



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

## New agreement marks major milestone in IETF Administrative Restructuring

By Peter Godwin - Editor, IETF Journal

After nearly twenty years of existence, the Internet Engineering Task Force has assumed oversight over the services that support the operations of the world's leading Internet standards development group.

A new agreement with NeuStar Secretariat Services LLC marks a major milestone in efforts to ensure that the IETF administrative support infrastructure will meet the future needs of the expanding IETF community.

The agreement (which was signed on December 15, 2005) was the outcome of extensive discussions and consultations between the IETF community and the IETF Administrative Support Activity (IASA) - a group created in April 2005 to examine ways of improving the IETF's administrative operations in support of the IETF standards process and technical activities.

A two-year Services Agreement with NeuStar Secretariat Services (NSS) was executed on behalf of IASA by Lynn St. Amour, President and CEO of the Internet Society. Mark Foster, Senior Vice President and CTO of NeuStar, Inc., represented NSS in the transaction.

Under the terms of the agreement, NeuStar Secretariat Services began work immediately on managing the IETF's secretariat, meetings, and document and data management services.

Speaking after signing the agreement with NeuStar, Lynn St. Amour said "The Internet Society is delighted to be able to bring this new level of support to the IETF."

Earlier in the day, NeuStar had reached agreement with the Corporation for National Research Initiatives (CNRI), to acquire the assets of CNRI subsidiary Foretec Seminars Inc - the incumbent secretariat service provider.

The IETF Trust was created at the time of the closing to ensure the utilization, maintenance, preservation and protection of IETF intellectual property for the benefit of the IETF. The agreement document was executed by CNRI President and CEO, Robert Kahn, and Lynn St. Amour as settlors, on behalf of their respective organizations.

Members of the IETF Administrative Oversight Committee and the IETF Administrative Director will serve as trustees. CNRI and the Internet Society donated their IETF related Intellectual Property to the Trust at its creation; the IETF also transferred its rights to its intellectual property to the Trust.

Following the Trust's first business meeting, a Trust Licensing Agreement was executed by and between the Trust and NeuStar Secretariat Services for its use of certain specified IETF intellectual property appropriate or necessary to its delivery of services to the IETF community in accordance with the Services Agreement.

"The IETF is not just getting older, it's growing up," said Leslie Daigle, IAB Chair and a leader in the IETF restructuring initiative. "Today marks the convergence of many hours and weeks of thoughtful discussion all around - we are coming together to set the IETF on a new administrative foundation to continue its technical work."

### Inside this issue:

New agreement marks major milestone .....	1
-----	
IETF64 Review .....	2
IETF64 Plenary .....	2
Routing .....	7
DNS .....	12
IPv6 .....	14
SHIM6 .....	15
Security .....	18
Mobility .....	20
Internationalized Email and Extensions ....	22
New BoFs .....	24
-----	
News from the IAB .....	25
News from the IRTF .....	28
News from the IAOC and IAD .....	30
News from the IETF Tools Team ..	32
Reflections on Architecture .....	33
IETF Glossary .....	37
Recent IESG Document and Protocol Actions ...	37
Calendar .....	38



# IETF64 Review: Plenary Sessions

By *Mirjam Kühne, ISOC*

The IETF plenary session was again organised in two parts: on Wednesday evening more administrative and operational aspects of the IETF were presented and discussed, such as reports from the IETF chair and the IESG, the IETF Administrative Director (IAD) and the IETF Administrative Oversight Committee (IAOC), RFC editor and IANA and finally the Process and Tools Team (PROTO). On Thursday the Technical Plenary session took place with a technical presentation of the Crypto Forum Research Group and reports from the IAB and the IRTF.

## Operations and Administrative Plenary

Brian Carpenter, the chairman of the IETF, opened the plenary by reminding everybody that we are approaching the 20th anniversary of the IETF. In January 1986 the first IETF meeting was held in San Diego, US, with 15 attendees. Now, almost 20 years later, there were 1291 attendees from 40 countries.

It is interesting to note that exactly one year ago 1,309 people from only 26 countries attended the IETF in Washington DC.

The IESG has some pretty good tools now, and is planning to review their own efficiency and working methods before IETF65.

Narrative minutes of IESG meetings can now be found at:  
<http://www.ietf.org/IESG/iesg-narrative.html>

There is also a new IESG projects page at: <http://unreason.com/jfp/iesg-projects.html>

At IETF64 Brian organised the pesci BoF (Process Evolution Committee for the IETF) to operate in design team mode as a way to bootstrap some progress on IETF process change. The outcomes will be submitted to the rough consensus process. The initial goal was to identify a list of principles for the change process:  
<http://www.rfc-editor.org/internet-drafts/draft-davies-pesci-initial-considerations-00.txt>

Brian ended his report with the announcement that Vint Cerf and Bob Kahn received the US Presidential Medal of Freedom (together with Muhammad Ali, Aretha Franklin, Alan Greenspan and others). According to the official press release (<http://www.whitehouse.gov/news/releases/2005/11/20051103-5.html>) they were awarded the medal as a result of their having "designed the software code that is used to transmit data over the Internet".

The next IETF meeting (IETF65) will be held in Dallas, Texas, USA, 19-24 March 2006. The Summer IETF will be held 9 - 14 July. The venue has not been finalised yet.

### Host address

Ed Juskevicius, representing Nortel, the host of this IETF, gave some insight into the tasks and challenges of an IETF host. They range from finding a suitable venue, fulfilling extensive network requirements all the way to providing tee shirts and an exciting social event. Ed thanked the many sponsors, advisors, volunteers and the NOC team.

### IAD update

Ray Pelletier, the IETF Administrative Director (IAD) presented the IETF budget for 2006. Of note is the increase in budget for the RFC editor provided by ISOC. By providing these additional resources, it is expected to reduce the RFC editing backlog.

## IETF64 Facts and Figures

**1291 registered attendees**

**from 40 countries**

**3 new WGs**

**3 WGs closed**

**435 new Internet-Drafts**

**833 updated Internet-Drafts**

**61 IETF Last Calls**

**92 approvals**

**around 100 published RFCs (47 standards and BCPs)**

**3 appeals**

Ray also confirmed that Foretec, the organisation that has provided secretariat and meeting support to the IETF since 1998, is being acquired by Neustar. A service contract between Neustar and the IETF Administrative Support Activity (IASA) for taking on the secretariat functions and the meeting organisation is under negotiation. *Editor's note: an agreement is now in place - see the article on page 1 for details.*

In December, the IAD will visit the RFC Editor and IANA for further discussions on improving efficiency and integration with IETF secretariat operations.

In 2007 a Request for Proposal (RFP) for the secretariat and meeting support will be issued. An RFP for the RFC editor function will be issued in 2006.

#### **IAOC update**

Lucy Lynch, the chair of the IETF Administrative Oversight Committee (IAOC), followed with an update on the IAOC activities. Recent activities include negotiations of the terms of the IETF trust and setting up a model license agreement for the trust assets. With respect to the IETF trust, the IAOC reached substantial agreement with CNRI and ISOC.

Right after the meeting the IAOC chair sent a call for consensus to the IETF mailing list asking for community affirmation of the IETF Trust document.

A list of frequently asked questions on trust matters has been developed by the IAOC: <http://koi.uoregon.edu/~iaoc/docs/TrustFAQv1.1.txt>

More information on the structure of the IASA, the IAOC members, minutes of IAOC meetings and more details about the IETF trust can be found here: <http://koi.uoregon.edu/~iaoc/>

#### **RFC Editor update**

Joyce Reynolds, representing the RFC Editor, reported on recent activities. Since the last IETF 105 documents (3000 pages) were published. People are working hard to reduce the backlog and results can be seen now. The RFC Editor collaborated on an experiment to introduce editing earlier in the IETF process. The results were presented during the techspec BoF at this IETF. Joyce further reported that delays introduced by normative references to as-yet-unapproved documents have become a major problem. Therefore the RFC Editor has decided not to work on a document until those references have been resolved. The publication queue is now automatically updated at <http://www.rfc-editor.org/queue.html>

#### **IANA update**

Barbara Roseman, operations manager of the Internet Assigned Numbers Authority (IANA), gave an update on IANA's recent activities.

David R. Conrad joined the IANA as General Manager in October. IANA now has seven staff members. Most requests are now handled within 30 days. There are still a number of older requests though. Barbara encouraged everyone who has a request pending that is older than 30 days to contact the IANA at [iana@iana.org](mailto:iana@iana.org).

The IANA will be working with the IESG to agree on time frames in which to complete requests and will report back to the community on the performance against those goals. With the new staffing level, Barbara said she is confident that the IANA is in a position now to address the full diversity of their responsibilities.

#### **Process and Tools (PROTO) team update**

Allison Mankin, one of the team leaders of the Process and Tools (PROTO) team, reported on the work of the team. Operational guidelines for WG chairs have been developed and many WG chairs are in fact using them. Since the guidelines have been published about a year ago, a lot of useful feedback has been received by the PROTO team.

In fact, during this IETF new tools have been used to allow WG chairs to upload presentations and proceedings directly to the IETF web site.



are currently ten Research Groups active in the IRTF. In the future there might be new work on small-group multicast.

The Routing RG held a meeting with the IAB to review the status of the research. Aaron has also been working with the IETF attorney to find out if the IETF Intellectual Property Rights (IPR) policy could be applied to the IRTF.

Finally, the IRTF started to use the Friday afternoon slots for RG meetings. At this IETF the Host Identity Protocol Research Group (hiprg) met.

The next presenter was David McGrew who gave a report on recent findings of the Crypto Forum Research Group (CFRG). The discussion on specific cryptography mechanisms concluded with a suggestion for people active in the security area to publish a document with recommendations for specific mechanisms (also see the article by Eric Rescorla in this issue of the IETF Journal).

The IAB Chair Leslie Daigle provided an expanded update at IETF64. Taking the opportunity of the NomCom cycle (looking for next year's IAB members) she provided an overview of the IAB's documented responsibilities and used that to give context to reported IAB activities (see 'News from the IAB' for a full IAB report).

### ***IAB Town Hall Session***

During the open Town Hall session following the technical presentations, a number of issues were raised and recommendations made to the IAB.



A view of Vancouver - the location of IETF 64  
photo: Mirjam Kühne

During this IETF week, IAB members took an active role in BoF meetings. In fact all BoF meetings are attended by at least one IAB member. It has been suggested though that the IAB would be even more actively involved in the formation on BoFs to get an early architectural review of new work brought into the IETF.

Overall, the community appreciates the IAB taking a more active role in the early stages of BoF and WG meetings. Also the IAB documents are seen to be useful.

A suggestion was made to create clearer guidelines for the formation of BoF meetings. Sometimes people who bring new work into the IETF think they have to shape the BoF or WG by themselves whereas in fact, it is a community issue. It is important

to understand the architecture and the big picture early on in the process. It was felt that a closer partnership between the IESG, the IAB and the BoF organisers is needed.

