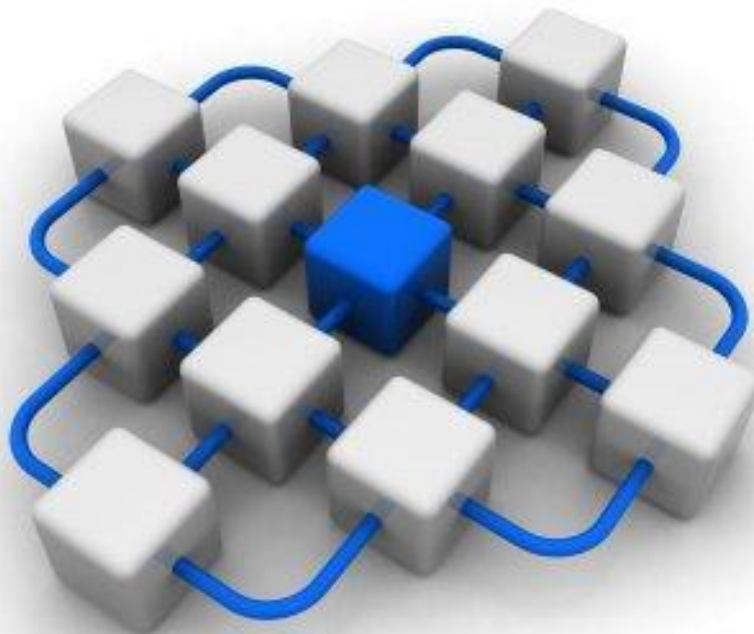


riverbed®

Think fast.™

## Network Performance Management Comes of Age



*Riverbed Cascade is a new type of tool that incorporates traffic monitoring, packet capture and protocol analysis to provide an application-aware view of the network. Now you can see the path of applications as they traverse the network, and get a user's eye view of availability and performance. Mapping the application path through the network and measuring performance along the way helps you solve current problems, analyse trends and plan future network or application changes*

