IIJ
Internet Initiative Japan

IPv4 Run-Out, Trading, and the RPKI

MENOG 3 / Salmiya

2008.04.15

Randy Bush <randy@psg.com>

http://rip.psg.com/~randy/080415.menog-v4-trad-rpki.pdf

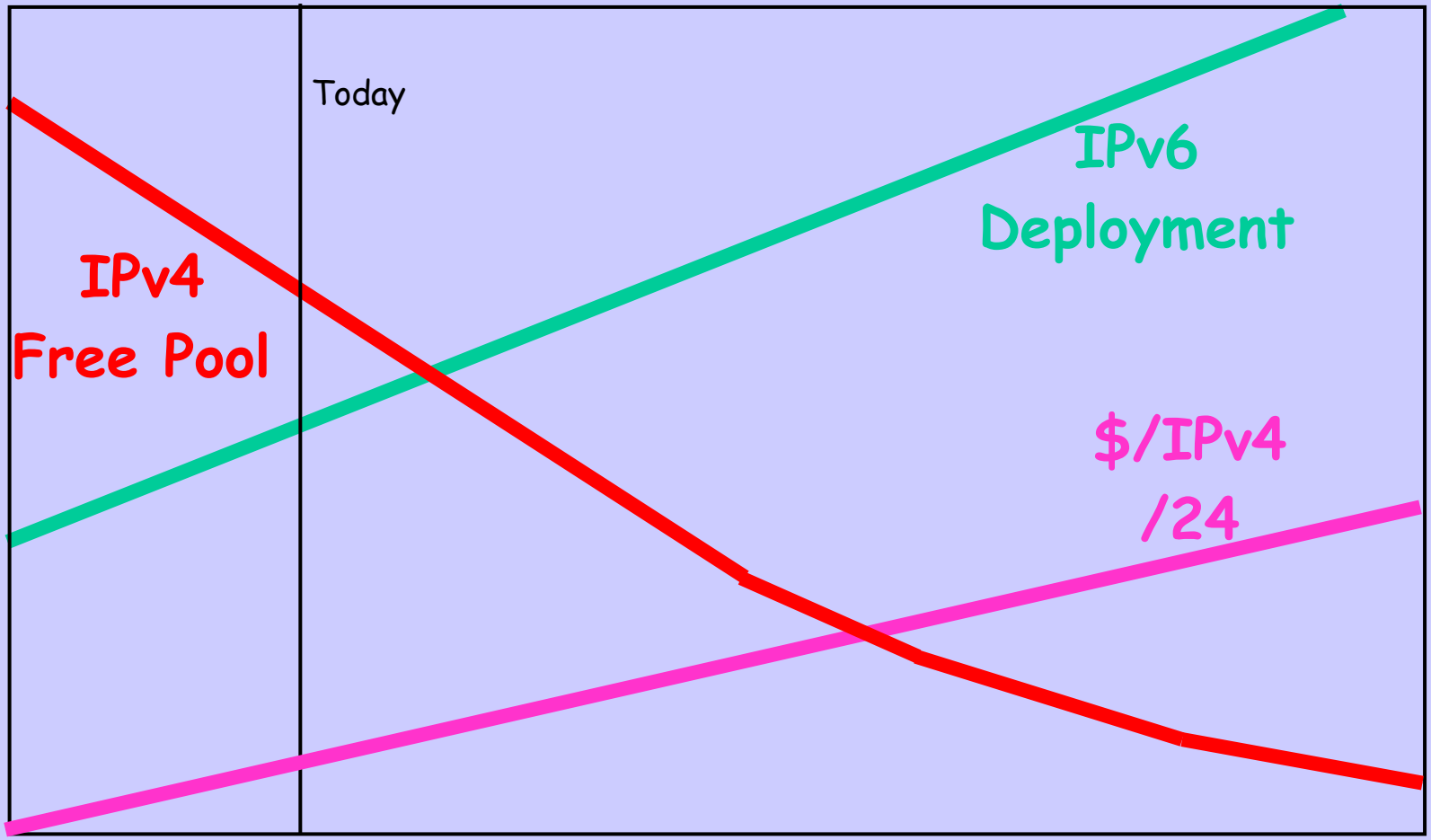
Internet Initiative Japan

- Originally, a government initiative to get Japan on the Internet
- Asian and some US backbone
- Commercial customer base
- Internet, not telephant, MPLS, ...
- First commercial IPv6 deployment
- WIDE, Kame IPv6 code base...

