APNIC

Apster

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

Issue 22 - June 2007

Root nameserver deployed in Fiji

A mirror of Internet F-root server went live in Suva, Fiji on 25 May 2007.

This is the first root nameserver to be deployed in the Pacific islands. It will bring significant improvements in speed and reliability to Internet users in the region.

Root servers are a critical part of the Internet's Domain Name System (DNS), providing information about the authoritative servers for the many top-level domains (such as .com, .org, .fj and .tv).

This deployment in Fiji brings the total number of root DNS servers in the Asia Pacific region to 35.

Geographic isolation and poor funding have posed challenges for implementing communications technologies in the Pacific. However, Internet development in the region has also been characterised by co-operation between government, business and the global community. This project was no exception.

APNIC has coordinated this deployment with Internet Systems Consortium (ISC) and the University of the South Pacific (USP).

ISC is a non-profit public benefit corporation responsible for implementing and supporting F-root operations. ISC also operates a DNS crisis centre, and has a long history of developing and maintaining quality open source software BIND and DHCP.

Joao Damas, ISC F-root Programme Manager, said, "ISC has been involved in a global effort to bring resilient and dependable DNS services to a new level. F-root anycast deployment is, together with our TLD hosting service, a part of that effort. Collaboration with APNIC and local agents has been crucial to enable delivery and it is with great joy that with the installation in Fiji we see a DNS root server present for the first time in the Pacific island states, servicing various communities in the region."

USP has 14 campuses spread over 12 islands in the Pacific region. USP provided a dedicated rack, a 24-hour backup electricity supply and a secure environment for the installation.

Simon Greaves, USP Systems & Networks Manager, said they were "very enthusiastic about hosting an F-root server here at the University of the South Pacific. The combination of our high-speed Internet connection and VSAT connections to 11 other Pacific Island countries uniquely places us to extend the benefits of the F-root server to the region."

Paul Wilson, Director General of APNIC, added, "The deployment of this root nameserver in Fiji is a positive example of Internet community coordination. The installation has involved the not-for-profit organisations and educational institutions working together to improve DNS stability and Internet response times for developing economies in the Pacific".

◀ This map shows the location of root servers in the Asia Pacific region. The latest installation in Suva, Fiji, brings the total to 35.

24th APNIC Open Policy Meeting

29 August - 7 September 2007 New Delhi - INDIA

FOSS network and security book released

The International Open Source Network (IOSN) has released a new book intended as reference for anyone interested in network administration and security.

The book, Free/Open Source Software: Network Infrastructure and Security, is written by Gaurab Raj Upadhaya. Gaurab is well known in the Asia Pacific community as a frequent tutor and speaker at APNIC meetings. Gaurab is employed as an analyst and engineer at Packet Clearing House, and was a founder of the Nepal Internet Exchange (NpIX). He is also Chair of SANOG.

The Free/Open Source Software (FOSS) movement is shaped by networked information environments, and also greatly influences these networks.

Free/Open Source Software: Network Infrastructure and Security introduces readers to network concepts and architectures. It also discusses network security functions with FOSS, including security best practice, and checklists.

The book addresses a community need to inexpensively minimise security and other risks that accompany the benefits of networks. Being able to respond to risks demands a high level of network design and maintenance, making developing countries particularly vulnerable. Because of its high degree of flexibility, free/open source software (FOSS) provides cost savings and is an excellent platform for implementing these critical requirements.

The book also contains useful tips for network planning, design and development, and provides information to help diagnose and solve problems that occur while running a network. This is especially helpful for network managers who are thinking about setting up, or have already set up, a network using FOSS.

Free/Open Source Software: Network Infrastructure and Security is part of the IOSN's Free/Open Source Software e-Primer Series. The IOSN is an initiative of the UNDP Asia-Pacific Development Information Programme, with support from the International Development Research Centre (IDRC) Canada.

Free/Open Source Software: Network Infrastructure and Security is available as a free download in PDF from:

http://www.iosn.net/publications/network/foss-network-primer

APNIC 23 policy update

Six policy proposals were discussed at APNIC 23 in Bali, Indonesia. However, no proposals reached consensus. The following four proposals have been returned to the Policy SIG mailing list for further discussion:

- prop-037: Deprecation of email updates for APNIC Registry
- prop-042: Proposal to change IPv6 initial allocation criteria
- prop-043: Proposal to remove reference to IPv6 policy document as an "interim" policy document
- prop-046: IPv4 countdown policy proposal

The following two proposals were abandoned:

- prop-044: Proposal to remove requirement to document need for multiple /48s assigned to a single end site
- prop-045: Proposal to modify "end site" definition and allow end sites to receive IPv6 allocations

A seventh policy proposal, prop-047: eGLOP multicast address assignments, was submitted after the deadline for policy proposals to be discussed at APNIC 23. Therefore, this proposal was presented as an informational presentation at APNIC 23. At APNIC 24, the community will decide whether to adopt, modify, or abandon prop-047.

For more information on APNIC 23 policy proposals, please see:

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

Study reveals spam attack risk factors

A recent study has revealed that email addresses published on websites attract 70% of spam.

In his paper entitled 'The Impact that Placing Email Addresses on the Internet has on the Receipt of Spam - An Empirical Analysis', Guido Schryen, from RWTH Aachen University, also notes that email addresses placed on newsgroups receive around 28% of spam, and email addresses subscribed to newsletters attract only around 1.4% of spam.

The findings also indicate that more than 43% of email addresses on the web, 27% on newsgroups and 4% of email addresses subscribed to newsletters have been subjected to a spam attack.

According to Schryen, these results highlight the importance of protecting email addresses through obscuration.

To access this paper, which includes a discussion of various obscuration techniques, please visit the Social Science Research Network website:

http://papers.ssrn.com

APRICOT update

APRICOT 2008 will be held in conjunction with APNIC 25 in Taipei, Taiwan, from 20 – 29 February 2008.

APRICOT is the leading operational forum in the Asia Pacific region, facilitating knowledge sharing among key Internet leaders in the region and worldwide.

During the coming months, *Apster* will feature regular updates from the APRICOT 2008 hosts, TWNIC (Taiwan Network Information Center).

The sponsorship program and other meeting details are already available on APRICOT's website.

For more information please see:

http://www.apricot2008.net

Stay tuned for future updates!

PDs rock APRICOT 2007

Musical group Packet Droppers (PDs) treated attendees at the APRICOT 2007 farewell dinner to a performance. The band leader, Tom Vest, said the group was born in Kyoto at APRICOT 2005, following an impromptu "all-geek jam session". "

Several band members later practiced together during NANOG 35, NZNOG 2006 and NZNOG 2007. However, getting enough members in the same place at the same time was difficult.

Their next opportunity to meet was in Bali at APRICOT 2007. PDs spent several nights playing informally in various hotel rooms, on the beach, and at a Westin Hotel bar. Band member Garin Ganis then secretly arranged for the band to perform at the APRICOT 2007 farewell dinner. The rest of the band only found out that they would be performing on the morning of the gig. However, the PDs members were undaunted and, said Tom, "rose to the occasion, working up a short set of rock standards during a couple of intensive, last minute practice sessions. Without Garin's leadership, Packet Droppers would almost certainly still be languishing in obscurity rather than basking in the current hot glow of international geek stardom."

A band website featuring pictures and videos from 2007 and details on future performances is coming soon.

▲ From left to right: Ole Jacobsen, IB Putra, Jonny Martin, Desiree Miloshevic, Tom Vest, Mathew Pounsett, Garin Ganis, Vicky Shrestha, Wahyoe Prawoto

index

More ROAP – Routing and addressing at IETF68

Geoff Huston

Over the past year or so there has been a heightened level of interest in the topic of Internet routing and addressing. The continued intense examination of the IPv6 protocol, and the associated speculation regarding the future role of the Internet, raises the possibility of the Internet supporting a world of tens or hundreds of billions of chattering devices. What does such a future imply in terms of the core technologies of the Internet? Does what we use right now scale into such a possible tomorrow?

Consideration of this topic has prompted a critical examination of aspects of the architecture of the Internet, including the scaling properties of routing systems, the forms of interdependence between addressing plans and routing, and the roles of addresses within the architecture. The IAB has been active in facilitating discussion of this topic, both in the IETF and in various Internet operational gatherings around the world. This IAB effort culminated in a two day workshop on routing and addressing in October 2006 to examine the characteristics of this space and to start identifying some of the interdependencies that appear to exist here. (The workshop report is close to completion, and there is also the author's informal report of impressions gained at the workshop).

