Master of computer network engineering, 60 ECTS

MASTER THESIS

Evaluation of Storage Area Network (SAN) security and performance

Siavash Hajirostam

Master thesis
15 ECT

Halmstad,Sweden 2013

Evaluation of Storage Area Network (SAN) Security and Performance

Master Thesis in Computer Network Engineering

November 2013

Author: Siavash Hajirostam

Supervisor: Tony Larsson

Examiner: Tony Larsson

School of Information Science, Computer and Electrical Engineering
Halmstad University
PO Box 823, SE-301 18 HALMSTAD
Sweden

Evaluation of Storage Area Network (SAN) Security and Performance
Siavash Hajirostam

Master thesis report IDE 1325
School of Information Science, Computer and Electrical Engineering
Halmstad University

Preface

I would like to express my appreciation to my supervisor, Professor Tony Larsson, for the many useful discussions, comments and suggestions on this thesis and also my thanks go to the staff of Halmstad University for giving me the opportunity to study in the computer network engineering program. Finally, my special thanks to my family for their encouragement and support during my studies.

Siavash Hajirostam
Halmstad, November 2013

Abstract

Due to growing the number of Information Technology (IT) users all around the world, consequently the amount of data that needs to be stored is increasing day by day. Single attached disks and old storage technologies cannot manage the storing these amounts of data. Storage Area Network (SAN) is a distributed storage technology to manage the data from several nodes in centralize place and secure. This thesis investigates how SAN works, the file system and protocols that are used in implementation of SAN. The thesis also investigate about other storages technologies such as Network Attached Storage (NAS) and Direct Attached Storage (DAS) to figure out the advantages and disadvantages of SAN, The main focus of the thesis project is on identifying the security vulnerabilities in SAN such as possible attacks in different SAN protocols. The thesis finally identifies the performance factors in SAN to figure out how to improve the performance with respect to security solutions aimed to enhance the security level in SAN.

Contents

1 Introduction

With advancement of information and communication technology (ICT) the amount of data that needs to be transferred and stored on disks has grown enormously in a computer network environment and growth from Gigabyte in early 1990 to Exabyte in 2010. Many technologies have been developed to manage and handle this traffic of data for use in different scales of networks such as LAN, MAN and WAN. Some examples of these technologies include Network Attach Storage (NAS), Direct Attach Storage (DAS) and Storage Area Network (SAN). Storage Area Network (SAN) is a high speed network of storages and fabrics that connect to computers and servers to provide shared pool of storages for different servers with different operating system, all the servers all around the network access to SAN storages like a local attach disk. SAN manages and stores data in high speed and centralized place with ease of management. Security has always been highest priority in such networks for network administrators, working with information and sensitive data of their companies. These networks encounter different attacks and storages on their own do not have any security features. Another important element for implementing SAN is performance of the system. Knowledge about the key performance elements as well as advantages and disadvantages of this technology is crucial to comprehend the dynamics between security and performance. Knowing the vulnerabilities is one of the critical tasks for making storage systems secure, knowledge about security elements and solutions can help storage administrators to improve the level of security and reliability of a network. Security, performance and reliability make SAN as a good solution for storing data in a larger scale network.

1.1 Societal and Ethical Aspects of SAN Technology

This thesis investigates SAN from security (including safe storage) and performance perspectives. Especially the security issue is important for the society since it depends on the secure storage and communication of large amounts of data. The problem with the rapid growth of computer and communication technology and access to information is to guarantee that they their data are safe and secure from unauthorized access.

1.2 Problem

This thesis analyses security and performance aspects of SAN technology, more specifically, the thesis addresses security risks, vulnerabilities, performance factors and solutions for improving security of SAN in relation to performance.

1.3 Thesis Goals

The main goal of this thesis is to find out the different security risks and attacks in SAN. Investigate methods that can improve security, compare between the security aspects, performances factors in different protocols that are used to implement the SAN such as iSCSI and FC, to find out which one is the most reliable and efficient in different scales of networks.

1.4 Thesis Questions

This thesis is aimed to answer the following questions:

- What are the security vulnerabilities and possible attacks in SAN?
- What are the performance improvement methods in the implementation of SAN?

1.5 Thesis Methodology

The methodology of this thesis is divided into a literature study part and a practical part. In the literature study part the different security methods of the SAN are investigated, to find out security solutions, vulnerabilities and attacks in different SAN protocols, compare between the functionality of these protocols and find out the performance elements of SAN in different SAN protocols to improve the performance. In the practical part a model of iSCSI based SAN is simulated to measure the performance and find out some of the security vulnerabilities and the solutions to make iSCSI SAN secure.

1.6 Thesis Structure

The rest of this thesis work is organized as follows: Chapter two explains the functionality of SAN and other technologies that is used in the storage area and make comparison between them, explain different protocols that are already used for implementing SAN and make a comparison between them about the working structure. Chapter three focuses more on the security aspects in SAN and discusses the security risks, threats and vulnerabilities in SAN and different types of attacks in each of the protocols that already SAN implements on them, such as iSCSI and FC and verifies the defence method for each one of them used to increase the level of security. Chapter four discusses the performance aspects in SAN and makes comparison between the performance elements of the SAN protocols and the effects of some security issues on the performance of the system. Chapter five contributes with a set of conclusions from the thesis work. Appendix shows the practical experiment of an ISCSI SAN using an open source operating system “Openfiler” for having deeper understanding of functionality and security risks of iSCSI SAN.

2 Background

Over the years storage network technology has been faced with significant changes and there are many new innovations try to improve the level of service and reliability in storage area. Information and data are essential part of any company and business today. Besides storing information generated from many applications, users need to access to this information in a fast and reliable way. Most companies need more storage capacity day by day for storing their data; SAN is one of the storage technologies that are used currently in different network size for storing and accessing the data in faster speed and reliable way.

2.1 Storage Area Network (SAN)

The Storage Network Industry Association (SNIA) defines SAN as a network in which the main purpose is to transfer data between servers and storages [3]. The network consists of several computers, servers and devices that are interconnected with each other; this infrastructure allows different computers to communicate with each other [4]. The operation of each SAN consists of basic elements for communication, which manages the physical connections, management layers for organizing the available connections, computer system and storage devices for reliable and secure handling of data. SAN manage the data at the block level and thus not at the file level for keeping track of and allocating free space on disk to the data. SANs are used to make a high speed connection between storages and servers [3] [1].

2.1.1 Storage Area Network objectives

The main objectives that make SAN a popular solution for storage networks are: disk utilization, disaster recovery methods, availability of data and fast backup data ability. SAN help users to use disk resources in a more efficient way, since all the disks in SAN are kept together as one resource so the management of disks become easier and disks can work better and more utilized, resulting in less waste of free space. One can therefor save power and increase the performance of the system. SANs are capable of adding or removing new disks for expanding the free space to servers and applications, whenever an application need more space, it is thus easier to make free space available without turning servers down or power them off to allocate free space to applications. SAN has good disaster recovery method; by mirroring the data to another disk that located in another place and also used different types of Redundant Array of Independent Disks (RAID) to provide mirroring and data duplication, SAN improve the communication I/O by using fibre optic cables and gigabit Ethernet LAN also reduce the physical space that need for keeping storage devices and servers, because SAN handle the data management with lower number of servers and higher number of disks. SAN components consist of basic elements such as connectivity part that typically is fibre optic in FC and fast or gigabit Ethernet for iSCSI, hubs, switches, directors, connectors and routers are the main components of SAN. Components can be from different storage devices e.g. tape, Just a Bunch of Disks (JBOD), Enterprise Storage Servers (ESS), Serial Storage Architecture (SSA) and IBM DS family storages. Different servers in SAN can use different operating systems such as Windows, UNIX and LINUX. By help of different communication techniques and communication protocols such as iSCSI and Fibre Channel Internet Protocol (FCIP) SAN allows the storage management over long distances with high speeds in centralized and efficient way. Traditional storage devices work with SCSI connectors for making communication with host, that makes the connection length limited to 25 meters but SAN with using fibre optic technology overcame to this limitation and extended it up to 10 kilometres and increased the number of connections that was 16 in SCSI to unlimited for FC [1], [8], [3].

Beside all these advantages of using SAN, some disadvantages also exist in SAN which makes SAN a less suitable solution for small installations since SAN devices are rather expensive and personnel supporting these devices needs to have good knowledge of architecture of SAN, budget and certain types of equipment to support and troubleshoot them. SAN cannot be a good solution if you need a file server to store and share files and data with others in your entire network, because there are several cheaper ways that exist to have a file server, such as using NAS or using sharing features in windows and UNIX operating systems. The cost of implementing of very simple and small SAN is around $100.000 so cost always can be an issue to using or not using one technology, if our network does not have a large number of servers which need to be reliable for working with several applications and large amount of data, SAN cannot be a good solution for small and medium sized companies [1], [8]. Figure 1 shows the basic components of SAN [35].

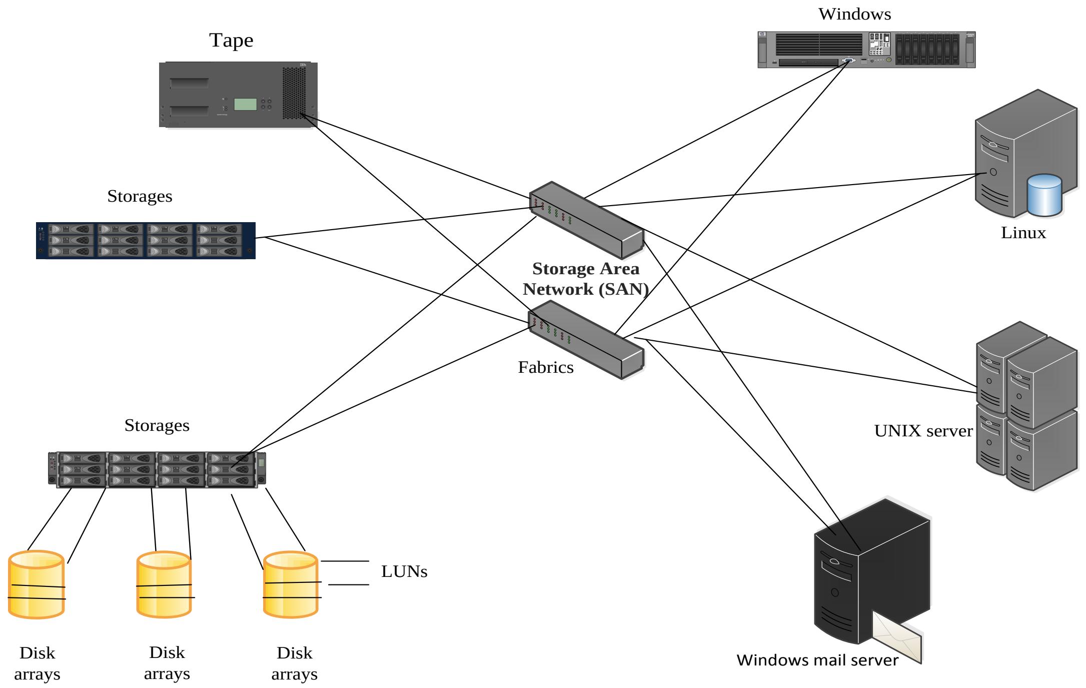


Fig 1-shows the SAN components [35]

DAS and NAS are other storage technologies for storing data as cheaper and simpler alternatives to SAN. SAN members such as servers and clients around the network need to access to same data at the same time, clustered file system is the technology that used for accessing of multiple servers to same data at the same time in SAN. Figure 2 show the architecture of SAN in network.

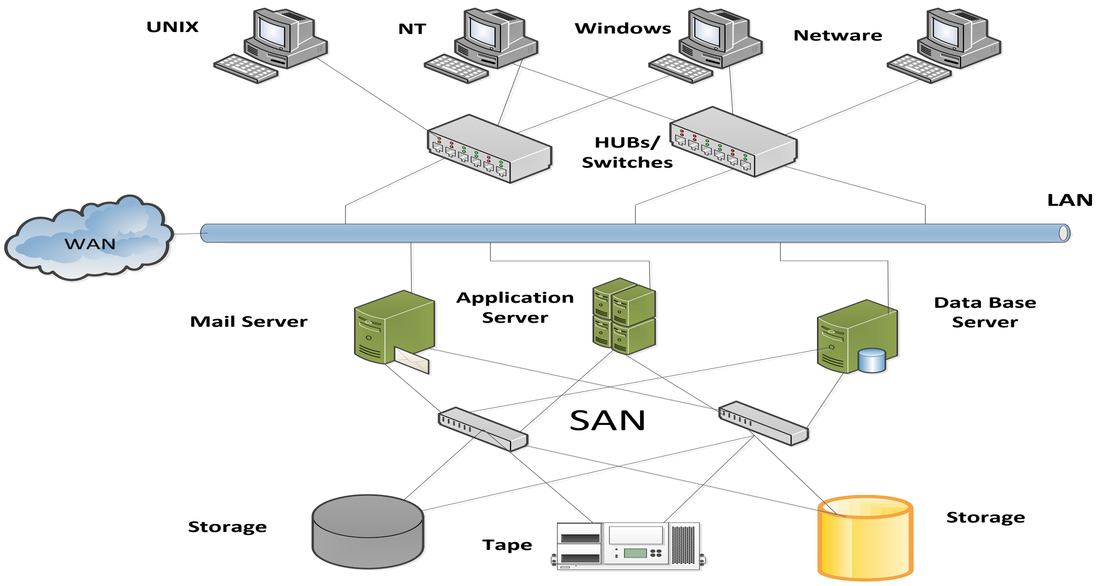


Fig 2- shows the architecture of the network that uses SAN.

2.1.2 SAN File System

A technique for handling of files is a part of each operating system and for this purpose it also controls the allocations on disk and has the task of creating and modifying the files and file directories. Each operating system uses its own file system, that each one of them has a different method and algorithm for allocating free space and creating and modifying files on disk. Clustering is the technology that used by file systems to improve the performance and traffic balancing on disks and improves the availability of the system. Cluster file system used in storage technologies e.g. SAN and NAS that needs to access the same data at the same time [11].

Each storage device that connects to a server or computer cannot do anything alone and thus it is the file system that makes the relation between disk blocks and operating system available to modify or create and changes any files on disks. Each file systems has table of information about the status of the disk blocks for managing and allocating disk blocks [12], [6], [2].

A SAN file system should enable any to any connection between all servers and all available disks in a SAN network. SAN in general is a shared disk technology and not a shared file system. All servers members of a SAN who connect to related shared disks should be able to modify and do changes to any files at any time without conflict with other server members work and it is not reachable with using of traditional file systems like File Allocation Table (FAT) and New Technology File System (NTFS) [13].

The cluster file system was developed to solve communication problem with disk blocks. A cluster file system is a combination of traditional file systems (e.g. FAT, NTFS) with the ability to multicast over the network for update the information about the changes that happened to other disks blocks to all the members in SAN by using the inter server connection between its members. The Cluster file system is aimed to work as a shared file system between servers in a SAN and is also known as a SAN file system (SFS). IF any node in a network fails or has functionality problem, other nodes on the network can continue their access to the blocks of data without any problem. Each file system consists of some basic elements e.g. super blocks, inodes and blocks of data. Super block has the task of keeping the information about control of the system and inodes keep information of individual files and data blocks also store the data of the files. File systems are located in core of each operating system to manage disk blocks allocation for different applications to share their resources with other applications [12], [6], [2], [14].

2.2 Storage Area Network protocols

A protocol is defined by a set of rules that enables the communication between two computers in any networks, communication between two devices from different vendors become capable by using protocol, because the protocol acts as the translator that all the devices talk to each other with the same language. There are several protocols for implementation of SAN, the common are internet Small Computer Interface (iSCSI) and Fibre Channel (FC).

2.2.1 Fibre Channel protocol (FC)

Fibre Channel (FC) Protocol maps the SCSI commands over FC. This protocol is primarily used for storage networking because FC can support the gigabit bandwidth speed on network. This protocol became a standard by an International Committee of Information Technology Standard (INCITS) and the American National Standard Institute (ANSI), the invention of FC was mainly for use in an industrial environment and then it became a standard, unlike the SCSI protocol that mainly developed as a standard. Some people refer to FC as the fibre version of the old SCSI technology [3]. FC started its work by being used in super computers and mainframes but because of the benefits of these standards, soon it became a popular standard in the SAN. FC supports two types of cables as a communication media, fibre optic and twisted pair cables [5], [3].

FC allows data to transfer in higher speed; the current available speed on FC is up to 16 GB/ Sec there are several products and vendors in the market currently using the high speed advantages of FC. FC is a multi-protocol support and it can carry the traffic from the other protocols as well [3].

SCSI was mainly developed for making connections between computers and the storage devices, as a good option for use in small scale networks. SCSI is used as a connection medium in DAS and carries and controls the blocks between the host and attached device. Use of SCSI had some limitations for the companies who wanted to use it as the communication protocol; these limitations confined growth of organization’s network in some aspects, scalability is one of the them, the other limitation in SCSI is low number of devices that can be serviced at the time, the maximum number of attached devices to bus topology can be support by SCSI is around fifteen, because of effecting to the performance of the system these number can be decrease to four or five. The other limitation on SCSI was the availability and reliability of the system. In SCSI, because of the large number of cables and connectors that are used for communication in the network, the probability of system failure is also high and any failure in the server or cables that connects to the storage devices can cause a system failure and lose the connectivity and data to applications. The other limitations of SCSI protocol is related to the speed and distance that can be supported by this protocol; the maximum of 25 meters long distance makes the SCSI protocol not a convenient solution for long distances. Device sharing in bus topology was also another problem [3].

