RPKI

Resource Public Key Infrastructure

p: (+64) (4) 931 6977 e: registry@nzrs.net.nz
f: (+64) (4) 931 6979 w: www.nzrs.net.nz
P.O. BOX 24361, WELLINGTON, NEW ZEALAND
NEW ZEALAND DOMAIN NAME REGISTRY LIMITED

So what’s it all about?

Route hijacking

- Illegitimate takeover of groups of IP addresses by corrupting Internet routing tables, often by:

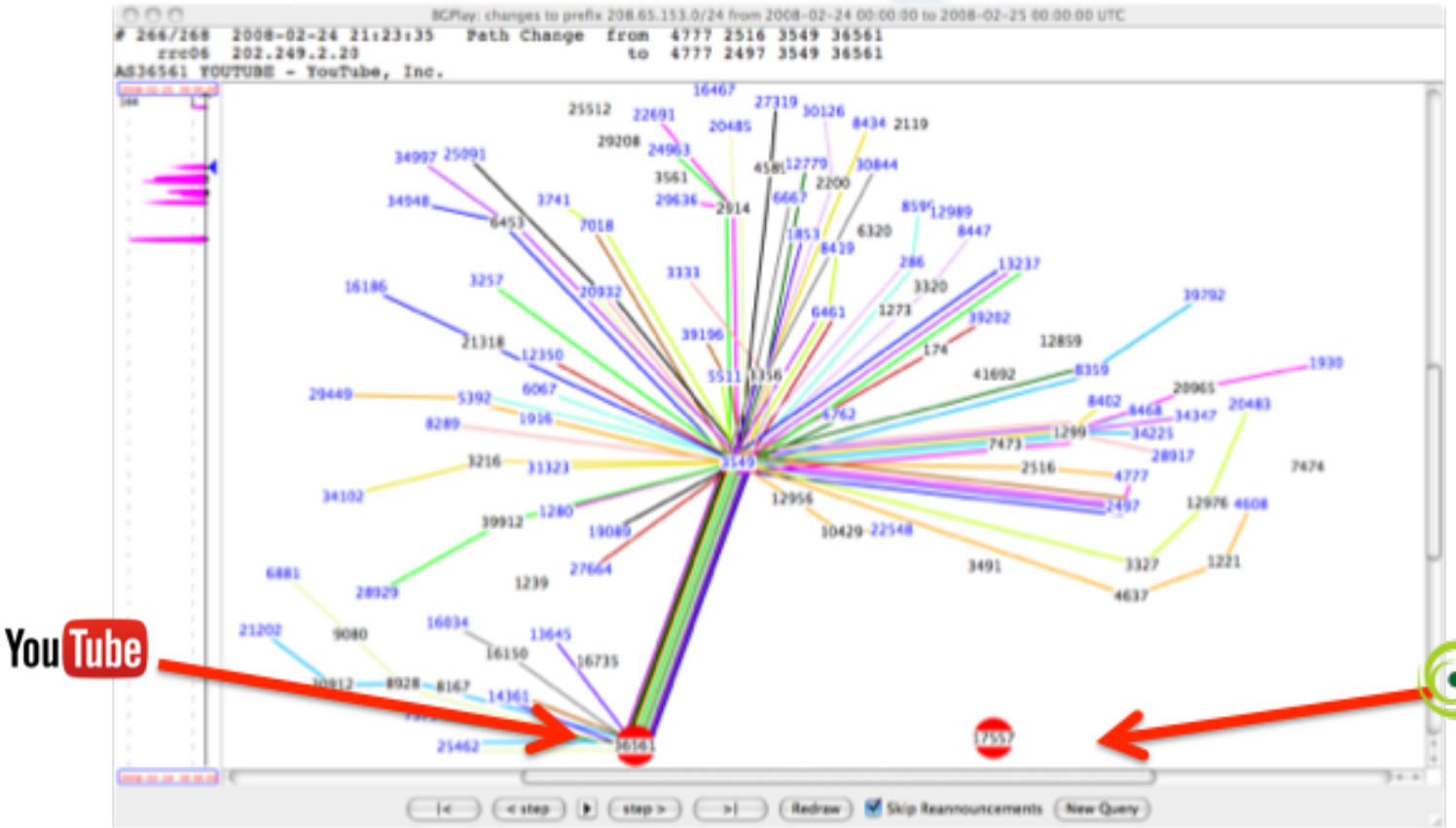
- Originating routes you're not meant to

