napatech

# Troubleshooting 10 Gbps with Packet Capture & Replay

**By Dan Joe Barry, Napatech**

The impending arrival of 40 Gbps Ethernet networks and the promise of 100 Gbps Ethernet in the near future have commanded headline coverage over the last year, but 2009 is more likely to be remembered as the year when 10 Gbps network deployments finally took off. One of the driving forces behind this development is the increased use of IP networks for a broad range of services ranging from Internet access to IPTV to hosted services; all services with very different requirement and characteristics.

For this reason, management of 10 Gbps networks will face new challenges as the network becomes more critical and availability is no longer a goal, but a guarantee!

Affordable tools are now available for full line-rate packet capture and replay at 10 Gbps. This opens up new possibilities for troubleshooting 10 Gbps networks.

## From network to application performance

With IP networks now being used as a converged services platform, the demands on network administrators are moving beyond simple network performance monitoring to application performance monitoring. IP networks continue to support traditional data services such as file transfer, email and Internet access, but must now also support real-time services such as voice and video. With the move to cloud computing, applications are no longer even resident on the network administrator's network, but still need to be supported for each user.

To ensure optimal application performance, the network administrator requires monitoring tools that can recognize applications, measure application response times and determine how much bandwidth is being used by each application on a per user basis.

Thankfully, these solutions exist today, even for 10 Gbps networks. High performance network appliances provide the ability to capture 10 Gbps data in real-time with zero packet loss and use the captured data to provide a comprehensive view of network and application performance.

But what happens when something goes wrong? How can these solutions be used to troubelshoot the 10 Gbps network?

## 10 Gbps Packet Capture & Replay

The Network and Application Performance Monitoring solutions mentioned above can provide a real-time view on what is happening in the network on a per user and per application basis. But, for troubleshooting purposes, there is a need to retrospectively review this data to discover the root cause of problems in the network. This requires

the ability to store captured packet data for later examination. It also requires the ability to replay this data in "real-time" – in other words, in exactly the same way as it was captured complete with timing, inter-frame gaps etc. Only with this information can a thorough analysis be performed.

To enable such a solution, there are a number of requirements that need to be met:

- All packet data needs to be captured in real-time with zero packet loss
- Each packet needs to be time-stamped to be useful for later forensic analysis
- A full-throughput capture-to-disk solution is required that can store all packet data in real-time
- It must be possible to replay all packet data as it was recorded with the same inter-frame gaps in order to fully re-create the conditions at the time of the network event.

At 10 Gbps, this is challenging, but solutions exist that address this. For example, at 10 Gbps, up to 15 million packets per second need to be captured per port, analyzed and stored to disk. That is a packet every 67ns. Needless to say, this requires high performance network probes or appliances to achieve.

There are large, proprietary hardware solutions available that meet these requirements, but these can be expensive. It is also possible to find more affordable packet capture and replay solutions that address the needs above based on standard PC server hardware using intelligent real-time network adapters designed for high-speed packet capture and replay.

## From availability to reliability

Troubleshooting IP networks has traditionally focused on ensuring availability and relied on simple, but well known tools. In the past, this has also been sufficient due to the original design intent for IP, namely that packets will reach their destination, even if there is a problem in the network. This is perfect for "bulk transfer", where information is exchanged in bursts of packets in a coordinated manner. If packets do not reach the destination or are delayed, then they are simply resent.

But, with IP networks now being used as a converged platform for almost all communication services, the requirements are quite different. "Streaming" of real-time data for voice or video is sensitive to delays and lost packets. Re-sending will not help, especially for real-time VOIP telephone conversations or when watching high-definition IPTV. The IP network can still guarantee that the stream will reach its destination through Quality of Service preferential treatment and very fast switchover to backup routes in the event of an error, but how good is the backup path? Does it have the bandwidth or performance required to handle the stream?

The key challenge for high speed networks is to adopt a strategy that moves beyond ensuring availability to assuring reliability and high performance for demanding applications. This will be crucial in supporting the general trend towards converged managed services, triple-play residential services and cloud computing.

By adopting a Network & Application Performance Monitoring solution with the capability to capture, store and replay packet data in real-time at 10 Gbps, network administrators have a powerful tool for not only troubleshooting network performance issues, but also application and service degradations, which are essential for converged services networks and cloud computing.

## Troubleshooting application performance

While Network and Application Performance Monitoring solutions provide the insight into the IP network in terms of applications and can help to pre-empt network problems, these problems can still occur.

Network Forensic tools help us to analyze real-time data to determine if there are anomalies in the network. Network probes provide the captured packet data, which is then analyzed centrally. Many Network and Application Performance Monitoring solutions include this capability.

An increasingly more popular approach is to store all captured packet data to disk, which can then be analyzed after the event to pin-point the cause of a problem in the past. This allows network forensic tools to be applied when and where they are needed.

To enable such a solution, there are a number of requirements that need to be met:

- All packet data needs to be captured in real-time with zero packet loss
- Each packet needs to be time-stamped to be useful for later forensic analysis
- A full-throughput capture-to-disk solution is required that can store all packet data in real-time
- It must be possible to replay all packet data as it was recorded with the same inter-frame gaps in order to fully re-create the conditions at the time of the network event.

At 10 Gbps, this is challenging, but solutions exist that address this. For example, at 10 Gbps, up to 15 million packets per second need to be captured per port, analyzed and stored to disk. That is a packet every 67ns. Needless to say, this requires high performance network probes or appliances to achieve.

There are large, proprietary hardware solutions available that meet these requirements, but these can be expensive. It is also possible to find more affordable packet capture and replay solutions that address the needs above based on standard PC server hardware using intelligent real-time network adapters designed for high-speed packet capture and replay.

With these tools in hand, a network administrators capabilities are significantly extended to allow more than just troubleshooting of connectivity, but also troubleshooting of service or application performance degradation.

## Looking to the future

The sheer bandwidth and number of packets that 10 Gbps in themselves necessitate more advanced troubleshooting capabilities. But the added dimension of more sensitive, real-time service requirements, as well as the move to cloud computing underlines the need for a new way of thinking in network troubleshooting and management. Ensuring availability is no longer enough – guaranteeing service and application performance should now be the focus of all network administrators. The good news is that the tools that you need to do this are available and improving every day, which should allow us all to look to the future with more confidence in our network infrastructure.