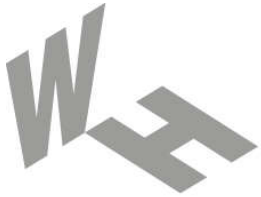


Westfälische Hochschule
Gelsenkirchen Bocholt Recklinghausen
University of Applied Sciences

Domain Name System (DNS)

Prof. Dr. (TU NN)
Norbert Pohlmann

Institut für Internet-Sicherheit – if(is)
Westfälische Hochschule, Gelsenkirchen
http://www.internet-sicherheit.de

Inhalt

- Ziele, Einordnung und Einleitung
- Hierarchische Namen/Namensvergabe im Internet
- Abbildung der Domain-Namen auf Adressen
- Aufbau von DNS
- Kommunikation mit den Name-Servern
- Aliasnamen
- Caching
- Zusammenfassung

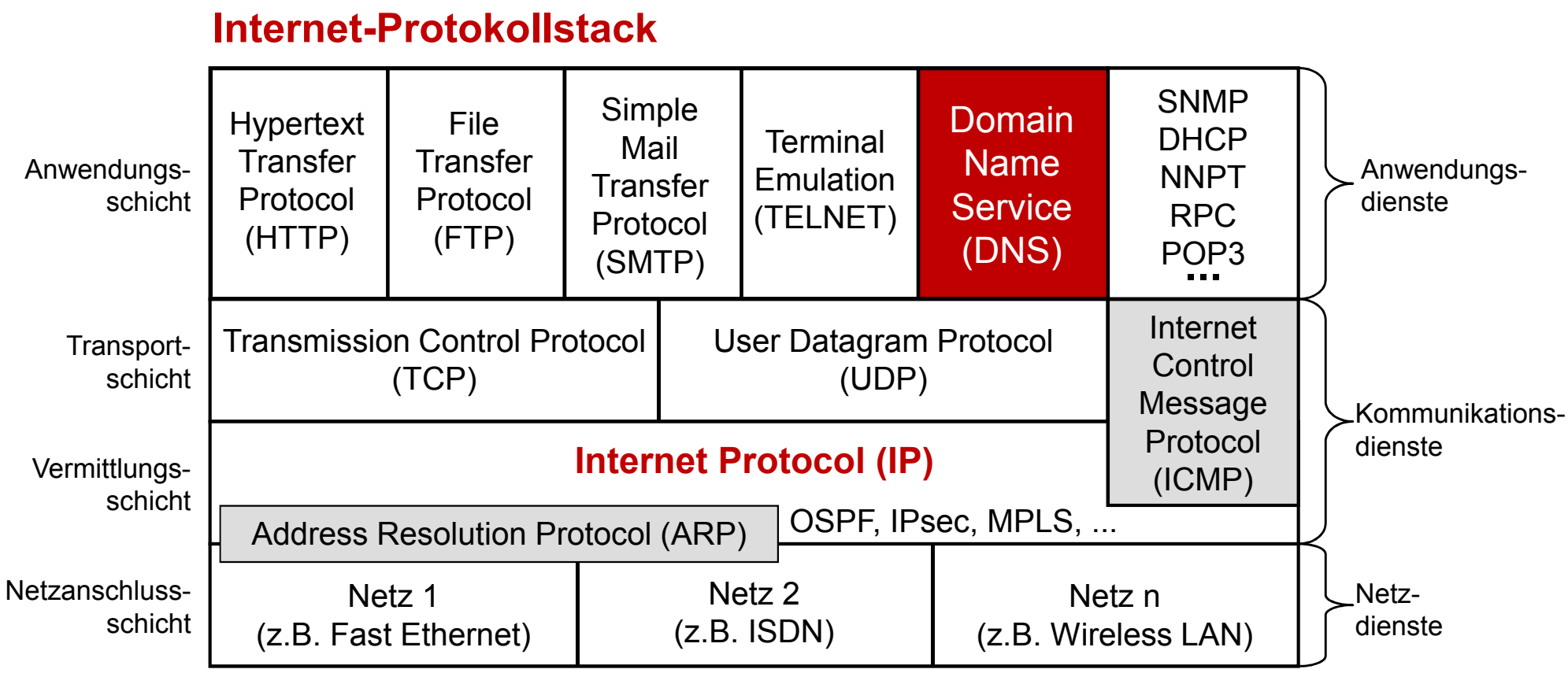
Inhalt

- **Ziele, Einordnung und Einleitung**
- Hierarchische Namen/Namensvergabe im Internet
- Abbildung der Domain-Namen auf Adressen
- Aufbau von DNS
- Kommunikation mit den Name-Servern
- Aliasnamen
- Caching
- Zusammenfassung

DNS - Domain Name System
→ Ziele

- Gutes Verständnis für das Domain Name System Konzept
- Erlangen der Kenntnisse über die Aufgaben, Prinzipien und Mechanismen des Domain Name Systems
- Gewinnen von praktischen Erfahrungen über DNS mit Hilfe von Protokollanalysen und Statistiken (IAS)

Die Anwendungsebene
→ Domain Name System (DNS) - Einordnung



DNS - Domain Name System
→ Standards

RFC 1034 - concept and facilities

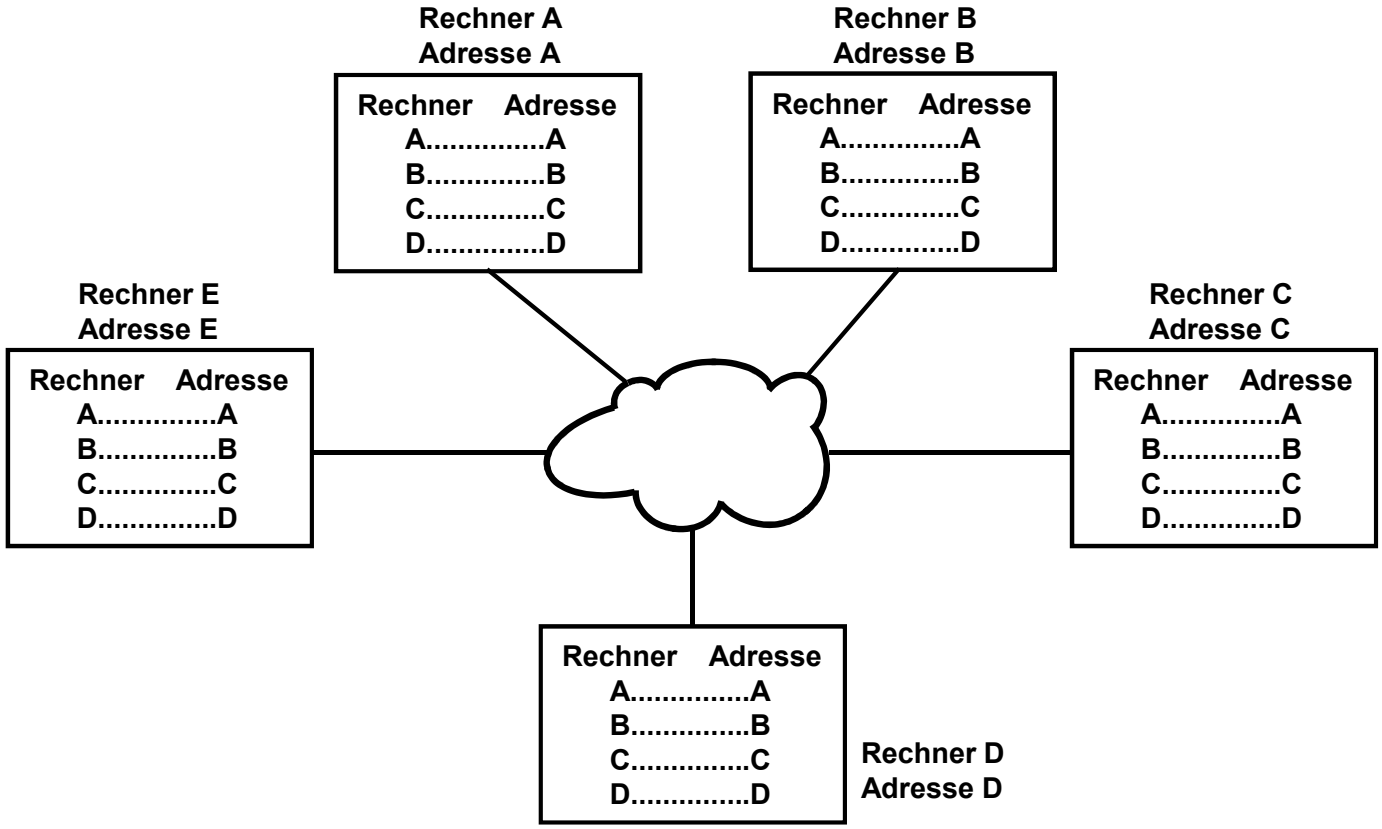
RFC 1035 - implementation and specification

RFC 2782 - A DNS RR for specifying the location of services (DNS SRV)

Domain Name System (DNS)
→ Einleitung (1/3)

- In den bisher besprochenen Protokollen wurde zur **Adressierung** eines Rechners eine **32-Bit Internet-Adresse** verwendet.
- Diese Adressen sind zwar eindeutig vergeben, es ist aber für Menschen **schwierig, sich diese zu merken.**
- Viel **einprägsamer ist ein Name**, den man an einen Rechner vergibt.
- Die Entstehungsgeschichte der Rechnerkommunikation ging von einfachen Punkt-zu-Punkt Verbindungen, bei denen Hardwareadressen verwendet wurden, zu kleinen lokalen Netzen, bei denen Rechner nach ihrem Einsatzgebiet, z.B. Entwickung, Accounting, ... benannt wurden.
- Hierzu musste auf jedem Rechner, der an der Kommunikation teilnehmen wollte, eine Zuordungstabelle gepflegt werden, in der ein Rechnername einer Rechneradresse zugeordnet wurde.
- Je mehr Maschinen an dieser Kommunikation teilnahmen, umso größer war der Aufwand diese Tabellen zu pflegen.
- Ein weiteres Problem ist die Auswahl des Namens und der begrenzte Namensraum (Doppelte Vergabe von Namen!).

Domain Name System (DNS)
→ Einleitung: Maschinennamen (2/3)



Domain Name System (DNS)
→ Einleitung (3/3)

- Um diese Probleme zu lösen, wurde das Domain Name System (DNS) konzipiert.
- Das **Konzept von DNS** ist einerseits
  - ein **hierarchisches domänenorientiertes** Namenssystem und anderseits
  - ein **verteiltes Dateisystem (Ressourcen Records)** zur Realisierung dieses Namenssystems.

Aufgabe von DNS

- DNS wird hauptsächlich benutzt, um **Rechnernamen und E-Mail-Adressen auf IP-Adressen abzubilden**, es kann aber auch zu anderen Zwecken dienen.

Inhalt

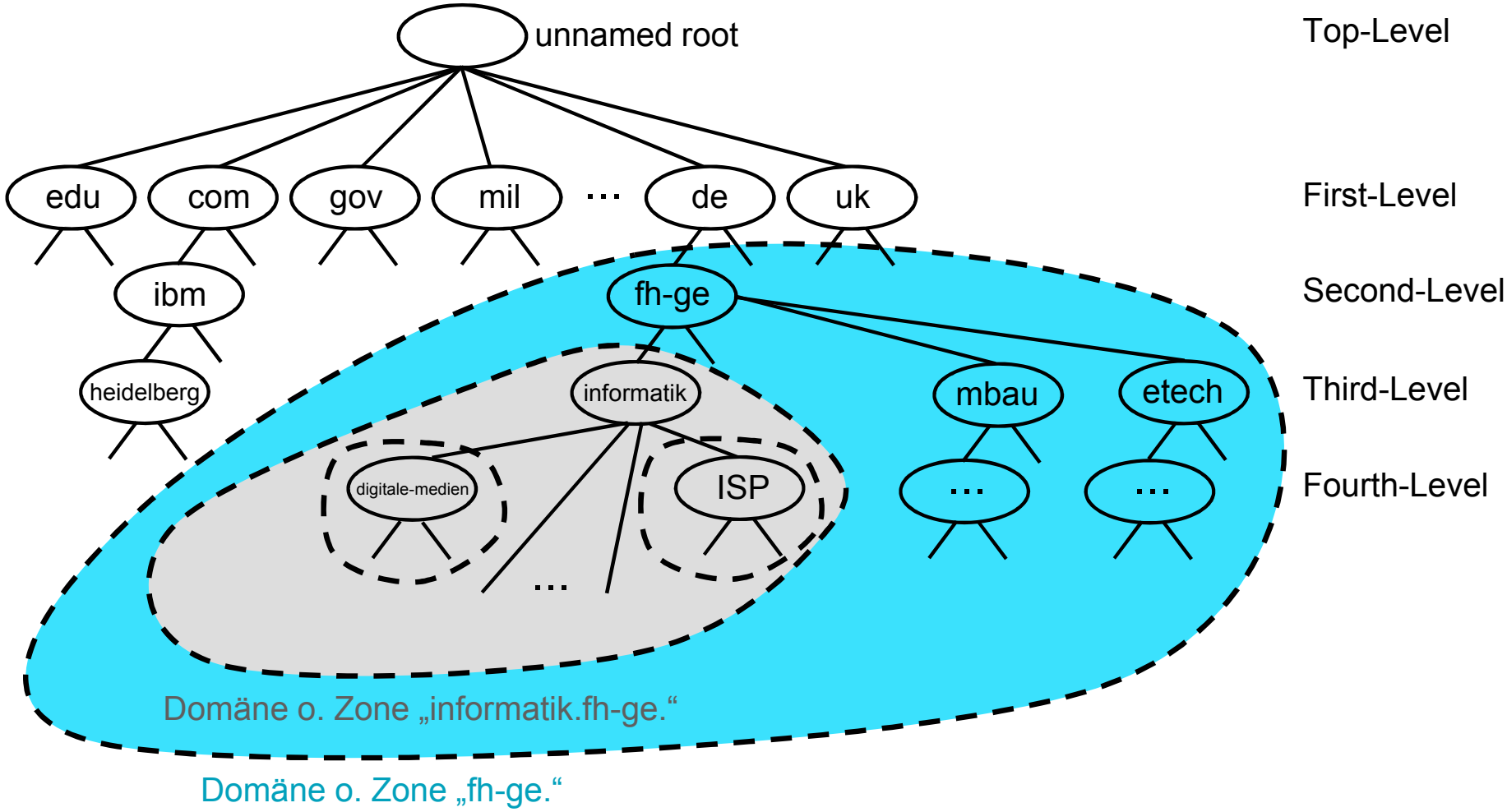
- Ziele, Einordnung und Einleitung
- **Hierarchische Namen**
  Namensvergabe im Internet
- Abbildung der Domain-Namen auf Adressen
- Aufbau von DNS
- Kommunikation mit den Name-Servern
- Aliasnamen; Caching
- Zusammenfassung

