Sixscape

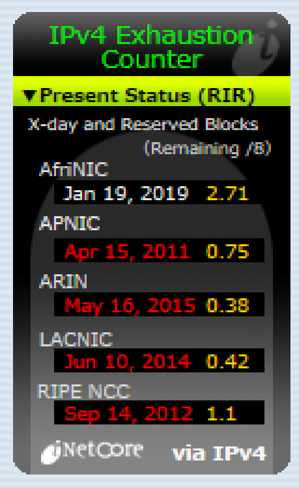
IRP - the Identity Registration Protocol

LAWRENCE E. HUGHES
CO-FOUNDER AND CTO
SIXSCAPE COMMUNICATIONS, PTE. LTD.

LHUGHES@SIXSCAPE.COM

The IPv4 Internet is Broken

- By the mid-1990's we realized that public IPv4 addresses would run out by 2000 or so, at the then current allocation rate
- There was no successor protocol that could be rolled out in time.
- As a *temporary* measure, we splintered the monolithic IPv4 Internet into millions of private internets hiding behind the few precious public addresses, using NAT. That gave us another 10-15 years, but those years are over now.
- The successor protocol (IPv6) is now mature and being deployed globally.



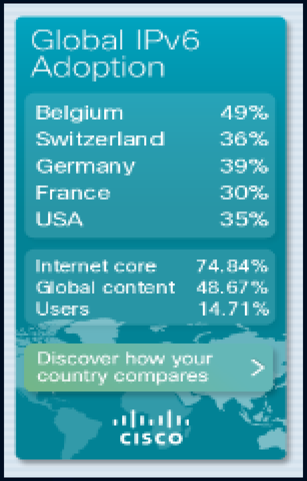
IPv4 Exhaustion Counter

▼Present Status (RIR)

X-day and Reserved Blocks (Remaining /8)

AfriNIC	
Jan 19, 2019	2.71
APNIC	
Apr 15, 2011	0.75
ARIN	
May 16, 2015	0.38
LACNIC	
Jun 10, 2014	0.42
RIPE NCC	
Sep 14, 2012	1.1

NetCore via IPv4



Global IPv6 Adoption

Belgium	49%
Switzerland	36%
Germany	39%
France	30%
USA	35%

Internet core	74.84%
Global content	48.67%
Users	14.71%

Discover how your country compares >

cisco

What are the main differences between the legacy IPv4 and new IPv6 Internets?

- Real address scopes (interface, link, site, global, etc)
- Working, scalable multicast
- More robust ICMP, now including IP address resolution
- Autonomous address generation by nodes
- But the two “biggies” are:
  - Ample global addresses
  - NO NAT!!!

So what cool new things can we do on our shiny new NAT-less IPv6 Internet?

- For the first time since the mid-1990's any node can, *in theory*, connect directly to any other node in the world.
- We can leap past Client/Server architecture (made necessary by NAT) to *Direct End2End connections*!
- BUT we need better address resolution to make this possible. DNS is not really up to the challenge.
  - DNS has no per-user authentication, so anyone can change registered addresses
  - DNS takes a long time for new registrations to propagate (not good for mobile devices that may change addresses multiple times in a single day)
  - DNS is woefully insecure, and it is *very* difficult to roll out DNSSEC on such a large, existing critical infrastructure (20M servers worldwide).
  - DNS registers the address of *nodes*, not of *people* (or more precisely, the last place some person has used their IRP-aware application).

Benefits of Direct End2End Connections

- No need for intermediary servers - No bottlenecks , reliability or security issues at intermediary nodes
- Traffic is decentralized – only goes over shortest path between the two communicating nodes
- More reliable – so long as there is network connectivity between the two nodes, communication can happen
- Higher performance – if the two nodes are in same site, bandwidth is not limited by ISP connection (could be Gigabit)
- Security is better – harder to monitor or block traffic than in the current Client/Server model
- Overall system capacity much higher
- Apps can use Diffie-Hellman for symmetric key exchange

IRP – the Next Generation Address Registry

- IRP allows any app to register the current IPv6 address of the logged-in user at any time
- It includes a user directory to provide per-user authentication, and linking the registered address to a *person*, not a *node*
- Connections to the IRP server can be IPv4 or IPv6, and are over explicit TLS (only one port required)
- Authentication to IRP server can be username/password, but it normally uses X.509 client certificate cryptographic authentication
- IRP includes full PKI certificate management – request, download, revoke, renew certs, plus obtain other users' certs, check cert validity and revocation status, get CA certs, etc. This allows hiding PKI complexity in the apps – making it mostly invisible to the users.
- IRP is XML based for easy implementation and extensions.

