International Research Journal of Engineering and Management Studies (IRJEMS)
Volume: 03 Issue: 03 | March -2019 e-ISSN: 2395-0126

# Big Data and Analysis of Data Transfers for International Research Networks Using NetSage

**SRI KRISHNA ADITHYA COLLEGE OF ARTS & SCIENCE**

**[1]SELVAPRIYA.R, [2] NASRUL HUQ T.A, [3] SANTOSH KUMAR. M**

**[1] Asst Porffessor, [2] Bsc CT, [3] Bsc CT**

[1]selvapriyar@skacas.ac.in [2] 16bct042nasrulhuqta@skacas.ac.in [3] 16bct049santoshkumarm@skacas.ac.in

**Abstract—Modern science is increasingly data-driven and collaborative in nature. Many scientific disciplines, including genomics, high-energy physics, astronomy, and atmospheric science, produce petabytes of data that must be shared with collaborators all over the world. The National Science Foundation-supported International Research Network Connection (IRNC) links have been essential to enabling this collaboration, but as data sharing has increased, so has the amount of information being collected to understand network performance. New capabilities to measure and analyze the performance of international wide-area networks are essential to ensure end-users are able to take full advantage of such infrastructure for their big data applications.**

**This paper addresses the basic NetSage architecture, its current data collection and archiving approach, and details the constraints of dealing with this big data problem of handling vast amounts of monitoring data, while providing useful, extensible visualization to end users.**

## I. INTRODUCTION

Much of modern science is now driven by data from scientific instruments, some producing even petabytes of data, which is then shared and analyzed by thousands or tens of thousands of scientists all over the world. Some of the "big data" challenges in this space are related to the growing archive of network data available for analysis, the diversity of available data sets, and the need for long-term storage in order to do trend analysis. New methods to monitor, analyze, and understand the performance of big data transfers are needed to assure that end-users are able to take full advantage of networking infrastructure. This complex cyberinfrastructure is rapidly increasing our ability to produce, manage, and use data .

The NetSage project is designed and developed to provide a network measurement service for use with the NSF International Research Network Connection (IRNC)-funded backbone and exchange point services. NetSage provides a unified view of the traffic on the links, and assists stakeholders in identifying congestion and bottlenecks. The data collection and visualization services are being developed to directly respond to questions that have been provided by the user community.

This paper describes the NetSage system. In Section 2 of this paper we provide an overview of NetSage and its use cases. In Section 3, we describe the NetSage monitoring architecture, with additional details given in Section 4 for the data sources. Section 5 describes the archive, and Section 6- the visualization. In each section, we detail the "big data" needs and challenges, and how we are approaching them.

## II. NETSAGE OVERVIEW

NetSage was originally developed to better understand the behavior of the NSF-funded International Research Network Connections (IRNC) backbone networks and exchange points, shown in Figure 1. The IRNC-funded backbones include: TransPAC4 , AmLight ExP , PIREN (Pacific Islands Research and Education Networks) , ACE (America Connects to Europe), AtlanticWave , StarLight , and Pacific Wave

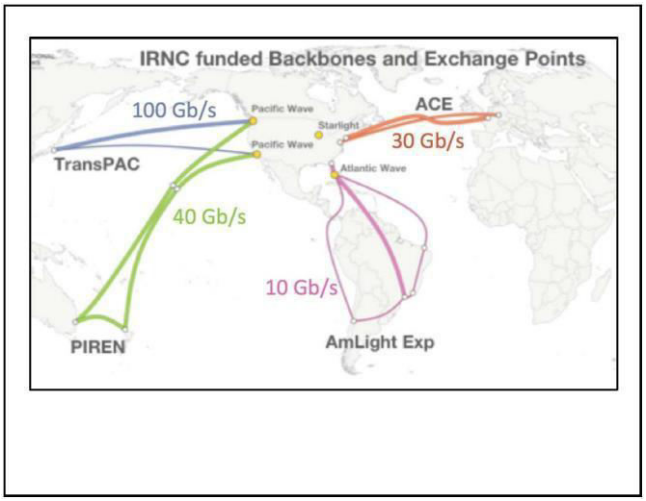


Figure 1. The current NSF IRNC-funded backbones and Exchange Points, showing link capacity for each network.

as well as their respective exchange points. Overall, these connections carry the majority of U.S. research traffic to and from their international collaborators. They operate 24 hours a day, 7 days a week, and combined, represent over 500Gb/s of network capacity.

