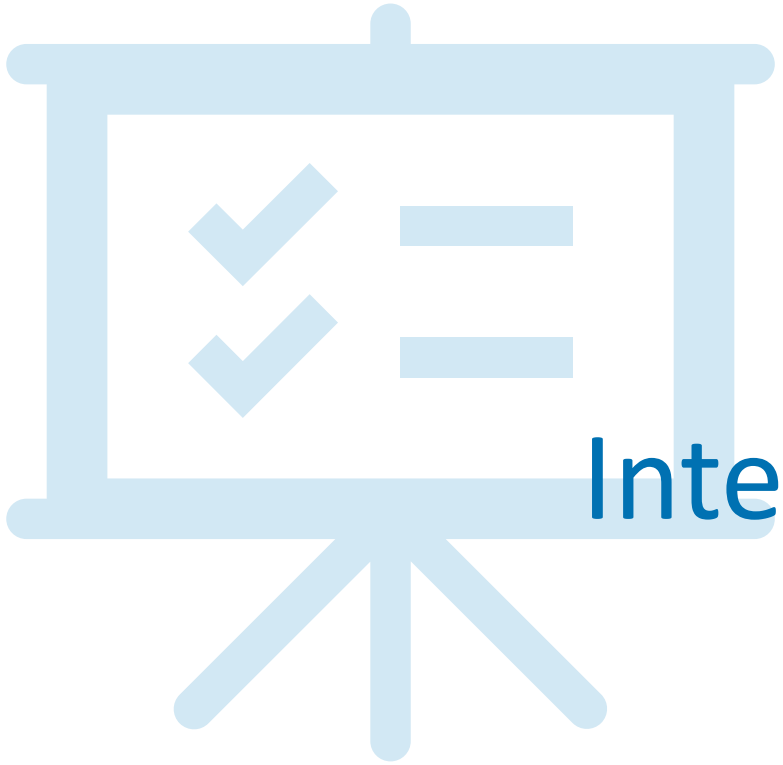

Netzwerke und Internettechnologien 1

Domain Name System (DNS)

Netzwerke und Internettechnologien 1

Lernziele

1. Namensauflösung

2. Aufbau und Funktion von DNS

3. DNS-Server
DNS-Client

Namensauflösung

- Als Namensauflösung wird ein Verfahren bezeichnet, dass Hostnamen in IP-Adressen und auch umgekehrt übersetzt.
- In diesen Prozess können Konfigurationseinstellungen, Dateien und Dienste eingebunden sein.
- Ablauf der Namensauflösung

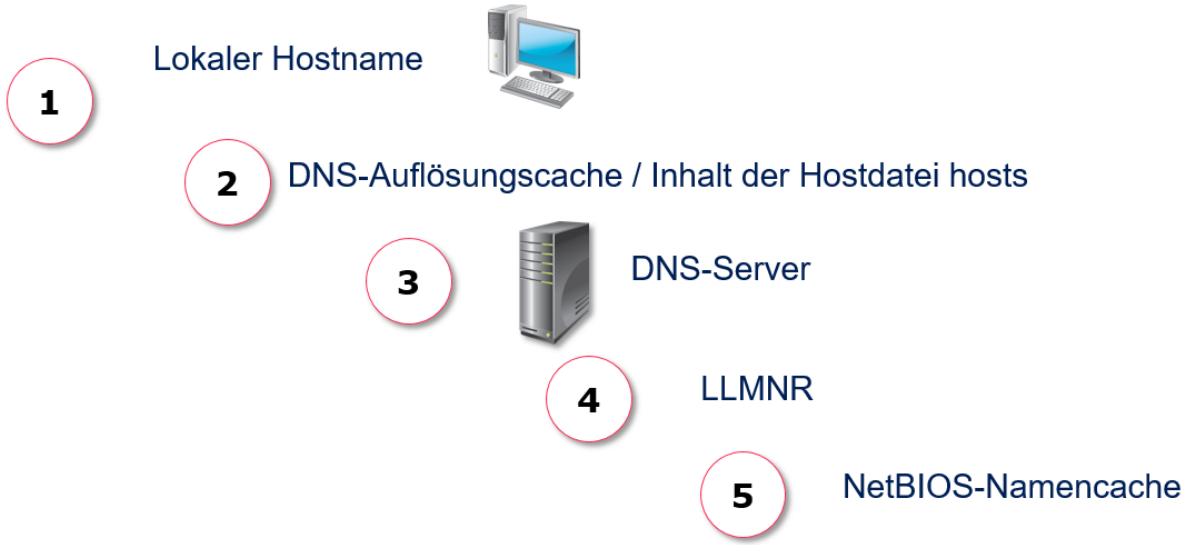

Abbildung 1: Namensauflösung (Quelle Microsoft, Eigene Darstellung)

