Welcome to 100G networks. Have you thought about performance monitoring?

The world is embracing high speed networks slow and steady. Many hardware vendors like Alcatel-Lucent, Cisco, Huawei and Brocade have announced support for 100Giga bit Ethernet and organizations around the world have also shown interest in launching 100G networks. All these events simply point to the advent of 100 Gigabit Ethernet in the commercial segment.

“Also of note were very strong shipment trends in 100GBase LR4 modules, demonstrating the widespread prototyping and trial activity now underway among 100 Gbps vendors and service providers,” notes Andrew Schmitt, directing analyst for optical at Infonetics Research.

Why move to 100G networks?

We often come across articles predicting bandwidth usage shoot up and doubling of video and VoIP traffic within a few years. The Cisco Visual Networking Index shows that the Business IP Traffic would triple by the year 2015.

<table>
<thead>
<tr>
<th>Business IP Traffic, 2010-2015</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
</tr>
<tr>
<td></td>
</tr>
<tr>
<td></td>
</tr>
<tr>
<td></td>
</tr>
<tr>
<td></td>
</tr>
<tr>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>By Network Type (Petabytes per Month)</th>
<th>2010</th>
<th>2011</th>
<th>2012</th>
<th>2013</th>
<th>2014</th>
<th>2015</th>
<th>CAGR 2010-2015</th>
</tr>
</thead>
<tbody>
<tr>
<td>Business Internet traffic</td>
<td>2,574</td>
<td>3,167</td>
<td>3,816</td>
<td>4,561</td>
<td>5,431</td>
<td>6,071</td>
<td>19%</td>
</tr>
<tr>
<td>Business managed IP traffic</td>
<td>1,293</td>
<td>1,580</td>
<td>1,890</td>
<td>2,254</td>
<td>2,690</td>
<td>3,017</td>
<td>18%</td>
</tr>
<tr>
<td>Business mobile data</td>
<td>63</td>
<td>147</td>
<td>305</td>
<td>543</td>
<td>876</td>
<td>1323</td>
<td>84%</td>
</tr>
</tbody>
</table>

Source: Cisco VNI 2011
Welcome to 100G Networks

A few observations from the report are:

- Annual global IP traffic will reach the zettabyte threshold (966 exabytes or nearly 1 zettabyte) by the end of 2015. In 2015, global IP traffic will reach 966 exabytes per year or 80.5 exabytes per month.

- Global IP traffic has increased eightfold over the past 5 years, and will increase fourfold over the next 5 years. Overall, IP traffic will grow at a compound annual growth rate (CAGR) of 32 percent from 2010 to 2015.

- In 2015, the gigabyte equivalent of all movies ever made will cross global IP networks every 5 minutes. Global IP networks will deliver 7.3 petabytes every 5 minutes in 2015.

- Business video conferencing will grow six fold over the forecast period. Business video conferencing traffic is growing significantly faster than overall business IP traffic, at a CAGR of 41 percent from 2010-2015.

Many organizations are encouraging telecommuting and business localization is being widely adopted. In such a scenario, be it for business discussions with remote customers or for communication between remote users or inter-branch connectivity, Internet based voice and video will be the solution. Most enterprises who use voice and video solutions have added real time, high definition, high quality, etc. in their immediate wish list. All these require a huge bandwidth capacity.

There are also factors like increase in number of business applications, more users due to business localization, need for efficient datacenter connectivity and being future ready, skipping the 40G network and thus a possible dual migration.

Another interesting point is the efficiency of 100G Ethernet compared to link aggregation that is used today. As of now, a 10 x 10G Ethernet link aggregation can only give a throughput of up to 30Gbps. This limitation can be overcome with a true 100G connection which can give a 100Gbps bandwidth, thus allowing high capacity links to scale even further. Considering all these, if not this year or the next, 100G will be widely adopted soon.

**The need for network performance monitoring**

Before switching to 100G networks, there is one thing that every network admin should be ready with – a comprehensive plan for network performance monitoring which involves bandwidth monitoring, traffic analytics and anomaly detection.

The higher speed that comes with the 100G network does not mean that bandwidth monitoring or traffic analytics is no longer a requirement. E-Commerce is growing and therefore the importance and dependency enterprises have on Internet connectivity too has increased. Network performance monitoring is a necessity in any network, be it a small enterprise, who wants their bandwidth to be used only for business applications or a large enterprise, with high speed bandwidth and high traffic volume.
Welcome to 100G Networks

Constant network monitoring can help create high performance networks. By knowing traffic patterns and finding peak usage patterns, you can ensure optimal bandwidth usage and decide when to schedule the backup jobs. You also get to know when a threshold value is being reached or when it is violated. With this information, you get to know about the issues before someone else reports it and maybe even would have found the root cause.

You also need monitoring to know when an application usage is hitting a peak, when there is unwanted traffic to the application server or to find if an application has incorrect QoS priority. Visibility into application details helps keep out spam applications, measure and increase performance of business applications and thus ensure application delivery.

