2015 Inter 6fe9d

2015 Internet2 Global Summit

2015 Internet2 Global Summit

- Tuesday
- 8:45 - 10am

• Science Gateways @ Mount Vernon B

- A science gateway is a community-developed set of tools, applications, and software
- Mostly instantiated as a web front-end (drupal, django, CMS, etc.) w/ a splash of grouper to back-end compute for sequencing, big data clusters, etc.
- Client → web interface and REST interface → workbench framework → XSEDE (for parallel) or Triton (for serial)
- People in US get access up to 50k core hours per year at no cost
- Galaxy science gateway
- Focus on reproducibility (many published analyses are not reproducible due to missing software, versions, parameters, etc.)
- A framework for building gateways
- Locking to dockerize SW versions to make reproducibility easier

• NSF Proposal Creation @ Mount Vernon A

- Downloaded presentation
- Tue 12-1

• Open NTAC Meeting @ Meeting Room 8/9

- IPv6 WG working on slides and metrics on IPv6 growth on Internet2
- Performance WG working docs for perfsonar, troubleshooting, measurement/network perf maturity model
- 3.6 will have more SDN support.
- Routing and Peering WG some transition of effort re: TR-CPS. Will focus on educating community to make use of TR-CPS, offer tutorials on BGP, etc.
- SDN no update, they're
- Security mtg tomorrow at noon. Creation of security WG will be proposed.
- Topics potentially to be addressed in the near future:

- Wireless
- Campus
- Should there be a social responsibility interest group?
- Around DC, multiple 100gb's now be deployed, particularly for AL2S in DC area
- OESS doesn't support 100gb lag, doing some shifting of VLAN's around to work around this
- Not a lot of visibility into traffic patterns from a service perspective, more focused on interface utilization, etc.
- Path to OpenFlow 1.3 being worked out note that I2's backbone is multi-vendor, so inter-operability is an issue
- QoS is big driver for OF 1.3
- Note: fair amount of skepticism around OF 1.3 adoption by hardware vendors
- That's okay. I2 can use multiple technologies, not just OF
- Tue 1:15

• Cloud Exploration & Implementation @ Grand Ballroom North
- Multi university effort to create a cloud cookbook, focused on
- Federation
- Case studies
- Policy and compliance
- User experience
- Tue 3pm

• Security Without Borders Meeting Room 12/13/14
- Downloaded presentation

•PerfSonar Mount Vernon A
- Been around for 11 years, very part time effort
- In last 2 years, ESNet, Internet2, Indiana U, and GEANT all started dedicating 1.5 FTE to develop and improve perfSonar
- 3.5 will be RC this summer and final release before Tech Exchange
- Should setup perfSonar node as part of RC 100gb
- perfSonar 3.5
- Better support for central host mgmt and node auto-config
- Support for low cost nodes

- Support for other OS choices (RhEL, Debian, VM install)
- Modernize the GUI
- psUI tool from GEANT will be another way to interact w/ perfSonar
- Central mgmt be able to add it to things like puppet, chef, saltstack, cfengine, etc. Sample puppet recipes will be part of 3.5
- New rpm bundles to support this
- Zero config
- Get a DHCP address, register w/ lookup service
- What hosts to run tests to
- Where to send test results
- BWCTL modernized and ported to python, lots of new features added, moved far past its original use case of just being a wrapper for iperf
- Low cost nodes
- Often ARM-based (beagle bone and raspberry pi)
- Can't hit 1gb yet
- Currently targeting around $200 a node, capable of achieving 1gb BWCTL, allows for Intel
- Best fit for HW
- Gigabyte brix
- Can hit up to 937mbps in testing
- Only draws 30w
- $225
- ECS Liva
- $120-$170
- 32-64gb eMMC, 2gb RAM
- 15w power, could be powered by PoE splitter
- Achieved 940mbps in testing
- Alan W on UH's low cost node deployment
- SWARM dense perfSonar deployment w/ lots of cheap devices ($50 per node)
- About 50 raspberry pi and beagle bone
- Issues seen
- 22 SD card failures
- 10 file system failures
- 1 corrupted firmware

- Class 10 cards are more reliable
- SanDisk Ultra 8gb class 10
- They liked beagle bone black a lot (sometimes scarce to buy)
- Will do raspberry pi if/when necessary
- Managing them via puppet
- Powstream is really amazing (but boring at first)
- / [Perfclub.org/](Perfclub.org) (perfsonar users group)

Wednesday

- 8:45am Internet2 Advanced Services Today, Mount Vernon A

• Network topology changes

- Added AL2S nodes
- Hartford, missoula, indianapolis, cincinatti
- Backbone upgrades
- Chi-ash 100gb
- Ash-mclean 100gb
- Optical network
- Hartford add/drop
- Atlanta metro (56 marietta)
- MANLAN and WIX
- Ana-200gb:
- 100gb Ny to London
- 100gb Mclean to Paris
- Layer3
- 10gb legacy port turndown
- 3rd 100ge between AL2S and IP in WASH
- Full mesh between chic, atla, wash, newy, clev
- TR-CPS
- Some re-work on west coast and upgrade in Dallas

• Service Updates

- ION Service Decommission on 4/1
- NDDI (precursor/test lab to AL2S) network consolidated into lab space

- TR-CPS capacity augments towards peers on west coast, Dallas (imminent!), NY
- General trend – more research traffic on Internet2 in the last year (driven by things like LHC)