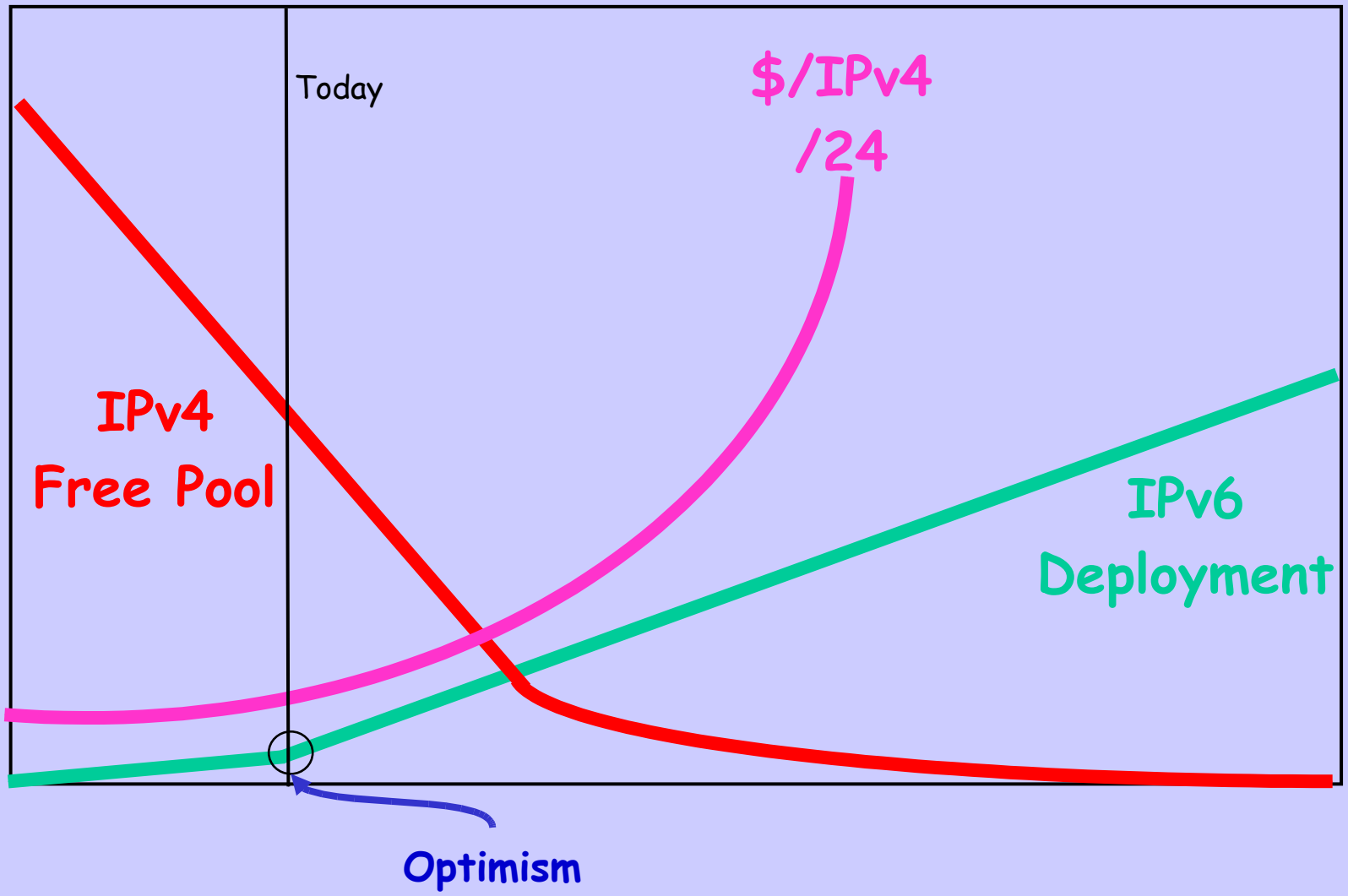
IPv4 Free-Pool Run-Out

- IPv4 Free Pool will run-out in a few years
- This is in line with the graphs of Frank Solensky over ten years ago
- IPv4 will go to a ***trading model***
- Registries will become t*itle agents*, not allocators, of IPv4 space
- RIRs are developing full multi-RIR/LIR open source software to certify and verify title to IPv4 and IPv6 resources