This was followed by a discussion on increased complexity in the transport layer and the risk to lose interoperability of various protocols. Some people felt however that this is an integral part of the IETF: "We don't do systems, we do pieces. We never say that all this works on the same box." said Bob Hinden. This has to be considered carefully when implementing. "If we want to change this, this would fundamentally change the work of the IETF," Bob Hinden added. He suggested to document this clearly (possibly as an IAB document?).

Pekka Nikander, a member of the IAB believes that in this context the identifier/locator split is the right approach. "If we want to have mobility and multi-homing at the same time, we need a new layer of indirection," said Pekka. He suggests to continue this discussion on the new mailing list:

[architecture-discuss@ietf.org](mailto:architecture-discuss@ietf.org).

The last topic brought up during this plenary session was related to the work and charter of the cross registry information service protocol (crisp) WG and the question if crisp can also be applied to Routing Registries. Leslie pointed out that crisp is focused on domain and address, but not on routing registries. Kurtis Lindqvist added that "there is a fundamental difference between an address object and routing objects." The Regional Internet Registries are actually working on a certificate mechanism to address the issue of route authentication.

In that context one should not forget that the routing topology looks different in different parts of the world: "In the ISP community in Japan hierarchical route management is an accepted concept." stated George Michaelson, co-chair of the crisp WG. But globally this is not the case.

In closing, Alex Zinin, one of the Routing Area Directors reminds people not to confuse hierarchy of routing and hierarchy in address allocation: "For routing, hierarchy is not needed, aggregation is what is important. As far as address allocation goes, the address space has to be managed." Alex said.

All presentations given during the IETF 64 plenary session can be found at:  
<http://www.ietf.org/meetings/past.meetings.html>

# IETF64 Review: Routing

By Geoff Huston

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

The following is a review of the current status of the working groups that either met at IETF64 or whose status was reported at the Routing Area meeting during the week of IETF64 in November 2005. This is of course a set of personal opinions and perspectives rather than an official report of the IETF.

## **Routing Area Working Group (rtgwg)**

Alex Zinin, one of the Area Directors of the Routing Area announced his intention to step down from this role in March 2006, at the expiration of his current term as AD. Alex has served for four years as an AD for the Routing Area of the IETF and has established a careful consultative style as an Area Director. I'd like to simply say here a personal thanks to Alex for his time and energy over the past four years.

RFC1264bis - a review of Routing Protocol Standardization Criteria. A number of changes are being proposed here, including turning the protocol analysis documentation, which was a mandatory requirement for Proposed or Draft Standard protocol specifications, into a chartered step if it is felt that such an analysis is a requirement for the protocol being developed. The experience with BGP was that this particular analysis was an exercise required for the IETF standards process, but was not felt to be a useful document in its own right. The current proposal is to either place the preparation of this document into the charter as an explicit Working Group deliverable, or do not prepare such an analysis. Also within scope of this review is a clarification of the independence of the two implementations from the proposed specification.

The area meeting also considered the manageability considerations proposal. This is a proposal for each routing protocol to have explicit consideration of manageability while designing the protocol. The discussion of this proposal highlighted the consideration that making this a required considerations section in a protocol specification may not necessarily be a lever to get people to think about this topic, and it stands the risk of adding more boilerplate text to specification documents. On the other hand, thinking about manageability early in the process of protocol specification may be a useful exercise. However, there was no overwhelming push to make this a mandatory part of routing protocol specifications.

IP Fast Reroute - the microloop prevention specification has been updated, as have the base protocol and framework documentation.

## **Common Control and Measurement Plane (ccamp)**

There has been a collection of RFCs published recently (RFCs 4201 through to RFC4210) on a common theme of Multi-Protocol Label Switching (MPLS) extensions and refinements, including six from the CCAMP Working Group on the topic of control and management extensions. A further eight documents are in the RFC Editor queue, nine documents have completed working group last call and seven are still being considered by the working group. Given this relatively high level of document generation, the pace of work in this working group has been quite intense in recent months. A revised charter for CCAMP reflects an intention to deliberately pace the next round of activity to match the capacity of the working group to carefully review material, but nothing dramatically different in terms of direction here. The meeting at IETF64 had a relatively full agenda, including the following items: The group is working on an update of RFC3946 in an attempt to clear up a potential ambiguity, and in the way of many similar efforts, what was in the first instance a relatively straightforward minor task of altering a condition that was 'greater than 1' to 'greater than or equal to 1' has become infused with all kinds of complexities relating to already deployed implementations that have interpreted the existing text literally, while others have used a more liberal interpretation. It was

reported that a resolution appears to be in sight, and it is expected that this will clarify some of the issues in interworking between the SONET and SDH systems.

Other activity includes consideration of addressing in GMPLS networks, Traffic Engineering LSPs and the interaction with the RSVP protocol. Related work is on a Network-to-Network Interface specification (NNI) for GMPLS and an associated area of study of inter-domain GMPLS. One of the proposed work items I found interesting was that of virtual concatenation coupled with Link Capacity Adjustment within a GMPLS framework, which is proposed for a general inverse multiplexing technique that could be used across a number of transport technologies, including SONET, SDH, PDH and OTN. For those of us who have struggled with various forms of inverse multiplexing over the years in an effort to treat a number of parallel circuits as a single virtual circuit with a capacity equal to the sum of the multiplexed components, this news of a generalized approach is indeed promising news.

### ***Forwarding and Control Element Separation (forces)***

It appears that this working group is relatively close to completion of its work. To recap from the charter of this working group, the emergence of off-the-shelf network processor devices that implement the fast path or forwarding plane in network devices such as routers, along with the appearance of a new generation of third party signalling, routing, and other router control plane software, has created the need for standard mechanisms to allow these components to be combined into functional systems. In other words ForCES is an effort to standardize a number of internal control interactions between the logical components of a routing engine. To continue from the charter, ForCES aims to define a framework and associated mechanisms for standardizing the exchange of information between the logically separate functionality of the control plane, including entities such as routing protocols, admission control, and signalling, and the forwarding plane, where per-packet activities such as packet forwarding, queuing, and header editing occur. At IETF64 there was an interesting presentation of a ForCES router implementation, with a control element and a forwarding element linked by ForCES protocol messaging. It seems that we are nearing the completion of this effort.

### ***Inter-Domain Routing (idr)***

From a somewhat personal perspective, the good news from this meeting was the completion of this Working Group's efforts with preparing the 4-byte AS proposal. This has been parked in the working group for some time awaiting two independent implementations of the specification before being able to proceed as a Proposed Standard. With the recent implementation report on these implementations this draft is now on its way to being a Proposed Standard. A similar issue was associated with the AS Confederations specification, and with the recent implementation report this specification has also completed working group review, and is ready for publication as a Draft Standard. The Working Group has also been working on a revised base specification for the BGP protocol, and this group of documents is now with the RFC Editor.

The new work being introduced into this working group includes the use of an explicit AS Time To Live (TTL) for BGP advertisements. Currently it is possible to specify a TTL of 1, by specifying 'NO EXPORT', but not any values higher than 1, so advertisements are either highly constrained to immediate BGP peers, or completely global. Like similar previous efforts with the 'NO PEER' community attribute, the TTL specification is an attempt to localize the propagation of a routing advertisement to a particular AS radius.

The IDR Working Group continues to see a wide variety of proposals for refinements to BGP, including outbound route filter grouping, aggregated withdrawals, dynamic AS renumbering, multicast signalling and explicit support for route tunnelling to support various forms of overlay configurations. The major criteria here for advancement of a proposal in the standards process is a writeup of two independent implementations of the proposed specification.

Of course there is also no shortage of proposals that appear to be on a continuous loop, and QoS routing, or in this context inter-domain QoS routing, is perhaps one of the best known of these proposals. It's not all that easy to identify precisely what has changed at each iteration of such proposals, and at each time the proposals tend to founder on one of the basic precepts of the Internet's inter-domain routing architecture, namely that routing is not a resource management system. The entire topic of how to manage a network's resources, and to how solve the associated feedback signalling mechanisms remain very resilient as outstanding problems in the routing space.

### ***IS-IS for IP Internets (isis)***

As reported to the routing area, the IS-IS working group has now pushed most of its drafts through the process, including link attributes and router capability advertisements. Rechartering of this working group is the logical next step, and the decision at this point in time is whether to identify a number of work items relating to further IS-IS extensions (such as Layer 2 end point definition) and refinements (such as logical tunnel concentration) and recharter the group to work on these items, or to leave the working group dormant for a period while the current drafts complete their path through the publication process and await a critical mass of new work proposals for IS-IS before reactivating the working group with a new charter.

### ***Layer 1 Virtual Private Networks (l1vpn)***

It is still early days for this particular working group, and this is their second meeting. Someone well versed in the 7-layer network model would see layer 1 as a media adaptation layer, primarily concerned with electrical voltages, plug and socket dimensions and encoding formats. This is not quite the case here. This form of VPN is based on a switched circuit-based network, that may be composed of optical cross-connects, time division cross-connects or fibre switches. The VPN control plane is used to provision a set of switching configurations to inter-connect Customer Edge (CE) devices in a specified topology. The working group is currently working on two documents, framework and applicability, and will shortly start looking at the solution aspects of this form of switch control. With a considerable level of interest in the research community in various form of light-path switched systems for very high speed point-to-point on demand circuits, this form of automation of control of the switching elements appears one promising way to handle on-demand high speed circuit provisioning.

### ***Mobile Ad-hoc Networks (manet)***

To quote from the charter of the ad-hoc autoconfiguration working group, from the IP layer perspective, a MANET presents itself as an IP multi-hop network formed over a collection of links. Thus, each ad-hoc node in the MANET is, potentially, acting as a router in order to provide connectivity to other nodes within the MANET. Each ad-hoc node maintains host routes to other ad-hoc nodes within the MANET, in addition to potentially holding network routes to destinations outside the MANET. If connected to the Internet, MANETs are edge networks, i.e. their boundary is defined by their edge routers. Due to the nature of the links over which a MANET is formed, ad hoc nodes within a MANET do not share access to a single multicast-capable link for signalling. This implies that the usual delivery semantics of link-local multicast and broadcast are not preserved within a MANET.

The specification for this topic is now relatively well fleshed out and the working group is now calling for early implementation reports of the MANET protocols. A small number of drafts remain active in the working group, concerning dynamic source routing, on-demand routing, a link-state routing protocol and a simplified multicast forwarding protocol. It is likely that these documents will be completed in early 2006. Also the group is spinning off activities in other areas, such as the autoconf working group in the Internet Area, and interest in a MANET research group to look at topics such as multicast, link metrics and the potential of QoS-related activity.

