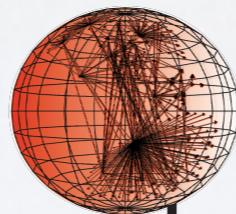


IODA - Internet Outages: Detection & Analysis

Alberto Dainotti
alberto@caida.org



caida

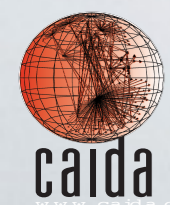
www.caida.org

Center for Applied Internet Data Analysis
University of California, San Diego

CAIDA

intro

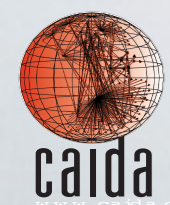
The Center for Applied Internet Data Analysis (CAIDA) is an independent analysis and research group based at the University of California's San Diego Supercomputer Center. CAIDA investigates both practical and theoretical aspects of the Internet.



CAIDA


research highlights

- topology analysis
 - Internet-scale router alias resolution
 - comparing IPv6 & IPv4 topology
 - Internet topology data sharing
- security & stability
 - large-scale Internet outages
 - botnet activity
 - BGP hijacks
- Internet peering analysis
 - inferring AS relationships
 - AS ranking
- interconnection economics
 - modeling peering strategies
 - transit pricing
- modeling complex networks
 - using hidden metric spaces
- geolocation analysis
 - comparing geolocation services
 - IP reputation vs. governance
- future Internet
 - IPv6
 - Named Data Networking
- visualization



CHRONOLOGY

CAIDA and Internet Outages

- **Jan/Feb 2011** - Internet Kill Switch in Egypt and Libya
- **Nov 2011** - We present a novel approach to study Internet Outages by **combining different types of Internet measurements**
- **Jan 2012** - We present a study on the impact of natural disasters on the network infrastructure
- **Sep 2012** - NSF funds CAIDA to further develop our methodology and build an **experimental operational deployment** to monitor the public IPv4 Internet (**IODA**) 
- **2012 - 2015** — more science and a lot of engineering
- **Today** a prototype that starts to be quite usable

BEFORE IODA

post-event manual analysis

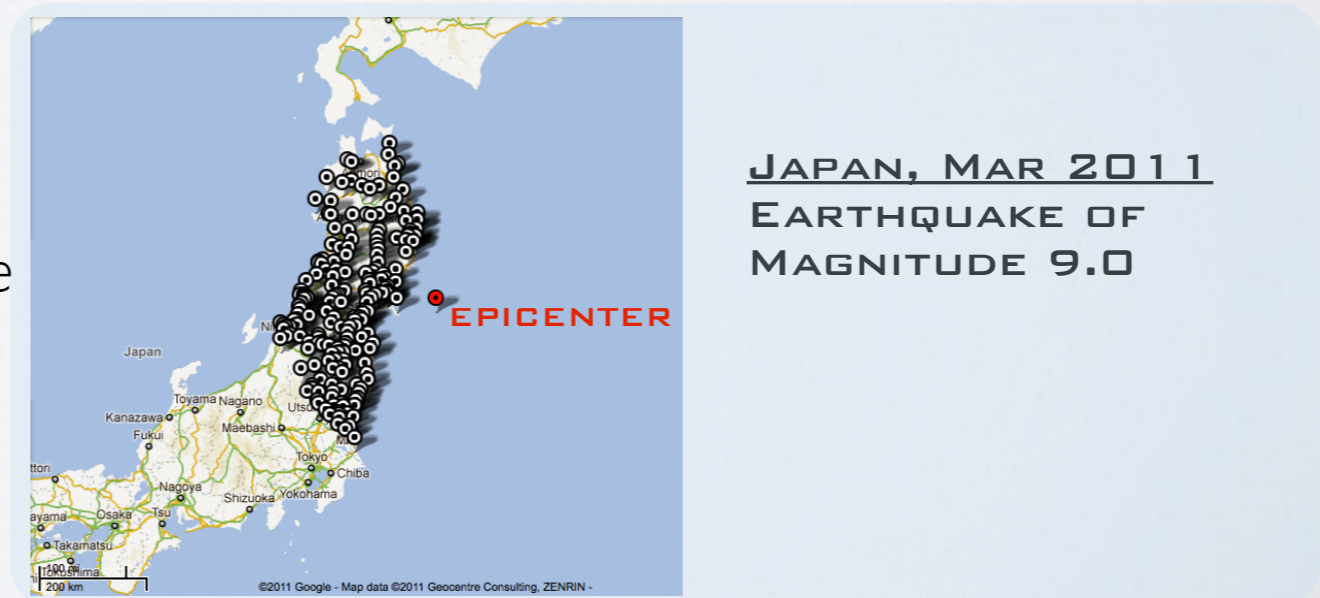
- Country-level Internet Blackouts during the Arab Spring

Dainotti et al. "Analysis of Country-wide Internet Outages Caused by Censorship"
ACM SIGCOMM IMC 2011



- Natural disasters affecting the infrastructure

Dainotti et al. "Extracting Benefit from Harm: Using Malware Pollution to Analyze the Impact of Political and Geophysical Events on the Internet"
ACM SIGCOMM CCR 2012

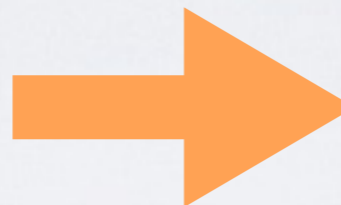


BEFORE IODA

post-event manual analysis



EGYPT, JAN 2011
GOVERNMENT ORDERS
TO SHUT DOWN THE
INTERNET



4 months of work

Analysis of Country-wide Internet Outages Caused by Censorship

Alberto Dainotti
University of Napoli Federico II
alberto@unina.it

Claudio Squarcella
Roma Tre University
squarccl@dia.uniroma3.it

Emile Aben
RIPE NCC
emile.aben@ripe.net

Kimberly C. Claffy
CAIDA/UCSD
kc@caida.org

Marco Chiesa
Roma Tre University
chiesa@dia.uniroma3.it

Michele Russo
University of Napoli Federico II

Antonio Pescapè
University of Napoli Federico II

ABSTRACT

In the first months of 2011, several North African countries and their citizens (in the form of multiple and in various instances) were affected by Internet outages. We analyze these outages by using network data, specifically data from the UCSD network telescope, traces and MaxMind's geolocation database to determine which within each country, as well as BGP announced using publicly available reports. We then analyzed policies and ASes from control plane and data plane which are presented in a given network diagram what we believe based blocking before disconnection. Our main dataset outages or similar geographic or topologic

Categories and S
C.2.3 [Network Opera
C.2.3 [Local and Wide

General Terms
Measurement, Security

Permission to make digital
copies or distributions may
not be made or distributed for
profit or commercial purposes
without express permission of
CAIDA. November 2-4, 2011
Copyright 2011 ACM 978-

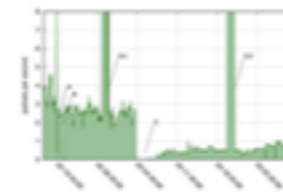


Figure 12: UCSD telescope's traffic coming from Libya. Labels A, B, C indicate the three outages. Spikes labeled D1 and D2 are due to backbone business denial of service attacks.

related to protests in the country. The web site of the Ministry of Communications (www.gov.eg) was attacked with a randomly-specified DoS attack just before the outage started, on January 26 at different times: 15:47 GMT (for 16 minutes), 16:55 GMT (17 minutes), and 21:09 GMT (53 minutes). Analysis of the backbone traffic to the domain allows estimation of the intensity of the attack in terms of packet rate, indicating average packet rates between 25k and 50k packets per second.

On February 2 the web site of the Egyptian Ministry of Interior (www.moi.gov.eg) was targeted by two DoS attacks just after the end of the censorship from 13:08 to 13:30 GMT and from 15:08 to 17:17 GMT. The same IP address was attacked another time the day after, from 08:06 to 08:42 GMT. In this case the estimated packet rates were smaller, around 7k packets per second.

5.2 Libya

5.2.1 Overview

Libya's Internet infrastructure is even more prone to manipulation than Egypt's, judging from its physical structure. International connectivity is provided by only two submarine cables, both ending in Tripoli [36], and the Internet infrastructure is dominated by a single, state-owned, AS. We only found two other ASes having a small presence in Libya, as described in Section 5.2.2.

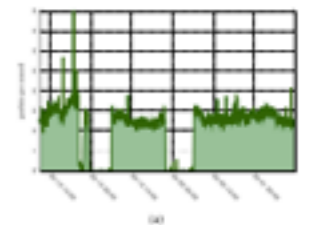
In Libya three different outages in early 2011 were identified and publicly documented (Figure 1). Figure 12 shows the traffic observed by the UCSD network telescope from Libya throughout an interval encompassing the outages. The points labeled A, B and C indicate three different blackout episodes; points D1 and D2 refer to two denial-of-service attacks discussed in Section 5.2.3. Toward the right of the graph it is difficult to interpret what is really happening in Libya because of the civil war.

5.2.2 Outages in detail

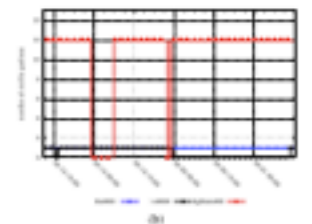
The first two outages happened during two consecutive nights. Figure 13(a) shows a more detailed view of these two outages as observed by the UCSD telescope. Figure 13(b) shows BGP data over the same interval: in both cases, within a few minutes, 12 out of the 15 IPv4 prefixes associated with IP address ranges officially delegated to Libya were withdrawn. These twelve IPv4 prefixes were announced by LibNetAS, the local telecom operator, while the remaining IPv4 prefixes were managed by IRIAS2. As of May 2011, there were no IPv4 prefixes in AfriNIC's delegated file for Libya. The MaxMind IP geolocation database further puts 12 non-contiguous IP ranges in Libya, all part of an encompassing IPv4

prefix announced by SatAS, which provides satellite services in the Middle East, Asia and Africa. The covering IPv4 prefix also contained 180 IP ranges in several other countries, predominantly in the Middle East. We considered this additional AS because the UCSD dataset generally observed a significant amount of truncated traffic coming from IPs in those 12 ranges before the first outage (about 5k packets each day). This level of background traffic indicates a population of customers using PCs likely infected by Conficker or other malware, allowing inference of network conditions. Traffic from this network also provided evidence of what happened to Libyan Internet connections based on satellite systems not managed by the local telecom provider.

Comparing Figures 13(a) and 13(b) reveals a different behavior than conflicts with previous reports [17]: the second outage was not entirely caused by BGP withdrawals. The BGP shutdown began on February 19 around 23:58:55 UTC, exactly matching the sharp decrease of distinct traffic from Libya (and in accordance with reports on Libyan traffic seen by Aben Networks [34]) but it ended approximately one hour later, at 25:02:52. In contrast, the Internet outage as shown by the telescope data and reported by the news [17] lasted until approximately February 20 at 6:12 UTC. This finding suggests that a different disruption technique – a packet-blocking strategy apparently adopted subsequently in the third outage and recognized by the rest of the world – was already being used dur-



(a)



(b)


Figure 13: The first two Libyan outages: (a) uncollected traffic to UCSD dataset coming from Libya; (b) visibility of Libyan IPv4 prefixes in BGP data from Rome/Aben and RIPE NCC/RIPE collectors. Note that the control-plane and data-plane observations of connectivity do not match, suggesting that different techniques for censorship were being used during different intervals.

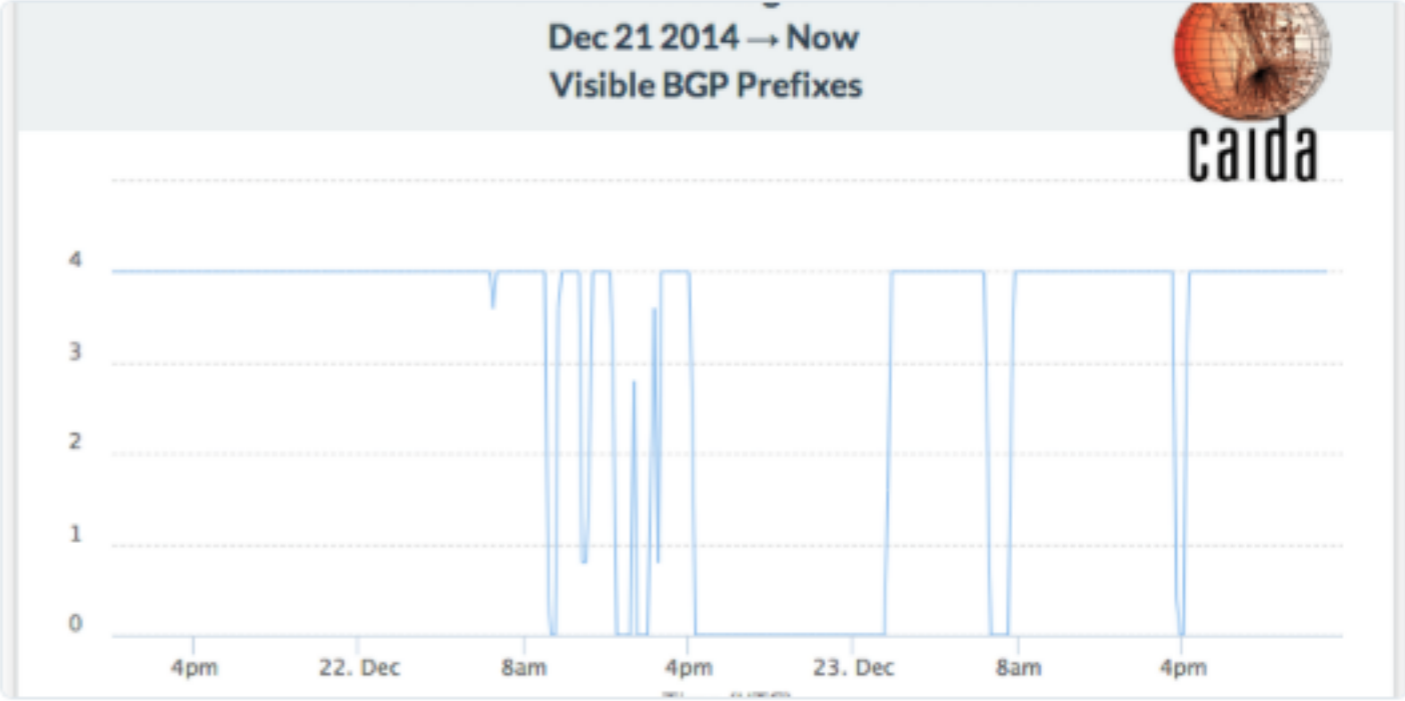
IODA TODAY

live Internet monitoring



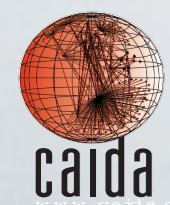
Last Christmas we made it possible for anybody to follow the North Korean disconnection almost live

