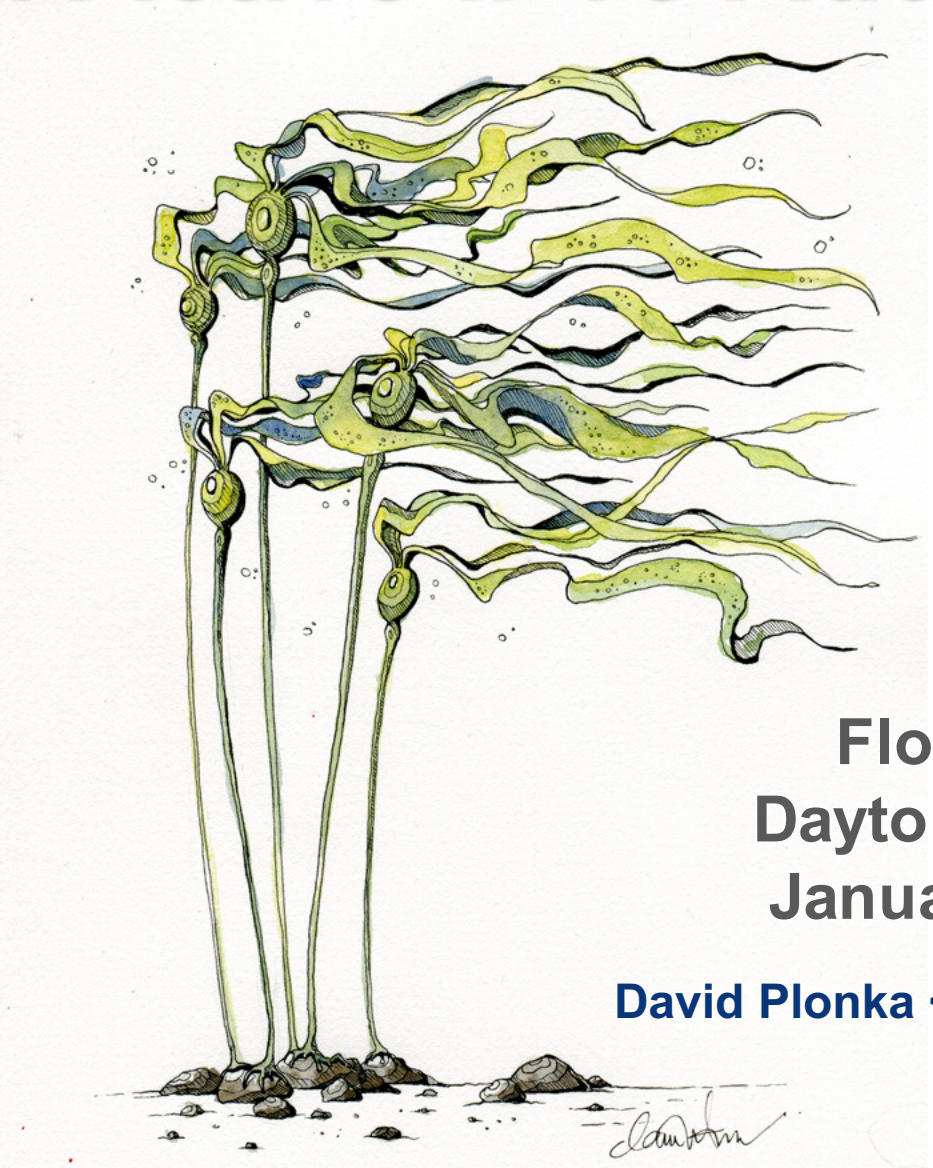
Monitoring and Classification of Active IPv6 Addresses

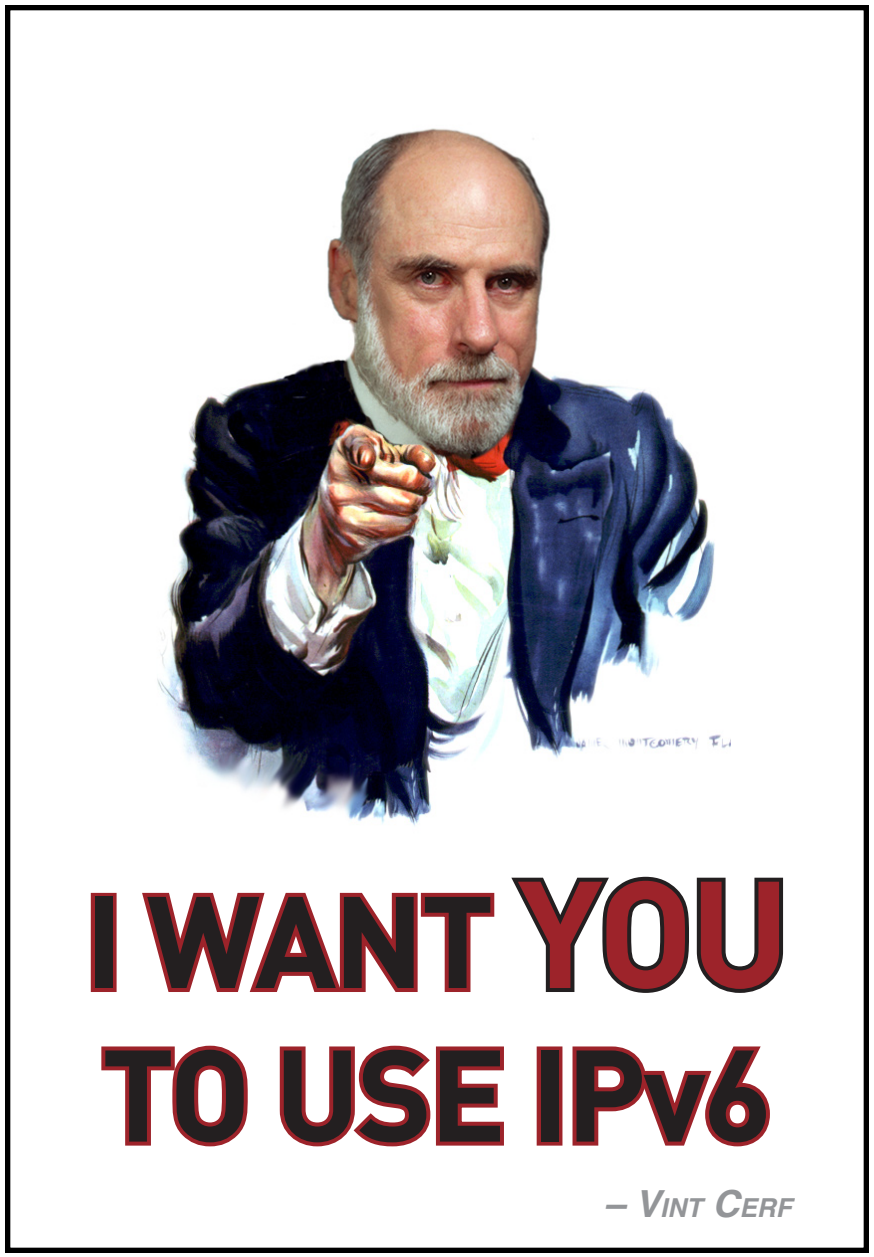


FloCon 2016
Dayton Beach, FL
January 13, 2016

David Plonka <plonka@akamai.com>

Illustration used by permission. http://clairewatson.com

Agenda



www.cs.brown.edu/~adf/cerf/

Agenda

Agenda

- Why network analysts care about IPv6
- Who uses IPv6 and when?
  - An introduction to IPv6 addresses
- How do we measure IPv6 activity?

- IPv6 Address Classification
  - Temporal
  - Spatial

- Data Visualization and Exploration Demo
- Take-aways

IPv6: Why Analysts Should Care

- IPv6 will operate **simultaneously** with IPv4 for the forseeable future.

  One Internet –
  Two protocol versions –
  sharing common rendezvous mechanisms, e.g., the DNS.

IPv6: Why Analysts Should Care

- IPv6 will operate **simultaneously** with IPv4 for the forseeable future.

  One Internet –
  Two protocol versions –
  sharing common rendezvous mechanisms, e.g., the DNS.

- IPv6 changes **client reputation** and **geolocation.**
- IPv6 changes **threat mitigation**, *e.g.,* access control and rate limits.
- IPv6 changes **privacy, log processing**, Real User Monitoring (**RUM**), *etc.*
- IPv6 changes **target selection** for active measurements.

An Introduction to IPv6 Addresses

IPv6 addresses in presentation format:

```
2001:db8:0:1cdf:21e:c2ff:fec0:11db
2001:db8:10:1::103
2001:db8:167:1109::10:901
2001:db8:4137:9e76:3031:f3fd:bbdd:2c2a
```

An Introduction to IPv6 Addresses

IPv6 addresses in presentation format:

```
2001:db8:0:1cdf:21e:c2ff:fec0:11db
2001:db8:10:1::103
2001:db8:167:1109::10:901
2001:db8:4137:9e76:3031:f3fd:bbdd:2c2a
```

An Introduction to IPv6 Addresses

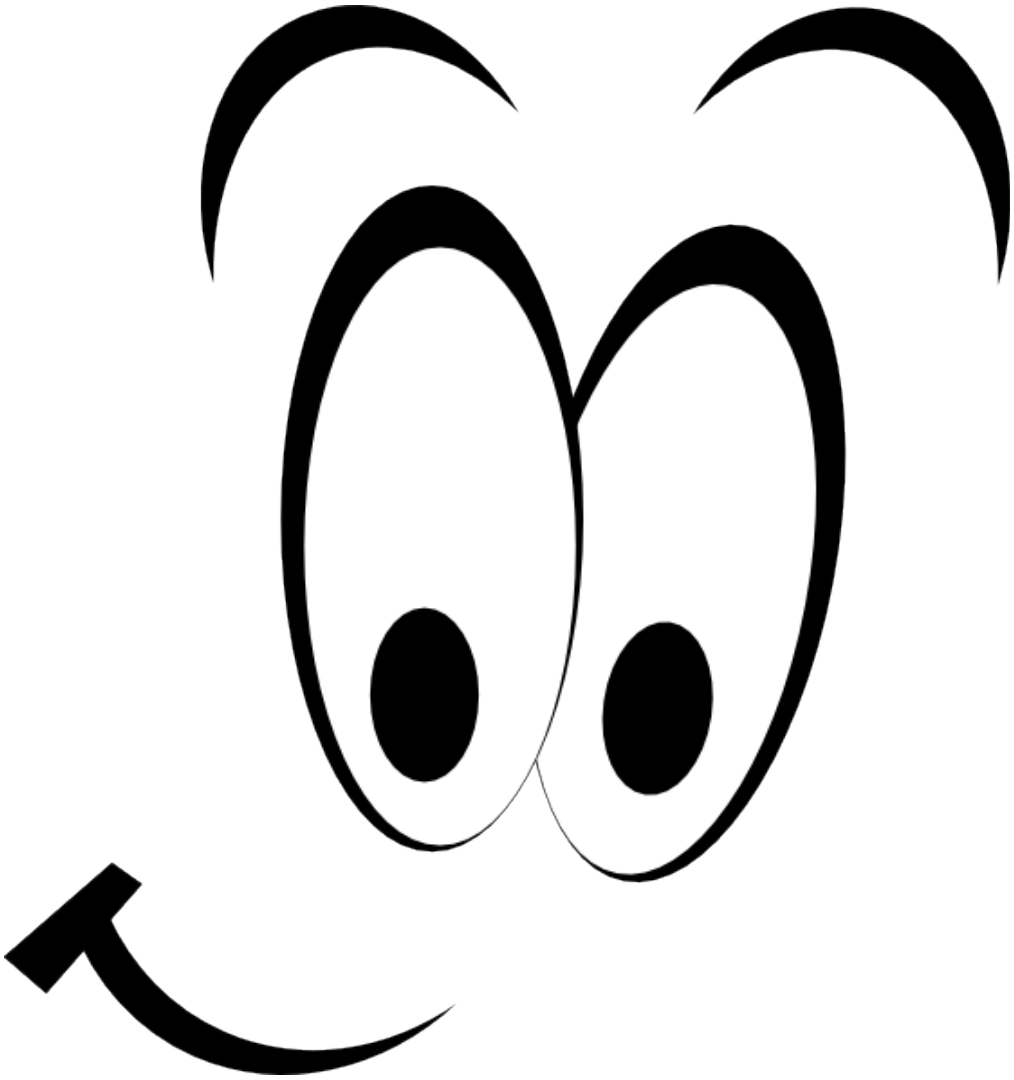
IPv6 addresses in presentation format:

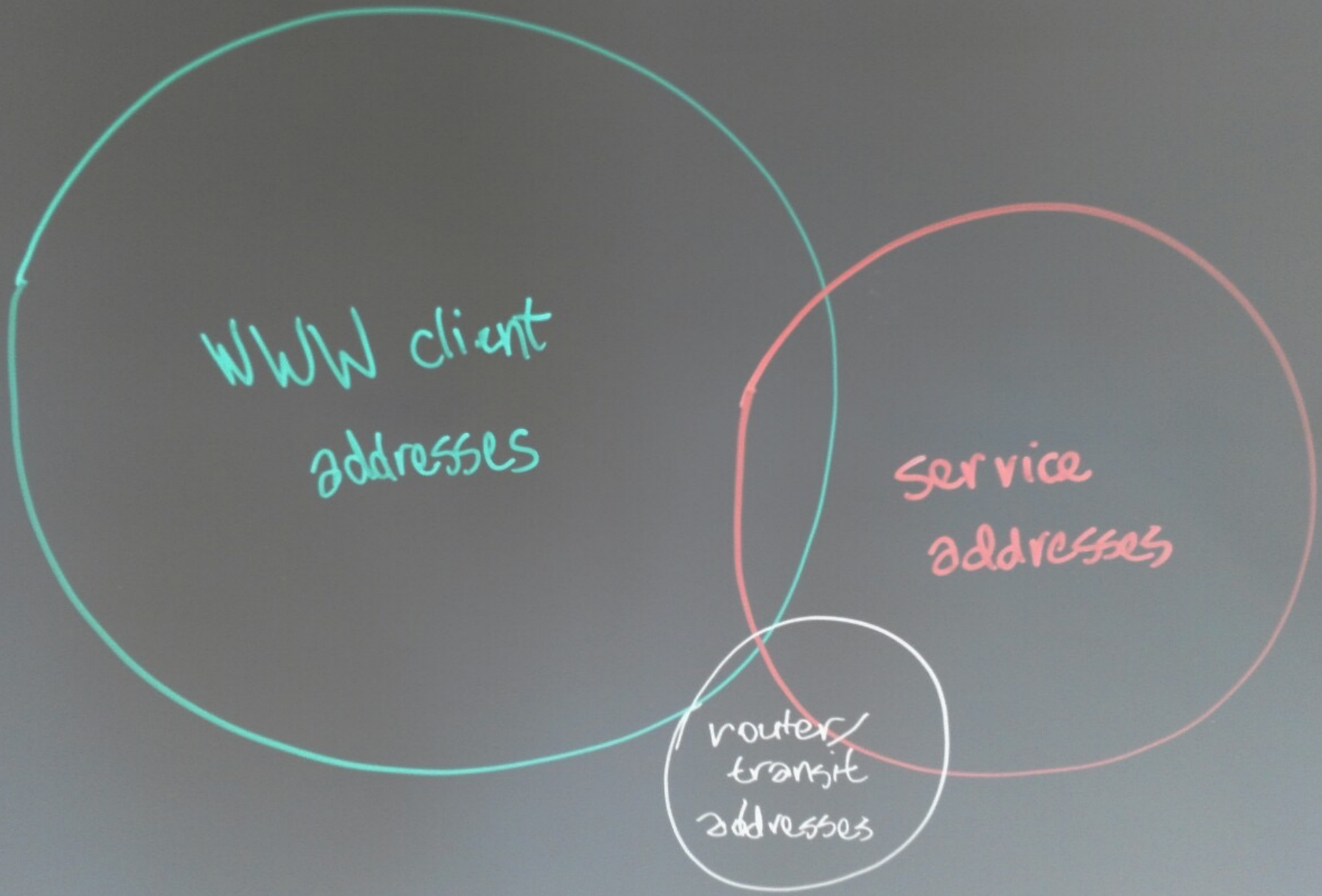
2001:db8:0:1cdf:**21e:c2ff:fec0:11db**
2001:db8:10:1::**103**
2001:db8:167:1109::**10:901**
2001:db8:4137:9e76:**3031:f3fd:bbdd:2c2a**

Consider 16-bit (4 character) and 4-bit (1 character) segments:

2001:0db8:0000:1cdf:**021e:c2ff:fec0:11db**
2001:0db8:0010:0001:**0000:0000:0000:0103**
2001:0db8:0167:1109:**0000:0000:0010:0901**
2001:0db8:4137:9e76:**3031:f3fd:bbdd:2c2a**

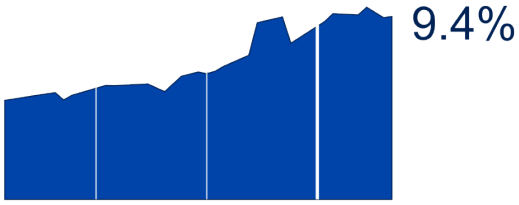
Who uses IPv6 and **when**? – Happy Eyeballs

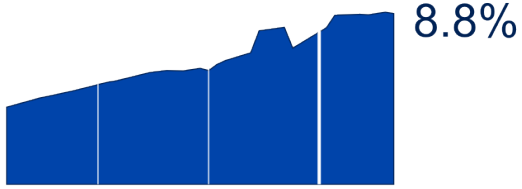


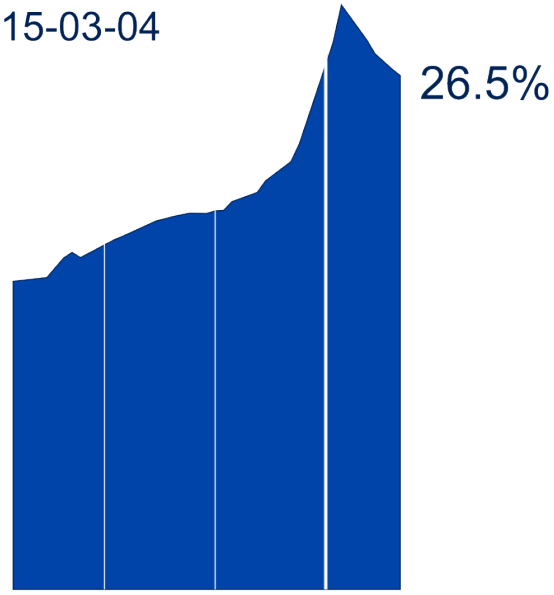

WWW client addresses
service addresses
router/ transit addresses

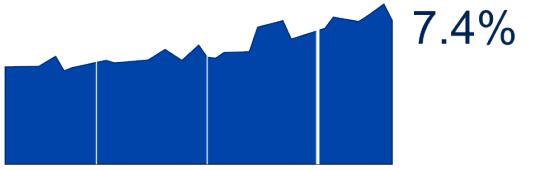
Who uses IPv6? – Major Content Providers

Global percent of requests over IPv6
to selected dual-stack object delivery hostnames
on Akamai from 2014-04-16 to 2015-03-04



