06 Storage Network Technologies

www.huawei.com

Copyright © 2018 Huawei Technologies Co., Ltd. All rights reserved.

HUAWEI

Foreword

- This module introduces the types of storage network and the comparison of the advantages and disadvantages between different types of storage networks.
- This module also introduces the definition of DAS, NAS, and SAN.
- This module also describes in detail on the architecture of DAS, NAS and SAN storage network, and its advantages and disadvantages.

Copyright © 2018 Huawei Technologies Co., Ltd. All rights reserved.

Objectives

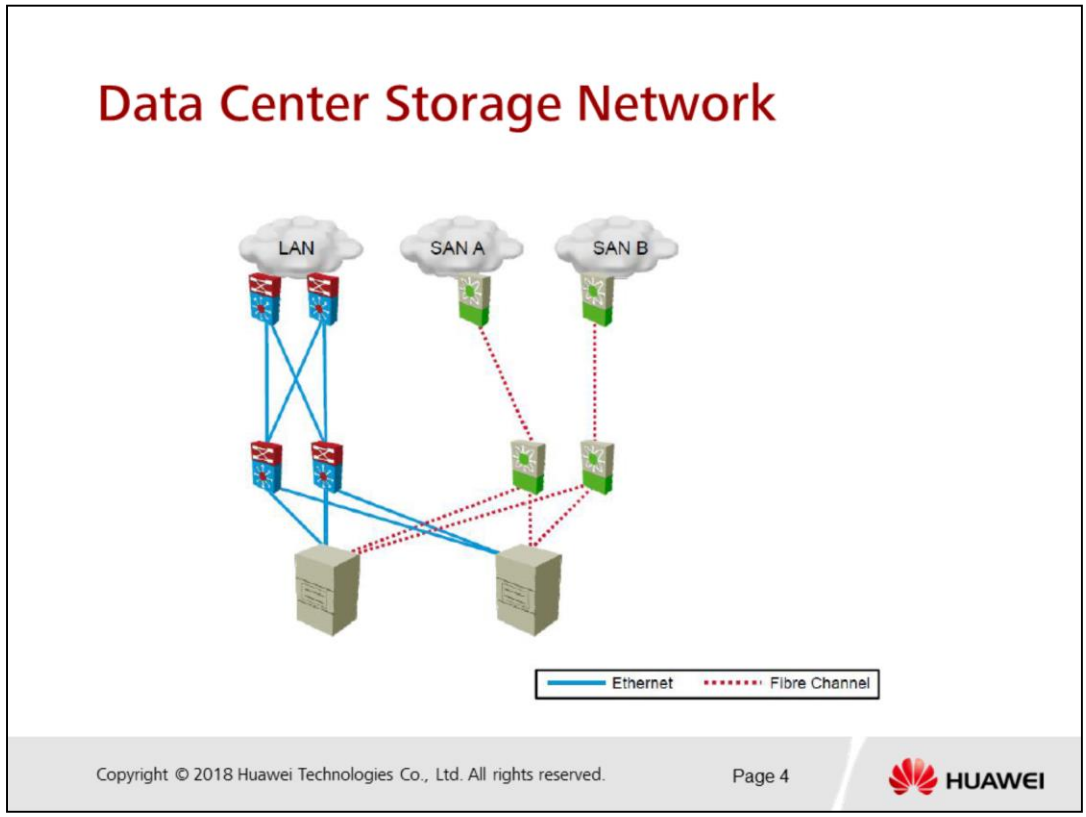
- Upon completion of this module, you will be able to:
  - Describe the characteristics of DAS, NAS and SAN storage network technologies.
  - Differentiate between the advantages and disadvantages of DAS, NAS, and SAN storage network technologies.

Copyright © 2018 Huawei Technologies Co., Ltd. All rights reserved.

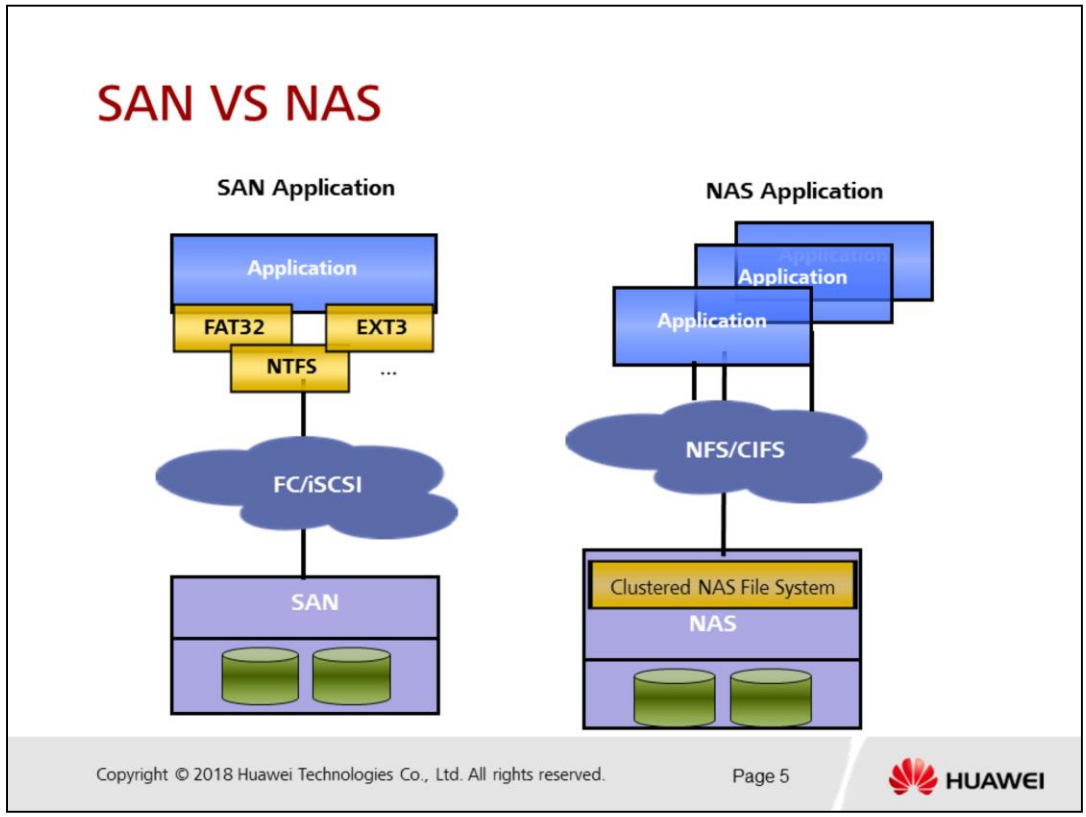
Contents

1. **Classification of Network Storages.**
2. DAS - Traditional Storage Technology.
3. SAN - Storage Area Network.
4. NAS - Network Attached Storage.

Copyright © 2018 Huawei Technologies Co., Ltd. All rights reserved.



- Data storage has become one of the popular technologies nowadays and created a new technological trend after the emergence of the Internet. It brings the web into a data centric era.
- Data storage went through 3 stages of development: Direct Attached Storage (DAS), Network Attached Storage (NAS), and Storage Area Network (SAN). DAS is a product of CPU centric era and adapted to the initial development of the computing industry. The biggest technological differences between SAN and NAS is the way they use dedicated protocol or existing IP technology and data sharing. The advantage of SAN is that it solved the initial problem of network bandwidth for storage issue, while the advantage of NAS is its versatility and data sharing capabilities.



- NAS (Network-Attached Storage)
  - Protocols: NFS/CIFS (Based on TCP/IP).
  - Provides file access, and suitable for file storage requirements.
  - Suitable for file sharing and file access application, supports heterogeneous file sharing platform.
  - File data migration is much simpler and reliable than raw device.
- SAN (Storage Area Network)
  - Protocols: FC/iSCSI
  - Supports raw device access, suitable for traditional database access.
  - Relies on application host to provide file access. Data sharing access requires the support of the cluster software, high overhead on processing access conflicts, lower performance, and hard to support data sharing between heterogeneous platforms.
  - Raw device data migration is difficult.

- With the growth of virtualization technology, more and more storages are required for virtual machines. The storage required for these virtual machines are often provided by SAN solutions. Raw device and raw device mapping (RDM) are also common technologies that exist in virtualization environment in data centers that ties closely to the storage environment such as SAN.
- In computing, specifically in Unix and Unix-like operating systems, a raw device is a special kind of logical device associated with a character device file that allows a storage device such as a hard disk drive to be accessed directly, bypassing the operating system's caches and buffers (although the hardware caches might still be used). Applications like a database management system can use raw devices directly, enabling them to manage how data is cached, rather than deferring this task to the operating system.
- Raw device mapping (RDM) is an option in the server virtualization environment that enables a storage logical unit number (LUN) to be directly connected to a virtual machine (VM) from the storage area network (SAN).
    - RDM is a mapping file in a separate volume that acts as a proxy for a raw physical storage device. The RDM allows a virtual machine to directly access and use the storage device. The RDM contains metadata for managing and redirecting disk access to the physical device.
    - The file gives you some of the advantages of direct access to a physical device while keeping some advantages of a virtual disk. As a result, it merges virtual volume manageability with raw device access.
    - RDMs can be described in terms such as mapping a raw device into a datastore, mapping a system LUN, or mapping a disk file to a physical disk volume. All these terms refer to RDMs.

Comparison of DAS, NAS and SAN (1)

Storage System Architecture	DAS	NAS	SAN
Data Transmission Protocol	SCSI/FC/ATA	TCP/IP	FC
Data Transfer Object	Block	File	Block
Uses Standard File Sharing Protocols	No	Yes (NFS/CIFS...)	No
Centralized Management	Not Exactly	Yes	Requires Management Tools
Increases Server Efficiency	No	Yes	Yes
Disaster Tolerance	Low	High	High, Dedicated Solutions

Copyright © 2018 Huawei Technologies Co., Ltd. All rights reserved.

HUAWEI

- The table above shows the comparison of DAS, NAS and SAN storage architecture.

