Public Policy Issues in the Communications and Infrastructure Services Policy area

Geoff Huston

APNIC

June 2011

A Perspective from an RIR

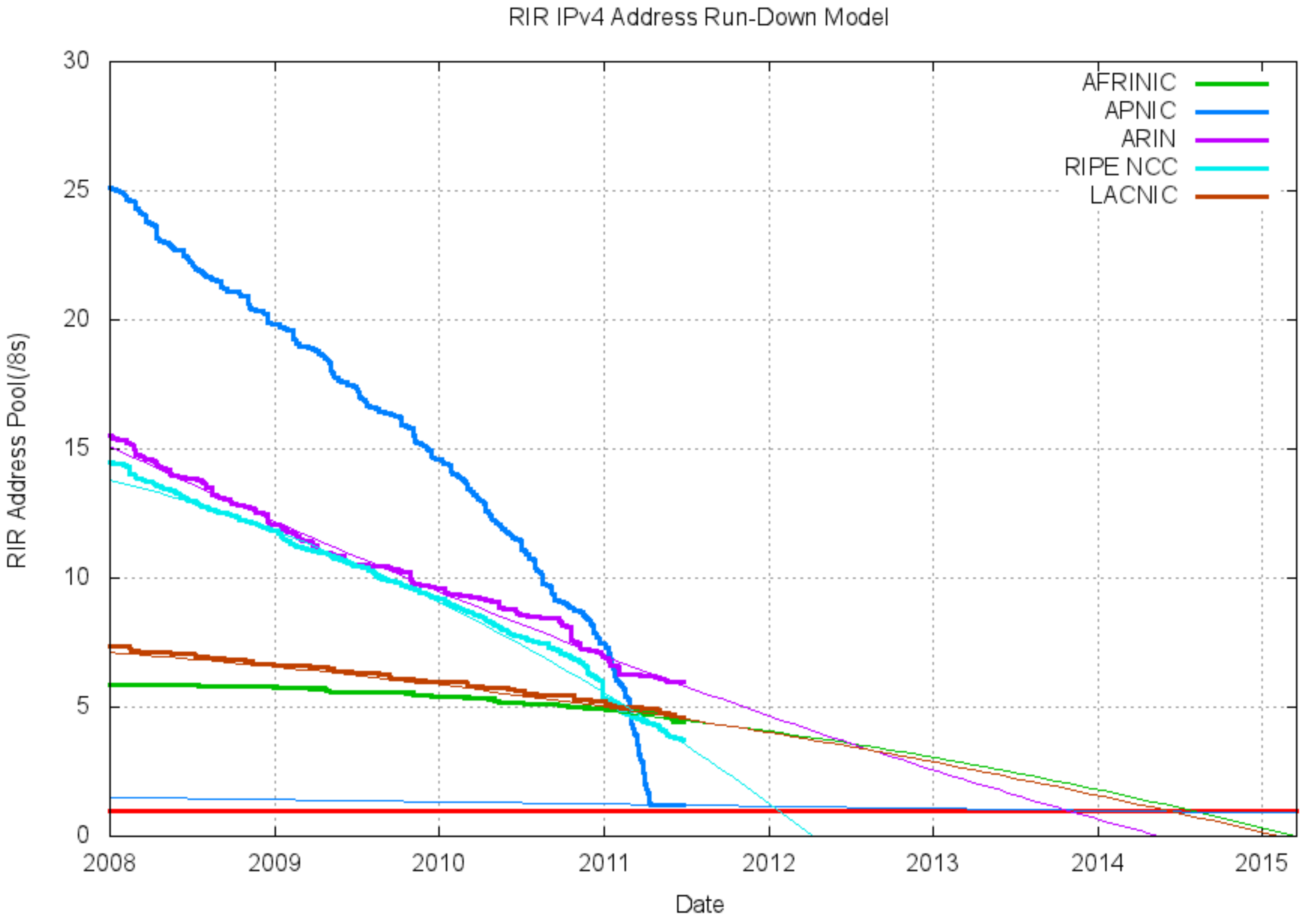
- There are many ways of addressing this question
- The filter I'll use here is one that concentrates on the Internet's service and infrastructure environment from the perspective of one of the Regional Internet Registries as it relates to the CISP agenda
- Which means I'm going to be quite selective as to which aspects of CISP are of interest to me!

