a major accomplishment this was given that VeriSign alone handles up to 60 billion DNS queries in a single day.

“I’m also sort of impressed and surprised that we managed to add DNSSEC without any gaps so that there was nothing to write about. Nothing happened, and that’s a good thing,” said Patrik Fältström, a distinguished consulting engineer with Cisco Systems.

Despite the promise of DNSSEC, Danny pointed out, DNSSEC addresses only one aspect of information security for the DNS: integrity. He added that DNSSEC neither addresses the confidentiality of the information inside the DNS nor fixes availability issues.

All it takes is a user to have his password with his domain name registrar compromised for the DNS to be infiltrated—even with DNSSEC deployed from end to end. “If any piece of the DNS chain is compromised, everything else in the system is useless,” Danny said.

Patrik warned that Internet engineers might be trusting DNS too much these days, now that DNSSEC is being deployed. For example, they may want to store large blocks of data in the DNS or add new services that would be better off as separate services that point to the DNS, he argued. “The risk is that we’re trusting the data we get and we bootstrap and jump into other protocols and rely on the data to be absolutely 100 percent correct, when the reality with DNSSEC is that it solves only the integrity part of DNS,” Patrik said. “I’m a little nervous that DNSSEC makes it interesting to add a little too much to DNS.”

Barry Leiba, Internet standards manager at Huawei Technologies, said the reliability and ubiquity of DNS are the reasons Internet engineers have used them for add-on security protocols such as DKIM (DomainKeys Identified Mail), SPF (Sender Policy Framework), and Sender ID. “A lot of these protocols have the common goal of associating a domain securely with an e-mail message, and they have a common mechanism for putting that information in DNS,” Barry said. “I know there are companies that are concerned about whether the people who manage their DNS will get all of these other records right and what the change control will be. So there is an administrative issue. But from a deployment perspective, [DNS] has made things like SPF and DKIM very easy to deploy.”

Lars-Johan Liman, a senior systems specialist at Netnod/Autonomica, pointed out that the DNS is more complex than many Internet engineers realize and that many applications stop working if DNS stops working. “DNS is a small idea that has scaled fantastically,” Lars-Johan said. “It was well designed to carry lots of information, and it will continue to do so for a long time. But it poses a few restrictions on what you can do. DNS is a hierarchy; I’m a bit worried about shifting the name space and flattening it too much because that does lead to operational problems.”

Lars-Johan predicted that the Internet will need additional look-up mechanisms rather than relying on DNS alone to transfer bulk data. “DNS
will take us far, but it doesn’t cover all the needs we have,” he said.

Despite the deployment of DNSSEC, the DNS will remain a prime target for hackers because it enables so many applications, panelists warned. “The hierarchy and the massively distributed nature of DNS are one thing, but it’s still prone to systemic attacks,” Danny said, pointing out that the many safeguards that are in place won’t prevent surgical strikes such as localized DDoS (distributed denial of service) or IP (Internet Protocol) address-spoofing attacks.

“DNSSEC is a huge, huge benchmark for us, and I think it’s great,” Danny said. “But we’ve still got a long way to go to provide protection in the network layer of the infrastructure. Besides DNSSEC, network routing and network-layer security are top of mind for me.”

When the panelists were done speaking, audience members questioned those experts about whether it was time for the IETF to begin a DNS Next Generation working group. The panelists, however, were not in favor of a big project to rewrite DNS on a par with the creation of IPv6 to replace IPv4, because it has taken so long for that upgrade to occur.

“I have visions of smaller, nimbler DNS-like protocols that will do very specific things and help locate other services, possibly with a different hierarchy—or not,” Lars-Johan said. “I think we need to look at other types of services for retrieving data.”

---

2010 Postel Award Recognizes Internet Pioneer in China

Honouring a pioneer who advanced Internet technologies and information access for Chinese research and educational communities.

IETF 78 served as the backdrop for the 2010 Jonathan B. Postel Service Award. Chinese technologist Jianping Wu received the prestigious award for his pioneering role advancing Internet technology, deployment, and education in China and the rest of Asia Pacific over the past 20 years.

Dr. Wu’s best-known contribution is in the form of the China Education and Research Network (CERNET), which he designed and developed and which became the first Internet backbone network in China. Created to establish a nationwide advanced network infrastructure for the support of education and research among universities, CERNET has since become the world’s largest national academic network. Since 1998, Dr. Wu has devoted much of his time to the design and development of a large-scale native IPv6 backbone in China that now connects more than 200 universities and millions of users.

