the IETF® Journal

Volume 6, Issue 3 • March 2011

*A report from IETF 79, November 2010, Beijing, China. Published by the Internet Society in cooperation with the Internet Engineering Task Force**

Inside this issue

Edging Toward the End of IPv4: A New Milestone in the History of the Internet

From the Editor's Desk, by Matthew Ford

Since the last issue of the *IETF Journal* went to press, the Internet passed a major milestone in its journey from research network to preeminent global communications medium. The final blocks of unicast IPv4 address space were allocated to the Regional Internet Registries on 3 February 2011. In this issue, Internet Architecture Board (IAB) chair Olaf Kolkman gives us his statement at this juncture in Internet history (page 3).

Photo/Peter Löthberg

Beijing, site of IETF 79

During IETF 79, the Internet Society hosted a panel discussion on the topic "Handheld, Wireless, and Open: Priorities for the Mobile Future Internet." The diversity of devices now connecting to the Internet is creating new challenges for engineers, operators and users alike. On page 5 we present a snapshot of the event itself and on page 12 we have a more detailed reflection from Leslie Daigle on some of the issues raised by "The Untethered Future of the Internet."

In addition to our other regular features, we include an opportunity to get to know the Internet Society Fellows who attended IETF 79 (page 11) as well as an in-depth look at the challenges being faced by operators in the presence of IPv4 address depletion and the need to deploy IPv6 throughout their service portfolio (page 4). Finally, Christian Jacquenet gives us some valuable insight into France Telecom's recent progress with IPv6 deployment (this page).

As usual, sincere thanks to all our contributors. We invite you to send comments and suggestions for future issues to ietfjournal@isoc.org.

Zero Addresses, One Solution, Two Problems

By Christian Jacquenet

The IPv4 world as we know it is coming to an end. IPv6 is the only perennial solution to global IPv4 address depletion, but transition will take several years, if not decades.

As a consequence, service providers have to deal with two distinct issues:

1. The need to face the forthcoming global IPv4 address depletion, which means the introduction of IPv6 capabilities into network and service infrastructures
2. The need to guarantee IPv4 service continuity during the transition period when global IPv4 addresses will become even more scarce: that is, make sure customers can still access IPv4 content from an IPv4 terminal despite the scarcity of public IPv4 addresses.

Continued on page 7

Message from the IETF Chair

By Russ Housley


Russ Housley, IETF Chair

The work of the IETF remains relevant and energetic!

IETF 79 was held in Beijing, China. It was a very successful meeting attended by 1177 people from 52 different countries. Many visited China for the first time. The Chinese were wonderful hosts and the facilities in the Shangri-La Hotel were outstanding. Many working groups made significant progress, and it was a genuine pleasure to see so many talented people engaged and collaborating.

CNNIC, the Internet Society of China, and Tsinghua University combined forces to host IETF 79, and they did a fantastic job. The host team coordinated with nine sponsors to make sure that the welcome reception, social event, and all of the breaks were memorable. The food was amazing; as Barry Leiba said during the open mic at the plenary on Wednesday, "The food at the breaks has never been better; I hope we can have dim sum from now on." The performances at the social event were amazing and memorable, as were the beautiful artwork and other artifacts in the museum.

Many working groups made significant progress, and it was a genuine pleasure to see so many talented people engaged and collaborating.

Since IETF 78, seven new working groups (WG) have been chartered, and five WGs were closed. We have 124 WGs. Between the meetings, the WGs and their individual contributors produced 545 new Internet-Drafts, and updated 1003 existing Internet-Drafts, some more than once. The Internet Engineering Steering Group (IESG) approved 92 Internet-Drafts for publication as RFCs. The RFC Editor published 108 new RFCs.

During the plenary session on Wednesday evening, the Itojun Service award was announced. This year's recipient was Bjoern A. Zeeb for his dedicated implementation work in making IPv6 a first class citizen in the open source UNIX world. This was the first time that Bjoern was able to attend an IETF meeting. He was amazed by the dedication and hard work that he witnessed. Bjoern promised to return to future IETF meetings.

IETF 80 will take place in Prague, Czech Republic on 27 March-1 April 2011 hosted by CZ NIC. Scheduling information for the upcoming IETF meetings can always be found at http://www.ietf.org/meeting/. I look forward to seeing you there.

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/DocProtoActions0603.shtml

Words from the IAB Chair

By Olaf Kolkman

Olaf Kolkman, IAB Chair

On 4 February the last five /8 IPv4 blocks from the free pool at IANA were allocated to the regional internet registries (RIRs). Below you can find the statement I made, as (Internet Architecture Board) IAB chair, during the press conference. I am well aware that with this text I am preaching to the choir, but it is an example of the kind of evangineering that the IAB gets into now and then.

The allocation of the final IPv4 free address blocks to the regional registries is both a significant and an insignificant event.

It is significant in that this moment has long been anticipated. The IETF, the standards organization for Internet protocols, started to work on an IPv4 successor almost 20 years ago, and IPv6 as we know it today was standardized 15 years ago and has matured ever since.

This event is insignificant in that next week the Internet will not be significantly different than it was a week ago. If we would run out of license plates there would not be any impact on our driving. Similarly, there will not be any notable short-term effects caused by the exhaustion of the IPv4 free address pool.

Therein lies a danger.

In the long term the application providers (and their clients) that utilize IPv4 addresses are likely to encounter issues because of the many kludges needed to keep those apps running. Meanwhile, applications that can communicate over IPv6 enabled networks will be more likely to encounter transparent end-to-end communication, enabling the continued development of innovative applications and services.

Suppose that you would compare the Internet of today with the Internet in 10 years.

If we continue to remain dependent on IPv4 we will need to spend increasing resources operating an increasingly brittle and non-transparent network incorporating NATs, ALG, CGNs, and other mechanisms needed to help the IPv4 network keep up with demand.

Such an Internet is likely to grow increasingly less capable in serving our needs than it is today. Rather than maintaining the "status quo", the IPv4 Internet is likely to degenerate.

On the other hand, with an IPv6 based Internet endless possibilities lie ahead, because every human on this planet, and their gadgets, will be able to communicate, play, do business, and supply services. That type of explosive growth of the Internet can only continue with the larger address space that IPv6 offers.

The transition to IPv6 will not be effortless and requires the attention of equipment vendors, ISPs, CTOs and CEOs, system - and network administrators, content providers, etc, etc. However, my mother, my neighbors and my kids should never notice. They will continue to be delighted by ongoing innovation and expanded services made possible by the architecture of the IPv6 Internet.

