

# SciPass

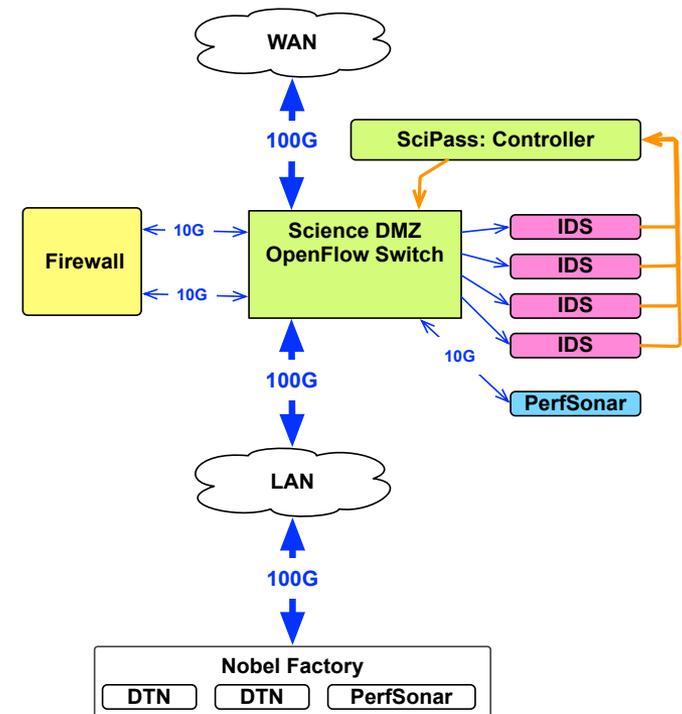
OpenFlow Based Load Balancer and  
Science DMZ

Edward Balas

AJ Ragusa

# Executive Overview

- We are presenting a Science DMZ that can
  - Define good science traffic
  - Detect good with IDS
  - Make good go fast
  - Be secure
- Covering initial performance testing and dev status

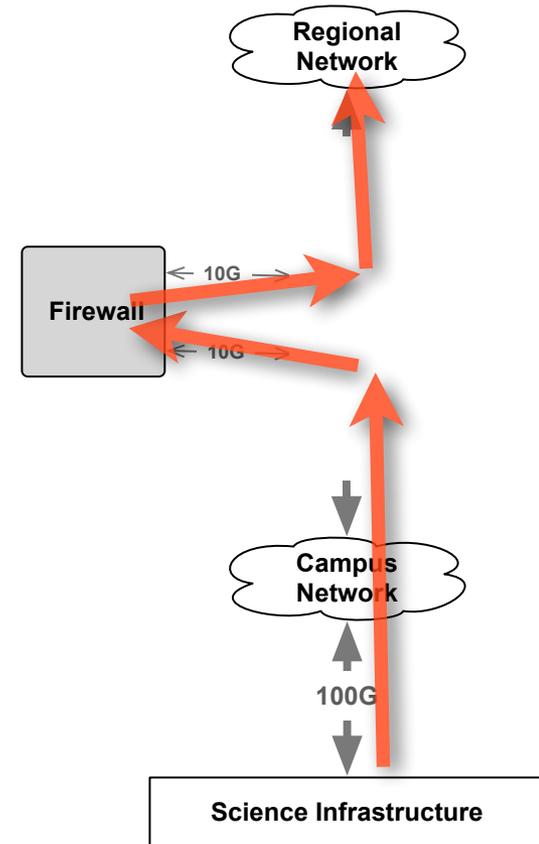


# Who is doing this?

- Indiana University
  - GlobalNOC
  - University Information Security Office
- Collaborating with
  - Bro Team
  - Anyone with good ideas
- Looking for other participants

# Problem

- Campus are enterprise infrastructure
  - large number of small flows
  - security is a required capability
- Not large flow friendly
- Cant just ignore security
- Verifying performance is hard