- Global Update
  - Response to requests from membership for science and education
  - Atlantic connections
  - ESNet – over 300gb to Europe, across a few circuits
  - Several NREN's have connections as well
  - Nordunet has 100gb between Amsterdam and NY
  - Internet2 has a 100gb as well
  - Completion of a multi-connection ring that doesn't have any single points of aggregation
  - Middle East
  - Open exchange point being built in UAE (Pujarah)
  - Contracted a ckt between Pujarah and Singepore
  - Will connect Pujarah back to London or Amsterdam as well
  - Will likely grow to aggregate many NREN's over the next several years
  - Singapore
  - Colo (10 racks) facility. 6 used, 4 still open
  - Direct links between singapore and HK (several NREN's there)

- Network Security
  - New security role established about a year ago
  - Approach
  - Baseline security risk assessment
  - Develop security program
  - Initiatives
  - Updated security and incident response policies
  - Technical improvements to IDS, strong auth, and vuln mgmt
  - Review access to publically available ops documentation that is sensitive
  - Design and implement a secure OOB mgmt network
  - Build a SOC
  - Guide and improve routing security

- Network Operations

  - Working on ISO 20000 certification

  - 100% availability through investments in infra

  - Strategic NOC plan for 2020

  - Define netxt gen process automation and predictive analytics

  - Customer driven SLA's

- Network Architecture and Planning

  - Technology

  - Understand tech landscape to build new innovative services, maintain a balance

  - Engagement

  - Engage customers to understand needs, understand vendor capabilities

  - Development

  - Pursue innnovative R&D

  - Expand scope of internet's architecture planning to embrace community needs

- Innovation Initiatives

  - Internet2 Service Taxonomy

  - AL1S (fiber and and optical transport)

  - NVS virtualized ethernet switching

  - General purpose VLAN Services – AL2S (SDN Controller)

  - Layer 3 services

  - Net +

  - Virtualized Services

  - OESS

  - ONOS

  - GENI Site Mgr

  - Duke's SDN Journey Mount Vernon A

- What is SDN?

  - Control functions decoupled from packet forwarding and switch

  - Controller can view network as a whole

  - Open standards based SW for forwarding decisions (like Openflow)

- Why SDN?

- Firewall and IPS = speed bumps

- Leverage SDN for automated configuration

- Self-service configurable research bypass of core network

- Researcher access to national backbones

• SDN at Duke

- Implementation of openflow

- Focused on the edge of the network not datacenter

- Goal: improve the speed, reliability, and performance of network used by researchers

• Current posture

- Sdn switches deployed in hub and spoke

- Switchboard dynamic SDN rule manager

- SDN controller (modified Ryu REST router)

- perfSonar nodes deployed across campus

- Efforts led to redesign of Duke core network

- Used an MPLS core and can switch to a VRF easily, so routing is every where

• Preparing for SDN

- Organizational

- infra and oper readiness,

- Staffing nework, devops, security

- Culture programmers and systems guys loose on the network

- Dedicated VRF for SDN control plane

• Infrastructure considerations

- Dedicated science network?

- Didn't like this option

- Converged/unified network?

- Fiber infra?

- Needs at the core?

- Needs at the edge?

• General SDN model at duke

- Integrated hosts connected to the network

- Hybrid network fabric has multiple options for routing
- Did not want to build/deploy a separate infra
- Hosts connected to SDN switches at 10gb
- Default path for traffic is production network
- Application applies rules to controller to route certain traffic over alternative path
- Typically subnet to subnet or host to host
- VLAN tagging supporting
- Plan to add functionality (port restrictions, VLAN flipping)

• SDN core network bypass

• Planning for SDN lessons

- perfSonar is your friend!
- 10gb cannons aimed at your network!
- Measure latency and bandwidth on a regular schedule
- Distribute nodes at multiple locations
- New version of ps can allow you to split across different interfaces
- Use ps to prove the network can handle the traffic you expect, BW measurements are useful
- Use puppet to manage ps
- Oversubscription
- Accidental or intentional
- Span ports, layer 2/3 domains
- Firewalls
- What are the real limits per stream / overall?
- How do they fall over / fail?
- IPS moved to edge, only IDS and taps in core

• IPS

- Where is traffic inspected

• It's another network upgrade!

• User-controlled SDN config

- Once plumbing was in place
- How did they provide users w/ access?

- Switchboard
  - Ruby on rails to simplify SDN config and track changes
  - Who is authorized?
  - Status of requests
  - Update SDN controller based on approved configs
  - Rollback/restore SDN controller state
  - Audit log of state of configs

- Deployment strategy
  - Start with intermittent BW intensive tasks
  - Backups
  - Bulk data moves
  - Data ingestion into protected enwtork segment
  - Run building edge switches in hybrid mode
  - Enable openflow ports where needed

- Next steps for RYU
  - Limit dhcp responses to authoritative dhcp servers
  - Vlan tags flipping to support linking VLAN's
  - Detect and throttle ARP flooding (and other potential DoS attacks on SDN controller)

- Lessons
  - Easy to simulate an SDN network
  - Ryu-rest router + mininet + open vswitch
  - Open vswitch is very capable
  - Openflow port you mot care about is disabled
  - Bad connections
  - How polished is your glass
  - Hybrid mode switches in wrong mode

- Endgame
  - Campus SDX (software defined exchange)
  - Campus core bypass links for science DMZ
  - Interconnects layer 2 services (AL2S, BEN, etc)
  - Start with a self-service app (switchboard)

- Then enable devops style automation and actions_approvals_audits via switchboard API

- Use cases
  - Science DMZ
  - AI2s path
  - Bypass packet inspection
  - Expand BW/capacity
  - Data migration (to protect network segment)
  - Support Duke/Duke Medicine researchers

- Work in progress
  - Mixed support for openflow
  - Netflow not necessarily built in

- Staffing_Skills_Culture
  - It was easier to teach a programmer to learn networking to run w/ SDN than it was to get a network engineer to learn enough programming/scripting to drive this
  - Get network engineers more involved in python scripting, curl etc

#learning/conferences