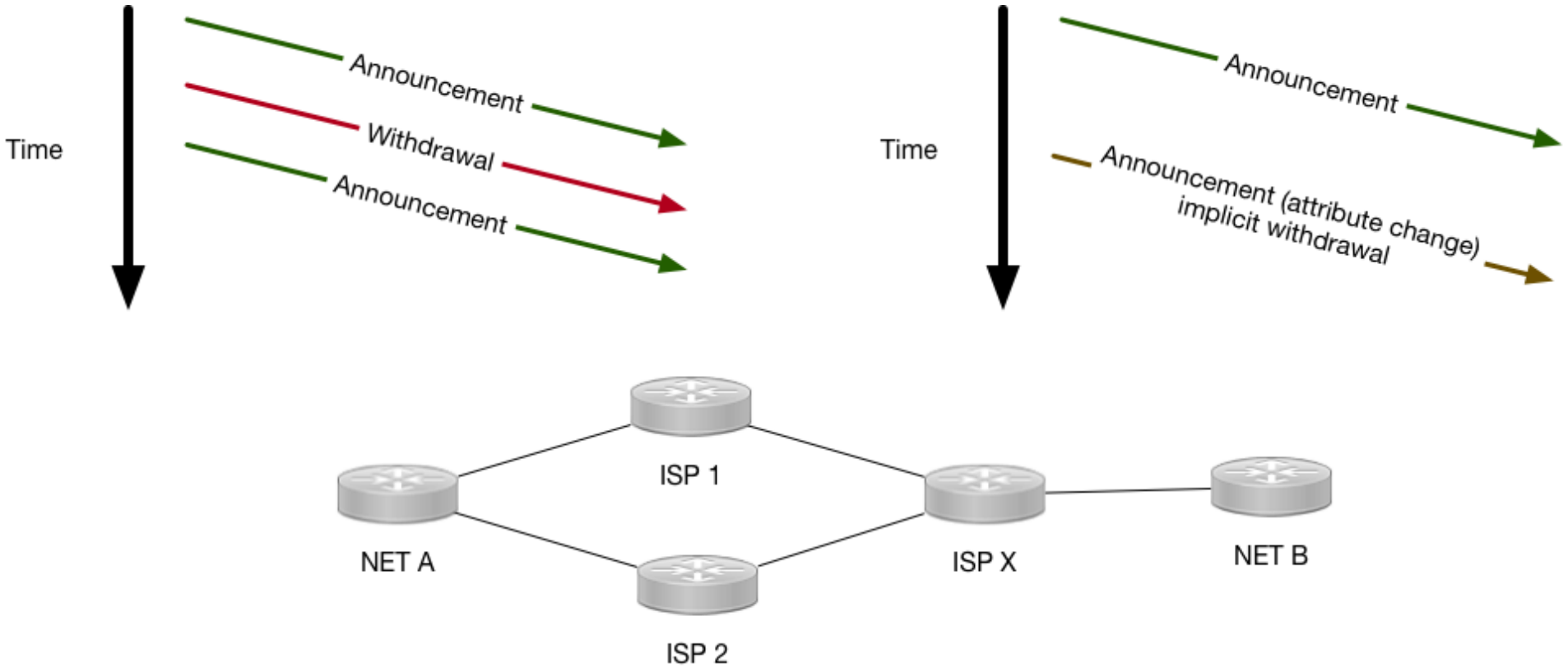
Reconsidering Route Flap Damping with the Help of BMP