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

IPv4, IPv6 Coexistence Challenges Network Operators

By Carolyn Duffy Marsan

IPv4 and IPv6 will coexist on the Internet for decades, creating the need for additional transition mechanisms because the dual-stack model won't solve all of the emerging problems for network operators.

That was the consensus view of a panel of experts who discussed IPv6 operations and transitional Issues at the Internet Architecture Board (IAB) technical plenary held 8 November in Beijing.

"We're going to have a very long transitional coexistence period," said Danny McPherson, chief security officer at VeriSign, who moderated the panel discussion. "There's a lot of work going on still for . . . some of the strategies for IPv4-only devices to speak to IPv6 networks where you don't have dual stack as an option."

Latency is a key issue that the cable company Comcast has run into during its ongoing public trials of several IPv4-to-IPv6 transition mechanisms. Comcast began its IPv6 deployment five years ago, and its network is largely dual stack, along with its back office functions and access network.

Comcast noticed that it had a large volume of tunnelled 6to4 traffic on its network and that these end-users were experiencing too much latency. So the company deployed its own 6to4 relays based on an open source Linux platform, and that has improved the performance of 6to4 traffic by 50 percent or better.

Comcast also tested the 6rd encapsulation mechanisms and found that they performed better than 6to4. It found the 6rd relays to be "extremely simple to deploy," said John Brzozowski, chief architect for the IPv6 programme at Comcast. "If your access networks cannot support native IPv6, [6rd] definitely feels like something that you should look at."

John pointed out that network operators will see their costs rise as they deploy additional IPv6 transition mechanisms. "The more you have to put out there for subscribers, the more the investment will be for you," he added.

One issue that is driving up the cost of Comcast's public IPv6 trials is its need to manually configure all of the customer premises equipment (CPE). "We used just shy of 300-some odd devices," John said. "We had to manually configure each and every one of them before we shipped them out to the trial users. That's clearly not going to be scalable long term."

Comcast said dual stack will offer its subscribers the best overall experience because it has direct end-to-end routing without translation, tunnelling, or encapsulation. In the future, Comcast hopes to be able to purchase CPE that supports native IPv6, but it still faces the challenge of dealing with older CPE that isn't upgradable to IPv6 and must be replaced.

"Operators should go with what's available to them now," John urged. "Get started. Really, don't wait until it's perfect."

Matsuzaki Yoshinobu of Internet Initiative Japan said he has run into several unexpected implementation issues with routers handling IPv6 traffic. Some routers only support lower prefixes while others have trouble sending bigger IPv6 packets. Packet filtering for IPv6 also can be problematic.

Another issue Matsuzaki noted is poor user experience, such as a lack of IPv6 connectivity in some countries and the poor performance of IPv6-over-IPv4 tunnelling offered by some ISPs. Other problems are broken discovery and the need for link-local addressing.

China Telecom is trying to move rapidly to IPv6 because it needs about 30 million IP addresses in 2011 alone to support its rapidly increasing subscriber base for broadband, IP television, and other services. But it has only 10 million IP addresses, leaving a gap of 20 million IP addresses.

"For a lot of new services, new applications, we still need several billion new addresses in the future five years," said Huiling Zhao of China Telecom.

Huiling said China Telecom is exploring four ways to meet this demand

for IP addresses: reusing existing IPv4 addresses, using private IPv4 addresses, purchasing additional IPv4 addresses, and deploying IPv6. "We think IPv6 is the best solution in the future," she added.

Huiling said there are problems with each of the existing IPv6 transition mechanisms. Dual stack requires a dedicated IPv4 address for each user, and it also has performance problems. NAT444 lacks carrier-grade performance and is difficult to deploy on a large scale. DS-Lite requires that home gateways be upgraded. Currently, China Telecom is studying additional mechanisms including NAT64, IVI/DIVI, and 6rd.

"Perhaps we finally need a cocktail method combining several tunnelling and protocol transition methods in order to meet our market requirement," she said, adding that one possibility is combining dual stack with private IPv4 addressing.

Xiaodong Lee of China Internet Network Information Center (CNNIC) said that the number of registered IPv6 addresses and the amount of IPv6 traffic are very small in China despite the presence of a large IPv6 network. In fact, Xiaodong said there are many more IPv6 users in Europe and America than in China.

"There is no strong requirement for . . . users to use IPv6," Xiaodong said. "The reason for this is because the user, they don't care what is IPv4 or IPv6. They only care about the application. . . So the killer issue is applications."

Bill Huang from China Mobile questioned whether the dual-stack model will work well enough to support the migration to IPv6 at the same time that the company's network is projected to grow as much as 100-fold over the next five years. He said most dual-stack configurations default to IPv4. Instead, he favors the creation of new traffic-steering protocols that will translate or tunnel traffic from an IPv4 network to an IPv6 network.

"The result is that we will be able to see more and more traffic being steered towards a pure IPv6 network," Bill said. "If we equipped a new generation of terminals with these types of technology . . . then by default the traffic will be steered."

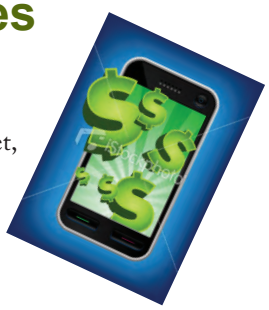
Jari Arkko of Ericsson concluded the panel with findings from his research of IPv6-only networks. He said several applications, including browsing, email, software updates, and streaming music work very well, while others, such as gaming and Skype, do not.

"I think we should still keep on recommending dual stack as the preferred mode. It has the least amount of problems," Jari summed up. "We can recommend IPv6 only as well for early adopters and mobile networks."

"Operators should go with what's available to them now. Get started. Really, don't wait until it's perfect." — John Brzozowski, Comcast

ISOC Panel Weighs Power, Billing Constraints of Smartphones

By Carolyn Duffy Marsan



When considering the future of the mobile Internet, network protocol experts are worried about two key issues: the power constraints of handheld devices and the high fees that carriers charge end-users for network- and application-generated events.

These two issues generated the most debate at a panel session entitled "Handheld, Wireless, and Open: Priorities for the Mobile Future Internet" that was sponsored by the Internet Society. The panel was held in Beijing on 9 November, concurrent with the IETF meeting.

Moderated by Leslie Daigle, chief Internet technology officer for the Internet Society, the panel considered the impact that a growing number of mobile devices and sensors will have on the Internet infrastructure.

"We already have 1.6 billion devices that were used to access the Internet in 2009, including PCs, mobile phones, and online gaming devices," Leslie said, highlighting the dramatic growth of these devices in China and India. "By 2013, that will grow to an estimated 2.7 billion devices."

