Interested in learning
more about security?

SANS Institute
InfoSec Reading Room

This paper is from the SANS Institute Reading Room site. Reposting is not permitted without express written permission.

Is Your Storage Area Network Secure? An Overview of Storage Area Network from Security Perspective

Overview of Storage Area Network (SAN) architecture and the potential security threats and solutions available in SAN environments.

Copyright SANS Institute
Author Retains Full Rights

AD

Is Your Storage Area Network Secure? An overview of Storage Area Network from security perspective.

Mohammed Haron

GSEC Practical Version 1.4 Option 1

Abstract

In this paper, I will discuss about Storage Area Network (SAN) architecture in general, such as topology, SAN components, and terminologies to give you an idea about SAN. Then I will go over the potential security threats and solutions available in SAN environments such as in SAN network, implementation, and management. I will also cover some of the attacks that will impact your SAN, and actions necessary for protecting it. Finally, future SAN protocols and technologies such as iSCSI, InfiniBand, FCIP and iFCP will be discussed. SAN is indeed a very exciting technology, looking forward to years to come. Read on.

Introduction to Storage Area Network

Due to the explosion of internet and the e-commerce, a tremendous amount of data has been created and made available to users. In addition to this, new type of data such as images, audio and video have been stored and integrated with applications and databases, further accelerating the demand for storage capacity.[1]

From this demand, it is estimated that the global storage market is worth $44 billion a year. According to International Data Corporation (IDC), an independent research firm that "network storage is one of the fastest growing segments of this market. IDC estimates that 1.3 million terabytes of storage will be sold by the end of 2002." Another independent research company, Gartner Dataquest, predicts that "the cost per megabyte of storage, which was 15 cents in 2000, could fall to as little as 3 cents per megabyte by 2003." [2]

Besides the need of additional storage at amazing rates, a research done by IDC reported that the requirement for stored data is growing 80% annually, while the number of IT personnel responsible for administering storage and systems is growing at only 5% per year. So, how are IT managers going to manage this explosion of data without a huge increase in overhead cost?[3]

The world is saved by existence of the Network Storage technologies, which is also the fastest growing the market. There are two different Network Storage technologies currently available in market. Network Area Storage (NAS) is available for low end market while Storage Area Network (SAN) is targeted for high end market.[4]

Both NAS and SAN really help IT departments in consolidating server storage into one central storage arrays, thus simplify the storage management task into one administration console. Even though both NAS and SAN look similar, there are main differences

© SANS Institute 2002, As part of the Information Security Reading Room. Author retains full rights.

between them that set them apart. NAS system connects to your LAN and provide file-level access for client-systems, while SAN system provides block-level access to data residing on shared storage arrays thru dedicated 1Gbps or 1Gbps storage networks that connect disk arrays, servers, tape libraries, and other peripherals to a switching fabric or hub. [5]

Why SAN? Of course, there must be a lot of benefit of block-level access to data provided by SAN. This highly scalable nature of a SAN has been a very hot topic in the industry with network of servers and storage devices interconnected with high speed Fibre Channel (FC) hubs and switches. Data management has been a big challenge for many companies especially with the e-commerce explosion. As disk space requirements increase and the server farms grow, the overhead associated with directly attached storage progressively become more out of control. SAN allow you to manage virtually all your storage needs proactively while at the same time creating the high availability required by the servers. [6]

Moving storage traffic from Local Area Network (LAN) into a dedicated high-speed network can reduce backup windows and significantly improve application performance by reducing bandwidth on production LAN. SAN management software can then be easily used to relocate storage space among servers without interrupting access to data.[7] For example, partition size can be change on the fly according to the need without requiring deletion and recreation of the partition. This is the real advantage of SAN in an ever demanding storage capacity.

As the key findings from a study done by KPMG Consulting and Brocade Corporation Inc. on two companies, Intuit, Inc. and Federal Express Corporation revealed SAN benefits to organizations as follow:

- SAN provide substantial business, financial, and operational benefits
- The major benefits of a SAN include:
    1. Reduced capital expenditures
    2. Increased IT staff efficiency
    3. Higher system and application availability
    4. Highly scalable, flexible storage architecture
    5. Enhanced ability to efficiently exploit the full value of a company's information assets
- The financial return from implementing a SAN is significant
- Companies can use SAN to improve their competitive position. [8]

Overview of SAN architectures

So, what is SAN? SAN is an independent network of storage systems that removes today's server-based storage installation into a scalable, high speed and direct access to the storage, without server ownership of storage subsystems. [9]

Before we can discuss about SAN security issues, let us take a look briefly at SAN architectures.

© SANS Institute 2002, As part of the Information Security Reading Room. Author retains full rights.

- Topology – Earlier version of SAN was designed using Arbitrated-Loop which is similar to Token Ring topology. However, due to its limitation, switch fabric, which is available at higher speed, was later introduced. Currently, most SAN implementations are using switch fabric and will be discussed here.
- SAN Components – SAN components consist of:
    1. Fibre Channel Switches (Also called SAN Fabric)
    2. SAN Fabric Management and Monitoring Software
    3. SAN Fabric Security and Access Control Software
    4. Storage Devices
    5. Hosts and Host Bus Adapters (HBA)
    6. Cabling and Cable Connectors:
    7. Gigabit Interface Converters (GBICs) that convert optical to electrical signals. [10]

