

Internet Traffic Database

John Haverlack

IT Manager, School of Fisheries and Ocean
Science, University of Alaska Fairbanks

jehaverlack@alaska.edu

RVTEC 2015-11-04



R/V Sikuliaq

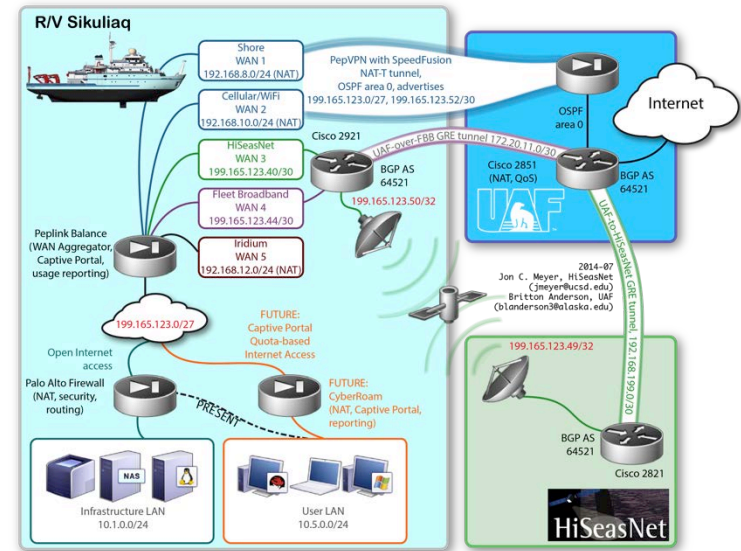
School of Fisheries
and Ocean Sciences

<https://www.sikuliaq.alaska.edu>



The Problem

- How much Internet capacity do we have?
- What is using our Internet connection?
- Are we using the capacity that we have efficiently?



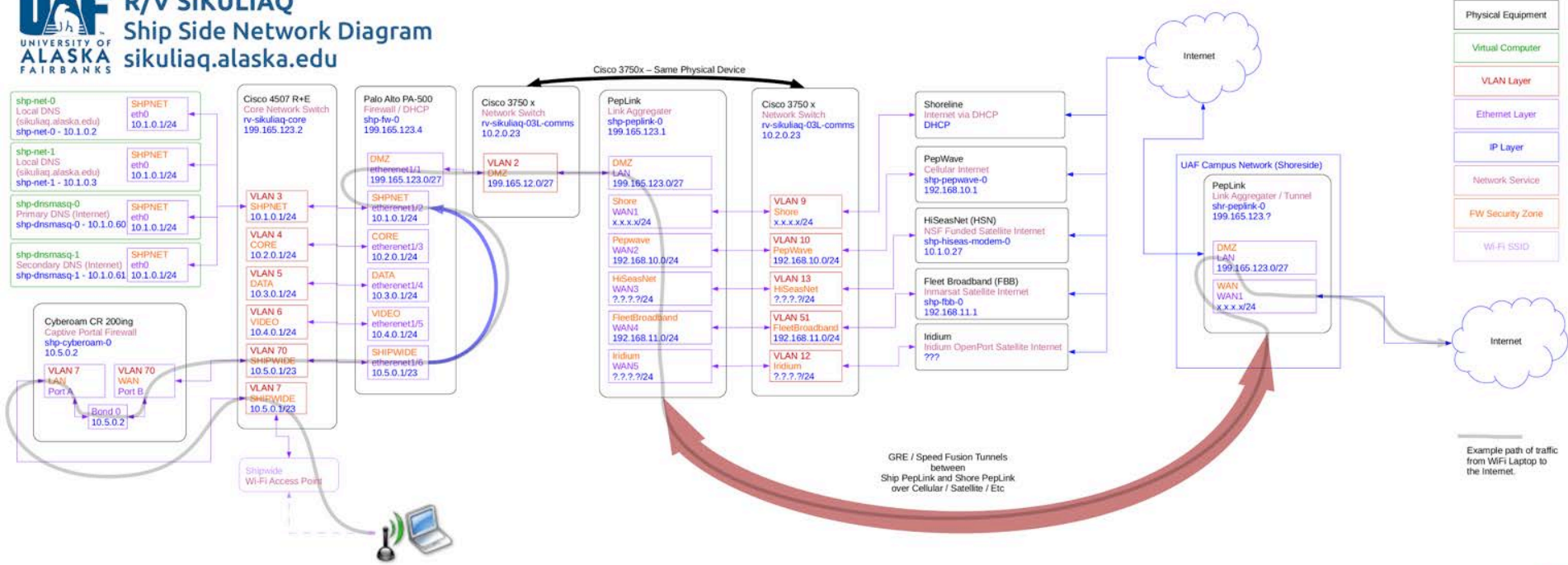
Relevant to Captive Portal

- How much Internet have I used and how much do I have left?
- Am I being a responsible user?