IETF68 saw some further steps in analysing these issues, and during the week there was a plenary session on routing and addressing, and meetings of the Internet and Routing Areas devoted to aspects of routing and addressing. This is a report of these sessions, and some conjecture as to what lies ahead along this path.

Plenary ROAP - The plenary session on routing and addressing

The plenary session at IETF68 presented an overview of the topic, looking at the previous initiatives in routing and addressing as well as providing some perspectives on the current status of work in this area. Routing and addressing, in the context of the Internet, has been visited on a number of occasions over the years; starting with the shift from the original 8/24 network and host part addressing to the Class A, B and C addressing structures, and the subsequent shift to the prefix-plus-length concepts of classless addressing. In the routing area there was the adoption of a peer model of routing with the introduction of BGP and the shift in BGP to support classless addressing in the form of CIDR. And, of course, there has been the design of IPv6. However, there still remains the concern that this is not completed work, and that the technology is not in an ideal state to scale by further orders of magnitude without further refinement. There are concerns over the scalability of routing, the 'transparency" of the network, renumbering issues, provider-based addressing and provider lock-in, service and traffic engineering and routing capabilities, to name but a few issues that are relevant and challenging today, and appear to be even more so for the Internet of tomorrow.

Are there architectural principles that are relevant here? In the large, diverse, but coupled set of networks that collectively define the Internet, it appears that each component network should operate within a general principle of containment or insulation of impact. The principle is that each network should be able to implement reasonable choices in their local configuration without undue impact on the operation or range of choices available to all other networks. In other words, each network should be able to make such local configuration choices relatively independently of the choices made by any other network. The relevant issue here is balancing this principle against the operation of the network as a whole, which can be seen as a binding of networks together as a coherent entity, supporting consistent and robust communications paths through this collection of networks.

We do not use a routing technology that effectively isolates individual network elements from each other, or even manages to localise the external impacts of local choices. On the contrary, far from being a protocol that damps instability, BGP manages to be a highly effective amplifier of noise components of routing events. So, while it is a remarkably useful information dissemination protocol with considerable flexibility, the properties of BGP in an ever-more connected world with ever-finer granularity of information raises some questions about its scaling properties. Will the imposed 'noise' of the protocol's behaviour completely swamp the underlying information content? Will we need to deploy significantly larger routers to support a much larger routing protocol load, but route across a network of much the same size as today's network?

There is a prospect that routing may become far less efficient; because as we increase the degree of interconnection and the information load simultaneously, the inability to insulate network elements from each other and effectively localise information creates a disproportionately higher load in network routing.

In addition, there is the continuing suspicion that the semantic load of addresses in the Internet architecture, where an address conveys simultaneously the concepts of "who", "where" and "how" has some side-effects that cause complexity to other aspects of the network, including routing complexity. To what extent can the semantic intent of endpoint identity (or "id") be pulled apart from the semantic intent of network location and forwarding lookup token (or "loc"), is a question of considerable interest. While the current IP address semantics remove the need to support an explicit mapping operation between identity and location, the cost lies in the inability to support an address plan that is cleanly aligned to network topology, and the inability to cleanly support functionality associated with device or network mobility. In the end, it's the routing system that carries the consequent load here. The questions in this area include an evaluation of the extent to which identity can be separated from location, and the impact of such a measure on the operation of applications. How much of today's Internet architecture would be impacted by such a change, and what would be the resultant benefits if this were to be deployed? Would the benefits of such a deployment be realised directly by those actors who would be carrying the costs? Is deployment a complete and disruptive phase shift in the Internet, or are there mechanisms that support incremental deployment? Are we looking at one single model of such an id/loc split, or should we think about this in a more general manner with a number of potential id/loc splits?

As well as consideration of these general architectural principles and their application in routing and addressing, there are also more specific sets of objectives that relate to Internet actors. For users there are objectives here about maximising the user's service and provider choices without cost escalation. For service providers there are the objectives of using cost-effective technologies that can accommodate a broad diversity of both current and projected business needs, as well as the very real need to maximise the value of existing investments in plant and operational capability.

Behind this is the observation that the routing and addressing space is not infinitely flexible, and, on the contrary, form a highly constrained space. Part of the motivation behind the id/loc splits is to take some of the inflexibility of the id part of an address, where persistence is a key attribute, and remove that from the locator part of an address. In split id/loc terms a mobile device is one that maintains a constant identity but changes locators. Multi-homing can be expressed in id/loc terms as a single identity simultaneously associated with two or more locators. Traffic

engineering can be expressed in terms of locator attributes without reference to identifiers, and so on.

Obviously the study of this topic of routing and addressing, and the related aspects of name space attributes and mapping and binding properties, is one with a very broad scope. The larger question posed here is whether this is an issue where resolution can be deferred to a comfortably distant future, or whether we are seeing some of these issues impact on the network of the here and now. Are we accelerating towards some form of near-term technical limit that will cause a significant disruptive event within the deployed Internet, and will volume-based networks economics hold, or will bigger networks start to experience disproportionate cost bloat or worse? Is it time to become alarmed? Well, there is the certainty of exhaustion of the unallocated IPv4 address pool in the coming years, but this sense of alarm in routing and addressing is more about whether there are real limits in the near future over the capability to continue to route the Internet within the deployed platform, using current technologies, and working within current cost performance relationships, irrespective of whether the addresses in the packet headers are 32 or 128 bits in size.

There was a strong sense of "Don't Panic!" in the plenary presentation, with the relatively confident expectation that BGP will be able to carry the Internet's routing load over the next three to five years without the need for major protocol surgery, and that Moore's Law would continue to ensure that the capacity and speed of hardware would track the anticipated growth rates. There was the expectation that the current technologies and cost performance parameters would continue to prevail in this timeframe. However, the subsequent plenary discussion exposed the viewpoint that such a prediction does not imply cause for complacency, and some sense of urgency is warranted given the criticality of this topic, the high level of uncertainty when looking at even near term growth prospects, and the ease with which this industry adopts a comprehensive state of denial over pending events, irrespective of their potential severity.

What we are up against as we consider these objectives as they relate to a future Internet is the relentless expansion of the network. Today the Internet sits in an order of size of dimension of around 109. There are some 1.6 x 109 routed addresses in the Internet and an estimate of between 108 and 109 attached devices. If we look out as far as four decades to around 2050 we may be looking at between 1011 to 1014 connected devices. (Yes, there's a large uncertainty factor in such projections!) Can we take the Internet along such a trajectory from where we are today? And if that's the objective, then how can we phrase our objectives over the next five years as steps along this longer-term path?

The immediate steps at the IESG level have been to take the IAB's initiative and work with a focus group, the Routing and Addressing Problem Directorate (ROAP), to refine the broad space into a number of more specific work areas, or "problem statements", and undertake a role of coordination and communication across the related IETF activities. In addition, as there is a relatively significant research agenda posed by such long term questions, the Routing Research Group of the IRTF has been rechartered and, judging by the participation at its most recent meeting just prior to IETF68, effectively reinvigorated, to investigate various approaches to routing that take us well beyond tweaking the existing routing toolset.

Internet ROAP – The Internet area meeting

The Internet area meeting concentrated on aspects of this approach of supporting an identifier / locator split within the architecture of the Internet, and, specifically, at the internetworking layer of the protocol stack, and gathering some understanding as to whether this approach would assist with routing scaling. One of the key considerations in this area is working through what could be called boundary conditions of the study. For example, is this purely a matter for protocol stacks within an endpoint, or are distributed approaches that have active elements within the network also part of the consideration? To what extent should a study consider mobility, traffic engineering, NATs and MTU behaviour? What appears to be clear at the outset is that this is not a 'clean slate' network. Any approach should be deployable on the existing infrastructure, use capability negotiation to trigger behaviours so that deployment can be incremental and piecemeal, allow existing applications and their identity referential models to operate with no changes, and, hopefully, have a direct benefit to those parties who decide to deploy the technology.

From the routing perspective the overall desire is to reduce the growth rates of the inter-domain routing space. The desired intent is to reduce the amount of information associated with locators, so that locators reflect primarily network topology in such a way that the locators can be efficiently aggregated within the routing system that attempts to maintain a highly stable view of the network's topology.