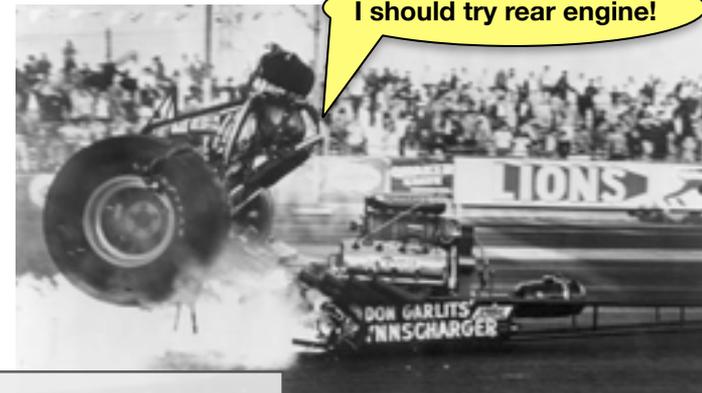


# Science DMZ

- Support big data / science apps at 100G
  - Reduce packet loss
  - Appropriate security
  - Integrate test points
- Go fast, keep it controlled
- <http://fasterdata.es.net/science-dmz/>



This



Not This

# Objective:

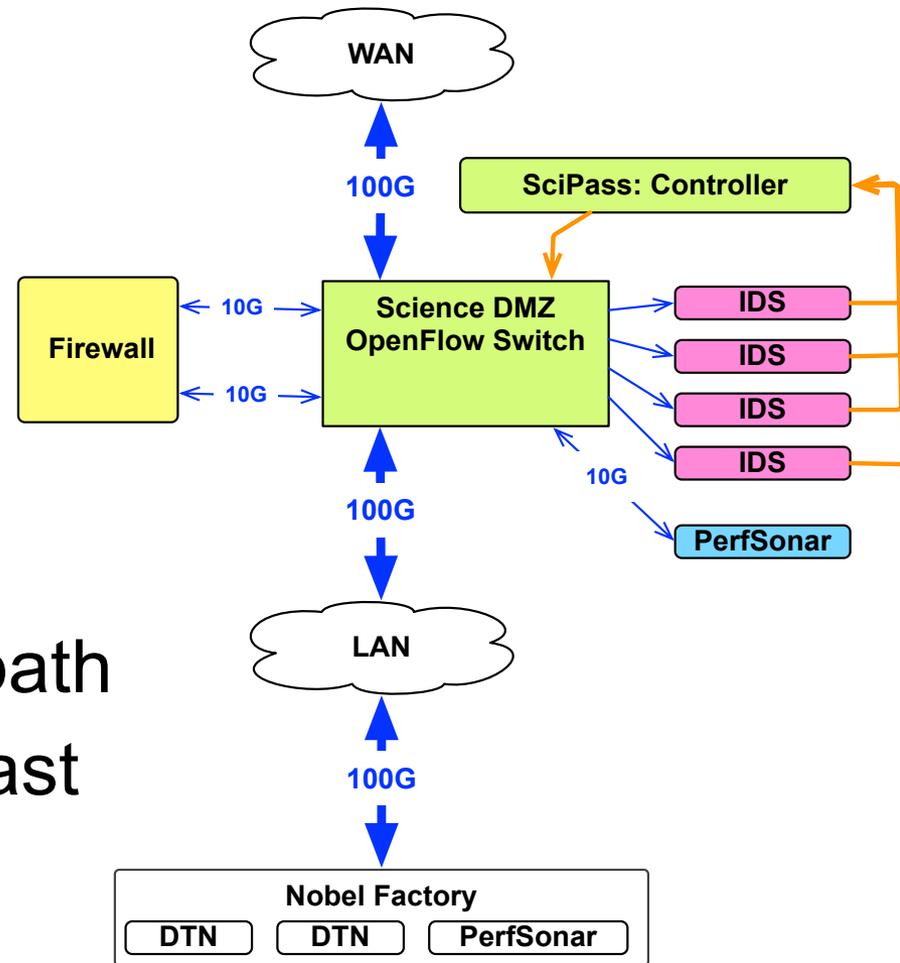
- Reconfigure existing components
- 100G Science DMZ
- Security features baked in.
  - Adaptive IDS load balancing
  - Hardware based forwarding
  - Controlled bypass of institutional firewall
  - Integrated measurement