Is there a way to measure Internet Usage?

UAF UNIVERSITY OF ALASKA FAIRBANKS
R/V SIKULIAQ
 Ship Side Network Diagram
 sikuliaq.alaska.edu



2015-03-06
 John Haverlax
 (jehaverlax@alaska.edu)



UAF UNIVERSITY OF ALASKA FAIRBANKS
R/V Sikuliaq
 School of Fisheries
 and Ocean Sciences

<https://www.sikuliaq.alaska.edu>



Network Bastion Point Devices

Where is the best place to capture network traffic data?

- Cisco Switches (SNMP)
- Cisco Routers (SNMP)
- PaloAlto Firewall (XML API)
- Cyberoam Captive Portal (No API)
- PepLink Connection Agregator (SNMP)



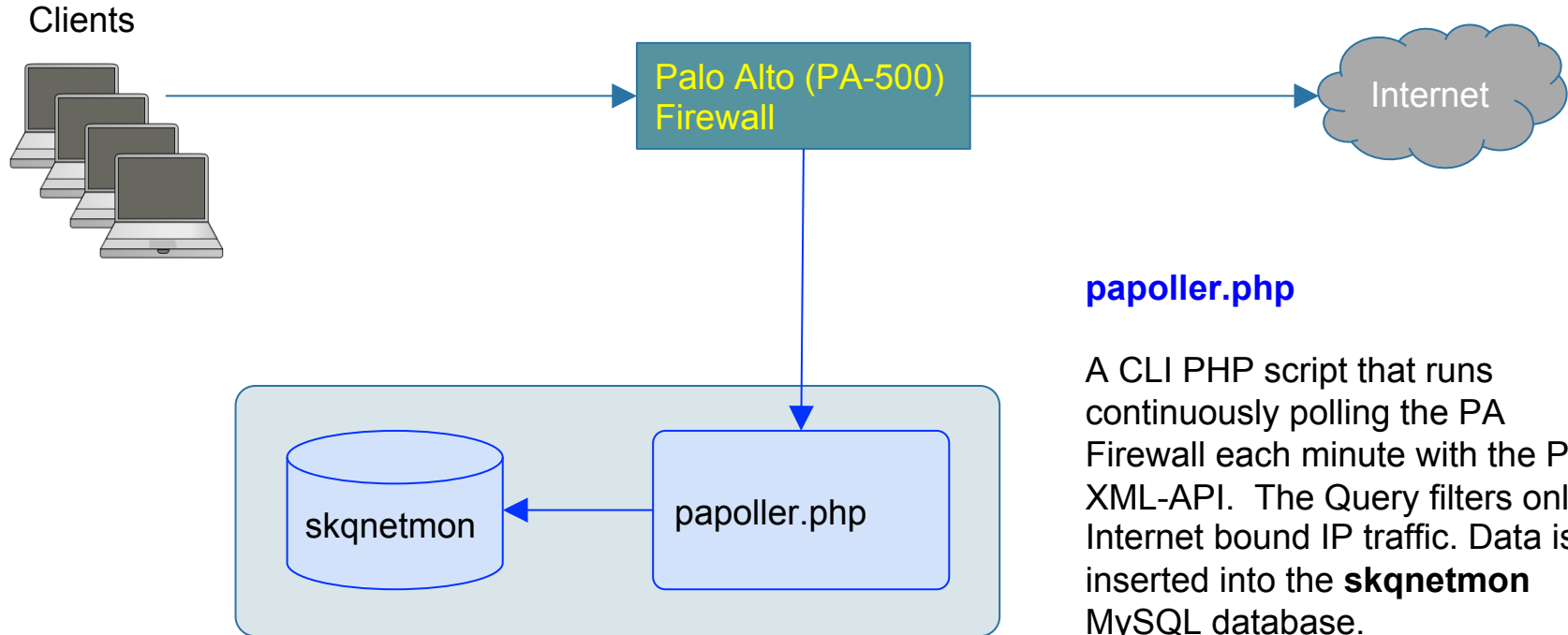
Network Bastion Point Devices

The best place is the **only place** we can get the data in which we are interested.

- Cisco Switches (SNMP)
- Cisco Routers (SNMP)
- PaloAlto Firewall (XML API)
- Cyberoam Captive Portal (No API)
- PepLink Connection Agregator (SNMP)



The Solution



papoller.php

A CLI PHP script that runs continuously polling the PA Firewall each minute with the PA XML-API. The Query filters only Internet bound IP traffic. Data is inserted into the **skqnetmon** MySQL database.



