White Paper

Pre and Post Deployment WAN Acceleration Assessments

The average network today is under assault. After a period of sporadic growth, deploying MPLS and migrating to a converged network to support VoIP, many budgets and IT staff numbers are shrinking within organizations. In order to keep costs in check while ensuring acceptable levels of service IT departments are commonly turning to point or distributed shaping, compression and acceleration solutions in lieu of adding costly bandwidth. By making a one-time capital purchase, IT organizations save on the recurring OpEx of greater bandwidth and many WAN acceleration ROIs, if taken at face value, are compelling.

Table of contents

FLUKE networks

Overview

One step that commonly is overlooked when investigating various proprietary acceleration technologies, is an independent assessment to quantify the perceived benefits and validate the expected ROI. For most organizations determining what applications are on the network, where and for what purpose users are consuming the majority of those resources, and characterizing typical traffic behavior patterns, is a major challenge.

The application of technology to the network that can throttle malicious or unnecessary traffic in real time is powerful but not always necessary. It is in an organizations interest to do a pre assessment which quantifies the benefits of acceleration or compression prior to a significant investment. Furthermore, once such technology is deployed, enterprises can leverage the same agile monitoring visibility used to do the pre-assessment, to create a consistent set of metrics that provide an independent check of the expected ROI.

Use of NetFlow

Because NetFlow Tracker relies on industry standard flow technology exports already available in the majority of today's deployed network infrastructure, it provides immediate insight on a per-user basis. NetFlow Tracker can immediately and cost effectively answer key questions like:

- Who are the users and what applications are they using?
- What are my busiest devices and what traffic do they regularly support?
- What was happening during a specific performance issue on the network?
- Are there worms and viruses in my network, where are they, where did they come from, and how widespread is the issue?
- How is quality of service improving performance?
- How do I report overall performance and usage of my network as a whole?

Use a Checklist

The following checklist walks a user through performing these and other assessments as a valuable and critical first step to deploying, managing and quantifying any additional WAN acceleration or compression technology.

This guide assumes the user has already configured the infrastructure for NetFlow and has a functional NetFlow Tracker deployment. If you need assistance enabling NetFlow or equivalent flow exports from your infrastructure or other support configuring NetFlow Tracker please contact Fluke Networks Technical Assistance 800 283-5853.

By using NetFlow information to complete the following pre-assessment checklist, users will definitively determine which, if any, sites will benefit from acceleration, the most effective type of acceleration to deploy for your environment, and the optimal scope of any deployment.

Pre-Assessment Checklist	Tracker Report	Status
Identify all applications on the network	Recognized Applications	
Identify any bandwidth abusers	Conversations	
Validate QoS configurations	Types of Service / Differentiated Services	
Determine congestion severity and frequency	Device view / Interface view	
Locate and profile all key servers and their usage	Destination Address Popularity	
Verify no worms or viruses present	Source Address Dissemination	
Characterize application distribution	Network Overview	

The First Step

The first step in preparing for any new end user quality of experience improvement is to identify what applications are on the network and at which sites. To get a quick snapshot of application distribution throughout the network it's best to start with the Recognized Applications report in Tracker.

