# Optimizing at the Service Layer

Service providers that build and operate networks as a business have long known that one of the best ways to attract and retain customers is to offer high-levels of service in terms of availability, reliability, and performance – all while keeping expenses low and operations efficient. As such, there is a constant need to get more from the network including optimizing the flow of high-demand traffic. But where it was previously sufficient to engineer traffic at the network-layer agnostic of content or applications, with the continued trend towards cloud and content delivery infrastructure, it's more important than ever to take a service-layer approach to traffic engineering.

## Challenge

Traffic Engineering begins with measuring traffic volumes along various paths throughout the network from the perspectives of the infrastructure that makes up those paths. And optimizing traffic for optimal service and application experience starts with service-layer traffic visibility. But for the most part, core network equipment or infrastructure has little to no service or content awareness. Of course, we can 'instrument' application or service visibility in certain pinpoints in the network. But to optimize the network and network infrastructure, we need to see service traffic at all the points where we need to make optimizations, even if it is at every individual router. As such, most service providers struggle extracting service-layer visibility from infrastructure-centered measurements.

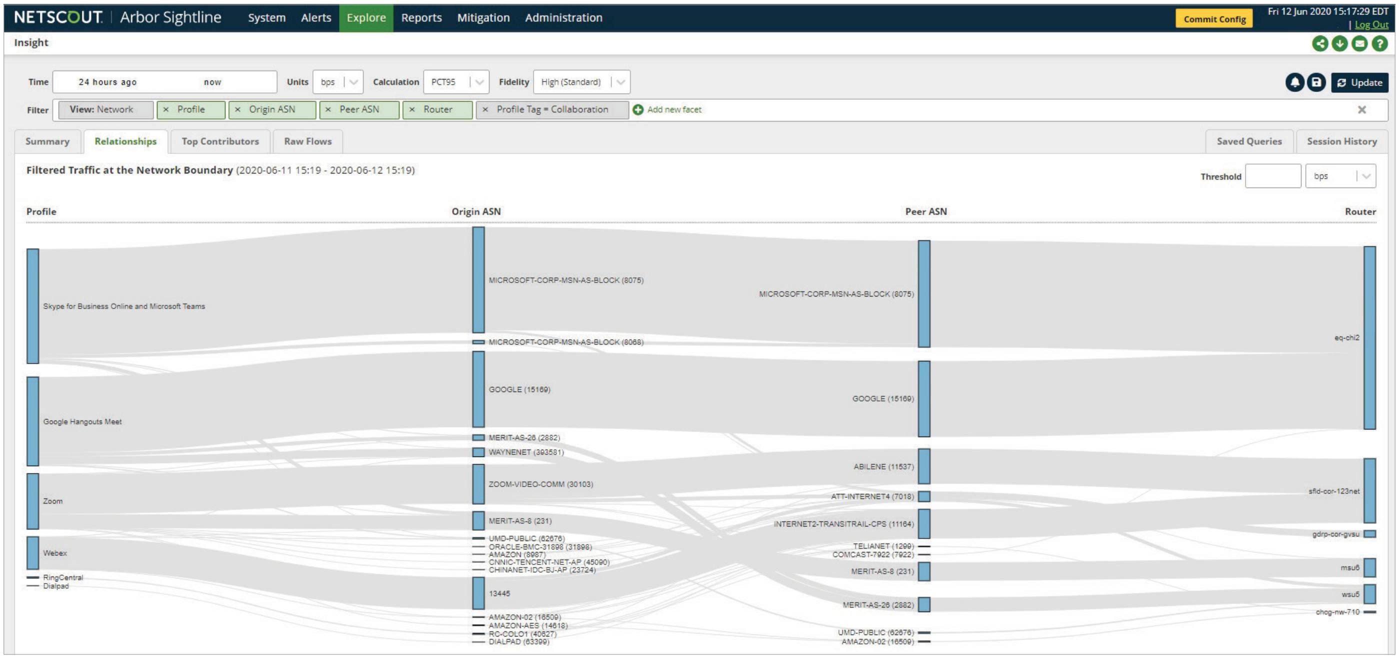
## Risk

Long gone are the days when users would access the internet largely to send email or shop online. Today most users are accessing the internet for everything from social networking, video and music streaming, and even using all manner of applications (SaaS). This makes access to the internet as critical to modern life as electricity and sets the bar for user experience very high. When a service provider fails to maintain high levels of service connecting users to content and applications on the internet, users do not just get frustrated, they start looking for alternatives. So it is not enough to conduct generic traffic engineering, it must be done with service-layer awareness to detect and prevent degradation to the most valued and most critical services.