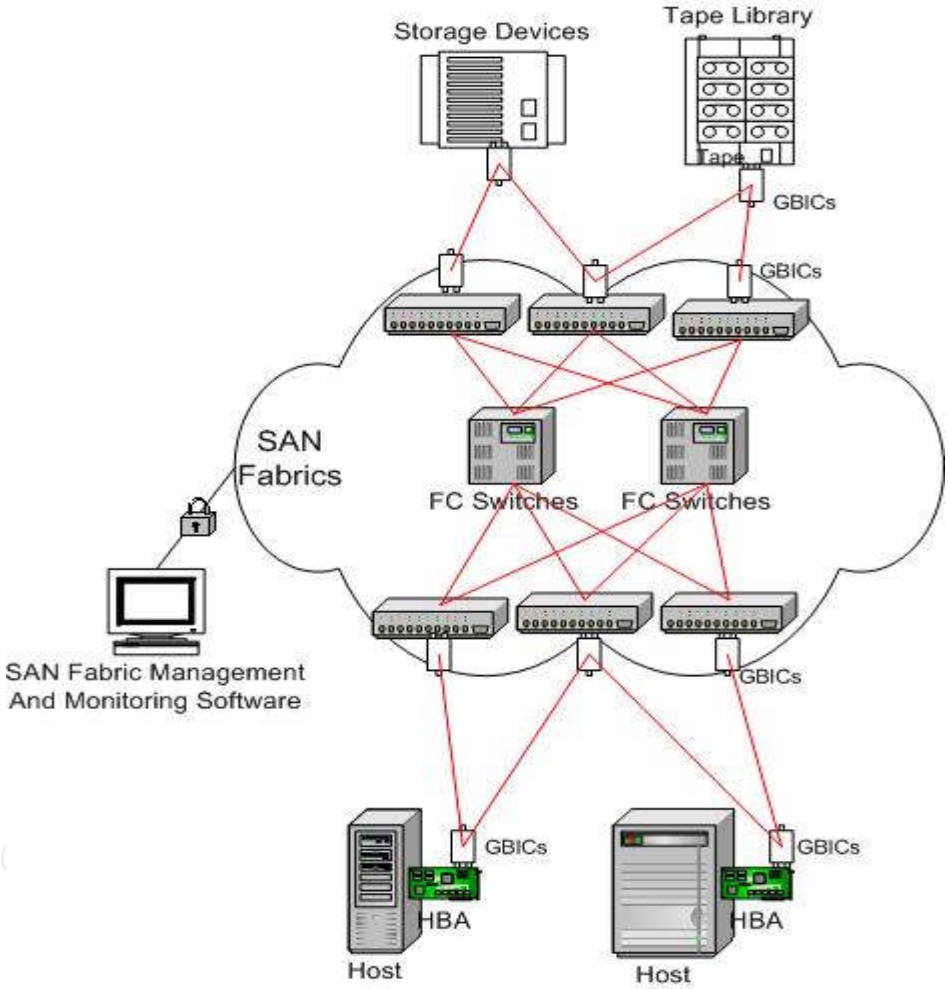

Figure 1: Basic SAN Components.[11]

- Fibre Channel Switches (SAN Fabric): Since these switches form the intelligent foundation of your SAN, it is really important to choose the right components that

© SANS Institute 2002, As part of the Information Security Reading Room. Author retains full rights.

satisfy business needs and security requirements. Careful considerations must be given to these items:

- Hardware redundancy: Partial redundancy or complete redundancy for optimal uptime.
- Port Count: Depending on the needs, a range of choices can be selected from entry-level (8-16 ports), up to enterprise level (64-128 ports).
- Management and Monitoring Software: Switch should offer easy to use tools such as Web-based management and monitoring tools in a secure manner.
- Security and Access Control Software: Switch should offer software that protects SAN from security breaches and secure storage resources across SAN.
- Integration with Third-Party Applications: Application Programming Interface (API) should be offered to integrate SAN tool sets with any third party vendors.
- Speed: Currently available switches support both 1Gbits and 2 Gbits throughput per port.
- Budget: Buy the best features affordable with budget available to ensure you can easily adding more components to the SAN as the need grows.
- Standards Involvement: Be sure switches adhere to industry standards
- Forward and Backward Compatibility: Switches should be forward and backward compatible with other switches in the product line so you can migrate from 1 Gbits to 2 Gbits SAN environments when needed. [12]

SAN Security

Since SAN is usually used in highly critical systems in which requires high availability, confidentiality and integrity, organizations must be aware of all potential points where a security breach might occur and to include these into consideration when designing SAN security solutions. Ability to identify the points of vulnerability and implement a reliable security solution is the key to securing a SAN fabric infrastructure.Ref#12). Clearly, physical isolation of the SAN is not a sufficient security measure when multiple departments share SAN resources. [13]

To help identify and address any security exposures, a comprehensive SAN security framework must provide the kind of security tools and controls commonly used in most other types of data network. A SAN framework should be developed around open industry standard and be highly scaleable, fully manageable, and extremely resilient, but at the same time must have the ability to manage Fibre Channel fabric devices in both new and existing standalone SAN islands and heterogeneous SAN fabrics in order for it to be truly secure and cost-effective.

© SANS Institute 2002, As part of the Information Security Reading Room. Author retains full rights.

Let's look at SAN security issues below:

- Network
- Implementation
- Management
- Possible Attacks
- Future Technologies and Challenges

Network Issues

One important issue in managing SAN is that, you need to make sure that users are only accessing and aware of those files they are given access to, and not others that are also available on the same storage devices. One common way is usually done by masking off the Logical Units (LUNs) that are not legitimately available to users. This so called "LUN security Problem" of masking and maintaining the masks can be handled in many ways.
One approach is to mask at the Host Bus Adapter (HBA) level by using HBA drivers that contain a masking utility that use the World-Wide Name (WWN) already supplied with each HBA. This masking utility can be run from a console which allows editing the WWNs visible to a host down to the set authorized for that host. However, this method requires coordination for a large SAN island with large number of hosts and a large number of LUNs on the storage devices.

