SDN Research and Operational Environments

Russ Clark/Ron Hutchins, et al
14 July 2015
LBNL

What is "Research," What is "Operational?"

- Research - "Hey, that's cool! Let's try it!" - implies the need for optimal, expeditious, continual changes toward the final goal, without the hindrance of supporting "real" users. ;-) The important part is making progress on the research.
- Operational - "Hey, I could lose my job for that!" - is the opposite, it implies the need for high levels of up time with change management so that users are not impeded in getting their work done. "Don't mess with my network!" The important part is to not rock the boat.
- Is there a way to combine these and do both? Sometimes… maybe…

What are past successes and hurdles of operationalizing research tools and technologies?

- It's mostly been easy to let researchers have access to campus fiber. Why?
- DNS researchers receive full DNS secondary feed to look for DNS security issues. How?
- BGP researchers receive full SOX routing table feed, live for BGP/SDN work. Why?
- Security researchers received network flow data until startup company formed. How?

GENI success was enabled through trust among people across both realms with common goals.

Real networking has more safeguards in place but GENI had enough for its goals.
Early days of GENI, operationalizing required agreement between researchers and operational engineers around:

- Ongoing clear communications across the stovepipes.
- Written policies describing practices/actions/workflow in various situations.
- Approvals up the food chain in order to deploy or change stuff (responsible parties).
- Change management - notification of outages in a pre-defined window only.
- Strong attention to detail around security issues (don't blackhole the campus, etc.)
- Campus SDN projects required changes to switches that production engineers were not comfortable supporting:
  - Changes caused crashing of hardware and instilled distrust in engineering staff.
  - Policy language is low level so requires very simple policies (VLANS) or much work to convince staff to trust.

Where are we today?

- GENI - In the Southeast, several campuses and the SOX regional optical network have deployed GENI racks, student and test projects have been implemented as demonstrations.
- Science DMZ's are under construction in places - many are not SDN driven, however.
- SDN as VLAN management - Internet2 is moving to VLAN management via SDN on the production network, augmenting OSCARS, etc.
- SDX/SDI as the next set of research topics:
  - Federation of controllers
  - Peering via dynamic policies vs. static rules
- Some rationale and current projects - …

Goals For SDN/SDI

More Agility and Control Of Our Network!

- Active Control Plane - control in real-time, not just maintenance windows

- Policy Management

  - better than VLANs, Subnets, Firewalls, IDS, IPS, etc

  - VLAN blunt instrument -> blunted further by Wi-Fi SSID

- Network Access Control

- Capacity Monitoring and Management

- Simplified Configuration - "virtual patch panel"

- Security, Data Privacy

  - better monitoring, finer-grained active control

- Better Student Projects!!! It makes teaching fun again.

Some of the SDN/SDI Projects at GT

- Original GENI Campus

  - began OpenFlow deployment in 2010, used in classes and research, Mesoscale resources, GENI racks today