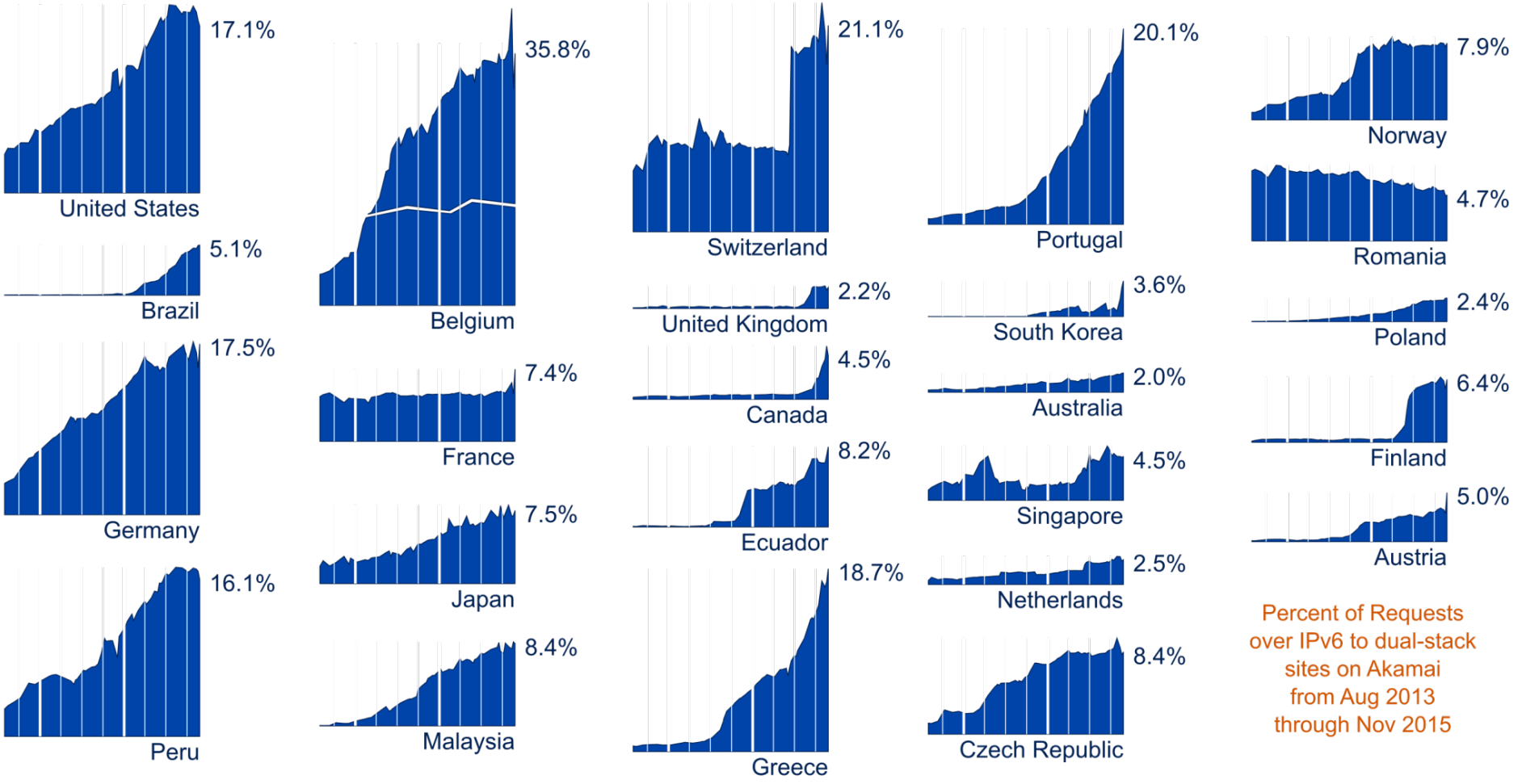






Thanks to Erik Nygren

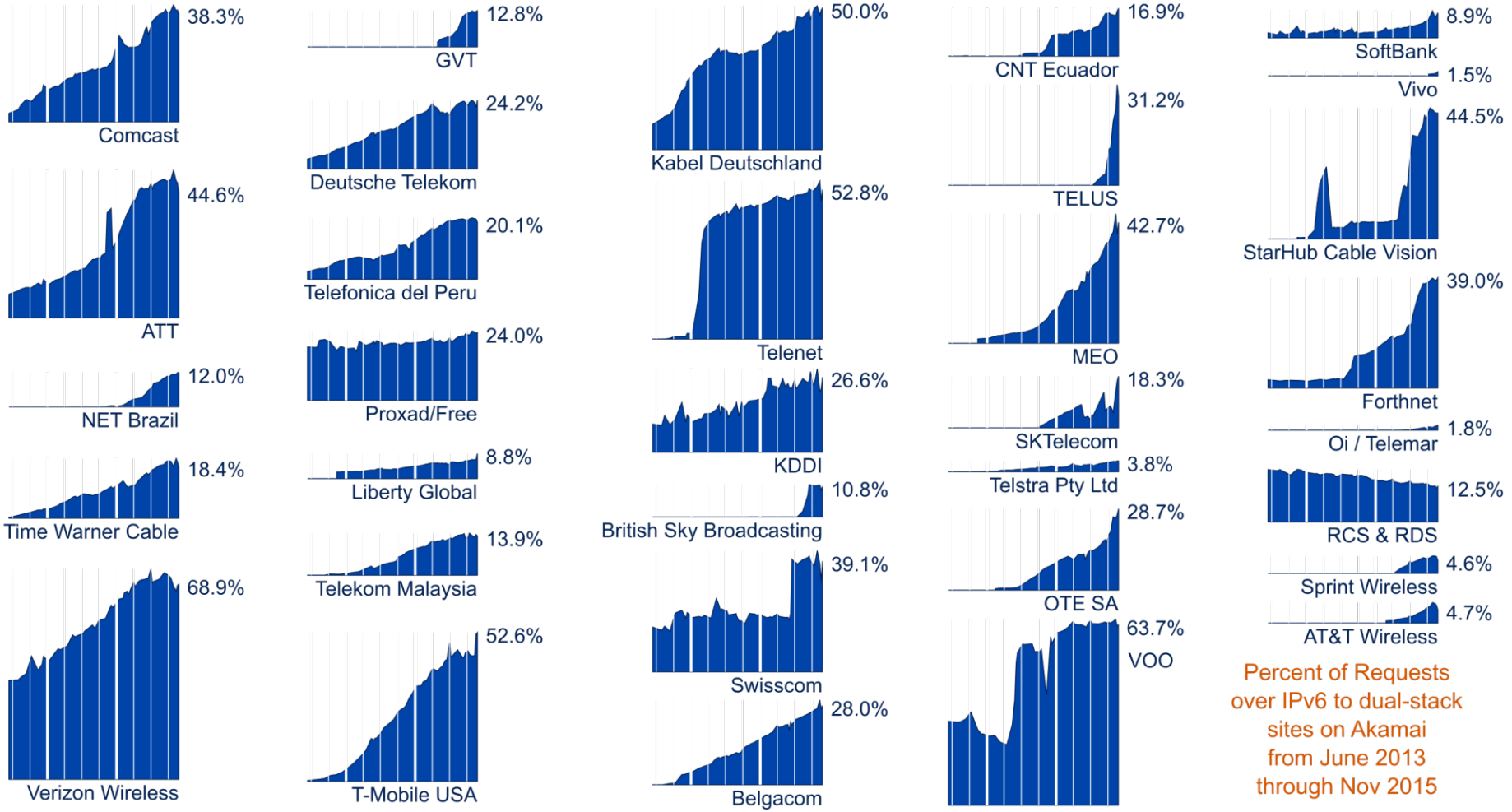
Who uses IPv6? – Leading Countries



Percent of Requests over IPv6 to dual-stack sites on Akamai from Aug 2013 through Nov 2015

Thanks to Erik Nygren

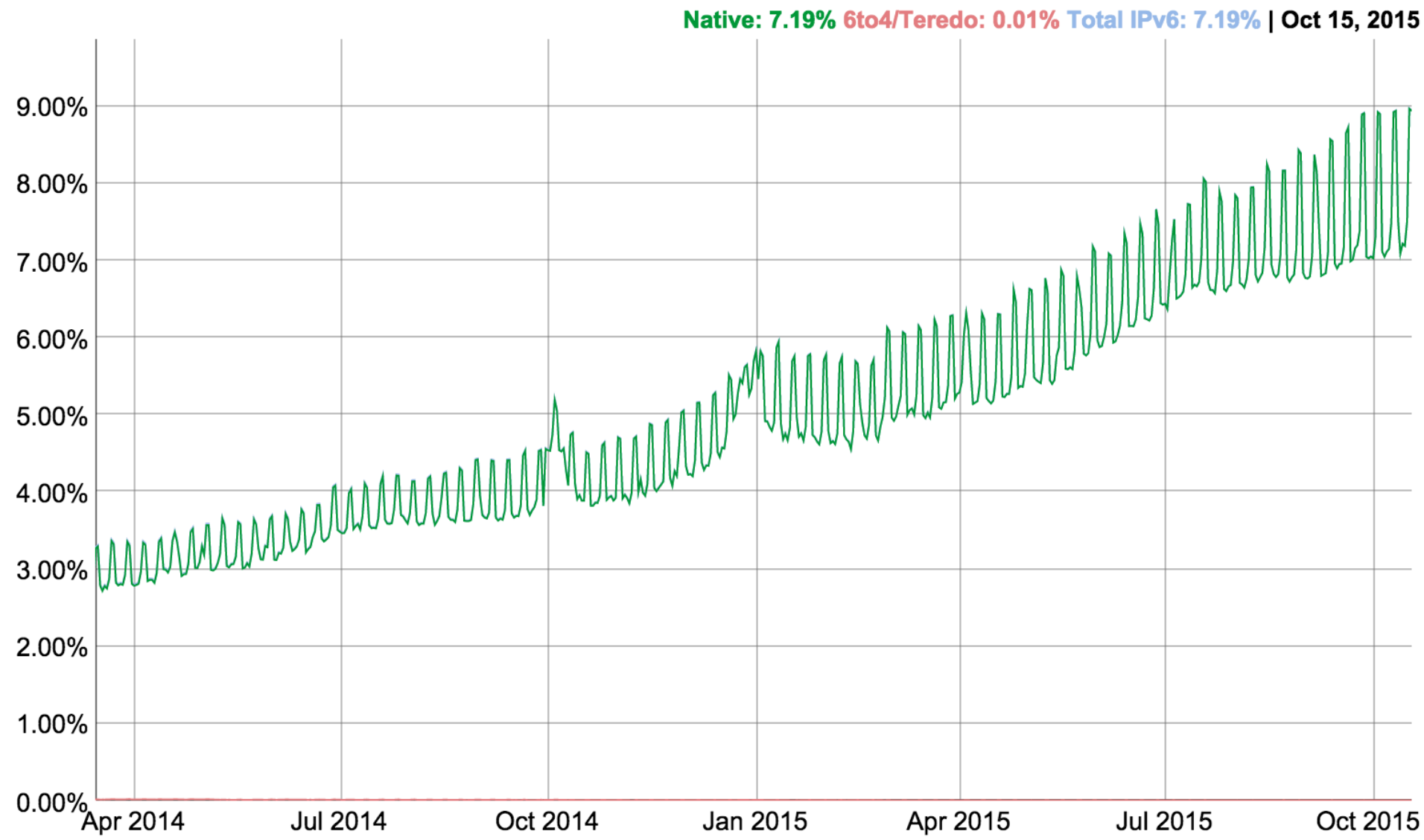
Who uses IPv6? – Leading Networks



Percent of Requests over IPv6 to dual-stack sites on Akamai from June 2013 through Nov 2015

Thanks to Erik Nygren

Who uses IPv6? – Counting IPv6



Source: Google, https://www.google.com/intl/en/ipv6/statistics.html, Oct 20, 2015

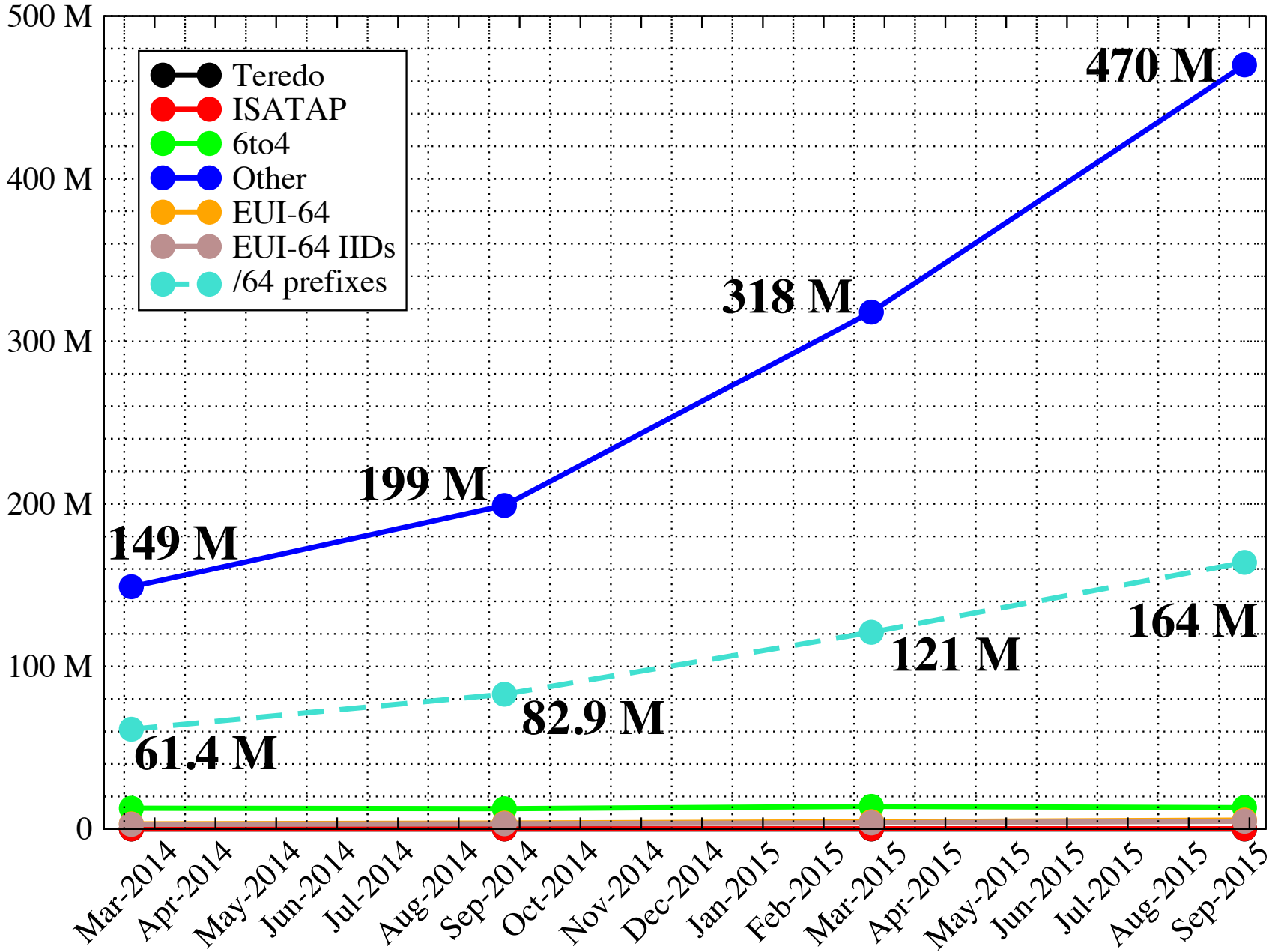
Active IPv6 WWW Client Addresses

***500 million* unique IPv6 client addresses per day.**

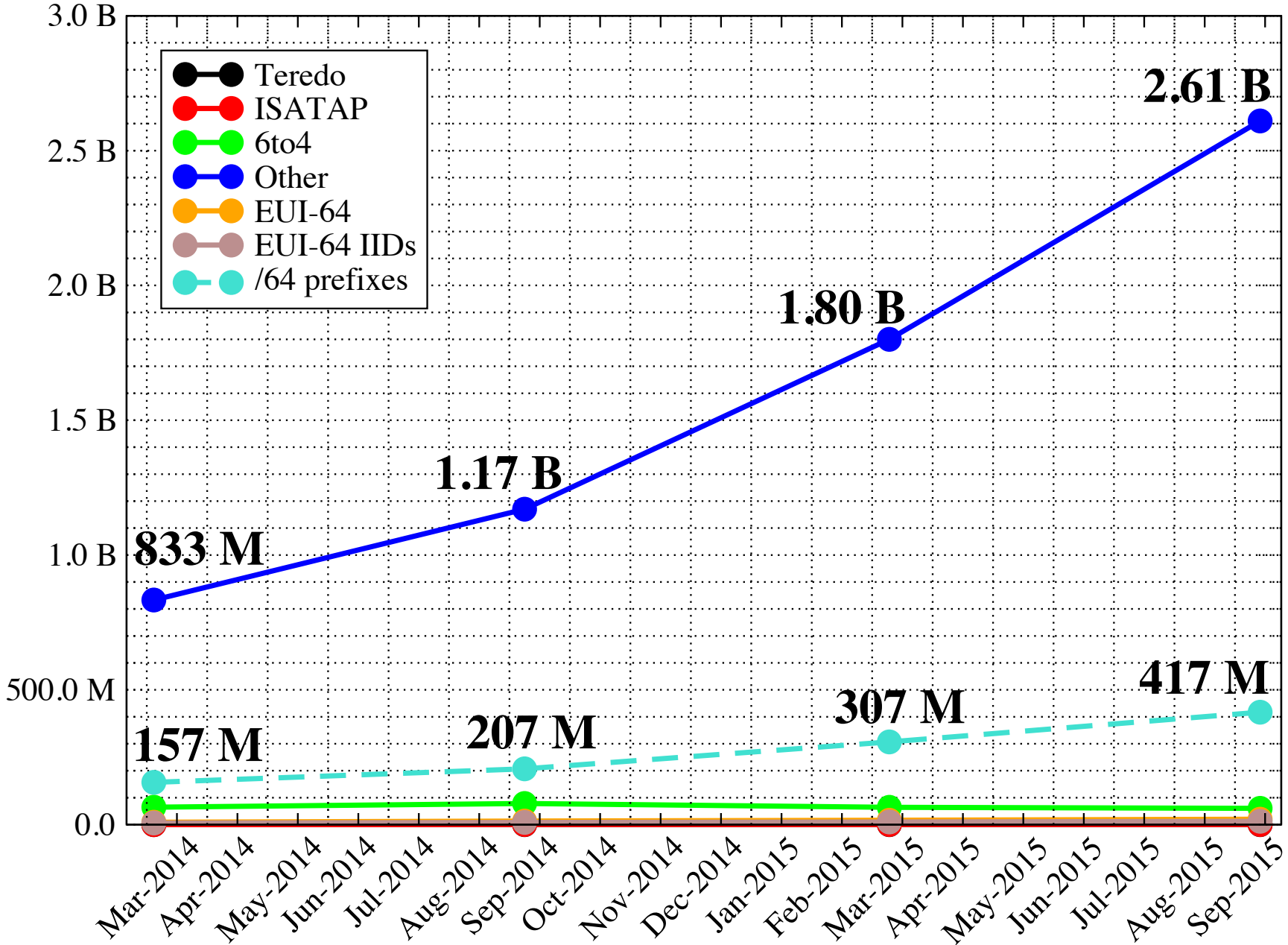
***10 billion* per month.**

Source: Akamai, Oct, 2015

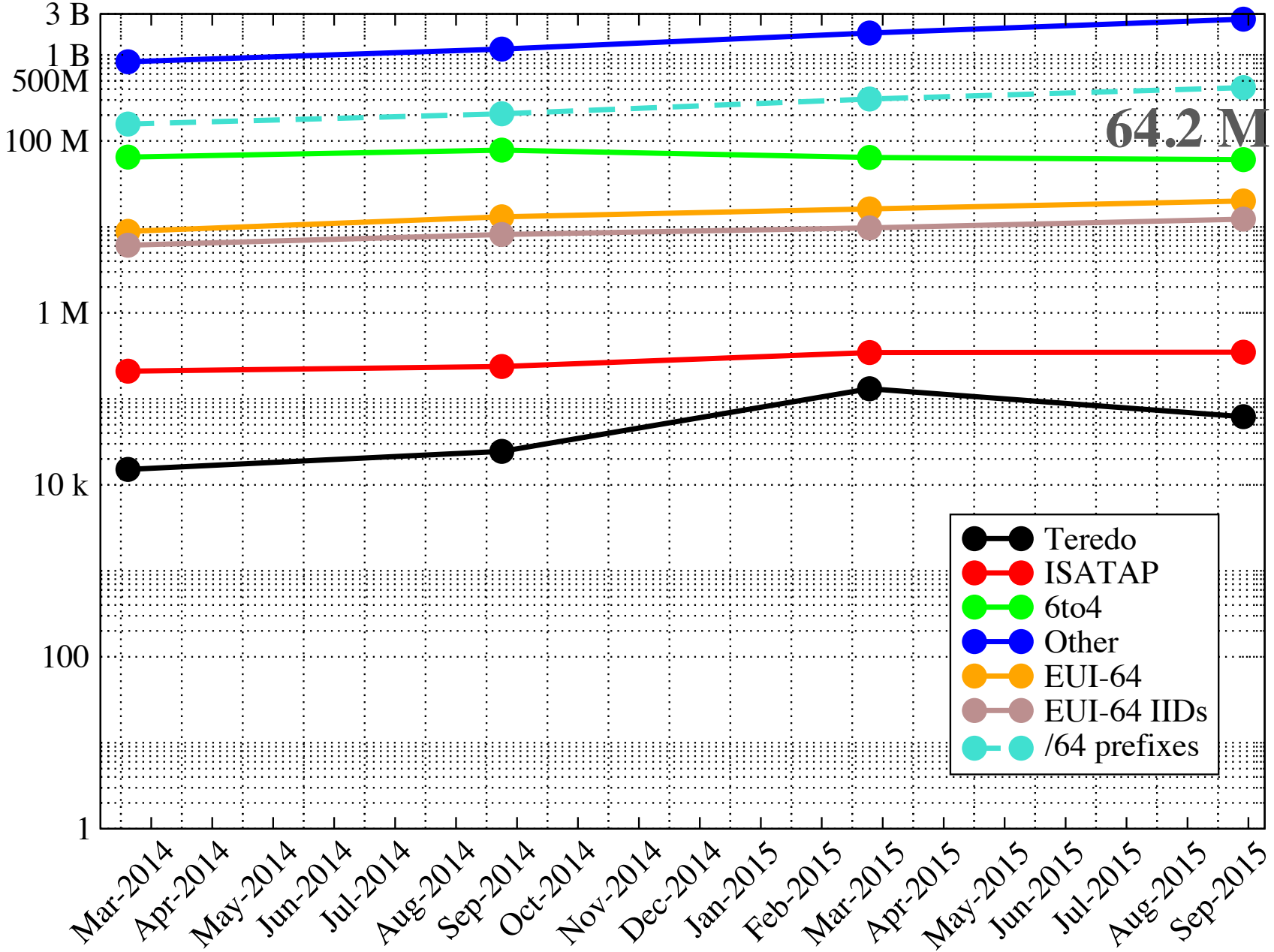
Active IPv6 WWW Client addresses: daily counts