The resultant system must be able to express, in routing terms, most of the flexibility we see in today's system, perhaps on a more ubiquitous scale. This includes site multi-homing across multiple providers, ease of provider switching and locator renumbering (assuming that locators may include some provider-based hierarchy), support for mobility, roaming and traffic engineering, and allowing for session resilience across various locator switch events. In and of itself these objectives form a challenging set, but it's not the complete set of objectives. In addition, it is necessary that these outcomes are achieved within tight cost constraints and volume economics that allow for scaling without disproportionate cost escalation. Of course, such systems should be resilient to various known (and currently unknown) forms of hostile attack.

Today's system uses two critical mapping databases to support the discovery of the binding between identifiers and addresses. The Domain Name System (DNS) is used to map between a human-oriented name space used at the application level (domain names) and IP addresses, and the routing database in each router is used to map from addresses to particular local forwarding decisions (the forwarding mapping from the RIB to the FIB data structures). The current mapping system assumes stable endpoints with simple resource requirements and rudimentary security.

When we consider in further detail the implications of disambiguating aspects of identity from those of network location, there are a number of dimensions to such a study, including the structure of the spaces, the mapping functions, and the practicalities of any form of deployment of such a technology.

The first of these topics is the desired properties and structure of these distinct identification and locator spaces. Should the identity space be a 'flat' space of token values, or use some internal structure within the token that matches some distribution hierarchy? Is "identity" something that is embedded into a device at the point of manufacture (such as IEEE-48 MAC addresses), or at the point of deployment (such as Domain Names)? Is uniqueness a statistically likely outcome or one that is assured though the structure of the token space? Are there properties of the identity space that aid or hinder the security properties of the use functions in terms of mapping and referral operations? Is there necessarily one identifier space or potentially many such spaces? There are similar questions about a dedicated locator space, particularly relating to the time and space properties of locator tokens.

The next critical topic appears to be how an identity mapping function relates to the forwarding mapping function. Assuming that existing name spaces remain unaltered, then the resultant framework appears to require distinct 'name' to 'identifier' mappings, 'identifier' to 'locator' mappings and 'locator to forwarding' mappings. It remains undefined at this point where these mapping functions should be performed, who should perform these functions, when they should be performed and the duration of the validity of the outcomes. Also yet to be defined are whether the mapping function outcomes are relative or universal, the scope and level of granularity in time and space of the map elements, the security of these mapping functions, and whether there is a simple operation in each mapping function or multiple operations.

P 6

There is also the issue of whether the mapping is explicit or implicit, what evidence of a previous mapping operation is held in a packet in a visible manner, and what is occluded from further inspection once the mapping operation has been performed. What level of state is required in each host, is there true end-to-end transparency and at what level? To illustrate some of the dimensions here, a particular approach to an identifier/locator split could see identifiers in the role of the end-to-end-tokens that are used by upper levels of the protocol stack. Where identifiers would be preserved in such a manner that both parties to a packet exchange use the same identifier pair for each transmitted packet, while locators would have a more elastic intent, and various identifier-to-locator and even locator-to-locator mappings could be performed while the packet is in transit. Another approach would take a more constrained view of locators, and attempt to protect the initial locator value in such a way that any attempts to alter this value during transit would be detected and discarded by the receiver.

The other aspect to consider here is what one presentation termed the "Incentive structure", where it was advocated that the most effective incentives are those where local change is performed as a means of alleviating local 'pain'. This would indicate that routing scalability is predominately a concern of service providers, whereas host mobility and service multi-homing and session resilience are matters of concern to the host and service provider and consumer. Its also useful in an incentive structure that benefit is realized unilaterally, in that one party's efforts at deployment provide local benefit to that party without regard to the actions of others, so that the problems of initial deployer penalties and lock-stepping are avoided.

It is likely, at least at this stage of the study, that there are a diversity of approaches to such a split, both in the intended roles of identifier and location tokens, and in their means of binding. Already in the HIP and SHIM6 approaches we've seen a difference of approach, where the SHIM6 approaches co-opts locators as identifiers on a per-host-pair basis, while the HIP approach uses a persistent identity value that cannot assume the role of a locator. The expectation at this stage of the study is that further ideas will surface here, and such ideas are helpful rather than distracting. It is unclear if a single solution can emerge from this activity, or whether different actors have a sufficiently different set of relative priorities that multiple approaches (each of which express different prioritization of functionality) are viable longer-term outcomes.

The critical consideration here is that it is unlikely that scaling routing over the longer term to very much larger networks is simply a matter of just changing the operation of the routing system itself. Real leverage in this area appears to also require an understanding of the meaning of the objects, or 'addresses' that are being passed within the routing system. The motivation for opening up the identifier/ locator space within the Internet area appear to be strongly tied to the notion that if you can unburden some of the roles of the addresses used in routing, and treat these routed tokens as unadorned network locality tokens, then you gain some additional capability in routing. The intended outcomes include being able to group 'equivalent' locators together, and thereby reduce the number of elements being passed within the routing system, ensure that the locator set readily maps into local forwarding actions and also, hopefully, reduce the amount of dynamic change that is propagated in routing. It would also be useful if such an approach facilitates traffic engineering, site multi-homing, various forms of mobility and roaming. It might also be possible to remove from the application's end-to-end model the consideration of not just endpoint locality but also the tokens used in the transport protocol, proving a different approach to IPv4 and IPv6 interoperability.

At this juncture there is no unity or even clarity of exact requirements or system design, let alone solutions for this work. The exploration of the inter-dependencies of mapping functions, the properties of identity and locator spaces, and the ways in which mapping functions can be supported in this environment is still at an early stage.

Routing ROAP – The Routing area meeting

The last of these ROAP sessions in IETF68 was that of the Routing area.

The first part of the Routing ROAP session looked at the trends in the routing system over 2005 and 2006. The overall trend appears to be a system that is increasingly densely interconnected; carrying more information elements, each of which expresses finer levels of granularity in reachability. As an example of some of the relativities here, it was reported that the amount of address space advertised in 2006 increased by 12% from January 2006 to December 2006, while the number of advertised ASNs increased by 13%, and the number of advertised prefixes increased by 17% over the same period. The report also considered the dynamic behaviour of the routing space, looking at various distributions of the 90 million prefix updates that were recorded for the year. One of the major aspects of BGP updates in both 2005 and 2006 is the skewed distribution of updates. In 2006, 10% of the announced prefixes were the subject of 60% of the BGP updates, and 60% of the announced prefixes generated just 10% of all updates. Looking at some known control prefixes, it appears that BGP appears to be an effective noise amplifier, where a single origin event can generate up to 11 updates at the measurement point.

There appears to be two forms of dynamic BGP load: the BGP "supernovas" that burst with an intense BGP update load over some weeks and then disappear, and "background radiation" generators that appear to be unstable at a steady update rate for months or even an entire year.

In looking at scaling the BGP routing environment, it appears that one form of approach is to look in further detail at this subset of prefixes and ASNs that are associated with the overall majority of BGP updates. One approach is to investigate whether damping of unstable prefixes in some fashion, or detecting routing instability that is an artefact of origination withdrawal, or deployment of propagation controls on advertisements, would be effective in reducing the overall dynamic load of BGP updates. This approach represents a behavioural change in local instances of BGP that reduce the potential for unnecessary updates to be propagated beyond a "need-to-know-now" radius. Another approach is to consider changes to BGP in terms of additional attributes to BGP updates, such as "withdrawal-at-origin" flag, or selective advertisement of "next best path", both of which are intended to limit the span of advertised intermediate transitions while the BGP distance vector algorithm converges to a stable state.

Again, the considerations of deployment were noted, where the Internet's routing system is now a large system with considerable inertia. The implication is that any change to the routing system needs to use mechanisms that allow for piecemeal incremental deployment, and where incremental benefit is realised by those who deploy. One potential case study of such a change is the 4-Byte ASN deployment.

It appears that we could improve our understanding of the operational profile of the routing space, particularly by looking at the various forms of pathological routing behaviours and comparing these against the observations of known control points. Such a study may also lead to some more effective models of projections of the size of the routing space in the near and medium-term future, and allow some level of quantification as to what "scaling of the routing space" actually implies.

The second part of the Routing ROAP session took a look at the current status of the routing world, updating some of the observations made at the IAB Routing Workshop, and outlining some further perspectives on this space.

