APNIC

Apster

Apster is the quarterly newsletter for APNIC members and the Internet community.

Issue 24 - December 2007

Clients First update: New form release

Newcomers to APNIC can now apply for membership and request resources using a single, simple form released in December.

Development of the new online membership and resource application form is part of an ongoing APNIC initiative called Clients First. The initiative was created in response to comments received through various channels including surveys, meetings, training events and daily helpdesk enquiries.

With this feedback in mind, the Clients First project aims to continuously review member services, improve online form usability and enhance understanding of APNIC policies.

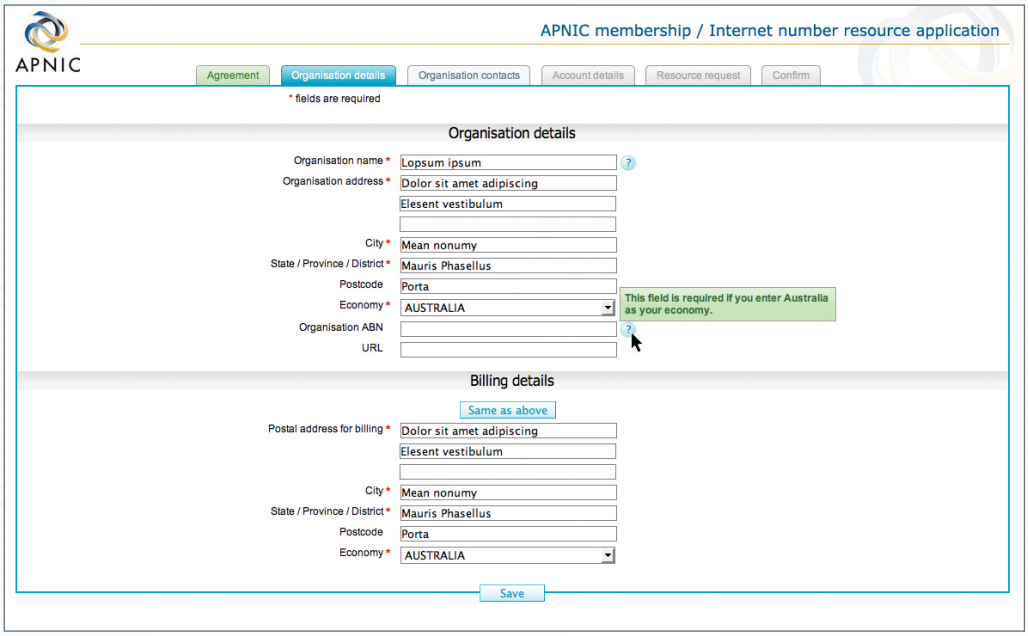
The first phase of the new membership and resource application form focused on creating a 'one stop shop', where newcomers can:

- Apply for APNIC membership
- Apply for IPv4 resources and Autonomous System Numbers (ASNs)
- Create person and maintainer objects (making it much easier to fulfil the initial APNIC Whois database requirements)

Stay tuned for more exciting developments in APNIC service delivery. Future Clients First projects include:

- Rebuilding other online resource request forms for existing members
- Developing a more user-focused forms engine
- Simplifying the procedures for requesting and granting digital certificates
- Improving APNIC web site navigation and revising web content
- Developing simple online tools for people to self-assess their eligibility for resources and the fees that will apply

http://www.apnic.net/services/member



◀ Fast and simple. The new APNIC membership and initial resource application form.

Message from the organisers of APRICOT 2008 Welcome back to Taipei!

The Taiwan Network Information Center (TWNIC) is greatly honoured to host APRICOT 2008 in Taipei. TWNIC welcomes everyone to join us and enjoy the beauty and energy of Taiwan.

Since 1996, APRICOT has established itself as the Asia Pacific's premier regional Internet Summit, providing a focal point for the convergence of the Internet community, as well as hosting annual meetings and other special events. In 2003, APRICOT was held in Taipei for the first time. Over 1,000 Internet technicians and experts from thirty economies attended the event, sharing their knowledge about new and developing Internet technologies while enjoying Taiwan's local hospitality.

Online registration is now open. Be sure to register as soon as possible, as the early-bird discount rates will not apply after 31 December 2007.

If you are interested in registering a presentation slot in the program, please see our website for the second conference call for papers.

http://www.apricot2008.net

Sponsor APNIC 25

We are pleased to announce that APNIC 25 sponsorship packages are now available.

Sponsors play an extremely important role in our Open Policy Meetings. Your support reduces the financial burden on meeting attendees and fosters strong and supportive relationships within the Internet community.

In return for your support, we offer you valuable opportunities to expose your organisation, products and services to an international audience of Internet leaders.

For more information about the benefits of sponsoring APNIC meetings, please download our short movie:

http://streaming.apnic.net/multimedia/sponsorship.mov

Sponsorship package details are available at:

https://www.apnic.net/meetings/25/sponsors

APNIC policy proposal update

Status after APNIC 24

prop-050 IPv4 resource transfer

This is a proposal to remove APNIC policy restrictions on the transfer of the registration of portable IPv4 address allocations and assignments between current APNIC account holders.

Status: Under discussion.

prop-048 IPv6 ULA-central

This proposes the assigning of IPv6 blocks within the 'Centrally Assigned Unique Local IPv6 Unicast Addresses' to organisations or individuals requiring it.

Status: Withdrawn. Not presented at APNIC 24.

▲ APNIC member meeting at APNIC 24 in New Delhi, India

prop-047 eGLOP multicast address assignments

This is a proposal for RIRs to begin assigning multicast addresses from the range specified in RFC 3138.

This proposal was submitted after the deadline for policy proposals to be discussed at APNIC 23. Therefore, this proposal was presented as an informational proposal at APNIC 23, and the decision to adopt, modify or abandon the policy proposal deferred until a later meeting.

