



Technische Berufsschule Zürich TBZ  
Informationstechnik

# Kapitel 2 - Serverdienst - DNS

Domain Name System

Modul 123

Andy Corsten, 08.11.2022



## Inhaltsverzeichnis

1.1	Die Geschichte des «Domain Name System» .....	3
1.2	Namensauflösung unter Windows.....	3
1.3	Die hosts-Datei.....	4
1.4	Die Hierarchische Struktur des DNS .....	4
1.4.1	Namespace .....	4
1.4.2	FQDN .....	4
1.4.3	Name-Server .....	5
1.5	Root-Server .....	5
1.6	.in-addr.arpa-Domain .....	5
1.7	Richtlinien zum Erstellen des Domänennamespace .....	6
1.8	Namensauflösung .....	6
1.8.1	Forward-Lookup .....	6
1.8.2	Reverse-Lookup .....	8
1.9	Protokoll .....	9
1.10	Typen von DNS-Servern .....	9
1.11	Zonen .....	10
1.11.1	Zonenname .....	10
1.11.2	Zonendatei .....	10
1.11.3	Zonentyp .....	10
1.12	Aufbau der DNS-Datenbank.....	10
1.12.1	Dateien des DNS .....	10
1.12.2	Zonendateien im Detail .....	11
1.12.3	Mögliche Einträge in der Zonendatenbankdatei .....	11
1.13	Dezentralisierung mit Anycast.....	12
1.14	Dynamisches DNS unter Windows .....	12
1.15	Switch.....	12
1.16	WINS - Der Windows Internet Name Service .....	12
2.1.1	Dienst kontrollieren .....	13

# 1 Domain Name System (DNS) - Wie der Client seinen Server findet

## 1.1 Die Geschichte des «Domain Name System»

Das Domain Name System (DNS) ist einer der wichtigsten Dienste in vielen IP-basierten Netzwerken. Seine Hauptaufgabe ist die Beantwortung von Anfragen zur Namensauflösung. Das DNS funktioniert ähnlich wie eine Telefonauskunft. Der Benutzer kennt die Domain (den für Menschen merkbaren Namen eines Rechners im Internet) - zum Beispiel example.org. Diese sendet er als Anfrage in das Internet. Die URL wird dann dort vom DNS in die zugehörige IP-Adresse (die „Anschlussnummer“ im Internet) umgewandelt - zum Beispiel eine IPv4-Adresse der Form 192.0.2.42 oder eine IPv6-Adresse wie 2001:db8:85a3:8d3:1319:8a2e:370:7347, und führt so zum richtigen Rechner.

TCP/IP greift auf andere Computer ausschliesslich über die IP-Adresse zu. Da sich Menschen aber Computernamen leichter merken als IP-Nummern, wurden Konzepte entwickelt, Computernamen IP-Adressen zuzuordnen. DNS ist das im Internet verwendete Konzept zur Namensauswertung. Es handelt sich um eine verteilte Datenbank.

Zu Beginn war das Internet eine überschaubare Menge zusammen geschalteter Rechner. Alle Administratoren erstellten auf jedem Rechner eine Datei, in der in jeder Zeile ein Pärchen aus IP-Adresse und Hostname stand. Pro Rechner im Netz also eine Zeile. Diese Dateien werden «hosts-Dateien» genannt.

Jeder Systemadministrator musste seine hosts-Dateien selber pflegen. Jedes Mal wenn ein Rechner neu dazu kam, musste eine neue Zeile eingetragen werden. Beim Ändern einer Adresse musste diese auch in allen hosts-Dateien geändert werden. Das Ganze wurde bald unübersichtlich, so dass unterschiedliche Versionen der hosts-Dateien herumgeisterten.

Aus diesem Grund folgte die Gründung von «Internic», einer Universitätsstelle die die hosts-Dateien verwaltete. Administratoren meldeten Änderungen dorthin und bezogen aktuelle Versionen von dort. Mit dem weiteren Anwachsen des Rechnerbestands war auch dieser Internic-Server bald einmal überlastet. Als Folge davon wurde das DNS-System entwickelt. Ein System von Namensservern, das nur bei Bedarf den benötigten Datensatz an den anfragenden Rechner sendet.

## 1.2 Namensauflösung unter Windows

*Unter Windows sind die folgenden Dateien für die Namensauflösung zuständig:*

Lokal verwaltet	LMHOSTS	für NETBIOS-Namen
	HOSTS	für Internet-Namen
Zentral in Datenbank verwaltet	WINS	NETBIOS-Namen
	DNS	Internet-Namen

## 1.3 Die hosts-Datei

Die hosts-Datei ist die günstigste und einfachste Variante zur Namensauflösung. Darum werden auf jeder Arbeitsstation des Netzwerks die IP-Adressen und Domänen-Namen aller Rechner eingetragen. Die hosts-Datei ist grundsätzlich auf jedem Rechner vorhanden. Sie wird als erste Informationsquelle vom «Resolver» kontaktiert.

```
Windows NT/2000    c:\windows\system32\drivers\etc
Linux              /etc
```

In Windows gibt es eine Beispiel-Datei «hosts.sam». Diese wird kopiert, individuell angepasst und im gleichen Verzeichnis gespeichert unter «hosts».

```
# Copyright (c) 1993-2009 Microsoft Corp.
# This file contains the mappings of IP addresses to host names.
# Each entry should be kept on an individual line.
# 102.54.94.97  rhino.acme.com      # source server
# 127.0.0.1    localhost
```

*Die hosts-Datei von Linux:*

```
# Syntax:
# IP-Address Full-Qualified-Hostname Short-Hostname
127.0.0.1    localhost
192.168.100.101 M123-Suse10_Scg.ARBEITSGRUPPE M123-Suse10-Scg
```

Die aktuellen hosts-Dateien sind erweitert um ipv6-Einträge.

Der Resolver ist die Software die für die Namensauflösung zuständig ist. Der Resolver ist Teil der Netzwerkdienste des Betriebssystems. Bei Linux zu finden unter «/etc/resolv.conf».

