

# FIBRE CHANNEL

SOLUTIONS GUIDE 2024



## **FIBRE CHANNEL**

Powering the next generation private, public, and hybrid cloud storage networks

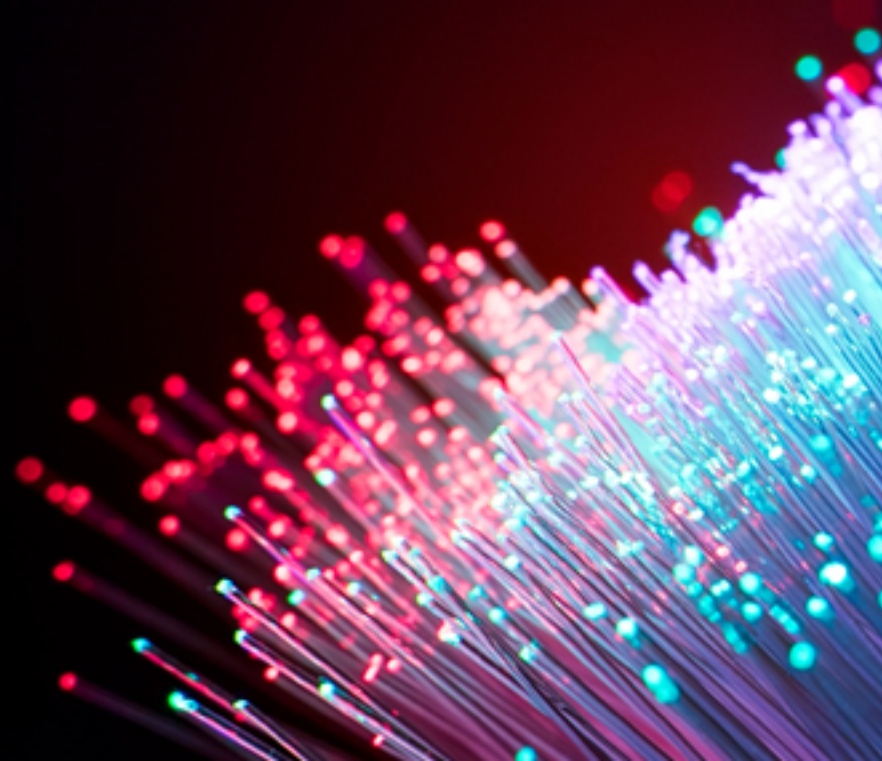
## **ABOUT THE FCIA**

The Fibre Channel Industry Association (FCIA) is a non-profit international organization whose sole purpose is to be the independent technology and marketing voice of the Fibre Channel industry.

We are committed to helping member organizations promote and position Fibre Channel, and to providing a focal point for Fibre Channel information, standards advocacy, and education.

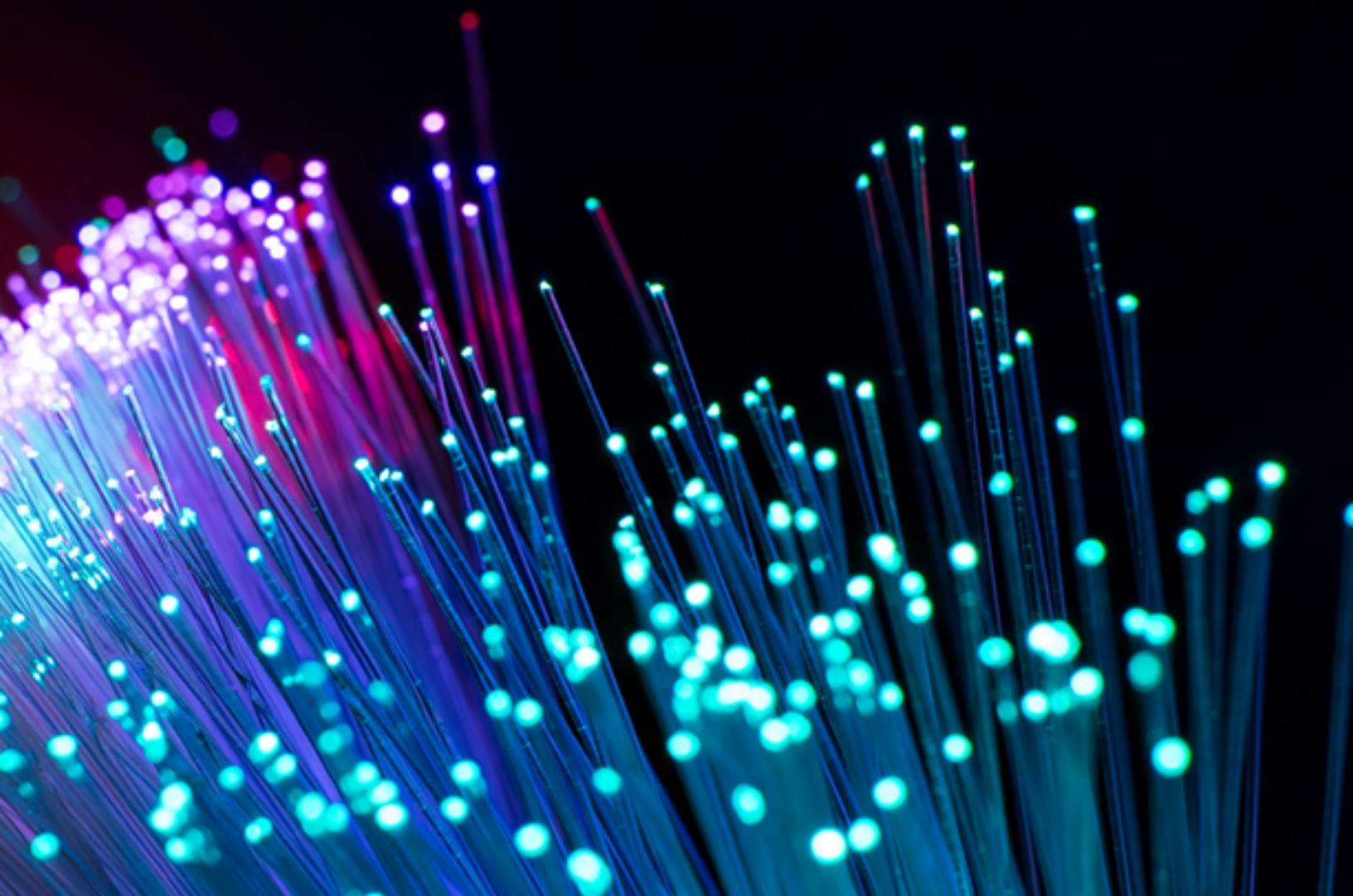
## **CONTACT THE FCIA**

For more information:  
[www.fibrechannel.org](http://www.fibrechannel.org) • [office@fibrechannel.org](mailto:office@fibrechannel.org)



# Contents

President's Intro	3
Supercharge Oracle TimesTen In-Memory Databases with Gen 7 Fibre Channel	6
The Art of Automation in Fibre Channel	9
Avoiding Disaster: 64G Fibre Channel Extensions over DWDM for superior network performance	12
Fibre Channel Advances Security in a Quantum World	15
Introducing 128G Fibre Channel for Storage Networking	22
Fibre Channel Industry Association (FCIA) Members	25



## 2024 FCIA Solution Guide

# President's Intro

Mark Jones – FCIA President Emeritus

Happy Anniversary to the Fibre Channel Industry Association (FCIA) – 30 years and still going strong! For three decades, this nonprofit international organization of manufacturers, system integrators, developers, vendors, industry professionals, and end users has pioneered our fast, secure, and scalable protocol for server-to-storage and server-to-server networking.