What Should Have Happened

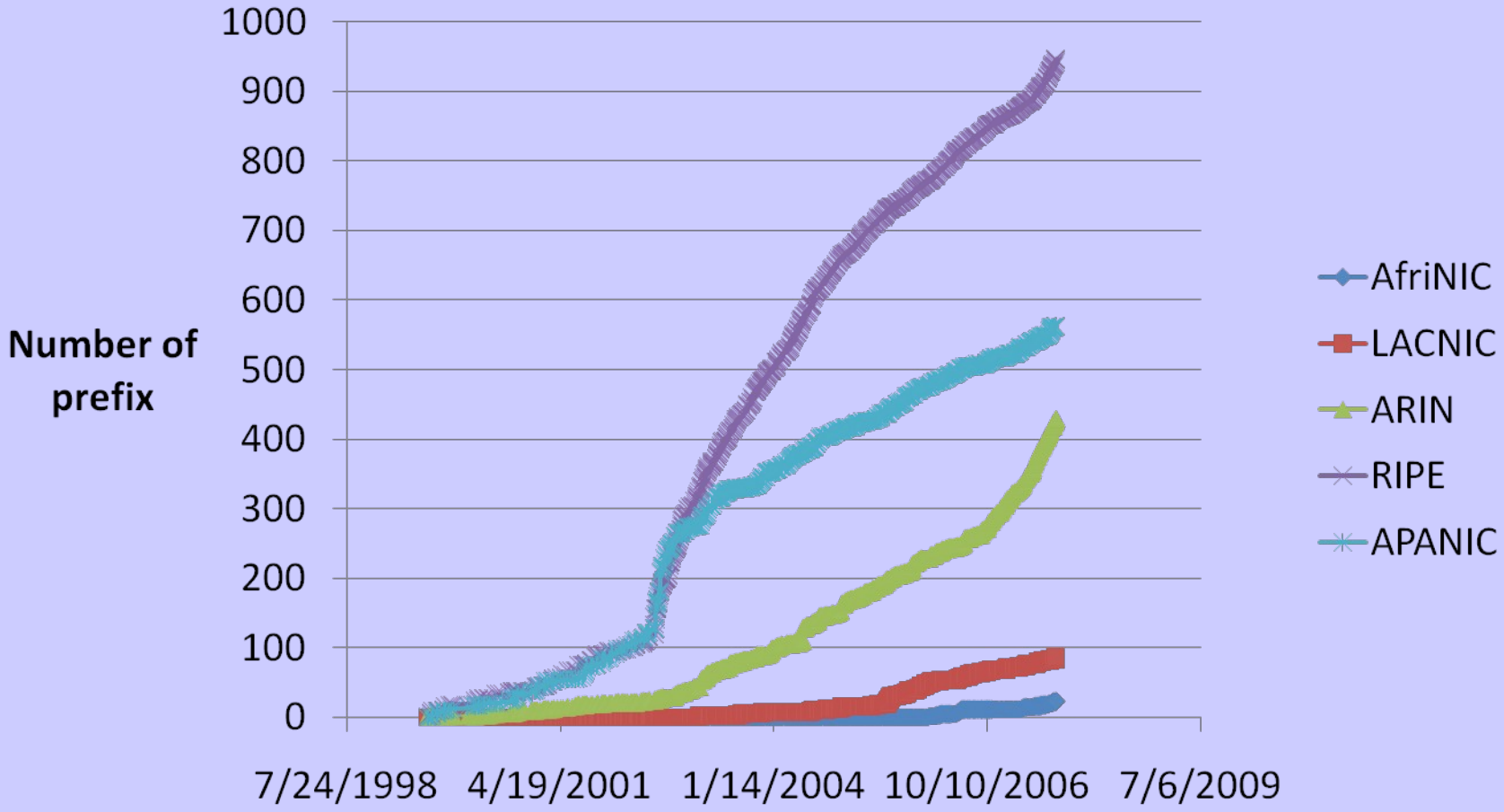


What Is Happening?

