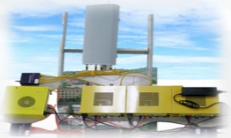
geni
Exploring Networks of the Future



GENI

Welcome to GEC23!

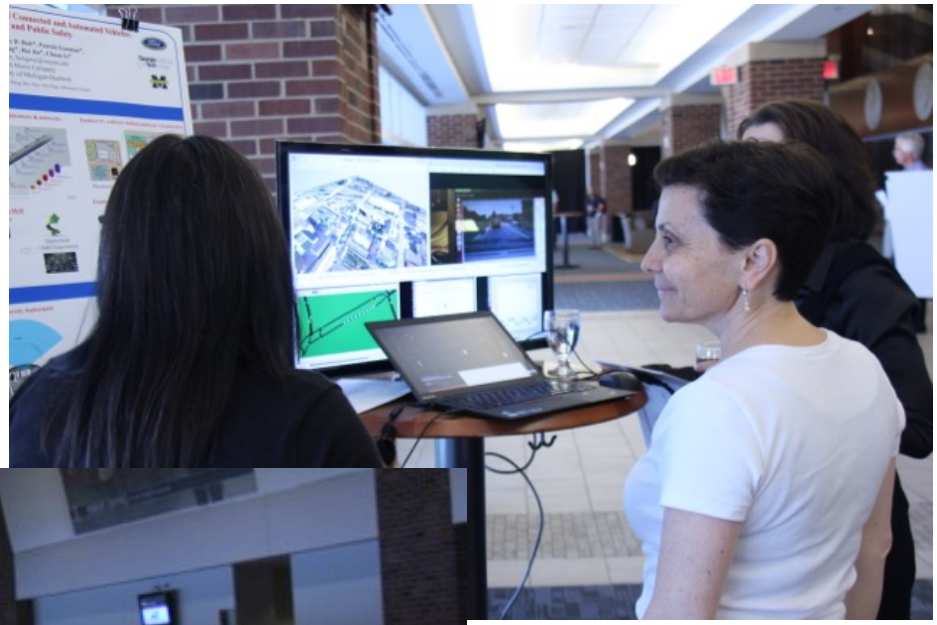
Mark Berman
June 17, 2015
www.geni.net

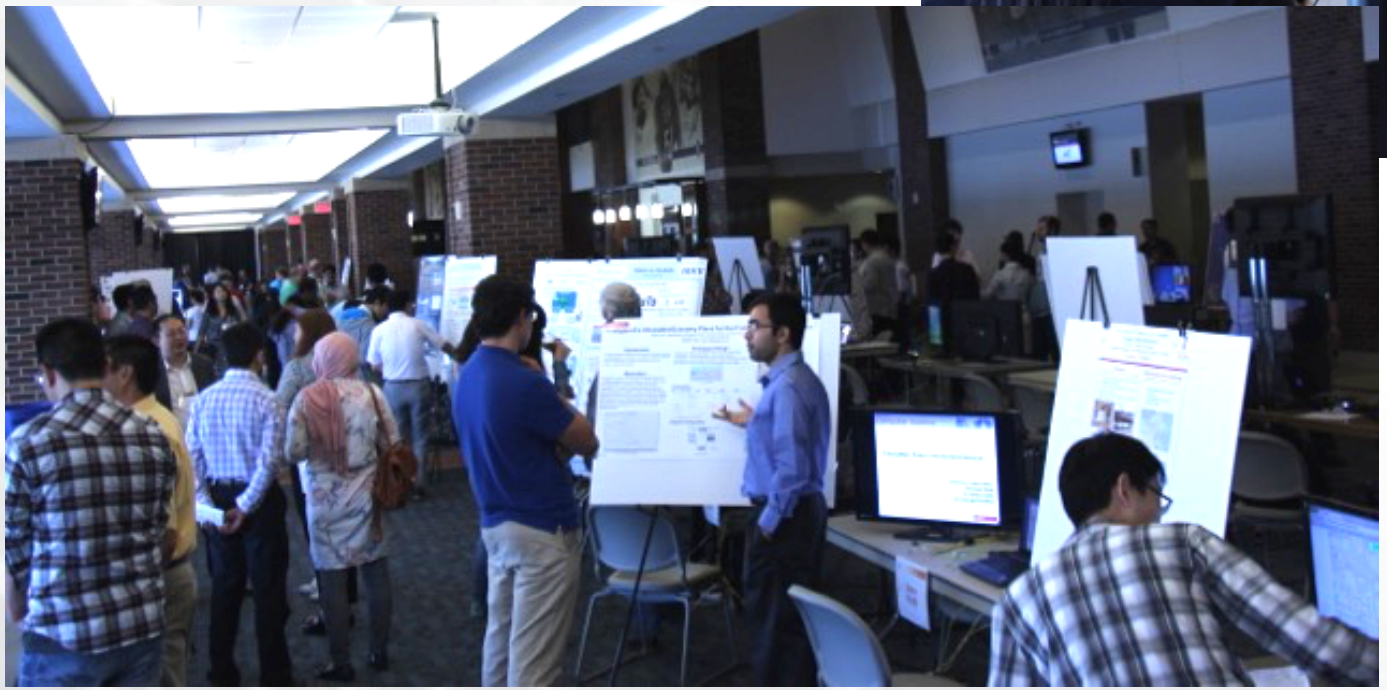
Sponsored by the National Science Foundation

Welcome to UIUC!

Thank you to our hosts

- University of Illinois at Urbana-Champaign
- Debbie Fligor
- Brighten Godfrey





Welcome to GEC23!

Mark Henderson

Chief Information Officer, UIUC

Welcome to GEC23!