The skqnetmon Database

1,335,912 Internet Traffic Records in the last week, limit to 10 to get a sample of data.

```
mysql> select count(*) from log_pa_internet_traffic_lweek;
```

```
count(*)
1335912
```

1 row in set (0.00 sec)

```
mysql> select * from log_pa_internet_traffic_lweek LIMIT 10;
```

litid	created	YYYY	MM	DD	hh	min	ss	sessionid	start	elapsed	src	src_fqdn	dst	dst_fqdn	proto	dport	bytes_sent	bytes_received	pkts_sent	pkts_received
1	2015-09-30 16:00:24	2015	9	30	23	57	6	45178	2015-09-30 15:57:06	63	10.1.0.105	crew-sdroberts3-macbook.sikuliah.alaska.edu	66.58.255.34	NULL	tcp	443	1785	5617	17	18
2	2015-09-30 16:00:24	2015	9	30	23	57	6	7875	2015-09-30 15:57:06	63	10.1.0.105	crew-sdroberts3-macbook.sikuliah.alaska.edu	66.58.255.34	NULL	tcp	443	3731	7295	25	25
3	2015-09-30 16:00:24	2015	9	30	23	58	8	51296	2015-09-30 15:58:08	1	10.1.0.60	shp-dnsmasq-0.sikuliah.alaska.edu	137.229.15.5	NULL	udp	53	127	131	1	1
4	2015-09-30 16:00:24	2015	9	30	23	58	8	34688	2015-09-30 15:58:08	1	10.1.0.61	shp-dnsmasq-1.sikuliah.alaska.edu	137.229.15.5	NULL	udp	53	78	82	1	1
5	2015-09-30 16:00:24	2015	9	30	23	58	8	2886	2015-09-30 15:58:08	1	10.1.0.61	shp-dnsmasq-1.sikuliah.alaska.edu	137.229.15.5	NULL	udp	53	78	82	1	1
6	2015-09-30 16:00:24	2015	9	30	23	58	7	43840	2015-09-30 15:58:07	1	10.1.0.61	shp-dnsmasq-1.sikuliah.alaska.edu	137.229.15.5	NULL	udp	53	127	131	1	1
7	2015-09-30 16:00:24	2015	9	30	23	58	6	10480	2015-09-30 15:58:06	1	10.1.0.61	shp-dnsmasq-1.sikuliah.alaska.edu	137.229.15.5	NULL	udp	53	78	82	1	1
8	2015-09-30 16:00:24	2015	9	30	23	58	6	45472	2015-09-30 15:58:06	1	10.1.0.61	shp-dnsmasq-1.sikuliah.alaska.edu	137.229.15.5	NULL	udp	53	78	82	1	1
9	2015-09-30 16:00:24	2015	9	30	23	58	7	28313	2015-09-30 15:58:07	0	10.1.0.60	shp-dnsmasq-0.sikuliah.alaska.edu	137.229.15.5	NULL	udp	53	78	82	1	1
10	2015-09-30 16:00:24	2015	9	30	23	58	7	23839	2015-09-30 15:58:07	0	10.1.0.60	shp-dnsmasq-0.sikuliah.alaska.edu	137.229.15.5	NULL	udp	53	78	82	1	1

10 rows in set (0.00 sec)

Simplify the Sample Data Query Results

```
mysql> SELECT YYYY, MM, DD, hh, mm, ss, elapsed, src, dst, proto, dport, bytes_sent, bytes_received, pkts_sent, pkts_received FROM log_pa_internet_traffic_lweek LIMIT 10;
```

YYYY	MM	DD	hh	mm	ss	elapsed	src	dst	proto	dport	bytes_sent	bytes_received	pkts_sent	pkts_received
2015	9	30	23	9	6	63	10.1.0.105	66.58.255.34	tcp	443	1785	5617	17	18
2015	9	30	23	9	6	63	10.1.0.105	66.58.255.34	tcp	443	3731	7295	25	25
2015	9	30	23	9	8	1	10.1.0.60	137.229.15.5	udp	53	127	131	1	1
2015	9	30	23	9	8	1	10.1.0.61	137.229.15.5	udp	53	78	82	1	1
2015	9	30	23	9	8	1	10.1.0.61	137.229.15.5	udp	53	78	82	1	1
2015	9	30	23	9	7	1	10.1.0.61	137.229.15.5	udp	53	127	131	1	1
2015	9	30	23	9	6	1	10.1.0.61	137.229.15.5	udp	53	78	82	1	1
2015	9	30	23	9	6	1	10.1.0.61	137.229.15.5	udp	53	78	82	1	1
2015	9	30	23	9	7	0	10.1.0.60	137.229.15.5	udp	53	78	82	1	1
2015	9	30	23	9	7	0	10.1.0.60	137.229.15.5	udp	53	78	82	1	1

10 rows in set (0.00 sec)



R/V Sikuliaq

School of Fisheries
and Ocean Sciences



<https://www.sikuliah.alaska.edu>

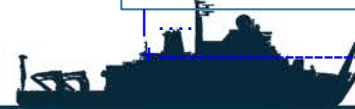
Database Tables

Data is stored in **1 table per day**.