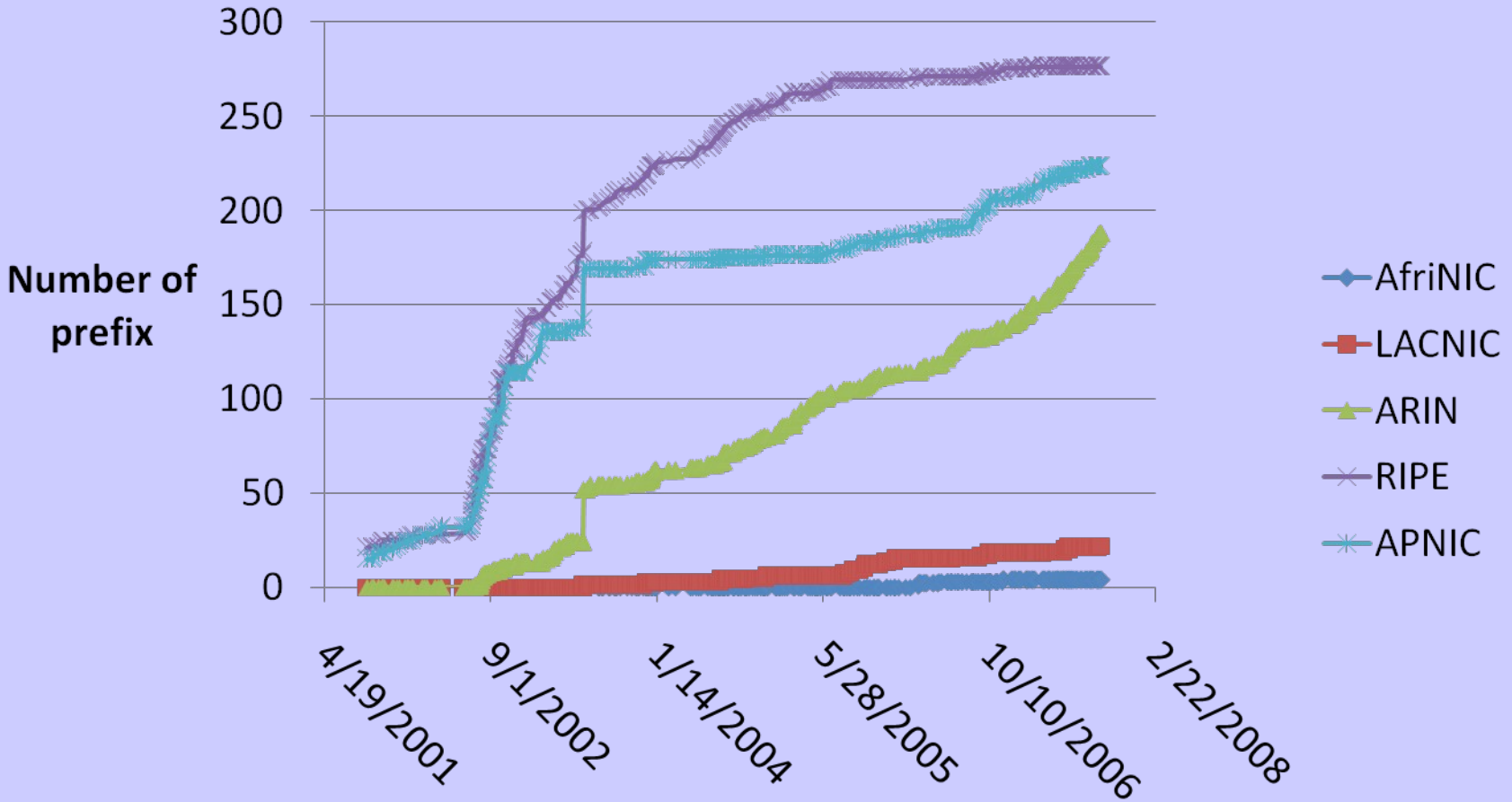


If You Think IPv6 is Being Deployed

IPv6 Prefix Allocations



BGP Prefix Announcements

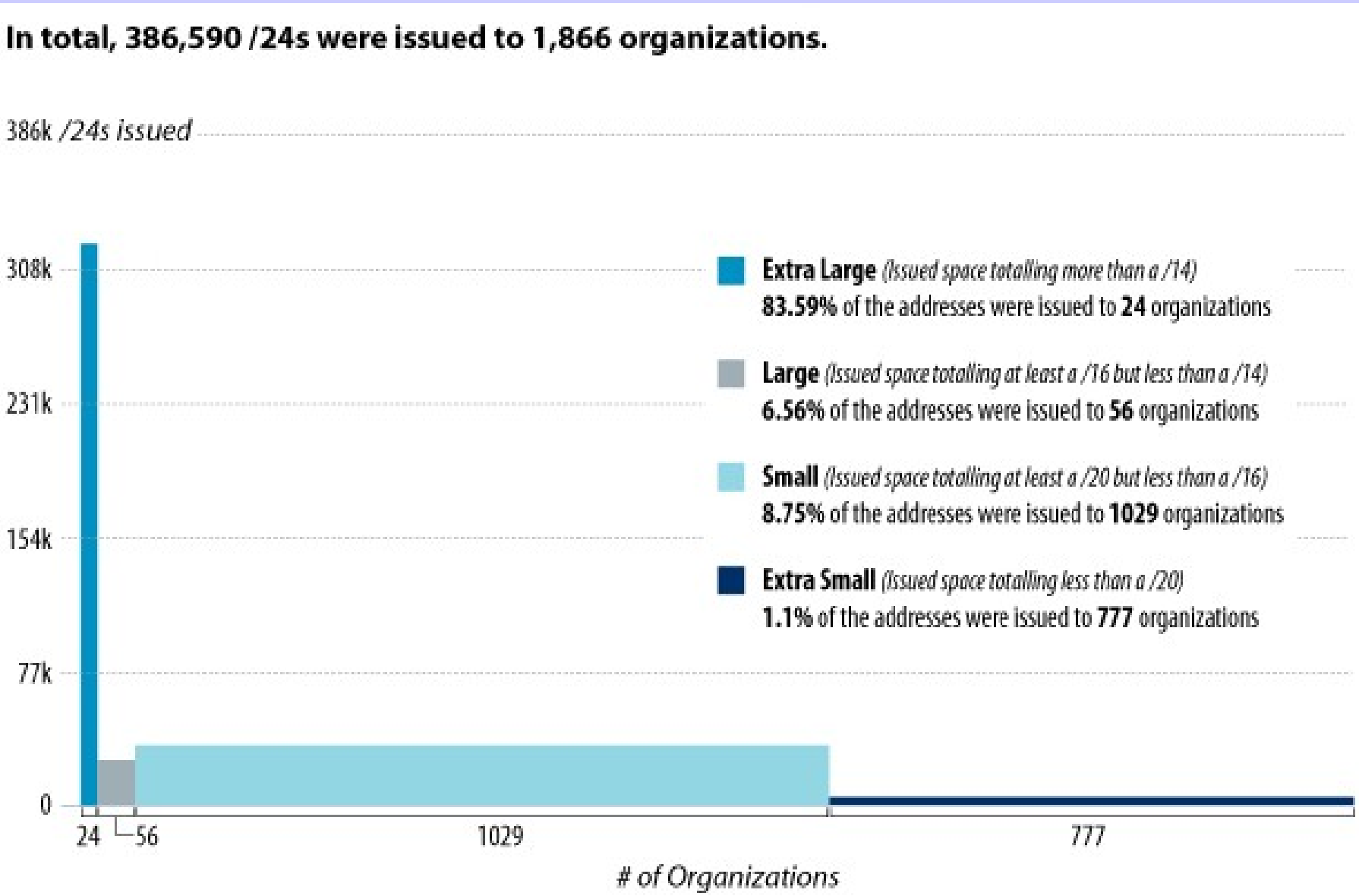


So We Need IPv4 Run-Out to be Reasonably Optimal and also Fair

Are current societal and administrative systems fair?

What's 'fair'?

Is This 'Fair'?


In total, 386,590 /24s were issued to 1,866 organizations.
386k /24s issued
308k
231k
154k
77k
0
24
56
1029
777
# of Organizations
Extra Large (Issued space totalling more than a /14)
83.59% of the addresses were issued to 24 organizations
Large (Issued space totalling at least a /16 but less than a /14)
6.56% of the addresses were issued to 56 organizations
Small (Issued space totalling at least a /20 but less than a /16)
8.75% of the addresses were issued to 1029 organizations
Extra Small (Issued space totalling less than a /20)
1.1% of the addresses were issued to 777 organizations

That was ARIN for 2006-7
Other regions have somewhat different distributions

Yes, it models the market concentration in North America but ...

Meanwhile a newcomer may not be able to 'justify' a /20-/24

The RIR communities have placed severe barriers to entry at the low end !

Is that how we think the last few /8s should be distributed?

