HAGELIN-CRYPTOS
CRYPTO AG

Storage Security Solutions

MARKETING WHITE PAPER

Table of Contents

1 Introduction to the world of storage networks

The task of a storage network is to store and manage large data quantities efficiently. “Efficient” in this case means the network has to transfer data fast and expand storage capacity easily and dynamically to meet growing requirements. It also has to make data available during backup and resume normal operations as quickly as possible following data restoration.

How have storage networks developed over the years to meet these challenges?

Initially, the use of **Direct Attached Storage** (DAS) offered the easiest solution. DAS systems consist simply of storage media (disks, tape) attached to an individual host. Each server receives its own DAS, usually connected via an SCSI or SATA connection to the server. This technology did not make efficient use of storage capacities, however, as it was unable to allocate free storage capacity to another server.

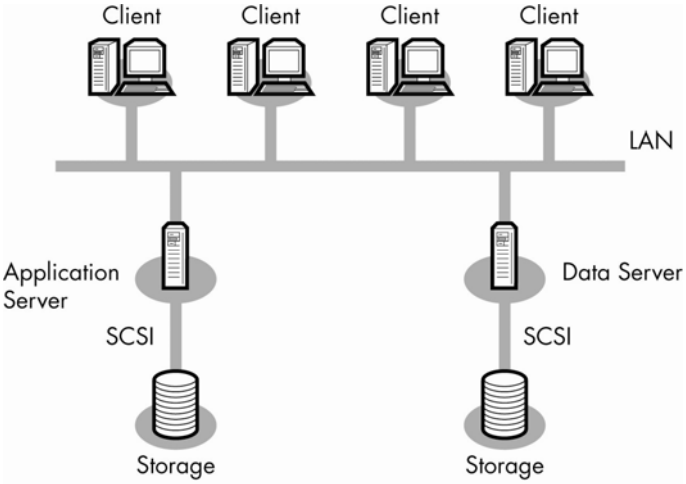

Figure 1: DAS use of dedicated storage devices for each server may result in an inefficient use of storage capacities.

This requirement for flexible storage allocation to other applications is being met with **Network Attached Storage** (NAS). The storage devices are able to accept and manage data from different servers, allowing dynamic use to be made of storage capacity. However, this system doubles the data traffic between the servers, because an application server has no storage (DAS) of its own. Another disadvantage is the protocol, which is not optimised for storage tasks and thus causes excessive overhead. In other words, it is not designed for fast access to a mass storage system.

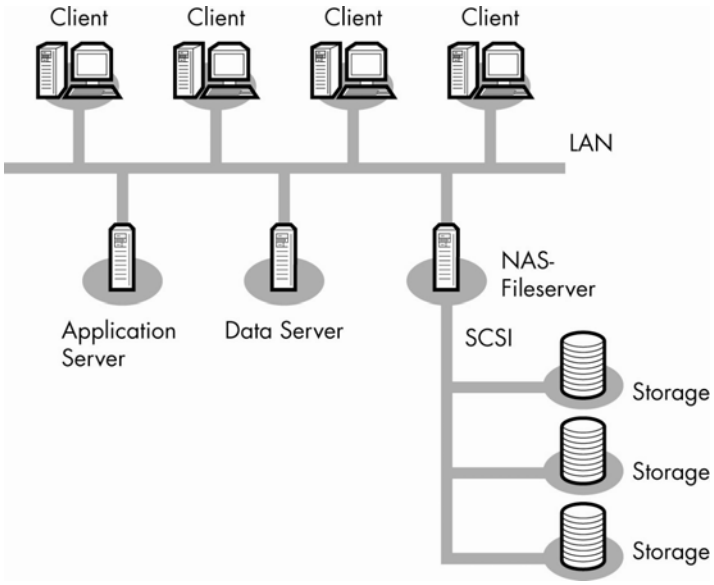

Figure 2: NAS save data from different servers but generate more data traffic in the LAN.

Consequently, an independent and separate **Storage Area Network** (SAN) was developed. A SAN is akin to an additional LAN network for storage devices. Communication between a LAN and a SAN is handled by application and data servers. The latter also organise data traffic between the storage media. Data traffic between servers and storage is made up of block-based data. A SAN generally utilises the SCSI communication protocol, which is superimposed as a transport protocol on Fibre Channel (FC) or iSCSI. The data being transported and stored are highly available in a SAN thanks to redundancy.

Advantages of a SAN:

- High availability of data
- Capacity utilisation
- Central administration/management

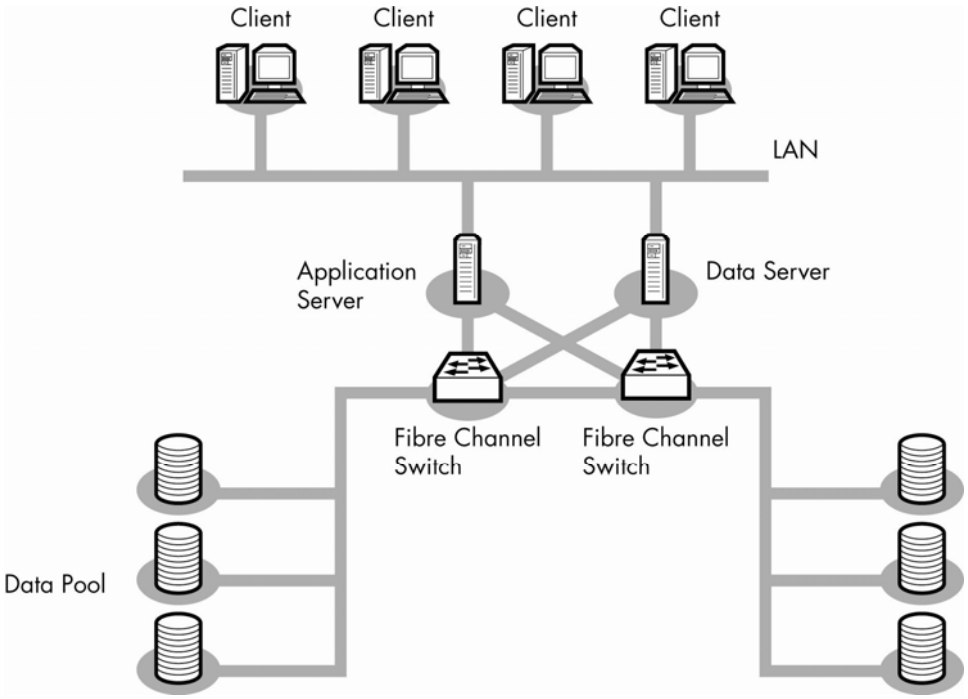

Figure 3: A SAN is a high-speed network with different storage media and is separate from the LAN.

