Explorations in the Public Peering Address Space

NANOG 41 Lightning Talk

John Kristoff
jtk@ultradns.net
Peer discovery using traceroute
Trace selection and collection

- Obtain list of exchange netblocks from peeringdb
  - Over 125 prefixes, mostly /24's
- Private shell nodes running traceroute
- http://www.scriptroute.org
- Combat Perl code to parse output
Speakeasy, AS 23504

- Equinix Ashburn (59)
- Equinix San Jose (40)
- Equinix Dallas (19)
- Equinix Chicago (41)
- Equinix Los Angeles (28)
Exchange Peering Graph

Equinix Ashburn (sample)
Netblock visibility

- Most networks seem to announce these netblocks
  - Sometimes globally, sometimes internally
  - Sometimes even into the global multicast RIB
- Why?
  - Some services only available via those addrs?
    - e.g. Route servers
  - Default redistribute connected?
- Do we care?
- Go see route-views and looking glass sites for detail
Final thoughts

- Enables easier BGP spoofing attacks?
- What if someone announced a more specific?
- Geographic DDoS attack vector?
- Network enumeration/privacy issues?
- Helps researchers better understand topology?
- Exchange operator market research?
- Hints for optimizing peering selection/placement?
- Facilitates transit theft
- Would published peering maps be of interest?