A very sophisticated approach is to zone servers and LUNs through Fibre Channel switch, which allows only certain server access certain storage elements. This method is expandable and can control a large number of servers, besides providing port-level masking for all the nodes known to the switch. [14]

This protection on the SAN network can be achieved thru:

- Fabric Configuration Servers: one or more switches can acts as trusted devices in charge of zoning changes and other security-related functions.
- Switch Connection Control: ACLs and digital certificates within the switch authenticate new switches and ensure that they can join the fabric. This method is accomplished using Public Key Infrastructure (PKI) technology to provide the most comprehensive security solution for SAN environments. Table 1 below compares PKI technologies to other types of security solutions.

	Authentication	Confidentiality	Integrity	Non-repudiation
Firewalls	X	X		

© SANS Institute 2002, As part of the Information Security Reading Room. Author retains full rights.

Access Control	X	X		
Encryption		X	X	
Public Key Infrastructure	X	X	X	X

Table 1. [15]

- Device Connection Controls: port level ACLs lock particular WWNs to specific ports.

Implementation

More and more organizations are requiring the highest level of system uptime and data availability, especially due to the emergence of the Internet and e-commerce. In such an extremely competitive market with increased customer and internal user expectations, organizations are currently striving to achieve at least 99.999 percent availability in their computing systems, which is equivalent to less than 5.3 minutes of downtime a year. Further downtime can severely impact business operations and most importantly, company image. These organizations usually represent industries that demand the highest level of systems and data availability such as financial institutions, brokerage, communications, utilities and many more. [16]

In order for them to achieve such a very high availability in their SAN implementation design, SAN vendor such as Brocade has come up with a high performance, dual-fabric SAN solution to address this need. These highly flexible SAN are based on the following principles:

- A thorough understanding of availability requirements throughout the enterprise
- A flexible design that incorporates fault tolerance through redundancy and mirroring.
- Simplified fault monitoring, diagnostics, and repair capabilities to ensure fast recovery
- A minimal amount of human intervention required during failover events
- A reliable backup and recovery plan to account for a wide variety of contingencies. [17]

To ensure systems can withstand varieties of failures, dual-fabric SAN capabilities will include:

- Highly available components with built-in redundancy and hot-plugging capabilities
- No single points of failure
- Intelligent routing and rerouting
- Dynamic failover protection
- Non-disruptive server and storage maintenance
- Hardware zoning for creating safe and secure environments
- Predictive fabric management. [18]

© SANS Institute 2002, As part of the Information Security Reading Room. Author retains full rights.

One way of achieving systems high availability is by implementing fully redundant SAN environment to ensure the highest possible systems availability.

SAN Management

Integrity of SAN can be compromised, whether intentionally or accidentally if unintended and unauthorized individuals have access to certain elements of SAN management. Some of the inappropriate accesses to SAN configurations are:

- Exposed network administration passwords allowing unauthorized individuals to access SAN in the role of administrator.
- Changes to zoning information allowing access to storage and read/write to data
- Changes to security and access control policies allowing unauthorized servers or switches to gain access to SAN. [19]

These elements of management communications such as passwords must be secured on some interfaces between the security management function and a switch fabric. Because security management impacts the security policy and configuration of the entire SAN fabric, administrator access controls can be used to work in conjunction with security management functions. In addition, administrator-level fabric password access provides primary control over security configurations. [20]

Possible Attacks

Since there are a lot of discussions already available on Operating Systems (OS), and applications' vulnerabilities already been discussed, let me cover several SAN specific attacks that might occur. These attacks could be:

- Man-in-the-middle type of attacks
- SNMP vulnerabilities

Man-in-the-middle Type Attacks

Man-in-the-middle attack is defined by Paul McFedries on his website The Word Spy as "A computer security breach in which a malicious user intercepts- and possibly alters – data traveling along a network." [21] Due to the fact that insiders pose the greatest threat to data security, [22] this type of inside attack is far more dangerous than outside attacks and should not be overlooked by any organizations.

Incidents reported by Cryptec Secure Communications on Enterprise Security showed that:

- "85% of computer crimes originate inside the network" (Intranet Security)
- According to a 2001 Information Security Magazine Survey, insider breaches of security are rampant and dangerous. Of those surveyed:
    - 58% experienced abuse of computer access controls

© SANS Institute 2002, As part of the Information Security Reading Room. Author retains full rights.

- 24% experienced intentional disclosure of proprietary data
- According to the FBI, the average cost of an insider breach is $2.4 million while the average cost of a break-in from the Internet is $27,000." [23]

There are several possible man-in-the-middle types of attacks to SAN such as:

1. World Wide Name (WWN) attack on the HBA
2. Management Admin attack – admin password unencrypted via telnet. Solution to use isolated subnet for management or do local management only

The World Wide Name (WWN) attack happens when a machine with different HBA and WWN id assigned is accessing unauthorized storage resources through the SAN fabric. Whether it happens intentionally or accidentally, it can compromise the confidentiality, availability and integrity of the data. This attack can possibly be achieved by using a compromised dual-home host with a Host Bus Adapter (HBA) to read, store, or distribute SAN files.[24] As a solution, Device Connection Controls can be used to bind a particular WWN to a specific switch port or set of ports and preventing ports in another physical location from assuming the identity of an actual WWN. [25]

SAN Management attack can occur when unauthorized individuals in the network is able to obtain elements of management communications such as Administrator password using some type of sniffer software such as dsniff, that can be used to grab passwords in the network.

