TransPac Flow Data: Collection and Analysis

INTERNATIONAL NETWORKS
At Indiana University

Hans Addleman
Network Engineer, International Networks
University Information Technology Services
Indiana University
addlema@iu.edu

Supported by the National Science Foundation

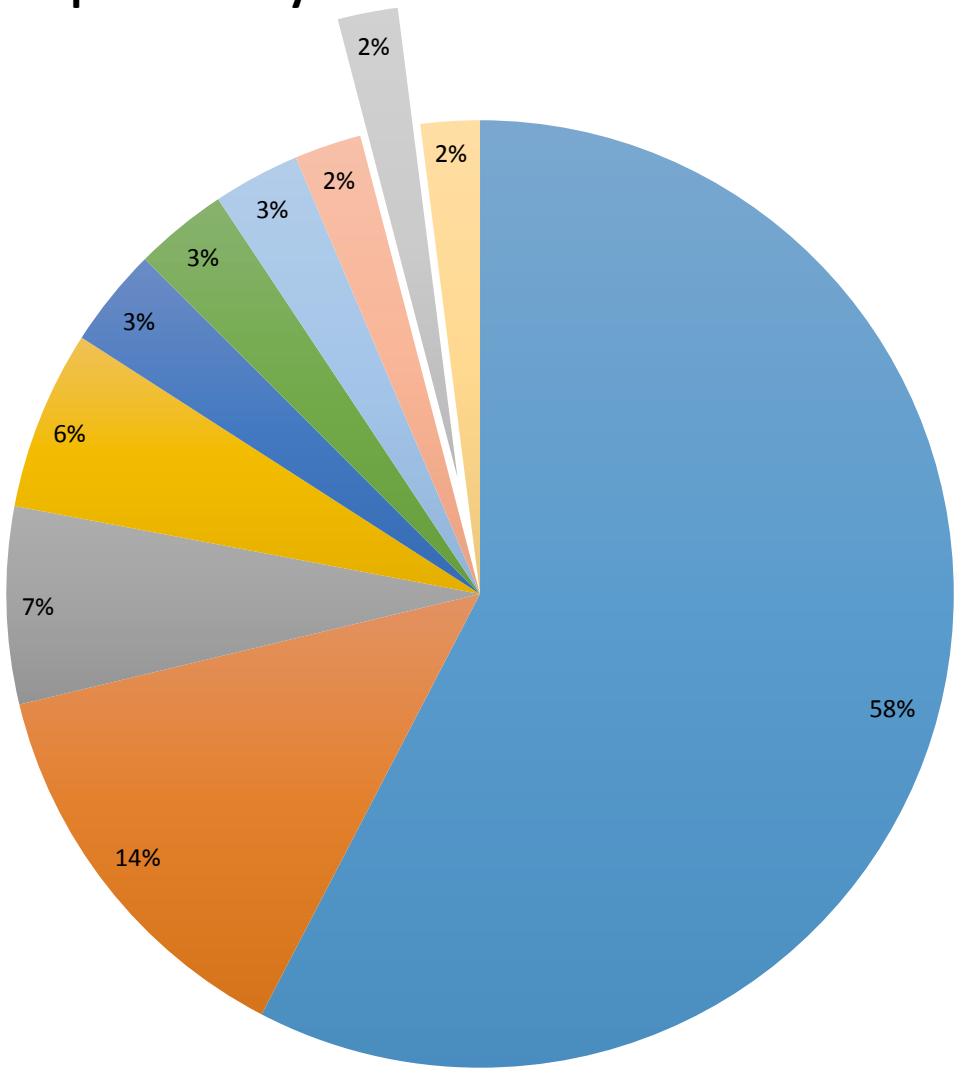
TransPAC Netflow Overview

- Started collecting flow records in February 2015
- Current collection is 1 in 50 packets
- Netflow Version 5
  - Moving to IPFIX for speed and IPv6 soon
- Using NFDUMP toolkit with NFSEN.

