APNIC

Apster

-ster *(suffix)* One that is associated with, participates in, makes, or does. For example: *songster.*
Source: ***www.dictionary.com***

www.apnic.net

Issue 12 December 2004

APNIC - Addressing the challenge of responsible Internet resource distribution in the Asia Pacific region

IP addressing in China

Managing the distribution of Internet resources, such as IP addresses and AS numbers, is a central responsibility of APNIC and the other RIRs around the world. However, for many in the Internet community, IP addressing and address policy are subjects which remain clouded by common misunderstandings.

Some of the most prevalent of these regard IP addressing in the Asia Pacific region, or in specific parts of the region, such as China. Press sources around the world have made claims on many occasions that IPv4 address space will run out imminently, or that addresses are in short supply in the Asia Pacific. The development of the Internet in China is often highlighted, but often with reports that Chinese organisations are unable to obtain appropriate amounts of address space.

Wherever APNIC has encountered these rumours, it has sought to correct them. In this article, we discuss some of the specific issues that have been raised in relation to IP addressing in China.

How much IPv4 space is left?

It has often been reported that the Internet will run out of IPv4 address space within the next few years. In contrast, experts including APNIC's Internet Research Scientist Geoff Huston have projected that at today's consumption rates IPv4 could last another 15 to 20 years. This projection is certainly not a prediction, as the future of the Internet is unknown; however, being based on several years' IPv4 address consumption (including the period of the dot-com boom), it is an important result.

Comparison of Chinese IP address holdings with MIT, Stanford etc.

During the early days of the Internet, IP address space was assigned according to the classful system, with address blocks available in 3 fixed sizes: class C, providing 256 addresses (/24 in today's terms); class B, providing 65,000 addreses (/16); and class A, providing 16 million addresses (/8). This was a period when address conservation was not seen as a priority and during the 1980s and into the early 1990s many large organisations, most of them in the United States, were assigned /8 address blocks. These organisations included large universities such as MIT and Stanford, as well as corporations like Apple Computer and Boeing.

A common misconception is that Chinese organisations hold a combined total of less address space than one of these 'legacy' /8 holders. This has not been true since sometime in 2000 or 2001, at which time total IP address holdings in 'CN' exceeded a /8. Today, China holds the equivalent of more than four of these blocks and this is constantly increasing.

Myth of address 'shortage' in China

Another prominent myth is that there is an IP address 'shortage' in China. Often this appears to be based on an observation of the static distribution of IP address space, which is indeed unfair due to the historical factors described above. However, to claim a shortage implies that addresses are somehow not available, and shows a misunderstanding of the role played by the RIRs, including APNIC.

Throughout the Asia Pacific region, APNIC allocates address space in response to allocation requests, and very few requests for address space are turned down. Mainland China now receives addresses at a faster rate than any other economy in the world (followed by Japan, then the USA). From an administrative perspective, China is receiving as many IP addresses as are requested, and allocations are made with few delays. While some allocations in China are made independently by CNNIC – the National Internet Registry (NIR) – APNIC works closely with CNNIC to ensure that supply of addresses is always maintained as needed.

The allocation of address space to RIRs from the IANA, and to ISPs from the RIRs (sometimes via National Internet Registries, or NIRs, in the APNIC region) is a continual process, and all allocations are made according to demonstrated need under

1

P 2

Details P 3

a consistent set of policies. There is no preallocation of addresses to any economy or region in the world, meaning that a 'shortage' in any one country or economy simply cannot happen, except (and in theory only) as a result of specific national circumstances, of a type which do not appear to exist in China.

IP addresses in China today

Recent presentations and publications by APNIC have demonstrated the strong growth in address space being allocated to China. These support the common knowledge of massive growth of the Internet which is sure to continue for many years to come.

The Director General's report at the recent APNIC 18 Open Policy Meeting demonstrated this growth over the past several years. This presentation is available on the APNIC website at:

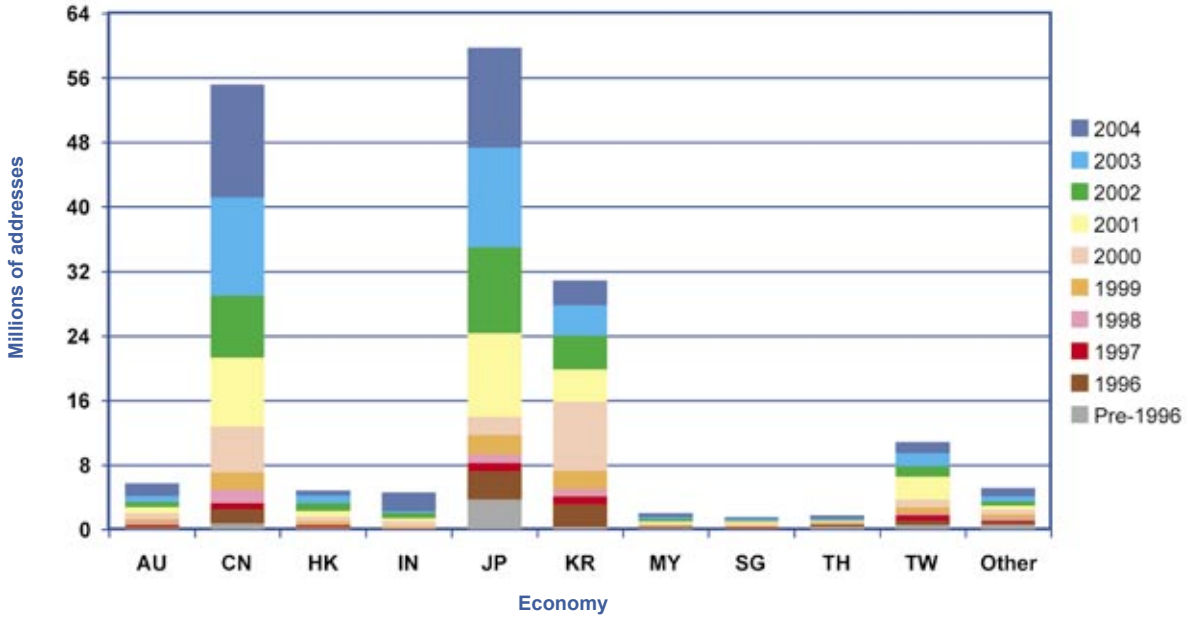
http://www.apnic.net/meetings/18/docs/amm/amm-pres-pwilson-opening.ppt

It is important to note that while the percentage of APNIC members in China is relatively small, this is because many Chinese organisations receive their address space through CNNIC. As seen in the chart below, China is currently the fastest growing destination for IPv4 address space allocated by APNIC – this in a year in which APNIC has allocated more address space than any of the other RIRs.