## 1.4 Die Hierarchische Struktur des DNS

### 1.4.1 Namespace

Eine DNS-Domäne ist ein Namensraum (Namespace) der begrenzt wird durch den Inhalt der DNS-Datenbank, die als Zonendatei bezeichnet wird. Der DNS-Name (FQDN) ist streng hierarchisch aufgebaut und wird von hinten nach vorne gelesen. Die Stammdomäne (Root) ist die oberste Domäne einer Hierarchie und verwendet eine Nullbezeichnung «.». Direkt unter der Stammdomäne befindet sich die erste Ebene (Top-Level-Domains). Diese TLDs werden nach Organisationstyp oder nach Land eingeteilt. Auf der nächsten Ebene (Second-Level-Domains) können sowohl Hosts als auch Teildomänen (firma.ch) enthalten sein. Darunter liegen die Domänen der dritten, vierten, etc. Ebene.

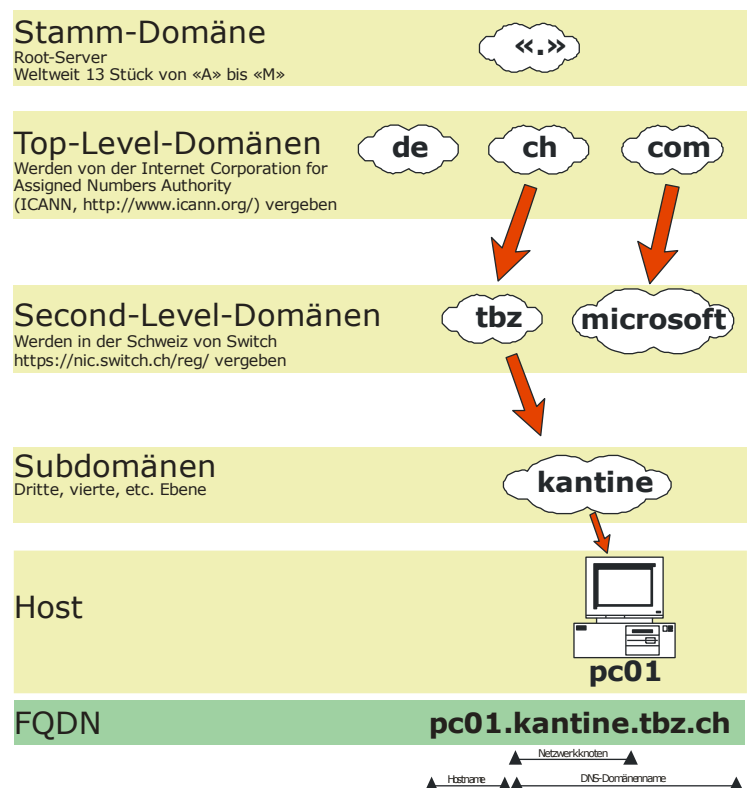


Abb. 1 Hierarchische Struktur des DNS

### 1.4.2 FQDN

Der komplette DNS-Name («FQDN» = «Fully Qualified Domain Name») für einen Host besteht aus dem Hostnamen und dem DNS-Domännennamen. Der Computer «pc01» ist Host in der DNS-Domäne «kantine.tbz.ch».

### 1.4.3 Name-Server

Gibt man im eigenen Browser einen Domännennamen ein, stellt der Rechner eine Anfrage an den Namensserver. Im Internet ist dies in der Regel der Namensserver des Providers. Sind die angeforderten Namen dort nicht verfügbar, so wird die Anfrage zu einem anderen Namensserver weiter geleitet. Jeder Namensserver besitzt eine fest konfigurierte Liste der Root-Server. Dort beginnt jeweils die Suche nach einem Namen. Die Root-Server kennen alle Namensserver die Toplevel-Domänen verwalten.

Ein DNS-Server tritt niemals alleine auf; es gibt immer einen Primary- und einen Secondary-Nameserver. Sie sind voneinander unabhängig und redundant ausgelegt. Der Secondary gleicht in regelmässigen Abständen seine Daten mit dem Primary ab. Jeder DNS-Server hat einen Cache, in dem er erfolgreiche DNS-Anfragen abspeichert. Die gespeicherten Daten haben eine TTL von ca. 2 Tagen.

Liste der Root-Server unter: <ftp://ftp.internic.net/domain/named.root>

## 1.5 Root-Server

Es gibt momentan weltweit 13 Root-Server. Jeder Namensserver muss die Adresse der Root-Server kennen.

<http://www.root-servers.org/> Zentrale Übersichtsseite der offiziellen DNS Root-Server.

A.ROOT-SERVERS.NET	198.41.0.4	H.ROOT-SERVERS.NET	128.63.2.53
B.ROOT-SERVERS.NET	128.9.0.107	I.ROOT-SERVERS.NET	192.36.148.17
C.ROOT-SERVERS.NET	192.33.4.12	J.ROOT-SERVERS.NET	198.41.0.10
D.ROOT-SERVERS.NET	128.8.10.90	K.ROOT-SERVERS.NET	193.0.14.129
E.ROOT-SERVERS.NET	192.203.230.10	L.ROOT-SERVERS.NET	198.32.64.12
F.ROOT-SERVERS.NET	192.5.5.241	M.ROOT-SERVERS.NET	202.12.27.33
G.ROOT-SERVERS.NET	192.112.36.4		

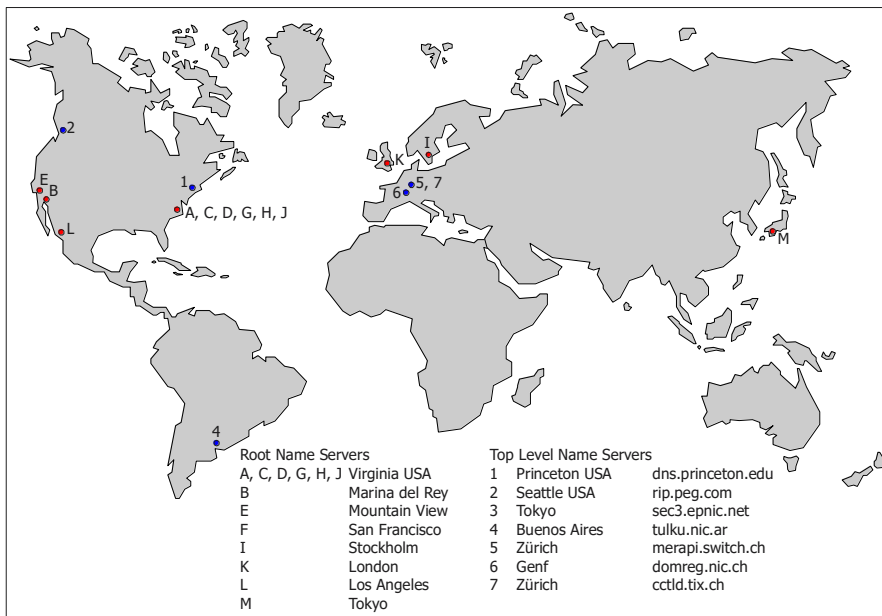


Abb. 2 13 Rootserver weltweit

## 1.6 .in-addr.arpa-Domain

Damit wurde die erste Top-Level-Domain eingerichtet, die später durch weitere Domains (.com, .net, etc.) abgelöst wurde. Die Top-Level-Domain .arpa führt jedoch bis heute ihr Eigenleben mit der Second-Level-Domain in-addr. Unterhalb von .in-addr.arpa sind die DNS-Einträge für das sog. Reverse-Mapping angelegt, mit dessen Hilfe man bekannte IP-Adressen in Domainnamen auflöst. Die in-addr.arpa-Domain wird auch als inverse Domain bezeichnet. Diese bildet man, indem die IP-Adresse rückwärts gelesen und der String .in-

