Pluribus Netvisor®2.0
Analytics Engine Features

Netvisor® is the Pluribus Networks network hypervisor, a distributed operating system that runs on bare metal hardware. Netvisor instances can work together to create a fabric-cluster that acts as "one big logical switch" with a distributed control plane and fabric-wide features such as virtual networks, analytics[1], and virtual flows.

[1] Pluribus Netvisor Analytics features are available in Advanced Software Defined Fabric (ASDF) and Software Defined Fabric (SDF) Netvisor software packages.

PLURIBUS NETWORKS

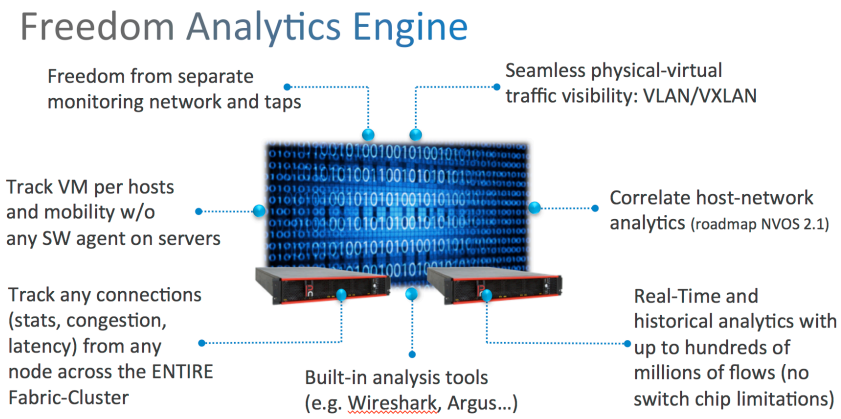
Pluribus Netvisor Analytics Engine Overview

There are many areas of networking that can benefit from technological advances, including manageability and programmability. Also tools that streamline orchestration and business enablement can mature as new technology comes to market. Little discussed but also very important is the ability to understand the state of the network, debug problems, and optimize network behavior. Frequently, when there is a problem in a computing facility, the network comes under scrutiny. That's because in most cases it is difficult to quickly assess the state of the entire network.

Basic questions that are easy to answer in other infrastructure can remain frustratingly unanswered in networking.

Can you quickly and easily obtain this kind of information from your network, network-wide?

- Port state for all ports
- Traffic volume to and from every port, or connection in the network, sorted by most active
- Critical information of every entity, including MAC address, IP address, and protocols
- End-to-end latency for every connection in the network
- Congestion and error information
- Statistical summaries and detailed data



- All of this information both in real time and historical reports

This information, and more, is available using the Pluribus Networks CLI, vManage® network management GUI, Netvisor operating system, scripting, and native C and Java APIs.

Even if your network infrastructure can be monitored as thoroughly as described, these capabilities usually involve extra tools, expense, and complexity.

With Pluribus Networks, the top-of-rack server-switches in a fabric respond as one logical switch, with one distributed point of control. This allows the network administrator, virtual network administrators, or applications to ask questions and get answers about the entire network infrastructure natively from our Netvisor hypervisor. With the Freedom and Open Network product lines, you get ***in*Network** single-point of management, ***in*Network Automation**, and ***in*Network Netvisor Analytics Engine**. No third party tools are required or no data copying to other products is needed. No taps or extra cabling is necessary.

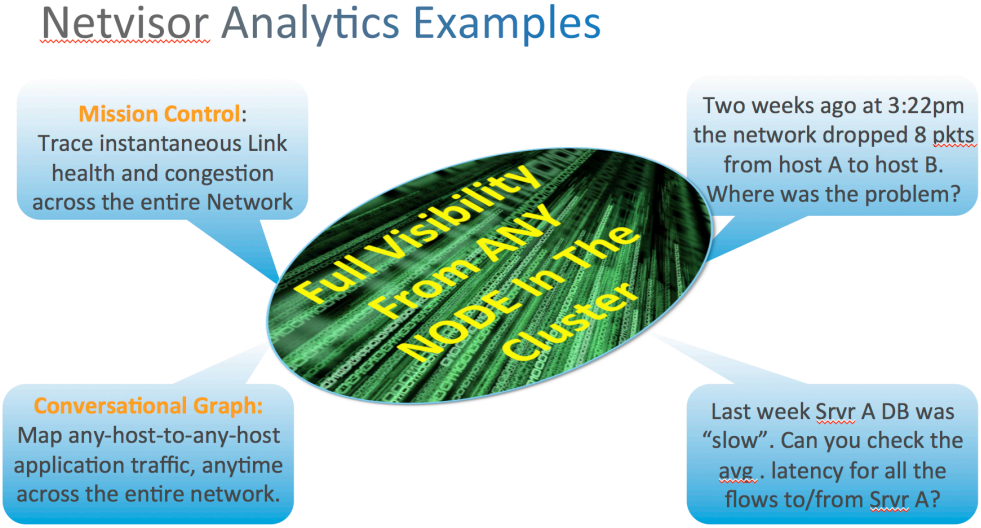
Because the analytics data gathering is distributed and pervasive, you don't need data or metadata to get to a certain spot in the network, such as core routers, for analysis. Some solutions only provide visibility at a point or network tier, but because Pluribus Networks solutions are top-of-rack, the server-switches are in the middle of all important data flows, all the time.

