When you want to visit a website, you type or paste the site’s **domain name** into your browser, or click on an html link.

That domain name is sent to a server which translates the name into a series of numbers – the Internet Protocol or **IP Address** - which the server uses to direct your request to the website’s physical location. **This all happens in the blink of an eye.**

Those names and numbers are called “**unique identifiers**” and are aligned with a standard set of **protocol parameters** that ensure computers can talk to and understand each other.

These are part of the **IANA functions**, which are managed by **ICANN**, the **Internet Corporation for Assigned Names and Numbers**.

These functions aren’t just limited to browsing the Internet - they also enable you to send an email or backup photos to the cloud, amongst other tasks.
A key IANA function is the global coordination of the Internet Protocol addressing systems, commonly known as IP Addresses. There are two types of IP addresses in active use: IPv4 (192.0.2.53) and IPv6 (2001:db8:582::ae33).

The allocation of blocks of AS numbers to Regional Internet Registries (RIRs) is another part of this function. AS numbers are used to identify the networks that control their own routing by connecting to multiple networks controlled by other organizations.

The allocation of IP addresses and AS numbers to RIRs are made according to global policies. The five RIRs, each of which serves a continental region, establish consensus-based global policies.

The Protocol Parameters management function involves maintaining many of the codes and numbers used in Internet protocols. This is done in coordination with the IETF.

ICANN currently performs the IANA functions on behalf of the global Internet community under a contract with the United States’ Department of Commerce. NTIA, an agency of the Department of Commerce, performs a process check before authorizing changes to the DNS’s authoritative root zone file.

DNSSEC is a technology that digitally ‘signs’ DNS answers so you can know they are valid. To be sure of an answer’s validity, a digital signature is needed at each stage in the hierarchy from the root zone to the final domain name (e.g., www.icann.org). DNSSEC does not encrypt DNS queries or answers. It lets you know whether a DNS answer is valid.

For more information, visit [www.icann.org](http://www.icann.org) and follow [@ICANN](https://twitter.com/ICANN) on Twitter.