ARIN American Registry for Internet Numbers

Review

A resource for Internet number resource users

2005
First 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.

ARIN XV

ARIN stakeholders and NAv6TF community to hold joint meeting

ARIN and the North American IPv6 Task Force (NAv6TF) will hold a joint meeting April 17-21, 2005. This unique event marries the missions of the sponsoring organizations, facilitating information and educational outreach in the area of IPv6. The meeting will take place in Orlando, Florida.

On Sunday, April 17, ARIN and NAv6TF will hold tutorials and an Open Policy Hour. Monday, April 18 - Wednesday, April 20, includes the ARIN Public Policy Meeting, the NAv6TF Summit, and the ARIN and NAv6TF Members Meetings. Thursday, April 21, will be a full day of the NAv6TF Summit.

All attendees are invited to attend the exciting social events - a Sunday evening foosball tournament and an off-site Monday evening social event.

ARIN 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. These proposals are listed on Page 10, along with their respective policy statements and links to policy information on the website. 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.

If you are unable to attend the meeting, please see our website for information about webcast and remote participation.

Meeting registration and additional information is at: **http://www.arin.net/ARIN-XV/**.

AfriNIC Transitions to a Regional Internet Registry

On February 21, 2005, the African Network Information Center (AfriNIC) began operating as a fully functional Regional Internet Registry serving the continent of Africa. When ICANN meets in Argentina in early April, ARIN and the Number Resource Organization (NRO) expect the ICANN Board of Directors to approve AfriNIC's application for full recognition as the fifth RIR.

AfriNIC
The Internet Numbers Registry for Africa

Transition activities have been underway for more than a year. The NRO has supported several workshops for AfriNIC personnel to provide information and insight into all aspects of registry operations. In June and July 2004, ARIN and the RIPE NCC held member meetings in their respective African service areas to help explain the pending transition and to discuss regional policies. On October 11, 2004, ICANN approved the provisional recognition of AfriNIC.

Continued on Page 4

A quarterly publication of the American Registry for Internet Numbers

Upcoming Internet Community Meetings

ICANN
April 4 - 8
Mar del Plata, Argentina

ARIN XV and NAv6TF Summit
April 17 - 21
Orlando, Florida, US

3rd WGIG Meeting
April 18 - 20
Geneva, Switzerland

AfriNIC II
April 26 - 27
Maputo, Mozambique

RIPE 50
May 2 - 6
Stockholm, Sweden

NANOG 34
May 15 - 17
Seattle, Washington, US

LACNIC VIII
June 27 - 30
Lima, Peru

Updates to this calendar can be found at:

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

Internet Community Meeting Reports

NANOG 33
January 30 - February 1
Las Vegas, NV

ARIN community and staff participated in NANOG 33, held in Las Vegas, Nevada. In addition to its focus on operations, this meeting set goals for improving input into NANOG from the operator community. Several ARIN members expressed their views on a series of topics including NANOG agenda creation and NANOG mailing list management.

Operators presented tutorials on network architecture and troubleshooting. The general sessions included a solicitation for operators to expand their review of and input to the Routing Protocol Security Requirements group on BGP security. The general session also assembled panels to discuss IP Fast-Reroute, network-based layer 2/3 VPN deployments, and new developments at several Internet Exchanges in the ARIN region.

http://www.nanog.org/mtg-0501/agenda.html

ISOC - NDSS '05
February 3 - 4
San Diego, CA

The focus of the Network and Distributed System Security (NDSS) Symposium was Wireless and Mobile Security. For the first time, the NDSS Symposium held a workshop preceding the conference with a variety of presenters and a panel identifying the vulnerabilities of mobility and methods on enhancing security. Previous symposiums included a day of security-focused tutorials. Since 1993, the NDSS Symposium has been held with the goal of fostering information exchange between hardware and software developers of network and distributed system security services to advance the state of available security technology. Authors of sixteen submitted papers, from universities and research centers throughout the world, were selected to present their research. NDSS'05 sessions included papers and presentations on Cryptography in Network Security, Denial of Service Attacks, Peer-to-Peer Approaches, Internet Defense, Intrusion Detection, and Platform Security.

There were two invited speakers during the event. The first was Amit Yoran, appointed by President Bush as the Administration's official in coordinating the nation's activities in cybersecurity. The second invited speaker was Stefan Savage, from the Computer Science Department at UCSD, who discussed Epidemiology and Defenses.

With another successful symposium completed, the focus for NDSS'06 will be on malware.

http://www.isoc.org/isoc/conferences/ndss/05/index.shtml

GSMNA Quarterly Meeting
February 7 - 11
Clearwater, FL

The GSM North America (GSMNA) meeting was held February 7 - 11 in Clearwater, Florida. GSMNA is the North American interest group of the GSM Association, and its mission is to meet, identify, and resolve issues related to the successful establishment and operation of the "GSM Family of Standards" in North America.

ARIN staff attended this quarterly meeting and participated in discussions held during the services and numbering working group sessions. There was some discussion about current mobile operator use of IPv4 address space. The subject of IPv6 was featured on the agenda during the services working group. Mobile operators continue to look to IPv6 for future service deployments.