Leslie said that most of these new mobile devices will be smartphones, and that smartphone users want to do the same things as PC users, such as using search engines, reading news, downloading music and videos, and exchanging email and instant messages.

She asked the panellists to consider ways in which smartphones challenge traditional thinking about how Internet hosts and applications should behave.

"Smartphones are becoming more and more smart and are having more and more advanced services," said Stefano Faccin, a standards manager with Research in Motion. He added that

Continued on next page

ISOC Panel, continued

while smartphones are getting more powerful, they still have some constraints. "Bandwidth is not unlimited. It will not be unlimited for a long time especially for cellular networks . . . but it will need to reach these devices at all times for a variety of services."

Stefano pointed out that the number of wireless sensors connected to the Internet also will rise. This means the Internet will have to support both really smart mobile devices and really dumb sensors.

"These devices will have different usage models and different networking issues," Stefano said. "The future Internet will have to cater to both types of devices even if their needs are totally different."

Ted Hardie, managing director for Panasonic's Wireless Research Laboratory, said power management is a key issue for future Internet applications to consider. He pointed out that as smartphones and other handheld devices function more like PCs, this trend will put strain on mobile operators, who have limited network spectrum, and on end-users, who have limited power.

"Users expect their mobile devices will behave as their wired devices behave," Ted said, adding that the challenge for the Internet engineering community is "how we can deliver on that expectation perhaps in ways that don't mimic the ways we did in the past."

Dave Thaler, a software architect in the Windows Networking and Devices Division at Microsoft, pointed out that in a power-constrained environment, wireless device users might not want to be reachable by all applications or all users. "I don't want to consume battery unless it's most important," Dave explained.

Hui Deng, deputy principle staff of China Mobile Research Institute, says this issue arises when mobile operators wake up a mobile device from its idle stage to activate a service. He said these decisions about waking up devices that occur in mobile application design and mobile network design also relate to the power consumption rates experienced by users.

Dave also focused on an issue he calls "bill shock," when end-users are hit with large and unexpected charges while in roaming mode. Dave says designers of mobile networks and applications need to take billing into consideration so they can help prevent such scenarios as when an end-user inadvertently downloads a software update while in roaming mode, rather than doing it when connected to a cheaper Wi-Fi connection.

"The user needs to be in control because the user is paying the bill. If something is going to affect the bill, you should expose that to the users." — Dave Thaler, Microsoft

"The user needs to be in control because the user is paying the bill," Dave said. "If something is going to affect the bill, you should expose that to the users."

Ted said end-users should have the ability to establish policies about the inbound messages they want to receive when they are in battery or roaming mode so that they can limit the ones that are going to cost more money.

Panellists agreed that the Internet engineering community will need to deal with power management and billing issues related to mobile devices for the foreseeable future.

"I think we're going to be stuck with the power issue for a long time," Stefano said. "Yes, the battery technology is improving dramatically, but at the same time a lot of the developments require more and more computational power . . . As long as certain mobile operators are going to have to pay so much for the frequency, we're going to have to be stuck with [bill shock] for quite a while."

IETF 79 At–A–Glance

Registered attendees: 1177
Newcomers: 320
Number of countries: 52
New WGs: 7
WGs closed: 5
WG currently chartered: 124
New Internet-Drafts: 545
Updated Internet-Drafts: 159
IETF Last Calls: 75
Internet-Drafts approved for publication: 92

RFC Editor Actions (July–October 2010)
RFCs published: 124
I-Ds submitted for publication: 108
- 75 IETF WGs
- 23 IETF individuals
- 10 IRTF, IAB, and independent combined

IANA Actions (July–October 2010)
IETF-related requests processed: 1468
- 717 private enterprise numbers
- 82 port numbers
- 54 TRIP ITAD numbers
- 23 language subtag requests
- 87 media-type requests

In addition, IANA:
- Reviewed 97 I–Ds in Last Call
- Reviewed 101 I–Ds in IESG Evaluation
- Reviewed 101 I–Ds prior to becoming RFC and 57 contained actions for IANA

Zero addresses, continued from page 1

The Need for IPv4 Service Continuity

The current thinking is that IPv4 service continuity can be addressed by introducing network address translation (NAT) capabilities into networks (also known as carrier-grade NAT or CGN) so that a global IPv4 address can be shared among several customers. But doing so may not be a good solution. While address-sharing issues and NAT hurdles have been extensively documented within the IETF, most service providers see them as little more than a necessary evil.

CGN Taxonomy

There are generally two kinds of CGN technologies: those that are used in addition to existing NAT capabilities and that are activated by customer-premises-equipment (CPE) devices, also known as double NAT, and those that rely on a single NAT.

Double NAT

Simply put, utilizing double NAT technology means that privately addressed IPv4 traffic that is sent by terminals located on the customer's premises will first go through one level of NAT (embedded in the CPE) and then go through another level of NAT (embedded in the CGN). This approach has the advantage of not requiring customers or service providers to upgrade existing CPE devices. This is an especially attractive option for service providers that do not manage CPE equipment.

There are, however, drawbacks to the double-NAT approach. First, in the double NAT design it is assumed that the regions of the network where CGN capabilities are activated enforce an IPv4 forwarding scheme based on the use of private IPv4 addresses. However, it is being done so at the cost of being exposed to the (complex) management of overlapping private addressing schemes in the network. That means the private addressing scheme enforced by the service provider in its network must not conflict with the customers' own private addressing scheme; it assumes an agreement between the service provider and its customers that the customers are not using private IPv4 addresses that are assigned to the portion of the service provider's network that is conveying privately addressed IPv4 traffic towards one of the available CGN capabilities.

Second, double NAT designs assume that the CPE devices that are serviced by the same CGN are not communicating with each other by default, because incoming privately addressed traffic is usually discarded by the firewall embedded in the CPE. Therefore, such traffic needs to cross the CGN so that the initial private-source address can be translated into a global IPv4 address, which is what hairpinning is all about.

Single-level NAT

The IETF currently standardizes one version of the single-level-NAT approach, which is called dual stack-lite or DS-lite. Within the context of a DS-lite design, privately addressed traffic sent by terminals located on the customer's premises is first encapsulated by the CPE into IPv6 datagrams, which are then forwarded to one of the available CGN capabilities.

The DS-lite CGN will then, in turn, decapsulate the privately addressed IPv4 traffic and perform the usual NAT operation. Entries maintained by a DS-lite CGN device in its BIB (binding information base) assume the manipulation of a specific parameter that will unambiguously identify the CPE to which return traffic will be forwarded. Typically this parameter is the IPv6 source address used by the CPE to forward privately addressed IPv4 traffic toward one of the available CGN capabilities that are deployed in the network.

