big switch networks

Big Tap Monitoring Fabric 4.5

SIMPLER, SCALABLE, ECONOMICAL

Big Tap Monitoring Fabric enables pervasive security and monitoring of network traffic for an organization and selectively delivers it to multiple security, monitoring, performance measurement and compliance tools—both Inline and Out-of-Band. Leveraging Open Ethernet switch fabric and an SDN controller, Big Tap is a highly scalable and ultra-low cost (CapEx & OpEx) network visibility solution.

BIG SWITCH NETWORKS

Our mission is to bring hyperscale networking to a broader audience—ultimately removing the network as the biggest obstacle to rapid deployment of new applications.

We do this by delivering all the design philosophies of hyperscale networking in a single solution.

The Big Tap Monitoring Fabric Features:

- Open Ethernet Switch Hardware to Reduce Cost
- SDN Controller Technology to Reduce Complexity
- Consolidated Tool Farm Designs to Innovate Faster

Get hands-on experience with our offering, register for a free online trial at:
labs.bigswitch.com

Contact our sales team at:
sales@bigswitch.com

For general inquiries contact us at:
info@bigswitch.com

BIG TAP MONITORING FABRIC OVERVIEW

Big Tap Monitoring Fabric is a modern 1G/10G/40G network visibility fabric that leverages high-performance, open Ethernet switches to provide pervasive security monitoring and visibility of an organization's network traffic at ultra-low CapEx/OpEx costs. Using an SDN-centric architecture, Big Tap enables scale-out fabric for enterprise-wide monitoring, single pane of glass for operational simplicity, and multi-tenancy for multiple IT teams (NetOps, DevOps, SecOps) to simultaneously perform network monitoring using tenant-specific inline or out-of-band tools and policies.

ARCHITECTURE: SDN SOFTWARE MEETS OPEN SWITCH HARDWARE

The Big Tap Monitoring Fabric is a next-generation Network Packet Broker (NPB) that has been designed from the ground-up to build a pervasive 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 Open Ethernet switch hardware, SDN controller software and centralized tool deployment.

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

- **Open Ethernet Switches (Bare Metal or Brite Box):** The term 'open' or 'bare metal' refers to the fact that the Ethernet switches are shipped without embedded networking OS. These switches include Dell Open Networking switches, as well as ODM switches from Accton and Quanta. 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 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.
- **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.