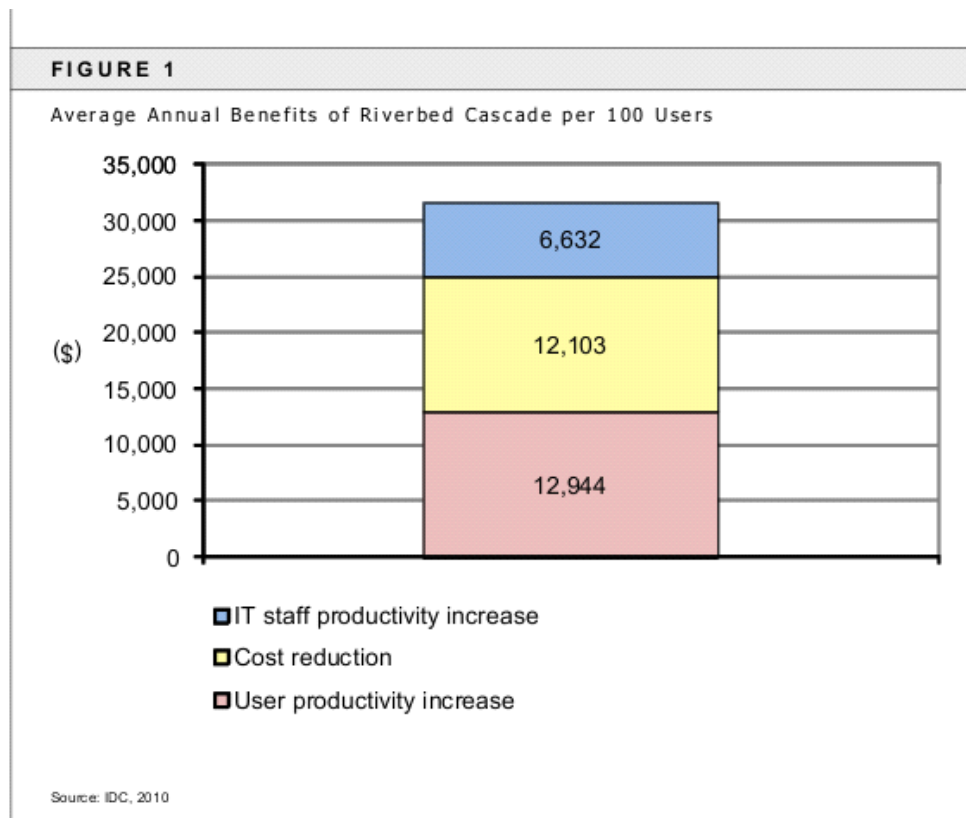
# Introduction

## *Why you need performance management*

As an IT or network manager, you know that what matters is the productivity that users get from your IT systems, and that this in turn depends on your entire infrastructure performing well. You may have various statistics and metrics available for measuring the network and the systems, but at the end of the day users don't care about the metrics as such; they really perceive IT performance in terms of application availability and application performance.

And the more that companies deploy VoIP, explore cloud-based services, or consolidate and virtualise data centres to deliver applications to remote offices from a centralised point, the more network professionals are called upon to improve application performance.

So what the network manager really needs to know about is application performance, whether it be to help developers understand what will work on a network, to spot poorly performing applications before users feel the effects, or to deliver LAN-like performance over the WAN to branch offices and remote locations.



Old-style network management tools typically cannot help here. They are designed to track availability and faults, sending alerts if a service or device is unavailable, or if a pre-defined threshold is missed, but they cannot readily detect problems and interactions at the application level.

Riverbed Cascade is a new type of tool that incorporates traffic monitoring, packet capture and protocol analysis to provide an application-aware view of the network. Now you can see the path of applications as they traverse the network, and get a user's eye view of availability and performance. Mapping the application path through the network and measuring performance along the way helps you solve current problems, analyse trends and plan future network or application changes.

## Collecting and analysing data on your network

Network data collection has become much more efficient with the widespread deployment within network devices (such as switches and routers) of flow protocols for traffic monitoring. Examples include Cisco's NetFlow protocol and similar protocols such as the IPFIX (Internet Protocol Flow Information eXport) standard, sFlow and others. These protocols export flow records containing information about the traffic going through the given device, sending the records to a collector device for analysis.

Flow records give a broad picture of the network while using minimal resources. However, they do not contain detailed application information, and some performance metrics must be collected from directly from the packets. With Cascade, you get the best of both worlds: flow records for a wide view across the WAN, and packet capture for deeper metrics at strategic locations on your network. All this data is combined into a single data set that a user can navigate and query without worrying how a particular piece of data was collected.

Even then, simply calculating network performance metrics is not enough: you also need to know how and when these metrics deviate from the norm – and that norm could involve daily, weekly or even longer cycles. If you can't readily detect deviation from the norm, you cannot track the degradation in performance before services fail and users feel the effects.

Using advanced behavioural analysis, Cascade performs this task automatically. It calculates performance metrics, such as response time and throughput, tracks these metrics over time – even learning automatically which events happen on a daily or weekly basis – and alerts you whenever they deviate from normal behaviour.

In effect, behavioural analytics takes existing tasks that network managers undertake every day, such as monitoring traffic and bandwidth consumption, and enhances them by applying automated learning that can measure performance, troubleshoot application slow-downs, and spot security threats. The best place to see application problems, which can otherwise be a mystery to solve, is in the data on the wire: once you know how to read the traffic – and that is what Cascade does for you – you can see what is really happening to the application.

#### **Case Study: Sappi**

*Sappi needed a solution for monitoring application performance and troubleshooting problems, and chose the Riverbed Cascade executive dashboard for this purpose. This allows Sappi to set service level agreements for application performance, and gives its executive team an easy way to track them. The dashboard uses the traffic light system to show that systems are either working well (green) or need investigating (amber and red). Sappi's network team will then use Cascade to drill down to identify the problem and resolve it.*

Cascade also plots application and network status on service dashboards, enabling anyone from business executives to IT administrators to spot problems and track breaches of service level agreements (SLAs). Once you know about a problem, you can drill down to the name of the application, the server and the user, and troubleshoot the problem all the way down to the packet level.

The network information collected by Cascade is useful not just for analysing current problems, but also for planning for the future. You can use the information to discover applications and servers and identify dependencies within the IT infrastructure – all with an easy-to-use, graphical display. This can be a vital tool when it comes to planning IT projects – server consolidation, virtualization and cloud projects, say.