 CAIDA @caidaorg · Dec 23
Follow outages in #NorthKoreaInternet in almost real-time (30min delay) at [charthouse.caida.org/public/kp-outage...](https://charthouse.caida.org/public/kp-outage)



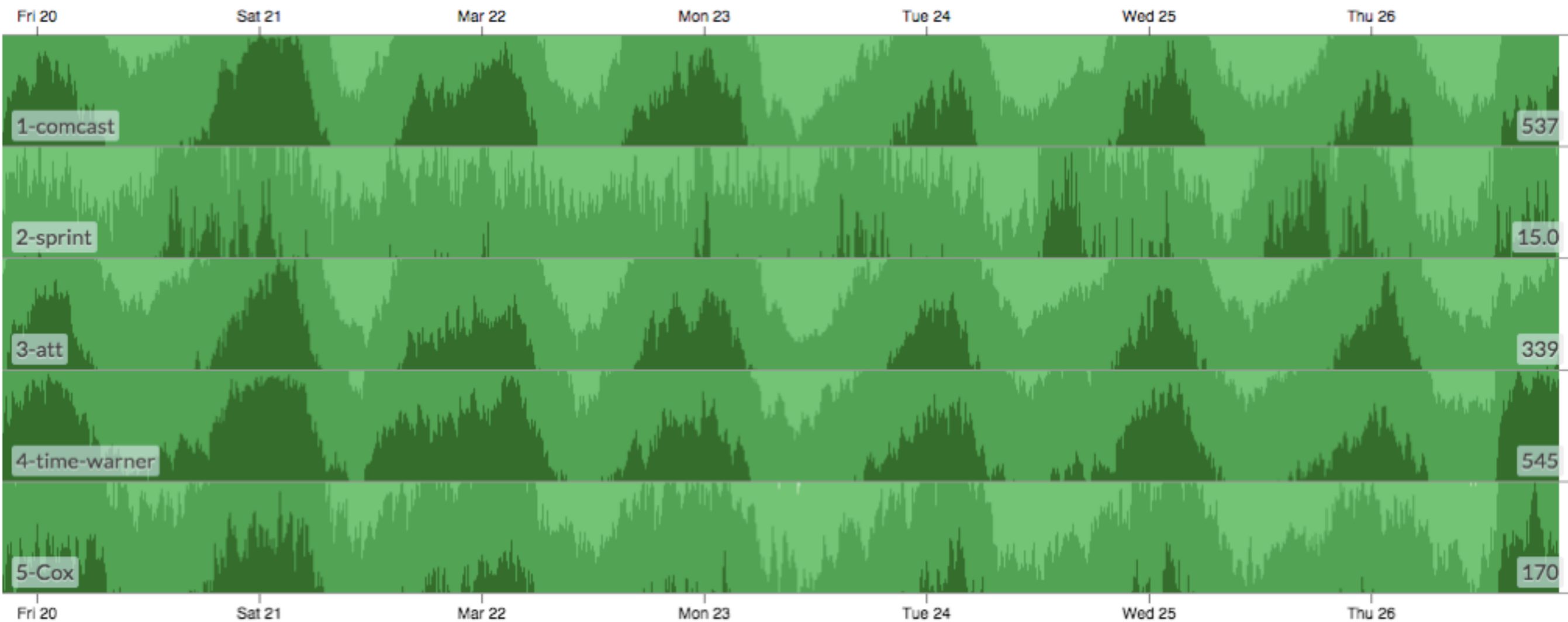
Dec 21 2014 → Now
Visible BGP Prefixes

← 3 ☆ 4 ⋮ View more photos and videos

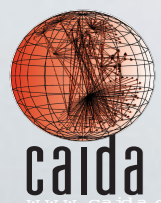


IODA TODAY

let's see how Internet providers are doing in the US

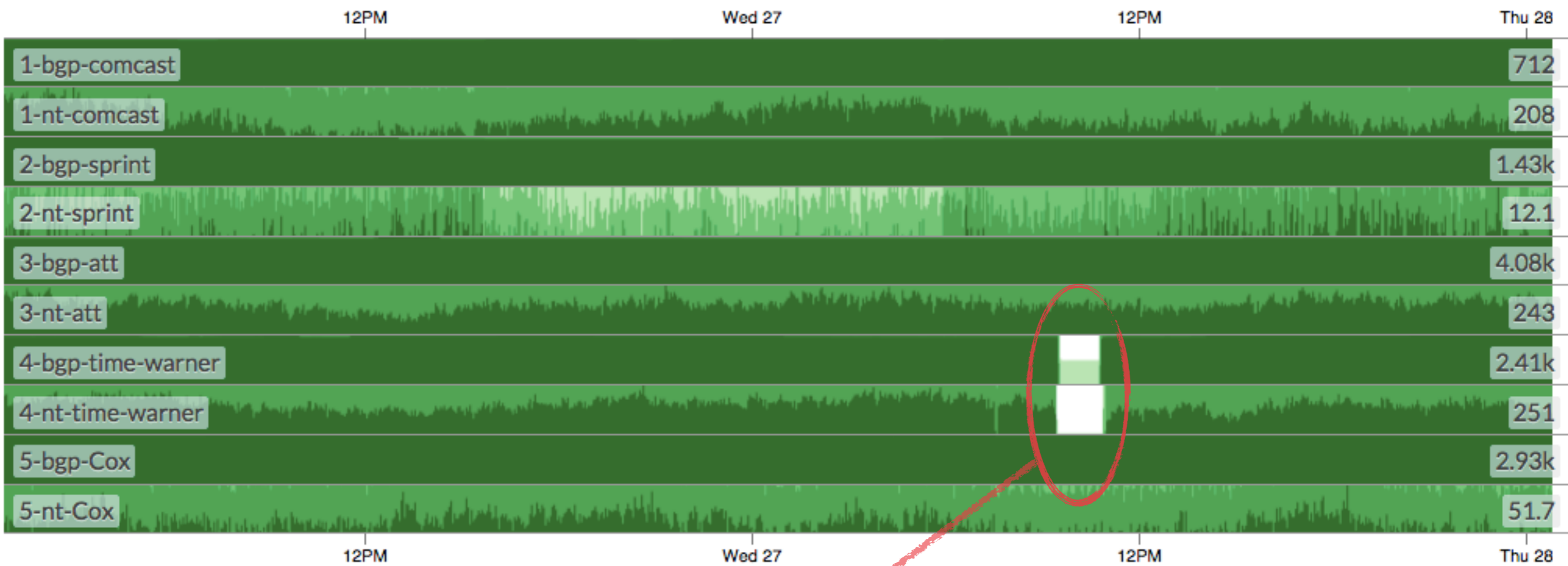


EVERYTHING LOOKS FINE...



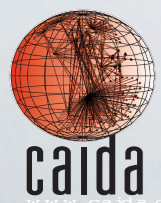
IODA TODAY

Same type of graphs at the end of August 2014



Series: 10 | # Points: 28800 | Data resolution: minute

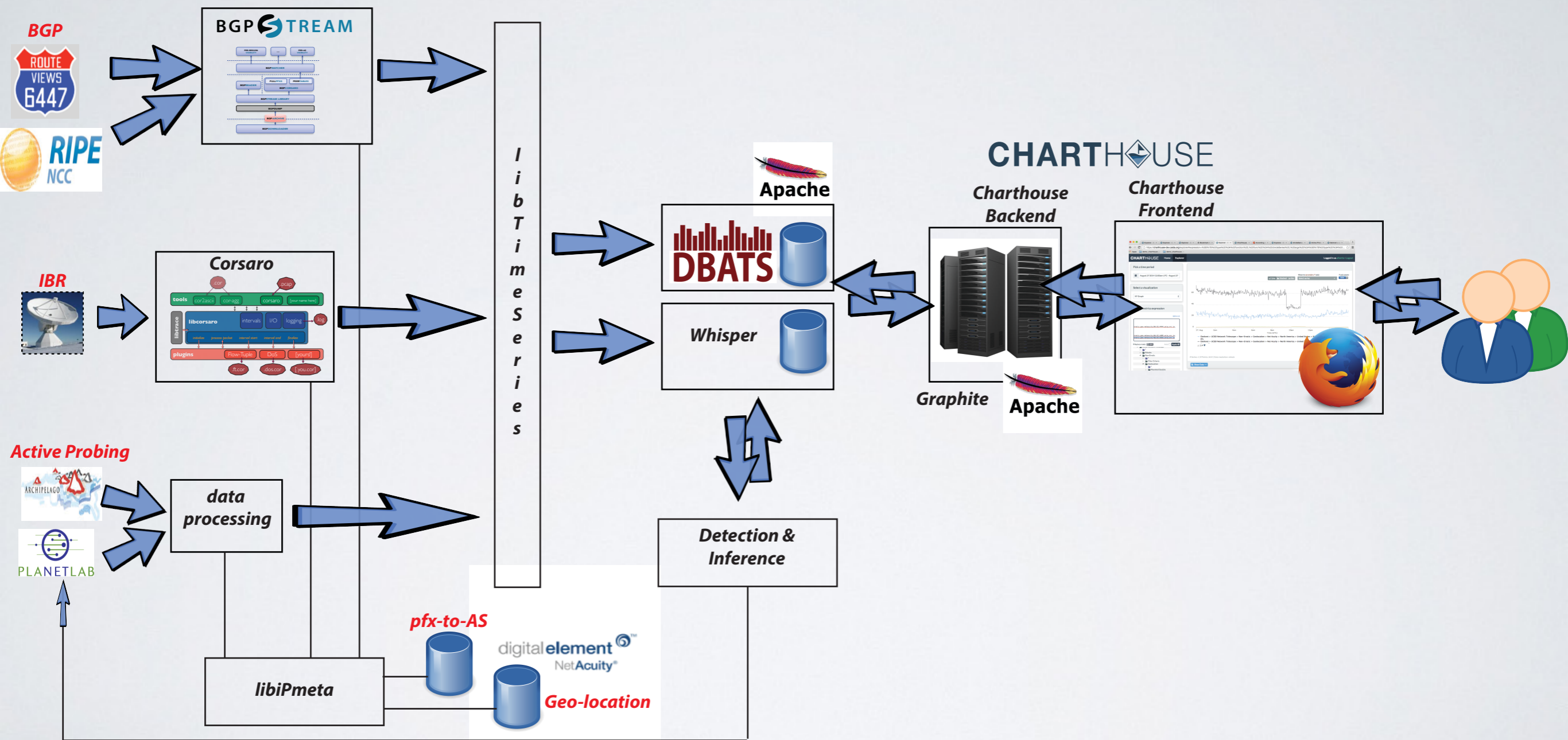
TWO INDICATORS SHOW SOMETHING WENT WRONG WITH TIME WARNER



Center for Applied Internet Data Analysis
University of California San Diego

IODA

the system at a glance



IODA

Internet Outages: Detection & Analysis

- **multiple** types of **sources and methodologies**

- Routing Plane [BGP]
- Data Plane
 - Active probing [pinging + traceroutes]
 - Passive [IBR]
- *easy to plug new sources*



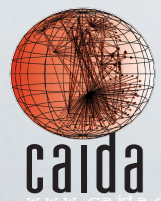
- **meta-data** to extract *liveness* signals for various aggregations (*countries, counties, cities, /24 address blocks, prefixes, ASNs*)

- combining signals to **detect & monitor**

- **trigger ad hoc active measurements** when an event is detected

- **visual interface** for analysis and dashboards

CHARTHOUSE



BGP

Border Gateway Protocol



- BGP

- The protocol that establishes routes between ISP networks (**autonomous systems**) all over the world

- Autonomous Systems (AS)

