Server Basics

HUAWEI

Foreword

- Servers are the foundation of all service platforms, including cloud computing platforms. But what is a server? What are the key technologies for servers? Let's find the answers in this course, and start our learning journey into cloud computing.

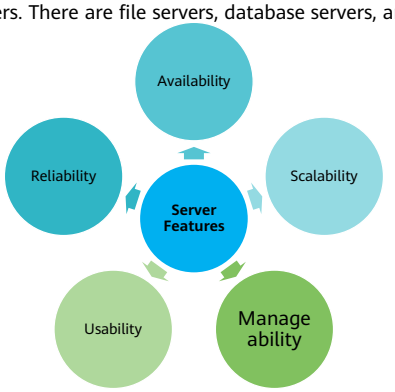
Objectives

- On completion of this course, you will be able to:
  - Understand what a server is.
  - Understand the type of server.
  - Understand the hardware composition and basic principles of the server.
  - Familiarize yourself with the key technologies of the server.

Contents

Server Definition and Features

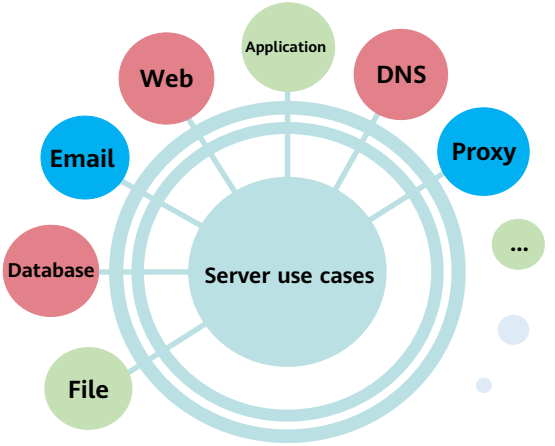
- Definition
  - A server is a type of computer. It runs faster, carries more loads, and costs more than ordinary computers.
  - A server provides services to users. There are file servers, database servers, and application servers.



HUAWEI

- A server is a mainstream computing product developed in 1990s. It can provide network users with centralized computing, information release, and data management services. In addition, a server can share dedicated communication devices connected to it, such as drives, printers, and modems with network users.
- A server has the following features:
  - R: Reliability – the duration that the server operates consecutively
  - A: Availability – percentage of normal system uptime and use time
  - S: Scalability – including hardware expansion and operating system (OS) support capabilities
  - U: Usability – easy to maintain and restore server hardware and software
  - M: Manageability – monitoring and alarm reporting of server running status, and intelligent automatic fault processing

Server Application Scenarios

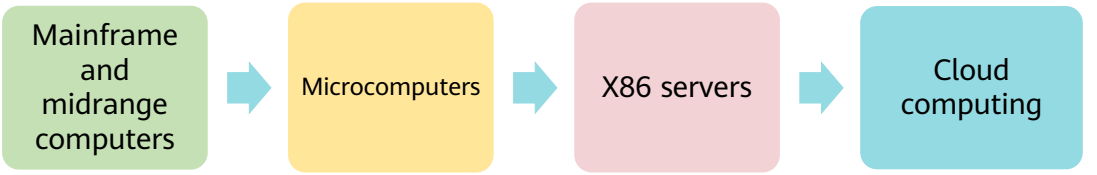


HUAWEI

- Servers have been widely used in various fields, such as the telecom carrier, government, finance, education, enterprise, and e-commerce. Servers can provide users with the file, database, email, and web services.
- Server application deployment architecture:
  - C/S: short for Client/Server. In this architecture, the server program runs on the server, and the client software is installed on the client. The server and client perform different tasks. The client carries the front-end GUI and interaction operations of users, and the server processes the background service logic and request data. This greatly improves the communication speed and efficiency between the two ends. For example, you can install the vsftpd program on a file server and start the service. After you install the FileZilla or WinSCP client on your PC, you can upload and download files using the client.
  - B/S: short for Browser/Server. In this architecture, users only need to install a browser. The application logic is centralized on the server and middleware, which improves the data processing performance. For example, when accessing a website, we only need to enter the domain name of the website in the browser, for example, **www.huawei.com**. Then we can see the web services provided by the background servers of the website. We do not need to care the background servers that provide services, such as the database service, proxy service, and cache service.

Contents

Server Development History

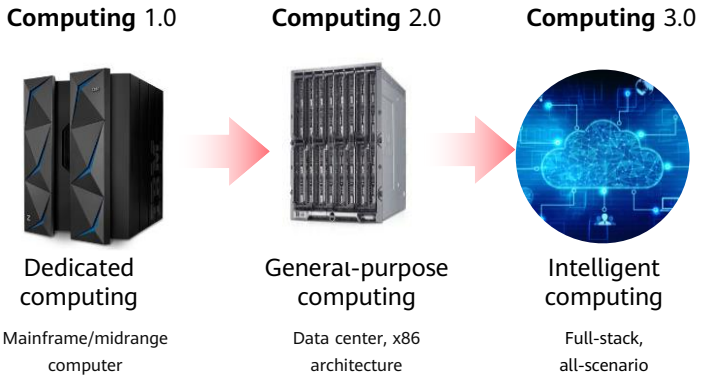


HUAWEI

- Mainframe phase
  - In the 1940s and 1950s, the first generation of vacuum tube computers emerged. The computer technology develops rapidly from vacuum tube computers, transistor computers, integrated circuit computers, to large-scale integrated circuit computers.
- Midrange computer phase
  - In the 1960s and 1970s, mainframes were scaled down for the first time to meet the information processing requirements of small- and medium-sized enterprises and institutions. The cost was acceptable.
- Microcomputer phase
  - In the 1970s and 1980s, mainframes were scaled down for the second time. Apple Inc. was founded in 1976, and launched Apple II in 1977. In 1981, IBM launched IBM-PC. After several generations of evolution, it occupied the personal computer market and made personal computers popular.
- x86 server era
  - In 1978, Intel launched the first-generation x86 architecture processor, 8086 microprocessor.
  - In 1993, Intel officially launched the Pentium series, which brought the x86 architecture processor to a new level of performance.
  - In 1995, Intel launched Pentium Pro, the x86 processor for servers, ushering in the x86 era. The standardization and openness of Pentium Pro also promoted the market development and laid a solid foundation for the cloud computing era.

- Cloud computing era
  - Since 2008, the concept of cloud computing has gradually become popular, and cloud computing becomes a popular word. Cloud computing is regarded as a revolutionary computing model because it enables the free flow of supercomputing capabilities through the Internet. Enterprises and individual users do not need to purchase expensive hardware. Instead, they can rent computing power through the Internet and pay only for the functions they need. Cloud computing allows users to obtain applications without the complexity of technologies and deployment. Cloud computing covers development, architecture, load balancing, and business models, and is the future model of the software industry.

A Leap from Computing 1.0 to Computing 3.0



HUAWEI

- The computing industry has developed for nearly half a century and continuously changed other industries. The computing industry itself is evolving.
- In the early mainframe and midrange computer era, dedicated computing is used, which is called computing 1.0. In the x86 era, under the leadership of Intel and driven by Moore's Law, computing has shifted from dedicated to general-purpose. A large number of data centers have emerged, which is called computing 2.0. With the rapid development of digitalization, the world is developing towards intelligent. Computing is not limited to data centers, but also enters the full-stack all-scenario (computing 3.0) era. This era is featured by intelligence, so it is also called intelligent computing.

Contents

Server Classification - Hardware Form

Hardware form		
Tower server	Rack server	Blade server
		

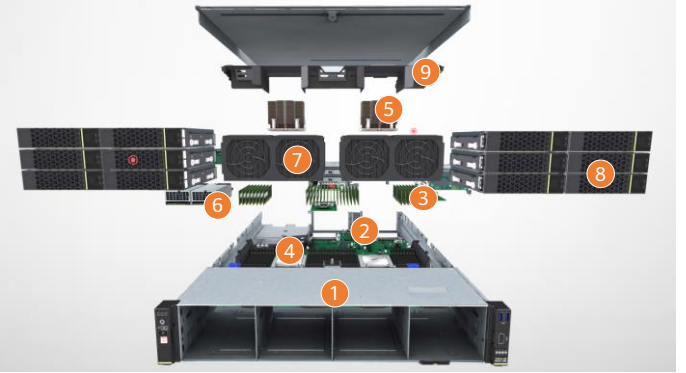
HUAWEI

- **Tower server:**
  - Some tower servers use a chassis roughly the same size as an ordinary vertical computer, while others use a large-capacity chassis, like a large cabinet.
- **Rack server:**
  - The appearance of a rack server is different from that of a computer, but is similar to that of a switch. The specifications of a rack server include 1 U (1 U = 1.75 inches), 2 U, and 4 U. A rack server is installed in a standard 19-inch cabinet. Most of the servers in this structure are functional servers. A rack server is usually small in size. Multiple servers can be placed in a cabinet at the same time to obtain a higher processing capability.
- **Blade server:**
  - Each blade server is a plugboard equipped with processors, memory modules, hard drives, and related components. Due to the special architecture, blade servers require dedicated chassis. Generally, a chassis can hold several to dozens of blade servers, suitable for scenarios such as high-performance computing, front-end servers running multiple applications, and backend central databases.

Contents

Hardware Structure

- Huawei TaiShan 200 server



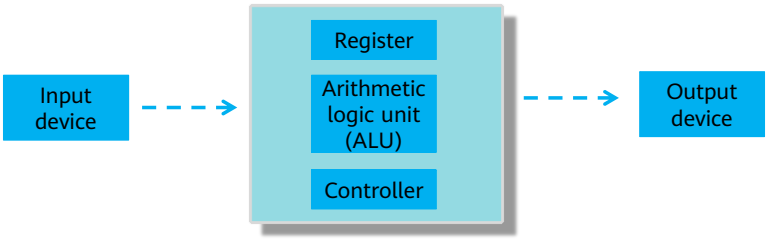
1 Chassis
2 Motherboard
3 Memory
4 CPU
5 CPU heat sink
6 Power supply unit (PSU)
7 Fan
8 Drive
9 Air duct

HUAWEI

- 3D model display for a Huawei TaiShan 200 server: https://support-it.huawei.com/server-3d/res/server/taishan2280e/index.html?lang=en

CPU Definition and Components

- Definition
  - The Central Processing Unit (CPU) is the computing and control core of a computer.
  - The CPU, internal storage, and input/output devices are key components of a computer.
  - The CPU interprets computer instructions and processes computer software data.
- Components
  - The CPU consists of a logic operation unit, a control unit, and a storage unit.



HUAWEI

- The CPU is the core processing unit on a server, and a server is an important device on the network and needs to process a large number of access requests. Therefore, servers must have high throughput and robust stability, and support long-term running. Therefore, the CPU is the brain of a computer and is the primary indicator for measuring server performance.
- The computer controls the entire computer according to a pre-stored program, and the program refers to an instruction sequence that can implement a function. The controller is an organization that issues commands to various logic circuits according to the instructions. The controller is a command center of the computer, controls work of an entire CPU, and determines automation of a running process of the computer.
- The ALU is a part of a computer that performs a variety of arithmetic and logical operations. Basic operations of an ALU include arithmetic operations such as addition, subtraction, multiplication, and division, logical operations such as AND, OR, NOT, and XOR, and other operations such as shift, comparison, and transfer. The ALU is also called the arithmetic logic component.
- The register is used to temporarily store the data involved in operations and the operation results. It can receive, store, and output data.

CPU Frequency

- Dominant frequency
  - The dominant frequency is also called clock speed. It indicates, in MHz or GHz, the frequency at which a CPU computes and processes data.
- External frequency
  - The external frequency is the reference frequency of a CPU, measured in MHz. The CPU external frequency determines the speed of the motherboard.
- Bus frequency
  - The bus frequency directly affects the speed of data exchange between a CPU and a dual in-line memory module (DIMM).
- Multiplication factor
  - The multiplication factor is the ratio of the dominant frequency to the external frequency.

Memory

- Definition
  - Storage is classified, by purpose, into main memory and external storage. Main memory, referred to as internal storage, is the storage space that the CPU can address.
  - Memory is used to temporarily store CPU operation data and the data exchanged with external storage devices such as hard drives.
  - Memory, one of important computer components, communicates with the CPU.
  - Memory consists of the memory chip, circuit card, and edge connector.

- Storage, an important computer component, is used to store programs and data. For computers, the memory function can be supported and normal working can be ensured only when the storage is available.
- As a main computer component, the memory is in opposition to the external storage. Programs, such as the Windows operating system, typing software, and game software, are usually installed on external storage devices such as drives. To use these programs, you must load them into the memory. Actually, the memory is used when we input a piece of text or play a game. Bookshelves and bookcases for putting books are just like the external storage, while the desk is like the memory. Generally, we store large volumes of data permanently in the external storage and store small volumes of data and a few programs temporarily in the memory.
- Memory, one of important computer components, communicates with the CPU. Memory performance has great impacts on computers because all computer programs operate in the memory. The memory consists of the memory chip, circuit card, and edge connector.
- DIMM slots and configuration principles:
  - DIMMs on the same server must be of the same model.
  - At least one memory module must be configured in the memory slot corresponding to the CPU.
  - Optimal memory performance can be achieved if the processors in a server are configured with the same number of DIMMs and the DIMMs are evenly distributed among the memory channels. Unbalanced configuration impacts memory performance and is not recommended.

Drive

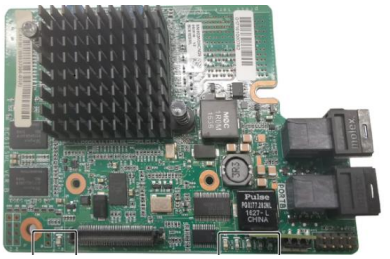
- The drive is the most important storage device of a computer.
- The drive interface, connecting a drive to a host, is used to transmit data between the drive cache and the host memory. The drive interface type determines the connection speed between the drive and the computer, how quickly programs run, and overall system performance.

	SATA	SAS	NL-SAS	SSD
Rotational speed (RPM)	7,200	15,000/10,000	7,200	N/A
Serial/Parallel	Serial	Serial	Serial	Serial
Capacity (TB)	1TB/2TB/3TB	0.6TB/0.9TB	2TB/3TB/4TB	0.6TB/0.8TB/1.2TB/1.6TB
MTBF (h)	1,200,000	1,600,000	1,200,000	2,000,000
Remarks	Developed from ATA drives, SATA 3.0 supports data transfer up to 600 MB/s. The annual failure rate of SATA drives is about 2%.	SAS drives are designed to meet high-performance enterprise requirements and are compatible with SATA drives. The transfer rate ranges from 3.0Gbit/s to 6.0 Gbit/s, and can increase to 12.0 Gbit/s. The annual failure rate of SAS drives is less than 2%.	An NL-SAS drive is an enterprise-level SATA drive with a SAS interface. It is used to implement tiered storage in a drive array, simplifying drive array design. The annual failure rate of NL-SAS drives is about 2%.	A solid-state drive (SSD) is a hard drive housing a solid-state electronic storage chip array. An SSD consists of a control unit and a storage unit (flash or DRAM chip). An SSD is the same as a common hard drive in terms of interface specifications and definition, function, usage, and product shape and size.

- MTBF: Mean Time Between Failures
- SATA and NL-SAS drives are cheaper, SAS drives are more expensive, and SSDs are the most expensive.

RAID Controller Card

- Also called the RAID card.
- Functions of the RAID controller card:
  - Combines multiple drives into a system managed by the array controller according to requirements.
  - Improves drive subsystem performance and reliability.



LSI SAS3108

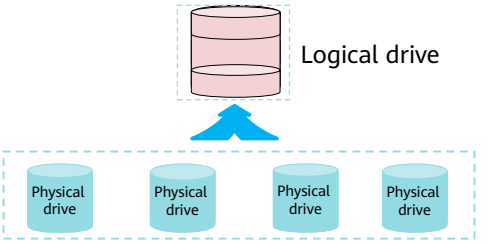
HUAWEI

- LSI SAS3108 RAID Controller Card User Guide: https://support.huawei.com/enterprise/en/doc/EDOC1100048773/653c6b1f

RAID

- Definition
  - Redundant Array of Independent Disks (RAID) is a data storage virtualization technology that combines multiple physical disk drive components into one or more logical units for the purposes of data redundancy, performance improvement, or both.

--Wikipedia

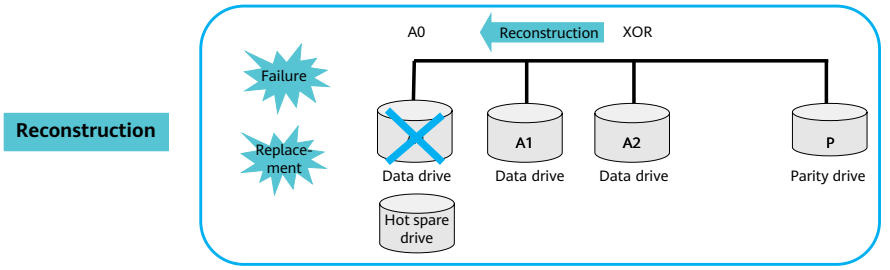


HUAWEI

- For details about the working principles of RAID, see the course of storage basics.

RAID Hot Spare and Reconstruction

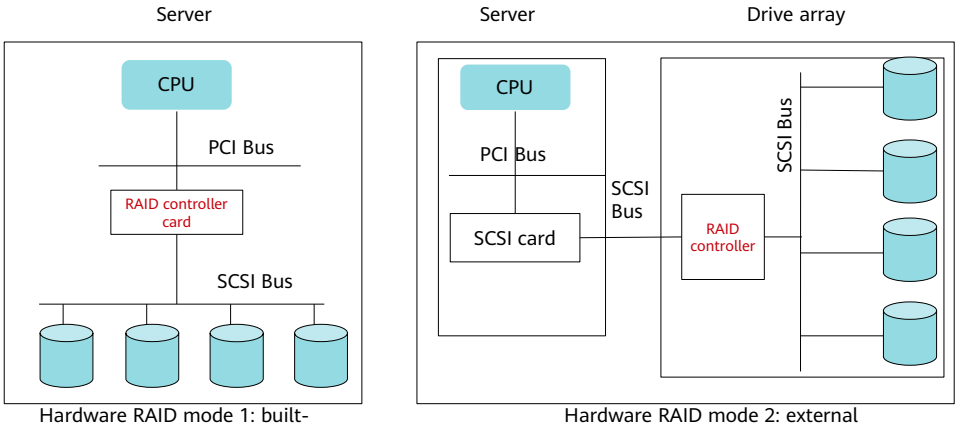
- Hot spare definition
  - If a drive in a RAID array fails, a hot spare is used to automatically replace the failed drive to maintain the RAID array's redundancy and data continuity.
- Hot spare types
  - Global: The spare drive is shared by all RAID arrays in the system.
  - Dedicated: The spare drive is used only by a specific RAID array.



HUAWEI

- Data parity: Redundant data is used to detect and rectify data errors. The redundant data is usually calculated through Hamming check or XOR operations. Data parity can greatly improve the reliability, performance, and error tolerance of the drive arrays. However, the system needs to read data from multiple locations, calculate, and compare data during the parity process, which affects system performance.
- Generally, RAID cannot be used as an alternative to data backup. It cannot prevent data loss caused by non-drive faults, such as viruses, man-made damages, and accidental deletion. Data loss here refers to the loss of operating system, file system, volume manager, or application system data, not the RAID data loss. Therefore, data protection measures, such as data backup and disaster recovery, are necessary. They are complementary to RAID, and can ensure data security and prevent data loss at different layers.

RAID Implementation - Hardware



Hardware RAID mode 1: built-in plug-in card

Hardware RAID mode 2: external independent drive array

HUAWEI

- Hardware RAID is implemented using a hardware RAID adapter card.
- The hardware RAID can be a built-in or external RAID.
- A RAID controller card has a processor inside and can control the RAID storage subsystem independently from the host. The RAID controller card has its own independent processor and memory. It can calculate parity information and locate files, reducing the CPU computing time and improving the parallel data transmission speed.

RAID Implementation - Software

- Definition
  - Software RAID implements RAID functions by installing software on the operating system.
- Characteristics
  - Software RAID does not require expensive RAID controller cards, reducing the cost.
  - RAID functions are performed by CPUs, requiring significant CPU resources, such as for large numbers of RAID 5 XOR operations.

- Software RAID does not provide the following functions:
  - Hot swap of drives
  - Drive hot spare
  - Remote array management
  - Support for bootable arrays
  - Array configuration on drives
  - S.M.A.R.T. for disks

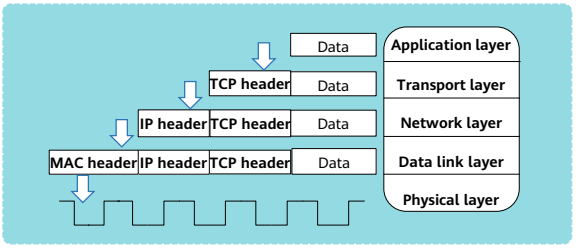
RAID Implementation - Mode Comparison

Mode	Software RAID	Built-in RAID	External RAID
Characteristics	All RAID functions are implemented by CPUs, resulting in high CPU usage and reduced system performance.	Built-in RAID improves performance by reducing host CPU usage caused by intensive RAID operations.	External RAID, connecting to a server through a standard controller, is independent of the operating system. All RAID functions are implemented by the microprocessor on the external RAID storage subsystem.
Advantages	▫ Low implementation cost ▫ Flexible configurations	▫ Data protection and high speed ▫ Better fault tolerance and performance than software RAID ▫ More cost-effective than external RAID ▫ Support for bootable arrays	▫ Provides ultra-large-capacity storage systems for high-end servers. ▫ Configures dual controllers to improve data throughput or provide shared storage for the two-node cluster. ▫ Supports hot swapping. ▫ Delivers better scalability.

NIC Definition and Functions

- Definition
  - A network interface card (NIC or network adapter) is an indispensable part of a computer network system. An NIC enables a computer to access networks.

- Functions
  - Fixed network address
  - Data sending and receiving
  - Data encapsulation and decapsulation
  - Link management
  - Encoding and decoding



Huawei Server NICs

- LOM card
  - It is embedded directly into the PCH chip on the server motherboard and cannot be replaced.
  - It provides two external GE electrical ports + two 10 Gbit/s optical/electrical ports. LOM cards do not occupy PCIe slots.
- PCIe card
  - Huawei has both self-developed and purchased PCIe cards. They can be installed in standard PCIe slots.
- FlexIO card
  - Huawei-developed, non-standard PCIe card, which can only be used with Huawei rack servers.
- Mezzanine card
  - Mezzanine cards are only used on the compute nodes of Huawei E9000 blade servers.

LOM card

PCIe card

FlexIO card

Mezzanine card

HUAWEI

- PCI-Express (PCIe) is the third-generation I/O bus, or 3GIO, following ISA and PCI buses. This bus was proposed by Intel at the Intel Developer Forum (IDF) in 2001 and renamed PCI-Express after being certified and released by the PCI special interest group (SIG). Its main advantages are high data transmission rate, strong anti-interference, long transmission distance, and low power consumption.
- For Huawei servers, a PCIe card refers to the NIC in a PCIe slot.
- Visit the link below to learn how to install and remove a PCIe card:

https://support.huawei.com/enterprise/en/doc/EDOC1100002169?section=o00d

- *FusionServer Rack Server Product Documentation*
- *TaiShan 200 DA121C Server Node Maintenance and Service Guide*
- *E9000 Blade Server Product Documentation*

PSU and Fan Module

- Supplies power to servers.
- Supports redundancy to prevent power supply failures.
  - Fault warning and prevention
  - Pre-fault preventive maintenance
  - Non-disruptive server services
- The power supply subsystem includes:
  - Intelligent PSU
  - Fan module

PSU

Fan module

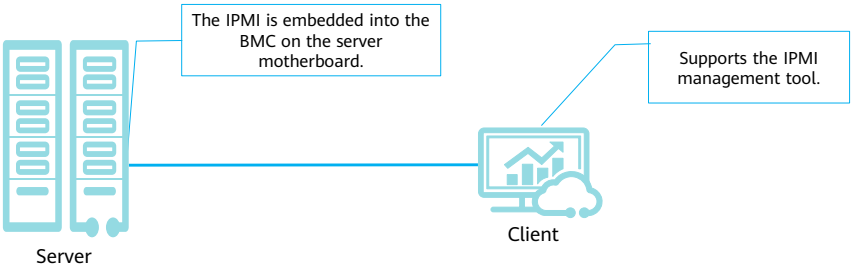
HUAWEI

- Power supply redundancy modes:
  - 1+1: In this mode, each module provides 50% of the output power. When one module is removed, the other provides 100% of the output power.
  - 2+1: In this mode, three modes are required. Each module provides 1/3 of the output power. When one module is removed, each of the other two modules provides 50% of the output power.
- *E9000 Blade Server Product Documentation*

Contents

What Is IPMI?

- Definition
  - The Intelligent Platform Management Interface (IPMI) is a set of open and standard hardware management interface specifications that defines specific methods for communication between embedded management subsystems.
  - IPMI information is exchanged using the baseboard management controller (BMC). Entry-level intelligent hardware, not the OS, handles management.



HUAWEI

- The IPMI is an industrial specification used for peripherals in Intel-based enterprise systems. This interface specification was laid down by Intel, HP, NEC, Dell, and SuperMicro. Users can use the IPMI to monitor the physical health status of servers, such as the temperature, voltage, fan status, and power status. Moreover, the IPMI is a free specification. Users do not need to pay for this specification.
- IPMI development:
  - In 1998, Intel, DELL, HP, and NEC put forward the IPMI specification. The temperature and voltage can be remotely controlled through the network.
  - In 2001, the IPMI was upgraded from version 1.0 to version 1.5. The PCI Management Bus function was added.
  - In 2004, Intel released the IPMI 2.0 specification, which is compatible with the IPMI 1.0 and 1.5 specifications. Console Redirection is added. Servers can be remotely managed through ports, modems, and LANs. In addition, security, VLANs, and blade servers are supported.

BMC

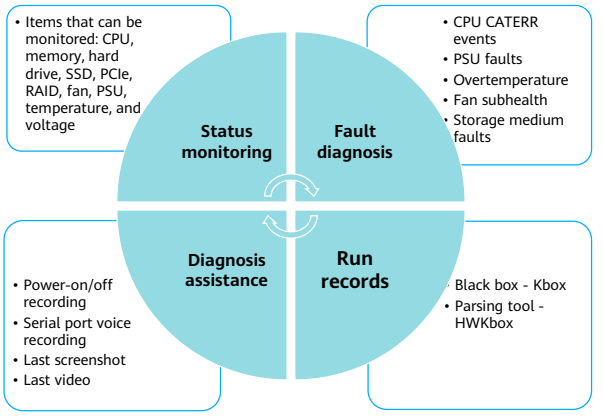
- Definition
  - The BMC complies with the IPMI specification. It collects, processes, and stores sensor signals, and monitors component operating status. It supplies the chassis management module with managed objects' hardware status and alarm information. The management module uses this information to manage the devices.

HUAWEI

- The BMC provides the following functions:
  - Remote control
  - Alarm management
  - Status check
  - Device information management
  - Heat dissipation control
  - Support for IPMItool
  - Web-based management
  - Centralized account management

iBMC

- The Huawei Intelligent Baseboard Management Controller (iBMC) is a Huawei proprietary embedded server management system designed for the whole server lifecycle.



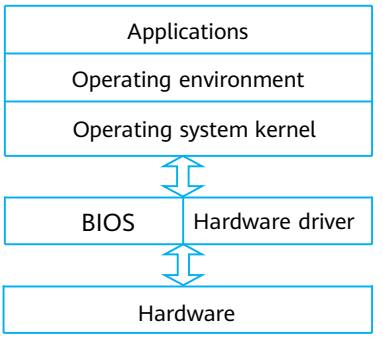
HUAWEI

- The iBMC provides a series of management tools for hardware status monitoring, deployment, energy saving, and security, and standard interfaces to build a comprehensive server management ecosystem. The iBMC uses Huawei-developed management chip Hi1710 and multiple innovative technologies to implement refined server management.
- The iBMC provides a variety of user interfaces, such as the CLI, web-based user interface, IPMI integration interface, SNMP integration interface, and Redfish integration interface. All user interfaces adopt the authentication mechanism and high-security encryption algorithm to enhance access and transmission security.

Contents

BIOS

- Basic Input/Output System (BIOS)
- The BIOS is a system's foundation: a group of programs providing the most direct control of system hardware.



BIOS functions:

- Hardware detection and initialization
- OS boot
- Advanced power management

HUAWEI

- The BIOS is a bridge between the system kernel and the hardware layer.
- Functions of the BIOS:
  - Software upgrade and loading
  - Basic OAM functions
  - Serial port management
  - Fault recovery
  - ECC management
  - Hardware diagnosis

Quiz

1. Which of the following statements are true about the NICs of Huawei servers?
   A. The LOM card is embedded into the PCH chip on the server motherboard and cannot be replaced.
   B. Huawei-developed PCIe cards can be installed in standard PCIe slots.
   C. A FlexIO card is integrated with the server panel for front-end service connection.
   D. Mezzanine cards can be used with Huawei rack servers.
2. The BMC complies with the IPMI specification. It collects, processes, and stores sensor signals, and monitors component operating status.
   A. True
   B. False

- Answers:
  - AB
  - A

Summary

- In this course, we have learned the basic concepts, development history, hardware components, and key technologies of servers. In the following course, we will learn about storage technologies. Stay tuned.

