Exceptional service in the national interest

SAND2012-3966P

Sandia National Laboratories

Turning Down the Lights: Darknet Deployment Lessons Learned

Casey Deccio

DUST 2012 - 1st International Workshop on
Darkspace and UnSolicited Traffic Analysis
May 14, 2012
SDSC, UCSD, San Diego, CA

U.S. DEPARTMENT OF ENERGY | NNSA

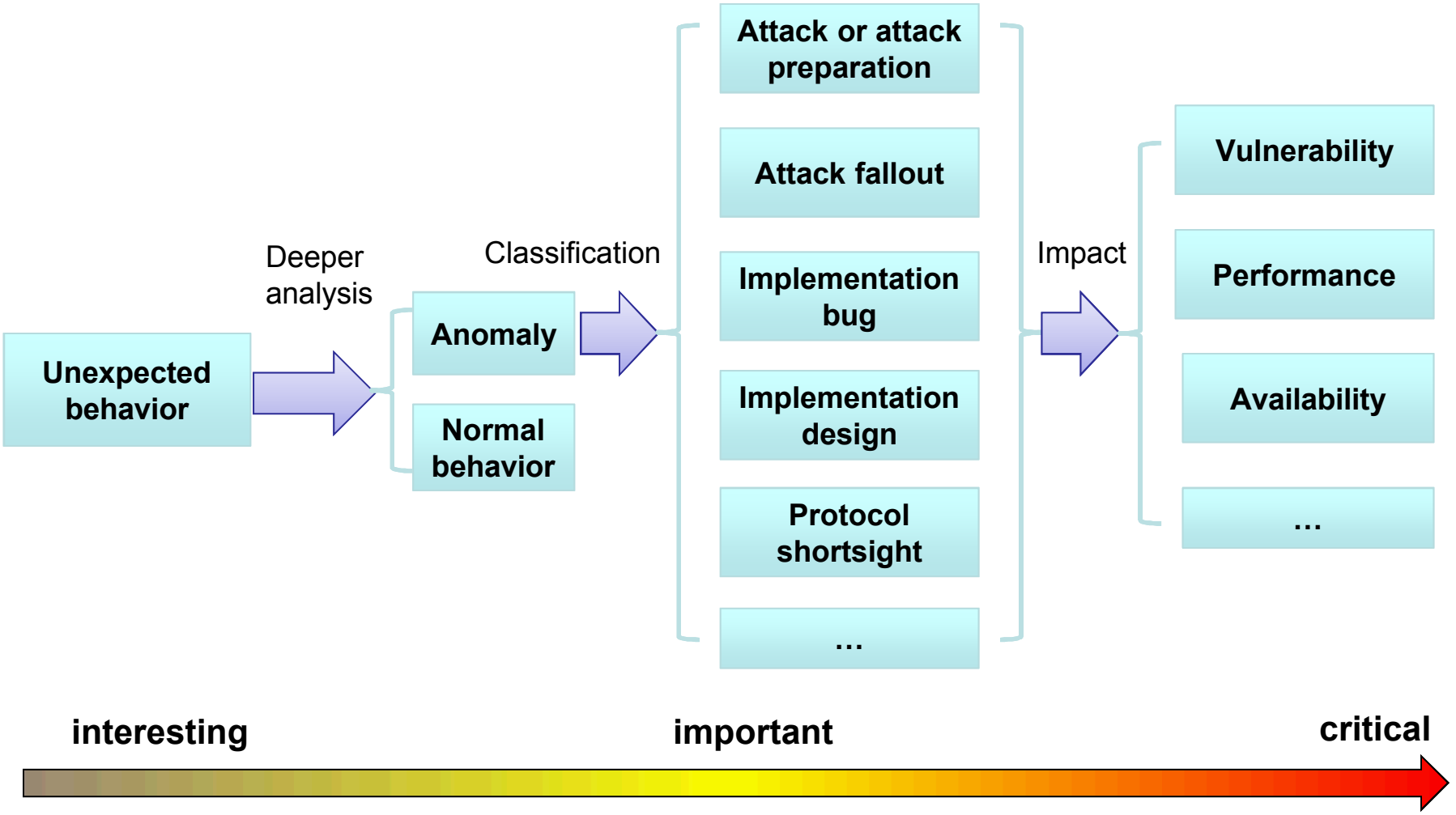
Sandia National Laboratories is a multi-program laboratory managed and operated by Sandia Corporation, a wholly owned subsidiary of Lockheed Martin Corporation, for the U.S. Department of Energy's National Nuclear Security Administration under contract DE-AC04-94AL85000.

Objectives

Sandia National Laboratories

- Motivate the importance of anomaly analysis
- Describe experiences in deploying an IPv6 darknet collector
- Share preliminary findings in IPv6 darknet traffic analysis

Anomaly Analysis – Motivation



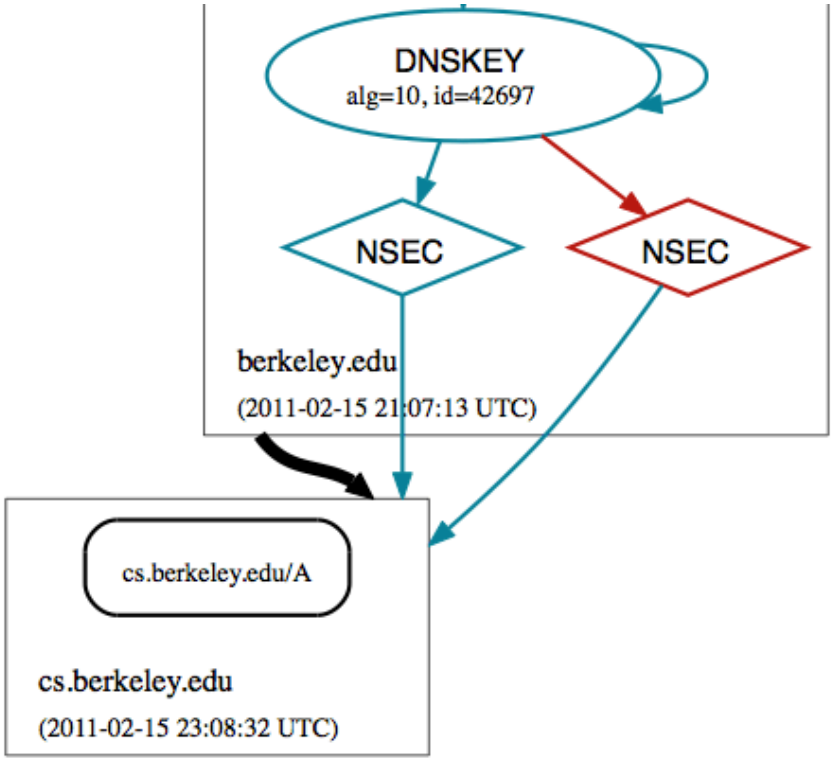
Anomaly Analysis Paradigms

Microanalysis
- Small scale
- Isolated environment
- Impact unknown

Macroanalysis
- Large scale
- Production environment
- Impact witnessed

Case 1: Bogus RRSIG for NSEC (DNSSEC)

- Feb 2011 – Sandia experienced validation errors for unsigned zone cs.berkeley.edu
- DNSViz showed two NSEC RRs returned, one with bogus RRSIG