Comparison of DAS, NAS and SAN (2)

Storage System Architecture	DAS	NAS	SAN
Suitable Clients	SME Servers, JBOD	SME, Monitoring, Broadcasting	Large Enterprises, Data Centers
Application Environment	Local Area Network(LAN). Low file sharing level, independent operating platform, and less server management	Local Area Network(LAN). High file sharing level, high demand in heterogeneous storage format.	Fibre Channel Storage Network. Complex network environment, high file sharing level, heterogeneous OS platform, high number of servers.
Capacity Expansion Capabilities	Low	Medium	High

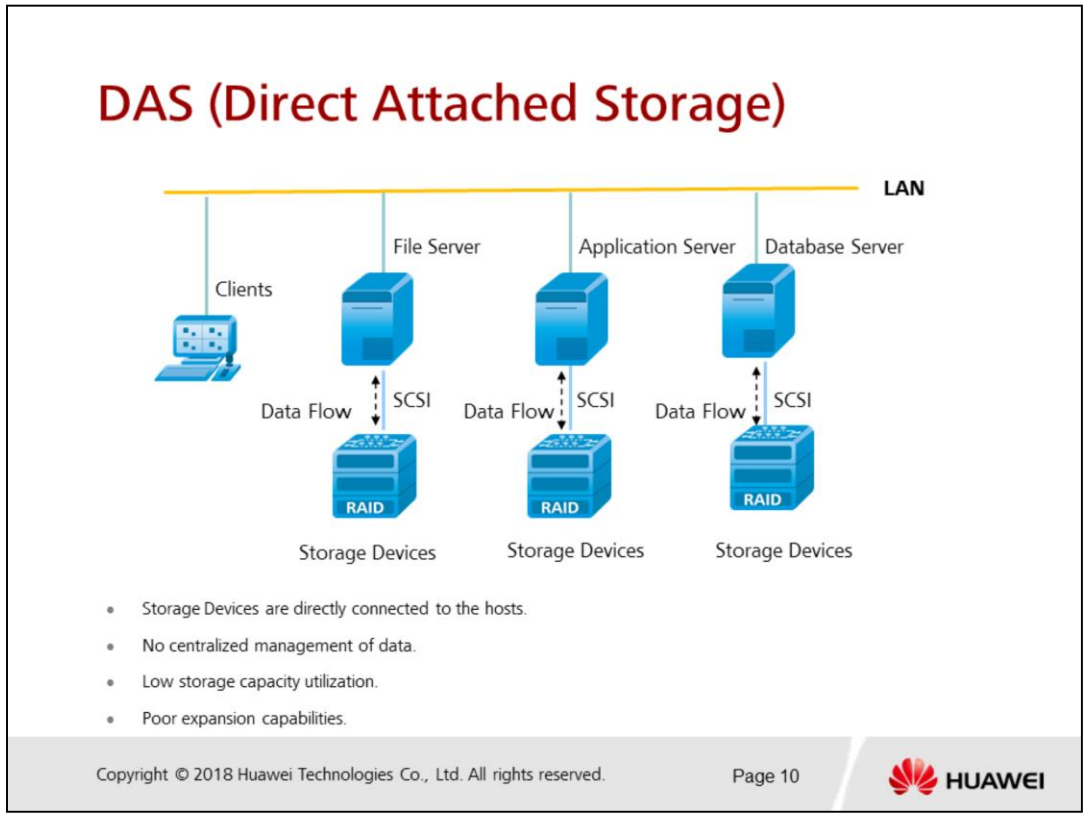
Copyright © 2018 Huawei Technologies Co., Ltd. All rights reserved.



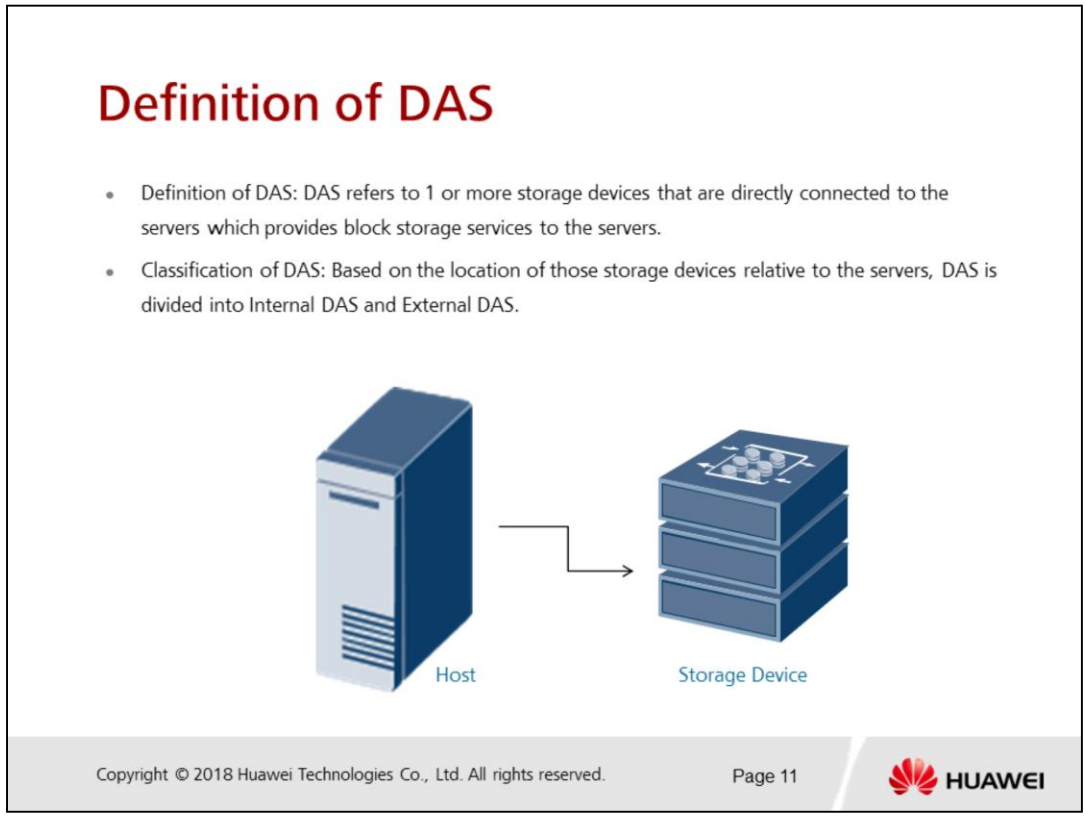
Contents

1. Classification of Network Storages.
2. **DAS - Traditional Storage Technology.**
3. SAN - Storage Area Network.
4. NAS - Network Attached Storage.

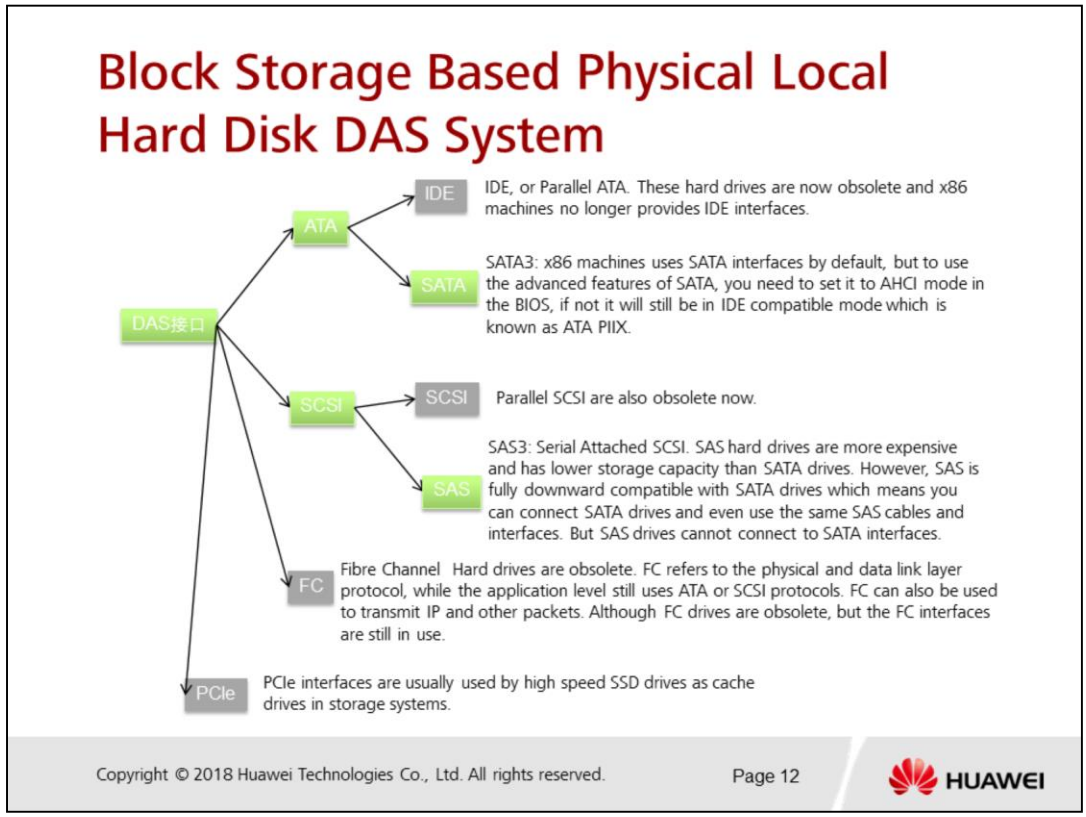
Copyright © 2018 Huawei Technologies Co., Ltd. All rights reserved.



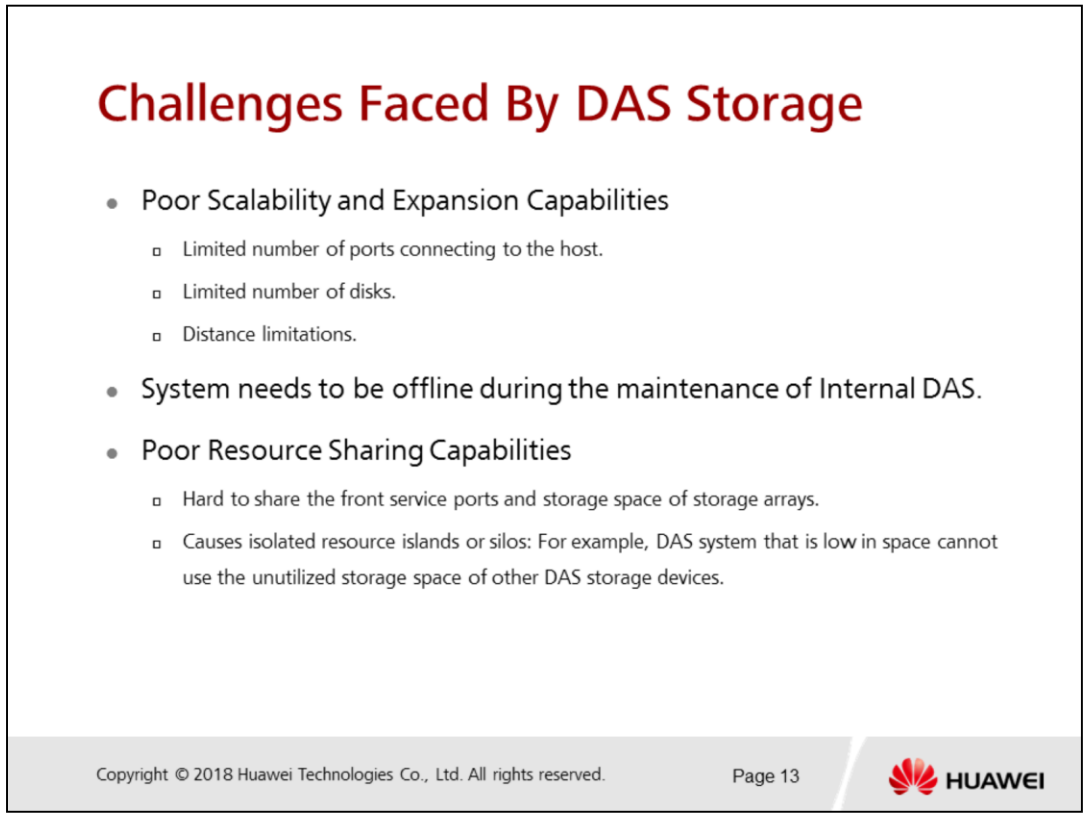
- DAS is very suitable for small or medium sized local area networks that has low storage capacity requirements and fewer number of servers. Its main advantage is easy and quick implementation of storage capacity expansion with small cost of investment.
- A typical DAS system is made of a data storage device (for example enclosures holding a number of hard disk drives) connected directly to a computer through a host bus adapter (HBA). The main characteristics of DAS is that between those two points (server and storage device), there is no network device (like hub, switch, or router).



