

# Fall 2017

## Fall 2017 NetGurus Meeting

Internet2 will provide NetGurus a room to be set in a closed Board style conference seating to support ~30 participants . The meeting will take place the Thursday after the Technology Exchange (October 15-18, 2017) conference concludes. We will have a projector and screen available if needed by participants.

### Summary

<b>Location</b>	San Francisco, CA
<b>Room</b>	Water Front A/B, <a href="#">Atrium Lobby Level</a>
<b>Date</b>	Oct. 19, 2017
<b>Time</b>	9:00am - 5:00pm

**NOTE:** Breakfast and lunch are on your own. A morning and afternoon break with snacks and beverages will be provided. We will go to dinner as a group the night before.

### Tentative Agenda

Time	Activity
Wed 6:00pm	Gurus and Guests Dinner
Thu Breakfast	On your own
Thu 9:00am	Gurus start
Thu 10:00-10:30am	Break and networking (Pacific Concourse Level shared with Advance CAMP group)
Thu Noon	Lunch on your own
Thu 2:30-3:00pm	Break and networking (outside the Water Front Rooms shared with other groups)
Thu 5:00pm	Festivities end, must clear out promptly.

\*\*\*Note that the dinner is on Wednesday night, instead of after the meeting Thursday.

### Attendance

\*\*\*Registration is currently closed as of 9/19/17. Please email Dan or Cas if you would like to be put on the cancellation list.

Contact Dan Brisson (dbrisson@uvm.edu) or Cas D'Angelo (cas.dangelo@oit.gatech.edu) to RSVP and for topics you wish to discuss during the meeting. Attendance limit is 30ish.

#	Name	Email
1	Dan Brisson	dbrisson@uvm.edu
2	Cas D'Angelo	cas.dangelo@oit.gatech.edu
3	Andrew Gallo	agallo@gwu.edu
4	Michael Van Norman	mvn@ucla.edu
5	Danny Shue	dyshue@unc.edu
6	Will Whitaker	will.whitaker@unc.edu
7	Adair Thaxton	sthaxton@email.unc.edu
8	Jose Santiago	jdsantiago@triton.uog.edu
9	Randy Dahilig	randyfd@triton.uog.edu
10	Chris Cook	chris.cook@nyu.edu
11	Georgi Stoyanov	georgi@lsu.edu
12	Kevin Mayeshiro	kmayeshiro@ucdavis.edu

13	Frank Seesink	frank@wvnet.edu
14	John Kristoff	jtk@depaul.edu
15	Matthew Teshima	mteshima@hawaii.edu
16	Alan Whinery	whinery@hawaii.edu
17	Tony Brock	anthony.brock@oregonstate.edu
18	Drew Lake	drew.lake@depaul.edu
19	Scott Friedrich	scott@gatech.edu
20	Brian Flanagan	brian.flanagan@oit.gatech.edu
21	Robb Brantley	robb.brantley@oit.gatech.edu
22	Jason Wang	j.wang@its.utexas.edu
23	Bruce Curtis	bruce.curtis@ndsu.edu
24	Laurie Collinsworth	ljc1@cornell.edu
25	Richard Machida	ramachida@alaska.edu
26	Eric Cronise	eric.cronise@cornell.edu
27	Amy Liebowitz	amylieb@umich.edu
28	Sam Ziadeh	sziade1@lsu.edu
29	Mark Boolootian	booloo@ucsc.edu
30	Charles Rumford	charlesr@isc.upenn.edu
31	Dave Farmer	farmer@umn.edu
32	Colin Murphy	murphy@umn.edu
33	Rich Ingram	rni@umn.edu
34	Jim Warner	warner@ucsc.edu
35	Josh Sakofsky	josh@nyu.edu
36	Joe Marentette	jmarentette@wustl.edu

## Discussion Topics and Notes

Topics are submitted by participants. Please contact Dan Brisson (dbrisson@uvm.edu) or Cas D'Angelo (cas.dangelo@oit.gatech.edu) to add an item to the agenda.

