What is DNS? A computer engineer explains this foundational piece of the web – and why it’s the internet’s Achilles’ heel

Doug Jacobson, University Professor of Electrical and Computer Engineering, Iowa State University

Published: October 31, 2025 8:43am EDT

Amazon Web Services, hosted in data centers like this one in Virginia, supports thousands of websites, apps and online services – but not during its recent DNS outage.
Nathan Howard/Getty Images

When millions of people suddenly couldn’t load familiar websites and apps during the Amazon Web Services, or AWS, outage on Oct. 20, 2025, the affected servers weren’t actually down. The problem was more fundamental – their names couldn’t be found.

The culprit was DNS, the Domain Name System, which is the internet's phone book. Every device on the internet has a numerical IP address, but people use names like amazon.com or maps.google.com. DNS acts as the translator, turning those names into the correct IP addresses so your device knows where to send the request. It works every time you click on a link, open an app or tap "log in." Even when you don't type a name yourself, such as in a mobile app, one is still being used in the background.

To understand why DNS failures can be so disruptive, it's helpful to know how the Domain Name System is constructed. The internet contains over 378 million registered domain names, far too many for a single global phone book. Imagine a single book containing every American's name and phone number. So DNS was intentionally designed to be decentralized.

Each organization that owns a domain, such as google.com, is responsible for maintaining its own DNS entries in its own DNS server. When your device needs to find an IP address, it asks a DNS server, which may ask others, until it finds the server that knows the answer. No single system has to hold everything. That's what makes DNS resilient.

Centralization equals vulnerability

So why did AWS, the largest cloud provider in the world, still manage to break the internet for so many, from Zoom to Venmo and smart beds?

Cloud providers host web servers but also critical infrastructure services, including DNS. When a company rents cloud servers, it often allows the cloud provider to manage its DNS as well. That's efficient – until the cloud provider's DNS itself has a problem.

Amazon disclosed that the specific cause of the recent disruption was a timing bug in the software that manages the AWS DNS management system. Whatever the cause, the effect was clear: Any website or service relying on AWS-managed DNS could not be reached, even if its server was perfectly healthy. In this way, the cloud concentrates risk.

This wasn't the first time DNS became a point of failure. In 2002, attackers attempted to disable the entire DNS system by launching a denial-of-service attack against the root DNS servers, the systems that store the locations of all other DNS servers. In a denial-of-service attack, an attacker sends a flood of traffic to overwhelm a server. Five of the 13 root servers were knocked offline, but the system survived.

In 2016, a major DNS provider called Dyn, which companies paid to run DNS on their behalf, was hit with a massive distributed-denial-of-service attack. In a distributed-denial-of-service attack, the attacker hijacks many computers and uses them to send the flood of traffic to the target. In the Dyn attack, tens of thousands of compromised devices flooded its servers, overwhelming them. For hours, major sites like Twitter, PayPal, Netflix and Reddit were functionally offline even though their servers were fully operational. Yet again, the issue wasn't the websites; it was the inability to find them.

The lesson is not that DNS is weak, but that reliance on a small number of providers creates invisible single points of failure. DNS was initially designed for decentralization. Yet, economic convenience, cloud services and DNS as a service are quietly steering the internet toward centralization.

Convenience over resilience

These failures matter far beyond shopping or streaming. DNS is also how people reach banks, election reporting systems, emergency alert platforms and the artificial intelligence tools now powering critical decision-making. It doesn't even need to fully go down to be dangerous. Simply delaying or misdirecting DNS can break authentication between users and services, block transactions or erode public trust at sensitive moments.

The uncomfortable reality is that convenience is quietly winning over resilience. As organizations increasingly outsource DNS and hosting to the same handful of cloud providers, they accumulate what could be called resilience debt – invisible until the moment it comes due. The internet was engineered to survive partial failure, but modern economics is concentrating risk in ways its original designers explicitly tried to avoid.

The lesson from the AWS outage isn't just about fixing one software bug. It's a reminder that DNS is critical infrastructure. That means technology companies can't afford to treat DNS as background plumbing, and resilience needs to be designed intentionally.

Individual DNS failures inconvenience people, but the reliability of DNS on the whole defines whether the internet still works at all.

Doug Jacobson does not work for, consult, own shares in or receive funding from any company or organization that would benefit from this article, and has disclosed no relevant affiliations beyond their academic appointment.