One critical perspective on BGP is the behaviour of BGP under load. BGP uses TCP as its transport protocol. This is a flow-controlled protocol, where the sender must await an advertisement of reception capability from the receiver (an advertised "window") before being able to send data. When this session is uncongested a BGP speaker will send updates as fast as they are locally generated (depending on the

Minimum Route Advertisement Interval (MRAI) timer). When the transmission is congested a local send buffer will form. Unlike conventional applications that treat TCP as a simple black box, most deployed BGP implementations use state compression on the advertisement queues (as a simple example, the queuing of a withdrawal should remove any already queued but as yet unsent updates for this prefix). This state compression of the advertisement queue should be on a peer-by-peer basis, so that a congested BGP peer does not slow down an uncongested peer. The implication is that the load characteristics of BGP alter as the load level increases, and BGP attempts to ensure that its peer only receives the latest state information when the peer signals (via TCP flow control) that it is not keeping pace with the update rate.

Another critical factor is the nature of "convergence" in BGP. Convergence is at least an O(n) sized issue, where n is the number of discrete routing entries. This may appear daunting, but the real question is: How important is convergence? The presentation included the claim that this was BGP's biggest, yet least important, problem. Convergence delays can be mitigated by graceful restart, non-stop routing, and fast re-route. One of the measures that exacerbates convergence is the use of Route Reflectors. Their model of information hiding is intended to reduce the number of BGP peer sessions and the update load, but the benefits they achieve are at the cost of slower convergence with a higher message rate during the intermediate state transitions. Perhaps it is appropriate to consider small scale changes to BGP behaviour, to mitigate the transient BGP update bursts caused by path hunting, including those already mentioned of "withdrawal-at-origin" notification and propagation of backup paths.

One approach is to take the current set of potential tools that are proposed to addresses or mitigate various BGP pathologies, and prune this set, by looking at those that align cost and benefit in deployment, allow piecemeal incremental deployment, and have beneficial changes on the load properties of BGP.

The approach advocated here is based on the perspective that BGP is not in danger of imminent collapse, and there is still considerable "headroom" for BGP operation in today's Internet. This allows the IDR Working Group of the IETF to focus on measures that include tools and behaviours that tweak the current behaviour of BGP in ways that could mitigate some of the more excessive behaviours of BGP; and allows the Routing Research Group the latitude to study the broader topics of fundamental changes that may be associated with novel routing and addressing architectures.

More ROAP?

So is there some urgency here in looking at this problem? It's not clear that the problem is pressing, in that it is likely that the Internet will still be around tomorrow and probably the day after tomorrow as well. However, like many other issues where there are complex feedback loops with internal amplification factors, it may not be apparent that there is a near-term problem with the health of the routing system until such time as the problems have already surfaced. By then, dire warnings of impending trouble are just too late! Also, by that stage there is not enough time to think about the various approaches to the space and the relative drawbacks and merits of each, as the pressure to simply deploy any measure to mitigate the issue is overwhelming.

The routing space is a classic example of the commons, where each party is at liberty to generate as many or as few routing entries as they see fit, and is also free to adjust these entries as often as they see fit. This allows each party to use routing to solve a multitude of business issues, including, for example: Using routing to perform load balancing of traffic over a set of transit providers, using a 'spot market' in Internet transit services, creating differentiated transit offerings using more specific routes and selective advertisements. The ultimate cost of these local efforts in optimising business outcomes through loading of the routing system is not necessarily a cost that is imposed back on the originating party. The ultimate cost lies in the increasing bloat in the routing system, and the consequent escalation in costs across the entire network in supporting the routing system. There are no "routing police"; nor is there a "routing market". There is no way to impose administrative controls on the global routing system, nor have we been able to devise a economic model of routing where the incremental costs of local routing decisions are visible to the originator as true economic costs for the business, and the benefit of a conservative and prudent use of the routing system reaps economic dividends in terms of relatively lower costs for the business. Like the commons, there are no effective feedback mechanisms to impose constraint on actors in the routing space, and, also like the commons, there is the distinct risk that the cumulative effect of local actions in routing creates a situation that pushes the routing system, either as a whole or in various locales, into a non-functioning state.

It appears that there are a number of avenues of approach here in attempting to place some constraints on the potential expansion of the routing system. What is less than clear is the ultimate value of such approaches in the context of the future Internet. Is making a functionally richer endpoint protocol stack a course of action that sits comfortably within a world of communicating RFID labels? Is the lack of a routing market and an associated routing economy such a fundamental weakness that no technical efforts to alleviate the situation can gain traction in a world dominated by the desire to perform local optimisations in the cheapest possible manner? Have we already constructed a massive multi-trillion dollar industry that now uses business models that assume particular routing behaviours, and would efforts to alter those behaviours simply founder because of trenchant resistance to change in the business models within the communications industry?

Whether a sense of urgency is required to motivate the work, or a sense that there can and should be a better way to plan a future than crude crisis management, the underlying observation is that the routing and address world is fundamental to tomorrow's Internet. Unless we make a concerted effort to understand the various inter-dependencies and feedback systems that exist in the current environment, and understand the interdependences that exist between network behaviours and routing and addressing models, then I'm afraid that the true potential of the Internet will always lie within our vision, but frustratingly just beyond our grasp.

Yes, more ROAP please!

Further reading

This is the set of references to further material on this topic, as presented in the plenary session.

http://www.ietf.org/internet-drafts/draft-iab-raws-report-02.txt

http://submission.apricot.net/chatter07/slides/future_of_routing/apia-future-routing-john-scudder.pdf

http://submission.apricot.net/chatter07/slides/future_of_routing/apia-future-routing-jari-arkko.pdf

http://www3.ietf.org/proceedings/07mar/slides/plenaryw-3.pdf

http://www3.ietf.org/proceedings/07mar/agenda/intarea.txt

http://www3.ietf.org/proceedings/07mar/agenda/rtgarea.txt

http://www1.tools.ietf.org/group/irtf/trac/wiki/RRG

http://www.ietf.org/IESG/content/radir.html

Analysis of IPv4 consumption in the AfriNIC region

Apster has recently featured several articles on IPv4 consumption. This article, by AfriNIC CEO Adiel Akplogan and Alain Patrick, is an analysis of future consumption of the IANA IPv4 central pool, and its impact on the AfriNIC region. The article examines the topic from the perspective of the developing Internet community of Africa, and is published with the kind permission of AfriNIC.

For some years now, studies have attempted to assess the dates of exhaustion of the IPv4 central pool at the level of IANA and the Regional Internet Registries. Geoff Huston's studies, for instance (published on http://www.potaroo.net/tools/ipv4), project that the exhaustion of the IANA pool of addresses will occur around 25 July 2011. (As at 27 February 2007 at 7:59 UTC +10. The website computes possible dates for the pool exhaustion in relation to IANA and RIR allocations in real time).

In light of this and other information available, there is undeniable concern among IP network operators, who ask questions such as: What will the situation be at the estimated date if operators cannot obtain public IPv4 addresses? Should there be reserves for addresses locally at the RIR level and/or even at the IANA level to cater for the most urgent needs?

Faced with such questions, operators in the APNIC region proposed a policy that plans to coordinate aspects of the exhaustion of the IPv4 central pool (http://www.apnic.net/policy/proposals/prop-046-v001.html). However, beyond this, there are still concerns about IPv4 consumption that have not been raised or addressed by the community; especially in regions where the Internet is still to expand, such as Africa and Latin America (under the management of AfriNIC and LACNIC respectively). Some of these questions are:

- What can the "small" registries (like AfriNIC) do to ensure their communities can continue to access IPv4 addresses when the IANA pool is exhausted?
- What will Internet number resource management look like after the exhaustion of the central IANA and AfriNIC pools?
- What about the IPv6 solution?

The objective of this document is to review different issues based on data for the African region, and to set up foundations for some solutions whilst leaving the discussion open for community contribution.

It is quite possible that, with the exhaustion of the IPv4 address pool, a black market will develop, with its law of supply and demand, and will not be favourable to ISPs in emerging regions.

Also, it is quite obvious that the natural deployment of IPv6 in African communities will be difficult, despite measures taken to encourage it.

Analysis of the situation

We have chosen to analyse the allocation of IPv4 addresses by AfriNIC to answer the questions raised above in the context of the AfriNIC community. This is in order to make projections on the final exhaustion of the AfriNIC pool following exhaustion of the IANA pool, and to prepare to manage this predicament.

In order to do this we have analysed allocations made from the prefix 41/8 (allocated to AfriNIC in April 2005 by IANA), which has been in use since 1 February 2006. We have analysed allocations over a period of 12 months (1 February 2006 to 1 February 2007), to determine the rate of consumption and make projections (Figure 1).