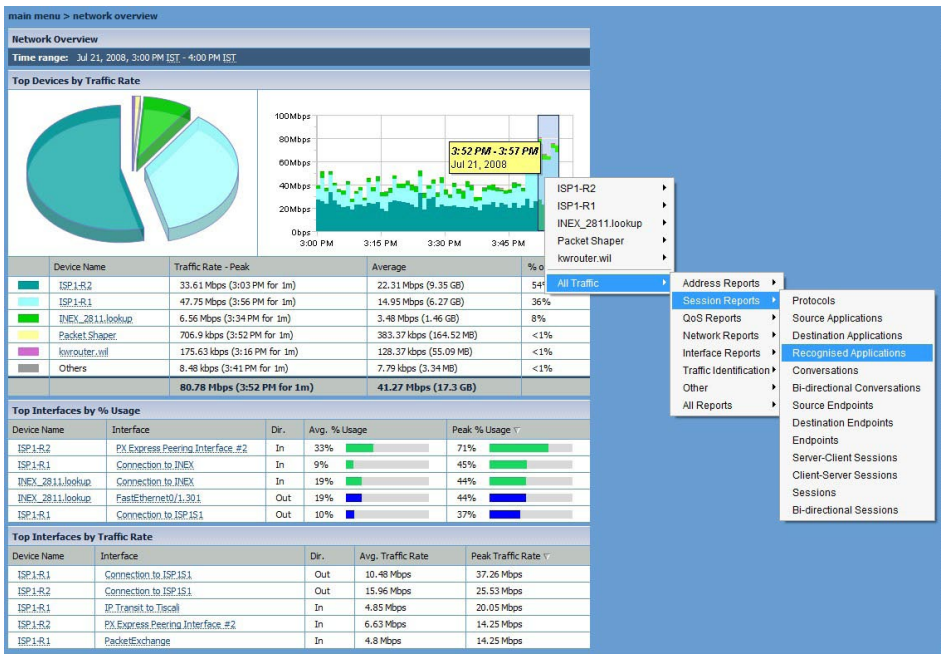
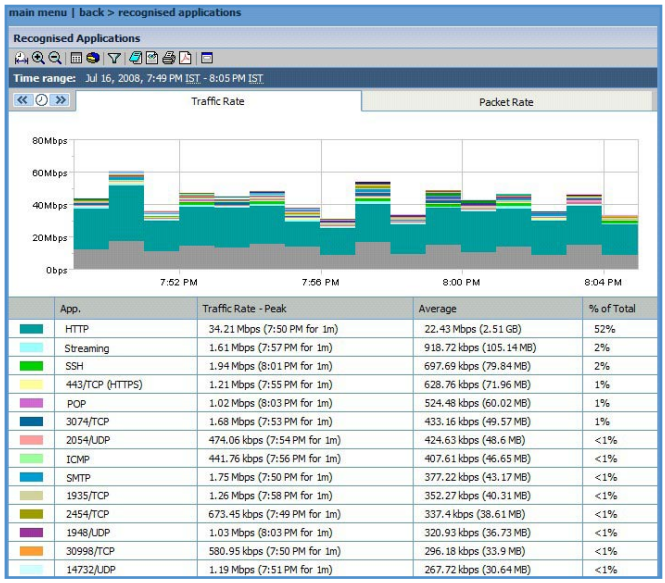


Figure 1 – Network Overview

The Recognized Applications view is ideal for identifying both application distribution as well as top talkers. In this example more than 50% of traffic is HTTP. Even more interesting is the list below HTTP of everything else – there is significant streaming for instance.



App.	Traffic Rate - Peak	Average	% of Total
HTTP	34.21 Mbps (7:50 PM for 1m)	22.43 Mbps (2.51 GB)	52%
Streaming	1.61 Mbps (7:57 PM for 1m)	918.72 kbps (105.14 MB)	2%
SSH	1.94 Mbps (8:01 PM for 1m)	697.69 kbps (79.84 MB)	2%
443/TCP (HTTPS)	1.21 Mbps (7:55 PM for 1m)	628.76 kbps (71.96 MB)	1%
POP	1.02 Mbps (8:03 PM for 1m)	524.48 kbps (60.02 MB)	1%
3074/TCP	1.68 Mbps (7:53 PM for 1m)	433.16 kbps (49.57 MB)	1%
2054/UDP	474.06 kbps (7:54 PM for 1m)	424.63 kbps (48.6 MB)	<1%
ICMP	441.76 kbps (7:56 PM for 1m)	407.61 kbps (46.65 MB)	<1%
SMTP	1.75 Mbps (7:50 PM for 1m)	377.22 kbps (43.17 MB)	<1%
1935/TCP	1.26 Mbps (7:58 PM for 1m)	352.27 kbps (40.31 MB)	<1%
2454/TCP	673.45 kbps (7:49 PM for 1m)	337.4 kbps (38.61 MB)	<1%
1948/UDP	1.03 Mbps (8:03 PM for 1m)	320.93 kbps (36.73 MB)	<1%
30998/TCP	580.95 kbps (7:50 PM for 1m)	296.18 kbps (33.9 MB)	<1%
14732/UDP	1.19 Mbps (7:51 PM for 1m)	267.72 kbps (30.64 MB)	<1%

Figure 2 – Recognized Applications

By monitoring the list of applications and their usages on an ongoing basis you will be able to determine how utilized WAN links currently are along with what and who is causing that utilization. After monitoring our applications for several days we determined that by applying an ACL that blocks unauthorized streaming, in this example, we could reduce our average utilization in the network by about five percent!

