Quantitative Analysis of BGP Route Leaks

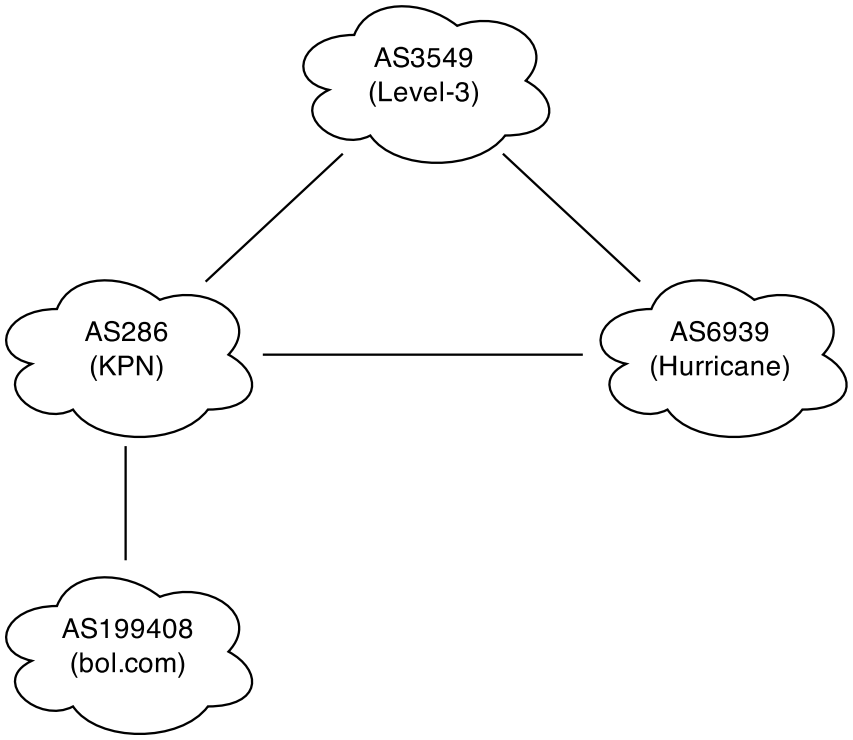
Benjamin Wijchers
Benno Overeinder

The Problem With Route Leaks

- Route leaks are not route hijacks (in my definition)
  - route hijack: originate prefixes you do not “own”
  - route leaks: forward BGP announcements you shouldn’t according policies
- Route leaks not easy to detect
- Potential security risk
  - examples Belarusian and Iceland traffic misdirection

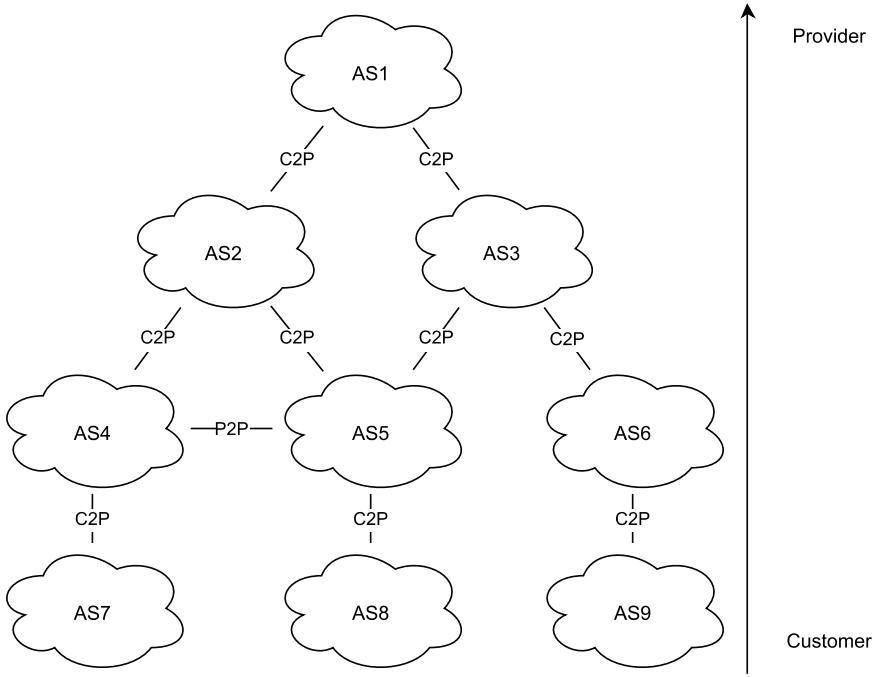
Business Relations and Route Leaks

- ASes have business relationship
  - Client pays provider
  - Provider provides transit
  - Peers share client routes
- Routing should reflect business relations
  - But in practice not always the case
    - Route leak