Status: Community considering abandoning proposal. Not presented at APNIC 24.

prop-043 Proposal to remove reference to policy document as an 'interim' policy document

This proposes to remove the reference to the "IPv6 Address Allocation and Assignment Policy" document as an 'interim' policy document.

The proposal was presented at APNIC 23, where it did not reach consensus. It was returned to the Policy SIG mailing list for further discussion.

Status: Withdrawn. Not presented at APNIC 24.

prop-042 Proposal to change IPv6 initial allocation criteria

This is a proposal to remove the need to have "a plan to make 200 /48 assignments in two years" and replace it with "a plan to make a reasonable number of assignments in two years".

This proposal was presented at APNIC 23, where the proposer agreed to modify the proposed change to "a plan to make assignments within two years". However, the proposal did not reach consensus at APNIC 23 and was returned to the Policy SIG mailing list for further discussion.

Status: Withdrawn. Not presented at APNIC 24.

Global policy proposal update

IANA policy for the allocation of ASN blocks to Regional Internet Registries

This proposal states that a global policy is required for the RIRs to receive blocks of Autonomous System Numbers (ASNs) from IANA.

Status in RIR regions:

AfriNIC	Last call
APNIC	Awaiting APNIC EC endorsement
ARIN	Last call
LACNIC	Awaiting Board approval
RIPE NCC	Accepted

IPv4 countdown (End policy for IANA IPv4 allocations to RIRs) and Global policy for the allocation of the remaining IPv4 address space

These two policy proposals focus on measures that could be taken globally in address management to prepare for exhaustion of the remaining IANA IPv4 pool.

In order to fulfill the requirements of these policies, at the time one of these policies is adopted, an identical number of IPv4 allocation units (N units) will be reserved by IANA for each RIR. These reserved allocation units will no longer be part of the available space at the IANA pool.

After the exhaustion of the available IPv4 IANA pool, IANA will automatically allocate the reserved IPv4 allocation units (N units) to each RIR.

The proposed value of N units proposed in the 'IPv4 countdown' proposal is equal to 1 and in the 'Global policy for the allocation of the remaining IPv4 address space' proposal it is 2.

Status in RIR regions:

AfriNIC	Rough consensus for N=2
APNIC	Further discuss N=1
ARIN	Further discuss N=1
LACNIC	Rough consensus for N=2
RIPE NCC	Discussing both

*Because both the policies discuss how to prepare for exhaustion of the remaining IANA IPv4 pool, the authors are now working together to propose a single policy across all RIRs.

For the full text related this these and other proposals please visit:

http://www.apnic.net/policy/proposals

index

IPv6 local addresses

Geoff Huston

In making the observation that I've always been fascinated by the process of network technology development I suppose I'm no different to many people who have spent some time in the Internet Engineering Task Force (IETF).

I've often heard this process being likened to that of the development of mathematical systems: The assumption that lurks behind the process is that every proposition is ultimately provably right or wrong, and that the exercise is one of exposing the reasoning that leads to this deterministic outcome. I've heard this deterministic perspective on technology development being used to support many of the processes used in the IETF. On the other hand, I've also heard the view that technology choices are often highly subjective and that technology decisions are often made for reasons that vary between the most whimsical and the most venal.

There are often cases where the 'right' thing to do is blindingly obvious, and other cases where a few basic technology principles can lead you to a sensible outcome. Avoiding complexity and preferring minimalism whenever possible is always a good standard to adhere to. Avoiding continual reinvention of basic tools and building upon experience is also helpful. But even so, there are times when it appears to me that a decision must be made between what appears to be non-technical propositions, and at some point the decision enters the realm of purely subjective judgement.

So how does all of this relate to IPv6 site local addresses? Let's see:

Private use addresses

So-called 'private use' addresses were not part of the original IPv4 address architecture. Addresses were considered to be plentiful, and anyone who asked was given addresses at no cost. It didn't matter whether these addresses were to be used in the context of the nascent global Internet or used in a purely private context. The consistent factor was that all addresses obtained through the address distribution process were unique and could be used in any context – private, semi-private or public – with no risk of collision.

However, this arrangement was not sustainable for two reasons:

- The IPv4 address pool is of finite size, a fact that we are painfully aware of these days, and providing globally unique address space for private use was exacerbating address consumption.
- It was not possible to run an address registry at no cost. While it was convenient that a third party was picking up the tab at the time, this was not a sustainable arrangement.

This was ultimately resolved by creating a distinction between public and private address use. Because private use contexts have no strict requirement for global uniqueness, it is possible for all private use contexts to use the same addresses, leaving globally unique addresses for use in public contexts. The IETF defined the concept of private use addresses in RFC 1597 in March 1994 and later refined it in RFC 1918 in February 1996. These address blocks, 10/8, 172.16/12 and 192.168/16, are defined for private use. This was subsequently coupled with Network Address Translators. The result is that it now appears that more of the Internet is now addressed using private address space than public space.

IPv6 site local addresses

One view of IPv6 is that, given the truly massive address span of 128 bits, the entire concept of address scarcity is irrelevant: In IPv6 there is simply no need to recycle IPv6 addresses for use in private contexts. IPv6 presented us with the ability to revive the consistency of the original IPv4 address architecture where an address had no implicit scope associated with it.

But while IPv6 addresses are abundant, they are not necessarily readily or freely available. The address distribution framework used today exposes the costs of operating the registry function to the address holders. There is also an associated policy framework that imposes qualifications on address holders according to the prevailing policies of address distribution. The costs and the associated policies are well aligned to the public use of addresses, where the value of the utility of these addresses offsets the costs associated with the registry functions. However, the same probably cannot be said with respect to private use. Why should I pay to have globally unique addresses registered simply to set up my home network?

