IETF

IETF Journal

IETF 69 • Chicago
October 2007
Volume 3, Issue 2

Published by the Internet Society in cooperation with the Internet Engineering Task Force

Inside this issue

IPv6 Captures the Spotlight at IETF 69

From the Editor's Desk, by Mirjam Kühne

If it were possible to assign a theme to the IETF 69 meeting in Chicago last July, the obvious choice would be IPv6. Now that IPv6 has become an integral part of the community, as evidenced by the number of working groups that are connected to it, it is the actual deployment of IPv6 that is capturing the attention of the IETF.

A good place to start is the summary of a special meeting that took place at IETF 69 with the IESG and the IAB (see below). The purpose of the meeting was to find out what the IETF can do to help with the deployment of IPv6. Similarly, Shane Kerr takes a look at the historical development of IPv6 in an effort to determine if opportunities were missed then and, if so, whether they might offer useful lessons on the deployment issues we face now. (See page 9.)

Photo by Alexandru Petrescu

Chicago, site of IETF 69

One topic that frequently comes up in discussions of IPv6 deployment is network address translation (NAT). For many, NAT is a fact of life when it comes to working with and around IPv4. It's also possible that ignoring that reality could mean missing the opportunity to standardise IPv6. Lixia Zhang offers her perspective on page 14.

Another notable event at IETF 69 was an informal panel discussion with several IAB members and former IETF chair Brian Carpenter. The discussion, organised by the ISOC Chicago chapter, offers interesting insights into the challenges that await the IETF as the Internet grows. (See "ISOC Chicago Arranges for Experts' Panel at IETF 69" on page 25.)

As always, we wish you fun reading, and we welcome both your comments and your contributions for future issues of this publication.

Paving the Way for IPv6

Community meets to discuss the challenges

At a joint IESG–IAB meeting, participants discussed the deployment of IPv6, the state of the IPv4 address pool, the challenges of both, and what the IETF can do about it all.

While predictions about timing may vary, there is virtually no disagreement that IPv4 addresses will, at some point, become unavailable. This concern has been the subject of debate and discussion among participants of the IETF and others for more than two decades. It also has been the key driver in the development and deployment of a number of new technologies, including IPv6. The IETF Journal was invited to join the discussion as part of a joint IAB–IESG meeting held in July in Chicago at IETF 69. What follows is a report by the *IETF Journal* on what transpired during that single meeting, one of several on this important topic. The discussion was led by Kurtis Lindqvist and Jari Arkko.

Continued on page 7

Message from the IETF Chair

By Russ Housley


Russ Housley, IETF Chair

By all accounts, IETF 69 was a success. Held in a grand hotel in downtown Chicago, we had in attendance 1,146 people from 40 countries. In spite of the noise from ongoing renovations to the hotel, progress was made in a number of working groups.

IETF 69 was hosted by Motorola, and the site network was subcontracted to Verilan Networks. As always, we depended on a team of dedicated volunteers. The week was filled with the usual mixture of working group meetings, BoF (birds-of-a-feather) sessions, research group meetings, and countless side meetings.

It was interesting to hear from Ken Zdunek, vice president of networks research at Motorola, which hosted IETF 42 in Chicago as well. Ken talked about the ways in which Chicago and the Internet have changed over the past nine years.

Since IETF 68, two new WGs were chartered and 10 WGs were closed. During that time, the WGs and their individual contributors produced 436 new drafts and generated 946 updated drafts. There are still approximately 120 chartered WGs. The Internet Engineering Steering Group approved 96 drafts for publication as requests for comments (RFCs). The RFC Editor published 103 new RFCs.

The RFC Editor contract was renewed with the University of Southern California's Information Sciences Institute (ISI). As most of you know, ISI has filled this role since the RFC series began. An RFC Editor style guide has been published and is available at http://www.rfc-editor.org/howtopub.html.

In addition, the IETF Secretariat Services request for proposals (RFP) was released on schedule, and the goal is to award one or more contracts in October 2007. The tools team did an outstanding job of rewriting all tools that do not require log-in—so as to resolve security flaws in those tools. As a next step, tools that require log-in will be rewritten to deal with their security issues.

One of the hot topics at IETF 69 was the transition from IPv4 to IPv6. The hope was to identify specific actions the IETF can take to facilitate a smooth transition. In the past, the IETF has operated on the assumption that the transition will occur before the IPv4 address space is exhausted. However, there is an increasing realisation that this may not be the case. The discussions at IETF 69 were attempts to revisit the topic. A variety of opinions were expressed, and a lively discussion ensued at the plenary, but ultimately, no consensus was reached on what the IETF can do right now. I believe this discussion will continue and that the IETF has a valuable contribution to make in this area.

I look forward to seeing you at IETF 70 in Vancouver on 2–7 December 2007 and at IETF 71 in Philadelphia on 9–14 March 2008. As always, scheduling information for upcoming IETF meetings may be found at http://www.ietf.org/meetings/meetings.html.

New BoF Meetings

Descriptions and agendas for all BoF meetings can be found at http://www.ietf.org/meetings/past.meetings.html.

Applications Area
biff: Notification from Mail Stores
httpbis: HyperText ransport Protocol Bis
vcarddav: vCard and CardDAV

Operations and Management Area
apm: Application Performance Metrics
nee: Netconf Extensions and Evolution
xsdmi: XSD for accessing SMIv2 data models

Security Area
tam: Trust Anchor Management


Olaf Kolkman, IAB Chair

Words from the IAB Chair

By Olaf Kolkman

The Internet Architecture Board (IAB) has a number of responsibilities, one of which is to maintain relationships between the IETF and external organisations. RFC 2850 describes the process in the following manner:

> The IAB acts as representative of the interests of the IETF and the Internet Society in technical liaison relationships with other organisations concerned with standards and other technical and organisational issues relevant to the world-wide Internet.

Relationships

The IETF has an intensive relationship with the Telecommunication Standardisation Sector of the International Telecommunication Union (ITU-T). In addition to serving as general liaison to the organisation, we have liaisons for MPLS (Multiprotocol Label Switching), NGN (Next Generation Network), and Study Group 15. We invited the ITU-T leadership to an informal meeting on the Saturday prior to the Chicago IETF for the sole purpose of getting to know the faces behind the e-mail addresses and to have an informal discussion about the things that drive our respective organisations. The get-together was motivated by the notion that collaboration is most effective and fruitful when personal contacts are established.

Several topics were discussed during the meeting. One in particular had to do with IETF concern over the use by Transport MPLS of the MPLS Ethertype, which was formally raised by the end of the week.[1] Both the informal discussion and the liaison on T-MPLS are examples of how the working relationship between ITU-T and the IETF proceeds on a day-to-day basis.

On a more strategic level, the IAB has responded to a questionnaire in which the ITU was seeking input on its role in Internet policy and standards development. In our response,[2] we reiterated that the IETF is the standards organisation responsible for a number of the topics covered in the questionnaire and that the IETF has mechanisms in place for the ITU-T and the ITU membership to participate in the work.

Architectural work

Since the previous issue of the IETF Journal, a number of IAB architectural documents have appeared as RFCs:

- RFC 4840: Multiple Encapsulation Methods Considered Harmful
- RFC 4903: Multi-Link Subnet Issues
- RFC 4907: Architectural Implications of Link Indications
- RFC 4924: Reflections on Internet Transparency

Continued on next page

1. https://datatracker.ietf.org/documents/LIAISON/file470.txt.
2. http://www.iab.org/documents/correspondence/2007-05-21-itu-resolution-102.html.

IETF 69 Facts and Figures

Registered attendees	1146
Countries	40
New WGs	2
Closed WGs	10
New Internet-Drafts	436
Updated Internet-Drafts	946
IETF Last Calls	74
Approvals	96

RFC Editor Actions (March–June 2007)

103 RFC published of which

- 47 standards track
- 5 BCP

IANA Actions (March–June 2007)

Processed ~1900 IETF-related requests of which:

- 981 Private Enterprise Numbers
- 90 Port Numbers
- 124 TRIP ITAD Numbers
- 42 media-type requests

Completed IANA Actions for 84 documents becoming RFCs

Plenary Report

By Mirjam Kühne

Note: This is not a complete report of the plenary sessions; rather, it is a summary of the highlights of the discussions. All IETF 69 presentations can be found at http://www.ietf.org/meetings/past.meetings.html.


Mirjam Kühne

Unlike previous IETF meetings, the IETF 69 plenary did not feature a technical presentation. Olaf Kolkman explained that it can be a challenge to find good speakers and topics that are interesting and relevant enough for the entire IETF community. The open mic discussion that ensued prompted several suggestions, including one by Aaron Falk, chair of the Internet Research Task Force (IRTF), who proposed that more research topics be included, which, he said, might have the added benefit of encouraging more researchers to participate in the work of the IETF. Another participant added that it might be beneficial to have an IETF working group (WG) or an IRTF research group (RG) present its work to a wider audience, such as IETF plenary participants, if the scope of the work is not too narrow.

In general, it was agreed that the session would benefit from presentations that coherently address the larger challenges for the Internet—such as IPv4 address exhaustion and cybercrime—but not only from a technical perspective. In other words, the IETF should be thinking more about benefits for end users instead of thinking only about engineering issues. Former Internet Architecture Board (IAB) chair Leslie Daigle supported that position, saying it would be good for IETF meeting planners to think about what makes a topic relevant to the IETF. For example, is it something that requires action on the part of the IETF? Or is it a topic of imminent importance to the community? "We tended to shy away from this in the past few years," she said. IAB member Elwyn Davies added that the IAB is taking steps to address the wider community by, for example, working with ISOC to raise awareness of unwanted traffic.

After a lively discussion about IPv6, firewalls, NAT (network address translation), and NAT traversal mechanisms, one participant commented that 10 years ago, when he started working in the IETF, he believed that the architectural principles, such as the end-to-end principle, represented a shared vision. Today, he said, there doesn't seem to be much in the way of coherent work that spans multiple areas. Instead, narrow pieces of standards work are being done, all of which are driven by business and the marketplace. "Where is the end-to-end-principle in applications these days?" he asked. "That underlying principle made the Internet grow the way it did. If this is not a shared vision anymore, this will have to be discussed."

In response, another participant suggested looking more at conclusions than at principles. "End-to-end was a conclusion," he said. In the 1980s, he added, former IETF chair Dave Clark wrote a document that discussed where in the network might be the best point to put complexity. At the time, Dave came to the conclusion that complexity and management are best placed at the edges of the network, which meant that end to end was an important feature. Since then, circumstances have changed. Putting complexity at the edges is no longer a good idea; there are too many of them. Furthermore, neither is putting network management at the core of the Internet a good idea. The speaker suggested that today, complexity should be at the point between the intranets (internal networks) and the Internet. "That is the point network operators have control over and can manage," he said. "Does that mean we need to get rid of old principles if they no longer

IAB Chair, Continued from page 3

The IAB also held a retreat, kindly hosted by Harvard University, where we discussed ongoing business and possible future work. Although concrete work items have not yet crystallised, our discussions have focused on fundamental Internet protocol issues, such as the routing and addressing problem, IPv6 deployment, and architectural problems associated with Network Address Translation. I don't think it is a coincidence that these are the same topics that happened to have been discussed during the technical plenary at IETF 69 in Chicago. I have also observed that these are topics on which folks within the IETF—and hence also within the IAB—have different perspectives, particularly in how they view both the problems and the possible solutions.

See you all at IETF 70 in Vancouver in December.

apply? The most important goal is to keep the robustness of the Internet."

On the subject of firewalls, Thomas Narten warned the IETF not to make the same mistake it made in earlier days. As Thomas explained, in the past the IETF did not make recommendations on the behaviour and use of firewalls, because firewalls were generally seen as "a bad thing." This created a gap that was filled by the industry in a way that created inconsistencies. Consequently, firewalls do not work very well. "If we want the IETF to help make the Internet work better, we have to admit that we missed an opportunity with respect to firewalls," he said. "Now we have the opportunity to influence firewall behaviour in IPv6." The same, he said, applies to NATs. "The industry filled a gap because the IETF made no clear recommendations," Thomas said. "This means there's no predictability regarding how applications work. Now we're having the same discussion with IPv6: Do we need NAT-PT [IPv6 NAT]? No, we don't. But the reality is that people will create NATs in IPv6. The point is that with NAT-PT, we may be making a big mistake by leaving a vacuum out there."

Other speakers added that what seems to be missing is for the end hosts to tell the firewall what kind of traffic it wants to receive. (Note: NAT just happens to let traffic through, whereas the behaviour of a firewall is a policy decision.) This has not been developed or successfully deployed.

Brian Carpenter referred to a paper by Mark Handley titled "Why the Internet Only Just Works" (see http://www.cs.ucl.ac.uk/staff/M.Handley/papers/only-just-works.pdf).