Pakistan becomes YouTube

- Back in 2008
- AS17557 (Pakistan Telecom) starts announcing 208.65.153.0/24 (YouTube)
- Misguided attempt at censorship

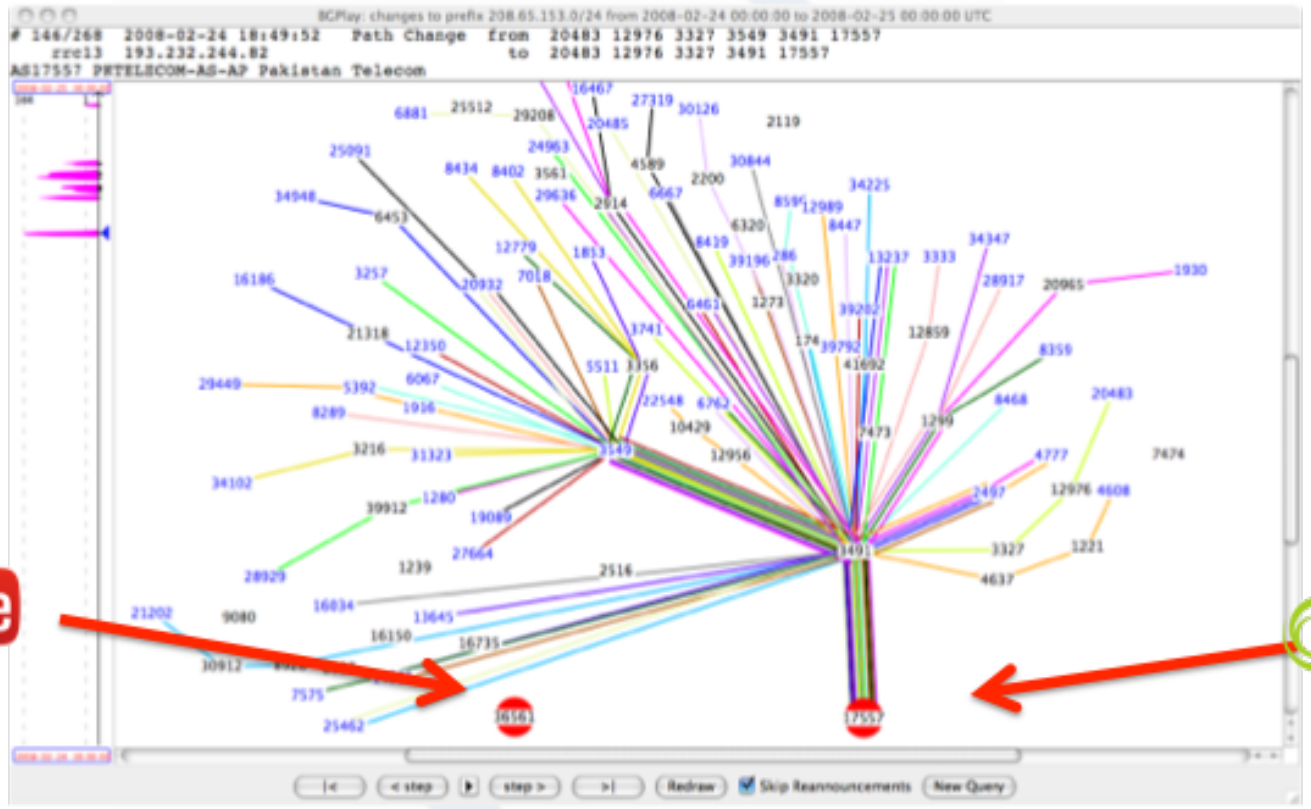
- https://www.ripe.net/internet-coordination/news/industry-developments/youtube-hijacking-a-ripe-ncc-ris-case-study

