Advancing the Art of Internet Edge Outage Detection

ACM Internet Measurement Conference 2018

Philipp Richter
MIT / Akamai

Ramakrishna Padmanabhan
University of Maryland

Neil Spring
University of Maryland

Arthur Berger
Akamai / MIT

David Clark
MIT

Internet Edge Outages

Lightning Strike Sparks Fire At AT&T Facility, Outage Impacts Internet Service

...restore service after an electrical fire at one of its facilities impacted internet service for customers.

TECHNOLOGY NEWS NOVEMBER 28, 2016 / 6:45 AM / 2 YEARS AGO

German internet outage was failed botnet attempt: report

Eric Auchard

HURRICANE MICHAEL'S IMPACT —

Verizon fiber suffered "unprecedented" damage from Hurricane Michael

...ge to Verizon fiber delays restoration of...

...2018, 12:40 PM

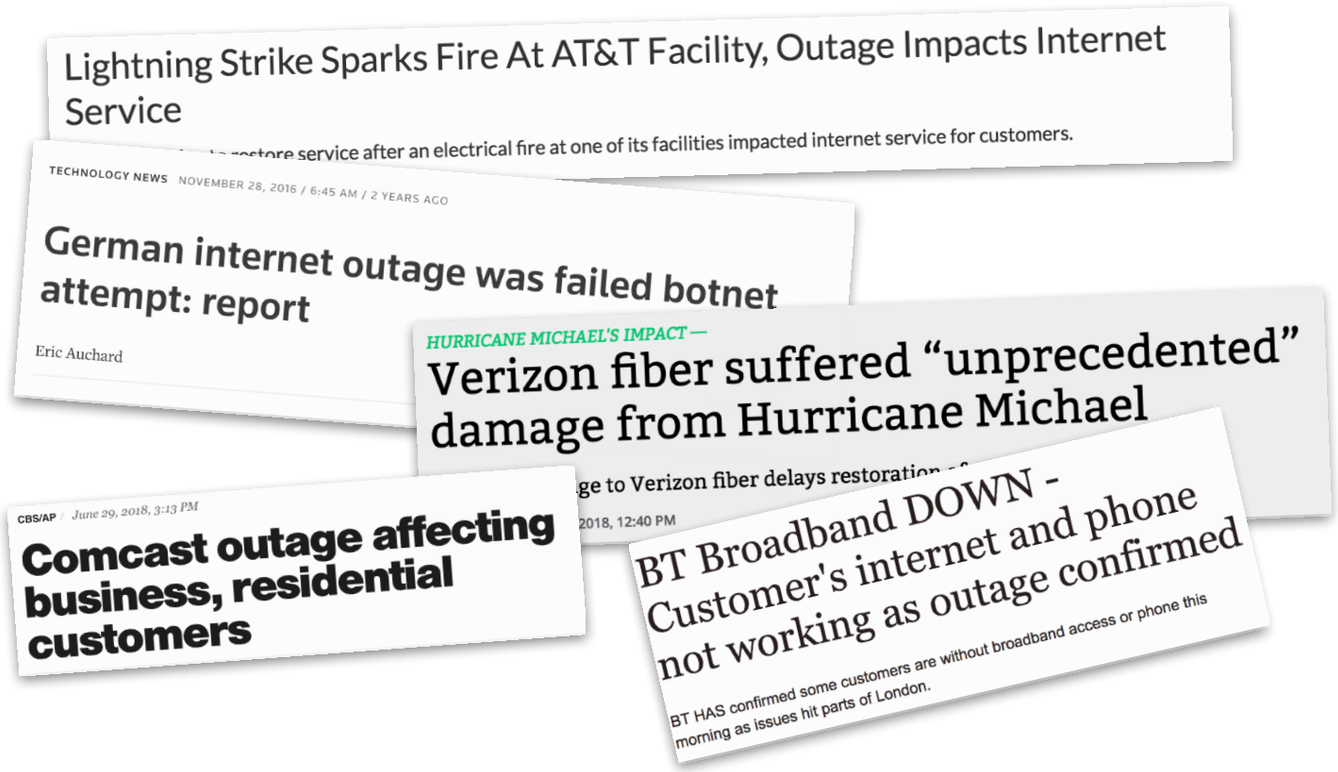
CBS/AP / June 29, 2018, 3:13 PM

Comcast outage affecting business, residential customers

BT Broadband DOWN - Customer's internet and phone not working as outage confirmed

BT HAS confirmed some customers are without broadband access or phone this morning as issues hit parts of London.

Internet Edge Outages

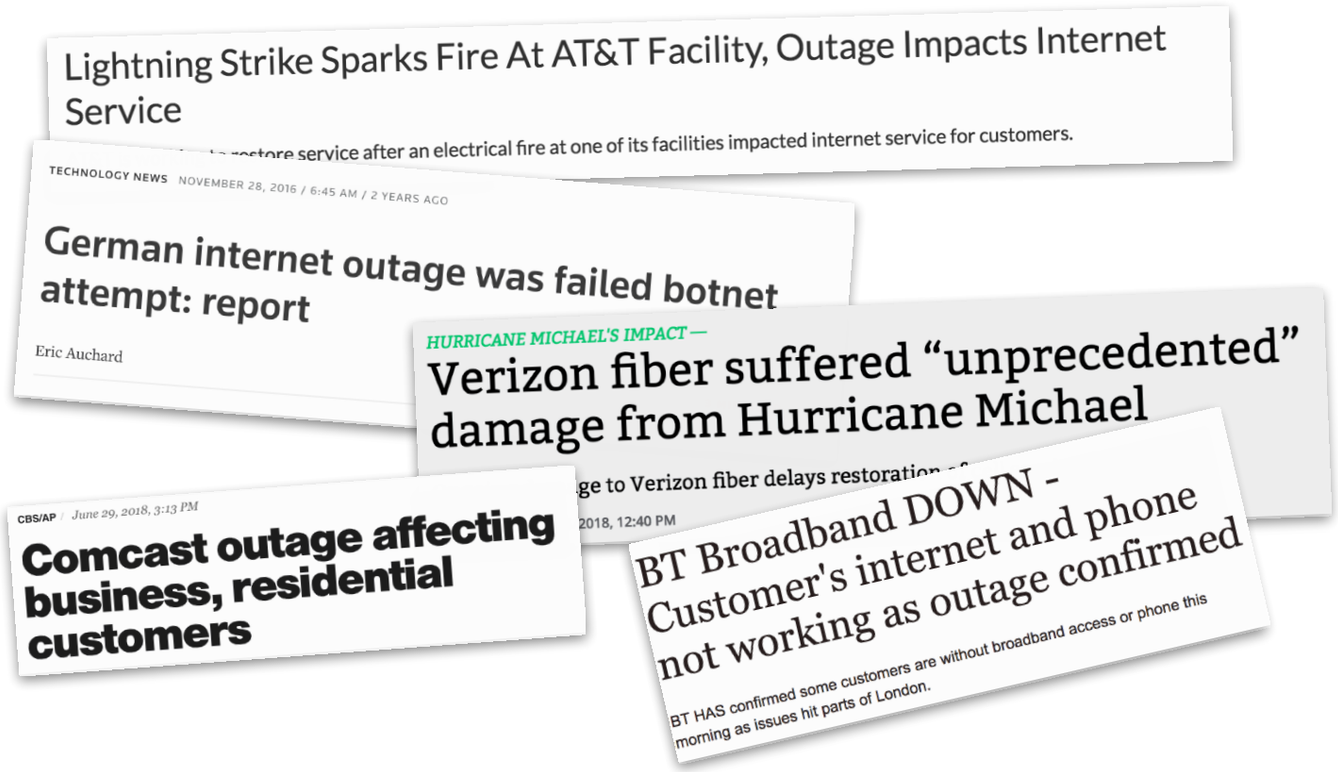


➡ **Uninterrupted Internet availability becomes increasingly critical**

➡ Growing interest in systems to detect Internet edge outages

➡ Regulatory Bodies, Governments, ISPs, Academic Research

Internet Edge Outages



➡ **Uninterrupted Internet availability becomes increasingly critical**

➡ Growing interest in systems to detect Internet edge outages

➡ Regulatory Bodies, Governments, ISPs, Academic Research

Goal: Track Internet edge outages on *(i)* a broad scale and *(ii)* a detailed level

Edge Outage Detection: Existing Approaches

- **Detecting outages in the control plane?**
  ➡ Edge outages often invisible in BGP

- **Deploying hardware in end user premises?**
  ➡ Potentially highly accurate, but does not scale

- **Actively probing addresses?**
  ➡ Challenging to scale, unresponsive addresses, difficult to interpret

Edge Outage Detection: Existing Approaches

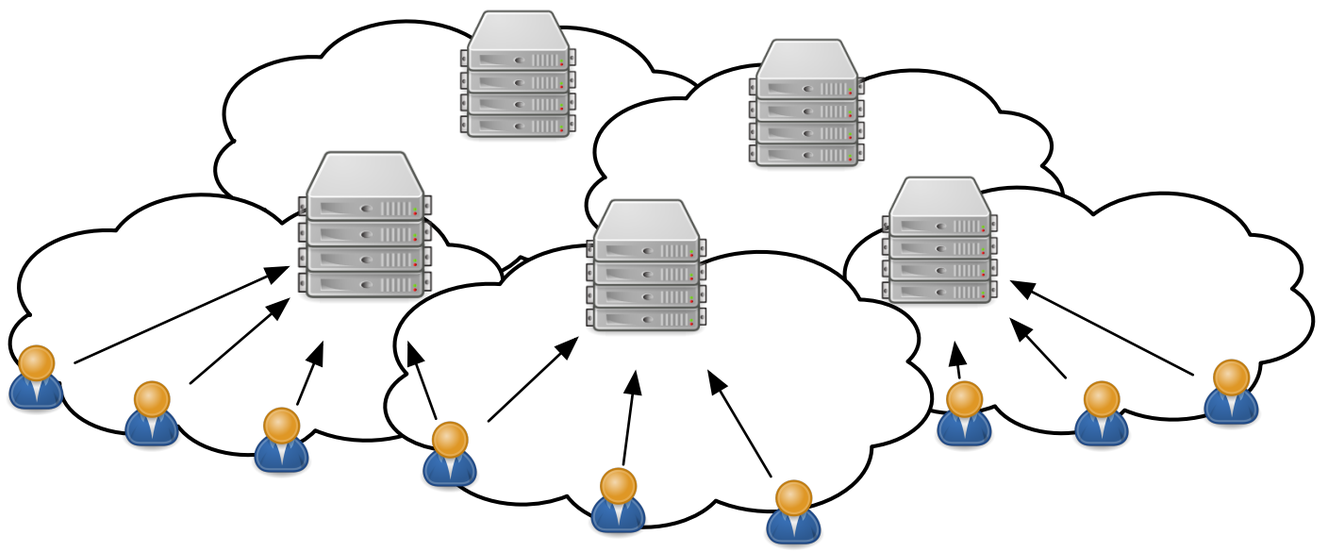
- **Detecting outages in the control plane?**
  - ➡ Edge outages often invisible in BGP
- **Deploying hardware in end user premises?**
  - ➡ Potentially highly accurate, but does not scale
- **Actively probing addresses?**
  - ➡ Challenging to scale, unresponsive addresses, difficult to interpret

This work:
Passive edge outage detection based on CDN request patterns

Outline

- **Disruption Detection**
- Global View on Disruptions
- Device-Centric View on Disruptions
- U.S. Broadband Case Study