# How Cascade works and how it enables IT performance

The ability to pull together information from across the network, plus the ability to automatically correlate it and map its behaviour over time, enables Cascade to successfully address five significant areas in network management:

- Proactive monitoring of application and network performance, with alerting;
- Troubleshooting, with the ability to drill down from the high-level status alert and analyse a problem at the server or even the packet level;
- Discovery and dependency mapping, detecting which systems and applications are using the network and how they relate to each other;
- WAN optimisation, working as a complement to Riverbed Steelhead, analysing and assessing performance problems and determining what needs to be optimised and where; and
- Security, detecting network attacks and abuse, and finding potential problems, by looking for anomalous behaviour.

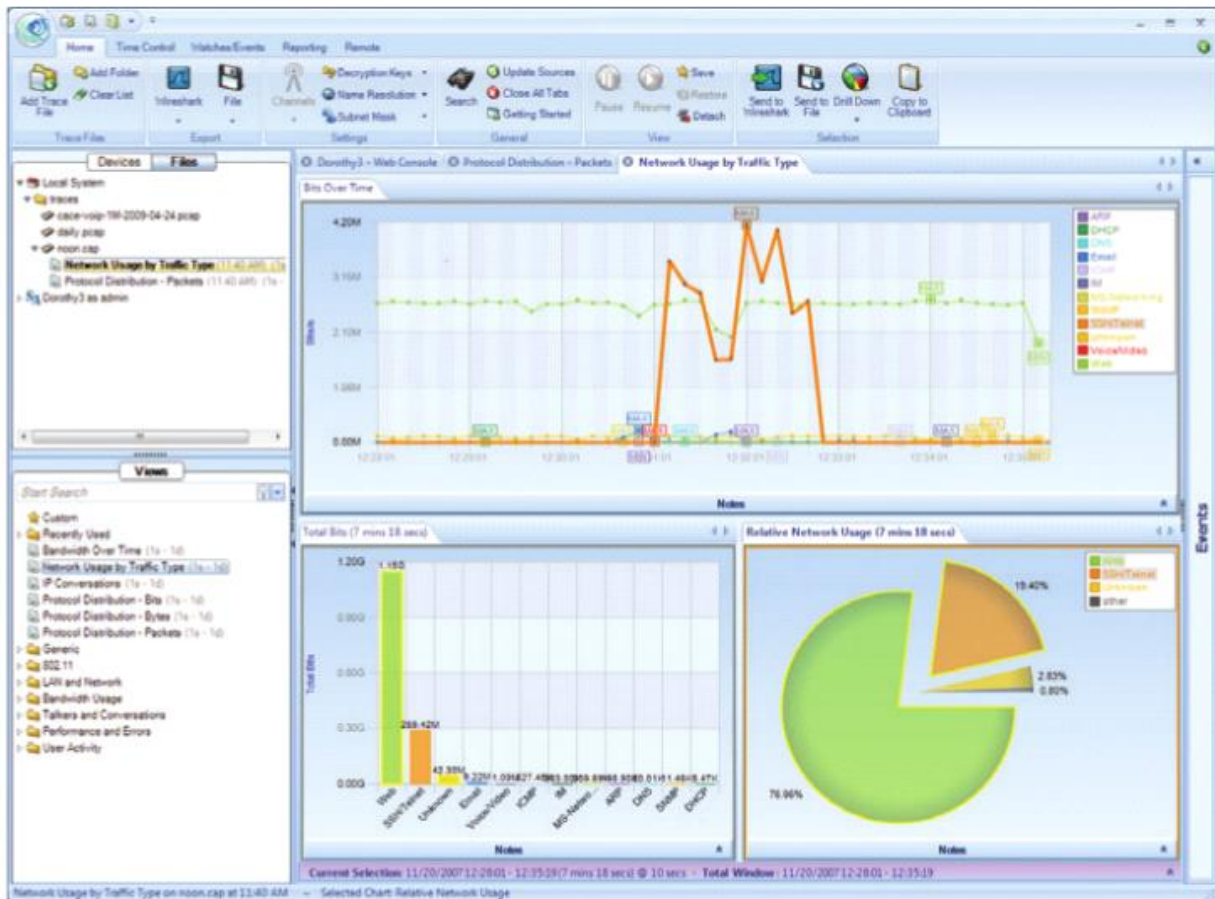
Let's take a look at how the different components of Cascade work together to address these areas.

