

# ESSC Report

W. R. Wing

*for the Steering Committee*

March 19, 2003

# So What's Been Happening?

- ESCC/Joint Techs meeting in Miami
- Organizing a Grid-Security Working Group
- Organized a Network Monitoring Group

*let's take these in order...*

# ESCC - February 2-6

- Sunday: Intros and Tutorials
  - Primarily IPv6
- Monday - Wednesday: General Sessions
  - Several talks from the ESCC community
- Wednesday - Thursday: Parallel Sessions
  - ESCC-specific sessions
  - Workshops and Hands-on sessions
- Generally positive feedback

# Some Photos -



# Wide Range of Talks -

- BRO talk:
  - Steve Lau - given remotely from LBL
- High-performance protocol lunchtime BOF
  - SABUL, TSUNAMI, FAST
- Complete Program -

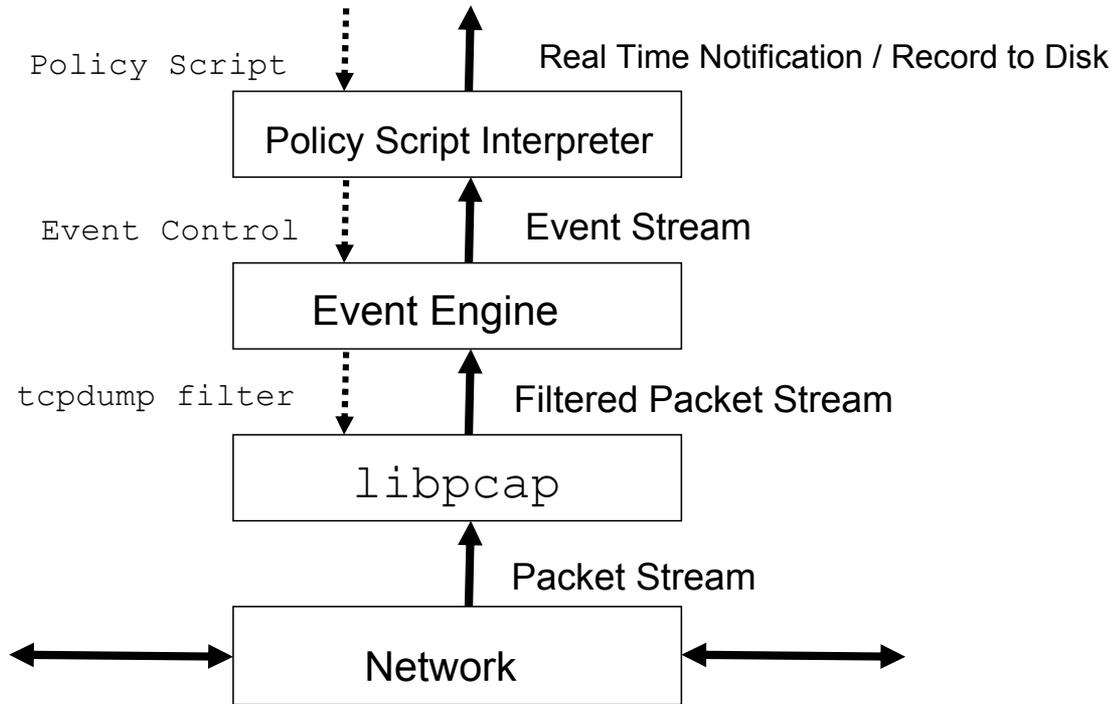
[http://www.csm.ornl.gov/~wrw/miami\\_web/index.htm](http://www.csm.ornl.gov/~wrw/miami_web/index.htm)

# Usage of the Bro System from a Practical Perspective

- ESCC/Internet2 Techs Workshop
  - Stephen Lau
  - NERSC/LBNL
  - February 4, 2003
-

- 
- High performance intrusion detection system developed at LBNL and ACRI
    - Vern Paxson primary developer
  - Based on operational experience with high performance networks
  - Grew out of tools developed to optimize and analyze network traffic
  - Bro Development Goals
    - High speed network monitoring
    - Low packet loss rate
    - Mechanism separate from policy