ESCC/Internet2 Joint Techs Workshop

February 13 - 16
Salt Lake City, UT

The Winter 2005 ESCC/Internet2 Joint Techs Workshop was held February 13-16 in Salt Lake City, Utah. The meeting was hosted by the University of Utah. The workshop offered a combination of tutorials, plenary presentations, in-depth subject discussions, and BoFs.

ARIN staff attended the workshop and presented a registry status report during one of the plenary sessions. The report focused on the status of the Internet number resource pool, current policy, and policies that have been proposed for discussion. ARIN's presentation also stressed the importance of community participation in the Internet Resource Policy Evaluation Process. Meeting attendees were encouraged to participate and were invited to join the Public Policy Mailing List and attend ARIN Public Policy meetings.

http://jointtechs.ornl.gov/SLC2005.html

APNIC 19 / APRICOT 2005

February 16 - 25
Kyoto, Japan

The 19th APNIC Open Policy Meeting (APNIC 19) was held in conjunction with Apricot 2005 from February 18 - 25, 2005 in Kyoto, Japan.

Tutorials and discussion groups took place on Monday and Tuesday and covered topics including APNIC's Internet policy development process, spam prevention, Internet governance, and security. A BoF session held on Thursday evening focused on CRISP (Cross Registry Information Services Protocol) and EPP (Extensible Provisioning Protocol).

The remainder of the week was devoted to the IPv6, Routing, IX, Policy, DNS, and NIR SIGs, as well as the APNIC Member meeting. The member meeting included presentations by all of the visiting RIRs, and an update on ICANN/NRO/WSIS. APNIC held elections during the member meeting for 4 open positions on APNIC's Executive Council. The winners were: Hualin Qian, Yan Ma, Kuo Wei Wu, and Moo-Ho Billy Cheon.

http://www.apnic.net/meetings/19/

62nd IETF

March 6 - 11
Minneapolis, MN

IETF 62 took place in Minneapolis with the fewest number of attendees since March 1996. Despite the low turnout, working groups seemed to make progress on a number of fronts.

During the Internet Engineering and Planning Group (IEPG) that preceded IETF 62, Larry Blunk of Merit gave a presentation on BGP::Inspect, a new tool for providing easy access to raw Routeview data and for analyzing and producing statistics.

Internationalized Domain Names (IDN) was the primary topic of discussion in the Applications Open Area Meeting. Recent homograph spoofing attacks have raised concerns about the inconsistent application by IDN implementers of user notification mechanisms. Specific proposals were made; however, there did not appear to be consensus on a solution.

During the IPv6 Working Group, there was a lively discussion about changes to the DNS section of the unique local unicast address proposal. New language was added to make clear that reverse DNS for local addresses should only resolve locally. Thomas Narten relayed information on the activities being discussed by the IAB-IPv6 Adhoc Committee.

One issue discussed was that the RIRs are receiving requests for larger amounts of IPv6 address space than IANA is currently allocating. He summarized the regional discussions about RIRs receiving larger allocations from IANA. In addition, Geoff Huston presented an individual draft to deprecate ip6.int. The draft proposes the phase-out of ip6.int for use in IPv6 DNS reverse mapping on June 1, 2005. Some attendees asked if the RIRs could provide statistics about the number of queries to their ip6.int zones.

For the Routing Policy Security Working Group, the absence of a key editor hindered the group's work on interdomain routing. The chair, Russ White, reported that the group made progress on documents related to generic routing threats and attack trees.

An interesting new BOF session was held on the final day. The Site Multihoming by IPv6 InterMediation (shim6) group appears on the fast tract to recognition as a working group. It is a follow-on to the multi6 WG, which was investigating solutions to site multihoming in IPv6. The shim6 group will work on architecture and implementation issues for the concept of identifier and locator information between the transport and internet layers.

http://www.ietf.org/meetings/past.meetings.html

Continued from Page 1

With NRO support, the three RIRs previously serving the AfriNIC region (APNIC, ARIN, and the RIPE NCC) transferred responsibility for registry services to AfriNIC on February 21, 2005. Currently, Internet number resource requests from the AfriNIC region are being submitted directly to AfriNIC using AfriNIC templates. Database registrations with postal addresses inside the emerging AfriNIC region are now being documented in the AfriNIC WHOIS database. APNIC, ARIN, and the RIPE NCC have continued to provide assistance and act as the final approving authorities, pending AfriNIC's formal recognition.

AfriNIC will serve a region continental in scope. Incorporated in Mauritius, the not-for-profit membership organization has distributed its operations among three countries: technical operations in South Africa; backup and disaster recovery in Egypt; and training coordination in Ghana.

For further information, please visit the AfriNIC website at:

http://www.afrinic.net.

DBWG Mailing List Closed

On December 30, 2004, ARIN closed the Database Implementation Working Group mailing list (**dbwg@arin.net**) and disbanded the working group.

This change was prompted by database-related discussions, especially those involved with policy changes, increasingly taking place on the Public Policy Mailing List (**ppml@arin.net**). With the closing of the DBWG list, the Public Policy Mailing List (PPML) will used as the list for all policy and database-related discussions.

