

DNS – Domain Name System

WAS IST DNS?

DNS ist eine verteilte Datenbank mit hierarchischer Struktur zur Auflösung von Internetnamen in IP-Adressen und umgekehrt.

Verwendung für:

- ⇒ Forward Lookup (Auflösung von Namen in IP-Adressen)
- ⇒ Reverse Lookup (Auflösung von IP-Adressen in Namen)
- ⇒ Suche nach Mailservern (MX-Record)
- ⇒ Suche nach Domänen-Controller (SRV-Records)

COMPUTERNAMEN

- ⇒ Hostname
 - bis zu 255 Zeichen lang
 - alphanumerische Zeichen, „ - “ und „ . “
 - Teil des FQDN
- ⇒ NETBIOS-Name
 - Steht für einen einzelnen Computer oder eine Gruppe von Computern
 - 15 Zeichen für den Namen
 - das 16. Zeichen steht für den Dienst, z.B. 00 - Arbeitsstationsdienst, 20 - Serverdienst

HAUPTBESTANDTEILE VON DNS:

- ⇒ DNS-Domain-Namespace
- ⇒ DNS-Zonen
- ⇒ DNS-Server

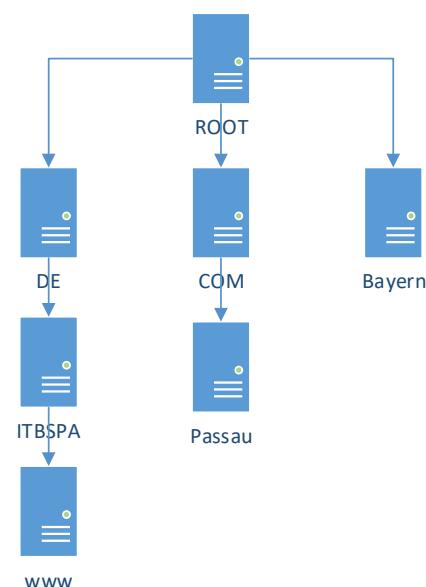
AUFBAU DES DNS-NAMESPACE

Der Namespace von DNS ist hierarchisch aufgebaut. Die Rootserver „ . „ verwalten alle Adressen aller Top-Level-Domains (TLD: z.B. .DE, .COM, .BAYERN ...)

Die Secondlevel-Domains werden von den TLDs verwaltet. (z.B. itbspa.de ist bei der Denic registriert, die zuständigen DNS-Server für itbspa.de sind hier mit Namen und IP-Adressen hinterlegt). Jede Second-Level-Domain benötigt dann einen eigenen DNS-Server, der die Hosts dieser Zone verwaltet.

Der komplette Name eines Hosts inklusive des Namens der Domäne wird als FQDN bezeichnet.

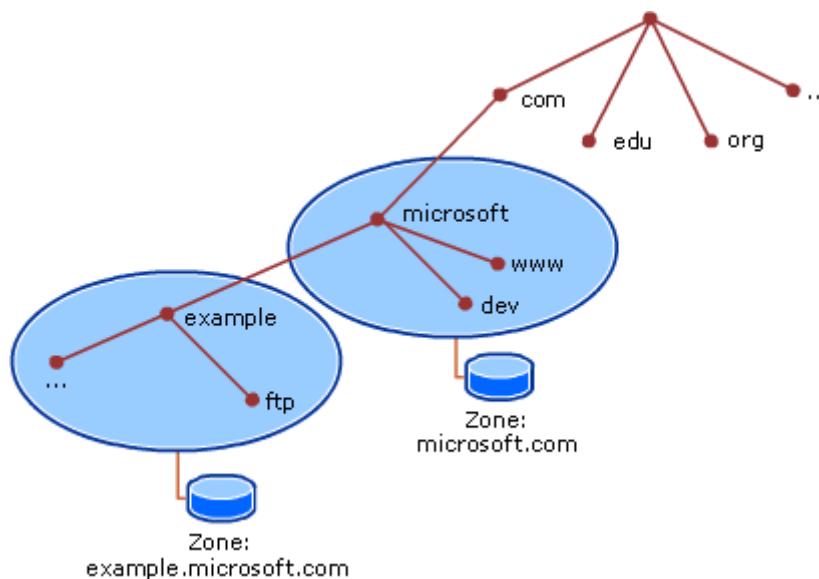
FQDN = Fully Qualified Domain Name



- ⇒ Hostname + vollständiger Domänenname

DNS – ZONEN

Zonen sind Untermengen des DNS-Namespace. Für jede Zone gibt es einen verantwortlichen DNS-Server, der für die Verwaltung der Hosts in der Zone zuständig ist.