- Next Generation I2 Infrastructure
  - Equipment
    - Risk tolerance with Vendor router vs. Whitebox
    - Confusion with Local peering vs. Gigapop model
    - Using a vendor platform helps campus engineers with management: "Internet2 is using Juniper"
    - Ratio of routers to Connectors – maybe Internet2 is trying to be at too many POPs
      - Maybe use packet optical to backhaul to routers
    - Whitebox: Separating software from hardware – helps with cost model
    - Complexity – centralized or distributed – pros and cons of both
    - Worth exploring whitebox by Internet2, might be early, but still worth it
  - End-to-end
    - Mission question: Does internet2 support big research AND network research...which is more important? Feelings that Big research is very important – balance?!?
    - Network researcher, ask him: would he be ok with a colleague at another researcher mucking with his traffic for an NSF grant
    - Factor in the cost of people when making decisions – people the most expensive
    - Stability of whitebox – who gets to program the pipeline (traffic flow)
    - Examining the processes that whitebox changed for Google/Facebook might be more important than the actual hardware
    - Looking at whitebox helps drive down cost from traditional vendors – I2 helps us all in that regard by leading the way
  - Flexible Edge
- How can I2 improve cloud connectivity
  - What does the community need
    - Even with direct cloud connect, need to make sure people understand latency still exists
    - Change the economics as much as possible, use bargaining power
    - Too late for some schools
    - Cloud providers moving to v6, we should be too

- SDN for real, not just as a plaything.
  - Intentionally provocative language for the title. Most of what I see in terms of SDN is point solutions (often around the Science DMZ) that seem more oriented towards solving the problem of not having SDN. That's fine at small scale, and it adds spice to the job, but is it really scalable? What does real SDN in a production, campus network look like? Probably not what has been done to date.
    - What is going to look like at campus scale
    - More on automation/orchestration than the "controller" model where every packet/flow is examined
    - What architectures/abstraction layers
    - Multivendor support is lacking
    - Building a network architecture that supports the needs of the software being deployed on campus (ex. Virtualization)
- Automation
  - Ansible and Salt
    - Starting with basic static config generation – helps get experience
    - Goal: don't login physically to boxes, make changes centrally
    - NLNOG Ring – [ring.nlnog.net](http://ring.nlnog.net)
    - Netguru git hub to share scripts? Slack channel?
    - Generate template and put on tftp server – Juniper Zero Touch Config
    - Automation – need to be concerned about process/procedure/people as much or more than technology
    - What is in control of the config: the database or the running config?
    - Build a database around the running-config – GR NOC does this
    - How do you handle exceptions
      - Key words in interface configs
    - Organizational idea: designate equipment where non-standard stuff can live
    - Any pushback from management using customized solutions
      - Document the heck out of the process and present that to management
    - Salt: agent-based config management
      - Persistent connection to "minions" means instant config changes
  - Docker, Docker Swarm, Kubernetes
    - Makes application deployment easier
    - Still pretty buggy, esp. when it comes to networking
    - Pluralsite web site has a great series on Docker, also at [Lynda.com](http://Lynda.com)
      - Pluralsite more technical than Lynda
- IPv6
  - State of IPv6 implementation on campuses across US - SLAAC vs DHCPv6
    - 2 votes for SLAAC
    - Issues with consumption of Privacy Addresses, hardware not supporting the number of clients
      - SLAAC with Stateless DHCP to give out DNS
    - Future is each client gets its own /64 with per-client RAs sending them unicast – cuts down on Neighbor table
    - Issues with Reverse DNS – ssh servers rejecting
      - Not an issue anymore
    - Even the smallest university should get a /40, but you can probably qualify for a /32 if you have residence halls
  - Device registration portal with IPv6 support - does such a thing exist?
    - No one is aware of a product
  - Challenges in tying IPv4 and IPv6 addresses to a user without .1x
    - Some clients do not send DUID
    - Farmer sending email re: RFC to address this
  - Experiences with NAT64 or some variant
    - Alan Whinery did a tutorial on this and will send out an email with a link to the video
    - Definitely viable at this point, although need to watch out for literals in code pointing to v4 addresses
    - Goal is to make clients work in a v4 world w/out any v4 services (routing, DNS)
- IPv4 - Buying more space vs. NAT?
  - NAT for clients with global v6 addresses
  - Can get a NAT64 allocation from ARIN if you can show that you're out of space from your initial allocation
  - Multiple folks re-IP'ing client networks to size properly
- Data Center Networking:
  - Virtualization of the networking
    - Cisco Fabricpath/OTV, Vxlan Fabric on the 9K series, Back-to-back VPC
  - NSX? Contrail? ACI?
  - EVPN? MPLS? VXLAN?
    - One migrating to EVPN with VXLAN
    - Stitch the fabrics together at spine level
  - Extending to the Cloud
    - One using Ptp VPN
    - Run VXLAN through IPSec tunnel into a virtual router in the cloud
- Wireless
  - 5ghz only SSID?
    - 5ghz only ssid, 24ghz only ssid
    - Still need 24ghz for legacy devices
    - Wireless toilet – crappy use of spectrum
    - Hospitality APs – maintenance ppl make sure students are not putting beds near the AP
    - Service Assurance
      - Vendors: Nyansa, Netbeez, Cape Networks, 7signal
      - Aruba/Cisco starting to coming out with similar tests
        - Issue with AP being a client that's not physically located where clients are
  - Freeradius
    - Network Radius (company)
      - Helped setup a couple servers with Freeradius 3 plus 1yr support for 15k
    - Onboarding (certificates):

