ARIN Review
A resource for Internet number resource users

2005
Third Quarter

In This Issue

About Review

Review is produced for the ARIN membership and Internet community. Articles and contributions dealing with Internet number resources are welcome from all sources.

If you have an idea about an article or just a suggestion, please contact webmaster@arin.net.

Double Feature in Tinseltown

Back-to-back meetings of NANOG 35 and ARIN XVI this October in Los Angeles

ARIN and the North American Network Operators Group (NANO are pleased to once again offer back-to-back meetings, v NANOG 35 and ARIN XVI taking place this October in Los Ange California. NANOG 35 will be held from October 23-25, 20 and ARIN XVI will immediately follow, from October 26-28. The meetings will be held at the Hilton Los Angeles/Universal City.

NANOG and ARIN's back-to-back meetings are a great chance for everyone to benefit from the technical and operational expertise of their colleagues, keep up on all the latest technical issues facing the network operator community, and contribute to Internet number resource policy discussions and development.

All meeting information is available on the ARIN website at: **http://www.arin.net/ARIN-XVI/**. A more detailed draft agenda has recently been posted.

See **ARIN XVI**, Page 4

Who's Behind Network Security?

Identity and the Foundations of Secure Origination

By Tom Vest, Research Program Manager, Packet Clearing House

Policing the Protocols

In recent years, growing recognition of the vulnerability of some of the Internet's core protocols has sparked a variety of security initiatives. Prominent among these are two parallel efforts – Secure BGP (sBGP) and Secure Origin BGP (soBGP) – to secure inter-domain routing, and DNSSEC, which promises to raise confidence levels in information propagated by the domain name system.

These initiatives address threat models involving malicious or accidental interference with network routing. With soBGP, routing announcements are cryptographically labeled with the announcement's originating Autonomous System (AS), thereby deterring any third party who might accidentally or intentionally introduce a conflicting route to the same resource. By contrast, sBGP defines security as "the correct operation of BGP routers," and seeks to provide this with hop-by-hop cryptographic authentication of routing announcements. Messages conveyed via sBGP are thus "secured" as a byproduct of their transmission from sender to receiver. DNSSEC involves a similar kind of infrastructure-based cryptographic authentication scheme, albeit one that secures individual DNS responses as originating with an expected, legitimate, cryptographically signed source. While DNSSEC may not provide the level of security for name service that sBGP and soBGP promise for tomorrow's routing infrastructure, DNSSEC's appeal is enhanced by real-world availability; while the BGP enhancements are in the early stages of development and experimental deployment, the

See **Network Security**, Page 6

Upcoming Internet Community Meetings

NANOG 35
October 23 - 25
Los Angeles, California, US

ARIN XVI
October 26 - 28
Los Angeles, California, US

IETF 64
November 6 - 11
Vancouver, BC, Canada

WSIS Phase II
November 16 - 18
Tunis, Tunisia

ICANN
November 30 - December 4
Vancouver, BC, Canada

AfriNIC-3
December 12 - 14
Cairo, Egypt

Updates to this calendar can be found at:

http://www.arin.net/meetings/calendar.html

Internet Community Meeting Reports

ICANN
July 11 - 15
Luxembourg City, Luxembourg

The Internet Corporation for Assigned Names and Numbers (ICANN), held its meeting in Luxembourg City from July 11-15, 2005. Representatives from ICANN discussed the organization's Strategic Plan, Internationalized Domain Names (IDNs), and Internet Governance with respect to the International Telecommunication Union (ITU).

On Sunday, July 10, the NRO and the Government Advisory Committee (GAC) held a joint roundtable on IP Addressing. The roundtable included an overview of how internet routing works, IPv4 & IPv6 address assignment policies and their constraints, IPv6 address distribution mechanisms, and concluded with questions and discussion.

