ARISTA WHITE PAPER

Application Visibility and Network Telemetry using Splunk

Arista Networks was founded to deliver software defined cloud networking solutions for large data center and high-performance computing environments. With more than one million cloud networking ports being deployed worldwide, Arista delivers a portfolio of 1/10/40 and 100GbE products that redefine network architectures, bring extensibility to networking, and dramatically change the price/performance of data center networks.
At the core of Arista's platform is the Extensible Operating System (EOS™), a ground-breaking network operating system with single-image consistency across hardware platforms, and modern core architecture enabling in-service upgrades and application extensibility.
This whitepaper details Arista's Network Telemetry Application for Splunk and EOS extensions that enable Arista switches to push network telemetry information into Splunk.

APPLICATION VISIBILITY CHALLENGE

As Enterprises and Service Providers evolve from traditional static networks to virtualized on-demand cloud networks, troubleshooting and monitoring toolsets also need to evolve to provide fine-grained visibility into application performance and network-wide monitoring capabilities that integrate with both industry standards and customer specific dev/ops solutions.

Arista EOS already has numerous features that provide visibility into network traffic such as Latency Analyzer (LANZ), Data Analyzer (DANZ), sFlow, Path Tracer, VM Tracer, MapReduce Tracer as well as tools like Advanced Event Monitor (AEM) that provides an on-switch record of data-plane forwarding changes.

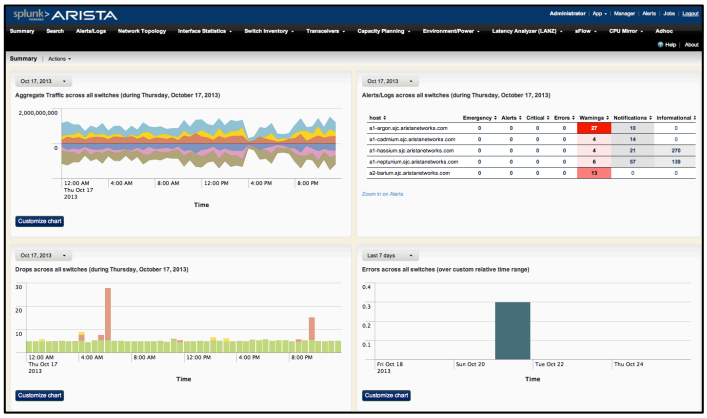


Figure 1: Arista Network Telemetry summary dashboard

Arista's Network Telemetry application for Splunk augments these with additional network telemetry data and by pushing the data into a centralized Splunk server where the Arista Network Telemetry App for Splunk provides pre-built dashboards, views, searches and add-ons for visualizing this network telemetry data. The types of data that can be pushed into Splunk include:

- Interface counters and statistics
- System logging data (syslog)
- Network topology discovered using LLDP
- Switch health and inventory data (modules and transceivers) including power consumption, optical light levels and switch capacity
- Latency Analysis data (LANZ)
- Data Analysis (DANZ) mirror-to-cpu decoded packets
- sFlow sampled packets (decoded)
- AEM events including MAC moves (L2), route updates (L3), VM vMotion events etc.

ARISTA

There are two parts to the Arista Network Telemetry Application for Splunk:

1. An Arista EOS Extension that runs on the switch. This extension provides the source data from various collectors and uses the Splunk Universal Forwarder (also running on the switch) to forward to one or more Splunk servers.

2. The Arista Network Telemetry App that runs on the Splunk server providing pre-built dashboards, views, searches and add-ons for visualizing supplied data

It is a prerequisite that Splunk is already installed and running.

INSTALLING AND CONFIGURING THE ARISTA EOS SPLUNK EXTENSION

The Arista EOS Splunk Extension is a standalone extension package (swix file) that can be loaded onto Arista switches running EOS-4.12 or later. Download the *arista-splunk-extension.swix* from the software download section of Aristanetworks.com, copy to the switch and install using the extension command:

```
switch# copy scp://<user>@<host>/<dir>/arista-splunk-extension.swix extension:
switch# extension arista-splunk-extension.swix
```

Log out and login into the switch to update the CLI with the new extension.

The Splunk Universal Forwarder RPM also needs to be installed on the switch. This can be downloaded from Splunk's website. The Arista EOS Splunk Extension provides instructions on how to download and install onto the switch if its not already installed (issue "show splunk-forwarder") or use the following commands:

```
switch# copy http://download.splunk.com/releases/5.0.3/universalforwarder/linux/
        splunkforwarder-5.0.3-163460.i386.rpm extension:

switch# extension splunkforwarder-5.0.3-163460.i386.rpm
```

Note this is the same Splunk Universal Forwarder Fedora/Red Hat x86-32 RPM binary that you would install on a Linux host or server unmodified. It can run on the control-plane of all Arista switches as-is.

Complete the installation of the extension by ensuring it is part of extensions:

```
switch# copy installed-extensions boot-extensions
```

At this point, the Arista Splunk Extension can be configured through the splunk-forwarder configuration sub-mode and defining one or more Splunk servers to forward events to and enabling:

```
switch# configure
switch(config)# splunk-forwarder
switch(config-splunk-forwarder)# splunk-server <ipaddr>
switch(config-splunk-forwarder)# no shutdown
```

By default the Arista Splunk Extension will forward switch logs in real time, interface counters and LANZ data every minute, switch health and inventory data (modules, transceivers), power consumption, optical light levels, switch capacity and network topology information every hour with a maximum data rate of 256Kbps (32KB/s or at most 2.7MB/day.)
You can verify this via "show splunk-forwarder" or "show run all section splunk":

```
switch# show run all section splunk
splunk-forwarder
   splunk-server <ipaddr> 9997
   index inventory interval 3600
```

```
   index topology interval 3600
   index interface-counters interval 60
   no index sflow
   index syslog follow-tail-only
   index lanz-data interval 60 threshold 1024 historic-data 7200
   max-data-rate 256
   no shutdown

switch# show splunk-forwarder
[…]
Forwarders Configured:
        <ipaddr>:9997

Items to index: (max-data-rate is 256 Kbps)
        Switch Inventory:         enabled (1h 0s intervals)
        Topology Information:     enabled (1h 0s intervals)
        Interface Statistics:     enabled (1m 0s intervals)
        Latency Analyzer (LANZ):  enabled (1m 0s intervals) [threshold: 1024]
        Syslog:                   enabled (Tail)
        Sflow:                    disabled
        Mirror CPU traffic:       None
        Custom Script:            None

Splunk Forwarder Status:

Operational state: running
splunkd is running (PID: 15131).

Active forwards:
        <ipaddr>:9997

switch#
```

