Penn State Science DMZ Researcher Engagement

July 12, 2016
Ken Miller
kdm193@psu.edu

Agenda

- Why the trouble?
- NSF CC*NIE Grant
- Researcher Engagement
- Security
- Data Compliance
- Science DMZ as a Service

- Wins/Opportunities
- sFlow Big Data Network Measurement

Enterprise Perspective

- Point of view from
  - Central IT, Networking, and Security
  - Not Research
- Penn State has decentralized IT but offers central IT services
  - Which means Colleges and Departments can select IT from central
  - Or can do your own thing

Why?

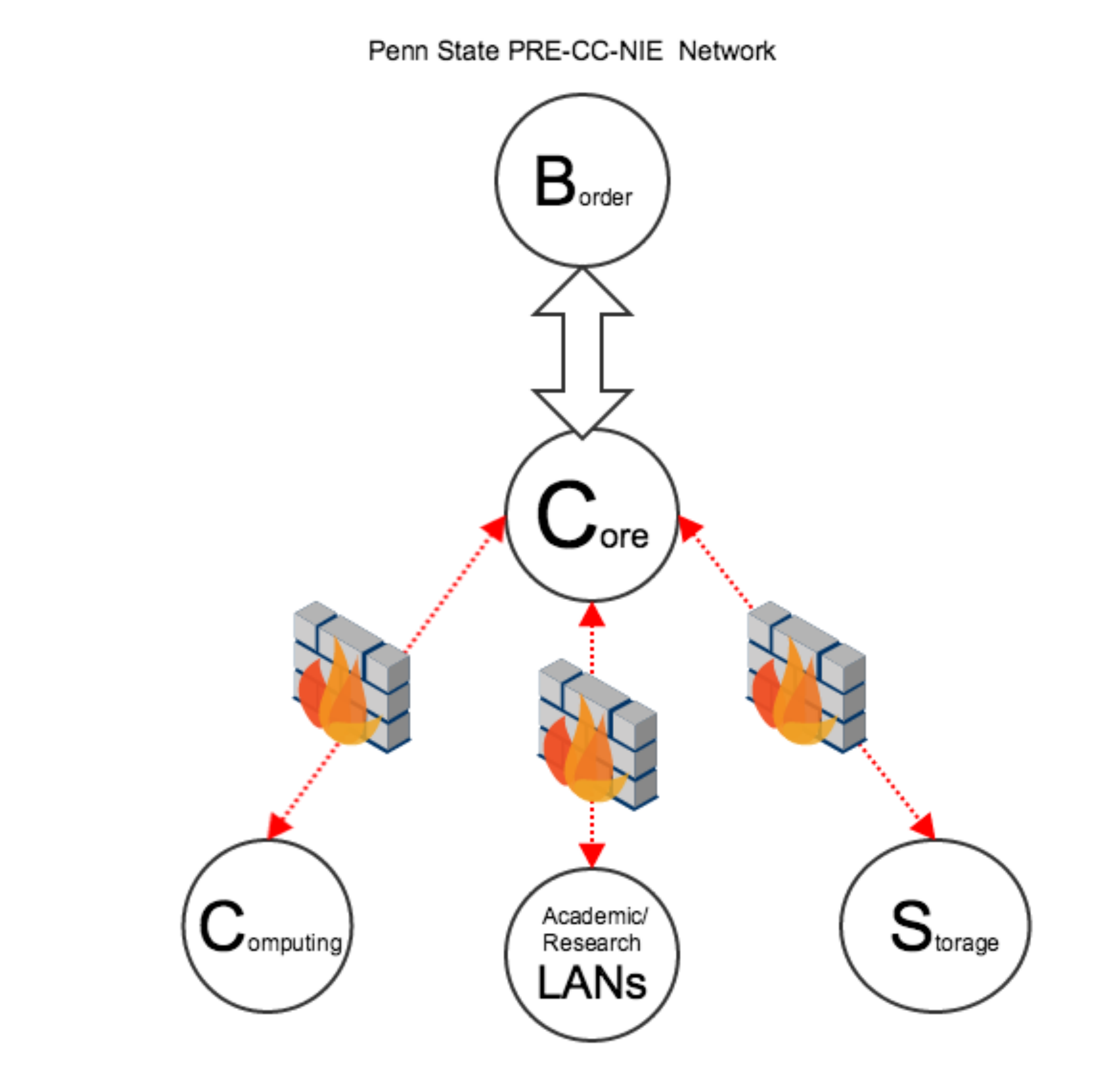
- Performance
  - Most networks are built for business system s or enterprise computing
  - Are researchers complaining of slow speeds?
  - Are local IT groups measuring performance?
- Security
  - Are research devices treated differently?
  - Are large research flows scanned too much?

Grant Specifics

- NSF Campus Cyberinfrastructure –
- Network Infrastructure and Engineering Program (CC-NIE)
- Data Driven Networking Infrastructure for the Campus and Researcher
- Building a 100G “Science DMZ"
- 10G dedicated edge switches

A Research Network based on a Science DMZ Model

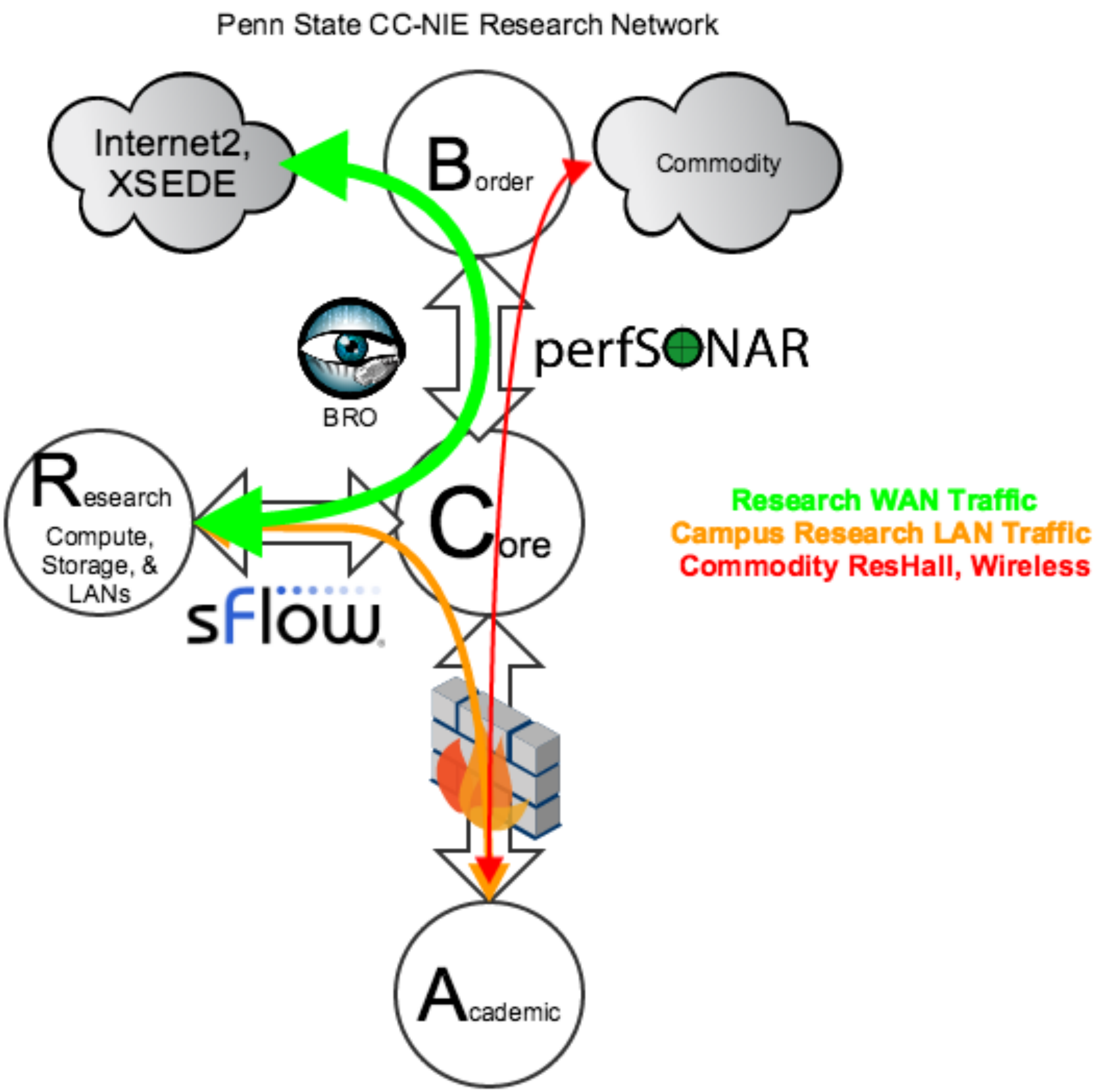
Why? PSU's Core



PSU Science DMZ

- Brocade won the RFP for new core, 100G, MPLS/VPLS, sFlow, SDN
- No Border Firewalls at PennState. All Customer Edge firewalls.
- Top 10 v4/v6 based on sFlow border data
- 2 MLXe Routers – 100G to core
- 2 VDX 8770s – vLAG'd to MLX
- 12 edge VDX 6740s from Top10 Border Capacity
  - Sequencers, Sensors
  - Instruments, Telescopes, Microscopes
  - HPC Compute/Storage
  - Central Storage

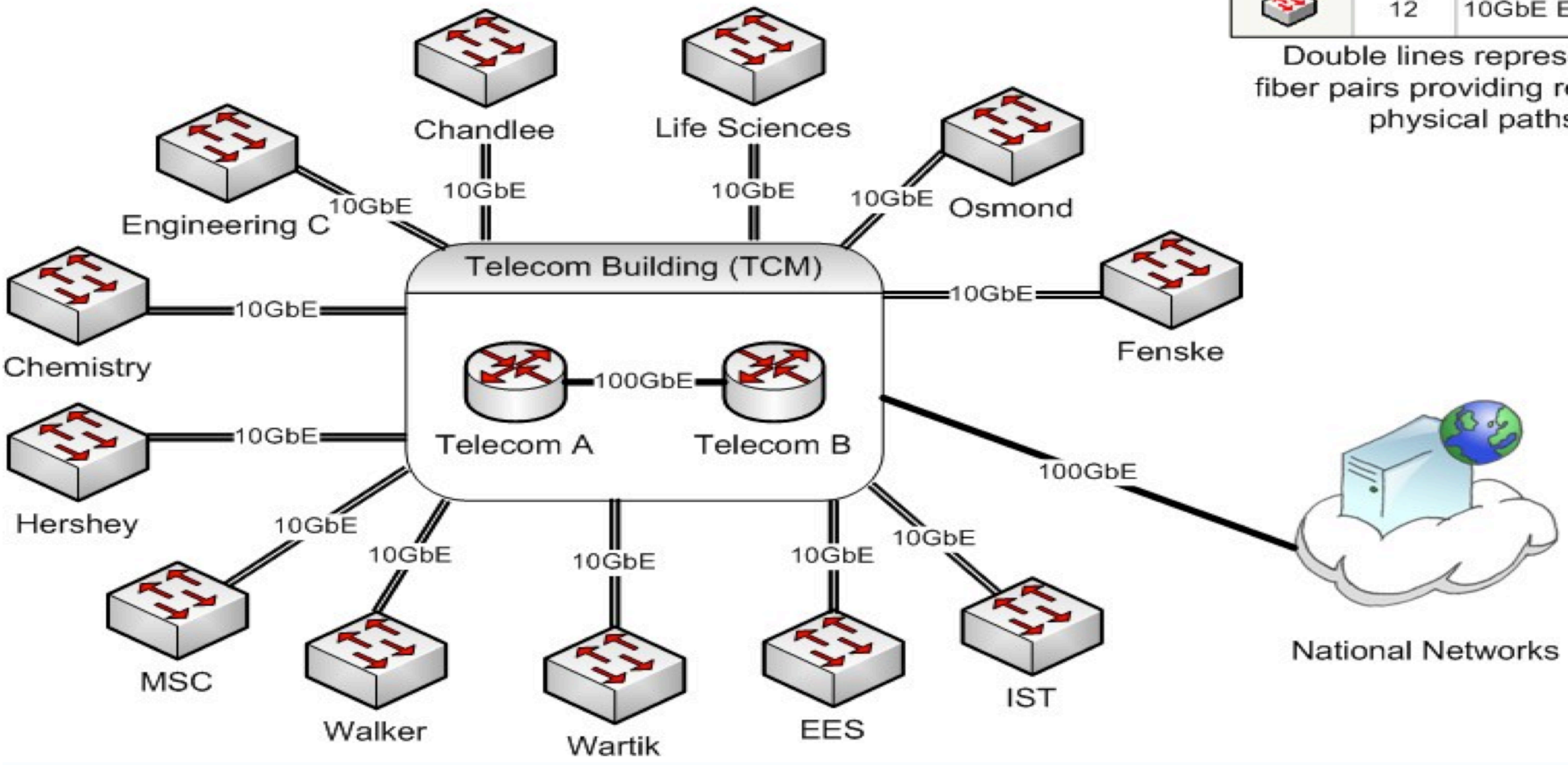
PSU Science DMZ


Penn State CC-NIE Research Network
Internet2, XSEDE
Border
Commodity
BRO
perfSONAR
Research Compute, Storage, & LANs
Core
sFlow
Academic
Research WAN Traffic
Campus Research LAN Traffic
Commodity ResHall, Wireless

Proposed Design

Conceptual Network Map		
Penn State Research Network		
Symbol	Count	Description
●	2	100GbE Core Router
●	12	10GbE Edge Switch

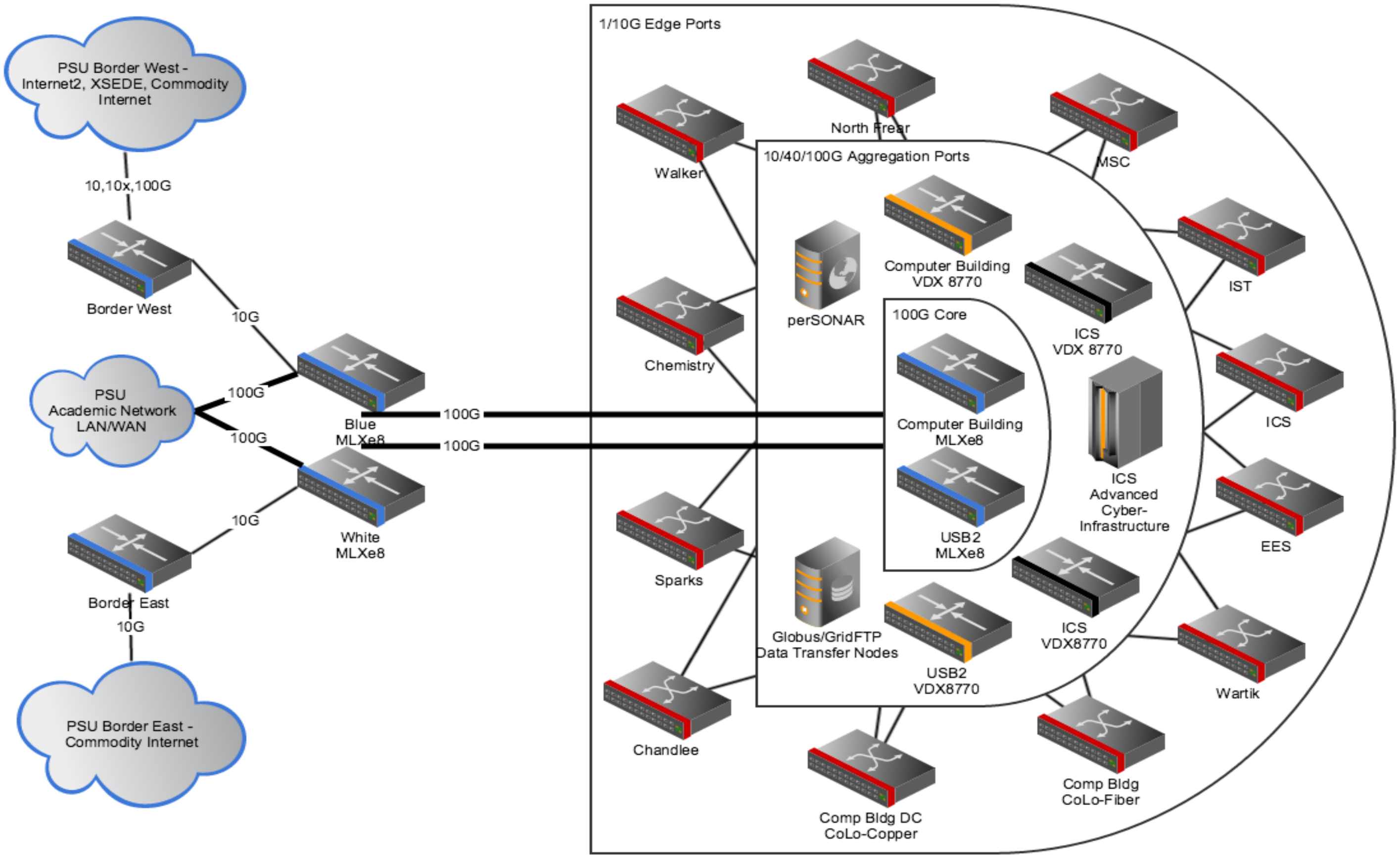
Double lines represent two fiber pairs providing redundant physical paths.



Working Design

PENNSTATE

Penn State University Research Network
"B1G D" Science DMZ



Big Data…

Big Discourse…

Big Discovery…

"Big D"

Research Networking @ Penn State

Problem:
Resolve last mile research data transfer friction points for both on-campus and off-campus data transfers

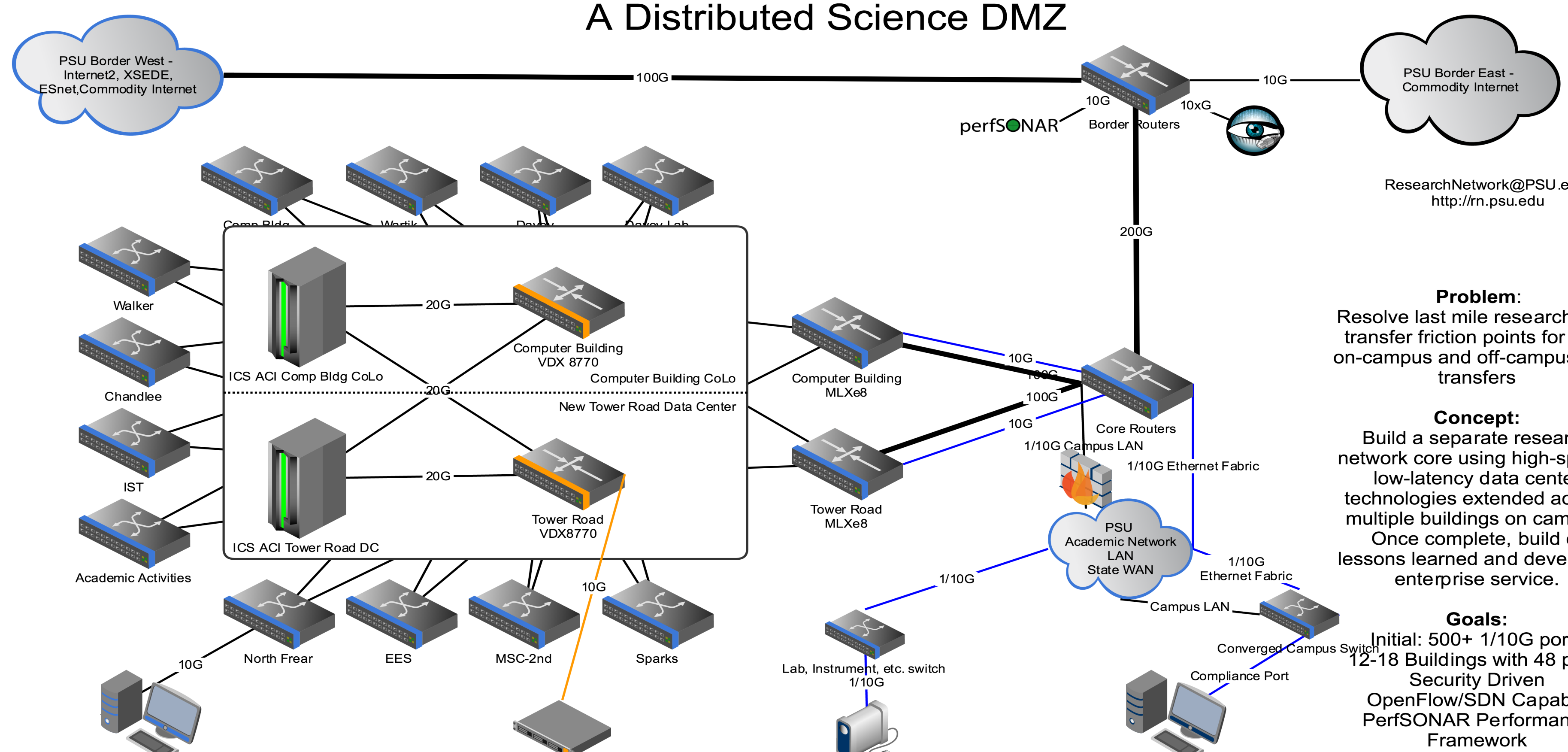
Concept:
Build a separate research network core using high-speed, low-latency data center technologies extended across multiple buildings on campus

Goals:
500+ 1/10G ports
12-18 Buildings with 48 ports
OpenFlow/SDN Capable
PerfSONAR Performance Monitoring