During the meeting, ICANN conducted consultation sessions seeking the views of the community on the July 2006 - June 2009 Strategic Plan. Sessions were run for ICANN's Supporting Organizations, Address Councils, and other constituency groups.

http://www.icann.org/meetings/luxembourg/

IETF 63
July 31 - August 5
Paris, France

The 63rd meeting of the Internet Engineering Task Force (IETF) was held in Paris, France during the first week of August 2005. Attendance increased from the spring meeting to the same level as Summer 2004.

One of the most significant items of interest for the RIR community came during the BGP status update during the Global Routing Operations Working Group (GROW) meeting.[1] Based on analysis of the Route Views data, a projection shows that 2-byte Autonomous System (AS) numbers are expected to be depleted by 2010. A realistic implementation plan estimates that it will take at least four years to make the necessary changes to the infrastructure to use 4-byte AS numbers. With 2006 as the latest deadline for beginning the effort, a sense of urgency led the community to discuss the issues impeding the progress of the Internet draft document draft-ietf-idr-as4bytes-10.txt.

Security in all of its forms was a concern of many subgroups within the IETF. Some of the most frequently exploited application-level vulnerabilities were identified in a presentation to the Applications Open Area Meeting.[2] It concluded by summarizing recommendations for some common sense precautions.

Security of the routing system was discussed in multiple forums. General discussion of ongoing efforts was covered in the Routing Protocol Security Working Group (RPSEC). During GROW, another presentation focused on the operational perspective of BGP security.[3] It raised more specific options for protecting the routing payload through the use of authenticatable attestations. APNIC shared further details about their plans for developing a PKI infrastructure to support the certification of number resources to a meeting of the engineering staff from all of the RIRs. The possibile need for this type of attestation was echoed during the Thursday night plenary presentation on Application Security.[4]

During the Cross Registry Information Service Protocol

Working Group (CRISP), the final changes to the Address Registry (areg) IRIS draft were summarized. The draft received consensus approval of the meeting attendees. The possibility for further revision of the domain registry (dreg) protocol was also brought up. The changes needed are minor. A revised non-WG proposal, first made at IETF 62, received WG scrutiny. The draft would extend the IRIS protocol to cover Routing Registry data. No decision was made about whether to adopt this as a WG item. The authors agree to revise the draft based on extensive problems identified by the members of the WG.

[1] http://www3.ietf.org/proceedings/05aug/slides/grow-5.pdf

[2] http://www3.ietf.org/proceedings/05aug/slides/apparea-4/sld1.htm

[3] http://www3.ietf.org/proceedings/05aug/slides/grow-2.pdf

[4] http://www3.ietf.org/proceedings/05aug/slides/plenaryt-1.pdf

APNIC 20

September 6 - 9
Hanoi, Vietnam

APNIC 20 was held from September 6-9, 2005 in Hanoi, Vietnam. The meeting started with a day that included an IPv6 technical workshop, and tutorials on spam and security. The two-day Open Policy Meeting included an Opening Plenary with a welcome speech by Thuy Nguyen of the local host Vietnam Network Information Center, and keynote presentations by Tom Vest ("Infrastructure, Innovation, and the Digital Divide: Lessons from Internet history") and Geoff Huston ("Internet Evolution and IPv6"). There were also many talks and presentations given during the two days in the various SIG sessions.

The following policy proposals were presented at APNIC 20:

1. prop-005-v005: Internet Assigned Numbers Authority (IANA) policy for allocation of IPv6 blocks to Regional Internet Registries. This was the updated version of the proposed global policy (the timeframe from 36 to 18 months). Consensus was found to move the proposal forward in the policy development process.

2. prop-031-v001: Proposal to amend APNIC IPv6 assignment and utilisation requirement policy. Proposal to: add /56 as default assignment for SOHO end sites; change the HD Ratio to .94; and base utilisation on /56 counts. Consensus was found for moving forward only the part about changing the HD Ratio to .94.

3. prop-029-v002: Proposal for discrete networks and national peering. A proposal to permit large ISPs to manage multiple country accounts under a single APNIC membership using the concept of discrete networks. This proposal was abandoned.