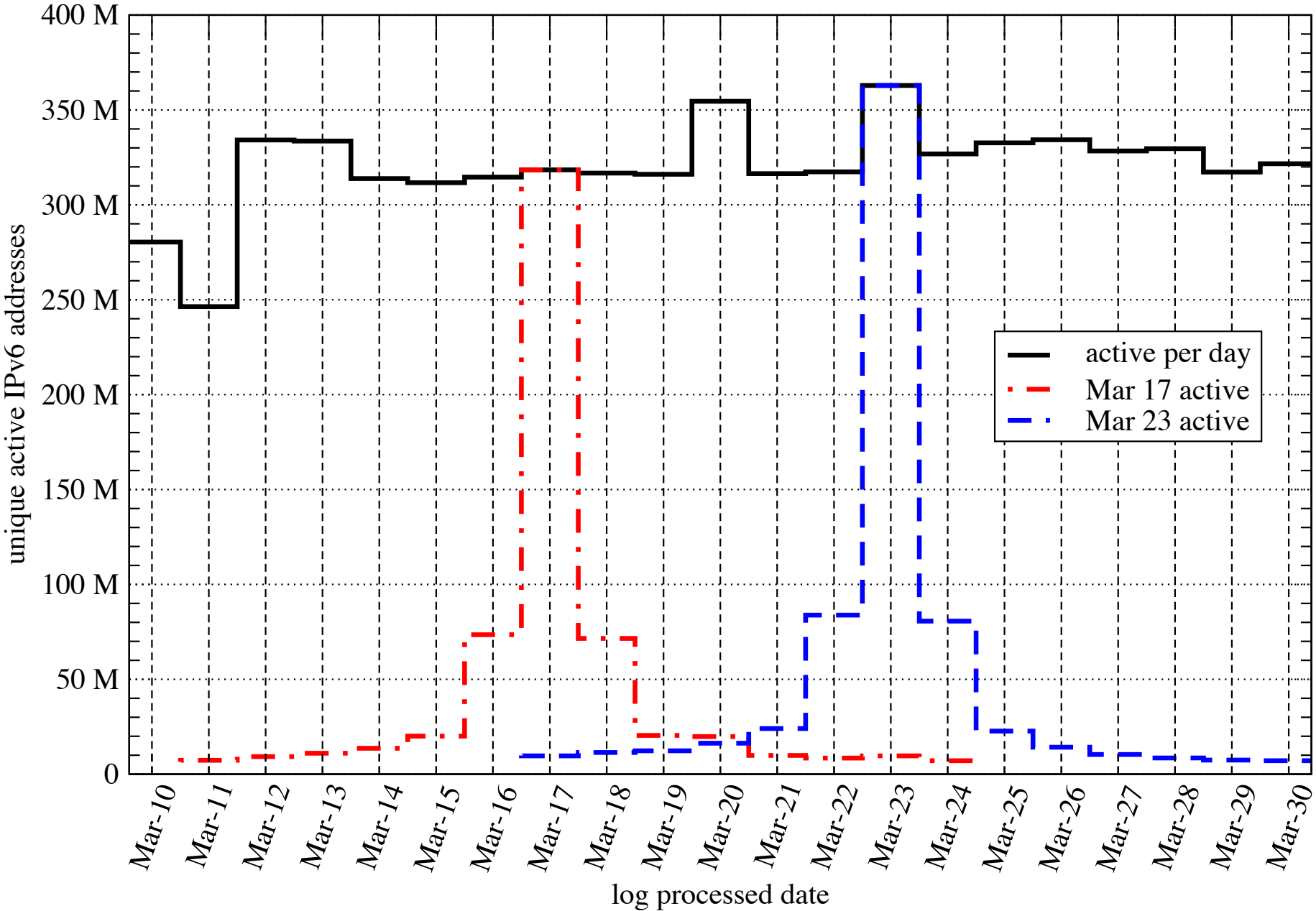
Active IPv6 WWW Client addresses: weekly counts



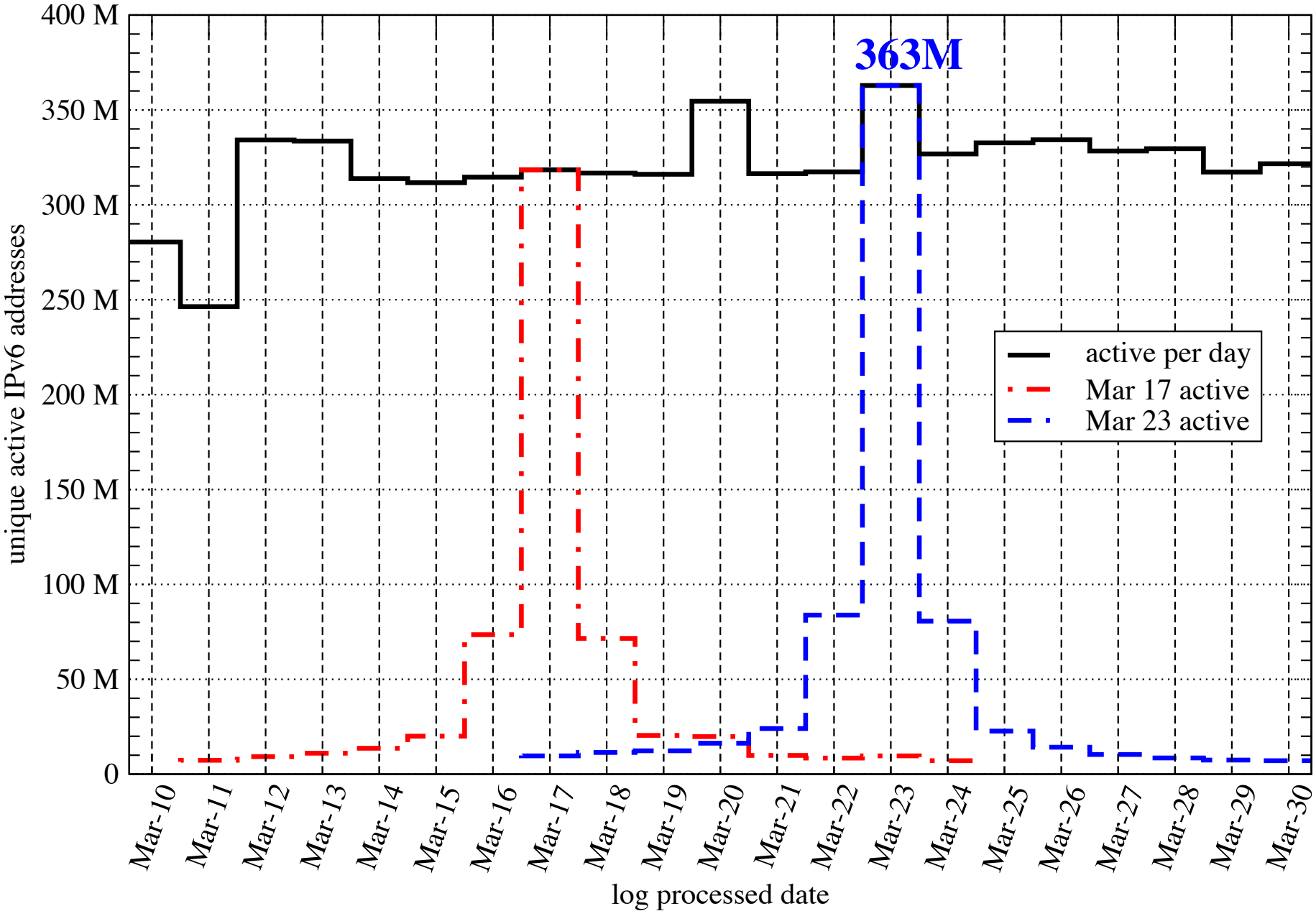
Active IPv6 WWW Client addresses: weekly counts (log scale)



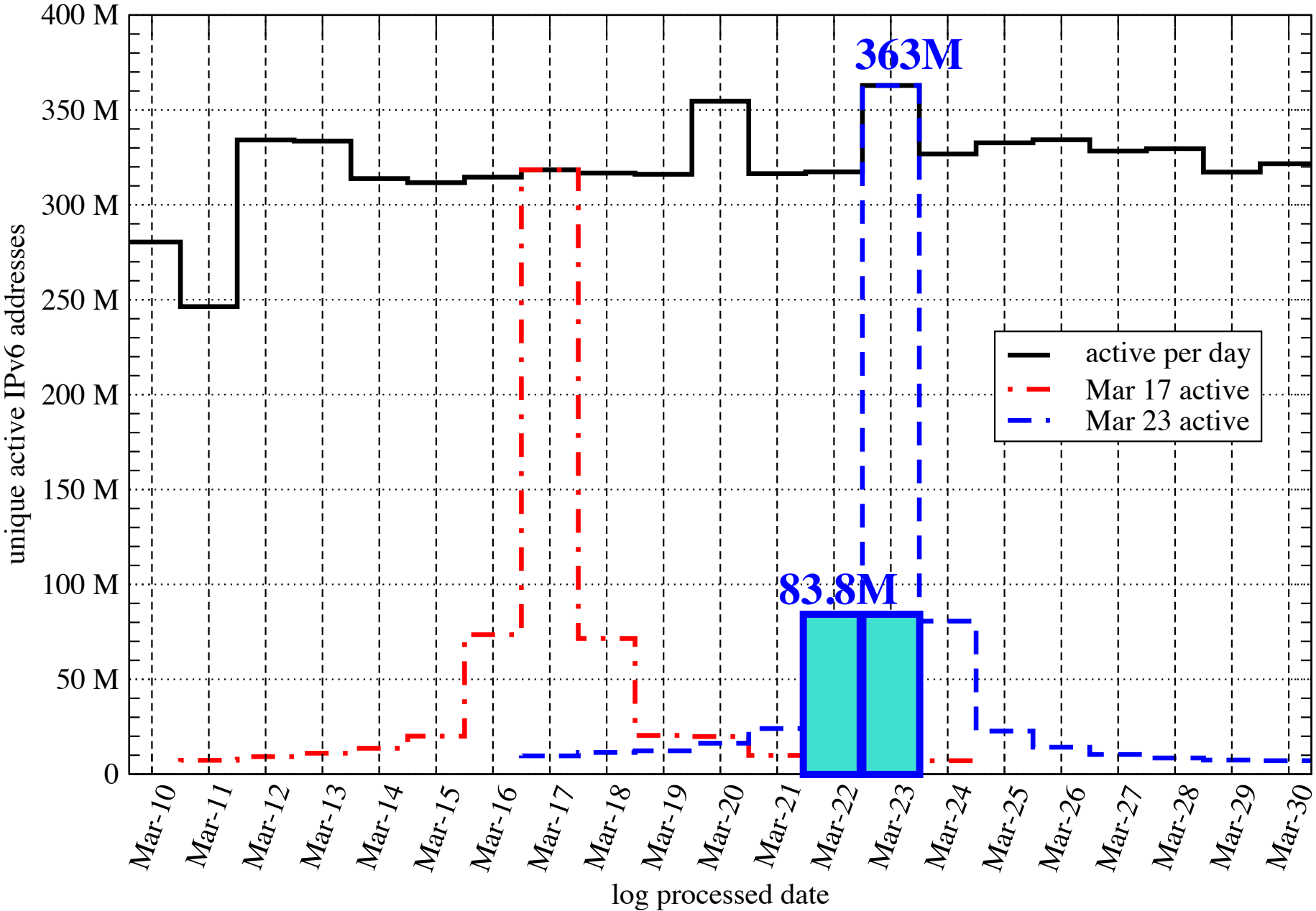
Temporal Address Classification: Stability Analysis



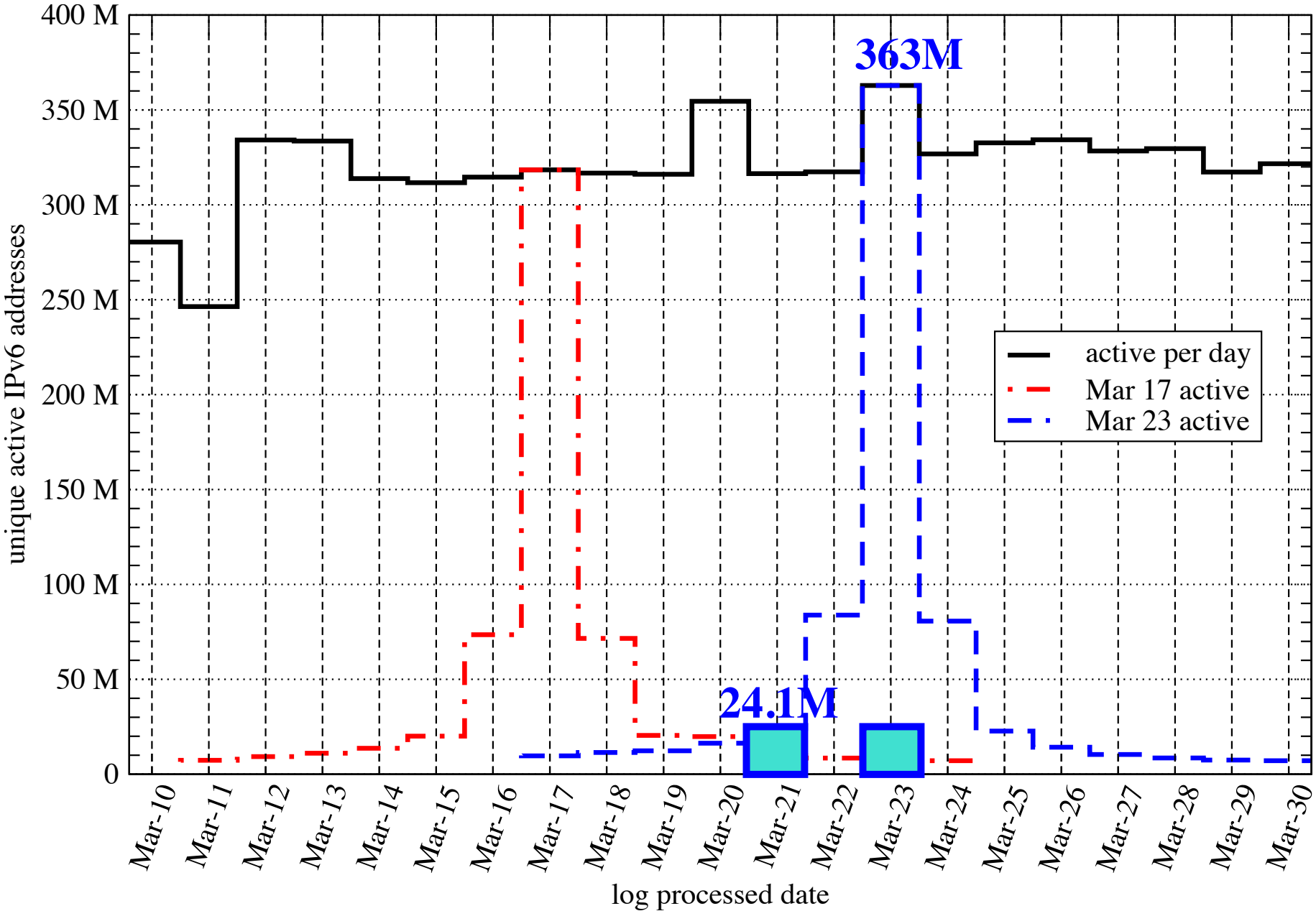
Address Stability: March 17-23, 2015 (1.80B v6 addresses)



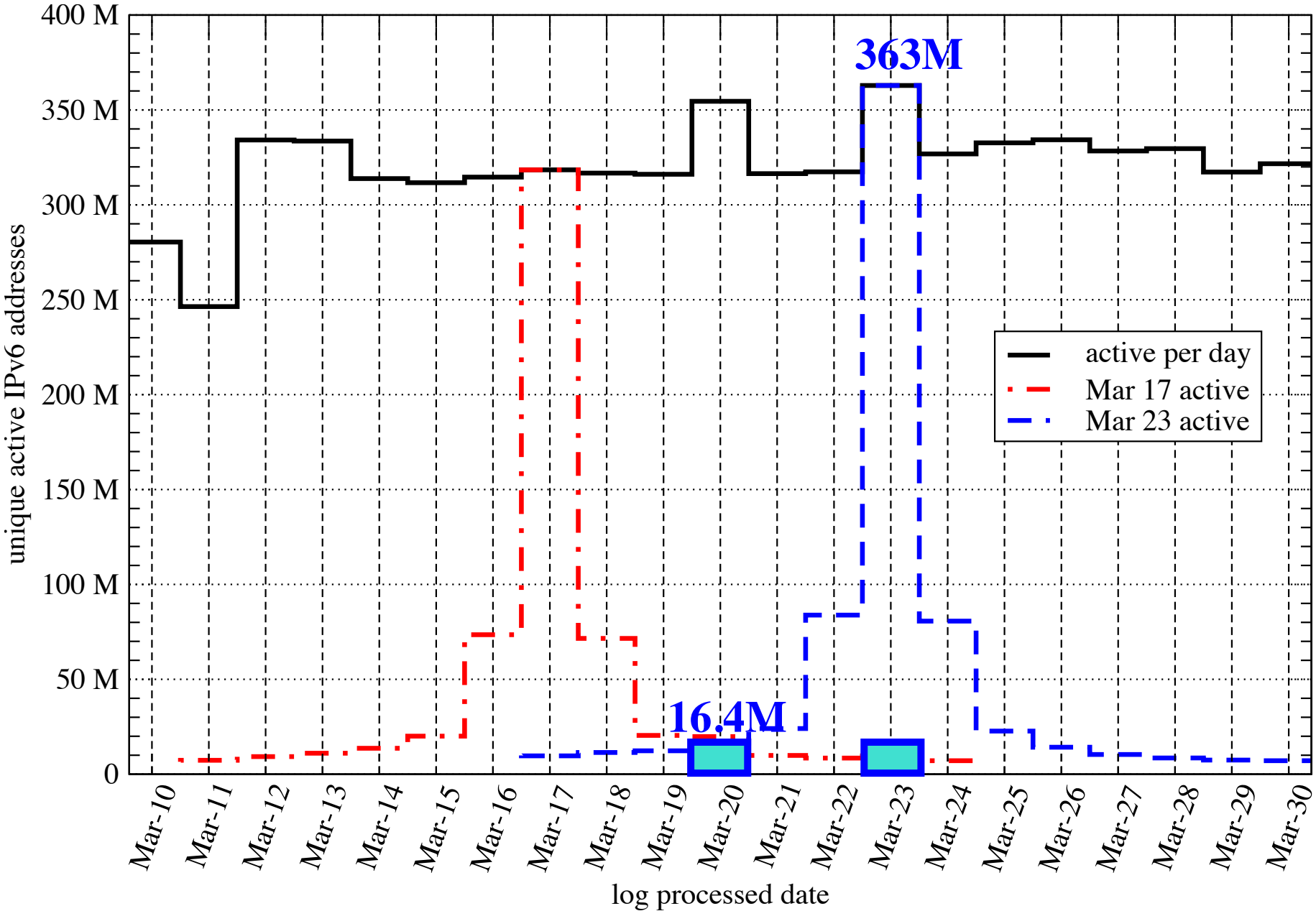
Address Stability: March 17-23, 2015 (1.80B v6 addresses)