2 Legal, strategic and operational aspects of storage area networks

The need for quickly accessible storage affording a high level of security will continue to increase sharply in the future for economic and legal reasons (Sarbanes Oxley Act SOX, EU Data Protection Directive, etc.).

SAN structures are characterised by the virtualisation of the connected storage sub-units. With this feature, applications can access data blocks in the storage area at will, and optimum use can be made of the available capacity.

The access speed must remain high regardless of the data quantity. This is a main prerequisite because time-critical paths often exist in this context (e.g. financial or stock exchange transactions, need for large data quantities for computations at large centres, etc.). As database access can potentially be limited or hindered by regular traffic, many users prefer to separate regular ICT structures physically from storage networks. In addition, a separate storage technology allows a network to be managed according to its own specific needs, also with respect to security requirements.

Another way of avoiding capacity bottlenecks is to provide extremely large bandwidths in the ICT structure, bandwidths of the kind now possible with Ethernet solutions. The latter are very affordable and easy to administer. In the longer term, many users will probably no longer want to pay for two different security architectures and the elaborate role separation involved. They will opt instead to have the same network technology for both tasks.

The widespread use of FC technology over the past decade is attributable to two factors: availability and manageability (with one dedicated SAN). In the years ahead, storage technology will see big advances in performance capacity as 10 Gigabit Ethernet networks become widely available for FcoE transport. These developments will shift the bottleneck from network capacity to the hardware units (i.e. servers).

Basic technical conditions will also change dramatically, as the flexibility of packet-based protocols makes the “everything-over-everything” principle a reality. It is therefore advisable to keep the OSI Layer model in mind in the assessment of possible protocol combinations. Besides “pure” protocols such as FC or Ethernet, there are also conversions such as iSCSI, FCIP, or iFCP. The ability to transport data over larger distances (and not just as an “internal” link at the site of the storage centre) plays an important part here, because protocols and network components must be sufficiently suited for this task.

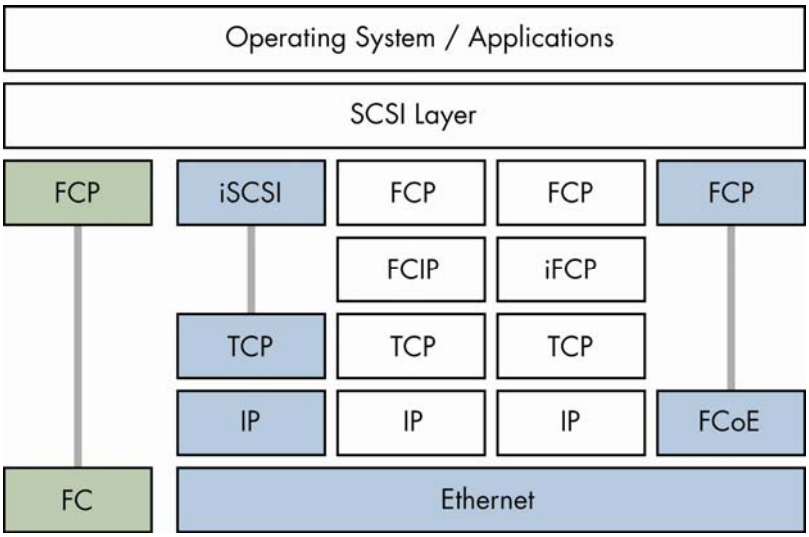

Figure 4: Fibre Channel (FC) and Ethernet are the protocols that now prevail in the storage sector. Ethernet can transport and integrate iSCSI, FCP, IP, TCP and FC.

3 The significance of SANs for the modern operations of organisations

Organisations and companies rely increasingly on jointly available data as part of their modern approach to work. The transfer of knowledge between decentralized project managers and central storage systems is therefore crucial to achieving lean, effective and efficient operations. All project staff members involved have to have fast access to all project information on their knowledge platform. Applications frequently used in this context are placed together on one portal such as an Intranet. The user has to authenticate himself only once. With this single sign-on, he is allowed to operate the programs and databases he needs on a daily basis. The way individuals work depends largely on the type (and quality) of central data storage involved. Ideally, the user can benefit from the advantages of this arrangement without having to have any special affinity to the technology.

This central data storage is usually viewed as part of the information and communication technology (ICT) system. In bigger organisations, however, this storage entails special requirements that can only be met with network and storage technology specifically geared to this purpose. These problems should be seen particularly in connection with the fast-growing deluge of data worldwide. In other words, many organisations require data to be available online at practically every location around the globe, as a vital nerve for the given organisation. And this availability must be achieved without requiring the user himself to have any affinity to the storage concept or technology. This capability is generally achieved with a separate Storage Area Network SAN, which ensures data transfer and storage on a large scale, with reliability and security guaranteed. However, the transition between regular ICT and SAN can be fuzzy, especially for technological or cost reasons.

Unprotected network links are the rule in WANs due to global networking. That means information security in a SAN is a major issue. After all, the stored or transferred data always include highly confidential information. Of course, valuable data also have to be protected against simple risks such as fire, water, weather, etc. (physical security). In designing a high-tech SAN, one therefore always tries to cover as many of these requirements as possible in a compact and efficient way.