4. prop-030-v001: Deprecation of ip6.int reverse DNS service in APNIC. Consensus was found to implement the proposal and gather statistics.

5. prop-028-v001: Abolishing IPv6 per address fee for NIRs. The proposal to abolish per address fees for NIRs reached consensus to move forward in the policy development process.

The final day was reserved for the APNIC Member Meeting where department updates were given, final policy discussions were held, and reviews of all of the SIGs were presented.

http://www.apnic.net/meetings/20/

WSIS PrepCom-3

September 19 - 30
Geneva, Switzerland

The Preparatory Committee for the Tunis phase of the World Summit on the Information Society (WSIS) held its third session from September 19-30, 2005, at the Palais des Nations in Geneva.

Representatives from 152 governments, 200 nongovernmental organizations and civil society entities, 54 international organizations, 36 business entities, and six UN agencies attended the PrepCom to discuss the future of Internet governance and other issues related to the information society. The NRO was represented throughout the session by staggered participation of the Executive Council.

A focus of the meeting was to discuss the draft text of the Internet Governance chapter of the Operational Part of the Final Document(s) of the Tunis phase. The group agreed on large sections of text, but did not complete its work. The text will be considered again during a resumed session of PrepCom-3, to be held back-to-back with the WSIS summit in Tunis in November 2005.

http://www.wsis.org

ARIN XVI, from Page 1

Activities

"Getting Started with IPv6 " Workshop

NANOG and ARIN are excited to jointly offer "Getting Started with IPv6," a workshop focusing on providing hands-on experience using IPv6 on Sunday, October 23, 2005 from 9:00AM to 4:30PM (PDT) at the Hilton Los Angeles/Universal City. All registered NANOG 35 and ARIN XVI attendees are invited to attend this IPv6 workshop free of charge.

Tutorials and Open Policy Hour

ARIN will hold tutorials and the Open Policy Hour on Tuesday. For anyone new to ARIN, there will be a "Getting to Know ARIN" tutorial on Tuesday afternoon from 1:00 to 1:30 PM. Once NANOG 35 concludes in the late afternoon, ARIN will hold a tutorial on Secure Routing from 5:00 to 5:45 PM, and the Open Policy Hour will take place from 6:00 to 6:45 PM.

ARIN XVI Public Policy and Members Meetings

All registered attendees are invited to attend both the Public Policy and Members Meetings. The Public Policy Meeting will take place Oct. 26 - 27, and the Members Meeting will be held the morning of Oct. 28. Policy discussions at this meeting will be focused on policy proposals recently introduced and those carried over from the previous meeting.

The Members Meeting on Friday is a forum where ARIN Department Directors report on recent and future activities, reports are provided from the Board of Trustees, the Advisory Council, and ARIN's Treasurer. In addition, ARIN will present information about the 2005 elections for open seats on the Board of Trustees and Advisory Council, and candidates for these seats are given a chance to speak. More information on the 2005 election cycle can be found on Page 5.

Registration Services and Billing Help Desks

ARIN XVI attendees may also take advantage of the ARIN Registration Services and Billing Help Desks to meet face-to-face with ARIN staff to discuss specific questions or concerns. In addition, the Registration Services Help Desk will be open at selected times during NANOG 35.

See the ARIN XVI Draft Agenda page for Help Desk hours and how to make an appointment. Again, all meeting information is available at:

http://www.arin.net/ARIN-XVI/

Remote Participation and Webcast

In its continuing effort to supply the community with an open forum, ARIN is offering individuals who cannot attend either the Public Policy or Members Meetings in person the opportunity to participate remotely. Remote participants may post questions and comments to be addressed in normal question and answer periods throughout the agenda. Detailed information about how to register for remote participation, the remote participation AUP, and about the webcast is available at:

http://www.arin.net/ARIN-XVI/webcast.html.