Disruption Detection using CDN Access Logs



200,000+ servers

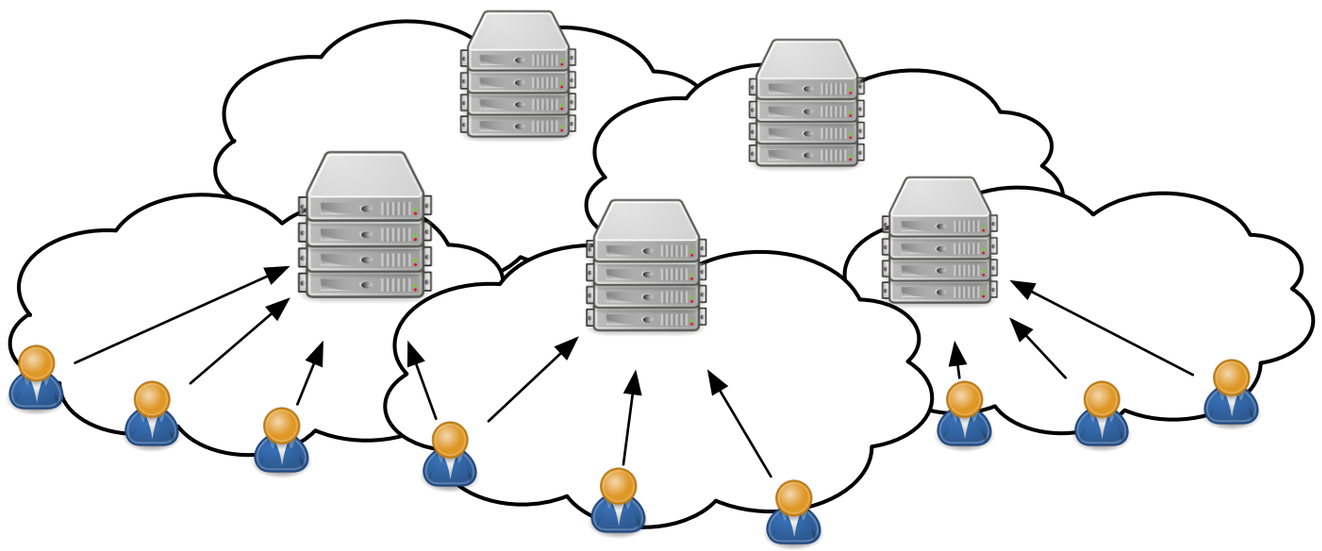
1500+ ASes

120+ countries

> 3 trillion daily requests

Dataset: Hourly request counts per IPv4 /24 address block

Disruption Detection using CDN Access Logs



200,000+ servers

1500+ ASes

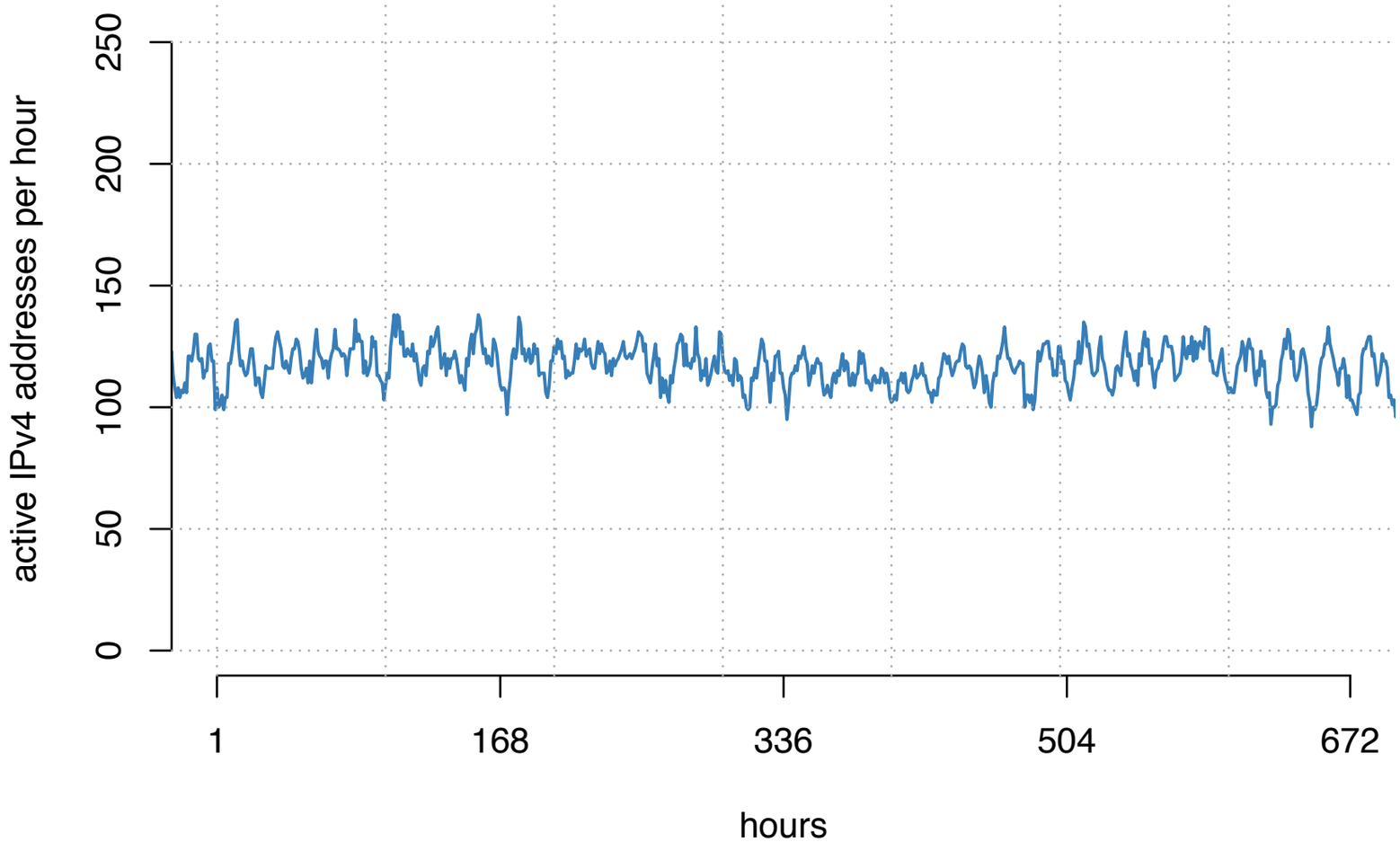
120+ countries

> 3 trillion daily requests

Dataset: Hourly request counts per IPv4 /24 address block

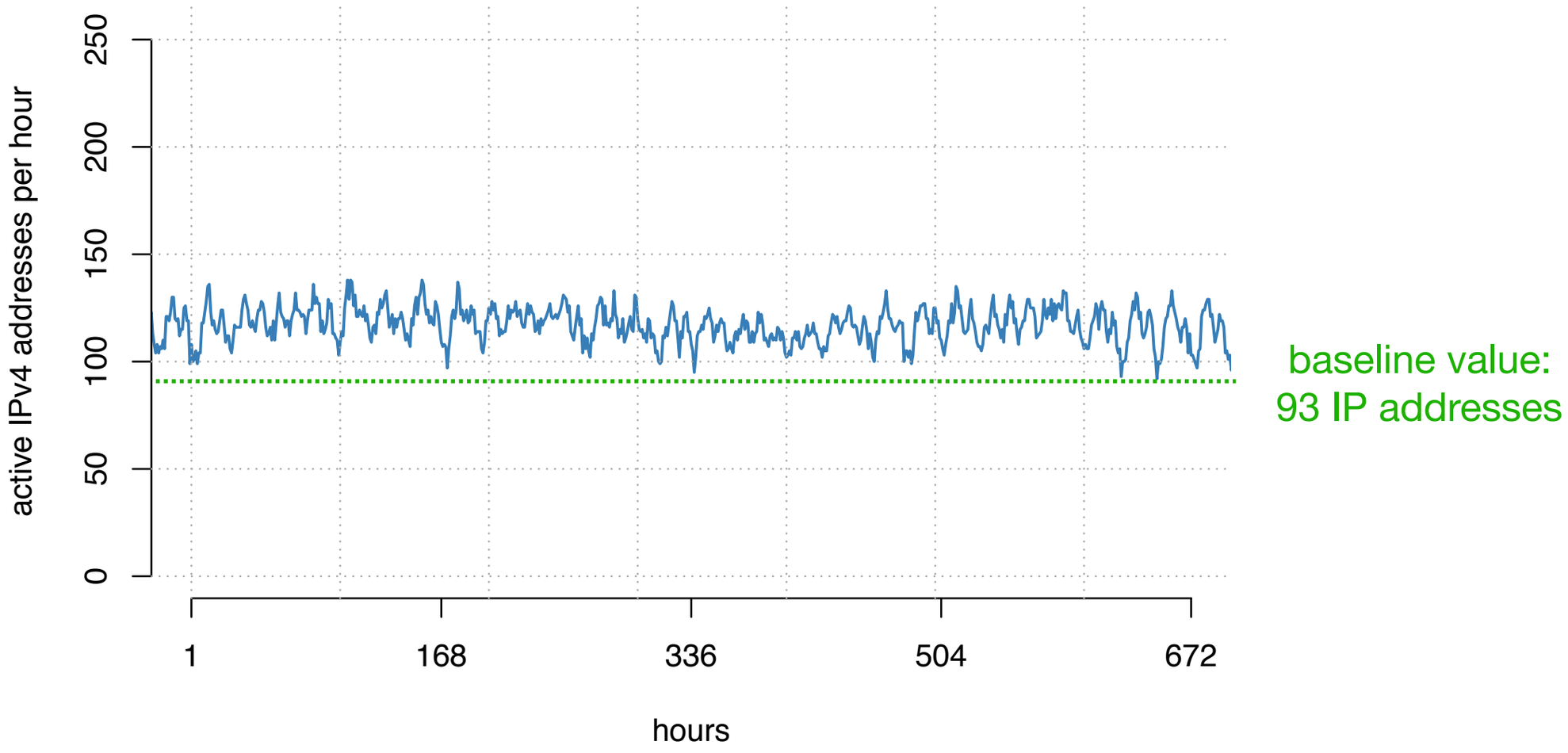
Assumption:
Edge outages will be reflected in absence/reduction of CDN requests.

Active IP Addresses per /24



typical residential /24 address block

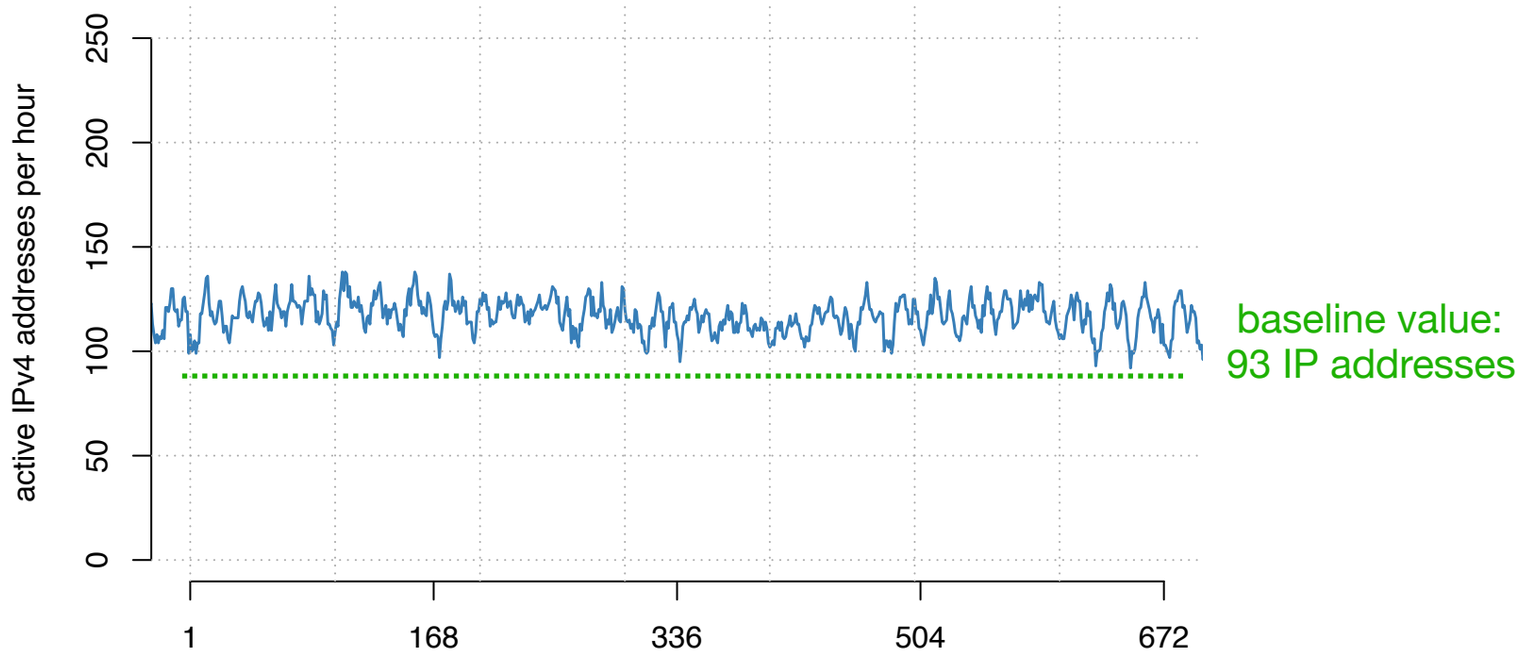
Active IP Addresses per /24: Baseline Activity



typical residential /24 address block

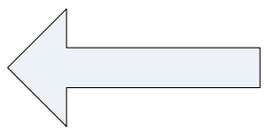
Number of addresses contacting the CDN every hour never drops below ‘baseline value’ value per block.

Active IP Addresses per /24: Baseline Activity



typical residential /24 address block

CDN

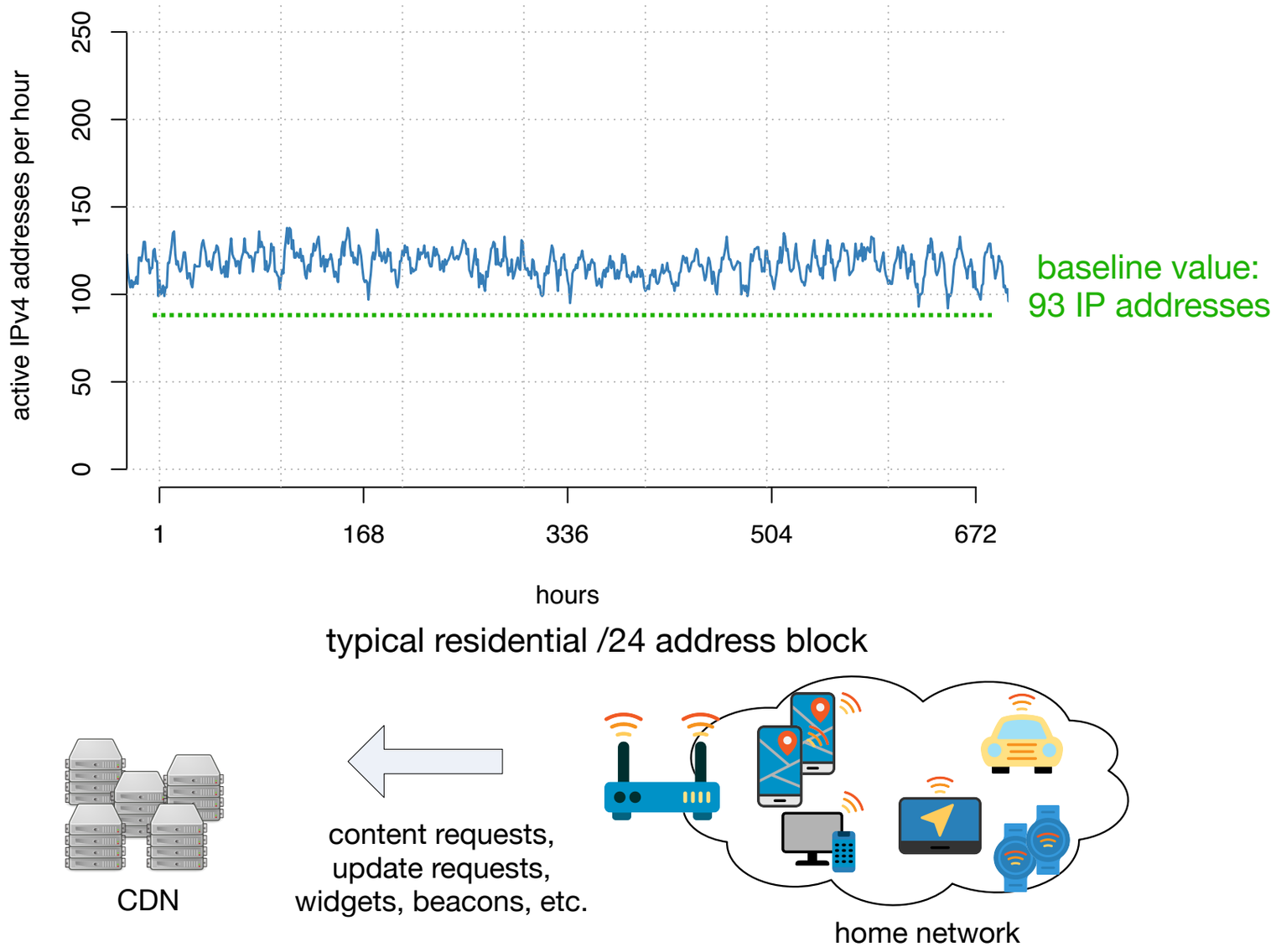


content requests,
update requests,
widgets, beacons, etc.

home network

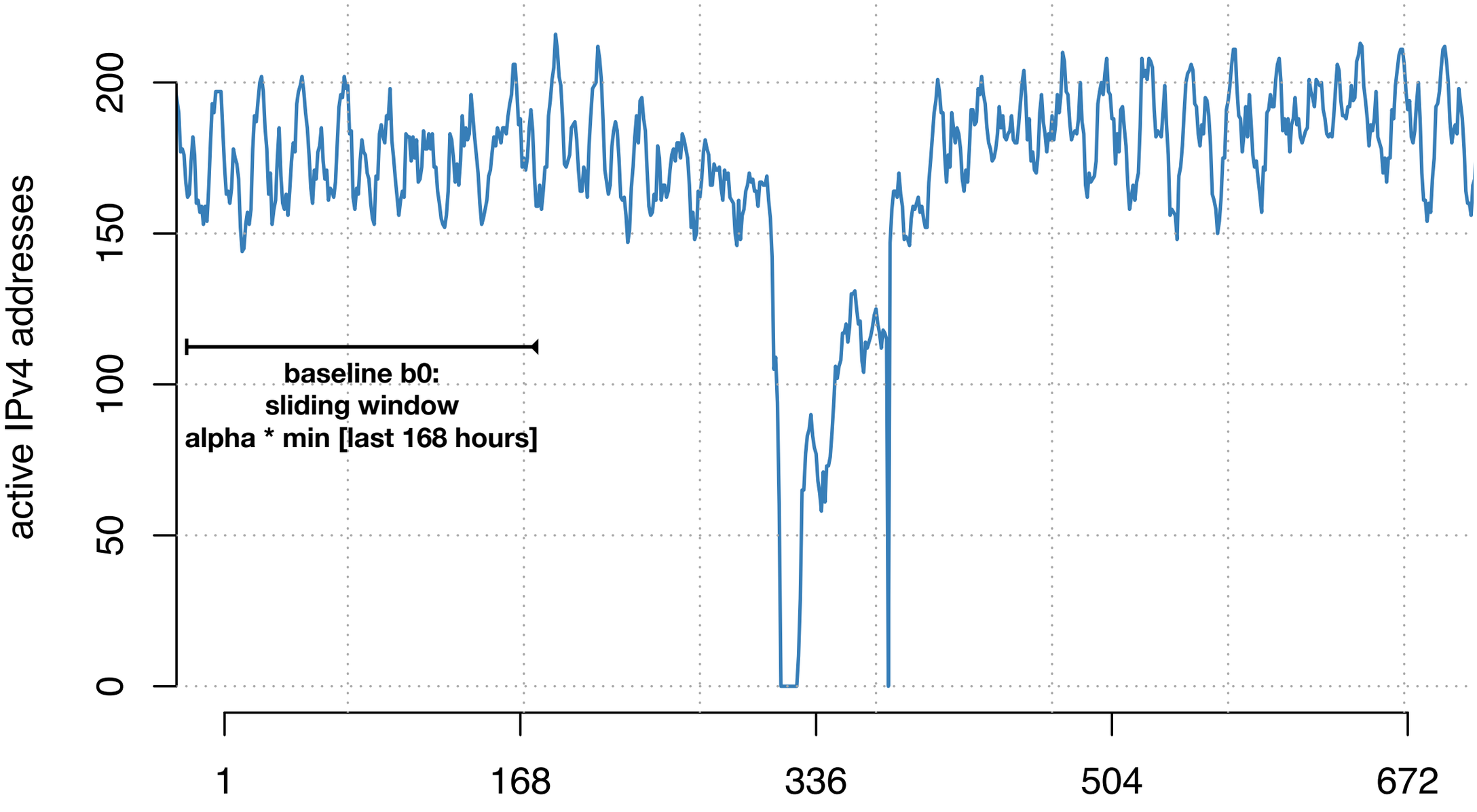
icons: mavadee / flaticon

Active IP Addresses per /24: Baseline Activity

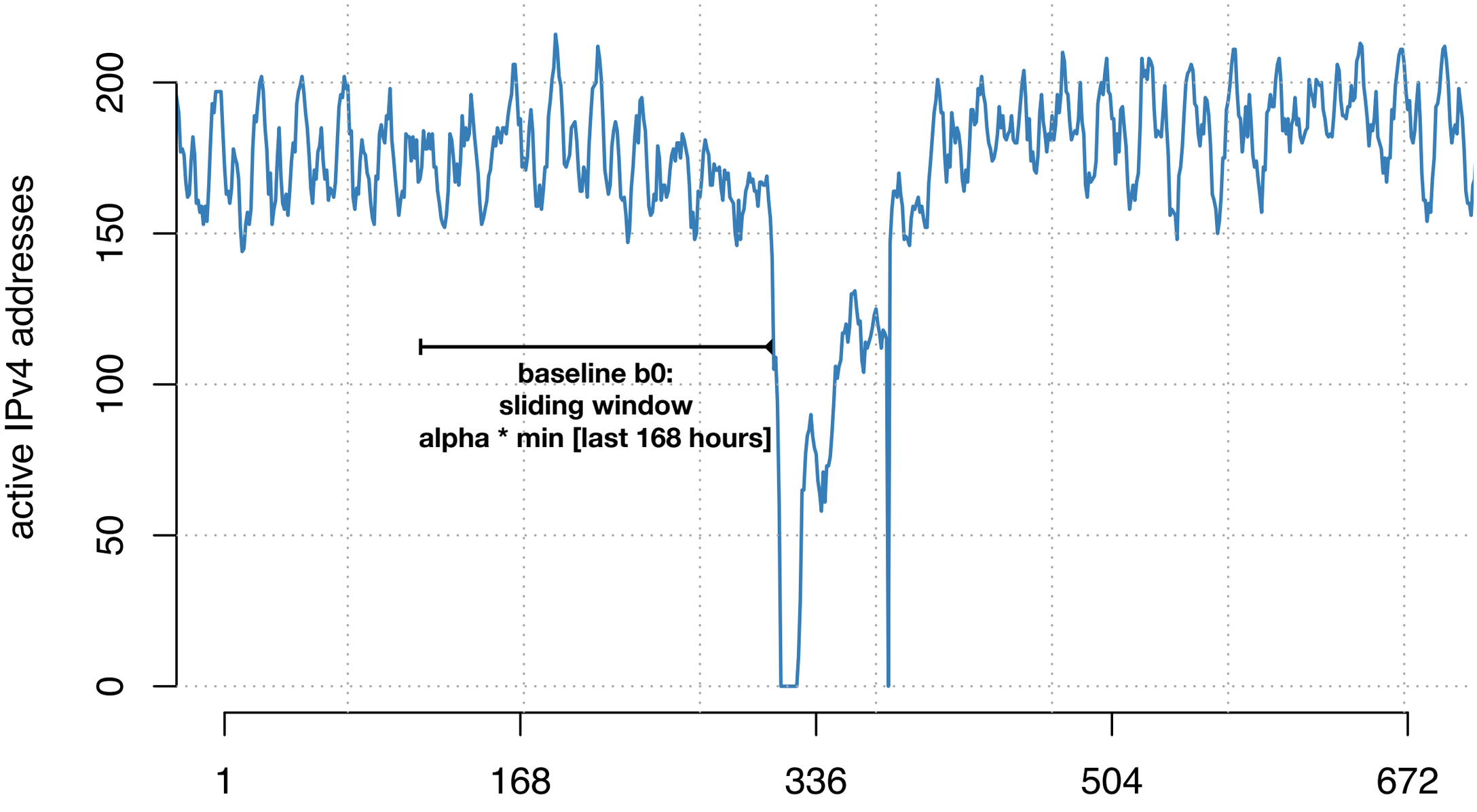


- Some 2.3M /24 address blocks (83% of all client IPs) baseline > 40
- Robust signal, largely independent of user-triggered activity
- Dependent on a functioning network