FC becomes a popular model of SAN because of the limitations of the previous technologies. FC overcame the limitations of the I/ O speed, flexibility and Distance limit of traditional protocols, in SAN all hosts can see the storage like local attach disks to the system, multi-protocol support is another advantage of SAN. FC has two types of cables for using shorter and longer distances, fibre optic cable can manage the connectivity for the longer distances and copper cable is used for shorter distances and the characteristics of FC make it compatible with a wide variety of devices that support FC [5],[3].

By definition of the American National Standard Institute (ANSI) FC is a multilayer network protocol. Like other types of network protocol standards FC can send information in a packets or frames formats. The FC hardware allows the delivery of packets in high performance mode. To overcome the distance and speed limitation, FC protocol uses the serial transfer method instead of using the parallel one. There are two nodes playing roles in FC, source and destination, source is a device such as server, PC or mainframe and destination can be a disk or tape drive. FC protocol is the flexible protocol that can support a wide variety of devices and technologies [3], [5].

FC has the ability to deliver data as fast as the destination is capable to receive it. FC used a combination of traditional I/ O technologies with the benefits of networking and this combination makes the FC capable to transfer the large amount of data in high performance and speed. FC is a reliable protocol with the lowest error probability and has the ability to guarantee the data delivery from source node to destination. FC is a flexible protocol that can support different types of data e.g. audio and video. The number of devices that can be addressed by the FC is unlimited. FC with these capabilities and advantages, except implementation cost, can be a preferable option for implementing SAN in larger scale network [15], [5].

2.2.2 Fibre Channel Layers

FC consists of five layers and two sections, that each one of these layers has its own responsibilities. Figure 3 shows the layered architecture of the FC protocol.

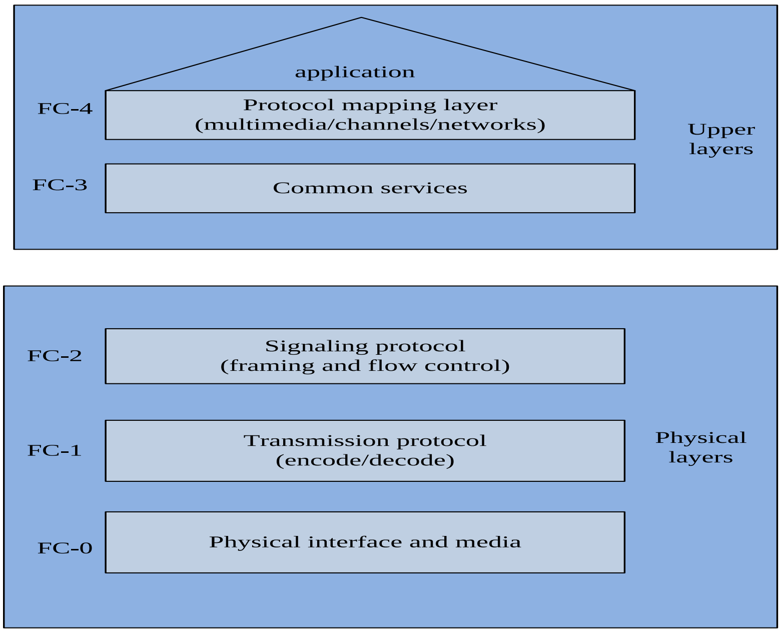


Fig. 3.FC protocol architecture that shows the different layers of FC protocol

According to figure 2, FC protocol divides into two sections, the upper layer and the lower one called physical layers, layer FC-0 known as physical interface, include the cabling elements and connectors and electrical parts. FC-1 known as transmission protocol, the task of this layer is to provide a method for reaching to the maximum length of the code. FC-2 is known as the signalling and framing protocol, the task of this layer is to provide a reliable communication and layer FC-2 is separate from the upper layer. These three layers together make the fibre channel, the signalling and physical interface. On the upper layer we have two other layers that start with FC-3 known as common services; the task of this layer is to function definition of single nodes. FC-4 is the last layer and known as the protocol mapping layer and the task of this layer is transporting of two different types of protocol over the same interface [5], [3].

Each FC frame has a limitation on data length that should be 528 words or 2112 bytes. For transmitting larger files FC divides them into several frames and then increasing the number of frames with growing the number of sequence and then makes the exchange. Figure 4 shows the architecture of the FC frame [3].

(SOF) 32 bit Start of frame	24 bit Destination port addres	24 bit Source port address	Control information words	Frame payload (0-2112 bytes)	CRC	EOF (end of frame)

Fig 4- FC frame architecture shows the different segments of each FC frame [3]

2.2.3 Naming Mechanism in FC

All nodes and ports that are used in FC SAN have a specific 64-bit address that used for their identification. Manufacturers assign this address to FC and when these addresses used internationally all around the world they become unique and called World-Wide Name (WWN), the address that assigns to port called worldwide port name (WWPN) and the address that assign to node known as World Wide Node Name (WWNN). Each WWN address consists of different parts, each part of the address contains different information, the name part represents the manufacturer, the other part of the address refers to address type and another part is assigned by the manufacturer to ports and nodes. Each WWN address is two hex digits like <07:33:11:54:65:00:D5:A0>. There are some other addressable devices such as disk drives, raid controller and logical drive, an 8 byte address has been assigned to them that are created by FC protocol known as logical Unit Number (LUN) that refers to specific drive [5].

2.2.4 Internet Small Computer System Interface (iSCSI)

The proposal of iSCSI protocol was developed in Internet Engineering Task Force (IETF) by IBM and Cisco. The first idea of this protocol was implementing a single network that based on IP for multipurpose tasks such as storage systems, data sharing, access to web services, mail services, voice and video [10].
Different elements of ISCSI SAN are summarised as follows:

Initiator: The initiator is software that is part of operating system for transferring the SCSI commands over the IP network from host to the target.

ISCSI target initiator: The target initiator is software that replies to requests from the host initiator.

I management: is a software that does the discovery of devices around the network and applies the policies and do some task on storages such as partitioning, mapping and volume management.

The iSCSI requests are encapsulated into TCP/ IP to transfer over the network. The iSCSI works on SCSI level 3 called SCSI-3. Mainly the iSCSI protocol works based on a client/ server model that in this model client known as initiator and server known as target. There are two types of transporting are exist in iSCSI, inbound and outbound, inbound mentioned to connection from initiator to target and outbound is mentioned to connection from target to initiator. Figure 5 shows the iSCSI packet format and it functionality [3], [33].

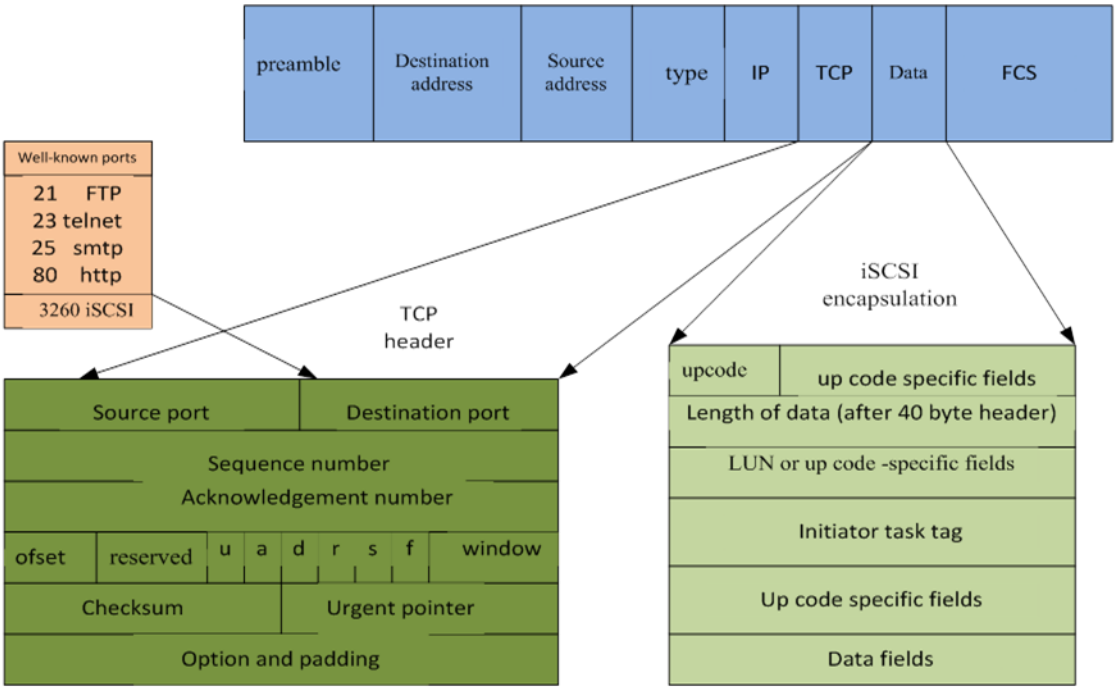


FIG 5-iSCSI packet format shows the architecture of the iSCSI packet [3]

The naming and discovery mechanism in iSCSI works with different methods, sending target commands to verify the iSCSI server is used in small networks and for larger network use iSNS server or Service Location Protocol (SLP) with ability of multicasting. Using iSCSI is very common in data centres for having the local access to storage pools also it is convenient for the situations that need to have a remote access to storages for doing the management of disks or backup and recovery of data [3].

The naming mechanism works based on identifier called World Wide Unique Identifier (WWUI) for identification of initiators and targets, WWUI is a part of iSCSI address, the format of this iSCSI address is (<IP address>:[<port no>]/ <WWUI>) IP address part can be IPV4 or IPV6 or a domain name, the port part can be TCP port number and WWUI part different for each device and it is unique and set by manufacturer [10].

The iSCSI protocol has some advantages in the connectivity of iSCSI devices, iSCSI support the wide variety of storage technologies such as SAN and DAS and make devices to work with LAN such as SAN and shared some devices with them. Support longer distance connectivity with the lower cost and has more availability and flexibility in implementation in comparison with FC SAN.

The availability of infrastructure in iSCSI is other advantages of this protocol; iSCSI works based on TCP/ IP protocol that most of the companies already have IP based infrastructure so there is no need to equip our network with new devices like FC switches that are expensive. The compatibility of devices that use TCP/ IP protocol in storage networks are more than FC.

The Backup task, control and manage by external server that manages backup plan with initiator that connects to the iSCSI target. Management of iSCSI devices is like direct attached SCSI devices and there are many IP based management software exists in IP network for control and monitor the traffic flow of storages. The cost of implementation is another subject that is lower than FC because of availability of the IP network devices such as switches, connectors and network cards for iSCSI, that already exist in most network infrastructure[10],[33]. Figure 6 shows the simple comparison between different SAN protocols and NAS.

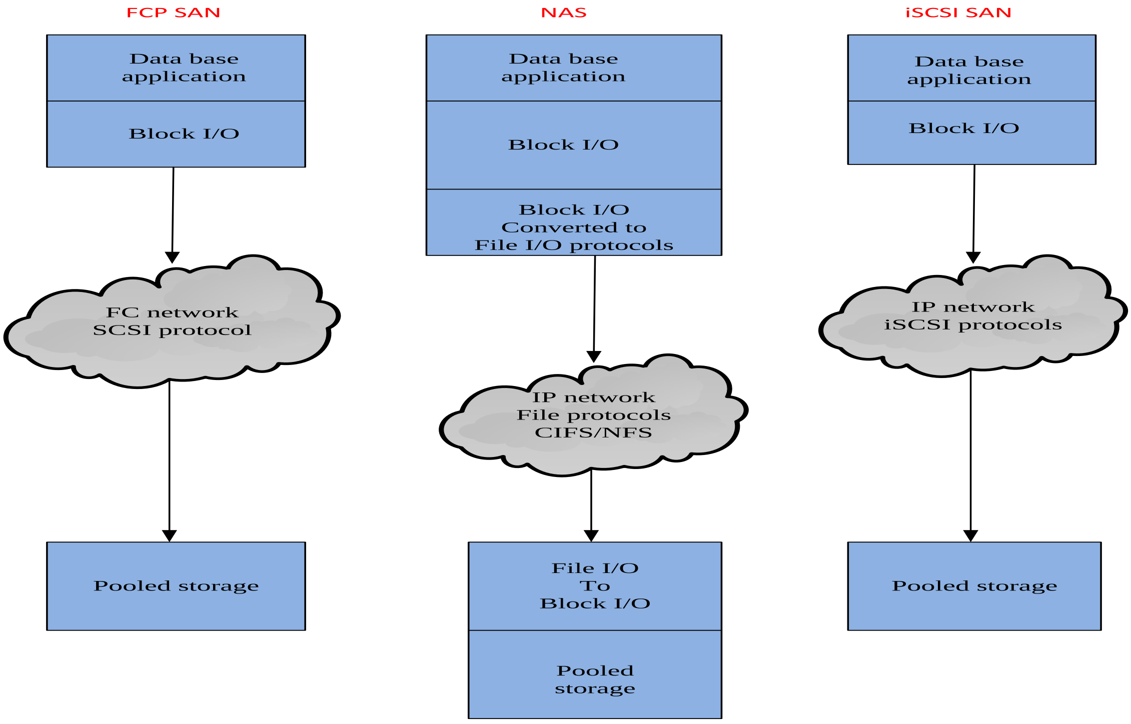


FIG 6-The simple comparison between different SAN protocols and NAS [10]

2.3 Internet protocol over fibre channel SAN

SAN use IP technologies to add some benefits to its features e.g. sharing and isolation become easier with the use of IP networks, allowing management and replication from the remote point and remote access to the devices for applying any configuration and changes to storage configuration. An IP network helps SAN to provide for lower cost and longer distance in comparison with FC with use of the benefits of both TCP/ IP and FC together [4], [5].

There are other protocols who work with SAN; these protocols are combination of iSCSI and FC. They use the speed and performance of FC and the flexibility of iSCSI together. These protocols are fibre channel over IP (FCIP), internet fibre channel protocol (iFCP) and ATA over Ethernet (AOE).

2.3.1 Fibre Channel over IP (FCIP)

This protocol use tunnelling for transferring packets over the TCP/ IP network. FCIP tunnels the fibre channel packets over the IP network and encapsulates the blocks of fibre channel packets to TCP/ IP socket. FCIP does not apply any changes to the packets and just encapsulates them to IP and then transmits them over TCP/ IP [3].

Tunnelling is a mechanism that allows a network to send data traffic of one network over another network. These mechanisms try to encapsulate protocols within packets to transmit them over the second network. Figure 7 shows the architecture of the FCIP [3].

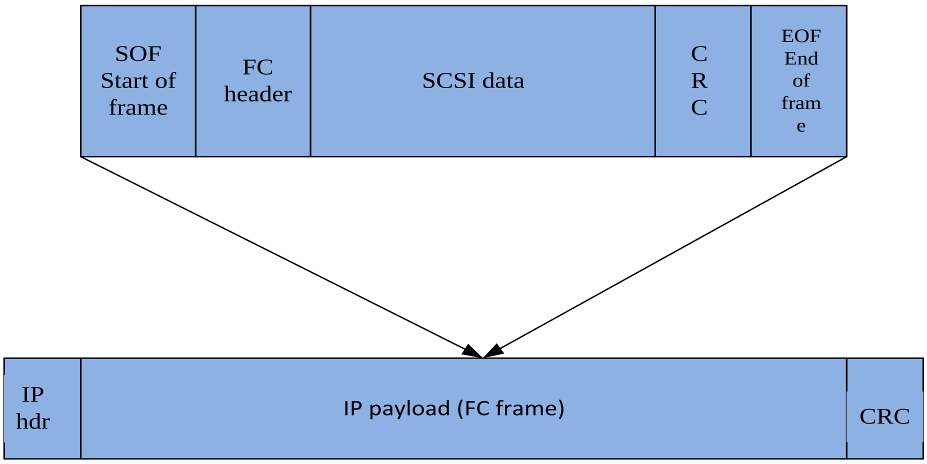


FIG 7.FCIP protocol architecture shows that the functionality of FCIP [3]

2.3.2 Internet Fibre Channel Protocol (iFCP)

IFCP also known as gateway to gateway protocol provides services of fibre channel devices from the fabric over IP. IFCP has several capabilities such as error detection, recovery and control the flow of the network data traffic through the TCP/ IP protocol. IFCP try to allow the connection between fibre channel devices over the IP based network and use mapping of FC header to the TCP. IFCP also use Internet Storage Name Services (iSNS) service as a naming discovery method. Figure 8 shows the architecture of the iFCP protocol [4],[5].

