9/13/17 Meeting Notes
Blue Jeans Meeting ID: 720160650

Attendees: Celeste Anderson, Dee Childs, James Deaton, William Deigaard, Harvey Newman
Staff: Rob Vietzke, Linda Roos, Kathleen Kay, George Loftus, John Moore, Paul Howell
Guests: Ana Hunsinger, Dale Finkelson
Not Attending: Roy Campbell, Wendy Huntoon, Michele Norin, Jim Stewart, Marc Wallman, Rod Wilson

William Deigaard welcomed the group to the September meeting of the NAOPpag and introduced the first strategic topic to be addressed.

Strategic topics:

-**International Peering Working Practice** (Dale Finkelson, Rob Vietzke)
(document: 170905 Draft International Peering Working Practice- can be viewed following these notes)
Dale Finkelson thanked the group for inviting him to speak and indicated that the draft document sent out in advance of this meeting clarifies what Internet2's R & E peering and transit policies say in the effort to bring the information up to date.
For example:

- Internet2 prefers to deal with larger organizations, rather than individual sites (however, there are cases when Internet2 is willing to peer with an individual site)
- The document clarifies routes we will provide to international peers and what TR-CPS we will or will not provide (this may not have been sufficiently clear in the past.)

Celeste pointed out that many large organizations & NRENS provide back up to other organizations causing a loop. She suggested, and Dale agreed, that a clause needs to be added to the policy addressing this. William and Celeste remarked that having the information in one concise location was helpful, particularly the transit information. Harvey asked about conditions under which peering would not be accepted and Dale indicated the policy is largely non-restrictive. Jim Deaton questioned the relevance of the advertisement matrix in the document. Rob agreed that this was something not yet well-defined and in need of clarification. He suggested that this be pared down to what we say "yes" to and that another document be prepared for the NOC, and a third document be created to address federal policy. It was further decided to call this a "practice" rather than a "policy" because policies require Board action. The draft is to be updated with suggested changes made, today's date applied, and it is to be posted on the Internet2 website.

-**Internet2 Community Proof of Concept projects** (John Moore, Rob Vietzke)
(documents: Community POC Planning NAOP; draft - Core Technology Evaluation POC – can be viewed following these notes)
John Moore provided an update on efforts to date in the development of the Proof of Concept projects currently being discussed. He referenced calls and meetings that have occurred in the community, including the Newport meeting with the Regional Principals and the call with the CIOs. The Core Technology Evaluation POC is the most fully formed at this point and John described where it stands:

- Looking at ADVA box as possible implementation of an end-to-end disaggregation platform with the potential to drive down cost per bit pricing.
- NYSERNET to host lab test in Syracuse
    i. 4 other organizations – UCAR, Oregon State, MAX, Kinber want to join testing

- Use cases will be developed to support the end-to-end platform
- John talked about the community that is forming around Facebook Voyager box. He feels there is value to Internet2 being present and giving use cases as it applies to R&E. Rob indicated that it is by no means the final solution but the need exists to create sufficient structure around the project to enable a functional conversation with the community.
- Other vendors have approached us on doing the same thing with them.

The 2nd (Flex Edge POC) and 3rd (Collaborative Service Delivery Project POC) POCs are not as fully fleshed out as the first, requiring more conversation with the community. MAX has expressed interest in collaborating in the Flex Edge Project. The Collaborative Service Delivery Project will probably take form as discussion proceeds on the other two projects. Rob indicated that developing these POCs is an attempt to figure out the arc where Internet2 needs to define itself and define the community's needs.

-**Approach to Attack Detection and Mitigation** (Paul Howell)
(document: Approach to attack detection and mitigation- can be viewed following these notes)
In advance of this meeting Paul Howell asked that the NAOP members read two blogs:
https://www.internet2.edu/blogs/detail/12234
https://www.internet2.edu/news/detail/13507/
He also sent out slides to create awareness about the current security climate and offered to engage with anyone to answer questions at any time. William commented on the layers of complexity involved in national threats, saying that many campuses haven't had the opportunity to adequately protect themselves. Paul noted that because the attackers morph and change strategy frequently, there is a need for several tools to draw upon. In addition to Ren-ISAC and the global NREN security group, Internet2 participates in governmental and industry-run services that try to anticipate what's going on. Harvey asked if Internet2 plans to join a security organization that engages in strategic actions to localize what's happening, and James suggested it would be beneficial to have Internet2 get into the weeds with the members, saying it would be good to see everyone working together to solve these issues.