Domain Name System (DNS)
→ Hierarchische Namen

- Die Hierarchie der Namen im Internet ist gegliedert in Domains (Gebiete oder Zonen).
- Ein Name setzt sich aus einer Sequenz von Teilnamen, getrennt durch Punkte, zusammen.
- Beispiel: **informatik.fh-gelsenkirchen.de**
- 3 Teile: **informatik**, **fh-gelsenkirchen** und **de**.
- Jeder Teil entspricht einer Domäne.
  - Die niedrigste Domäne ist: **informatik.fh-gelsenkirchen.de**
    → Third-Level-Domain
  - Die nächst höhere **fh-gelsenkirchen.de** (der Domänenname der FH-GE)
    → Second-Level-Domain
  - Die höchste **de** (der Domänenname für Deutschland)
    → Top-Level-Domain / First-Level-Domain
- Der Rechnername selbst wird dann, getrennt durch einen Punkt, vor den Namen der Domäne, in der er sich befindet, geschrieben.
- So ist z.B. der Rechner **skripte**.informatik.fh-gelsenkirchen.de ein Rechner in der Domäne informatik.fh-gelsenkirchen.

Domain Name System (DNS)

→ Aufteilung des Namensbaums in Domänen, Zonen



Domain Name System (DNS)
→ Namensvergabe im Internet (1/9)

- Die Top-Level Domains (TLD) sind vom **Internet assigned Numbers Authority (IANA), unterorganisation der Internet Corporation for Assigned Names and Numbers (ICANN),** fest vorgegeben und in unterschiedliche Nutzerprofile oder lokale Gruppen eingeteilt.
- Top-Level Domains werden in vier Gruppen aufgeteilt:
  - Generic TLDs (gTLDs), unterteilt in sponsored und unsponsored
  - Länderspezifische TLDs, country-code TLDs (ccTLDs)
  - Infrastruktur-TLDs (iTLD)

Domain Name System (DNS)
→ Namensvergabe im Internet (2/9)

generic Top Level Domains (gTLD)

- **Sponsored**, werden von Unternehmen oder Organisationen vorgeschlagen. Diese formulieren eigene Regeln für die Nutzung
- Beispiele:

TLD	Bedeutung	Anspruchsberechtigung	Sponsor
.aero	Aeronautics	Luftfahrt	Société Internationale de Télécommunications Aéronautiques
.asia	Asia	Für Personen/Unternehmen aus Asien/Australien/Pazifik	
.coop	Cooperatives	Für Gesellschaften	Dot Cooperation LLC
.edu	Educational	Für Bildungseinrichtungen	
.gov	Government	Regierungsorgane der USA	
.int	international	Multinationale Organisationen	IANA

Domain Name System (DNS)
→ Namensvergabe im Internet (3/9)

generic Top Level Domains (gTLD)

- Beispiele (**sponsored**):

TLD	Bedeutung	Anspruchsberechtigung	Sponsor
.jobs	jobs	Unternehmen mit Stellenangeboten	
.mil	military	Militärische Einrichtungen der USA	
.mobi	Cooperatives	Dienste die auf Mobilen Endgeräten funktionieren	mTLD
.museum	museums	Für Museen	Museum Domain Management Association
.tel	telephone	Zum vereinfachten Anrufen von Unternehmen und Personen	
.travel	travel	Für die Reise-Industrie	
.xxx	Sex	Für erotische und sexuelle Inhalte	ICM Registry. Inc

Domain Name System (DNS)
→ Namensvergabe im Internet (4/9)

generic Top Level Domains (gTLD)

- Beispiele **(Unsponsored)**:

TLD	Bedeutung	Anspruchsberechtigung
.arpa	Arpanet	TLD des Arpanets (früher) heute verwendet als Address and Routing Parameter Area. „Infrastruktur-Domain“
.biz	Business	Nur für kommerzielle Verwendung
.com	Commercial	Ursprünglich für Unternehmen, heute für jeden
.info	Information	Für Informationsanbieter gedachte
.name	Name	Nur für natürliche Personen oder Familien
.net	Network	Für Netzverwaltungseinrichtungen, heute für jeden
.org	Organization	Für nichtkommerzielle Organisationen (Non-Profit-Organisationen)
.pro	Professionals	Für Anwälte, Steuerberater, Ärzte, Ingenieure

Domain Name System (DNS)
→ Namensvergabe im Internet (5/9)

Länderspezifische TLDs, country-code TLDs (ccTLDs)

- Beispiele

TLD	Registrar	Domains
.com	VeriSign	91.294.560
.de	DENIC	14.001.252
.net	VeriSign	13.557.708
.uk	Nominet	8.879.192
.org	PIR	8.972.090
.info	Afilias	7.293.717
.cn	CNNIC	6.047.926
.nl	SIDN	4.109.192

Domain Name System (DNS)
→ Namensvergabe im Internet (6/9)

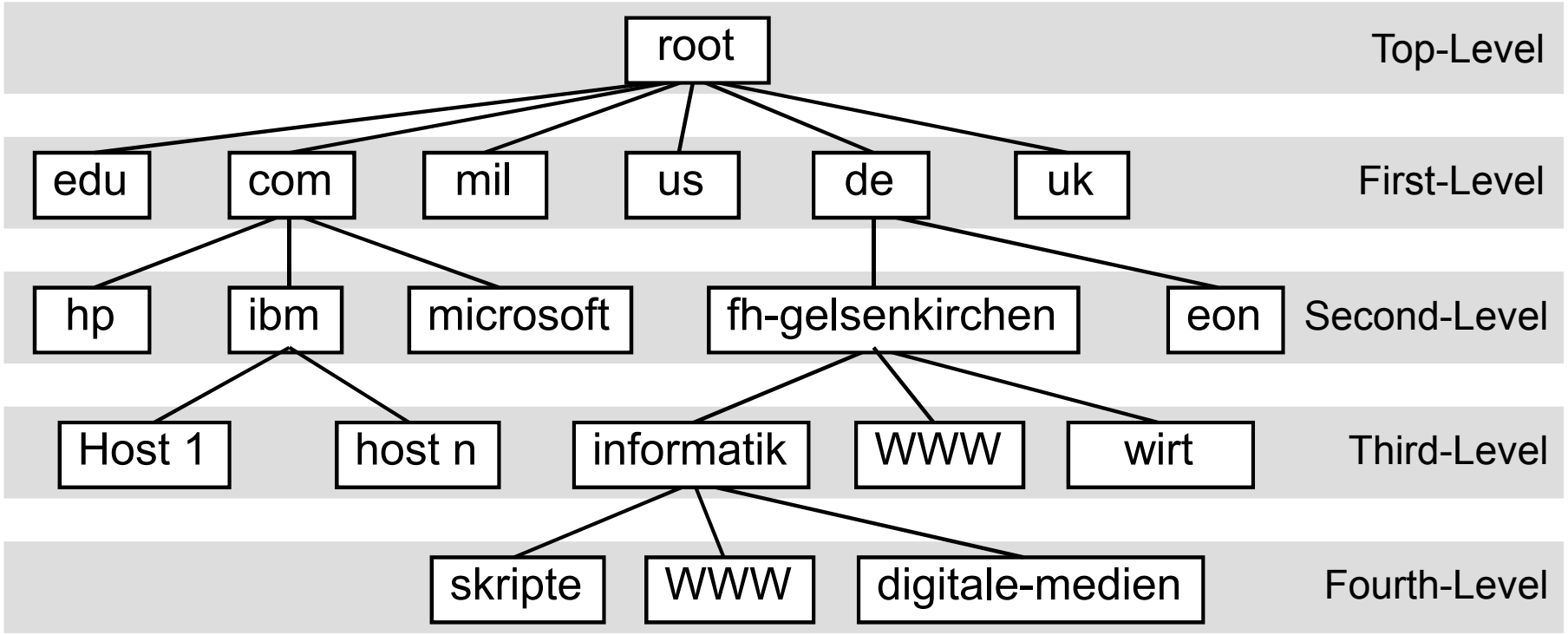
- Die Verwaltung der Domänen wird von verschiedenen Organisationen vorgenommen.
- Die Top-Level-Domäne **de** wird z.B. durch die DENIC (Domain Verwaltungs- und Betriebsgesellschaft -Internet Service Provider getragene Genossenschaft) verwaltet, die Domänen com, org oder net verwaltet die INTERNIC.
- In jedem Land gibt es eine Organisation, die unter Berücksichtigung der nationalen Gesetzgebung die Vergabe der Länder-Domäne organisiert.
- Es steht dabei jedem frei, sich bei einer solchen Organisation einen Namen eintragen zu lassen.
- Die Vergabe wird nach dem „first come, first serve“-Prinzip durchgeführt!
- Kostenbeitrag
  - 0,80 € / Monat für DE bei deutschem Anbieter.
  - 10$/Jahr in den USA für biz, com, co.uk, info, me.uk, net, org,us, etc

Domain Name System (DNS)
→ Namensvergabe im Internet (7/9)

- Es ist auch durchaus üblich, dass sich z.B. eine Firma mehrere Domains reserviert.
- Die Richtlinien der DENIC schreibt vor, dass jede Second Level Domain mindestens über 2 Name-Server (primary and secondary) verfügt und diese nach Möglichkeit noch an unabhängigen Standorten stehen.

Domain Name System (DNS)
→ Namensvergabe im Internet (8/9)

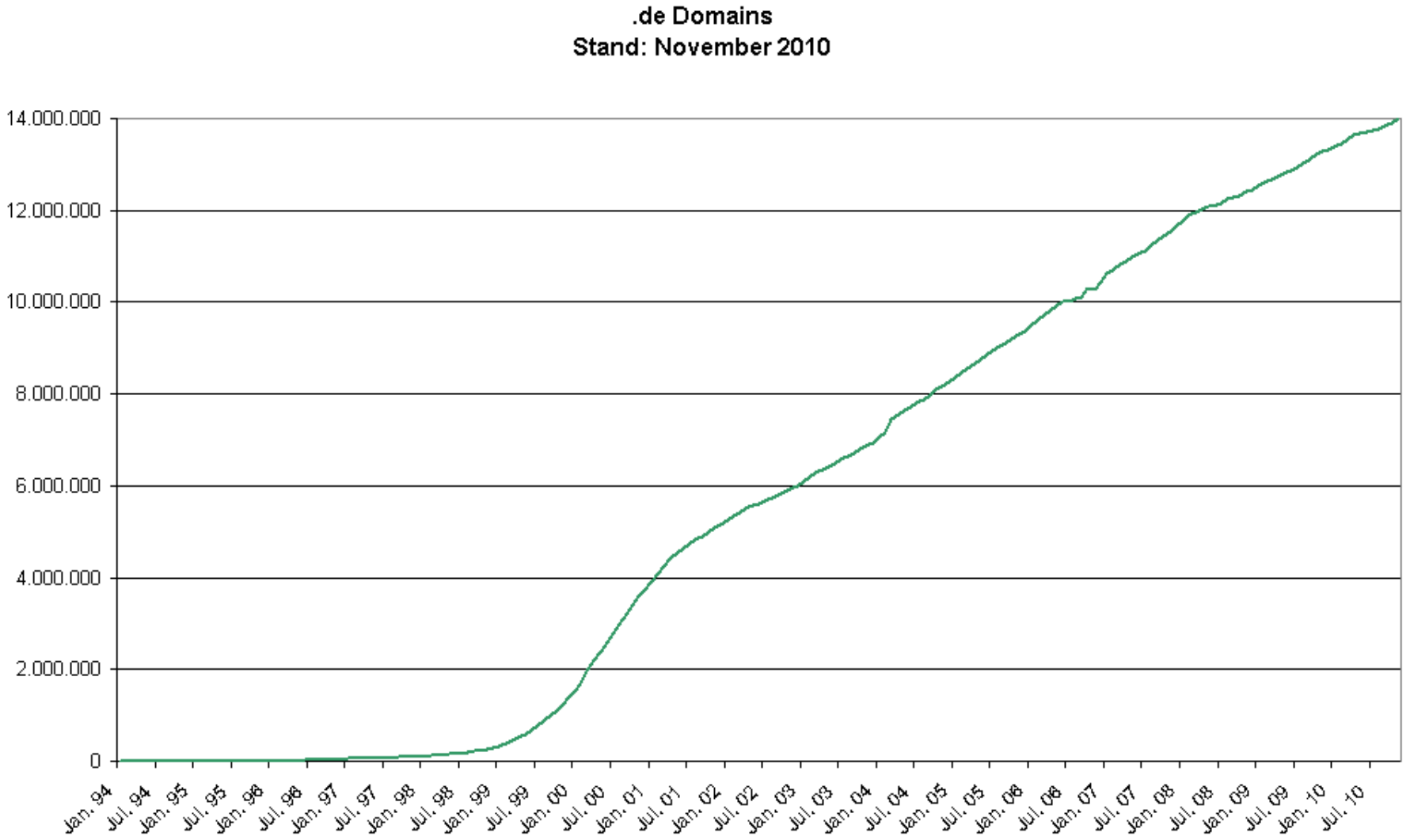
- Die **Vergabe von Subdomains** kann von dem jeweiligen **Eigner der Domäne** selber vorgenommen werden.
- So hat z.B. die FH-Gelsenkirchen u.a. die Subdomains
  informatik.fh-gelsenkirchen.de
  wirt.fh-gelsenkirchen.de
  pt.fh-gelsenkirchen.de