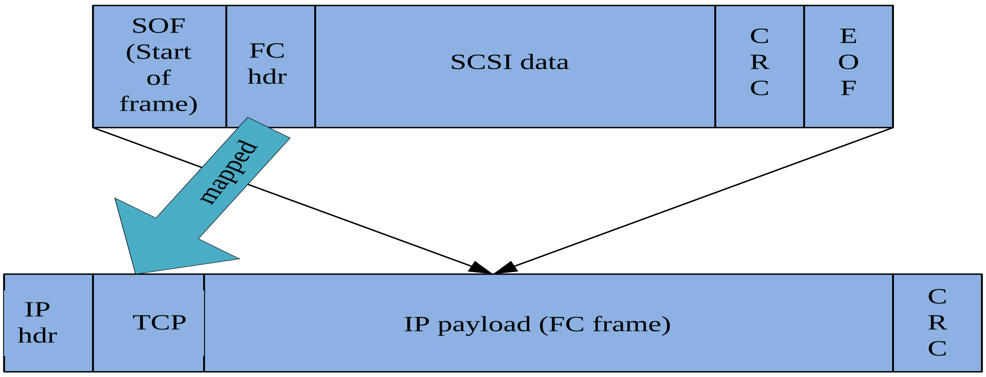


FIG 8-iFCP frame shows the functionality of the iFCP frame [4]

2.3.3 Internet Storage Name Services (iSNS)

ISNS is a name discovery service to implement on storage network and has the ability to discover, manage and configure the storage devices for both iSCSI and FC.

2.4 ATA over Ethernet (AOE)

AOE is another network protocol that has been developed by *(coraid)* company for providing simple and high performance access to storage devices over the data link layer; thus, this protocol cannot support any IP based routing protocol and services. AOE is not a complex protocol and it is easy to implement and configure, the cost of implementing the AOE is five to eight times less than the price of other storage protocols, in performance point of view AOE can be a good solution for virtualization of servers and storages. The AOE has some disadvantages that make this technology not popular in an enterprise network, the AOE is a single vendor protocol that it confine your implementation options, the AOE does not support the sequencing mechanism that makes differentiating between different request in Ethernet frames, this protocol does not support of retransmission for recovery or packet loss detection it also does not have any strong security mechanism for applying to network, the only supported security feature is the MAC address filtering that it can easily spoof and sniff by attackers [16],[17].

2.5 Fibre Optic Cables

The main communication device between source and destination in FC SAN is fibre optic cables. Fibre optic cables are made from a special kind of glass called silica that the thickness of them is like hair. Light is enters from one side of the fibre and exit from the other side. The maximum power that can be sent through a fibre optic cable is 0.5 watts. Fibre optic cables are available in two types, single mode and multi-mode. FC SAN can be implemented with both fibre optic and copper cables. Fibre optic cables are noiseless but the dust and dirt can effect on their functionality, in general fibre optic cables have better performance in compare with Ethernet cables [5], [9].

Multimode fibre optic cables are used for shorter distance and single mode used for longer distance. FC SAN work with both types of fibre optic cables. Fibre optic cables are working with short and long wave laser, shortwave laser is just works with multimode fibre optic and long wave laser can work with both types of fibre optic cables, single mode and Multimode. The core size of the Multimode cables is 50 and 62.5 micron and the core size of single mode cables is around 8.3 micron [9],[4].

2.5.1 Host Bus Adapter (HBA)

HBA is an network Interface that used to make connections between fabrics and storage in FC-based SAN. HBA converts the signals from parallel to serial and transmit it through the SAN. HBAs have one or more ports, choosing the right HBA vendor is an important task in implementing a SAN because some HBAs are not compatible with some SAN devices [3],[4].

2.6 Network Attached Storages (NAS)

NAS defined as the hard disk drive that is connected to the network. NAS consist of one or more hard disk in a bunch together. NAS is a shared storage that connects to the network and accessible directly over the local area network (LAN) by any of the users or servers that are attached to the network and it works like a file server that stores and shares the data over the network. The main function of a NAS is file sharing over the internet protocol (IP) network. Data can be sent or received over TCP/ IP protocol [36], [1].

NAS is working with file level access to data and support different operating system to share and access to files on shared storage. There are two protocols exist in implementing of NAS for making NAS compatible with different operating systems, Network File System (NFS) that belongs to UNIX operating system and Common Internet File System (CIFS) for windows operating system. Accessing to files in NAS is over the speed of Local Area Network (LAN), accessing to files is sometimes become impossible with some delays or bottlenecks in the network, companies need to use equipment with better performance and need to transfer larger amount of data such as rendering movies or online transactions they often switched from NAS to SAN. SAN is compatible with MAC, UNIX, LINUX and windows [36], [34], [1].

2.7 Direct Attached Storage (DAS)

DAS is a dedicated disk or any kind of storage device that connects directly to the host or server. DAS can be a good solution for small businesses that need a low cost solution to expand their storage capacity. DAS is not a network storage technology like SAN or NAS and uses point-to-point connectivity with server. The connection media in DAS can be fibre optic or SCSI connectors and the point-to-point topology is the simplest way of communication that exists in storage systems. Access to stored data on DAS is directly through the server; if for any reason the server shutting down or the power turns off, the applications and users who work with DAS do not have access to data. DAS also working with block level access to storages. DAS can be an economical solution for applications such as accounting, mail servers, or any kind of database program such as Microsoft SQL. There is some research about the comparison between different companies that use DAS and SAN technology as the storage technology and the results shows the one who used DAS, disk utilization was around 40% or less and those who used SAN was around 80%, so the disk utilization rate in a SAN is better than DAS. DAS is a cost effective solution but it is not scalable and if the amount of data is increase, it cannot be a good solution to handle the data traffic [8].

3 Storage Area Network security issues

Storing and availability of data is an important issue in IT world today. After investigating the architecture of SAN to see the functionality of SAN and type of file system and protocols used in SAN and what is the objectives of this technology in this chapter try to make an overview of security attacks and investigate about the defence method in SAN technology. SAN has some vulnerability that needs to verify, because of sensitivity of the stored data, storage administrators need to apply good security configuration on their network to achieve to highest level of security and availability of data.

SAN implemented on two protocols that we mentioned to them earlier, iSCSI and FC that both have their own security attacks and vulnerabilities. Security is not just doing one task or applying a customised security policy to the network, security like a chain that each one of the circles has especial responsibility for improving the security.

3.1 Storage Area Network access control

To increase the security level in SAN we need to verify the security risks and vulnerabilities of stored data and communications between SAN elements. Access control methods in the SAN are:

Authentication: used to identify the person, software or hardware to have permission for using system. Authentication doesn't exist by default in SAN. Most of the people who works with storages thought that security is exist somewhere else in the network and there is no need to be worried about security features in storages and new technologies such as SAN. Authentication is not inherently exist in SAN but through some other applications we can provide it to SAN such as SAN management software's and applications that have access to control SAN devices, some authentication models such as Diffie-Hellman-Challenge Handshake Protocol (DH-CHAP), Fibre Channel Authentication Protocol (FCAP) and Fibre Channel Security Protocol (FC-SP) provide security for different connection type such as switch-to-switch, node-to-node, node to switch connections [7].

Authorization: authorization is used for verifying level of access to devices in a SAN and it's provided by the WWN address of the node or port that known as WWNN and WWPN [7].

Encryption: encryption by default does not exist in most of storage devices, but it provide by using some third party applications but in general there is no encryption method exists in layer 0 to 4 in FC [7].

Availability: checking the availability of devices is same as QOS and exists in layer 2 of FC that known as error control on frames. Availability and ability of detecting and controlling errors is one of the essential tasks on implementing a SAN [7].

3.2 Fibre Channel Storage Area Network attacks

All communications in FC are transmitted in clear text mode; low level security and clear-text mode communication make SAN insecure and vulnerable with attacks. SAN does not have any encryption method on frame level but not having an encryption method is not a big problem because having encryption on frame level put load on a system and decrease the performance of the system. Lack of security and clear text communication method helps attackers to gain to information easier. The information in FC SAN that the attackers try to gain are mentioned as follows: [7]

- Domain identification
- Switch name server information
- sequence ID
- WWN (worldwide name)
- FC layer 2 frame information
- 24 bit address
- route information
- management information
- session control number

Hacking in SAN known as having unauthorized access to the information and stored data or access to management console of SAN. Common attack types in FC SAN are [7], [30]:

- session hijacking
- LUN masking attacks
- Man In The Middle Attack (MITM)
- name server pollution
- WWN spoofing
- zone hopping
- switch attack

There are some security weaknesses in different parts of FC SAN that increase vulnerabilities e.g. weakness in sequence is caused session hijacking attacks in SAN, weaknesses in fabric addresses cause MITM attack, weaknesses in Fabric Login (FLOGI) and Port Login (PLOGI) cause of name server pollution, weaknesses in HBA can be a cause of WWN spoofing and LUN masking attacks and weaknesses in FC switch fabric can be cause of zone hopping attack [7].

FC and IP based SAN have several mutual attacks that most of them are in layer 2 of FC known as frame and flow control layer and layers 2 and 3 in IP SAN that known as network and data layers. Layer 2 of FC contains 24 bit frame header that stores several main information about the frame that helps attackers to gain access to SAN easier. Figure 9 shows the content of 24 bit address.

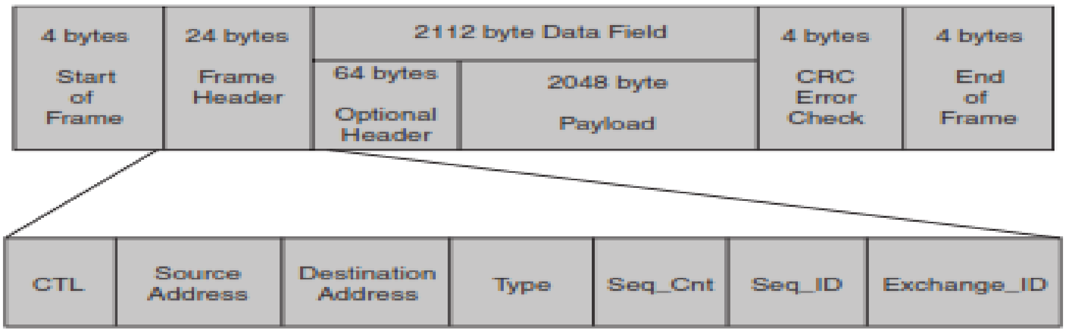


FIG.9-24 bit frame header architecture shows 24bit address [7]

3.2.1 Session hijacking attack

Accessing to the session between two trusted nodes by untrusted third party attacker to gain the control to connection among them known as session hijacking attack. Each session consist of two identification parts sequence ID and sequence Count, same responsibilities of these two elements also exist in FC known as Initial Sequence Number (ISN). Telnet can be one of these types of attacks. Session hijacking was first developed in IP base network because of weaknesses of ISN in TCP header but there are some types of session hijacking attack also exist in FC SAN because of low authentication method for verifying the participant or two nodes for having authorized access. Session hijacking attack happens because of the weaknesses in sequence. This attack has higher risk for the system and we can use the strong sequence ID and sequence Count in order to confine risk of this type of attack [7].

3.2.2 Address Weakness attack

Another attack in FC SAN that cause denial of service and damage system is because of weaknesses in 24 bit address, 24 bit fabric address used for routing between storage elements and use as SAN node information in name server that is kind of name database in SAN and use this 24 bit addresses to link to the 64 bit WWN address and check authorization between LUNs and WWNs for having access to them. The 24 bit address is an essential part of identification in some of the security methods in SAN such as hard and soft zoning, changing the 24 bit address effects on functionality of SAN and cause of denial of service [7],[30].

There are three types of login exist in FC SAN, Port Login (PLOGIN), Fabric Login (FLOGIN) and Node Login (NLOGIN). FLOGIN is the process that a node is log in to the fabric and PLOGIN is the process that the node registers the 24 bit address into the name server [30], [7].

3.2.3 Man-In-The-Middle attack

Man in the Middle Attack (MITM) is an attack that untrusted third party attackers try to intercept the communication between two trusted participants and direct it to wrong direction without awareness of the participants. In FC SAN this attack is used for spoofing the 24 bit address and nodes WWN. The risk level of this attack is low and in this attack unauthorized person or nodes try to gain the access to untrusted frames. MITM was introduced first in IP network and the probability of that in FC is lower than IP networks, security risk of this attack is lower in FC than iSCSI. In FC SAN for performing MITM attack, the malicious node needs to change the 24 bit address of itself to the address of the target to perform this attack. Most of the time MITM happens in PLOGIN session because of lack of authentication, also it happens when a name server wants to update its information, the malicious node send the fake PLOGIN frame information to the name server for registering 24 bit address of target to the WWN of the attackers. Improving security in MITM attack is a hard task and need to have a good knowledge of FC architecture, using strong authentication method in PLOGIN and FLOGIN can decrease the risk of this attack [7].

3.2.4 Name Server Pollution attack

In this attack, attacker try to corrupt the information on the name server and change them with the wrong information from the attacker node, when other nodes wants to communicate with target the traffic is redirect to the wrong address the malicious node, the attacker change its own 24 bit address information to the WWN of the target. The risk level of this attack is high because the attackers can gain to the sensitive data with this attack. Improving the security level for this attack is not a hard task and need to have a good knowledge on the FC protocol. The way that can improve the risk of this attack is to examine the PLOGIN frame when they want to update their information on the name server to do not let them to interfere and change the information tables on the name server [7].

3.3 Internet Small Computer System Interface attacks

The iSCSI SAN transfer SCSI commands over the IP networks, security risks on iSCSI SAN are same as IP networks plus the specific security attacks that specify to iSCSI SAN [20].

3.3.1 Man-in-the-middle Attack

To providing MITM attack, an attacker needs some information from architecture of the network. First step is to finding iSNS server address by using the third-party sniffing software to sniff TCP port 3205, after finding iSNS server address attacker try to replace the iSNS server address with the fake address to redirect all network traffic to the fake address, by doing this action attacker control registration requests from clients and targets and has the access to apply changes in domain sets and remove or change security policies and settings in authentication and encryption methods [7].

Authorization of iSCSI SAN does with initiator node name, the architecture of initiator node name shows in figure 10. Each part of the address is contains information about that node such as type, date, domain name and the host name. Information is transmitting in clear text mode; thus, the attackers can easily sniff and change them by using a network analyser tools by monitoring the traffic on TCP port 3260. This information can be used to gain access to iSCSI devices on the network [7], [30].

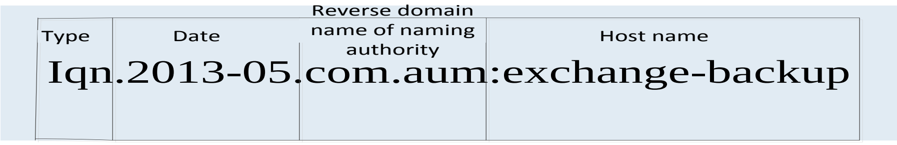

Type
Date
Reverse domain name of naming authority
Host name
Iqn.2013-05.com.aum:exchange-backup

FIG.10-initiator node name architecture [7]

3.3.2 Internet Simple Name Server Domain Hopping

Hopping attack in iSNS server is like VLAN or Zone hopping. IQN include domain and host name of the initiator, Attacker by knowing these information and change their IQN to the IQN of the target, cause the iSNS server update their information table with the wrong and spoofed data from the attacker and cause denial of service and gain to authorized access to sensitive information of organization [7].

3.3.3 Authentication Attack

Authentication on iSCSI devices is provides by CHAP protocol by using username and password for connecting to LUNs, CHAP is not used by default and is an optional feature. CHAP is not a secure method for authentication because it can sniff and spoof by using simple third-party tools to steal passwords and information of the network. Authentication attack try to sniff the packets on TCP port 3260 to gain to CHAP usernames and passwords by using sniffer tools and password dictionary to verify passwords and connect to the iSCSI SAN devices [30], [7].

3.4 Fibre Channel security solutions

Data that needs to be protected are divided into two types, Data in Flight (DIF) and Data at Rest (DAR). Data in flight mention to data and information that transmitted from source to target such as packets, Protocol Data Unit (PDU) protecting data during transmission known as data in flight security. Data at rest known as the security of stored data on disks such as encrypting the stored data or applying secure access to the stored data on disks[18].

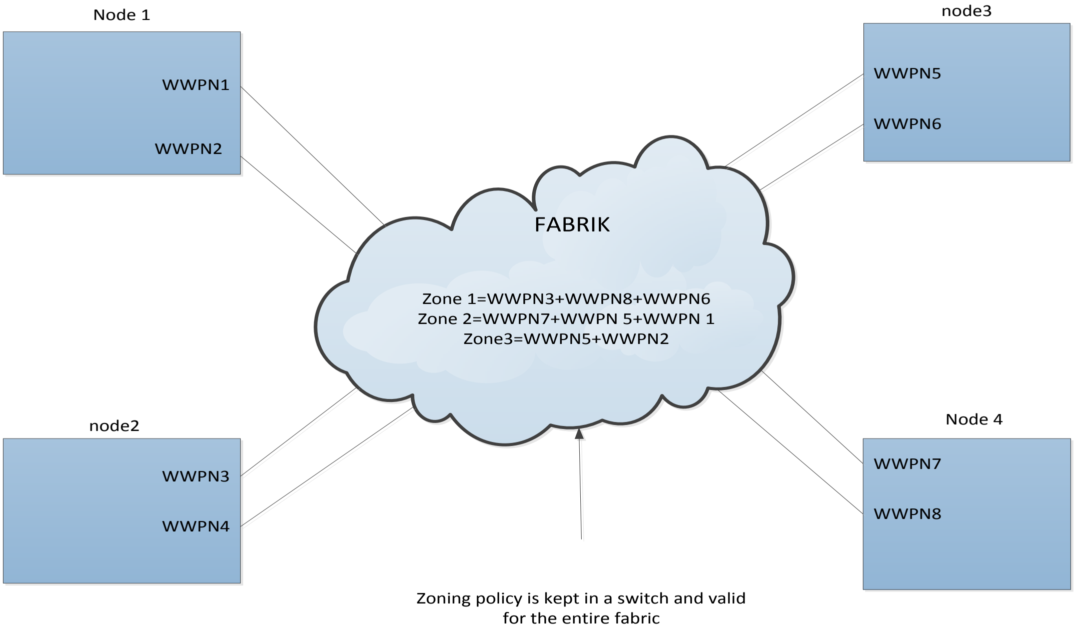
Data confidentiality known as guarantee the information from accessing by unauthorized persons and data integrity has responsibility of guarantee the stored data to do not apply any change or corruption after storing on disk [3].