# Bro Structure



# Experiment: Network Research PI presentations

- Presentations in four main areas:
  - Network parameter estimation - K. C. Claffey, Wu Feng, Deb Agarwal, Warren Matthews
  - Performance improvement - Tom Dunigan, Wu Feng, Nagi Rao
  - Services - Mica Beck, Karsten Schwan
  - Simulation - Jim Rome

# Thursday Morning -

- ESCC technical talks:
  - Burrencia - Performance Centers, Secure Net
  - Metzger - Load Sharing
  - Debugging Multicast - Bell
  - PKI Update - Genovese
- ESnet Update - Jim Leighton
- Washington Update - George S.

# Grid Security

- Bob Cowles and Tony Genovese forming the core
- Initial charter being negotiated
- They will extend membership
- Generate “rfc-like” recommendations for Globus developers

# Future Meetings -

- Summer Meeting in Lawrence Kansas, week of August 4th
- Winter Meeting Jan 2004 in Hawaii
- Summer 2004 will be at Argonne

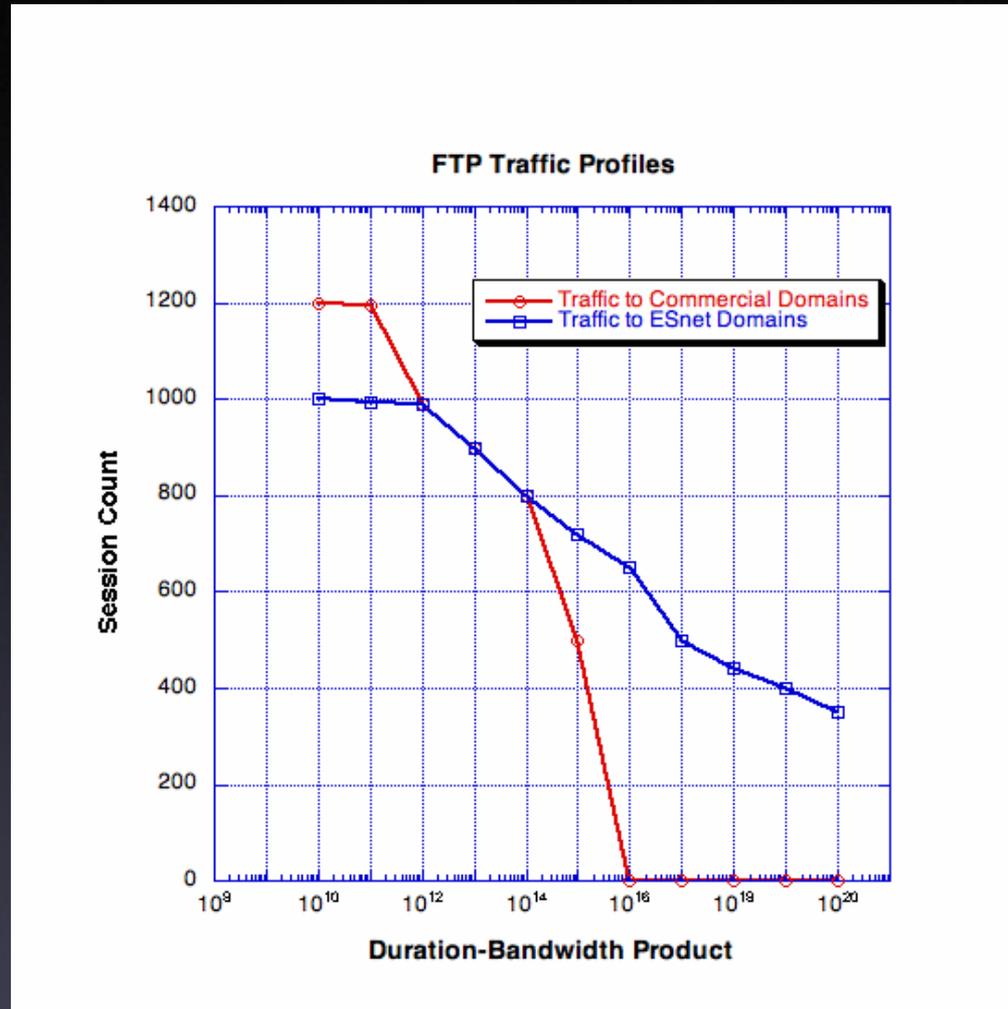
# And... Network Monitoring

- January Network Town Hall Meeting - Walt said: “If I had \$20M - ESnet isn’t even on my radar.”
- “Show me the data.”
- Asked for:
  - Trend data (with lab and program-level detail)
  - Data to prove ESnet is “Science Driven”
  - Data to show ESnet couldn’t be ISP-based
  - Six sites: ANL, FNAL, LBL, NERSC, ORNL, SLAC
- Wanted it by March(!)