The global system for IP address distribution is constantly evolving, in response to requirements and proposals which arise through the APNIC Open Policy process. APNIC and the other RIRs have ensured that this occurs in an open, transparent, and bottom-up system, meaning that no single economy or region is advantaged or disadvantaged. All parties have their chance to participate in the policy-making processes and to promote their own interests, and in a world of finite resources, this has proven itself an outstandingly successful solution.

Paul Wilson
Chris Buckridge

IPv4 address distribution, by economy, by year



AfriNIC prepares for operations

AfriNIC, the emerging RIR for Africa, is continuing to prepare for full operations. After its progress was welcomed at the ICANN meeting in Kuala Lumpur (May 2004), AfriNIC now expects to seek full recognition as an RIR during 2005.

Under the leadership of Adiel Akplogan, AfriNIC will distribute its technical and administrative operations across several locations spanning the continent.

All existing RIRs are committed to continuing to provide support to AfriNIC to help it take these final steps toward full recognition, including training, software, and administrative assistance.

One visible display of this support is the new AfriNIC logo, which was designed by APNIC's graphic designer, Chiaki Kanno.

When AfriNIC commences full operations, it will assume responsibility for many economies currently served by the other RIRs. Those in the current APNIC region that will be transferred to AfriNIC are Comoros, Madagascar, Mauritius, Mayotte, Reunion and Seychelles. There are currently four APNIC members in those economies.

AfriNIC
The African registry for Internet Numbers

"I really like this logo not only because it is beautiful but also because it has a particular meaning for us. The feathers symbolise hope; and for Africa we need that to move ahead! Moreover the colors look very attractive for me!" – *Adiel Akplogan*

APNIC Open Policy Meeting

21 – 25 February 2005 Kyoto – Japan

APNIC invites members, and those with an interest in the development of the Internet in the Asia Pacific to attend the 19th APNIC Open Policy Meeting (APNIC 19), which will be held from 21-25 February 2005 in conjunction with APRICOT 2005.

The meeting will be held at the Kyoto International Conference Hall (KICH) in Kyoto, Japan, and will include tutorials, Special Interest Groups (SIGs), Birds of a Feather sessions (BoFs), hostmaster consultations, the APNIC Member Meeting (AMM), and a social event. Some details are listed below:

Tutorials **21 - 22 February 2005**	Tutorials on APNIC policy development, spam, and security issues will be available.
Special Interest Groups **23 - 24 February 2005**	Members of the Internet community are invited to present and participate. The call for presentation proposals is now open. See below for details.
AMM **25 February 2005**	The AMM is open to all. APNIC members can attend free of charge.

Meeting features

Meeting attendees, along with those in other parts of the world, will be able to follow and participate in meeting proceedings via:

- **Video streaming**
- **Live transcripts**
- **Jabber chat**

Call for proposals

A request for contributions is currently open for those who would like to make either informational or policy proposal presentations at the APNIC 19 SIGs. Proposals are welcome from anyone interested in Internet resource management in the Asia Pacific region.

If you would like to take part in any SIGs, please submit a proposal by 19 January 2005, using the online form at:

http://www.apnic.net/cgi-bin/policy_proposal.pl

Alternatively, you can send your proposal in text format to the appropriate SIG, CCing <sig@apnic.net>. Proposals will be forwarded to the appropriate SIG mailing list by the Secretariat.

Please forward any enquiries regarding APNIC 19 to meetings@apnic.net.

For more information see:

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

APNIC 19 will be held at the Kyoto International Conference Hall

index

Introducing DNSSEC

With the help of a 'potential' news story, **Olaf Kolkman** explains why the Internet needs DNSSEC, how it works, and what is needed for its full scale implementation.

Olaf Kolkman is a System Architect in the New Projects Department of the RIPE NCC. Among other things he is co-chair of the IETF DNSEXT working group that developed the DNSSEC standard and is author of the Net::DNS::SEC Perl library.

The Junee Business Times

Junee, 33 November 2004

BE-rt and erNie merger stung in DNS scam

The Junee branch of Interpol's cyber crime department has arrested five individuals who are supposedly linked to the US$50 million stock fraud that occurred last month in relation to the merger of BE-rt Inc and erNie Ltd. The gang operated by exploiting weaknesses in the Domain Name System (DNS). The DNS is the system that is used to translate names like www.apnic.net into the addresses of individual computers. The DNS is used whenever someone uses a name to access a service on the Internet.

An Interpol spokesman explained. "The gang used exploits in the DNS to reroute and intercept emails that related to the merger between the two companies. After obtaining prior knowledge on the stock rate and the date of the merger the gang used the same DNS exploits to reroute a stock-ticker service. By inserting false stock rate information for BE-rt Inc, they managed to influence the stock market on the day prior to the merger in a way that maximised the gang's prior knowledge. Through clever trading of stock options these guys earned US$50 million".

Insider knowledge was suspected when complaints about the false stock ticker information surfaced. Only after a full audit of the erNie Ltd computer environment was it shown that the information was not consciously leaked by the senior management of the two companies.

The scenario as described in the fictional article above is not as far-fetched as it may seem. In virtually all interactions between computers on the Internet, services are located using the DNS. Email recipients are identified using the DNS; web services are found using the DNS; and applications like messengers, stock tickers, and Internet telephony all use the DNS to find the machines that one needs to connect to for interaction.