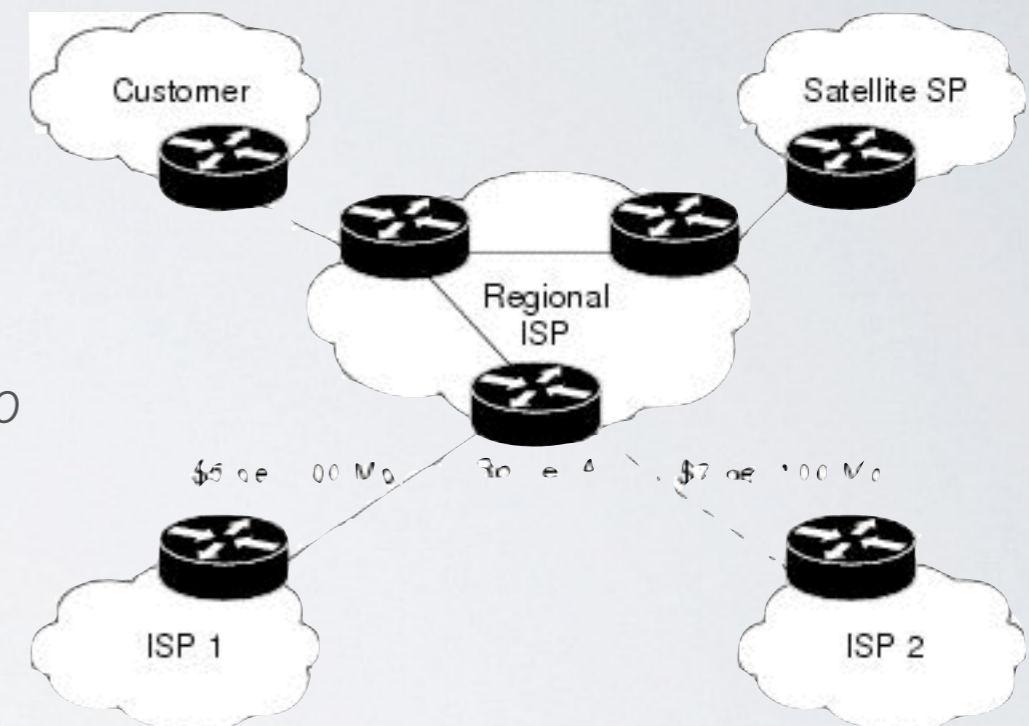
- “a set of routers under a single technical administration, using an interior gateway protocol and common metrics to determine how to route packets within the AS, and using an inter-AS routing protocol to determine how to route packets to other ASs.” - RFC 4271

- Network Prefixes

- Smaller networks are identified by a network address and a network mask

- e.g. prefix $192.172.0.0/16$ is assigned to AS99 and is reachable by AS67 through the **AS path**: $AS67 \rightarrow AS44 \rightarrow AS15 \rightarrow AS99 \rightarrow 192.172.0.0/16$

- AS paths are computed by exchanging **BGP update messages**: “Hey, I’m AS44 and can reach $192.172.0.0/16$ through $AS15 \rightarrow AS99$ ”



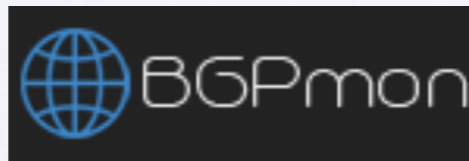
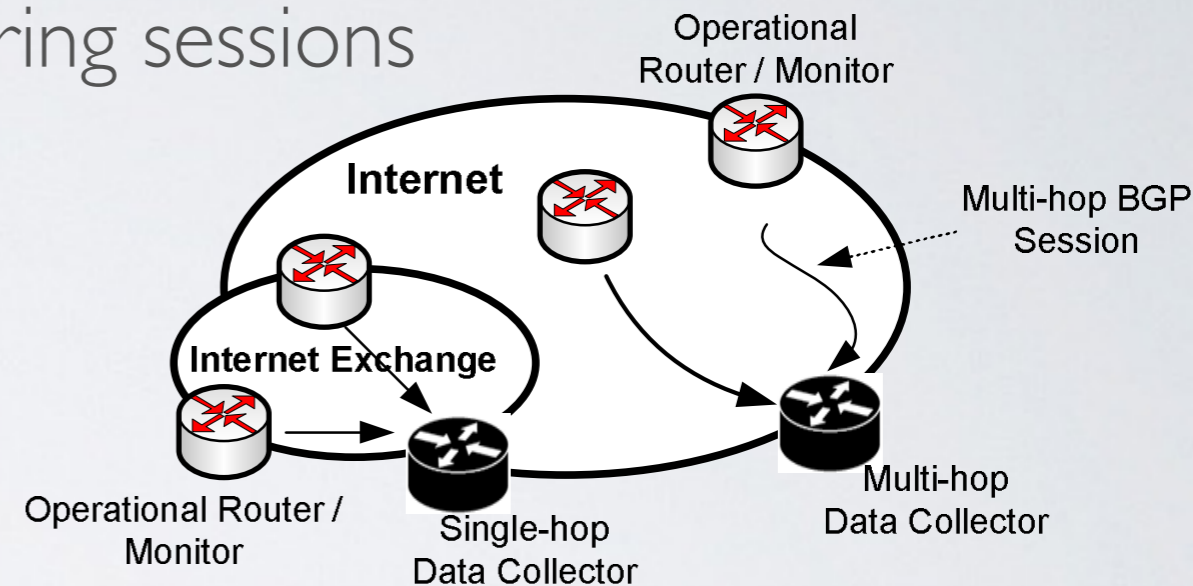
BGP DATA COLLECTION

Route Collectors and Route Monitors



- BGP measurement projects establish peering sessions with ASes to receive their routing tables (no exchange of other traffic)

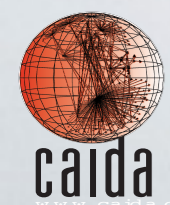
- RouteViews (Univ. Oregon): 371 peers
- RIPE RIS (RIPE NCC): 508 peers
- BGPmon (Colorado State Univ.): 330 peers



<http://www.routeviews.org>

<https://www.ripe.net/data-tools/stats/ris>

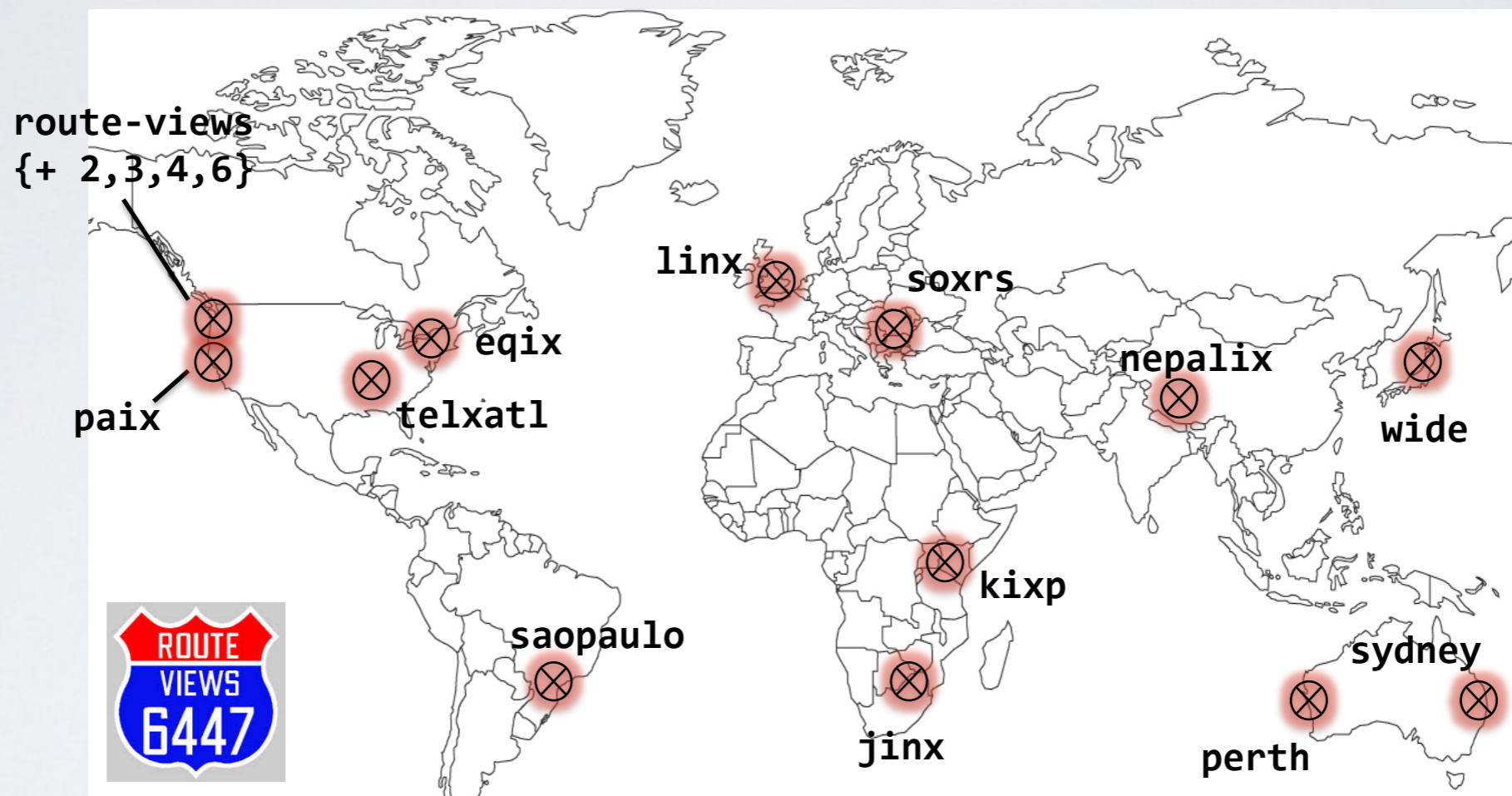
<http://bgpmon.netsec.colostate.edu>



Center for Applied Internet Data Analysis
University of California San Diego

BGP DATA COLLECTION

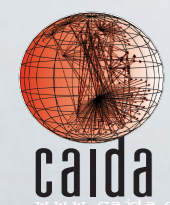
RouteViews Collectors



<http://www.routeviews.org>

BGP DATA COLLECTION

IPv4/IPv6 BGPmon peers around the world



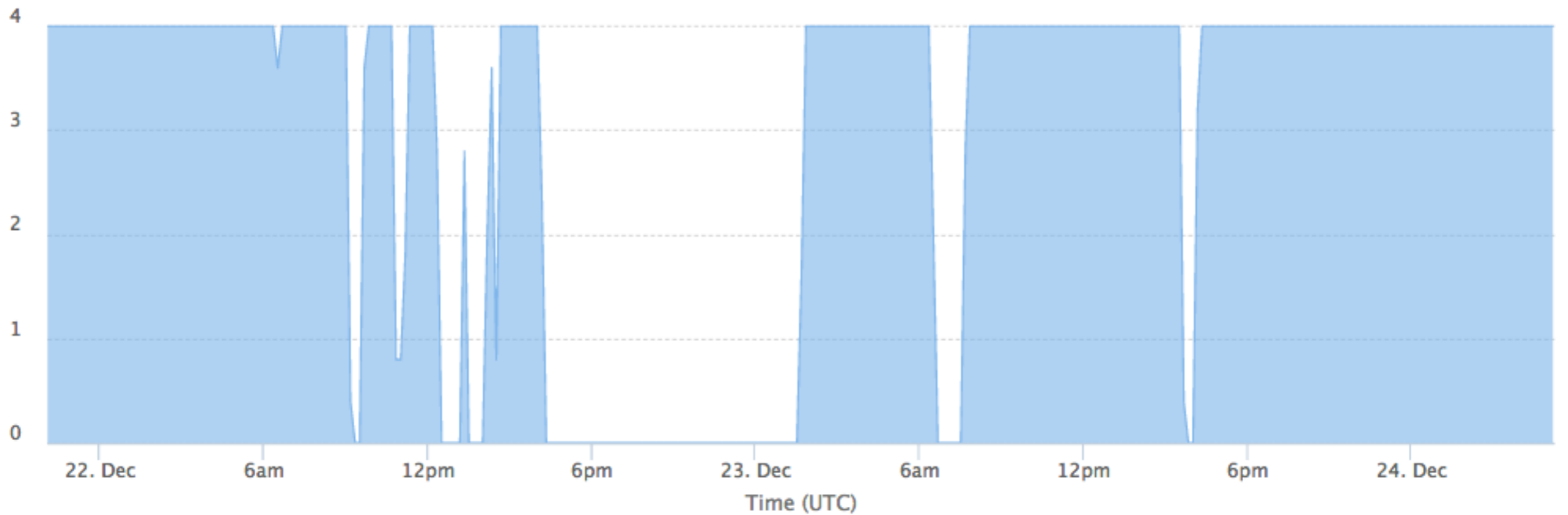
Center for Applied Internet Data Analysis
University of California San Diego