NetSage is building and deploying advanced measurement services and an exploratory visualization platform to benefit science and engineering communities dealing with big data transfers in multiple ways by focusing on providing a better understanding of:

- current traffic patterns across IRNC links, and the ability to better understand growth trends for capacity-planning purposes;
- the main sources and sinks of "large, long fat network" (LFN) or "elephant flows," to know where to focus attention on outreach and training;
- where packet loss is occurring, whether or not the loss is caused by congestion or other issues, and the impact of this on end-to-end performance;
- how the IRNC links are being used by the different research domains and institutions.

NetSage services will provide an unprecedented combination of passive measurements, including SNMP data [2] [3], flow data [4], and traffic header analysis [5], as well as active measurements [6], to create longitudinal network performance data visualizations.

For monitoring and analysis to be effective, it must begin with a clear understanding of the intended audience and the types of insight needed by that audience. The NetSage project defines four sets of end users for their data and visualization services:

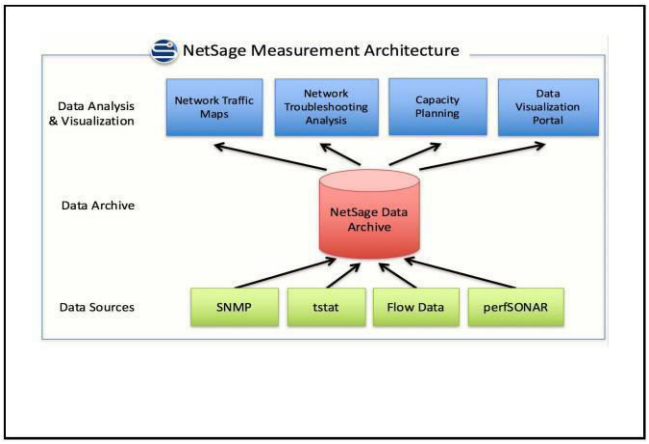
1. Project oversight managers. These include National Science Foundation Program Directors and other higher-level users, and they may be concerned with issues such as showing that the traffic on the links are exhibiting broad societal relevance
2. The IRNC Network Operations Center (NOC) and other network operators. Network operators may use the NetSage

data to understand performance issues or identify developing problems.

3. Project planners for the IRNC-funded backbone networks and exchange points. Owners of the backbones and exchange points may want to use NetSage data to do capacity planning or to understand points of contention.

4. Application engagement staff. Several projects have funded application engagement staff in order to assist end users in getting better performance over the funded circuits or exchange points. NetSage data could be used to identify some of these classes of users. NETSAGE MONITORING ARCHITECTURE

The NetSage architecture design was primarily driven by the application/algorithm needs and the system/platform-level requirements as described in NetSage consists of a 3-layered architecture, shown in Figure 2, similar to many other monitoring approaches. The bottom layer consists of various data sources. The monitoring systems that we deploy are capable of running at 10Gbps or higher, support both IPv4 and IPv6, support Layer-2 circuit technologies, and do not impact the production traffic. These data sources combine multiple, different active and passive measurements, as detailed in Section 4.




began by collecting SNMP data since each of the backbones and exchange points were already collecting this data and archiving the data sets in public archives.

The second layer consists of the NetSage archive service. In order to enable the ability to perform analysis in near-real time and to enhance the system's performance when coping with the inherently different data types (Time series data and aggregations of data) several approaches were explored. The first uses the Time Series Data Service (TSDS) to implement a shared archive with the IRNC NOC (detailed in Section 5). This service provides a standard interface to upload data from the various data sources, as well as a standard interface to higher level services to integrate and query for these multisource time series data from the same repository. The second approach uses the "ELK stack" to

create aggregations summaries of individual flow records. (detailed in Section 5).

The third layer is a suite of visual analytics tools that address the questions outlined in Table 1. This is detailed in Section 6.

