Network Traffic as a Federated Testbed Service

Jack Brassil

Dept. of Computer Science

Princeton University, USA

IEEE
Future Networks™
WORLD FORUM • 2022

◆IEEE

FABRIC

- An emerging NSF-funded networking research infrastructure
- Built in part on fiber plant from ES-Net
- In-network compute, storage and programmable networking
- Plans to connect dozens of university campuses
- Federated – connectivity to other testbeds, public compute clouds, instruments (CERN)

Problem

- Some experimental networking research infrastructures (e.g., FABRIC) carry no production traffic
  - Electing *idealism* (e.g., reproducibility) over traffic *realism*
- Experimenters burdened with creating test traffic at ever higher bit rates
  - Foreground and background traffic

- Goal – develop a safe, decentralized, scalable, campus-based traffic injection service to ease this burden

Solution: Science Traffic as a Service (STAAS)

- Create a secure, scalable, system-wide, first-class experiment service to source `offered' traffic on experimenter request from many edge nodes (i.e., campuses).
- Leverage existing campus networking infrastructure (e.g., monitoring frameworks, packet brokers)
- Dynamically connect to FABRIC experiment container

STAAS Design Goals

- Data exchange upon two-sided agreement
- Maintain `essential' traffic characteristics
- STAAS service should not interfere with campus network ops
- Achieve traffic realism
- Ensure data privacy

Key STAAS Prototype Components

- Request
  - Traffic Manager (Flask web framework)
- Capture
  - Passive Optical TAPs, Port Mirrors
- Distribute
  - Network Packet Broker (Arista Monitoring Fabric w/ReSTful API)
- Clean
  - Payload processing appliance (DPDK based slicing, masking)
- Redirect
  - Programmable packet manglers (P4 and nftables) perform destination header substitution

Example: STAAS Operation
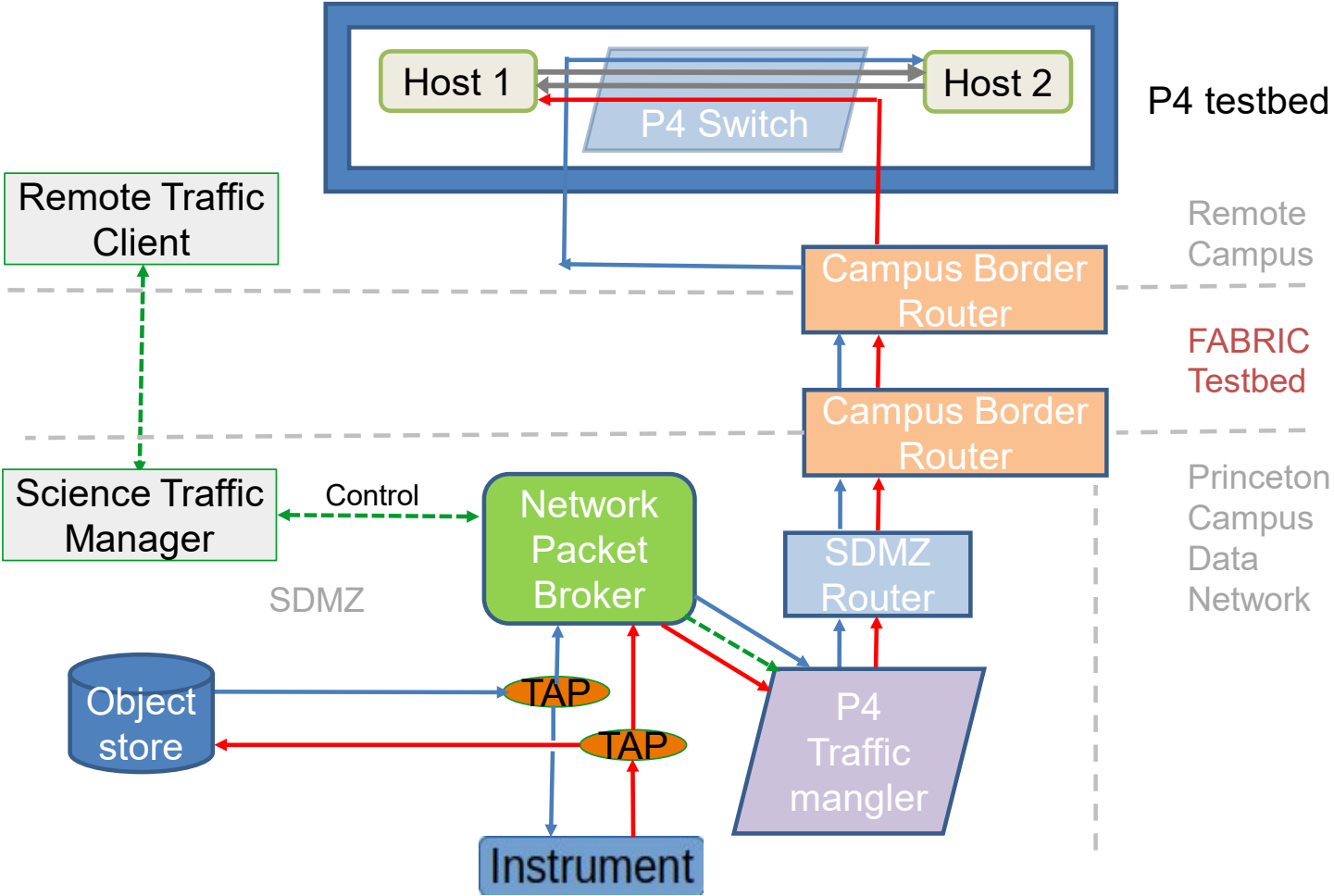
What campus flows can be redistributed?