TransPAC Netflow Hardware

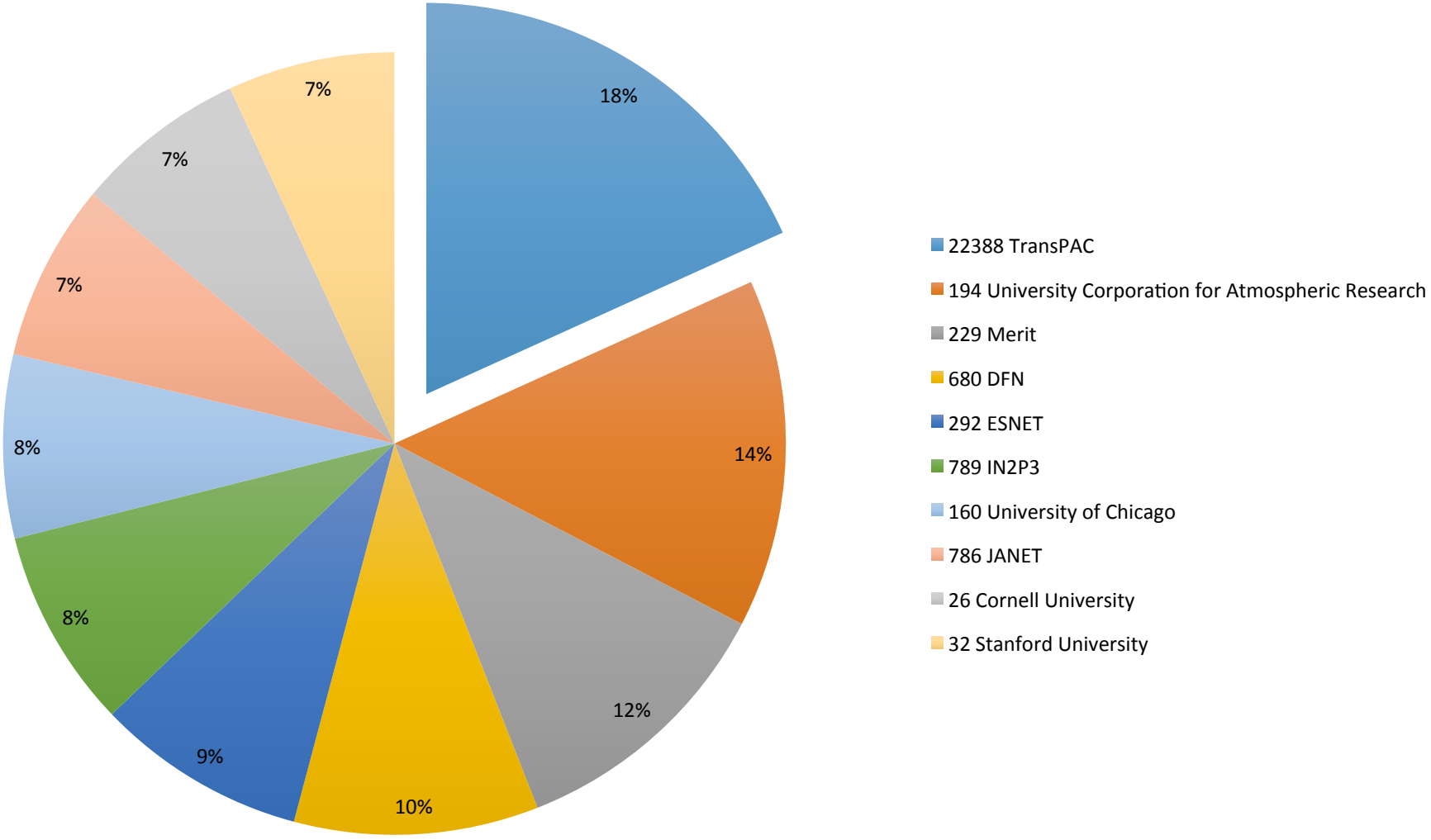
- 2 Dell Servers do the work
  - Flow Collector
    - Dell R720 with Xeon E5-2650 processors
    - 4.2TB total storage space on RAID5 array
  - Flow Processor
    - Dell R420 with Xeon E5-2430 (24 cores)
    - 384G ram
  - Servers connected by dedicated 10G link.
  - Collecting ~35G a month of netflow data.