Obviously, DS-lite designs assume an upgrade of the existing CPE so that it can support an IPv4-in-IPv6 encapsulation scheme. In addition, CPE devices need to be provisioned with the IPv6 reachability information of the CGN.

Some might object to this kind of approach, arguing that it sustains the use of IPv4 instead of moving toward IPv6. In reality, DS-lite CGN technology can be seen as a true catalyst of IPv6 deployment because it requires that at least the access infrastructure is IPv6-enabled, which is not true of a double-NAT approach.

The Impacts of CGN

The introduction of CGN capabilities into networks raises a number of issues, the most important of which is the handling of user-generated content (UGC), meaning content that is provided and maintained by customers and that need to be accessed from the Internet. A UGC context assumes the ability to assign a specific port number to the device that supports such contents within the customer premises (for example, Port #80 for a website).

This is currently handled in some environments by means of an Internet gateway device (IGD) protocol machinery specified by the UPnP (Universal Plug and Play) forum, where the terminal that maintains the contents will send a port number allocation request to the CPE, which will, in turn, manage the corresponding pinhole.

In a DS-lite CGN environment, there is no NAT capability activated in the CPE anymore, hence raising an important UGC-inferred issue. From this perspective, the IETF has recently chartered a working group to specify the port control protocol (PCP) that aims to control a CGN (or a firewall) for port-number-management purposes.

The PCP protocol relies upon a simple, client/server architecture. The PCP client can be embedded in the CPE, which, in this case, acts on behalf

Continued on next page

Zero addresses, continued

of the terminals connected to the CPE. This assumes the availability of an interworking function that, for instance, will convert IGD-formatted port number allocation requests into PCP-formatted messages that can be sent to a PCP server.

Upon receipt of a PCP request message, the PCP server will then solicit the CGN to make sure the request can be satisfied (such as by allocating several port numbers to a given customer during a limited period of time). The base PCP protocol specification is expected to be published as a Standards Track RFC before H2 2011 and is seen as a key asset by some service providers for consolidating CGN design.

CGN designs are not solutions to the global IPv4 address depletion; rather, they are meant to rationalize global IPv4 address usage during the transition period. They should not be regarded as alternatives to the deployment of IPv6; they should, in fact, encourage it.

France Telecom and IPv6

In 2008, France Telecom launched the IPv6 group-wise programme after more than 10 years of expertise in IPv6. The purpose of the programme is to define the group's IPv6 strategy and support enforcement of this strategy by contributing to country-specific IPv6 projects being developed by the group's affiliates.

The programme covers both residential and corporate markets and encompasses both fixed and mobile environments. It is organized into three major phases:

- Phase 1 (2008–2010) focused on introducing elementary IPv6 capabilities into networks (including management of IPv6 addressing schemes, IPv6 forwarding and routing policies, IPv6-inferred devices, and customer management policies) and restricting the scope of the service to Internet access alone.
- Phase 2 (2009–2012) focuses on IPv6 instantiation of the whole range of service offerings provided by France Telecom, including advanced IP services, such as voice-over-Internet-Protocol (VoIP) and Internet Protocol television (IPTV) as well as emerging services, such as machine-to-machine communication,
- Phase 3 (2012 and beyond) will mean the introduction of IPv6 customers, networks, and services, yielding the design and the deployment of IPv6-only access and backbone infrastructures according to the revisited Pv4 address-depletion forecasts.

Service-wise, the group's IPv6 strategy relies on a dual-stack architecture. Figure 1 offers a high -level, networking overview of this approach for fixed environments.

In this architecture, CPE devices become dual-stack routers that are dynamically assigned an IPv6 prefix by means of DHCPv6 (dynamic host configuration protocol for IPv6).

Both corporate and residential CPE devices are assigned a /56 prefix by default (in RIPE-dependent regions), but corporate customers can request the assignment of /48 prefixes as an option of the IPv6 virtual-private-network service offering that was launched in May 2009 (see http://www.orange-business.com/en/mnc2/footer/news/enterprise_briefing/april2009/technology.jsp, for example).

For fixed environments, this design will inevitably include DS-lite CGN capabilities for the reasons that have been discussed earlier.

The corresponding design depends on the distribution of DS-lite CGN capabilities that are, from an IP-forwarding standpoint, as close to the customer as possible. This is for several reasons, including performance (efficiency of the forwarding policy, time to access the service) and scalability (the number of customers to be serviced by a given DS-lite CGN capability will be equivalent to the number of customers who are currently connected to a given digital subscriber line access multiplexer, or DSLAM, device.

Mobile Services

The release 9 of the 3rd Generation Partnership Project specifications allows access to IPv4- and IPv6-formatted content using a single packet-data-protocol (PDP) context, hence an

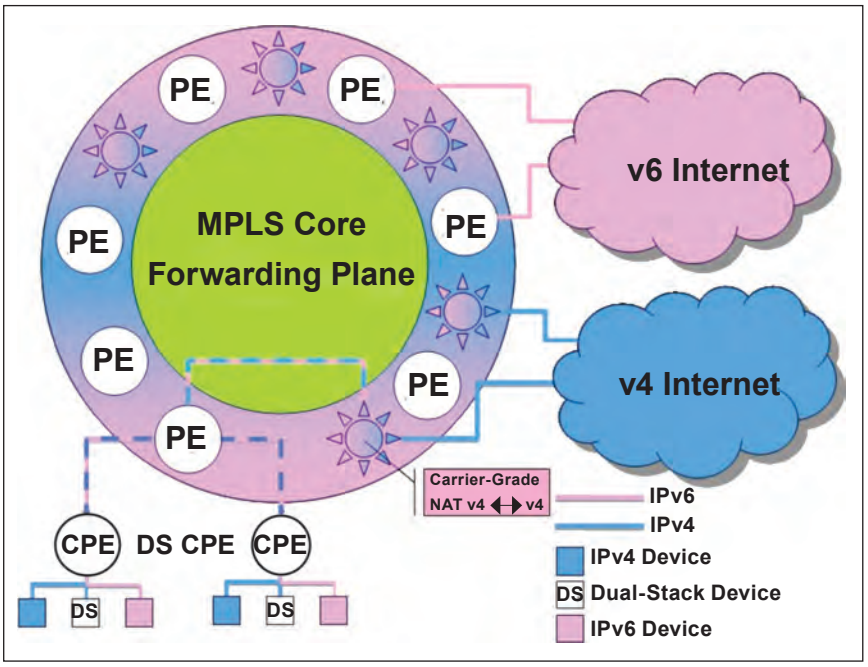


Figure 1: Dual-Stack architecture (networking view)

optimization of bandwidth resources. Applications should be address-family independent, meaning they should be used indifferently over an IPv4 or IPv6 stack so as to avoid any extra mobile handset complexity or cost for the customer while migrating towards IPv6.