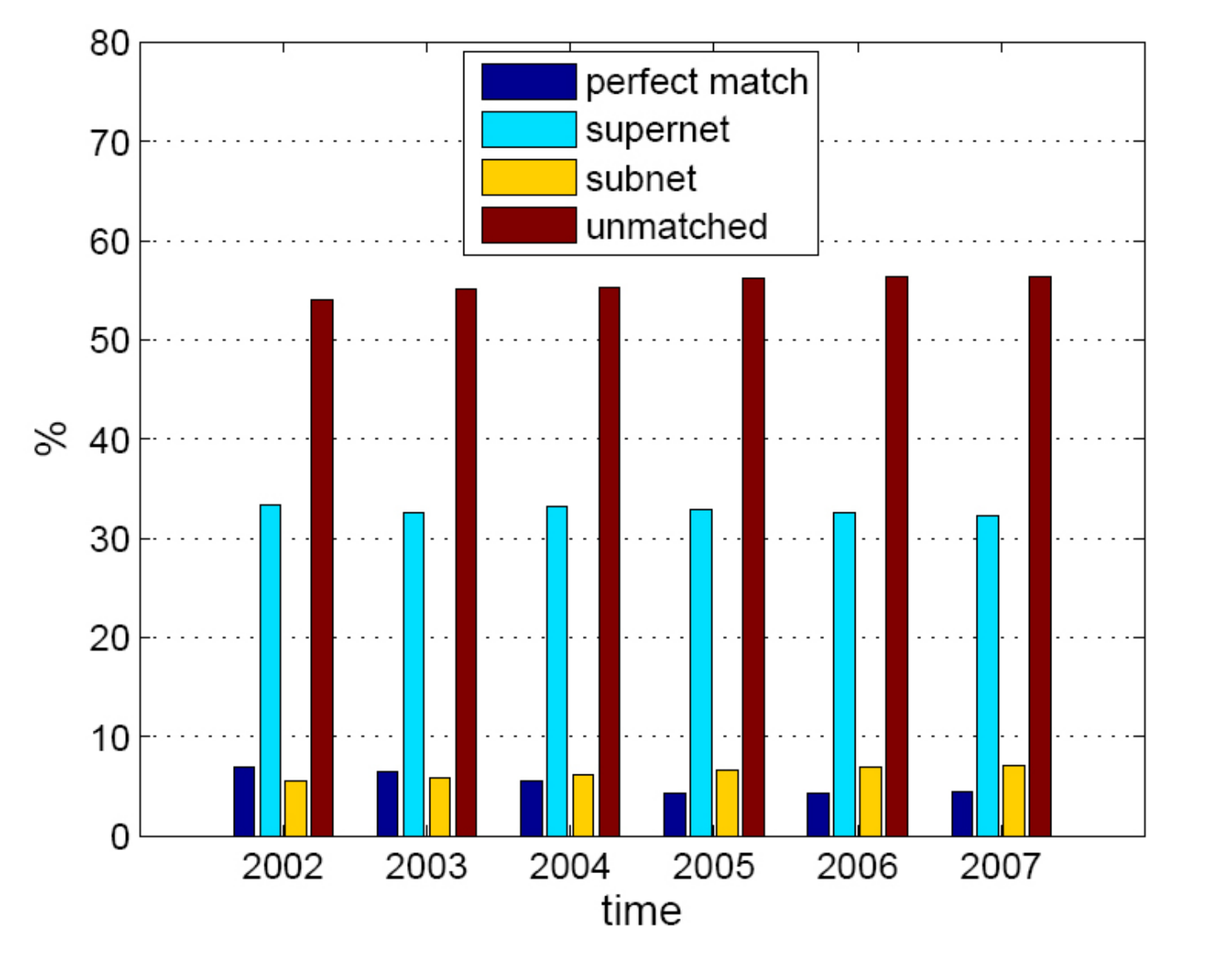
Why is This?

- We're saving routing table size at the expense of barrier to entry
- Should we be doing this at the end?
- Instead, give me tools deal with folk who de-aggregate unnecessarily

What Might We Do?

- I am not an expert, but I admit it, which is a differentiator :)
- Even distribution to RIRs of the last /8s
- Within RIRs, damp big request[er]s
- Enable small requests
- Save the last /16 in each region for unknowns and emergencies
- Open market with transparency

