Protocol Analysis for High Speed Fabrics in the Data Center

David J. Rodgers
May 2015

Summary
Ethernet and Fibre Channel fabric speeds are evolving at a phenomenal pace and require support for a diverse set of applications and protocols, including Client/Server, Web Hosting, Unified Communications, Virtual Machines and Storage traffic.

Introduction
Ethernet and Fibre Channel fabric speeds are evolving at a phenomenal pace and require support for a diverse set of applications and protocols, including Client/Server, Web Hosting, Unified Communications, Virtual Machines and Storage traffic. These applications and services are placing ever increasing demands on the network infrastructure, and the Data Center Managers, with high speed storage leading the pace of deployment needs.

The growth of the data center storage is exponential. The storage area network (SAN) now incorporates a combination of SAS/SATA spindle drives – in either RAID or JBOD configurations – new SSD arrays, and NAS appliances. These are connected to the servers via Fibre Channel, and increasingly over the high-speed Ethernet fabrics.

Recent information regarding Co-Lo datacenter construction is estimated at <20% annually through 2018.1 The advent of High Speed Fabrics - 10Gb/s and 40Gb/s Ethernet and Gen 5 Fibre Channel (16Gb/s) – and their integration into the data center, have brought about the need to reassess the test and measurement tools and techniques to keep up with deployment and maintenance demands.

These fabrics have become subject to the nuances of other high-speed bus protocols, i.e. PCIe Gen3, 12G SAS, and even USB, in the requirement for bus training and auto-negotiation sequences to ensure reliable connections. The 40Gb/s and the fast approaching 100Gb/s Ethernet interfaces will add Forward Error Correction (FEC) as a mandatory requirement for many common data center cabling media.ii

No longer are virtual probes, SPAN or diagnostic ports, and WireShark™ type packet inspection tools alone enough to thoroughly and effectively determine root cause for issues impacting the storage fabrics. In order to deploy, maintain and ensure the reliability of the fabric, the addition of tools that address the inherent challenges must be evaluated and incorporated into the data center tool chest.

Saving Your SAN (& Sanity)
The driving force behind adopting new tools and processes is the desire to understand, predict, and mitigate the impact of Sick but not Dead (SBND) conditions in datacenter fabrics, which are becoming more and more prevalent lately. The growth and centralization of datacenter SAN environments has exposed the fact that many small yet seemingly
insignificant problems have the potential of becoming large scale and impactful events, unless properly contained or controlled.

Root cause analysis requirements now encompass all layers of the fabric architecture, and new storage protocols that usurp the traditional network stack (i.e. FCoE, iWARP, NVMe over Fabrics, etc.) for purposes of expedited data delivery place additional analytical demands on the datacenter manager.

To be sure, all tools have limitations in their effectiveness and areas of coverage, so a well-constructed “collage” of best practices and effective and efficient analysis tools must be developed. To that end, recognizing and reducing the effect of those limitations is essential.

Assembling the “Collage”

Network Monitoring Software:
The ubiquitous tool in the cabinet, network monitoring utilities, come in a variety of packages and configurations. Often, these may be included by the switch, server, or SDN provider. These tools are “product centric” and utilize the diagnostic or TAP port features the vendor exposes. In some instances, these tools do offer the ability to aggregate SPAN or TAP ports from other appliances in the data center for more generalized management utility. Overall, the vendor supplied tools are designed for optimizing the operation of the given vendors tools, and the information is limited to that which the vendor chooses to expose.

There is a burgeoning market too of 3rd party applications for all sizes and types of network configurations. These are invaluable tools in assessing the real time performance of any, and often every, port in the fabric. They range from freeware applications like Microsoft’s Network Monitor, to packages licensed by seat, site, or node (i.e. Solar Winds and LogicMonitor). Some of these tout the ability to “learn” about the network under observation; others require some rather extensive setup and configuration time.

Overall, network monitoring software provides a higher level view of traffic patterns and fabric utilization so as to alert the data center manager to issues needing investigation. They can indicate trends, highlight instances of security breaches and are the primary alarm mechanism of the pending ill health of the network. In some cases, they can compartmentalize the area of concern for the further analysis by the data center manager. They are limited however for root cause determinations of the line rate issues under assessment and they are not useful in a stand-alone capacity when testing in the lab is required.

Packet Analysis Software:
The packet analysis software market is broad and deserving of an entire paper of its own. An internet search for “Ethernet packet analysis tools” will return a host of options in this segment. Some of the network monitoring applications noted herein have packet level diagnostic capabilities in addition to their other features. Suffice it to say, there is a myriad of options and choices for packet analysis including several freeware packet inspection applications.