Service Design

PENNSTATE

Penn State University Research Network
A Distributed Science DMZ



ResearchNetwork@PSU.edu
http://rn.psu.edu

#1: Premium Switch Option
Brocade VDX Switch installed locally
20 Gb/s fiber connectivity back to each data center
48 1 Gb/s sopper or 10Gb/s fiber edge ports
Fastest Connection for many ports

#2 Data Center Option
Your Server racked in the data center
10x Gb/s connectivity
Fast Connection for a
Single OS or VM host

#3 Ethernet Fabric Option
Brocade ICX switch
10Gb/s Ethernet Fabric Speedy connection for multiple users
24or 48 1Gb/s copper ports with 1 10Gb/s fiber port
Coming Fall 2016

#4 Converged Port
Your Device
1Gb/s connection for compliance
Any number of converged ports
Proof of Concept

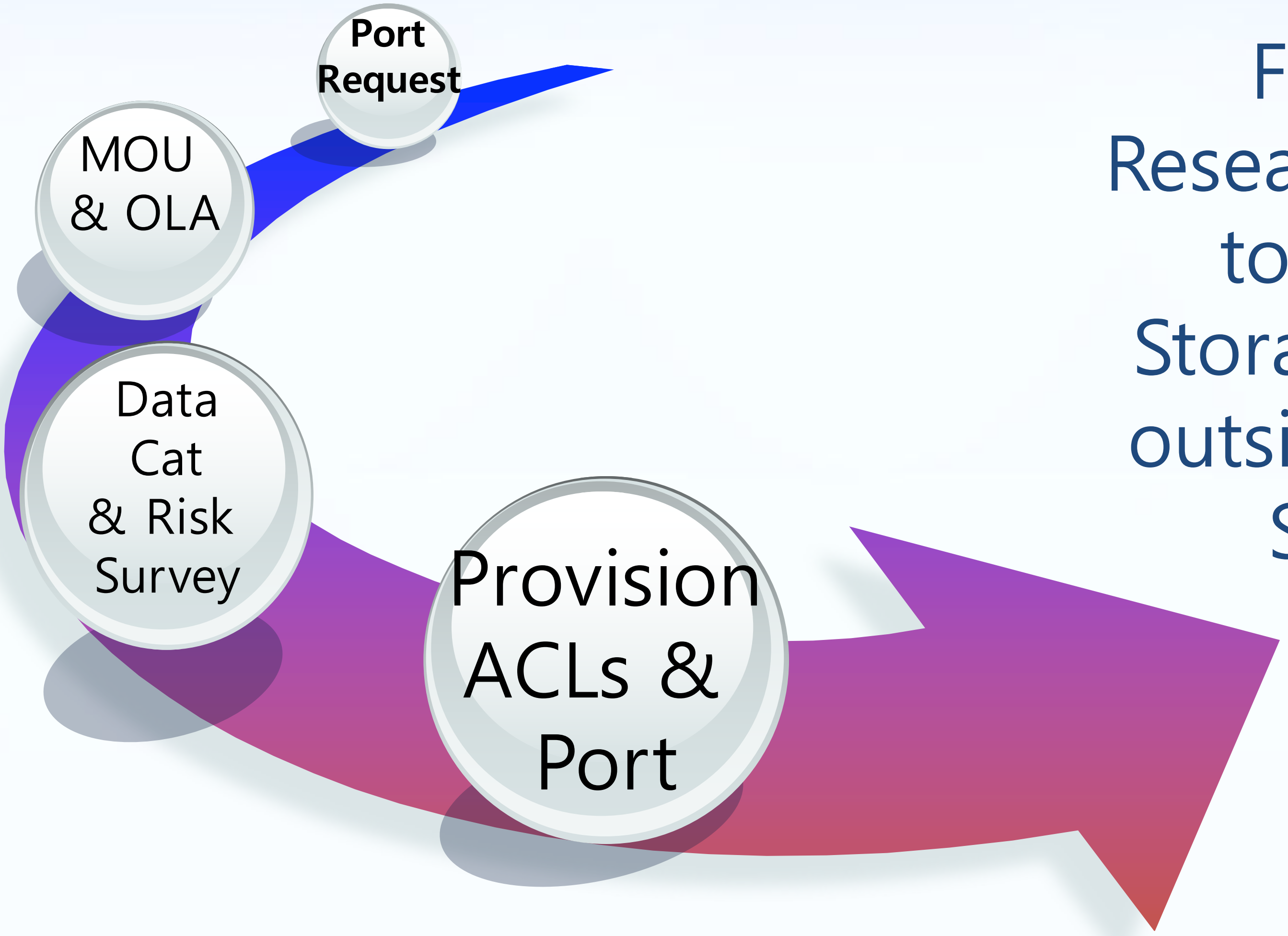
Problem:
Resolve last mile research data transfer friction points for both on-campus and off-campus data transfers

Concept:
Build a separate research network core using high-speed, low-latency data center technologies extended across multiple buildings on campus. Once complete, build on lessons learned and develop an enterprise service.

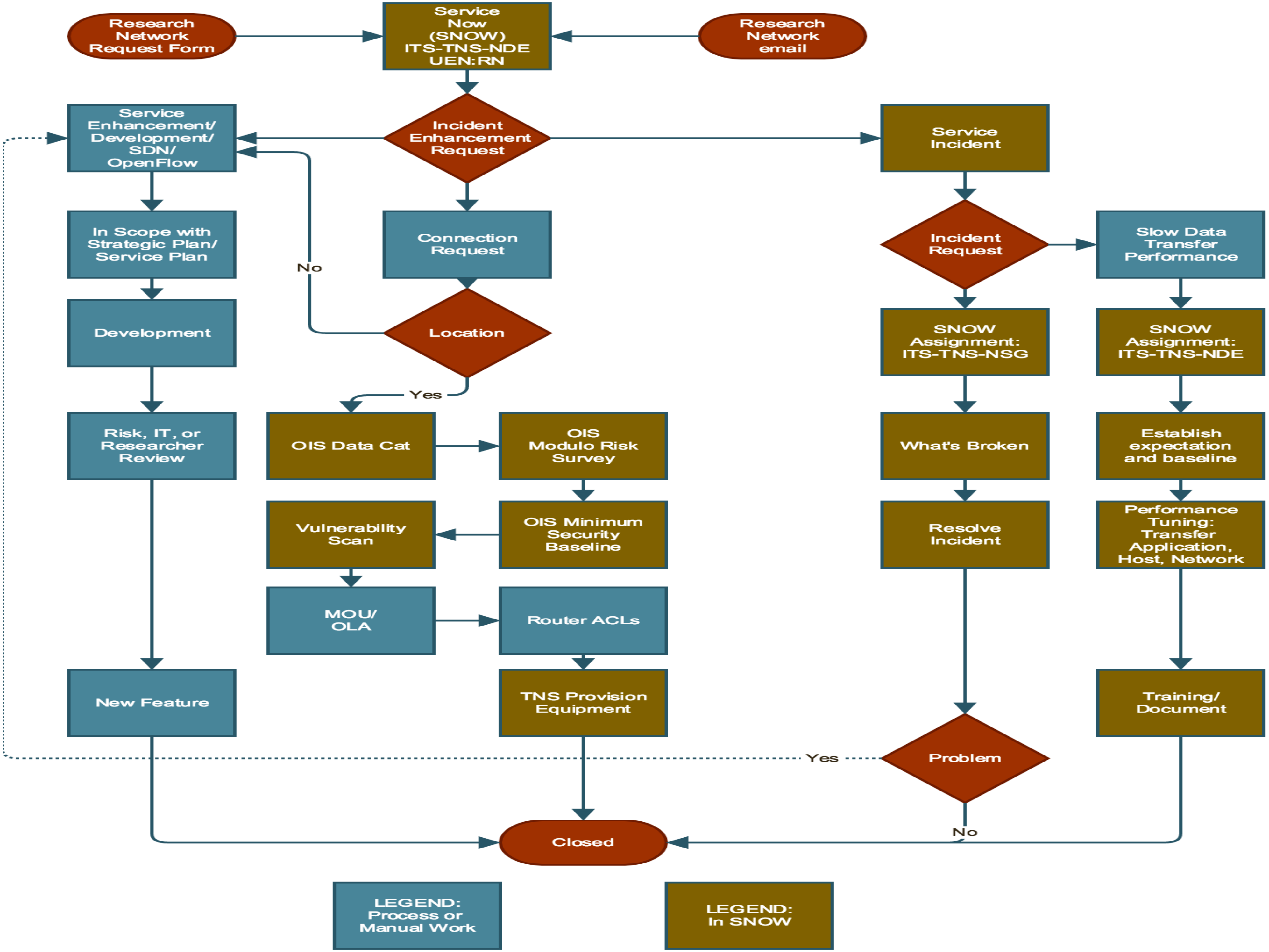
Goals:
Initial: 500+ 1/10G ports
12-18 Buildings with 48 ports
Security Driven
OpenFlow/SDN Capable
PerfSONAR Performance Framework
sFlow Monitoring

NSF BROCADE INTERNET2 XSEDE Extreme Science and Engineering Discovery Environment perfSONAR globus inMon The Inventors of sFlow®

Secure Researcher On-Ramp and Engagement



Faster Research Data to HPC, Storage, and outside Penn State


Research Network Request Form
Service Now (SNOW) ITS-TNS-NDE UEN:RN
Research Network email
Service Enhancement/ Development/ SDN/ OpenFlow
Incident Enhancement Request
Service Incident
In Scope with Strategic Plan/ Service Plan
No
Connection Request
Incident Request
Slow Data Transfer Performance
Development
Location
SNOW Assignment: ITS-TNS-NSG
SNOW Assignment: ITS-TNS-NDE
Yes
Risk, IT, or Researcher Review
OIS Data Cat
OIS Modulo Risk Survey
What's Broken
Establish expectation and baseline
Vulnerability Scan
OIS Minimum Security Baseline
Resolve Incident
Performance Tuning: Transfer Application, Host, Network
MOU/ OLA
Router ACLs
New Feature
TNS Provision Equipment
Training/ Document
Yes
Problem
No
Closed
LEGEND: Process or Manual Work
LEGEND: In SNOW

Research On-Boarding with Cyber Security and Data Compliance

- Deny all traffic by default
- OIS - Data Categorization
- OIS - Modulo Risk Survey
- OIS - Minimum Security Baseline
- OIS – MOU, Vulnerability Scanning, Host Mitigation
- Once OIS OK'd, open up IPs and ports per researcher engagement and needs
- Every denied packet will syslog an event to OIS

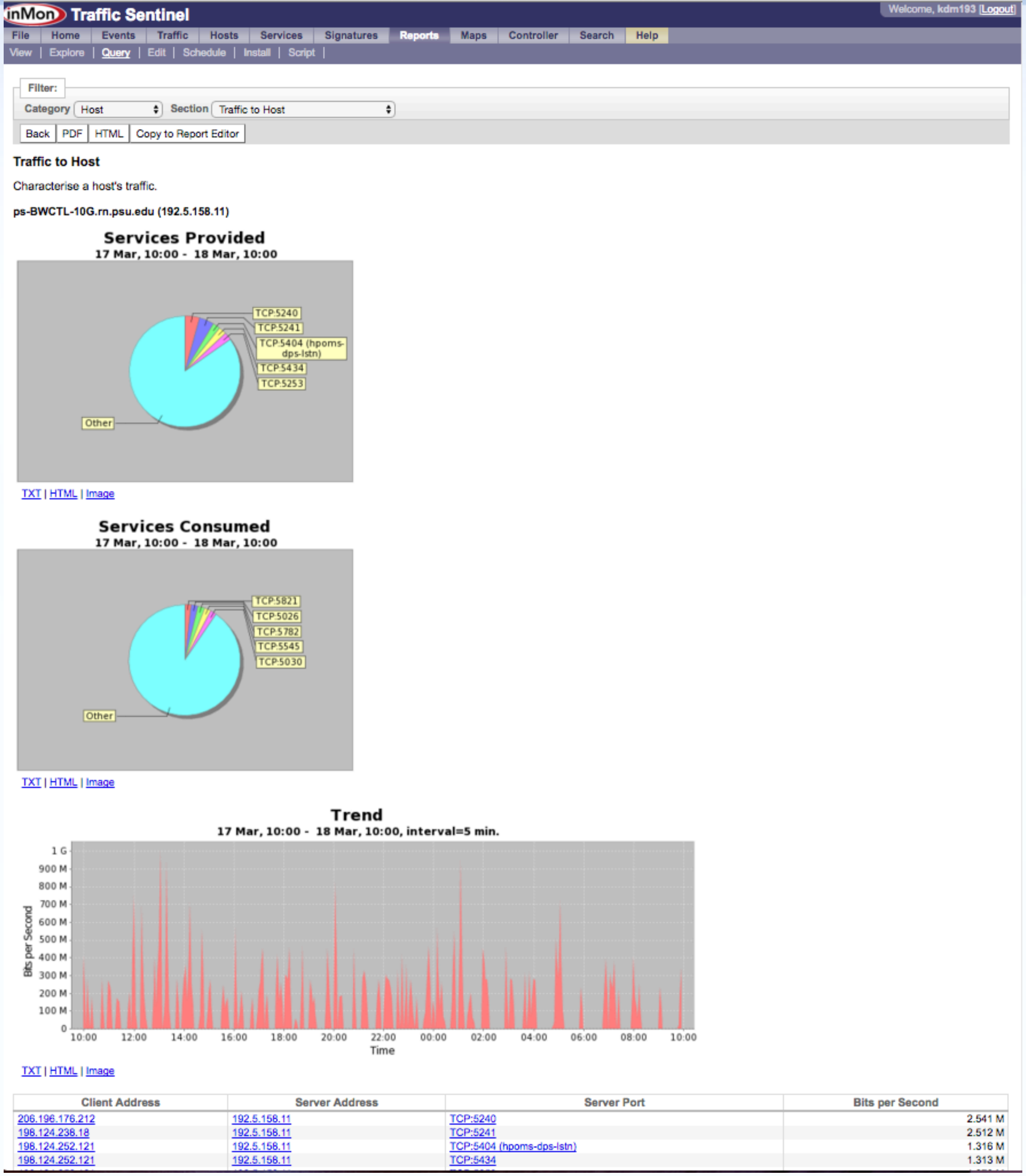
K.I.S.S.

- 3 questions have told us a lot
  - How much data do you have to move?
  - How do you move it now?
  - Where do you store it?
- Then, establish a baseline with:
  - How long does it take now?
  - How long do you think it should take?

From a baseline, pull stats

- From Central networking, do
  - SNMP interface counters
  - sFlow from Border, Core and possible edge
  - Top 10 v4/v6 based on sFlow border data
  - sFlow port and application data
  - If offsite,
    - run traceroute and perfSONAR reverse traceroute
- Now we have data to show the researcher, what they are doing.

Sample Researcher Report …


inMon Traffic Sentinel
Welcome, kdm193 [Logout]
File | Home | Events | Traffic | Hosts | Services | Signatures | Reports | Maps | Controller | Search | Help
View | Explore | Query | Edit | Schedule | Install | Script |
Back | PDF | HTML | Copy to Report Editor
TXT | HTML | Image

Filter:

Category: Host

Section: Traffic to Host

Traffic to Host

Characterise a host's traffic.

ps-BWCTL-10G.rn.psu.edu (192.5.158.11)

Services Provided

17 Mar, 10:00 - 18 Mar, 10:00

Services Consumed

17 Mar, 10:00 - 18 Mar, 10:00

Trend

17 Mar, 10:00 - 18 Mar, 10:00, interval=5 min.

Client Address	Server Address	Server Port	Bits per Second
206.196.176.212	192.5.158.11	TCP:5240	2.541 M
198.124.238.18	192.5.158.11	TCP:5241	2.512 M
198.124.252.121	192.5.158.11	TCP:5404 (hpoms-dps-lstn)	1.316 M
198.124.252.121	192.5.158.11	TCP:5434	1.313 M

Secure Researcher On-Boarding

- Engagement
  - Researcher Interview
    - Workflow
    - Data Source
    - Data Destination
    - Data Cat
      - Before Compute
      - After
  - Local IT Support
    - Policies
    - Configuration

- Guidelines/Compliance
  - ITS-SOS MOU
  - Risk Survey
  - Data Categorization
  - Minimum Security Baseline
  - Operating Level Agreements -OLA
  - Vulnerability Scanning
  - Host mitigation

Research Device Security

Host-Based

- Firewall
  - iptables, ip6tables, firewalld
- Host Intrusion Detection OSSEC
- Anti-Virus, Malware

Network

- Deny All then ACLs are built around researcher requirements
- RFC1918 private IPv4 to limit public access to workstations and servers
- Use IPv6 DTN for public IP and data transfer
- In the future:
  - MAC security per port
  - Research project/building specific VLANs

Researcher IT Best Practices

Department Level

- On-boarding
- Local Policies vs. central policies
- IT directors reporting to
  - Deans?
  - Finance?
  - Dept Head?

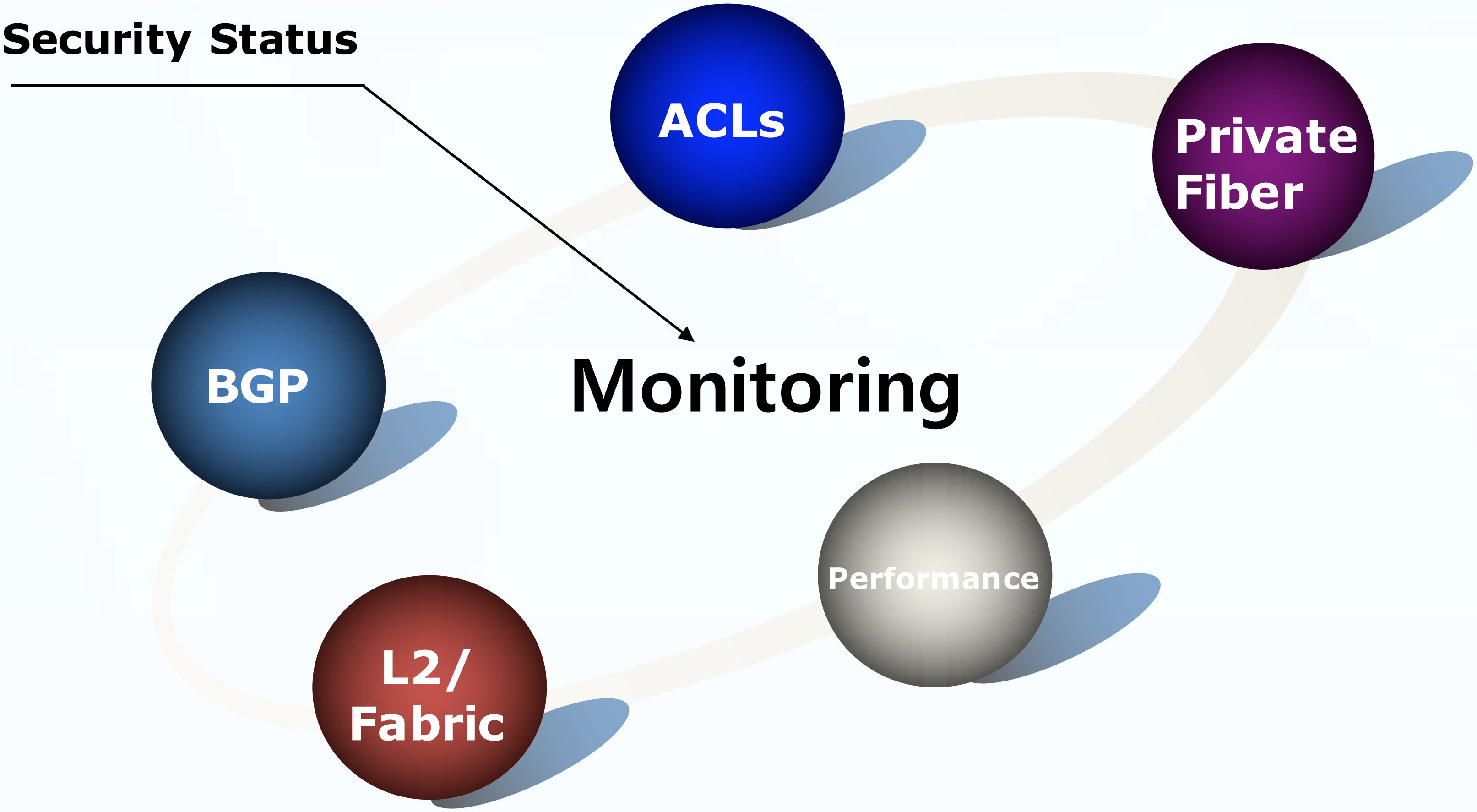
Stop Opt-Out

- Create an enabled exception
- Try to build to 80% of Researcher needs
- No dual homed machines

