**Intro to Networks**

**Internet protocols**

TCP/IP (transmission Control Protocol/ Internet protocol)

* a set of rules that allows computers to communicate over the internet

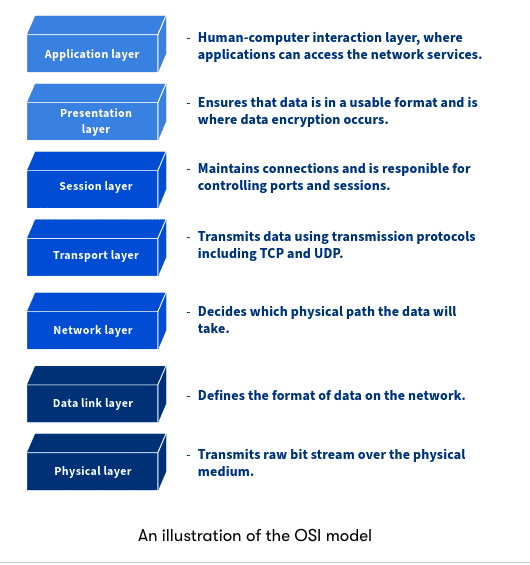
**IP addresses**.

Each device has unique address

* IPV4 = older style 198.192.1.1 for eg
  + We are now outgrowing the available addresses in this format.
* IPV6 = newer/Longer Hexadecimal addresses.
  + Eg 2001:0db8:85a3:0000:0000:8a2e:0370:7334
  + 128 bits long
  + 8 groups of 4 digits

**OSI Model (open systems Interconnection model)**

A conceptual framework used to understand and standardize how different networking systems communicate with each other. It divides the communication process into **seven distinct layers**, each with specific functions.



The **OSI model** is useful because it provides a structured way to understand, design, and troubleshoot computer networks. Here's how it's helpful:

**1. Standardization**

* Provides a universal set of guidelines for different systems to communicate.
* Ensures compatibility between hardware and software from different vendors.

**2. Troubleshooting**

* Helps identify where a network problem occurs (e.g., is it a physical cable issue or a transport layer error?).
* Allows IT professionals to isolate and fix issues more efficiently by layer.

**3. Modularity**

* Each layer operates independently, so changes in one layer (e.g., upgrading a router) don’t affect others.
* Makes system development, upgrades, and repairs more manageable.

**4. Clear Communication**

* Provides a common language for network professionals.
* Helps in teaching, learning, and documenting network processes.

**5. Interoperability**

* Supports communication between different systems and technologies.
* Encourages open and vendor-neutral networking solutions.

**6. Security and Design**

* Allows security to be applied at different layers (e.g., encryption at the presentation layer, firewall at the network layer).
* Helps in designing layered network defences.

**Logical Networking**

Logical networking involves the configuration of networks that are largely independent of the physical setup. Instead of relying on hardware alone, logical networks utilise software to manage, segment, and secure network traffic. This approach not only simplifies physical infrastructure but also enhances scalability and adaptability.

**Virtualisation**

* Creates multiple simulated environments from one physical system
* Often used to run multiple virtual servers on a single physical server
* Maximizes resource use and efficiency

**Software-Defined Networking (SDN)**

* Centrally controls the network through software
* Automates and optimizes network resource management
* Increases network flexibility and responsiveness

**Network Function Virtualisation (NFV)**

* Runs network functions in virtual environments instead of hardware
* Reduces reliance on specific hardware
* Lowers costs and speeds up deployment of network services

Networks

**Hardware**

**Hub**

* Basic device that connects multiple computers in a network
* Sends data to **all devices** (not smart)
* Slower and less secure

**Switch**

* Connects devices in a network
* Sends data **only to the correct device**
* Faster and more efficient than a hub

