Protocol Analysis in the Data Center:
The case for line-rate analysis tools in the Data Center Managers Tool Chest

David J. Rodgers

September 2020

Summary

Data Center Managers and IT professionals are tasked with even more responsibility than ever before with maintaining the health and viability of the compute services they oversee. Advancements in Ethernet and Fibre Channel fabric speeds and new storage solutions 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

The breakneck pace of IEEE 802.3 specification adoption and the resulting application leveraging new, higher speed networks are well documented. Data center managers are challenged now more than ever when incorporating new equipment into the rack. Fueling this "need for speed" is the exponential growth in and demand for application support by the user base.

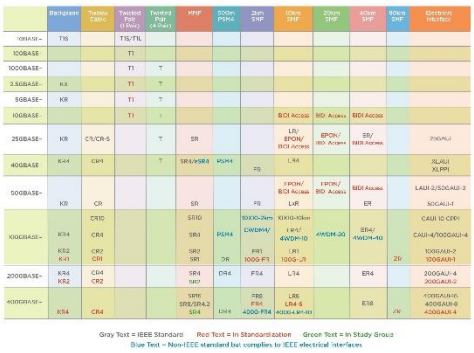
The storage area network (SAN) has evolved to support a combination of legacy SAS/SATA spindle drives – in either RAID or JBOD configurations – NAS appliances, and now new SSD arrays. These are connected in a variety of methods via high-speed Fibre Channel, and increasingly over the Ethernet fabrics.

The data center manager (DCM) and IT departments are required to be more self-sufficient and less reliant on the equipment and application vendors to ensure reliable service for their users. They must be able to determine the root cause of a problem quickly, and then affect timely and lasting remediation.

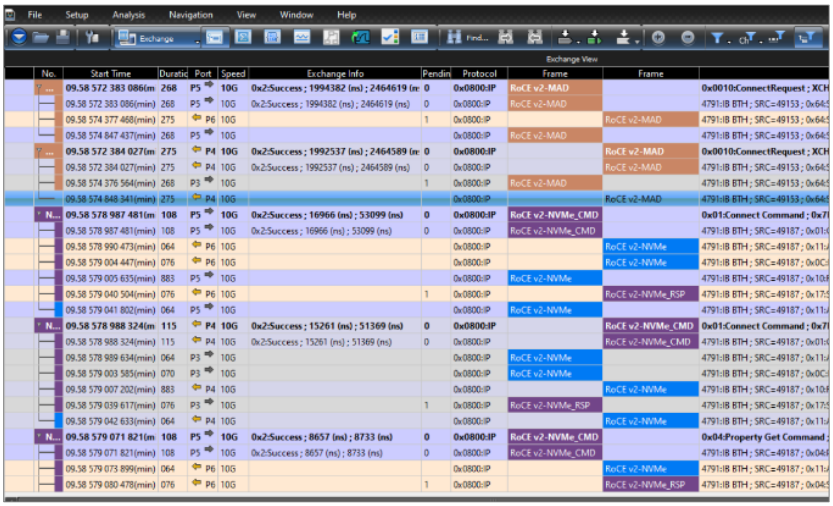
Incorporating the 'new' while maintaining the 'legacy' infrastructure has presented the DCM with a myriad of new test, maintenance, and observation requirements, and more specifically for the Storage Area Network. The DCM's responsibilities include maintaining the underlying physical structure as well as the contents of the transiting data. These advancements in hardware and supporting applications to meet the infrastructure growth require new and advanced test, validation and diagnostic tools.

Ethernet Advancements

The Ethernet Alliance 2020 Roadmap currently tracks over a dozen IEEE emerging and existing data rates, from 10MB to 400GbE, transiting over 11 copper and/or optical interconnect options, supported by over 20 IEEE 802.3 electrical signaling interfaces.



Ethernet is becoming the underlying transport technology for most all network attach storage and the compute space within the datacenter, most notably the increased demands on storage capacity and access. Solid state drive (SSD) arrays are connected directly via Ethernet or Fibre Channel fabrics, often both, obviating the need for SAS controllers and connectors. New storage protocols, like NVMe, have usurped traditional SCSI for the speed and efficiency of networks.