Top Talkers by Source AS Inbound to TransPAC

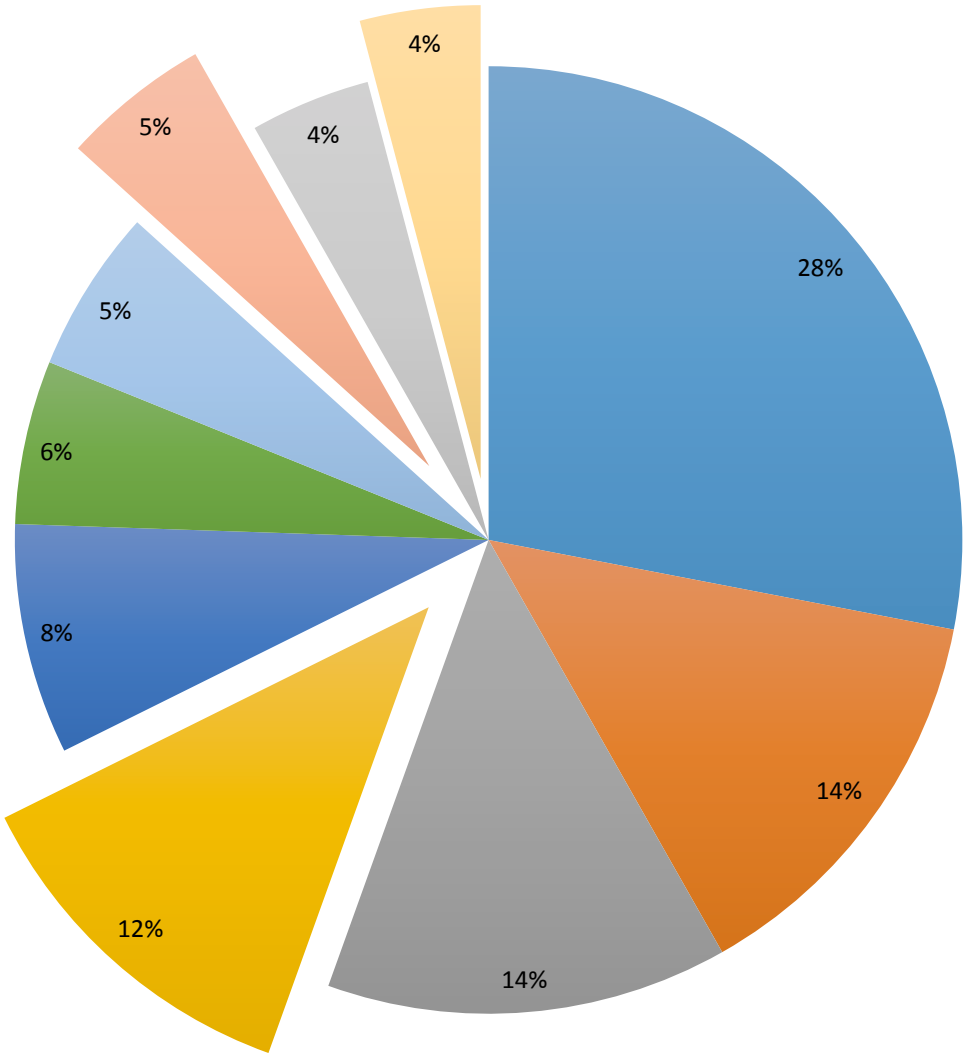


- 2501 The Univeristy of Tokyo
- 7660 Asia Pacific Advanced Network
- 17716 National Taiwan University
- 18127 Tsukuba-WAN Network
- 9264 Academic Sinica Network
- 1237 Korea Institute of Science and Technology Information Network
- 3836 Thai Social/Scientific, Academic and Research Network
- 2500 WIDE Project
- 23456 2 byte to 4 byte
- 4621 UNINET-TH