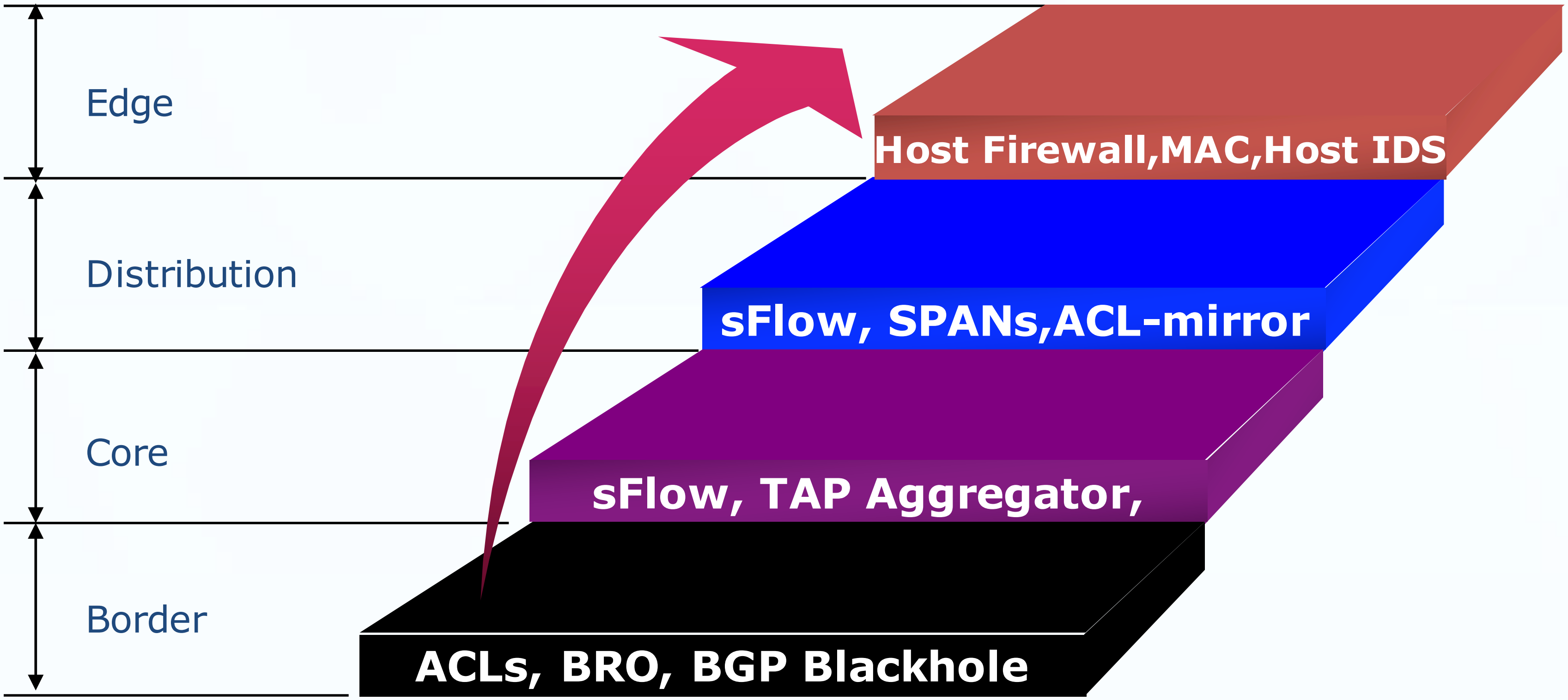
TrustedCI.org Peer Review with Utah

- http://trustedci.org/cc-nie/
- We Discussed:
  - Problems or Research bottlenecks
  - Design
  - Architecture
  - Host, Data, Network Security
- I HIGHLY recommend this.
- Contact CTSC Director Von Welch(vwelch@iu.edu) at the Center for Trustworthy Scientific Cyberinfrastructure

Secure DMZ Network



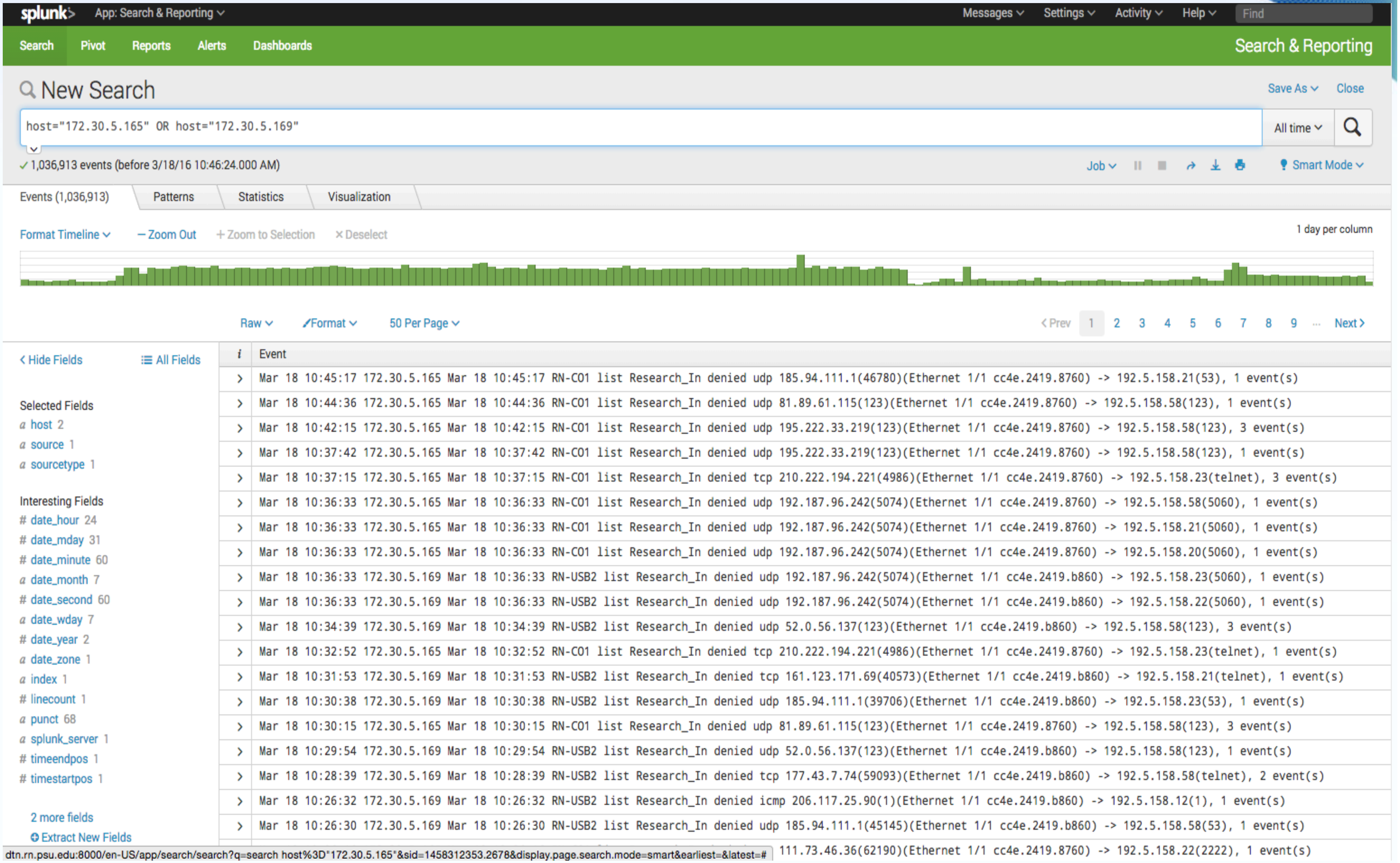
Next Steps


Edge
Distribution
Core
Border
Host Firewall,MAC,Host IDS
sFlow, SPANs,ACL-mirror
sFlow, TAP Aggregator,
ACLs, BRO, BGP Blackhole

Syslog ACL deny

```
sequence 15100 permit tcp any host 192.5.158.11 eq 61617 log
sequence 15101 permit tcp any host 192.5.158.11 eq 8090 log
sequence 15102 permit tcp any host 192.5.158.11 eq 8096 log
sequence 15103 permit tcp any host 192.5.158.11 eq 4823 log
sequence 15104 permit tcp any host 192.5.158.11 range 6001  6200 log
sequence 15105 permit udp any host 192.5.158.11 range 6001  6200 log
sequence 15106 permit tcp any host 192.5.158.11 range 5001  5900 log
sequence 15107 permit udp any host 192.5.158.11 range 5001  5900 log
sequence 15108 permit tcp any host 192.5.158.11 eq 861 log
sequence 15109 permit udp any host 192.5.158.11 range 8670  9960 log
sequence 15110 permit tcp any host 192.5.158.11 range 3001  3003 log
sequence 15111 permit tcp any host 192.5.158.11 eq 7123 log
sequence 15112 permit tcp any host 192.5.158.11 eq 8000 log
sequence 15113 permit tcp any host 192.5.158.11 range 8001  8020 log
sequence 15114 permit tcp any host 192.5.158.11 eq http log
sequence 15115 permit tcp any host 192.5.158.11 eq ssl log
sequence 15116 permit tcp any host 192.5.158.11 eq ssh log
sequence 15117 permit icmp any host 192.5.158.11 any-icmp-type log
sequence 15118 permit udp any host 192.5.158.11 range 33434  33634 log
sequence 15119 permit tcp any host 192.5.158.11 eq 8090 log
sequence 15120 deny any host 192.5.158.11 log
```

ACL syslog in splunk



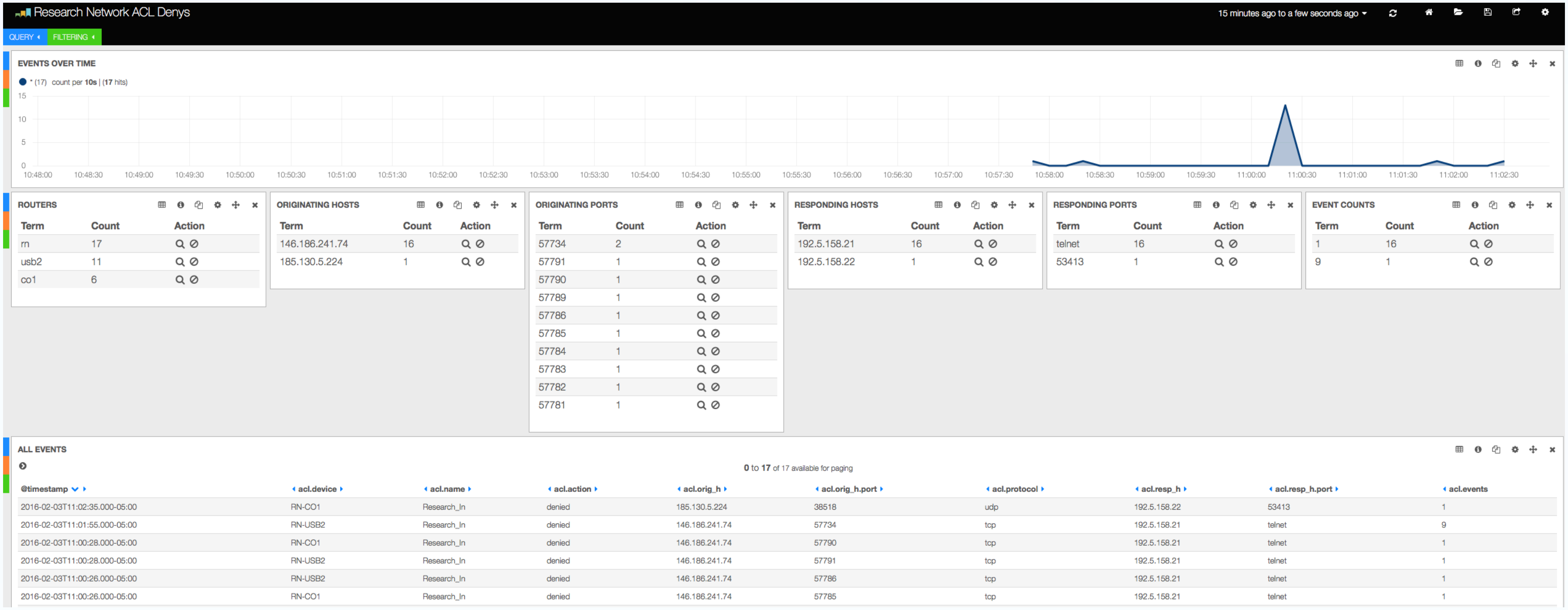
```
host="172.30.5.165" OR host="172.30.5.169"
```

✓ 1,036,913 events (before 3/18/16 10:46:24.000 AM)

```
Mar 18 10:45:17 172.30.5.165 Mar 18 10:45:17 RN-C01 list Research_In denied udp 185.94.111.1(46780)(Ethernet 1/1 cc4e.2419.8760) -> 192.5.158.21(53), 1 event(s)
Mar 18 10:44:36 172.30.5.165 Mar 18 10:44:36 RN-C01 list Research_In denied udp 81.89.61.115(123)(Ethernet 1/1 cc4e.2419.8760) -> 192.5.158.58(123), 1 event(s)
Mar 18 10:42:15 172.30.5.165 Mar 18 10:42:15 RN-C01 list Research_In denied udp 195.222.33.219(123)(Ethernet 1/1 cc4e.2419.8760) -> 192.5.158.58(123), 3 event(s)
Mar 18 10:37:42 172.30.5.165 Mar 18 10:37:42 RN-C01 list Research_In denied udp 195.222.33.219(123)(Ethernet 1/1 cc4e.2419.8760) -> 192.5.158.58(123), 1 event(s)
Mar 18 10:37:15 172.30.5.165 Mar 18 10:37:15 RN-C01 list Research_In denied tcp 210.222.194.221(4986)(Ethernet 1/1 cc4e.2419.8760) -> 192.5.158.23(telnet), 3 event(s)
Mar 18 10:36:33 172.30.5.165 Mar 18 10:36:33 RN-C01 list Research_In denied udp 192.187.96.242(5074)(Ethernet 1/1 cc4e.2419.8760) -> 192.5.158.58(5060), 1 event(s)
Mar 18 10:36:33 172.30.5.165 Mar 18 10:36:33 RN-C01 list Research_In denied udp 192.187.96.242(5074)(Ethernet 1/1 cc4e.2419.8760) -> 192.5.158.21(5060), 1 event(s)
Mar 18 10:36:33 172.30.5.165 Mar 18 10:36:33 RN-C01 list Research_In denied udp 192.187.96.242(5074)(Ethernet 1/1 cc4e.2419.8760) -> 192.5.158.20(5060), 1 event(s)
Mar 18 10:36:33 172.30.5.169 Mar 18 10:36:33 RN-USB2 list Research_In denied udp 192.187.96.242(5074)(Ethernet 1/1 cc4e.2419.b860) -> 192.5.158.23(5060), 1 event(s)
Mar 18 10:36:33 172.30.5.169 Mar 18 10:36:33 RN-USB2 list Research_In denied udp 192.187.96.242(5074)(Ethernet 1/1 cc4e.2419.b860) -> 192.5.158.22(5060), 1 event(s)
Mar 18 10:34:39 172.30.5.169 Mar 18 10:34:39 RN-USB2 list Research_In denied udp 52.0.56.137(123)(Ethernet 1/1 cc4e.2419.b860) -> 192.5.158.58(123), 3 event(s)
Mar 18 10:32:52 172.30.5.165 Mar 18 10:32:52 RN-C01 list Research_In denied tcp 210.222.194.221(4986)(Ethernet 1/1 cc4e.2419.8760) -> 192.5.158.23(telnet), 1 event(s)
Mar 18 10:31:53 172.30.5.169 Mar 18 10:31:53 RN-USB2 list Research_In denied tcp 161.123.171.69(40573)(Ethernet 1/1 cc4e.2419.b860) -> 192.5.158.21(telnet), 1 event(s)
Mar 18 10:30:38 172.30.5.169 Mar 18 10:30:38 RN-USB2 list Research_In denied udp 185.94.111.1(39706)(Ethernet 1/1 cc4e.2419.b860) -> 192.5.158.23(53), 1 event(s)
Mar 18 10:30:15 172.30.5.165 Mar 18 10:30:15 RN-C01 list Research_In denied udp 81.89.61.115(123)(Ethernet 1/1 cc4e.2419.8760) -> 192.5.158.58(123), 3 event(s)
Mar 18 10:29:54 172.30.5.169 Mar 18 10:29:54 RN-USB2 list Research_In denied udp 52.0.56.137(123)(Ethernet 1/1 cc4e.2419.b860) -> 192.5.158.58(123), 1 event(s)
Mar 18 10:28:39 172.30.5.169 Mar 18 10:28:39 RN-USB2 list Research_In denied tcp 177.43.7.74(59093)(Ethernet 1/1 cc4e.2419.b860) -> 192.5.158.58(telnet), 2 event(s)
Mar 18 10:26:32 172.30.5.169 Mar 18 10:26:32 RN-USB2 list Research_In denied icmp 206.117.25.90(1)(Ethernet 1/1 cc4e.2419.b860) -> 192.5.158.12(1), 1 event(s)
Mar 18 10:26:30 172.30.5.169 Mar 18 10:26:30 RN-USB2 list Research_In denied udp 185.94.111.1(45145)(Ethernet 1/1 cc4e.2419.b860) -> 192.5.158.58(53), 1 event(s)
111.73.46.36(62190)(Ethernet 1/1 cc4e.2419.8760) -> 192.5.158.22(2222), 1 event(s)
```

dtn.rn.psu.edu:8000/en-US/app/search/search?q=search host%3D"172.30.5.165"&sid=1458312353.2678&display.page.search.mode=smart&earliest=&latest=#

Science DMZ ACL syslog dashboard in ELK



ROUTERS

Term	Count	Action
rn	17	🔍 ⊘
usb2	11	🔍 ⊘
co1	6	🔍 ⊘

ORIGINATING HOSTS

Term	Count	Action
146.186.241.74	16	🔍 ⊘
185.130.5.224	1	🔍 ⊘

ORIGINATING PORTS

Term	Count	Action
57734	2	🔍 ⊘
57791	1	🔍 ⊘
57790	1	🔍 ⊘
57789	1	🔍 ⊘
57786	1	🔍 ⊘
57785	1	🔍 ⊘
57784	1	🔍 ⊘
57783	1	🔍 ⊘
57782	1	🔍 ⊘
57781	1	🔍 ⊘

RESPONDING HOSTS

Term	Count	Action
192.5.158.21	16	🔍 ⊘
192.5.158.22	1	🔍 ⊘

RESPONDING PORTS

Term	Count	Action
telnet	16	🔍 ⊘
53413	1	🔍 ⊘

EVENT COUNTS

Term	Count	Action
1	16	🔍 ⊘
9	1	🔍 ⊘

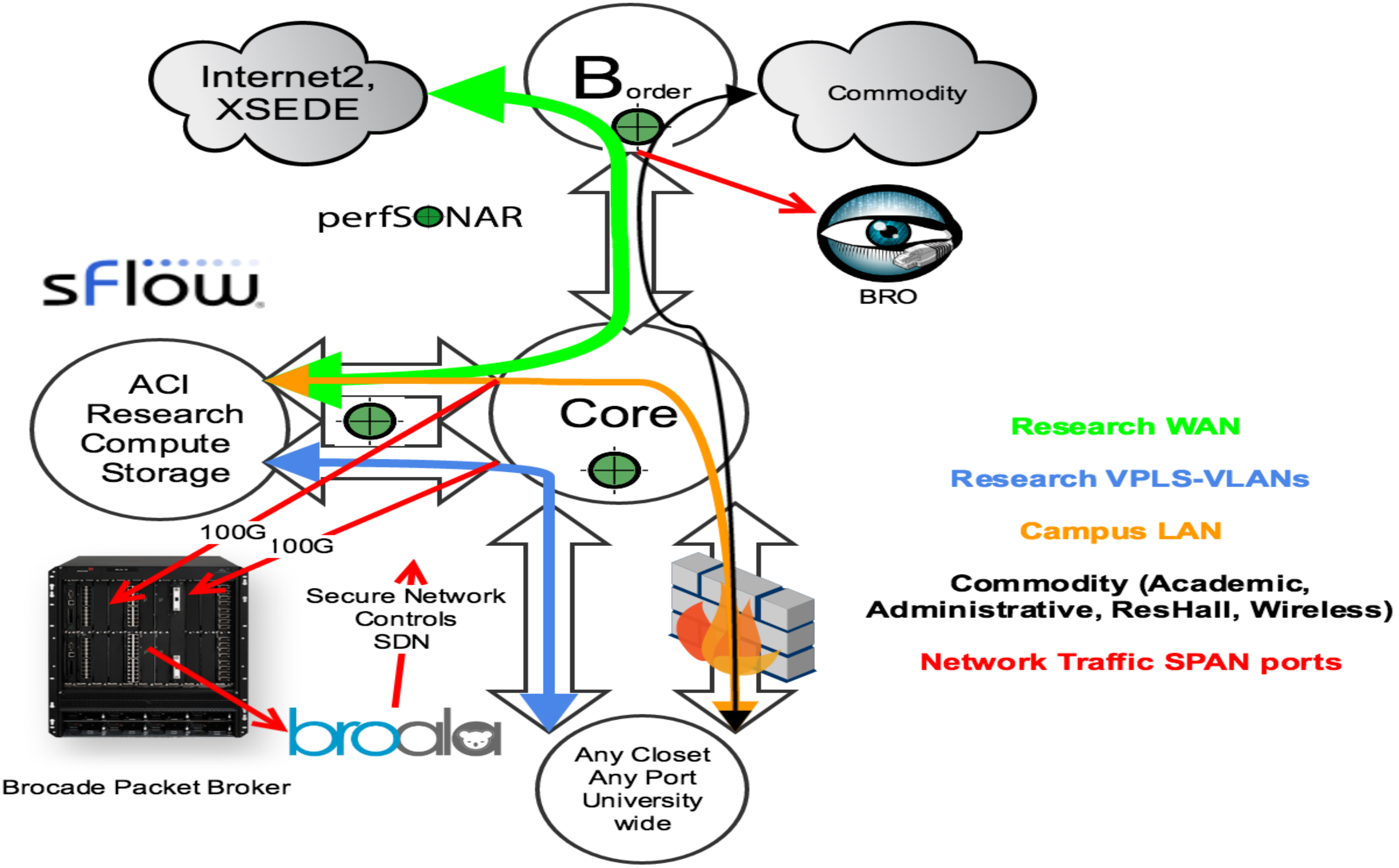
ALL EVENTS

0 to **17** of 17 available for paging

@timestamp	acl.device	acl.name	acl.action	acl.orig_h	acl.orig_h.port	acl.protocol	acl.resp_h	acl.resp_h.port	acl.events
2016-02-03T11:02:35.000-05:00	RN-CO1	Research_In	denied	185.130.5.224	38518	udp	192.5.158.22	53413	1
2016-02-03T11:01:55.000-05:00	RN-USB2	Research_In	denied	146.186.241.74	57734	tcp	192.5.158.21	telnet	9
2016-02-03T11:00:28.000-05:00	RN-CO1	Research_In	denied	146.186.241.74	57790	tcp	192.5.158.21	telnet	1
2016-02-03T11:00:28.000-05:00	RN-USB2	Research_In	denied	146.186.241.74	57791	tcp	192.5.158.21	telnet	1
2016-02-03T11:00:26.000-05:00	RN-USB2	Research_In	denied	146.186.241.74	57786	tcp	192.5.158.21	telnet	1
2016-02-03T11:00:26.000-05:00	RN-CO1	Research_In	denied	146.186.241.74	57785	tcp	192.5.158.21	telnet	1