addr.arpa angehängt wird. Somit findet man die Reverse-Mapping-Informationen für die IP-Adresse 62.96.227.70 im Domänennamen 70.227.96.62.in-addr.arpa.

## 1.7 Richtlinien zum Erstellen des Domänennamespace

Eine DNS-Struktur darf bis zu 5 Ebenen enthalten.

Die Namen für Subdomänen einer Domäne müssen eindeutig sein.

Die maximale Länge eines Domänennamens beträgt 63 Zeichen (inkl. Punkte).

Die Gesamtlänge eines FQDN beträgt maximal 255 Zeichen.

## 1.8 Namensauflösung

Bezeichnet den Vorgang, bei dem ein DNS-Namensserver zu einer IP-Adresse den zugehörigen Hostnamen ermittelt. Auch der umgekehrte Weg ist möglich. Anwendungen wie http, telnet oder ftp verwenden DNS zum Auffinden von Zielcomputern.

### 1.8.1 Forward-Lookup

Name wird eingegeben → IP-Adresse wird gesucht

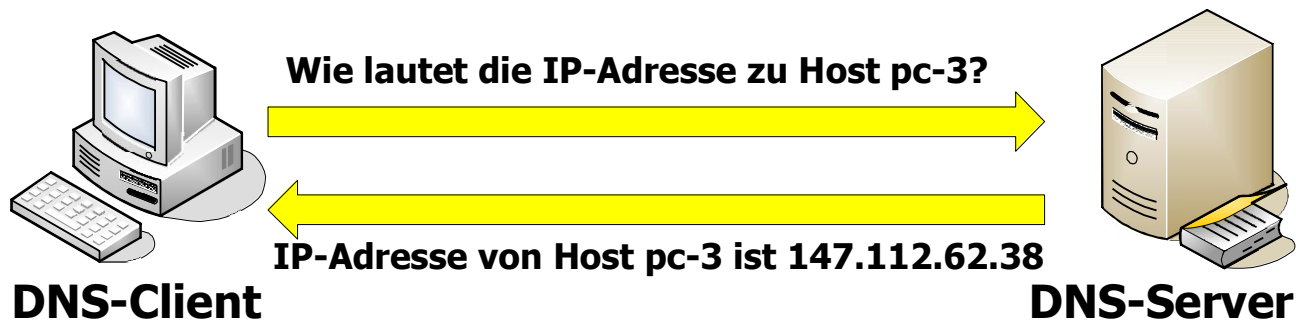


Abb. 3 Forward-Lookup

Die Namensauflösung wird logisch immer an der Wurzel des Baums gestartet, und arbeitet dann «abwärts». Die Namensauflösung wird durch einen DNS Client (DNS resolver), der in die Applikation (z.B. Browser) eingebunden ist, initiiert. Ein Namensserver kann nur solche Namen auflösen, für die er autorisiert ist, d.h. für die er Einträge in seiner DNS-Datenbank (=Zonendatei) besitzt. Erhält ein Namensserver eine Abfrage die er selbst nicht auflösen kann, übergibt er die Anfrage an einen übergeordneten (Root-)Namensserver.

### 1.8.1.1 Beispiel: Reales Leben - Wie funktioniert eine Anfrage nach Adresse

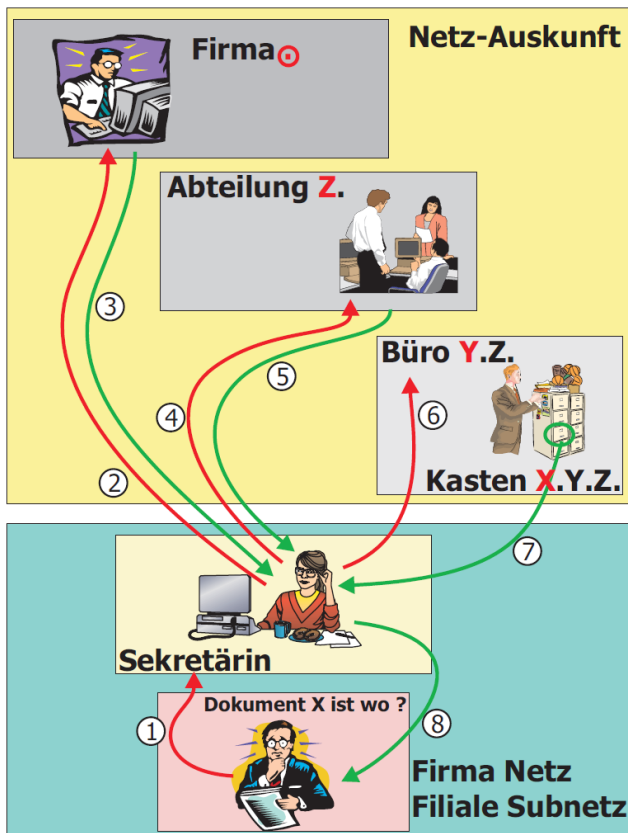


Abb. 4 Beispiel reales Leben: Wie funktioniert eine Anfrage nach Adresse

### 1.8.1.3 Rekursive Anfragen

Bei einer rekursiven Anfrage übergibt der Client seine Anfrage komplett einem Name-Server. Falls dieser den Namen selber nicht auflösen kann, kontaktiert dieser den nächsten zuständigen Server und erlaubt jenem wieder ein rekursives Bearbeiten der Anfrage. Erhält ein Namens-Server eine Anfrage, prüft er, ob der Name in seinem eigenen Unterbaum liegt. Ein Client (resolver) muss also nur die Adresse eines (bzw. «seines») Namens-Servers kennen. Da die meisten Abfragen lokal sind, werden in der Realität viele Abfragen lokal beantwortet. Sie belasten das Netzwerk nur wenig.