The origins of the FCIA date back to 1994 when the two existing Fibre Channel-protocol trade organizations, the FCA (Fibre Channel Association) and FCLC (Fibre Channel Loop Community), merged to form what is now known as the FCIA. The original development of the Fibre Channel standard can trace its origins even further back, to 1988, making the protocol over 35 years old!

According to Quillin Research, Fibre Channel achieved another major milestone this year by exceeding the \$50 Billion barrier in cumulative adapter and switch revenue since 1998 (Figure 1). This is significant because it points to the value of an industry that works as one to solve market needs through innovation while fostering a multigenerational technology trend that rewards participating product vendors with long-term revenue generation. Over this period, more than 160 million Fibre Channel ports have been shipped with an estimated 35 million in service today. The forecast for Fibre Channel is strong, with consistent and expected growth to exceed 180 million ports shipped by 2027.

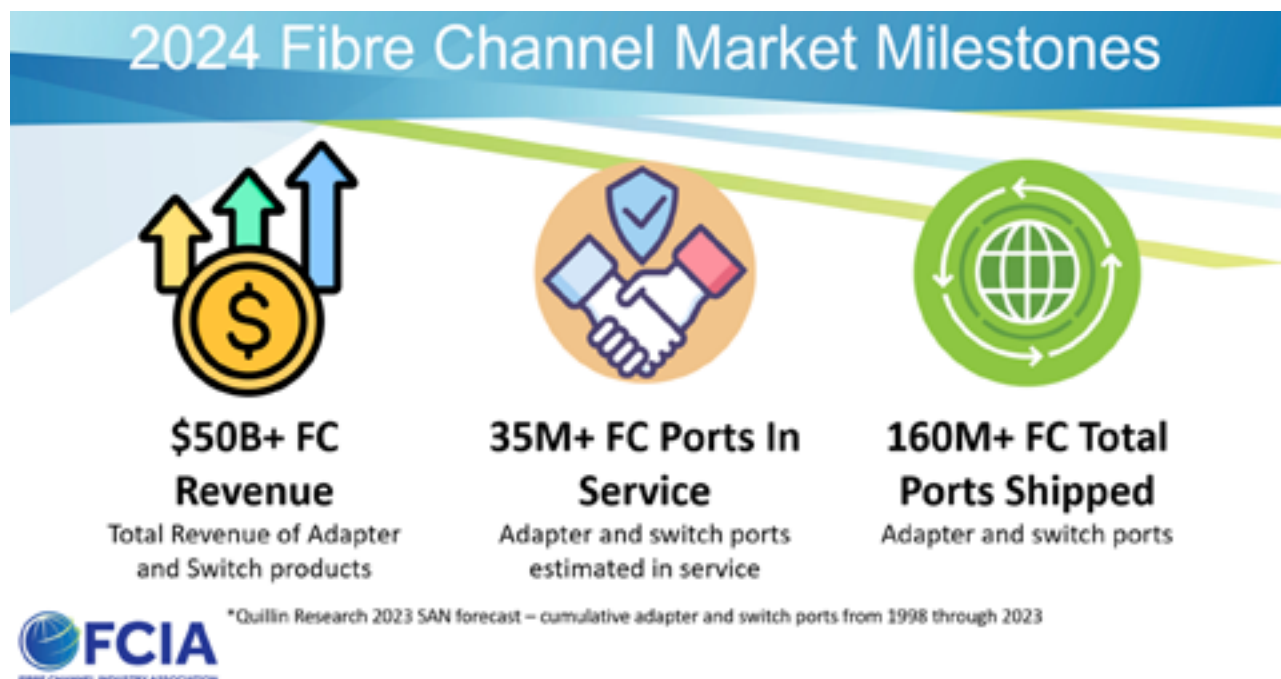


Figure 1

Fibre Channel is well into its 7th speed generation: 64GFC, or Gen 7, has been in the marketplace for a number of years and is becoming the dominant speed that is shipped today. Crehan Research Inc. announced in June 2024 that the 64GFC HBA (Host Bus Adapter) market had posted its second consecutive quarter of 30% revenue growth (Figure 2). The adoption of 64GFC is now starting to surpass that of 32GFC in the marketplace.

