Correlating Internet Performance Changes and Route Changes to Assist in Trouble-shooting from an End-user Perspective

Connie Logg, Jiri Navratil, and Les Cottrell

Stanford Linear Accelerator Center, 2575 Sand Hill Road, Menlo Park, CA 94025

Connie Logg, cal@slac.stanford.edu,
Jiri Navratil, jiri@slac.stanford.edu,
Les Cottrell, Cottrell@slac.stanford.edu

Abstract.[1] With the growth of world wide data intensive scientific collaborations, there is a need to transfer large amounts of data to and from data repositories around the world. To effectively enable such transfers, high speed, predictable networks are needed. In turn, these require performance monitoring to ensure their quality. One tool/infrastructure that has been successfully used for the analysis and monitoring of critical paths is IEPM-BW[1]. Based on experience gained from the *achievable* throughput monitoring in IEPM-BW, we developed ABwE[2], a tool to enable quick (< 1 second), low impact (40 packets) measurements of *available* bandwidth. Using ABwE we have been able to quickly detect significant changes in available bandwidth on production links up to 1Gbps, and report this information to the appropriate Network Operations Centers (NOCs) for repair, as such changes are often associated with route changes. This paper discusses this set of tools and their effectiveness together with examples of their utilization.

1 Introduction

With the growth of world wide data intensive scientific collaborations, there is a need to transfer large amounts of data to and from data repositories and collaborator sites around the world. To effectively enable such transfers, high speed, efficient, predictable networks are needed. In turn, these require continual performance monitoring to ensure optimal network performance for the applications to run. One tool/infrastructure that has been successfully used for the analysis and monitoring of critical paths (i.e. paths for which optimal performance is required) is IEPM-BW[1]. Based on experience gained from the achievable throughput monitoring in IEPM-BW, we developed ABwE[2], a tool to facilitate quick (< 1 second), low impact (40 packets) measurements of available bandwidth. Using ABwE we have been able to quickly (within minutes) visually identify significant changes in available bandwidth on production links with up to 1Gbps bottlenecks. Investigating such changes, in

[1] This work is supported by U.S. DOE Contract No. DE-AC03-76SF00515.

particular degradations, we have found, not surprisingly, that many can be associated with route changes. Once such a significant performance change is discovered, the main problem for the end-user (e.g. network administrator at an end-site) is to: gather relevant information to identify the magnitude of the change; the time(s) it occurred; identify the before and after routes; see if the change affects multiple paths; discover common points of change in the paths; identify the probable relevant Internet Service Providers; and report this information to the appropriate Network Operations Centers (NOCs). In our experience once the above has been done, the NOCs are fairly quick in responding with the cause of the change and often a fix. We have therefore developed a set of tools to facilitate the above process. The tools measure traceroutes at regular intervals, record them in an archive, and provide tools to enable simple visualization, navigation and integration with other tools such as ABwE and IEPM-BW, and a topology display. This presentation will present this set of tools and discuss their effectiveness together with examples of their utilization.

2 History and Methodology

In November 2001, a monitoring host with a 1 GE interface was set up at SLAC. Remote hosts (35-45) at collaborating sites around the world were chosen as target hosts for network performance tests. Accounts with SSH[3] access were set up on these remote hosts to provide for communicating with them. Several tools were evaluated and eventually PING, IPERF[4] (TCP/UDP transfer tool), BBFTP[5] (file transfer tool), BBCP [6] (another file transfer tool), QIPERF[7], and GridFTP[8] were selected. Currently at regular intervals PING, TCP transfers (using IPERF), file transfer tools BBFTP and GridFTP, and ABwE measurements are run. Note that the ABwE measurements are made in both the forward and reverse directions. In addition, forward *and* reverse trace-routes are run approximately every 10-12 minutes between SLAC and all the remote hosts. The results of these tests and the trace-routes are analyzed to: identify unique routes and assign route numbers to them for each remote host; identify significant route changes; and to turn the data into more useful formats (web browsable for users, text format to embed in email to Internet Service Providers, log format for debugging etc.). The data is stored in a data base with the measurement time and other test parameters for access by Web Services[9], MonALISA[10], and other visualization and analysis tools.

3 Visualization

The simplest visualization technique involves time series graphs of the ping minimum and average Round Trip Times (RTTs), the results of the achievable and available bandwidth test results, the file transfer throughputs, and indicators on the time series graphs which denote when the route to or from a node has changed. This allows for visual correlation of significant changes in RTT, available and achievable bandwidth, and route changes in one or both directions. Fig. 1 is an example of this. Fig. 1 type

graphs can be very dense, however there are options available with them to individually plot the components and to vary the time scale.