- Directly Attached Storage (DAS): is a storage architecture where the storage devices are directly connected to the servers. DAS provides block storage (not file storage) services to the servers. Example of DAS are: internal hard drive of servers, directly connected tape libraries, directly connected external disk enclosures. Based on the location of the storage device relative to the server, DAS can be divided into Internal DAS and External DAS.
- Internal DAS:
  - In the architecture of Internal DAS, storage devices connects to the server internally via parallel or serial connections. However, due to the physical distance limitation of the system bus, it could only support short distance high speed data transmission. Additionally, there is also limitation on the number of devices that can be connected internally. It takes up a lot space when these storage devices are placed within the server's chassis, causing difficulties for maintenance of other parts within the server.
- External DAS:
  - In the architecture of External DAS, external storage devices are connected directly with the servers, and not located within the servers itself. In most scenarios, these storage devices communicate between each other using FibreChannel (FC) protocols or SCSI protocols. In comparison with Internal DAS, External DAS has overcame the limitation of distance and limitation of number of connected devices. Other than that, External DAS even provides centralized management of storage devices making management and maintenance of these devices much easier.



- Direct-Attached Storage(DAS), can be explained simply as using local hard drives for storage and these drives are connected using local interface. X86 architecture usually uses ATA (IDE or SATA) interfaces, minicomputers and high end x86 servers uses SCSI (SCSI or SAS) interface. In high performance scenarios, FC optical interface are used. However, with the developments of serial interface technologies, even the slower SATA interface speed also have exceeded the speed of hard drives read/write speed, which means that SATA interface speed is sufficient for even SSD drives. As the serial interface technology such as SATA becomes much faster, the FC hard drives becomes obsolete and SAS usage are gradually decreasing. High speed SSD cache drives on the other hand uses PCIe interface directly for much higher performance.

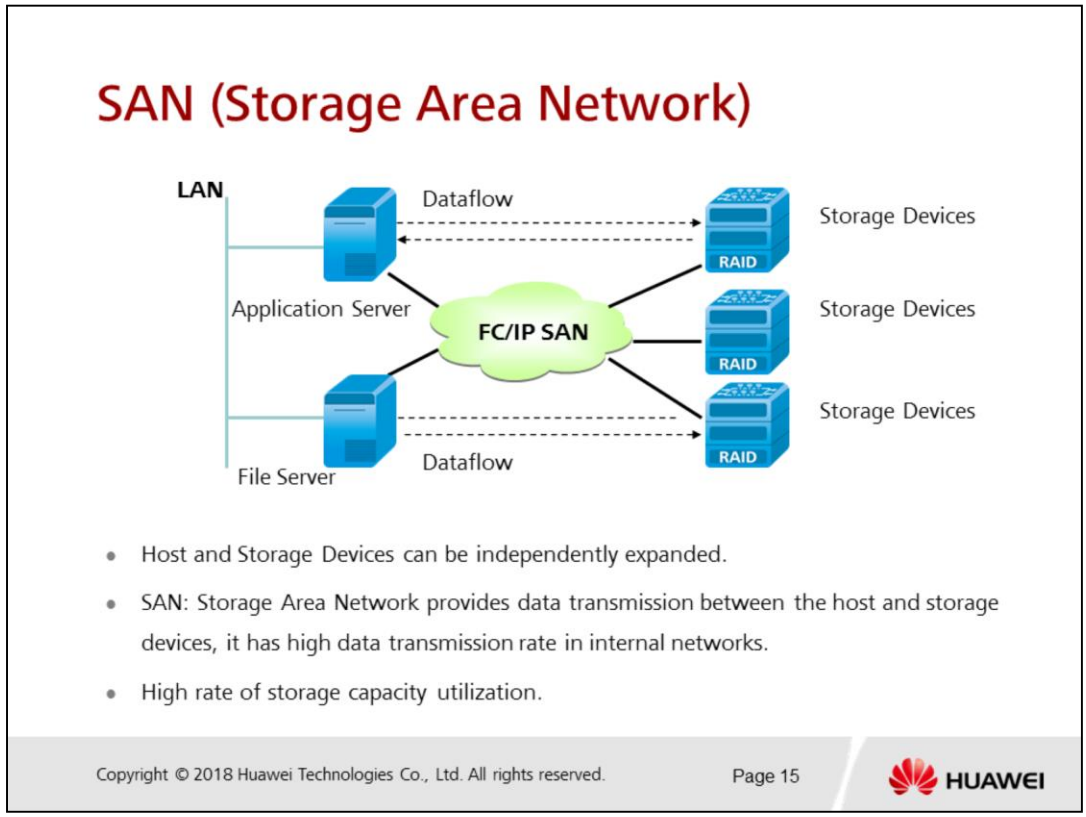


- DAS has poor scalability and expansion capabilities. Limited number of usable host ports caused a limitation on number of host that can be connected to the storage. At the same time, limited bandwidth of DAS devices caused it to have limited IO processing capabilities. When the IO processing requirement from the connected host is high and reaching the upper limit of the DAS devices IO processing capabilities, the service on the host will be affected and even will cause a chain reaction affecting the performances of all the connected host of the DAS storage.
- Due to the limited sharing capabilities of the front end host ports, it caused DAS to have low resource utilization rate. In the DAS system, to reallocate and configure the remaining unutilized storage space is difficult causing the formation of resource islands or silos. As some of the DAS devices are under utilized with remaining lots of space and some are over utilized with critically low storage space, the fact that DAS devices cannot do resource sharing between devices does not able to help or solve this situation. Additionally, disk utilization rate, throughput, internal memory of DAS devices also affects the performance of DAS storage systems. Additional factors such as RAID group level configuration, host storage controller protocol type and host bus efficiency also affects the performance of DAS system. The main advantage of DAS system compared to other storage architecture lies only on the fact that it does not have the complexity for devices interconnection and network latency between storage devices.

Contents

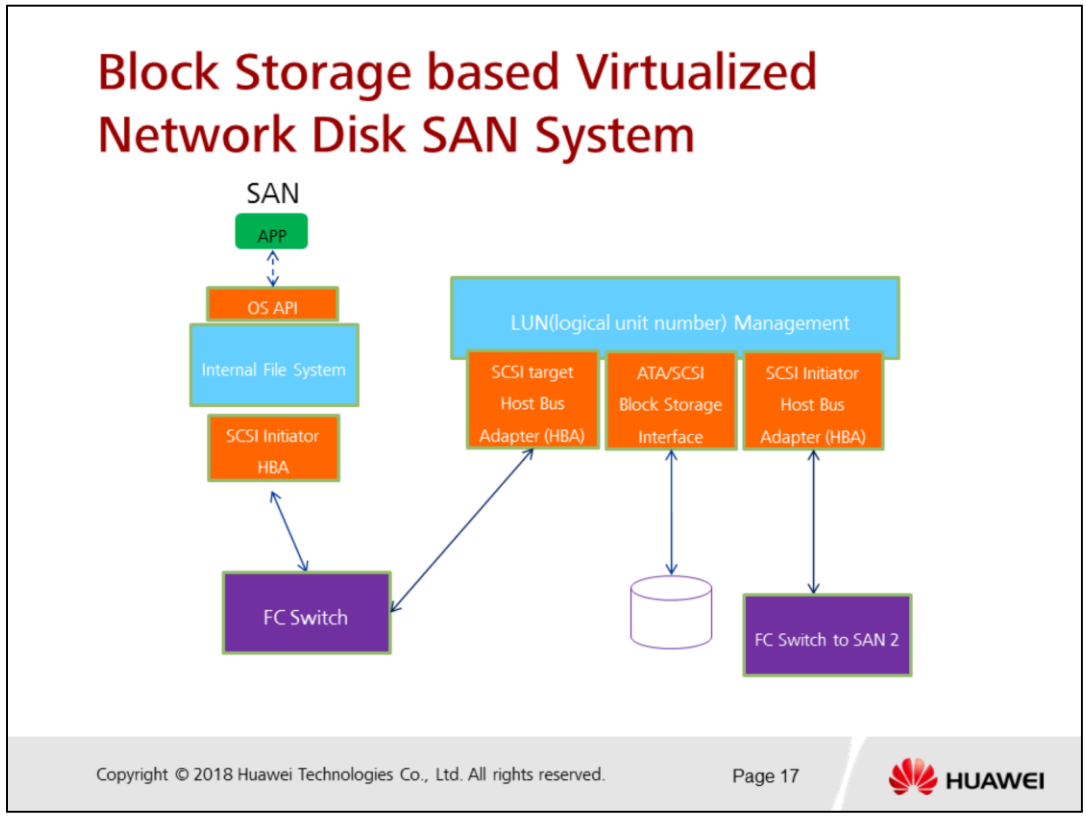
1. Classification of Network Storages.
2. DAS - Traditional Storage Technology.
3. **SAN - Storage Area Network.**
4. NAS - Network Attached Storage.

Copyright © 2018 Huawei Technologies Co., Ltd. All rights reserved.