- GENI Regional Deployment at SoX

- Network Access Control

  - demonstrated captive portal system - *Resonance*

- Video Distribution and Manipulation - Magic Window

- SDX - Software Defined Exchange - Regional and International
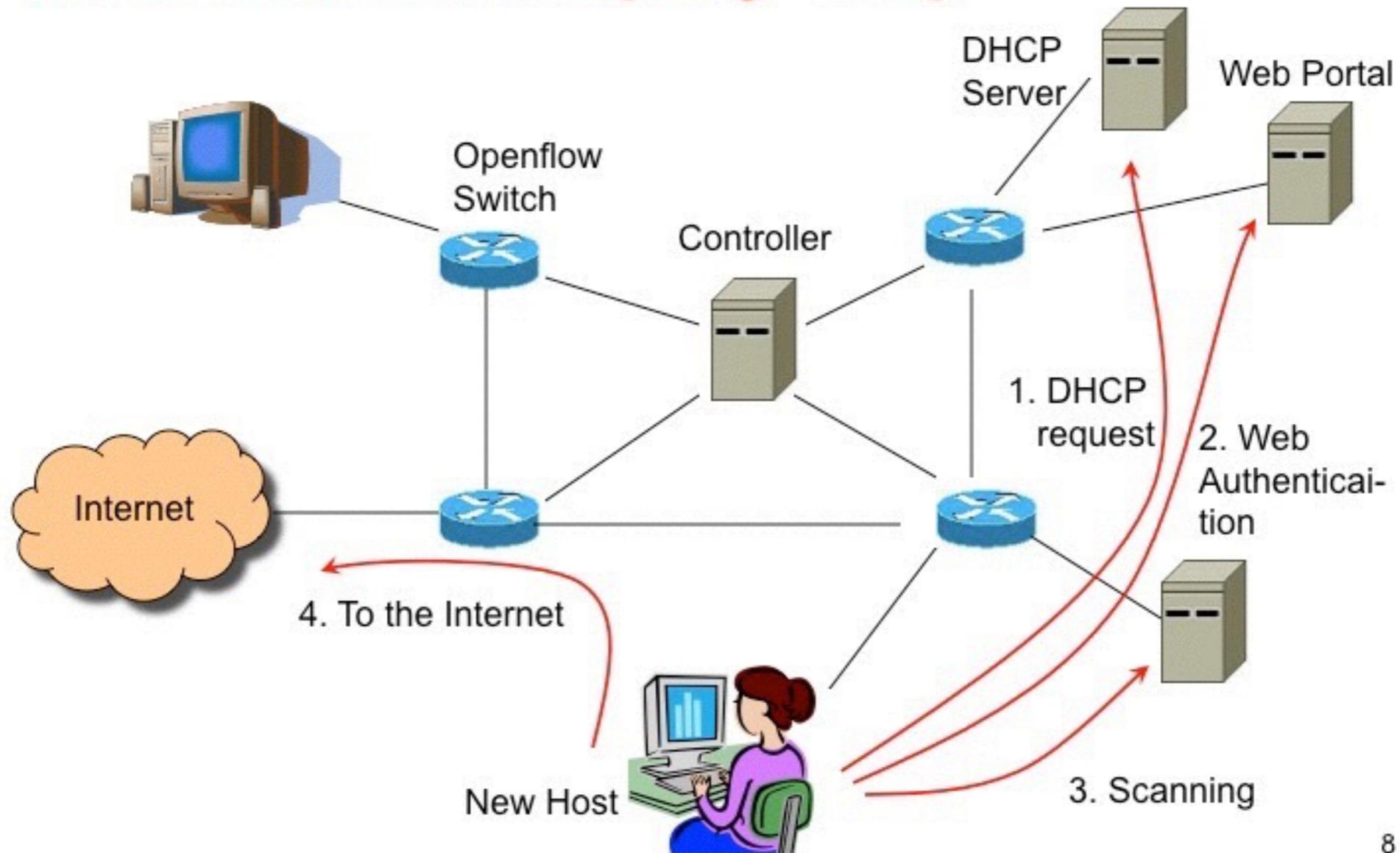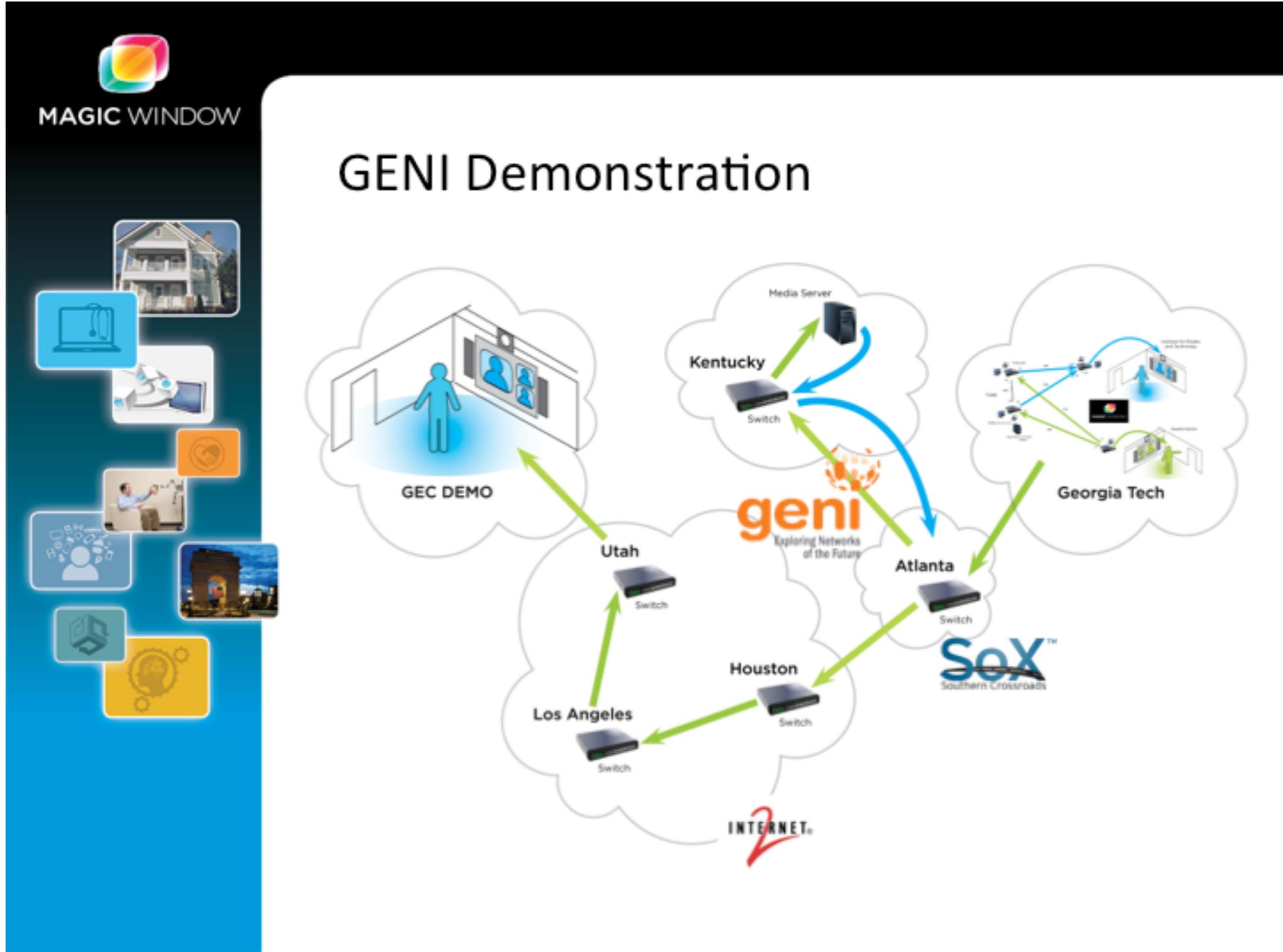
