big switch networks

SOLUTION GUIDE

Open SDN for Network Visibility

Simplifying large scale network monitoring systems with Big Tap

This solution guide describes how Big Tap, a network monitoring application from Big Switch Networks, simplifies large network monitoring systems. Big Tap works with network packet brokers and security appliances and with application performance monitoring and network performance monitoring tools to deliver a flexible, unified system for large scale monitoring of flow and packet data.

Table of Contents

Large-Scale Monitoring Networks

Networks are, increasingly, the core of our businesses. In many cases, they are more important than phone services—because they carry voice traffic along with email, web, and back-office applications. For some enterprises, the network facilitates business and enables collaboration. For others, the network carries every business transaction. And for still others, the network is their business; providing networks, applications and networked services and even "click-to-compute" environments is a growing enterprise. In each of these cases, a company cannot function without a high-performance network.

Preventing performance issues and outages in such networks is critical to maintaining the pace of business, and, as networks grow, monitoring and managing performance on the network becomes increasingly complex and expensive. Traditional approaches simply do not scale to the needs of modern networks, especially in virtualized datacenter deployments.

Monitoring in Traditional Networks

Historically, monitoring systems have relied on a variety of protocols and a fragmented set of tools. Certainly, analyzing the actual network packets has been part of monitoring systems, but sifting through terabytes of data or even getting access to the data has posed challenges, increasing the time to resolution for many network problems. Networks are replete with tools for analyzing traffic. Adding those tools to network operations is the first step towards operational visibility. In addition to packet data, those tools use any of several meta protocols for providing data about networks, such as SNMP, NetFlow, and sFlow. The problem that remains, however, is stitching these tools to the traffic so that they can monitor and manage in a flexible, cost-effective manner. Such tools include network performance monitoring, application performance monitoring, and security analysis tools, such as IDS/IPS. A second step in the pursuit of network visibility involves an emerging class of systems known as network packet brokers (NPBs). NPBs provide, among other services, tap aggregation, time stamping, and payload obfuscation. Whether the tool is a traditional monitoring system or a security server, getting traffic to these tools is the root of many barriers to more efficient network troubleshooting and problem resolution. Big Tap solves this problem, completing the steps necessary to achieve network visibility.

Delivering traffic to tools efficiently removes the final barrier to efficient network monitoring. For example, while flow data is important in monitoring switches and demonstrating trends and host interdependencies, it only provides limited information for troubleshooting. Troubleshooting is dramatically simplified if filtered packet data is available to network administrators. In the past, when most data center traffic egressed the local site and headed "north" to an external network or came inbound, for example from the Internet, there was an obvious place to tap traffic or install a probe. Monitoring the ports where traffic enters and exits a DMZ or by duplicating traffic on a port used by a load balancer were obvious points to monitor. Similarly, port-mirroring at the top of rack could be used for some applications and in older networks monitoring at the aggregation layer worked as long as the tools could keep up with network speeds and as long as there wasn't contention between tools and teams, for example between the security team and the network team.

Monitoring in a modern data center

In the last several years, three trends have come together to break traditional monitoring models. First workloads became virtualized, so tying monitoring tools to a physical port grew more difficult. Second, performance has increased from 1Gbps to 10Gbps and to 40Gbps and even 100Gbps. These speeds make it difficult to tap at the aggregation layer without specialized equipment and without proliferating tools to every segment where the equipment is deployed. These speeds also make port mirroring impossible to use reliably because the monitoring port becomes swamped and drops packets. And finally, traffic patterns shifted dramatically, from the north-south model, where security boundaries and load-balancers provided an obvious place to capture traffic, to an east-west model where the traffic never leaves the local network and instead is sent to hosts within the data center. In a modern data center, host mobility, performance, and east-west traffic make monitoring more difficult and expensive.

Initial approaches to solving these problems involved aggregating tapped traffic in high performance systems and then forwarding that traffic to monitoring tools. Devices, such as NPBs, often offer additional features, like payload manipulation or recording. Deploying NPBs everywhere the traffic must be captured has proven too expensive, leaving little budget for the tools required to achieve visibility. Similarly, deploying tools to every "silo" within the network is inefficient, especially when multiple instances of tools are required because traffic levels are too high for a single instance to handle. Further, adding aggregation systems and tools sometimes requires repeated waits on maintenance windows, which can delay deployment or require multiple steps because traffic must first be routed around the desired port, then the tap must be added, and then administrator must revert to original routing configuration. These approaches increase the cost of building out monitoring infrastructure and, once deployed, fix the traffic to a single toolset in a static fashion, which can lead to "port contention" and "stove-piping," where information available to one team is hidden or difficult for another team to access.