Domain Name Service (DNS)

- DNS ist ein Dienst, der vollqualifizierte DNS-Namen und andere Hostnamen in IP-Adressen auflöst.
- DNS stellt diesen Dienst mithilfe einer in einer Datei oder in AD DS gespeicherten Datenbank von Namen und IP-Adressen bereit.
- Aufgaben:
  - Auflösen von Hostnamen in IP-Adressen und von IP-Adressen in Hostnamen
  - Suche nach Dienstanbietern Domaincontroller, Globalen Katalogservern, E-Mail-Servern, KMS-Host

Hostnamen

- Der Hostname ist ein Computername, der einem Domänennamen und der Top-Level-Domain zu einem vollqualifizierten Domänennamen (Fully Qualified Domain Name, FQDN) hinzugefügt wird.

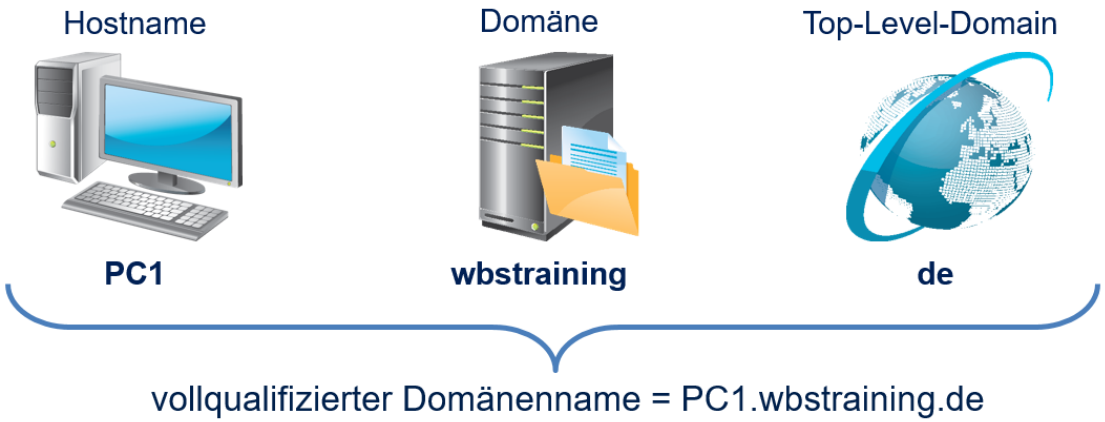

Abbildung 2: Hostnamen (Eigene Darstellung)

- Kurznamen oder NetBIOS sind veraltet und finden kaum noch Verwendung

Domain Name Service (DNS)

- DNS ist als verteilte hierarchische Datenbank aufgebaut.
- Die Daten sind auf einer Vielzahl an Servern überall auf der Welt gespeichert.
- Hierarchie (Auszug):

