Big Tap

Monitor Traffic Everywhere, Deliver Traffic Anywhere

Big Tap leverages a high-performance, OpenFlow-enabled Ethernet switch fabric and the Open SDN platform to ubiquitously monitor traffic everywhere and selectively deliver traffic to your security and monitoring appliances.

Big Tap™ is an advanced network monitoring application that leverages a high-performance OpenFlow-enabled Ethernet switch fabric to provide the most scalable and flexible monitoring network to tap traffic everywhere in your network and deliver it by policy to any of your performance monitoring or security tools. Big Tap delivers ubiquitous network monitoring functions, optimizing the utility of security tools, monitoring tools, and network packet brokers (NPBs). Big Tap provides unprecedented visibility into application traffic, getting the right traffic to the right tool at the right time.

Traditional Network Monitoring Challenges

Network monitoring is a critical function for debugging, monitoring performance, and enforcing security compliance in all networked environments. While network monitoring is a powerful tool, it is underutilized in the average network due to the excessive cost to deploy and the inflexibility of managing at scale using conventional monitoring architectures.

In a traditional networking monitoring deployment, monitoring appliances must be directly connected to each network tap or SPAN port. If you want to create network-wide visibility, you must either manually connect target network segments to the monitoring appliances; or, you must purchase and deploy expensive security and monitoring appliances at each network segment. As a result, only a small segment of your network traffic is typically available to network security and performance monitoring tools. And, typically silos of monitoring networks must be deployed and supported for each IT function – server admins, network admins and security operations.

New network monitoring aggregation tools have been brought to market to address these challenges, but they still present significant flexibility and scalability challenges. The relatively inflexible and expensive nature of networking monitoring and network taps imposes undesirable limitations on how, when, and where network traffic can be inspected. To complicate things further, the migration of networks from 1Gbps to 10Gbps to 40Gbps creates further scalability challenges and introduces unnecessarily high implementation costs for the monitoring and security appliances trying to ingest data at these rates.

The Solution: Big Tap

Big Tap is a proactive SDN application that leverages the flexibility and programmability of the Open SDN architecture to create an elastic network monitoring fabric on top of high-performance, OpenFlow-enabled Ethernet switches that can dynamically deliver targeted network flows to your security and monitoring tools.

Enterprise-Wide Network Visibility

Utilizing OpenFlow-enabled Ethernet switches, Big Tap creates a centrally controlled monitoring network fabric to filter all monitored traffic by policy, to selectively modify packets using NPBs, and to deliver traffic to any number of targeted performance monitoring or security tools. Big Tap can program OpenFlow switches to filter terabits of incoming traffic through multiple match conditions to reduce traffic rates to monitoring appliances, and replicate traffic to multiple appliances or numerous other traffic filters. Big Tap optimizes tool and NPB utilization and increases the scope, usability, and performance of your entire network monitoring system while dramatically reducing the cost of building monitoring networks.

Programmable Fabric Supports Multi-Tenant Network Monitoring and Eliminates Silos of Tools

Big Tap creates a unified network monitoring domain that enables network operators to create dynamic filtering and delivery policies between any identified network flow and any downstream tool, while at the same time providing multi-tenancy features to securely support the monitoring needs of various group within the IT organization.

Big Tap supports role-based access control (RBAC) and associated user views, so roles can be assigned by administrators and enforced during authentication that limit the switches, ports, and filter rules available to users. With Big Tap RBAC support and the user interface, IT organizations can enable monitoring support for multiple end user groups across different business units in a segmented way without having to build and maintain separate monitoring networks for each user organization or function.

Using RBAC, network administrators can, for example, delegate select protocol or network flows to application admins without exposing other extraneous network traffic and without creating a security compliance risk associated with broader network access. User views and RBAC enable self-service monitoring, including simultaneous monitoring of the same flows by disparate parties (within their respective user view permissions).

