

**Internet2 PAS  
Triannual Report  
12-1-14 through 4-1-14**

**Introduction**

This is the first in a series of periodic reviews of the Internet2 Performance Assurance System (PAS) infrastructure. The goal is to examine what is working and what isn't with an eye toward improvements and a focus on what information is important to the community for their decision-making process.

The Performance Assurance System was approved and funded very late in 2013. The September 3, 2013 outage event on AL2S illustrated a critical need for an alerting system that existed outside the boundary of a traditional L2/3 node. As an immediate solution, SmokePing was installed on existing servers located at every AL2S (node?) in order to provide alerts while a more comprehensive solution was developed. That more comprehensive solution is the Internet2 Performance Assurance System. It consists of four components: An internal perfSonar (pS) mesh with operational alerting, an external pS capability to work with our partners, a Service Monitoring capability to test and alert on issues above layer 4, and an ad hoc performance testing capability to fill gaps from the first three.

**Report Overview:**

- Internal perfSonar*
- External perfSonar*
- Ad Hoc Infrastructure*
- Service Monitoring*
- Quarterly Goals*

## Internal perfSonar

The goal of the internal perfSonar system is to ensure a 100% clean backbone. The internal pS mesh makes up the core of the I2 PAS. A server is collocated next to each AL2S node. It is connected to the L2 node and to the L3 node if one is present.

```
DESCRIPTION          UDP Throughput (iperf)
TOOL                  bwctl/iperf, BWUDP
BWTestDuration        6, BWUDPBandwidthLimit  9500m,
BWBufferLen           60k, BWWindowSize      96m,
BWTestInterval        750, BWTestIntervalStartAlpha  1,
BWReportInterval      1
```

```
DESCRIPTION          One-Way Latency
TOOL                  powstream
OWPINTERVAL           0.1, OWPLOSSTHRESH      10.0,
OWPSESSIONCOUNT     10800, OWPSAMPLECOUNT
600, !OWPPACKETPADDING, OWPBUCKETWIDTH      0.001
```

The tests results are fed to Nagios and alerts are generated. IE: Any loss in the last 180 seconds triggers an alarm, with 2 retries before a hard alarm is generated. We warn on bandwidth below 9.5 GB/s and raise a critical alarm at 9.0Gb/s, with one retry before a hard alarm status. Packet loss issues are treated the same way as Circuit Down events; for example: after-hours the on-call engineer is contacted and works to resolve the performance issue.

## **External perfSonar**

The external perfSonar capabilities run alongside the internal mesh on the same server hardware. The intent is to provide a well-documented resource that network engineers within and outside Internet2 can use to help troubleshoot performance related issues. This will be accomplished by running a regular scheduled test to each connector of the L2 and/or L3 node at that site, with public visibility into the results.

## **Ad Hoc Infrastructure**

There is a need to provide an infrastructure for performance related testing that falls outside of the regular internal and external tests. This may be ad-hoc iPerf and perfSonar tests for support of an individual project, or testing over some longer period of time or through some new mechanism. Three of the existing Internet2 Observatory machines are being upgraded and targeted for this capability.

## **Service Monitoring**

Internet2 offers several services to users. One service might be Support for Data Intensive Sciences, and the internal/external pS testing might be thought of as specialized monitoring for that service. That leaves a number of other services with either no monitoring or only lower-level component monitoring. For example, circuits are provisioned on AL2S through the use of the OESS tool, either interactively through the web or by using an API call. While many of the components of the OESS provisioner are monitored there is no end-to-end monitoring of the service. The Service Monitoring infrastructure is targeted at solving this. It would make calls to the API and/or web interface in an attempt to actually USE the service. Service Monitoring is expected to support both internal Internet2 services, such as the OESS provisioner and Net+ services, Alerting on internal services.

## **Goals over the next four months**

- We need to integrate back in to the pS community. As a part of good Business Relationship Management it is critical that we be involved in our pS community and integrated well in to the needs and experiences of others.
- We need to develop a series of “usage metrics” for each of four aspects of the PAS. This needs to be twofold: both what our overall coverage is and what impact the infrastructure is having. IE: are we making an impact and if not what do we need to do?
- We need to determine what we will and will not support in terms of tests to external peers. The interval, the length, etc.
- It is assumed that there will be end-host issues. We need to develop some internal documentation both for our own staff and to point users to at the common performance issues faced.
- We’d like to expand the PAS to include WIX, MANLAN, and Singapore.
- We’d like to set up regular testing with at least 50% of our connectors. This includes a provisioning process.
- We need a series of web pages integrated in to the I2 site that provides details on the service.
- We will need to run a project to identify the server resources in the pops and determine which servers can now be deprecated.
- We’d like to baseline AWS performance and extend general service monitoring to 25% of our services, both internal and Net+ connectors.

