Table of Contents

C1.1: Introduction to IT Infrastructure

IT infrastructures become more complicated due to new types of applications:

- Mobile computing - Cloud computing - Big data - Artificial Intelligence - Internet of Things
- **Streetlights (IoT)** are equipped with sensors that detect traffic flow & send data to a cloud-based system. - **Big data** techniques are used to identify traffic patterns & predict congestion. - An **AI algorithm** automatically adjusts the timing of the streetlights to optimize traffic flow or alert drivers about potential delays. - A **mobile app** allows citizens to access real-time traffic information & adjust their routes accordingly.

Agile adaptations requires infrastructures:

Solid	- Loosely coupled (min dependency) - Highly cohesive (max relationship)
Scalable	- Ability to handle increased load without performance degradation
Modular	- Smaller, independent & reusable components / modules

IT Infrastructure

Definition Source	**Component**					**Objective**
	Hardware	**Software**	**Network**	**Facilities**	**Services**	
Wikipedia	✅	✅	✅	■	■	As a foundation of an **IT service**
ITIL	✅	✅	✅	✅	■	To **develop**, **test**, **deliver**, **monitor**, **control** or **support** IT services
Techopedia	✅	✅	✅	■	✅	For the **existence**, **operation** and **management** of an enterprise IT environment.

Gartner	✅	✅	■	✅	✅	To **support the delivery** of business systems & IT-enabled processes.
IBM	✅	✅	✅	✅	✅	For the **operation & management** of enterprise IT services and IT environments.

People Point of View

Subject to who & point of view:	**Infrastructure**		
	Business analyst	**End user**	**System manager**
Business process	✅	■	■
Information	✅	■	■
Application	✅	✅	■
Server	✅	✅	✅
Building	✅	✅	✅
Electricity provider	✅	✅	✅

IT Architecture

Definition	Architecture defines purpose, intent & structure of a system
Uses	Architecture is crucial to control the infrastructure when it is: Designed, In use & Changed

Strategy vs Technology Focus

	Enterprise Architects	**Solution Architects**	**Domain Architects**
Strategy focus	High	Moderate	Low
Technology focus	Breadth (wide)	Moderate	Depth
Expert on	Align IT landscape with the business activities	IT solutions, technical & authority of a project	Business technology topic

Work for	Align the business needs with current & future IT	Project architectural decisions	Infrastructure / software vendors
Assists	CIO & business units	Project manager	Solution architects

IT Building Blocks

Management	**Building Block**	**Description**
Functional Management	Process / info	● Business processes implemented to fulfil company's mission and vision ● Business **processes** create & use **information**
Application Management	Application	● Usage ○ Single-user application ○ Multi-user application ● Source ○ Commercial off-the-shelf (COTS) 商用现货 ○ Custom software ● Architecture ○ Standalone applications ○ Multi-tier applications (front-end, API & backend (database)) ● Timeliness ○ Real-time system: timeliness is critical ○ Interactive applications: respond to user actions ○ Batch-based systems: Regular processing
Platform Management	Application platform	● Application servers ○ A server that hosts applications or software ● Container platforms ○ A software solution that enables the management of containerized applications 能够管理容器化应用程序的软件解

		决方案 ● Connectivity ○ Application server to database ○ Application server to container platform ○ Databases in container ● Databases ○ Provides ways to store & retrieve data
Infrastructure Management Processes: ● Information Technology Infrastructure Library (ITIL) ● Control Objectives for Information and Related Technology (COBIT) ● DevOps Tools are used for: ● Monitoring ● Backup ● Logging	End user devices	Devices used by end users to work with applications: ● PCs ● Laptops ● Thin clients ● Mobile devices ● Printers
	Operating systems	A collection of programs that manage a computer's internal workings: ● Memory ● Processors ● Devices ● File system
	Compute	Physical & virtual computers in the datacenter
	Storage	Storage are systems that store data: ● Hard disks ● Tapes ● Direct Attached Storage (DAS) ● Storage Area Networks (SANs)
	Networking	Networking connects all components: ● Routers ● Switches ● Firewalls ● WAN ● LAN ● Internet access ● VPNs Includes infrastructure services: ● DNS

		● DHCP ● Time services
	Datacenters	Datacenters hosts most IT infrastructure hardware ● Uninterruptible power supplies (UPSs) ● Heating, Ventilations and Air Conditioning (HVAC) ● Computer racks ● Physical security measures

C1.2: Introduction to IT Infrastructure

Cloud Computing

Definition	Cloud computing is a **number of datacenters** that are still filled with hardware (compute, networking and storage)
Objective	Enables **ubiquitous** 随处可见, **convenient**, **on-demand** network access to a **shared pool** of **computing resources** for **rapid** provision & release with **minimal** management **effort** / service provider **interaction**
Datacenters	● On premises ● On cloud ● On hybrid mode: premises + cloud
Model	● Outsourcing. To cut cost while focusing on core business
Popular public cloud providers	● Amazon Web Services (AWS) ● Microsoft Azure ● Google Cloud Platform (GCP)

Cloud Characteristics

On demand self-service	● Min systems **management** effort is needed for deployment ● End users can configure, deploy, start & stop systems **on demand**
Rapid Elasticity	● Able to **quickly scale-up** & **scale-down** resources
Resource Pooling	● Provides **resources** from a **shared pool** (using virtualization technologies)
Measured service	● The actual resource usage is **measured** and **billed** ● There are **no capital expenses** 资本支出, **only operational expenses**
Broad network access	● Capabilities are **available** over the network

Cloud Deployment Models

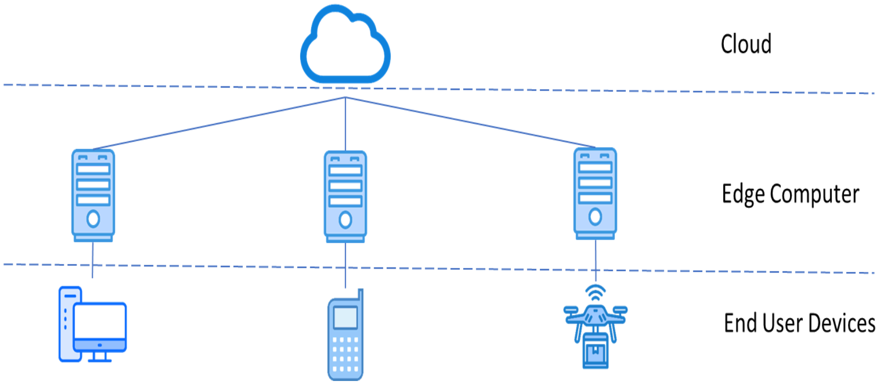
	Owned, managed and	**Uses**	**Pros**

	operated by		
Public cloud	Cloud service **provider** & **public**	**Internet**	**Economies** of scale (Lower cost due to shared infrastructure)
Private cloud	**Single** organizations / a **third-party**	**Virtualization** & **standardisation**	**Reduce** systems management **cost** & **staff**
Community cloud	**One** / **more** of the parties in the community / **third party**	For communities with **shared concerns**	
Hybrid cloud	**Public** + **community cloud** private cloud	**Public**: Run generic services (email servers) **Private**: Host specialized services (specific apps)	

Cloud Service Models

Software-as-a-Service (SaaS)	Consume	**Application** Building Block	● Delivers **full applications** ● **Little** / **no configuration** needed ● e.g.: Microsoft Office365, LinkedIn
Platform-as-a-Service (PaaS)	Build	**Application Platform** Building block	● Delivers a **scalable**, **high available**, open programming **platform** ● Used by developers to **build applications** ● e.g.: Microsoft Azure Cloud Service, Google App Engine
Infrastructure-as-a-Service (IaaS)	Host	**Infrastructure** Building Block	● Delivers **virtual machines**, **networking** & **storage** ● **Needs to install and maintain the OSs** & the layers above that ● e.g.: Amazon Elastic Cloud (EC2 and S3) and Microsoft Azure IaaS

Edge Computing

<table>
<tr><td colspan="2">
</td></tr>
<tr><td><b>Definition</b></td><td>Brings <b>computing power</b> and <b>data storage closer</b> to where it is needed</td></tr>
<tr><td><b>Objective</b></td><td><b>Min cloud / on-premises datacenter access</b></td></tr>
<tr><td><b>Components</b></td><td>Routers, gateways, switches & sensors</td></tr>
<tr><td><b>Pros</b></td><td>● <b>Low latency</b>
● <b>Low bandwidth needs</b>
● <b>Real-time processing</b></td></tr>
<tr><td><b>Application</b></td><td><b>IoT applications</b> (a large number of devices generate data to be processed in real time)</td></tr>
</table>

C2: Introduction to Non-Functional Attributes

Non-Functional Attributes

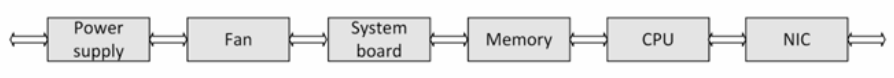
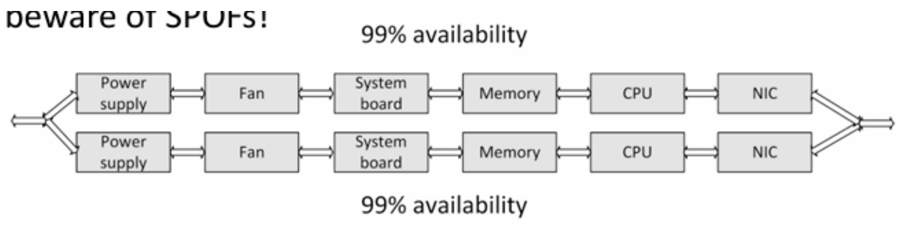
Purpose	- To describe the **qualitative behavior of a system** - For the **successful implementation, use & acceptance** of an IT infrastructure
A.k.a.	Non-functional requirements or NFRs
Delivered by	Infrastructure
Components	- **Availability** - **Performance** - **Security**
Conflicts	- Security vs User friendliness - Performance vs Cost

Availability

Definition	Uptime / ability to provide products or services without interruption / downtime
Measured by	Expressed as a percentage of uptime (in one year / one month basis)
Characteristics	Cannot be guaranteed upfront
Carrier grade availability	- 99.999% uptime (for one component) - For a full IT system: 99.8% or 99.9% (per month) - For the IT infrastructure: 99.99% or higher

Availability Calculations

Metrics to measures availability - **Mean Time Between Failures (MTBF)** → Uptime - **Mean Time to Repair (MTTR)** → Downtime	
Single Component	One defect leads to downtime $Availability = \frac{MTBF}{MTBF+MTTR} \times 100\%$

Serial Components	 One defect leads to downtime $Total\ Availability = Availability \times Availability$
Parallel Components	 beware of SPOFs! 99% availability Power supply Fan System board Memory CPU NIC Power supply Fan System board Memory CPU NIC 99% availability One defect leads to no downtime but beware of Single Point of Failures (SPOFs) $Total\ Availability = 1 - (1 - Availability) \times (1 - Availability)$

Preventions and Recovery

Minimize MTTR / downtime	1. Having a **service contract with the supplier** 2. Having **spare parts on-site** 3. Automated **redundancy** & **failover**
Steps to complete repairs	1. **Notification** of the fault (time before seeing an alarm message) 2. **Processing the alarm** 3. Finding the **root cause** of the error 4. Looking up **repair information** 5. Getting **spare components** from storage 6. Having **technician** come to the datacenter with the spare component 7. Physically **repairing** the fault 8. **Restarting** & **testing** the component

Sources of Unavailability

- **Human errors** (accident)
- **Software bugs** (software complexity)
- **Planned maintenance** (upgrade, migration, changes)
- **Physical defects** (mechanical part likely to break first)
- **Bathtub curve** (new component likely to fail)

- **Environmental issues** (failing facilities, disaster)
- **Complexity** of the infrastructure (complex system)

Achieving High Availability

Redundancy

- **Duplication** of critical components in a single system
- e.g. A single component having 2 power supplies

Failover

- A (semi) **automatic switch-over** to a standby system from the **same** location
- e.g. Windows Server failover clustering

Fallback

- **Manual switchover** to an identical standby computer system in a **different** location
- Used for: Disaster recovery
- Solutions:

	Hot Site	**Cold Site**	**Warm Site**
Hardware, Power & Cooling	Fully equipped & configured	Hardware (Basic infrastructure only, need full setup)	Ready (partial equipped site, requires some setup)
Application	Installed on servers	Needs to be installed	Not be installed
Data kept	● Up-to-date ● For full mirror	● Current data ● Restored from backup	● Need to restore ● Restored from backup
Pros	Accurately mirrors	Low cost	Hot + cold site
Cons	Requires constant maintenance	Least preference method	Testing needed. Slow.

Availability in the Cloud

Regions & Availability Zones

	Regions	Availability Zone
Definition	A **geographically defined area** that contains multiple Availability Zones.	A physically **isolated location** within a Region.
Scope	**Broader**	**Localized** within region
To maintain availability	**Fallback**	Local **failover** (using **update** & **fault domains**)

Fault & Update Domains

	Fault Domains	Update Domains
Definition	A group of virtual machines that share a common power source and network switch	A group of virtual machines that can be rebooted during planned maintenance
Protection against	Hardware and infrastructure failures	Downtime during planned maintenance and updates
Example	When a fault domain fails (e.g. rack outage), VMs within that domain are affected, but VMs in other fault domains remain online.	When an update domain is rebooted, it's given a recovery time (e.g. 30 minutes) before the next update domain is affected

Business Continuity

IT Disaster

Definition	An irreparable problem in a datacenter due to unusable	
Types	Natural disaster	● Floods ● Hurricanes ● Tornadoes ● Earthquakes
	Man-made disaster	● Hazardous material spills ● Infrastructure failure ● Bio-terrorism
Impact	Infrastructure become unavailable	
Solutions	Business Continuity Management	● IT ● Managing business processes

	(BCM)	● Availability of people and workplaces in disaster situations
	Disaster Recovery Plan (DRP)	● A set of measures to take if disaster ● To accommodate the IT infrastructure in an alternative location

RTO & RPO

RTO and RPO are critical components of BCM and DRP	
RTO	● **Recovery Time Objective** (RTO) ● The **maximum duration to be restored after a disaster** ● To avoid unacceptable consequences ● A **shorter RTO** implies a **faster recovery** and often **requires more resources**
RPO	● **Recovery Point Objective** (RPO) ● The **point (in time) to which data must be recovered considering some "acceptable loss" in a disaster situation** ● A **lower RPO** means **less data loss** and usually **requires more frequent backup**

Performance

Definition	Perceived performance refers to how quickly a system appears to perform its task
Indicator	Inform the user about how long a task will take, using progress bars, splash screens

Performance Calculation

Performance during infrastructure design phase

Nature	● Complexity ● Extremely difficult ● Unreliable
Considerations	● When the system works as expected → normal ● When the system is in a special state (e.g. failing parts, maintenance state, performing backup and running batch job)

Evaluation	Benchmark	Definition	● Uses a test program to assess the relative performance of an infrastructure component
		Scope	● Performance of various subsystems ● Across different system architectures
		Example	Compare the raw speed of parts of an infrastructure (processor)
	Vendor experience	● Vendors have experience running their products in various configurations ● Vendors can provide: Tools, Figures & Best practices	
	Prototype	A.k.a.	Proof of concept (PoC)
		Aim	To measure the performance of a system at an early stage, for part with highest risk
		How	● Hiring equipment from suppliers ● Using datacenter capacity at a vendor's premise ● Using cloud computing resources
	User Profiling	Definition	Predict the load a new software system to the infrastructure before the software is actually built to get expected usage of the system
		How	1. Define a number of typical user groups 2. Create a list of tasks personas will perform on the new system 3. Decompose tasks to infrastructure actions 4. Estimate the load per infrastructure action 5. Calculate the total load
How	Scalable cloud environment ● In cloud environments, it offers rapidly elasticity ● Cloud environments have extensive logging and monitoring capabilities		

Performance of a running system

Manage bottleneck	Definition	● A component causing the system to **reach limit**, that **negatively influence performance** ● **Every system** has **at least 1 bottleneck** that limits its

		performance - If the bottleneck has no negative impact to performance of the system under the highest expected load, it is OK
	Based on	- The **performance of all its components** - The **interoperability of various components**
Performance test	Types	- **Load test**: Shows how a system performs under the expected load - **Stress test**: Shows how a system reacts when it is under extreme load - **Endurance test**: Shows how a system behaves when it is used at the expected load for a long period of time
	Breakpoint	- How: Ramp up / increase the load 提升/增加负载 - Ideal using: **Cloud** environment, due to: ○ Rapidly **elasticity** ○ Reduce the **cost** ○ **Simulating** a very large number of users
	Software	One or more servers to act as injectors - Each **emulating** a number of users - Each **running** a sequence of interactions A test conductor - **Coordinating** tasks - **Gathering** metrics from each of the injectors - **Collecting** performance data for reporting purposes
	Where	- **Production-like** environment (for reliability) - **Temporary (hired) test** environment (for min cost)

Performance Patterns (to improve performance)

Increase upper layer	Working	● Database & application tuning ● Prioritizing tasks ● Working from memory than disk ● Making good use of queues and schedulers
Disk caching	Components	● Disk ● Disk controllers ● Operating system
	Working	Stores all / same data recently read from disk
Web proxies	Definition	A web proxy server is a type of cache
	Working	Earlier accessed data can be fetched from cache, instead of from the internet
	Pros	● Faster ● More bandwidth for use (due to no download needed)
Operational Data Stores (ODS)	Definition	A database designed to consolidate and integrate current operational data from various sources 数据库旨在合并和整合各种来源的当前运行数据
	Pros	● Real time access to operational transactions ● The main database is used less for retrieving info, no degrade
Front-end server	Definition	● A.k.a. Web server ● To serve data to end users
	Pros	● Min traffic, due to store static (picture) data ● Reversed proxy available (auto-cache mort requested data)
In-memory databases	Definition	● The database is run from memory instead of from disk ● Special arrangements must be made to ensure data is not lost when a power failure occurs
	Pros	Ideal for high performance application
Edge server	Working	Edge locations can be used to cache data in close

		proximity to end users
	Ideal for	Cloud providers with datacenter around the world
Scalability	Definition	To ease of a system to modify, to handle increasing load
	Working	Vertical scaling ● Scale up ● Add resources to a single component ● Pros: Easy ● Cons: Quickly reaches a limit ● e.g. Server - Add more memory Horizontal scaling ● Scale out ● Add components to the infrastructure ● Pros: Faster ● Cons: Bottleneck ● Ideal for: Cloud computing ● e.g. Storage system - Add disk cabinets
Load balancing	Definition	Load balancing uses multiple servers that perform identical tasks
	Working	The application running on a load balanced system must be able to be handled by a different server Load balance ● Spreads the load to available machines ● Checks the current load on each server in the farm ● Sends incoming requests to the least busy server Advanced load balancers ● Spread the load based on Server side's number of connections and response time
	Pros	A load balancer increases availability
	Application	● Server load balancer: spread the requests to servers ● Network load balancer: spread network load over connections ● Storage load balancer: spread the load of R & W
High	Definition	Provide a vast amount of computing power by combining

performance cluster		many computer systems
	Working	Combine a large number of off the-shelf servers to create a large supercomputer
	Ideal for	Calculation-intensive systems: Weather forecasts
Grid computing	Definition	A high performance cluster that consists of systems that are spread geographically
	Cons	● Limited bandwidth ● Security concern
Design for use	Tips	● Know the system purpose (online/batch/etc) ● Spread the system load ● Special product for certain system (real-time / in-memory) ● Use standard implementation plan (vendor's plan) ● More rarely used data from main system to other system (speed up processing)
Capacity management	Aims	● Guarantees high performance of a system in the long term ● To ensure performance, performance must be monitored
	Working	● Trend analyses (to predict performance degradation) ● Anticipate on business changes