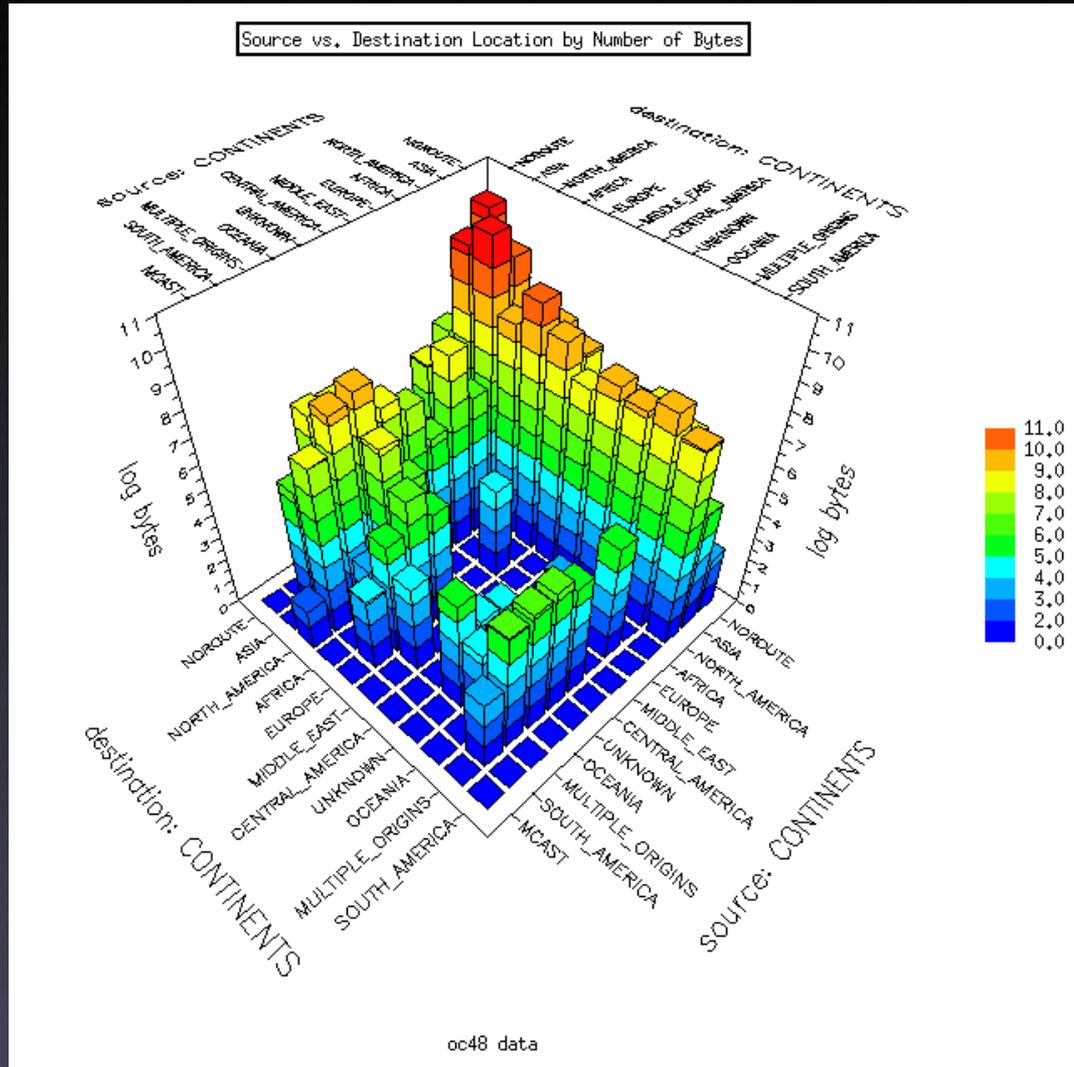
# Tall Order

- No time for new tools
- No money for new hardware
- So, investigate and use what was available
  - Cisco - NetFlow
  - PICS - Firewall
  - BRO
  - CAIDA - Coral Reef
- How to prove ESnet is Science Driven?