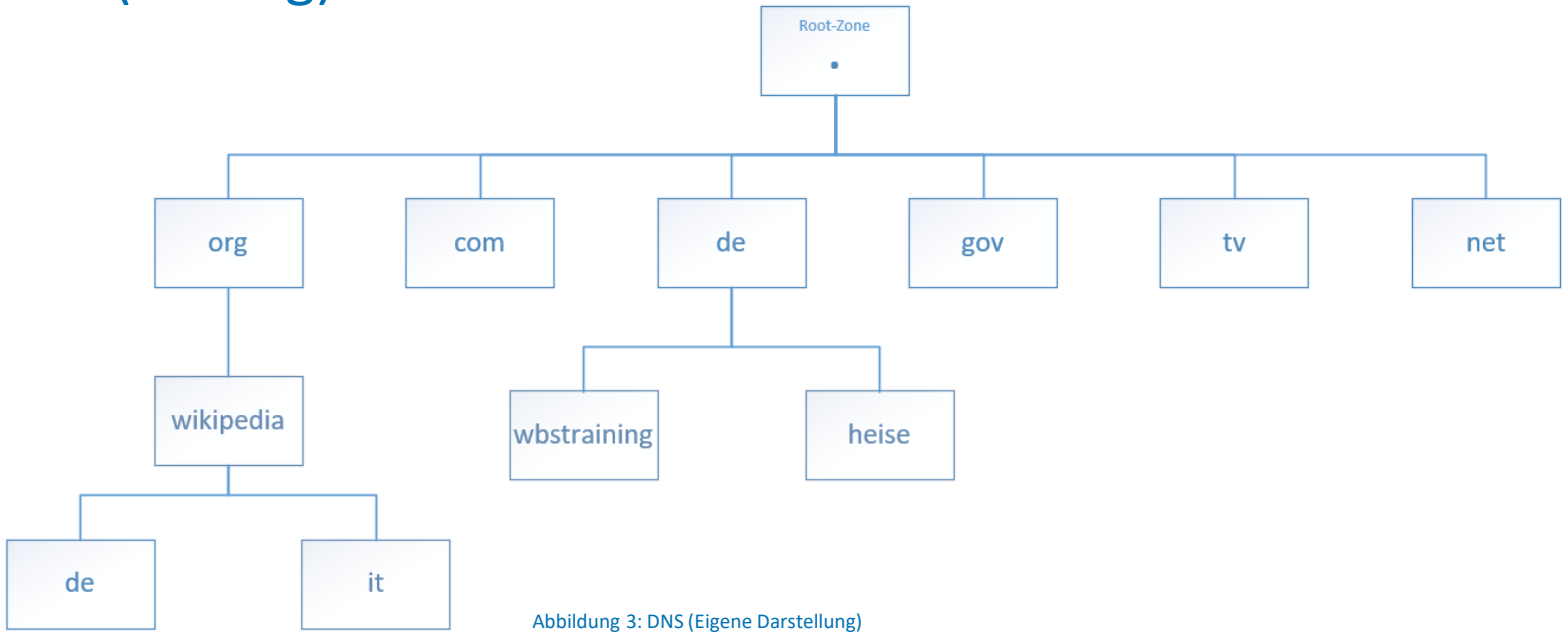

Abbildung 3: DNS (Eigene Darstellung)

Root Server

- Es gibt 13 Root-Nameserver, die nach dem Schema x.root-servers.net benannt sind.
- Jeder Root-Nameserver ist sowohl unter einer IPv4-Adresse, wie auch einer IPv6-Adresse erreichbar.
- Bei der Kommunikation mit den Root-Nameservern wird Anycast zur Lastverteilung eingesetzt. Die 13 Adressen werden von mehreren hundert Servern weltweit bedient.

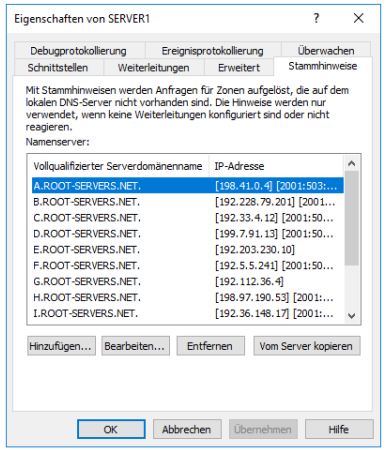

Abbildung 4: Stammhinweise (Eigene Darstellung)