***Multiprotocol Label Switching (mpls)***

As with IDR, OSPF and IS-IS, the MPLS working group is now one of the more venerable working groups in the routing area. Most of its chartered goals and milestones have been achieved, and the current work is focussed on a number of matters relating to ICMP handling, management considerations and OAM requirements and framework, failure detection and graceful restart mechanisms, point-to-multipoint paths. The decision point appears to be rapidly approaching whether to recharter MPLS, or to wind up with this working group and charter more specific working groups on the basis of demonstrated interest in specific areas of further MPLS refinement.

***Open Shortest Path First IGP (ospf)***

There has been some good progress on some long-standing work items in this working group, with work on refresh and flooding in stable networks, graceful restart and prioritization and congestion avoidance all being published as RFCs. The working group is currently completing work on IANA Considerations to create a number of IANA registries for OSPF types and options, as well as traffic engineering extensions for OSPF v3. Current activity includes consideration of multi-topology routing, where a number of basic approaches including reuse of the IPv4 Type of Service (TOS) bits with altered semantics in the context of OSPF v2, or use of OSPF v3 with separate instances of OSPF for each topology instance, or the use of tagging OSPF protocol elements with Type Length Value (TLV) headers to allow a number of routing contexts to co-exist in one OSPF environment. The OSPF working group is also looking at the integration of the Mobile Ad-hoc network (MANET) requirements into OSPF v3, looking, in particular, at how to manage potential flooding instances and reduction in the level of formed adjacencies. Rechartering of the OSPF Working Group also appears to be a near term option.

***Path Computation Element (pce)***

The PCE Working Group is chartered to specify a Path Computation Element (PCE) based architecture for the computation of paths for MPLS and GMPLS Traffic Engineering LSPs. In this architecture path computation does not occur on the head-end label switching device, but on some other entity that may physically not be located on the head-end device. As reported to the Routing Area, this working group is evidently making good progress, with the architecture description at a mature state and the requirements document also close to completion. The group is intending to complete these documents before heading into the protocol specification phase of their work. At this stage the working group is looking at candidate path computation communications protocols, and protocols of the discovery of path computation elements.

***Routing Protocol Security Requirements (rpsec)***

This group did not meet at IETF-64. As reported to the routing area meeting, the main work item at present is the security requirements document for BGP. This document is supported by reasonable agreement on most aspects, but there remain a small number of strongly contested items, and there is no clear way forward at this stage to resolve this. There has evidently been some discussion in the working group on starting a work item on Interior Routing security requirements at this stage, and defer the resolution of the remaining BGP items for the moment.

***Source-Specific Multicast (ssm)***

The SSM architecture document has been approved by the IESG. As this was the last remaining work item for the working group, it may be that the working group has now completed all its work!

***BoF Sessions***

One way to charter new work in the IETF is via the BoF, which is a more informal session designed to assess the level of interest in the work, and see what related

issues may be exposed when considering a particular topic. Two BoFs were held in the IETF-64 within the Routing Area:

### ***Secure Inter-Domain Routing (sidr)***

The BoF reviewed the current status of RPSEC, and the current state of design activity in the area of secure inter-domain frameworks. The proposition was advanced that while RPSEC has not concluded as yet, there is sufficient impetus to commence work on infrastructure and protocol support mechanisms intended to address aspects of securing inter-domain routing. The specific area where there has been clear agreement in the requirements specification activity is that of authentication of route origination.

The proposed work would include consideration of the relevant certificate infrastructure to support information validation. It was noted that the outcomes of this activity should be capable of supporting hierarchical rooted PKI models as well as decentralized "web of trust" models if at all possible, as the intended scope of application of this framework encompasses a broad diversity of deployment environments.

There was support from the BoF attendees for the aspects of the work where there is clear agreement on requirements, concerning authentication of route origination information and use of associated certificate frameworks, to be undertaken immediately. The question of charter scope was considered and the rough consensus in the BoF was to support a charter that encompassed a more comprehensive security framework for inter-domain routing, but with a caveat that commencement on any particular component of the work would be conditional on clear agreement on requirements from the RPSEC Working Group.

### ***GMPLS-controlled Ethernet Label Switching (gels)***

When all you have is a hammer, then everything looks like a nail, or so goes the saying. So when all you have is Generalized Multi-Protocol Label Switching (GMPLS), then everything looks like a collection of potential label switching devices! (Although some people have been heard to comment that when all you have is GMPLS then, unfortunately, everything still looks like a nail!). This session was to see if there was interest in applying GMPLS to Ethernet switches in support of point-to-point label switched paths. This is very close to the existing effort in CCAMP, but with the addition of wanting to place label information into the Ethernet frame and then coordinate the switches via a GMPLS superstructure. The proposed work was to include definition of protocol-independent attributes for describing links and paths that are required for routing and signalling Ethernet switched point-to-point paths, and specification of routing protocol extensions (OSPF, ISIS) and signalling protocol extensions (RSVP-TE) required for Ethernet switched point-to-point path establishment.

If you are looking for a clean delineation between layers 2 and 3 of the OSI protocol stack model in this work you are probably not going to see it! This a blurring of the original protocol model that attempts to create logical point-to-point circuits between Ethernet switching devices, where the circuits are constructed using a label path across label switching devices using some form of routing mechanism to determine edge-to-edge paths. Not all BoFs become chartered as working groups in the IETF, and there was evidently little support in this case to continue with this work in the IETF.

# IETF64 Review: DNS

By Jaap Akkerhuis and Peter Koch

The DNS ext working group started with business as usual - a run down of the status of various Internet Drafts (ID). For a complete list, see the agenda at: <http://www3.ietf.org/proceedings/05nov/agenda/dnsextd.htm>.

Draft minutes of the working group are available here: <http://www3.ietf.org/proceedings/05nov/minutes/dnsextd.txt>.

The mDNS ID returned to the working group. The chairs post a summary about the comments to the mailing list with a request for review.

## **DNS Testing**

The Tahi group reported on their first interoperability testing effort. They tested one DNS client and found some bugs in the client and some bugs in the testing tool. They did not find any issues with the basic DNS specifications. The next scheduled Tahi testing event is at the end of January 2006.

## **NSEC3 Update**

The definition of the NSEC3 records is progressing rapidly. Among the things that got discussed was whether a new record type might be needed for storing meta data. This would help to prevent collisions of hash names and legitimate zone names. A decision about this is delayed until experience is gathered from real implementations. Such experiments should take place before the document is advanced. A testing and engineering workshop might be held at the beginning of 2006.

## **The Big Trust Anchor Management debate**

The way the trust anchor for DNSSEC in the resolver is managed is not defined, but this needs to be done. Doing things manually is error prone so people are looking into ways for automating this process. Currently there are four proposals - with IDs already written for three of them. There are various intellectual property claims to a couple of these ideas, but the strength of each individual claim is not clear. During the discussion it became evident that all solutions are struggling with at least two different problems: Initial key distribution and key roll over. The need is felt for a short requirements document. Some volunteers have stepped forward to write this within a short time frame (three months).

## **The Sky is falling!**

The crypto algorithms used in DNSSEC come from standard sources. One of these, the SHA-1 is under attack and some weaknesses have been found. The way that DNSSEC uses SHA-1 is not affected by this weakness, so the sky is not really falling. Since there is not yet widespread deployment of DNSSEC, it is better to replace SHA-1 by SHA-256 now, just in case SHA-1 gets even more tainted in future. For this purpose a new ID will be written which will make SHA-256 mandatory to implement.

## **Workload Review**

The chairs suggested that for a working group document to advance or to be accepted at least four or five people should have committed to review. If not, it will be dropped by the group and authors will have to do a personal submission. The room hummed consensus.

## **DNSOP**

The WG has a new co-chair, Peter Koch, replacing David Meyer. The participants agreed to work on the document backlog one-by-one to significantly reduce the number of open and close-to-finished documents before the next meeting in Dallas.

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

This is why no new work was adopted as WG items. For a list of current work items, see <http://www3.ietf.org/proceedings/05nov/agenda/dnsop.txt>

#### *6to4 Reverse DNS Delegation*

The (expired) draft-huston-6to4-reverse-dns-03.txt describes a potential mechanism for entering a description of DNS servers which provide "reverse lookup" of 6to4 addresses into the 6to4 reverse zone file and is asked by an IAB IPv6 ad-hoc to be published by the DNSOP WG. After some discussion whether the WG should publish other people's work, it was agreed to do so. Some reviewers stepped forward.

#### *Cross-WG review*

Other WGs (e.g. ENUM, GEOPRIV, ECRIT) are increasingly asking for review of their drafts by DNSOP (and DNSEXT), often via the IESG. As an example, the ENUM WG feels the need for clarification about ENDS(0) and volunteers were found to write such a document. Here the question was also how to communicate to both vendors and network operators that EDNS0 is a sheer necessity in today's DNS operations, particularly needed for ENUM and DNSSEC, but considered non-optional in the general case.

The DNSOP WG minutes are available at <http://www3.ietf.org/proceedings/05nov/dnsop.html>

#### ***New work: AS 112 in a box***

Queries to domains such as 168.192.in-addr.arpa or 8.e.f.ip6.arpa leak all over the Internet and end up at the root-servers. There is a network of volunteers (see <http://www.as112.net/>), operating (anycasted) domain name servers trying to answer these queries, before they hit the root servers. For a description see the <http://public.as112.net/> website. The new work proposes that resolvers themselves should directly return authoritative answers for special domains

# IETF64 Review: IPv6

By Mikael Lind

The 64th IETF was a big milestone for IPv6. It marked the end of the IPv6 working group and hopefully the beginning of large scale adoption of IPv6. It was concluded that this would be the last face-to-face meeting of the IPv6 WG but that the working group should stay open until all unfinished work is done. There are no big items left on the charter although several documents are currently being revised (e.g. address selection RFC 3484). The largest remaining task is perhaps the shepherding of the core specifications to Internet standard. During its existence the IPv6 working group has produced 69 RFCs and it still has 11 drafts on their way to RFC.

## **Neighbor discovery**

RFC2461bis is one of the documents underway and the last remaining piece was the issue about the meaning of the 'Managed address configuration' flag and the 'Other configuration' flag. The accepted solution at the meeting was to say that M flag indicates a client should use DHCPv6 for all configuration information and only use DHCPv6lite if just the O bit is set. Related to the management flag discussion was the issue when an ISP wants to force a user to use a specific address. Even if the management bit is set by a router there is no guarantee that the client doesn't use any other address such as privacy addresses. This will create problems with access control since the client address isn't always predictable. One solution would be not to include a prefix in the router advertisements.