# Head-Scratching Time...



# Another Suggestion...



# Site Coordinators

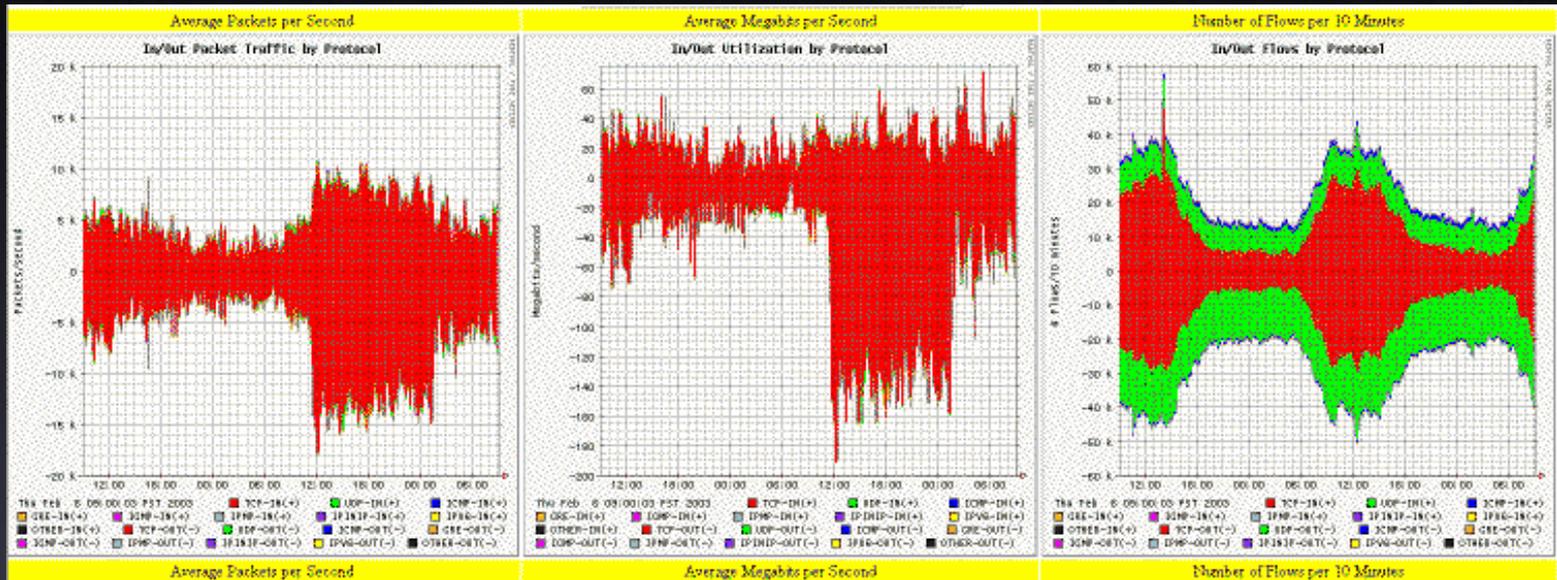
- ANL: Stacy Williams (and Rich Carlson)
- FNAL: Donna Lamore
- LBL-ESnet: Jim Leighton
- NERSC: Bill Kramer
- ORNL: Bill Wing (and Tom Dunigan)
- SLAC: Paola Grosso (Connie Logg)

