Big Tap Monitoring Fabric enables monitoring of network traffic of an organization’s entire network and selectively delivers traffic to security, monitoring, performance measurement and compliance tools. Its design leverages modern architectural principles of bare Metal Ethernet switches and SDN controller to create a highly scalable, easy to manage, and ultra-low cost (CapEx & OpEx) monitoring solution.

**Big Tap Monitoring Fabric Overview**

Big Tap Monitoring Fabric is a modern 1G/10G/40G network visibility fabric that leverages high-performance bare metal Ethernet switches or Dell Open Networking switches to provide pervasive and scalable monitoring of an organization’s network traffic at ultra-low CapEx/OpEx costs. Using an SDN-centric architecture, Big Tap enables multiple IT teams (NetOps, DevOps, SecOps) to tap traffic everywhere in the network and deliver it to a set of troubleshooting and/or monitoring/compliance tools, including Network Performance Monitoring (NPM), Application Performance Monitoring (APM), Data Recorders, Security (DDoS, Advanced Threat Protection, Intrusion Detection, etc.), and SLA measurement tools.

As data center networks transition to modern 10G/40G designs to meet demands of cloud computing, data analytics and/or 4G/LTE mobile services, the corresponding traffic monitoring networks also need to transition to next-generation designs. The exponential growth seen in data center size, bandwidth and traffic, as well as the demand for a higher portion of network traffic to be monitored have been testing the limits of the traditional monitoring/visibility designs. Traditional box-by-box approach based on proprietary Network Packet Brokers (NPBs) has proven to be cost prohibitive and operationally complex for organization wide monitoring.

With Big Tap’s scale-out architecture, simplified operations and bare metal switch economics, it is rapidly becoming an attractive replacement for NPBs, creating two popular use cases:

- **TAP Every Rack** (monitor every link)
- **TAP Every Location** (monitor every remote DCs/POPs/branch/site)

**The Big Switch Architecture:**

**SDN Software Meets Bare Metal Hardware**

The Big Tap Monitoring Fabric has been designed ground-up to build the next-generation visibility fabric that addresses the challenges of current NPB-based monitoring solutions. Big Tap’s architecture is inspired by Hyperscale Networking designs, which consist of bare metal switch hardware, SDN controller software and centralized tool deployment.

The Big Tap Monitoring Fabric architecture consists of the following components:

- **Bare Metal or Dell Open Networking switches.** The term ‘bare metal’ refers to the fact that the Ethernet switches are shipped without embedded networking OS. The merchant silicon networking ASICs used in these switches are the same as used by most incumbent switch vendors and have been widely deployed in production in hyperscale datacenter networks. These bare metal switches ship with Open Network Install Environment (ONIE) for automatic and vendor-agnostic installation of third-party network OS.
- **Big Switch's SDN-enabled Switch Light OS** running on the switches, which can be deployed via ONIE.
- **A cluster of SDN-enabled Big Tap Controllers** – an HA pair of virtual machines or hardware appliances – that enable centralized configuration, monitoring and troubleshooting in a simplified manner.
Significant CapEx/OpEx Savings

The Big Tap Monitoring Fabric enables optimized and efficient monitoring while providing a multi-fold reduction in total cost of ownership (TCO). High TCO of NPB-based approach is due to ever expanding box-by-box deployment and proprietary hardware. Additionally, under-utilization (or inefficient use due to organizational silos) of the monitoring tools further increases TCO.

Bare Metal Economics

Big Tap Monitoring Fabric utilizes the underlying cost efficiencies and high performance (1G/10G/40G) of bare metal Ethernet switches, and as a result, it is much more cost-effective to monitor larger volumes of network traffic than vertically integrated NPB solutions.

SDN-Enabled Operational Efficiencies

Big Tap Monitoring Fabric is provisioned and managed through the single pane of glass – Big Tap controller CLI, GUI or REST APIs. This operating model allows for an easier integration with existing management systems as well as monitoring tools and hence significantly reduces the operational costs associated with box-by-box management of traditional NPBs.

