Measurement and Analysis for the Internet of Things

Measurement and Analysis for Protocols Research Group (maprg)
Berlin, July 18, 2016

Dave Plonka <plonka@{cs.wisc.edu,akamai.com}>

Outline

- **Case Study**: The Internet of Things Old and Unmanaged
  (with Elisa Boschi)
  https://down.dsg.cs.tcd.ie/iotsu/subs/IoTSU_2016_paper_25.pdf

- **IoTSU**: Internet of Things Software Update, June 2016
  https://www.iab.org/activities/workshops/iotsu/
  - Unconference topic:
    Measurement & Analysis for IoT
    (with Daniel Thomas)

Case Study: Netgear SNTP clients

- Flawed Routers Flood University of Wisconsin Internet Time Server (2003)
  http://www.cs.wisc.edu/~plonka/netgear-sntp/

- The Internet of Things Old and Unmanaged (Updated for 2016)
  https://down.dsg.cs.tcd.ie/iotsu/subs/IoTSU_2016_paper_25.pdf

Case Study: Affected Netgear Products

RP614v2, **RP614**: 4-Port Cable/DSL Router with 10/100 Mbps Switch
C-NET Editors' Choice, July 2002
RP614v2: upgrade to v5.13, released 2003/07/11
RP614: upgrade to v4.14, released 2003/08/20

MR814: 802.11b Cable/DSL Wireless Router
Innovations International CES, Design & Engineering Showcase Honors, 2003
MR814: upgrade to v4.13, released 2003/08/20

DG814: DSL Modem Internet Gateway
Macworld Editors' Choice
DG814: upgrade to v4.8, released 2003/07/09

HR314: 802.11a Cable/DSL High-Speed Wireless Router
HR314: upgrade to v1.4.2, released 2003/09/05

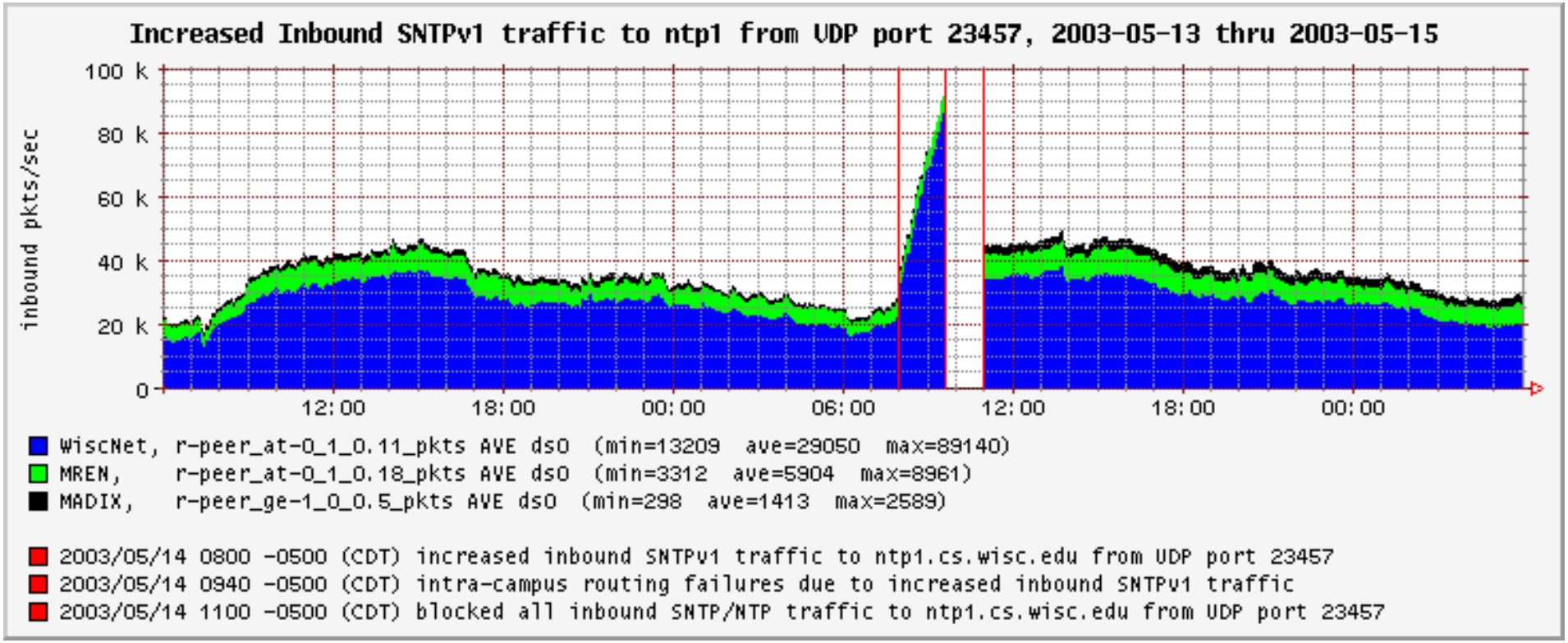
Case Study: How is this IoT?