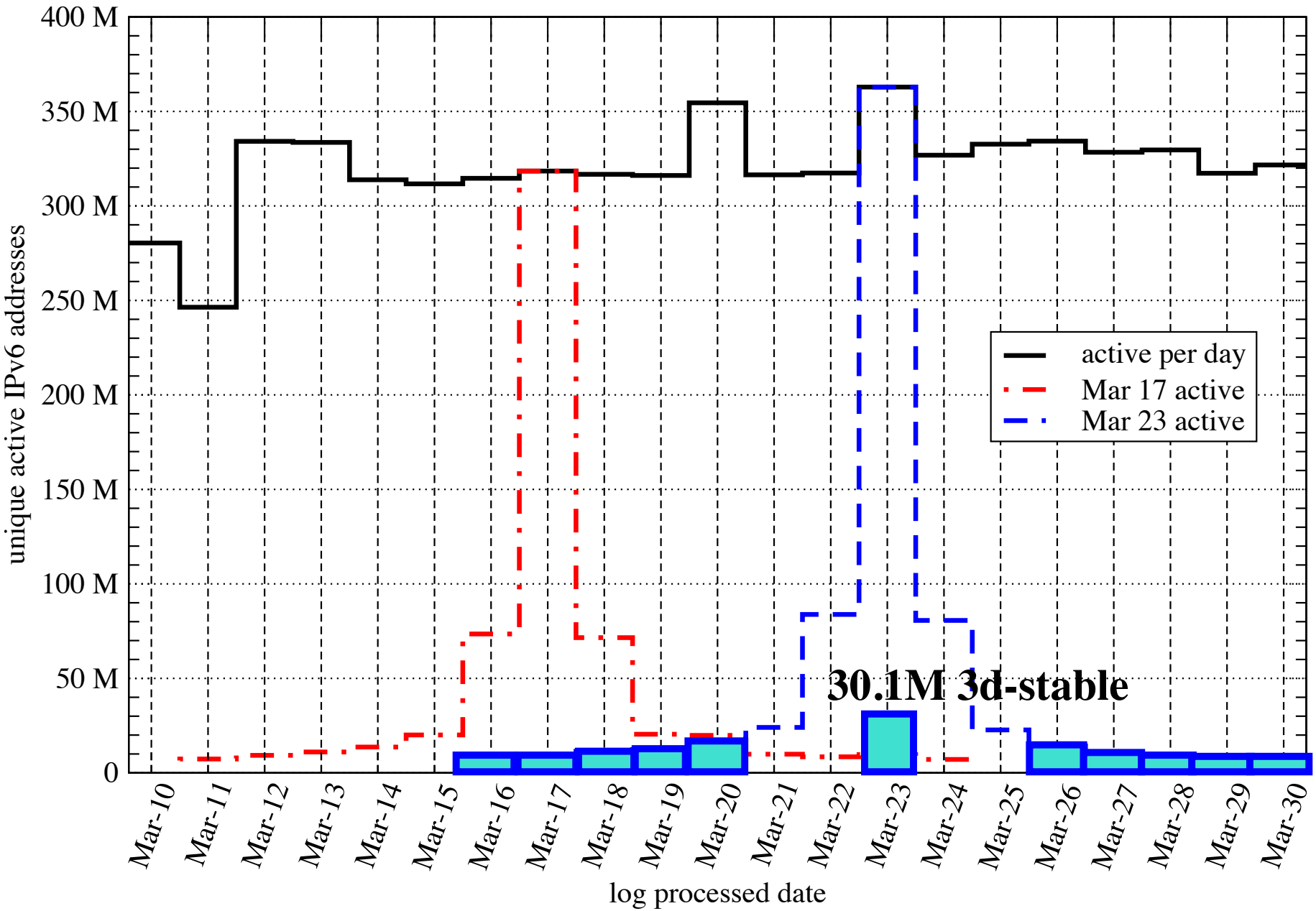
Address Stability: March 17-23, 2015 (1.80B v6 addresses)



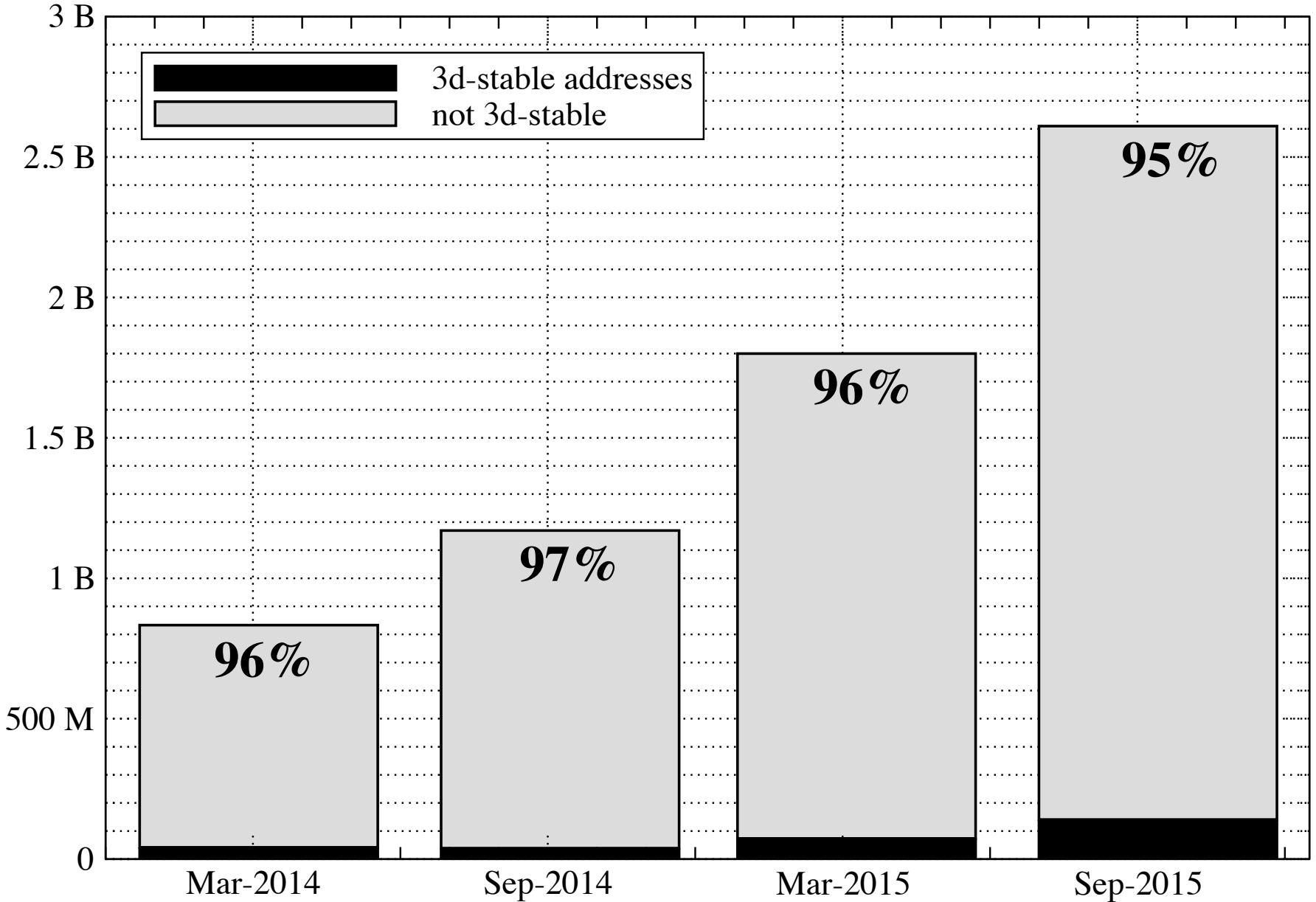
Address Stability: March 17-23, 2015 (1.80B v6 addresses)



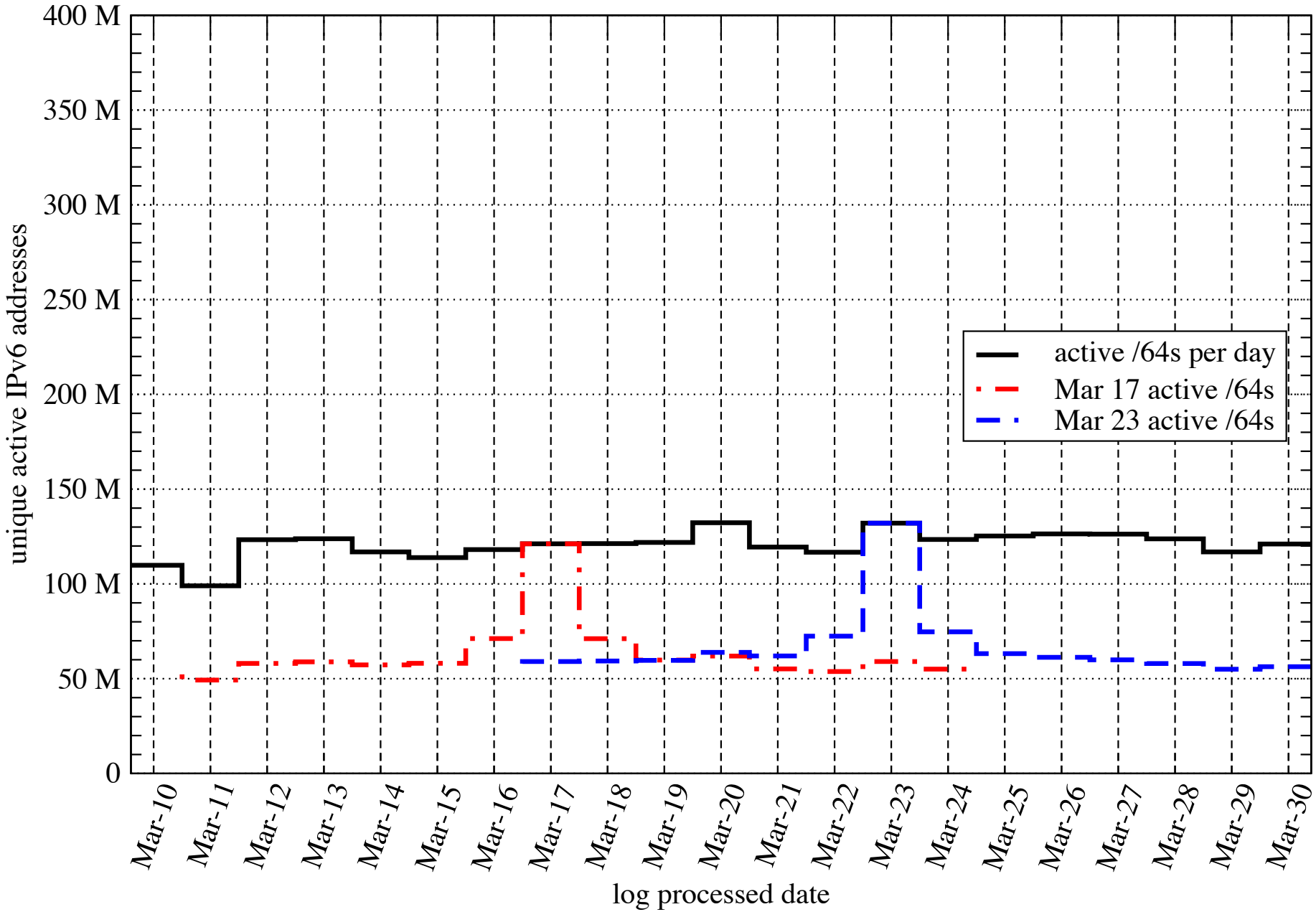
Address Stability: March 17-23, 2015 (1.80B v6 addresses)



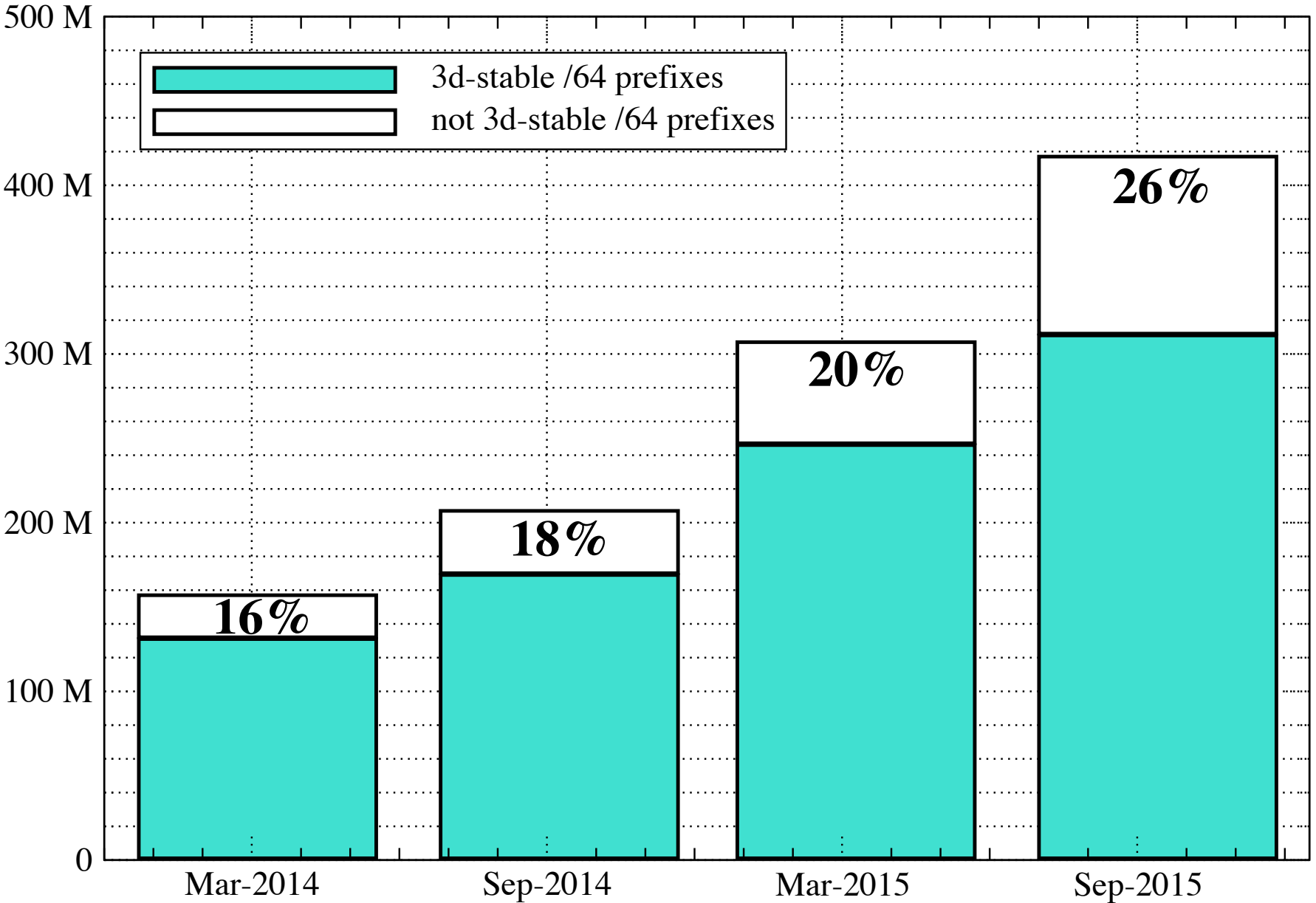
Address Stability: weekly



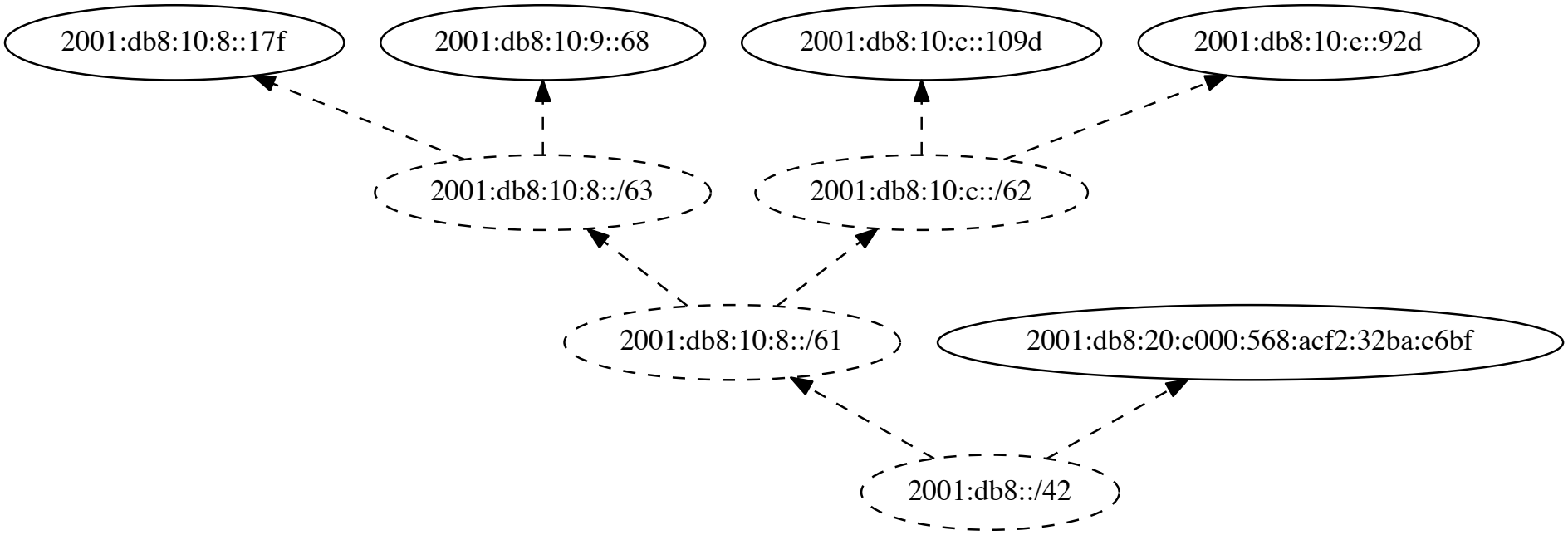
/64 Prefix Stability: March 17-23, 2015 (307M /64 prefixes)