John Kristoff <jtk@depaul.edu>
Chris Kanich <ckanich@uic.edu>

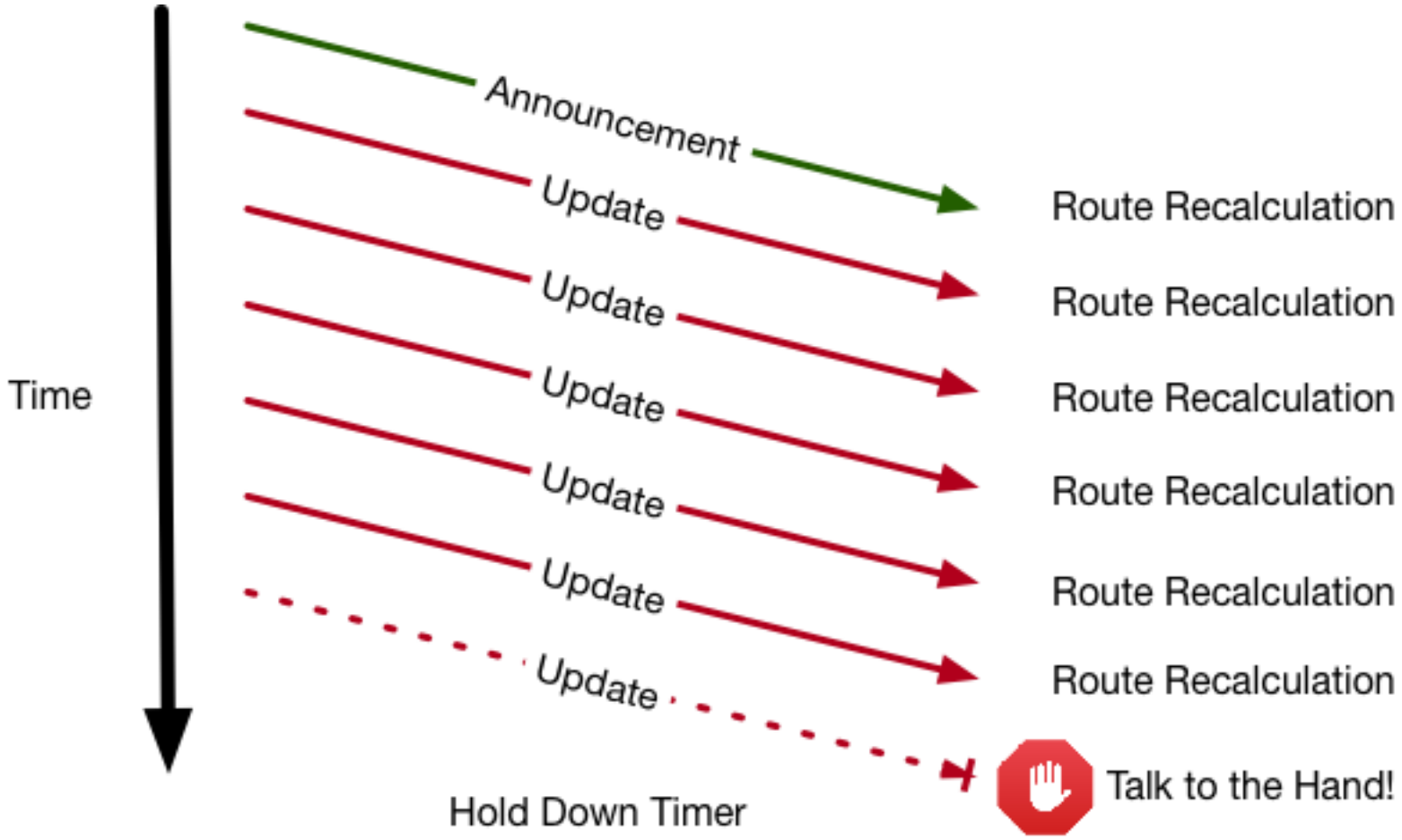
Outline

- Review of Route Flapping and Damping
- Overview of BGP Monitoring Protocol (BMP)
- Research Motivation
- Experiment Environment
- Observations
- Future Work