Stellt ein Client eine Anfrage an einen Name-Server, prüft dieser zunächst, ob er für den angefragten Rechner zuständig ist. Wenn nicht, überprüft der lokale Server, ob ein entsprechender Eintrag im Zwischenspeicher (=Cache) vorhanden ist. Wenn ja, wird dem Client dieses zwischengespeicherte Ergebnis übermittelt, ohne dass der lokale Server die Anfrage an den wirklich zuständigen Server weiterleitet. Das Ergebnis wird in der Antwort des Servers als nonauthoritative (nicht autoritativ, nicht massgebend) ausgewiesen. Zusätzlich wird dem Client die Adresse des Servers übermittelt, von dem die weitergegebene Information stammt.

### 1.8.1.2 Beispiel: DNS - Anfrage nach Adresse «webmail.unizh.ch»

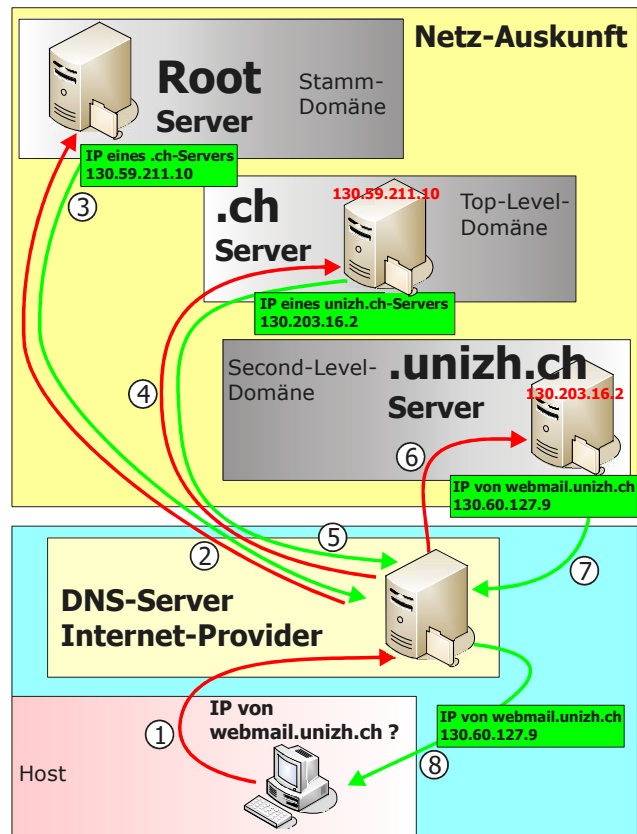


Abb. 5 Beispiel DNS: Anfrage nach Adresse «webmail.unizh.ch»

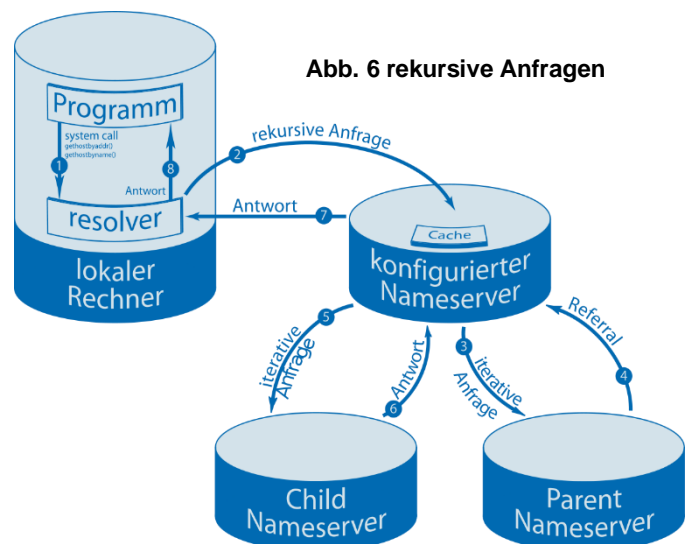


Abb. 6 rekursive Anfragen



### 1.8.1.4 Iterative Anfragen

Hierbei fragt der Client selber jeweils jeden im vorherigen Schritt ermittelten Server und gelangt über die Antworten schliesslich zum zuständigen Name-Server, der bei einer letzten Anfrage die Adresse übermittelt. Hierbei muss der Client evtl. viele Anfragen stellen was intensiven Netzwerkverkehr verursacht.

### 1.8.2 Reverse-Lookup

IP-Nummer wird eingegeben → Name wird gesucht

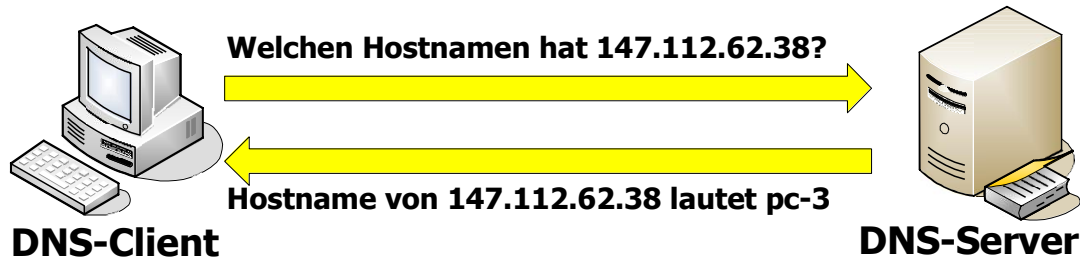


Abb. 7 Reverse-Lookup

Die spezielle Second-Level-Domain «in-addr.arpa.» enthält eine nach IP-Adressen organisierte Hierarchie. «in-addr.arpa.» ist somit ein Index für die Suche nach IP-Adressen.