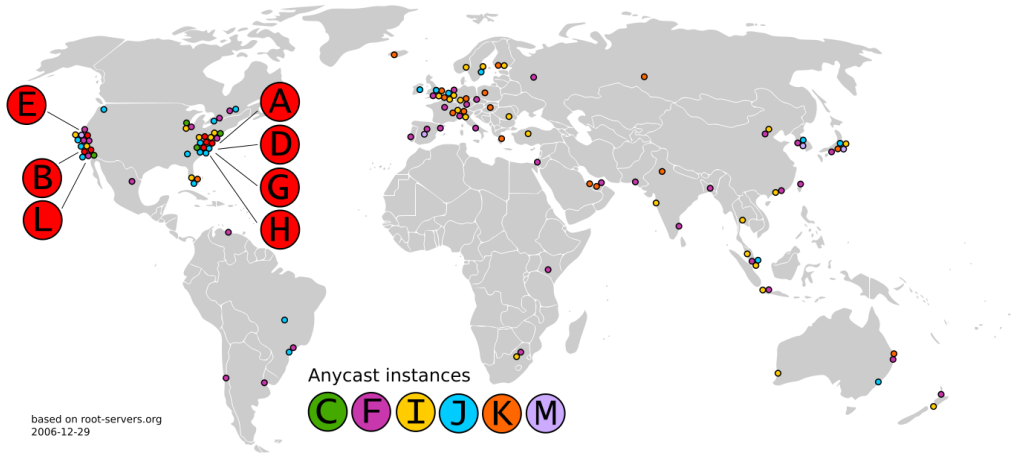

Abbildung 5: Root-Server (Quelle Wikipedia)

DNS - Namensraum

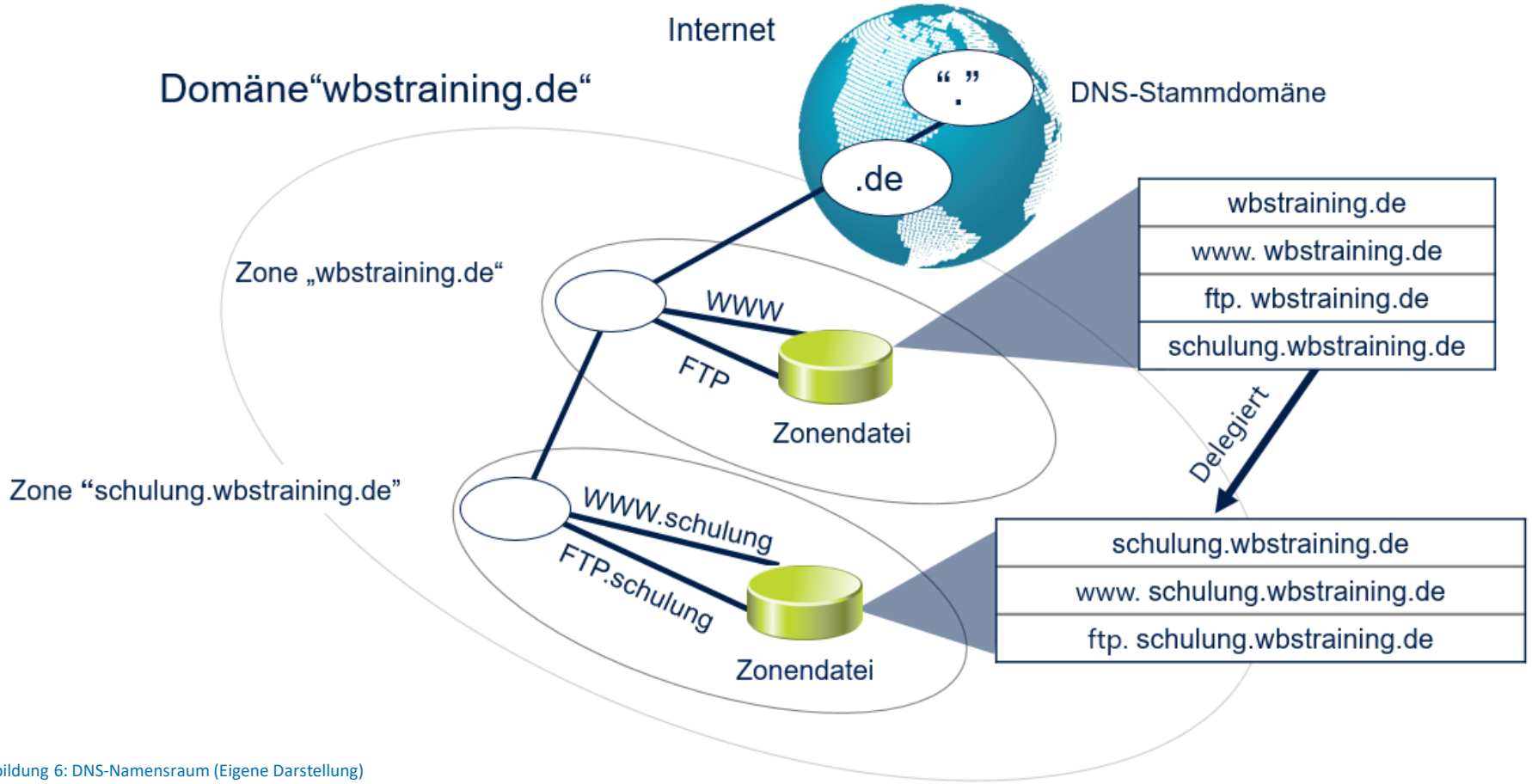

Abbildung 6: DNS-Namensraum (Eigene Darstellung)