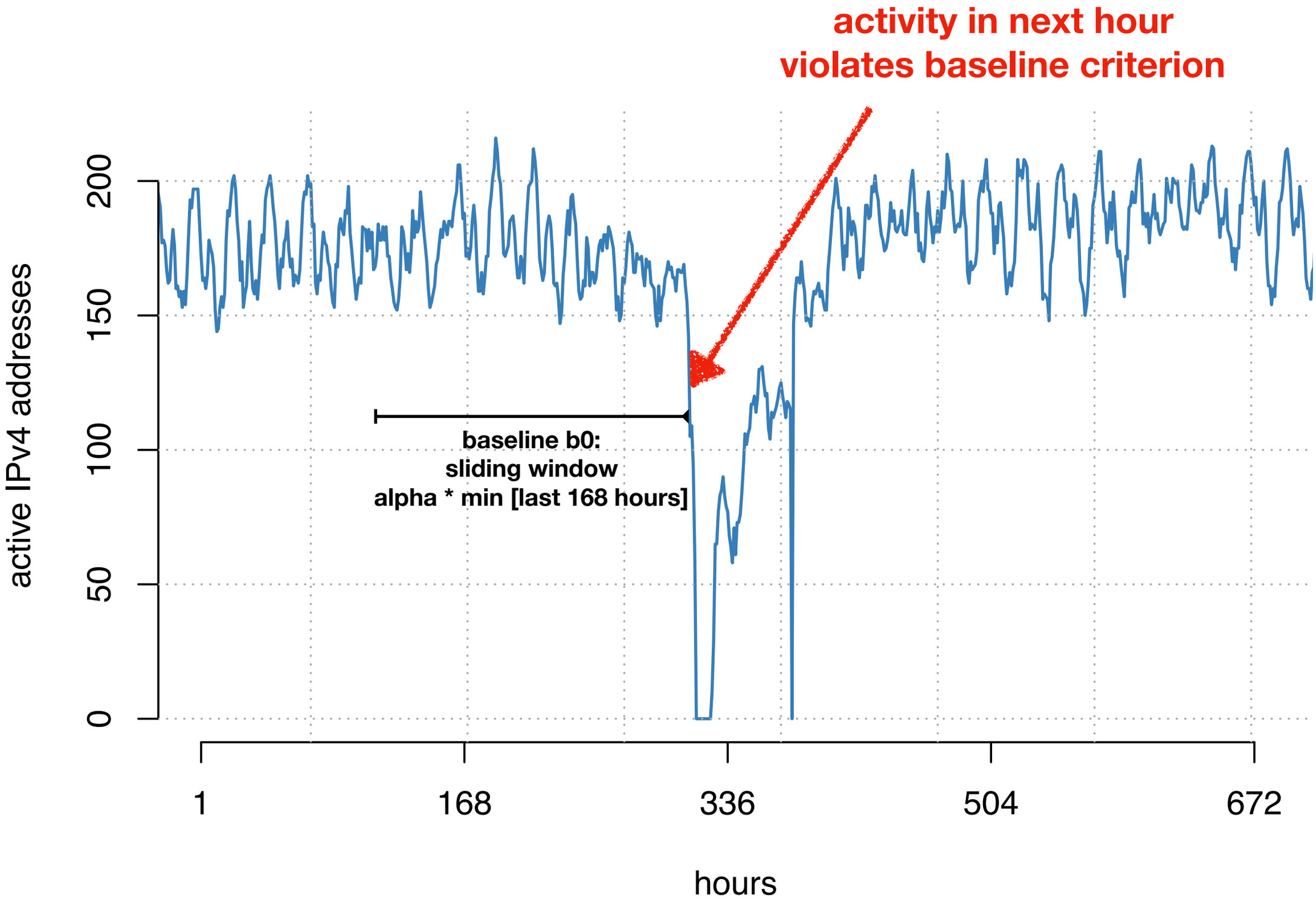
Disruption Detection



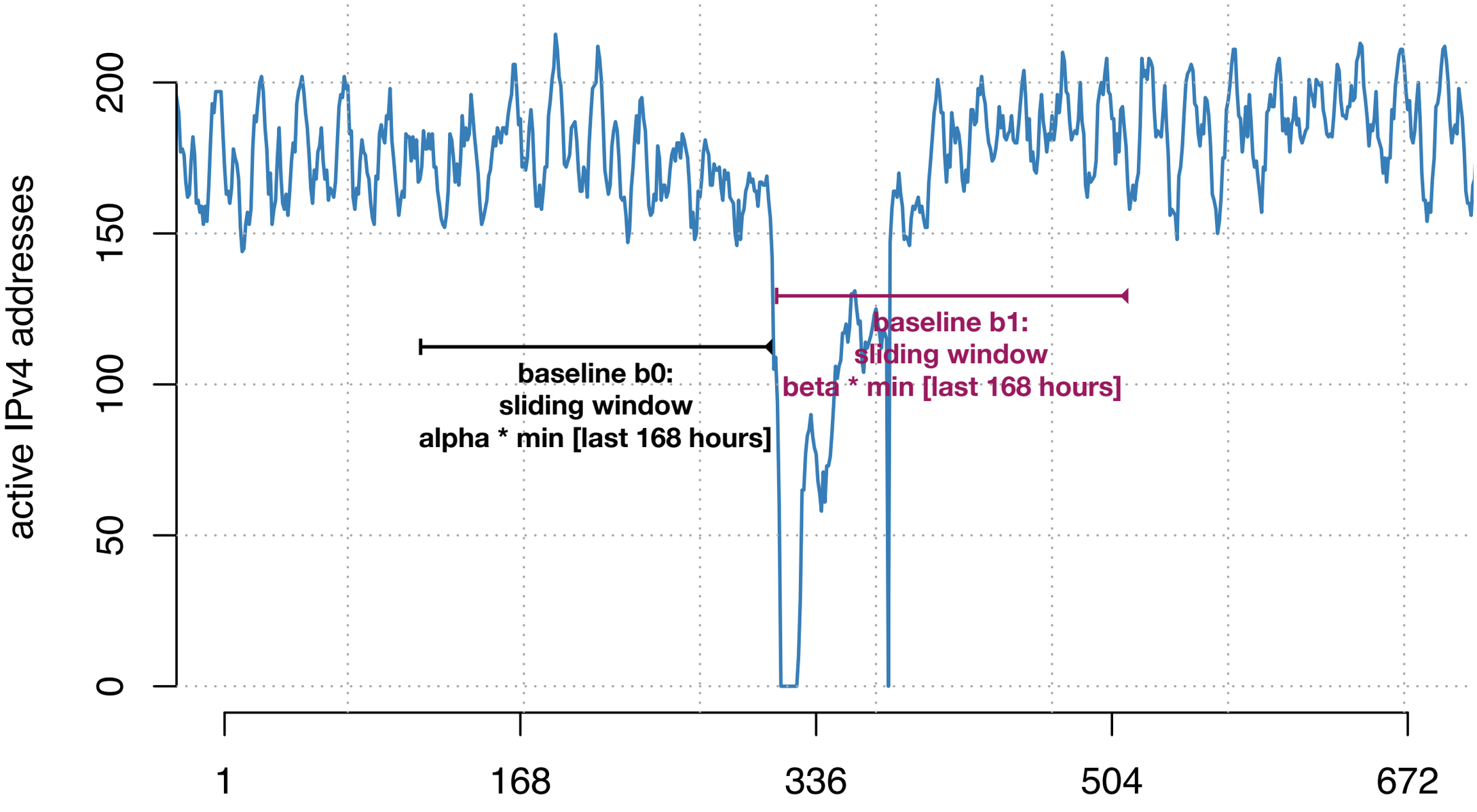
Disruption Detection



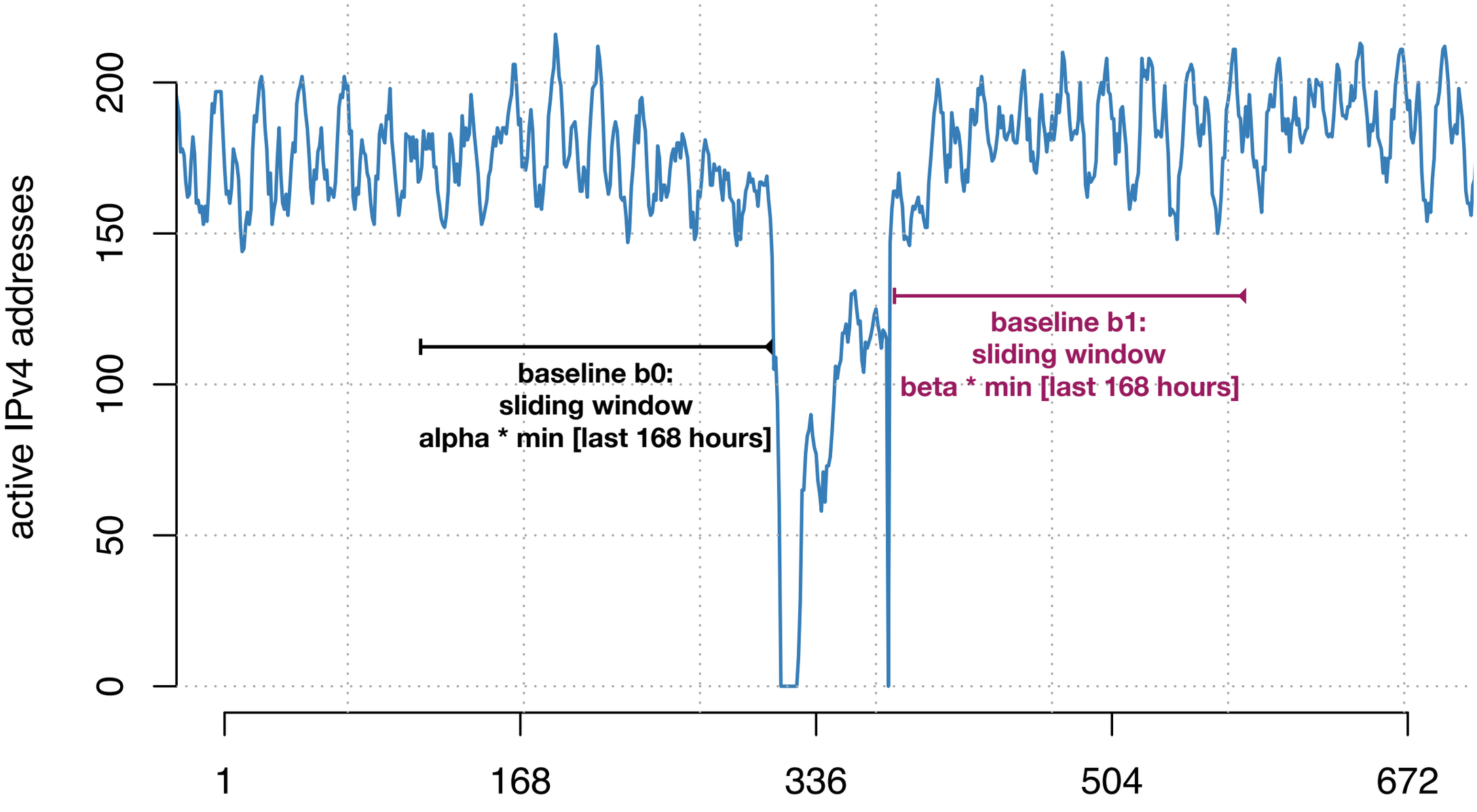
Disruption Detection



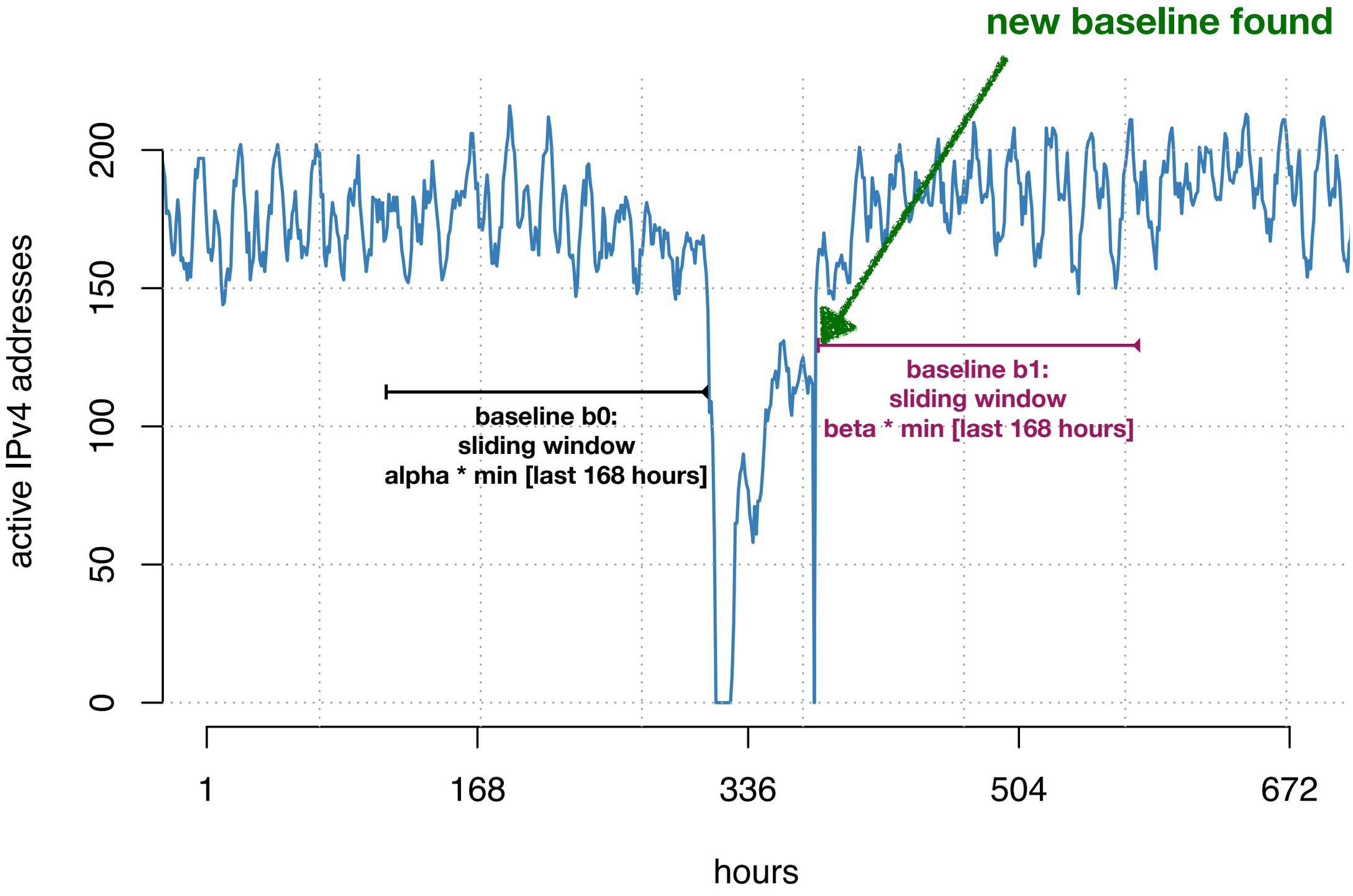
Disruption Detection



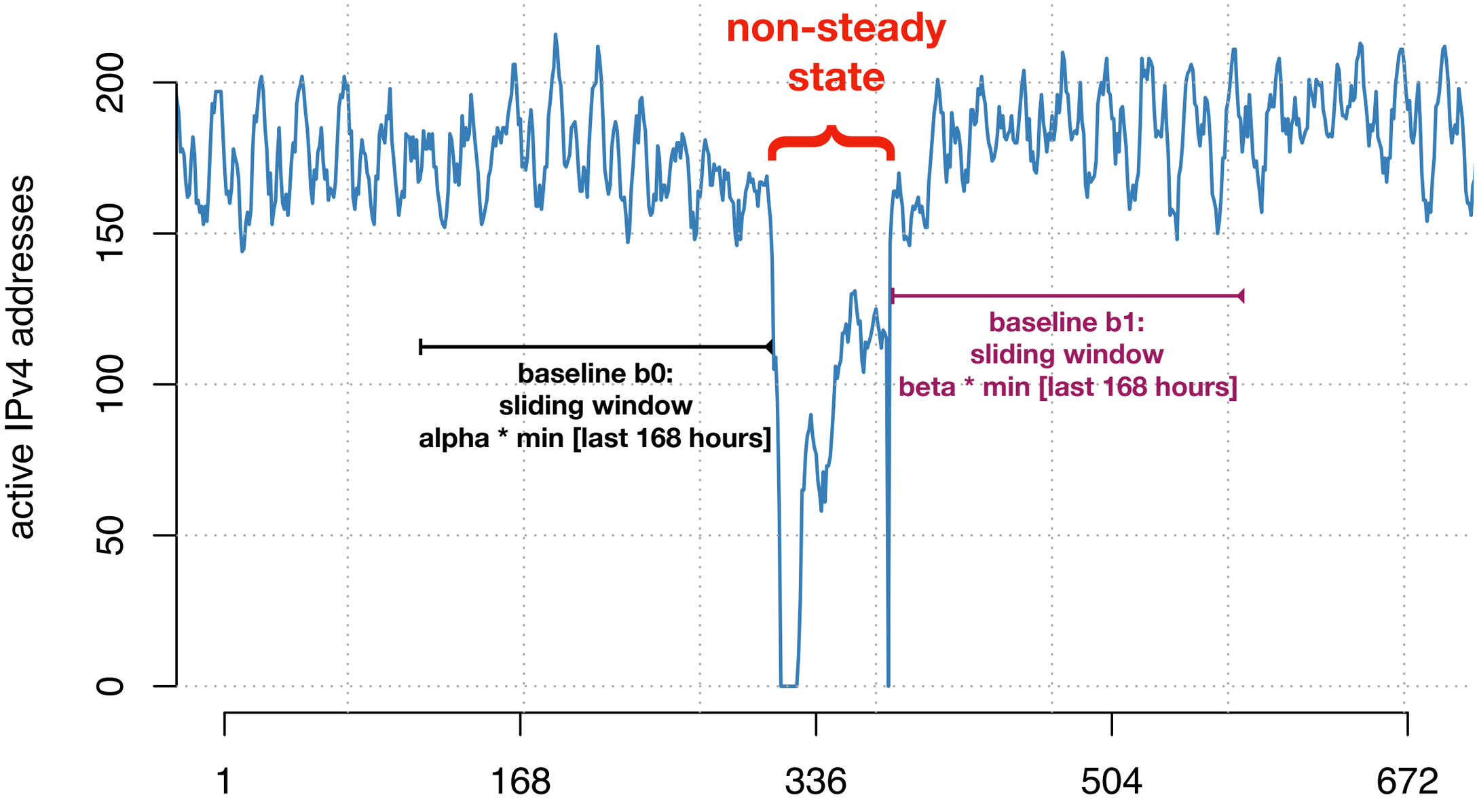
Disruption Detection