Recommendations

- Huawei iLearning
  - https://e.huawei.com/en/talent/portal/#/
- Huawei Support Case Library
  - https://support.huawei.com/enterprise/en/knowledge?lang=en

Acronyms and Abbreviations

- BIOS: Basic Input/Output System
- BMC: Baseboard Management Controller
- B/S: browser/server architecture
- C/S: client/server architecture
- CPU: Central Processing Unit
- iBMC: Huawei Intelligent Baseboard Management Controller
- IPMI: Intelligent Platform Management Interface
- MTBF: Mean Time Between Failures
- NIC: Network Interface Card
- RAID: Redundant Array of Independent Disks

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.

Storage Technology Basics

HUAWEI

Foreword

- Data is the most important asset for every enterprise. This course describes how and where data is stored, and provides the key data storage technologies in cloud computing.

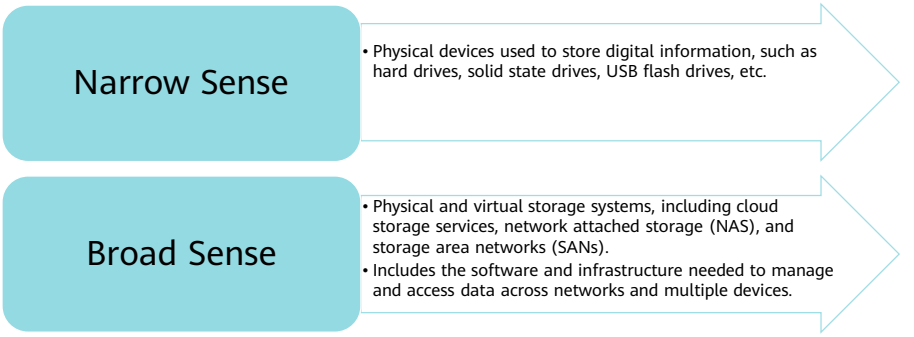
Objectives

- On completion of this course, you will be able to:
  - Understand mainstream data storage modes and network topologies.
  - Master RAID and Huawei RAID 2.0+ block virtualization technologies.
  - Distinguish between centralized and distributed storage.
  - Understand storage protocols and application scenarios.

Contents

What Is Storage?

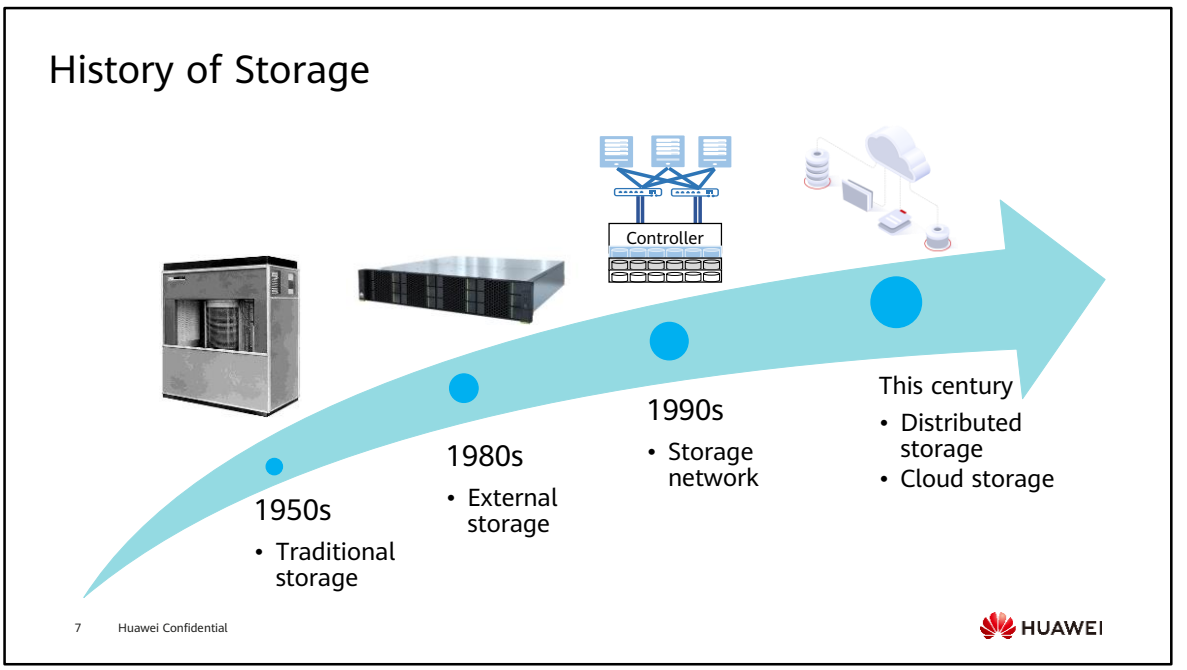
- Storage refers to the process of storing and managing digital information on a computer or other electronic device. It can include both physical storage devices, such as hard disks and solid state disks, and virtual storage systems, such as cloud storage services.
- The goal of storage is to provide a reliable and secure way to store and access data as needed.



HUAWEI

- Storage in a narrow sense: CDs, DVDs, ZIP drives, tapes, and disks...
- Storage in a broad sense:
  - Storage hardware (disk arrays, controllers, disk enclosures, and tape libraries)
  - Storage software (backup software, management software, and value-added software such as snapshot and replication)
  - Storage networks (HBAs, Fibre Channel switches, as well as Fibre Channel and SAS cables)
  - Storage solutions (centralized storage, archiving, backup, and disaster recovery)

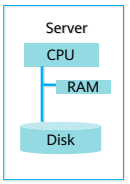
Contents



- The storage architecture has gone through the following development phases: traditional storage, external storage, storage network, distributed storage, and cloud storage.
- Traditional storage refers to individual disks. In 1956, IBM invented the world's first mechanical hard drive that has fifty 24-inch platters and the total storage capacity of just 5MB. It is about the size of two refrigerators and weighs more than a ton. It was used in the industrial field at that time and was independent of the mainframe.
- External storage refers to direct-attached storage. The earliest form of external storage is JBOD, which stands for Just a Bunch of Disks. JBOD is identified by the host as numerous independent disks. It provides large capacity but low security.
- A storage area network (SAN) is a typical storage network that transmits data mainly over a Fibre Channel network. Then, IP SANs emerge.
- Distributed storage uses general-purpose servers to build storage pools and is more suitable for cloud computing. This will be introduced later.

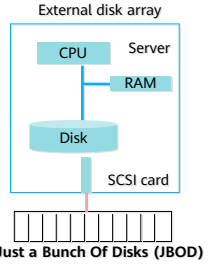
Storage Development - from Server Attached Storage to Independent Storage Systems

Disk in the server



Restrictions:
- Disks become the system performance bottleneck.
- The number of disk slots is limited, thereby limiting capacity.
- Data is stored on a single disk, lowering data reliability.
- Storage space utilization is low.
- Data is scattered in local storage systems.

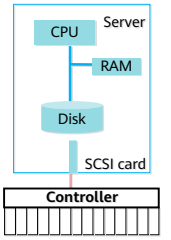
External disk array



JBOD logically connects several physical disks to increase capacity.

Problem solved:
- The number of disk slots is limited, thereby limiting capacity.

Intelligent disk array

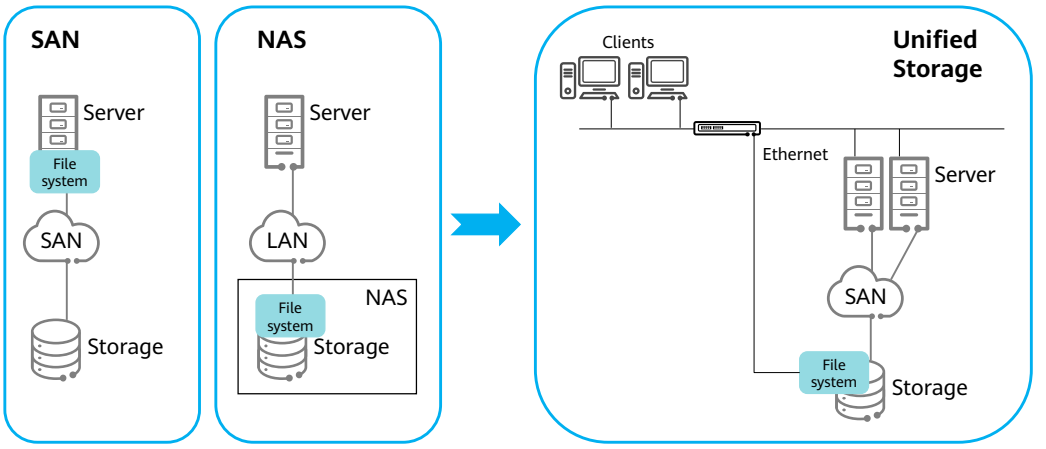


A controller provides the RAID function and large-capacity cache, and enables the disk array to have multiple functions for better read/write performance and data security.

Problems solved:
- Disks become the system performance bottleneck.
- The number of disk slots is limited, thereby limiting capacity.
- Data is stored on a single disk, lowering data reliability and read/write performance.

HUAWEI

From Separation to Convergence

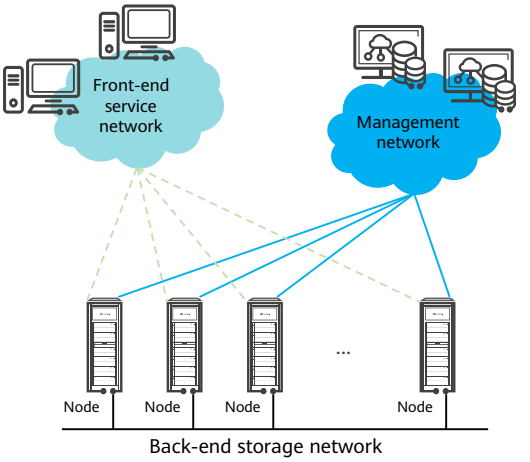


HUAWEI

- DAS has the following characteristics:
  - Scattered data
  - Low storage space utilization
- Storage development requirements:
  - Data sharing
  - Improved resource utilization
  - Distance extension
- The emergence of networks infuses new vitality to storage.
  - SAN: establishes a network between storage devices and servers to provide block storage services.
  - NAS: builds networks between servers and storage devices with file systems to provide file storage services.
- In 2011, unified storage that supported both SAN and NAS protocols became popular. Storage convergence set a new trend: NAS and SAN were converged to provide both database and file sharing services, simplifying storage management, and improving storage utilization.

Scale-out Storage

- Physical resources are organized using software to form a high-performance logical storage pool, ensuring reliability and providing multiple storage services.
- Generally, scale-out storage scatters data to multiple independent storage servers in a scalable system structure. It uses those storage servers to share storage loads and uses location servers to locate storage information.

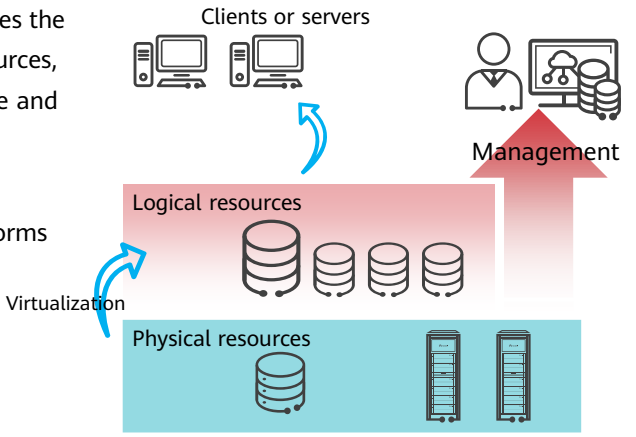


HUAWEI

- The scalability and flexibility of storage systems in the traditional architecture are limited.
- Scale-out storage architecture:
  - Universal hardware, unified architecture, and storage-network decoupling
  - Linear expansion of performance and capacity, up to thousands of nodes
  - Elastic resource scaling and high resource utilization

Storage Virtualization

- Storage virtualization consolidates the storage devices into logical resources, thereby providing comprehensive and unified storage services.
- Unified functions are provided regardless of different storage forms and device types.

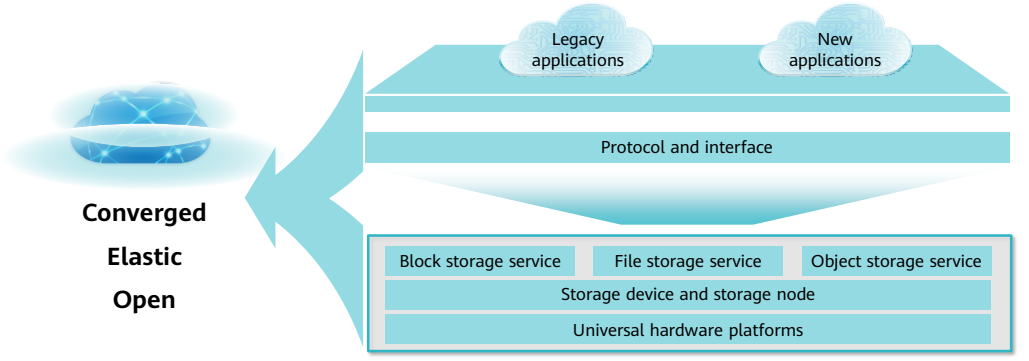


HUAWEI

- In storage virtualization, a virtualization layer is added between the physical storage system and servers to manage and control all storage devices, and provide storage for servers.
- The addition, deletion, replacement, splitting, and combination of storage hardware are transparent to servers.
- Functions:
  - Simplify the management of physical devices.
  - Integrate existing functions.
  - Eliminate the limitation of the physical capacity.

Cloud Storage

- The cloud storage system combines multiple storage devices, applications, and services. It uses highly virtualized multi-tenant infrastructure to provide scalable storage resources for enterprises. Those storage resources can be dynamically configured based on organization requirements.



HUAWEI

- The cloud storage system uses clustered applications, grid technologies, or scale-out file systems to coordinate various storage devices over the networks to provide data storage and service access.

Contents

Introduction to Disks

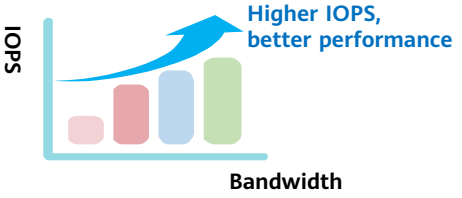
- Disks can be considered the most important storage device of a computer.
- A disk interface is a component used to connect a disk to a host. It transmits data between the disk cache and the host memory. The disk interface type determines the connection speed between the disk and the computer, the program running speed, and system performance.

	SATA	SAS	NL-SAS	SSD
Rotational speed (rpm)	7,200	15,000/10,000	7,200	N/A
Serial/Parallel	Serial	Serial	Serial	Serial
Capacity (TB)	1 TB/2 TB/3 TB	0.6 TB/0.9 TB	2 TB/3 TB/4 TB	0.6 TB/0.8 TB/1.2 TB/1.6 TB
MTBF (h)	1,200,000	1,600,000	1,200,000	2,000,000
Remarks	Being developed from ATA disks, SATA 3.0 supports up to 600 MB/s data transfer. The annual failure rate of SATA disks is about 2%.	SAS disks are designed to meet enterprises' high performance requirements, and are compatible with SATA disks. The transmission rate ranges from 3.0 Gbit/s to 6.0 Gbit/s, and will be increased to 12.0 Gbit/s. The annual failure rate of SAS disks is less than 2%.	NL-SAS disks are enterprise-class SATA drives with SAS interfaces. They are applicable to storage tiering in a disk array, which simplifies the design of the disk array. The annual failure rate of NL-SAS disks is about 2%.	Solid state disks (SSDs) are made up of solid-state electronic storage chip arrays. Each SSD consists of a control unit and a storage unit (DRAM or flash chip). SSDs are the same as the common disks in the regulations and definition of interfaces, functions, usage, as well as the exterior and size.

- MTBF: Mean Time Between Failure
- Increasing order of price: SATA and NL-SAS disks, SAS disks, and SSDs

Disk Key Indicators

- Disk capacity
- Rotational speed (HDD only)
- Average access time
- Data transfer rate
- Input/Output operations per second (IOPS)



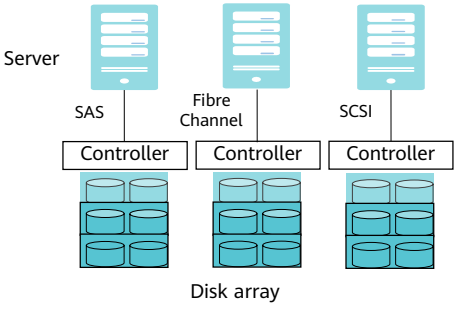
Disk Type	IOPS (4 KB random write)	Bandwidth (128 KB sequential read)
SATA	330	200 MB/s
SAS 10K	350	195 MB/s
SAS 15K	450	290 MB/s
SATA SSD	30,000 to 60,000	540 MB/s
SAS SSD	155,000	1000 MB/s
NVMe SSD	300,000	3500 MB/s

HUAWEI

- **Disk capacity**: The capacity is measured in MB or GB. The factors that affect the disk capacity include the single platter capacity and the number of platters.
- **Rotational speed**: The rotational speed is the number of rotations made by disk platters per minute. The unit is rotation per minute (rpm). In most cases, the rotational speed of a disk reaches 5400 rpm or 7200 rpm. The disk that uses the SCSI interface reaches 10,000 rpm to 15,000 rpm.
- **Average access time** = Average seek time + Average wait time
- **Data transfer rate**: The data transfer rate of a disk is the speed at which the disk reads and writes data. It is measured in MB/s. The rate consists of the internal data transfer rate and the external data transfer rate.
- **Input/Output operations per second (IOPS)**: indicates the number of input/output operations or read/write operations per second. It is a key indicator to measure disk performance. For applications with frequent random read/write operations, such as online transaction processing (OLTP), IOPS is a key indicator. Another key indicator is the data throughput, which indicates the amount of data that can be successfully transferred per unit time. For applications that require a large number of sequential read/write operations, such as video editing and video on demand (VoD) at TV stations, the throughput is more of a focus.

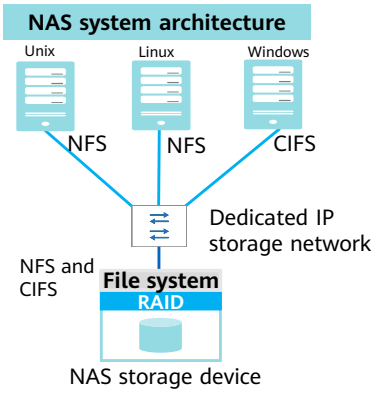
Contents

Introduction to DAS



- **Direct attached storage (DAS)**
- **Time**: 1970s
- **Background**: Data explosion drove up huge demand for storage. A simple storage architecture, DAS, was then introduced.
- **Connection mode**: **Fibre Channel, SCSI, or SAS**
- **Access mode**: The connection channels between DAS and server hosts often use SAS.
- **Link rate**: 3 Gbit/s、6 Gbit/s、12 Gbit/s
- **Provides functions, such as snapshot and backup.**

Introduction to NAS(1)

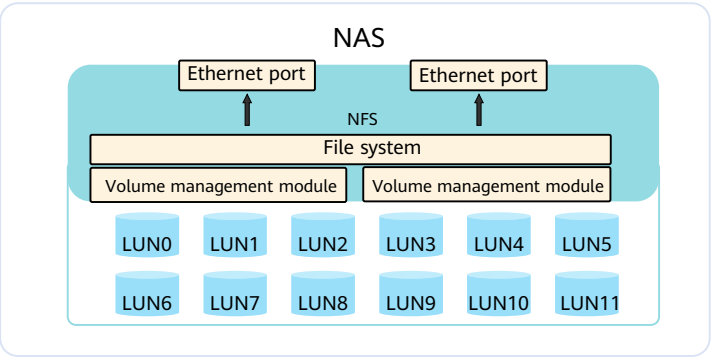


- **Network attached storage (NAS)**
- **Time**: early 1990s
- **Background**: Developing networks drove the need for large-scale data sharing and exchange, leading to dedicated NAS storage devices.
- **Access mode**: Multiple front-end servers share space on back-end NAS storage devices using CIFS or NFS Concurrent read and write operations can be performed on the same directory or file.
- **The file system is on the back-end storage device.**

- **Network File System (NFS)** is an Internet standard protocol created by Sun Microsystems in 1984 for file sharing between systems on a local area network (LAN).
- Linux NFS clients support NFSv2 [RFC1094], NFSv3 [RFC1813], and NFSv4 [RFC3530]. NFSv2 that uses the User Datagram Protocol (UDP) is outdated due to its limited data access and transmission capabilities.
  - NFSv3, released in 1995, is widely used because Transmission Control Protocol (TCP) is added for transmission.
  - NFSv4, released in 2003, achieves better performance and security.
- NFS uses the Remote Procedure Call (RPC) protocol.
  - RPC provides a set of operations to achieve remote file access that are not restricted by machines, OSs, and lower-layer transmission protocols. It allows remote clients to access storage over a network like accessing a local file system.
  - The NFS client sends an RPC request to the NFS server. The server transfers the request to the local file access process, reads the local disk files on the server, and returns the files to the client.
- **Common Internet File System (CIFS)** is a network file system protocol used for sharing files and printers between machines on a network. CIFS is mainly used to share network files between hosts running Windows.

Introduction to NAS(2)

- NAS supports the centralized management of scattered and independent data, facilitating access to various hosts and application servers.

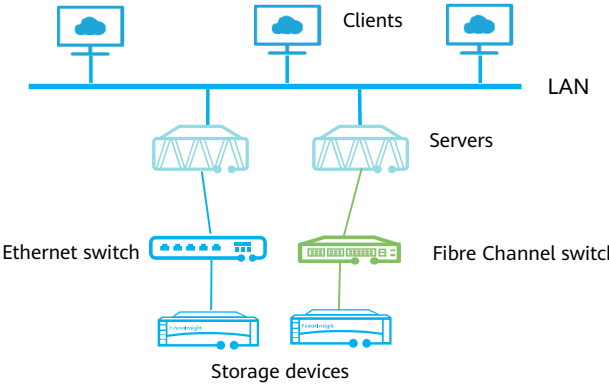


HUAWEI

- NAS can serve as a network node and be directly connected to the network. In theory, NAS can support various network technologies and topologies. As Ethernet is the most popular network connection mode nowadays, we mainly discuss the NAS environment on the Ethernet.
- NAS supports multiple protocols (such as NFS and CIFS) and supports various OSs. Users can conveniently manage NAS devices by using Internet Explorer or Netscape on any work station.

Introduction to SAN

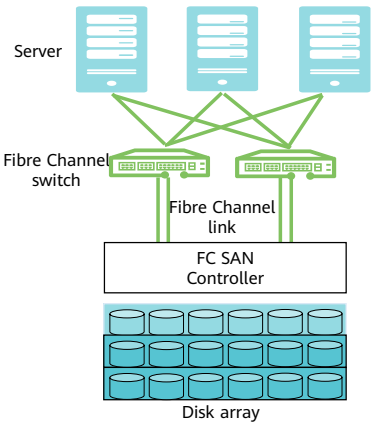
- A storage area network (SAN) is a dedicated storage network that connects one or more network storage devices to servers.



HUAWEI

- A SAN is a high-performance and dedicated storage network used between servers and storage resources. It is a back-end storage network independent from a LAN. The SAN adopts a scalable network topology for connecting servers and storage devices. The storage devices do not belong to any of the servers but can be shared by all the servers on the network.
- The SAN that uses Fibre Channel Protocol (FCP) to set up connections between servers and storage devices through Fibre Channel switches is called an FC SAN. Fibre Channel is especially suitable for SANs, because it supports long-distance and large-block transfer. The SAN mainly applies to high-end and enterprise-class storage applications, which have demanding requirements for performance, redundancy, and data availability.
- With the development of storage technologies, IP SANs based on TCP/IP also gains popularity. IP SANs feature high scalability, flexible interworking, long-distance data transmission, easy management and maintenance, and cost advantages.
- The major difference between NAS and SAN is that NAS provides a file operation and management system while SAN does not. SAN provides only data management, which is the layer below file management. SAN and NAS do not conflict with each other. They can coexist on the same network. However, NAS implements storage space management and resource sharing through a public interface, while SAN provides only a quick dedicate back-end channel for servers to store data.

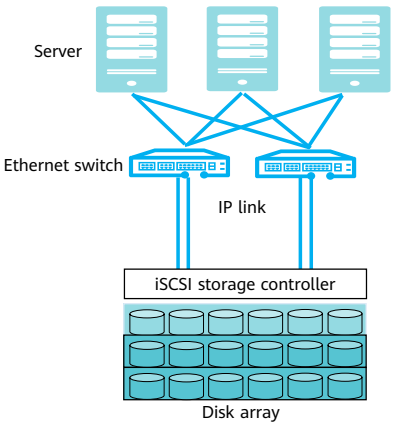
Introduction to FC SAN



- **Fibre Channel storage area network (FC SAN)**
- **Time**: middle and late 1990s
- **Background**: To solve the poor scalability issue of DAS, storage devices was networked. More than 100 servers can be connected in a network.
- **Connection mode**: Fibre Channel link; Fibre Channel switch
- **Access mode**: The storage space on the back-end storage device can be divided into multiple LUNs. Each LUN belongs to only one front-end server.
- **Link rate**: 2 Gbit/s, 4 Gbit/s, or 8 Gbit/s
- **Provides advanced data protection functions, such as snapshot and disaster recovery.**

- Fibre Channel (FC) is a standard data storage network used to transmit 100 Mbit/s to 4.25 Gbit/s signals over fiber or copper cables. It is a high-speed transport technology used to build SANs. Fibre Channel is primarily used for transporting SCSI traffic from servers to disk arrays, but it can also be used on networks carrying ATM and IP traffic.

Introduction to IP SAN



- **IP storage area network (IP SAN)**
- **Time**: 2001
- **Background**: IP SAN is designed to solve the price and management issues of the FC SAN.
- **Connection mode**: Ethernet link; Ethernet switch
- **Access mode**: The storage space on the back-end storage device can be divided into multiple LUNs. Each LUN belongs to only one front-end server.
- **Link rate**: 1 Gbit/s, or 10 Gbit/s
- The IP SAN provides advanced data protection functions, such as snapshot and disaster recovery.
- iSCSI is a mainstream choice because:
  - Mature IP network management tools and infrastructure can be used.
  - IP networks are widely used, which can reduce a large number of construction, management, and personnel costs.

HUAWEI

- **Internet Small Computer System Interface (iSCSI)** is a storage technology based on the Internet and SCSI-3 protocol. It transmits the SCSI protocol, originally used only for local hosts, over the TCP/IP network to extend the connection distance. In the following course, we will learn about the protocol encapsulation, working principles, and application scenarios.

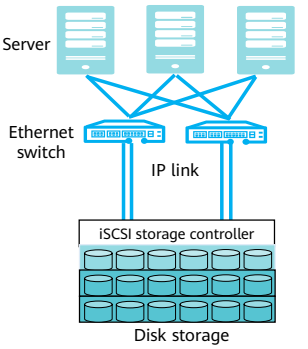
Comparison Between Storage Networking Types

	DAS	NAS	SAN	
			FC SAN	IP SAN
Transmission mode	SCSI, Fibre Channel, and SAS	IP	Fibre Channel	IP
Data type	Block-level	File-level	Block-level	Block-level
Application scenario	Any	File servers	Database applications	Video security
Advantage	Easy to understand; robust compatibility	Easy to install; low cost	High scalability and performance; high availability	Strong scalability; low cost
Disadvantage	Difficult management; limited scalability; low storage space utilization	Low performance; inapplicable to some applications	Expensive and complex configuration; poor networking compatibility	Low performance

Contents

Centralized Storage

- A centralized storage system refers to one set of storage system consisting of multiple devices. Enterprises often deploy their storage devices on a centralized environment. For example, the Huawei storage system may need several cabinets to house devices. In terms of technical architectures, centralized storage is classified into SAN (including FC SAN and IP SAN) and NAS storage.
- Centralized storage has a simple deployment structure, which means you do not need to consider how to deploy multiple nodes for a service, or the distributed collaboration between multiple nodes.

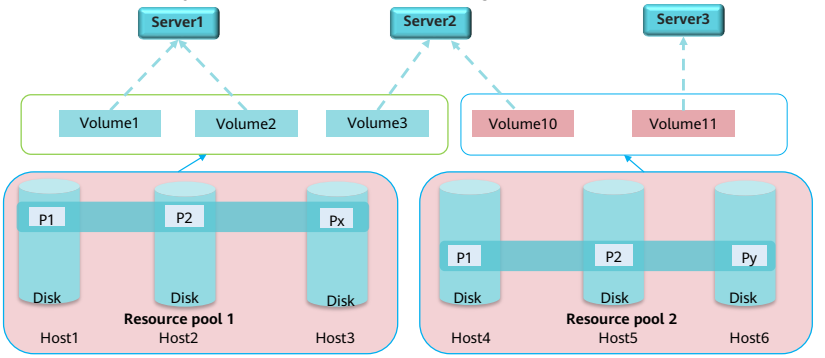


HUAWEI

- Disadvantages of centralized storage:
  - Isolated storage resources: Storage devices are connected to a limited number of servers through a dedicated network.
  - Scale-up by adding disk enclosures: The hardware controller performance (a single controller with disks) becomes a bottleneck.
  - Scale-out by connections between controllers: The hardware controller performance becomes a bottleneck.
  - No resource sharing: Storage devices and resources are provided by different vendors, and resources cannot be shared among devices. Storage pools are isolated in data centers.
  - Centralized metadata management: The system concurrency is limited by the metadata service performance. The metadata service becomes the performance bottleneck.
- How to solve the capacity expansion and performance bottleneck issues of traditional centralized storage?