a year later,  
engine in rear

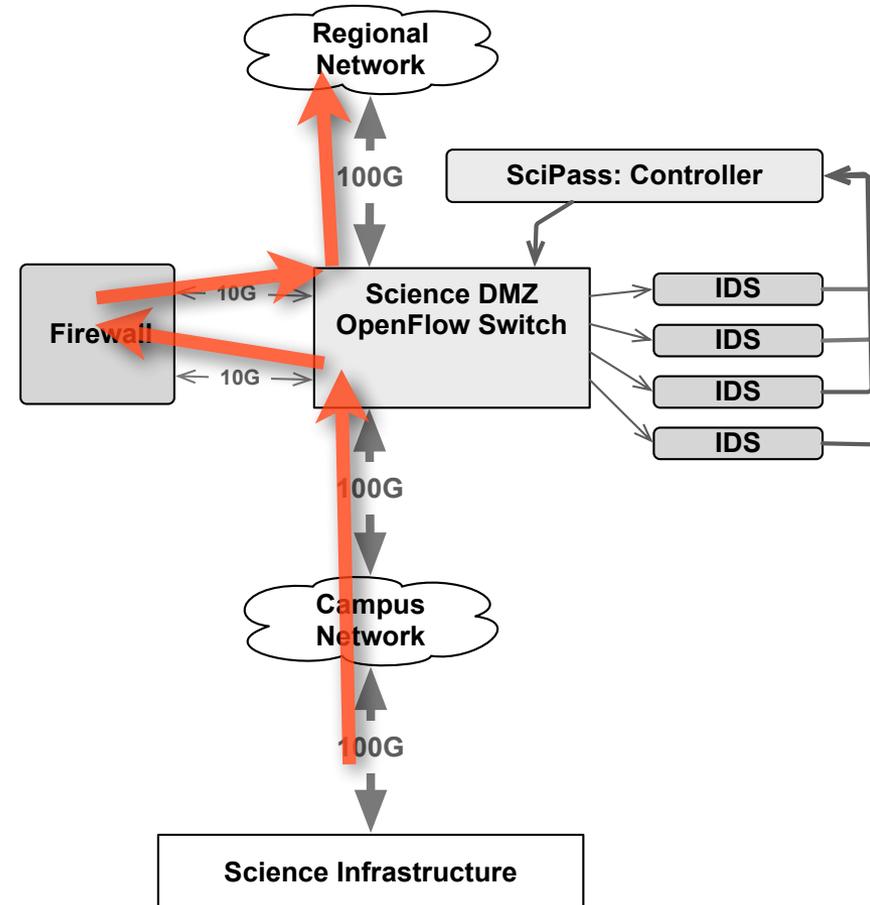
# Approach

- Combine
  - OpenFlow Switch
  - Bro
  - PerfSonar
- Create adaptive system
- Default to secure / slow path
- IDS controls what goes fast