- SecureW2
  - Clearpass
  - Cloudpath
  - Cisco ISE can't do MsCHAPv2 against LDAP
  - Web page that user can hit to report problems tied into wireless backend – gives real-time information on user statistics
- Guest wireless
  - Netflix says HD needs 5Mb/s
  - AT&T runs guest wireless for one campus
- On-campus speed test/self network diagnostic tool solution
  - Ookla speedtest on-campus
    - 1 server for free, \$2k/yr per node
  - Fast.com
  - Peering with local ISP who has an on-site speedtest server 1-2ms away
  - perfSONAR nodes out in campus
- On-campus CDN installs
  - Netflix, Google Global Cache (GGC), Facebook (FNA)
  - Attend NANOG meetings to make connections with CDNs
- Security topics
  - DNS RPZ feeds
    - OpenDNS, Akamai
      - OpenDNS just on Wireless/Guest Wireless
      - Support for IPv6?
      - Future attractive options for I2 coming soon
    - Rolled our own BIND
      - Manual entry by local InfoSec
    - SafeDNS with option to unfiltered DNS
  - Border/Edge Firewalls
    - Palo Alto Next Gen Firewalls
    - Insert firewalls between Border Router and Core Routers
  - IDS/IPS in-band/out-of-band
    - Out-of-band passive fiber taps, Ixia as a packet broker
    - Arista
    - Port mirror at trunk ports
      - Be careful not to overrun backplane
    - Nexus can port replicate just the header
    - Apcon
      - Cheaper than Gigamon – 1/3 to 1/2 price
      - More useable
      - Support really good
      - Generic optics
  - NAC & Client Posture Assessment
    - Network Quarantine
      - Redirected to a web page
      - Self remediate
- Inter-domain ASM Multicast
  - Kill ASM and move to SSM = MSDP killed
  - One campus monitored for 2 months and saw no outbound multicast, so they killed it – no problems reported
- Traffic flow and pcap monitoring tools
  - Internal netflow
    - Diagnosed a DNS problem
    - See what's going on over the last few months
  - SILK
  - BMP
- On-campus IPTV
  - XFINITY on-campus
  - Appogee
  - Philo Cornell
  - YoutubeTV allows 6 students share one subscription
- R&E Connectivity
  - \$75k/yr for a non-research school
  - Hard to justify the cost when compared to commodity Internet
- Cooperative grant funding projects and ideas
  - Work together to strengthen proposals

## Dinner Options

TBD



### **Thanks for the Support**

Many thanks to our sponsors who have made this meeting possible:

Marie Modrell  
Kelly Faro  
George Loftus  
Internet2