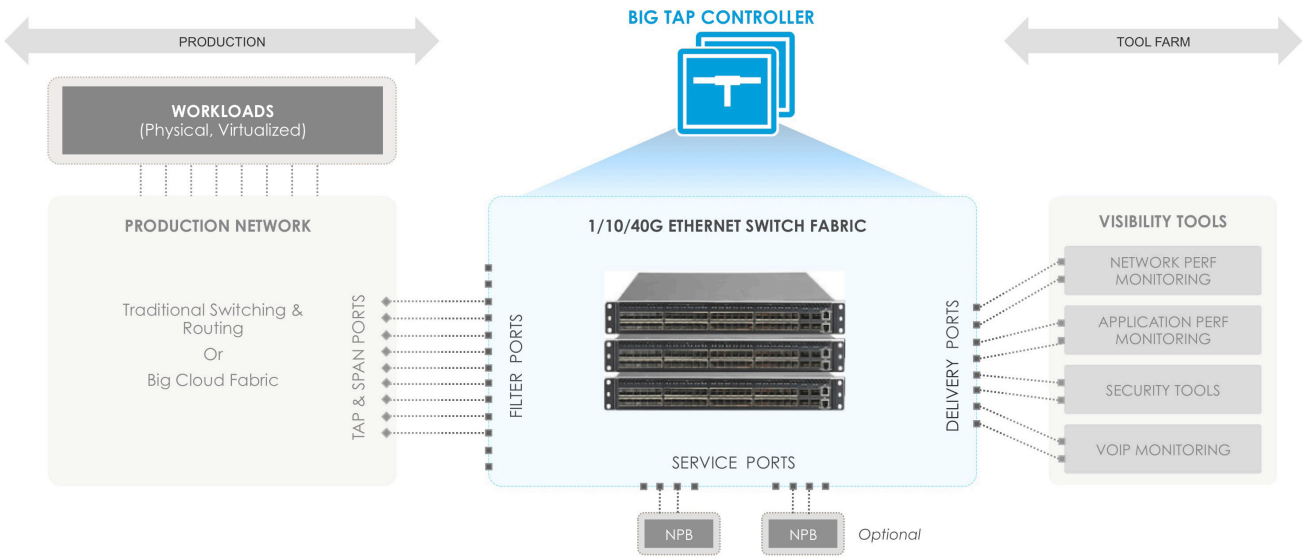


Figure 1: Big Tap Monitoring Fabric—Architecture

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.

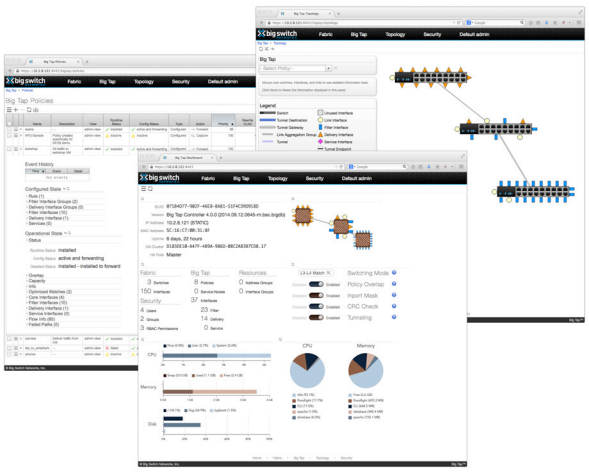
Open Ethernet Switch Economics

Big Tap Monitoring Fabric utilizes the underlying cost efficiencies and high performance (1G/10G/40G) of open 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.

Figure 2: Monitoring Fabric—Graphical User Interface (GUI)



BIG TAP MONITORING FABRIC—PRODUCT DESCRIPTION

Big Tap switches can be deployed in either of the two deployment modes:

- **Out-of-Band**—Deployed adjacent to the production network. Connects to SPAN/TAP ports from the production network.
- **Inline**—Deployed in the DMZ (production network).

Big Tap Controller continues to be the single point of management for all switches within the Big Tap fabric, running in either deployment mode.

Some of the advanced features of Big Tap Monitoring Fabric include:

Application Protocol Recognition (or Deeper Packet Matching): 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.

sFlow Generation: Big Tap supports sFlow generation capability that provides real-time flow-level visibility into the production network. sFlow is an industry standard technology that is available on most Open Ethernet switches. It provides real time application level visibility, including tunneled or encapsulated traffic, enables detection of security attacks like DoS/DDoS and supports sub-second triggering.

The sFlow configuration for Big Tap is done centrally through the controller and is applied to filter switches/interfaces. Advantages of using sFlow on Big Tap Monitoring Fabric include:

- Centralized, simple and consistent configuration across all switches, using the centralized configuration through Big Tap controller
- Off-loads sFlow record generation burden from the production switches to the monitoring fabric
- sFlow offers visibility into the whole protocol stack as opposed to only outer TCP-IP fields