The FC protocol has some authentication methods such as Switched Link Authentication Protocol (SLAP) and Fibre Channel Authentication Protocol (FCAP), SLAP is used to make trust area between switches that wants to connect to each other and FCAP is a public key infrastructure that used cryptographic authentication for making trusted area between switches and HBAs and do this task by exchanging the certificate between switches and fabrics [3].

3.4.1 Fibre Channel Zoning

Communication method in SAN is any to any, there is no limitation for devices in SAN to communicate with each other, by default there is not any security mechanism for controlling SAN devices access from other sources and other networks. The lack of security is one of drawbacks of SAN if it used in large scale networks from both security and access control aspects. Zoning is a mechanism for controlling the access from different sources by making zones and groups and assign them to devices and entities to organize their access to disks. Only the members of one zone have access to devices and not the members of other zones. Zoning defined on switch, each node can be access to devices if they allow by their WWNN or WWPN to that zone. Zoning can restrict the access to data that is more sensitive and control traffic flow through the fabric, error detection on fabric becomes faster and easier by using zoning. There are two types of zoning exist in switches, hard and soft zoning [5], [3].

Hard zoning apply zoning on port numbers or identifier on switches. Hard zoning is easier to implement and more secure than soft zoning, the problem of this method is policies that applied to physical port on switches, by changing or moving devices, the port needs to reconfigure and become a part of another zone, this can make a security problem on the network [7],[5]. Soft zoning also known as name server zoning and works based on the WWN address table in fabric and give access to nodes or ports by their WWNN or WWPN identifier. In soft zoning there is no need to reconfigure the settings with changing or moving the cables on fabrics, because they applied to the WWN identifier of nodes and ports, soft zoning cannot be a good method for applying security to the fabrics because WWN is vulnerable by spoofing attack and WWN are not unique and can be change by changing the HBAs or by the users [7], [30]. Figure 11 shows zoning mechanism in SAN [5].



Zoning policy is kept in a switch and valid for the entire fabric

FIG. 11 – this figure shows zoning mechanism in SAN to assigning different zone to different WWPN [5]

3.4.2 Logical Unit Number masking

Each disk divided into smaller parts that known as volume or partition, this volume on disks are identified in SAN with Logical Unit Number (LUN), masking generally implement on FC HBA, LUN masking make LUNs available by some host and unavailable by others [19].

The LUN masking can implement on software or hardware modes, hardware LUN masking are provides on routers, switches and controllers of disks and software LUN masking provides by coding that store on the computer who connects to SAN [4]. LUN masking limits or gives access of some ports to disks LUNs by their WWPN identifier. Figure 12 shows LUN masking mechanism in SAN [5].

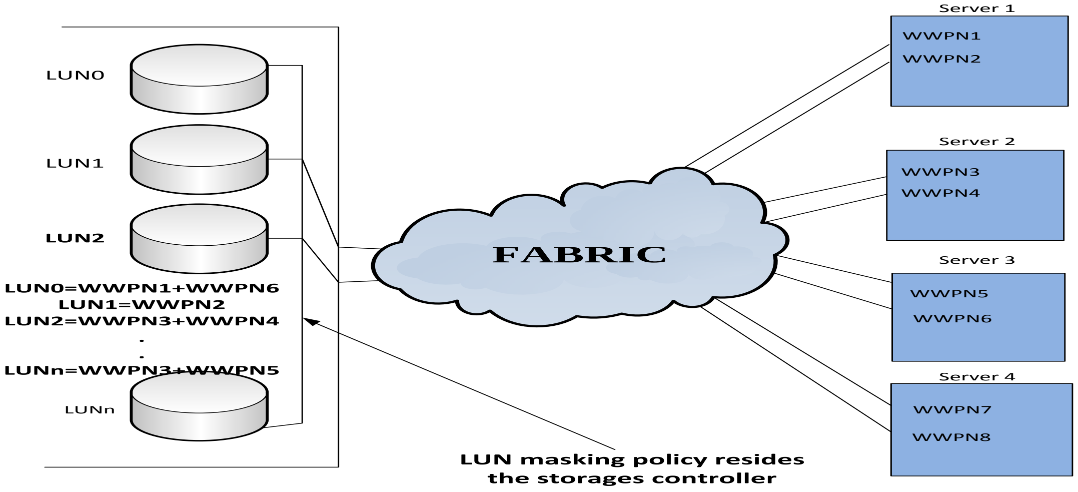


FIG.12 –this figure shows the architecture of LUN masking mechanism that allows specific WWPN to accessing to different LUNs [5].

3.4.3 Port Binding

Binding applies on switches and used to set permission for node and port access to fabrics, binding works based on WWN address. Binding applied on ports, switches or fabrics. On port binding each port that connected to the switch get a policy based on their WWPN and any change or replacement on fabrics needs to reconfigure policies. Binding on switches is works based on mapping of WWNN to switch, changing or swapping the cables does not need to rebuild the policy configurations. Fabric binding prevents access of unauthorized switches to the fabrics [5].

3.5 Internet Small Computer System Interface SAN security solutions

Authentication, authorization and encryption are three basic security elements in SAN, authentication in iSCSI SAN is provided by using Challenge Hand Shake Protocol (CHAP) for authorization control SAN used initiator node name and for encryption used IP Sec and Secure Socket Layer (SSL) [7], [20]. Most of SAN device vendors believe that SAN is not a vulnerable technology because it works on Gigabit Ethernet infrastructure and SAN is a point to point technology so attackers are not capable to snoop or hijack SAN easily and it just happen if they have physical access to SAN devices [7].

The iSCSI SAN has basic identification elements such as iSCSI Qualified Name (IQN), LUN and iSCSI Simple Name Services (iSNS) server. IQN is an identifier of iSCSI client's initiators that act like MAC address in Network Interface Card (NIC). The only available authorization method in iSCSI SAN is IQN that is not safe method; they are spoof able and sniff able and cannot be a good method for authorization. LUN is a logical part of storage devices, each storage devices is divided into several LUNs; LUNs works like partitioning the logical disk on desktop computers.

iSCSI works on TCP port 3260, ISNS server can be on any iSCSi devices or operating systems, each iSCSI initiator or target is registered in iSNS server. iSNS is responsible for informing clients about available iSCSI devices around the network and inform clients about different security settings that used in SAN for communicating with targets, iSNS server work on TCP port 3205 [30].security features that used in iSCSI SAN consist of:

3.5.1 Challenge Hand Shake protocol

For applying authentication in IP based storages such as iSCSI SAN, one of the commonly used method is CHAP, this protocol exist on iSCSI SAN devices. CHAP provides authentication between initiator and target by using encryption shared key. After the connection has been established between initiator and target, authorization rules apply to the initiator from the source. Classification of network traffic, also applying some management security method in SAN can be allowed by using CHAP. CHAP also classified the network traffic by using different classification methods e.g. IP address of the source, IQN and VLAN ID [4].

3.5.2 Remote Authentication Dial In User Services server

RADIUS server is another authentication method in SAN but currently it is not commonly used in IP based storage networks. RADIUS server is a remote authentication method for verifying the users who wants to use the network. RADIUS server works as a centralized server that managed accounting, authentication and authorization of the network users [4].

3.5.3 Kerberos V5 protocol

Kerberos is a mutual client/ server authentication protocol that provides cryptography by using shared secret key between client and server as trusted service. Kerberos protocol is used in windows logon process in windows based systems [39].

3.6 Results comparison

SAN like other storage technologies needs to pay attention to security of data and communication between devices in network. Configuration is the most important part of starting to build a secure network, testing and checking network configuration with network analysis tools to find out security holes and weaknesses in configuration of the network and apply the proper policies and security configuration to the network. There are some simple tasks that each network administrator must do to improve the security in iSCSI SAN networks such as using mutual authentication method instead of using one simple method like CHAP for authentication, enable the Cyclic Redundancy Check (CRC) for find out errors and use encryption methods such as IP Sec and SSL in both iSNS server and ISCSI devices if it is possible and does not decrease the performance of the system [7], [30]. Authentication on iSCSI devices is disabled by default and the only authentication method is CHAP also iSNS server does not have a good protection method and devices communicate with each other in clear text mode same as FC network [30].

The source of most of attacks in SAN are insiders, insider known as the people who work with SAN management console and storage devices, most of the attackers from outside target these management consoles because the majority of management consoles are working over TCP/ IP protocol and attackers are familiar with IP networks and their security holes. The most common attacks in SAN are internal attacks, the first step of improving SAN security is begun with insiders. Vulnerabilities from insiders are related to the contractors and authorized person who has access to work with SAN.

Control and defence of these types of attacks need to limit the responsibilities and access of the person who works with management devices and divide their responsibilities into different groups with different level of access. Using different username and password for each one of members with different level of access to the management console and devices, isolating the physical devices and servers if it is possible to separate them with other network devices and use access card and finger print at entrance. Control the system logs and activities of the administrators to verify changes and why these changes happened to the system and by whom [30].

4 Storage area network performance

4.1 Storage Area Network performance aspects

Whenever talk about performance in SAN it mentioned to some factors such as workload of the network bandwidth, capabilities of storages to handling data traffic, type of servers used in SAN, topology of the network, applications and configurations [38]. Solving the performance issues on storage networks such as taking too much response time of applications is always be an essential task of storage administrators, having better view of performance elements and characteristics of storages can help us to solve problems easier and in a shorter time. Collecting data and reports from management consoles can help to improve performance of the system [38]. Performance in every aspect of computer networks is always being critical and effects on functionality of the network. Traffic congestion in network is always happening because of poor network configuration or lack of good network settings that apply to the network that build on IP overhead and protocols that used in network topologies [21].

The throughput and bandwidth of the network is always an important factor of storage networks performance, monitoring the iSCSI traffic and find out the best connectivity and performance method in SAN devices is an important task of SAN administrator, most of the time simplest topology has the best performance [21].

4.1.1 Storage performance metrics

The performance metrics in area of storage consist of [40]:

- Throughput, known as transferred bytes through the network in specific portion of time in GB/ s or MB/ s.
- IOS, mentioned to the maximum amount of input or output of data in one second.
- Response time, mentioned to average time that needed for performing I/ O in millisecond.
- Cache read/ write, reading and writing data from cache to reduce the response time.
- Caches miss; perform I/ O by reading and writing data directly from disk.

The most important metrics in storage systems are throughput and response time. The throughputs of storage system are measured for storage partitions and volume such as LUNs, fibre channel ports, switches, storages and RAID arrays.

Storage performance divided into two main sections, front end and back end I/ O. front end I/ O related to the traffic among the servers and storages and back end I/ O related to the traffic among the cache of storage and disks [40].

4.1.2 Redundant Array of Independent Disks

Redundant Array Independent Disks (RAID) is a technology that helps to improve the reliability and performance in storages by using multiple disks and manage distribution of data. RAID can implement on both hardware and software models and the combination of these two. RAID has different levels from 1 to 6, each level of RAID has they own specifications and offers different features to use by storages. SAN also use RAID for implementation of SAN to have better performance and more reliability on storing and accessing to data and load balancing over the SAN network. RAID levels that are most common are RAID levels 0, 1 and 5. RAID 0 make the data striping over multiple disks, RAID 1 makes mirroring of data simultaneously among two disk, RAID 5 write data and parity simultaneously over multiple disks [4].

The best model of RAID is hybrid models that use the combination of two RAID type together to improve and increase the performance and reliability and access time to access the data, the common RAID models that used in SAN are RAID 10 (1+0) and RAID 50 (5+0) that use the advantages of two types together. RAID use the array of disks to apply mirroring and striping the data. Mirroring help to have a copy of data all the times and if one disk fail the other disk can handle the traffic and response to requests and system always up, using data striping can help the storage to make the trade-off between different disks [4].

4.2 Internet Small Computer System Interface SAN performance

The following tasks can improve the iSCSI SAN performance. Do not use iSCSI for applications that require using high speed network bandwidth, If it is possible assigns the dedicate LAN just for traffic that related to iSCSI devices and always use upgrade and update version of the iSCSI initiator, using the devices that supports the higher bandwidth such as 1 to 10 GB/ Sec network devices in your network architecture. Using CAT 6 cabling has better effect on speed of the network and performance. Separating subnet range of the network users from iSCSI traffic can be effective to improve performance on iSCSI SAN [21].

Another useful issue for performance improvement is using balanced network bandwidth, which means that use of equal or higher bandwidth between host initiators and targets and only assigns one or two storages to any NIC or HBA and put one of them as active and the other as standby. Using jumbo frame also can be a good idea for increasing the performance of the system, the normal frame size in IP networks is 1500 bytes with using jumbo frame we can increase it up to 9000 bytes in size and improve the throughput and performance of iSCSI network up to 50% more so it contains more iSCSI commands and frame payload than normal frame size also jumbo frame is a convenient solution for longer distance [21].

iSCSI SAN faced with some other problems as well such as performance of devices that works with Ethernet base servers and switches, in general these devices do not need high performance for sharing their facilities with others but if we want to implement a SAN in a larger scale networks these devices cannot handle traffic and over load of the networks and we should switch to high performance ones.

The other factor that effects on the performance of the iSCSI SAN is the initiator software type and version that used in our network for communication between storage devices, choosing the right software or hardware initiator can also effects on the performance of SAN. The current built in initiator software that used in operating systems are working well in general use but if the traffic overload goes higher and the network becomes larger with higher bandwidths and work load that is better to change the software initiator with the hardware one [22].

4.2.1 TCP Offload Engine (TOE)

Using some of security methods such as IPsec in SAN cause system face with bottlenecks and increase CPU usage and effects on system performance so TOE was invented to reduce the network load on the CPU and improve the service time and performance in NIC card in the network.

The idea of implementing TOE was about to increase the CPU performance with using the gigabit Ethernet connection as the network infrastructure for transferring the data, when data transfer over the network the CPU has to manage all the request that comes from different applications and users for accessing the stored data on disks, it makes CPU always busy with responding to requests and decrease the performance, TOE become as the solution by invent of iSCSI and used as the standard for transferring data over IP network to the block level of the storages, TOE was implemented as an option for reducing the load on CPU and performance improvement, the only problem that when we want to use the TOE NIC card in our network, is the cost, that sometimes is more than the FC HBAs that is not economical [26], [27].

4.2.2 Back up task performance in iSCSI SAN

Back up task on iSCSI network because of using current network infrastructure and transmit data traffic on current bandwidth of the network also effects on performance of the system and increase the response time to requests by applications, the idea for improving the backup task is using a network devices that supports Gigabit Ethernet in infrastructure of the network instead of using old fast Ethernet that is available up to 10 GB/ Sec [10].

4.2.3 Caching in Storage Area Network

To improve the security and performance in SAN, several methods have been proposed [32]. One example is cashing that has suggested using the log disk system and parts of the RAM to cache the traffic of iSCSI. This method is referred to as icache that aim to speed up the iSCSI transfer rate [32]. In fact, icache works simple and uses the small part of Non-Volatile RAM (NVRAM) and log disk for making caching in two levels for iSCSI requests. The functionality of this method can be divided into three steps, step one convert the requests that are small into the larger one before sending them to target storage in step two makes log structure utilized to speed up the process of write data for caching the data into log systems of the disk and by applying this method to the system can effect on improving the reliability and in last step cache both user and meta data into the log disk [32].

Icache is completely transparent to OS and there is no need to access to kernel of the OS and apply or update any changes to it. Icache by localizing the SCSI commands and hand shake operation help the system to reduce the traffic over the network and act like filter for storages to reject the amount of data request that cause to reduce the bandwidth and make system face with bottleneck because of the limitation of bandwidth and help system to improve the performance of iSCSI between 53 to 78% with using of this method [32].

4.3 Fibre channel performance

Fibre channel (FC) is a protocol that can provide flexibility in different network topologies with overcome to speed and distance limitation in high performance, FC provide availability and redundancy of storage. FC supports SAN topologies with large number of users. FC works with common transport media such as single and multimode fibre optic cables and high speed copper cables. FC is a reliable protocol that provides performance and scalability to cover the needs in SAN and reduce the number of error rates in network. FC support up to 5000 KM by using different cabling method, multimode fibre optic cable support up to 2 KM, single mode fibre optic cable support up to 10 KM and FC over IP can increase this distance up to 5000 KM [41].