Within this context, IPv6-only PDP contexts will be established and access to IPv4-formatted content will rely on NAT64 capabilities to be deployed in the network (such as at the GGSN, or gateway GPRS support-node, level in 3G environments).

VoIP Services

Migration of VoIP services towards IPv6 will be gradual: IPv6 capabilities will first be introduced in the access-network infrastructure, meaning that access-session-border-controller devices become dual stack while the core of the network will remain IPv4.

CPE devices also embed an IPv6 session-initiation-protocol user agent.

IPTV Services

Very often, existing IPTV services rely on a walled-garden design, wherein private IPv4 addressing schemes are used in overwhelming numbers, hence lowering the pressure to move towards IPv6. However, the simplification of access network infrastructures assumes the allocation of a unique, global IPv4 address to the CPE in order to access the network. As a consequence, IPTV services will be impacted by the global IPv4 address depletion. Similarly, as IPTV services evolve, they will likely include access to content located on the Internet. In that case, IPTV services would encompass so-called Web TV services, which naturally assumes a global IP addressing scheme, which will encourage the use of IPv6.

Finally, we can expect homogenization of the IP interface through which a whole range of services can be accessed. As Internet services move toward a progressive introduction of IPv6 capabilities in network and service infrastructures (which it will need to do in order to access and deliver content), access to IPv6-formatted IPTV content becomes straightforward. And since multiprotocol label switching contributes to the overall QoS enhancement, it will become the primary forwarding scheme for conveying both IPv4- and IPv6-formatted content.

The introduction of IPv6 in set-top boxes will primarily impact applications that solicit the network layer, such as when selecting a television programme or conducting a personal videoconference.

Current Status

Twelve country-specific IPv6 projects have been initiated since 2010, yielding IPv6 pilot deployments in Belgium, France, Moldova, Poland, Romania, and Senegal.

Additional field trials will begin in 2011 while commercial IPv6 connectivity service will be available as early as 2012 for some country affiliates. These field trials will cover the scope of the migration phase of the programme, meaning some of the group's affiliates will experiment with IPv6-enabled VoIP and IPTV services.

Lessons Learned

The IPv6 projects that were launched back in 2009 demonstrated that evangelization is key: decision makers need to thoroughly understand that there is no way but the IPv6 way if we are to sustain existing business and develop new markets.

We have also learned that IPv6 deployment should not be presented as a tedious and complex set of isotropous operations (while major technological locks reside in the CPE devices and the IT infrastructure, there are not many in the network itself).

The IPv6 projects that were launched back in 2009 demonstrated that evangelization is key: decision makers need to thoroughly understand that there is no way but the IPv6 way if we are to sustain existing business and develop new markets.

Rather, IPv6 evangelists should promote the tremendous opportunities in terms of business development as well as cleaning up network designs that have proven to be inefficient, particularly when it comes time to forward VoIP or IPTV traffic.

The forthcoming transition period will undoubtedly bring some difficulties, including the need for service providers to guarantee IPv4 service continuity when it will not be possible to assign a global IPv4 address to each and every (new) customer, which is likely to degrade the quality of service, particularly for those customers who will be serviced by a CGN. Even so, this does not mean we should not be encouraging, if not accelerating, migration toward IPv6.

Last, but not least, there are still some vendors (mostly in the CPE and set-top box areas) who are not yet IPv6-minded. The oft-repeated "lack-of-business drivers" argument is no longer convincing thanks to a set of consolidated positions from the service and content providers' communities.

From that standpoint, standard bodies (and especially the IETF) have a key role to play in the promotion of IPv6: it is not only a matter of making sure the voice of service and content providers can be heard (by vendors), but also making sure that the standardization effort remains focused on IPv6 deployment issues.

The clock is ticking, and we must be on IPv6 time.

RPKI: One Perspective on Implementation

By Alex Band

This is an invited article to describe a specific implementation and operational perspective on a developing IETF specification, RPKI.

Routing on the Internet is a system that depends on every network operator working together, and in most cases working around other people's mistakes by routing differently until the source problem is fixed. Today, the vast majority of mis-announcements are accidental originations of someone else's prefix. But routing errors have a high customer impact because entire networks can become unreachable. In a sense, we are lucky that more problems do not occur, and we can still point to the YouTube vs. Pakistan Telecom incident as a recent example, even though that happened in early 2008. Still, there is an urgent need to make this system more robust before a routing event occurs that causes major, widespread problems.

Now that there are no longer any IPv4 addresses in the IANA pool, the registry function of the five regional Internet registries (RIRs) is more important to the Internet community than ever. People are going to be searching all nooks and crannies for the remaining IPv4 addresses and this may not always be done in an orderly fashion. It is extremely important to know who is the legitimate holder of a block of IP addresses.

This has always been one of the main drivers behind the RIRs' plans to deploy a system that attaches digital certificates to Internet number resources (IP address blocks and AS numbers). This resource certification system is based on PKI (Public Key Infrastructure) principles. A *resource certificate* is an electronic document proving that its holder has been officially assigned or allocated a particular Internet resource, which means a block of IPv4 or IPv6 addresses, or an AS Number. This takes shape in the form of an X.509 certificate with "Extensions for IP Addresses and AS Identifiers" as described in RFC 3779.

Even though the vulnerabilities of Border Gateway Protocol (BGP) were identified in the 1980s, work on making it more robust started in 2000, when Stephen Kent, Charles Lynn, and Karen Seo published *Secure Border Gateway Protocol (S-BGP),* their paper on Secure-BGP. The goal is to perform origin validation to prevent damage caused by accidental misconfiguration and misorigination. Preventing malicious attacks requires path validation, which is a lot more complex to solve. Discussions on a recharter of the IETF Secure Inter-Domain Routing working group to cover this aspect have recently started (see http://www.ietf.org/mail-archive/web/sidr/current/msg02396.html).

In 2006, the RIPE NCC started working on a resource certification system. ARIN and APNIC had started work on an implementation a year before that. Resource certification mirrors the way in which Internet number resources are distributed. That is, resources are initially distributed by the IANA to the RIRs, which in turn distribute them to local Internet registries (and, in some regions, national Internet registries), which then distribute the resources to their customers. In this implementation, initially the RIRs become *certificate authorities,* issuing X.509 certificates along with Internet resources.