As Handley says in the paper, the Internet is going to suffer growing pains as it moves from providing 80 percent of the functionality to providing more than 90 percent of the functionality, as called for by the new requirements. The track record, he writes, is not at all good. Historically, all of the major changes that were successful were implemented at the last minute. This, Brian pointed out, should not be a surprise. "There are always too many immediate issues to be concerned with to invest time and money on those that are not currently critical," he said. "And consensus for architectural change is very hard to reach unless you're faced with a specific and pressing problem."

Continued on next page

ISOC Fellowship Program

Five technologists, educators, and students from the developing world were named recipients of the Internet Society's Fellowship to the IETF. The fellows were selected prior to IETF 68 in Prague from a large pool of well-qualified applicants. In addition to the financial and administrative support that enabled the fellows to attend IETF 69 in Chicago, each fellow was paired with a mentor from the community of experienced IETF participants.

IETF fellows and mentors in Chicago

ISOC fellow Burmaa Baasansuren is director of the .MN ccTLD registry for Datacom, the Mongolian Internet service provider. Burmaa has an interest in issues related to the Domain Name System and IPv6. She was mentored by Marcos Sanz Grosson, deputy head of system development at DENIC, the ccTLD registry for Germany.

Sandra L. Céspedes is professor of information technology at ICESI University in Colombia. She is interested in the work of a number of IETF working groups, including ipv6, mipshop, sip, and manet. Sandra was mentored by Alain Durand, who is director of the office of the chief technology officer at Comcast.

Originally from Nepal, Raj Gurung is a graduate student in computer science at Western Illinois University. He, too, is interested in a number of working groups, including manet, mpls, IPv6, and dhc. Raj was mentored by Dave Meyer, director of advanced research and development at Cisco.

Both Martín Germán and Alberto Castro are graduate students at the Universidad de la República Oriental del Uruguay. They have actively participated in the PCE working group. Jean-Louis Leroux of France Télécom, who is also active in the PCE WG, served as mentor for both fellows.

The next round of applications was announced in August.

The Internet Society expresses its gratitude to the IETF 69 mentors as well as those who served on the fellowship application review and selection committee, including James Galvin, Jaap Akkerhuis, Alain Patrick Aina, Sanjaya, and Frederico Neves.

Special thanks to Afilias and Google for their sponsorship of the fellowship program. Support for this important program by businesses and organisations is welcome. Complete information about the program, including sponsorship benefits, can be found at http://www.isoc.org/educpillar/fellowship/.

Plenary, continued from page 5

Thomas agreed, adding that there is a brief window of one to three years before people will need to look at IPv6. Only in that short window can things be fixed, he said. "The IETF tends to work best when things really hit, and yes, things are starting to hit now."

A number of other issues were raised during the plenary, including the concern that there appears to be no formal procedure for revisiting older specifications or RFCs. In some cases, the WG, or even the entire IETF area, is no longer in existence, which makes it difficult to address requests to revise or revisit specifications.

Following that was a lengthy discussion on an issue related to the IPv6 WG. Some disappointment was expressed that the WG did not meet during IETF 69 despite requests from within the WG. It's expected that the WG will be rechartered to include maintenance issues, but it's also possible that the group will take on new work, such as issues related to the deployment of IPv6. Some people felt that multiple WGs might be needed: one to address protocol work and others to address more-operational issues. In addition, the IPv4-to-IPv6 transition mechanisms may need to be revisited. One participant said he believed that the slow deployment of IPv6 is the result of its having been created inside the IETF instead of in cooperation with industry players. In most cases, when work comes to the IETF, a deployment constituency is already in place. IPv6, on the other hand, has been developed internally by the IETF with the assumption that it's needed and that it will eventually be adopted by the market. With this in mind, the IETF will need to think about how to sell IPv6 to the world.

Photo by By Mirjam Kühne

The Art Institute of Chicago

Another topic raised during the open discussion was the update of RFC 2026, which describes the standards process. The RFC currently describes the standards process as a three-step procedure, but in reality, one or more steps are often omitted before the industry starts using it. Many folks within the IETF agree that the RFC should be updated to reflect how the standards process is realised in practice, which not only would be fairer to newcomers to the IETF but also would benefit the entire community. It was agreed, however, that any adjustments to the RFC should be viewed as a "process documentation correction" and not a change in the actual process. In other words, the underlying principles should be kept in place. One participant suggested that this be represented as an ongoing process and not as a three-step process, because many protocols will, in fact, never be completely finished (many require ongoing maintenance). In conclusion, it was agreed that when important documents, such as the standards procedure documents, get changed, one must be sure that the outcome is what the entire community wants.

News and Announcements from the IAB and the IETF

Reports from the IAB workshop on Unwanted Traffic and the workshop on Routing and Addressing are currently in the RFC Editor queue and will be soon published as RFCs.

In addition, there are a few nonarchitectural documents:

- RFC 4844: The RFC Series and RFC Editor
- RFC 4845: Process for Publication of IAB RFCs
- RFC 4846: Independent Submissions to the RFC Editor

A number of personnel changes were announced at IETF 69. Ted Hardie has been appointed to the ISOC Board of Trustees. Loa Andersson is now IAB liaison to the Internet Engineering Steering Group. Danny McPherson has been appointed IAB liaison to the NomCom. Stewart Bryant will serve as liaison for ITU-MPLS. And Scott Brim has stepped down as liaison for ITU-NGN.

It was announced that the ITU has been looking for input on its role in Internet policy and standards development. Those who are interested can find the IAB's input at http://www.iab.org/documents/correspondence/2007-05-21-itu-resolution-102.html.

There was also an informal gathering between the IETF and the ITU on 21 July 2007. The goal of the meeting was primarily to get to know each other better and to develop personal working relationships so that future

collaborations can be effective and fruitful.

The next IAB retreat will cover the following topics:

- Routing and Addressing: Actively following developments and building common understanding of architectural issues
- IP Fundamentals: What assumptions are made in stacks and how they relate to original design goals; IP and NAT (architectural questions)
- Bridging gaps with partner organisations like ISOC, the IRTF and others

At the last IETF meeting, the IETF Trust produced a license agreement for authors who want to sign their RFCs over to the Trust. It is a bit disappointing to see that not many people have done that so far. The license agreements can be found on the IETF Administrative Support Activity (IASA) Web site at http://trustee.ietf.org/authorlic.html.

With respect to the IASA budget, there is a shortfall between the planned budget and the current income for meeting the budget line in 2007. However, special thanks are extended to Microsoft and Cisco Research for hosting IETF 70 in Vancouver, Canada.

Paving the Way, continued from page 1

IPv4 Address Space Allocation and Policies

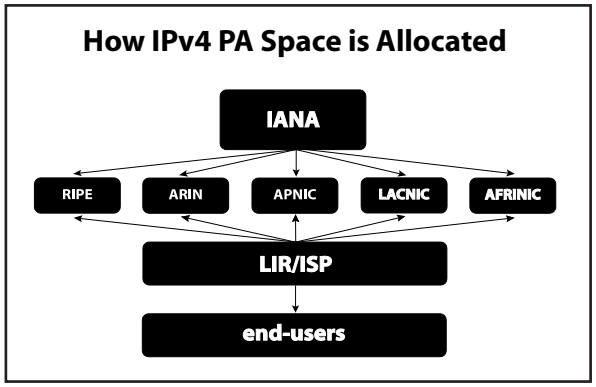
IPv4 PA (provider-aggregatable) allocations flow from IANA to the RIRs (Regional Internet Registries), which include the RIPE NCC, ARIN, APNIC, LACNIC, and AFRINIC. From there, address space flows to the LIRs (Local Internet Registries) and then trickles down to the end users.

Similarly, IPv4 PI (provider-independent) allocations begin with IANA and then flow to the RIRs. From there, address space is assigned directly to end users.

Each RIR is responsible for forming its own address allocation policy within its regional community in an open, bottom-up process. Today, IANA allocates address blocks of /8 to the RIRs, and it plans to continue allocating sufficient IPv4 address space to support RIR registration needs for at least 18 months. (Visit http://aso.icann.org/docs/aso-001-2pdf for the IANA allocation policy.)

When Will the IPv4 Address Space Become Exhausted?

In May 2007, Geoff Huston announced that his model for determining the projected date of IANA unallocated IPv4 address exhaustion has changed. As reported at http://www.potaroo.net/tools/ipv4/, the new predictive model is based on a quadratic equation, which, he believes, offers a closer fit to the underlying data set. Here the exhaustion point is the date that the first RIR exhausts its available pool of addresses and no further addresses are available in the IANA unallocated pool to replenish the RIRs' pool. The data available suggests a best-fit predictive model whereby this will occur in January 2011. A related prediction is the exhaustion of the IANA unallocated number pool, which this model predicts will occur in June 2010.



In a report titled A Pragmatic Report on IPv4 Address Space Consumption (http://www.cisco.com/web/about/ac123/ac147/archived_issues/ipj_8-3/ipv4.html), Tony Hain describes a slightly different methodology for arriving at predictions regarding the time constraints for the exhaustion of IPv4 address space. As Tony writes, "Depending on the model chosen, the nonlinear historical trends . . . covering the last 5- and 10-year data show that the remaining 64 /8s will be allocated somewhere between 2009 and 2016, [assuming there is] no change in policy or demand."

Regardless of the differing methodologies and assumptions, both Geoff and Tony have been vocal advocates for the need to "commence investment in IPv6-based service infrastructure," as Geoff describes it in a response to Tony's projections.

The abounding sense of urgency related to the deployment of IPv6 within the IETF community, as Kurtis points out, affects—and is affected by—both policy and market forces. "The dates tell us how much time we have, and the RIRs must come up with a good model or a process to handle [the transition]," he says. As one attendee mentioned, RIRs are allocating addresses under the current model, and as long

Continued on next page

Paving the Way for IPv6, continued from page 7

The question that is most on the minds of the IETF community is, What will it take for the market to begin the deployment of IPv6? At some point, the costs of obtaining IPv4 address space will be higher than the costs of deploying IPv6.

as the model doesn't change dramatically, reasonable predictions can be made, but the RIRs are beginning to see policy change requests, which could alter those predictions.

The question that is most on the minds of the IETF community is, What will it take for the market to begin the deployment of IPv6? At some point, the costs of obtaining IPv4 address space will be higher than the costs of deploying IPv6. Transition to IPv6 is fraught with challenges—including the expense of new equipment—but the biggest challenge appears to be that there is no seamless way to transition back and forth from IPv4 to IPv6.

IANA and the RIRs are actively encouraging their communities to deploy IPv6. ARIN and LACNIC, as well as ICANN, have all published statements promoting the move to IPv6. While the proposal by ARIN to set a date for IPv4 termination was not adopted, the discussion within the RIRs remains active.

Implications for the Future of the Internet

As Kurtis and Jari explained, perhaps the most significant implication of IPv4 exhaustion on the Internet is that NAT (network address translation) is "here to stay." Other predictions regarding the implications of IPv4 address-space exhaustion for the next phase of the Internet include:

- Some IPv6 deployment
- Some kind of market space forming for addresses
- Security of routing becoming more interesting
- More routing pain; smaller prefix blocks

Some of the political implications are likely to include:

- The appearance of last-chance-allocation panic
- Discussions about address allocation policies
- Debates about fairness between different parties, such as old/new users, different registries, IANA versus registries, and developed world versus developing world
- Market creation to be driven by political and legal battles

What Is the Role of the IETF?

Deciphering the role of the IETF with regard to IPv4 address space depletion and the deployment of IPv6 was a large part of the discussion at the IAB-IESG meeting. Kurtis and Jari outlined a number of aspects that fall outside the IETF's purview, such as consideration of the allocation rate of existing address space (a discussion that should happen within the RIR communities) and policies that affect how that address space gets allocated (also the responsibility of IANA and the RIRs, which all have active and open discussion forums for debating those policies). Other aspects not applicable to the IETF include the possible address space markets (which should be left to registries, contracts, and the courts) and NATs and IPv6, which may well be IETF issues.

The area that Kurtis and Jari said they believe does fall under the auspices of the IETF is delivery of the technical components that the address space market will require. As they pointed out, NATs are "a fact of life," and they should continue to be taken into account. The deployment of any significant new technology on the Internet, such as IPv6, "is going to be painful." Both suggested it may be time to take another look at IPv6 transition mechanisms. "Things related to IPv6 will have to be fixed as deployment goes on," said Jari. "This is maintenance work, and the IETF is good at that."

Kurtis agreed, adding that transition mechanisms exist but they often require purchasing new equipment, handling implementation issues, and training staff, all of which requires considerable investment. What the IETF may need to consider is whether there is anything it can do to make the transition easier. "This is what we have to solve," Kurtis said.