Normal YouTube



NZITF December 2014

Whoops



YouTube

ptcl hello to the future

NZITF December 2014

15 % of global Internet traffic for 18 minutes

2010

REPORT TO CONGRESS

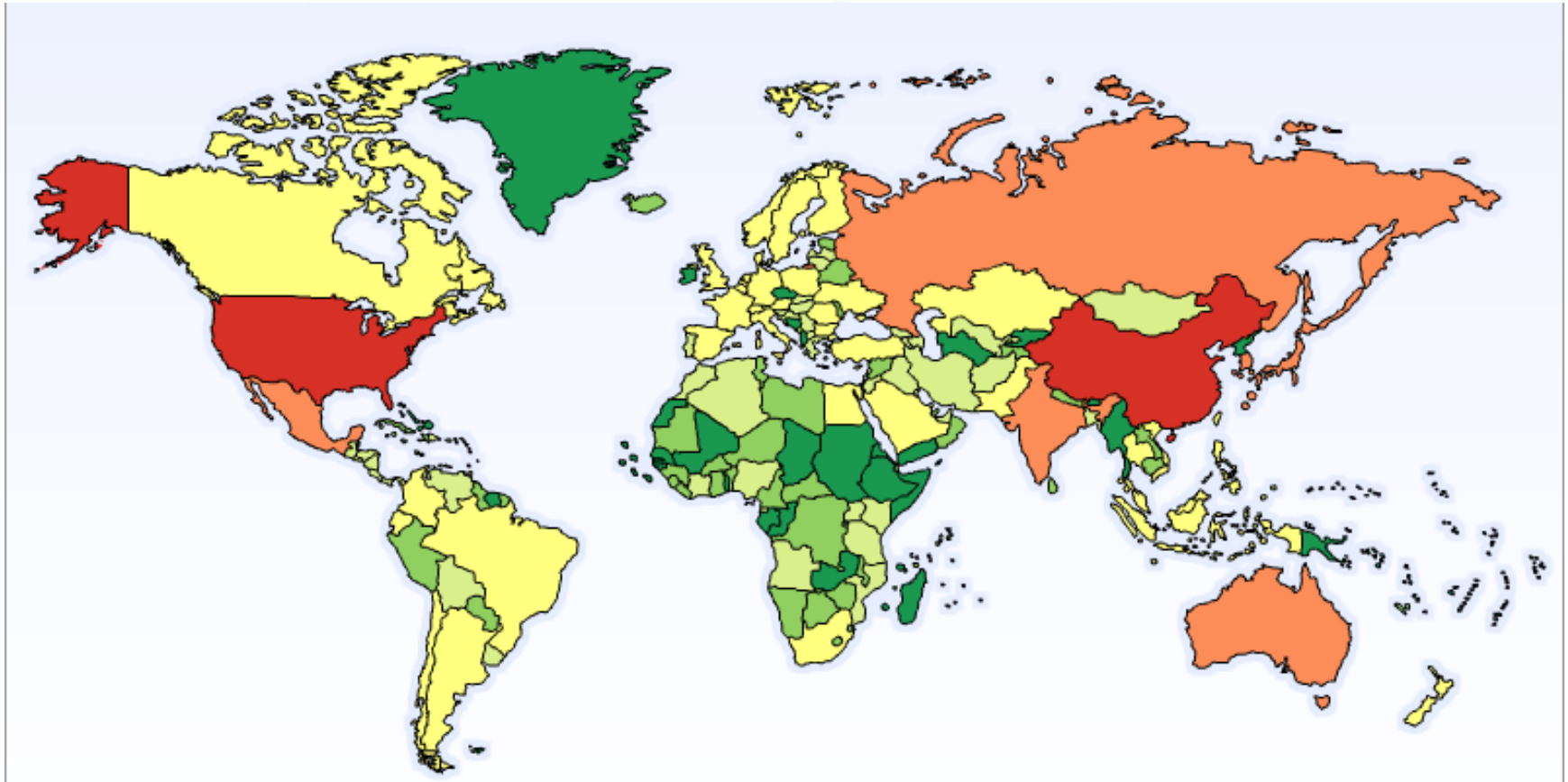
of the

U.S.-CHINA ECONOMIC AND SECURITY REVIEW COMMISSION

Interception of Internet Traffic

For a brief period in April 2010, a state-owned Chinese telecommunications firm "hijacked" massive volumes of Internet traffic.* [114] Evidence related to this incident does not clearly indicate whether it was perpetrated intentionally and, if so, to what ends. However, computer security researchers have noted that the capability could enable severe malicious activities.[115]