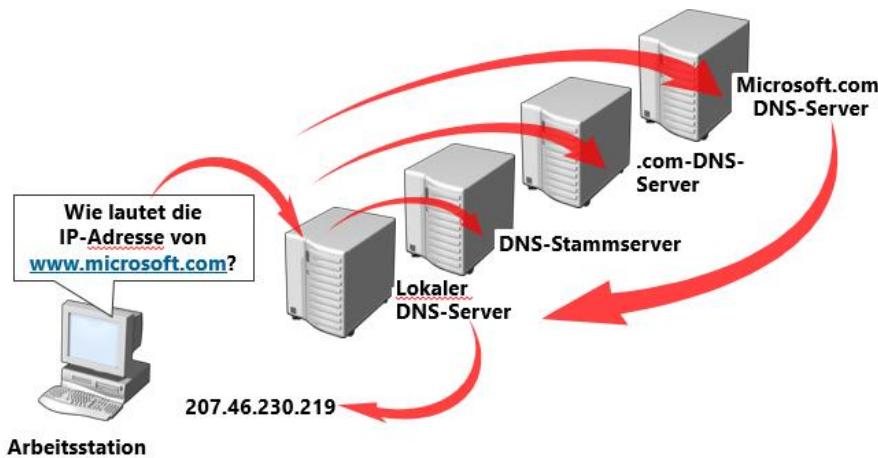
- | | |
|--|---|
| Primärer DNS-Server:
- speichert das Primary Zone Database File
- besitzt Lese- und Schreibrechte | Sekundärer DNS-Server:
- besitzt eine Kopie des DNS-Datenbank-Files
- besitzt nur Leserechte |
|--|---|

DNS – SERVER

DNS-Server sind für die Verwaltung der DNS-Datenbank zuständig. Die Einträge in den verwalteten Zonen (Forward-Lookup- und Reverse-Lookup-Zone) werden als Ressource Records bezeichnet.

RESSOURCE-RECORDS:

- ⇒ Host (A)-Einträge – IP-Adresse und Name
- ⇒ Host (AAAA) – Einträge – Ipv6-Adresse und Name
- ⇒ Alias-Einträge (CNAME) – Verweis auf anderen Host
- ⇒ Diensteinträge (SRV) – gibt die IP-Adresse u. Port-Adresse für spezielle Dienste an, z.B. Active Directory Anmeldeserver
- ⇒ MX-Einträge (Mail Exchanger) – gibt einen Mailserver an
- ⇒ SOA-Einträge (Start of Authority) – speichert Informationen zur Zone, z.B. Nameserver, TTL
- ⇒ Einträge für Namenserver (NS) – zuständige Nameserver für eine Zone
- ⇒ PTR – Record – weist einer IP-Adresse einen Namen zu.

DNS-ANFRAGEN**ABLAUF:**

- 1 Der Arbeitsplatz schaut in eigenen Cache nach, ob der Name schon aufgelöst ist.
- 2 Wenn nein: Die Arbeitsstation fragt rekursiv wegen dem Domain-Namen www.microsoft.com beim lokalen DNS-Server an.
- 3 Der lokale DNS-Server leitet iterativ die Anfrage an den DNS-Stammserver (root) weiter und bekommt die IP-Adresse des TLD-Servers zurück ("com").
- 4 Der lokale DNS-Server leitet iterativ die Anfrage an den Top-Level-Server für "com" weiter und bekommt die IP-Adresse des Second-Level-DNS-Servers ("microsoft.com").
- 5 Der lokale DNS-Server leitet die Anfrage an den "microsoft.com"-DNS-Server weiter.
- 6 Er bekommt die Adresse des FQDN "www.microsoft.com" = 207.46.230.219 zurück gesendet und speichert im DNS-Cache diesen Eintrag.
- 7 Er meldet die Adresse an die Arbeitsstation (als nicht autorisiert) rekursiv zurück.
- 8 Der Eintrag wird im lokalen DNS-Cache auf Zeit gespeichert (DNS TTL).

Rekursiv:

der Client fordert die komplette Auflösung des Namens an

Iterativ:

Anforderung des bestmöglichen Ergebnisses, dies kann auch nur ein Verweis auf einen anderen DNS-Server sein.

BEGRIFFE:**DNS-Forwarder:**

Ist ein DNS-Server, der DNS-Anfragen nach externen DNS-Namen an externe DNS-Server weiterleitet.
(Bsp.: Home-Router)

Root-DNS-Server:

DNS-Server der obersten Instanz. Sie kennen alle Nameserver der Top-Level-Domains.