As can be seen in Fig. 1, route changes frequently do not cause throughput changes, but throughput changes often correlate with route changes. Table 1 presents a summary of visually identifiable route and throughput changes for 32 nodes monitored via IEPM-BW for the period 11/28/03 – 2/2/04. Often (see Table 1) a change in throughput is associated with a route change. This suggests that the first thing to check for when evaluating throughput changes would be a route change.

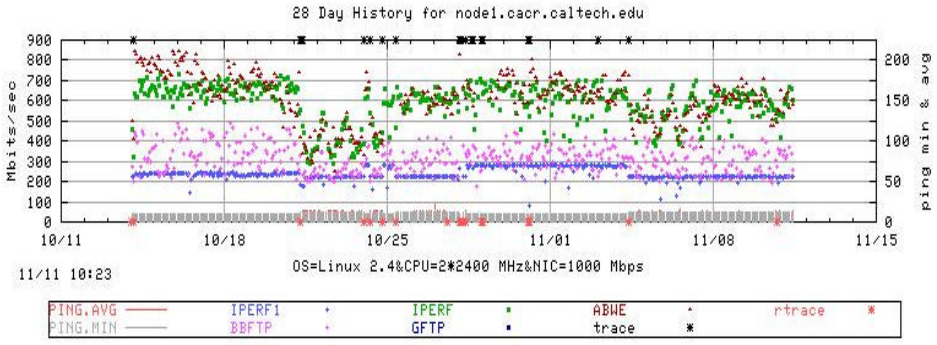

Fig. 1. Time series plot with route changes indicated. The asterisks along the top axis indicate the forward traceroute changes. The asterisks along the bottom axis indicate reverse route changes. Note the correspondence between throughput changes and forward route changes

Table 1. Summary of Route and Throughput Changes for 11/28/03 - 2/2/04

Location (# nodes)	# route changes	# with thruput increase	# with thruput decrease	# thruput changes	# thruput change with route	# thruput change w/o route
Europe(8)	370	2	4	10	6	4
Canada & U.S. (21)	1206	24	25	71	49	22[2]
Japan (3)	142	2	2	9	4	5

We also observe, not unexpectedly since many of the routes to remotes hosts share subroutes, that a route change to one host often corresponds with changes in the routes

[2] Note that 9 of these throughput changes are regular variations on Friday nights due to regularly scheduled large data transfers on one of the target networks.

to other hosts. A web accessible route daily summary page (Fig. 2) is created and updated throughout the day. At the top of the page are links to "Yesterday's Summary", today's "Reverse Traceroute Summary", and the directory containing the historical traceroute summaries. Under those links is the traceroute summary table which provides "at a glance" visualization of traceroute change patterns. This facilitates the observation of synchronized route changes for multiple hosts in the cases that a common subroute changes for some of them.

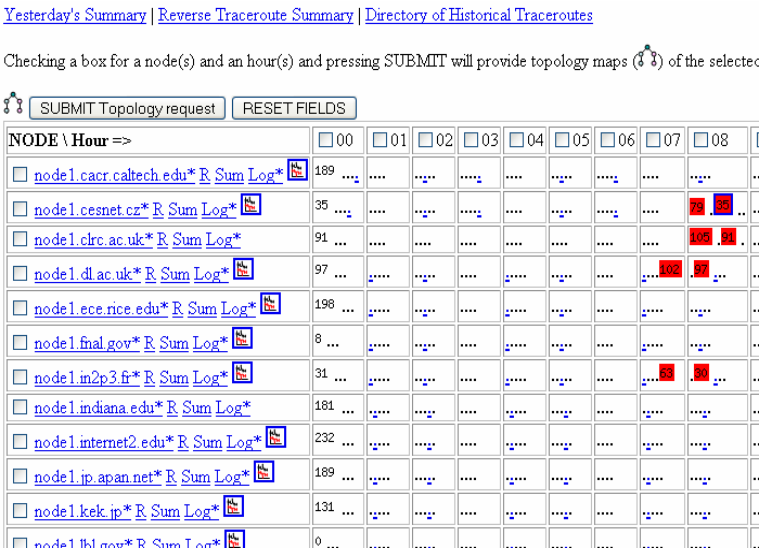

Fig. 2. Screen shot of part of a traceroute summary web page with summary table

To facilitate further investigation of changes, there are highlighted links in this table that allow one to: view all the traceroutes for a selected remote host (as a color coded web table accessible by clicking on the nodename); access text suitable for attaching to trouble reports (Sum); review the log files (LOG*); review the route numbers ("R") seen for a given host together with when last seen; view the available bandwidth time-series for the last 48 hours ( ); and to select times and remote hosts for which one wishes to view topology maps.