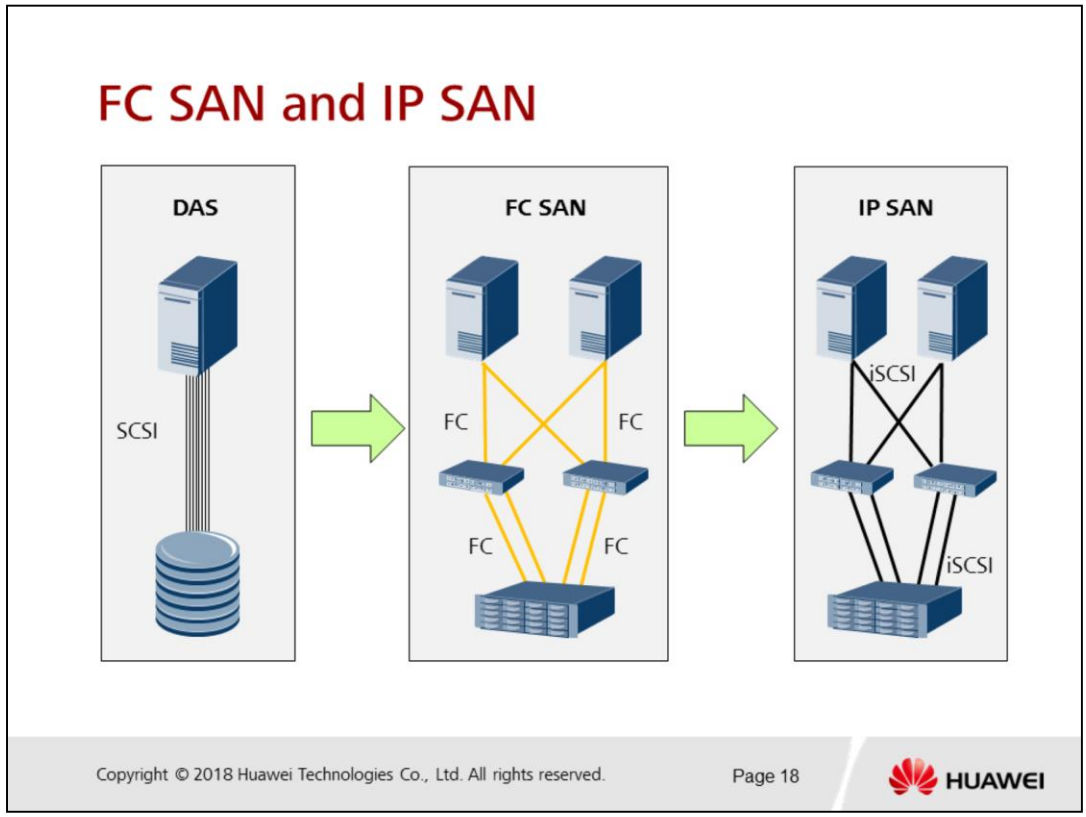


- SAN is the abbreviation of Storage Area Network, it is a type of dedicated network for high speed reliable data access and transmission between host and external storage devices or between independent storage resources.
- SAN implements an expandable and scalable network topology connecting the servers and storage devices, and each storage devices does not belong to a dedicated server, as it allows equal level of resource sharing between all of the storage devices and hosts within the network.
- A complete SAN includes: host devices that support SAN, storage devices that support SAN, connectivity devices used to connect all the devices in the SAN, management software that supports SAN, and finally services that supports SAN.
- Storage Area Network (SAN) : is a dedicated high performance network implemented between the server and storage resources. It has been optimized specifically for high amount of raw data transmission. Hence, FC SAN can be seen as an expanded form of SCSI protocols in terms of long distance application. The default protocols used by FC SAN is SCSI and Fiber Channel. Fiber Channel is especially suitable for SAN implementation due to the fact that it is capable of transmitting large blocks of data and is also capable of long distance transmission. The market for FC SAN is mostly centered at high end enterprise grade storage devices implementations. These storage implementations has high requirements for performance, redundancy and availability. For an example, components such as storage arrays and backup devices are storage devices.

- A SAN architecture can support up to 16.77 million of connected storage device. Connection distance of the storage components can reach up to a distance of 20,000km. The data transmission speed of the SAN architecture has improved by great bounds since the first SAN was physically implemented. Nowadays, data transmission speed in SAN has reached the speed of 16Gb/s and could even reach up to 40 Gb/s.
- A SAN environment, although it consists of many components and features, can be quite easily managed because of the existence of multiple tools used for monitoring, management and reporting. However, currently there is no company that is able hit this upper limit for devices in the scale of deployed physical SAN infrastructure. But we noticed that, nowadays some equipment of large enterprises need to provide services to support business activities that span across the globe, for example from China to US or from Europe to Africa. Employees around the world may need to access company data at any given time, for example an employee from Brazil needs to access storage on the servers located at Shenzhen, Hong Kong servers. As globalization occurs in the industries around the world, business activities are no longer limited to a single geographical region and are growing and spanning across the globe internationally, which means that IT equipment such as SAN need to be able to adapt to these changes and able to support these business activities globally.



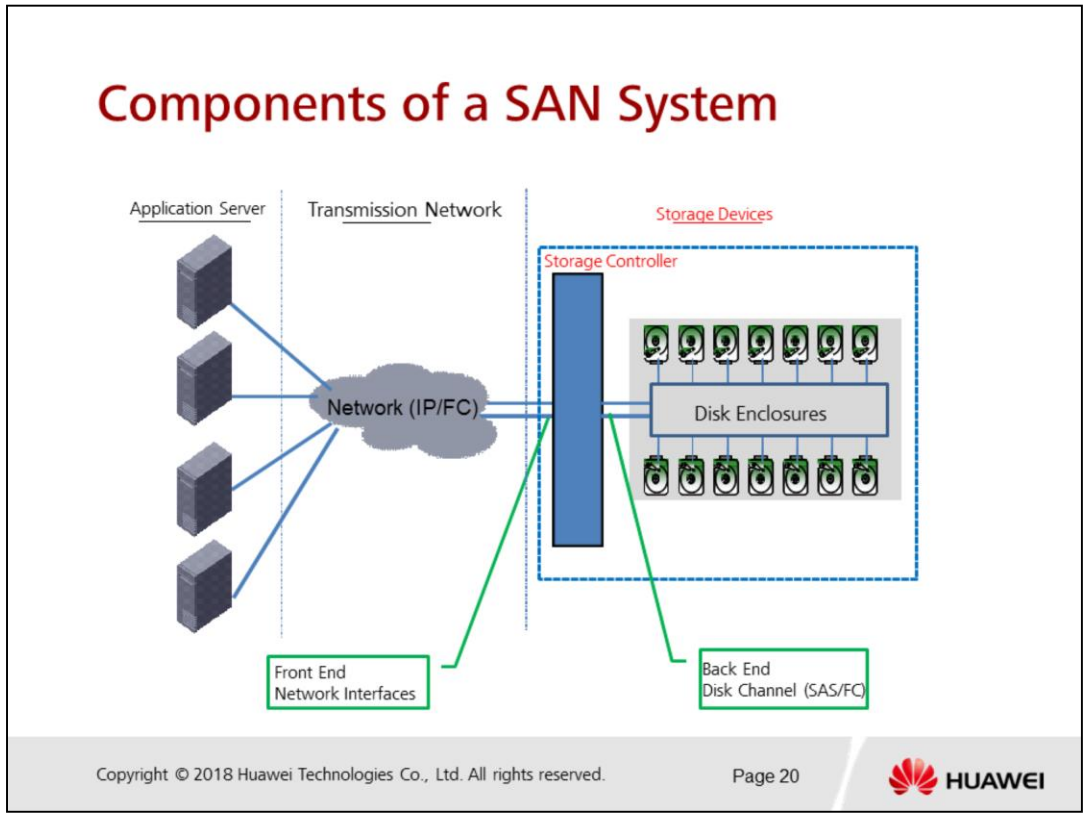
- SAN provides block storage similar to DAS, but also has the advantages of remote connection using network similar to NAS.
- In computer storage, a logical unit number (LUN), is a number used to identify a logical unit, which is a device addressed by the SCSI protocol or Storage Area Network protocols which encapsulate SCSI, such as Fibre Channel or iSCSI.
- SCSI initiator is the endpoint that initiates a SCSI session, that is, sends a SCSI command. The initiator usually does not provide any Logical Unit Numbers (LUNs).
- On the other hand, a SCSI target is the endpoint that does not initiate sessions, but instead waits for initiator's commands and provides required input/output data transfers. The target usually provides to the initiators one or more LUNs, because otherwise no read or write command would be possible.



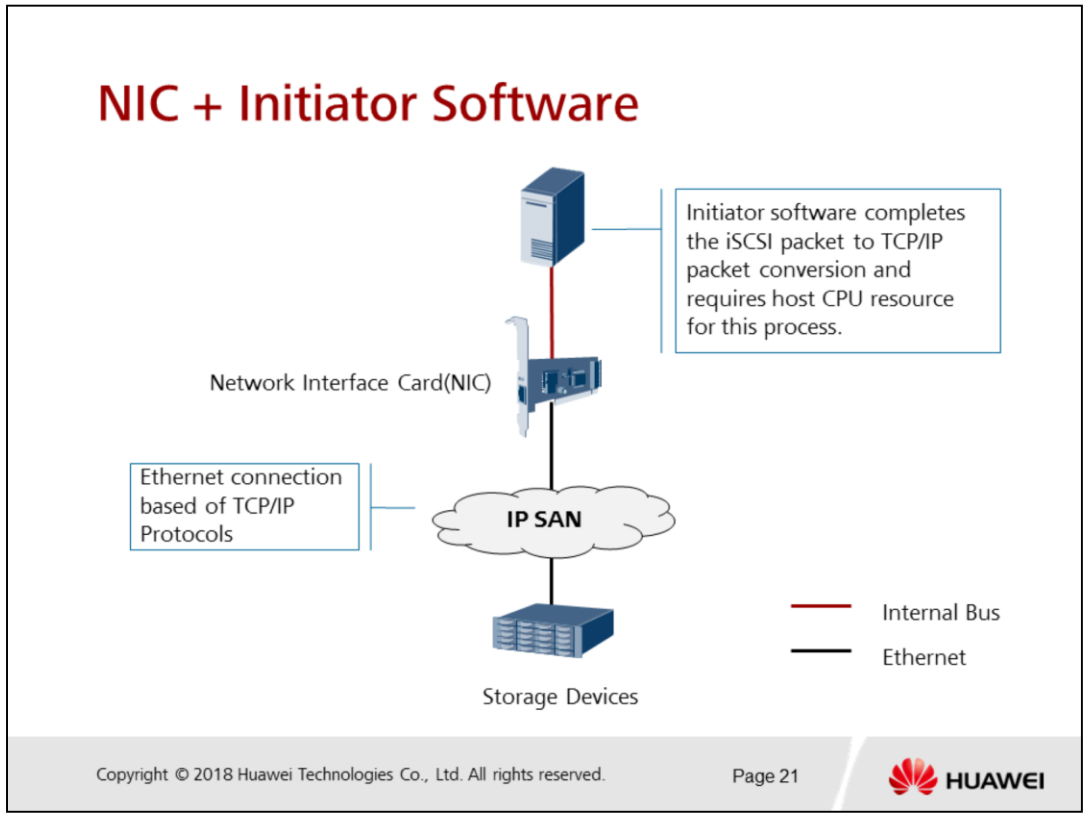
- What is IP SAN?
  - It uses TCP/IP as the base level transmission protocol, and is a storage area network architecture that uses Ethernet as the transmission medium.
  - Default protocol for IP SAN is iSCSI, which defines the encapsulation of SCSI commands in packets and the transmission of those packets over the IP network.
- IP-SAN default networking methods are:
  - Direct Connection: The host and storage devices are directly connected via Ethernet network cards, TOE (TCP Offload Engine) cards, or iSCSI HBA cards. These types of connection are simple, economical but will be difficult to share storage resources in scenarios where there a large number of hosts.
  - Single Switching: Hosts and storage devices are connected through a single Ethernet switch, where the connection on the ends of the host and storages are still using Ethernet network cards, TOE cards or iSCSI HBA cards. This type of connection allows multiple host to share the same storage device, has good scalability, but has a single point of failure at the network switch. If the network switch is faulty, all the host are unable to access the storage devices.

    - Dual Switching: There are multiple redundant paths connecting between the host to the front end service port of the storage array, has good scalability, and eliminates the single point of failure that exist at the network switch level. In this connection, each host has a minimal of 2 different paths to reach the storage, and if one of the path is down, the host can use the redundant path to reach the storage device.