## **IPv6 Operations**

There's no lack of operational issues related to IPv6. One big task at the meeting was to figure out what to take up as work within the WG and what to send off to other groups. Documents that already are WG items and now starting to be finalized are Broadband deployment scenarios, Enterprise Analysis, and Network architecture protection. The Broadband deployment document will ship without an updated cable networks section since the new cable network specification isn't quite ready. The Enterprise analysis will just have a small rewording regarding DSTM before moving to the IESG. One document that was taken up as a new WG item was IPv6 Implications for TCP/UDP Port Scanning. There are many other interesting documents in the working group and the work would definitely gain from a wide community review since all operational input is useful.

## **Softwires**

At IETF63, Softwires was a BoF but it has been very active and has held an interim meeting to finalize the problem statement. Softwires was approved as WG during IETF64 and will now start working on flexible tunneling mechanisms that work in two different scenarios; the first being hubs and spokes and the second mesh. These more or less represent end host and core network cases. One of the important goals is to make the mechanisms independent of the tunnelling protocol so that it can be optimized to different networks and provide integrity when needed.

## **IPv6 over IEEE 802.16(e) Networks**

This was a BoF to start a working group that would work with IPv6 over 802.16 networks or WiMax. There was some confusion as to what was the actual problem since it is possible to run IPv6 over 802.16 today. The statement was that the functions in 802.16 networks make IPv6 perform poorly and that there has to be additional work done. One question many asked was if this shouldn't be something that should be fixed in the 802.16 standard instead of in the IETF. In the end there was no clear consensus on how to proceed and there will not be a WG created right now.

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

## IETF64 Review: SHIM6

By Geoff Huston

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

It's always handy in a working group to have had some other working group do all the heavy lifting in terms of defining the problem, sorting out requirements, looking at the threats and documenting the basic architectural issues. In the case of SHIM6 this includes working through a relatively hefty collection of candidate proposals and identifying an approach that appears to offer the most promise. In the case of SHIM6, much of the work was already undertaken by its predecessor, the MULT16 working group, which looked at the more general topic of multi-homing in IPv6.

So to briefly recap here over some well covered territory, when the scaling issues with the Internet were examined in the early 1990's, two basic problems were identified. The first was that the IP environment was indeed running out of addresses, and secondly that the routing space was running out of capacity. The interim approach was to adopt a new address architecture in IPv4 that removed the 'class-based' semantics of an address, and instead used an explicitly specified prefix length for all address prefixes. The longer term approach was to work on a protocol specification that extended the address space significantly. The approach adopted by the IETF in this new protocol was a relatively conservative one that extended the address space from 32 to 128 bits, but made no other basic changes to the IP architecture. So the question remained on the table: how do you solve the routing capacity problem in IPv6?

The response to this open question has been to devise address allocation policies that lean very heavily towards provider-based address aggregation. In other words the response to the routing capacity problem has been to attempt to adopt strict policies that suppress the advertisement of more specific prefixes in the inter-domain routing space and instead attempt to work from the basic premise that the inter-domain routing space will be populated exclusively by Internet service provider aggregate prefix advertisements.

This approach raises a number of issues around the concepts of protocol support for services that support mobility, nomadism and multi-homing. Indeed these topics are all artefacts of a more basic and long-standing issue in the IP architecture: IP managed to combine the concepts of network level identity, network level location and network level packet forwarding into one object, namely that of an IP address. In other words the basic concepts of who, where and how are all encompassed in a single IP address. When you need to split these concepts apart and separate the 'who' from the 'how' or the 'where', then the work gets quite challenging. So far we've managed to put a name to the general class of the problem, and these days when you hear the term 'id/loc split', you've just heard a reference to this issue of the overloaded semantics of an IP address.

SHIM6 is concerned with a particular aspect of this more general topic of the disambiguation of identity and network location, namely that of a collection of inter-connected hosts, or a 'site', that uses multiple service providers for connectivity services, and where the site exclusively uses address prefixes drawn from these upstream providers. In other words the 'site' is 'homed' with multiple service providers.

The approach used in IPv4 was that of using a unique address prefix for the site (preferably an address that is not part of any provider's address prefix), and announcing reachability to this address prefix to all upstream providers simultaneously. The global inter-domain routing system is used to stitch all this together, and provide, hopefully, seamless and reliable connectivity such that even when there is a failure in the services provided by one or more of the upstream providers, basic connectivity is maintained, and application level connectivity is maintained and no application needs to be aware that there are multiple upstream

providers, or even when the underlying network paths switch between these providers. This works relatively well, but at the expense of the scalability of the routing system. While the global routing system today can support some tens of thousands of multi-homed end-sites, most folk would agree that current technologies and deployed equipment would be incapable of scaling this to numbers of the order of tens of millions of such multi-homed sites, and some folk would be worried even at numbers in the hundreds of thousands.

So is there a way in IPv6 to avoid overloading the routing system with provider-independent address prefixes, and still preserve the essential functionality of multi-homing? To enter into one level of further detail, the objective can be phrased as how to support IPv6 end-site configurations that have multiple external connections to support application-level session resiliency across connectivity failure events, and how to use IPv6 multi-addressing and connection-based address aggregates to avoid overloading the routing system with site-based specific address advertisements.

It was this general question that was studied in the multi6 working group, and a very wide diversity of approaches was evaluated by the working group. The approach selected by the multi6 working group, the so-called "Level 3 Shim" is the approach that the SHIM6 Working Group is tasked to complete.

The major aspect of this approach is that no provider-independent address is assumed, and each host within the site obtains an address from the router advertisements corresponding to each upstream provider's address prefix. Each host will use one of these addresses as its source address, and when it is talking to a remote host who also has multiple address prefixes, it will chose the first 'working' address as the chosen destination address, where 'working' is interpreted as an address that elicits a response. The basic approach of initial contact in a multi-addressed configuration is documented in RFC 3484.

The challenge here is not in the initial contact, but further on, when there are one or more active application sessions using a particular provider's address prefix, and the network path of that provider fails. How is this failure detected? How is a 'working' prefix identified? And how can the local host switch across to working addresses without disrupting the operation of any of the active upper level sessions? And how can this address agility functionality be provided in a secure fashion that is resilient to various forms of hostile attack?

The approach, like most other approaches to this problem space, uses a rewriting of the protocol header part of the protocol data unit (PDU), substituting a 'working' address in place of the upper level address in a manner that is not directly visible to the upper level protocol state. In other words the upper level protocols perform a rendezvous using an 'identity' which is preserved across the life of the protocol session, while the lower level of the protocol stack substitutes a 'locator' in place of this identity before passing the packet into the network, and perform a reverse substitution when receiving a packet from the network.

The SHIM6 approach has made a number of specific design decisions in order to devise a prototype model. The identity/locator substitution is performed within the host's own protocol stack, rather than remotely in an edge router or in some other remote network-level agent. Secondly, this mapping between identities and locators, and associated state information, is maintained at the IP level of the protocol stack in the host, implementing a host-to-host context of this mapping, in preference to a transport-level mapping. Thirdly this is a dynamically negotiated capability, and is only activated after a certain threshold of time or quantity of packet exchange has already taken place. And, finally, there is no new identifier space associated with this design – the addresses used to make initial contact with the remote host are nominated as the persistent identity tokens once the SHIM module is activated.

The basic operation of SHIM6 is that of a functional module located at the IP level of the protocol stack, where there is no explicit knowledge of transport level session establishment or tear-down. At this level there are simply packets being passed

between the local host and remote hosts, where the remote host is identified by the destination address in the PDU passed through the SHIM6 module. Initial contact with a remote host elicits no particular SHIM6 response. The application is expected to undertake a pass through all address pairs in order to achieve confirmed contact, in the manner specified by RFC 3484. Only when a certain communication threshold has been achieved with the remote host (by time, packet counters or some combination) will the local shim module attempt to establish a shared state with the remote host. This entails an initial handshake with the remote host to confirm that the remote host is also equipped with this model and is prepared to activate it on this host-pair. The modules then exchange a currently active set of locators or each host, and then drop into a passive failure detection mode. In the event of a detected failure of the current locator pair the shim6 modules will test the locator pool in order to establish a new working locator pair. Once this is confirmed the shim6 module is now activated, and all subsequent packets sent to the remote host will have a shim context packet header added to the packet, and the source and destination addresses of the packet altered by the shim module to the value of the currently active locator pair.

At some future point, using a local trigger based on an inactivity timer, or some other local condition, the local host will garbage collect the shim context for a remote host, and any subsequent locally-initiated contact will follow the same process.

SHIM6 is chartered to complete the specification of this particular protocol to a level of a Proposed Standard, such that independently developed implementations of the specification interoperate in an acceptable fashion. It is also chartered to complete an architectural description of the technology, as well as documenting the anticipated applicability of the approach.

The approach taken by the working group is to make a number of very conservative design decisions in order to complete an initial base protocol specification, and once this is complete to then explore a number of refinements that may include areas of support for a richer bi-directional signalling path between the shim module and cooperating upper level protocols, particularly including considerations of the transport-level session interaction with the shim module, support for site-based traffic engineering directives or preferences, support for initial contact-less SHIM6 (i.e. allow the upper level protocol to use identifiers from the outset where the identifiers do not also function as working locators), support for various refinements in failure detection, support for rapid locator failover, and explore the space associated with the problems of source address-based ingress filtering and the associated issue of source address selection by the host.

As can be seen by the length of this supposedly short introduction to SHIM6, this is a relatively rich area of study, with both a long history, reaching back to proposals such as '8+8' and 'GSE', and a diverse current activity profile today with efforts including MobileIPv6, MANET, SCTP and HIP. This is perhaps to be expected, as the original binding of identity and location within the semantics of an IP address was indeed a fundamental part of the IP architecture. When we explore ways in which to uncouple this tight association of identity and location in an IP address it's not clear that any of these approaches, either currently or previously studied, will turn out to be the uniquely 'right' approach. There are a set of constraints that are proving challenging to reconcile, including security, resilience against hostile attack, simplicity in host stacks, uniformity of routing, host agility, site policies, traffic engineering, service performance, adaptive responses to various transport and application profiles, to name but a few.

As we progress in SHIM6 to complete the base protocol specification and then as we explore various forms of refinements and extensions to this approach, I'm sure that there will be much more to learn here about what is possible with an IP architecture that makes a clearer distinction between the 'who', the 'where' and the 'how' of networking.

# IETF64 Review: Security

By Eric Rescorla

The buzz in the Security Area at IETF 64 was all about hash functions. Hash functions—in particular MD5 and SHA-1—are a key part of nearly every IETF security protocol, so it was big news in 2004 when Wang et al. announced a practical attack on MD5 (<http://eprint.iacr.org/2004/199.pdf>) and even bigger news in February 2005 when it was announced that the security level of SHA-1 was substantially less than its design goal of 80 bits (<http://theory.csail.mit.edu/~yiqun/shanote.pdf>). Improved attacks have since lowered the security level of SHA-1 to 63 bits, just inside the range of what's practical.