Since the launch of the Resource Certification service in the beginning of this year, hundreds of local Internet registries (LIRs) have enabled the service, providing them with several benefits.

First, certification verifies the legitimacy of a resource's allocation or assignment by an RIR. In other words, it offers validated proof of holdership. This can be vital when transferring Internet resources between parties. How can you confirm who is the rightful holder of the addresses? How can you be sure this block hasn't already been sold? Certification helps to make resource transfers reliable and secure.

Second, there is the routing aspect. It's one thing to have people claim address blocks that are not theirs, it's another for them to actually use those addresses on the Internet. We live in a world where any network operator can announce any prefix on their router, either intentionally or by mistake. We currently have Internet routing registries (IRRs) to help mitigate this issue, but there are more than 30 IRRs, with no means of confirming that all of the information in those IRRs is actually correct.

Now that there are no longer any IPv4 addresses in the IANA pool, the registry function of the five Regional Internet Registries (RIRs) is more important to the Internet community than ever.

The resource certification system allows for the prefix holder checking to be automated in a dependable, transparent, and standardized way. It has the potential to streamline ISP workflows while facilitating better routing security.

The system works through the creation of Route Origin Authorization (ROA) objects. An ROA is a standardized document stating that the holder of a certain prefix authorizes a particular Autonomous System (AS) to announce that prefix. A valid ROA can only be created by the holder of the certificate for that address space. Anyone on the Internet can now validate if a

route announcement is authorized by the legitimate holder of the address space. Several router manufacturers have committed to building certification support into their hardware, further expanding the potential.

When building the roadmap for the certification service the RIPE NCC offers, we had to make critical decisions on which features to offer that the standards describe. We made a conscious choice to start with a limited feature set, and expand it over time as the IETF standards matured. In order to make the entry barrier into the system as low as possible, initially we are providing a hosted solution only. This means an LIR can log into a secured portal and generate a resource certificate covering their Internet number resources. The certificate is generated on the system and it not retrievable from the hardware security modules (HSM) we have in place. This creates a dilemma, because anyone who understands security will argue that you should always be the holder of your own private key, in all cases.

How can you confirm who is the rightful holder of the addresses? How can you be sure this block hasn't already been sold? Certification helps to make resource transfers reliable and secure.

In the end, though, we felt that quite a number of organizations would understand and accept the security trade-off of not being the owner of the private key for their resource certificate and trust their RIR to run a properly secured and audited service. Moving forward, we will focus on expanding the feature set of the service by making it possible for LIRs to run their own, local certificate authority that interfaces with the RIPE NCC.

Second, we will build a notification system that warns the user if ROAs do not match real-world routing and lastly, we will work on a more comprehensive validator.

For more information, please visit http://ripe.net/certification.

Alex Band is product manager at the RIPE NCC

Internet Society, Standards Work Draw ICT Professionals to IETF 79

Four information technology professionals from Africa, Asia, and South America attended their first IETF meeting in November 2010 as part of the Internet Society's Fellowship to the IETF Programme. Now in its sixth year, the programme, which operates under the aegis of the Internet Society'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.

IETF 79 First-time Fellows
Odira Elisha Abade (Kenya)
Jeronimo Bezerra (Brazil)
Khoudia Gueye Sy (Senegal)
Yoon-Kit Yong (Malaysia)

IETF 79 Mentors
Richard Barnes (BBN Technologies)
Randy Bush (Internet Initiative Japan)
Ross Callon (Juniper)
Marshall Eubanks (Iformata Communications)
Cristel Pelsser (Internet Initiative Japan)
Atarashi Ray (Internet Initiative Japan)

Returning Fellows
Baasansuren Burmaa (Mongolia)
João Marcelo Ceron (Brazil)
Sandra L. Céspedes (Colombia)
Dorcas Muthoni Gachari (Kenya)
Fernando Gont (Argentina)
Muhammad Haris Shamsi (Pakistan)
Pedro Rodrigues Torres, Jr. (Brazil)
Carlos Alberto Watson Carazo (Costa Rica)


Jeronimo Bezerra (Brazil)


Khoudia Guey Sy (Senegal)


Yoon-Kit Yong (Malaysia)


Odira Elisha Abade (Kenya)


Internet Society Fellows and Returning Fellows at IETF 79 in Beijing

For more information, see http://www.InternetSociety.org/leaders

The Untethered Future of the Internet

By Leslie Daigle

RFC 1122: Requirements for Internet Hosts—Communication Layers and RFC 1123: Requirements for Internet Hosts—Application and Support lay out the basic, somewhat idealized, expectations of Internet hosts, circa 1989. As we look at the Internet that exists today, we can see that much has already changed from the ideal laid out in those documents, with more change to come as people increasingly use devices that can operate "untethered"—from any particular network, or fixed source of power. This article reviews the historical perspective from those documents, looks at today's reality in comparison, and draws some conclusions about the approach to updating our notions of Internet host requirements in the face of future realities for devices and the Internet.

RFC 1122 and 1123 lay out the basic, somewhat idealized, expectations of Internet hosts, circa 1989. They acknowledge that the Internet's reality was changing, and expressed the expectation that updates would follow. In point of fact, there have been no major updates (beyond RFCs updating specific points of protocol usage), and these documents remain the baseline ideal for Internet host requirements.

These RFCs enumerate standard protocols that a host connected to the Internet must use, with the expectation that the specifications of these documents "must be followed to meet the general goal of arbitrary host interoperation across the diversity and complexity of the Internet system." These documents recognize that Internet hosts span a wide range of size, speed, and function, ranging in size "from small microprocessors through workstations to mainframes and supercomputers", and ranging in function from "single-purpose hosts (such as terminal servers) to full-service hosts that support a variety of online network services, typically including remote login, file transfer, and electronic mail."

To give a sense of the expectations from those documents, their introductory paragraphs outline:

A host computer, or simply "host," is the ultimate consumer of communication services. A host generally executes applications programs on behalf of user(s), employing network and/or Internet communication services in support of this function. […]

An Internet communication system consists of interconnected packet networks supporting communication among host computers using the Internet protocols. The networks are interconnected using packet-switching computers called "gateways" or "IP routers" by the Internet community[…].

The current Internet architecture is based on a set of assumptions about the communication system. The assumptions most relevant to hosts are as follows:

(a) The Internet is a network of networks.

Each host is directly connected to some particular network(s); its connection to the Internet is only conceptual. Two hosts on the same network communicate with each other using the same set of protocols that they would use to communicate with hosts on distant networks.

(b) Gateways don't keep connection state information.

