Big Tap Monitoring Fabric
SDN Enabled, Ultra Low Cost Network Visibility

Big Tap™ Monitoring Fabric is an advanced network monitoring solution that leverages high-performance bare metal Ethernet switches to provide the most scalable, flexible and cost-effective monitoring fabric. Using an SDN-centric architecture, Big Tap enables tapping traffic everywhere in the network and delivers it to any troubleshooting, network monitoring, application performance monitoring or security tools.

At its core is the centralized Big Tap Controller software that compiles user-defined policies into highly optimized flows that are programmed into the forwarding ASICs of bare metal Ethernet switches running production grade Switch Light™ Operating System. Big Tap Monitoring Fabric delivers unprecedented network visibility with bare metal economics, 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 network 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 known as “network packet brokers” (NPBs) have been brought to market to address some of these challenges. These single box devices multiplex ports coming in from taps to ports going out to tools, but they still present significant flexibility and scalability challenges. The relatively inflexible and expensive nature of these appliances imposes undesirable limitations on how, when, and where network traffic can be inspected. To complicate things further, the migration of networks from 1Gbps to 10/40Gbps (and 100Gbps on the horizon) creates further scalability challenges and introduces unnecessarily high implementation costs for the monitoring and security tools trying to ingest data at these rates.
The Big Switch Approach: SDN Software Meets Bare Metal Hardware

The Big Tap Monitoring Fabric is designed from its inception to address the challenges with current monitoring solutions. The fabric solution features SDN design principles and bare metal Ethernet switch hardware, delivering advanced monitoring functionality with bare metal economics.

SDN Design Principles
Centralized configuration, monitoring and troubleshooting are done on the CLI or GUI of a controller—an HA pair of virtual machines (or hardware appliances) running the Big Tap Controller software. The controller provides an extremely simplified and intuitive policy creation mechanism. It then optimizes the user-defined policies into highly targeted, topology-aware flows that are programmed into the forwarding ASICs of the Ethernet switches.

Bare Metal Ethernet Switch Hardware
The term ‘bare metal’ (or ‘white box’) refers to the fact that the Ethernet switches come directly from large original design manufacturers (ODMs) and unlike traditional networking devices, are shipped without software. The ASICs used in these switches are the same as used by most large switch vendors and widely deployed in the production datacenter networks. To enable this powerful yet low-cost data plane, Big Switch provides an ONIE-enabled, lightweight, production-grade Switch Light Operating System that runs on the bare metal switches.

Big Tap Monitoring Fabric: Architecture
A typical 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) represent the primary functions of the Big Tap Monitoring Fabric.

In advanced designs, “service interfaces” may be configured where packets can be sent to legacy NPBs for various packet modification services. This investment protection mechanism ensures that features of these expensive, older NPBs can be used more efficiently and at higher scale in these monitoring fabric designs.

Features and Benefits
Network-Wide Visibility – Any Tap to Any Tool at Any Time
With Big Tap Monitoring Fabric the choice of where to tap is completely decoupled from the size or location of the tools. Big Tap Controller creates a centrally provisioned, easy-to-use monitoring fabric to filter all traffic based on user defined policies, to selectively modify packets using NPBs, and to deliver traffic to any number of targeted performance monitoring or security tools. This is done using automatic, topology-aware programming of the bare metal switches running Switch Light OS. As a result, Big Tap Monitoring Fabric can reduce traffic rates to tools by filtering terabits of incoming traffic through multiple match conditions or replicate traffic flows to multiple monitoring appliances and tools.
Flexible, Scale-Out Fabric Deployment

Big Tap Monitoring Fabric can be designed and configured to cater to the requirements of any large network. It supports 1-Tier, 2-Tier, or 3-Tier fabric architectures to handle various traffic loads and range of tools.

Adding more taps, tools, or service nodes (NPBs) simply requires extending the monitoring fabric with bare metal Ethernet switches with the requisite capabilities (1/10/40Gbps) and desired port density or switch form factors. Unlike single box designs, the Big Tap Monitoring Fabric does not require all capacity needs to be purchased and provisioned on day one, nor does it put any restrictions on how different fabric ports are provisioned.

Multi-Tenant Tap and Tool Sharing

Network infrastructure teams can provision physical assets (taps, tool farms, NPB service nodes) as shared resources and then offer On-Demand Monitoring-as-a-Service to their internal customers (e.g., security team, network ops team, and so forth).