IRP – Security Issues

- Connections over IRP are secured with TLS 1.2, usually with X.509 certificate based strong client authentication. These certs can be obtained from the Domain Identity Registry (DIR) servers.
- Once obtained, these client certs can also be used for website cryptographic authentication, S/MIME, network access, etc. IRP provides the necessary PKI for validity and revocation checking.
- Like DNSSEC, all registered information is digitally signed on the server, and those signatures are delivered along with the information.
- Unlike DNS, the DNSSEC aspects are designed in from the start – no complex transition after a massive infrastructure is in place.
- The key management for the DNSSEC aspects are “built in”.

IRP – Decentralized Deployment

- There is one Domain Identity Registry server for each Internet domain (just like DNS). The collection of all DIR servers is a Global Identity Registry.
- The nodename of the DIR server for a given domain is published in DNS via SRV records– no need to configure the DIR address.
- Any node can easily find the DIR server that issued a certificate in order to check validity and revocation status.
- Like DNS, this allows the service to scale to the global level – potentially billions of addresses and client certificates.
- Current PKI can handle server certs, but the volume of client certs is orders of magnitude greater. It *must* be decentralized, like DNS.

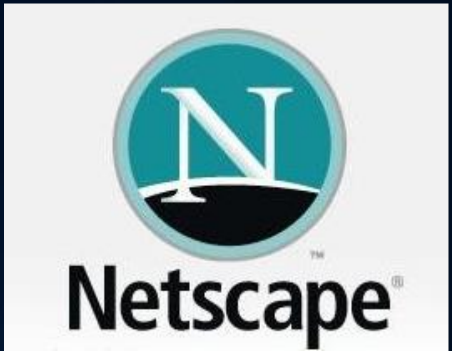
IRP Submitted to IANA, Issued Port 4604

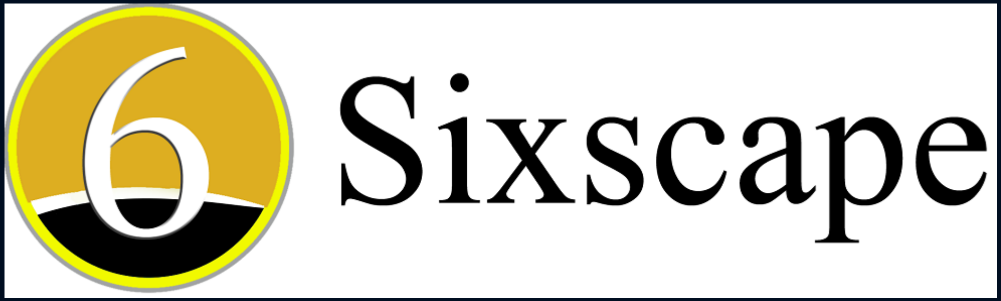
- I submitted the basic specification of IRP to IANA. It was reviewed by Lars Eggert (chair of IRTF). It was determined to be viable and novel (did not duplicate any existing IETF protocols), so it was issued port 4604.
- I have created engineering prototypes of the Domain Identity Registry server and a first client (SixChat – kind of a decentralized "Whatsapp" with true end2end automated security).
- Sixscape Communications is now productizing these and will be creating additional products that leverage IRP:
  - Microsoft Outlook add-in to simplify S/MIME email
  - Microsoft Office add-in for signing, encrypting and securely exchanging documents

SixChat Protocol Submitted to IANA, Issued Port 4605

- The SixChat protocol allows true End2End secure communications over IPv6 – no intermediary nodes required for normal use.
- It includes a new *Peer to Peer* handshake equivalent to the one in TLS – using Diffie-Hellman for symmetric key exchange and client certs for mutual strong authentication (SSL/TSL is hopelessly tied to Client/Server architecture).
- Sixchat currently supports chat and S/MIME email, soon will support file transfer, and later voice and video.
- SixChat User Agents can originate *and* accept multiple connections.
- SixChat User Agents depend on IRP for address resolution and PKI.

In case you are wondering what inspired our name and logo…





Netscape Communications made an enormous contribution to the IPv4 Internet with the first viable web browser, first viable web server, SSL and many other innovations.

Sixscape Communications intends to make the same kind of contributions to the IPv6 Internet, with the Global Identity Registry, IRP and SixChat protocols, and *End2End Direct* connectivity.

THANK YOU