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<sup>™</sup>), a groundbreaking 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 networkwide 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



Figure 1: Arista Network Telemetry summary dashboard

Advanced Event Monitor (AEM) that provides an onswitch record of data-plane forwarding changes.

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.



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.

splunk>ARISTA								Admini	istrator   App -   Mai	ager   Alerts	Jobs   Logout		
Summary Search Alerts/Logs Netw	vork Topology	Interface Statistics	- Switch Inventory -	Transceivers -	Capacity Planning 👻	Environment/Power -	Latency Analyzer (LANZ) 👻	sFlow - CPU Mirror	- Adhoc		Help   About		
Show timeline													
host ¢			Emergency \$	Alerts \$	Critical \$	Errors ‡	Warnings ¢	Notifications \$	Informati	onal ¢			
a1-argon.sjc.aristanetworks.com			0	0	0	0	27	10		0			
a1-cadmium.sjc.aristanetworks.com			0	0	0	0	4	14		0			
a1-hassium.sjc.aristanetworks.com			0	0	0	0	4	21		270			
a1-neptunium.sjc.aristanetworks.com			0	0	0	0	6	57		139			
a2-barium.sjc.aristanetworks.com			0	0	0	0	13	0		0			
a1-hassium.sjc.aristanetworks.com Warnin	ngs drilldown (dur	ing Thursday, Oct	ober 17, 2013)										
_time \$ severity	y_desc ¢	facility \$ r	nsg ¢	message \$	;								
10/17/13 1:48:49.963 PM Warning	gs	LACP F	FALLBACK_MISMATCH	Unable to e	nter fallback mode on interfa	ace Port-Channel612 due to m	ismatched fallback configuration	with MLAG peer.					
10/17/13 1:38:49.738 PM Warning	gs	MLAG I	NTF_INACTIVE_PEER	Interface Po	0 0 13 0 0 ge 2 to enter falback mode on interface Port-Channel612 due to mismatched falback configuration with MLAG peer. e Port-Channel641 is link down on the MLAG peer. MLAG 641 is inactive.								
10/17/13 1:38:29.700 PM Warning	gs	MLAG I	NTF_INACTIVE_PEER	Interface Po	ort-Channel641 is link down	on the MLAG peer. MLAG 64	l is inactive.						
10/17/13 1:38:04.361 PM Warning	gs	MLAG I	NTF_INACTIVE_LOCAL	Local interfa	ace Port-Channel641 is link	down. MLAG 641 is inactive.							



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:

sp	lunk >	AR	ISTA	A.							Admi	nistrator   App -	Manager   A	lerts   Jobs	Logout
Sumn	nary S	Search .	Alerts/Logs	Network Topology	Interface Statistics 👻	Switch Invent	ory - Trans	ceivers - Capacit	y Planning 👻	Environment/Power -	Latency Analyzer (LANZ) -	sFlow -	CPU Mirror 👻	Adhoc	
														🕐 Help	About
Multi	ple Interf	ace Rates	by Switch)	Actions -											
Oct	17, 2013	•													
switcl	h: a1-ai	rgon.sjc.ari	stanetworks.o	com \$											
in Hic	le Q	Zoom out	€ Zoom to s	election [a] Deselect									Linear scal	e∙ 1 bar	= 1 hour
600															600
1 T 2	2:00 AM hu Oct 17 013			4:00 AM		8:00 AM		12:00 PM	1	4:00 PN	1	8:00 PM			
Interi « pre	ace stati	stics on a	1-argon.sjc.a 5 6 7	ristanetworks.com fro 8 9 10 next »	om 8 AM to 4 PM on Thu	rsday, October 1	17, 2013 (4,780	data points)							
	interface	¢ desc ¢	ifSpeed \$	inRate \$	outRate \$	inOctets \$	outOctets \$	inErrors \$	inDiscard	s ¢ outErrors ¢	outDiscards \$	inUcast	Pkts ‡ inBroa	dcastPkts ‡	inMultic
1	Ethernet1	mg.e1	10 Gbps	<b>-</b>			h					A			JWW
3	Ethernet1	0 co.e51	1 Gbps									~~~~	<u></u>		
4	Ethernet1	2 nh.e13/	1 10 Gbps									~~~			
5	Ethernet1	3 b.e43	10 Gbps		•	<u></u>							~		
6	Ethernet1	4 ba.e51	10 Gbps				m					r.v	v		
7	Ethernet1	5 cd1/3	10 Gbps	المستحدث المستحد			h						····-		
8	Ethernet1	7 cn.e3/3	10 Gbps			- mm									-~~~
9	Ethernet1	8 po.e52	10 Gbps			- mm									
10	Ethernet1	9 k.e3/2	10 Gbps			- ~~~~	www					\A	<u> </u>		