Get Deeper Information

Digging deeper we're able to do a conversation analysis.

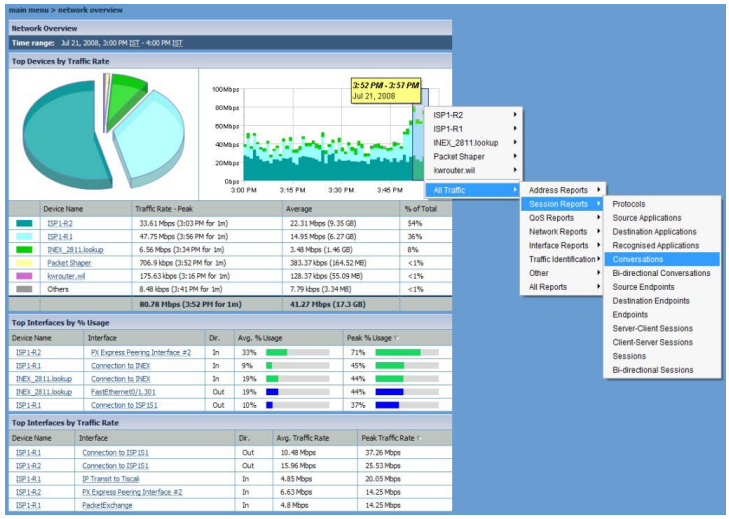
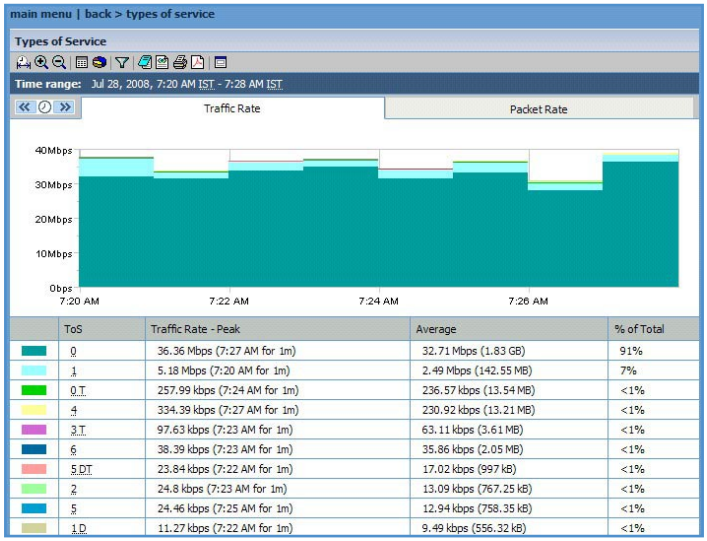


Figure 3 – Top Devices

The Conversations report shows usage by user for a specific time. By having visibility on a per-user basis, we're able to separate business usage from recreational usage and in most cases save additional bandwidth by bringing bandwidth abuse to the user's attention as well as applying additional policies in the network.

Once the picture of applications and user's daily typical usage is clear, the network can be checked for any misconfigurations impacting those applications and users. One of the most common issues in a modern MPLS network is known as a QoS Mismatch – when the intended priority of an application is not configured equally at every location in the network. With no or limited visibility this is a difficult problem to identify because it only surfaces during periods of severe usage. After hours testing or waiting for another report of the problem rarely reproduces the symptoms.