Bryan Lyles

Program Director
NSF CISE/CNS

Photo © Marc Smith, CC-BY 2.0 license

Erwin Gianchandani

Deputy Division Director
NSF CISE/CNS

GEC23 Outstanding Demo Awards

1st place

- Symbiotic Evolution of CAV Applications & Networks – Yuehua Wang

2nd Place

- GENI for Classes and GENI for the Masses – Fraida Fund

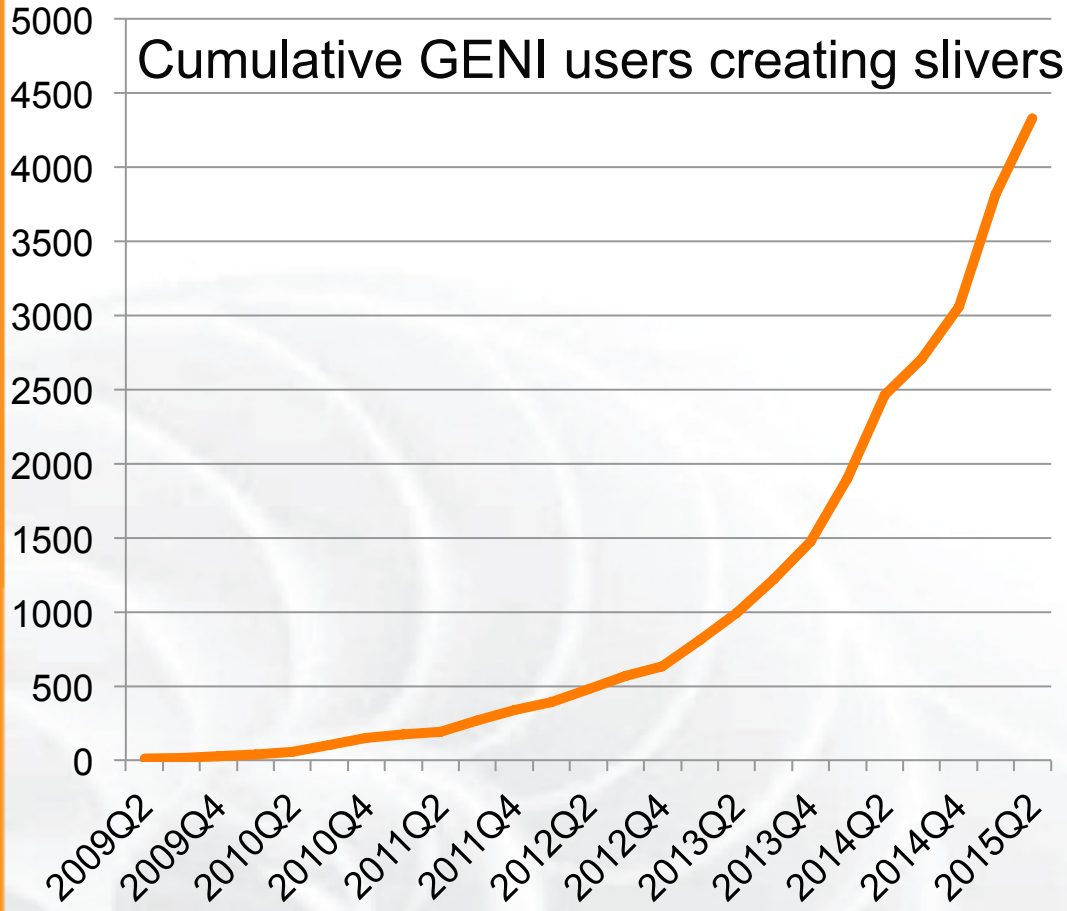
3rd Place

- Resilience of KanREN OpenFlow Network to Large-scale Disasters – James Sterbenz

Introducing Dorene Ryder

Please welcome Dorene as GENI project manager.

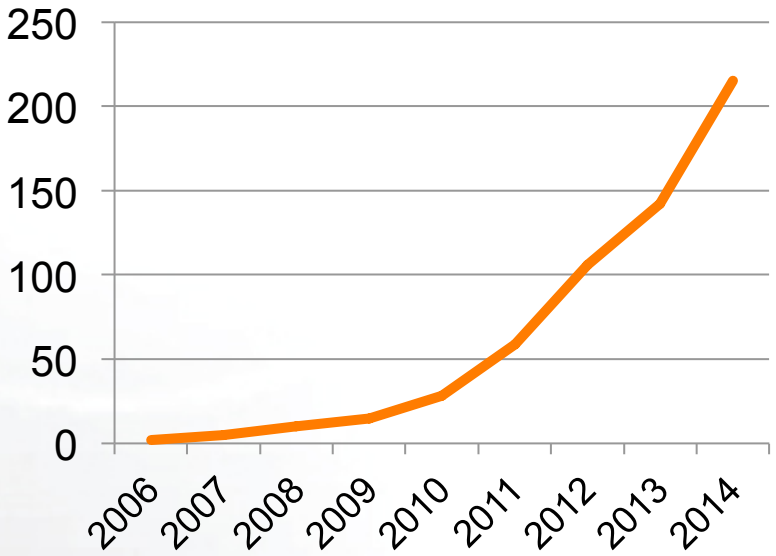
GENI Update
Strong User Uptake and Research Results



Over 4300 GENI users to date!

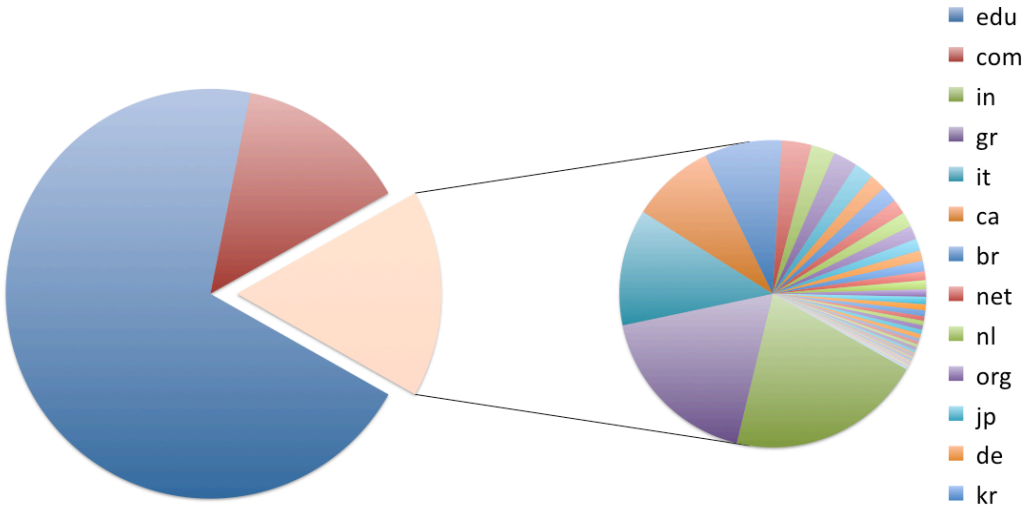
More than 200 papers in GENI bibliography.

- Missing yours? Please let us know.