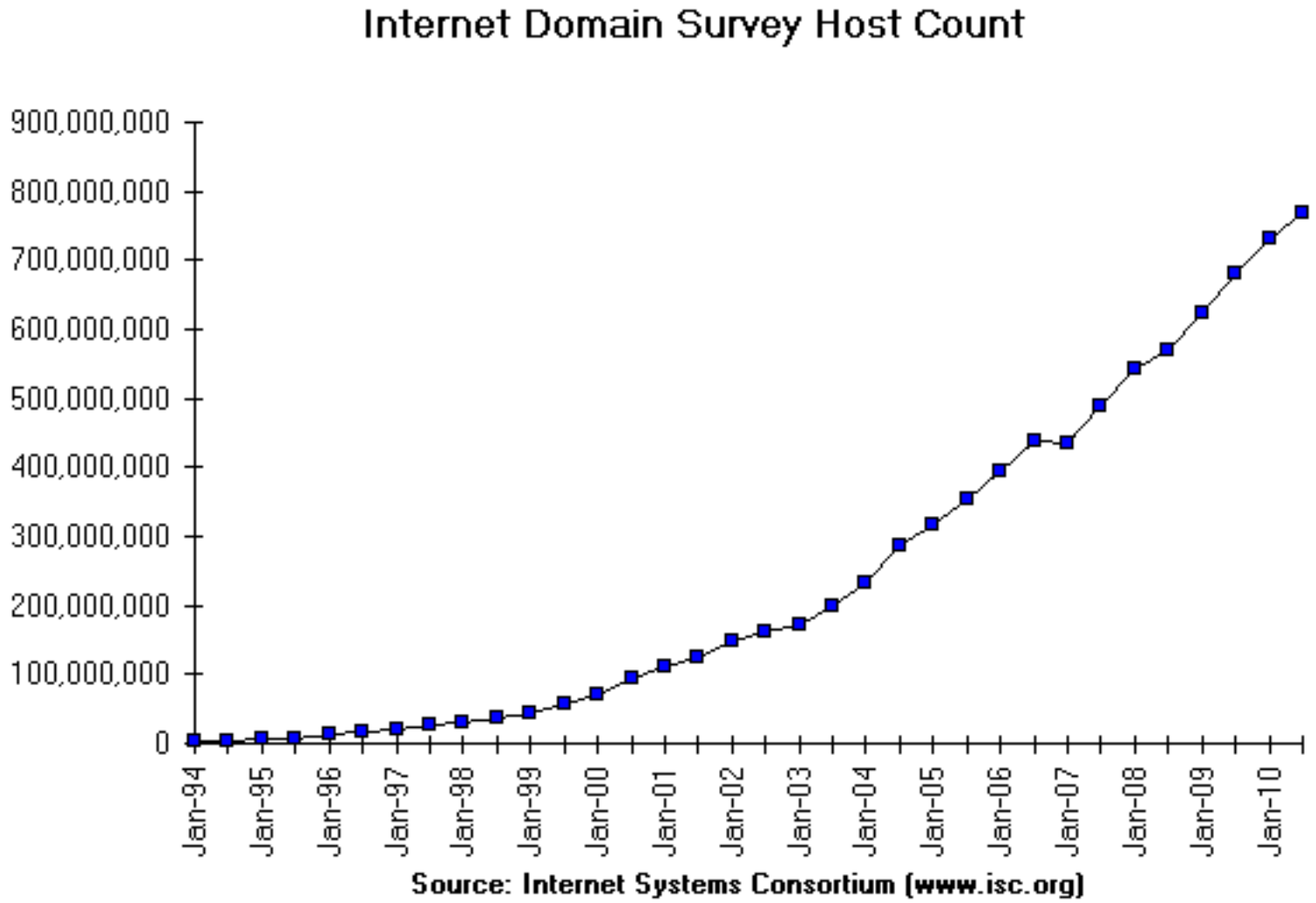
Domain Name System (DNS)
→ Namensvergabe im Internet (9/9)

- Die Syntax für die Namensgebung von Domänen sieht vor, dass jeder Knoten einen Namen mit einer Länge von bis zu 64 Zeichen haben darf.
- Die Gesamtlänge des Domänennamens darf **255 Zeichen** nicht überschreiten.
- Es darf eine Teilmenge des 7-Bit-ASCII-Zeichenvorrats enthalten.
- Dazu gehören die Großbuchstaben von **A bis Z**, die Kleinbuchstaben von **a bis z**, die Zahlen von **0 bis 9** sowie der Punkt (**.**) und der Bindestrich (**-**) sowie Umlaute.
- Punkt und Bindestrich dürfen nicht als erstes Zeichen des Namens verwendet werden.
- Zu beachten ist auch, dass bei der Adressermittlung **kein Unterschied zwischen Groß- und Kleinschreibung** gemacht wird.

Domain Name System (DNS)
→ Wachstum der DE-Domains



Domain Name System (DNS)
→ Wachstum der Hosts



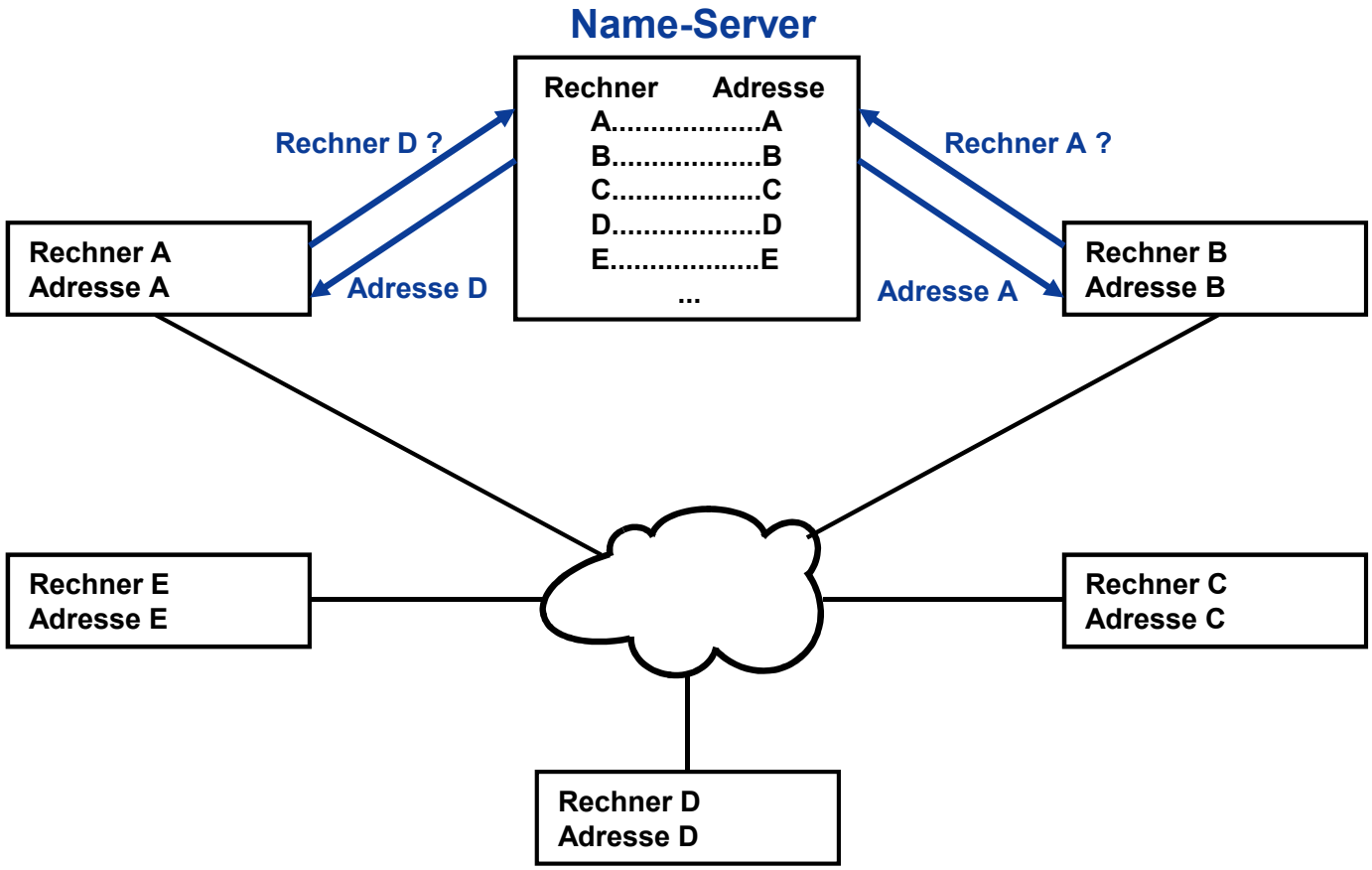
Inhalt

- Ziele, Einordnung und Einleitung
- Hierarchische Namen/Namensvergabe im Internet
- **Abbildung der Domain-Namen auf Adressen**
- Aufbau von DNS
- Kommunikation mit den Name-Servern
- Aliasnamen
- Caching
- Zusammenfassung

Domain Name System (DNS)
→ Abbildung der Domain-Namen auf Adressen (1/5)

- Um das Problem der lokalen Pflege von Listen zu umgehen, wurden sogenannte **Name-Server** eingeführt.
- Ein Name-Server ist ein Programm, welches eine Übersetzung eines Namens in eine IP-Adresse vornehmen kann.
- Ein Rechnername muss bei der Verwendung eines Name-Servers nur ein mal, und zwar im Name-Server, gepflegt werden.
- Rechner, die eine Adresse benötigen, fragen diese beim Name-Server ab.
- Ein Rechner muss also nicht mehr alle Rechneradressen kennen, sondern nur noch die des Name-Servers.
- Dabei verwaltet ein Name-Server die Rechnernamen einer Domäne oder Subdomäne (es ist auch möglich, dass ein Name-Server mehrere Domänen und Subdomänen verwaltet).

Domain Name System (DNS)
→ Abbildung der Domain-Namen auf Adressen (2/5)



Domain Name System (DNS)
→ Abbildung der Domain-Namen auf Adressen (3/5)

- Für eine weltweite Kommunikation muss ein **Netz von Name-Servern** aufgebaut sein.
- Dieses Netz besteht aus mehreren **Root-Servern** (2010 - 13 Stück), zum Großteil in den USA.
- An diesem Verbund von Root-Servern sind die Domän-Server der **First-Level-Domän** (de, com, edu, ...) in der nächsten Ebene aufgehängt.
- Eine Ebene tiefer folgen dann die Name-Server der Second-Level-Domäne wie z.B. fh-gelsenkirchen.
- An der Fachhochschule Gelsenkirchen gibt es die Domäne fh-gelsenkirchen.de und mehrere Subdomänen, z.B. **informatik**.fh-gelsenkirchen.de, **wirt.**fh-gelsenkirchen.de, **pt.**fh-gelsenkirchen.de**.**
- Diese werden alle gemeinsam von den Name-Servern „rz1.fh-gelsenkirchen.de“ und „deneb.dfn.de“ verwaltet.
- Die **informatik.**fh-gelsenkirchen.de Domäne wird verwaltet von dns-se.informatik.fh-gelsenkirchen und dns-pe.informatik.fh-gelsenkirchen.

Domain Name System (DNS)
→ Abbildung der Domain-Namen auf Adressen (4/5)

- **Root-Domain-Server (13)**
  - (root) nameserver = A.ROOT-SERVERS.NET
  - (root) nameserver = H.ROOT-SERVERS.NET
  - (root) nameserver = C.ROOT-SERVERS.NET
  - (root) nameserver = G.ROOT-SERVERS.NET
  - (root) nameserver = F.ROOT-SERVERS.NET
  - (root) nameserver = B.ROOT-SERVERS.NET
  - (root) nameserver = J.ROOT-SERVERS.NET
  - (root) nameserver = K.ROOT-SERVERS.NET
  - (root) nameserver = L.ROOT-SERVERS.NET
  - (root) nameserver = M.ROOT-SERVERS.NET
  - (root) nameserver = I.ROOT-SERVERS.NET
  - (root) nameserver = E.ROOT-SERVERS.NET
  - (root) nameserver = D.ROOT-SERVERS.NET
  - A.ROOT-SERVERS.NET internet address = 198.41.0.4
  - H.ROOT-SERVERS.NET internet address = 128.63.2.53
  - C.ROOT-SERVERS.NET internet address = 192.33.4.12
  - ...