Additional data items can also be sent to Splunk including decoded sampled data plane traffic (sFlow), decoded Mirror-to-CPU traffic as well as any other data collected within EOS, either via custom-scripts that run CLI commands or any commands from within Linux like a bash command. Some examples include:

- Collect decoded sFlow sampled traffic:
  `switch(config-splunk-forwarder)# index sflow`

- Collect DANZ mirror-to-CPU traffic from interface Ethernet10:
  `switch(config-splunk-forwarder)# index mirror-cpu interface ethernet10`

- collect L2 MAC address moves in the last minute every minute:
  ```
  switch(config-splunk-forwarder)# index custom-script source-type arista_mac_moves
     interval 60 cli show event-monitor mac match-time last-minute
  ```

- track TCP stack performance on the switch with Linux's native 'netstat' command:
  ```
  switch(config-splunk-forwarder)# index custom-script source-type arista_netstat
     interval 300 bash netstat -s
  ```

Its also possible to selectively push any data from the switch into Splunk in an adhoc or unstructured manner. e.g. to send the contents of the BGP table into Splunk as a one-off:

```
switch# show ip bgp | splunk-adhoc
```

As Splunk can index unstructured data there are no limits to what data can be sent towards Splunk. The skill is being able to formulate searches and queries in Splunk to extract data around finding whatever is being looked for. This is where the Arista Network Telemetry App that runs on the Splunk server with pre-built dashboards, views, searches and add-ons for visualizing supplied data comes into play.

ARISTA NETWORK TELEMETRY APPLICATION FOR SPLUNK

The Arista Network Telemetry Application for Splunk can be downloaded from Splunk's website. You can find it using App -> Find More Apps -> and search for Arista Networks.

Once installed, access it via App -> Arista Networks within Splunk (typically <splunkurl>/app/aristanetworks/) and a summary is presented:

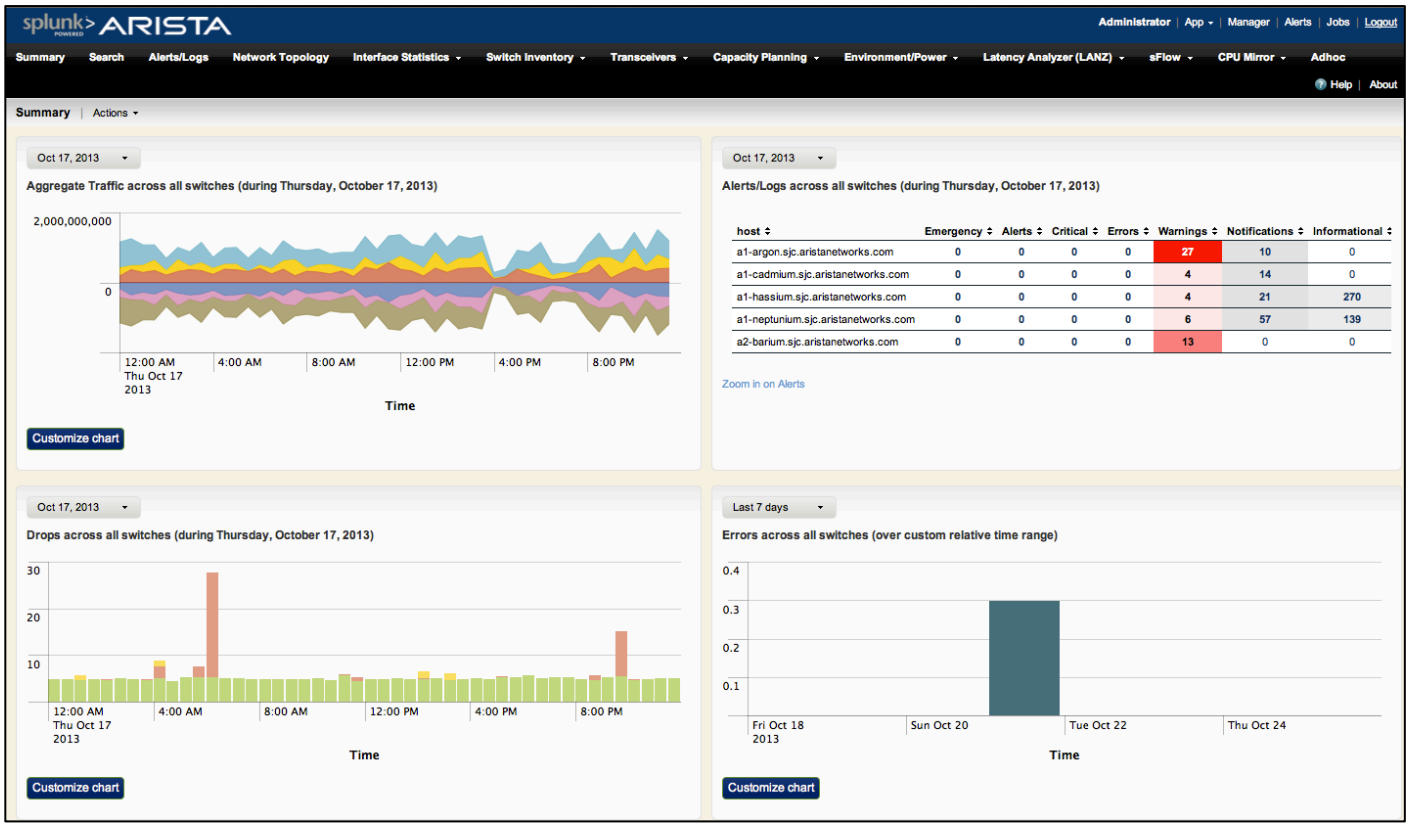


Figure 2: Arista Network Telemetry summary dashboard

The summary view displays aggregate traffic levels across all switches (top left), alarms/alerts on all switches (top right), and drops/errors across switches (bottom left/right). The time periods of each of these can be customized and one can drill down to look further into any detail by clicking on elements.