Security

Definition	Security is the combination of ● Availability: Authorised user has reliable access when needed ● Confidentiality: Sensitive info is accessible by authorized user only ● Integrity: Maintain accuracy & trustworthiness of data
Characteristics	Focused on the recognition and resistance of attacks
Core infrastructure security	● Irreversibility of hash keys ● Practical unbreakable encryption ● Unbreachable virtualization
Reason for crime	● Personal exposure and prestige (visibility / perceivability by

against IT infrastructure	others) ● Creating damage ● Financial gain ● Terrorism ● Warfare	
Cloud security	The public cloud applies a shared responsibility model: ● The cloud provider takes care of security of the cloud, with many specialists ● The customer takes care of security in the cloud	
Prevention	● Design for minimum risk (using source code analysis, standalone system) ● Incorporate safety devices (using firewall, hardened screened routers) ● Implement training & procedures (to mitigate risk, ensure proper use)	
Implementation	Zero trust	Assumes no implicit trust regardless of location & requires continuous verification of users and devices before granting access
	Segregation of duties	Granting users only the minimum necessary access rights to perform their job functions
	Privileged Access Management (PAM)	Manage & monitor access to sensitive resources and privileged accounts
	Layered security	Multiple security controls to protect against different types of threats
	Identity and Access Management (IAM)	Manage user identities & access rights across an organization
	Authentication	Verify the identity of a user or device before granting access
	Password	A secret string of characters used to authenticate a user's identity
	Role Based Access Control (RBAC)	Control access to resources based on user roles
	Cryptography	Secure communication & data by transforming it into an unreadable format, making it incomprehensible to unauthorized

	Encryption	Encode data using algorithm & keys, converting readable information (plaintext) into an unreachable format (ciphertext)
	Computer Emergency Response Team (CERT)	A team that responds to computer security incidents

C3: Datacenters

Definition	Most IT infrastructure hardware, except for end user devices, are hosted in datacenters
Functions	● Power supply ● Cooling ● Fire prevention and detection ● Equipment racks

Datacenter Categories

Datacenter	**Sub Equipment Room (SER)**	**Main Equipment Room (MER)**	**Organization owned datacenter (OOD)**	**Multi-tenant datacenter (MTD)**
Size	Patch closet 配线间 / small room / closet that house networking / electrical equipment	A small datacenter in the organization's subsidiaries 子公司 / buildings	A datacenter that contains all central IT equipment for the organization	Used by service providers that provide services for multiple other organizations
	Smaller (office building)	**Larger** (centralized room)	**Larger** (purpose-built facility)	**Largest** (facility shared by multiple organizations)
Key function	As a distribution point for network connections	Houses core network infrastructure	House an organization's entire IT infrastructure	Host their IT equipment

Locations

Determined by:

- **Environment** of the datacenter
- **Visibility** of the datacenter
- **Utilities** available to the datacenter
- Datacenters located in **foreign countries**

Physical Structure

Floors

Datacenter floor load	Carry 1500 to 2000 kg/m^2 ● A fully filled 19" computer rack: 700 kg ● The footprint of a rack is 60 x 100 cm: 1166 kg/m^2
Office floor load	Carry approximately 500 kg/m^2
Raised floor	● Made of metal framework with removable floor tiles (60 x 60 cm) ● Cons: ○ Expensive ○ Total available height in the datacenter is decreased ○ Maximum floor load is limited ○ Doors and equipment loading slopes are hard to install ○ Fire could easily spread through the entire datacenter ● As alternative, use overhead cable trays
Vents	Provide cool air flow to the racks placed on the floor

Walls, Windows, Doors

Walls	● Reach from the floor to the building's ceiling ● Adequate fire rating 防火等级 is needed to serve as a physical firewall
Windows	● NOT desirable in a datacenter ● If there are windows, they must be: ○ Translucent 半透明 ○ Shatterproof 防碎 ○ Impossible to open
Doors	● Large enough to have equipment and must resist forced entry

Water and Gas Pipes

- Leakage from water pipes in the ceiling could lead to damage of equipment
- Datacenter operators should know where the shutoff values are

Layout of Datacenter

Computer room	The actual IT infrastructure components are installed

UPS generator	A diesel generator provides electrical power in case the utility power input fails. The fuel for the generator should be kept outside of the building or in an isolated room, but also close by and secured
Input Power Transformers	Input transformers from the power utility company
UPS	The Uninterruptible Power Supply system
UPS batteries	A set of batteries providing short term power used in the system
Cooling	The cooling systems
Fire extinction	Fire extinction systems
Operator room	This room has a large window looking into the equipment room to spot unusual activity
Storage room	Store spare hardware and other equipment
Endurance	Entrance room to the other rooms. Does not have windows
Meeting room	For staff meetings and visitor meetings. This room has window to allow direct sunlight, but this window must be secured (shatterproof)

Power Supply

Power Density

The **amount of power available in a datacenter**, kilowatts per m^2	
Power drawn	● 1 rack of servers: kilowatts (kW) ● Large facilities: megawatts (MW) ● Normal-density datacenter: 2 - 6 kW/m^2 ● High-density datacenter: 10 & 20 kW/m^2 (racks filled with 40 - 80 servers)
Server rack	Cannot be fully equipped due to: ● **Suitability & transport** ● **Power & cooling** ● **Accessibility & maintenance** ● **Future expansion** ● **Cable management**

Uninterruptible Power Supply (UPS)

Objective	To prevent power issues that lead to downtime & damage to equipment
Characteristic	● Independent of the utility power supply ● Provides high quality electrical power
Installation	● Filters ● A diesel power generator ● A set of batteries or a flywheel system
Battery powered UPSs	● A.k.a. Standby UPS systems / off-line systems ● Used in small setups (a few workstations or servers) ● Line interactive UPS systems ○ Use a transformer between the utility power & the IT equipment ○ Works as a filter for many of the power issues ● Double conversion UPS systems ○ Convert the AC utility power to DC power & then back to high quality AC power. (AC: Alternating Current, DC: Direct Current)

Power Distribution Unit (PDU)

A device with multiple outlets 多个插座 that distributes power to equipment located in the datacenter.	
Types	**Floor PDUs** ● Used in larger datacenters to distribute power to multiple racks or equipment. **Rack PDUs** ● Mounted in standard 19-inch equipment racks, offering a range of power distribution options.
To achieve high availability	Infrastructure components can be equipped with two power supplies for redundancy & at least two power strips 插座 to power equipment in a rack

Cooling

Objective	To dissipated heat	
Types	Computer Room Air Conditioners (CRAC)	Refrigerant-based units 制冷剂型机组 connected to outside condensing units 外部冷凝机组
	Computer Room Air Handlers (CRAH)	Chilled water 冷冻水 based & connected to outside chillers. A chiller produces chilled water via a refrigeration process
The efficiency of a cooling system	Energy Efficiency Ratio (EER)	The measure of efficiency at maximum air conditioning load. The ratio between output cooling in BTU per hour and the electric energy input in Watts at a given operating point
	Seasonal Energy Efficiency Ratio (SEER)	Same as EER, but seasonal data is used for the measurement. The time of year the cooling system is used most (typically in the summer)
	Coefficient of Performance (COP)	The ratio between cooling load in kW and the electric energy input in kW. Normal values are between 3 and 10
Operating temperature	● The **air temperature** in the datacenter usually ranges from **18 to 27** ℃ ● Servers **shut themselves down** at an air inlet temperature 进气温度 of **40** ℃ ● Using **higher temperature saves cooling capacity and power**: Raising the temperature with one ℃, lowers the cost for cooling by 5%	
Airflow	An optimized airflow **eliminates hot spots in racks & components** as much as possible without having to cool the air in the datacenter too much.	
Liquid cooling	● Ideal for **large datacenters** ● It immerses components in a special **non-conductive & non-corrosive fluid** ● System boards can be placed closer, which **increases CPU density** in the datacenter	
Humidity and Dust	● The **humidity** of the air in a datacenter should between **40% and 60%** ● Minimize the number of dust particles in a datacenter ○ **Don't allow visitors** in the datacenter ○ **Wear dust-free clothing** (like white costs) and protective	

	sleeves around their shoes

Fire Prevention, Detection and Suppression

- A **short circuit** in a cable or defect equipment may cause fire
- Fires can spread around very quickly because of the air flow and use of **raised floors**
- **Smoke** could **damage equipment**
- Suppressing fire in a datacenter consists of four levels:

1. Fire **prevention**	**Avoid** a fire
2. Passive fire protection	**Limit** the exposure of the fire once it has started
3. Fire **detection**	**Detect** smoke and fire
4. Fire **suppression**	**Extinguish** the fire once it is detected

Equipment Racks

- A **19" (inch)** rack is a standardized metal enclosure to house IT infrastructure components
- The height of a rack is measured in rack unit or 'U'. **One U is 44.5 mm**
- A typical rack is **42U high**

Datacenter Energy Efficiency

- Energy cost > Server cost
- The **Power Usage Effectiveness (PUE)** measures the power used by the datacenter
  $PUE = Power\ used\ by\ the\ datacenter \div Power\ used\ to\ run\ the\ IT\ equipment\ in\ it$
- Typical PUE value of a datacenter is between **1.1 and 2.0**
- For a datacenter with a PUE of 1.5 means
  - 1 watt of power used by the IT equipment
  - 0.5 watt is used by the rest of the datacenter

Datacenter Availability

The availability tier classification only describes the **availability of the datacenter facilities**, not the availability of the IT infrastructure components, based on **uptime, redundancy & fault**

tolerance

	Tier 1	**Tier 2**	**Tier 3**	**Tier 4**
Infrastructure	Basic	Adds some redundancy & backup path for power & cooling	Multiple, redundant paths for power & cooling, allow maintenance without down time	Fully fault tolerant, with redundant systems for power, cooling & all IT equipment
Expected uptime	99.671%	99.741%	99.982%	99.995%

Redundant datacenters	● Multiple redundant datacenters can be used to **increase availability** ● Multiple datacenters are a must when **higher availability than 99.995%** is needed ● Redundant datacenters should be **at least 5 km apart**
Floor management, by floor manager	● **Minimize personnel walking** around the server racks ● Keeping the datacenter **floor tidy** ● Changing **backup** tapes ● Providing **power connections** to the racks ● **Maintain** & **test** the fire extinguishing system & UPS systems

Datacenter Performance

The datacenter itself does not provide performance to IT infrastructures, except for the **bandwidth** of the **Internet connectivity** & the **scalability** of the **location**

Datacenter Security

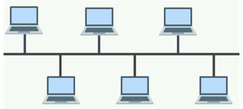
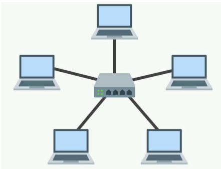
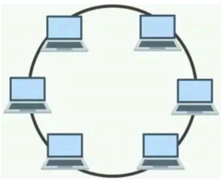
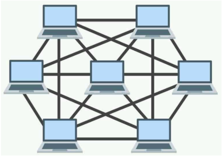
Physical security

- Ensure that equipment is physically safe behind the datacenter doors
- Physical **access** to the datacenter must be **restricted** to selected and qualified staff
- An **entry registration** system should be used
- A **log** should be maintained containing all staff entering and leaving the data center

- Doors must be secured using **conventional locks / electronic locks** (with authentication)
- Entry points can be implemented as:
    - Regular **doors, Mantraps** 密码锁**, Revolving doors** 旋转门
    - Equipped with **weighting scales** to ensure only 1 person enters the restricted area

C4: Networking

Network Topologies

	Bus	Star	Ring	Mesh
				
Connection by	Single cable / bus	Central hub / switch	A circular fashion	By connected to multiple devices
Data transmission	Along the bus, to intended recipient	Through the central point	In 1 direction around the ring	Routed through different paths
Pros	Simple & inexpensive to implement	Easy to manage and troubleshoot	Simple & efficient	Fault-tolerant
Cons	Prone to performance issues	Central hub as a SPOF	Disruptive to add / remove devices	Expensive to implement

Networking Building Blocks

- OSI Reference Model (OSI-RM) defines the different stages that data must go through to travel from one host to another over a network

Physical Layer

<table>
<tr><td colspan="3">● Deal with the physical components that carry the data
● Data transmission media and connectors
● Signal characteristics
● Network topology</td></tr>
<tr><td><b>Cables</b></td><td>Twisted pair cables</td><td><u>Unshielded Twisted Pair (UTP)</u>
● Consists of twisted wire pairs without any additional shielding
● Used in Ethernet networks and for telephone systems</td></tr>
</table>

		● Pros: ○ Cost-effective ○ Easy to install ○ More flexible ● Cons: ○ Susceptible to interference 易受干扰 ○ Lower data rate <u>Shielded Twisted Pair (STP)</u> ● Suitable for most home and office networks where interference isn't a major concern ● Used in factories, datacenters, or areas with high electrical noise ● Pros: ○ Reduce interference ○ Higher data rates ● Cons: ○ More expensive ○ More complex installation ○ Less flexible
	Fiber Optic Cables	<u>Multimode</u> ● Core diameter: 50 or 62.5 microns (larger) ● Light source: LEDs (multiple paths) ● Used in LAN, datacenter, short distance ● Cost: Less expensive <u>Single-mode</u> ● Core diameter: 9 microns (smaller) ● Light source: Laser (single path) ● Used in telecommunication, long distance ● Cost: More expensive
	Coaxial cables	For TV & Internet connection, outside Malaysia
Patch Panel	Function	Provides a centralized location to organize and manage network cables
	Pros	● Organise cables ● Ease changes ● Protect connections ● Provide clear reference for labelling & documentation
Cablin	Vertical Cabling	<u>Pros</u>

g		● **Enhance network reliability**: fault isolation, increase uptime, disaster recovery ● **Improve network performance**: Load balancing, reduce latency ● **Simplify network management**: Centralized management, ease troubleshooting Connection ● The main distribution cabling connects the patch panels on the floors to the datacenter ● Connects floors and buildings Cable Types ● Fiber Optic (primary) ● Twisted pair ● Coaxial Distance Limit ● Long distance
	Horizontal Cabling	Pros ● Same with vertical cabling Connection ● Endpoints in the walls are connected to the patch panels ● Within a specific floor / building Cable Types ● Twisted pair (primary) ● Fiber optic Distance Limit ● Limited to 90 meters
Leased lines 租赁线路	Definition	● A **dedicated data connections** between two locations ● Provided by a telecom provider
	Types	T or E lease line ● Definition: **Not standard** industry terms for leased lines ● Pros: ○ **Low data rate**: T (1.544 Mbps), E (2.048 Mbps) ● Used in ○ T (USA, Canada and Japan)

		○ E (most other countries) Synchronous Optical Network (SONET) ● Definition: Transmit large amounts of data using **fiber optic** ● Pros: ○ **High data rate** ○ **Low latency** ● Used in: ○ Connecting corporate offices & datacenters ○ Enabling high-speed data replication & backup ○ Supporting real-time applications with low latency requirements Synchronous Digital Hierarchy (SDH) ● Definition: The international standard equivalent to SONET ● Pros: ○ **High reliability** ○ **Scalability** ● Used in: ○ Telecommunications to transmit multiple digital data stream over a fiber optic Dark Fiber ● Definition: **Unused fiber optic cables that have been installed but are not actively transmitting data** ● Pros: ○ **High bandwidth** ○ **Low latency** ○ **Security** ○ **Scalability** ○ **Reliability** ● Used in: ○ To accommodate future growth ○ Leassee then installs their own equipment to "light up" the fiber and create their own private network
Internet Access	Dedicated Internet Access (DIA)	Characteristics ● **High speed** ● **Reliable connectivity** ● **Guaranteed bandwidth**

		Connection ● Dedicated cable connection to single business Ideal for ● Business with critical applications
	Broadband	Characteristics ● **High-speed** over cable, Digital Subscriber Line (DSL) or fiber optic networks Connection ● Shared among multiple users Ideal for ● Internet browsing ● Email
	WiFi	Characteristics ● Includes Wi-Fi, cellular data and satellite Internet Connection ● Shared connection **without physical cable** Ideal for ● Wirelessly

Data Link Layer

- Ensure reliable & error-free data transfer between devices
- Takes packets received & breaks them into frames
- Detect errors in the frames
- Manage how devices access the physical medium to prevent collisions

Network

	PAN	**LAN**	**MAN**	**WAN**
Distance	Within a few meters	Home, office building or school	A city or a large campus	Large geographical area
Used in	Connecting personal devices within a few meters	Setting up a network in a home office, or campus for fast local	Linking multiple LANs across a city or large institution	Connecting networks across cities, countries or globally

		access		
Protocols	Bluetooth (L2CAP), Zigbee, Infrared	Ethernet (CSMA/CD), Wi-Fi (CSMA/CA)	Metro Ethernet, DQDB	PPP, HDLC, Frame Relay

Common Protocols Used

	Ethernet	**WiFi**	**PPP**
Technology	Wired	Wireless	Direct connection between two devices
Used for	Connecting devices in a LAN	Connecting to the Internet wirelessly	VPNs, dial-up & Internet connection

Implementation

- Ethernet
- Switching: Split a single network segment into multiple segments, for each device
- Public wireless networks:

	Features	**Used in**
1G	Limited data speeds and security features	(Analog) Support voice calls
2G	Improved call quality and security	(Digital) Improved call quality and security
3G	Increased data speeds, allowing for mobile internet access	Support email, web browsing
4G	Further speed improvements	Streaming videos and online gaming
5G	Faster speeds, lower latency (delay) and greater capacity	Internet of Things (IoT), virtual reality and self-driving cars

Network Layer

- Define the route the data is sent to the recipient
- Implementations:
  - IPv4
  - IPv6
  - Routing and addressing

IP Protocol

A unique numerical label assigned to each device connected to a network

Server can have multiple IP addresses, both public and private

- Load balancing
- Hosting multiple websites
- Providing different services on the same server

	Public IP Address	Private IP Address
Visible to	Entire network	Within a local server within a private network
Used for	● Web server ● Email server ● Public-facing applications	● Internal communication
Purpose	Enables external users to access services hosted on your server	Not routable on the internet, enhancing security

Why need both?

- A server might use a public IP to allow users to access a website, while using a private IP for internal tasks like database communication or backups
- Helps with load balancing, hosting multiple websites and providing different services on the same machine

Addressing

	Static IP Address	Dynamic IP Address
Nature	Constant	Change periodically
Ideal for	● Public servers ● Services that need consistent access (e.g. VPN email servers)	● Internal servers ● Devices that don't need constant external access

Why need both?