The DNS is vulnerable to attacks where the name-to-address mapping is being modified by an attacker. This problem was identified years ago. Since then, engineers have joined forces in the Internet Engineering Task Force (IETF) to develop extensions to the DNS that allow these name-to-address mappings to be secured. The security extensions are known as DNSSEC and are expected to be published as RFCs (Request for Comments, the IETF's standard documents) late in 2004.

After many years of development, DNSSEC has reached production quality in both specification and implementation. The BIND9.3.0 and NSD2 name server implementation both use DNSSEC. DNSSEC is now ready for the public Internet.

DNSSEC is based on public key cryptography mechanisms and allows DNS data to be verified for integrity and authenticity. In other words, by using DNSSEC one can tell wether or not somebody inserted a fake IP address for the mail server for 'BE-rt Inc' and that the IP address for the stock-ticker service was replaced. DNSSEC would have prevented the mail and the stock-ticker service redirect in the above virtual example.

One could argue that this attack would not have been possible if the mails between the two companies had been encrypted and if the stock ticker server had used secured http. But in reality, encrypted email and secure stock tickers rarely happen. Deployment of DNSSEC raises the bar for a large set of attacks on all kinds of applications for which maintaining security on the application level may be too expensive to do correctly. Many end-users do not use mail encryption because it is too difficult or too expensive.

It is expected that DNSSEC deployment will slowly pick up in 2005. As with all early deployment there will be a few hurdles that need to be cleared: tools for DNSSEC administration are in their infancy and the benefits of early deployment are small, as there are very few signed zones and very few validating name servers On the other hand, early deployment may provide competitive benefits in case DNSSEC deployment ever becomes urgent. Numerous parties, including top-level domain (TLD) registries are planning pilot projects for the deployment of DNSSEC and the RIRs are actively tracking developments while planning for deployment.

Although the protocol and implementation details of DNSSEC are somewhat esoteric, the principles are fairly simple. As noted above, the protocol is based on public key cryptography. Public key cryptography schemes are based on 'key-pairs' consisting of a private and a public key. Users generate such pairs, publish the public key to other users and keep the private key securely secret. If Alice signs a piece of data with her private key, then Bob can verify that the data originated from Alice with the public key. If Bob did not obtain the public key from Alice directly, then he will still be able to validate the data provided a chain of trust exists between a key that Bob has securely obtained and Alice's key.

This is also the way that secure http works. You have securely obtained the root certificate, these sign a web servers key, hence you trust the web server. In DNSSEC the Alices of the world are the people who put together the zone data. They have a private key with which they sign the DNS data. The Bobs of the world are the DNS clients that will use the DNS to build chains of trust to validate the DNS data. For successful deployment, we will need Alices to sign DNS data and Bobs to validate this data.

This 'chicken and egg' problem is one of the major deployment hurdles. Very few people will configure their recursive name servers to validate DNSSEC data in the absence of DNSSEC zone data. Few zone administrators will sign their data in the absence of validating clients. Few application developers will build new (presumably very interesting) applications based on top of DNSSEC, without an infrastructure being present. We can only hope that this deadlock is broken by deployment initiatives before the first major DNS attack takes place.

Further reading on DNSSEC

The scope of this article is too limited to go into the details of the DNSSEC protocol, its implementation, and its operation. Below are some relevant resources.

The IETF has finalised work on the protocol definition; the following documents are about to be published as 'standard-track' RFCs:

ftp://ftp.ietf.org/internet-drafts/draft-ietf-dnsext-dnssec-intro-13.txt

ftp://ftp.ietf.org/internet-drafts/draft-ietf-dnsext-dnssec-records-11.txt

ftp://ftp.ietf.org/internet-drafts/draft-ietf-dnsext-dnssec-proto-09.txt

A good portal to DNSSEC-related information is available at:
http://www.dnssec.net/

A 'how to' guide on installing and operating DNSSEC is available at:
http://www.ripe.net/projects/disi/dnssec_howto/

Miek Gieben wrote an instructive article in the *Internet Protocol Journal*, available at:
http://www.cisco.com/en/US/about/ac123/ac147/archived_issues/ipj_7-2/dnssec.html

Some assorted DNSSEC pilots are:
http://www.nlnetlabs.nl/dnssec/

http://www.dnssec-net.verisignlabs.com/

http://dnssec.nic-se.se/

Some DNSSEC operational issues are addressed in:
ftp://ftp.ietf.org//internet-drafts/draft-ietf-dnsop-dnssec-operational-practices-02.txt

Training

The RIPE NCC provides a course on DNSSEC, material for which is available at:
http://www.ripe.net/training/dnssec/material/

APNIC has also developed DNSSEC content for its Advanced DNS Workshop, which will be featured in the next issue of *Apster*.

Privacy of customer assignments policy

As reported in the last issue of *Apster*, the APNIC Secretariat has now implemented the database changes for the privacy of customer assignments policy. LIRs can now decide whether or not their customer registration details will be publicly visible in the APNIC Whois Database. If an LIR chooses not to designate its customer assignment information as 'public', database queries on address ranges assigned to downstream customers will be directed to the upstream provider's registration information.

By default all customer information is now regarded as private. LIRs who wish to make their assignments public must make the change in MyAPNIC, or by contacting the APNIC helpdesk.

This new policy reflects growing concerns surrounding privacy in the Internet community. Similar changes are currently under discussion in the ARIN community.

Significant efforts have been made to keep the community informed of the progress of this change and to notify all LIRs by email. There may still be some temporary problems, however, as people adjust to the new system. Some downstream customers, who are not themselves members of APNIC, may have been unaware of the change and been unprepared for the removal of their public whois listings from the APNIC Whois Database.

The change also means that upstream providers who do not make their customer assignments public become the only registered contact for their customer address ranges and may experience increased correspondence about the use of this address space. LIRs should take this into account when considering whether or not to make their downstream registration information publicly available.

