Messaging, Malware and Mobile Anti-Abuse Working Group

M³AAWG Technology Summaries

November 2026

M³AAWG Technology Summary: DNS Resolution

What DNS resolution is:

DNS stands for Domain Name System, which is commonly explained as the process by which applications convert domain names, such as example.com, into the IP addresses, such as 172.66.147.243, that computers and other devices need to look up and connect to websites, email servers, and other internet resources. When DNS resolution fails, due to server misconfiguration, for example, internet services frequently suffer outages.

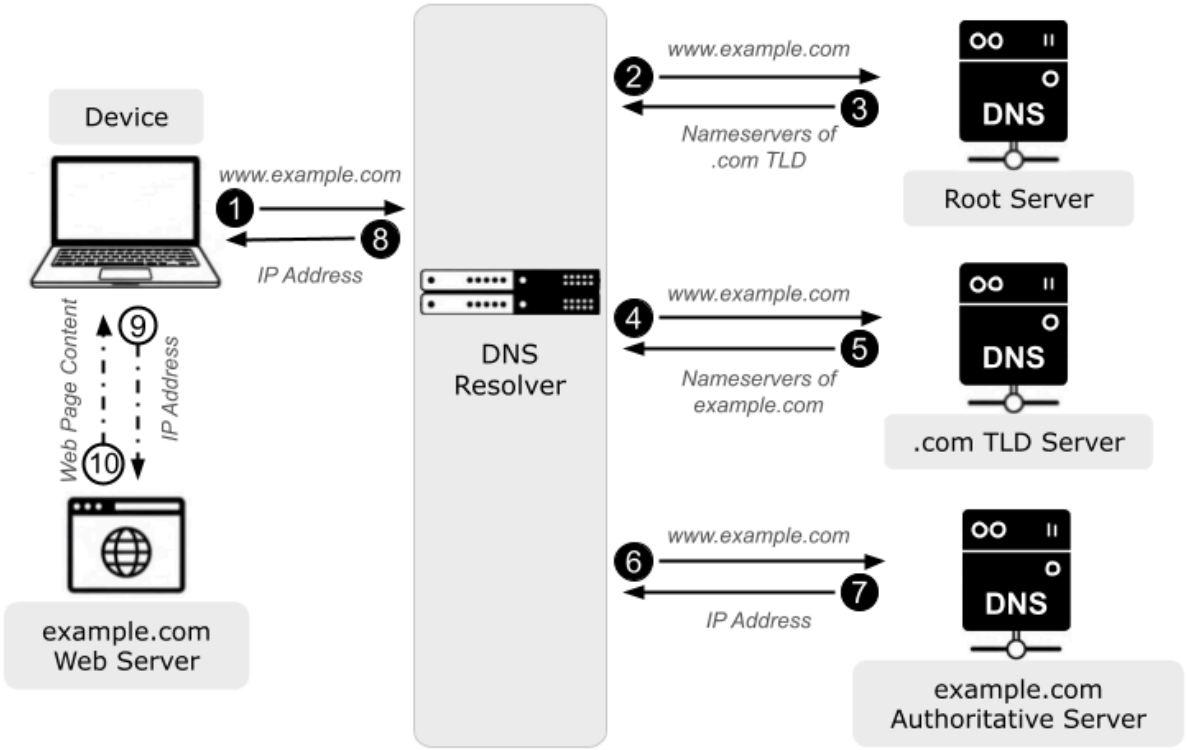
DNS resolution is the decentralized process of resolving a domain name. Beyond IP addresses, DNS data includes Mail Exchanger (MX) records that locate mail servers and TXT records that hold text data, including specialized records like Sender Policy Framework (SPF), Domain-based Message Authentication, Reporting and Conformance (DMARC), DomainKeys Identified Mail (DKIM)[1], and more. The same resolution process is used regardless of the data type being queried.

The DNS is a tree-like hierarchy using authoritative servers, or nameservers, that store information about their allocation of the DNS hierarchy, or "tree." To access this information, DNS resolvers are used. A DNS resolver is software that queries nameservers on behalf of an application to map DNS names, for example, a domain, to IP addresses.

An end user's system or application is configured to use one or more DNS resolvers to query relevant authoritative nameservers. In our example, the DNS resolver queries the .com and example.com zones to "walk" the tree to reach the information needed. Each server provides information to identify the next level of the hierarchy, until the requested IP address or other DNS information is reached.

The DNS resolution process (reference image below):

- The device, or user, requests the IP for a hostname (www.example.com) via its assigned resolver (1)[2].
- The device's DNS resolver goes to a root nameserver (2, 3) to locate a Top-Level Domain (TLD[3]) nameserver (com). Note: most queries sent to the DNS resolver are typically cached for a period of time, which is set by a time-to-live value (TTL) found within the DNS record, and will be returned immediately to the device without traversing the DNS tree.
- The device's DNS resolver queries the TLD nameserver to locate the nameservers for the domain (example.com) (4, 5).
- The device's DNS resolver queries the IP address or other information about the domain (example.com) from the authoritative nameservers for the hostname (www.example.com) (6, 7).
- The device's DNS resolver provides the information requested to the device (8).
- The device uses the requested information to connect to the resource, for example, a website (9, 10).



What DNS resolution does not do:

- Guarantee that a response was not altered in-transit. While Domain Name System Security Extensions (DNSSEC[4]) can ensure this, it is not often enabled.
- Provide assurance that DNS query results are intended by the domain owner (even with DNSSEC), for example, if the account was compromised.
- Guarantee query results are updated and synced across all DNS servers.
- Provide reputational data about the domain, the resulting location, or other information.
- Encrypt queries so they cannot be eavesdropped on. However, DoT (DNS over TLS) and DoH (DNS over HTTP) can encrypt them similarly to HTTPS web pages for resolvers and nameservers that support DoT or DoH.

References:

Domain Name System – Wikipedia

[1] For more information on DNS records, see the M3AAWG Glossary and Technology Summaries.

[2] In practice, an application will usually query the on-device resolver, often called the stub, which then asks the assigned DNS resolver it is configured to use. Most often, this is the device's ISP or corporate network DNS resolver. However, it is possible to choose other resolvers to send queries. For example, popular public DNS resolvers include Google's 8.8.8.8, Cloudflare's 1.1.1.1, and Quad9's 9.9.9.9.

[3] TLD is the rightmost visible label in a hostname run by a domain name registry, for example, com, org, net, or uk.

[4] DNSSEC (RFC 9364) is a cryptographic protocol to ensure a published DNS answer is verifiable by the requestor. It does not provide reputational data about the resolved location or content.

© 2026 Messaging, Malware and Mobile Anti-Abuse Working Group (M3AAWG) M3AAWG-161