- Access to campus flows is key policy question to study
- Different questions than `secondary use of research data'
- Each campus determines `offered' flows
- All flow captures require owner/authorized party permission with dictated sanitization
- Characterizing traffic
  - Plentiful low hanging fruit includes science traffic (e.g., distribution of public datasets, encrypted instrumentation)
  - Out-of-reach traffic includes campus administrative data traffic, dorm wireless traffic, DNS, etc.
- Stakeholders – IRBs, PIs, network operators, campus administrators, CISOs

Conclusion

- STAAS elevates network traffic to first class infrastructure service
  - Increasingly unrealistic to ask experimenters to generate traffic to study without more sophisticated tools and instrumentation support
  - Integrate synthetic traffic generation as needed
  - Allows experimenters to focus on innovative research

- Prototype development in progress
  - connecting to Princeton's FABRIC edge node
  - Ongoing surveys to determine experimenters' needs
  - Replication at other endpoints if successful

- Learn more
  - http://cs.princeton.edu/~jbrassil/public/projects/staas/staas.html

PRINCETON UNIVERSITY

Quad Chart for: *Science Traffic as a Service (STAAS)*

Challenge Project Seeks to Address:

- Some experimental networking research infrastructures (e.g., FABRIC) carry no production traffic
- Experimenters burdened with creating test traffic at ever higher bit rates
- Goal – develop a safe, decentralized, scalable, campus-based traffic injection service to ease this burden

Solution:

- Source `offered' traffic on experimenter request from many edge nodes (i.e., campuses).
- Leverage existing campus networking infrastructure (e.g., monitoring frameworks, packet brokers)
- Dynamically connect to experiment container
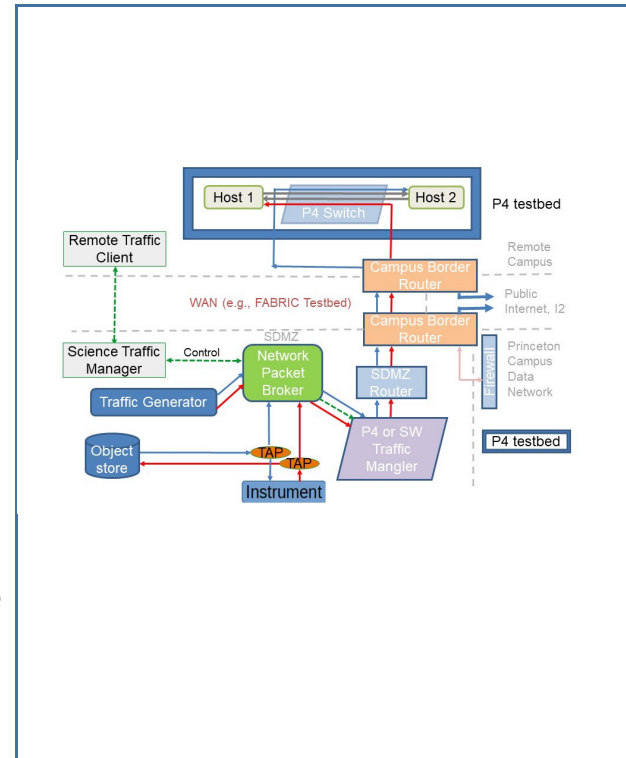
Scientific Impact:

- Increasingly unrealistic to ask experimenters to generate traffic to study without more sophisticated tools and instrumentation support
- Allows experimenters to focus on innovative research

Learn more:

- *http://cs.Princeton.edu/~jbrassil/ public/projects/staas/staas.html*