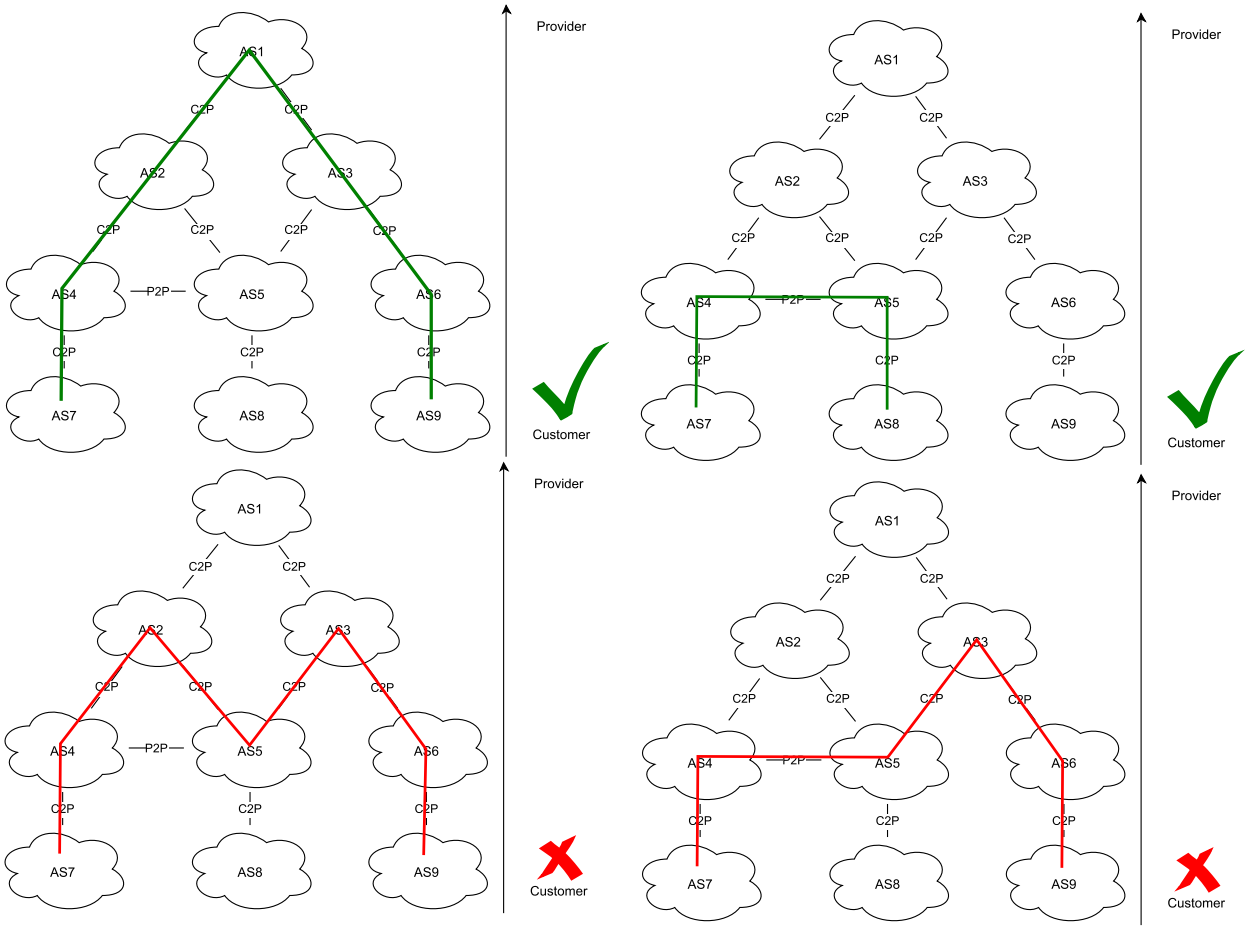


The Valley Free Rule

- Relations between ASes:
  - Customer-provider
  - Peer-peer
  - Siblings
- Valley Free Rule:
  - C2P(*) – P2P (1|0) – P2C (*)

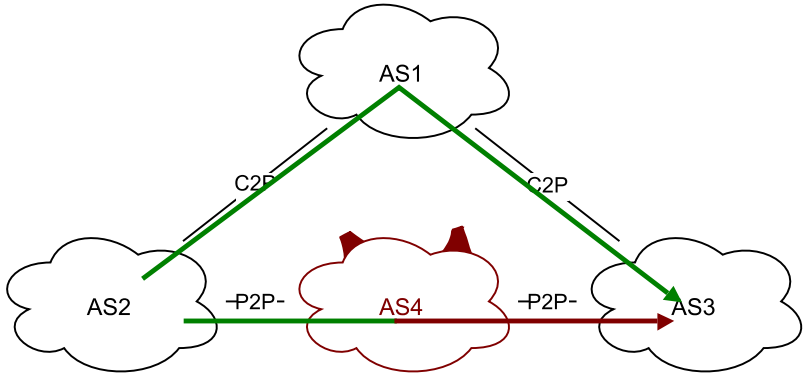


The Valley Free Rule



Origins of Route Leaks

- Misconfiguration
- Malicious
  - Man in the middle
- Intentional
  - Indirect peering
    - IXP
    - Research / Educational
  - Complex relations



- Find characteristics for categorizing

Why Analyse Them?

