Cloud Computing

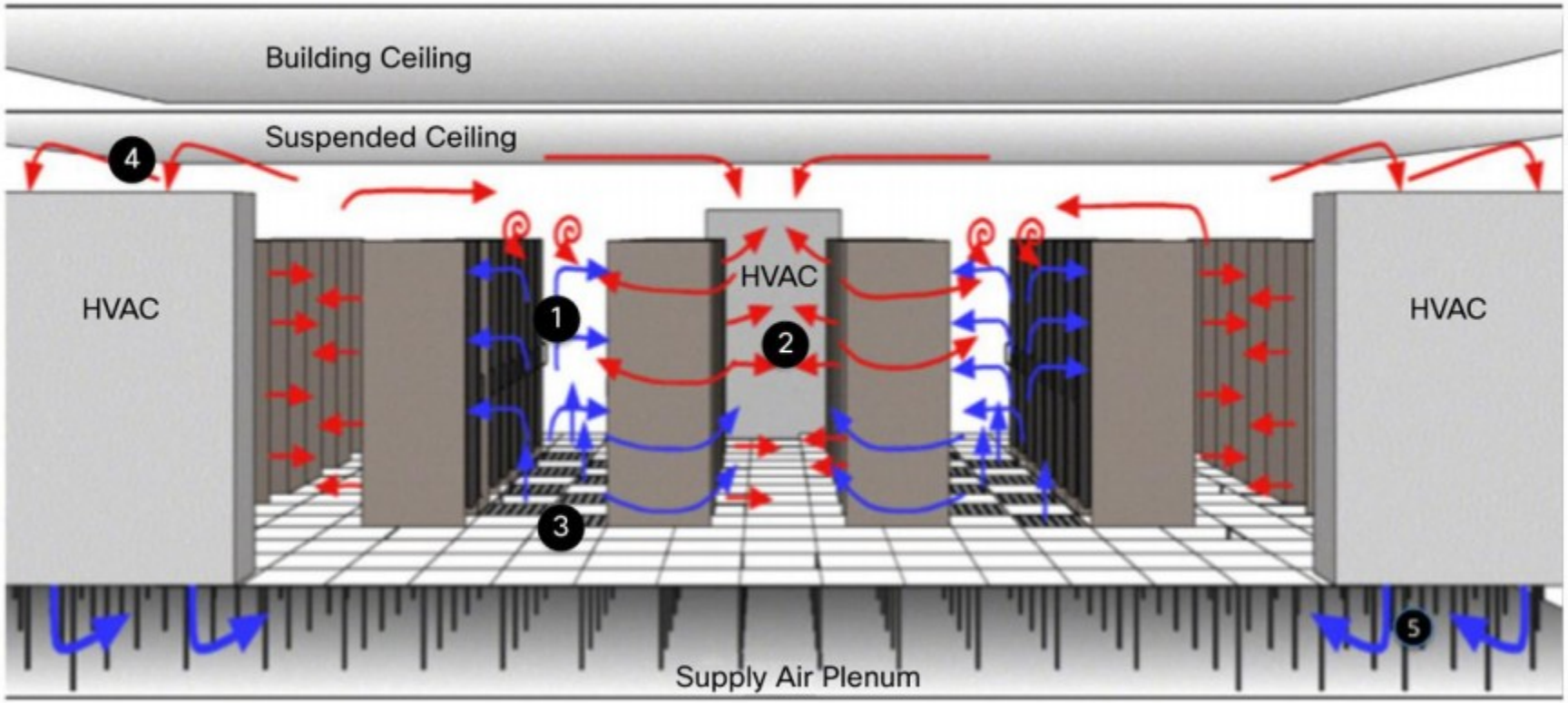
Datacentre Components

- Climate Control
  - Servers generate heat.
  - Air conditioning
  - HVAC – Heating, Ventilation, Air Conditioning
    - Humidity levels are important

Datacentre Components

- https://www.bbc.co.uk/news/technology-44368813
- Physical Security
- Climate Control
  - Servers generate heat.
  - Air conditioning
  - HVAC – Heating, Ventilation, Air Conditioning
- Power