## Cascade Profiler: Top-Down Network Visibility

Many network and application monitoring systems are expensive to install and maintain because they rely on dedicated probes installed around the network, or on software agents running on the application servers, but Riverbed Cascade is different because it efficiently leverages flow data whenever possible. In effect, Cascade uses existing network devices including routers, switches and Steelhead WAN optimisation appliances as its probes.

Cascade Profiler is an appliance that pulls together flow data from across the network (using a flow data collector called Cascade Gateway), blends it seamlessly with packet

data for a single view of the network, and tracks network and application behaviour over time. In essence, it learns what is normal on the network and watches for when things change.



### Cascade Pilot's Interactive and Visually Oriented User Interface

Cascade Profiler provides top-down visibility via service-level dashboards, designed to be easy to use and to make sense to both business managers and IT staff. The dashboards use familiar green/yellow/red status indicators to report on application and network status and show how the network is delivering critical applications. Network managers can select which services to display based on their business needs, and view them by application or location. Starting at the high-level status indication, they can locate the source of a problem by drilling down into detailed performance information, and even into the raw packets if necessary.

Setting up a service dashboard is easy thanks to Cascade's discovery and dependency mapping capabilities which graphically show the delivery path of an application. Using the

Service Discovery Wizard you can add a service to the dashboard by simply selecting servers and clients based on automatically discovered dependencies.

Detailed SLA reports show how business services map to the network, how they have performed recently, which components have had problems, and which performance alerts have been sent. These reports are presented in an easy to understand, non-technical format, so they can be sent to executives to provide network visibility at a higher corporate level.

## **Cascade Shark and Pilot: Packet Capture and Analysis**

Since flow data is not enough for deep application analysis, Cascade can also capture (record) packet data at key locations around the network. The Cascade Shark appliance records network data to be replayed later or analysed via the Cascade Pilot network analysis tool and the open source Wireshark network protocol analyser.

Cascade Shark uses high-performance 1G and 10G Ethernet cards for sustained, multi-gigabit per second recording of network traffic without packet drops. It can manipulate and analyse multi-terabyte network traffic recordings, and supports packet filtering based on Wireshark BPF and Display filters. It indexes the packets for high query performance and low network overhead.

Although Wireshark underpins Cascade, Cascade goes far further. Cascade Pilot greatly expands and enhances upon Wireshark's reporting capabilities, by adding numerous graphical views with the ability to drill down into the application and the underlying packet data. In fact, Cascade Shark and Pilot were developed by the very same team that started the Wireshark project, so the integration with Wireshark is the most complete in the industry.

## **Riverbed Steelhead: Remote Site Visibility**

WAN connections can have a major effect on network and application performance. Typically, as well as bandwidth constraints, they introduce latency and they may also add other unexpected and unwelcome effects such as packet loss. Many organisations are

deploying Riverbed Steelhead WAN acceleration devices to improve the performance of two to three key traffic types, only to discover that their network also carries five or six other protocols that could benefit from acceleration. It is also very common to find applications on their WAN that they didn't know were running there.

While Steelhead's management console already provides visibility into its activities, it has not been so easy in the past to understand the device's effect on the overall WAN. Adding Cascade changes all that. Now, Steelhead becomes a remote data collector for Cascade, thanks to its built-in packet capture and flow export capabilities, so the network manager can see how WAN optimisation affects the network. As an added benefit, Steelhead can monitor LAN traffic at the remote site, again eliminating the need for a dedicated probe.

#### **Case Study: Zumtobel**

*Zumtobel AG was already a Riverbed customer and had installed Steelhead appliances to optimise application performance over the WAN. Whilst this did overcome the issue of poor application performance, on occasion users would still complain that they were experiencing delays when accessing data and files. Even with Steelhead appliances deployed, there can still be issues which cannot be overcome with WAN optimisation e.g. problems with a database or the client server. These are difficult to identify - especially so in Zumtobel's case, as it had outsourced many of its services. By installing Cascade, Zumtobel can now monitor application performance in better detail and try to troubleshoot problems before they affect users.*

Cascade can also help you understand a device or application's effect on the WAN. Does it issue unrecognised commands or protocols, say? What is it doing in the background? What bandwidth or latency does it expect? And it can help you distinguish between problems that WAN acceleration can and cannot solve. For example, acceleration may not help WAN connections that suffer from high packet loss. It can reduce the load on those connections, but you need to know about and address the packet loss before you can really improve application performance.