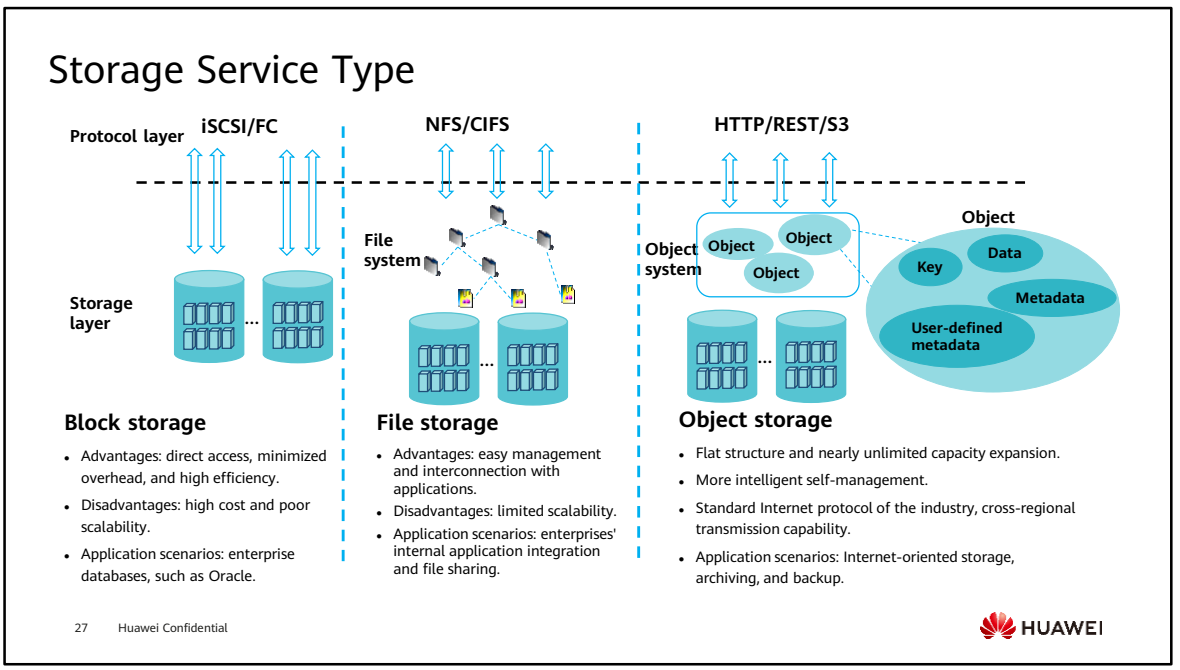
Distributed Storage

- A distributed storage system stores data on multiple independent devices. It adopts a scalable system architecture and enables multiple storage servers to share the storage load, improving scalability, reliability, availability, and access efficiency. As distributed storage is becoming more popular, some applications requiring high performance, such as databases of financial systems, also use distributed storage.



HUAWEI

- Distributed storage uses software to simulate the functions of the original hardware controllers, avoiding the disadvantages of the hardware controllers.
- Resource pool: A resource pool is similar to a RAID group in SAN storage.



- Users can access data in an object storage as fast as in a SAN storage and can share data as easy as in a NAS storage. Object storage has high reliability and secure data sharing between platforms. The following describes the comparison among the object storage, block storage, and file storage:
  - **Block storage** directly accesses the storage layer, featuring fast speed, minimum overhead, and maximum efficiency. However, block storage has the high cost and poor scalability. Block storage employs iSCSI and Fibre Channel. Therefore, it is difficult to transmit data across networks. Block storage is applicable to enterprise databases, such as Oracle.
  - **File storage** creates a file system on the basis of block storage. Data is organized in the directory-directory-file mode, facilitating data management. The objects operated by most application programs are files. Therefore, file storage enables easier interworking with application systems. File systems are restricted by directory trees. Therefore, a file system can be typically expanded to dozens of PB at most. The scalability is limited. File systems are applicable to application integration and file sharing in an enterprise.

- **Object storage** creates the object management layer above block storage. Compared with the file system, the object system is flat with little expansion limitation. An object consists of a unique key, file, data (file), metadata, and user-defined metadata. An object contains self-management information. Therefore, object storage is more intelligent. Using compatible standard Internet protocol interfaces, object storage supports cross-region transmission. Object storage applies to storage scenarios for Internet services, and internal arching and backup scenarios for enterprises.

Contents

What Is RAID?

- Redundant Array of Independent Disks (RAID) combines multiple physical disks into one logical disk in different ways, improving read/write performance and data security.
  - RAID levels based on combination methods

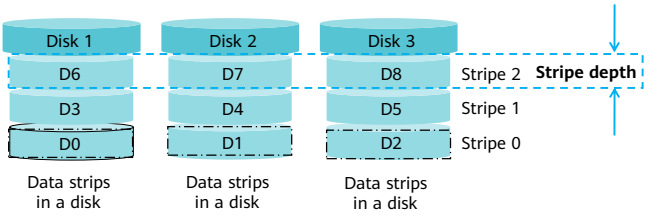
RAID 0	Data striping, no parity
RAID 1	Data mirroring, no parity
RAID 3	Data striping, with dedicated parity
RAID 5	Data striping, with distributed parity
RAID 6	Data striping, with double distributed parity

  - RAID levels by using two different RAID modes

RAID 0+1	Create RAID 0 and then RAID 1, providing data striping and mirroring.
RAID 10	Similar to RAID 0+1. The difference is that RAID 1 is created before RAID 0.
RAID 50	Create RAID 5 and then RAID 0, effectively improving the performance of RAID 5.

RAID Data Distribution

- Disk striping: Space in each disk is divided into multiple strips of a specific size. Written data is also divided into blocks based on the strip size.
- Strip: A strip consists of one or more consecutive sectors in a disk, and multiple strips form a stripe.
- Stripe: A stripe consists of strips of the same location or ID on multiple disks in the same array.

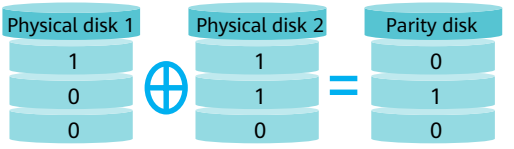


HUAWEI

- Stripe width
  - Indicates the number of disks in an array for striping. For example, if a disk array consists of three member disks, the stripe width is 3.
- Stripe depth
  - Indicates the size of a stripe.

RAID Data Protection

- 1. Mirroring: Data copies are stored on another redundant disk.
- 2. Parity check algorithm (XOR)
  - XOR is widely used in digital electronics and computer science.
  - XOR is a logical operation that outputs true only when inputs differ (one is true, the other is false).
    - 0 ⊕ 0 = 0, 0 ⊕ 1 = 1, 1 ⊕ 0= 1, 1 ⊕ 1 = 0



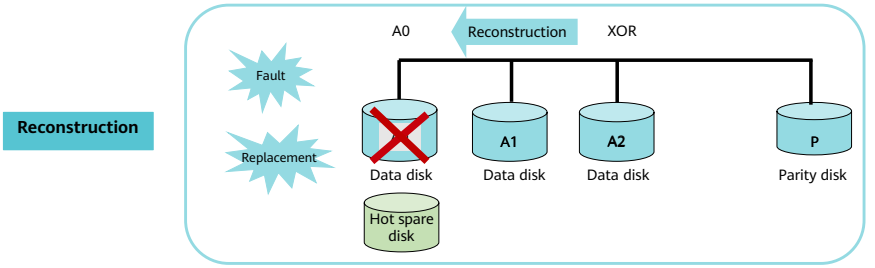
XOR for redundant backup

HUAWEI

- RAID generally protects data by the following methods:
  - Stores data copies on a redundant disk to improve reliability and read performance.
  - Uses the parity check algorithm. Parity data is additional information calculated using user data. For a RAID array that uses parity, an additional parity disk is required. The XOR (symbol: ⊕) algorithm is used for parity.

RAID Hot Spare and Reconstruction

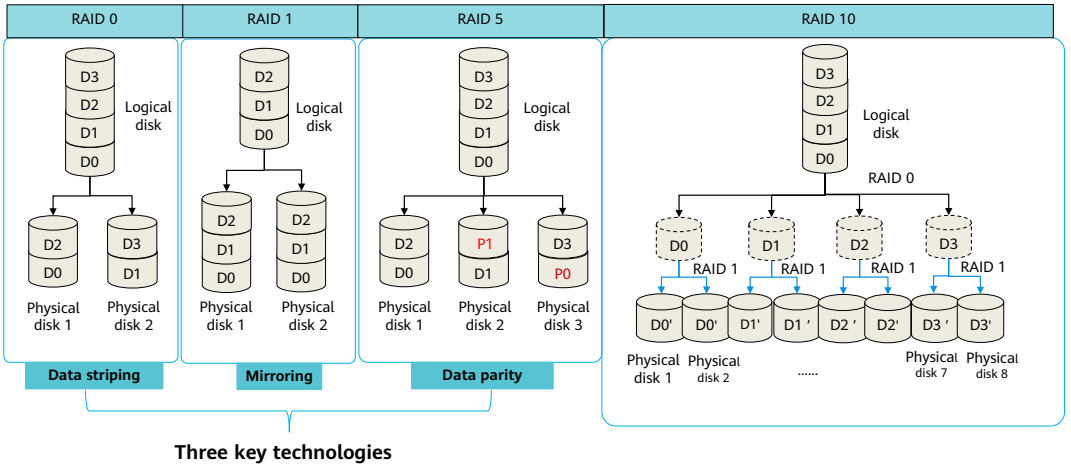
- Hot spare
  - If a disk in a redundant RAID group is faulty, a functional backup disk in the RAID group can automatically replace the faulty one to ensure RAID system redundancy.
- Hot spare can be classified into the following types:
  - Global: The spare disk is shared by all RAID groups in the system.
  - Dedicated: The spare disk is used only by a specific RAID group in the system.



HUAWEI

- Data parity: Redundant data is used to detect and rectify data errors. The redundant data is usually calculated through Hamming check or XOR operations. Data parity can greatly improve the reliability, performance, and error tolerance of the disk arrays. However, the system needs to read data from multiple locations, calculate, and compare data during the parity process, which affects system performance.
- Generally, RAID cannot be used as an alternative to data backup. It cannot prevent data loss caused by non-disk faults, such as viruses, man-made damages, and accidental deletion. Data loss here refers to the loss of operating system, file system, volume manager, or application system data, not the RAID data loss. Therefore, data protection measures, such as data backup and disaster recovery, are necessary. They are complementary to RAID, and can ensure data security and prevent data loss at different layers.

Common RAID Levels

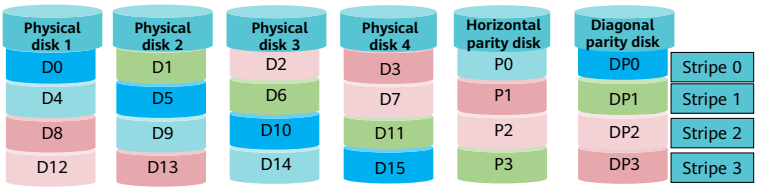


HUAWEI

- RAID 0 consists of striping without fault tolerance. Data of the RAID group is evenly distributed on all disks in stripe form.
- RAID 1, also called mirroring, can simultaneously write data into the primary disk and mirror disk.
- RAID 3 consists of striping with dedicated parity. Data is striped on data disks, and parity data is stored on a dedicated parity disk.
- RAID 5 is similar to RAID 3 except that parity information is evenly distributed among data disks. RAID member disks store both the data and the parity information, and data blocks and corresponding parity information are stored on different disks. RAID 5 is one of the most commonly used RAID levels.
- RAID 10 combines mirroring and striping. The first level is RAID 1 mirrored pairs, and the second level is RAID 0. RAID 10 is also a widely used RAID level.

Working Principles of RAID 6 DP

- Double parity (DP): In addition to the horizontal XOR parity disk used in RAID 4, it adds another disk to store diagonal XOR parity data.
- P0 to P3 on the horizontal parity disk are the parity information of horizontal data on all data disks.
  - For example, P 0 = D 0 XOR D 1 XOR D 2 XOR D 3
- DP 0 to DP 3 in the diagonal parity disk represent the diagonal parity data for respective data disks and the horizontal parity disk.
  - For example, DP 0 = D 0 XOR D 5 XOR D 10 XOR D 15



HUAWEI

- RAID 6 DP has two independent parity data blocks: horizontal parity data and diagonal parity data.
- Parity values in the horizontal parity disk are also called parity check values, which are obtained by performing the XOR operation on user data in the same stripe.As shown in the following figure,P0 is obtained by performing an XOR operation on D0, D1, D2, and D3 on a stripe 0, and P1 is obtained by performing an XOR operation on D4, D5, D6, and D7 on a stripe 1. Therefore, P0 = D0 ⊕D1⊕ D2⊕D3, P1 = D4⊕D5⊕D6⊕D7, and so on.
- The diagonal parity uses the diagonal XOR operation to obtain the row-diagonal parity data block. A process of selecting a data block is relatively complex. DP0 is obtained by performing an exclusive OR operation on D0 on a stripe 0 of a hard disk 1, D5 on a stripe 1 of a hard disk 2, D10 on a stripe 2 of a hard disk 3, and D15 on a stripe 3 of a hard disk 4. DP1 is obtained by performing an exclusive OR operation on D1 on a stripe 0 of a hard disk 2, D6 on a stripe 1 of a hard disk 3, D11 on a stripe 2 of a hard disk 4, and P3 on a stripe 3 of a first parity hard disk. DP2 is obtained by performing an exclusive OR operation on D2 on a stripe 0 of a hard disk 3, D7 on a stripe 1 of a hard disk 4, P2 on a stripe 2 of an odd even hard disk, and D12 on a stripe 3 of a hard disk 1. Therefore, DP0 = D0⊕D5⊕D10⊕D15, DP1 = D1⊕D6⊕D11⊕P3, and so on.

- A RAID 6 array tolerates failures of up to two disks.
- Performance of a RAID 6 group: Dual-disk verification is used, and the performance is relatively slow. Therefore, RAID 6 applies to the following two scenarios:
    - Data is critical and should be consistently online and available.
    - The disk capacity is large (usually greater than 2 TB). The reconstruction of a large-capacity disk takes a long time. Data will be inaccessible for a long time if two disks fail at the same time. A RAID 6 array tolerates failure of another disk during the reconstruction of one disk. Some enterprises want to use a dual-redundancy RAID array for their large-capacity disks.

Introduction to RAID 2.0

- **RAID 2.0**
  - RAID 2.0 is an enhanced RAID technology that effectively resolves the following problems: prolonged reconstruction of an HDD, and data loss if a disk is faulty during the long reconstruction of a traditional RAID group.
- **RAID 2.0+**
  - RAID 2.0+ provides smaller resource granularities (tens of KB) than RAID 2.0 to serve as the units of standard allocation and reclamation of storage resources, similar to VMs in computing virtualization. This technology is called virtual block technology.
- **Huawei RAID 2.0+**
  - Huawei RAID 2.0+ is a new RAID technology that overcomes traditional RAID issues. Huawei RAID 2.0+ evolves in line with the storage architecture virtualization to implement two-layer virtualized management instead of the traditional fixed management. Based on the underlying disk management that employs block virtualization (Virtual for Disk), RAID 2.0+ uses Smart-series efficiency improvement software to implement efficient resource management that features upper-layer virtualization (Virtual for Pool).

- Block virtualization is to divide disks into multiple contiguous storage spaces of a fixed size called a chunk (CK).

RAID 2.0+ Block Virtualization

- If data is not evenly stored on SSDs, some heavily loaded SSDs may become the system bottleneck.
- The storage system uses RAID 2.0+ for fine-grained division of SSDs to evenly distribute data to all LUNs on each SSD and balance loads.

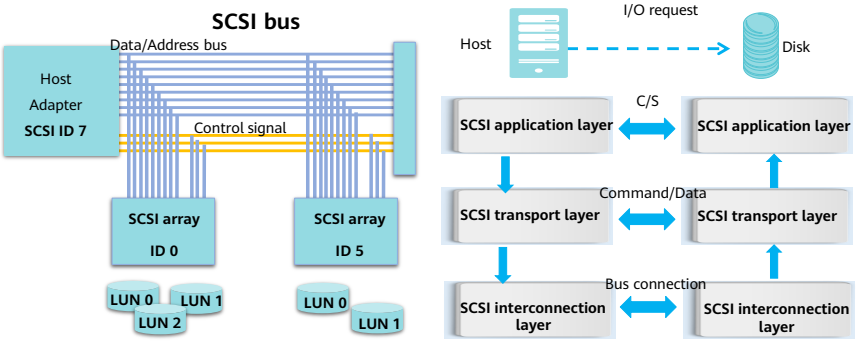
1. Multiple SSDs form a storage pool.
2. Each SSD is then divided into CKs of a fixed size (typically 4 MB) for logical space management.
3. CKs from different SSDs form chunk groups (CKGs) based on the RAID policy specified on DeviceManager.
4. CKGs are further divided into grains (typically 8 KB). Grains are mapped to LUNs for refined management of storage resources.

- RAID 2.0+ has the following advantages over traditional RAID:
  - Balanced service loads for zero hotspots. Data is evenly distributed to all SSDs in a storage resource pool, ensuring no SSD becomes a hotpot, thereby lowering the SSD failure rate.
  - Quick reconstruction for a lowered data loss risk. Faulty SSDs trigger data reconstruction on all the other SSDs in the storage pool. This many-to-many reconstruction is rapid and significantly reduces data vulnerability.
  - All SSDs in a storage resource pool participate in reconstruction, and each SSD only needs to reconstruct a small amount of data. Therefore, the reconstruction process does not affect upper-layer applications.

Contents

SCSI

- Small Computer System Interface (SCSI) is an interface technology developed for midrange computers and used for connecting between hosts and peripheral devices.



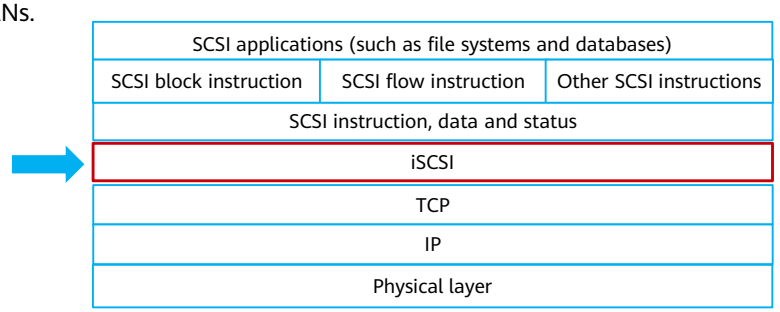
HUAWEI

- Computers communicate with storage systems through buses. The bus is a path through which data is transferred from the source device to the target device. To put it simple, the high-speed cache of the controller functions as the source device and transfers data to target disks, which serve as the target devices. The controller sends a signal to the bus processor requesting to use the bus. After the request is accepted, the controller's high-speed cache sends data. During this process, the bus is occupied by the controller and other devices connected to the same bus cannot use it. However, the bus processor can interrupt the data transfer at any time and allow other devices to use the bus for operations of a higher priority.
- A computer has numerous buses, which are like high-speed channels used for transferring information and power from one place to another. For example, the universal serial bus (USB) port is used to connect an MP3 player or digital camera to a computer. The USB port is competent to the data transfer and charging of portable electronic devices that store pictures and music. However, the USB bus is incapable of supporting computers, servers, and many other devices.

- In this case, SCSI buses are applicable. SCSI, short for Small Computer System Interface, is an interface used to connect between hosts and peripheral devices including disk drives, tape drives, CD-ROM drives, and scanners. Data operations are implemented by SCSI controllers. Like a small CPU, the SCSI controller has its own command set and cache. The special SCSI bus architecture can dynamically allocate resources to tasks run by multiple devices in a computer. In this way, multiple tasks can be processed at the same time.

iSCSI

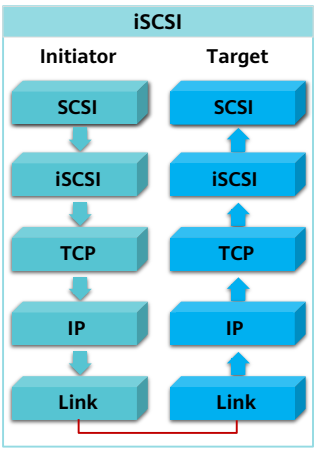
- iSCSI encapsulates SCSI commands and block data into TCP packets and transmits the packets over an IP network. iSCSI uses mature IP network technologies to implement and extend SANs.



- The SCSI controller card is used to connect to multiple devices to form a network. The devices can communicate with each other on the network but cannot be shared on the Ethernet. If devices form a network through SCSI and the network can be mounted to an Ethernet, the devices can interconnect and share with other devices as network nodes. As a result, the iSCSI protocol evolved from SCSI. The IP SAN using iSCSI converts user requests into SCSI codes and encapsulates data into IP packets for transmission over the Ethernet.
- The iSCSI scheme was initiated by Cisco and IBM and then advocated by Adaptec, Cisco, HP, IBM, Quantum, and other companies. iSCSI offers a way of transferring data through TCP and saving data on SCSI devices. The iSCSI standard was drafted in 2001 and submitted to IETF in 2002 after numerous arguments and modifications. In Feb. 2003, the iSCSI standard was officially released. The iSCSI technology inherits advantages of traditional technologies and develops based on them. On one hand, SCSI technology is a storage standard widely applied by storage devices including disks and tapes. It has been keeping a fast development pace since 1986. On the other hand, TCP/IP is the most universal network protocol and IP network infrastructure is mature. The two points provide a solid foundation for iSCSI development.
- Prevalent IP networks allow data to be transferred over LANs, WANs, or the Internet using new IP storage protocols. The iSCSI protocol is developed by this philosophy. iSCSI adopts IP technical standards and converges SCSI and TCP/IP protocols. Ethernet users can conveniently transfer and manage data with a small investment.

iSCSI Initiator and Target

- Initiator
  - The SCSI layer generates command descriptor blocks (CDBs) and transfers them to the iSCSI layer.
  - The iSCSI layer generates iSCSI protocol data units (PDUs) and sends them to the target over an IP network.
- Target
  - The iSCSI layer receives PDUs and sends CDBs to the SCSI layer.
  - The SCSI layer interprets CDBs and gives responses when necessary.



HUAWEI

- The iSCSI communication system inherits some of SCSI's features. The iSCSI communication involves an initiator that sends I/O requests and a target that responds to the I/O requests and executes I/O operations. After a connection is set up between the initiator and target, the target controls the entire process as the primary device.
- There are three types of iSCSI initiators: software-based initiator driver, hardware-based TCP offload engine (TOE) NIC, and iSCSI HBA. Their performance increases in that order.
- iSCSI targets include iSCSI disk arrays and iSCSI tape libraries.
- The iSCSI protocol defines a set of naming and addressing methods for iSCSI initiators and targets. All iSCSI nodes are identified by their iSCSI names. This method distinguishes iSCSI names from host names.
- iSCSI uses iSCSI names to identify initiators and targets. Addresses change with the relocation of initiator or target devices, but their names remain unchanged. When setting up a connection, an initiator sends a request. After the target receives the request, it checks whether the iSCSI name contained in the request is consistent with that bound with the target. If the iSCSI names are consistent, the connection is set up. Each iSCSI node has a unique iSCSI name. One iSCSI name can be used in the connections from one initiator to multiple targets. Multiple iSCSI names can be used in the connections from one target to multiple initiators.

Discussion:

- We have learned the FC SAN and IP SAN. Now assume that two sites use different networks FC SAN and TCP/IP. How can storage devices at the two sites communicate with each other?

  - To converge Fibre Channel and TCP?

Convergence of Fibre Channel and TCP

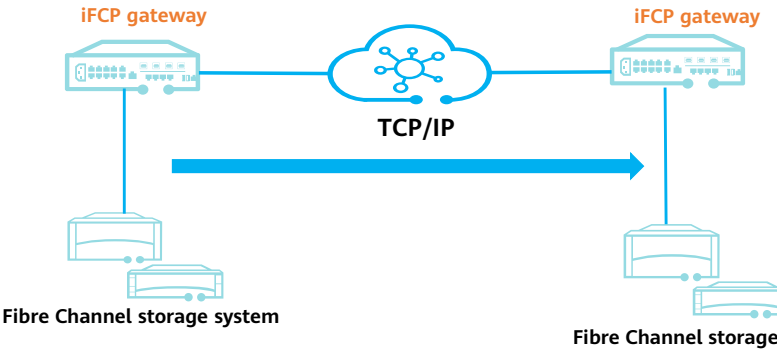
- Ethernet technologies and Fibre Channel technologies are both developing fast. Therefore, it is inevitable that IP SAN and FC SAN that are complementary coexist for a long time.
- Fibre Channel over a TCP/IP network:
  - iFCP
  - FCoE

HUAWEI

- **Fibre Channel over IP (FCIP)** is an IETF proposed standard that defines the Fibre Channel architecture over TCP/IP links. FCIP uses the current IP protocol and facilities to connect the tunnels of two Fibre Channel SANs at different places.
- **Internet Fibre Channel Protocol (iFCP)** is a gateway-to-gateway protocol that provides Fibre Channel communication services for optical devices on TCP/IP networks. iFCP delivers congestion control, error detection, and recovery functions through TCP. The purpose of iFCP is to enable current Fibre Channel devices to interconnect and network at the line rate over an IP network. The frame address conversion method defined in this protocol allows Fibre Channel storage devices to be added to the IP-based network through transparent gateways.
- **Fibre Channel over Ethernet (FCoE)** transmits Fibre Channel signals over an Ethernet, so that Fibre Channel data can be transmitted at the backbone layer of a 10 Gbit/s Ethernet using the Fibre Channel protocol.
- **IP over Fibre Channel (IPFC)** uses the Fibre Channel connections between two servers as IP data exchange media. To do this, IPFC defines how to transmit IP packets over a Fibre Channel network. Like all other application protocols, IPFC is implemented by a device driver in an operating system. The **ifconfig** or **ipconfig** command is executed for local IP connections. Then the IPFC driver addresses the Fibre Channel HBA. After that, IP packets can be transmitted through Fibre Channel.

iFCP

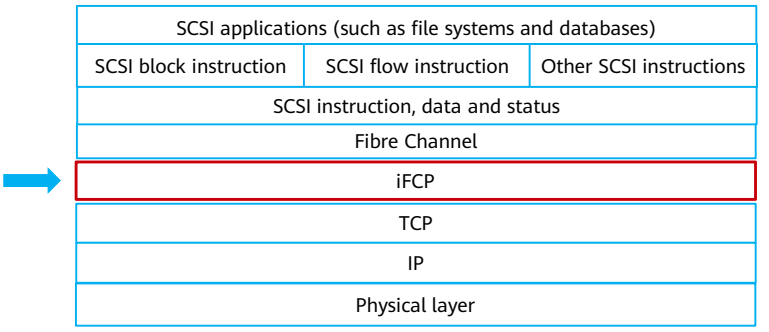
- Internet Fibre Channel Protocol (iFCP) is a gateway-to-gateway protocol that provides Fibre Channel communication services for optical devices on TCP/IP networks to implement end-to-end IP connection.



- iFCP is a gateway-to-gateway protocol that provides Fibre Channel communication services for optical devices on TCP/IP networks to implement end-to-end IP connection. Fibre Channel storage devices, HBAs, and switches can directly connect to iFCP gateways. iFCP provides traffic control, error detection, and error recovery through TCP. It enables Fibre Channel devices to interconnect and network at the line rate over an IP network.
- The frame address conversion method defined in the iFCP protocol allows Fibre Channel storage devices to be added to the TCP/IP-based network through transparent gateways. iFCP can replace Fibre Channel to connect to and group Fibre Channel devices using iFCP devices. However, iFCP does not support the merge of independent SANs, and therefore a logical SAN cannot be formed. iFCP outstands in supporting SAN interconnection as well as gateway zoning, allowing fault isolation and breaking the limitations of point-to-point tunnels. In addition, iFCP enables end-to-end connection between Fibre Channel devices. As a result, the interruption of TCP connection affects only a communication pair. SANs that adopt iFCP support fault isolation and security management, and deliver higher reliability than SANs that adopt FCIP.

iFCP Protocol Stack

- iFCP is between Fibre Channel and TCP/IP, which means that iFCP can interwork with either Fibre Channel or TCP/IP.

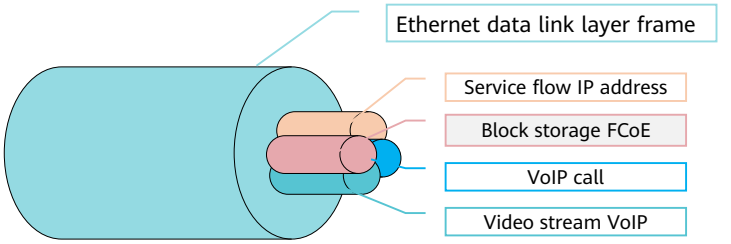


HUAWEI

- The main function of the iFCP protocol layer is to transport Fibre Channel frame images between locally and remotely attached N_Ports. When transporting frames to a remote N_Port, the iFCP layer encapsulates and routes the Fibre Channel frame comprising each Fibre Channel information unit, and transmits the frame via a predetermined TCP connection over the IP network.
- In the IP SAN that uses iFCP, iFCP devices take the place of Fibre Channel switches, which means that iFCP switches can also function as Internet Storage Name Servers (iSNSs) to provide the name discovery service for terminal nodes. The iFCP switch allocates a 4-byte IP address to each Fibre Channel terminal node. When a Fibre Channel device sends an SNS name query request, the request is intercepted by the iFCP switch and interpreted by the iSNS server.