The three big questions on people's minds were:

- 1) Is my protocol still secure?
- 2) What hash function should I be using now?
- 3) How and when do I make the transition to a new protocol?

Although there were some differences of opinion, the consensus answers to these questions were more or less as follows:

- 1) Most protocols are still safe, even if they use MD5. The one big exception here is protocols that use MD5 for digital signatures. This practice should be stopped as soon as possible. HMAC-MD5, which is in wide use for message integrity, is still believed safe but Cryptography Forum Research Group (CFRG) chair David McGrew expressed concern that it might be broken in the near future.
- 2) Security Area Director Russ Housley recommends that new protocols not use SHA-1 and that the best current choice for a hash function is NIST's SHA-256, however many attendees expressed hope that better candidates would emerge in the near future.
- 3) Steve Bellovin, Russ Housley, and Eric Rescorla have studied the problem of hash function transitions in a number of existing IETF protocols (IPsec, S/MIME, SSL/TLS, DNSSEC, and OCSP) and in every case there are protocol problems preventing a clean transition. This means that transition steps have to be taken deliberately but need to start fairly soon.

Russ Housley has issued a call for the Security Area to review every major security protocol to determine the impact of hash function vulnerabilities and study transition strategies. Protocols that have working groups will be studied within those WGs. LTANS, PKIX, SMIME, Kerberos, and TLS have already started this process. Protocols that do not have WGs will be studied by the Security Area Advisory Group (SAAG). Volunteers are actively being solicited for this work.

Security Area Working Group meetings were fairly peaceful, with work quietly being accomplished. The Security Area held two BoFs: DKIM and EMU and one Security-related BoF (SIDR) was held in Routing.

Domain Keys Identified Mail (DKIM) is a protocol designed to allow e-mail servers to take responsibility for the messages they send. The intention is that this will be a useful tool for fighting spam and e-mail based fraud. This was the second DKIM BoF (the first was held in Paris) and the attendees were mostly in favor of the formation of a working group.

EAP Method Update (EMU) was an outgrowth of the SechMech BoF held at IETF63 in Paris. The intention here is to have a forum for the standardization of a small set of EAP methods that meet existing requirements from other SDOs. The mechanisms under consideration include additional shared secret mechanisms as well as public

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

key based ones. There was general enthusiasm in the group for moving forward with this work.

Secure Inter-Domain Routing (SIDR) is an effort to design security mechanisms for Inter-Domain Routing (i.e. BGP) while avoiding some of the focus problems that the Routing Protocol Security (RPSEC) Working Group has had. There were presentations on the three major contending protocols: soBGP, sBGP, and psBGP. This work will also probably go forward, with the understanding that rather than picking one design the final design will pick the best technologies from each candidate.

# IETF64 Review: Mobility and Wireless

By James Kempf

IETF64 saw the establishment of two new working groups related to mobility and wireless:

*MONAMI6* - working on a problem statement and standards track specifications addressing issues associated with the simultaneous use of multiple addresses for mobile hosts using Mobile IPv6 or mobile routers using NEMO Basic Support.

*AUTOCONF* - working to standardize mechanisms by which ad hoc network nodes can configure locally or globally routable IPv6 addresses.

In addition, there were BoFs related to mobility and wireless:

*NETLMM* - second BoF on network-based, localized mobility management;

*16NG* - discussed 802.16 wireless link architectures and work needed to run IPv6 over 802.16;

*EMU* - standardizing Extensible Authentication Protocol (EAP) methods.

This article will discuss the results of the first meeting of the AUTOCONF working group and progress in the DNA (Detecting Network Attachment) working group. Both working groups are in the Internet Area.

The AUTOCONF working group met for the first time at IETF64, after two BoFs. The objective of the working group is to standardize a way to configure locally routable and globally routable addresses within an ad hoc network. Part of this problem may involve discovery of routers that connect a collection of ad hoc nodes to the Internet. The working group will focus on IPv6 only, to take advantage of the more powerful local link configuration protocols available in IPv6.

One of the major issues that came up during the chartering of the working group was that the IETF has really not considered what a Mobile, Ad hoc NETWORK (MANET) is and what makes it different from a standard IP network. The first working group meeting discussed the architecture of MANETs in some detail. One presentation characterized the difference very succulently as follows: in other IP networks, the links form the network, while in MANETs, the network forms the links. MANETs tend to be characterized by half broadcast links, little or no specialized infrastructure for routing (the hosts act as routers themselves), and relatively flat routing control structures.

In the past, addresses within MANETs could be local (i.e. valid only within the collection of ad hoc hosts forming the MANET), but there is now increasing interest in hybrid MANETs, where the MANET is connected to the Internet through a gateway router. Because the nodes participating in the MANET and the links between nodes are quite fluid, MANETs see network partitions and the joining of two networks more often than other IP networks, and such operations can be thought of as a common part of a MANET's operation rather than an error condition. This kind of shifting network structure is difficult to accommodate with traditional IP network address and routing configuration. Up until now MANETs have been thought of as principally a routing problem, but work in the ad hoc research community, which is well-represented among the AUTOCONF working group members, has come up with some additional areas where standardization is necessary for good interoperability.

The DNA working group has been chartered to devise a more robust network attachment and movement detection protocol for IPv6 than currently is available. RFC 3775, the Mobile IPv6 specification, specifies passive movement detection as the default. The mobile node waits until it hears a multicast Router Advertisement, then checks whether the router was seen before. If not, the mobile node infers that it

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

has moved. The frequency of Router Advertisements is increased to 50 ms. This technique of movement detection has many disadvantages. Besides generating lots of Router Advertisement traffic, the requirement to wait until a Router Advertisement beacon is seen slows down the process of handover. In addition, if a link is configured with multiple routers, the protocol could cause the mobile node to conclude that it had moved to a new link when it really only is seeing a router advertisement from another router.

In order to improve movement detection, the working group is developing Best Current Practice (BCP) specifications for configuring hosts and routers without any additional protocol support to facilitate better network attachment and movement detection.

The DNA protocol design itself was finished by the design team. The design is based on having the host respond to a Layer 2 hint indicating that it has changed to a new access point. The host then multicasts a Router Solicitation to the All Routers Multicast Address, and receives unicast Router Advertisements from routers on the link. Both the Router Solicitation and Router Advertisement are enhanced for DNA, with additional options.

These options allow the host to indicate the link it thinks it is on, and for the router to reply indicating if the host is correct. If the router indicates to the host that it is on a new link, the router returns enough information so that the host can quickly autoconfigure a new IPv6 address on the new link and otherwise become established. The Router Advertisements are returned without the delay required by RFC 2461. Such delays can significantly hamper the ability of a mobile node to quickly configure on the new link. The protocol also contains security features to limit the ability of an attacker to subject the link to a Denial of Service attack.

# IETF64 Review: Internationalized Email and Extensions (IEE)

By Marcos Sanz

More than one and a half years have gone since the last Internationalizing Email Address BoF, which took place at the IETF 59 in Seoul, and apparently the time has now come at the IETF 64 for a working group to be formed and to take a stab at the issue of fully internationalized email addresses. The biggest push for this work comes from IETFer colleagues in China, Japan and Korea. And not without reason: imagine you have to transliterate your names from Hangul or Kanji into ASCII for most of the email addresses you type. This is not only a cumbersome and alienating process, but also an error-prone one. On top of that consider, you only would have to do that for the left hand side of the '@' character, since the right hand side of the address, the domain names, are already internationalized by the IDNA standard (RFC 3490). Now, how incoherent is this current situation?

Different to the IDNA solution, the current approach, as discussed at the IEE BoF, is not occurring at the presentation level, but consists of a series of far-reaching modifications to the underlying protocols:

- The definition of a mailbox in RFC 2821 is revisited and updated in order for the Local Part (everything left of the '@') to support the full Unicode range of characters, not only ASCII, and for the Domain part (everything right of the '@') to support the IDNA standard. This new form of mailbox is called the Internationalized eMail Address (IMA).
- The mail transfer protocol SMTP needs a service extension that will allow mail transmission agents (MTAs) to signalize to their clients at the moment of the session establishment that they support IMAs. Clients that are confronted with that extension will then be able to transmit IMAs in raw UTF-8 encoding to the MTAs in the SMTP commands. The IMA extension is dependent on previous support of the 8BITMIME (RFC 1652) extension by the MTA.
- IMAs will not be confined to the SMTP envelope, but spread all over the headers of an email, so the need for characters beyond ASCII in the values of header fields becomes obvious. Though MIME-Extensions (RFC 2047) already provide for partial internationalization support in headers by means of different encodings on the wire, these extensions don't go far enough. Now with IMA, the definition of header fields as of RFC 2822 will be updated for them to natively support the whole Unicode character space. If an SMTP client communicates with an MTA with IMA support, the client can encode any header field in raw UTF-8. The syntax of header names, however, remains unchanged.
- A last, but crucial issue: downgrade mechanisms are defined for the case in which any of the MTAs involved in the delivery chain of a mail would not support the IMA extension. Basically, the MAIL and RCPT SMTP commands will support an optional parameter (ALT-ADDRESS) that allows a client to convey an alternative non-internationalized address, which could be used as a fallback instead of the original IMA. This alternative address could also be automatically generated by applying an ASCII encoding mechanism similar to the ACE used for domain names to the whole IMA, thus mapping it into ASCII. The latter kind of downgraded addresses would be marked accordingly. It would be up to the final MTA (or mail delivery agent) to decode the downgraded fields to turn them back into IMAs. As a last resort, when everything else fails, the mail could always be bounced back to the sender.

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

These mechanisms, in the form of four I-Ds, are targeted at becoming experimental RFCs. Since it was recognized as a prime directive not to fragment the existing email system, these RFCs will not find their way on to the standards track before implementations appear and the extensions are thoroughly evaluated in daily operations.

Impact on other protocols which make use of email addresses, notably POP and IMAP, and on others such as LDAP, ACAP or S/MIME, will be evaluated and additional documents will be produced. Interaction with mailing lists and similar distribution mechanisms will be studied and operational guidelines for IMA deployment will be documented.

Internationalized domain names are often associated to phishing and other security problems, like the so-called homograph attack. That is partly unfair: to be true, the whole of the spoofing-attempt mails received by the author at the moment, which are not few, come from traditional ASCII domain names. Since the advent of IDNA, however, some lessons have been learnt and it is a widespread belief that the amount of characters allowed by IDNA is far beyond what is actually needed. To the eyes of the author, the internationalized email addresses effort should try to apply this knowledge from the beginning, constraining the syntax of the Local Part of the email as necessary. It would be sensible to base upon work done by other experts, like for instance, the General Security Profile for Identifiers defined by the Unicode Consortium.

All in all, a challenging, multidisciplinary task, which will need as much peer review as possible. What are you waiting for?

