What happens with browser queries?

DNS names are read by browsers from right to left. e.g.

- http://server.example.com -> com - example - server - protocol

> Definition of a domain: Top Level Domain (TLD) - Second Level Domain (SLD) - Subdomain (optional) - Protocol

This ensures that a local search is performed first and that a resolution request is only forwarded to a “resolver” if information is not available locally.

In local home networks, this is always solved on each device with the “/etc/hosts” file (Microsoft: C:\Windows\System32\drivers\etc\hosts).

With an increased number of devices in the home network, this management becomes inefficient and error-prone over time!

This is why local DNS resolvers (a device that is announced via DHCP or by manual entry on a device) are also used in home networks if required (typical representatives: bind9, dnsmasq, PI-Hole, AdGuard, Technitium and certainly many others). This is where the wheat is separated from the chaff... You have to master the DNS part of the tools and know what you are doing! So far, none of this has anything to do with http:// or https://!

http:// - https:// Resolution

We want to concentrate on SSL = https://! When the browser has processed the above topic, it checks whether a corresponding web server (e.g. apache2, Nginx, others...) provides an accessible page. AND now it gets interesting!!!! The browser uses the certificate stored by the web server to check / query locally whether a trustworthy root certification authority is stored! And this causes the home network with https & domain name to fail! You can find the standard root certification authorities for:

MAC : /Library/Keychains/System.keychain
Linux : /usr/local/share/ca-certificates
Windows : certmgr.msc

But not for the reader, of course! We take this into our hands and realize the concept for a home network!

Revision #2
Created 18 June 2025 08:56:32 by tomek
Updated 18 June 2025 09:09:00 by tomek