<http://bgpmon.netsec.colostate.edu>

BGP: OUTAGES



North Korea (AS131279) - Dec 2014

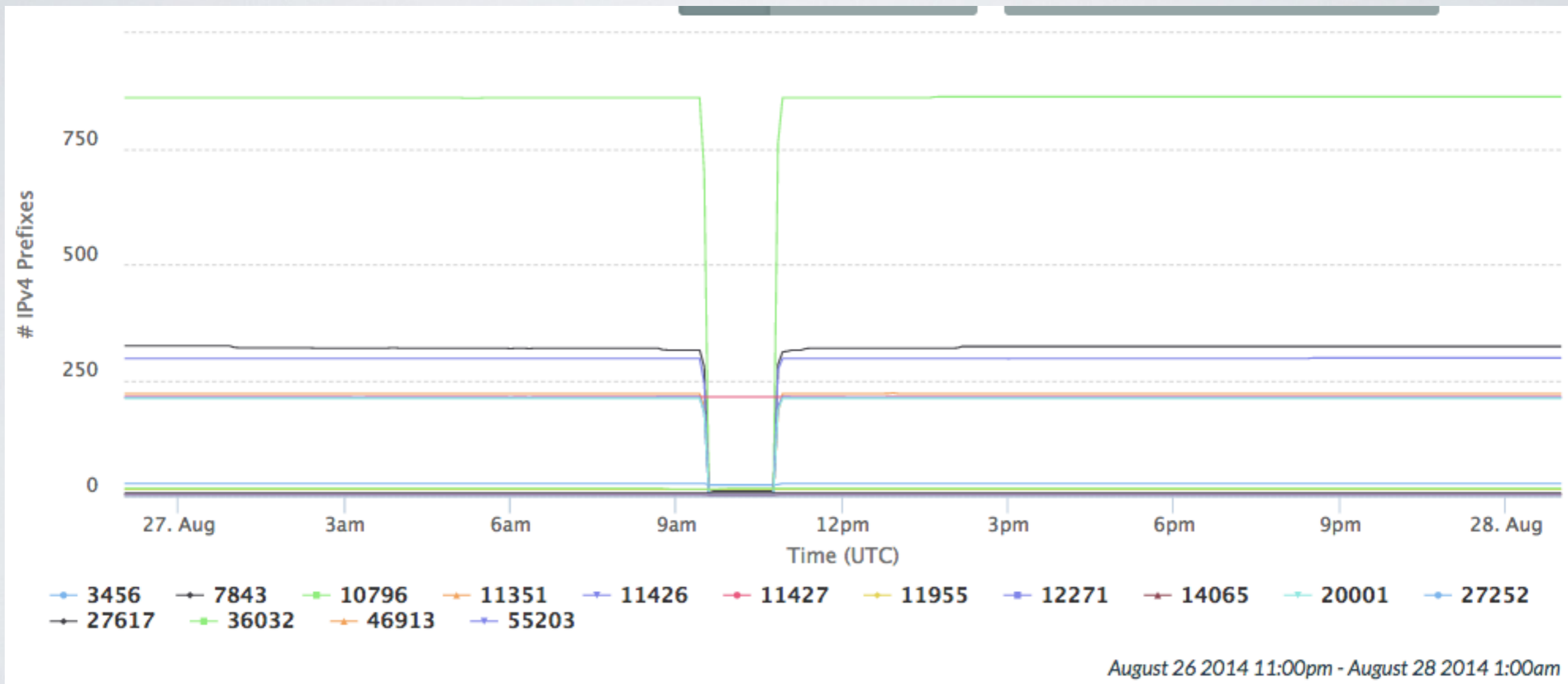


December 21 2014 10:04pm - December 24 2014 5:13am

BGP: OUTAGES



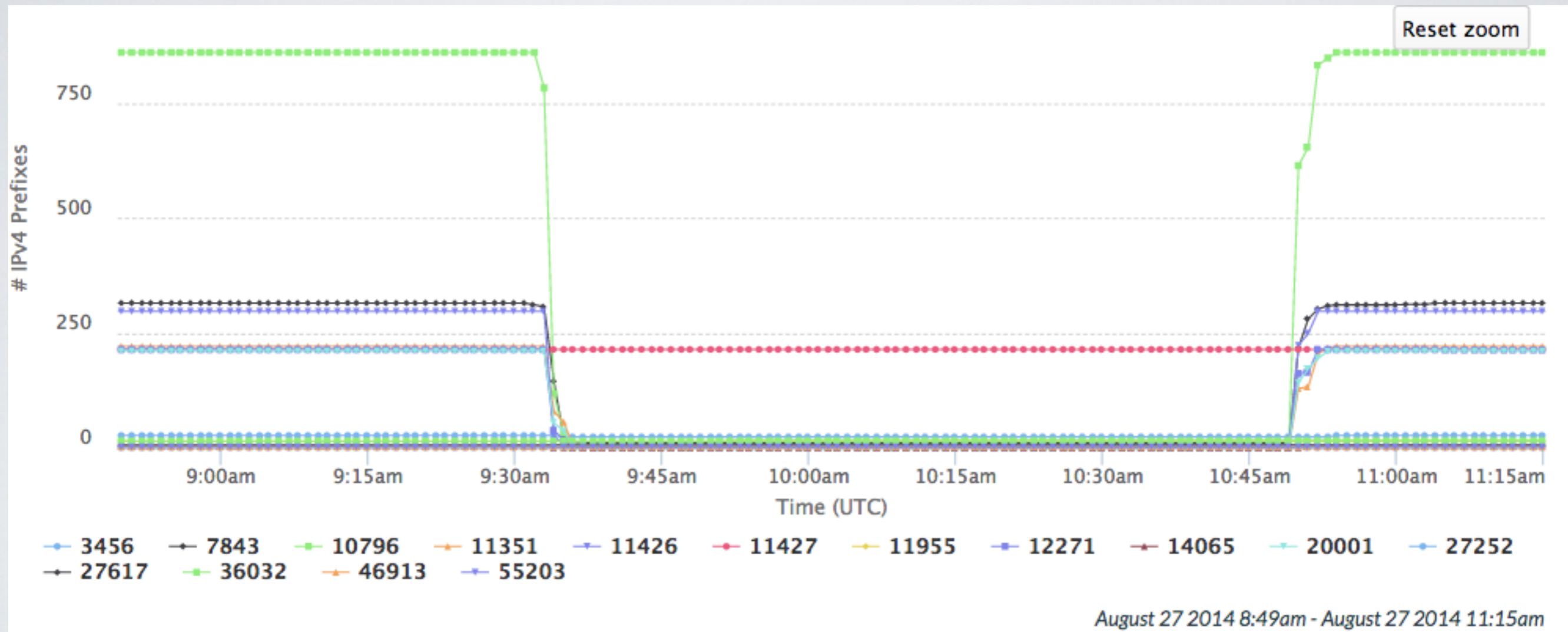
Time Warner Cable - 27th Aug 2014



BGP: OUTAGES



Time Warner Cable - 27th Aug 2014

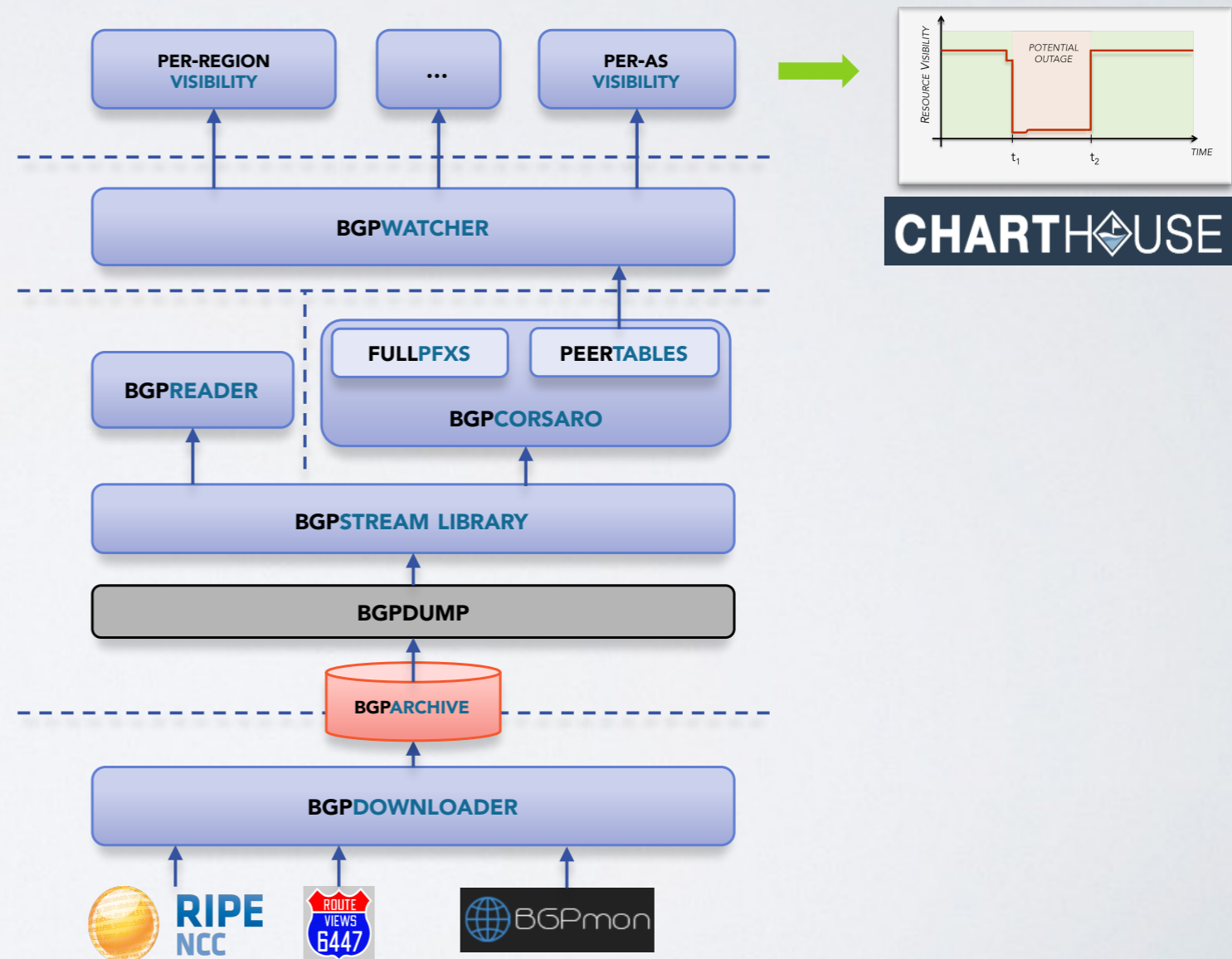


BGPSTREAM

our BIG DATA framework for BGP



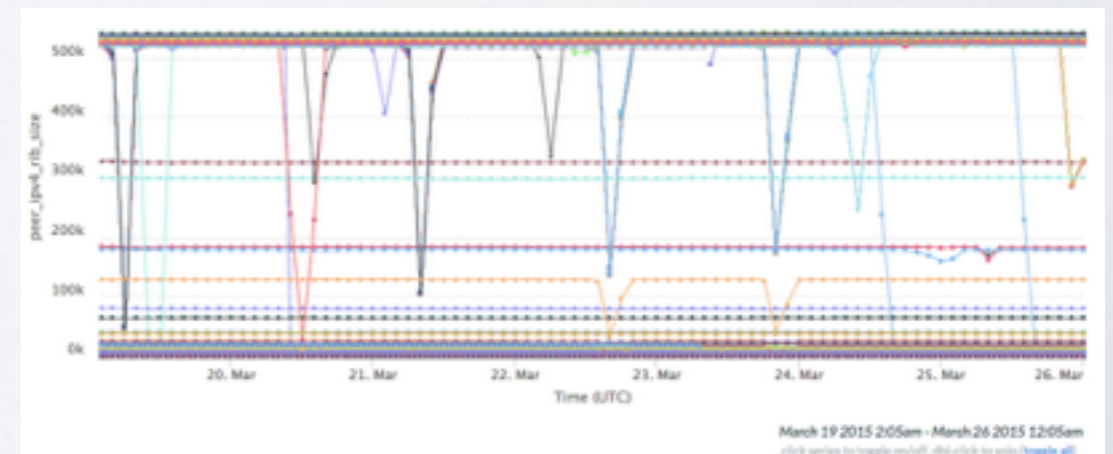
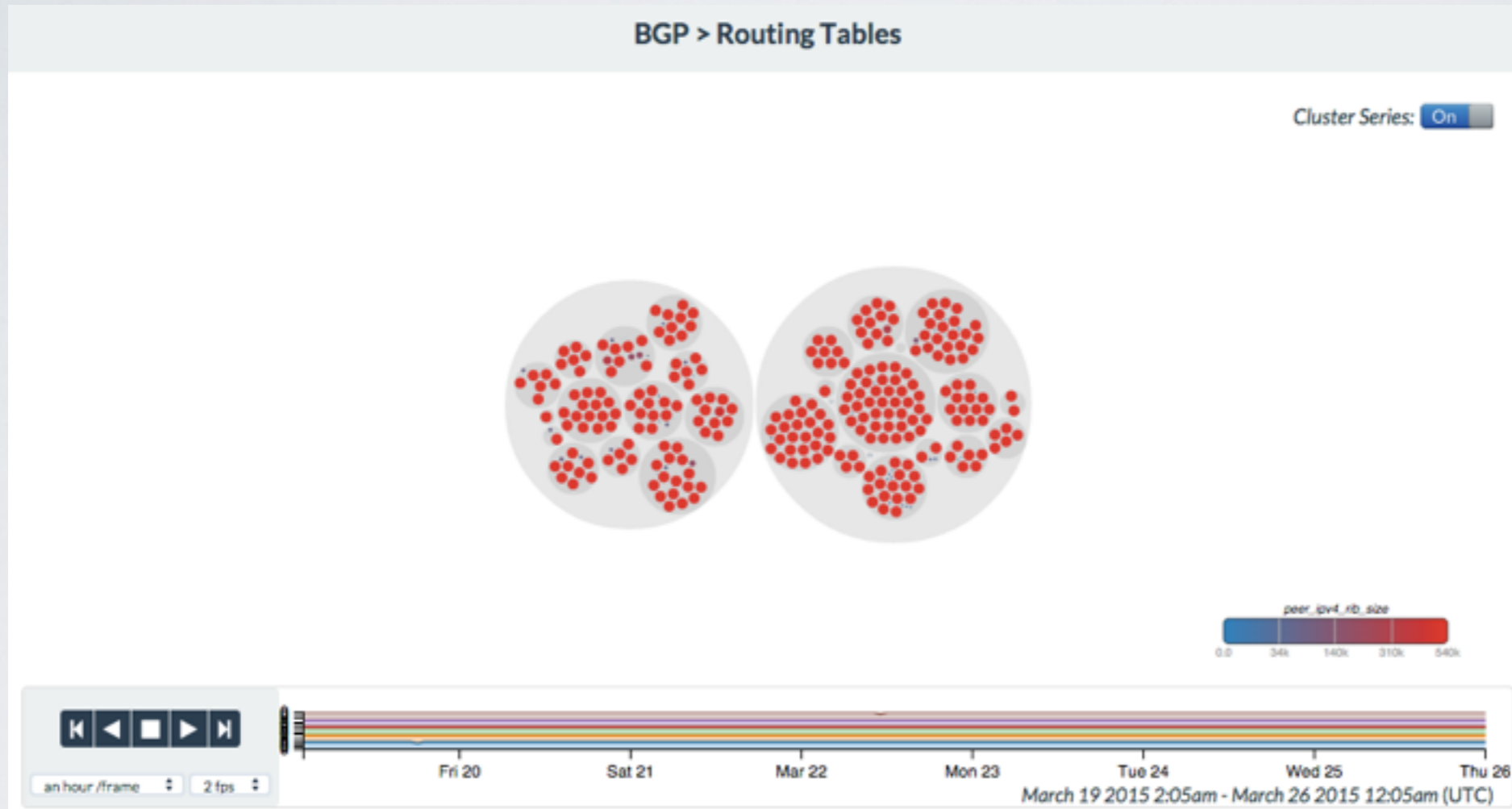
- Enables **large-scale realtime BGP analysis**
- Stacked modular framework
- To monitor for **outages** and **hijacks** we run ~30 instances of BGPCorsaro in parallel
- data is filtered and aggregated
- creates a **global view of BGP** every minute



MONITORING..



