Enhancing Science Through Custom Paths For Trusted Users

ZONGMING FEI, UNIVERSITY OF KENTUCKY

Cybersecurity Research Acceleration Workshop and Showcase, Indianapolis, IN
October 11, 2017

Enhancing Science Through Custom Paths for Trusted Flows

Zongming Fei

University of Kentucky

(This is a joint work with James Griffioen, Ken Calvert, Sergio Rivera, Jacob Chappell, Mami Hayashida, Pinyi Shi, Charles Carpenter, Yongwook Song, Hussamuddin Nasir)

UNIVERSITY OF KENTUCKY

This work is supported in part by the National Science Foundation under NSF grant ACI-1541426.

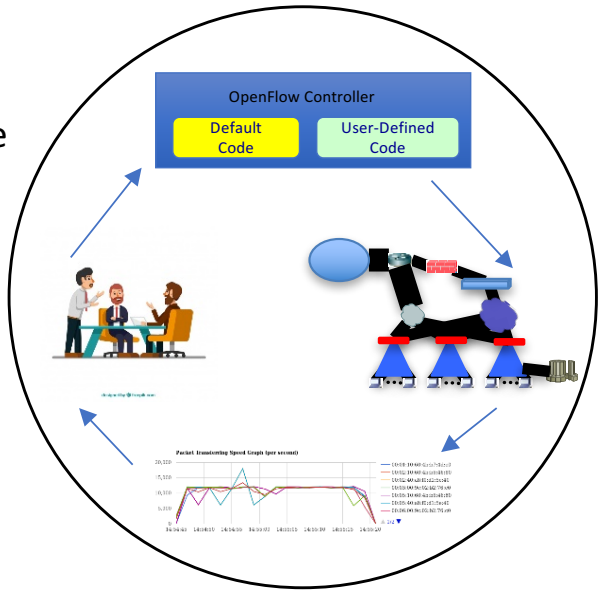
Cybersecurity Research Acceleration Workshop and Showcase

October 11, 2017 | Indianapolis, IN

Quad Chart for: Enhancing Science Through Custom Paths For Trusted Users

Challenge:

Provide the ability for pre-authorized, trusted users to create flows that bypass middleboxes, thereby enabling those users to achieve substantially better performance while maintaining security and policy compliance for other network traffic.



Solution:

- Install SDN-enabled routers/switches in the campus network.
- Create two paths to the campus edge.
- By default, forward all packets through the existing campus core and policy-enforcing middleboxes.
- Develop a VIP Lanes server to dynamically install SDN rules (with higher priority) to "pick off" approved flows and forward them directly to the campus edge, by-passing middleboxes.

NSF ACI #1541426
University of Kentucky
PI: James Griffioen
Team: Zongming Fei (co-PI), Sergio Rivera, Jacob Chappell, Mami Hiyashida, Pinyi Shi, Charles Carpenter, Yongwook Song, Hussamuddin Nasir, Ken Calvert (former co-PI)

Value proposition:

- Provide better performance for data transfer to big data researchers while still maintaining security and policy compliance for other traffic.
- Deploy SDN on campus networks.
- Presents an opportunity for users and providers to work together to develop solutions that enable explicit negotiation that can lead to trust

What we need to TTP

- Your feedback
- Learn from experience of other projects
- Opportunities to collaborate with researchers and IT from other universities