Given the proven utility of private use addresses in IPv4, it was not surprising that the IPv6 address architecture included a private use address pool. This address block, FEC0::/10, was intended for local private use. It was defined in many ways similar to IPv4 private space with overlapping use, no registration requirement, and no usage costs.

Problem solved – right?

Unfortunately, not so!

The problem appeared to be that 'site' was an ill-defined concept. To quote from RFC 3879:

Depending on whom we ask, the definition of the site scope varies. It may map security boundaries, reachability boundaries, routing boundaries, QOS boundaries, administrative boundaries, funding boundaries, other kinds of boundaries, or a combination of these. It is very unclear that a single scope could satisfy all these requirements. In summary, the current concept of site is naive, and does not map operational requirements.

Oddly enough, that was not considered to be a show-stopping problem for IPv4 private use addresses, but for IPv6 this was seen as a significant problem.

However, removing private use addresses altogether from the IPv6 address architecture was not on the cards either. It was not possible to re-implement the concept of a common pool of 'scope-neutral' addresses that had potential use in private or public contexts. The address registry framework was already highly attuned to supporting the public network, with a strong emphasis on supporting provider-based address hierarchies that attempted to keep the inflation of the routing domain under control. In the public IPv6 address distribution framework, you needed to be a service provider to qualify for an address allocation, and all the policies and costs were attuned to the characteristics of the ISP sector.

IPv6 unique local addresses

What was offered to replace a single site local address prefix (where every user would potentially collide with any other user in the event that these local use prefixes leaked out) was a very large set of local-use address prefixes. The intention was that the collection of such local use address prefixes was large enough to meet some reasonable prediction of total demand. It was also anticipated that the prefix selection mechanism would allow each intending user the ability to select a prefix that was unique, preferably without incurring the additional overheads of using an address registry to ensure this. Uniqueness of the local addresses would ensure that even if there were some level of intersection of locally addressed realms, the result would be benign because there would be no consequent address collision.

The IETF's original formulation of these Unique Local Addresses (ULAs) was a two-part approach.

The first part of the approach was to have locally selected ULAs, described in RFC4193. Here, a block of addresses is reserved for local private use (FC00::/7), and one half of that block (FD00::/8) is used with a local selection method. Each intended user generates a 40-bit value at random, and appends to 0xFD to create a 48-bit local use address prefix. This self-selection mechanism certainly satisfies the criteria of being freely available, but the question of true uniqueness in this approach probably needs closer investigation.

How unique are these self-selected ULAs?

When two parties each make a random selection from a 40-bit space, the number of discrete values is 1,099,511,627,776, so the chance that these two selections would collide is around one in a trillion. These can probably be considered acceptably low odds.

More generally, making N selections from a pool of M numbers gives a probability p that any two will collide as:

p = 1 - (N! / N**M x (N-M)!)

Solving this probability for the 40-bit ULA address pool gives the result that the probability of a collision will rise above 0.5 when there are more than 1.24 million random selections from the pool. In a use context strictly limited to private networks, this could still be quite a comfortable outcome. However, if these prefixes were ever to be used in a colliding space, such as in the reverse DNS, or in the public routed network, then any probability of address collision is not an acceptable outcome.

To address this issue of 'almost but not quite unique', the second half of the local use address block, FC00::/8 was to be managed in a more conventional manner using a central address registry to ensure that all selections of address prefixes from this pool were 'assuredly unique'. These 'centrally assigned ULAs', or ULA-Cs, are distinct from the self-selected ULAs.

When this second part of the ULA approach was conveyed to the address policy forums, the reaction was somewhat negative. If these address prefixes are indeed truly unique, then what prevents them being treated in the same fashion as any other piece of public unicast address space? If these addresses are indeed identical to public address blocks in everything but name, then it appears pretty obvious that these addresses would find their way into the public space. The problem with this possibility was that such addresses have no hierarchical structure. They are very similar to the original /24 address blocks in the IPv4 address architecture, and the public use of such addresses has a similar potential to cause routing inflation in the IPv6 world.

The ULA-C proposal was withdrawn for a couple of years, but resurfaced early in 2007 as an active topic. The discussion resumed as to whether it was truly necessary to have 'assuredly unique' local use addresses in addition to the self-selected ULAs that are already defined.

We are now at the essential question here: Are these assuredly unique local use addresses useful or not?

ULA-C addresses and public addresses

The concept of 'uniqueness' is sometimes a poorly understood concept, and maintaining true uniqueness is neither easy nor cheap. Uniqueness is not a private property or an unequivocal attribute of an address. Uniqueness is a public assertion that has very overt displacement properties in both time and space. My public claim that the address I hold is 'unique' displaces any claim you may want to make about the same address being unique to you. If I never make my claim public, then you have no idea that I hold such a claim, and even if I dispute your claim you have no basis to see whether my disputation is valid or not.

Uniqueness is a public assertion relating to the association of an entity with an address. The public nature of the uniqueness assertion immediately brings into the realm of consideration the concept of the validation of such assertions, and the use of trusted third parties in the form of registries. The issues of registries, registry behaviours, costs, policies and public registry properties are all relevant to this topic. If uniqueness is a public assertion about the properties of an association between an address and a holder, should the identity of the holder be a secret? What properties make sense in the context of uniqueness? How should such a unique local address registry be managed? Who should pay the registry operation costs? What registry behaviours are appropriate in this context? What policies are appropriate for entry to the registry?

At this point, the essential difference between global unicast address space and these centrally assigned ULA's becomes fascinating. Given that there are no guarantees about the local or global routability of unicast address space, what is the essential difference between global unicast address space and ULA-C address space?