With the noted caveat above, there are two main categories of packet inspection and capture tools to consider; those applications relying on the output of a fabric interface (i.e. NIC/CAN.TO, diagnostic TAP, SPAN, or mirror port) and those tools that operate in conjunction with a stand-alone acquisition module or appliance.
In the category of those software tools leveraging fabric connections, the most pervasive of these is the venerable WireShark™. Developed by and for network engineers, it is a robust tool supported by an extensive community of developers and contributors. WireShark supports over 1500 protocol decodes and that list grows with each iterative release. It is arguably one of the most complete packet inspection tools and certainly one that sets the standards the competition strives to overcome.

Although highly convenient method for capture, reliance on fabric participants to supply the data to be examined, and the fact the fabric participant may be part of the problem, the integrity of the captured data can be compromised. Over GigE and lower data rates, the NIC/TOE could adequately output the data stream with little effect on the operation of the NIC/TOE interface. With speeds of 10GE and 16GFC, and beyond, the ability to provide a consistent data stream to the packet analysis software becomes questionable at best. Either the passing traffic is throttled to accommodate the data collection, providing false performance information or more often, the packets are dropped and voids created in the captured traffic under analysis.

Line Rate or In-Band Analysis Tools and Software:
Relatively new to the datacenter and the SAN eco-system is the use of line rate, or in-band traffic and protocol analyzers. As stand-alone instruments, protocol analyzers do not rely on diagnostic ports, NIC or other fabric components for capture of the traffic. These tools are deployed in-line with a link under test and record all frames, sequences and primitives in the analyzers dedicated hardware. The data is then decoded and presented in the associated software.

The challenge of capturing and analyzing data on high speed fabrics is mitigated with a purpose built analyzer. Protocol analyzers offer a complete, thorough and agnostic view of the traffic on the link, and depending on the depth of decodes supported, they present the information in user readable form for all layers of traffic. Some analyzers (i.e. the SierraNet™ from Teledyne LeCroy) even allow for export of the captured data to third party tools, like Wire Shark.

A line rate protocol analyzer may be used in both the datacenter as well as on the bench in the test lab. Ideally, when the fabric management utilities indicate issues, the protocol tools will pinpoint root cause of the problem under investigation. Through the use of pre-capture filters and refined triggering methodologies, these tools can be deployed in the suspect link and provide concise and explicit information to the data center manager.

One additional benefit of the SierraNet is the ability to obfuscate or jam live traffic for purposes of problem recreation and testing a vendor supplied remediation to a known issue. The InFusion™ jamming function proves especially useful when an issue is marginal in nature and occurs randomly. Forcing nonconforming behavior on the fabric participants in order to induce failure or to test the link is especially valuable in root cause analysis and then validation testing of the “fix” before going live.

Summary:
Datacenter networks are fast approaching carrier rate speeds and as such have brought about significant changes to the testing of Ethernet and Fibre Channel fabrics. Add to this fact the evolution of protocols transiting the network and the IT professionals tasked with integrating and supporting the new switches, servers, and storage arrays are subject to new and unique challenges that have outpaced the efficacy of existing tools.

Equipment manufacturers are advancing new features in the software tools they include in effort to keep pace with the demands of the networks; however these tools are typically geared around the specific product functions and do not offer a complete test and validation solution. Network management software gives overall visibility and brings disparate equipment into one management utility and alerts the datacenter manager to abnormal events needing further investigation. Packet analysis software will highlight areas of concern providing the diagnostic port is capable of supplying the data without dropping frames or eliciting issues of their own in the fabric.
The SierraNet family of protocol analyzers provide the datacenter professional with a definitive, complete and agnostic view of the network links needing investigation. Used in concert with the fabric management utilities, the IT manager is quickly and efficiently able to determine root cause for these events, supply vendors with information for remediation work, and then test the solutions prior to general deployment in the network rack.

For more information regarding the Teledyne LeCroy family of SierraNet protocol analyzer tools and InFusion jammer utilities, please visit http://teledynelecroy.com/protocolanalyzer/.

Acknowledgments:

i “Data Center Construction Expected to Boom” (Leopold, 17 April, 2014)  

ii IEEE 40 and 100 Gigabit Ethernet Architecture” (Ganga, 2010)  
http://www.comsocscv.org/docs/Workshop_101310stdClassArch.pdf and “100G Link Training Proposal” (Lusted and Ganga, May 2012)  

iii “12 of the Most Recommended Network Monitoring Tools” (Frye, 12 April, 2010)  


https://www.wireshark.org/download.html#stable-rel