Z.B.: Die Telefonnummer +46-8-9761234 soll in einen DNS-Namen umgewandelt werden:

Es werden alle Zeichen entfernt die keine Zahlen sind	4689761234
Zwischen jede Zahl wird ein Punkt gesetzt:	4.6.8.9.7.6.1.2.3.4
Die Zahlen werden umgedreht:	4.3.2.1.6.7.9.8.6.4
Ans Ende wird «.in-addr.arpa.» hinzugefügt:	4.3.2.1.6.7.9.8.6.4.in-addr.arpa

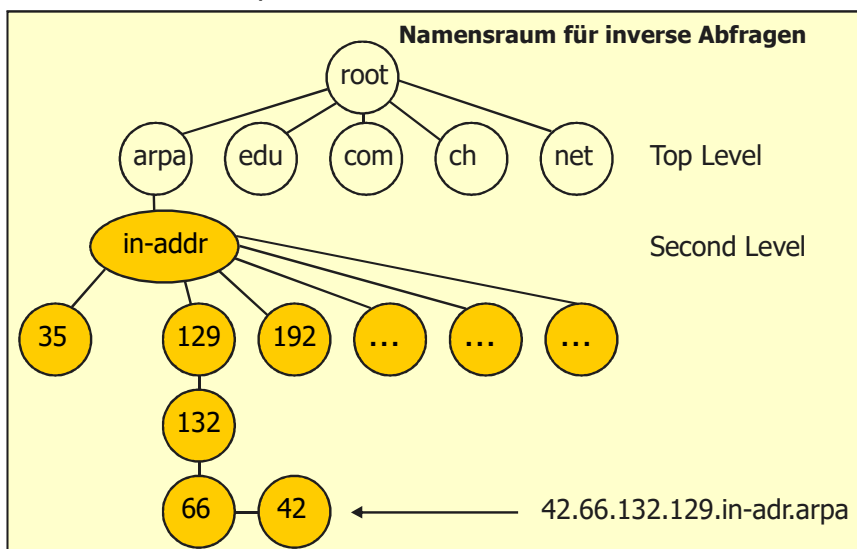


Abb. 8 Namensraum für inverse Abfragen



## 1.9 Protokoll

DNS ist auf der Anwendungsschicht des OSI-Modells angeordnet. Es nutzt zur Übertragung TCP und UDP auf dem **Port 53**.

In der Regel verwendet der Resolver das UDP-Protokoll. Wenn die Antwort grösser als 512 Byte gross ist, werden nur 512 Byte übertragen. Anschliessend muss der Resolver seine Anfrage noch einmal über TCP wiederholen, damit die Antwort in mehrere Segmente aufgeteilt werden kann. Der Datenaustausch zwischen Primary- und Secondary-DNS-Server wird nur mit TCP geregelt.

### TCP Vs. UDP

No.	TCP	UDP
1.	Connection Oriented Protocol	Connection-less Protocol
2.	Connection in byte stream	Connection in message stream
3.	It does't support multicasting and broadcasting	It supports broadcasting
4.	It provides error control and flow control	Error Control and Flow control is not provided
5.	Supports full Duplex	Does not support full Duplex
6.	TCP packet is called as Segment	UDP packet is called as User Datagram



Abb. 9 Die Protokolle TCP und UDP

## 1.10 Typen von DNS-Servern

Root	Root-Server	DNS-Server der obersten Hierarchie-Ebene. Zuständig für die Root-Domäne. Jeder DNS-Server muss die Root-Server kennen.
Zone	Primärer DNS-Server	Übernimmt die Zuständigkeit für eine (oder mehrere) Zonen. Er ist für die betreffenden Zonen autorisierend.
Zone	Sekundärer DNS-Server	Ist abhängig vom primären DNS-Server. Er holt sich regelmässig Kopien der DNS-Datenbank vom primären DNS-Server. Er hat zwei Möglichkeiten um das zu machen: Er lädt die komplette Zonendatenbank herunter (AXFR). er lädt nur Änderungen innerhalb eines bestimmten Zeitintervalls herunter (IXFR). Der sekundäre DNS-Server ist nicht autorisierend. Er kann keine Änderungen an der Zonen-Datenbank vornehmen. Er dient nur der besseren Verfügbarkeit des Dienstes und dem Lastausgleich.
Zone	Active Directory DNS-Server	Existiert nur auf Windows-Domänencontrollern.
	Caching-Only-DNS-Server	Speichert keine Zonendatenbank. Erhält keine Aktualisierung von einem primären DNS-Server. Dient nur dem Zwischenspeichern der Abfragen um den Netzwerkverkehr zu entlasten.
	Weiterleitende DNS-Server (Forwarder)	Leiten Anfragen weiter, die sie selbst nicht beantworten können.

Abb. 10 Typen von DNS-Servern

## 1.11 Zonen

### 1.11.1 Zonenname

In einer Zone werden Namen definiert, die in einer bestimmten Zonendatei (z.B. firma.ch.dns) verwaltet werden. Eine grössere Domäne kann in mehrere Zonen aufgeteilt werden. Ein DNS-Server kann eine oder mehrere Zonen verwalten. Üblicherweise wird eine Zone nach der höchsten Domäne in der Hierarchie benannt, der die Zone angehört (z.B. ch-Zone).

### 1.11.2 Zonendatei

Die Zonendatei beinhaltet alle Daten für die Namensauflösung. Standardmässig wird der Zonenname mit der Erweiterung .dns versehen. Wenn der Zonenname beispielsweise firma.ch lautet, wird als Standardname für die Zonendatenbankdatei der Name firma.ch.dns verwendet. Die Datei wird im Verzeichnis «C:\WINDOWS\System32\DNS» gespeichert.

### 1.11.3 Zonentyp

Es kann zwischen drei Zonen unterschieden werden:

**Primär:** In einer primären Zone wird die Original-Zonendatei von einem primären DNS-Server verwaltet.

**Sekundär:** In einer sekundären Zone kopiert ein sekundärer DNS-Server die Zonendatei eines anderen Servers, der wiederum primär oder sekundär sein kann. Das gewährleistet eine Redundanz und verteilt die Last der Namensauflösung.

**Active Directory-integriert:** Die Zonendatei wird im Active Directory gespeichert. Bei der Active Directory-Verzeichnisreplikation werden nur die relevanten Änderungen übermittelt. Daher ist sie schneller und effizienter als die Standard-DNS-Replikation.

## 1.12 Aufbau der DNS-Datenbank

### 1.12.1 Dateien des DNS

C:\WINDOWS\system32\dns\	
soltec.intern.dns	Zonendatenbankdatei für Forward-Lookup-Abfragen in der Zone soltec. Die Datenbank ist nach Hostnamen indiziert.
100.168.192.in-addr.arpa.dns	Zonendatenbankdatei für Reverse-Lookup-Abfragen in der Zone soltec. Die Datenbankdatei ist nach IP-Adressen indiziert.
cache.dns	In dieser Datei werden Ergebnisse von Namensauflösungen gespeichert, die für eine begrenzte Zeit zur Namensauflösung herangezogen werden.
root.dns	Diese Datei ist optional und wird vom Stammmamensserver gepflegt. Sie steuert das Starten des DNS-Dienstes.