From the address registry operator's perspective, what is the difference between ULA-C space and IPv6 Provider Independent space? There is essentially no difference in terms of registry functions, and that being the case, the cost to the address holder to maintain the registration entry in the registry, which is an essential condition to ensure uniqueness, should be identical. The registry performs the same actions in maintaining a registry entry in both cases.

What's the difference from the perspective of the end user? It appears that ULA-C space has very strange routing properties. In theory it's not globally routable, but given that there is no clear and coherent distinction between global and local routing, that is a somewhat strange assertion. ULA-C addresses should not be used in certain contexts that we cannot coherently define. Obviously, this does not appear to make a whole lot of sense! On the other hand, unicast addresses have a similar amount of fuzziness: They are not assuredly routable, whatever that may imply.

So what is the real motivation behind the ULA-C proposal? What 'problems' do they solve in local contexts through the subtle distinction of being assuredly unique, as distinct from being probably unique? Are such problems of sufficient magnitude that they would justify the cost of setting up a complete address distribution framework and associated registry operation?

Some further questions about ULA-Cs

Are ULA-Cs really an effort to further dilute the concept of provider-independent address space, as some sort of policy bypass operation? Is there a perceived problem with the Regional Internet Registries' IPv6 address allocation policies? Is the current lack of IPv6 uptake related to having such restrictive address allocation policies that it has become necessary to create an alternative IPv6 address distribution channel to break the current logjam that is withholding IPv6 from its global destiny?

On the other hand, are the prevailing address distribution policies for IPv6 really very topical or useful anymore? What is the objective of those policies? Are we still trying to use current address allocation policies to solve the 1999 routing explosion problem? To what extent do these address allocation policies place limitations and costs on addresses that are based on historical issues that are not relevant in today's environment? Are ULA-Cs a somewhat strange form of uniqueness-lite that is a reaction to the perception that the existing address registry function is too burdensome?

It seems to me that the entire picture behind ULA-Cs is one of confusion, mixed motives, unclear expectations and no coherent concept of the problem that these local use addresses are intended to solve. This tends towards the conclusion that this is a classic case of application of the First Law of Holes. (In case you haven't heard of this law, its pretty simple: If you are in one,

P 6

stop digging!) Why are ULA-Cs needed? What's the true problem here? Are ULA-Cs the most sensible response? Are there other potential responses? What are their relative merits and risks? Why do we need local-use addresses that are assuredly unique in any case?

In trying to craft technical solutions, we are often faced with the proposition that we are attempting to use technology to solve issues that are not necessarily technical in the first place. Is the entire issue that is purported to be about these assuredly unique local addresses really all about how good a job we've done so far with setting up an IPv6 address distribution framework that meets our apparent needs? Are there glaring deficiencies in the current framework of public address distribution for IPv6 that ULA-Cs can solve in a useful and productive manner?

This leads me back to the original proposition: Technology design is often the outcome of entirely subjective decisions. The process can at times be entirely deterministic and logical, while at other times we are placed into a position of having to make decisions that are very much value judgements. In the case of these centrally assigned Unique Local Addresses I suspect that there is no clear right or wrong answer, but instead there are simply a collection of individual opinions. This is going to make any judgement of 'consensus', however rough, quite a tough call.

IETF Documents on IPv6 Site Local and ULA Addresses

RFC1918, "Address Allocation for Private Internets", Y. Rekhter el.al, February 1996.

RFC3879, "Deprecating Site Local Addresses", C. Huitema, B. Carpenter, September 2004.

RFC4193, "Unique Local IPv6 Unicast Addresses", R. Hinden, B. Haberman, October 2005.

Internet Draft (draft-ietf-ipv6-ula-central-02.txt), "Centrally Assigned Local IPv6 Addresses", R. Hinden, G. Huston, T. Narten, June 2007.

Problem /8s

Leo Vegoda, IANA

IPv4 has proven to be exceedingly popular, so it should be no surprise that the time is rapidly approaching when the last /8 block will be allocated and the IANA free pool of address space will be empty. At the time of writing, Geoff Huston of APNIC is projecting that the IANA free pool will run out in mid-2010. Unfortunately, it is possible that some of these remaining /8s may cause problems for enterprise and ISP network operators when they are put back into use. Note: These are not the /8s that have been returned to IANA by the original registrants; these are previously unassigned address blocks.

There are many issues involved with the IANA free pool depletion, but one of these issues seems particularly straightforward to identify and fix. A number of organisations have chosen to use unregistered IPv4 addresses in their internal networks; and, in some cases, network equipment or software providers have chosen to use unregistered IPv4 addresses in their products or services. In many cases, the choice to use these addresses was made because the network operators did not want the administrative burden of requesting a registered block of addresses from an RIR. In other cases, operators may not have realised that RFC 1918 set aside three blocks of address space for private networks, so they just picked what they believed to be an unused block. It is also possible that the operators' needs exceeded the space that could be provided by RFC 1918. Other organisations used default address ranges, suggested by equipment vendors or supplied in example documentation, to configure NAT devices. Regardless of the reasons, this unregistered address usage will come into conflict with routed addresses when the /8s in question are eventually assigned to ISPs or enterprise users.

Examples of /8s where problems are likely to occur include:

1.0.0.0/8
Widely used as private address space in large organisations whose needs exceed those provided for by RFC 1918.

5.0.0.0/8
Used by one of a number of zero-configuration Internet applications (including the Hamachi VPN service).

42.0.0.0/8
The default range used in the NAT configuration of at least one Internet appliance (the HP Procurve 700wlv).