Database-related topics will continue to be discussed during the general session of the ARIN Public Policy Meetings. The archives of the Database Implementation Working Group mailing list will be preserved for historical purposes. The mailing list archive, as well as all other mailing list information, is available at:

http://www.arin.net/mailing_lists/

ARIN Board of Trustees Report

The ARIN Board of Trustees met on January 5, 2005. The following are highlights of Board actions and discussions in the past quarter:

- Elected officers for this year. John Curran was selected as Chairman of the Board; Scott Bradner was selected as Secretary, and David Conrad was selected as Treasurer.

The Board met again in March 2005, but minutes of that meeting were not available at the time of publication.

ARIN Advisory Council Report

The ARIN Advisory Council met on January 27, 2005. The following are highlighted actions and discussions from the past quarter:

- Elected Ron da Silva as Chair of the Advisory Council. Ron appointed Alec Peterson as Vice-Chair.
- Recommended that the ARIN Board of Trustees adopt Policy Proposal 2004-5 "Address Space for Multiple Discrete Networks."
- Accepted the following new policy proposals:
    - Policy Proposal 2005-1: Provider Independent IPv6 Assignments for End-sites
    - Policy Proposal 2005-2: Directory Services Overhaul
    - Policy Proposal 2005-3: Lame Delegations
- Rejected the submitted policy template titled "Adding an HD ratio choice for new IPv4 allocations" as a formal proposal. After the author requested a petition under the processes outlined in the Internet Policy Evaluation Process (IRPEP) and insufficient support was found, this was considered closed.

The Advisory Council also met in March, but minutes for that meeting were not available at the time of publication.

More Information

Minutes of the Board of Trustees meetings are available at: **http://www.arin.net/meetings/minutes/bot/**

Advisory Council meeting minutes are available at: **http://www.arin.net/meetings/minutes/ac/**

IPv6 Deployment State 2005

By Jim Bound

Chief Technology Officer, IPv6 Forum

IPv6 deployment in 2005 consists predominantly of network pilot programs, though some IPv6 production services are now available and emerging on the public Internet. IPv6 products exist in the market today for deployment, but the required management, applications, middleware, or security infrastructure required for most production networks is not available. Plans for transition and operational deployment are beginning to emerge, and the business case has become more obvious within specific market sectors, driven by the new technology advantages of IPv6. Different geographies are preparing for IPv6 at different rates, with different public commitments. This paper can only reference that which is public knowledge and shared with the author for public consumption. In addition this paper will present models of current deployment, and where those models will assist the pervasive market adoption of IPv6 productions networks. The paper will discuss a set of models from the aggregates of the current deployments in process world wide for IPv6 as learned from within the sphere of work globally, from within the IPv6 Forum and its sub-chapter task forces. See http://www.ipv6forum.org for more information on the IPv6 Forum.

Initial network pilot deployments of IPv6 were chaotic, testing the underlying protocol capabilities of IPv6, but a focus is emerging along with several different views of how to deploy IPv6. The current focus is network infrastructure deployment, driven by provider, enterprise, consumer, multimedia, and mobility requirements for next generation networks. Multimedia is the primary market driver; users want to be mobile when using their multimedia, and the requirement causes new network infrastructure components within Provider, Enterprise, and Consumer Networks (PECN). The network pilots in 2005 will assist preparation for the network infrastructure deployment for PECN, and define a set of deployment and transition models that can be used by industry and government.

This article will present the current deployment models and views, and discuss how they are assisting production deployment of IPv6. To support a successful IPv6 deployment, the network infrastructure, applications, middleware, security, and management for the PECN markets and users must first be implemented. The planning and operational analysis to deploy IPv6 pervasively within a network requires planning and testing that is still to be done with IPv6. However, it is not necessary to have all of this done before network infrastructure deployment, and the current IPv6 deployment demonstrates that axiom.

IPv6 deployment also faces some technological and business challenges in order to implement models depicted in this paper, based on assumptions used for today's operational networks. The market benefits from IPv6 assuming an end-to-end model, but this is not the model of most networks today, thus a technology transformation for the new model is required, in addition to a transition to IPv6. The business strategy to determine the costs and benefits of IPv6 deployment models is a process that is now in progress for the PECN target markets.

1. Deployment Models and Views

The PECN market has a common fulcrum required to implement a successful deployment of IPv6, and that is the provider. The enterprise and consumer deployments will require interoperation with a provider and each of them can also be a provider to their environment. This is not obvious when preparing for IPv6 deployment, and why many of the requirements and functions for IPv6 deployment are common across the PECN. A provider provides prefixes to an enterprise and the enterprise provides prefixes to its Intranet, or the consumer to their home network devices. IPv6 address assignment is similar across the PECN. This is also true of the deployment models being tested within network pilots and prototype implementations.

Network pilots are testing several deployment models, these are: IPv6 support within the Internet routing core; IPv6 support at the provider and customer edge; and IPv6 support on client networks. Then within this model, both sparse and wide-use views exist for IPv6 Intranet nodal and sub-networks deployment.

The Internet or provider core is most difficult to test when it comes to a transition to IPv6. The Internet core initially will either tunnel packets across the core, encapsulating IPv6 within IPv4, or use the Mult-Protocol Label Switching (MPLS) protocol to move IPv6 packets across the Internet core transparent to the IPv4 infrastructure. Network pilots exist that can test moving IPv6 packets over an Internet core and those network pilots are beginning to connect with each other across multiple geographic areas, which is good for testing an Internet core paradigm. To see a list of network pilots' world wide please visit the IPv6 Forum website at www.ipv6forum.org, which also references the network pilots in each geographic area which are subchapters of the IPv6 Forum.