- Counter-measures planned
  - part of ongoing IETF SIDR WG activities
  - discussions in the context of BGPSEC
- Traffic routes incorrectly causing:
  - ASes paying for transit of other ASes clients
  - Potentially slower connections
  - Potential hijacking of data (mitm)
- Not much statistics available

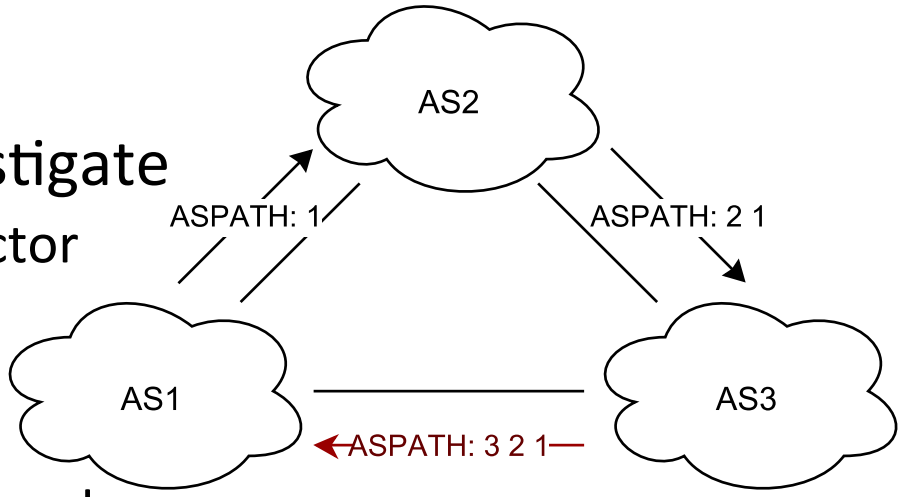
Previous Work

- Jared Mauch
  - Detection without relation data
  - Not much statistics
    - List of route leaks
    - General counts

updates.20140630.1915.bz2	2014-06-30 19:33:11.424139	103.18.32.0/23	11686 19782 174 701 2914 45300 45312	701	3	701
updates.20140630.1915.bz2	2014-06-30 19:33:11.417319	103.18.32.0/23	852 6453 701 2914 45300 45312	701	3	701
updates.20140630.1915.bz2	2014-06-30 19:33:11.40613	103.18.32.0/23	11686 3356 701 2914 45300 45312	701	3	701
updates.20140630.1915.bz2	2014-06-30 19:33:11.398365	103.18.32.0/23	3356 701 2914 45300 45312	701	3	701
updates.20140630.1915.bz2	2014-06-30 19:33:11.38199	103.18.32.0/23	3549 701 2914 45300 45312	701	3	701
updates.20140630.1915.bz2	2014-06-30 19:33:11.3807	210.209.87.0/24	11686 19782 4323 701 6453 45474 174 17444	6453	3	45474
updates.20140630.1915.bz2	2014-06-30 19:33:11.379346	210.209.87.0/24	2497 701 6453 45474 174 17444	6453	3	45474
updates.20140630.1915.bz2	2014-06-30 19:33:11.377608	210.209.87.0/24	11686 19151 3356 6453 45474 174 17444	6453	3	45474
updates.20140630.1915.bz2	2014-06-30 19:33:11.374013	210.209.87.0/24	852 1299 6453 45474 174 17444	6453	3	45474
updates.20140630.1915.bz2	2014-06-30 19:33:11.371406	192.58.232.0/24	11686 4436 2914 701 3356 6629 6629 6629 6629	701	3	701
updates.20140630.1915.bz2	2014-06-30 19:33:11.370065	192.58.232.0/24	852 2914 701 3356 6629 6629 6629	701	3	701

Detecting Valleys

- Relations between ASes
  - Non-disclosure agreement
  - Inferred relations
- BGP data dumps to investigate
  - RIPE Remote Route Collector
  - RouteViews
- ASPATH attribute
  - Shows path of ASes traversed