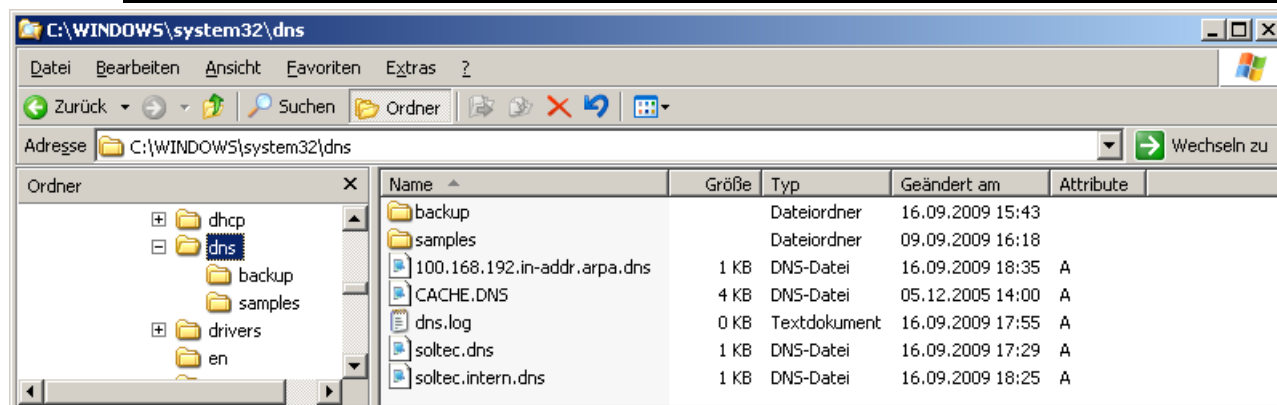


Abb. 11 Dateien des DNS

### 1.12.2 Zonendateien im Detail

Informationen innerhalb einer bestimmten Domain werden in so genannten Zonendateien gespeichert, die auf einem Nameserver im lokalen Netz oder im Internet liegen. Logisch gesehen sind sie eine Datenbank, die über spezielle DNS-Befehle abgefragt werden können.

Als Beispiel die Zonendatei der Domain *netplanet.org*:

Domain	Klasse	Typ	Eintrag
netplanet.org.	IN	SOA	ns.eplan.net.
			hostmaster.eplan.net (
			2003053102;serial
			28800 ; refresh
			7200 ; retry
			604800 ; expire
			86400 ) ; minimum
	IN	NS	ns.eplan.net.
	IN	NS	ns1.eplan.net.
	IN	NS	ns2.eplan.net.
	IN	MX	10 mailsrv1.eplan.net.
	IN	MX	20 mailsrv2.eplan.net.
	IN	A	80.245.65.1
www	IN	A	80.245.65.1

**Abb. 12 Zonendatei der Domain netplanet.org**

Die einzelnen Einträge in einer Zonendatei werden als Resource Record (RR) bezeichnet. Diese haben den Aufbau «Domain - Klasse - Typ - Eintrag»:

Die Domain enthält den Namen der Domain, für die die Zonendatei zuständig ist. In diesem Beispiel lautet diese Domain «netplanet.org» und gibt somit an, dass die Zonendatei entsprechend für diese Domain zuständig ist.

Die Klasse gibt das Netz an, für das der Eintrag gelten soll. Hier steht «IN» für das Internet. Daneben gibt es noch weitere Klassentypen, die jedoch für vergangene oder experimentelle Netze stehen.

Der Typ kennzeichnet den Typ des DNS-Eintrages. Befehle und Attribute siehe unten.

Der Eintrag enthält schliesslich die individuellen Werte und definiert die einzelnen Einträge innerhalb der Domain.

### 1.12.3 Mögliche Einträge in der Zonendatenbankdatei

Einträge in den Zonendatenbanken heissen Ressourceneinträge.

Objekt und Kürzel	Erklärung
Autoritätsursprung , SOA	Ressourceneintrag für den Stammmamensserver der jeweiligen Zone
Namensserver, NS	Jeder DNS-Server einer Zone wird anhand eines solchen Ressourceneintrags in der Zonendatenbank vermerkt.
Host, A	Ressourceneintrag für Forward-Lookup-Abfragen; diese Ressourceneinträge werden dynamisch aktualisiert.
Zeiger, PTR	Ressourceneintrag für die Namensauflösung im Reverse-Lookup-Verfahren. Der Wert eines Zeigers sind das letzte Oktett einer IP-Adresse und der Hostname.
Dienst, SRV	Mit einem Serverressourceneintrag können Netzwerkressourcen und Netzwerkdienste vermerkt und von Clients gefunden werden. Möchte ein Benutzer beispielsweise ein Dokument per Fax versenden, muss die IP-Adresse des Faxservers ermittelt werden.
Alias, CNAME	Ressourceneintrag für einen alternativen Hostnamen
Mail-Exchanger, MX	Ressourceneintrag für den Server, der eine Verbindung zu einer anderen Domäne herstellen kann
Hostinfo, HINFO	Ressourceneintrag für das Betriebssystem und die CPU des Hosts.

**Abb. 13 Einträge in Zonendatenbankdatei**

## 1.13 Dezentralisierung mit Anycast

Die RIPE NCC8 Organisation und DeNIC installierten einen DNS Root Server in Frankfurt. Dabei handelt es sich nicht um einen der 13 Root-Server, sondern es ist eine Spiegelung eines Root Servers mit Hilfe der Anycast Technik. Dieser gespiegelte Server verfügt über die gleiche IP wie der Root Server. Ein Anycast Server enthält die genau gleichen Daten wie sein Master. In diesem Fall ist der Master der K-Root Server. So lässt sich ein Verbund von Rechnern aufbauen, der über die gleiche IP-Adresse angesprochen wird. Die Stabilität erhöht sich, die Antwortzeiten sind kürzer und der DNS ist resistenter gegen DDoS. Ähnliches wurde mit dem F-Root Server gemacht und es ist geplant weitere Anycast Server zu installieren. Die Server sollen weltweit verteilt werden, sodass keine Konzentration von Root Servern mehr besteht.

Anycast kommuniziert mit einem Sender zum nächstgelegenen Empfänger aus einer Gruppe von möglichen Empfängern.