GENI @ SoX
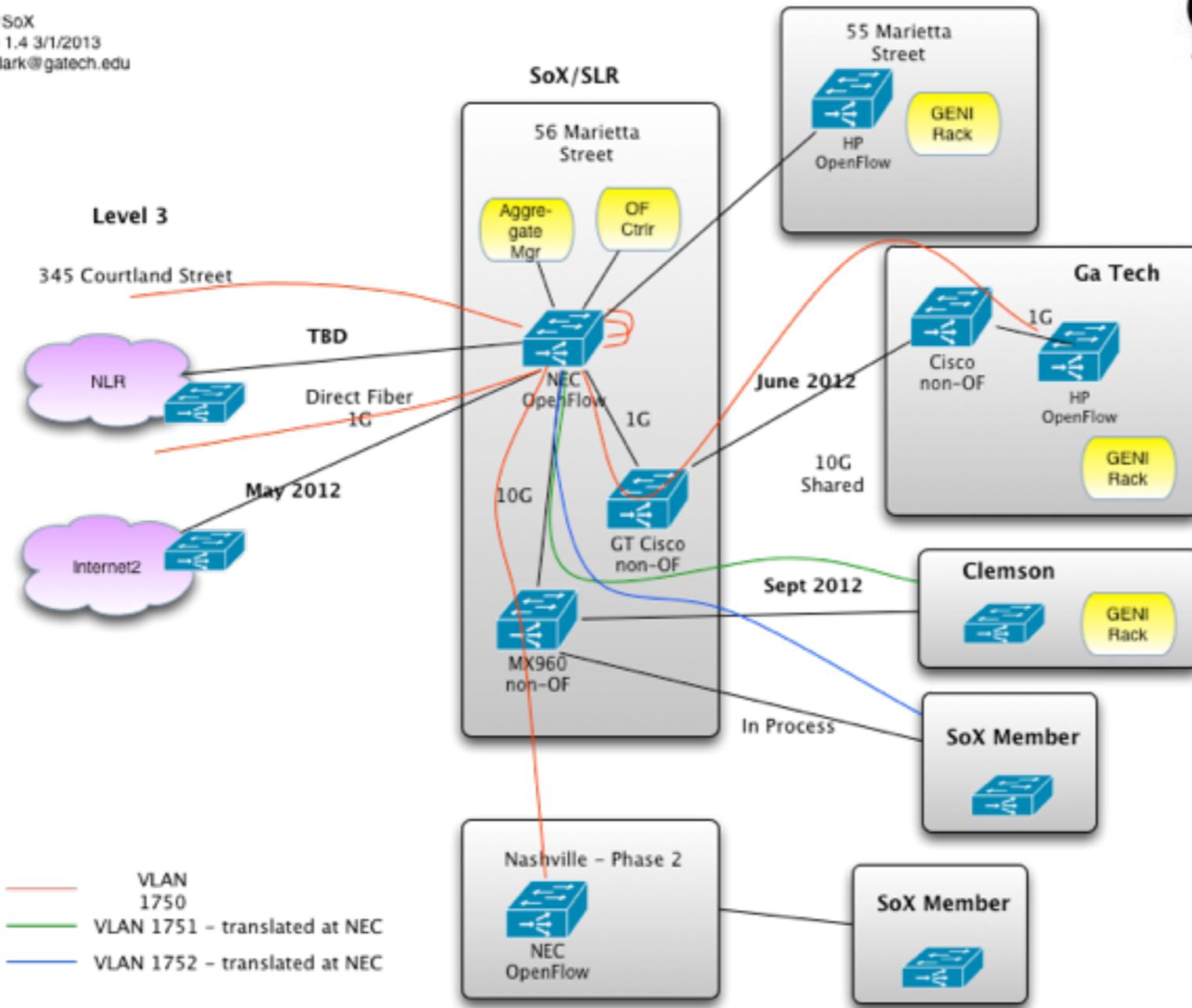
- NEC PF5820 Switch Deployed - June 2012
- FOAM and FlowVisor - July 2012