DNS - Server

- Serverarten
  - Primary DNS-Server (Master)
    - Hostet die Datenbank eines Bereiches von DNS, der als Zone bezeichnet wird.
    - Die Datenbank auf dem Master ist beschreibbar.
  - Sekundärer DNS-Server (Slave)
    - Verfügt eine, vom Master replizierte, schreibgeschützte Kopie der Zonendatenbank.
  - Caching-only-Server (Hint)
    - Speichern selbst keine Datenbanken, sondern leiten Anfragen nur weiter.

DNS - Zone

- Eine DNS-Zone besteht aus einer Reihe von Ressourceneinträgen, sogenannte Ressource Records (RRs), die in der Regel eine Zeile umfassen.
- Es gibt verschiedene Typen von RRs:
  - SOA-Einträge (Start of Authority)
  - A-Einträge (Host)
  - NS-Einträge (Nameserver)
  - MX-Einträge (Mailexchanger)
  - CNAME-Einträge (Alias)
  - PTR-Einträge (Pointer)
  - SRV-Einträge (Service Locator)

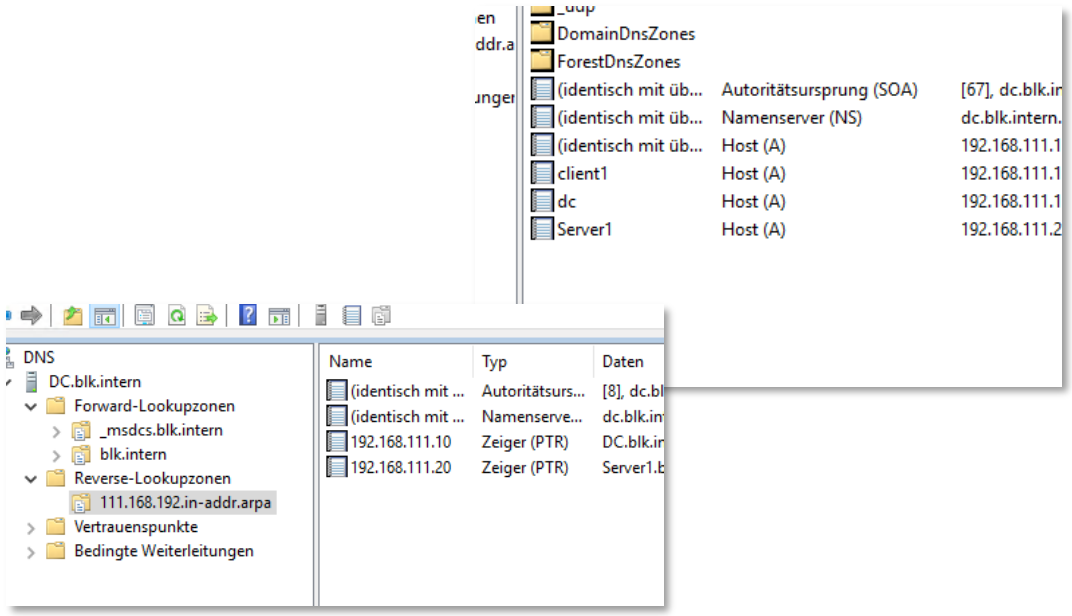

Abbildung 7: DNS-MMC (Eigene Darstellung)

DNS - Zonen

- PRIMARY ZONE
  - Eine Standard Primary Zone ist eine Lese-/Schreib-Kopie einer DNS-Datenbank. Diese befindet sich in Format einer Text-Datei in einem Teil des DNS-Subsystems. Der DNS-Server-Dienst lädt diese Text-Datei in seinen Speicher, wenn er gestartet wird.
  - Durch einen Prozess namens Zone-Transfer wird die Text-Datei, die die Standard Primary Zone enthält, wird auf alle DNS-Server kopiert, die die Secondary Zone beinhalten.