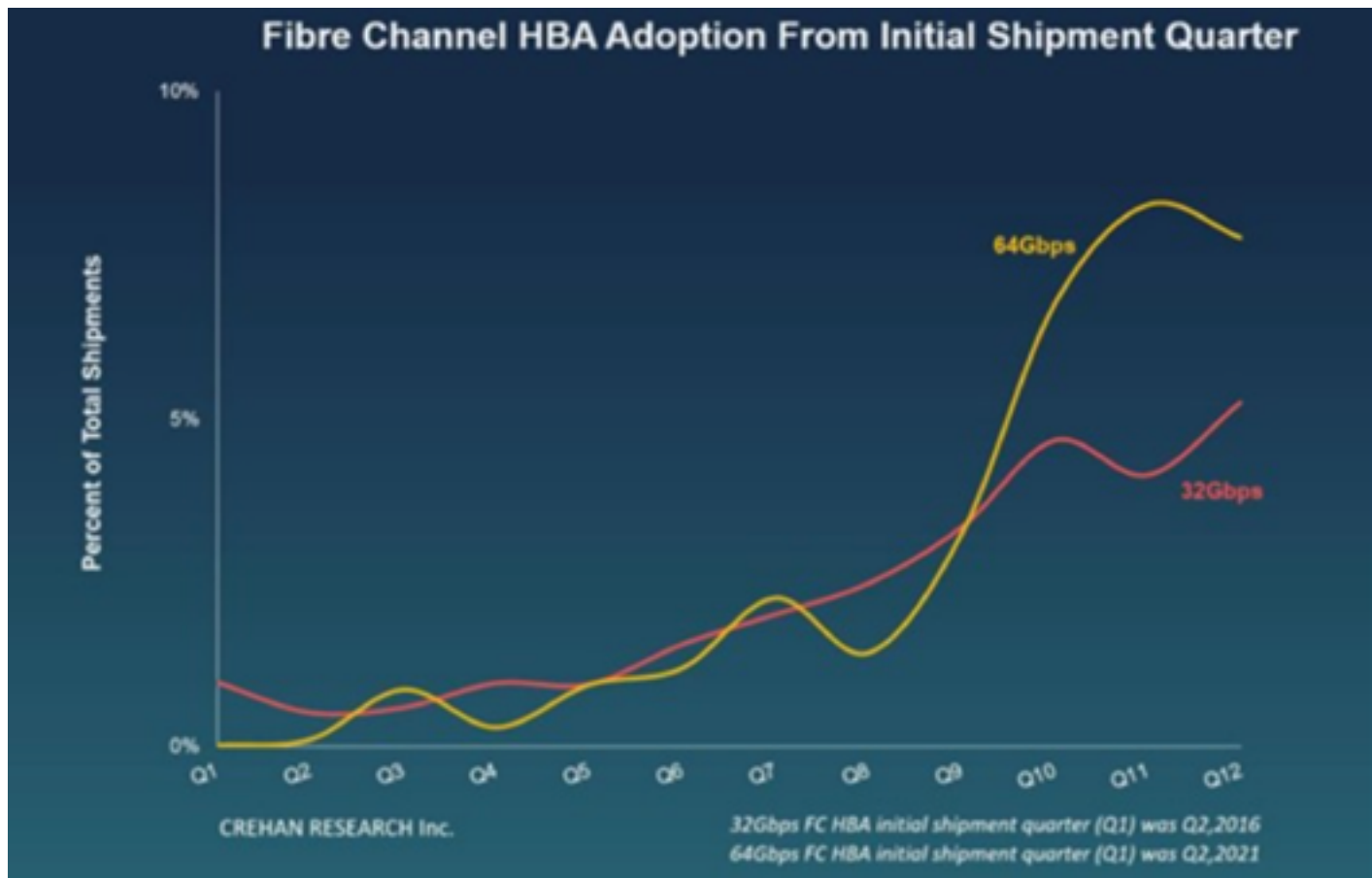



Figure 2

In late 2023, the FCIA hosted its 41st plugfest event at the University of New Hampshire InterOperability Laboratory. The event was the first plugfest with a broad ecosystem of 64G Fibre Channel Gen 7 devices to be held under a single roof. The results of this plugfest provide assurance to the Fibre Channel SAN community that the latest 64GFC specification meets the needs of flash storage technologies. The nine participating companies are the major vendors of FC HBA, fabric switch, optics, cable, and test equipment products.



Development of the Fibre Channel standard continues within INCITS/Fibre Channel (formerly INCITS/T11), the group of engineers and technical architects from a diverse group of companies that regularly meet to work on a series of enhancements to keep Fibre Channel at the forefront of data center technology. The committee completed the FC-PI-8 standard (the standard for 128GFC Fibre Channel speed) in 2023, and already the group has started on FC-PI-9, the single-lane standard for 256GFC. Additional major initiatives include FC-RDMA, which is the mapping of the remote direct memory access (RDMA) protocol to run over Fibre Channel. FC-RDMA will help folks that use RDMA applications take advantage of the advanced management and security inherent within a Fibre Channel fabric. The T11 workgroup FC-SP-3 is advancing Fibre Channel security capabilities by updating the standard to meet future government data encryption regulations while at the same time allowing for FC in-flight encryption to be automatic and ubiquitous in the future.

Other approaches to end-to-end encryption involve application-based mechanisms that are both expensive due to licensing and prevent storage array features such as compression and de-duplication from delivering customer value. Encrypting automatically between zero-trust endpoints, such as Secure HBAs, will help customers meet upcoming government regulations while saving significant cost and maintaining advanced array features.

Looking forward to the next 30 years of Fibre Channel, education is a key initiative within the FCIA. The [FCIA Brighttalk channel](#) regularly adds new content presented by the technology experts that craft the industry standards for storage networking. Please visit the [FCIA website](#) to find [future roadmaps](#), articles, blogs, and the latest news on Fibre Channel technologies and products. The FCIA also offers its [YouTube channel](#) highlighting dozens of video presentations organized into playlists according to skill level – something for everyone from Fibre Channel basics to expert’s courses. Please follow the FCIA progress by visiting on social media at [@FCIAnews on twitter](#) and [Facebook](#).

Thank you all for being part of this important community, and best wishes for the next 30 years!

# Supercharge Oracle TimesTen In-Memory Databases with Gen 7 Fibre Channel

By Vikram Umachagi | ECD Technical Marketing and Performance Engineer Broadcom Inc

---

## Technology Overview

### Oracle TimesTen In-Memory Database

In-memory databases have been around for a long time. They operate by managing data in random access memory (RAM) instead of the non-volatile storage that traditional relational database management system (RDBMS) databases rely on. An in-memory database runs completely from system main memory, thus improving the speed of transactions with dramatic gains in responsiveness and throughput. Unfortunately, this comes with the added cost of storing the data in system memory (RAM), which is also limited in capacity.

Since data volumes are constantly increasing, so does the cost of in-memory databases, so their use is typically limited to specific applications demanding real-time, high-volume online transaction processing (OLTP) in industries such as telecom, financial services, and location-based services.

### Gen 7 Fibre Channel

Improved performance in any application requires changing the underlying hardware, which can also deliver higher capacity at scale. For faster compute, the improvements are delivered by the latest CPUs and memory technologies. For faster storage, new flash-based storage arrays have significantly improved access times. For faster applications, a faster interconnect is also required. This blog discusses one example of a modern application or workload accelerated by a faster interconnection technology, the Gen 7 Fibre Channel (FC) Storage Area Network (SAN) protocol. Fibre Channel is the most trusted high-speed networking technology used in data centers today. The latest, seventh generation of Fibre Channel provides double the throughput from 32G (in Fibre Channel 6?) to 64G.

## Business Challenge

In-memory databases need persistent storage to store the backup, logs, snapshots, and redo operations, etc., required to recover from power outages and server downtime issues. This means that one copy of the data in some format has to be stored in persistent storage. For enterprise data centers, that usually means their persistent storage is a Fibre Channel SAN.

The data stored as persistent storage on a Fibre Channel SAN has to be loaded into main memory (RAM) at database startup after planned or unplanned server downtime. As the scale of a database increases, this usually means hours or even days are needed to restore the database into main memory before the database can start serving users.

## Solution Overview

### Benefits of Gen 7 Fibre Channel

Startup of an in-memory database requires moving all the database data residing in SAN storage to the host memory. The sooner that's done, the sooner the application is back online. Time for loading the database into RAM will depend on system capacity and database size. When using a Gen 7 FC Host Bus Adapter (HBA) you can . double the throughput over a Gen 6 FC HBA.

