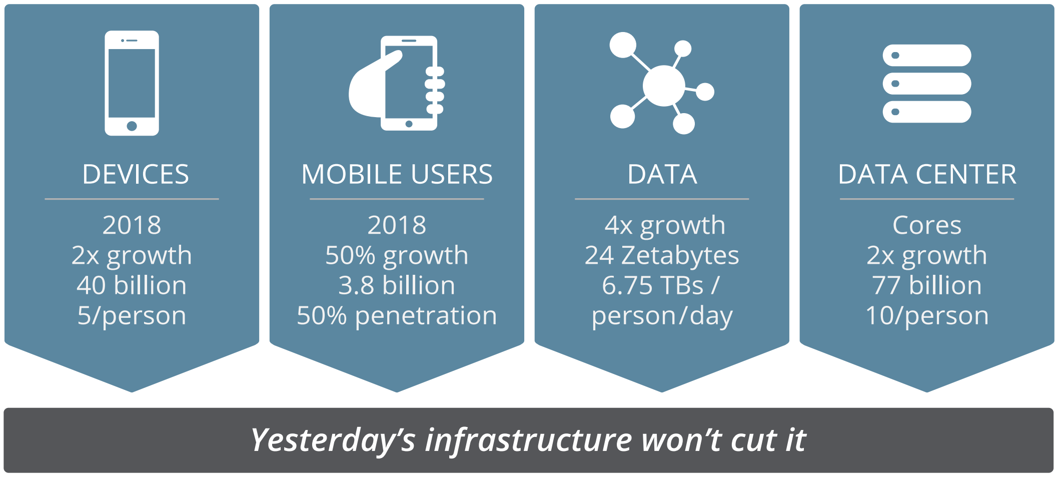
NETSCOUT

Optimize Monitoring and Security Systems for 100G and 40G Networks

Want to transition to 100G and 40G networks, but the existing investment in 1G and 10G tools is giving you pause? Learn how you can extend the life of your tools, while gaining unified packet visibility across your entire network.

The next three years will bring a veritable avalanche of data, putting new demands on networks. Data centers are forced to migrate to higher bandwidth network infrastructure, supporting speeds up to 40G and 100G. These network links must continue to be monitored and secured as before, which involves deploying multiple systems for both performance management and security assurance. Unfortunately, many systems available today cannot ingest high-speed traffic, because they lack both the physical interfaces and processing power to do so. Even when certain tools begin to support 40G or 100G interfaces, moving to new tools and systems is expensive and many products will be unable to keep up with line rate traffic at 40G or 100G.



DEVICES
2018
2x growth
40 billion
5/person

MOBILE USERS
2018
50% growth
3.8 billion
50% penetration

DATA
4x growth
24 Zetabytes
6.75 TBs / person/day

DATA CENTER
Cores
2x growth
77 billion
10/person

Yesterday's infrastructure won't cut it

Source: IDC (September 2015): Market Analysis Perspective: Worldwide Data center Trends, 2015}

To plan your migration to 40G and 100G networks, consider implementing a unified packet visibility architecture across your network. Look for the following capabilities:

Speed Conversion

Network tools and security systems are typically behind the curve when it comes to keeping up with network traffic. Even if a tool is offered with a 40G or even a 100G interface, the throughput performance is likely to be significantly lower than that of the network. Packet loss—which can lead to significant monitoring gaps—will result if a tool's performance maximum is exceeded.

More typically, however, the tools and systems available to the network group are only capable of handling traffic speeds of 1G and 10G, so copied network traffic must be converted in real time to the appropriate speed. Speed conversion (and a mix of port types) is an essential feature of a packet visibility solution for 100G/40G networks.

Packet Filtering

Filtering based on L2-4 header information (or a custom offset) can be used to eliminate unnecessary traffic, such as ARP requests, or to apply policies to it, such as mapping to a specific monitoring or security system. Even in applications in which all packets without exception must be directed to a monitoring tool or tools, filtering should still be available as an option. It can be useful for ad hoc network troubleshooting or for use when additional, potentially specialized tools are added to the monitoring and security architecture.

Packet Slicing

Packet slicing discards the unneeded portion of a packet, based on a defined value such as number of bytes from end of TCP header. One common application for packet slicing is the elimination of the packet payload, which significantly reduces the amount of traffic that is sent to the tools, in turn allowing them to function more efficiently. In some applications, the payload cannot be stored due to security or compliance protocols, so eliminating it before it reaches the tools (a process that is done on the packet flow switch in real time using purpose-built hardware), cuts down on the amount of processing done at the tool and ensures that the payload never reaches a tool that has persistent storage capability.

