TERIDION

A Teridion Technical Paper

How Teridion Works

A Technical Overview of the Teridion Virtual Network

Teridion Engineering

February 2017

Introduction

Sub-second application response time is an important but often unrealized goal for SaaS providers. Everyone knows that application responsiveness is directly linked to user productivity. However, inconsistent Internet performance makes response times of over 5 seconds typical, particularly for end users who are located far from the application's data center.

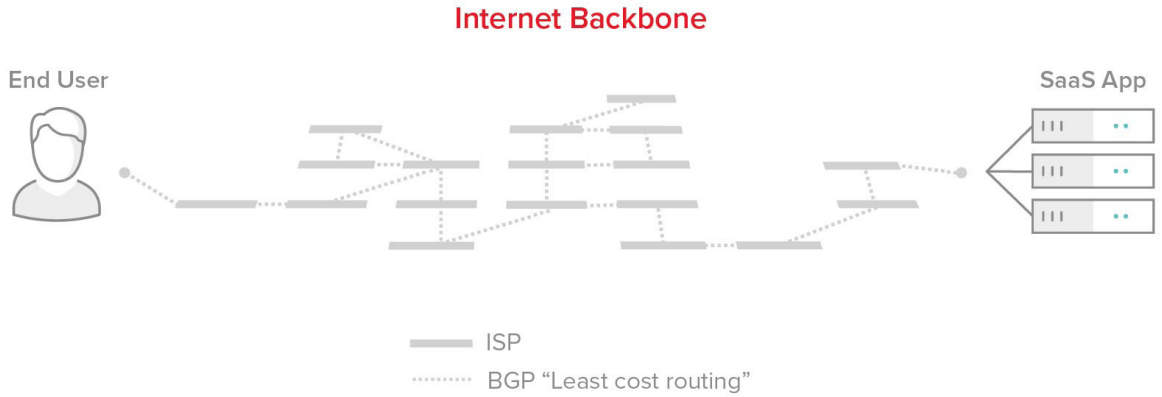
> "When a computer and its users interact at a pace that ensures that neither has to wait on the other, productivity soars"
>
> **IBM RESEARCH**
> 1983

With Teridion, SaaS providers are now able to take back control of their application's performance to deliver the best possible user experience. This paper describes how the Teridion Virtual Network works and how it solves the "Internet Backbone Problem" to deliver better performance and ROI.

The Internet Backbone Problem

What is the Internet Backbone?

Nearly all web content flows through the Internet Backbone. The Internet Backbone is made up of many large Network Service Providers which interconnect with each other. These large networks charge ISPs to transport data packets long distances.



How Least Cost Routing Hurts Performance

Within the Internet Backbone, there is no mechanism for SaaS providers to pay ISPs more to deliver traffic faster. Thus the only way for an ISP to maximize profitability is to minimizing the costs of sending traffic. Least cost routing is the process of selecting the path traffic will take along the Internet Backbone based on the lowest cost, not on performance.

Least cost routing happens as a result of rules that are baked into Border Gateway Protocol (BGP), the routing protocol of the Internet Backbone. These BGP rules allow providers to prioritize traffic using cost-based weighting factors. This puts the customer experience for SaaS providers at the mercy of the network providers cost-cutting routing tables.

How BGP Hurts Performance

BGP is what network providers use to route data from their own machines to others, and vice versa. When you visit a website, that data traverses networks all over the world, through machines belonging to many different organizations. In order to ensure that data transmissions eventually get to their intended locations, Internet Backbone routers keep a table of known, trusted routes.

The negative performance impact to SaaS providers of the Internet relying on BGP is that the protocol's rules for moving traffic between networks (called EBGP) dictate that traffic between two points will always take the same path regardless of network congestion. The combination of least cost routing and lack of congestion detection explain much of the performance problems on the Internet Backbone.

How TCP/IP Hurts Performance

Among routing protocols, BGP is unique in using Transmission Control Protocol (TCP) as its transport protocol. TCP/IP provides the Internet with reliable, ordered and error-checked delivery of data between two systems. By design, TCP/IP is optimized for accurate delivery rather than timely delivery. Thus TCP sessions can incur long delays (often for seconds) while waiting for out-of-order messages or retransmissions of lost messages. For this reason, real-time applications like VOIP opt to use different protocols.