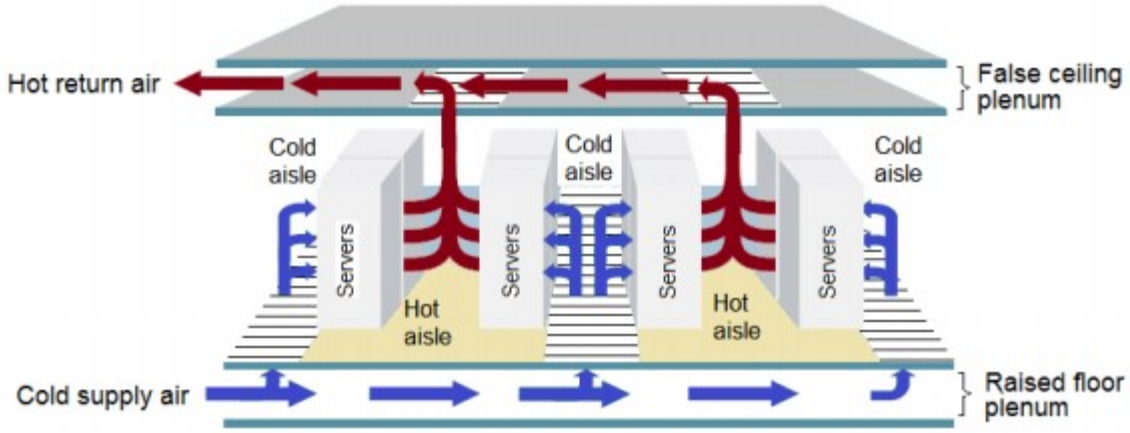
Climate Control



1. Server Inlet
2. Server Exhaust
3. Floor Tile supply temperature
4. HVAC unit return air temperature
5. Computer room AC unit supply temperature

Climate Control

- Hot Aisle and Cold Aisle Layout



Hot aisle- Cold aisle Layout

- Heaviest and most power dense at the bottom
  - Reduces tipping risk
  - Coldest Air at bottom
- Heat and power are connected

Datacentre Components

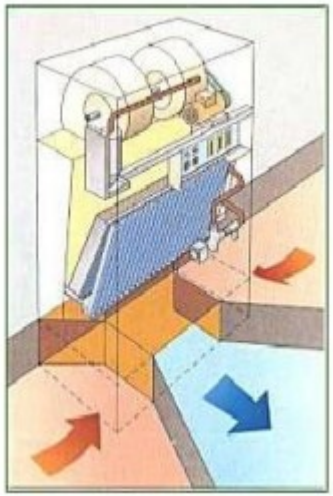
- Power Redundancy
- UPS
  - Emergency Diesel Generator
  - Inverter
- Power Outlets
- Power Capacity

Datacentre Components

- Cooling
  - Air Cooling
    - dissipate heat using cool air
    - Doesn’t damage equipment
    - Easy to circulate
    - Hot spots/cold spots form
  - Direct Liquid Cooling
    - Targeted to where the heat is generated
    - Avoids heating air and then cooling air
    - Complicated to maintain
    - Leakages are a hazard

Datacentre Components

- Cooling Equipment
  - Up-flow units – air discharged from the top
  - Down-flow units – intake at the top and discharged through base. Common in data centres for under floor cooling.



- Cooling Redundancy is expensive

Bandwidth

- Bandwidth is the rate at which data is sent to or received from the Internet.
  - Bandwidth is measured in terms of Megabits per second (Mb/s, often shortened to mbs or mbps).
  - Bandwidth represents the number of bits per second of data sent to or received from the Internet.

Orchestration

- Delivers a service from the cloud
  - Composing of architecture, tools, and processes used by humans to deliver a defined Service.
  - Stitching of software and hardware components together to deliver a defined Service.
  - Connecting and Automating of workflows when applicable to deliver a defined Service.
- manages complex cross-domain (system, enterprise, firewall) processes and handles exceptions.
- Used in fulfillment, assurance, and billing processes
- service-aware orchestrators make adjustments based on feedback from monitoring tools.
- At the most basic level, an orchestrator is a human.