Organisations using these address ranges in products or services may experience problems when more specific Internet routes attract traffic meant for internal hosts. Alternatively, they may find themselves unable to reach the legitimate users of those addresses because they are being used internally. The users of unregistered networks may also find problems with reverse DNS resolution, depending on how their DNS servers are configured. These problems are likely to result in additional calls to enterprise and ISP helpdesks and security desks, because end-users might find this unexpected behaviour hard to diagnose. Users of unregistered address space might also experience problems with unexpected traffic being received at their site if they leak internal routes to the public Internet. Many ISPs have already had experience with this type of routing inconsistency when recent /8 allocations have reached routing tables and bogon filters have been updated.

There are several alternatives to using unregistered IPv4 address space:

- Use RFC 1918 IPv4 address space (there is no need to obtain this from an RIR)
- Use IPv4 address space registered with an RIR
- Use IPv6 address space registered with an RIR
- Use IPv6 Unique Local Address space (there is no need to obtain this from an RIR)

Obviously, all of these efforts will involve renumbering networks, which is sometimes painful and time-consuming. In order to avoid address clashes and routing difficulties, operators using unregistered unique IPv4 address space should look at renumbering their networks or services before the previously unallocated /8s are allocated.

Additionally, vendors and documentation writers can clean up their configurations to ensure they use either RFC 1918 addresses, or make it abundantly clear to their users that they must use registered addresses to avoid routing conflicts.

All RIRs provide free telephone helpdesks where you can seek advice about obtaining unique IPv4 or IPv6 address space. However, if you want to continue using unregistered space and can transition to IPv6, the prefix selection mechanism described in RFC 4193 reduces the probability of a clash to a mere one in 550 billion. Ultimately, transitioning to IPv6 is most likely the

best solution, and taking this approach would offer an opportunity for operators who already need to renumber parts of their IPv4 network to avoid having to subsequently renumber into IPv6.

IANA allocates address space to RIRs according to the global IPv4 and IPv6 policies. Enterprise and ISP networks need to obtain IP addresses from their upstream provider or from the appropriate RIR.

Note: This is a revised version of an article previously published in the Internet Protocol Journal

Sources:

IPv4 projections:

http://www.potaroo.net/tools/ipv4/

RFCs:

http://www.ietf.org/rfc/rfc1918.txt

http://tools.ietf.org/id/draft-hain-1918bis-01.txt

http://www.ietf.org/rfc/rfc4193.txt

HP Procurve:

http://www.hp.com/rnd/support/faqs/700wl.htm

Hamachi:

https://secure.logmein.com/products/hamachi/howitworks.asp

http://en.wikipedia.org/wiki/Hamachi

ICANN allocation policy:

http://www.icann.org/general/allocation-IPv4-rirs.html

http://www.icann.org/general/allocation-IPv6-rirs.htm

APNIC IPv6 transit exchange

APNIC is facilitating IPv6 adoption in the Asia Pacific region by introducing an IPv6 transit exchange. This will allow APNIC to support IPv6 while increasing the awareness, understanding and use of IPv6 in the Asia Pacific region.

The IPv6 transit exchange is a research and development project that will continue to run for as long as the participants require APNIC to provide the service. However, this situation will be reviewed when commercial providers begin to offer native IPv6 services.

APNIC will also advertise prefixes and negotiate peers for both 2-byte and 4-byte Autonomous System Numbers (ASNs) to IPv6 neighbours of this service.

The preference for the IPv6 exchange is a Multi-Lateral Peering Agreement (MLPA) style service. That is, we will re-advertise all routes presented to us. The more routes you are willing to advertise, the better! As such, any offers from organisations to provide full transit will be greatly appreciated.

Any organisation with an IPv6 prefix is welcome and encouraged to join.

Fore more information, please see the latest ICONS blog entry at:

http://icons.apnic.net

Member news

Resource Certification update

The goal of certification is to facilitate increased trust in resource management. The depletion of the available IPv4 pool increases the likelihood of resource transfers in the future. This means that being able to establish clear title for your resources and the resources of others will become increasingly important. The same services will also permit more secure routing models to be deployed and help to control risk on the Internet. This article outlines the current resource certification developments at APNIC.

Project status

APNIC is continuing with its project to develop software and services that will support resource holder certification processes in the future. The current activity involves developing a system that can be deployed by your organisation's IT department to manage the exchange of certificates between APNIC and your organisation. This will be controlled by your organisation through MyAPNIC.

The Resource Certification System is intended to be a publicly visible registry that will enable your organisation to view a secure 'audit trail'. It provides verifiable proof that a given entity has control of a resource, and that any entity that is granted control of or transfers a resource can be audited to show they have effective control, and that it has been properly delegated.

The Resource Certification System code is open source and can be independently developed as the need arises. OpenSSL is used to provide the cryptographic services, which can also use a Hardware Security Module (HSM) to provide additional protection for the keying materials.

The system will be deployed towards the end of 2007 for initial public tests, and released as a service in early 2008.

Stay tuned for service availability announcements, and expect to see a presentation at the next APNIC meeting.

APNIC and ARIN to conduct system interoperability tests

APNIC and ARIN have agreed to conduct interoperability tests while they develop their respective Resource Certification systems. These tests are designed to ensure that resource holders and other parties that rely on this information can be confident that the in-house resource management systems they use to interface with APNIC or ARIN (or any other resource certification service provider using their code) will work properly.

Interoperation is also required to control the management of historical resources that were distributed before the establishment of the Regional Internet Registries.

APNIC reverse DNS management update

APNIC has recently upgraded its DNS management system. This upgrade tackles APNIC reverse DNS stability issues brought about by the complex interactions with the NIRs in 'sharing' the management of APNIC in-addr.arpa/ip6.arpa zones. The upgrade also satisfies the desire of APNIC members to have a faster, more codified, and secure update mechanism. The recent work also provides a platform for future augmentation of the user-facing APNIC reverse DNS management system.