For SaaS providers, this means that the TCP/IP data transfer algorithms are not efficient, particularly for larger files which require many round trips to transmit. TCP/IP requires each chunk of data to be acknowledged by the receiver before the sender sends the next batch

of data. Since these data chunks are typically small, typically a thousand bytes, it means that transferring even 1 MB of data can require hundreds of separate trips through the Internet Backbone.

Teridion Solves the Internet Backbone Problem

Teridion opens up a fast lane through the Internet that gives the end-users of SaaS providers sub-second application performance around the globe. Teridion's Virtual Network routes traffic around the congested networks in the Internet Backbone eliminating the need for workarounds. This in-turn reduces the cost and complexity of application, storage and networking infrastructure.

How Teridion Works

Teridion's Virtual Network intelligently analyzes the Internet Backbone to find the fastest routes between any two endpoints, avoiding congestion and overcoming the performance problems caused by least cost routing. In the process it delivers 20x better data transfer performance. Teridion is deployed across public clouds and delivered "as-a-Service," so there is no hardware or caching to configure.

How Teridion Complements CDNs

Content Delivery Networks (CDNs) are distributed servers that serve cached content to users based on their geographic location. CDNs are excellent for serving static content to users near the CDN Point of Presence (PoP), but do not handle dynamic data that must created "on the fly," nor can they accelerate uploads or bi-directional data transfers.

CDN caches help end users avoid having to request content from the origin. Teridion Virtual Networks accelerate content requests from the origin. Both approaches improve the end user experience.

Teridion excels at accelerating uploads and dynamic content, making Teridion a natural complement to CDNs within a SaaS application architecture. Teridion can complement a CDN in several ways:

- **Accelerate dynamic or uncacheable content:** Teridion does not require the replication or synchronization of data at the edge to PoPs. Instead, Teridion accelerates the data to the end-user directly from the origin server.
- **Meet stringent regulatory requirements:** Replicating content across a global network of CDN caches may conflict with financial regulations, EU data residency laws and Chinese Internet Content Provider licenses.
- **Support security requirements:** CDNs cache unencrypted static content in many locations, breaking the chain of custody for security conscious SaaS providers and opening up potential security vulnerabilities.

How Teridion Complements SD-WANs

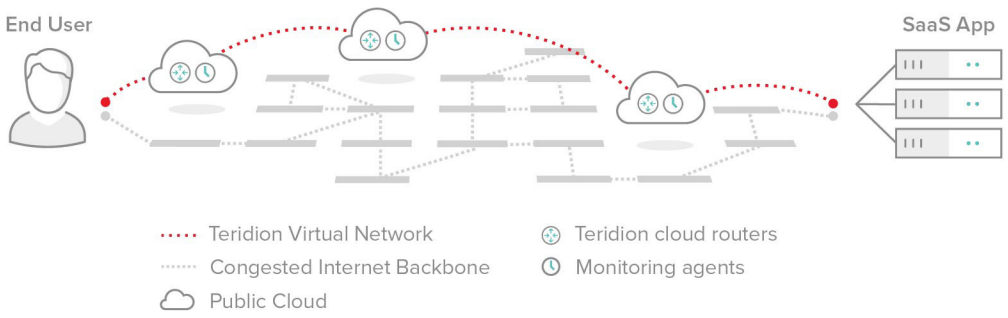
Software-Defined Wide Area Networks (SD-WANs) optimize internal point-to-point business communications between central and branch offices. Teridion is able to deliver private network quality of service over the public internet at a fraction the price of traditional leased line solutions like MPLS. Teridion can add value to a traditional SD-WAN deployment in several ways:

- **Remote Office Workers:** Teridion improves networking to remote workers in small regional offices where an SD-WAN may not be cost effective.
- **Mobile Workforce:** Teridion can improve network performance for corporate mobile users anywhere in the world.

Teridion Architecture

Teridion's virtual network is comprised of three components deployed globally across hundreds of public cloud data centers:

- **Teridion Monitoring System (TMS):** Orchestrates virtual agents that are constantly calculating the fastest path between for every route.
- **Teridion Cloud Routers (TCR):** Virtual router VMs that direct traffic along the fastest paths (calculated by TMS) and using the most efficient algorithms.
- **Teridion Portal:** A network administrator UI for monitoring traffic and troubleshooting connectivity issues.



Teridion is unique in leveraging public cloud infrastructure to provide optimal routing across the Internet backbone. Other Internet overlay providers are trapped in expensive and inflexible private clouds. Teridion takes advantage of the scale of public cloud investment in both location and in peering relationships with local ISPs. Teridion also has an advantage of neutrality over public cloud vendors in being able to pick the optimal cloud providers for each region.