Netvisor analytics are not statistical, although sFlow is supported for backward-compatibility with existing monitoring infrastructures. For example, you can generate absolute information about every connection that flows through a fabric member, including when it occurred, the details and the performance.

Our infrastructure provides practical and usable information. Sites using other vendors' products, when replaced by Pluribus server-switches, are gaining more useful, more detailed, and more actionable information. Is there congestion, and if so where and when and to what extent? Does a TCP connection today have worse latency than a similar connection from yesterday? Rather than monitoring by exception, Netvisor is constantly listening to the network for information about the fabric, network, and system administrators.

Pluribus Netvisor Analytics Engine

Although the provided information can be used for reports, it can also be used in real time, interactively, to drill down into issues. The queries can be iterative, such as "repeat this information every ten minutes", or differential, such as, "what has changed in the last five seconds?" at a given time or time span, and for the entire timespan since the fabric became active.



Pluribus Networks server-switches are built with server CPUs, memory, storage, and I/O available for use in managing and monitoring the network. All of these activities happen without performance impact, because the switch chip is constantly monitored by the Netvisor operating system running on the server component, removing the need to query the switch for this information. And analytics can be performed fabric-wide, or per "virtual network", a resource subset of the fabric that is controlled and administered separately. The Netvisor Analytics engine is especially useful in overlay networking situations, which by nature cause complicated traffic flows and interactions and can be difficult to analyze and debug. Many of the features available via the Netvisor Analytics Engine would otherwise require the use of expensive third-party equipment, with resulting complexity and support effort increases.

Examples of Pluribus Networks Netvisor Analytics Engine

Analytics information is available through the Pluribus vManage® network management software, from the view displaying the entire fabric to individual connection details. The dashboard shows a summary of all fabric activities, including performance, connectivity, and attached devices and assets.