- Static IPs are crucial for services that require a stable address for DNS records or remote access
- Dynamic IPs are cost-effective and suitable for general use, reducing the need for manual configuration

Routing

- Routers compile routing tables to make IP packet forwarding decisions
- Routing in the context of a server, covers:
    - Network Routing

        - Direct data packets are from the server to the other network devices
    - Application-Level Routing
        - Handle incoming requests within the server itself: load balancing, Content Delivery Networks (CDNs), application-specific routing

Transport Layer

- Maintain flow control
- Provide error checking
- Recovery of data between network devices

Protocols Used

	Transmission Control Protocol (TCP)	**User Datagram Protocol (UDP)**
Function	Provides reliable delivery of a stream of data between applications	Reduced latency over reliability by sending data without checking if the data arrived
Used in	● FTP ● Web browsing ● Email	● Live stream ● Online games ● VoIP
Used for	Large DNS queries	Small DNS queries

DNS - Domain Name System

- Port 53 is specifically for DNS. Other services should not use this port.
- Firewalls should allow traffic on port 53 for DNS to function correctly

Session Layer

- Provides mechanisms for opening, closing and managing a session between end-user application processes

Virtual Private Network (VPN)

- Uses a **public network** to **interconnect private sites** in a secure way, a.k.a. VPN tunnel
- Uses "virtual" connections based on **IPsec / SSL**
- Most network providers also offer private VPNs based on MPLS
- VPNs use **strong encryption** and strong user authentication. Using the Internet for transmitting sensitive data is considered safe
- VPN tunnels are often used for **remote access to the LAN** by users outside of the

organization's premises

- Most common VPN communication protocol standards:

	Point-to-Point Tunneling Protocol (PPTP)	**Layer 2 Tunneling Protocol (L2TP)**	**IPsec**
Uses	For individual client to server connections	For individual client to server connections	For network-to-network connectivity. IPsec is built into IPv6 standard and is implemented as an add-on to IPv4
Security	Least	No encryption and relies on IPSec for encryption and authentication	Provides encryption and authentication for network traffic
Used in	Legacy system or when speed is prioritized over security	Paired with IPSec for a more secure VPN connection	VPNs and other secure network applications

Presentation Layer

- Takes the data provided by the application layer and converts it into a standard format that the other layers can understand

	Secure Socket Layer (SSL)	**Transport Layer Security (TLS)**
Nature	SSL is considered insecure and should not be used	TLS is securing WWW traffic carried by HTTP to form HTTPS

Application Layer

- Interacts with the OS or application

Roles of application layer in servers

- Protocol implementation
- Data formatting
- Error handling
- Security
- Session management

Protocols used

Protocol	**Definition**	**Function**

Domain Name System (DNS)	● DNS is a distributed database that links IP addresses with domain names ● DNS was not designed with security in mind ● Updates to DNS records are done in non-encrypted clear text ● Authorization is based on IP addresses only	Translates human-readable domain names (like google.com) into machine-readable addresses
DNS Security Extensions (DNSSEC)	Provides origin authentication of DNS data for data integrity	Verifies the authenticity & integrity of DNS data
IP Address Management (IPAM)	● IPAM systems are appliances that can be used to plan, track and manage IP addresses in a network ● IPAM systems integrate DNS, DHCP and IP address administration in one high available redundant set of appliances	Plans, tracks and manages the IP address space within a network
Network Time Protocol (NTP)	● NTP ensures all infrastructure components use the same time in their real-time clocks ● Particularly important for: Log file analysis, clustering software, Kerberos authentication	Synchronization clocks of computers in a network to a common time source
Post Office Protocol (POP)	Used by email clients to retrieve email messages from a mail server	Retrieves emails from a mail server
Simple Mail Transfer Protocol (SMTP)	Used to send email messages from a mail client to a mail server or between mail servers	Sends emails from a mail client to a mail server or between mail server
Multipurpose Internet Mail Extensions	Enables SMTP to support file attachments in email messages	Transmits non-text data (like images, audio, video) in email

(MIME)		
File Transfer Protocol (FTP)	A protocol for transferring files between computers	Transfers files between computers over a network
Hypertext Transfer Protocol (HTTP)	Defines how messages are formatted and transmitted, and how web servers and browsers should respond to various commands	Transfers hypertext (HTML, CSS, JavaScript, images, etc)
Hypertext Transfer Protocol Secure (HTTPS)	Used when browsing the web with a web browser	Protected data during transfer

* Example refers to images

Networking Virtualization

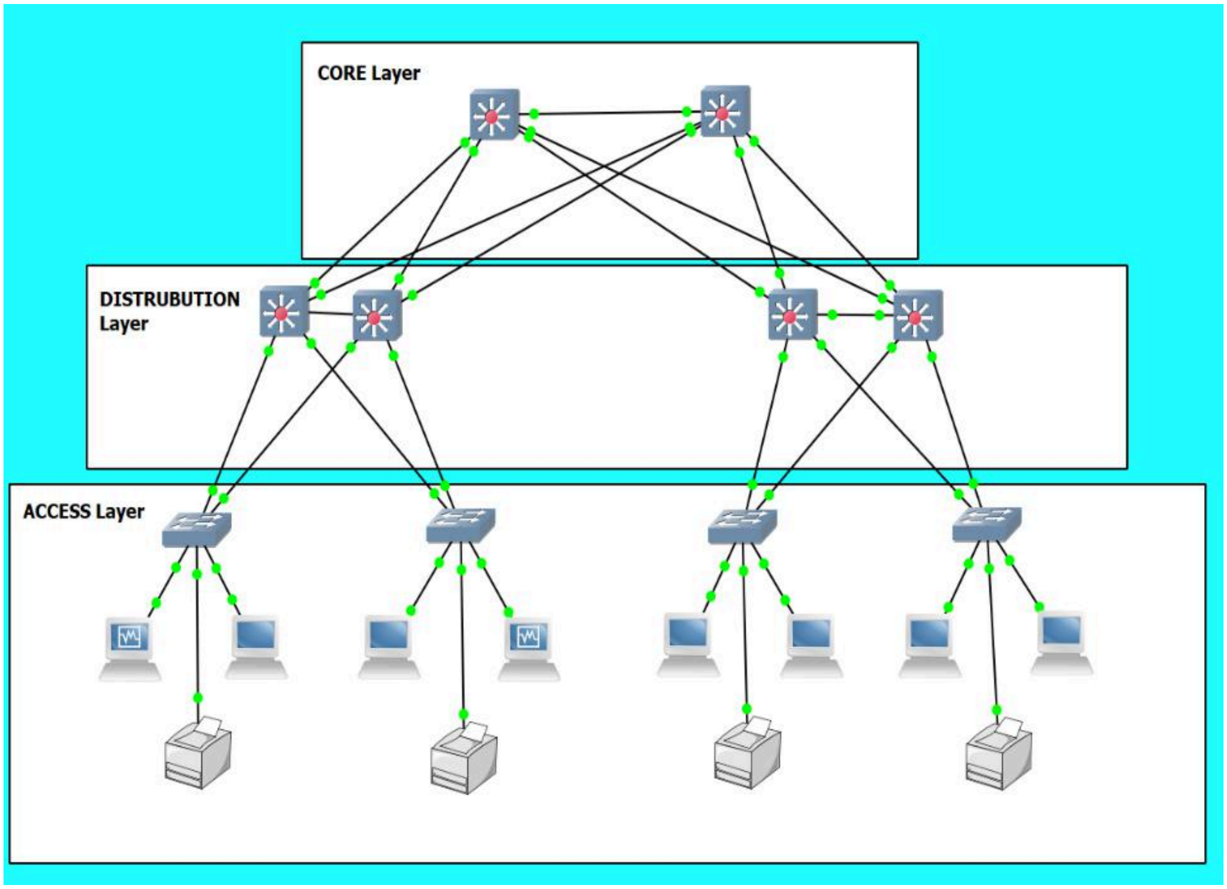
Approaches	**Used for / as**	**How**
Virtual LAN (VLAN)	Logical grouping (for network segmentation)	Logically divides a single physical network into multiple broadcast domains (operate at Layer 2 with supporting up to 4096 VLANs)
Virtual Extensible LAN (VXLAN)	Network virtualization technology	Uses encapsulation to create virtual networks that can span across physical networks, allowing for greater scalability and flexibility compared to VLANs (operate at Layer 2 over Layer 3 with supporting 16 million VXLANs)
Virtual Routing and Forwarding (VFR)	Network routing technology (for segmentation)	Hosts multiple independent routing tables in a single physical router
Virtual Network Interface Controllers (VNIC)	Software-based representation of a network interface	Enables virtual machines to connect to the network and communicate with other virtual machines or physical devices

Virtual Switch (VS)	Software-based equivalents of physical network switches	Manages network traffic within a virtualized environment, providing functionalities like VLAN tagging, traffic shaping and connection to physical networks
Software Defined Networking (SDN)	Software-based controllers (Abstract control plan from data plane)	Manages network traffic and resources, enabling dynamic and programmable network configurations
Network Function Virtualization (NFV)	Network architecture (virtualize network function)	Replaces traditional dedicated network hardware appliances with virtualized software instances running on commodity servers

* Example refers to images

Networking Availability

Layered network topology

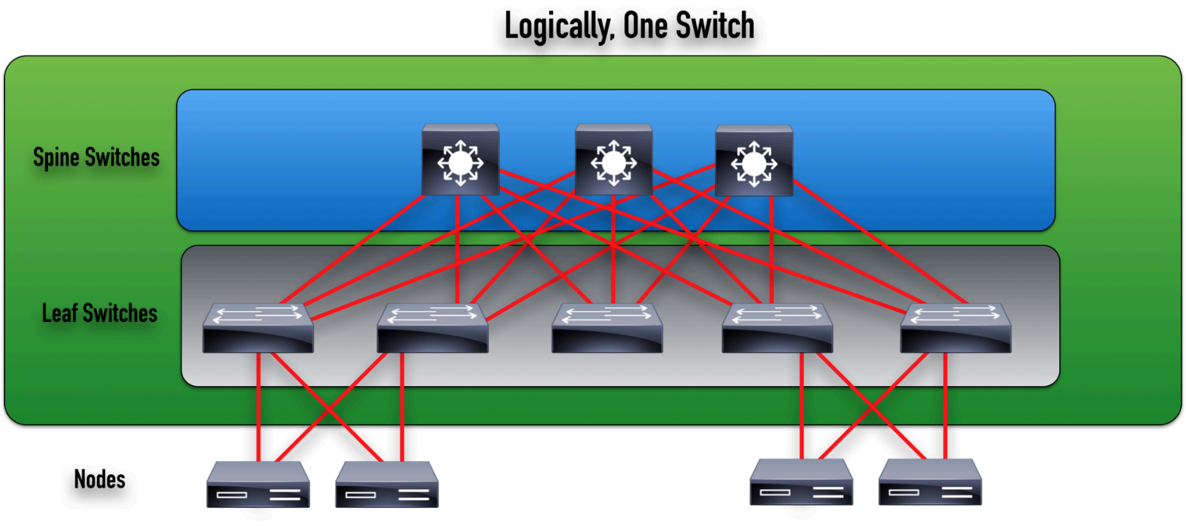


Definition	Divides a network into multiple layers, each with specific functions and responsibilities
A.k.a.	Tiered or hierarchical topology
Components	Core Layer ● Definition ○ The center of the network ○ The backbone of the network ○ It typically uses high-capacity routers & switches ● Nature ○ High-speed network backbone between network segments ● Function ○ Offer rapid & reliable transfer for large volume of data Distribution / Aggregation Layer ● Definition

	○ It combines the access layer data and sends its combined data to one or two ports on the core switches ● Nature ○ Sits between the core (in datacenter) & access layers (in patch closet) ● Function ○ Performs routing functions, implements security policies, access and core layers Access Layer ● Definition ○ For servers, located at server racks / in blade enclosures ○ For workstations, placed in patch closets ● Nature ○ Connect workstations & servers to the distribution layer ● Function ○ Connect end-users and devices to the network
Benefits	● Improve availability & performance (with multiple paths to any piece of equipment) ● Provides scalability ● Provides deterministic routing: advance determination of the routes between given pairs of nodes ● Avoids unmanaged ad-hoc data streams 避免未经管理的临时数据流

* Example refers to images

Spines and Leaf topology

 Logically, One Switch Spine Switches Leaf Switches Nodes	
Definition	A modern datacenter network architecture designed to address the

	limitations of traditional three-tier hierarchical designs
Natures	● The spine switches are not interconnected ● Each leaf switch is connected to all spine switches ● Each server is connected to two leaf switches ● The connections between spine and leaf switches typically have 10 times the bandwidth of the connectivity between the leaf switches and the servers
Key components	Spine Switches ● Function ○ Form the core of the network ● Nature ○ Interconnected in a full-mesh topology, providing redundancy & load balancing ● Working (Retail Industry) ○ The spine layer serves as the core of the network, connecting all leaf switches Leaf Switches ● Function ○ Connect to servers and other end devices ● Nature ○ Each leaf switch connects to all spine switches, creating multiple paths for traffic ● Working (Retail Industry) ○ Leaf switches act as access points, connecting servers, point-of-sale (POS) systems, inventory management systems, and other devices to the network
Working	A simple physical network is used that can be programmed to act as a complex virtual network. Such a network can be organized in a spine and leaf topology
Benefits	● Highly scalable: There are no interconnects between the spine switches ● Simple to scale: Just add spine or leaf servers ● Physical servers can be connected using relatively few switches ● Predictable latency: Each server is always exactly four hops away from every other server

* Example refers to images

Network Teaming

A.k.a.	Link aggregation, port trunking, network bonding
Definition	A method of combining multiple network interface cards (NICs) into a single logical interface
Objective	● Provides a virtual network connections using multiple physical cables ● To achieve high availability and increased bandwidth ● To improve network performance and reliability
Working	Bonds physical NICs together to form a logical network team: ● Sends traffic to the team's destination to all NICs in the team ● Allows a single NIC, cable or switch to be unavailable without interrupting traffic

* Example refers to images

Spanning Tree Protocol (STP)

Definition	An Ethernet level protocol that runs on switches
Working	● Guarantees only one path is active between two network endpoints at any given time ● Redundant paths are automatically activated when the active path experiences problems ● Ensures no loops are created when redundant paths are available in the network
Pros	● Shortest Path Bridging (SPB) allows all paths to be active simultaneously, enables much larger topologies, supports faster convergence times ● Improves efficiency by allowing traffic to be load balanced across all paths. While STP can take 30 to 60 seconds to respond to a topology change, SPB can respond to changes in less than a second
Cons	It is not using half of the network links in a network, since it blocks redundant paths

* Example refers to images

Multihoming

Definition	Connecting a network to two different Internet Service Providers (ISPs)
Methods	● Single router with dual links to a single ISP ● Single router with dual links to two separate ISPs ● Dual routers each with its own link to a single ISP ● Dual routers each with its own link to a separate ISP

Pros	● Improve availability
Cons	It is not always guaranteed that multiple network paths actually run on a different set of cables. Cables are used by multiple carrier providers.

Networking Performance

Factors affect the speed of a connection

Throughput and bandwidth

Definition	Amount of data that is transferred through the network during a specific time interval
Constraint	Throughput is limited by the available bandwidth
Working	When an application requires more throughput than a network connection can deliver: ● Queues in the network components temporarily buffer data ● Buffered data is sent as soon as the network connection is free again ● When more data arrives than the queries can store in the buffer, packet loss occurs

Latency

Definition	The time from the start of packet transmission to the start of packet reception
Depend on	● The physical distance a packet has to travel ● The number of switches and routers the packet has to pass
Rules	● 6 ms latency per 100 km ● WANs: Each switch in the path adds 10 ms to the one-way delay ● LANs: Add 1 ms for each switch
Types	One way latency ● The time from the source sending a packet to the destination receiving it Round-trip latency ● The one-way latency from source to destination plus the one-way latency from the destination back to the source A "ping" can be used to measure round-trip latency

Quality of Service (QoS)

Definition	Ability to provide different data flow priority to different applications, users or types of data
Nature	Allows better service to certain important data flows compared to less important data flows
Used for	Real-time applications like video and audio streams and VoIP telephony
Implementations methods	Congestion Management ● To prioritize traffic ● Defines action when the amount of data to be sent exceeds the bandwidth of the network ● Packets can either be dropped or queued Queue Management ● To make the wait time more manageable and transparent ● Defines criteria for dropping packets that are of lower priority before dropping higher priority packets ● When queue are full, packets will be dropped Link efficiency ● To ensure efficient use of available resources ● Ensures the link is used in an optimized way ● By fragmenting large packets with low QoS, allowing packets with a high QoS to be sent between the fragments of low QoS packets Traffic shaping ● To prioritize certain types of traffic over others ● Limit the full bandwidth of streams with a low QoS ● High QoS streams have a reserved amount of bandwidth

WAN Link Compression

Definition	Data compression reduces data size before it is transmitted
Pros	WAN acceleration appliances: ● Provide compression ● Perform some caching of regularly used data at remote data

* Example refers to images

Networking Security

Network Encryption

Definition	Encryption is often a feature in the datacenter
Types	● Encrypting data in transmit: Encrypting data on the network ● Encrypting data at rest: Encrypting data in the storage ● End-to-end encryption: Encrypting data between 2 end-points, with network traffic encryption

Firewalls

Definition	● Firewalls separate 2 / more LAN / WAN segments for security reasons ● Firewalls block all unpermitted network traffic between network segments ● Permitted traffic must be enabled by configuring the firewall to allow it
Implementation	● In hardware appliances ● As an application on physical servers ● In virtual machines
Host based firewall	● Protect a server or end user computer against network based attacks ● Part of the operating system
Traffic control methods	Packet Filtering ● Data packets are analyzed using preconfigured filters ● This function is always available on routers & most OS Proxy ● A proxy terminates the session on the application level on behalf of the server (proxy) or the client (reverse proxy) and creates a new sessions to the client or server Stateful Inspection ● Inspects the placement of each individual packet within a packet stream ● Maintains records of all connections passing through the firewall and determines whether a packet is the start of a new connection, part of an existing connection, or is an invalid packet

Intrusion Detection System (IDS) or Intrusion Prevention System (IPS)

Definition	Detects & prevents activities that compromises system security (a hacking attempt)
Working	● Monitors for suspicious activity ● Alerts the systems manager when these activities are detected ● Stop attacks by changing firewall rules on the fly
Types	Network-based IDS (NIDS) ● Placed at a strategic point in the network ● Monitors traffic to and from all devices on that network ● The NIDS is not part of the network flows, but just "looks at it", to avoid detection of the NIDS by hackers Host-based IDS (HTDS) ● Runs on individual servers or network devices ● It monitors the network traffic of that device ● It also monitor user behavior and the alteration of critical (system) files

* Example refers to image

De-Militarized Zone (DMZ)

Definition	A DMZ is a network that serves as a buffer between a secure protected internal network and the inaccurate internet

* Example refers to image

Remote Authentication Dial In User Service (RADIUS)

Definition	RADIUS is a networking protocol that provides centralized user and authorization management for network devices

* Example refers to image

C5: Storage

Storage Building Blocks

Disks - Command Sets

- Disks are connected to disk controllers using command set, based on either ATA or SCSI