Analysis available at: **http://dnsviz.net/d/cs.berkeley.edu/TVsHcQ/dnssec/**

Bogus RRSIG – Further Analysis

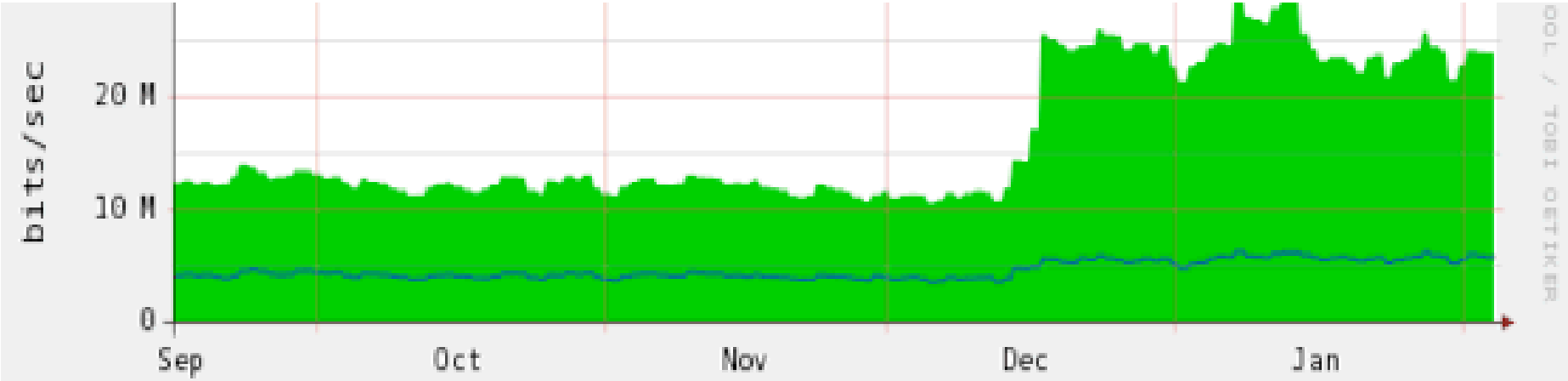
- Some servers serving different NSEC with same RRSIG
- Case of NSEC was not preserved during transfer after upgrade
- Fortunately, servers upgraded incrementally
- Impact: Jan 2011 – .br servers suffered same bug on half of their authoritative servers

Case mismatch: “edu” vs. “EDU”

Name	TTL	Type	Data	Status	192.35.225.133	192.5.4.1	128.223.32.35	128.32.136.14	128.32.136.6	128.32.136.3
cs.berkeley.edu		DS		Empty Answer	Y	Y	Y	Y	Y	Y
cs.berkeley.edu	300	NSEC	cs-kickstart.berkeley.edu. NS RRSIG NSEC	OK	Y	Y	Y		Y	
	300	RRSIG	NSEC 10 3 300 20110321231808 20110214231808 42697 berkeley.edu. cmstKEKH0hIUfa4lJIDodcNZUL6XNzlx A227/gVLObvVKP0ZFksQTNqAnALI4WJd oi4od/ubNm9zA5H+gI+ALoJR/wFihgog pVKK9tvSDSFkO1j65W5TfKrf38CGDm/S VW3yhW0suHt3S9ylY5iub5ERG6Wvh9PX BLo4QXojo7A=	OK	Y	Y	Y		Y	
cs.berkeley.edu	300	NSEC	cs-kickstart.Berkeley.EDU. NS RRSIG NSEC	OK				Y		Y
	300	RRSIG	NSEC 10 3 300 20110321231808 20110214231808 42697 berkeley.edu. cmstKEKH0hIUfa4lJIDodcNZUL6XNzlx A227/gVLObvVKP0ZFksQTNqAnALI4WJd oi4od/ubNm9zA5H+gI+ALoJR/wFihgog pVKK9tvSDSFkO1j65W5TfKrf38CGDm/S VW3yhW0suHt3S9ylY5iub5ERG6Wvh9PX BLo4QXojo7A=	BOG				Y		Y

Case 2: "Roll Over and Die?" (DNSSEC)

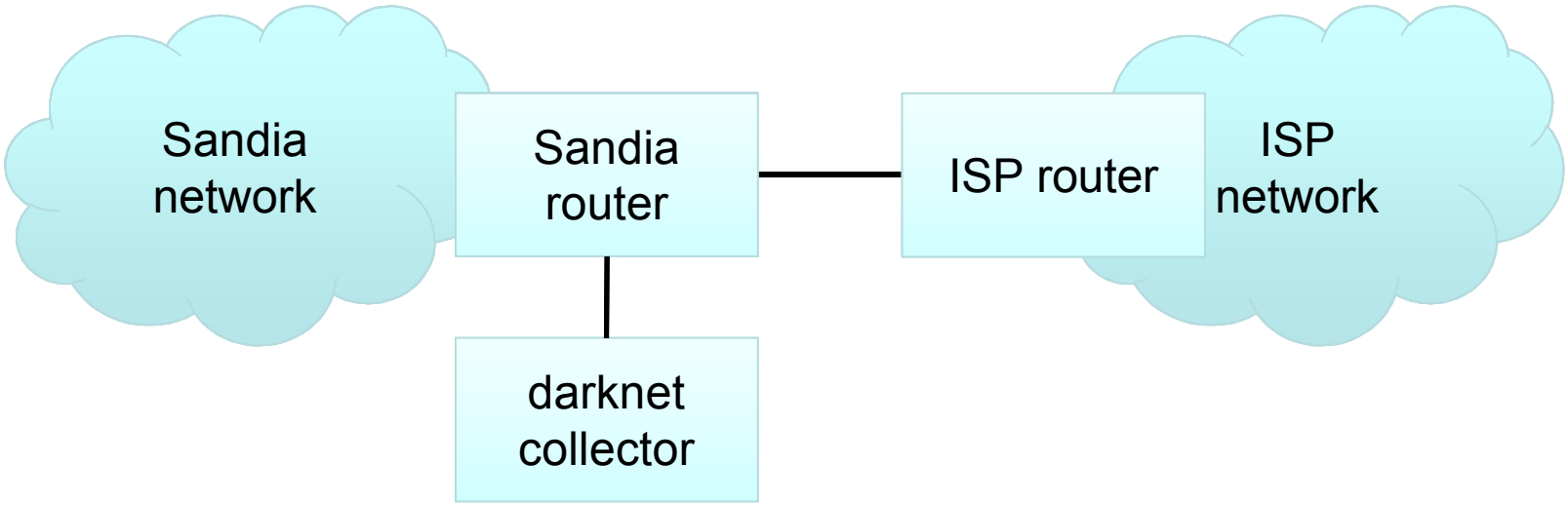
- Jan 2010 – Sandia experienced validation errors for 192.in-addr.arpa zone due to expired RRSIG
  - Sandia observed excessive queries from its validating resolvers
- Feb 2010 – Michaelson, et al., report on resolver behavior in the face of broken chains of trust
  - Graphed traffic for subdomain of in-addr.arpa after trust anchors in Fedora distribution became stale



Full analysis available at: **http://www.potaroo.net/ispcol/2010-02/rollover.html**