An FAQ page on the impact of the customer privacy policy implementation is available at:

http://www.apnic.net/info/faq/privacy-faq.html

ERX project nears completion

The four RIRs, including APNIC, are about to enter the final stage of the Early Registration Transfer (ERX) project.

This project is a coordinated effort to move whois records for address space registered before the advent of the RIRs into the whois database of the RIR in whose region the registrant is based. It has been underway for approximately six months and has already transferred a large number of early registrations to their appropriate databases.

In this final stage of the project, whois records for registrations within 192.0.0.0/8 will be moved from the ARIN database. This change will affect those people operating networks within 192.0.0.0/8 who have:

- registration information in more than one RIR database, or
- a postal address that lies outside the ARIN service region.

If this describes your situation, you will receive an email regarding your registration in the coming weeks. This will explain in which database we believe the registration is meant to reside. The message will also explain how to indicate which contact information should be recorded.

More information on the ERX project and APNIC's role in it can be found at:

http://www.apnic.net/db/erx/

Opinion: ICANN, the ITU, and Internet governance

Geoff Huston provides a perspective on the current international discussions on Internet governance. This is an edited version of an *ISP Column* article originally published online in October 2004 at http://www.potaroo.net/ispcolumn.

It may have taken some three decades to get here, but there's now no doubt that the Internet is a major public communications utility. That's hardly the most important piece of news you are likely to read today, but the implication of this public role is that there are legitimate issues of public policy to consider when looking at the broad topic of coordinating various aspects of Internet infrastructure. In other words, 'Internet governance' is a matter of significant concern to many.

In this column we will look at the various range of views about ICANN and its rationale and role over its brief history. Of course, no look at Internet governance would be complete without also looking at the role of the International Telecommunications Union (ITU) as well as the broader background to this topic.

It is a large topic and it's already been the catalyst for numerous articles. Here I'll try to be as succinct as I can!

Data networking and public networks

Whether it was because of its antecedents in the research community, or simply because it was not originally envisaged that the Internet would become a global communications platform in its own right, or for whatever set of reasons, the administration of the Internet's infrastructure was not originally crafted with conventional public network coordination in mind. The retrofitting of a model that incorporates considerations of a public utility role is proving to be a rather involved process.

For example, the original hierarchical name space for the Internet used a set of generic top level root zone names: 'edu', 'net', 'com', 'gov', and 'mil'. Adding country codes to the root of the name space was a later modification. Even then, the original country code delegations were undertaken to individuals or entities who appeared to have some form of link to the national Internet community, rather than specifically seeking out an appropriate office of the national administration of communications services as the point of delegation. Similarly, IP addresses were structured without any form of national prefix, nor were IP addresses distributed along any national lines. In these respects, the Internet was really no different to any of the other computer networking protocols of the 1980s, such as DECnet, XMS, Appletalk, or IBM's SNA, where names and addresses were defined in the limited context of the scope of the network, rather than within some broader public name framework.

There were two notable exceptions to this characterisation of computer network protocols and both were designed with a public communications utility as their primary objective, namely X.25 and OSI. Both these protocols have an indirect bearing on the current situation with the Internet. X.25 and OSI can be regarded as offerings from the data services sector of the established telephone industry. X.25, the earlier of these two protocols, had a very obvious relationship to telephony, complete with the notion of a 'call' as the means of establishing a data connection and as the unit of a transaction. The addressing scheme used a structured space that drew heavily on the telephone number structure, complete with a national prefix and nationally defined sub-fields. Like telephony there was no associated name scheme: end systems were identified by their numeric X.25 protocol address. OSI represented a later effort to design a packet switched network architecture that was intended to reflect an increasing level of experience with this technology. OSI continued to draw heavily on telephony design for the structure of the address space, and still included the concept of a call as one of its basic transactions. Much was written about OSI at the time, and it would be a diversion to explore it in depth here. However, the salient observation here is that despite the extensive effort invested into its promotion, OSI was a market failure, and whatever its technical merits it was simply not accepted by the communications industry.

OSI was supported by the ITU, and by virtue of this very active sponsorship of this technology, the implication, in the aftermath of OSI, was that the ITU was simply out of touch with data networking. It was perceived that the ITU was coming from a mindset that was incapable of engaging with either the data communications industry or the broader consumer market for data services. From the perspective of data networking the failure of OSI was seen as a failure of the ITU itself.

The ITU and the Internet

Not only was the ITU perceived as being out of touch with the data communications sector more critically, it was perceived as being incapable of making the necessary reforms to its mode of operation and policy setting to bring it back into relevance for the rapidly changing communications industry of the 1990s. The inference drawn was that the ITU was in a state of denial over progressive deregulation of national communications sectors. In many cases, the national position had moved to a position of lightweight regulation, relying on strong competitive pressures to enforce regimes of efficiency and effectiveness in the supply of communications services to consumers. The ITU, as an intergovernmental organisation, was increasingly being seen as an anachronistic relic of an earlier era of communications service provision.

It was also evident that this critical view of the ITU was most strongly held within the US, and in particular those parts of the US administration and industry that were involved with the growth of the Internet. It was perhaps no coincidence that in these growth industries of personal computer technologies and the related Internet industry, it was US enterprises that were the poster children of this new model of industry-led deregulated communications services. Their consequent rapid expansion into the massive undertaking of the global Internet was perhaps the most eloquent statement about the effectiveness of deregulation and the degree to which the previous regulatory model had simply not managed to encompass the burgeoning demand for data services in a timely fashion.

From this perspective it should be no surprise that when the transition of the IANA function – from a fully federally-funded research activity to some form of new foundational base – was being considered by the US administration, it appears that the ITU was never seriously contemplated as a viable home for this function. If the Internet was a child of deregulation and industry initiative-taking on the outcomes of research activity, then it was appropriate that the IANA function should also progress from a research context to an enterprise context. It was felt that IANA should be responsive to industry needs, and to best achieve this the IANA function itself should be undertaken as a task housed within the deregulated private enterprise sector, rather than establish yet another public bureaucracy, or use existing bureaucracies for the role. ICANN was the embodiment of this aspiration on the part of the US administration.