- SECONDARY ZONE
  - Eine Standard Secondary Zone ist eine Nur-Lese-Kopie der DNS Datenbank. Auch hier sind die Daten in einer Textdatei gespeichert.
  - Diese Zone wird zum Zwecke des Load-Balancings, sowie für einfache Fehlertoleranz verwendet.
  - Die Standard Secondary Zone kann nur via Zone-Transfer Prozess aktualisiert werden.

DNS - Client

- Der DNS-Client ist kein eigenständiges Programm oder Dienst, sondern eine Bibliothek (Resolver genannt)
- Der Resolver ist mit Anwendungen gelinkt, die eine DNS-Namensauflösung durchführen müssen.
- Windows-Systeme enthalten Windows enthalten einen clientseitigen DNS-Cache.
- Der DNS-Cache kann mit dem Kommando **`ipconfig /displaydns`** angezeigt und mit dem Kommando **`ipconfig /flushdns`** geleert werden.

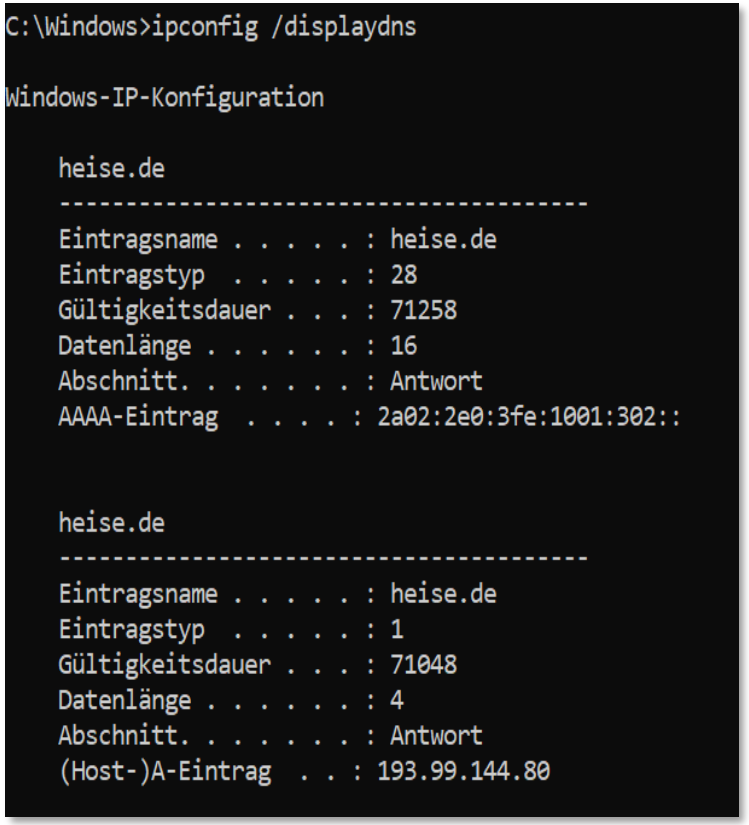

Abbildung 8: Kdo. (Eigene Darstellung)

DNS-Server abfragen

- Der Befehl **nslookup**, der Name bedeutet „Name Server look up“, kann auf der Kommandozeile verwendet werden, um DNS-Server abzufragen.
- Mit **nslookup** kann eine Vorwärts- oder Rückwärtsauflösung durchgeführt werden. Standardmäßig wird der konfigurierte DNS-Server zur Auflösung des Namens verwendet
- Der Befehl kennt zwei Modi, den nicht interaktiven Modus (Standard) und den interaktiven Modus.