# Initial Efforts

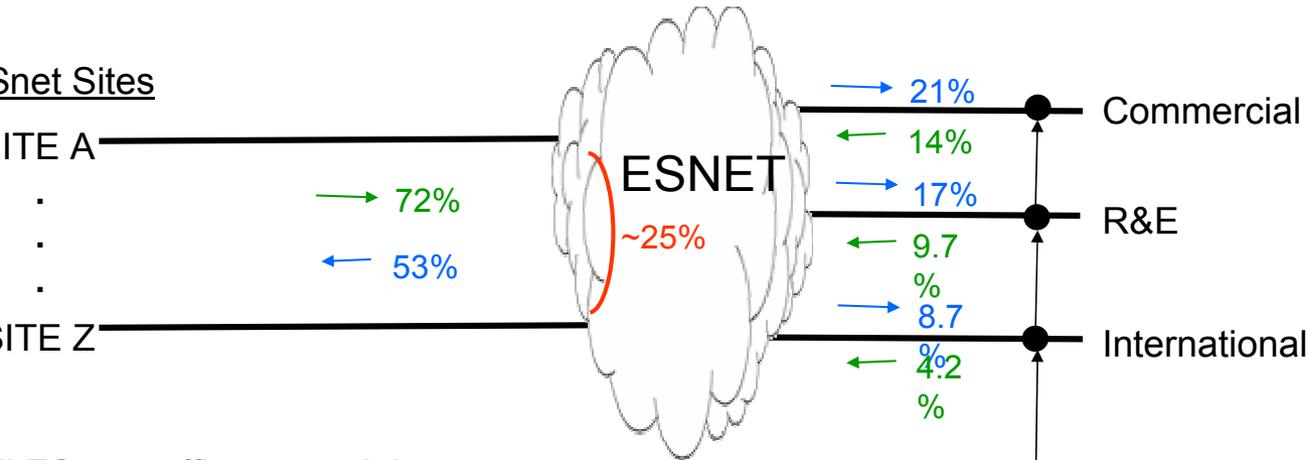
- SLAC - Has been doing monitoring for years using Cisco tools
- NERSC - Adapted libpcap (tcpdump), used BRO experience
- ESnet - Mined the traffic stats
- ORNL - Adapted OSU/I2 tools and PICS data

# SLAC

<http://www.slac.stanford.edu/~cal/netflow/netflow.html>



ESnet Inter-Sector Traffic Summary  
Jan 2003



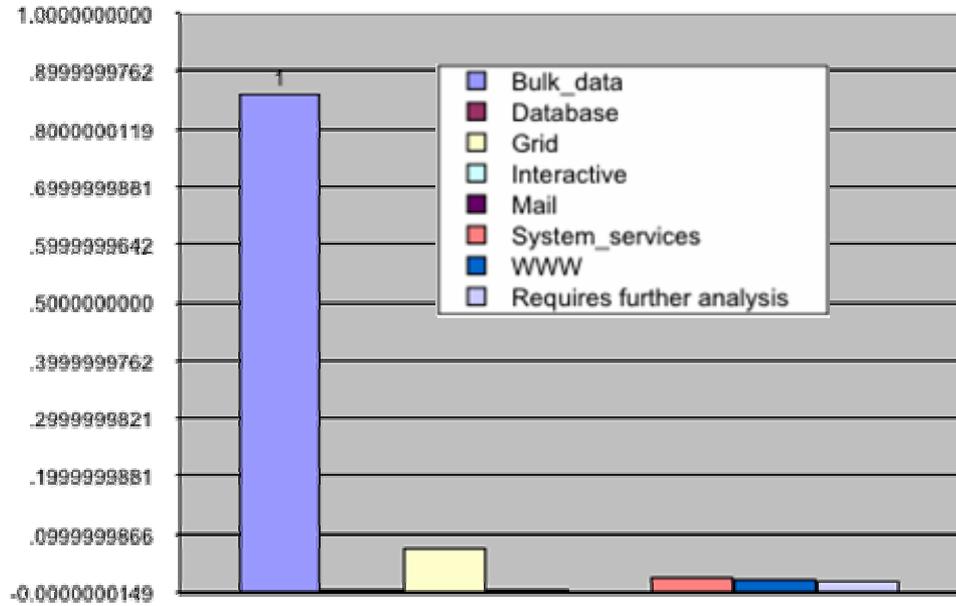
All ESnet traffic must originate and/or terminate on an ESnet site (no transit traffic is allowed)

