

26 August 2004, HPR TAC meeting notes

1. Bash the Agenda (add one item - Brian Court RANCID protection)

2. Roll-Call/Introductions

3. Status Reports/Updates

a. Chief Executive/Operations Officer report (Dolgonas)

funding for CDP is shifting from K-12/Prop 98 to the individual County Departments of Education. proposals from the County DOE's are due on Monday, August 30. funding for the CDP is available through the current fiscal year.

the California Teleconnect funds have been cut from the state budget. an amendment passed in the California State Assembly and Senate to reinstate the Teleconnect fund. in the future, a surcharge will appear on monthly phone bills to pay for the Teleconnect fund.

the CENIC board is searching for another entity to take ownership of the *Gigabit or Bust* initiative. the board's desire is to provide no more funding for the initiative beyond FY04-05. the shift in priorities is driven by CENIC's increasing direct involvement in engineering, building and operating national and international high speed networks.

CENIC expects an announcement funding WHREN. WHREN is a network proposal to provide dark fiber between the North and South American continents. CENIC is also working to install a dark fiber solution to CUDI in Mexico.

the Coachella Valley network project is in a lull as additional solutions are explored. this presents a challenge for the College of the Desert. they were expecting a set of DS3 circuits by the start of the new school year. College of the Desert is operating on T1 service.

the CENIC board has a retreat scheduled to plan the funding of future projects. the board requests the HPR TAC to determine when we think the GSRs need to be replaced. we are being asked to consider if the GSRs are: outdated technology, obsolete or end-of-lifed by Cisco. the board would like to include the replacement of the GSR in their funding plans if necessary.

August marks the one-year anniversary of Chris Taylor chairing the DC-TAC. Mick Holsclaw (holsclm@losrios.edu) will chair the DC-TAC this year. Johanna Madjedi (jmadjedi@calpoly.edu) will be the vice-chair.

b. Chief Technology Officer report (Dave Reese)

Dave Reese announced personnel changes of CENIC staff. CENIC sites should not notice any change in the way they interact with CENIC. Brian Court is now the Director of Network Engineering and will focus on long-term engineering projects that CENIC is leading. Cindy Abercrombie is now the CENIC NOC Manager. Sherilyn Evans is the Director of Operations. Heather Sherman has joined the core engineers and is leading the CENIC documentation effort.

CENIC continues to schedule maintenance events to alleviate the troubles caused by the continuing 15808 optical issues. as reported earlier, 15808 modules intermittently un-equip themselves without warning. cisco has not determined the cause(s) of these continuing troubles. this condition does not appear in the 155XX series of equipment. cisco says that the design of the 15808 will not allow the addition of diagnostic code that might help determine the cause. cisco committed to send spares to each 15808 site, but CENIC has held up that offer. sometimes reseating a card alleviates the trouble. Dave said a module CENIC determined to be a hard fail from the Soledad site was sent to cisco. cisco has not been able to duplicate the module failure. there are two other cisco customers that have 15808s. at least one is experiencing the same trouble CENIC is. from an operational standpoint, module swaps are fairly expensive. Dave estimates it costs CENIC about \$400.00 per failure to make a site visit. the cisco TAC actually asks CENIC engineers to travel long distances to remote sites and report back to them about which LEDs are illumined, before cisco will send spares. due to the on-going trouble, CENIC insists that spares be sent before anyone makes a site visit.

NLR continues to be built. CENIC is working on provisioning bandwidth for the Super Computer O4 Conference. during the HPR TAC meeting, Dave sent out a powerpoint slide outlining the preliminary wave structure for SC04. Dave made a mention of "Western Lights". aim your browser at the following link to obtain lots of information:

<http://www.scd.ucar.edu/nets/presentations/nsf.briefing/NSF.briefing.PO.pdf>

Dave briefly discussed a fiber project being driven by the BIRN initiative (<http://nbirn.net/>). a proposal for fiber between Sacramento and California somehow falls into the fold.

Dave asked to have three new working groups formed to help CENIC with network planning. the paragraphs below come from an e-mail distributed on the TCT list:

1. Optical Backbone Committee
2. HPR Architecture Committee
3. DC Architecture Committee

We have a number of projects that come across our desks from time to time, some more likely to happen than others. Many of these, if they happen, would impact one or more of the backbones and I think it would be useful if we had a standing committee that could review the projects and designs. These committees could then report back to the TACs as the projects moved from the proposal stage into real potential projects.