Teridion Management System

The Teridion Management System (TMS) is a centralized orchestration service that automatically operates Teridion Virtual Networks. The TMS is responsible for finding optimized paths and providing management APIs for configuring virtual networks.

The TMS gets performance data from Teridion Measurement Agents (TMA) which are installed in each of the hundreds of public clouds that Teridion operates in. These agents performs real time measurements of Internet performance between other data centers and send that data to the TMS.

These Teridion orchestration components operate in the control plane and have no access to the data flowing through the Teridion Virtual Network. The TMA is written Scala to enable the real-time parallel processing of large numbers of data events.

TMS is architected according to a number of cloud best practices, including:

- **Multi-cloud:** TMS can deploy virtual networks across over a dozen cloud providers and hundreds of cloud data centers.
- **Elastic scaling:** TMS orchestration automatically scales up and down TCR VMs based on real time demand for each region
- **Resilient:** TMS can detect and recover from a number of failure scenarios, including DNS, network and data center outages.

Teridion Cloud Routers

A TCR is a virtual router that runs on public cloud Linux VMs. TCRs take advantage of public cloud peering relationships with local ISPs to provide a fast "on-ramp" to the Internet Backbone for end users anywhere in the world.

The TMS orchestrates deployment of sets of TCRs in the public cloud to create a Teridion Virtual Network. TCRs are dedicated to a particular SaaS providers virtual network and do not cache or store network content. DNS CNAME redirection is used to map a particular origin server target to a Teridion Virtual Network.

Each TCR VM performs network monitoring to detect and recover from network interruptions. TCRs support multiple protocols (TCP, UDP, SIP, FTP, SFTP) and can use service chaining to add additional protocols and services. For example, TCRs can be configured to capture Teridion SessionFlow data which provides end-to-end visibility into how content moves across the Internet.

Teridion's Approach to High Availability

Teridion was designed as a self-healing network that is resilient to a wide range of potential outages, including problems affecting entire data centers or regions.

DNS provider failure: Every Teridion Virtual Network has multiple Domain Name Server (DNS) providers. If one provider fails or slows significantly, Teridion will switch to a secondary DNS provider.

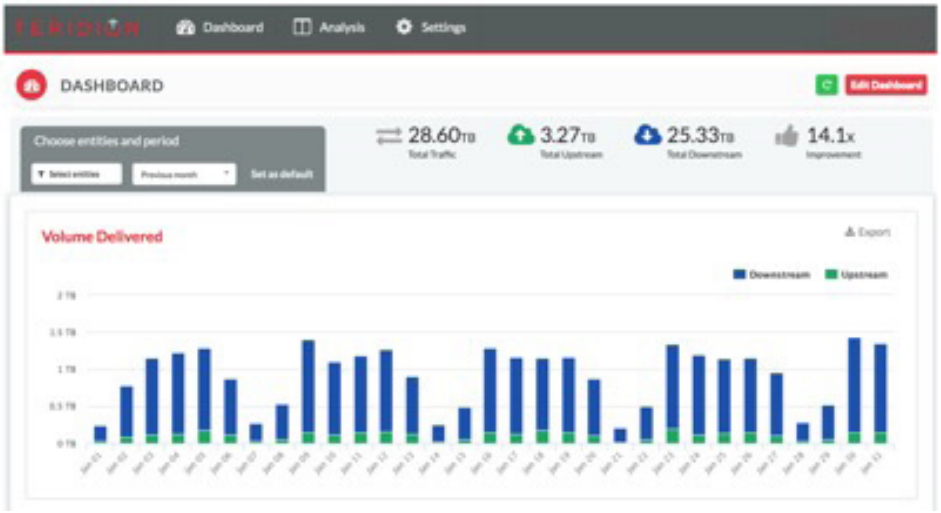
- **Network failure:** The TMS automatically reroutes traffic in response to any network congestion, including data center or network failures. This makes Teridion more reliable than dedicated MPLS lines for large outages.
- **TCR edge failure:** TCRs are constantly monitored and unresponsive TCRs are automatically removed from a virtual network.
- **TCR core failure:** The TMS automatically sets edge TCRs to route directly to the origin server if core TCRs become unavailable (for example through a data center outage).
- **TMS failure:** a TMS failure will not affect the Teridion Virtual Networks, however automated routing adjustments to avoid congestion will stop until TMS is back online. Every element of TMS is replicated for high availability and mirrored for disaster recovery.
- **Teridion Portal failure:** Teridion's network performance is unaffected by the availability of the Teridion Portal.