Several steps can be taken as protection against this type of attack, such as using SAN management software that encrypts password from some interfaces like Management Console, to a switch fabric. Management Console can also be placed in an isolated, dedicated network to protect it from 'Man-in-the-middle' type attack.

SNMP vulnerabilities

Even though Simple Network Management Protocol (SNMP) has been considered by security experts as insecure for a long time, the CERT Coordination Center (CERT/CC), a computer security consortium, announcement that the Oulu University Secure Programming Group in Finland had discovered that SNMP is riddled with security holes that are more damaging than were first perceived. SNMP is a standard protocol that let network devices communicate information about their operational state to a central system, and has been used since this protocol appeared in 1989. This become a serious security issue because SAN vendors and storage-management software vendors has been supporting this protocol in their products all along. [26]

Oulu University researchers found SNMP to be vulnerable to Denial of Service (DoS) attacks, service interruptions in which an attacker can gain access to an affected device. This can seriously compromise the integrity, availability and confidentiality of SAN fabric and the data being stored. Fortunately, while some SAN software vendors use

© SANS Institute 2002, As part of the Information Security Reading Room. Author retains full rights.

SNMP for some basic storage-management operations, they more often implement higher-level functions using proprietary technology.

Several strategies have been proposed by CERT/CC to counter the vulnerabilities in SNMP, but none is ideal. First is to determine whether the specific device vendor has developed a patch or workaround. CERT/CC has provided a list of vendors' responses to the SNMP alert on CERT Web site at http://www.cert.org/advisories/ca-2002-03.html.

Another recommendation is to disable or disconnect SNMP devices that are not essential to the operation of the SAN. If this is not viable, then ingress filtering can be used to block SNMP traffic from entering into network, because external hosts seldom need to initiate inbound traffic to machines that provide no external services. Other ideas include configuring SNMP agents to refuse messages from unauthorized systems, or segregating SNMP traffic onto a separate management network. CERT/CC has advised all companies to take action immediately because the SNMP vulnerabilities are real and dangerous to their network. [27]

Future Technologies and Challenges

There are several technologies that will extend SAN capabilities into more flexible data storage solutions, data storage security, business continuity and disaster recovery functions, thus a more challenging security environment into SAN.

Some of those emerging technologies are:

- Internet Small Computer Systems Interface (iSCSI)
- Infiniband
- Fibre Channel over Internet Protocol (FCIP)
- Internet Fibre Channel Protocol (iFCP)

Let us take a look at these technologies.

iSCSI

iSCSI technology allows SAN to utilize Ethernet as a storage network technology besides the Fibre Channel (FC) currently in use. This is a very promising technology with the availability of 1 Gigabit Ethernet and the expectation of even reaching 10 Gigabit speeds, while at the same time, removing requirements of setting up and managing two different technologies, i.e. data and storage.

iSCSI extended SAN capabilities by enabling access to storage devices and SAN over dedicated or even shared standard Ethernet-based TCP/IP network. Fibre Channel (FC) is no longer required. In addition, IP storage network can be extended to Wide Area Network (WAN) by using standard IP routers and switches which is beneficial for applications such as synchronous and asynchronous remote disk copy, or tape backup and restore. In addition, iSCSI benefits from Transport Connection Protocol (TCP) protocol

© SANS Institute 2002, As part of the Information Security Reading Room. Author retains full rights.

in the WAN which will ensure data reliability manage network congestion and adapt retransmission over WAN delays.

Just like the standard SCSI protocol, iSCSI works as a transport system between an initiator and a target using drivers installed in servers to initiate iSCSI packets. Next, this packet of block-oriented SCSI data is encapsulated into an iSCSI wrapper and then routed across IP network towards a target which is an iSCSI device that reversed the process back to SCSI data.

Some examples of iSCSI real benefits in an enterprise environment are:

- **Remote Backup:** Storage can be backed up from any location as long as there is an IP connection. It is claimed that standard IP network security technologies such as firewalls, encryption and authentication tools can be used to secure storage from unauthorized access. However, backing up large storage across WAN is still too slow to be practical.
- **Remote Data Access:** Enterprise users can access remote storage resemble local storage attached to their machines; while improving security, allow no users to access business-critical data from anywhere globally.
- **Enterprise Storage Consolidation:** Multiple servers and different network operating systems can be consolidated into a pool storage efficiently for cost-saving by reducing equipments and staffs. [28] iSCSI can save companies from typically expensive investment for Fibre Channel backend. [29]

However, there are still some security concerns on key issues such as encryption and domain name addressing for iSCSI. "iSCSI can only be realized probably when we have a 10 Gigabit Ethernet working" said Gene Chesser, HP technical director for storage solutions. He also discourages the immediate use of the technology. In addition, Charlie Trentacosti, vice-president for HP Network Storage Solutions in Asia Pacific said "Storage over IP is not recommended," "Not until we let go of standardization concerns across platforms and architectures through IP, we would not see immediate industry support for the technology." [30]

The good news is that recently, The Storage Network Industry Association IP Storage Forum (SNIA IPS Forum) has announced on September 4, 2002, that Internet Small Computer Systems Interface (iSCSI) standard is now technically complete and accurate and expected that products to roll out by late fall 2002 or early 2003. [31]

Infiniband

What is InfiniBand Architecture? InfiniBand Architecture as defined by InfiniBand Trade Association "is an industry standard, channel-based, switched fabric, interconnected architecture for servers. Infiniband architecture changes the way servers are built, deployed, and managed." [32] In short, it is basically a high-speed I/O switching fabric. [33] It is used to interconnect processing nodes to I/O nodes to form a System Area Network. [34]

© SANS Institute 2002, As part of the Information Security Reading Room. Author retains full rights.