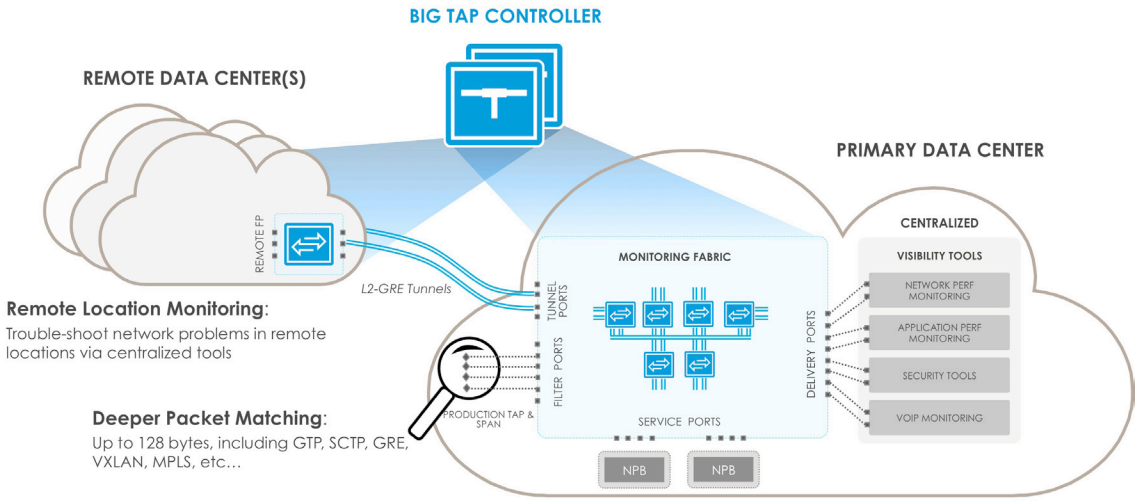


Figure 3: Big Tap Monitoring Fabric—Monitor Every Location with Centralized Tools and Management

BIG TAP: OUT-OF-BAND

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 open switch economics, it is rapidly becoming an attractive replacement for NPBs, creating two popular use cases:

- **Monitor Every Rack** (monitor or tap every link)
- **Monitor Every Location** (monitor or tap emote DCs/POPs/branch/site)

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 open Ethernet switches labeled as "filter" switches and a layer of open 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
- Monitor (Tap) 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.

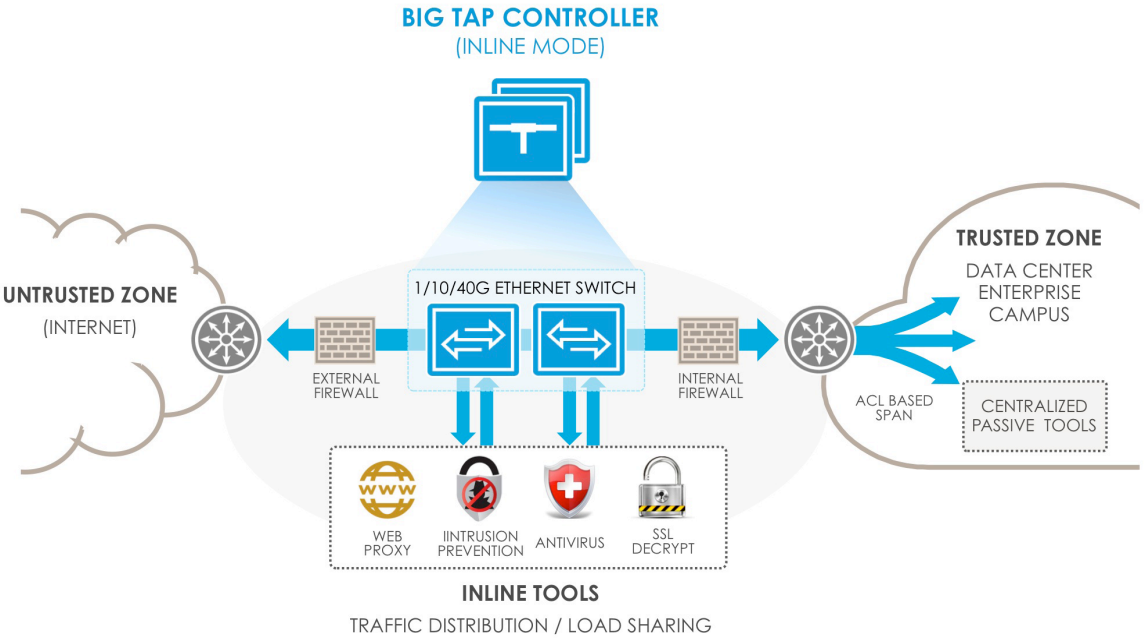


Figure 4: Big Tap Inline—In-band Security & Monitoring Tool Chaining in the DMZ

BIG TAP: INLINE

Network security for organizations has never been more important in light of continued cyber attacks. Additionally, security practices that monitor / secure the network are rapidly changing, as the networks are demanded to provide more services like cloud computing, Big Data, and BYOD.