The provider and customer edge of network pilots currently are testing native IPv6 and IPv6-in-IPv4 tunnel packets to the edge of an Internet core. If not native IPv6 to the Internet core, then various IPv6 transition mechanisms are being used to move IPv6 through an IPv4 infrastructure using a dual-stack method for IPv6 deployment. What the dual-stack method states is that the network and nodes transitioning to IPv6 are capable of supporting both IPv4 and IPv6. This affords the PECN markets the ability to test and verify a deployment model that fits their business requirement to support a sparse or wide-use view for the IPv6 deployment model. The provider edge can also use IPv6 with MPLS at the edge to move IPv6 packets across an Internet core supporting MPLS, whether that core supports IPv6 or IPv4, and is being tested in several network pilots.

The nodal and sub-networks implementations within an Intranet or PECN network pilot currently deploy assuming a dual-stack environment for either sparse or wide-use views for the IPv6 deployment model. The sparse view of deployment is that only nodes or networks that require IPv6 will be upgraded to use IPv6 within the PECN markets. The wide-use view of deployment is that IPv6 routing will be dominant (preferred over IPv4) on the Intranets backbone and the sub-networks.

2. Network Infrastructure Deployment

Current deployment is verifying the network infrastructure to support the installation of IPv6 networks within the PECN markets. Network infrastructure includes the hardware, software, and infrastructure applications for an IPv6 network to begin data communications and support the Internet Protocol Suite implementation on a network and across an Internet core network for end-to-end communications.

Deployment uses products from participating IT vendors representing multiple geographies, and has demonstrated that network infrastructure can provide IPv6 connectivity and interoperability across multiple implementations. The routing implementation for the IPv6 network infrastructure has been verified. The core network infrastructure applications have been used and tested widely such as node-to-node communications for autoconfiguration, configuration of network parameters for the network and nodes, file transfer, electronic messaging, web access and services. The application program interfaces for IPv6 have been verified and tested so application providers can perform the necessary porting of those applications to support IPv6.

Transition mechanisms have been implemented and tested on currently deployed networks and demonstrate the ability to support a matrix of combinations of IPv6 and IPv4 interoperation. Sparse and wide-use views have been implemented on several network pilots supporting native IPv6 peering networks such as Moonv6 www.moonv6.org and 6net www.6net.org. The deployment has verified that PECN users will have a set of options for transition depending on their business and technology view to deploy IPv6 and no single transition mechanism will support all use cases required for transition.

The IPv6 network infrastructure deployment thus far supports the following assertions for PECN markets:

- IPv6-capable dual-stack products exist on the market and can be purchased.
- IPv6 link or subnet communications between nodes can be supported today.
- IPv6 links and subnets can communicate over an Internet core network.
- IPv6 core-applications infrastructure can be supported over an IPv6 network.
- IPv6 transition mechanisms exist to support the interoperation of IPv4 and IPv6 on a network.

Current network pilots have begun to deploy mobility using IPv6 and have started to verify the advantages of IPv6 for Mobile Ad Hoc Networks and Seamless Mobility.

The IPv6 network infrastructure deployed above provides a base for wider IPv6 deployment to support the development of next generation networks within the PECN markets.

3. Applications, Middleware, and Management for IPv6 Deployment

The applications and middleware being used for current deployment are usually freeware software and have permitted the testing of multimedia and web services, which have clearly demonstrated applications, that can run and perform well over an IPv6 network. But the production applications for streaming media, web proxy caches, security applications infrastructure-like intrusion detection and prevention, or public key infrastructure, database, manufacturing applications, enterprise resource applications, and many others simply have not been ported to IPv6 by 2005. This is a significant road block to the deployment of IPv6 and it is critical for 2006-2007 that applications be available for PECN markets to begin production deployment adoption at that time.

Another functional requirement for IPv6 that has had some minimal testing with current deployment is the network management of IPv6 and the interoperation of IPv4 and IPv6 transition requirements. Network views for IPv6 using SNMP have been done, but not integrated with IPv4, and that will be a requirement for production deployment on most networks. The range of management software for IPv4 networks must be ported to support IPv6.

4. Security Deployment and Business Challenge for IPv6

Today many users who access networks enter the network within a security model where authentication is based on a firewall or the use of the authentication, authorization, and accounting (AAA) protocol suite implementation. Many users are behind Network Address Translation (NAT) routers that perform translation of the Internet Protocol (IP) header source addresses and keep the state of those addresses for communications with nodes and applications remote from their Intranet network. In addition, network access for remote users is often accomplished with Virtual Private Network (VPN) tunnels, where the security is enforced at the edge of the network. Generally speaking, the security model of many users is based on a model where security is at the edge of the network as depicted in Figure 1 below.