## Solution

We need sources of network telemetry that are pervasive providing the broadest, most complete coverage as well having minimal impact on the network itself. But also, we need sources of network telemetry that captures the service layer and the content awareness that comes with it. Rather than looking for a single source that captures all the necessary attributes, it could be sufficient to identify separate sources that each excel at one attribute and then analyze the sources together with an eye towards correlating all the attributes for a composite perspective.

The best source of pervasive network telemetry is NetFlow, the forwarding digests exported by most routers. NetFlow's primary metric is volume, both bits-per-second and packets-per-second. This volume measured at various routers along the many paths through the network gives us both network capacity and traffic consumption allowing us to identify where and when the network is exhausted as well as where room remains available for use. But NetFlow goes beyond this by also providing a range of transactional attributes, including IP addresses, protocol, and ports, to help distinguish traffic and provide powerful correlations of meaning with volume.



Time: 24 hours ago – now
Units: bps
Calculation: PCT95
Fidelity: High (Standard)

Filter: View: Network | × Profile | × Origin ASN | × Peer ASN | × Router | × Profile Tag = Collaboration | Add new facet

**Filtered Traffic at the Network Boundary** (2020-06-11 15:19 - 2020-06-12 15:19)

Threshold: bps

**Figure 1: Here we can see a variety of conferencing and collaboration services, their respective originating networks, what peers they use to reach our network, and finally the border routers receiving that traffic.**

One of the most ubiquitous sources of application or content telemetry is recursive DNS. Whenever a user types a URL in a browser or launches an application, a DNS transaction precedes any transfer of traffic over the network. DNS also provides that content-identifying domain name as well as the IP addresses used to reach it. Using the IP addresses from DNS as a mapping key with NetFlow allows us to correlate traffic volume with the application that triggered it, or the content contained within.

Correlating DNS with NetFlow is the ideal method for bringing service-layer visibility to network traffic analysis, and when combined with other network data sources, such as BGP for topology awareness and SNMP for infrastructure awareness, allows service-layer oriented traffic engineering to be conducted by finally achieving content awareness.

Arbor Sightline is the premier NetFlow collection and analysis platform designed from the start not only for complete DDoS attack detection and defense but also for comprehensive network visibility and traffic analysis. Sightline's NetFlow processing pipeline scales to the largest intercontinental networks as well as provides a thorough break-down of all the primary traffic attributes allowing for a variety of correlations bringing immediate and practical meaning to volume-based traffic analysis. Sightline also directly connects with routers via BGP allowing Sightline to see and understand the forwarding paths as the routers see them and how traffic will follow those paths not only when exchanging with adjacent networks but also across the internet. Utilizing these key traffic and data inputs, Sightline presents actionable traffic engineering clearly identifying the various routers and interfaces across the network as well as their traffic capacity and utilization over time. This enables not only identification of immediate service degradation due to capacity exhaustion but also shows traffic growth over time so similar exhausting events can be detected early and prevented.

Arbor Sightline With Sentinel enables the integration with NETSCOUT® InfiniStreamNG®, the leading packet-capture and service-assurance technology, and provides DNS transactions used by Arbor Sightline to achieve service-layer visibility.

Arbor Sightline With Insight is the big-data powered, advanced-analysis technology that maximizes the correlations among the various dimensions of traffic. It elevates traffic engineering to the next level and helps peel back the layers of ambiguity plus reveals the content and applications within the service-layer as well as how they relate to routing topology and network infrastructure–all at the same time.

## Summary

Arbor Sightline With Sentinel and Insight take the legwork out of collecting and analyzing traffic and routing data plus takes the guesswork out of bringing in service-layer visibility into traffic engineering, thus puts the service provider in the best position to excel and succeed.

NETSCOUT.

**Corporate Headquarters**
NETSCOUT Systems, Inc.
Westford, MA 01886-4105
Phone: +1 978-614-4000
www.netscout.com

**Sales Information**
Toll Free US: 800-309-4804
(International numbers below)

**Product Support**
Toll Free US: 888-357-7667
(International numbers below)

NETSCOUT offers sales, support, and services in over 32 countries. Global addresses, and international numbers are listed on the NETSCOUT website at: www.netscout.com/company/contact-us