Network Visibility and Analytics

Penn State Science DMZ and Research Network connecting ACI anywhere



Research WAN

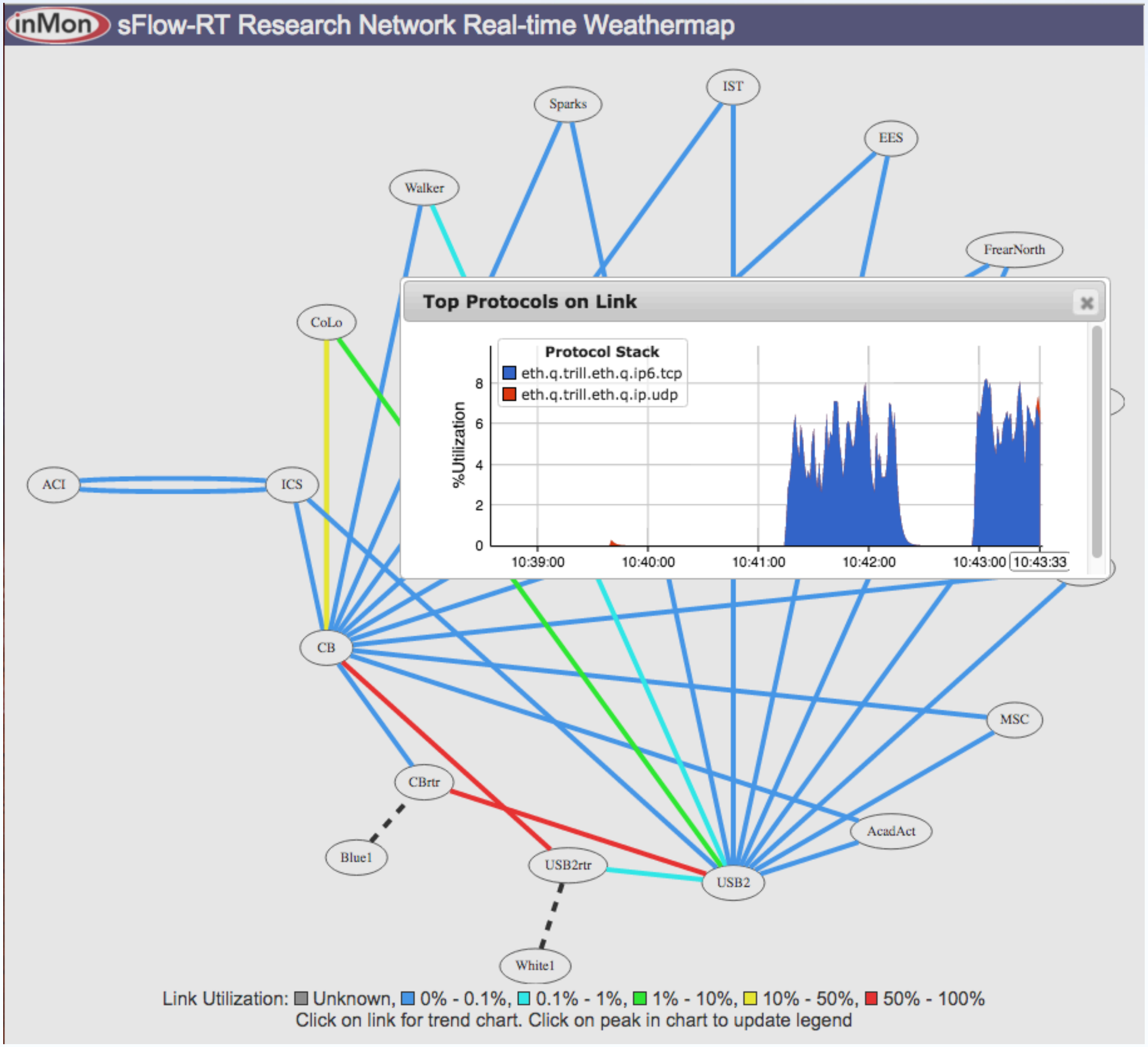
Research VPLS-VLANs

Campus LAN

Commodity (Academic, Administrative, ResHall, Wireless)

Network Traffic SPAN ports

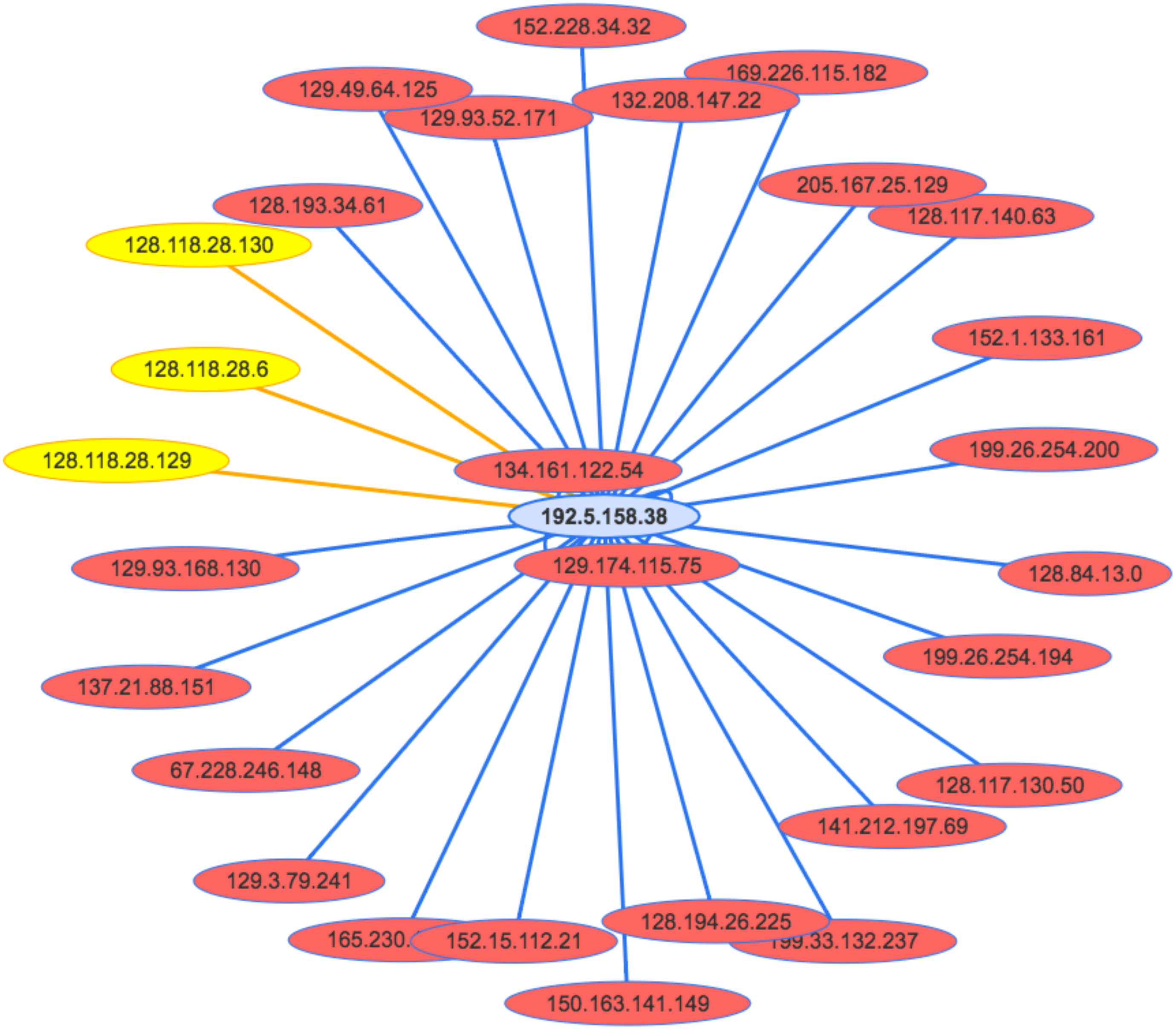
sFlow-RT Real-time Weathermaps



sFlow-RT Research Network Real-time Weathermap

Link Utilization: ◼ Unknown, 🟦 0% - 0.1%, 🟦 0.1% - 1%, 🟩 1% - 10%, 🟨 10% - 50%, 🟥 50% - 100%
Click on link for trend chart. Click on peak in chart to update legend

sFlow Real-time Connections to Host



The Host node is colored Blue

Yellow nodes on the Penn State enterprise network, but outside of the Science DMZ

Red nodes are connections established from outside Penn State.

After the grant…

Building on the Science DMZ idea

Grant connected 12 buildings with 2x10G fiber uplinks back to each data center and HPC compute/storage.

How can we take what we learned and expand to connect more researcher?

How do we turn seed money into a scalable enterprise service?

Building a build/service model

- Lifecycle funding with equipment refresh
- Boilerplate documentation of Science DMZ capabilities and connectivity for future researcher grants
- Offer and Support multiple options for
  - Data Transfer Speed
  - Cost effective
  - Data Security
  - Data Compliance
- Service Governance from customer base

Science DMZ as a Service options

1. 48 1/10G VDX fabric switch with 2-10G fiber uplinks back to the RN
   - ~$200 per month + Fiber + ports
   - 10G fiber server port ~$15/month
   - 1G copper server port ~$.57/m
2. 1/10G uplinks in Computer Building and UP Data Center (working on Hershey)
   - 10G fiber server port ~$15/month
   - 1G copper server port ~$.57/m

Science DMZ as a Service options

3. 24 or 48 ports switch with a 1/10G uplink VLAN’d back to Science DMZ.
   - $50-70 per month with $0/ports
   - Private VLANs can be offered per data type, data compliance, or joining department's
4. ~ $4 Per port on converged switch stacks.
   - Again, private VLANs can be offered

RESEARCH COMPUTING AND CYBERINFRASTRUCTURE

RCCI Shared Governance of Research Computing and Cyberinfrastructure

- Advisory Council for Research Computing and Cyberinfrastructure
- Executive Committee for Research Computing and Cyberinfrastructure
- Senior Advisor for Research Computing and Cyberinfrastructure
  - Aka, the Research Guru
- Working Groups

RCCI Working Groups

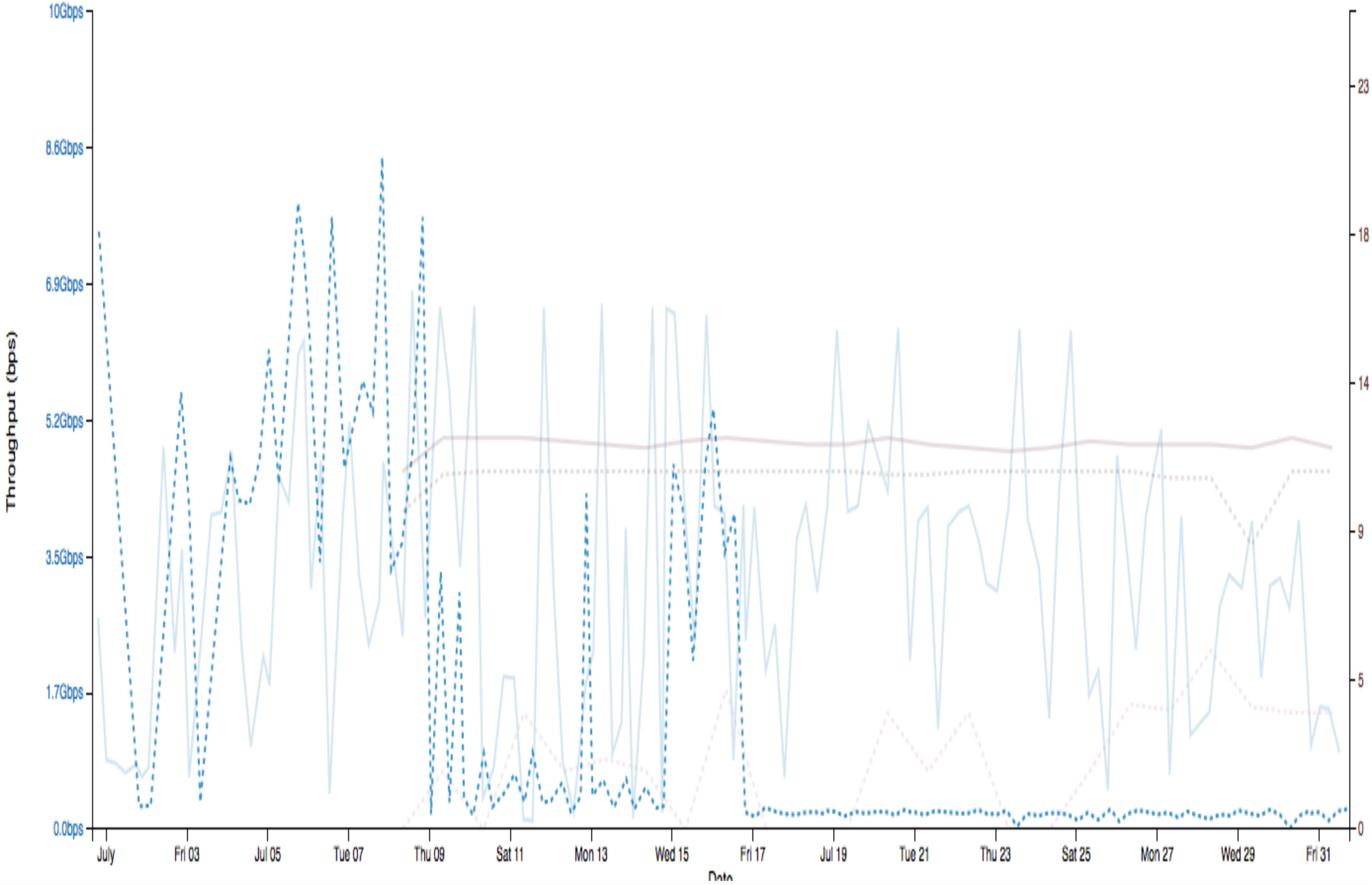
- The **Data Centers Working Group** provides input into the processes and policies of the University's Data Centers.
- The **Data Governance Working Group** focuses on issues surrounding data, data governance, data preservation, data dissemination, data security, and managing the scientific data life cycle.
- The **High-Performance Computing Working Group** focuses on issues surrounding HPC at Penn State.
- The **IT/HR Job Classification and Compensation Working Group** considers issues of IT job classification and compensation, with an eye on ensuring that Penn State can attract and retain highly-qualified IT professionals with skills appropriate to supporting research.
- The **Research Network and Data Classification Policies Working Group** examines parameters and plans for access to the new high-speed Research Network.
- The **Software Working Group** will ease the identification and acquisition of software by researchers.

Opportunities

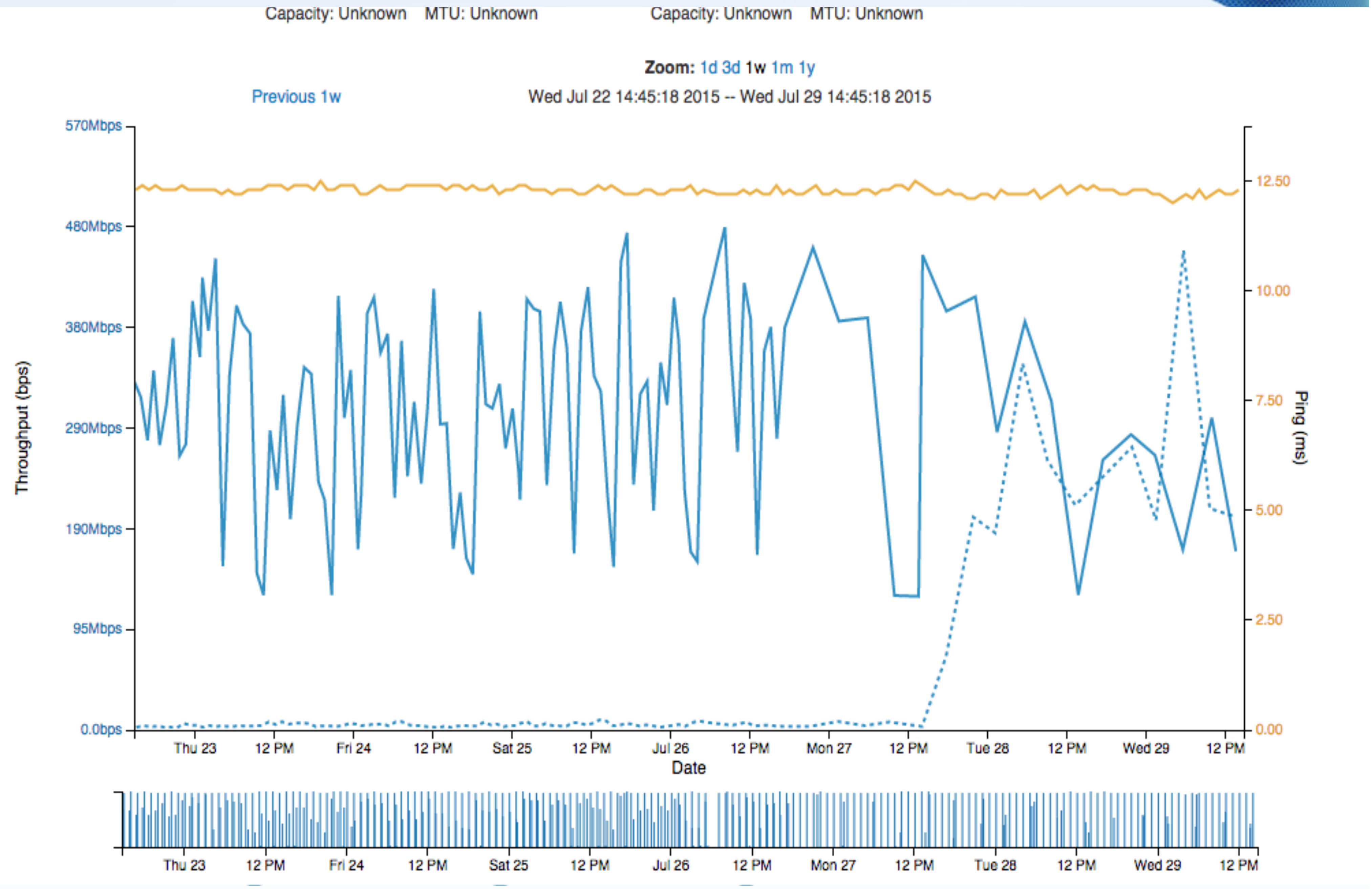
Opportunities

- Network as an instrument
  - Measurement with perfSONAR
  - Monitoring with sFlow
- Interactive sessions on fast network
- PSU firewalls all over with no consistency
- Data Transfer Applications vary by group or experience
- Outreach