Top-Level

Domain Name System (DNS)
→ Abbildung der Domain-Namen auf Adressen (5/5)

- **DE-Domain-Server (11)**
  - de nameserver = AUTH03.NS.DE.UU.NET
  - de nameserver = DNS.DENIC.de
  - de nameserver = SSS-AT.DENIC.de
  - de nameserver = SSS-NL.DENIC.de
  - de nameserver = SSS-DE1.DE.NET
  - de nameserver = SSS-UK.DE.NET
  - de nameserver = DNS2.DE.NET
  - de nameserver = SSS-JP.DENIC.de
  - de nameserver = SSS-US1.DE.NET
  - de nameserver = SSS-US2.DENIC.de
  - de nameserver = SSS-SE.DENIC.de
  - AUTH03.NS.DE.UU.NET internet address = 192.76.144.16
  - DNS.DENIC.de internet address = 81.91.161.5
  - SSS-AT.DENIC.de internet address = 193.171.255.34
  - SSS-NL.DENIC.de internet address = 193.0.0.237
  - SSS-DE1.DE.NET internet address = 193.159.170.187
  - ...

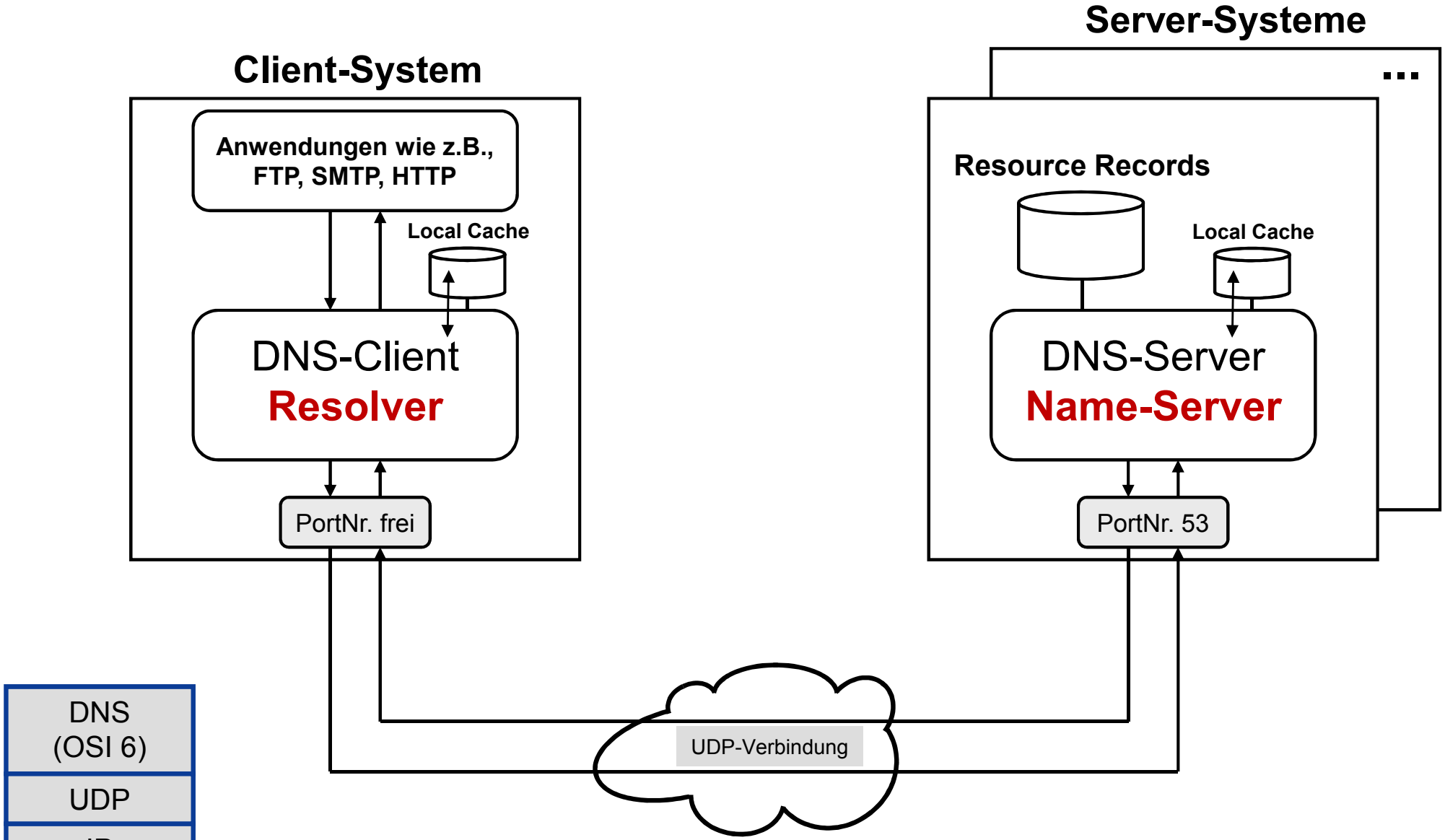
First-Level

Inhalt

- Ziele, Einordnung und Einleitung
- Hierarchische Namen/Namensvergabe im Internet
- Abbildung der Domain-Namen auf Adressen
- **Aufbau von DNS**
- Kommunikation mit den Name-Servern
- Aliasnamen
- Caching
- Zusammenfassung

Domain Name System (DNS)

→ Aufbau von DNS: Client-Server Beziehung (1/5)



Domain Name System (DNS)
→ Aufbau von DNS (2/5)

- Das Domain Name System arbeitet im Rahmen einer Art Client/Server-Beziehung mit einem **Resolver** (einem Programm, das Anfragen für einen Domain Name Server erzeugt) und einem Name-Server zusammen.
- Während der Name-Server typischerweise ein selbständiges Rechnersystem (Host) ist, ist der Resolver normalerweise Teil eines Betriebssystemkerns oder einer entsprechend systemnahen Routine.
- Der Name-Server enthält eine Datenbank mit Resource Records, in der die Beziehungen zwischen den Namen verschiedener Rechnersysteme und den jeweils zugeordneten IP-Adressen und einigen anderen Parametern aufgelistet sind.
- Der Name-Server stellt die Informationsquelle des DNSs dar.
- Für jede Domäne existiert ein sogenannter „Primary“ Name-Server, der die Verwaltung aller Namen und Adressen der in seiner Domäne befindlichen Rechner übernimmt.

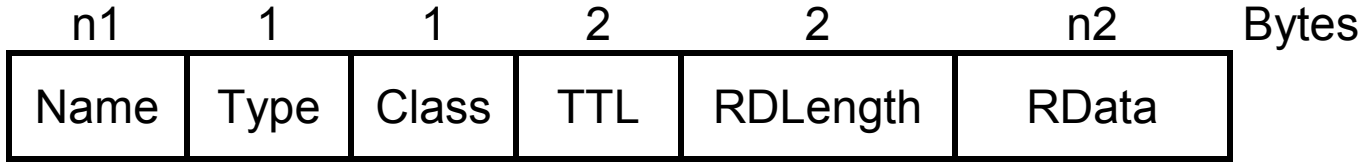
Domain Name System (DNS)
→ Aufbau von DNS (3/5)

- Weiter unten in der Hierarchie angesiedelte Domänen (Subdomains) werden entweder von diesen Name-Servern mitverwaltet oder die Verwaltung wird an einen eigenen Name-Server delegiert.
- Der sogenannte Domain Name Space ist die Grundlage des Name-Systems.
- Die hierarchische Baumstruktur wird auf der lokal betreuten Datenbank mit entsprechenden Datensätzen (den **Resource Records**) abgebildet.
- Die Datensätze enthalten eine Beschreibung des jeweiligen Rechnersystems.
- Anfragen können mit allen verfügbaren, aber auch nur mit ausgewählten Informationen beantwortet werden.
- Die Resource Records werden so zusammengefasst, dass bestimmte Domänen aus einer Datenbank für einen klar abgegrenzten Bereich in der Baumhierarchie Informationen bereithalten.

Domain Name System (DNS)

→ Aufbau von DNS: Aufbau eines Resource Record (4/5)

- **Resource Records**, die im Name-Server gespeichert sind, bestehen aus insgesamt sechs Feldern.



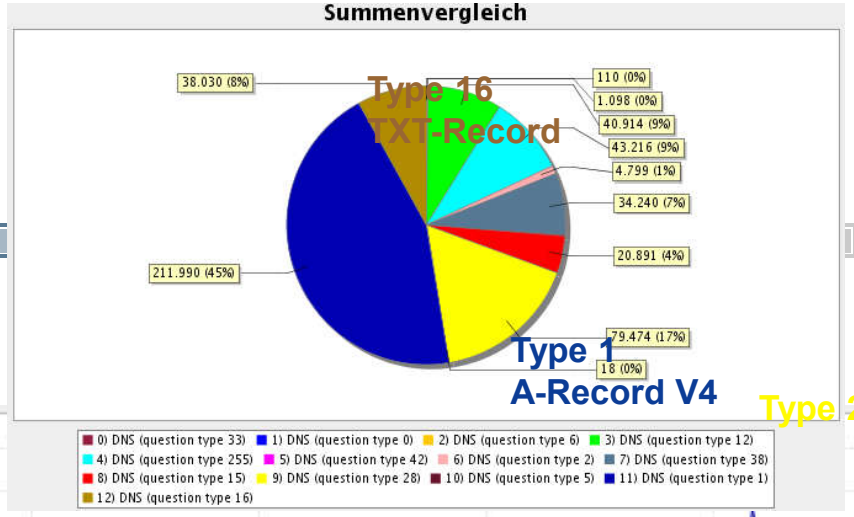
Bezeichnung	Inhalt	
Name	Das Feld enthält den Namen der Domäne, der diesem Resource Record zugeordnet ist.	
Type	Das Zwei-Byte-Feld gibt den Type des Resource Record an.	
	A	Type = 1 RData enthält die zu "Namen" gehörende IP-Adresse
	NS	Type = 2 (NS = Name Server) RData enthält den Domänennamen des für "Name" zuständigen Domänenservers.
	CNAME	Type = 5 (CNAME = Canonical Name, kanonischer Name) RData enthält den Namen zu "Namen" (Aliasname)
	SOA	Type = 6 (SOA = Start Of Area, Anfrag der Zone) RData gibt den Anfang einer Zone an.
	PTR	Type = 12 (PTR = Pointer, Zeiger) RData enthält einen Zeiger auf eine IP-Adresse für das Reverse Mapping
	HINFO	Type = 13 (HINFO = Host Information) RData enthält eine ID für die Hardware und das Betriebssystem von "Name"
	MX	Type = 15 (MX = Mail Exchange) RData enthält den Domänennamen eines für "Name" zuständigen E-Mail Servers.
	TXT	Type = 16 Rdata enthält einen in doppelten Anführungszeichen eingeschlossenen Text.

Domain Name System (DNS)

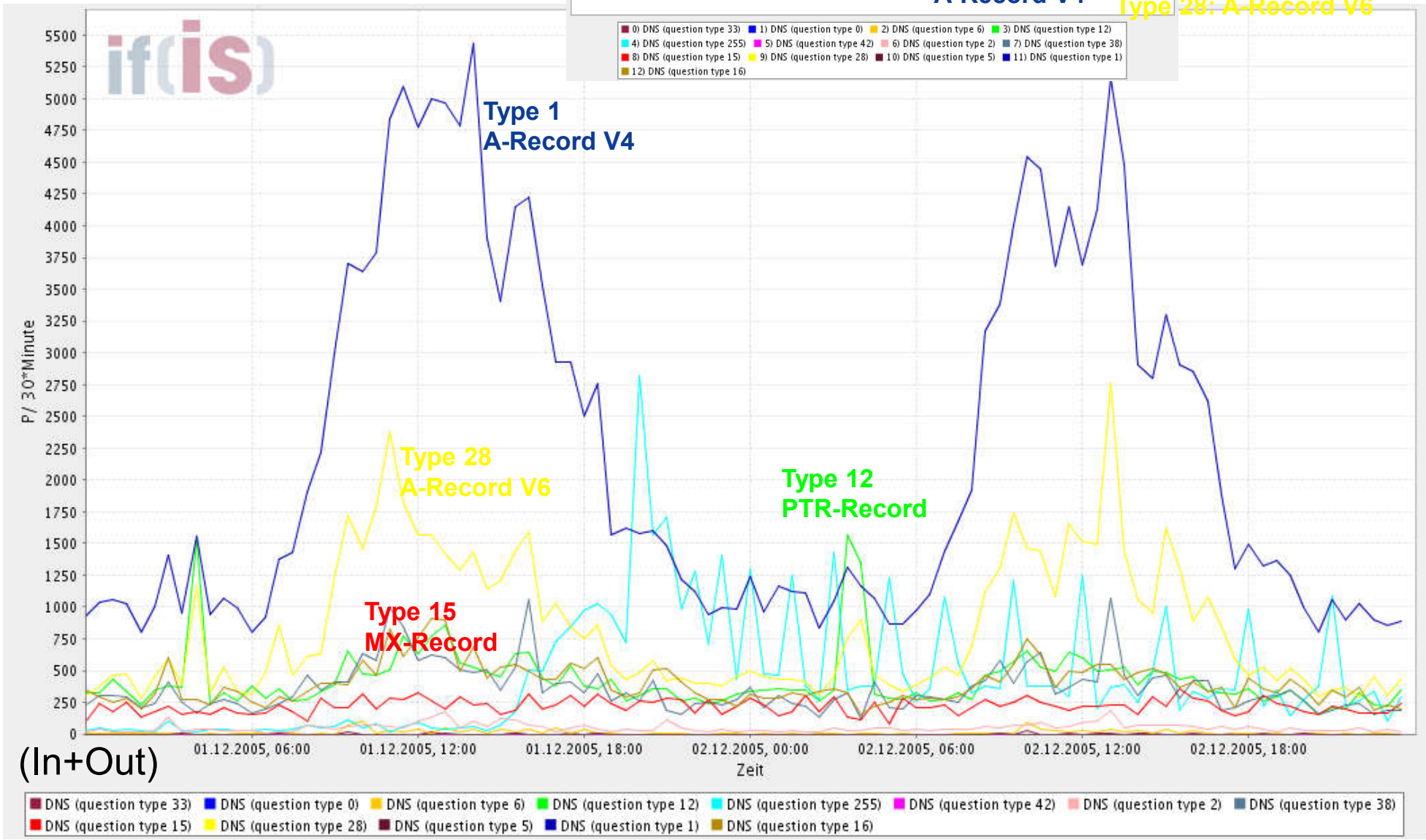
→ Aufbau von DNS: Aufbau eines Resource Record (5/5)

