Route Servers and BGPSEC

IETF-81, SIDR WG, 28-Jul-2011

chris.hall@highwayman.com

Route Servers and Internet Exchanges

- Route Server solves the $O(n^2)$ connection problem
  - new user is automatically connected to existing users
  - existing users are automatically connected to new ones
- Essential properties:
  - transparency – RS connection equivalent to connecting directly
    - anything less inhibits use – and use is subject to “network effect”
  - some per-client policy support (“peering-matrix”)
    - if only we had draft-ietf-idr-add-paths…
  - see: draft-jasinska-ix-bgp-route-server
- Deployment
  - Large IXs in Europe – 200..300+ clients (each)
  - Has become “standard issue” for IXs at all scales

Route Servers and BGPSEC

- Currently some RS filtering of incoming routes
  - from filtering bogons up to filtering based on IRR
- Clients announce own and customer routes
- Some (perhaps partial) transit
- IXes and RSes
  - significant parts of the infrastructure
  - not simply bilateral exchange of routes which go no further
  - allies in the push toward ubiquitous adoption

Hence: this pitch for Route Server support to be a requirement.

General Requirements

- Transparency – in particular:
  - AS Path Length must not be changed by the RS

    Currently: AS Path is not changed, so the RS is **invisible**

    There is no shame in being a Route Server Client, but…

    …the bigger boys tend not to be

- Ease of use
  - Configure and forget – unless picky about who to peer with
    - automatic connection of new clients
  - No special equipment or software at the client end
  - Minimal configuration at the client end

(1) Route Server as Proxy

- Each RS Client creates a key for the RS to use on its behalf
  - Currently the only obviously available option
    - does not require any further function in any part of the system
  - Preserves all current properties of an RS – transparent and invisible

BUT:

Requires complete trust in the RS administrator

- RS administrators are generally Good Chaps…

  …so this is a plausible back-stop

(2) Route Server Signs for Itself

- RS uses its own key(s) to sign outgoing AS Paths
  - Requires AS Path Length calculation to ignore the RS' AS
    - which is new function in BGPSEC
  - Maintains all current properties of RS
    - is even easier to use than an RS proxy signer – client does not even have to create a separate key
  - Does not require absolute trust in the RS

EXCEPT: not <u>invisible</u>

…so, need to establish whether invisibility is a strong requirement – to not "reveal more than is currently revealed in the operational inter-domain routing environment" ?

…happy to canvas opinion and report

(3) Otherwise ?

- Client signs for all possible destinations
  - cf: add-paths – mechanism must be standard for BGPSEC
  - BUT: also requires RS to be able to advise client of current possible destinations (for “configure and forget”), in-band with BGPSEC (for “no special equipment/software”)
  - also: requires client border router to be ready to generate all possible signatures, which could delay adoption
- RS communicates out-of-band with Client signer
  - to meet “no special equipment/software”, this could be built-in to the system that collects/distributes signing keys ?
  - requires extra configuration to set up the out-of-band connection.
- Other, much better approaches ?

In conclusion

- Support for Route Servers should be a requirement… discuss.

- But of what:
  - BGPSEC the protocol ?
  - BGPSEC the system – including RPKI, RPKI/Router Protocol, BGPSEC the protocol, et al ?
  - some other name for the system ?