**Network Infrastructure**

A network is a set of computer systems connected in some way so that they can communicate, transmitting information to and from the **nodes** in the network. A node can be a computer system or some part of the network infrastructure itself, that enables communication, like a router or a switch. Nodes can be connected with cable, or via wireless connections, or even with technologies like radio broadcasts (such as when NASA communicates with deep space probes).

Some key terms:

**Node** – Any single element in a network that transmits or receives information

**Client –** A node in a network that receives information from another node

**Server –** A node in a network that transmits (serves) information to another node

**Peer** – Synonymous with node and used only in describing peer-to-peer networks

**Topology –** The design of a network (star, bus, mesh, grid, hybrid and so on)

**Terminator** – the end-point of a network (only applies to some network topologies like a bus)

**ISP –** Internet Service Provider. A company or service that provides connectivity to the Internet

**Packet –** A collection of data containing a header and a payload (user data) sent as a single unit on a network

**Router** – Acts as a gateway to an ISP, and routes signals from one input (the ISP) to multiple outputs (nodes)

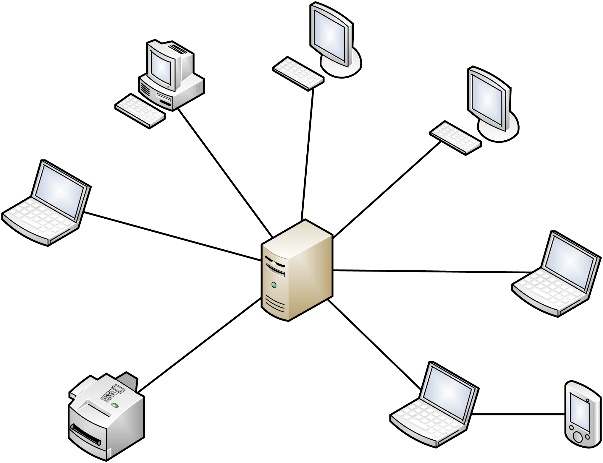
**Switch** – Splits signals from one or more inputs to one or more outputs. Similar, but not the same as a router

**Hub –** Connects multiple points in a network and ensures all inbound packets are visible to all connected nodes

Network Architectures

There are two main architectures you need to be aware of. These are not the same as topologies – architecture refers to how the network is more generally designed, not the precise ins-and-outs of bus vs. star network, although there are similarities. We can **abstract** a good deal in a network architecture, leaving out things like, for example, connections over the Internet, or routers and switches.

**Client-server** – this is a network where clients receive data from a central server (or more than one server). A client can be a server too (think of a server that requests information from another server to fulfil a client request). There can be components between a client and a server (like when requesting a webpage, you’ll travel over lots of different connections to get to the web server). Typically they look like a hub-and-spoke diagram:

[](https://www.google.com/url?sa=i&rct=j&q=&esrc=s&source=images&cd=&cad=rja&uact=8&ved=2ahUKEwiB8ramkLThAhWhoXEKHaqbAZ8QjRx6BAgBEAU&url=https%3A%2F%2Fitpeernetwork.intel.com%2Ftop-10-reasons-to-setup-a-client-server-network%2F&psig=AOvVaw28YqYxrctTohHC9Z__5Ad6&ust=1554387859764931)

**Demo – Using tracert**

Advantages of client-server networks:

* Centralised control of security policies, access and audit
* Easy to find resources like files or database records
* Good vertical scaling (basically, means we can upgrade the central server)
* Easy to connect to other networks

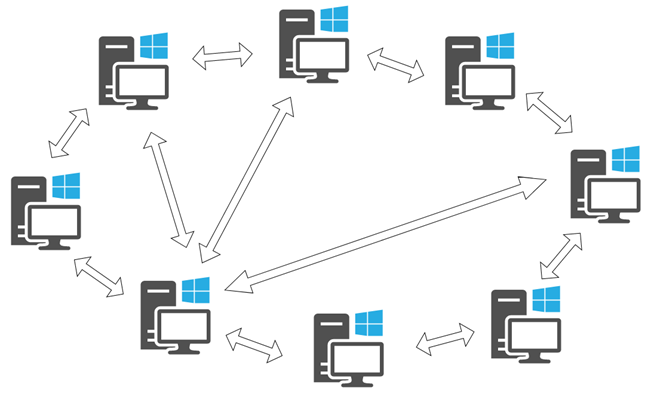
Disadvantages of client-server networks

* Susceptible to load problems (leading to denial of service – DoS)
* Single point of failure
* Central servers are expensive
* Requires ongoing maintenance

**Peer-to-peer**

A peer-to-peer network is a collection of nodes with no centralised control. Instead, the nodes will share common software which allows them to communicate. Every peer is both a client and a server.