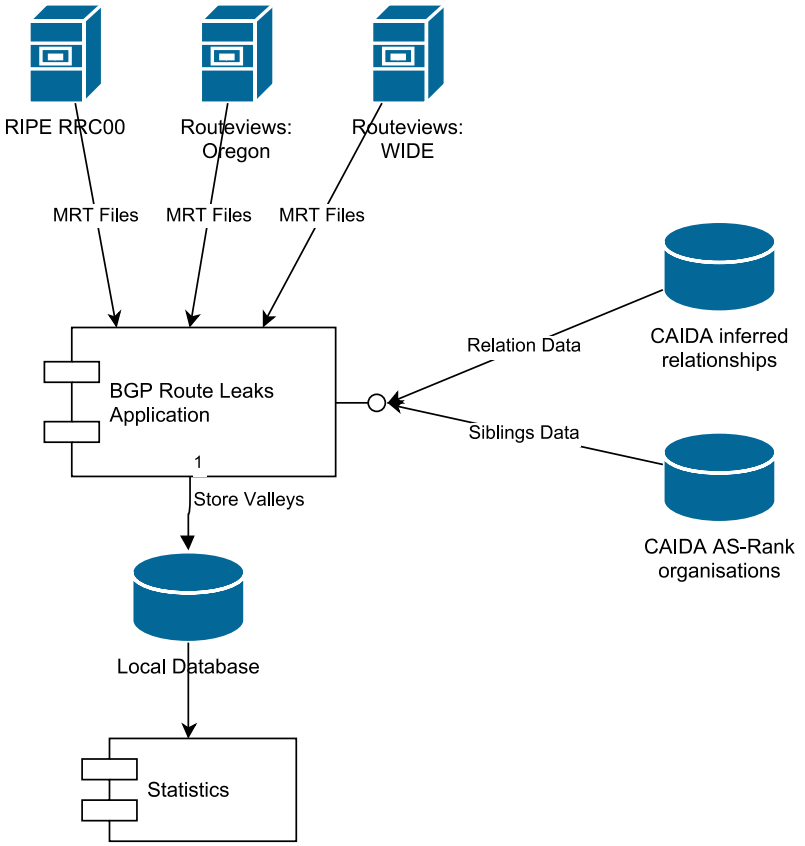


Relation Inferences

- Lixin Gao
  - Valley free rule
- Ricardo Oliveira et al (UCLA)
  - Every non-tier-1 AS is (indirect) client (or peer) of tier-1
- Matthew Lucky et al (CAIDA)
  1. C2P to reach global connectivity
  2. Peering clique at top of topology
  3. No cycles of C2P links
- CAIDA chosen for project
  - Validation of relations
  - No valley freeness used in inference

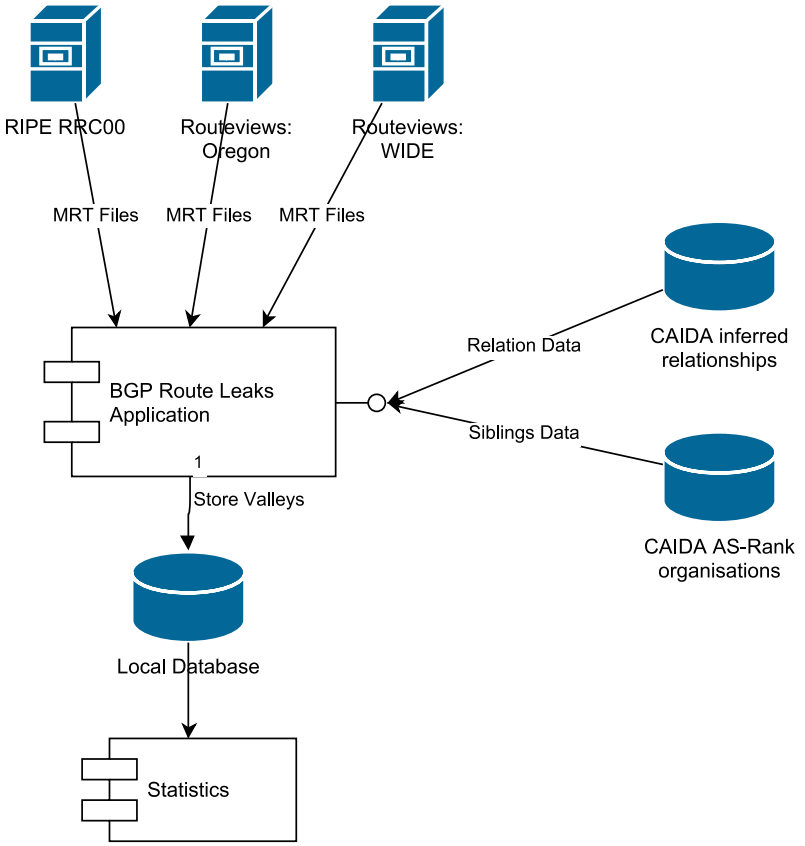
Methodology

- CAIDA relationship data
  - Combined with siblings data
- BGP MRT files from
  - RIPE RIS RRC00
  - Routeviews WIDE
  - Routeviews Oregon
- Custom BGPdump
- Detecting valleys



Methodology (2)

- All valleys in database with
  - violation type
    - e.g. P2C-C2P
  - AS Leak triplet
    - leaked from, leaker and receiver
  - duration
    - check updates for same AS & prefix