Poor performance after router code upgrade



perfSONAR found bad fiber



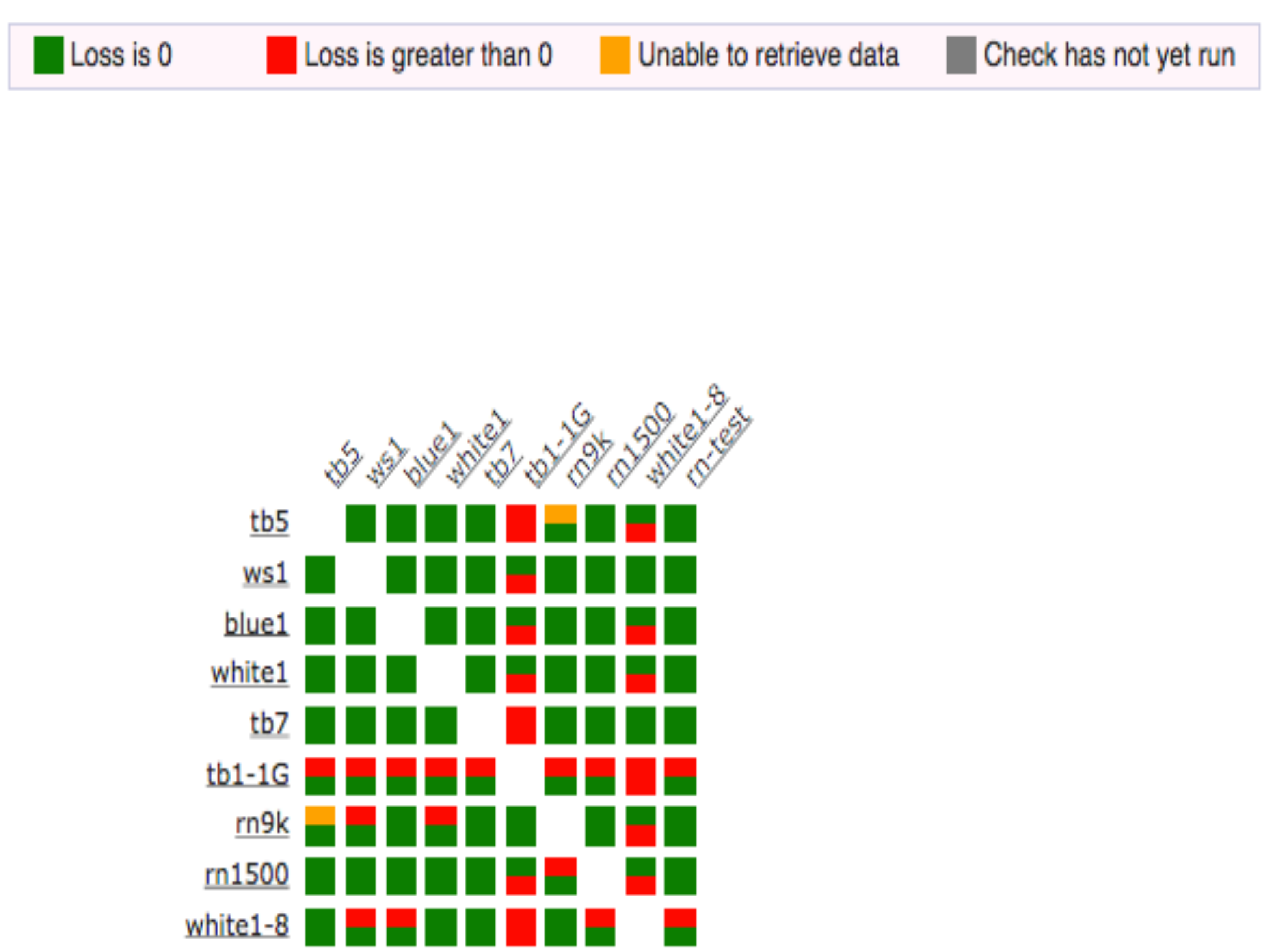
Capacity: Unknown MTU: Unknown Capacity: Unknown MTU: Unknown

Zoom: 1d 3d 1w 1m 1y

Previous 1w

Wed Jul 22 14:45:18 2015 -- Wed Jul 29 14:45:18 2015

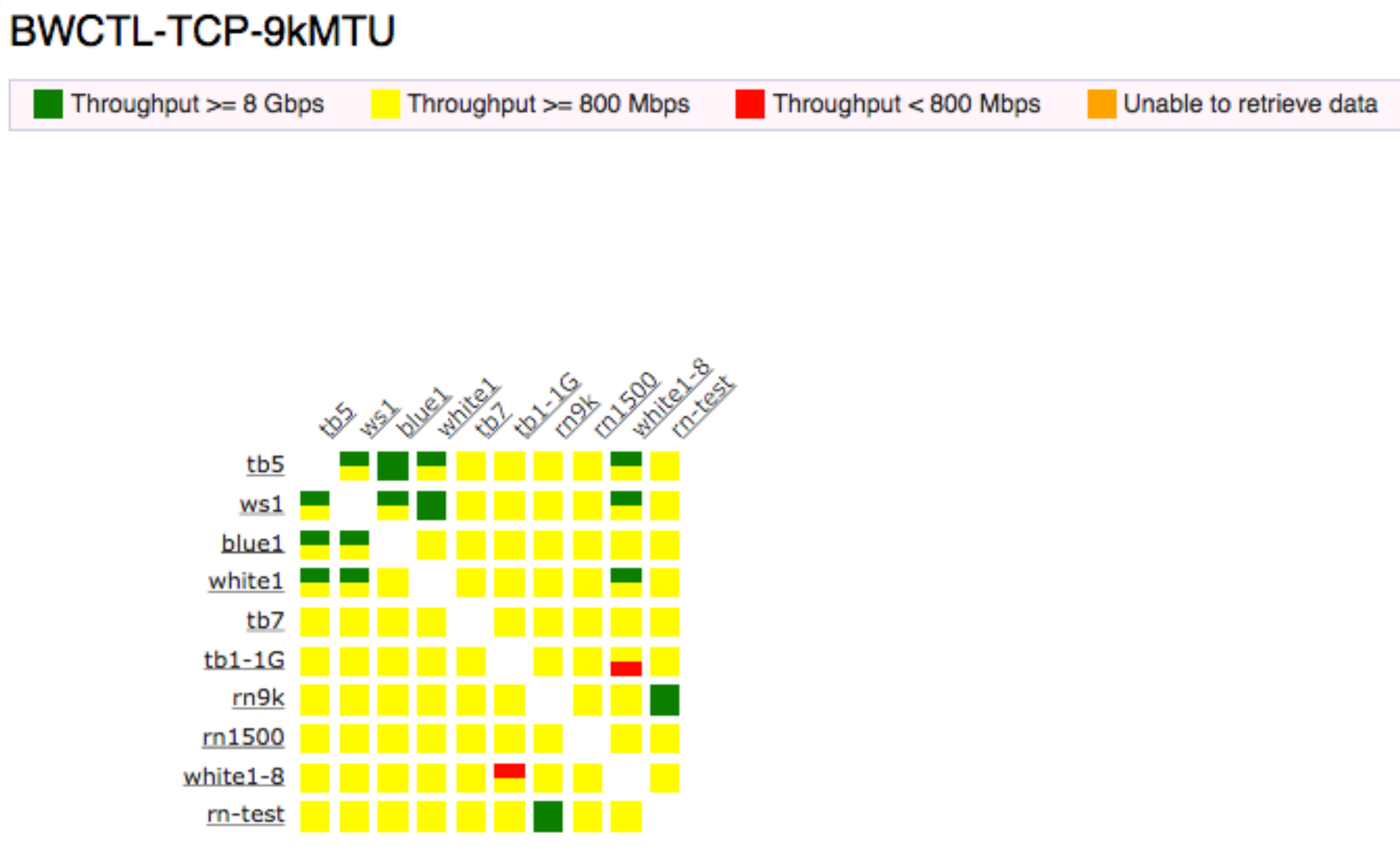
OWAMP Dashboard



🟩 Loss is 0 🟥 Loss is greater than 0 🟧 Unable to retrieve data ⬛ Check has not yet run

	tb5	ws1	blue1	white1	tb7	tb1-1G	rn9k	rn1500	white1-8	rn-test
tb5		🟩	🟩	🟩	🟩	🟥	🟧🟩	🟩	🟩🟥	🟩
ws1	🟩		🟩	🟩	🟩	🟩🟥	🟩	🟩	🟩	🟩
blue1	🟩	🟩		🟩	🟩	🟩🟥	🟩	🟩	🟩🟥	🟩
white1	🟩	🟩	🟩		🟩	🟩🟥	🟩	🟩	🟩🟥	🟩
tb7	🟩	🟩	🟩	🟩		🟥	🟩	🟩	🟩	🟩
tb1-1G	🟥🟩	🟥🟩	🟥🟩	🟥🟩	🟥🟩		🟥🟩	🟥🟩	🟥	🟥🟩
rn9k	🟧🟩	🟥🟩	🟩	🟥🟩	🟩	🟩		🟩	🟩🟥	🟩
rn1500	🟩	🟩	🟩	🟩	🟩	🟩🟥	🟥🟩		🟩🟥	🟩
white1-8	🟩	🟥🟩	🟥🟩	🟩	🟩	🟥	🟩	🟥🟩		🟥🟩

BWCTL Dashboard

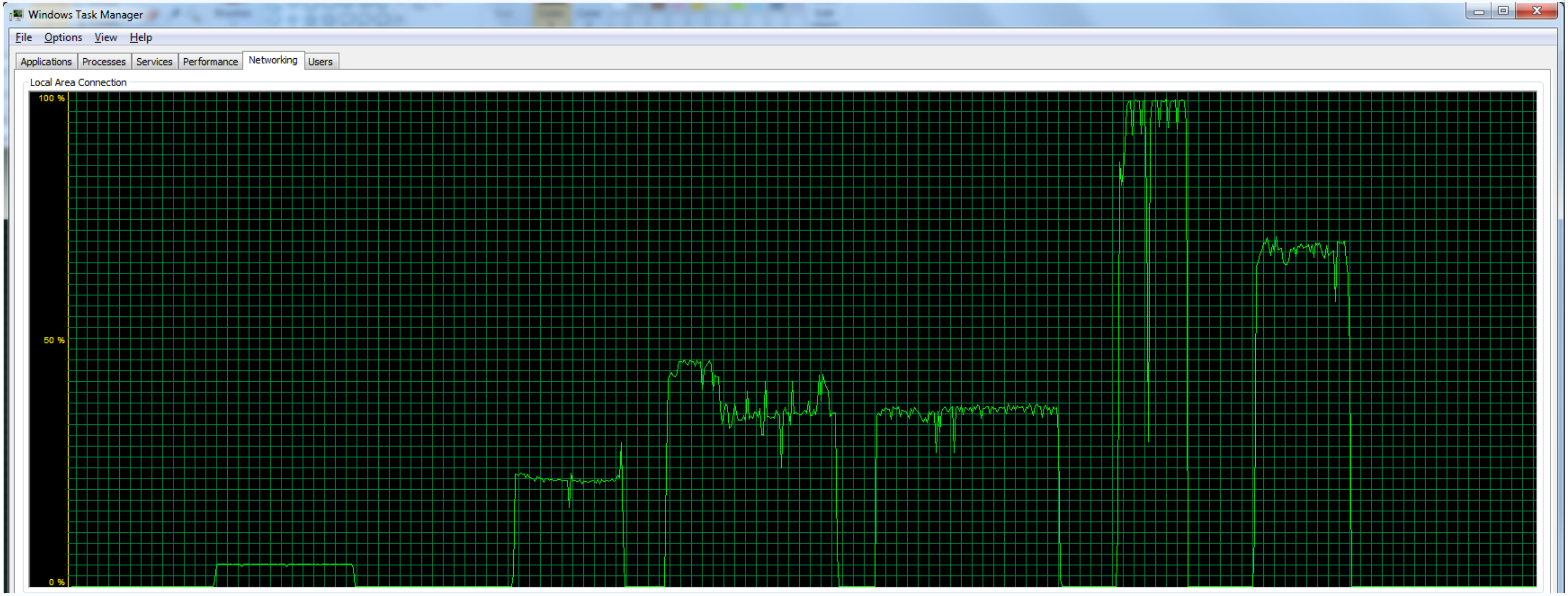


BWCTL-TCP-9kMTU

🟩 Throughput >= 8 Gbps 🟨 Throughput >= 800 Mbps 🟥 Throughput < 800 Mbps 🟧 Unable to retrieve data

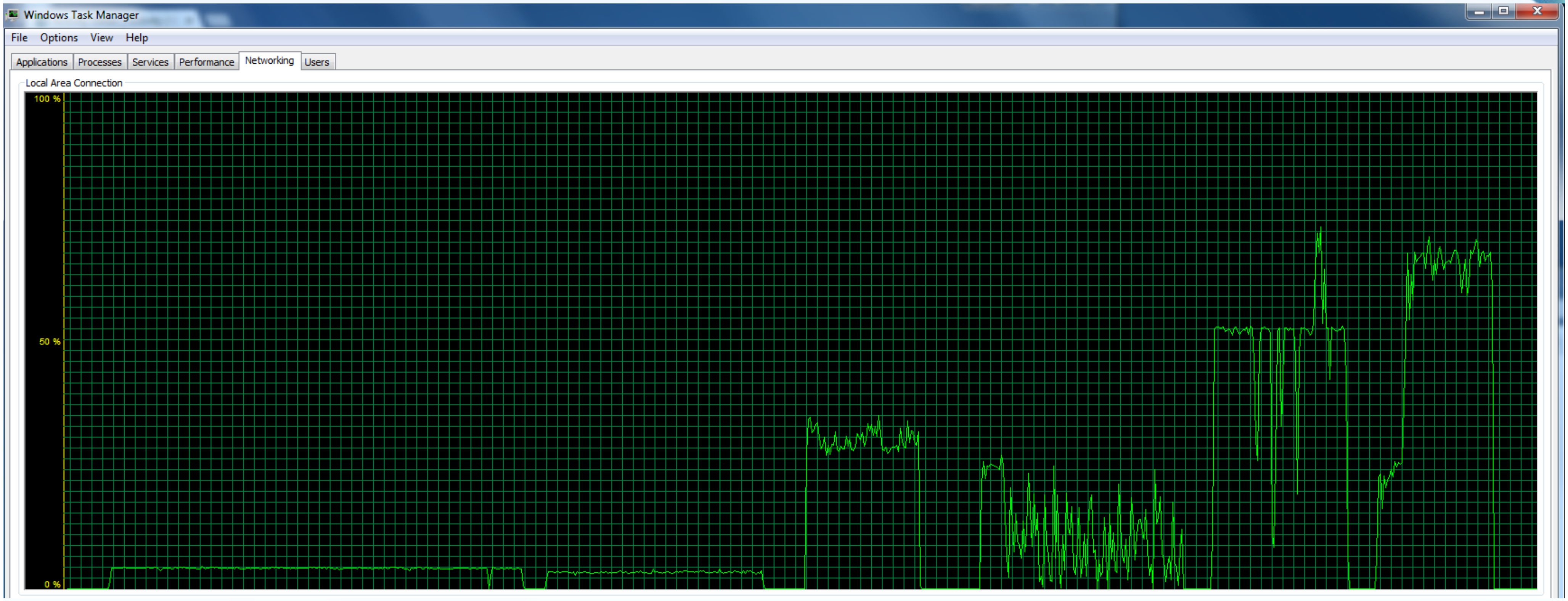
	tb5	ws1	blue1	white1	tb7	tb1-1G	rn9k	rn1500	white1-8	rn-test
tb5		🟩🟨	🟩	🟩🟨	🟨	🟨	🟨	🟨	🟩🟨	🟨
ws1	🟩🟨		🟩🟨	🟩	🟨	🟨	🟨	🟨	🟩🟨	🟨
blue1	🟩🟨	🟩🟨		🟨	🟨	🟨	🟨	🟨	🟨	🟨
white1	🟩🟨	🟩🟨	🟨		🟨	🟨	🟨	🟨	🟩🟨	🟨
tb7	🟨	🟨	🟨	🟨		🟨	🟨	🟨	🟨	🟨
tb1-1G	🟨	🟨	🟨	🟨	🟨		🟨	🟨	🟨🟥	🟨
rn9k	🟨	🟨	🟨	🟨	🟨	🟨		🟨	🟨	🟩
rn1500	🟨	🟨	🟨	🟨	🟨	🟨	🟨		🟨	🟨
white1-8	🟨	🟨	🟨	🟨	🟨	🟥🟨	🟨	🟨		🟨
rn-test	🟨	🟨	🟨	🟨	🟨	🟨	🟩	🟨	🟨	

Windows 7 Application Uploads



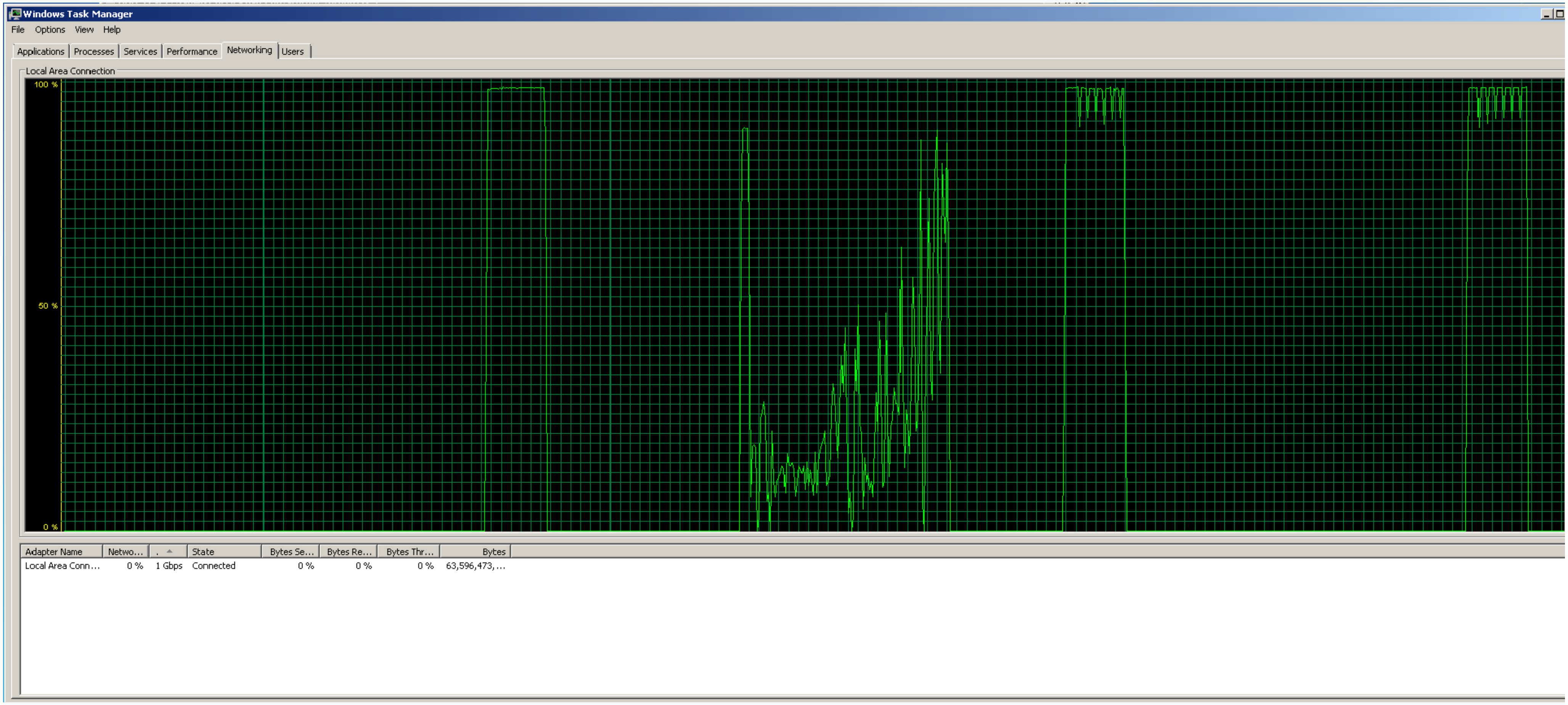
- ACI:SSHFS, Secure Shell, SFTP, NetDrive, Globus), PASS

Windows 7 Application Downloads



SSHFS, Secure Shell, SFTP, NetDrive, Globus, PASS

Windows 7 SSD to ACI GPFS & NAS



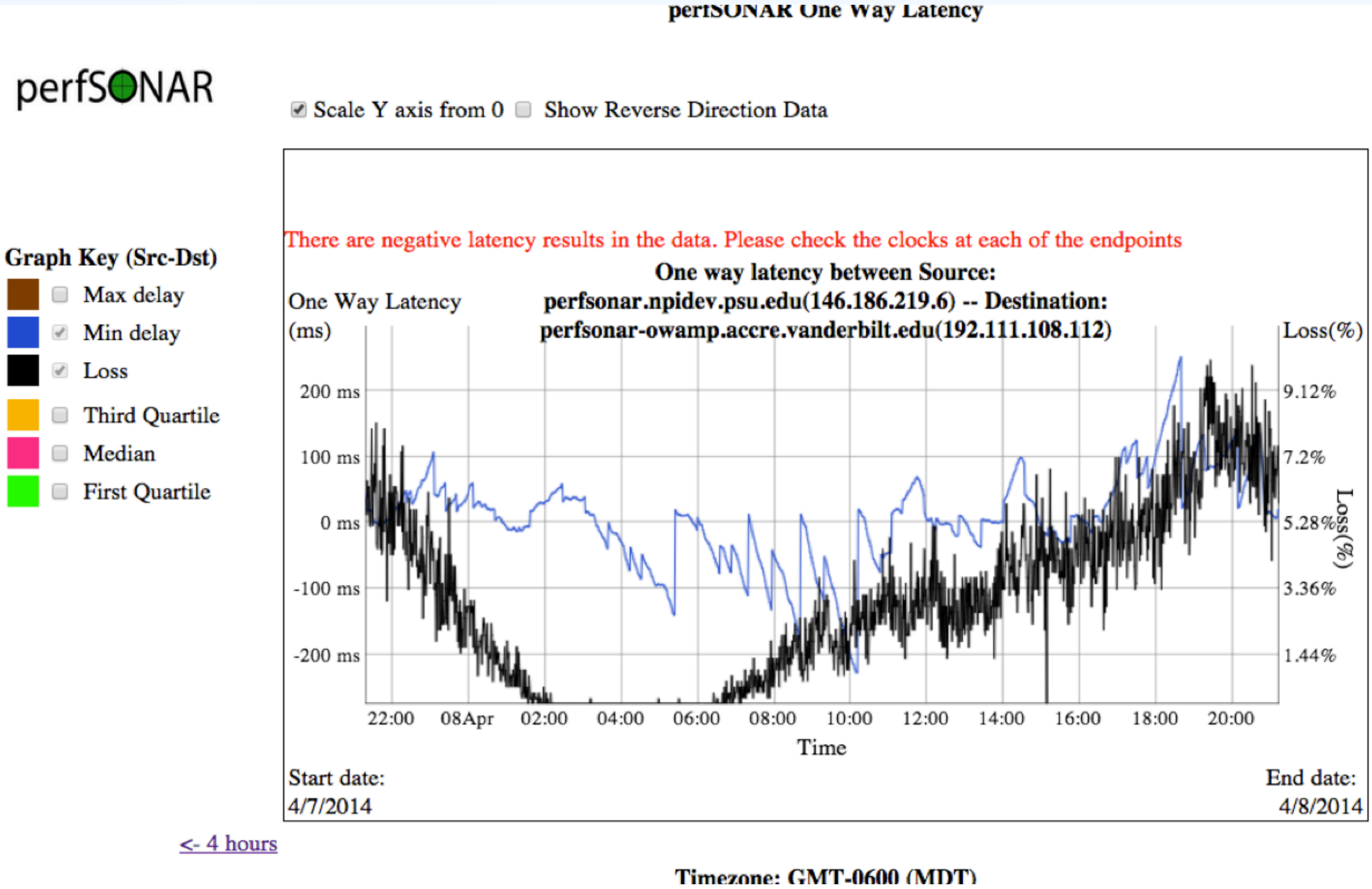
Adapter Name	Netwo...	.	State	Bytes Se...	Bytes Re...	Bytes Thr...	Bytes
Local Area Conn...	0 %	1 Gbps	Connected	0 %	0 %	0 %	63,596,473,...