Big Tap Monitoring Fabric – Product Description

Big Tap Monitoring Fabric supports topology agnostic, highly scalable fabrics. Depending on the customers’ requirements, a range of topologies is supported – from a single-switch fabric to a scale-out, multi-switch/multi-layer fabric. A typical multi-layer Big Tap Monitoring Fabric design has a layer of bare metal Ethernet switches labeled as “filter” switches and a layer of bare metal Ethernet switches labeled as “delivery” switches. Most switch interfaces in the filter-switch layer are wired to passive optical taps or switch/router/firewall SPAN ports in the production network and are configured as “filter interfaces” in the Big Tap controller software user interface. Switch interfaces in the delivery-switch layer are wired to tools and are configured as “delivery interfaces”. Filter interfaces (where packets come in to the fabric) and delivery interfaces (where packets go out of the fabric to tools) represent the primary functions of the Big Tap Monitoring Fabric.

In scale-out designs,

- A 3-layer topology is recommended in which the 3rd “core” layer of switches may be used between the “filter” and the “delivery” switch layers. These switches aggregate traffic from the filter switches and send them to requisite delivery switches to forward to the necessary tools.
- “Service interfaces” may be configured where packets can be sent to one or multiple NPBs for specific packet modification services, like de-duplication or data obfuscation, in a chain prior to delivery to the security or performance monitoring tool. As the deployments shift from NPBs to next generation Big Tap architecture, customers can re-purpose their existing high-priced NPBs in an even more efficient manner, by using them as services nodes attached to the Big Tap Monitoring Fabric.
Big Tap Monitoring Fabric also has some advanced features requested by customers:

- **Tap (Monitor) Every Location**: Big Tap Monitoring Fabric can be extended across L3 WAN to enable monitoring of remote DCs/POPs, colo facilities, campus/branch locations, as well as retail sites. This allows centralization of monitoring tools and staff in few data centers, thus dramatically reducing CapEx and OpEx cost while allowing operations teams to monitor networks across the entire organization. By simply deploying a commodity Ethernet switch at each monitored location, the entire Big Tap monitoring fabric (including remote location switches) is operated and managed centrally via the Big Tap Controller with high availability.

- **Application Protocol Recognition**: Big Tap Monitoring Fabric enables HW-based deeper packet matching capability (as shown in Figure 3) to recognize application protocols and their attributes. With ability to match up to 128 bytes of each packet at line rate, Big Tap allows more sophisticated monitoring policies to be written that can match on inner header fields for encapsulated packets such as MPLS, VXLAN and GRE and/or mobile 4G/LTE protocols such as GTP and SCTP.
### Big Tap Features And Benefits