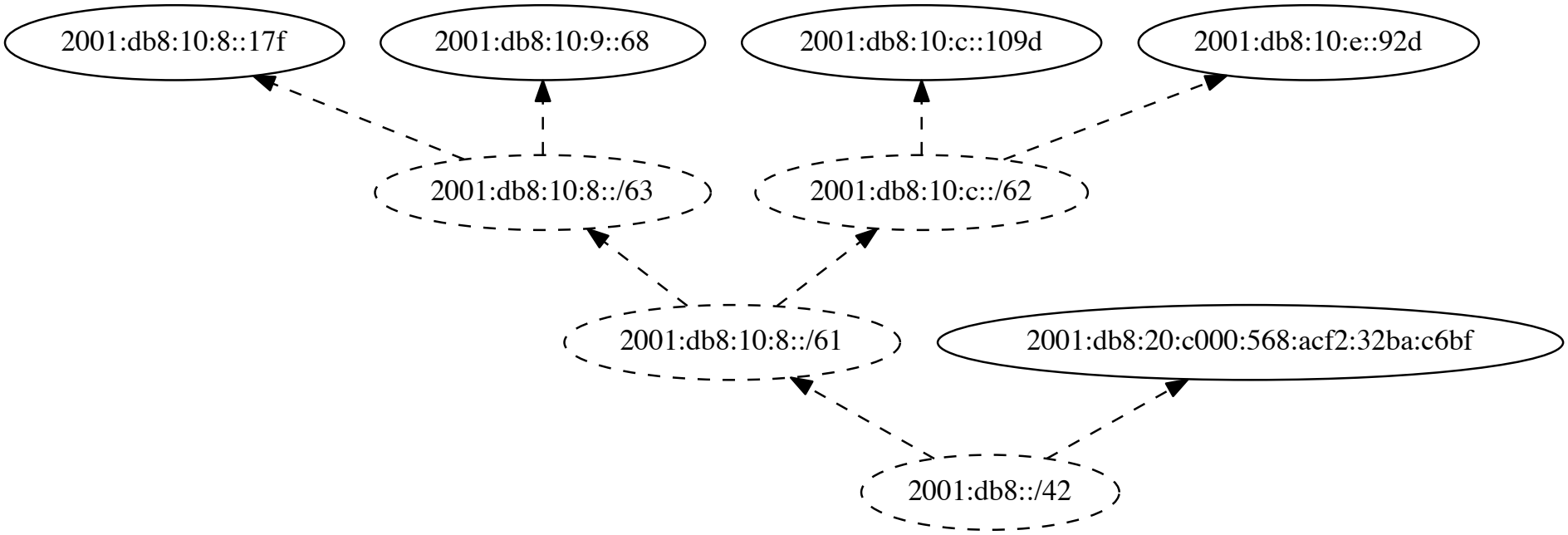
/64 Prefix Stability: Weekly



Spatial Address Classification: Level-Compressed Trees

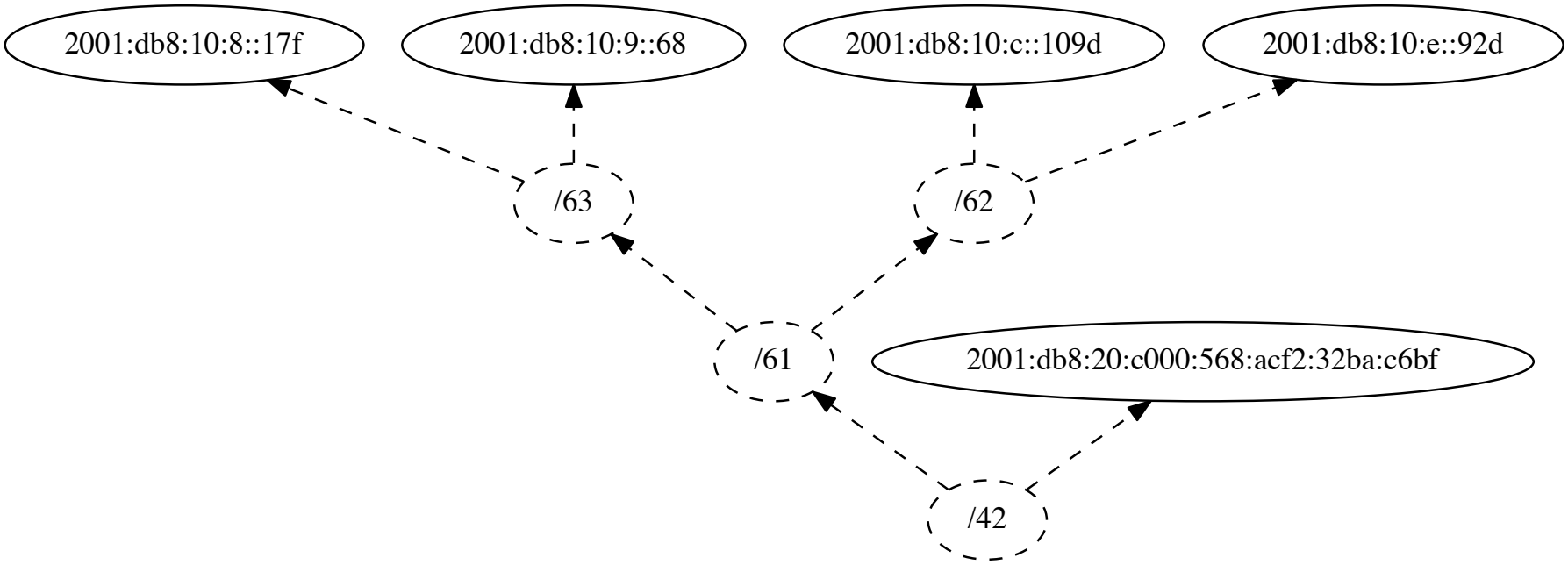


Binary PATRICIA Trie Example: Sample addrs, JP TelCo /32



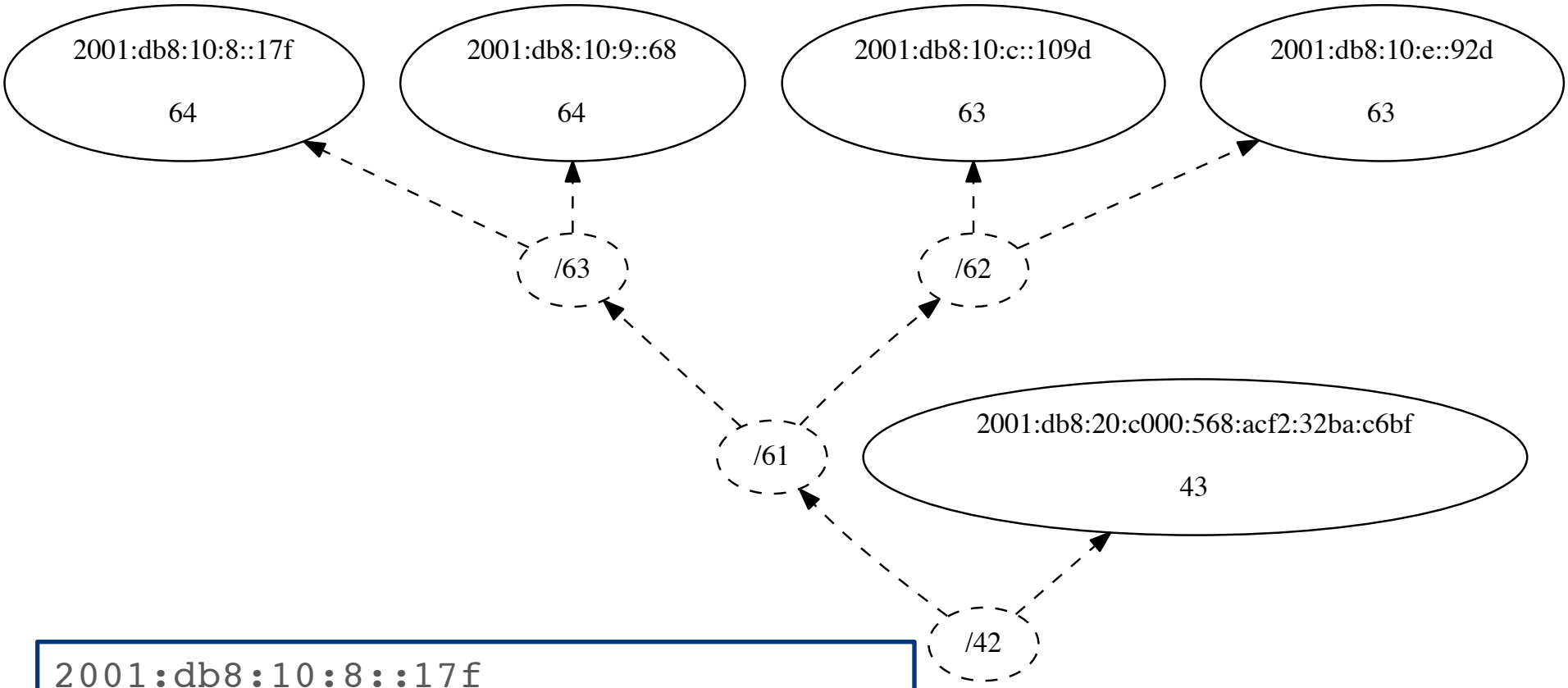

```
2001:db8:10:8::17f
2001:db8:10:9::68
2001:db8:10:c::109d
2001:db8:10:e::92d
2001:db8:20:c000:568:acf2:32ba:c6bf
```

Binary PATRICIA Trie Example: Sample addrs, JP TelCo /32



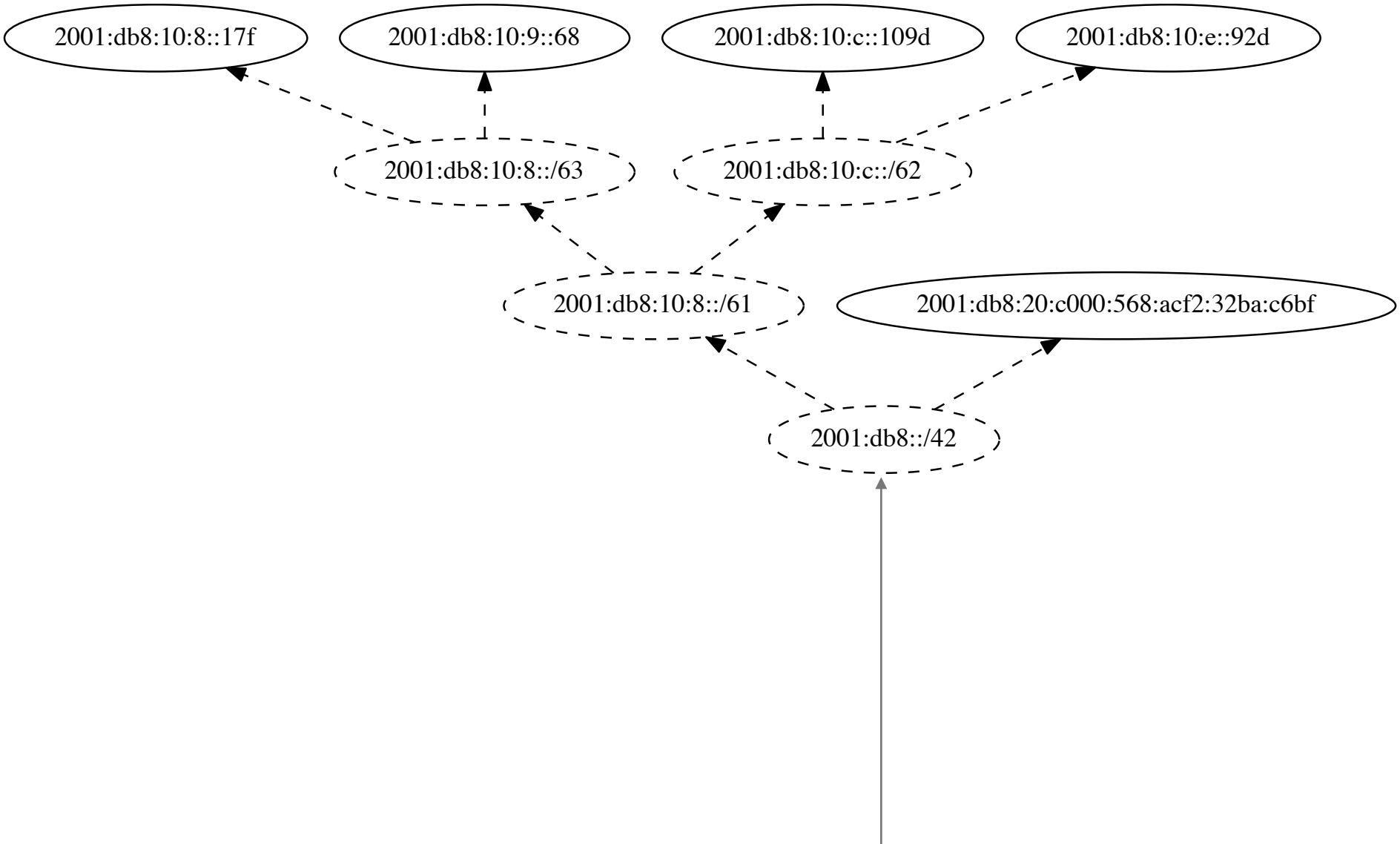

```
2001:db8:10:8::17f
2001:db8:10:9::68
2001:db8:10:c::109d
2001:db8:10:e::92d
2001:db8:20:c000:568:acf2:32ba:c6bf
```

Binary PATRICIA Trie Example: Sample addrs, JP TelCo /32

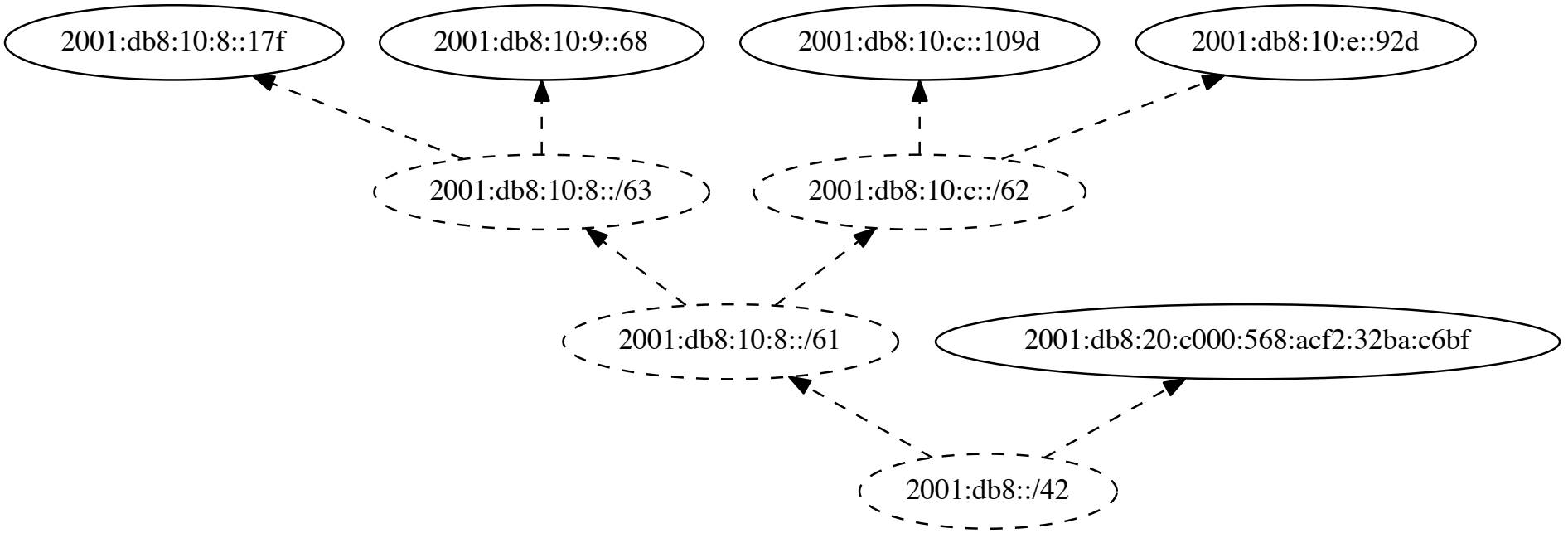



```
2001:db8:10:8::17f
2001:db8:10:9::68
2001:db8:10:c::109d
2001:db8:10:e::92d
2001:db8:20:c000:568:acf2:32ba:c6bf
```

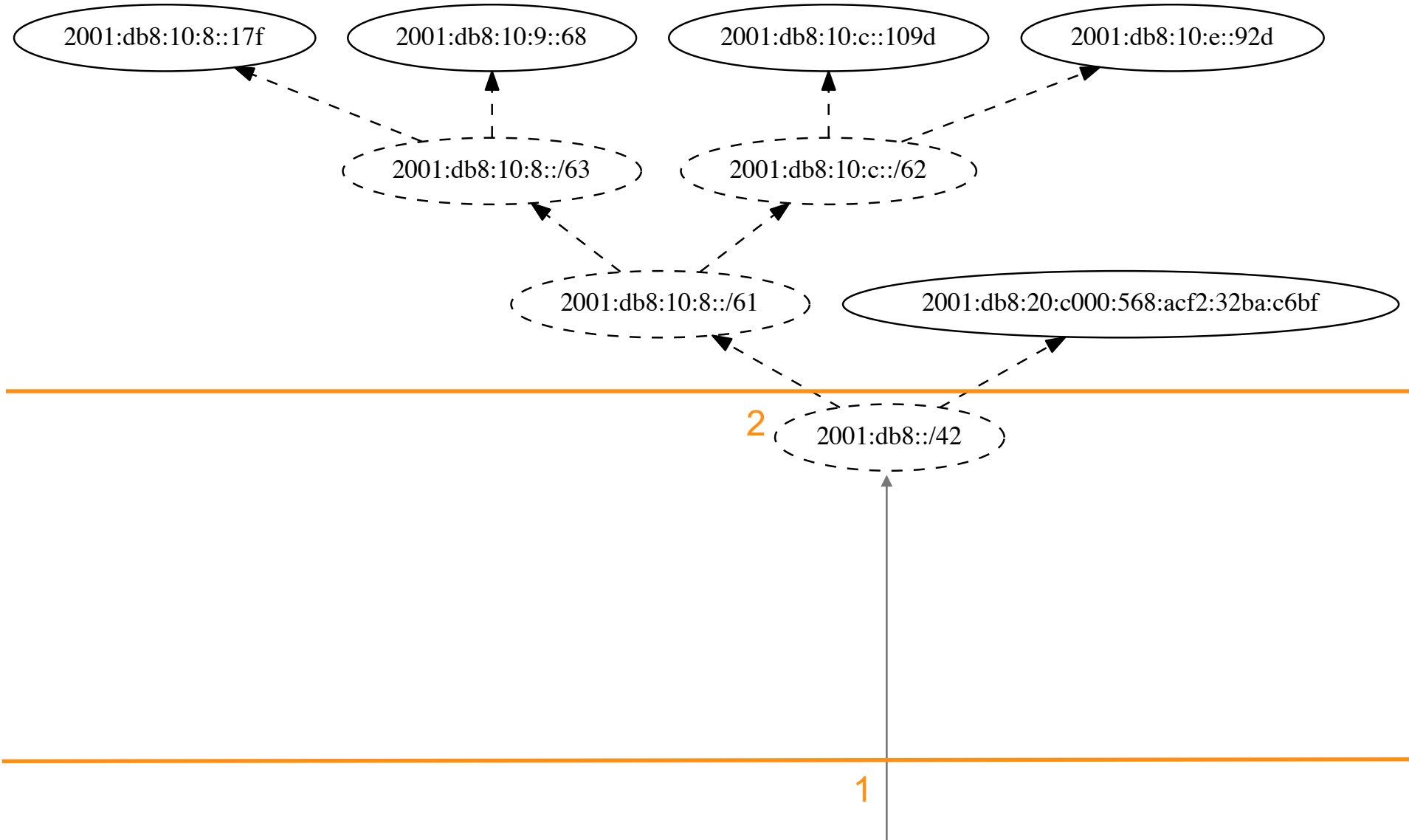
Spatial Address Classification: Level-Compressed Trees



