

Spectroscopy of Private DNS Update Sources

Vocal and lyrics:

Andre Broido, Evi Nemeth, kc claffy & elves
(broido, evi, kc) @ caida.org

CAIDA/SDSC/UCSD

WIAPP

San Jose

22 jun 03

www.caida.org/presentations/

Acknowledgements

Paul Vixie

Peter Loshier

Nevil Brownlee

Betty Tso Yuen

Young Hyun

Brad Huffaker

Margaret Murray

Marina Fomenkov

Part I

Introduction

DHCP

Dynamic Host Configuration Protocol

Configures IP addresses, gateways, nameservers automatically

Has a server part and client part

Server leases addresses etc.

Client requests them and accepts them

Client also requests renewals when lease gets short

DNS

Distributed Database of Names and IP Address Mappings

Since 1996 can do dynamic updates

DHCP gives an IP address

DHCP tells DNS

DNS updates zone's A and PTR records

Life is good

RFC1918 Private Address Space

Addresses in 10/8, 172.16/12, 192.168/16

For use inside an organization

Dont need permission from anyone

Should never leak outside local site

Can use DHCP and dynamic DNS

Life should be very good

Root Servers

DNS servers for the top of the tree

Know about .com, .net, .org, .de, .uk, etc.

Dont know about your private address space domains

Don't care either

Getting zillions of updates for private address space

The growth started in 2000

Life is not good

AS112 Project

Root servers overwhelmed by update load

Always refuse all updates

Delegated the private address zones to other servers

prisoner.iana.org: 192.175.48.1

blackhole-1.iana.org: 192.175.48.6

blackhole-2.iana.org: 192.175.48.42

These are anycast servers

Several machines have these IP addresses

Addresses identify a service not a network interface

Routing system finds closest server to bogus updater

Any ISP can run one, see www.as112.net

Life is getting better, but

Updates per minute by Internet Registry, D1

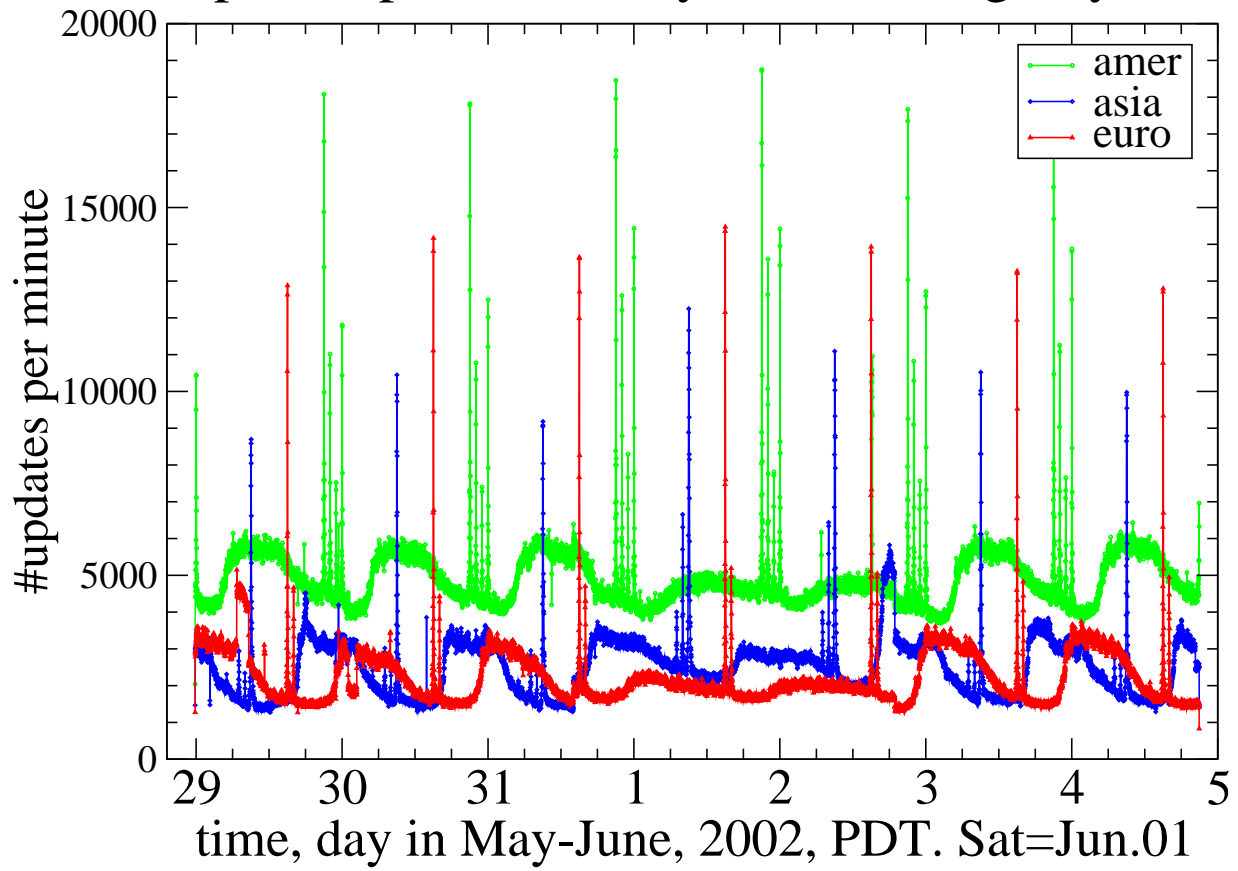


Figure 1:

A week of update counts

Can see weird spikes at midnight, local time

4 in the US, 3 in Asia, 2 in Europe

Can see weekday, weekend patterns

Can see that Asians work on the weekend

Can see that Europeans and Asians get to work on time

Largest observed: 1200 updates/sec (Nov.2002)

Surge at midnight EDT. Mon 2002-07-29

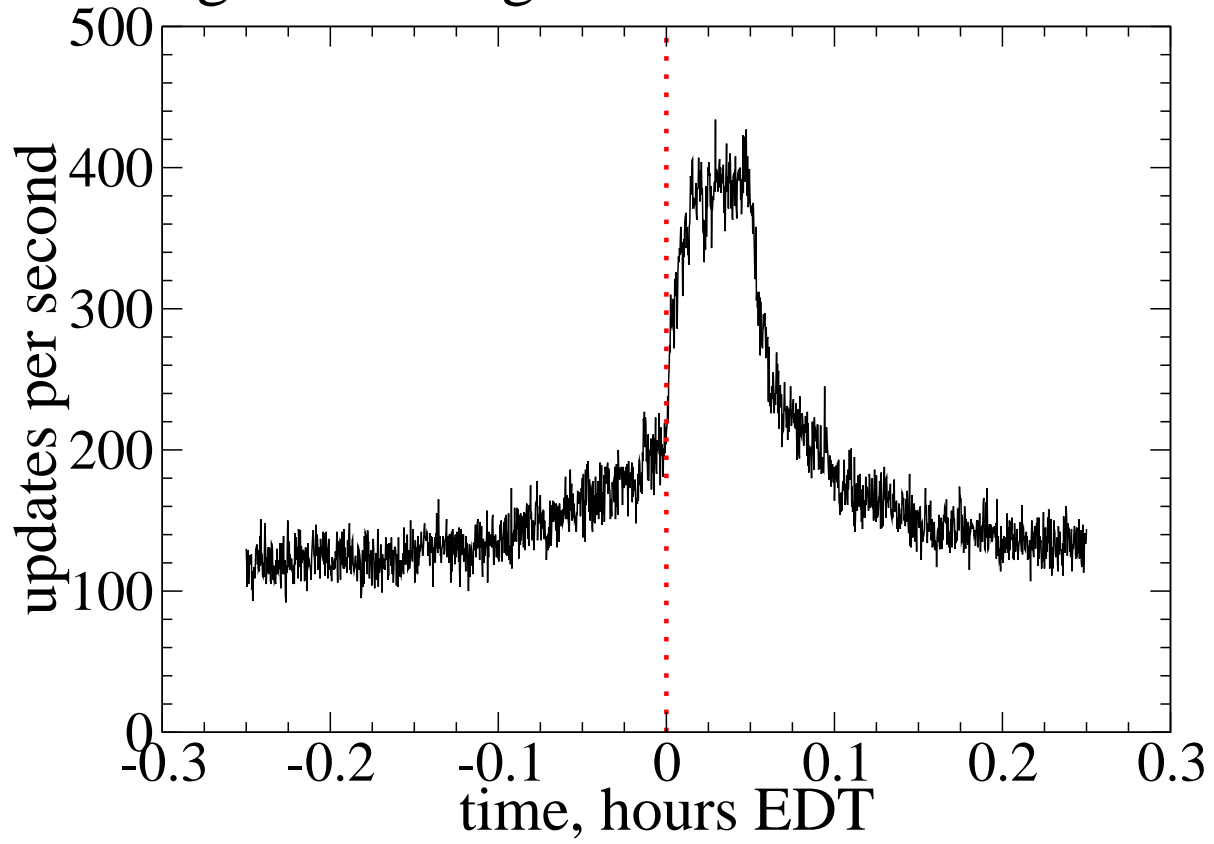


Figure 2:

A spike in detail

Midnight US Eastern time

Four-fold increase over about 2 minutes

Spread is over about 6 minutes

Clock skew, home users don't run NTP

We are very lucky they don't

Duration of source activity, D2

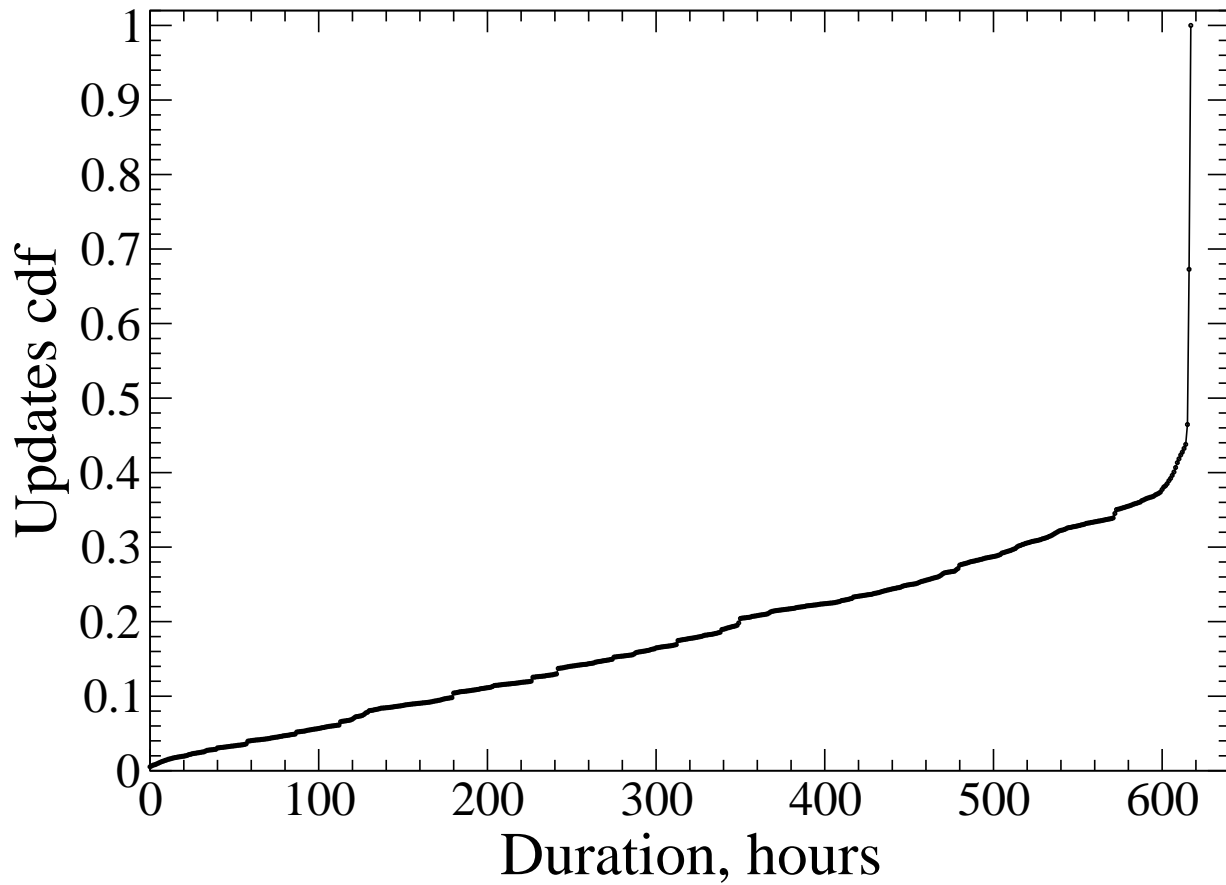


Figure 3:

60% of updates are from permanently active sources

Who is trying to update the roots?