InfiniBand is intended as replacement for PCI and not intended as replacement for Ethernet nor Fibre Channel. As such, InfiniBand is designed to be used within a computer room facility with less than 100 meters diameter. It is not a new technology, but rather InfiniBand is built on Best-of-Breed technologies.

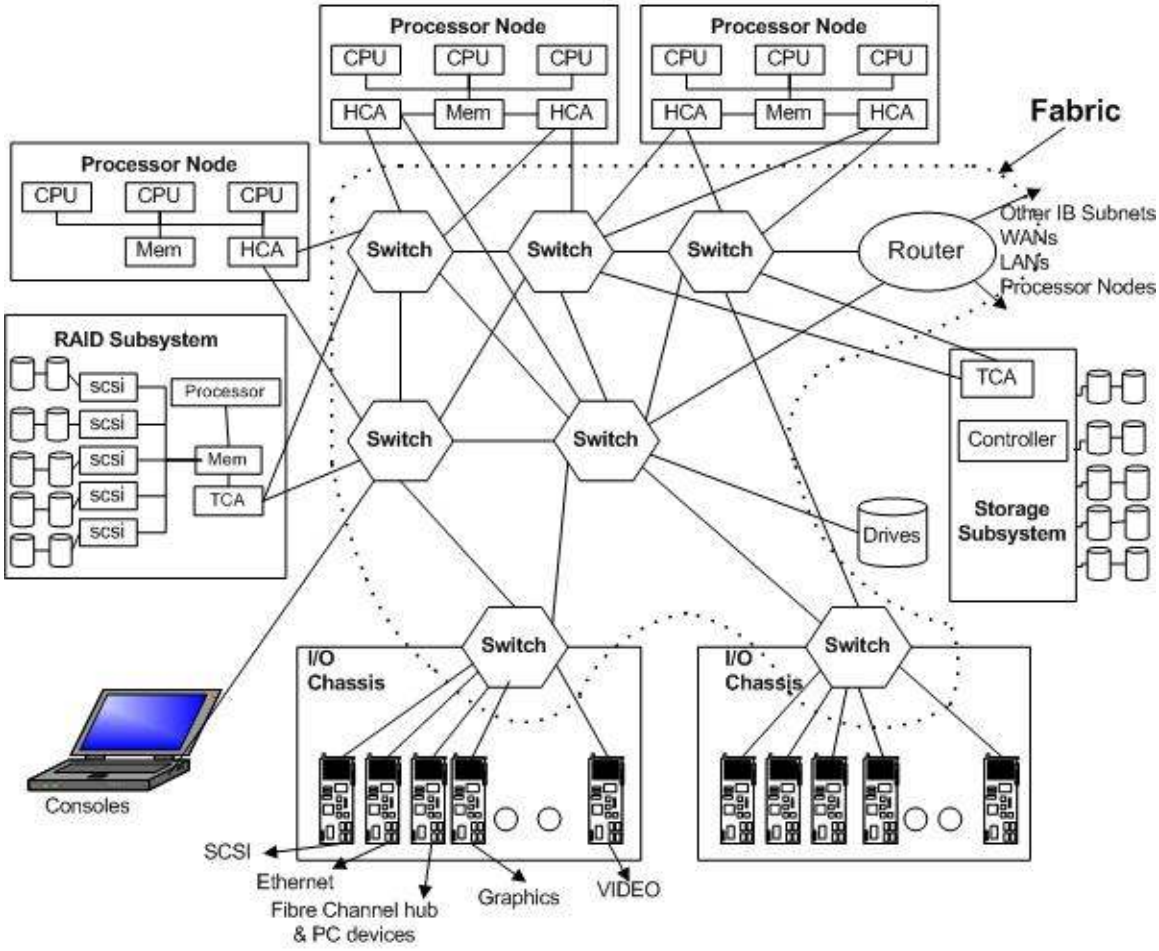

Figure 2: Typical InfiniBand Topologies. [35]

InfiniBand specification offers three levels of performance – 2.5Gbits, 10Gbits and 30Gbits. Higher throughput compared to standard protocols can be achieved by low latency communication enabled within the fabric. For this unique feature, InfiniBand can be the I/O interconnects of choice for data centers.

FCIP

Fibre Channel over Internet Protocol (FCIP or FC/IP) is defined as a tunneling protocol for connecting geographically distributed Fibre Channel SAN transparently over IP networks. [36] For that reason, it is also known as Fibre Channel tunneling or storage tunneling. [37] It combines the benefits of mature Fibre Channel technology optimized for high speed storage-data movement within SAN and data center, with a mature Internet

© SANS Institute 2002, As part of the Information Security Reading Room. Author retains full rights.

Protocol technology optimized for data movements across WAN distance. FCIP may be one of the solutions for companies need to extend their Fibre Channel storage farther than 10 kilometers that currently supported by FC protocol.[38]