- **What is IoT?**
  - These things are devices with homogenous configuration that are typically rapidly designed, manufactured, and deployed and that *depend on the Internet* [where such devices did not, previously.]

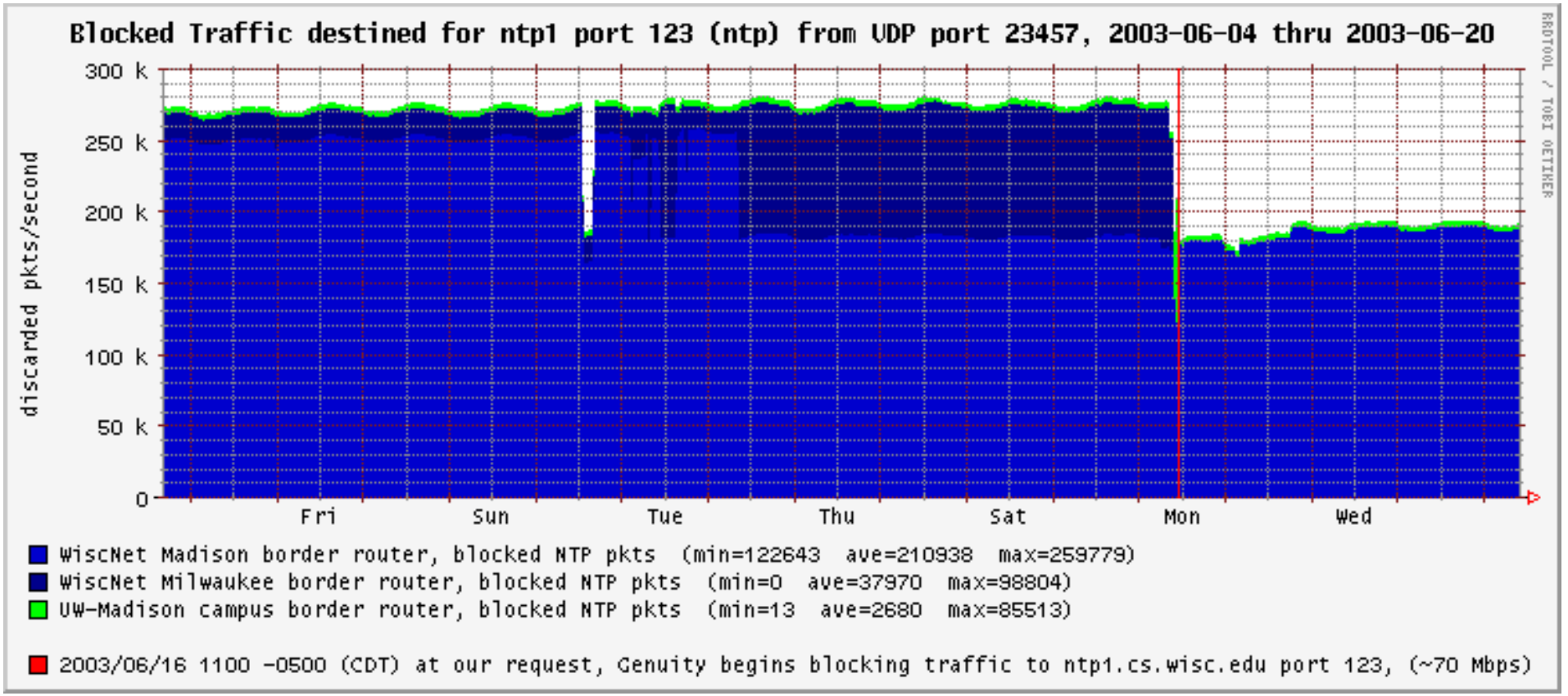
- In this case, these CPE switches/routers/access-points are curious in that they are *Internet* devices rather than merely network devices.

- We are not usually informed about the arrival of hosts on the Internet.
  - IoT presents performance, reliability, and security challenges.