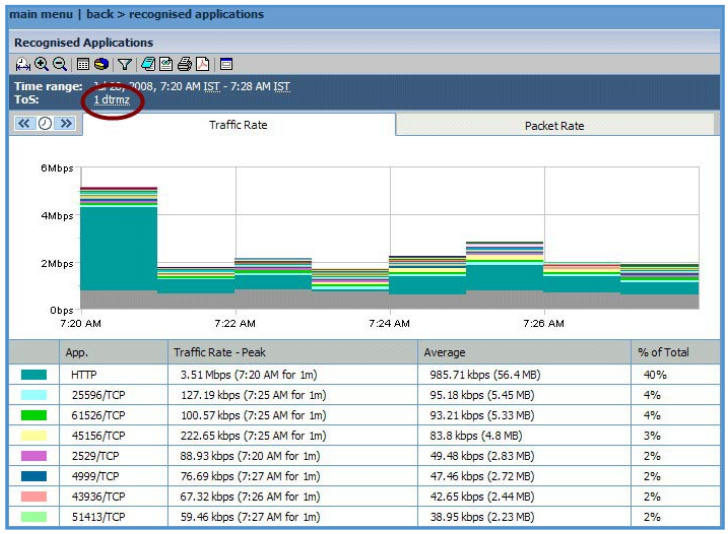
NetFlow Tracker can quickly display for any and every location throughput by Class of Service (ToS or DiffServ) and users can drill down from there to ensure proper configuration.



ToS	Traffic Rate - Peak	Average	% of Total
0	36.36 Mbps (7:27 AM for 1m)	32.71 Mbps (1.83 GB)	91%
1	5.18 Mbps (7:20 AM for 1m)	2.49 Mbps (142.55 MB)	7%
0 T	257.99 kbps (7:24 AM for 1m)	236.57 kbps (13.54 MB)	<1%
4	334.39 kbps (7:27 AM for 1m)	230.92 kbps (13.21 MB)	<1%
3 T	97.63 kbps (7:23 AM for 1m)	63.11 kbps (3.61 MB)	<1%
6	38.39 kbps (7:23 AM for 1m)	35.86 kbps (2.05 MB)	<1%
5 DT	23.84 kbps (7:22 AM for 1m)	17.02 kbps (997 kB)	<1%
2	24.8 kbps (7:23 AM for 1m)	13.09 kbps (767.25 kB)	<1%
5	24.46 kbps (7:25 AM for 1m)	12.94 kbps (758.35 kB)	<1%
1 D	11.27 kbps (7:22 AM for 1m)	9.49 kbps (556.32 kB)	<1%

Figure 4 – Types of Service

In this example users are reporting poor quality VoIP calls. VoIP should be configured as the highest priority, ToS 1, and we're able to verify that with just a couple clicks. By drilling into the ToS 1 Applications, however, HTTP is making up 40% of the prioritized traffic and there is no VoIP! In these cases performance of applications can be worse than it was prior to migrating to MPLS with QoS.



App.	Traffic Rate - Peak	Average	% of Total
HTTP	3.51 Mbps (7:20 AM for 1m)	985.71 kbps (56.4 MB)	40%
25596/TCP	127.19 kbps (7:25 AM for 1m)	95.18 kbps (5.45 MB)	4%
61526/TCP	100.57 kbps (7:25 AM for 1m)	93.21 kbps (5.33 MB)	4%
45156/TCP	222.65 kbps (7:25 AM for 1m)	83.8 kbps (4.8 MB)	3%
2529/TCP	88.93 kbps (7:20 AM for 1m)	49.48 kbps (2.83 MB)	2%
4999/TCP	76.69 kbps (7:27 AM for 1m)	47.46 kbps (2.72 MB)	2%
43936/TCP	67.32 kbps (7:26 AM for 1m)	42.65 kbps (2.44 MB)	2%
51413/TCP	59.46 kbps (7:27 AM for 1m)	38.95 kbps (2.23 MB)	2%

Figure 5 – Traffic Usage of recognised applications for a specific time range

Taking a step back, an analysis should be done to identify any network usage hot spots in a topology. By monitoring the Device and Interface view of NetFlow Tracker over a sample of network usage any spikes at any location will immediately become apparent.