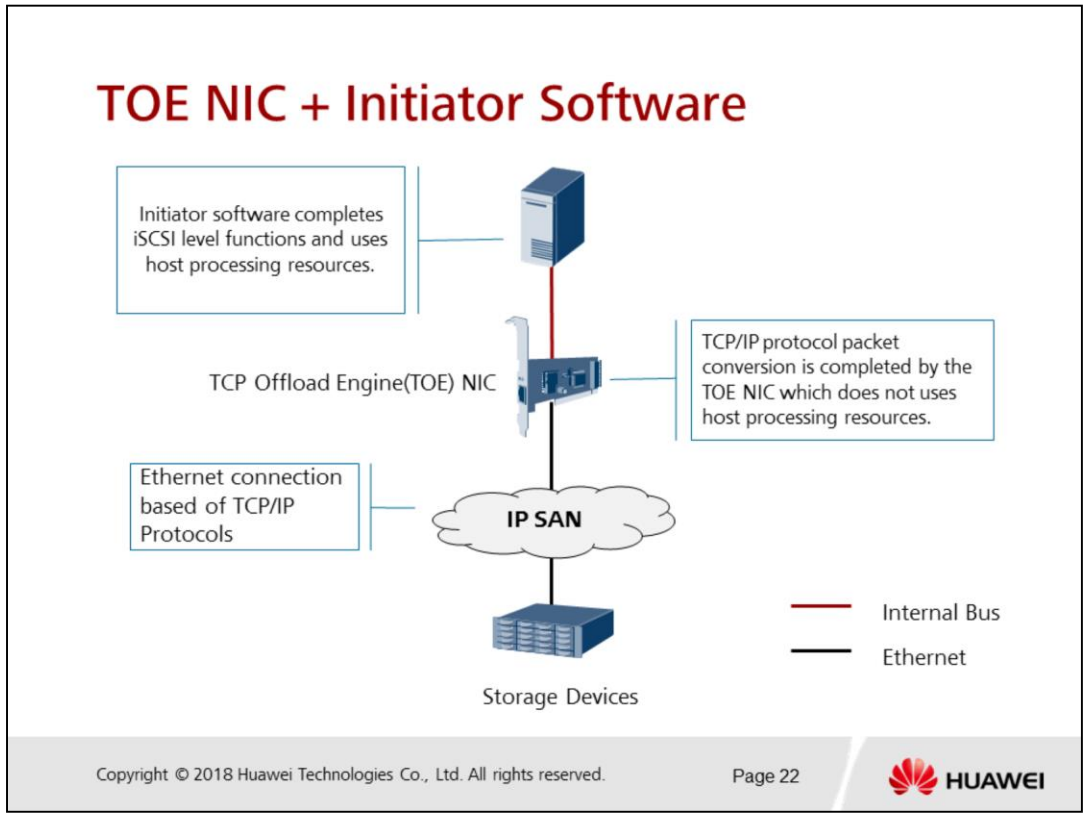
- SAN architecture commonly uses these 3 types of protocols:
    - FC (Fibre Channel) protocol: SAN that uses this protocol are called FC SAN.
    - iSCSI (Internet SCSI) protocol: SAN that uses this protocol are called IP SAN.
    - FCoE (Fibre Channel Over Ethernet) protocol: This protocols allows FC packets to be transmitted in IP networks over Ethernet.
- FC protocol and iSCSI protocol are commonly used in modern SAN architecture, while FCoE protocol is being used more and more frequently during the scenario where the servers need to converge the services of SAN and LAN.



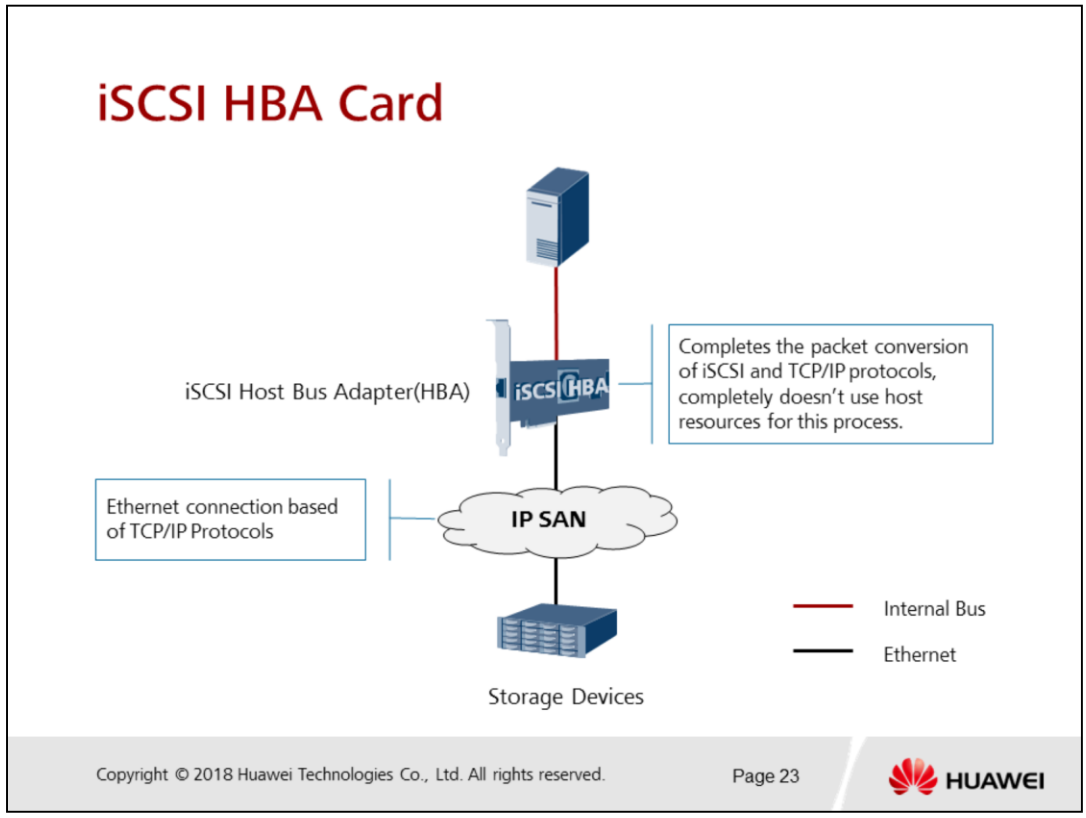
- As shown on the diagram above, a complete SAN system commonly includes the front end application server, transmission network, and storage devices. Servers refers to x86 servers, minicomputers or clustered servers that are running operating systems such as Windows, Linux or Unix. Transmission network can be FC network or IP network, and the types of network and interface cards used within the SAN depends on the type of network that the key storage equipment supports.
- Storage devices consists of the front end network interfaces storage controllers, back end disk channel, disk enclosures and hard drives. Storage controller is the core of the storage device. It is a manifestation of processing performance, and can have corresponding optimization measures for various protocol architectures. There is no obvious difference among various storage devices.
- Hence, the difference in storage devices lies at the front end network interfaces (IP or FC), and the back end disk channel (SAS or FC). Based on the different combination of the front end and back end technologies, it formed 4 main storage device architecture: which are IP+SAS, IP+FC, FC+SAS, FC+FC. Commonly, FC SAN refers to storage devices that connects to server using FC protocols through the FC network interface, while IP SAN refers to the storage devices that connects to the server using iSCSI protocol through IP network interface.



- Host devices such as servers and workstations, connects to Ethernet switches using standard NIC cards, and iSCSI storage devices are also connected to Ethernet switches or directly to the host NIC card. Initiator software is installed on the host to virtualize the Ethernet card as an iSCSI card which is used to send and receive iSCSI packets and makes both iSCSI and TCP/IP protocol data transmission possible between the host and the iSCSI storage device. This implementation has the lowest hardware cost due to the use of standard Ethernet cards and Ethernet switches, eliminating the need for additional adapters. However, this mode of implementation needs to occupy host processing resources when performing iSCSI and TCP / IP data packet conversion, which in turn increases host operating overhead and reduces system performance. However, the basic requirements for data access are met in applications or scenarios with low I/O and bandwidth requirements.



- TOE NIC cards handles the TCP/IP protocol level functions, while the host processes the iSCSI protocol level functions. Hence, by using TOE NIC allows a high increase in data transmission rate. Compared to the method where only software is used, this method greatly reduces the host operation overhead and does not increase the cost of building the network greatly which serves as a configuration solutions that offers good compromise for performance and costing.
- The TCP/IP offload engine is a technology that is gaining popularity in high-speed Ethernet systems for the purpose of optimizing throughput. TOE components are incorporated into one of the printed circuit boards, such as the network interface card (NIC) or the host bus adapter (HBA).
- In recent years, the communication speed in Ethernet systems has increased faster than computer processor speed. This produces an input/output (I/O) bottleneck. The processor, which is designed primarily for computing and not for I/O, cannot keep up with the data flowing through the network. As a result, the TCP/IP flow is processed at a rate slower than the speed of the network. TOE solves this problem by removing the burden (offloading) from the microprocessor and I/O subsystem.



- iSCSI HBA cards are installed on the hosts to achieve highly efficient data transmission between host and switches and between host and storage devices. iSCSI and TCP/IP protocol level functions are both completed by the HBA card installed on host, which bring the host CPU resource consumption during data transmission to the minimum. This method provides the best data transmission performance, however it comes with the highest cost to build this network compared to other methods.
- The iSCSI communication system inherits some of the features of SCSI protocol. In iSCSI communication, there is an Initiator device that initiates I/O requests and a Target device that responds to requests and performs actual I/O operations. After a connection is established between the Initiator and Target, the Target acts as master in the data transmission operation and controls the entire process. Examples of the target includes: iSCSI disk arrays and iSCSI tape libraries.

- iSCSI protocols defined a set of naming and addressing scheme for the Initiator and Target. All the iSCSI nodes are identified by using its ISCS name. This naming scheme avoids the conflict or confusion of iSCSI name and the host name within the network.
- iSCSI uses iSCSI Qualified Name (IQN) to differentiate between the initiator and target devices. The address of the iSCSI device will change when the hardware is changed to another location or server but the IQN name of the iSCSI device will not change. When you establish a iSCSI connection, the initiator send out a request, and the target receives that request and checks if the targeted IQN within the request is the same with its IQN, if it is identical, then the connection is successfully established. Each iSCSI node is only allowed to have 1 single IQN. A single IQN can be used to establish connections between 1 initiator device and multiple target device, or multiple IQN can be used to establish connections between 1 target device to multiple initiator device. In simpler terms: 1 initiator IQN → multiple target, or 1 target IQN → multiple initiator.