Unicast kommuniziert mit einem Sender zu einem Empfänger.

Multicast kommuniziert mit einem Sender zu einer Gruppe von Empfängern.

## 1.14 Dynamisches DNS unter Windows

*Ein DNS-Client kann dem DNS-Server seinen Hostnamen und seine IP-Adresse mitteilen, wenn Hostname oder IP-Adresse des Clients geändert werden. Damit verringert sich der Verwaltungsaufwand. Computer, die häufig an verschiedenen Orten im Netzwerk aufgestellt werden (Notebooks), sollten im Idealfall ihre IP-Konfiguration über den DHCP-Dienst zugeteilt bekommen. Dynamisches DNS und DHCP spielen so zusammen, dass die Zuordnung von Hostnamen zu IP-Adressen vom DHCP-Server an DNS mitgeteilt wird.*

Die Workstation fordert vom DHCP-Server eine IP-Adresse an.

Der DHCP-Server weist der Workstation eine IP-Adresse zu.

Der DHCP-Server übergibt den Hostnamen und die IP-Adresse zur Registrierung an DNS.

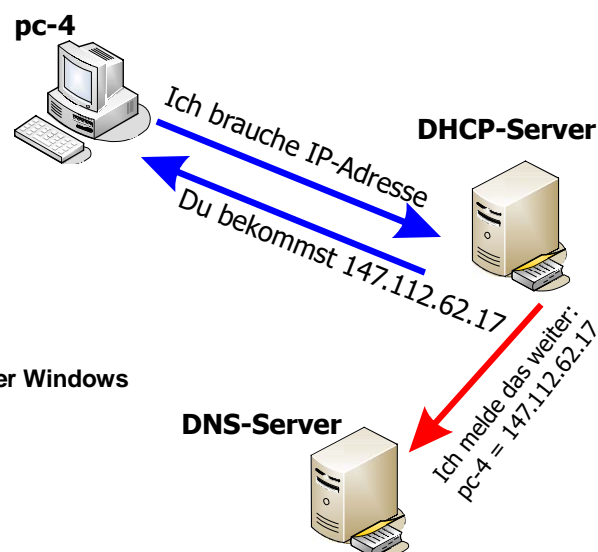


Abb. 14 Dynamisches DNS unter Windows

## 1.15 Switch

Wer in der Schweiz eine Homepage einrichten will, kommt um Switch nicht herum. Die Stiftung hält das Monopol. Es ist die vom Bundesamt für Kommunikation beauftragte Registrierungsstelle. Die Stiftung, die auch Internetdienstleistungen für Schweizer Hochschulen erbringt, registriert alle Domains mit den Endungen «.ch» und «.li». Gemäss Stiftungsurkunde verfolgt Switch weder kommerzielle Zwecke, noch ist sie auf Gewinnausgerichtet.

## 1.16 WINS - Der Windows Internet Name Service

Der primäre Zweck des Windows Internet Name Service (WINS) besteht darin, die Anfragen von Windows-Systemen zu beantworten, die versuchen, einen Computer im Netzwerk über dessen NetBios-Namen zu finden. Der WINS-Server übermittelt dabei dem anfragenden PC die IP-Adresse des gewünschten Computers, damit dieser anschliessend eine direkte

Verbindung (z.B. zu einer Freigabe) herstellen kann. Um diese Funktionalität zu erzielen, müssen die WINS-Clients (also die am Netzwerk angeschlossenen PCs) ihre jeweiligen NetBios-Namen sowie ihre IP-Adressen dynamisch beim WINS-Server registrieren, der diese Einträge in einer Datenbank verwaltet. Neben den Computernamen werden in WINS auch die IP-Adressen der Domänencontroller von Windows-Domänen (NT/2000/2003) registriert. Die Adressregistrierungen müssen von den Clients in regelmässigen Abständen erneuert werden, andernfalls gilt der PC als offline. WINS gibt also auch darüber Auskunft, ob ein Windows-System gerade aktiv ist oder nicht.

Gegenüber dem im Internet gebräuchlichen Namensauflösungsdienst DNS hat WINS verschiedene Nachteile. Der bedeutendste ist, dass er nur einen flachen Namensraum unterstützt. Dies hat zur Folge, dass die Namen von PCs und Windows-Domänen bzw. Workgroups eindeutig sein müssen, sofern alle denselben WINS-Server verwenden oder sich in demselben Subnetz befinden. Dies ist schon bei der Einrichtung eines Firmennetzes schwierig zu realisieren, für ein Netz im Massstab des Internet ist es jedoch ein Ausschlusskriterium. WINS findet daher nur in überschaubaren Netzwerken Verwendung, die unter einheitlicher Administration stehen. Es ist zudem auf Windows-Systeme beschränkt.

#### *Ablauf der Namensauflösung:*

- Der Client prüft seinen lokalen Cache, ob eine Adresse für den Namen vorliegt.
- Findet er keine Adresse, konsultiert er die Datei «hosts».
- Findet er keine Adresse, stellt er eine Anfrage an den DNS-Server.

#### *Zusätzliche Adress-Suche unter Windows:*

- Findet der Client via DNS-Server keine Adresse, wird der WINS-Server angefragt.
- Findet er auch dort keine Adresse, führt er einen NetBios-Rundspruch aus.
- Führt auch das nicht zum Ziel, hat Microsoft als letzte Möglichkeit die Datei «lmhosts» vorgesehen.

## **2 Einrichten eines DNS-Servers**

Beachten Sie die Links, die Ihnen zusammen mit dieser Theorie-Datei abgegeben wurden.