..the measurement & monitoring infrastructures



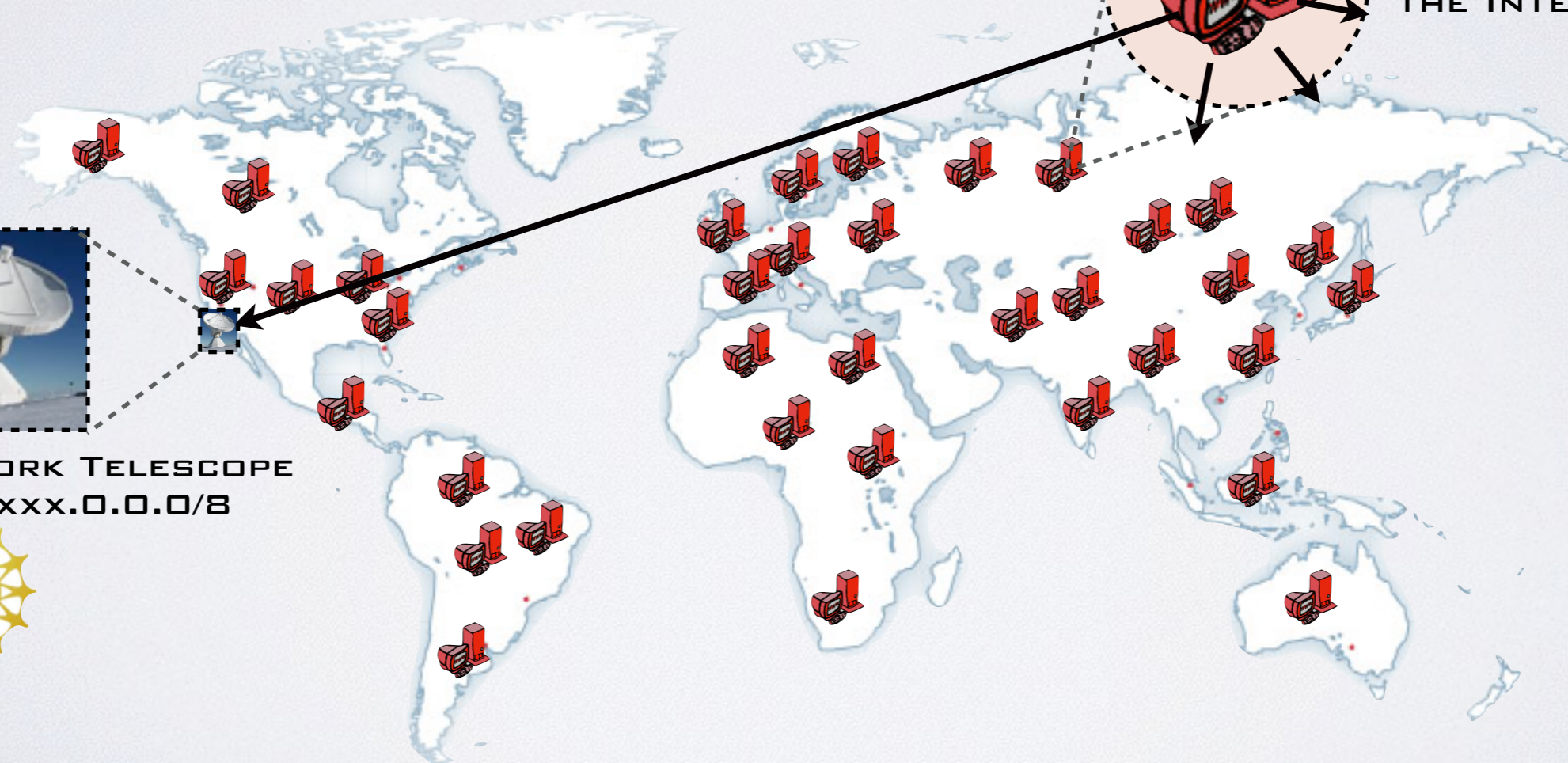
IBR

“Extracting benefit from harm..”

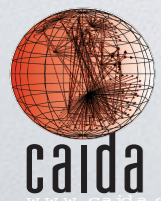


- Use *Internet Background Radiation (IBR)*, mostly generated by *malware-infected hosts* as a “signal”

INFECTED HOST
RANDOMLY SCANNING
THE INTERNET



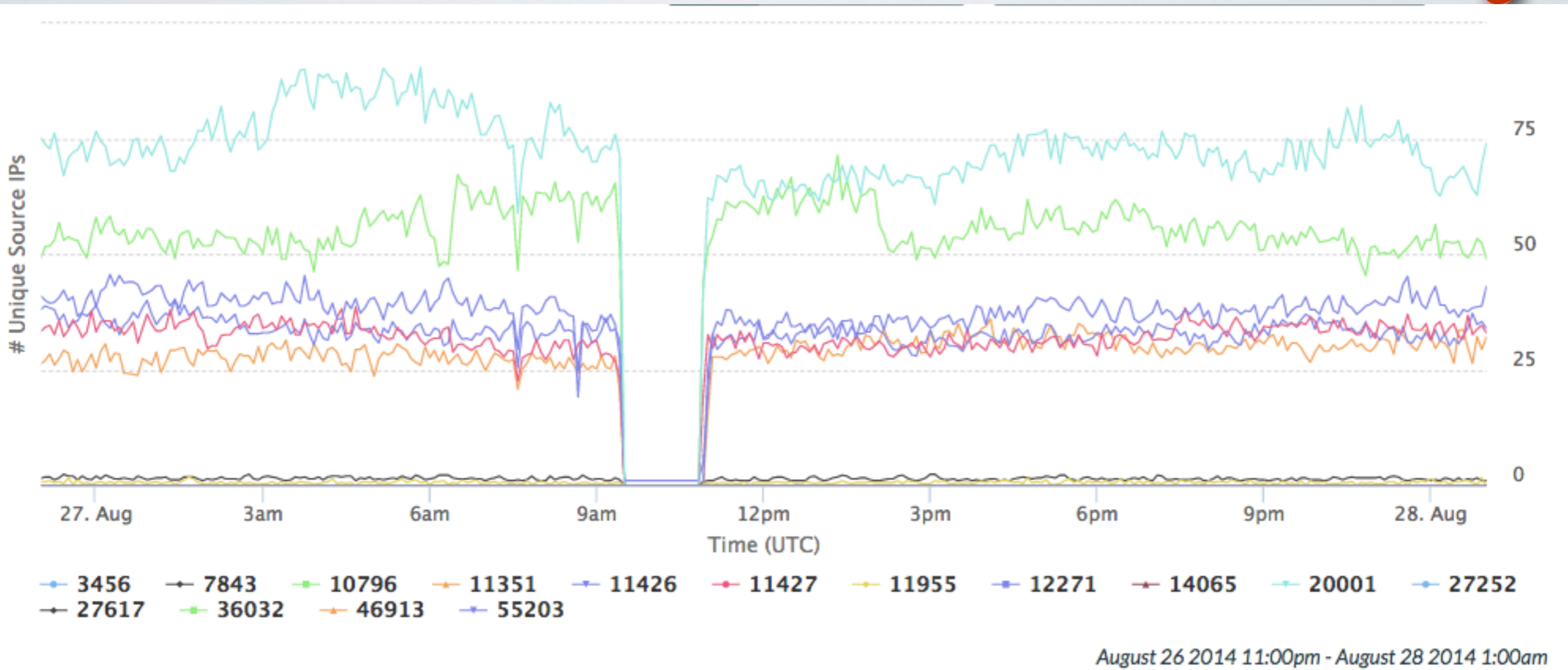
UCSD NETWORK TELESCOPE
DARKNET XXX.0.0.0/8



Center for Applied Internet Data Analysis
University of California San Diego

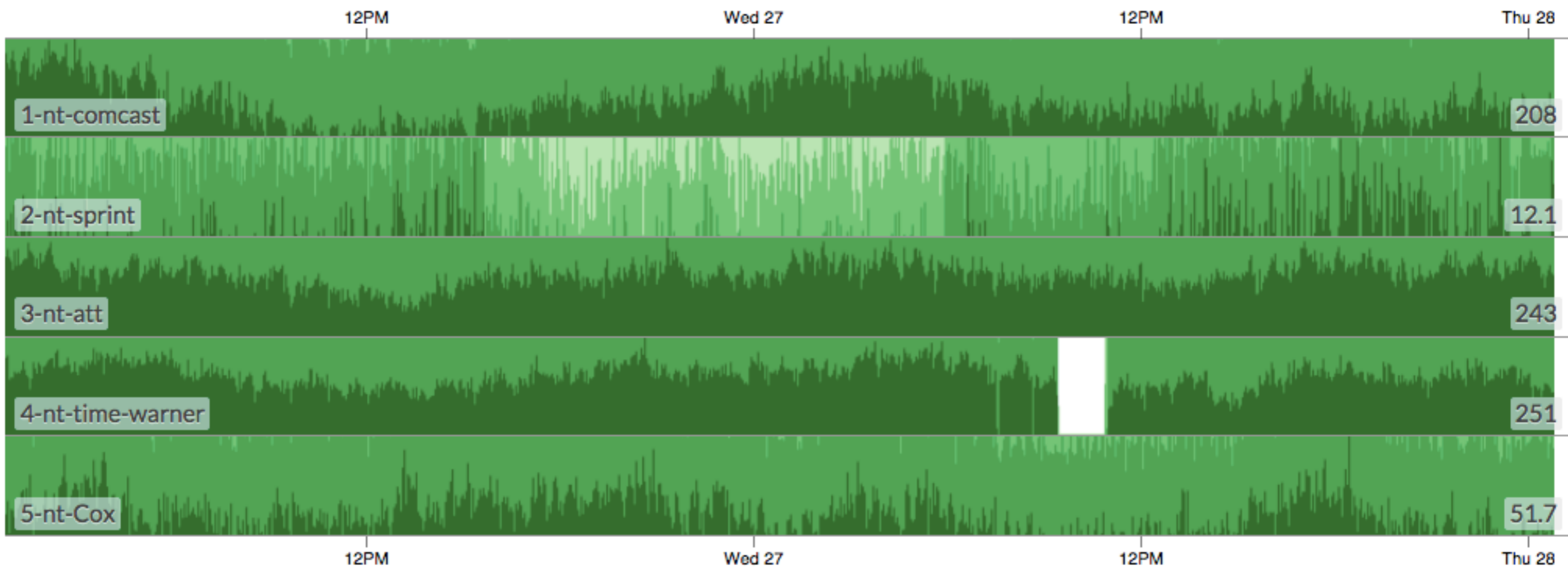
IBR

Time Warner Cable - 27th Aug 2014

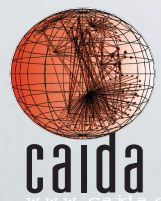


IBR

TWC outage: a look at few ISPs



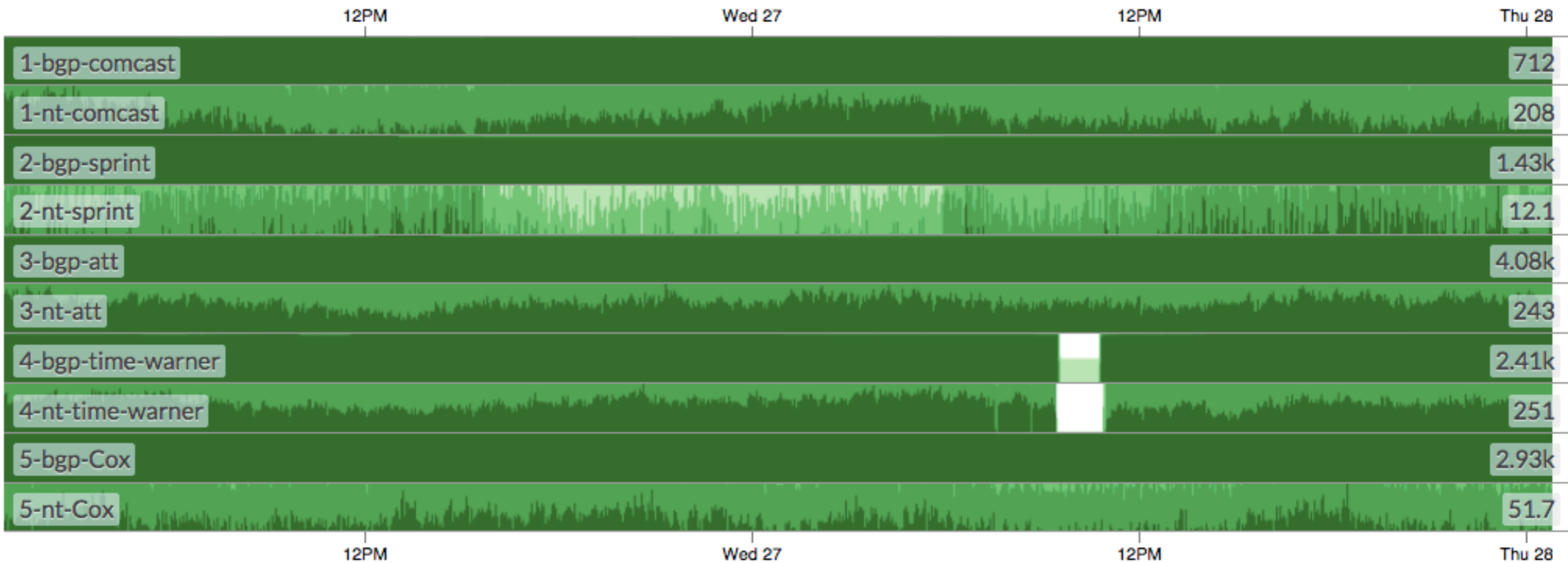
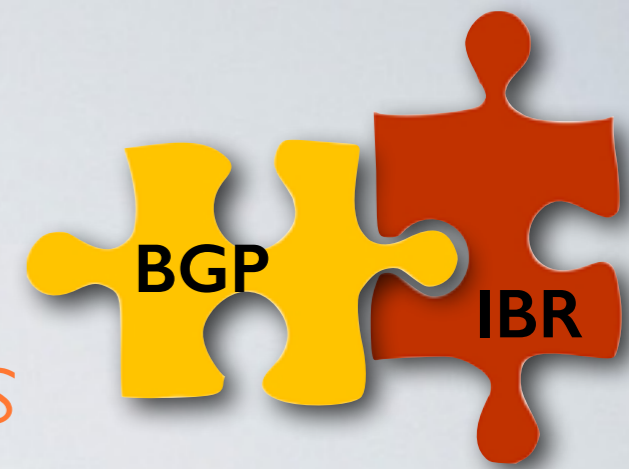
Series: 5 | # Points: 14400 | Data resolution: *minute*



