

NAS Storage

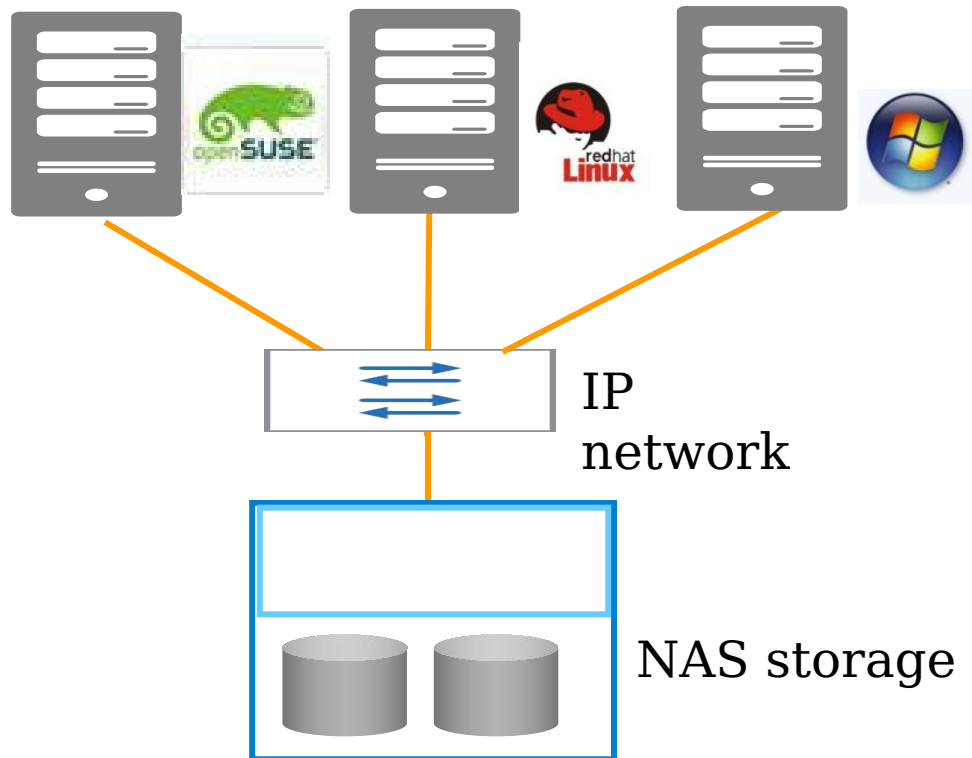


Contents

1. **NAS Overview**
2. NAS Technology
3. NAS Products
4. NAS Applications

What Is NAS?

NAS, or network attached storage, is a framework that shares storage resources over a network and acts as a file server for file access.



Features:

- Easy to use, no need for dedicated IT experts
- Cost-effective, using IP switches
- Secure and reliable
- Easy data backup and recovery

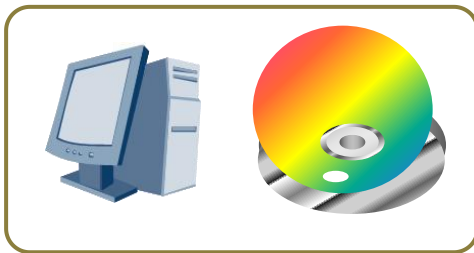
History of NAS

The development of the Internet has created a need for unstructured data sharing, giving rise to the popularity of NAS storage.

1946 - World's first computer, but no network.



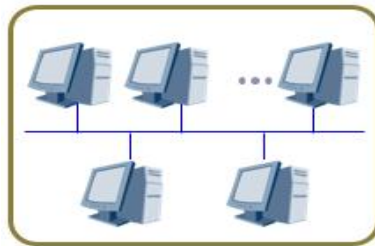
Media sharing
FD, CD, HDD, USB



1974 - Invention of TCP/IP.
1979 - Duke University first implemented file sharing without media.



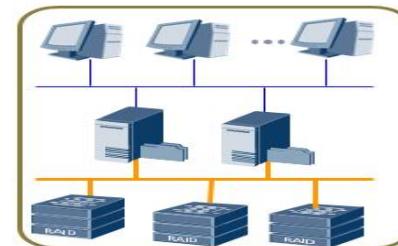
File sharing and directory



1984 - Sharing of network servers achieved by IBM, Novell, Microsoft, and 3Com.



File sharing server



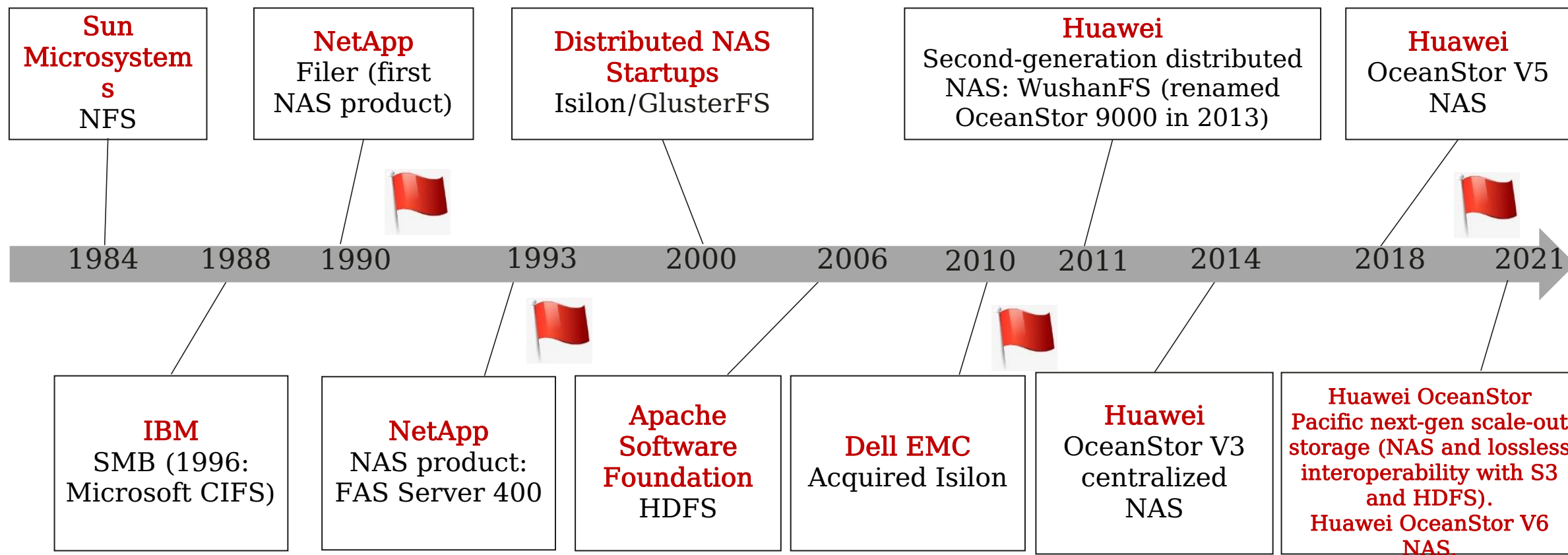
1990 - The Internet connected commercial and enterprise networks.



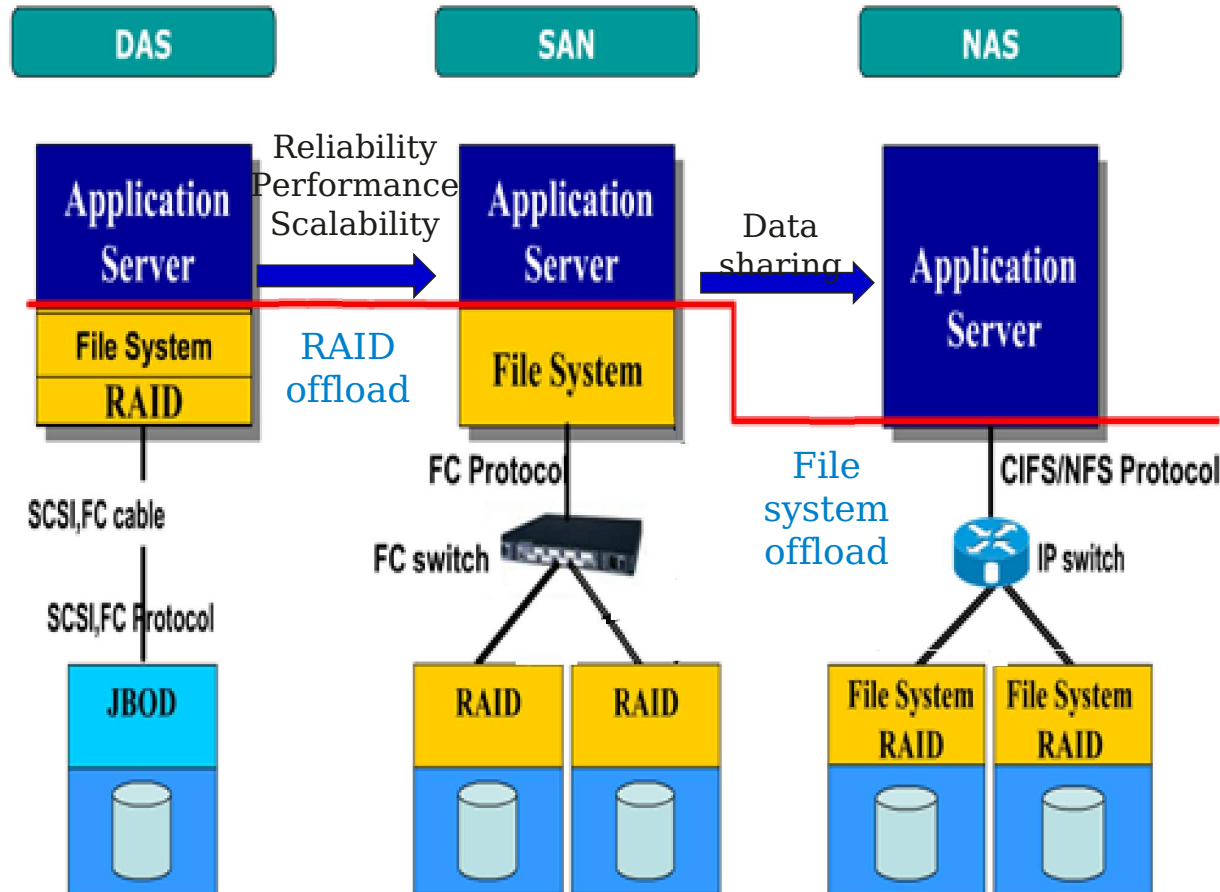
NAS storage



NAS Evolution



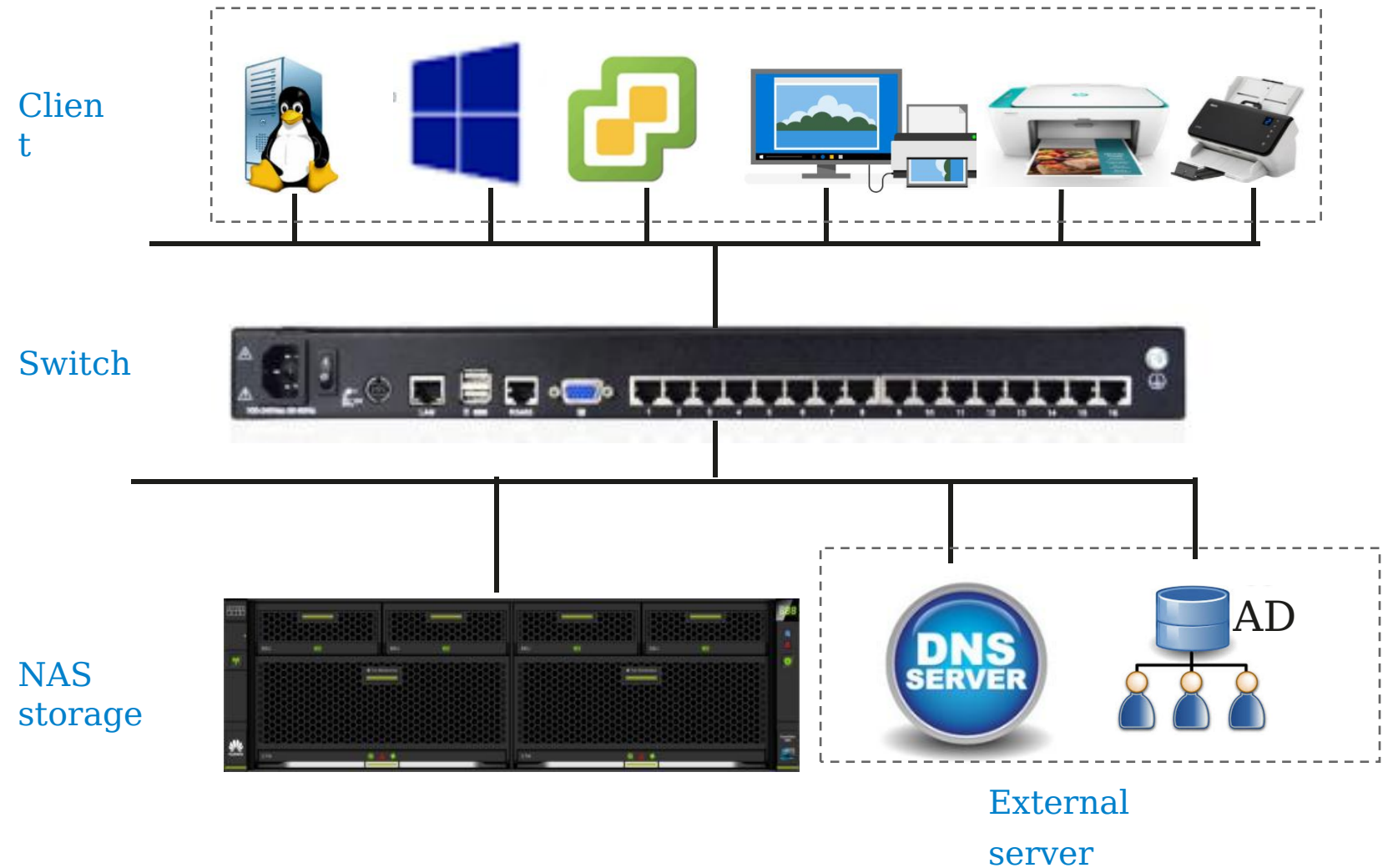
Differences Between DAS, SAN, and NAS



Item	DAS	SAN	NAS
Network	Direct connection	Dedicated SAN	LAN
Protocol	SAS, ATA, SCSI	FC, iSCSI, SCSI	NFS, CIFS
Data package	Block	Block	File
HBA	SAS HBA	FC HBA and iSCSI client	GE, 10GE
Data sharing	Low	High	Highest
Scenario	Small-scale servers	Database and VMware	File sharing, archiving, and backup
DR solution (complexity)	Low	High, dedicated	High
Capacity	Low	High	High