Global impact



http://research.dyn.com/2010/11/chinas-18-minute-mystery/

Now that’s odd

- In this redirection all the traffic that went into China came back out again!
- Nothing broke!

- Almost too ‘perfect’ a mistake

Indosat redirection

- April 2014
- Leaked 320,00 routes
- Including Akamai
- DDoS'd themselves
- Some networks more than 50% of routed traffic going to Indosat.

The New Threat: Targeted Internet Traffic Misdirection

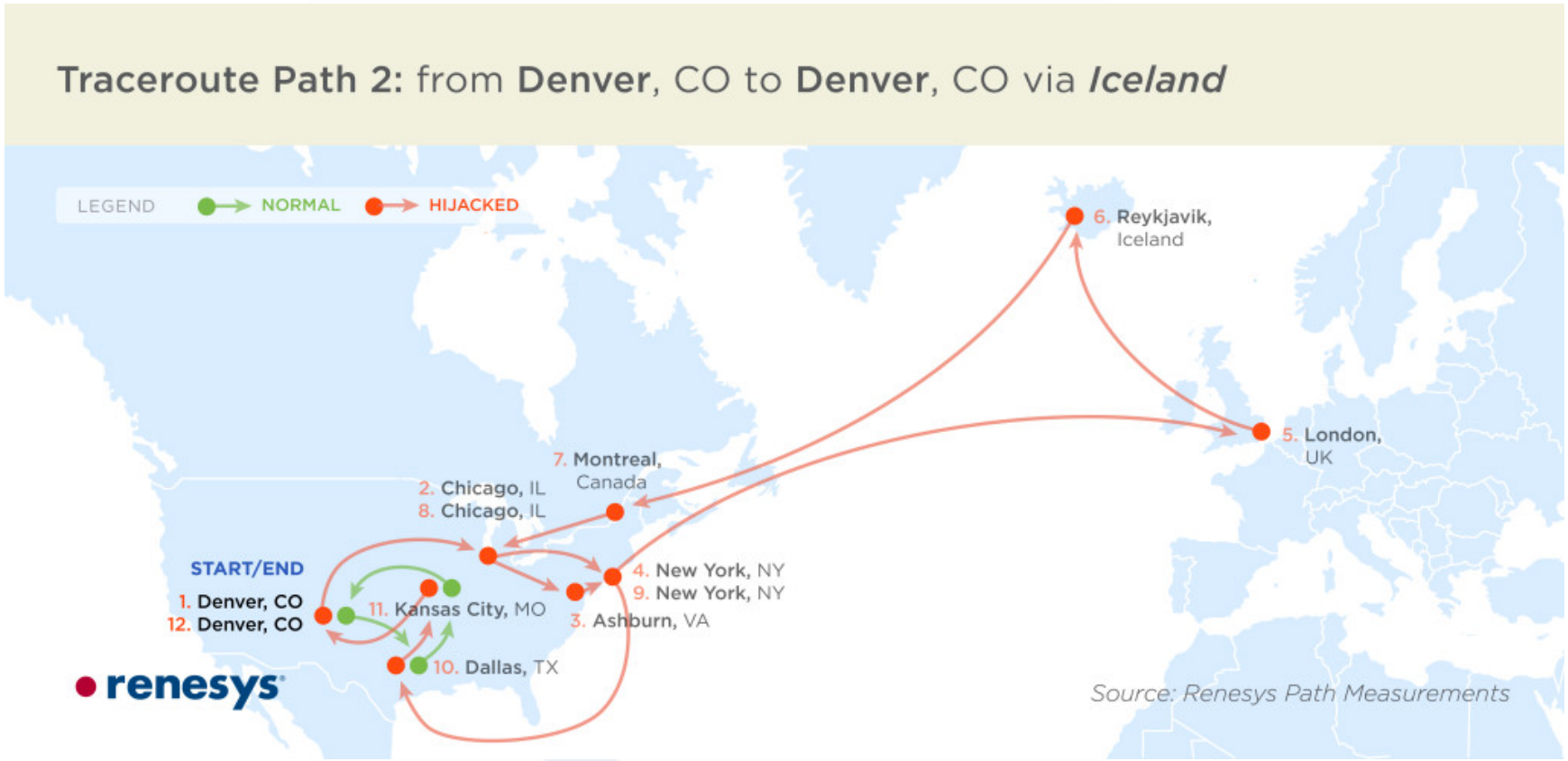
- Observed live Man-In-the-Middle (MITM) hijacks on more than 60 days in 2013
- About 1,500 individual IP blocks have been hijacked, in events lasting from minutes to days, by attackers working from various countries