Route Flapping



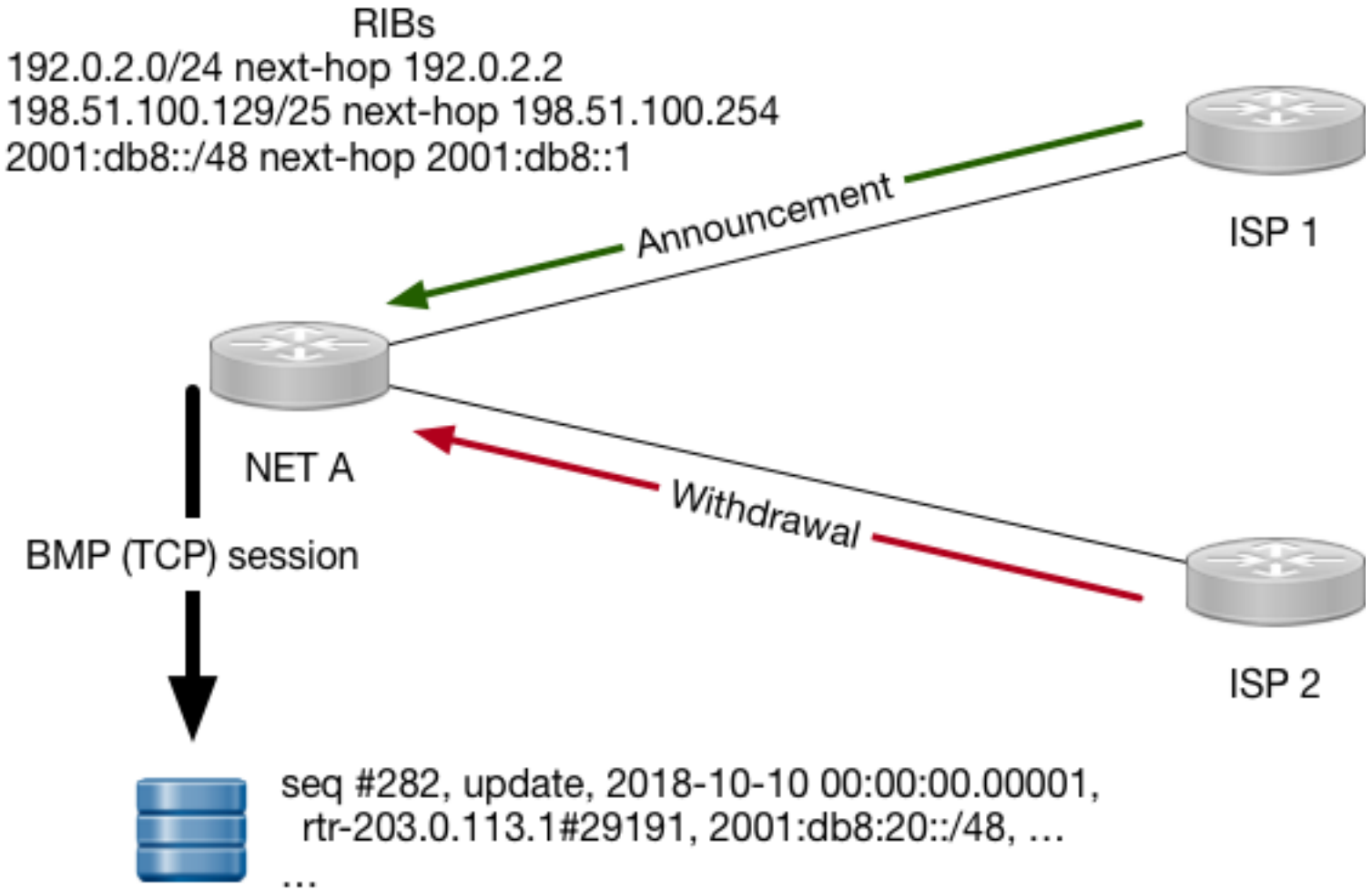
Damping


Time
Announcement
Update
Update
Update
Update
Update
Update
Route Recalculation
Route Recalculation
Route Recalculation
Route Recalculation
Route Recalculation
Route Recalculation
Hold Down Timer
Talk to the Hand!

Flapping and Damping Activity

- Making Route Flap Damping Usable, IETF RFC 7196 (based on 2011 PAM paper)
- BGP Route Dampening: obsolete or still used in the industry, Noction blog, August 1, 2018
- Anecdotally: damping not widely deployed today
- Note: past activity focused primarily on router CPU effects and problems with loss of connectivity. No indication of a route flapping as a security issue.