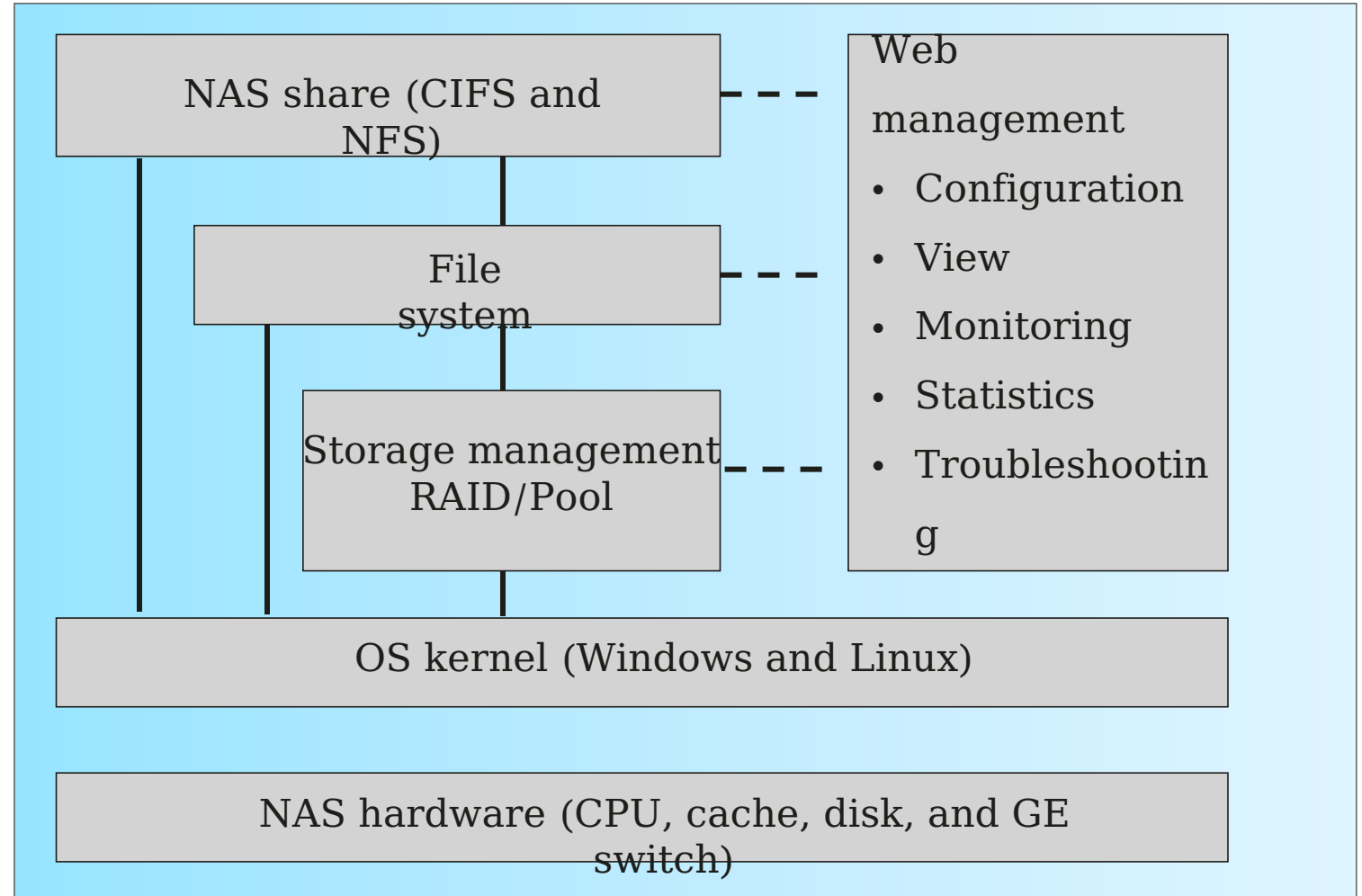
NAS Components

- **NAS storage**
- **External server**
 - a. DNS server
 - b. AD/LDAP server
- **IP switch**
- **NAS client**
 - a. Server/Mainframe
 - b. Computer
 - c. Printer
 - d. Scanner



NAS Storage Software

- **OS kernel**
 - a. Windows
 - b. Linux
- **Storage management**
 - a. RAID 0, 1, 10, 5, 6, 50
 - b. EC ($N+M$)
 - c. Multi-copy
- **File system**
 - a. OceanStor FS
 - b. Quota and WORM
- **NAS share**
 - a. CIFS, NFS, FTP, and HTTP
- **Web management**

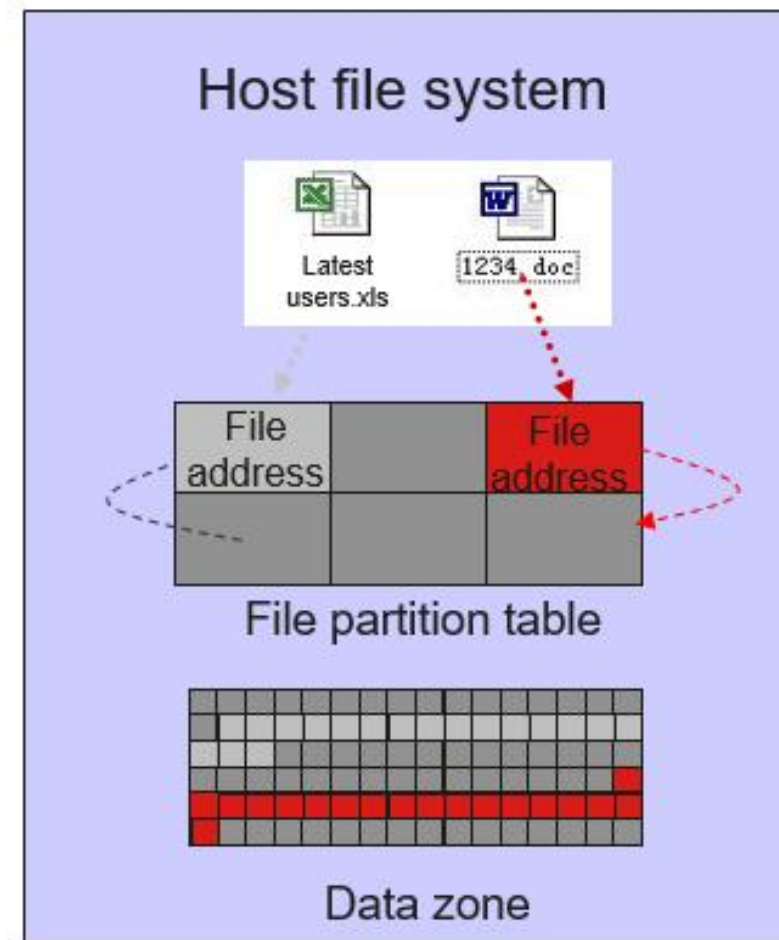


File System

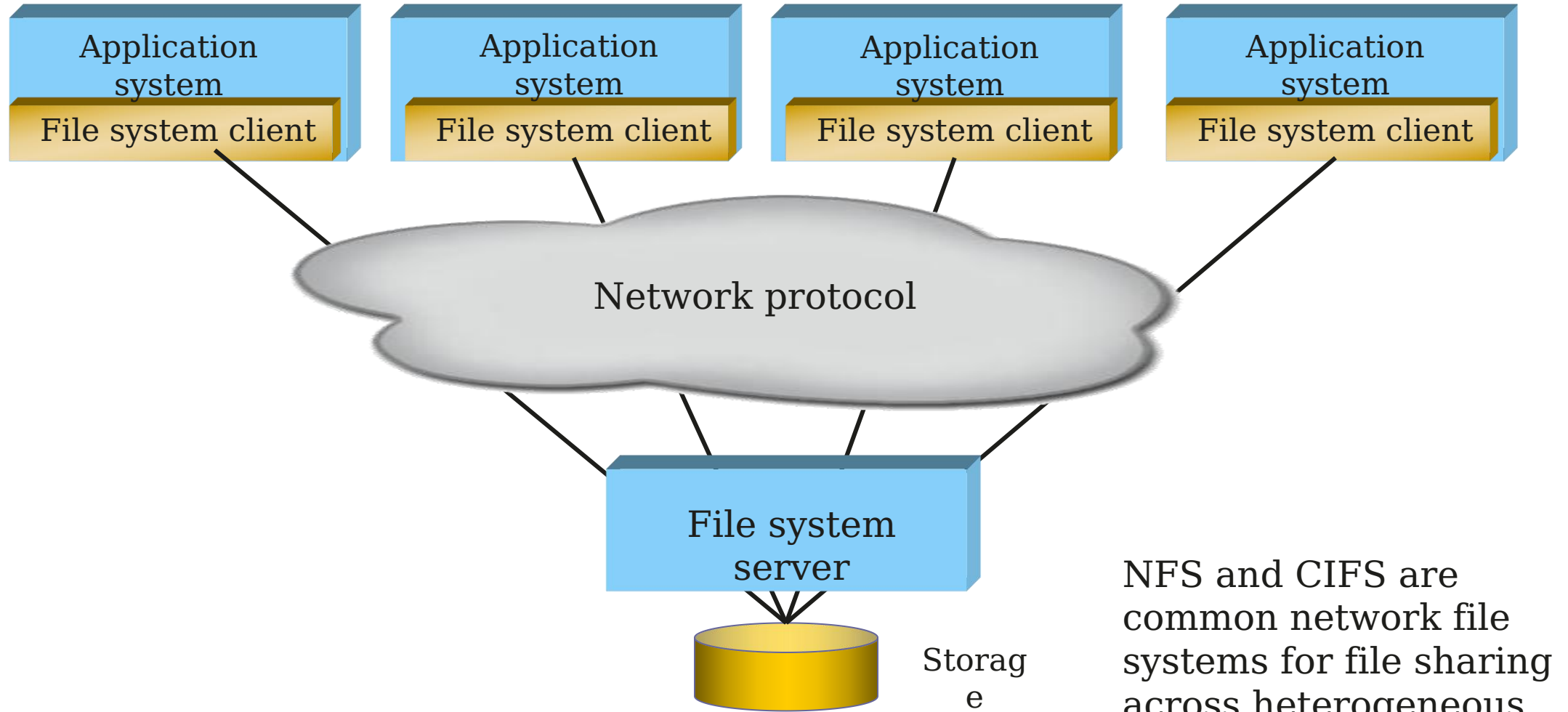
File system: defines the data structure and management for files stored on disks.

To enable data access on disks, a logical data storage structure, such as a file system, must be established between associated sectors.

The process of creating a file system on disks is called formatting.



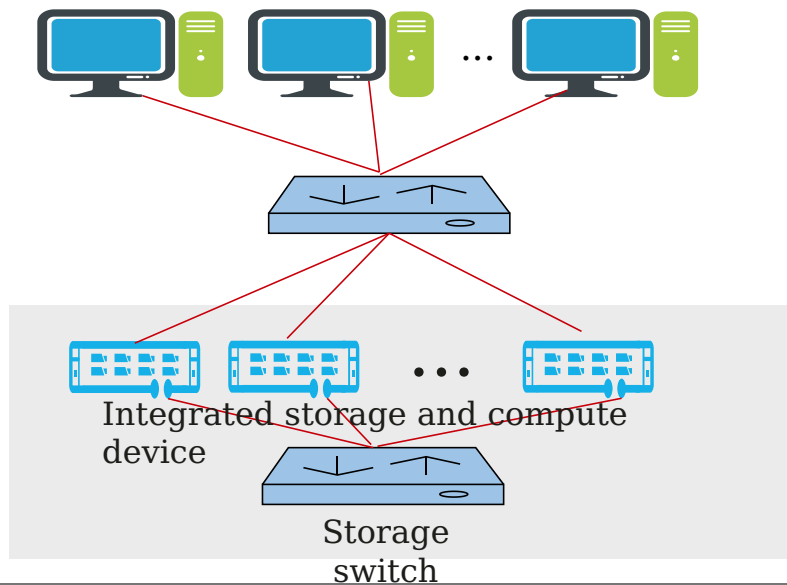
Network File System



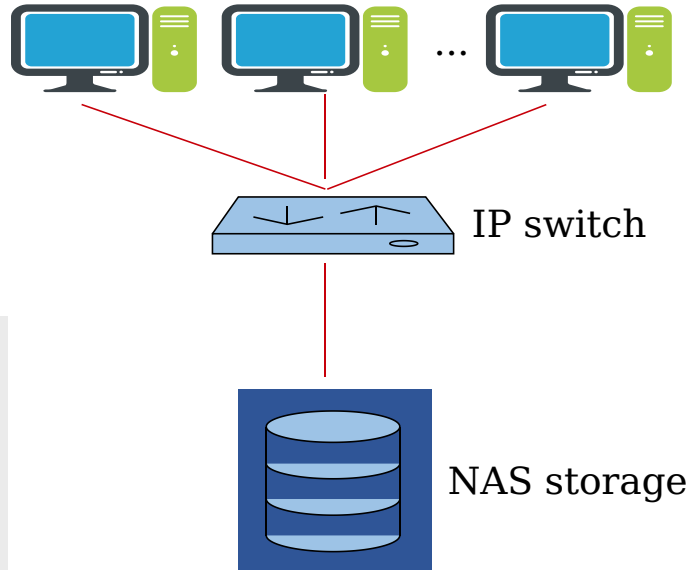
NFS and CIFS are common network file systems for file sharing across heterogeneous platforms.