IP addresses of update sources, D1

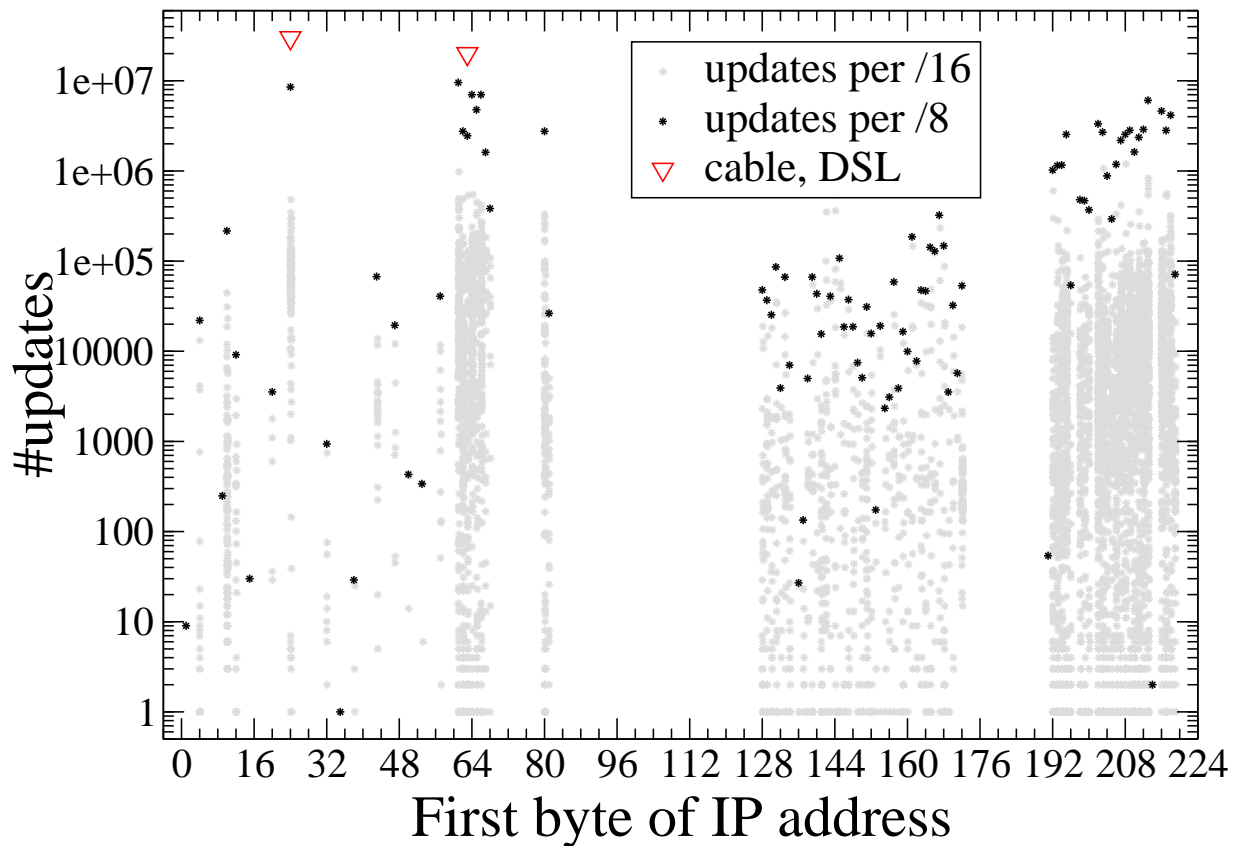


Figure 4:

Hosts are behind DSL and Cable modem ISPs mostly

Academy and medium-sized businesses (class B) are low

Top 20 AS sources of RFC1918 updates

AS	Updates	Percent	Cumul.	
4134	7329178	7.51	7.51	CHINALINK, China
3352	6166266	6.32	13.84	Ibernet (TDE), Spain
7132	4559748	4.67	18.51	SW Bell, US
5673	3271669	3.35	21.86	Pac Bell, US
5676	2936073	3.01	24.87	Pac Bell, US
4813	2765227	2.83	27.71	China Telecom Guandong
4812	2644362	2.71	30.42	China Telecom Shanghai
852	2176242	2.23	32.65	Telus, Canada
6128	2083593	2.14	34.79	Cablevision, US
2828	1855065	1.90	36.69	XO, US
11427	1753091	1.80	38.49	Road Runner, US
7843	1504131	1.54	40.03	Adelphia, US
4760	1413921	1.45	41.48	Netvigator, Hong Kong
2914	1393102	1.43	42.90	Verio, US
1221	1378306	1.41	44.32	Telstra, AU
11509	1226816	1.26	45.58	Pajo, US

4436	1142608	1.17	46.75	SantaCruz Community, US
11426	1135058	1.16	47.91	Road Runner, US
10994	1129898	1.16	49.07	Time Warner, US
2548	1091393	1.12	50.19	Business Internet, US

