BGP, some Python, and a DB

Theo Baschak

BSides Winnipeg 2015-11-15

Slides

Reveal.js slides
ciscodude.net/presentations/bsideswpg2015-mb-bgplogger
Beamer PDF slides
ciscodude.net/presentations/bsideswpg2015-mb-bgplogger.pdf

exabgp-logger daemon project at
github.com/tbaschak/exabgp-logger

Who I Am

- Network Architect @ Daemon Defense Systems.
- Avid Open Source Software user/fanatic, and contributor.
- Obsessed with network monitoring and routing.
- Involved with several nonprofits in Winnipeg.
    1. Board of the Manitoba Internet Exchange (MBIX).
    2. Board of Coldhak
        - Coldhak is a nonprofit dedicated to furthering privacy, security and freedom of speech.

Overview

- Inspiration
- The idea
- Design
- Building the logger
- Running it
- Peering
- Scaling it up
- Scaling it futher
- Finding things
- Automating

Inspiration

- Talked about BGP hijacking in my BSidesWpg 2013 talk.
- Dyn Research blogs (formerly Renesys Corporation):
  - 2 days after BSidesWpg 2013, November 19 2013, Targeted Internet Traffic Misdirection
  - March 2015, UK traffic diverted through Ukraine
- BGPmon & BGP Stream

The idea

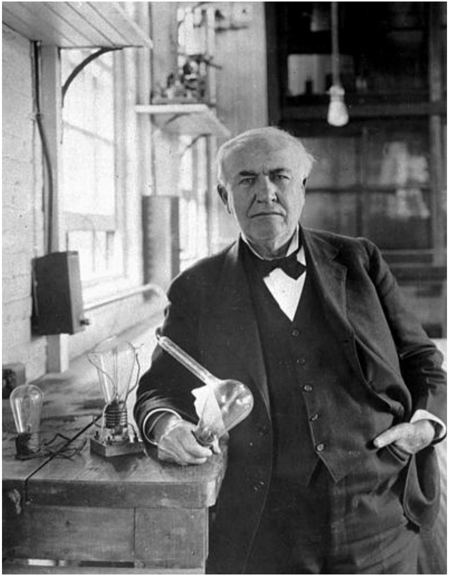

Figure 1:Edison electric light

Design

- Exabgp (the BGP, and the Python)
  - one process, per AF, per peer (v4 and v6 separate)
  - outputs BGP updates as JSON
- Couchdb (the DB)
  - stores JSON objects
  - one database per peer (v4 and v6 combined)
  - replicate each peer into common DB

Building

- Uses exabgp
  - Exabgp config defines actions for route input and output
  - Just input in this case, not advertising
  - Bash while loop to read line by line and POST to couchdb

Running

- Able to run without a peer for basic config checks
- Need a live BGP peer to start viewing BGP update record format
- First tests
  - First version just cat appended the JSON to a file so I could look at the records
- Growing Pains

Peering

0. MFNERC
1. MERLIN. Gracious statement of support on MBIX-Tech list as well.
2. 3T Systems
3. Les.net

Scaling Up

- Moved VM
- Offsite replication
- Increased size of VM and went 64bit

Finding things

-

Automating

The End

Reveal.js slides
ciscodude.net/presentations/bsideswpg2015-mb-bgplogger
Beamer PDF slides
ciscodude.net/presentations/bsideswpg2015-mb-bgplogger.pdf

exabgp-logger daemon project at
github.com/tbaschak/exabgp-logger