BGP Monitoring Protocol (BMP)



BMP Summary

- Export BGP stats/status//updates to a monitor
- IETF RFC 7854 published June 2016
- Shipping code in Junos and IOS for a few years
- One-way TCP data session from monitored router
- Replaces screen scrape (`show [ip] route` scripts)
- Key, new analytical capabilities:
  - Real-time BGP updates per peer
  - pre- and post- import/export policy results

Motivation

- Config cleaning: 15+ year-old BGP damping policy
  - Community BCPs updated multiple times
  - No documented problems from damped routes
- Advice from netops and current RFC co-authors
  - Diametrically opposed positions on damping
- This sounds like a research opportunity
  - And an opportunity to play BMP

Experiment Environment

- MX-10/80 Junos 14.1R7.4 with HE.net upstream

```
routing-options {
    bmp {
        station monitor.example.edu {
            local-address 192.0.2.1;
            connection-mode active;
            station-address 198.51.100.1;
            station-port 1790;
    }
}
```

- Bitten by Juniper PR1154017 (rpd crash)
- Started to look at SNAS, settled on pmbmpd

BMP Monitor System

- Debian 32 GB RAM, 500 GB HDD VM
- /usr/local/etc/pmbmpd.conf

```
bmp_daemon: true
bmp_daemon_port: 1790
bmp_daemon_allow_file: pmbmpd.allow.conf
bmp_daemon_msglog_file: log_$peer_src_ip
bmp_dump_file: dump.$peer_src_ip%Y%m%d%H%M
bmp_dump_refresh_time: 300
```

- Ran for ~3 weeks
- ~7.4 GB log file (some BGP restarts for maintenance)

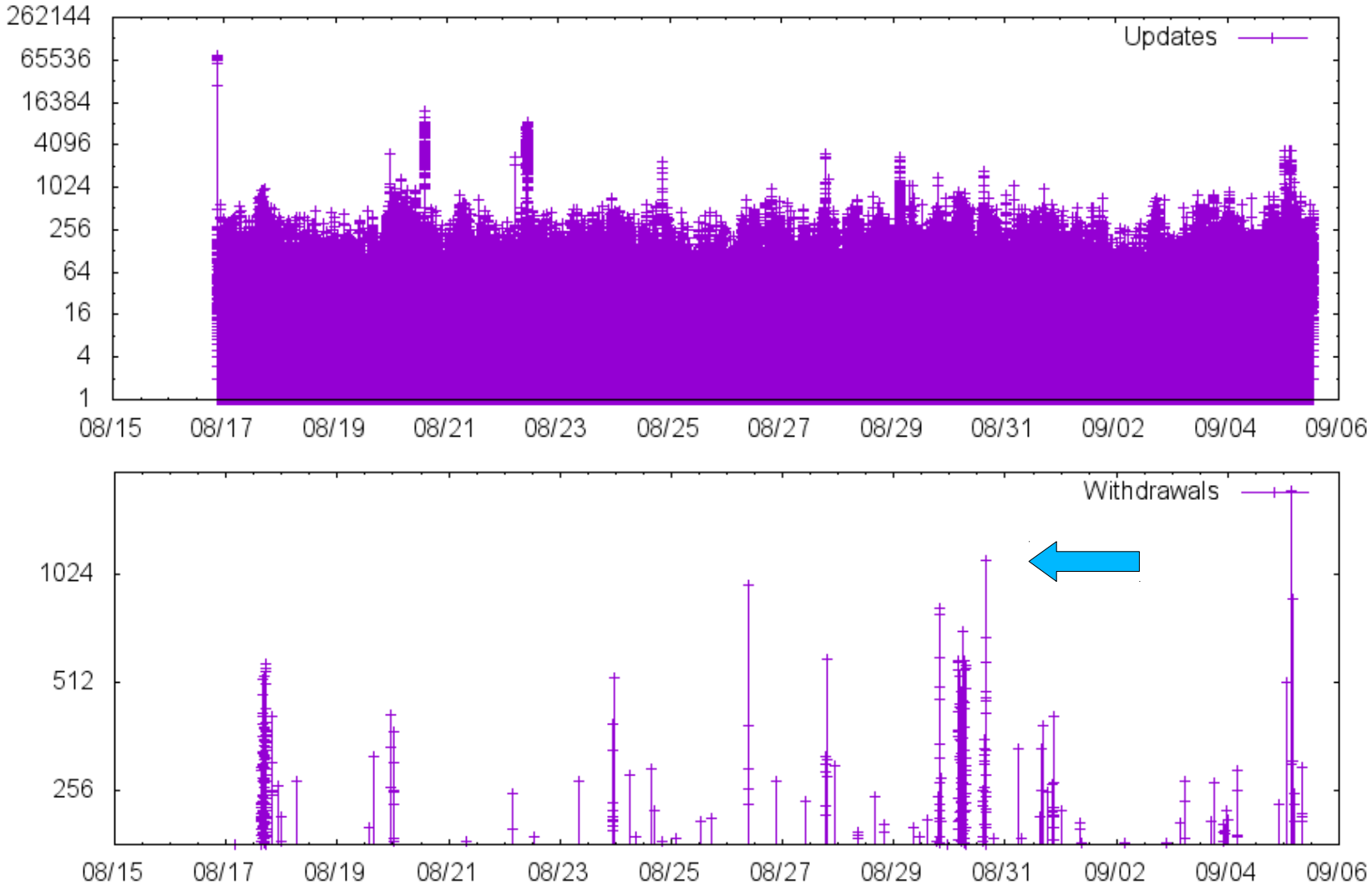
Rudimentary JSON to DB Import

```
data = []
conn = psycopg2.connect("dbname=bmp")
cur  = conn.cursor()

for line in fileinput.input():
    data    = json.loads(line)
    columns = data.keys()
    values  = [data[column] for column in columns]
    insert_statement =
              'INSERT INTO bmp (%s) values %s'
    cur.execute(insert_statement,
        (AsIs(','.join(columns)), tuple(values)))

conn.commit()
cur.close()
conn.close()
```