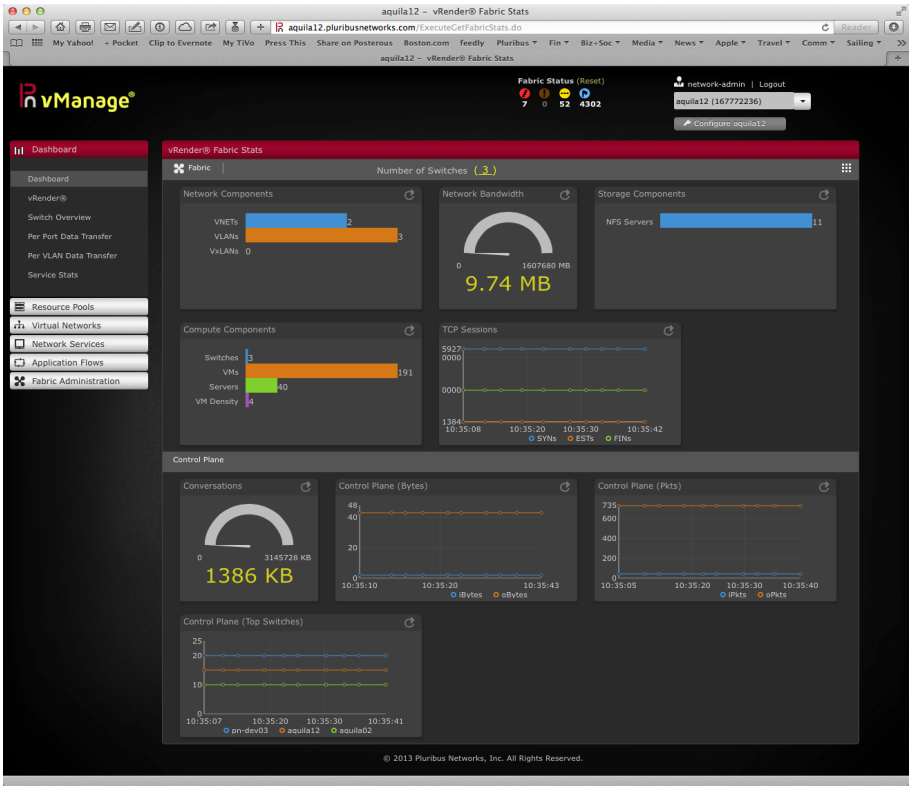


Figure 1 - vManage Analytics Dashboard

Pluribus Netvisor Analytics Engine

vRender® displays in a single view all fabric members and devices attached to the fabric, with color-coding of th

roughput traffic. Connection details and other views available using mouse hover and click actions.