Top Talkers by Destination AS Inbound to TransPAC

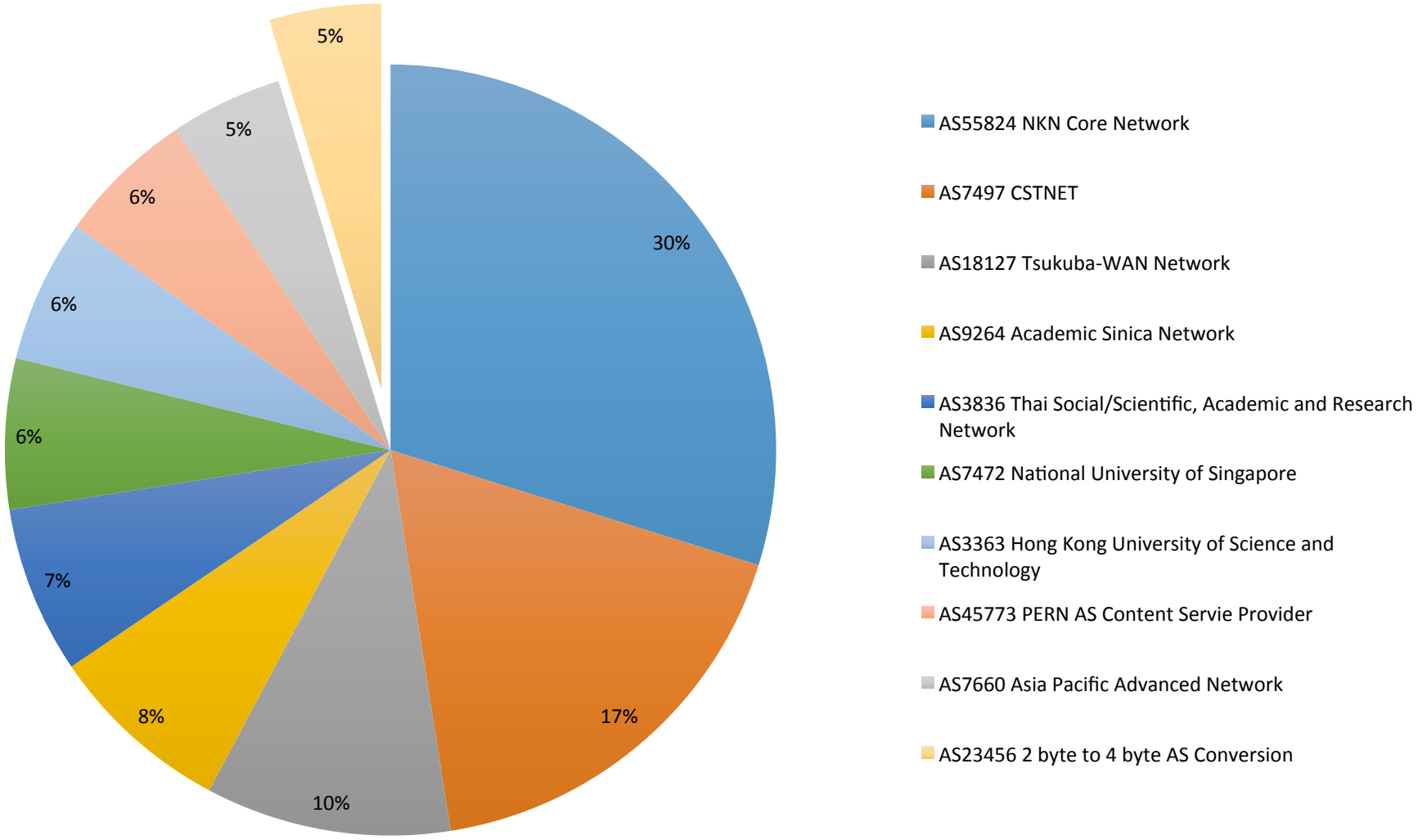


Top Talkers by Source AS Outbound from TransPAC

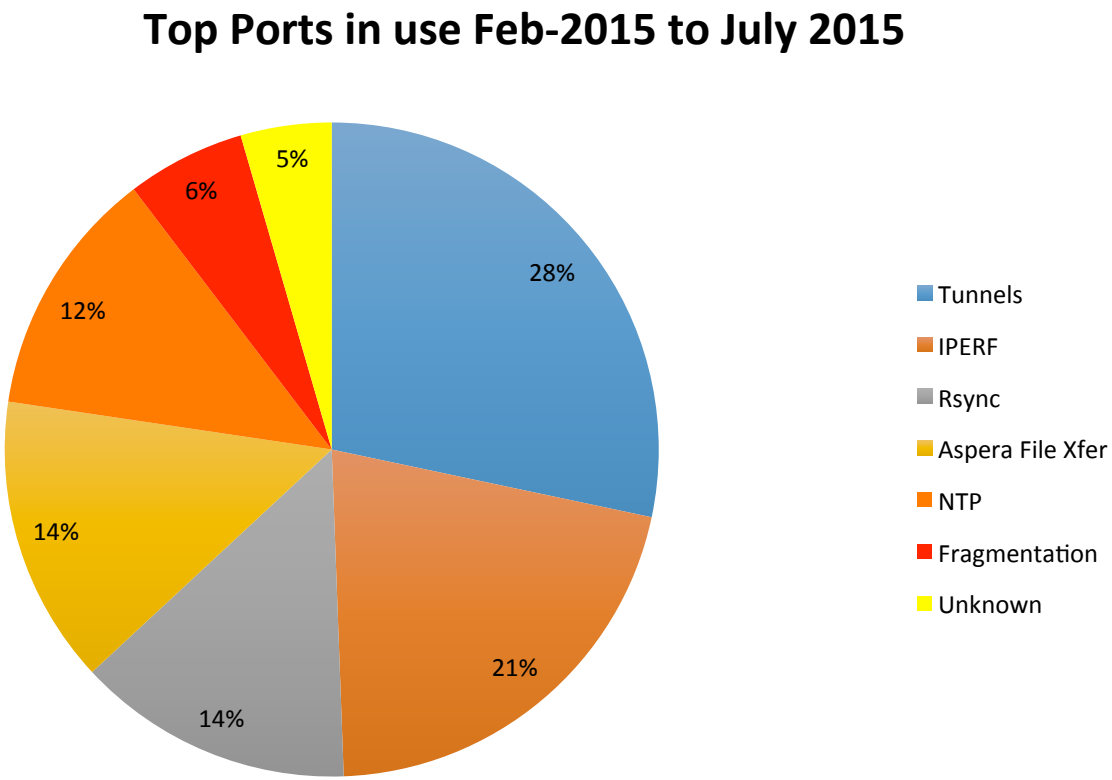


- AS7941 Internet Archive
- AS1701 National Aeronautics and Space Administration
- AS70 National Library of Medicine
- AS6629 NOAA
- AS195 San Diego Supercomputer Center
- AS5663 US Geological Survery
- AS3152 Fermi National Accelerator Laboratory
- AS194 University Corporation for Atmospheric Research
- AS11318 Georgetown University
- AS20033 National Climatic Data Center