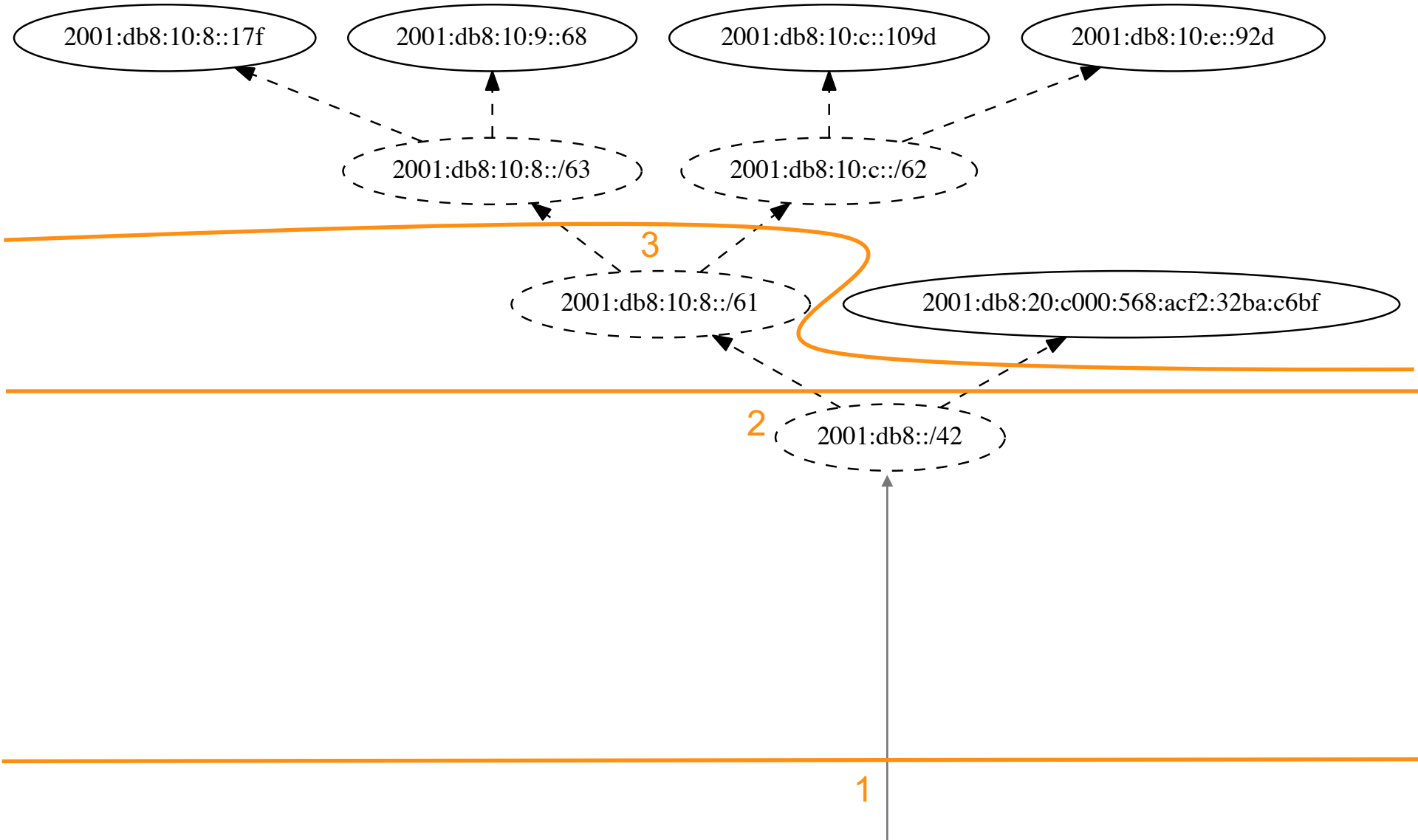
Spatial Address Classification: Level-Compressed Trees



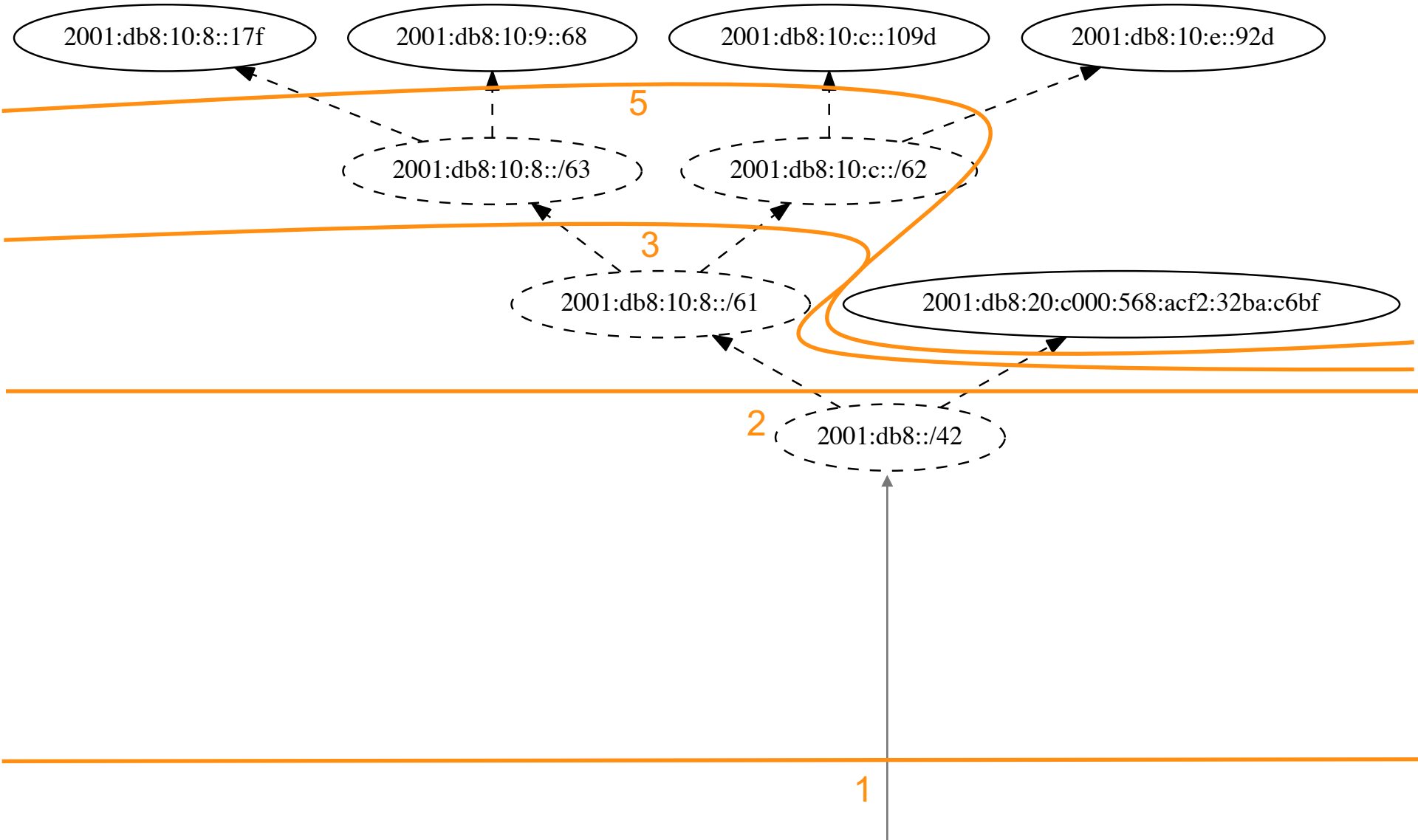
Spatial Address Classification: Level-Compressed Trees



Spatial Address Classification: Level-Compressed Trees

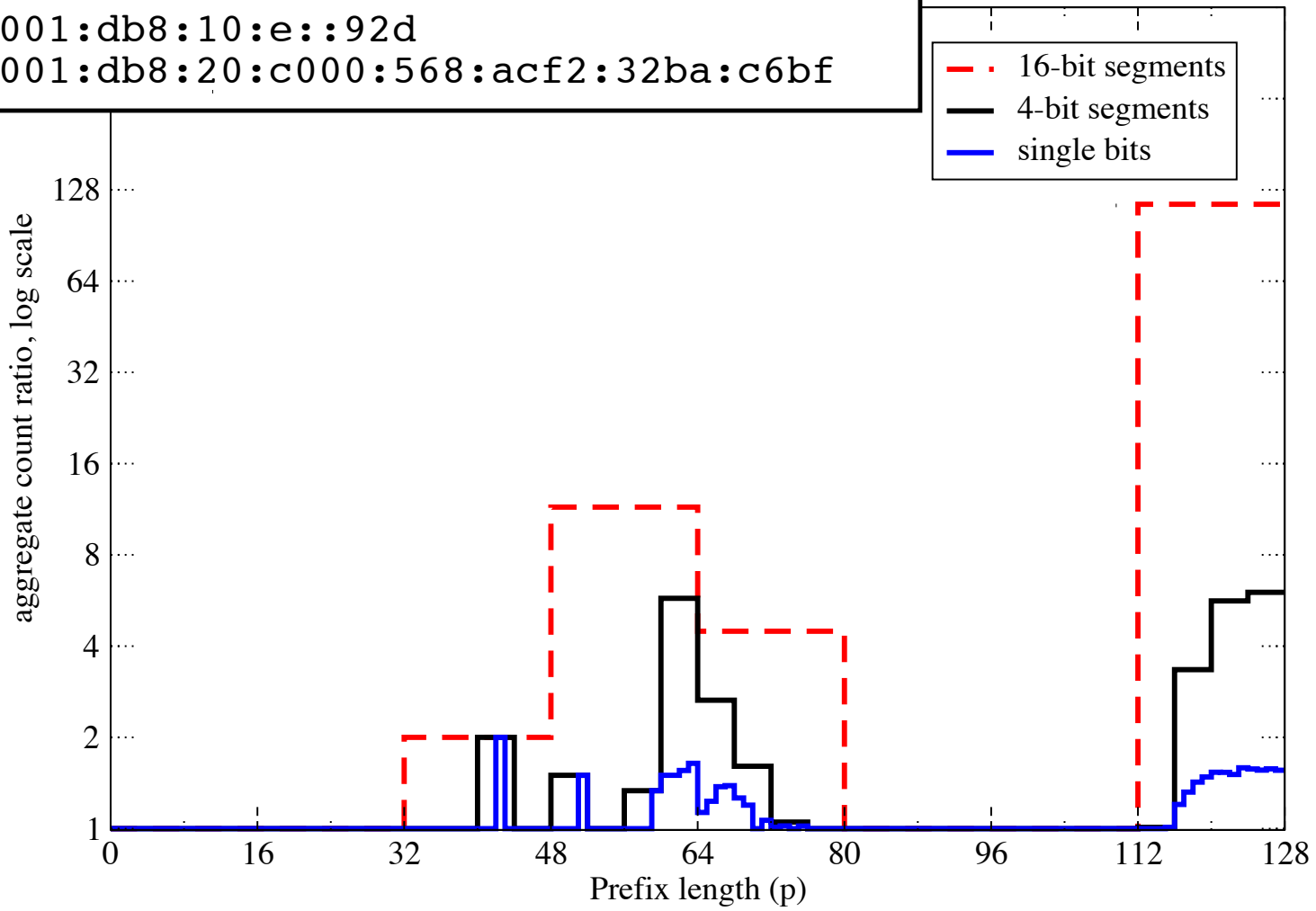


Spatial Address Classification: Level-Compressed Trees



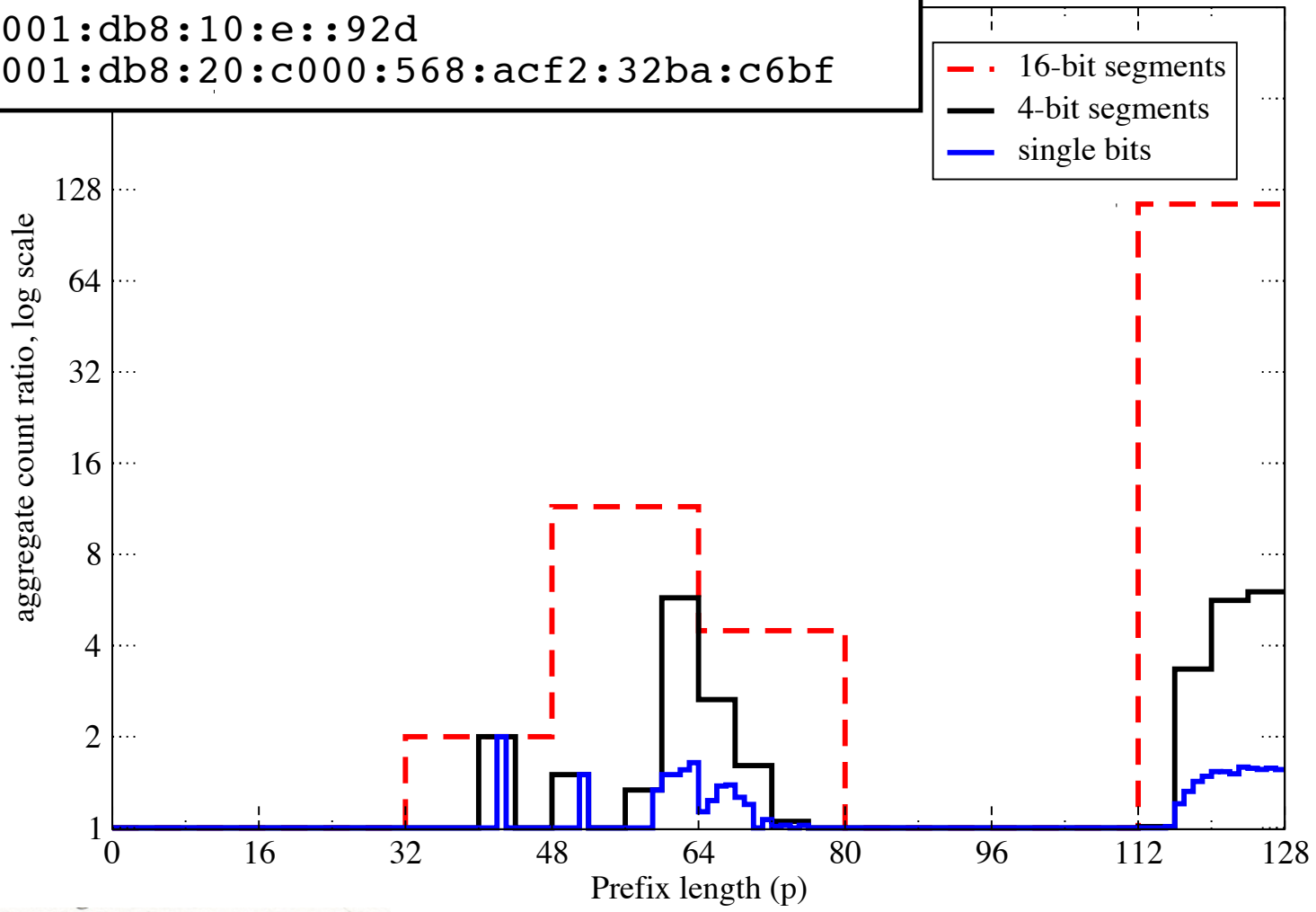
From Tree to Multi-Resolution Aggregate (MRA) Plot…

```
2001:db8:10:8::17f
2001:db8:10:9::68
2001:db8:10:c::109d
2001:db8:10:e::92d
2001:db8:20:c000:568:acf2:32ba:c6bf
```



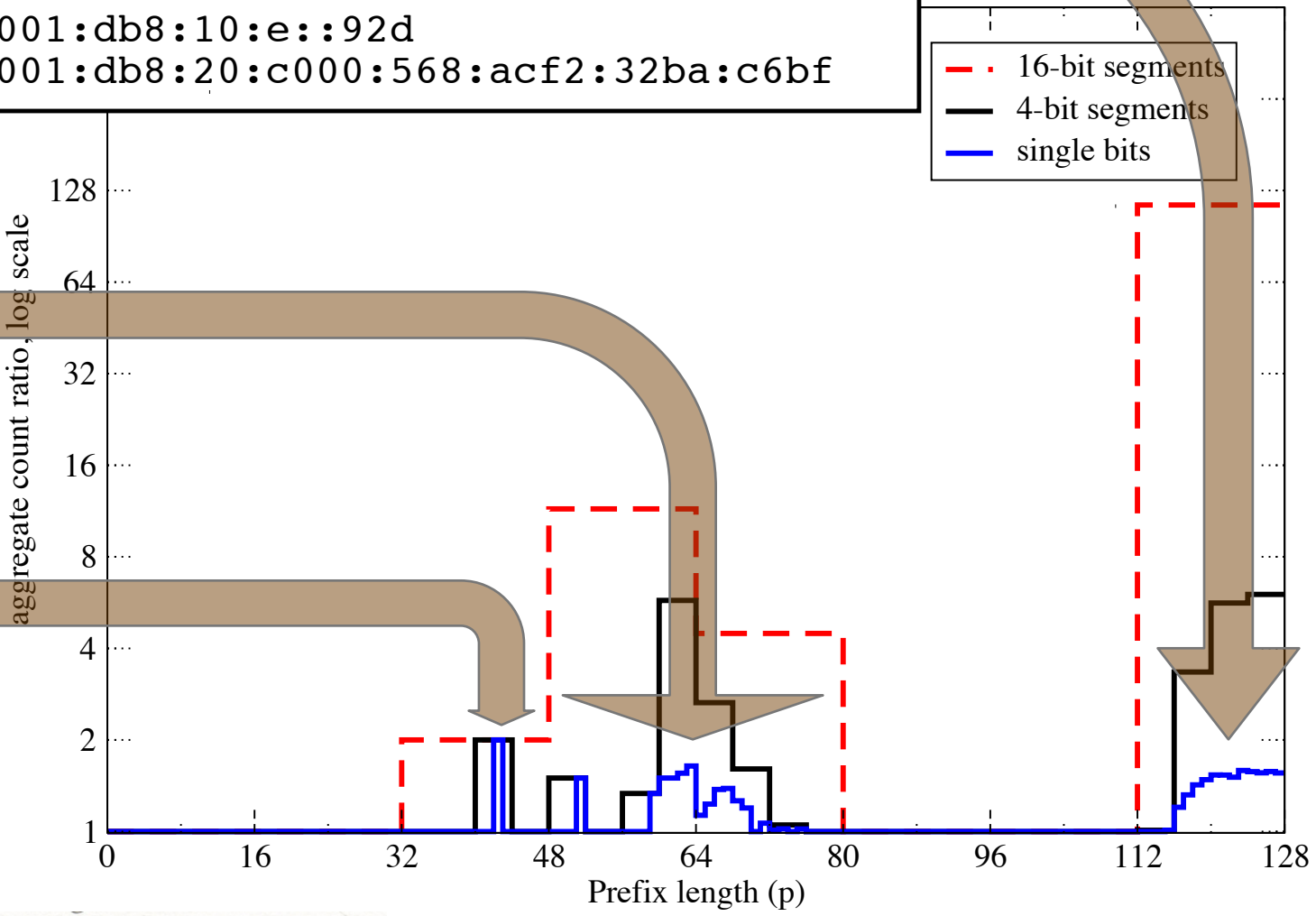
From Tree to Multi-Resolution Aggregate (MRA) Plot…

```
2001:db8:10:8::17f
2001:db8:10:9::68
2001:db8:10:c::109d
2001:db8:10:e::92d
2001:db8:20:c000:568:acf2:32ba:c6bf
```