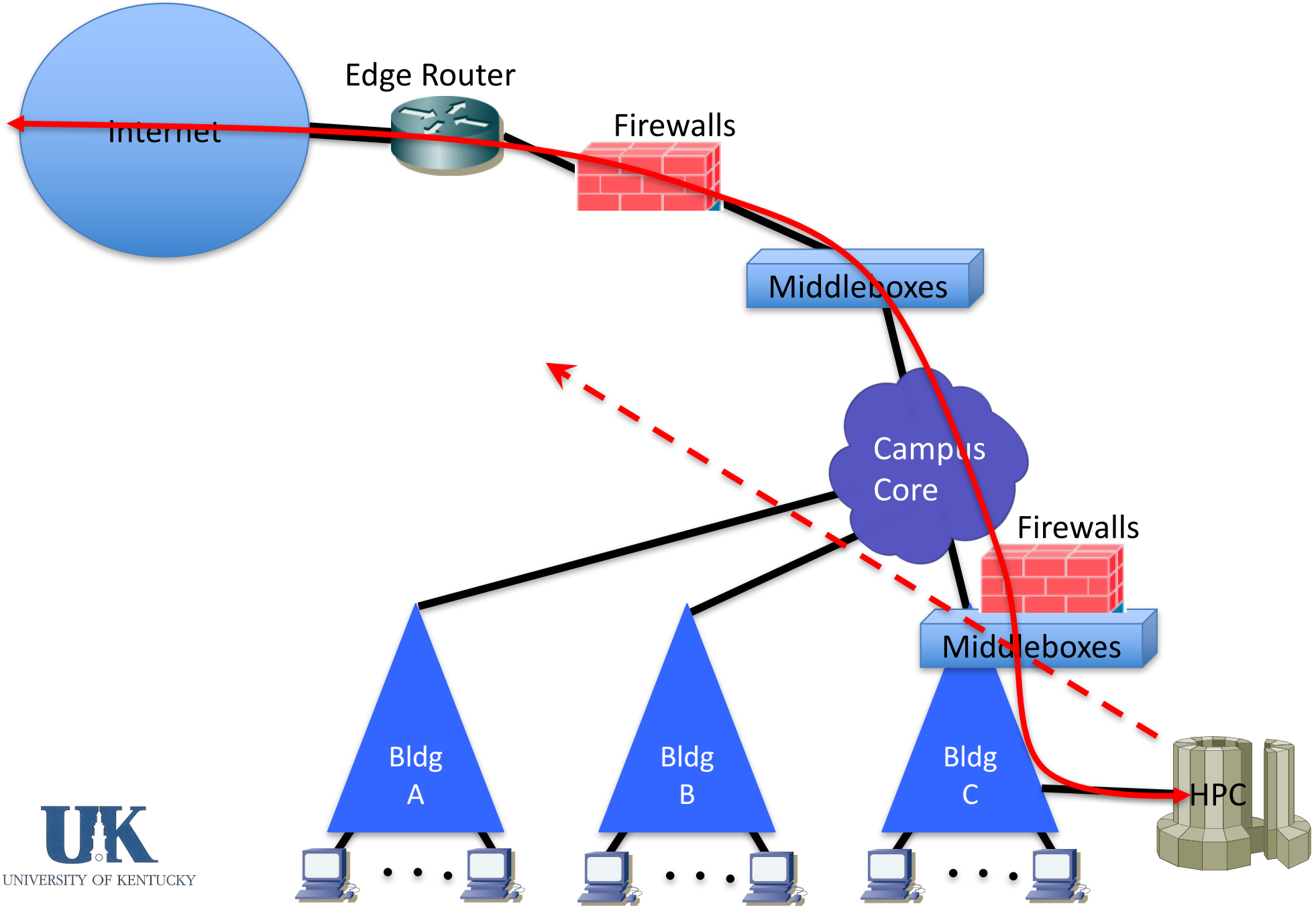
Contact us

- griff@netlab.uky.edu
- fei@netlab.uky.edu

Challenges

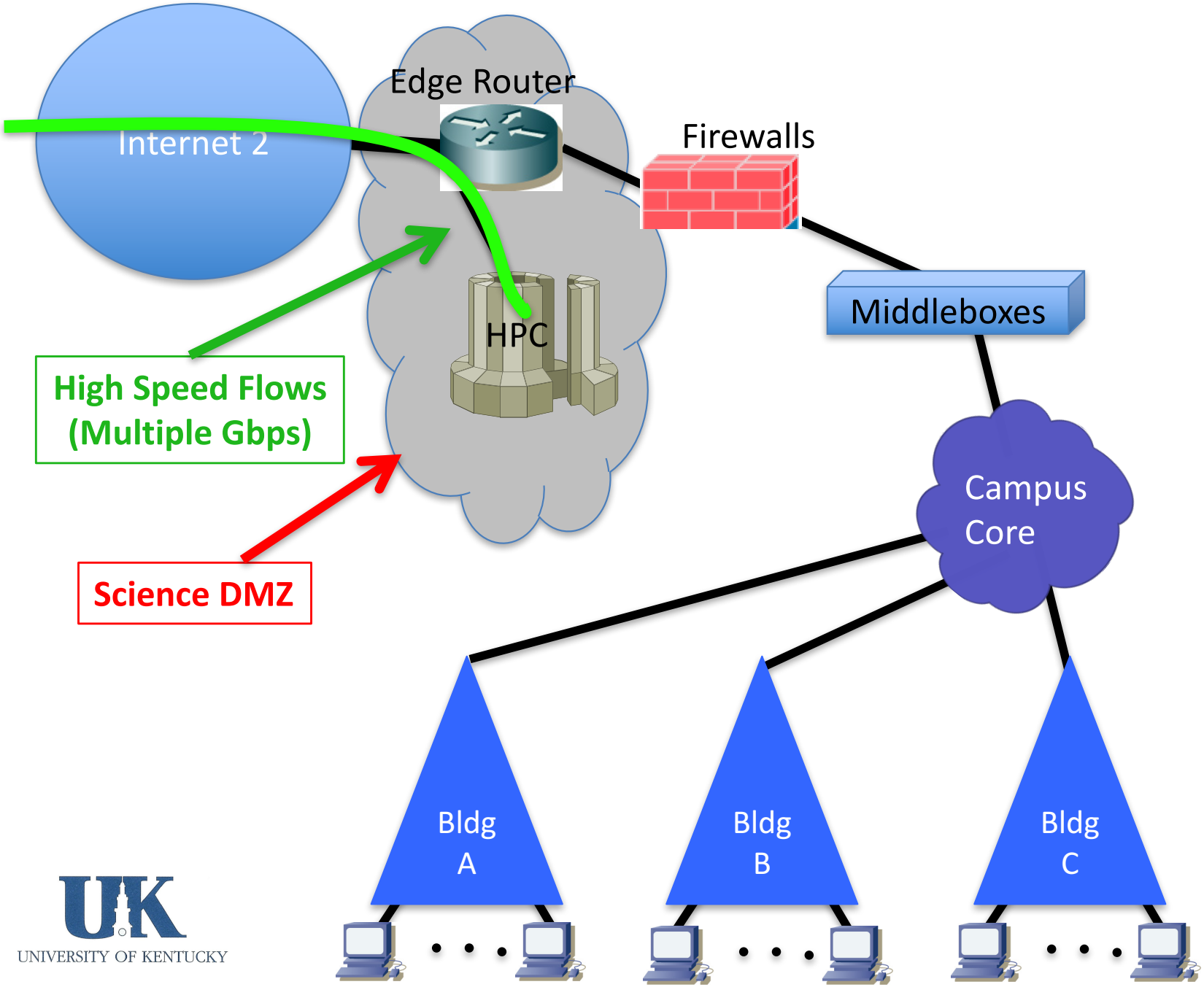
- Sharing Big Data in Campus Networks
  - Bid data is driving many research techniques nowadays across all disciplines.
  - The need: share these big data sets efficiently with other researchers.
  - The problem: Campus infrastructure is not designed to support high-throughput transmissions of big datasets.
- Middleboxes
  - Provide important services that enforce policy and offer enhanced functionality (firewalls, VPN).
  - Offer functionalities involving deep packet inspection (IDSs, etc).
  - Provide other functions (NAT, traffic shaping/QoS enforcement, Load Balancers, caching).
  - Middleboxes are placed strategically throughout the network, not just at the edge.
- Because middleboxes operate on packets, they pose a bottleneck to network performance, especially for big data transfer.