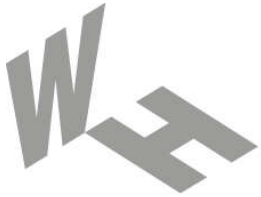
Bezeichnung	Inhalt	
Class	Mit diesem Zwei-Byte-Wert wird die Protokollfamilie beschrieben.	
	IN	Internet, Class = 1
	CS	CSNET, Class = 2
	CH	CHAOSnet, Class = 3
	HS	Hesiod, Class = 4
TTL	Mit diesem Vier-Byte-Wert wird die Anzahl Sekunden festgelegt, die ein Resolver den Resource Record in seinem Cache hält, bevor er ihn löscht und/oder eine Aktualisierung durchführt. TTL ist die Abkürzung für Time To Live.	
RDLength	Dieser Zwei-Byte-Wert gibt die Länge des Felds RData in Byte an	
Rdata	Längenvariantes Feld, das abhängig von den Eintragungen in einigen der zuvor beschriebenen Felder unterschiedlich zu interpretierende Daten enthält.	

IAS: FB Informatik
→ Type



Type 28: A-Record V6





Westfälische Hochschule
Gelsenkirchen Bocholt Recklinghausen
University of Applied Sciences

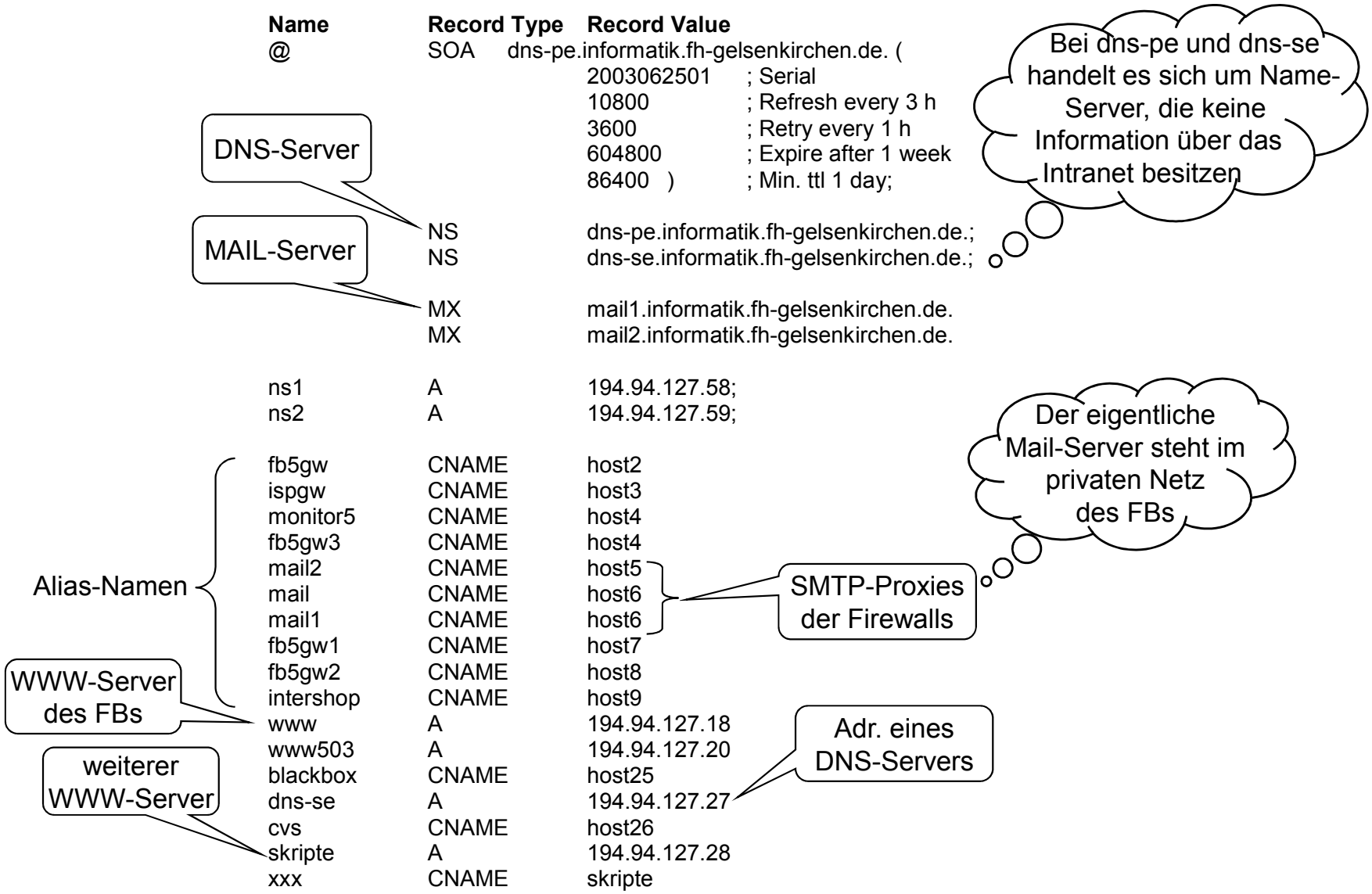
Beispielauszug aus DNS-Datenbank von „dns-pe.informatik.fh-gelsenkirchen.de“

Prof. Dr. (TU NN)
Norbert Pohlmann

Institut für Internet-Sicherheit – if(is)
Westfälische Hochschule, Gelsenkirchen
http://www.internet-sicherheit.de

Domain Name System (DNS)
→ Auszug einer DNS-Datenbank (1/2)

- Auszug: DNS-DB Domäne **dns-pe.informatik.fh-gelsenkirchen.de (1/2)**



Domain Name System (DNS)
→ Auszug einer DNS-Datenbank (2/2)

- Auszug: DNS-DB **dns-pe.informatik.fh-gelsenkirchen.de** **(2/2)**

Name	Record Type	Record Value
sun2	A	194.94.127.82
dns-pe	A	194.94.127.83
trikon-tv	A	194.94.127.88
trikontv	CNAME	trikon-tv
fachschaft	CNAME	host98
host1	A	194.94.127.1
host2	A	194.94.127.2
host3	A	194.94.127.3
host4	A	194.94.127.4
host5	A	194.94.127.5
host6	A	194.94.127.6
host7	A	194.94.127.7
host8	A	194.94.127.8
host9	A	194.94.127.9
host10	A	194.94.127.10
host11	A	194.94.127.11
host12	A	194.94.127.12
host13	A	194.94.127.13
host14	A	194.94.127.14
host15	A	194.94.127.15
host16	A	194.94.127.16
host17	A	194.94.127.17
host18	A	194.94.127.18
host19	A	194.94.127.19
host20	A	194.94.127.20
host21	A	194.94.127.21
host22	A	194.94.127.22
host23	A	194.94.127.23
host24	A	194.94.127.24
host25	A	194.94.127.25
host26	A	194.94.127.26
host27	A	194.94.127.27
host28	A	194.94.127.28
host29	A	194.94.127.29
host30	A	194.94.127.30
host31	A	194.94.127.31
host32	A	194.94.127.32
host33	A	194.94.127.33
host34	A	194.94.127.34
host35	A	194.94.127.35
host36	A	194.94.127.36
host37	A	194.94.127.37
host38	A	194.94.127.38
host39	A	194.94.127.39
host40	A	194.94.127.40
host41	A	194.94.127.41
host42	A	194.94.127.42
host43	A	194.94.127.43
host44	A	194.94.127.44
host45	A	194.94.127.45
host46	A	194.94.127.46
host47	A	194.94.127.47
host48	A	194.94.127.48
host49	A	194.94.127.49
host50	A	194.94.127.50
host51	A	194.94.127.51
host52	A	194.94.127.52
host53	A	194.94.127.53
host54	A	194.94.127.54
host55	A	194.94.127.55
host56	A	194.94.127.56
host57	A	194.94.127.57
host58	A	194.94.127.58
host59	A	194.94.127.59
host60	A	194.94.127.60
host61	A	194.94.127.61
host62	A	194.94.127.62
host63	A	194.94.127.63
host64	A	194.94.127.64
host65	A	194.94.127.65
host66	A	194.94.127.66
host67	A	194.94.127.67
host68	A	194.94.127.68
host69	A	194.94.127.69
host98	A	194.94.127.98
host114	A	194.94.127.114
host115	A	194.94.127.115
host116	A	194.94.127.116
db-dek	CNAME	host116
host117	A	194.94.127.117
epa	CNAME	host117

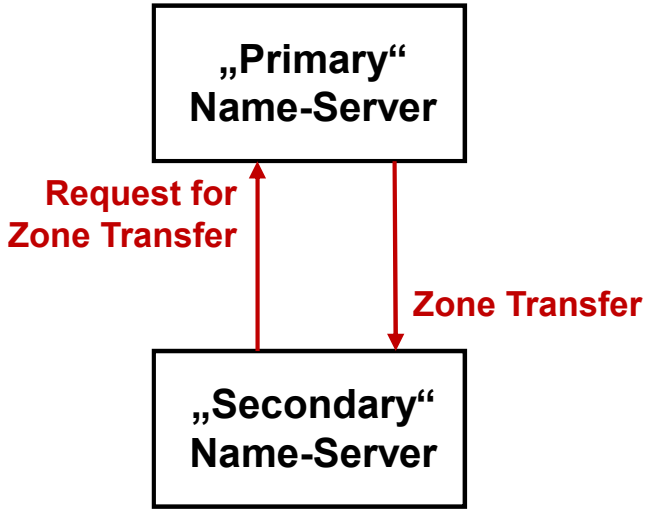
Adr. des 2. DNS-Servers

Rechner der Fachschaft

Adr. des Rs. der Fachschaft

Domain Name System (DNS)
→ Zonen-Management

- Die Verfügbarkeit des DNS Service spielt eine sehr große Rolle bei den wichtigsten TCP/IP-Anwendungen.
- Aus diesem Grund werden die Name-Server redundant aufgebaut.
- Es gibt zwei Typen von Name-Servern:
  - **Primary Name-Server**
    bezieht seine Information aus dem Master File (DNS-DB), der vom Systemadministrator erstellt wird.
  - **Secondary Name Server**
    kopiert in regelmäßigen Abständen die Zonen-Informationen vom Primary Name Server: Zonentransfer
- **Zonentransfer**



Inhalt

- Ziele, Einordnung und Einleitung
- Hierarchische Namen/Namensvergabe im Internet
- Abbildung der Domain-Namen auf Adressen
- Aufbau von DNS
- **Kommunikation mit den Name-Servern**
- Aliasnamen
- Caching
- Zusammenfassung

Domain Name System (DNS)
→ Kommunikation (1/8)

- Wenn ein Name-Server eine Abfrage von einem Rechner seiner Domäne erhält, prüft er zuerst, ob der zu übersetzende Name in seiner Domäne liegt.
- Wichtig ist hier, dass ein Rechner, der einen Namen in eine Adresse übersetzen lassen will, immer den Name-Server abfragt, dessen Adresse (nicht sein Name) in der TCP/IP-Software hinterlegt ist; in der Regel ist dies der lokale Name-Server der Domäne.
- Kann der Name-Server den Namen auflösen, schickt er die passende IP-Adresse an den fragenden Rechner zurück.
- Ist dies nicht der Fall, so muss zwischen einer rekursiven und einer nicht-rekursiven Abfrage des Clients unterschieden werden.
- Mit einer **rekursiven Abfrage** verlangt ein Client von einem **Name-Server eine vollständige Auflösung des Namens**.
- Der Name-Server hat also die Aufgabe solange nach einem Name-Server zu suchen, bis die Anfrage vollständig beantwortet ist.