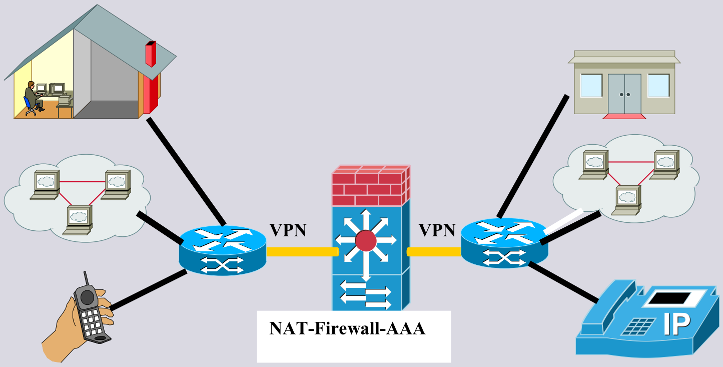


Figure 1

Often, users today connect to the network trusting a third party, usually with NAT on the edge of their network. Emerging technology like the IPsec protocol for end-to-end and peer-to-peer applications with encryption cannot be achieved because the IP address is used as a key for secure communications or the IP address is required to be globally routable on an Internet network. The current model prohibits the end-to-end trust model between two nodes, users, or applications whether stationary on a network or mobile. In addition, NAT prevents many applications from operating in a peer-to-peer manner once they must operate external from an Intranet and across an Internet network and prevents seamless mobility across Internet networks. IPv6 will restore the use of applications using both models, but that technological evolution will have disruptive ramifications to the security model that the Internet currently assumes operationally for deployment.

A new model emerging with IPv6 can support the current and a new end-to-end security model, but how that is architected, managed, deployed, and implemented operationally is a question to be discussed. One view is presented in Figure 2

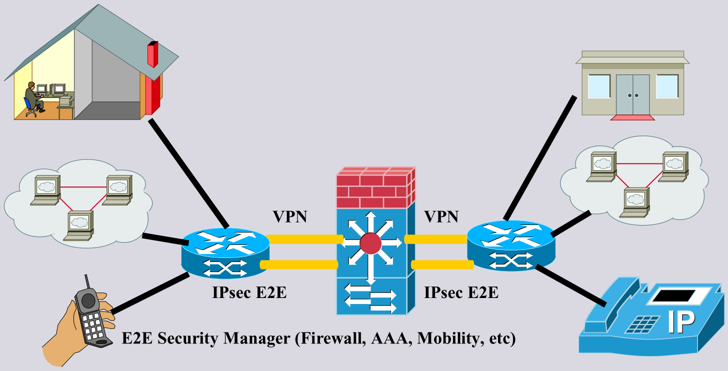


Figure 2

The updated model in Figure 2 permits the current model, but removes NAT to support the evolution of peer-to-peer applications in addition to end-to-end security. The VPN is still available, but the Security Manager permits an end-to-end pass-through trust model for security protocols like IPsec. The current firewall model becomes an ambient security management domain for the network edge, permitting multiple security models. The Security Manager also will support network Intrusion Detection (IDS), and if there is a breach on the network, can shut down the end-to-end communications, and force all communications through the firewall perimeter as an Intranet operation for Internet communications. The security view now takes on a network-wide view not a single point of entry view, which begins to support an ambient and a network-centric view for network security.

This end-to-end model can also support the emerging use of wireless networks with seamless mobility as depicted in Figure 3.

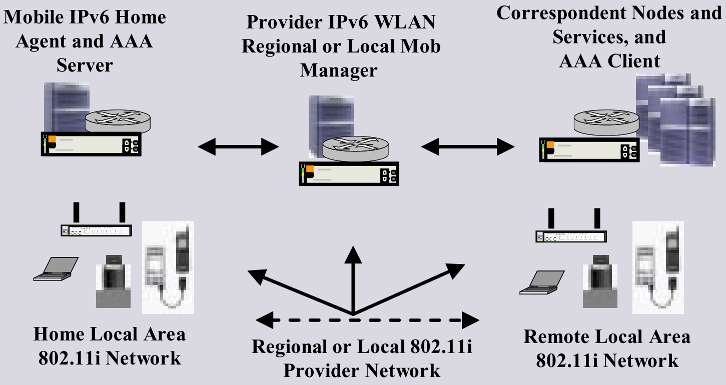

Mobile IPv6 Home Agent and AAA Server
Provider IPv6 WLAN Regional or Local Mob Manager
Correspondent Nodes and Services, and AAA Client
Home Local Area 802.11i Network
Regional or Local 802.11i Provider Network
Remote Local Area 802.11i Network

Figure 3

In Figure 3 the benefits of the Security Manager can be used with AAA methods to ensure secure access to wireless networks in addition to the encryption supported by IEEE 802.11i, which supports the encryption of Layer 2 packet access to the wireless networks. The E2E Security Manager with 802.11i will support seamless secure mobility in conjunction with the Mobile IPv6 extensions to the IPv6 architecture for deployment. The emerging IEEE 802.11n work to provide higher throughput will further reinforce 802.11i wireless access security and provide enhanced performance to this emerging security method.

The integral technology to move networks to an end-to-end and peer-to-peer secure model has been defined, but the deployment of this model will be an extremely disruptive technology in the market. The evolution will impact current network operational methods and business practices across an Internet network. An example of the technical challenges is that current firewalls, filters, and IDS assume knowledge below the IP header within the transport data payload, which will not be available to implementations when the payload is encrypted, for example by IPsec or 802.11i entering the wireless network. Only the IP header will be exposed to the edge devices on an end-to-end supported network. From a business practice perspective today, deployment and operational models for Internet networks are usually based on encryption from the edge network node view.