Update properties

Source contribution sizes, D1

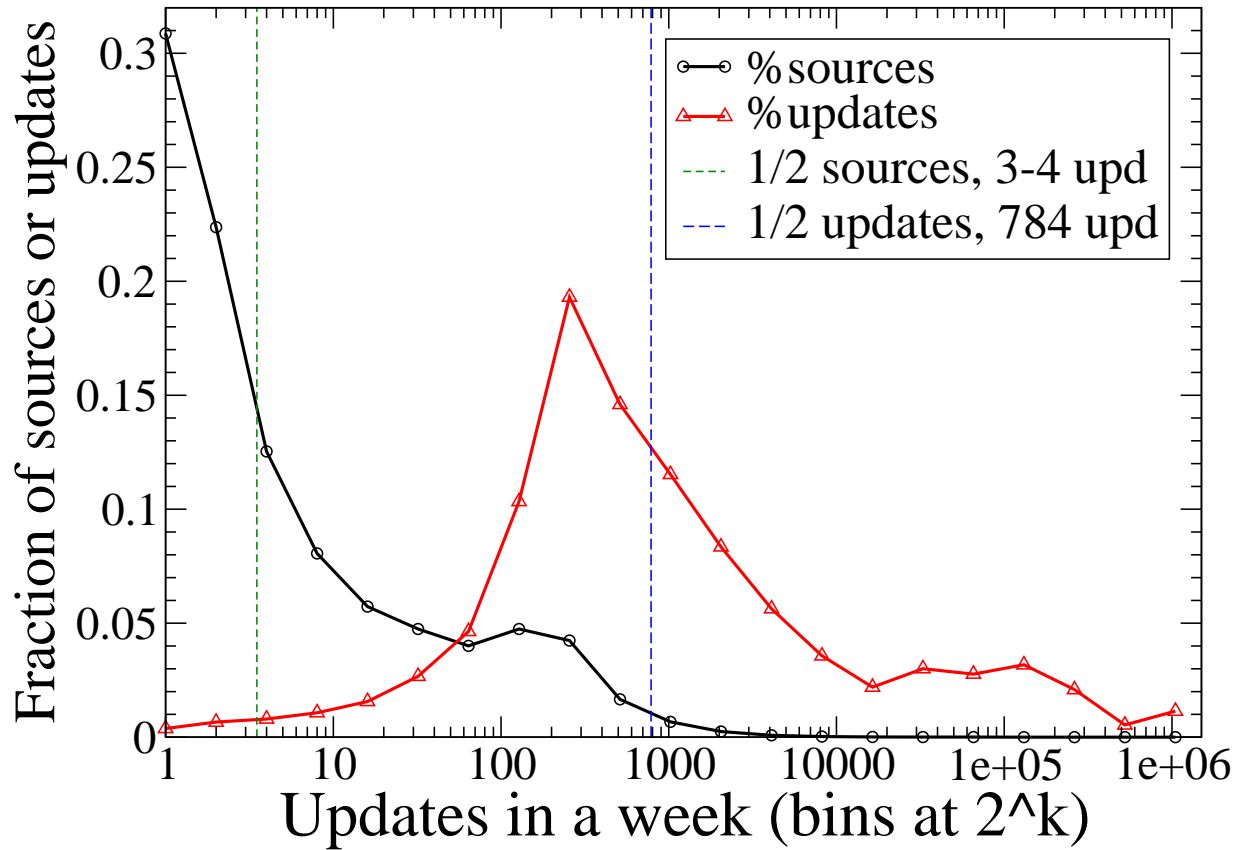


Figure 5:

Mules, not mice or elephants send the bulk of updates

Scaling of updates' ccdf, D1

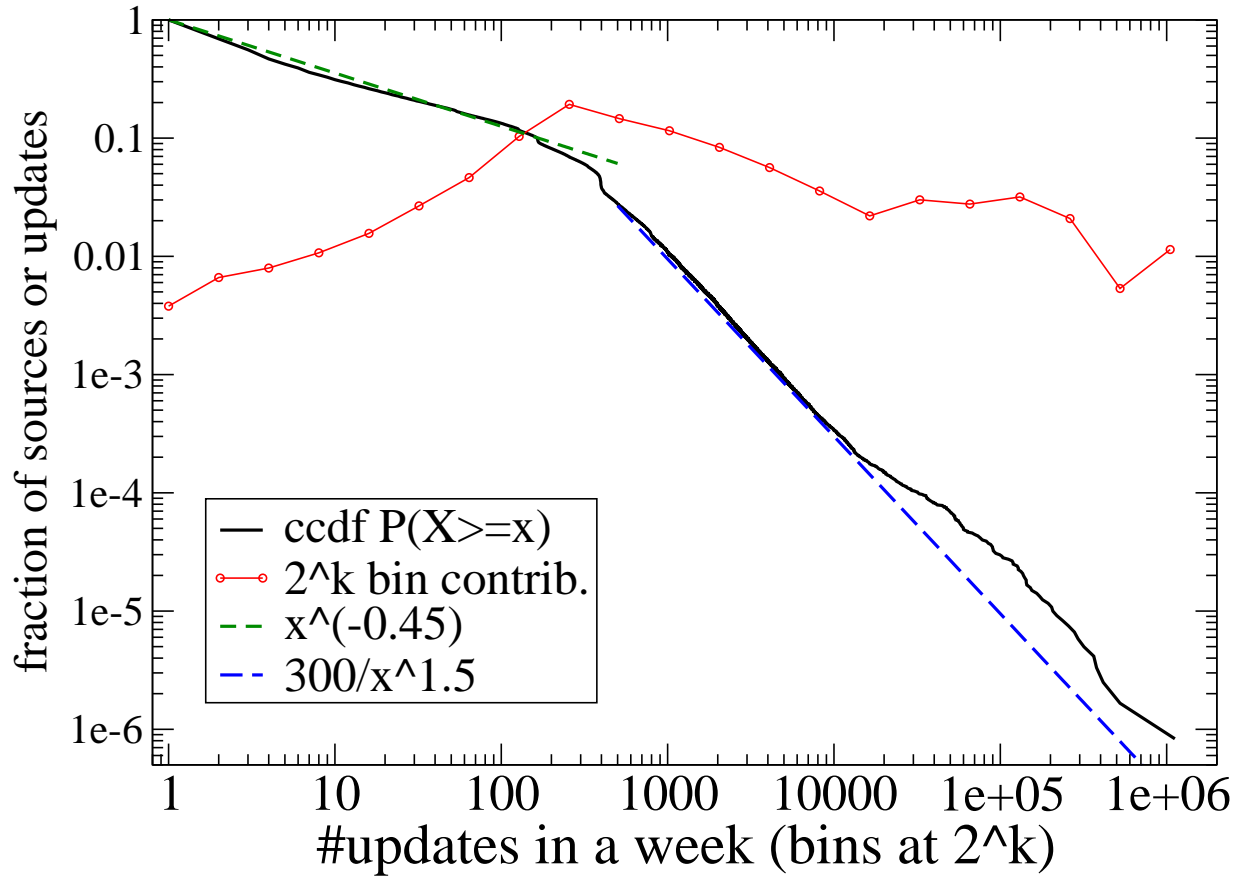


Figure 6:

Mules' prevalence causes two scalings in ccdf

Interarrival times, D2

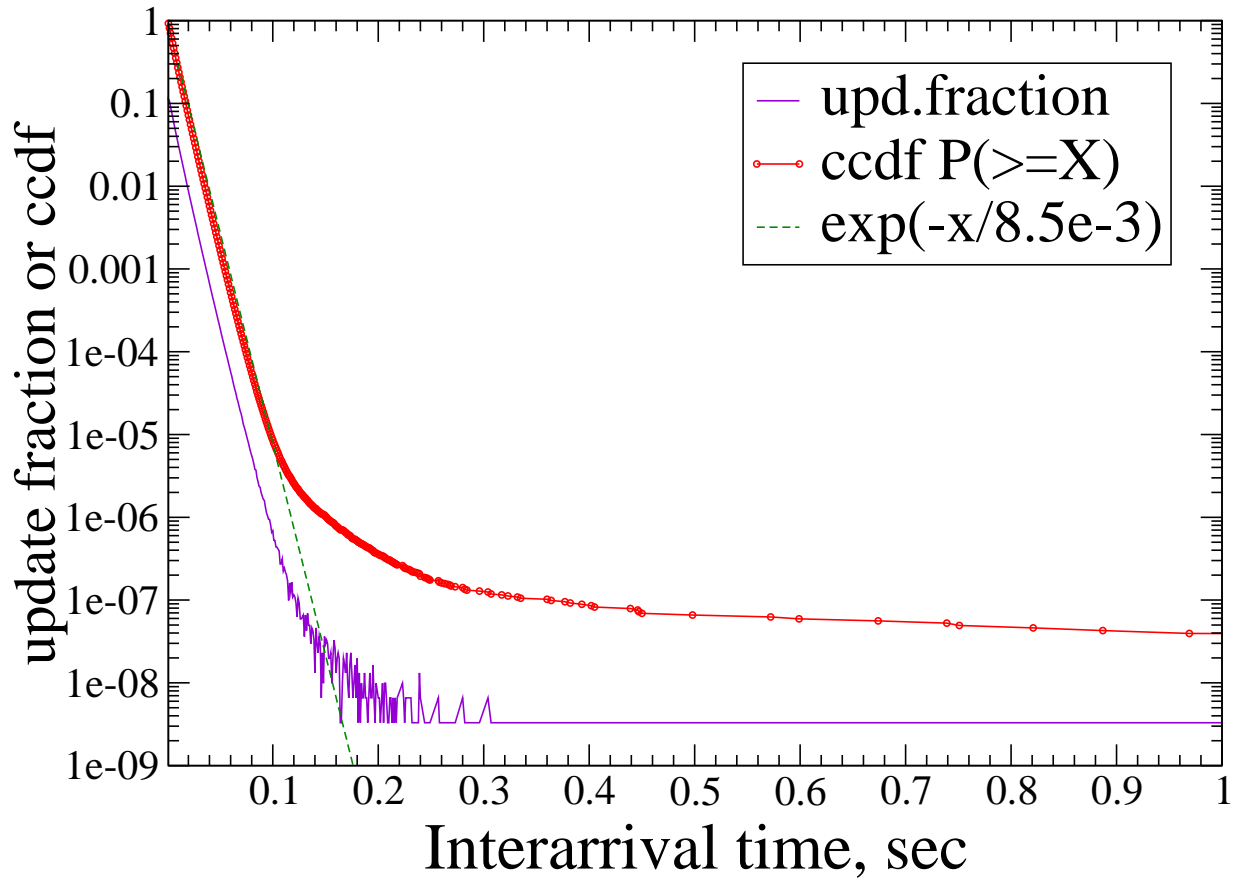


Figure 7:

Exponential interarrival times in the total stream

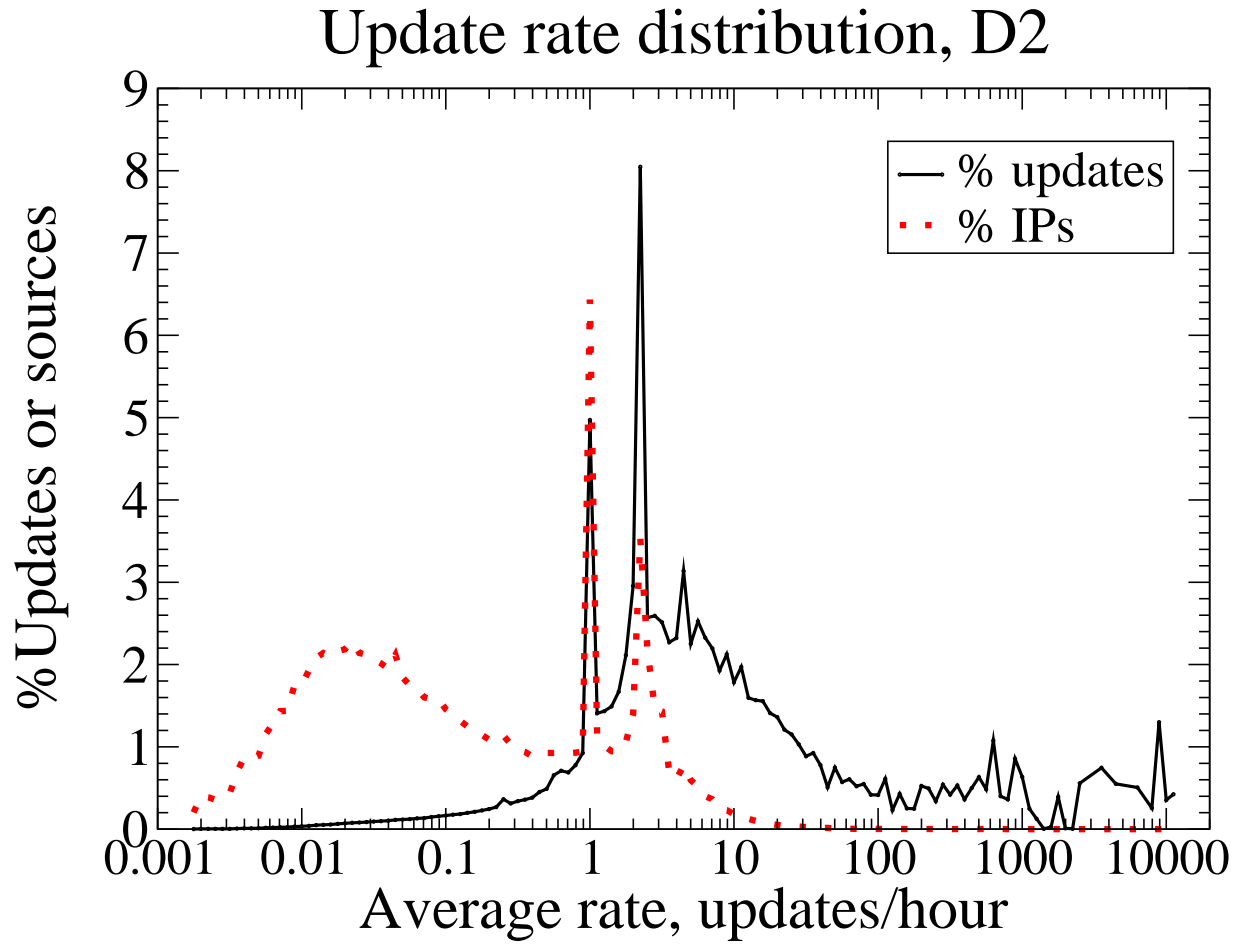


Figure 8:

Surprisingly, many sources are periodic

Update periods, D1

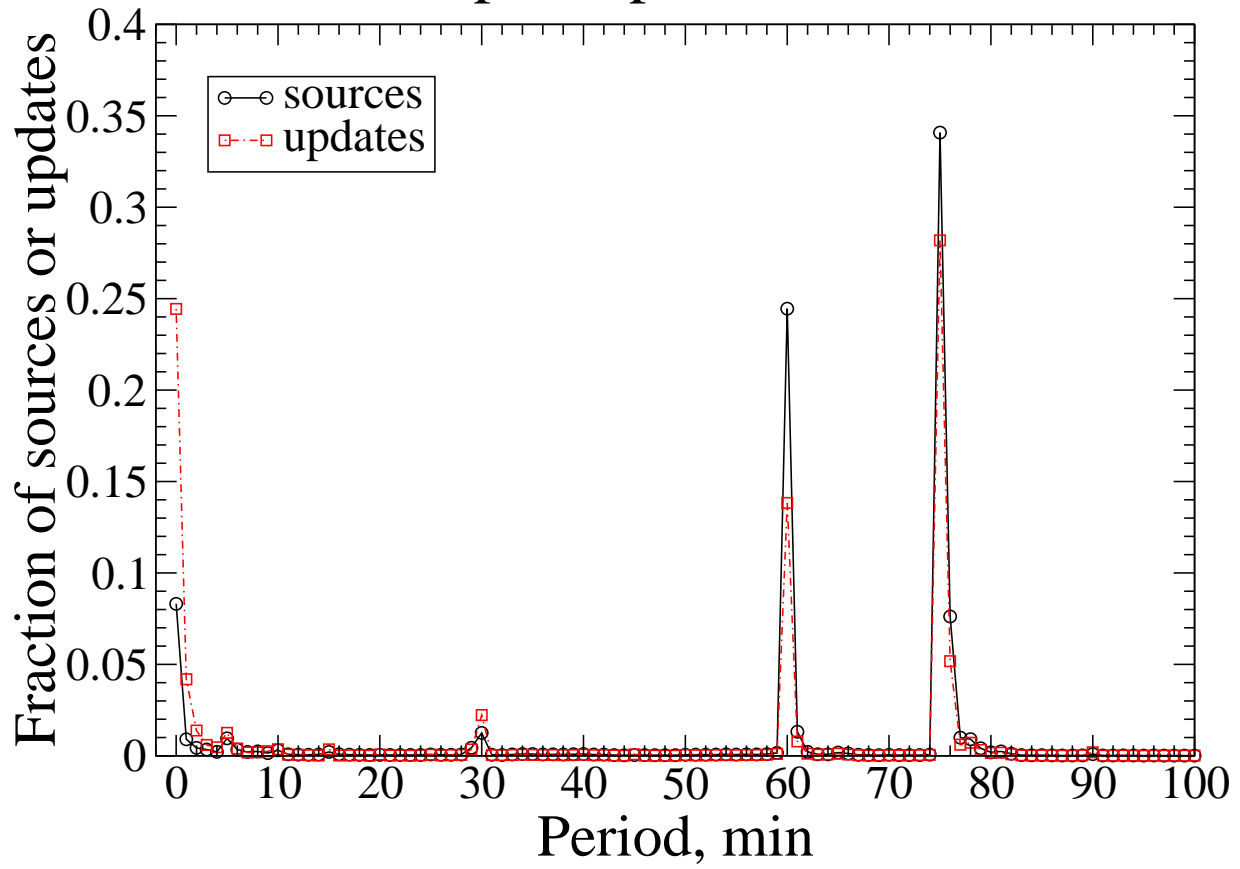


Figure 9:

Periods are 60 minutes or 75 minutes

Can we blame Microsoft?

Maybe

Updates are periodic

75 minute one is 5+10+60

Try an update, get refused back

Wait 5 minutes

Try an update, get refused back

Wait 10 minutes

Try an update, get refused back

Wait 60 minutes

Repeat forever and ever

Windows 2000 Server does that

Observed in test lab:

16 packets sent to server per update

13 packets received

At 1200 updates/sec, about 30 Kpps at one server

More Microsoft Evidence

Lots of hosts use ports in 1024-5000 range

Win2k does that

44.3% of all updates are from that range

17 times more updates from port 5000 than 5001

Need more info to determine who dunnit

NOPE, it's MICROSOFT

Need to determine default behavior of DHCP server/client

Does it renew/expire leases at midnight?

YES, NETLOGON

Does it default to dynamic updates?

YES

Does it update periodically with either 60 or 75 minute periods

YES

“By default, DNS records are re-registered dynamically and periodically every 24 hours by Windows 2000 Professional and every 1 hour by Windows 2000 Server and Windows 2000 Advanced Server.”

“A statically configured client does not communicate with the DHCP server and dynamically updates A and PTR RRs every time it boots up, changes its IP address or per-adapter domain name”

The update sequence consists of the following steps:

1. A client, using an SOA query, locates the primary DNS server and zone authoritative for the record to be registered.
2. The client sends to the located DNS server an assertion or prerequisite-only update to verify an existing registration. If the registration does not exist, the client will send the appropriate dynamic update package to register the record.
3. If the update fails the client will attempt to register the record with another primary DNS server if the authoritative zone is multimaster. If all primary DNS servers failed to process the dynamic update it will be repeated after 5 minutes and, if fails again, after another 10 minutes. If registration still failed, the described pattern of the registration attempts will be repeated after 50 minutes after the last retry.¹

¹This is probably a typo: our laboratory measurements revealed a delay of 60 minutes, not 50 minutes.

Who else could it be?

MacOS is not guilty, doesn't do dynamic updates at all

UNIX maybe, but DHCP is off by default

UNIX might be the small bump at 30 minute period

Win2K by default does dynamic DNS updates to the closest enclosing domain

If you are using 192.168/16 addresses

Tries 168.192.in-addr.arpa, but

If not configured, tries 192.in-addr.arpa, and

If not configured, tries in-addr.arpa, and even

arpa, but in-addr.arpa is served by the roots

Now, referred to prisoner.iana.org anycast servers

6% root traffic are update SOA queries

Conclusions

The updates are sent by Microsoft

This was almost like a DDoS attack on root servers

Took a lot of community effort to organize defence:

AS 112

dedicated blackhole servers

reserved addresses

Update-related traffic still reaches root servers

Software vendors should keep infrastructure stable