Policy Proposals for Discussion at ARIN XVI

Policy discussions at this meeting will be centered on policy proposals recently introduced to the Public Policy Mailing List (PPML), and those carried over from the previous Public Policy Meeting.

Policy Proposals recently introduced on PPML:

- 2005-4: AfriNIC Recognition Policy
- 2005-5: IPv6 HD ratio
- 2005-6: IPv4 Micro-allocations for Anycast Services
- 2005-7: Rationalize Multi-Homing Definition and Requirement
- 2005-8: Proposal to amend ARIN IPv6 assignment and utilisation requirement

Policy Proposals carried over from the previous Public Policy Meeting:

- 2005-1: Provider Independent IPv6 Assignments for End-sites
- 2005-2: Directory Services Overhaul

A summary of the active policy proposals under discussion can be found at:

http://www.arin.net/policy/proposal_archive.html

The entire Internet community is invited and encouraged to participate in these policy discussions. Your active participation in these discussions is vital to the process and will help to form policies that are beneficial to all.

2005 Election Information

Board of Trustees and Advisory Council

ARIN General Members in Good Standing have the opportunity to help shape the future of ARIN by voting in the 2005 Board of Trustees and Advisory Council elections. Please make sure your organization has a designated member representative (DMR) listed and that your organization is eligible to vote in this year's Board and AC elections. Contact **memsvcs@arin.net** with questions about your membership status.

On May 2, ARIN issued an open call for nominations to fill two Board seats and five AC seats which will become vacant at the end of this year. All new terms are for three years and will begin on January 1, 2006.

The Board seats opening are currently held by David Conrad and Bill Woodcock.

The candidates for the Board of Trustees are:

- Vijay Gill, AOL
- Lee Howard, Stanley Associates
- Doug Humphrey, Joss Heavy Industries
- Bill Woodcock, Packet Clearing House

The Advisory Council seats opening are currently held by: Bill Darte, Andrew Dul, Alec Peterson, John Sweeting, and Suzanne Woolf.

Candidates for the Advisory Council are:

- Dan Alexander, Comcast
- Bill Darte, CAIT - Washington University St. Louis
- James Deleskie, Teleglobe
- Owen DeLong, Blue Water Aquatics
- Andrew Dul, Connexion by Boeing
- Teresa Gurney, America Online, Inc.
- Alec Peterson, Catbird Networks
- Matt Pounsett, Canadian Internet Registration Authority
- Allie Settlemyre, Microsoft Corporation
- John Sweeting, Teleglobe
- Suzanne Woolf, Internet Systems Consortium

Candidate biographies and information about the election process are available at:

http://www.arin.net/elections/

Voting is open to all ARIN General Members in good standing. The online voting booth will open at 12:00 PM ET on Friday, October 28. All votes must be cast and confirmed by 12:00 PM ET on Friday, November 4.

New Online Voting Procedure

ARIN has updated its online Voting Booth, making it easier for DMRs to cast and confirm their votes.

ARIN will send a message containing the Election Headquarters URL to DMRs via e-mail. DMRs will need to register by entering their e-mail account on file with ARIN. The DMR e-mail account must include the DMR's name or initials and the organization domain name. Role accounts are not allowed.

Valid DMRs will then be sent an e-mail with the Voting Booth URL. After entering a password, DMRs will cast and confirm their vote online. For the vote to be counted, the organization must be a member in good standing (have no invoice more than 60 days past the due date) at the time voting opens.

NRO Number Council

The Number Resource Organization Number Council (NRO NC) representatives now fulfill the role of ICANN's ASO Address Council. On May 3, ARIN issued an open call for nominations to fill the vacancy created by the expiration of Lee Howard's term. The appointed representative will serve a three-year term beginning January 1, 2006.

The NRO Number Council candidates are:

- Joe Abley, ISC
- Martin Hannigan, VeriSign
- Tom Vest, Packet Clearing House

This year, the NRO NC seat will be appointed by the Board of Trustees, in accordance with the NRO's Memorandum of Understanding.