An end-to-end security model will be disruptive, but also provides a required new security model that is superior and more efficient for peer-to-peer communications for networks that want to support an end-to-end trust model as an operational requirement. The end-to-end security model also has performance and management advantages operationally, once the infrastructure is created to support an ambient secure model for peer-to-peer applications, which will be driven by the evolution of a seamless mobile communications for applications and the rise of a mobile society for businesses and people in general. This new model can also be an economic stimulus for new business, early adopters, and suppliers who provide products and services for the transition to an end-to-end security model, and these early adopters will be the ones potentially who will gain the most profit from this disruptive technology event.

Additionally, IPv6 provides many benefits to next generation networks and mobile users because of its ability to perform stateless node discovery and network operations. However, on a wireless network the nodes and network infrastructure supporting that stateless environment bring new security concerns that must be addressed for network operations.

Current deployment has begun to test IPsec end-to-end, and the above security model is in its design stages for deployment in several network pilots. The security software infrastructure for IPv4 must be ported to IPv6 for the pervasive deployment of IPv6 on production networks.

Acknowledgements

The author would like to acknowledge the information shared and thank the IPv6 Forum regional IPv6 Task Forces and members world-wide, and the enterprises, vendors, government personnel, and individuals that provided supporting data for the current deployment depicted in this paper.

About the Author

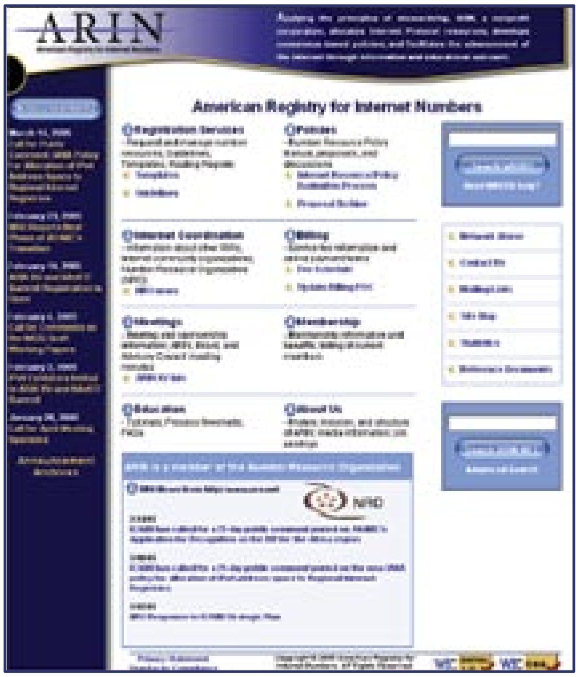
Jim Bound is the IPv6 Forum Chief Technology Officer, **www.ipv6forum.com**; Chair of the North American IPv6 Task Force, **www.nav6tf.org**; Hewlett-Packard Fellow; and is an active contributor within the Internet Engineering Task Force (IETF) standards body. He can be reached at **Jim.Bound@hp.com**.

New ARIN Website Revealed!

Three years after the last redesign of the website, ARIN will release the latest version of its website in early April.

While the overall design of the pages will be familiar to those who have visited the site before, there have been both subtle and major changes. To assist you in using the site and finding the information you need, here are some highlights of what's in store.

New and Reorganized Content



Many of the URLs you may have bookmarked for the ARIN site will not change, but both because of additional content and reorganization of existing pages, we have installed many redirects and you should update your bookmarks accordingly.

One of the biggest changes is the addition of a "Billing" section. Most of the content under this section already existed, but was located deep within other sections. The new section now includes a reorganized Fee Schedule page and all ARIN billing forms.

Another change is the expansion and repurposing of the ARIN Registration Services Guidelines. There are now ten documents that provide targeted step-by-step guidance and instruction on every aspect of Internet number resource request and management at ARIN. The goal of these pages is to make the "Registration Services" section easier to use through process-based documentation. The interactive Registration Process Flowcharts are still available on complement these revised guidelines.

Other changes include the promotion of our training and educational material to be a top-level navigation item in an "Education" section; a refocusing of the old "Library" section to be the new "Reference" section; an enhanced display of search results for our site's search engine, an enhanced and expanded "About Us" section, and what we believe is a more usable and uniform format for policy proposal pages.

Compliance and Accessibility

An important goal in this redesign was to create a site that met accepted W3C standards, including XHTML and CSS. Most of the site can be easily validated against these standards, though some historical archival and scripted content still has issues. However, we have tried to make sure the pages the community uses on a normal basis meet the standards. One benefit of this is that the pages "degrade gracefully" under most older and text-only browsers.

Another goal was accessibility. Through the use of Cascading Style Sheets (CSS), the new design completely separates the content of the page from how it is displayed. This will allow greater accessibility for a broader range of users. In addition, we have endeavored to use semantic markup, so we only use tables to display tabular data, and not for the layout of content, ensuring that the content of pages is more easily accessed by screen readers and other alternative browsing methods.