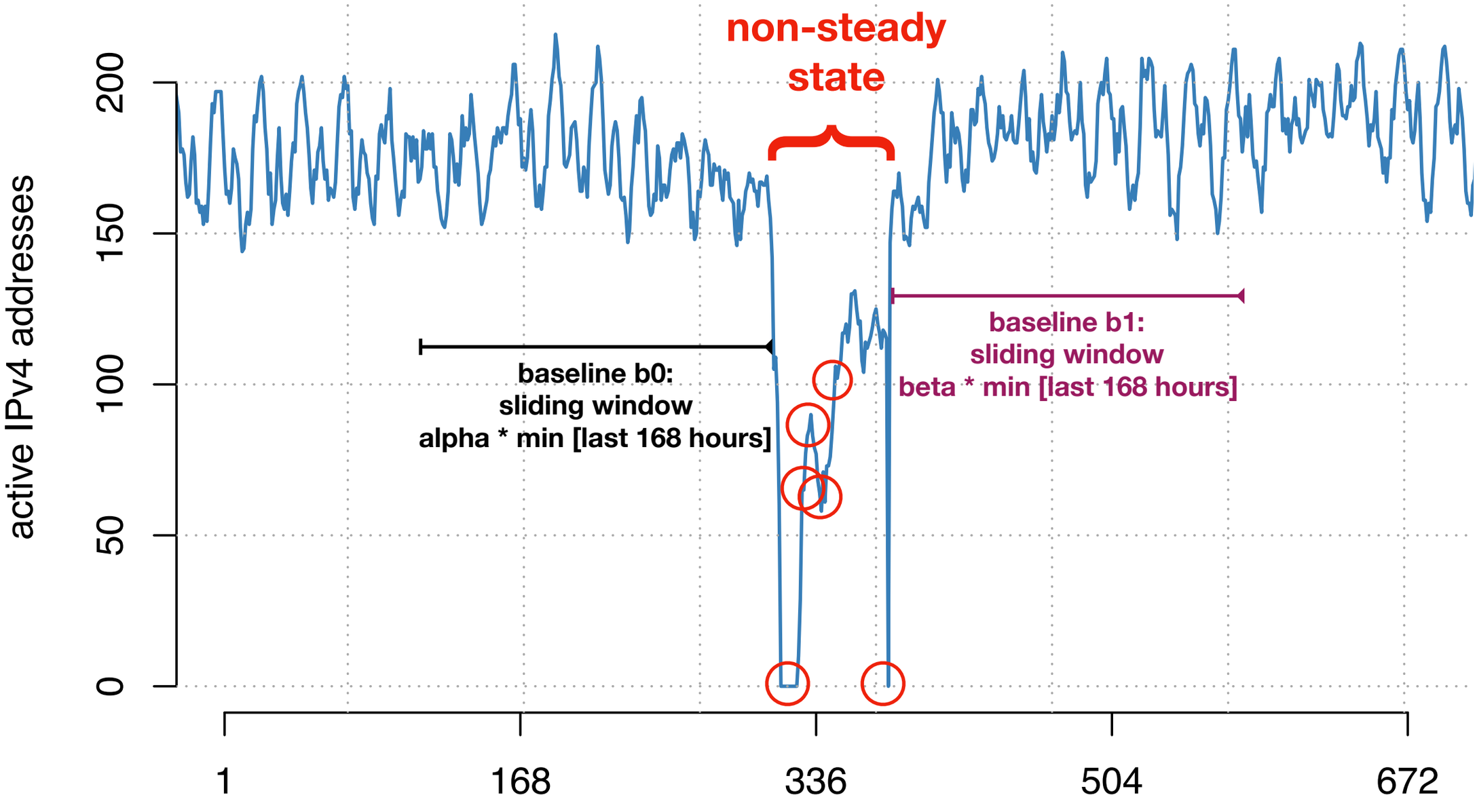
Disruption Detection



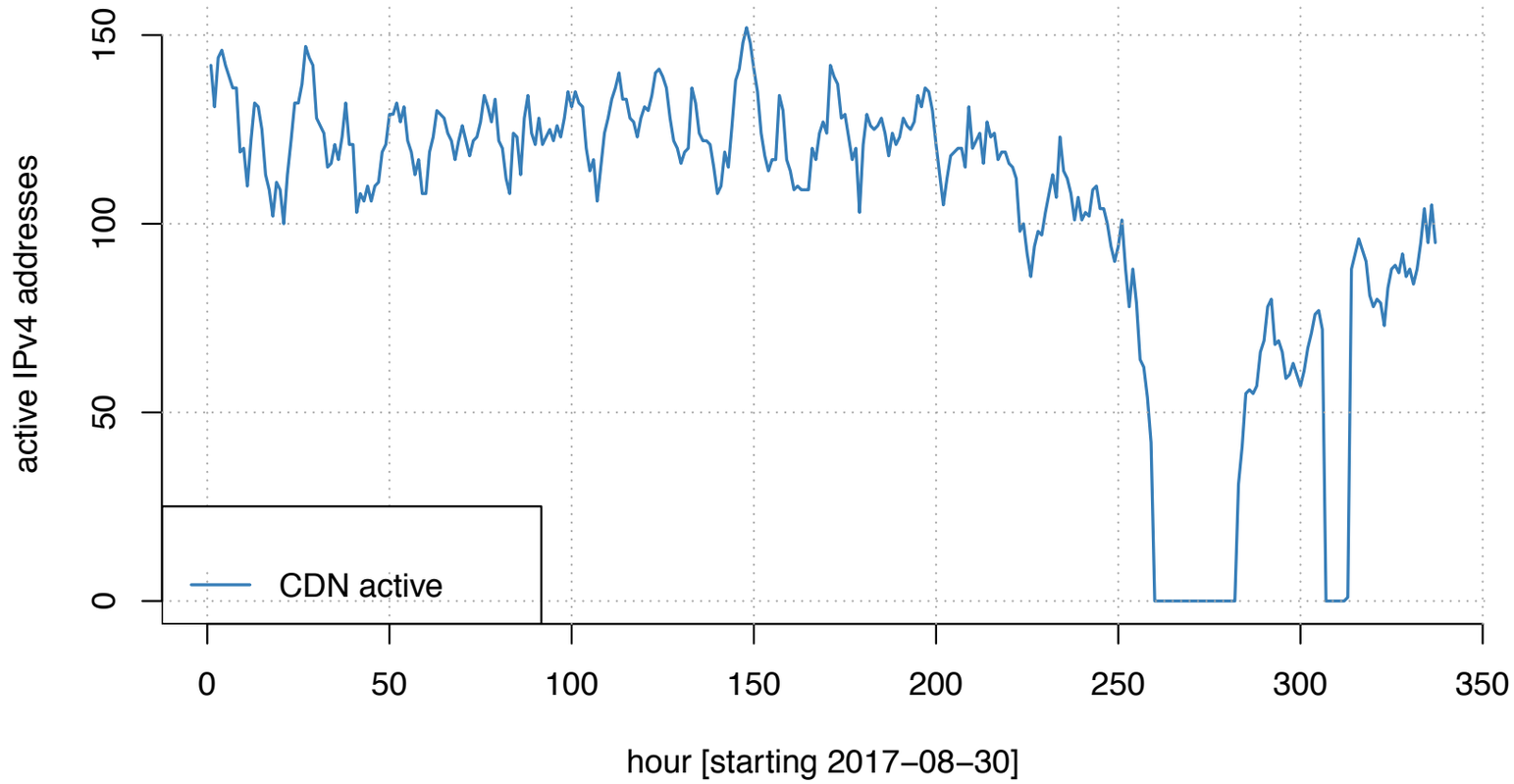
Disruption Detection



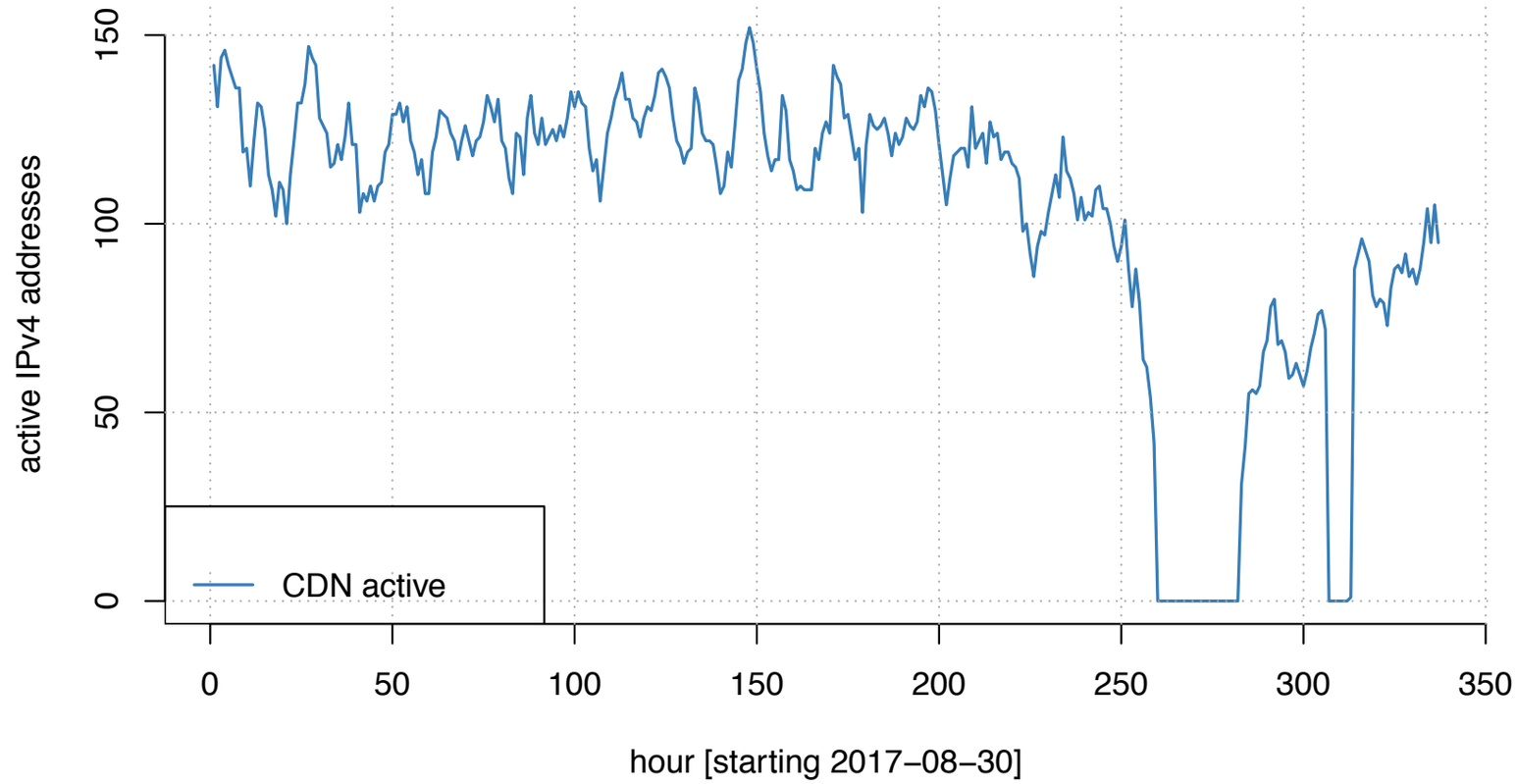
Disruption Detection



Did this Address Block really go offline?



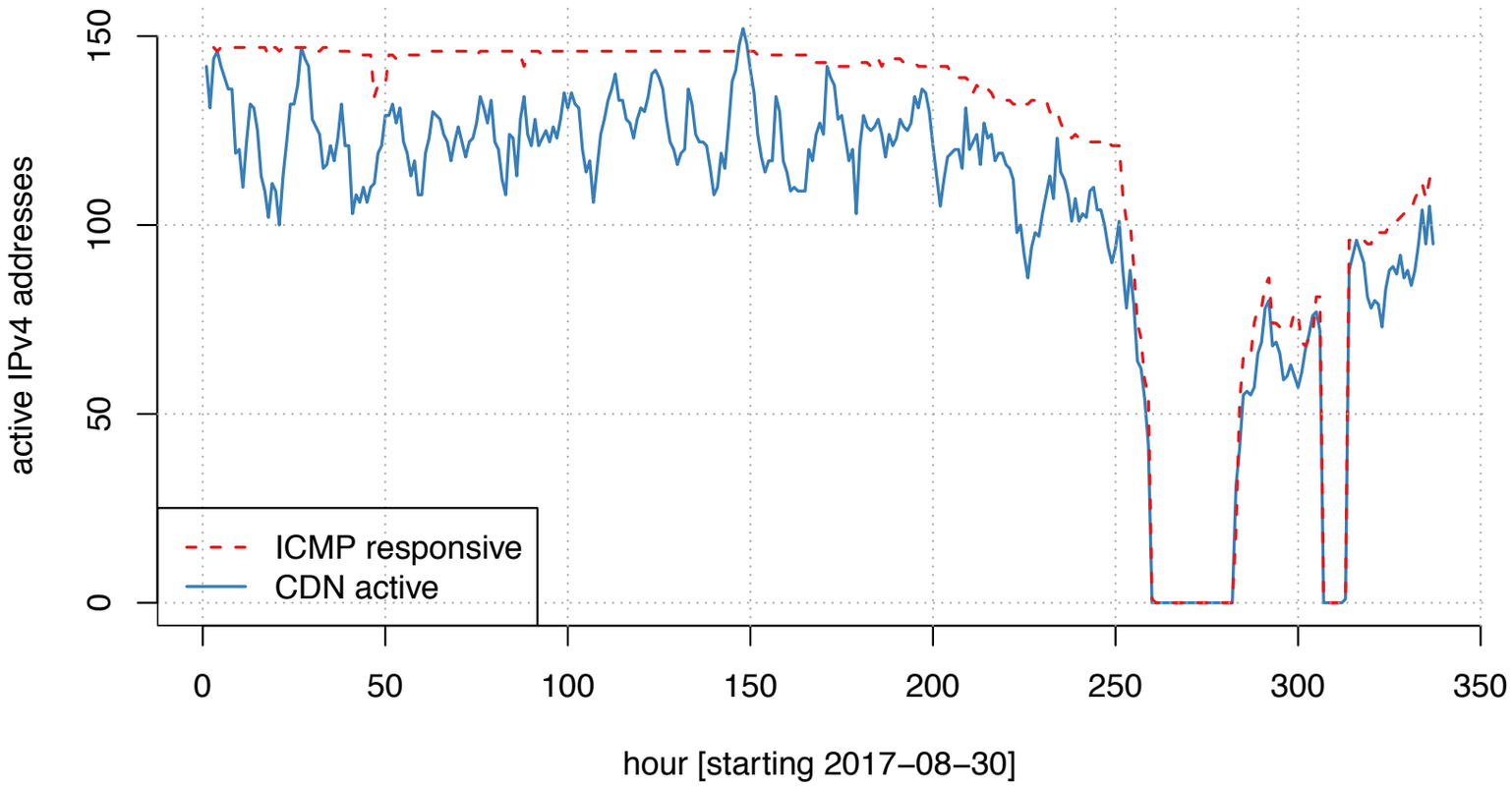
Did this Address Block really go offline?