The formation of ICANN

Whatever the original motivation in creating ICANN to administer the IANA responsibilities, it is now apparent that ICANN was deliberately structured to confront the industry with an alternative structure of governance within national and

international communications sectors to that of the ITU. The critical difference is that ICANN has not placed governments at the forefront of visible activity, but instead placed industry needs and the operation of a competitive, deregulated international communications sector as being the major thrust of coordination activities.

As with any novel model of public policy determination, ICANN's acceptance has ranged from cautious to highly sceptical. Even within the US administration ICANN has not been 'unleashed' and it continues to operate under the terms of a Cooperative Agreement with the National Telecommunications and Information Administration of the US Department of Commerce under a sole source cooperative agreement. Formally, the US administration has not yet passed any authority to ICANN, or admitted it any true autonomy of operation. As per the US General Auditor's Office report on ICANN, ICANN continues to be an advisory body to the US National Telecommunications and Information Administration (NTIA) in the matter of functions performed by the NTIA in the administration of Internet infrastructure elements. In this light, ICANN appears to be a cautious step in a bold direction.

ICANN undertakes activities of management of Internet protocol infrastructure in the areas of the content of the root of the DNS and the identification of parties to whom are delegated administrative and operational control of the top level domains and the associated specification of terms and conditions of this delegation. ICANN, through IANA, also manages the pool of unallocated IP addresses (IPv4 and IPv6 addresses and AS numbers), and also manages the protocol parameter registries as defined by IETF Standards Actions.

ICANN MkI

The initial structure of ICANN had three supporting organisations, focusing on:

- coordination of the DNS with the Names Supporting Organization (NSO);
- coordination of address policies with the Address Supporting Organization (ASO); and
- operation of Internet protocol parameter registries with the assistance of the Protocol Supporting Organization (PSO).

The intended role of these supporting organisations was to provide a venue where interested parties could develop and consider policy proposals, leaving the task of ultimate identification of broad support for particular policy initiatives to the ICANN Board.

As has been evident to any observer of the ICANN process, things did not proceed within the parameters of that particular plan.

The PSO was placed under strong pressure to include the ITU-T and ETSI and the W3C was also enlisted, in addition to the IETF. If the objective of the PSO was oversight and policy formulation concerning the role of protocol parameter registration of IETF protocols, then this enlarged membership of the PSO was unwarranted. Even within the terms of consideration of the PSO as a source of standards-based technical advice to the ICANN Board, the presence of these additional organisations was somewhat puzzling in terms of the match of the resultant structure of the PSO to its intended role. The PSO, however, had a role in seating individuals on the Board of ICANN, and it was likely that this aspect of the PSO was the reason for the interest in broader institutional membership. Uncertainty about the extent of the role of ICANN saw many groups attempting to gain access to Board seats.

The ASO was formed within the parameters of a different model. The Regional Internet Registries had already developed a considerable history of working within their communities, and had been widely accepted by these communities as an appropriate means of coordination of activity in the role of number resource administration and distribution. The ASO was formed with membership of the associated Council based on processes determined by each RIR. Even then, it was unclear as to the relationship between the RIRs' already well-established open policy development process and the ASO and ICANN. The RIRs were unwilling to pass all regionally-developed policies to ICANN for a second round of consideration and potential alteration. They insisted that only those policies that were considered to be 'global', in that they were both common to all the RIRs and unable to be altered regionally, would be passed into this ICANN sphere.

The NSO struck problems due to the diversity of interests that were encompassed by the DNS domain, including emerging national and regional interests in the country code top level domains, the operators of the generic top level domains, the trademark and intellectual property collection of interests, the emerging industry of registrars, and the continuing interest of individuals who maintained that they had legitimacy of inclusion by virtue of their representation of interests of end users and consumers, or, to use an emerging ICANN lexicon, the 'at large' constituency.

Missing from this mosaic of diverse interests was the inclusion of various national public communications sector entities who also felt that they had clear legitimacy to undertake an active role within the ICANN policy development process. In response to this, the Government Advisory Committee (GAC) was formed.

ICANN evolution and reform

If a camel is a horse designed by a committee, then it's unclear whether ICANN was a three-humped camel or a three and three quarter-humped camel as a result of all this, but a camel it undoubtedly was.

- The PSO was dysfunctional and missing any tangible agenda of activity. A fracture was apparent in the relationship between ICANN the IETF. Attempts to create an agreement between ICANN and the IETF over the IANA function were not recognised by the US administration, who continued to insist that, formally, the IANA function for the IETF was undertaken at the behest of the US Department of Commerce rather than the IETF. This was not a view shared by the IETF.
- The ASO was accused by ICANN itself of being insufficiently 'representative' of the addressing community and the ICANN Board established its own ad hoc advisory committee on addresses and, in so doing, alienated the RIR community from the entire ICANN framework.
- The NSO was hopelessly wedged into factional-based politics.
- The GAC decided at the outset that it would operate behind closed doors, in contrast to ICANN's continuing efforts to operate in an open and transparent manner. ICANN was unable to exercise any formal control over the operators of the DNS Root Servers and a formal contract or agreement between these operators and ICANN was not looking as if it would happen any time soon.
- The 'at large' election process undertaken by ICANN appeared to be of dubious validity due to problems in establishing a reliable constituency database of individuals who had an interest in ICANN and a direct election process was attempted only once.

Not surprisingly, ICANN fell into some disarray under these pressures and, by early 2002, the CEO of ICANN at the time, Stuart Lynn, was warning all who cared to listen that ICANN was paralysed, dysfunctional, and in danger of an imminent demise.

Whether this message was directed to a fractious ICANN Board, or to the fractious set of communities that had some intersection with ICANN, or to the US administration who had been influential in determining the original ICANN structure, was not entirely clear to any observer of the process.