Evolving Requirements

In today's networks, monitoring systems must include elements that provide packet services, such as time stamping, slicing, de-duplication and payload obfuscation. Monitoring networks must also enable dynamic tapping and address the needs of multiple user groups, and they must combine flow information and packet captures in a unified system, and, a modern system, must achieve port density at a cost that leaves budget for tools. They also need to enable rapid provisioning to get data into the hand of troubleshooting staff quickly, and scale out without introducing silos that "stove pipe" information and unnecessarily hide it from some users. Ultimately, such a system should enable self-service data analysis where a user with the correct permissions can access the data they need to complete a task without requiring a change order from network operations.

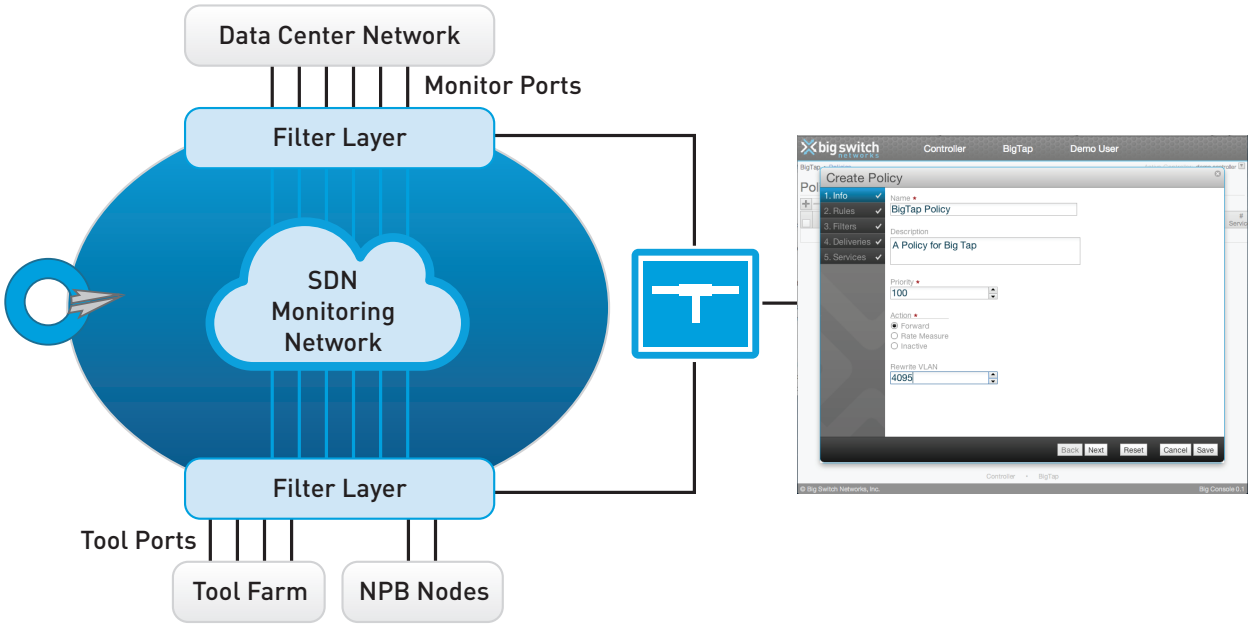

Figure 1: OpenFlow enables a large-scale SDN monitoring network

The requirements for such a next-generation monitoring system can be separated into three layers:

- Filter Layer:
  - Monitor-port termination
  - Drops all traffic by default
  - De-duplication of data
  - Aggressive stats export (NetFlow, sFlow)
- SDN Monitoring Network:
  - Aggregates Flows
  - Forwards to Service Nodes and Delivery Layer
  - Enables policy-based service insertion
- Delivery Layer
  - Stream duplication
  - Flow-aware tool load balancing
  - Policy-based delivery to tools, service nodes, and NPBs

These requirements can only be met through the use of a monitoring SDN, a software-defined network that delivers flow and packet data from filter ports to delivery ports and that can combine multiple delivery ports into a service chain. A service chain enables NPBs and other service nodes to be used selectively and in combination, optimizing the deployments of these systems.

Big Tap: SDN application delivers flexible and unified network visibility

Big Tap, from Big Switch Networks, meets these requirements and enables unified network monitoring, while delivering significant flexibility and visibility to data center network operators. In contrast to traditional port mirroring or tapping solutions, Big Tap can put a layer in front of tap aggregation systems and tools that enables users to achieve a high level of flexibility, and in large scale systems it is dramatically more cost effective than traditional monitoring systems or NPBs alone. Big Tap helps network administrators deliver a monitoring network that works at the pace of a networked business.