The Big Tap controller 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 groups within the IT organization. Fine-grain role-based access control (RBAC) capabilities of Big Tap ensure that only authenticated users get access to designated switches, ports or tools.

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 for those flows.

Operational Simplification with Centralized Programmability

All switches in the Big Tap Monitoring Fabric solution are managed from a central place – the Big Tap Controller (via CLI or GUI). This centralized deployment, configuration, and troubleshooting, as well as single place for policy authoring and provisioning provides a true single pane of glass fabric management.

Open REST APIs and interactive REST<>CLI mode in the Big Tap software enables rapid integration with existing operations/business support systems (OSS/BSS) for automated operation. Because CLIs and GUI are built on top of REST APIs, the entire solution is fully programmable (unlike traditional NPBs where APIs are an afterthought). Using these comprehensive REST APIs, operators can quickly develop innovative and advanced solutions to address their operational requirements (e.g., program the fabric policies based on external triggers such as traffic thresholds, anomalies in flow data, network flow patterns, etc.).

Significant Cost Savings

Costs for monitoring systems stem from the ever expanding and costly NPB infrastructure as well as the underutilization (or inefficient use due to organizational silos) of the expensive monitoring tools. With Big Tap Monitoring Fabric running on bare metal (white-box) switches, the Big Switch solution allows for a multi-fold reduction in total costs.

Bare Metal Economics

Big Tap Monitoring Fabric utilizes the underlying cost efficiencies and high performance of bare metal 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. The economics associated with the production of bare metal switches at some of the largest original design manufacturers (ODMs) ensure that the costs-per-switch-port are significantly lower than traditional vendors.

Eliminating Tap & Tool Silos

Big Tap Monitoring Fabric enables increased tapping of segments in the network as well as provides extensive filtering capability of the tapped traffic. In turn, this enables delivery of more flows to expensive security and performance monitoring tools, thereby increasing the efficacy and utility of the tool and NPB investment. For example, Big Tap supports more efficient use of your NPBs by using them as service nodes in the monitoring 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. Such optimal sharing of tools and service nodes, as well as service node chaining can be used to leverage the long tail of important but less frequently used features found in today’s network packet brokers (NPBs), effectively extending their useful life by a few more years.

SDN-Enabled Operational Efficiencies

Big Tap Monitoring Fabric is provisioned and managed through a centralized controller (CLI, GUI or REST APIs). This operating model allows for an easier integration with existing management systems and significantly reduces the operational costs associated with box-by-box management of traditional NPBs.
**Feature** | **Benefit**
--- | ---
**Network-Wide Visibility** | • Brokers bare metal Ethernet switch based monitoring network fabric centrally  
• Ensures efficient utilization of bare metal switch capabilities via new and improved controller policy optimizer engine.  
• Filter Interfaces selectively forward packets and capture statistics depending upon Match Rule policies  
• Delivery Interfaces copy and deliver traffic to select tools. 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 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  
• Host tracking enables you to maintain a time-sorted inventory of IP-MAC bindings of hosts across your production network and track the data centrally. It helps track down ownership of IP addresses dynamically assigned to the hosts as well as their location in the network.  
• Packet manipulation services via 3rd party NPBs, include de-duplication, 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** | • TACACS+ authentication & authorization  
• Role-Based Access Control (RBAC) implements administratively defined access control per user  
• Support for advanced overlapping policies enable multiple user groups to monitor the traffic from the same tap interface to various tool interfaces – providing true multi-tenancy  
• Web-based management GUI enforces fine grain RBAC-based User View privileges

**High Performance, Highly Scalable Network Monitoring Fabric** | • Centralized-policy definition and instrumentation of bare metal Ethernet 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 at a single site  
• Link Aggregation (LAG) in the bare metal Ethernet fabric and across deliver interfaces  
• 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 security, monitoring and NPB tools from a variety of vendors

**Support for Ethernet-Based Bare Metal Switch Vendors** | Support for 1G, 10G and 40G ODM switching platforms (with logical pathway to 100G and beyond) with Switch Light OS for Broadcom. For supported switch configurations, please consult the Hardware Compatibility List (HCL).

---

**About Big Switch Networks**

Big Switch Networks is the Bare Metal SDN company. The company’s SDN Fabric solutions embrace industry standards, open APIs, open source and vendor-neutral support for both physical and virtual networking infrastructure. Big Switch Networks SDN Fabric solutions support a broad range of networking applications, including Unified Physical + Virtual (P+V) Cloud Switching and Monitoring.

For more information, follow us @bigswitch or visit www.bigswitch.com.