In the early days of computing, people used to share files through software like Napster and Pandora. Later (and today) people share files through torrents. These are files that are accessible to all nodes in a network and hosted on many (or all nodes). Certain modern technologies like blockchain (used for Bitcoin) rely on peer-to-peer networking.

[](https://www.google.com/url?sa=i&rct=j&q=&esrc=s&source=images&cd=&cad=rja&uact=8&ved=2ahUKEwih7YedkbThAhXFRBUIHTBGATAQjRx6BAgBEAU&url=https%3A%2F%2Fwww.digitalcitizen.life%2Fwhat-is-p2p-peer-to-peer&psig=AOvVaw2inOo0Idfn7I9-brWOWy8L&ust=1554388144031973)

Advantages of peer-to-peer networks

* Very resilient to failure – removal of any node does not damage the network
* No central server to maintain – reduces costs
* Can sustain long periods of high load with redundant routing

Disadvantages of peer-to-peer networks

* Difficult to manage files centrally
* Lack of accountability (some peer-to-peer software is used for pirating)
* Difficult to maintain software versions across all nodes (inconsistency)

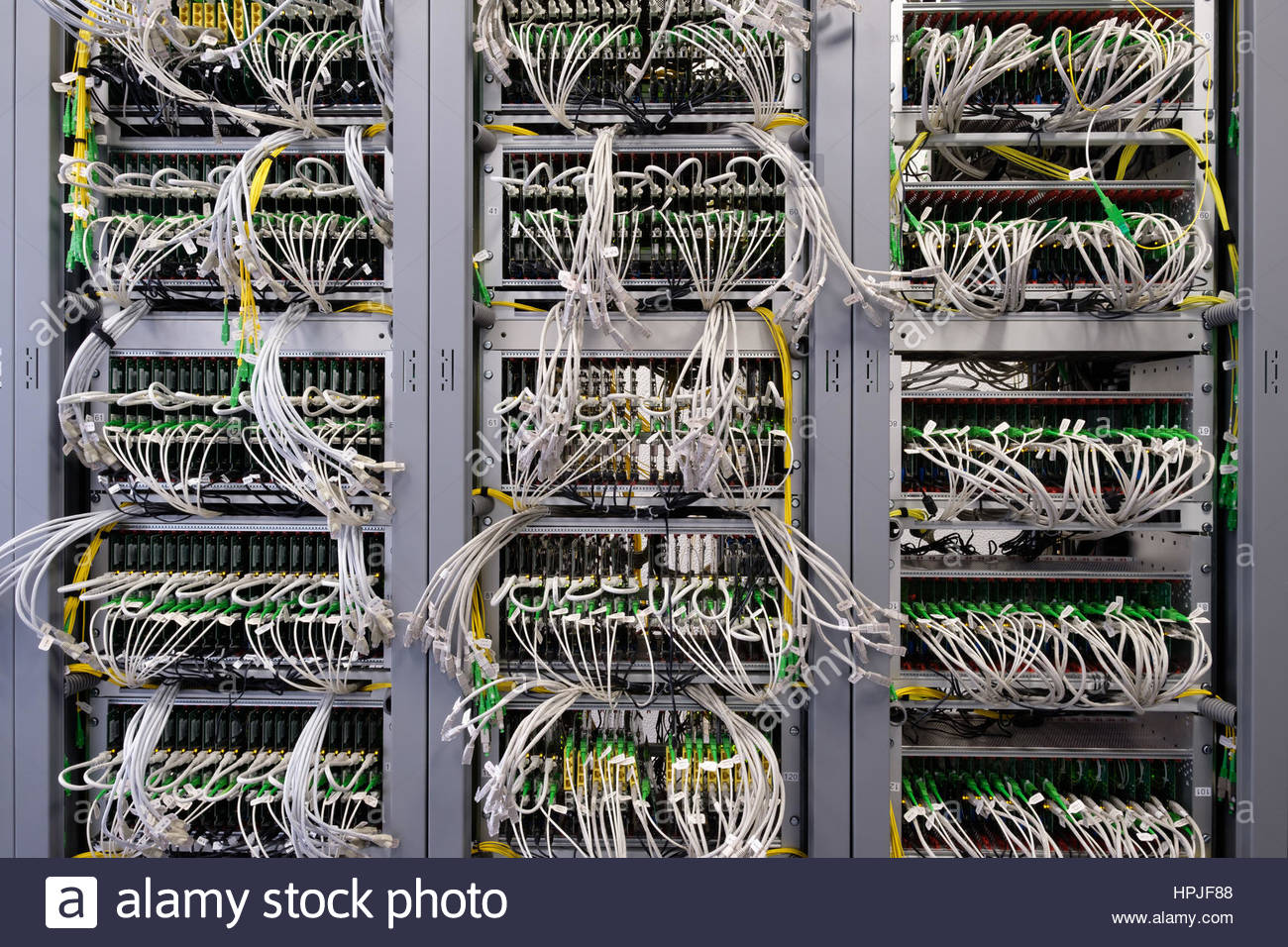
**Introduction to the OSI Model**

We will cover more of this in a later lesson and the details aren’t too important – but you’ll need to know about the OSI model for the exam!

The OSI model is a **7-layer model** that is just an abstract **idea** of the way that networks are structured.

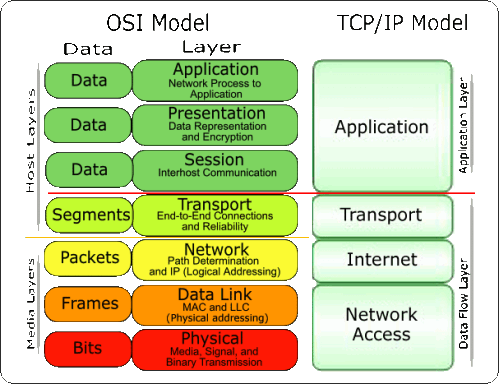