As a result, it is paramount to design and maintain the high-performance and resilient characteristics of the network, while ensuring that it is compliant and secure against intrusions/attacks. To address these challenges, customers prefer using inline monitoring and security in their DMZ environment. Security tools, by virtue of being inline, can assess every packet and actively prevent or block intrusions that are detected before they can manifest and do the damage. However, inline security architecture poses new challenges in terms of high availability, continued maintenance, and scalability.

Big Tap Inline enables pervasive security in the DMZ and addresses the challenges faced by traditional solutions while offering lower-cost and SDN-centric operational simplicity.

Big Tap Inline consists of a Big Tap Controller and open Ethernet switches deployed in High availability configuration. The inline security tools directly connect (optionally via link aggregation) to these Ethernet switches. Leveraging the Big Tap controller as the central point of management, Big Tap Inline configures policies that create paths through the inline tools. The solution supports load balancing across multiple instances of the same tool as well as chaining of a set of tools on a per-policy basis.

Key Feature Highlights:

- **High Availability Architecture**
  - Highly resilient against network, tool or controller failures.
  - Supports inline Tool Health heck.
- **Tool Chaining**
  - Support chaining of multiple tools. Supports different tool chains for traffic coming into / leaving the DMZ.
- **Tool Oversubscription/Load Balancing**
  - Load balance higher data bandwidth (10G/40G) across multiple instances of lower bandwidth tools (1G/10G).
- **Enhance Tool Efficiency**
  - Send only relevant traffic (as opposed to all traffic).
  - Supports dynamic, programmatic (REST API based) configuration to drop certain marked flows (e.g. DDoS) at the switch. In such scenarios, the fabric switch drops the marked flows, rather than sending the flows to the tool to drop them.
- **Simplify Multi-team operational workflows**
  - Single Pane of Glass management/configuration; No complex, error-prone PBRs needed; Easily load-balance or chain tools.
  - Replicate certain traffic (at line-rate) via a rule-based SPAN to send to offline tools for further processing.
  - The Big Tap Controller is the unified, single point of management for inline / offline monitoring.

BIG TAP MONITORING FABRIC FEATURES

FEATURE	BENEFITS
Network-Wide Visibility (Monitor or 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 open 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 open Ethernet 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 open 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, Telemetry and Analytics	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. • DHCP Tracker: shows which subnets, served by DHCP servers are in the production network. • DNS Tracker: shows which DNS are being used to resolve domain names in the production network. • Sflow Generation: provides clear visibility on the activities in the production network.

DATASHEET

FEATURE	DESCRIPTION / BENEFIT
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, TCP Flags, DSCP matching.
Packet Manipulation Services	• Packet Manipulation services (such as de-duplication, packet slicing, payload obfuscation and time-stamping) can be enabled for the Big Tap by service chaining 3rd party NPBs as service nodes to the Big Tap Monitoring Fabric
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. • Additional 1TB hard disk available • Configurable auto deletion of older pcap files.
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	• 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 Open 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.

ENVIRONMENT	VERSION
Linux KVM	Ubuntu 12.04
VMware ESXi	Version 5.1 U1 Version 5.0.0 U1 Version 5.1.0 U1 Version 5.5.0 U1 Version 5.5.0 U2

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 (BTAP-CTRL-HW, BTAP-CTRL2-HW)

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

FEATURE	TECHNICAL SPECIFICATION
Form Factor (H x W x D)	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

DATASHEET

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

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.

big switch networks

Headquarters
3965 Freedom Circle, Suite 300, Santa Clara, CA 95054

+1.650.322.6510 **TEL**
+1.800.653.0565 **TOLL FREE**

www.bigswitch.com
info@bigswitch.com