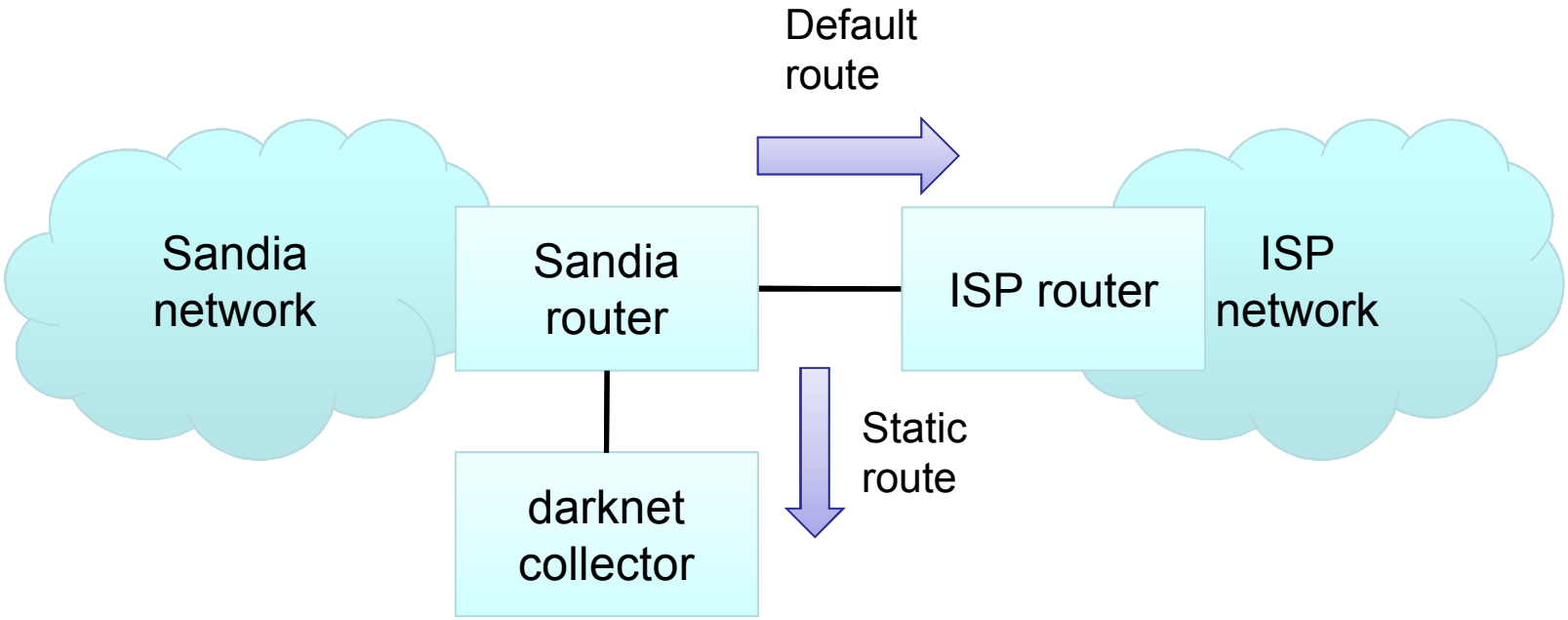
2400::/12

- 2400::/12 – largely unallocated IPv6 prefix in APNIC region
- Geoff Huston (APNIC) has presented previous analyses from traffic routed to the darknet
- APNIC graciously allowed Sandia to host the collector and announce the route
- Sandia's announcement of 2400::/12 began April 24, 2012



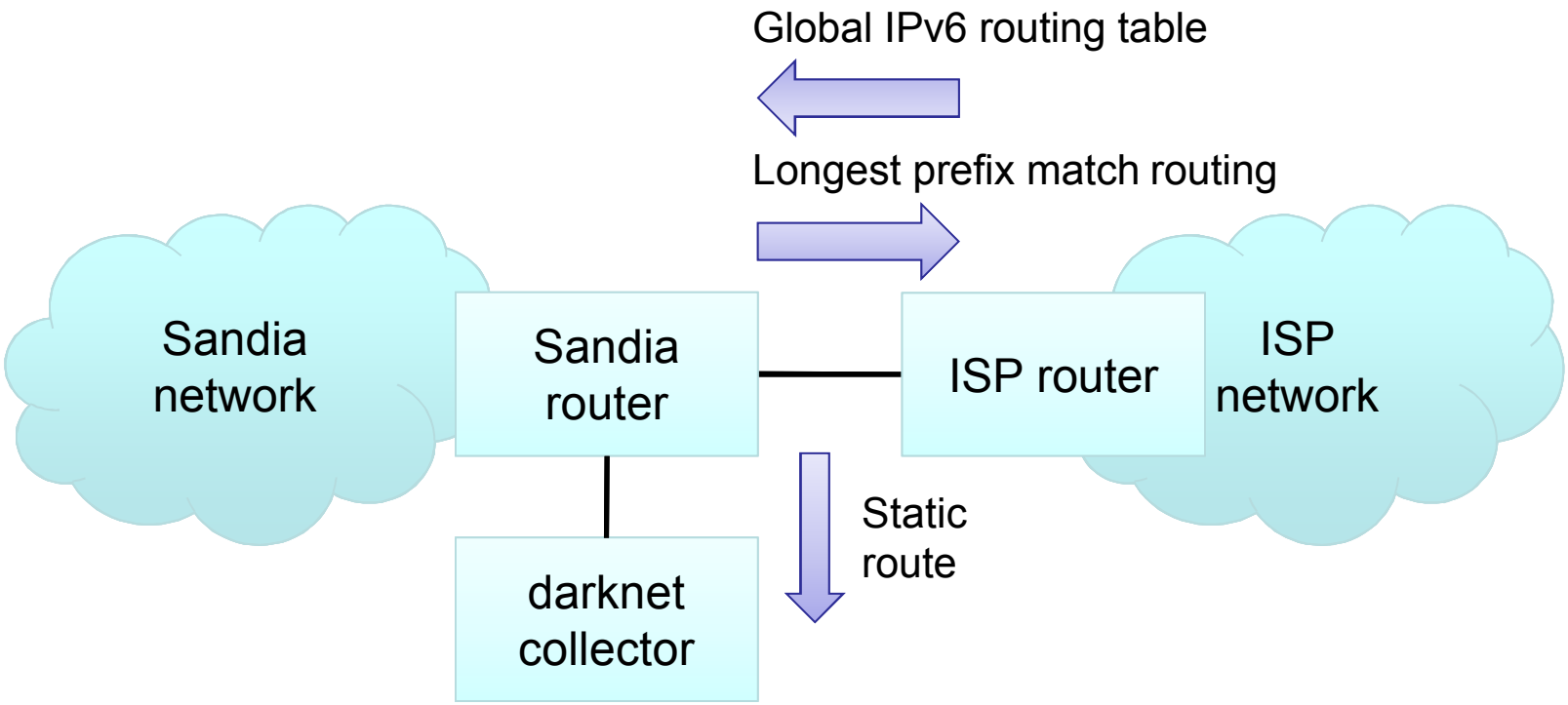
Darknet Routing – Take 1

- Sandia is a stub ASN with a default route
- When we added the static route for 2400::/12, we observed a lot of traffic
- …unfortunately much of it was legitimate traffic for allocated address space