High Performance, Highly Scalable OpenFlow Network Monitoring Fabric

Big Tap utilizes the underlying cost efficiencies and high performance of Ethernet switches, and as a result, it is much more cost-effective to monitor larger volumes of network traffic than other vertically integrated network monitoring solutions. Big Tap supports a variety of OpenFlow-enabled Ethernet switches from market leading vendors, including Dell/Force10, Extreme Networks, and IBM. Big Tap also supports bare metal switches running Big Switch Networks Switch Light™ for Broadcom thin-switching software running on a variety of switches, including those from Quanta.

Big Tap can scale from a small number of monitored network segments and monitoring devices to hundreds or thousands of segments and devices. For example, customers can start with a single OpenFlow Ethernet switch to support initial deployments, but can then scale out the OpenFlow monitoring switch fabric to support a growing number of ingress ports from monitor segments and egress ports to monitoring devices. As you grow your OpenFlow monitoring fabric, Big Tap automatically discovers neighbor switches in the OpenFlow switch fabric, and creates multiple redundant links for multi-path, redundancy and failover. And, Big Tap supports link aggregation (LAG) to increase network throughput in the OpenFlow core fabric and to load balance monitor traffic across a group of similar tools.

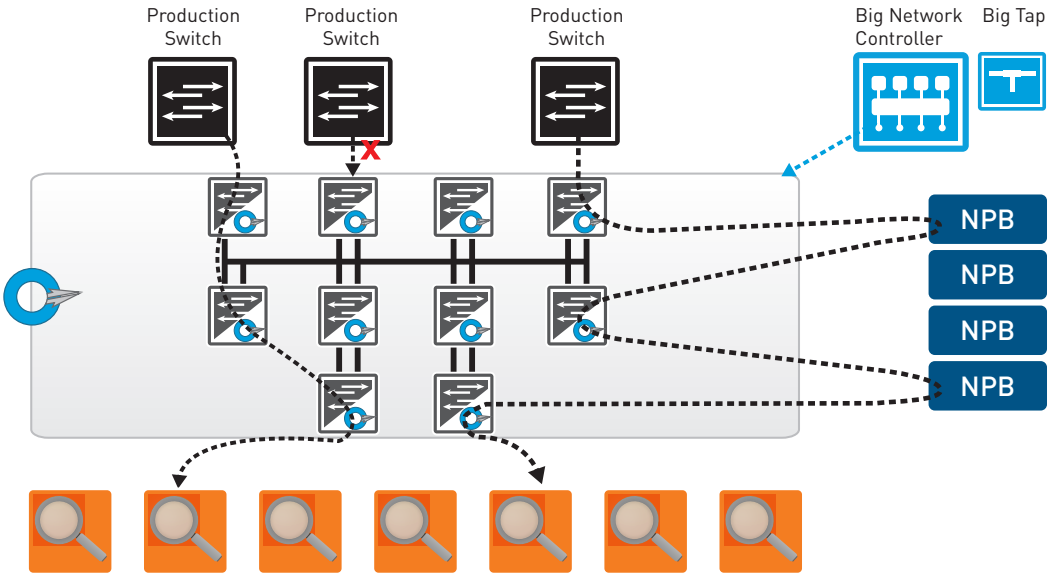

Figure 1 - Big Tap orchestrates an OpenFlow fabric to filter and deliver traffic from any TAP/SPAN port to any tool.

Advanced Services and Dynamic Policies Optimize Tool Usage

By enabling the flexible delivery of more flows to your expensive security and performance monitoring tools, Big Tap increases the efficacy and utility of your tool and NPB investment. For example, Big Tap supports more efficient use of your NPBs by using them as service nodes in the OpenFlow fabric to selectively provide packet manipulation services, like time-stamping or data obfuscation, in a chain prior to delivery to the ultimate security or performance monitoring tool.