Teridion Portal

The Teridion Portal enables network administrators to view and analyze traffic flowing through the Teridion Virtual Network. There are two main tabs:

- **Dashboard:** Shows performance and state of your traffic flowing through the Teridion Virtual Network.
- **Analysis:** Provides in-depth analysis and comparisons of traffic flows through the Teridion Virtual Network.

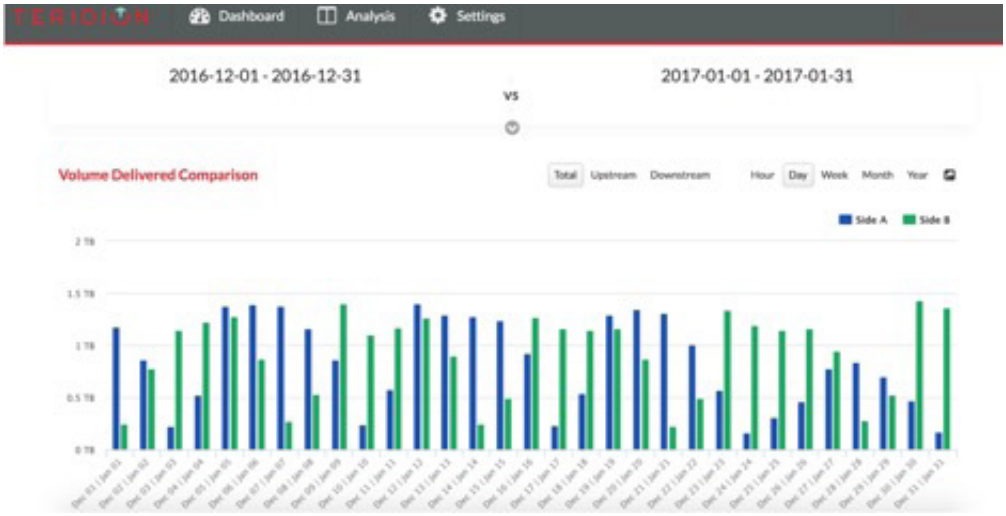
Dashboard Tab



The Teridion Portal Dashboard tab is customizable and includes programmable widgets that display upload and download traffic by time period, by region and by end user domain. For each widget, the dashboard can also show the performance improvement between the Teridion Virtual Network and the standard Internet.

To validate performance improvements, Teridion uses a third party web monitoring service to measure performance, latency and throughput for both the standard internet and the Teridion Virtual Network. This service compares end user performance from ISPs around the globe and the presents the results through the Teridion portal.

Analysis Tab



The Analysis tab shows traffic delivery and performance across time periods. For example, this can be used to compare traffic volumes delivered over several months.

Teridion SessionFlow Data

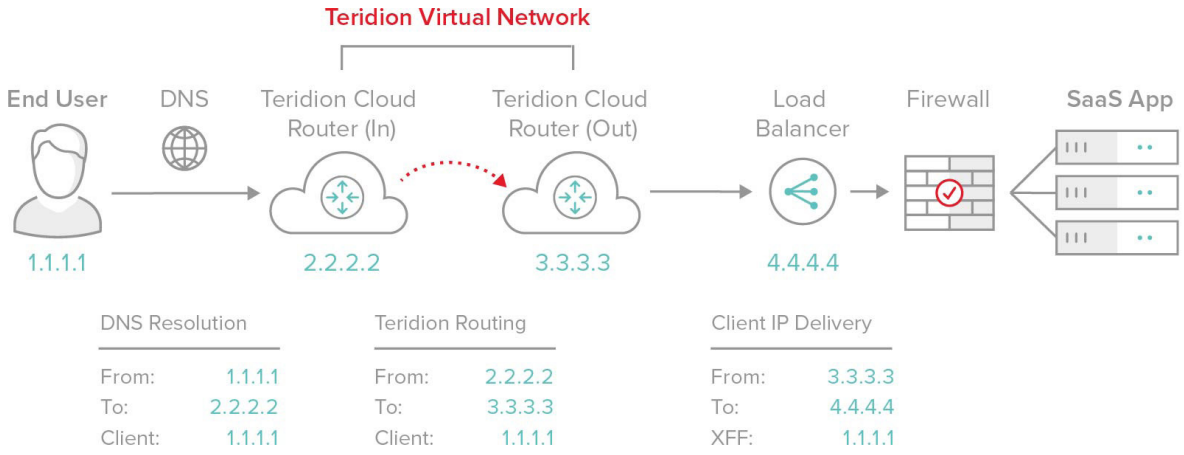
SessionFlow data is newly available in Teridion version 2.0. This structured data output provides network administrators with end-to-end, real-time visibility into their Internet traffic. SessionFlow provides a fast way to pinpoint network connectivity and throughput issues. The following is sample SessionFlow output:


```
"session-info": [
        {
            "domain-name": "dlnyc.teridion.com",
            "end-time": "2017-02-02T09:37:22Z.307ms",
            "hop-location": "IN",
            "hop-order": 1,
            "in": {
                "incoming-bytes": 205815,
                "incoming-throughput": 72435,
                "outgoing-bytes": 22646470,
                "outgoing-throughput": 7970250,
                "read-idle-time-ms": 22789,
                "retransmits": 0,
                "rtt": 60,
                "termination-type": "FIN Sent",
            },
            "ip": "5.102.254.127",
            "next-hop": "3e7bc2-digitalocean-ams2-roni2-n.teridion.work",
```