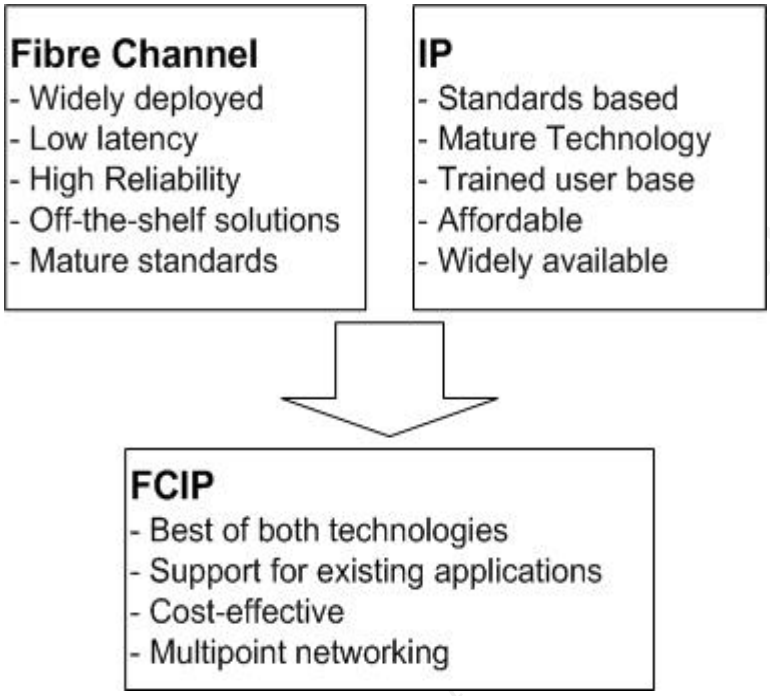

Figure 3: FCIP combines the best benefits of both IP and Fibre Channel technologies.[39]

© SANS Institute 2002, As part of the Information Security Reading Room. Author retains full rights.

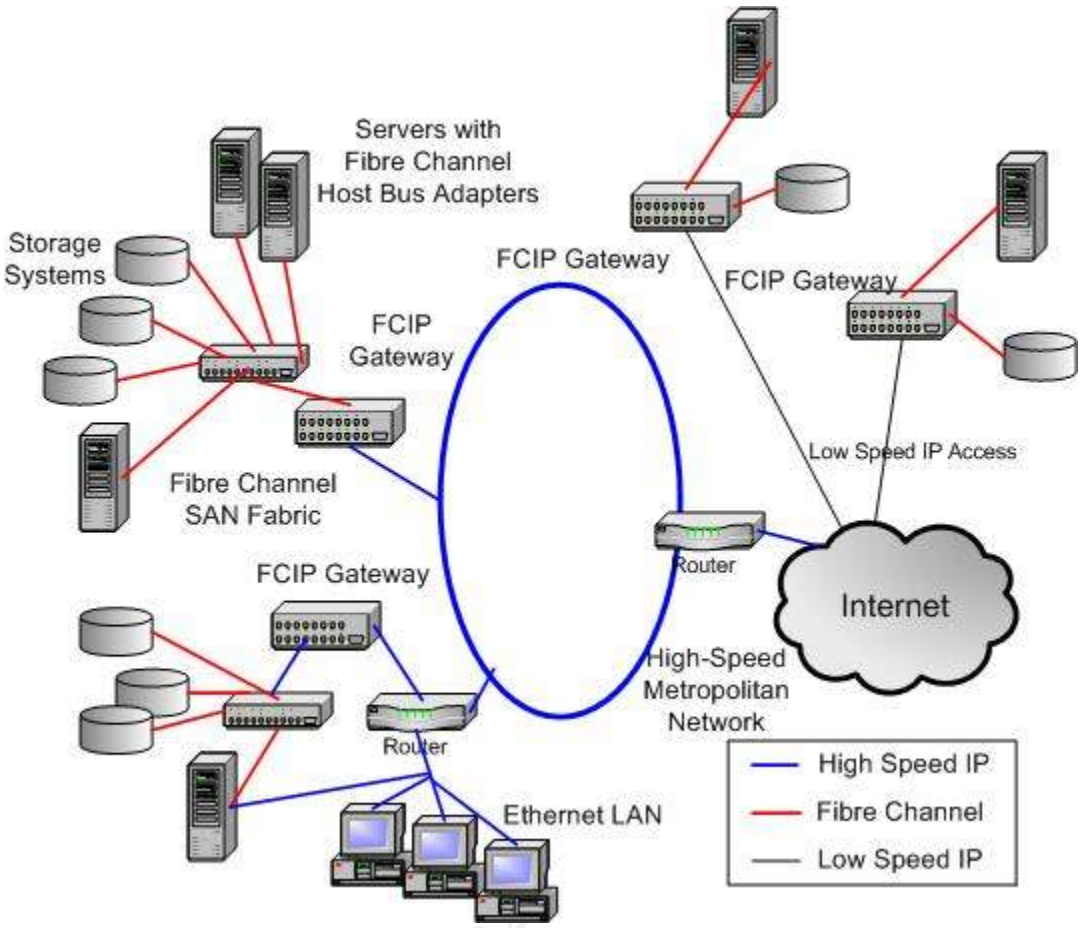

Figure 4: A typical FCIP network configuration.[40]

While the storage industry is inclined towards the Internet, FCIP is only equipped to work within the Fibre Channel environment. This is the downside of FCIP since FCIP is a tunneling protocol that encapsulates Fibre Channel data and forwards it over a TCP/IP network as an extension of the existing Fibre Channel network.[41]

iFCP

iFCP (Internet Fibre Channel Protocol) is an emerging standard for extending Fibre Channel storage across networks across the Internet. iFCP provides a means of passing data to and from Fibre Channel storage devices in a local Storage Area Network (SAN) or on the Internet using TCP/IP. iFCP can either replace or be used in conjunction with existing Fibre Channel protocols, such as FCIP (Fibre Channel over IP). iFCP is another protocol besides FCIP that can extend Fibre Channel storage farther than 10 kilometers that currently supported by FC protocol.[42]

One advantage of iFCP over FCIP is that because iFCP gateways can either replace or complement existing Fibre Channel fabrics, iFCP can be used to facilitate migration from a Fibre Channel SAN to an IP SAN or a hybrid network.[43]

© SANS Institute 2002, As part of the Information Security Reading Room. Author retains full rights.

