

Using Pinpoint Packet InspectionTM

for 10G Application and Network Monitoring Infrastructure

The Need for Control

Application and Network Monitoring is analogous to Air Traffic Control. Could you imagine air travel without Air Traffic Control? Not only would the situation be chaotic, but it would also be impossible for an airline to provide on-time, safe departures and arrivals or hope. Without some form of control, how could the service be profitable? The same holds true for today's applications and the networks on which they



rely. Without Application and Network Monitoring, organizations that rely upon high speed networks could not productively run their businesses or provide competitive end user or customer service levels.

The 10G Monitoring Dilemma

Let's take the analogy one step further. Imagine that Air Traffic Control now had to manage 10 times as many planes in the air! Current systems could not handle the additional number of planes concurrently in flight. This is the dilemma for data centers and networks today! With 1Gb/s Ethernet to the desktop now commonplace, 10Gb/s Ethernet is used for the aggregation and core Ethernet switches. At the same time, an ever increasing number of applications are being added to the network. How do you handle or monitor your traffic when the demands continue to increase exponentially?

Existing network monitoring infrastructure does not provide enough visibility into 10G networks. The problem is that the existing infrastructure only operates on fixed header information. That is analogous to the airport security only checking luggage and packages on the outside but never looking inside to inspect the contents.



How safe would you feel flying with that type of security? Beyond security, monitoring application performance in 10G networks is equivalent to trying to drink water from a fire hydrant.



Monitoring 10G networks requires the ability to pinpoint application or network traffic regardless of where the traffic is in the packet. **Pinpoint Packet InspectionTM** provides that ability at 10G and at full-line rate - even with jumbo Ethernet frames up to 9,000 bytes. To better understand **Pinpoint Packet InspectionTM**, let's consider the Open Systems Interconnect (OSI) model and how traditional filtering is used to identify or classify traffic.

The OSI model is based upon the concept of layering and encapsulation. While there are seven layers in the OSI, there is often an emphasis on Layer 2 through Layer 4 as it is at those layers that the vast majority of traffic classification occurs.

Current Limitations

Switches and routers are able to forward Ethernet frames and IP packets at full line rate by limiting the switching or routing process/classification to only the Layer 2 through Layer 4 header information, which contains source/destination as well as type of traffic. Further processing on the payload can cause performance issues.

Existing network monitoring infrastructure classifies traffic in the same way – using traditional fixed-offset filtering at Layers 2 - 4. Traditional filtering poses 3 significant challenges:

- 1) If the standard header information is not at the same fixed offset every time, **traditional filtering incorrectly classifies the traffic**. This is the case when MPLS, GRE, GTP and other tunneling technologies are used.

- Applications are no longer based upon specific TCP or UDP ports at Layer 4. Many new applications can be tunneled in any TCP or UDP port and are only identifiable by **digital signatures or character strings that can appear anywhere in the payload**. This is the case of IPTV as well as many peer-to-peer applications.
- Faster networks (10G and beyond) require at least **10 times the processing in order to perform traditional filtering** at full line rate. Even more processing is required to perform enhanced, content-based filtering for Layer 2 through Layer 7 traffic anywhere in the payload.

The Solution

Pinpoint Packet InspectionTM allows for content-based filtering to classify application or network traffic *regardless of where the traffic appears in the packet*. Once classified, RedDot Networks can optionally insert or remove portions of the traffic as well as add a timestamp before sending the traffic of interest to one or many monitoring tools using dynamic session load balancing.

Pinpoint Packet InspectionTM

is a requirement for 10G and greater network monitoring infrastructure. It overcomes the limits of traditional fixed offset filtering in much the same way as Deep Packet Inspection does for security, policy enforcement and traffic shaping solutions today.



Conclusion

The end result is that CIOs, IT Directors, Network Managers and Security Administrators can monitor 10G networks for maximum application and network visibility. **Pinpoint Packet InspectionTM** enhances application and network traffic monitoring to prevent overwhelming existing tools, and enables the most cost-effective deployment of 10G and 1G monitoring tools. **Pinpoint Packet InspectionTM** maximizes the value of existing and future investments in network equipment and monitoring tools.

What are you waiting for? Contact RedDot Networks today!

Pinpoint Packet InspectionTM and the OSI Layers