### **2.1.1 Dienst kontrollieren**

*Nslookup ist ein Befehlszeilen-Verwaltungsprogramm, das zusammen mit dem Protokoll TCP/IP installiert wird. Verwenden Sie dieses um die DNS Serverfunktionen zu testen. Öffnen Sie ein Konsolenfenster und geben Sie den Befehl nslookup mit Parametern ein.*

*nslookup.exe kann in zwei Modi ausgeführt werden:*

- interaktiv
- nicht interaktiv

Um nslookup.exe im interaktiven Modus zu starten, geben Sie «nslookup» in der Eingabeaufforderung ein:

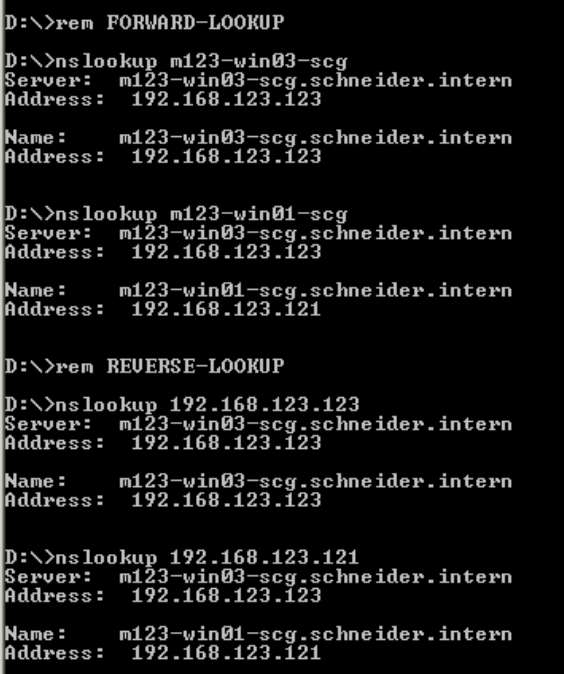
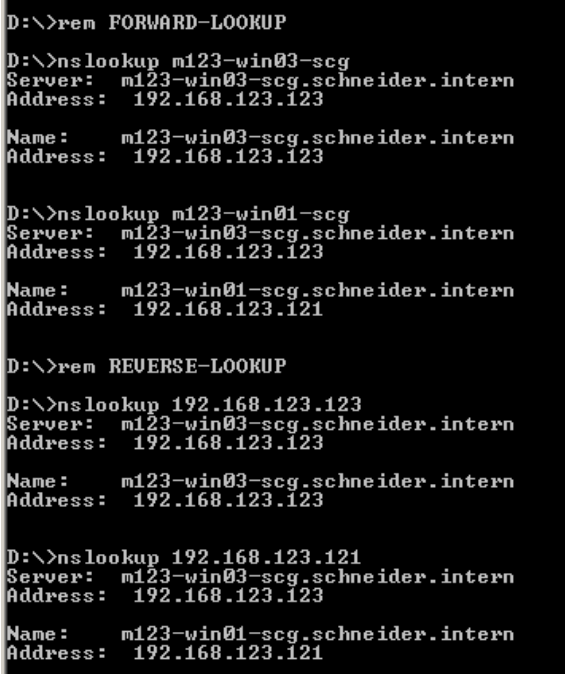
```
C:\> nslookup
Server:    m123-win2003.schneider.intern
Adress:    172.16.100.100
>
```

Interaktive Befehle können Sie mit Ctrl-C unterbrechen. Um den interaktiven Modus zu verlassen und auf die Eingabeaufforderung zurückzukehren, geben Sie exit (oder Ctrl-C) ein.

Der nicht interaktive Modus ist sinnvoll, wenn nur eine Dateneinheit zurückgeliefert werden soll. Syntax für den nicht interaktiven Modus:

```
nslookup [-option] [hostname] [server]
```

```
nslookup 192.168.100.100
nslookup m123-win2003
nslookup soltec.intern
nslookup srv2003.soltec.intern
nslookup m123-winXP.schneider.intern
```

Kontrolle auf dem Server	Kontrolle auf dem Client
 <pre>D:\&gt;rem FORWARD-LOOKUP D:\&gt;nslookup m123-win03-scg Server: m123-win03-scg.schneider.intern Address: 192.168.123.123  Name: m123-win03-scg.schneider.intern Address: 192.168.123.123  D:\&gt;nslookup m123-win01-scg Server: m123-win03-scg.schneider.intern Address: 192.168.123.123  Name: m123-win01-scg.schneider.intern Address: 192.168.123.121  D:\&gt;rem REVERSE-LOOKUP D:\&gt;nslookup 192.168.123.123 Server: m123-win03-scg.schneider.intern Address: 192.168.123.123  Name: m123-win03-scg.schneider.intern Address: 192.168.123.123  D:\&gt;nslookup 192.168.123.121 Server: m123-win03-scg.schneider.intern Address: 192.168.123.123  Name: m123-win01-scg.schneider.intern Address: 192.168.123.121</pre> <p><b>Abb. 15 Auslesen Zonendatei auf Server</b> Damit werden die Zonendateien ausgelesen</p>	 <pre>D:\&gt;rem FORWARD-LOOKUP D:\&gt;nslookup m123-win03-scg Server: m123-win03-scg.schneider.intern Address: 192.168.123.123  Name: m123-win03-scg.schneider.intern Address: 192.168.123.123  D:\&gt;nslookup m123-win01-scg Server: m123-win03-scg.schneider.intern Address: 192.168.123.123  Name: m123-win01-scg.schneider.intern Address: 192.168.123.121  D:\&gt;rem REVERSE-LOOKUP D:\&gt;nslookup 192.168.123.123 Server: m123-win03-scg.schneider.intern Address: 192.168.123.123  Name: m123-win03-scg.schneider.intern Address: 192.168.123.123  D:\&gt;nslookup 192.168.123.121 Server: m123-win03-scg.schneider.intern Address: 192.168.123.123  Name: m123-win01-scg.schneider.intern Address: 192.168.123.121</pre> <p><b>Abb. 16 Kontrolle Zonendatei auf dem Client</b> Hier muss dasselbe stehen wie auf dem Server</p>

## 3 Abbildungsverzeichnis

<b>Abb. 1 Hierarchische Struktur des DNS</b>	4
<b>Abb. 2 13 Rootserver weltweit</b>	5
<b>Abb. 3 Forward-Lookup</b>	6
<b>Abb. 4 Beispiel reales Leben: Wie funktioniert eine Anfrage nach Adresse</b>	7
<b>Abb. 5 Beispiel DNS: Anfrage nach Adresse «webmail.unizh.ch»</b>	7
Abb. 6 rekursive Anfragen	7
<b>Abb. 7 Reverse-Lookup</b>	8
<b>Abb. 8 Namensraum für inverse Abfragen</b>	8
Abb. 9 Die Protokolle TCP und UDP	9
Abb. 10 Typen von DNS-Servern	9
<b>Abb. 11 Dateien des DNS</b>	10
Abb. 12 Zonendatei der Domain netplanet.org	11
Abb. 13 Einträge in Zonendatenbankdatei	11
Abb. 14 Dynamisches DNS unter Windows	12
Abb. 15 Auslesen Zonendatei auf Server	14
Abb. 16 Kontrolle Zonendatei auf dem Client	14