According to the connection speed fibre channel divided into three models FC-base2, 10 and T [41]. FC-base 2 is the common model of fibre channel that used in fabric and Inter Switch Link (ISL) that used for inter connection between switches and also used in disk drives and support both types of cabling options fibre optic and copper. FC-base 10 normally used for making connection between switches ISL. FC-base T support only copper cabling such as cat 5e/ 6/ 6a and used RJ45 as a connector and user are capable to work with fibre channel without applying any changes in structure of the network or cabling [41].

Transfer speed in fibre channel is between 1 to 8 GB/ s and is the convenient option for using in both front end and back end devices in any network topology. Front end devices effects on performance and can apply some limitation to it. The average speed rate of FC in around 90% of the rated speed that means about 180 MB/ s for each FC port and this amount is between 50-85% for iSCSI that is around 50-85 MB/ s for each iSCSI link, the number FC back end devices also effects on I/ O and can makes it limited [41].

There are three different topologies for implementing FC, switched fabric, arbitrated loop and point-to-point. FC devices used 24 bit address space so switched fabric model can support up to 2^24 interconnect by switches, fibre channel devices identify to the fabric by their identification number that called WWN,WWNN and WWPN. Arbitrated loop can support up to 127connection in one shared loop and point-to-point topology just support two ports over dedicated link; figure 13 shows the different FC topology [41].

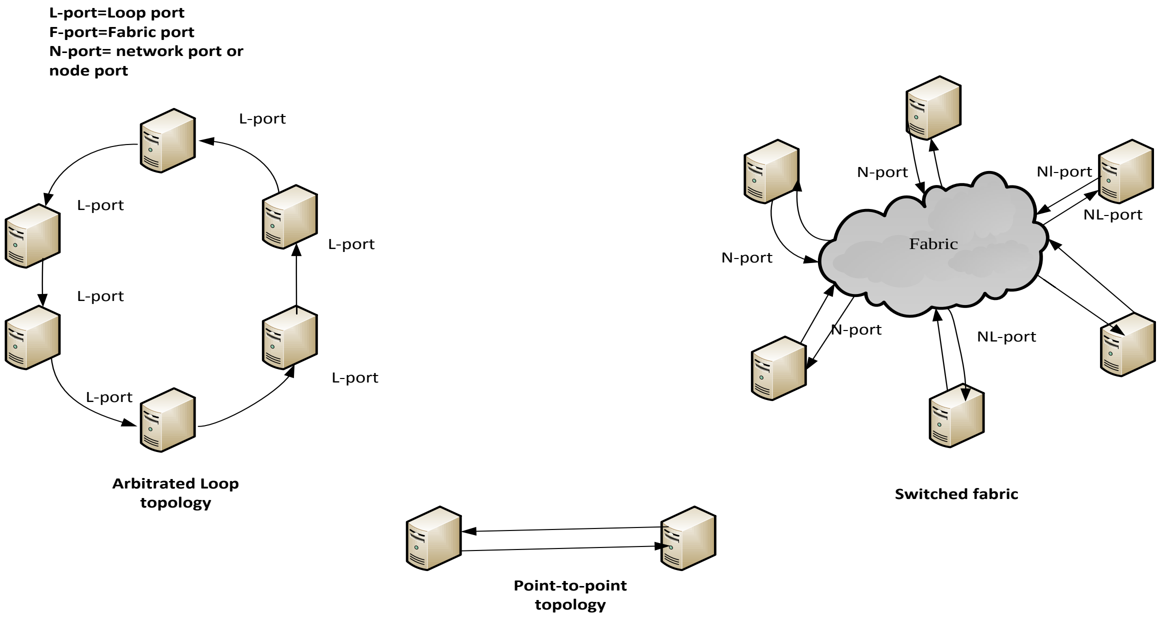


Figure 13-shows the different FC topologies

4.3.1 Performance comparison of SSL and IP Sec

IP storage networks like FC needs to use some security methods for applying security to storages and to the data that transfer in their network. Performance factors are important in storages and any security method wants to apply to them should be simple, compatible with the other elements, safe and cost effective in implementation. There are some securities and encryption method exist in IP network e.g. Secure Socket Layer (SSL) and Transport Layer Security (TLS) that works on the application layer and IP sec that work on network layer. Secure transferring of data from any host to the any targets or storages and then from the storages to the hosts [31].

IP Sec offer strong method of authentication and encryptions to transmitted data on IP packets, using encryption for large amount of data provides high CPU usage and put too much load performance to the system. This article compares SSL and IPsec on different condition of the network to see which one is more efficient than the other. Applying SSL v2 on the network decrease the performance of the system that this change is because of the need of SSL to generate source code for encryption, on the other condition they apply the IP Sec as the encryption method to the network and see delay of the network to respond to requests is more than SSL v2 and it shows that using the IP Sec as the security method can effect on the performance of the system and IP Sec first need to secure the packets and then transfer them though the network but in SSL security is implemented in the socket or ports level and then apply to the packets and has better performance than IP Sec [31].

4.4 Results comparison

The iSCSI and FC are both have equal abilities to work with storage systems and applications but most of the people who works with this technologies believe that using iSCSI have some limitations in comparison with FC to work with some applications, some of the applications have large Amount of transactions that IP-based infrastructure cannot handle the traffic of these applications like FC, iSCSI in comparison with other protocols has some limitations. The good thing when you design a SAN network is that your network should be capable of working with both available protocols and all the applications that used in your network can work on both iSCSI and FC, from experts points of view who works with storages the iSCSI SAN has higher performance than FC SAN [22].

In performance comparison between iSCSI and FC SAN most of the time, iSCSI is standing one level behind the FC, if iSCSI configures and implements properly can cover this gap and reduce the response time to a few milliseconds and can improve the functionality of iSCSI for using in larger networks [23].

Most of IT companies have to use both iSCSI and FC protocols for making connectivity between devices, to optimize their networks performance and their storage devices functionality, FC mostly use for working with applications, that need more bandwidth speed and higher performance and iSCSI use when the cost is an important issue and need to expand our storage network devices with lower cost [37].

For designing a solution for storage systems iSCSI can be a convenient option when manageability, connectivity and cost of implementation of the system are the key factors, on the other hand when you need performance and availability as your implementation requirements, FC can be a good model. FC is design for the business applications that needs more performance, such as SQL or exchange database and the iSCSI for files and departmental server use, most of the IT companies looking for the SAN solution that can handle the entire price, performance, reliability and the scalability of the system [37].

To providing a SAN over the 10 Gb/ Sec , iSCSI makes it available to use the high-speed and high performance devices over the IP infrastructure, use the low cost IP-based devices such as switches and routers are closely compete with FC in terms of performance, speed and cost [37], [38].

According to the research on the Storage Networking Industry Association (SNIA) that makes performance comparison between 4000 nodes which using SQL and using the both iSCSI and FC protocols shown that there is not much difference between the performance of the iSCSI and FC. Figure 14 shows the performance comparison between FC and iSCSI in working with SQL [24].

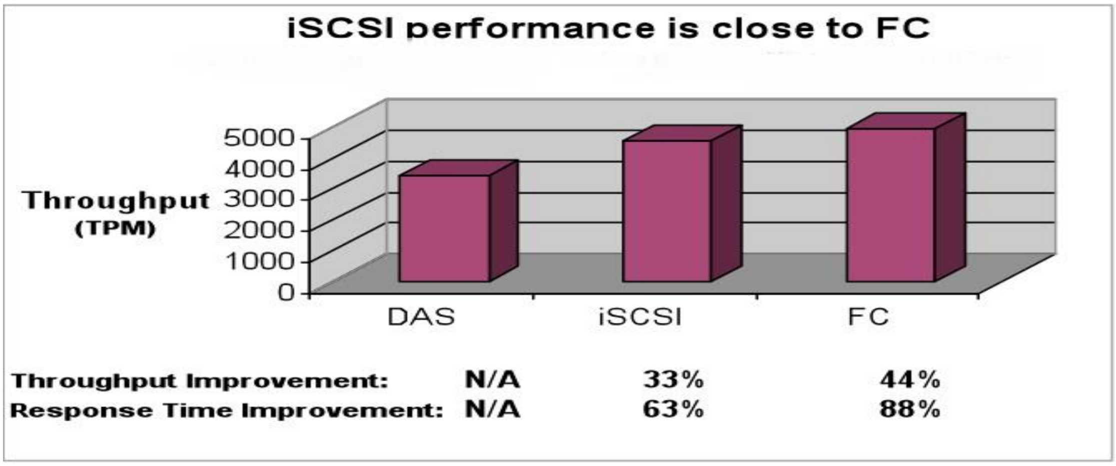


Fig.14-performance comparison between iSCSI and FC in different network that using SQL [24]

FC has the offensive addressing method and road map performance; it is more flexible and secure. iSCSI can easily grows in windows based networks that used SAN for their virtualization platform [24]. iSCSI can be a good solution for small and medium sized businesses (SMB) that more often cost is an important factor more than performance, speed of iSCSI reduce because of the limitation on the speed of the Ethernet LAN that is about 1 Gb/ Sec but the FC HBAs can support up to 4GB/ Sec Ethernet [25].

5 Conclusion

This thesis investigates about objectives of SAN such as:

- Architecture
- Networking
- File system
- Protocols
- Security aspects (vulnerabilities, attacks, defense method)
- Performance aspects

Architecture: the architecture of SAN is built to make the connection between servers and shared storages pool: fast, reliable, easy and secure.

Networking componets: SAN can be built on the use of fiber optic or gigabit Ethernet according to the SAN architecture and connectivity protocol. Other networking components of SAN are hubs, switches, directors, connectors, switches and routers.

File system: SAN use a clustered file system to respond to the requests for accessing the same data at the same time from different nodes. Other file systems such as FAT and NTFS cannot handle different requests at the same time.

Protocols: this thesis studied two protocols iSCSI and FC most commonly used for implementation of SAN and compared their functionality and security features in order to explore their advantages and disadvantages and their scalability.

Security and performance: this thesis investigate the security and performance of SAN and identifies the common attack types in SAN such as session hijacking, FC address weaknesses, man in the middle attack, sniffing and spoofing the data, zone hopping and switch attacks to find out effective solutions needed to improve the security of SAN networks.

Storage systems by their own do not have any security features; this lack of security makes storages vulnerable by different attacks. The best method to ensure security in SAN is the combination of authentication, authorization and encrypting data. Result also shows that the most vulnerable part of security in storages is insiders, people who have access to the storage devices and their management consoles.

Security solutions in iSCSI SAN consist of different authentication methods such as DH-CHAP, RADIUS server and Kerberos v5, the best result is when using the combination of these authentication methods with an encryption method such as IPsec. In FC SAN some specific security solutions exist such as using (hard or soft) zoning, LUN masking and port binding.

The result also shows some performance improvement methods in both iSCSI and FC such as using the latest OS version with updated software or hardware initiators for iSCSI devices or using compatible HBA for our FC devices, using NIC with TOE support for increasing the CPU performance of the system when using encryption methods such as IPsec, separating the network traffic with iSCSI traffic can also be an issue to improve the performance of the system.

Implementation the model of iSCSI SAN in order to have deeper understanding of functionality of iSCSI SAN technology and its security vulnerabilities and Performance in SAN also another part of this work discussed in the study.

Knowing the security and performance features of these protocols can help the storage administrators to have better configuration on their network with the respect to performance. Security is not a single task that can do just by single configuration; security is like a chain that all the circles in this chain are needed to be connected to each other. This work can be helpful for the people who want to start working with SAN technology to have better understanding that how it works and what are security risks and their solutions to improve these vulnerabilities on SAN and about the performance aspects. Knowing this information can help the storage administrators to make decisions related to trade-off between security and performance in their network. The results of this investigation shows that SAN is a convenient data storing solution when availability, data sharing, speed of transferring data and security are main goals.

As the future works, I aim at combining the security features in order to increase the security level of the system and searching to enhance the performance of the security technology in the storage devices.

6 References

[1] T. Clark, designing storage area network, second edition. Addison wesley, 2003.

[2] C. Brooks, H. Dachuan, D.jackson, M. A.miller, and M. Rosichini, IBM total storage SAN filesystem, Fourth edition. IBM, 2006.

[3] J.Tate, F.Lucchese, and R. moore, Introduction to Storage Area Networks, Fourth edition. IBM, 2006.

[4] J. Tate, P. beck, I.Hector hugo, K.Shunmugarathan, and L. Miklas, Introduction to Storage Area Networks and System Networking, Fifth edition. United States, IBM, 2012.

[5] G. Geiselhart, R. Brennman, T. Gutenberger, J. Lafitte, W. Ventura, and S. Williams, Linux for Zseries fiber channel protocol implementation guide, first. IBM, 2004.

[6] G.Silberschatz, Operating System concepts, chapter 17 Distributed file systems. Addison-Wesley Publishing Company, ISBN 0-201-59292-4`,1994.

[7] H. Dwivedi, Securing storage: A practical guide to SAN and NAS security, First edition. 2012.

[8] C. Poelker and A.Nikitin, Storage area network for dummies, Second. Wiley, 2009.

[9] U. Troppens, R.Erken, and W. Muller, Storage networks explained. Wiley, 2004.

[10] R. Hernandez, k. Carmichael, D.Malen, B.Moore, G. lane, and j.Earhart, Using iSCSI solution planning and implementation, First. IBM, 2002.

[11] H.M.Abdol-wahab , Old dominain university,2012, File system implementation, http:/ / www.cs.odu.edu/ .

[12] The Storage Networking Industry Association, understanding storage area network, 2002, http:/ / www.snia.org.

[13] Microsoft tech net, chapter 10 disk and file system architectures, http:/ / technet.microsoft.com.

[14] Disk management and file system interface, M.Nesterenko Computer Science Department Kent State University, spring 1999, http:/ / vega.cs.kent.edu.

[15] Fibre channel industry association, Fibre Channel Features, San Francisco, Chris Lyon, 2012, http:/ / www.fibrechannel.org/ .

[16] Search networking, ATA over Ethernet for converged data centre networks, I.Peplnjak, September 2010, http:/ / searchnetworking.techtarget.com.

[17] “iSCSI vs. fibre channel SAN, white paper, coraid, april 2011, http:/ / www.horoa.net/ .

[18] SAN and storage solutions and managements, Approaches encryption data at rest enterprise White paper, R.Dhorma, V.Venugopal, S.Sake, V.Dinh, 2011, http:/ / www.emc.com/ .

[19] SAN security, Storage area network (SAN) security FAQ, Network System Architects, Inc. 2010, http:/ / www.sansecurity.com/ .

[20] H-Yi, T., et al. Performance study of software-based iSCSI security. Security in Storage Workshop, Proceedings, First International IEEE, 2002.

[21] EMC best practice for performance and availability of storages, Whitepaper, Corporate Headquarters, march 2011, http:/ / www.emc.com.

[22] iSCSI vs. fibre channel explained , fibre channel takes rightful place beside fibre channel, S.J.Bigelow, 13 July 2007, http:/ / www.cuttedge.com.

[23] Fibre Channel vs. iSCSI: The war continues, M.Prigges, 12 July 2010, http:/ / www.infoworld.com.

[24] D.Dale,Net App, Benefits of networked storages, Storage consolidation with IP storage, 2007, www.snia.org.

[25] Comparison between SCSI over IP and FC over Ethernet, Whitepaper, CISCO system, 2009, http:/ / www.cisco.com.

[26] Network work research centre, TCP offload engine (TOE), network buzz issue, 2009, http:/ / www.networkworld.com/ .

[27] TCP/ IP offload engine (TOE), M.Rose , October 2008, http:/ / searchnetworking.techtarget.com.

[28] Open filer information and configuration, G.Porter, December 2010, http:/ / greg.porter.name/ wiki/ .

[29] Open filer introduction and standard installation method, graphical installation, 2013, http:/ / www.openfiler.com/ .

[30] ISCSI Security (Insecure SCSI), H.Dwivedi, Fall 2005, https:/ / www.blackhat.com/ .

[31] First International Conference on Networks & Communications, securing internet protocol (IP) storage (case study), SIVA RAMA KRISHNAN SOMAYAJI, Ch.A.S MURTY,2009.

[32] A Caching Strategy to Improve iSCSI Performance, Xubin He, Qing Yang, and Ming Zhang, University of Rhode Island, National Science Foundation under grants,2002, ISBN: 0-7695-1591-6 .

[33] J. Satran, et al., iSCSI draft standard, RFC 3720, 2001, http:/ / www.ietf.org/ .

[34] J. Katcher, Post Mark A New File System Benchmark, Network Appliance Technical Report TR3022,1999.

[35] All San storage area network solutions, 2001, www.allsan.com.

[36] M.lovelace, V.Boucher, S. Nayak, C. Neal, L. Razmuk, J. Sing, and J.Tarella, IBM scale out network attached storage, architecture planning and implementation basics, First IBM, 2010.

[37] iSCSI vs. FC SANs ,three reasons not choose sides, position paper, November 2010, http:/ / www.davenportgroup.com/ .

[38] K.Orlando, D.Frueh, P. D'angelo, L. Dean, SAN storage performance management using tivoli storage productivity center., Third. IBM, 2011.

[39] iSCSI security: Networking and security options, M.Taylor, June 2012, www.computerweekly.com.

[40] Storage performance, R. Lucchsi, 2008 , Network Industry Association (SNIA), www.snia.org.