Wins

PennState to Vanderbilt transfer

- Vanderbilt BioInformatics transfer
  - 14 days down to 30 hours
- Higher resolution Meteorology data
  - Ability to handle larger data set as well as multiple times a day
  - Ability to also distribute data from Penn State
- Internet preference set to Research first, commodity second
- Detecting network loss outside of PennState

One-way Latency through Philadelphia



perfSONAR One Way Latency

perfSONAR

☑ Scale Y axis from 0 □ Show Reverse Direction Data

There are negative latency results in the data. Please check the clocks at each of the endpoints

Graph Key (Src-Dst)

🟫	□	Max delay
🟦	☑	Min delay
⬛	☑	Loss
🟧	□	Third Quartile
🟥	□	Median
🟩	□	First Quartile

One way latency between Source: perfsonar.npidev.psu.edu(146.186.219.6) -- Destination: perfsonar-owamp.accre.vanderbilt.edu(192.111.108.112)

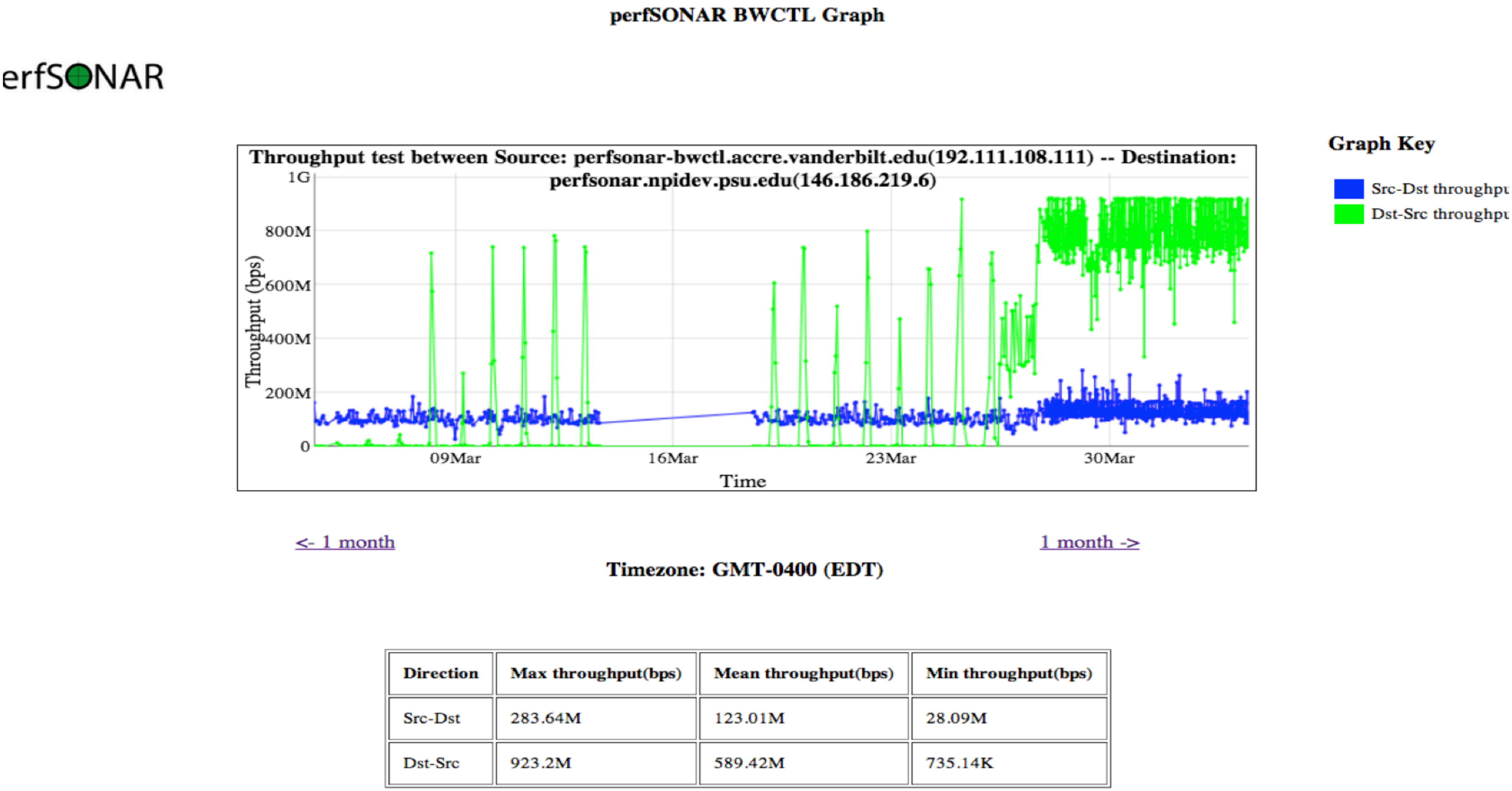
Start date: 4/7/2014

End date: 4/8/2014

<- 4 hours

Timezone: GMT-0600 (MDT)

Routing change to prefer Internet2



perfSONAR BWCTL Graph

erfSONAR
Throughput test between Source: perfsonar-bwctl.accre.vanderbilt.edu(192.111.108.111) -- Destination: perfsonar.npidev.psu.edu(146.186.219.6)
Throughput (bps)
1G
800M
600M
400M
200M
0
09Mar
16Mar
23Mar
30Mar
Time
Graph Key
Src-Dst throughpu
Dst-Src throughpu

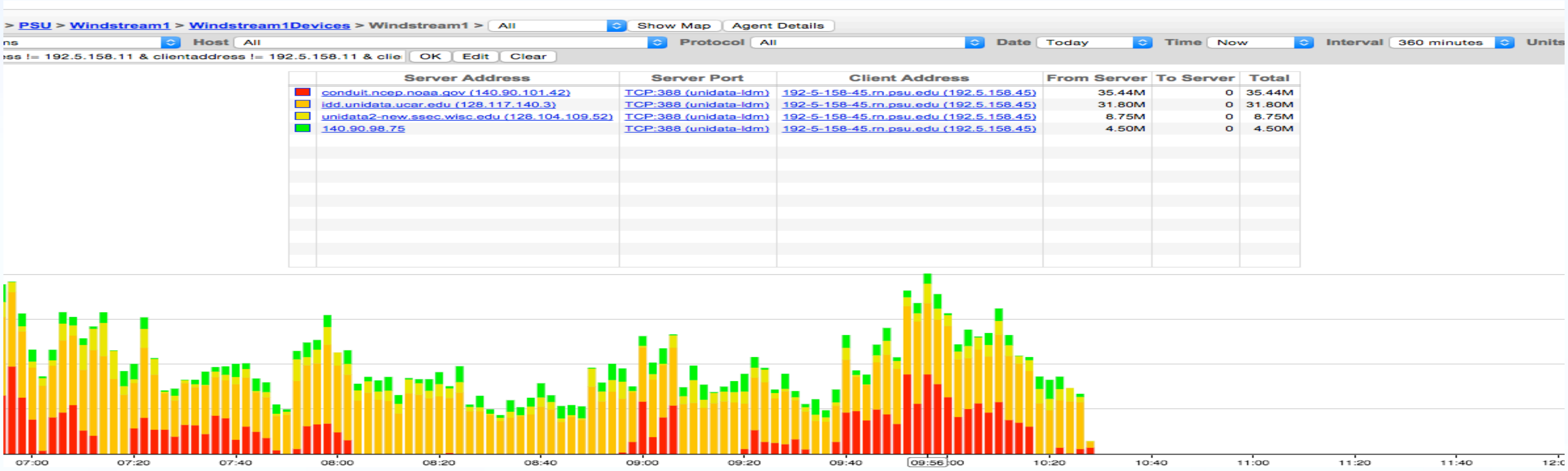
<- 1 month

1 month ->

Timezone: GMT-0400 (EDT)

Direction	Max throughput(bps)	Mean throughput(bps)	Min throughput(bps)
Src-Dst	283.64M	123.01M	28.09M
Dst-Src	923.2M	589.42M	735.14K

Research Route Optimization with Internet2

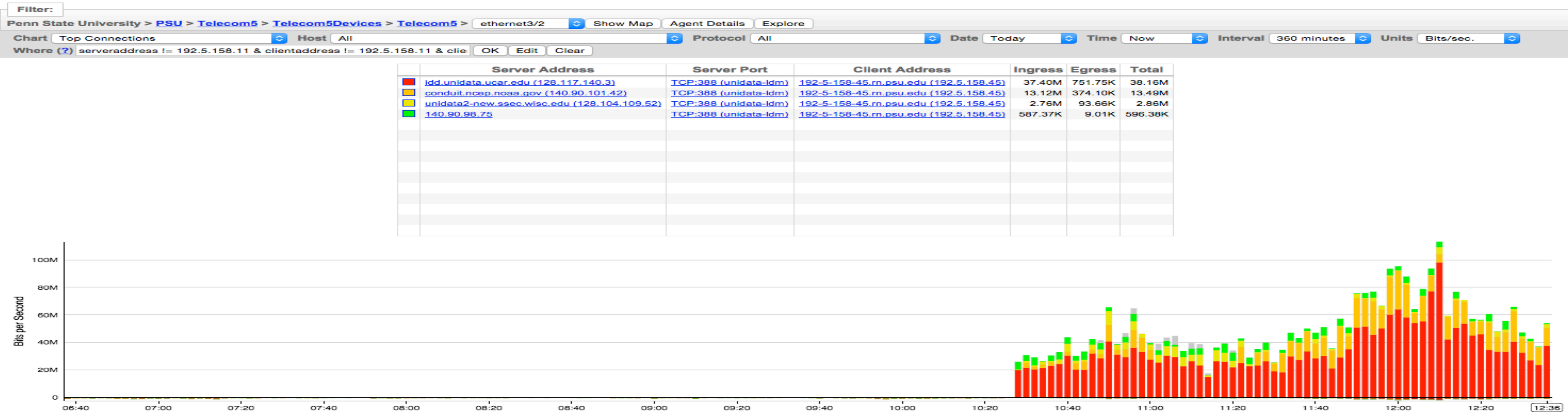


> PSU > Windstream1 > Windstream1Devices > Windstream1 > All

ns | Host: All | Protocol: All | Date: Today | Time: Now | Interval: 360 minutes | Units

ess != 192.5.158.11 & clientaddress != 192.5.158.11 & clie

	Server Address	Server Port	Client Address	From Server	To Server	Total
🟥	conduit.ncep.noaa.gov (140.90.101.42)	TCP:388 (unidata-ldm)	192-5-158-45.rn.psu.edu (192.5.158.45)	35.44M	0	35.44M
🟧	idd.unidata.ucar.edu (128.117.140.3)	TCP:388 (unidata-ldm)	192-5-158-45.rn.psu.edu (192.5.158.45)	31.80M	0	31.80M
🟨	unidata2-new.ssec.wisc.edu (128.104.109.52)	TCP:388 (unidata-ldm)	192-5-158-45.rn.psu.edu (192.5.158.45)	8.75M	0	8.75M
🟩	140.90.98.75	TCP:388 (unidata-ldm)	192-5-158-45.rn.psu.edu (192.5.158.45)	4.50M	0	4.50M



Filter:

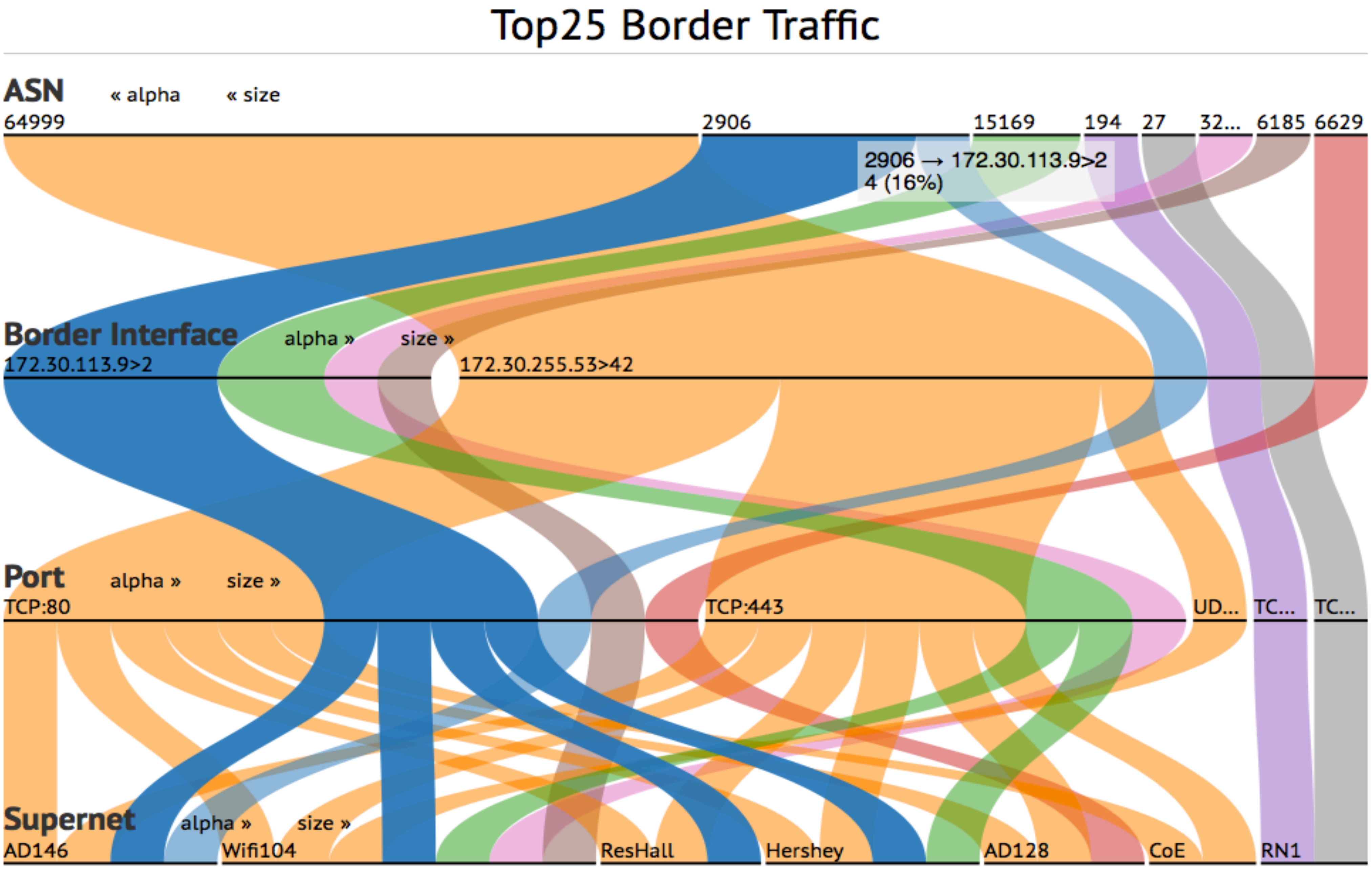
Penn State University > PSU > Telecom5 > Telecom5Devices > Telecom5 > ethernet3/2

Chart: Top Connections | Host: All | Protocol: All | Date: Today | Time: Now | Interval: 360 minutes | Units: Bits/sec.

Where (?) serveraddress != 192.5.158.11 & clientaddress != 192.5.158.11 & clie

	Server Address	Server Port	Client Address	Ingress	Egress	Total
🟥	idd.unidata.ucar.edu (128.117.140.3)	TCP:388 (unidata-ldm)	192-5-158-45.rn.psu.edu (192.5.158.45)	37.40M	751.75K	38.16M
🟧	conduit.ncep.noaa.gov (140.90.101.42)	TCP:388 (unidata-ldm)	192-5-158-45.rn.psu.edu (192.5.158.45)	13.12M	374.10K	13.49M
🟨	unidata2-new.ssec.wisc.edu (128.104.109.52)	TCP:388 (unidata-ldm)	192-5-158-45.rn.psu.edu (192.5.158.45)	2.76M	93.66K	2.86M
🟩	140.90.98.75	TCP:388 (unidata-ldm)	192-5-158-45.rn.psu.edu (192.5.158.45)	587.37K	9.01K	596.38K

sFlow Top25 Flows

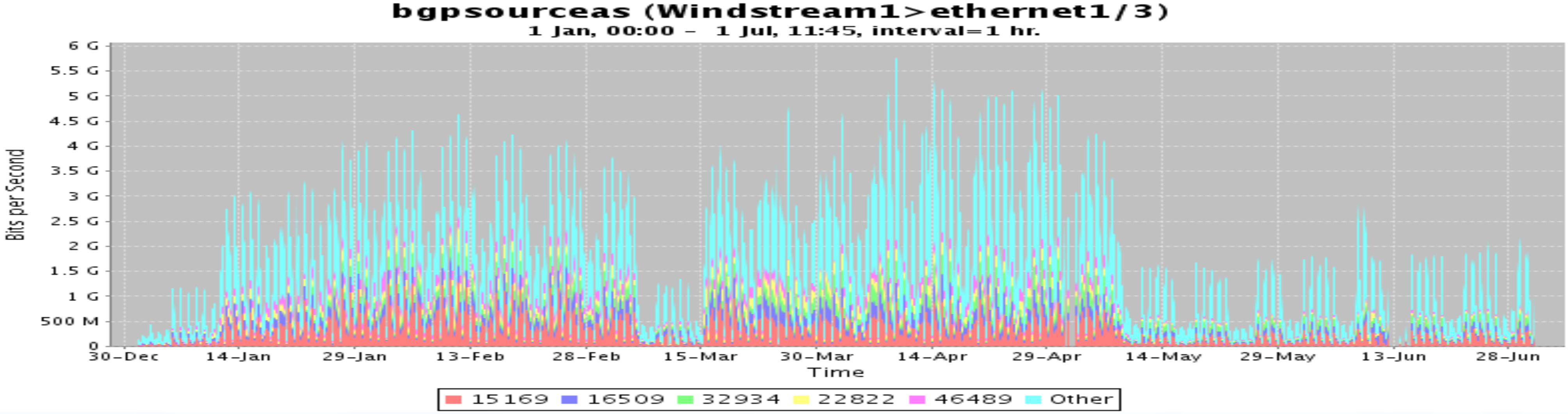


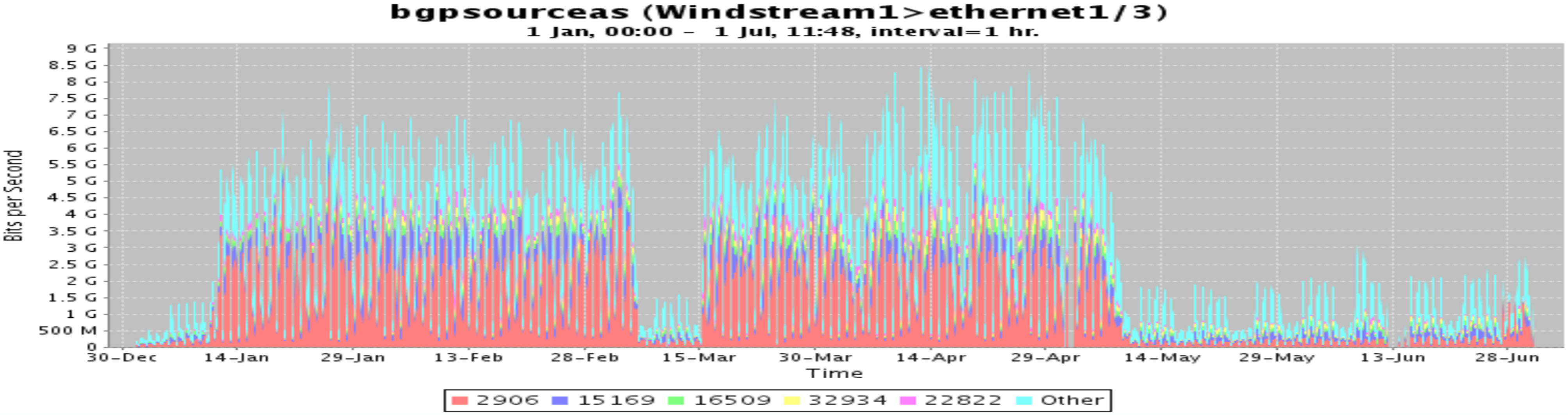
Top25 Border Traffic

Application Latency

- Application Metrics - Do your protocols support IPv6?
- DNS
- Email
- www/http/https
- DHCP
- NTP
- SSH
- LDAP