To improve robustness of the communication system, gateways are designed to be stateless, forwarding each IP datagram independently of other datagrams. As a result, redundant paths can be exploited to provide robust service in spite of failures of intervening gateways and networks. All state information required for end-to-end flow control and reliability is implemented in the hosts, in the transport layer or in application programs. All connection control information is thus colocated with the end points of the communication, so it will be lost only if an end point fails.

(c) Routing complexity should be in the gateways.

Routing is a complex and difficult problem, and ought to be performed by the gateways, not the hosts. An important objective is to insulate host software from changes caused by the inevitable evolution of the Internet routing architecture.

(d) The System must tolerate wide network variation.

A basic objective of the Internet design is to tolerate a wide range of network characteristics—e.g., bandwidth, delay, packet loss, packet reordering, and maximum packet size. Another objective is robustness against failure of individual networks, gateways, and hosts, using whatever bandwidth is still available. Finally, the goal is full "open system interconnection": an Internet host must be able to interoperate robustly and effectively with any other Internet host, across diverse Internet paths.

Experiences of the past 20 years have already challenged some of the key points in RFCs 1122, 1123. The development and deployment of network address translators (NATs), as a mechanism for using a single IP address to give several computers access to the Internet, inherently challenges some of the principles of "Internet host." Either the NAT "is" the Internet host, or the computers behind it are nonconforming hosts (because they are not individually addressable on the Internet—the "end to end" principle outlined in 1122/1123).

Nor do Internet hosts typically conform to the applications expectations outlined in RFC 1123. In general, there has been a trend away from having each Internet host running a full suite of application services. The endpoints that Internet service providers enabled by providing access to home consumers were not naturally equipped or maintained as host servers. ISPs prevented,

or charged extra ("business service") for customers running their own server software (Web, mail, other). This was argued on the basis that these servers generated unwanted traffic—either in terms of legitimacy (spam) or simply volume.

As the final unused IPv4 addresses are assigned, further distance from the requirements outlined in RFC 1122/23 can be expected in the IPv4 Internet, at least, with the deployment of "Carrier Grade NATs" (CGNs), which share a single IP address across multiple customer (networks) at a time.

There is little argument that the Internet is still in full "growth mode". More users are coming online, and more people have more devices connected to the Internet at any given time, between their desktops, laptops, and (smart) mobile phones. They may even have some of which they are not aware—their home entertainment boxes, their thermostats, and maybe eventually their refrigerators.

The development and deployment of network address translators (NATs), as a mechanism for using a single IP address to give several computers access to the Internet, inherently challenges some of the principles of "Internet host."

Some "size" numbers, from http://www.idc.com/about/viewpressrelease.jsp?containerId=prUS22110509&sectionId=null&elementId=null&pageType=SYNOPSIS:

"There were more than 450 million mobile Internet users worldwide in 2009, a number that is expected to more than double by the end of 2013. Driven by the popularity and affordability of mobile phones, smartphones, and other wireless devices, IDC's Worldwide Digital Marketplace Model and Forecast (an IDC Database service) expects the number of mobile devices accessing the Internet to surpass the one billion mark over the next four years.

[...]

The most popular online activities of mobile Internet users are similar to those of other Internet users: using search engines, reading news and sports information, downloading music and videos, and sending/receiving email and instant messages."

and

"• More than 1.6 billion devices worldwide were used to access the Internet in 2009, including PCs, mobile phones, and online videogame consoles. By 2013, the total number of devices accessing the Internet will increase to more than 2.7 billion.

• China continues to have more Internet users than any other country, with 359 million in 2009. This number is expected to grow to 566 million by 2013. The United States had 261 million Internet users in 2009, a figure that will reach 280 million in 2013. India will have one of the fastest growing Internet populations, growing almost two-fold between 2009 and 2013."

Apart from the obvious indicators of growth, what these data show is that the future Internet will feature many more untethered devices, and, importantly, that people expect to be able to do all their "usual" Internet activities while on the move.

The realities faced by mobile and other networks of small devices (sensor networks) were discussed during the week of IETF 79 at an Internet Society hosted panel discussion (see page 5). Some of the issues identified are not actually new—constrained bandwidth, concerns about processing power being insufficient to support the full Internet protocol suite. However, the shear number and scope of the expected growth in the area of Internet access through mobile handsets, sensor networks, etc, suggest that the expected impact and design decisions should be reviewed.

Untethered devices are typically more constrained in their processing capabilities than traditional Internet hosts. Sensor hardware development has pushed back on implementing the full Internet protocol stack on the claim of lack of processing capability (and lack of perceived need for all those features). While the modern smartphone has more processing power than the average Internet host had when 1122/23 were written, their display and input capabilities are still quite limited as compared to more general purpose Internet hosts.

Power is a real concern for untethered devices: it is finite. Furthermore, it may be necessary to ensure some power reserves in order to carry out a primary function (e.g., make a phone call; communicate an update from a sensor, etc). Therefore, untethered devices tend not to be "always on", and can't reasonably be the policy enforcement point for deciding which traffic to ignore: unwanted traffic is expensive, and a device that is deciding whether it is acceptable or not has already received at least some portion of the traffic.

Connectivity often poses a problem, as well. Bandwidth may be relatively constrained, and is currently costly to the end user. These are somewhat tied to business models of the access providers, but those, in turn, are influenced by the finite availability of spectrum, and the costs of obtaining licenses, for example.

Altogether, these untethered devices highlight further possible stretching of the expectations of Internet hosts. The number of users (people) associated with a given host may be 0 (sensor), 1 (mobile handset), or several (server machines, shared computers), or even fractional

Continued on next page

The Untethered Future, continued

(one user's context spread across several devices). This has implications in terms of expectations for identifiers—for hosts and for users. In today's Internet, there is an (often inaccurate) operational assumption that individual accountability can be tied to an IP (host) address. This will be increasingly inaccurate as the model of users-to-connections evolves.

The challenge, going forward, will be to determine which of these present new Internet architecture design requirements, because of a change in nature or scale, and which of them represent technology growing pains that have been seen before and will be overcome again.

Certainly, there is, and has long been, work done within the IETF to address some of the base issues. There have been a number of working groups focused on mobile IP (Mobile IP WG and follow on work) and policy frameworks (e.g., COPS-PR—RFC3084). Application protocols have looked to accommodate different user realities (numbers of users per device, device capabilities, etc). Delay Tolerant Networking has explored the issue of handling networking in a context with unprecedented round trip times and other related constraints—in interplanetary IP. And there are ongoing discussions of whether or how to introduce new identifiers within the application or routing infrastructures. Each represents a fascinating challenge in its own right. The questions raised, but not answered, during the briefing panel, suggest answers that run through the fabric of many working groups, recognizing the changing landscape of Internet hosts, rather than point solutions.