The committees could draw in additional resources (i.e. reps from impacted sites, etc.) as needed for the projects. Examples: The recent SoCal redesign project for Coachella valley, and a few other currently active proposal projects (but still in the draft stages) such as Monterey Bay Aquarium Research Institute (MBARI).

c. Director of Engineering (Brian Court)

a number of regional and international networks have expressed interest in connecting to LALALAN, with a wave to the Seattle gigapop. Brian showed a slide presentation during the meeting.

Brian filled the group in on the continuing efforts of the BAM (Bay Area Metro) retrofit team. a number of announcements have been made outlining the on-going

changes and interruptions of service to the various lists. Brian thanked the volunteers outside of CENIC (Ken Lindahl and Michael Sinatra of UC Berkeley) for helping with this project.

EGM failures continue, but there is light at the end of the tunnel. the "loss of signal" trouble from the Northern Telecomm mux is attributed to a firmware bug. Brian expects the bug to be fixed by the end of October. Brian reports that SBC has improved their response to EGM service trouble tickets, but SBC isn't quite where CENIC would like them to be.

an on-going problem with the UC Berkeley EGM circuit was discussed. CENIC will ask SBC for specifics regarding the status of the circuit.

d. DC-TAC report (Chris Taylor - CSU Monterey Bay)

Chris thanked the HPR-TAC for the opportunity to represent the DC-TAC at the regularly scheduled HPR-TAC meetings. the next DC-TAC meeting is supposed to be in early October.

e. Network Operations Center (no representation)

according to my notes, the NOC was not represented at the HPR-TAC meeting. Brian having just moved to the Bay Area was unable to fill in.

f. CalVIP oversight committee (Michael Van Norman - UCLA)

a schedule of the CalVIP events has been placed at:

<http://www.cenic.net/calvip/CVSSched/index.html>

g. Backbone redesign/Coachella Valley project (Dave Reese)

CENIC is working on the DS3 circuit for College of the Desert. they are still using a pair of T1s. the Coachella Valley project is supposed to provision the new DS3 service. The Berger Foundation folks have been "studying" the viability of the project. as a consequence, the College of the Desert did not get their DS3 service by the start of their school year.

h. MPLS and RSVP forwarding (Tom Hutton - SDSC)

Tom along with other folks have been busy putting together the MPLS path to North Carolina. they were preparing to test the path when suddenly the I-TECH testing center in North Carolina was struck by lightning. the test (as of the TAC meeting) has been rescheduled.

i. Conference Program Committee (Phil Reese)

Bill Reese introduced himself, but the note taker failed to collect contact information. Bill asked us to think about what we would like to see at the CENIC 2005 conference.

4. HPR infrastructure for campus 10GE connectivity (Court)

The routing infrastructure for HPR is out of real estate. CENIC needs more chassis space to provide all HPR sites 10GE connections to the backbone. How does CENIC spread the financial pain to members without punishing the early implementers? A discussion of GSR upgrades, wave equipment, 65XX purchases, politics, routing architectures, etc ensued.

5. HPR-TAC representative to BAC (Jerry Keith - UCR)

The BAC would appreciate a representative from the TAC to help guide technical discussions involving money. Michael Van Norman echoed the request and has a call out for volunteers.

6. HPR and DC route choices w/BGP (Lea Roberts - Stanford)

or as Lea states “Local Prefs are bad for your health.”

Lea raised that AS-path works to prefer HPR paths over DC paths. a long discussion regarding the configuration of local-prefs, MEDs, metrics and AS-path settings in BGP processes occurred. this discussion to be continued.

does advertising campus routes via ISP peering points make sense? HPR connected campuses who lose connectivity to HPR and don't accept default from CENIC may not hear route announcements over DC. so, though a site can get to x.com or to a DC site, they may not be able to reach other HPR sites.

Jim Warner warns against announcing campus routes over ISP peerings. the ISP/DC paths are not engineered to support the capacity HPR services require. if a campus has BGP mis-configured, we may not realize that until a failure of the HPR network occurs. recognizing that announcing routes in the current manner assures us that BGP sessions are configured properly - even though HPR sites will lose connectivity to each other during an HPR failure.

7. Performance Testing (Michael Van Norman and Lea Roberts)

UCSD, UCLA and UC Berkeley will arrange to carry out performance testing of the CENIC backbone using smart bits boxes. Brian Court requests that testing begin after the BAM retrofit is completed. now that Stanford is routing over HPR, Brian feels better that testing will occur over HPR and not impact DC. Brian is concerned about the cisco 4000 switches and the EGM circuit paths. Brian has no concerns about the ONI gear. Brian asks that stress testing of the EGM circuits be performed off-hours.