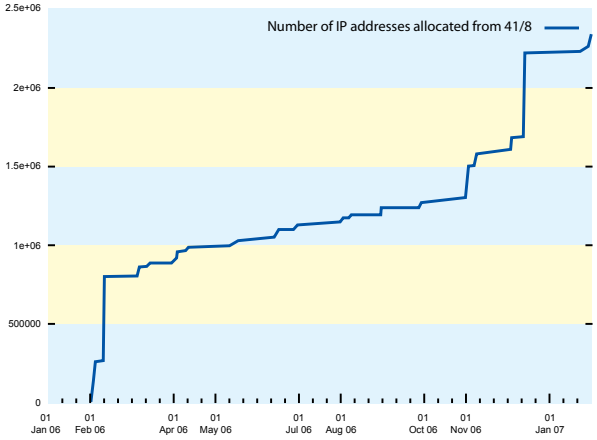


Figure 1: Number of IP addresses allocated from 1 January 2006 to 1 February 2007

In order to study the model used to analyse the allocations, we represented the data in a logarithmic scale (Figure 2). The period from 9 April 2006 to 1 November 2006 (211 days) shows a linear behaviour, indicating exponential growth.

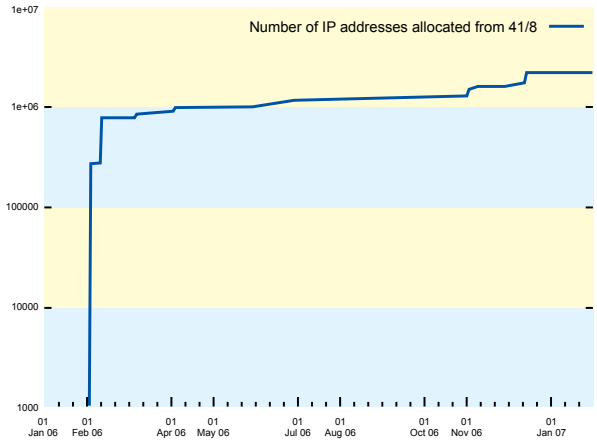


Figure 2: Number of IP addresses allocated from 41/8 (logs-scale format)

The instantaneous growth rate of allocations, derived from the formula X (t) =X0ekt, is 0.29%. The rest of the graph shows a similar behaviour. A way of modeling the global evolution is to extend the exponential model in the remaining period (from 2 November 2006 to 1 February 2007), 302 days in total.

Figure 3 represents the real data, and the data obtained using our model. The result on 1 February 2007 on both graphs reassures us about the accuracy of our model. We can use it to make projections on the following dates:

- Date of qualification for a new /8 from IANA (50% of utilisation of the actual block)
- Date of exhaustion of the 41/8 block

As previously mentioned, we first study the hypothesis of the constancy of conditions and actual rates of allocation. The model shows that AfriNIC will be at 50% utilisation of the 41/8 block, (8,388,608 IP addresses) at around 22 April 2008. This is the date at which AfriNIC will qualify to receive a new /8 from IANA. See Figure 4.

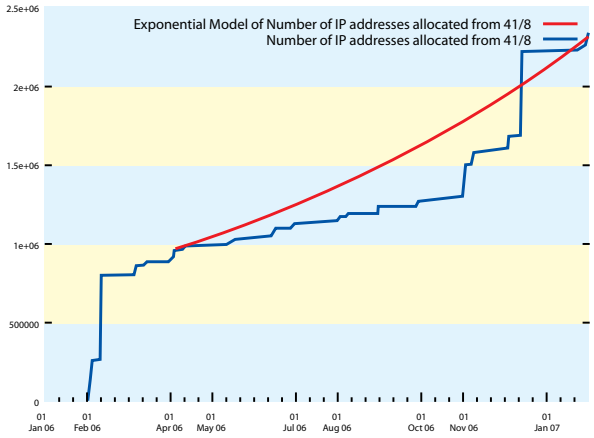


Figure 3: Exponential model of number of IP addresses allocated from 41/8

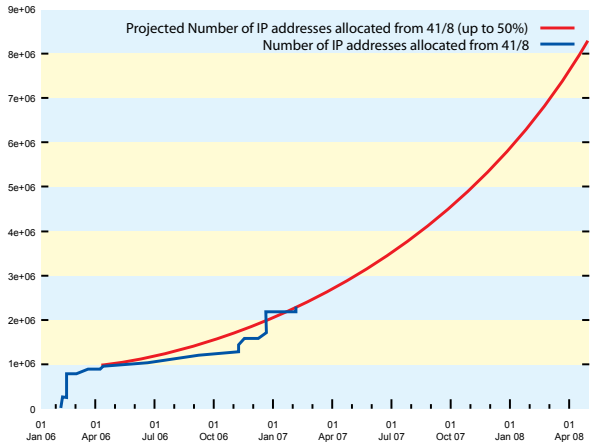


Figure 4: Projected number of IP addresses allocated from 41/8 (up to 50%)

By calculating a fragmentation rate of 10% in the allocation (unallocated addresses), AfriNIC will exhaust the pool (after an allocation of 15,099,494.4) by 11 November 2008.

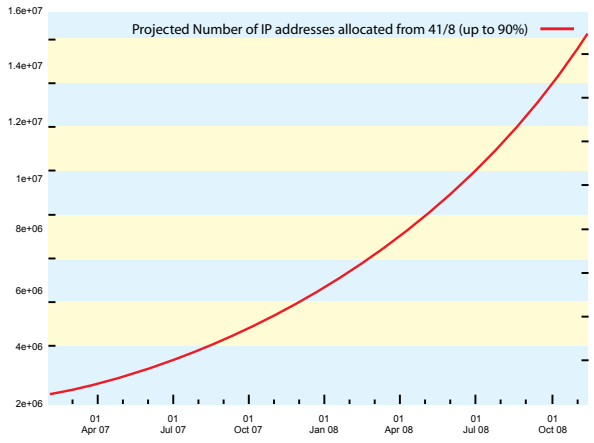


Figure 5: Projection of the exhaustion of the actual pool

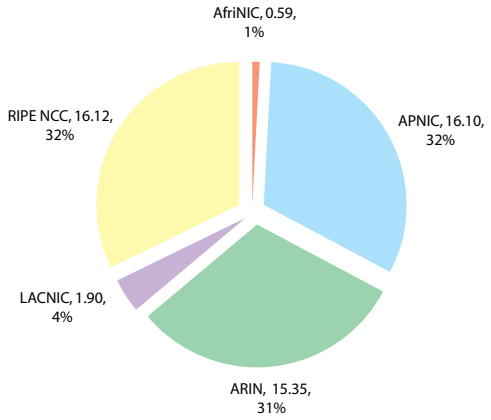
AfriNIC should request a new /8 from IANA by 22 April 2008. The IANA pool should be able to meet this request. The new block will be operational by 11 November 2008. By 11 January 2011, AfriNIC should also request a new /8. Based on current exhaustion projections IANA should also be able to fulfil this request. The new block will be effective on 11 August 2011 and will be exhausted by 11 April 2014. This is the situation if the actual rate of utilisation is maintained and predictions about the exhaustion date of the IANA pool are accurate.

But, what will it look like in reality?

Some history on IP addressing in the AfriNIC region

Our continent was probably the last to be connected "full IP" to the Internet. At that time there was a widespread (mistaken) belief among Internet operators in the region they might not receive the amount of IPv4 they requested. Hence, there was very extensive use of NAT. Some networks even have several levels of NAT. It is not uncommon to see big operators supplying a whole country with small provider aggregatable assignments (in the APNIC region this is known as a portable allocation) behind a NAT. These issues still persist despite the passing of time and the evolution of knowledge. Other factors include the size of our ISPs, which, when considering the market, and especially the economic situation of the countries, are quite insignificant. This situation was also aggravated by IP address allocation policies applied by RIRs that served the various regions of the continent before the establishment of AfriNIC.

It should, however, be noted that utilisation and consumption of public IP addresses started to evolve recently due to several factors, such as the creation of AfriNIC, availability of large bandwidth connections to an increasing number of African countries, and access to fibre links in several countries.



Distribution of IPv4 address space by RIRs

Despite this progress, our region still has the lowest IP address consumption rate. This is accompanied by significant indifference of the majority of the actors in our community to the problems linked to the system of IP addressing in particular, and Internet governance in general.

What will happen?