[41] Fibre channel technologies "current and future", Dr.M.K jibbe, LSIcorporation (ESG), T. Hammond-Doel (ESG), Steven Wilson (brocade) 2007, Network Industry Association (SNIA), www.snia.org.

7 Appendix

iSCSI SAN experiment

Openfiler works on Linux kernel. Filer in general related to the servers that dedicated to storage devices. After running and installing the openfiler on the virtual machine, it works on two modes, web based GUI and CLI mode, it can be used for implementing both SAN and NAS by supporting of file level access protocols e.g. NFS and CIFS that the protocols used in NAS and block level access protocols for ISCSI and FC protocols that use in SAN environment [28].

In this scenario I implement the iSCSI SAN, with two LUNs to allocate to the users and servers all around the network. The number of LUNs is up to the network administrators and main disk capacity, there is no limitation for defining more LUNs. I define two LUNS in different capacity just to see the functionality of the SAN to see how it looks like to the operating system. During or after the installation we can define hard disk partitions that later want to makes them as the LUN.

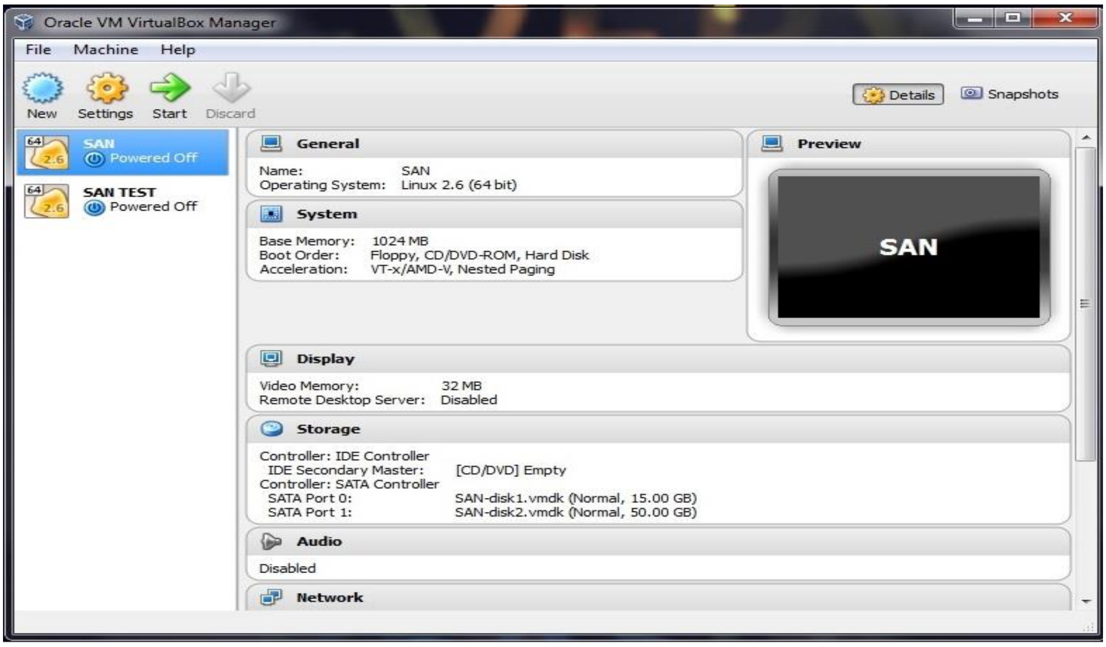
Storage by default does not use any specific types of security so it is easy to access to LUNs from any operating system initiator and searching the network for available IQN of the LUNs to make connections with them. The only available method for using to apply security on disks is the CHAP protocol. By using CHAP we can set password for making connections to LUNs.

CHAP is not a strong security method for using in storages and it is easy to sniff by the monitoring software. One the famous network monitoring software that we use to monitor our network traffic from on different ports is wireshark.

Wirshark is a free network monitoring tools that you can use to monitor the traffic fellow on different protocols and ports on your network. Another security method that we can apply to our network for increasing the security level of our network is IP sec that is an encryption method for using on IP based storage network. The disadvantages of using the IP sec is the overload on CPU that we need to use the NIC card to reduce the CPU load of the system.

The first step is installing the open filer ISO file in virtual machine figure 15 shows the virtual box virtual machine. The hardware requirements for installing open filer are [29].

- X86 or x64 based computer with at least 512MB RAM and 1GB storage for the OS image.
- At least one supported network interface card.
- A CDROM or DVD-ROM drives if you are performing a local install.
- A supported disk controller with data drives attached.



Name: SAN
Operating System: Linux 2.6 (64 bit)

Base Memory: 1024 MB
Boot Order: Floppy, CD/DVD-ROM, Hard Disk
Acceleration: VT-x/AMD-V, Nested Paging

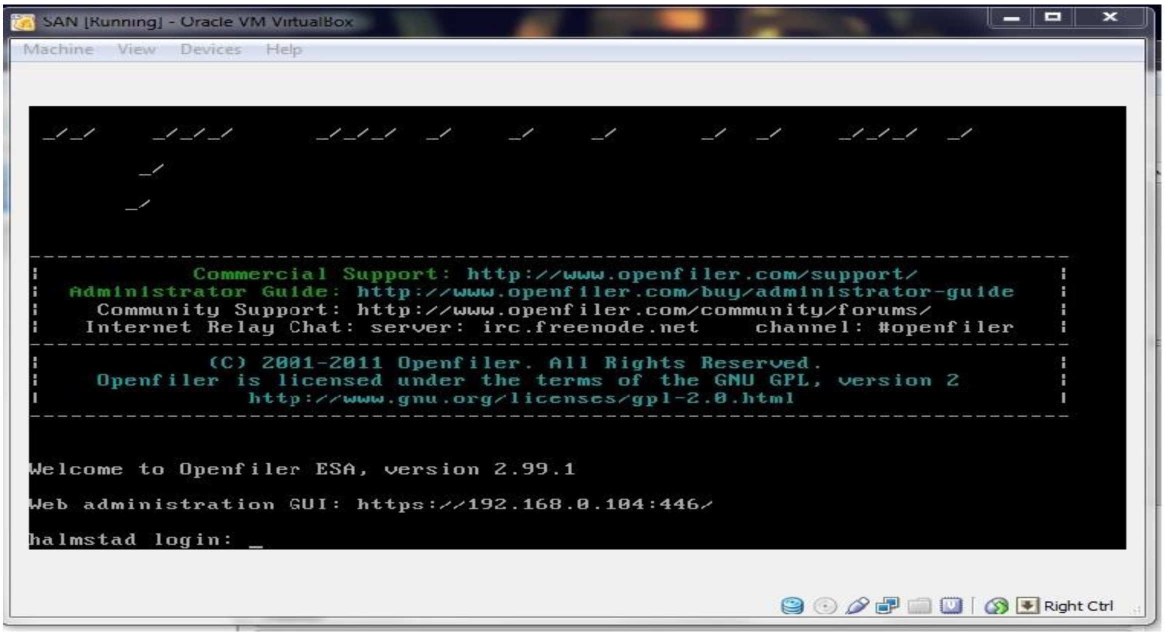
Video Memory: 32 MB
Remote Desktop Server: Disabled

Controller: IDE Controller
IDE Secondary Master: [CD/DVD] Empty
Controller: SATA Controller
SATA Port 0: SAN-disk1.vmdk (Normal, 15.00 GB)
SATA Port 1: SAN-disk2.vmdk (Normal, 50.00 GB)

Disabled

FIG.15-virtualbox VM interface

During the installation it asked some questions e.g. time, location and root partition to install kernel, network configuration that can be dynamic through the DHCP or static (manually). After this step installation of open filer is begin. After install and reboot the system the open filer get an IP address from DHCP and gives us two options for entering the management console through the Command line (Figure 16 shows the command line controller of openfiler) or from the web based management console that works on HTTPS with port no 446 (Figure 17 shows the web controller console of openfiler) [29],[28

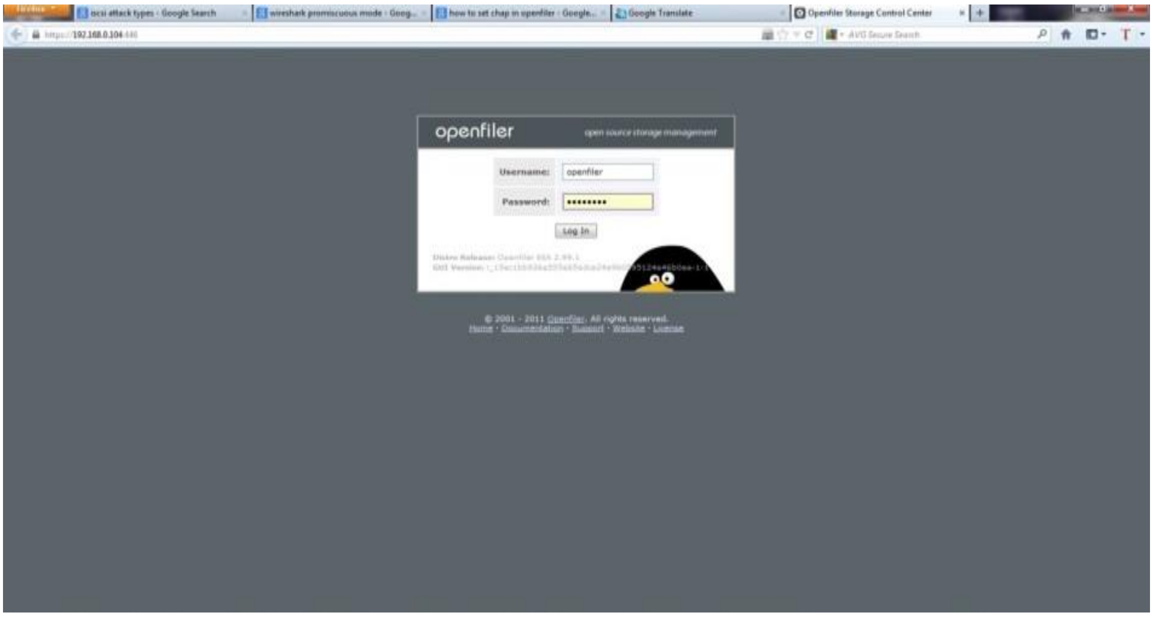


```
-----------------------------------------------------------------------------
|          Commercial Support: http://www.openfiler.com/support/           |
|   Administrator Guide: http://www.openfiler.com/buy/administrator-guide  |
|     Community Support: http://www.openfiler.com/community/forums/        |
|    Internet Relay Chat: server: irc.freenode.net    channel: #openfiler  |
-----------------------------------------------------------------------------
|              (C) 2001-2011 Openfiler. All Rights Reserved.               |
|     Openfiler is licensed under the terms of the GNU GPL, version 2      |
|                 http://www.gnu.org/licenses/gpl-2.0.html                 |
-----------------------------------------------------------------------------


Welcome to Openfiler ESA, version 2.99.1

Web administration GUI: https://192.168.0.104:446/

halmstad login: _
```

FIG.16-command line interface (CLI) login page of openfiler

We don’t need to use the command line interface because all the configurations are done though GUI web Interface. That we easily access to the console by this address (https:/ / Domain.name:446).

The default username and password that use to access to web console is:
Username: openfiler
Password: password

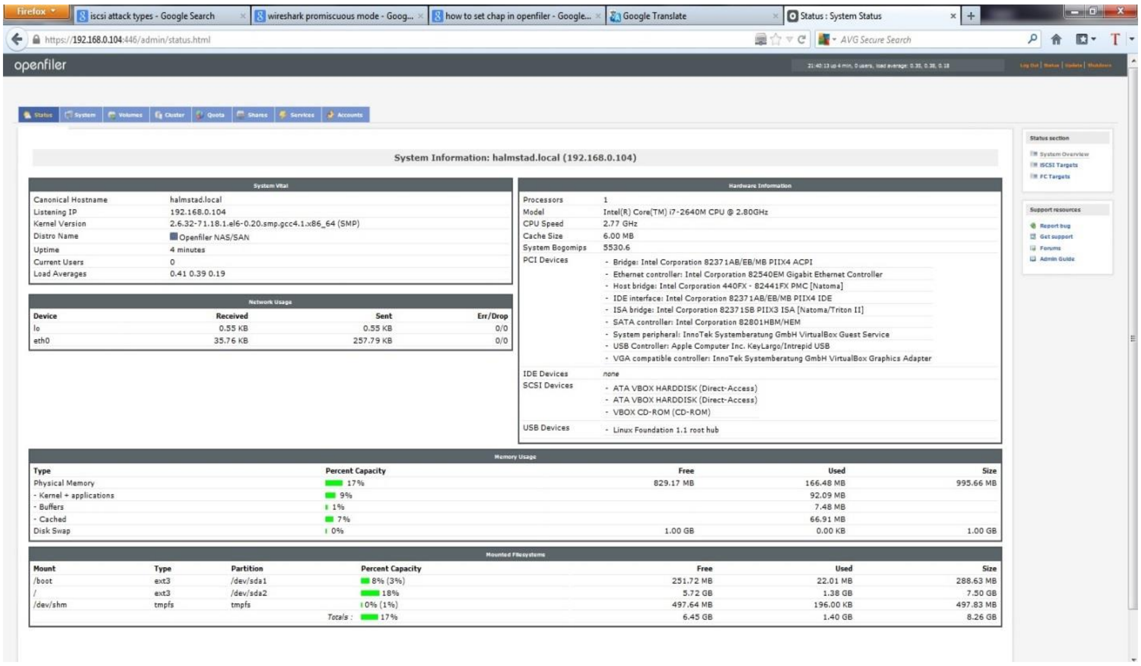


iscsi attack types - Google Search
wireshark promiscuous mode - Goog...
how to set chap in openfiler - Google...
Google Translate
Openfiler Storage Control Center
https://192.168.0.104:446
AVG Secure Search
openfiler
open source storage management
Log In
© 2001 - 2011 Openfiler. All rights reserved.
Home · Documentation · Support · Website · License

Username: openfiler
Password: •••••••••

FIG.17-web access login page to openfiler console

After login into the management console the main page (Figure 18 shows the status page of the system) includes the basic details and tables that show the system information on the status tab e.g. System vital that shows the host name and the IP address of the host, the kernel version of the OS and up time of the system. The next box is including the hardware information of the system and number of hard disks and network adapter that attached to the system. The network and memory usage boxes also show the status of usage of memory and network.


Firefox
iscsi attack types - Google Search
wireshark promiscuous mode - Goog...
how to set chap in openfiler - Google...
Google Translate
Status : System Status
https://192.168.0.104:446/admin/status.html
AVG Secure Search
openfiler
21:40:13 up 4 min, 0 users, load average: 0.35, 0.38, 0.18
Log Out | Status | Update | Shutdown
Status
System
Volumes
Cluster
Quota
Shares
Services
Accounts
Status section
System Overview
iSCSI Targets
FC Targets
Support resources
Report bug
Get support
Forums
Admin Guide

System Information: halmstad.local (192.168.0.104)

System Vital

Canonical Hostname	halmstad.local
Listening IP	192.168.0.104
Kernel Version	2.6.32-71.18.1.el6-0.20.smp.gcc4.1.x86_64 (SMP)
Distro Name	Openfiler NAS/SAN
Uptime	4 minutes
Current Users	0
Load Averages	0.41 0.39 0.19

Network Usage

Device	Received	Sent	Err/Drop
lo	0.55 KB	0.55 KB	0/0
eth0	35.76 KB	257.79 KB	0/0

Hardware Information

Processors	1
Model	Intel(R) Core(TM) i7-2640M CPU @ 2.80GHz
CPU Speed	2.77 GHz
Cache Size	6.00 MB
System Bogomips	5530.6
PCI Devices	- Bridge: Intel Corporation 82371AB/EB/MB PIIX4 ACPI - Ethernet controller: Intel Corporation 82540EM Gigabit Ethernet Controller - Host bridge: Intel Corporation 440FX - 82441FX PMC [Natoma] - IDE interface: Intel Corporation 82371AB/EB/MB PIIX4 IDE - ISA bridge: Intel Corporation 82371SB PIIX3 ISA [Natoma/Triton II] - SATA controller: Intel Corporation 82801HBM/HEM - System peripheral: InnoTek Systemberatung GmbH VirtualBox Guest Service - USB Controller: Apple Computer Inc. KeyLargo/Intrepid USB - VGA compatible controller: InnoTek Systemberatung GmbH VirtualBox Graphics Adapter
IDE Devices	*none*
SCSI Devices	- ATA VBOX HARDDISK (Direct-Access) - ATA VBOX HARDDISK (Direct-Access) - VBOX CD-ROM (CD-ROM)
USB Devices	- Linux Foundation 1.1 root hub