One issue dominates all others at the moment from the perspective of APNIC…

And, surprisingly, its an issue that has failed to gain significant traction in the public space beyond the technical and operational community.

And it’s an issue that lies at the heart of the direction of the Internet’s evolution over the coming years…

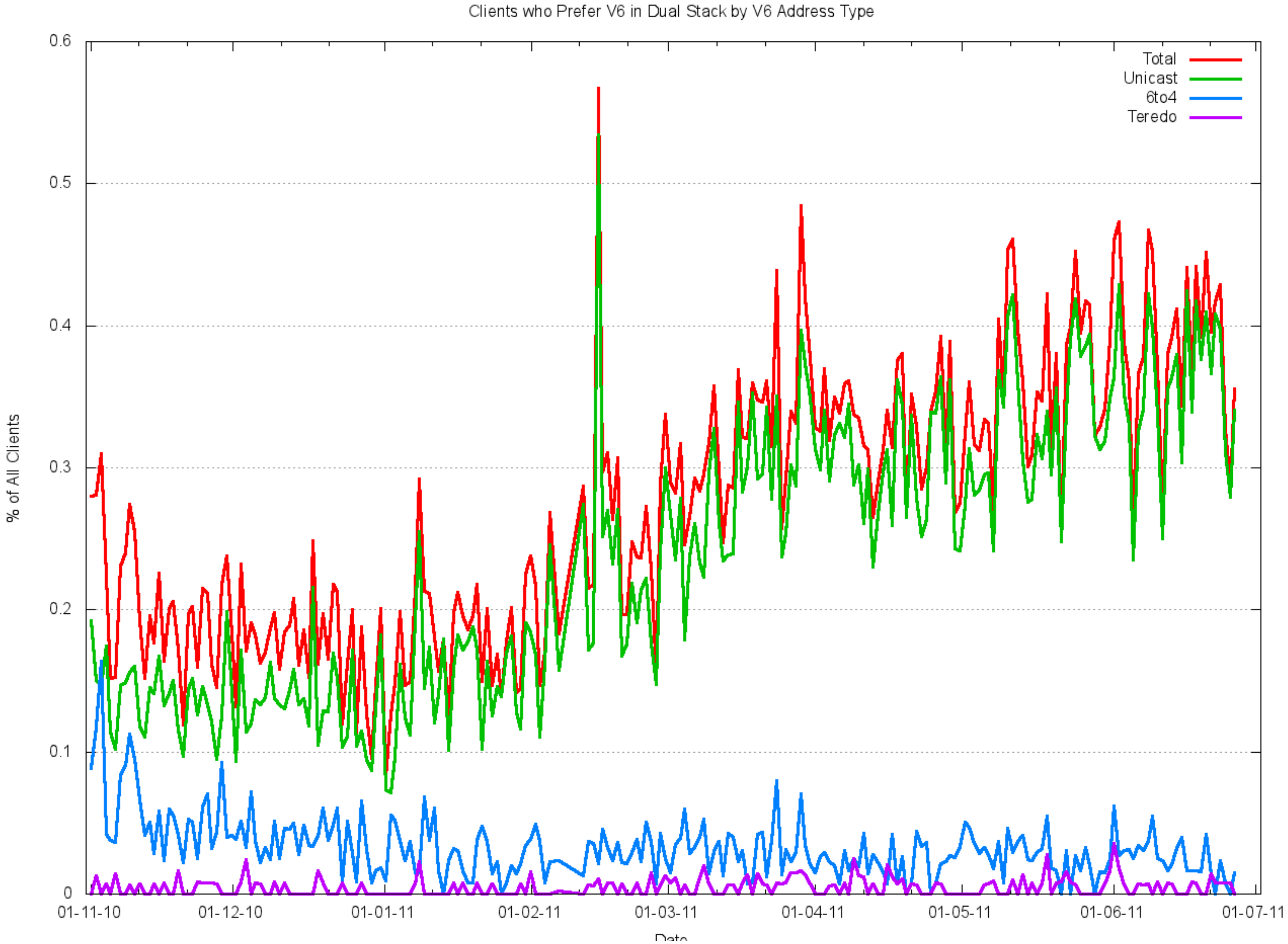
We are Running on Empty!