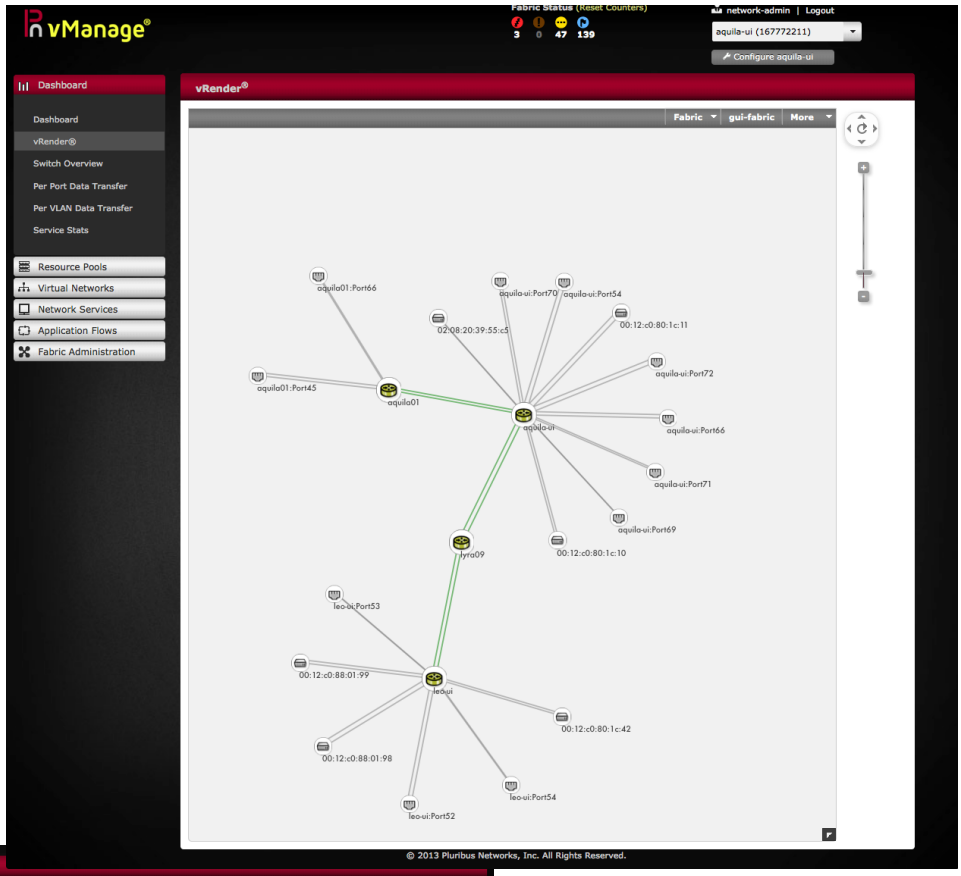


Figure 2 - vRender Fabric

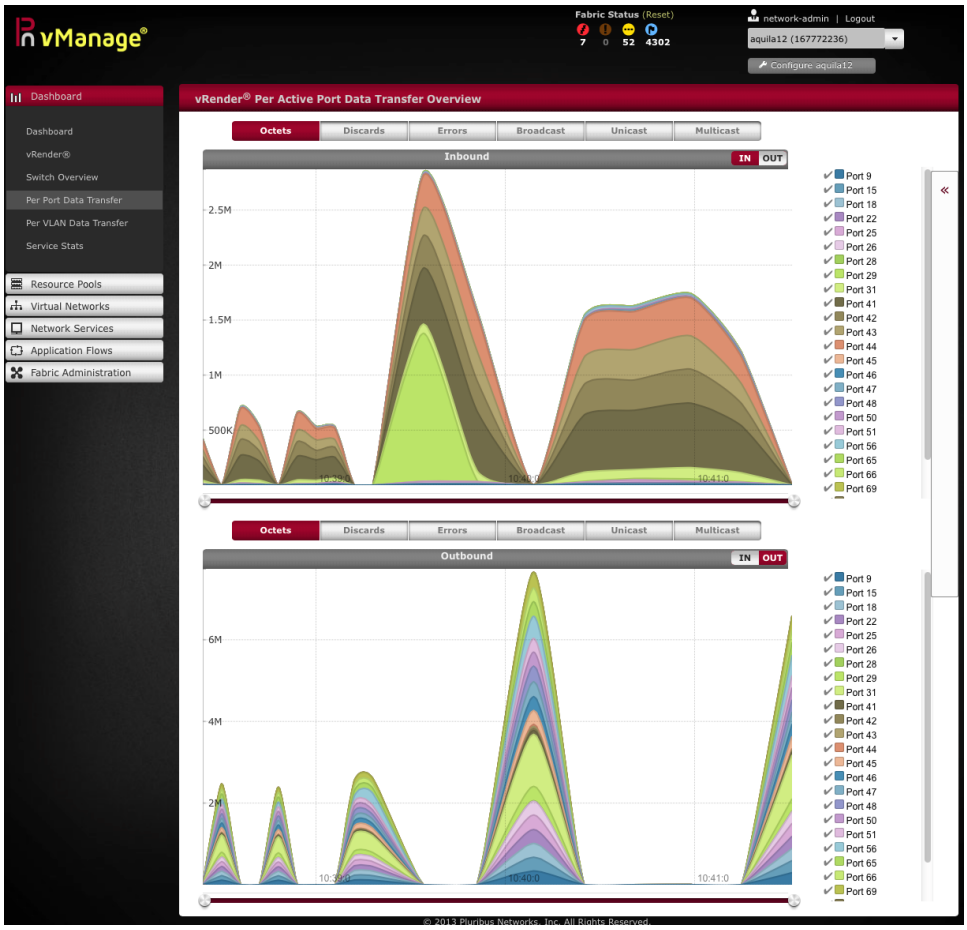
vManage also reveals other details from the Netvisor Analytics Engine, such as fabric-wide connections and data movement. In this image, you can see data transfer over time, in-bound and out-bound, unicast, multicast, errors and discarded packets. vManage® can also display per-port activity in a variety of chart and graph formats.

Figure 3 - vManage Data Details

Pluribus Netvisor Analytics Engine

Per-port information is important as well, and so can be displayed in a variety of ways, including different data elements such as discards and errors and different chart formats.

Figure 4 - vManage per-Port Details



The Netvisor Command Line Interface (CLI) provides powerful analytical commands and all data is also available to Netvisor APIs. For example, you may want to know which server-switches are in the current fabric:

```
CLI (network-admin@ss-green) > fabric-node-show
name     fab-name mgmt-ip        mgmt-vlan mgmt-vxlan version  state  device_state
ss-green pn-fab   10.1.1.147/16 0         0          1.2.4261 online ok
ss-red   pn-fab   10.1.1.137/16 0         0          1.2.4261 online ok
```

Note that output has been abbreviated and text highlighted for clarity. Commands are shown in **bold**.

How are the switch ports for the entire fabric configured?

```
> port-show
switch   port ip            mac               vlan vxlan hostname status                        config
ss-green 19   10.1.10.199   00:0c:29:f9:b2:9a 1    0              up,host,dhcp                    fd,1g
ss-green 19   10.1.10.65    f4:6d:04:0e:77:60 1    0              up,dhcp
ss-green 21   10.19.1.25    64:0e:94:2c:00:dd 5    0              up,host,uplink,stp-port-fast    fd,1g
ss-green 65   10.17.15.3    66:0e:94:4c:a4:96 6    0     ss-green up,dhcpsvr
ss-green 66                                     0              up,stp-port-fast                fd,10g
ss-red   18                                     0              up                              fd,1g
ss-red   19   10.3.9.225    64:0e:94:2c:01:0c 1    0              up,host,LLDP                    fd,1g
```

Notice that a single port can have multiple MAC and IP addresses associated with it. For example, a port might connect to a switch, or a server running virtual machines and therefore has multiple MAC and IP addresses. The Netvisor fabric provides useful information about all connected devices.