In Fig. 2 for hours "07" and "08", it can be seen that there were multiple route changes to European nodes in the same time frame. Each entry (there can be multiple for each box representing an hour) provides a dot to denote that the route has not changed from the previous measurement. If the route has changed, the new route number is displayed. The first measurement for each day is displayed with its route number. This very compact format enables one to visually identify if several routes changed at similar times, (i.e. route numbers appear in one or two columns for multiple hosts (rows)), and whether the changes occur at multiple times and/or revert back to the original routes.

Note that the table has check boxes before the nodes and above the hour columns at the top of the table. By checking boxes for nodes and hours, and then clicking on

"SUBMIT Topology request" the viewer can generate a topographical map of the routes.

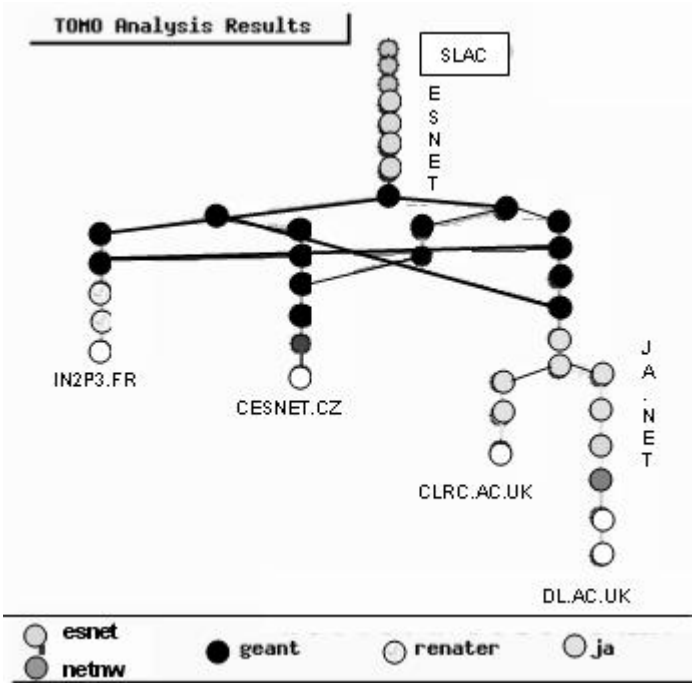

Fig. 3. Topology visualization of routes from SLAC to 4 European sites between 07:00 and 09:00 Jan 15 '04

Fig. 3 is an example of such a topology map showing routes from SLAC between 07:00 and 09:00 on Jan. 15 2004 to European sites in France, the Czech Republic, and 2 sites in the UK. This corresponds to the route changes seen in Fig. 2, and the multiple routes used can be clearly seen. The topology maps display the hop routers colored by ISP, provide the router and end host names by "mouse over", and provide the ability to zoom in to help disentangle more complex sets of routes.

4 Example of the Visualization of Achievable and Available Bandwidth Changes, and Route Changes

The measurements of achievable and available bandwidth use very different techniques. We measure achievable bandwidth via an IPERF TCP memory to memory transfer between two hosts over many seconds (usually 10 seconds). IPERF is network intensive as it sends as much TCP data as possible for the duration of the measurement. Thus we make IPERF measurements every 90 minutes. We measure

available bandwidth using ABwE in less than a second by sending 20 UDP packet pairs, and measuring the time dispersal of the inter-packet delays upon arrival at the remote host. We repeat the ABwE measurements every minute. Fig. 4 is the graph of the IPERF bandwidth data points and the ABwE measurements from SLAC to Caltech for a 24 hour period on October 9, 2003. ABwE provides estimates of the current bottleneck capacity (the top line in Fig. 4), and the cross-traffic (the bottom line in Fig.4) and the available bandwidth (middle line). The available bandwidth is calculated by subtracting the cross-traffic from the bottleneck capacity. The IPERF measurements are displayed as black dots on the graph. The two measurements are performed independently from two different hosts at SLAC. Note the corresponding drop observed by the two bandwidth measurements at about 14:00. To understand what has happened here, it is only necessary to look at the traceroute history for this day.