Memory Usage

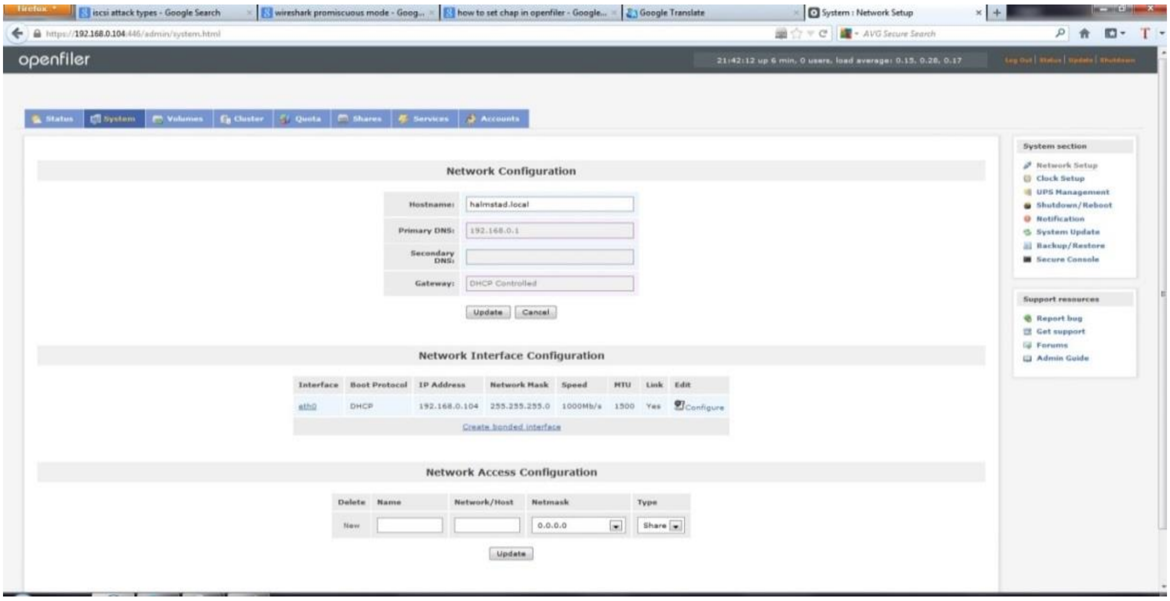
Type	Percent Capacity	Free	Used	Size
Physical Memory	17%	829.17 MB	166.48 MB	995.66 MB
- Kernel + applications	9%		92.09 MB	
- Buffers	1%		7.48 MB	
- Cached	7%		66.91 MB	
Disk Swap	0%	1.00 GB	0.00 KB	1.00 GB

Mounted Filesystems

Mount	Type	Partition	Percent Capacity	Free	Used	Size
/boot	ext3	/dev/sda1	8% (3%)	251.72 MB	22.01 MB	288.63 MB
/	ext3	/dev/sda2	18%	5.72 GB	1.38 GB	7.50 GB
/dev/shm	tmpfs	tmpfs	0% (1%)	497.64 MB	196.00 KB	497.83 MB
		Totals :	17%	6.45 GB	1.40 GB	8.26 GB

FIG.18-openfiler system status page that shows the status and performance of the system

Next image related to the system tab that we can do the host and IP configuration on Openfiler and define or change the IP address or host and make an access list for signing in as a specific user to have an access to system. Figure 19 shows the network configuration of the system.



Network Configuration

Hostname: halmstad.local
Primary DNS: 192.168.0.1
Secondary DNS:
Gateway: DHCP Controlled

Network Interface Configuration

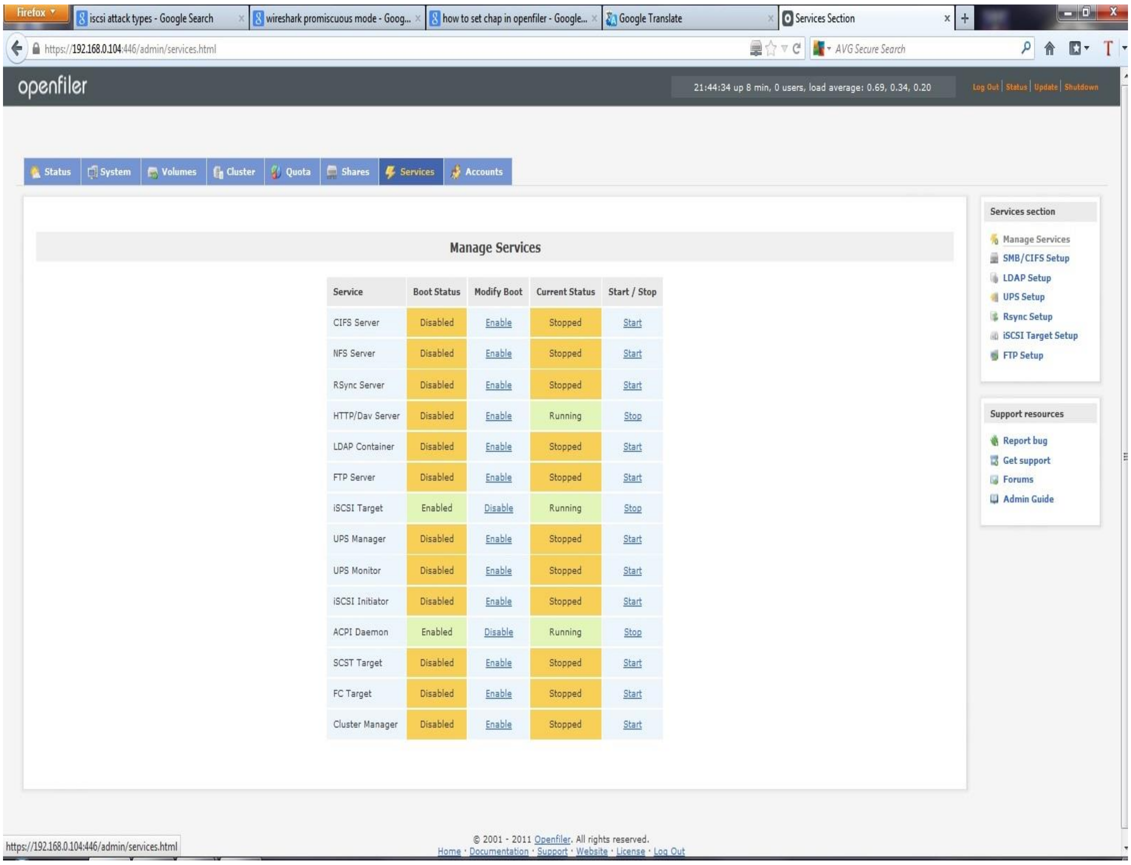
Interface	Boot Protocol	IP Address	Network Mask	Speed	MTU	Link	Edit
eth0	DHCP	192.168.0.104	255.255.255.0	1000Mb/s	1500	Yes	Configure

Network Access Configuration

Delete	Name	Network/Host	Netmask	Type
New			0.0.0.0	Share

FIG.19- domain and IP configuration of the network that can be over DHCP or static IP

The first step that we must to do is creating a physical volume but before creating physical volume we have to enable the ISCSI target service on open filer service tab, then creating physical volume from the disks that already attached and exist to our system, physical volume is the block device e.g. disk or partition. After creating a physical volume we have to define a volume group that gathered physical volume and logical together for administration unit. When defining the volume group we must create volume in any size that we need, here I defined two volume 10GB and 40GB that use ISCSI file system. Then we need to map Logical Unit Number (LUN) to our target with their specific ISCSI Qualified Name (IQN) to have an access to them through the network by ISCSI initiator. Figure 20 shows enabling the ISCSI target service before creating the physical volume.

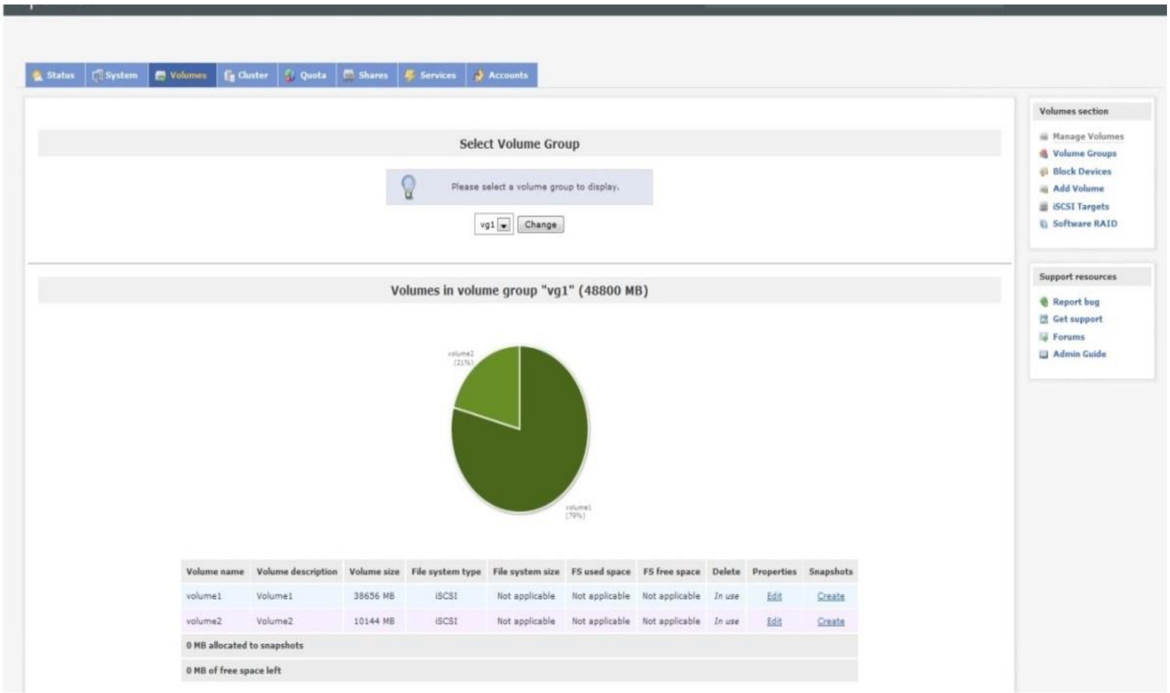

Firefox
iscsi attack types - Google Search
wireshark promiscuous mode - Goog...
how to set chap in openfiler - Google...
Google Translate
Services Section
https://192.168.0.104:446/admin/services.html
AVG Secure Search
openfiler
21:44:34 up 8 min, 0 users, load average: 0.69, 0.34, 0.20
Log Out | Status | Update | Shutdown
Status
System
Volumes
Cluster
Quota
Shares
Services
Accounts

Manage Services

Service	Boot Status	Modify Boot	Current Status	Start / Stop
CIFS Server	Disabled	Enable	Stopped	Start
NFS Server	Disabled	Enable	Stopped	Start
RSync Server	Disabled	Enable	Stopped	Start
HTTP/Dav Server	Disabled	Enable	Running	Stop
LDAP Container	Disabled	Enable	Stopped	Start
FTP Server	Disabled	Enable	Stopped	Start
iSCSI Target	Enabled	Disable	Running	Stop
UPS Manager	Disabled	Enable	Stopped	Start
UPS Monitor	Disabled	Enable	Stopped	Start
iSCSI Initiator	Disabled	Enable	Stopped	Start
ACPI Daemon	Enabled	Disable	Running	Stop
SCST Target	Disabled	Enable	Stopped	Start
FC Target	Disabled	Enable	Stopped	Start
Cluster Manager	Disabled	Enable	Stopped	Start

FIG.20-openfiler services page for enabling the services that need to communication

Figure 21 shows the volume that I defined in the volume group that consist of two volume10GB and 40 GB for using in the network after mapping to the LUN.



Select Volume Group

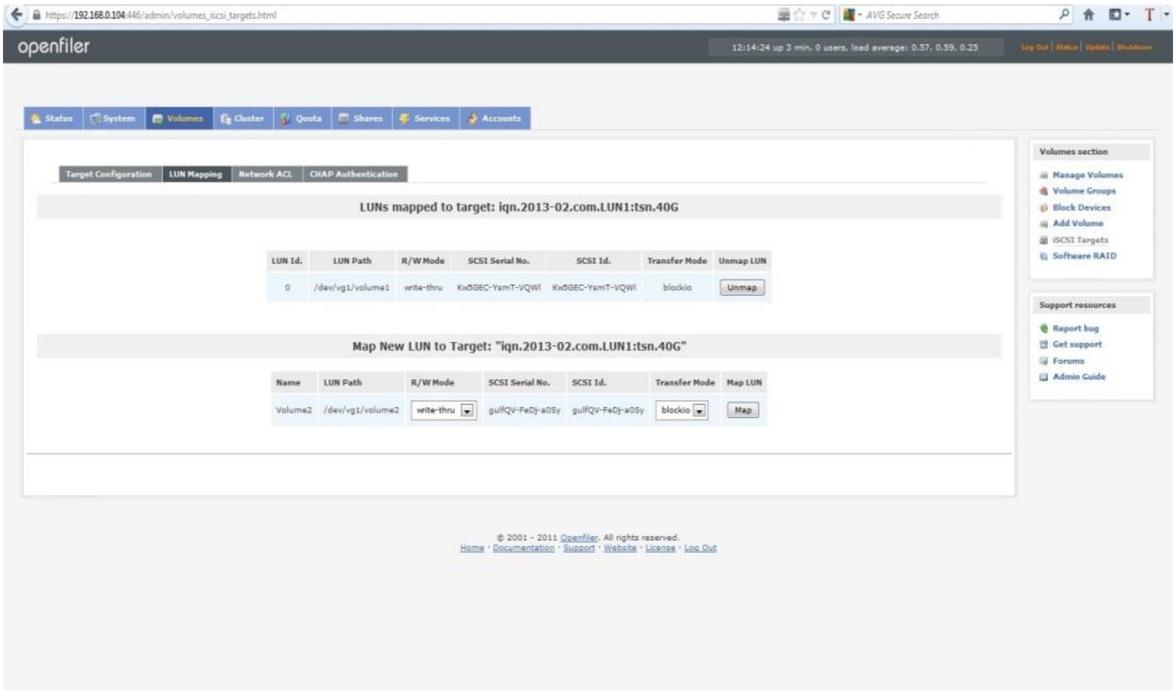
Please select a volume group to display.

Volumes in volume group "vg1" (48800 MB)

Volume name	Volume description	Volume size	File system type	File system size	FS used space	FS free space	Delete	Properties	Snapshots
volume1	Volume1	38656 MB	iSCSI	Not applicable	Not applicable	Not applicable	*In use*	Edit	Create
volume2	Volume2	10144 MB	iSCSI	Not applicable	Not applicable	Not applicable	*In use*	Edit	Create
0 MB allocated to snapshots									
0 MB of free space left									

FIG.21- volume group shows the capacity and the number of available LUN in system that here are two LUNs 10 and 40

After defining volume in volume group the next step is to map the LUN to the targets that these targets are the volume that I created before (Figure 22 shows the LUN mapping to the target).



LUNs mapped to target: iqn.2013-02.com.LUN1:tsn.40G

LUN Id.	LUN Path	R/W Mode	SCSI Serial No.	SCSI Id.	Transfer Mode	Unmap LUN
0	/dev/vg1/volume1	write-thru	Kw5GEC-YsmT-VQWl	Kw5GEC-YsmT-VQWl	blockio	Unmap

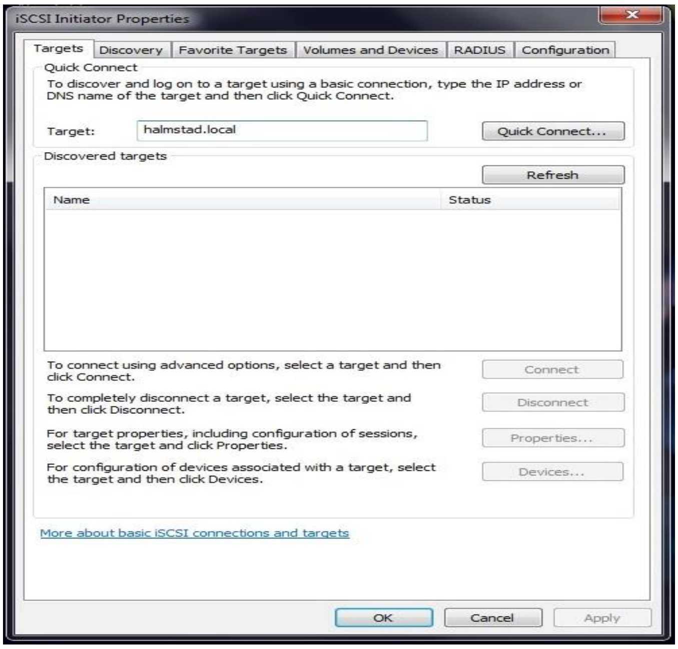
Map New LUN to Target: "iqn.2013-02.com.LUN1:tsn.40G"

Name	LUN Path	R/W Mode	SCSI Serial No.	SCSI Id.	Transfer Mode	Map LUN
Volume2	/dev/vg1/volume2	write-thru	gulfQV-FeDj-a0Sy	gulfQV-FeDj-a0Sy	blockio	Map

© 2001 - 2011 Openfiler. All rights reserved.
Home · Documentation · Support · Website · License · Log Out

FIG. 22-openfiler LUN mapping, map the specific IQN name to the specific LUN

After this step our configuration of the LUN to access over the network is finished and we have to check the availability of the LUNs from the clients that wants to connect to these LUNs. For checking the connectivity I use Microsoft ISCSI initiator (figure 23 shows the Microsoft iSCSI initiator).



To discover and log on to a target using a basic connection, type the IP address or DNS name of the target and then click Quick Connect.

Target: halmstad.local

To connect using advanced options, select a target and then click Connect.