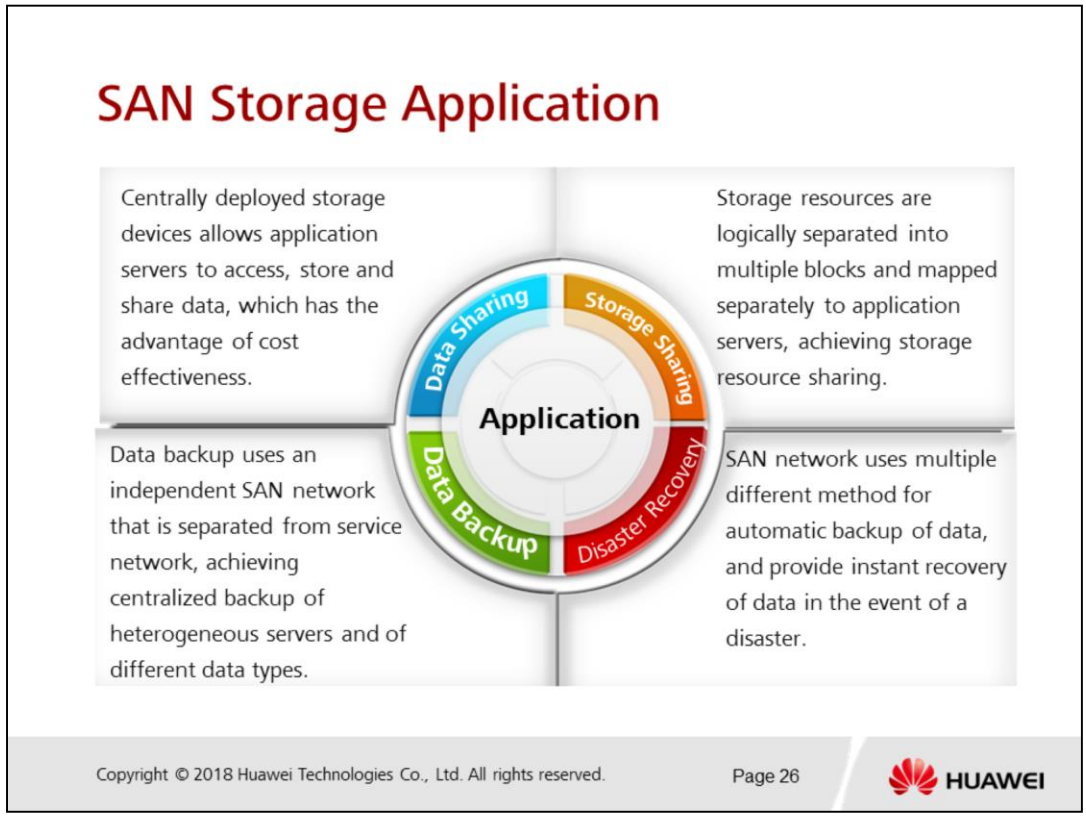
Comparison between FC SAN and IP SAN

Description	FC SAN	IP SAN
Network Speed	4Gb、8Gb、16Gb	1Gb、10Gb、40Gb
Network Architecture	Custom built optical network and HBA cards.	Uses existing IP networks.
Transmission Distance	Limited by optical transmission distance.	Theoretically no distance limitation.
Management & Maintenance	Complex management and technologies.	Easy operation like normal IP devices.
Compatibility	Poor compatibility.	Compatible with all IP network devices.
Performance	Very high transmission and read/write performance.	Mainstream of 1Gb/s, and 10 Gb/s speed is still growing.
Cost	Purchase (FC Switches, HBA cards, FC Disk Arrays),and Maintenance (Train Personnel, System Configuration and Monitoring) costs are high.	Compared to FC SAN, the purchase and maintenance cost are lower with higher ROI.
Disaster Recovery	Disaster recovery hardware and software cost are high.	Can achieve local and remote disaster recovery with lower cost.
Security	Higher security.	Lower security.

Copyright © 2018 Huawei Technologies Co., Ltd. All rights reserved.

HUAWEI

- IP SAN only requires very less hardware configurations, and these hardware are widely in use, so this makes the cost of implementing IP SAN much lower than FC SAN. Most of the host are already equipped with suitable network interface cards (NIC) and connected to suitable switches, and these NIC and switches are also suitable (although not perfect) for iSCSI protocol based data transmission. High performance IP SAN on the other hand often requires custom iSCSI HBA cards to be installed and connected to high end switches in order to achieve high performance data access and transmission.



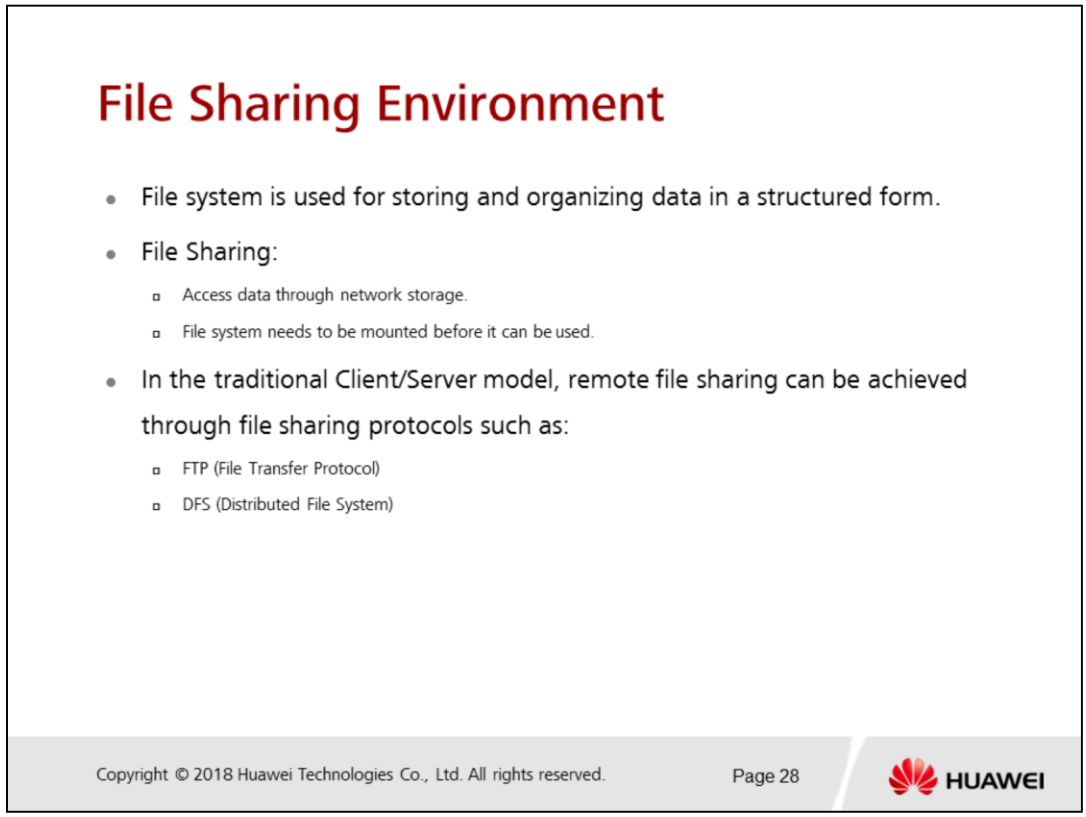
- A SAN storage solution has a high total cost of ownership (hardware and experienced IT personnel), so SAN is mostly used in medium or large enterprises. Data requirement of these companies are usually:
  - Has high requirement regarding the response time, reliability, scalability for critical database applications.
  - Centralized backups and high storage performance, and also data integrity and data reliability.



Contents

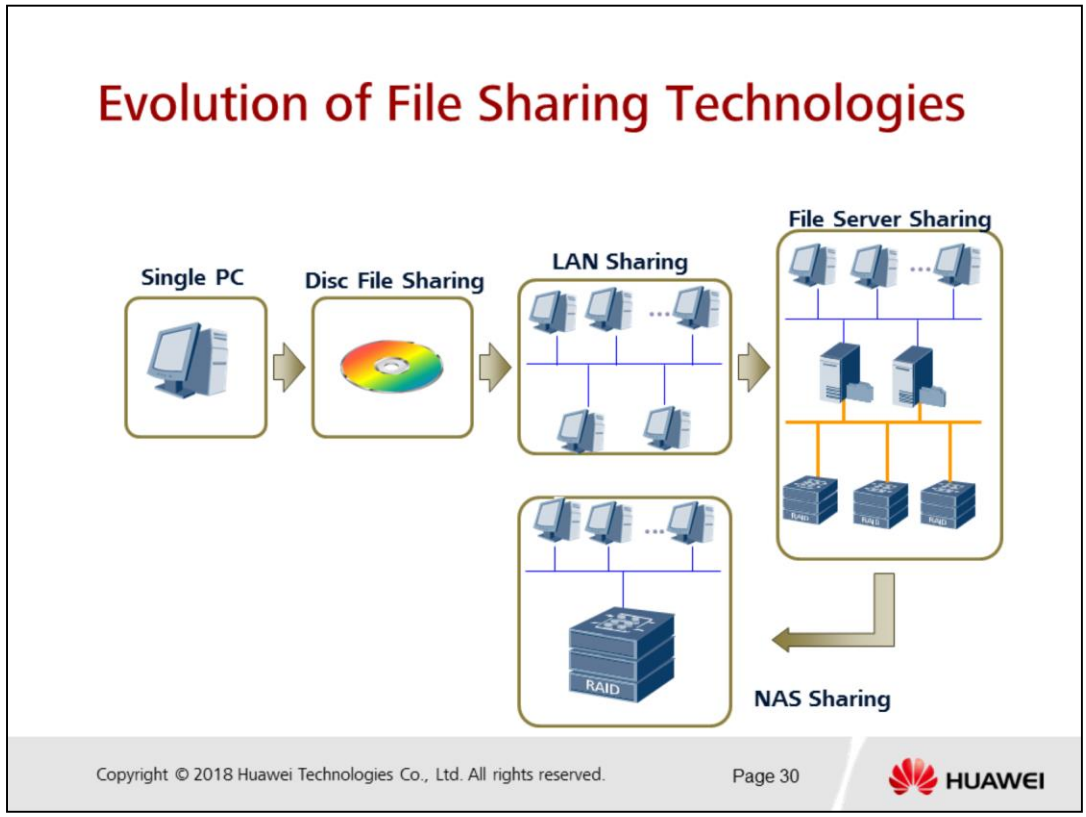
1. Classification of Network Storages.
2. DAS - Traditional Storage Technology.
3. SAN - Storage Area Network.
4. **NAS - Network Attached Storage.**

Copyright © 2018 Huawei Technologies Co., Ltd. All rights reserved.