Other commands display physical port configurations, signal strengths, and transceiver details.

Pluribus Netvisor Analytics Engine

How much traffic is flowing over each port fabric wide?

```
> port-stats-show
switch   port ibytes iUpkts iBpkts iCongDrops ierrs obytes oUpkts oBpkts oCongDrops oerrs
ss-green 13   112M   466K   9.93K  0          0     1.01G  8.80M  1.55M  0          0
ss-green 14   467M   1.09M  3.72K  0          0     1.11G  9.67M  1.55M  0          0
ss-green 17   36.3M  564K   3.49K  0          0     897M   8.25M  1.55M  0          0
ss-green 19   297M   1.44M  26.5K  0          0     2.08G  10.4M  1.53M  0          0
ss-green 21   877M   2.25M  180K   0          0     1.78G  10.3M  1.01M  0          0
ss-red   19   12.7G  22.2M  420K   0          0     8.04G  30.3M  1.16M  0          0
ss-red   21   731M   5.04M  37.5K  0          0     1.67G  9.77M  1.39M  0          0
ss-red   23   1.48G  6.34M  20.2K  0          0     3.60G  15.5M  1.54M  0          0
```

Many commands also display differences over time. For example, you can display, every 5 seconds, what has changed on all ports in the fabric:

```
> port-stats-show show-diff-interval 5
switch   port ibytes iUpkts iBpkts iCongDrops ierrs obytes oUpkts oBpkts oCongDrops oerrs
ss-green 13   1.36K  17     0      0          0     31.3K  301    65     0          0
ss-green 14   0      0      0      0          0     31.9K  312    65     0          0
ss-green 17   1.25K  20     0      0          0     30.8K  293    65     0          0
ss-green 19   59.1K  214    3      0          0     239K   555    62     0          0
ss-green 21   9.03K  80     8      0          0     35.3K  364    37     0          0
```

The `l2-table-show` command output displays MAC addresses known on the fabric, and associated ports, IP addresses, hits (number of packets), migrations (virtual machine moved from one port to another), and dropped packets due to congestion.

```
> l2-table-show
switch   mac               ip            vlan vxlan port     blocked-port last-seen           hit     migrate drops active
-------- ----------------- ------------- ---- ----- -------- ------------ ------------------- ------- ------- ----- ----
ss-green e0:06:e6:c5:ad:98 10.11.10.197   1    0     45                    2013-12-30,08:54:33 89      0       0     no
ss-green e0:f8:47:2c:01:f8 10.11.10.212   1    0     45                    2013-12-30,09:19:45 85      0       0     yes
ss-green 10:dd:b1:b3:65:b4 ::             1    0     56                    2013-12-30,08:59:43 4       2       0     yes
ss-green 20:16:d8:ce:5d:eb 10.3.10.186    1    0     45                    2013-12-30,07:44:47 109     0       0     no
ss-green 66:0e:94:7c:80:b9 10.3.20.70     1    0     41-44                 2013-12-29,23:34:19 7       0       0     no
ss-black 64:0e:94:18:00:03 10.3.10.112    1    0     48                    2013-12-30,09:19:34 1477    0       0     yes
ss-black 00:e0:81:e4:02:6e 10.3.18.118    1    0     13                    2013-12-30,09:15:11 1365    0       0     yes
```