Cumulative GENI bibliography entries by year of publication

GENI Update
Portal Usage Statistics

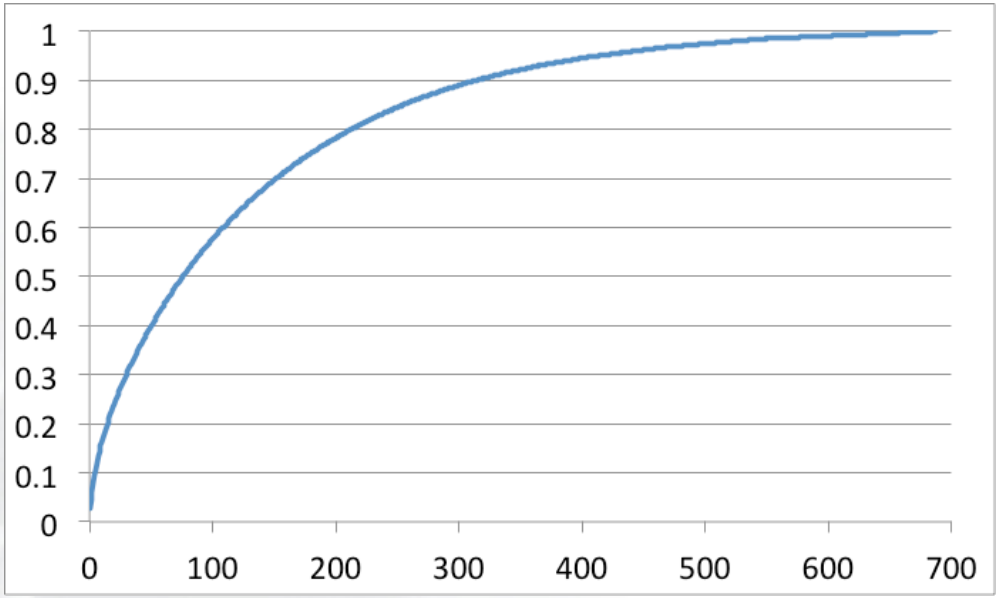


Portal users

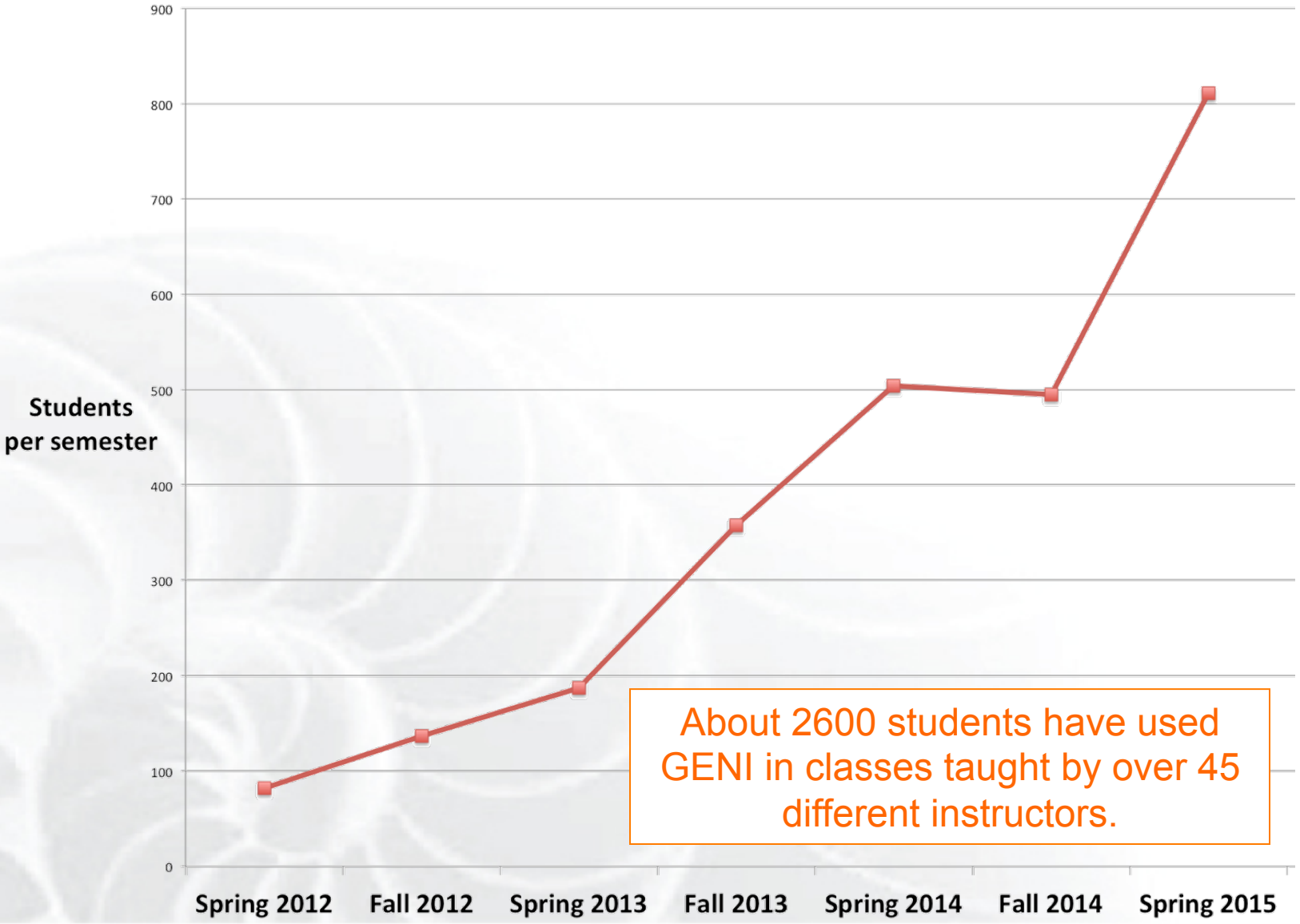
Distribution by top-level domain

Recent reservations

CDF of distribution by user



Students in Classes Using GENI



About 2600 students have used GENI in classes taught by over 45 different instructors.

GENI Summer Camp 2015

University of Connecticut, Storrs
26 – 30 May 2015
Host: Bing Wang

18 participants, 15 institutions

Five group projects
- 3 SDN projects
- 1 Hadoop project
- 1 Wireless + SDN project

GENI at Conferences and Workshops

TRIDENTCOM
Testbeds and Research Infrastructures for the Development of Networks and Communities

Tutorial: Building Experiments Using the GENI and SAVI Testbeds
24 June 2014
Vancouver, Canada

Computer and Networking Experimental Research using Testbeds
29 June 2014
At ICDCS in Columbus, OH

Papers and demos on research validated using testbeds

Project Silver
Rethinking Security in the Era of Cloud Computing

Cloud Security Curriculum Development Workshop

Tutorial on Network Function Virtualization using GENI
Organized by Jay Aikat, U. of North Carolina

Upcoming GENI Training Events

FGRE Summer Camp
6 – 10 July 2015
iMinds, Belgium
Hosted by Becht Vermullen

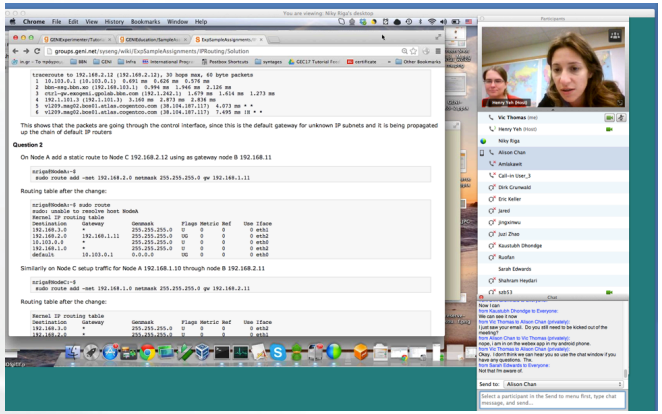
Tutorials on using GENI and FIRE tools and resources

GENI Regional Workshop
18 – 19 September 2015
Northeastern Illinois University
Hosted by Graciela Perera