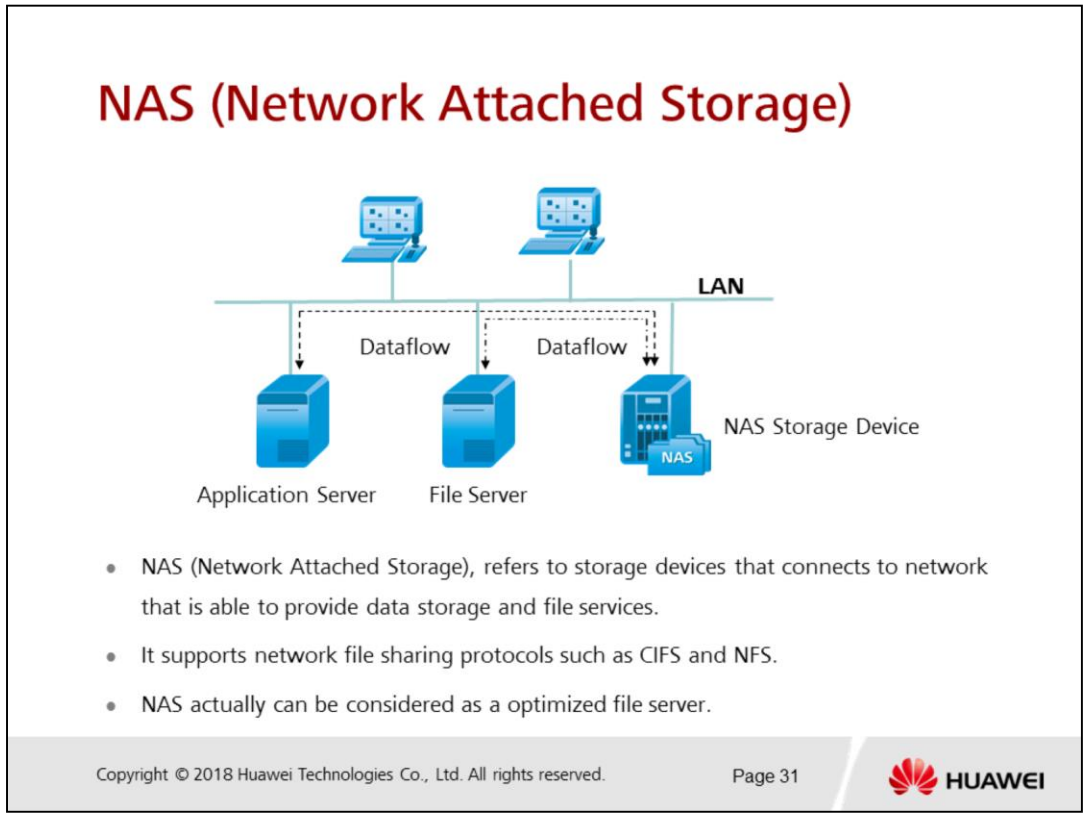


- File sharing involves data storage and access. In a file sharing environment, users who create files can specify file usage permissions (read, write, execute, append, delete, list) for other users and can control file changes. When files are shared, if more than one user accesses the same file at the same time, a method of protection is needed to maintain the integrity of the data. The method used in the traditional Client/Server (C/S) model is by implementing file sharing protocols and using Distributed File System (DFS). The following are some examples of these implementations:
    - File Transfer Protocol (FTP) allows the transmission of data in networks. It is a standard file transmission protocol, and uses TCP/IP protocol in the server end and client end of the data transmission process. FTP data are not encapsulated during transmission, which means that there is no security protection on the data transmission. FTP over Secure Shell (SSH) added the security protection features on top of the FTP protocol that allows data to be transmitted over the network securely without data security concerns compared to FTP.

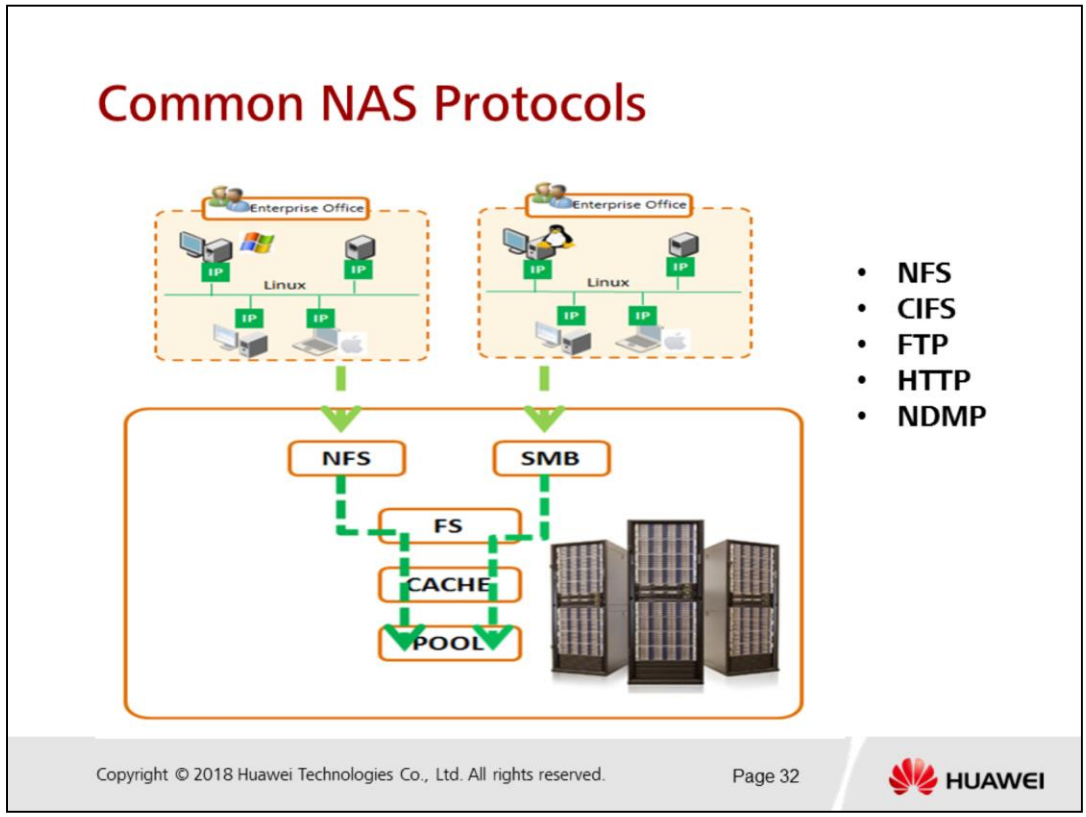
    - Distributed File System (DFS) allows the file system to be distributed across multiple hosts, allowing any host to access the entire file system. DFS provides highly efficient data management and data security protection. A distributed file system is a client/server-based application that allows clients to access and process data stored on the server as if it were on their own computer. When a user accesses a file on the server, the server sends the user a copy of the file, which is cached on the user's computer while the data is being processed and is then returned to the server.
- In the traditional C/S model, there is another mechanism for file sharing protocol to provide remote file sharing. In this model, a remote file system can be mounted on a client computer. The standard C/S file sharing protocol is NFS(Network File System) for UNIX operating system and CIFS (Common Internet File System) for Windows operating systems. For a specific user or group, the owner of the file can set access permissions as needed, such as read-only or write-only. In these two sharing protocol implementations, the user does not know where the file system is located.
- Other than that, naming systems such as DNS (Domain Name System), LDAP (Lightweight Directory Access Protocol)、NIS (Network Information Services) allows users to differentiate and access unique resources on the network. Naming service protocols creates a namespace which contains the unique name of each network resources and helps to differentiate between all the different resources available on the network.



- Back in the past, Kilobyte(GB) level file sharing floppy disk was widely used. However, as time progresses, the need for larger share volumes across organization increases, which lead to the inventions of removable storage media such as flash drive that is able to store data on Gigabyte(GB) level, which in turn fully replaced floppy disks over time.
- Enterprises needs to not only store large amounts of data, but also needs to share those data over networks, where NAS undoubtedly becomes a good choice. For servers and hosts, NAS is a external device that has great flexibility for over the network deployment. NAS also provides file based storage and not block based storage, which makes it easy for clients to access those data over the network.

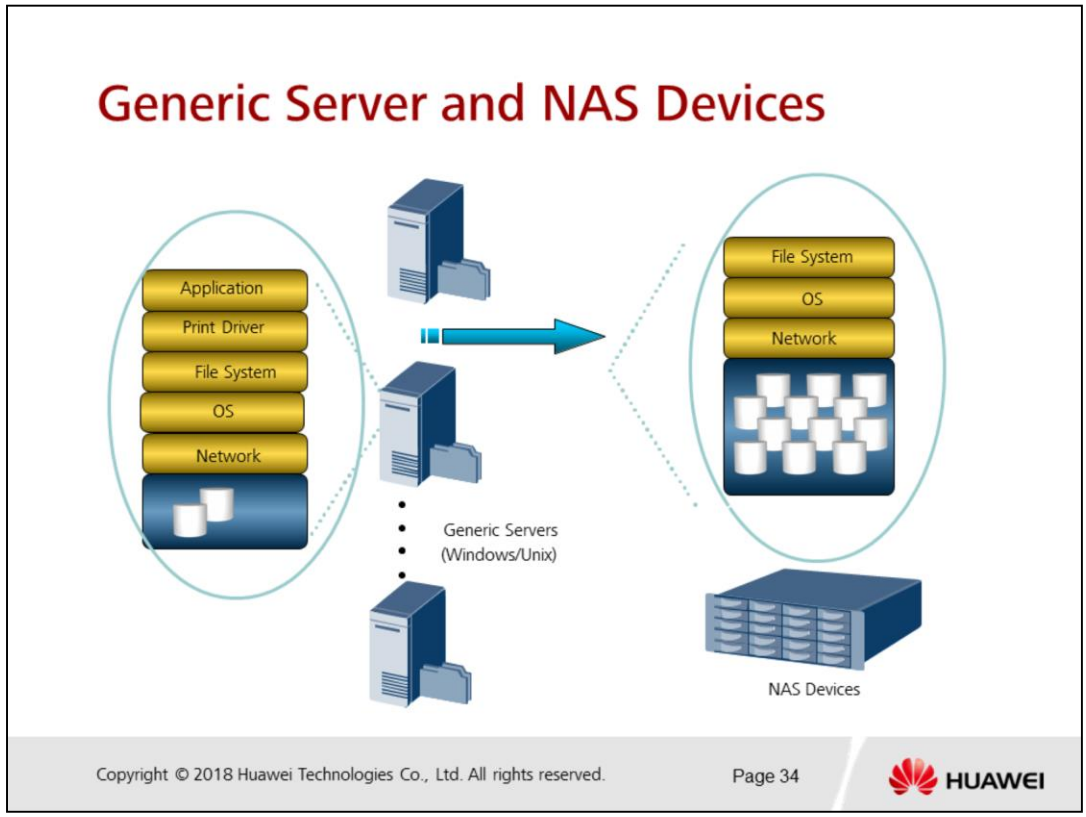


- NAS (Network Attached Storage) connects storage devices to an existing network to provide data and file services. NAS generally consists of several components such as storage hardware, operating system and a file system. It is based on the TCP / IP protocol to achieve file-level data access services.
- Instead of relying on a common operating system, NAS connects storage devices through a standard network topology, eliminating the need for a dedicated server to access the network. NAS uses a simplified user-oriented operating system designed for data storage with all the required protocols built in, therefore making the management and setup of the entire system relatively simple.
- NAS is mainly used for highly efficient file sharing services, which is suitable for scenarios where large capacity file transmission or sharing over the network is required.