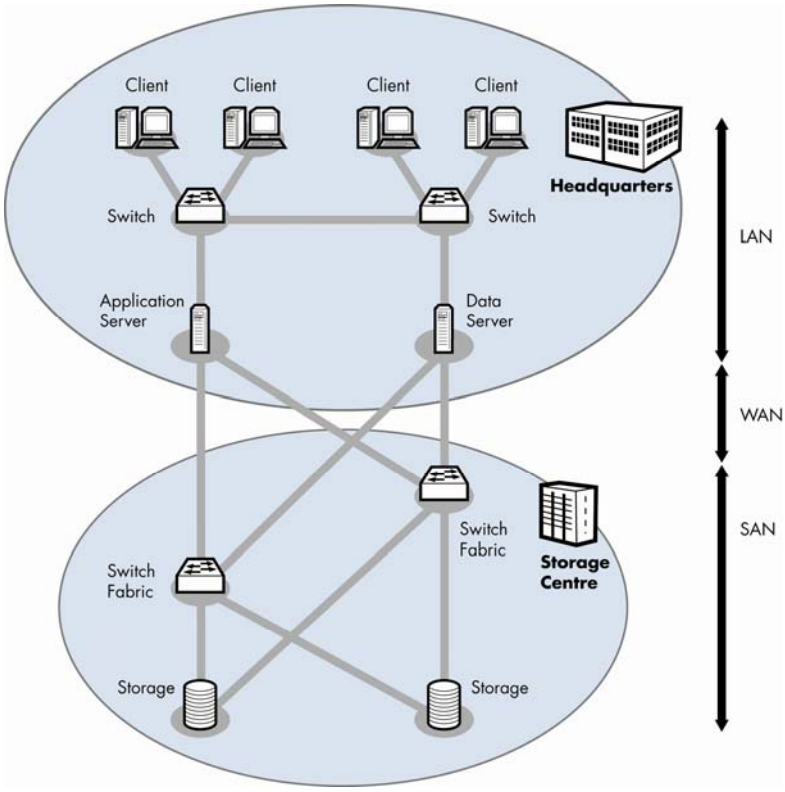

Figure 5: The switch connecting servers and storage in a SAN is called Switch Fabric. Fibre Channel Switching connects each server with each storage device, generally taking a redundant approach.

4 The requirements for SAN from the perspective of an organisation

High-security real-time data access in large organisations is typically provided by an encrypted high-performance network linked to the various locations (which could well be far away geographically).

In many cases, data are stored redundantly by the block in virtually divided mass storage units. Connecting links are always implemented redundantly. The result is a special storage infrastructure called a SAN fabric. This fabric is disaster tolerant, i.e. capable of making available the entire data quantity online again in the event of data losses in sub-areas and capable of doing so without the user even noticing. Transport networks for time-critical data access may have too little capacity at times, so a common practice up until now has been to use a separate network as storage infrastructure. Frequently, another transmission protocol may even be used for security reasons to be able to uncouple network management from the ICT (role separation). At the same time, a security policy specifically defined for data storage can also be established (known as secrecy splitting).

In keeping with its pivotal importance for the efficiency and security of an organisation's work, a SAN is subject to specific topology requirements. Technology requirements (e.g. the available network base) and costs also play a decisive role.

The following requirements are certainly among the major ones that have to be met by a SAN:

- Fast storage: Complex arrays of extremely fast, often spatially separated, and high-capacity storage units linked redundantly with each other. They are controlled with specific procedures that optimise the desired criteria, e.g. sufficient redundancy, optimum risk spread and fast access.
- Fast data links with sufficient back-up bandwidth between the storage locations
- The possibility of fast switchover to redundant channels
- Redundant overall system: In the interest of continuous availability, redundancy is an objective for all components necessary for operations.
- Automated processes/services running in the background unbeknownst to the user, particularly to protect information while it is being transported and stored
- Physical security: Spatial separation of storage sites can avoid the risk of a total loss of data holdings, but physical security (protection against fire, water, earthquake, terrorism, unauthorized access, etc.) must still be provided at each individual location. This protection is afforded by means of structural measures, bunker systems, line monitoring, multi-path line routing, alarm and security equipment, etc.
- Logical security: Data may only be transported and stored in encrypted form. In addition, further security aspects must be considered, e.g. variable user authorisation and protection against electronic attacks on network components.

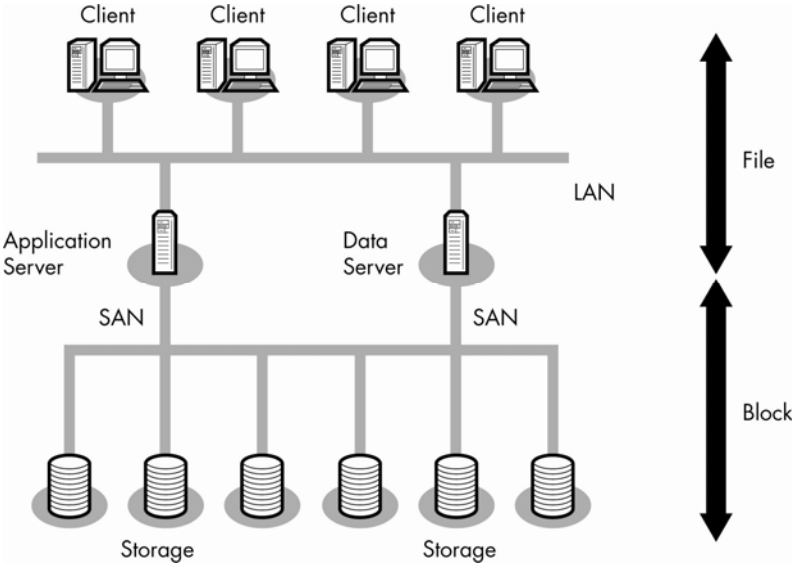

Figure 6: In a SAN, one refers to block data instead of files. Block data always have the same length and can therefore be optimally stored and reread again (calculable).