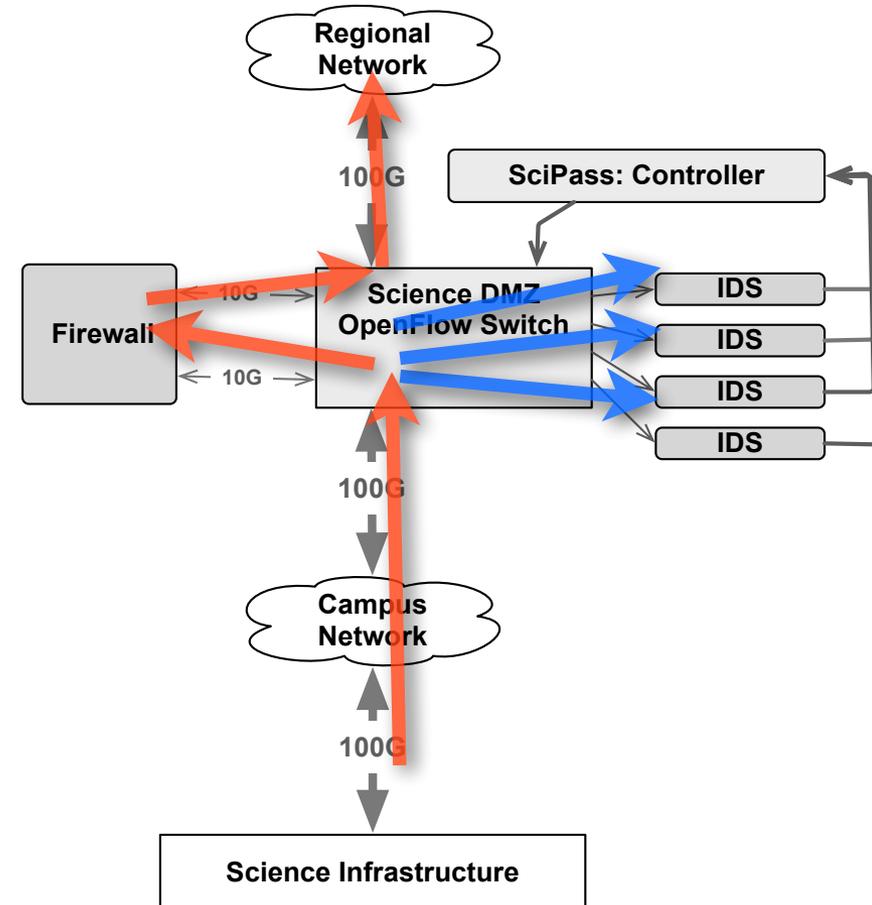
# Default Behavior

- Traffic goes through firewall



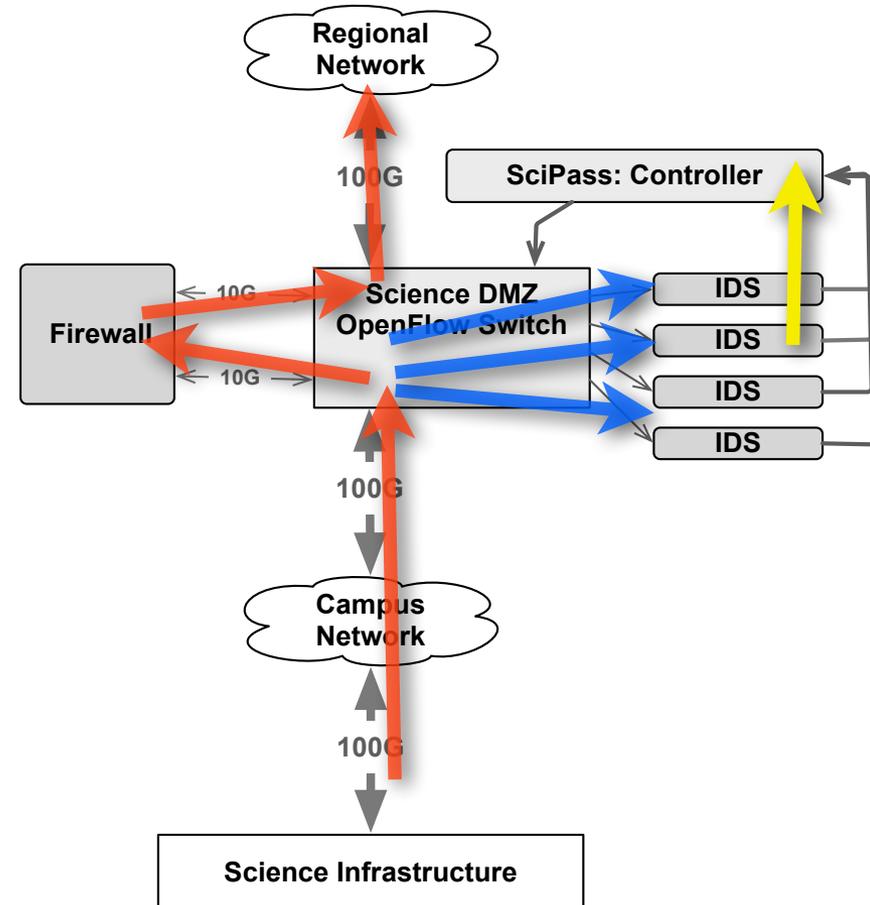
# Default Behavior

- Copies of packets are sent to IDS ports
- Load balancing techniques employed



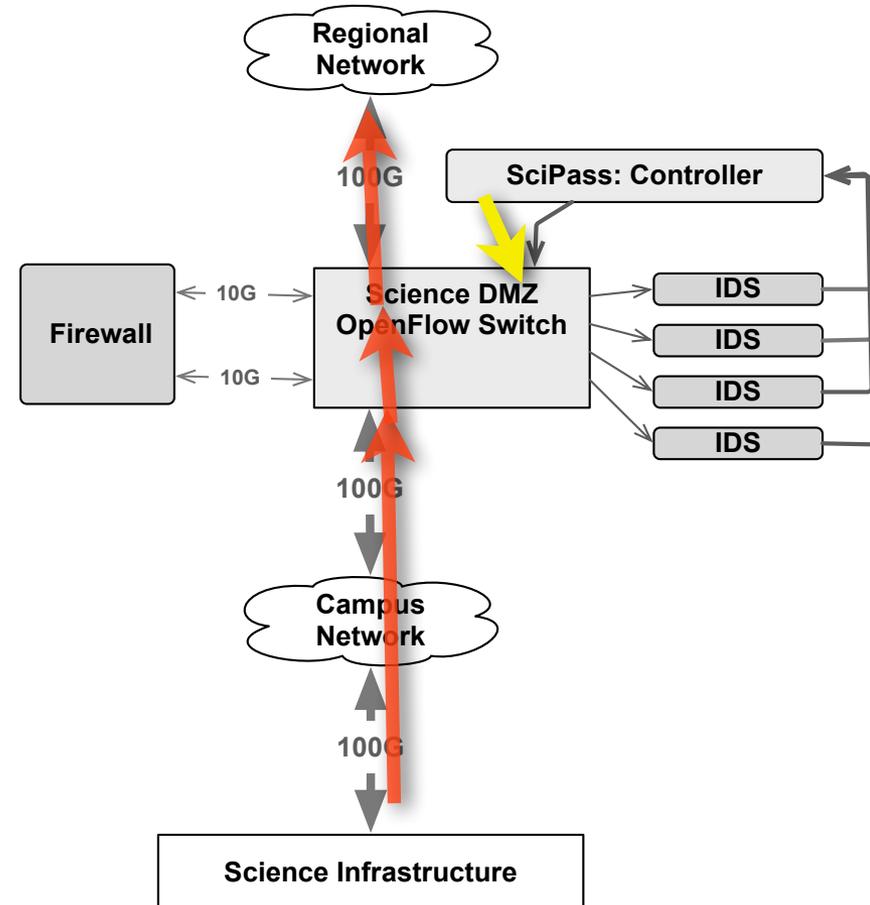
# IDS detects **good**

- IDS inspects traffic
- Identifies “good” science flows
- Signals SciPass
  - setup fast path
  - dont send to IDS
  - per flow



# SciPass Bypasses Firewall

- Based on input SciPass installs fast path rule
  - Firewall is bypassed
  - Traffic not sent to IDS
- Better throughput
- Reduced load on IDS and Firewall



# Defining Good Flows

- Today
  - Protocol being used
  - Src / Dst Host
- Future
  - Time of day / day of week
  - App Specific
    - files in a particular directory



# Simple Load Balancing

- Similar to binary search
- Break traffic into set of subnets
- Observe traffic volume and load
- If needed
  - Move prefixes to different sensor
  - Sub divide a prefix
- Repeat every N seconds

# Technical Details

- Stand alone / appliance SDN Deployment
- Combines Bro with SciPass to create a reactive / adaptive system
- The **new thing** here is that we are **fingerprinting GOOD** traffic and enhancing its path through the DMZ.

# Operation Modes

- Science DMZ
  - Inline forwarding control
- Inline IDS Load Balancer
  - Forward traffic and copy to IDS
  - Blacklisting
- Passive IDS Load Balancer
  - Aggregate taps and balance

# Load Balancing Features

- Progressive, binary search like approach
- Prefix based
  - Traffic volume
  - Sensor load (as reported by sensor)
- Configurable thresholds for rebalancing
- Configurable review frequency ( 10 sec )

# Traffic Control Features

- Whitelist
  - Traffic forward through switch
  - Firewall bypassed
  - Sensor bypassed
- Blacklist
  - Traffic dropped at ingress