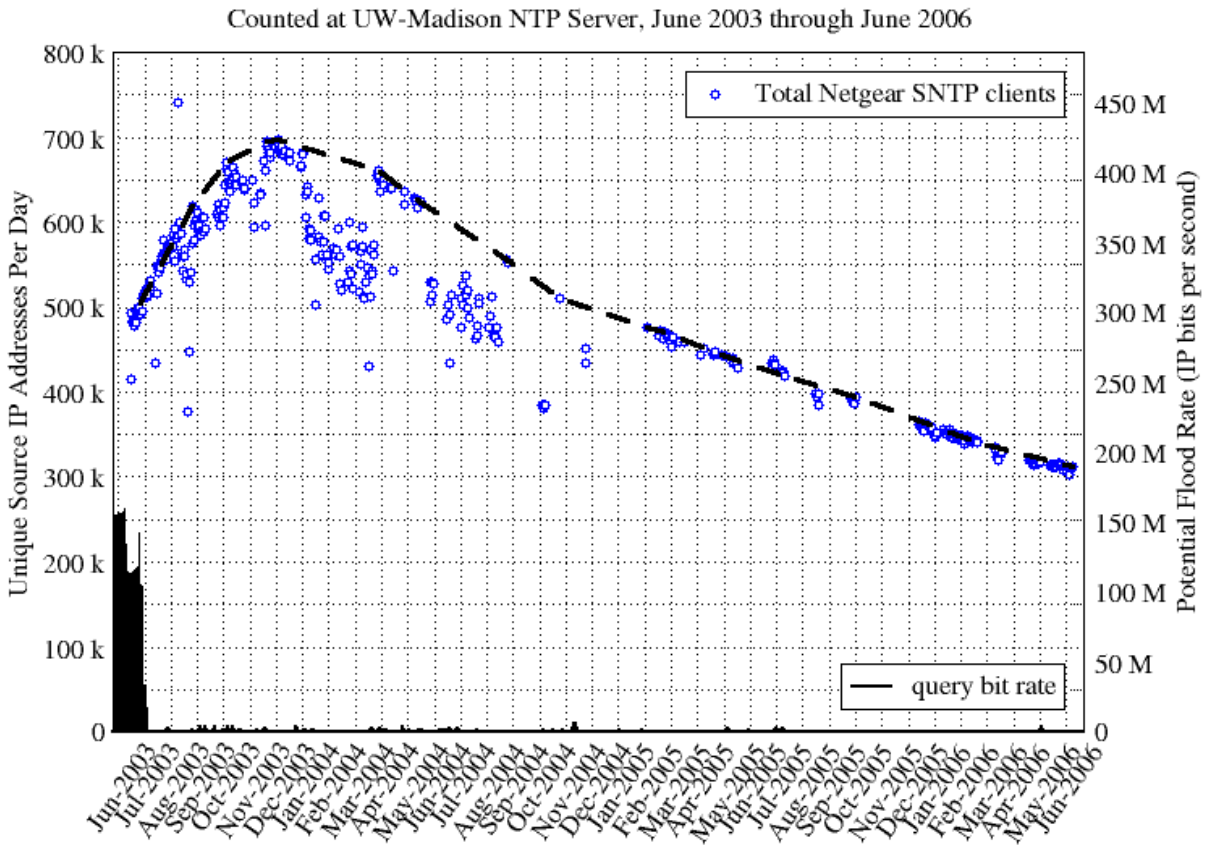
Case Study: The Flood Arrives, May 2003