5 The core issues in technical realisation

The current technology has a broad range of possible functions and features for meeting the requirements outlined in Chapter 4. The following list contains the key criteria for designing or expanding a SAN:

- The SAN fabric principle: Every storage site is always connected to every other one to ensure maximum redundancy. With the dense supply of public networks, there is a large choice today of suitable sites with broadband access. Ideally, this situation allows several networks from different providers to be used, which further increases redundancy.
- Broadband/quality of service: Owing to the large reserves of broadband capacity, fast data access is guaranteed even with large volumes. If capacity is leased on broadband links at a provider, dynamism on the part of the user cannot be maintained unchecked over extended periods. That is why it is indispensable to apply criteria for quality of service (QoS). These criteria are part of a leased-line agreement with the provider. The network manager for the user organisation, for his part, must constantly monitor capacity utilisation and, where appropriate, make timely adaptations in QoS criteria before disruptive delays occur in data availability.
- Latency/real-time processing: When SAN links are planned, distance problems, e.g. the number of hops, must be taken into account in the concept. Individual optimisations may be achieved by getting the providers involved, depending on the selected technology. It is also important to bear in mind that encryption should not impair latency time to any substantial extent. Encryption is normally done on Layer 2 for that reason. Units from Crypto AG are exceedingly well suited for SAN applications in this respect.
- Redundancy: The concept of SAN fabrics includes the idea that there is a redundant connection for each link wherever possible. This is the only way to ensure virtually complete availability. Ideally, different paths (networks) are used for this purpose. This approach is not always technically feasible, however, and cost can be an issue. Redundant channels should ideally not have a lesser bandwidth or QoS. And each link must be integrated in the encryption system. A redundancy channel presumably used only in an emergency could lay the system open to attack (e.g. after a successful physical attack on the regular connections!)
- Transport protocols: The task varies greatly with the size of the organisation. High-performance Layer 1 and 2 protocols are preferred for transport in light of the performance required. However, the data can also be loaded on Layer 3, which creates multiple nesting arrangements. For medium and larger systems, FC frequently serves as the basic protocol. Lately, technological advances have resulted in hybrid concepts employable for new as well as expanded SANs (refer to Chapter 8).
- Security solutions: SAN security solutions focus on ensuring data protection without impairing performance and on the efficient, trouble-free operation of the SAN as an overall entity. Key words in this context:

    - High encryption performance, i.e. 100% of the network bandwidth, so that no disruption of data throughput can occur
    - High level of reliability/availability through the use of redundant components with automatic switchover
    - Important parts designed for long mean times between failures (MTBF)
    - Hardware-based solutions incorporating high-security cryptographic solutions
    - Encryption of all transport protocols in hybrid/mixed solutions with the same level of performance and security
    - Automatic key changes that go forward without disrupting operations, are programmable for a given time and occur without staff being present
    - Simple central security management – online, in-band and/or out-of-band
    - Technologically smooth implementation in the networks with a one-network philosophy being applied
    - Optimum maintenance and logistics concept (lifecycle management)

- Cost of the entire system: Technology advances are also opening up new possibilities with regard to total costs. FC components are generally relatively expensive. That means the trend to hybrid solutions may well be cost-driven. However, other factors such as physical security may have greater relevance for the total bill. An organisation can boost efficiency substantially by fully integrating a SAN project in its ICT infrastructure and not least, obtain a homogeneous information security solution in the process. The parallel use of transport links by SAN and ICT (with virtual separation of services and high-security SAN encryption) can potentially cut costs considerably.

6 Fibre channel as the most wide-spread technical solution to date

FC remains the most widely used protocol for large-capacity storage networks down to the present day. Its position can be explained by its history (serial transport; over several parallel channels if need be) and its large performance capacity (small header, big payload). As a protocol standard, it is very open and does not have its own command set (only data transport between two FC devices/units). It is easy to install and highly reliable. FC was created as a protocol for use over longer distances within storage centres.

The partial openness of the FC standard has the disadvantage that manufacturers often integrate proprietary features in their systems. This drawback is more than made up by the fact that the network is potentially virtually unlimited in size and is scalable to any extent desired.

Because FC is (almost) strictly a storage technology, FC components have remained niche products of sorts in network traffic globally (very few providers) and have correspondingly high price tags. At the same time, FC is used in over 80% of SAN applications. And owing to the simplicity of this technology, operating costs after installation are probably not as high as is often alleged.

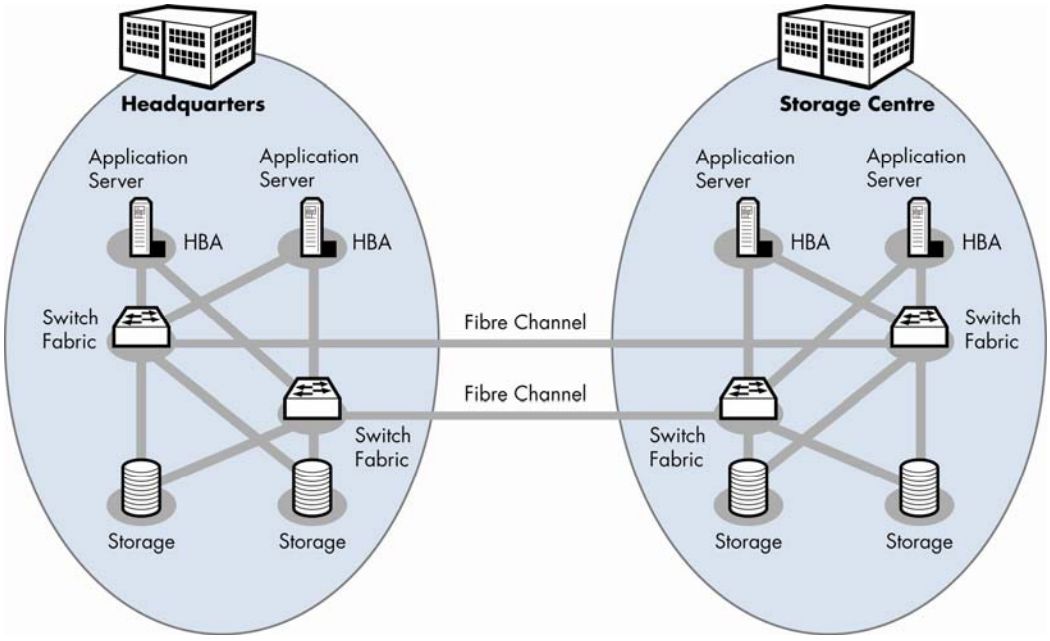

Figure 7: FC link connecting computing and storage centre. Host bus adapter (HBA) connect server with the fibre channel network.