Center for Applied Internet Data Analysis
University of California San Diego

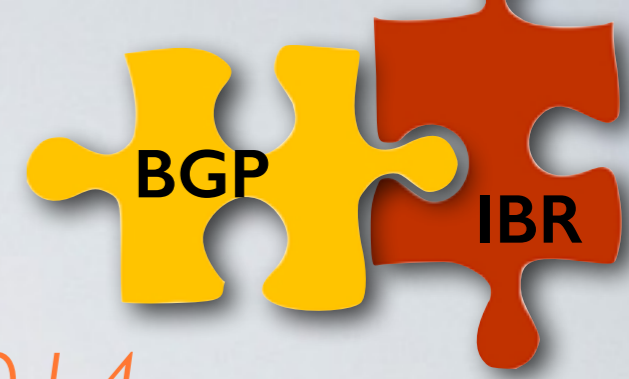
IBR + BGP

TWC outage: a look at few ISPs

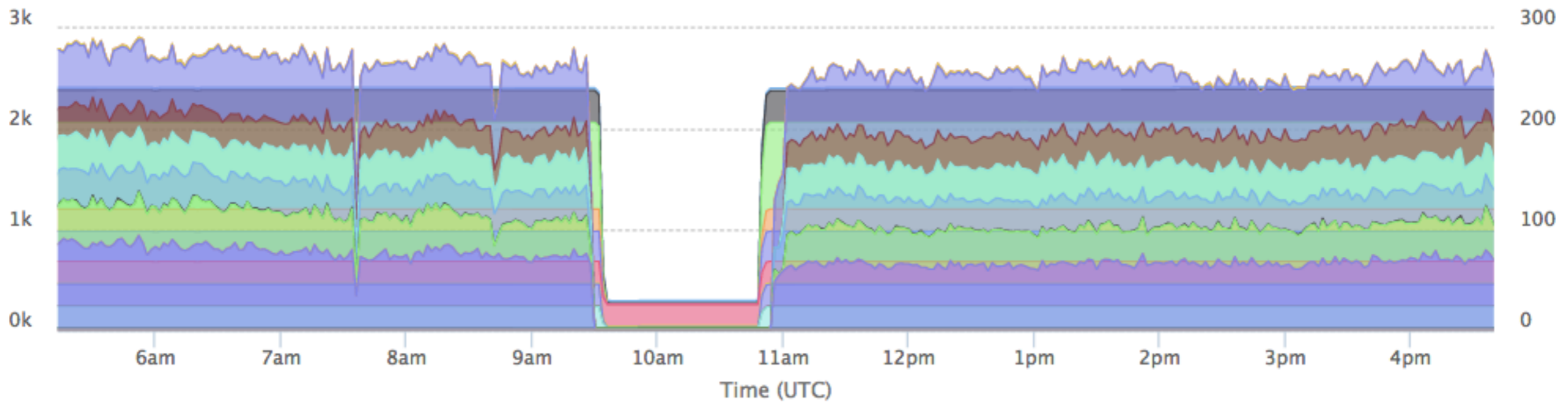


Series: 10 | # Points: 28800 | Data resolution: minute

IBR + BGP



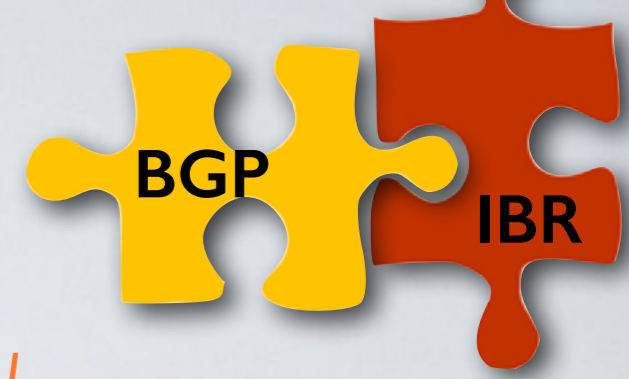
Time Warner Cable - 27th Aug 2014



- BGP > Global Prefix Visibility > Autonomous System Number (ASN) > 3456 > # IPv4 Prefixes [y1]
- BGP > Global Prefix Visibility > Autonomous System Number (ASN) > 7843 > # IPv4 Prefixes [y1]
- ▲ 1/23 ▼

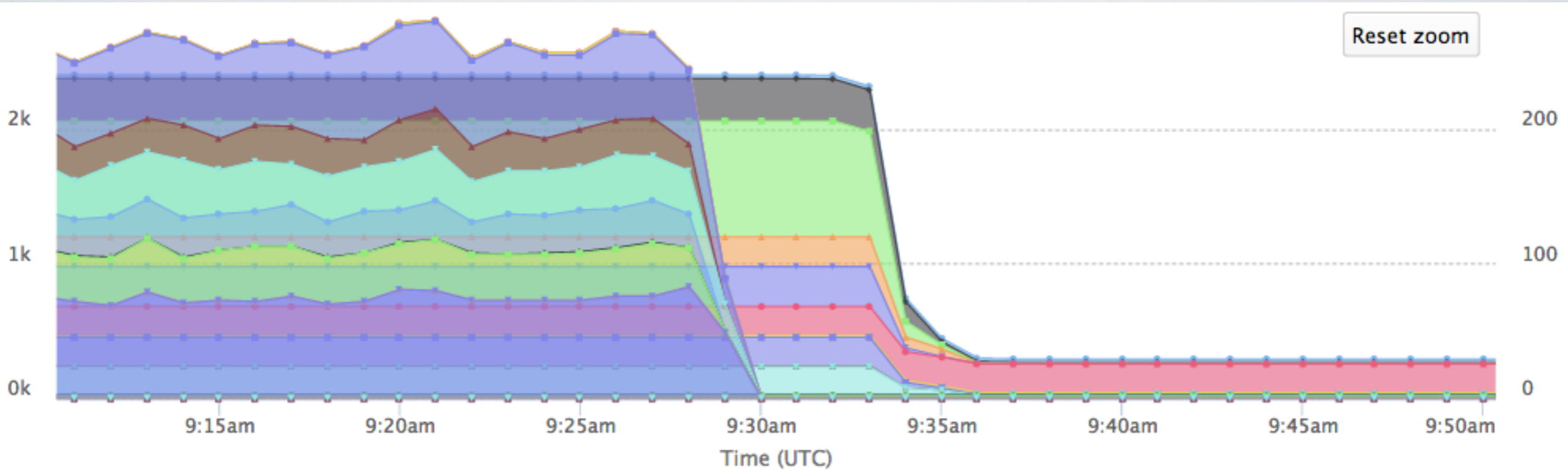
August 27 2014 5:13am - August 27 2014 4:39pm

IBR + BGP

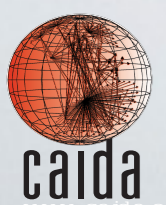


BGP convergence/propagation delay

Reset zoom



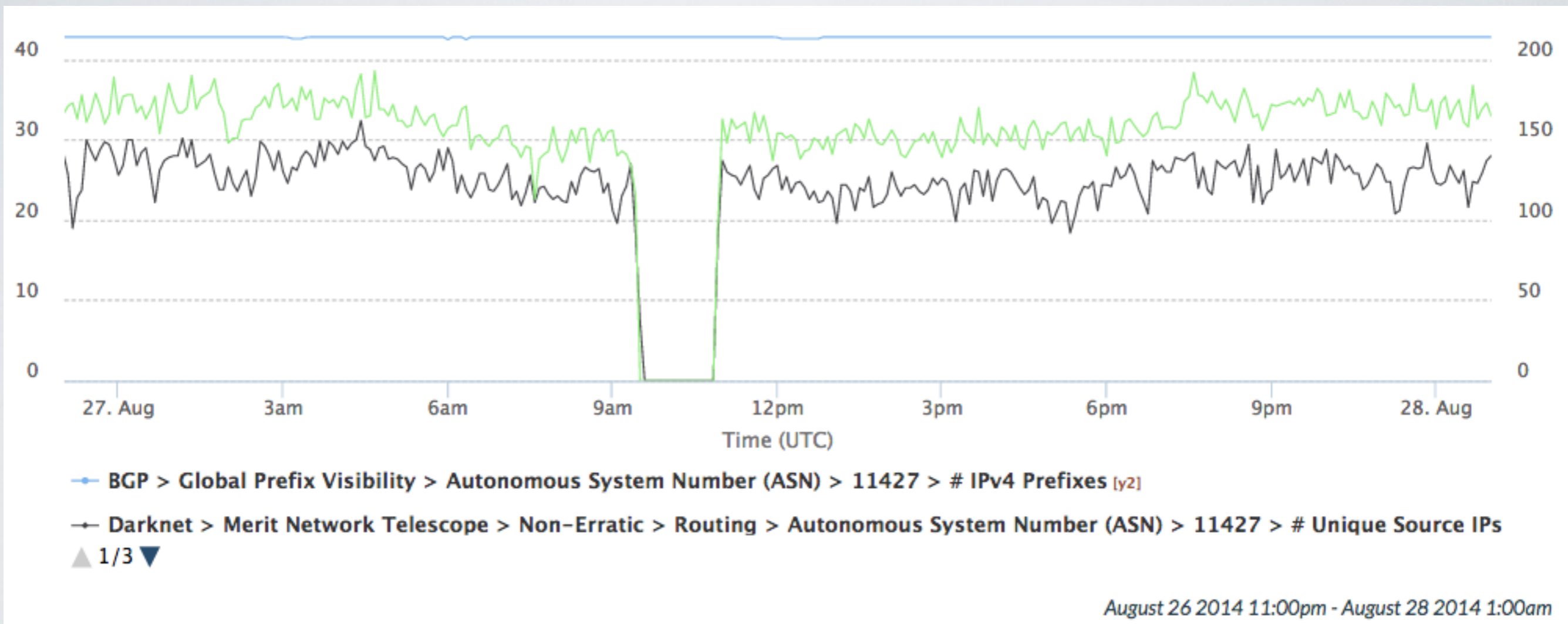
- BGP > Global Prefix Visibility > Autonomous System Number (ASN) > 3456 > # IPv4 Prefixes [y1]
- BGP > Global Prefix Visibility > Autonomous System Number (ASN) > 7843 > # IPv4 Prefixes [y1]
- ▲ 1/23 ▼



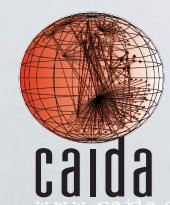
IBR



TWC outage: AS 11427 seen by 2 Darknets + BGP



*2nd Darknet provided by Merit Networks Inc.
Collaboration with Michalis Kallitsis
<http://www-personal.umich.edu/~mgkallit/>*