Something else that monitoring can help with is validating the performance of QoS policies. This way, you will know if VoIP really has higher priority over web traffic or if the QoS policy implemented to prioritize the CRM application traffic is actually causing a drop in web traffic.

Monitoring can also detect network behavior anomalies that surpass the intrusion detection system or firewalls. Most enterprises allow web traffic, but a number of threats and malwares too can reach your network disguised as web traffic. In certain cases, malwares may physically be carried in by an employee whose laptop was compromised. Internal and external traffic monitoring will detect all types of anomalies, be it those that spread from your network to the outside or those which enter your network over the WAN and thereby help mitigate the effect of a major malware. Monitoring also helps in planning network changes, find VoIP and video traffic usage and measure its performance, get data for SLA reports, capacity planning, etc.

All this leads to one advantage – Increased cost savings by reduced network downtime and better performance from business applications.

What type of monitoring?

Monitoring a high speed network is not the same as monitoring a low bandwidth, low traffic, less number of devices and users, single office network. The number of branches (be it offices, datacenters or server farms) are higher, the number of devices used at different network layers would have increased considerably and there definitely will be an exponentially higher volume of traffic than ever before, after all one wouldn’t upgrade to a 100G network just for the sake of being technologically advanced.

With a 100G network, network admins can no longer be satisfied with just SNMP based reports about IN and OUT bandwidth usage. Probably, administrators may not even be too concerned about link utilization as the available bandwidth itself is high. The important question in a network administrator’s mind will be WHO ON EARTH is using all that bandwidth and thus a technology that can show the WHO, WHAT, WHEN and WHERE of traffic will be the requirement.
Welcome to 100G Networks

The era of high speed networks may also signal the end of packet inspection tools that cannot scale up to handle huge volumes of data. But the ones that do scale up can be really expensive. Further, packet inspection requires a huge volume of storage space and thus continuous packet capture and long term storage is not mostly undertaken. For example, a continuous packet capture from a 25% utilized 100Gbps link will end up generating 11250GB of data in an hour (1). In many enterprises, such implications leads to starting a packet capture for analysis only after a problem is reported. The downside of this is? When you start a packet capture and analysis after the problem occurs, in most probability, the packets captured may not be associated with the problem and thus a root cause analysis is rendered impossible. The solution needed is a continuous network monitoring system which will keep a track of all network activities with no impact on storage and the network.

The answer is a technology called NetFlow and its variants. NetFlow (or sFlow or IPFIX and all related flow formats) captures specific IP packet information from your device interfaces with no significant overhead on its performance or bandwidth. At the same time it gives visibility into the WHO, WHAT, WHEN and WHERE of traffic. You get information about traffic and application details, network conversations, traffic time stamp, the network path and traffic route, QoS values, MPLS labels, VLAN id, etc. Another advantage of NetFlow is that the volume of data involved is not huge as it captures only specific header information from IP traffic. This allows you to do a continuous NetFlow capture but with no impact on storage and thus go back in time to analyze issues. This very reason makes NetFlow the most apt technology for traffic analytics in high speed networks.

Something else that NetFlow can be used for is network behavior anomaly detection. Since NetFlow carries detailed information on different aspects of an IP packet, the information available can be leveraged on to detect a network anomaly.

Network performance monitoring is not only about traffic analytics using NetFlow technology. You need to adopt technologies that can do deep packet inspection for advanced application recognition, find performance of the CBQoS policies implemented to manage WAN traffic, measure link performance when carrying different traffic types like VoIP, video and data and even measure performance of UDP and TCP protocols over a link. Further required is tracking the performance of ‘now being widely adopted’ video traffic.

What should the monitoring tool offer?

An important factor to consider when choosing a flow analyzer is how adaptable the tool is. Networks are no longer made of single vendor devices, where administrators make do with whatever options available. In the 100 Gigabit era and in many cases today itself, networks consist of multi-vendor devices, each handling different requirements. We now have datacenter switch, core switch, the distribution layer device, the firewall, the edge router, the WAN optimization device – each from a different vendor, chosen based on cost, capability and most of all, the network’s requirement. When selecting your monitoring tool, verify if the tool supports the different vendor-dependent flow formats including those not widely used proprietary flow formats which your device might be exporting. The
other factors to check for are, can the tool scale up to handle different volumes of flow data, whether more data collectors can be added as and when the network grows and if it is capable of reading new information fields available in newer NetFlow versions.

A good NetFlow analyzer tool should provide flexible data storage options. It is preferable to be able to store raw NetFlow data for at least a couple of months or as per user requirements and also store an aggregate of the data for an infinite period. This way you can analyze each network activity/conversation until you decide to discard them and still view the ‘Top N’ number of activities from history as and when needed.

Something to keep in mind when monitoring a high speed network is that you could now be managing more branches, remote offices or even a datacenter. Opt for a tool that can work in a distributed network model and handle time zone differences. A distributed monitoring model ensures that monitoring goes on at other locations even if a data (flow) collector goes down somewhere else and the time zone handling lets you view reports in your time zone instead of an unrelated time zone.