ARIN Legacy Prefix Announcements



Unannounced /24 Equivalents

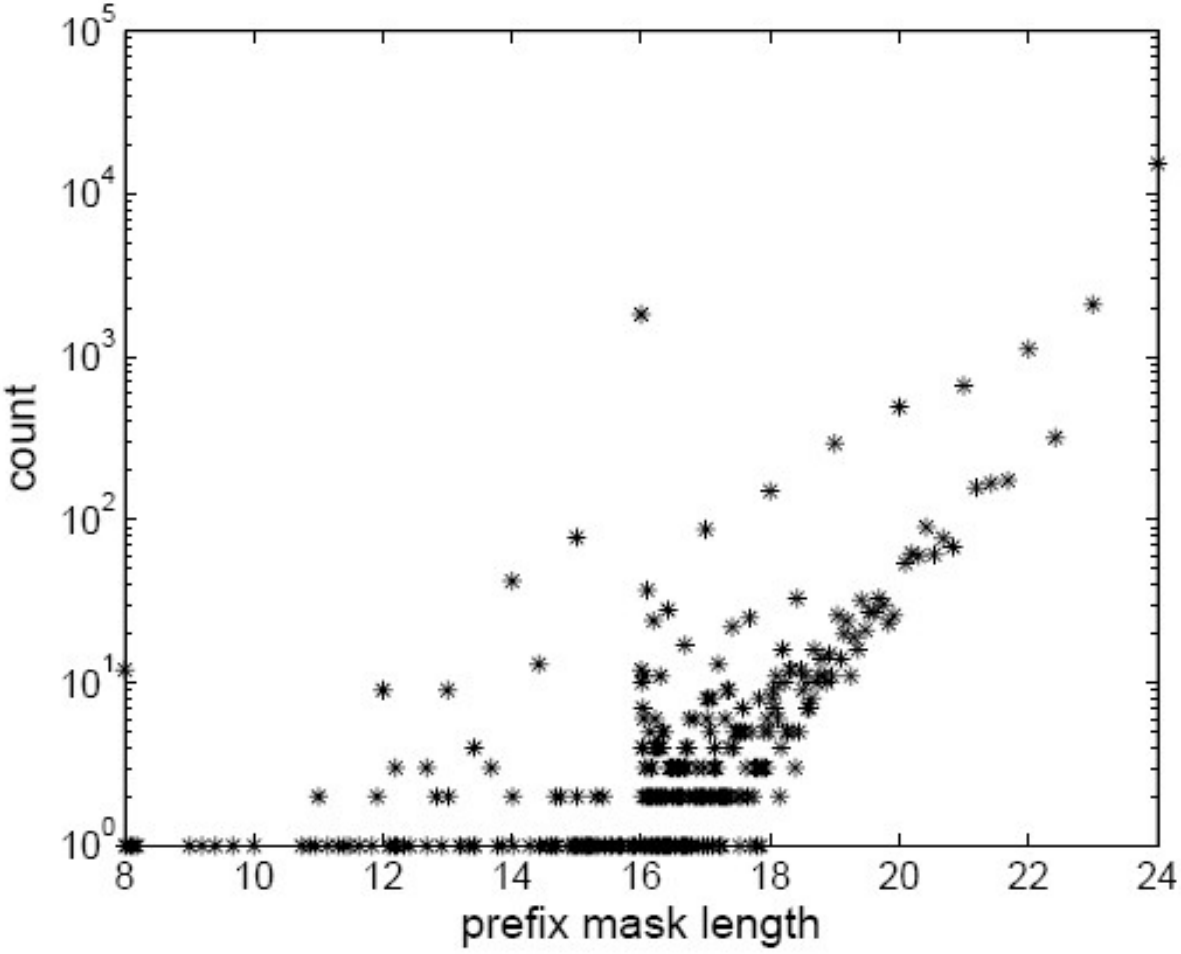


Figure 11: Histograms of the unannounced IP block

That's Legacy Space

There is also a lot of underutilized RIR Space Post-Legacy

How to Put IPv4 Space to Best Use?

Best Use
is Supposed to be
What Markets Do

There Already is a

Black Market in

IPv4 Address Space

Would you Rather Have a Black Market or an Open Market?

I personally prefer a possibly flawed open market to amateur over-regulators

So How Do We Make the Market Transparent and Safe?

The First Problem is that the Buyer Needs Assurance that the Seller can Actually Convey Title

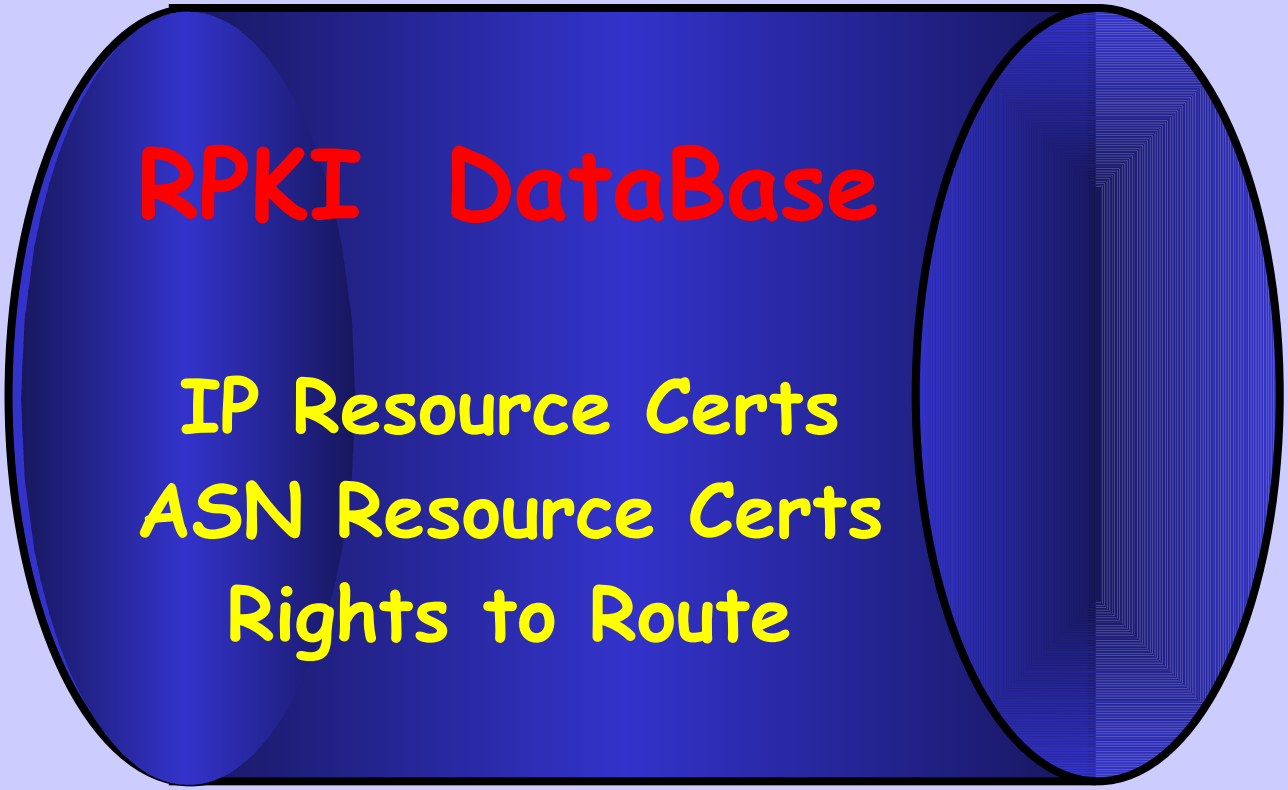
Serious Problems!

- Poor quality of whois data
- Poor quality of IRR data
- No formal means of verifying if a new customer legitimately holds IP space X
- No formal means of verifying routing announcements

Requirements

- Formally verifiable assertions of rights in IP Address Space and ASNs
- Formally verifiable assertions of rights of ASNs to originate prefixes
- Formally verifiable assertions of the correctness of routing announcements
- Formally verifiable Assignment, Transfer, … of IP prefixes and ASNs

Resource Public Key Infrastructure



Application Range

- Handle both resource ownership
  - ASNs and IP space
- And verifiable transactions with others:
  - Allocation
  - Sub-Delegation
  - Transfer, Trade, Sale, Lease, ...