➡ **“Address Space Survey Data” (provided by ISI)**

- ➡ Ping *every* address in 1% of the allocated IPv4 /24s every 11 mins
- ➡ Some address blocks show a very steady number of responsive IPs

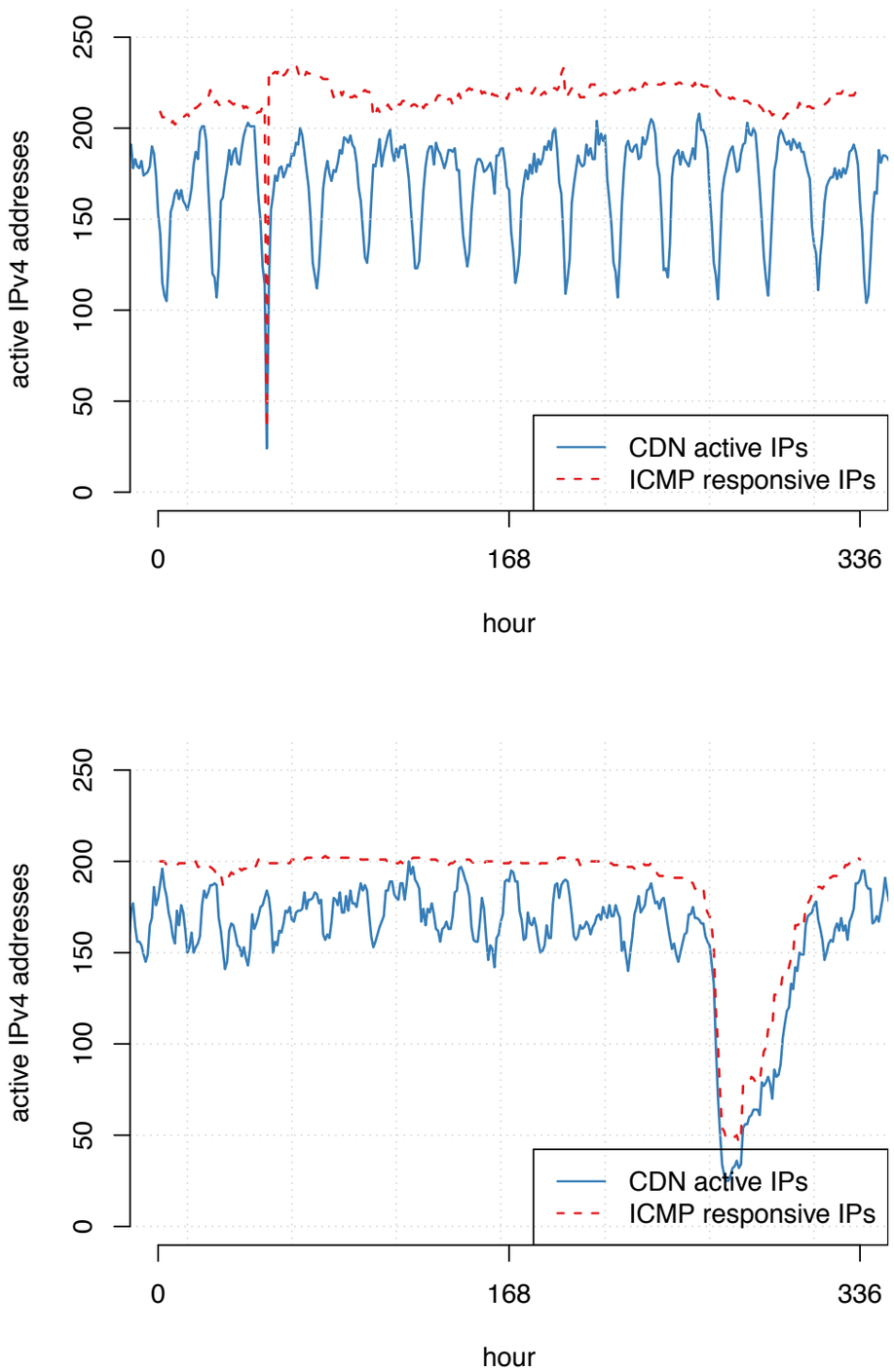
Did this Address Block really go offline?

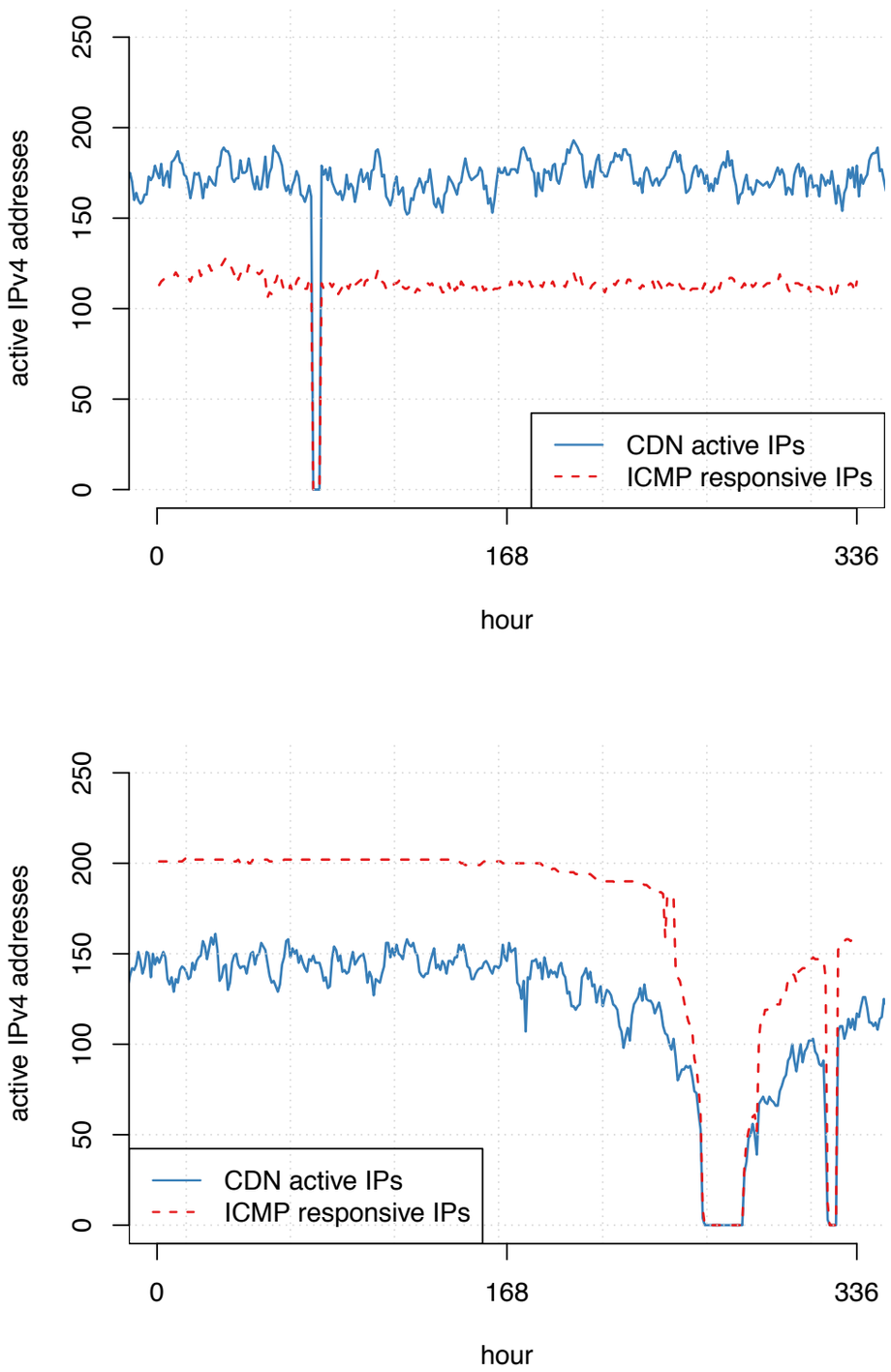


➡ **“Address Space Survey Data” (provided by ISI)**

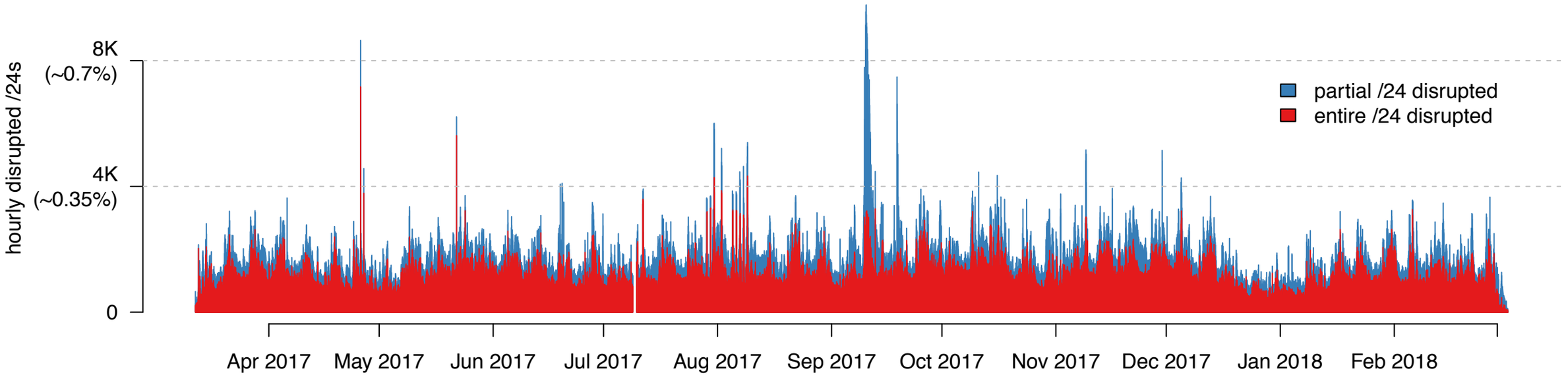
- ➡ Ping *every* address in 1% of the allocated IPv4 /24s every 11 mins
- ➡ Some address blocks show a very steady number of responsive IPs

CDN Disruptions vs. ICMP



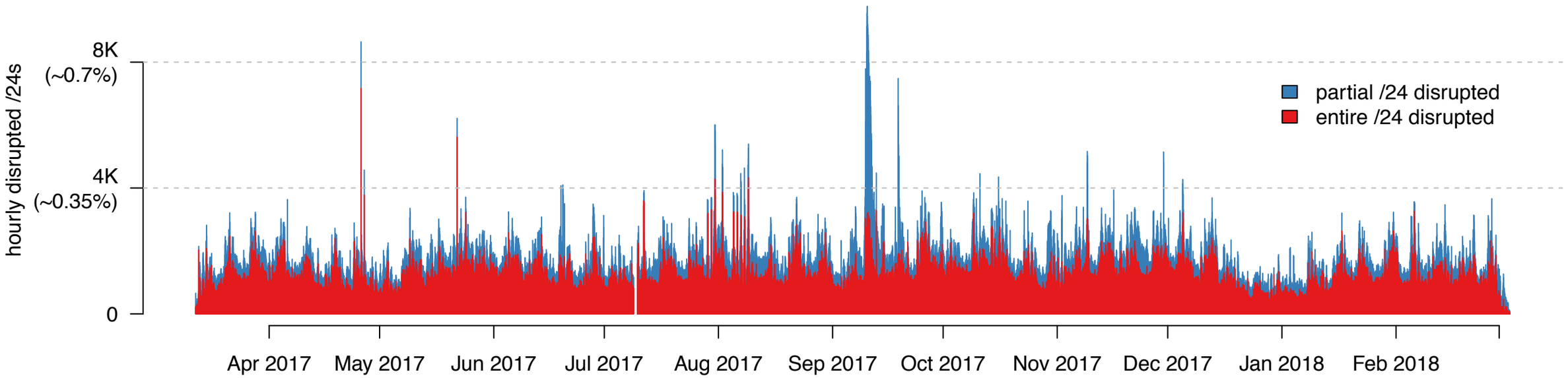


Global View on Disruptions



1.5M disruption events over the course of one year

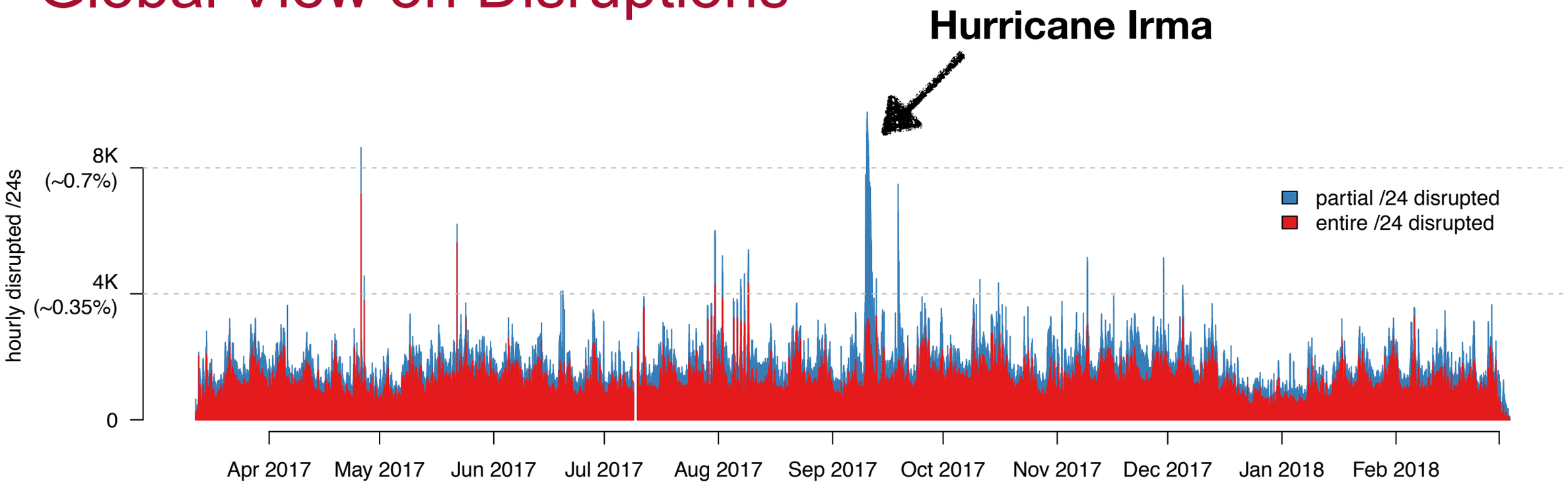
Global View on Disruptions



1.5M disruption events over the course of one year

- At least 0.2% of the monitored space faces a disruption
- Natural disasters, intended Internet shutdowns
- Weekly pattern, mostly absent during Christmas/NYE