MySQL Merge tables are used to concatenate recent data.

- Easy to clean up old data, just archive and delete tables
- Efficient to query recent data
- Able to perform comprehensive data queries

```
mysql> show tables;
+-----+
| Tables_in_skqnetmon |
+-----+
| log_pa_internet_traffic_3days |
| log_pa_internet_traffic_1week |
| log_pa_internet_traffic_skq201505S |
| log_pa_internet_traffic_2015_06_20 |
| log_pa_internet_traffic_2015_06_21 |
| log_pa_internet_traffic_2015_06_22 |
| log_pa_internet_traffic_2015_06_23 |
| log_pa_internet_traffic_2015_06_24 |
| log_pa_internet_traffic_2015_06_25 |
| log_pa_internet_traffic_2015_06_26 |
| log_pa_internet_traffic_2015_06_27 |
| log_pa_internet_traffic_2015_06_28 |
| log_pa_internet_traffic_2015_06_29 |
| log_pa_internet_traffic_2015_06_30 |
| log_pa_internet_traffic_2015_07_01 |
| log_pa_internet_traffic_2015_07_02 |
| log_pa_internet_traffic_2015_07_03 |
| log_pa_internet_traffic_2015_07_04 |
+-----+
```



Database Schema

```
CREATE TABLE log_pa_internet_traffic_YYYY_MM_DD (  
  litid          SERIAL PRIMARY KEY,  
  created        TIMESTAMP DEFAULT CURRENT_TIMESTAMP ON UPDATE CURRENT_TIMESTAMP,  
  YYYY          INT UNSIGNED NOT NULL,  
  MM            TINYINT UNSIGNED NOT NULL,  
  DD            TINYINT UNSIGNED NOT NULL,  
  hh            TINYINT UNSIGNED NOT NULL,  
  min           TINYINT UNSIGNED NOT NULL,  
  ss            TINYINT UNSIGNED NOT NULL,  
  sessionid     MEDIUMINT UNSIGNED NOT NULL,  
  start         TIMESTAMP NOT NULL,  
  elapsed       MEDIUMINT UNSIGNED NOT NULL,  
  src           VARCHAR(15) NOT NULL,  
  src_fqdn      VARCHAR(255),  
  dst           VARCHAR(15) NOT NULL,  
  dst_fqdn      VARCHAR(255),  
  proto         VARCHAR(10) NOT NULL,  
  dport        SMALLINT UNSIGNED NOT NULL,  
  bytes_sent    INT UNSIGNED NOT NULL,  
  bytes_received INT UNSIGNED NOT NULL,  
  pkts_sent     SMALLINT UNSIGNED NOT NULL,  
  pkts_received SMALLINT UNSIGNED NOT NULL,  
  UNIQUE KEY (sessionid, start, elapsed)  
) ENGINE=MYISAM;
```



Merge Table Schema

```
CREATE TABLE log_pa_internet_traffic_3days (  
  litid SERIAL PRIMARY KEY,  
  created TIMESTAMP DEFAULT CURRENT_TIMESTAMP ON UPDATE CURRENT_TIMESTAMP,  
  YYYY INT UNSIGNED NOT NULL,  
  MM TINYINT UNSIGNED NOT NULL,  
  DD TINYINT UNSIGNED NOT NULL,  
  hh TINYINT UNSIGNED NOT NULL,  
  min TINYINT UNSIGNED NOT NULL,  
  ss TINYINT UNSIGNED NOT NULL,  
  sessionid MEDIUMINT UNSIGNED NOT NULL,  
  start TIMESTAMP NOT NULL,  
  elapsed MEDIUMINT UNSIGNED NOT NULL,  
  src VARCHAR(15) NOT NULL,  
  src_fqdn VARCHAR(255),  
  dst VARCHAR(15) NOT NULL,  
  dst_fqdn VARCHAR(255),  
  proto VARCHAR(10) NOT NULL,  
  dport SMALLINT UNSIGNED NOT NULL,  
  bytes_sent INT UNSIGNED NOT NULL,  
  bytes_received INT UNSIGNED NOT NULL,  
  pkts_sent SMALLINT UNSIGNED NOT NULL,  
  pkts_received SMALLINT UNSIGNED NOT NULL,  
  UNIQUE KEY (sessionid, start, elapsed)  
 ) ENGINE=MERGE UNION=(log_pa_internet_traffic_2015_03_30, log_pa_internet_traffic_2015_03_31,  
 log_pa_internet_traffic_2015_04_01) INSERT_METHOD=NO;
```