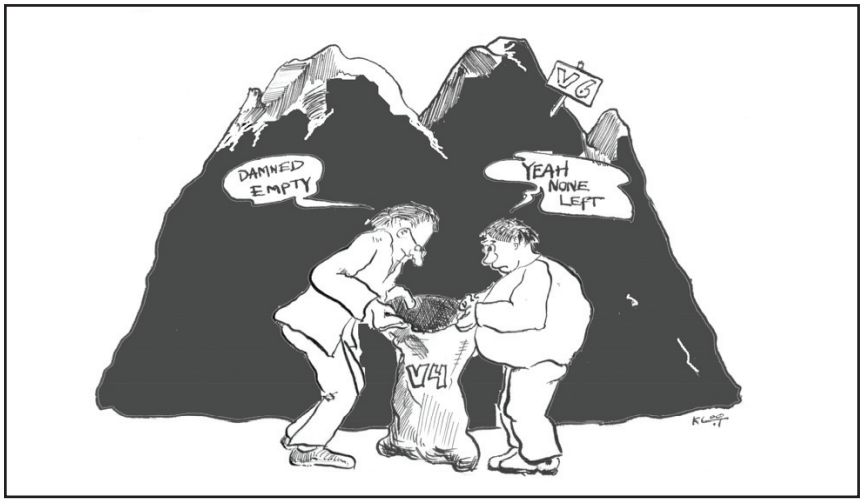
According to Joe Abley, the perception is that the only generic transition mechanism is dual stack, but the dual-stack solution could double the cost for companies and organisations. "In many cases," he said, "it is easier to implement only IPv6, but there is no good way to get back to the IPv4 Internet from there." Achieving that, he said, could solve the problem.

Elwyn Davies suggested that in light of there being no interworking transition mechanism, it might make sense to go back and develop one that works better than NAT-PT (network address translation–protocol translation). "It would be easier if IPv4 were a special case in IPv6," said Elwyn. "Then we would not have the inter-

working issues between the two networks. But that is not the case."

So what can the IETF do about the diminishing IPv4 address space in and the smoothing of the transition to IPv6? Distributing the remaining IPv4 address space is the responsibility of the RIR community. If the RIRs need any technology support, such as in the case of classless interdomain routing (CIDR), the IETF is there to help. With regard to the transition mechanisms, it would probably be best to wait and see what the market is doing. If it turns out that the existing mechanisms don't work or that people have difficulties with them, then the IETF will have to look at that.

It may be true that there is little the IETF can do apart from encouraging the market to be proactive in testing and deploying IPv6. However, what drives the market today are economics and regulation. With that in mind, Dave Thaler suggested that the IETF consider providing review of the technical setup and requirements of government agencies. "IETF participants or working groups could help find out what the market demand is going to be—particularly by looking at what large government agencies are rolling out," he said. "A lot of the other things are outside the scope of the IETF."



IETF Support for IPv6 Deployment

By Shane Kerr

Note: This article does not provide a complete summary of all IETF activities in this area. It reflects the author's personal perspective on some current highlights.

One of the common themes within the IETF community is that the IETF has not done enough either to encourage adoption of IPv6 or to make the technology useful. While it may be true that IPv6 has problems, the assumptions about support from the IETF are wrong.

Until a few years ago, when Geoff Huston started publishing his analyses, estimates of when we could expect to see the last unallocated IPv4 address were quite vague. Geoff's research indicates that the unallocated address pool will be exhausted in the next few years. His arguments are compelling, and his estimates have been widely accepted. By contrast, folks in the Regional Internet Registry (RIR) community usually choose a date far in the future—a strategy intended to build trust in the current IP allocation regime.

Under the current IPv4 allocation regime, when new addresses are needed they get allocated from an unallocated part of the address space. Once the entire address space has been allocated, the process will need to change. As awareness of the need for change grows, the group of people who are thinking about the implications of a depleted IPv4 address pool has become larger and more diverse. This is not surprising: the Internet is important, and the effects of running out of IPv4 addresses could be wide reaching. Also as a result, those who have long been following the development of IPv6 are repeating their observations, either as complaints or as encouragement.

As people begin learning about IPv6, it's natural for them to ask questions. As IPv4 address space moves closer to exhaustion, lack of widespread IPv6 adoption begins to look more and more like a problem. There are genuine concerns about the technology—for example, that IPv6 autoconfiguration wastes half of the address space. Some of the concerns are valid; others are not. In this environment, however, even questions can seem like criticisms.

Early Days and Design Decisions

Note: There are a number of resources on the Internet that cover the early history of IPv6. Google is your friend if you're interested.

Continued on next page

IETF Support for IPv6 Deployment, continued from page 9

From its beginning, IPv6 was the creation of a group of talented engineers who were working in a difficult area: attempting to design a protocol for an unknown future.

It has been nearly 20 years since the IETF began considering the problem of IPv4 address exhaustion.[1] Serious work on ways to deal with the problem began more than 15 years ago. While the Internet was certainly successful at the time, it was still used mostly by technical professionals. Identifying the "end of life" for IPv4 was the first in a long series of issues identified and dealt with by the engineers working in the IETF.

Several new technologies, ranging from minor tweaks of IPv4 to completely new approaches to addressing and routing, were proposed to deal with the problem. Following the usual IETF process, a number of decisions were made in those early days. For instance:

- There would be no "flag days" to switch from one protocol to the next.
- A longer, but still fixed-length, address would be required.
- Addresses would continue to be used in a hierarchy.
- Routing would be basically the same.

Other components were added to IPv6, such as multiple addresses per interface, address autoconfiguration, and multicast support. This is understandable, considering the prevailing assumption that IPv6 would be the "final" version of IP—at least for the lifetime of the people designing it. There was an effort to limit the number of changes and additions, but many made it in.

For any given decision, you can argue that it was the wrong one. For any given feature, you can argue that it is unnecessary or poorly specified. People did then! That doesn't mean that IPv6 as a whole is poorly designed, however, or that it fails to meet the goals set out for it.

Transition Plans and Tools

The core IPv6 protocol was defined in 1995. Even before that, a lot of thought had been given to how the Internet would switch from using IPv4 to using IPv6. Shortly after the IPv6 protocol became an RFC, other RFCs were published that documented ideas and tools to help with the transition. The engineers who designed and implemented IPv6 knew that real-world network administrators would still have to change their networks and that advice and tools that would make the work easier were essential. The ngtrans working group was created as a place to work on those technologies as well as to coordinate with the 6bone project (more on the 6bone later).

At the time, and as it is today, it was understood that there is no one-size-fits-all method for converting to IPv6. Every network is unique, and each would experience different problems in an effort to migrate to IPv6. So more than one idea was explored, and each was documented. If you look at the old ngtrans page,[2] you will see that there are quite a few RFCs on the subject, some of which cover multiple scenarios.

From one point of view, the ngtrans working group was unsuccessful; IPv6 is not widely used, and it certainly has not replaced IPv4. On the other hand, the working group did meet its stated goals. There are now a number of defined mechanisms that are useful in implementing IPv6 networks.

Even today, though, nobody knows how IPv6 will actually get adopted, nor does anyone know what it will look like when it does. Ten years ago, I was told that IPv6 would arrive from the edges and move in. Now I hear it will arrive at the core and move to the edges.

Rather than being negligent, the engineers within the IETF actually did the best thing possible, which is to consider IPv6 transition in many different environments, some of which would turn out to be used infrequently. There was no way to know which of these environments would be the most common, so extra effort was spent to try to cover them all.

IETF™ Brand Dog Food

When a company uses the product it makes, that phenomenon is sometimes called *eating your own dog food*. The IETF is mainly a standards-making organisation, not a product development company or a network operations company. However, the IETF does have computers on the Internet. And thousands of people *attend* IETF meetings. And the IETF has always made some effort to use the standards it develops, including the IPv6 standards.

Using IPv6 at IETF meetings has not always been painless. At many past IETF meetings, I had to disable IPv6 connectivity on my computer because the routing went through such a poorly connected system of IPv6 tunnels that it was basically unusable. Nevertheless, this is exactly the kind

1. See the *Running out of Internet addresses?* thread: http://www-mice.cs.ucl.ac.uk/multimedia/misc/tcp_ip/8813.mm.www/0121.html.
2. See http://www.ietf.org/html.charters/OLD/ngtrans-charter.html.

of operational experience that results in useful information.

A long-standing complaint[3] about the IETF is that there is not enough operator participation. Whether this is true or not, the IETF has tried to get some of its own experience, at least in recent years. The IETF has not always been a first adopter (as recently as two years ago, the IETF servers were not IPv6 reachable[4]) but it's often an early adopter.

6bone

Shortly after the first IPv6 RFCs were published, a group of engineers created a test bed network called the 6bone. While the 6bone was not an IETF project, many of the 6bone participants were also active in the IETF, and there are RFCs that document the address allocation and operation of the network. Originally started to test standards and implementations, the 6bone evolved into a test bed for operations and, finally, into an almost-production-quality network[5].

The end of the 6bone, on 06-06-2006, is a sign of its success. An Internet-wide IPv6 test network is no longer needed, as IPv6 is used more widely on the "real" Internet now than it ever was on the 6bone.

Coordination

Even before IPv6 appeared for the first time on the Internet, the IETF was coordinating with the Internet Assigned Numbers Authority (IANA) and with the RIRs.

The IANA maintains not only a number of registries that are necessary for IPv6 to function, including the address space registry itself, but also other IPv6-related information, such as DHCPv6 option codes or ICMPv6 parameters. Most of the interaction between the IETF and the IANA is straightforward, because the IANA is an administrative body and able to implement the recommendations of the IETF when appropriate.

Conclusion

The IETF has done a lot to make it easier for the people using the Internet to adopt IPv6. The IETF mission is to produce documents (see RFC 3935), and from this point of view, the IETF has done exactly what it should.

The engineers who designed and implemented IPv6 knew that real-world network administrators would still have to change their networks and that advice and tools that would make the work easier were essential. The ngtrans working group was created as a place to work on those technologies as well as to coordinate with the 6bone project

Coordination with the RIRs is more complex, as each RIR has its own policies and methods for updating policies. In many ways, working with an RIR is similar to working with the IETF. Discussions occur on open mailing lists, and consensus is generally required for decisions to be made. This means that the policies are bottom-up and that they reflect the requirements of the network operator community. But creating new policies or changing existing policies is difficult in this environment; it requires considerable education, on the part of both the IETF and the RIR communities. The IETF and the RIRs worked closely together during the development of the first IPv6 policies to ensure that the technical requirements were met. The RIRs have all had working IPv6 policies for years now. Coordination between the operator communities and the IETF is still important, but it now follows the regional RIR policy development procedures.

Documents will not by themselves cause people to adopt IPv6. Software must be developed, networks built, users educated, and policies updated. At the end, IPv6 adoption is largely a business decision, and money saved by using IPv6 may motivate the work. These activities often depend on the documents the IETF produces, but they are outside the IETF mission. Individuals in the IETF and the organisations they work for can do a lot to encourage IPv6 adoption outside the scope of the IETF.

New standards are being produced to create and extend protocols, and recommendations are made for developers, users, and operators, and these should not try to duplicate the work already done. Remember the work that has already been done when considering what the IETF can do for IPv6.

3. "As the field has grown explosively, specialisation has set in, and market pressures have risen, there has been less and less operator participation in the IETF," Harald Alvestrand noted back in 2003: http://www1.ietf.org/mail-archive/web/ietf/current/msg28011.html.
4. See the IETF servers aren't for testing thread: http://www1.ietf.org/mail-archive/web/ietf/current/msg36786.html.
5. See RFC 2772.

IPv6 Type 0 Routing Header

By Arnaud Ebalard

Note: This article does not provide a complete summary of all IETF activities in this area. It reflects the author's personal perspective on some current highlights.

At both the corporate and Internet network infrastructure levels, IP-based routing decisions are performed on the destination address of IP packets by following global routing tables' content and associated policies.

Both the IPv4 and IPv6 protocols provide the option for a packet emitter to force the routing path followed by its packets. This ability for users to inflect the routing implemented by operators is known as source routing.

When a packet from a source to a target follows a natural path (in blue in picture on following page), the inclusion of a source routing extension in this packet with the address(es) of intermediary router(s) (waypoint in the picture) modifies the routing path (in red in the picture). In other words, the packet is routed from the source to the waypoint and then from the waypoint to the target. Including more intermediary routers not only gives more control on the forced path but also provides more discovery capabilities.

For decades, the benefits and drawbacks of this capability have been discussed. During that time, the IPv4 Loose and Strict Source Routing options (LSSR and SSR) and the IPv6 Type 0 Routing Header extension (RH0) have been implemented in IP stacks. However, IPv4 network administrators have gotten into the habit of preventing the processing of source routing options on routers, which has resulted in the default disabling of source routing in most IPv4 devices.

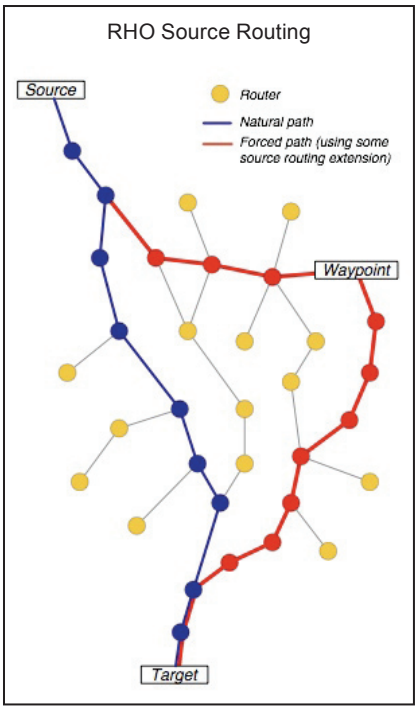
As more IPv6 testing and deployment gets conducted, the more serious negative security impacts associated with the Type 0 Routing Header are becoming better understood. As a result, the IETF has begun taking action to deprecate the mechanism in the IPv6 specification. This overview of the process provides a good illustration of how the IETF works and what makes it such a unique standardisation body; that is, following a rough consensus, a draft providing a pragmatic response to a security problem has been published.