Quality Of Service

- The ability to provide different priority to different applications, users, or data flows, or to guarantee a certain level of performance
  - Loss: probability that a flow's data is lost
  - Delay: time it takes a packet's flow to get from source to destination
  - Delay jitter: maximum difference between the delays experienced by two packets of the flow
  - Bandwidth: maximum rate at which the source can send data

Redundancy

- Redundancy in cloud computing can be defined as the supplying of duplicate copies of various data, equipment, systems, or the like, to be used in the event that part of one's cloud computing system fails or cannot be accessed. This redundancy is made available by having fully replicated data several times on multiple computers or units involved in the same data centre.

Service Level Agreement (SLA)

- A **service level agreement** (SLA) is a **contract** between a **service** provider (either internal or external) and the end user that defines the **level** of **service** expected from the **service** provider. SLAs are output-based in that their purpose is specifically to **define** what the customer will receive.

SLA

- A description of the service being provided – maintenance of areas such as network connectivity, domain name servers, dynamic host configuration protocol servers
- Reliability – when the service is available (percentage uptime) and the limits outages can be expected to stay within
- Responsiveness – the punctuality of services to be performed in response to requests and scheduled service dates

SLA

- Procedure for reporting problems – who can be contacted, how problems will be reported, procedure for escalation, and what other steps are taken to resolve the problem efficiently
- Monitoring and reporting service level – who will monitor performance, what data will be collected and how often as well as how much access the customer is given to performance statistics
- Consequences for not meeting service obligations – may include credit or reimbursement to customers, or enabling the customer to terminate the relationship.
- Escape clauses or constraints – circumstances under which the level of service promised does not apply. An example could be an exemption from meeting uptime requirements in circumstance that floods, fires or other hazardous situations damage the ISP's equipment.

SLA

- mean time between failures (MTBF)
- mean time to recovery, response, or resolution (MTTR)

https://www.youtube.com/watch?v=NX4-GKtBSHQ

https://www.youtube.com/watch?v=TDqF11rRobg

DNS

DNS – Port 53

https://www.youtube.com/watch?v=S6uYZ8V1vRc

https://www.youtube.com/watch?v=mpQZVYPuDGU

FQDN – Fully Qualified Domain Name

https://www.youtube.com/watch?v=p9NpwwZM4rU

https://www.youtube.com/watch?v=_6q3wiYzbXg

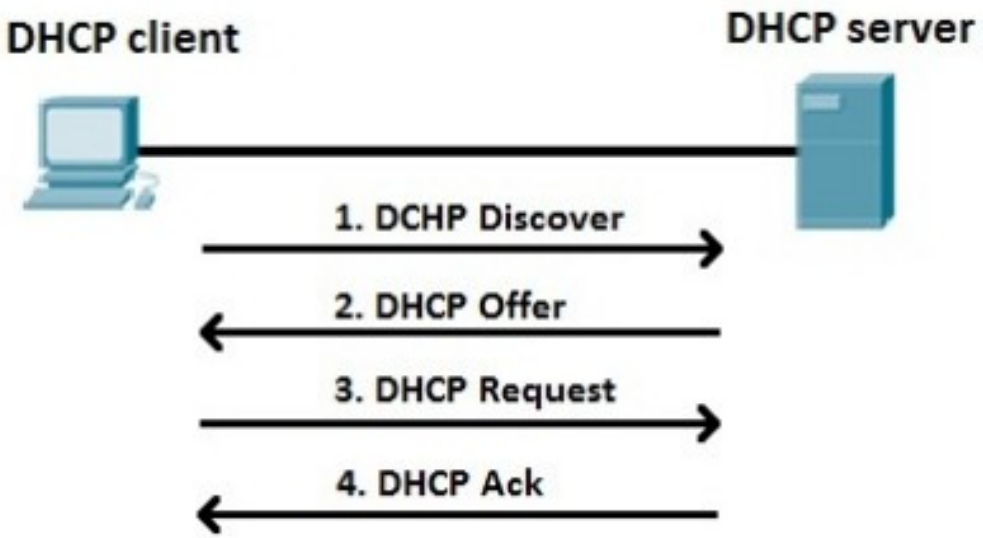
A Records - http://help.dnsmadeeasy.com/managed-dns/records/record/