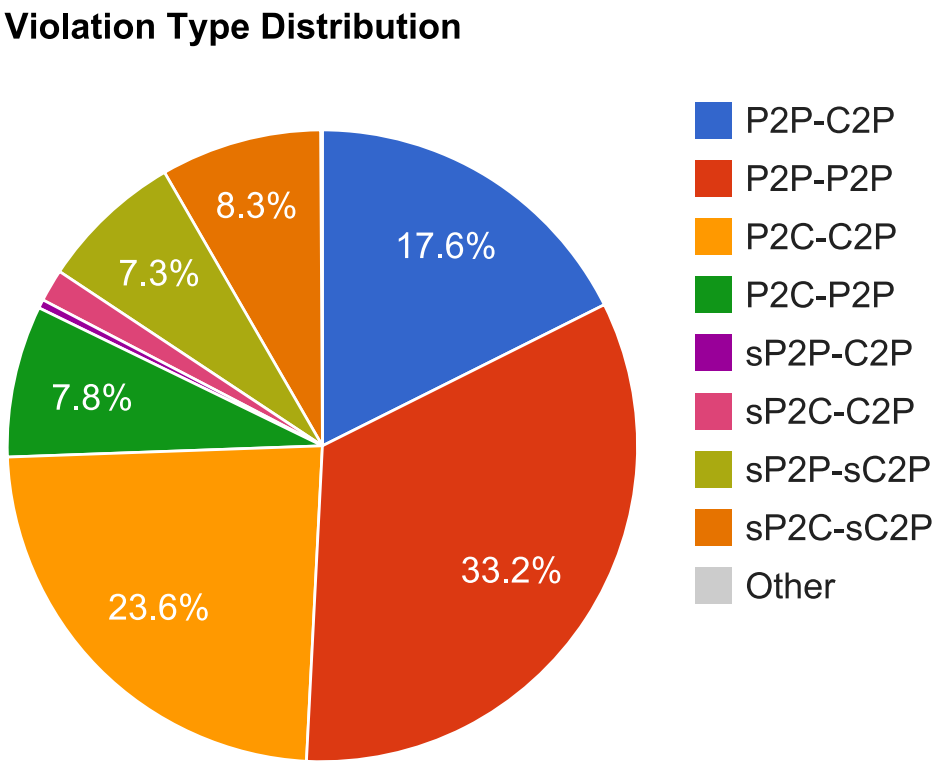


About the results

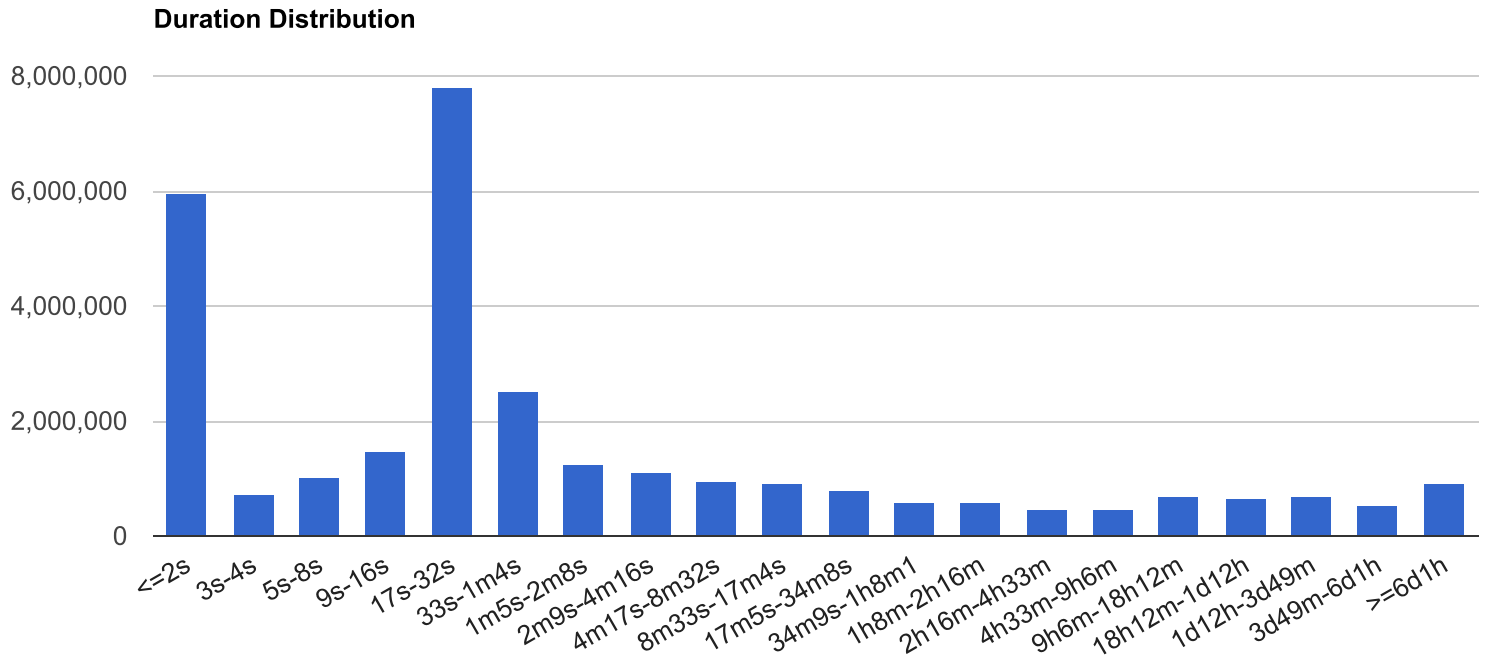
- Current results from 1 month from RIPE, Oregon and WIDE
  - ~4% of routes investigated valley
  - Over 36 000 000 valley announces detected