Traditional Solution: Science DMZ



UNIVERSITY OF KENTUCKY

Traditional Solution: Science DMZ



UNIVERSITY OF KENTUCKY

Science DMZ Solution

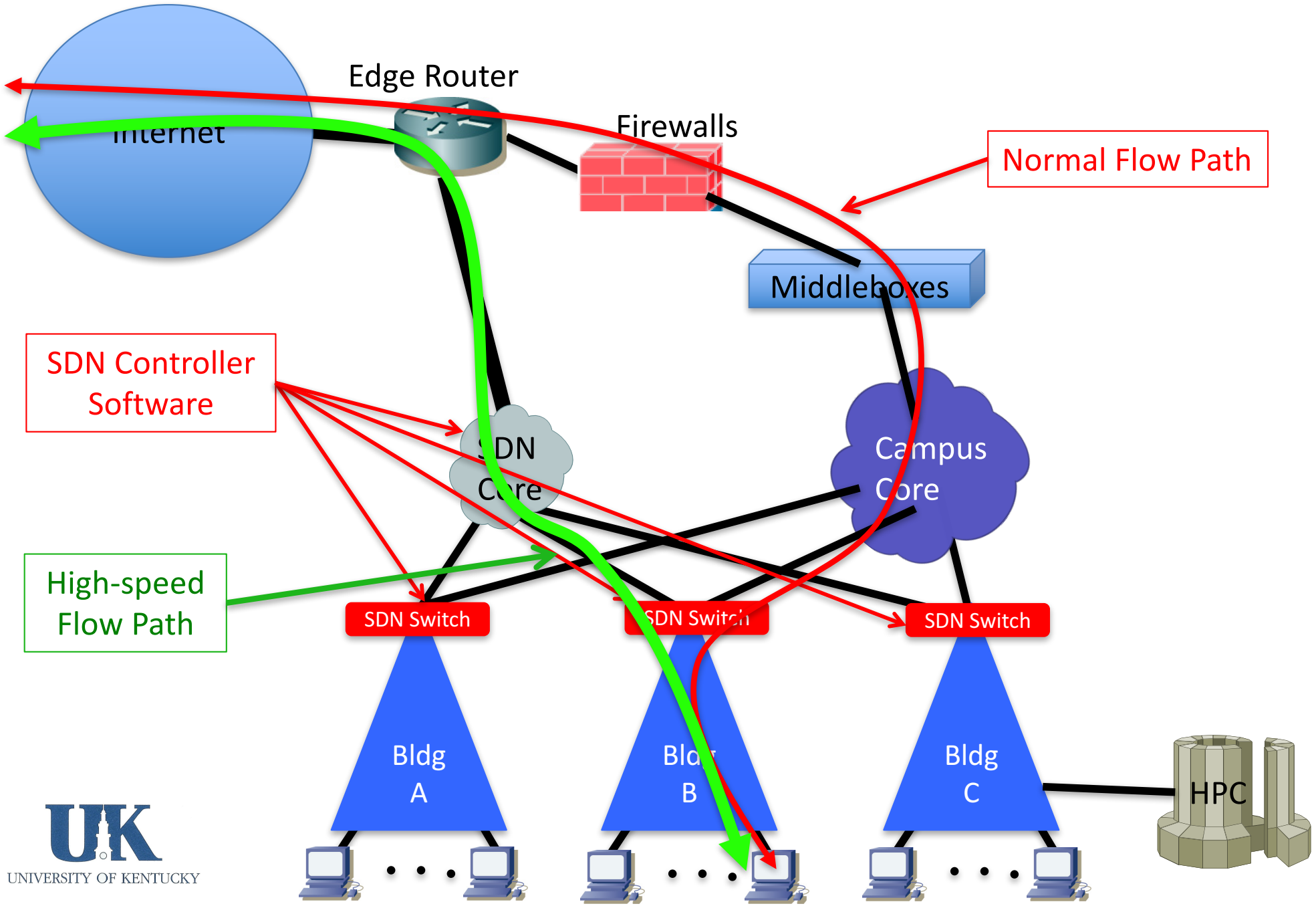
- Deploy a Science DMZ network connected to the network edge.
- Move HPC and some other machines to the Science DMZ network
- Advantages:
  - Traffic from HPC machines bypass middlebox bottlenecks
- Disadvantages:
  - Science DMZ machines are not protected by middleboxes.
  - Campus (middlebox) policy enforcement is not applied to any traffic from Science DMZ machines. Even non-science flows (e.g., Netflix) bypass campus policy enforcement.
  - Researchers must decide whether to connect their machines to the Science DMZ or the Campus Network.