Now if you want to analyze traffic behavior at Layer 3 in the network stack, display all connections across the fabric, since the fabric was booted, including the states, latencies, bytes, and network details:

```
> connection-show
switch   vlan vxlan vnet client-ip   server-ip      server-port cur-state latency obytes ibytes total-bytes age
-------- ---- ----- ---- ----------- -------------- ----------- --------- ------- ------ ------ ----------- -----
ss-green 1    0          10.3.9.197  10.3.9.186     8080        est       57.3us                            0s
ss-green 1    0          10.20.9.137 10.3.18.221    49          fin       132us   54     18     72          0s
ss-green 1    0          10.3.99.18  10.3.10.153    nfs         syn                                        1s
ss-green 1    0          10.20.9.137 10.3.18.221    49          fin       0.00ns  0      0      0           2s
ss-green 1    0          10.12.1.25  10.3.18.221    49          rst       88.2us  0      0      0           3s
ss-green 1    0          10.3.9.197  10.3.9.186     8080        fin       153us   781    294    1.05K       5s
ss-green 1    0          10.12.1.25  10.3.18.221    49          rst       119us   1      1      2           9s
ss-green 1    0          10.3.9.197  10.3.9.186     8080        fin       136us   781    294    1.05K       10s
ss-green 1    0          10.12.1.25  10.3.18.221    49          rst       36.8us  0      0      0           10s
ss-green 1    0          10.20.9.137 10.3.18.221    49          fin       0.00ns  0      0      0           12s
ss-green 1    0          10.20.9.137 10.3.18.221    49          fin       0.00ns  0      0      0           13s
```

And now a statistical summary for an interesting IP address:

```
> connection-stats-show ip 10.3.9.9
switch    mac               vlan ip        port iconns oconns ibytes obytes total-bytes last-seen-ago
--------  ----------------- ---- --------- ---- ------ ------ ------ ------ ----------- -------------
ss-green  00:25:90:22:80:f6 1    10.3.9.9  29   4385   11     221K   656M   656M        21s
ss-black  00:25:90:22:80:f6 1    10.3.9.9  48   1383   3      135K   380M   380M        41s
ss-red    00:25:90:22:80:f6 1    10.3.9.9  43   0      0      4.54K  62.1K  66.6K       7h17m26s
```

Or a summary per IP address:

```
> client-server-stats-show
switch   vlan vxlan client-ip server-ip   server-port syn est fin obytes ibytes total-bytes avg-dur avg-lat last-seen
-------- ---- ----- --------- ---------- ----------- --- --- --- ------ ------ ----------- ------- ------- -----------
ss-green 1    0     10.3.9.9  10.3.9.86   44297       0   0   1   73     29     102         5.00m   50.4us  20m8s
ss-green 1    0     10.3.9.9  10.3.18.124 53571       0   0   1   73     29     102         1.71m   3.92ms  10h35m59s
ss-green 1    0     10.3.9.9  10.3.9.78   35008       0   0   1   74     29     103         5.00m   113us   11h1m38s
ss-green 1    0     10.3.9.9  10.3.11.18  59129       0   0   2   146    58     204         5.00m   66.5us  9h3m8s
ss-green 1    0     10.3.9.9  10.100.1.14 44575       0   0   2   146    58     204         5.01m   264ms   4h55m54s
```

Or, maybe you want to display statistics per client per TCP port:

```
> connection-show sum-by client-ip,server-port
switch   count client-ip    server-port latency obytes ibytes total-bytes
-------- ----- ------------ ----------- ------- ------ ------ -----------
ss-green 1461  10.3.10.162  http        71.3ms  2.73M  36.1M  38.9M
ss-green 1     10.87.1.6    5900        78.5us  0      0      0
ss-green 1     10.3.9.9     44297       50.4us  73     29     102
ss-green 1     10.87.1.6    ssh         64.8us  0      0      0
ss-green 9     10.87.1.6    http        156ms   3.56K  66.4K  70.0K
ss-green 14    10.88.1.6    ssh         107us   28.2K  1.24M  1.26M
```

To look at network traffic in a different way, what are latencies across all traffic?

```
> connection-latency-show
switch   min    max    num-conns percent avg-dur obytes ibytes total-bytes
-------- ------ ------ --------- ------- ------- ------ ------ -----------
ss-green 0.00ns 20.0us 13        0%                0      0      0
ss-green 20.0us 40.0us 80        3%      1.28us  146K   305K   451K
ss-green 40.0us 60.0us 671       28%     14.9us  1.19M  2.50M  3.69M
ss-green 60.0us 80.0us 649       27%     19.2us  1.16M  2.42M  3.57M
ss-green 80.0us 100us  337       14%     12.9us  615K   1.25M  1.86M
ss-green 100us  120us  219       9%      10.2us  400K   835K   1.21M
ss-green 120us  140us  114       4%      6.33us  208K   434K   642K
ss-green 140us  160us  63        2%      4.01us  115K   241K   356K
ss-green 160us  180us  58        2%      4.19us  106K   222K   327K
ss-green 180us  200us  35        1%      2.85us  63.9K  134K   198K
```