However, given that ICANN had been set up as an example of a new form of international coordination of communication infrastructure support activities that was based on private sector activity rather than governmental fiat, this message of imminent failure was interpreted both as a potential failure of ICANN and a sign of failure of this new model of coordination of international activity. ICANN was seen as a point of vulnerability with respect to the US administration's diplomatic efforts to reform this international activity sector. The ITU-T's activities in this same area were re-invigorated, with considerable support from national sectors who saw their national interests being potentially advantaged in a ITU-led international environment.

ICANN MkII

While still firmly positioned as a private sector activity, and while still making no concessions in the direction of the ITU, ICANN has managed to reorganise its structure through a protracted evolution and reform process.

- With respect to the ASO, the RIRs formed their own coordination entity, the Number Resource Organization, and have proposed this entity to ICANN as the means of interfacing between the addressing community and ICANN's policy development activities.
- The PSO was abolished, to be replaced by a Technical Liaison Group which, apart from its function of seating an individual on the ICANN Board, is a group without an obvious agenda.
- The NSO was forced to recognise the fundamental difference between the generic top level domains, which fall under a more direct relationship with ICANN and its processes, and the country code domains, which have, from the outset, been quite wary of ICANN. From the ICANN reform process emerged the Country Code Name Supporting Organization (CCNSO) and the Generic Names Supporting Organization (GNSO), a recognition that these two groupings are so dissimilar that they have almost nothing in common.
- In addition, an At Large Advisory Committee was formed. This was a curious move, in that the role of representing the interests of end users in international domains has traditionally been that of government, and the current role of the At Large Advisory Committee appears to be somewhat opaque to the outside observer.

Staffing of ICANN has increased significantly, as has ICANN's level of expenditure.

The reform process has had some more tangible outcomes, in that formal open meetings of the ICANN Board of Directors have managed to be progressively refined from efforts at direct dialogue and debate into highly structured events with many formalisms and appropriate quantities of ceremony.

ICANN today

Despite the effort to encompass coordination activities in the areas of names, addresses, and protocol parameters, ICANN has been largely captured by the names industry and ICANN's agenda, activity focus, and outcomes are by and large concentrated in the name domain.

In this activity, the track record of ICANN is very mixed. To its credit, it has managed to:

- dismantle the most objectionable parts of the monopoly hold over the generic top level domains;
- create an operational model that makes a clear distinction between registry operators and registrars;
- impose price and business controls on the registry operation as a means of controlling the natural tendency of the registry operation to reflect its unique position in the form of monopoly rentals; and
- assist in the creation of a global network of competitive enterprises, with the expectation that competition will instil operational and price efficiency in the registrar business.

In addition, ICANN has been successful in not only introducing new gTLDs to compete with the established brands of .com, .net, and .org, but also in moving .org and .net to new registry operations (.net is underway at the time of writing this article).

Despite these positive achievements, it is not clear that this new regime has been entirely successful.

True competition in the name space is still some way off, with the recently introduced gTLD brands failing to gain expected leverage within the market. The name market itself remains one where the role of name speculators continues to play a significant role in terms of proportion of registered names. The dominance of .com as a brand has continued.

The nature of the relationships between the IETF, ICANN, and the US administration over the protocol parameter registries remains unresolved. There is also the lingering set of concerns that if ICANN were once more to explore positioning itself on the brink of imminent demise, the collective task of picking up the pieces and continuing to support the operation of the Internet is one that appears to have an uncomfortable level of uncertainty.

The DNS Root Server operators continue to operate as an independent group. The recent moves to dramatically increase the number of DNS root servers and improve the overall robustness of DNS resolution through anycasting root servers and distributing anycast instances across the globe has been an initiative that has been well received. The fact this has occurred without any form of ICANN involvement is an interesting commentary on the ability of ICANN to engage with the operational parts of the Internet's infrastructure. Comparable activities to improve the DNS in terms of resolution services within the ICANN sphere have become protracted exercises that impose a very heavy burden on the patience of the players. The moves to introduce IPv6 AAAA records into the DNS root have been anticipated for many years, and the response to the recent ICANN announcement is, in general, of the tenor, "why didn't this happen some years ago?" The continuing frustration to get the DNS root to include DNSSEC key information continues to illustrate a perspective that the ICANN process appears to be unresponsive to technical needs and end user imperatives.

The situation today is that ICANN appears to enjoy a mixed level of success. It has managed to establish itself as a means of administering the infrastructure elements of the Internet Protocol in a manner that is reflective of the deregulated nature of the Internet industry. It has managed to reform parts of the landscape and generate an industry structure that uses open competition as the major control mechanism. ICANN has managed to bring much of the discussion about the administration of Internet infrastructure out into the open. All of these are major milestones, and it is to the credit of many dedicated individuals that ICANN has managed this impressive set of outcomes. However, it has been able to achieve all this with the continued sponsorship of the US administration, and the question of whether it can firmly establish itself in its own right in the coming years remains today perhaps a matter of hope rather than absolute certainty.

ICANN and the NRO sign MoU on the Address Supporting Organization

On October 21, 2004, the Number Resource Organization (NRO) and ICANN signed a formal Memorandum of Understanding (MoU) which specifically concerns the Address Supporting Organization (ASO). It stipulates how the NRO will fulfill the role, responsibilities, and functions of the ASO as outlined in the ICANN Bylaws. The signing ceremony took place at the ARIN XIV meeting held in Reston, USA.

For the Internet community, the new ASO MoU outlines a policy process that promotes industry self-regulation of the unallocated number resource pool (IPv4, IPv6, and AS numbers). The same policy process has been in practice for years in each of the RIRs that comprise the NRO.

“This is an important development for the global Internet community,” said Paul Wilson, NRO Chair. “The MoU fosters RIR cooperation, providing mutual benefit for the development of global policies that affect all RIR communities, while preserving the individual policy development procedures used by the various RIR communities to make their own decisions".

The ASO was originally formed in 1999 by an MoU between the RIRs and ICANN, with the purpose of reviewing and developing recommendations on number resource policy and advising the ICANN Board on these matters.