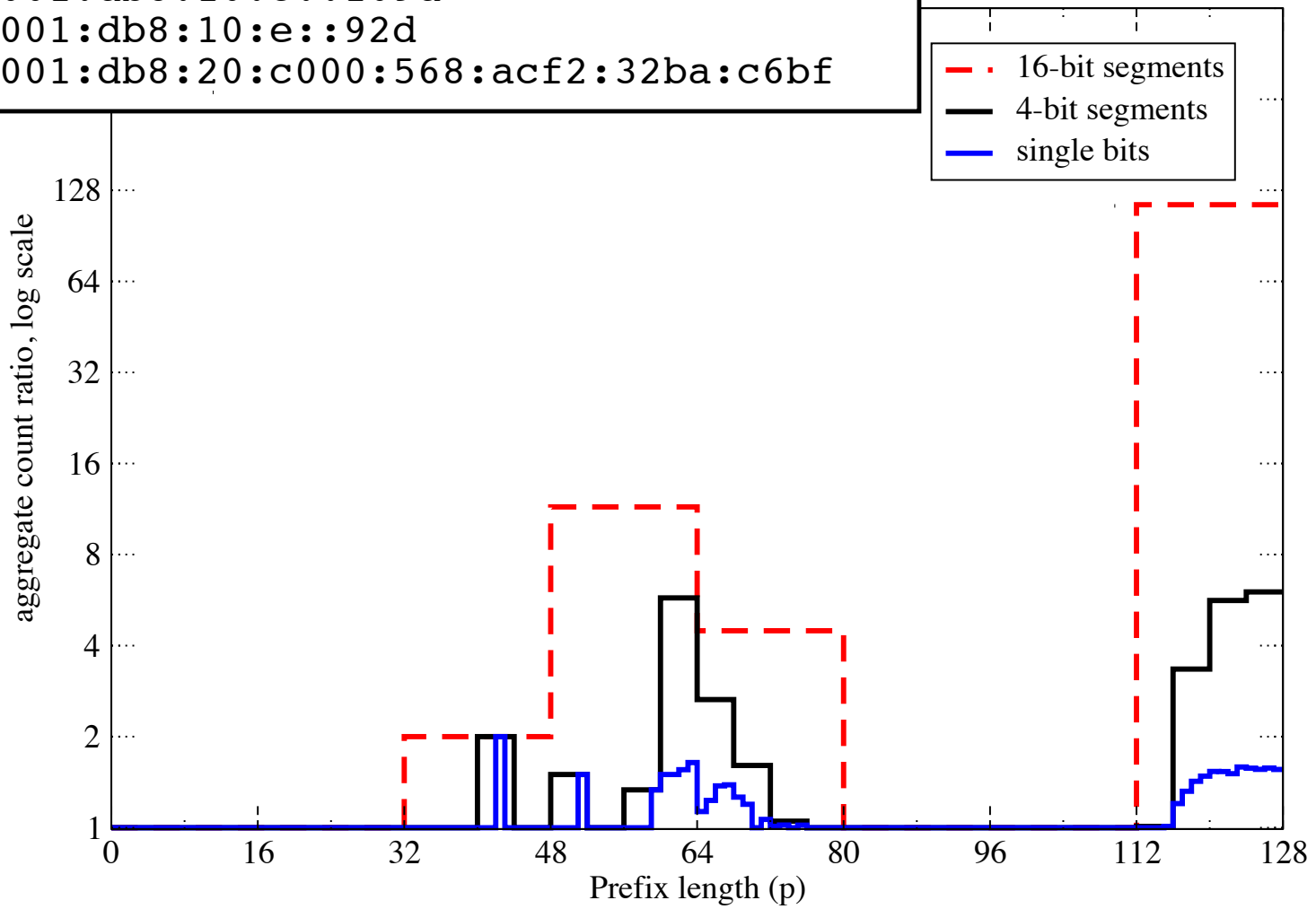
A Japan-inspired explanation of the MRA Plot

```
2001:db8:10:8::17f
2001:db8:10:9::68
2001:db8:10:c::109d
2001:db8:10:e::92d
2001:db8:20:c000:568:acf2:32ba:c6bf
```



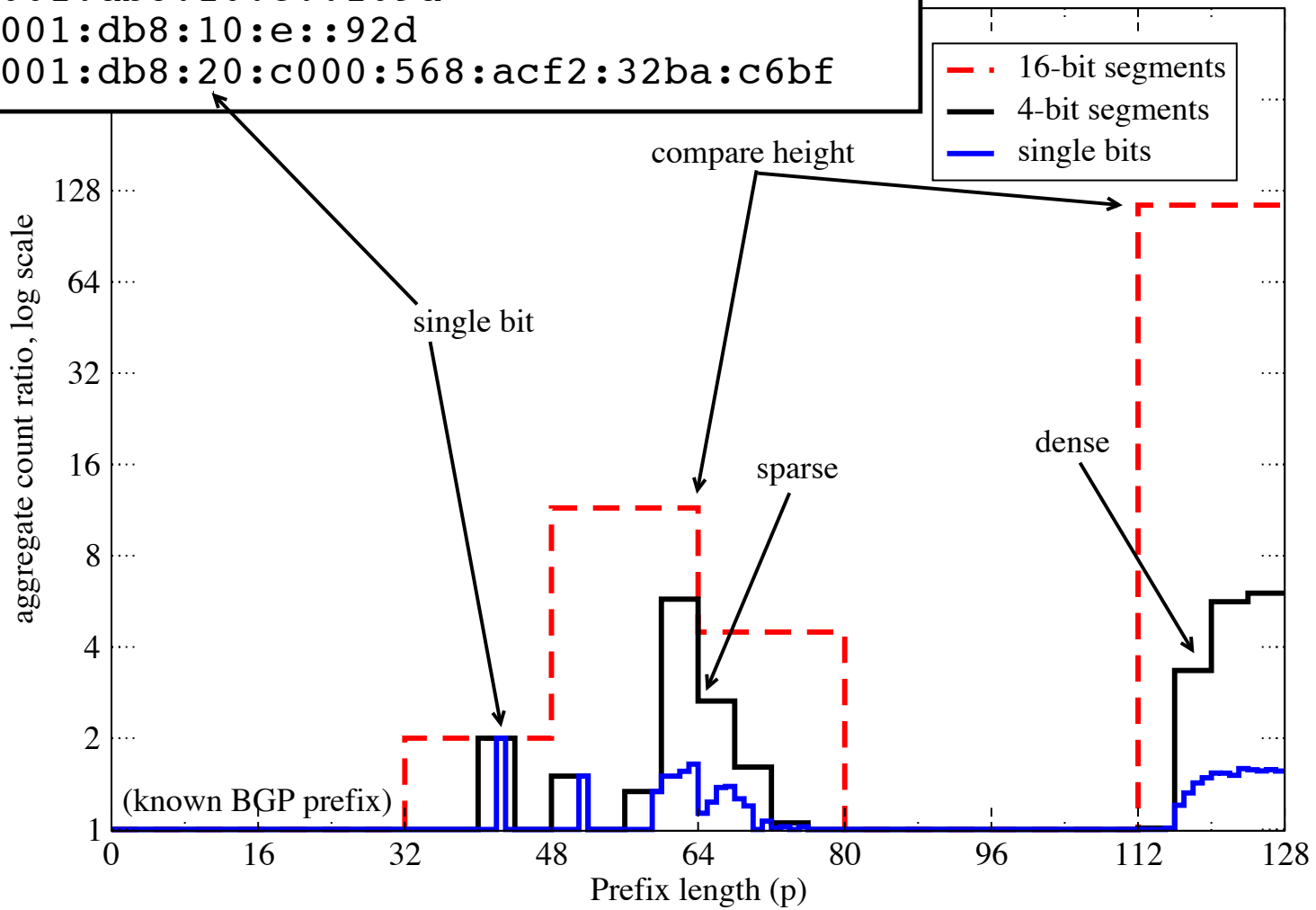
MRA Plot: JP TelCo /32 (~12K active WWW client addrs)

```
2001:db8:10:8::17f
2001:db8:10:9::68
2001:db8:10:c::109d
2001:db8:10:e::92d
2001:db8:20:c000:568:acf2:32ba:c6bf
```



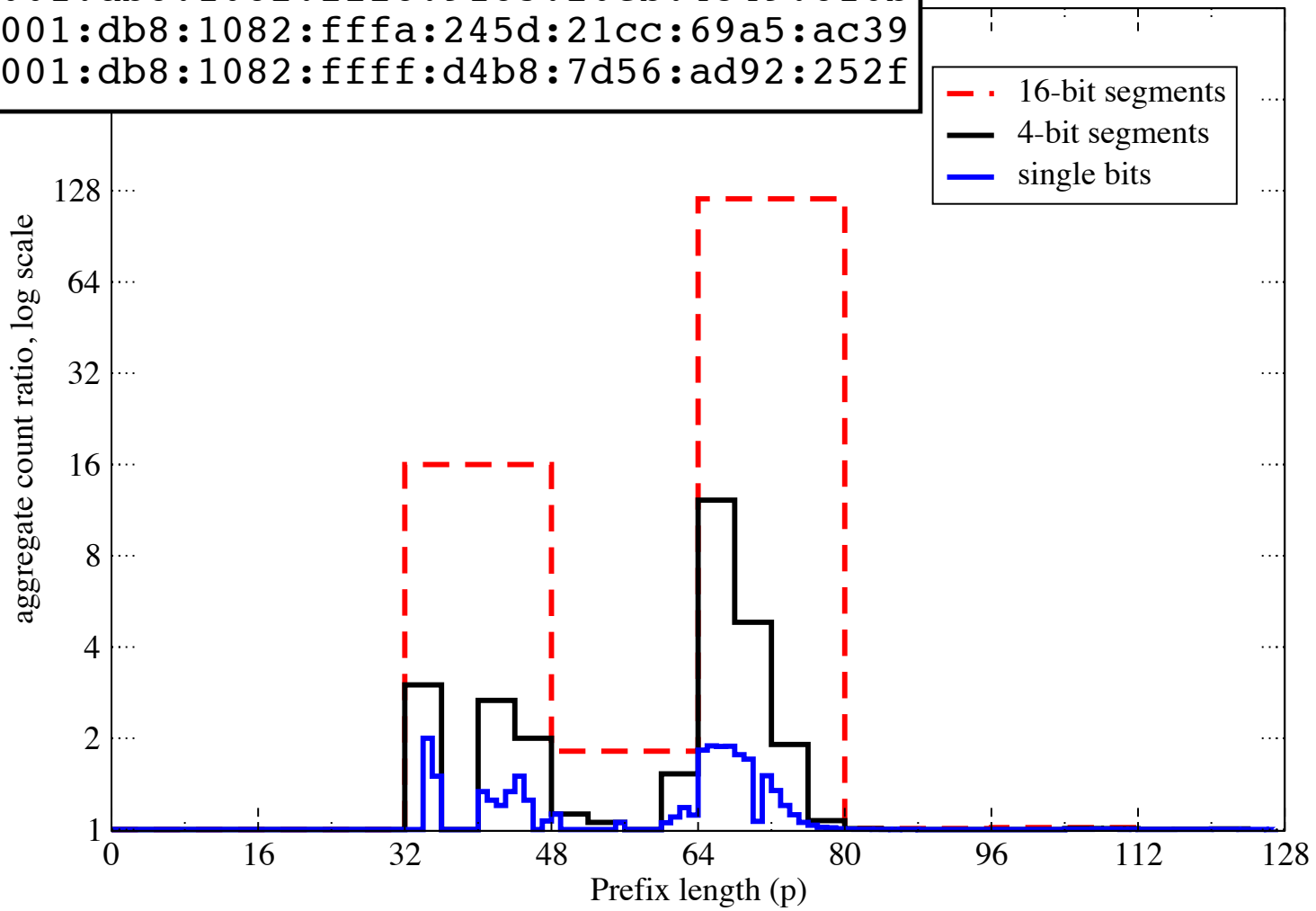
MRA Plot: JP TelCo /32 (~12K active WWW client addrs)

```
2001:db8:10:8::17f
2001:db8:10:9::68
2001:db8:10:c::109d
2001:db8:10:e::92d
2001:db8:20:c000:568:acf2:32ba:c6bf
```



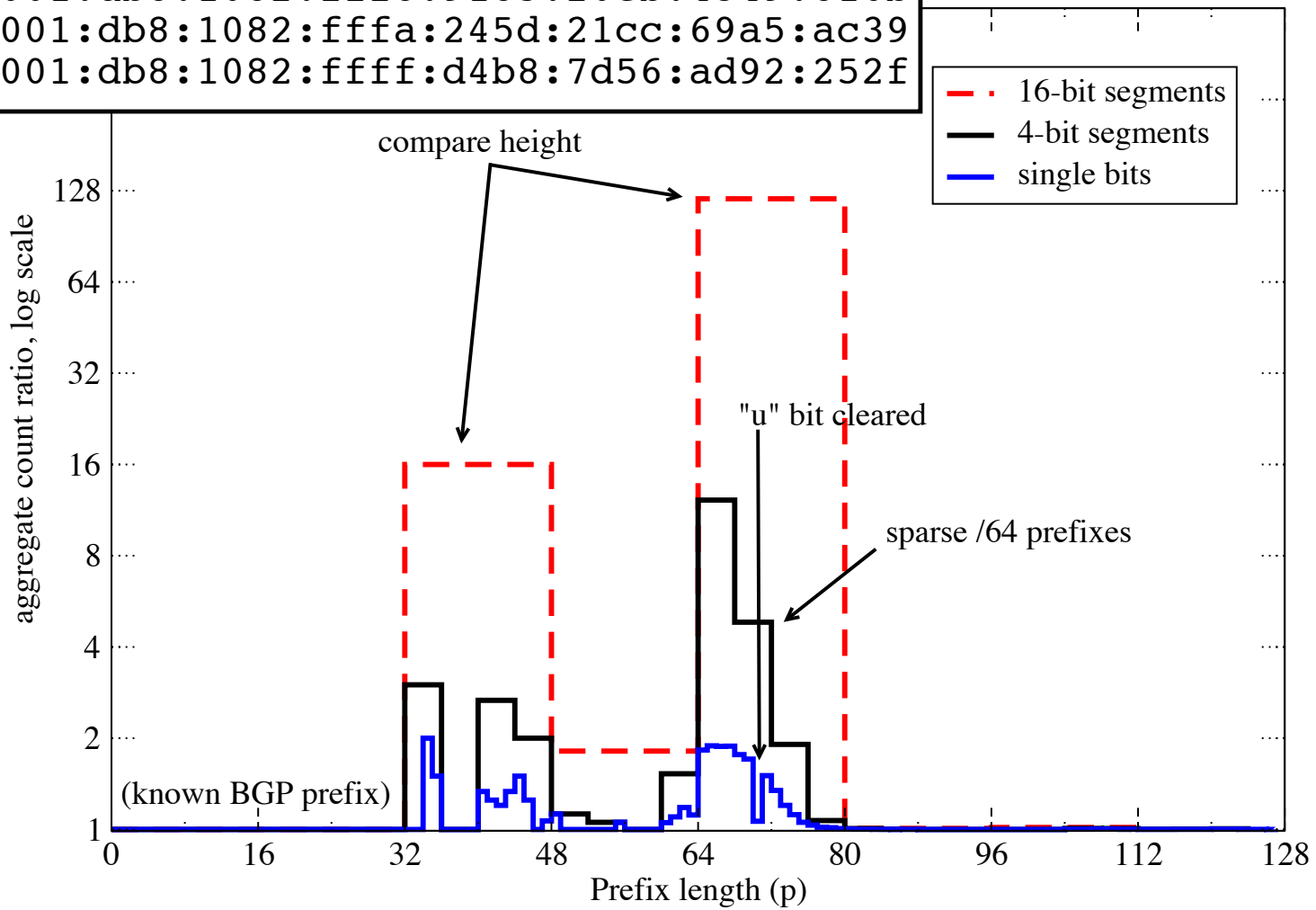
MRA Plot: US Uni /32 (~7K active WWW client addrs)

```
2001:db8:e:0:e174:5522:1ada:1e5b
2001:db8:1082:fff8:ab:ebfd:9b16:6095
2001:db8:1082:fff8:9185:20eb:4349:816b
2001:db8:1082:fffa:245d:21cc:69a5:ac39
2001:db8:1082:ffff:d4b8:7d56:ad92:252f
```

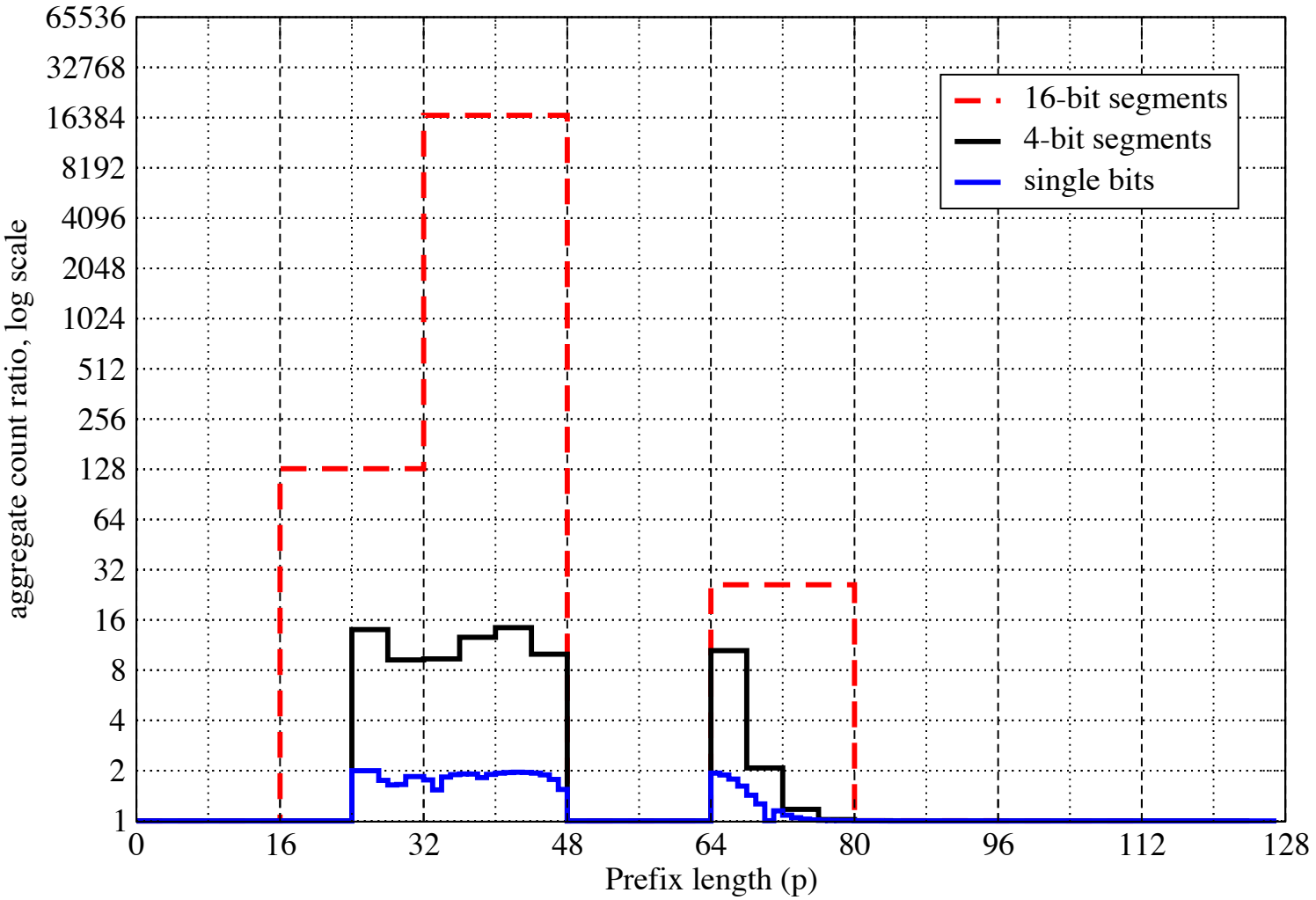


MRA Plot: US Uni /32 (~7K active WWW client addrs)