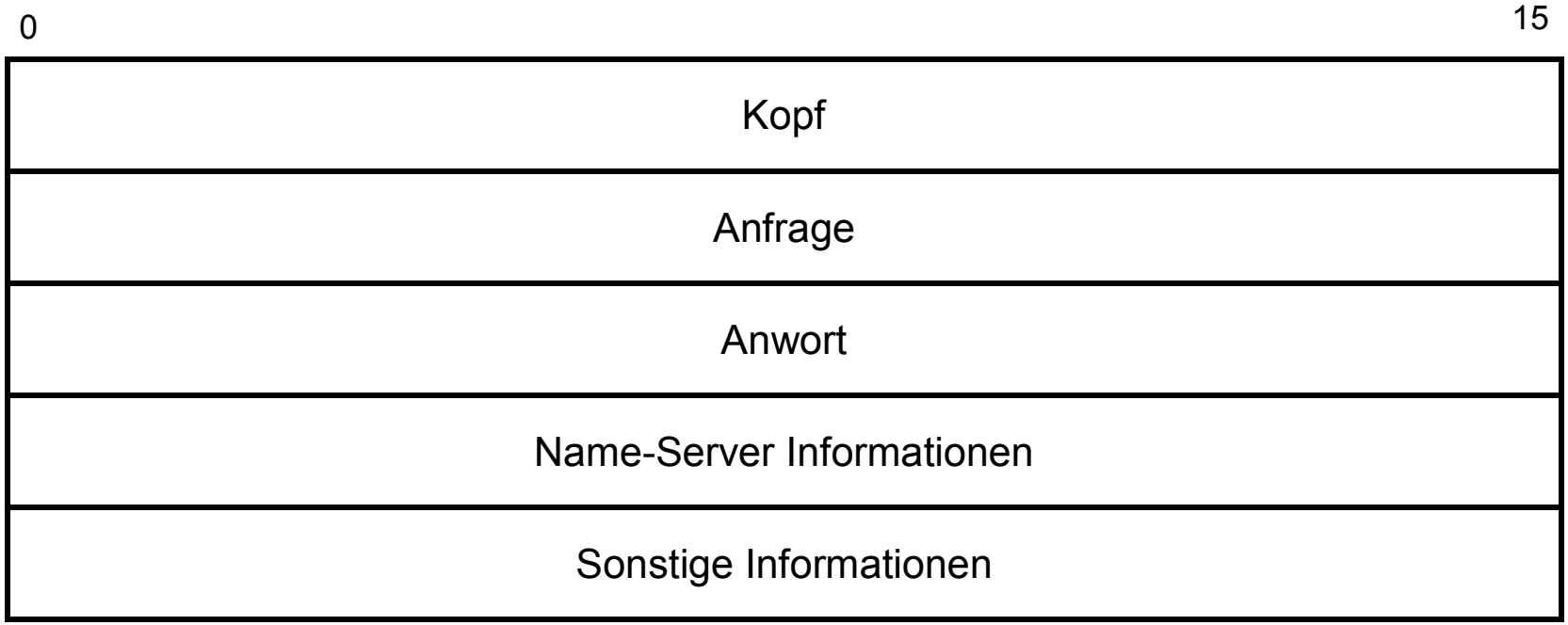
Domain Name System (DNS)
→ Kommunikation (2/8)

- Eine **nicht rekursive, interaktive Abfrage** bedeutet, dass der Client für die Abfrage weiterer Name-Server selbst zuständig ist, wenn der Name-Server die Abfrage des Clients nicht beantworten kann.
- In der Regel werden aber **rekursive Abfragen** durch den Client ausgeführt.
- Der Algorithmus für die Abfrage eines Namens, den ein Name-Server nicht selbst auflösen kann, ist, dass sich der Name-Server sofort an einen der Root-Server wendet und dieser die Adresse des nächsten Name-Servers zurückgibt, der bei dieser Abfrage weiterhelfen kann.
- Dies geschieht so lange, bis der Name-Server gefunden ist, in dessen Domäne der Name enthalten ist, und dieser die passende IP-Adresse zurückgeben kann.
- Somit sind die einzigen Informationen, die ein Name-Server braucht, die IP-Adressen von einigen Root-Servern.
- Die Root-Server kennen nur die IP-Adressen der Domänen-Server, usw.

Domain Name System (DNS)
→ Kommunikation (3/8)

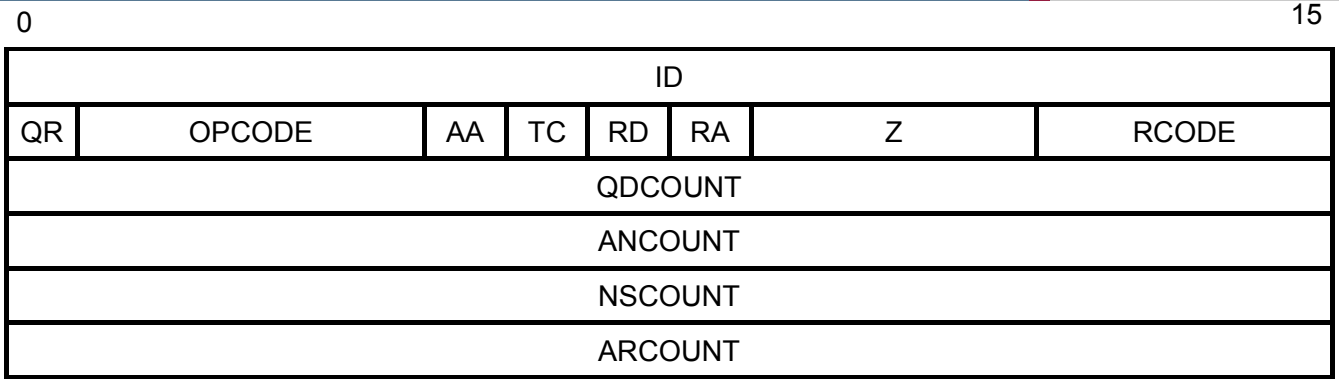
- Der Abfragemechanismus im Netzwerk beruht entweder auf einem verbindungslosen UDP- oder auf einem verbindungsorientierten TCP-Dienst.
- Als Antwort auf die Anforderungen kann ganz oder teilweise der gewünschte Resource Record oder eine Fehlermeldung zurückkommen.
- Soweit dies für die Aktualisierung der Informationen erforderlich ist, kommunizieren Name-Server miteinander auf der Basis von TCP (seltener eingesetzt, wegen der größeren Netzbelastung) oder UDP.
- Unabhängig vom gewählten Protokoll auf der Transportebene wird die Portnummer 53 verwendet.

Domain Name System (DNS)
→ Kommunikation: Das Format des DNS-PDU (4/8)



Domain Name System (DNS)
→ Kommunikation: Das Format des DNS-Kopfes (5/8)

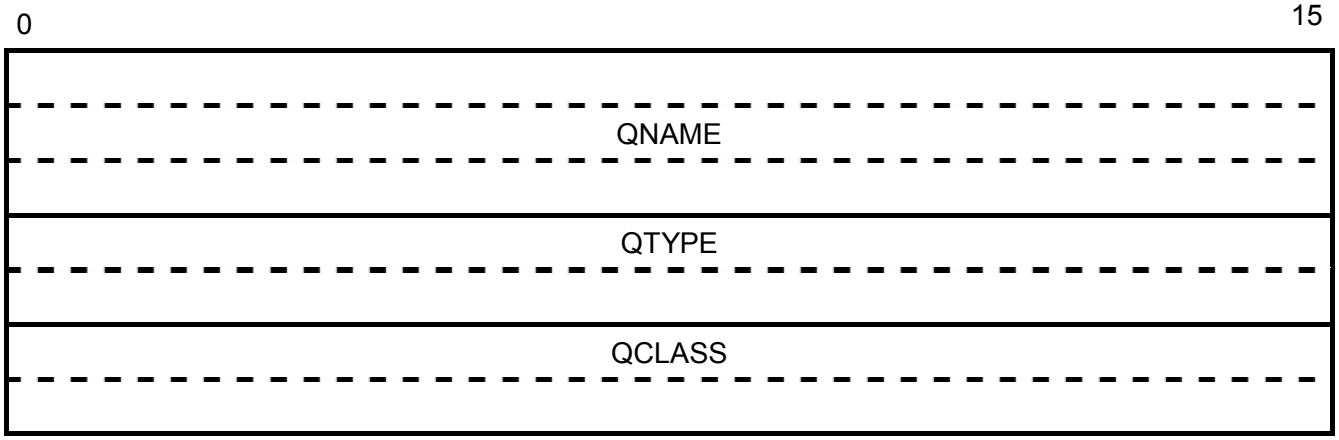
- Der Kopf ist immer vorhanden



Bezeichnung	Inhalt
ID	Wird vom anfragenden Programm erzeugt und vom Name Server in die Antwort kopiert, dient zum Identifizieren des Infoblocks. Zwei-Byte-Ganzahl
QR	Spezifiziert, ob der Infoblock eine Anfrage (nicht gesetzt) oder eine Antwort (gesetzt) ist. Länge: 1 Bit
OPCODE	Dient zur Spezifizierung des Anfragetyps. Länge: 4 Bit (Standard=0, Inverse=1, ...)
AA	Wird gesetzt, wenn der Name Server ein Primary Server für die Domäne ist. Länge: 1 Bit
TC	Gibt an, dass das Protokollelement nicht korrekt übertragen werden konnte. Länge 1 Bit
RD	Wird bei der Anfrage gesetzt, wenn der Name Server rekursiv arbeiten soll. Länge 1 Bit
RA	Wird gesetzt, wenn der Name Server rekursiv arbeiten kann. Länge 1 Bit
Z	Feld für zukünftige Verwendung.
RCODE	Mit 4 Bit wird eine Fehlerinformation dargestellt (Kein Fehler=0, Format Fehler=1, ...)
QDCOUNT	Gibt die Anzahl der Einträge im Infoblock Anfrage an.
ANCOUNT	Gibt die Anzahl der Resource Records im Infoblock Antwort an.
NSCOUNT	Gibt die Anzahl der Resource Records im Infoblock Name-Server-Information an.
ARCOUNT	Gibt die Anzahl der Resource Records im Infoblock Sonstiges an.

Domain Name System (DNS)

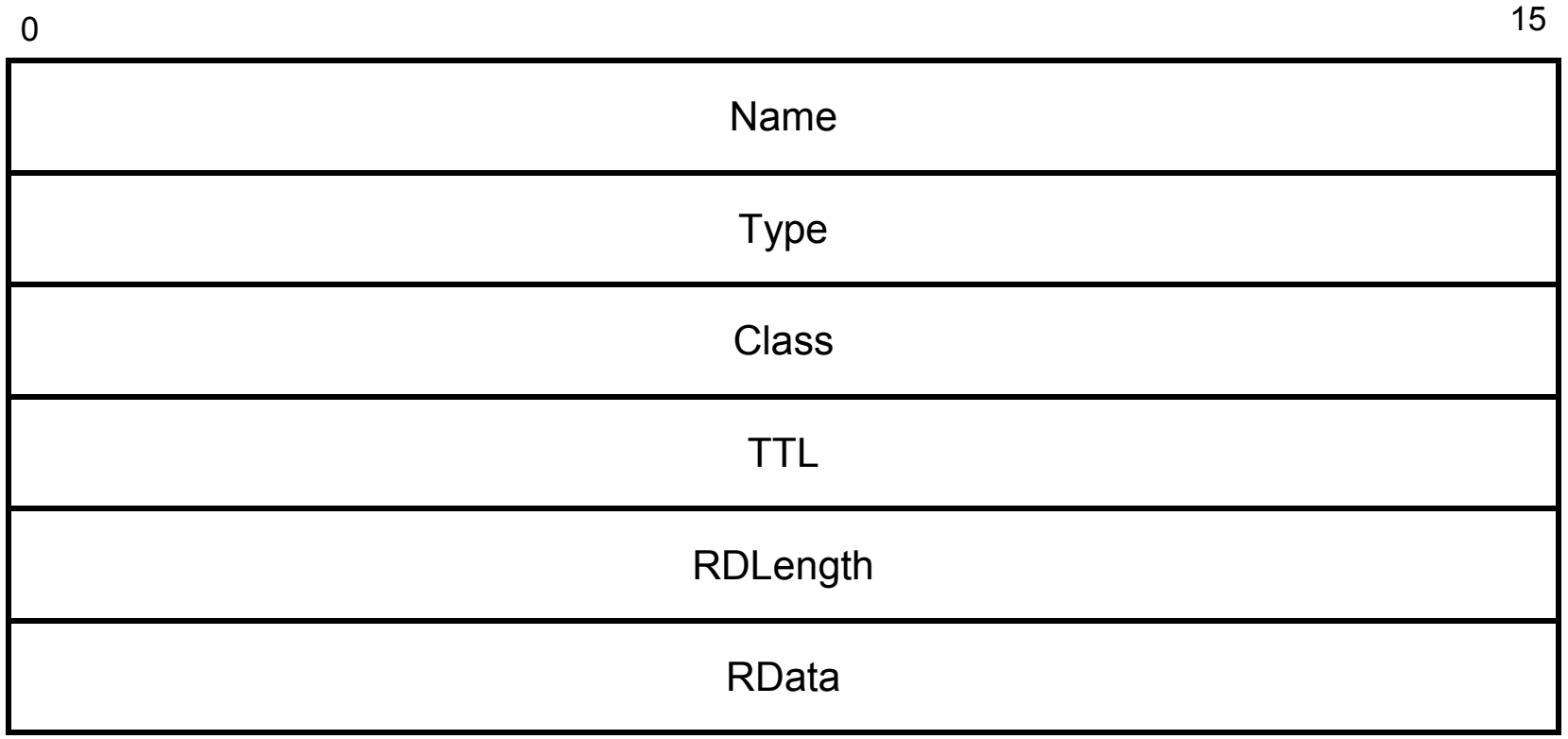
→ Kommunikation: Das Format des DNS-Anfrageteils (6/8)



Bezeichnung	Inhalt
QNAME	Ein als Labelsequenz dargestellter Domainname. Jedes der Labels beginnt mit einem Byte, das die Labellänge angibt.
QTYPE	Zwei-Byte Feld, das den Type einer Anfrage enthält.
QCLASS	Zwei-Byte Feld, das die Klasse einer Anfrage spezifiziert.