Threats

There are a number of potential consequences associated with the ability of a user to select the path followed by its packets in the routing infrastructure, ranging from network discovery to denial-of-service (DoS) attacks. Some are described in "IPv6 Type 0 Routing Header Security" (available at http://www.secdev.org/conf/IPv6_RH_security-csw07.pdf), but more can be found in a document titled "Deprecation of Type 0 Routing Headers in IPv6," which is a work in progress (available at http://www.ietf.org/internet-drafts/draft-ietf-ipv6-deprecate-rh0-01.txt). The most significant consequence—the one that led to the deprecation of the mechanism in the IPv6 protocol—is a DoS attack, which is described briefly later.

Under IPv4, the source routing mechanism is implemented as an option that synthetically carries a list of the waypoint addresses through which the packet will travel. The size of the list is inherently limited by the maximum size of IPv4 options (40 bytes), which leaves room for, at most, nine addresses.

Under IPv6, source routing is implemented as an extension header, which is found between the IPv6 header and the upper-layer payload. As with IPv4, it is seen mainly as a list of waypoint addresses that the packet will visit on its path to its final destination. Unlike IPv4, the number of addresses in IPv6 is limited only by the maximum size of the packet. On paths with a Maximum Transmission Unit (MTU) of 1,500 bytes, one can inject packets containing up to 90 waypoints. This is a renewed version of the old IPv4 source routing threat, but perhaps doped on steroïds: the amplification effect is indeed 10 times worse.



When a packet that includes a routing header arrives at the destination found in the destination field of the IPv6 header, the node inspects the routing header and, by default, forwards the packet to the next waypoint. This behaviour was true for most rout-

ers as well as for some host operating systems, at least until a few months ago.

Since no filtering or limitations are typically implemented with regard to that behaviour, some specific lists of addresses in the RH0 extensions can lead the packet to oscillate between two selected routers (used as waypoints), creating an amplification attack on the path between the two targets. An attacker with a 2 Mbit/s upload link can saturate a 100 Mbit/s link.

What happened?

During a presentation at the CanSecWest 2007 Security Conference in April 2007, a number of threats with regard to the IPv6 Type 0 Routing Header extension were described, including the negative impacts on Internet infrastructure elements. That information probably filled the gap between what attendees were hearing at the conference and the numerous theoretical warnings that had been proclaimed by researchers in the IPv6 community.

In light of the recent momentum gained by IPv6, the presentation generated a lot of publicity, resulting in a number of articles being published on SecurityFocus ("Experts Scramble to Quash IPv6 Flaw," by Robert Lemos, 9 May 2007), on Dark Reading ("Five Security Flaws in IPv6," by Kelly Jackson Higgins, 8 May 2007), on eWeek ("IPv6 Headers Problem Revealed," by Lisa Vaas, 4 May 2007), and on Techworld ("IETF Moves against IPv6 Threat," by Matthew Broersma, 14 May 2007), among others. The publicity also led to Security Advisories for major end hosts and router operating systems. Most of the advisories blamed the IPv6 specification and not the implementation.

As more IPv6 testing and deployment gets conducted, the more serious negative security impacts associated with the Type 0 Routing Header are becoming better understood.

Soon after the event, the Open Source community took measures to deactivate default processing of the mechanism, including Linux 2.6 kernel (after 2.6.20.9) and most flavours of BSD. After a time, Apple patched its kernel for preventing RH0 processing (10.4.10 security update). As of this writing, Cisco and Juniper have not yet altered the defaults on their products.

Presenters at the CanSecWest 2007 Security Conference also warned against a practical threat directed toward anycast architectures, such as the F instances of the IPv6 root name servers. As a result, the operators of the F root server (the Internet Systems Consortium) took immediate action by dropping, without further processing, all packets that include an RH0 extension. The information has also been relayed to operators of other root name servers.

IETF Response

On 23 April 2007, two days after the CanSecWest Security Conference, the issue appeared on the IETF dns-ops and ipv6-ops working group mailing lists. A few hours later, it was being discussed on the IETF IPv6 working group mailing list (ipv6@ietf.org).

On 25 April 2007, IPv6 WG chairs Robert Hinden and Brian Haberman officially raised the issue to the IPv6 WG.

In parallel with those discussions, two drafts were quickly assembled for review by the IPv6 working group. The first one, by Joe Abley, advocated for deprecation of the mechanism. The second one, by Pekka Savola and Georges Neville-Niel, proposed that a disable-by-default behaviour be implemented.

With the working group widely in favour of deprecation, on 14 May 2007 the IPv6 WG requested that the two drafts be combined.

At the time of this writing, the draft is a work in progress.

Conclusion

The consensus reached by the IETF regarding the deprecation of the RH0 mechanism from the IPv6 specification comes as a welcome, albeit late, conclusion to the source routing threat. The positive aspects of this decision are most notably:

- Early discovery and subsequent remediation, which prevented potential exploitation against production networks;
- Limited impact with regard to current implementations' changes for deactivation or removal; and
- A gain in terms of future stack implementation through reduced complexity, size, and development time requirements.

It is also expected that future proposals for source-routing-related mechanisms (through a new type of Routing Header) will be followed with great care within the IETF.

Special thanks to Merike Kaeo and Joe Abley for thier contributions to this article.

A Retrospective View of NAT

By Lixia Zhang

Note: This article does not provide a complete summary of all IETF activities in this area. It reflects the author's personal perspective on some current highlights.

Today, network address translators are everywhere. Their ubiquitous adoption was promoted neither by design nor by planning but by the continued growth of the Internet, which brings forth an ever-increasing demand not only on IP address space but also on other functional requirements that network address translation (NAT) is perceived to facilitate. This article provides a personal perspective on the history of NAT, the lessons we may learn from it, and some articulations on best ways forward from where we are today.

Introduction

NAT commonly refers to a box that interconnects a local network to the public Internet, where the local network runs on a block of private IPv4 addresses as specified in RFC 1918. In the original Internet architecture design, each IP address is defined to be *globally unique* and *globally reachable*. In contrast, a *private* IPv4 address is meaningful only within the scope of the local network behind a NAT and, as such, the same private address block can be reused in multiple local networks, as long as those networks do not *directly* talk to each other. Instead, they communicate with each other—and with the rest of Internet—through NAT boxes.

Like most unexpected successes, NAT's ubiquitous adoption was not foreseen when the idea first emerged more than 15 years ago (RFC 1287 and RFC 1335). Back then, had anyone foreseen where NAT would be today, it is possible that the NAT deployment itself might have followed a different path: one that was better planned and standardised. The set of Internet protocols that have developed over the past 15 years might have also evolved differently, and we might have seen less overall complexity in the Internet than what we have today.

Although the clock cannot be turned back, I believe it's a worthwhile exercise to revisit the history of NAT so that we may learn some useful lessons. It may also be worthwhile to assess—or reassess—the pros and cons of NAT, as well as to take a look at where we are today in our handling of NAT and how best to proceed into the future.

I would like to emphasise that this writing represents a *personal view*, and my recall of history is likely to be incomplete and to contain errors. My personal view on this subject has also changed substantially over time, and it may continue to evolve, as we are all in a continuing process of understanding this fascinating and dynamically changing Internet.

How NAT Works

As I mentioned earlier, IP addresses were designed to be globally unique and globally reachable. This property of the IP address is a fundamental building block in supporting the Internet's end-to-end architecture. Until very recently, almost all of the Internet protocol designs, especially those below the application layer, have been based on the aforementioned IP address model. However, the explosive growth of the Internet in early 1990s not only signalled the danger of IP address space exhaustion but also created an instant demand on the IP addresses: suddenly, connecting large numbers of user networks and home computers demanded IP addresses instantly and in large quantity. Such demand could not possibly be met by going through the regular IP address allocation process. NAT came into play to meet that instant high demand.

Because NAT was not standardised before its wide deployment, a number of different NAT products exist today, each with somewhat different functionality and different technical details. Since this article is about the history of NAT deployment—and not an explanation of how to traverse specific NAT boxes—I will describe a popular NAT implementation as an illustrative example. Interested readers may visit Wikipedia to find out more about various NAT products.

A NAT box **N** has a public IP address for its interface connecting to

Photo by Peter Löthberg

Lixia Zhang and Tony Li at IETF 69 in Chicago

the global Internet and a private address facing the internal network. **N** serves as the default router for all of the destinations that are outside the local NAT address block. When internal host **H** sends an IP packet **P** to a public IP destination address **D** in the global Internet, the packet will be routed to **N**. **N** translates the private source IP address in **P**'s header to its public IP address and adds an entry to its internal table that keeps track of the mapping between the internal host and the outgoing packet. This entry represents a piece of state, which enables all subsequent packet exchanges between **H** and **D**. For example, when **D** sends a packet **P'** in response to **P**, **P'** will arrive at **N**, and **N** can find the corresponding entry from its mapping table and replace the destination IP address—which is its own public IP address—with the real destination address **H**, so that **P'** will be delivered to **H**. This mapping entry times out after a certain period of idleness, which is normally set to a vendor-specific value. In the process of changing the IP address carried in the IP header of each passing packet, a NAT box must also recalculate the IP header checksum—as well as the transport protocol's checksum—if it is calculated based on the IP address, as in the cases for TCP and UDP checksums.

From this description, it is easy to see the major benefit of NAT: one can connect a large number of hosts to the global Internet by using a *single* public IP address. Other benefits of NAT also became clear over time, as discussed in more detail later.

At the same time, a number of NAT's drawbacks can also be identified immediately. First and foremost, NAT changed the end-to-end communication model of the Internet architecture in a fundamental way: Instead of allowing any host to talk directly to any other host on the Internet, hosts behind a NAT now must go through the NAT to reach others, and all communications through a NAT box can be initiated only by an internal host first in order to set up the mapping entries. In addition, since ongoing data exchange depends on the mapping entry kept at the NAT box, the box represents a single point of failure: if the NAT box crashes, it may lose all of the existing state, and the data exchange between all of the internal and external hosts will have to be restarted. This is in contrast to the original IP's goal of delivering packets to their destinations as long as *any* physical connectivity exists between the source and destination. Furthermore, because NAT alters the IP addresses carried in a packet, all protocols that are dependent on IP addresses are affected. In certain cases, such as TCP checksum, which includes IP addresses in the calculation, the NAT box can hide the address change by recalculating the TCP checksum when forwarding a packet. For some of the other protocols that make direct use of IP addresses, such as IPSec, the protocols can no longer operate on the end-to-end basis as originally designed; for some application protocols that embed IP addresses in the application data, application-level gateways are needed to handle the IP address rewrite. As discussed later, NAT also introduced some other drawbacks that surfaced only recently.

Like most unexpected successes, NAT's ubiquitous adoption was not foreseen when the idea first emerged more than 15 years ago. Back then, had anyone foreseen where NAT would be today, it is possible that the NAT deployment itself might have followed a different path: one that was better planned and standardised.

A Recall of NAT History

I started graduate school at Massachusetts Institute of Technology to work on network research at the same time as RFC 791, the Internet Protocol Specification, was published in September 1981. Thus I was fortunate to witness the most fascinating unfolding of this new system called the Internet. During the next 10 years, the Internet grew rapidly. RFC 1287, *Towards the Future Internet Architecture,* was published in 1991 and is probably the first RFC that raised the concern about IP address space exhaustion in a foreseeable future.

RFC 1287 also discussed three possible directions for extending IP address space. The first one pointed to a direction similar to today's NAT:

> Replace the 32 bit field with a field of the same size but with different meaning. Instead of being globally unique, it would now be unique only within some smaller region ...

RFC 1335, published in May 1992, provides a more elaborate description of the use of internal IP addresses (in other words, private IP addresses) as a solution to IP address exhaustion. The first paper describing the NAT idea, "Extending the IP Internet Through Address Reuse," appeared in the Janu-

Continued on next page

NAT, continued from page 15

As pointed out in RFC 1287, the continued growth of the Internet exposed strains in the Internet architecture as originally designed, the two most urgent of which were routing system scalability and exhaustion of IP address space.

ary 1993 issue of *Computer Communication Review* and was published a year later as RFC 1663. Although these RFCs may be considered forerunners in the development of NAT, as explained later, for various reasons the IETF did not take actions to standardise NAT.