DNS

- A Records
  - point a domain or subdomain to an IP address
- CNAME
  - used to point a domain or subdomain to another hostname
- Mail Exchanger (MX) records
  - used to help route email according the domain owners preference.
  - The MX record itself specifies which server(s) to attempt to use to deliver mail to when this type of request is made to the domain.
  - Require a “priority” value as a part of their entry
- TXT Record
  - Used to store any text-based information that can be grabbed when necessary

DHCP

- Dynamic Host Configuration Protocol
  - IP Address
  - Subnet Mask
  - Default Gateway
  - Domian Name
  - DNS Server
  - Lease time



- DHCP – Port 67 (Server) & 68 (Client)

Items from CompTia A+

- Identify cable types
  - CAT5
  - COAX
  - FIBRE

- CLI Utilities
  - ipconfig / ifconfig
  - ping
  - tracert / traceroute
  - nslookup
  - netstat
  - net

Passwords

- Poor, weak passwords
  - The password contains less than eight characters
  - The password is a word found in a dictionary or atlas (English or foreign)
  - Names of family, pets, friends, co-workers, fantasy characters, etc.
  - Computer terms and names, commands, sites, companies, hardware, software.
  - Birthdays and other personal information such as addresses, car number plates, and phone numbers.
  - Word or number patterns like aaabbb, qwerty, zyxwvuts, 123321, etc.
  - Any of the above spelled backwards.
  - Any of the above preceded or followed by a digit (e.g., secret1, 1secret)
- Strong passwords
  - Contain both upper and lower case characters (e.g., a-z, A-Z)
  - Have digits and punctuation characters as well as letters, e.g., 0-9, !@#$%^&*()_+|~-=\`{}[]:";'<>?,./)
  - Are at least six alphanumeric characters long.
  - Are not a word in any language, slang, dialect, jargon, etc.
  - Are not based on personal information, names of family, etc.
- Passwords should never be written down or stored on-line.

Load Balancing

- What is Load Balancing?
  - https://www.youtube.com/watch?v=7LMaAVwZE2c
  - https://www.youtube.com/watch?v=q5ON4jqin18
- IP Hash Load balancing (Session Persistence)
  - https://www.youtube.com/watch?v=LJLkk26LOeI

Scale Up and Scale Out

- Scale-up or Vertical Scaling
  - adding more resources to an existing system to reach a desired state of performance
- Scale-out or Horizontal Scaling
  - Adding additional infrastructure capacity

https://storageswiss.com/2013/12/09/scale-out-or-scale-up-6-key-considerations-for-the-flash-array-buyer/

Multi Factor Authentication (MFA)

- Multi-factor authentication (MFA) is a method of confirming a user's claimed identity in which a user is granted access only after successfully presenting 2 or more pieces of evidence (or factors) to an authentication mechanism:
  - knowledge (something they and only they know)
  - possession (something they and only they have)
  - inherence (something they and only they are)
- E.g. ATM access (Card and PIN)

Two Step Verification

- Two-step verification or two-step authentication is a method of confirming a user's claimed identity by utilizing something they know (password) and a second factor other than something they have or something they are
- E.g. Amazon log in

Two Factor Authentication (2FA)

- A type of multi-factor authentication.
- A method of confirming a user's claimed identity by utilizing a combination of two different factors:
  - something they know
  - something they have
  - something they are

RAID Intro

- https://www.youtube.com/watch?v=U-OCdTeZLac
- https://www.youtube.com/watch?v=wTcxRObq738
- https://www.youtube.com/watch?v=6uhet7sT5FQ

FCoE (Fibre Channel Over Ethernet)

- Storage Protocol
- Traditional:
  - Ethernet for networks (LAN)
  - Fibre Channel for storage (SAN)
- Allows fibre Channel communications over Ethernet – High Speed Data Connection
- Increasingly common between servers
- Needs high speed Ethernet infrastructure
- Reduce Switch Complexity
- Up to 10 Gbps