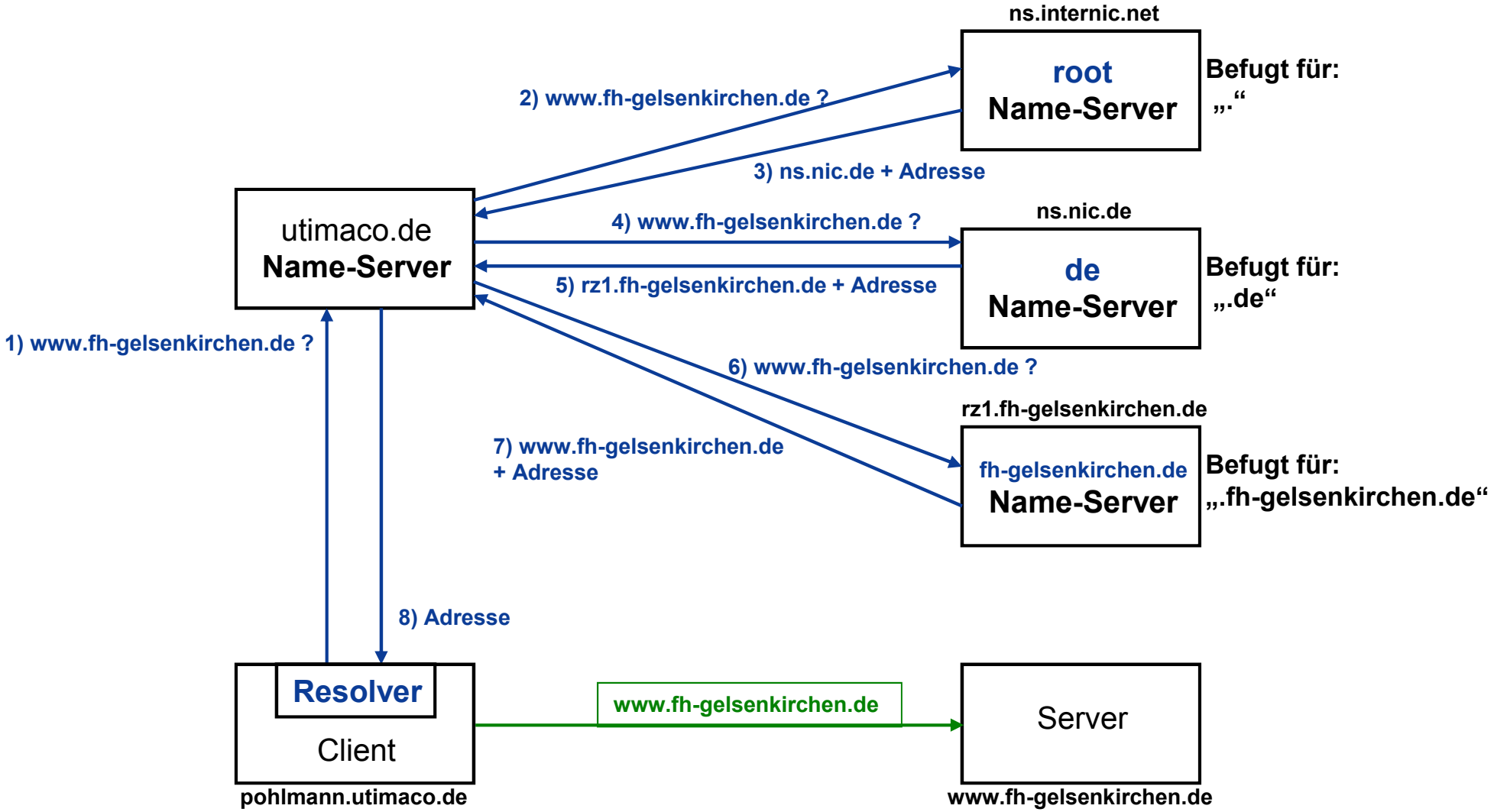
Domain Name System (DNS)

→ Kommunikation: Das Resource Record Format (7/8)



- Die „Antwort“, „Name-Server Informationen“ und die „sonstigen Informationen“ nutzen das Resource Record Format.

Domain Name System (DNS)
→ Kommunikation (8/8)



Westfälische Hochschule
Gelsenkirchen Bocholt Recklinghausen
University of Applied Sciences

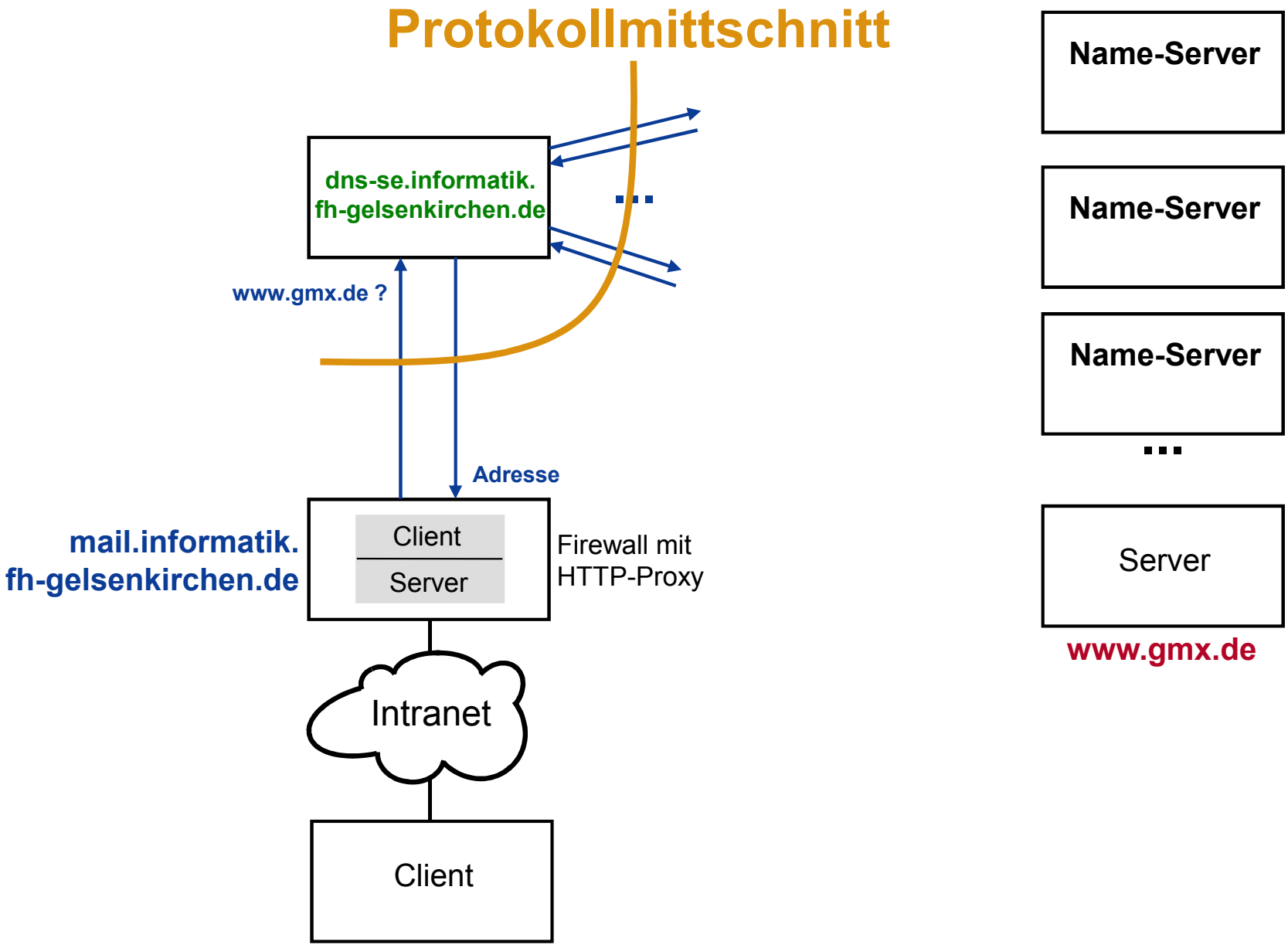
Beispiel einer DNS-Anfrage

Prof. Dr. (TU NN)
Norbert Pohlmann

Institut für Internet-Sicherheit – if(is)
Westfälische Hochschule, Gelsenkirchen
http://www.internet-sicherheit.de

if(is) internet-sicherheit.

Domain Name System (DNS)
→ Kommunikation: Beispiel (1/17)



Domain Name System (DNS)
→ Kommunikation: Beispiel (2/17)

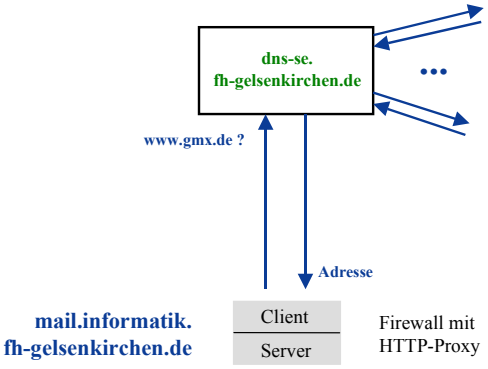
- ***Anmerkung:***
  Der Name-Server „**dns-se.informatik.fh-gelsenkirchen.de**“ wurde neu gestartet und daher ist der Cache leer.
- Der HTTP-Proxy der Firewall mit dem Namen „**mail.informatik.fh-gelsenkirchen.de**“ fragt den Name-Server „**dns-se.informatik.fh-gelsenkirchen.de**“ nach der IP-Adresse von „**www.gmx.de**“.
- Protokollmitschnitt: Anfrage (a)

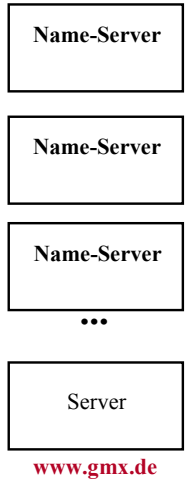
No.	Time	Source	Destination	Protocol	Info
1	0.000000	mail.informatik.fh-gelsenkirchen.de	dns-se	DNS	Standard query A www.gmx.de

1 Domain Name System (query)
Queries
www.gmx.de: type A, class inet

Frage nach der IP-Adresse

Internet





Domain Name System (DNS)
→ Kommunikation: Beispiel (3/17)

- Da der Cache des Name-Servers „**dns-se.informatik.fh-gelsenkirchen.de**“ leer ist, wird eine Anfrage an einen ROOT-Name-Server durchgeführt.
- Die IP-Adressen der ROOT-Name-Server stehen in der Konfigurationsdatei des Nameservers.
- Protokollmitschnitt: Anfrage (b)

No.	Time	Source	Destination	Protocol	Info
7	0.437416	dns-se	B.ROOT-SERVERS.NET	DNS	Standard query A www.gmx.de

7 Domain Name System (query)
Queries
www.gmx.de: type A, class inet

Domain Name System (DNS)
→ Kommunikation: Beispiel (4/17)

- Da der ROOT-Name-Server die Domäne „gmx.de“ nicht verwaltet, sendet er als Antwort eine Liste von Name-Servern, die für die Domäne „de“ verantwortlich sind.
- Protokollmitschnitt: Antwort (b)

No.	Time	Source	Destination	Protocol	Info
10	0.611543	B.ROOT-SERVERS.NET	dns-se	DNS	Standard query response

```
10  Domain Name System (response)
  Queries
     www.gmx.de: type A, class inet
  Authoritative nameservers
     de: type NS, class inet, ns AUTH03.NS.DE.UU.NET
     de: type NS, class inet, ns DNS.DENIC.de
     de: type NS, class inet, ns SSS-AT.DENIC.de
     de: type NS, class inet, ns SSS-NL.DENIC.de
     de: type NS, class inet, ns SSS-DE1.DE.NET
     de: type NS, class inet, ns SSS-UK.DE.NET
     de: type NS, class inet, ns DNS2.DE.NET
     de: type NS, class inet, ns SSS-JP.DENIC.de
     de: type NS, class inet, ns SSS-US1.DE.NET
     de: type NS, class inet, ns SSS-US2.DENIC.de
     de: type NS, class inet, ns SSS-SE.DENIC.de
  Additional records
     AUTH03.NS.DE.UU.NET:  type A, class inet, addr 192.76.144.16
     DNS.DENIC.de:         type A, class inet, addr 81.91.161.5
     SSS-AT.DENIC.de:      type A, class inet, addr 193.171.255.34
     SSS-NL.DENIC.de:      type A, class inet, addr 193.0.0.237
     SSS-DE1.DE.NET:       type A, class inet, addr 193.159.170.187
     SSS-UK.DE.NET:        type A, class inet, addr 62.53.3.68
     DNS2.DE.NET:          type A, class inet, addr 81.91.162.5
     SSS-JP.DENIC.de:      type A, class inet, addr 210.81.13.179
     SSS-US1.DE.NET:       type A, class inet, addr 206.65.170.100
     SSS-US2.DENIC.de:     type A, class inet, addr 167.216.196.131
     SSS-SE.DENIC.de:      type A, class inet, addr 192.36.144.211
```

