**Theoretische Grundlage**

### DNS

#### Vorgängermodelle

##### Host.txt

Die früher verwendete host.txt (RFC 226) Datei war damals für wenige hunderte oder tausende Rechner ausreichend. Diese Datei wurde jeden Tag einmal aktualisiert und damit auf den neuesten Stand gebracht. Heute findet man im Ordner C:\Windows\System32\Drivers\etc. immer noch (auch auf Windows10) diese host.txt Datei. Die Datei enthält unter Windows10 keine Einträge, da diese nichtmehr auf der host.txt, sondern am DNS abgespeichert werden.

#### WINS

Ein Bild, das Text enthält.

Automatisch generierte BeschreibungEine heute nichtmehr gebräuchliche Art des DNS ist der WINS. Der Windows Internet Naming Service ist ein veralteter, nur mehr auf älteren Windows Systemen zu findender Dienst. Im Unterschied zum heute herkömmlichem DNS wandelt WINS keine hierarchisch angeordneten Namen in IP-Adressen um. Hier werden NetBIOS Namen umgewandelt. NetBIOS Namen haben keine Struktur. Es wird beispielsweise nicht Angerer.server.at, sondern Angerer eingegeben. Windows arbeitet hier mit dem PDC.

Abbildung 2 Screenshot vom privaten Computer host.txt; Dateipfad C:\Windows\System32\Drivers\etc.

#### DNS

Der Gebrauch der host.txt Datei war damals für die wenigen Tausend Rechner ausreichend. Laut ITU werden im Jahr 2022 voraussichtlich 410 Millionen Computer verkauft werden. Das ergibt rund 13 Stück pro Sekunde. Auf diese Menge an Rechnern kann das Prinzip der host.txt Datei auf Grund der enormen Menge nicht mehr angewendet werden. Hier kommt das Domain Name System zum Einsatz. Ein einziger DNS-Server ist hier nicht ausreichend. Durch den hohen Datentransfer auf einen einzigen Server würde der theoretisch auf dem Application Layer verankerte Service direkt überlasten. Daher das Konzept der Zonen. Einige dieser TLDs sind .com, .at, .org, .net, oder .ch. TLDs bezeichnen den letzten Abschnitt einer Domain, dieser ist die hierarchisch am höchsten gelegene im Namensraum. Jede Zone hat mehrere eigene DNS-Server zur Verfügung. Die österreichische Verwaltung ist im Internet unter <https://www.nic.at> zu finden.

Jede im Internet erreichbare Zone muss zwingend einen DNS-Server betreiben. Hierarchisch an höchster Stelle liegen insgesamt 13 Root-DNS-Server. Diese kennen alle darunter liegenden, jeweils die für eine spezifische Zone zuständigen DNS-Server.

Ein Bild, das Diagramm enthält.

Automatisch generierte Beschreibung

Abbildung 3 Aufbau DNS Server; https://www.elektronik-kompendium.de/sites/net/bilder/09011414.gif

#### Beispiel

Ausgegangen wird, dass der bediente PC angerer.bsp.com heißt. Dieser will auf den Rechner www.server.com zugreifen. Da der PC die IP-Adresse von www.server.com benötigt, schickt er eine Anfrage an den DNS-Server dns.bsp.com. Da die beiden Maschinen in der gleichen Zone liegen und hierarchisch gleichrangig sind, wird dns.bsp.com die Anfrage sofort beantworten können.

Nun will der gleiche PC angerer.bsp.com aber auf eine in einer höheren Zone liegenden Website edelmann.bsp.at zugreifen. Der Server dns.bsp.com hat die IP-Adresse von edelmann.bsp.at nicht gespeichert. Er gibt also die Anfrage an den DNS-Server dns.bsp.at weiter. Wenn die IP-Adresse für edelmann.bsp.at nun gespeichert ist, wird diese über dns.bsp.com an das Ziel weitergeleitet.