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:

s	ummary	Search Alerts/Logs Network Topology Interfa	ce Statistics - Switch In	ventory - Transceivers -	Capacity Planning - Environment/Power -	Latency Analyzer (LA	NZ) - sFlow - C	PU Mirror - Adhoc	🕐 Help   About
s	witch In	ventory Table   Actions -							
F	ilter usinç	any field [ switchname=* make=* model=* description=* serialnum=	* switchtype=* systemmacaddr:	=* mfgdate=*					
filt	er								
Γ	mfgdate	>2011 Last 30 days •	Search						
	Matchi	ng events							
		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:

Summa	ry Search	Alerts/Logs Ne	twork Topology	Interface Statistics 👻	Switch Inventory -	Transcelvers -	Capacity Planning 👻	Environment/Power -	Latency Analyzer (LANZ) -	sFlow - CPU Mirror	- Adhoc	🕐 Help   Abou
Field R	emovable Unit	Inventory   Actions	•									
Switch												
a2-eu	opium.sjc.arista	anetworks.com	Last 30 days	- Search								
Matc	ning events											
	switchname	•		slot	make \$	model \$	interfa	e ≑ desc	ription \$ serialn	um ÷	hwrev ÷	mfodate ≑
1	a2-europium.	jc.aristanetworks.com		Fan4		FAN-7000-R			N/A			
2	a2-europium.s	jc.aristanetworks.com		PSU1		PWR-460AC-R			K193K	N00MC1BZ		
3	a2-europium.s	ijc.aristanetworks.com		PSU2		PWR-460AC-R			K193K	N00MD1BZ		
4	a2-europium.	jc.aristanetworks.com				DCS-7050T-52	Etherne	t48	JAS12	420017	02.02	
5	a2-europium.	jc.aristanetworks.com				SFP-10G-SRL	Etherne	t49	XCW10	053FE0Y5	0002	
6	a2-europium.s	jc.aristanetworks.com				SFP-10G-SRL	Etherne	t50	XCW10	053FE0W1	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:

Summar	/ Search	Alerts/Logs	Network Topology	Interface Statistics 👻	Switch Inventory	- Transcelv	ers - Capacity Planning -	Environment/Power -	Latency A	nalyzer (LANZ)	sFlow -	CPU Mirror +	Adhoc 🕐 Help   Abou
Switch 0	PU/Memory	Actions -											
Filter usir	g any field [ swite	chname=* ]											
filter													
			Oct 17, 20	013 - Search									
Match	ing events												
	switchname :	•	ports_use	d ¢ ports_unused ¢	mem_total ‡	mem_used ¢	mem_used_history \$		cpu_idle ‡	cpu_user ¢	cpu_system ¢	cpu_idle_histor	ry ÷
1	a1-argon.sjc.a	ristanetworks.con	n 19/24	5/24	4017088	91.02%			38%	58%	4%		
2	a1-cadmium.sj	c.aristanetworks.	com 6/104	98/104	3990500	76.95%			91%	8%	2%	llesseslitette	
3	a1-hassium.sj	c.aristanetworks.c	om 53/192	139/192	7643792	57.96%			94%	6%	0%		
4	a1-neptunium.	sjc.aristanetworks	.com 5/52	47/52	3992548	77.57%			85%	14%	2%	dina dini bin	
5	a2-barium.sjc.	aristanetworks.co	m 3/52	49/52	4017088	71.74%			90%	9%	1%		
6	a2-europium.s	jc.aristanetworks.	com 7/52	45/52	3992548	76.35%			89%	10%	1%		

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:

Sumr	nary	Search Alerts/Logs	Network Topology	Interface Statistics +	Switch Inventory -	Transceivers -	Capacity Planning 👻	Environment/Power -	Latency Analyzer (LANZ) 👻	sFlow -	CPU Mirror +	Adhoc	Relp	p   About
Swite	h har	dware capacity   Actions -												
Filter	using a	ny field [ switchname=* ]												
filter														
			Oct 17, 20	013 - Search										
Ma	tching	events												
	sw	itchname \$	platform_lpm_cap	acity \$ platform_lpm_us	ed_history ≎	platform_a	cl_capacity \$ platform_	acl_used_history \$	platform_mac_cap	acity \$ platfo	orm_mac_used_hi	istory ¢	ipv4_host_r	routes ¢
	a1-	argon.sjc.aristanetworks.com							0.20%				0	
	<sup>2</sup> a1-	cadmium.sjc.aristanetworks.cor	n			1.82%			0.00%					
	3 a1-	hassium.sjc.aristanetworks.com	4%			8.33%			0.17%				630	
4	4 a1-	neptunium.sjc.aristanetworks.co	m 1%			0.00%			0.00%				5	
1	5 a2-	barium.sjc.aristanetworks.com							0.02%				0	
	a2-	europium.sjc.aristanetworks.com	n 1.89%			4.38%			0.00%				91	