Transfers Compete with Netflix



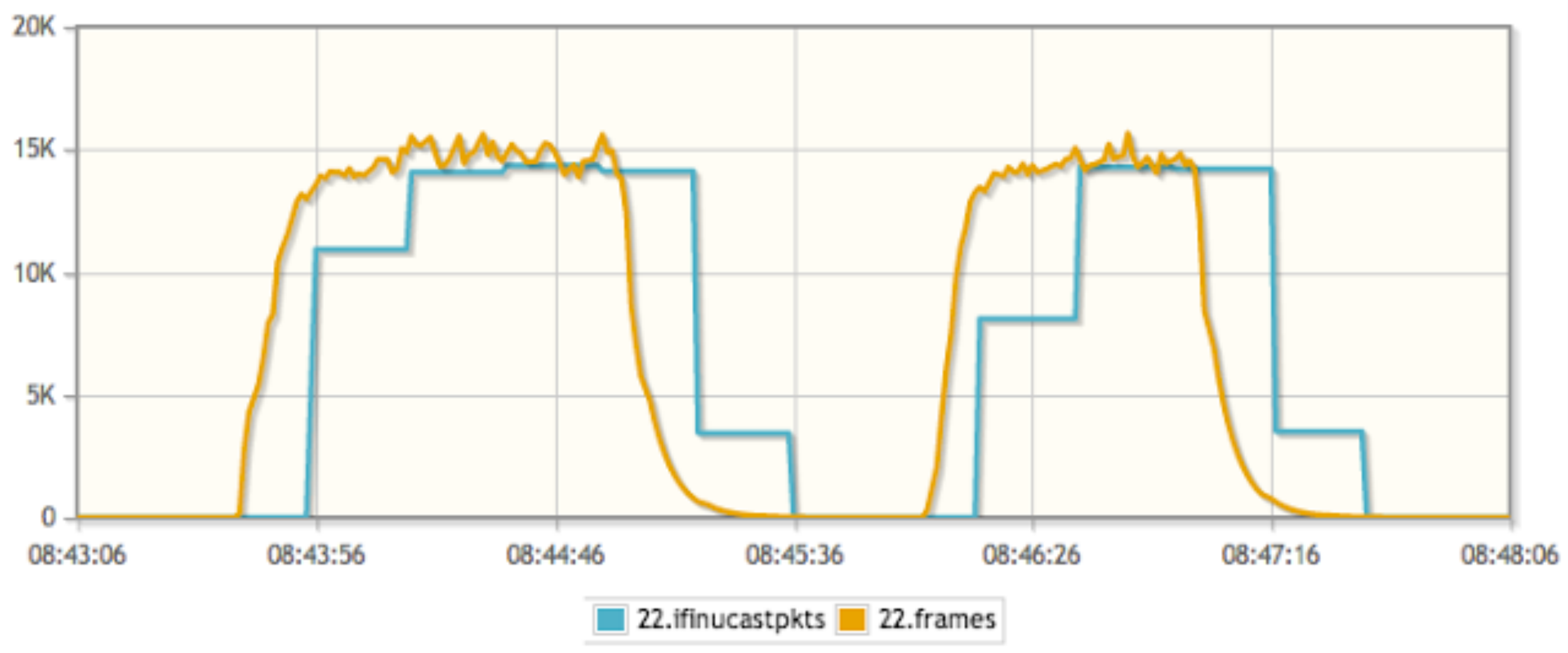


Measurement with sFlow

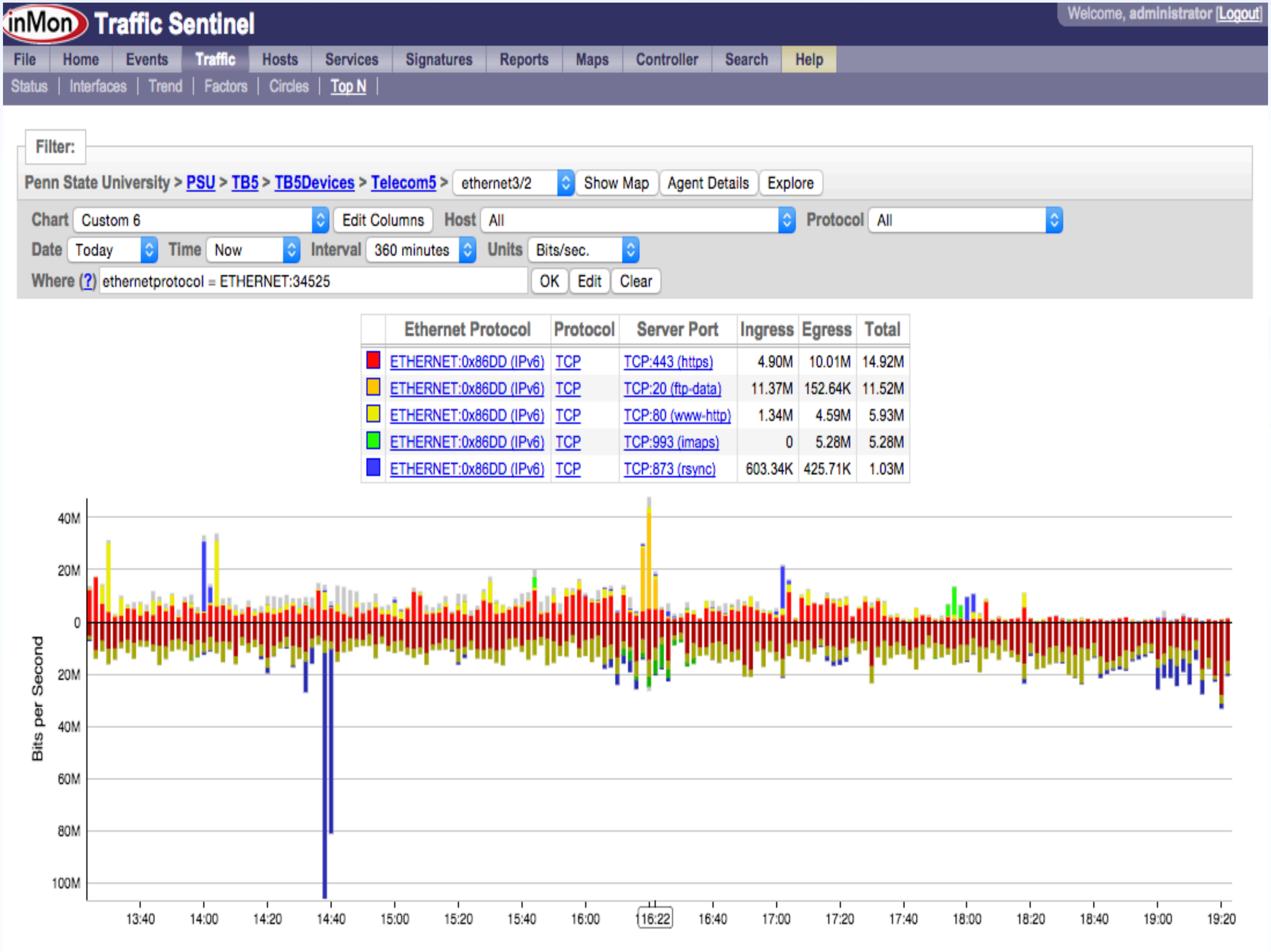
sFlow – Packet Sampling

- Exports truncated packets, together with interface counters
- An sFlow system consists of multiple dev ices performing two types of sampling:
  - random sampling of packets or application l ayer operations
  - time-based sampling of counters

sFlow Push vs SNMP counter poll



sFlow can push interface counters out every 20 seconds
instead of polling with SNMP every 1-5 minutes



Penn State University > PSU > TB5 > TB5Devices > Telecom5 > ethernet3/2

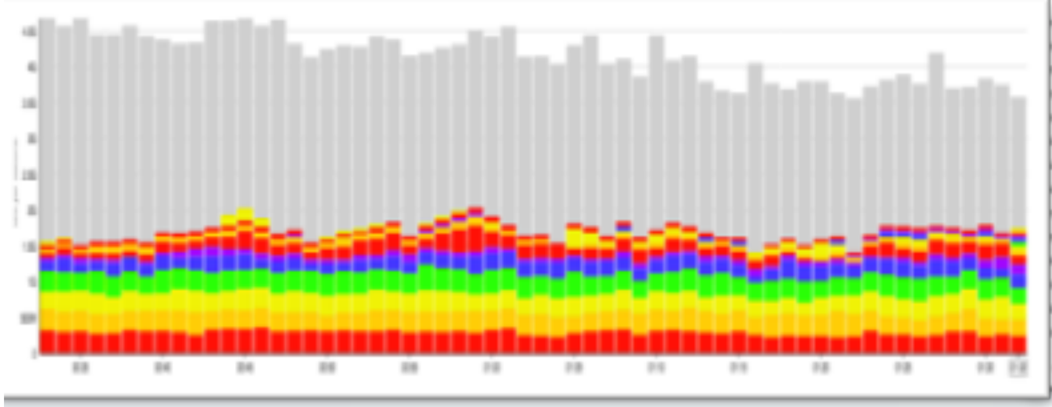
Chart Custom 6 Host All Protocol All

Date Today Time Now Interval 360 minutes Units Bits/sec.

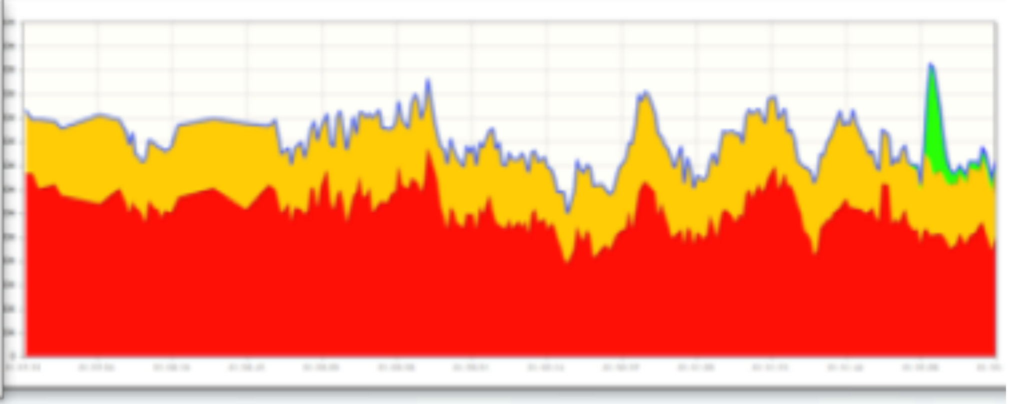
Where (?) ethernetprotocol = ETHERNET:34525

	Ethernet Protocol	Protocol	Server Port	Ingress	Egress	Total
🟥	ETHERNET:0x86DD (IPv6)	TCP	TCP:443 (https)	4.90M	10.01M	14.92M
🟧	ETHERNET:0x86DD (IPv6)	TCP	TCP:20 (ftp-data)	11.37M	152.64K	11.52M
🟨	ETHERNET:0x86DD (IPv6)	TCP	TCP:80 (www-http)	1.34M	4.59M	5.93M
🟩	ETHERNET:0x86DD (IPv6)	TCP	TCP:993 (imaps)	0	5.28M	5.28M
🟦	ETHERNET:0x86DD (IPv6)	TCP	TCP:873 (rsync)	603.34K	425.71K	1.03M