It’s an easy idea - there are different components of a network. The cables and physical hardware, for example, we can draw as a network but it would look pretty meaningless without some context about **why** they are plugged in the way they are. However the hardware diagram would be interesting to an engineer.

Here’s a real-life photo of the back of some servers cabled together in a data centre. It looks completely different to, for example, a client-server network diagram.

[](https://www.google.com/url?sa=i&rct=j&q=&esrc=s&source=images&cd=&cad=rja&uact=8&ved=2ahUKEwiK8KrDlLThAhV9URUIHYOBA9oQjRx6BAgBEAU&url=https%3A%2F%2Fwww.alamy.com%2Fstock-photo-detail-of-cable-management-on-a-data-centre-server-room-134402136.html&psig=AOvVaw2wC1Sxdh6297l4VAFsFjs7&ust=1554389029883218)

This is because the physical hardware is at OSI Level 1 – when we talk about client-server architecture, we’re talking up at OSI Level 3. If we wanted to talk about how a web server processes a request for a web page from your Internet browser, we’re right up at OSI Level 7.

The OSI model is structured like this. You will need to remember the layers and their names for your exam!



Watch the video for an introduction to each layer.

<https://www.youtube.com/watch?v=Hh3AYZf4bIk>

**Internet – DNS, hosting, cloud**

Watch ‘A packet’s tale’ <https://www.youtube.com/watch?v=Gfoc3Cxgnpk>

This will introduce you to some of the key components in Internet connectivity.

**Demo –** Look at the Akamai web monitor and Kaspersky threat cybermap.

<https://www.akamai.com/uk/en/resources/visualizing-akamai/real-time-web-monitor.jsp>

<https://cybermap.kaspersky.com/>

**Demo – talk through DNS, show-and-tell of DNS records on fasthosts**