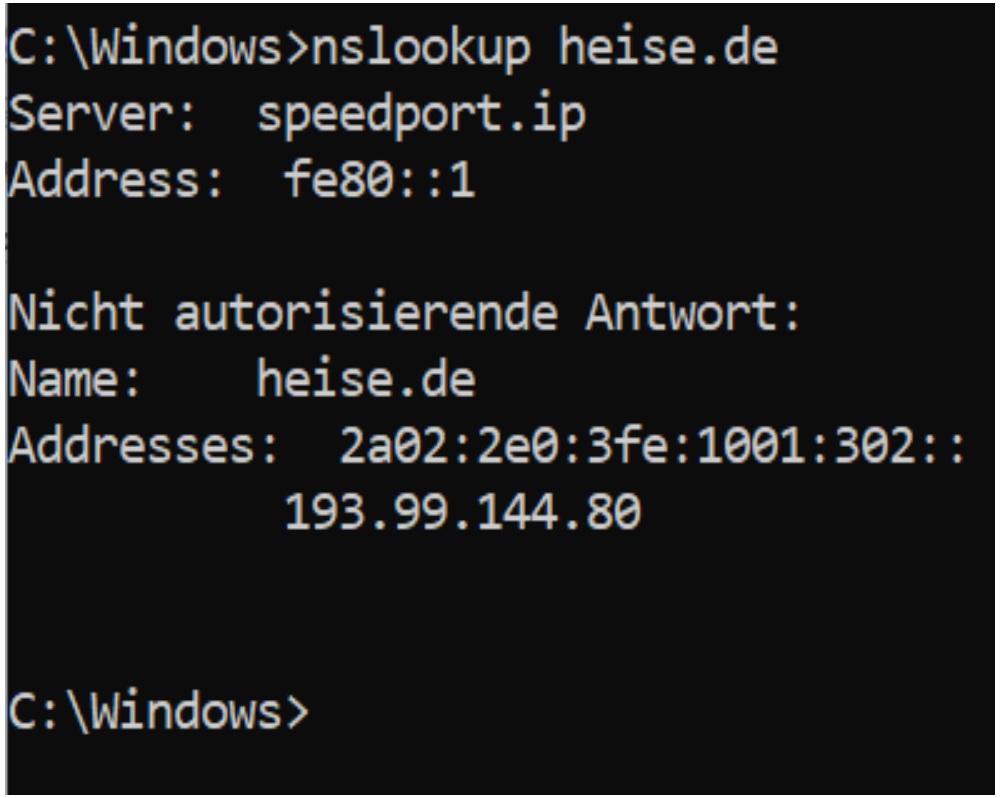

Abbildung 9: nslookup (Eigene Darstellung)