Fig. 5 is a snapshot of the traceroute table for Caltech corresponding to Fig. 4. Note the change from route #105 to route #110 at 14:00, and back again to route #105 about 17:00. By selecting those hours and the Caltech node and submitting the topology request, we can get a graph (Fig. 6) of the topology change responsible for the bandwidth changes.

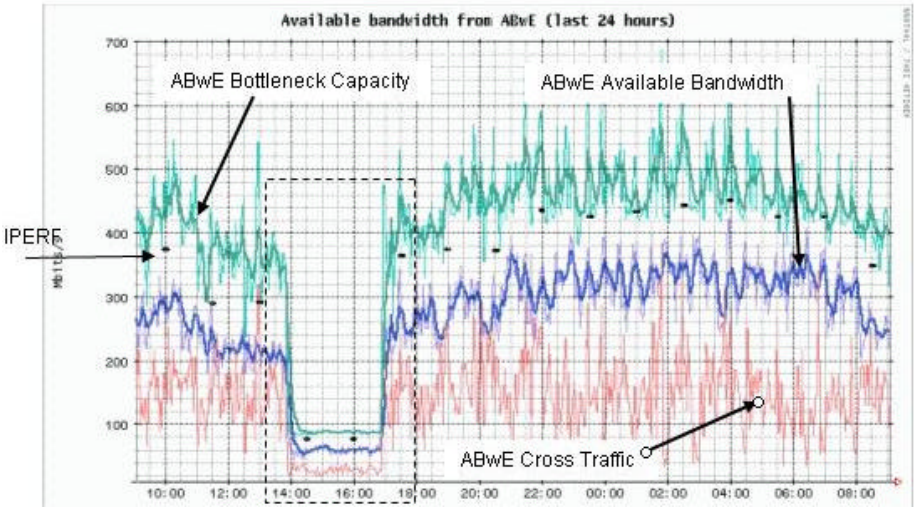

Fig. 4. Plot of ABwE (available bandwidth) measurements and corresponding IPERF (achievable bandwidth) measurements