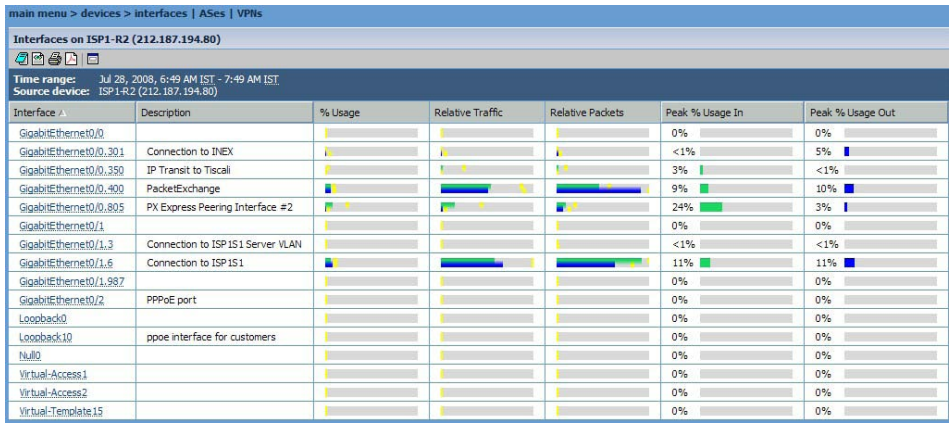


Figure 6 – Manage Interfaces

These higher level network-centric views can highlight sites and services that are used the most and provide more insight into the paths the majority of communications take. A key step in determining what acceleration to deploy is identifying how many and which locations will benefit the most from it.

Manage your in-house applications

One significant driver of day-to-day network utilization is in-house applications sourced from in house servers. It is not uncommon for a network group tasked with improving the end user quality of experience to also not have knowledge of where and what each server in the network is as that function may belong to a separate internal group. In any case NetFlow Tracker's unique ability to do an analysis based on conversation frequency, as opposed to top-talker based bandwidth usage, allows for reporting that highlights all popular servers. Those views are called Source Address Dissemination and Destination Address Popularity.

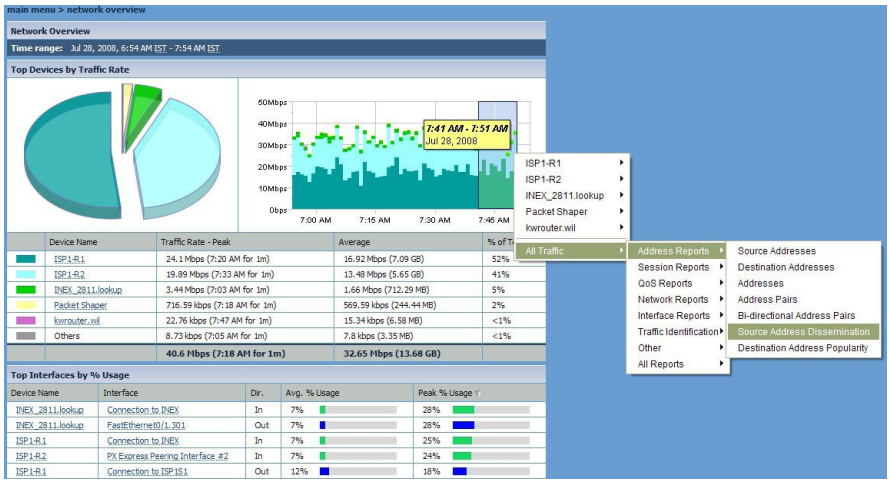


Figure 7 – Top Devices by Traffic Rate

By identifying which locations and users are hosting servers, business serving or unauthorized serving, you can determine if simply relocating or consolidating servers will save on bandwidth and make more network resources available to other traffic.