Our Approach:
SDN-based Custom Paths for Trusted Flows

- Observation: Science DMZs enable "privileged traffic" – traffic that has been pre-approved to by-pass campus middleboxes.
- Approach: Use Software Defined Network (SDN) capabilities to intercept approved science flows and route around performance-limiting middleboxes.
  1. Install SDN-enabled routers/switches in the campus network. (Where?)
  2. Create two paths to the campus edge
     - One through the existing campus core network
     - One through a new middlebox-free path to the campus edge.
  3. By default, forward all packets through the existing campus core and policy-enforcing middleboxes.
  4. Dynamically install SDN rules (with higher priority) to "pick off" approved flows and forward them directly to the campus edge, by-passing middleboxes.

UNIVERSITY OF KENTUCKY

VIP Lanes for Trusted Flows



UNIVERSITY OF KENTUCKY

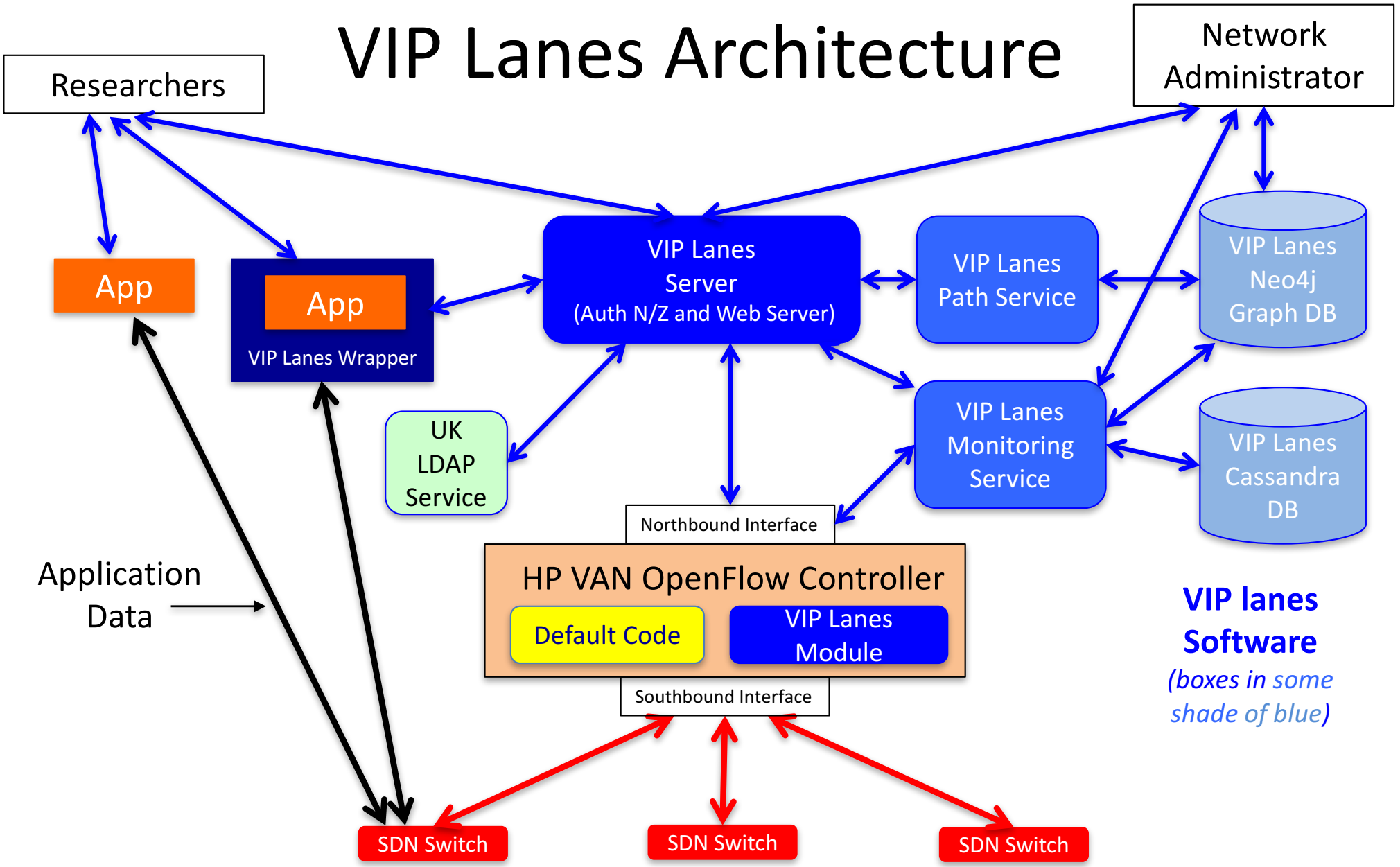
The SDN Control Software (aka VIP Lanes)

Prereq:

- Switches/Routers must be configured to process packets “normally” by default
- Multiple ways to achieve this. Easy way is to insert a “normal” rule.