Three Types of NAS Devices

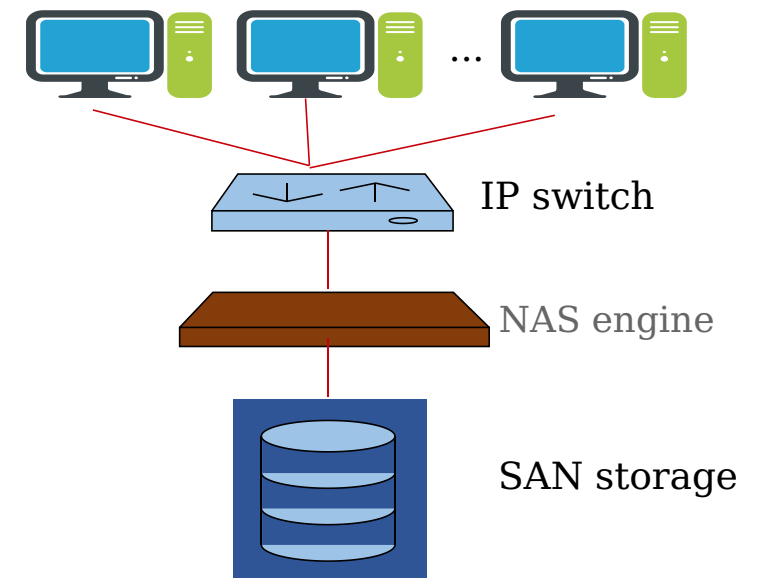
Distributed NAS



Centralized NAS



Gateway NAS



NAS Type	Device Model	Scale-out	RAID/EC	Scenario	Main Product	Huawei
Distributed	Integrated compute and storage device (x86 server), no independent controller or gateway	Up to 4000	EC ($N+M$)/Multi-copy	Cloud and big data	Dell EMC PowerScale Ceph	OceanStor Pacific
Centralized	Controller + disk (capacity expansion)	≤ 24	General RAID	File sharing, archiving, and backup	NetApp FAS/AFF Dell EMC Unity	OceanStor Dorado/OceanStor hybrid flash storage
Gateway	NAS gateway + SAN storage	≤ 4	SAN-based RAID	File sharing, archiving, and backup	HDS HNAS IBM	OceanStor Dorado V3 (EOM)

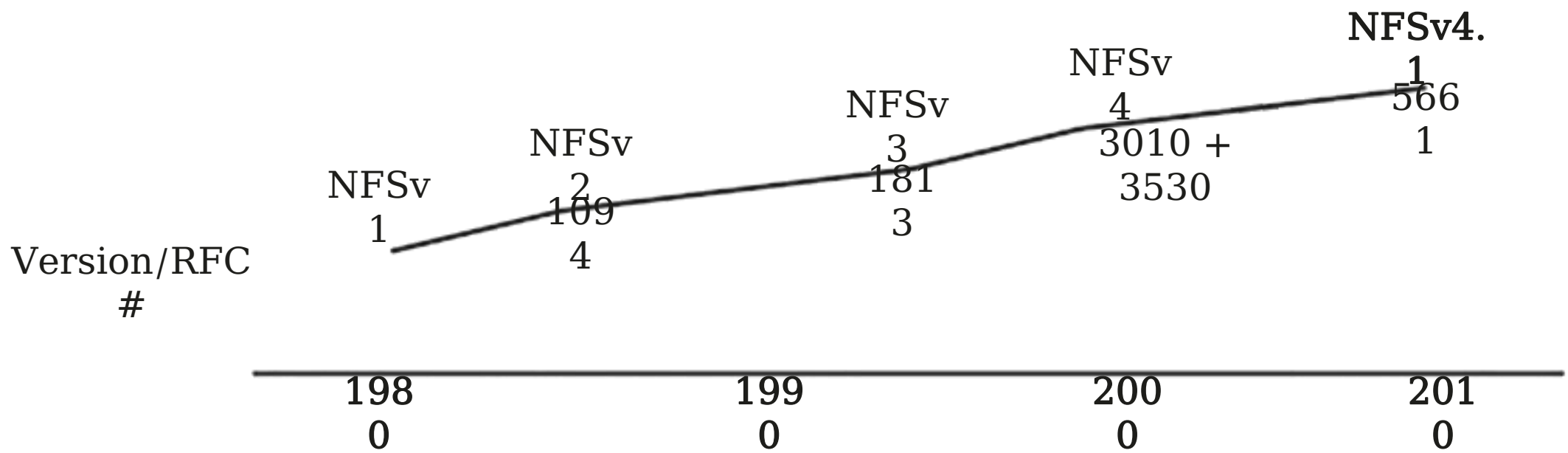
Contents

1. NAS Overview
- 2. NAS Technology**
3. NAS Products
4. NAS Applications

NFS

Network File System (NFS) is a distributed file system protocol developed by Sun Microsystems (Sun) in 1984. It is an open standard defined in a Request for Comments (RFC), which means anyone can implement the protocol.

In 2003, Sun Microsystems transferred NFS protocol development to the **Internet Engineering Task Force (IETF)**.





NFS Evolution

NFSv2 (RFC 1094)

- 1.UDP only
- 2.Stateless
- 3.2 GB file read and write
- 4.NLM-dependent lock mechanism

NFSv3 (RFC 1813)

- 1.UDP and TCP
- 2.64-bit files
- 3.Asynchronous write (commit)
- 4.READDIRPLUS
- 5.More info in file properties to prevent repetitive interaction
- 6.Client authentication

NFSv4 (RFC 3530)

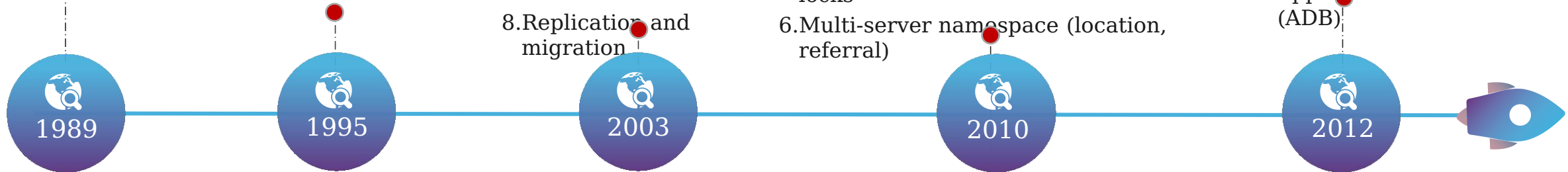
- 1.TCP only
- 2.State mechanism
- 3.Client cache
- 4.NFS server namespace (virtual root directory)
- 5.Kerberos authentication
- 6.NFS ACL
- 7.File locking and share reservations
- 8.Replication and migration

NFSv4.1 (RFC 5661)

- 1.Enhanced agents
 - a.Directory lease
 - b.Optimized reapplication and denial agent operations
 - c.File/directory notification mechanism
 - d.Clients' agent selection
- 2.Session and multichannel mechanism
- 3.ACL enhancement
- 4.Data retention
- 5.Notification of availability of byte-range locks
- 6.Multi-server namespace (location, referral)

NFSv4.2

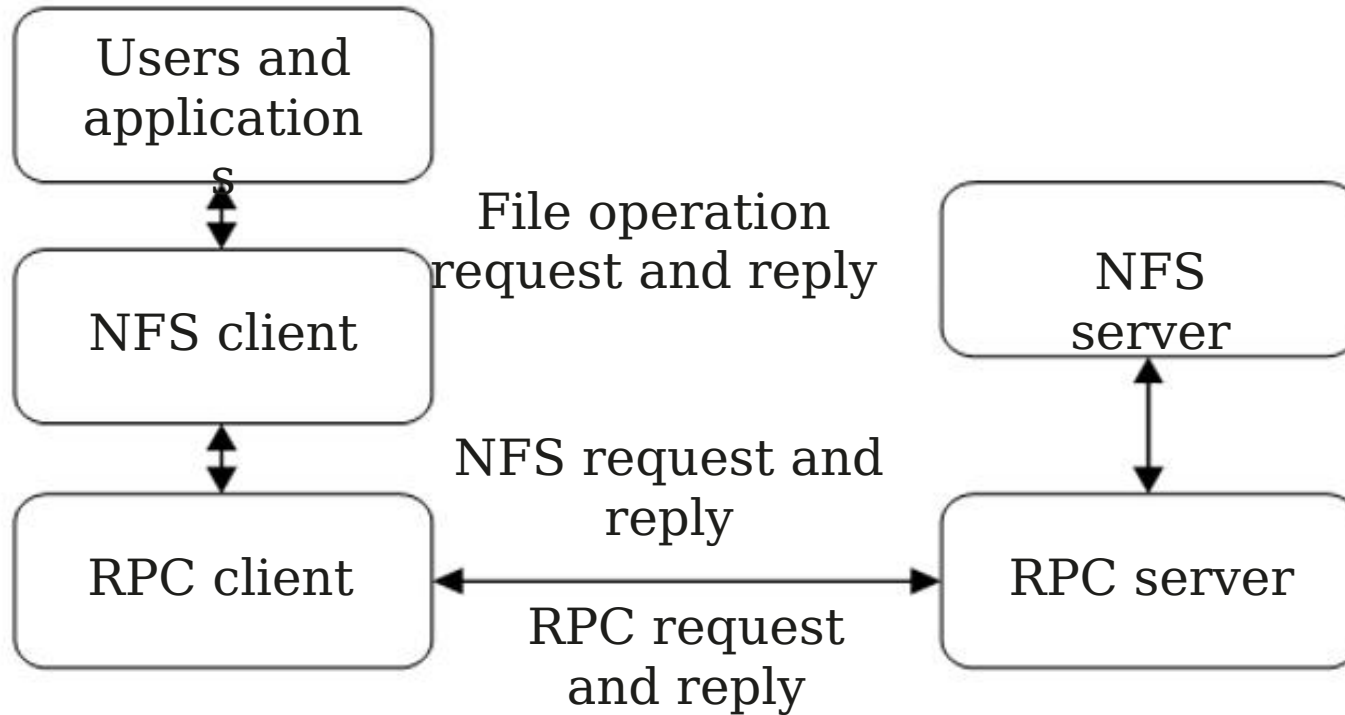
- 1.Application I/O hints
- 2.VAAI and ODX applications: server offload read and write
- 3.MAC: labeled NFS
- 4.Space reservation
- 5.Sparse files
- 6.Application Data Block (ADB)



Operating System	Release Date/Period	NFSv3	NFSv4	NFSv4.1
VMware ESXi 6.0-7.0	2015-09-10	Y	N	Y
Red Hat 4.0-6.3	2005-2012	Y	Y	N
Red Hat 6.4-8.3	2013-2020	Y	Y	Y
SUSE 9-11 SP2	2004-2012	Y	Y	N
SUSE 11 SP3-15 SP2	2013-2020	Y	Y	Y
CentOS 4-6.3	2005-2012	Y	Y	N
CentOS 6.4-8.3	2013-2020	Y	Y	Y

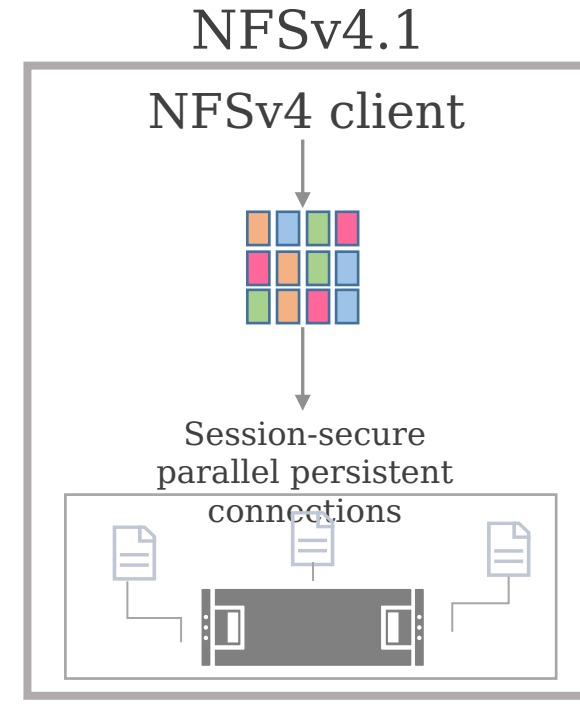
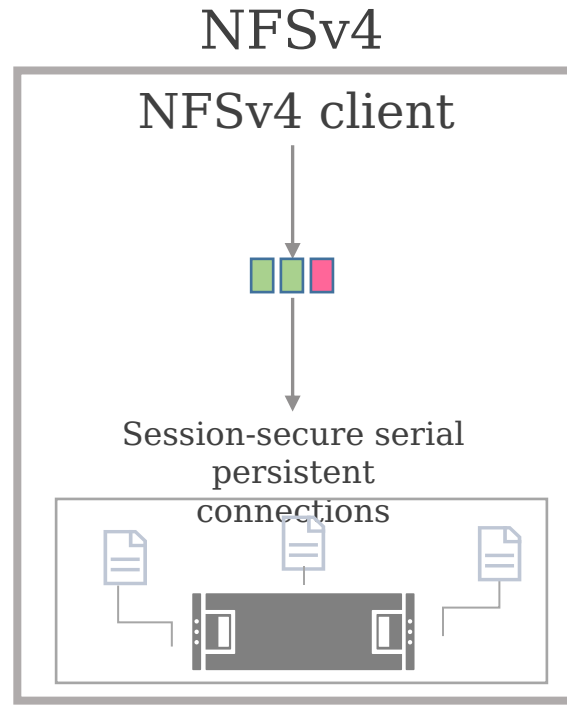
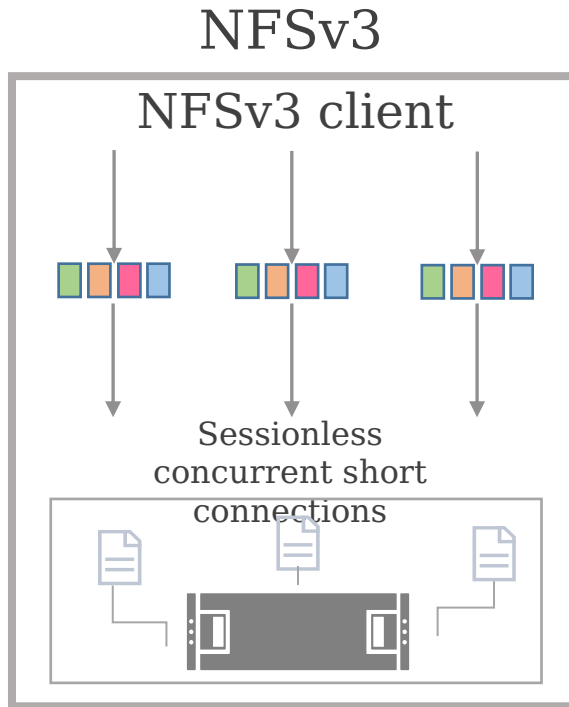
NFS Working Principles

NFS implements remote communication based on the Remote Procedure Call (RPC) protocol. RPC uses the client-server model.



1. The RPC client sends a call request with parameters to the RPC server and waits for a response.
2. Upon receipt of the call request, the RPC server obtains the process parameters, outputs the calculation results, and sends the reply to the client.
3. The RPC client receives the reply and obtains the call results.