FCoE

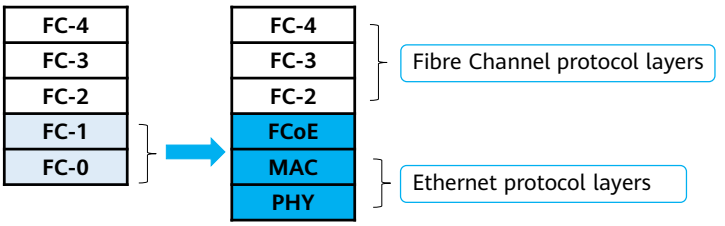
- Fibre Channel over Ethernet (FCoE) allows the transmission of LAN and FC SAN data on the same Ethernet link. This reduces the number of devices, cables, and network nodes in a data center, as well as power consumption and cooling loads, simplifying management.
- FCoE encapsulates FC data frames into Ethernet frames and allows service traffic on a LAN and SAN to be transmitted over the same Ethernet.



- FCoE offers standard Fibre Channel services, including discovery, global naming, and zoning. These services run in the same way as the original Fibre Channel services with low latency and high performance.
- From the perspective of Fibre Channel, FCoE enables Fibre Channel to be carried by the Ethernet Layer 2 link. From the perspective of the Ethernet, FCoE is an upper-layer protocol that the Ethernet carries, like IP or IPX.

FCoE Protocol Encapsulation

- FCoE encapsulates contents in the FC-2 and above layers into Ethernet packets for transmission.



HUAWEI

- The Fibre Channel protocol stack has five layers. FC-0 defines the medium type, FC-1 defines the frame coding and decoding mode, FC-2 defines the frame division protocol and flow control mechanism, FC-3 defines general services, and FC-4 defines the mapping from upper-layer protocols to Fibre Channel.

Discussion:

- What are the application scenarios of FCoE?
- What are the application scenarios of iFCP?

Quiz

1. Which of the following statements about FC SAN are true?
   A. Fibre Channel switches are required.
   B. Ethernet switches are required.
   C. Fibre Channel links cannot be used between storage devices.
   D. Data packets comply with the Fibre Channel protocol stack.
2. The performance of SATA disks is better than that of SAS disks.
   A. True
   B. False

- Answers:
  - AD
  - B

Summary

In this course, we covered:

- Mainstream data storage modes and network topologies
- RAID and Huawei RAID 2.0+ block virtualization technologies
- Differences and relationships between centralized storage and distributed storage
- Storage protocols and their application scenarios

In the next course, we will learn the network technologies.

Recommendations

- Huawei iLearning
  - https://e.huawei.com/en/talent/#/
- Huawei Support Case Library
  - https://support.huawei.com/enterprise/en/knowledge?lang=en

Acronyms and Abbreviations

- FC: Fibre Channel
- FCIP: Fibre Channel over IP
- FCoE: Fibre Channel over Ethernet
- iFCP: Internet Fibre Channel Protocol
- iSCSI: Internet Small Computer System Interface
- IPFC: IP over Fiber Channel

Acronyms and Abbreviations

- IOPS: Input/Output per second
- MTBF: Mean Time Between Failure
- NAS: Network Attached Storage
- RAID: Redundant Array of Independent Disks
- SAN: Storage Area Network
- SCSI: Small Computer System Interface

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.

Network Technology Basics

HUAWEI

Foreword

- Network technologies are the basis for the interconnection of all platforms and services. What exactly is a network? What are the basic principles of network communication? And what are the common network technologies? This course will answer these questions and more.

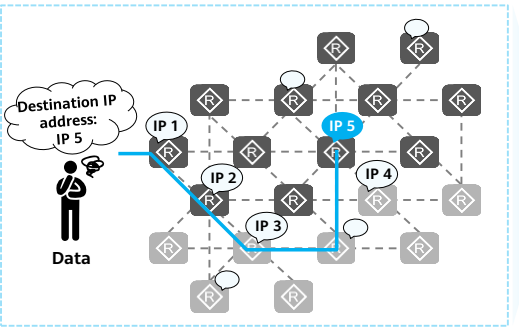
Objectives

- On completion of this course, you will be able to:
  - Understand the classification and subnetting of IP addresses.
  - Understand the basic principles of network communication.
  - Familiarize yourself with the operating principles of switches and routers.
  - Understand the technical principles and basic configuration methods of VLAN.

Contents

What Is an IP Address?

- An IP address is a unique logical address used to identify a device that sends or receives data packets on a network.
- The functions of an IP address are to:
  - Identify a host or network device (identifying its network interface and indicating its location on the network).
  - Implement network addressing



IP Address

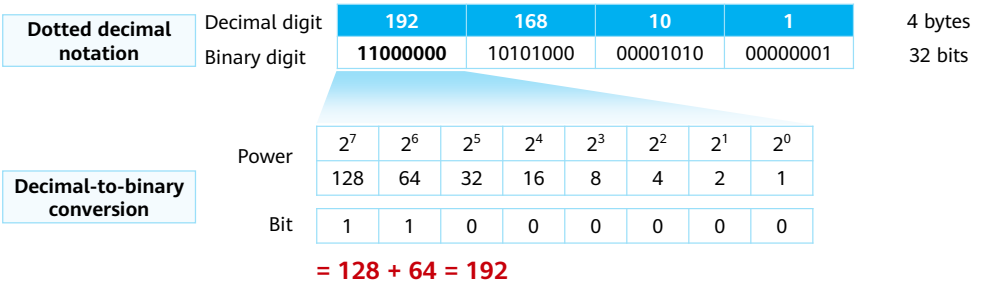
An IP address is like a real-world address. It identifies a node on a network, and is used to find the destination.

HUAWEI

- On an IP network, to connect a PC to the Internet, you need to apply an IP address for the PC. An IP address is like a real-world address. It identifies a node on a network, and is used to find the destination. Global network communication is based on IP addresses.
- An IP address is an attribute of an interface on a network device, not an attribute of the network device itself. To assign an IP address to a device is to assign an IP address to an interface of the device actually. If a device has multiple interfaces, each interface requires at least one IP address.
- Note: An interface that requires an IP address is usually the interface on a router or a computer.

IP Address Format

- An IPv4 address has 32 bits.
- An IPv4 address is usually represented in dotted decimal notation.



- IPv4 address range: 0.0.0.0–255.255.255.255

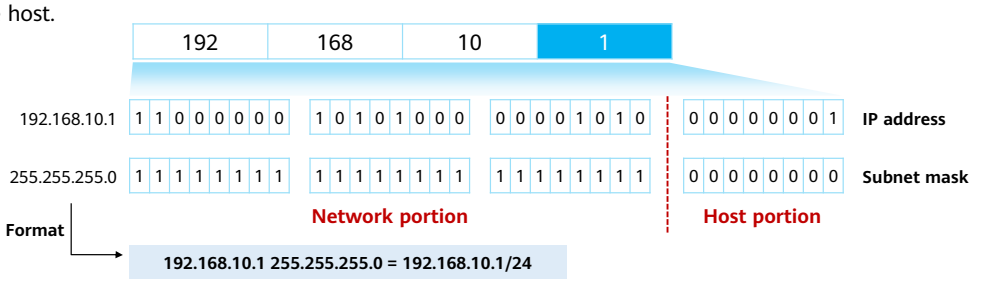
HUAWEI

- IP address format:
  - An IP address has 32 bits and consists of four bytes. For the convenience of reading and writing, an IP address is usually in the format of dotted decimal notation.
- Dotted decimal notation:
  - This type of IP address format is commonly used because it is easy to understand. However, a communication device uses binary digits to calculate the IP address. Therefore, it is necessary to master the conversion between decimal and binary digits.
- IPv4 address range:
  - 00000000.00000000.00000000.00000000–11111111.11111111.11111111.11111111 in binary, and 0.0.0.0–255.255.255.255 in decimal.

IP Address Structure

- **Network portion**: identifies a network segment.
- **Host portion**: uniquely identifies a host on a network segment.

- **Subnet mask**: specifies which portion of an address refers to the subnet and which portion refers to the host.

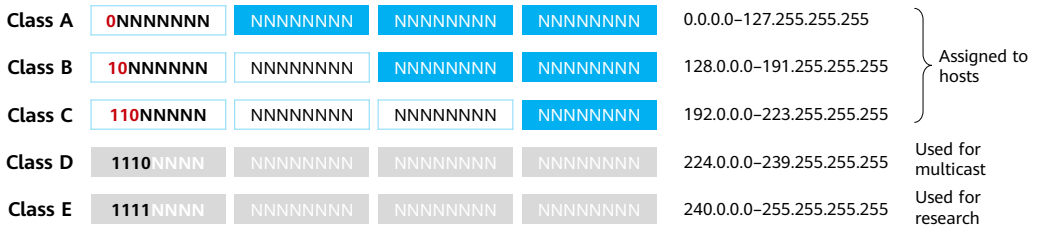


HUAWEI

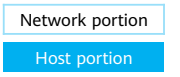
- An IPv4 address consists of two parts:
  - Network portion: identifies a network segment.
    - IP addresses do not show any geographical information. The network bits indicate the segment to which an IP address belongs.
    - Network devices with same network bits are located on the same network, regardless of their physical locations.
  - Host portion: uniquely identifies a host on a network segment.
- A subnet mask is also called a netmask:
  - Same as an IP address, a subnet mask consists of 32 bits, and is also displayed in dotted decimal notation generally.
  - A subnet mask is not an IP address. A subnet mask written in the binary format consists of consecutive 1s and 0s.
  - Generally, the number of 1s in a subnet mask is the length of the subnet mask. For example, the length of the subnet mask 0.0.0.0 is 0, and that of 252.0.0.0 is 6.
  - How to identify the network and host bits in an IP address: In a subnet mask, bits with the value of 1 correspond to the network bits in an IP address, while bits with the value of 0 correspond to the host bits. In other words, the number of 1s in a subnet mask equals to the number of network bits in an IP address, while the number of 0s equals to the number of host bits.

IP Address Classes (Classified Addressing)

- IP addresses are classified into five classes to facilitate IP address management and networking.



- Default subnet masks:
  - Class A: 8 bits, 0.0.0.0–127.255.255.255/8
  - Class B: 16 bits, 128.0.0.0–191.255.255.255/16
  - Class C: 24 bits, 192.0.0.0–223.255.255.255/24

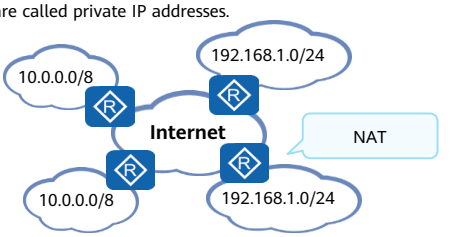


HUAWEI

- IP addresses are classified into five classes to facilitate IP address management and networking:
  - The easiest way to determine the class of an IP address is to check the first bits in its network bits. The class fields of class A, class B, class C, class D, and class E are binary numbers 0, 10, 110, 1110, and 1111, respectively.
  - Class A, B, and C addresses are unicast IP addresses (except some special addresses). Only these three types of addresses can be assigned to hosts.
  - Class D addresses are multicast IP addresses.
  - Class E addresses are used for special experimental purposes.
  - This section focuses only on class A, B, and C addresses.
- Comparison between class A, B, and C addresses:
  - Networks using class A addresses are called class A networks. Networks using class B addresses are called class B networks. Networks using class C addresses are called class C networks.
  - The number of network bits of a class A network is 8. The number of network bits is small, so the number of addresses that can be assigned to the hosts is large. The first bit in the network bits of a class A network is always 0. The address range is 0.0.0.0-127.255.255.255.
  - The number of network bits of a class B network is 16, and the first two bits are always 10. The address range is 128.0.0.0–191.255.255.255.
  - The number of network bits of a class C network is 24. The number of network bits is large, so the number of addresses that can be assigned to the hosts is small. The first three bits in the network bits of a class C network are always 110. The address range is 192.0.0.0-223.255.255.255.
- Note:
  - A host refers to a router or a computer, and the IP address of an interface on a host refers to the host IP address.
  - Multicast address: Multicast refers to one-to-many message transmission.

Public and Private IP Addresses

- **Public IP address**
  - Public IP addresses are assigned by the Internet Corporation for Assigned Names and Numbers (ICANN) to ensure that each IP address is unique on the Internet. Public IP addresses can be used for accessing the Internet.
- **Private IP address**
  - Some networks do not need to connect to the Internet, for example, a network in a closed lab of a university. However, the IP addresses of network devices in the lab network still need to be unique to avoid conflicts. Some IP addresses of classes A, B, and C are reserved for this kind of situation. These IP addresses are called private IP addresses.
    - Class A: 10.0.0.0–10.255.255.255
    - Class B: 172.16.0.0–172.31.255.255
    - Class C: 192.168.0.0–192.168.255.255



NAT is used to connect a private network to the Internet

HUAWEI

- Private IP addresses are used to resolve IP address shortage. They are used for internal networks or hosts, and cannot be used for public networks.
  - Public IP address: Network devices connected to the Internet must have public IP addresses assigned by ICANN.
  - Private IP address: increases the number of available IP addresses. A private IP address can be repeatedly used on different private networks.
- Connecting a private network to the Internet: A private network is not allowed to directly connect to the Internet because it uses a private IP address. Due to actual requirements, many private networks also want to be connected to the Internet to communicate with the Internet or other private networks through the Internet. The interconnection between a private network and the Internet is implemented through the network address translation (NAT) technology.
- Note:
  - NAT is used to translate private IP addresses into public IP addresses.
  - ICANN is a standards organization that oversees global IP address allocation.

Special IP Addresses

- There are some special IP addresses that have special meanings and functions.

Special IP Address	IP Address Range	Function
Limited broadcast address	255.255.255.255	Packets that use this address as the destination address will be sent to all hosts on the same network segment. (The destination range is limited by the gateway.)
Any address	0.0.0.0	This address is the network address of any network, or the IP address of an interface on a network.
Loopback address	127.0.0.0/8	This address is used to test the software system of a device.
Link-local address	169.254.0.0/24	When a host fails to obtain an IP address automatically, the host can use a link-local address for temporary communication.

- 255.255.255.255
  - This address is called a limited broadcast address and can be used as the destination IP address of an IP packet.
  - After receiving an IP packet whose destination IP address is a limited broadcast address, a router stops forwarding the IP packet.
- 0.0.0.0
  - If this address is used as a network address, it refers to the network address of any network. If this address is used as a host address, it refers to an interface IP address of a host on the network.
  - For example, when a host does not obtain an IP address during startup, it can send a DHCP Request packet with the source IP address being 0.0.0.0 and the destination IP address being a limited broadcast address to the network. The DHCP server will assign an available IP address to the host after receiving the DHCP Request packet.
- 127.0.0.0/8
  - This address is a loopback address that can be used as the destination IP address of an IP packet. It is used to test the software system of the device.
  - An IP packets whose destination IP address is a loopback address cannot leave the device which sends the packet.
- 169.254.0.0/16
  - If a network device is configured to automatically obtain an IP address but does not find an available DHCP server on the network, the device uses an IP address on the 169.254.0.0/16 network segment for temporary communication.
- Note: DHCP is used to dynamically allocate network configuration parameters, such as IP addresses.

Subnet Mask and Available Host Address

- Generally, the network range defined by a network ID is called a network segment.
- **Subnet mask**: Used to calculate the network ID (network address) and host ID (host address) in an IP address.

  Example: 192.168.10.0/24

192	168	10	00000000

- **Broadcast address**: Used as a special destination address to send data to all hosts on the network.

  Example: 192.168.10.255/24

192	168	10	11111111

- **Available address**: Assigned to a node or an interface of a device on a network.

  Example: 192.168.10.1/24

192	168	10	00000001

Note

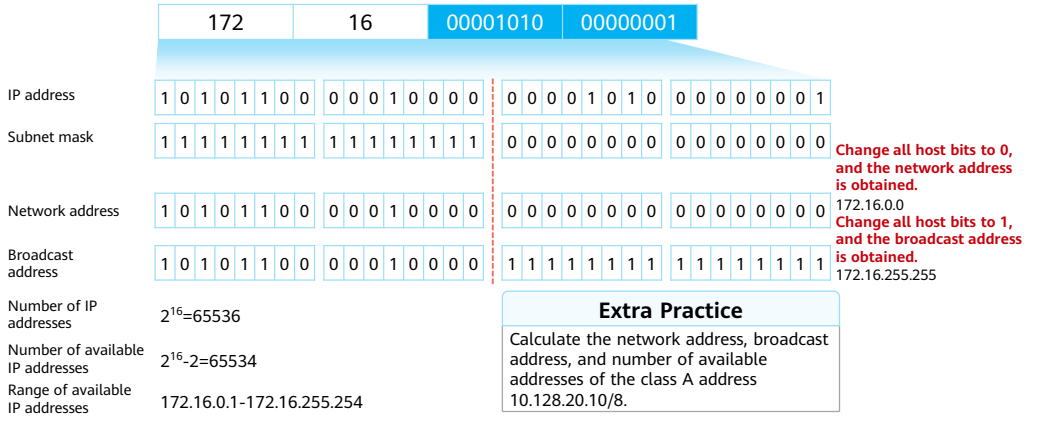
- Network addresses and broadcast addresses cannot be used as the address of nodes or network devices.
- The number of available IP addresses on a network segment is $2^n - 2$ (n is the number of host bits).

HUAWEI

- Broadcast address
  - Each bit of the host ID is 1.
  - It cannot be allocated to a specific interface on a host.
- Available address
  - It is also called a host address and can be allocated to a specific interface on a host.
- Calculation of the number of available IP addresses on a network segment
  - If the number of host bits of a network segment is n, the number of IP addresses on the network segment is 2^n, and the number of available host addresses is $2^n - 2$ (subtracting the network address and broadcast address).

IP Address Calculation

- Calculate the network address, broadcast address, and number of available addresses of the class B address 172.16.10.1/16.



HUAWEI

- Network address: Change all host bits of an IP address to 0, and the result is the network address of the network to which the IP address belongs.
- Broadcast address: Change all host bits of an IP address to 1, and the result is the broadcast address of the network to which the IP address belongs.
- Number of IP addresses: 2^n, where n indicates the number of host bits.
- Number of available IP addresses: $2^n - 2$, where n indicates the number of host bits.
- Answer to the practice:
  - Network address: 10.0.0.0
  - Broadcast address: 10.255.255.255
  - Number of IP addresses: 224
  - Number of available IP addresses: 222 (224 - 2)
  - Range of available IP addresses: 10.0.0.1-10.255.255.254

Subnetting

- Why do we need subnetting?
- The variable length subnet mask (VLSM) technology is used in subnetting.
  - VLSM allows an organization to divide a network into multiple subnets based on the network scale for different departments to use.
- For example, a company is assigned a class C IP address 201.222.5.0. Assume that 20 subnets are required and each subnet contains five hosts. How should we divide the subnets?

Subnet Address	Available Host Addresses
201.222.5.8/29	201.222.5.9-201.222.5.14
201.222.5.16/29	201.222.5.17-201.222.5.22
...	...
201.222.5.232/29	201.222.5.233-201.222.5.238
201.222.5.240/29	201.222.5.241-201.222.5.246

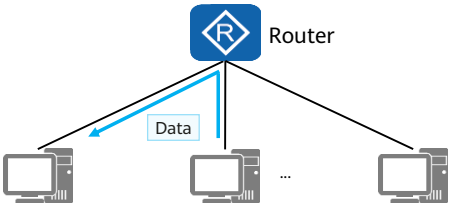
- Why do we need subnetting?
- In practice, if a class A network is assigned to an organization but the number of hosts in the organization is less than 16777214, a large number of IP addresses will be idle and wasted. Therefore, a more flexible method is required to divide the network based on the network scale. The idea is to divide a network into multiple subnets for different organizations to use through VLSM. VLSM can be used on both public networks and enterprise networks.
- In the preceding example, 201.222.5.0 is a class C address, whose default subnet mask is 24. Assume that 20 subnets are required and each subnet contains five hosts. The last byte (8 bits) of 201.222.5.0 should be divided into subnet bits and host bits.
- The number of subnet bits determines the number of subnets. As this address is a class C address, the total number for subnet bits and host bits is 8. Because the value 20 is in the range of 2^4 (16) to 2^5 (32), 5 bits should be reserved for subnet bits. The 5-bit subnet part allows a maximum of 32 subnets. The 3 bits left are host bits, which means that there are a maximum of 2^3 (8) IP addresses. Except for one network address and one broadcast address, six addresses can be used by hosts.
- The network segments are:
  - 201.222.5.0-201.222.5.7
  - 201.222.5.8-201.222.5.15
  - 201.222.5.16-201.222.5.23
  - ...
  - 201.222.5.232-201.222.5.239
  - 201.222.5.240-201.222.5.247
  - 201.222.5.248-201.222.5.255

Contents

Concept of Network Communication

- Communication refers to the information transfer and exchange between people, between people and things, and between things through a certain medium and action.
- Network communication refers to communication between terminal devices through a computer network.
- Examples of network communication:

A. Files are transferred between two computers (terminals) through a network cable.



B. Files are transferred among multiple computers (terminals) through a router.

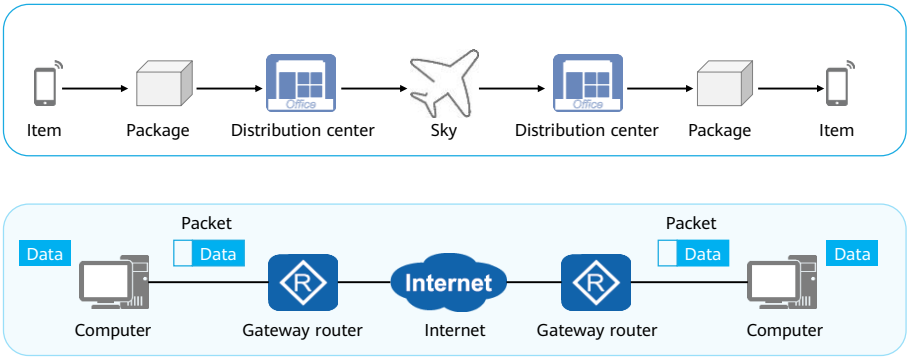
C. A computer (terminal) downloads files through the Internet.

HUAWEI

- Examples of network communication:
  - A: Two computers are connected through a network cable to form a simple network.
  - B: A router (or switch) and multiple computers form a small-scale network. In such a network, files can be freely transferred between every two computers through a router.
  - C. If a computer wants to download files from a website, it must access the Internet first.
- The Internet is the largest computer network in the world. Its predecessor, Advanced Research Projects Agency Network (ARPANET), was born in 1969. The wide popularization and application of Internet is one of the signs of entering the information age.

Information Transfer Process

- Virtual information transfer is similar to real object transfer.

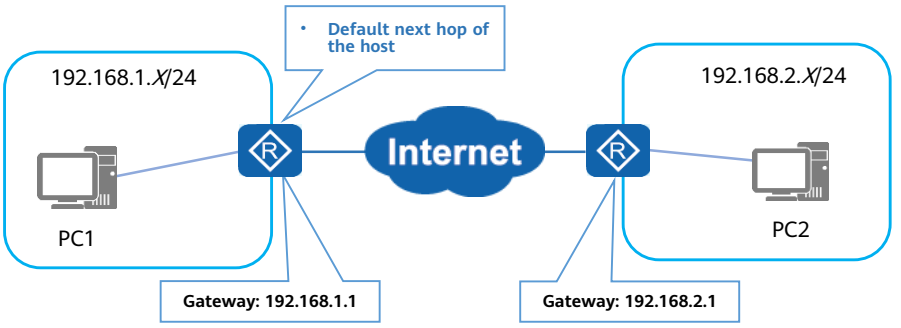


HUAWEI

- Comparison between the express delivery process and network communication process:
- Items to be delivered:
  - The information (or data) generated by the application
- The item is packed into a package and pasted with a package label containing the receiver's name and address.
  - The application packs the data into an original data payload and adds a header and a tail to form a packet. The important information in the packet is the address of the receiver, that is, the destination address.
  - Encapsulation is a process in which new information segments are added to an information unit, forming a new information unit.
- The package is delivered to a distribution center in which packages are sorted based on the destination addresses. The packages destined for the same city are placed in the same plane for airlift.
  - The packet reaches the gateway through a network cable. After receiving the packet, the gateway decapsulates the packet, obtains the destination address, re-encapsulates the packet, and sends the packet to different routers based on the destination address. The packet is transmitted through the gateway and router, leaves the local network, and is transmitted through the Internet.
  - The network cable is the medium for information transmission, and plays the same role as the highway for item transmission.

- After the plane arrives at the destination airport, the packages are taken out for sorting, and the packages destined for the same area are sent to the same distribution center.
    - The packet is transmitted through the Internet and reaches the local network where the destination address resides. The gateway or router of the local network decapsulates and encapsulates the packet, and then determines the next-hop router according to the destination address. Finally, the packet reaches the gateway of the network where the destination computer resides.
- The distribution center sorts the packages according to the destination addresses on the packages. The courier delivers the packages to the receiver. The receiver unpacks the package, confirms that the items are intact, and signs for the package. The entire express delivery process is complete.
    - After the packet reaches the gateway of the network where the destination computer resides, the gateway decapsulates and encapsulates the packet, and then sends the packet to the corresponding computer according to the destination address. After receiving the packet, the computer verifies the packet. If the packet passes verification, the computer accepts the packet and sends the data payload to the corresponding application program for processing. A complete network communication process is complete.

What Is a Gateway?



HUAWEI

- A gateway is also called an inter-network connector or a protocol converter. By default, a gateway implements network interconnection above the network layer.
- Just like you must walk through a door when entering a room, information sent from one network or network segment to another must pass through a gateway. We can say the gateway is the door to another network.
- Functions of a gateway — A gateway plays significant roles in not only its role but also its configuration:
  - When a host (such as a PC, server, router, or firewall) wants to access another network segment, the gateway is responsible for sending ARP packets, and receiving and forwarding subsequent data packets.
  - After the gateway is configured, the default route is generated on the host, with the next hop being the gateway.

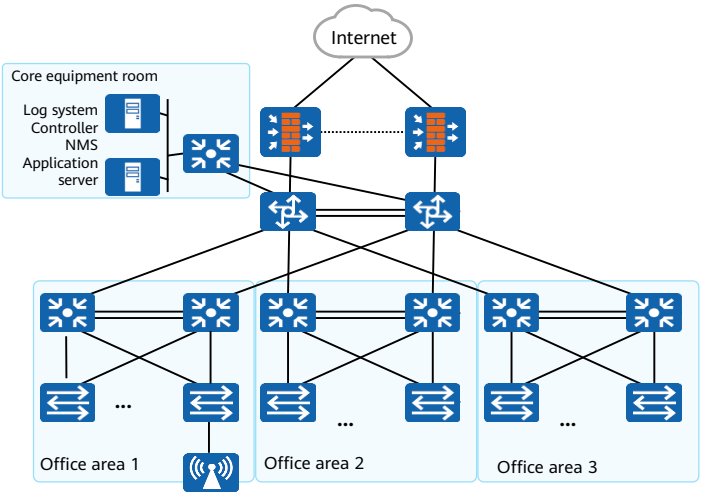
Basic Architecture of a Communication Network

- Communication network

  A communication network consists of routers, switches, firewalls, PCs, network printers, servers, and more.

- Function

  The basic function of a communication network is to implement data communication.

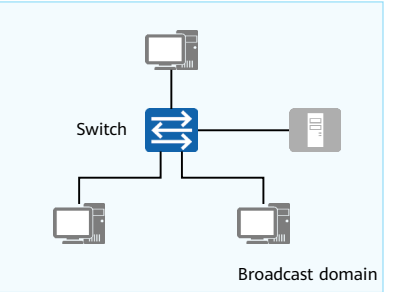


HUAWEI

- Take the enterprise data center network (DCN) as an example. The major requirements of an enterprise for the DCN include service operation and computing, data storage, and service access.
- The DCN thereby needs to enable device-device and device-user interconnection and provide external access capabilities for services. Devices on such a network collaborate with each other to implement communication:
  - Access switches connect to user hosts in office areas.
  - Aggregation switches aggregate traffic from access switches.
  - Routers forward traffic between different office areas and between internal and external networks.
  - Firewalls implement access control for areas of different security levels and between internal and external networks to ensure secure access.

Network Device - Switch

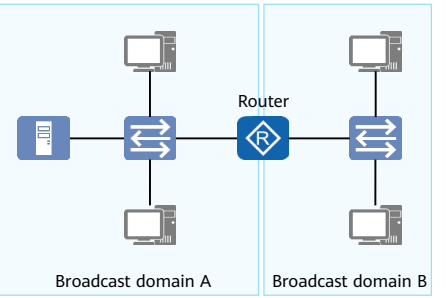
- As the device closest to end users, a switch connects end users to a network and forwards data frames. A switch can:
  - Connect terminals (such as PCs and servers) to the network.
  - Isolate collision domains.
  - Broadcast unknown packets.
  - Learn MAC addresses and maintain the MAC address table.
  - Forward packets based on the MAC address table.