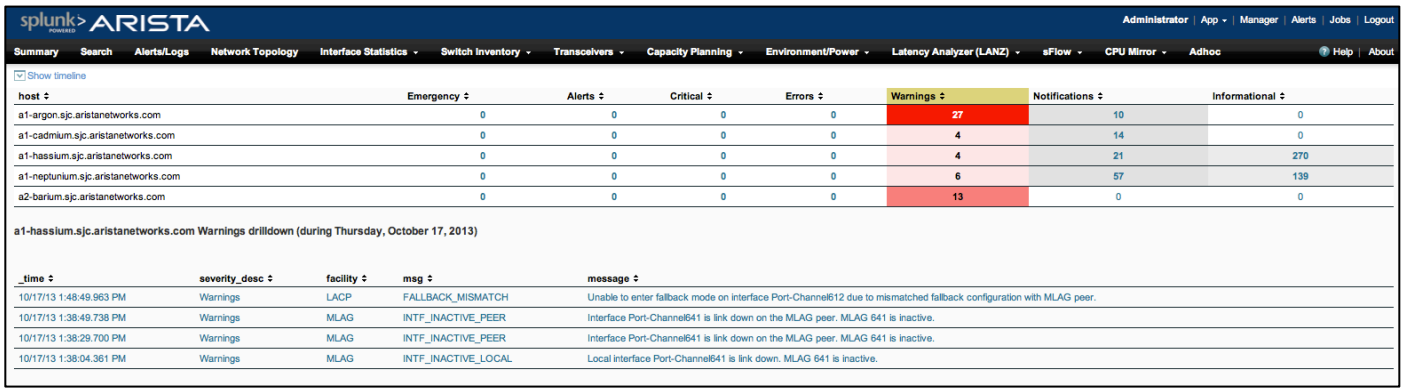


Figure 3: Drilldown to alerts/logs – showing warnings summary

Navigation bar across the top allows the user to look closer at any aspects of the data being sent to Splunk, e.g. clicking on “Network Topology” will provide a network topology diagram based on what has been discovered using LLDP:

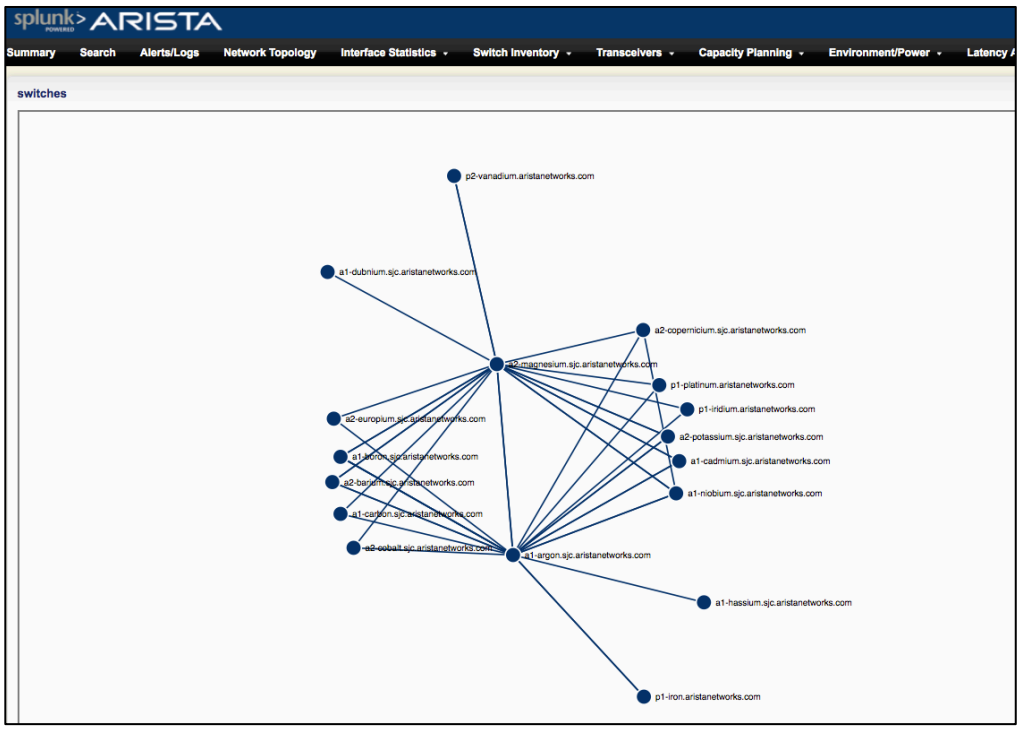


Figure 4: Network Topology diagram

Under Interface Statistics individual interface statistics (bytes, rates, packets, errors) can be graphed either by switch (Figure 5) or by individual interfaces on a switch (Figure 6).

When displaying multiple interfaces at the same time, Spark Line graphs are used to show rate changes and a traffic-light color scheme (red/orange/green) is used to denote interface traffic levels and/or any errors. One can zoom into any date/time by highlighting any part of the timeline, 8am-4pm on 17 October shown below:

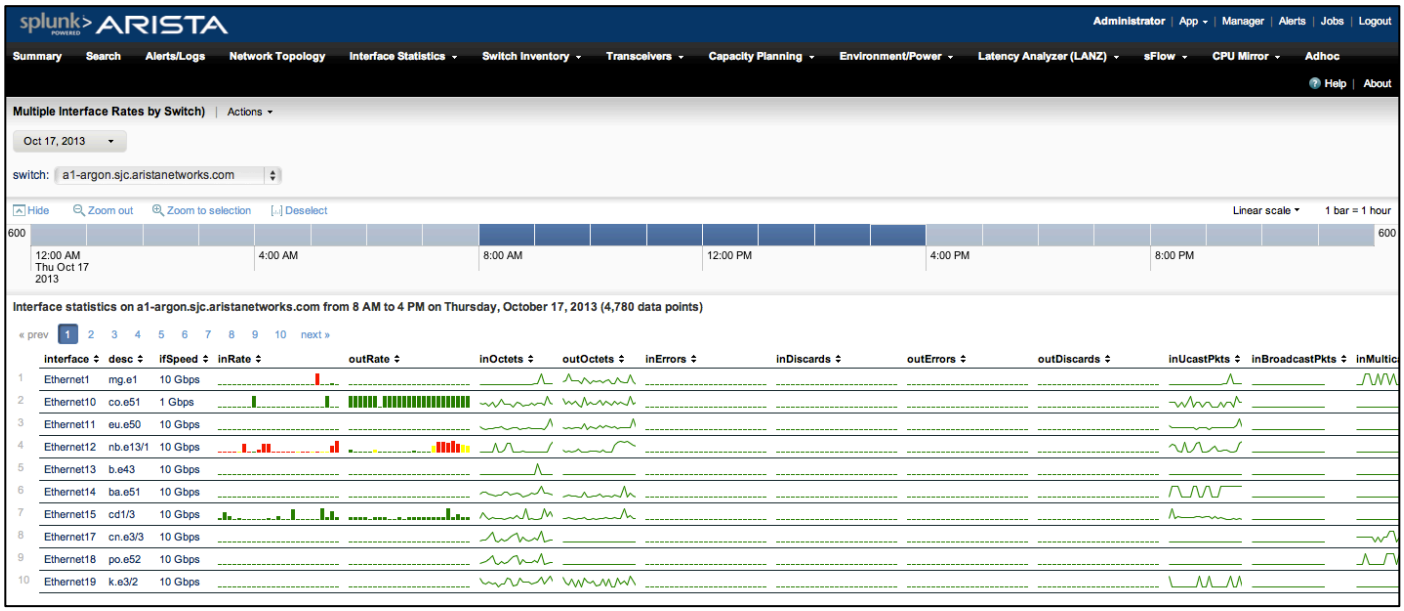


Figure 5: Multiple Interfaces rates dashboard

Since switches push information such as interface descriptions out to Splunk, interface statistics can be located based on what the switch is attached to without having to know physical interface connectivity (Figure 6). Also shown in single interface rates are drops/errors highlighted using bar graphs alongside interface rates:

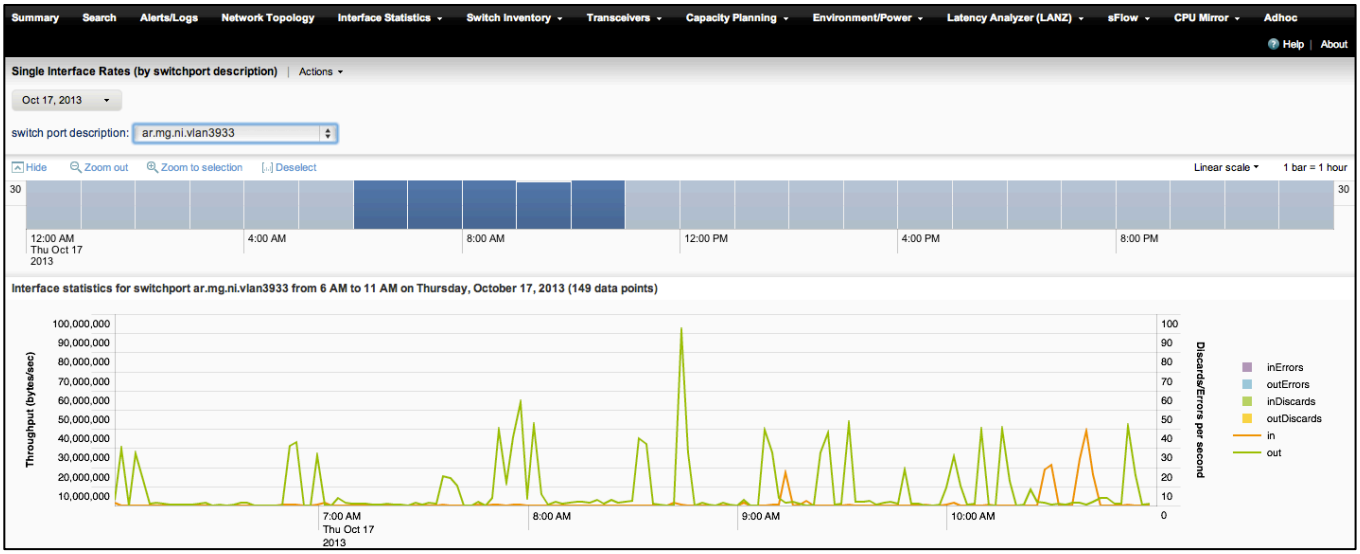
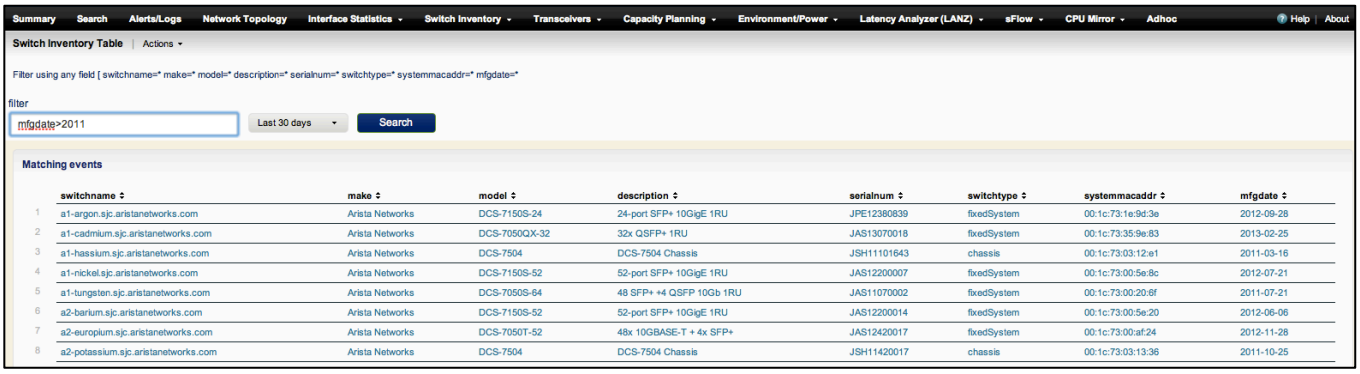


Figure 6: Single Interfaces rates using switch port description

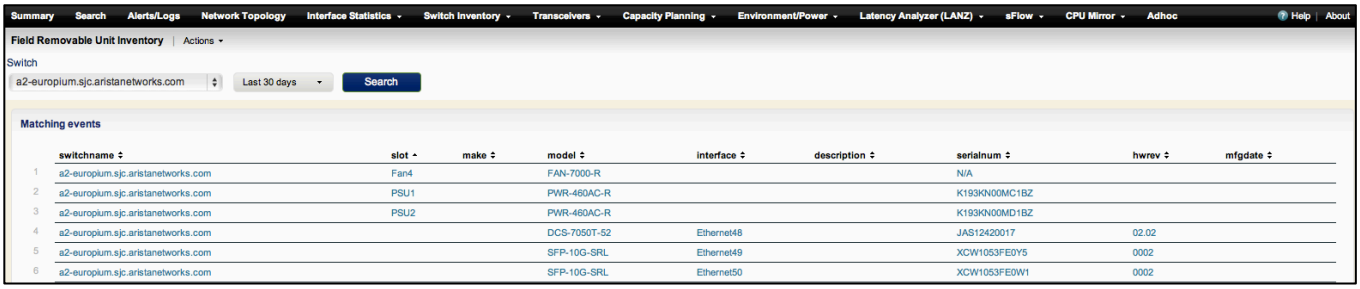
Dashboard views for Switch Inventory show a summary of what devices are known and can be filtered based on any fields. For example below, we are listing all switches with a manufacturing date of 2011 of later:



	switchname	make	model	description	serialnum	switchtype	systemmacaddr	mfgdate
1	a1-argon.sjc.aristanetworks.com	Arista Networks	DCS-7150S-24	24-port SFP+ 10GigE 1RU	JPE12380839	fixedSystem	00:1c:73:1e:9d:3e	2012-09-28
2	a1-cadmium.sjc.aristanetworks.com	Arista Networks	DCS-7050QX-32	32x QSFP+ 1RU	JAS13070018	fixedSystem	00:1c:73:35:9e:83	2013-02-25
3	a1-hassium.sjc.aristanetworks.com	Arista Networks	DCS-7504	DCS-7504 Chassis	JSH11101643	chassis	00:1c:73:03:12:e1	2011-03-16
4	a1-nickel.sjc.aristanetworks.com	Arista Networks	DCS-7150S-52	52-port SFP+ 10GigE 1RU	JAS12200007	fixedSystem	00:1c:73:00:5e:8c	2012-07-21
5	a1-tungsten.sjc.aristanetworks.com	Arista Networks	DCS-7050S-64	48 SFP+ +4 QSFP 10Gb 1RU	JAS11070002	fixedSystem	00:1c:73:00:20:6f	2011-07-21
6	a2-barium.sjc.aristanetworks.com	Arista Networks	DCS-7150S-52	52-port SFP+ 10GigE 1RU	JAS12200014	fixedSystem	00:1c:73:00:5e:20	2012-06-06
7	a2-europium.sjc.aristanetworks.com	Arista Networks	DCS-7050T-52	48x 10GBASE-T + 4x SFP+	JAS12420017	fixedSystem	00:1c:73:00:af:24	2012-11-28
8	a2-potassium.sjc.aristanetworks.com	Arista Networks	DCS-7504	DCS-7504 Chassis	JSH11420017	chassis	00:1c:73:03:13:36	2011-10-25

Figure 7: Switch Inventory Table dashboard

It's possible to drill down further into what field removable units (FRUs) exist in a given switch and use this to track transceivers, power supplies, fans etc., being added/removed or reused across different switches over time:



	switchname	slot	make	model	interface	description	serialnum	hwrev	mfgdate
1	a2-europium.sjc.aristanetworks.com	Fan4		FAN-7000-R			N/A		
2	a2-europium.sjc.aristanetworks.com	PSU1		PWR-460AC-R			K193KN00MC1BZ		
3	a2-europium.sjc.aristanetworks.com	PSU2		PWR-460AC-R			K193KN00MD1BZ		
4	a2-europium.sjc.aristanetworks.com			DCS-7050T-52	Ethernet48		JAS12420017	02.02	
5	a2-europium.sjc.aristanetworks.com			SFP-10G-SRL	Ethernet49		XCW1053FE0Y5	0002	
6	a2-europium.sjc.aristanetworks.com			SFP-10G-SRL	Ethernet50		XCW1053FE0W1	0002	

Figure 8: Field Removable Unit Inventory dashboard

Most tables can also be displayed as charts too, for example under Transceivers you can get a summary view of what transceivers are deployed across all switches:

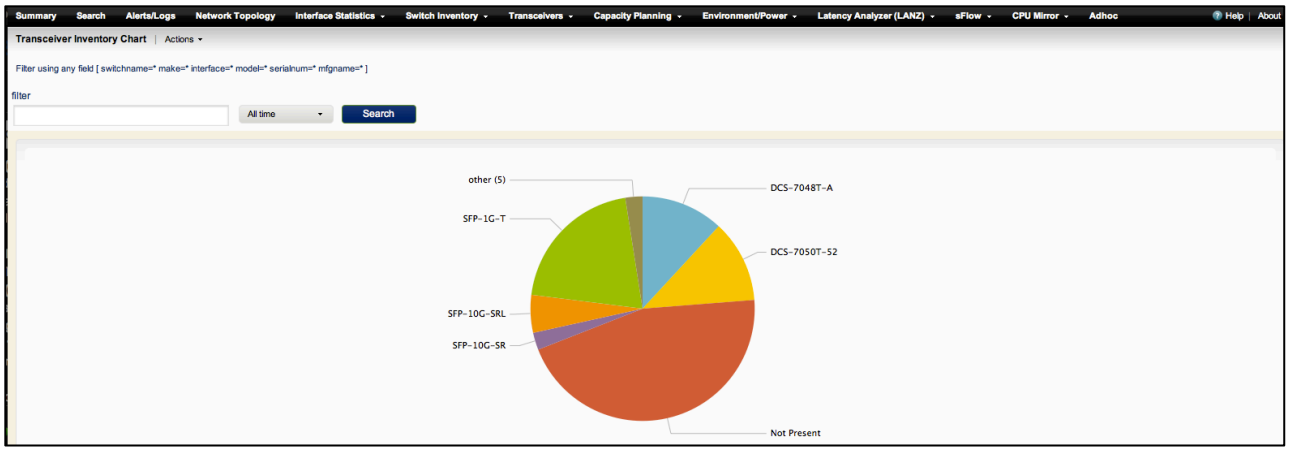


Figure 9: Transceiver Inventory Chart dashboard

Capacity Planning information like the number of used/free ports and switch control-plane capacity (CPU and memory utilization) are also recorded and available as a dashboard allowing for historical reporting and comparison. Simple traffic-light reporting (green/yellow/red) is also provided in this view providing easy interpretation of whether there are any capacity problems that need further attention:

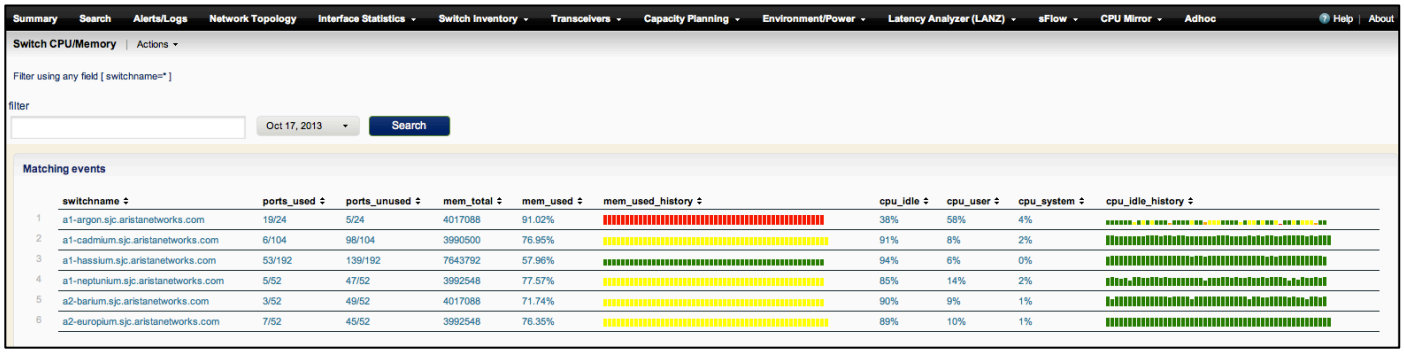


Figure 10: Switch CPU/memory/ports used dashboard

Capacity planning information about the data-plane hardware forwarding tables (MAC tables, LPM and Host Routes) is also pushed into Splunk and is available on a dashboard, again with simple traffic-light reporting (green/yellow/red) providing for easy interpretation, historical usage and trend over time:

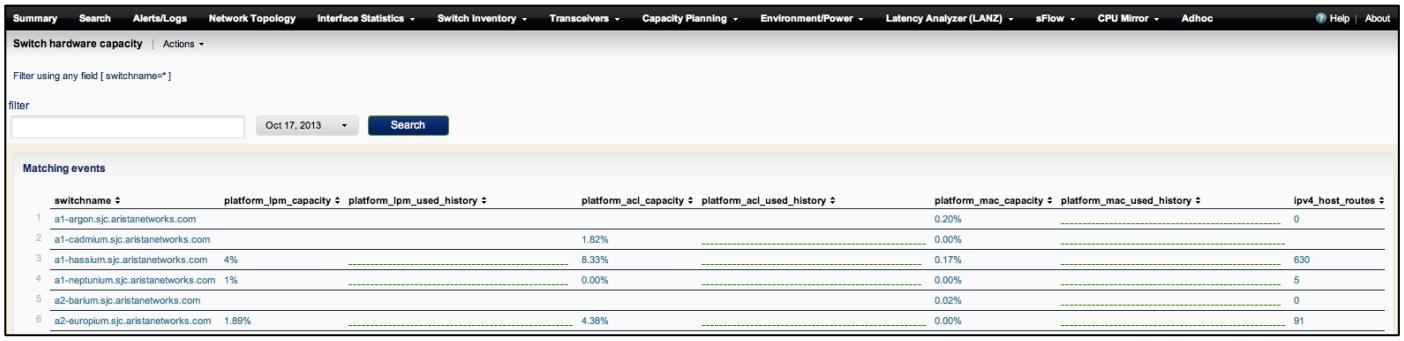


Figure 11: Switch data-plane capacity planning dashboard

Switch Environmental/Power statistics are also available, pushed into Splunk and with dashboard views that provide this data across switches:

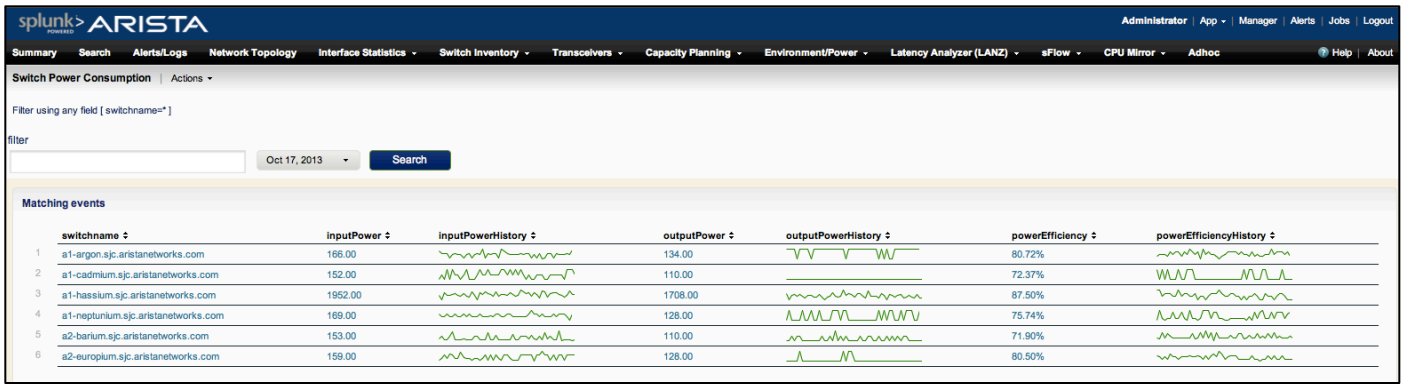


Figure 12: Switch Power Consumption dashboard

Some of the best and most useful network telemetry data available is provided by Latency Analyzer (LANZ) on Arista switches. LANZ provides visibility into congestion events and microbursts. LANZ can provide details on when congestion happened, for how long, the queue depth (bytes), and maximum latency. There are two pre-built dashboards that provide this data, allowing drill-down on delay (usec) and maximum queue depth (bytes).

In Figure 13 below Splunk is used to look into a congestion event at 8:06am on the switch “nickel”, interface ethernet38 that recorded 152 LANZ events during that minute.