“Jianping Wu has dedicated his career in China to developing a broadly accessible Internet that brings people together,” said Internet Society president and CEO Lynn St. Amour. “Twenty years ago, Dr. Wu recognized the importance of the Internet and the pivotal role it would play in terms of its impact on social reform, technology advancement, and economic growth for China. He has worked tirelessly to bring his vision to life. As a result, the networks that sprang from his determination and hard work have played an important role in driving Internet development in China and have had a significant impact on the Internet worldwide.”

The Internet Society presented the award, including a USD 20,000 honorarium and a crystal engraved globe, to Dr. Wu during the IETF 78 plenary in Maastricht, Netherlands, in July 2010.

The Postel Award was established by the Internet Society to honour individuals or organizations that, like Jon Postel, have made outstanding contributions in service to the data communications community.
ISOC Fellows Get Inside View of Standards Work at IETF 78

Six information technology professionals from Africa, Asia, the Middle East, and South America attended their first IETF meeting in July 2010 in Maastricht, Netherlands, as part of the Internet Society’s Fellowship to the IETF Programme. Now in its fifth year, the programme, which operates under the aegis of ISOC’s Next Generation Leaders Programme, enables Internet technologists from developing regions to participate more fully in the IETF’s standards work by facilitating their attendance at an IETF meeting. Here’s what some of them are accomplishing in their home countries—and what they took away from their experience at IETF 78.

First-time Fellows

Fahd Batayneh (Jordan)
Mentor: Hugo Koji Kobayashi

Ernest Brown (Ghana)
Mentor: Samita Chakrabarti

Hassen Redwan Hussen (Ethiopia)
Mentor: Pascal Thubert

Humberto Silva Galiza de Freitas (Brazil)
Mentor: Eduardo Ascenco Reis

Sharon Yalov-Handzel (Israel)
Mentor: Al Morton

Bilal Zafar (Pakistan)
Mentor: Carsten Bormann

Returning Fellows

Alejandro Acosta (Venezuela)
Vinayak Hegde (India)
Subramanian Moonesamy (Mauritius)

“...you get to meet the big players in the technical Internet industry, and you get to meet interesting people as well, such as the Father of the Internet and Mr. RFC 1.”
—Fahd Batayneh (Jordan)

“The experience and research ideas gained from the [IETF] meeting will be helpful when I proceed with my Ph.D. education.”
—Hassen Redwan Hussen (Ethiopia)

“...the openness and friendliness of participants [at IETF] willing to help and share information, especially with the first-timers.”
—Ernest Brown (Ghana)

With a research-intensive background, Hassen spent five years in a community-based nongovernmental organization as ICT manager and another six years at Addis Ababa University’s College of Developmental Studies. One of the reasons he was motivated to apply to the ISOC Fellowship to the IETF is his interest in team-based research and development studies related to computer science, engineering, and ICT. Hassen is interested in 6LoWPAN fragmentation security, wireless sensor networks, mobile ad hoc networks, and security and privacy in ubiquitous networks and systems. “The IETF meeting will help me in learning about new technological advancements and applications,” he wrote.
ISOC Fellows and Returning Fellows at IETF 78 in Maastricht, Netherlands
IPv6 Neighbor Discovery Optimization

By Samita Chakrabarti

What makes IPv6 Neighbor Discovery useful in 6LoWPAN and other networks.

It wasn’t too long ago that I first saw 6LoWPAN working group (WG) cochair Geoff Mulligan conducting a demonstration of smoke detectors communicating using IPv6, User Datagram Protocol, Internet Control Message Protocol version 6, and Simple Network Management Protocol over an Institute of Electronics Engineers (IEEE) 802.15.4 low-power wireless network in the hallways of Sun Microsystems. That day I was part of a discussion with Geoff and my colleagues Gabriel Montenegro and Erik Nordmark to launch at IETF a birds of a feather on running IPv6 on tiny devices (4K to 64K RAM, 8- to 16-bit CPU) over IEEE 802.15.4 networks. Shortly after that, 6LoWPAN WG was born.