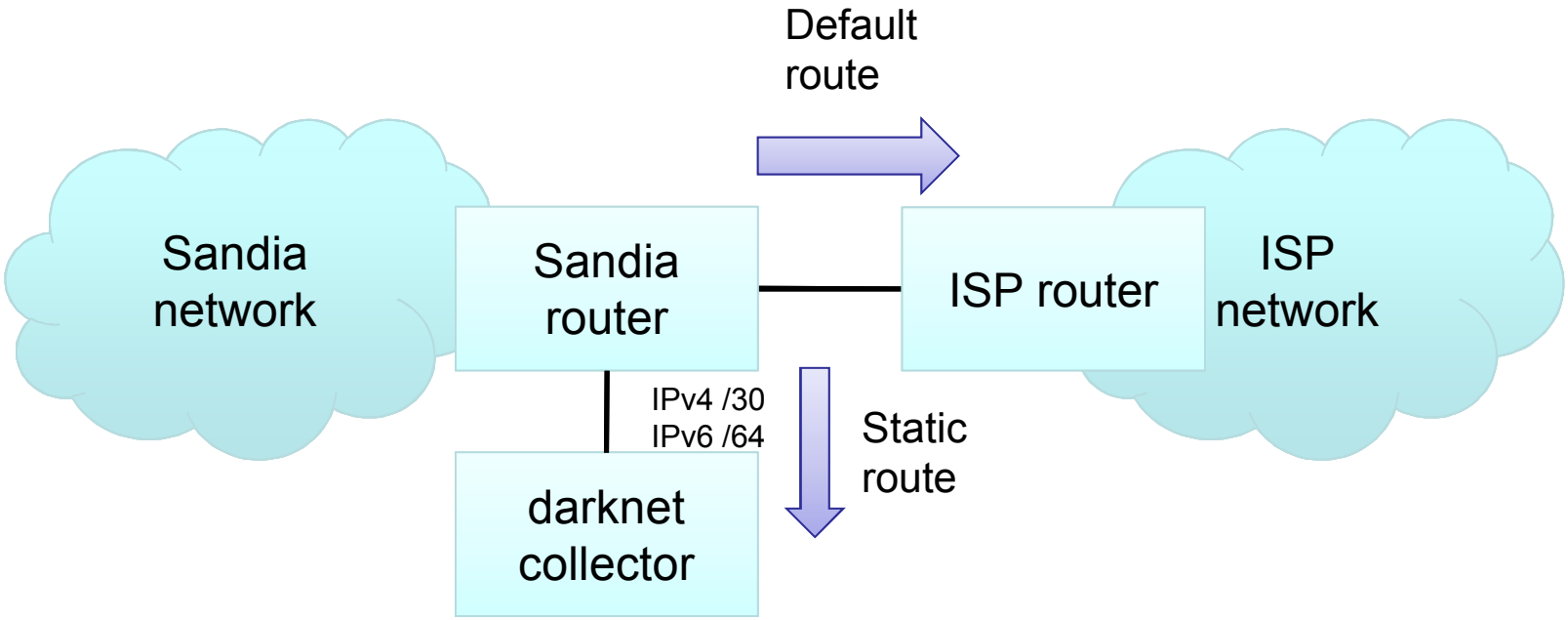
Darknet Routing – Take 2

- Router pulls down global IPv6 routing table
- Traffic routed via longest prefix match



Collector addressing

- Collector network has its own IPv4 (/30) and IPv6 (/64) address space (not in 2400::/12!)
- Static route points to collector IPv6 address as next hop

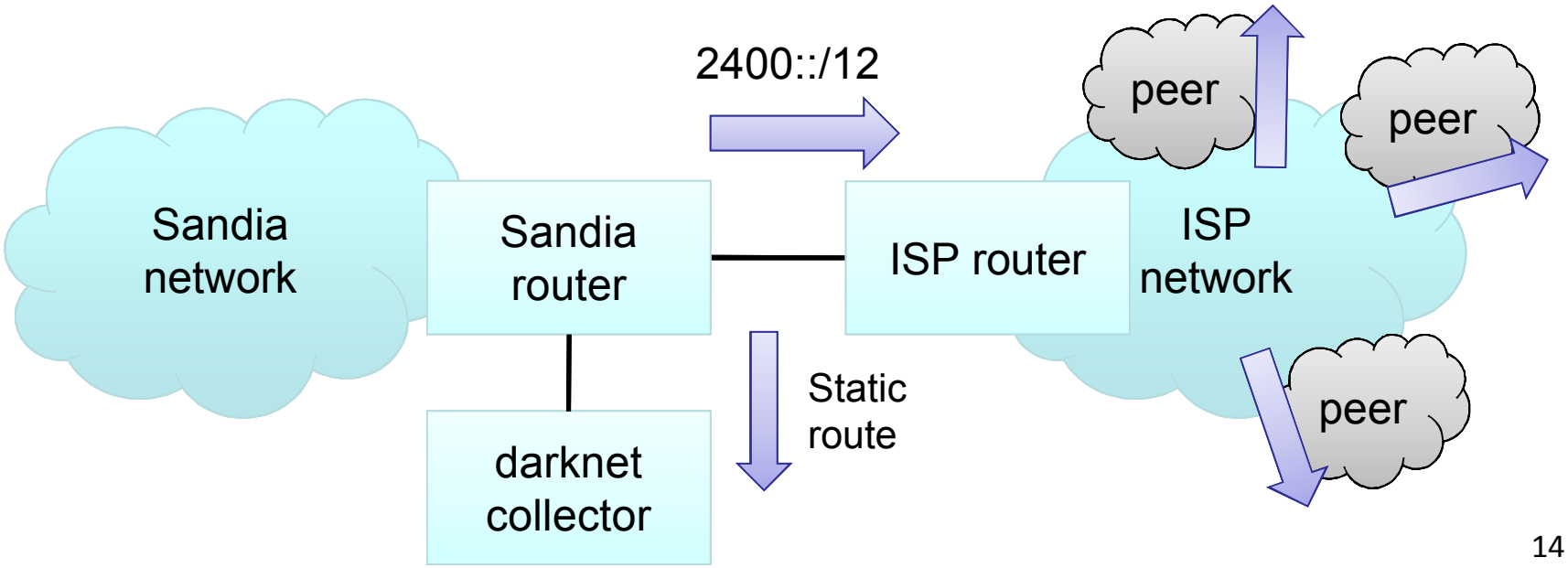


Traffic Collection

- ip6tables configured to drop any incoming traffic for 2400::/12 and any outgoing traffic with source 2400::/12
  - Mostly an extra measure to avoid unexpected responses from otherwise “dark” space
  - Rules might be softened in the future to interact with incoming TCP packets
- tcpdump as daemon:
  - /usr/sbin/tcpdump -i <interface> -s 0 -G <flush_interval> -z gzip \
    -w /path/to/files/2400_12-%Y-%m-%d-%H%M.pcap \
    net 2400::/1

2400::/12 Route Announcement

- Route announcement requires coordination between originating AS, ISP (if stub), and ISP peers.
- Administrative logistics took nearly two months!