Distribution of Violation Types

- Top left area are no real valleys
- P2P-P2P occurs most frequently



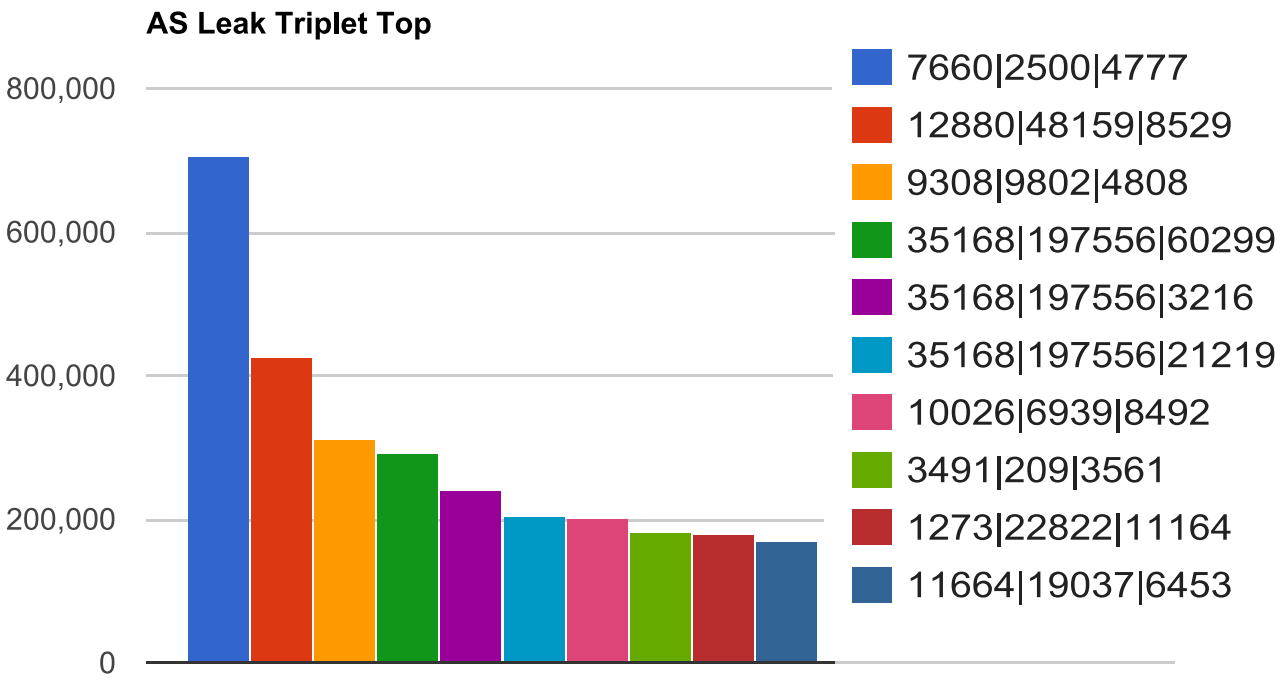
Distribution of Durations



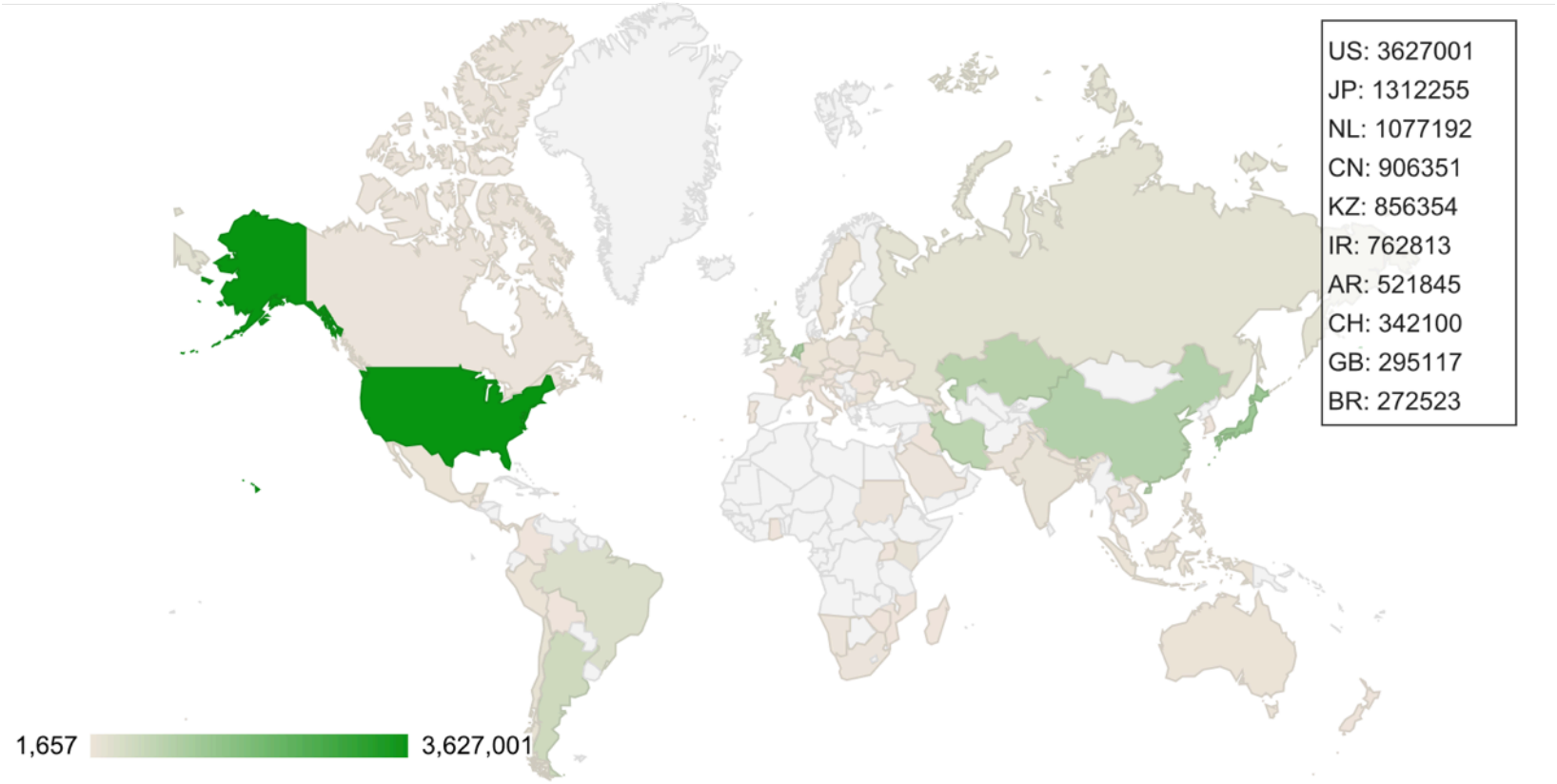
- Peaks at <2 seconds and 17-32 seconds