The invention of the Web further accelerated Internet growth in the early 1990s. The explosive growth underlined the urgency to take action toward solving both the routing scalability and the address shortage problems. The IETF took several follow-up steps, which eventually led to the launch of the IPng development effort. I believe the expectation at the time was to get a new IP developed within a few years, followed by a quick deployment. However, the actual deployment during the next 10 years took a rather unexpected path.

The planned solution

As pointed out in RFC 1287, the continued growth of the Internet exposed strains in the Internet architecture as originally designed, the two most urgent of which were routing system scalability and exhaustion of IP address space. Since long-term solutions require a long lead time to develop and deploy, efforts started on developing both a short-term solution and a long-term solution to those problems.

Classless Inter-Domain Routing, or CIDR, was proposed as a short-term solution. CIDR removed the class boundaries embedded in the IP address structure, thus enabling more efficient address allocation, which helped extend the lifetime of IP address space. CIDR also facilitated routing aggregation, which slowed the growth of the routing table. However, as stated in RFC 1481, *IAB Recommendation for an Intermediate Strategy to Address the Issue of Scaling*, "This strategy (CIDR) presumes that a suitable long-term solution is being addressed within the Internet technical community." Indeed, a number of new IETF working groups that started in late 1992 aimed at developing a new IP as a long-term solution, and the Internet Engineering Steering Group (IESG) set up a new IPng area in 1993 to coordinate the efforts.

CIDR was rolled out quickly, which effectively slowed the growth of the global Internet routing table. Because it is a quick fix, CIDR did not address emerging issues in routing scalability—in particular, the issue of site multihoming. A multihomed site would want to be reachable through any of its multiple provider networks. In the existing routing architecture, this requirement translates into having the prefix, or prefixes, of the site listed in the global routing table, thereby rendering provider-based prefix aggregation ineffective. (Interested readers are referred to the article "An Overview of Multihoming and Open Issues in GSE," published in the September 2006 issue of the *IETF Journal* for a more detailed description on multihoming and its impact on routing scalability.)

The new IP development effort, on the other hand, took much longer than anyone imagined when the effort first began. At the time of this writing, the IETF is finally wrapping up the IPv6 working group, almost 13 years after its establishment.[1] The IPv6 deployment has also been slow in coming. As of today, there have been a small number of IPv6 trial deployments. There is one known operational deployment in a provider network, but there are no known commercial user sites that use IPv6 as the primary protocol for their Internet connectivity.

If one day someone sits down to write an Internet protocol development history, it would be very interesting to look back and understand the major reasons for the slow development and adoption of IPv6. But even without doing any research, one could say with confidence that NAT played a major role in meeting the IP address need that arose out of the Internet growth, which at least deferred the demand for a new IP.

The unplanned reality

While largely unexpected, NAT has played a major role in the explosive growth of Internet access; in fact, the growth of the Net turned in large part on NAT growth. Nowadays it is common to see multiple computers, or even multiple LANs, in a single home. It would be unthinkable for every home

1. The creation of the IPng working group (later renamed to IPv6) was announced on 7 November 1994.

to obtain multiple IP addresses from its network service provider. Instead, a common setting for home networking is to install a NAT box that connects one home network or multiple home networks to a local provider. Similarly, most enterprise networks deploy NAT as well. It is also well-known that countries with large populations, such as India and China, have most of their hosts behind NAT boxes; the same is true for countries that got connected to the Internet only recently. Without NAT, the IPv4 address space would have been exhausted a long time ago.

For reasons discussed later, the IETF did not standardise NAT implementation or operations. However, despite the lack of standards, NAT was implemented by multiple vendors, and the deployment spread like wildfire. This is because NAT has several attractions, as described here.

It is also well-known that countries with large populations, such as India and China, have most of their hosts behind NAT boxes; the same is true for countries that got connected to the Internet only recently. Without NAT, the IPv4 address space would have been exhausted a long time ago.

Why NAT Succeeded

NAT started as a short-term solution while we were waiting for a new IP to be developed as the longer-term solution. The first set of recognised NAT advantages were stated in RFC 1918:

> With the described scheme many large enterprises will need only a relatively small block of addresses from the globally unique IP address space. The Internet at large benefits through conservation of globally unique address space which will effectively lengthen the lifetime of the IP address space. The enterprises benefit from the increased flexibility provided by a relatively large private address space.

Today, NAT is believed to offer advantages well beyond that modest claim. Essentially, the mapping table of a NAT provides one level of indirection between hosts behind the NAT and the global Internet. As the popular saying goes, "Any problem in computer science can be solved with another layer of indirection." This one level of indirection enables the following features associated with NAT:

- NAT can unilaterally be deployed by any end site, without any coordination from anybody else.
- One can use a large block of private IP addresses—up to 16 million—without asking for permission, and one can connect to the rest of the Internet by using only a single allocated IP address. In fact, for most user sites, it is difficult to get an IP address block that is much bigger beyond their immediate need.
- This one level of indirection means that one never needs to worry about renumbering the internal network when changing providers—other than renumbering the NAT box.
- Similarly, a NAT box also makes multihoming easy. One NAT box can be connected to multiple providers and use one IP address from each provider. Not only does the NAT box shelter the connectivity to multiple ISPs from all the internal hosts, but also it does not require any of its providers to "punch a hole" in the routing announcement (such as making an ISP deaggregate its address block). Such a hole punch would be needed if the multihomed site takes an IP address block from one of its providers and asks the other providers to announce the prefix.
- This one level of indirection is also perceived as one level of protection, because external hosts cannot directly initiate communication with hosts behind a NAT, nor can they easily figure out the internal topology.

Last, but not least, another important reason for NAT's quick adoption is that its gains were realised on day one, while its potential drawbacks showed up only slowly and lately.

The other side of the NAT

NAT disallows the hosts behind a NAT from being reachable by external hosts and hence disables them from being a server. However, in the early days of NAT deployment, many people believed they would have no need to run servers behind a NAT. Thus this architectural constraint was viewed as a security feature and believed to have little impact on users or network usage otherwise. For example, RFC 1335 gave four reasons for the use of private addresses:

1. In most networks, the majority of the traffic is confined to its local area networks. This is due the nature of networking applications and the bandwidth constraints on inter-network links.

Continued on next page

NAT, continued from page 17

2. The number of machines that act as Internet servers, i.e., running programs waiting to be called by machines in other networks, is often limited and certainly much smaller than the total number of machines.
3. There are an increasingly large number of personal machines entering the Internet. The use of these machines is primarily limited to their local environment. They may also be used as "clients" such as ftp and telnet to access other machines.
4. For security reasons, many large organisations, such as banks, government departments, military institutions and some companies, may only allow a very limited number of their machines to have access to the global Internet. The majority of their machines are purely for internal use.

As time goes on, however, the above reasoning has largely been proved wrong.

Today, network bandwidth is no longer a fundamental constraint. In the past few years, VoIP (voice over IP) has become a popular application. VoIP changed the communication paradigm from client-server to a peer-to-peer model, meaning that any host may call any other host. Given that more than half of the Internet hosts are behind NAT, a number of NAT traversal solutions need to be developed in order to support VoIP. A number of other recent peer-to-peer applications, such as BitTorrent, have also become popular recently, and each has to develop its own NAT traversal solution.

In addition to the change of application patterns, a few other problems also arise due to NAT's use of private IP addresses. For instance, a number of business acquisitions and mergers have run into situations where two networks behind NAT needed to be interconnected, but, unfortunately, they were running on the same private address block, resulting in address conflicts. Another problem emerged more recently. The largest allocated private address block is 10.0.0.0/8, commonly referred to as "net 10." The business growth of some provider and enterprise networks is leading to, or has already resulted in, the net 10 address exhaustion. An open question facing these networks is what to do next. One provider network migrated to IPv6; a number of others simply decided on their own to use another unallocated IP address block.

It is also a common misperception that a NAT box makes an effective firewall. This may be due partly to the fact that in places where NAT is deployed, firewall function is often implemented in the NAT box. A NAT box alone, however, does not make an effective firewall. Numerous home computers behind NAT boxes have been compromised and have been used as launchpads for spam or DDoS attacks. Firewalls set up control policies on both incoming and outgoing packets to minimise the chances of internal computers' getting compromised or being abused. Making a firewall serving as a NAT box does not make it more effective in fencing off bad packets; good control polices do.

Given that more than half of the Internet hosts are behind NAT, a number of NAT traversal solutions need to be developed in order to support VoIP. A number of other recent peer-to-peer applications, such as BitTorrent, have also become popular recently, and each has to develop its own NAT traversal solution.

Why the IETF Missed the Opportunity to Standardise NAT

During the decade following NAT's deployment, a big debate arose in the IETF community about whether NAT should, or should not, be deployed. Due to its use of private addresses, NAT moved away from the IP's basic model of providing end-to-end reachability between any hosts, thus representing a fundamental departure from the original Internet

Recent IESG Document and Protocol Actions

A full list of recent IESG Document and Protocol Actions can be found at http://ietfjournal.isoc.org/DocProtoActions0302.shtml

architecture. This debate went on for years. As late as April 2000, a message posted to an IETF mailing list stated that NATs are "architecturally unsound" and that the IETF and the IESG "should in no way endorse their use or development." Whoever posted that message was certainly not alone in holding that position.

These days most people would accept the position that the IETF made a mistake not to standardise NAT early on. How did we miss the opportunity? A simple answer could be that the crystal ball was cloudy. I believe that a little digging would reveal a better understanding of the factors that clouded our eyes at the time. From my personal viewpoint, the following factors played a major role.

First, I believe the feasibility of designing and deploying a brand-new IP was misjudged, as were the time and effort needed for such an undertaking. Those who were opposed to standardising NAT had hoped to get a new IP developed in time to meet the needs of a growing Internet. However, the miscalculation was off by perhaps an order of magnitude. While the development of a new IP was taking its time, Internet growth did not wait. NAT is simply an inevitable consequence, which the IETF community failed to see clearly at the time.

Another closely related factor was an inadequate understanding on how to make engineering trade-offs. Architectural principles should be treated as guidelines for problem solving; they help guide us toward developing better overall solutions. However, when the end-to-end reachability model was interpreted as an absolute rule, it ruled out NAT as a feasible means to meet the demand for IP addresses at the time. Furthermore, viewing the architectural model in an absolute way contributed to the one-sided view of NAT's drawbacks—hence the lack of a full appreciation about NAT's advantages as covered earlier, let alone any effort to develop a NAT solution that can minimise NAT's impact on end-to-end reachability.

The misjudgment on NAT cost us dearly. While the big debate went on, NAT deployment was rolled out, and the absence of a standard led to a number of different behaviors among various NAT products. A number of new Internet protocols were also developed or finalised during this time—such as IPSec, SAP, and SIP, to name a few. All of their designs were based on the original model of IP architecture, wherein IP addresses are assumed to be globally unique and reachable. When those protocols became ready for deployment, they faced a world that was mismatched with their design. Not only did they have to solve the NAT traversal problem, but also the solution had to deal with a variety of NAT box behaviors.

Although NAT has been accepted as a reality today, not all of the confusions around NAT deployment have been clarified. One example is the recent debate over Class-E address block usage. Class-E refers to the IP address block 240.0.0.0/4 that has been on reserve until now. As such, many existing router and host implementations block the use of Class-E addresses. Putting aside the issue of required router and host changes to facilitate Class-E usage, the fundamental debate is whether the address block should go to the public address allocation pool or to the collection of private address allocations. The latter would give those networks that face net-10 exhaustion a much bigger private address block to use. However, this gain is also one of the main arguments against it, which is raised in an effort to press those networks to migrate to IPv6 instead of staying with NAT. Such a desire sounds familiar, because similar arguments had been used against NAT standardisation in the past. If the past is any indication of the future, we should know that pressures do not dictate protocol deployment; rather, economical feasibility does. This argument does not imply that migrating to IPv6 has no economical feasibility. On the contrary, I believe it does. New efforts are needed both in protocol developments (in order to make it a reality) and in documentations (to show clearly the short- and long-term gains from moving to IPv6).

Those who were opposed to standardising NAT had hoped to get a new IP developed in time to meet the needs of a growing Internet. However, the miscalculation was off by perhaps an order of magnitude.

What Can and Should Be Done Now?

The long-ago predicted IPv4 address space exhaustion is finally upon us today, yet the IPv6 deployment is barely visible on the horizon. What can and should the IETF do to enable the Internet to grow along the best path into future? I hope the review of NAT history helps shed some light on the answer.

Continued on next page

NAT, continued from page 19

Accepting the existence of NAT in today's architecture does not mean we simply take the existing NAT traversal solutions as given. Instead, we should fully explore the NAT traversal design space to steer the solution development toward adherence to the Internet architecture model.