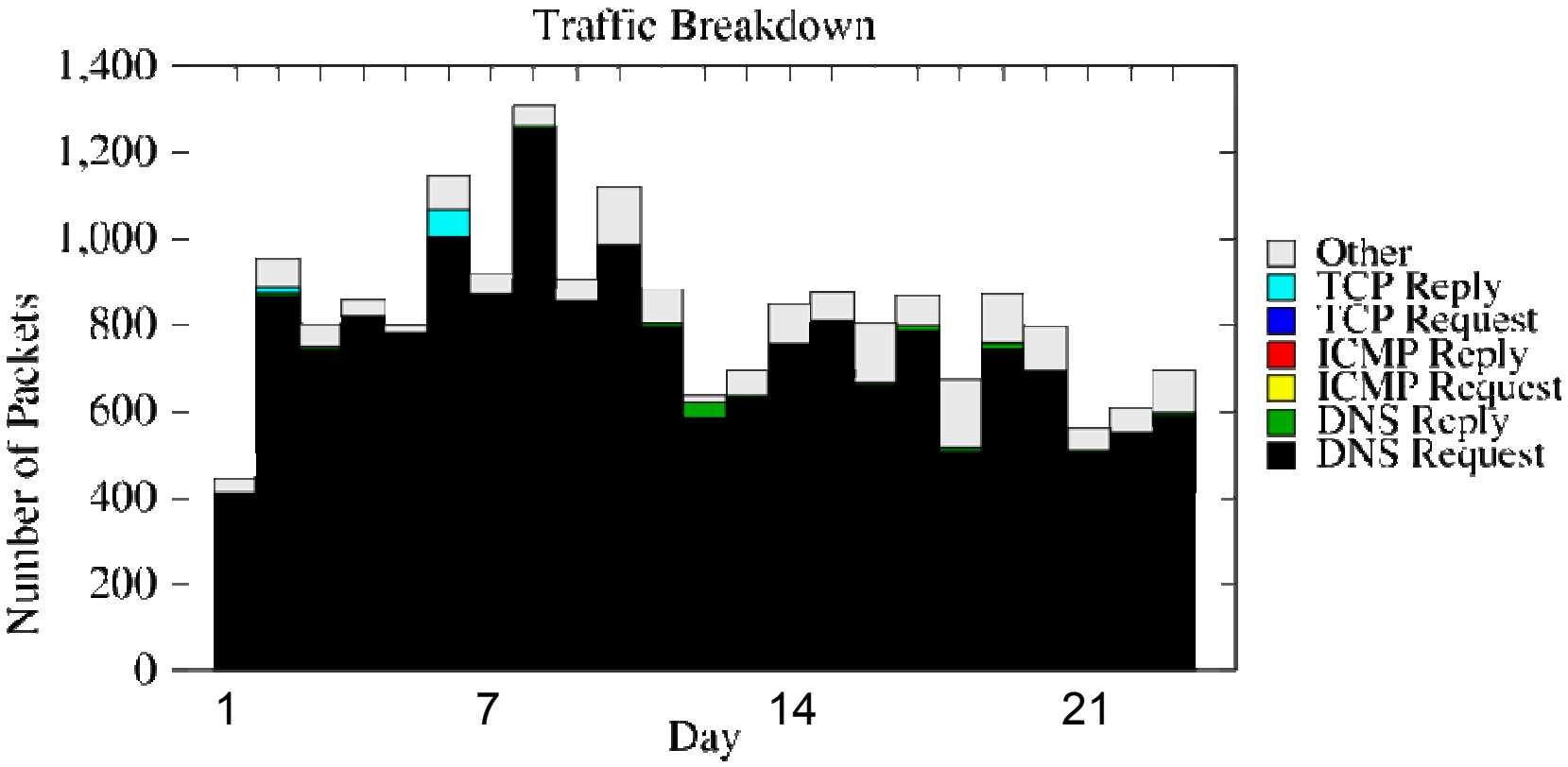
Analysis Overview and Terms

Sandia National Laboratories

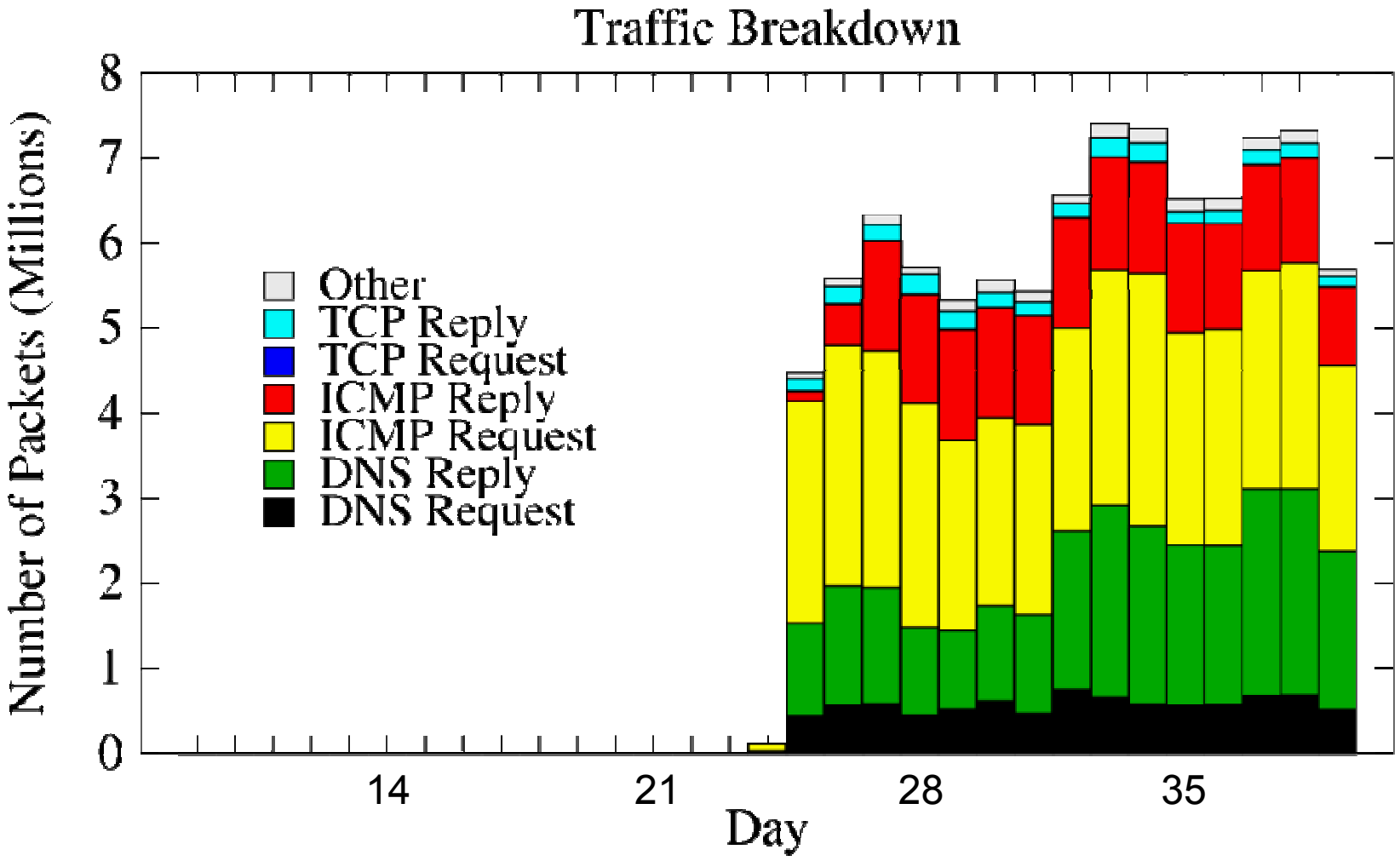
- Roughly six weeks of data
  - Four weeks prior to announcing route
  - Two weeks after announcing route

Term	Description	Possible Reason(s)
Request	- ICMPv6 echo request - TCP SYN - DNS query	Misconfigured server address; route announcement obsolete
Response	- ICMPv6 echo request - TCP SYN/ACK - DNS response	Corresponding requests sent from address with no advertised return route