**Router**

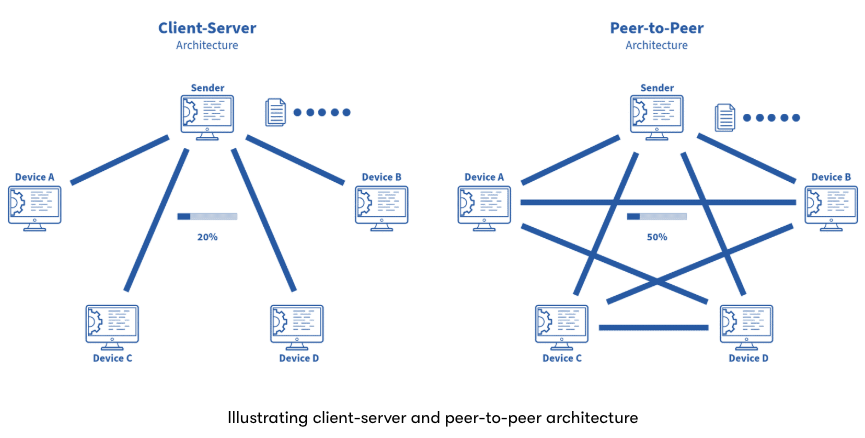
* Connects **different networks** (e.g., home network to the internet)
* Chooses the **best path** for data to travel
* Often includes built-in firewall and Wi-Fi

**Firewall**

* **Protects** the network by controlling incoming and outgoing traffic
* Blocks **unauthorized access**
* Can be hardware, software, or both

**VPN Concentrator**

* Manages **secure VPN connections** for many users
* Encrypts and decrypts VPN traffic
* Used in large businesses for remote secure access



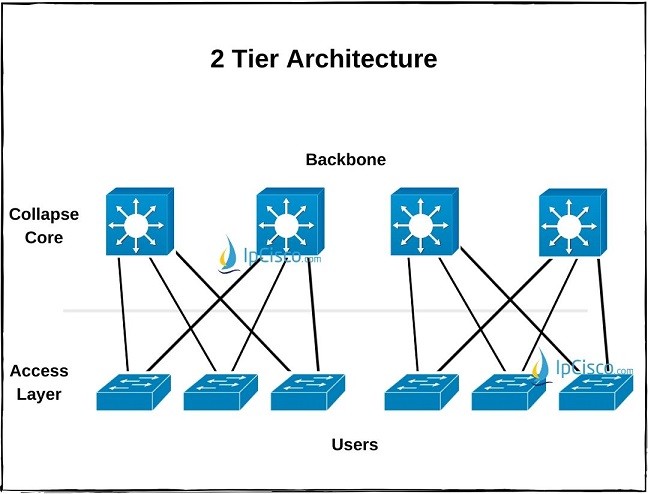
**Client – Server model**

**Peer to Peer**

|  |  |
| --- | --- |
| **Advantages** | **Disadvantages** |
| Easy to set up | No centralised administration |
| Scalable Lower cost | Not as secure |
| Used for simple tasks: transferring files and | Limited reliability |
| sharing printers | Slower performance |

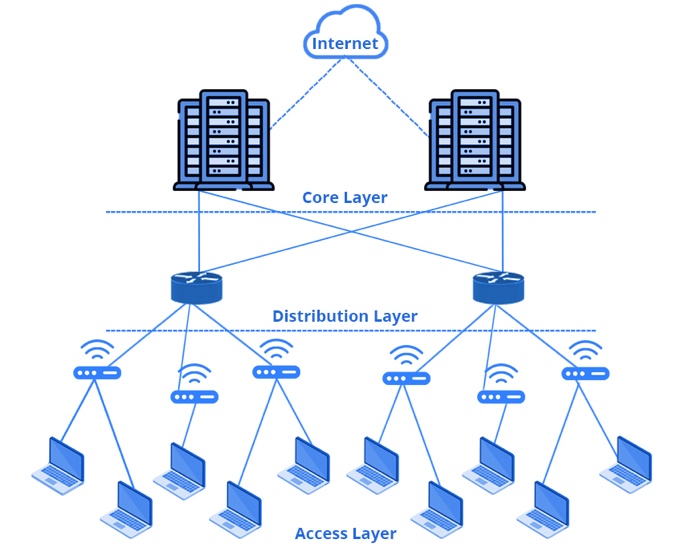
**2-Tier Network (Collapsed Core)**

* **What it is:** Combines the Distribution and Core layers into one "collapsed core" layer above the Access layer
* **Layers:**
  + **Access Layer:** Connects end devices (PCs, printers)
  + **Collapsed Core Layer:** Handles both switching and routing/aggregation
* **Pros:** Simpler design, cost-effective, ideal for small–medium environments
* **Cons:** Less redundancy—single point of failure at the collapsed core