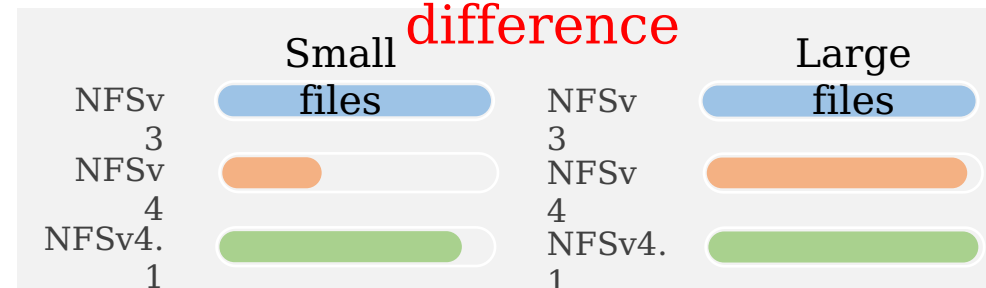
NFS Version Differences



Security difference

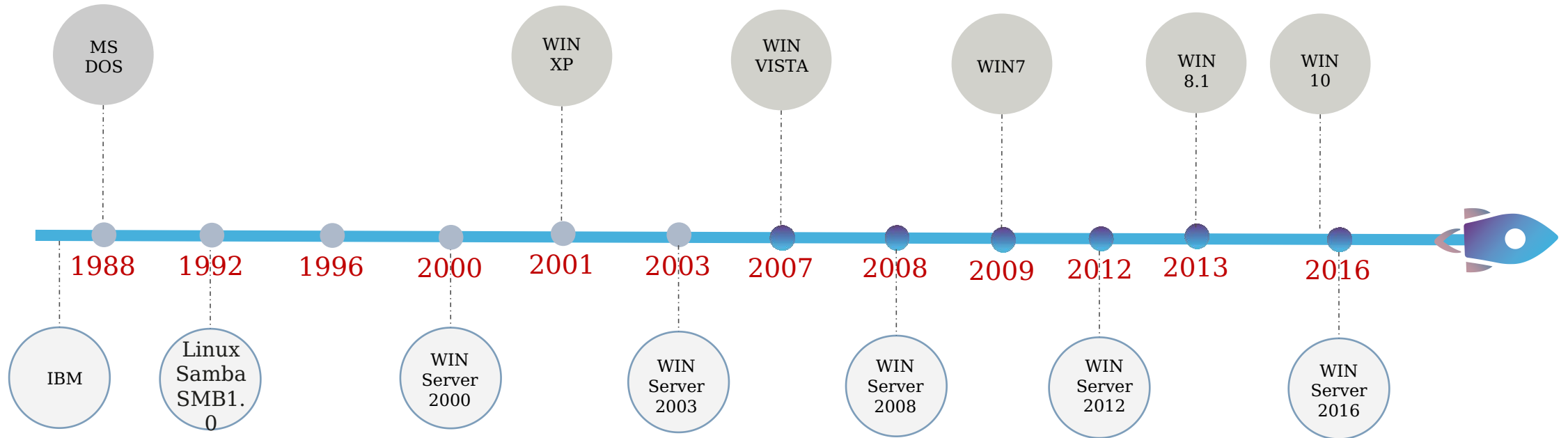
Performance difference

Item	NFSv3	NFSv4	NFSv4.1
User authentication	Host-based local authentication	Kerberos authentication	Kerberos authentication
Client control	IP address, IP address segment, host name, or network group name		
File permission control	UGO permission	ACL permission	ACL permission



SMB Evolution

- **Server Message Block (SMB)** is a protocol for network file sharing. One of the most popular versions is Microsoft SMB.
- The **Common Internet File System (CIFS) Protocol** is a dialect of SMB. Both SMB and CIFS are also available on ESXi, Unix, Linux and Mac.



Operating System	Release Period	SMB1.X	SMB2.X	SMB3.X
Windows XP, Windows 2000, Windows Server 2003	2000-2003	Y	N	N
Windows Vista, Windows Server 2008, Windows 7	2007-2009	Y	Y	N
Windows Server 2012, Windows 8.1, Windows 10, Windows Server 2016	2012-2016	Y	Y	Y

NFS vs. CIFS/SMB

Item	NFS	CIFS/SMB
Accessing Operating System	Linux, Unix	Windows
Development Group	IETF	Microsoft
Security Authentication	Client IP, domain user	Local user, domain user
Supported Domain System	NIS, LDAP	AD
Session State	Stateless	Stateful
Transport Protocol	TCP, UDP	TCP

HDFS

HDFS (Hadoop Distributed File System) was designed and developed based on a Google File System (GFS) paper. In addition to the features of other distributed file systems, HDFS provides:

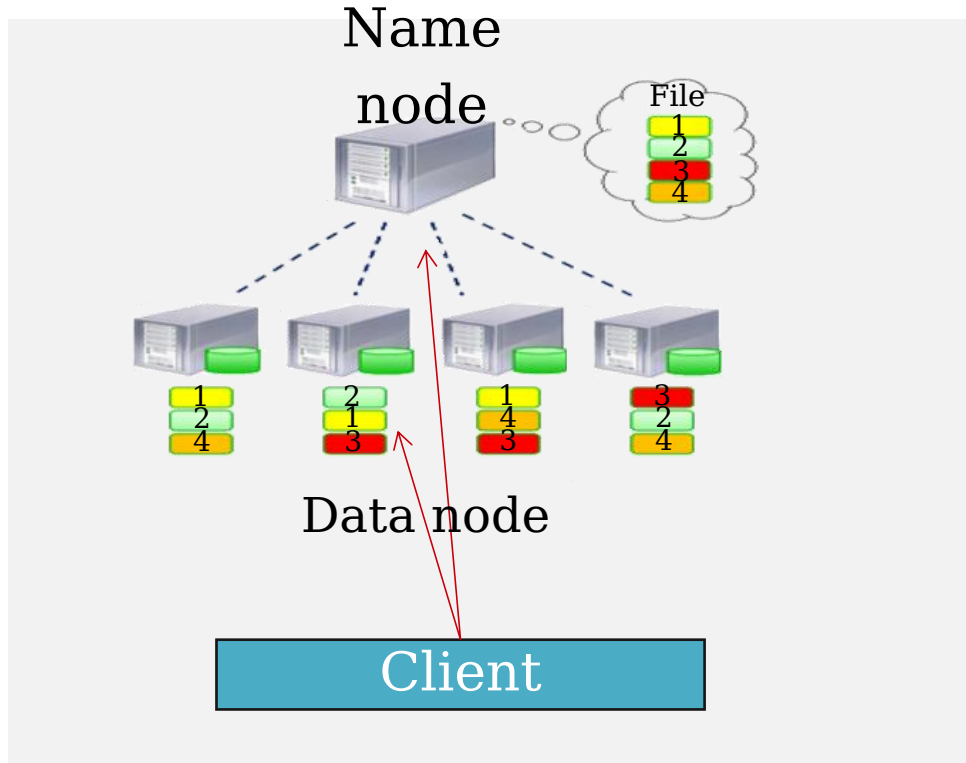
- High error tolerance: Hardware is considered always unreliable.
- High throughput: High throughput support is provided for applications that have massive amounts of data access.
- Large file storage: Data storage at the TB or PB level is supported.

HDFS is suitable for:
Large file storage and stream data access

HDFS is not suitable for:
Random writing of a large number of small files and low-latency read

Who is using HDFS

Hadoop HDFS Architecture



Hadoop HDFS component

HDFS mainly works in active/standby mode, with its architecture consisting of three components: name node, data node, and client.

- Name node
 - Stores and generates metadata for a file system
 - Runs one instance
- Data node
 - Stores the actual data and reports blocks it manages to the name node
 - Runs multiple instances
- Client
 - Supports service access to HDFS and obtains data from the name and data nodes and sends it to services
 - Runs multiple instances together with services

Hadoop file management

- A file is split into blocks (default size: 64 MB), and each block has **multiple copies** stored on different machines. The number of copies can be specified (default: 3) when the file is being generated. This ensures data reliability.
- A file cannot be modified after being created, written, or closed.

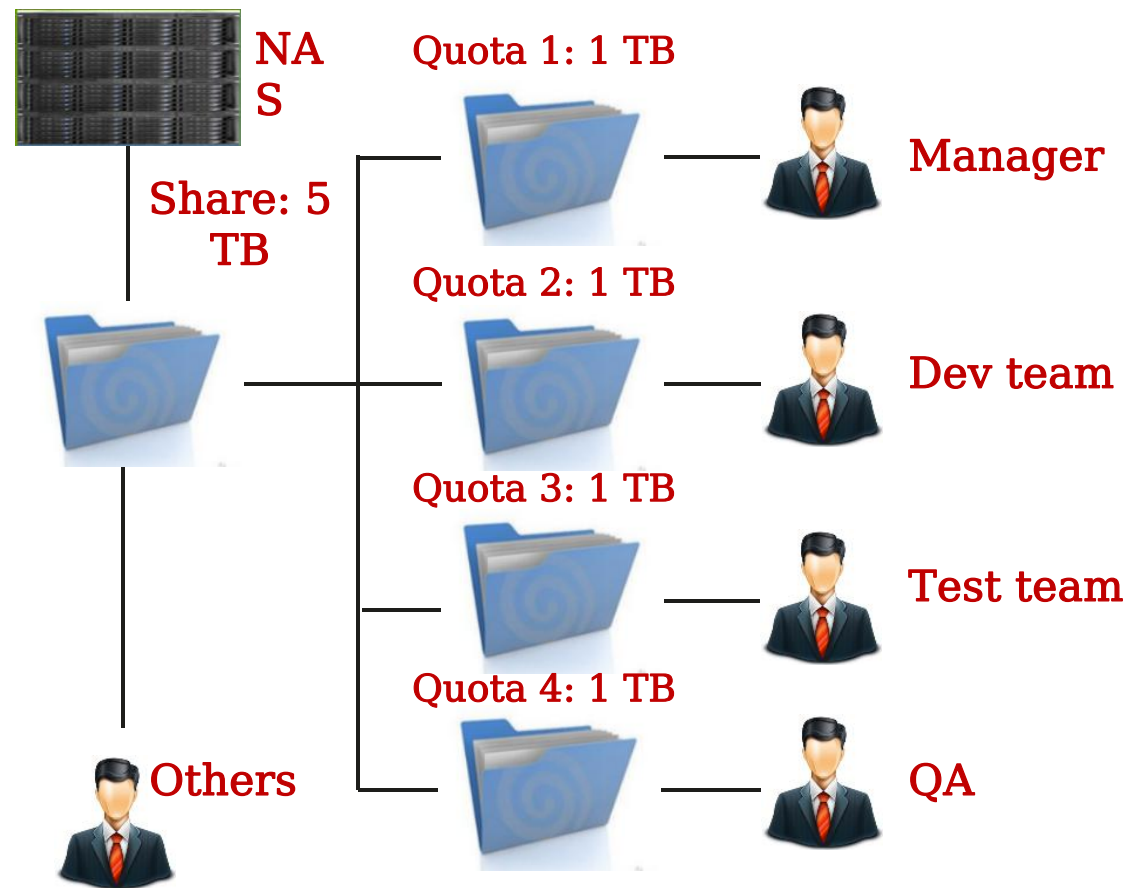
Quotas

Problem: With rapid growth in information assets and file sharing, storage space management is becoming more and more complex.

When multiple users access a shared directory, some users will overuse the space and others will not even be able to use it. In the worst cases, the entire system will run abnormally.

Solution: Quota mechanism

By limiting the file capacity or number of users, users can be prevented from occupying excessive storage resources, thereby improving system reliability.

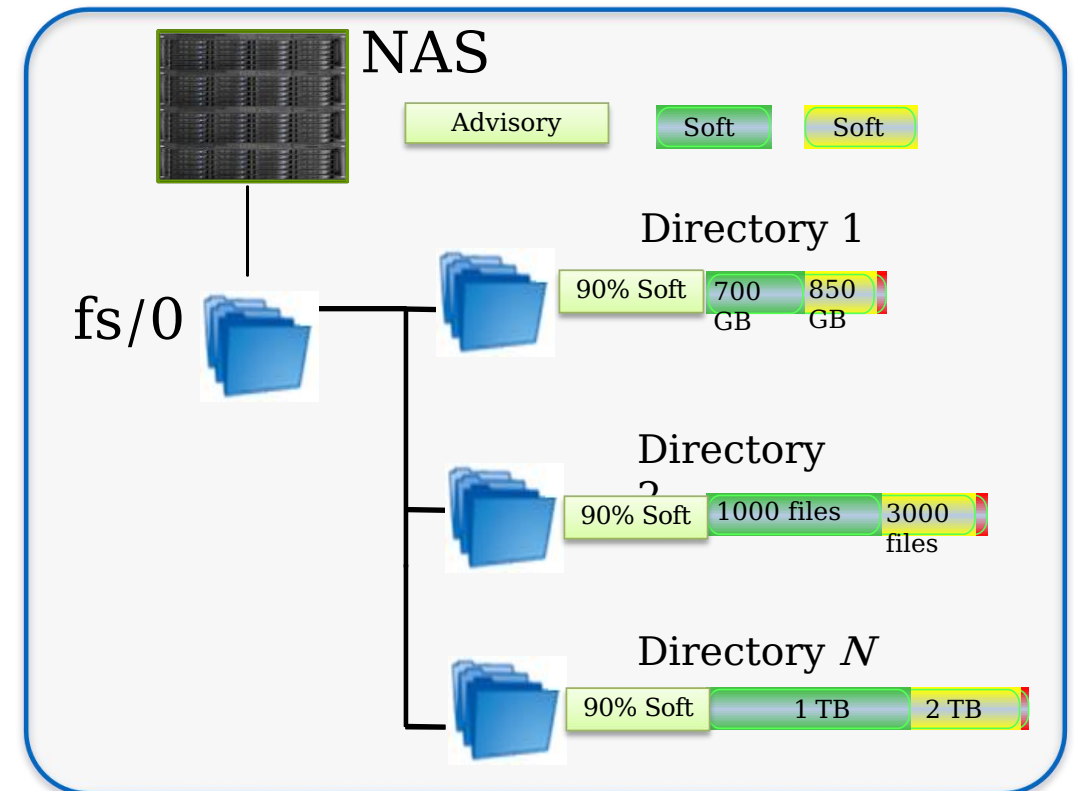


Quota Levels

Three Quota Levels

Level	Threshold	I/O Restriction
Hard Quota	High	Denying I/O operations and reporting alarms
Soft Quota	Middle	Reporting alarms and allowing data writes during a grace period, restricting data writes immediately after the expiration
Advisory Quota	Low	Only reporting alarms and not restricting writes

Example



Quota Working Principles

Quota Support Matrix

Dimensions

- Capacity
- File quantity

Objects

- Directory
- User
- User group

Resource	Level	Directory	User	User Group
Capacity	Advisory quota	Y	Y	Y
	Soft quota	Y	Y	Y
	Hard quota	Y	Y	Y
File quantity	Advisory quota	Y	Y	Y
	Soft quota	Y	Y	Y
	Hard quota	Y	Y	Y

WORM

Write Once Read Many (**WORM**) is a **data protection mode**. After data is written, the file enters the protection mode through manual setting or after a certain period of time.



What applications support WORM?

CD/DVD-ROM, electronic exam, electronic contract, and archive
 Others?