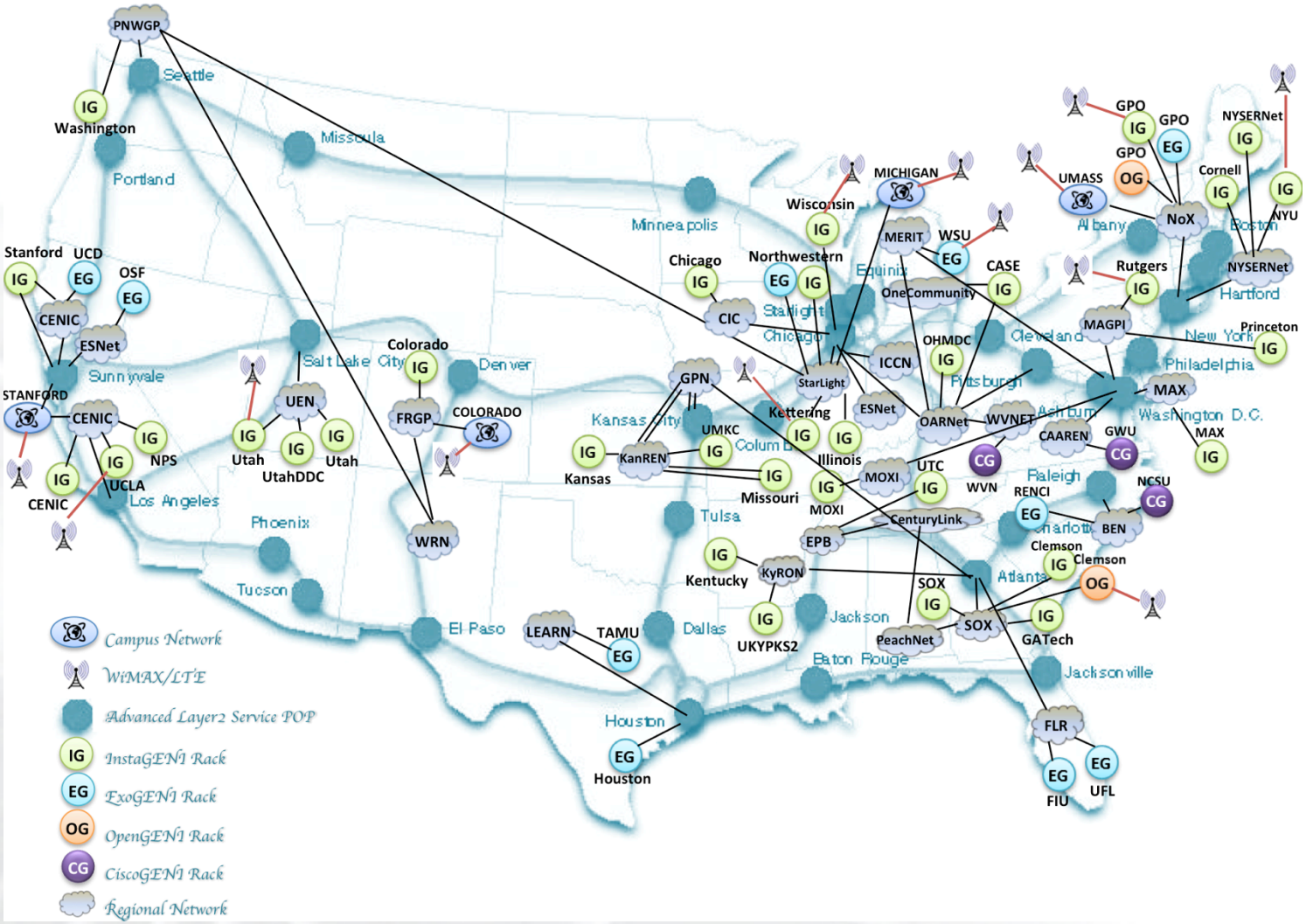
GEC-like tutorials

Train-the-TA
Fall 2015

Tips for instructors and TAs running classes on GENI

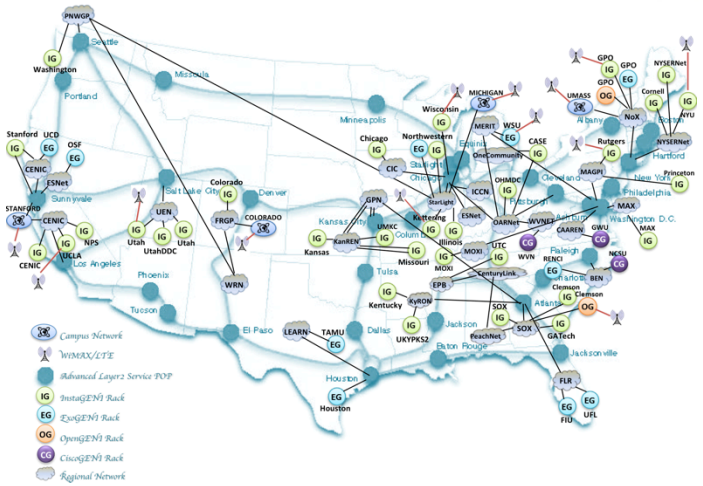


Building Out the GENI Infrastructure



Infrastructure Engineering

- 61 racks deployed/in progress
  - 13 ExoGENI, 42 InstaGENI
  - 2 OpenGENI (Dell) racks
  - 3 Cisco racks
  - 1 Ciena rack prototype
  - Documentation: http://groups.geni.net/geni/wiki/GENIRacksHome



- Major progress in GENI stitching
  - 27 sites: http://groups.geni.net/geni/wiki/GeniNetworkStitchingSites
  - New stitching AMs (AL2S, Utah-Stitch) & stitching computation service (SCS) in production. MAX and StarLight stitching aggregates in development.
  - ION stitching decommissioned in favor of AL2S.

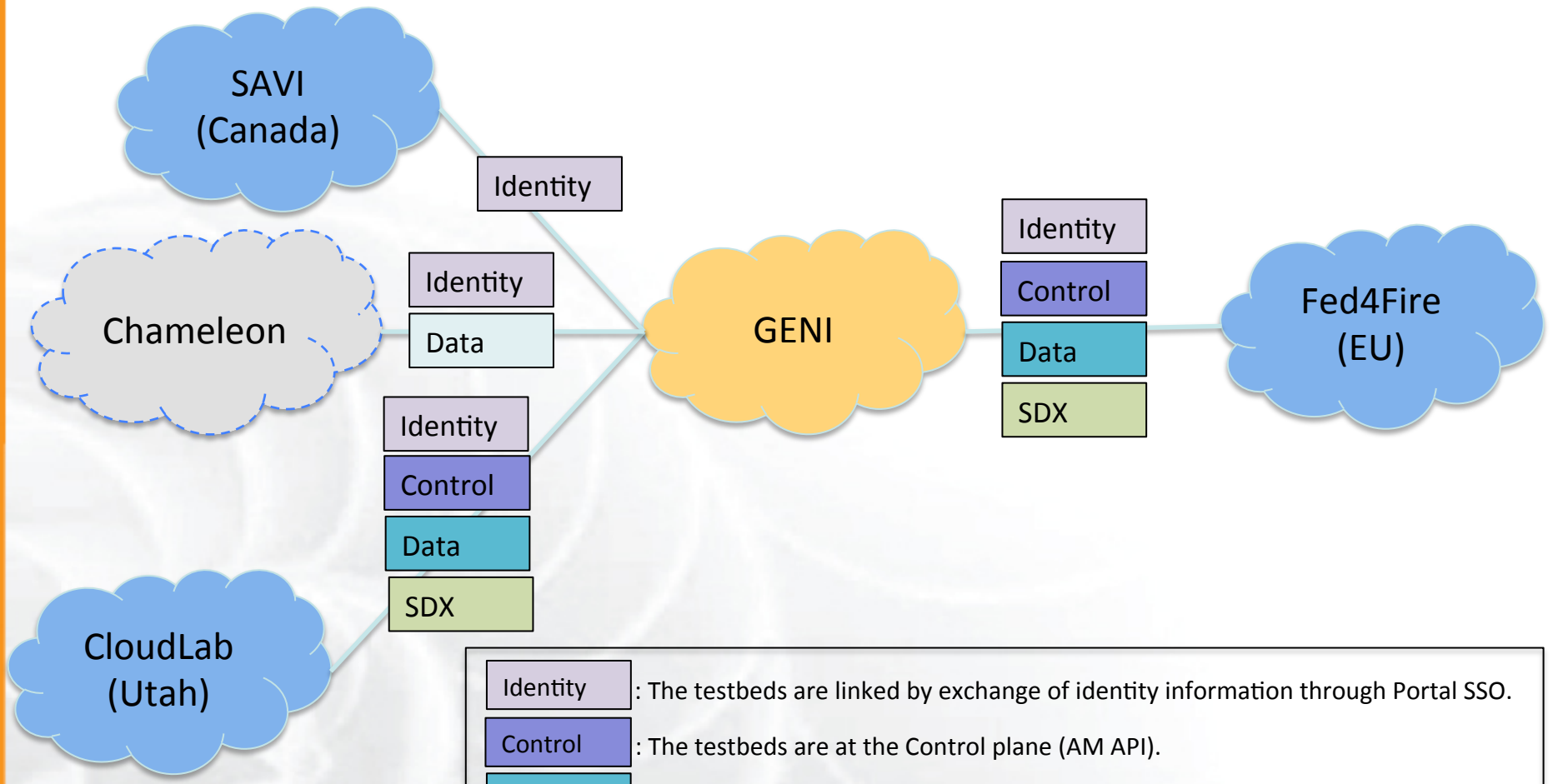
Over 90 aggregates available via GENI portal

Infrastructure Engineering (cont.)

- GENI integration with Internet2 updated FSFW and OESS software
- OpenFlow Slicer (FV replacement based on I2 FSFW) integration testing with CENIC, NYSERNet
- Updated GENIMon OpenFlow controller integration testing with Internet2
- Write/Review procedures for Operations Trials (Welcome UKY to Ops)

GENI Federation: Status and Plans

GENI is expanding its scope by federating with additional cloud testbeds.