Currently, in order to carry out a DNS delegation of a reverse zone, our members must either log in to MyAPNIC or submit a domain object to Whois via email with their authorisation credentials present as cleartext. Neither of these processes is truly amenable to automation or integration into members' IP address management systems; however, the upgraded system is built around dynamic DNS and a REST update model.

This means that when updates for APNIC zones are supplied by a XML/REST via HTTPS API using your APNIC certificate, they will be propagated to the DNS in less than two minutes. The current process of submitting objects via Whois has a two-hour turnaround time.

The new system has been released for the NIRs to use because they represent key focus points for changes in the DNS. We expect to make this service available to the entire APNIC membership in the first half of 2008.

Before this occurs, documentation and training materials will be completed, and the XML schema will possibly be modified to support DNSSEC. The current XML schema can be viewed at

http://www.apnic.net/specs/reversedns/1.0

Who is your corporate contact?

It is vital that your organisation has an up-to-date corporate contact. This person should be someone who is entrusted with the authority to make high-level decisions for your organisation. The corporate contact has important responsibilities relating to:

- **Voting**
- **Using MyAPNIC to manage resources**
- **Authorising other APNIC contacts for your organisation**
- **Communicating with APNIC about membership changes**

Want to know more? Please see:

http://www.apnic.net/member/corp-contacts

ICONS feedback

Many of our readers may be familiar with APNIC's Internet Community of Online Networking Specialists (ICONS). This site is designed to enable sharing of network operation experience and knowledge, and promote events in the Internet operator community.

ICONS has been altered a few times since its inception in August 2005. In response to member feedback, cosmetic changes have been made to the site, and it has moved from forum to blog format. It also now includes news feeds and user guides.

APNIC 24, held in September this year, featured a well-attended ICONS BoF. The purpose of the session was to create awareness and demonstrate key sections of the site, seek feedback about ICONS and discuss ways to improve the site and broaden its user base.

While there are many technical forums available, many of them are confined to smaller regions, such as the Pacific. The ICONS site enables users to connect with other users from all over the Asia Pacific. Recent partnerships formed with SANOG, APRICOT and AfriNIC have further extended the site's reach.

We encourage anyone who is interested to visit our site:

http://icons.apnic.net

and send feedback to icons@apnic.net

MyAPNIC improvements

The latest MyAPNIC release runs ten times faster than the previous version. In addition to this performance enhancement, users can now save time by using MyAPNIC to add, update and delete the following Whois objects:

- Person object
- Role object
- Maintainer object
- Route object
- Aut-num object
- Domain objects

Other recent updates allow you to:

- View your organisation's full billing history
- Download and pay membership renewal invoices online
- Download Whois data at any subnet level
- Vote online and nominate voting contacts (corporate contacts only)

In the future, members will also be able to use MyAPNIC to:

- Reduce the time it takes to complete resource request forms
    - Details of previous assignments will automatically be inserted into the request from MyAPNIC. Administrative and technical contacts will be chosen from drop-down lists of existing organisational contacts.
- Perform a 'search and replace' for APNIC Whois database updates
- Set up username and password access
- Facilitate forward and reverse secondary DNS hosting
- Add, update and delete Whois inet6num objects

Are you using MyAPNIC?

To find out more about how MyAPNIC can help you manage your resources please visit:

http://www.apnic.net/services/myapnic

or contact helpdesk@apnic.net

Community interface

AusNOG 2007

In November this year, the first Australian Network Operators Group meeting was held in Sydney. In this article, APNIC's Geoff Huston discusses his experience of the conference.

It's been too many years since Australian network operators got together and had their own workshop that was focused on their common interests in network operational technology. Various network operators groups, or 'NOGs' are active all over the world, so it was all the more welcome to see the first Australian Network Operators' Group meeting in November 2007.

The topics that interest network operators are certainly many and varied, ranging from the trials and tribulations of deploying competitive DSL infrastructure in Australia, through to a detailed analysis of the differences between wireless and wired infrastructure for non-metropolitan areas.

Because Australia is an island, it's not surprising that if you want high capacity connectivity in and out of Australia, submarine cable is an absolute requirement. The latest developments in cable technology and forthcoming cable installations were discussed at this AusNOG meeting.

This high frontier of long distance telecommunications infrastructure is no longer an activity that is the exclusive preserve of the legacy telephone operators, as a new wave of competition is entering this once tightly controlled space. Workshop attendees were also given an in-depth analysis of the next set of DSL standards and how DSL is managing to get up to 50Mbps out of a single copper pair, with the prospect of a further doubling of this speed with the latest Australian research on this topic.

It's pretty much mandatory at the moment to have an update on the looming exhaustion of the IPv4 address pool and the state of IPv6 deployment (or lack of it), and this workshop was no exception. We also heard about a less well known exhaustion issue within the Autonomous System (AS) number space used by Internet routing and the way in which this is being addressed at the operational level in the BGP protocol. Put this together with information about botnet activity, device-driven networks and overlay service delivery, and you have a very full agenda of operational topics.

▲ Virtual world network administration: As we looked on, another collaborating network administrator placed an ACL against an attacking machine, using an in-world metaphor for interaction.

http://caia.swin.edu.au/urp/l3dge

Network engineers and operators, and the vendors who sell to this industry weren't the only people in attendance at this conference. Some of the issues that are exposed in these operational venues are substantial research issues; and, like other NOG venues across the globe, the AusNOG workshop attracted interest from researchers who are working in this area.

Participation at AusNOG from the Swinburne University of Technology's Centre for Advanced Internet Architecture was notable in this respect. Their approach to real time network monitoring using a 3D game engine was truly innovative, and if I had to nominate what I found to be the most novel presentation of the workshop it would have to be these researchers and their network management game engine.