A Big Tap deployment optimizes the utility of security monitoring and NPM or APM appliances and filters and directs traffic to meet analytical tool needs. A complement to purpose-built aggregation devices, Big Tap works with OpenFlow-enabled switches and exploits Ethernet switching cost efficiency & performance scalability.

In addition to meeting the needs for modern monitoring systems, Big Tap is a strong candidate for an enterprise's first SDN deployment, because it operates on the monitoring network and can be deployed incrementally. Big Tap can transform OpenFlow-enabled, high-performance Ethernet switches into aggregation devices and work with NPBs to filter and selectively forward network traffic to security and monitoring appliances. Big Tap enhances the functionality of each network security and monitoring appliance by dynamically extending its reach to any traffic flow within the network fabric. Utilizing OpenFlow Ethernet switches from ecosystem partners or a white-box switch running Switch Light for Broadcom from Big Switch Networks, Big Tap can filter ingress traffic flows from any network tap or SPAN port and forward it to an aggregation, security, or monitoring tool over the SDN. Big Tap can program OpenFlow switches to filter through terabits of incoming traffic by source and destination address (L2 or L3) and filter by protocol to reduce traffic rates to monitoring appliances. Big Tap can also replicate traffic to multiple appliances.

Big Tap delivers the flows of interest to the appropriate aggregation appliance and analysis tools, optimizing tool utilization and increasing the scope, usability, and performance of the entire network monitoring system, while dramatically reducing the cost of building monitoring networks. Big Tap is compatible with OpenFlow switches manufactured by ecosystem partners such as IBM, Dell, and Extreme Networks. Big Tap is also qualified with switches based on Switch Light, a thin-switching software platform from Big Switch Networks. As customer networks evolve from 1Gbps, to 10Gbps, to 40Gbps, Big Tap can support the upgrade and replacement cycles as new data plane elements are added to the Open SDN, allowing security and monitoring to scale directly with the network.

Simplified Network Monitoring with Role-Based Access Control

Rolling out Big Tap simplifies network monitoring and achieves network-wide visibility more cost-effectively than traditional approaches. In a Big Tap deployment, the network is configured to forward a wide range of traffic from monitoring ports to an OpenFlow based filtering layer. This filtering layer drops traffic by default. When monitoring is needed, whether to troubleshoot a specific problem or to, for example, record all traffic of a certain type, a user simply logs in and subscribes to the required traffic. A user who needed to monitor web traffic to investigate and resolve a particular problem signs in and defines a policy such as, "steer port 80 traffic to an APM tool for analysis." With Big Tap, this is as simple as signing in to the Big Tap console or Big Tap GUI and then defining the source of the traffic, the required filter, and the desired destination.

Support for role-based access control and user-specific rules ensures that only the traffic of interest to a particular role is available to a user. These "User View" privileges are mapped out by the Big Tap Administrators and can include the following properties:

- Filter switches/ports
- Delivery ports
- Service ports
- Match rules on IP subnets, Host, TCP/UDP Ports, MAC