Software Defined Exchanges (SDXs) at WIX and iMinds

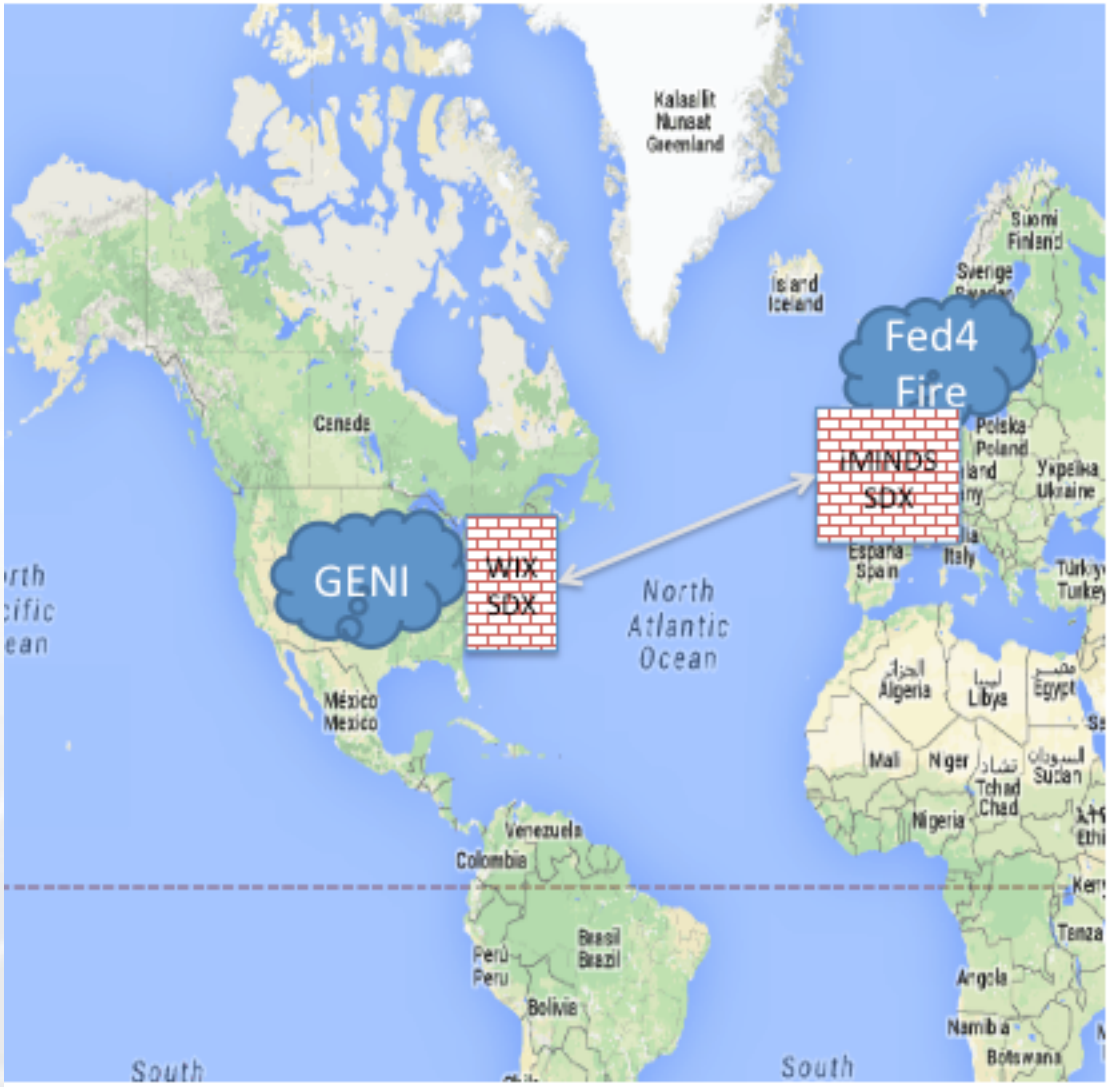
In a joint collaboration between GENI and Fed4Fire, we have established two prototype SDX sites at:

- WIX (Washington Internet Exchange)
- iMinds (Belgium)

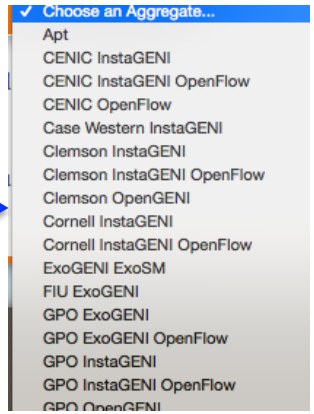
These sites are full aggregates at which one can allocate compute and storage resources.

But they also serve as 'gatekeepers' for allocation of network resources across the US and EU domains.

Authorization engine and prototype policies limit BW or VLAN allocation by users from one side to the other.



Recent Tool Progress

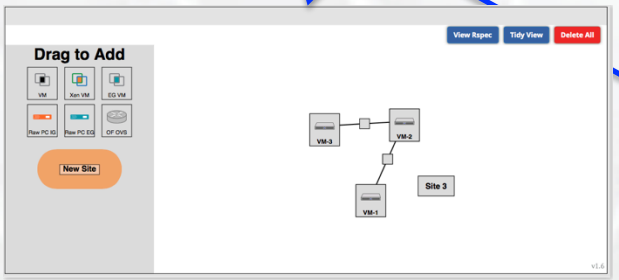


33 new aggregates, including: APT, AL2S, OpenGENI, CloudLab, iMinds Virtual Wall

GCF / omni / stitcher

Enhanced Support for:

- Stitching (AM API v3)
- ExoGENI
- Update()
- Client tools using GCF



Jacks Topology Editor and Viewer Integration

- Constraint system guides users to feasible topologies
- Just draw a link for stitched topologies

jFed CloudLab SAVI

Integration with additional resource testbeds

GENI Portal, Clearinghouse, Tools (GCF) software released in GitHub

GENI Monitoring Available Racks, Networks, Slices, Slivers

GENI Monitoring: Exploring the System from the User Perspective

Tutorial at Ops Session: Wednesday 4.00pm - 5.30pm

http://genimon.uky.edu/login

GENI Transition

What's coming up next?

Now – Fall 2015 (5 months): Transition planning

- Broad community participation – both GENI participants and others. (Invite your friends!)
- Brainstorm & solicit participation – now
- Gather & analyze community input – Aug / Sep
- Complete & publish plan – Oct / Nov

Fall 2015 – Fall 2017 (2 years): Transition to community governance

- GENI project office handoff in 2017

GENI Transition

Goals

- Operations, sustainment, improved reliability, modest growth in scale and capability
- Growing research and educational user community
- Maximize influence on upcoming research cyberinfrastructure programs through federation (US and international)
  - Control plane / API, data plane, SDX

NSF is committed to a GENI transition that assures ongoing GENI operations and fosters community growth.

Shaping the Future of Research Testbeds

This is a very dynamic time for design and development of research cyberinfrastructure

- Recent and upcoming workshops have helped scope the challenge
  - Infrastructure for the Wireless edge (Nov. 2014)
  - Mid-Scale cyberinfrastructure control plane (Oct. 2014)
  - SDX (multiple)
- NSF Cloud program is underway
  - Both teams are closely integrating with GENI
- We can anticipate future NSF interest in this area

The GENI community is uniquely positioned to have a powerful influence on the next generation of cyberinfrastructure.

Changes coming to GECs

Recent GECs have covered the range from newcomer tutorials to demos and from curriculum development to design debates. Upcoming events will be more specialized

- Regional events with tutorial emphasis
- Community events with researcher and educator emphasis
- GECs, likely smaller, and with increased emphasis on engineering

New meeting structure is an experiment to be revisited during the transition process.

Mark your calendars!