<table>
<thead>
<tr>
<th>Features</th>
<th>Benefits</th>
</tr>
</thead>
</table>
| **Network-Wide Visibility (Tap Every Rack)** | - Packet Filtering, Aggregation, Tool Port Load-Balancing and Packet Replication functions.  
- Single switch or scale-out 1 / 2 / 3 layer Fabric designs: 1GE, 10GE & 40GE.  
- Centralized fabric / policy definition and instrumentation of bare metal Ethernet switches within the network.  
- Programmatic Event-triggered monitoring (via REST API).  
- Packet Manipulation services (such as de-duplication, packet slicing, payload obfuscation and time-stamping) by service chaining 3rd party NPBs as service nodes.  
- Multiple Overlapping Match Rules per Filter Interface based on a variety of L2, L3, L4 header as well as via Deeper Packet Matching (DPM) attributes.  
- Time / packet based scheduling of Policies.  
- Ensures efficient utilization of bare metal switch capabilities via Controller Policy Optimizer Engine. |
| **High Performance, Highly Scalable Network Monitoring Fabric** | - High-Availability for the Controller as well as the Fabric.  
- Auto Fabric Path Computation that detects and responds to failures in the monitoring network.  
- Policy-based load balancing of core links with failover detection to efficiently utilize fabric bandwidth and ensure resiliency.  
- Detection of service node/link failure and an option to bypass the service.  
- Link Aggregation (LAG) in the bare metal Ethernet fabric (including across core links, service node links and delivery links).  
- Tagging policy or tap (filter) interfaces.  
- Supports a variety of security and monitoring tool vendors.  
- Supports a variety of NPBs as stand-alone or chained Service Nodes. |
| **Centralized management, configuration, troubleshooting** | Big Tap Controller is single pane of glass for fabric and policy management.  
- Policies can be configured from a centralized controller to forward flows from multiple filter interfaces to multiple delivery interfaces, including optional service nodes. Packet replication is made at the last common node to optimize the fabric bandwidth.  
- GUI, REST API, and CLI for configuration and viewing operational state.  
- Centralized interface, flow and congestion statistics collection. |
| **Multi-DC/multi-site Tunneling (Tap Every Location)** | - Centralized monitoring of remote DCs/POPs/branches/sites (across L3 WAN).  
- Remote tools located in a centralized DC.  
- Replication of packets across tunnels.  
- Tunneling at 1G, 10G and 40G bandwidths.  
- Rate limiting of monitored traffic before entering L3 WAN.  
- Tunneling enabled on a per-switch basis. |
| **Production Network Visibility** | Big Tap Monitoring Fabric further facilitates trouble-shooting and simplifies operations and management with the Production Network Visibility features:  
- Host Tracker: shows detailed information about hosts in the production network.  
- Subnet Tracker: shows IP subnets used in the production network.  
- Tap Tracker: shows devices connected to TAP interfaces in the production network. |
| Advanced Filtering & Deeper Packet Matching capabilities | • L2/L3/L4 header filtering on ingress and packet replication (as required) in the fabric for multiple egress tools.  
• Deeper Packet Matching (DPM) with masking (up to 128 bytes in packet). Supports matching on inner header fields for encapsulated packets (e.g MPLS, VXLAN, GRE) and/or protocols (e.g. GTP, SCTP).  
• IPv4 and IPv6 based filtering.  
• IPv4, IPv6, MAC Address masking. |
<table>
<thead>
<tr>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>Packet Manipulation Services</td>
<td>• Packet Manipulation services (such as de-duplication, packet slicing, payload obfuscation and timestamping) can be enabled for the Big Tap by service chaining 3rd party NPBs as service nodes to the Big Tap Monitoring Fabric.</td>
</tr>
</tbody>
</table>
| Security and Controlled Access (Monitoring as a Service) | • TACACS+ authentication & authorization.  
• Role-Based Access Control (RBAC) for administratively defined access control per user.  
• Multi-tenancy for advanced overlapping policies across multiple user groups to monitor the traffic from the same tap interface to various tool interfaces.  
• Tenant-aware Web-based management GUI, CLI and REST API.  
• Self-service monitoring across multiple groups/business units using the same underlying infrastructure. |
| Packet Capture (With Controller Hardware Appliance only) | • Quick and easy 1G packet capture on the controller hardware appliance. |
| Marker Packet Generation | • Injection of a “marker” packet into the tool or pcap file. |
| Header Stripping Functions | • L2GRE tunnel packet decapsulation.  
• VLAN tag stripping – Useful for stripping RSPAN tag.  
• Match on inner packet post stripping. |
| Fabric wide CRC check Enable/Disable | • Allow/Disallow bad CRC packets in the production network to reach the tools for analysis. |
| Rich Web-based GUI (Graphical User Interface) | • The Dashboard shows the resources used by the fabric as well as a bird’s eye-view of the topology.  
• A highly attractive as well as functional GUI Topology view which shows:  
  • All the switches / ports in the fabric.  
  • Paths taken across the fabric on a per-policy basis.  
  • An intelligent Context sensitive Properties Panel triggered by a mouse-over on a topology object.  
• Customizable tabular views which are persisted as user preferences.  
• Various table export options like JSON, CSV are available throughout the GUI.  
• Presents a highly intuitive, simplified management and operations workflow. |
| Support for Ethernet-Based Bare Metal Switch Vendors | Support for 1G, 10G and 40G switches from Quanta, Accton and Dell. The common supported switch configurations are:  
- 48x1G + 4x10G  
- 48x10G + 4x40G (BRCM Trident/Trident+ ASIC)  
- 48x10G + 6x40G (BRCM Trident-II ASIC)  
- 32x40G (BRCM Trident-II ASIC)  
For the complete list of supported switch vendors/configurations as well as optics/cables, included in the Big Tap Hardware Compatibility List (HCL), please contact the Big Switch Sales Team (sales@bigswitch.com). |
Big Tap Controller Appliance Specification
The Big Tap Controller can be deployed either as a Virtual Machine appliance on an existing server or as a Hardware Appliance.