The low-power network (LoWPAN) is characterized by a low-powered, short-range, low-bit-rate, low-maximum-transmission-unit, low-cost network. The devices on the network, most of which are battery powered and have limited-capacity processing power, are designed to perform in sleep-wake cycles. Although LoWPAN is closely associated with sensors, it can be composed of many different devices that may or may not always require sensing functions, such as home and ZigBee devices. Given that IPv4 addresses are in short supply and that these low-power networks constitute huge number of tiny devices, IPv6 is the obvious choice for IP-addressing a device. While IEEE 802.15.4 layer 2 technology is gaining momentum as a low-power, wireless, personal-area network, HomePlug and power-line communication technologies are also candidates for using the 6LoWPAN stack for end-to-end IP communications. Recently, IPv6 over IEEE 802.15.4 (http://www.ietf.org/rfc/rfc4944.txt) was selected as one of the protocol requirements for Smart Energy 2.0 (http://tools.ietf.org/html/draft-sturek-6lowapp-smartenergy-00). ZigBee (http://www.zigbee.org), too, decided to use Smart Energy 2.0 and a standard-compliant IPv6 and 6LoWPAN stacks. The ZigBee Alliance’s IP group is the first user of IPv6 Neighbor Discovery Optimization for Low-power and Lossy Networks (http://tools.ietf.org/html/draft-ietf-6lowpan-nd-12) as part of IPv6 address autoconfiguration inside a building network or a home network.

So, the obvious question is, Why should I implement 6LoWPAN-neighbor discovery (ND) optimization? In theory, the traditional IPv6 ND should be able to run as it is. 6LoWPAN is the adaptation layer between the IPv6 stack and the IEEE 802.15.4 data link layer. While IEEE 802.15.4 supports broadcast at the link layer, it does not specify multicast support at the link layer. RFC 4861 was developed primarily for wired traffic on the shared medium, and it uses periodic router-advertisement multicast addresses with router solicitation, neighbor solicitation, address resolution, and duplicate-address detection. While periodic multicast signalling and solicited-node multicast signalling are useful for network stability in the standard Ethernet-based shared network, the limited-lifetime, battery-operated devices in the IEEE 802.15.4 network conserve energy with less signalling and by sending broadcast messages only once in a while. The multicast messages in the IPv6 ND are translated to broadcast messages in the network. In most cases, the 6LoWPAN-ND (http://tools.ietf.org/html/draft-ietf-6lowpan-nd-12) optimizes multicast messages to unicast messages. It eliminates the need for relatively expensive address resolution by sending a neighbor registration option along with a neighbor solicitation; it supports sleepy nodes in the networks; and it optimizes the protocol constants while eliminating periodic router-advertisement messages. Thus, if measurements taken on the IPv6-ND-control messages in the local network are compared with those taken on

Figure 1. 6LoWPAN network using route-over topology sharing a single IPv6 prefix in the LoWPAN
6LoWPAN-ND, we may observe a significant drop in signalling messages. By saving a number of controlling messages in a network of hundreds of nodes, a sizable amount of energy is saved; and at the same time, the lifetime of the node battery increases, which contributes to cost savings in maintaining such a huge network.

Another interesting and unique property of a low-power and lossy network is that the boundary of a link or IP subnet is redefined by the short radio range of these devices. The devices are usually configured for lower-than-maximum radio strength to save battery life. Thus, the local link of a node depends on the neighbors it can reach. The list of such neighbors also may change in time due to the lossy nature of the low-power radio link. Thus, the 6LoWPAN-ND supports two types of topology: route-over topology and mesh-under topology. The difference between mesh under and route over is similar to that between a bridged network and an IP routing using Ethernet: In a mesh-under network, all nodes are on the same link, which is served by one or more routers and which we call 6LoWPAN Border Routers (6LBR). In a route-over network, there are multiple links in the 6LoWPAN. Unlike fixed IP links, these links' members may be changing due to the nature of the low-power and lossy behaviour of LoWPAN wireless technology. Thus, a route-over network is made up of a flexible set of links interconnected by interior routers, which we call 6LoWPAN routers (6LR). However, for purposes of simplicity and compatibility with the existing concept, we assume that each route-over network shares a single global IPv6 prefix and that the interior routers (6LR) either (1) use a default router to forward the packets to the destination in an inefficient way or (2) run a hop-by-hop routing protocol such as RPL (http://tools.ietf.org/html/draft-ietf-roll-rpl-11).