First, we should recognise not only that IPv4 NAT is widely deployed today but also that some forms of network address translation boxes will be likely with us forever. We should have a full appraisal on the pros and cons of such boxes; the discussion earlier on IPv4 NAT merely serves as a starting point. We should not view all network address translation approaches as a "bad thing" that must be avoided at all cost. Several years ago, an IPv4 to IPv6 transition scheme called Network Address Translation–Protocol Translation (NAT-PT, RFC2766) was developed but later classified to historical status[2]—due mainly to concerns that (1) it works much in the same way as an IPv4 NAT does and (2) it doesn't handle all of the transition cases. However, in view of IPv4 NAT history, it seems worthwhile to revisit that decision. IPv4, as well as IPv4 NAT, will be with us for years to come. NAT-PT seems to offer a unique value in bridging IPv4-only hosts and applications with IPv6-enabled hosts and networks. There have also been discussions on the desire to perform address translations between IPv6 networks, which deserve further attention. The Internet would be better off with well-engineered standards and operational guidelines for bridging the IPv4 and IPv6 worlds and for traversing IPv4 and IPv6 NATs that aim at maximising interoperability rather than repeating IPv4 mistakes.

Accepting the existence of NAT in today's architecture does not mean we simply take the existing NAT traversal solutions as given. Instead, we should fully explore the NAT traversal design space to steer the solution development toward adherence to the Internet architecture model. A new effort in this direction is the NAT Traversal through Tunneling (NATTT[3]) project. Contrary to most existing NAT traversal solutions, which are server based and protocol specific, NATTT aims to provide generic, incrementally deployable NAT traversal support for all applications and transport protocols.

Last, but not least, I believe it is important to understand that successful network architectures can and should change over time. All new systems start small. Once successful, they grow larger. The growth will bring the system to an entirely new environment that the original designers may not have envisioned, together with a new set of requirements that must be met. In order to properly adjust a successful architecture, we must have a full understanding of such an architecture's key building blocks as well as the potential impacts of any changes to them. I believe the IP address is this kind of key building block that touches—directly or indirectly—all other major components in the Internet architecture. The impact of IPv4 NAT, which changed IP address semantics, provides ample evidence. During IPv6 development, much of the effort also involved a change in IP address semantics, such as the introduction of new concepts like that of the link-local address and the site-local address. The site-local address was later abolished and partially replaced by Unique Local IPv6 Unicast Addresses (ULA), another new type of IP address. The debate over the exact meaning of ULA is still going on. The original IP design clearly defined an IP address as being globally unique and globally reachable and identified an attachment point to the Internet. As the Internet architecture evolves, proposals to change the original IP address definition continue to arise. What should be the definition, or definitions, of an IP address today? I believe an overall examination of IP address's role in today's changing architecture deserves special attention at this critical time in the Internet's growth.

Acknowledgment

I sincerely thank Mirjam Kühne for her encouragement and patience in helping put this article together. I also thank Wendy Rickard for her hard work in making the article more readable.

2. *Historical status* means that a protocol is considered obsolete and thus removed from the Internet standard protocol set.
3. The NATTT Web site can be found at http://www.cs.arizona.edu/~bzhang/nat/.

Update on Routing and Addressing at IETF 69

By David Meyer

Note: This article does not provide a complete summary of all IETF activities in this area. It reflects the author's personal perspectives on some current highlights.

The IAB's Routing and Addressing Workshop[1], held in October 2006 in Amsterdam, rekindled interest in scalable routing and addressing architectures for the Internet. Among the many issues driving current interest are concerns about the scalability of the routing system and the imminent depletion of the IPv4 address space. This article is a summary of the Routing Research Group (RRG) meeting at IETF 69 in Chicago, where discussions took place about the proposals designed to address the problems and issues that were identified in Amsterdam.

Since the Amsterdam workshop, several proposals have emerged that attempt to address concerns expressed both there and elsewhere[2]. In general, those proposals are based on the so-called ID/Locator separation[3], which makes the assumption that separating the endpoint identification and routing locator functions of the IP address will lead to advantages for aggregatability (our only real tool to make the core routing system scale), mobility, and security. Among the proposals presented at the RRG meeting at IETF 69 were eFIT[4], LISP[5], and Six/One[6] (an interesting hybrid incorporating elements of shim6[7] and 8+8/GSE[8]). Note that these proposals seek a degree of incremental deployability, and in general they assume that the core routing system will not change. In addition, several of the proposals also require a system to map from "ID" to "Locator." (Proposals presented in the mapping space included APT[9], LISP-CONS[10], and NERD[11]).

Most of the existing routing and addressing proposals leverage the one or more levels of indirection inherent in the ID/Locator separation idea to create one or more new namespaces. In most cases, two namespaces are utilised. One namespace—the Endpoint Identifiers (or EIDs)—is used to address hosts. The other space, known as Routing Locators (or RLOCs), is used for packet routing across a transit domain. The goal of this indirection is to allow efficient aggregation in the RLOC space (which can be thought of as the current Default Free Zone, or DFZ) in order to provide persistent identity in the EID domain and, in some cases, to provide for secure and efficient mobility.

The RRG meeting in Chicago focused on the current set of proposals in this space, which fall into two broad categories: (1) map-and-encap and (2) address rewriting. The approaches differ depending on whether the translation occurs through address rewriting or tunneling and, in one case (Six/One), depending on where the indirection is implemented. The proposals are outlined as follows.

Proposals

Map-n-encap

The general idea behind so-called map-and-encap (written map-n-encap) schemes, as originally described by Bob Hinden and Steve Deering, is that there are two address spaces: one used within a domain (the EID space) and one used to transit between domains (the RLOC space). The hope is that since the RLOC space is, in theory, decoupled from nontopologically assigned EID space, map-n-encap schemes will provide for efficient aggregation of the RLOC space—that is, the global routing state.

In the map-n-encap scheme, when a packet is generated, both its source and its destination "addresses" are taken from the site's EID space. When a

Continued on next page

1. D. Meyer et al., "Report from the IAB Workshop on Routing and Addressing," RFC (Request for Proposal) 4984.
2. T. Narten et al., "Routing and Addressing Problem Statement," draft-narten-radir-problem-statement-00.txt.
3. N. Chiappa, "Endpoints and Endpoint Names: A Proposed Enhancement to the Internet Architecture," http://ana.lcs.mit.edu/~jnc//tech/endpoints.txt.
4. D. Massey, L. Wang, B. Zhang, and L. Zhang, "A Proposal for Scalable Internet Routing and Addressing," draft-wang-ietf-efit-01.txt.
5. D. Farinacci et al., "Locator/ID Separation Protocol (LISP)," draft-farinacci-lisp-03.txt.
6. C. Vogt, "Six/One: A Solution for Routing and Addressing in PIPv6," draft-vogt-rrg-six-one-00.txt.
7. E. Nordmark, "Shim6: Level 3 Multihoming Shim Protocol for IPv6," draft-ietf-shim6-proto-08.txt.
8. M. O'Dell, "GSE—an Alternate Addressing Architecture for IPv6," http://www.watersprings.org/pub/id/draft-ietf-ipngwg-gseaddr-00.txt.
9. D. Jen et al., "APT: A Practical Transit Mapping Service," draft-jen-apt-00.txt.
10. D. Meyer et al., "LISP-CONS: A Content Distribution Overlay Network Service for LISP," draft-meyer-lisp-cons-02.txt.
11. D. Massey, L. Wang, B. Zhang, and L. Zhang, "A Proposal for Scalable Internet Routing and Addressing," draft-wang-ietf-efit-00.txt.

Update on Routing and Addressing at IETF 69, continued from page 21

packet is addressed to a destination in another domain, it traverses the domain's infrastructure to a border router (or other border element). The border router maps the destination of the EID to an RLOC, which corresponds to an entry point in the destination's domain (hence the need for an EID-to-RLOC mapping system; mapping proposals are discussed later). This is the "map" phase of map-n-encap. The border router then encapsulates the packet and sets the destination address to the RLOC returned by the mapping infrastructure (if any; it may be statically configured as well). This is the "encap" phase of the map-n-encap model. Note that since map-n-encap works by appending a new header on an existing IP packet, it can work with both IPv4 and IPv6. While the destination EID is mapped to an RLOC in all of the proposals discussed here, the source EID in the packet may be treated differently within each proposal; specifically, it may or may not be mapped to an RLOC in the encapsulated packet. When the packet arrives at the destination border router, it is decapsulated and sent on to its destination. Note that this suggests that EIDs may need to be routable in some scope—most likely scoped to the local domain.

Two map-n-encap proposals were discussed at the RRG meeting: Enable Future Internet Innovation through Transit Wire, or eFIT[12], and the Locator/ID Separation Protocol, or LISP[13]. The idea behind eFIT is that user networks and transit networks are separated in terms of both addressing and routing. User networks use EIDs, and transit networks use RLOCs. In eFIT, user and transit network routing domains are also separated. One of the interesting features of this proposal is that provider routing does not interact with routing in the user domains, which is different from the Border Gateway Protocol (BGP), wherein user networks "peer" with provider networks using the same routing protocol and address space. In particular, there is no routing protocol operating across the links between the user networks and the transit core.

In contrast, LISP does not propose any classification of address spaces beyond the EID and RLOC spaces. (More specifically, it has no concept of user or transit network spaces.) Rather, in the LISP formulation, a site is assigned an EID prefix from which it addresses its hosts. When a host wants to send a packet to a remote domain, both the source and the destination in the packet contain an EID. At the domain boundary, routers do the same map-n-encap operation as described earlier.

Another major difference between LISP and eFIT is that LISP assumes there will be no changes to the core routing infrastructure. That is, LISP is transparent to the BGP infrastructure, whereas eFIT introduces boundaries between the user and the transit core networks that are not present in the current interdomain (BGP) routing architecture. In particular, eFIT specifies that "There is no routing protocol operating across the links between the user networks and the transit core," which represents a change from the current architecture.

It is worth noting that map-n-encap schemes have the benefit of not requiring host changes or changes to the core routing infrastructure. However, there is some difference in opinion over whether the encapsulation overhead of map-n-encap schemes is problematic or not.

Address Rewriting

The idea behind the address rewriting schemes—which were proposed originally by Dave Clark and later by Mike O'Dell[14]—is to take advantage of the 128-bit IPv6 address and use the top 64 bits as the routing locator (otherwise known as routing goop, or RG) and the lower 64 bits as the endpoint identifier. In this scheme, when a host emits a packet destined for another domain, the source address contains its identifier (frequently an IEEE MAC address) in the lower 64 bits and a special value (a unique "unspecified" value) in the RG. The destination address contains the fully specified destination address. (It has been proposed that the Domain Name System [DNS] would be used to find the destination address, but then how does one find the address of the DNS servers?)

When a packet destined for a remote domain arrives at the local domain's egress router, the source RG is filled in (forming a full 128-bit address) and the packet is routed to the remote domain. On ingress to the remote domain, the destination RG is rewritten with the unspecified value. This ensures that the host doesn't know what its network prefix is and, as such, enables the renumbering that would be required to maintain the congruence between prefix assignment and physi-

12. Ibid.
13. Farinacci, op. cit.
14. O'Dell, op. cit.

cal network topology that is required for the kind of "aggressive envisioned" in the 8+8/GSE specification.

Six/One was the address rewriting approach presented at the RRG meeting. Six/One is interesting because it borrows ideas from both shim6 and 8+8/GSE. In particular, Six/One borrows the shim6 concept that multihomed edge networks use provider-assigned addressing space from each of their providers and that hosts can use addresses from all of their providers interchangeably without breaking active transport sessions. Six/One borrows the 8+8/GSE idea of rewriting the high-order bits while packets are in flight. It also introduces the concept of edge networks. An edge network can independently route packets between two attached hosts, and predictably, edge networks connect to transit networks for global connectivity.

In Six/One, a host's addresses differ only in their high-order bits (in much the same way as they do in 8+8/GSE). However, in a Six/One, an edge network (or other service provider) may change the address in a packet depending on the provider to which the packet is being routed. As a result, the destination address a host puts into a packet serves as a suggestion to the edge network about which provider the host's packets should be routed to. The edge network may choose to either follow that suggestion or rewrite the high-order bits of the address in accordance with a provider of its own choice. Note that this is different than in shim6, where the host selects the transit network; in Six/One, edge networks retain the ability to select a particular provider via rewriting. Hosts adapt to address rewrites in that they modify subsequent packets accordingly before injecting them into the network. Unlike 8+8/GSE, Six/One also adds to packets certain information that enables the receiving hosts to reverse address rewrites.

What's new about Six/One is that regardless of address changes, an edge network can also use the added information to identify a remote host.

What's new about Six/One is that regardless of address changes, an edge network can also use the added information to identify a remote host. The main difference between Six/One and 8+8/GSE, then, is that hosts are aware of their full addresses (including the RG) and can suggest a network provider to their local domain (in the much same way that is enabled by the shim6 protocol). One of the many interesting aspects of the Six/One proposal is that it combines the host-based locator selection feature of shim6 with a modified version of the address-rewriting approach of 8+8/GSE. Finally, note that unlike the map-n-encap solutions described earlier, a Six/One host looks up the entire 128-bit address of the destination host in the DNS (which may return multiple AAAA records for the destination). Therefore, like shim6, no additional mapping system is needed.