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:

splu	nk>ARISTA							Administrator   App -   Manager   Alerts	Jobs   Logout
Summar	y Search Alerts/Logs N	letwork Topology	Interface Statistics 👻	Switch Inventory - Transceivers -	Capacity Planning 👻	Environment/Power - Latency Ana	iyzer (LANZ) 👻 sFlow 👻 Cl	PU Mirror - Adhoc	Help   About
Switch I	Power Consumption   Actions -								
Filter usir	ig any field [ switchname=* ]								
filter									
		Oct 17, 20	013 - Search						
	· · · · · · · · · ·								
Match	ing events								
	switchname \$		inputPower \$	inputPowerHistory \$	outputPower \$	outputPowerHistory \$	powerEfficiency \$	powerEfficiencyHistory \$	
1	a1-argon.sjc.aristanetworks.com		166.00	~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~	134.00	~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~	80.72%	~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~	
2	a1-cadmium.sjc.aristanetworks.com	n	152.00	MVV-VVV-V	110.00		72.37%	WVVVV_V	
3	a1-hassium.sjc.aristanetworks.com	1	1952.00	~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~	1708.00	~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~	87.50%	m	
4	a1-neptunium.sjc.aristanetworks.co	m	169.00	~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~	128.00		75.74%	~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~	
5	a2-barium.sjc.aristanetworks.com		153.00	Markan Marka	110.00	~_~^~~~	71.90%	~	
6	a2-europium.sjc.aristanetworks.com	n	159.00	~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~	128.00	_//	80.50%	www	

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.

splu		TA							Ad	ministrator   App -	Manager   Ak	rts   Jobs	Logo
ummary	Search Alerts/L	ogs Network Topology	Interface Statistics 👻	Switch Inventory	Transceivers +	Capacity Planning 👻	Environment/Pov	ver - Latency Analyzer (LANZ) -	sFlow - CPU M	irror - Adhoc		Help	Abou
switch: interfac	a1-hassium.sjc.arista e: Ethernet3/25 \$	networks.com \$											
	te 🖸 Zoom out 🕮	Zoom to selection [] Des	alact								Linear ecole •	1 bar =	1 day
900 600 300		2001 to seector pij best									Lifeal scale ·	i bai -	900 600 300
		Sun Sep 29		Sun Oct 6			Sun Oct 13		Sun Oct 20				
« prev	1 2 3 4 5	6 7 8 9 10 nex	t »			ze (bytes)	7,500,000						
41	_time =	t_end	17 tc 7	duration =	max_q_lengtn =	e Si							
42	10/14/13 10:22:10:000 PI	10.22	42 PM 1	1	19090	nen	5,000,000						
43	10/14/13 10:19:41:000 PI	A 10.15	92 PM 1	1	60076	Ø							- 1
44	10/14/13 10:18:38.000 PI	A 10:18	-28 DM 1	1	19090	Ē							
45	10/14/13 10:13:03 000 PI	4 10:10	-04 PM 1	1	19090		2,500,000						
46	10/14/13 9:55:41 000 PM	09:55	:42 PM 1	1	12528								
47	10/14/13 9:49:03:000 PM	09:49	04 PM 1	1	13232		12:00	AM 12:00 PM	12:00 AM	12:	00 PM		
48	10/14/13 9:43:46.000 PM	09:43	:47 PM 1	1	592384		Sun Oc 2013	t 13	Mon Oct 14				
49	10/14/13 9:37:03.000 PM	09:37	:04 PM 1	1	18080				Time				
50	10/14/13 9:34:49.000 PM	09:34	:50 PM 1	1	12528								

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 '<u>sourcetype=arista\_switch\_sflow http | geoip ip\_dst</u>' 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.



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

#### **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.

Ireland-International Headquarters

Moylish Park Limerick, Ireland

9 Temasek Boulevard

Singapore 038989

#29-01, Suntec Tower Two

Hartnett Enterprise Acceleration Centre

Singapore-APAC Administrative Office

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

Copyright © 2013 Arista Networks, Inc. All rights reserved. CloudVision, Extensible Operating System, and EOS are registered trademarks and Arista Networks is a trademark of Arista Networks, Inc. All other company names are trademarks of their respective holders. Information in this document is subject to change without notice. Certain features may not yet be available. Arista Networks, Inc. assumes no responsibility for any errors that may appear in this document. 11/13