- Georgia Tech - July 2012
- Clemson University - Sept 2012
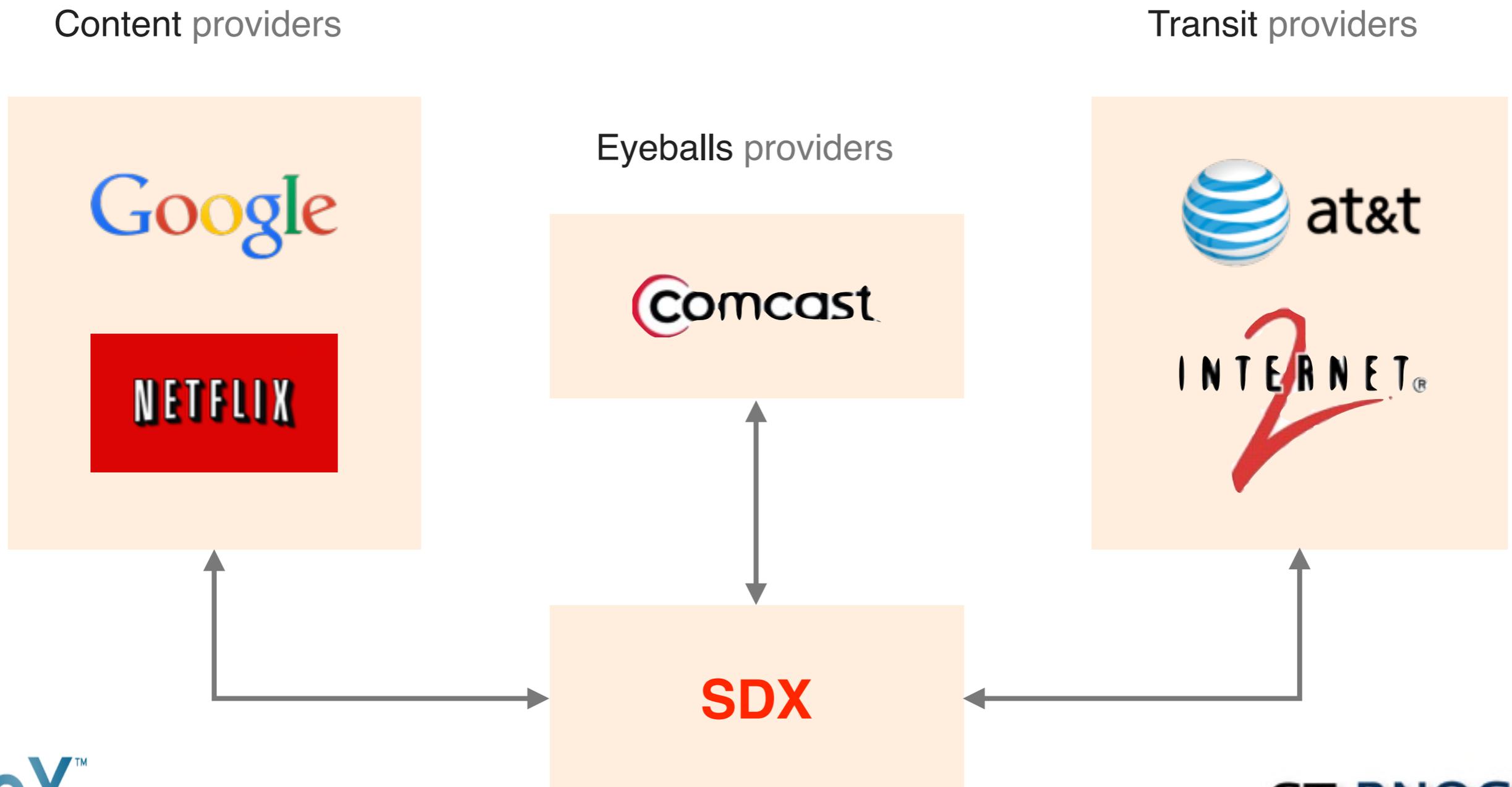- GENI racks in 2013
- Ready for more campuses