We were curious to see if that advantage would hold up in the real world amid variations in system design and components. Hence, we put the newer HBA to the test and benchmarked 64G and 32G performance for this blog.

## Solution Architecture

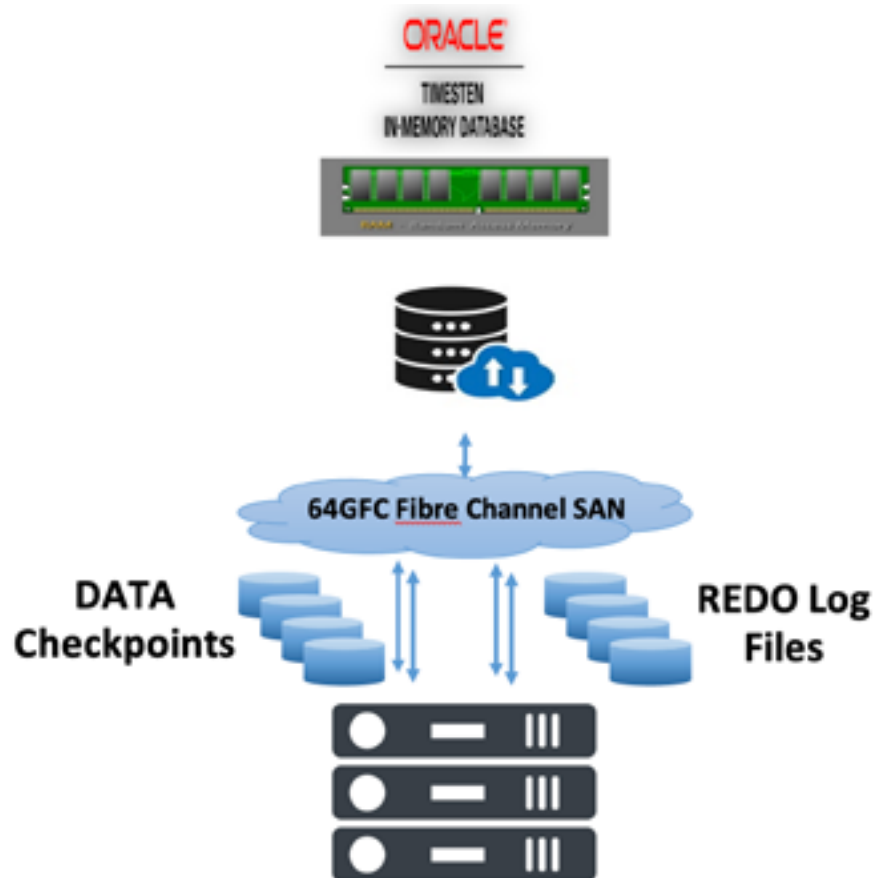


Figure 1



## Performance

A sample workload was created using an x86 Intel Eagle Stream server connected to an all-flash array (Figure 1). The SAN array provided the permanent storage used by the Oracle TimesTen Database (TimesTen). The TimesTen database was installed on the server. The database was filled via the sample data generator application provided by the TimesTen developer website located here.

This data was stored in the main memory of the server for faster access along with redo logs and checkpoint data, which gets written to the file system mapped from the Fibre Channel SAN array. After the server restart, the database services started reading the data from permanent storage into main memory through the FC SAN. TimesTen allows for the parallel reading of the checkpoints to load the data faster. As the data is read in parallel from multiple checkpoint files, the transfer of data was limited by the throughput of the FC technology in use, i.e. 32G for Gen 6 FC and 64G for Gen 7 FC.

Even for a small database with around 100GB of data in checkpoint files, we saw that the time taken for data transfers was 85% longer with 32G than 64G (Figure 2). In a large data center deployment we would expect to see an even greater improvement in data transfer time with 64G compared to small test setup used here.

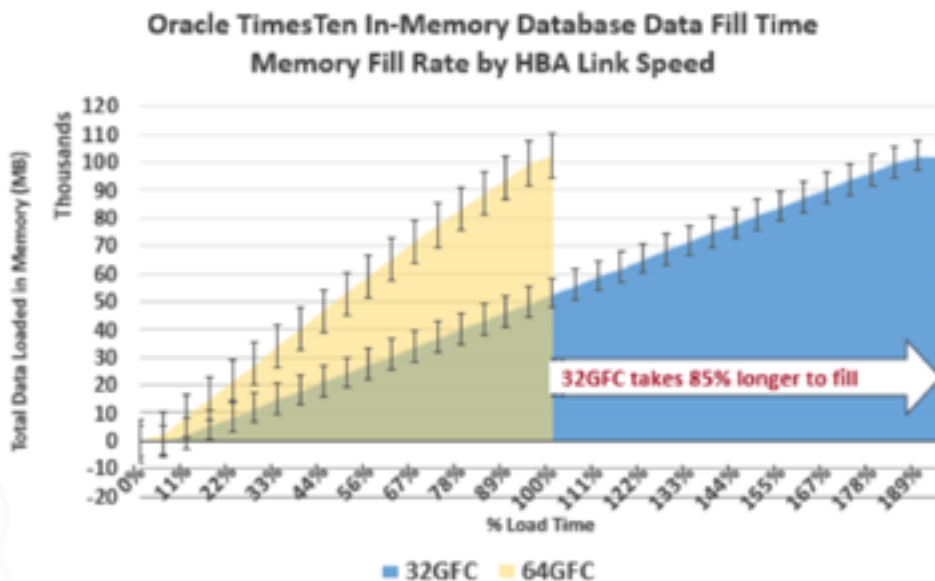


Figure 2

## Conclusion

In the dynamic world of software applications, startup times play a crucial role in user experience. The symbiosis between software applications and hardware leads to optimal performance. This need for instant engagement drives the convergence of advanced technologies. As demonstrated in testing, the Gen 7 FC HBA supercharged the startup of the TimesTen database and provided an applause-worthy performance.

# The Art of Automation in Fibre Channel

By Howard Johnson, FCIA Member, INCITS/Fibre Channel chair, Broadcom Technology Architect

---

I cannot wait for self-driving cars! I want to be able to hop in my car, say, “go to work,” and have it get me there safe and sound – under any circumstances. Yet, with all of the advancements from the likes of Tesla, BMW, Mercedes, and the big three, it is going to be a while before we get to that point. In the meantime, I am enjoying some of the cool features that make the task of driving easier like lane detection, keeping, and centering. Just thinking of all the technology needed to make these features work reveals the challenges for any system attempting this level of automation. One of the biggest challenges is determining how to assimilate and condense the massive amounts of information presented to the system at any given time.


In the 2020 Solutions Guide, we introduced Fabric Notifications, which is an element of automation for the Autonomous SAN in Fibre Channel. It addresses the challenge of processing device-generated data by a) enlisting the existing features of Fibre Channel SANs to invoke notifications for detected problems and b) condensing the information into a simple description used by the participating devices to drive the automation.