**Praktischer Teil**

Nach Inbetriebnahme des Servers wird zuerst der Befehl “sudo apt install bind9” ausgeführt. “Sudo” führt einen Befehl mit Root-Rechten aus. Vor jeder Ausführung eines Befehls mit Root-Rechten wird das Passwort für den jeweiligen Benutzer abgefragt. Der Zusatz “apt” (Advanced Package Tool) ist für die vereinfachte und schnelle Installation von Packages verantwortlich. Es basiert auf Debian und Ubuntu basierenden Distributionen und ist das Dienstprogramm, welches für die Paketverwaltung zuständig ist. Dieser Befehl kann in der Befehlszeile mit “apt [comand] [package]” ohne weiteres verwendet werden. Da doch die meisten Befehle auf der Systemebene passieren, ist der vorher genannte Befehl “sudo” wichtig. “apt install” installiert in diesem Fall BIND-9.

BIND-9 ist eine DNS-Server Komponente und enthält grundlegende Informationen, welche für einen funktionierenden DNS-Server notwendig sind. In der Konfigurationsdatei können DNS-Servernahmen, Port auf den gehört werden soll, und DNS-Root-Server Adressen definiert werden. Durch einen Eintrag in diese Datei können ebenfalls Zonen und deren DNS-Einträge definiert werden.

Nach der Installation dieser Pakete wird mit “sudo apt install dnsutils” ein hilfreiches Tool installiert, welches gern für Troubleshooting und Testen von DNS-Problemen verwendet wird. “Dnsutils” ist üblicherweise schon vorinstalliert, bei diesem Server war das nicht der Fall, daher wird die erstmalige Installation mit dem genannten Befehl durchgeführt.

Im Verzeichnis „/var/cache/bind“ wird unter „forwarders“ die IP-Adresse 8.8.8.8 eingegeben. Diese ist eine öffentliche Adresse, welche Google als DNS-Resolver verwendet. Damit können Anfragen an Google gesendet werden. Die Erklärung dazu lautet wie folgt: wenn eine Datenabfrage erfolgt, wird zuerst im lokal Cache nach einer Antwort gesucht. Falls dieser die gewünschte Information nicht liefern kann, wird auf den in den „forwarders“ angegebenen Pfad zurückgegriffen.

Zuerst wird im Verzeichnis „db.local“ die Zone für die Domain „angerer.com“ erstellt.

Ein Bild, das Text enthält.

Automatisch generierte Beschreibung

Abbildung 23 Verzeichnis unter /etc/bind/db.local

„zone“ steht vor dem Domainnamen, für welchen DNS-Einträge erstellt werden sollen. „IN“ bedeutet, dass es sich um eine Internet-Adresse handelt. Nach der geschwungenen Klammer werden dann alle benötigten Konfigurationsparameter entworfen. „type master“ gibt an, dass es sich hierbei um eine Master-Zone handeln soll. Einfach ausgedrückt ist der Server angerer.com nun die primäre Informationsquelle. Die nächste Zeile beschreibt, dass alle DNS-Einträge für diese Zone im Verzeichnis „db.angerer.com“ abgespeichert werden, wie zum Beispiel die Informationen, die vom DNS-Server verwendet werden. Die geschwungene Klammer schließt die Konfiguration ab. Dieses Verzeichnis kann nun verlassen werden. Nun wird der Befehl „sudo cp /etc/bind/db.local /etc/bind/db.angerer.com“ angewendet, um die Datei „db.local“ in die im gleichem Verzeichnis liegende Datei „db.angerer.com“ zu kopieren.

Anschließend wird das Verzeichnis unter „nano /etc/bind/db.angerer.com“ geöffnet.

Ein Bild, das Text enthält.

Automatisch generierte Beschreibung

Abbildung 24 Einstellung im Verzeichnis /etc/bind/db.angerer.com

$TTL 604800 gibt an, dass der DNS-Server lokale Kopien der DNS-Einträge 6048000 Sekunden, bzw. eine Woche lang im Cache speichert. Nach dieser Woche wäre ein erneutes Abrufen der Einträge nötig. Die darauffolgende Zeile bestimmt, dass der Server „angerer.com“ der SOA-Server und der root.angerer.com der Verantwortliche ist. Serial ist die Versionsnummer der erstellten DNS-Zone. Durch diese Nummer wird sichergestellt, dass DNS-Clients immer die neusten Informationen vom DNS-Server erhalten. Die Refresh-Dauer gibt an, dass der angerer.com Server mindestens einmal wöchentlich aktualisiert werden muss, um immer auf neuster Informationsebene zu sein. „86400 ;Retry“ bedeutet, dass der DNS-Server, falls keine sofortige Verbindung aufgebaut werden kann, alle 24 Stunden erneut versucht wird. Die SOA-Informationen sollen, wenn dieser nicht erreichbar ist, 28 Tage lang im Cache behalten werden.