Upcoming GENI events

- GENI community event in conjunction with ICNP
  - Nov 10, San Francisco
- GENI regional conference
  - 18-19 September 2015, Chicago
  - Hosted by Graciela Perera, Northeastern Illinois University
- GEC24 – Spring 2016
  - Interested in hosting? Speak to Mark or Dorene.


geni
Exploring Networks
of the Future

Looking Beyond The Internet

Chip Elliott
GENI Project Office

Looking Beyond the Internet

A proposal for next steps

Chip Elliott
GENI Project Office

A vision for NSF CISE Experimental Midscale Infrastructure

A common vision:

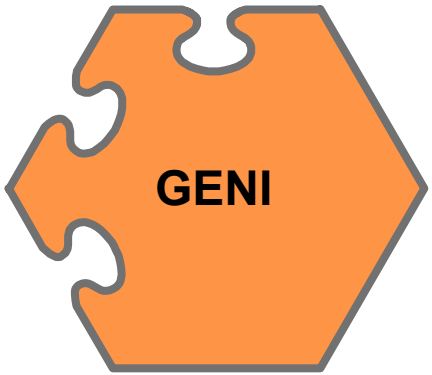
Is there a need for midscale infrastructure? *Yes!!*

> *"A nationwide, multi-tiered system (national/regional R&E backbones, data centers, campuses) that is sliced, deeply programmable, virtualized, and federated so that research experiments can run `end to end' across the full suite of infrastructure."*

- *multi-tiered system (national/regional R&E backbones, data centers, campuses:* core/edge networking, computation, clouds
- *sliced, virtualized:* one (logically shared) physical infrastructure
- *programmable*: platform for innovation
- *federated:* organic growth, skin-in-the-game business model

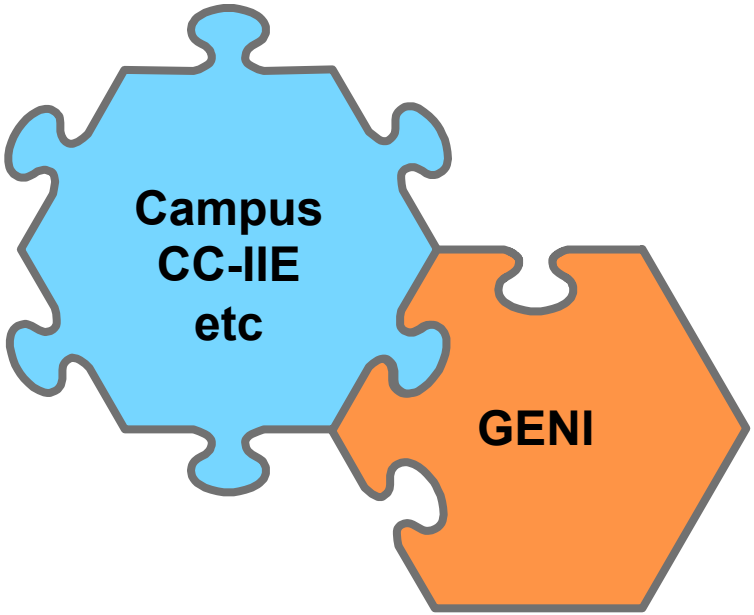
"Midscale infrastructure investments to support computing research", 2013. Committee chaired by Jim Kurose, this slide by Steve Corbató et al.

c. 2010



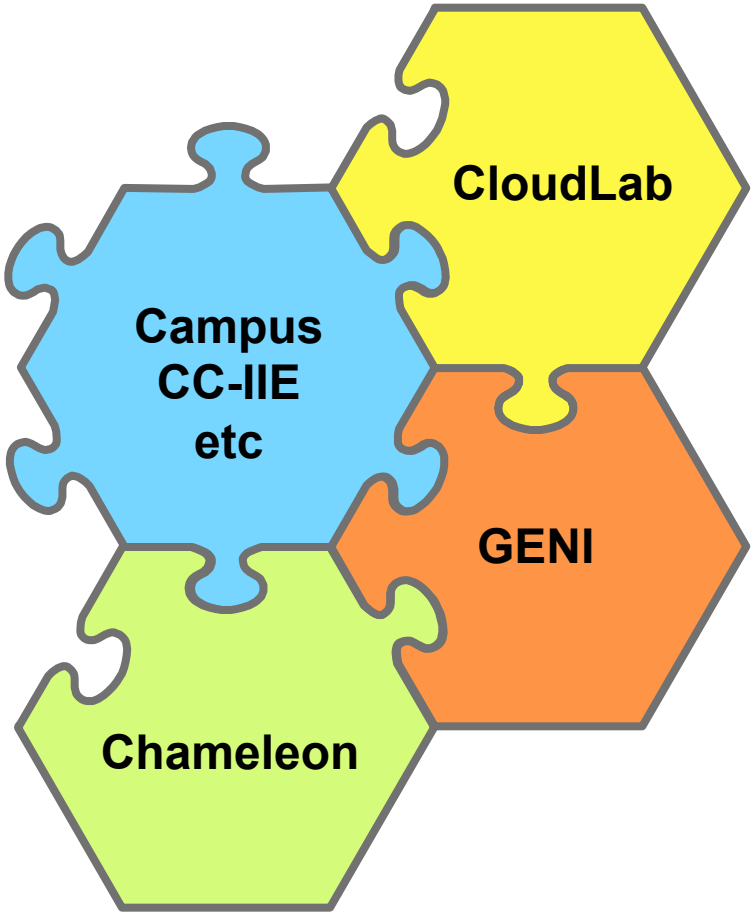
Interoperable systems supporting end-to-end slices

c. 2013



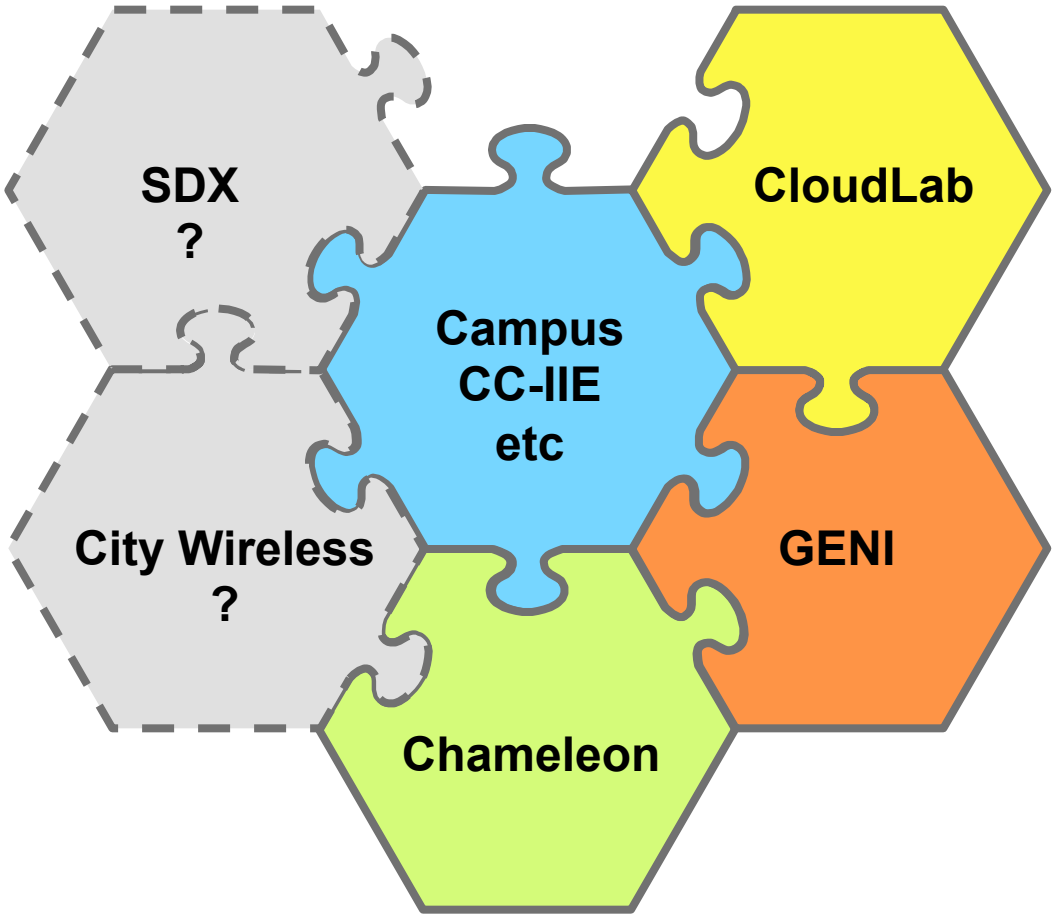
Interoperable systems supporting end-to-end slices