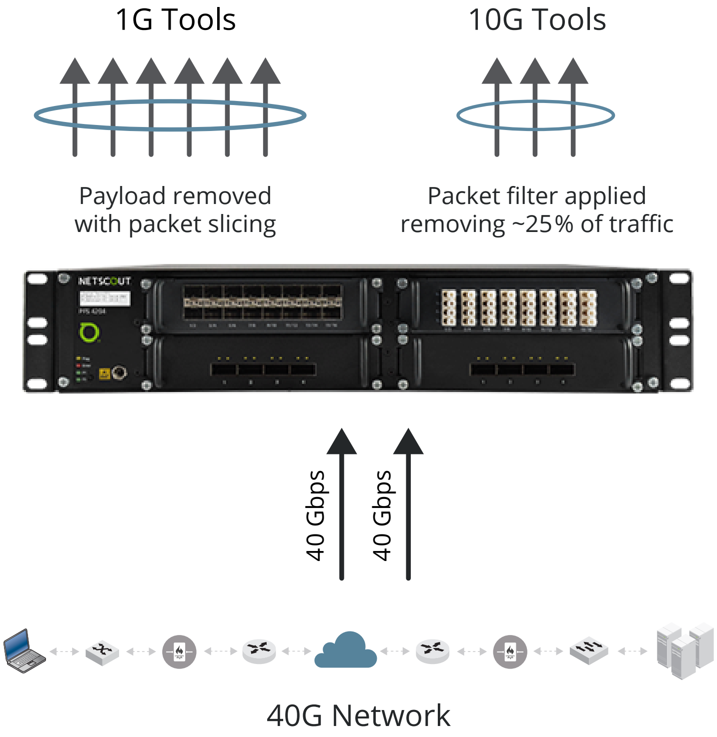

1G Tools
10G Tools
Payload removed with packet slicing
Packet filter applied removing ~25% of traffic
NETSCOUT
40 Gbps
40 Gbps
40G Network

Figure 1. Speed conversion, packet slicing and filtering allow use of 1G and 10G tools in a 40G network environment..

(Heterogeneous) Port Density

After the traffic is sufficiently optimized for the tools (using filtering and/or slicing), the correct mix of ports/speeds—based on traffic utilization, preprocessing, and accounting for redundancy—must be determined

To determine necessary monitor port density on a packet flow switch, start with expected network utilization, and then subtract the amount of traffic that will likely be eliminated using optimization features such as filtering and slicing. Redundancy requirements should then be factored in to come to the total monitor throughput, which can then be converted into port count, depending on the throughput performance of the tools. It's also a good idea to think about long term future growth and how the packet visibility solution can accommodate it, perhaps using a modular design or systems approach.

Flow Aware Load Balancing

Load balancing logically binds multiple monitoring ports, allowing traffic to be mapped to a group, rather than manually split across individual ports. Once the traffic is mapped to a group, the traffic will be automatically spread across the ports based on user-defined flow criteria. Load balancing traffic across the monitor ports has several advantages: it can prevent overflow of any one port; sessions won't be broken up—they'll be consistently maintained to the same port; and in the event that a port in the group fails, the traffic load will be redistributed to the remaining ports.

High-Availability Backplane

All passive packet visibility solutions are designed to be non-intrusive to network infrastructure, preventing them from affecting network uptime, regardless of operation or failure. Unfortunately, not all such systems are designed for high availability monitoring. In particular, most blade-and-chassis packet visibility solutions do not accommodate redundant backplane channels, instead relying on additional port consumption for redundancy, or offering none at all.

NETSCOUT packet flow switches provide multiple redundant channels, appliances or ports to ensure operational continuity in the unlikely event that one of these fails.

High-throughput System Interconnect

The packet visibility solution for a 100G or 40G network should be able to scale, either by adding blades, or by connecting into a system of packet flow switches. NETSCOUT delivers the highest capacity available, capable of scaling to hundreds of nodes and thousands of ports, providing vast coverage of the network.

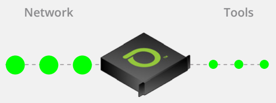
Summary

If the network has yet to be upgraded to 40G or 100G, it's still critical to future proof the monitoring tools for eventual network upgrade by using a modular packet visibility system that can accommodate seamless additions—in the form of appliance, slot, or blade—that don't disrupt the existing architecture. Contact us for a consultation on architecting a comprehensive packet visibility system for the network tools and security systems of today and tomorrow.

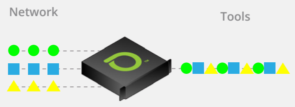
Key capabilities of NETSCOUT packet flow switches

Packet flow switches from NETSCOUT deliver high-speed network feeds to legacy network monitoring tools and security systems without packet loss — extending the life of these systems and maximizing their usage. Packet flow switches operate at line speed, using purpose built hardware, and are specifically designed to deliver customized traffic to each network tool and security system.

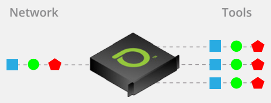
Speed Conversion



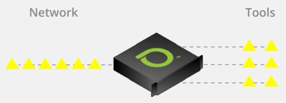
Aggregation



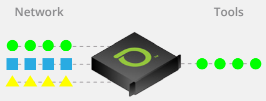
Replication



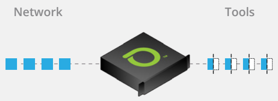
Load Balance



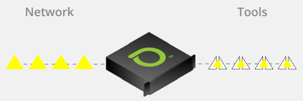
Filter



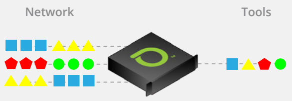
Slicing



Stripping



De-Duplication



Packet flow switches perform essential functions such as aggregation, load-balancing, packet stripping, slicing, replication and de-duplication, all designed to make your performance management and security systems more efficient and able to focus on the task at hand.

The NETSCOUT packet flow switches are easy to scale, so that any changes to the network or monitoring tools — in capacity, throughput, or speed — can be seamlessly accommodated.

NETSCOUT

Americas East
310 Littleton Road
Westford, MA 01886-4105
Phone: 978-614-4000
Toll Free: 800-357-7666

Americas West
178 E. Tasman Drive
San Jose, CA 95134
Phone: 408-571-5000

Asia Pacific
17F/B
No. 167 Tun Hwa N. Road
Taipei 105, Taiwan
Phone: +886 2 2717 1999

Europe
One Canada Square
29th floor, Canary Wharf
London E14 5DY, United Kingdom
Phone: +44 207 712 1672

NETSCOUT offers sales, support, and services in over 32 countries.

For more information, please visit www.netscout.com or contact NETSCOUT at 800-309-4804 or +1 978-614-4000