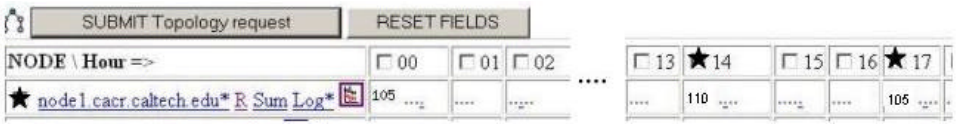

Fig. 5. Snapshot of traceroute summary entry for Caltech at 14:00 and 17:00

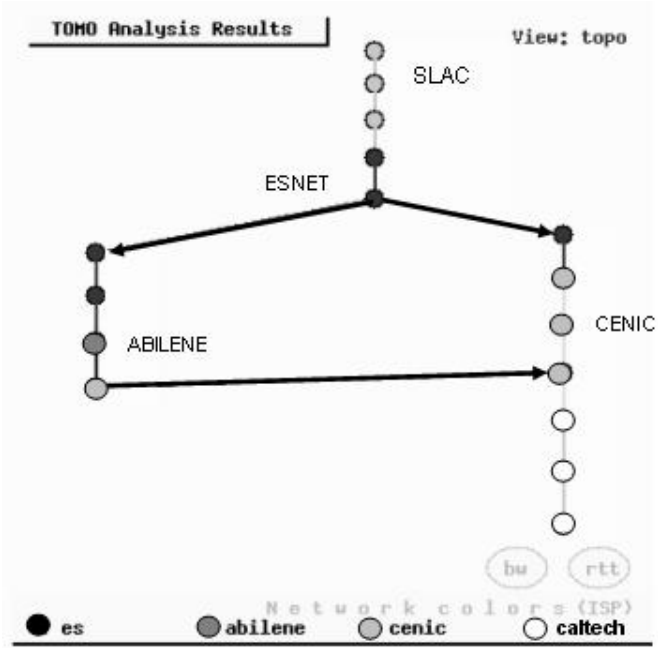

Fig. 6. Graphical traceroute display. Note hop to ABILENE on the way to CENIC

5 Challenges in Traceroute Analysis

Analyzing traceroute data to identify unique routes and to detect "significant" changes in routes can be tricky. At many hops there can be non-responsive router responses (see hop "12" in Fig. 7) one or more times, where no information is returned.

```
traceroute to NODE1-GIG.NSLABS.UFL.EDU (xx.yy.160.3)
 1  SLAC-RTR1  0.164 ms
 2  SLAC-RTR2  0.368 ms
 3  i2-gateway.stanford.edu (192.68.191.83)  0.288 ms
 4  STAN.POS.calren2.NET (171.64.1.213)  0.369 ms
 5  SUNV--STAN.POS.calren2.net (198.32.249.73)  0.626 ms
 6  Abilene--QSV.POS.calren2.net (198.32.249.162) 0.959 ms
 7  kscyng-snvang.abilene.ucaid.edu (198.32.8.103) 36.145 ms
 8  iplsng-kscyng.abilene.ucaid.edu (198.32.8.80) 53.343 ms
 9  atla-iplsng.abilene.ucaid.edu (198.32.8.78)  60.448 ms
 10  a713.c12008.atla.abilene.ucaid.edu (192.80.53.46) 71.304 ms
 11  ssrb-ewan-gsr-g20.ns.ufl.edu (128.227.254.122)  71.323 ms
 12  *
 13  nslab-bpop-rsm-v222.nslabs.ufl.edu (128.227.74.130) 76.356
```

Fig.7. Traceroute output

This can happen for a variety of reasons due to the configuration of the router at that hop and/or the type of software that it is running. There can be multiple non-responses

for the same hop. There can be hop changes within a network provider's domain. In many cases these are transparent and no effect on the throughput is seen, while at other times these can be significant. Looking at the trace route output unfortunately does not solve the problem. In our processing of traceroutes to detect significant routing changes, we basically ignore non-responders. However route changes, even within a network provider's domain are considered significant. In the topology graphs responsive and non-responsive hops are displayed.

6 Challenges in Identifying Throughput Changes

Ideally we would like to automate the detection of throughput changes and compare them automatically to the traceroute changes. We have mentioned the problem with identifying significant traceroute changes. Identifying throughput changes is also tricky. One has to set "thresholds" of change to use in order to pick out throughput changes. These thresholds must vary according to the throughput level. On a gigabit link which handles high volume data transfers, a drop of 100-200 megabits (10%-40%) may simply be the result of a long/large data transfer, and may not be significant. On a 100 megabit link, a drop of 50 megabits (50%) may very well be significant, or again it may mean that there is a sustained high volume data transfer occurring.

The frequency of the data points also needs to be taken into consideration, to avoid false "alerts" which are worse than no alerts, ideally one wants to identify a "sustained" drop before alerting. If the data points are one hour apart, it may take several hours to have enough data to be sure it is a sustained drop. If the data points are once a minute, 10 minutes or slightly more may be adequate. Even with one minute samples, the identification may be difficult. In some cases we have seen the drop happen gradually over a day or two, and thus the percent change threshold is never exceeded.

7 Utilization

This set of tools has been in production use at SLAC for several months. It has already been successfully used in several problem incidents and is being enhanced as a consequence of its use. We will report on specific examples illustrating how the tools have been used to identify and pin-point performance problems in various networks. In some of these cases the problem went unidentified for several days or even weeks in one case, but once identified and reported, the problem was fixed in hours. With the large number of important collaborating sites, it is impractical to manually review all the performance graphs for all the paths and detect problems quickly. This identifies the need to automate the reliable detection of significant changes.

8 Future Plans

Work is in progress to automate the identification of significant changes, and to automatically assist in gathering the associated relevant information (e.g. current, and trace routes before and after a performance change, time and magnitude of the change, topology map, and time series plots of the performance changes). This will be gathered into email and a web page and sent to the local network administrator. We expect to report on progress with this automation by the time of the conference. We are also analyzing the ratio of significant performance problems caused by route changes and vice-versa, and the duration of significant performance degradations, and will also report on this.

References:

1. *Experiences and Results from a New High Performance Network and Application Monitoring Toolkit*, Les Cottrell, Connie Logg, I-Heng Mei, SLAC-PUB-9641, published at PAM 2003, April 2003.
2. *ABwE: A Practical Approach to Available Bandwidth Estimation*, Jiri Navratil, Les Cottrell, SLAC-PUB-9622, published at PAM 2003.
3. SSH: http://www.ssh.com/solutions/government/secureshell.html
4. IPERF: http://dast.nlanr.net/Projects/Iperf/
5. BBFTP: http://doc.in2p3.fr/bbftp/
6. BBCP: http://www.slac.stanford.edu/~abh/bbcp/
7. QIPERF: http://www-iepm.slac.stanford.edu/bw/iperf_res.html
8. GridFTP: http://www.globus.org/datagrid/gridftp.html
9. Web Services: http://www.w3.org/2002/ws/
10. MonALISA: http://monalisa.cacr.caltech.edu/