Mapping Systems

Since both map-n-encap and rewriting schemes rely on the addition of a level of indirection to the addressing architecture, it is necessary to map from the locally used address (EID) to the routing locator (RLOC). In the case of the map-n-encap schemes, it is a direct translation: an EID gets mapped to an RLOC. The situation is subtly different for the rewriting schemes: in general, such schemes must look up the entire destination address (which usually resides in the DNS) but it also must somehow find the source RG when rewriting the source address at a domain border. Six/One is a hybrid, since in that model the hosts know their entire address (including the RG), which can be looked up in the DNS, a property that is shared by shim6.

In the case of map-n-encap schemes, an EID-to-RLOC mapping service is required to make the service scale reasonably. (Could the same database be used to lookup RGs in the 8+8/GSE case?) There are three important parameters to consider in the creation of the architecture for a mapping service: the rate of updates to the database, the state required to be held by the mapping service, and the latency incurred during lookup. That is, a mapping system must minimise rate x state while still optimising lookup latency. Because most estimates put the size of the mapping database at O(10 10), the implication is that the update rate must be small. (Note that this is a primary reason that current mapping proposals do not incorporate reachability information into the mapping database.) In addition, the choice of push versus pull also has an effect on latency: if you push the entire database close to the edge, you improve lookup latency at the cost of increased state, and if you build a service that requires a mapping request in order to find an authoritative server for that mapping (in other words, pull), you reduce state in the core but you also increase laten-

Continued on next page

Update on Routing and Addressing at IETF 69, continued from page 23

Concerns about the scalability of the routing system, the effect of IPv6 on that scalability, and the rapid depletion of the IPv4 "free address pool" have fueled a growing interest in this area as well as in the broader topic of scalable routing and addressing architectures for the Internet.

cy. This suggests that a hybrid push/pull architecture might be the most effective. Regardless, architects need to take care not to import the dynamics (and hence the concomitant problems) of the routing system into the mapping database. If that were to happen, we wouldn't have solved the problem; we would have only moved it.

Three mapping services were discussed at the RRG meeting: APT (A Practical Transit Mapping Service)[15], NERD (a Not-so-Novel EID to RLOC Database)[16], and LISP-CONS (a Content Distribution Overlay Network Service for LISP)[17]. The proposals can be broadly classified as either push or pull (though LISP-CONS might be considered a hybrid protocol) based on how they distribute the database.

Both APT and NERD are push protocols; that is, they push the mapping database to the edges for distribution. APT and NERD differ primarily (1) in how far toward the edge network the database is propagated (for example, APT has the concept of a default mapper so that some nodes can carry less than the complete database, whereas in NERD all nodes hold the complete database; in APT, the default mapper also winds up in the data path whenever it is used); (2) in database format (the APT database format isn't specified, and NERD uses XML); and (3) in how the database is distributed and maintained (APT uses BGP, and NERD uses HTTP).

On the other hand, LISP-CONS is primarily a pull protocol. That is, mappings must be pulled (via a query mechanism) from the authoritative severs. The actual EID-to-RLOC mappings reside in authoritative Content Access Resources (CARs), and mapping queries and replies traverse a hierarchical overlay from requester to the authoritative CAR (and back).

Conclusions

Over the past 15 years, two major architectural approaches to the IP/Locator split have emerged: map-n-encap and address rewriting. Proposals regarding both of those approaches were presented at the IETF 69 RRG meeting. While much progress has been made since the IAB Routing and Addressing workshop in October 2006 in Amsterdam, significant unresolved issues remain within all of the proposals, including the question of whether the ID/Locator separation solution is actually the best approach to a scalable Internet routing architecture. Other questions remain, such as whether map-n-encap schemes are superior to rewriting schemes such as 8+8/GSE. And what about host-based schemes, such as Six/One? How do these schemes interact with other protocols being developed in this space, such as shim6 or HIP[18]). Finally, since in most cases these schemes require another name resolution (ID to Locator lookup), there are questions about how best to build such a resolution system and whether such a system can be built in a scalable way that also is secure and minimises latency.

Concerns about the scalability of the routing system, the effect of IPv6 on that scalability, and the rapid depletion of the IPv4 "free address pool" have fueled a growing interest in this area as well as in the broader topic of scalable routing and addressing architectures for the Internet. More work needs to be done in the areas of security and mobility. And a deeper understanding of cost/benefit relationships—as in, Who bears the cost and who stands to benefit?—would prove useful. More generally, even transition mechanisms are not well understood. It all adds up to a very interesting set of RRG meetings for IETF 70.

15. Jen, op. cit.
16. E. Lear, "NERD: A Not-So-Novel Eid-to-Rloc Database," draft-lear-lisp-nerd-02.txt.
17. Meyer, op. cit.
18. R. Moskowitz et al., "Host Identity Protocol," draft-ietf-hip-base-08.txt.

ISOC Chicago Arranges for Experts' Panel at IETF 69

When the IETF comes to town, the ISOC chapters in the region are encouraged to take advantage of the experts. At IETF 69, not only did ISOC Chicago members get free passes to attend the Newcomers' Tutorial and the Plenary session; they also organised a panel discussion featuring a handful of IAB members. The panel was intended to help the area's chapter members gain insight into current issues as well as developments at the IETF and on the Internet in general.

While the speakers are currently members of the IAB and former members of the IESG, their comments were made on their own behalf.

Panellists: Brian Carpenter (former chair of the IETF), Olaf Kolkman (IAB chair), Danny McPherson, Dave Oran, and Lixia Zhang

Moderator: Bill Slater, ISOC Chicago chapter president

What do you see as current threats to the Internet, and how are they being addressed within the IETF?

Danny: Unwanted Traffic and Security crosses all areas of the IETF. There is a lot of work going on in many IETF working groups on this topic, from infrastructure security for DNS and routing systems to application-layer security. We've got a great deal of work to do and there's no 'silver bullet.' It's all about layered security and incremental advances.

Dave: Making protocols less susceptible to threats is also important. Very often, adding features that are intended to prevent threats can be counterproductive. Some of those mechanisms overreact, such as by not allowing any traffic to pass through. Therefore, we need to be sufficiently aware of the work going on in other areas in the IETF.

Olaf: There are a number of areas where problems arise because of the content of the data being transmitted and the IETF is not able to prevent that bad content from occurring in the payload of the protocols, as happens with viruses, botnets, and spam. The IETF develops protocols through which entities communicate regardless of the content of the communication. You can include protection mechanisms when developing the protocol, such as DKIM, but you cannot foresee what might be the actual data that is being transmitted.

Brian: This is an important point. For example, when the mail protocol delivers spam, it's doing exactly what it's supposed to do—at least from a protocol point of view.

How does the work of ICANN affect the IETF and its work?

Brian: The IETF does not engage in politics. There's an MoU [memorandum of understanding] between the IETF and ICANN that draws a precise line: IANA assigns technical parameters according to instructions it gets from the IETF, except for policy questions related to the assignment of TLDs and IP address space—unless those TLDs and IP addresses are used for purely technical purposes. As long as we stay within those boundaries, things are clear for the IETF, so we don't need to care about what TLD is delegated and why.

What are the big challenges for the future of the Internet in both the near term and the long term, and how do you propose to meet those challenges?

Lixia: It's always hard to predict the future, but looking at the past can offer some hints for the future. Back in the early days of networking, there were two difficult problems: congestion and routing. Over the years, we seem

Continued on next page

Photo by Joanna Roguska

Together with chapter members, ISOC Chicago chapter panellists gathered at IETF 69 with ISOC president Lynn St. Amour (seated, fourth from left). Pictured (seated) are moderator Bill Slater (third from left) and panellists Olaf Kolkman (fifth from left) and Brian Carpenter (far right). Also pictured (standing, second row) are panellists Lixia Zhang (fourth from left), and Danny Pherson (far right). Not pictured, Dave Oran.

Experts' Panel, continued from page 25

to have gotten a good handle on the congestion problem: not only did we develop successful congestion control protocols, but also several technological advances helped out tremendously. Congestion control can prevent congestion collapses, but good performance requires adequate bandwidth, which is met by technology advances.

Routing, however, remains a major problem today—not because we've made no progress but because the problem has changed: the goal used to be picking the best or shortest path. Nowadays data must follow paths that cost the least money, and complex policies were introduced in the routing. In addition, the global routing table is growing out of control. Late last year we passed the 200,000 threshold. Today we have 240,000 entries, which is faster than linear growth.

Aside from the ongoing routing challenge, we also now face the relatively new challenge of network security. This is a much tougher problem than scalability is. However, we shouldn't be surprised that we have a security problem today. Some research papers say the original design of the Internet did not take security into account, but that assessment is not entirely fair. Initially, the Internet was designed for a specific environment it was supposed to work in. And the original designers of the Internet did a great job, which is the reason the Internet has been able to grow to its current size.

We should keep in mind, however, that good design is not the sole enabler: Without the evolution of technology—especially the technology of affordable and ever-faster computers—the Internet would not have been able to grow as big or as quickly as it did. Unfortunately, the adage that "Everything that can be used can also be abused" applies to the Internet. Affordable computers with Internet connectivity have enabled innovation and changed society, but they also have been used for more dubious purposes.

Olaf: Indeed, the Internet grew more than anyone expected. As a result, there needs to be serious reimplementation to make scaling properties better so the Internet can scale for the next 15 to 20 years. Such reimplementation not only needs to happen but also needs to be paid. We also want the Internet to be affordable to everyone, which is a challenge. The Internet is an important mechanism to make information accessible to everyone—including people in developing countries—but we shouldn't forget that solving the scalability issues will create more complexity. In the near term, in addition to the routing problem, we're still working on IPv4 and with the fact that IPv4 address space is limited and will run out fairly soon. IPv6 has been developed, and we expected that it would get picked up by the industry. Now the deployment to IPv6 is becoming more and more important and some problems associated with that transition are more pressing.

The Internet grew more than anyone expected. As a result, there needs to be serious reimplementation to make scaling properties better so the Internet can scale for the next 15 to 20 years.

Brian: There's a strong temptation for ISPs to keep their dinosaur business models alive and to protect their walled gardens—that is, closed service with lower quality that cannot fully reach the Internet. WiMAX could become such a limited service, but I'm not sure the IETF can do anything about that except preach.

Dave: I agree. This is a substantial danger, and one that could cause serious fragmentation. But I see other challenges as well. The first is that the nature of peer-to-peer traffic today is substantially different from what we've seen before. The traffic profile is substantially different, and only now are we starting to understand it both economically and technically. Peer-to-peer traffic has the effect of finding spare bandwidth wherever it can and using it, the result being that an ISP adds capacity, and before it can make any profit from the increased capacity, the bandwidth is already being consumed by peer-to-peer traffic.

What is peer-to-peer traffic? It means that people are sharing data, legally or otherwise. From a technical standpoint, they form on a dynamic community that makes available everything they are interested in, and allows the community to get the data in small pieces from each other. The traffic patterns look much more random, and traffic engineering is much more challenging.

Another challenge is the evolution of mobile devices. Today a very small fraction of those devices is Internet enabled, but the number is likely to grow dramatically. Yet another challenge is what I refer to as *the Internet of things*. The number of those devices can be extremely large. Every lightbulb, switch, and so on will have the potential to be Internet enabled.

Danny: I believe mobility and scalability are going to put pressure on

the Internet. Another challenge is the convergence of various security threats. For example, the perception is that your ISP is sending 'filthy water', and you think, All this junk is coming down my pipe, isn't there anything my ISP can do to filter it out? No, there isn't anything they can do, or at least doing so is much more complex than most folks realise. Much of the infrastructure does not allow segmentation of traffic or services based on individual users. Then there are consumer privacy rights, providing a subscriber with the ability to clean their system, and regulatory and other service requirements, such as maintaining availability of VoIP-enhanced 911 services.

Brian: Botnets are serious threats to the Internet, as described in the Unwanted Traffic Report. We don't know how to deal with the botnet problem. However, it's important to point out that it's not a problem of the network; it's a problem of the end system.

Marcos Sanz (ISOC chapter member): I've read the Unwanted Traffic Report and, since then, I've had nightmares. Can someone offer some comforting words so I can get back my sleep?

Olaf: If after reading the Unwanted Traffic Report you're having sleepless nights, then the report was a success. People need to be woken up. We also need to reach out to people outside the technical community, and we're working with ISOC to do just that.

Brian: Many enterprises and organisations spend a lot of money to keep unwanted traffic out of their networks. But this is a small price to pay compared with not doing business on the Net at all.

Olaf: It's cynical, but the bad guys are interested in keeping the Net running because they want to use it to do their bad business.

Danny: We've performed a lot of analysis on those security threats. Network congestion-inducing worms, such as Slammer, are not used so much anymore, mainly because they melted parts of the network when propagating and they were far too visible. Nowadays, threats happen much more quietly; they fly under the radar while compromising and remotely administering systems, rather than appearing as loud infection and propagation vectors. Much of the threat today is economically motivated and, believe it or not, the miscreants often provide service-level availability agreements as well. If the network is not up, they can't collect their spoils.

Olaf: People who engage in this kind of activity are highly skilled. They probably cash big paychecks.