7 Technical advances expected in the next five years

Until now, FC has been practically unsurpassed in terms of bandwidth performance and its position was uncontested for that reason. The most common bandwidth at present are 4 Gbit/s – 8 Gbit/s (10 Gbit/s) occur less often. This position is being threatened now by Ethernet, because 10 Gbit/s performance has quickly become the standard in this sector. There is little talk yet about a bandwidth increase for FC to 16 Gbit/s.

Consequently, 2008 saw the start of the demise of FC. A technology shift is expected to occur over the next five years. The determining factor for the replacement of FC is that beyond this 10 Gbit/s bandwidth potential, Ethernet will have a greater transport capacity than the FC protocol. In addition, Ethernet components are much cheaper to obtain. After FC-based servers, users are now finding it worthwhile to convert the protocol to Ethernet and send the data in this form over the link.

Of course, an enterprise that already has a reliable FC infrastructure could conceivably upgrade it to 8/10 Gbit/s FC for simplicity's sake and thereby avoid having to build up expertise in a new technology.

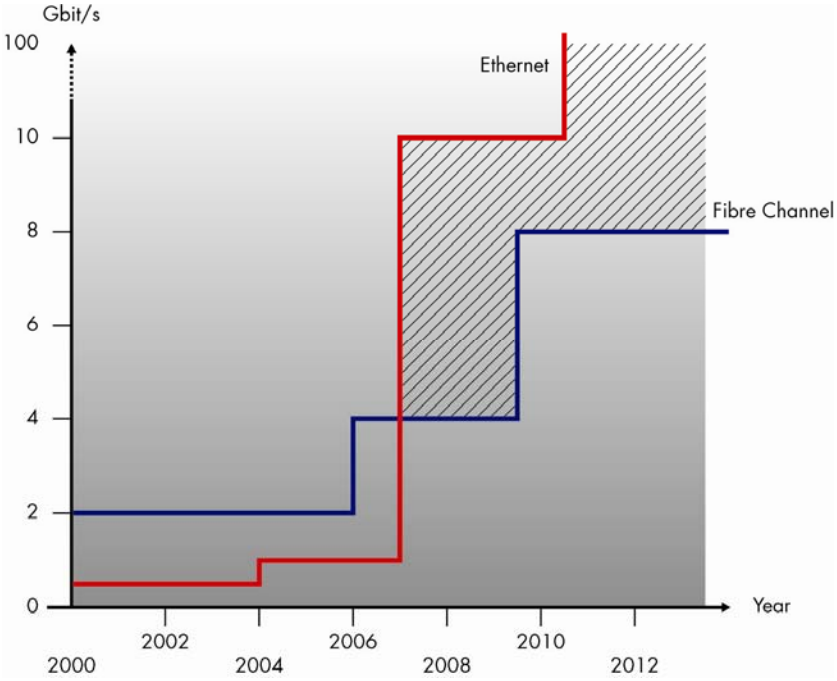

Figure 7: Comparison of bandwidth development for FC (blue) and Ethernet (red). FC has multiplied its performance capacity by a factor of 2 (2, 4, 8 Gbit/s) whereas Ethernet has done so by a factor of 10 (10 Mbit/s, 100 Mbit/s, 1 Gbit/s, 10 Gbit/s).

Many who have used FC until now will soon have fundamental decisions to make about storage technology (also as regards upgrades). In all probability, FCoE will probably win the day over the longer term in large-scale SANs for cost reasons. The FC investment can continue to be used. Building up Ethernet links concurrently, however, opens up several new perspectives for further protocol combinations in the future.

The large Ethernet bandwidth solves, inter alia, the problem of network loading due to data accesses over co-used channels. For this reason alone, a user no longer needs a second network and can consistently pursue a one network strategy. Multi-pathing redundancy can also be reliably implemented on an Ethernet basis. FCoE assumes high quality Ethernet, also known as Converged Enhanced Ethernet (CEE) or Data Centre Ethernet (DCE).

Further expansion possibilities are being opened up by new HBAs or NICs, which are obtainable for all common protocols. Almost any combinations of transport networks can now be used as SAN fabric components. Gradual conversion and mixed expansion with different protocols are consequently also possible. This approach could potentially be a reasonable strategy if organisations or enterprises merge. A solution of this kind can also be viewed as a one network concept with regard to the ICT infrastructure.

Many users will take advantage of this situation to make a fundamental decision on whether to continue pursuing a multi-network strategy (security, administration, redundancy) or to converge the technologies for cost reasons and pursue a one network strategy. Of course, this decision involves more than the issue of technology. It also entails risk assessment for the organisation and the organisation's own security policy.

It is widely believed that SAN networks in ICT systems are less secure than separate networks. This view is incorrect if the SAN incorporates high-security encryption using customer-specific algorithms, of the type offered by Crypto AG. Hardware-based encryption creates such a "hard" virtual separation and renders the administration of the SAN structure so completely independent that security remains at the same high level.