## Lane Detection

Lane detection was the first step toward self-driving cars. Automobiles outfitted with cameras gather information about the road, which is fed into an onboard computing complex to provide warnings if the car deviated from its lane.

Similarly, devices in a SAN have significant capabilities to detect anomalies and generate messages associated with those anomalies. The difficulty is that the ever-increasing number of devices in storage and SAN infrastructures challenges administrators with ever-increasing amounts of data to be processed. Devices have significant detection and reporting mechanisms that log information that administrators have to process to find the source of problems detected and reported by the devices. As the system grows, the amount of information in the logs grows beyond the administrator’s capacity to process it in a timely manner. Even worse, the sheer volume and velocity of the data produced by the devices in the system can turn the smallest problem into hours, if not days, of time to isolate and mitigate.

For example, in a large storage network, a faulty optic can cause each layer of the system to generate log messages. The network hardware (e.g., switches) logs that a transmission error occurred, the transport



hardware (e.g., HBAs) logs that an IO request error occurred, the IO system software (e.g., multi-pathing) logs that an IO retry occurred, and the application (e.g., backup application) logs that a read or write request timed out. Each layer of the system produces log entries for the same instance of the error. Often in communications networks, the process repeats numerous times depending on the volume of traffic and frequency of failures caused by the faulty optic. The result is a large amount of log data for the administrator to wade through!

## Lane Keeping

The task of the administrator is to sort through all of these messages to find the one message that indicates a transmission error occurred. It is no wonder administrators are turning to various devOps tools to help them process log data for pertinent messages and generate summaries.

Typically, these devOps tools provide a kind of lane-keeping function similar to what is available in newer vehicles. With lane keeping, the car assists the driver to maintain its position in the lane – it tries to keep the vehicle between the lines. In a storage network, the devOps tools leverage the device APIs to extract information and condense it into actions that keep the system from wandering too far off course. These tools can often generate work tickets that summarize the actions necessary to resolve a particular problem.

This level of automation provides the valuable function of reducing the massive quantity of log data generated by the system into a much smaller set of tasks that help keep the environment running. However, the administrators are not off the hook because they react to the tickets generated by the system, execute the instructions summarized on the ticket, and determine if the actions described in the ticket actually resolve the problem.

## Lane Centering

The current state of self-driving technology provides a lane-centering function that does more than keep the car between the lines; it optimizes the car's position in the lane. Rather than warning the driver that the car is outside of the lane or noticeably correcting the car's path, lane centering constantly monitors the data to keep it centered.

Fabric Notifications takes a similar approach for Fibre Channel networks. It leverages the intelligence of the devices in the system and provides a method for condensing and sharing the information with the device's peers. Each device evaluates the information in the notification to determine the most appropriate action to keep the system functioning optimally – keep it centered.

## The Art of Automation

On the road to self-driving cars, the automation of driving evolved from lane detection to lane keeping to lane centering. With each innovation, a new level of possibilities is revealed. Automation in the data center is also a continuously evolving endeavor. Each step produces solutions that reveal the objectives for the next level of the automation.

The art of the possible begins with an idea that expands and evolves simply. Fabric Notifications embraces this concept and allows solutions to evolve and expand as needed. Storage arrays have adopted Fabric Notifications to address the problem of information overload impeding problem determination, isolation, and mitigation. The arrays register to receive notifications and store the notifications in their system logs. This provides a key for devOps tools to locate and surface, which reduces problem determination time. The notifications include the location of the detected event leading to a reduction in the problem isolation time. Finally, knowing the nature and location of the problem reduces the problem-mitigation time from days to minutes.

Similarly, a Fabric Notifications-enabled server with a multi-path solution leverages the detection capabilities of the devices to locate the occurrence of the intermittent physical issues. The detecting device generates the notification sent to its peers affected by the event, and the multi-path solution instantly knows the location and nature of the physical error. It can then “route around” the impacted path by utilizing good, alternate paths. Much like lane centering for the self-driving car, the administrator is not involved in the identification, isolation, and recovery of the error.

## Self-driving SANs

The Fibre Channel technical committee developed the architecture for Fabric Notifications to improve the resiliency of Fibre Channel SANs. The objective was to simplify the task of administrators as the scale of their systems grew. By employing the intelligence inherent in the system at the point of detection, the Fabric Notifications architecture produced flexible solutions that can adapt and move closer toward full automation.



# Avoiding Disaster: 64G Fibre Channel Extensions over DWDM for superior network performance

---

As data demands continue to grow exponentially, the need for robust and reliable high-speed data transport solutions is paramount. 64G Fibre Channel (64GFC) technology is becoming a critical tool in the arsenal of modern data centers, offering enhanced performance, scalability, and security. It's powering shared storage arrays in large organizations, low-latency financial service transactions, and scientific research, among many others. This chapter explores the latest advancements in 64GFC, highlights its integration with Dense Wavelength Division Multiplexing (DWDM) systems, and describes best practices for its deployment in mission-critical environments.

## Fibre Channel vs. Ethernet for Data Center Interconnects

While Ethernet interconnections are popular in data centers, Fibre Channel remains a preferred and even necessary choice for storage applications in mission-critical environments such as banking, government, and healthcare due to its reliability, deterministic low latency, and robust performance. Fibre Channel networks are designed specifically to achieve the lossless and in-order data delivery that storage applications require, and that Ethernet cannot consistently guarantee. Additionally, Fibre Channel's unique addressing scheme is separate and distinct from IP routing, making Fibre Channel fabrics not reachable from IP networks. This shields the fabric from IP network-based cyber threats and increases security, making Fibre Channel a resilient option for sensitive data transport. When combined with DWDM transport, Fibre Channel can operate over distances of 100km or more.

## The Advantages of 64G Fibre Channel and DWDM

64GFC technology delivers a significant leap in performance over 32GFC, providing ultra-low latency and doubling data transfer speeds. These attributes make it particularly well-suited for applications requiring high-speed storage, real-time analytics, synchronous replication, and disaster recovery. The integration of 64GFC with modern Optical Transport Network (OTN) DWDM systems enhances these capabilities, allowing for greater scalability, geographic diversity, and operational efficiency.

## Maintaining Data Integrity with Fibre Channel Extensions

Fibre Channel is designed to deliver data with unmatched reliability and integrity for mission-critical applications. By using link-based forward error correction and end-to-end error detection and recovery mechanisms, Fibre Channel ensures that data is received accurately and without loss. Unlike many other transport protocols, Fibre Channel guarantees consistent in-order delivery, eliminating the risk of data corruption due to out-of-order reception.