Internet Usage per Day

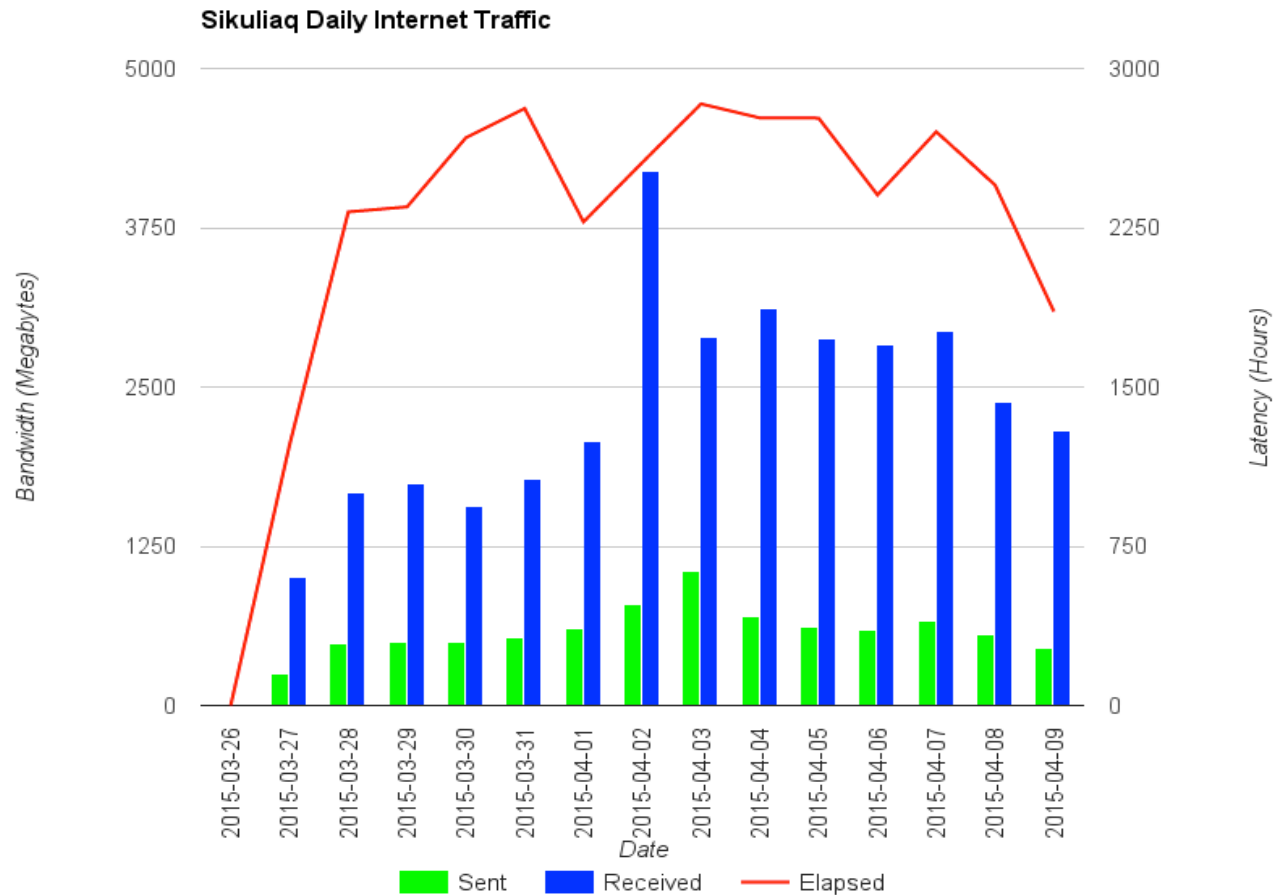
```
mysql> SELECT CONCAT(YYYY, '-', MM, '-', DD) AS Date, SUM(
bytes_sent)/(1024*1024) AS Sent, SUM(bytes_received)/(1024
*1024) AS Received, SUM(Elapsed)/3600 AS Elapsed FROM log_
pa_internet_traffic_skq201505s GROUP BY YYYY, MM, DD ORDER
BY start;
```