Since 6LoWPAN-ND assumes that a 6LoWPAN (mesh under or route over) shares the same IPv6 prefix across the network, it ensures local mobility in route-over topology. In mesh-under topology, the whole network is regarded as a single IPv6 subnet served by the border router (6LBR), which has regular IPv6 on one interface and 6LoWPAN on the IEEE 802.15.4 interface. Note that an IPv6-over-IPv4, 6RD, or 6to4-style tunnel technology may be applied on the IPv6-interface of the 6LBR if the IPv6 interface side is attached by way of an IPv4 network. Moreover, 6LBR may be capable of running an Internet gateway routing protocol on the IP-network side of the interface in order to offer seamless connectivity of the 6LoWPAN devices to the IP network. Border router 6LBR also acts as a gateway between the IPv6 interface and 6LoWPAN interface.

In the 6LoWPAN-ND optimization, the 6LBR is capable of disseminating the IPv6 prefix and header compression context information across the 6LoWPAN. The border router may also maintain a 6LoWPAN-wide cache of the nodes' IPv6 addresses and unique identifiers. The IEEE 802.15.4 device contains an extended unique identifier (EUI)-64 identification number and can form 64-bit MAC addresses based on EUI-64 ID. They are also allowed to allocate 16-bit media-access-control (MAC) addresses or short addresses for local use due to the low maximum transmission unit (127 bytes) of today's deployed 802.15.4 networks. However, the 6LoWPAN-ND optimization work assumes that each IPv6 address is derived from an EUI-64 unique MAC address. Thus, by default it requires neither any duplicate address detection nor address resolution, because the mapping of MAC address to IPv6 address is as accurate as possible. But the document provides an optional mechanism for duplicate-address detection (DAD) for IPv6 addresses that are not derived from an EUI-64 identifier. However, the specification requires that the node possess an IEEE-assigned EUI-64-compliant device number, even if the node uses an IPv6 address that is not derived from the EUI-64 number. In route-over topology, the intermediate router (6LR) acts as a first-hop default router; if it is configured to do multihop DAD, it sends the EUI-64 and address-to-register information to the border router (6LBR), which maintains the network-wide information and thus is able to catch duplicate addresses. This technique of multihop DAD has limitations in a large network when all nodes are started at the same time. Therefore, the multihop DAD technique should be configured carefully for a low-density 6LoWPAN. And the intermediate routers should be brought up gradually, as if a wave is propagating from the 6LBR to the leaves or hosts.

Continued on next page
of the network. Note that alternatively, DHCPv6 may be used to ensure unique 16-bit MAC addresses as well as the unique IPv6 addresses in the network when the devices do not support EUI-64-style MAC addresses, but this requires modification in DHCPv6 service and specifications, which is out of the scope of this discussion.

Figure 1 illustrates the basic components of a 6LoWPAN in a route-over topology and optional prefix and context dissemination from the border router to the hosts via the intermediate routers. The 6LBR acts as a gateway between the regular IPv6 network and 6LoWPAN that facilitates connectivity across nodes in different networks.

As mentioned earlier, neighbor discovery optimization simplifies ND signalling for low-power and lossy networks and replaces address resolution with address registration for a specific lifetime during which the address should stay valid. The length of time it is valid is configurable, and the system is refreshed periodically. Address registration allows for ease of mobility of the 6LoWPAN nodes in the future and provides useful information about the neighboring hosts for the routing protocol. The address registration takes place in the nearest default intermediate routers of a host unless multihop DAD is requested. In the case of multihop DAD, address registration and duplicate detection are also performed at the central location (6LBR) because 6LBR has a view of the whole network. The message sequence in figure 2 provides a typical view of optimized neighbor discovery messages.

Although the IPv6 neighbor discovery protocol has been extended for the 6LoWPANs for running IPv6 over IEEE 802.15.4-2003 networks, the optimizations are also applicable to future versions of IEEE 802.15.4 specifications and other networks where

optimizations are useful for saving control messages and power. The solution of optimization of neighbor discovery is designed to expand so as to consider secure neighbor discovery usage and other possible extensions in the future. The current solution of optimized ND is not a replacement for DHCPv6, yet it offers limited provisioning capability for a small and simple network, such as a home network. Since the entire 6LoWPAN uses a single prefix in the current 6LoWPAN architecture, the optimized ND automatically offers local mobility of the nodes within a single 6LoWPAN.

In the future, the work may be extended to provide different levels of functionalities as the usage and applications in the sensor networks and home or enterprise networks are deployed. Finally, the author acknowledges her co-authors of the optimized neighbor discovery specification—Erik Nordmark and Zach Shelby—for their original ideas and contributions, which shaped the optimized IPv6 neighbor discovery document.