When extended over well-designed DWDM systems, Fibre Channel continues to maintain this high level of data integrity. Modern DWDM systems apply their own error correction schemes and are transparent to Fibre Channel's native error-checking protocols, allowing data to traverse long distances without degradation.

## Enhanced Security Through Double Encryption


Security is a critical concern when extending Fibre Channel networks, especially when data traverses outside of secure environments. Encryption provides a strong defense against data breaches and unauthorized access. With DWDM, users can benefit from independent SAN switch encryption and DWDM layer-1 encryption, enhancing overall security through a layered Defense-in-Depth approach.

DWDM layer-1 encryption is capable of encrypting multiple FC rates as well as other data protocols that may be transported on the data center interconnect (DCI) network. It does so without reducing throughput, transparent to the higher-layer protocols, allowing for independent FC protocol encryption.

In multi-tenant environments where the DWDM system encrypts the traffic of all tenants, this double encryption approach provides additional assurance that data remains secure even if one layer is compromised. This strategy also addresses potential vulnerabilities where only frame payloads are encrypted, leaving headers or metadata exposed. By encrypting at additional layers, Fibre Channel extensions safeguard all components of the data, including metadata that could otherwise be exploited.

## Robustness Against Fiber Cuts and Network Failures

Fibre Channel extensions over DWDM benefit from enhanced protection mechanisms. They are designed with robustness and reliability in mind, particularly in the face of physical network disruptions like fiber cuts. DWDM systems that conform to OTN standards implement rapid failover and protection schemes that significantly minimize downtime and data loss.



If a fiber cut occurs, OTN devices automatically forward the Non-Operational Signal (NOS) to downstream devices, prompting the SAN switch to perform the Link Init protocol and eventually recalculate fabric topology if it becomes necessary. This automatic response helps maintain the integrity of the fabric by swiftly indicating to the switch that a link is no longer operational and enabling the switch to use its native Fibre Channel methods to re-establish the link, reroute traffic and react to a persistent change in topology.

Additionally, DWDM systems can be deployed with fiber-path redundancy using protection schemes that can restore the connectivity of Inter-Switch Links (ISLs) within milliseconds after a fiber cut, allowing restoration of connectivity before the Link Init protocol becomes necessary, further reducing recovery time and maintaining high availability.

For environments without path redundancy, or in cases where the protection system has failed to restore the signal, shutting off the laser on the affected port can signal a hard failure, prompting recalculation of fabric topology to minimize impact. However, deploying DWDM systems with path protection is recommended where possible, as this provides an affordable and effective means to handle fiber cuts and maintain network stability.

### **Inter-Switch Link (ISL) DWDM Integration**

For optimal performance, DWDM systems should be configured to be transparent to all Physical Coding Sublayer (PCS) characters on the ISL, supporting standard Fibre Channel traffic as well as vendor-specific implementations.

Latency, including total and differential latency, should be minimized to maintain high performance and support a wide range of applications. Planning DWDM fiber paths with an understanding of application requirements is essential to maximize the performance of ISL features.

### **Summary**

The 64GFC rate is setting new standards for performance and reliability in data center interconnects. By integrating 64GFC with DWDM and adhering to best practices for encryption, link management, and redundancy, organizations can ensure their data centers are equipped to handle the demands of modern, high-speed data environments. Using DWDM extension of 64G Fibre Channel offers a set of robust, secure, scalable, and efficient transport solutions, enabling mission-critical applications across interconnected data centers, allowing fabrics to scale between facilities, and playing an indispensable role in supporting business continuity and disaster recovery objectives.



# Fibre Channel Advances Security in a Quantum World

*Barbara Porter – Product Marketing Manager, Broadcom Inc.*

---

Data breaches are becoming more frequent and more expensive. In industries categorized as critical infrastructure – health care, financial services, pharmaceutical, energy, transportation, and industrial – the losses are significantly higher than in other sectors. In 2024, the health care industry experienced the highest average data loss cost at US\$9.77 million per breach, double the average breach cost of US\$4.88M million.<sup>1</sup>

That's worrisome because powerful new quantum computers will bring grave new threats on top of the increasing baseline risk. Cybersecurity experts fear that quantum computers will be able to crack cryptographic algorithms that have long resisted cyberattack by traditional computers.

## The Quantum Threat

Although current computing technology might theoretically be able to solve the math behind current cryptographic solutions, the possibility remains speculative given the prohibitive expense of trying it. It's been demonstrated, however, that quantum computers will be able to solve such complex problems in a fraction of the time.

Quantum computing relies on physics at extremely small scale and at low temperatures to execute an [entirely new category of algorithms](#). "Security" as it is known in the classical computing context is no longer secure.

In response, governments around the world have developed new laws and regulations aimed at modernizing data centers. The Fibre Channel industry has responded with new standards that tighten the security on what is already considered the world most secure – and in fact, air-gapped – network technology upon which critical infrastructures rely for their most valuable data assets.



## The Hack

The [2020 SolarWinds attack](#) spurred governments around the world to initiate a slew of new regulations. By managing to insert malicious code into a SolarWinds software product update, hackers gained access to the networks, systems, and data of thousands of SolarWinds customers, including federal government systems. The company's update of its Orion network monitoring software inadvertently infected 18,000 of its customers. The scope of the hack is unprecedented and is one of the largest ever documented (if not the largest).

## Governments Step In with Zero Trust Architecture Mandates



In response to the SolarWinds hack, the U.S. President Joe Biden on May 12, 2021, issued a Presidential Executive Order to Improve the Nation's Cybersecurity. The order included a mandate that government suppliers modernize their data centers, including adopting the principles of Zero Trust Architecture. The United Kingdom's National Cyber Security Centre (NCSC) issued its own guidance for enterprise environments focused on zero trust concepts. The fundamental tenets of zero trust include authentication between all entities and encryption of all data flows. The essence of zero trust: "Never trust any network,

especially your own.”

A zero trust architecture is defined by seven key tenets, each essential for its effective inclusion in a company’s cybersecurity infrastructure:




## Preparing for a Quantum Future



PRESS RELEASE | Sept. 7, 2022

NSA Releases Future Quantum-Resistant (QR) Algorithm Requirements for National Security Systems



Of course, zero trust solutions would be ineffective if they didn't account for the quantum computing threat. Accordingly, in 2022 the U.S. National Security Agency (NSA) issued its CNSA 2.0 requirements, mandating the use of new quantum resistant algorithms (QRAs). This followed up on the initial CNSA 1.0 advisory in 2016, which recommended higher strength classical algorithms until the NSA could complete its quantum resistant algorithm investigation. In parallel, the European Union announced its Cyber Resilience Act (CRA), which mandates common EU requirements for hardware and software.