NAOPpag standing agenda items:

Rob reported that Howard has mostly completed his initial listening tour with members, partners and staff. He seems to have understood our community well, and may share his impressions on what he's learned and his future approach as early as at TechX.

Network Services is currently meeting to look to future infrastructure strategy, find greater balance toward research needs, cloud strategy for end users, future network needs, sustainability of TIER & trust & identity services.

Papers being developed on the POC models will be sent out to this group.

Other topics:

With no other topics raised, the meeting was adjourned at 3pm ET.
Next meeting: October 11, 2017, 2-3pm ET via BlueJeans connection

Internet2 International Peering & Transit Policies

PEERING

I. IP Peering Policy for International Access to Internet2 Research & Education Network

Internet2 will make an effort to peer with any national research and education network (NREN) making a request to peer where the goal is to exchange traffic with users of the Internet2 network and when establishing the peering is technically feasible. Typically, this means that if a NREN presents itself for peering at an international exchange point where Internet2 is located with a research and education peer that also includes research and education routes, Internet2 will work to establish a BGP session with them and will share Internet2's R&E routes with them.

Peering with Internet2 R&E Network provides access to Research and Education participants of the network, including Internet2 member campuses, and other educational, research and related institutions, including state government, K12 schools and public libraries. Access to specific US Government Federal Networks that connect to Internet2 can be provided when Internet2 is authorized by the Federal Network to share routes with a particular peer.

Internet2 encourages the development of pan-continental networks for the interconnection of groups of NRENs throughout the world and will interconnect with pan-continental networks following the same guidelines as interconnections for individual NRENs. In general, Internet2 will encourage use of pan-continental networks over direct connections, however Internet2 will also not deny direct connections when they are technically and administratively reasonable.

Internet2 requires that peering NRENs have a 7x24 network operations center and a security operations contact, and that they regularly participate in regional or global forums for R&E network operators. Internet2 strongly encourages peers to adhere to the Global Network Architecture standards, including performance, operations and service capability standards.

Internet2 Prefix Advertisement Matrix

US Internet2 R&E Network Participants		International Peers
Federal Peer Network		When authorized by Federal Network
Sponsored Participant (K20/USUCAN)		YES
Sponsored Ed Group Participant K20/US-UCAN		YES
Member University Network Participant		YES
Commercial Participant (Industry Member)		YES
Connector Only (State or regional network backbone)		NO
Internet2 Net+ Service Provider		NO

II. IP Peering Policy for International Access to Internet2 Commercial Peering Service

Internet2 will offer access to its Layer-3 Commercial Peering Service at Internet2 points of presence and Internet2-connected international exchange points on a paid basis through a Master Services Agreement (MSA) and Service Schedule. Internet2 requires that peering NRENs have a 7x24 network operations center and a security operations contact and that they regularly participate in regional or global forum for R&E network operators. Internet2 strongly encourages peers to adhere to the Global Network Architecture standards, including performance, operations and service capability standards.

Routes available in the peering service include high-value peers including providers like Google, Facebook, Apple, and many domestic US and international internet service providers. As of July 2017, the routing table includes almost 300,000 IPv4 and IPv6 prefixes.

III. Interconnection Policy for International Access to US-Based Commercial Cloud Providers at Layer 2 or 3

Internet2 will offer dedicated Layer 2 or Layer 3 access to commercial cloud services that are available on the Internet2 network via Internet2 points of presence and Internet2-connected international exchange points on a paid basis with appropriate contractual agreements. Typically, a requesting NREN would need to establish its own contractual arrangements with the cloud provider for access to the services and then would work with Internet2 to establish VLANs, ports or virtual routing tables to interconnect the international NREN to the cloud service provider.

International Transit
(traffic between NRENs across the Internet2 Backbone)

IP Transit Policy for Research and Education Network traffic

Internet2 will offer settlement-free (no-cost) International transit between Internet2-connected International exchange points on a best-effort basis using the Internet2 backbone for Research and Education traffic. Transit will be for use by international NRENs to reach other NRENs across the Internet2 backbone. This service, described in the Commons White Paper of the GNA, is offered in reciprocity for other NRENs contributing capacity from their infrastructures to Internet2 that can be used by Internet2 members collaborating with those NREN participants and to encourage resiliency and reliability of the global NREN fabric. Internet2 may also offer upon request point to point Layer 2 connections between international connection points on its network.