It is very probable that the perception of exhaustion will pressure LIRs and RIRs in the other regions (ARIN, RIPE and APNIC) into accelerated consumption and faster exhaustion of the IANA pool, which is currently projected for 25 July 2011. If this occurs one year beforehand (that is on 25 July 2010) then AfriNIC's /8 request for 11 January 2011 will not be fulfilled due to the exhaustion of the IANA pool. Therefore the AfriNIC pool would be completely empty in August 2011 instead of April 2014.

Coming back to the initial questions that drove us to these long and perhaps boring studies and analyses:

- What can the "small" registries (like AfriNIC) do to ensure continued access to IPv4 addresses to their communities once the IANA pool is exhausted?
- What will global number resource management look like after the exhaustion of the central IANA and AfriNIC pools?
- What about the IPv6 solution?

The results of our analysis project that the exhaustion of the IANA pool will occur on approximately 25 July 2010, and that

P 10

the AfriNIC pool will be exhausted by 11 August 2011, that is, four years and six months from now.

How can AfriNIC plan for a date that will most probably occur earlier than projected?

Several actions are possible. All require local, regional and global action. Let us try to define the foundations of some possible approaches:

- To sensitise the community to the situation, enabling operators the opportunity to avoid surprises and emergencies, and be better prepared for exhaustion. This sensitisation should include short- and long-term solutions. In this context, the creation of a SIG (Special Interest Group) dedicated to this problem and to solutions focused on the realities of our region is recommended.
- To start an active campaign to recover unrouted allocated addresses in the AfriNIC region. How many will there be? For how many months or years will the life of the pool be extended? What resources does AfriNIC have to recover those blocks, of which the significant part is derived from the allocations made before the RIR system, and is identified as legacy space?
- To constitute a reserve in the remaining pool to be used to supply critical infrastructure, the sustainability and development of which are vital for the stability of the network after 11 August 2011. What size should this reserve be? Will the global community support the allocation of IP to RIRs to satisfy this reservation?

  A new definition of the term "critical infrastructure" would perhaps be necessary. Currently the definition includes root servers and IXPs. What will the critical infrastructure be defined as in 2011? Governmental or inter-governmental networks? Research centre networks? Medical networks? Networks for monitoring and preventing natural disasters?
- To open a global debate on the use of the 16 /8s reserved by the IETF for "future use".
- To open discussions on a global level for the management of the remaining pool. Will an equitable distribution of the remaining pool among all five RIRs be conceivable?

What will the situation be after 11 August 2011?

AfriNIC would probably be able to satisfy "critical infrastructure", but may not be able to do much for the other categories. The latter will be confronted by the black market of IP addresses. It will be very difficult and expensive to get IPv4 addresses and there will be an excessive inclination towards NAT, which will negatively impact networks.

Will registries certifying addresses help the regulation of the market that will emerge? Resource certification could allow services such as the integrity of transferred resources, transfer of ownership, and exclusivity of transfers.

What about the IPv6 solution?

All the suggested actions listed above, and those based on IPv4, will only be temporary. In reality there will be a transition solution to extend the use of IPv4 for a while. The solution resides in the long-term perspective: the availability of a broader range of addresses offered by IPv6. It is imperative for the survival of the Internet that particular attention is paid to IPv6 in the AfriNIC region.

This mobilisation must occur at all development levels in communication technologies. Governments have a pivotal role to play in this arena: to deploy IPv6-ready networks and applications. It will also be necessary for governments to get firmly involved in the IPv6 information campaigns and training.

The SIG will have, among others, a role to establish a reliable document database aimed at the operators regarding transition and migration mechanisms of IPv4 networks to IPv6. In December 2005, AfriNIC launched an information campaign promoting awareness of the removal of financial charges for allocation of IPv6 addresses. AfriNIC has been able to train network operators in eight African countries and increase the number of IPv6 allocations in the region by more than 400%. However, this still represents less than 10% of the networks currently using IPv4. Daily BGP statistics (http://airrs.afrinic.net/bgp/reports6.html) show that less than 30% of IPv6 allocations are visible on the Internet. The path is still long and requires collective responsibility.

Notes

A similar study done by Cisco using different methods:

http://www.cisco.com/web/about/ac123/ac147/archived_issues/ipj_8-3/ipv4.html

Please note:

The exhaustion projection figures quoted in this article have been updated since this article was written. For the latest information regarding IPv4 consumption projections please see:

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

Olaf Kolkman elected IAB Chair

Ex-RIPE NCC staffer Olaf Kolkman (who is currently working with R&D firm NLnet Labs) was recently appointed Chair of the Internet Architecture Board (IAB). The IAB is a committee of the Internet Engineering Task Force (IETF), and is responsible for:

- Confirming the IETF Chair and IESG Area Directors, from nominations provided by the IETF Nominating Committee.
- Overseeing and occasionally commenting on aspects of Internet protocol architecture and procedures.
- Overseeing the process used to create Internet standards and serving as a complaints appeal board.
- Managing the editing and publication of the Request for Comments (RFC) document series, and administering the assignment of IETF Protocol parameter values.
- Representing the IETF's interests in liaison relationships with other organisations concerned with standards, technical and other Internet issues.
- Advising ISOC on technical, architectural, procedural, and, where appropriate, policy matters pertaining to the Internet and its enabling technologies.
- Selecting the Internet Research Task Force (IRTF) Chair for a renewable two-year term.

APNIC would like to wish Olaf every success in his new role.

Managing IPv4 consumption - policy proposal and discussion update

This year there has been increasing worldwide focus on the rate of IPv4 address consumption, with discussions taking place in many parts of the global community. Special sessions have been held at each of the RIR meetings this year, covering the current and future IPv4 consumption rates, and their many technical, operational and policy implications.

These sessions have been catalysts for vigorous discussion and debate. However, although most people agree that some sort of action is needed, it appears at this stage that the community is far from reaching agreement on the best way forward.

APNIC

At APNIC 23, Toshiyuki Hosaka from JPNIC presented the 'IPv4 countdown' proposal. This proposal, written by 10 prominent members of the Japanese Internet community, argues that IPv4 consumption needs to be addressed in an orderly way, and that a policy is required to set out a consumption plan.

At the meeting, there was general support for the following three principals in the proposal:

- All five RIRs should synchronise their activities related to dealing with IPv4 consumption
- RIRs and IANA should maintain the current policy and practices in the lead-up to IPv4 depletion
- Recovery of unused address space should be discussed separately

The remaining principle that some IPv4 blocks should be reserved was split into two:

- The last date of allocation should be defined in advance
- Some unicast IPv4 blocks should be reserved for possible use in the future

At APNIC 23, there was no consensus on these two elements of the remaining principle.

JPNIC's proposal did not reach consensus at the ARIN XIX, LACNIC X, or RIPE 54 meetings. The proposal was submitted as an informational proposal at AfriNIC 6.

ARIN

David Conrad's 'IPv4 Soft Landing' proposal, submitted after the 'IPv4 countdown' proposal was discussed at ARIN XIX, suggests a different approach. His proposal aims to "provide for a smoother transition away from IPv4 towards IPv6," suggesting that RIRs impose increasingly strict requirements for new address allocations as the amount of address space available in the IANA unallocated IPv4 address pool decreases. These provisions include:

- Implementing more stringent reassignment and utilisation percentages
- Requiring documented IPv6 infrastructure services and connectivity provision
- Requiring reuse of IPv4 address space used for internal infrastructure

The ARIN Address Council has decided to work with David Conrad to adjust the proposal before it can be accepted as a formal ARIN policy proposal.

LACNIC

'Global Policy for the allocation of the remaining IPv4 address space in the Regional Internet Registry system', was presented and reached consensus at LACNIC X in May 2007. The proposal suggests that when a greater proportion of the IPv4 pool is consumed, the remaining unallocated IANA IPv4 pool be divided equally among the five RIRs. Currently, the practice is that RIRs request blocks from IANA as needed.

In the near future, this proposal will be submitted to the remaining four RIRs.

Other recent developments

In addition to direct policy proposals dealing with IPv4 consumption, recent RIR meetings have included panels and BoFs on the issue.

An ARIN XIX 'IPv4 discussion panel' examined issues such as address hoarding, reclamation, lack of community awareness of IPv4 consumption, and possible IPv4 routing table bloat due to fragmentation.

At AfriNIC 6, the 'IPv4 exhaustion BoF' discussed a number of potential actions to mitigate IPv4 consumption, including possibly using 240.0.0.0/4, address recovery, and financial incentives to use IPv6.