Updates and Withdrawals



2018-08-30 Withdrawals Anomaly

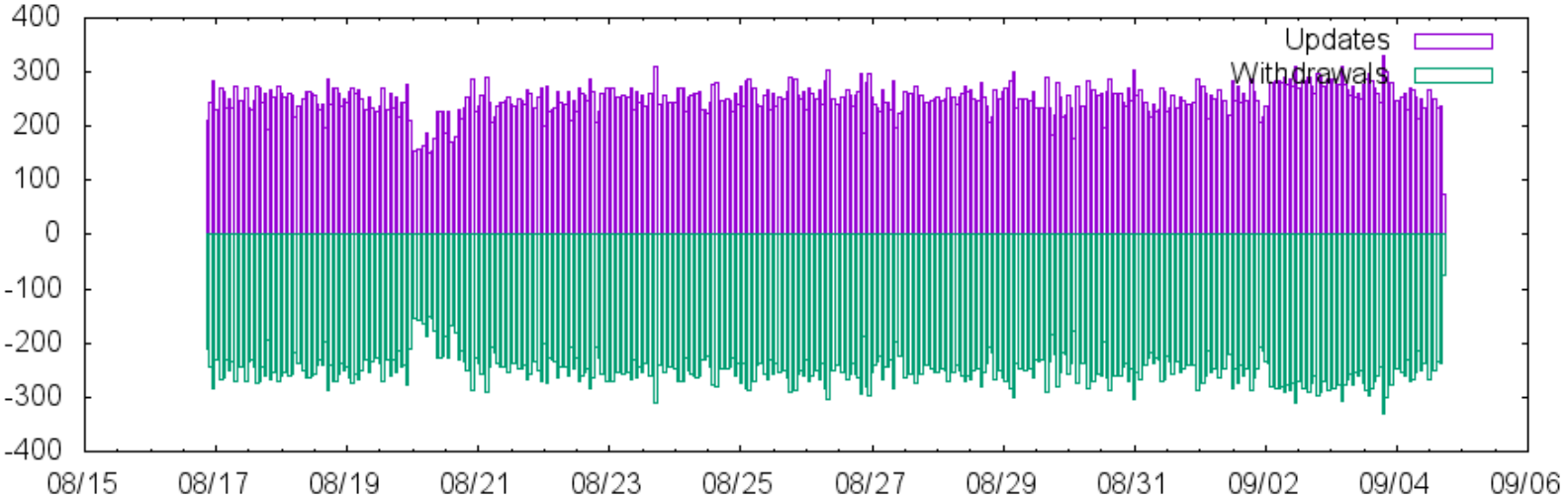
- 1126 distinct withdrawals
- 221 distinct AS_PATH withdrawals… hmmm
- 157 prefixes withdrawn by AS_PATH:

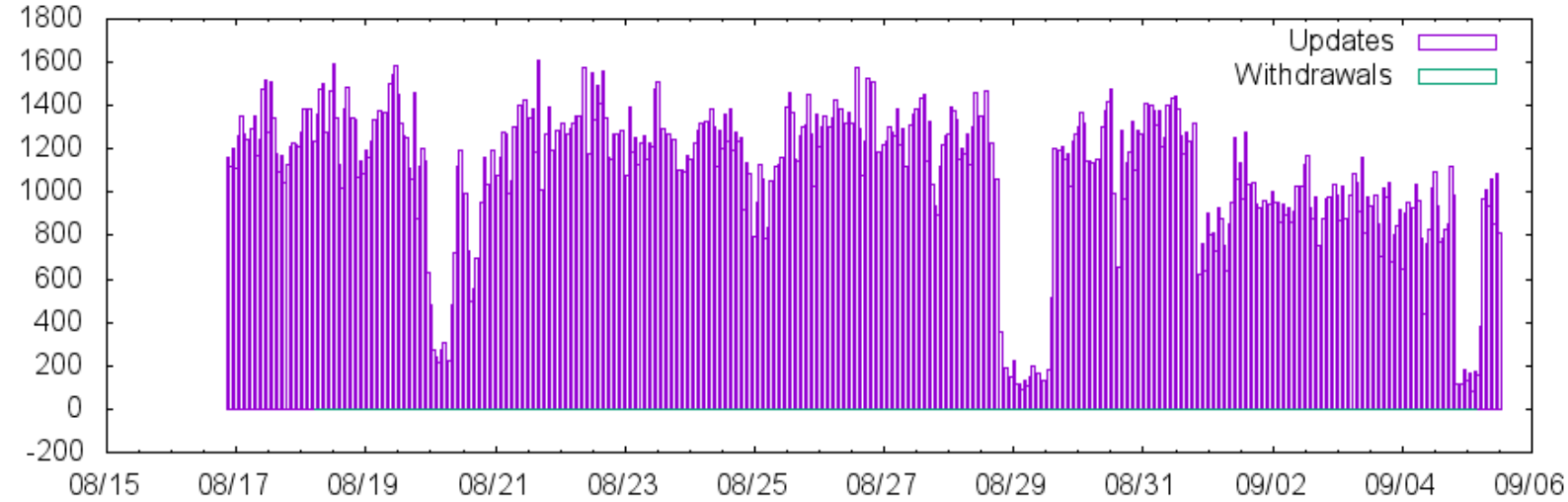
  “6939 262589 262195 10481”
- Instability for AS 10481 prefixes for 1-2 days
- But enough instability to dampen? Maybe not

Are We Concerned Yet? No.

- Route churn isn't particularly problematic today
- MX-10/80 CPU isn't great, but this is old hardware
- Ops prefer some instability of damped routes
- Is the instability acceptable?

Particularly Egregious Updates 64.70.30.0/24 and 128.0.164.0/22





Can Damping Be Made Usable?

- More conservative suppression values suggest yes
- But seemingly not strictly required for any net
- Can damping be used against yes? Possibly
- Its not clear whether damping should be a BCP
- Is BGP route stability a non-goal?
- Security-related concerns may be more important

Future Work

- Updating damping tested with new Junos rev
- Long term measurement of what gets damped
- Possibly propose updated talk for NANOG 75
- Much more interested in BMP generally
- Big data analysis and projects seem interesting
  - Verifying route updates with public collectors
    - and vice versa
  - Trending and detection of update pathologies
- OpenBMP/SNAS deployment