Differences between WORM files and common files

Operation	WORM File	Common File
Read	✓	✓
Modify	✗	✓
Delete	✗	✓
Rename	✗	✓

WORM Modes

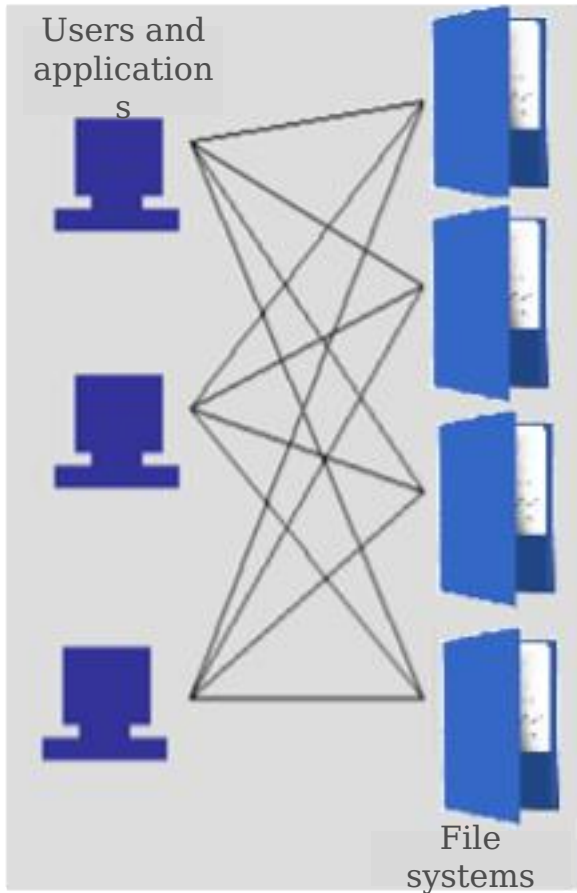
- **Enterprise WORM:** Allows administrators to flexibly manage files. This mode is mainly used for internal enterprise control.
- **Compliance WORM:** Enables enterprises to protect data in compliance with laws and regulations, so to prevent legal risks when archiving confidential documents.

Mode Differences

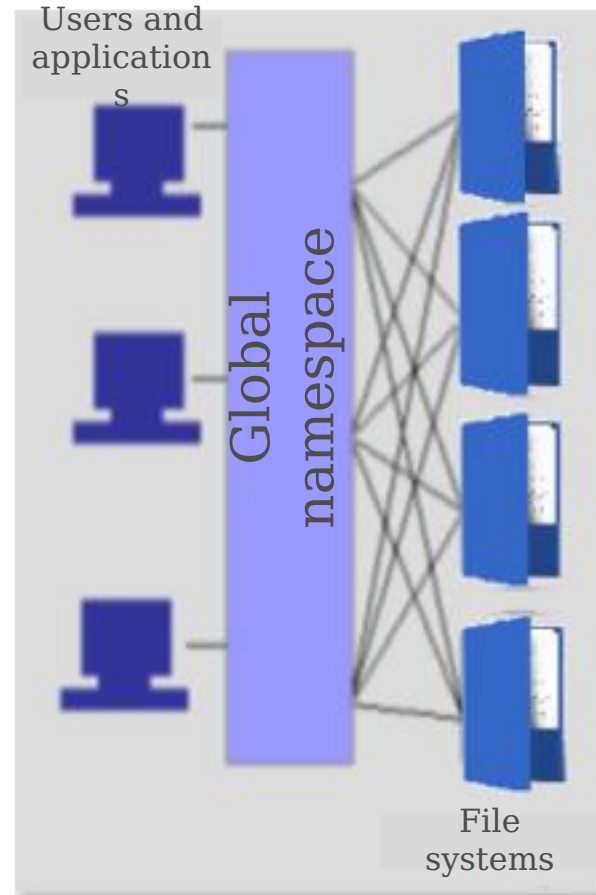
Operation	Enterprise WORM	Compliance WORM
Privileged deletion		
SEC 17a-4 compliance		

Global Namespace

NAS Nightmare



Solution: Global Namespace (GNS)



- **File virtualization:** Aggregates file systems and provides unified namespace.
- GNS allows clients to access files even if they do not know the location of discrete files, similar to accessing a website without knowing its IP address.

DNS

- **DNS**

The domain name system (DNS) is a network service that translates domain names into IP addresses.

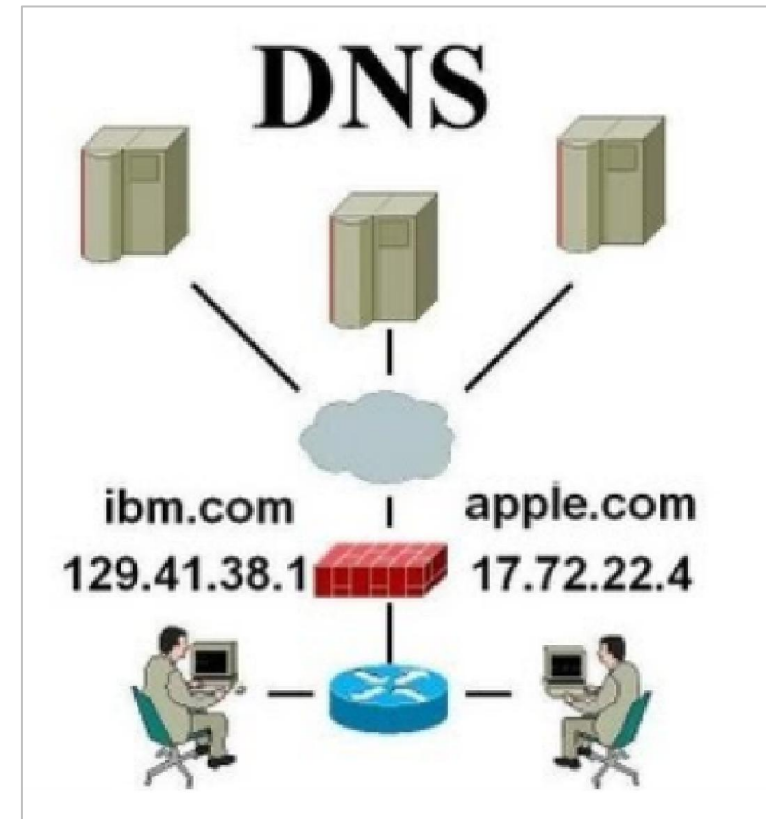
- **DNS Server Functions**

- ✓ Domain name resolver
- ✓ Load balancing

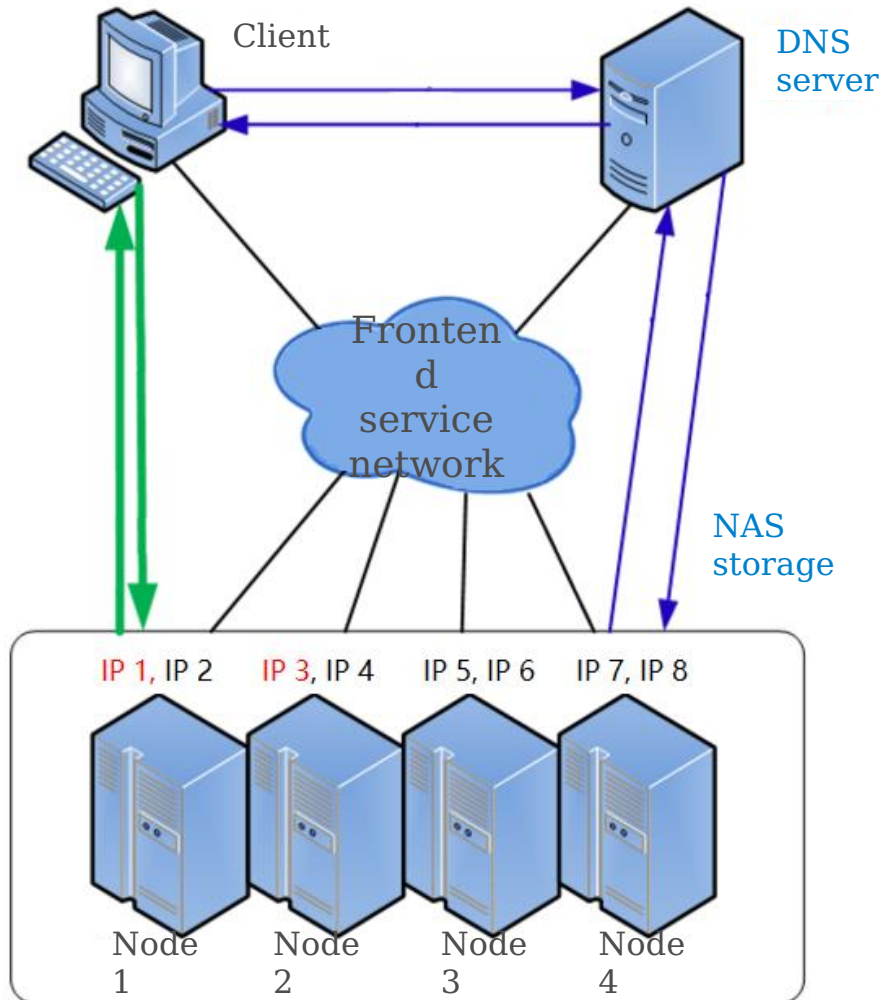
- **Benefits**

- ✓ Access to the Internet without having to remember each IP address
- ✓ More balanced access, no single-point bottleneck

Domain name resolver



DNS-based Load Balancing



- **Principles**

1. A user uses a domain name to access NAS services.
2. The DNS client sends a DNS request to the DNS server to obtain an IP address based on the domain name.
3. The DNS server selects an IP address and returns it to the client.

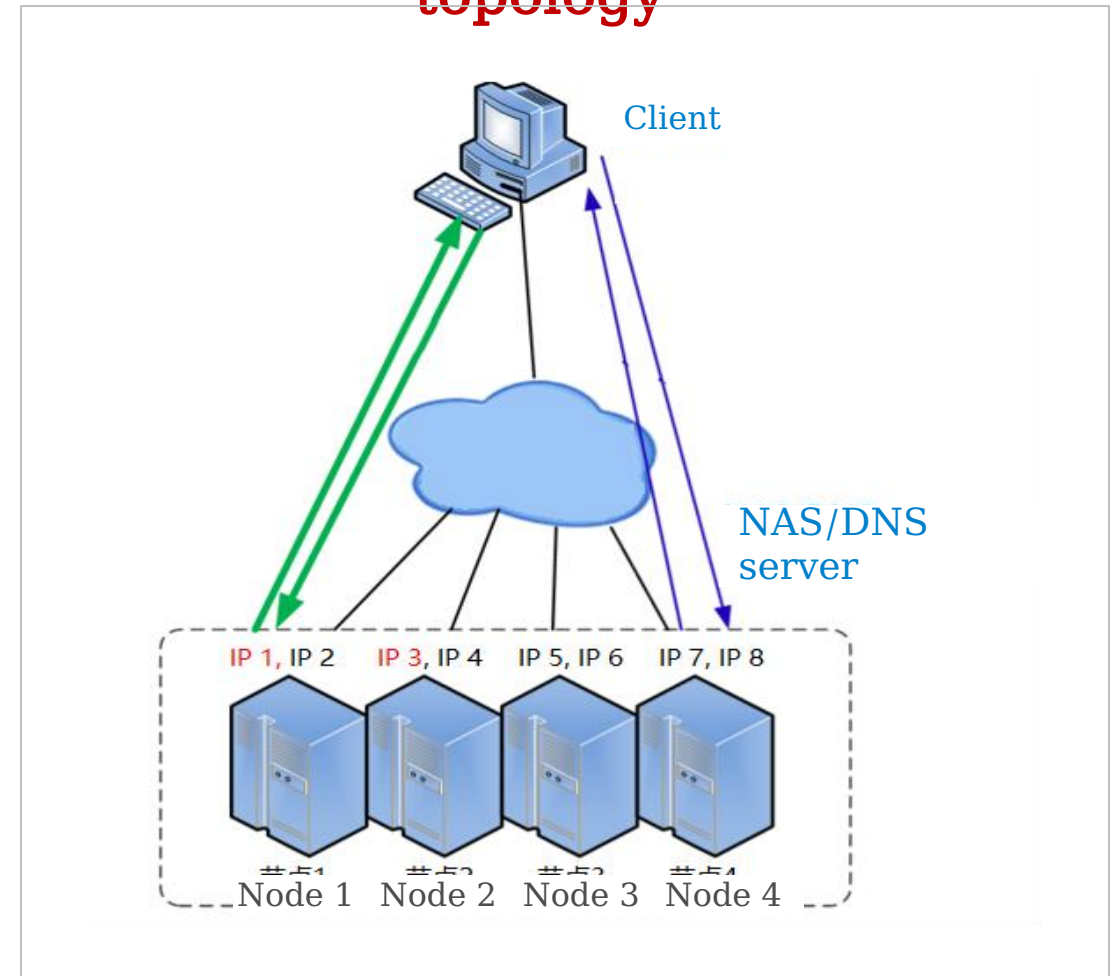
- **Load balancing policies**

1. Round-robin
2. CPU usage of each node
3. Number of connections of each node
4. Port bandwidth usage of each node
5. Comprehensive load of each node

Embedded and External DNS Servers

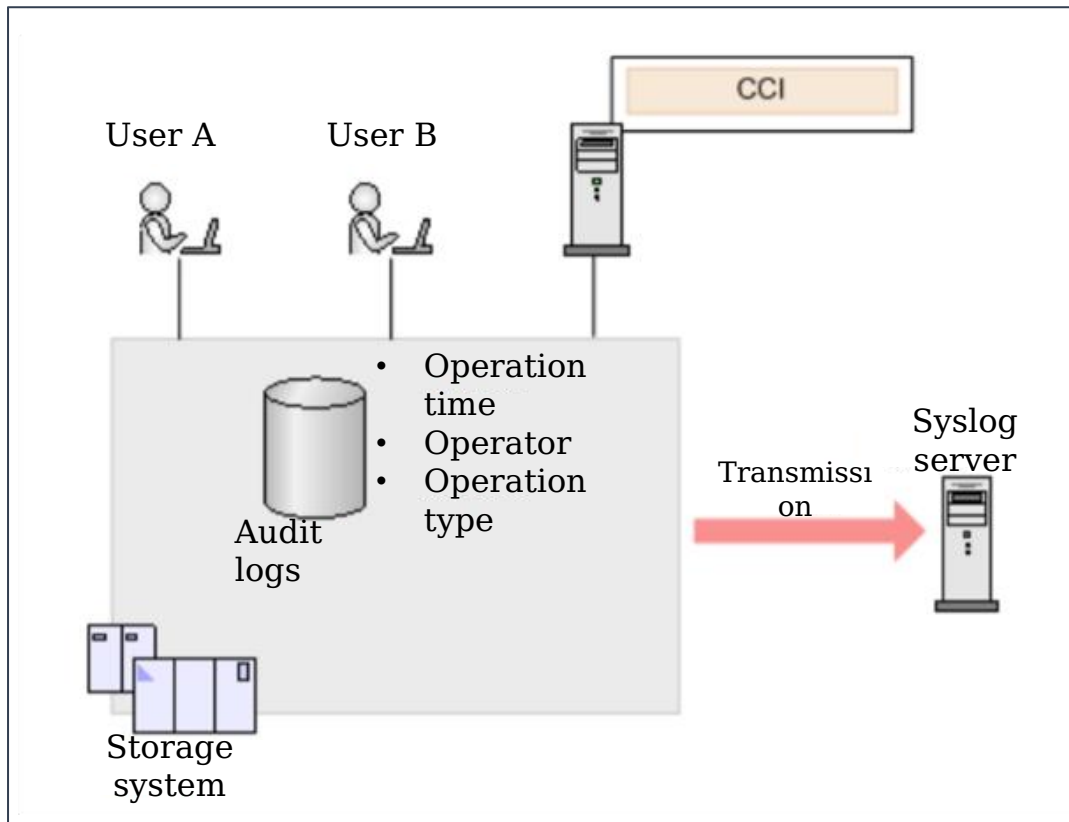
- **External DNS server** options include Windows DNS server and Open BIND.
Advantages: unified management of multiple NAS systems
- **Embedded DNS server**
Advantages: high reliability, low cost, and simple networking

Embedded DNS topology



NAS Audit Logs

NAS audit logs are used in **security audit scenarios** to trace each file operation. When a file is accessed, the system records the operation in NAS audit logs.