The last couple of years have seen a rise in the number of malwares and DoS attacks. NetFlow data that you use for bandwidth monitoring and traffic analytics is also rich in information about network anomalies. Network behavior anomaly detection can be achieved by additional processing of the NetFlow data with complex pattern matching and rule based algorithms. So, remember to select a flow analyzer which can leverage on NetFlow data to detect network anomalies. This way you can detect threats that come beyond your intrusion detection system and firewall, thereby ensuring your network is always ready to mitigate the effect of a malware.

There are many features that may look minor, but cannot be done away with. Grouping options for better management, usage based alerts, auto emailing of reports, multiple data export options, customized reports, usage based billing, growth or change reports, SLA verification, capacity planning, etc. are some of these necessary features.

There are various other technologies available which can add a lot more value to NetFlow based bandwidth monitoring and traffic analytics. Some of the notable ones are NBAR for deep packet inspection and application classification, CBQoS monitoring for validating QoS policy performance, Cisco IPSLA to measure network performance of VoIP and data traffic, Cisco Medianet for video traffic monitoring and Cisco WAAS reports for traffic optimization visibility. When selecting a network monitoring tool, choose one which supports all or most of the mentioned technologies. With that you will own a complete network monitoring suit instead of just a bandwidth monitoring tool.

You may also have noticed that most of the mentioned technologies are from Cisco. Though Cisco leads in providing performance monitoring technologies for free to users, more users using or asking for similar monitoring technologies, should prompt other vendors to add them to their product line.
Welcome to 100G Networks

Conclusion

To get the best out of the 100G network you are investing in, leverage on the technologies available for free at your disposal. Go for a tool which can meet the demands of a high speed network, include features to add value to monitoring and has multiple monitoring technologies. A proactive monitoring solution will not only help in quicker drill down to root cause but can also help prevent small issues from turning into a network showstopper.

Something to note and remember is that a performance monitoring system is not only for the 100G network. Any network, be it 1G, 10G, 40G or 100G, requires performance monitoring as long as the priority goals of the network are uptime and application delivery. In such a case, the set of rules that applies when selecting a performance monitoring system for 100G networks applies when selecting a monitoring tool for any enterprise network.

About NetFlow Analyzer

ManageEngine NetFlow Analyzer is one tool that includes most of what was outlined. The product, which supports multiple flow formats and stores both raw and aggregated NetFlow data, has a distributed edition, which is capable of reporting in different time zones and can detect network anomalies. It supports Cisco Flexible NetFlow and features like Cisco NBAR, Cisco CBQoS, Cisco IPSLA, Cisco Medianet and Mediatrace and Cisco WAAS reports.

You can evaluate the fully featured trial for 30 days and decide if it meets the requirements of your network. ManageEngine also provides free technical support during evaluation.

About ManageEngine

ManageEngine is the leading provider of low-cost enterprise IT management software. The ManageEngine suite offers enterprise IT management solutions including Network Management, HelpDesk & ITIL, Bandwidth Monitoring, Application Management, Desktop Management, Security Management, Password Management, Active Directory reporting and a Managed Services platform. ManageEngine products are easy to install, setup and use and offer extensive support, consultation, and training. More than 40,000 organizations from different verticals, industries, and sizes use ManageEngine to take care of their IT management needs cost effectively. ManageEngine is a division of ZOHO Corporation.

For more information, please visit www.manageengine.com.
Contact Us

NetFlow Analyzer offers **FREE technical support** during evaluation period. Contact our support team for any product related assistance.

- **Support:** netflowanalyzer-support@manageengine.com
- **Request a call back:** [http://www.manageengine.com/products/netflow/support.html](http://www.manageengine.com/products/netflow/support.html)
- **Forums:** [http://forums.netflowanalyzer.com](http://forums.netflowanalyzer.com)
- **Blogs:** [http://blogs.netflowanalyzer.com](http://blogs.netflowanalyzer.com)
- **Live Online demo:** [http://demo.netflowanalyzer.com/](http://demo.netflowanalyzer.com/)
Notes and References

1. Calculation of 25% utilized 100Gbps link generating 11250GB of data in an hour:

A 25% utilization of 100Gbps link means data speed is 25Gbps. This means data was transmitted at the rate of 25 GB per second. Thus, an hour leads to (25 GB x 60 seconds x 60 minutes) 90,000 GB which is 11250GB. For those argue that 25Gbps of data transfer may never happen in real world, my point is that even 5% of that volume is huge.

http://www.fiercetelecom.com/press_releases/optical-transceiver-market-35-1h11-over-1h10-100g-ramp-will-be-faster-40g#ixzz1d05dCDkL
http://en.wikipedia.org/wiki/100_Gigabit_Ethernet#Routers_and_switches_with_100GE_interfaces
http://blog.advaoptical.com/can-100g-tame-the-network/
http://www.fiercetelecom.com/press_releases/optical-transceiver-market-35-1h11-over-1h10-100g-ramp-will-be-faster-40g