Dates of important election milestones can be found at:

http://www.arin.net/elections/elec_calendar.html

Network Security, from Page 1

first DNSSEC-enhanced country-code TLD (.se) is expected to become fully operational before the end of the year.

Loose Ends Remain

With the Internet playing an increasingly central role in many lives and livelihoods, these efforts to secure core Internet transmission processes have inspired a variety of productive partnerships and elicited a measure of support that is noteworthy in the diverse and sometimes fractious technical community. Given the gravity of the risks and the demonstrated willingness of many public institutions and commercial enterprises to work together on protocol and process-oriented remedies, one might expect to see similar cooperation in pursuit of "security of payload" or security from "bad ends," or more simply as the problem of identity.

These terms all refer to features that distinguish actors from each other in a particular context. In this context, the actors are those who originate or retransmit Internet control messages that are protected in transit by the security extensions described above, i.e., DNS providers and particularly Autonomous System operators.

Identity matters for network security for the simple reason that no amount of security in transmission can guarantee that what is so delivered is not itself a threat to the security of the recipient. The development of secure routing and name service protocols was motivated in part by the expectation that network transmission vulnerabilities would become an attractive target for malicious users (a.k.a. "bad guys"). Today, abuse of DNS with larcenous or worse intent is no longer a rare occurrence, and some operators have observed that the incidence of suspiciously similar anomalies in routing behavior is also rising. It is perhaps inevitable that BGP-speaking bad guys will sooner or later pass out of the realm of the mythical and become a genuine, real-world problem for everyone else. Indeed, the recent adoption of AS numbers as a proxy measure for value in some peering negotiations may tend to encourage the commercial misuse of routing protocols. If it's even possible that secure Internet identity could help forestall this eventuality, and/or mitigate the consequences of its arrival, then the pursuit of this goal deserves serious consideration by the Internet community.

Responses to the Identity Challenge

What does it mean to "know the identity" of an Internet subject? Many issues and complexities may differentiate the Internet from other domains of human experience – but this question, its challenges and possible solutions, are not among them.

As elsewhere, an Internet identity is often given or imposed by a recognized authority. This is sometimes called the "correspondence theory" of identity: what a thing "is" is defined by virtue to its relationship to some other super-ordinate reference entity, that is itself defined by a higher authority. I am (name X), because that is my given name. Even in the mundane world, a name alone is rarely sufficient to satisfy a demand to "identify yourself", so it is often accompanied by a string of historically contingent facts and information, all subject to some kind of formal verification today, but also to revision at any time in the future. In the Internet today, this kind of correspondence-rooted identity is conferred upon new network operators by the RIRs at the time of their emergence as autonomous network operators, and vested in the form of a whois entry for the corresponding ASN. Today every new ASN is identified in this manner. However, the continuing existence of over one thousand active ASNs that predate the RIR system (plus many thousands more that are now inactive), coupled with the tensions inherent the RIR role as both coordinator and subject of member-defined policies, complicate the maintenance of the assigned number whois record over time. Even so, a rough estimate based on current Resource Services Agreement (RSA) participation levels suggests that ASN-level whois data for the ARIN region may be close to 70% complete and functionally accurate – arguably close enough that achieving near-perfect completeness and a very high level of accuracy is not an unrealistic goal.

. . . identity imposed via authority is not the only kind in play.

Of course, identity imposed via authority is not the only kind in play. The identity of a given subject might also be regarded as the sum of actions and behaviors as directly experienced (the "extrovert" orientation) or observed and recorded by third parties (the "introvert" orientation) over time – a perspective that might be described as the "coherence theory" of identity. I am (the best fitting current set of mutually non-contradictory self-descriptions of my own characteristics and experiences), tempered more or less by (the cumulative descriptions of me suggested by others over time), depending on who is doing the describing. Off-net, the self-description approach is often associated with solipsism, and the scientifically disreputable ideas of post-structuralism. Even so, certain aspects of this approach may be discerned in more introverted identity construction, in the tendency for trust and recognition to be based on perceived self-similarity between two Internet subjects.