---

**DNS—the Perspective from a Single Moment in a Long History**

*By Leslie Daigle*

During the IETF 78 administrative plenary, meeting attendees enjoyed a champagne toast in recognition of the recent signing of the Domain Name System (DNS) root zone. As many have noted, that signing was a momentous occasion, marking the cornerstone in development of DNS—securing technology (DNS Security Extensions, or DNSSEC) after a long development process. It also seemed like the right moment to look to the future of the DNS, as we did via the Internet Society—sponsored panel event The DNS, Secure at 27: What Next? while also kicking off a process for collecting and understanding the long and involved history of DNSSEC itself.

**The DNS, Secure at 27: What Next?**

On 27 July 2010, the Internet Society convened a panel of experts to talk about the DNS and to give insight into the state of the DNS's overall security. In addition to the work they do in their day jobs—involving developing, deploying, and operating the DNS and related technologies—the panellists have each been involved in IETF activities as contributors, working group (WG) chairs, and Internet Engineering Steering Group and Internet Architecture Board members. Patrik Falström, Barry Leiba, Lars-Johan Liman, and Danny McPherson have seen DNS technology issues from all angles. While their comments on the security of DNS are reported elsewhere (see “DNSSEC Doesn't Mitigate All DNS Threats,” page 8), the panel discussion itself first highlighted a number of ways the DNS has become more than a host name/number lookup system and then emphasized that it will continue to evolve.

By many of the metrics for protocol success that the IAB has cited in RFC 5218: What Makes for a Successful Protocol? the DNS is a successful protocol. It met a real need, it has had freely available code sources, and it has been openly maintained through IETF processes (such as the DNSOPS WG) for years. Furthermore, it has demonstrated its extensibility (through new uses) and its scalability (with tens
of millions of domain names registered across all top-level domains); and with DNSSEC in place, threats are being mitigated.

The panellists said the DNS is a little hard to position in the layer model of protocol design. Lars-Johan said the DNS is the glue between the transportation and application layers and that much of our use of the Internet (through applications and services) would simply stop without it. With its global footprint, it has become the go-to infrastructure for services that share some need for resource lookup.

Patrik said that by storing materials in the DNS, which is now even more trustworthy, the DNS can be used for bootstrapping other infrastructure when DNSSEC is deployed.

Barry outlined a case in point: the work of the DKIM (DomainKeys Identified Mail) is using aspects of the DNS to let domains publish (in the DNS) information about their practices in applying signatures to email and to take responsibility, using digital signatures, for having taken part in the transmission of an email. By storing this information in the DNS, the DNS becomes a critical component in the process of receiving (not just sending) email.

To be successful in such approaches, Patrik said, it’s sometimes important to store a pointer to data (not the data itself): the DNS infrastructure for any given zone is likely administered separately from the dependent application using it to make data available, and sometimes the referenced data is larger than would reasonably be stored in a DNS record. It’s important to align administrative responsibility and data characteristics to be consistent with the DNS’s own architecture and expectations.

Lars-Johan emphasized the same point, saying that even though the DNS can hold a lot of data across its namespace, hierarchy is important. For example, caching is important for keeping stress off higher levels. If you’re going to use the DNS to store some application data, it is imperative to ensure that your applications’ data needs—and data reference needs—fit into the DNS model.

Panellists also discussed the importance of considering operational realities in order to ensure successful protocol extensions. Sometimes, designs that make perfect sense mathematically turn out to be operationally un-supportable. A case in point involved DNS bit string labels (RFC 2673), which worked well in theory but were too complex to consider deploying extensively in operational practice. That case underscores the need to design, conduct test deployments, and consider operational realities before committing to full-scale standardization and deployment. The ability to step back and reevaluate is an important part of overall successful protocol development and evolution.

The DNSSEC History Project

Along those lines, the signing of the DNS root also inspired an effort to take a step back and consider the long history of DNSSEC itself. Steve Crocker observed that the history of DNSSEC has been a very long arc, featuring work by a great number of people; false starts; facing technical, operational, and political challenges; and enduring a long hard march to success.

Steve Crocker observed that the history of DNSSEC has been a very long arc, featuring work by a great number of people; false starts; facing technical, operational, and political challenges; and enduring a long hard march to success.

Currently, some of the areas of observation are:

• Determination of the need: What drove the work?
• Technical design: What were the key design goals and how were they addressed? What were the alternatives?