c. 2015

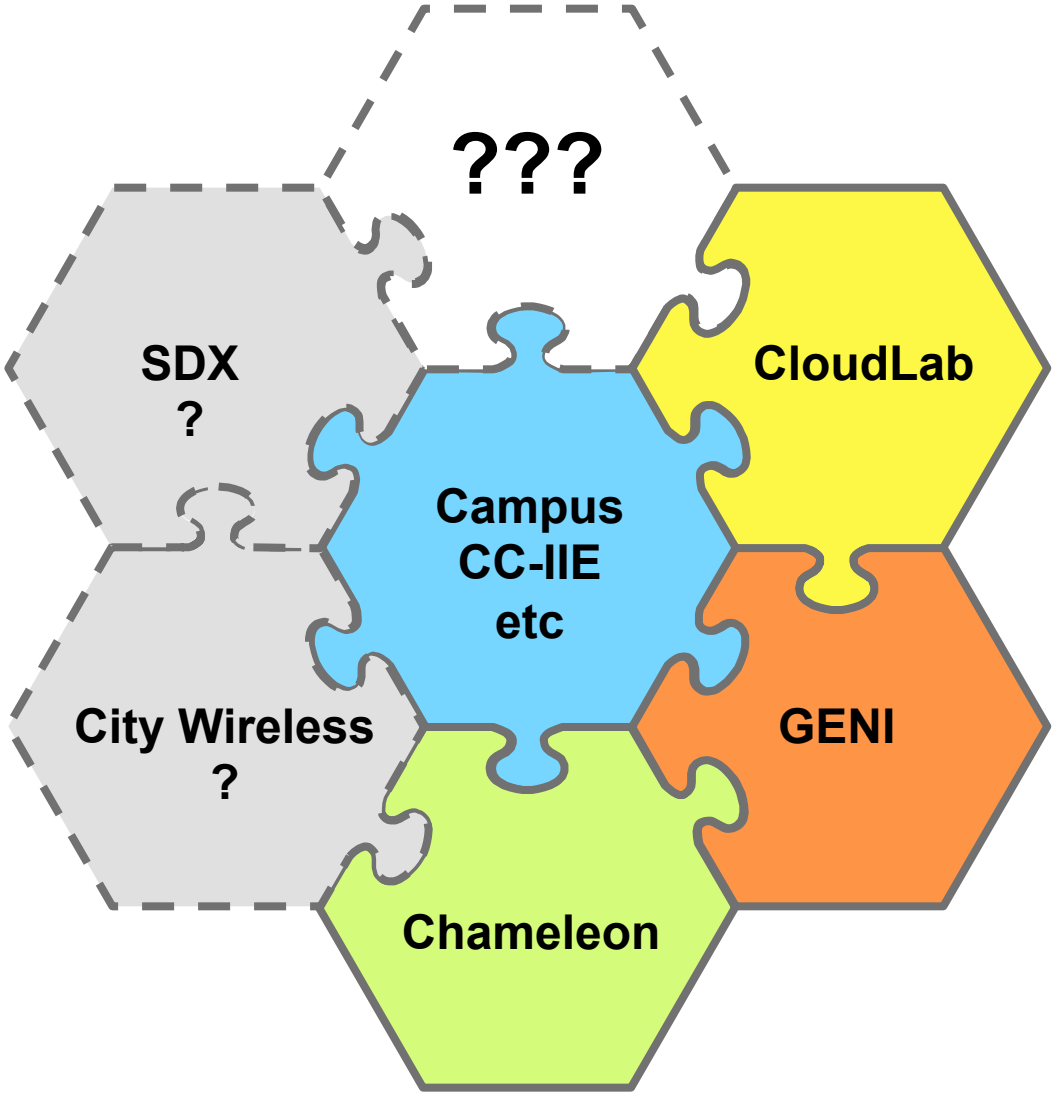


Interoperable systems supporting end-to-end slices

c. 2018 ?



c. 2018 - other good ideas ?



“Looking Beyond the Internet” proposal submitted to NSF

- Key NSF workshops to date – including the Workshop on Operationalization of Software-Defined Networks (SDN) in December 2013, the Software Defined Exchange (SDX) Workshop in June 2014, and the Future Research Infrastructure for the Wireless Edge in November 2014 – have made it abundantly clear that experimental research in this area can bring very high payoffs for society and our economy.

- **Now is the time, therefore, to make concrete plans** for exploring these emerging planetary-scale cloud / wireless / network systems beyond the Internet.

Proposed goal

- **Draw up a candidate set of concrete plans** for exploring these emerging planetary-scale cloud / wireless / network systems beyond the Internet

- **Do so by engaging the network and distributed systems research communities** (broadly construed) to identify exciting and challenging research problems in this space

- Based on these key research problems, **identify the requirements for mid-scale infrastructure** that can support experimental research in this area.

Proposed Approach

- **Stand up a Planning Group** to help organize and engage the relevant communities, and to document both the emerging research challenges and their requirements for infrastructure.

- **Organize a set of targeted workshops** in this area, under the auspices of the Planning Group, which will engage and gather inputs from the relevant research communities, summarizing the discussions and recommendations of each workshop in a public document.

- **Draw up a planning document** for the CISE research community that incorporates observations and recommendations from both the Planning Group itself and the workshops it has run.

- In parallel, we will ask the Computing Community Consortium (CCC) to **solicit white papers** in this area from the research communities as inputs for consideration by the Planning Group.

Proposed topic areas

- **SDX Research.** Researchers working on SDX-related issues including those who are building prototypes.

- **City-Wireless Research.** Researchers (SDX, cellular/ wireless, smart cities) and potential commercial partners, to investigate the potential of next-generation wireless/cloud systems, with an eye towards research experimentation in city-scale deployments.

- **Novel Apps and Services.** Cellular/wireless researchers, SDX researchers, smart city researchers, and application developers.

Interested? Want to participate?

- This is meant to be a very open, interactive process with broad participation
- Do you have ideas ? Are you interested ?
- Let's talk !

But remember – this is only a proposal ! We will see if it gets funded . . .


geni
Exploring Networks
of the Future

Guest Talk: NCSA Experience Protecting an Open Computational Environment

Randal Butler
Director of Cybersecurity
National Center for Supercomputing Applications

NCSA Cyber Security Directorate (CSD) GEC23

Randy Butler

June, 2015

National Center for Supercomputing Applications
University of Illinois at Urbana-Champaign

- NCSA Overview
- Open Science Computing Environment
- NCSA Cyber Security
  - CSD
  - Influences
  - Threats
  - High-level Approach
  - Developing Concerns

The National Center for Supercomputing Applications (NCSA)

- NCSA is a hub of interdisciplinary research and digital scholarship.
- Provides computing, data, networking, and visualization resources & services that help scientists, engineers, and across the country better understand our world.
- Established in 1986 as one of the original sites of the National Science Foundation's Supercomputer Centers Program, NCSA is supported by the state of Illinois, the University of Illinois, the National Science Foundation, and grants from other federal agencies.