At one level, there is something quite appealing to my inner geek about shooting an Access Control List into a recalcitrant router! On a slightly more serious level, it is really heartening to see that there is still active academic and research interest in networking, and that researchers in the Asia Pacific region are considering some truly innovative approaches to meet some of the tougher outstanding challenges in network operations.

Training trips

During this quarter of 2007, APNIC has conducted a number of significant training events. We played a major role in a very successful Internet crime workshop and advanced DNS training held recently at IntERLab in Thailand. We also delivered training in Laos and the Maldives for the first time.

During the IntERLab workshop in **Thailand**, we were pleased to be able to further develop our collaboration with the USA's Team Cymru who joined with us to conduct our training. Internet crime is at epidemic proportions and has generated a significant underground economy. Participation in a seminar on the topic clearly reflected the local community's great interest and enthusiasm for collaborative and co-ordinated action. We will be working with Team Cymru and others in the security community to promote and facilitate development of a viable NSP-SEC-AP forum that will act as a volunteer incident-response mailing list and co-ordinate interaction between ISPs and NSPs to track and respond to exploits on ISP networks in near real-time.

We also visited **PNG** after a long absence and were very well received by a community keen for training and information. The event was sponsored by The International Training Institute (ITI). In the words of one participant: "This was a REALLY GOOD workshop…would very much like you guys to continue giving such trainings here in countries like ours who are not so advanced with new changes. I understood and liked the workshop very well."

We conducted our first training event in **Laos** with the assistance of IntERLab and the National University of Laos (NUOL). The participants included faculty staff and ISPs. This event was also a successful outcome for our train-the-trainer initiative: APNIC Hostmaster Annie Tallents participated in delivering the IRME (Internet Resource Management Essentials) course and the routing workshop. The continued development of this program will enable hostmasters and member services staff to be involved in training and meet with members face-to-face. The director of the computer department at NUOL indicated strong support for our training initiatives and was very keen for us to return in the near future.

In November we conducted the first IPv6 workshop to be held in **Sri Lanka**, sponsored by Lanka Internet Services, a founder member of APNIC.

Participants were particularly concerned about IPv4 address depletion and the effects on developing economies. There was considerable interest in further discussion and we hope to conduct a South Asian event in the near future.

Dhiraagu sponsored our inaugural **Maldives** training. Around 40 people attended the training, which covered resource management and some security issues. Again, participants asked for further training and information about IPv6.

We would like to thank our sponsors and hosts whose support is vital in helping us conduct our training throughout the Asia Pacific.

▲ Training in Sri Lanka

China Netcom

China Mobile

The University of the South Pacific

IntERLab

National University of Laos

International Training Institute

DHIRAAGU

Lanka Internet Services

Representing our members on the world stage

▲ NRO brochure: Continuing Cooperation

In addition to organising and attending events in the Asia Pacific, APNIC representatives have also recently attended international community events.

The Internet Corporation for Assigned Names and Numbers (ICANN) public meeting was held in Los Angeles, USA in late October. ICANN is responsible for the global coordination and distribution of the Internet's system of unique identifiers, such as domain names, country codes and IP addresses. APNIC Director General Paul Wilson spoke at the Internet Assigned Numbers Authority (IANA) IPv6 workshop, which focussed on practical issues regarding IPv6 deployment. Presentation details are available at

http://losangeles2007.icann.org/node/36

The second Internet Governance Forum (IGF) was held in Rio de Janeiro in November. The IGF's purpose is to support the United Nations Secretary-General in carrying out the mandate from the World Summit on the Information Society (WSIS) with regard to convening a new forum for multi-stakeholder policy dialogue. APNIC participated as a member of the Number Resource Organization (NRO). The NRO was one of the organisers of the 'IPv4 to IPv6: challenges and opportunities' workshop. Paul Wilson and Adiel Akplogan (AfriNIC) were speakers. Presentation details are available at

http://www.intgovforum.org/wks_session_info.php?numes=30

The NRO recently published a report entitled 'Continuing Cooperation' which was distributed to IGF particpants. Any interested party can download a PDF of the report at

http://www.nro.net/archive/news/continuing-cooperation.html

Printed copies can be requested via secretariat@apnic.net

▲ Paul Wilson (second from left) presenting at IGF

Secretariat spotlight - What's new at APNIC?

Software Engineering update

The Software Engineering Unit operates behind the scenes at APNIC, working on many of the systems and interfaces that our members use every day. Some of the projects the team have been working on recently include:

MyAPNIC performance improvement

Optimisation of APNIC's web application technologies has resulted in a 10x performance improvement to most MyAPNIC pages. This effort is part of an ongoing project to enhance the MyAPNIC user's experience.

Clients First form

For several months, Software Engineering has been working on the back end of a form that enables users to apply for membership and submit their first resource requests at the same time. This work includes writing scripts that enable APNIC Whois Database objects to be created automatically.

Reverse DNS web service

APNIC will soon be taking its first step towards offering a full suite of XML services to its members. Software Engineering is currently working with Network Operations on an XML-based web service that members can use to update their reverse DNS records. Stay tuned for more details.

Resource Certification

The Software Engineering Unit is currently working on an APNIC Resource Certification service, which is set to be integrated into MyAPNIC in 2008.

Office Management update

The Office Management Unit is a small team comprised of just three staff members. You may have spoken to Ensi and Cheryl on the phone, as they are responsible for reception and various other aspects of APNIC's office administration.

The Office Unit provides administrative support to the APNIC Secretariat and supports essential day-to-day operations. Our staff also assist with various events including APNIC meetings and training.

Current projects include streamlining processes and improving efficiency by developing a culture of continuous improvement. We believe high quality administrative support is vital for the smooth running of every area within APNIC.