  - Default MRAI Cisco: 30 seconds
  - Probably unintentional

Most Frequent Leak Triplets

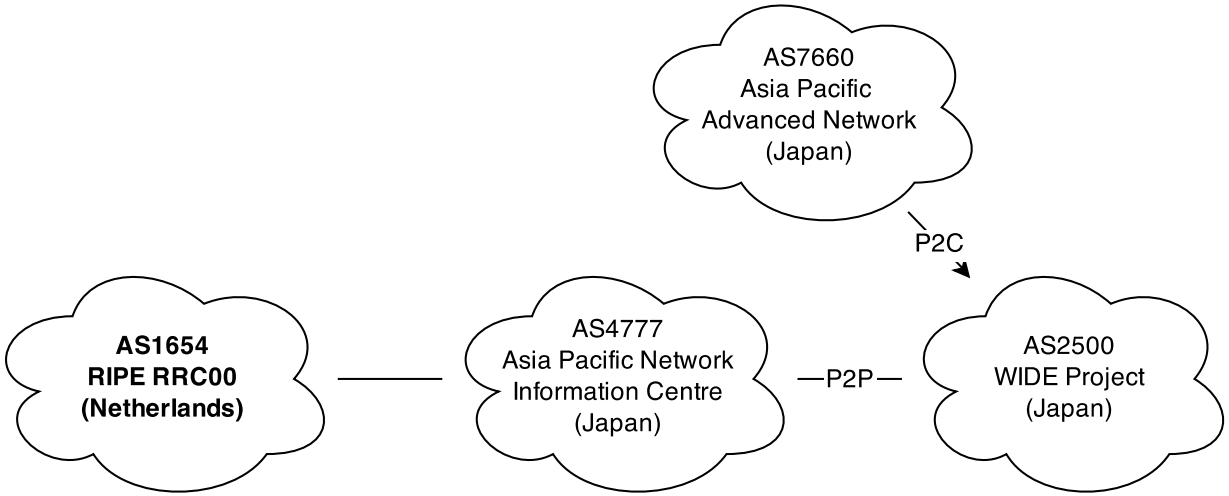
- Duration > 1 minute
- ~12% of valleys found in top 10
- Next challenge
  - categorize in classes