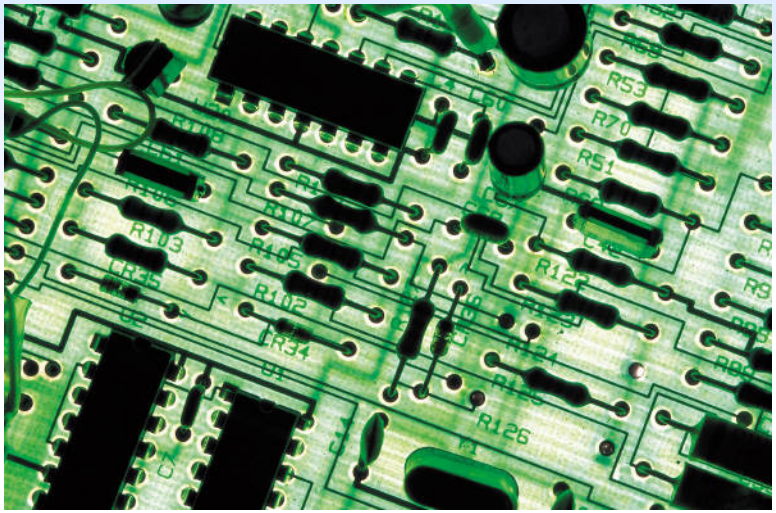
National Petascale Computing Facility (NPCF)

- NCSA's computing, networking, and data systems.
- BlueWaters Supercomputer
  - 1 quadrillion calculations per second sustained
  - More than 13 times faster than that at peak speed
  - Balanced processing speed, data storage and communications
    - 22,640 Cray XE6 nodes
    - 4,228 Cray XK7 nodes with NVIDIA graphics processor acceleration.
    - XE6 nodes have 64 GB of memory per node
    - XK7s have 32 GB of memory
    - 26 petabytes of online storage
    - 380 petabytes of nearline tape storage
  - https://bluewaters.ncsa.illinois.edu/hardware-summary

Open Scientific Computing Environment

- NCSA's network domain lives outside of the University of Illinois in what could be called a predecessor to today's Science DMZ networks.
- It is optimized for performance and open access.
- Hosts many systems and services
  - BlueWaters
  - iForge which is a supercomputer dedicated to industrial use
  - Many federal and state funded systems and services
- Serving the University of Illinois, State of Illinois, Industry and the Nation's academic research community.

NCSA Environment



- Network
  - Class B across 5 security zones
  - 160GB → 450GB WAN
- Systems
  - Big: HPCs & Archive
  - Medium: VM farms, OpenStack, and Oracle clusters for Nat'l science projects
  - Small: Long tail of smaller research projects & desktops
- Identity & Access Management
  - SecurID, Kerberos, LDAP, OAuth/MyProxy, Training accounts
- Security Group
  - Hybrid R&D/Operations team
  - 24/7 Operations responsibility

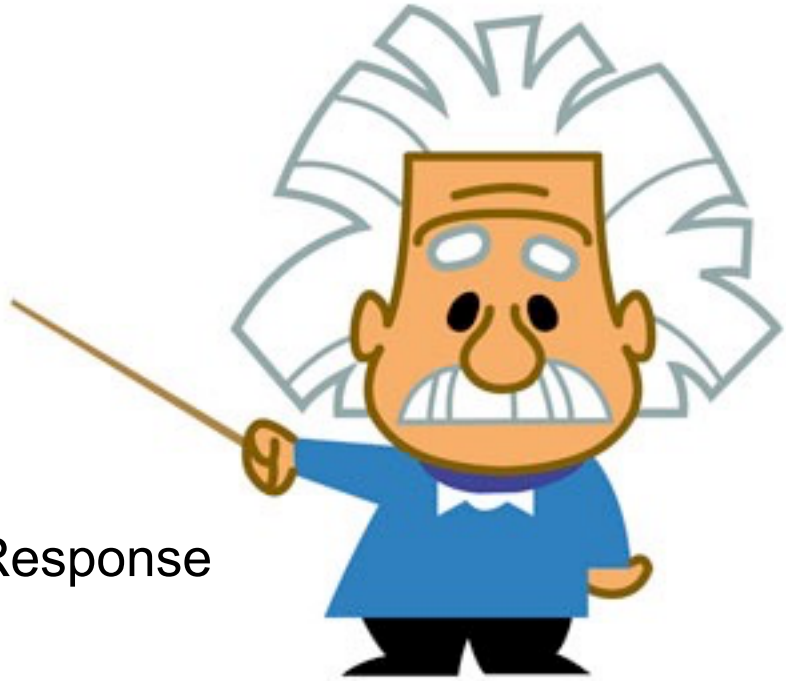
NCSA Cyber Security Directorate (CSD)

- Protect NCSA Digital Assets by applying and operating advanced cyber security solutions.
  - Risk-Based Approach
  - Integrating state-of-the art solutions

- Filling in the Gaps
  - Design, develop, and apply trusted cyber-infrastructure in support of science, & engineering
  - Driven by community engagements.

- Partnering operations together with research and development efforts.

CSD Expertise



- Established Areas of Expertise
  - Identity Management
    - MyProxy & CILogon
  - Security Prevention, Detection, & Response
    - Black Hole Router System
    - Bro Intrusion Detection
  - HPC Operational Cyber Security
  - Cyber Security Risk Analysis
- Developing Areas of Expertise
  - Cyber Security Intelligence Analysis
  - Intermix of Open and Controlled Environments
    - HIPPA, FERPA, ITAR

Operational Cyber Security

5 Pillars

- Incident Response (24/7)
- Preventative Security
- Security Monitoring
- Security Awareness
- Security Collaboration

Activities

- Staff Training & Education
- Security Policy & Process Development
- Network Security Monitoring
- Active Response & Blocking of Attacks
- 24/7 Incident Response
- Security Hardening Guidelines
- Syslog Collection & Monitoring
- Developing Secure System Architectures
- Forensic Postmortems
- Custom Instrumented SSH monitoring
- Secure Bastion or Jump Hosts
- OAuth Portal and MyProxy CA service
- Vulnerability Scanning & Prioritization
- Security Vetting & Hardening
- Firewall Management
- Brute-force Mitigation
- Risk Assessments
- Security Auditing

Threat Sources & Targets

- Threats
  - Ankle-biters – inexperienced script kiddies
  - Cybercriminals – interested in profit
  - Traditional crackers – someone with a cause
  - Mistakes/Accidents – operator error
  - APTs – State sponsored espionage and terrorism
- Targets
  - Un-targeted - harvesting bots/accounts
  - Resource Theft, Bitcoin Mining
  - Reflection Attacks/DDOS
  - Vandalism
  - Reputation based attacks
  - Data Exfiltration/Espionage

Security Architecture

- Risk-based Approach
- Network zones (define trust levels/internal monitoring)
- Bastion/jump Hosts (2fa)
- Centralized log collection
- One-way admin access
- Passive Monitoring
  - Network
  - System Logs
  - Keystrokes (optional)
- Active response/blocking
- Vetting and Hardening procedures
- Vulnerability scanning

Monitoring Log & Network Data, and Analysis

- Our open environment relies heavily upon monitoring
- Bro and syslog logs collected
  - Splunk and OSSEC
- Interactive SSH sessions logged by instrumenting sshd
  - Gives greater visibility, don't have to rely on shell history
  - Active research to monitor and analyze this data
- Other logs for incident response including:
  - Netflows
  - Keystroke command logs on BW

Active response mechanisms

- Black hole Routing used to block “bad actors”
- Bro triggers response to certain events:
  - Port scanning
  - SSH password guessing
  - Network scanning
  - Quick mitigation to many new threats
- Syslogs fed into OSSEC and rules can trigger a response:
  - Failed attempts to login
- Investigating Federated Intelligence Sharing via CIFv2

Evolution of Network Security Monitoring at NCSA

- Initially two network links: 1G and 10G
- Phase 2 went to 16 10GB links
  - Moved to a Bro Cluster approach with Gigamon link aggregation
- Phase 3 moving to 4 100GB links
  - Monitoring 100GB is challenging
  - Rely on specialized network hardware, but machines can't really do 100GB NICs
  - Need new approach:
    - Cut out network traffic that consumes large amounts of bandwidth won't interest us from a security perspective
    - Can SDN help us to route "known trusted" flows past monitoring?

Challenges and Opportunities

- Virtualizing Technologies such as OpenStack
  - How to manage with less control of the system
- Network Bandwidth Speeds
- Software Define X
  - Networking – mostly we see this as an opportunity
  - Security – the same

Follow-up Contact

Security Contact – security@ncsa.illinois.edu

Randy Butler – r-butler@illinois.edu

CSD Website – http://security.ncsa.illinois.edu/


geni
Exploring Networks
of the Future