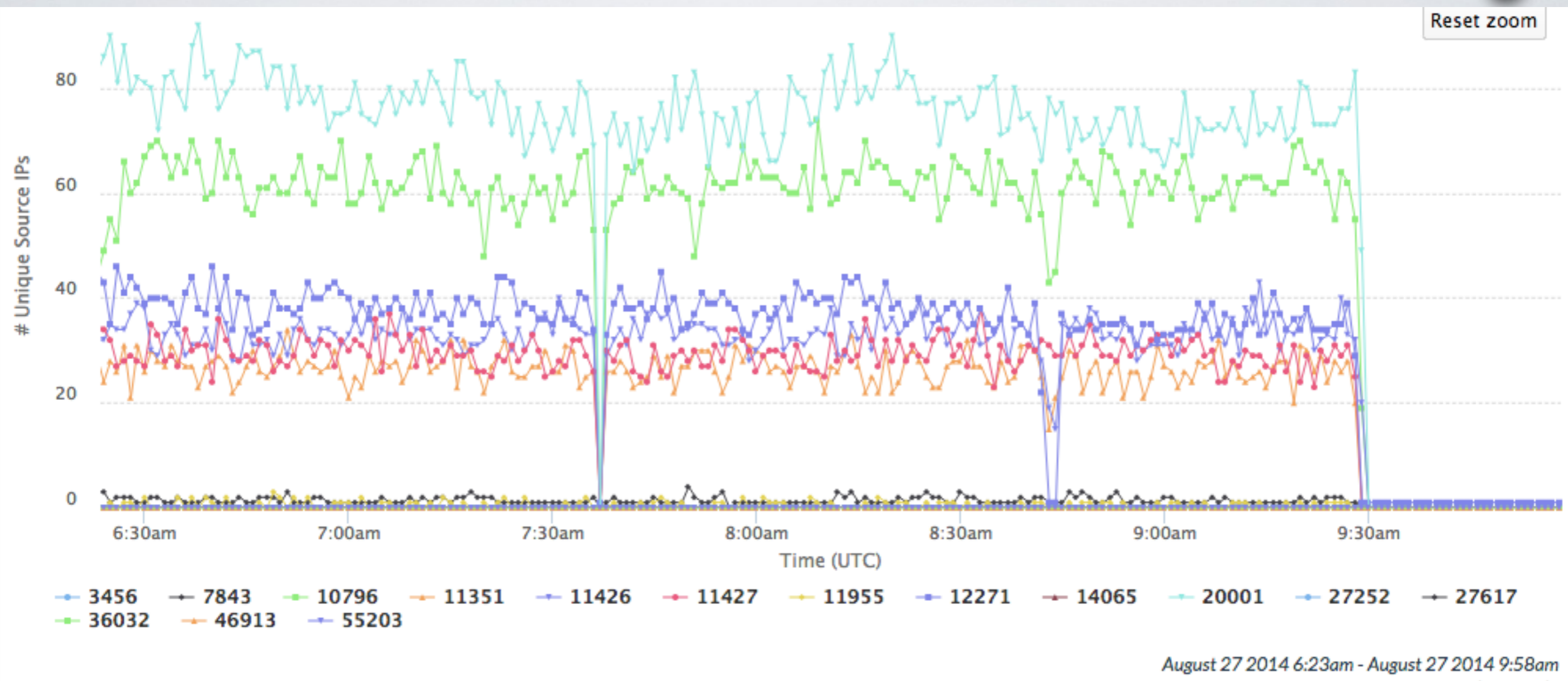


IBR

TWC outage: a couple of hours before

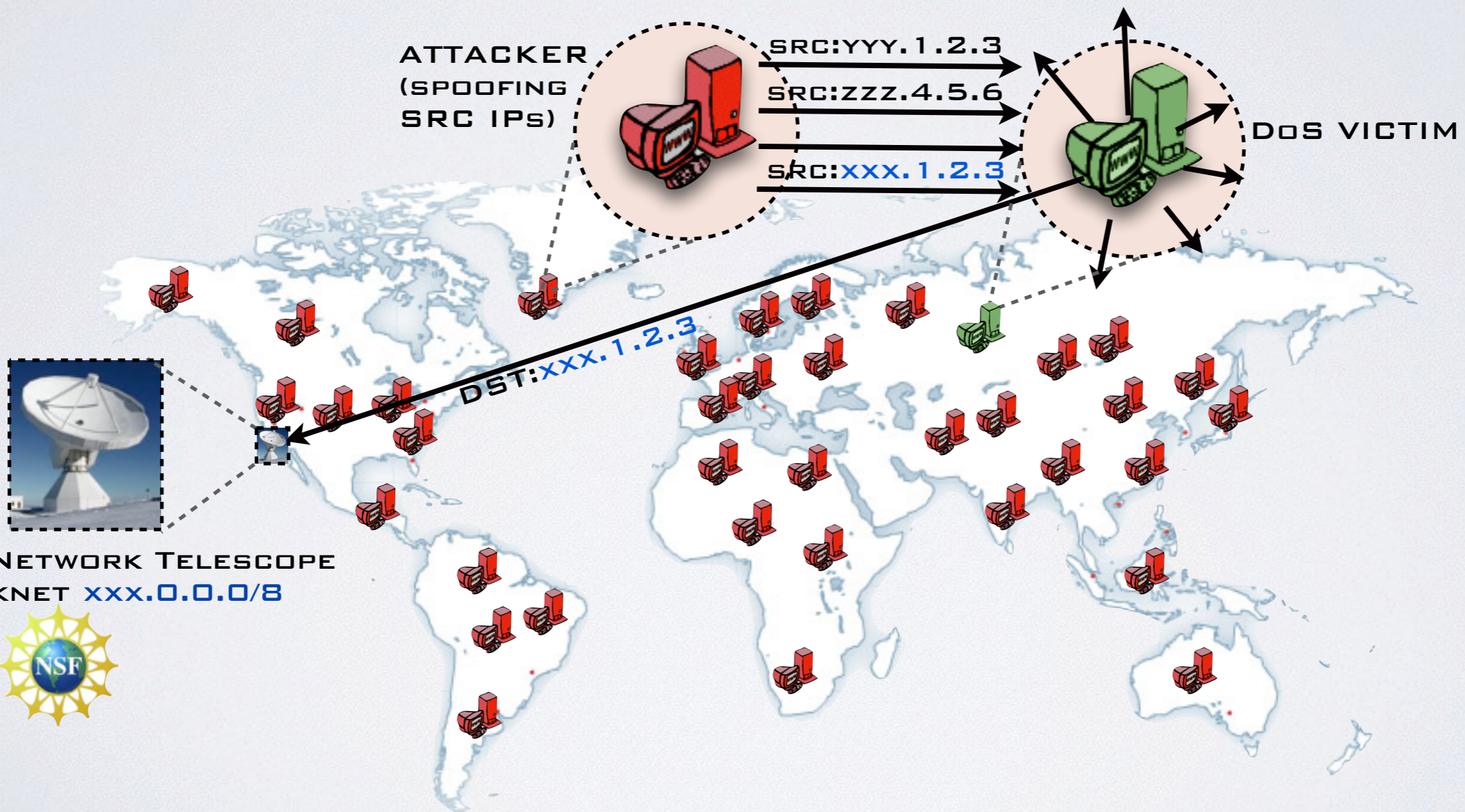


Reset zoom

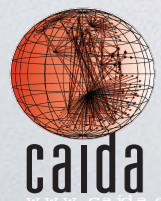


BACKSCATTER

e.g., SYN+ACK replies to spoofed SYNs



UCSD NETWORK TELESCOPE
DARKNET xxx.0.0.0/8



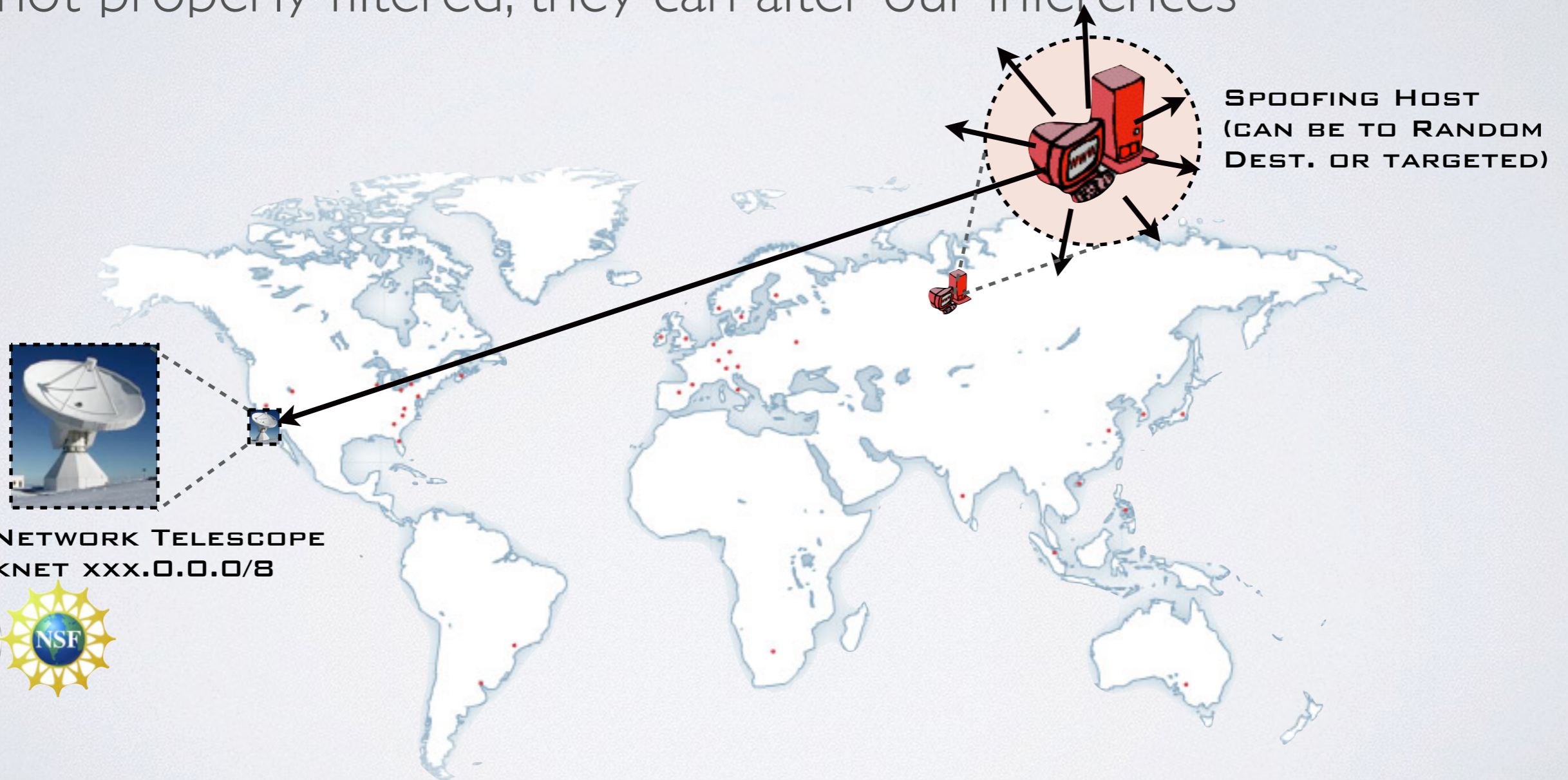
Center for Applied Internet Data Analysis
University of California San Diego

SPOOFED IBR

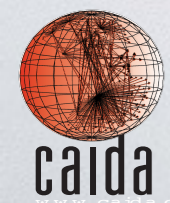
forged/corrupted packets



- IBR contains also packets with a spoofed source address. If not properly filtered, they can alter our inferences



UCSD NETWORK TELESCOPE
DARKNET xxx.0.0.0/8



Center for Applied Internet Data Analysis
University of California San Diego

IBR

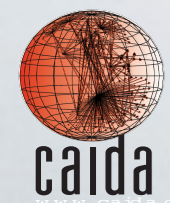
cleaning the signal



- We developed a methodology to monitor IBR and generate **filters** that automatically remove large-scale and bursty spoofing
- Small-scale spoofing does not constitute a problem
- Also, targeted spoofing attacks are difficult to implement:
 - each network has a “fingerprint” that the attacker would need to know
 - absence of traffic cannot be reproduced
 - we monitor more than one darknet
 - darknet address blocks are not widely known
- We also monitor IBR to identify large-scale coordinated activities that create noise in the signal and exclude such traffic
 - e.g., backscatter from spoofed scanning for open DNS resolvers

	Filter	Characterization
General	TTL > 200 and not ICMP	Large-scale/Bursty
	Least signif. byte src addr 0	Large-scale/Bursty
	Least signif. byte src addr 255	Large-scale/Consistent
	Protocol 0	Large-scale/Bursty
	Protocol 150	Large-scale/Consistent
	Same Src. and Dst. Addr.	Small-scale

*Dainotti et al. “Estimating Internet Address Space Usage through Passive Measurements”,
ACM SIGCOMM CCR 2014*



CORSARO

our packet processing framework

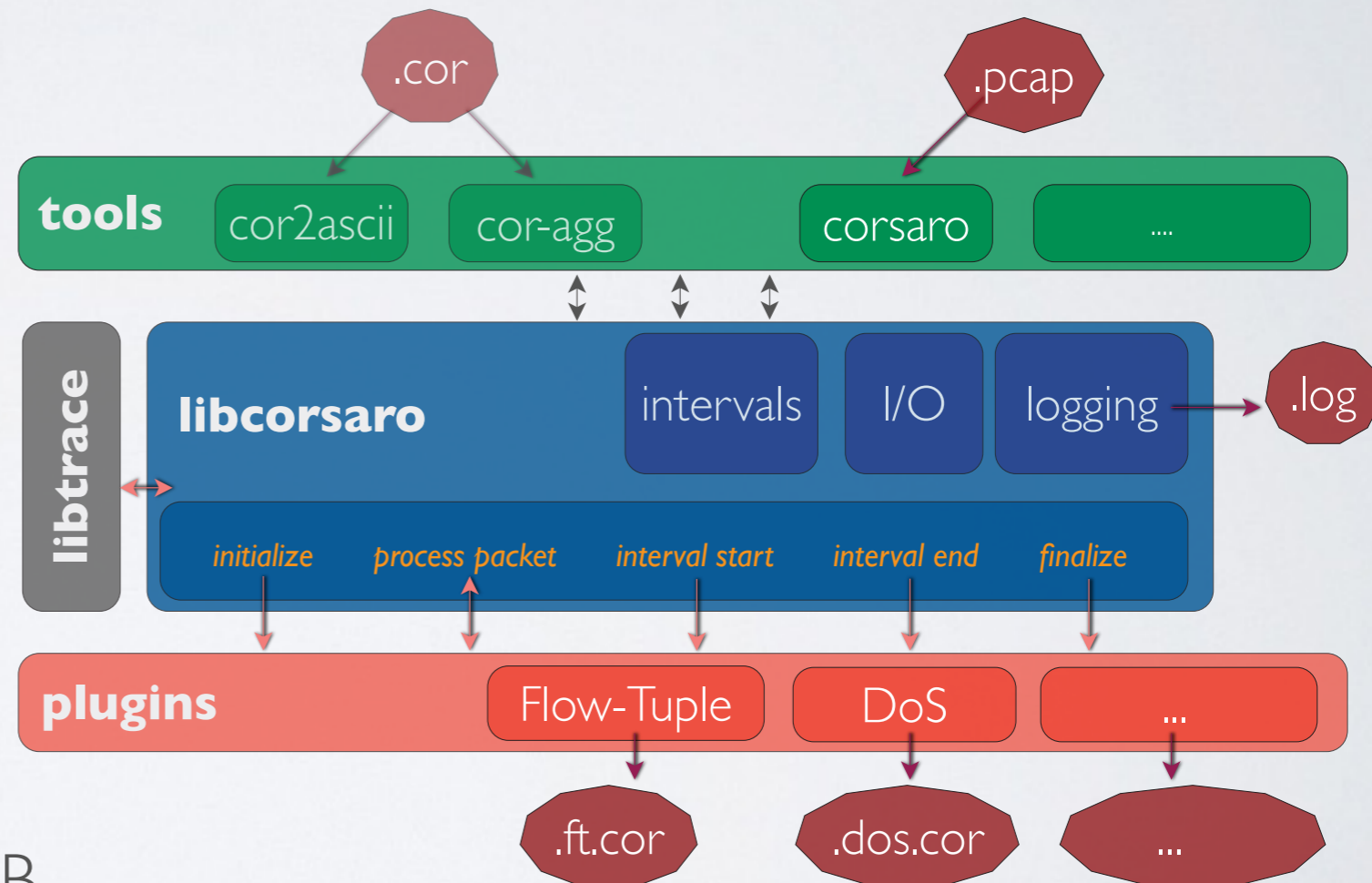


- Enables **large-scale near-realtime traffic analysis**

- Modular framework.