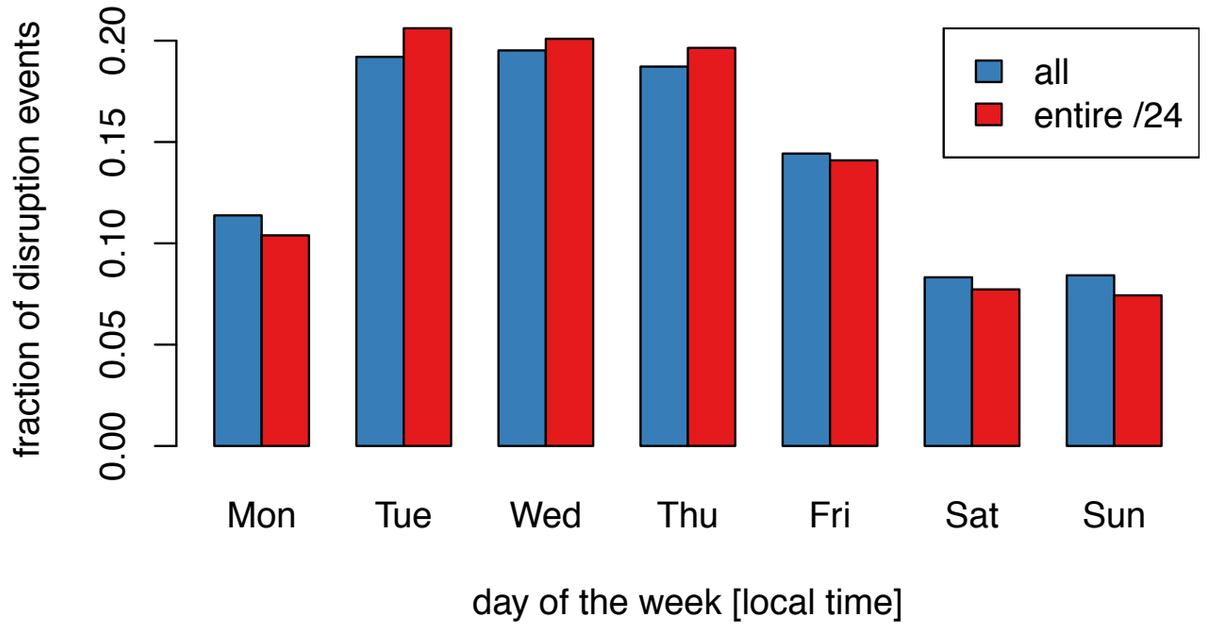
Global View on Disruptions



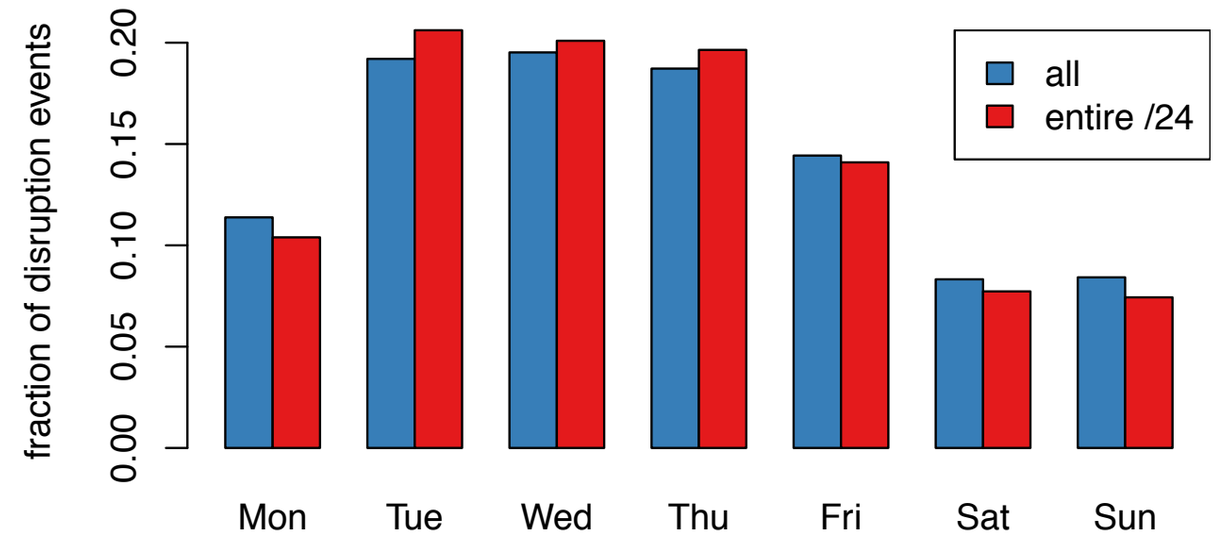
1.5M disruption events over the course of one year

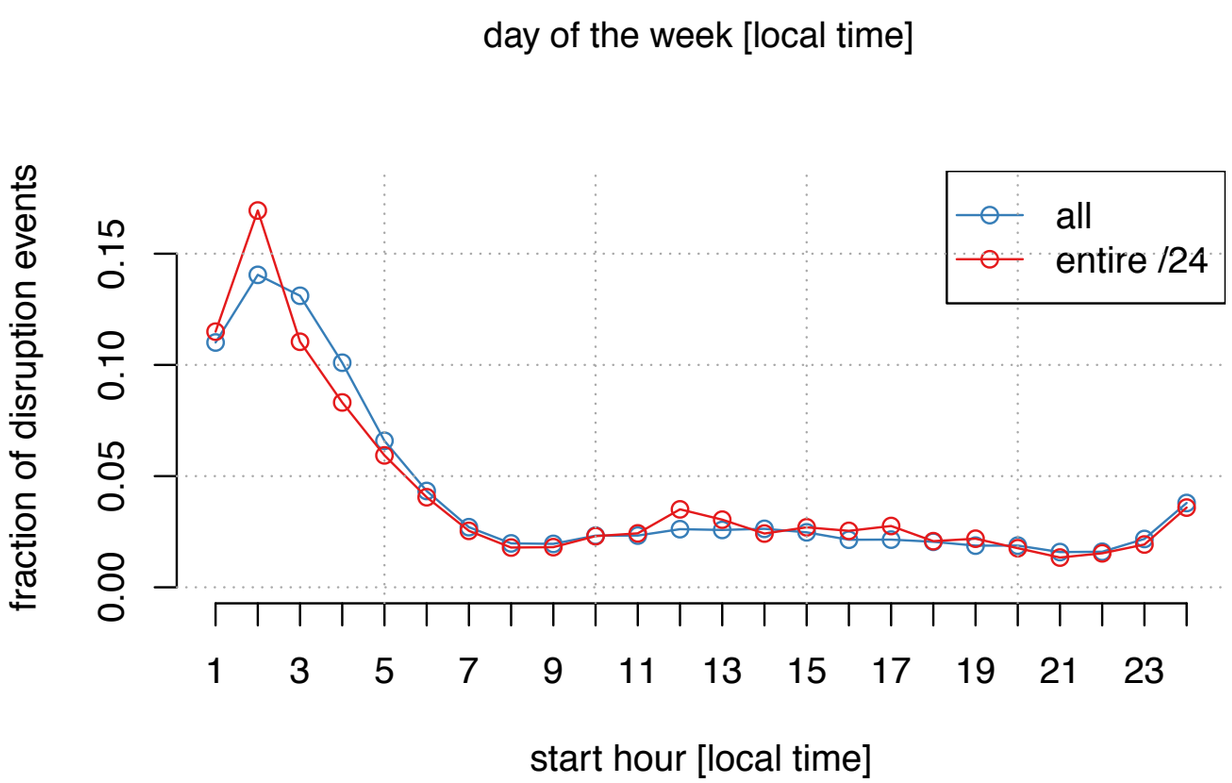
- At least 0.2% of the monitored space faces a disruption
- Natural disasters, intended Internet shutdowns
- Weekly pattern, mostly absent during Christmas/NYE

Weekly Pattern

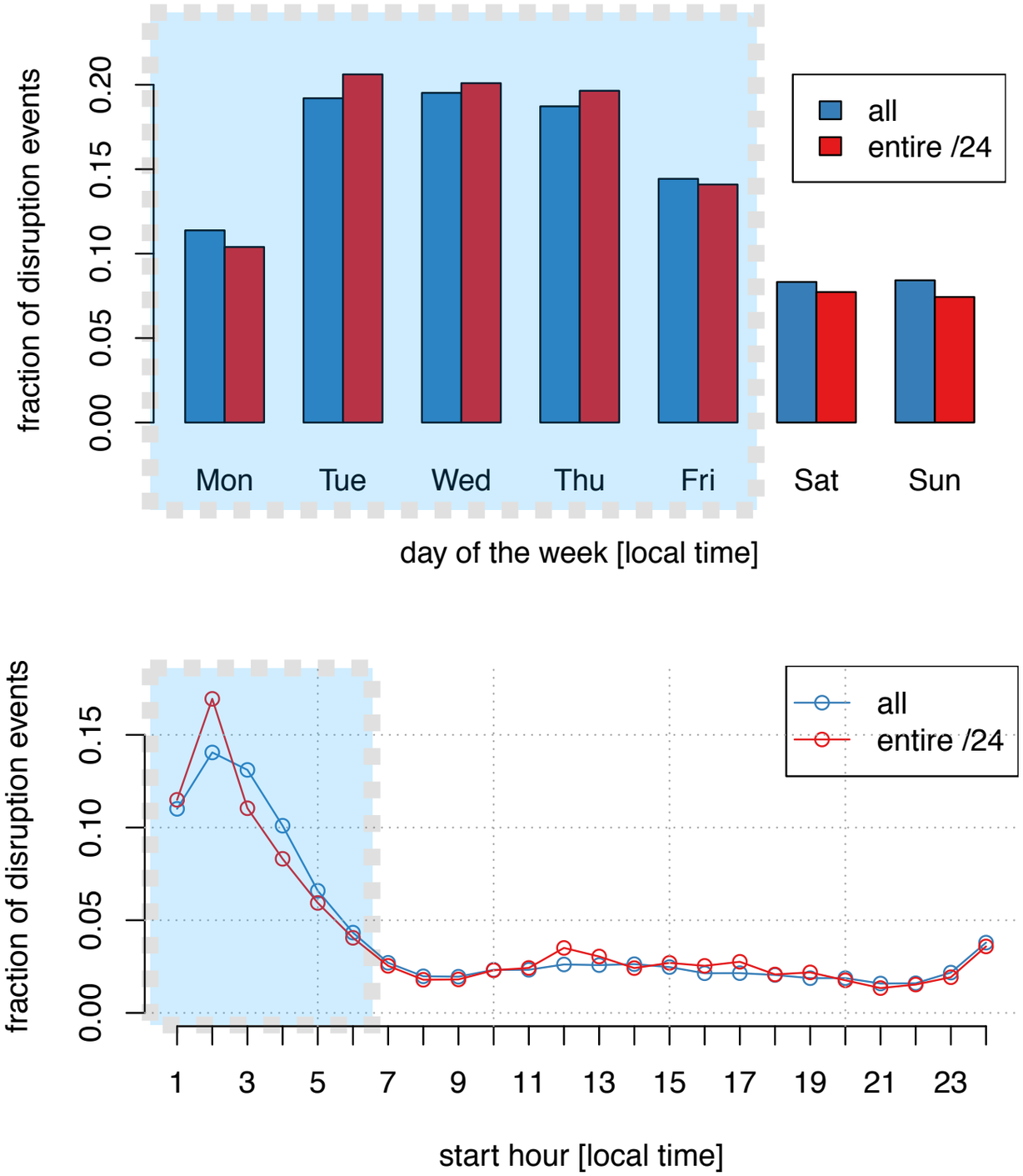


Weekly Pattern





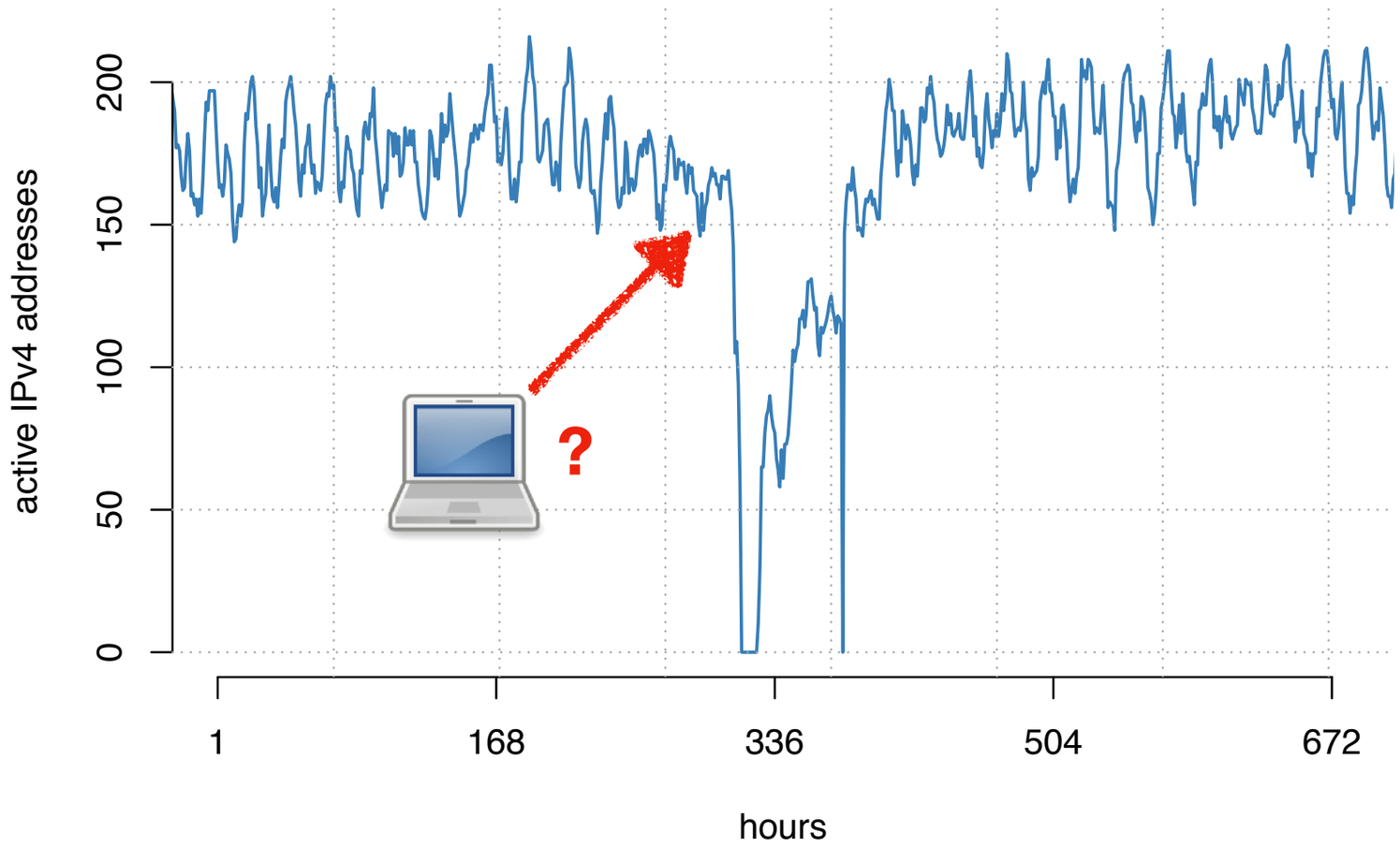
Weekly Pattern: Scheduled Maintenance Window



Outline

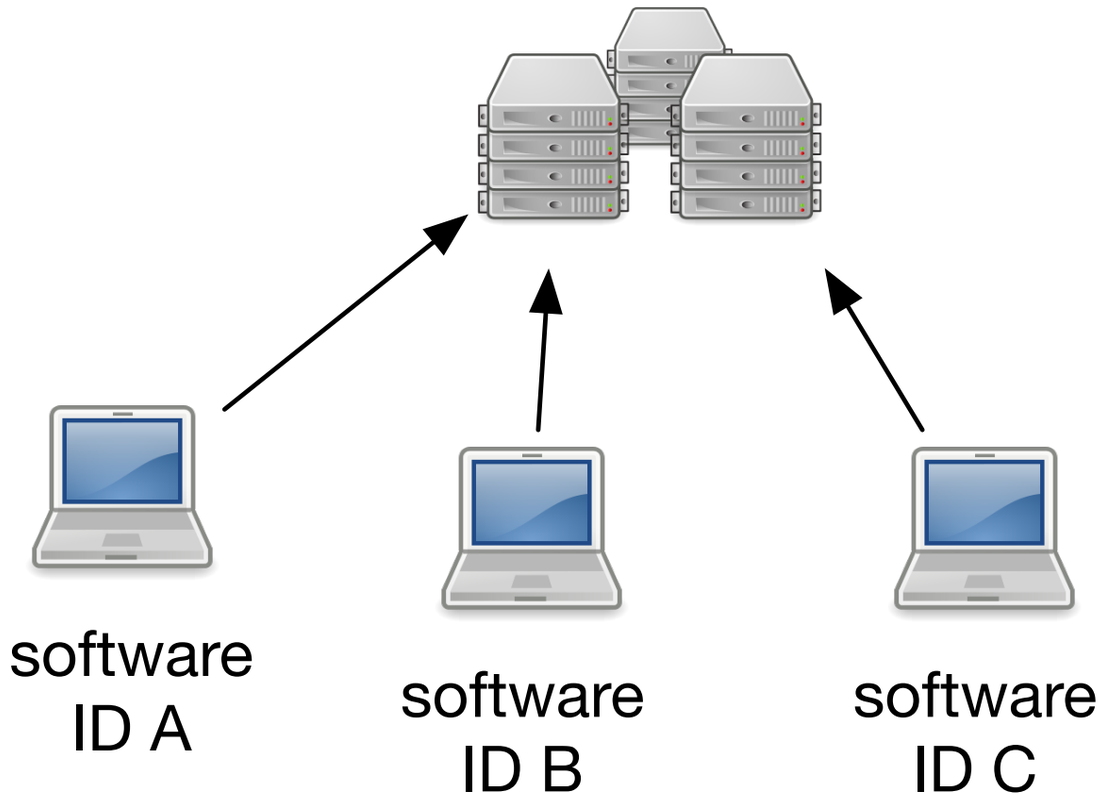
- Disruption Detection
- Global View on Disruptions
- **Device-Centric View on Disruptions**
- U.S. Broadband Case Study

Device Perspective on Disruptions

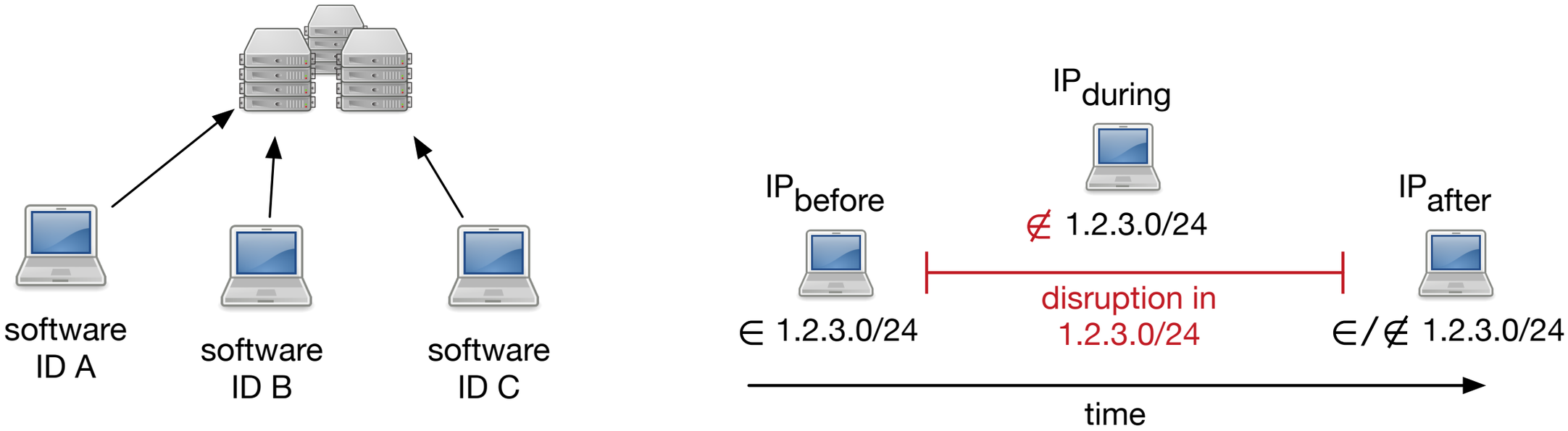


- ➡ Established that this *address block* lost connectivity
- ➡ Do *devices* really lose Internet connectivity?
- ➡ Or can they connect from somewhere else?