Analytics are time-based, so (among many other options) you can display all the connections that started and finished during a specific time frame, summarized by any appropriate field and sorted by any field:

```
> connection-show start-time 9:00 end-time 9:01 transition-state started-and-ended sum-by \
client-ip
count client-ip    server-ip      server-port cur-state latency total-bytes
----- ------------ -------------- ----------- --------- ------- -----------
3     10.3.9.73    10.3.9.9       nfs         fin       0.00ns  0
1     10.3.9.186   173.165.164.42 ssh         fin       18.8ms  5.36K
3     10.3.10.72   10.3.18.125    http        fin       535us   13.8K
1     10.3.9.21    10.23.9.147    http        fin       318us   94.6K
3     10.3.9.21    10.3.9.9       nfs         fin       116us   94.6K
1     10.3.9.186   173.165.164.42 ssh         fin       18.8ms  5.36K
```

You can display individual packets, and possibly you want more information about that first active connection and the high end-to-end latency:

```
> vflow-snoop name deeplook scope fabric src-ip 10.3.10.140 dst-ip 64.94.107.62 proto tcp \
action copy-to-cpu
switch: ss-green, flow: deeplook, port: 48, size: 66, time: 10:51:13.58465230
src-mac: 10:dd:b1:b5:c6:1b, dst-mac: e0:91:f5:f8:a5:20, etype: ip
src-ip: 10.3.10.140, dst-ip: 64.94.107.62, proto: tcp
src-port: 50588, dst-port: 80

switch: ss-red , flow: deeplook, port: 48, size: 66, time: 10:51:13.58481087
src-mac: 10:dd:b1:b5:c6:1b, dst-mac: e0:91:f5:f8:a5:20, etype: ip
src-ip: 10.3.10.140, dst-ip: 64.94.107.62, proto: tcp
src-port: 50588, dst-port: 80
```

Pluribus Netvisor Analytics Engine

Netvisor® vFlow commands are very powerful tools for network traffic. Instead of displaying the packets matching a vFlow request, you can write the information to the optional Fusion IO storage or disk drives. You simply add the "log-packets" option. You can then NFS mount the PCAP log file to a laptop and run Wireshark to see the packets as they are logged.

You can use vFlow to perform tasks other than capturing and viewing data. You can prioritize or drop network traffic, for instance. This capability means that you can use vFlow to implement distributed ACL-based firewall functionality. For example, simply create a vFlow with action "drop" to add firewall functionality for any Layer 2, Layer 3 or Layer 4 traffic as it attempts to enter the fabric.

Pluribus Networks Netvisor includes industry standard monitoring and analytics solutions out of the box, and works with your existing monitoring infrastructure as well.

- inNetwork Wireshark (http://www.wireshark.org): Netvisor captures packets as directed by vFlow commands to PCAP-formatted files for analysis. Even more powerful is the ability to feed PCAP data live, as the packets are captured, to Wireshark running on in a server-switch or on a separate system with a mounted file system provided by Netvisor®. Netvisor® appends matching packets to the PCAP file, and Wireshark can pipe this content into a capture filter for continuous live packet viewing. Also included is the text-based "tShark" packet display tool (similar to tcpdump).

- sFlow (http://www.sflow.org): sFlow is an industry standard format (http://www.ietf.org/rfc/rfc3176.txt) for network flow metadata, and Netvisor provides full sFlow-formatted data to sFlow collectors such as Solarwinds.

- inNetwork Argus (http://qosient.com/argus): Argus is an Audit Record Generation and Utilization System that is focused on developing network activity audit strategies and prototype technology to support network operations, performance and security management. The Argus sensor processes packets as delivered by Netvisor and generates detailed status reports of the 'flows' that it detects in the packet stream.

There are more features in the Netvisor Analytics Engine than covered in this whitepaper, but this exploration provides a glimpse at the power available to administrators of next generation networking powered by Pluribus Networks software and hardware.