	Advanced Technology Attachment (ATA), now SATA (Serial ATA)	Small Computer System Interface (SCSI)
Description	A.k.a. IDE, uses a relatively simple hardware and communication protocol to connect disks to computers (mostly PCs)	A set of standards for physically connecting and transferring data between computers (mostly servers) and peripheral devices, like disks and tapes
Primary use	Desktop & laptop HDD	Servers, workstation, high-end systems
Cost	Least expensive	More expensive
Performance	Slower than but comparable to SCSI, especially with SATA	Historically faster
Expandability	Limited	High
Command set	Smaller	Larger (Complex)
Example (Retail industry)	Ideal in every day retail operations like POS systems and inventory management	Less common in retail. Better suited for the demanding requirements of datacenters & high-volume transaction processing

Mechanical Hard Disks vs Solid State Drive

	SATA (Serial ATA)	SAS (Serial Attached SCSI)	NL-SAS (Nearline SAS)	SSD (Solid State Drive)
Types	Mechanical disk (spinning platters 旋转盘片& magnetic head)			Flash memory
Primary used in	PCs & some	Enterprise	Applications	Laptops,

	entry-level servers	servers & storage systems requiring high performance, reliability & availability	require more capacity than standard SAS but need reliability & performance of SAS	desktops & servers where performance is crucial & high performance storage systems
Performance	Good for general use, but slower than SAS for demanding applications	High performance, lower latency than SATA	Performance falls between SATA and SAS	Faster speeds compared to both SATA & SAS HDDs
Cost	Most affordable	More expensive than SATA	More expensive than SATA but less expensive than traditional SAS	More expensive per gigabyte than HDDs, but prices have been decreasing
Capacity	High	Varies	Higher capacity than standard SAS drives	128GB - 4TB (for consumer models)
Reliability	Lower reliability	High reliability (dual-porting for redundancy & error correction)	Dual-porting, but poorer reliability than higher-end SAS drives	A limited number of write cycles before they wear out
Pros	● Cost effective ● Suitable for general-purpose storage	● High performance ● High reliability ● Supports redundancy	● A balance between SATA and SAS ● Better performance & reliability than SATA ● Lower cost than high-performance SAS drives	● High data transfer rate ● Reliability & redundancy ● Support multiple devices
Cons	● Slower than SAS	● More expensive	● Not as fast as full SAS	● Expensive ● Complex to

		than SATA	drives	configure & manage ● Obsolete (old technology)
Example (Retail industry)	● POS systems ● Basic inventory management ● Storing customer data ● General office use	● Data warehousing ● Advanced analytics ● High-volume transaction processing ● Systems require high uptime	● Archiving, large-scale data storage ● When both cost & performance are important	● High-end POS systems / managing large product databases However, the higher cost, complexity, make it less appealing for general retail use

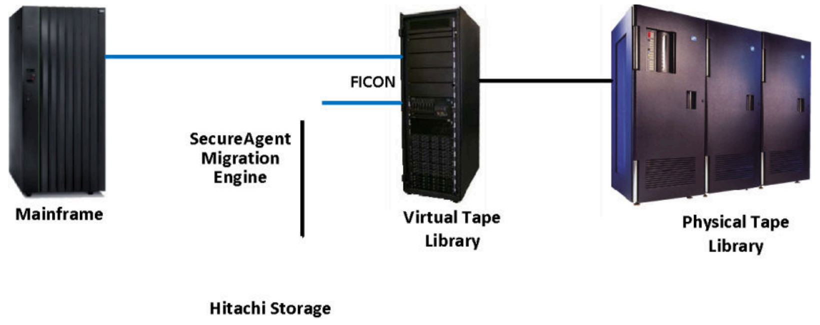
Tapes

- Tape is the **most inexpensive option to store large amounts of data**
- Suitable for archiving:
    - Tape manufacturers guarantee a **long life expectancy**
    - DLT, SDLT and LTO Ultrium cartridges are guaranteed to be readable after 30 years on the shelf
- Cons:
    - **Fragile**, manual handling can lead to mechanical defects
    - Tape cartridges contain mechanical parts. **Manually changed tapes get damaged easily**
    - Frequent rewinding 倒带 causes stress to the tape substrate 磁带基板. Leads to **lower reliability** of data reads
    - **Tapes are extremely slow -** they only write and read data sequentially

	Super Digital Linear Tape (SDLT)	**Linear Tape Open (LTO)**
Application	Older technology, large obsolete	Widely used
Technology	A second-generation DLT (Digital Linear Tape) technology developed by Quantum	More recent, open tape storage standard developed jointly by HP, IBM and Seagate

Capacity	Lower capacity	Higher capacity
Performance	Slower data transfer rates	Faster data transfer rates

Tape Library & Virtual Tape Library

	Virtual Tape Library	**Tape Library**
Picture	 Mainframe FICON SecureAgent Migration Engine Virtual Tape Library Physical Tape Library Hitachi Storage	
Storage	Disk-based storage	Magnetic tapes
Performance	Faster	Slower
Management	**Simplified management** as it integrates with **existing backup software** and **eliminates manual tape handling**	Requires **manual handling** of tapes, including loading, unloading and storage
Cost	Lower	Higher
Reliability	**More reliable** due to fewer moving parts	More **prone to mechanical failures**
Scalability	More scalable	Less scalable
Data protection	**Good for speed and efficiency**, also supports **offsite replication** 异地复制 and **cloud backups**	Good for **long-term archiving**
Example (retail industry)	Ideal for retailers who need **fast backups and recoveries**, especially for point-of-sale systems and online transactions	Ideal for **archiving data** for regulatory compliance and **long-term storage**

Comparison between HDD, SSD & Tape

Feature	**HDD**	**SSD**	**Tape**
Performance	Slower (moving parts, rotational latency)	Faster (instantaneous access 即时访问, no moving parts)	Slowest (sequential access, needs rewind 倒带)
Capacity	Highest capacity options available	Lower capacity than HDDs at comparable price	Highest theoretical capacity
Cost per GB	Lower cost per GB	Higher cost per GB	Very low cost per GB
Reliability	More susceptible to physical damage 更容易受到物理损坏	Less susceptible to physical damage	Highly durable, long archival lifespan

Controllers

- Controller can implement:
    - High performance (using RAID technology)
    - High availability (using RAID technology)
    - Virtualized storage (using RAID technology)
    - Cloning
    - Data deduplication
    - Thin provisioning
- Controller splits up all disks in small pieces called physical extents
- From these physical extents, new virtual disks (Logical Unit Numbers - LUNs) are composed and presented to the operating system

Redundant Array of Independent Disks (RAID)

- RAID solutions provide:
    - **High availability of data**
    - **Improvements of performance**
- RAID uses **multiple redundant disks**

RAID	**0**	**1**	**10**	**5**	**6**
A.k.a.	Stripping	Mirroring	Stripping & mirroring	Stripping with distributed parity	Stripping with distributed double parity
Operatio	Data is split	Data is	A combination	Data is	Similar to

n	into blocks & distributed across all disks in the array	duplicated (mirrored) onto two or more disks	of RAID 1 & RAID 0. Data is mirrored & then stripped 剥离 across the mirrored sets	stripped across multiple disks & parity info is calculated & stored on a separate disk This parity info allows for data reconstruction if one disk fails.	RAID 5, but uses two sets of parity info, allowing it to tolerate the failure of two disks
Performance	Best R (Read) & W (Write)	Faster R, limited W	High R & W	Good R, moderate W	Slower R than RAID 5
Pros	● Easy ● Cheap ● Increase performance	● High reliability ● High availability	● High performance ● High availability	● High redundancy	● High redundancy
Cons	● Low availability	● High cost	● Waste of resources	● Slow	● Slow
Example (Retail)	Ideal for **temporary data storage** or for systems where **high speed**, but **data loss is not critical**	Ideal for **storing critical data** (e.g. customer records, transaction history & employee info)	Suitable for **high-performance** systems requiring both **speed & data redundancy** (e.g. large databases or e-commerce platforms, ERP systems)	A common choice for servers & systems that need a **balance of performance & data protection** (e.g. inventory management, CRM systems)	Suitable for situations where **data loss is extremely critical** (e.g. financial transaction processing systems)

Data Compression

- Data on disk and tape is typically **stored in a compressed format**

- Allows 2 to 2.5 times the amount of data to be stored on the same media
- The **degree of compression is never guaranteed**
    - If the data is very diverse, the compression ratio may be correspondingly lower

Data Deduplication

- **Searches the storage system for duplicate data segments (disk blocks or files) and removes these duplicates**
- Used in archived as well as in production data
- The deduplication system keeps a table of hash tags to quickly identify duplicate disk blocks
    - The **incoming data stream is segmented**
    - **hash tags are calculated** of those segments
    - The **hashes are compared to hash tags of segments already on disk**
    - If an **incoming data segment is identified as a duplicate**, the **segment is not stored again**, but a **pointer to the matching segment is created** for it instead
- Deduplication can be done **inline** or **periodically**
- Inline deduplication **checks for duplicate data segments before data is written to disk**
    - **Avoids duplicate data on disks at any time**
    - Introduces a relatively **large performance penalty**
- Periodically: **writing data to disk first, and periodically check if duplicate data exists**
    - **Duplicate data is deduplicated by changing the duplicate data to a pointer to existing data on disk, and freeing disk space of the original block**
    - This process can be done at times when **performance needs are low**
    - Duplicate data will be stored on the disks for some time

Deduplication	**Inline**	**Periodic**
Processing	Immediate	Scheduled
Pros	Reduce storage	Improve availability
Cons	Slower	Required more storage
Example (Retail Industry)	For point-of-sale (POS) systems, inventory management databases, or customer relationship management (CRM) systems where **real-time data is critical**	For archival data, backups, or less frequently accessed data warehouses, where **minimizing storage space is more important than real-time performance**

Cloning and snapshots

- With cloning and snapshotting, a **copy of data is made at a specific point in time that can be used independently from the source data**
- Usage:
    - **Create a backup at a specific point in time**, when the data is in a stable, consistent state
    - **Creating test sets of data and an easy way to revert to older data** without restoring data from a backup
- Cloning: the storage system **creates a full copy of a disk**, much like a RAID 1 mirror disk
- Snapshot: represents a **point in time of the data on the disks**
    - **No writing to those disks is permitted** anymore, as long as the snapshot is active
    - **All writing is done on a separate disk volume** in the storage system
    - The **original disks still provide read-access**

	Clone	**Snapshot**
Characteristics	Writable	Read only
Storage required	High	Very high
Speed	Nearly instant	Instant
Usages	For dev/test, duplication, migration	For backup, rollback, consistency
Example (Retail Industry)	Retailers create sandbox environments for developers & testers by **cloning production databases / application servers**. This allows them to experiment with new features, configurations / code changes without affecting live systems	Retailers can use snapshots to **create regular backups of critical data** (e.g. customer info, inventory records & sales data.) This allows for **rapid recovery in case of data loss** due to hardware failure, software bugs or accidental deletion

Thin Provisioning

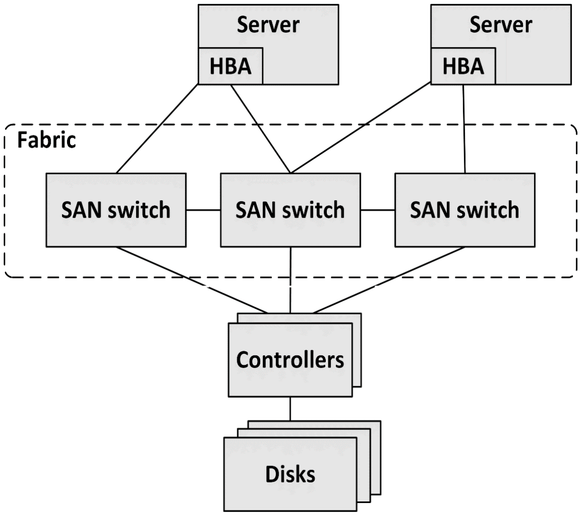
- Enables the **allocation of more storage capacity to users than is physically installed**
- Thin provisioning still provides the applications with the required storage
    - **Storage is not really available on physical disks**
    - Uses **automated capacity management**
    - The **application's real storage need is monitored** closely

- ○ **Physical disk space is added when needed**
- Typical use: Providing users with large sized home directories or email storage

Direct Attached Storage (DAS)

Definition	A **storage directly connected to a single computer**, typically via USB, SATA or SAS cables
Pros	● **Simple to set up and use** ● **Relatively inexpensive** ● **Good performance for a single user**
Cons	● **Not easily shared between multiple computers** ● **Limited scalability** ● **No centralized management**
Example	An external hard drive connected to a laptop
Example (Retail Industry)	Simple setup and low cost make it suitable for small retail businesses, or specific departments needing local, high-speed storage

Storage Area Network (SAN)



- **Connects large pool of central storage to multiple servers**
- SAN physically **connects servers to disk controllers** using specialized networking technologies like **Fibre Channel** or **iSCSI**
- Via the SAN, disk controllers **offer virtual disks to servers**, a.k.a. **LUNs (Logical Unit Numbers)**

● LUNs are only available to the server that has that specific LUN mounted ● In SANs, a large number of disks are installed in one or more disk arrays ● The number of disks varies between dozens of disks and hundreds of disks ● Most used SAN connectivity protocols: ○ **Fibre Channel** ○ **FCoE** ○ **iSCSI**	
Definition	A dedicated, high-speed network specifically for connecting storage devices to servers
Pros	● **High performance** ● **High scalability** ● **Suitable for large enterprise environments** ● **Dedicated network means less impact from other network traffic**
Cons	● **More complex** ● **More expensive to set up and manage** ● **Requires specialized expertise**
Example	A storage network in a data center, connecting multiple servers to a large array of hard drives
Example (Retail Industry)	Large retail chains with high-volume transactions, databases, and critical applications requiring high performance and reliability

Fibre Channel (FC), Fibre Channel over Ethernet (FCoE) & iSCSI

To connect servers to storage dev	**Fibre Channel (FC)**	**Fibre Channel over Ethernet (FCoE)**	**iSCSI**
Purpose	Designed specifically **high-speed**, **low-latency** storage networking	**Converges FC traffic & traditional Ethernet traffic** onto a single network infrastructure	Allows storage devices to be accessed over **standard IP networks** using the SCSI protocol
Technology	**Uses a dedicated network infrastructure** (FC switches, HBAs) with **specialized cabling** (fiber optic or copper)	**Encapsulates FC frames within Ethernet frames**, requiring **lossless Ethernet** and specific hardware (CNAs - Converged Network Adapters)	**Uses TCP/IP and Ethernet**, making it compatible with existing network infrastructure

Performance	**Best performance and reliability**, ideal for demanding workloads & large enterprise environments	Can achieve **performance comparable to FC**, especially with the use of lossless Ethernet and proper configuration	Generally **lower performance than FC and FCoE** due to TCP/IP overhead and potential for network congestion
Costs	**Higher cost** due to specialized hardware requirements	Can be **more cost-effective than FC** alone, as it leverages existing Ethernet infrastructure, but still requires specific hardware components	**Most cost-effective** option due to reliance on standard Ethernet components
Complexity	Can be **more complex to deploy and manage compared to iSCSI**	Can be **more complex than iSCSI** due to need for lossless Ethernet and specialized hardware	**Easiest to deploy and manage** due to familiarity with TCP/IP and Ethernet
Used when	Performance and reliability are paramount, and cost is less of a concern	Converge storage and network traffic and want to leverage existing Ethernet infrastructure	Cost-effectiveness and ease of deployment are primary concerns
Example (Retail Industry)	Large retail chains with high transaction volume & stringent 严格 performance requirements might opt for FC	As Ethernet speeds continue to increase, FCoE may become more attractive, offering the potential for both performance & cost savings	Smaller retailers or those with less demanding needs might find iSCSI a more cost-effective & practical solution

Network Attached Storage (NAS)

- NAS is often an appliance that **implements the file services and holds the disks on which data is stored**
- NAS appliance could also **use external disk storage provided by a SAN**
- Can **provide snapshot and clone technology at a file level**, enabling features like "un-erasing" deleted files by end users
- Difference between a SAN and NAS:
    - SAN:
        - **Offers disk blocks** (unformatted disks called LUNs) that can be used

by only one server
        - **Uses iSCSI, Fibre Channel or FCoE** as the communication layer
    - NAS:
        - **Offers a shared filesystem to store files that can be used by multiple servers**
        - **Connects to** for instance to an **LDAP** or **Active Directory service** in order to **set file and / or folder permissions**
        - **Uses SMB/CIFS** or **NFS over TCP/IP** as the communication layer
- **Clustered NAS** is a **NAS that uses a distributed file system running simultaneously on multiple servers**
    - **Distributes data and metadata across storage devices**
    - Still **provide unified access to the files from any of the cluster nodes**, unrelated to the actual location of the data
- File shares can also be provided by public cloud providers
    - AWS offers File Gateways
    - Azure has Storage Accounts
    - GCP has Filestore

Definition	● A.k.a. File server ● NAS is a storage device connected to a network
Pros	● **Easy to share files** ● **Centralized storage** ● **Relatively simple to set up and manage**
Cons	● **Performance can be impacted by network traffic** ● **Not as scalable as SAN for very large deployments**
Example	A dedicated box with multiple hard drives, connected to a home or office network
Example (Retail Industry)	Suitable for retail businesses needing to share files, folders and digital assets across multiple computers or POS systems

Object Storage

- **Data in object storage cant be modified**
    - If a file is modified, the original file is deleted, and a new file is created
- **Unsuitable for frequently changing data**

Definition	Storing data as objects with associated metadata
Architecture	Data is stored in a flat structure (no hierarchical file system) with associated metadata that describes the object

Scalability	● **High scalable** ● **Stored in multiple locations** ● **Often used for cloud storage, with unlimited capacity**
Accessibility	Data is **accessed via HTTP**, making it suitable for web applications and cloud services
Ideal for	**Data that does not change much** such as office documents, backups, archives, video and audio files, and virtual machine images
Provider	Amazon S3, Google Cloud Storage, Azure Blob Storage
Example (Retail Industry)	A retailer might use object storage to archive old sales data or store high-resolution product images for their website

Software Defined Storage (SDS)

- Software Defined Storage (SDS) abstracts data and storage capabilities (a.k.a. control plane) from the underlying physical storage systems (data plane)
- SDS **virtualizes all physical storage into one large shared storage pool**
  - **Data can be stored in various storage systems while being presented and managed as one storage pool to the servers** consuming the storage
- Storage can be implemented as software running on commodity x86-based servers with direct attached disks
- Physical storage can also be SAN, a NAS, or an Object Storage system
- SDS **provides servers with virtualized data storage pools**
  - With the required performance, availability and security
  - Delivered as block, file or object storage
  - Based on policies
- **APIs can be used to provision storage pools and set the availability, security and performance levels of the virtualized storage**
- Using APIs, **storage consumers can monitor and manage their own storage consumption**

Definition	Separating storage software from hardware, allowing for greater flexibility, automation and resource pooling
Architecture	Storage management is handled by software, allowing for abstraction of underlying hardware and the ability to manage resources from different vendors
Scalability	SDS can scale dynamically as storage needs change, adding or removing capacity as needed

Accessibility	SDS can work with various hardware, including different vendors and types of storage, and can be deployed on-premises or in the cloud
Provider	Various SDS solutions from different vendors, often used in conjunction with virtualization and cloud technologies
Example (Retail Industry)	A retailer could use SDS to pool storage resources from multiple locations into a single, manageable entity, enabling them to scale storage capacity as needed

Storage Availability

- Uptime of your storage system
- How often is it accessible for storing, retrieving and managing your data?