## The security side

Most of today's security tools focus on prevention - of unauthorised access, unwanted activity and so on. But in order to prevent something, we first have to know that it exists and is happening. In other words, we need the ability to detect the unknown and unexpected.

Quite simply, as the threats multiply and become more targeted, we can no longer rely on relatively static tools based on industry-wide shared signatures that represent known vulnerabilities or threats. Those protective defences – firewalls, IDS/IPS (Intrusion Detection/Prevention Systems), and so on – are still needed, of course, but they are not enough on their own, as they may not be effective against unknown threats such as insider attacks.

That is why analysts such as Gartner are recommending that enterprises rebalance their security priorities and investments to boost the detection and monitoring side<sup>1</sup>. The challenge is that in most cases we cannot subscribe to external feeds for this - we have to work out for ourselves what malicious activity looks like on our network. This can require significant effort to reduce the number of false positives, tune detection systems to suit the local environment and add the necessary context.

This is where behaviour analytics add the critical value. After all, what you are looking for is unusual or irregular activity on the network – activity that might signal an application performance problem in one case, or a security or policy breach in another – and if you want to detect abnormal behaviour then an analytics-based tool is essential.

What this reflects and demonstrates is the convergence between networking and security operations. The two are no longer separate nor can they be – security needs to be intrinsic to the network, not an afterthought or add-on, and with Cascade there is an opportunity to use the same solution for both.

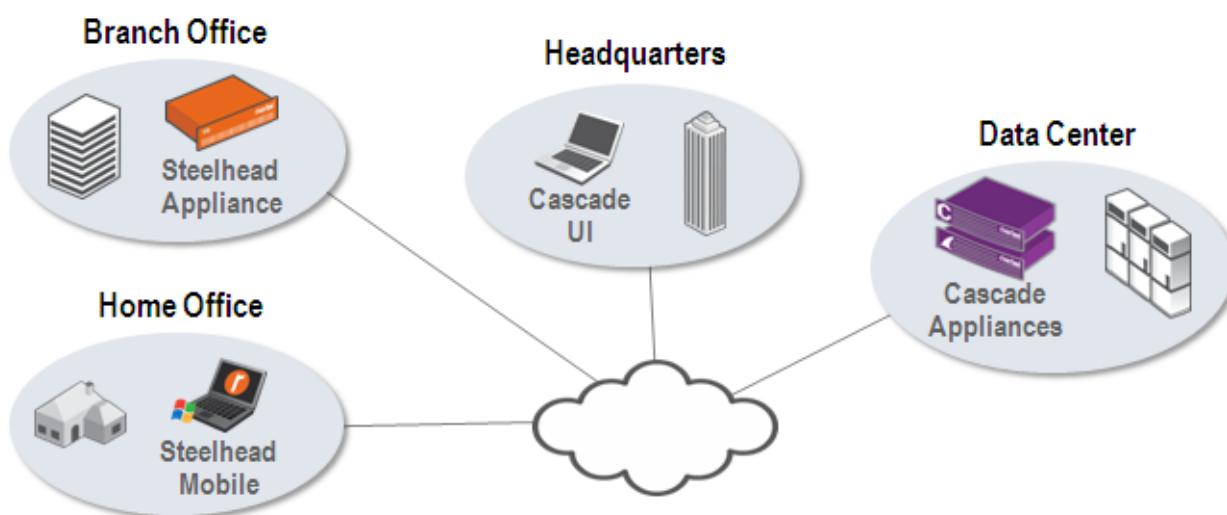
---

<sup>1</sup> [http://blogs.gartner.com/neil\\_macdonald/2010/07/15/security-thought-for-thursday-protection-prevention-detection/](http://blogs.gartner.com/neil_macdonald/2010/07/15/security-thought-for-thursday-protection-prevention-detection/)

## Detecting Threats

Cascade's behavioural analytics engine monitors and analyses network traffic, looking for patterns that could indicate network abuse or problems, or perhaps a zero-day attack. Examples might be a server sending too many queries or trying to connect to the Internet in the middle of the night. In doing so, Cascade adds another layer of security – so as well as the anti-malware scanner detecting known attacks, say, Cascade can help detect undocumented vulnerabilities and unknown threats, even before the security breach impacts network performance or results in significant loss of data.