In 2006 we embarked on a green office initiative. The ecoAPNIC project team engages and educates staff about modifying behaviours and practices to reduce our organisation's ecological footprint. This began with APNIC greeting cards being produced electronically (with the money saved on printing and postage donated to charity).

To date we have switched to environmentally friendly paper products and are currently researching and implementing greener options for other office products. We recently replaced 200 fluorescent light tubes with a more advanced type that uses the same amount of electricity but emits a much brighter light. This has effectively halved the amount of electricity APNIC consumes for lighting.

▲ Software Engineering Unit

▲ Office Management Unit

NIR training

APNIC recently hosted two colleagues from CNNIC. Zhao Wei was our guest from October to November, shortly followed by Zhang Jian who visited us from November to December.

Both visitors received training within the Resource Services Unit and learned about our hostmaster, billing, technical, administration and policy functions.

▲ Zhao Wei

▲ Zhang Jian

Staff updates

John Tan
Training Officer (eLearning)

John joined APNIC in November 2007. He has a Masters of Information Technology and brings to APNIC his experience in web application development, database implementation and multimedia applications. He is also a skilled IT instructor and online training facilitator, and will focus on the development and delivery of APNIC's online training.

Ben Peters
Systems Administrator (Infrastructure)

Ben joined APNIC in December 2007. In his previous role he gained experience in supporting internal and wide area networks, and has had exposure to a broad range of servers, operating systems and applications. As part of the Network Operations team, his primary responsibilities at APNIC are maintaining the network and associated environments.

The APNIC Secretariat would like to thank you for your support this year.

We wish you a happy and safe festive season and a prosperous new year.

Training schedule

2008

January

10-18 Dhaka, Bangladesh, in conjunction with SANOG 11

23-25 Dunedin, New Zealand, in conjunction with NZNOG 08

February

20-29 Taipei, Taiwan, in conjunction with APNIC 25/APRICOT 2008

TBA Indonesia

TBA Australia

March

TBA Manila, Philippines (hosted by ASTI)

TBA Kuala Lumpur, Malaysia

April

TBA Kathmandu, Nepal (hosted by NPIX)

TBA Pakistan, in conjunction with NSP

TBA India

May

TBA Japan, in conjunction with JPNIC

TBA China

June

TBA Singapore

TBA Phnom Penh, Cambodia (hosted by Angkor Net/Anana Computer)

TBA Bangkok, Thailand (hosted by AIT)

TBA Ulaanbaatar, Mongolia (hosted by Datacom)

July

TBA Vietnam

The APNIC training schedule is subject to change. Please check the web site for regular updates at:

http://www.apnic.net/training

If your organisation is interested in sponsoring APNIC training sessions, please contact us at:

training@apnic.net

Calendar

SANOG 11

10-18 January 2008
Dhaka, Bangladesh
http://www.sanog.org/sanog11/

PTC '08

13-16 January 2008
Honolulu, USA
http://www.ptc08.org/

25th APAN meeting

20-25 January 2008
Hawaii, USA
http://www.apan.net/meetings/hawaii2008/

NZNOG '08

23-25 January 2008
Dunedin, New Zealand
http://2008.nznog.org/

JANOG21

24-25 January 2008
Kumamoto, Japan
http://www.janog.gr.jp/index-e.html

CNNOG 5

TBD January 2008
Beijing, China
http://www.cnnog.org/future-e.htm

ICANN 31st International Public Meeting

10-15 February 2008
New Delhi, India
http://www.icann.org/meetings

ICT Africa

13-15 February 2008
Addis Ababa, Ethiopia
http://ictafrica.nepadcouncil.org/

NANOG 42

17-20 February 2008
San Jose, USA
http://www.nanog.org/

APNIC 25/APRICOT 2008

20-29 February 2008
Taipei, Taiwan
http://www.apnic.net/meetings/25/

71st IETF

9-14 March 2008
Philadelphia, USA
http://www.ietf.org/meetings/0mtg-sites.txt

MENOG3

25-27 March 2008
Cairo, Egypt
http://www.ripe.net/meetings/menog/

Frost and Sullivan OSS BSS Asia Pacific Summit 2008

27-28 March 2008
Grand Copthorne Waterfront Hotel, Singapore
http://www.frost-oss.com/

ARIN XXI

6-9 April 2008
Denver, Colorado, USA
http://www.arin.net/ARIN-XXI

PITA

21-24 April 2008
Palau (TBC)
http://www.pita.org.fj/index.cfm?action=events

How to contact APNIC

Street address	Level 1, 33 Park Road, Milton, Brisbane, Qld 4064, Australia
Postal address	PO Box 2131, Milton Qld 4064, Australia
Phone	+61-7-3858-3100
SIP	info@voip.apnic.net
Fax	+61-7-3858-3199
Web site	www.apnic.net
General enquiries	info@apnic.net
Hostmaster (filtered)	hostmaster@apnic.net
Helpdesk	helpdesk@apnic.net
Training	training@apnic.net
Webmaster	webmaster@apnic.net
Apster	apster@apnic.net

Member Services Helpdesk

The Member Services Helpdesk provides APNIC members and clients with direct access to APNIC Hostmasters.

www.apnic.net/helpdesk

helpdesk@voip.apnic.net

helpdesk@apnic.net

+61 7 3858 3188

Helpdesk Hours: 9:00 am to 7:00 pm (UTC + 10 hours) Monday - Friday

Are you using MyAPNIC?

APNIC members can use MyAPNIC to:

- View APNIC resources held by their organisation
- Monitor the amount of address space assigned to customers
- View current and past membership payments
- View current tickets open in the APNIC email ticketing system
- View staff attendance at APNIC training and meetings
- Vote online

For more information on MyAPNIC's features see:

www.apnic.net/services/myapnic

eco APNIC
This issue of *Apster* is printed on ONYX recycled paper.