„@ IN NS ns.angerer.com“ definiert den Namenserver-Zuständigkeitseintrag für die Zone „angerer.com“. Unser Eintrag beschreibt, dass der DNS-Server „ns.angerer.com.“ dafür zuständig ist. In der nächsten Zeile wird die IP-Adresse des Hosts, bzw. die Adresse mit der der Domainname „angerer.com“ verknüpft ist angegeben - in diesem Fall: 192.168.1.10. Die vorletzte Zeile gibt einen AAAA-Eintrag für „root.angerer.com“ an. Das bedeutet, dass eine IPv6-Loopback-Adresse nun definiert ist. „::1“ ist die IPv6 Version der IPv4 Loopback-Adresse 127.0.0.1. Diese wird verwendet, um einen Netzwerkaufbau zu sich selbst zu simulieren. Dadurch wird sichergestellt, dass auf den lokalen DNS-Server über IPv6 zugegriffen werden kann.

Als nächstes wird die Datei „named.conf.local“ mit dem Befehl „nano etc/bind/named.conf.local“ geöffnet.

Ein Bild, das Text enthält.

Automatisch generierte Beschreibung

Abbildung 25 Einstellung im Verzeichnis /etc/bind/named.conf.local

Hier werden typischerweise lokale Zonen und Forward-Lookup-Informationen konfiguriert. Nach diesem Prinzip ist der erste Eintrag eine Forward-Lookup-Zone für „angerer.com“, der zweite Eintrag beschreibt die Reverse-Lookup-Zone für den IP-Addressbereich 192.168.0.0/24. Die als erstes definierte Zone gibt an, dass der Namensserver der Master für die Forward-Lookup-Zone ist und unter „/etc/bind/db.angerer.com“ zu finden sein wird. In dieser Datei sind alle DNS Einträge, wie A-Records, MX-Records etc., für alle Hosts in der Domain „angerer.com“ definiert.

Die letzere Zone definiert eine Reverse-DNS-Zone für das Netz 10.0.2.0/24. Diese Zone ist nötig, um Geräte im Netzwerk untereinander identifizieren zu können. Es wird der Netzwerkadressbereich der IP-Adressen umgekehrt angegeben. Daraus folgt, dass „10.0.2.in-addr.arpa“ der umgekehrte Netzwerkadressbereich der IP-Adressnen im Netzwerk 10.0.2.0/24 ist. „type master“ gibt an, dass der lokale BIND-Server die primäre Quelle für alle Änderungen in dieser Zone ist. „etc/bind/db.10“ gibt den Pfad zu den Zonendateien für diese Zone an.

Nun wird auf die Datei db.10 zugegriffen.

Ein Bild, das Text, Screenshot, Elektronik, Computer enthält.

Automatisch generierte Beschreibung

Abbildung 26 Einstellung im Verzeichnis /etc/bind/db.10

$TTL ist gleich wie unter db.angerer.com definiert. Die nächste Zeile gibt Auskunft über die Zone und den Server, der für die Verwaltung der jeweiligen Zone verantwortlich ist. Hier ist das „@“ Platzhalter für den vorher in Datei „/etc/bind/named.conf.local“ Namen der Zone.

Die vorletzte Zeile weist den Namenserver „ns“ als autoritativer Nameserver für die in der Datei „named.conf.local“ definierten Zone zu. Die letzte Zeile beschreibt einen Reverse-DNS-Eintrag für die IP-Adresse 10.0.2.0. Das bedeutet, dass die genannte IP-Adresse auf den Hostnamen „ns.angerer.com“ aufgelöst wird. PTR bedeutet Pointer und wird verwendet, um Reverse DNS-Auflösung zu ermöglichen. Das bedeutet, dass eine IP-Adresse auf den entsprechenden Hostnamen aufgelöst wird.