Cascade does this by learning what normal network behaviour looks like, and then monitoring network traffic to see if it changes from that norm. Rather than simply take an initial benchmark and call that "normal", its learning capabilities allow it to identify cycles within network behaviour and include them within the norm - cycles that might result from periodic application runs, for example. After all, no-one wants security alerts going off every time the weekly backup run kicks off.



**Riverbed devices on your network provide a fully distributed network analysis solution**

However, if a relatively lightly used server begins propagating many requests or an internal host calls out to an Internet server, Cascade might suspect it has been infected with a worm or Trojan. Policy breaches, such as enterprise application traffic using the firewall's Port 80 web port instead of one of the secure ports, might also ring bells. Network security managers can then use their management tools to block or quarantine traffic, say, or to apply a filter or access control list.

### **Threats to look for**

*Three types of network behaviour can reveal potential security problems:*

- *Protocol* – packets that are too short, have ambiguous options or breach specific application layer protocols. These may result from host-level attacks.
- *Rate-based* – such as traffic floods, which typically signify a denial-of-service attack.
- *Relational or behavioural* – involves changes in how hosts or groups of hosts interact on a network. These can indicate a range of problems, including malware and insider abuse.

Because Cascade looks for changes in network behaviour rather than a specific attack signature, it can identify zero-day attacks for which no signature yet exists, as well as insider network abuse and policy violations. Cascade's learning approach also makes it less prone to false positives, and means that it requires very little on-going maintenance, unlike many traditional security technologies.

### **A distributed challenge**

Cascade can help deploy network security out to remote offices. Instead of deploying software agents to all the hosts – an expensive and hugely difficult to manage task, given a large distributed network that takes in dozens or even hundreds of sites – or installing IDS/IPS sensors at each remote site, Cascade simply uses the existing network infrastructure. This means simply using the flow data that comes back from that site's router or the Riverbed Steelhead WAN optimisation appliance deployed at that location.

This demonstrates one of the most interesting and useful things about behavioural

analytics: its versatility and therefore its cost-effectiveness. As well as being able to detect and identify previously unknown attacks, Cascade can also provide performance analytics. By consolidating multiple capabilities into a single system, it cuts both deployment complexity and solution cost.

## Why WAN optimisation also needs network visibility

WAN optimisation products, such as Riverbed Steelhead, enable you to do things that were not practical before – consolidate branch office IT into a central data centre over intercontinental distances, say, or replicate data to a remote disaster recovery site over a Gigabit connection.

However, they also bring new challenges, especially when it comes to network monitoring and management. That is in part because WAN optimisation can distort key network and site statistics, for example by disguising traffic or changing the packet headers, and in part because when you accelerate or optimise in one area, it can create unexpected side-effects elsewhere – in some cases it simply moves the bottleneck.

And of course before you optimise, you need to know what to optimise and where. As the saying goes, “You can't manage what you can't see.” That in turn means you need to know what is running over the WAN, where it is coming from, and what the key problems are – for example, whether it is latency, packet loss, bandwidth congestion, etc.