Redundancy and Data Replication

- Synchronous replication
    - Each **write to the active storage system** and the **replication to the passive storage system must be completed before the write is confirmed to the operating system**
    - **Ensures data on both storage systems is synchronized** at all times and data is never lost
    - When the physical cable length between the two storage systems is more than 100 km, latency times get too long, slowing down applications, that **have to wait for the write on the secondary storage system to finish**
    - Risk: a **failing connection between both storage systems** a write is never finished, as the data cannot be replicated. This effectively leads to **downtime of the primary storage system**
- Asynchronous replication
    - **After data has been written to the primary storage system, the write is immediately committed to the operating system, without having to wait for the secondary storage array to finish its writes as well**
    - Asynchronous replication **does not have the latency impact** that synchronous replication has
    - Disadvantage: **potential data loss when the primary storage system fails before the data has been written to the secondary storage system**

Replication	**Synchronous**	**Asynchronous**
Replication	● Not protect against data erasure / data integrity problems due to a software bug ● If this happen, the deleted data will also be replicated	

Process	Writing data to both the primary and replica simultaneously	Writing to the primary first and then replicating to the replica
Pros	● Zero data loss ● High data integrity	● Lower latency ● Faster performance ● Greater distance ● Lower bandwidth requirement
Cons	● High latency ● Reduced availability ● Distance constraint	● Higher data loss ● Increase complexity
Example (Retail Industry)	Financial transactions, real-time inventory management, and point-of-sale systems where data consistency is critical	Backup & disaster recovery for less critical data, replicating data to offsite location, and managing large datasets

Backup and Recovery

Topic	Key Points / Explanation
Definition	● Backups are **copies of data** used to restore data to a previous state in case of **data loss, corruption, or disaster**.
Purpose	● Serve as a **last resort** when all else fails. ● Used for **disaster recovery** and **business continuity**.
Retention Period	● Backups are **short-term** copies. ● Usually **not kept for long**, as older data is less useful. ● Typically only a few **weeks old**.
Effect of Restoring	● Restoring a backup **takes you back in time**. ● However, external factors (customers, partners) **do not go back in time**, so synchronization issues may arise.
Backup vs. Archiving	● **Backup:** Protection against data loss. ○ Data type: Active, changing data ○ Frequency: Regular (daily / weekly) ○ Retention period: short to medium ○ Access speed: Fast (for quick restore) ○ Storage cost: Higher (performance-focused) ● **Archive:** Long-term data storage for **legal and compliance** purposes. ○ Data type: Inactive, historical data

	○ Frequency: As needed ○ Retention period: Long-term ○ Access speed: Slower (not for frequent access) ○ Storage cost: Lower (capacity-focused) ● **Common Mistake:** Using backups as archives.
Data Management Principle	● **Do not delete** data in production systems. ● **Older data** can be **archived** to secondary systems/databases.
Backup Frequency	● Should be **regular**. ● Typically **daily**. ● **Hourly or continuous** in critical environments.
3-2-1 Backup Rule	● **3 copies** of your data. ● On **2 different media types**. ● **1 copy** stored **off-site** (different location).
Secondary Site Requirement	● Backup copies must be stored at a **secondary site**. ● Maintain a **minimum distance of 5 km** from the main site to prevent shared disaster risk.
Other Items to Backup	● **Operating system installation files.** ● **Printed procedures** for rebuilding systems. ● **Software license keys**, including restore tools.
Testing Backups & Restores	● **Full restore test:** At least **once per year**. ● Include **hardware rebuild** steps. ● Ideally performed by **third parties** or **different personnel** (fresh perspective).
Monthly Restore Check	● **Test monthly** to ensure backup media work properly. ● Restore **some files** to verify **data integrity** and **readability**.
Good Practice Tip	● Always verify that **backup tapes/media actually contain valid data** before relying on them.

Backup Schemes

- A backup scheme describes what data is backed-up, when, and how
- Five basic backup schemes:
  - Full backup
  - Incremental backup
  - Differential backup

    - Incremental backup
    - Continuous data protection (CDP)
- **Full backup**
    - A complete copy of all data
    - Full backups are only created at relatively large intervals (like a week or a month)
    - Creating them takes much time, disk or tape space, and bandwidth
    - Restoring a full backup takes the least amount of time
- **Incremental backup**
    - Save only newly created or changed data since the last backup, regardless of whether it is a previous incremental backup or full backup
    - Restoring an incremental backup can take a long time
        - Especially when the last full backup is many incremental backups ago
- **Differential backup**
    - Save only newly created or changed data since the last full backup
    - Restoring a differential backup is quite efficient, as it implies storing a full backup and only the most recent differential backup
- **Incremental forever backups**
    - Make an initial full backup, after which only incremental backups are sent to the backup system
    - Metadata about the increments are stored in the backup system, allowing the backup system to compile a point in time restore from the increments
- **Continuous Data Protection (CDP)**
    - Guarantees that every change in the data is also simultaneously made in the backup system
    - The RPO (Recovery Point Objective) is set to zero, because each change immediately triggers a backup process
    - Expensive technology, and therefore only used in specific situations

Backup Scheme	**Description / Process**	**Advantages**	**Disadvantages / Notes**
Full Backup	Creates a **complete copy of all data**. Usually done **weekly or monthly**.	● **Fastest restore time**. ● Simple and reliable recovery process.	● **Slow to create**. ● Consumes **large storage** and **bandwidth**.
Incremental Backup	Saves **only new or changed data** since the **last backup** (full or incremental).	● **Fast and small** backups. ● **Efficient** in space and time.	● **Slow restore**, requires last full + all incrementals. ● Higher dependency

			chain.
Differential Backup	Saves **changes since the last full backup**.	● **Faster restore** (only need full + latest differential). ● Easier management than incremental.	● Backup size **grows daily** until the next full backup. ● Slightly slower than incremental.
Incremental Forever Backup	One **initial full backup**, then only **incremental backups** are taken. The system uses **metadata** to rebuild any restore point.	● **Highly space-efficient**. ● Enables **point-in-time recovery**.	● Needs **advanced backup software** to manage metadata. ● Complex to set up.
Continuous Data Protection (CDP)	**Real-time backup** — every data change is immediately copied to backup storage.	● **RPO = 0** (no data loss). ● Ensures **maximum protection**.	● **Very expensive**. ● High **system and network load**. ● Used only in **critical systems**.

Backup Data Retention Time

- Backup data retention time is the **amount of time in which a given set of data will remain available for restore**
- Defines **how long backups are kept and at which interval**
- In practice, a Grandfather-Father-Son (GFS) based schedule is often used:
    - Each day a backup is made
    - After a week, there are seven backups, of which the oldest backup is renamed to a weekly backup
    - After the second week, the same is done and the daily backups of the week before are deleted
    - Now there are eight backups, seven daily, two weekly
    - Every four weeks, the weekly backup is renamed as a monthly backup and the weekly backups are reused

    - The daily backups are the son, the weekly backups are the father, and the monthly backups are the grandfather

Archiving

- Archiving is mostly done for **compliancy and regulation reasons**
- **Non-compliance to law and regulation can lead to serious business disruption, fines and even jail time**
- Archived data is **read-only** to protect it from being altered
    - Very important for **regulatory compliance and non-repudiation**
    - Some archiving systems **store data in an encrypted form** and **use digital signatures to prove data is not tampered with**
    - Some systems allow data to be written to it for archiving, but disallow changing or deleting data
        - CD / DVD / Blu-ray
        - WORM tapes
- Data must be kept in such a way that it is guaranteed the data can be read after a long time
    - **Digital format** (like a Microsoft Word file or a JPG file)
    - **Physical format** (like a DVD or magnetic tape)
    - **Storage environment** (temperature, humidity)
- Use open standards for storing archived data
    - **Open standards are well documented**
    - Reading data will always be feasible, using emulation software if needed
    - **Storing all documents in structured human-readable XML text files** is one way to ensure data can be read for many decades
- Transfer data that is to be kept for a long time to the latest storage media standard every 10 years

Storage Performance

- Disk performance is dependent on:
    - **Disk rotation speed**
    - **Seek time**
    - **Interface protocol**
- Disks cannot spin much faster than 15,000 RPM
    - At this speed, the velocity at the edge of a 3.5" disk is 250 km/h
    - Increasing this velocity would physically destroy the disk
- Seek time is the time it takes for the head to get to the right track
    - Average seek times:
        - 3 ms for high-end disks (e.g. SSD)
        - 9 ms for low-end disks (e.g. HDD)

IOPS

- Input / output Operations Per Second (IOPS) is a **measure of how many read and write operations a disk can completed in one second**
- $\frac{1000}{Rotational\ delay\ (ms) + Seek\ time\ (ms)}$
- Writing is typically a bit slower than reading

RAID Penalty

- In RAID sets, multiple disks are used to form one virtual disk (LUN)
- **Writing data on multiple disks introduces some delay**, known as the **RAID penalty**
- Penalties for various RAID configurations are:
  - RAID 0: no penalty
  - RAID 1: penalty of 2
  - RAID 10: penalty of 2
  - RAID 5: penalty of 4
  - RAID 6: penalty of 6

Interface Throughput

- Storage performance is also dependent on **how fast the interface can move data from the disks to the systems consuming the data** and vice versa

Caching

Cache Type / Concept	**Description / Process**	**Advantages (Why It's Useful)**	**Disadvantages / Notes (When to Use / Caution)**
Read Cache	Acts as a buffer for read operations. When the same data is requested multiple times, it is served directly from cache instead of the disk.	Faster read performance for frequently accessed data. Reduces disk I/O load.	Limited benefit if data is not reused. Cache capacity is limited. Best for web servers or static content.
Write-Through Cache	Data is written to cache and disk simultaneously. The write is acknowledged only after the data is safely written	Very reliable. Maintains data integrity between cache and disk.	Slower write speed because the system waits for disk confirmation. Suitable for systems where data

	to the disk.		safety is more important than speed.
Write-Back Cache	Data is written to cache first and acknowledged immediately. Actual writing to disk occurs later when the disk is ready.	Faster write performance because it does not wait for the disk. Good for high-volume transactional systems.	Risk of data loss if power fails before cache data is written to disk. Can be protected using battery-backed cache. Common for databases and write-intensive systems.
Cache Sizing and Selection	The type and size of cache depend on the application workload and access pattern.	Properly sized cache improves system efficiency and performance.	Incorrect cache configuration can waste memory or reduce performance. Read cache suits web servers; write cache suits databases.

Storage Tiering

- Tiered storage **creates a hierarchy of storage media, based on cost, performance requirements, and availability requirements**
- Example:
  - Tier 1: Production data (SSD and SAS disks)
  - Tier 2: Seldom used data, like email archives (NL-SAS disks)
  - Tier 3: Backups (Virtual Tape Libraries on NL-SAS disks)
  - Tier 4: Archived data (Tape or NL-SAS disks)
- **The more tiers are used, the more effort it takes to manage the tiers**
- Automated tiering usually checks for file access times, file creation date and file ownership and automatically moves data to the storage medium that fits best
- Storage tiering is especially important when storing data in the public cloud, as it has different storage costs for each tier

Load Optimization

- Storage performance is highly dependent on the type of load
- Most vendors recommend a specific storage configuration for their systems or applications
  - For example, Oracle recommends a combination of RAID 1 and 5 for its database in order to optimize performance

Storage Security

Protecting Data at Rest

Topic	Description
Data States	● Data can exist in three states: ○ **In transit** – transported over a network ○ **In use** – accessed by an application or cache ○ **At rest** – stored on disk or tape
Data at Rest Security	Can be protected using **encryption** to prevent unauthorized reading or writing without the correct key.
Disk Encryption (Datacenter Limitations)	● Databases and applications require unencrypted data for normal operation. ● Provides limited benefit since datacenter disks are already in secure areas.
When Disk Encryption is Useful in Datacenter	● Protects data if a “faulty” disk is removed and not destroyed. ● Ensures data remains secure even if the disk fails and cannot be accessed. ● Allows safe return of failed disks to vendors under maintenance contracts. ● Makes it harder for attackers to recover old data from “empty” disk space.
Self-Encrypting Drives (SEDs)	● Commonly used in laptops and desktops. ● Require user authentication (password) before boot. ● Encryption is built into hardware. ● Keys are stored on the drive itself.
Cryptographic Disk Erasure (CDE)	● Works by deleting the disk’s encryption key. ● Renders all data unreadable (same effect as full wipe). ● Considered one of the most effective ways to erase disk contents.

SAN Zoning

- SAN zoning is a method of **arranging Fibre Channel devices into logical groups on a SAN fabric for security purposes**
  - SAN zoning is **implemented in the SAN switches**
  - SAN zones are comparable with VLANs in Ethernet networks
  - **Fibre Channel devices can only communicate with each other if they are**

members of the same zone

SAN LUN Masking

- In a SAN, LUN masking **makes a LUN available to some hosts and unavailable to other hosts**
- LUN masking is **implemented primarily at the HBA level**, not in the SAN switches
- It is good practice to use a combination of SAN zoning and LUN masking

C6: Compute

Compute Building Blocks

Computer Housing

Tower Server	● **Standalone units** that can be **placed on the floor or on a table**
Rack Server	● **Mounted in a rack**, a standardized enclosure that can **hold multiple servers** ● **Blade server has less wiring compared to traditional server** ● Therefore, it is **more reliable and lower costs**
Blade Server	● **More compact than rack servers** ● They are **housed in a blade chassis 刀片式机箱**, which **provides shared resources like power, cooling and networking**

Processors

- In computer, Central Processing Unit (CPU) - or processor - **executes a set of instructions**
- CPU is the electronic circuitry that **carries out the instructions of a computer program by performing the basic arithmetic, logical, control and input / output (I/O) operations specified by the instructions**

Processor Instructions

- CPU can perform fixed number of instructions such as ADD, SHIFT BITS, MOVE DATA, and JUMP TO CODE LOCATION, called the instruction set
- A program created using CPU instructions is referred to as machine code
- Each instruction is associated with an English like mnemonic
    - Easier for people to remember
    - Set of mnemonics is called the assembly language

Processors - Programming

- The assembler programming language is the lowest level programming language for computers
- Higher level programming languages are much more human friendly
    - C#
    - Java
    - Python
- Programs written in these languages are translated to assembly code before they can

run on specific CPU
- This compiling is done by a high-level language compiler

Processors - Speed

- CPU needs a high frequency clock to operate, generating so-called clock ticks or clock cycles
  - Each machine code instruction takes one or more clock ticks to execute
  - An ADD instruction typically costs 1 tick to compute
- The speed at which the CPu operates is defined in GHz (billions of clock ticks per second)
  - A single core of a 2.4 GHz CPU can perform 2.4 billion additions in 1 second

Processors - Word Size

- Each CPU is designed to handle data in chunks, called words with a specific size
  - First CPUs had a word size of 4 bits
  - Today, most CPUs have a word size of 64 bits
- The word size is reflected in many aspects of a CPU's structure and operation:
  - Majority of internal memory registers are the size of one word
  - The largest piece of data that can be transferred to and from the working memory in a single operation is a word
  - A 64-bit CPU can address 17, 179, 869, 184 TB of memory (64-bit word)

CPUs Created by Computer Manufacturers

- To be less dependent on the large CPU manufacturers, large computer manufacturers started creating their own CPU designs
  - The M1, M2 and M3 processors, developed by Apple, are based on the ARM architecture. They are used for specific Mac computers and the iPad Pro from November 2020. The M3 Max has 16 cores, running at 4.05 GHz
- Public cloud providers also develop their own processors now
  - AWS developed the Graviton processors to deliver the best performance for cloud workloads. Graviton is a 64-bit ARM-based CPU. Today, the most powerful CPU contains 64 cores, running at 2.4 GHz.
  - Microsoft also launched their own CPU: the Ampere Altra for their Azure cloud platform. It has up to 64 CPU cores and is also based on the ARM architecture
  - Google's Argos is a video optimized CPU for YouTube video encoding purposes

GPUs

- Graphics processing units (GPUs) can be used together with CPUs to accelerate specific calculations
- A GPU has a massively parallel architecture consisting of thousands of smaller, more

efficient cores designed for handling multiple tasks simultaneously
  - For example, the NVIDIA Tesla GP100 GPU has 3840 cores, runs at 1.3 GHz and - including cache memory - comprises 150 billion transistors
- GPUs are used in **Artificial Intelligence (AI)** and **Machine Learning (ML)**. They can **process ML/AI data sets**, with each GPU having the processing power of about 100 general CPUs. GPUs are especially used in **exploring and training AI models**
- GPUs are also used in **game consoles -** the GPU in the Microsoft X-box series X provides 12,000 GFLOPS
- The Sony PS5 features a custom GPU based on AMD's RDNA 2 architecture hardware that delivers 10,000 GFLOPS

RAM Memory

Type / Concept	Description	Key Characteristics
RAM (Random Access Memory)	Memory that allows data to be read or written in the same amount of time, regardless of its location.	● Based on transistor technology (ICs) ● Data is **volatile** (lost when power is off)
Static RAM (SRAM)	Stores each bit using **flip-flop circuits**.	● Uses **6 transistors per bit** ● **Faster** but **more expensive** ● Commonly used in CPU cache
Dynamic RAM (DRAM)	Stores each bit using a **capacitor** and **1 transistor**.	● **Cheaper** and **denser** (more data per chip) ● Data must be **refreshed** regularly (about 16 times per second) ● Commonly used as main system memory (e.g., DDR4, DDR5)

BIOS

- The Basic Input / Output System (BIOS) is a **set of instructions stored on a memory chip located on the computer's motherboard**
- The BIOS **controls a computer from the moment it is powered on, to the point where the operating system is started**
- Mostly implemented in a Flash memory chip
- It is good practice to **update the BIOS software regularly**

- Upgrading computers to the latest version of the BIOS is called BIOS flashing

Interfaces

- Connecting computers to external peripherals is done using interfaces
- External interfaces use connectors located at the outside of the computer case
- USB and Thunderbolt are mostly used today

USB

- The Universal Serial Bus (USB) was introduced in 1996 as a replacement for most of the external interfaces on servers and PCs
- Can provide operating power to attached devices
- Up to seven devices can be daisy-chained
  - Hubs can be used to connect multiple devices to one USB computer port
- USB 3.1
  - Provides a throughput of 10 Gbit/s
- USB Type-C
  - Smaller connector
  - Ability to provide more power to connected devices, including powering laptops
  - In order to transport this much power, the voltage of the USB-C power charger is raised automatically to maximum of 20V
- USB-C connector can provide USB 4 protocol, delivering up to 40 Gbit/s throughput

Thunderbolt

- A.k.a. Light Peak
- Thunderbolt 3
  - Provide a maximum throughput of 80 Gbit/s
  - Provide 100 W power to devices
  - Uses the USB Type-C connector
  - Backward compatible with USB 3.1

PCI

- Internal interfaces, typically some form of PCI, are located on the system board of the computer, inside the case, and **connect expansion boards like network adapters and disk controllers**
- **Uses a shared parallel bus architecture**
  - Only one shared communication path between two PCI devices can be active at any given time