- Switch:
  - Generally, on a campus network, switches are closest to end users, and Layer 2 switches (also known as Ethernet switches) are deployed at the access layer. Layer 2 refers to the data link layer of the TCP/IP model.
  - An Ethernet switch can implement the following functions: data frame switching, access of end users, basic access security, and Layer 2 link redundancy.
  - Broadcast domain: a group of nodes, among which a broadcast packet from one node can reach all the other nodes.
  - Collision domain: an area where a collision occurs when two devices on the same network send packets at the same time.
  - Media Access Control (MAC) address: uniquely identifies a network interface card (NIC) on a network. Each NIC requires and has a unique MAC address.
  - MAC address table: exists on each switch and stores the mappings between MAC addresses and switch interfaces.

Network Device - Router

- Working at the network layer, a router forwards data packets on the Internet. Based on the destination address in a received packet, a router selects a path to send the packet to the next router or destination. The last router on the path is responsible for sending the packet to the destination host. A router can:
  - Implement communication between networks of the same type or different types.
  - Isolate broadcast domains.
  - Maintain the routing table and run routing protocols.
  - Select routes and forward IP packets.
  - Implement WAN access and network address translation (NAT).
  - Connect Layer 2 networks built through switches.



HUAWEI

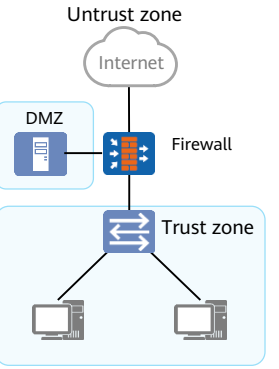
- Router:
  - A router works at the network layer of the TCP/IP model.
  - A router can maintain the routing table and routing entries, discover routes, select paths, forward data, isolate broadcast domains, implement WAN access, translate network addresses, and provide specific security functions.

Discussion

- What are the differences between a Layer 2 switch and a router that are both used for network connection?
- What are their application scenarios?

Network Device - Firewall

- As a network security device, a firewall is used to ensure secure communication between two networks. It monitors, restricts, and modifies data flows passing through it to shield the information, structure, and running status of internal networks from the public network. A firewall can:
  - Isolate networks of different security levels.
  - Implement access control (using security policies) between networks of different security levels.
  - Perform user identity authentication.
  - Implement remote access.
  - Encrypt data and provide virtual private network (VPN) services.
  - Implement NAT.
  - Provide other security functions.



- Firewall:
  - Located between two networks of different trust levels (for example, an enterprise intranet and the Internet), a firewall controls the communication between the two networks and forcibly implements unified security policies to prevent unauthorized access to key information resources, ensuring system security.

Contents

OSI Reference Model

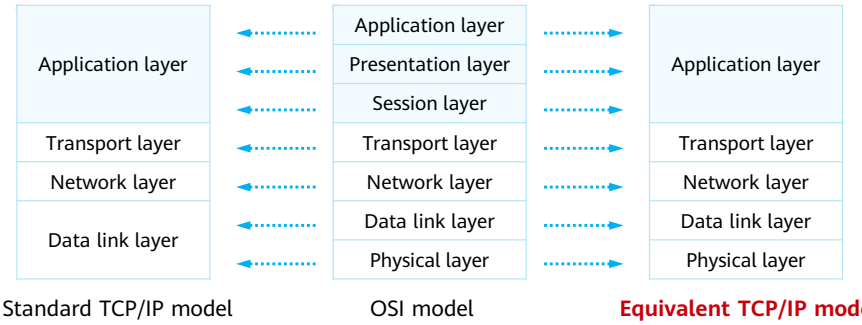
- To achieve compatibility between networks and help vendors produce compatible network devices, the International Organization for Standardization (ISO) launched the Open Systems Interconnection (OSI) reference model in 1984. It was quickly adopted as the basic model for computer network communication.

7. Application layer	Provides interfaces for applications.
6. Presentation layer	Converts data formats to ensure the application layer of one system can identify and understand the data generated by the application layer of another system.
5. Session layer	Establishes, manages, and terminates sessions between two parties.
4. Transport layer	Establishes, maintains, and cancels one-time end-to-end data transmission processes, controls transmission speeds, and adjusts data sequencing.
3. Network layer	Defines logical addresses and transfers data from sources to destinations.
2. Data link layer	Encapsulates packets into frames, transmits frames in P2P or P2MP mode, and implements error checking.
1. Physical layer	Transmits bit streams over transmission media and defines electrical and physical specifications.

- The Open Systems Interconnection (OSI) model was included in the ISO 7489 standard and released in 1984. ISO stands for International Organization for Standardization.
- The OSI reference model is also called the seven-layer model. The seven layers from bottom to top are as follows:
  - Physical layer: transmits bit streams between devices and defines physical specifications such as electrical levels, speeds, and cable pins.
  - Data link layer: encapsulates bits into octets and octets into frames, uses link layer addresses (MAC addresses in Ethernet) to access media, and implements error checking.
  - Network layer: defines logical addresses for routers to determine paths and transmits data from source networks to destination networks.
  - Transport layer: implements connection-oriented and non-connection-oriented data transmission, as well as error checking before retransmission.
  - Session layer: establishes, manages, and terminates sessions between entities at the presentation layer. Communication at this layer is implemented through service requests and responses transmitted between applications on different devices.
  - Presentation layer: provides data encoding and conversion functions so that data sent by the application layer of one system can be identified by the application layer of another system.
  - Application layer: provides network services for applications and is closest to users.

TCP/IP Reference Model

- The TCP/IP reference model has become the mainstream reference model of the Internet because the TCP and IP protocols are widely used and the OSI model is too complex.

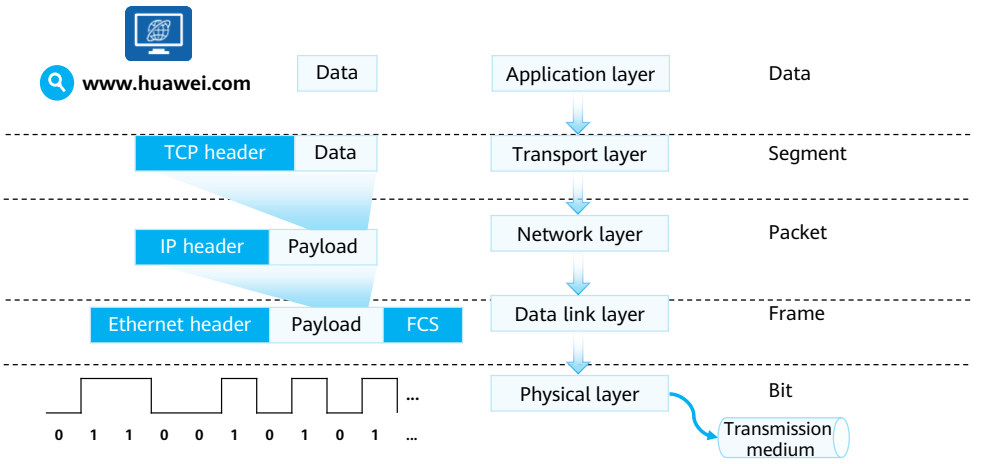


HUAWEI

- Similar to the OSI model, the Transmission Control Protocol/Internet Protocol (TCP/IP) model adopts a hierarchical architecture, and adjacent layers are closely related.
- The standard TCP/IP model combines the data link layer and physical layer in the OSI model into the network access layer. This division mode is contrary to the actual protocol formulation. Therefore, the equivalent TCP/IP model that integrates the standard TCP/IP model and the OSI model is proposed. Contents in the following slides are based on the equivalent TCP/IP model.
- TCP/IP was originated from a packet switched network research project funded by the US government in the late 1960s. Since the 1990s, the TCP/IP model has become the most commonly used networking model for computer networks. It is a truly open system, because the definition of the protocol suite and its multiple implementations can be easily obtained at little or even no cost. It thereby became the basis of the Internet.
- Like the OSI reference model, the TCP/IP model is developed in different layers, each of which is responsible for different communication functions. The difference is, the TCP/IP model has a simplified hierarchical structure that consists of only five layers: application layer, transport layer, network layer, data link layer, and physical layer. As shown in the figure, the TCP/IP protocol stack corresponds to the OSI reference model and covers all layers in the OSI reference model. The application layer contains all upper-layer protocols in the OSI reference model.
- The TCP/IP protocol stack supports all standard physical-layer and data-link-layer protocols. The protocols and standards at the two layers will be further discussed in following chapters.

- Comparison between the OSI reference model and TCP/IP protocol stack:
  - Similarities
    - They are both hierarchical and both require close collaboration between layers.
    - They both have the application layer, transport layer, network layer, data link layer, and physical layer. (Note: The TCP/IP protocol stack is divided into five layers here to facilitate comparison. In many documents, the data link layer and physical layer of TCP/IP are combined into the data link layer, which is also called network access layer.)
    - They both use the packet switching technology.
    - Network engineers must understand both models.
  - Differences
    - TCP/IP includes the presentation layer and session layer into the application layer.
    - TCP/IP has a simpler structure with fewer layers.
    - TCP/IP standards are established based on practices during the Internet development and are thereby highly trusted. In comparison, the OSI reference model is based on theory and serves as a guide.

Data Encapsulation on the Sender

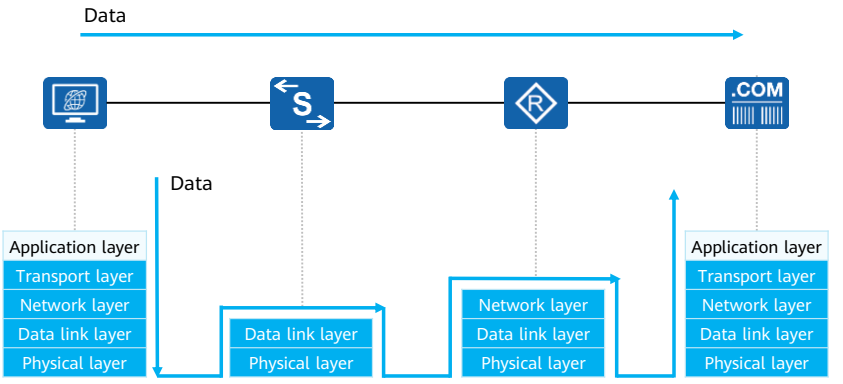


HUAWEI

- Assume that you are using a web browser to access Huawei's official website. After you enter the website address and press **Enter**, the following events occur on your computer:
  - Internet Explorer (application) invokes HTTP (application-layer protocol) to encapsulate the application-layer data. (**Data** in the figure should also include the HTTP header, which is not shown here.)
  - HTTP uses TCP to ensure reliable data transmission and thereby transmits the encapsulated data to the TCP module.
  - The TCP module adds the corresponding TCP header information (such as the source and destination port numbers) to the data transmitted from the application layer. The protocol data unit (PDU) is called a segment.
  - On an IPv4 network, the TCP module sends the encapsulated segment to the IPv4 module at the network layer. (On an IPv6 network, the segment is sent to the IPv6 module for processing.)
  - After receiving the segment from the TCP module, the IPv4 module encapsulates the IPv4 header. Here, the PDU is called a packet.
  - Ethernet is used as the data link layer protocol. Therefore, after the IPv4 module completes encapsulation, it sends the packet to the Ethernet module (such as the Ethernet adapter) at the data link layer for processing.
  - After receiving the packet from the IPv4 module, the Ethernet module adds the corresponding Ethernet header and FCS frame trailer to the packet. Now, the PDU is called a frame.
  - After the Ethernet module completes encapsulation, it sends the data to the physical layer.
  - Based on the physical media, the physical layer converts digital signals into electrical signals, optical signals, or electromagnetic (wireless) signals.
  - The converted signals are then transmitted on the network.

Data Transmission on the Intermediate Network

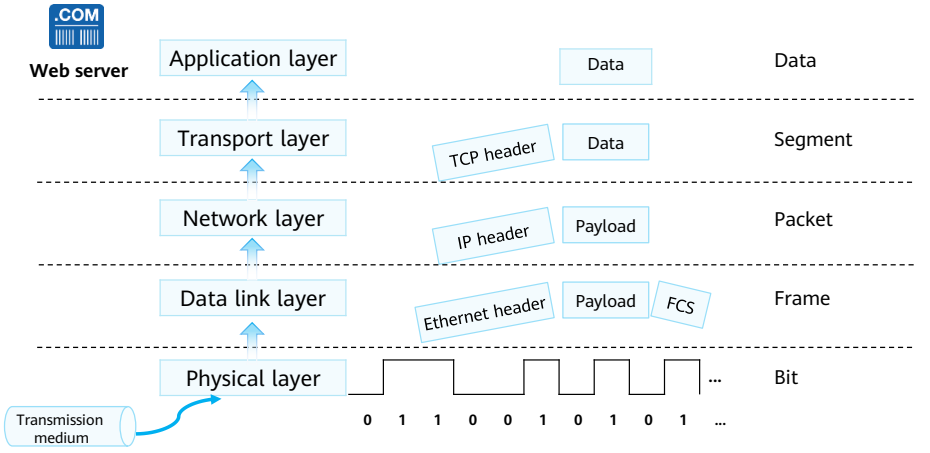
- Encapsulated data is transmitted on the network.



HUAWEI

- In most cases:
  - A Layer 2 device (such as an Ethernet switch) only decapsulates the Layer 2 header of the data and performs the corresponding switching operation based on the Layer 2 header information.
  - A Layer 3 device (such as a router) only decapsulates the Layer 3 header and performs the corresponding routing operation based on the Layer 3 header information.
  - Note: The details and principles of switching and routing will be described in the following chapters.

Data Decapsulation on the Receiver



HUAWEI

- After being transmitted over the intermediate network, the data finally reaches the destination server. Based on the information in different protocol headers, the data is decapsulated layer by layer, processed, transmitted, and finally sent to the application on the web server for processing.

Contents

Common TCP/IP Protocols

- The TCP/IP protocol stack defines a set of standard protocols.

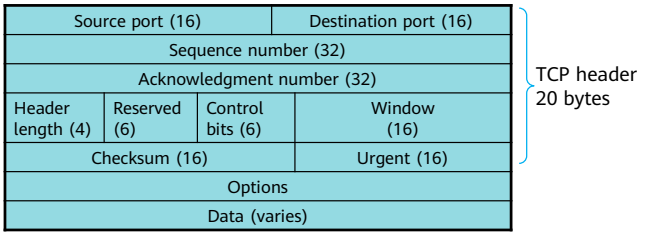
<table>
<tr><td rowspan="2">Application layer</td><td>Telnet</td><td>FTP</td><td>TFTP</td><td>SNMP</td></tr>
<tr><td>HTTP</td><td>SMTP</td><td>DNS</td><td>DHCP</td></tr>
<tr><td>Transport layer</td><td colspan="2">TCP</td><td colspan="2">UDP</td></tr>
<tr><td rowspan="2">Network layer</td><td colspan="2">ICMP</td><td colspan="2">IGMP</td></tr>
<tr><td colspan="4">IP</td></tr>
<tr><td rowspan="2">Data link layer</td><td colspan="4">PPPoE</td></tr>
<tr><td colspan="2">Ethernet</td><td colspan="2">PPP</td></tr>
<tr><td>Physical layer</td><td colspan="4">...</td></tr>
</table>

- Overview of protocols:
  - Hypertext Transfer Protocol (HTTP): used to access various pages on web servers.
  - File Transfer Protocol (FTP): used to transfer data from one host to another.
  - Domain Name Service (DNS): translates domain names of hosts into IP addresses.
  - Transmission Control Protocol (TCP): provides reliable and connection-oriented communication services for applications. Currently, TCP is used by many popular applications.
  - User Datagram Protocol (UDP): provides connectionless communication services, without guaranteeing the reliability of packet transmission.
  - Internet Protocol (IP): encapsulates transport-layer data into data packets and forwards packets from source sites to destination sites. IP provides a connectionless and unreliable service.

- Internet Group Management Protocol (IGMP): manages multicast group memberships. Specifically, IGMP sets up and maintains memberships between IP hosts and their directly connected multicast routers.
- Internet Control Message Protocol (ICMP): sends control messages based on the IP protocol and provides information about various problems that may exist in the communication environment. Such information helps administrators diagnose problems and take proper measures to resolve the problems.
- Address Resolution Protocol (ARP): a TCP/IP protocol that discovers the data link layer address associated with a given IP address. It maps IP addresses to MAC addresses, maintains the ARP table that caches the mappings between IP addresses and MAC addresses, and detects IP address conflicts on a network segment.

TCP

- TCP provides connection-oriented and reliable services for applications.
- Reliability of TCP
  - Connection-oriented transmission
  - Maximum segment size (MSS)
  - Transmission acknowledgment mechanism
  - Checksum of the header and data
  - Flow control



HUAWEI

- TCP provides reliable and connection-oriented services for applications.
- TCP provides reliability in the following aspects:
  - Connection-oriented transmission: A connection must be established before either side sends data.
  - MSS: limits the maximum length of a TCP packet sent to the receiver. When a connection is established, both parties of the connection advertise their MSSs to make full use of bandwidth resources.
  - Transmission acknowledgment mechanism: After the sender sends a data segment, it starts a timer and waits for an acknowledgment from the receiver. If no acknowledgment is received when the timer expires, the sender resends the data segment.
  - Checksum of the header and data: TCP maintains the checksum of the header and data, implementing end-to-end check to verify whether the data changes during transmission. If the checksum of a received segment is incorrect, TCP discards the segment and does not acknowledge the receipt of the segment. In this case, TCP starts the retransmission mechanism.
  - Flow control: Each party of a TCP connection has a buffer with a fixed size. The receiver allows the sender to send only the data that can be stored in the receive buffer, which prevents buffer overflow caused by the high transmission rate of the sender.

UDP

- UDP provides connectionless services for applications. Before data transmission, no connection is established between the source and destination ends.
- UDP does not maintain connection states or sending and receiving states. Therefore, a server can transmit the same message to multiple clients at the same time.
- UDP applies to applications that require high transmission efficiency.

- UDP provides connectionless services for applications. That is, no connection needs to be established between the source and destination ends before data transmission. UDP does not maintain connection states or sending and receiving states. Therefore, a server can transmit the same message to multiple clients at the same time.
- UDP applies to applications that require high transmission efficiency or have the reliability guaranteed at the application layer. For example, the Remote Authentication Dial-In User Service (RADIUS) protocol used for authentication and accounting and Routing Information Protocol (RIP) are based on UDP.

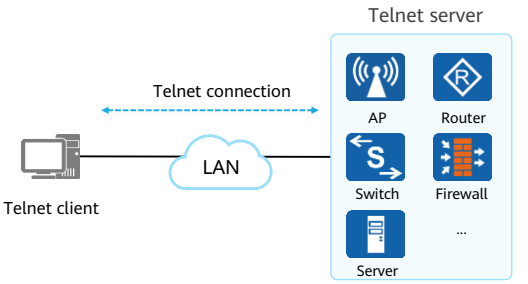
TCP vs. UDP

TCP	UDP
• Connection-oriented • Reliable transmission with flow and congestion control • Header length: 20–60 bytes • Applies to applications that require reliable transmission, such as file transfer	• Connectionless • Unreliable transmission, with packet reliability guaranteed by upper-layer applications • Short header length of 8 bytes • Applies to real-time applications, such as video conferencing

- TCP is reliable, but its reliability mechanism leads to low packet transmission efficiency and high encapsulation overhead.
- UDP is connectionless and unreliable, but its transmission efficiency is higher.

Telnet

- Telnet provides remote login services on data networks. It allows users to remotely log in to a device from a local PC. Telnet data is transmitted in plaintext.
- A user connects to a Telnet server through a Telnet client program. The commands entered on the Telnet client are executed on the server, as if the commands were entered on the console of the server.



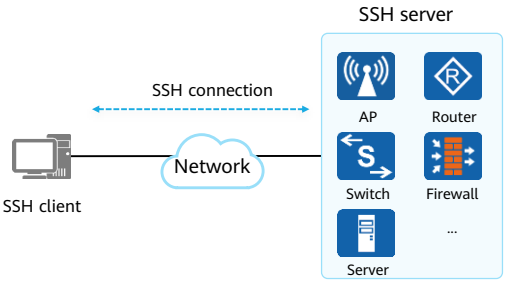
HUAWEI

- Telnet enables network administrators to remotely log in to network devices for configuration and management.
- However, Telnet has the following disadvantages:
  - Data is transmitted in plaintext, which does not ensure confidentiality.
  - The authentication mechanism is weak. Users' authentication information is transmitted in plaintext and may be eavesdropped. Telnet supports only the traditional password authentication mode and is vulnerable to attacks.
  - A client cannot truly identify the server. As a result, attackers can use a bogus server to launch attacks.

    SSH was designed to resolve the preceding issues.

SSH

- SSH is a network security protocol that employs encryption and authentication mechanisms to implement services such as secure remote access and file transfer.
- SSH was developed to resolve security issues that Telnet may bring, ensuring secure remote access to network devices.
- SSH uses the client/server architecture and involves three layers: transport layer, authentication layer, and connection layer.



- SSH protocol layers:
  - Transport layer: establishes a secure encryption channel between a client and a server to provide sufficient confidentiality protection for phases that require high data transmission security, such as user authentication and data exchange.
  - Authentication layer: runs over transport-layer protocols and helps a server authenticate login users.
  - Connection layer: divides an encryption channel into several logical channels to run different applications. It runs over authentication-layer protocols and provides services such as session interaction and remote command execution.
- SSH packet exchange consists of the following phases:
  - Connection setup
  - Version negotiation
  - Algorithm negotiation
  - Key exchange
  - User authentication
  - Service request
  - Data transmission and connection shutdown

Telnet vs. SSH

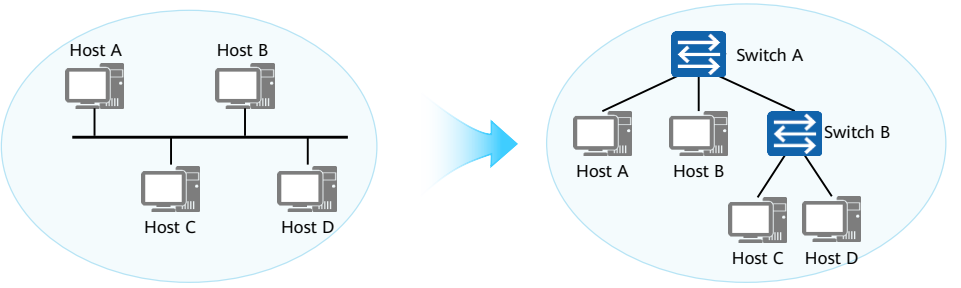
Telnet	SSH
• Data is transmitted in plaintext. • Weak authentication mechanism: User authentication information is transmitted in plaintext. • Only traditional password authentication is available. • A client cannot truly identify a server.	• Data is transmitted in ciphertext. • User authentication information is transmitted in ciphertext. • In addition to password authentication, SSH servers support multiple user authentication modes, such as public key authentication that has higher security. • Encryption and decryption keys are dynamically generated for communication between the client and server. • Provides the server authentication function for clients.

- SSH encrypts data before sending it, ensuring data transmission security. It applies to scenarios where encrypted authentication is required.
- Telnet is still used in tests or scenarios where encryption is not required (such as on a LAN).

Contents

Ethernet Protocol

- Ethernet is the most common communication protocol standard used by existing local area networks (LANs). It defines the cable types and signal processing methods that are used on a LAN.



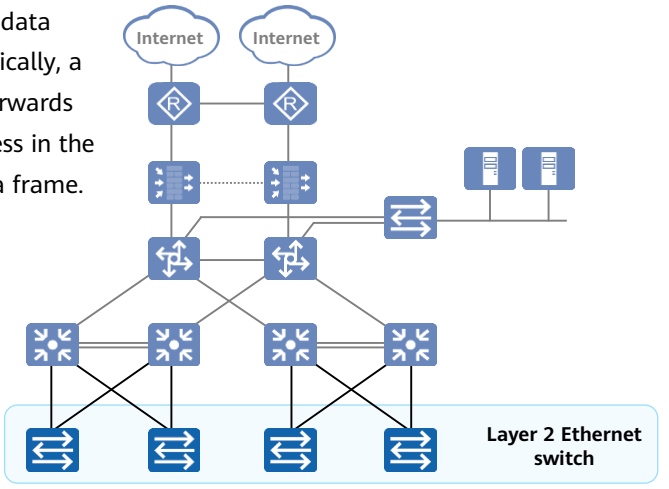
Early Ethernet **Switch networking**

HUAWEI

- Early Ethernet:
  - Ethernet networks are broadcast networks established based on the Carrier Sense Multiple Access with Collision Detection (CSMA/CD) mechanism. Collisions restrict Ethernet performance. Early Ethernet devices such as hubs work at the physical layer, and cannot confine collisions to a particular scope. This restricts network performance improvement.
- Switch networking:
  - Working at the data link layer, switches are able to confine collisions to a particular scope, thereby helping improve Ethernet performance. Switches have replaced hubs as mainstream Ethernet devices. However, switches do not restrict broadcast traffic on the Ethernet. This affects Ethernet performance.

Layer 2 Ethernet Switch

- Layer 2 Ethernet switches forward data through Ethernet interfaces. Specifically, a switch performs addressing and forwards data only based on the MAC address in the Layer 2 header of an Ethernet data frame.

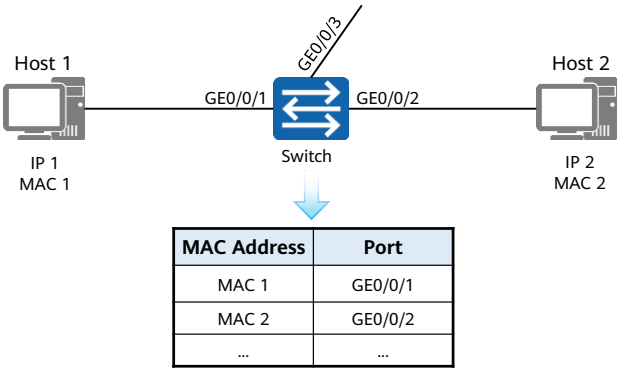


HUAWEI

- We have discussed the architecture and composition of a communication network. Layer 2 Ethernet switches are located at the edge of a communication network and function as access devices for user and terminal access.
- Layer 2 Ethernet switch:
  - On a campus network, a switch is the device closest to end users and is used to connect terminals to the campus network. Switches at the access layer are typically Layer 2 switches.
  - A Layer 2 switch works at the second layer (data link layer) of the TCP/IP model and forwards data packets based on MAC addresses.
- Layer 3 Ethernet switch:
  - Routers are required to implement network communication between different LANs. As data communication networks expand and more services emerge on the networks, increasing traffic needs to be transmitted between networks. Routers cannot adapt to this development trend because of their high costs, low forwarding performance, and small interface quantities. New devices capable of high-speed Layer 3 forwarding are required. Layer 3 switches are such devices.
- Note: The switches involved in this course refer to Layer 2 Ethernet switches.

MAC Address Table

- Each switch has a MAC address table that stores the mappings between MAC addresses and switch interfaces.

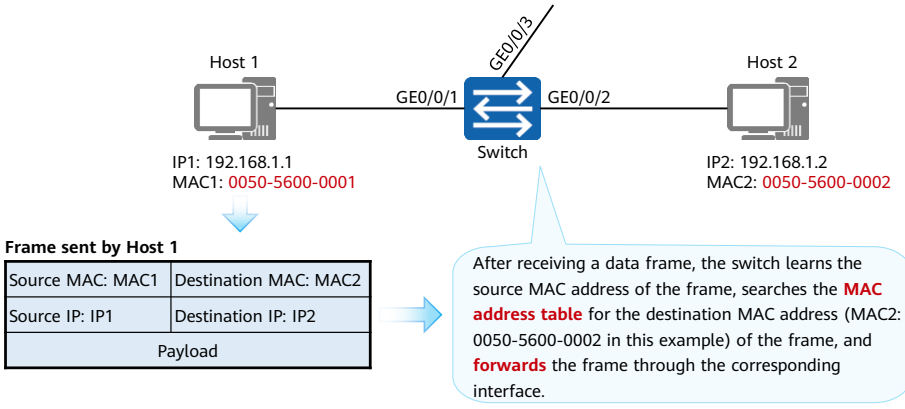


MAC Address	Port
MAC 1	GE0/0/1
MAC 2	GE0/0/2
...	...

HUAWEI

- A MAC address table records the mappings between MAC addresses learned by a switch and switch interfaces. When forwarding a data frame, the switch looks up the MAC address table based on the destination MAC address of the frame. If the MAC address table contains an entry mapping the destination MAC address of the frame, the frame is directly forwarded through the outbound interface in the entry. If there is no match of the destination MAC address of the frame in the MAC address table, the switch floods the frame to all interfaces except the interface that receives the frame.