(e.g. a commercial site cannot exchange traffic with an international site across ESnet. This is effected via routing restrictions and implementation.

Traffic from a site →  
 Traffic to a site ←  
 ESnet Ingress Traffic = Green  
 ESnet Egress Traffic = Blue  
 Traffic between sites )  
 % = of total ingress or egress traffic

# NERSC Traffic

(Jan 28 – Feb 18, 2003)



# ORNL -

<http://www.csm.ornl.gov/~dunigan/weekly/20030224/>

<http://www.csm.ornl.gov/~dunigan/daily/>

user: ORNL, passwd: ORNL

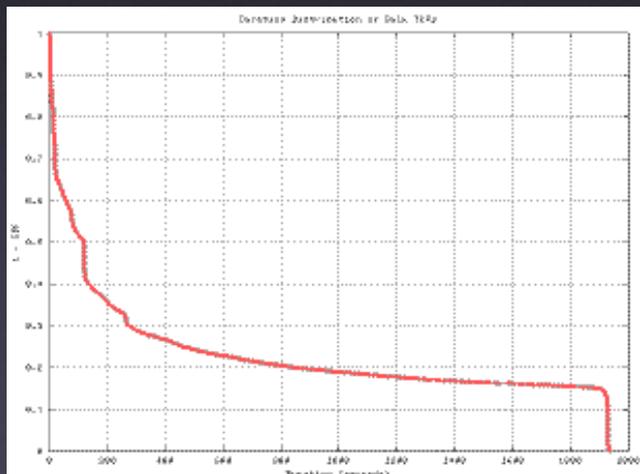
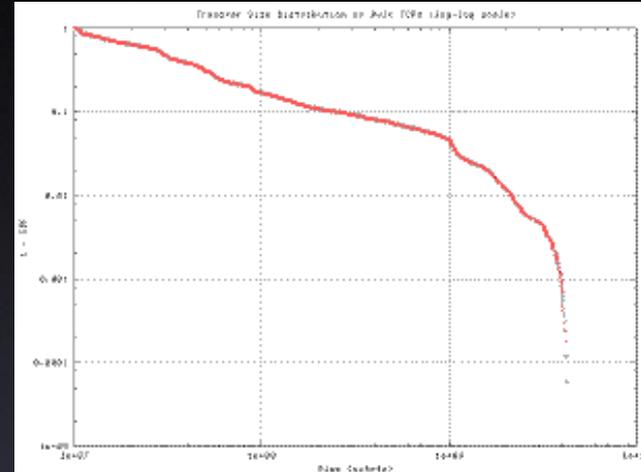
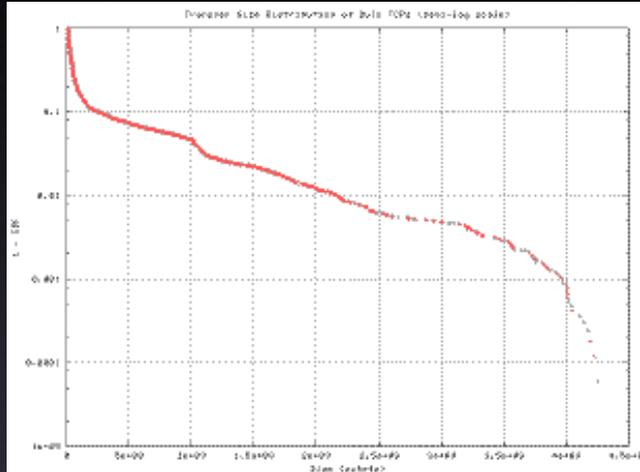
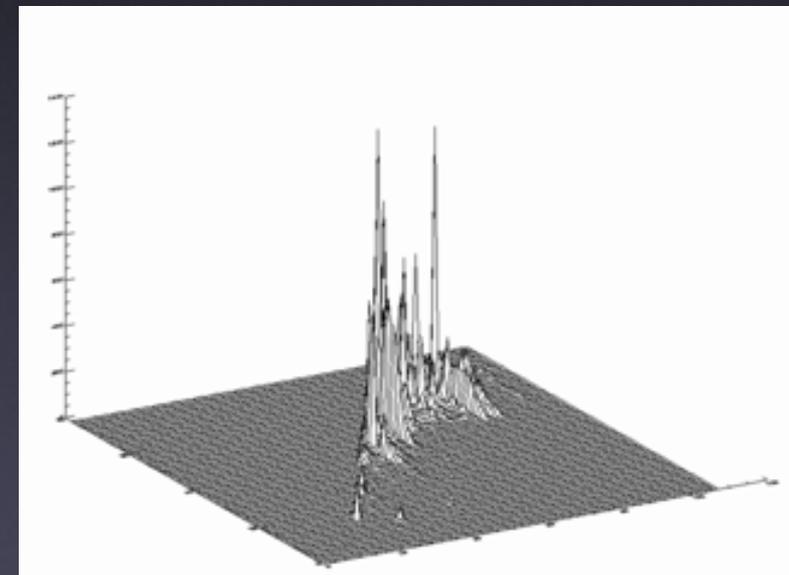
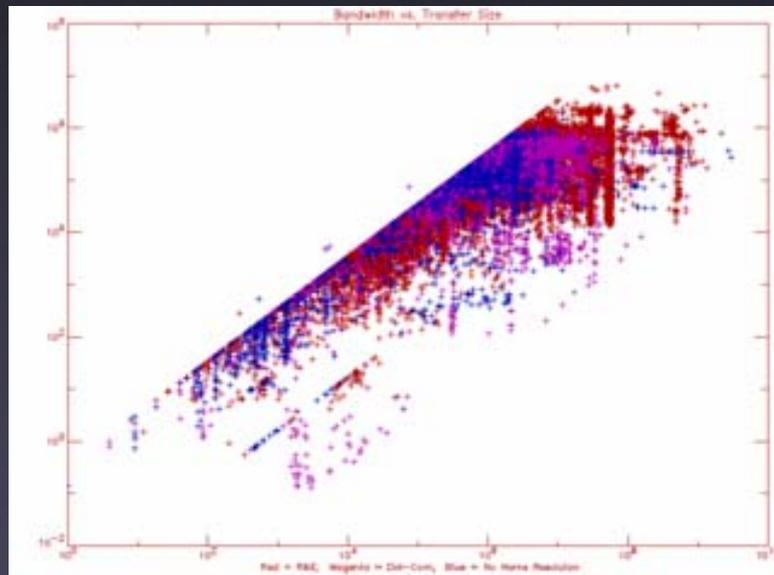
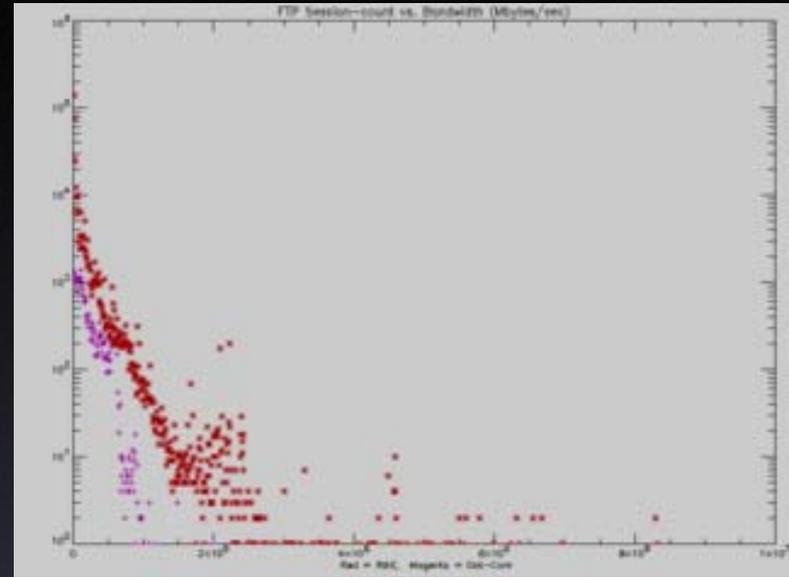
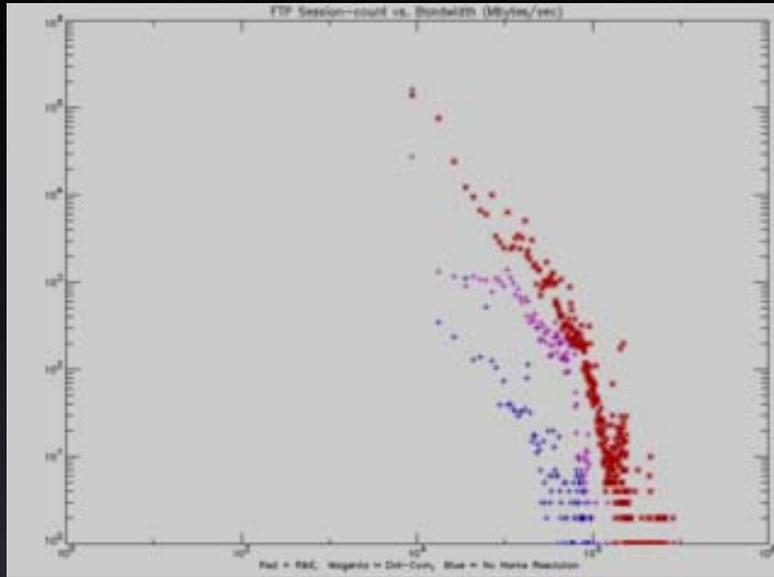