Geography of Most Frequent Leaks

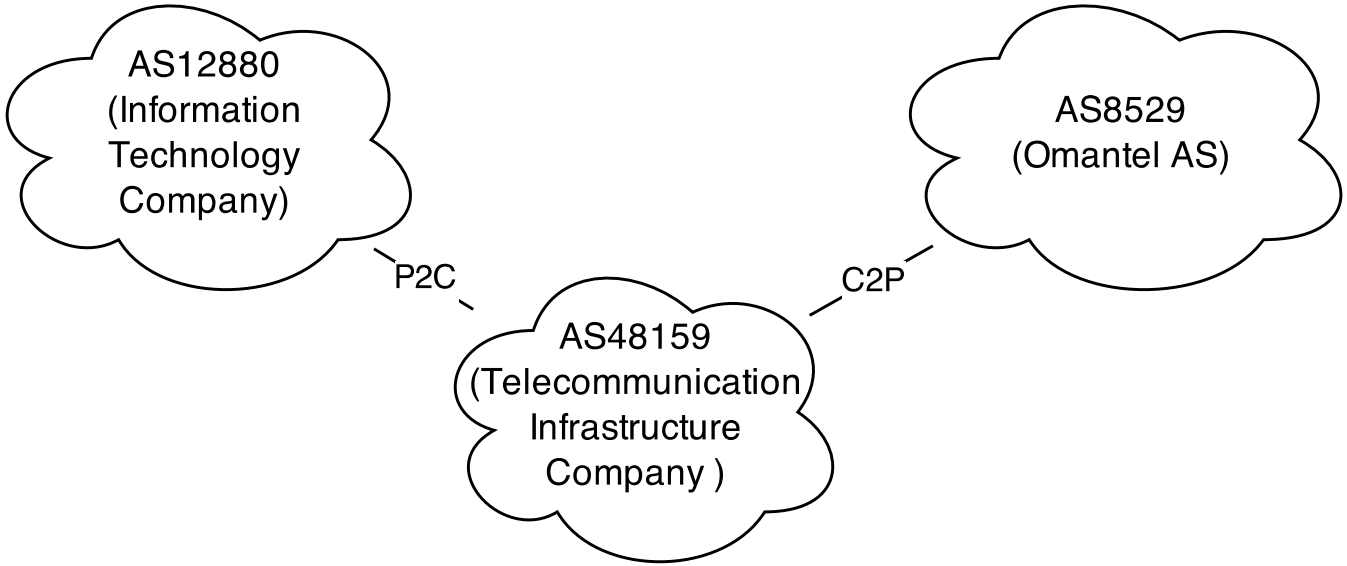


Top Leaks Further Investigated



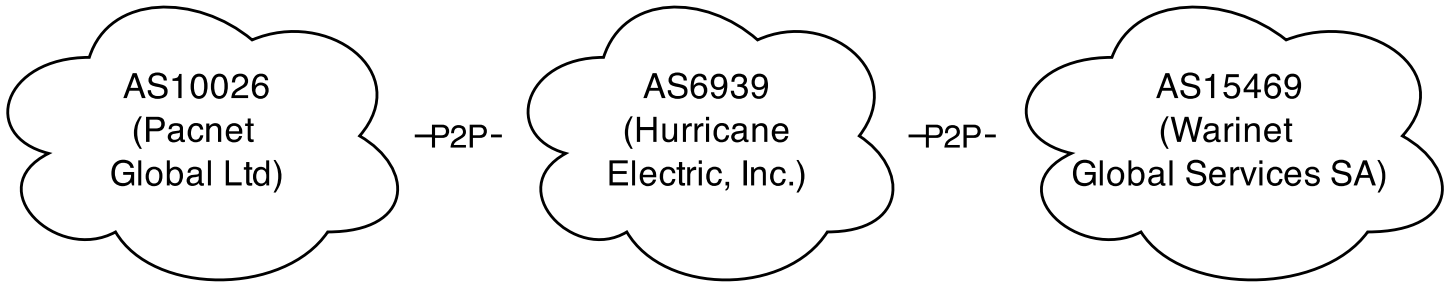
- WIDE appears to provide transit for peer APNIC
- APAN, WIDE and APNIC are all research ASes
  - who commonly have “special” relationships
- Likely intentional behaviour

Top Leaks Further Investigated



- Both AS12880 and AS48159 from Iran
  - possible merge -> sibling
  - cannot say for certain with data available
- WHOIS AS12880 no mention of AS48159
  - WHOIS AS48159 mentions AS12880 as default route

Top Leaks Further Investigated



- Different policies IPv4 and IPv6
  - mp-import: afi ipv6.unicast from AS6939 action pref=150; accept ANY
  - mp-import: afi ipv4.unicast from AS6939 action pref=150; accept AS-HURRICANE

Conclusion

- Most route leaks are peer routes propagated to other peers
- ~65% valleys are very short-lived (< minute)
  - but ~6% very persistent (> day)
- About 12% AS triplets reoccur frequently in found route leaks
  - most of them “special” relations
  - not enough knowledge to define others

Future Work

- Broader date range
  - monthly reports, history with less storage
- Separate relation data IPv4/IPv6
- RPSL data usage for automatic detection of complex relations

Questions

- Acknowledgments
  - Jared Mauch
  - Stella Vouteva