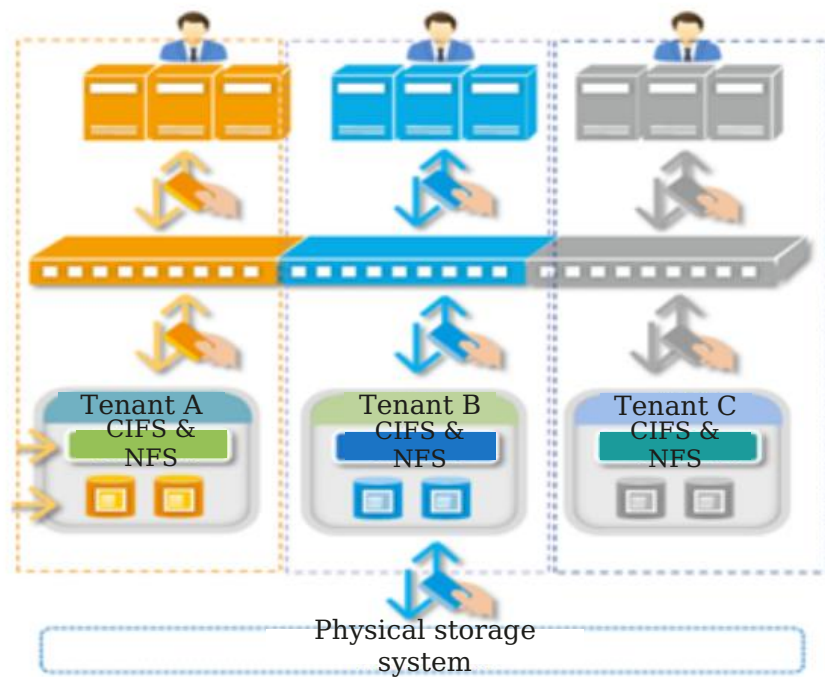


- **File operations:**
 - a. Create, delete, and rename
 - b. Open and close
 - c. Read and write
 - d. Get attributes (Get_attr) and set attributes (Set_attr)
 - e. Get security attributes (Get_security) and set security attributes (Set_security)
- **Supports integration with third-party log servers.**

Multi-Tenancy

Pain points

- Security issues arise when enterprises or users use the same physical storage device and access or interfere with each other's logical resources.
- IT service providers need to pay extra costs to manage users.



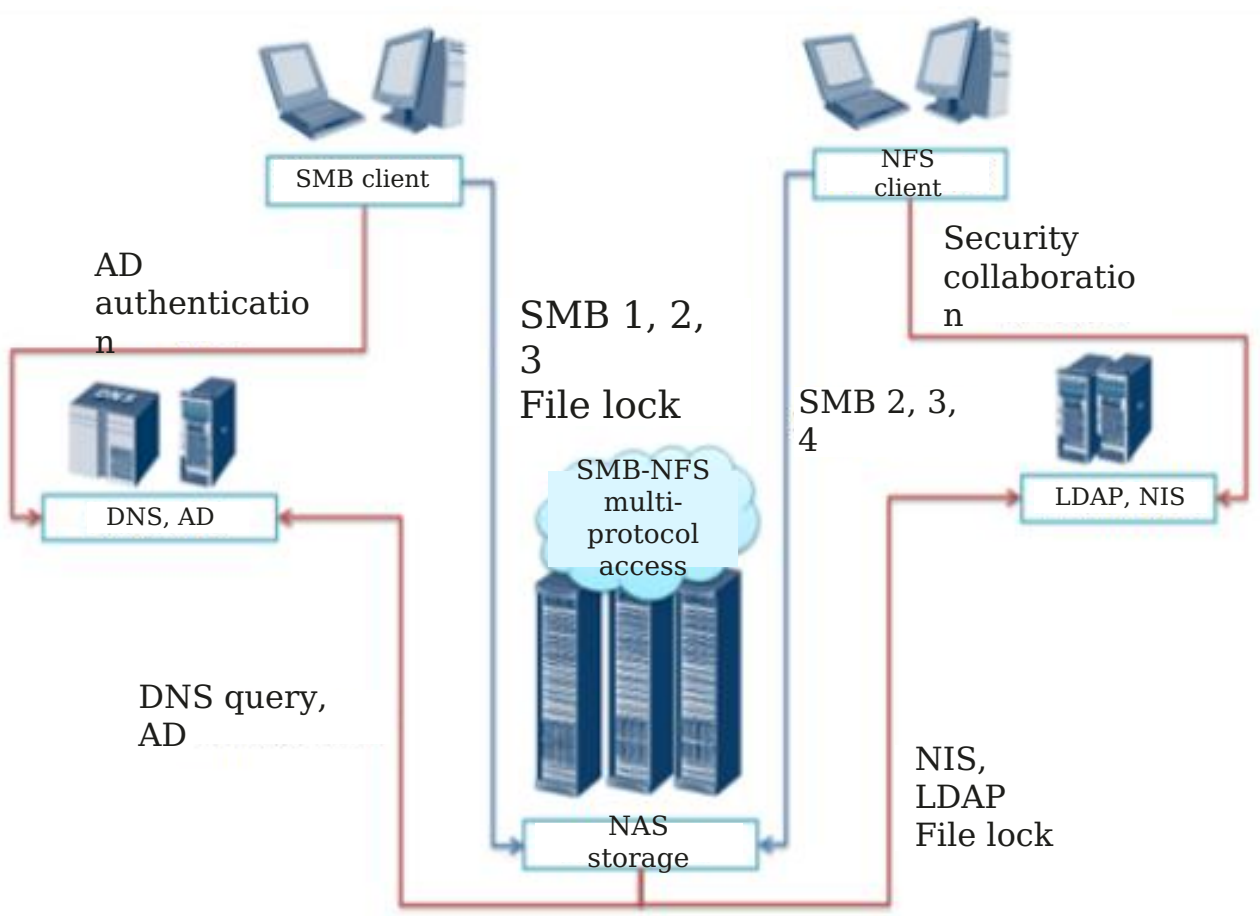
Each tenant has independent NAS protocol services, including:

1. Domain service (AD, LDAP, and NIS)
2. CIFS service
3. NFS service
4. NDMP service

Each service can be disabled and enabled separately.

Multi-Protocol Access

Multi-protocol access enables **Windows, Linux, and Unix clients to access the same directory or file at the same time.**



Multi-protocol access security

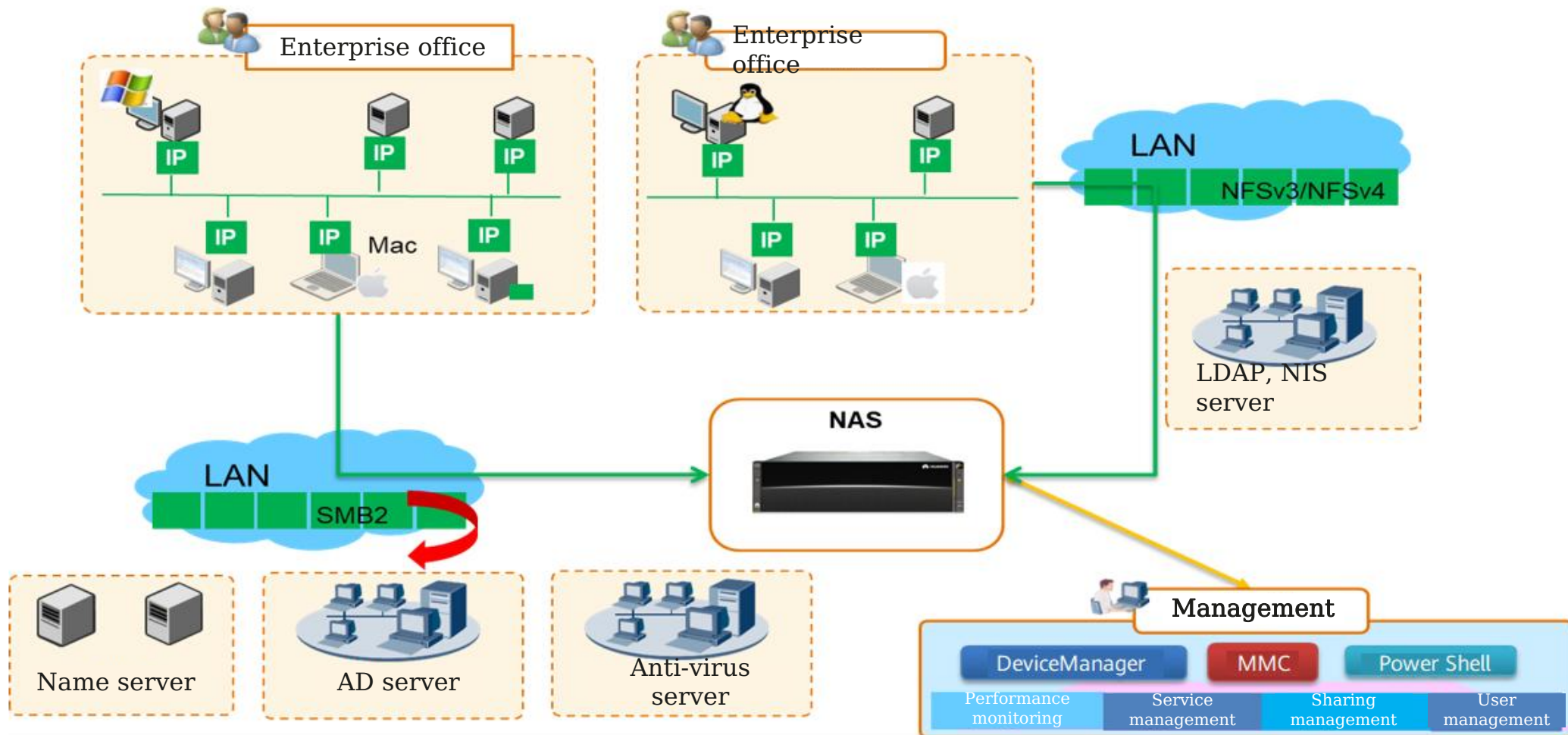
Item	Permission	User
SMB	NT ACL	Local user AD server
NFS	UNIX mode NFSv4 ACL	Client NIS/LDAP

Consistency of shared access files

Item	Reading File	Writing File
Reading file	Yes	No
Writing file	No	No

Multi-Protocol File Sharing

Application scenario: enterprise office file sharing



Contents

1. NAS Overview
2. NAS Technology
- 3. NAS Products**
4. NAS Applications

Centralized NAS: OceanStor Dorado

Overview

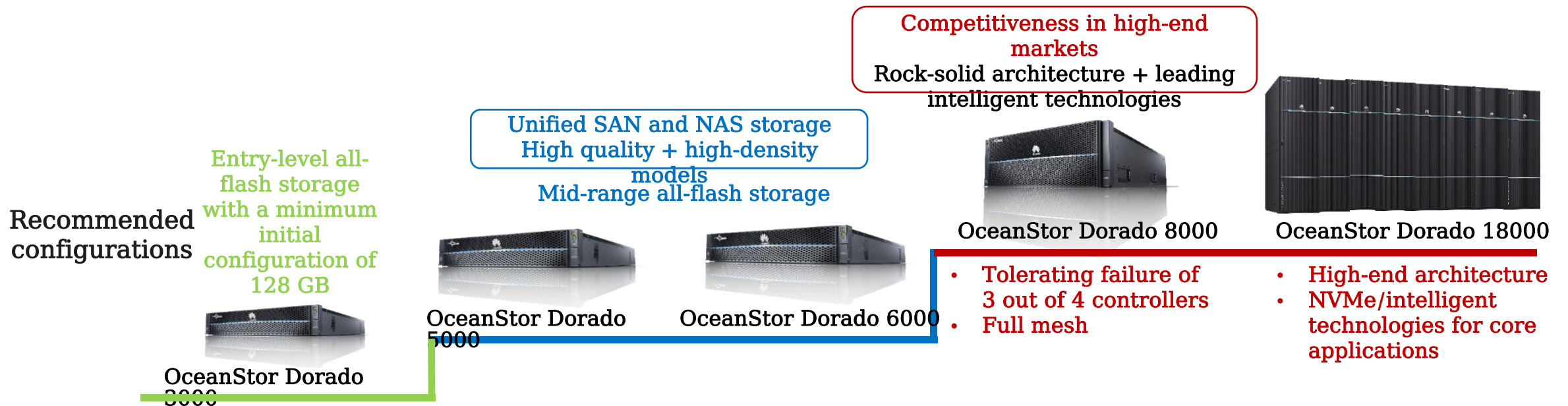
OceanStor Dorado all-flash unified storage **sets a new benchmark** with its industry-leading stability, SAN and NAS performance, intelligence, and efficient management and O&M.