Daily Darknet Traffic – First Weeks

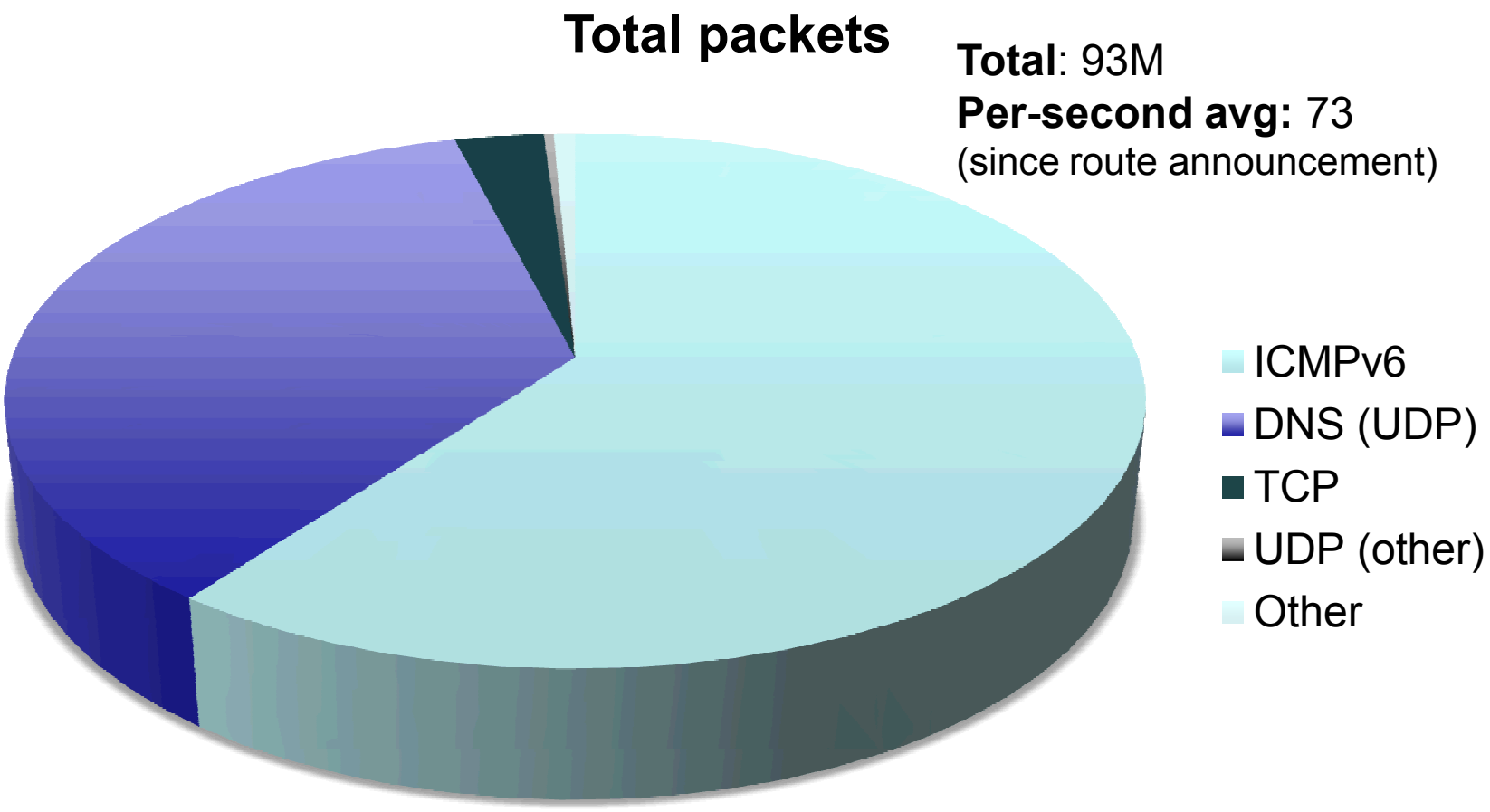


Daily Darknet Traffic – After Route Announcement



Traffic Breakdown

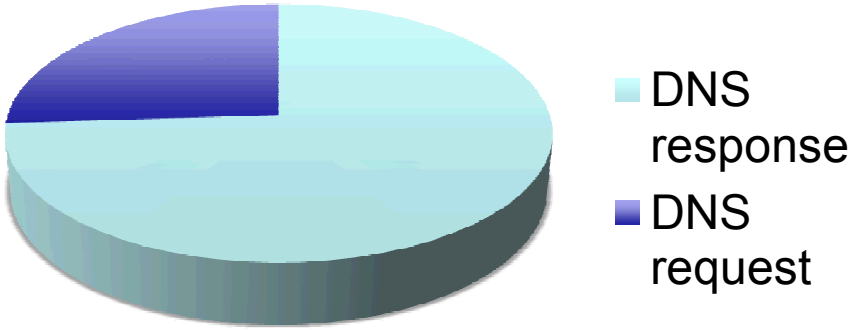