PCIe

- PCI Express (PCIe) **uses a topology based on point-to-point serial links, rather than a shared parallel bus architecture**
  - A connection between any two PCIe devices is known as a link
  - A collection of 1 or more links is called a lane
- Routed by a hub on the system board acting as a crossbar switch
  - The hub allows multiple pairs of devices to communicate with each other at the same time
- Despite the availability of the much faster PCIe, conventional PCI remains a very common interface in computers

Compute Virtualization

A.k.a.	● Server virtualization ● **Software Defined Compute**
Purposes	● Introduces an **abstraction layer between physical computer hardware and the operating system using that hardware** ○ **Allows multiple operating systems to run on a single physical machine** ○ **Decouples 解耦 and isolates 隔离 virtual machines from the physical machine and from other virtual machines**
Details	● A **virtual machine** is a **logical representation of a physical computer in software** ● New virtual machines can be **provisioned without the need for a hardware purchase** ○ With a few mouse clicks or using an API ○ New virtual machines can be installed in minutes ● **Costs can be saved** on hardware, power and cooling by consolidating many physical computers as virtual machines on fewer (bigger) physical machines ● Because fewer physical machines are needed, the **cost of maintenance contracts can be reduced** and the **risk of hardware failure is reduced**

Public Cloud

- Public cloud providers are only able to exist thanks to the large-scale use of virtualization
- Virtualization **allows users to create, start and stop virtual machines (VMs) in a portal, CLI or by calling an API**

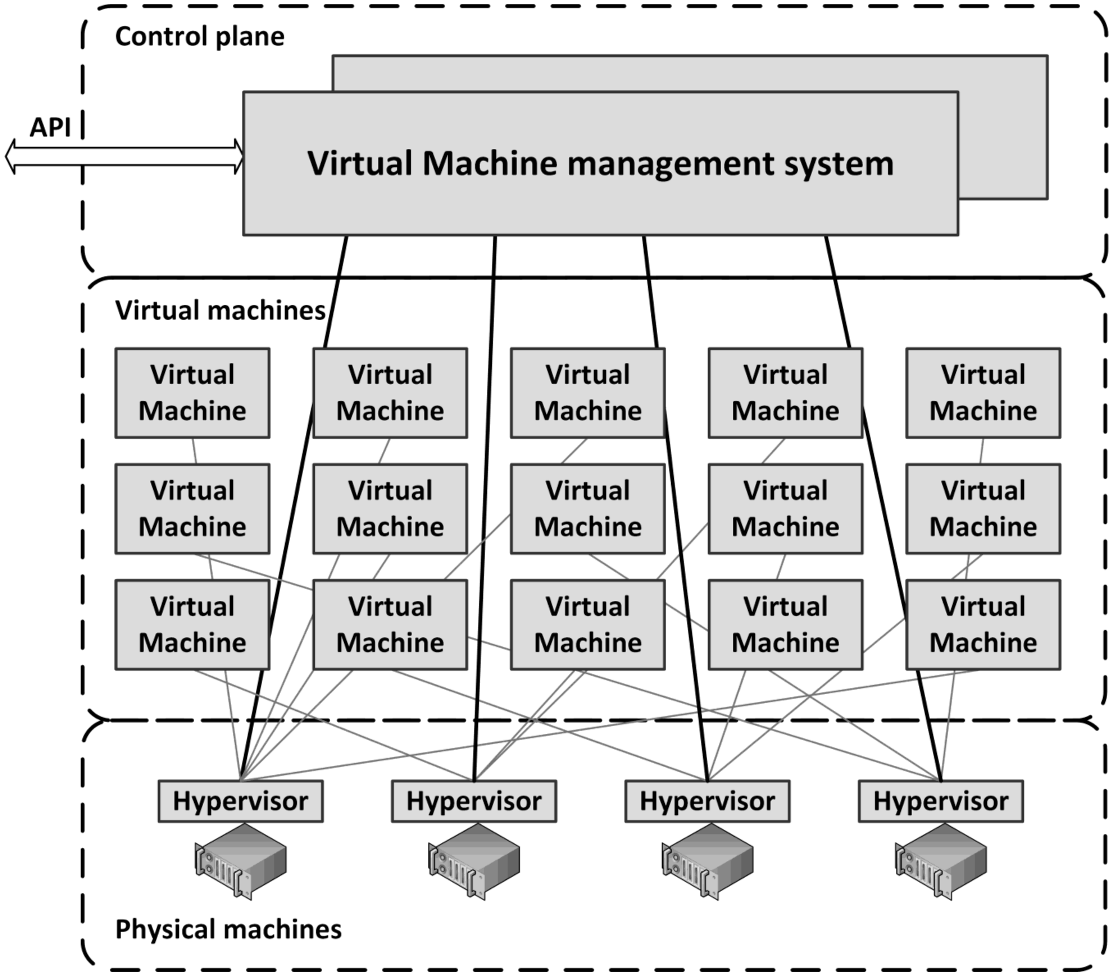
- Cloud-based VMs characteristics
  - There are **general purpose VMs, VMs with extra memory, with extra I/O capacity, with many CPUs**, etc
  - The machines each have a **fixed number of sizes** - there is **no way to choose any number of CPUs or any amount of memory**; there is only a fixed set of sizes to choose from
- Naming can vary:
  - In Azure, VMs are simply called Virtual Machines
  - In GCP, they are VM instances
  - In AWS, the are called EC2 instances

Compute Virtualization vs Public Cloud

	Compute Virtualization	**Public Cloud**
Objective	Aims to optimize resource utilization, improve hardware efficiency and simplify management	Provides scalability, flexibility and cost-effectiveness by allowing users to access resources on demand without needing to manage the underlying infrastructure
Deployment	On-premises or in a public cloud environment	Off-premises, with the provider managing the infrastructure
Virtual Machines (VMs)	Allows users to create, start and stop VMs in a portal, CLI or by calling an API	Cloud based virtual machine ● Azure uses Virtual Machines ● GCP uses VM instances ● AWS uses EC2 instances

Virtual Machine Management

- Virtual machines are typically **managed using one redundant centralized virtual machine management system**
  - Enables systems managers to **manage more machines with the same number of staff**
  - Allows **managing the virtual machines using APIs**
- All physical machines are running a hypervisor and all hypervisors are managed as one layer using management software
- Some virtualization platforms **allow running virtual machines to be moved automatically between physical machines**



- Benefits:
    - When a **physical machine fails**, all virtual machines that ran on the failed physical machine can be **restarted automatically on other physical machines**
    - Virtual machines can automatically be **moved to the least busy physical machines**
    - Some physical machines **can get fully loaded while other physical machines can be automatically switched off, saving power and cooling cost**
    - Enables **hardware maintenance without downtime**
- Disadvantages of computer virtualization:
    - Because creating a new virtual machine is so easy, virtual machines tend to get created for all kinds of reasons
        - This effect is known as "**virtual machine sprawl**"
        - All VMs:
            - **Must be managed**
            - **Use resources of the physical machine**

      - **Use power and cooling**
      - **Must be back-upped**
      - **Must be kept up to date by installing patches**
  - **Introduction of an extra layer in the infrastructure**
    - License fees
    - System managers training
    - Installation and maintenance of additional tools
  - **Virtualization cannot be used on all servers**
    - Some servers require additional specialized hardware, like modem cards, USB tokens or some form of high speed I/O like in real-time SCADA systems
  - **Virtualization is not supported by all application vendors**
    - When the application experiences some problem, systems managers must reinstall the application on a physical machine before they get support

Virtualization Technologies

Emulation	● Can run programs on a computer, other than the one they were originally intended for ● Run a mainframe operating system on a x86 server
Logical Partitions (LPARs)	● Hardware based ● Used on mainframe and midrange systems
Hypervisors	● Control the physical computer's hardware and provide virtual machines with all the services of a physical system ○ Virtual CPUs ○ BIOS ○ Virtual devices ○ Virtualized memory management ● Three types: ○ Binary translation ○ Paravirtualization ○ Hardware assisted virtualization (most used on x86 servers)

Container Technology

- Container technology is a **server virtualization method** in which the **kernel of an operating system provides multiple isolated user-space instance**, instead of just one

- Containers looks and feel like a real server from the point of view of its owners and uses, but they **share the same operating system kernel**
- Developers define the contents of containers
  - Security officers lose control of the containers, which could lead to unnoticed vulnerabilities in a container
- Containers are a balance between **isolation** and **overhead of running isolated applications**
- Virtual machines are isolated from the hardware using special CPU instructions
- Containers don't have that level of isolation
- Benefits:
  - **Isolation**
    - Applications or application components can be encapsulated in containers, each operating independently and isolated from each other
  - **Portability**
    - Since containers typically contain all components the application needs to function, including libraries and patches, containers can be run on any infrastructure that is capable of running containers using the same kernel version
  - **Easy deployment**
    - Containers allow developers to quickly deploy new software versions, as their containers can be moved from the development environment to the production environment unaltered

Container Implementation

Containers are based on 3 technologies that are all part of the Linux kernel:	
Chroot (also known as a jail)	● **Changes the root directory for the current running process** ● Ensures **processes cannot access files outside the designated directory tree**
Namespaces	● Allows **complete isolation of an applications' view of the operating environment** ● Process trees, networking, user IDs and mounted file systems
Cgroups	● **Limits and isolates the resource usage of a collection of processes** ● PU, memory, disk I/O, network

Container Orchestration

- Container orchestration **abstracts the resources of a cluster of machines and**

provides services to containers

- A container orchestrator **enables containers to be run anywhere on a cluster of machines**
    - **Schedules the containers to run on any machine that has resources available**
    - **Acts like a kernel for the combined resources of an entire datacenter**

Example

- Kubernetes is by far the most popular container orchestration framework
- Kubernetes (also spelled as K8S) is an open source project hosted by the Cloud Native Computing Foundation (CNCF), based on Google's internal Borg System
- Kubernetes provides:
    - Replication: to deploy multiple instances of an application
    - Load balancing and service discovery: to route traffic to these replicated containers
    - Basic health checking and repair: to ensure a self-healing system
    - Scheduling: to group many machines into a single pool and distribute work to them
- Public cloud Kubernetes implementation:
    - Amazon Elastic Kubernetes Service (EKS)
    - Azure Kubernetes Services (AKS)
    - Google Kubernetes Engine (GKE)

Serverless Computing

- In serverless computing, **application source code can be run directly by a cloud provider**
- Serverless computing **allows developers to build and run applications and services without having to manage infrastructure**
- The provider **charges based on the actual number of resources used by an application**, rather than charging for pre-allocated amounts of computing resources
- All major public cloud providers offer serverless computing:
    - AWS has Lambda
    - Azure has Azure Functions
    - GCP has Google Cloud serverless
- Serverless **locks the organization into the platform**, as serverless computing often uses special features that are only available on the specific cloud platform

Mainframes

- A mainframe is a **high-performance computer made for high-volume, I/O-intensive computing**

    - **Expensive**
    - Mostly used for **administrative processes**
    - Optimized for **handling high volumes of data**
- **Highly reliable**, typically running for years without downtime
- **Much redundancy** is built in
    - Hardware can be upgraded and repaired while the mainframe is operating without downtime
- Mainframe consists of:
    - Processing units (PUs)
    - Memory
    - I/O channels
    - Control units
    - Devices, all placed in racks (frames)

Mainframe Architecture - PU, Memory and Disks

- In the mainframe world, the term PU (Processing Unit) is used instead of CPU
    - A mainframe has multiple PUs, so there is no central processing unit
    - The total of all PUs in a mainframe is called a Central Processor Complex (CPC)
- Each book package in the CPC cage contains from four to eight memory cards
    - For example, a fully loaded z16 mainframe has four book packages that can provide up to total of 10 TB of memory
- Disks in mainframes are called DASD (Direct Attached Storage Device)
    - Comparable to a SAN in a midrange or x86 environment

Mainframe Architecture - Channels and Control Units

- A channel provides a data and control path between I/O devices and memory
- Today's largest mainframes have 1024 channels
- A control unit is similar to an expansion card in an x86 or midrange system
    - Contains logic to work with a particular type of I/O device, like a printer or tape drive

Channel Types:	
OSA (Open Systems Adapter)	● Connectivity to various industry standard networking technologies, including Ethernet
FICON (Fiber connection)	● The most flexible channel technology, based on fiber optic technology ● With FICON, I/O devices can be located many kilometers from the mainframe
ESCON	● An earlier type of fiber-optic technology

(Enterprise Systems Connection)	● Almost as fast as FICON channels, but at a shorter distance

Mainframe Virtualization

- Logical partitions (LPARs) are the default virtualization solution
- LPARs are equivalent to separate mainframes
- A common number of LPARs in use on a mainframe is less than 10
- The mainframe operating system running on each LPAR is designed to concurrently run a large number of applications and services, and can be connected to thousands of users at the same time
- Often one LPAR runs all production tasks while another runs the consolidated test environment

Midrange Systems

<table>
<tr><td><b>Definition</b></td><td colspan="2">● Positioned between the mainframe platform and the x86 platform
● Built using parts from only one vendor, and run an operating system provided by that same vendor
● This makes the platform:
○ <b>Stable</b>
○ <b>High available</b>
○ <b>Secure</b></td></tr>
<tr><td><b>Evolution (today)</b></td><td>IBM</td><td>● Power Systems series
● Operating system: AIX UNIX, Linux and IBM i</td></tr>
<tr><td></td><td>Hewlett-Packard</td><td>● HP Integrity systems
● Operating system: HP-UX UNIX and OpenVMS</td></tr>
<tr><td></td><td>Oracle</td><td>● Sun Microsystems's based SPARC servers
● Operating system: Solaris UNIX</td></tr>
<tr><td><b>Architecture</b></td><td colspan="2">● Uses multiple CPUs
● Based on a shared memory architecture

<u>Types</u>
<table><tr><td><b>Uniform Memory</b></td><td>● The earliest styles of multi-CPU architectures, typically used in systems with no more than 8 CPUs</td></tr></table></td></tr>
</table>

<table>
<tr><td></td><td><table>
<tr><td><b>Access (UMA)</b></td><td>● The machine is organized into a series of nodes containing either a processor, or a memory block
● Nodes are interconnected, usually by a shared bus</td></tr>
<tr><td><b>Non Uniform Memory Access (NUMA)</b></td><td>● NUMA is a computer architecture in which the machine is organized into a series of nodes
● Each node contains processors and memory
● Nodes are interconnected using a crossbar interconnect
● When a processor accesses memory not within its own node, data must be transferred over the interconnect
○ Slower than accessing local memory
○ Memory access items are non-uniform</td></tr>
<tr><td><b>Symmetric Multi-Processing (SMP)</b></td><td>● UMA systems are also known as Symmetric Multi-Processor (SMP) systems
● SMP is used in x86 servers as well as early midrange systems
● Can be implemented inside multi-core CPUs
○ The interconnect is implemented on-chip in the CPU
○ A single path to the main memory is provided between the chip and the memory subsystem</td></tr>
</table></td></tr>
<tr><td><b>Midrange Virtualization</b></td><td>● Most midrange platform vendors provide virtualization based on Logical partitions (LPARs)
● LPARs are a type of hardware partitioning
○ IBM AIX: Workload / Working Partitions (WPARs)
○ HP: nPARs
○ Oracle Solaris: zones and containers</td></tr>
</table>

x86 Servers

Definition	● A family of instruction set architectures initially developed by Intel commonly used in personal computers and servers ● The x86 platform is the most dominant server architecture today ● Most used OSs are Microsoft Windows and Linux
Vendors	HP, Dell, Lenovo, HDS (Hitachi Data Systems), Huawei
Architecture	● Defined by a CPU from x86 family

<table>
<tr><td></td><td>
<ul>
<li>Integrated with x86 chipset</li>
<li>Architectures:</li>
</ul>
<table>
<tr><td><b>Earlier x86</b></td><td>Uses northbridge / southbridge architecture</td></tr>
<tr><td><b>Platform Control Hub (PCH)</b></td><td>Uses RAM & PCIe data path for direct connection to CPU</td></tr>
<tr><td><b>System on a Chip (SOC)</b></td><td>Direction connection of PCIe lanes, SATA, USB, High Density (HD) video</td></tr>
</table>
</td></tr>
<tr><td><b>Virtualization</b></td><td>
<ul>
<li>Most servers only run one application each, but less efficient use of CPU than midrange</li>
<li>By running multiple OS, each in one virtual machine, on a large x86 server, resource utilization can be improved</li>
<li>The most used products for virtualization on the x86 platform are:
<ul>
<li>VMware vSphere</li>
<li>Microsoft's Hyper-V</li>
<li>Citrix XenServer</li>
<li>Oracle VirtualBox</li>
<li>Red Hat RHEV</li>
</ul>
</li>
</ul>
</td></tr>
</table>

Supercomputers

Definition	The fastest computer architecture designed to maximize calculation speed
Used for	Highly compute-intensive tasks requiring floating point calculations ● Weather forecast calculations ● Oil reservoir 油藏 simulations ● Rendering of animation movies
Evolution	● Cray-1 (1976): For Cray Research, 250 MFLOPS (Million Floating Point Operations per second) ● Cray-2 (1985): For Cray Research, 1,900 MFLOPS ● Nowadays: Ryzen 7950x Zem4 CPU has a peak performance of 1011 GFLOPS; more than 530 times the performance of the Cray-2 ● The fastest computer array is a cluster with 8,730,112 CPU cores, calculating at 1,685,650,000 GFLOPS, running Linux (top500.org)

Quantum Computers

Definition	A computer based on quantum mechanics
Working	Using tiny particles called qubits 量子比特, which can be in multiple states at once and can be connected across vast distances

Compute Availability

Hot Swappable Components	Definition	**Server components that can be installed, replaced or upgraded while the server is running**
	Working	The virtualization and operating systems using the server hardware must be aware that components can be swapped on the fly while it is in operations or in progress, without stopping or pausing the process
Parity Memory	Definition	**Uses parity bit to detect memory failure & data error but no correction**
Error-Correcting Code (ECC) Memory	Definition	**Use Hamming Code or Triple Modular Redundancy (TMR) as the method of error detection and correction**
	Why use ECC?	● **Memory errors are proportional to the amount of RAM in a computer** as well as the duration of operation ● The **likelihood of memory errors is relatively high** and hence they require ECC memory
Virtualization Availability	Uses	**Failover clustering** ● When a **physical machine fails**, the virtual machines running on that physical machine can be **configured to restart automatically on other physical machines** ● When a **virtual machine crashes**, it can be **restarted automatically on the same physical machine**
	Protection	● A **physical hardware failure** ● An **OS crash in a virtual machine**
	Working	● To cope with the effects of a failure of a physical machine, a spare physical machine is needed ○ All hypervisors are placed in a virtualization

		cluster ○ The hypervisors on the physical machines check the availability of the other hypervisors in the cluster ○ One physical machine is running as a spare to take over the load of any failing physical machine