Russ Hobby starts a discussion about the Internet2 piPES project.

<http://e2epi.internet2.edu/>

Tom Hutton has funding via I-TECH to place BWCTL tools in the backbone at Sunnyvale or UC Davis and the greater Los Angeles area. Tom and Brian Court will work together in design the testing of the backbone using the piPES toolkits. a discussion regarding tools, tests, hardware platforms and operating systems ensued.

8. Network Documentation (Heather Sherman)

Heather outlined CENIC's documentation roadmap. documentation will be presented in an all web-based fashion. no special applications will be needed to edit or acquire archived information. Heather is using standard tools such as Apache, MySQL and PERL.

documentation will include tabular optical information. Heather presented a series of slides showing samples of documentation to be expanded upon. standard names for circuits, wave-lengths, VLANs and route paths will be created. Heather admits that she has a lot to consider when creating a paradigm for circuit names.

Heather asks the HPR-TAC community for input on how to label logical circuit IDs. the intent is to never change the name of a logical circuit ID.

physical circuits (T1s, EGMs, ONI fiber, etc) will be documented according to the provider's paradigm.

Heather will describe physical circuit layout records for point-to-point connections through WDM, provider circuits, routers, switches, etc.

the preliminary work can be found at <http://sandbox.cenic.net>. contact the NOC for login name and password.

9. Arbor Networks DDOS detection tool (Nihar Mehta - CENIC)

CENIC recognizes the changes in the type and frequency of DOS attacks. CENIC is looking at ways to get ahead of the curve by identifying problems and mitigating them. CENIC does not yet have real time layer 3 and 4 analysis tools.

CENIC is evaluating Arbor Networks "PeakFlow" to deal with DDOS and WORM attacks. PeakFlow uses SNMP, BGP and netflow version 5 exports to collect and analyze real time data. PeakFlow is being evaluated as a response to the DO\$ attack experienced by UC Irvine in late March and Early April of 2004. Abilene has deployed PeakFlow. it is a completely passive tool.

PeakFlow supports two types of analysis. the first is anomaly detection and fingerprinting. examples are large ICMP flows in a short period of time and SYN attacks.

the second type of analysis is dynamic profiling (DO\$). this compares traffic patterns to dynamically generated baselines. PeakFlow detects anomalous flows

PeakFlow has decent analysis and reporting mechanisms. it can recommend ACLs for juniper and cisco routers and facilitate insertion of BGP blackhole routes. PeakFlow has trace-back capabilities that show attack trajectory across the network. it can trace-back the flow to the router or interface that the flow enters the network through.

PeakFlow requires a significant amount of time and work to fully implement. PeakFlow does not itself directly solve the DO\$ attack, but it does a decent job of identifying it - so the technical staff can solve it. in the academic environment PeakFlow is susceptible to false positives due to the research applications across the backbone.

PeakFlow is extremely expensive to purchase and maintain. it is cost prohibitive to monitor the entire CalREN2 backbone. CENIC believes an increase of operational staff would be needed in order to see the benefits of this tool.

a presentation of slides was shown of observations made of PeakFlow in action. the slides showed all kinds of cool stuff like: bandwidth use, source and destination addresses, port and service and in/out interface transit through routers that were monitored.

the HPR TAC held a discussion about how PeakFlow could be used on CalREN2.

9. DDOS blackholing (Mark Boolootian - UCSC)

we held a limited discussion to get an update on blackholing. Level(3) and Qwest offers this service. WilTel claims they will offer it by the end of this year. Cogent will not be offering this service.

CENIC is looking at implementing blackholing based on the NANOG recommended implementation.

during the meeting, we decided that a tag of 666 will block everything (including HPR, DC and ISP), but a tag of 667 will only black-hole the route to transit providers (including ISP). there's a desire to have this implemented before the start of school in "September".

10. RANCID protection (Brian Court)

Brian asked for and was granted permission to password protect the backup configurations of CENIC equipment. a recently announced exploit of OSPF on routers led to this request. knowing of the exploit, how it works and being able to look at configurations of CENIC equipment online, caused concern amongst the CENIC staff.

11. Future Meeting Schedule

the next HPR-TAC meeting will be held at UC Berkeley on Thursday, 28 October 2004 from 1000-1500.

this document was prepared by mike scott: mscott@uci.edu