## III.NETSAGE DATA SOURCES

The core of the NetSage infrastructure is the collection of data related to both the network links and exchange points. These are a combination of passive measurements, such as SNMP, flow data, and data from packet header inspection, and active measurements, currently perfSONAR.

The Simple Network Management Protocol (SNMP) is an application–layer protocol defined in RFC1157 for collecting and organizing information about managed devices on IP networks. SNMP is commonly used by routers and switches to monitor networks for conditions that warrant administrative attention. This data is commonly collected and openly archived by most R&E networks. The SNMP data is collected every 60 seconds for each of the links.

A second set of passive data can be acquired by means of packet header inspection tools that examine the headers of a network flow and pulls out valuable data from them, without touching the payload of the message. Initially, the NetSage project studied the possibility of using Bro [19] for this purpose. However, after analyzing its performance in a test lab, we found that the Bro TCP analyzer was very CPU intensive, and that large numbers of packets were dropped when even moderate numbers of flows were analyzed.

Instead, we are currently deploying the "Tstat" tool for our packet header inspection tool. Tstat is part of the EUMeasurement Plane (mplane) FP7 project developed by Munafó and Mellia at Politecnico di Torino, and can be used to analyze either real-time or captured packet traces. It rebuilds each TCP connection by looking at the TCP header in the forward and reverse direction. Tstat reports a number of useful TCP statistics, including congestion window size and number of packets retransmitted, which can be used to analyze the health and performance of the link. We expect this data to grow to the order of at least about 1 TB per month per link, depending on what additional parameters we request.

Another source of passive data for networks is related to flow data collection. Depending on the hardware, this might be NetFlow , sFlow , or IPFIX. Flow data will allow us to answer several of the questions desired by our end users: which science domains are using the networks, what do elephant flows look like, etc. Currently, the TransPAC and ACE links

generate 40-100GB of flow data per link per month. Flow data collected from exchange points is expected to be around 10 times bigger, up to 400GB - 1TB per exchange point per month.

Analysis of the flow data indicates that distribution of flows in R&E networks is heavily skewed towards large number of small flows (<100kB), and significant but comparatively smaller, number of very large flows. Flows with sizes of >100MB account for majority of the of the traffic, and that influenced decision to limit analysis of flows of that size or larger ("elephant flows"). Since such flows are much smaller in number, this eases strain on hardware for analysis and helps manage dataset sizes for multiple links and exchange points, from our preliminary tests we expect an average data reduction of 2 orders of magnitude.

The NetSage measurement services include active measurements as well, currently in the form of perfSONAR tests to gather latency and bandwidth information. PerfSONAR is a network measurement toolkit designed to provide federated coverage of paths and help to establish end-to-end usage expectations. We have developed a perfSONAR exporter tool that pulls data from an open perfSONAR MA and inserts it into our archive, TSDS. We have set up tests for each of the backbone links and exchange points across the full project. The current IRNC perfSONAR dashboard of tests is available at TransPAC dashboard. PerfSONAR data is collected every 6 hours for bandwidth tests and every 60 seconds for losses. We are currently storing around a few GB of PerfSONAR monthly data.

## IV. NETSAGE ARCHIVES

The second layer of the NetSage architecture is the data archive. NetSage uses a three -tier approach to flow data archives. With each tier having a specific set of capabilities and intended use After flow data is de-identified these individual flow records are stored as raw unindexed messages in canonical repository. The canonical storage is not used for analysis directly, its purpose is to ensure we can regenerate later tiers if we need to redesign.

After raw storage, the flow records are inserted into an Elasticsearch database using Logstash. This tier provides flexible query access to indexed individual flow records. This data is kept for multiple weeks and is used to generate aggregated summaries of traffic activity and to perform adhoc / exploratory data analysis.

The final tier contains pre-generated aggregates statistics derived from the individual flow records stored in Elasticsearch. The types of

summaries include: the distribution of traffic volume by protocol over time, the distribution of traffic by source, etc.

We are using the Time Series Data Service (TSDS) , an Open Source software developed on commodity hardware, that provides a common archive shared with IRNC NOC. The system allows for well-structured and high performance storage and retrieval of time series data. TSDS is capable of tracking and reporting based on metadata, for example the system allows to view interface throughput from the viewpoint of a VLAN or BGP peer sessions from a particular AS.