Conclusion

One of the key issues with this IP storage is that the TCP/IP stack that ensures delivery of packets uses up a lot of CPU resources, and that slows down server performance. Added with the large data volumes across the Gigabits network can really used up most of the CPU capacity. One solution to this is by moving the packet-delivery notification loads to the Host Bus Adapters (HBA). These HBAs will accept SCSI information from servers, convert it to iSCSI, off-load the TCP/IP stack and carry blocks of data over Ethernet to their storage destination.

However, many companies are still reluctant to use these new technologies for real sensitive data due to security concern. Helen Chen, a member of the technical staff at Sandia National Laboratories said "TCP/IP is prone to security attacks." "While we're opening our data up to Ethernet, it's very important we make sure it's protected from Internet attacks."[44]

References:

1. Brocade, "The Essential Elements of a Storage Networking Architecture" p.1.
2. Leslie, p.1.
3. Coffed, p.1.
4. Leslie, p.1.
5. Weitz, p.1.
6. Fetters, p.1.
7. Leslie, p.1.
8. KPMG Consulting, p.3.
9. Coffed, p.1.
10. SAN Info Center, Brocade "Learn the basics of SAN: Evaluate, Step 2: Basic SAN Components", p.1.
11. SAN Info Center, Brocade "Learn the basics of SAN: Evaluate, Step 2: Basic SAN Components", p.1.
12. KPMG Consulting, p.3.
13. Coffed, p.1.
14. SAN Info Center, Brocade "Plan and Design, Step 3: Determine Your SAN Components", p.1.
15. Clark, p.1.
16. Brocade White Paper Library, Brocade "Improving System Availability with Storage Area Networks", p.3.
17. Brocade White Paper Library, Brocade "Improving System Availability with Storage Area Networks", p.3.
18. Brocade White Paper Library; Brocade "Improving System Availability with Storage Area Networks", p.4.
19. SAN Info Center, Brocade "Manage Step 4: Secure Your SAN", p.4.
20. SAN Info Center; Brocade "Advancing Security in Storage Area Networks", p.1.
21. McFedries, p.1.

© SANS Institute 2002, As part of the Information Security Reading Room. Author retains full rights.

22. Cryptec Secure Communications, p.1.
23. Cryptec Secure Communications, p.1.
24. SAN Info Center; Brocade "Manage Step 4: Secure Your SAN", p.1.
25. SAN Info Center, Brocade "Advancing Security in Storage Area Networks", p.1.
26. King, p.1.
27. King, p.1.
28. Coffed, p.1.
29. Mears, p.1.
30. Plaza, p.1.
31. Storage Networking Industry Association "iSCSI standard ready for primetime", p.1.
32. Specification FAQ, p.1.
33. Mears, p.1.
34. Ruwart, p.1-21
35. Ruwart, p.8. Figure 1
36. A Storage Networking Industry Association (SNIA) White Paper "The Emerging FCIP Standard for SAN Connectivity Across TCP/IP Networks", p.1.
37. "Fibre Channel over IP", p.1.
38. "iFCP", p.1.
39. A Storage Networking Industry Association (SNIA) White Paper "The Emerging FCIP Standard for SAN Connectivity Across TCP/IP Networks", Fig.1.
40. A Storage Networking Industry Association (SNIA) White Paper "The Emerging FCIP Standard for SAN Connectivity Across TCP/IP Networks", Fig.2
41. "iFCP", p.1.
42. "iFCP", p.1.
43. "iFCP", p.1.
44. Garvey, p.1.

Sources:

1) Leslie Wood "Storage Technologies to Watch - An Industry Perspective" May 24, 2002; page 1-3
http://www.enterprisestorageforum.com/technology/features/article/0,,10564_1144871_1,00.html

2) Fetters, Dave "Building a Storage Area Network" May 15 2000; page 1-3
http://www.networkcomputing.com/1109/1109ws1.html

3) SAN Info Center; Brocade Corp. "Manage Step 4: Secure Your SAN".
http://www.brocade.com/san/manage/zoning_security.jsp

4) Clark, Tom "Storage Area Network Security" October 8, 2001
http://www.storageadmin.com/Articles/Index.cfm?ArticleID=22805

© SANS Institute 2002, As part of the Information Security Reading Room. Author retains full rights.

5) Weitz, Mark "Storage Area Networks" June 2002
http://www.storageadmin.com/Articles/Index.cfm?ArticleID=24889

6) King, Elliot "SNMP Vulnerabilities Pose a Threat to Storage Networks" March 25, 2002 http://www.storageadmin.com/Articles/Index.cfm?ArticleID=24568

7) SAN Info Center; Brocade Corp. "Learn the basics of SAN: Evaluate, Step 2: Basic SAN Components"
http://www.brocade.com/san/evaluate/learn_basics.jsp

8) Coffed , Jeffrey D. "Security for the SAN Workgroup" ATTO Technology, Inc. ©2000 page 1-9
http://www.attotech.com/pdfs/SANSecure.pdf

9) Cook, Rich "SAN approaches to LUN security" 01 Apr 2002 page 1
http://searchstorage.techtarget.com/tip/1,289483,sid5_gci812895,00.html

10) Cook, Rich "Design for high reliability" 10 Dec 2001 page 1
http://searchstorage.techtarget.com/tip/1,289483,sid5_gci785127,00.html

11) Brocade White Paper Library; Brocade Corp. "Improving System Availability with Storage Area Networks" pages 1-22
http://www.brocade.com/san/white_papers/pdf/HA_WP_02.pdf

12) SAN Info Center; Brocade Corp. "Advancing Security in Storage Area Networks"
http://www.brocade.com/san/Feature_Stories/advancing_security.jsp