Date	Sent	Received	Elapsed
2015-3-26	0.0315	0.4121	0.2836
2015-3-27	245.6690	1002.3526	1225.7939
2015-3-28	486.2423	1672.8752	2324.5017
2015-3-29	497.1199	1740.7115	2348.3669
2015-3-30	500.1793	1566.1931	2673.9889
2015-3-31	536.1364	1773.3232	2811.7033
2015-4-1	602.7032	2071.5144	2277.5997
2015-4-2	790.8056	4195.2148	2557.1444
2015-4-3	1054.1565	2887.2841	2833.2742
2015-4-4	694.1730	3119.8923	2767.1881
2015-4-5	616.1213	2884.4700	2766.2283
2015-4-6	587.5304	2833.9949	2404.4144
2015-4-7	668.2687	2940.2123	2702.0506
2015-4-8	556.5085	2381.1070	2451.0817
2015-4-9	450.3210	2159.7080	1855.4378

15 rows in set (5.58 sec)



Internet Usage per Day



R/V Sikuliaq

School of Fisheries
and Ocean Sciences

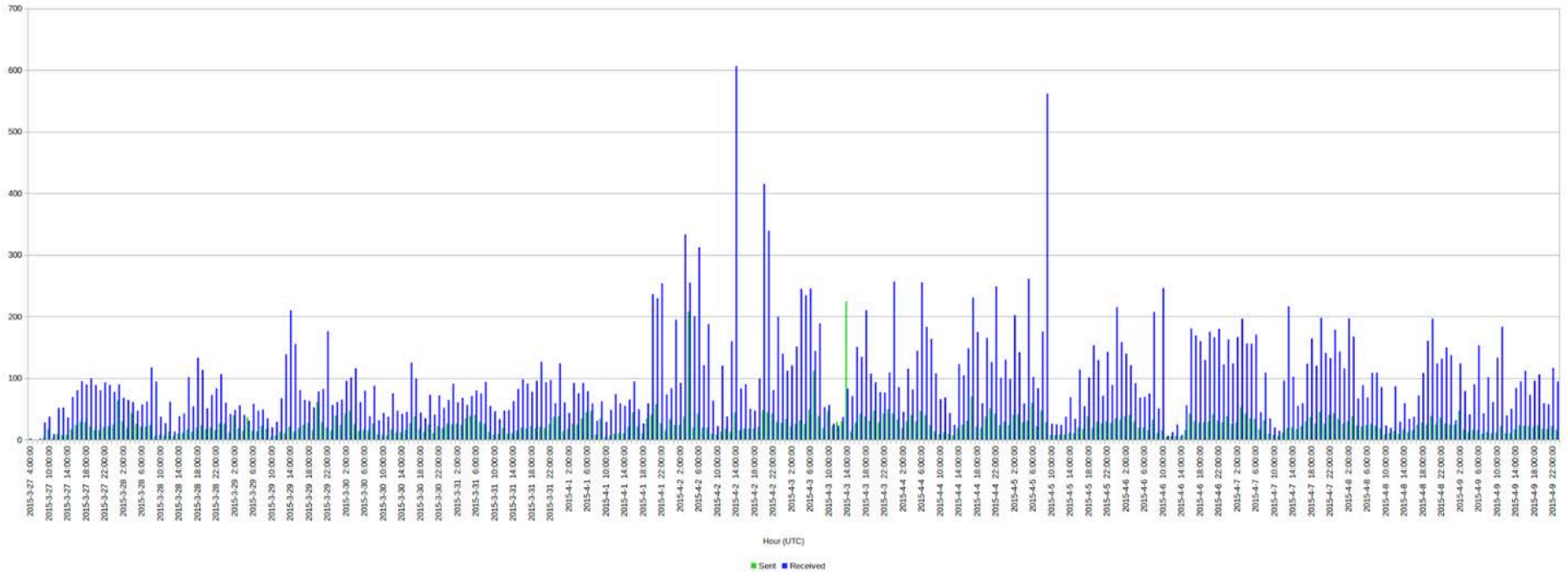
<https://www.sikuliaq.alaska.edu>