## IETF64 Review: New 'Birds of a Feather' (BoF) Meetings:

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

### ***Applications Area:***

xmlpatch - XML-Patch-Ops BoF

iee – Internationalised Email and Extensions BoF

### ***General Area :***

pesci – Process Evolution Consideration for the IETF BoF

techspec – Requirements for IETF Technical Specification Publication BoF

### ***Internet Area:***

softwire – Softwire BoF (met for the second time)

netlmm - Network based localised mobility BoF (met for the second time)

16ng – Ipv6 over IEEE 802.16(e) Networks BoF

### ***Ops/Mgmt Area:***

callhome – Reversing Traditional Client/Server Conn. Model BoF

### ***Routing Area:***

gels – GMPLS Controlled Ethernet Label Switching BoF

sidr – Secure Inter-Domain Routing

### ***Transport Area:***

voipeer – VoIP Peering and Interconnect BoF

fecframe – FEC over Transport Framework BoF

### ***Security Area:***

dkim - Domain Keys Identified Mail BoF (met for the second time)

emu – EAP Method Update BoF

## News from the IAB

By *Leslie Daigle, IAB Chair*



**Leslie Daigle**  
IAB Chair

The IAB has to fulfill a number of roles and responsibilities, described in RFC2850 (BCP39). In the light of the current NomCom cycle (looking for next year's IAB members) this issue's IAB update includes additional material elaborating the broad range of those responsibilities.

First, how are IAB members selected? Candidates for the IAB are selected by the IETF NomCom except for Ex-Officio members (IRTF chair and the IAB Executive Director) and Liaison members (ISOC, RFC Editor and IESG). Every year, the IAB elects a chair from within its membership.

### ***Appointment of the IESG, the RFC Editor and the IANA***

From BCP39, the IAB has a role in the appointment of the IESG, RFC Editor, and IANA. Formally, this includes:

- Confirmation of the IESG: The NomCom annually provides a list of candidates for vacant IESG seats and for the IETF chair (if vacant). The IAB reviews the candidates, consenting to some, all or none.
- RFC series: The IAB approves the appointment of an organisation to act as RFC Editor and the general policy followed by the RFC Editor.
- IANA: The IAB approves the appointment of an organisation to act as IANA on behalf of the IETF.

With the introduction of BCP101, while the IAB continues to maintain oversight of the relationships with the RFC Editor and IANA, the IETF Administrative Support Activity (IASA) means that the IAB now has fewer responsibilities for practical management of the relationships.

During IETF64, the IAB was involved in leading the TechSpec BoF (Requirements for IETF Technical Specification Publications), to discuss the specific requirements of the IETF's technical publication process. This comes from the IAB's work to oversee the RFC Editor process, and is aimed at providing further clarification of requirements there.

### ***Oversight over the Standards Process***

Even before BCP39, BCP 9 (RFC2026) defines the role of the IAB in oversight of the IETF standards process :

- The IAB provides oversight of the process to create Internet Standards
- The IAB serves as an appeals board for complaints of improper execution of the standards process

Lately, the IAB has been fortunate not to have had any appeals to deal with.

### ***The IAB is responsible for liaison relationships with other organisations***

The IAB carries out various tasks to ensure the IETF's continued open communications with other organizations to carry out our work.

- The IAB acts as a source of advice and guidance to officers and the Board of Trustees of the Internet Society (ISOC) concerning technical, architectural, procedural and (where appropriate) policy matters pertaining to the Internet and its enabling technologies.
- The IAB acts as representative of the interests of the IETF and ISOC in technical liaison relationships with other organisations concerned with standards and other technical and organisational issues relevant to the world-wide Internet.

- The IAB appoints the IETF liaison to the ICANN Board of Trustees.

While there were no new liaison relationships established between IETF63 and IETF64, the IAB has appointed some new external liaison representatives. The IAB has also established a subcommittee to work with ISOC on technical communications.

### ***Oversight of the architecture for the protocols and procedures used by the Internet***

BCP39 describes a number of specific activities in which the IAB engages.

*The IAB provides input to the IESG regarding BoFs and possible (subsequent) WG formation*

BoF meetings were attended by at least one IAB member (see more discussion on IAB's involvement in BoF formation in the summary of the plenary sessions on page 2). IAB members work to provide additional feedback to the IESG in reviewing the BoF outcome and potential working group formation.

*The IAB sponsors and organises the IRTF as well as reviewing proposed IRTF research groups*

The IRTF regularly reports at the plenary sessions. The IAB reviews the charters of WGs and RGs. At IETF64, the Routing RG had a meeting with the IAB to review the status of the Routing RG.

*The IAB can convene invitational workshops to perform in-depth reviews of particular architectural issues*

The IAB is planning to hold a workshop – called "Network Architecture meets Network Reality" at IETF64, and subsequently renamed to "Unwanted Traffic" in the first quarter of 2006.

*The IAB can organise ad-hoc groups of independent experts to discuss and provide input on various topics*

The IDN ad-hoc committee has concluded. The IPv6 ad-hoc committee will continue its work. In addition to that the IAB has established a committee to work with ISOC on technical communications and publications.

*The IAB can write (informational) documents*

The IAB has recently published a number of documents:

- "Internet Denial of Service Considerations"  
[draft-iab-dos-03.txt](#)
- "What's in a Name: False Assumptions about DNS Names"  
[draft-iab-dns-assumptions-03](#)
- "IAOC Member Selection Guidelines and Process"  
[draft-iab-iesg-iaoc-selection-03.txt](#)

As reported in the last issue of the IETF Journal, the IAB is currently focusing on the following technical issues:

- IPv6

The IAB has organised an IPv6 Multihoming Bof at the recent NANOG35 meeting to get input from the operators community. This will bring other perspectives to the discussions at the IETF. The IAB expects to organise more such sessions in the future. For more details see <http://www.iab.org/documents/open-mtgs/>

- Internet Architecture  
a new mailing list has been set up to discuss architectural issues:  
[architecture-discuss@ietf.org](mailto:architecture-discuss@ietf.org) (also see Pekka Nikkander's article elsewhere in this issue of the IETF Journal).
- Bad Net Traffic  
The IAB agreed to set up a workshop on "Unwanted Traffic". It is expected to be held in February 2006.

## News from the IRTF

By Aaron Falk, IRTF Chair

As reported at the last IETF, the IRTF is reaching out to the research community. In order to attract more researchers to actively work in the IRTF, an article was published in the ACM Computer Communication Review:

<http://www.acm.org/sigs/sigcomm/ccr/archive/2005/october/p69-falk.pdf>

In the meantime two new Research Groups have been created:

### **Transport Modelling (TMRG)**

This Research Group will develop drafts on how to evaluate congestion control mechanisms and simulation & testbed scenarios. It is further planning to produce documents on best current practices and admission control mechanisms. Sally Floyd will be chairing the group.

### **Internet Congestion Control (ICCRG)**

The ICC Research Group is chaired by Srinivasan Keshav and Mark Handley and is expected to work on a roadmap on congestion control.

In addition to that there are currently ten Research Groups active in the IRTF:

### **ASRG: Anti-Spam RG (chair: John Levine)**

The group is currently writing a draft on using the DNS to distribute blacklists and whitelists. It is further planned to work on measurements on if/how e-mail message mutation breaks a signature—related to Domain Keys Identified Mail (dkim).

### **CFRG: Crypto Forum Research Group (chairs: David McGrew, Ran Canetti)**

CFRG is currently working on an improved variant of the SHA-1 hash function and is evaluating randomised hash function and key derivation proposals. It is also reviewing the UMAC message authentication code.

### **DTNRG: Delay Tolerant Networking Research Group (chair: Kevin Fall)**

This RG is in the process of finalising the DTN architecture and protocol specs. It has recently requested a provisional URI prefix 'dtn' from IANA. It is now transitioning from architecture and design to more testing and trials. A DTN workshop took place at SIGCOMM05 which was attended by about 60 people.

### **end2end: End-to-End Research Group**

Bob Braden has retired as E2ERG chair after a 20 year tenure. Craig Partridge and Karen Sollins will act as interim chairs. Bob will continue to run the end2end mailing list and will stay on the IRSG as an ad-hoc member.

### **HIP: Host Identify Payload Research Group (chairs: Andrei Gurtov, Tom Henderson)**

This group is very active, there are currently 6 revised drafts. It is likely that some topics from the hip RG will migrate into a re-chartered hip WG.

### **MobOpts: Mobility Optimisation Research Group (chairs: Radjeev Koodli, William Arbaugh)**

This RG completed its work on "Advances in Mobile IPv6 Route-Optimized Communication". The group is now busy building testbeds and investigating the following issues:

- Link-assisted Fast Handovers
- Location Privacy with Mobility
- Network-introduced Handovers



Aaron Falk  
IRTF Chair

***NMRG: Network Management Research Group (chair: Jürgen Schönwälder)***

There will be a RG meeting in January in Oslo or Stockholm. The agenda will cover "promise theory" and P2P approaches to network management. The group is also involved in network management traffic measurements.

***RRG: Routing Research Group (chair: Avri Doria)***

The RRG has a new co-chair: Dan Massey from the University of Colorado. A number of new RG topics are under consideration: from proposals for improving convergence times to new routing architectures. The group is planning to meet at INFOCOM in Barcelona to increase participation from the research community.

There are two more IRTF research groups: the ***IMRG: Internet Measurements RG (chair: Mark Allman)*** and the ***P2PRG: Peer-to-Peer RG (Co-chairs: Bill Yeager and Bobby Bhattacharjee)***.

We continue to discuss the possibility of a research group on small-group multicast.

The Routing RG had a meeting with the IAB to review the status of the research. Aaron has also been working with the IETF attorney to find out if the IETF IPR policy could be applied to the IRTF.

Finally, the IRTF started to use the Friday afternoon slots for RG meetings. At this IETF the Host Identify Protocol Research Group (hiprg) met.

## News from the IAOC and IAD

By Lucy Lynch and Ray Pelletier

Among the most significant tasks the IAOC has been undertaking recently are negotiating terms of the IETF Trust, establishing contracts with service organisations and developing a budget for the following years.

Substantial agreement has been reached with both CNRI and ISOC on the founding document for an IETF Trust. The IETF Trust is a private legal construct (in this case established under the laws of Virginia, USA) allowing assets (in this case, intellectual property rights and other property) to be held and administered for the benefit of the IETF and hence the Internet Standards process.

Upon signing, procedures which will bind the Trustees to the same conditions for Review and Appeal as those applied to the IAOC in BCP 101 will be enacted. Both, CNRI and ISOC will put any currently held IETF related IPR into the IETF Trust at initial signing.