On and off the Internet, coherence-based identities abound. Off-net, most people recognize a "circle of friends" with whom they share bonds of affinity and trust. Many who work in large organizations will over time identify with a network of colleagues with whom they can complete difficult tasks faster, easier, and more efficiently than by identifying and then using more "official channels." On the Internet, many similar functional arrangements have emerged to help offset the perceived limitations or inconveniences of working through the current, correspondence

-rooted identity system. Informal communications systems like the PCH INOC-DBA VoIP network enable trusted operators to communicate with each other directly. Informal self-identification tools like Jared's Famous NOC List make it possible for operators to self-define their own Internet identities, and informal reporting mechanisms like the NSP-SEC mailing list enable members of the trusted collective to keep each other informed about real and potential network security risks. Members of these informal collectives -- constituting perhaps 15-20% of the universe of active autonomous systems operators -- are bound by a diffuse web of mutual recognition and reciprocal trust that in many way functions independently of the Internet's official authority-based identity arrangements.

For some members, participation in these informal systems represents a pragmatic decision driven by concerns about the accuracy and hence utility of official correspondence-based identity systems. Some may be further motivated by fidelity to universally lauded Internet design principles like catnet-style organizational forms and avoidance of single points of failure. However, for some participation may also be rooted in a principled resistance against a future in which Internet management and service delivery patterns and policies more closely resemble those from the legacy PSTN era. On this view, greater dependence on correspondence-rooted identities handed down by a centralized external authority suggests a logic that, taken to its extreme, leads to the nationalization of Internet service management. Some of the most vocal critics of the correspondence approach advocate instead a comprehensive shift to consensus-based systems, wherein Internet identity is completely effaced, leaving behind only a set of loosely coupled "behavioral histories" tied together by any common protocol or traffic artifact (e.g., an IP address, domain name, email, etc.).

. . . the Internet remains an overlay network. . .

Since slippery slope arguments like this are insusceptible to counterevidence, it may be more useful to consider some of the possible weaknesses in pure reputation-based identity systems. First, it is unclear whether such arrangements would be any more robust than correspondence-rooted identity systems in the face of serious security threats posed by highly competent and motivated bad guys. It may be that current patterns of informal trust network membership and usage are substantially orthogonal to national boundaries (the actual answer is unknown), but in a real crisis the pressures to "ratchet down trust" could be substantial. In addition, the scalability of pure trust-based systems is not obvious. If the historical observation requirements of a pure coherence-rooted system causes the growth of a "trusted network core" to lag substantially behind the overall growth of the Internet, this might doom the arrangement to gradual irrelevance for most Internet users. In effect, the trusted core might come to replicate the kind of "donut pattern" that some researchers have used to explain the relative decline of "tier one" Internet backbone providers.

Finally, it should be noted that even in the "pure" coherence-rooted systems envisioned by researchers, some kind of fixed, authority-derived identity tag remains necessary to serve as a key field to link successive behavioral observations together. Without such a key field, no cumulative behavioral history could be assembled, so no reputation could develop; under such circumstances it is unclear how trust could ever evolve.

Identity Indispensable?

The final observation above deserves repeating. In the absence of some commonly recognized criterion around which to organize direct experiences and third party observations, the emergence of a coherence-oriented, behavioral history, or reputation-based Internet identity is extremely problematic. For all of its twenty thousand and counting principal subjects, the Internet remains an overlay network – not only as frequently observed over the legacy telecommunications infrastructure, but also over the vast universe of ad-hoc groups, universities, commercial enterprises, public and nonprofit institutions, criminal gangs, military, intelligence, and other government agencies, and private individuals that populate the off-net world.

To the extent that these conventional actors enjoy the ability to anonymously don the network persona and resources of any one of thousands of currently opaque, unidentified legacy ASNs, and then to move to another, then perhaps later to a new, under-identified ASN, the potential for existing network operators to develop new, coherence-based identity judgments will remain highly subjective, if not arbitrary. The old web of trust may remain just that – and the legacy ASNs may remain opaque indefinitely.