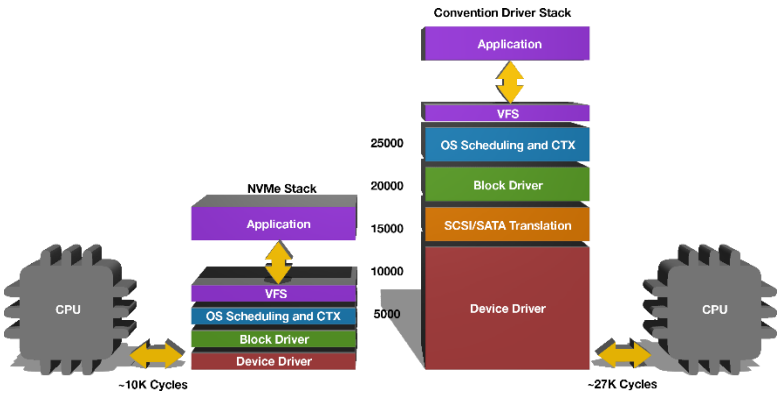
The growth of the data center storage demands is exponential as the importance of content access and cloud compute increases. The storage area network (SAN) incorporates a combination of the legacy SAS/SATA spindle drives – in either RAID or JBOD configurations – new SSD arrays, and NAS appliances. These are traditionally connected to the servers via Fibre Channel [1], and now increasingly over the high-speed Ethernet fabrics.[2] This growth of Ethernet adoption for mission critical applications combined with the advancements in link speed have brought about the need for DCMs to reassess the test and measurement tools and techniques they employ to keep up with deployment and maintenance demands.

Data-center manager job descriptions[3] include reference to the responsible person having “expert knowledge” on all the hardware and software systems in use and being able to monitor, identify and troubleshoot those same systems for any issues. The list of responsibilities is daunting at best; however, it depicts the need for the DCM to leverage any tools and experience to ensure timely integration of all new and legacy systems with adherence to industry standards and best practices.

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 need to understand, predict, and mitigate the impact of Sick but not Dead (SBND) conditions in the datacenter and enterprise network. 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. Concurrently, the requirement of the DCM to be able to pinpoint and correct the issues has grown exponentially in support of maintaining network uptime.



Root cause analysis requirements encompass all layers of the fabric architecture, from physical link bring up to and through application services. Many of the new storage protocols usurp the traditional network stack (i.e. FCoE, RoCE, NVMe, NVMe over Fabrics, etc.) for purposes of expedited data delivery and 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 and debug tools must be developed. To that end, recognizing and reducing the effect of those limitations and adding the right tools to the tool chest is essential.

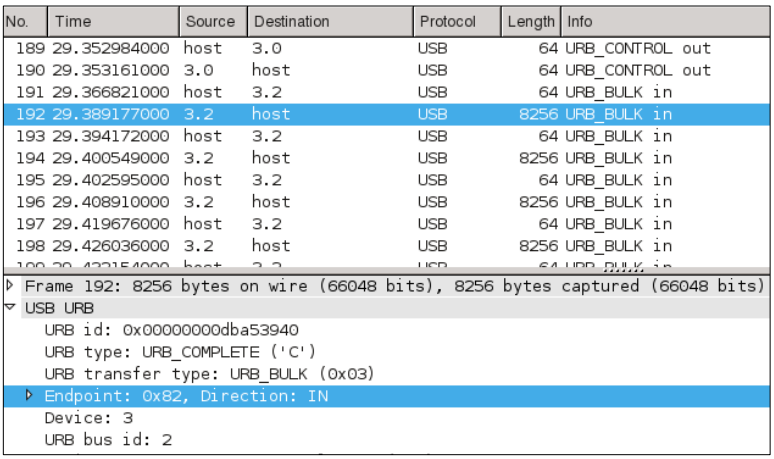
Assembling the "Collage"

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 applications tout the ability to "learn" about the network under observation; others require some rather extensive setup and configuration time.[4]

Overall, network monitoring software provides a higher-level view of traffic patterns and fabric utilization 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.[4]

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.TOE, 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[5] 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 a 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 10GbE and 16GFC, and faster, 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.

The use of packet capture and analysis software is limited too in its ability to pinpoint areas of concern as the user is required to “mine” the data for anomalies or errors.