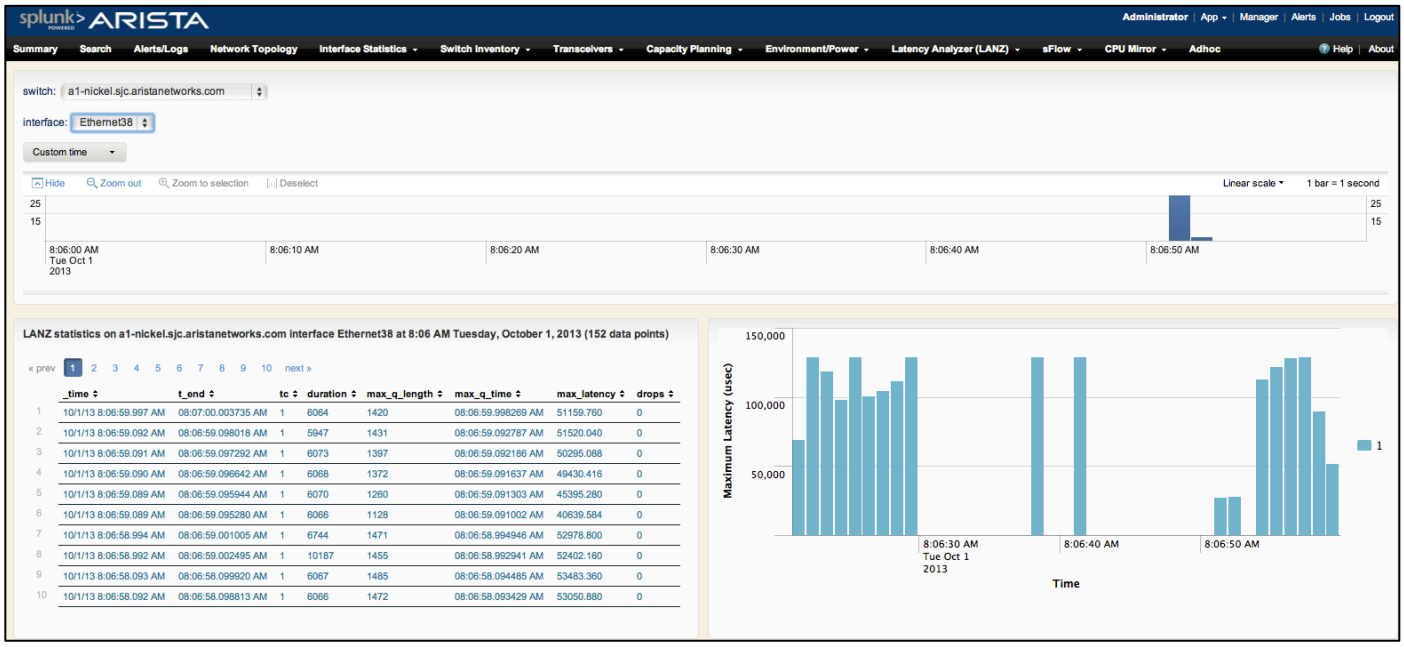


Figure 13: LANZ Latency dashboard

In Figure 14 below one is exploring a congestion/performance issue on 14 October. Using the LANZ Maximum Queue Size dashboard its clear that there was a large congestion event around midday on that day. Given the visualization one could then dive further into that time to see what was going on.

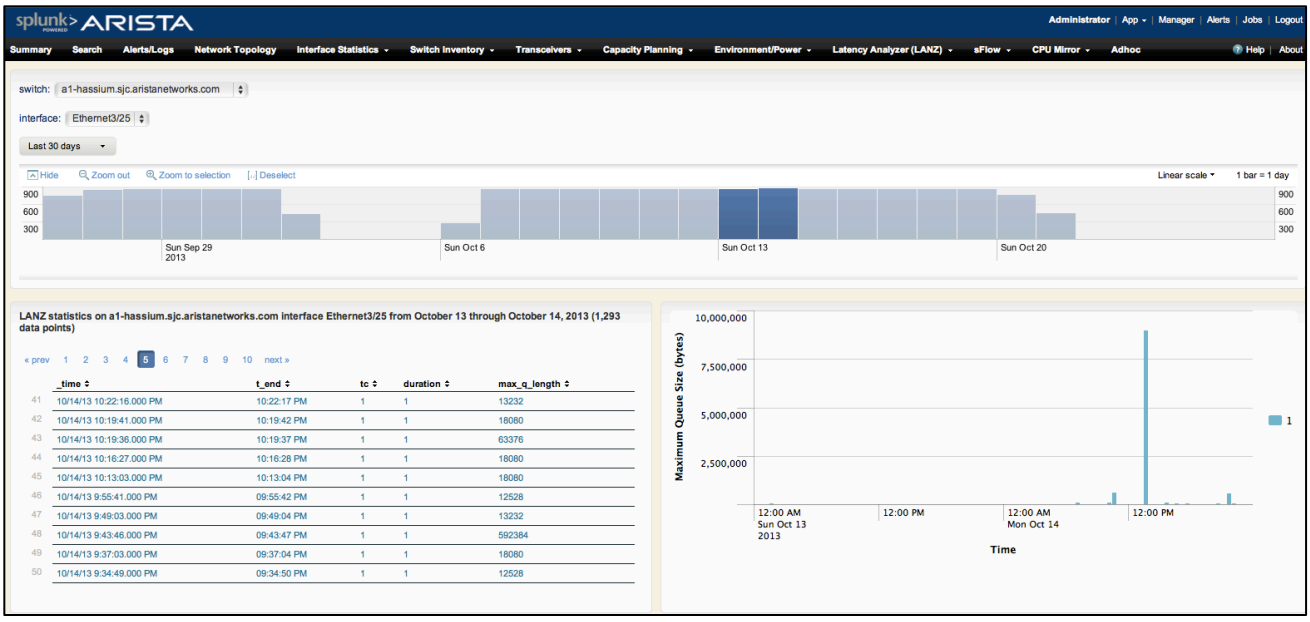


Figure 14: LANZ Maximum Queue size dashboard

Enabling sFlow on Arista switches provides for data-plane traffic sampling where 1 in N packets is sampled and sent to a sFlow collector. This can be augmented by enabling sFlow collection within the Arista EOS Splunk Extension where sFlow sampled packets will be decoded and pushed to Splunk.

A nice aspect of sFlow is that it samples the first 128 bytes of every packet which means that we can conduct some protocol analytics based on things other than Layer 2 to Layer 4 headers, i.e. we can also see protocols and decode those. Figure 15 below shows an example of conducting a search in Splunk to show frames in VLANs numbered over 1,000 and then showing the top 10 traffic sources at layer 2 (eth_src). The search query in Splunk is simply 'sourcetype=arista_switch_sflow sflow_245_vlan_in>1000':