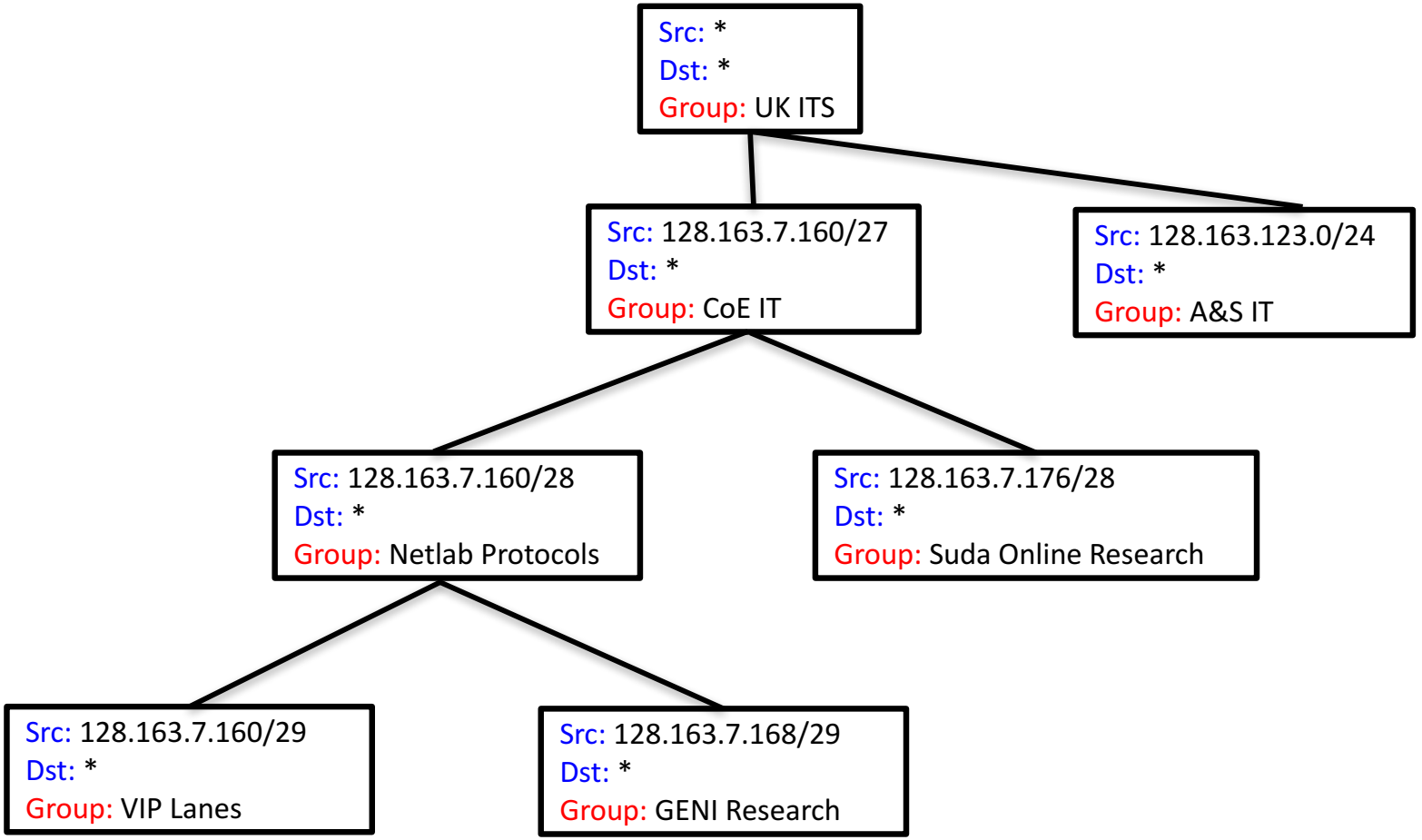
1. OpenFlow controller module
   - Discover topology information and makes it available to VIPlanes services
   - Accept requests to insert a set of rules comprising a flow
2. VIPlanes services
   - Discover the placement/role of middleboxes
     - Via topology discovery and config files
   - Accept requests to enable “privileged flows”
     - VIPlanes server authenticates/authorizes requests
   - Compute paths that by-pass middleboxes
     - Path computation service uses topo info to compute middlebox free paths
   - Compute SDN rules and invokes controller to insert them to “pick off” privileged flows
     - Path computation service and new controller module create and install rules
   - Ensure rules remain in place for the duration of the flow
   - Remove rules that are no longer needed
   - Gracefully handle failures