The open Internetwork application framework is what has permitted the creation of novel applications without requiring permission from network operators or device manufacturers for deployment.

The notion of connectivity is put into question by untethered devices that must cope with power reserve limitations. Rather than being always-on, always-reachable, individual hosts may choose to be selective about the time and type of connections accept. This is consistent with the 1122/23 model of putting control at the endpoints, but challenges the premises of supporting a set of always-on services in each conforming Internet host. Alternatively, considering a "split node" approach, with a set of policies implemented on a fixed server governing policies for which traffic gets forwarded to the untethered device, would allow the support for those application services in the split-node host, but may challenge the principle of putting the control at the endpoint (untethered device, in this case).

Untethered devices further challenge the notion of network positioning: future Internet hosts may be stable in the network, mobile within one network type, mobile between network types (e.g., wifi and mobile data), or even providing multiple network interfaces with different policies in place at the same time. That is, a mobile handset may be open to all traditional Internet host connections over the wifi interface, but operating in selective mode over a mobile data network, at the same time.

Perhaps the best way to look at the future is to look away from the trendlines, and focus on "what good looks like".

For users, the important thing is for their experience of Internet-delivered services to be consistent across network locations and hosts. In the last decade, this has been at the heart of arguments for a single DNS root, and efforts to prevent "balkanization" of the Internet. The principle is important, going forward, even as the differences of access platforms will necessarily challenge the definition of "same".

Diversity and openness remain critical in Internet deployment, in order to continue to foster innovation. 1122/23 stress the importance of recognizing that individual networks would be set up and operated according to local design choices. The open Internetwork application framework is what has permitted the creation of novel applications without requiring permission from network operators or device manufacturers for deployment. The World Wide Web was one such idea that took hold like wildfire. Time and again, users and usage of Internet have laid the groundwork for the Internet's evolution, not some master control. It's important to retain the ability to support that kind of innovation and open experience, as provided for in the hosts requirements in 1122/23. In that light, the notion of an open standard "split node" model, with individual users establishing and controlling preferences for policies, would allow more growth and innovation than, for instance, "one size fits all" policy assumptions implemented as network operator private controls.

In the end, then, it's clear the future Internet will support many users and uses based on untethered devices, and thus feature hosts that exceed the expectations of 1122/23. But the framework in those documents is sound: provide a set of requirements for interoperation at the transport and application levels, and unfettered innovation will follow. Time will tell whether the requirements of hosts are updated to accommodate the practical realities of power and bandwidth constraints understood with untethered devices, or whether the "host" will become some tethered server supporting multiple roaming devices, for example. The only wrong choice is no choice at all.

IRTF Update

By Aaron Falk


Aaron Falk, IRTF Chair

What follows is a summary of the IRTF chair's report, which was delivered during the IETF 79 technical plenary. Four of the 13 Internet Research Task Force (IRTF) research groups (RGs) met during the week:

- Scalable, Adaptive Multicast RG
- Host Identity Payload RG
- Delay Tolerant Networking RG
- Virtual Networks RG

The RFC Editor published an RFC from the Peer-to-Peer RG, RFC 6029: A Survey on Research on the Application-Layer Traffic Optimization (ALTO) Problem. Internet drafts from the Routing, Mobility Optimization, and Internet Congestion Control RGs are nearing publication.

An email list has been created for discussion of topics related to the IRTF, specifically including discussion of the creation of new RGs. The list is irtf-discuss@irtf.org and the subscription page is https://www.irtf.org/mailman/listinfo/irtf-discuss.

Two new topics continue to be discussed as possible RGs. The first is machine learning and communications systems (as described in draft-tavernier-irtf-lccn-problem-statement-00.txt), which focuses on how learning algorithms can be utilized within network nodes or collections of network nodes to adapt their behaviour in response to external events, such as traffic or failure conditions. The second is the "Internet of Things." Topics of interest in this area include building networks, emergency networks, and naming services, among others.

As a postscript to my report from IETF 79, I would like to add an update on the role of IRTF chair. On 29 November 2010, the Internet Architecture Board (IAB) announced the selection of Dr. Lars Eggert as the new IRTF chair. Lars is a principal scientist at Nokia Research Center in Helsinki, Finland, and a member of Nokia's CEO Technology Council. He is also an Adjunct Professor at Aalto University. Lars has worked on research projects ranging from internetwork architecture, transport protocols, virtual networks to resource scheduling. He is a senior member of the ACM and the IEEE, an individual member of the Internet Society, and an active participant in the IRTF and IETF, where he currently serves as area director of the Transport Area. Lars serves on the programme committees of several ACM and IEEE conferences and workshops as chair and member, such as IEEE Infocom. Before joining Nokia in 2007, Lars was a senior researcher at the NEC Network Laboratories in Heidelberg, Germany. He received a Ph.D. in Computer Science in the fall of 2003 from the University of Southern California (USC) where he was a graduate research assistant at USC's Information Sciences Institute (ISI). Lars will start his role as IRTF chair during the IETF 80 week. He brings a wealth of leadership experience in Internet research and engineering and will be an excellent chair of the IRTF. Welcome, Lars!


From left, IETF chair Russ Housley, Internet Society president and CEO Lynn St.Amour, itojun Service Award recipient Bjoern A. Zeeb, and WIDE Project director Jun Murai at IETF 79 in Beijing.

Prof. Xing Li of Tsinghua University addressing IETF 79 participants in Beijing.

Attendees taking a break between sessions at IETF 79.

Photos/Peter Löthberg

IETF Meeting Calendar

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

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

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

IETF 83
25–30 March 2012
Host: TBD
Location: Paris, FR

For more information about past and upcoming

IETF Meetings

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

Special thanks to

Tsinghua University
Internet Society of China
China Internet Network Information Center

for hosting IETF 79

The Internet Society Fellowship to the IETF is sponsored by

Afilias Global Registry Services
Google
intel
Microsoft
Backing from nominet trust

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

Afilias Global Registry Services
ARIN
comcast
Ripe NCC
SIDN
Tsinghua University
WIDE Project

IETF® Journal
IETF 79
Volume 6, Issue 3
March 2011

Published three times a year by the Internet Society

Galerie Jean-Malbuisson 15
1204 Geneva
Switzerland

Editor
Mat Ford

Associate Editor
Wendy Rickard

Contributing Writer
Carolyn Marsan

Editorial and Design
The Rickard Group, Inc.

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

Editor's Note:
The IETF Journal adheres to the *Oxford English Dictionary* Second Edition

Internet Society