To completely disconnect a target, select the target and then click Disconnect.

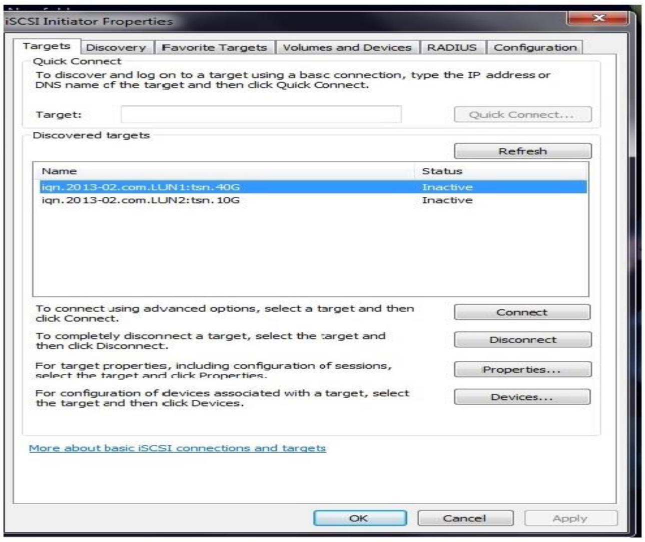
For target properties, including configuration of sessions, select the target and click Properties.

For configuration of devices associated with a target, select the target and then click Devices.

More about basic iSCSI connections and targets

FIG.23-microsoft initiator for searching and make connections to available LUNs

By typing the target host name or IP and use quick connect button the list of available LUNs on the network appears on the initiator (Figure 24 shows the available LUNs) that we can choose connect or disconnect to them, here we have two LUNs that defined before that shows on the figure below and they detect by their IQN identifiers address.



To discover and log on to a target using a basc connection, type the IP address or DNS name cf the target and then click Quick Connect.

Target:

Name	Status
iqn.2013-02.com.LUN1:tsn.40G	Inactive
iqn.2013-02.com.LUN2:tsn.10G	Inactive

To connect using advanced options, select a target and then click Connect.

To completely disconnect a target, select the :arget and then click Disconnect.

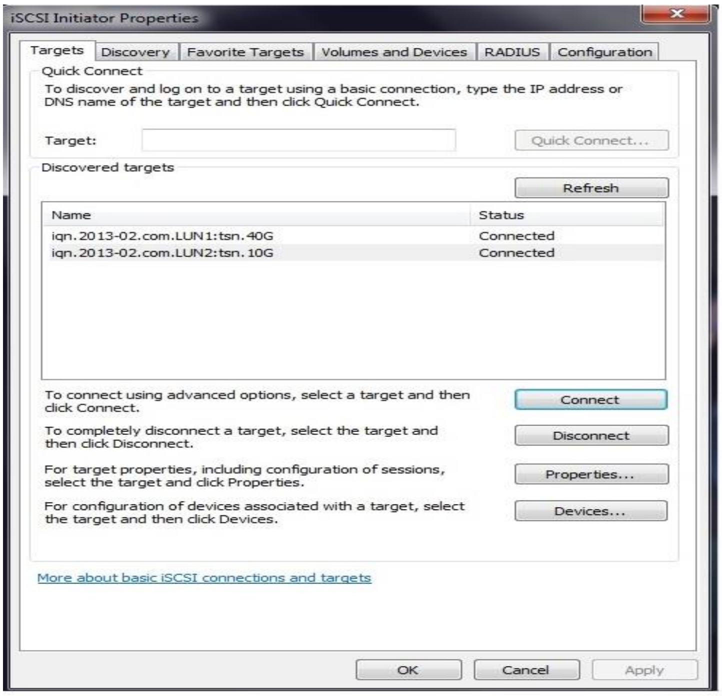
For target properties, including configuration of sessions, select the target and click Properties.

For configuration of devices associated with a target, select the target and then click Devices.

More about basic iSCSI connections and targets

FIG.24-accessing to LUNs over the Microsoft iSCSI initiator

After selecting each LUN we can connect to them and use them as part of physical disk drive on our computer. (Figure 25 shows the connectivity of the LUN in Local computer)



To discover and log on to a target using a basic connection, type the IP address or DNS name of the target and then click Quick Connect.

Target:

Name	Status
iqn.2013-02.com.LUN1:tsn.40G	Connected
iqn.2013-02.com.LUN2:tsn.10G	Connected

To connect using advanced options, select a target and then click Connect.

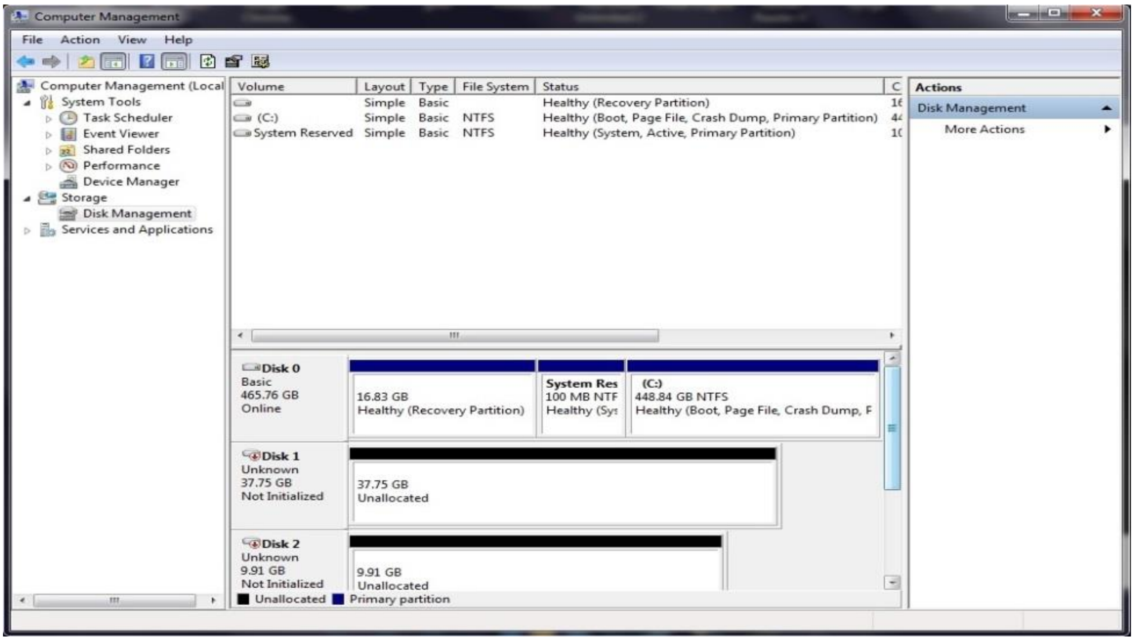
To completely disconnect a target, select the target and then click Disconnect.

For target properties, including configuration of sessions, select the target and click Properties.

For configuration of devices associated with a target, select the target and then click Devices.

FIG.25 –shows the connection status to the LUNs

After connecting to the LUNs we can access to them like our physical storage that directly attached to our computer and we have access to formatting, partitioning the disk just like are local disks. Figure 26 shows the Microsoft disk management console.



Volume	Layout	Type	File System	Status	C
	Simple	Basic		Healthy (Recovery Partition)	1€
(C:)	Simple	Basic	NTFS	Healthy (Boot, Page File, Crash Dump, Primary Partition)	44
System Reserved	Simple	Basic	NTFS	Healthy (System, Active, Primary Partition)	1(

Disk 0
Basic
465.76 GB
Online

16.83 GB
Healthy (Recovery Partition)

System Res
100 MB NTF
Healthy (Sys

(C:)
448.84 GB NTFS
Healthy (Boot, Page File, Crash Dump, F

Disk 1
Unknown
37.75 GB
Not Initialized

37.75 GB
Unallocated

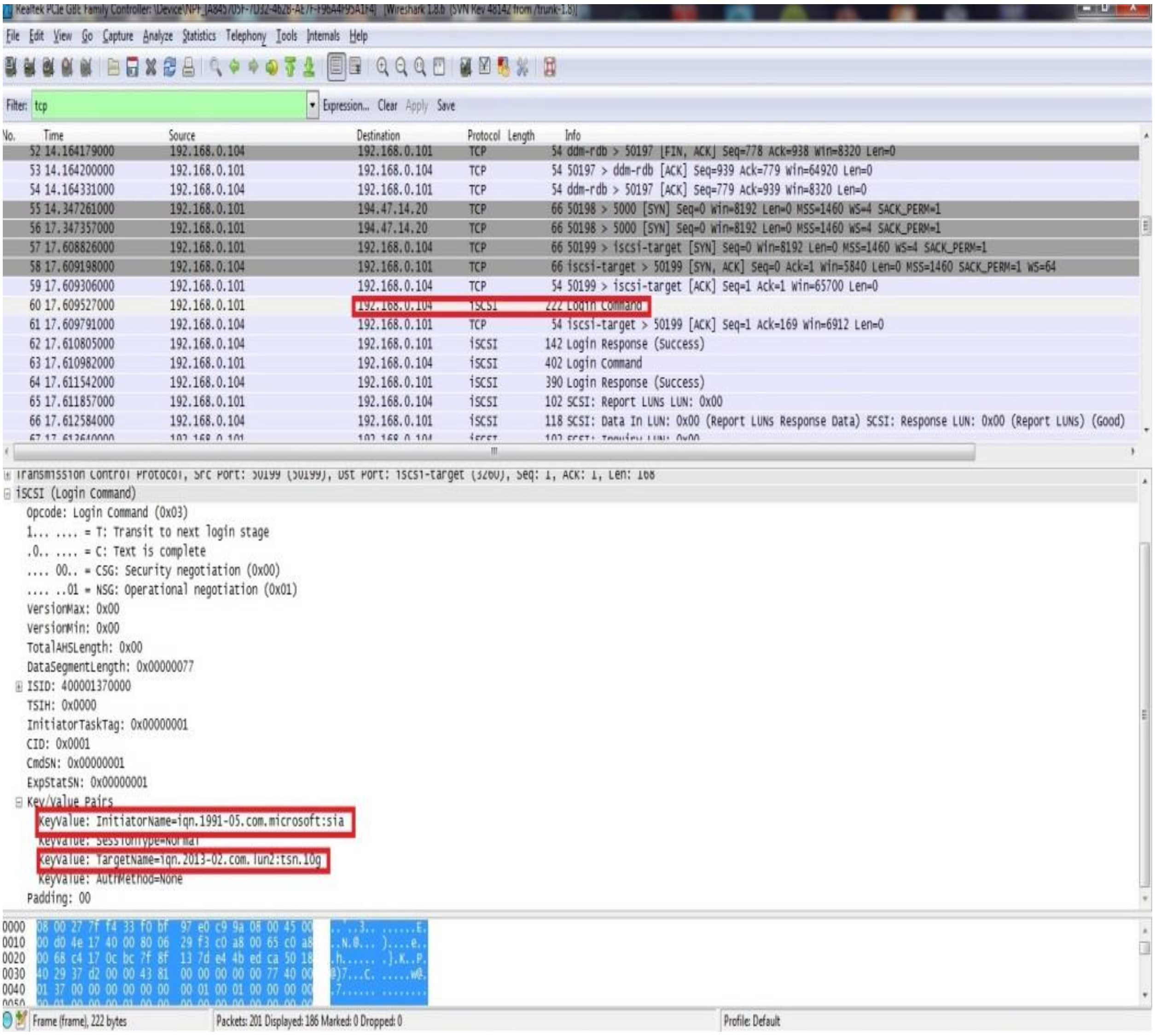
Disk 2
Unknown
9.91 GB
Not Initialized

9.91 GB
Unallocated

■ Unallocated ■ Primary partition

FIG.26-shows the local access to connected LUNs like locally attached disks

Communication through the ISCSI is in clear text mode so it is not a safe method and easy to sniff. Figure-27 shows the accessing to the IQN of the target by wireshark packet sniffer tools to gain access to LUNs.


Realtek PCIe GBE Family Controller: \Device\NPF_{A845705F-7D32-4626-AE7F-F96A4F95A1F4} [Wireshark 1.8.6 (SVN Rev 48142 from /trunk-1.8)]
File Edit View Go Capture Analyze Statistics Telephony Tools Internals Help
Filter:
Expression... Clear Apply Save

Filter: tcp

```
No.  Time             Source          Destination     Protocol Length  Info
52 14.164179000  192.168.0.104   192.168.0.101   TCP      54 ddm-rdb > 50197 [FIN, ACK] Seq=778 Ack=938 Win=8320 Len=0
53 14.164200000  192.168.0.101   192.168.0.104   TCP      54 50197 > ddm-rdb [ACK] Seq=939 Ack=779 Win=64920 Len=0
54 14.164331000  192.168.0.104   192.168.0.101   TCP      54 ddm-rdb > 50197 [ACK] Seq=779 Ack=939 Win=8320 Len=0
55 14.347261000  192.168.0.101   194.47.14.20    TCP      66 50198 > 5000 [SYN] Seq=0 Win=8192 Len=0 MSS=1460 WS=4 SACK_PERM=1
56 17.347357000  192.168.0.101   194.47.14.20    TCP      66 50198 > 5000 [SYN] Seq=0 Win=8192 Len=0 MSS=1460 WS=4 SACK_PERM=1
57 17.608826000  192.168.0.101   192.168.0.104   TCP      66 50199 > iscsi-target [SYN] Seq=0 Win=8192 Len=0 MSS=1460 WS=4 SACK_PERM=1
58 17.609198000  192.168.0.104   192.168.0.101   TCP      66 iscsi-target > 50199 [SYN, ACK] Seq=0 Ack=1 Win=5840 Len=0 MSS=1460 SACK_PERM=1 WS=64
59 17.609306000  192.168.0.101   192.168.0.104   TCP      54 50199 > iscsi-target [ACK] Seq=1 Ack=1 Win=65700 Len=0
60 17.609527000  192.168.0.101   192.168.0.104   iSCSI   222 Login Command
61 17.609791000  192.168.0.104   192.168.0.101   TCP      54 iscsi-target > 50199 [ACK] Seq=1 Ack=169 Win=6912 Len=0
62 17.610805000  192.168.0.104   192.168.0.101   iSCSI   142 Login Response (Success)
63 17.610982000  192.168.0.101   192.168.0.104   iSCSI   402 Login Command
64 17.611542000  192.168.0.104   192.168.0.101   iSCSI   390 Login Response (Success)
65 17.611857000  192.168.0.101   192.168.0.104   iSCSI   102 SCSI: Report LUNs LUN: 0x00
66 17.612584000  192.168.0.104   192.168.0.101   iSCSI   118 SCSI: Data In LUN: 0x00 (Report LUNs Response Data) SCSI: Response LUN: 0x00 (Report LUNs) (Good)
67 17.612640000  192.168.0.101   192.168.0.104   iSCSI   102 SCSI: Inquiry LUN: 0x00
```

```
⊞ Transmission Control Protocol, Src Port: 50199 (50199), Dst Port: iscsi-target (3260), Seq: 1, Ack: 1, Len: 168
⊟ iSCSI (Login Command)
    Opcode: Login Command (0x03)
    1... .... = T: Transit to next login stage
    .0.. .... = C: Text is complete
    .... 00.. = CSG: Security negotiation (0x00)
    .... ..01 = NSG: Operational negotiation (0x01)
    VersionMax: 0x00
    VersionMin: 0x00
    TotalAHSLength: 0x00
    DataSegmentLength: 0x00000077
  ⊞ ISID: 400001370000
    TSIH: 0x0000
    InitiatorTaskTag: 0x00000001
    CID: 0x0001
    CmdSN: 0x00000001
    ExpStatSN: 0x00000001
  ⊟ Key/Value Pairs
      KeyValue: InitiatorName=iqn.1991-05.com.microsoft:sia
      KeyValue: SessionType=Normal
      KeyValue: TargetName=iqn.2013-02.com.lun2:tsn.10g
      KeyValue: AuthMethod=None
    Padding: 00
```

```
0000  08 00 27 7f f4 33 f0 bf  97 e0 c9 9a 08 00 45 00   ..'..3.. ......E.
0010  00 d0 4e 17 40 00 80 06  29 f3 c0 a8 00 65 c0 a8   ..N.@... )....e..
0020  00 68 c4 17 0c bc 7f 8f  13 7d e4 4b ed ca 50 18   .h...... .}.K..P.
0030  40 29 37 d2 00 00 43 81  00 00 00 00 00 77 40 00   @)7...C. .....w@.
0040  01 37 00 00 00 00 00 00  00 01 00 01 00 00 00 00   .7...... ........
```

Frame (frame), 222 bytes | Packets: 201 Displayed: 186 Marked: 0 Dropped: 0 | Profile: Default

FIG.27-wireshark IQN sniffing for getting access to the IQN address of LUNs

There are some security issues that can help to increase the security and decrease the vulnerabilities e.g. changing the password regularly and change the default configuration and username and passwords. Check the level of access for different group and people and check the authorization and configuration on the network. Use SSL for safe connection to the management console. Increase the level of physical security to access to devices. Always ensure that the platform of the network is secure enough for making remote connection. Check the security patches and configuration for making remote access on the operating systems. Isolate the physical devices and control the access of the persons who quit working in a company [4].