Top Talkers by Destination AS Outbound from TransPAC



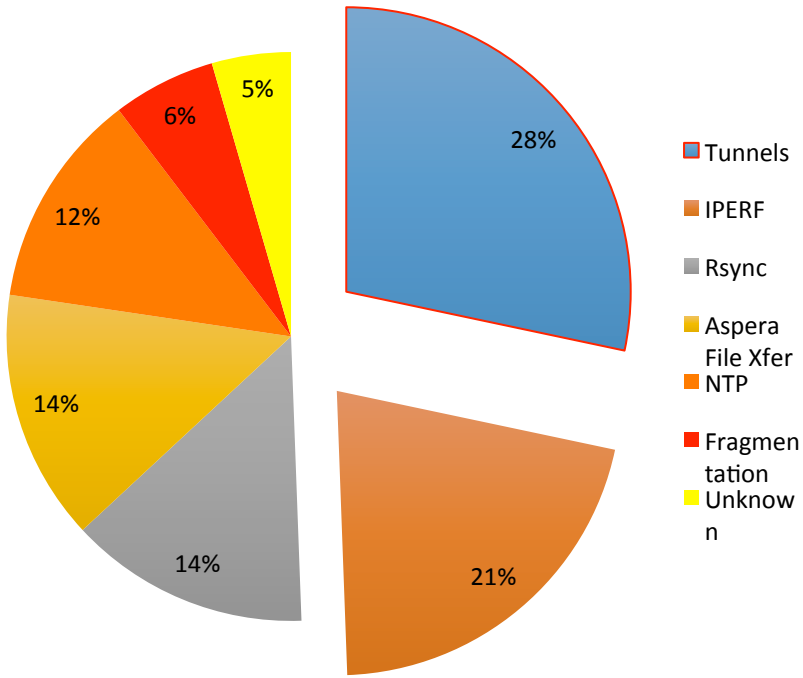
TransPAC Top Ports



Testing and Tunneling

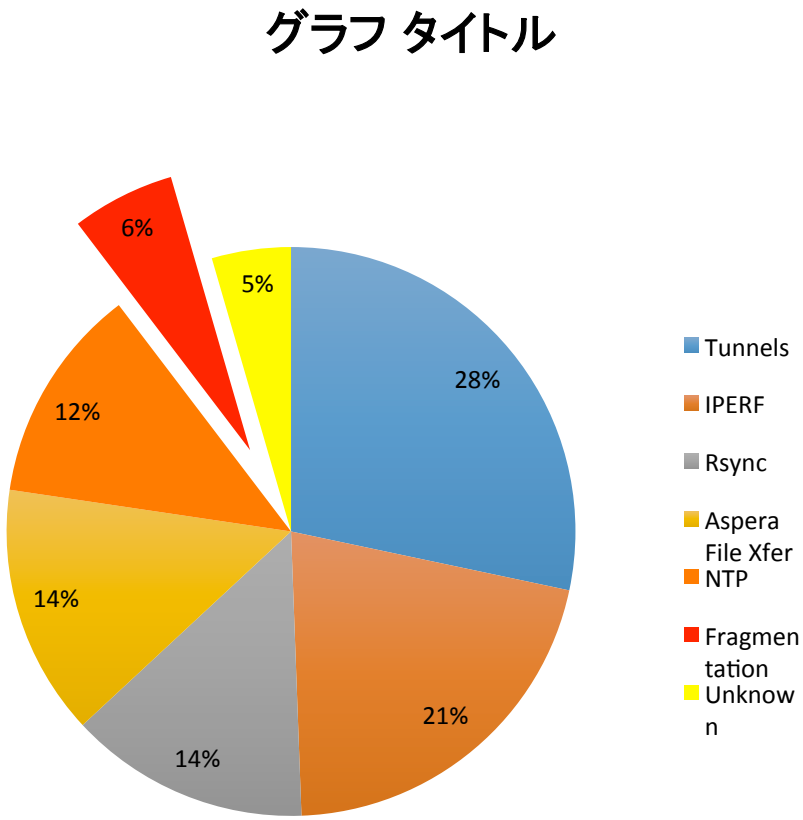
- **Lots of traffic transiting TransPAC is secure.**
- **Lots of test traffic flowing. (iperf, bwctl, perfsonar)**

Top Ports in use Feb-2015 to July 2015



UDP/TCP Port 0

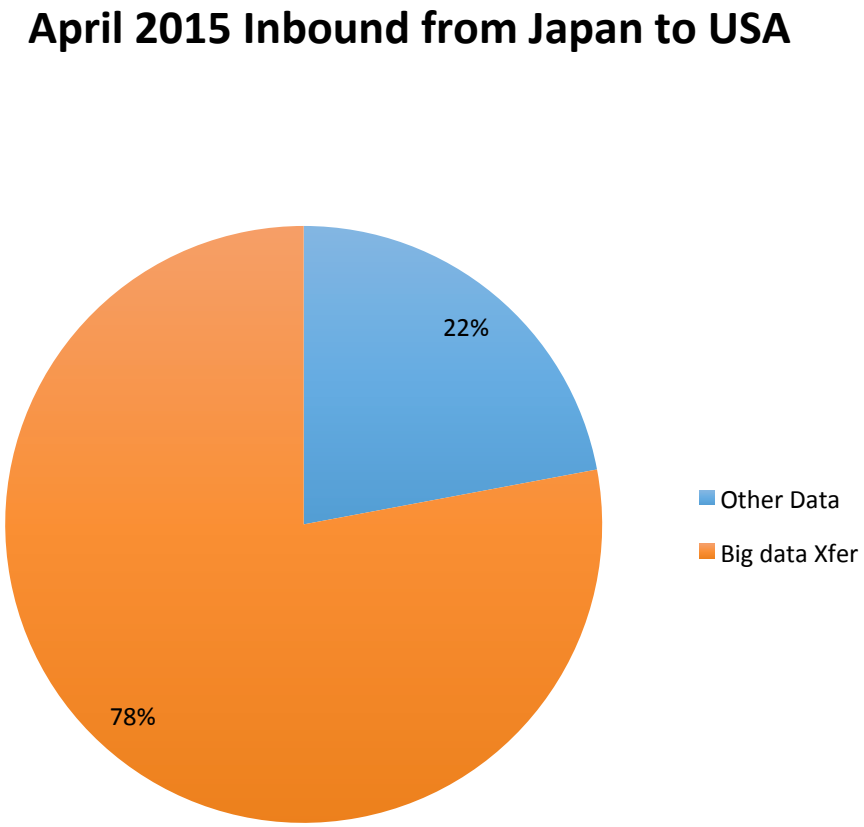
- Lots of traffic on UDP and TCP port 0.
- Fragmentation?
- A network may not have Jumbo Frames enabled in the path