The new MoU describes a procedure for global policy development. This is a 15-step process for global policies that the RIR communities cannot ratify on their own, such as policies defining how IANA allocates address space to the RIRs. This ensures that global policies continue to be developed in the bottom-up, open, and transparent manner common to all RIR communities. The MoU does not affect how each regional community and RIR arrives at a policy position. The regional community for each RIR will continue to determine the processes used to arrive at a policy position for their region.

Another new feature of the MoU is the replacement of the members of ASO Address Council (AC) with the members of the NRO Number Council (NC). The voting scheme for the NRO NC is similar to the former voting scheme used for the ASO AC, where two members are selected by the regional policy forum of each of the RIRs. The only difference is that for the NRO NC, the Executive Board of each RIR also appoints one person from its respective region.

As was the case in the original MoU, the ASO AC will provide recommendations to the Board of ICANN about recognising new RIRs and will define procedures for selecting individuals to serve on other ICANN bodies (such as the ICANN Board). The RIRs will also continue to provide all funding for the ASO.

Full text of the new ASO MoU is available at:

http://www.nro.net/documents/aso-mou.html

More information about the NRO is available at:

http://www.nro.net

NRO comments at ICANN WSIS Workshop

The recent ICANN meeting in Cape Town, South Africa, included a panel session to discuss the newly formed Working Group on Internet Governance (WGIG). In that session, held on 1 December 2004, Paul Wilson, NRO Chair and APNIC Director General, made the following statement on behalf of the NRO.

The Regional Internet Registries have been participating in WSIS for over two years, individually and, more recently, through the Number Resource Organization, which represents RIRs globally. There are a few WSIS areas where we might like to spend our time, but the WGIG is now demanding all of our attention.

We are participating in WSIS as experts in the area of IP addressing and as supporters of ICANN. We’ve given our support not as components of ICANN, but as independent members of this broader framework of Internet administration, which ICANN itself is intended to support.

In the second round of WSIS, the RIRs will continue to play an active role, especially in the WGIG. We will continue to support ICANN, and to work with ICANN to address the genuine questions that it faces.

We feel that within WSIS, the principle issues are those of the independence and genuine internationalisation of ICANN. The NRO has called on ICANN to continue its work in this area, not by building a monolithic multinational organisation, but rather by increased cooperation and collaboration with its core stakeholders.

We’ve also called on ICANN to work with the US government to publish a genuine, unambiguous plan for its independence after the current MoU and to commit to this plan before the conclusion of the second phase of the WSIS. This is critical to provide the WSIS community with certainty as to the future form and status of ICANN after WSIS, a question which is certainly still unclear to many.

Also as a critical issue of Internet governance, the NRO rejects any concept of an alternative Internet administrative model located within any governmental or intergovernmental structure. We acknowledge fully that there is a valid role for governments in the administration of the Internet; however, this can and should be placed in the context of the current model.

Recently, the NRO posted a public response to Houlin Zhou’s memorandum on Internet governance, addressing the proposal for a national allocation scheme for IPv6 addresses. Like others, such as the Japanese Internet Governance Taskforce, we have serious and very genuine concerns about the technical and operational implications of such a scheme.

The assertion of sovereign concerns in this case is a certainly powerful and legitimate argument; however, there are mechanisms either in place now or certainly feasible, which may address the same concern with far lower risk. For the sake of the stability and security of the Internet, such solutions should certainly be explored.

Finally, in relation to the WGIG, I’d like to revisit some comments I made during the Geneva meeting last week. It seems that the definition of Internet governance, which is the first of WGIG’s tasks, is being driven by negative aspects of the Internet, as a list of 'problem areas' of the Internet. Or in other words, as a list of bugs rather than features.

P 10

The point here is that many aspects of the Internet are not being suggested as topics of governance, simply because they currently work well enough not to be on the radar. These include such things as the routing system (which is pretty stable), competition between alternate root servers (which would certainly be an issue in the absence of the concerted efforts that have been made to avoid it), and the global interoperability of all parts of the Internet (which is assumed without question, but by no means guaranteed).

I suggested to the Working Group last week that these and other aspects of the Internet must not be taken for granted and the famous principle of 'do no harm' should be borne strongly in mind. I suggested that rather than seeing Internet governance as a list of bugs, WGIG should consider features of the Internet which are to be appreciated and preserved, and include this consideration in the scope of its work. The risk of overlooking them – and this is a real risk – is to 'do harm' to the Internet, and potentially, therefore, to leave a longer list of problems for some future Working Group to solve.

Working Group on Internet Governance (WGIG) formed

On 11 November 2004, Secretary-General Kofi Annan of the United Nations announced the formation of a Working Group on Internet Governance (WGIG) to prepare for the second phase of WSIS (World Summit on the Information Society), to be held in Tunisia in November 2005.

The purpose of the group is to develop a working definition of Internet governance, to develop a common understanding about the roles and responsibilities of participants in Internet governance, and to identify public policy issues relevant to Internet governance.

The WGIG will be chaired by Nitin Desai, Special Adviser to the Secretary-General for the World Summit and includes 40 members from around the world, representing a diverse range of stakeholders, including governments, the private sector, international organisations, and civil society.

The RIRs are represented by Raúl Echeberría, the Executive Director of LACNIC, who has been selected as one of the members of WGIG. The Asia Pacific community is represented by the following WGIG members:

- Peng Hwa Ang, Dean, School of Communication, Nanyang Technological University, Singapore
- Kangsik Cheon, Chief Operating Officer, International Business Development, Netpia, Seoul
- Dev Erriah, Chairman, ICT Authority of Mauritius
- Qiheng Hu, Adviser, Science and Technology Commission, Ministry of Information Industry, China; former Vice-President, Chinese Academy of Sciences
- Rajashekar Ramaraj, Managing Director, Sify Limited, Chennai
- Masaaki Sakamaki, Director, Computer Communications Division, Ministry of Internal Affairs and Communications, Japan
- Joseph Sarr, President, NTIC Commission, Dakar Regional Council

The WGIG is expected to submit a report on its findings to the Secretary-General in July 2005. The report will then be available to the WSIS second phase in Tunis.