Big Tap also can also increase the utility of your security and performance monitoring tools by dynamically redirecting flows based upon real-time network events. Utilizing application programming interfaces (APIs) available in Big Tap, administrators can establish dynamic polices that react to events on the network and that automatically sends traffic to tools for troubleshooting, recording, or security applications. Dynamic policies can be created to deliver more meaningful network flows to tools based on events, such as anomalies in flow data or when applications encounter transport issues.

As the filter, service, and delivery policies grow, Big Tap will automatically maintain overlapping monitoring policies that also ensure compliance within the role-based access control (RBAC) assigned to particular users. Importantly, multiple user groups can monitor the same traffic flows if they are all authorized to those flows.

Feature	Benefit
Enterprise-Wide Network Visibility	• Brokers OpenFlow-based monitoring network fabric centrally. • Automatically converts high-level policy into device semantics for filter, delivery and service interfaces. • Filter Interfaces selectively forward packets or capture statistics depending upon Match Rule policies. • Delivery Interfaces copy and deliver traffic to select tools. Policies can be configured from multiple filter interfaces to multiple delivery interfaces, including optional service nodes. Packet replication is made at the last common hop to optimize the fabric bandwidth. • Services nodes can be selectively configured with service chaining to apply services en route between Filter and Delivery Interfaces. • Virtual Tap feature enables selective filtering directly on production network switches feeding into monitoring fabric and provide centralized statistics. • Host tracking enables you to maintain IP-MAC bindings of hosts across your production network and track the data centrally. • Packet manipulation services via 3rd party NPBs, include packet-slicing, payload obfuscation and time-stamping. • Supports multiple overlapping Match Rules per Filter Interface based on a variety of L2, L3 and L4 header attributes.
Security Features and Controlled Administrative Access	• Inlcudes TACACS+ authentication & authorization. • Inlcudes Role-Based Access Control (RBAC) implements administratively defined access control per user. • Inlcudes support for overlapping policies enables multiple user groups to monitor the traffic from the same tap interface to various tool interfaces – providing true multi-tenancy. • Inlcudes Web-based management GUI enforces RBAC-based User View privileges.
High Performance, Highly Scalable OpenFlow Network Monitoring Fabric	• Provides centralized-policy definition and instrumentation of Open Flow switches within the network. • Supports single-switch networks, where filter and delivery are completed within a single device. • Supports two-tier and three-tier monitoring fabrics to scale with the largest network monitoring needs. • Multi-site monitoring support can be managed by cluster of controllers residing on single site. • Link Aggregation (LAG) enabled in the OpenFlow fabric and across delivery interfaces. • Uses policy-based load balancing of core links with failover detection to efficiently utilize fabric bandwidth and ensure resiliency. • Filter, Core and Deliver switch support delivers a range of configuration, services and topologies. • Support for a variety of 1G, 10G and 40G OpenFlow switching platforms, with logical pathway to 100G and beyond. • Support for security, monitoring and NPB tools from a variety of vendors.
Support for a Range of Ethernet-Based OpenFlow Switch Vendors	• Support for a variety of OpenFlow-enabled Ethernet switches, including Dell/Force10, Extreme Networks, and IBM. • Supports bare metal switches (eg, from Quanta) with Switch Light for Broadcom thin-switching OS.

About Big Switch Networks

Big Switch Networks is the leading platform-independent Software-Defined Networking (SDN) vendor. The company's highly scalable Open SDN architecture leverages industry standards and open APIs that enable customers to deploy dynamic and flexible networking applications, including data center network virtualization. Big Switch Networks is backed by the largest SDN ecosystem of OpenFlow applications and physical and hypervisor switches. The company's commercial controller, network virtualization, and applications, which accelerate delivery of cloud services, are in customer trials today. For more information, visit www.bigswitch.com

Headquarters
100 West Evelyn Street, Suite 110
Mountain View, CA 94041, USA
Phone: +1.650.322.6510
or: +1.800.653.0565
bigswitch.com

DS03-04-EN July 2013