Although the proposals and discussion about how to best approach IPv4 consumption have been varied, there has been general agreement that some action must be taken to address the issue.

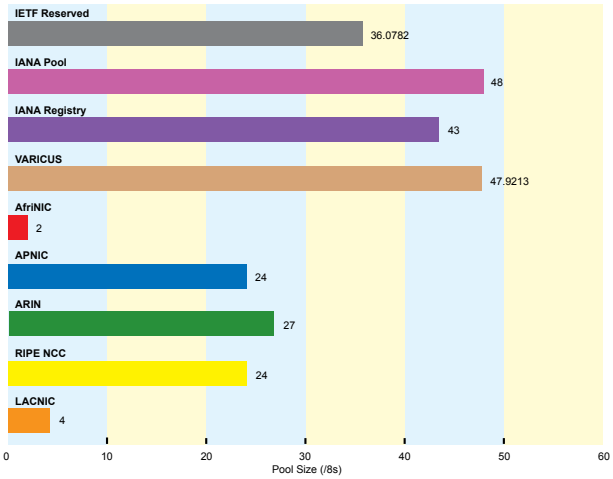
On 7 May 2007, the ARIN Board of Trustees took the unusual step of passing a resolution to formally advise the Internet community that supply of IPv4 addresses "can not be assured indefinitely"; that IPv6 is available and suitable for many Internet applications; and that "migration to IPv6 numbering resources is necessary for any applications which require ongoing availability from ARIN of contiguous IP numbering resources".

This resolution is likely to provide more impetus for all RIR communities to develop a new, coordinated policy approach.

For links to regional discussions on IPv4 consumption, please see:

http://www.apnic.net/news/hot-topics/ipv4-consumption

IPv4 address pool status



Source: Geoff Huston, http://www.potaroo.net/tools/ipv4

4-byte ASNs in the wild

On 1 January 2007, APNIC began processing applications for 4-byte (or 32-bit) Autonomous System Numbers (ASNs). This article provides a brief update on their uptake and implementation status.

How are 4-byte ASNs assigned?

The new 4-byte ASNs were first released in the APNIC region on 1 January 2007, under a transitional policy. For now, APNIC assigns 2-byte ASNs by default, but users can ask to receive a 4-byte number instead. From 1 January 2009, APNIC will assign 4-byte ASNs by default, unless the user specifies otherwise. Then, from 1 January 2010, APNIC will cease to make the distinction and will operate AS number assignments from an undifferentiated 4-byte AS number pool.

How many 4-byte ASNs exist?

The autonomous system number space is a 32-bit field, with 4,294,967,296 unique values. From this pool 1,023 numbers are reserved for local or private use, and three are reserved for special use. The remaining pool is available to support the Internet's public inter-domain routing system. IANA holds the pool of unallocated ASNs, while the remainder have already been allocated to RIRs. The breakdown of IANA-allocated ASN blocks to each of the RIRs is as follows:

Status	AS Pool	16-bit	32-bit
IETF Reserved	66562	1026	65536
IANA Unallocated Pool	4294851584	20480	4294765568
Allocated	49150	44030	5120
RIR Data			
AfriNIC	2228	1204	1204
APNIC	5779	4755	1024
ARIN	22455	21431	1024
RIPE NCC	15879	14855	1024
LACNIC	2809	1785	1024

Source: Geoff Huston, http://www.potaroo.net/tools/asn32

How many 4-byte ASNs are currently visible?

Any individual AS number can be in any one of four states:

- part of the IANA unallocated number pool
- part of the unassigned pool held by an RIR
- assigned to an end user entity but not advertised in the routing system
- assigned and advertised in BGP

As at 22 May 2007 the current totals of AS numbers according to this set of states is:

Checking 4-byte ASN states

The RIPE NCC has an online tool that allows users to enter an AS number and check if it is in an AS path. This query will work for ASNs allocated by all RIRs.

http://www.ris.ripe.net/perl-risapp/asinuse.html

User experiences

Mainstream use of 4-byte AS numbers is still a long way off. This is to be expected, considering technological constraints and the short time that has elapsed since the first 4-byte ASNs were allocated. RIPE NCC, LACNIC, and AfriNIC indicate that 4-byte ASNs allocated within their regions are currently being used only for experimental purposes.

RIPE NCC Senior Project Manager Henk Uijterwaal has received some feedback from operators, explaining "I hear that ASN32 with software routers … works fine except that there is an occasional issue with reconstructing the ASN32# when the transition AS is in the path." He does note that this error does not limit functionality.

Speaking at RIPE 54 in May, Erik Romijn elaborated on this situation. He indicated that the AS_PATH was usually reconstructed correctly, but not always. Presently the cause is not fully understood. An example is included below:

30844 3356 4637 1221 23456	(should be 2.2)
30844 3356 3549 1103 1125 23456	(should be 3.5)
30844 3356 2914 4697 23456	(should be 2.3)

Implementation of 4-byte AS for BGP

Geoff Huston has observed that Quagga and OpenBGPD have patches available, and that some Juniper routers are also compatible. Cisco IOS-XR has had this functionality available since release 3.4, and it is expected that many Cisco IOS models will include 4-byte AS for BGP in 2008.

A global policy for IANA allocation of 4-byte ASNs to RIRs is expected to be released in 2007.

We will provide updates in future editions of Apster as more data on 4-byte ASN uptake and implementation becomes available.

Further reading

Geoff Huston, '32-bit AS Numbers - The View from the Old BGP World'

http://www.potaroo.net/ispcol/2007-01/asn32.html

Geoff Huston, 'Exploring AS numbers'

http://www.potaroo.net/ispcol/2005-08/as.html

RIR	RIR Pool	Unadv	Adv	16-bit	Unadv	Adv	32-bit	Unadv	Adv
AfriNIC	1957	132	139	936	129	139	1021	3	0
APNIC	1474	1327	2978	466	1315	2974	1008	12	4
ARIN	3504	7542	11409	2484	7538	11409	1020	4	0
RIPE NCC	2293	3872	9714	1284	3860	9711	1009	12	3
LACNIC	1600	406	803	577	405	803	1023	1	0
TOTAL	**10828**	**13279**	**25043**	**5747**	**13247**	**25036**	**5081**	**32**	**7**

Source: Geoff Huston, http://www.potaroo.net/tools/asn32

APNIC executive council election results

An open election to fill four EC vacancies was held at APNIC 23 in Bali, Indonesia on Friday 2 March 2007.

The EC member positions up for election were previously held by Kuo-Wei Wu, Moo-Ho Billy Cheon, Qian Hualin, and Ma Yan.

The election was hotly contested, with eleven candidates vying for the positions.

The successful candidates were Ming-Cheng Liang, Kusumba Sridhar (the first ever member from India), and Mao Wei. Kuo-Wei Wu was re-elected to the EC.

The APNIC EC now consists of the following members:

- **Maemura Akinori (Chair)**
- **Che-Hoo Cheng (Secretary)**
- **Kuo-Wei Wu (Treasurer)**
- **Ming-Cheng Liang**
- **Kusumba Sridhar**
- **Wei Mao**
- **Vinh Ngo**

Three EC positions will be due for re-election at APNIC 25 in Taipei, Taiwan.

For more information about the role and duties of EC members please see:

http://www.apnic.net/ec/ec-duties.html

Maemura Akinori (Chair)

Che-Hoo Cheng (Secretary)

Kuo-Wei Wu (Treasurer)

Ming-Cheng Liang

Kusumba Sridhar

Wei Mao

Vinh Ngo

AfriNIC and SANOG join ICONS

The Internet Community of Online Networking Specialists, otherwise known as the web site ICONS, has grown, with the recent additions of AfriNIC, APRICOT, and SANOG.

APNIC originally launched ICONS in 2005 to create an interactive space for networking experts and operators to share experience, and learn about Internet technologies and best practice.

ICONS allows registered users to create blog style entries on topics of interest to the addressing community. ICONS also contains how-to guides, network tools, and news feeds on a range of networking issues. ICONS users can interact with each other via its built-in social networking tools.

With the addition of AfriNIC, APRICOT, and SANOG, ICONS now brings together more experiences and perspectives than ever before.

AfriNIC, the RIR for the African region, commenced formal operations in 2005. It serves 55 economies in a culturally and linguistically diverse region. Many AfriNIC members face the challenges of a developing continent, including restricted bandwidth, poor technical infrastructure, and difficult economic conditions. In representing their interests, AfriNIC has become a dynamic part of the local community and a clear voice in international forums.