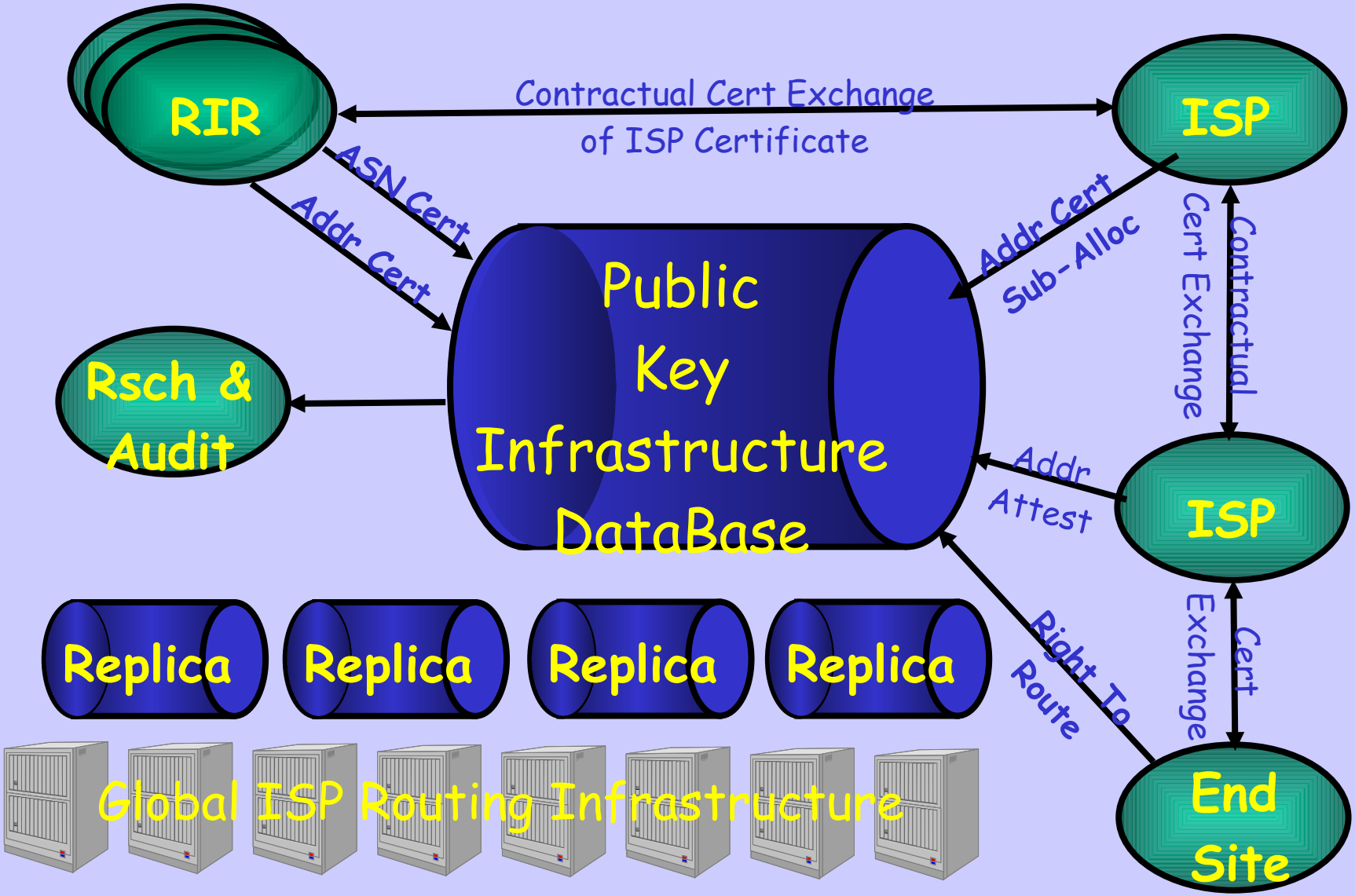
The Approach

- Components
  - Use X.509 v3 Public Key Certificates with IP Address and ASN Extensions (RFC 3779)
  - Use Existing Technology where possible
  - Leverage existing Open Source software, tools, and deployed systems
  - Contribute to Open Source solutions
- OpenSSL as the foundation platform
  - Add RFC 3779 Extensions for IPs and ASNs
- Certification framework anchored on the IP resource distribution function

Operate Across RIRs

- With different kinds of IP/ASN allocations
  - Normal
  - Experimental
  - Legacy, …
- And resources received from multiple RIRs/LIRs