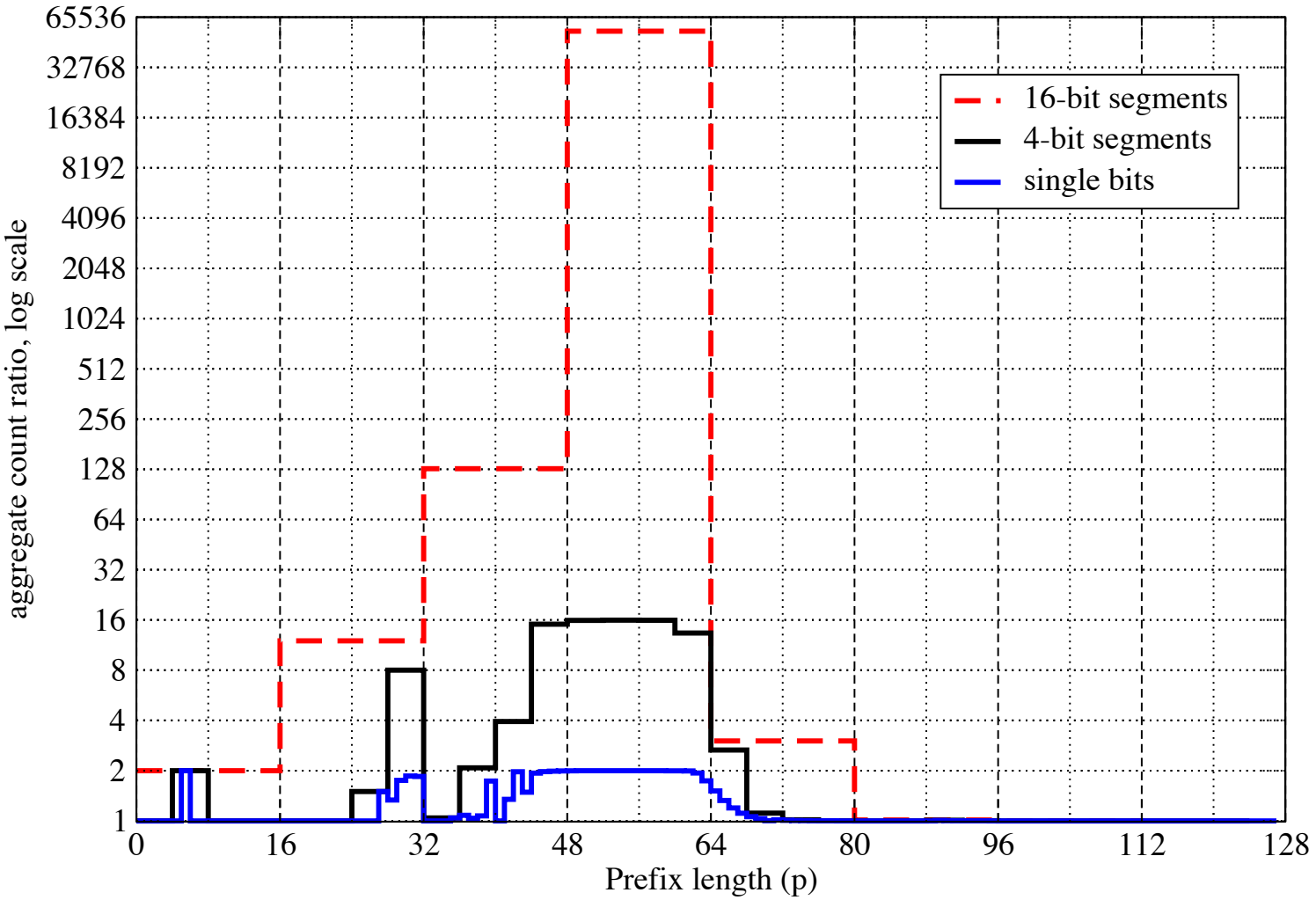
```
2001:db8:e:0:e174:5522:1ada:1e5b
2001:db8:1082:fff8:ab:ebfd:9b16:6095
2001:db8:1082:fff8:9185:20eb:4349:816b
2001:db8:1082:fffa:245d:21cc:69a5:ac39
2001:db8:1082:ffff:d4b8:7d56:ad92:252f
```



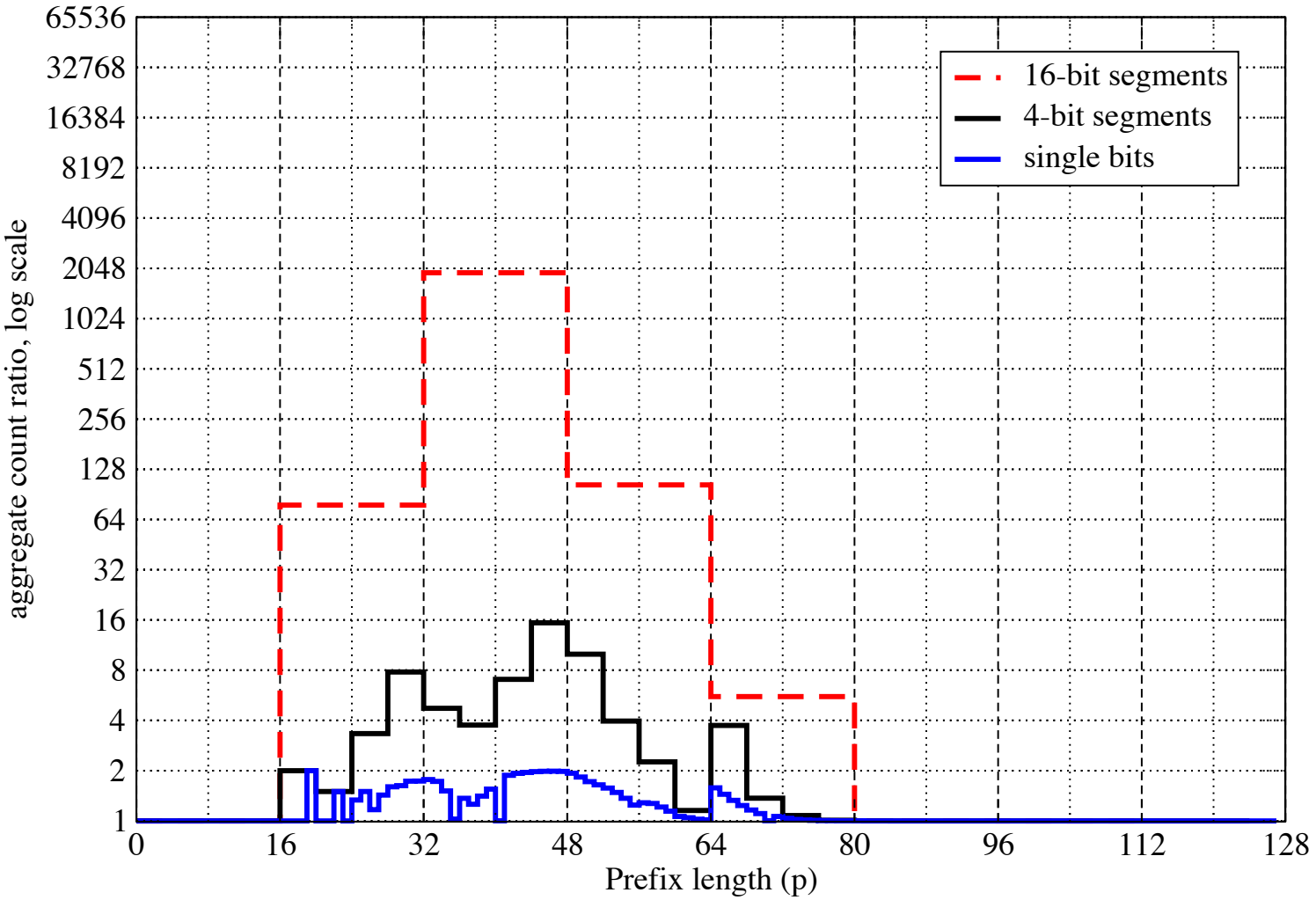
MRA Plot: JP ISP: 57.0M active client addrs, 2.18M /64s



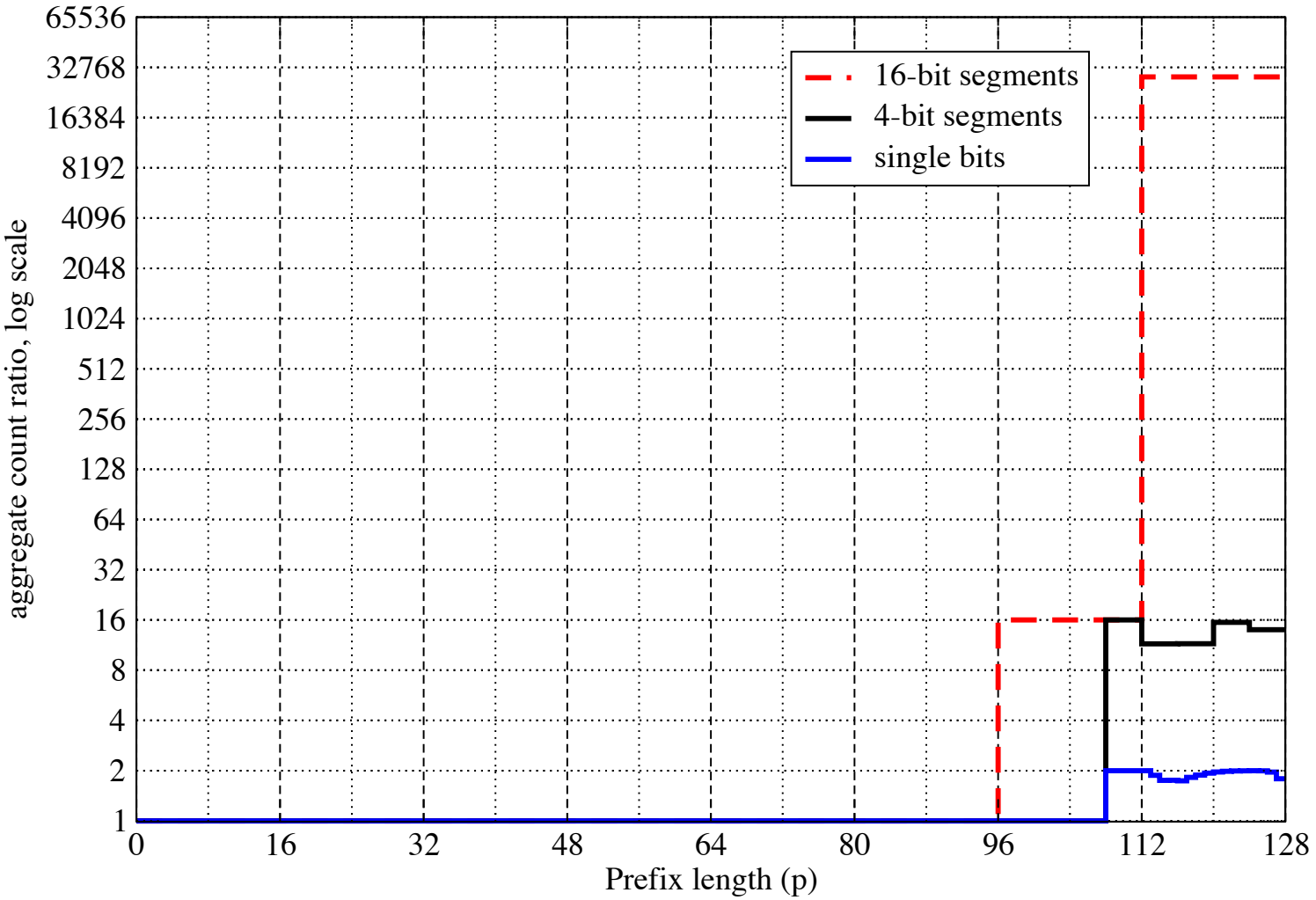
MRA Plot: US mobile: 510M active client addrs, 167M /64s



MRA Plot: EU ISP: 86.2M active client addrs, 15.5M /64s



MRA Plot: a /56 prefix: 459K active client addrs, 1 active /64



Visualizing the Active Internet: IPv4 by Hilbert Curve Heatmap

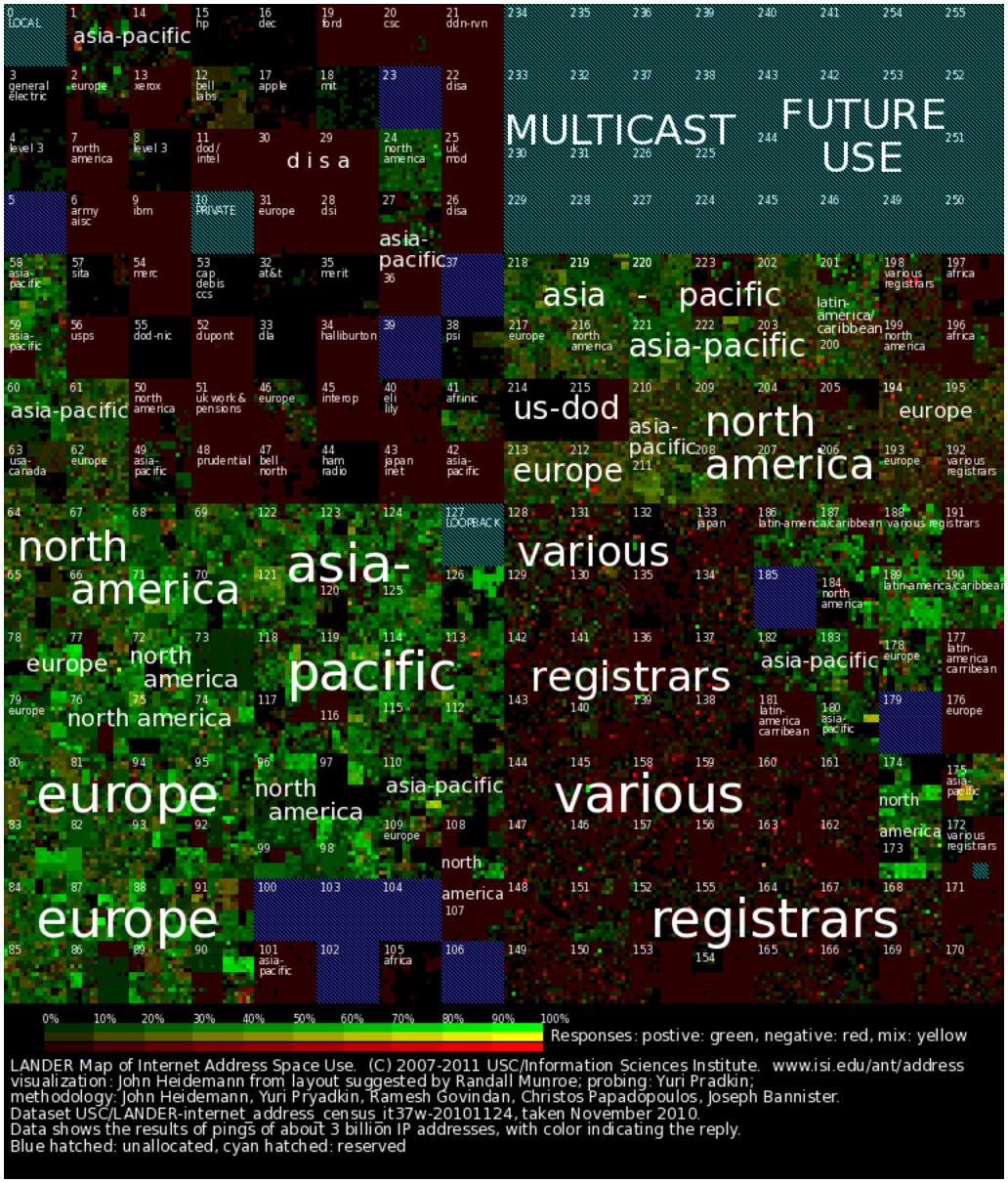
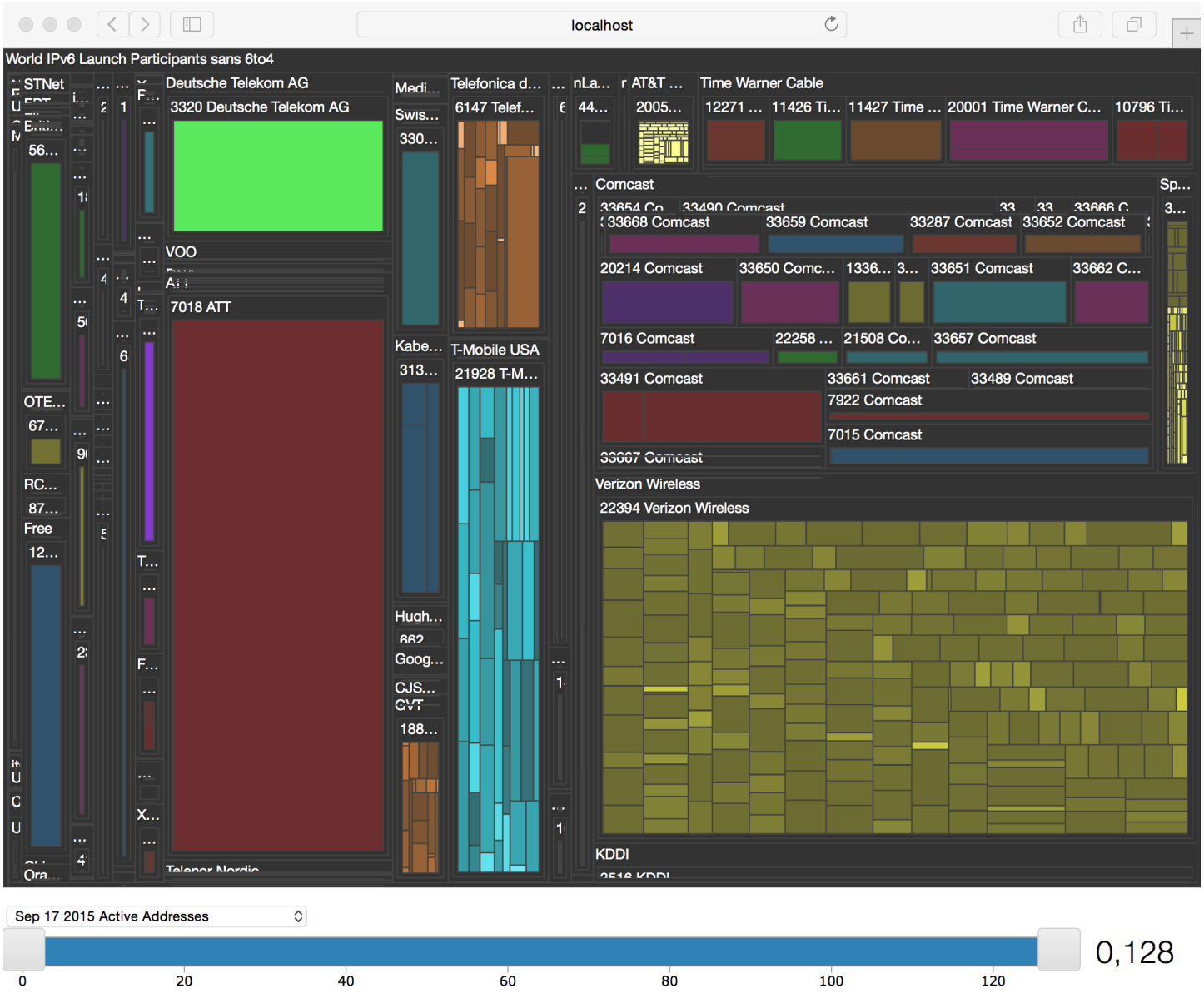


Image courtesy of John Heidemann, `https://ant.isi.edu/address/`

Visualizing the Active Internet: IPv6 by “Classified” Treemap

Demo: Exploring the active IPv6 address space



Take-aways for Me, You, and Everyone we know

- IPv6 changes **client reputation** and **geolocation.**
- IPv6 changes **threat mitigation**, *e.g.,* access control and rate limits.
- IPv6 changes **privacy, log processing**, Real User Monitoring (**RUM**), *etc.*
- IPv6 changes **target selection** for active measurements.

Take-aways for Me, You, and Everyone we know

- IPv6 is **relevant** to network analysis, flow-based and otherwise.
- IPv6 is **different** than what we're used to.
- We've made **progress** developing techniques, but there's **more to do**.

Take-aways for Me, You, and Everyone we know

- IPv6 is **relevant** to network analysis, flow-based and otherwise.
- IPv6 is **different** than what we're used to.
- We've made **progress** developing techniques, but there's **more to do**.

WE WANT YOU TO *UNDERSTAND* IPv6

“**Temporal and Spatial Classification of Active IPv6 Addresses**” (IMC 2015)
also: Sample IPv6 Active WWW Client Address Aggregate Counts Data

`http://www.akamai.com/technical-publications/`

Thanks!
Questions? Comments?

David Plonka <plonka@akamai.com>