A pipeline of plugins:

- filter traffic (e.g., *spoofed*)
- classify it (e.g., *backscatter*)
- tag packets (e.g., *by geolocation*)
- aggregate tagged packets and extract time series data points at each interval (e.g., *1 min*)
- writes data in our high-performance time-series DB



<http://www.caida.org/tools/measurement/corsaro/>

ACTIVE PROBING

background info



- Collect measurements by injecting packets into the network
 - Ping
 - Sends “ECHO requests” packets to a destination host and receives back “ECHO replies”
 - **if:** the host is reachable, is up, is configured to reply to echo requests, etc...
 - measures reachability and Round Trip Time
 - Traceroute
 - Similar concept but tries to “ping” each hop on the path to the destination host through a careful use of the TTL IP header field
 - **if:** the hop is reachable, is up, is configured to reply, etc...
 - measures reachability, Round Trip Time for all (replying) hops, enables inference of IP-level path and AS-level path

ACTIVE PROBING

collaboration with ISI/USC



- John Heidemann's methodology: "Trinocular"
 - probing based on *pings* (ICMP echo requests)
 - includes an outage inference methodology based on Bayesian principles
 - /24 IPv4 blocks granularity
 - currently 3 vantage points
- Inferences and raw data shared through the DHS PREDICT project
 - we started working on importing historical data into Charthouse for analysis
- Planning to collaborate to integrate realtime feed with our system

*Quan et al. "Trinocular: Understanding Internet Reliability Through Adaptive Probing",
ACM SIGCOMM 2013*

ARK

Archipelago



- CAIDA active measurement infrastructure
 - supports ongoing 24/7 Internet-wide topology measurement as well as customized experiments
 - IPv4, IPv6, TCP, UDP, ICMP
 - active since 2007
- 107 vantage points (and growing)



- Planning to implement a variation of ISI's *Trinocular* exploiting the availability of more vantage points



<http://www.caida.org/projects/ark/>

PINGING IN THE RAIN



probing from PlanetLab

- Collaboration with Aaron Schulman (Stanford) and Neil Spring (Univ. Maryland)
 - Schulman, Spring, "Pinging in the Rain", ACM Internet Measurement Conference 2011
- Originally focused on how weather affects residential Internet connections in the US
- Probing from PlanetLab
 - 1342 nodes at 666 sites.
- We observe drops in % of hosts replying to pings



<http://www.cs.umd.edu/~schulman/thunderping.html>

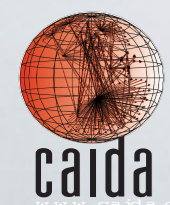
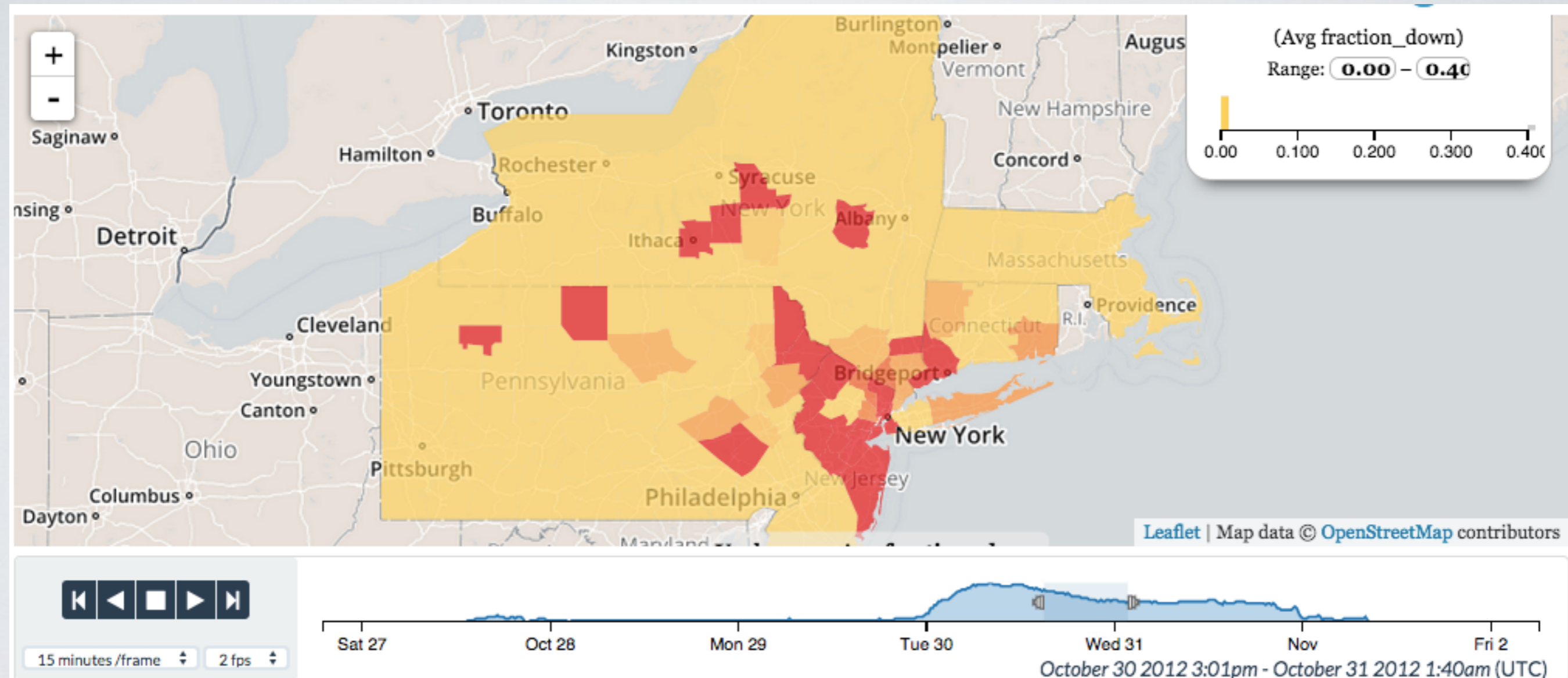
<https://www.planet-lab.org>



PINGING IN THE RAIN

ACTIVE
PROBING

probing from PlanetLab



Center for Applied Internet Data Analysis
University of California San Diego

ON DEMAND PROBING

ACTIVE
PROBING

Ark measurements on demand

- Ark offers (to authorized users only) an API for on demand probing
- helps with validation, allows finer time granularity, multiple vantage points, diagnostics with traceroutes, not only ICMP (e.g., TCP, UDP), ...

Create a Basic Measurement

Define a measurement to ping or traceroute a single target from a single source.

Destination

Enter an address/prefix/hostname:

Method

ping
 traceroute

Protocol

ICMP
 UDP
 TCP

Note: ICMP is the only supported protocol for ping.

Vantage Point

By Name | By Continent | **By Country** | By Org Type

Monitors with IPv6 have an asterisk in their name.

Submit Reset

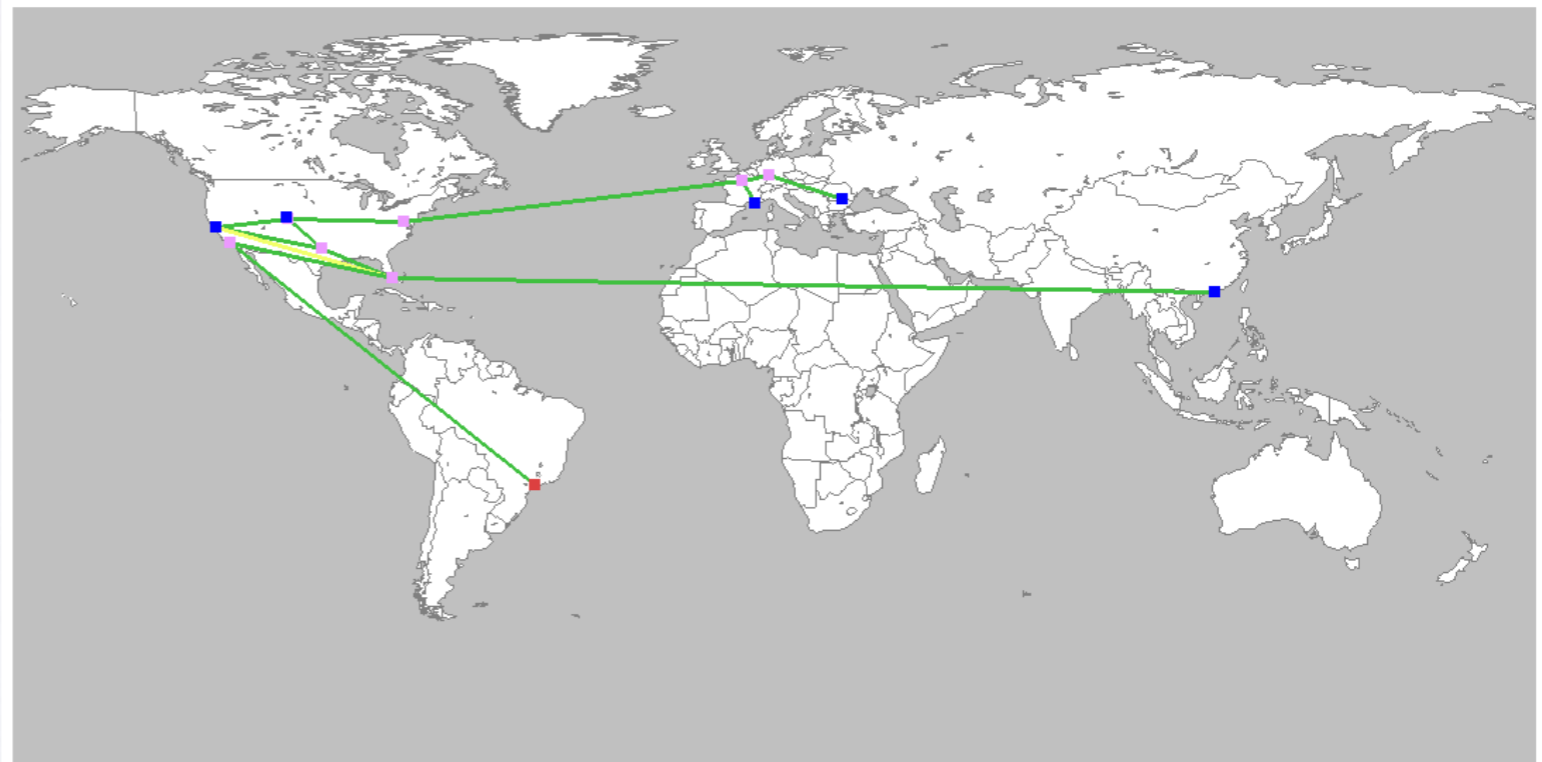
Home

Australia
mel-au
per-au *
syd-au *
Austria
vie-at *
Brazil
gig-br
sao-br
sao2-br
Canada
yow-ca *
yfo-ca
yyz-ca
Chile
scl-cl *
China
hkg-cn *
pek-cn
she-cn
Finland
hel-fi *

traceroute to sao2-br.ark.caida.org from commercial network (6) using ICMP

Traceroute Geo Map

Node Color Key: ■ Source ■ Intermediate ■ Destination
Link Color Key: — Direct — Indirect

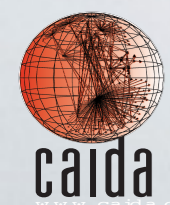


Other Views: [USA](#) | [South America](#) | [Europe](#) | [China](#) | [Japan](#)

TEAM

credits

Vasco Asturiano
Karyn Benson
KC Claffy
Alberto Dainotti
Marina Fomenkov
Young Hyun
Bradley Huffaker
Ken Keys
Alistair King
Ryan Koga
Alex Ma
Chiara Orsini
Josh Polterock
Cindy Wong



THANKS
questions?