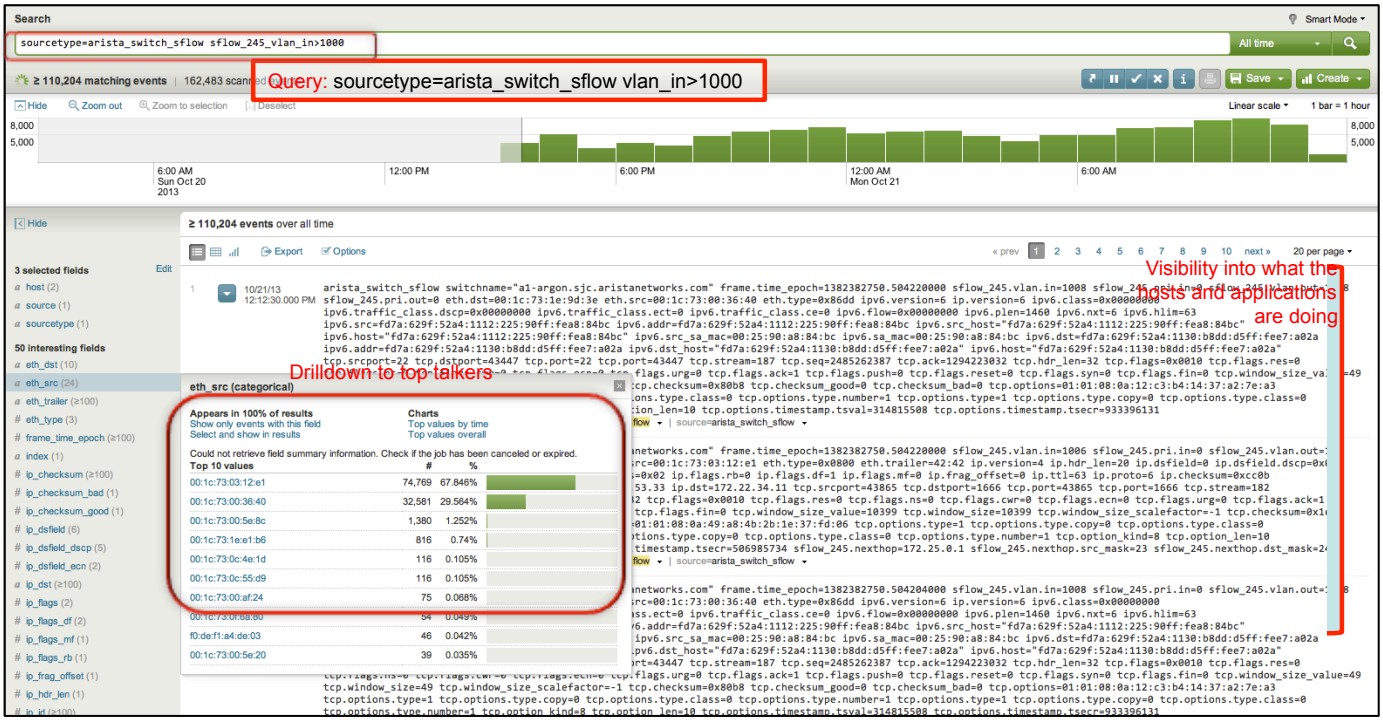


Figure 15: sFlow sampled data decoded and pushed to Splunk

Showing the power of ad-hoc searches and Splunk's powerful visualization capabilities one could change this search to be something like "show me where all HTTP traffic is going". The search in Splunk would be as simple as 'sourcetype=arista_switch_sflow http | geoip ip_dst' which will show any sFlow sampled traffic from Arista switches that contain HTTP fields, and conduct a geo-location lookup on the destination IP address. This can then be plotted on a map as shown below showing the most common locations where HTTP requests are going to:

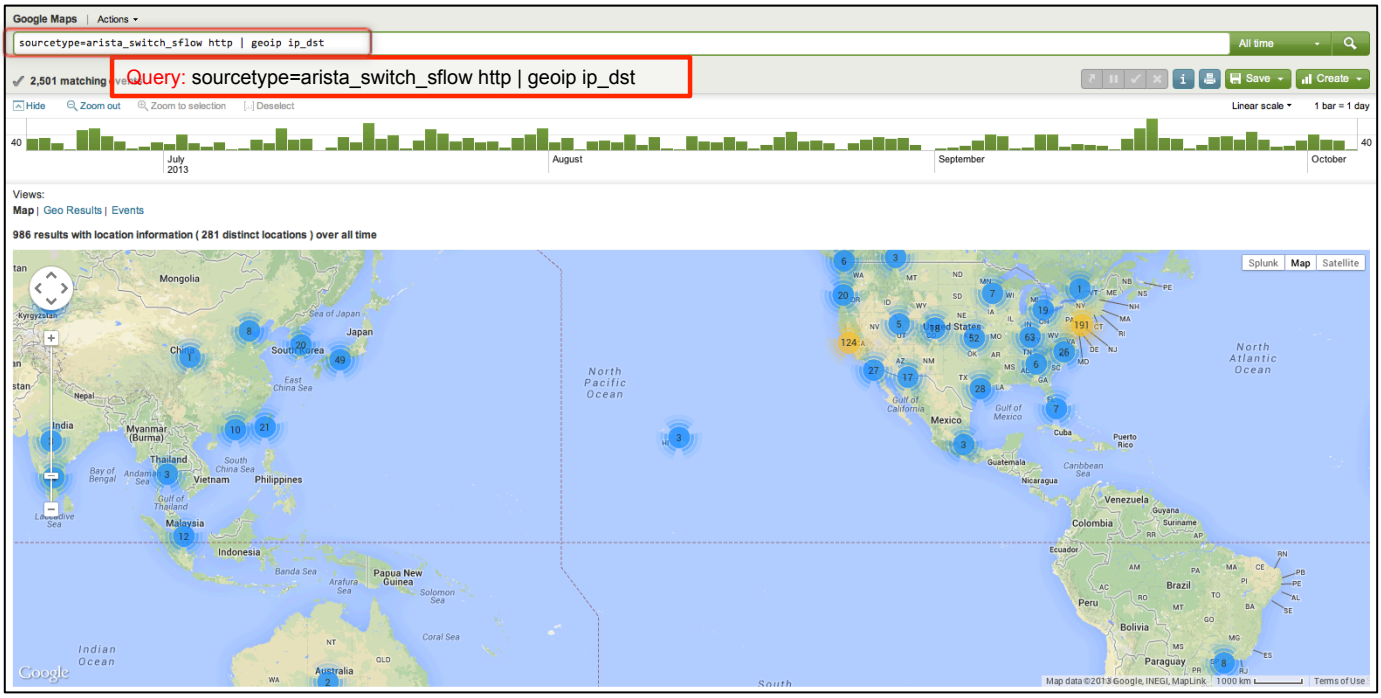


Figure 16: sFlow sampled HTTP requests decoded with geolocation lookup plotted on Google Maps

SUMMARY

There are many more pre-built dashboards and views available in addition to those listed here. The real power of Arista Network Telemetry data being pushed into Splunk is in combining multiple input data sources with network telemetry data and using that for analytics, capacity planning and troubleshooting.

Arista Network Telemetry including the Network Tracers provides real-world solutions to the real-world problems of Data Center network visibility, monitoring and troubleshooting. Arista Network Telemetry enables tight linkages between the physical and virtual infrastructure and applications running within the infrastructure resulting in considerable savings in operational expenditures.

ARISTA

Santa Clara—Corporate Headquarters
5453 Great America Parkway
Santa Clara, CA 95054
Tel: 408-547-5500
www.aristanetworks.com

San Francisco—R&D and Sales Office
1390 Market Street Suite 800
San Francisco, CA 94102

India—R&D Office
Eastland Citadel
102, 2nd Floor, Hosur Road
Madiwala Check Post
Bangalore - 560 095

Vancouver—R&D Office
Suite 350, 3605 Gilmore Way
Burnaby, British Columbia
Canada V5G 4X5

Ireland—International Headquarters
Hartnett Enterprise Acceleration Centre
Moylish Park
Limerick, Ireland

Singapore—APAC Administrative Office
9 Temasek Boulevard
#29-01, Suntec Tower Two
Singapore 038989

ABOUT ARISTA NETWORKS

Arista Networks was founded to deliver software-defined cloud networking solutions for large data center and computing environments. The award-winning Arista 10 Gigabit Ethernet switches redefine scalability, robustness, and price-performance. More than one million cloud networking ports are deployed worldwide. The core of the Arista platform is the Extensible Operating System (EOS®), the world's most advanced network operating system. Arista Networks products are available worldwide through distribution partners, systems integrators, and resellers.

Additional information and resources can be found at www.aristanetworks.com.