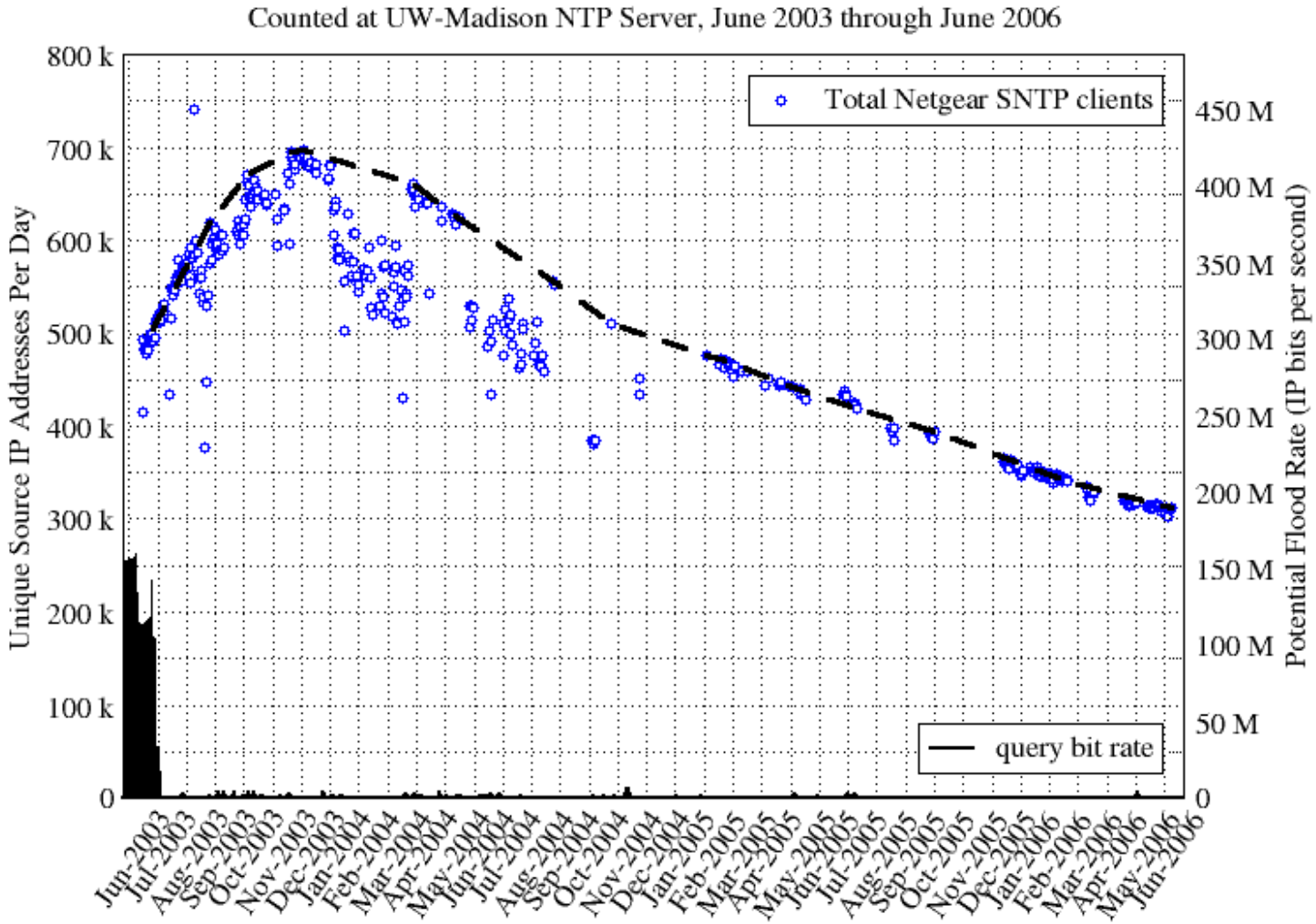


Case Study: The Flood Continues, June 2003

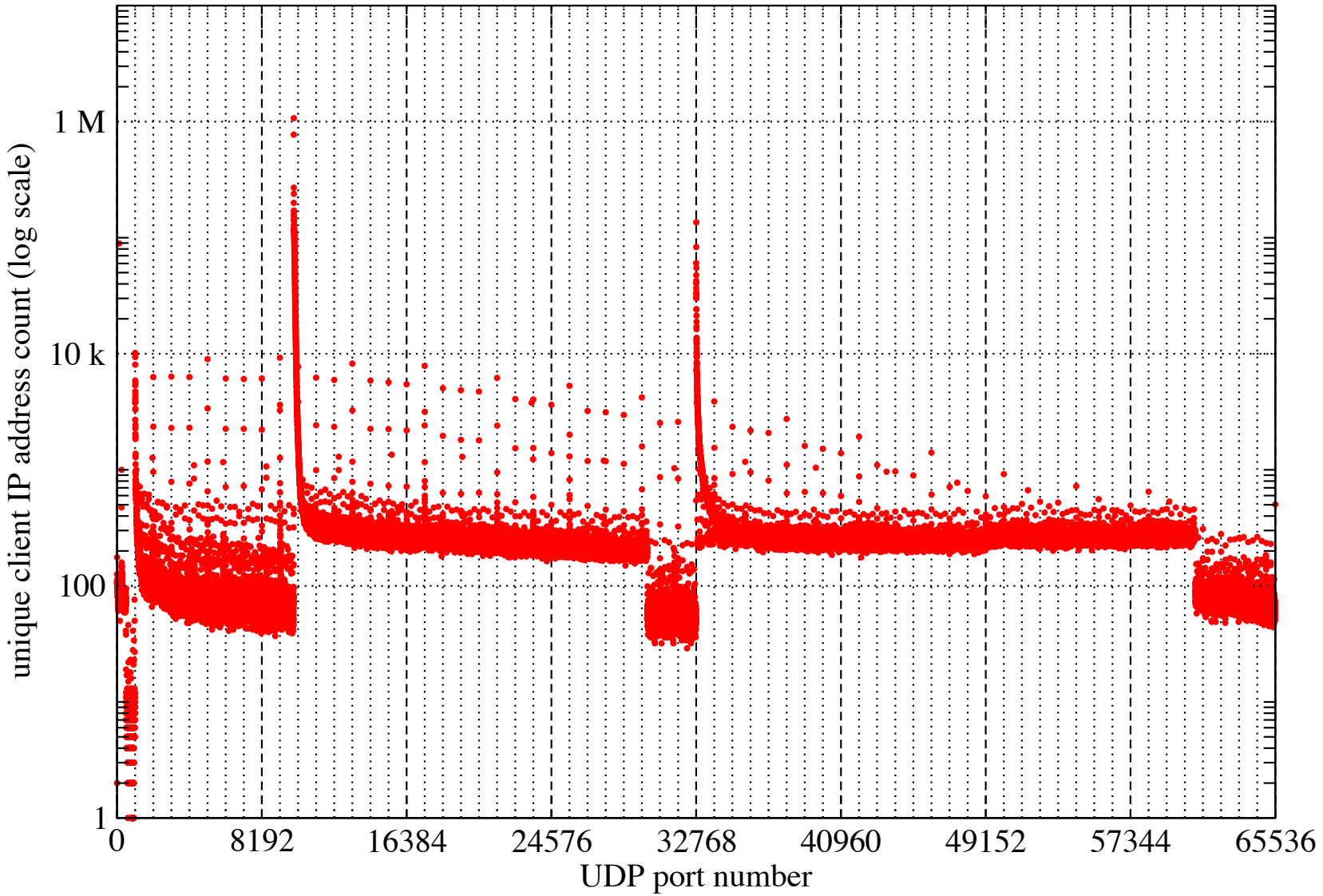