Working Principles of Switches

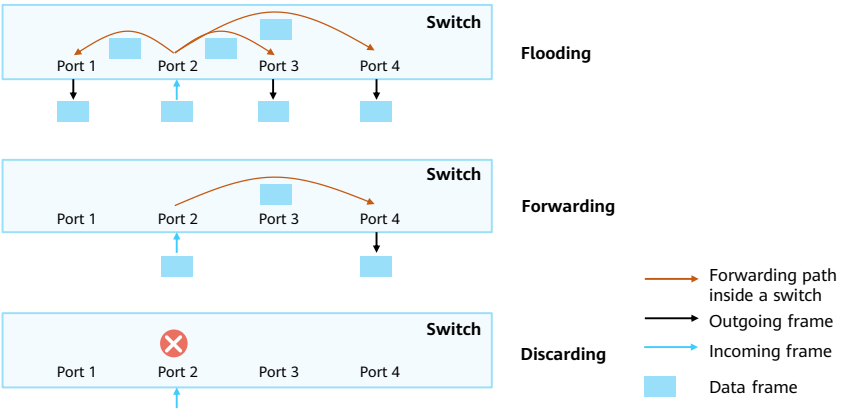


HUAWEI

- Layer 2 switches work at the data link layer and forward frames based on MAC addresses. Different interfaces on a switch send and receive data independently, and each interface belongs to a different collision domain. This effectively isolates collision domains on the network.
- Layer 2 switches maintain the mappings between MAC addresses and interfaces by learning the source MAC addresses of Ethernet frames in a table called a MAC address table. Layer 2 switches look up the MAC address table to determine the interface to which a frame is forwarded based on the destination MAC address of the frame.

Three Frame Processing Behaviors of a Switch

- A switch processes the frames entering an interface over a transmission medium in three ways:



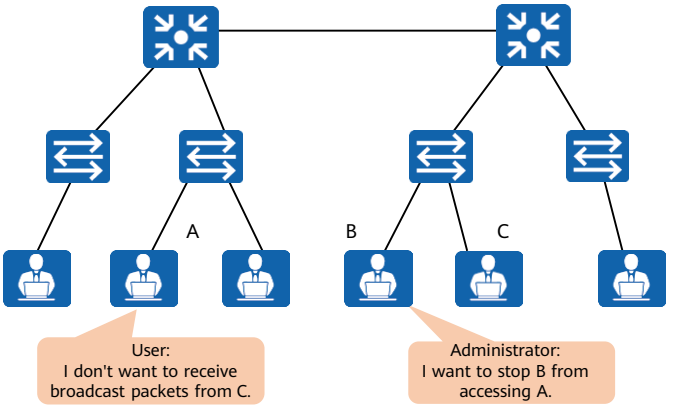
HUAWEI

- A switch forwards each frame that enters an interface over a transmission medium, which is also the basic function of a switch.
- A switch processes frames in three ways: flooding, forwarding, and discarding.
  - Flooding: The switch forwards the frames received from an interface to all other interfaces.
  - Forwarding: The switch forwards the frames received from an interface to another interface.
  - Discarding: The switch discards the frames received from an interface.

Contents

Why Do We Need VLANs?

- Broadcast packets have a wide-ranging impact on a network. However, Ethernet has no method for forwarding control.

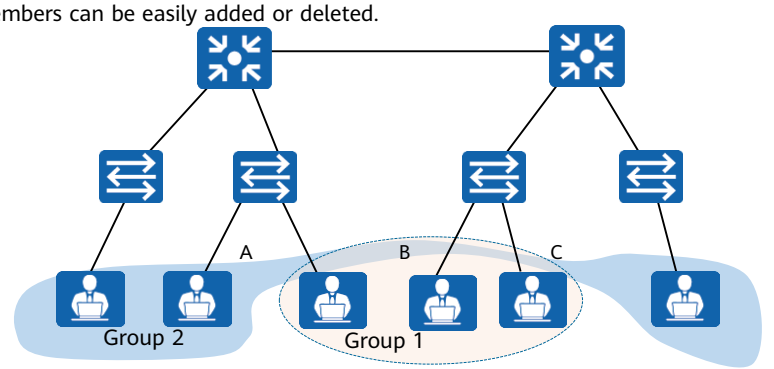


HUAWEI

- Traditional Ethernet switches learn source MAC addresses (MAC addresses of hosts connected to the switch interfaces) of received frames to generate a forwarding table, based on which the switch then forwards frames. All the interfaces can communicate with each other, meaning that maintenance personnel cannot control forwarding between interfaces. Such a network has the following disadvantages:
  - Low network security: The network is prone to attacks because all interfaces can communicate with each other.
  - Low forwarding efficiency: Users may receive a large number of unnecessary packets such as broadcast packets, which consume a lot of bandwidth and host CPU resources.
  - Low service scalability: Network devices process packets on an equal basis and cannot provide differentiated services. For example, Ethernet frames used for network management cannot be preferentially forwarded.

Objectives of the VLAN Technology

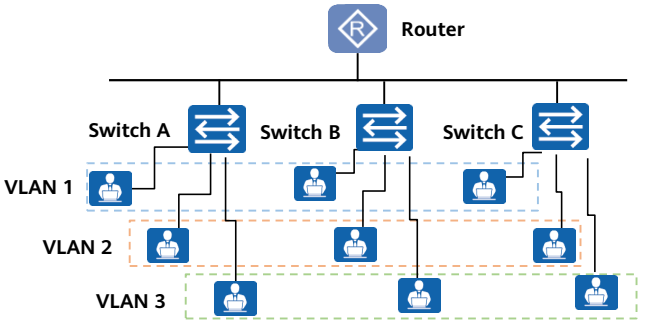
- The Virtual Local Area Network (VLAN) technology divides users into multiple logical groups (networks). Intra-group communication is allowed, whereas inter-group communication is prohibited. Layer 2 unicast, multicast, and broadcast packets can be forwarded only within a group. In addition, group members can be easily added or deleted.



- The VLAN technology provides a management method for controlling the communication between terminals. As shown in the figure above, PCs in Group 1 and PCs in Group 2 cannot communicate with each other.

What Is VLAN?

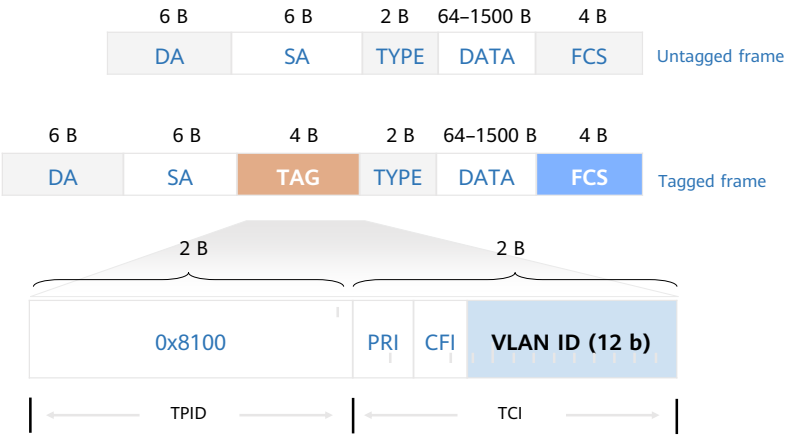
- The VLAN technology logically divides a physical LAN into multiple VLANs (broadcast domains).



HUAWEI

- Hosts within a VLAN can communicate with each other but cannot communicate directly with hosts in other VLANs. This confines broadcast packets within a single VLAN. Inter-VLAN communication is not allowed, which improves network security. For example, if enterprises in the same building establish their own LANs, the cost is high. If enterprises share the same LAN in the building, there may be security risks. In this case, the VLAN technology can be adopted to enable enterprises to share the same LAN while ensuring information security.
- The figure above shows a typical VLAN networking. Three switches are deployed at different locations, for example, on different floors of a building. Each switch is connected to three PCs that belong to different VLANs (for example, VLANs for different enterprises).

VLAN Frame Format

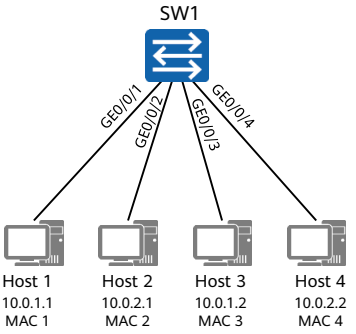


HUAWEI

- IEEE 802.1Q adds a 4-byte VLAN tag to an Ethernet frame header.
- Tag Protocol Identifier (TPID): identifies a frame as an 802.1Q-tagged frame. This field is of 2 bytes and has a fixed value of 0x8100.
- Tag Control Information (TCI): indicates the control information of an Ethernet frame. This field is of 2 bytes.
  - Priority: identifies the priority of an Ethernet frame. This field is of 3 bits. The value of this field ranges from 0 to 7, providing differentiated forwarding services.
  - Canonical Format Indicator (CFI): indicates the bit order of address information in an Ethernet frame. This field is used in token ring or FDDI source-routed MAC methods and is of 1 bit.
  - VLAN Identifier (VLAN ID): controls the forwarding of Ethernet frames based on the VLAN configuration on a switch interface. This field is of 12 bits, with its value ranging from 0 to 4095.
- Since VLAN tags are adopted, Ethernet frames are classified as untagged frames (without 4-byte VLAN tags) or tagged frames (with 4-byte VLAN tags).
- In this course, only the VLAN ID field is discussed.

VLAN Assignment Methods

- How are VLANs assigned on a network?



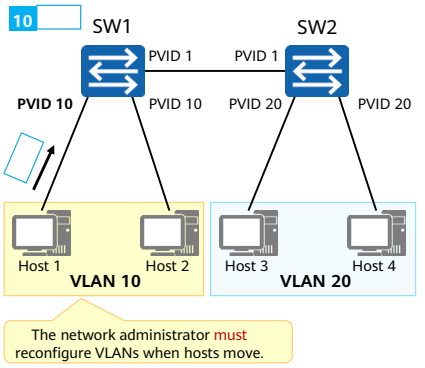
VLAN Assignment Method	VLAN 10	VLAN 20
Interface-based	GE0/0/1, GE0/0/3	GE0/0/2, GE0/0/4
MAC address–based	MAC 1, MAC 3	MAC 2, MAC 4
IP subnet–based	10.0.1.*	10.0.2.*
Protocol-based	IP	IPv6
Policy-based	10.0.1.* + GE0/0/1+ MAC 1	10.0.2.* + GE0/0/2 + MAC 2

HUAWEI

- PCs send only untagged frames. After receiving such an untagged frame, a switch that supports the VLAN technology needs to assign the frame to a specific VLAN based on certain rules.
- Available VLAN assignment methods are as follows:
  - Interface-based assignment: assigns VLANs based on switch interfaces.
    - A network administrator preconfigures a port VLAN ID (PVID) for each switch interface. When an untagged frame arrives at an interface of a switch, the switch tags the frame with the PVID of the interface. The frame is then transmitted in the specified VLAN.
  - MAC address–based assignment: assigns VLANs based on the source MAC addresses of frames.
    - A network administrator preconfigures the mapping between MAC addresses and VLAN IDs. After receiving an untagged frame, a switch tags the frame with the VLAN ID mapping the source MAC address of the frame. The frame is then transmitted in the specified VLAN.
  - IP subnet–based assignment: assigns VLANs based on the source IP addresses and subnet masks of frames.
    - A network administrator preconfigures the mapping between IP addresses and VLAN IDs. After receiving an untagged frame, a switch tags the frame with the VLAN ID mapping the source IP address of the frame. The frame is then transmitted in the specified VLAN.

- Protocol-based assignment: assigns VLANs based on the protocol (suite) types and encapsulation formats of frames.
    - A network administrator preconfigures the mapping between protocol (suite) types and VLAN IDs. After receiving an untagged frame, a switch tags the frame with the VLAN ID mapping the protocol (suite) type of the frame. The frame is then transmitted in the specified VLAN.
- Policy-based assignment: assigns VLANs based on a specified policy, which means VLANs are assigned based on a combination of interfaces, MAC addresses, and IP addresses.
    - A network administrator preconfigures a policy. After receiving an untagged frame that matches the policy, a switch adds a specified VLAN tag to the frame. The frame is then transmitted in the specified VLAN.

Interface-based VLAN Assignment

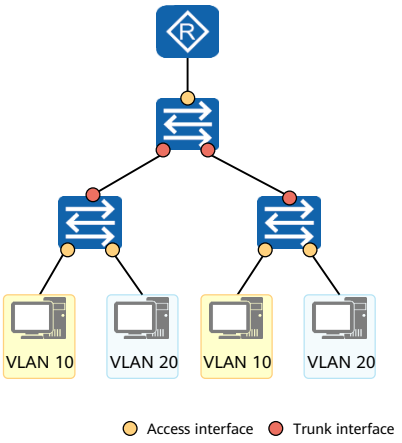


Interface-based VLAN assignment

- **Principles**
  - VLANs are assigned based on interfaces.
  - A network administrator preconfigures a **PVID** for each switch interface to assign each interface to the VLAN corresponding to the PVID.
  - After an interface receives an untagged frame, the switch adds a tag carrying the PVID of the interface to the frame. The frame is then transmitted in the specified VLAN.
- **PVID (Port VLAN ID)**
  - Default VLAN ID of an interface
  - Value range: 1–4094

- Assignment rule:
  - VLAN IDs are configured on physical interfaces of a switch. All PC-sent untagged frames arriving at a physical interface are assigned to the VLAN corresponding to the PVID configured on the interface.
- Characteristics:
  - This VLAN assignment method is simple, intuitive, and easy to implement. Currently, it is the most widely used VLAN assignment method.
  - When a PC is connected to another switch interface, the frames sent by the PC may be assigned to a different VLAN.
- PVID: default VLAN ID
  - Each switch interface must be configured with a PVID. All untagged frames arriving at a switch interface are assigned to the VLAN corresponding to the PVID configured on the interface.
  - The default PVID is 1.

VLAN Interface Types



Interface type
• **Access interface** An access interface is used to connect a switch to a terminal, such as a PC or server. In general, the NICs on such terminals receive and send only untagged frames. An access interface can be added to only one VLAN.
• **Trunk interface** A trunk interface is used to connect a switch to another switch or a sub-interface on a device such as a router or firewall. This type of interface allows frames that belong to multiple VLANs to pass through and differentiates the frames using the 802.1Q tag.
• **Hybrid interface** Similar to a trunk interface, a hybrid interface also allows frames that belong to multiple VLANs to pass through and differentiates the frames using the 802.1Q tag. You can determine whether to allow a hybrid interface to send frames that belong to one or multiple VLANs VLAN-tagged.

- The interface-based VLAN assignment method varies according to the switch interface type.
- Access interface
  - An access interface often connects to a terminal (such as a PC or server) that cannot identify VLAN tags, or is used when VLANs do not need to be differentiated.
- Trunk interface
  - A trunk interface often connects to a switch, router, AP, or voice terminal that can accept and send both tagged and untagged frames.
- Hybrid interface
  - A hybrid interface can connect to a terminal (such as a PC or server) that cannot identify VLAN tags or to a switch, router, AP, or voice terminal that can accept and send both tagged and untagged frames.
  - By default, hybrid interfaces are used on Huawei devices.

Contents

Basic VLAN Configuration Commands

- Create VLANs.

[Huawei] **vlan** *vlan-id*

- Create a VLAN and enter the VLAN view, or enter the view of an existing VLAN.
- The value of *vlan-id* is an integer that ranges from 1 to 4094.

[Huawei] **vlan batch** { *vlan-id1* [**to** *vlan-id2*] }

Create VLANs in a batch.

- **batch**: creates VLANs in a batch.
- *vlan-id1*: specifies the start VLAN ID.
- *vlan-id2*: specifies the end VLAN ID.

- The **vlan** command creates a VLAN and displays the VLAN view. If the VLAN to be created exists, the VLAN view is displayed directly.
- The **undo vlan** command deletes a VLAN.
- By default, all interfaces belong to the default VLAN, that is, VLAN 1.
    - Commands:
    - vlan *vlan-id*
        - *vlan-id*: specifies the VLAN ID. The value is an integer that ranges from 1 to 4094.
    - vlan batch { *vlan-id1* [to *vlan-id2*] }
        - **batch**: creates VLANs in a batch.
        - *vlan-id1* **to** *vlan-id2*: specifies the IDs of VLANs to be created in a batch.
            - *vlan-id1* specifies the start VLAN ID.
            - *vlan-id2* specifies the end VLAN ID. The value of *vlan-id2* must be greater than or equal to that of *vlan-id1*. *vlan-id1* and *vlan-id2* identify a VLAN range.
        - If **to** *vlan-id2* is not specified, the VLAN specified by *vlan-id1* is created.
        - The values of *vlan-id1* and *vlan-id2* are integers that range from 1 to 4094.

Basic Access Interface Configuration Commands

- Set the interface type.

  [Huawei-GigabitEthernet0/0/1] **port link-type access**

  - In the interface view, set the link type of the interface to access.

- Configure the default VLAN of the access interface.

  [Huawei-GigabitEthernet0/0/1] **port default vlan** *vlan-id*

  - In the interface view, configure the default VLAN of the interface and add the interface to the VLAN.
  - *vlan-id*: specifies the default VLAN ID. The value is an integer that ranges from 1 to 4094.

Basic Trunk Interface Configuration Commands

- Set the interface type.

  [Huawei-GigabitEthernet0/0/1] **port link-type trunk**

  - In the interface view, set the link type of the interface to trunk.

- Add the trunk interface to specified VLANs.

  [Huawei-GigabitEthernet0/0/1] **port trunk allow-pass vlan** { { *vlan-id1* [**to** *vlan-id2*] } | **all** }

  - In the interface view, add the trunk interface to specified VLANs.

- (Optional) Configure the default VLAN of the trunk interface.

  [Huawei-GigabitEthernet0/0/1] **port trunk pvid vlan** *vlan-id*

  - In the interface view, configure the default VLAN of the trunk interface.

- Command: port trunk allow-pass vlan { { *vlan-id1* [to *vlan-id2*] | all }
  - *vlan-id1* [**to** *vlan-id2*]: specifies the VLANs to which the trunk interface is added.
    - *vlan-id1* specifies the start VLAN ID.
    - **to** *vlan-id2* specifies the end VLAN ID. The value of *vlan-id2* must be greater than or equal to that of *vlan-id1*.
    - The values of *vlan-id1* and *vlan-id2* are integers that range from 1 to 4094.
  - **all**: adds the trunk interface to all VLANs.
- Command: port trunk pvid vlan *vlan-id*
  - *vlan-id*: specifies the default VLAN ID of the trunk interface. The value is an integer that ranges from 1 to 4094.

Basic Hybrid Interface Configuration Commands

- Set the interface type.

  [Huawei-GigabitEthernet0/0/1] **port link-type hybrid**

  - In the interface view, set the link type of the interface to hybrid.
- Add the hybrid interface to specified VLANs.

  [Huawei-GigabitEthernet0/0/1] **port hybrid untagged vlan** { { *vlan-id1* [**to** *vlan-id2*] } | **all** }

  - In the interface view, add the hybrid interface to specified VLANs. Frames that belong to these VLANs then pass through the hybrid interface in untagged mode.

  [Huawei-GigabitEthernet0/0/1] **port hybrid tagged vlan** { { *vlan-id1* [**to** *vlan-id2*] } | **all** }

  - In the interface view, add the hybrid interface to specified VLANs. Frames that belong to these VLANs then pass through the hybrid interface in tagged mode.
- (Optional) Configure the default VLAN of the hybrid interface.

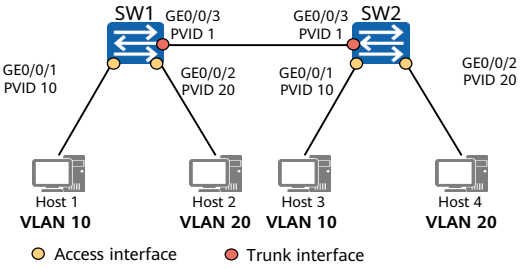
  [Huawei-GigabitEthernet0/0/1] **port hybrid pvid vlan** *vlan-id*

  - In the interface view, configure the default VLAN of the hybrid interface.

- Command: port hybrid untagged vlan { { *vlan-id1* [to *vlan-id2*] } | all }
  - *vlan-id1* [**to** *vlan-id2*]: specifies the VLANs to which the hybrid interface is added.
    - *vlan-id1* specifies the start VLAN ID.
    - **to** *vlan-id2* specifies the end VLAN ID. The value of *vlan-id2* must be greater than or equal to that of *vlan-id1*.
    - The values of *vlan-id1* and *vlan-id2* are integers that range from 1 to 4094.
  - **all**: adds the hybrid interface to all VLANs.
- Command: port hybrid tagged vlan { { *vlan-id1* [to *vlan-id2*] } | all }
  - *vlan-id1* [**to** *vlan-id2*]: specifies the VLANs to which the hybrid interface is added.
    - *vlan-id1* specifies the start VLAN ID.
    - **to** *vlan-id2* specifies the end VLAN ID. The value of *vlan-id2* must be greater than or equal to that of *vlan-id1*.
    - The values of *vlan-id1* and *vlan-id2* are integers that range from 1 to 4094.
  - **all**: adds the hybrid interface to all VLANs.
- Command: port hybrid pvid vlan *vlan-id*
  - *vlan-id*: specifies the default VLAN ID of the hybrid interface. The value is an integer that ranges from 1 to 4094.

Configuration Example: Configuring Interface-based VLAN Assignment

- Networking requirements
  - There are many users connected to an enterprise's switches. Currently, users of the same service access the enterprise network through different switches. To ensure communication security, the enterprise requires that users with the same service can directly communicate only with each other.
  - To meet this requirement, configure interface-based VLAN assignment on the switches and add interfaces connecting users with the same service to the same VLAN. In this way, users in the same VLAN can directly communicate only with each other at Layer 2.



HUAWEI

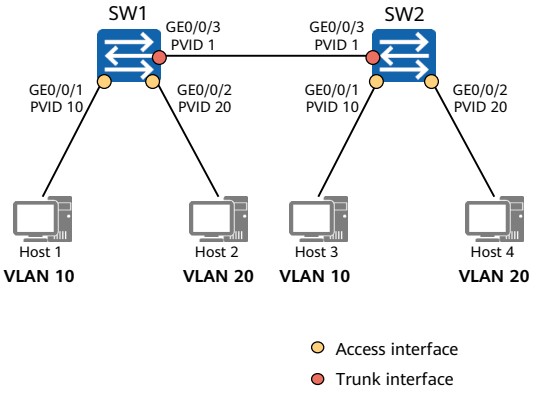
- Configuration roadmap:
  - Create VLANs and add interfaces connecting users to the VLANs to isolate Layer 2 traffic between users with different services.
  - Configure interface types and specify allowed VLANs for interfaces on SW1 and SW2 to allow users with the same service to communicate through SW1 and SW2.

Creating VLANs

Create VLANs:

```
[SW1] vlan 10
[SW1-vlan10] quit
[SW1] vlan 20
[SW1-vlan20] quit
```

```
[SW2] vlan batch 10 20
```



Configuring Access and Trunk Interfaces

Configure access interfaces and add the interfaces to corresponding VLANs.

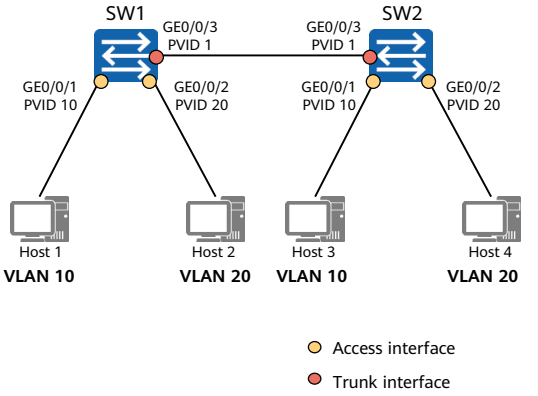
```
[SW1] interface GigabitEthernet 0/0/1
[SW1-GigabitEthernet0/0/1] port link-type access
[SW1-GigabitEthernet0/0/1] port default vlan 10
```

```
[SW1] interface GigabitEthernet 0/0/2
[SW1-GigabitEthernet0/0/2] port link-type access
[SW1] vlan 20
[SW1-vlan20] port GigabitEthernet0/0/2
[SW1-vlan20] quit
```

Configure a trunk interface and configure allowed VLANs for the interface.

```
[SW1] interface GigabitEthernet 0/0/3
[SW1-GigabitEthernet0/0/3] port link-type trunk
[SW1-GigabitEthernet0/0/3] port trunk pvid vlan 1
[SW1-GigabitEthernet0/0/3] port trunk allow-pass vlan 10 20
```

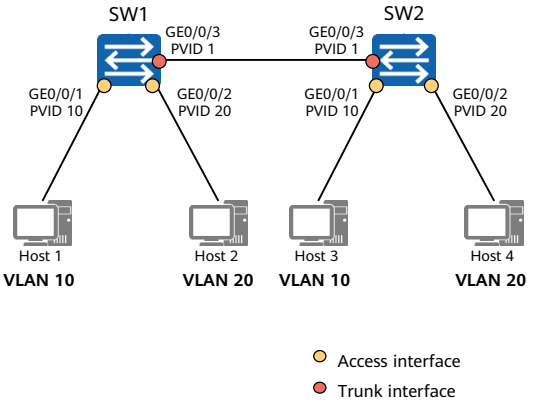
Note: The configuration on SW2 is similar to that on SW1.



HUAWEI

Verifying the Configuration

```
[SW1]display vlan
The total number of vlans is: 3
--------------------------------------------------------------------------------
U: Up;        D: Down;         TG: Tagged;         UT: Untagged;
MP: Vlan-mapping;              ST: Vlan-stacking;
#: ProtocolTransparent-vlan;   *: Management-vlan;
--------------------------------------------------------------------------------
VID         Type        Ports
--------------------------------------------------------------------------------
1           common      UT:GE0/0/3(U)          ...
10          common      UT:GE0/0/1(U)
                        TG:GE0/0/3(U)
20          common      UT:GE0/0/2(U)
                        TG:GE0/0/3(U)
```



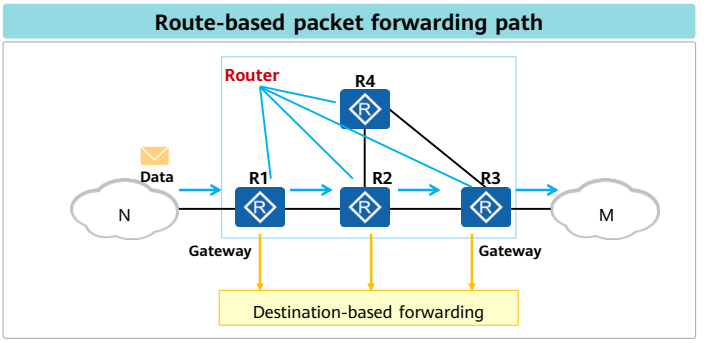
HUAWEI

- The **display vlan** command displays information about VLANs.
- Description of the command output:
  - **Tagged/Untagged Port**: interfaces that are manually added to a VLAN in tagged or untagged mode.
  - **VID** or **VLAN ID**: VLAN ID.
  - **Type** or **VLAN Type**: VLAN type. The value **common** indicates a common VLAN.
  - **Ports**: interfaces added to a VLAN.

Contents

Routes

- Routes are the path information that is used to guide packet forwarding.
- A routing device is one that forwards packets to a destination network segment based on routes. The most common routing device is a router.
- A routing device maintains an IP routing table that stores routing information.

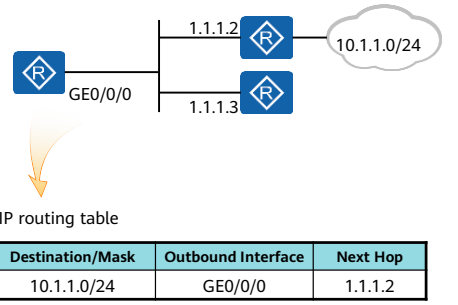


HUAWEI

- A gateway and an intermediate node (a router) select a proper path according to the destination address of a received IP packet, and forward the packet to the next router. The last-hop router on the path performs Layer 2 addressing and forwards the packet to the destination host. This process is called route-based forwarding.
- The intermediate node selects the best path from its IP routing table to forward packets.
- A routing entry contains a specific outbound interface and next hop, which are used to forward IP packets to the corresponding next-hop device.

Routing Information

- A route contains the following information:
  - Destination network: identifies a destination network segment.
  - Mask: identifies a network segment together with a destination IP address.
  - Outbound interface: indicates the interface through which a data packet is sent out of the local router.
  - Next hop: indicates the next-hop address used by the router to forward the data packet to the destination network segment.
- The information identifies the destination network segment and specifies the path for forwarding data packets.



IP routing table

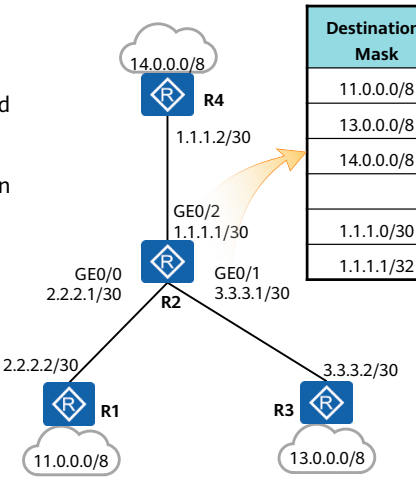
Destination/Mask	Outbound Interface	Next Hop
10.1.1.0/24	GE0/0/0	1.1.1.2

HUAWEI

- Based on the information contained in a route, a router can forward IP packets to the destination network segment along the corresponding path.
- The destination address and mask identify the destination address of an IP packet. After an IP packet matches a specific route, the router determines the forwarding path according to the outbound interface and next hop of the route.
- The next-hop device for forwarding the IP packet cannot be determined based only on the outbound interface. Therefore, the next-hop device address must be specified.

Routing Table

- A router discovers routes using multiple methods.
- A router selects the optimal route and installs it in its IP routing table.
- A router forwards IP packets based on routes in the IP routing table.
- Routers manage path information by managing their IP routing tables.