13) Storage Networking Industry Association "iSCSI standard ready for primetime" Mountain View, CA September 4, 2002
http://www.snia.org/news/press_releases/2002/20020904_iscsi_standard.pdf

14) Brocade Communication Systems, Incorporated. "The Essential Elements of a Storage Networking Architecture" White Paper: © 2001
http://www.brocade.com/san/white_papers/pdf/Architecture.pdf

15) KPMG Consulting; © 2001 by Brocade Communications Systems Incorporated. "Case Studies On The Business Impact And Strategic Value Of Storage Area Networks" page 3;
http://www.hp.com/products1/storage/promos/san/san_roi.pdf

16) Cryptec Secure Communications. "An inside out look at enterprise security";
http://www.ciscoworldmagazine.com/webpapers/2001/12_cryptek.shtml

17) McFedries, Paul "man in the middle attack"; The Word Spy; A Web site by Paul McFedries

© SANS Institute 2002, As part of the Information Security Reading Room. Author retains full rights.

http://www.wordspy.com/words/maninthemiddleattack.asp

18) Fine, Bob "iSCSI Enables Ethernet storage nets" Network World Nov 12, 2001. http://www.nwfusion.com/news/tech/2001/1112tech.html

19) Plaza, Gerry "HP OFFICIAL: Storage Management over Internet not yet feasible" INQ7.net Jul 30, 2002 http://www.inq7.net/inf/2002/jul/31/inf_1-1.htm

20) Ruwart, Thomas M. "InfiniBand – The Next Paradigm Shift in Storage" 18th IEEE Symposium on Mass Storage Systems and 9th NASA Goddard Conference on Mass Storage Systems and Technologies; Apr 17th 2001 Ciprico, Inc.; Pages 1-21; http://storageconference.org/2001/Tutorials/IBTA.pdf

21) Specification FAQ; InfiniBand Trade Association http://www.infinibandta.org/specs/faq/

22) A Storage Networking Industry Association (SNIA) White Paper "The Emerging FCIP Standard for SAN Connectivity Across TCP/IP Networks" http://www.storagesearch.com/snia-art-1.html

23) Mears, Jennifer "The ins and outs of interconnects" Network World, Sept. 9 2002 http://www.i-tech.com/Storage%20Info%20Center/indnews64.php

24) "iFCP"; searchStorage.com Definations – powered by whatis.com; http://searchstorage.techtarget.com/sDefinition/0,,sid5_gci834321,00.html (Jul 09 2002)

25) "Fibre Channel over IP"; searchStorage.com Definations – powered by whatis.com http://searchstorage.techtarget.com/sDefinition/0,,sid5_gci750990,00.html (Jun 18 2002

26) Garvey, Martin J. "A Better Way to Store Data?" InformationWeek.com; Apr 29, 2002 http://www.informationweek.com/story/IWK20020425S0005

27) SAN Info Center; Brocade Corp. "Plan and Design, Step 3: Determine Your SAN Components" http://www.brocade.com/san/design/determine_components.jsp

© SANS Institute 2002, As part of the Information Security Reading Room. Author retains full rights.

Last Updated: May 24th, 2013

Upcoming SANS Training

Click Here for a full list of all Upcoming SANS Events by Location

SANS Malaysia @ MCMC 2013	Cyberjaya, MY	Jun 03, 2013 - Jun 08, 2013	Live Event
SANS Pen Test Berlin 2013	Berlin, DE	Jun 03, 2013 - Jun 08, 2013	Live Event
Industial Control Systems Security Training - Houston	Houston, TXUS	Jun 10, 2013 - Jun 15, 2013	Live Event
Security Impact of IPv6 Summit 2013	Washington, DCUS	Jun 14, 2013 - Jun 16, 2013	Live Event
SANSFIRE 2013	Washington, DCUS	Jun 14, 2013 - Jun 22, 2013	Live Event
SANS Canberra 2013	Canberra, AU	Jul 01, 2013 - Jul 13, 2013	Live Event
Digital Forensics & Incident Response Summit 2013	Austin, TXUS	Jul 09, 2013 - Jul 16, 2013	Live Event
SANS London Summer 2013	London, GB	Jul 09, 2013 - Jul 16, 2013	Live Event
SANS Rocky Mountain 2013	Denver, COUS	Jul 14, 2013 - Jul 20, 2013	Live Event
SANS Mumbai 2013	Mumbai, IN	Jul 22, 2013 - Jul 27, 2013	Live Event
SEC528 SANS Training Program for the CompTIA® New Advanced Security Practitioner (CASP) Certification	Washington, DCUS	Jul 22, 2013 - Jul 26, 2013	Live Event
SANS San Francisco 2013	San Francisco, CAUS	Jul 29, 2013 - Aug 03, 2013	Live Event
SANS SEC 560: Network Penetration Testing @ Bangalore 2013	Bangalore, IN	Aug 05, 2013 - Aug 10, 2013	Live Event
SANS Boston 2013	Boston, MAUS	Aug 05, 2013 - Aug 10, 2013	Live Event
Critical Security Controls Summit	Washington, DCUS	Aug 12, 2013 - Aug 18, 2013	Live Event
Industrial Control Systems Security Training - DC	Washington, DCUS	Aug 12, 2013 - Aug 16, 2013	Live Event
SANS Thailand 2013	Bangkok, TH	Aug 19, 2013 - Aug 31, 2013	Live Event
SANS Virginia Beach 2013	Virginia Beach, VAUS	Aug 19, 2013 - Aug 30, 2013	Live Event
Mobile Device Security Summit 2013	OnlineCAUS	May 30, 2013 - Jun 06, 2013	Live Event
SANS OnDemand	Books & MP3s OnlyUS	Anytime	Self Paced