Device-Specific Dataset for Subset of Users



Device-Specific Dataset for Subset of Users

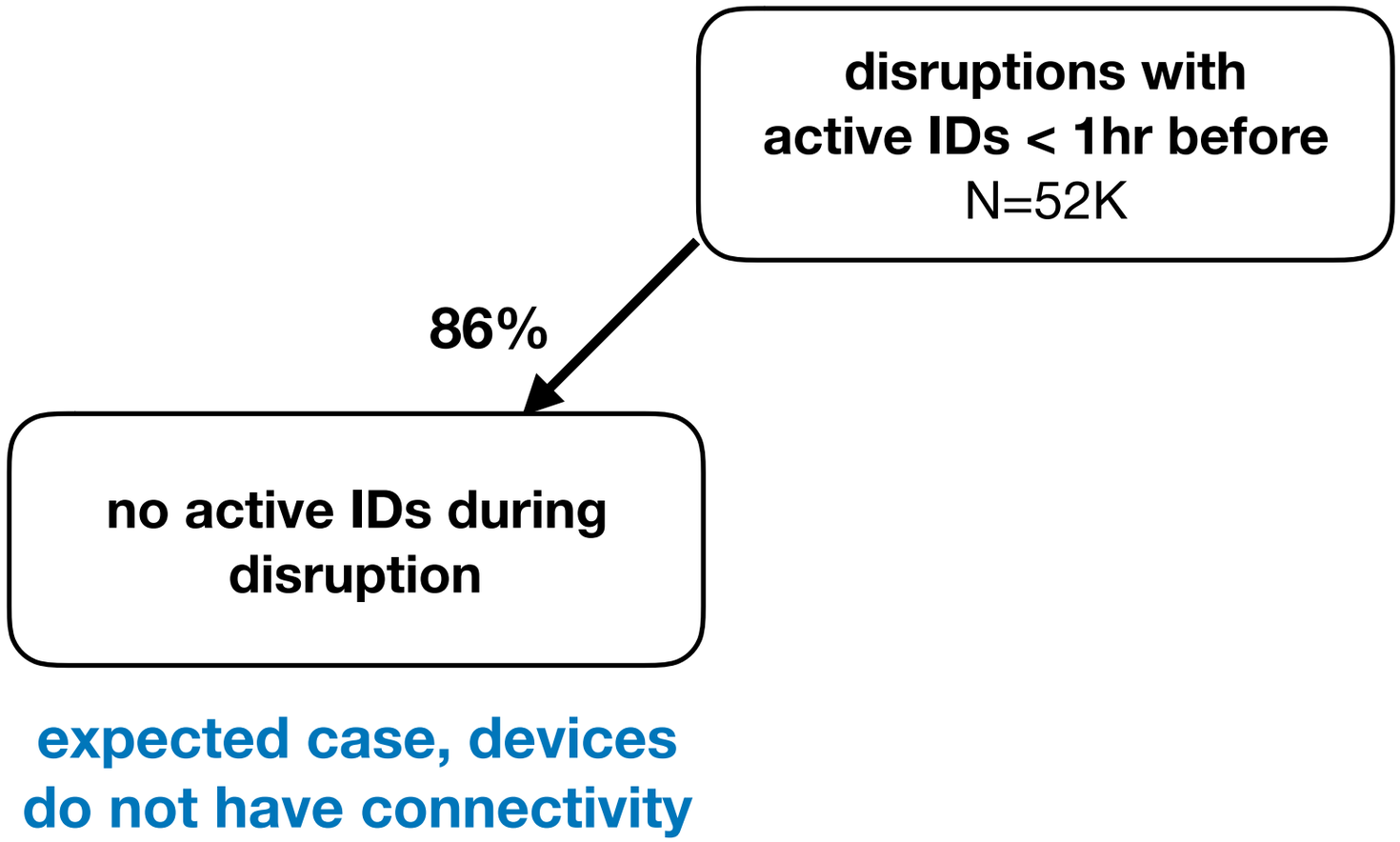


- ➡ Device-information for 52K “entire /24” disruption events
- ➡ Only consider disruptions which affected an entire /24
  (no activity during the disruption)

Device Perspective on Disruptions

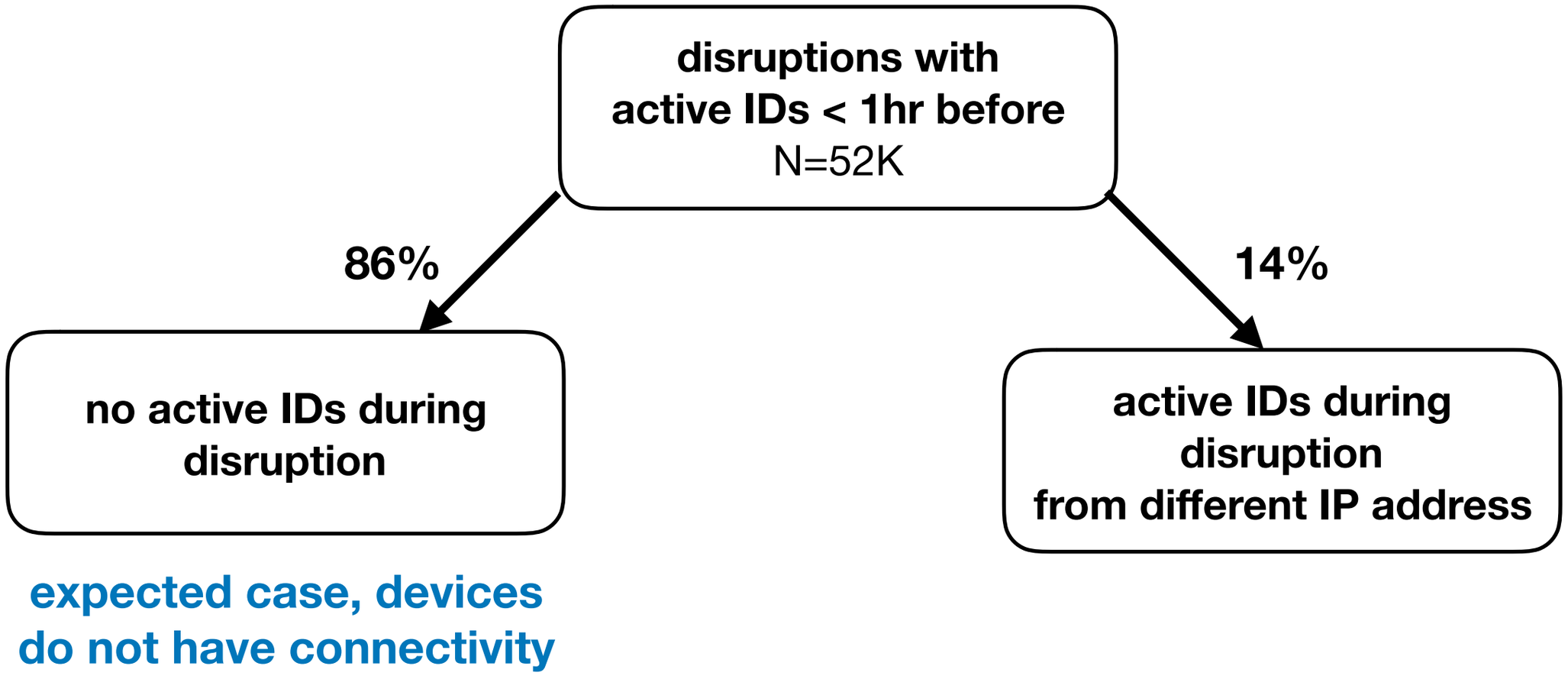
disruptions with
active IDs < 1hr before
N=52K

Device Perspective on Disruptions



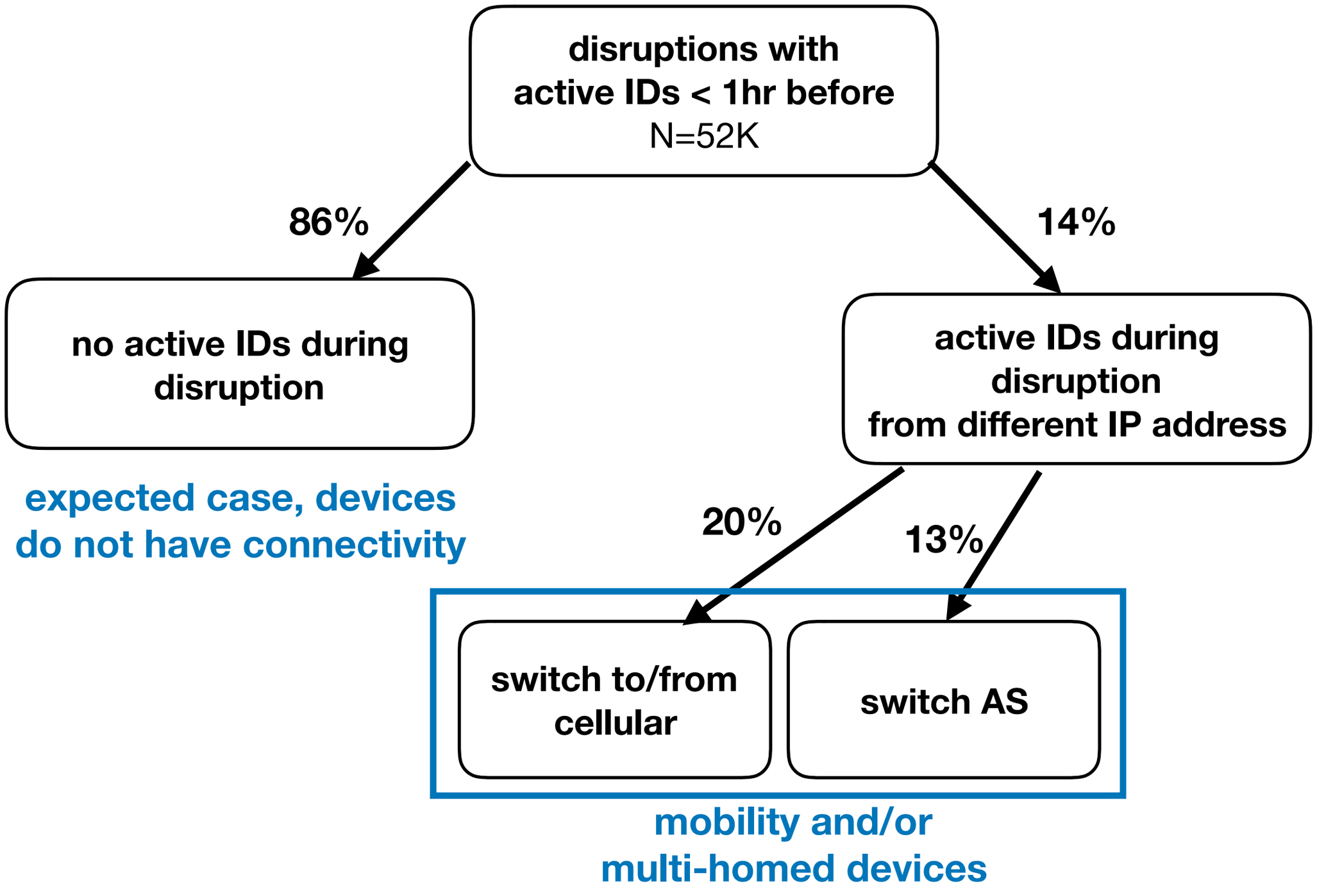
expected case, devices do not have connectivity