Destination/ Mask	Next Hop	Outbound Interface
11.0.0.0/8	2.2.2.2	GE0/0
13.0.0.0/8	3.3.3.2	GE0/1
14.0.0.0/8	1.1.1.2	GE0/2
...		
1.1.1.0/30	1.1.1.1	GE0/2
1.1.1.1/32	127.0.0.1	GE0/2

HUAWEI

- A router forwards packets based on its IP routing table.
- An IP routing table contains many routing entries.
- An IP routing table contains only optimal routes.
- A router manages routing information by managing the routing entries in its IP routing table.

Checking the IP Routing Table

```
<Huawei> display ip routing-table
Route Flags: R - relay, D - download to fib
------------------------------------------------------------------------------
Routing Tables: Public
         Destinations: 6        Routes: 6

Destination/Mask    Proto   Pre  Cost      Flags NextHop         Interface

        1.1.1.1/32  Static  60   0           D   0.0.0.0         NULL0
        2.2.2.2/32  Static  60   0           D   100.0.0.2       Vlanif100
      100.0.0.0/24  Direct  0    0           D   100.0.0.1       Vlanif100
      100.0.0.1/32  Direct  0    0           D   127.0.0.1       Vlanif100
      127.0.0.0/8   Direct  0    0           D   127.0.0.1       InLoopBack0
      127.0.0.1/32  Direct  0    0           D   127.0.0.1       InLoopBack0
```

Destination network address/Mask

Protocol type

Route preference

Cost (metric)

Flag

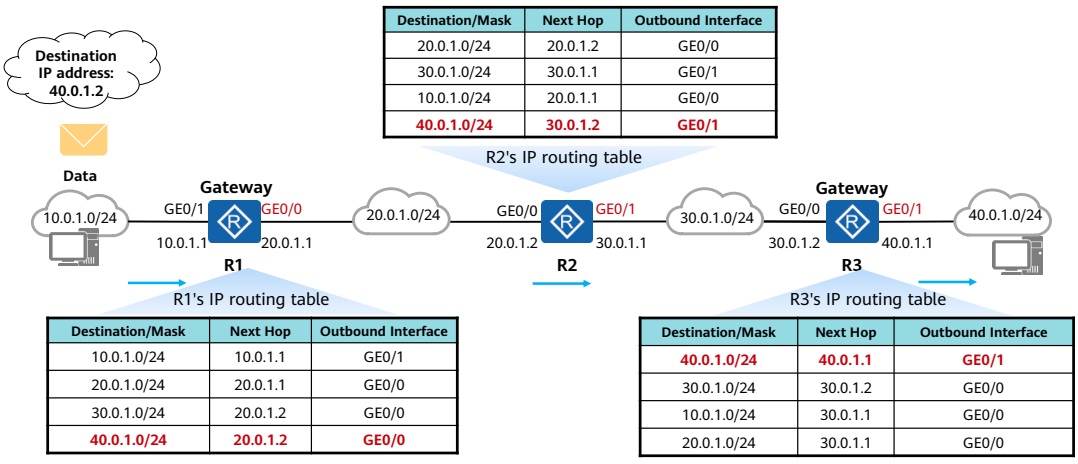
Next-hop IP address

Outbound interface

HUAWEI

- Destination/Mask: indicates the destination network address and mask of a specific route. The network segment address of a destination host or router is obtained through the AND operation on the destination address and mask. For example, if the destination address is 1.1.1.1 and the mask is 255.255.255.0, the IP address of the network segment to which the host or router belongs is 1.1.1.0.
- Proto (Protocol): indicates the protocol type of the route, that is, the protocol through which a router learns the route.
- Pre (Preference): indicates the routing protocol preference of the route. There may be multiple routes to the same destination, which have different next hops and outbound interfaces. These routes may be discovered by different routing protocols or manually configured. A router selects the route with the highest preference (with the lowest preference value) as the optimal route.
- Cost: indicates the cost of the route. When multiple routes to the same destination have the same preference, the route with the lowest cost is selected as the optimal route.
- NextHop: indicates the local router's next-hop address of the route to the destination network. This field specifies the next-hop device to which packets are forwarded.
- Interface: indicates the outbound interface of the route. This field specifies the local interface through which the local router forwards packets.

Route-based Forwarding Process



R2's IP routing table

Destination/Mask	Next Hop	Outbound Interface
20.0.1.0/24	20.0.1.2	GE0/0
30.0.1.0/24	30.0.1.1	GE0/1
10.0.1.0/24	20.0.1.1	GE0/0
40.0.1.0/24	**30.0.1.2**	**GE0/1**

R1's IP routing table

Destination/Mask	Next Hop	Outbound Interface
10.0.1.0/24	10.0.1.1	GE0/1
20.0.1.0/24	20.0.1.1	GE0/0
30.0.1.0/24	20.0.1.2	GE0/0
40.0.1.0/24	**20.0.1.2**	**GE0/0**

R3's IP routing table

Destination/Mask	Next Hop	Outbound Interface
40.0.1.0/24	**40.0.1.1**	**GE0/1**
30.0.1.0/24	30.0.1.2	GE0/0
10.0.1.0/24	30.0.1.1	GE0/0
20.0.1.0/24	30.0.1.1	GE0/0

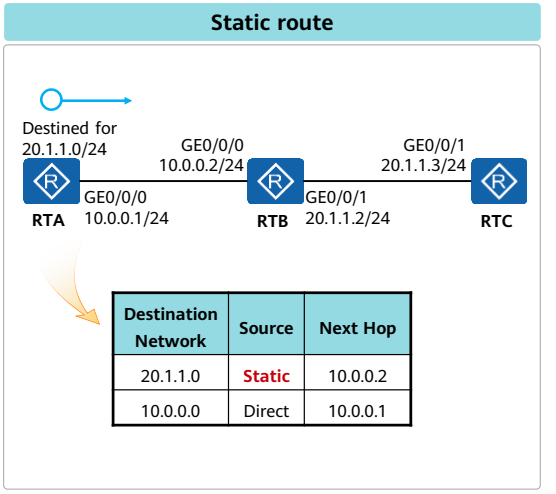
HUAWEI

- The IP packets from 10.0.1.0/24 need to reach 40.0.1.0/24. These packets arrive at the gateway R1, which then searches its IP routing table for the next hop and outbound interface and forwards the packets to R2. After the packets reach R2, R2 forwards the packets to R3 by searching its IP routing table. After receiving the packets, R3 searches its IP routing table, finding that the destination IP address of the packets belongs to the network segment where a local interface resides. Therefore, R3 directly forwards the packets to the destination network segment 40.0.1.0/24.

Contents

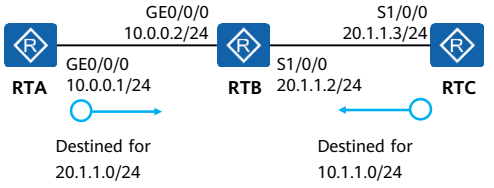
Introduction to Static Routes

- Static routes are manually configured by network administrators, have low system requirements, and apply to simple, stable, and small networks.
- However, static routes cannot automatically adapt to network topology changes and so require manual intervention.
- Packets destined for 20.1.1.0/24 do not match the direct route in RTA's IP routing table. In this case, a static route needs to be manually configured so that the packets sent from RTA to 20.1.1.0/24 can be forwarded to the next hop 10.0.0.2.



HUAWEI

Configuration Example



Configure RTA.

```
[RTA] ip route-static 20.1.1.0 255.255.255.0 10.0.0.2
```

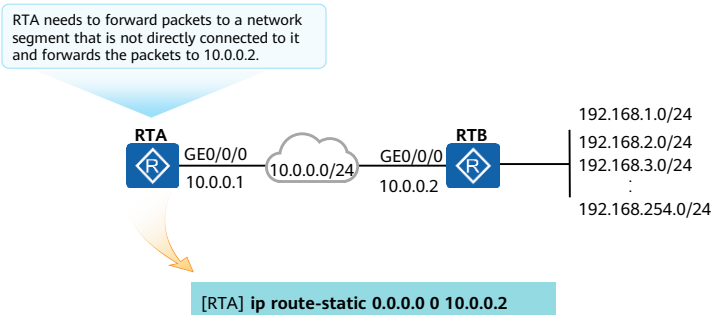
Configure RTC.

```
[RTC] ip route-static 10.0.0.0 255.255.255.0 S1/0/0
```

- Configure static routes on RTA and RTC for communication between 10.0.0.0/24 and 20.1.1.0/24.
- Packets are forwarded hop by hop. Therefore, all the routers along the path from the source to the destination must have routes destined for the destination.
- Data communication is bidirectional. Therefore, both forward and return routes must be available.

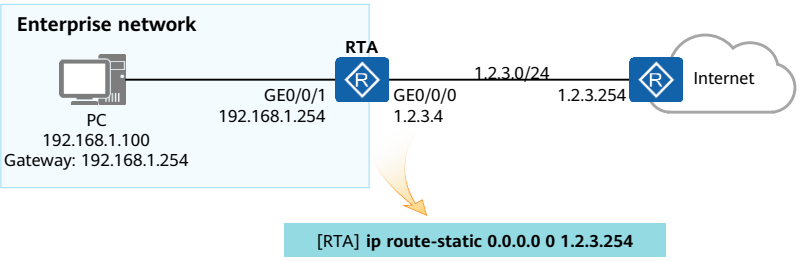
Default Route

- Default routes are used only when packets to be forwarded do not match any routing entry in an IP routing table.
- In an IP routing table, a default route is the route to network 0.0.0.0 (with the mask 0.0.0.0), namely, 0.0.0.0/0.



Application Scenarios of Default Routes

- Default routes are typically used at the egress of an enterprise network. For example, you can configure a default route on an egress device so that the device forwards IP packets destined for any address on the Internet.



[RTA] **ip route-static 0.0.0.0 0 1.2.3.254**

HUAWEI

Quiz

1. Which of the following are functions of firewalls?
   A. Isolating networks of different security levels
   B. Authenticating user identities
   C. Implementing NAT
   D. Performing route calculation
2. Default routes are typically used at the egress of an enterprise network. For example, you can configure a default route on an egress device so that the device forwards IP packets destined for any address on the Internet.
   A. True
   B. False

- Answers:
  - ABCD
  - A

Summary

- In this course, we have learned the composition of IP addresses, subnetting, basic principles of network communication, and basic operations and application scenarios of common network protocols. In the following course, we will learn operating system basics. Stay tuned.

Recommendations

- Huawei Learning
  - https://e.huawei.com/en/talent/portal/#/
- Huawei Support Knowledge Base
  - https://support.huawei.com/enterprise/en/knowledge?lang=en

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.

Operating System Basics

HUAWEI

Foreword

- The operating system (OS) plays an important role in the interaction between the user and the computer. But what exactly is an OS? What are the types of OSs? What are the basic commands of the Linux system? This course explores these questions, and more, to help you better understand OSs.

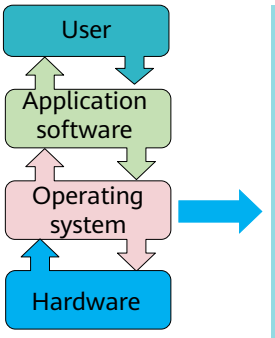
Objectives

- On completion of this course, you will be able to:
  - Understand the definition and composition of the operating system.
  - Familiarize yourself with the classification of operating systems.
  - Master the basic operations of the Linux operating system.

Contents

Operating System Definition and Functions

- An operating system (OS) is a computer program (system software) that manages and controls computer hardware and software resources.



Core functions:

- System call interface
- Process management
- Memory management
- File system management
- Driver management

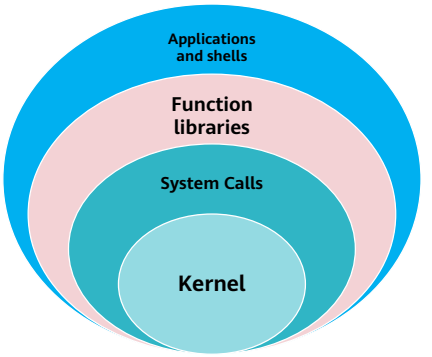
HUAWEI

- An operating system is a special computer program that controls the computer, connects the computer and the user, and coordinates and manages hardware resources, including the CPU, drive, memory, and printer. These resources are required for running programs.
- Mainstream OSs:
  - From the perspective of application field, OSs are classified into the following types:
    - Desktop OS, server OS, host OS, and embedded OS.
  - Based on whether an OS is open source, it is classified as:
    - Open source OS (Linux and Unix) or close source OS (Windows and Mac OS).

Contents

Components of an Operating System

- From the perspective of users, an OS consists of a kernel and various applications, that is, the kernel space and user space.
- The user space is where upper-layer applications run.
- The kernel is essentially a software program used to manage computer hardware resources and provide a system call interface to run upper-layer application programs.

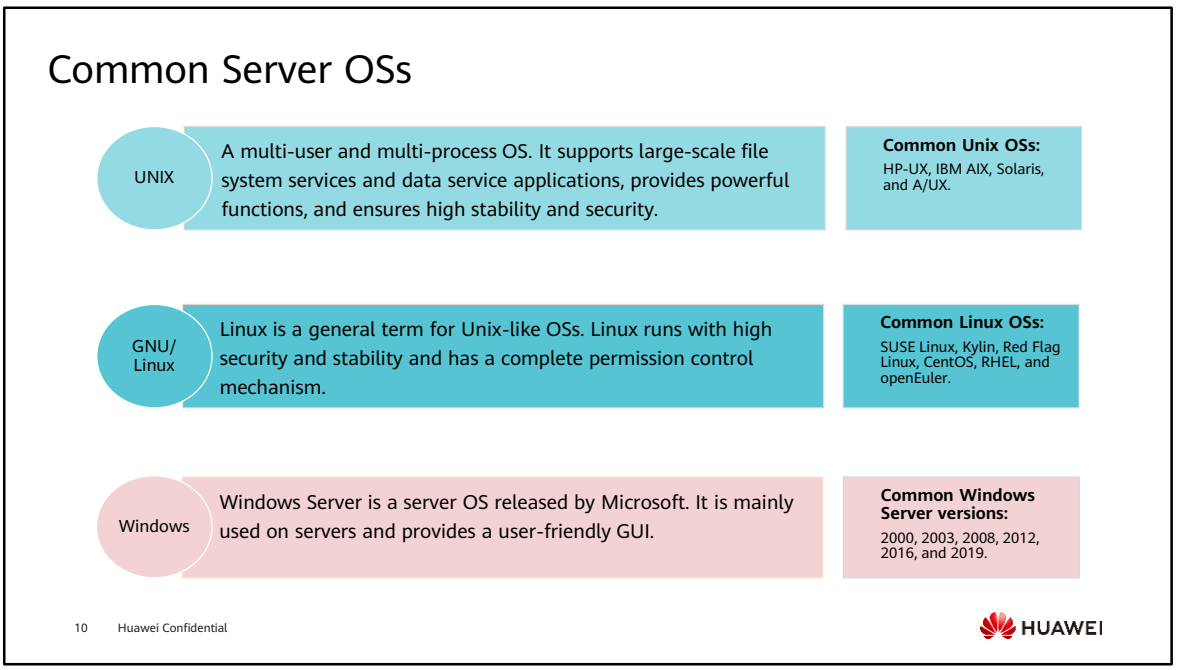


HUAWEI

- System calls: The execution of applications depends on resources provided by the kernel, including the CPU, storage, and I/O resources. To enable upper-layer applications to access these resources, the kernel must provide an access interface, that is, the system call interface.
- Library functions: System calls are encapsulated as library functions to provide simple service logic interfaces to users. Simple access to system resources can be completed using system calls. Library functions allow for complex access to system resources.
- Shell: A shell is a special application program, which is also called the command line interface. It is a command interpreter in essence. It can execute texts (scripts) that comply with the shell syntax. Some shell script statements encapsulate system calls for convenient use.

- The kernel controls hardware resources, manages OS resources, and provides a system call interface for applications.
    - Process scheduling and management: The kernel creates and destroys processes and handles their input and output.
    - Memory management: The kernel creates a virtual address space for all processes based on limited available resources.
    - File system management: Linux is based on the concept of file system to a large extent. Almost anything in Linux can be seen as a file. The kernel builds a structured file system on top of unstructured hardware.
    - Device driver management: Drivers of all peripherals in the system, such as hard drives, keyboards, and tape drives, are embedded in the kernel.
    - Network resource management: All routing and address resolution operations are performed in the kernel.
- Summary: User-mode applications can access kernel-mode resources using the following:
    - System calls
    - Shell scripts
    - Library functions

Contents



- Relationship between Linux and Unix:
  - Linux is a Unix-like OS with optimized functions and user experience. Linux mimics Unix in terms of appearance and interaction.
  - The Linux kernel was initially written by Linus Torvalds for a hobby when he was studying at the University of Helsinki. Frustrated by MINIX, a Unix-like OS for educational purposes, he decided to develop his own OS. The first version was released in September 1991 with only 10,000 lines of code.
  - Unix systems are usually compatible only with specific hardware. This means that most Unix systems such as AIX and HP-UX cannot be installed on x86 servers or PCs. On the contrary, Linux can run on various hardware platforms.
  - Unix is commercial software, while Linux is open source and free of charge.
- The GNU Project:
  - The GNU Project was publicly announced on September 27, 1983 by Richard Stallman, aiming at building an OS composed wholly of free software.
  - GNU is a recursive acronym for "GNU's Not Unix". Linux provides a kernel, and GNU provides a large amount of free software to enrich the various applications run on the kernel.

Contents

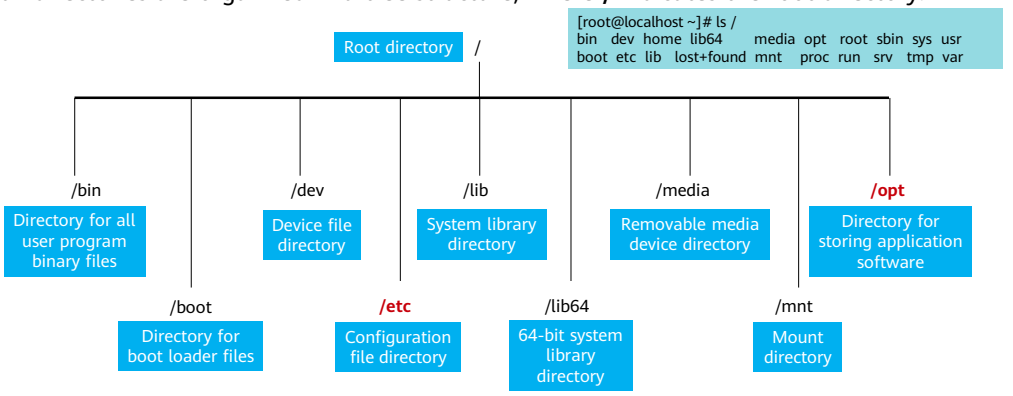
Features of Linux

- Multi-platform design
  - Linux can run on multiple hardware platforms. The Linux kernel is also used in embedded systems that run on devices such as handheld computers and set-top boxes.
- Multi-user and multitasking
  - System resources can be used by different users. Multiple programs can run simultaneously and independently.
- Free to use
  - The source code of Linux is available for free. Users can edit and modify the source code as required.
- Fully compatible with the POSIX.1 standard
- Inherits the design concept of Unix
  - Everything is a file.

- The Portable Operating System Interface (POSIX) is a family of standards specified by IEEE. POSIX defines the application programming interfaces (APIs) of software runs on Unix. The family of POSIX standards is formally designated as IEEE 1003 and the ISO/IEC standard number is ISO/IEC 9945. The name of POSIX consists of the abbreviation of Portable Operating System Interface and an X that indicates the inheritance of Unix APIs.
- Linux is a popular multitasking and multi-user OS with the following features:
  - Multitasking: Linux is a multitasking operating system that allows multiple tasks to run at the same time. DOS is a single-task OS and cannot run multiple tasks at the same time. When the system executes multiple tasks, the CPU executes only one task at a time. Linux divides the CPU time into time slices and allocates them to multiple processes. The CPU runs so quickly that all programs (processes) seem to be running at the same time from the user's perspective.
  - Multi-user: Linux is a multi-user OS that allows multiple users to use it at the same time. In Linux, each user runs their own or public programs as if they had a separate machine. DOS is a single-user OS and allows only one user to use it at a time.
  - Pipeline: Linux allows the output of a program to be used as the input of the next program. Multiple programs are chained together as a pipeline. By combining simple tasks, you can complete complex tasks, improving the operation convenience. Later versions of DOS learned from Linux and implemented this mechanism.
  - Powerful shells: Shells are the command interpreters of Linux. Linux provides multiple powerful shells, each of which is an interpreted high-level language. Users can create numerous commands through programming.

Linux File Directory Structure

- Linux OS adopts "Everything is a file" design.
- Linux directories are organized in a tree structure, where **/** indicates the root directory.



HUAWEI

- The core philosophy of Linux is "everything is a file", which means that all files, including directories, character devices, block devices, sockets, printers, processes, threads, and pipes, can be operated, read, and written by using functions such as **fopen()**, **fclose()**, **fwrite()**, and **fread()**.
- After logging in to the system, enter the **ls /** command in the current command window. The command output similar to the figure is displayed. The directories are described as follows:
  - **/bin**: short for binary. This directory stores the frequently used commands.
  - **/boot**: stores some core files used for booting the Linux OS, including some links and images.
  - **/dev**: short for device. This directory stores peripheral device files of Linux. The method of accessing devices on Linux is the same as that of accessing files.
  - **/etc**: stores all configuration files and subdirectories required for system management.
  - **/lib**: stores basic shared libraries of the system. A library functions similarly to a dynamic link library (DLL) file on Windows. Almost all applications need to use these shared libraries.
  - **/mnt**: temporary mount point for other file systems. You can mount the CD-ROM drive to **/mnt** and then go to this directory to view the contents in the CD-ROM.
  - **/opt**: stores additional software installed on the host. For example, if you install an Oracle database, you can save the installation package to this directory. By default, this directory is empty.

Contents

Background of openEuler

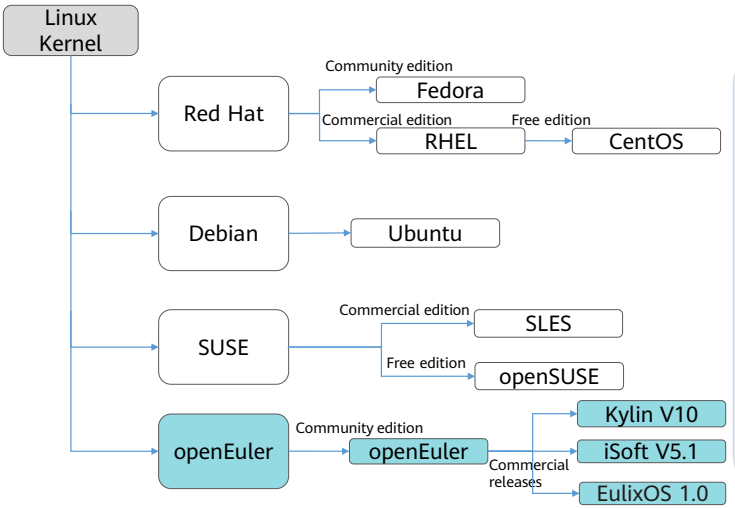
- EulerOS is a server OS that runs on the Linux kernel and supports processors of multiple architectures, such as x86 and ARM. It is ideal for database, big data, cloud computing, and artificial intelligence (AI) scenarios.
- Over the past decade, EulerOS has interconnected with various Huawei products and solutions. It is respected for its security, stability, and efficiency.
- Cloud computing, in addition to Kunpeng processors, has sparked the growth of EulerOS to become the most powerful software infrastructure in the Kunpeng ecosystem.
- To develop the Kunpeng ecosystem and build prosperity of the computing industry in China and around the world, the open source version of EulerOS was officially released as openEuler at the end of 2019.

Introduction to openEuler

- openEuler is a free open source Linux distribution that supports multiple processor architectures including x86, ARM, and RISC-V.
- All developers, enterprises, and business organizations can simply use the openEuler community version, or use it to build, develop, and release their own OS versions.

https://openeuler.org/
https://gitee.com/openeuler

Relationship Between openEuler and Mainstream OSs



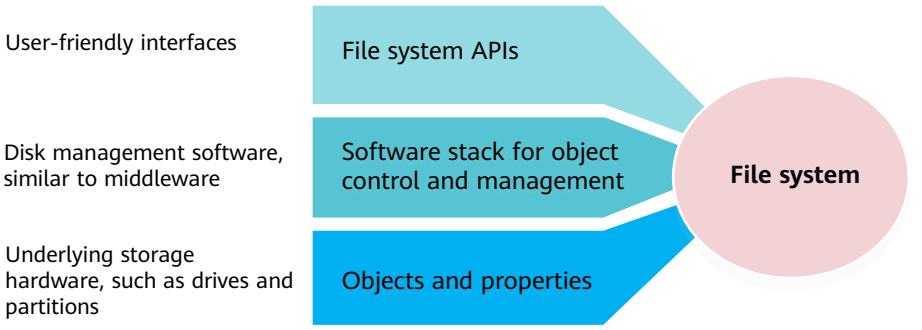
- The upstream community of openEuler, SUSE, Debian, and Red Hat is the kernel community www.kernel.org.
- The openEuler community releases free long-term support (LTS) versions, enabling operating system vendors (OSVs) such as Kylinsoft, iSoft, Sinosoft, and GreatDB to develop commercial releases.

HUAWEI

Contents

File System Overview

- A file system is a method and a data structure used by an OS to identify files on a storage device or a partition, that is, a method of organizing files on a storage device.
- In an OS, a software structure that manages and stores file data is referred to as a file management system, or file system for short.



HUAWEI

- Function: The file system organizes and allocates the space on file storage devices, stores files, and protects and retrieves the stored files. Specifically, it is responsible for creating files for users, saving, reading, modifying, and dumping files, controlling access to files, and canceling a file that is no longer in use. Functions of a file system include: manages and schedules storage space of a file, and provides the logical structure, physical structure, and storage method of the file; maps file identifiers to actual addresses, controls and accesses files, shares file information, provides reliable file confidentiality and protection measures, and provides file security measures.

File Systems on openEuler

- The openEuler kernel is derived from Linux. The Linux kernel supports more than 10 types of file systems, such as Btrfs, JFS, ReiserFS, ext, ext2, ext3, ext4, ISO 9660, XFS, Minix, MSDOS, UMSDOS, VFAT, NTFS, HPFS, SMB, SysV and PROC. The following table describes the common file systems.
- The default file system on openEuler is ext4.

Common File System	Description
Ext	File system specially designed for Linux. The latest version is ext4.
XFS	A high-performance log file system developed for the IRIX OS by Silicon Graphics in 1993. Later ported to the Linux kernel, it excels in large-file processing and provides smooth data transfer.
VFAT	On Linux, VFAT is the name of the FAT (including FAT16 and FAT32) file systems in DOS and Windows.
ISO 9600	The standard file system for optical disc media. Linux supports this file system, allowing the system to read CD-ROMs and ISO image files, and burn CD-ROMs.

Contents

Contents

Linux GUI and CLI

- A graphical user interface (GUI) presents all elements as graphical. The mouse is used as the main input tool, and buttons, menus, and dialog boxes are used for interaction, focusing on ease of use.
- All elements on a command line interface (CLI) are character-based. The keyboard is used as the input tool to enter commands, options, and parameters for executing programs, achieving high efficiency.

- Example:
  - Start the calculator on the Windows GUI. Choose **Start** > **Programs** > **Windows Accessories** > **Calculator**. In the calculator, click buttons to enter an expression. Similarly, a small keyboard is displayed when a certain program requires you to enter a password, asking you to click the numbers. This method is very user-friendly, and the calculator looks similar to the input device used at bank ATMs all around the world. The difference here is that you click it using a mouse, rather than using your own hands.
  - In the Linux CLI, enter **bc** to start the calculator. Enter the calculation **1** + **1** and press **Enter**. Result **2** is obtained.

Why We Use CLIs

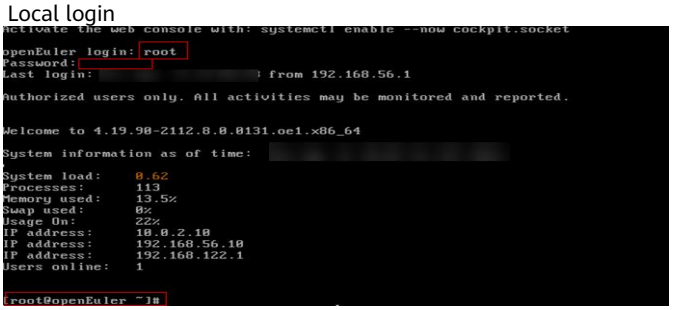
- Higher efficiency
  - On Linux, it is faster to perform operations on a keyboard than using the mouse.
  - A GUI-based operation cannot be repeated, while a CLI script can be used to complete all required tasks, for example, deleting outdated log files.
- Lower overheads compared with a GUI
  - Running a GUI requires a large amount of system resources. With the CLI, system resources can be released and allocated to other operations.
- Sometimes, the only choice
  - Most servers choose not to install a GUI.
  - Tools for maintaining and managing network devices do not provide a GUI.