Line Rate or In-Band Analysis Tools and Software:

Although used by the manufacturing community, a relatively new offering to the datacenter and the SAN eco-system is the use of line rate, or in-band traffic and protocol analyzers. Protocol analyzers are stand-alone instruments and do not rely on diagnostic ports, NICs or other fabric components for capture of the traffic. They are fully self-contained with appropriate probing and link maintenance capabilities that capture the entire framed, primitive, and link layer traffic for a complete view of the link and network under observation. Being self-contained, they impose no restrictions and have no impact on other components in the link, thereby capturing the information cleanly and without embedding any anomalies or features of their presence.

Feature Definition

Deep Packet Inspection	Deep packet software inspection is a technique for monitoring network and application traffic at the packet level. These utilities require output from a TAP, SPAN, diagnostic port, or other component in the network to supply access to the traffic to be inspected.
Protocol Decoding	Protocol decoding is the process of translating an electrical signal from a serial bus into meaningful bit sequences as defined by the standards of the protocol being analyzed.
Phy Layer Observation	The ability to capture and review the transmission of raw bit stream over a physical medium
Unfiltered Reporting	The capture and review of all transactions, events, and bits transiting a network or link under observations. Limitations in certain diagnostic tools or ports filter Phy layer information.
Trigger for Event Capture	A focused and targeted method to capture a defined error condition, traffic pattern, datagram, or specific event of interest
Self-Contained Observation	Stand alone and complete test equipment and utilities, operate independently of other equipment or access points of the link/network under observation. Represents the entire link condition, from physical layer through application services.

The protocol analyzer may be deployed in-line with the link(s) under test or attached to a network or fabric TAP or mirror port of a switch to record all frames, sequences and primitives in the analyzer’s dedicated hardware. The data is then decoded and presented in the associated software and may be correlated with information reported by other diagnostic tools in the DCM’s tool chest. The key benefit of these tools is the ability to capture the entire link condition, from the physical layer to and through the application layers of the network, amassing the information into a consolidated and complete picture of the link under test.

Protocol Analyzer vs DPI Software vs Diagnostic Switch

Feature	Diag Switch	DPI Software	Protocol Analyzer
Deep Packet Inspection capabilities	Access point only, no native protocol inspection. Access point may filter physical layer and unrecognized or unassociated traffic.	Relies on access point within the network/link under test. Unable to report Phy layer issues	Provides for complete physical layer through application layer DPI capabilities
Protocol Decoding	Not available	Supported	Supported
Phy Layer Observation	Possible depending on vendor	Not available	Supported
Unfiltered reporting	Possible, depending on vendor	Possible, depending on vendor and implementation	Supported
Trigger for Event Capture	Possible for some common or simple events	Possible for some common or simple events	Provided for all simple and complex scenarios
Self-Contained Observation	Supported for limited event observation	No, Requires network access points	Supported

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. Using 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. The SierraNet offers users a substantial capture memory depth, in some cases up to 128GB, with detailed pre-capture filtering options, to ensure events needing analysis are retained along with corresponding information required to understand and debug the condition(s) of interest.

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 can supply 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 data center 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/.

Acknowledgements

[1] "Fueling growth in Financial Services with High Performance NVMe Data Storage" (Herd, 7 Feb. 2019)
https://www.dataversity.net/fueling-growth-in-financial-services-with-high-performance-nvme-data-storage/

[2] "NVMe™ over Fabrics (NVMe-oF™) Explained" (Western Digital Corporation)
https://blog.westerndigital.com/nvme-of-explained/

[3]"Data Center Manager Responsibilities and Duties"
https://www.greatsampleresume.com/job-responsibilities/information-technology/data-center-manager

[4] "The Top 20 Free Network Monitoring and Analysis Tools for Sys Admins" (Tabona, 23 July, 2013)
http://www.gfi.com/blog/the-top-20-free-network-monitoring-and-analysis-tools-for-sys-admins/

[5] "WireShark: Supported Protocols" WireShark version 1.12.4 (4, March, 2015)
https://www.wireshark.org/download.html#stable-rel

[6] "The 2020 Ethernet Roadmap" (Ethernet Alliance, Jan 2020)
https://ethernetalliance.org/technology/2020-roadmap/