The DNSSEC History Project wiki was established (https://wiki.tools.isoc.org/DNSSEC_History_Project). The aim of the project is to collect information—in the forms of anecdotes, design documents, observations, and other contributions—from everyone who has material to share. Please do have a look at the wiki and contribute where you can.

Currently, some of the areas of observation are:

• Government planning: R&D and policies
• Implementation and testing cycle: Bake-offs and other field events
• Public and policy-awareness events and activities
• Controversies
• Friction in deployment: Inertia, business cases
• Vendor view

The intention of the project is to collect as much raw material as possible, with a view to being able to abstract some coherent lessons learned. These will be important lessons for all protocol development, not just for the DNS or DNSSEC: many of the same hurdles are faced by other broad-scale technologies.

A Single Moment in a Long History

The champagne at the administrative plenary may have been but a single moment, but it was a good vantage point from which to consider the past as it illuminates the future for the DNS in general and DNSSEC in particular.
Impact of New Undersea Capacity on KENET and East Africa

By Kevin Chege

Until 2009 on this part of the African continent, connectivity to the Internet was via satellite only. That meant speeds that were slow and connectivity that was expensive. In Tanzania, the price of 1 megabit per second (Mbps) of bandwidth cost anywhere from USD 4,000 to USD 12,000 per Mbps; in Kenya and Uganda, the cost was around USD 2,000 to USD 3,500. (The prices represent bandwidth with a 1-to-1 contention ratio.) Cheaper options were available, but they were probably from a shared pool with no guarantee on the bandwidth. It was possible to find some terrestrial fibre for local loop connectivity, but it was not widespread and was primarily by way of the big telecommunications companies in each of the countries.

In 2008, word of undersea connectivity began to spread, but many in the region grew skeptical when the landing dates for the cables kept changing. Finally, three cables arrived in the region: SEACOM and TEAMS, each with 1.28 terabit-per-second capacity, and the EASSy cable, with a capacity of 3.8 terabits. SEACOM, which would land on Kenya’s coast at Mombasa and on Tanzania’s coast at Dar es Salaam, would connect the two countries to London via Marseille; TEAMS would connect Mombasa only to Fujairah in the United Arab Emirates. EASSy, which was to land in nine countries from South Africa to Sudan along Africa’s east coast, was meant primarily to interconnect African countries internally.

In 2009, two cables were completed: SEACOM in June and TEAMS in July. In addition to greater Internet capacity, many in the region were looking forward to lower connectivity prices. SEACOM had a head start by having arranged for its connectivity to be carried all the way to Uganda and Rwanda via Kenya and also by arriving a month earlier than the competition’s. Part of the reason the price of connectivity on the SEACOM cable was more favourable than on the TEAMS cable was that Internet Protocol transit costs in London were much less than they are in Fujairah. In London, the prices that the Kenya Education Network Trust (KENET) received ranged from USD 2 to USD 15 depending on the amount of bulk bandwidth purchased. In Fujairah, transit costs ranged from USD 70 to USD 90 per 1 Mbps, also varying with the amount purchased. Eventually, the TEAMS cable was put into service, though in Kenya there was some fallout among some of the members who owned the TEAMS cable, which resulted in some shares’ being bought out. EASSy was not completed until mid-2010.

Of the three regions, Kenya appears to be the best served in terms of capacity, with all three cables landing at Kenya’s port of Mombasa. In late 2009, the new pricing started reaching consumers. In Kenya, prices dropped to around USD 600 per Mbps. One of the large Internet service providers (ISPs) offered a buy-one-get-four offer, so the price ultimately climbed to USD 150 per Mbps, but only if a consumer purchased 4 Mbps. With a store of unused capacity available, the ISPs could afford to be generous. Some ISPs had activated 10 gigabits per second (Gbps) of capacity, but only 2.5 Gbps were typically in use.

At KENET, we expected universities to be using as much as 5 or 10 times their previous usage, but despite the faster speeds to the Internet (up from the previous 700 to 800 milliseconds (ms) round-trip time (RTT) to 180 to 300 ms RTT), they were not. We discovered that the low usage was due primarily to poor internal networks that were sufficient for VSAT (very-small-aperture terminal) but not for fibre. In addition, the networks were not well set up, so high speeds were observed only at the edge of the network—near the router gateway to KENET—and there was a low ratio of personal computers to users. (See http://eready.kenet.or.ke.)