Internet Usage per Hour of Day

SIKULIAQ Internet Traffic 2015-03-27 to 2015-04-09

Total per Hour



R/V Sikuliaq

School of Fisheries
and Ocean Sciences

<https://www.sikuliaq.alaska.edu>



Internet Usage per Dest Protocol/Port

SIKULIAQ Internet Traffic 2015-03-27 to 2015-04-09

99% of traffic Bytes and Elapsed Time (Seconds) per Protocol and Port



R/V Sikuliaq

School of Fisheries
and Ocean Sciences

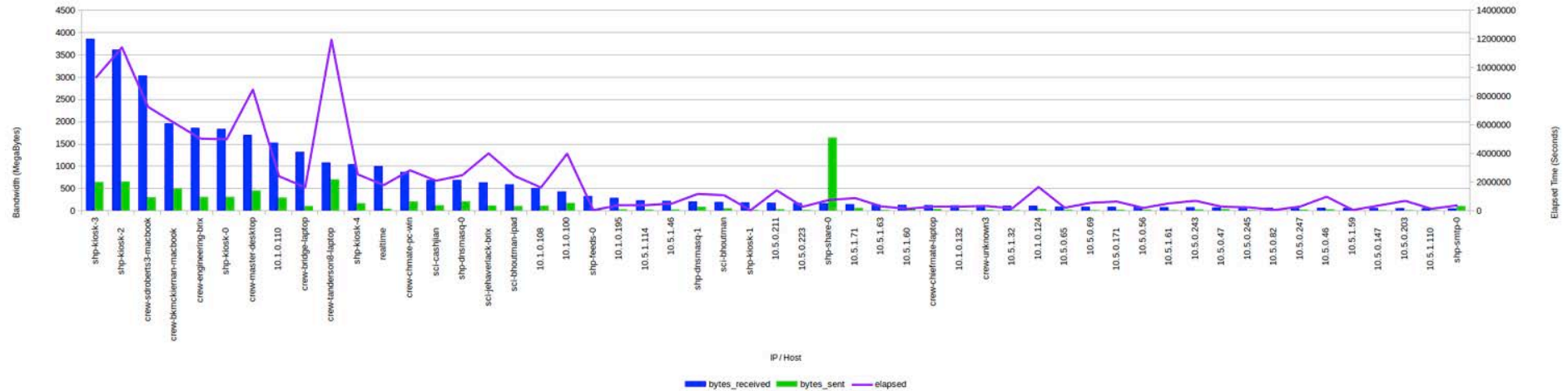
<https://www.sikuliaq.alaska.edu>



Internet Usage per Source IP

SIKULIAQ Internet Traffic 2015-03-27 to 2015-04-09fic

Bandwidth and Elapsed Time by Source IP

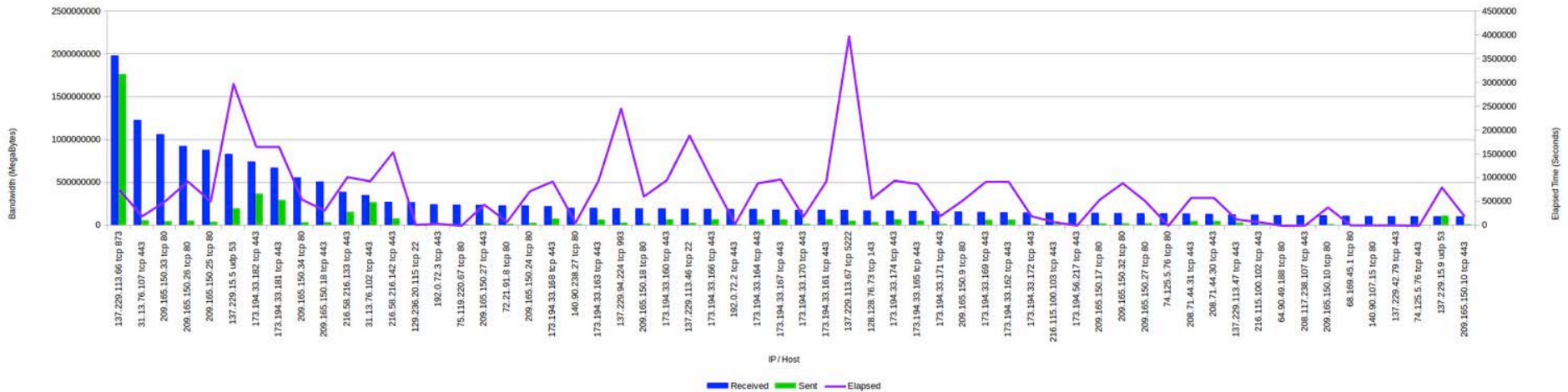


Internet Usage per Destination IP

July - September 2015

SIKULIAQ Internet Traffic 2015-03-27 to 2015-04-09

Bandwidth and Elapsed Time by Destination IP Protocol and Port