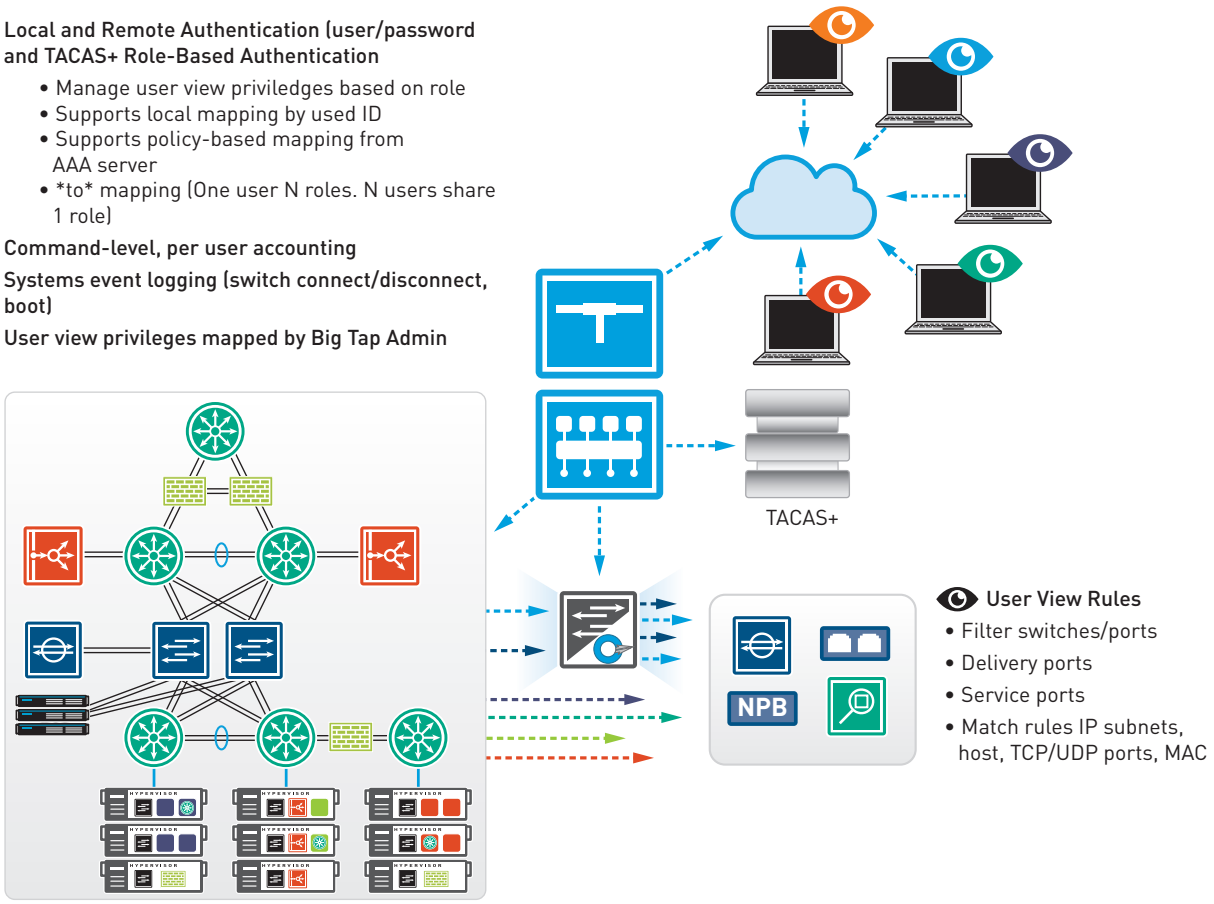

Figure 2: RBAC and user views enable multitenant network monitoring

A broad and systematic use of Big Tap might involve filtering SSL traffic from a particular web application, steering it to a decryption service and then to a recording device. The process for defining this service chain is similar to ad-hoc analysis. The user signs in and defines the traffic they need to send to the host or physical port where the decryption device receives traffic. The user would filter on port 443 and define a delivery port by IP. Then the user

defines a policy for the port from which the decryption device sends the clear-text traffic. This additional policy will cause the switch to send the traffic to a recording device. This policy, too, would require that the role-based access controls allow the user to access these resources.

Big Tap, the OpenFlow-based SDN monitoring network, works according to the policy:

1) The filter layer drops packets by default
2) A user-defined policy installs a Flow Filter on a filter port
3) The required traffic is forwarded through the SDN Monitoring Network
4) The traffic of interest is delivered to the right tool or device.
5) If a subsequent rule chains the traffic, so it can be processed by a network packet broker or another service node, then traffic entering the SDN monitoring network is transported and delivered to the correct device until the service chain is exhausted.

A Big Tap-based monitoring SDN can accept traffic from SPAN ports or probes or TAPs. The SDN-based monitoring network can consist of a single switch to start and can scale out to a multi-tier network consisting of hundreds of filter ports and thousands of delivery ports.

In an Open SDN-based monitoring network, statistics and flow information can be effectively combined with packet data through automated events that use the available REST API. For example, when a web flow for a certain application crosses a specified threshold within one tool or service node system, the filter policy or service chain can be modified dynamically, to deliver more or less or different traffic to other devices. This example of flexibility and scale demonstrates how Big Tap helps to bind monitored flows and packet data to the available tools and NPBs efficiently and without requiring that tools or NPB systems be brought to every location where traffic might need to be analyzed.