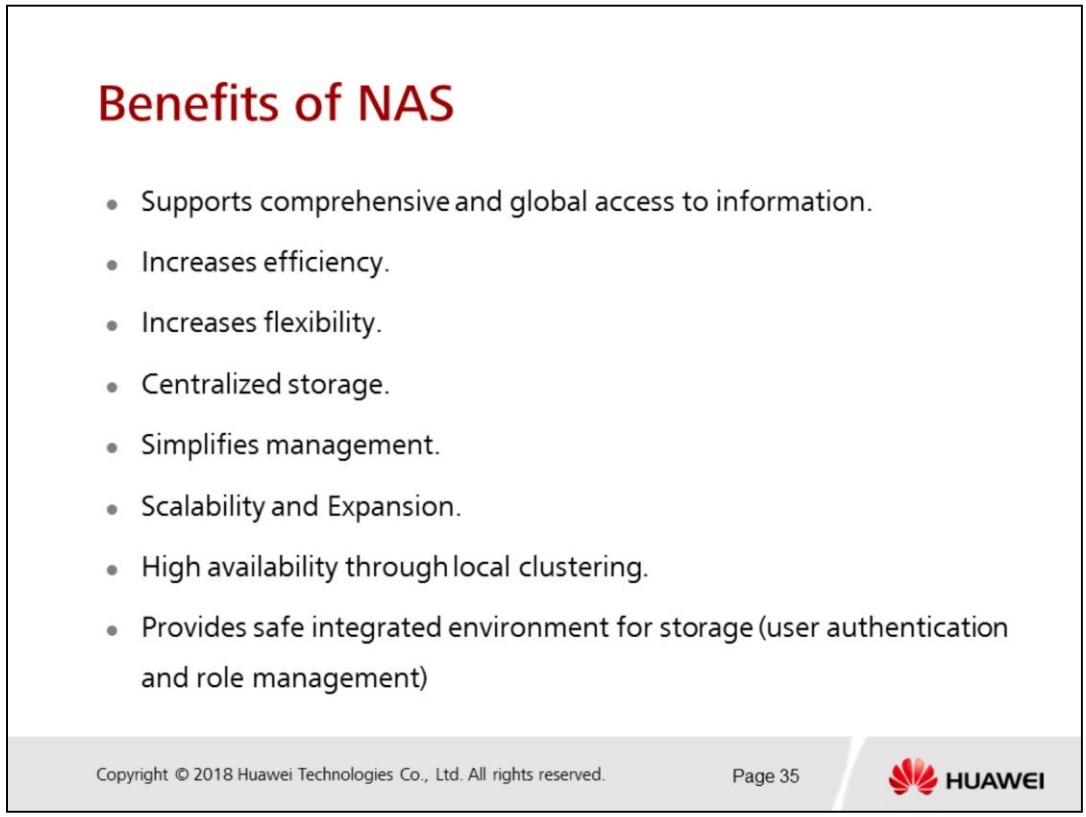


- CIFS (Common Internet File System), is a file sharing protocols that works under the Microsoft Windows environment, it is based on Server Message Block(SMB) protocol.
- NFS (Network File System) protocol is the traditional file sharing protocol under the UNIX operating system environment.
- Most NAS devices support multiple file service protocols to handle remote file system I/O requests. As mentioned earlier, NFS and CIFS are common file-sharing protocols. NFS is primarily used in UNIX-based operating environments; while CIFS is used in Microsoft Windows-based operating environments. These file sharing protocols allow users to share file data across different operating environments and provide users with transparent migration of files across operating systems.
- NFS is a client/server application that uses Remote Procedure Calls (RPCs) to communicate between computers. Users updates the files on the remote NAS as if they are updating files on their local storage.
- The user's system needs an NFS client to connect to the NFS server. Since, NFS servers and clients uses TCP/IP protocol to transmit files, the clients and server system must install the TCP/IP protocol stack before NFS can work properly.

- A user or system administrator can use NFS to mount a portion of any file system or portion of the file system (any portion of the directory or subdirectory hierarchy tree). The mounted file system has permissions to control access (for example, read-only or read-write permissions).
- CIFS is a network-based sharing protocol that requires high reliability of network transmission, so it usually uses TCP/IP. NFS is used for independent transport, so it uses TCP or UDP.
- The disadvantage of NFS is that it requires the clients to be installed with dedicated software. CIFS on the other hand is already integrated in the operating system and does not require additional software.
- NFS is a stateless protocol, and CIFS is a stateful protocol. NFS connection automatically resumes after connection failure, but CIFS can not automatically . CIFS sends only a bit of redundant information, so it has higher transmission efficiency than NFS.
- HTTP (Hypertext Transfer Protocol) is the set of rules for transferring files (text, graphic images, sound, video, and other multimedia files) on the World Wide Web. As soon as a Web user opens their Web browser, the user is indirectly making use of HTTP. HTTP is an application protocol that runs on top of the TCP/IP suite of protocols (the foundation protocols for the Internet). For example, the NAS devices control portal page uses HTTP protocols for remote management of NAS devices over the Internet.
- NDMP (Network Data Management Protocol) is an open protocol used to control data backup and recovery communications between primary and secondary storage in a heterogeneous network environment.
- NDMP specifies a common architecture for the backup of network file servers and enables the creation of a common agent that a centralized program can use to back up data on file servers running on different platforms. By separating the data path from the control path, NDMP minimizes demands on network resources and enables localized backups and disaster recovery. With NDMP, heterogeneous network file servers can communicate directly to a network-attached tape device for backup or recovery operations. Without NDMP, administrators must remotely mount the network-attached storage (NAS) volumes on their server and back up or restore the files to directly attached tape backup and tape library devices.



- Generic server refers to all the different types of servers such as web server, application server, web server, mail server and virtual servers. In this context, the diagram above shows that NAS devices are compatible and able to provide storage and file services universally to any type of servers as long as they support the same file system.
- NAS devices are optimized on the basis of common servers, hence they have the features such as file service, storage, search and retrieval, and access to client application files.
- As shown on the diagram, a generic server can be used to install any types of application, and it runs on a common operating system(OS). NAS differs from generic servers, it is solely dedicated for file services, and it provides file sharing to other operating system through standard open protocols. In order to increase the high availability performance of NAS devices, some NAS vendors even provides NAS clustering feature.
- NAS devices consist of the following components:
  - NAS controller (CPU and Memory Etc.)
  - One or more network interface cards (NIC) which provides network connectivity. For example, Ethernet and Gigabit Ethernet network cards.
  - An optimized operating system for NAS feature management.
  - File sharing protocols such as NFS and CIFS.
  - Disk resources that supports industry standard storage protocols such as ATA, SCSI, FC.
- NAS environment includes the clients that access NAS devices through IP network using standard protocols.



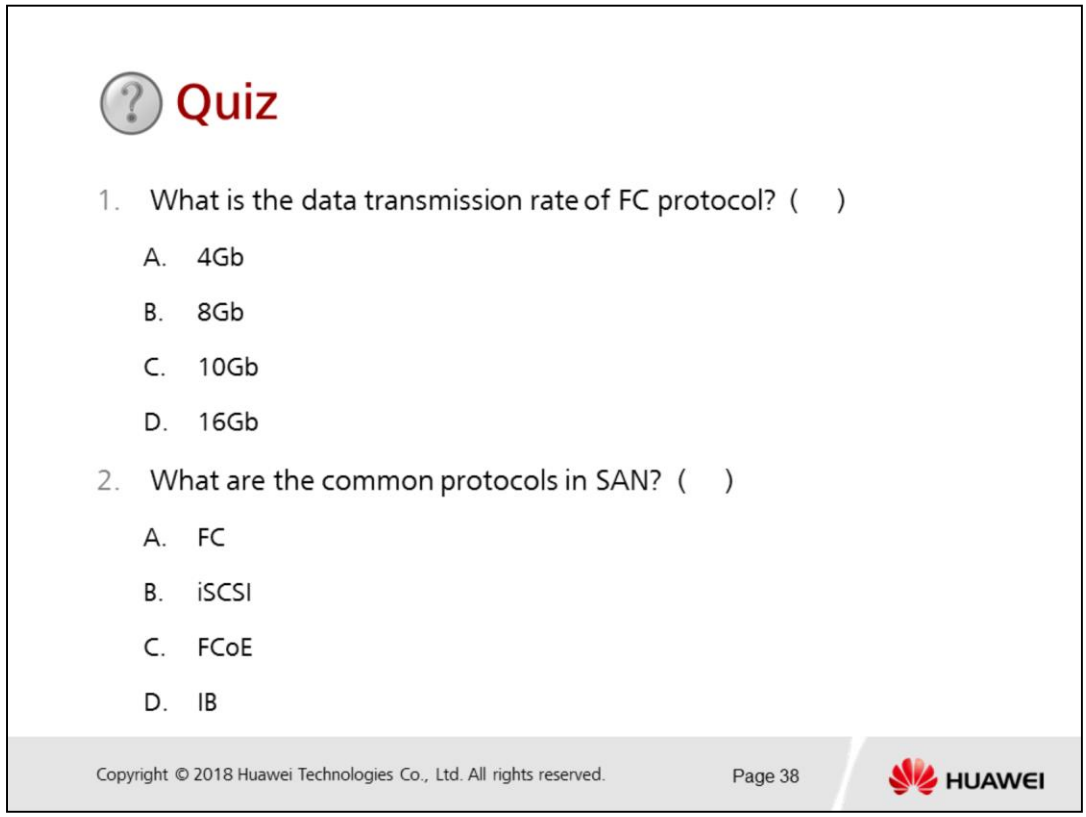
- NAS provides the following benefits:
  - Supports comprehensive global access to information: NAS provides high efficiency file sharing, and supports many to one or one to many configuration. Many to one configuration allows the NAS to be accessed by multiple clients simultaneously, while one to many configuration allows a single client to connect to multiple NAS devices.
  - Increases efficiency: NAS devices provides dedicated optimized OS for file services, which can lower file service operation through file servers, increases the utilization ratio of generic servers, and eliminates the bottleneck faced by generic servers when accessing files.
  - Increases flexibility: NAS uses industry standard protocols, and has great compatibility with Windows and Unix clients. It can flexibly provide file services to different types of clients that accesses the same resource.
  - Centralized Storage: NAS allows storages to be centralized and minimize the data duplication on client workstations, simplifies data management and provides higher data protection.

- Simplifies management: NAS provides centralized management through a control platform, which allows effective local files system management.
- Scalability and expansion: Based on different utilization ratio configuration and service applications, high performance and low latency expansion of storage can be achieved.
- High availability through local clustering: NAS devices can use clustering technology for service failover. NAS uses redundant network components, multiple connection options to eliminate single point of failures. It has rich options for data replication and data restoration to achieve high availability data storage.
- Security: NAS ensures data security through implementations of user authentication, file locking and user role management that fits into the industry standard data safety architecture.

Summary

- This module mainly introduces:
  - Data Center Storage Network.
  - Network Architecture of DAS, SAN and NFS.
  - Advantages and Disadvantages of DAS, SAN and NFS Network Technologies.

Copyright © 2018 Huawei Technologies Co., Ltd. All rights reserved.



- Answers:
  - ABD.
  - ABC.

Thank You

www.huawei.com