Table 3. Aggregated Application Types (Bulk TCP)

Traffic Type	Octets		Packets		Flows	
Measurement	58.64%	1.639T	55.62%	1.253G	15.43%	3.003k
Data Transfers	25.43%	711.0G	26.82%	604.5M	41.28%	8.034k
Encrypted Traffic	7.26%	202.9G	7.01%	158.0M	9.25%	1.800k
Advanced Apps	0.48%	13.29G	0.39%	8.878M	6.30%	1.227k
File Sharing	0.27%	7.575G	0.35%	7.919M	0.87%	170.0
Misc	0.18%	5.108G	0.20%	4.594M	1.20%	234.0
Audio/Video	0.13%	3.691G	0.13%	2.993M	0.69%	134.0
Other	0.03%	797.4M	0.03%	637.2k	0.17%	33.00
Unidentified	7.58%	211.8G	9.44%	212.7M	24.79%	4.824k
Total	100.00%	2.795T	100.00%	2.254G	100.00%	19.46k

# ORNL - Firewall Data



# Next Steps -

- Walt has said he is willing to iterate
- But - he seems to want -
  - Both some low-maintenance, long-lived trending tools
  - Some (possibly one-off, hero-level) detailed measurements

# Possible Path Forward

- Some combination of NetFlow and OSU tools could provide automated, web-visible, trend tools for long-term data
- Refined PICS data can possibly provide desired one-off
- Extensions questionable

Thanks...