The IASA will license IPR as needed to various service contractors in the future. Any IPR created by those contractors as part of the terms of such a contract will then be assigned back to the IETF Trust. It is not the intention of the settlors to modify the IETF-community approved policies and procedures regarding intellectual property rights in IETF standards documents and other contributions to the standards process.

The IETF Trust may accept additional donations if the Trustees determine that it is in the interests of the IETF and in line with BCP 101. The members of the IAOC will act as Trustees.

The IAOC believes that the IETF Trust will allow the IASA to engage in contracts that require the use of IETF assets and to license those assets as needed. The IAOC chair has issued a consensus call to the IETF community mailing lists asking the IETF community for affirmation of the IETF Trust document. The IETF Trust, a model License agreement and an FAQ are available on the IAOC web site.

NeuStar has completed a Sale and Purchase Agreement with CNRI for Foretec Inc. The IASA is engaged in talks with NeuStar regarding the provisioning of IETF support services. An initial two year service agreement will be followed by an open RFP for: - network infrastructure - meeting services - the clerk's office - mail and archive support

A number of draft contract documents for secretariat functions have been discussed with Neustar: service contract, statement of work, service level agreement and operating budget.

Finally, the IAD together with the IAOC is developing a budget based on IASA controlled meeting revenues and IASA administered contracts.

The IAD will integrate existing tools created by the tools team into the IETF web site as well as develop new tools.

In the next few months the IAOC will focus on:

- signing off on the IETF Trust
- completing the initial service agreement with NeuStar
- developing full RFPs for all major service contracts
- publishing regular contract performance and budget reports

That means, the management of operations and expenses is the top priority.

More information, including supporting documents for the IETF Trust, the Statement of Work documents with NeuStar and a list of IAOC members can be found on <http://koi.uoregon.edu/~iaoc/>



**Lucy Lynch**  
IAOC Chair



**Ray Pelletier**  
The IETF's new  
Administrative Director  
(IAD)

***The Structure of the IETF Administrative Support Activity (IASA)***

The IAOC's mission is not to be engaged in the day-to-day administrative work of IASA, but rather to provide appropriate direction, oversight and approval. The IASA structure is designed to ensure accountability and transparency of the IETF administrative and fiscal activities to the IETF community.

The IAD is responsible for negotiating and maintaining contracts or equivalent instruments with outside organisations as well as providing any coordination necessary to make sure the IETF administrative support functions are covered properly.

All functions whether contracted to outside organisations or performed internally within the IASA, must be clearly specified and documented with well-defined deliverables, service level agreements and transparent accounting for the cost of such function.

The IASA is responsible for managing all intellectual property rights (IPR), including but not limited to trademarks, and copyrights that belong to the IETF. The IASA is responsible for undertaking any required actions on behalf of the IETF to obtain, protect and manage the rights that the IETF needs in order to carry out its work.

***Members of the IAOC***

Lucy Lynch, appointed by the IESG (Initial Chair)

Kurtis Lindquist, appointed by the IAB

Steve Crocker, appointed by the ISOC Board of Trustees

Brian Carpenter, IETF Chair (ex officio)

Leslie Daigle, IAB Chair (ex officio)

Lynn St.Amour, ISOC President/CEO (ex officio)

Jonne Soininen, appointed by the NomCom (2 year term)

Ed Juskevicius, appointed by the NomCom (1 year term)

Ray Pelletier, IETF Administrative Director (non-voting)

## News from the IETF Tools Team

By *Mirjam Kühne, ISOC*

The purpose of the IETF Tools Team is to provide IETF feedback and guidance during the development of software tools to support various parts of IETF activities.

Henrik Levkowitz is chair of the tools team and is putting a lot of effort into this activity. See <http://tools.ietf.org/members> for a full list of team members.

The first tool the team has considered is an Internet Draft (ID) submission tool. With this in place, other tools will follow, as listed in the milestones on <http://tools.ietf.org/charter-page>

It is not the team's task to do the actual development - however, the team understands the tool development process, and has the ability to formulate and communicate the IETF's needs with respect to the individual tools. It is also not prohibited for team members to actively develop tool implementations.

An inventory of all IETF tools written by other developers is available on the tools site. All scripts written by the tools team are freely available and can be downloaded.

The WG-status pages <http://tools.ietf.org/wg/> is a one-stop shop for all active or concluded WGs. This tool is a great entry point to other useful tools. It lists the status of each WG along with a pointer to the mailing list archives. One can also find the history of each WG document and the diffs between each version of a document. It produces HTML versions of each document allowing for easy navigation through Internet Drafts. Auto-converted PDF versions are available for those who prefer this format for easy printing. It is also planned to set up a Wiki for each WG for them to use as they wish.

Another useful tool is the agenda tool. As an example, the IETF 64 agenda is available at: <http://tools.ietf.org/agenda/64/>

It shows the meeting agenda with all WG and BoF meetings and pointers to the agendas and document status of each WG as available. It is updated every five minutes based on the submissions sent to the IETF mailing list. It also contains instructions on how to join a jabber room. This allows people to follow discussions during the meetings remotely. The tools team is currently working on a plug-in for iCalendar.

There are a number of new tools in progress, one of the most interesting for the wider IETF community being the 'Build-your-own-notifications' tool. This tool receives notifications of new Internet Drafts, changes in document status, new BoFs and WGs. Anybody can create their own pages based on specific criteria (e.g. 'notify me of all activities in a certain IETF area'). One can choose to be notified by e-mail or to create an html page. This will make it much easier for the community to follow developments in the IETF.

Before this tool can be provided, all notifications have to be converted into XML. Once this is done, it will be easier for people to build their own tools.

See <http://www1.tools.ietf.org/wiki> for more tools in progress.

# Reflections on Architecture

By Pekka Nikander

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

I happen to have an architect's mind. Looking at the network of today, I strongly feel the pain of the current architecture's cracking and squeaking. Consequently, I believe that we - the wider IETF community responsible for Internet technology - need to re-think the architecture. We need to find a way to re-create the core of the Internet in a way that leads to a new era of innovation and intellectual prosperity. The highlight of my IETF64 meeting in Vancouver was that I started to see signs of interest and activity in the broader community to pursue such a goal.

Thinking about the architecture is not easy. The existing, real, out-there Internet architecture is no more the simple one that the founders designed it to be and that many of us wish it still was. We all know that. What we perhaps don't consider very often is the fact that there are huge asset values embedded in various parts of the network. As the slower-than-expected migration to IPv6 has amply demonstrated, some parts of the current Internet are painfully hard to change. This makes any long-term architectural thinking and planning difficult.

Any change requires a reason to overcome the associated hurdle. Consequently, I have found it very instructive to try to think about the network and protocols in terms of assets, incentives, costs, and benefits. Whether we like it or not, every design decision we make embeds value propositions into the system. Basic understanding of micro-economics helps us to understand which assets are harder to change, what kind of incentives and disincentives we need to design into our protocols, and what likely benefits there are that may justify the cost of any change. For example, stateless protocol design [1] and client puzzles [2] have been known in various forms for a number of years. They help in resisting certain kinds of bad traffic by increasing the sender's cost compared to the recipient's cost, thereby providing a direct incentive for their adoption. However, they are still rarely used, presumably because many protocol designers fail to see their benefit, perhaps because they do not really understand the underlying micro-economic mechanisms. More recently, a wider community of computer science researchers and economists have started to pay more attention to these issues, resulting in publications and books, such as "Economics and Information Security" [3].

The Internet is a complex system, and changing complex systems is difficult, often with unanticipated consequences. However, it helps if we are able to understand that there are different types and sources of complexity. Some complexity is inevitable in any large system. This type of complexity is sometimes called emergent or systemic complexity, as it is the result of the large amount of interaction between networked components. It is a hot research area and likely to remain so for some time.

Another form of complexity is what might be called engineering or architectural complexity [4]. It is an (unintended) result of human design decisions, made during the design and evolution of a complex system. The resulting complexity is not so much a result of a very large number of networked components and their interactions but stems more from designed or accidental nonlinear and cyclic interactions between protocols and other architectural elements within a single network element. Kolmogorov complexity [5] appears to be a good theoretical framework for understanding this kind of complexity.

While we can at most work towards understanding emergent complexity in the first place, there is a great deal we can do about architectural complexity. We can try to design simpler protocols, attempt to resist featuritis, and even simplify the architecture when it becomes apparent that a common piece of functionality is being repeatedly implemented by several protocols. A key for working towards a simpler

architecture is attitude. We need to look at our protocols as a whole, attempting to recognise repeated functionality. Once we see that a certain function is being implemented repeatedly in several different protocols, we can try to accomplish the protocol architecture equivalent of software refactoring, where during development of new code some time is also spent on re-writing old code to make it simpler and more general [6].

Given the current state of the Internet architecture, simplification may appear hopeless. Indeed, any attempt at simplification would probably be pointless without some understanding of the goal and the likely end result. We need some kind of an architectural vision and a related transition path; an idea of where we are heading and perhaps how we could get there.

My vision includes peaceful co-existence of both IPv4 and IPv6 for a fairly long time to come. While I would like to see a day when the last IPv4 node is shut down, it is more likely that only future generations will see that happening. In my vision it is possible to use any application I want wherever I am and whatever kind of connection I may have. Indeed, I imagine being able to use multiple wireless networks most of the time, and at least one almost always. I dream of once more being able to communicate with anyone, anywhere on the Internet, independent of the application we want to use, not artificially hindered by NATs or other non-premeditated middle boxes. Finally, in my vision we have baseline security as a built-in feature of the architecture, providing cryptographically strong end-to-end security and sufficient hooks for attaching different kinds of security infrastructures, some based on organisational management and some based on grassroots attempts to model interpersonal human trust relationships with decentralised authorisation systems.

It looks very likely that fulfilling my vision requires adding a new layer, a new "waist", to the architecture [7]. We have to implement mobility, multi-homing, and the envisioned baseline security somewhere in the stack. If we want connectivity to span the partition between IPv4 and IPv6 networks, it looks necessary to build the functionality on the top of the existing hop-by-hop functionality of the IP layer. If we want connectivity to nodes behind IP addressing boundaries, we apparently need a name space that is located on top of the current IP address spaces. If we want decentralised baseline security without administrative overhead, the names in the new name space should be strongly integrated with cryptographic keys, enabling end-to-end security. We certainly could implement this all at any layer above the current IP layer. However, implementing it at transport protocols or anywhere higher seems to imply repeated realisation, leading to increased architectural complexity; something I greatly dislike. Hence, as much as I wish I could see multiple choices, I currently see no real options except the shim approaches that propose to inject the new functionality between the end-to-end and hop-by-hop functions of the IP layer, interfacing it with the functions below (such as routing) and above (including security).