An essential authority in computing standards is the National Institute of Standards and Technology (NIST), a scientific partner of the NSA. Together, the organizations formulate U.S. cryptographic policy. NIST authorizes suitable encryption algorithms for widespread use by servers and standardizes cryptographic solutions. Original encryption algorithms used in classical computers were once considered very secure, as computers did not have the strength or processing capabilities to decrypt these algorithms. One such algorithm, the most commonly and widely used and accepted form of encryption, is the Rivest-Shamir-Adleman (RSA) algorithm. It is an asymmetric algorithm that ensures a reliable level of confidentiality in the classical computing context. Classical computers simply do not possess the processing capabilities or efficiency required to realistically crack such encryption.

The landscape changed in January 2019 with the introduction of the first fully integrated, circuit-based commercial quantum computer, the IBM Q System One. Five years later, quantum computers are being deployed in universities and research labs and are expected to scale solutions over the next 10-20 years. A cryptanalytically relevant quantum computer (CRQC) is a quantum computer that is theoretically capable of attacking real-world cryptographic systems.. A CRQC could possess the ability to decrypt public key (also known as asymmetric key) encryption systems. This is a significant concern among security analysts today, as almost all of today's information systems rely on the asymmetric key method to secure sensitive data. Namely, quantum-performed algorithms, such as Grover's search and Shor's algorithms, pose a significant threat to the RSA algorithm.

The concern that hackers could "catch now and crack later," (i.e. steal and store data now, and decrypt it later with a quantum computer) is real. Think about presumed encrypted messages or files from 20 years ago that would still be relevant today. Even if CRQCs are not available for 20 years, quantum resistant cryptography needs to be deployed now.

NIST has formally released standards to cover all major cryptography needs. It is widely believed that the EU, and most of the rest of the world, will adopt the CNSA algorithm suite.

## Governments Set Timelines for Quantum Resistant Algorithms

So where does this new cryptography stand today? The timeline for CNSA and ENISA (European Union Agency for Cybersecurity) compliance requirements is coming up fast. In 2025, shipments of IT equipment into the U.S. government are recommended to include CNSA 1.0 or 2.0 components. In 2030, shipments are required to include CNSA 2.0 components. In 2026, ENISA expects Quantum Resistant algorithms to be adopted.

NIS 2 (Network and Information Systems Directive) in the EU also has important upcoming deadlines. By October 2024, enterprises need to adopt and publish measures intended to improve the security of network and information systems across the EU. The EU's Digital Operations Resilience Act (DORA) will by 2025 require compliance with legislation to improve the IT security of financial institutions and their third-party service providers. The urgency continues to build as governments around the world enact new security compliance regulations and enterprises must be ready.

## Encryption of Data In-flight on Fibre Channel Networks

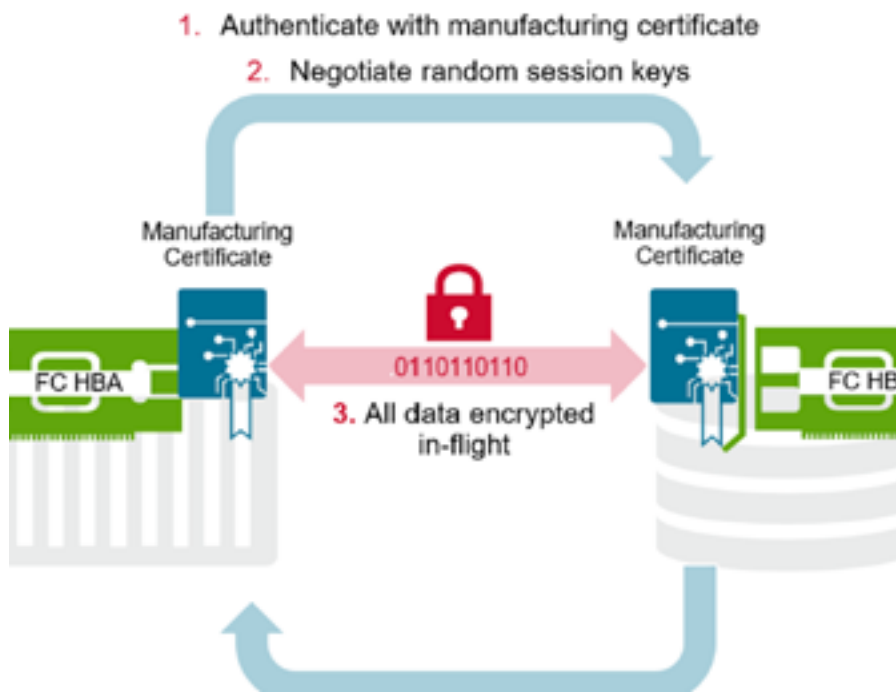
The focus of concern that drives all of these government-led initiatives is to protect critical infrastructure, the value of which was revealed in the pandemic. As the preferred storage solution for mission-critical data center solutions, Fibre Channel must take the lead in post-quantum and zero trust solutions.

The new Fibre Channel SP3 (FC-SP-3) standards support authenticated encryption of data in flight (EDIF) using quantum resistant algorithms. The new algorithms are incorporated into FC HBAs starting in 2025 for both servers and storage. This allows fibre channel SANs to both meet zero trust requirements as well as CNSA timelines for quantum resistance.

Once ratified, FC-SP-3 will enable governments and enterprises to comply with CNSA 2.0 mandates ahead of the required 2025 and 2030 deadlines.

The goal of FC-SP-3 was to deliver an open, easy to implement solution that made it easy for enterprises to comply with CNSA mandates. Research shows that in 2023 organizations with high levels of security system complexity reported a US\$1.4M increase in data breach cost over organizations with low system complexity.<sup>1</sup> The FC-SP-3 solution solves the encryption complexity problem. The solution involves

manufacturing certificates stored on Fibre Channel Host Bus Adapters (HBAs) authenticating as valid and, once identities are established, negotiating random session keys. All data is then encrypted in flight between the servers and storage arrays. A huge benefit of this approach is that it uses session-based keys and does not require a complex external key management application, making it very easy to deploy and manage.



**Figure 1: Fibre Channel EDIF - Session-based Encryption**

The solution is also cost-effective. It can run on an existing Fibre Channel network without new hardware (apart from deploying HBAs that support FC-SP-3).

Unlike application-based encryption, where individual applications implement their own encryption schemes, Fibre Channel encryption encrypts all data in flight, providing complete coverage for all apps at a lower cost. It also has no impact on storage array features such as compression and deduplication.

Compared to general purpose Ethernet (IPSEC) adapters, modern Fibre Channel HBAs have dedicated hardware offload for crypto functions to avoid degrading performance and provide simple management.

The FC-SP-3 standard is expected to be completed in 2025 with both server and storage solutions available in the marketplace that same year.

## Completing Fibre Channel Zero Trust Solutions

Zero trust architecture requires continual authorization, requiring establishment of trust at every possible digital interaction. This approach acknowledges that threats can come from inside and outside the network. Fibre Channel vendors have implemented, or will be implementing, zero trust components which may include:

Silicon Root of Trust- uses unalterable hardware- based on signature validation to ensure authentic ASIC and firmware.