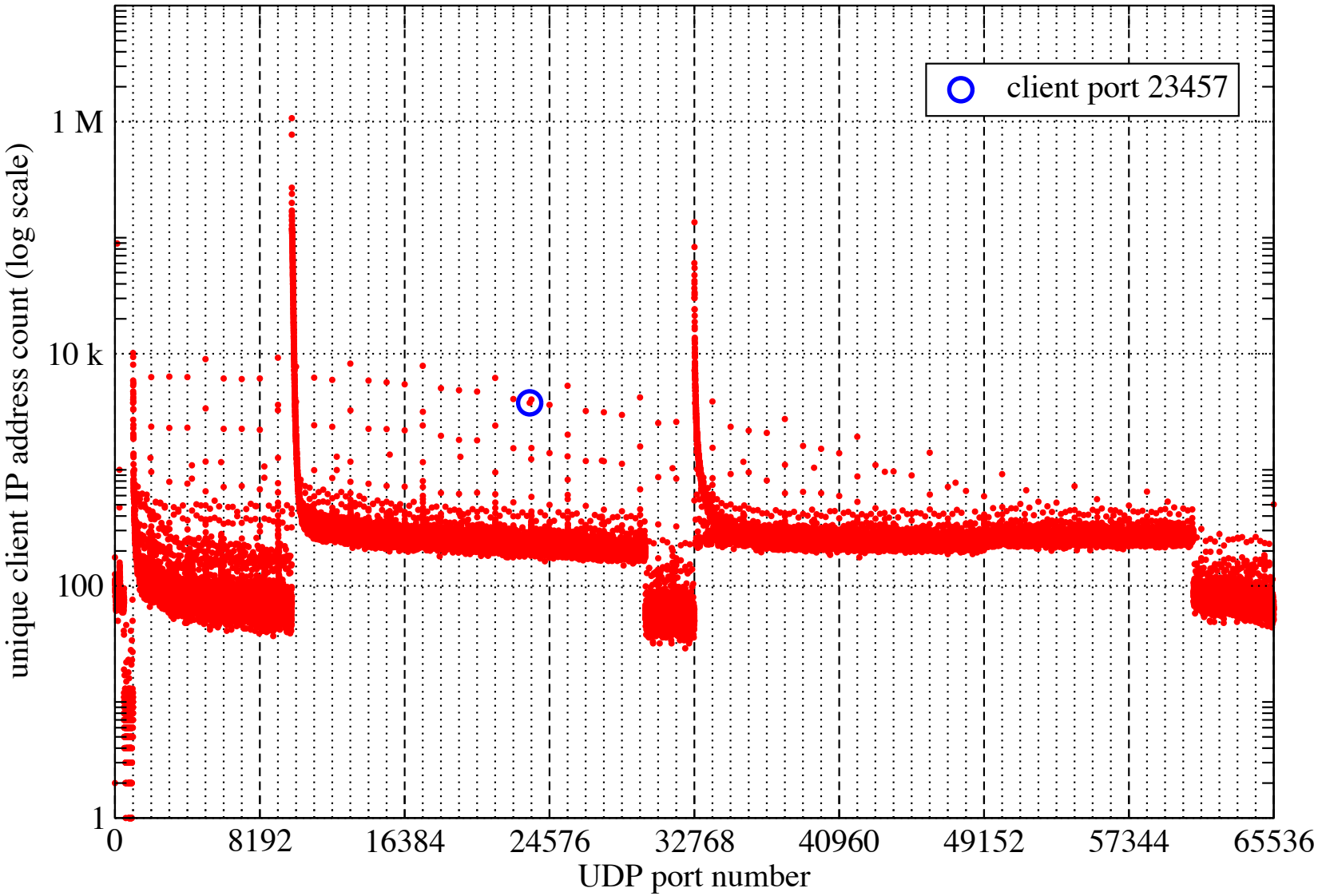
Case Study: Active Device Counts, June 2006