Linux CLI Shortcuts

- Tab completion
  - Use the **Tab** key to complete a command or file name, which is time-saving and accurate.
  - When no command is entered, press **Tab** twice to list all available commands.
  - If you have entered a part of the command name or file name, press **Tab** to complete it automatically.
- Cursor control
  - ↑: Press ↑ several times to display historical commands for quick execution.
  - ↓: Press ↓ together with ↑ for choosing a historical command.
  - **Home**: Press **Home** to move the cursor to the beginning of the line.
  - **Ctrl**+**A**: Press **Ctrl**+**A** to move the cursor to the beginning of the line.
  - **Ctrl**+**E**: Press **Ctrl**+**E** to move the cursor to the end of the line.
  - **Ctrl**+**L**: Press **Ctrl**+**L** to clear the screen.

Login to Linux

- You can log in to Linux in either of the following ways:
  - Local login



  - Remote Login
    - Using clients such as PuTTY and Xshell to remotely log in to openEuler.

HUAWEI

- After you log in to the system as the **root** user, **#** is displayed in the command prompt.

Changing the Password

- Passwords are used to ensure the security of system and data.
- To ensure system security, you should:
  - Change the password upon the first login.
  - Change passwords periodically.
  - Set a complex password, for example, a password containing more than eight characters and at least three types of the following characters: uppercase letters, lowercase letters, digits, and special characters.
- You can run the **passwd** command to change the password.

```
[root@openEuler ~]# passwd                                  # Change the password of the current user.
Changing password for user root.
New password:                                               # Enter the new password.
Retype new password: # Enter the new password again.
passwd: all authentication tokens updated successfully
[root@openEuler ~]# passwd test1                            # Change the password of a common user as the root user.
Changing password for user test1.
New password:
BAD PASSWORD: The password is a palindrome
Retype new password:
passwd: all authentication tokens updated successfully.
```


HUAWEI

- For security purposes, openEuler does not display the password when you enter it and does not use any placeholders to indicate the number of characters.

Types of Linux Users

- On Linux, a UID is used to uniquely identify a user.
- Based on different UIDs, there are three types of users in Linux (openEuler is used as an example):
  - Super user
    - The super user is also called the super administrator. Its UID is 0. The super user has all system permissions. It is similar to the administrator in Windows.
  - System user
    - System users, also called program users, have UIDs ranging from 1 to 999. A system user is created by a program and is used to run the program or service.
  - Common user
    - Common users are generally created by the super administrator (the root user) to perform limited management and maintenance operations on the system. UIDs of common users range from 1000 to 60000.

Creating and Deleting a Linux User

- Creating a user (common user by default): **useradd username**
- Viewing user information: **id username**
- Switching users: **su - username**
- Deleting a user: **userdel username**

```
[root@openEuler ~]# useradd user01                    # Create user user01.
[root@openEuler ~]# id user01                         # View information about user01 as the root user.
uid=1001(user01) gid=1001(user01) groups=1001(user01)
[root@openEuler ~]# su - user01                       # Switch to the user01 user. The command prompt changes to $.
[user01@openEuler ~]$ id                              # Use the id command to view information about the current user
                                                        by default.
uid=1001(user01) gid=1001(user01) groups=1001(user01)
[user01@openEuler ~]$ exit                            # Log out of the current user.
logout
[root@openEuler ~]# userdel user01                    # Delete user user01.
```

Contents

Basic openEuler Operations

- Basic Knowledge of Linux Commands
- Basic openEuler Commands
- Text Processing on openEuler
- Network Management on openEuler

Power Supply Commands: shutdown and reboot

- **shutdown** is used to shut down the computer, which requires root permissions.
  - Main options:
    - **-h**: powers off the computer after it is shut down.
    - **-r**: powers on the computer after it is shut down. (This operation is equivalent to restarting the computer.)
    - **-p**: explicitly indicates that the system will be shut down and the main power supply will be cut off.
- **reboot** is used to restart the computer, which requires system administrator permissions.
  - Main options:
    - **-w**: writes records to the **/var/log/wtmp** file. It does not restart the system.
    - **-d**: does not write records to the **/var/log/wtmp** file.
    - **-i**: restarts the system with network settings disabled.

- The **shutdown** command can safely shut down the system. It is dangerous to shut down the Linux system by directly powering off the system.
- Different from Windows, Linux runs many processes in the background. Therefore, forcible shutdown may cause loss of process data, making the system unstable and even damaging hardware in some systems.
- If you run the **shutdown** command to shut down the system, the system notifies all users who have logged in that the system will be shut down and the **login** command will be frozen, prohibiting new user logins.

File Paths

- Absolute path: a path starting from the root directory (/), for example, /root/Desktop.
- Relative path: a path starting from the current path, for example, ./Desktop.
- ./ or . indicates the current path. ../ or .. indicates the upper-level directory of the current path.
- pwd: Viewing the current path.
- cd: Switching paths.

```
[root@localhost ~]# pwd                          # View the current path.
/root
[root@localhost ~]# cd /root/Desktop             # Go to the Desktop directory using the absolute path.
[root@localhost Desktop]# cd                                  # Run the cd command without a parameter to go to the home directory of the current user by default.

[root@localhost ~]#
[root@localhost ~]# cd ./Desktop                              # Go to the Desktop directory using a relative path.
[root@localhost Desktop]# pwd
/root/Desktop
[root@localhost Desktop]# cd ~                                # Switch to the home directory of the user. ~ indicates the home directory of the current user.

[root@localhost ~]# pwd
/root
```


- The **cd** command is used to change the current working directory.
- Syntax: **cd** *[directory]*
  - **cd /usr**: goes to the **/usr** directory.
  - **cd ..**: goes to the upper-level directory. Double dot indicates the upper-level directory.
  - **cd.**: goes to the current directory.
  - **cd**: goes to the home directory by default if no parameter is added.
  - **cd -**: goes to the previous directory. This command is used to quickly switch between two directories.
  - **cd ~**: goes to the home directory.

Viewing Files

- **ls**: Viewing the content of a directory.

```
[root@localhost ~]# ls –a                                    # List all files and directories.
ifcfg-lo      ifdown-eth   ifdown-isdn   ifdown-routes
[root@localhost ~]# ls –l                                    # Display detailed information about types, permissions,
                                                               owners, and sizes of the files.
total 228
-rw-r-----  1 root root    86 Jun 15  19:03 ifcfg-eth0
-rw-r-----  1 root root   254 Jun 15  19:03 ifcfg-lo
```

- **cat**, **tail**, or **head**: Viewing the content of a common file.

```
[root@localhost ~]# cat ifcfg-eth0                  # View all contents of the file.
DEVICE="eth0"
BOOTPROTO="dhcp"
ONBOOT="yes"
TYPE="Ethernet"
PERSISTENT_DHCLIENT="yes"
[root@localhost ~]# tail -2 ifcfg-eth0              # View the last two lines of the file.
TYPE="Ethernet"
PERSISTENT_DHCLIENT="yes"
[root@localhost ~]# head -2 ifcfg-eth0              # View the first two lines of the file.
DEVICE="eth0"
BOOTPROTO="dhcp"
```


- The **ls** command is used to view contents of a directory.
  - **-a**: lists all files including hidden files.
  - **-l**: displays file details in long format.
  - **-R**: lists files in the subdirectories recursively.
  - **-t**: lists files by modification time.
- The **cat** command is used to view contents of a small file. This command displays all lines in a file.
- The **tail** command is used to view the last 10 lines of a file by default.
  - **-n**: followed by a number, for example, 5, indicating that the last five lines of a file are viewed. You can also enter a number directly without the **-n** option.
  - **-f**: dynamically displays file changes. This option is commonly used for viewing log files.
- The **head** command is used to view the first 10 lines of a file by default.
- The **less** and **more** commands are used to view large files page by page. Enter **q** to exit. Enter a slash (**/**) and a keyword to search for the keyword in the file.

Creating Files

- **mkdir**: Creating directories (folders)
  - **-p**: cascades to create multiple directories recursively.

```
[root@localhost ~]# mkdir my_dir_01                    # Create a my_dir_01 directory.
[root@localhost ~]# ls
anaconda-ks.cfg  my_dir_01
[root@localhost ~]# mkdir -p my_dir_02/sub_dir         # Create a my_dir_02 directory and its subdirectory sub_dir.
```

- **touch**: Creating common files.

```
[root@localhost ~]# touch test01.log test02.log        # Create files test01.log and test02.log.
[root@localhost ~]# ls -lt
total 0
-rw-------. 1 root root 0 Jul 29 15:06 test01.log
-rw-------. 1 root root 0 Jul 29 15:06 test02.log
```

Copying Files

- **cp**: Copying files or directories
  - **-a**: copies the files of a directory while retaining the links and file attributes.
  - **-r**: If the source file is a directory, all subdirectories and files in the directories are copied recursively and the attributes are retained.

```
[root@localhost ~]# ls
test01.log  test02.log
[root@localhost ~]# cp /etc/passwd passwd.back              # Copy the /etc/passwd file to the current directory and rename the
                                                              file to passwd.back.
[root@localhost ~]# cp -r /var/log/audit ./                 # Copy the audit directory and all files in it to the current directory.
[root@localhost ~]# ls
audit  passwd.back  test01.log  test02.log
[root@localhost ~]# cp -s /etc/passwd passwd_link           # Create a symbolic link passwd_link of the passwd file.
[root@localhost ~]# ls
audit  passwd.back  passwd_link  test01.log  test02.log
[root@localhost ~]# ls -l
total 8
drwx------. 2 root root 4096 Jul 29 15:24 audit
-rw-------. 1 root root 2546 Jul 29 15:24 passwd.back
lrwxrwxrwx. 1 root root   11 Jul 29 15:25 passwd_link -> /etc/passwd
-rw-------. 1 root root    0 Jan 2 19:20 test01.log
-rw-------. 1 root root    0 Jul 29 19:20 test02.log
[root@localhost ~]#
```


- The **cp** command is used to copy files and directories. You can copy one or more files at a time. Exercise caution when running this command because data loss risks are involved.
- Syntax: **cp** *[OPTION]... SOURCE... DIRECTORY*
  - **-a**: copies the files of a directory while retaining the links and file attributes.
  - **-p**: copies the file content, modification time, and access permissions to the new file.
  - **-r**: if the source file is a directory, all subdirectories and files in the directories are copied recursively.
  - **-l**: creates a hard link of the source file instead of copying it.
  - **-s**: creates a soft link of the source file instead of copying it.
- **cp f1 f2**: copies file f1 and renames it to f2.
- **cp f1 d1/**: copies f1 to the d1 directory without renaming it.
- **cp f1 f2 f3 d1/**: copies multiple files to a directory.
- **cp -i f1 f2**: waits for the user's confirmation before overwriting f2 if f2 already exists.
- **cp -r d1 d2**: copies a directory recursively if the **-r** option is added.
- **cp -a f1 f2**: if the **-a** option is added, the attributes of the source file are retained. This option is used to copy block devices, character devices, and named pipes.
- By default, the **cp** command does not ask the user before overwriting files. Therefore, many shells have made **cp** as an alias for **cp -i**. The **-f** option in the **cp** command does not indicate forcible overwriting.

Moving and Renaming Files

- **mv**: Moving or renaming a file
  - The **mv** command is used to move a file or directory. Exercise caution when running this command because data loss risks are involved.
  - If the source file and target file are in the same directory, the **mv** command is used to rename the file.

```
[root@localhost ~]# ls
passwd_link  test01.log  test02.log
[root@localhost ~]# mv test02.log test03.log      #Change the name of the test02.log file to test03.log
[root@localhost ~]# ls
passwd_link  test01.log  test03.log
[root@localhost ~]# mv test01.log /root/test      # Move the test01.log file to the /root/test directory.
[root@localhost ~]# mv –f test01.log test03.log  # Forcibly overwrite the test03.log file with the content of
                                                    the test01.log file.
```


- The **mv** command is used to move a file or directory. Exercise caution when running this command because data loss risks are involved.
- If the source file and target file are in the same directory, the **mv** command renames the file.
- Syntax: **mv** *[option] source_file_or_directory target_file_or_directory*
  - **-b**: backs up a file before overwriting it.
  - **-f**: forcibly overwrites the target file without asking the user.
  - **-i**: overwrites the target file after obtaining the user's consent.
  - **-u**: updates the target file only when the source file is newer than the target.

Deleting Files

- **rm**: Deleting files or directories
  - The **rm** command is a high-risk command. No tool can guarantee recovery of files deleted by the **rm** command, which does not move a file to a recycle bin like in GUIs. Therefore, you cannot undo the deletion.

```
[root@localhost ~]# ls
audit_back  passwd.back test01.log  test03.log
[root@localhost ~]# rm test01.log                    # Delete the test01.log file with a prompt
                                                       before deletion.
rm: remove regular empty file 'test01.log'? yes
[root@localhost ~]# rm -rf test03.log                # Forcibly delete the test03.log file.
[root@localhost ~]# rm -rf audit_back/               # Delete the mail.bak directory, including all
                                                       files and subdirectories in it.
[root@localhost ~]# ls
passwd.back
[root@localhost ~]#
```

Obtaining Help Information About a Command

- **help**: Obtaining simple help information about a command.
  - To navigate the massive number of commands on Linux, you can run the **help** command to obtain help information.
  - Syntax: *[command]* **--help** or **help** *[command]*.

```
[root@localhost ~]# help pwd
pwd: pwd [-LP]
    Print the name of the current working directory.
    Options:
      -L        print the value of $PWD if it names the current working directory
      -P        print the physical directory, without any symbolic links

    By default, `pwd' behaves as if `-L' were specified.

    Exit Status:
    Returns 0 unless an invalid option is given or the current directory cannot be read.
[root@localhost ~]# systemctl  --help
systemctl [OPTIONS...] {COMMAND} ...

Query or send control commands to the systemd manager.

  -h --help           Show this help
     --version        Show package version
     --system         Connect to system manager
  -H --host=[USER@]HOST.....
```

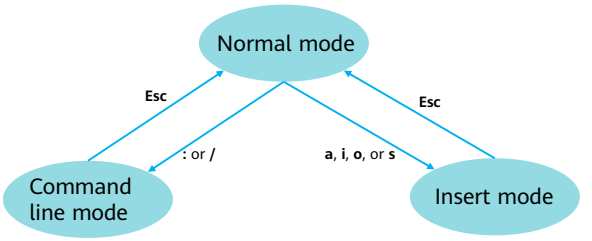
Contents

Basic openEuler Operations

- Basic Knowledge of Linux Commands
- Basic openEuler Commands
- Text Processing on openEuler
- Network Management on openEuler

Linux Text Editor - Vim

- Vim is a customizable text editor derived from Visual Editor (vi) that inherits, improves and adds many features to vi's original base.
- Common Vim modes:
  - Normal mode: used to copy, paste, and delete text, undo previous operations, and navigate the cursor.
  - Insert mode: used to edit and modify text.
  - Command line mode: used to save, exit, search for, or replace text. Enter a colon (**:**) to switch to this mode.



HUAWEI

- Vim is not installed on openEuler 20.03 LTS by default. You need to manually install it.

Normal Mode of Vim

- By default, Vim begins to run in normal mode after you open a file with the **vim** command.

```
vim  [options]  [file]...          Edit specified files.
vim  [options]  -                  Read text from standard input (stdin).
vim  [options]  -t  tag            Edit the file where the tag is defined.
vim  [options]  -q [errorfile]     Edit the file where the first error occurs.
```

- Common options:
  - **-c**: runs a specified command before opening a file.
  - **-R**: opens a file in read-only mode but allows you to forcibly save the file.
  - **-M**: opens a file in read-only mode and does not allow you to forcibly save the file.
  - **-r**: recovers a crashed session.
  - **+***num*: starts at line *num*.

Common Operations in Vim Normal Mode

- Cursor control
  - Arrow keys or **k**, **j**, **h**, and **l** keys move the cursor up, down, left, and right, respectively.
  - **0**: moves the cursor to the beginning of the current line.
  - **g0**: moves the cursor to the leftmost character of the current line that is on the screen.
  - **:***n*: moves the cursor to line *n*.
  - **gg**: moves the cursor to the first line of the file.
  - **G**: moves the cursor to the last line of the file.
- Data operations
  - **yy** or **Y**: copies an entire line of text.
  - **y***[n]***w**: copies 1 or *n* words.
  - **d***[n]***w**: deletes (cuts) 1 or *n* words.
  - *[n]* **dd**: deletes (cuts) 1 or *n* lines.

Insert Mode of Vim

- Use the **vim** *filename* command to open a file and enter the normal mode by default. Type **i**, **I**, **a**, **A**, **o**, or **O** to enter the insert mode.
- If the *filename* file exists, the file is opened and the file content is displayed; otherwise, Vim displays **[New File]** at the bottom of the screen and creates the file when saving the file for the first time.
- Press **Esc** to exit the insert mode and return to the normal mode.

```
[root@openEuler ~]# vim  test.txt                    # Enter the normal mode by default.
~
~
"test.txt" [New File]
[root@openEuler ~]# vim  test.txt                    # Press i, I, a, A, o, or O to enter the insert mode.
~
~
-- INSERT --
```

Command Line Mode of Vim

- Search
  - **:/***word* **or /***word*: searches for a *word* string after the cursor. Press **n** to continue to search forwards or press **Shift+n** to search backwards.
- Replace
  - **:1,5s/***word1***/***word2***/g**: replaces all occurrences of *word1* in lines 1 to 5 with *word2*. If **g** is not specified, only the first occurrence of *word1* in each line is replaced.
  - **%s/***word1***/***word2***/gi**: replaces all occurrences of *word1* with *word2*. **i** ignores the case of matches.
- Save and exit
  - **:w**: Save the file and do not exit.
  - **:wq**: Save the file and exit.
  - **:q**: Exit without saving the file.
  - **:q!**: Exit forcibly without saving changes to the file.
  - **:wq!**: Forcibly save the file and exit.

Contents

Basic openEuler Operations

- Basic Knowledge of Linux Commands
- Basic openEuler Commands
- Text Processing on openEuler
- Network Management on openEuler

Important Network Concepts in openEuler

- **Host network device**: a network adapter on the host.
- **Interface**
  - Interfaces on devices are created by drivers for the system access.
- **Broadcast address**
  - An IP address used to send packets to all hosts on the network segment
- **Subnet mask**
  - A number that distinguishes the network address and the host address within an IP address
- **Route**
  - Next-hop IP address when IP packets are transmitted across network segments
- **Link**: connection between the device and the network.

Commands for Querying IP Addresses

- **ip** and **ifconfig** commands are used to view IP addresses of the current host.
- Viewing information about all network adapters on a host.

```
[root@openEuler ~]# ifconfig –a
[root@openEuler ~]# ip addr show
```

- Viewing information about a specified interface on a host.

```
[root@openEuler ~]# ifconfig enp0s3
[root@openEuler ~]# ip addr show enp0s3
```


- Viewing the current IP addresses and subnet masks of all interfaces: **ip addr**

Configuring Static IP Addresses Using Network Adapter Configuration Files

- Query the path of the network adapter configuration file:

```
[root@openEuler ~]# ls /etc/sysconfig/network-scripts/ifcfg-*
/etc/sysconfig/network-scripts/ifcfg-enp0s3  /etc/sysconfig/network-scripts/ifcfg-enp0s8
```

- Parameter description:

Parameter	Description
TYPE	Interface type
BOOTPROTO	Boot-time protocol
ONBOOT	Whether to activate the device at boot-time
IPADDR	IP address
NETMASK	Subnet mask
GATEWAY	Gateway address
BROADCAST	Broadcast address
HWADDR/MACADDR	MAC address. Only one MAC address needs to be set. New MAC addresses cannot share the same name as another when they are set at the same time.
PEERDNS	Whether to specify the DNS server address. If the DHCP protocol is used, the default value is yes.
DNS{1, 2}	DNS server addresses
USERCTL	User permission control
NAME	Network connection name
DEVICE	Physical interface name

Configuring the IP Address - Configuration File Example

- Set the static IP address of the enp0s3 interface to **192.168.56.100/24**.

```
TYPE=Ethernet
BOOTPROTO=static
NAME=enp0s3
DEVICE=enp0s3
ONBOOT=yes
IPADDR=192.168.56.100
NETMASK=255.255.255.0
```

- Restart the network.

```
[root@openEuler ~]# nmcli connection reload enp0s3
[root@openEuler ~]# nmcli connection up enp0s3
Connection successfully activated (D-Bus active path: /org/freedesktop/NetworkManager/ActiveConnection/12)
```


- Sometimes, too many configuration items increase the difficulty of network troubleshooting.

Configuring the Static IP Address Using the nmcli Command

- Check network connections of the current host.

```
[root@openEuler ~]# nmcli connection show
NAME    UUID                                  TYPE      DEVICE
enp0s3  3c36b8c2-334b-57c7-91b6-4401f3489c69  ethernet  enp0s3
enp0s8  00cb8299-feb9-55b6-a378-3fdc720e0bc6  ethernet  enp0s8
```

- Configure a static IP address.

```
[root@openEuler ~]# nmcli connection modify enp0s3 ipv4.method manual ipv4.addresses "10.0.2.10/24" ipv4.gateway "10.0.2.2"
```

- Restart the network.

```
[root@openEuler network-scripts]# nmcli connection reload enp0s3
[root@openEuler network-scripts]# nmcli connection up enp0s3
Connection successfully activated (D-Bus active path: /org/freedesktop/NetworkManager/ActiveConnection/18)
```

- View the IP address.

```
[root@openEuler ~]# ip addr show enp0s3
2: enp0s3: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc fq_codel state UP group default qlen 1000
    link/ether 08:00:27:7d:e1:a5 brd ff:ff:ff:ff:ff:ff
    inet 10.0.2.10/24 brd 10.0.2.255 scope global noprefixroute enp0s3
       valid_lft forever preferred_lft forever
```


- **conn**: indicates that an operation is to be performed on a connection.
- **add**: adds (a connection)
- **type**: type of the connection
- **con-name**: connection name
- **<ifname>**: name of the network adapter
- **mod**: modifies (a connection)

Introduction to Routes

- To facilitate communication between two hosts in different subnets, a mechanism is required to describe the path for traffic. This mechanism is called routing, which is set using routing entries.
- A routing entry is a pair of predefined addresses, including the destination and gateway. It indicates a gateway through which the destination can be reached.
- The routing table is a collection of routing entries.

- Detailed description of routes: https://docs.freebsd.org/en/books/handbook/advanced-networking/#network-routing

Route Management and Configuration

- In openEuler, the **route** command is used to view, configure, and manage local routes.
- In addition to the **route** command, the **ip** command can also be used to manage system routes.
- These commands will modify the routing table of the system. When the system is started, the routing table is loaded to the memory and maintained by the kernel.

- The **route**, **ip**, and **nmcli** commands can be used to manage routes. The following uses the **route** command as an example.

Viewing the Routing Table Using the route Command

- Run the **route** command to view the routing table.

```
[root@openEuler ~]# route -n
Kernel IP routing table
Destination     Gateway         Genmask         Flags Metric Ref    Use Iface
0.0.0.0         192.168.110.254 0.0.0.0         UG    100    0        0 enp4s0
192.168.110.0   0.0.0.0         255.255.255.0   U     100    0        0 enp4s0
192.168.122.0   0.0.0.0         255.255.255.0   U     0      0        0 virbr0
```


- When the **-n** option is used to display routes, the values in the **Destination** column are IP addresses.
- Eight fields are displayed when you run the route command to view routes. The possible values of the **Flags** field include:
  - **U** (up) indicates that the route is up.
  - **H** (host) indicates that the gateway is a host.
  - **G** (gateway) indicates that the gateway is a router.
  - **R** (reinstate) indicates that the route is reinstated for dynamic routing.
  - **D** (dynamically) indicates that the route is dynamically written.
  - **M** (modified) indicates that the route is dynamically modified by the routing daemon or redirect.
  - **!** indicates that the route is closed.

Adding a Route Using the route Command

- Add a (temporary) route to a network segment or host.

```
route [-f] [-p] [Command [Destination] [mask Netmask] [Gateway] [metric Metric]] [if Interface]]
```

- Example:

```
[root@openEuler ~]# route add -net 192.168.101.0 netmask 255.255.255.0 dev enp4s0
[root@openEuler ~]# route add -host 192.168.100.10 dev enp4s0
[root@openEuler ~]# route
Kernel IP routing table
Destination     Gateway         Genmask         Flags Metric Ref    Use Iface
default         _gateway        0.0.0.0         UG    100    0        0 enp4s0
192.168.100.10  0.0.0.0         255.255.255.255 UH    0      0        0 enp4s0
192.168.101.0   0.0.0.0         255.255.255.0   U     0      0        0 enp4s0
192.168.110.0   0.0.0.0         255.255.255.0   U     100    0        0 enp4s0
192.168.122.0   0.0.0.0         255.255.255.0   U     0      0        0 virbr0
```


- You can use the **route** command to add routes. The added routes are stored in the memory and become invalid after the system is restarted.
- The **route add -net 192.168.101.0 netmask 255.255.255.0 dev enp3s0** command adds a route to the 192.168.101.0/24 segment through the enp3s0 device.
- The **route add -host 192.168.101.100 dev enp3s0** command adds a route to the 192.168.101.100 host through the enp3s0 device.
- The output of the **route** command shows that routes to hosts have a higher priority than routes to network segments.

Deleting a Route Using the route Command

- Deleting a route to a network segment or host using the **route del** command.
- Syntax:

```
route del [-net|-host] [netmask Nm] [gw Gw] [[dev] If]
```

- Example:

```
[root@openEuler ~]# route del -host 192.168.100.10 dev enp4s0
[root@openEuler ~]# route
Kernel IP routing table
Destination     Gateway         Genmask         Flags Metric Ref    Use Iface
default         _gateway        0.0.0.0         UG    100    0        0 enp4s0
192.168.101.0   0.0.0.0         255.255.255.0   U     0      0        0 enp4s0
192.168.110.0   0.0.0.0         255.255.255.0   U     100    0        0 enp4s0
192.168.122.0   0.0.0.0         255.255.255.0   U     0      0        0 virbr0
```


- The **route del -net 192.168.101.0 netmask 255.255.255.0 dev enp3s0** command deletes the route to the 192.168.101.0/24 segment. To delete a route to a network segment, the network segment and subnet mask parameters are mandatory, while the device parameter is optional.
- The **route del -host 192.168.101.100 dev enp3s0** command deletes the route to the 192.168.101.100 host. The device parameter is optional.
- To delete routes in the **route** file, use the vi editor to edit the file and restart the network.

Host Name

- A host name identifies a device in a local area network (LAN).
- The device can be a physical or virtual machine.
- The host name is stored in the **/etc/hostname** file.

```
[root@openEuler ~]# cat /etc/hostname
openEuler
```

Setting the Host Name

- Setting a temporary host name: **hostname new-name**
- Setting a permanent host name: **hostnamectl set-hostname new-name**
- Setting a host name by modifying the file: write **new-name** to the **/etc/hostname** file.

```
[root@openEuler ~]# hostname
openEuler
[root@openEuler ~]# hostname huawei
[root@openEuler ~]# hostname
huawei
[root@openEuler ~]# hostnamectl set-hostname openEuler01
[root@openEuler ~]# hostname
openEuler01
[root@openEuler ~]# echo "HCIA-openEuler" > /etc/hostname
```


- To make the setting take effect, log in again or run the **source .bashrc** command.
- Run the **hostname** command to view the host name of the current system.

Introduction to the hosts File

- Hosts in a LAN can be accessed through IP addresses.
- IP addresses are difficult to remember when a large number of hosts exist in the LAN. Therefore, we want to access the hosts directly through their host names.
- In this case, the hosts can be located using a table that records the mapping between host names and IP addresses. This table is the **hosts** file.

```
[root@openEuler ~]# cat /etc/hosts
127.0.0.1   localhost       localhost.localdomain       localhost4      localhost4.localdomain4
::1         localhost       localhost.localdomain       localhost6      localhost4.localdomain6
```


- The **hosts** file is a system file without a file name extension. Its basic function is to establish a "database" of frequently used domain names and their corresponding IP addresses.
- When a user enters a website URL in the web browser, the system searches for the corresponding IP address in the **hosts** file. Once the IP address is found, the system opens the corresponding web page.
- If the URL is not found, the system sends the URL to the DNS server for IP address resolution.
- Run the **cat /etc/hosts** command to view the **hosts** file.

Modifying the hosts File

- You can edit the **hosts** file in the following format:

```
# Ip domain.com
192.168.10.20     www.example.com
```

- To delete an entry, add **#** to comment it out. For example:

```
#ip domain.com
#192.168.10.20     www.example.com
```

Quiz

1. Which of the following statements is incorrect about file systems?
   A. A file system is a method and a data structure used by an OS to identify files on a storage device or a partition.
   B. The software structure that manages and stores file data is referred to as a file management system.
   C. The file system manages and controls computer hardware and software resources.
   D. The file system organizes and allocates the space on file storage devices, stores files, and protects and retrieves the stored files.
2. Linux is a multi-user OS that allows multiple users to log in at the same time and allows one user to log in multiple times.
   A. True
   B. False

- Answer:
  - C
  - A

Summary

- This course discusses the basic components and types of OSs and basic operations of Linux. Now, we have finished learning the basics about computing, storage, network, and OS technologies. In cloud computing, how can we use and manage the resources to provide services for applications? We will address these issues in the next course about virtualization technology.

Recommendations

- Huawei iLearning
  - https://e.huawei.com/en/talent/portal/#/
- Huawei Support Knowledge Base
  - https://support.huawei.com/enterprise/en/knowledge?lang=en

Acronyms and Abbreviations

- CLI: Command Line Interface
- GUI: Graphical User Interface
- POSIX: Portable Operating System Interface

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.