Sandia National Laboratories



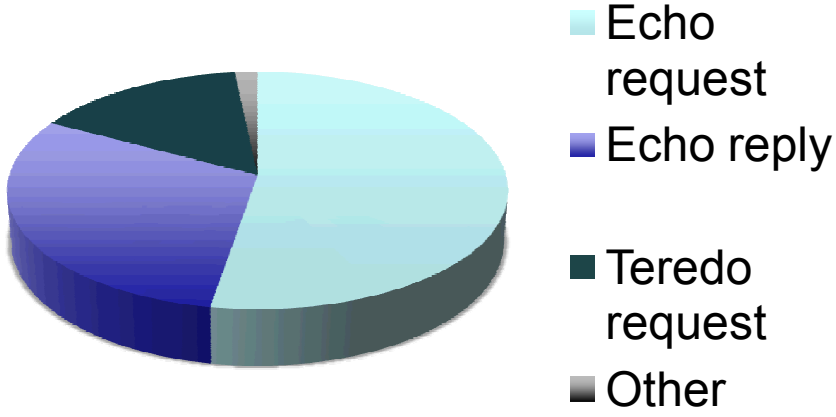
Traffic Breakdown

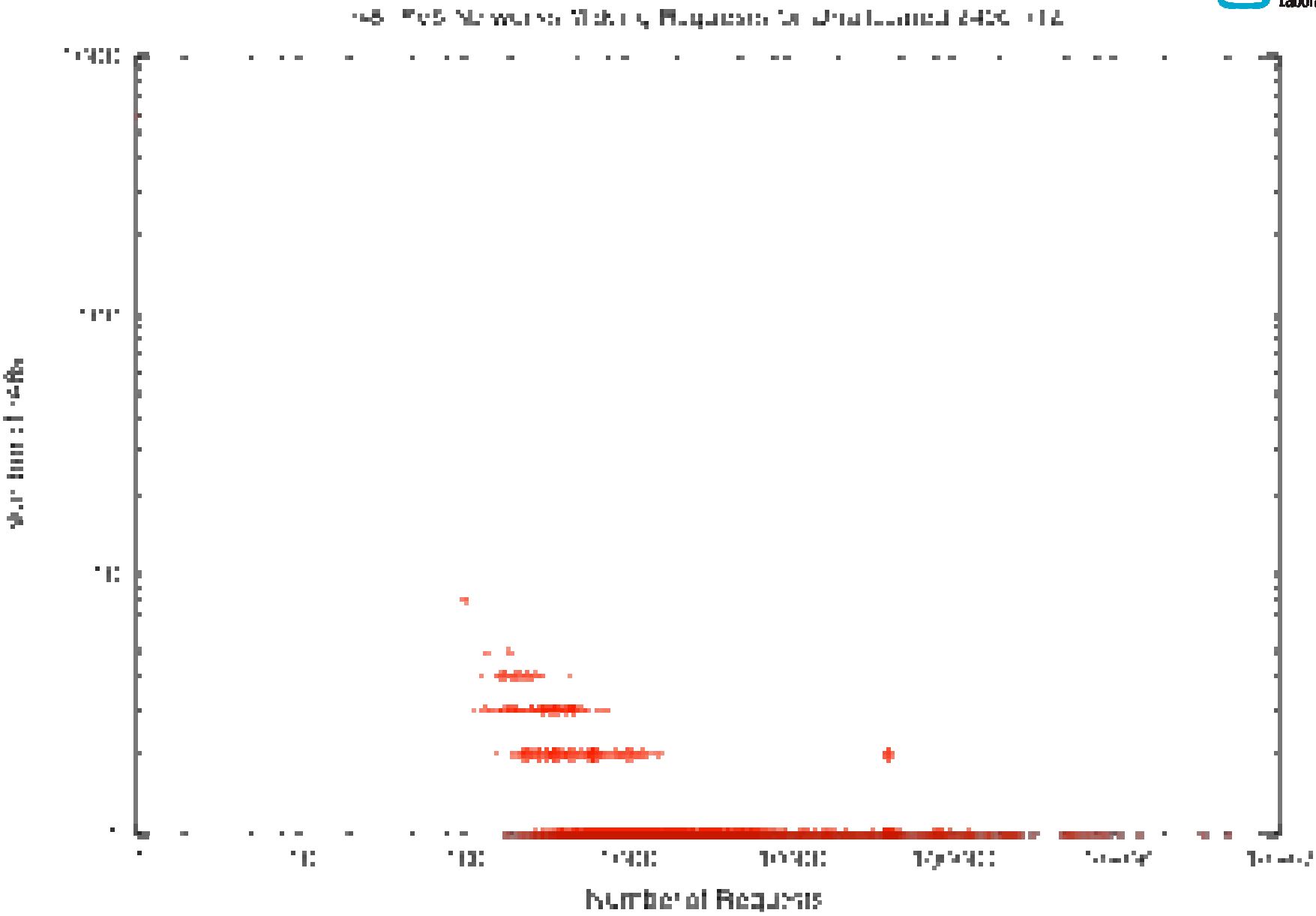
Sandia National Laboratories

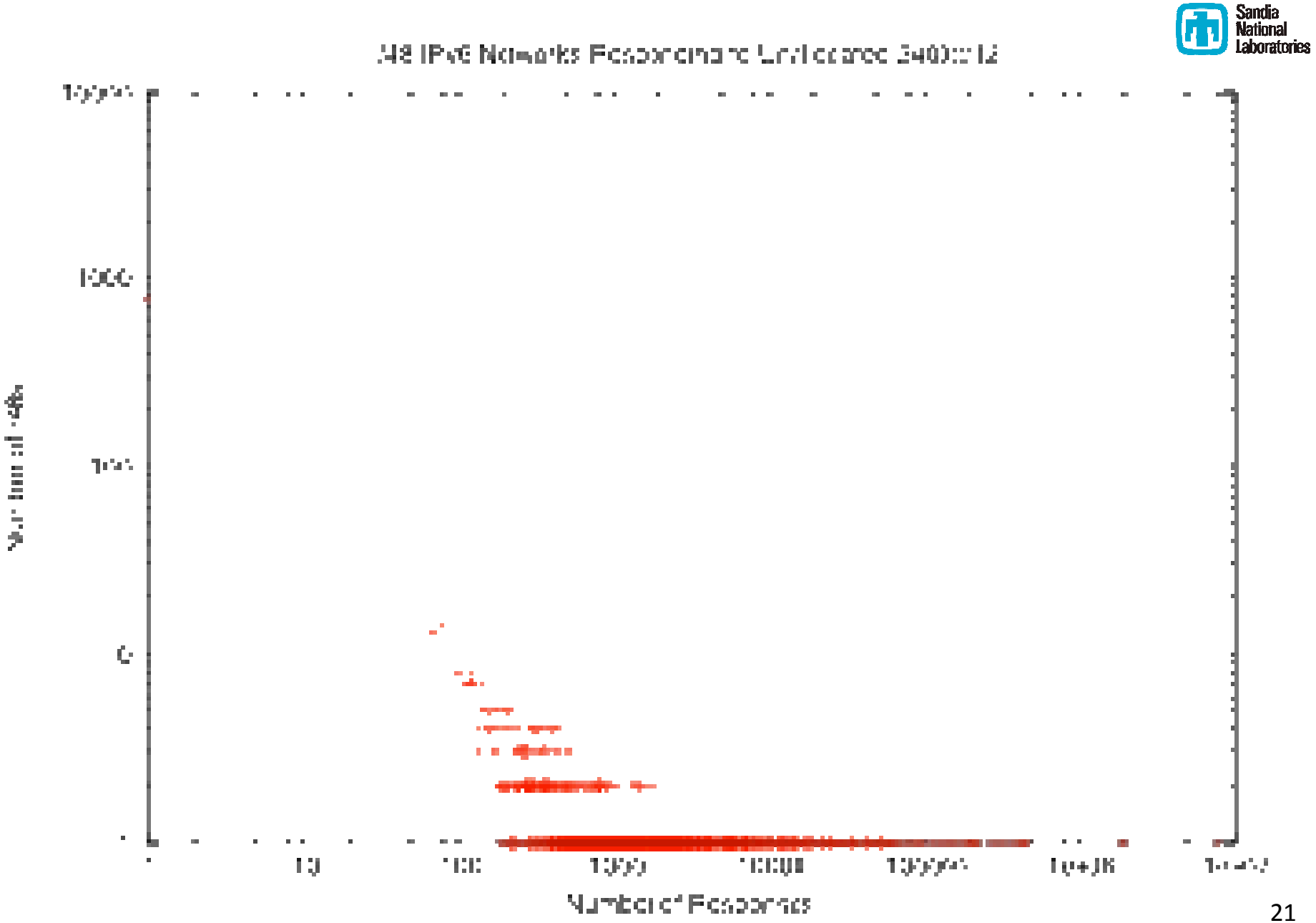
DNS packets (33M)