Internet2 will monitor and measure transit traffic to ensure that the transit traffic stays at levels less than 30% of Internet2's overall national traffic on any link. If international transit exceeds that level, Internet2 may work to identify top international transit users and may seek contributions or revaluation of the settlement-free peering.

For long term or persistent usage, including support of standing science programs and other production workflows, Internet2 requires collaboration with the project or organization to track and forecast capacity utilization and potentially to consider reasonable support for the ongoing use of the Internet2 network. Internet2 reserves the right to deprioritize or deny long-term transit traffic from organizations or projects that have not made arrangements for ongoing support. Internet2 also reserves the right to deny high capacity transit flows when Internet2 has not been notified these flows would be occurring. Evaluation of long-term transit traffic will include a degree of judgment about the value to Internet2 members and how the particular transit use case contributes (or does not contribute) to the mission of Internet2 and its members. Example questions asked in evaluating transit traffic include questions like: "Does the traffic from this project or organization transit the Internet2 backbone routinely?", "Does the traffic materially affect Internet2's headroom for its own members or create a need for augmentation on the Internet2 backbone?", "Does the traffic cause congestion resulting in dropped packets on the Internet2 backbone?" "Is the project or organization's transit on Internet2 offering a reciprocal benefit to Internet2's members"?

APPENDIX A - Typical Internet2 International Peering Agreement Preamble

Goal of the Peering Relationship: Peering is viewed as a partnership between equal partners. Its goal is to facilitate the advance of science, networking and cooperation between our organizations and the user communities we service. Science is increasingly a global endeavor and its success depends in no small measure on the ability of individual scientists to communicate, exchange data and interact, regardless of distance and borders. In order to accomplish this goal, we agree to peer as explained above and within the strictures of our individual Appropriate Use Policies enable traffic to flow between our connected members. It is also agreed that we will, upon request and with all parties consenting, transit traffic between peers.

Understanding that these are complex networks, we also agree to have the respective network operators – the Internet2 Network Operations Center (NOC), and the operator of "the partner network" cooperate in their use of policy-based routing and router configuration technology and to assist in diagnosing and solving connectivity and security issues should they arise. Internet2 hopes the cooperation with its peers, both national and international, would extend beyond sending and receiving traffic. Activities like participating in international forums, conferences and engaging in individual discussions are important to developing a successful relationship.

Core Technology Evaluation Proof of Concept (PoC) - draft September 6, 2017

Objectives

Primary Objective: Develop a recommendation for one or more packet optical platform solutions that the community (backbone, regionals, and/or campuses) might utilize to satisfy projected bandwidth requirements at a radically lower cost per bit in the next 2-5 years.

Secondary Objectives: a) Explore and understand the development of open network equipment and opportunities for production or research/educational engagement in the open source network community. b) Assuming the initial evaluation is favorable (that the equipment works), engage faculty at community institutions to determine their interest in participating in a broader test of the platforms.

Description

As the community looks forward to a next generation national network and several regional networks are exploring new architecture options, a group including Internet2 and NYSERNet seeks partners primarily from the connector and campus community who are willing to commit resources to an evaluation of emerging low-cost optical network technologies. Ideal partners/participants will have a research, education, or production interest in new/next generation optical network transport, have background in optical networking and be prepared to commit time (and possibly fiscal resources) to an evaluation effort and report back to the community.

Planning will include timelines, a clear set of goals, distribution of effort and expected outcomes/deliverables. Beginning with the team’s current understanding of the landscape, the project will focus initially on the efforts by the Telecom Infra Project (TIP) to develop the open transponder platform called Voyager. Commercially built and supported products based on Voyager are available from ADVA - Voyager-based products from other companies that appear on the market should be considered as part of the evolving plan. In addition, other vendors that

provide comparable platforms may be considered, as appropriate.