Compute Performance

The performance of computers is dependent on the architecture of the server, the speed of the memory and CPU, and the bus speed			
Moore's Law	Definition	**The no. of transistors that can be placed inexpensively on an integrated circuit doubles approx. every 2 years**	
	However	● Moore's law only speaks of the no. of transistors; not the performance of the CPU ● The performance of a CPU is dependent on clock speed, caches and pipelines, data bus width	
Increasing CPU and memory performance	**Increasing clock speed**	Definition	● **CPU instructions are fetched, decoded, executed and stored to memory** ● **Each step in the sequence is equals to 1 clock tick** ● CPU clock speed is measured in Hertz (Hz) - clock ticks or cycles per second
		Today	● CPUs use clock speeds as high as 6 GHz (6,000,000,000 clock ticks per second) ● But, oscillator (electronic components that generate clock signal) cannot run at this speed ● The oscillator speed is known as the Front Side Bus (FSB) speed
	Cache memory	Definition	**A relatively small piece of high speed static RAM on the CPU**
		Function	**Temporarily stores data received from slower main memory**
		Speed	Cache memory runs at full CPU speed (say 3 GHz), main memory runs at the CPU external

			clock speed (say 100 MHz, which is 30 times slower)
		Nature	• Most CPUs contain 2 types of cache: level 1 and level 2 cache • Some multi-core CPUs also have a large level 3 cache; a cache shared by the cores
	Pipeline	Definition	**While the first instruction is being executed, the second instruction can be fetched**
		Nature	Since that circuitry is idling anyway, creating instruction overlap
	Prefetching and branch prediction	Definition	• **Prefetching is done by the cache memory system** • Using prefetching, **when the first instruction is fetched from main memory, also the second instructions are fetched and stored in cache**, so that when the **CPU needs it, it is already available in cache**
		However	Most programs contain jumps (a.k.a. branches), resulting in cache misses - the next instruction is not the next instruction in memory
		Solution	The **cache system tries to predict the outcome of branch instructions before they are executed by the CPU (called branch prediction)**
	Superscalar CPUs	Definition	**Can process more than 1 instruction per clock tick**
		Working	**Simultaneously dispatches 发送 multiple instructions (through multiple data path) to redundant functional units on the processor**
		Cons	CPU logic more complex
	Multi-core CPUs	Definition	**A CPU with multiple separate cores (multiple processors in a package)**
		Pros	The **cores in a multi-core CPU run at a lower**

			frequency ● **Reduce power consumption** ● **Reduce heat (no hot spots)**
		Today	CPUs with tens or even hundreds of cores
	Hyper-threading	Definition	**A single processor core virtually works as a multi-core processor**
		Pros	**Increase in system performance** by keeping the processor pipelines busier
Virtualization Performance	Problem	● Consolidating multiple virtual machines on 1 physical machine increases CPU usage and reduce CPU idle time ● The physical machine needs to handle the disk and network I/O of all running virtual machines. This can easily lead to an I/O performance bottleneck	
	Selection of host	Factors to choose a physical machine to host virtual machines: ● **Much CPU and memory capacity** ● **Capability of very high I/O throughput**	
	Pros	● **Database servers can easily be migrated to other physical machines without downtime** ● **Management of the servers is unified when all servers run hypervisors**	
	Cons	● Resources required to run the hypervisor ● Reduce performance on virtual machines due to operation transformations	
	Application: Database	● Often one physical server is needed per database ● Databases generally require a lot of network bandwidth and high disk I/O performance ● This makes databases less suitable for a virtualized environment ● Solution: Uses Raw Device Mapping (RDM) allows a virtual machine exclusive access to a physical storage medium	

Compute Security

Physical Security	Physical Server	● **Disable external USB ports in the BIOS** ● **BIOS settings protected using a password** ● Some servers allow the **detection of the physical opening of the server housing** ○ An event can be sent to a central management console using for instance Simple Network Management Protocol (SNMP) traps ○ Enable this to detect unusual activities	
	Data in use (data that actively processed / used)	● Data in use is an important data privacy and security concern ● **Data in use can be protected by implementing a hardware-based Trusted Execution Environment (TEE), which is a secure area of a CPU**	
Virtualization Security	Reason	The use of virtualization introduces new security vulnerabilities of its own	
	To minimize attack	● **Uses firewalls & Intrusion Detection Systems (IDSs) in the hypervisor** should be deployed ● The **virtualization platform itself needs patching (process of applying software updates)** too ● The **size and complexity of the hypervisor should be kept to minimum**	
	To improve virtualization security	De-militarized Zone (DMZ)	● **Uses separate physical machines that run all the virtual machines** ● Pros: Improve **security**, **performance** and **control** ● Cons: **Increases costs and complexity**
		System management console	● The **systems management console connects to all hypervisors and virtual machines** ● If the **systems management console is hacked**, **all virtual machines are affected** ● **Special user accounts and passwords** should be configured for high risk operations ● **All user activity in the systems**

			management console logged

C7: Operating Systems

Popular Operating Systems

Definition	**A set of programs that controls all the other programs in a computer**	
Function	Provide services to applications in the form of Application Programming Interfaces (APIs), e.g.: ● **File management** ● **I/O interfaces (like video and keyboard)** ● **Hardware drivers (like printer drivers)**	
Popular Operating Systems	IBM z/OS	● The most used mainframe OS ● Typical use of z/OS: ○ Batch processing: read & write large amounts of data & perform relatively simple calculations on it ○ Interactive users: supports thousands of interactive users
	IBM i (OS/400)	● An OS only used on IBM's Power Systems midrange systems ○ The operating system was previously known as OS/400 ○ The midrange system was previously known as AS/400 ● Advantages include: ○ Communications ○ Transaction processing ○ Relational database manager ○ Features for the implementation and maintenance of data security ● The latest version is "IBM i 7.5", released in 2023
	UNIX	● Uses hierarchical file system with nested subdirectories - the directory tree ● UNIX - file system ○ All files and directories appear under the so-called root directory "/" ○ UNIX has no concept of drive letters, like Windows or DOS ● UNIX - system tools ○ To perform complicated tasks commands can

		be combined using a system called pipes
	Linux	● Linux commands, file structure, scripting language, pipes are almost similar to those of UNIX ● Almost all internet services run on Linux ● LINUX - GNU / LINUX ○ The GNU project was launched in 1984 by Richard Stallman ○ Combining Linux with the GNU system resulted in a complete OS: the GNU / Linux system ○ Linux and the GNU tools are licensed under the GNU General Public License ● LINUX - Distribution ○ Vendors compiled the Linux source code, added some tools and configurations of their own, and releasing it in a distributable format ○ Best-known Linux distributions: Red Hat, SuSe, Ubuntu, Debian ● LINUX - Support ○ Linux can be downloaded from the internet for free ○ Most organizations demand professional support for their software ○ Professional support is not free ○ Most Linux distribution vendors, like Red Hat and SuSe, and some independent vendors, offer support contracts for Linux ● BSD ○ Berkeley Software Distribution (BSD) is a UNIX operating system derivative ○ BSD was the basis for 3 open source development projects: ■ FreeBSD (Most widely used, a complete operating system) ■ NetBSD (Ported to 57 hardware platforms across 15 different processor architectures, often used in embedded systems) ■ OpenBSD (Most secure BSD version, developers audit the source code for software bugs and security problems)
	Windows	● A popular x86 operating system, used on PCs and servers

		● Microsoft provides a fairly complete stack of business solutions like SharePoint, BizTalk, SQL Server and Exchange ● They also provide development environment (Visual Studio and the .Net framework) ● Microsoft Azure cloud runs on a slimmed down version of Windows ● Many organizations have a "Microsoft unless" strategy ○ Software is purchased from Microsoft or built using Microsoft tools, unless there is no solution from Microsoft available ● Windows for desktop ○ 1985: Windows 1.0 ○ 1987: Windows 2.0 ○ 1990 - 1992: Windows 3.x ○ 1995: Windows 95 ○ 1998: Windows 98 ○ 2000: Windows 2000 ○ 2001: Windows XP ○ 2006: Windows Vista ○ 2009: Windows 7 ○ 2012 / 2013: WIndows 8 / 8.1 ○ 2015: Windows 10 ○ 2021: Windows 11 ● Windows for server ○ 1992: Windows NT 4.0 server ○ 2000: Windows 2000 server ○ 2003: Windows server 2003 ○ 2016 and onwards: Windows server 2016, 2019, 2022, 2025 ● Windows Support ○ Windows is closed source software: Users are dependent on Microsoft for support and updates ○ Users must follow updates and software upgrades to get support ■ Extended support is sometimes possible, but at a price ■ This leads to frequent (and usually costly) upgrade projects
	MacOS	● It comes preinstalled on every Macintosh computer ● Cannot be run on any other hardware

		● Under the GUI, it uses BSD UNIX as its code base
	OS for mobile devices	● iOS is the OS for Apple's iPhone and iPad mobile devices, based on macOS ○ iOS introduced the concept of the App Store ○ iOS introduced a user interface based on direct manipulation using multi-touch gestures such as swiping, tapping and pinching ● Android is an open source mobile OS based on Linux ○ Google's version (most widely used) is proprietary because it comes with additional proprietary closed-source software preinstalled ○ Android applications can be installed from the Google Play Store
	Special purpose operating systems	● Some OSs are created for special purposes, like: ○ Firewalls ○ Intrusion detection and prevention systems ○ Routers ○ Phones ○ ATM machines ○ Media centers ● Based on existing operating systems: Linux or Windows ○ Stripped of all unneeded features ● A special type of OS is a real-time OS (RTOS) ○ Guarantee to perform tasks in a predefined amount of time ○ Used where handling events within a predefined time is critical

OSs Building Blocks

Building Blocks	Kernel	The kernel is the heart of an OS ● **Starts and stops programs** ● **Manages the file system** ● **Scheduler access to hardware to avoid conflicts for simultaneous accesses** 调度访问硬件，避免同时访问时发生冲突
	Drivers	Drivers are **small applications that connect specific hardware devices to the kernel**

	Utilities	Utilities are applications that are considered part of the OS ● **User interfaces** ● **Logging tools** ● **Editors** ● **System update processes**
	Applications	Applications consist of **one or more processes that communicate with the OS using system calls that are invoked through Application Programming Interfaces (APIs)**
OS Functions	Process scheduling (process or management)	● **OSs schedules each process to run only during a short time frame** ● Process scheduling is **fairly complex** ○ Must be **well-balanced** ○ **Switching processes introduces some overhead** ○ The **scheduling algorithm guarantees each process gets fair CPU time**
	File systems	● The OS provides a file system to application ○ File systems consist of directories (a.k.a. folders) with files or other directories ● The OS: ○ **Handles individual disk blocks or communication with a SAN or NAS** ○ **Manages the files and the directory structure** ○ **Security**: permission to read, write, create and delete files and directories ● Most OSs handle multiple types of file systems on multiple disks at the same time ● Popular file systems are: ○ FAT (File Allocation Table), vFAT, and FAT32: used in MS-DOS ○ NTFS (New Technology File System): used in Windows ○ UFS (Universal File System) & VxFS (Veritas File System): used in UNIX ○ Ext (and Ext2, Ext3, Ext4): used in Linux ● Journaling file systems (keep track of changes made to files in a journal log), facilitate higher availability and fast recovery in case of a malfunction ● File systems must be mounted before they can be used by the OS ○ A disk and the file system must be recognized by the OS and attached to it

		○ After mounting, the file system is typically given either: ■ A drive letter (Windows) ■ A drive name (OpenVMS) ■ A mount point in the global directory tree (UNIX and Linux) ● Most OSs provide file sharing functionality ○ Enables files on one system to be accessed by (users on) other systems ○ File sharing protocols: ■ NFS: originates from UNIX ■ SMB/CIFS: originates from Windows
	APIs and System Calls (device management)	● System calls are **programming functions that provide a hardware-independent interface to tasks the OS can perform for applications** ● The OS takes care of: ○ **Look-up the file in a file allocation table** ○ **Look up the disk blocks on disk** ○ **Instruct the disk controller to fetch the needed disk blocks** ○ **Copy the disk blocks to memory** ○ **Provide a pointer to the disk blocks in memory** ● System calls are grouped and presented to application processes as Application Programming Interfaces (APIs) ● APIs describe the available system calls in an OS and how they can be used ● Each OS has its own API ○ UNIX and Linux use the POSIX standard ○ Windows has its own API
	Device Drivers	● The OS manages all hardware ● I/O devices are controlled using device drivers ○ **Interact with the device's hardware** ○ **Provide an Application Programming Interface (API) to the OS**
	Memory Management	● The OS: ○ **Allocates and de-allocates memory on behalf of applications** ○ **Manages when the amount of requested memory exceeds the physical amount of memory** ● Memory management includes: ○ Cache management ○ Paging

		○ High volume data transfers ○ Memory management units (MMUs) ○ Thin memory provisioning (memory overcommitting) ○ Direct Memory Access (DMA) ● The OS takes care of all of this and just provides chunks of memory to applications ○ **Direct Memory Access (DMA)** ■ Allows devices to access main memory directly without CPU assistance ■ It frees up the CPU to perform other tasks ○ **Paging and swapping (memory management techniques)** ■ Paging: a process's virtual address space is divided into blocks called pages ● When main memory is low, pages can be moved from main memory to disk, called "paging out" ● When a process needs a page that is paged out, it is read from disk and put it back into main memory, a process called "paging in" ■ Swapping: Entire processes are moved between main memory and disk ■ Paging is usually not a problem, but swapping should be avoided as much as possible. Swapping makes the system extremely slow
	Shells, CLIs, and GUIs	● Shell provides a UI to the OS: to launch other programs by end users or scripts ● Two types of shells: ○ **Command-Line Interfaces (CLIs)** ■ The user types commands on a keyboard on a command-prompt ■ e.g. UNIX shells (bash, sh, csh) and Windows' cmd.exe (a.k.a. DOS box) ○ **Graphical User Interfaces (GUIs)** ■ The user uses a mouse to click on icons or buttons ■ e.g. Microsoft Windows and X Windows (UNIX and Linux)
	Operating System Configurati	● **The configuration of an OS is stored in an OS specific database or in text files** ● e.g.:

	on	○ Windows registry ○ Files in the Linux /etc directory ○ AIX Object Data Manager (ODM) database ● For most used configuration parameters, user-friendly tools are provided ○ These tools still edit the text files, but that is hidden from the user

Operating System Availability

Failover Clustering

Definition	● A **group of independent servers running identical OS** (a.k.a. "nodes") ● **Controlled by cluster software running on the nodes** ● A **group of interconnected servers** (a.k.a. nodes), that **work together to ensure continuous operation of applications and services** ● **If one node fails, another node automatically takes over the workload, minimizing downtime**. This process is called failover.
Benefits	Provides **high availability to applications** by **managing running application within a node as a package of application components**, called a resource pool or an application package
Working	● A resource pool is the single unit of failover within a cluster ● It contains: ○ Application name and identifier ○ Start script for the application ○ Stop script for the application ○ Monitor script for the application ○ Virtual IP address the application can be addressed with ○ Mount points for storage - the disks that must be available to the application
Cluster Software Products	● Parallel Sysplex - for IBM mainframes ● HACMP - for IBM AIX UNIX ● MC/Service Guard - for HP-UX UNIX ● Windows Cluster Service - for Microsoft Windows ● Heartbeat and Pacemaker - for Linux
Components	● A **cluster network** consists of **redundant physical Ethernet connections**, **carries heartbeat between all nodes in the cluster**

	● A **heartbeat allows nodes to detect the unavailability of nodes** by regularly **sending packets to each other's network interfaces** ● **Monitors the health of the OS and applications running on the node**
Shared Storage	● All nodes are able to **access data on shared storage**, via: ○ **Shared nothing clustering**: Every individual disk is mounted to one active application only at any given time ○ **Distributed Lock Management (DLM) clustering**: Each cluster node can access the same resource (e.g. disk), at the same time. A lock mechanism is responsible to manage data to avoid corruption
Configuration	● In a cluster, every active application has a standby counterpart available on a passive node ● After a failover, this standby application becomes active and provides service to clients ● The passive node should have enough capacity to run the failed-over application without performance degradation ● In case of a server crash or a power outage, all applications running on that server node will not be brought down cleanly ● When the applications are restarted on another node in the cluster, standard crash recovery should take place. The file system must take care of performing necessary code file system checks before mounting, and the application must perform its standard recovery on startup
Spare Node	● **N+1 cluster** ○ A **spare node could be added to a cluster to handle failovers**. N represents the **number of nodes with active applications** ○ In larger cluster, N+2 or N+3 can provide more redundancy ● **N to N cluster** ○ There is **no spare idle node**, but **each node has some spare capacity to host additional application in case of a failover** ○ Pros: ■ The **available hardware is always used** ■ **All memory and CPU cycles in the OS can be used by all running applications** ○ Cons: ■ When a **failover** occurs, **less memory and CPU cycles are available** to the applications, possibly leading to some **performance degradation**
Problem	● When a cluster with an even number of nodes (most clusters contain

(Cluster Failure)	two nodes) nodes are disconnected from each other, the status of the other nodes is unknown to each node. This means that one of two situations occurs: ○ Each node decides that the other node must be down, so each node decides to be the new active node in the cluster (leading to a so-called split-brain situation) 每个节点都认为另一个节点肯定宕机了，因此每个节点都决定成为集群中新的活动节点（导致所谓的 "分脑 "情况） ○ Each node decides that it has lost contact with the active cluster, so both nodes decide to stop (effectively bringing down the cluster) 每个节点都认为自己与活动集群失去了联系，因此两个节点都决定停止活动（实际上导致集群瘫痪 ）
Solution (Voting and quorum disks)	● A voting mechanism **determines which part of the cluster is faulty and which part of the cluster is working properly** ● A quorum disk is a **virtual third node used in a two-node cluster** (due to no majority). It **acts as one vote in the voting system and always assigned to one (and only one) node at any time** ● A **faulty node releases it quorum assignment automatically** ● The **working node gets two votes: one from itself, the other from the quorum disk** ● The **faulty node will stop working, because it has only one vote**
Cluster-aware applications	● Cluster-aware applications run active instances on multiple nodes ● E.g.: ○ Oracle RAC (Real Application Cluster) ○ Microsoft SQL Server Always On Failover Cluster ○ Microsoft Exchange Server ○ Enhances switch-over times in case of a failure ● In case of a failure, the application does not need to be started on another node before it can service clients ● Cluster-aware applications provide scalability in addition to high availability ● Client requests can be distributed among multiple cluster nodes ● Handle increased demand and traffic by adding additional nodes to the cluster

Operating System Performance

Factors Affects the Performance of an OS	● **The performance of the underlying hardware** ● **The type of load generated by the applications** ● **The configuration of the operating system itself**

To improve OS's performance	**Increase memory**	● An **OS should have enough memory to run all applications needed at any time** ● When an application needs more than the available memory, memory is freed 释放 by: ○ **Paging**: Moving less used memory pages to disk ○ **Swapping**: When memory is really low, moving an entire application's allocated memory to disk ● When memory is really low, moving an entire application's allocated memory to disk: ○ Swapping ○ Runs the performance of an operating system ○ Data stored on disk is at least three orders of magnitude slower than data stored in RAM memory ○ Swapping must be avoided at all time ■ Increase memory ■ Run less (demanding) applications ● **Increasing memory** benefits the operating systems' performance ● All memory not used by applications is used to cache disk blocks ○ This is the main reason why the performance of OS usually increased when memory is added ● OSs use highly sophisticated algorithms to optimize disk caching ● Tweaking the memory management system of an operating system provides little benefits
	Decrease Kernel Size	● Some operating systems (like UNIX and Linux) allow **tuning kernel parameters of the OS** ● **Unused features (like support for IPv6 or floppy disk drives) can be switched off for a smaller kernel size** ● To create a smaller kernel, the **kernel must be recompiled or re-linked** 重新编译或重新链接内核. This is a **highly automated, low risk operation** on most UNIX and Linux systems ● A restart of the OS is needed after a kernel rebuild ● Not all operating systems allow rebuilding the kernel. For instance, the Windows kernel cannot be rebuilt ● A smaller kernel has the following benefits:

		○ It simplifies the kernel: ■ **Lower risk of crashes** ■ **Smaller security attack surface** ○ The kernel must be in memory at all times: ■ **It cannot be pages or swapped-out** ■ **A smaller kernel will free up memory for applications and disk caching** ○ Switched-off features don't need patching to keep them up-to-date ○ The OS starts faster when the kernel is small

Operating System Security

Patching	● **OS vendors provide small software updates called patches**, to / for: ○ **Fix bugs or design flaws** ○ **Close security holes** ○ **Small improvements** ● In general, patches come in three categories: ○ **Regular patches**: To fix low priority software bugs ○ **Hot-fixes**: Repairs a bug or flaw in the OS that needs to be fixed fast. Used to close a security hole or to fix an error introduced by another patch or service pack ○ **Service packs** (a.k.a. support packs / patch packs): A collection of patches / hot-fixes / new functionality that are packed together and can be installed in one deployment ● It is good practice to **install all patches as soon as possible** ● **Test them before deployment in production** ○ They could introduce unwanted effects in the infrastructure ● **Patches hot-fixes and service packs are provided with release notes**: ○ They describe what changes are made to the operating system ○ Read release notes before installing the patch ○ When a patch or hot fix does not have impact on a specific deployment, it can be discarded
Hardening	● A step by step process of **configuring an OS to protect it against security threats** ● The OS is reduced to support only essential services & processes ○ **Unnecessary protocols and subsystems are switched off** ○ **Unused user accounts are removed or disabled** ○ **All new / relevant hot-fixes, patches and service packs are applied** ● Harden all OSs in the infrastructure using a hardened OS configuration

	template ○ This template is used to instantiate new OSs ○ Ensure security is optimal and is consistent in all deployments
Virus Scanning	● Windows, Linux and end user OSs are vulnerable to viruses ● Virus scanners can have an impact on the performance of the OS ○ The **virus scanner must be configured to only scan high risk files and directories based on a risk analysis**
Host-Based Firewalls	● Most OSs provide a built-in host-based firewall ● A host-based firewall is a software firewall ● **Host-based firewalls typically block all incoming network traffic** ● **Rule sets define the type of traffic is allowed to communicate with the OS, based on:** ○ **Source and destination IP address** ○ **TCP and UDP port** ○ **The running process sending and / or receiving the network traffic**
Limitations of User Accounts	● **OSs have local user accounts that can login to the OS** ● Most OSs also have a **special super user account** called "root", "supervisor", "admin" or "administrator" ○ These accounts **have almost unlimited power** ○ **Used only to provide permissions to user account** ○ It should be possible to do all work using a user-bound account with sufficient rights
Hash Passwords	● **OSs should only store hashed passwords** ○ **When a user logs in, her password is hashed** ○ **The hashed password is compared to the stored hash** ○ **If the two are equal, the login succeeds** ● **No way to extract the original password from the hashed one**

C8: End User Devices

End User Devices Building Blocks

Desktop and Laptop	Desktop	Pros: ● **Cost-effective** ● **Simple solutions** ● **Complexity of the PC itself** ● **Very advanced OSs** ● **The amount of locally installed software** ● **The performance, availability and security issues related to all of these aspects**
	Laptop	● Laptops connected to a docking station (a.k.a. port replicator) using a USB-C cable ○ **Docking station**: **Provides external ports** for connecting a keyboard, mouse, camera, speakers and microphone, as well as one or more displays ○ **USB-C cable**: **Charge the laptop's battery & connect to the docking station**
Mobile Devices	● Devices that **connect to the IT infrastructure using wireless public or off-site Wi-Fi networks** ● Typical mobile devices are: ○ Smartphones and tablets ○ Cars ○ Smart watches ○ Music players ○ Digital cameras ● Computing power of mobile devices is getting comparable to desktop and laptop computers ● Specific properties: ○ Connect to the IT infrastructure using public networks ■ UMTS or LTE technology ■ Low bandwidth connectivity ■ Fluctuating connection speed ■ Low reliability of connections ○ Small form factor (screen, keyboard) ■ Applications' user interfaces must be re-engineered to handle these smaller sizes	
Bring Your	Definition	● **Allows people to bring personally owned, mobile devices to the office**

Own Device (BYOD)		● **Accesses the organization's applications, data & personal applications and data**	
	Conflicts	Organization	● **Stability** ● **Security** ● **Control**
		Worker	● **Freedom** ● **Privacy** ● **Control**
	Policy and Security Measures	Policy & Training	● BYOD policy **outlining acceptable devices, security protocols and data usage** ● **Training on secure practices and potential risks** is essential
		Mobile Device Management (MDM)	● **Allows remote management of devices** ● **Enforces password complexity, data encryption and remote wipe capabilities** in case of device loss or theft
		Secure Applications	**Accesses organization applications designed with robust security features** like **multi-factor authentication** and **data encryption** in transit and at rest
		Separation of Work & Personal Data	**Encouraging the use of separate work profiles on personal devices** or **dedicated devices for work** purposes can **minimize the risk of data breaches**
Printers	Laser Printers	● **Produce high quality text and graphics using toner** ● Color printers uses four toners	
	Inkjet Printers	● **Create text and graphics by propelling droplets of ink onto paper** 将墨滴喷射到纸上，创建文字和图形 ● Benefis: ○ **No warm up time** ○ Use much **less energy** ○ Relatively **cheap** ○ Produce **high quality printouts**, usually in color ○ Can be used to **produce wide format printing**	
	Multi-Functional	● An office device that acts as a: **Printer + Scanner + Photocopier + Fax machine**	

	Printers	● Provides **centralized document management and production in an office setting**	
	Specialized printers	Dot Matrix Printers	● **Characters are drawn out of a matrix of dots** ● **Prints one line of text at a time**, **character-by-character** ● **Noisy** due to hammer-like mechanism in the print head ● **Uses continuous fanfold paper** rather than cut-sheets 使用连续折叠纸张，而不是裁切纸张
		Line Printers	● **High speed printers that print one complete line of text at once**
		Thermal Printers	● **Uses heating thermal paper and thermal print head** ● Thermal printers are **quiet**, **fast**, **small** and **low power** ● **Outputs are not durable**

Desktop Virtualization

Application Virtualization	**Isolates applications from some resources of the underlying OS and from other applications** 将应用程序与底层操作系统的某些资源和其他应用程序隔离开来
Server Based Computing (SBC)	● SBC is a concept where **applications and / or desktops run on remote servers** ● **Many users share the resources (OS, CPU and RAM)**
Virtual Desktop Infrastructure (VDI)	● Similar to SBC ● All **large public cloud providers offer VDI environments as a service, with a pay per use** ● Pros: ○ **Each user has exclusive use of the OS, CPU and RAM** ● Cons: ○ VDI tends **not to scale well in terms of CPU resources and storage IOPS** ○ **Each client uses an entire virtual machine**
Thin Clients	● **Uses resources housed inside a central server** ● **Connects to a server for applications and data** ○ **Zero client**

	■ Has **limited hardware**, often **consisting of a processor, memory and network interface** ○ **Preboot eXecution Environment (PXE) boot** ■ It **allows desktop PCs / thin clients to boot from an OS disk image stored on the network** instead of from a local hard disk ■ An **active network connection is needed** ■ **Implementing a high performing TFTP server** is crucial for fast start-up times (Trivial File Transfer Protocol) server is a server that uses the Trivial File Transfer Protocol to transfer files over a network, serving as a lightweight, simplified version of the File Transfer Protocol (FTP).)

End User Devices Availability

Reliability	● To keep the cost low, they are designed to last only 3 to 5 years ● Mobile devices physically damaged quite easily which may lead to downtime for a user ● Quality Components: **Ensure devices are equipped with high-quality components** ● Regular Maintenance: **Conduct routine maintenance, including cleaning, dusting and checking for physical damage** ● Redundancy: **Consider using redundant components**, such as **dual power supplies** or **redundant network connections**, to improve reliability

End User Devices Performance

- PCs and laptops:
  - **Add more RAM** increases the performance more than choosing a faster CPU
  - A **faster disk**, preferably an **SSD disk**, can positively affect the performance
- **Make sure enough bandwidth is available** for each end user device

End User Devices Security

- Securing end user devices is quite a challenge, due to:
  - They are not located in a locked down datacenter
  - They are spread around offices, homes and client locations
- Solutions:

General	● Provide **laptop cable locks to prevent theft** ● **Malware protection software (virus scanner)** be installed on each device ● **For the devices at the end-of-life / need repair, erase the hard disk first** ● **Encrypt the full hard disk**
Mobile Device Management (MDM)	● Used to **monitor, maintain and secure devices that are not regularly connected to the organization's network** ● **Allow systems management to remotely erase the device's content** ● Can **install software to locate the stolen device**
End User Authorization and Awareness	● End users should: ○ **NOT remove / install / alter system files / log files / software** ○ **NOT have the administrator password of their device** ● **BIOS password** ○ To further increase security ○ To **prevent booting from USB sticks** ● Common security guidelines including: ○ The possibility of **social engineering** (an attempt to trick someone into revealing info) ○ Use **strong passwords** ○ **Know how to handle sensitive data**
Network Access Control (NAC)	● Used at the network end points, where end user devices (like laptops) can be connected to the network ● It **allows predefined levels of network access** based on: ○ A **client's identity** (is the laptop known to the organization?) ○ The **groups to which a client belongs** ○ The **device complies with the organization's governance policies** ● If a client device is not compliant, NAC provides a mechanism to **automatically bring it into compliance**, e.g.: ○ **Installing the latest virus scanner updates** while connected on an isolated LAN segment ○ **After the update finishes, access is granted** to the rest of the network

C9: Infrastructure Management

Infrastructure Deployment Options

On-Premises

Definition	**You own and manage all the hardware and software in your own data center**
Building must have	● Enough space ● An uninterruptible power supply (UPS) ● Options to install sufficient cooling ● Fire prevention and detection ● External redundant network capabilities with enough bandwidth ● Sufficient floor loading capacity
Pros	● **High control** ● **High security**
Cons	● **High costs** ○ Setting up on-premises infrastructure requires **significant investment in hardware, software license and IT staff** to manage everything ○ On-premises infrastructure **require ongoing maintenance and upkeep** such as hardware upgrades, software updates, security patching, and power and cooling costs ○ **Companies can become locked into specific hardware and software vendors** due to compatibility and integration challenges. This can limit flexibility and potentially inflate costs when upgrades and changes are needed ● **Poor scalability** ○ Scaling on-premises infrastructure up or down can be **difficult and time-consuming** ○ **Adding new servers or storage** requires **physical installation and configuration** ○ **Deploying new applications or services can be slow** due to the **physical infrastructure limitations** and the need for **manual configuration** ● **Limited redundancy and disaster recovery** ○ A **single point of failure** is a risk with on-premises hosting. If a server or storage device fails, downtime can be significant ○ **Implementing robust disaster recovery solutions adds to the complexity and cost**

	● **Security concerns** ○ Securing an on-premises infrastructure **requires dedicated IT security expertise** ○ **Businesses need to invest in firewalls, intrusion detection systems and skilled personnel** to manage them, increasing the overall security burden

Public Cloud

- You **rent computing resources (servers, storage, etc) from a cloud provider** like Amazon AWS, Microsoft Azure or Google GCP
- It is **cost effective** and **scalable**, but **security and control are limited**
- Depending on the deployment model chosen, the organization delegates more or less systems management
- With IaaS, the organization has to do most of the management itself, while with SaaS it has to manage the least
- In case of **green field situation (startup company)**, **hosting the entire virtual infrastructure in the public cloud** could be a viable option
- Public cloud can bring innovative technology
  - **Cloud providers can innovate much faster than most other organizations**
  - **Customers can easily take advantage of these innovations**
  - **Innovations become available quickly, and are immediately production-ready**

Deployment Model	**Organization**	**Cloud Provider**
Infrastructure as a Service (IaaS)	● Operating System ● Application ● Data ● User Access	Other parts of infrastructure
Platform as a Service (PaaS)	● Application ● Data ● User Access	Infrastructure
Software as a Service (SaaS)	● Data ● User Access	Infrastructure

Private Cloud

- Similar to on-premises, but the **infrastructure is dedicated to your organization and**

can be hosted by a provider

- **Offers high security and control**, but still **requires significant investment**
- A private cloud is not a cloud in the pure sense of the word
    - It **has limited scaling**
    - **No pay per use**
- A private cloud a.k.a. software-defined datacenter (SDDC), is an architecture all infrastructure resources - compute, storage and networking - are virtualized, and **can be configured using software APIs**
- An SDDC is an extension of an enterprise infrastructure. All resources are virtualized and managed by SDDC automation and orchestration software
- Private cloud software is comparable to IaaS services of public clouds
- A private cloud is characterized by:
    - **Automation**
    - **Orchestration** 协调
    - **Abstraction of resources into software and code**
- Changes are managed by an automated workflow
- An **orchestrated change can lead to a number of automated changes in various resources**
- Developers, DevOps teams and systems managers can **create and deploy new infrastructure** using:
    - A manual self-service portal
    - A combination of a build server and APIs
- Allows the user to request:
    - **Desired infrastructure components**
    - **Their sizing to meet performance demands**
    - **Their required availability**
- Private cloud software provides tools for:
    - **Costing**
    - **Logging**
    - **Reporting**
    - **Scaling (up and down)**
    - **Decommissioning of the infrastructure resources** 基础设施资源退役
- Examples of private cloud automation and orchestration products:
    - OpenStack Horizon
    - IBM Cloud Orchestrator
    - VMware vRealize

Hybrid Cloud

- **Combines public and private cloud** for a mix of benefits
- You can **store sensitive data in the private cloud** and **use the public cloud for non-critical tasks or scaling needs**
- **Offers flexibility** but can be **complex to manage**

- Most organizations choose not to migrate all of their existing infrastructure to the public cloud at once
  - **Complex infrastructure components cannot be moved overnight**
  - **Not cost effective to migrate an entire datacenter as-is via a lift and shift migration** 通过提升和转移来迁移整个数据中心的成本效益不高
- A **phased approach** is often taken. Some of the infrastructure remains on-premises and some is migrated to the public cloud
- A **connection must be established between the on-premises datacenter and the public cloud provider**. This is called a hybrid cloud
- A hybrid cloud often remains in place for several years, because it take a long time to completely phase out the on-premises environment for a variety of reasons
- Some drawbacks of a hybrid cloud are:
  - **Knowledge of both the existing on-premises environment and the new cloud environment must be present and maintained**
  - There is a **combination of pay-as-you-go costs in the cloud and investment and licensing costs in the on-premises environment**

Infrastructure Automation

Definition	The use of technology to **automate tasks traditionally performed manually by IT professionals when managing and provisioning IT infrastructure**	
Benefits	• **Increased efficiency** (No need to hire many staff) (e.g. self drive truck / car / bus) • **Reduced errors** • **Improved scalability** (can easily expand based on user needs) • **Enhance agility** (Easily break down the server into many portions) • **Reduced costs**	
Common IT Infrastructure Automation Tools	**Configuration Management Tools**	• These tools **automate the configuration of servers, network devices and other infrastructure components**, ensuring **consistency across your environment** • These tools **constantly checking your IT systems** against a set of blueprints • If **anything deviates 偏离 from the desired state** (e.g. software missing, a setting changed), the **tools fix it automatically**
	Infrastructure as Code (IaC)	• IaC **treats infrastructure like software code**, allowing you to **define configurations in code files** and **automate deployment and management**

		● Terraform is an open-source Infrastructure as Code (IaC) tool developed by HashiCorp ● It allows you to define and manage your infrastructure across various platforms (cloud providers, on-premises data centers) in a human readable configuration language called HashiCorp Configuration Language (HCL) or optionally JSON	
		Version Control ● **Keep track of changes to software code over time** ● **Files of software code are stored in repositories** ● Repository **automatically created a new version of the code when code is pushed to the repository** ● Git, GitHub and GitLab are the most widely used tools for version control ○ Git: distributed version control system with a standalone command line interface ○ GitHub: web-based platform for hosting Git repositories ○ GitLab: provides features similar to GitHub, but can be self-hosted	
	Orchestration Tools	● **Coordinate and automate complex workflows involving multiple IT infrastructure components**	
		Workflow Automation	● Orchestration tools **automate complex IT workflows involving multiple infrastructure components** ● This can involve tasks like provisioning servers, configuring software, deploying applications and scaling resources
		Dependency Management	● They **manage dependencies between different tasks in a workflow** ● If one task fails, the tool can handle retries, rollbacks or alternative execution paths to ensure overall workflow success

		Resource Coordination	- These tools **coordinate the use of various resources across different platforms** (cloud providers, on-premises infrastructure) - They ensure resources are allocated, configured and released efficiently
	Cloud Management Platforms (CMPs)	- For cloud environments, CMPs **provide a centralized platform to automate tasks** like provisioning, monitoring and managing cloud resources	

Infrastructure Documentation

- Documenting an IT infrastructure is essential for **maintaining a reliable, secure and effective IT environment** - **Valuable knowledge about the IT infrastructure can be lost** when **systems managers leave the organization**. Documenting **preserves this knowledge and allows it to be transferred to new team members** - Documentation shows **how an infrastructure is configured** and **how it is supposed to work**. This helps with **troubleshooting and maintenance tasks**. In the event of a disaster, it helps ensuring that the **infrastructure can be restored to its previous state** as quickly as possible	
Configuration Management Database (CMDB)	- CMDB is an inventory of all hardware, software and networking components in the infrastructure - For each components, it should include make and model, location and function - Many CMDB tools provide the ability to correlate components. This can be very helpful when making changes or finding the root cause of an application failure - A CMDB is needed as a basis for Information Technology Infrastructure Library (ITIL) processes. It should be kept up to date as much as possible, using automated tools if possible
Diagrams	- A topology diagram shows the relationships between different components and how they are connected - There is no widely accepted formal standard for documenting IT infrastructures. Microsoft Visio or Diagrams.net diagrams are popular tools - ArchiMate is an open and independent standard for enterprise

	architecture modeling ● In simpler terms, it is a language that helps describe, analyze and visualize the structure and behavior of an organization's IT systems, business processes, information flows, and other core components
IaC Tools	● Automation tools can be used as a way to document how the infrastructure is built and the reasons behind certain decisions ● Pros: ○ It can be done during modifications to the IaC code ○ For any future changes, the documentation in the code can easily be updated immediately ● Cons: ○ The code must be read to get an understanding of the architecture of the infrastructure ○ It does not provide you with an instant overview of the setup, like diagrams do

Documenting Procedures

At a minimum, written procedural documentation should include:

- Procedures for routine tasks, such as software updates
- An infrastructure naming convention that describes how infrastructure components should be named
- An IP addressing plan that shows how IP addresses are distributed to devices based on the network architecture
- A DNS naming convention that describes how DNS records should be named in the various network segments, such as internal DTAP segments and the DMZ
- A fallback procedure that describes how to perform a fallback of the infrastructure to the secondary datacenter
- A disaster recovery plan
- Backup and recovery procedures