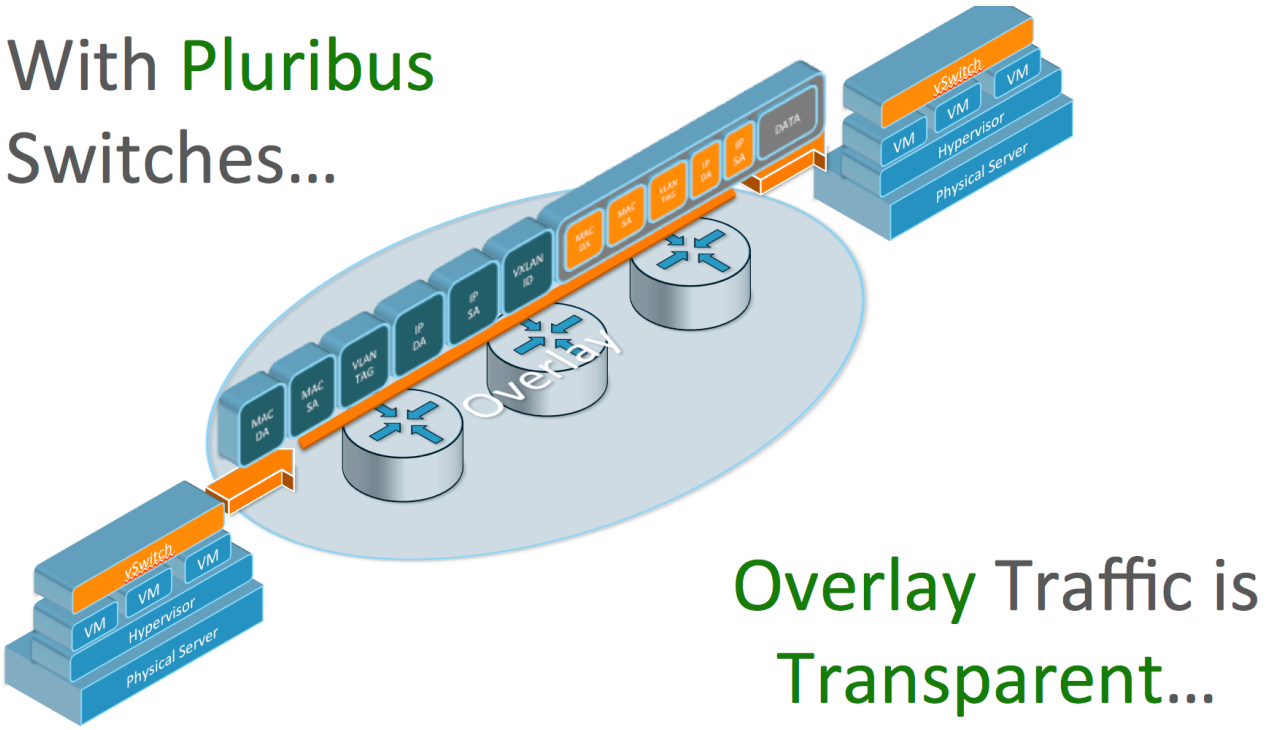
Pluribus Netvisor Analytics Engine

Pluribus Networks Products

Pluribus Networks enables you to transform a network from a cost center into a competitive asset, unlock software innovation on top of the network, and consolidate multiple services in a fully virtualized, multi-tenant environment.

Our products include:

- The Freedom Series F64, combining the performance of an industry-leading two-socket Intel server with a best-of-breed 64-port 10Gb switch.
- The Freedom Series E68, an entry level into the Freedom product line server-switch with advanced fabric-cluster features and automation.
- The NetVisor distributed network operating system Open Networking Software (ONS) product, which provides you with cloud underlay, virtualization, multi-tenancy, L2-L7 services features and functions that are widely deployed in the Data Center.



Pluribus Netvisor Analytics Engine

Pluribus Networks Services and Support

Pluribus Networks is a leader in performance-enabled network virtualization services and support. Our services allow you to bring revenue-generating capabilities online faster so you can realize bigger productivity gains and faster deployments of new business models. Pluribus Networks ensures operational excellence by optimizing your network utilization while maintaining required levels of performance, reliability, and availability.

Warranty

Pluribus Networks switches have a 1-year limited warranty. The warranty includes hardware replacement with a 10-day turnaround from receipt of a return materials authorization (RMA).

For more information, please visit
www.pluribusnetworks.com

Information in this document is based on the feature set of the general-availability NetVisor Operating System. All features are subject to change without notice.

PLURIBUS NETWORKS

Corporate and Sales Headquarters

Pluribus Networks, Inc.

2455 Faber Place, Suite 100

Palo Alto, CA 94303

www.pluribusnetworks.com

1-855-GET-VNET

To purchase Pluribus Networks solutions, please contact your Pluribus Networks representative at sales@pluribusnetworks.com.