R/V Sikuliaq

School of Fisheries
and Ocean Sciences

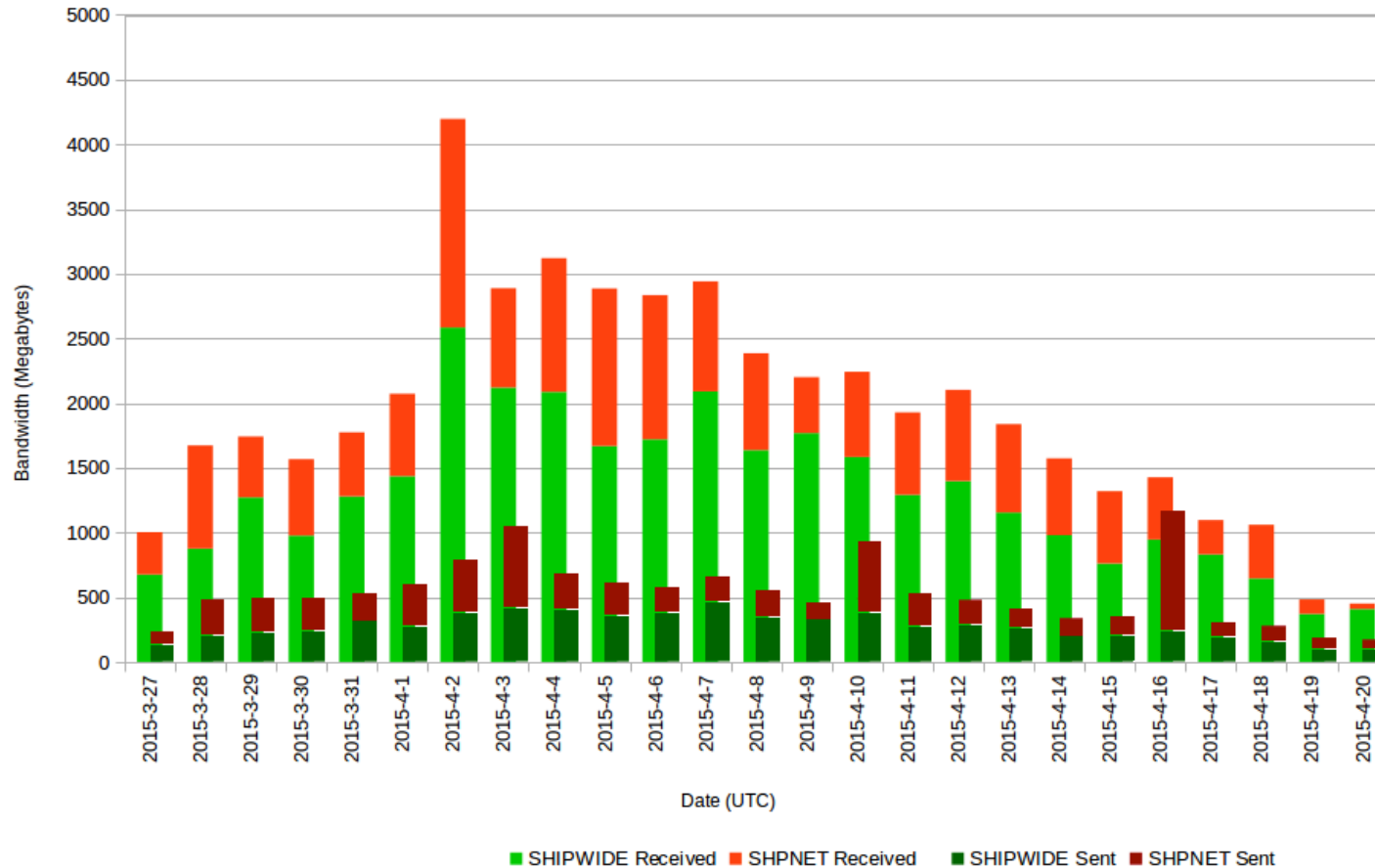
<https://www.sikuliaq.alaska.edu>



Internet Usage per Source IP Subnet

SIKULIAQ Internet Traffic Mar 27 to Apr 20 2015

Traffic for SHPNET and SHRNET



R/V Sikuliaq
School of Fisheries
and Ocean Sciences

<https://www.sikuliaq.alaska.edu>



Next Steps

1. Automated Webpage to help users see their usage.
2. Automate Usage Reporting back to Shore



R/V Sikuliaq

School of Fisheries
and Ocean Sciences

<https://www.sikuliaq.alaska.edu>



The End

The PAPoller Source Code and link for this presentation can be found at:

<https://www.sikuliahq.alaska.edu/ops/?q=node/206>



R/V Sikuliaq

School of Fisheries
and Ocean Sciences

<https://www.sikuliahq.alaska.edu>