SANOG is the South Asian Network Operators Group, a non-profit forum for data network operators in South Asia. SANOG provides a regional forum to discuss operational issues and technologies of interest to data operators in the South Asian Region. This occurs most prominently through SANOG meetings, which are major gatherings of the South Asia technical community. The next APNIC Open Policy Meeting will be held with SANOG 10 in New Delhi, India.

APRICOT, the Asia Pacific Regional Internet Conference on Operational Technologies, is well-known by the APNIC community as the major operational conference in this region. The first APNIC Open Policy Meeting of each year is held in conjunction with APRICOT. The next APRICOT will be held in Taipei, Taiwan, from 20-29 February 2008.

ICONS is now available at all of the following addresses:

http://icons.afrinic.net

http://icons.apnic.net

http://icons.apricot.net

http://icons.sanog.org

ASO AC selects Raimundo Beca to serve a new term on the ICANN Board

▲ Raimundo Beca will serve a further three year term on the ICANN Board. (Photo by Joi Ito, 2007, reproduced under the Creative Commons license.)

On 2 May 2007, the Address Council of the Address Supporting Organisation (ASO AC) confirmed the appointment of Raimundo Beca to serve a further three year term on the ICANN Board of Directors. He will now continue his current term, which expires at the ICANN meeting, in June 2007.

One of the ASO's main functions is to select an individual to serve on the ICANN Board of Directors. It does this through a lengthy selection process, including a public call for nominations, interviews with eligible candidates, background checks, a public comment period, and a vote by all ASO AC members.

Mr Beca is a partner at Imaginacción, a Chilean consulting company, and is on the board of several companies, including Puerto San Vicente Talcahuano, where he is Vice chairman of the Board; and Armamater, a company that trains and employs disabled people who live in extreme poverty.

Raimundo is a Chilean citizen, with a degree in Civil Engineering and a Masters in Mathematical Economics. He has previously served as a member of the ASO Address Council, appointed first by ARIN and then by LACNIC.

He was first appointed to the ICANN Board in 2004, where he has served on the Finance Committee, the Audit Committee, the ICANN Board – GAC Joint Working Group, and the President's Strategy Committee.

Training update

APNIC training is designed to support our members to effectively manage their Internet resources and operations.

Recent activities

This year we have conducted courses in Bangladesh, Pakistan, Australia, Malaysia, Nepal, the Philippines, China, Singapore and Thailand.

During some of our recent training sessions we used our remote training lab (which features several routers) to conduct practical workshops, and were very pleased with its performance.

The training team also participated in major events such as JANOG, NZNOG, APRICOT, SANOG, and the Malaysia IPv6 Summit.

In March, Team Cymru from the United States visited the APNIC office and conducted a workshop for the training team. The workshop provided an understanding of network attacks and how to combat them, and how to undertake network forensics. We would like to extend our thanks and appreciation to Ryan Connolly and Steve Gill from Team Cymru for this valuable training.

Coming soon

We are currently planning training to be conducted in the second half of this year in Cambodia, Vietnam, Mongolia, India, China, Hong Kong and Pacific islands.

In order to improve APNIC's training scope, delivery, and availability, and better respond to our members' needs, we are currently undertaking several initiatives:

- This year we intend to expand our remote training lab to include servers, and to extend its use in our training.
- We are currently incorporating material from the Team Cymru workshop into our new security module. We are also planning further collaborative activities with Team Cymru.
- In the next few months we hope to sign MoUs with a number of partners in the region for training facilitation, support and collaboration. These partnerships will assist us in our efforts to provide training on a regular basis to our members in those areas.
- We are currently further developing our e-learning facilities, and later this year plan to release web-class options and additional e-learning modules.
- The training team is currently facilitating and delivering a program that will train other staff within the APNIC Services Area to become associate trainers. This program will enable more member contact and expand APNIC staff skills.
- We will be undertaking a mini-survey to elicit member views, concerns, needs, and ideas on how we can best provide training and educational activities. Survey participation is open to all members. We will contact you directly soon to invite you to give us your valuable feedback.

Thanks

Sponsors and local hosts play a major role in making our training possible. For their tremendous support and involvement we would like to express our appreciation to:

- Advanced Science and Technology Institute – Philippines (ASTI)
- China Telecom
- Nepal Internet Exchange (NPIX)
- ISP Association of Bangladesh (ISPAB)
- Networkers Society of Pakistan (NSP)

Contact us at training@apnic.net

Staff updates

Technical

John Kennedy, Systems Administrator

John joined APNIC in February 2007. He has a Bachelor of Information Technology, majoring in Information Systems and Artificial Intelligence, and has seven years experience in systems administration. As part of the Network Operations team, his responsibilities at APNIC include implementing, managing and maintaining server applications.

Drew Ward, Systems Administrator

Drew joined APNIC in February 2007. He has a Bachelor of Business majoring in Information Systems, and has experience in network and server administration. As part of the Network Operations team, his responsibilities at APNIC include maintaining the network and associated environments.

Communications

Vania Soon, Communications Officer

Vania joined APNIC in February 2007. She has Bachelor of Business Management, a Bachelor of Business Communication, and a Diploma in Business Administration. Vania provides support to the Communications Area. She is originally from Singapore.

Business

Clemensia Valiandra, Administration Assistant

Clemensia (Ensi) joined APNIC in February 2007. She has a Bachelor of Arts degree and customer service experience. She is responsible for running the APNIC reception, as well as providing office administration services. She is originally from Indonesia.

Cheryl Fisher, Office Administrator

Cheryl joined APNIC in March 2007. She has an Honours degree in Communication Studies, combined with varied experience in administration and promotional roles. Working in the Business area, her responsibilities at APNIC include handling travel arrangements, as well as a broad range of administration duties. She is originally from Singapore.

Training schedule

2007

June

4-7 Bangkok, Thailand

11-14 Ulaanbaatar, Mongolia

July

9-13 Cambodia

16-20 Vietnam

TBA Laos

August

TBA Solomon Islands (In conjunction with PacIPv6 2007)

TBA Fiji

TBA Malaysia

September

TBA New Delhi, India (In conjunction with APNIC 24 / SANOG 10)

TBA India (FLAGTEL)

TBA Sri Lanka

TBA Maldives

TBA China

October

TBA Papua New Guinea

TBA Australia

November

TBA Hong Kong

TBA India

TBA New Zealand

TBA Guam

TBA Singapore

TBA Pakistan

December

TBA Bhutan

TBA Indonesia

TBA Thailand

The APNIC training schedule is subject to change. Please check the web site 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

Interop Tokyo 2007
13-15 June 2007
Tokyo, Japan
http://www.interop.jp

Korea IPv6 Summit
14-15 June 2007
Seoul, Korea
http://www.ipv6.or.kr/eng

PACNOG 3
16-22 June 2007
Avarua, Rarotonga, Cook Islands
http://www.pacnog.org

ICANN Meeting
25-29 June 2007
San Juan, Puerto Rico
http://www.icann.org/meetings

IPv6 Technical Summit
30 June 2007
Karachi, Pakistan
http://www.nsp.org.pk/schedule.php

QUESTnet
10-13 July 2007
Cairns, Australia
http://www.questnet.net.au

69th IETF
22-27 July 2007
Chicago, USA
http://www.ietf.org/meetings/meetings.html

PACIPv6 2007
15-21 August 2007
Pacific Islands
http://www.ipv6forumpacific.org

AP* retreat
26 August 2007
Xi'an, China
http://www.apstar.org/retreat/xian_2007/xian_2007.html

9th APNG Camp
27-29 August 2007
Xi'an, China
http://www.apng.org/9thcamp.htm

24th APAN Meeting
27-31 August 2007
Xi'an, China
http://www.apan.net/meetings/xian2007

APNIC 24/SANOG 10
3-7 September 2007
New Delhi, India
http://www.apnic.net/meetings

AfriNIC 7
24-28 Septmber 2007
Durban, South Africa
http://www.afrinic.net/meeting

ARIN XX
17-19 October 2007
Albuquerque, USA
http://arin.net/ripe/meetings

RIPE 55
22-26 October 2007
Amsterdam, Netherlands
http://ripe.net/ripe/meetings/current.html

ICANN Meeting
29 October - 2 November 2007
Rio de Janeiro, Brasil
http://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
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

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
- 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.