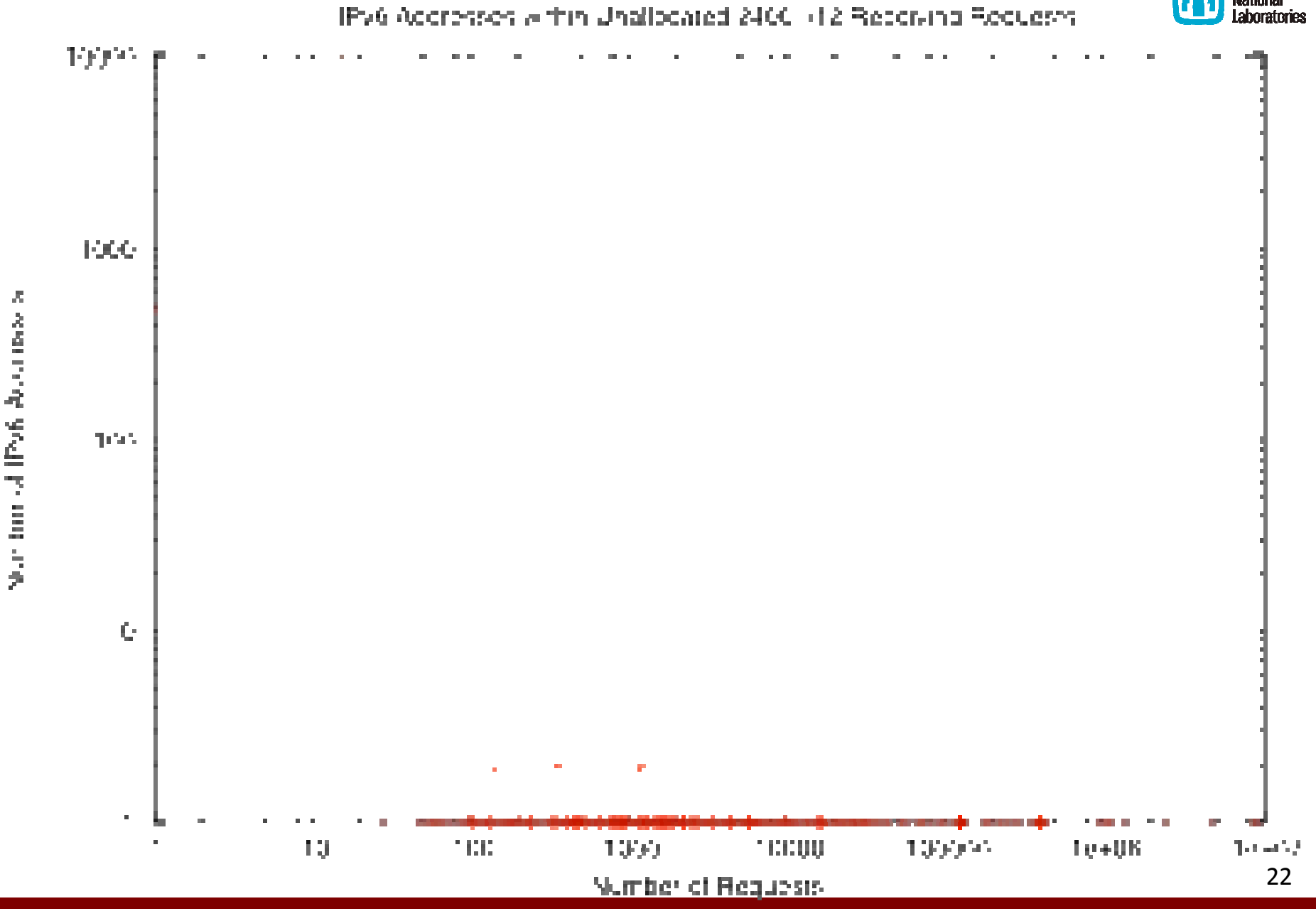


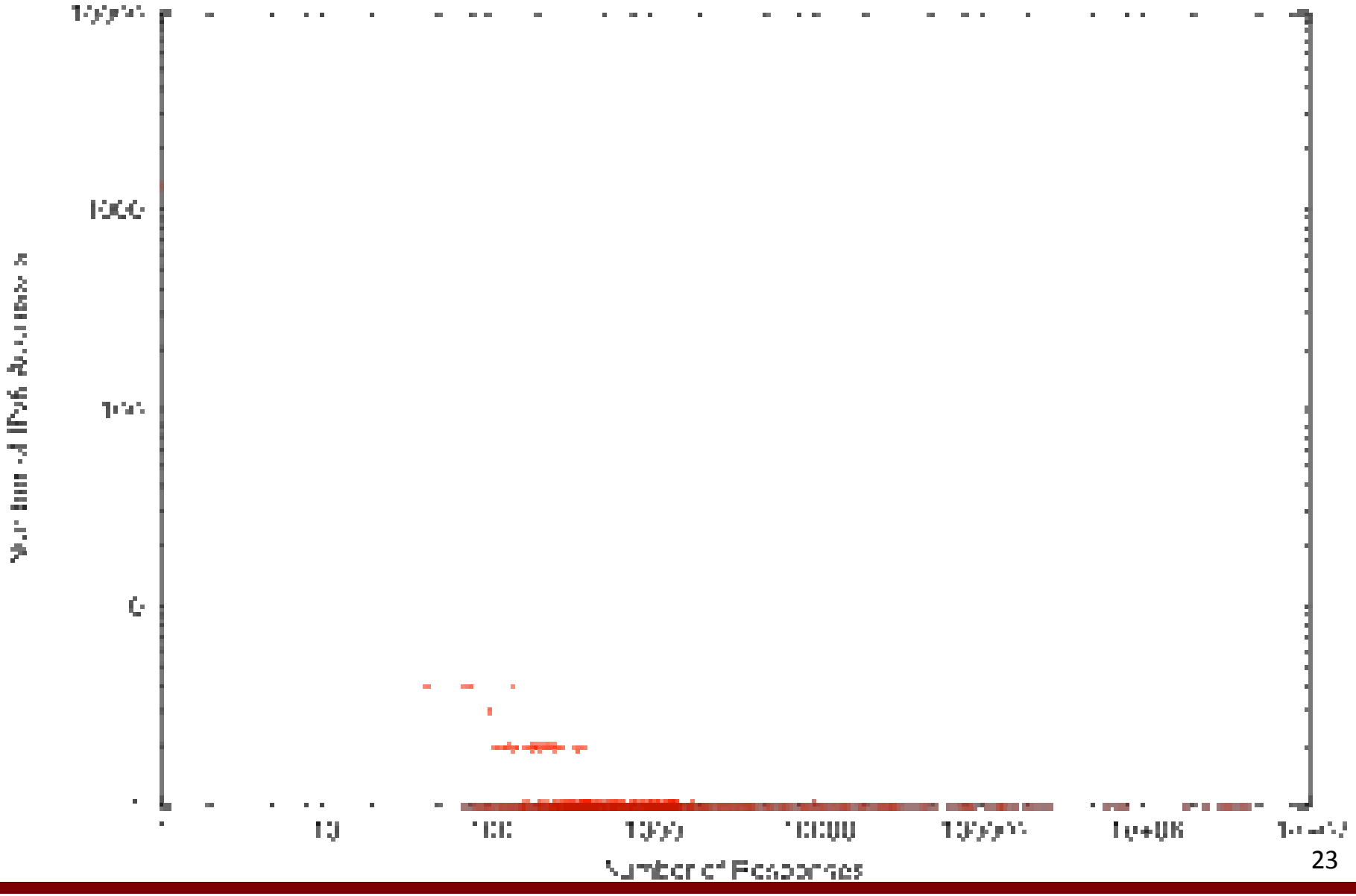
ICMPv6 traffic (56M)




Number of Requests







Summary

Sandia National Laboratories

- Analyzing network anomalies is important, as they potentially have impact on the Internet and its users
- When setting up a darknet collector, work with peers from the start to coordinate routing and announcement
- The collector receiving traffic destined for unallocated 2400::/12 receives roughly 70 packets per second

Questions?

- ctdecci@sandia.gov