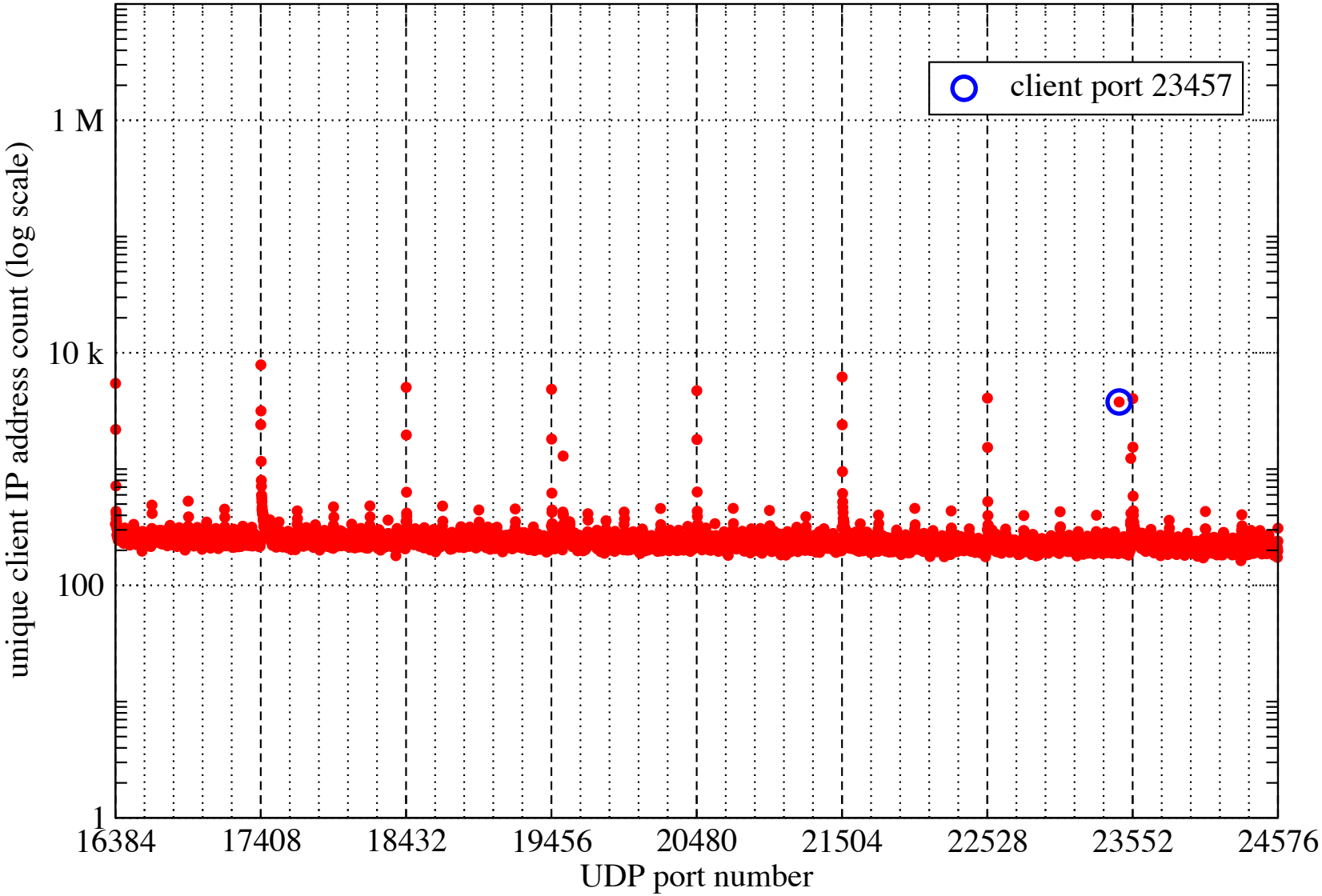



Counted at UW-Madison NTP Server, June 2003 through June 2006
Unique Source IP Addresses Per Day
Potential Flood Rate (IP bits per second)
Total Netgear SNTP clients
query bit rate
800 k
700 k
600 k
500 k
400 k
300 k
200 k
100 k
0
450 M
400 M
350 M
300 M
250 M
200 M
150 M
100 M
50 M
0
Jun-2003
Jul-2003
Aug-2003
Sep-2003
Oct-2003
Nov-2003
Dec-2003
Jan-2004
Feb-2004
Mar-2004
Apr-2004
May-2004
Jun-2004
Jul-2004
Aug-2004
Sep-2004
Oct-2004
Nov-2004
Dec-2004
Jan-2005
Feb-2005
Mar-2005
Apr-2005
May-2005
Jun-2005
Jul-2005
Aug-2005
Sep-2005
Oct-2005
Nov-2005
Dec-2005
Jan-2006
Feb-2006
Mar-2006
Apr-2006
May-2006
Jun-2006