- http://www.renesys.com/2013/11/mitm-internet-hijacking/

Belarus redirection

http://www.renesys.com/2013/11/mitm-internet-hijacking/

Icelandic redirection



http://www.renesys.com/2013/11/mitm-internet-hijacking/

How does RPKI help?

Three things

- Signing
- Validation
- Policy

Step 1 - Signing

- Get your address space signed
  - more specifically your routes
- Asserts only you can originate the routes
- Analogous to DNSSEC but different

Signed object - ROA

- Route Origination Authentication
  - Also called:
    - Route Origin Attestation
    - Route Origin Assertion
- Generated by your RIR based on your trust relationship

Four things in a ROA

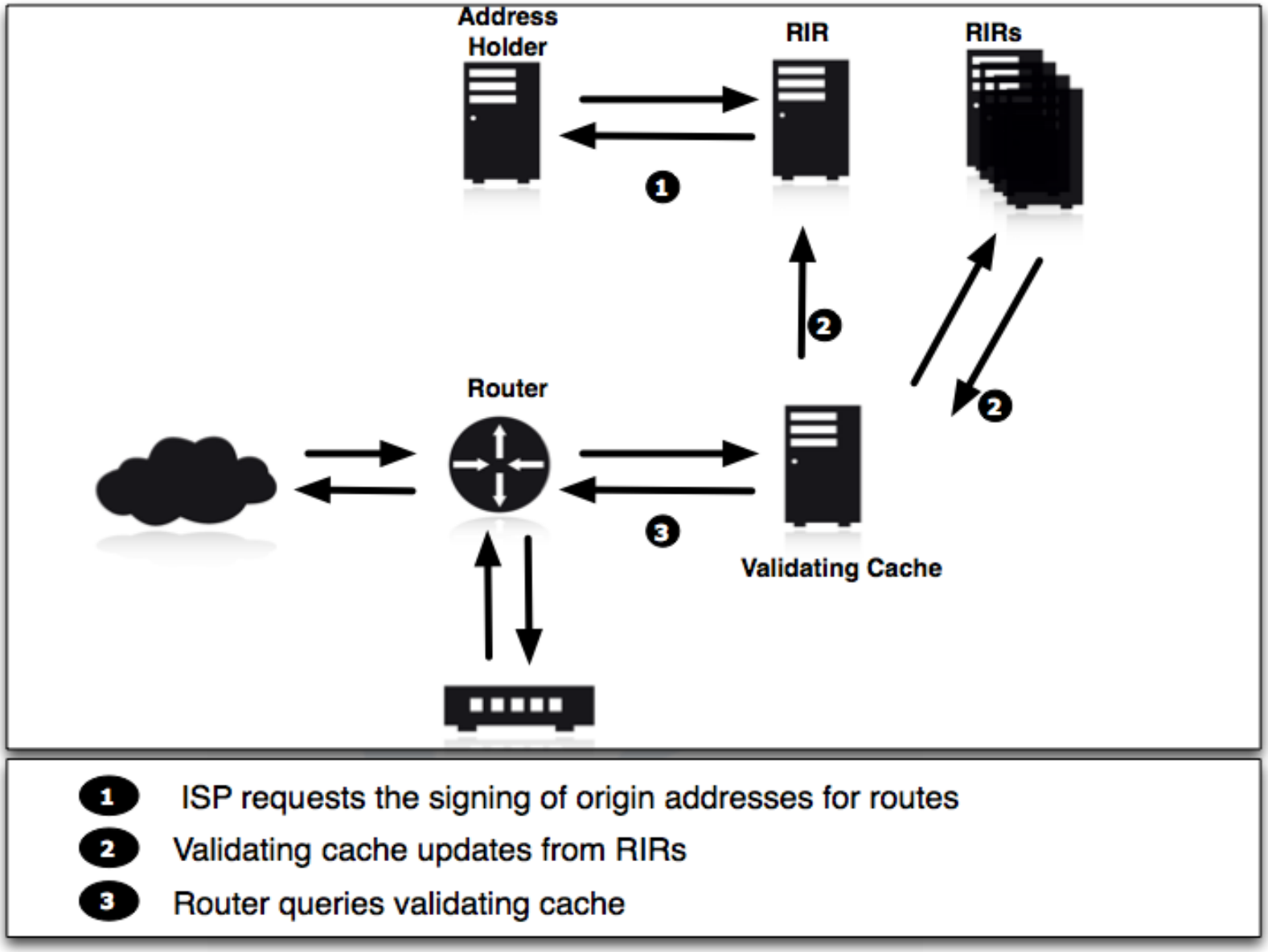
1. AS Number
2. IP address block
3. Largest prefix advertised
4. Valid period

RIRs as signing authorities

- RIRs are globally recognised signing authorities
- An address block holders trust relationship is with their RIR.
- The membership relationship is the trust relationship
- An address holder can request their resource records (ROA) signed by the RIR

Step 2 - Validation

- Validating caches are used
  - analogous to DNS resolvers.
- Routers validate against the cache
- Caches query RIR caches for ROAs


Address Holder
RIR
RIRs
1
2
2
Router
3
Validating Cache
1 ISP requests the signing of origin addresses for routes
2 Validating cache updates from RIRs
3 Router queries validating cache

Three responses from validator

1. Valid
2. Invalid
3. Not Known

Policy

- Choose your own routing policy
- Decide how to act for each response
- May block invalid routes
- May decide to do nothing

Interested?

Help from NZRS

- We run a validating cache as part of general Internet measurement.
- We will make appropriate data available
  - for reuse and research.
  - hope to report on where RPKI is
- The validating cache is open:
  - validator.rpki.net.nz

Any questions?

Jay Daley, jay@nzrs.net.nz

Better still, talk to the research team:

Sebastian Castro, sebastian@nzrs.net.nz

Jamie Horrell, jamie@nzrs.net.nz