Another advantage of this approach is the flexibility provided users in viewing the site. Depending on the capabilities of your browser, you can choose to use the style sheet we provide, use one of your own making, or use no style sheets at all and still view all the information on the page in a readable format. Further down the road, we hope to create alternate style sheets for those browsers that support this feature.

The use of robust and compliant CSS also allowed us to create separate style sheets for printing and handheld devices. There is no need for "printer-friendly" or "PDA-friendly" links. Pages will print out with all the content formatting, but none of the website navigation, making it easier than ever to print out and share ARIN documentation. For handheld devices that use browsers with support for the "media='handheld'" meta tags, content will appear automatically resized and reformatted for your display.

The ARIN website is a core part of our service to the community, and we are very interested in your feedback on the new design. Please send any comments, suggestions, or questions to webmaster@arin.net.

Active Policy Proposals for Discussion at ARIN XV

2004-3: *Global Addresses for Private Network Inter-Connectivity*

Policy Statement: "*End-users not currently connected to an ISP and/or not planning to be connected to the Internet are encouraged to use private IP address numbers reserved for non-connected networks (see RFC 1918). When private, non-connected networks require interconnectivity and the private IP address numbers are ineffective, globally unique addresses may be requested and used to provide this interconnectivity.*

This text supersedes section 4.3.5 Non-connected Networks."

2004-8: *Allocation of IPv6 Address Space by the Internet Assigned Numbers Authority (IANA) Policy to Regional Internet Registries*

Policy Statement: *"This document describes the policy governing the allocation of IPv6 address space from the IANA to the Regional Internet Registries (RIRs). This document does not stipulate performance requirements in the provision of services by IANA to an RIR in accordance with the policy. Such requirements should be specified by appropriate agreements among the RIRs and ICANN.*

1. Allocation principles

** The minimum and initial IPv6 allocation from IANA to an RIR in a /12;*

** The IANA will allocate sufficient IPv6 address space to each RIR to support its registration needs for at least a 18 month period;*

** The IANA will allow each RIR to apply its own respective chosen allocation and reservation strategies in order to ensure the efficiency and efficacy of its work.*

2. Initial allocations

On inception of this policy, each current RIR shall be allocated a new /12 by the IANA. Also, a new RIR shall, on recognition by ICANN, be allocated a new /12 by the IANA.

3. Additional allocations

3.1 Eligibility for additional allocations

A RIR is eligible to receive additional IPv6 address space from the IANA when it has utilized (allocated or reserved) more than 50% of its total IPv6 address space holdings.

3.2 Size of additional allocations

Each additional allocation to an RIR will be a number (one or more) of /12 blocks, sufficient to ensure that the RIR holds at least 18 months' supply of IPv6 address space.

4. Announcement of IANA allocations to the RIRs

When address space is allocated to a RIR, the IANA will send a detailed announcement to the receiving RIR. The IANA will also make announcements to all other RIRs, informing them of the recent allocation. The RIRs will coordinate announcements to their respective membership lists and any other lists they deem necessary.

The IANA will make appropriate modifications to the "Internet Protocol V6 Address Space" page of the IANA website and may make announcements to its own appropriate announcement lists. The IANA announcements will be limited to which address ranges, the time of allocation and to which Registry they have been allocated."

2005-1: *Provider Independent IPv6 Assignments for End-sites*

Policy Statement: "To be added to NRPM Section 6, IPv6, a new sub-section:

6.11 Assignments to End-sites with Autonomous System Numbers

Any end-site which meets the current criteria for assignment of an autonomous system number (ASN) shall also qualify for one IPv6 prefix assignment of the minimum size justified under the ARIN guidelines for assignment by an LIR. If the organization grows to require more space, it will not be entitled to an additional block, but rather may obtain a new, replacement block of sufficient size to meet its needs in exchange for making the commitment to return its existing block within 24 months, so that it may be reassigned."

2005-2: *Directory Services Overhaul*

Policy Statement: "Replace all of section three with the following rewrite.

3. Directory Services

3.1 ARIN Directory Services Databases

The ARIN Public Information Database (APID) is a collection of information created and collected by ARIN during the due course of business which the ARIN membership has deemed public information and decided to publish.

The ARIN Confidential Information Database (ACID) is a collection of information created and collected by ARIN during the due course of business which the ARIN membership has deemed is confidential information that should be kept under a strict privacy policy.

3.2 Directory Information Made Public

ARIN shall publish verified contact information and the resource(s) allocated (including identification for that allocation, like date of allocation or other information identified by ARIN) in the APID in the following cases:

- All resources delegated by ARIN.
- If allowed by the parent delegation, and requested by the contact listed with the parent, a subdelegation of a resource.

ARIN shall insure all contact information in the APID is verified from time to time and is correct to the best of ARIN's ability. ARIN staff shall maintain verification criteria and post it on the ARIN web site.

3.2.1 Non-Responsive Contacts

If ARIN is unable to verify contact information via the normal verification procedure ARIN shall attempt to notify the parent of the resource to have the information updated. If there is no parent, or if the data is not corrected in a reasonable amount of time the resource shall be SUSPENDED.

Once the resource is suspended ARIN shall make one more request of all contacts listed with the resource and the parent resource (if available), and if no response is received in a reasonable amount of time the resource shall be reclaimed.