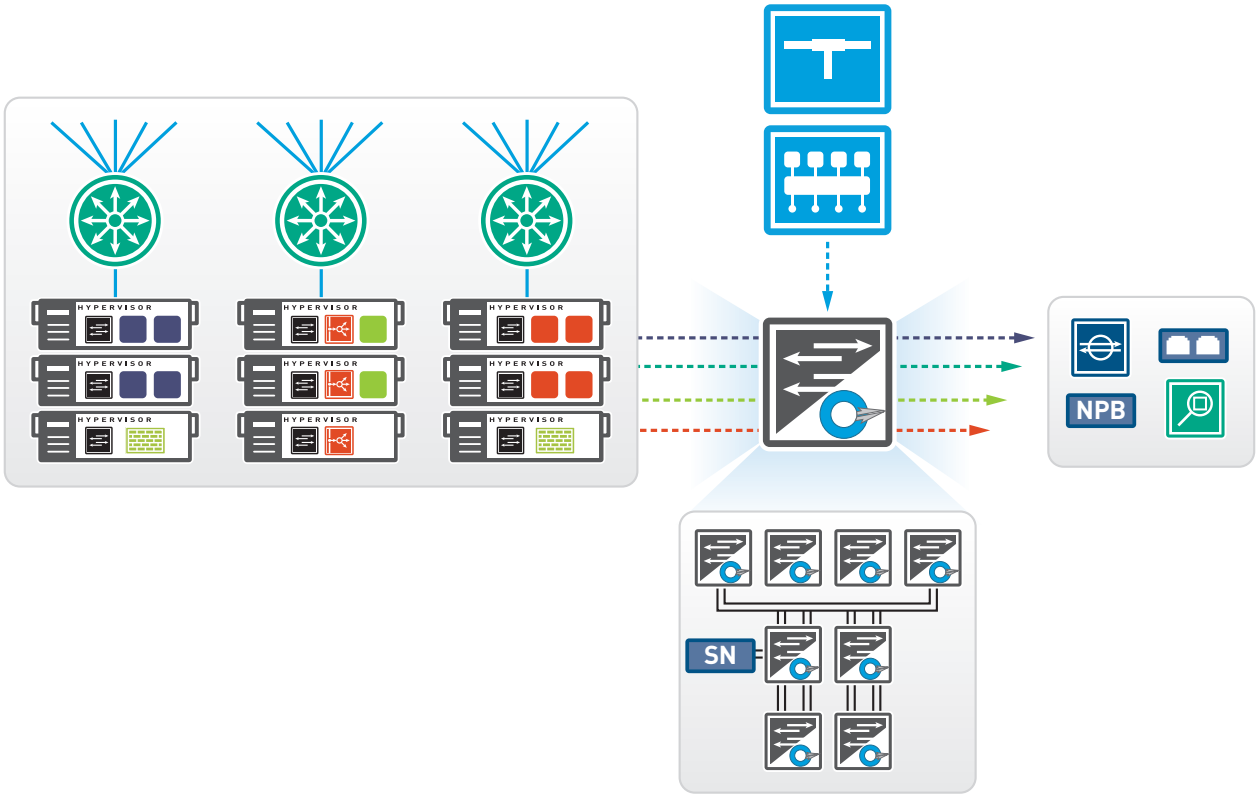

Figure 3: Big Tap simplifies statistics monitoring, flow tracing, and active tapping with an Open SDN.

Big Tap can bring together application owners, developers, and operations staff and enable them to collaborate more effectively by creating a monitoring SDN based on virtual switches and OpenFlow physical switches. By delivering the right traffic to the right tool at the right time, Big Tap enables a cost-effective approach to pervasive visibility. Because Big Tap enables teams to do more with less, staff can more effectively reduce mean-time-to-resolution for problems, while avoiding contention between teams and between traffic-aggregation budget and NPM or APM tools budgets. A monitoring SDN that uses Big Tap in combination with TAP infrastructure and analysis tools can increase security and simplify maintaining compliance by ensure that NPBs remove personal information from packets. Big Tap optimizes the use of NPBs and delivers improved availability and responsiveness. A monitoring network that includes Big Tap enjoys accelerated troubleshooting, while minimizing downtime during problem resolution. Whether your network team is supporting a transactional data center deployment, building out a "click-to-compute" system, or managing an enterprise network that supports converged services, including voice, email, web, and back office, Big Tap meets emerging requirements and delivers a next-generation monitoring network.

About Big Switch Networks

Big Switch Networks is the leader in open source Software-Defined Networking (SDN) products, delivering unmatched network agility, automated network provisioning, and dramatic reductions in the cost of network operations. The company's Open SDN™ platform offers an OpenFlow switch fabric that can run on bare metal switches and hypervisor virtual switches, and enables a wide variety of SDN network applications including data center network virtualization and network monitoring. 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

SG012-02 July 2013