Resonance: Step by Step

GENI Demonstration

SDX is a platform that enables multiple stakeholders to define policies/apps over a shared infrastructure

Content providers

Transit providers

Eyeballs providers

SDX

SDX enables a wide range of novel applications

security

Prevent/block policy violation

Prevent participants communication

Upstream blocking of DoS attacks

forwarding optimization

Middlebox traffic steering

Traffic offloading

Inbound Traffic Engineering

Fast convergence

peering

Application-specific peering

remote-control

Influence BGP path selection

Wide-area load balancing

- Five year NSF Project

- Support large data flows from new telescopes in South America

- Includes stitching and SDI capabilities

- Must support dynamic allocation across multiple domains

Ongoing SDN Efforts
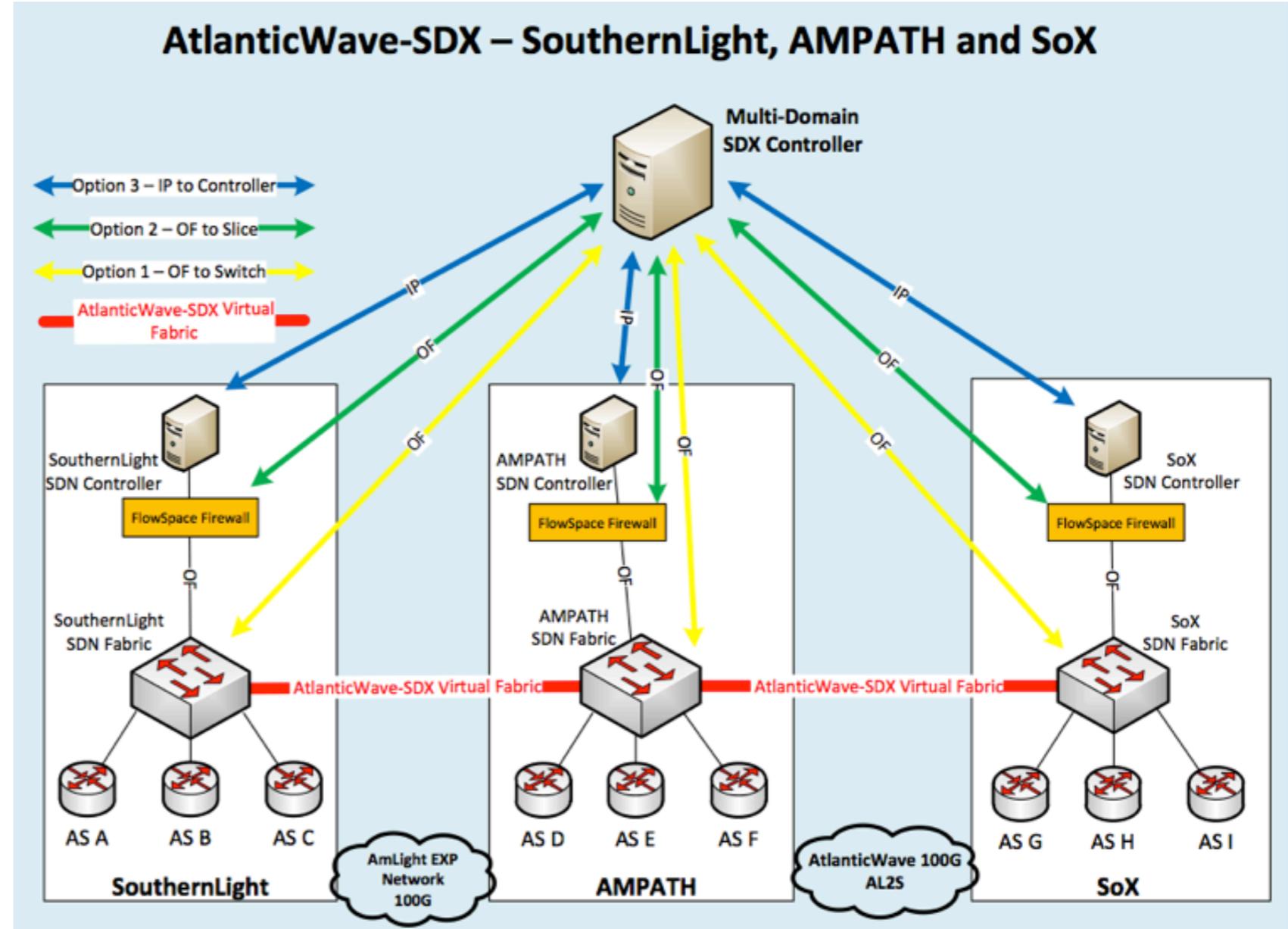
- Protected Data Management Architectures

    - providing storage and compute for sensitive data (e.g. HIPAA)

- Personal Devices in the Enterprise

    - dealing with dozens of personal/consumer devices on the enterprise network - e.g. give each user a "personal network" abstraction

- Video Distribution

    - MPEG-dash over SDN

What's needed to get to where we need to be?

- How do we share production traffic with researchers while not impaction production quality?
- How do we do early deployment in a production environment without putting "uptime" at risk?
- How do we train production engineers on the new technologies. "Trust me" isn't going to work in the future, even if it sometimes did in the past.
- How do we show security capability of at least as good or better than without SDN?
- We need to show that the capabilities of SDN bring enough value to the table to outweigh the "pain" of implementing them in the production network.
- Protected data management is a great focus for SDN/SDI. The agility benefits must be auditable! We want to leverage SDN to help deal with (HIPPA, FERPA, ITAR, PCI) but all of those require separate physical infrastructure today and we need to be able to show that SDN allows us to provide the security/privacy requirements via slicing/virtualization.
- Discussion?