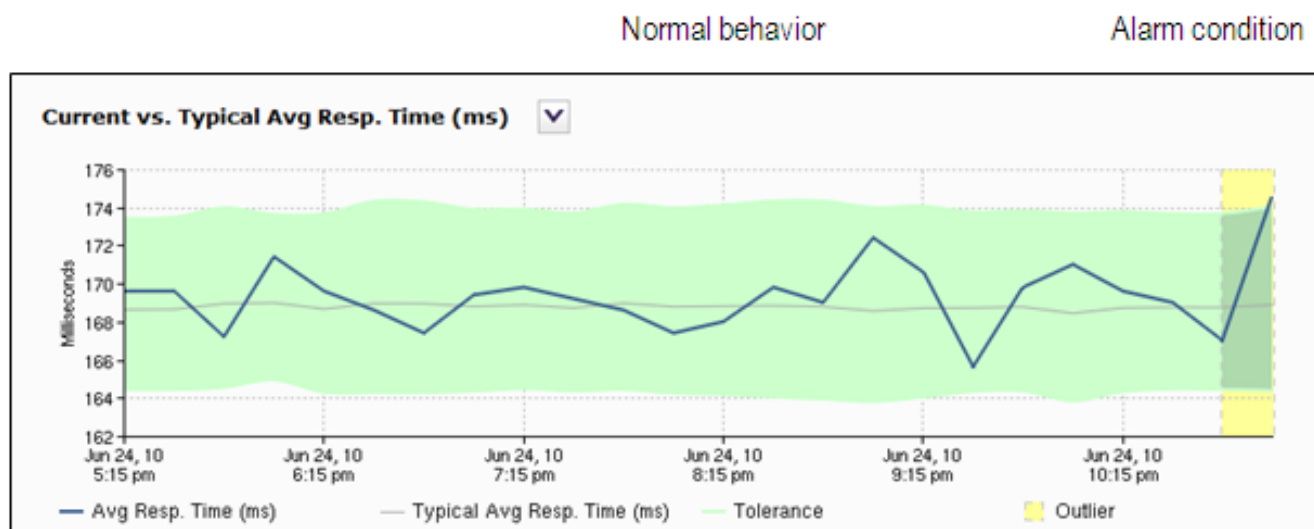
This is where Riverbed Cascade comes in. By using packet and flow data retrieved from Steelhead appliances in branch offices, as well as from switches and other devices in the network core, it can build a picture of network and application performance right across the WAN.

## Optimisation vs. troubleshooting

This means you can use Cascade not only to spot when things are going wrong, but to look for things that could go wrong or cause problems later, and fix them before they do. Network admins can analyse application traffic to identify the optimal candidates for optimisation, or identify unexpected traffic spikes.

Indeed, Cascade can be used before Steelhead deployment, both to identify suitable candidates for acceleration and obtain a performance baseline, and after deployment to verify the effects and see how the traffic patterns have changed

By examining the packet flows directly Cascade can tell you what protocols and applications are really running on your network, plus which servers and users are responsible for them. And it is a rare network manager who will not find a few surprises in there, whether it be the intern in India running BitTorrent or the manager in Mozambique with a liking for streamed Internet radio.



**Cascade learns normal application behaviour and alerts you to any meaningful changes**

And where having WAN optimisation devices in place was once a drawback when it came to network performance management, because they made the remote site less visible, with Cascade and Steelhead working together the reverse is the case: more visibility, not less. That is because the Steelhead appliance becomes yet another management asset, feeding useful network performance data back from the remote site – for optimised and non-optimised applications alike.

## The adaptive WAN and business services

Having Cascade on hand also opens the doors to the adaptive WAN - a wide-area network that can support business change by adjusting to suit as the mix of applications changes. In order to have an adaptive WAN, you need to be able to measure what is going on over the network, so you can respond to network changes or congestion, for example by adjusting quality-of-service (QoS) parameters or adding bandwidth shaping.

Reactive WAN management is therefore giving way to continuous assessment, where IT aims to stay a step ahead of problems and changes, dealing with them before they affect users enough for them to complain.

The planning aspect is also important here. In order to minimise disruption, Cascade's network monitoring and dependency mapping capabilities enable you to plan network changes, such as moving a server from one office to another, or server consolidation. However, if there are Steelhead appliances in place, the effect of those changes will be different, so it is important that Cascade understands what Steelhead does.

Cascade's ability to measure and visualise application performance also makes it useful for anyone looking to add business services to the network or offer differentiated services. That's because Cascade's dashboards allow you to select which business-critical services to monitor and how – by application or location, say. This is aided by its ability to discover services and dependencies, which lets you map network traffic to the appropriate business applications in a graphical format.

You can then use the tools within Steelhead to identify, categorise and optimise that business-critical traffic, for example by deploying QoS policies to allocate minimum and maximum bandwidth, and to prioritise latency-sensitive applications.

The result is a WAN adapted to the critical services that need to run across it, plus the ability to monitor and manage application performance. Then, as service loads, customer demands or WAN resources change, the network can be re-tuned to suit.