To the extent that new and existing network institutions can continue to operate in the Internet without associated, verifiable, correspondence-based identities, other, self-identifying operators will probably continue to regard the whois record as deeply suspect, and so perhaps pass up an opportunity to use their considerable influence to encourage greater confidence in and commitment to this important resource. Authority and observed behavior, correspondence and coherence – the establishment of secure Internet identities, and so of true end-to-end network security -- may ultimately depend on the ability of operators to recognize these as equally essential and interdependent, rather than opposing alternatives.

Tom Vest is Research Program Manager for Packet Clearing House (PCH), a nonprofit research institution that has pioneered the localization of Internet routing and DNS delivery in developed and developing countries since 1994.

A list of references for this article is available at:
http://www.arin.net/newsletter/2005_tv_ref.html

NRPM version 2005.1 - New Policy Implementations

On June 16, 2005, the ARIN Board of Trustees, based on the recommendations of the Advisory Council and noting that the Internet Resource Policy Evaluation Process had been followed, adopted the following policy proposals:

- 2004-3: Global Addresses for Private Network Inter-Connectivity
- 2004-5: Address Space for Multiple Discrete Networks
- 2004-8: Allocation of IPv6 Address Space by the Internet Assigned Numbers Authority (IANA) Policy to Regional Internet Registries
- 2005-3: Lame Delegations

The following two policy proposals took effect September 7, 2005:

- 2004-3: Global Addresses for Private Network Inter-Connectivity
- 2004-5: Address Space for Multiple Discrete Networks

Policy Proposal 2004-8 has been inserted into Chapter 10 of the ARIN Number Resource Policy Manual (NRPM) as a proposed global policy.

Editorial updates have been made in the NRPM per the recommendation of the Advisory Council and the subsequent adoption by the Board of Trustees at their meeting on August 8, 2005.

Version 2005.1 of the NRPM took effect on September 7, 2005. This version supersedes all previous versions. See Appendix A of the NRPM for information regarding changes to the manual.

The NRPM, and a link to Appendix A, can be found at: **http://www.arin.net/policy/nrpm.html**

ARIN Review

Editor-in-Chief: *Jason Byrne*
Contributors:
Einar Bohlin
Erika Goedrich
Megan Kruse
Cathy Murphy
Leslie Nobile
Guest Article: *Tom Vest*

Board of Trustee Actions

During the third quarter of 2005, the ARIN Board of Trustees met on August 8. The following are highlights of Board actions and discussions at this meeting:

- Adopted the Standing Rules for ARIN Board Meetings
- Approved editorial updates to the ARIN Number Resource Policy Manual (NRPM)
- Discussed proposed liaisons between the NRO and the IETF and between the NRO and ITU-T

Minutes for all Board of Trustees meetings are available on the ARIN website at:

http://www.arin.net/meetings/minutes/bot/

Advisory Council Actions

In this quarter, the AC held teleconferences on August 31, August 18, and July 21.

The AC conducted their initial review of proposed policies and moved the following forward as formal proposals for discussion by the community: 2005-6, 2005-7, 2005-8.

Concerning the policy proposal submission "*IPv6 Direct assignments to end sites*," the AC decided that there was enough similarity between this proposal and Policy Proposal 2005-1 that the AC will work with both authors to merge the two proposals into Policy Proposal 2005-1.

Ron da Silva and Paul Andersen provided a report to the rest of the Advisory Council on a trip to LACNIC's recent meeting.

The Advisory Council also reviewed and approved editorial changes to the Number Resource Policy Manual.

Minutes for all Advisory Council meetings are available on the ARIN website at:

http://www.arin.net/meetings/minutes/ac/

Annual Report Available Online

The ARIN 2004 Annual Report is available online at:

http://www.arin.net/about_us/corp_docs/annual/report2004.pdf