Phase 1: Baseline Testing and Selection

Due to a desire to move the process forward quickly, NYSERNet plans to acquire Voyager boxes on loan from ADVA and execute basic functionality tests in a lab setting, with support from Internet2. The result of this effort will be a report for the community on the stability, manageability, performance and operational readiness of the platform. The intent of this “sniff test” is to provide input to the next step - devising one or more field trials to evaluate how it performs in situ. Once the hardware arrival dates are confirmed, NYSERNet will plan a ‘lab week’ in Syracuse, NY where anyone interested in coming for the initial setup and testing is welcome to join.

In parallel with the lab test, volunteers from the team will survey the industry to see if there are comparable open platforms or vendor development efforts that hold the promise to meet the objectives of the PoC. Promising products will then be considered for a full evaluation cycle.

Results from the initial evaluation(s) and the landscape survey will culminate in a choice of one or more platforms for a more extensive field evaluation.

If the Voyager platform is deemed stable and interesting enough to proceed, team resources will be assigned to follow and participate in appropriate TIP working groups to both contribute (case studies, test results, etc.) to the TIP effort and leverage the information and facilities available to active members.

Phase 2: Field Testing

Once one or more platforms are chosen from the baseline testing, a plan will be developed for a field test. The aim is to develop an understanding of how the platform performs in a real environment over time. A phased plan will be developed that should include testing and evaluation of bringup and integration, management, performance, stability over time, software upgrading and monitoring. Over time, the responsiveness of the vendor to bug reports, feature requests, etc should also be considered.

The scope of the initial testing will need to be considered, as some of the likely platforms will be primarily packet optical boxes, but may be able to provide some higher level services and features that would be valuable to test. Those features may be provided by a separate software vendor, so consideration should be included in the testing to consider the impact of dealing with multiple vendors.

During the field test phase, the products under test will likely need to be purchased in order that the evaluation can proceed over several months and through multiple phases, culminating in using the system to deliver real traffic, if appropriate.

The deployment should spread over a wide enough area to include the footprint of multiple regionals, multiple campuses and Internet2. The configuration should be built with practical considerations in mind. One such consideration might be to develop the topology along a busy route, where it might serve to supplement production traffic when deemed ready.

Those interested in participating (or who may have a faculty researcher or research group interested in participating) in Phase 2 testing should contact John Moore at Internet2 (jmoore@internet2.edu).

Roadmap Issues

One key outcome of this effort should be to develop a projection of the future development of the platforms under test. This somewhat subjective evaluation should be based on the experience gained by using the platform and working with the vendor(s).

Reporting

Though the timeline will depend on the availability of the hardware, we plan to provide a report from Phase 1 within 60 days of hardware arrival. Planning for Phase 2 will include specific formal reports to be delivered, and appropriate opportunities to update the broader community on progress.

Community PoC Planning

NAOP

September 13, 2017

Status of PoC efforts

Core Technology PoC

- NYSERNet playing a lead role - draft description provided

Flexible Edge Technology PoC

- MAX has volunteered to play a lead role
- Discussion planned in DC Sept 20 to organize effort and community outreach

Collaborative Service Delivery PoC

- Still in discussion phase internally

Approach to Network Attack Detection & Mitigation

September 2017

Network Services, Internet2

Detection

- Network flow data
  - Deepfield Defender – commercial product for (D)DoS attack detection
  - Open source tools
- Full packet capture
  - Use of Bro or similar packages in carefully selected environment (e.g., secure management network)
- Syslog data
  - Splunk alerts/reports on syslog from network devices (e.g., authentication failures)
- Firewall filter counters
  - Patterns of abuse identified from counters of executed firewall filters

Detection Continued

- BGP monitoring
  - Open source packages to identify route hijacks or similar malicious activity
- Unauthorized access of PoPs
  - Door scan logs from PoP providers matched with authorized staff access
- Social media and web posts
  - Claims of attacks
  - Threats to reputation
  - Environmental scan of open source media sources
- Threat intelligence
  - Dept of Homeland Security security threat sharing
  - Cisco Aegis threat sharing
  - REN-ISAC (i.e., Reports from members plus dailywatch report)
  - FBI Infragard threat sharing
  - Industry reports
- External notification

Mitigation

- Application layer (i.e., layer 7) DDoS
  - Net+ (e.g., Cloudflare)
- Volumetric network DDoS - Available to both Internet2 and members
  - Real time black holing (i.e., destination filtering)
  - Flowspec (i.e., source filtering)
  - Commercial scrubbing (i.e., Zenedge)
- Case by case incident response for non-DDoS attacks