We tried to solve the problem of poor internal infrastructure by offering more consultations and trainings. In March 2010, a workshop was conducted in partnership with the Network Startup Resource Center (NSRC) and the University of Oregon covering campus network design, which is the foundation of developing a robust, high-performance National Research and Education Network (NREN). The main objectives of the workshop were to train university network engineering
staff on how to develop and implement a strategic design plan for their campus networks, with particular emphasis on layers 1 and 2, and to strengthen the KENET technical community (human network) in developing KENET’s cyberinfrastructure.

Funding and support for the training came from the National Science Foundation (NSF) and the Partnership for Higher Education in Africa (PHEA) via the NSRC. As an additional benefit of the training, the NSRC donated 2.5 tons of technical reference books and networking equipment (routers, wireless equipment and gigabit network switches) that have been distributed to the universities for live deployment following the training. This equipment is making a significant impact in improving the functionality of the respective campus networks, which helps to achieve KENET’s goal of getting more faculty members and students using the Internet for research and education activities.

In addition, more emphasis was put on bandwidth management and optimization because even though there was more capacity, it was not being shared properly: one or two users were still able to consume the majority of the available capacity available to the universities. KENET is undertaking an effort to extend this programme further and to provide more online information on the topic, including how-tos and online training materials hosted at KENET (see http://bmo.kenet.or.ke and http://training.kenet.or.ke). The information is also available to the neighbouring national research and education networks that form part of KENET’s mailing lists on the topic.

KENET had previously signed a two-year VSAT contract with a supplier for 200 Mbps of capacity. Though the contract became effective in January 2009, the resources that were to be made available by means of a World Bank grant to improve Internet capacity at the universities got delayed. Regardless, KENET managed to negotiate with the provider for half of the anticipated capacity with fibre—meaning, KENET would remain active, with 100 Mbps VSAT and 100 Mbps equivalent by way of fibre when it became active. Thus, KENET would have 350-Mbps capacity on fibre and 100-Mbps capacity on VSAT plus an additional 155 Mbps via a KENET-owned link to the UbuntuNet router in London connecting KENET to GÉANT and allowing for peering via UbuntuNet.

Since that expansion, KENET went from 12 Mbps in 2008 on VSAT to 450 Mbps on VSAT plus fibre in 2009, to more than 600 Mbps combined capacity in 2010—all in a span of 18 months. Usage has peaked, and the need for additional capacity is anticipated due to users’ increased awareness of better speeds, which leads to increased use of the Internet for reading newspapers online, conducting research, streaming video, and visiting social networking sites.

In response to rising demand, KENET has increased its infrastructure for core services like DNS and email, which have become more essential than ever. There is also more demand for online services, such as email filtering and Web hosting as more of our universities increase their online communication facilities. KENET is building both a network operations centre and a data centre to facilitate deployment of additional services, such as Web-based conferencing, caching, backup services, and storage.

Today in Kenya, with more users online than ever, more companies than ever are using e-marketing. However, there are issues related to online security—particularly with recent identification of Kenya as the country most hit by viruses, a problem that also affects the country’s universities. KENET is planning to address that problem by examining its policies and increasing its security training in the coming year. KENET is also seeing more peer-to-peer traffic, a concern that is also being addressed through education and training. At this time, not all of the universities are in a position to control such problems, so the idea is to empower them to be able to control and manage their capacities. For even our most remote universities, VSAT is no longer an option, and since fibre is not available throughout the country, we are hard-pressed to find viable solutions that include last-mile-high-capacity radios to backhaul to the nearest point of fibre.

In closing, the impact of increased capacity is more demand for online, high-quality services as well as a big drop in the cost of capacity. Universities have been able to scale up to as much as 10 times their previous capacity—from 10 Mbps on VSAT to 60 Mbps on fibre. The biggest constraint for Universities in Kenya and East Africa is the last-mile reach and cost, which is slowly improving. However, the universities are working on upgrading their internal networks and KENET is working on deploying wireless networks in the campuses. The current cost is now around USD 280 per Mbps with the price set to fall even further in 2011 as more ISPs and KENET drop their VSAT contracts.

It is big news when an undersea cable is cut, as was evident when the main cable, SEACOM, experienced a repeater failure for two weeks in July 2010. KENET was forced to purchase restoration capacity in order to support our VSAT redundancy capacity, which was too slow for users. Our capacity of 606 Mbps is now fully used up. In order to meet ever-growing demand, we are planning to activate more capacity via the TEAMS cable before the end of 2010 and we anticipate our capacity in January 2011 to be 750 Mbps and 1.2 Gbps later that year.