DNS - Namensauflösung

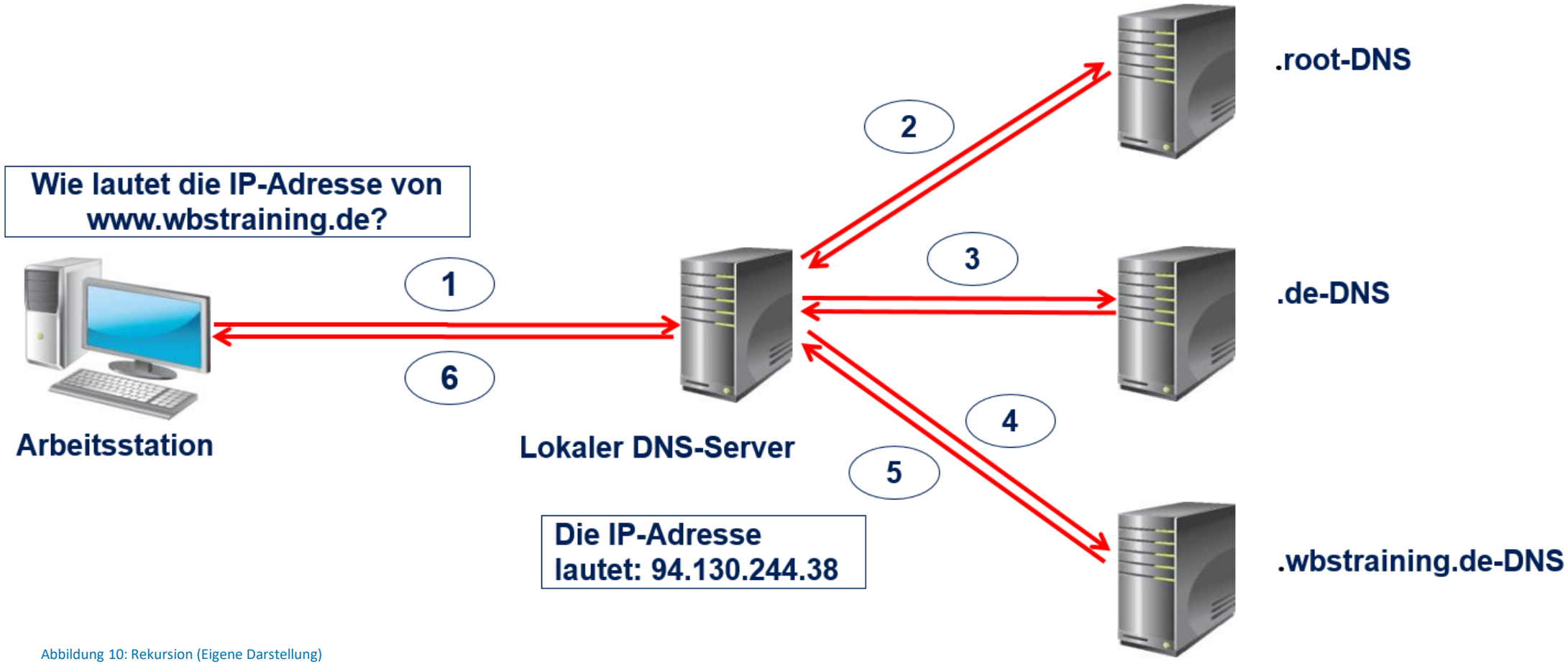

Abbildung 10: Rekursion (Eigene Darstellung)

Dynamic Domain Name System (DynDNS)

- DynDNS oder DDNS ist ein System, das dynamische IP-Adressen von Domain-Namen aktualisieren kann.
- Das beinhaltet das dynamische Erstellen, Registrieren oder Aktualisieren von Einträgen eines DNS-Clients in einer Zone.
- Dynamische Aktualisierungen können, von dafür geeigneten, Clients oder vom DHCP-Server realisiert werden.
- Vorteile:
  - Automatische Aktualisierung von DNS-Einträgen beim Einsatz von DHCP.
  - Weniger administrativer Aufwand.

Domain Name System Security Extensions (DNSSEC)

- DNSSEC ist eine Erweiterung des Domain Name System, die DNS-Daten kryptografisch der Authentizität und Integrität der DNS-Daten gewährleistet.
- Es wird sichergestellt, dass die erhaltenen DNS-Daten auch tatsächlich identisch sind mit denen, die der Ersteller der Zone autorisiert hat.
- Der Empfänger einer DNS-Nachricht (DNS-Response) kann anhand einer darin eingebetteten Signatur und zweier kryptografischer Schlüssel prüfen, ob die übermittelte DNS-Information unverfälscht und authentisch ist, also vom zuständigen DNS-Server stammt.
- Wenn beide Prüfungen zu positiven Ergebnissen führen, gilt die DNS-Antwort als vertrauenswürdig (valide).

Quellen

Buchquelle

Kersken, Sascha (2017): IT-Handbuch für Fachinformatiker. Der Ausbildungsbegleiter. 8. Auflage, revidierte Ausgabe. Bonn: Rheinwerk Verlag; Rheinwerk Computing.

Schreiner, Rüdiger (2014): Computernetzwerke. Von den Grundlagen zur Funktion und Anwendung. 5., erw. Aufl. München: Hanser.

Srocke, Dirk (2018): Was ist DNS (Domain Name System)? In: IP-Insider, 01.08.2018. Online verfügbar unter https://www.ip-insider.de/was-ist-dns-domain-name-system-a-579256/, zuletzt geprüft am 06.05.2021.

Reihenfolge der Microsoft TCP/IP-Hostnamensauflösung (2021). Online verfügbar unter https://support.microsoft.com/de-de/topic/reihenfolge-der-microsoft-tcp-ip-hostnamensaufl%C3%B6sung-dae00cc9-7e9c-c0cc-8360-477b99cb978a, zuletzt aktualisiert am 06.05.2021, zuletzt geprüft am 06.05.2021.

Abbildungen

5 „Ende 2006 gab es zusammen mit allen Anycast-Instanzen 123 Root-Server“ Lizenz: No machine-readable author provided. Matthäus Wander assumed (based on copyright claims). (https://commons.wikimedia.org/wiki/File:Root-current.svg), „Root-current“, https://creativecommons.org/licenses/by-sa/3.0/legalcode

VIELEN DANK!