Controller VM Appliance Specification
The Big Tap Controller is available as a Virtual Machine appliance for the following environments.

<table>
<thead>
<tr>
<th>Environment</th>
<th>Version</th>
</tr>
</thead>
<tbody>
<tr>
<td>Linux KVM</td>
<td>Ubuntu 12.04</td>
</tr>
<tr>
<td>VMware ESXi</td>
<td>Version 5.1 U1</td>
</tr>
<tr>
<td></td>
<td>Version 5.5 U1</td>
</tr>
</tbody>
</table>

Note: The above table explicitly indicates the Major/Minor/Maintenance versions tested and supported by Big Tap Monitoring Fabric. Versions other than the ones listed above will not be supported.

Minimum VM Requirements
- 2 vCPU with a minimum scheduling of 1GHz.
- 4 GB of virtual memory.
- 20 GB of Hard disk.
- One virtual network interface reachable from physical switches.

Note: A VM's performance depends on many other factors in the hypervisor setup, and as such, we recommend using hardware appliance for production deployment.

Controller Hardware Appliance Specification
The Big Tap Controller is also available as an enterprise-class hardware appliance designed to deliver the right combination of performance, and reliability.

<table>
<thead>
<tr>
<th>Feature</th>
<th>Technical Specification</th>
</tr>
</thead>
</table>
| Form Factor      | 1U Rack Server
                  | (4.28cm x 43.4cm x 60.7cm)                                                             |
| Processor        | Intel Xeon E5-2430 v2 2.50GHz, 15M Cache, 7.2GT/s QPI, Turbo, 6 Cores, 1 Socket, 80W     |
| Memory           | 2 x 16GB RDIMM, 1600MT/s, Low Volt, Dual Rank, x4 Data Width                             |
| Hard Drive       | 2 x 500GB 7.2K RPM SATA 3Gbps 3.5in Hot-plug Hard Drives; RAID 1 for H710/H310           |
| Networking       | Embedded NIC: Broadcom 5720 Dual Port 1Gb LOM                                            |
|                  | Network Adapter: Intel X520 Dual Port 10Gb DA/SFP+ server adapter                        |
| Power            | 2 x Hot Plug Power Supplies 350W                                                        |
| Additional Features | Fan fault tolerance; ECC memory, interactive LCD screen; ENERGY STAR® compliant        |
### Environment Specification

<table>
<thead>
<tr>
<th>Environment</th>
<th>Specification</th>
</tr>
</thead>
<tbody>
<tr>
<td>Temperature – Continuous Operation</td>
<td>10°C to 35°C (50°F to 95°F)</td>
</tr>
<tr>
<td>Temperature - Storage</td>
<td>-40°C to 65°C (-40°F to 149°F) with a maximum temperature gradation of 20°C per hour</td>
</tr>
<tr>
<td>Relative Humidity – Continuous</td>
<td>10% to 80% with 26°C (78.8°F) maximum dew point (maximum wet bulb temperature)</td>
</tr>
<tr>
<td>Relative Humidity – Storage</td>
<td>5% to 95% at a maximum wet bulb temperature of 33°C (91°F), atmosphere must be non-condensing at all times</td>
</tr>
<tr>
<td>Altitude – Continuous</td>
<td>-15.2m to 3048m (-50ft to 10,000ft)</td>
</tr>
<tr>
<td>Altitude – Storage</td>
<td>-15.2m to 12,000m (-50ft to 39,370ft)</td>
</tr>
</tbody>
</table>

### About Big Switch

Big Switch Networks is the market leader in bringing hyperscale data center networking technologies to a broader audience. The company is taking three key hyperscale technologies – OEM/ODM bare metal and open Ethernet switch hardware, sophisticated SDN control software, and core-and-pod data center designs – and leveraging them in fit-for-purpose products designed for use in enterprises, cloud providers and service providers. For additional information, email info@bigswitch.com, follow @bigswitch or visit www.bigswitch.com.