VIP Lanes Architecture



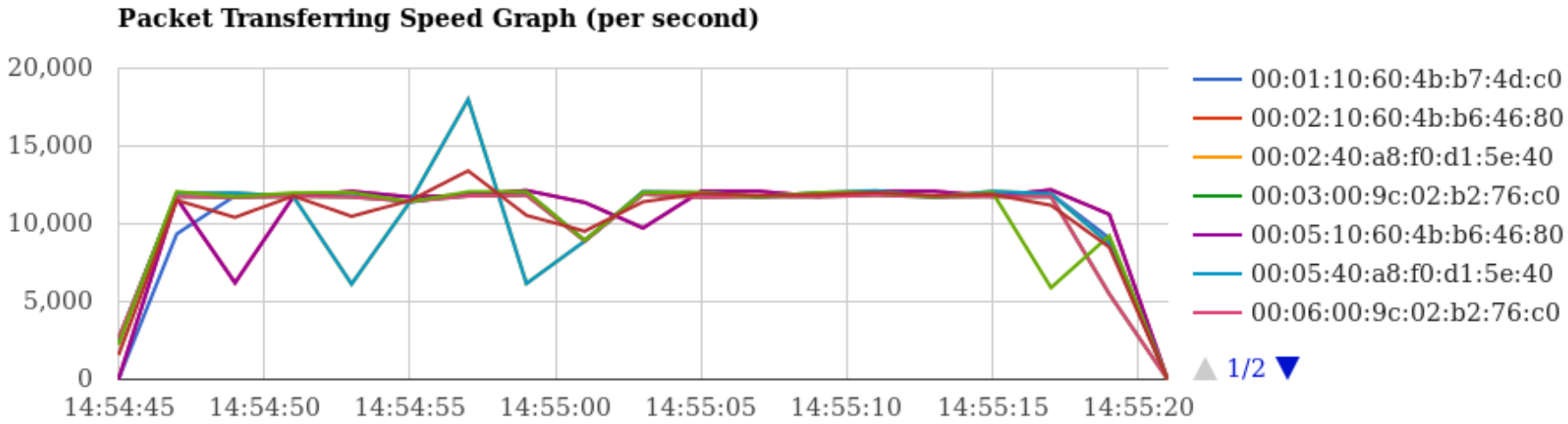
UNIVERSITY OF KENTUCKY

Example Flow Space Tree



Another Advantage:
Flow-level Monitoring

- OpenFlow support flow metrics (packet/byte counts) that enable flow-level monitoring
- Allows Users/IT to monitor performance of specific data transfers
- Can also be used for bandwidth management and debugging purposes



UNIVERSITY OF KENTUCKY

Deployment on UK Campus Network

- Deployed a new SDN Core network (OpenFlow) and connected it directly to the campus edge router.
- Deployed SDN-enabled switches/routers at the head-end of multiple science buildings. Some buildings are fully SDN-enabled.
- Deployed the VIP Lanes server to control the two buildings hosting CS department and Laboratory for Advanced Networking.

Sites	Normal (Mbps)	VIP Lanes (Gbps)	Speedup
ga-ptl.es.net (San Diego)	20.2	1.73	**85.6x**
hous-ptl.es.net (Houston)	34.6	3.00	**86.7x**
chic-ptl.es.net (Chicago)	55.98	4.86	**86.9x**
Wash-ptl.es.net (D.C.)	79.49	6.96	**87.6x**