Products

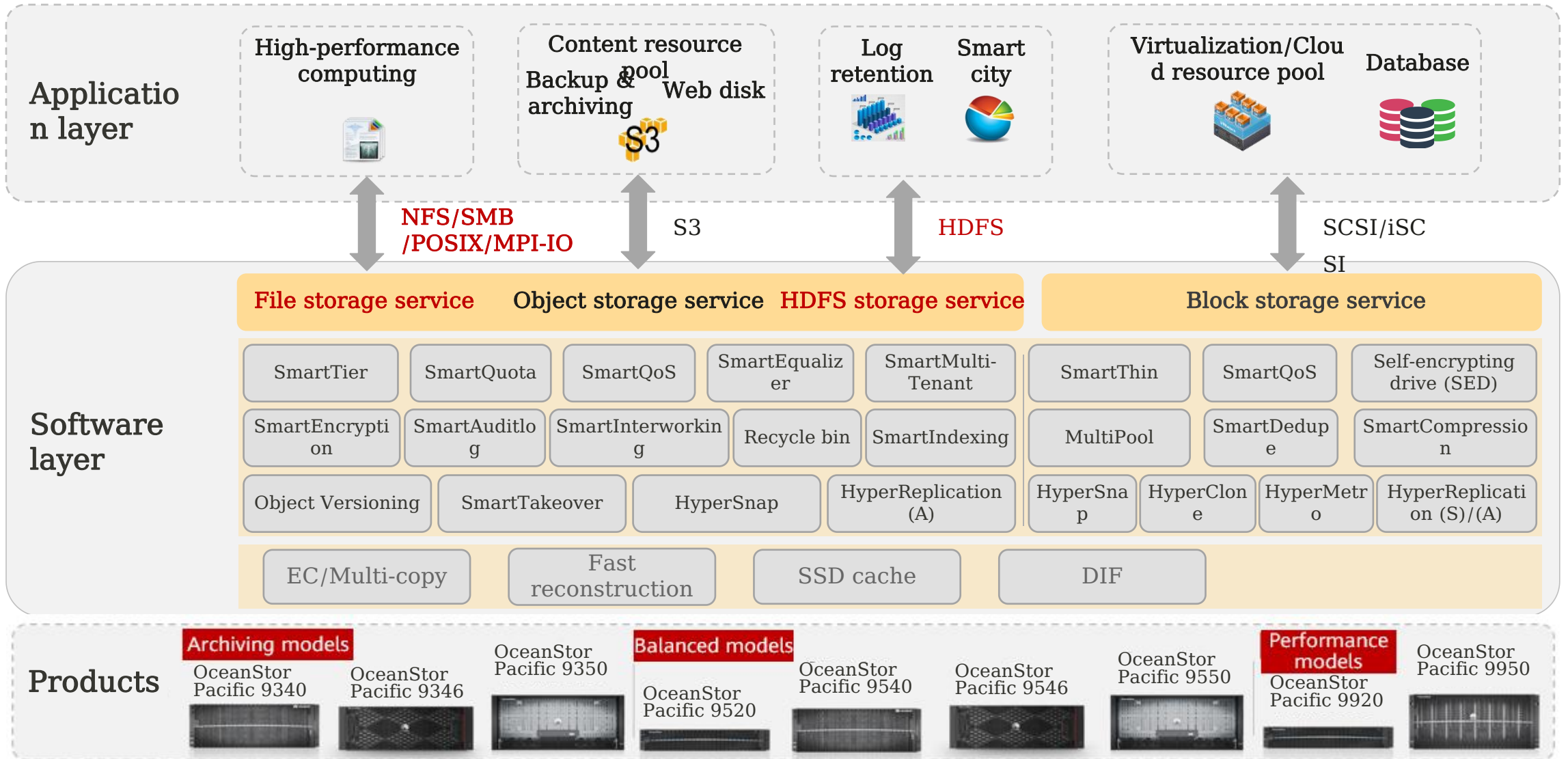
- OceanStor Dorado 3000 is an entry-level storage product, boasting **high cost-effectiveness** to expand its footprint in the market.
- OceanStor Dorado 5000 and OceanStor Dorado 6000 are mid-range storage systems that **outperform** competitors with their high quality and high density.
- OceanStor Dorado 8000 is an entry-level high-end storage system. Its stable architecture and competitive mid-range pricing **are key to expanding its market share**.
- OceanStor Dorado 18000 is a high-end storage system. Its stable architecture, top-notch performance, and intelligence **are key qualities that allow it to** expand its presence in high-end markets and empower benchmark projects for core NAs.

NAS

Focusing on high-performance NAS scenarios, such as EDA simulation, carrier CDRs, and financial data exchange platforms



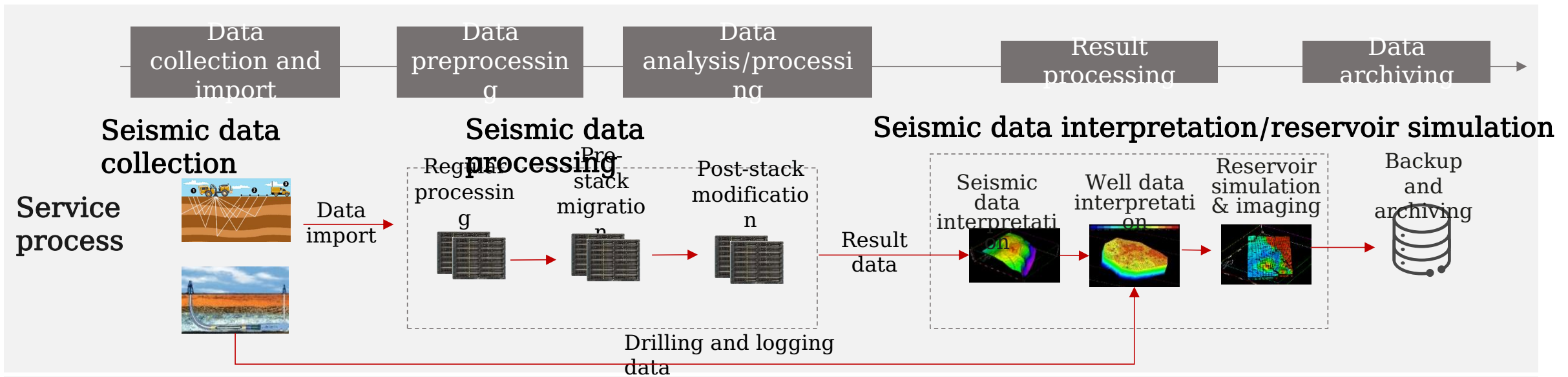
Scale-Out NAS: OceanStor Pacific Series



Contents

1. NAS Overview
2. NAS Technology
3. NAS Products
- 4. NAS Applications**

Energy Exploration



Service requirements

Data size: **1-20 TB/day**

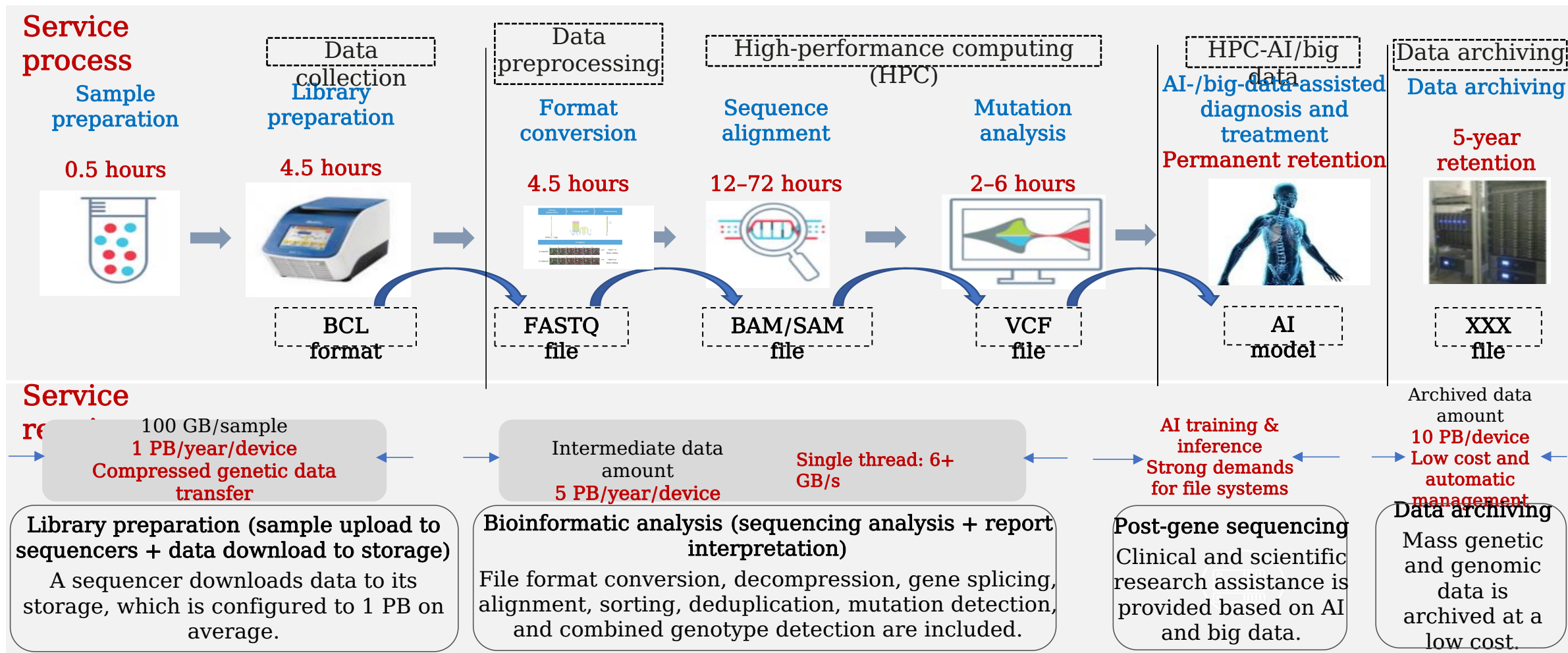
I/O model: GB-level files, sequential large I/Os
 Large bandwidth: **2-20 GB/s (per PB)**

Image loading: **100,000 IOPS**
 Latency: **ms-level** response

Solutions

- **Seismic data processing + interpretation/reservoir simulation: OceanStor Pacific 9920/9950 + OceanStor Pacific 9546/9550 + automatic tiering**

Gene Sequencing

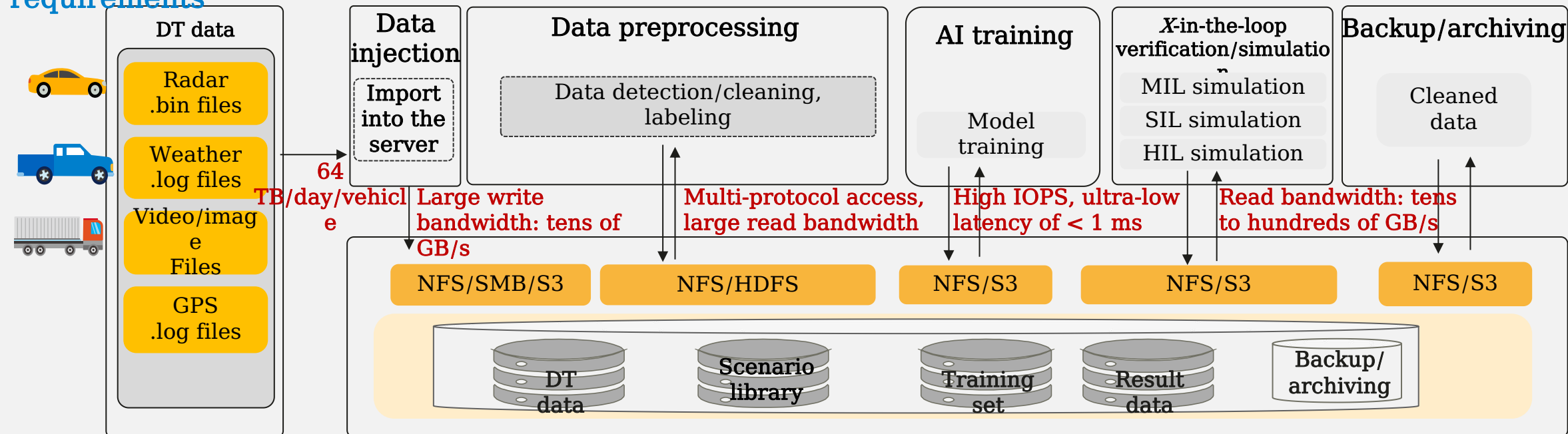


Solution • Production and archive storage: OceanStor Pacific 9546/9550

S

Autonomous Driving

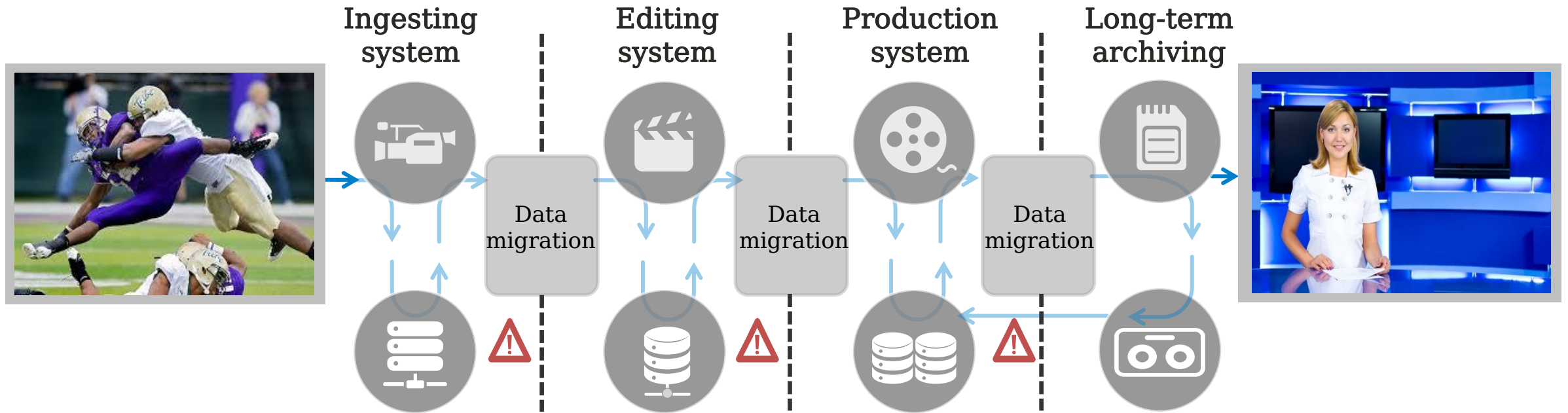
Service process and requirements



Solutions

- Scenarios involving AI training: OceanStor Pacific 9920/9950 + OceanStor Pacific 9546/9550 + automatic tiering
- Common scenarios: OceanStor Pacific 9546/9550

Non-Linear Media Editing System



Solutions

Functions and requirements for production

1. Stable high bandwidth, large files, large I/O blocks (> 1 MB)
2. SMB 2/SMB 3 in Windows and macOS clients
3. Easy scalability for performance and capacity
4. Easy data migration