Third parties may report the inability to make contact with a party via information in the APID. In this case ARIN shall attempt the contact verification procedure for that contact immediately. If a response is received, ARIN should document that a problem occurred, and the response from the resource holder. Offenders who fail to respond to third parties more than 4 times per month for three months may have their resources reclaimed at the discretion of ARIN staff.

If a third party submits reports of the inability to make contact that are subsequently disproven, ARIN may choose to ignore reports from specific companies, people, e-mail addresses, or any other classification means as appropriate.

The ARIN staff shall publish the time thresholds and procedural details to implement this policy on the ARIN web site.

If a resource is reclaimed under no circumstances shall the holder of that resource be entitled to a refund of any fees.

3.3 Data Distribution

3.3.1 Methods of Access

ARIN shall publish the APID in the following methods using industry standard practices:

- Via the WHOIS protocol.
- Via a query form accessible via the HTTP protocol.
- Via FTP to users who complete the bulk data form.
- Via CDROM to users who complete the bulk data form.
- Via the RWHOIS protocol.

3.3.1.1 Outside Sources

ARIN may refer a query to a outside source (for instance via RWHOIS or HTTP redirect). Outside sources must:

1. Have an AUP deemed compatible with the ARIN AUP by ARIN staff.
2. Meet the requirements in section 3.3.3.
3. Support the applications in section 3.3.1.
4. Prohibit the applications in section 3.3.2.

3.3.2 Acceptable Usage Policy

All data provided shall be subject to an AUP. The AUP shall be written by ARIN staff and legal and posted on the ARIN website. ARIN may require a signed copy of the AUP before providing bulk data.

3.3.3 Requirements for Internet Accessible Services

For any method of access which is provided in real time via the Internet the following requirements must be met:

- The distributed information service must be operational 24 hours a day, 7 days a week to both the general public and ARIN staff. The service is allowed reasonable downtime for server maintenance according to generally accepted community standards.
- The distributed information service must allow public access to reassignment information. The service may restrict the number of queries allowed per time interval from a host or subnet to defend against DDOS attacks, remote mirroring attempts, and other nefarious acts.
- The distributed information service must return current information.

3.4 Distribution of the ARIN Public Information Database

3.4.1 Supported Uses

ARIN shall make the APID available for the following uses (supported uses):

1. ARIN's use in implementing ARIN policies and other business.
2. Community verification, allowing members of the community to confirm the proper users of the various resources ARIN controls.
3. Statistic gathering by ARIN and third parties on resource utilization.
4. As a contact database to facilitate communication with the person or entity responsible for a particular resource.

3.4.2 Prohibited Uses

ARIN prohibits the use of the APID for the following uses:

1. Sending any unsolicited commercial correspondence advertising a product or service to any address (physical or electronic) listed in the APID.

2. Using data in the APID to facilitate violating any state, federal, or local law.

3.4.3 Other Uses

ARIN shall allow all non-prohibited uses of the APID, however unless those uses are listed as a supported use the data set may be changed in such a way as to render them ineffective, or they may be blocked outright as deemed necessary by ARIN staff. Users of applications not listed who are concerned that they are supported should introduce a proposal to add their application to the supported list.

3.5 Distribution of the ARIN Confidential Information Database

ARIN Staff shall use industry standard procedures to prevent the distribution of any data in the ARIN Confidential Information Database.

3.6 Implementation Details

ARIN Staff shall document all implementation specific details for directory services in a single document available on the web site. The document must contain, but is not limited to:

- *Database field definitions.*
- *Update procedures.*
- *Templates.*
- *Points of contact.*
- *Copies of the AUP.*
- *Verification procedures.*

3.7 [Routing Registry] Copy Verbatim from the existing 3.4.

Section 4.2.3.7.4: Replace with:

All reassignment information for current blocks shall be submitted to ARIN prior to submitting a request for a new allocation.

Section 4.2.3.7.6: Strike."

2005-3: *Lame Delegations*

Policy Statement: "This policy proposal replaces section 7.2 of the ARIN NRPM.

ARIN will actively identify lame DNS name server(s) for reverse address delegations associated with address blocks allocated, assigned or administered by ARIN. Upon identification of a lame delegation, ARIN shall attempt to contact the POC for that resource and resolve the issue. If, following due diligence, ARIN is unable to resolve the lame delegation, ARIN will update the WHOIS database records resulting in the removal of lame servers."

More Information

Listings of active and past policy proposals, complete with previous versions, full policy text and rationale, as well as policy-specific information from the Public Policy Mailing List, and the ARIN Board of Trustees and Advisory Council meetings is available at:

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

Minutes of past Public Policy meetings is available at:

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

Information about ARIN mailing lists, including archives and subscription information for the Public Policy Mailing List, is available at:

http://www.arin.net/mailing_lists/

Unable to attend the ARIN XV? Visit the link below for information about the meeting webcast and remote participation opportunities.

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

ARIN Review

Editor-in-Chief: ***Jason Byrne***

Contributors:

Susan Hamlin
Richard Jimmerson
Megan Kruse
Ginny Listman
Cathy Murphy
Leslie Nobile
Michael O'Neill

Guest Article: ***Jim Bound***