TSDS also provides the: "Time Series Query Language," which grants the possibility of easily generating reports about gathered data, including the ability to aggregate/summarize data over time, aggregate/summarize data based on one or more non-time dimensions, execute sub-queries to obtain incremental results, as well as the ability to perform a set of common aggregation functions for determining central tendency, frequency distribution etc. To give an example, once flow data is stored along with sufficient meta data in TSDS, a single query can be used to show the distribution of data transfer sizes between all known science facilities over the previous year, summarized by month and broken out by science domain.

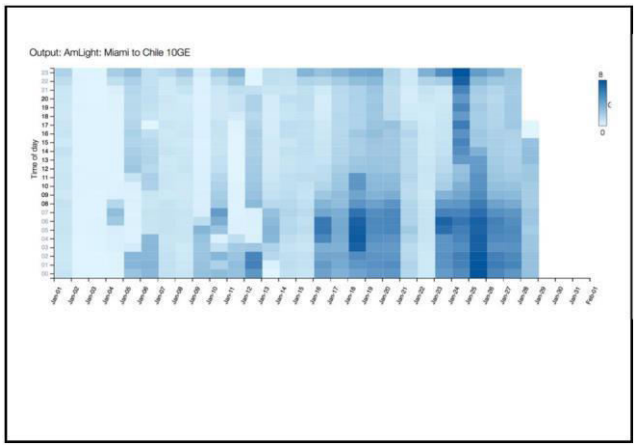
## V. NETWORK DATA VISUALIZATION

The top layer of the architecture as depicted in Figure 2, contains the data analysis systems and visualization components that will query the underlying database. The NetSage visualization service will enable both near-real time monitoring and longitudinal analysis of the interconnected R&E networks that are necessary to address the inquiries. Large-Scale networks have become increasingly challenging to manage by system administrators and/or network managers. Network anomaly detection is difficult due to its vast data volume, large numbers of attributes, interconnectivity/causality and high dynamics (i.e., connections can be established or broken at any moment, because users may come and go). Even when data mining and machine learning have proven effective in detecting anomalies, it is often the case that patterns are not known ahead of time by network administrators and operators . Visualization tools are needed to allow them environments. To achieve this multi-faceted view NetSage leverages SAGE2 (the Scalable Amplified Group Environment) a widely used open source middleware system for supporting visualization on large ultra high resolution

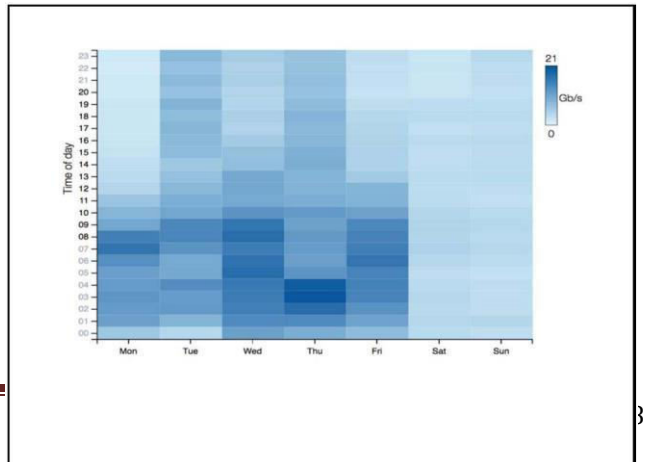
displays. NetSage was designed so that each query can generate its own independent visualization. These visualizations can then be combined as needed in SAGE2 like jigsaw pieces in a puzzle to help the user answer complex questions about the networks,backbones and exchange points. Darker lines and nodes represent higher bandwidth. To find these patterns by examining past data. While numerous network management and visualization tools have existed in the past, few of them are lightweight enough or specifically designed towards anomaly detection in dynamic network traffic data. The area of visualizing anomalous events in particular is still actively been studied by the visualization research community and is an area of interest in the NetSage project as well.