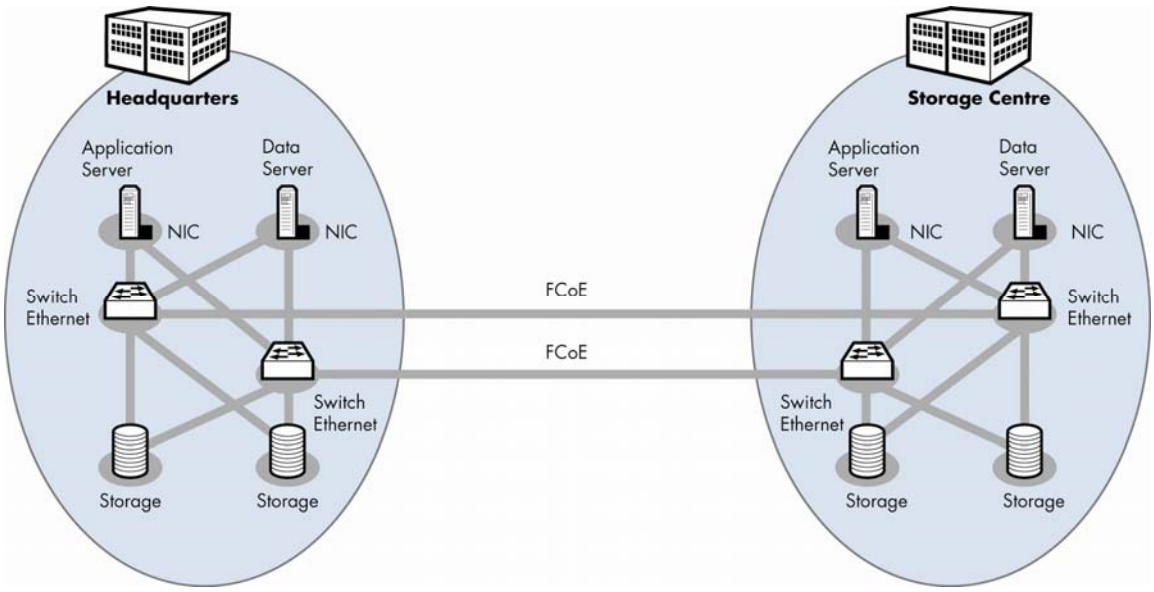

Figure 9: Computing and storage centre connected by an FcoEthernet link. Network interface cards (NIC) connecting servers to the Ethernet network.

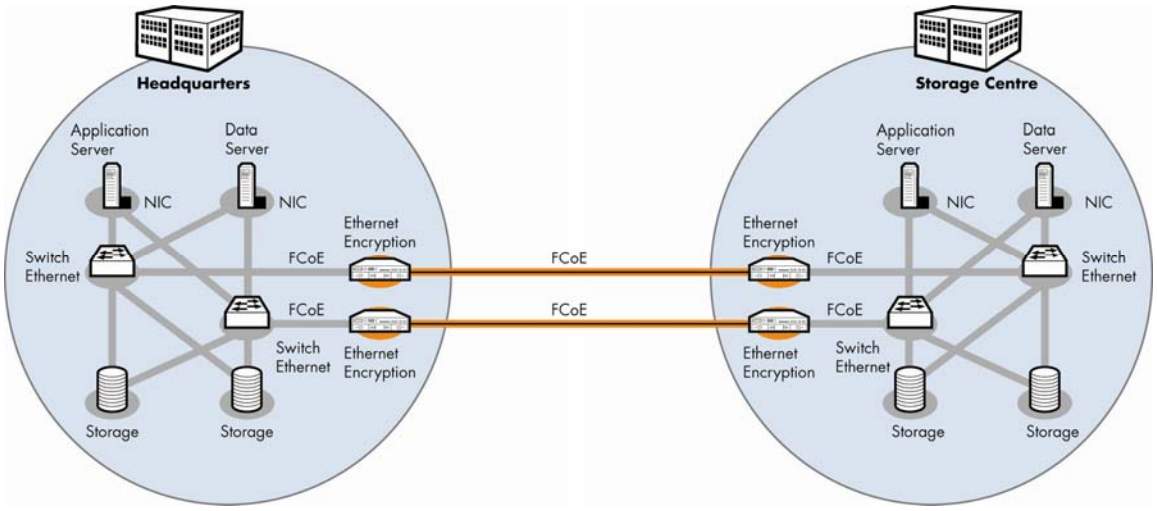

Figure 10: Direct use of Ethernet encryption units in an Ethernet SAN.

8 Potential for further (hybrid) one network solutions

Based on the known OSI Layer Model, myriad combinations ("everything over everything") of packet-based protocols can be implemented. The greater the use of Ethernet, SDH or other widespread Layer 1/2 protocols, the fewer the compatibility problems that can arise. The availability of multiplexers and integrated HBAs (for numerous protocols) can lead to entirely new configurations. The most promising versions for the future:

- FCoE: The efficient expansion of existing FC structures by means of FC data uploads for longer links on a Converged Enhanced Ethernet (CEE) or Data Centre Ethernet (DCE; with a suitable HBA converting the data back to FC at the server).
- FC via SDH: Where a provider offers an SDH interface, FC can also be efficiently sent multiplexed over longer distances via SDH instead of via Ethernet. SDH has certain advantages in terms of operational reliability (ring networks).
- iSCSI over Ethernet: Originally an internal bus system, SCSI had several advantages for internal connections within the storage centre, but is increasingly also used (packed in IP packets) for external link transports via WAN Ethernet. All-IP enterprises can thus implement their SAN architecture on an IP basis. Some experts are even saying that FC structures could also be replaced by IP-based iSCSI SANs in the future.