Kevin Chege is network manager of Kenya Education Network Trust
IETF Update

By Aaron Falk

This is a status report on the Internet Research Task Force (IRTF) and an introduction to the Transport Modeling Research Group based on the report presented at IETF 78 in Maastricht, Netherlands.

IRTF Status

Eight of the 13 IRTF research groups (RGs) met at IETF 78. Eleven research groups are active at this time, either because they are holding meetings or because they have an active mailing list. The Internet Architecture Board met with the chairs of the recently formed Virtual Networks RG to discuss the group’s charter, activities, and plans.

No new IRTF-stream RFCs have been published since IETF 77. The Internet Advisory Oversight Council is sponsoring an effort to modify the IETF Draft Tracker in order to show progress of non-IRTF-stream Internet–Drafts, including IRTF-stream documents. ID draft-hoffman-alt-streams-tracker collects the review and approval states of IRTF documents and other tracker modifications that are required.

A new mailing list has been created for public discussion of IRTF-related topics, such as new RG proposals. The list address is irtf-discuss@irtf.org. (This is a corrected address from one given in a prior status report.)

Several topics are under discussion to become candidates for new IRTF RGs, including cloud computing, economics and policy, Internet of things, machine learning and communication systems, and social networks.

In spring 2011, I will be stepping down from the position of IRTF chair, which I have held for six years. An effort is under way to identify candidates for the position. If you would like to be considered for the position, please contact Internet Architecture Board (IAB) chair Olaf Kolkman (olaf@NLnetLabs.nl) or me housley@vigilsec.com). The IRTF chair is approved by the IAB.

Introduction to the Transport Modelling RG

The goal of the Transport Modeling RG is to improve methodologies for evaluating transport protocols. The charter sets out to produce a variety of deliverables, including (1) a survey of models being used in simulations, analysis, and experiments for the evaluation of transport protocols; (2) a broad set of simulation test suites; and (3) a slate of recommendations for test suites that can be used as experiments in test beds.

A transport model is a set of assumptions about network and traffic conditions implicit in protocol evaluation. It addresses the topology, round-trip times, flow arrivals and durations, and flow greediness. Note that it need not be a mathematical model.

A recent discussion in the RG covered evaluation of the effect of faster flow start-up. There has been a proposal in the IETF to increase the TCP initial window, and some of the measurements taken at data centres show improvement in flow completion times. The RG is considering how one would assess degradation to other users from this more aggressive approach, with special consideration of users with slow connections.

Other IETF and IRTF efforts involve transport protocols and congestion control. Therefore, it is useful to be clear about what the Transport Modeling RG is not chartered to do. Specifically, the group does not discuss either the design of new congestion control mechanisms or modifications to existing congestion control mechanisms (except in terms of models needed for the evaluation of such
mechanisms). Neither does the group produce evaluations of specific congestion control mechanisms.

The RG has produced a variety of outputs, including:

- Metrics for the Evaluation of Congestion Control Mechanisms, RFC 5166
- Tools for the Evaluation of Simulation and Testbed Scenarios, draft-irtf-tmrg-tools
- Common TCP Evaluation Suite, draft-irtf-tmrg-tests
- An NS2 TCP Evaluation Tool Suite, draft-irtf-tmrg-ns2-tcp-tool

Future work will include consideration of metrics for evaluating admission control systems and documenting known so-called corner cases in transport modeling.
IETF Meeting Calendar

IETF 79
7–12 November 2010
Host: Tsinghua University
Location: Beijing, China

IETF 80
27 March–1 April 2011
Host: CZ.NIC
Location: Prague, Czech Republic

IETF 81
24–29 July 2011
Host: Research in Motion (RIM)
Location: Quebec City, Canada

IETF 82
13–18 November 2011
Host: Taiwan Network Information Center (TWNIC)
Location: Taipei, TW

For more information about past and upcoming

IETF Meetings

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

Special thanks to
SIDN
for hosting IETF 78

The ISOC Fellowship to the IETF is sponsored by

Microsoft

This publication has been made possible through the support of the following

Platinum Programme supporters of ISOC

Afilias
ARIN
comcast

Ripe
WIDE

The Oxford English Dictionary Second Edition

Email
ietfjournal@isoc.org
Find us on the Web at
http://ietfjournal.isoc.org

Editor's Note:

The IETF Journal adheres to

Pub-IETFJv6.2-20101206-en