**3-Tier Network**

* **What it is:** A three-layered architecture with distinct roles for each layer
* **Layers:**
  1. **Access Layer** – User devices connect here
  2. **Distribution Layer** – Applies policies, inter-VLAN routing, centralizes control
  3. **Core Layer** – High-speed backbone, connects distribution switches and external networks
* **Pros:** High scalability, strong fault tolerance with redundancy, better performance and network segmentation
* **Cons:** Higher complexity and cost; more equipment required



**Clusters**

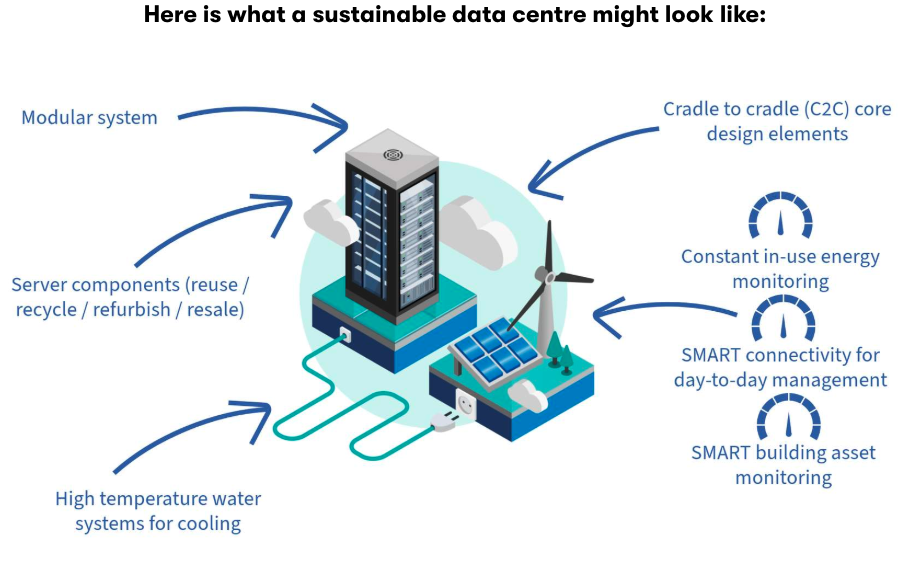
* A cluster is a set of loosely or tightly connected computers that work together, so they can be viewed as a single system.
* used to improve performance and availability, providing a scalable solution for data-intensive applications.
* allow for load balancing and high availability, ensuring that services remain operational even if some nodes fail.
* Can also enable parallel processing, significantly speeding up data processing tasks.

Cluster Management solution examples

* **Hadoop:** An open-source framework that allows for the distributed processing of large data sets across clusters of computers using simple programming models.
* **Spark:** A unified analytics engine for big data processing, with built-in modules for streaming, SQL, machine learning, and graph processing.
* **Yarn:** A cluster management technology used with Hadoop to manage resources in a cluster.
* **Mesos:** A cluster manager that provides efficient resource isolation and sharing across distributed applications or frameworks.

**Data Centres**

Sustainable Networks



* **Energy-Efficient Hardware:** Utilising low-power devices and optimising resource utilisation to reduce energy consumption.
* **Network Design:** Implementing efficient network topologies and protocols to minimise energy use.
* **Green Data Centres:**Data centres designed for energy efficiency and environmental sustainability. These centres use advanced cooling systems, renewable energy sources, and AI to optimise operations.

**Infrastructure Costs**

Cost Components

* **Hardware:** Servers, routers, switches, and other physical equipment.
* **Software:**Operating systems, management tools, security software, and application licenses.
* **Maintenance:** Regular updates, repairs, and technical support to ensure optimal system performance.
* **Energy Consumption:**Power usage of the equipment and cooling systems, which can be significant, especially in data centres.

Optimisation startegies

* **Adopting Energy-Efficient Technologies:** Implementing green technologies that reduce power consumption.
* **Regular System Updates and Maintenance:** Ensuring that systems are running efficiently and securely, which can save costs related to security breaches and downtime.
* **Scalable Solutions:**Employing modular systems that can be expanded as needed, avoiding the initial expense of oversized infrastructures.

TCO (total cost of ownership) = Hardware Cost + Software Cost + Maintenance cost + Energy Cost.