For more information, see:

United Nations press release:

http://www.un.org/News/Press/docs/2004/pi1620.doc.htm

WGIG web site: http://www.wgig.org

WGIG timeline: http://www.wgig.org/timeline.html

APNIC and South Asian ISP bodies sign MoUs

As part of the organisation's ongoing outreach programme, APNIC has recently signed Memoranda of Understanding (MOUs) with four of South Asia's major ISP associations: the Internet Service Provider Association of India (ISPAI), the Internet Service Provider Association of Bangladesh (ISPAB), the Internet Service Provider Association of Nepal (ISPAN), and the Internet Service Provider Association of Pakistan (ISPAK).

These agreements create closer relationships between APNIC and some of the region's key organisations. While they are non-binding, and do not entail any legal commitments from any of the parties, the MOUs will create new opportunities for members of APNIC, the four ISP Associations, and the Internet community in general.

The key areas of collaboration under these MOUs are:

- Promotion of infrastructure development and business development in the relevant region.
- Exchange of information and materials, and mutual assistance.
- Promotion of seminars, conferences, and training programs.

This means that all parties will work toward promoting and organising conferences and training programs throughout South Asia, with the aim of further developing Internet knowledge in the region.

APNIC looks forward to collaborating with these organisations for the benefit of the whole Internet community.

Secretariat update

Staff changes

Member Services Department

Tom Bounxokvan
Internet Resource Analyst

In October, APNIC welcomed a new hostmaster, Tom Bounxokvan. Born in Laos, Tom is fluent in Lao and Thai, as well as speaking some Japanese and Vietnamese. He is a recent graduate of the Queensland University of Technology, and holds a Bachelor's degree in IT and a Masters in International Economics and Finance. He has worked previously as a Windows NT network administrator and as a Lotus Notes developer.

As part of the Member Services Department, Tom will process requests for IP address space and AS number allocations within the Asia Pacific region.

Finance Department

Sudha Manian
Finance Officer

The newest addition to the APNIC team, Sudha Manian joined the Finance Department in early December. Originally from India, Sudha is now a permanent resident of Australia, and holds a Bachelor of Commerce. Before coming to Australia, she worked as an auditor in India, and has more than four years experience as an assistant accountant and accountant in Australia. She is fluent in English, Hindi, Tamil, and Telugu.

As a member of the Finance Department, Sudha's responsibilities will include assisting with accounts and billing, various reporting analysis, and providing support to the Finance Department.

Communication Department

Anne Lord
Communications Director

The most recent round of strategic planning in the APNIC Secretariat has meant a number of changes to the staff structure. The most significant of these is the creation of a new position, Communications Director, which has been filled by Anne Lord, who was previously serving as Policy Liaison Manager.

Special thanks to the following APNIC training sponsors:

REPUBLIC POLYTECHNIC

nan โทรคมนาคม CAT TELECOM

Sri Lanka Telecom

香港教育城 HKedCity

Training schedule

2005

January

- 20 Dhaka, Bangladesh
- 22 - 23 Kathmandu, Nepal (in conjunction with the APAN conference)

February

- 2 Auckland, New Zealand
- 6 - 13 Dhaka, Bangladesh (in conjunction with SANOG V)
- 16 - 25 Kyoto, Japan (in conjunction with APNIC 19/APRICOT 2005)

March

- 15 Port Moresby, Papua New Guinea
- 29 - 31 Cebu, Philippines

April

- 12 - 13 Vellore, India
- 15 Delhi, India
- TBA Fiji (In conjunction with the PITA AGM)

May

- 9 Sydney, Australia
- TBA Pakistan

June

- 13 Bangkok, Thailand
- 14 - 17 Bangkok, Thailand
- 20 Vientiane, Laos
- 22 Phnom Penh, Cambodia

The APNIC training schedule is provisional and subject to change. Please check the website for regular updates at:

www.apnic.net/training

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

training@apnic.net

Calendar

ICANN Meetings
1-5 December 2004
Cape Town, South Africa
www.icanncapetown.co.za

United States IPv6 Summit 2004
7-10 December 2004
Reston, USA
www.usipv6.com

SANOG V
11-18 January 2005
Dhaka, Bangladesh
www.sanog.org

NZNOG 3
2-4 February 2005
Hamilton, New Zealand
www.nznog.org

APNIC 19/APRICOT 2005
16-25 February 2005
Kyoto, Japan
www.2005.apricot.net

62nd IETF
6-11 March 2005
Minneapolis, USA
www.ietf.org

ICANN Meeting
4-8 April 2005
Mar del Plata, Argentina
www.icann.org/meetings

ARIN and NAv6TF Joint Meeting
17-24 April 2005
Orlando, USA
arin.net/announcements/20041122.html

RIPE 50
2-6 May 2005
Stockholm, Sweden
ripe.net/ripe/meetings

ICANN Meeting
11-15 July 2005
Luxembourg City, Luxembourg
www.icann.org/meetings

SANOG VI
16-23 July 2005
Thimphu, Bhutan
www.sanog.org

63rd IETF
31 July - 15 August 2005
Paris, France
www.ietf.org

RIPE 51
8-14 October 2005
Amsterdam, Netherlands
ripe.net/ripe/meetings

ARIN XVI
26-28 October 2005
Venue TBA
arin.net/membership/meetings

64th IETF
6-11 November 2005
Canada, Venue TBA
www.ietf.org

ICANN Meeting
5-9 December 2005
North America, Venue TBA
www.icann.org/meetings

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
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

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

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

Member Services Helpdesk

helpdesk@apnic.net

www.apnic.net/helpdesk

☎ +61 7 3858 3188

+61 7 3858 3199

APNIC

Communicate with APNIC via 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

For more information on MyAPNIC's features, see:

www.apnic.net/services/myapnic