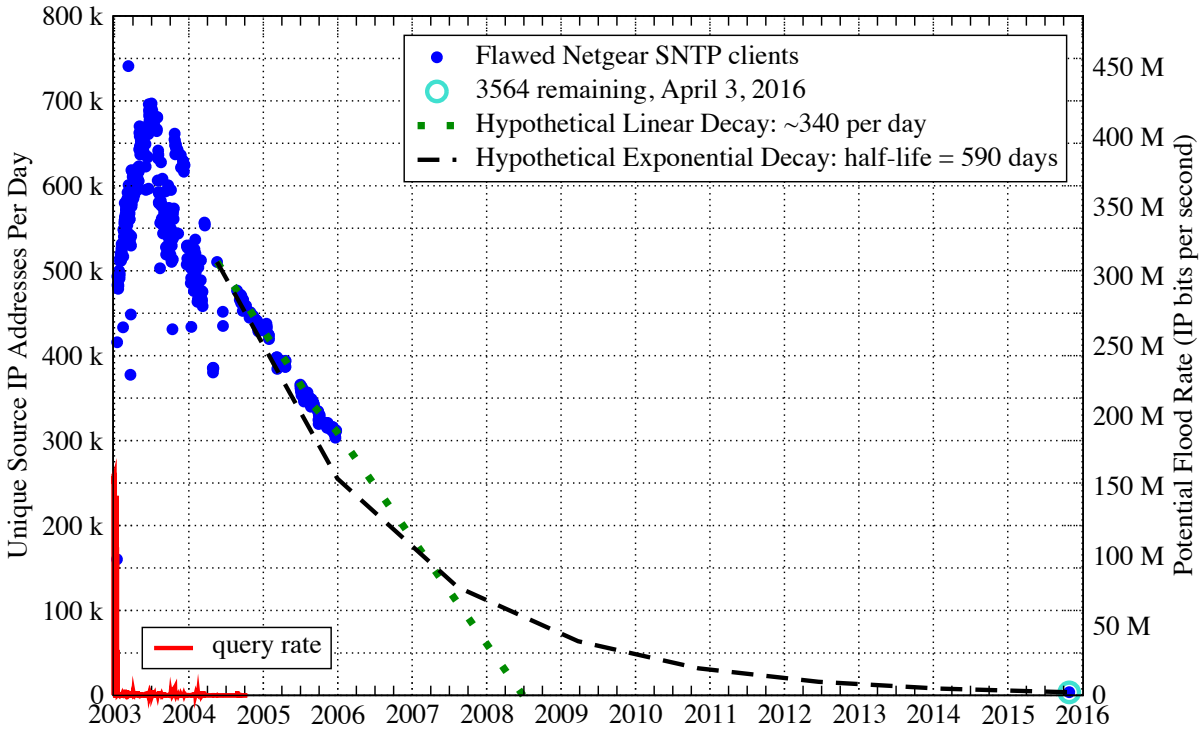
Case Study: 10 years hence…

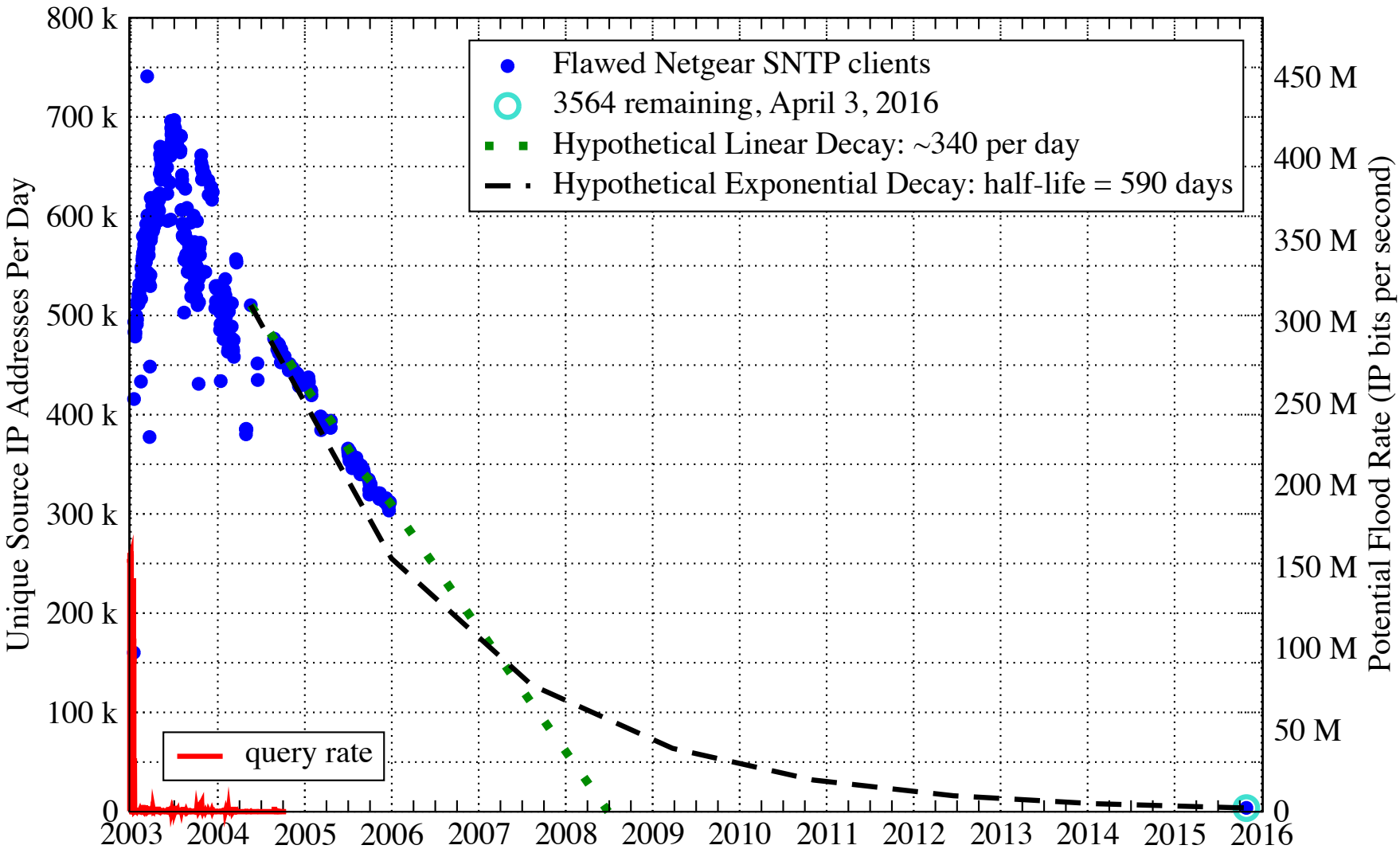

1 M
10 k
100
1
unique client IP address count (log scale)
0
8192
16384
24576
32768
40960
49152
57344
65536
UDP port number


client port 23457
1 M
10 k
100
1
unique client IP address count (log scale)
0
8192
16384
24576
32768
40960
49152
57344
65536
UDP port number


client port 23457
1 M
10 k
100
1
unique client IP address count (log scale)
16384
17408
18432
19456
20480
21504
22528
23552
24576
UDP port number

Case Study: Active Device Counts, June 2016




Flawed Netgear SNTP clients
3564 remaining, April 3, 2016
Hypothetical Linear Decay: ~340 per day
Hypothetical Exponential Decay: half-life = 590 days
query rate
Unique Source IP Addresses Per Day
Potential Flood Rate (IP bits per second)
800 k
700 k
600 k
500 k
400 k
300 k
200 k
100 k
0
450 M
400 M
350 M
300 M
250 M
200 M
150 M
100 M
50 M
0
2003
2004
2005
2006
2007
2008
2009
2010
2011
2012
2013
2014
2015
2016

Measurement & Analysis for IoT

- Real counts or other measurements of IoT devices active/deployed?
- Who are the stakeholders for measurements about active devices?
- Kinds of measurements?
- Privacy/anonymity?
- IPv6?

Counts of Active/Deployed IoT Devices

- **Netgear:** over 700,000 flawed devices (SMTP client)
  - Not updated
- **Electric Imp:** over 500,000 “Imps”
  - Updated in field
- **Others?**

Stakeholders for IoT Measurements

- **Manufacturers**
  - Supply chain: how many manufactured but not active?