Device Perspective on Disruptions



expected case, devices do not have connectivity

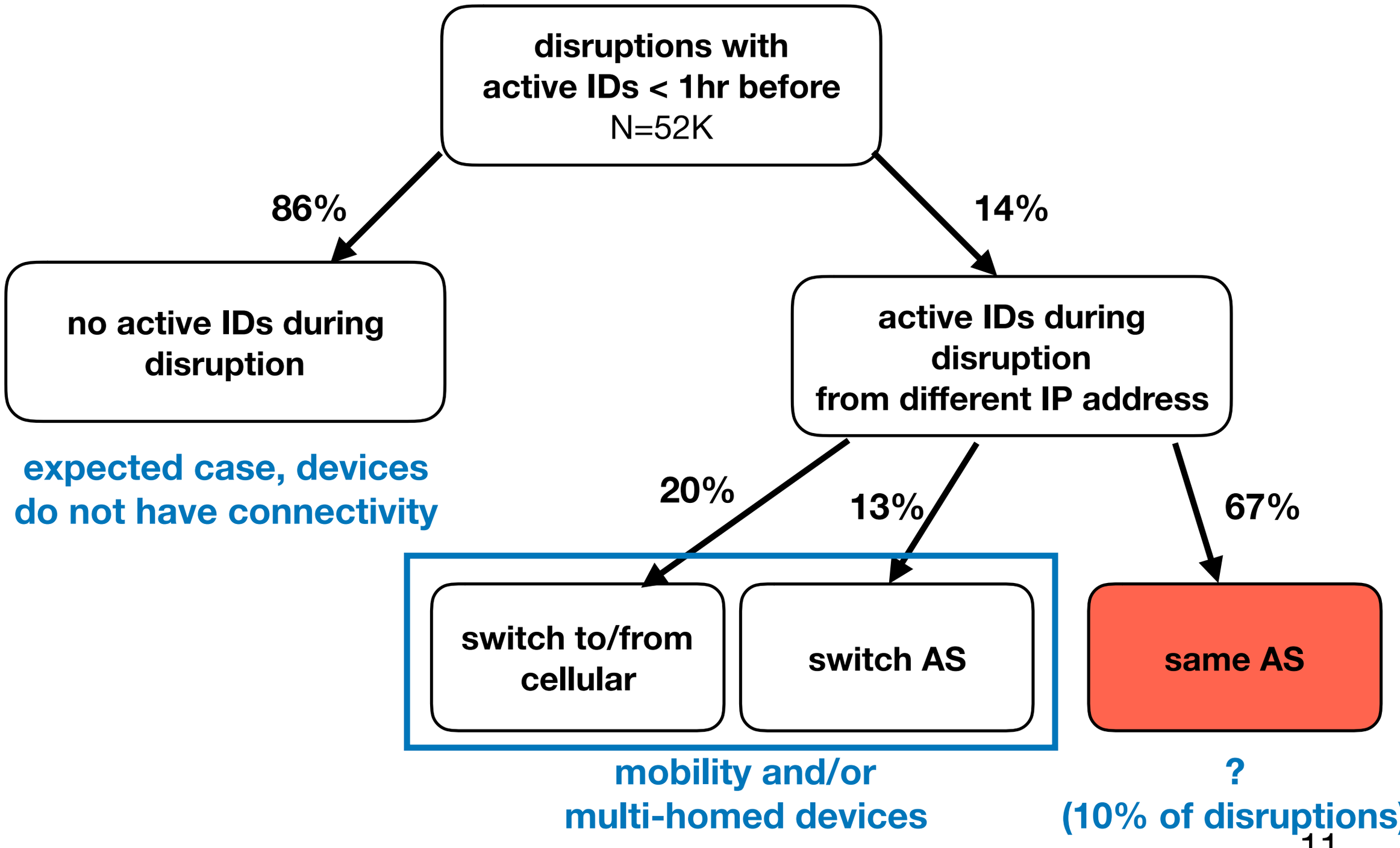
Device Perspective on Disruptions



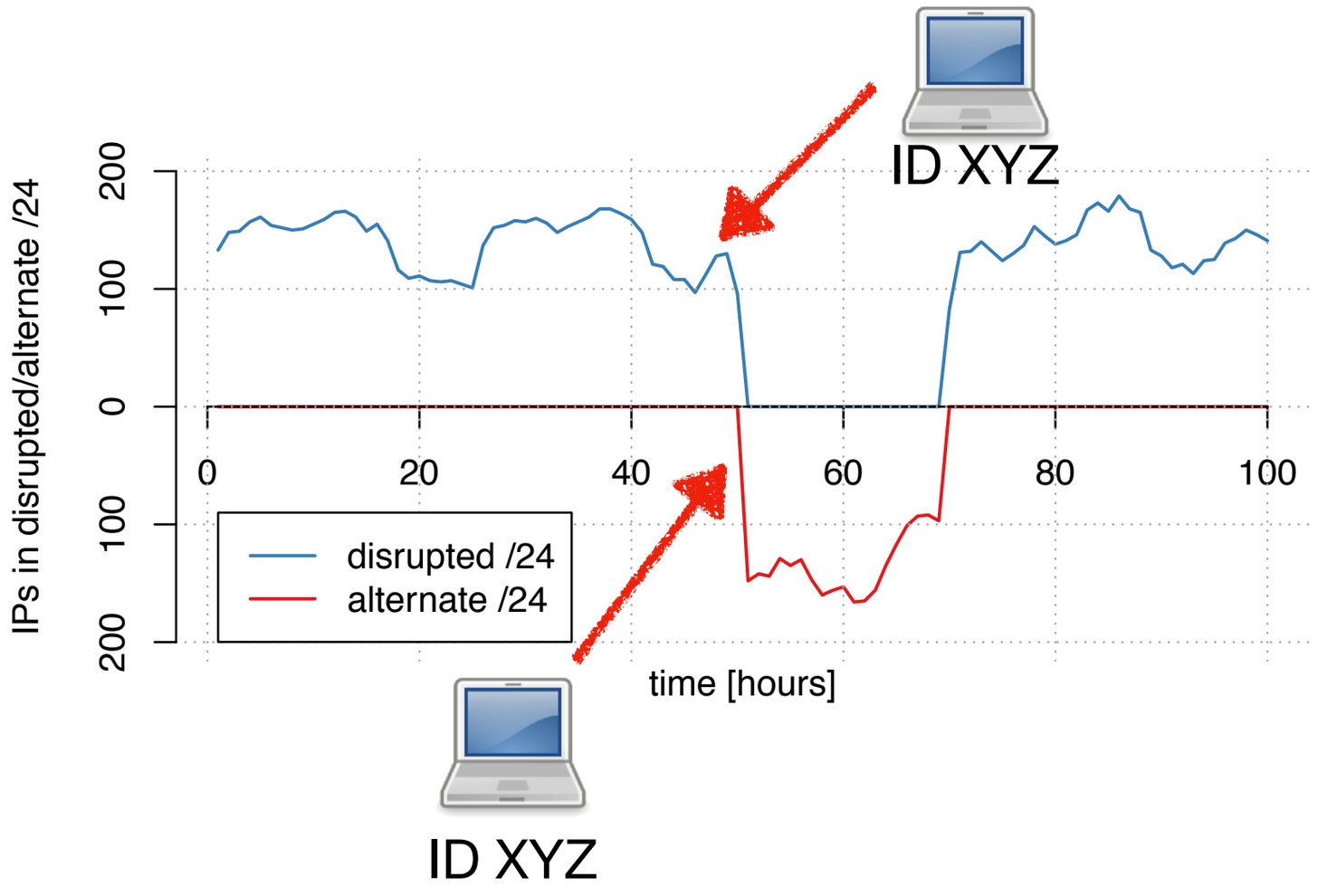
expected case, devices
do not have connectivity

mobility and/or
multi-homed devices

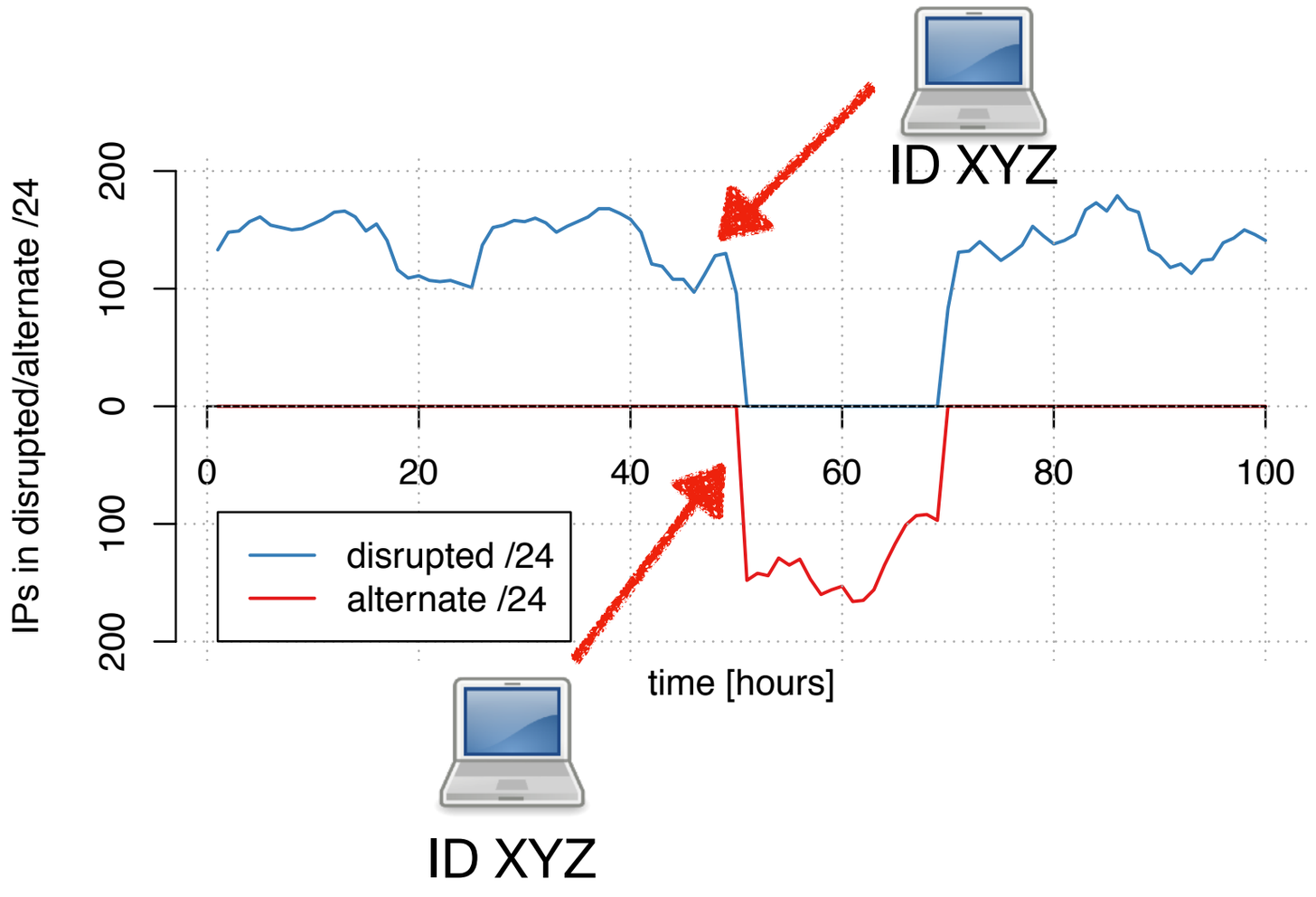
Device Perspective on Disruptions



Anti-Disruptions: Temporary Surges in Address Activity



Anti-Disruptions: Temporary Surges in Address Activity

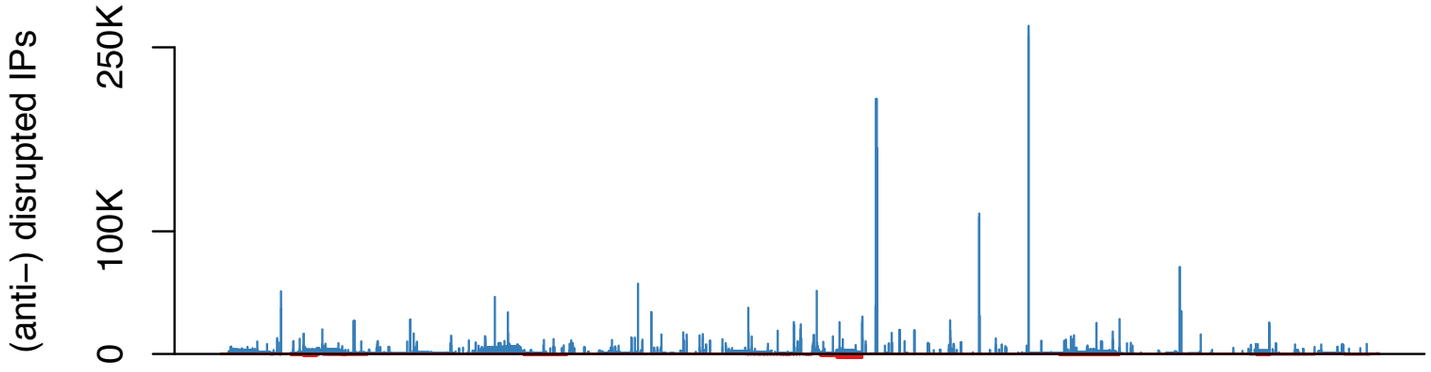


➡ **Some disruptions not service outages but address reassignment!**

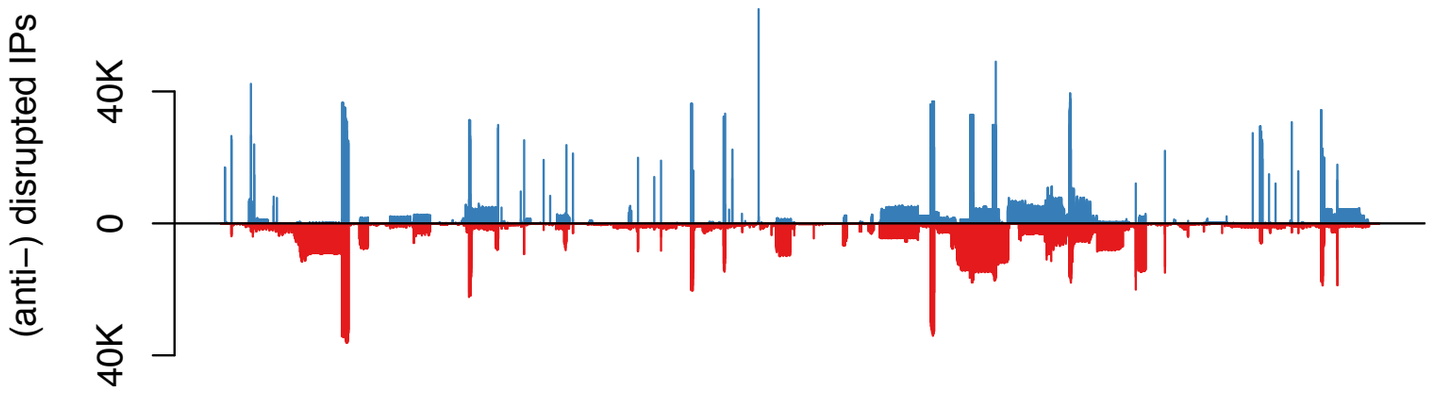
➡ Developed mechanism to detect anti-disruptions

➡ Rank ASes by correlation of disruptions with anti-disruptions

AS-Level Disruptions and Anti-Disruptions

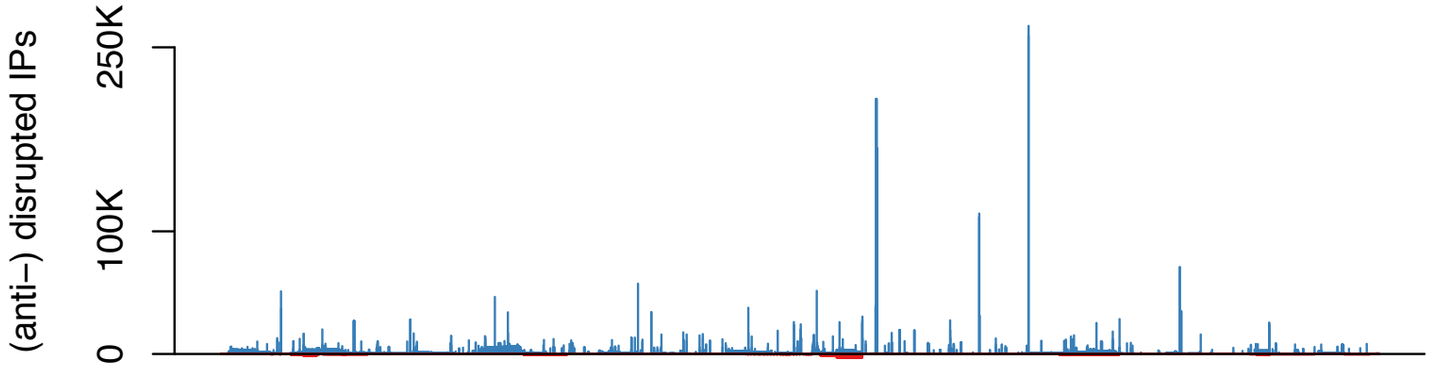


major US cable ISP: No correlation between disruptions and anti-disruptions
(pearson r= 0.02)

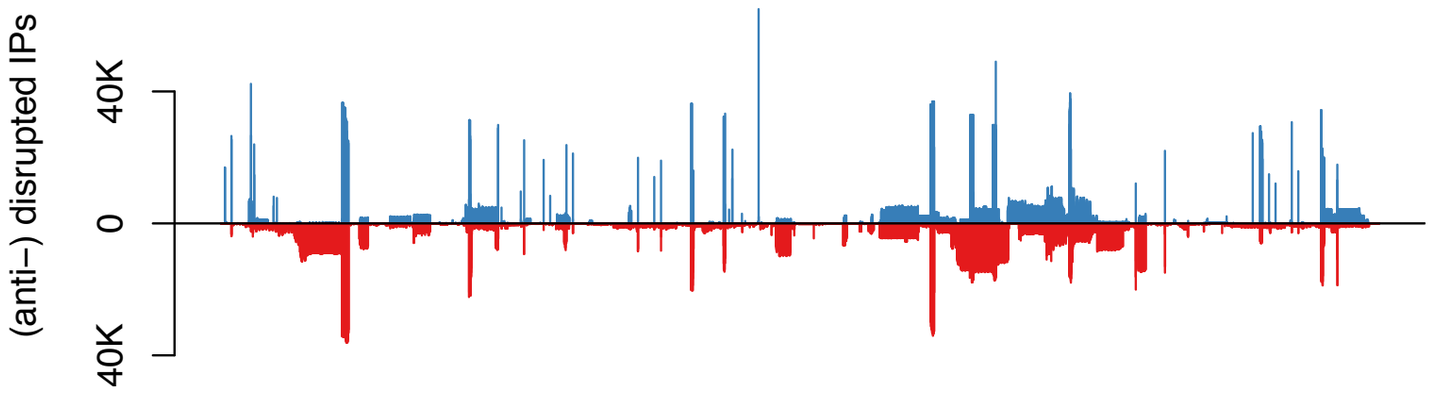


Uruguayan ISP: Strong correlation between disruptions and anti-disruptions
(pearson r= 0.63)

AS-Level Disruptions and Anti-Disruptions



major US cable ISP: No correlation between disruptions and anti-disruptions
(pearson r= 0.02)



Uruguayan ISP: Strong correlation between disruptions and anti-disruptions
(pearson r= 0.63)

Anti-Disruptions can heavily skew per-AS and per-country assessment of Internet reliability

Case Study: US Broadband ISPs

	ISP A Cable	ISP B Cable	ISP C Cable	ISP D DSL	ISP E DSL	ISP F DSL	ISP G DSL

Case Study: US Broadband ISPs

	ISP A Cable	ISP B Cable	ISP C Cable	ISP D DSL	ISP E DSL	ISP F DSL	ISP G DSL
anti-disruption correlation	0.22	0.03	-0.02	0.03	0.00	-0.04	0.05
% disruptions w/ intermittent activity	4%	1%	1%	0%	3%	6%	14%

Most major US broadband ISPs do not show strong signs of anti-disruptions.

Case Study: US Broadband ISPs

	ISP A Cable	ISP B Cable	ISP C Cable	ISP D DSL	ISP E DSL	ISP F DSL	ISP G DSL
anti-disruption correlation	0.22	0.03	-0.02	0.03	0.00	-0.04	0.05
% disruptions w/ intermittent activity	4%	1%	1%	0%	3%	6%	14%
% /24s only disrupted maintenance window	67%	54%	75%	29%	60%	71%	62%

All (but one) ISP has majority of all disrupted /24s during scheduled maintenance window (Mo-Fr Midnight-6AM).

Case Study: US Broadband ISPs

	ISP A Cable	ISP B Cable	ISP C Cable	ISP D DSL	ISP E DSL	ISP F DSL	ISP G DSL
anti-disruption correlation	0.22	0.03	-0.02	0.03	0.00	-0.04	0.05
% disruptions w/ intermittent activity	4%	1%	1%	0%	3%	6%	14%
% /24s only disrupted maintenance window	67%	54%	75%	29%	60%	71%	62%
% /24s only disrupted during Hurricane Irma	11%	1%	2%	23%	1%	0%	3%

ISP A: Some 80% of all disruptions fall in the maintenance window, or are caused by force majeure (Hurricane Irma).

Relevant for SLAs, policies, and reliability assessment.

Implications

- **Outage Detection: Methodological Insights**
  - Baseline activity enables fine-granular detection of disruptions
  - Anti-disruptions due to reassignment
    - ➡ Can bias active and passive outage detection systems
- **Interpreting Service Outages**
  - Majority of outages (for many ISPs) during scheduled maintenance
    - ➡ Implications for SLAs, reporting requirements, regulations