# Implementation Details

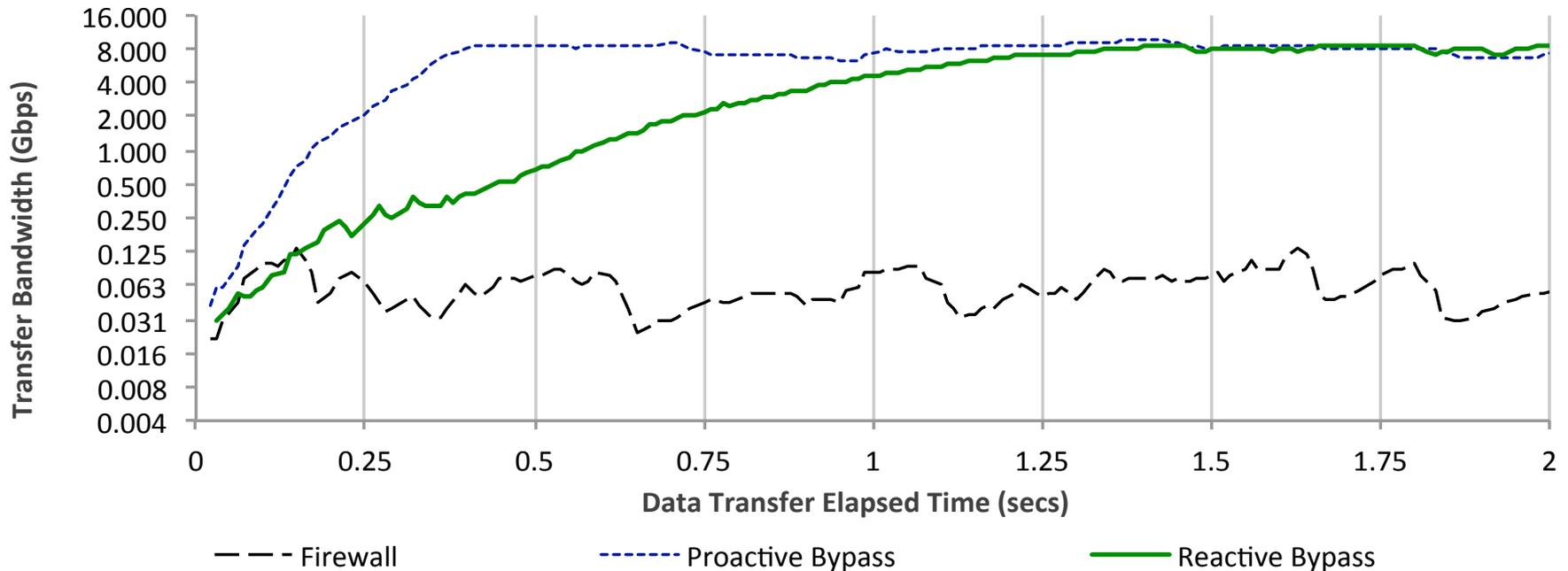
- UNIXy in feel
  - cli centric but with web services
- Modular architecture
- Python App
- RYU controller for now
- Bro scripts to integrate

# Testing

- DMZ deployed in InCNTRE Indianapolis lab
  - Brocade MLXe switch
  - Netscreen 5200
- Tested to ESnet well known test points over 5 production administrative domains
  - 7ms of delay to the Argonne server
  - <http://fasterdata.es.net/performance-testing/DTNs/>

# Reactive Bypass Performance

- 64 ms - time to detect and bypass
- 250 ms - doubled throughput of firewall
- 1.5 sec - same throughput as no firewall



# Interpretation

- This approach looks quite promising
- We expect to reduce detection time as our software and vendor software improves
- Even today suitable for long lived science flows
- May have other applications

# Status

- Tested in lab
- 10g bypass tested between IU and ESnet
- Campus trials of IDS load balancing to start after SC14
- Demo or die
  - Layer123
  - Internet2 Technology Exchange
  - SC14

# Roadmap

- Q4 trial deployment
- Q4 eval OpenDayLight
- Q1 operations enhancements
- Q2 ???



# Related Efforts

**BROCADE**  **ARISTA**



- Several folks working with Bro and Arista on IDS balancing
- Efforts underway at NCSA, LBL NERSC
- Corsa also in this space
- Brocade working on app
- others?

# Why not have end host signal?

- Protocols such as XSP may be a complimentary addition
- Consider carefully
  - trust
  - separation of duty
- For future, explore XSP proactive signaling into SciPass

# Future Exploration

- How this might work with XSP
- Investigate use of rate limiting via meter table support, think bandwidth calandering
- Explore policy definition techniques that take a community centric approach

# More Info

- Project Page
  - <http://globalnoc.iu.edu/sdn/scipass.html>
- Code Repository
  - <https://github.com/GlobalNOC/SciPass>
- email
  - [scipass-users@grnoc.iu.edu](mailto:scipass-users@grnoc.iu.edu)