Digitally Signed Drivers- verified by the operating system to be authentic code written by the manufacturer before they can be installed.

SPDM (Security Protocol and Data Model) - cryptographically authenticates Fibre Channel HBAs with host CPUs.

## Conclusion

Cybersecurity is a focal point of enterprises and governments globally, as the frequency and cost of data breaches continue to rise and the quantum computing era grows nearer. To address these concerns, governments have responded with regulations such as CNSA 2.0, NIS and DORA, mandating enterprises to modernize their IT infrastructures.

New Fibre Channel standards deliver a cost-effective, easy-to-manage solution to meet compliance requirements with support for Zero Trust and EDIF to protect data as it moves across databases, applications, servers, and storage. Fibre Channel HBAs supporting FC-SP-3 utilize quantum-resistant algorithms, ensuring post-quantum readiness. The session-based key management solution does not require complex and costly key management software. Compared to other encryption methods such as application-based encryption and Ethernet IPSEC, Fibre Channel HBAs can encrypt all applications, at a lower cost, and with no impact on storage array services such as dedupe or compression. Considering this will be done with no performance impact, FC-SP-3 based fibre channel solutions will play a pivotal role in protecting critical infrastructures.

---

1. Ponemon Institute, Cost of Data Breach Report, 2023, IBM Security

# Introducing 128G Fibre Channel for Storage Networking

By Chris Lyon, Amphenol CS Standards & Technology Group and FCIA Chairman.

The technology landscape is continuously evolving with ever-growing demands for faster data access, storage, and transmission. One of the latest advancements in this domain is the introduction of the 128GFC (128 Gigabit Fibre Channel), often called Gen 8. Fibre Channel has long been the go-to protocol for mission-critical, high-performance storage networks, primarily in data centers. This new iteration promises to significantly boost data throughput, reduce latency, and provide greater scalability.

## INCITS FC-PI-8: The 128G Fibre Channel Standard: An Overview

FC-PI-8, which stands for Fibre Channel Physical Interface 8, is the latest iteration in the Fibre Channel physical interface standards. It doubles the data rate of the previous 64GFC standard to 128 gigabits per second. This enhancement is crucial as data demands continue to escalate across industries, driven by trends like big data analytics, data warehousing, and virtualization.

FC-PI-8 introduces several key features, including:

- **Increased Data Rate:** The 128GFC standard significantly boosts throughput, allowing for faster data transfers and improved performance in storage networks.
- **Backward Compatibility:** FC-PI-8 128GFC ensures compatibility of up to two generations of previous Fibre Channel speeds and is cable- and connector-compatible, allowing organizations to transition smoothly without requiring a complete overhaul of existing infrastructure. 128GFC uses LC cable connectors and the SFP+ form factor and is capable of 100 meter cable lengths using OM4/5 cable plants.
- **Modulation for 128GFC:** 128GFC uses PAM4 modulation and is 112.2Gbps (56.1Gb)
- **Enhanced bit error rate:** (BER) of 1e-15
- **Forward Error Correction:** Mandatory for all 128GFC links

The development of FC-PI-8 kicked off in December 2022 and took place within the INCITS Fibre Channel technical committee, which is responsible for creating and maintaining Fibre Channel standards. The FC-PI-8 committee comprises industry experts from various sectors, including hardware manufacturers, software developers, and end users. This collaborative environment ensures that the standards developed are practical and address real-world needs. The standards development process encompassed:

- **Research and Requirements Gathering:** The process began with a thorough analysis of the industry needs. This work included assessing performance bottlenecks in existing Fibre Channel systems and forecasting future demands.
- **Drafting and Proposals:** After establishing requirements, the committee drafted initial proposals for FC-PI-8, outlining the technical specifications and objectives.
- **Testing and Validation:** Prototypes and implementations of the standard were rigorously tested to validate performance metrics, signal integrity, and compatibility with existing systems. Feedback from these tests was crucial in refining the standard.
- **Finalization and Approval:** After multiple rounds of review and revisions, the final standard was approved by INCITS. This included contributions from a diverse range of stakeholders, ensuring that FC-PI-8 meets the needs of a broad audience.

## Benefits of 128GFC for Customers

### Improved Data Throughput

One of the most significant advantages of 128GFC is the substantial increase in data throughput. Using 128GFC, customers can transfer much larger amounts of data in less time than with earlier Fibre Channel iterations. This improvement translates to faster backups, quicker data recovery, and a smoother flow of information between systems. Enterprises managing vast volumes of structured data, such as data warehousing, decision support systems, and financial services, will benefit immensely from the increased throughput.

### Higher Scalability for Growing Data Needs

As data storage requirements grow exponentially, so does the need for infrastructure capable of scaling without compromising performance. The 128GFC standard allows organizations to scale up their SANs more easily, ensuring they can meet future data demands without overhauling their existing infrastructure. The new technology is backward-compatible with previous generations of Fibre Channel, making it easier for companies to upgrade at their own pace without immediate disruption.





### **Enhanced Reliability and Security**

Fibre Channel technology is known for its reliability, and 128GFC continues this tradition. SANs powered by 128GFC are designed for maximum uptime and offer robust error-correction mechanisms, ensuring data integrity even during high-speed transmissions. This is critical for industries with zero tolerance for data loss or corruption, such as banking, government, and healthcare sectors. Moreover, Fibre Channel networks are inherently secure, operating in isolated storage networks that reduce the risks associated with open, internet-based protocols like Ethernet.

### **Cost-Effectiveness Through Improved Efficiency**

While adopting newer standards often comes with a significant upfront investment, the long-term savings from the efficiency gains offered by 128GFC can be considerable. The increased speed and reliability reduce the need for duplicate infrastructure and allow companies to get more value from their existing systems. As data centers move toward energy efficiency, the streamlined processes that 128GFC enables can also reduce power consumption and cooling costs, further boosting cost-effectiveness.

### **Conclusion**

The FC-P1-8 standard development for 128GFC was completed by the end of 2023 and signals the start of product development by Fibre Channel component suppliers. We expect to see 128GFC products in the marketplace by the end of 2025. The 128GFC standard marks a significant advancement in Fibre Channel technology, offering a suite of benefits tailored to the needs of modern enterprises. By improving throughput, reducing latency, enhancing reliability, and supporting future growth, 128GFC promises to transform the performance of mission-critical applications. For businesses that depend on fast, secure, and scalable data transmission, upgrading to 128GFC is not just an option but a crucial step in staying competitive in an increasingly data-driven world.

Fibre Channel Industry  
Association (FCIA) Members

Adtran Amphenol®



Hewlett Packard  
Enterprise



**SANBlaze**  
Technology, Inc.