With SessionFlow data, network administrators can diagnose and troubleshoot traffic in real-time. SessionFlow data includes latency and throughput at each TCR location. The TCR data is sent asynchronously to a cloud storage location chosen by the SaaS provider, for example Amazon's S3 service.

Teridion Reference Architecture

Teridion carries content along a virtual network of TCRs, so Teridion looks to the rest of the network like any other network proxy - such as a load balancer, SSL offload or CDN cache. The end user connects to a TCR, which then routes that traffic along the virtual network to the origin server. Because TCRs act as network proxies, the connection request that reaches the origin server will have the IP address of a local TCR, referred to as a "TCR Out".



The Teridion Virtual Network uses Proxy Protocol to give the load balancer at the origin connection information from the end user requesting a connection to the origin server. The load balancer then adds connection information to the `X-Forwarded-For` headers of each TCP request such as the source IP address, destination IP address, and port numbers.

The following is an example of the Proxy Protocol format for IPv4. This format gives client IP, proxy IP, client port and proxy port, each separated by a single space):

```
PROXY TCP4 198.51.100.22 203.0.113.7 35646 80\r\n
```

Getting Started with Teridion

Teridion accelerates traffic from an end user to an origin server by using DNS to redirect traffic across a Teridion Virtual Network. Before implementing Teridion, there are several network considerations:

- **DNS:** Confirm that you have the ability to add a CNAME to your DNS configuration to redirect traffic to the Teridion Virtual Network.
- **Whitelist:** Teridion will provide you with a list of the TCR IP addresses which make up your Teridion Virtual Network along with an api and process for making changes to that list. Confirm that can add TCR IPs to your firewall whitelist and can provide these IPs to customers with firewalls.
- **Client IP:** Confirm that your load balancer supports Proxy Protocol or that you can add a device or service that provides this support.
- **XFF:** Confirm that your Intrusion Detection System (IDS) and web application can obtain client IP information from the X-Forwarded-For header.
- **Security:** Teridion does not access or store network content, nor does it require SSL certificates. This makes Teridion a good choice for SaaS vendors who wish to maintain full control of their encryption and security workflows.

Onboarding a web application to use the Teridion Virtual Network involves three basic steps:

1. **Redirect DNS:** Create a CNAME record to redirect the origin URL to the Teridion Virtual Network.
2. **Whitelist TCRs:** Ensure that the origin firewall whitelists TCR IPs.
3. **Forward IPs:** Use the load balancer proxy protocol to pass client IP addresses from the Teridion Virtual Network to the origin server.

Teridion APIs

Teridion's customers are also able to access metrics and data about their traffic via a documented REST API. The key benefit of the API is that it allows developers to

programmatically access the metrics and data and feed it to whatever third-party reporting, analytics or business intelligence software of their choosing.

Licensing and Pricing

Teridion deploys one or more virtual networks for each customer and URL it accelerates. The Teridion virtual network is priced with a flat monthly fee for the network itself and a variable fee per gigabyte of traffic passed through the network. For a specific pricing proposal, contact sales@teridion.com.

Next Steps

- Start a FREE Trial: Contact us.
- Questions: Contact us.
- Case Studies: Learn how SaaS providers are succeeding with Teridion
- Datasheets: Learn more about Teridion
- Whitepaper: “Internet Backbone Problem”