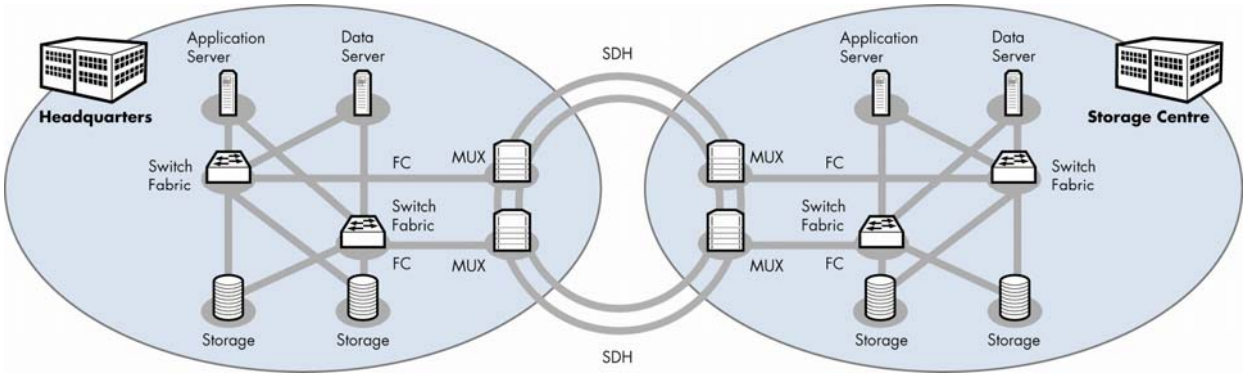

Figure 11: SAN with hybrid links: That means the Fibre Channel protocol is converted in the multiplexer to an SDH protocol for transmission to the data centre.

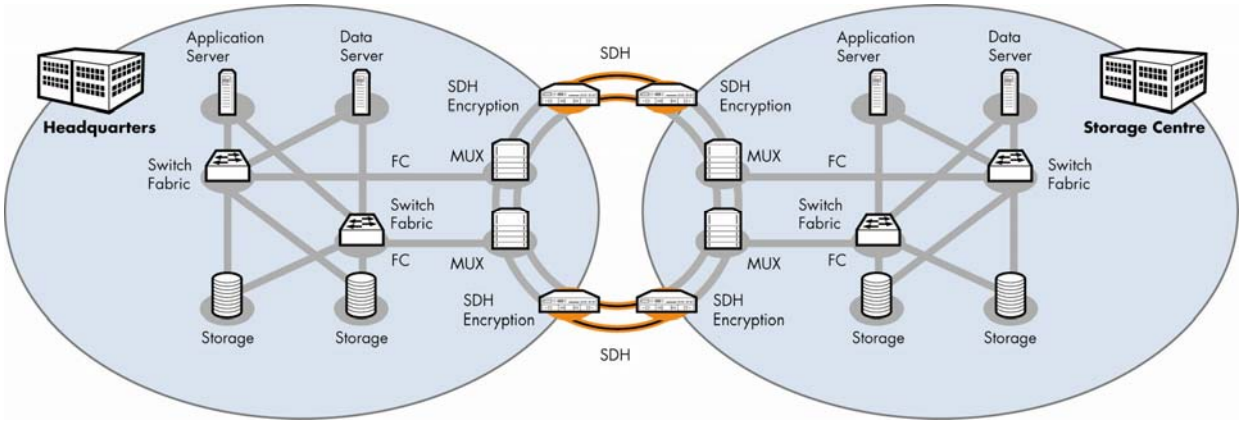

Figure 12: After the multiplexer (MUX) converts the FC protocol to SDH, the protocol can be encrypted with SONET/SDH encryption units.

9 Hardware encryption solution ensures perfect autonomy and security

As protected zones, storage centres are generally secure enough for data to be exchanged in plain text between the individual storage areas. High-security encryption of the data flow is mandatory, however, if individually protected storage centres or areas are connected together (or with the user's data centre) via links that leave the protected zones. The fact that SAN structures can now be rendered more flexible also gives users more freedom of choice on this key issue of information security. In particular, they can gradually converge their network technologies for ICT and SAN to create a (strategically lasting) uniform security architecture in the SAN fabric regardless of the protocols that are or were originally used. And they can do so at a reasonable price.

Security solutions in the SAN fabric are based on encryption of data in separate hardware modules shielded off from the network. This approach is the only one that delivers maximum security (secret, customer-specific algorithm base, no integration of vulnerable network components, protection against attacks from the network). In addition, transport performance is not impaired and the latency time remains virtually unchanged. Each encryption device can be accessed individually and directly for purposes of security management. Key changes are based on time or throughput criteria and are programmable automatically without any disruption to operations. In other words, absolute availability, such a crucial factor here, is never impaired.

A further basic advantage of hardware-based encryption within SANs is that the network status of encryption units can be monitored and managed independent of regular network management. This feature eliminates the need for physical separation with an additional network.

10 iSCSI - the cost-effective and scalable SAN technology for small and medium-sized businesses

For storage area network (SAN) applications, the Fibre Channel FC protocol has been able to acquire a large market share over recent years on account of its performance. However, this position is now being challenged by Ethernet, in the protocol combination of FC over Ethernet (FCoE). For large SAN applications this can be very advantageous as it allows for better consolidation of the network, simpler management and more cost-effective set-up and operation.

However, the tremendous technical development now presents a further new possibility for smaller SAN applications: the use of the already 20-year-old SCSI protocol – originally only intended for intra-system connections – over any distance. This was achieved by packaging SCSI commands in TCP and their block-by-block transport using IP. This meant that the "machine protocol" of the storage units was also used for the longer transmission routes, allowing a more direct data flow between the centres and a correspondingly simpler server consolidation. This technology is called iSCSI, enables global logical networking and can be easily administered using IP. The performance is very high thanks to today's large IP network capacities – and not every user really needs a super-fast SAN. With iSCSI, future SAN operators do not need to develop any additional know-how and can implement SAN and LAN on the same infrastructure (Ethernet/IP). iSCSI SAN applications are particularly suitable for the replacement of existing NAS configurations: initial investment is not great (Ethernet switches are cheaper than FC) and the implemented solution can be easily scaled at a later point. The reservation expressed previously, that only physically separated SAN applications are really secure against misuse, is easy to refute nowadays because using high security encryption of the virtual SAN areas, the separation is de facto just as thorough – with considerably less effort. And the iSCSI also performs well as regards logical security: technical stability is high and after an interruption the recovery can generally take place without any special intervention.