Running on Empty

- IANA exhausted its pool of IPv4 addresses in February 2011
- APNIC exhausted its pool of IPv4 addresses in April 2011
- RIPENCC – late 2011 / early 2012
- ARIN – late 2013
- AFRINIC, LACNIC – mid 2014

and IPv6 uptake is very slow



Some Policy Issues

- A protracted Dual Stack transition environment means staying with IPv4 for some time yet
  - Can an after-market in addresses function effectively? What, if any, are the special considerations here?
  - Will incumbents set up prohibitive barriers to entry?
  - How do new competitors enter the carriage services market?
  - Will all future content now be bound to carriage service providers? How will new entrants fare?

Some more Policy Issues

Incentives for IPv6?

- Are current incentives for industry to adopt IPv6 as a service platform adequate?
- Will the pressures from new entrants be enough to force incumbents to invest in IPv6 service infrastructure?
- Or will the open Internet stall and revert to walled gardens of IPv4?

Some more Policy Issues

Risks of Failure?

- What are the risks posed to the communications environment if industry fails to adopt IPv6?
  - Broadband programs and the desire for ubiquitous access to the Internet?
  - Security and Integrity of the network and transactions that take place over the network?
  - Market distortions through compromise of the end-to-end architecture
  - Threat to a vibrant competitive supply sectors in carriage and content services

IPv4 and CGNs

- IPv4 address exhaustion is prompting a further response from ISPs in the addition of Carrier Grade NATs into the network as a means of further extending the useful lifetime of IPv4
- These carrier-controlled network elements add some additional issues that have significant policy dimensions

Some Policy Issues

CGNs log the NAT binding – i.e. they log the source and destination address and ports of every network transaction or conversation

What personal privacy issues are raised when an access carrier has a comprehensive log of all individual network transactions performed by each customer?

Some Policy Issues

To what extent can an open and neutral service platform be maintained in the face of CGN-managed port rationing?

- Is this a market-based issue, in which case would this place the carrier in a dominant position with a privileged position ability to distort the content market?
- When the port resource is scarce what rationing mechanism is fair? How can openness and neutrality be enforced when the carriage provider controls the rationing point?

Infrastructure Security

There is an increasing awareness of the diversity of security issues that are being posed by the broad adoption of information services

- Consumer protection from individual fraud and theft strikes
- Impact on various financial services from organized criminal activities
- Broader impact as a consequence of highly organized disruptive attack on national infrastructure

Integrity of the name and address infrastructure is an essential component of an effective defense against many forms of sophisticated attack

Securing the Address Infrastructure

DNSSEC work added public/private keys to the DNS in an effort to prevent deliberate falsification of DNS information

RIR effort to add public/private keys to the address registry infrastructure in an effort to prevent deliberate misrepresentation over who is authorized to negotiate addresses

- Application in registry operations and routing

Some Policy Issues

- How is trust negotiated in the RPKI?
- Could external bodies placed in unique positions of potential control over the root of trust in the RPKI?
- Is a public certification infrastructure for Internet Addresses subject to national judicial or law enforcement orders relating to issuance and revocation of certificates?