When visualizing large volumes of data, it is often difficult to see the bigger picture in the details. To improve big data exploration NetSage's approach is to enable visualizations from multiple queries to be juxtaposed simultaneously to provide a multi-faceted view of the network phenomenon being investigated. Prior research in ultra-high resolution display walls show that users are able to come to conclusions with greater creativity, speed, accuracy, comprehensiveness, and confidence using such The NetSage web site shows a default dashboard that provides an overview of the current state of all IRNC links for the last three hours. The Dashboard, which updates every five minutes, begins with a map, Links are colored on a blue scale while nodes are colored on an orange scale. Grey links and white nodes have no data for the last three hours. While viewing the visualizations hovering over the data points shows the underlying data values.

As one example, the NetSage query: "What is the max, min, average in bandwidth use across the IRNC network in




The horizontal axis represents days and the vertical axis represents time of day. Darker squares show higher data transmissions at those hours.



the last 7 days?" automatically produces visualizations similar to the ones described earlier except that based on users customized query parameters.

As another example of how NetSage is leveraging the visualizations to address managing large scale data during long periods of time, the NetSage query: "What is the duration and are there any periodic patterns or peak periods in bandwidth use across the IRNC network in the last month?" automatically produces a series of heatmaps over the period selected. These heatmap visualizations allow to cluster data by day or weekday without losing resolution in the input data. As it can be seen in Figure 9**,** in the vertical axis we have the hour of day in the horizontal axis we have a progression of days. The darker the color in the heatmap the higher amount of data was transmitted in that given periods of time. The chart to the right, also shown in Figure 10, shows an aggregation of the same information over weekly periods. Hovering the mouse over a particular data point shows more detailed information. This same visualization approach, as shown in Figure 11, can effectively be applied to other measurements such as perfSONAR tests for network loss or latency.

As mentioned earlier, all new queries are created in new tabs to facilitate comparisons of the data across large displays or walls, as shown in Figure 4. Each of these queries generate unique URLs which allows charts to be easily shared between network users and administrators to help them troubleshoot problems together.

## VI. CONCLUSIONS AND FUTURE WORK

The NetSage project is developing a framework for unified measurement and monitoring of the big data transfers over the IRNC-funded backbones and exchange points, with an emphasis on open source software, privacy, analysis and visualization. The suite of tools being deployed will enable end-users to better understand network performance in a scalable and flexible way.

Presently the fundamental components of NetSage have been deployed to enable us to begin to collect, archive and visualize data from the IRNC backbones and exchange points. Next steps include expanding the data sources, both in terms of types and coverage and working to include measurement data from common data sources. At the same time, we are working on creating a science registry which will allow us to map flows to science projects in order to understand how the IRNC networks are being used and to gain insight into new research questions that have not yet been

addressed. For example: how do researchers worldwide in various disciplines share data with each other. In terms of analytics and visualization, the next steps include creating meaningful aggregations of flow data and creating tools to visualize those aggregations to gain insight on big data transmissions and elephant flows. We also intend to implement machine learning capabilities for predicting future use or predicted losses as well as tools to automatically detect patterns on the visualizations to reduce the cognitive effort of NetSage users.

While the big data challenge for NetSage's data gathering effort is in overcoming the sheer volume of the data, the challenge for visualization is helping network troubleshooters understand the complex relationships between network parameters that ultimately affect network performance.

The portal can currently be accessed from http://www.netsage.global and there is already growing interest by international network partners in adopting our methodology so that in the future an open standard for the collection, sharing, and analysis of network data can be created.

## REFERENCES

[1] Atkins, D Revolutionazing Science and Engineering Through Cyberinfrastructure: Report of the National Science Foundation Blue-RibbonAdvisoryPanelon Cyberinfrastucture, 2003. www.cise.nsf.gov/sci/reports/toc.cfm

[2] Case, J., Fedor, M., Schoffstall, M. Davin, J. Simple Network Management Protocol (SNMP). 1990

[3] Case, J., Fedor, M., Schoffstall, M. Davin, J. RFC1157. 1990

[4] Claise, B., Ed., Trammell, B., Ed., Aitken, P., Specification of the IP Flow Information Export (IPFIX) Protocol for the exchange of Flow information. 2013

[5] Marco M., Renato Lo C., Fabio N., Measuring IP and TCP behavior on edge nodes with Tstat, Computer Networks, Vol.47, No.1, pp.1-21, ISSN: 1389-1286. 2005