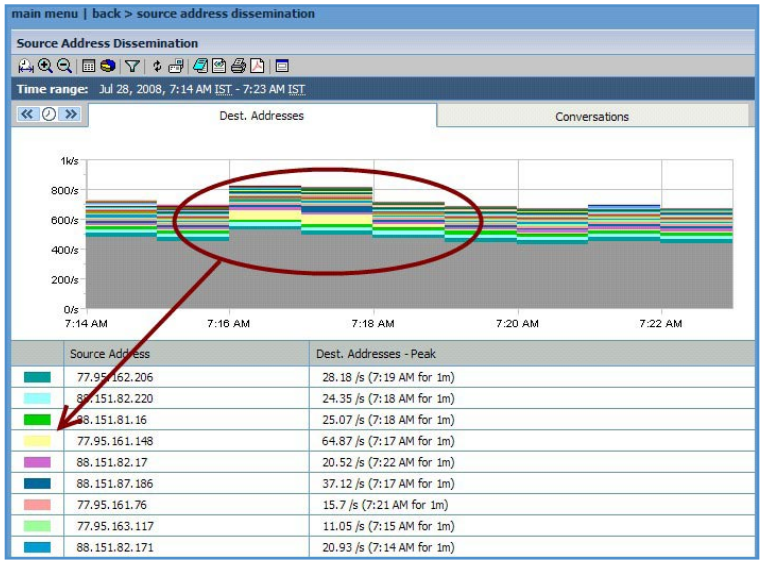


Figure 8 – Source Address Dissemination

In the above Source Address Dissemination report we can see that suddenly for a brief 2 minutes one particular IP address was talking with nearly 65 unique addresses every second and then stopped again. Most business servers are steadily busy and so this is a pattern that may warrant further investigation. By using the interactive UI to drill down and view those conversations, we can characterize the traffic to the individual user(s) level. Another common cause of patterns like this are worms and viruses and by leveraging NetFlow Trackers new baseline alerting capability you can always be instantly alerted to a new and dramatic increase of conversation frequency anywhere in the network.

A final step

As a final step to assessing a network for a WAN Acceleration project it is necessary to characterize at a big picture level the behavior of the networked applications. By monitoring the real-time Network Overview screen a user can quickly get a sense of busy times and locations during the course of a day as well as the types of usage that are causing that activity. This is key to selecting the type of acceleration technology to deploy.

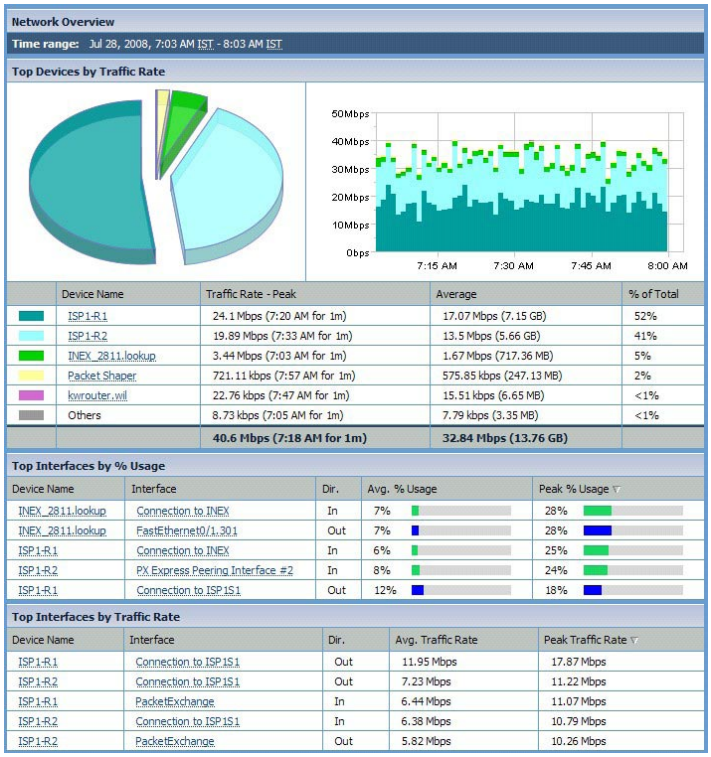


Figure 9 – Top Devices by Traffic Rate

Once the selected method of acceleration has been deployed the Network Overview can also instantly reflect those bandwidth savings and other traffic behaviors. One common cause of continued performance problems post-deployment is an unforeseen or misconfigured route in the network that causes some of the traffic to bypass the acceleration. By continuing to use a third party, vendor agnostic monitoring approach users can maintain total visibility at the common network bottleneck points – routers and switches.

Download a free 7-day evaluation NetFlow Tracker - http://www.flukenetworks.com/netflowdemo