Once we start to consider how to introduce the changes needed to progress towards any vision, it becomes apparent that the two hardest-to-change assets are the existing routing infrastructure and the set of all existing applications. Consequently, if we can introduce incremental changes that do not require changes to the routing infrastructure nor to the legacy applications, they have better a chance to survive than other changes. A new application is always easy - the main hurdle today is lack of network transparency. But network transparency is exactly what we should re-establish, as a ubiquitous utility instead of requiring each new application to do it themselves, each slightly differently. Changing the protocol stack is hard, but changes that are backwards compatible and allow consenting hosts to gain immediate benefits seem feasible. If a change is self-supporting, requiring no new services or pieces of infrastructure, it is more likely to succeed than one that depends on anything that may create new scaling problems.

Using a term that Brian Carpenter recently coined, I propose that we aim at providing new *Architected Network Transparency* (ANT). There seem to be three or

four potential migration paths towards ANT. One possibility is to utilise a Cryptographically Generated Addresses (CGA) [8] based security model in the IPv6 Site Multi-homing by Inter-Mediation (SHIM6) [9] to provide end-to-end security and mobility even when IPv6 traffic is shimmed. Another possibility might be to build on top of Mobile IP by providing a new security model and capability of using multiple interfaces at the same time. A third way could build on existing IPsec, IKEv2, and NAT-T, combining them with IKEv2 Mobility and Multi-homing (MOBIKE) [10] for mobility and multi-homing and with Better-Than-Nothing Security (BTNS) [11] for easier and more scalable deployment. However, independent of which of the available paths happens to become the winning one, my suspicion is that the end result will be cunningly similar to the Host Identity Protocol (HIP) [12]. Hence, I follow with keen eyes the ongoing HIP experiment [13], hoping that we as a community can learn from any snags it encounters.

A pivotal impediment in any path towards the outlined ANT heaven seems to be the ability to include the envisioned baseline security in existing legacy applications without requiring any changes in them. One possible means might be Keyed Hash Identifiers (KHI, pronounced as the Greek letter X) [14], currently subject to heated debate in the int-area and ipv6 mailing lists. Whether KHIs should be considered as an important but transitory stepping stone or as despicable opening of the flood gates to occupy the IPv6 address space with varmints remains to be seen.

The IAB has recently created a new mailing list, *architecture-discuss* [15], for wider discussion of architectural issues, which I hope will develop into a valuable forum over time. I hope to see you there.

- [1] Aura and Nikander, Stateless connections, in *International Conference on Information and Communications Security, ICICS'97*, Beijing, November 1997, pp. 87-97, Lecture Notes in Computer Science 1334, Springer, 1997.
- [2] Aura, Nikander, and Leiwo, DOS-resistant Authentication with Client Puzzles, in *Security Protocols, 8th International Workshop*, Cambridge, UK, April 25-27 2001, LNCS 2467, pp. 12-26, Springer, 2002.
- [3] Lewis, *Economics of Information Security*, Kluwer Academic Publishers, 2004.
- [4] Nikander, *Why architectural complexity is like body fat - food for thought*, <http://www.tml.tkk.fi/~pnr/FAT/>, 2005.
- [5] Li, and Vitányi, *An Introduction to Kolmogorov Complexity and Its Applications*, Springer, 1997.
- [6] Fowler, Beck, Brant, Opdyke, and Roberts, *Refactoring: Improving the Design of Existing code*, Addison-Wesley Professional, 1999.
- [7] Deering, *Watching the Waist of the Protocol Hourglass*, in *Proceedings of 51st IETF meeting*, <http://www.iab.org/documents/docs/hourglass-london-ietf.pdf>, IETF, 2001.
- [8] Aura, *Cryptographically Generated Addresses (CGA)*, RFC 3972, IETF, 2005.
- [9] *Site Multihoming by IPv6 Intermediation*, IETF Working Group, <http://www.ietf.org/html.charters/shim6-charter.html>
- [10] *IKEv2 Mobility and Multihoming*, IETF Working Group, <http://www.ietf.org/html.charters/mobike-charter.html>
- [11] *Better-Than-Nothing Security*, IETF Working Group, <http://www.ietf.org/html.charters/btns-charter.html>
- [12] *Host Identity Protocol*, IETF Working Group, <http://www.ietf.org/html.charters/hip-charter.html>
- [13] *Host Identity Protocol*, IRTF Research Group, <http://www.irtf.org/charter?gtype=rg&group=hip>
- [14] Nikander, Laganier, and Dupont, *A Non-Routable IPv6 Prefix for Keyed Hash Identifiers (KHI)*, Internet Draft (work in progress), 2005.
- [15] *Architecture Discuss mailing list*, <https://www1.ietf.org/mailman/listinfo/architecture-discuss>

## IETF Glossary

<b>6LOWPAN</b>	IPv6 over Low power WPAN WG
<b>ALIEN</b>	Anonymous Identifiers BoF
<b>ARP</b>	Address Resolution Protocol
<b>AUTOCONF</b>	Ad Hoc Network Configuration WG
<b>BCP</b>	Best Current Practice
<b>BGP</b>	Border Gateway Protocol
<b>BoF</b>	Birds of a Feather
<b>CADR</b>	Client Authenticated DNS Request
<b>CAPWAP</b>	Control And Provisioning of Wireless Access Points WG
<b>CCAMP</b>	Common Control and Measurement Plane WG
<b>DHC</b>	Dynamic Host Configuration WG
<b>DHCP</b>	Dynamic Host Configuration Protocol
<b>DKIM</b>	Domain Keys Identified Mail
<b>DNS</b>	Domain Name System
<b>DNSEXT</b>	DNS Extensions WG
<b>DNSOPS</b>	Domain Name System Operations WG
<b>DNSSEC</b>	DNS Security Extensions
<b>DOCSIS</b>	Data Over Cable Service Interface Specification
<b>EAP</b>	Extensible Authentication Protocol (an extension to PPP)
<b>FQDN</b>	Fully Qualified Domain Name
<b>GEOPRIV</b>	Geographic Location/Privacy WG
<b>GMPLS</b>	Generalized Multiprotocol Label Switching
<b>HASH</b>	One-way Hash Function BoF
<b>HD Ratio</b>	Host Density Ratio
<b>HIP</b>	Host Identity Protocol
<b>IAD</b>	IETF Administrative Director
<b>IANA</b>	Internet Assigned Numbers Authority
<b>IAOC</b>	IETF Administrative Oversight Committee
<b>IASA</b>	IETF Administrative Support Activity
<b>ICANN</b>	Internet Corporation for Assigned Names and Numbers
<b>ICMP</b>	Internet Control Message Protocol
<b>ID</b>	Internet Draft
<b>IESG</b>	Internet Engineering Steering Group
<b>IETF</b>	Internet Engineering Task Force
<b>IKEv2</b>	Internet Key Exchange v2
<b>IMAD</b>	IPv4 Multicast Address Architecture BoF
<b>IPR</b>	Intellectual Property Rights
<b>IRTF</b>	Internet Research Task Force
<b>ISOC</b>	Internet Society
<b>ITU</b>	International Telecommunications Union
<b>LRW</b>	Lightweight Reachable Softwires BoF
<b>LSP</b>	Label Switched Path
<b>MAC</b>	Media Access Control
<b>MANET</b>	Mobile Ad-hoc Networks WG
<b>MASS</b>	Message Authentication Signature Service BoF
<b>MIP4</b>	Mobility for IPv4 WG

<b>MIP6</b>	Mobility for IPv6 WG
<b>MIPSHOP</b>	MIPv6 Signaling and Handoff Optimization
<b>MOBIKE</b>	IKEv2 Mobility and Multihoming WG
<b>MOBOPTS</b>	IP Mobility Optimizations Research Group
<b>MONAMI6</b>	Mobile Nodes and Multiple Interfaces in IPv6 WG
<b>MPLS</b>	Multiprotocol Label Switching
<b>NAT</b>	Network Address Translation
<b>NEMO</b>	Network Mobility WG
<b>NETLMM</b>	Network Based Localized Mobility Management WG
<b>NSEC</b>	NextSECure (NSEC) DNS resource record
<b>PANA</b>	Protocol for Carrying Authentication for Network Access
<b>PROTO</b>	Process and Tools Team
<b>RFC</b>	Request for Comments
<b>RG</b>	IRTF Research Group
<b>RIP</b>	Routing Information Protocol
<b>RR</b>	DNS Resource Record
<b>RSVP</b>	Resource Reservation Protocol
<b>RTGWG</b>	Routing Area WG
<b>RUI</b>	Remote User Interface BoF
<b>SDH</b>	Synchronous Digital Hierarchy
<b>SDO</b>	Standards Development Organization
<b>SECMECH</b>	Security Mechanisms BoF
<b>SONET</b>	Synchronous Optical Network
<b>TLD</b>	Top Level Domain
<b>TTL</b>	Time To Live
<b>UN</b>	United Nations
<b>VOIPEER</b>	VoIP Peering and Interconnect BoF
<b>VPN</b>	Virtual Private Network
<b>WG</b>	IETF Working Group
<b>WiMAX</b>	IEEE 802.16 wireless standard
<b>WSIS</b>	World Summit on the Information Society

---

## Recent IESG Document and Protocol Actions

A full listing of recent IESG Document and Protocol Actions can be found at:

<http://ietfjournal.isoc.org/DocProtoActions0102.htm>

---

## Calendar

Spring 2006 - 65th IETF  
March 19-24, 2006  
Host: Nokia  
Location: Dallas, Texas

Spring 2007 - 68th IETF  
March 18-23, 2007  
Host: TBD  
Location: TBD

Summer 2006 - 66th IETF  
July 9-14, 2006  
Host: TBD  
Location: TBD

Summer 2007 - 69th IETF  
July 22-27, 2007  
Host: TBD  
Location: TBD

Autumn 2006 - 67th IETF  
November 5-10, 2006  
Host: TBD  
Location TBD

Autumn 2007 - 70th IETF  
December 2-7, 2007  
Host: TBD  
Location: TBD

## IETF@20

The IETF is 20 years old in 2006. Join the celebrations at the 65th IETF in Dallas, Texas, and look out for a special report in the next issue of the IETF Journal.

### IETF Journal

Winter 2005/2006  
Volume1, Issue 2

Published three times  
per year by:  
Internet Society  
4 rue des Falaises  
CH-1205 Geneva  
Switzerland

*Editor:* Peter Godwin

*Editorial Board:*  
Brian Carpenter  
Leslie Daigle  
Mirjam Kühne  
Peter Godwin

*Contributing Editors:*  
Mirjam Kühne

*Design:*  
Peter Godwin

E-mail:  
[ietfjournal@isoc.org](mailto:ietfjournal@isoc.org)

IETF Journal  
on the Web

*Find us at:*  
[ietfjournal.isoc.org](http://ietfjournal.isoc.org)

### INTERNET SOCIETY

IETF Journal  
4 rue des Falaises  
CH-1205 Geneva  
Switzerland