April 2015 Large Transfer

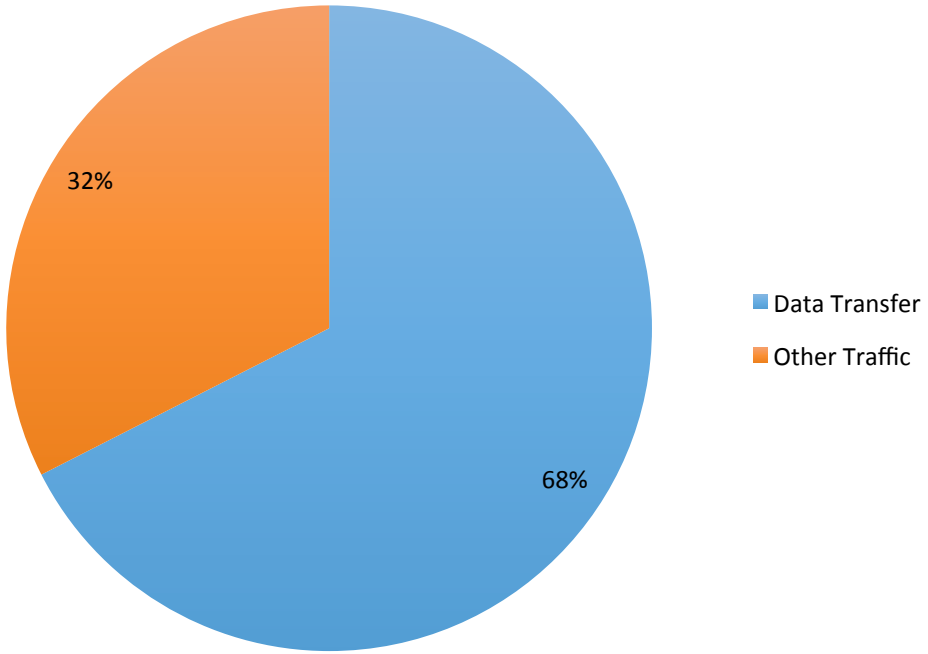
- 78% of the top 10 traffic in April was between 2 institutions.
  - The University of Tokyo
  - National Center for Atmospheric Research
  - Inbound towards NCAR

- Large file transfer between 2 institutions
- Can we help make this transfer better?
- Gives us a clue to what type of researchers are using our network.
- Reach out to other researchers in same field.
- Smaller transfers but still large noticed in March as well.



March 2015 Large Transfer

- 68% of the Top 10 Traffic in March was a data transfer
  - Georgetown University to the Academic Sinica Network



Netflow Final Thoughts

- **Great for statistics and traffic analysis.**
- **Netflow is ALSO a powerful tool for finding ongoing trouble in your network.**

Questions / Comments

- http://internationalnetworking.iu.edu

- Hans Addleman - addlema@iu.edu

- TransPAC4 NSF IRNC Award: #1450904