- **Service Providers: IoT as a Service for Management**
  - How to manage infrastructure for IoT?
  - Risk Assessment
  - Enterprises, Network Operators
- **Standards Organizations, Vendor Consortiums, Researchers**
- **Regulators: governments and lawmakers**
- **Users, owners, customers**
  - Discover devices, audit premises, inform insurers

Kinds of IoT Measurements

- **WWW User-Agent strings**
- **IPv6 clients with Modified EUI-64 addresses**
  - MAC randomization
- **Requirements/Methods for determining authenticity** (anti-spoofing)?
- **Volume of traffic**
- **Uptimes, faults/interval**, e.g., resets
- **Others?**

IoT Privacy/Anonymity

- **Requirements differ by stakeholder**
- **Version number homogeneity**
- **Demonstrable privacy in measurements**
  - e.g., k-anonymity
  - EPID: enhanced privacy identifier
    asymmetric crypto for keys across multiple devices
  - Sketch: [ab]use the DNS and have the IoT device fetch a page periodially to provide some local control and anonymity, but still allow counting

IPv6oT

- **Some IoT vendors say customers do not demand IPv6 support.** (sound familiar?)

- **Thus, many IoT devices do not support, or do not choose to *use*, IPv6.**
  - *e.g.,* smart TVs and streaming content
  - These devices can be very long-lived, might not be updated, and therefore may present a floor for (decreased) IPv4 activity.

Measurement and Analysis for the Internet of Things

Thanks!
Questions, Comments?