RPKI Interfaces/Users



IP Delegation Chain

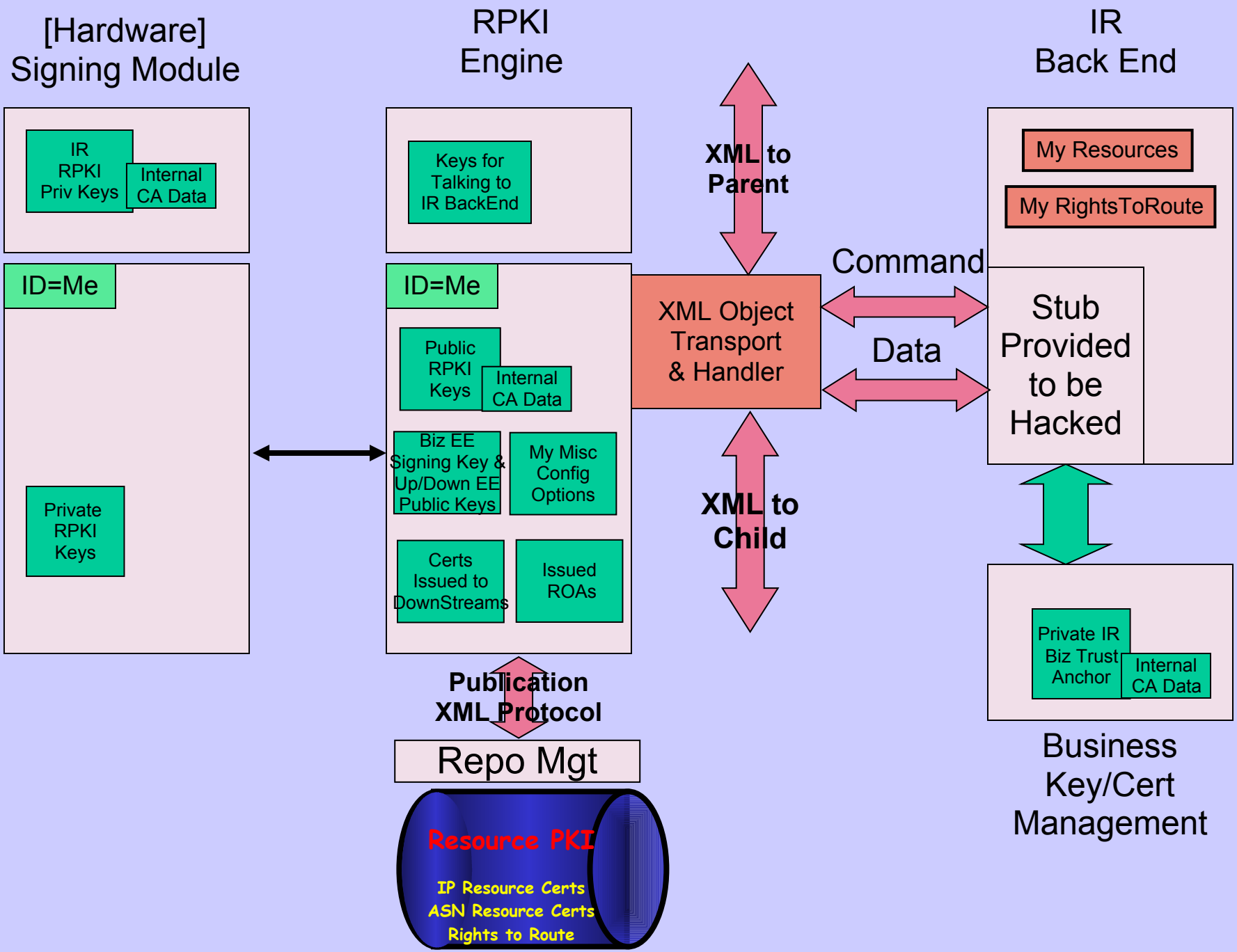
- RIR allocates to ISP
  S.rir (192.168/16, *isp*)
- ISP allocates to Downstream
  S.isp (192.168.128/17, *dstr*)
- Downstream allocates to User
  S.dstr (192.168.142/24, *user*)
- Anyone can verify it all, because the public keys *rir*, *isp*, *dstr*, and *user* are in the public RPKI

Business Certificates

- RIRs generate business certs for members
- Need only be reproducible, they are not formal identities, because are only used
  - In business transactions where they are exchanged and managed by contract, or
  - To sign transport of IP or ASN certs
- May be based on 'external', e.g. Thawte certs, used to generate a business cert within the RIR Business PKI
- ISPs may use an RIPE Biz Cert for an APNIC allocation or business transaction

Underlying Certificate RPKI Architecture

- Allows any open implementation to be used by all
- Allows each RIR/LIR to have own business processes and front end
- And allows ISPs and end sites to build their own processes using the base tool-set


[Hardware]
Signing Module
RPKI
Engine
IR
Back End
IR
RPKI
Priv Keys
Internal
CA Data
Keys for
Talking to
IR BackEnd
My Resources
My RightsToRoute
XML to
Parent
Command
ID=Me
ID=Me
XML Object
Transport
& Handler
Stub
Provided
to be
Hacked
Data
Public
RPKI
Keys
Internal
CA Data
Biz EE
Signing Key &
Up/Down EE
Public Keys
My Misc
Config
Options
Private
RPKI
Keys
XML to
Child
Certs
Issued to
DownStreams
Issued
ROAs
Private IR
Biz Trust
Anchor
Internal
CA Data
Publication
XML Protocol
Repo Mgt
Resource PKI
IP Resource Certs
ASN Resource Certs
Rights to Route
Business
Key/Cert
Management

Tools for RIRs

- Create root ASN and IP space certificates
- Issue IP and ASN allocations to ISPs and End Sites
- Generate and lodge ISP certs
- Manage their own cert sets
- Run and Manage a Repository

Tools for ISPs

- Acquire business certs from RIRs
- Generate IP and ASN requests to RIRs and/or Upstreams
- Generate biz certs for customer ISPs and End-User sites
- Validate resource certificates
- Run and Manage a Repository

State of Play

- APNIC did a simple prototype
- OpenSSL 3779 done by ARIN
- Full system almost done by ARIN
- R&D teams almost finished with multi-RIR and ISP/user protocols
- APNIC & ARIN driving the protocol, designs, model, essentially XML/CMS
- The result are all open source

What We Can Do

- We can't make more IPv4 Space
- We can't fix the speed of light
- We can use markets/trading to get the best use of IPv4 space
- We can see that those markets are safe

Thanks To

ARIN and ISOC for continuing support of Research and Development

APNIC, RIPE, LACNIC, AfriNIC

Internet Initiative Japan