How many IPv6 addresses are there, and is there a name for this number?

Olaf: 340 undecillion – 3.5. x 10^{38}, or 340 trillion trillion trillion. That's not the number of addresses that is truly usable. It's basically chopped into halves: 64 bits identify a station, and 64 bits identify the individual network where the station sits. Still, with many trillions of addresses, we don't think we'll run out of addresses very soon.

Is the impact of the IPv4-to-IPv6 transition comparable to Y2K—the switch from 1999 to 2000? Are there reasons, from an end-user perspective, that we need to be concerned about the transition?

Brian: The transition from IPv4 to IPv6 is different from the Y2K switch, primarily because there is no drop-dead date. Still, in terms of strategic planning, one should start now. In a few years, the Regional Internet Registries will not have IPv4 addresses to hand out. People think there will be a market for IPv4 address space, but at some point it will be cheaper to switch to IPv6. But as I said, this will not happen on a certain date, like in the case of Y2K.

There is one way, however, in which it's the same as Y2K: you have to check to see if the router and the rest of your equipment and software are IPv6 compatible. The devil is in the details.

Network congestion-inducing worms, such as Slammer, are not used so much anymore, mainly because they melted parts of the network when propagating and they were far too visible. Nowadays, threats happen much more quietly; they fly under the radar while compromising and remotely administering systems, rather than appearing as loud infection and propagation vectors.

Dave: Actually, the problem is much worse than Y2K. Much of the industry is still only building IPv4. There are 2 million to 4 million Cisco IP phones that have little or no ability to be field upgraded to run IPv6. They don't even have enough memory to run dual stack. There are millions of devices being built every month by myriad manufacturers that are not IPv6 capable.

Danny: One of the big challenges with IPv6 is related to translating between

Continued on next page

Experts' Panel, continued from page 27

No one can predict what the next killer applications will be. The only thing we know for sure is that they will come. Look at MySpace, YouTube, and Facebook. Those killer apps keep popping up out of nowhere.

IPv6 and IPv4. Strict use of *transition* is the wrong term. There will be IPv6, and we need to provide for solutions that ease deployment burdens, such as enhanced NAT–PT, but IPv4 will still be around for a very long time.

Brian: The good news is that people are starting to understand that something has to be done.

Olaf: But people really need to start looking at their networks to see what needs to be done in order to move over to IPv6.

It's possible that by 2016, Moore's law will become void due to the limitations of physics and the current manufacturing technologies—such as photolithography. It is projected that the impact of this on the computing world will be a requirement to write better and more-optimised software, because we could be stuck with the latest, fastest processor for several years. Does the IETF foresee any such potentially disruptive events in the world of the Internet in the coming years?

Brian: We're going to be moving toward more parallel processing as well as other mechanisms. We also have to work on power issues. Otherwise, the computer will simply be melting.

Dave: This will hit the router community long before 2016. A lot of parallelism will have to be developed, such as channelised inverse multiplexing.

WiFi and WiMAX are everywhere. The average person might think this is magic. Are there other technologies on the horizon? Is there a model to make this kind of thing profitable?

Danny: If it's not a strict-access, services-based subscription model and the question is, Who is subsidising WiFi and WiMAX? the answer is likely "the advertisers," or at least the folks who find advertising revenue. The providers will give you access, but it's demographic-based advertising that's paying for it. There are economic motivators here as well, I assure you.

Olaf: This kind of advertising-sponsored access is a typical-use case for the World Wide Web and not for applications that run over IP.

Lixia: The value of the Internet is in its applications. If we step up a level and look at a bigger picture, we may see a different view regarding whether [offering ubiquitous wireless access] is something to be subsidised or something that will return value in another way. In the early days, people kept looking for 'killer applications' but the reality has taught us better: No one can predict what the next killer applications will be. The only thing we know for sure is that they will come. Look at MySpace, YouTube, and Facebook. Those killer apps keep popping up out of nowhere. Their inventors were nobodies. Look at Wikipedia, which serves as a showcase of what the online community as a whole can accomplish. You give connectivity to people, and you open the door to infinite innovations in great applications.

Corrections

Due to editing errors, two statements appeared incorrectly on page 14 of "Update on DNS," by Jaap Akkerhuis and Peter Koch (*IETF Journal,* May 2007, Volume 3, Issue 1). The subhead for AS112 should read: AS112 in a Box Work Continues. In addition, according to the authors, AS112 does not cover the local top-level domains .lan or .local, as stated in the article.

In the same issue, due to typographical errors, several figures were misrepresented on page 17 of "More ROAP: Routing and Addressing at IETF 68," by Geoff Huston. The statement in question should read: Today the Internet sits in an order of size of dimension of around 10^9. There are some 1.6 x 10^9 routed addresses in the Internet and an estimate of between 10^8 and 10^9 attached devices. If we look out as far as four decades to around 2050 we may be looking at between 10^{11} to 10^{14} connected devices.


Aaron Falk, IRTF Chair

IRTF Report

By Aaron Falk

Below are summaries of several updates on the Internet Research Groups (RGs), as reported during the Technical Plenary at IETF 69.

Currently, 14 research groups are working on topics related to Internet protocols, applications, architecture, and technology. Some groups have significant ties to IETF work; others, not so much. Most groups are open, and all maintain open mailing lists. There is room for overlap in scope, and the management style within each is diverse.

A recently published document describes the IRTF RFC review and publication process (draft-irtf-rfcs-01). One new IRTF RFC has been published since IETF 68: RFC 4838, Delay-Tolerant Networking Architecture.

At IETF 69 in Chicago, seven of the 14 RGs met. Below is a summary of some recent events as well as developments reported by some of the RGs during the IETF 69 technical plenary.

Anti-Spam RG (asrg)

The RG is currently working on DNS Black Lists. There is some progress toward publishing the DNS Black List definitions draft. A DNS Black List Guidelines draft may follow.

The AS RG is also seeking interest in the taxonomy of anti-spam strategies.

Crypto Forum Research Group (cfrg)

This RG published a new message authentication code called VMAC: Message Authentication Code Using Universal Hashing. On the mailing list are discussions on a variety of technical issues (AES-based KDFs, AEAD, SIV draft).

Delay-Tolerant Networking Research Group (dtnrg)

The DTN Architecture document has been published as RFC 4838. In addition, there are 17 drafts in the queue, with four nearing RFC readiness. At an interim meeting that took place in Dublin in May, much of the discussion was related to security. The RG also met during IETF 69, where the discussion focused mostly on reliability and neighbour discovery. The next in-person meeting is planned for IETF 71 in March 2008 in Philadelphia.

End-Middle-End Research Group (eme)

The EME RG held a joint meeting with HIP RG at IETF 69, resulting in a number of suggestions for joint activities. EME can complement the HIP RG work on providing name space as well as the development of a mechanism for relaying policy requests. It could also help HIP with Network Address Translation traversal research. There is a potential for future collaboration with HIP to conduct some larger-scale experiments.

Continued on next page

IRTF, continued from page 29

Host Identity Protocol Research Group (hip)

A joint meeting with the EME RG was held to explore possible architectural synergy. The purpose of the joint meeting was to explore the relationship between HIP and EME architectures, because there has been interest within the HIP community with middlebox-oriented architectures and because some in the HIP community believe that namespaces such as the EME namespace will need to be built on top of the cryptographic host names.

In addition to this joint discussion, three new proposals were presented at that meeting: two related to HIP as part of the P2PSIP architecture, and one related to the applicability of the shim6 REAP protocol to HIP. The next planned meeting of the RG is at IETF 70 in Vancouver, Canada.

Internet Congestion Control Research Group (iccrg)

After an interim meeting earlier this year and lively discussions on the mailing list, the ICC RG decided to meet during IETF 69. Currently, the RG is working mainly on two documents:

- One is a survey of current congestion control RFCs with the intention to provide congestion control designers with a guide to related work.
- The other is a survey of open congestion control research issues.

In addition, the RG is starting to look at congestion control proposals for the IETF Transport area. The next in-person meeting is planned in conjunction with PFLDnet 2008.

Internet Measurement Research Group (imrg)

Date and location for the workshop called Application Classification and Identification (WACI) has been set for 3 October 2007 at BBN Technologies in Cambridge, Massachusetts.

IP Mobility Optimisation Research Group (mobopts)

The document titled Unified L2 Abstractions for Fast Handovers has completed Internet Research Steering Group (IRSG) review. The RG met at IETF 69 and is now working on location privacy and mobility and on multicast mobility.

Network Management Research Group (nmrg)

At IETF 68, the group discussed adaptive monitoring work that permits trade-offs between overhead and accuracy. In the meantime, some work has been done on management trace analysis. Apart from that, the RG was pretty quiet since IETF 68 in Prague, and it is now considering future workshops and meetings.

Peer-to-Peer Research Group (p2prg)

The P2P RG is looking for both new chairs and new work items that will then be fed into the charter of the RG.

Update from the NomCom

NomCom Members 2007
Derek Atkins
Fred Baker, ISOC Liaison
Steven Blake
Christopher Boulton
Ian Chakeres
Lakshminath Dondeti, Chair
Lars Eggert, IESG Liaison
Ole Jacobsen
Andrew Lange, Advisor
Simon Leinen
Danny McPherson, IAB Liaison
Attila Takacs
Thomas Whalsh
Craig White
Dan Wing

During IETF 69, the NomCom collected feedback on member qualifications. Candidate interviews and community feedback will take place at IETF70 in Vancouver.

Number of people eligible to volunteer:	~900+
Number of volunteers:	108

The number of volunteers increased following a decrease in 2005 and 2006. This is a good sign. There is still a limited number of candidates for open positions in the IESG, IAB and IAOC. There could be a number of reasons why this would be, including the time commitment that's required. There might also be a mismatch of the requirements for the positions (or at least a perceived one). Finally, potential candidates might think that the 'incumbants are doing a fine job' and therefore hesitate to volunteer.

The NomCom encourages the community to provide feedback to the NomCom at nomcom07@ietf.org on issues such as:

- desirable qualifications for positions
- possible time commitment
- how IESG, IAB and other parts of the IETF are functioning

More input and more candidates would be helpful for the NomCom and for the whole IETF.

The following positions are up for considerations for the next term:

IAOC

Ed Juskevicius

IAB

Leslie Daigle
Elwyn Davies
Kevin Fall
Olaf Kolkman
David Oran
Eric Rescorla

IESG

Jari Arkko (Internet area)
Ross Callon (Routing area)
Cullen Jennings (Real-time Applications and Infrastructure area)
Lisa Dusseault (Applications area)
Sam Hartman (Security area)
Dan Romascanu (Operations and Management area)
Magnus Westerlund (Transport area)

Routing Research Group (rrg)

This RG has been active recently, particularly on the ram@irtf.org mailing list but also as part of a full-day meeting during IETF 69. A number of proposals have been submitted with the aim of bringing some of the design goals into alignment. Please see a more detailed description of the current work of the RRG on page 21.

Scalable, Adaptive Multicast Research Group (samrg)

The SAM RG met during IETF 69 and discussed the current active drafts:

- SAM framework
- Application-Layer Multicast (ALM) Router on PlanetLab

The next meeting is planned for IETF 71.

Transport Modelling Research Group (tmrg)

The document titled Evaluation Metrics for Congestion Control is now in IRSG review. A new document, titled An NS2 TCP Evaluation Tool Suite, along with a Web page with simulation scripts, is currently under discussion.

For more information about the Internet Research Task Force, see http://www.irtf.org/.

IETF Meeting Calendar

Fall 2007—IETF 70
2–7 December 2007
Hosts: Microsoft and Cisco Research
Location: Vancouver, BC, Canada

Spring 2008—IETF 71
9–14 March 2008
Host: Comcast
Location: Philadelphia, PA, USA

Summer 2008—IETF 72
27 July–1 August, 2008
Host: TBD
Location: Europe (Provisional)

Fall 2008—IETF 73
November 16-21, 2008
Host: Google
Location: Minneapolis, MN, USA

Register now for
IETF 70
2–7 December 2007
Vancouver, British Columbia, Canada

http://ietf.org/meetings/70-IETF.html

Early bird registration: 700 USD (through 23 November 2007)
Regular registration: 850 USD

IETF 70 is being hosted by Cisco Research Center and Microsoft
Additional sponsors include Huawei and Telus

Special thanks to

MOTOROLA

for hosting IETF 69

The ISOC Fellowship to the IETF is sponsored by

Afilias GLOBAL REGISTRY SERVICES Google

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

Afilias GLOBAL REGISTRY SERVICES ARIN CISCO
MOTOROLA NEUSTAR Ripe NCC

IETF Journal
IETF 69
October 2007
Volume 3, Issue 2

Published three times a year by the Internet Society

4 rue des Falaises
CH–1205 Geneva
Switzerland

Managing Editor
Mirjam Kühne

Associate Editor
Wendy Rickard

Editorial and Design
The Rickard Group, Inc.

E-mail
ietfjournal@isoc.org
Find us on the Web at
ietfjournal.isoc.org

Internet Society