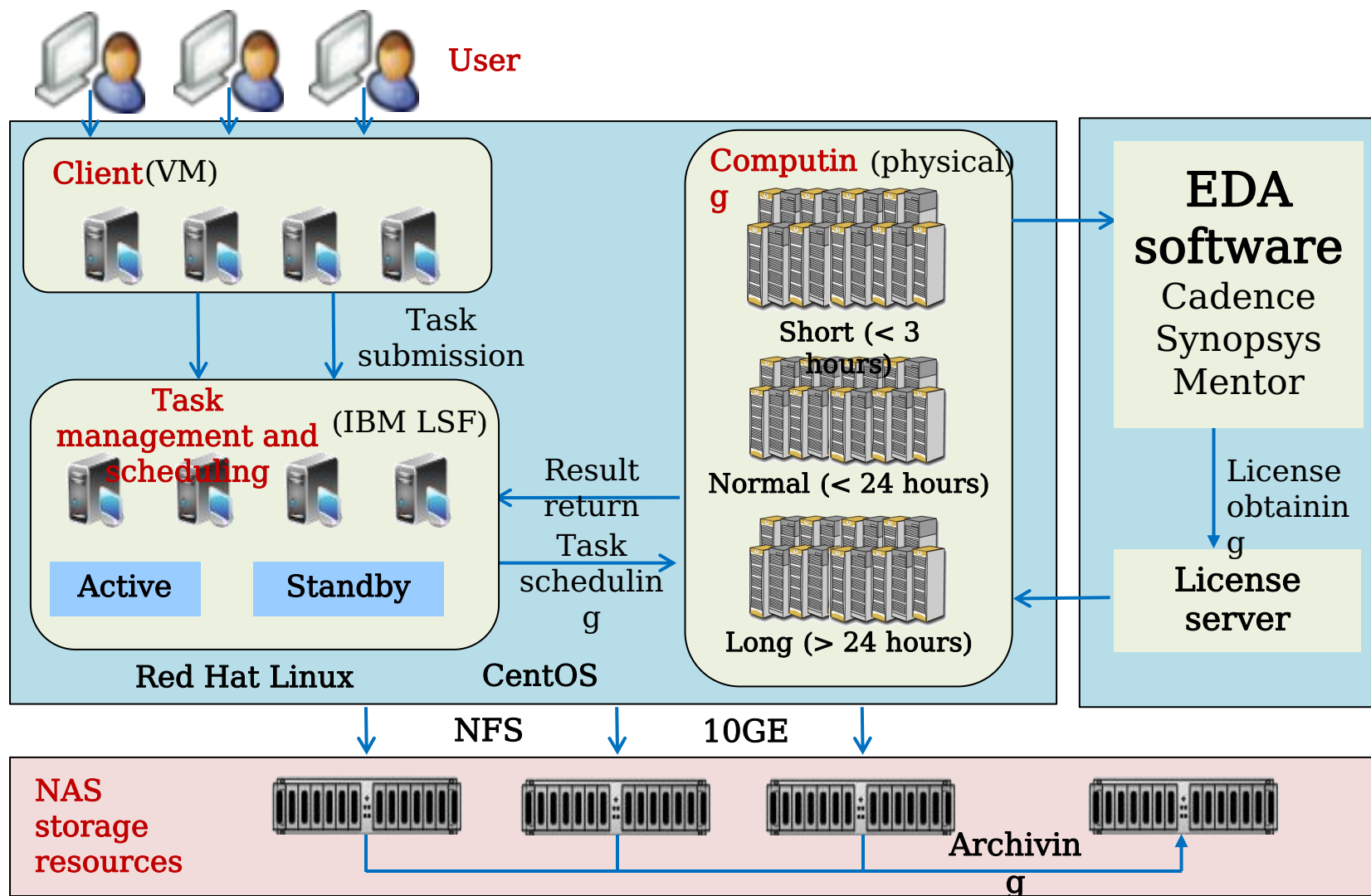
Solution: OceanStor Pacific 9920/9950, 9546/9550

Functions and requirements for archiving

1. Massive capacity
2. Low TCO

Solution: OceanStor Pacific 9546/9550

EDA System



NAS applications

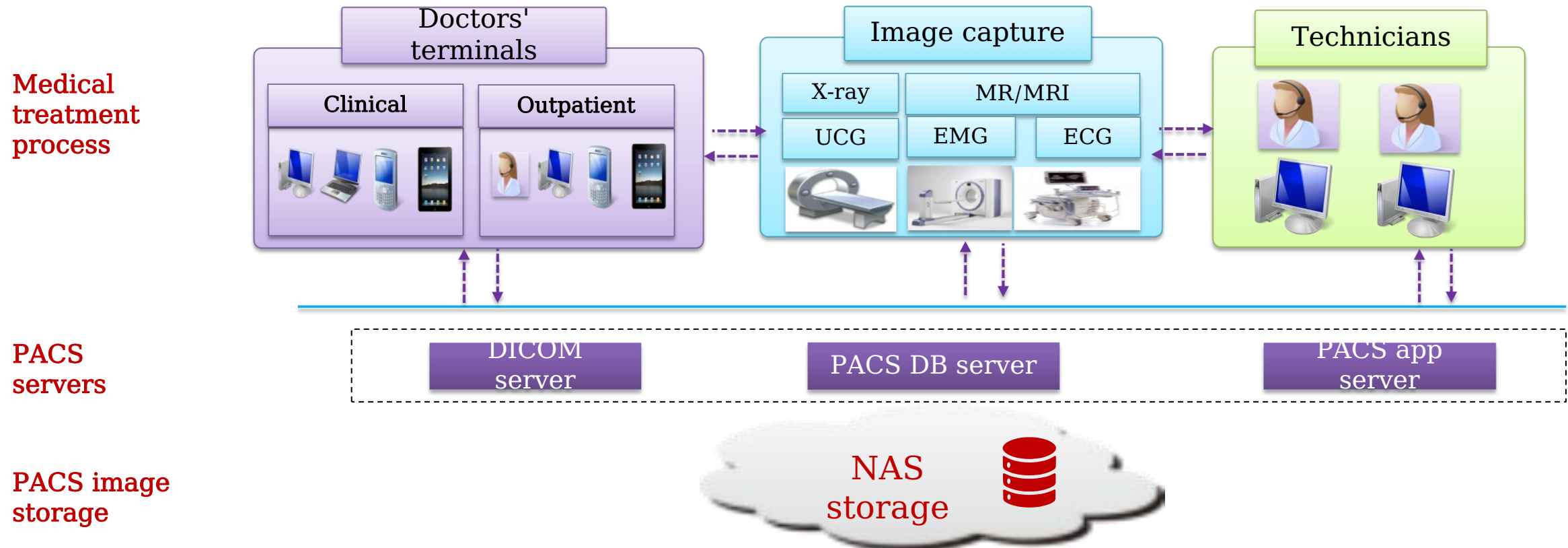
- EDA development
- EDA test

Service features

- Mass small files: > 4 billion
- File size (95% of files) < 128 KB
- Concurrent access, high OPS, and low latency

Solution: OceanStor Dorado NAS

Medical PACS System



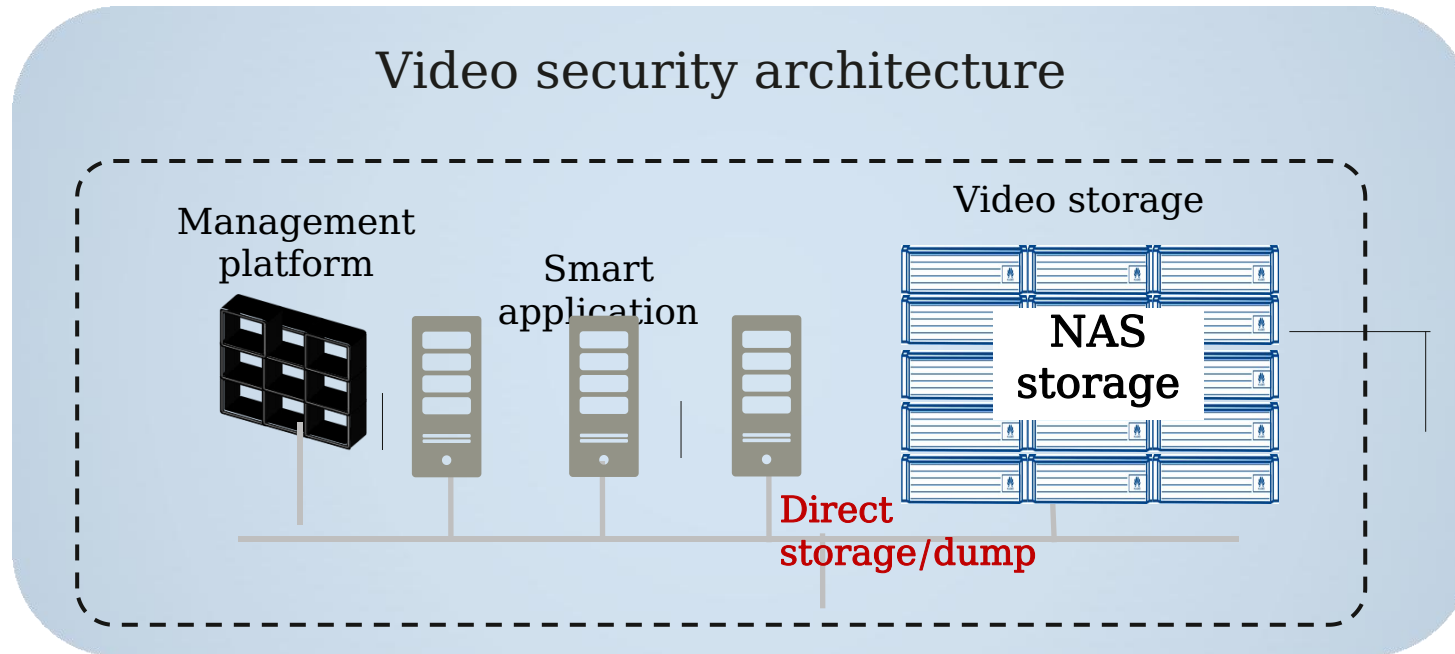
PACS functions and requirements

- Mass small files (most ranging from 128 KB to 1 MB)
- High OPS and low I/O latency
- High reliability

Solutions

- **Primary storage: OceanStor Dorado/Hybrid flash storage NAS**
- **Archive storage: OceanStor Pacific series**

Video Security System



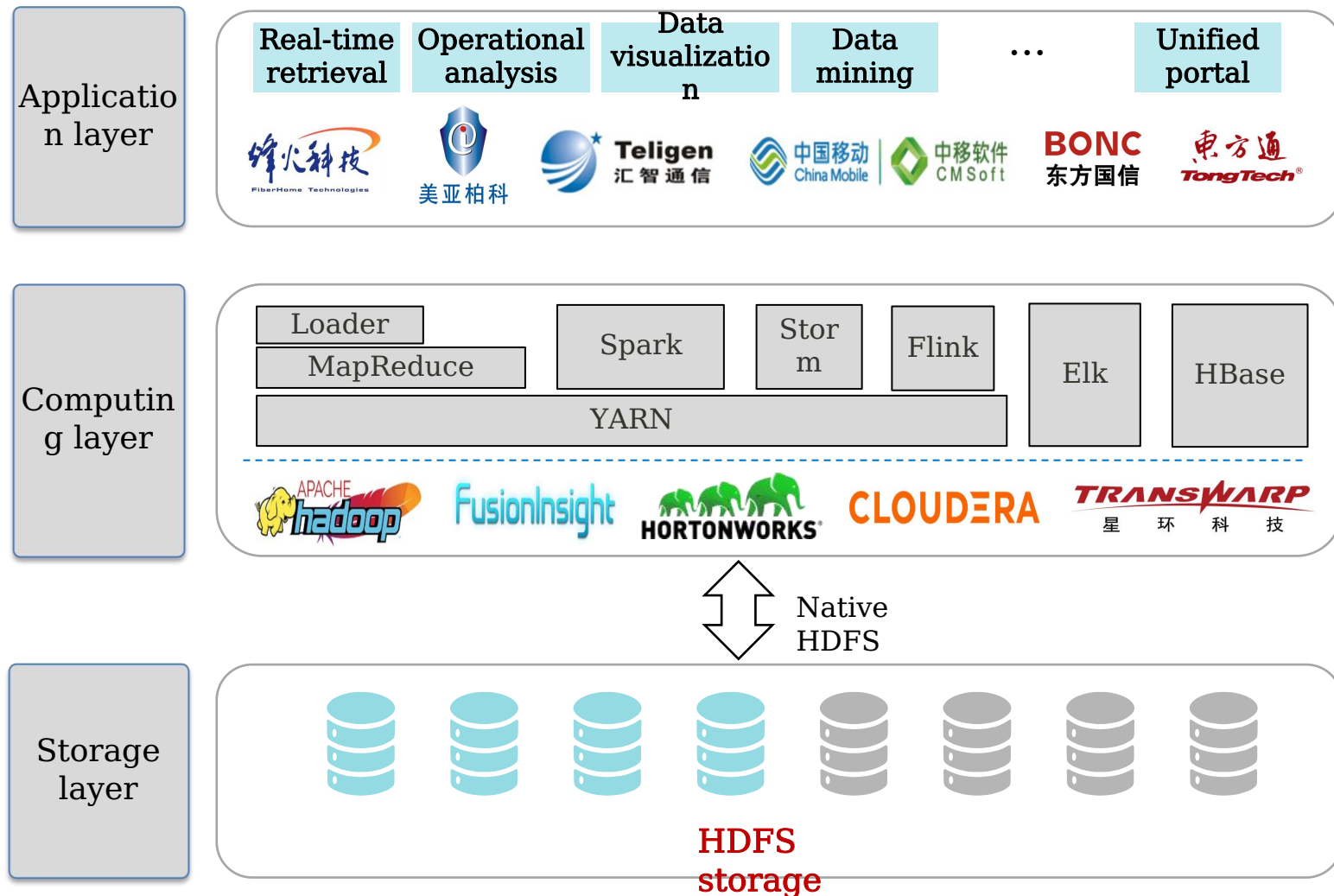
Functions and requirements

- Large files and I/O blocks (> 1 MB)
- High-bandwidth sequential write
- Massive capacity, easy scale-out
- Centralized management

Solutions

- Dump: OceanStor Pacific 93xx
- Direct storage: IVS3800

Big Data Analysis



Functions and key requirements

- On-demand computing and storage expansion to avoid resource wastage
- Compatible with big data clusters on the live network to protect existing investments
- Stringent requirements for cost reduction due to mass data sets

Solutions

- OceanStor Pacific 9546/9550 big data storage

Thank you.

把数字世界带入每个人、每个家庭、
每个组织，构建万物互联的智能世界。
Bring digital to every person, home, and
organization for a fully connected,
intelligent world.

**Copyright©2023 Huawei Technologies Co., Ltd.
All Rights Reserved.**

The information in this document may contain predictive statements including, without limitation, statements regarding the future financial and operating results, future product portfolio, new technology, etc. There are a number of factors that could cause actual results and developments to differ materially from those expressed or implied in the predictive statements. Therefore, such information is provided for reference purpose only and constitutes neither an offer nor an acceptance. Huawei may change the information at any time without notice.