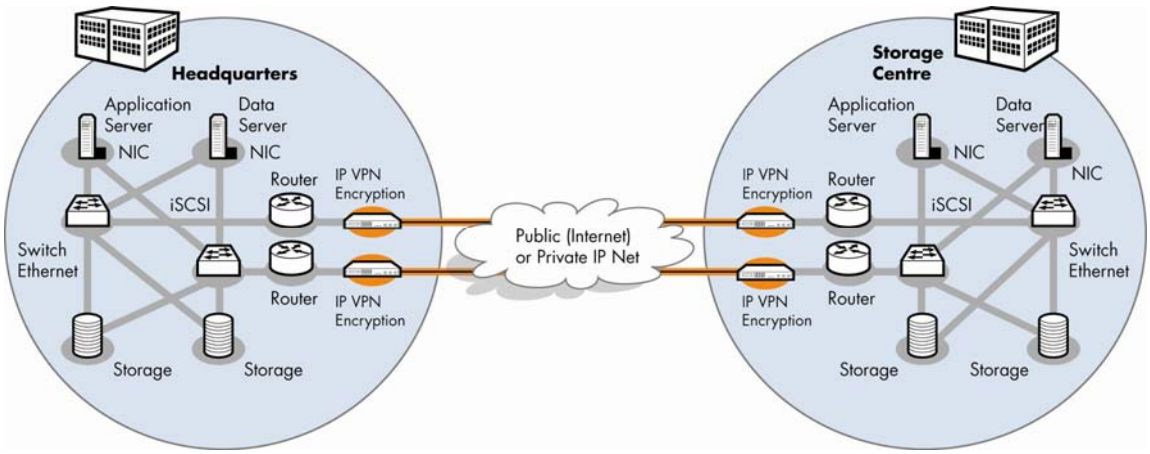

Illustration 13: A SAN is operated via iSCSI on the same infrastructure (Ethernet/IP) as a LAN.

11 Glossary

SAN fabric	A network designed specifically for data distribution in storage centres. Its typical characteristics include multipathing, redundant transport channels and high data throughput rates.
Ethernet	As the most widely used transport protocol for LAN (Local Area Network) and WAN (Wide Area Network), Ethernet has affordably priced components and guarantees good compatibility thanks to robust standards.
SDH **Synchronous Digital Hierarchy**	Widespread WAN protocol usually used on fibre optic links. Focus is on high availability. Typically created with ring networks.
FC **Fibre Channel**	Special transport protocol for SAN applications. Each unit is uniquely identified, as is each port of the unit. This allows easy direct networking using switches. In particular, it simplifies and accelerates the operation of virtual storage areas in disk arrays.
SCSI **Small Computer System Interface**	Parallel interface originally developed for connections within a computer. Today it is also used for networking in SAN. iSCSI as an advanced version: The data are packed in IP packets for transport over WAN.
Multiplexing	Data transport process with which several signals can be bundled and simultaneously transmitted over a single medium (copper cable, optical fibre, radio link).
MUX, Multiplexer	Selection switch with which signals from different sources can be bundled and combined into parallel data streams. The reverse process is demultiplexing, which is used to filter out/separate out individual signals from the bundle.
HBA (Host Bus Adapter)	Adapter in the server (also known as an NIC, Network Interface Converter) with an interface function.
ISO **International Standards Organisation**	Organisation that developed the OSI Model (Open Systems Interconnection Model)
LAN **Local Area Network**	Local, private, geographically limited network
WAN **Wide Area Network**	A wide-area traffic network that can cover large geographic areas and distances. WANs generally operate on Layers 1 + 2 of the OSI Model.
OSI **Open System Interconnection**	A model depicting how data are transported within (and between) networks (or subscribers) and which functions are used for this purpose. The designation “protocol” is used for the individual functions because the open system can only function with documented standardizations.
Router	Active element (node) for connecting two networks at the network level. Routers usually operate independent of protocol (multiprotocol operation) and determine the route based on information in the data packet. Internet nomenclature also uses the term “gateway”.

www.crypto.ch

Crypto AG – To Remain Sovereign

Crypto AG is your ideal partner for the efficient and secure handling of information. As a legally and economically independent Swiss company, we are not subject to any export restrictions.

We have developed, manufactured and implemented custom security solutions for over 55 years. The package we offer features the latest technology solutions and comprehensive services. Throughout the entire lifetime of your system, we provide you with support services to guarantee autonomous operation and high availability whatever the user environment.

You too can rely on the expertise and capabilities of Crypto AG – just like our customers in over 130 countries.

Crypto AG, Headquarters

Crypto AG
P.O. Box 460
CH-6301 Zug
Switzerland
Tel. +41 41 749 77 22
Fax +41 41 741 22 72
crypto@crypto.ch
www.crypto.ch

Crypto AG, Regional Offices

Abidjan
Crypto AG
01 B.P. 5852
Abidjan 01
Ivory Coast
Tel. +225 22 41 17 71
Fax +225 22 41 17 73

Abu Dhabi
Crypto AG – Abu Dhabi
P.O. Box 41076
Abu Dhabi
United Arab Emirates
Tel. +971 2 64 22 228
Fax +971 2 64 22 118

Buenos Aires
Crypto AG
Maipu 1256 PB "A"
1006 Buenos Aires
Argentina
Tel. +54 11 4312 1812
Fax +54 11 4312 1812

Kuala Lumpur
Crypto AG
Regional Office Pacific Asia
Level 9B Wisma E&C
2, Lorong Dungun Kiri
Damansara Heights
50490 Kuala Lumpur
Malaysia
Tel. +60 3 2080 2150
Fax +60 3 2080 2140

Muscat
Crypto AG
Regional Office
P.O. Box 2911
Seeb PC 111
Sultanate of Oman
Tel. +968 2449 4966
Fax +968 2449 8929

A member of
The Crypto Group