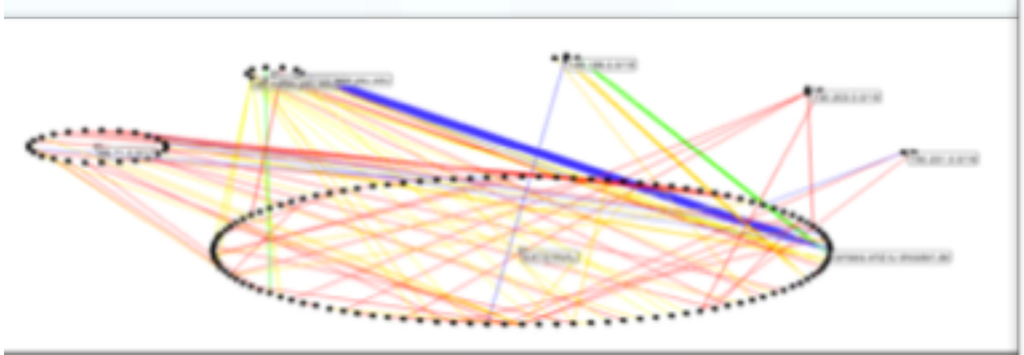
Interface sFlow Trend



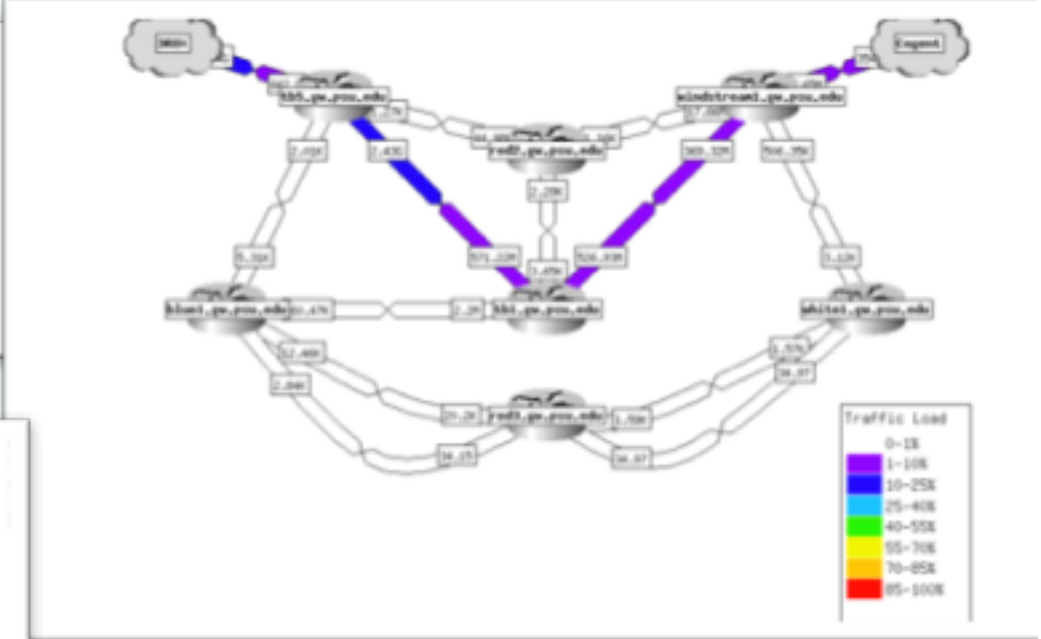
sFlow Research Flow Query



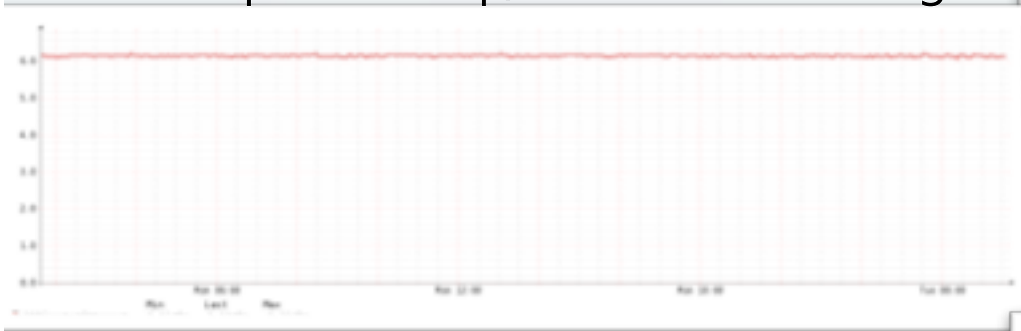
Science DMZ Fabric View



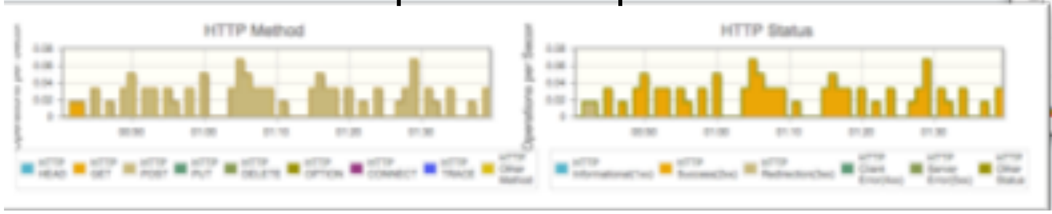
Border/Science DMZ/Core Weathermap



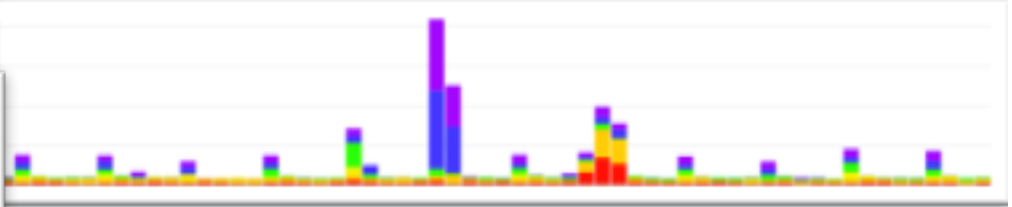
100G Optical Temp/Power Monitoring



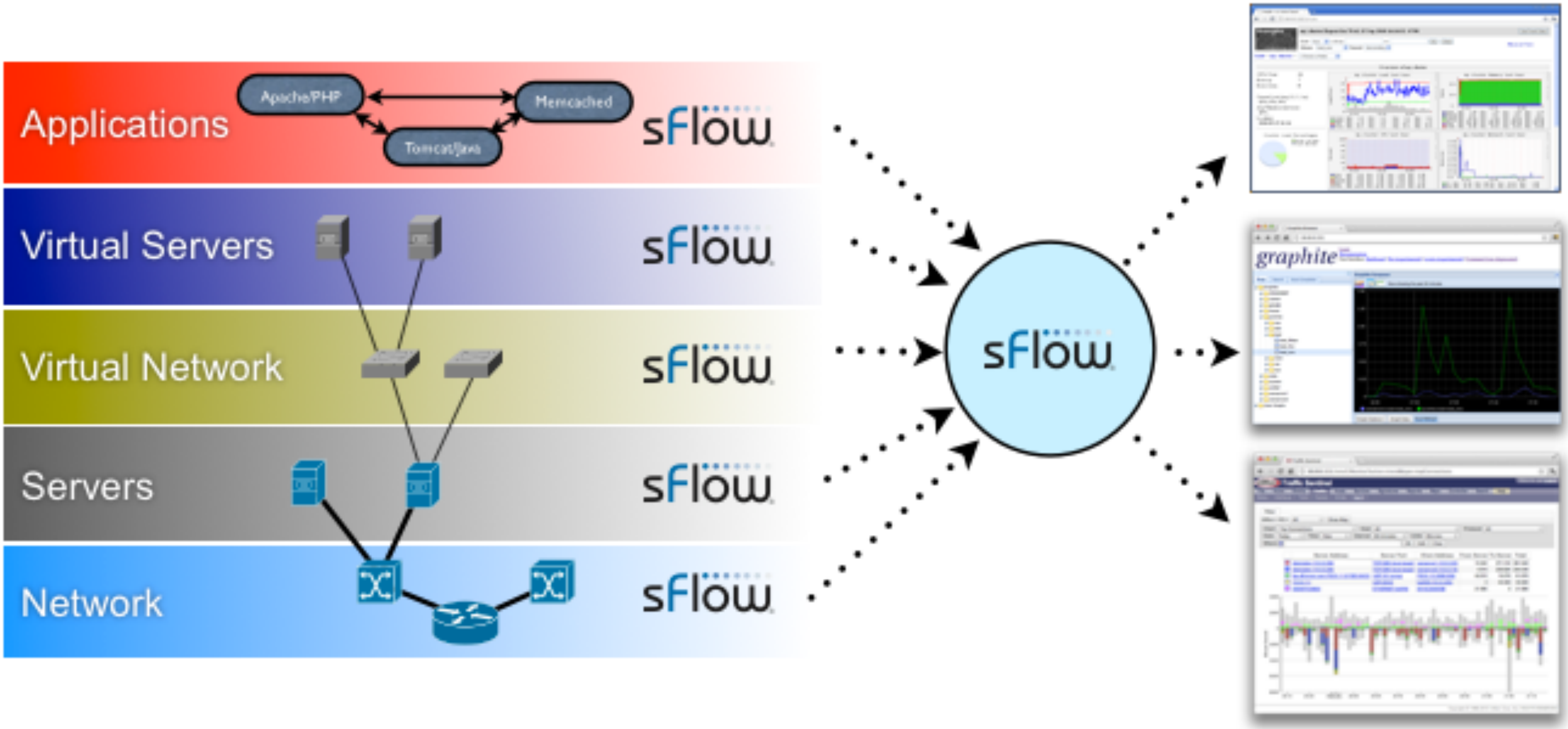
Apache httpd



ISCSI Storage Network



sFlow Visibility



Applications

Apache/PHP

Memcached

Tomcat/Java

Virtual Servers

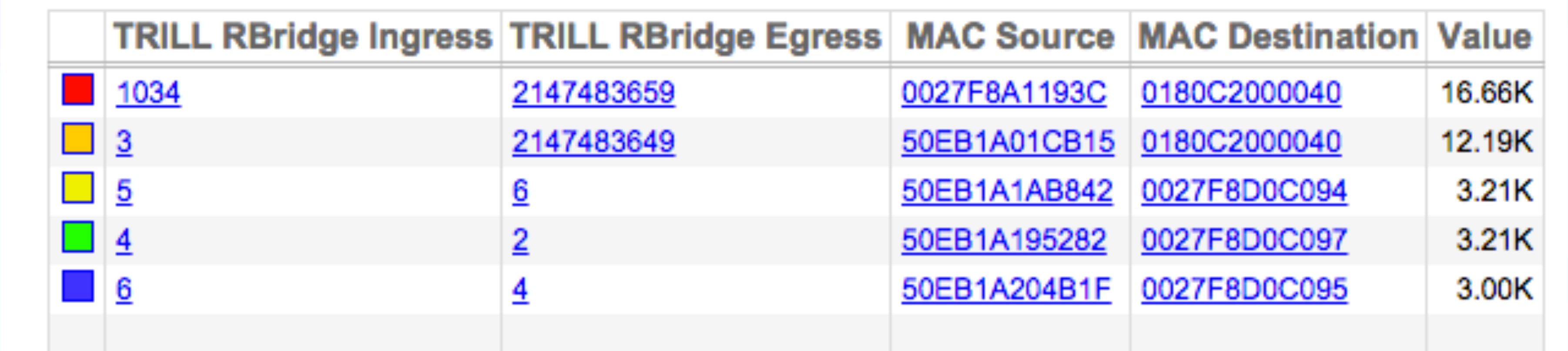
Virtual Network

Servers

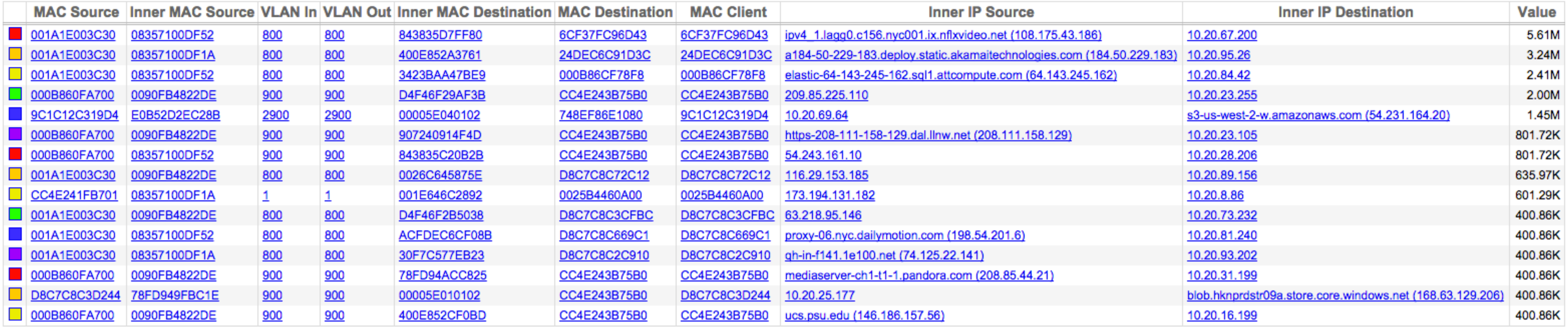
Network

sFlow

L2-L7 Tranparency with sFlow



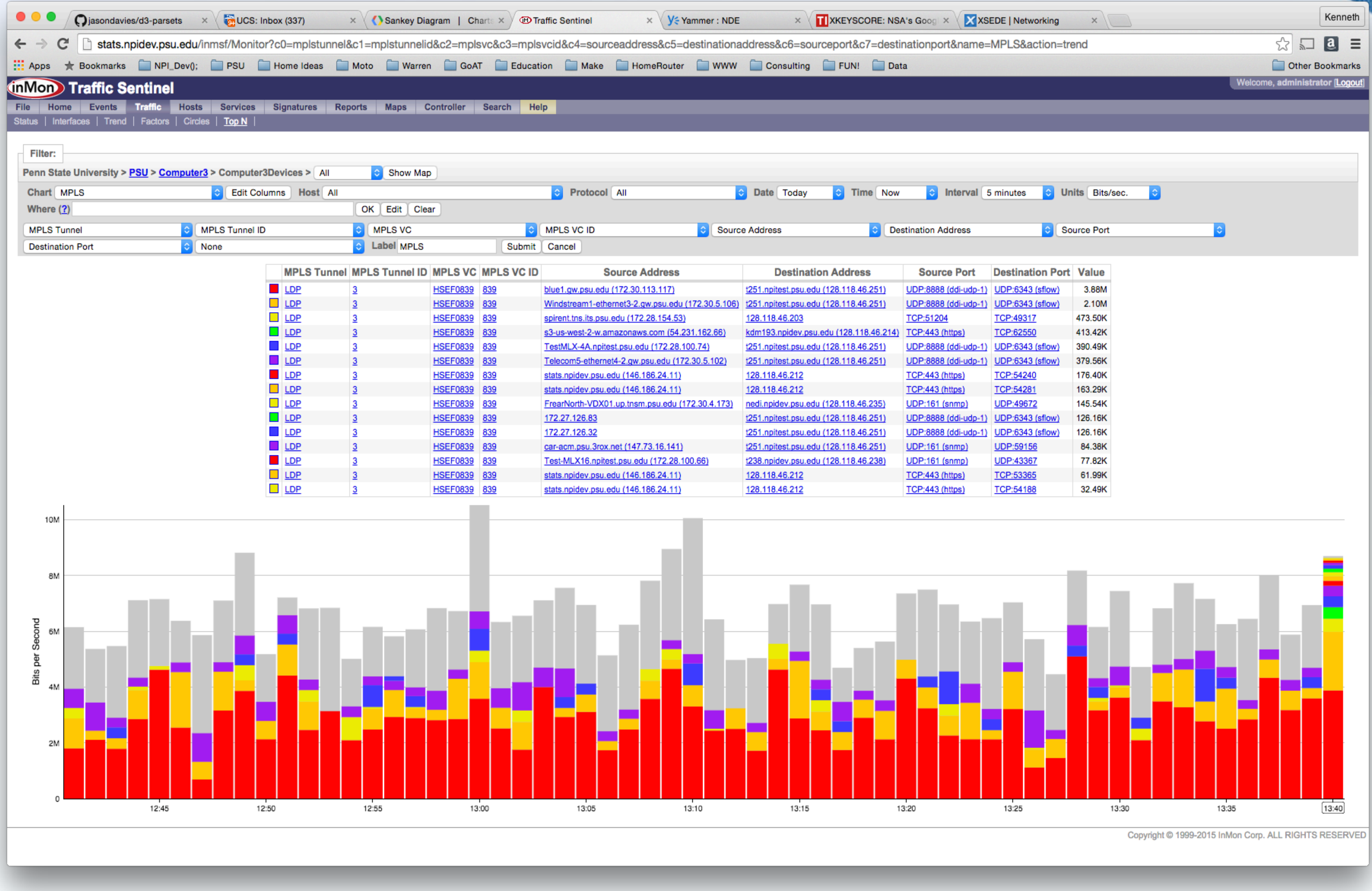
	TRILL RBridge Ingress	TRILL RBridge Egress	MAC Source	MAC Destination	Value
🟥	1034	2147483659	0027F8A1193C	0180C2000040	16.66K
🟧	3	2147483649	50EB1A01CB15	0180C2000040	12.19K
🟨	5	6	50EB1A1AB842	0027F8D0C094	3.21K
🟩	4	2	50EB1A195282	0027F8D0C097	3.21K
🟦	6	4	50EB1A204B1F	0027F8D0C095	3.00K



	MAC Source	Inner MAC Source	VLAN In	VLAN Out	Inner MAC Destination	MAC Destination	MAC Client	Inner IP Source	Inner IP Destination	Value
🟥	001A1E003C30	08357100DF52	800	800	843835D7FF80	6CF37FC96D43	6CF37FC96D43	ipv4_1.lagg0.c156.nyc001.ix.nflxvideo.net (108.175.43.186)	10.20.67.200	5.61M
🟧	001A1E003C30	08357100DF1A	800	800	400E852A3761	24DEC6C91D3C	24DEC6C91D3C	a184-50-229-183.deploy.static.akamaitechnologies.com (184.50.229.183)	10.20.95.26	3.24M
🟨	001A1E003C30	08357100DF52	800	800	3423BAA47BE9	000B86CF78F8	000B86CF78F8	elastic-64-143-245-162.sql1.attcompute.com (64.143.245.162)	10.20.84.42	2.41M
🟩	000B860FA700	0090FB4822DE	900	900	D4F46F29AF3B	CC4E243B75B0	CC4E243B75B0	209.85.225.110	10.20.23.255	2.00M
🟦	9C1C12C319D4	E0B52D2EC28B	2900	2900	00005E040102	748EF86E1080	9C1C12C319D4	10.20.69.64	s3-us-west-2-w.amazonaws.com (54.231.164.20)	1.45M
🟪	000B860FA700	0090FB4822DE	900	900	907240914F4D	CC4E243B75B0	CC4E243B75B0	https-208-111-158-129.dal.llnw.net (208.111.158.129)	10.20.23.105	801.72K
🟥	000B860FA700	08357100DF52	900	900	843835C20B2B	CC4E243B75B0	CC4E243B75B0	54.243.161.10	10.20.28.206	801.72K
🟧	001A1E003C30	0090FB4822DE	800	800	0026C645875E	D8C7C8C72C12	D8C7C8C72C12	116.29.153.185	10.20.89.156	635.97K
🟨	CC4E241FB701	08357100DF1A	1	1	001E646C2892	0025B4460A00	0025B4460A00	173.194.131.182	10.20.8.86	601.29K
🟩	001A1E003C30	0090FB4822DE	800	800	D4F46F2B5038	D8C7C8C3CFBC	D8C7C8C3CFBC	63.218.95.146	10.20.73.232	400.86K
🟦	001A1E003C30	08357100DF52	800	800	ACFDEC6CF08B	D8C7C8C669C1	D8C7C8C669C1	proxy-06.nyc.dailymotion.com (198.54.201.6)	10.20.81.240	400.86K
🟪	001A1E003C30	08357100DF1A	800	800	30F7C577EB23	D8C7C8C2C910	D8C7C8C2C910	qh-in-f141.1e100.net (74.125.22.141)	10.20.93.202	400.86K
🟥	000B860FA700	0090FB4822DE	900	900	78FD94ACC825	CC4E243B75B0	CC4E243B75B0	mediaserver-ch1-t1-1.pandora.com (208.85.44.21)	10.20.31.199	400.86K
🟧	D8C7C8C3D244	78FD949FBC1E	900	900	00005E010102	CC4E243B75B0	D8C7C8C3D244	10.20.25.177	blob.hknprdstr09a.store.core.windows.net (168.63.129.206)	400.86K
🟨	000B860FA700	0090FB4822DE	900	900	400E852CF0BD	CC4E243B75B0	CC4E243B75B0	ucs.psu.edu (146.186.157.56)	10.20.16.199	400.86K

Feature	NetFlow	sFlow
Packet capture	No	Partially
Sampling packets	Partially	Yes
Industry standard	No	Yes
Protocols		
- Packet headers	No	Yes
- Ethernet/802.3	No	Yes
- IP/ICMP/UDP/TCP	Yes	Yes
Layer 2		
- Input/Output interface	Yes	Yes
- Input/Output priority	No	Yes
Layer 3		
- Source subnet/prefix	Yes	Yes
- Destination subnet/prefix	Yes	Yes
- Next hop	Yes	Yes
BGP4		
- Source peer AS	Partially	Yes
- Destination peer AS	Partially	Yes
- Communities	No	Yes
- AS path	No	Yes
MPLS		
- Tunnel name	No	Yes
- VC (name, ID, CoS)	No	Yes
- FEC information (type, length, etc.)	No	Yes
Real-time data collection	Partially	Yes
Configuration		
- Configurable without SNMP	Yes	Yes
- Configurable via SNMP	No	Yes
- Set sampling rate per interface	No	Yes
Low cost	No	Yes
Scalable (switch IFS/collector)	No	Yes
Wire speed	Partially	Yes

MPLS/VPLS



stats.npidev.psu.edu/inmsf/Monitor?c0=mplstunnel&c1=mplstunnelid&c2=mplsvc&c3=mplsvcid&c4=sourceaddress&c5=destinationaddress&c6=sourceport&c7=destinationport&name=MPLS&action=trend

Filter:

Penn State University > PSU > Computer3 > Computer3Devices > All | Show Map

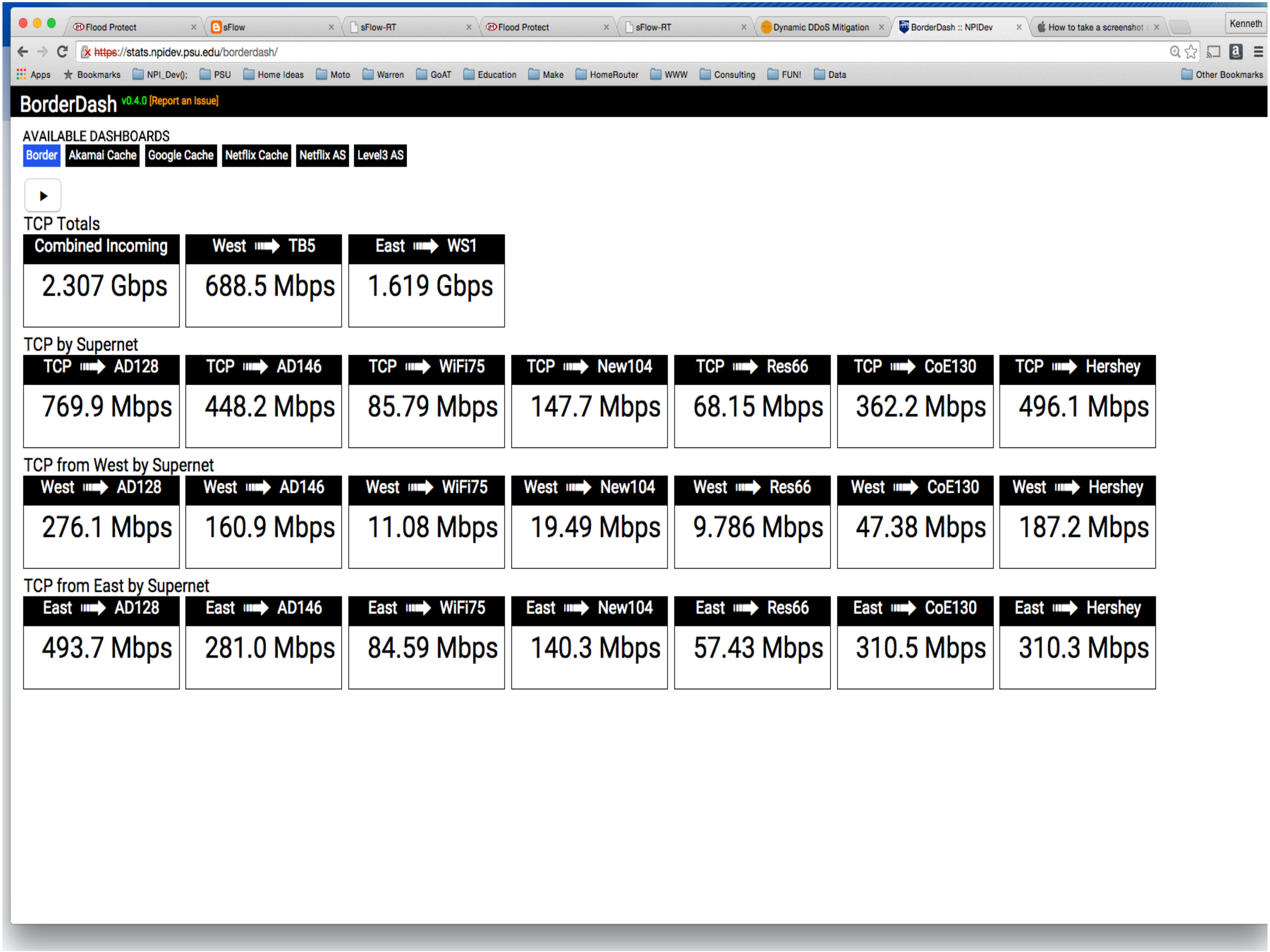
Chart: MPLS | Edit Columns | Host: All | Protocol: All | Date: Today | Time: Now | Interval: 5 minutes | Units: Bits/sec.

Where (?) | OK | Edit | Clear

MPLS Tunnel | MPLS Tunnel ID | MPLS VC | MPLS VC ID | Source Address | Destination Address | Source Port

Destination Port | None | Label: MPLS | Submit | Cancel

	MPLS Tunnel	MPLS Tunnel ID	MPLS VC	MPLS VC ID	Source Address	Destination Address	Source Port	Destination Port	Value
🟥	LDP	3	HSEF0839	839	blue1.gw.psu.edu (172.30.113.117)	t251.npitest.psu.edu (128.118.46.251)	UDP:8888 (ddi-udp-1)	UDP:6343 (sflow)	3.88M
🟧	LDP	3	HSEF0839	839	Windstream1-ethernet3-2.gw.psu.edu (172.30.5.106)	t251.npitest.psu.edu (128.118.46.251)	UDP:8888 (ddi-udp-1)	UDP:6343 (sflow)	2.10M
🟨	LDP	3	HSEF0839	839	spirent.tns.its.psu.edu (172.28.154.53)	128.118.46.203	TCP:51204	TCP:49317	473.50K
🟩	LDP	3	HSEF0839	839	s3-us-west-2-w.amazonaws.com (54.231.162.66)	kdm193.npidev.psu.edu (128.118.46.214)	TCP:443 (https)	TCP:62550	413.42K
🟦	LDP	3	HSEF0839	839	TestMLX-4A.npitest.psu.edu (172.28.100.74)	t251.npitest.psu.edu (128.118.46.251)	UDP:8888 (ddi-udp-1)	UDP:6343 (sflow)	390.49K
🟪	LDP	3	HSEF0839	839	Telecom5-ethernet4-2.gw.psu.edu (172.30.5.102)	t251.npitest.psu.edu (128.118.46.251)	UDP:8888 (ddi-udp-1)	UDP:6343 (sflow)	379.56K
🟥	LDP	3	HSEF0839	839	stats.npidev.psu.edu (146.186.24.11)	128.118.46.212	TCP:443 (https)	TCP:54240	176.40K
🟧	LDP	3	HSEF0839	839	stats.npidev.psu.edu (146.186.24.11)	128.118.46.212	TCP:443 (https)	TCP:54281	163.29K
🟨	LDP	3	HSEF0839	839	FrearNorth-VDX01.up.tnsm.psu.edu (172.30.4.173)	nedi.npidev.psu.edu (128.118.46.235)	UDP:161 (snmp)	UDP:49672	145.54K
🟩	LDP	3	HSEF0839	839	172.27.126.83	t251.npitest.psu.edu (128.118.46.251)	UDP:8888 (ddi-udp-1)	UDP:6343 (sflow)	126.16K
🟦	LDP	3	HSEF0839	839	172.27.126.32	t251.npitest.psu.edu (128.118.46.251)	UDP:8888 (ddi-udp-1)	UDP:6343 (sflow)	126.16K
🟪	LDP	3	HSEF0839	839	car-acm.psu.3rox.net (147.73.16.141)	t251.npitest.psu.edu (128.118.46.251)	UDP:161 (snmp)	UDP:59156	84.38K
🟥	LDP	3	HSEF0839	839	Test-MLX16.npitest.psu.edu (172.28.100.66)	t238.npidev.psu.edu (128.118.46.238)	UDP:161 (snmp)	UDP:43367	77.82K
🟧	LDP	3	HSEF0839	839	stats.npidev.psu.edu (146.186.24.11)	128.118.46.212	TCP:443 (https)	TCP:53365	61.99K
🟨	LDP	3	HSEF0839	839	stats.npidev.psu.edu (146.186.24.11)	128.118.46.212	TCP:443 (https)	TCP:54188	32.49K



BorderDash v0.4.0 [Report an Issue]

AVAILABLE DASHBOARDS

Border | Akamai Cache | Google Cache | Netflix Cache | Netflix AS | Level3 AS

▶

TCP Totals

Combined Incoming	West → TB5	East → WS1
2.307 Gbps	688.5 Mbps	1.619 Gbps

TCP by Supernet

TCP → AD128	TCP → AD146	TCP → WiFi75	TCP → New104	TCP → Res66	TCP → CoE130	TCP → Hershey
769.9 Mbps	448.2 Mbps	85.79 Mbps	147.7 Mbps	68.15 Mbps	362.2 Mbps	496.1 Mbps

TCP from West by Supernet

West → AD128	West → AD146	West → WiFi75	West → New104	West → Res66	West → CoE130	West → Hershey
276.1 Mbps	160.9 Mbps	11.08 Mbps	19.49 Mbps	9.786 Mbps	47.38 Mbps	187.2 Mbps

TCP from East by Supernet

East → AD128	East → AD146	East → WiFi75	East → New104	East → Res66	East → CoE130	East → Hershey
493.7 Mbps	281.0 Mbps	84.59 Mbps	140.3 Mbps	57.43 Mbps	310.5 Mbps	310.3 Mbps

- Thanks to Jason Z for everything
- Thanks to ESNet and Engagement Team
- Thanks to NSF for the funding
- Thanks to Nick Buraglio, Anita Nikolich, Dale Carder, Securing the SDN WAN, October 30, 2014
- http://meetings.internet2.edu/2014-technology-exchange/detail/10003432/
- Thanks to VonWelch on http://trustedci.org/ and Joe Breen of Utah for the Science DMZ security and engagement peer review