Domain Name System (DNS)
→ Kommunikation: Beispiel (5/17)

- Der Name-Server „**dns-se.informatik.fh-gelsenkirchen.de**“ führt jetzt eine Anfrage an den DE-Name-Server „sss-uk.de.net“ durch, um an eine IP-Adresse eines Name-Servers von „gmx.de“ zu gelangen.
- Protokollmitschnitt: Anfrage (c)

No.	Time	Source	Destination	Protocol	Info
12	0.626329	dns-se	sss-uk.de.net	DNS	Standard query A www.gmx.de

12 Domain Name System (query)
Queries
www.gmx.de: type A, class inet

Domain Name System (DNS)
→ Kommunikation: Beispiel (6/17)

- Da der DE-Name-Server „sss-uk.de.net“ die Domäne „gmx.de“ nicht verwaltet, sendet er als Antwort eine Liste von Name-Servern, die für die Domäne „gmx.de“ verantwortlich sind.
- Protokollmitschnitt: Antwort (c)

No.	Time	Source	Destination	Protocol	Info
13	0.656547	sss-uk.de.net	dns-se	DNS	Standard query response

13 Domain Name System (response)
Queries
www.gmx.de: type A, class inet
Authoritative nameservers
gmx.de: type NS, class inet, ns dns.gmx.net
gmx.de: type NS, class inet, ns ns.schlund.de

Domain Name System (DNS)
→ Kommunikation: Beispiel (7/17)

- Der Name-Server „**dns-se.informatik.fh-gelsenkirchen.de**“ fragt nach der IP-Adresse des Name-Servers von „ns.schlund.de“ bei einem anderen DE-Name-Server „sss-jp.denic.de“, da er diese nicht kennt und der erste DE-Name-Server diese nicht mitgesendet hat.
- Protokollmitschnitt: Anfrage (d)

No.	Time	Source	Destination	Protocol	Info
14	0.664020	dns-se	sss-jp.denic.de	DNS	Standard query A ns.schlund.de

14 Domain Name System (query)
Queries
ns.schlund.de: type A, class inet

Domain Name System (DNS)
→ Kommunikation: Beispiel (8/17)

- Zusätzlich möchte der Name-Server „**dns-se.informatik.fh-gelsenkirchen.de**“ bei dem zweiten Name-Server, der für die Domäne „gmx.de“ verantwortlich ist (dns.gmx.net), ein Anfrage stellen.
- Da er aber keinen Name-Server für „net“ kennt, fragt er wieder bei einem ROOT-Name-Server nach.
- Protokollmitschnitt: Anfrage (e)

No.	Time	Source	Destination	Protocol	Info
15	0.666071	dns-se	L.ROOT-SERVERS.NET	DNS	Standard query A dns.gmx.net

15 Domain Name System (query)
Queries
dns.gmx.net: type A, class inet

Domain Name System (DNS)
→ Kommunikation: Beispiel (9/17)

- Da der ROOT-Name-Server die Domäne „dns.gmx.net“ nicht verwaltet, sendet er als Antwort eine Liste von Name-Servern, die für die Domäne „net“ verantwortlich sind.
- Protokollmitschnitt: Antwort (e)

No.	Time	Source	Destination	Protocol	Info
26	0.867239	L.ROOT-SERVERS.NET	dns-se	DNS	Standard query response

```
26 Domain Name System (response)
  Queries
     dns.gmx.net: type A, class inet
  Authoritative nameservers
     net: type NS, class inet, ns A.GTLD-SERVERS.net
     net: type NS, class inet, ns G.GTLD-SERVERS.net
     net: type NS, class inet, ns H.GTLD-SERVERS.net
     net: type NS, class inet, ns C.GTLD-SERVERS.net
     net: type NS, class inet, ns I.GTLD-SERVERS.net
     net: type NS, class inet, ns B.GTLD-SERVERS.net
     net: type NS, class inet, ns D.GTLD-SERVERS.net
     net: type NS, class inet, ns L.GTLD-SERVERS.net
     net: type NS, class inet, ns F.GTLD-SERVERS.net
     net: type NS, class inet, ns J.GTLD-SERVERS.net
     net: type NS, class inet, ns K.GTLD-SERVERS.net
     net: type NS, class inet, ns E.GTLD-SERVERS.net
     net: type NS, class inet, ns M.GTLD-SERVERS.net
  Additional records
     A.GTLD-SERVERS.net: type A, class inet, addr 192.5.6.30
     G.GTLD-SERVERS.net: type A, class inet, addr 192.42.93.30
     H.GTLD-SERVERS.net: type A, class inet, addr 192.54.112.30
     C.GTLD-SERVERS.net: type A, class inet, addr 192.26.92.30
     I.GTLD-SERVERS.net:  type A, class inet, addr 192.43.172.30
     B.GTLD-SERVERS.net: type A, class inet, addr 192.33.14.30
     D.GTLD-SERVERS.net: type A, class inet, addr 192.31.80.30
     L.GTLD-SERVERS.net: type A, class inet, addr 192.41.162.30
     F.GTLD-SERVERS.net: type A, class inet, addr 192.35.51.30
     J.GTLD-SERVERS.net: type A, class inet, addr 192.48.79.30
     K.GTLD-SERVERS.net: type A, class inet, addr 192.52.178.30
     E.GTLD-SERVERS.net: type A, class inet, addr 192.12.94.30
     M.GTLD-SERVERS.net: type A, class inet, addr 192.55.83.30
```

Domain Name System (DNS)
→ Kommunikation: Beispiel (10/17)

- Der Name-Server „**dns-se.informatik.fh-gelsenkirchen.de**“ führt jetzt eine Anfrage an den NET-Name-Server „h.gtld-server.net“ durch, um die IP-Adresse von dem Name-Server „dns.gmx.net“ zu erhalten.
- Protokollmitschnitt: Anfrage (f)

No.	Time	Source	Destination	Protocol	Info
29	0.922138	dns-se	h.gtld-servers.net	DNS	Standard query A dns.gmx.net

29 Domain Name System (query)
Queries
dns.gmx.net: type A, class inet

Domain Name System (DNS)
→ Kommunikation: Beispiel (11/17)

- Da der DE-Name-Server „sss-jp.denic.de“ die IP-Adresse „ns.schlund.de“ nicht verwaltet, sendet er als Antwort eine Liste von Name-Servern, die für die Domäne „schlund.de“ verantwortlich sind.
- ***Hinweis:***
  Dies ist die Anwort aus der Anfrage (d)
- Protokollmitschnitt: Antwort (d)

No.	Time	Source	Destination	Protocol	Info
30	0.943825	sss-jp.denic.de	dns-se	DNS	Standard query response

30 Domain Name System (response)
  Queries
    ns.schlund.de: type A, class inet
  Authoritative nameservers
    schlund.de: type NS, class inet, ns nsa.schlund.de
    schlund.de: type NS, class inet, ns nsa2.schlund.de
  Additional records
    nsa.schlund.de: type A, class inet, addr 195.20.224.98
    nsa2.schlund.de: type A, class inet, addr 212.227.123.18

Domain Name System (DNS)
→ Kommunikation: Beispiel (12/17)

- Der Name-Server „**dns-se.informatik.fh-gelsenkirchen.de**“ fragt den Name-Servern, der für die Domäne „schlund.de“ verantwortlich ist, nach der IP-Adresse von „ns.schlund.de“.
- Die IP-Adresse des Name-Server kommt von der Antwort (d).
- Protokollmitschnitt: Anfrage (g)

No.	Time	Source	Destination	Protocol	Info
31	0.949373	dns-se	nsa.schlund.de	DNS	Standard query A ns.schlund.de

31 Domain Name System (query)
Queries
ns.schlund.de: type A, class inet

Domain Name System (DNS)
→ Kommunikation: Beispiel (13/17)

- Der NET-Name-Server „h.gtld-server.net“ sendet als Antwort eine Liste von Name-Servern, die für die Domäne „gmx.de“ verantwortlich sind.
- ***Hinweis:***
  Die ist die Anwort aus der Anfrage (f)
- Protokollmitschnitt: Antwort (f)

No.	Time	Source	Destination	Protocol	Info
32	0.961864	h.gtld-servers.net	dns-se	DNS	Standard query response A 213.165.64.1

```
32 Domain Name System (response)
  Queries
     dns.gmx.net: type A, class inet
  Answers
     dns.gmx.net: type A, class inet, addr 213.165.64.1
  Authoritative nameservers
     gmx.net: type NS, class inet, ns ns.schlund.de
     gmx.net: type NS, class inet, ns dns.gmx.net
  Additional records
     dns.gmx.net: type A, class inet, addr 213.165.64.1
```

Domain Name System (DNS)
→ Kommunikation: Beispiel (14/17)

- Der Name-Server „**dns-se.informatik.fh-gelsenkirchen.de**“ fragt den Name-Server „dns.gmx.net“, der für die Domäne „gmx.de“ zuständig ist, nach der IP-Adresse von „**www.gmx.de**“.
- Protokollmitschnitt: Anfrage (h)

No.	Time	Source	Destination	Protocol	Info
33	0.966762	dns-se	dns.gmx.net	DNS	Standard query A www.gmx.de

33 Domain Name System (query)
Queries
www.gmx.de: type A, class inet

Domain Name System (DNS)
→ Kommunikation: Beispiel (15/17)

- Der GMX.DE-Name-Server „dns.gmx.net“ sendet als Antwort an den Name-Server „**dns-se.informatik.fh-gelsenkirchen.de**“ die IP-Adresse des Rechners „**www.gmx.de**“.
- Protokollmitschnitt: Antwort (h)

No.	Time	Source	Destination	Protocol	Info
35	0.985743	dns.gmx.net	dns-se	DNS	Standard query response A 213.165.65.100

35 Domain Name System (response)
- Queries
  - www.gmx.de: type A, class inet
- Answers
  - www.gmx.de: type A, class inet, addr 213.165.65.100
- Authoritative nameservers
  - gmx.de: type NS, class inet, ns ns.schlund.de
  - gmx.de: type NS, class inet, ns dns.gmx.net
- Additional records
  - dns.gmx.net: type A, class inet, addr 213.165.64.1

Domain Name System (DNS)
→ Kommunikation: Beispiel (16/17)

- Der Name-Server „**dns-se.informatik.fh-gelsenkirchen.de**“ sendet als Antwort an die Firewall „**mail.informatik.fh-gelsenkirchen.de**“ die IP-Adresse des Rechners „**www.gmx.de**“.
- Protokollmitschnitt: Antwort (a)

No.	Time	Source	Destination	Protocol	Info
36	0.991247	dns-se	mail.informatik.fh-gelsenkirchen.de	DNS	Standard query response A 213.165.65.100

36 Domain Name System (response)
- Queries
  - www.gmx.de: type A, class inet
- Answers
  - www.gmx.de: type A, class inet, addr 213.165.65.100
- Authoritative nameservers
  - gmx.de: type NS, class inet, ns ns.schlund.de
  - gmx.de: type NS, class inet, ns dns.gmx.net
- Additional records
  - ns.schlund.de: type A, class inet, addr 195.20.224.97
  - dns.gmx.net: type A, class inet, addr 213.165.64.1

Ergebniss

Domain Name System (DNS)
→ Kommunikation: Beispiel (17/17)

- Die Anwort von Anfrage (g) wurde nicht mehr dargestellt!
- Da parallel weitere Anfragen, die nichts mit unserem Beispiel zu tun haben, an den Name-Server „**dns-se.informatik.fh-gelsenkirchen.de**“ gesendet worden sind, sind die Numerierungen der DNS-Pakete, zum Teil nicht chronologisch.

- Dies Beispiel zeigt, dass die Anfrage nach einer IP-Adresse sehr aufwendig sein kann!
- Aus diesem Grund sind die Caches in den Rechnerssytemen (Resolver) und in den Name-Servern wichtig, um den Datentransfer für DNS so gering wie möglich zu halten.

Inhalt

- Ziele, Einordnung und Einleitung
- Hierarchische Namen/Namensvergabe im Internet
- Abbildung der Domain-Namen auf Adressen
- Aufbau von DNS
- Kommunikation mit den Name-Servern
- **Aliasnamen**
- Caching
- Zusammenfassung

Domain Name System (DNS)
→ Aliasnamen (1/3)

- Es ist auch möglich, für Rechner Aliasnamen zu vergeben.
- Mit einem Alias wird ein Rechnername mit einem weiteren, z.B. applikationsbezogenen Namen versehen.
- Dies kann z.B. für folgenden Anwendungsfall wichtig sein:
- Ein verteiltes System aus z.B. 2 Server-Rechnern Server1 und Server2 existieren.
- Auf diesen Servern sind verschiedene Server-Prozesse eines Buchungssystems für eine Reisebuchung aktiv:

Server	Applikation
Server1	Flugauskunft, Flugbuchung
Server2	Hotelreservierung

Domain Name System (DNS)
→ Aliasnamen (2/3)

- An diese Server sind mehrere tausend Clients angeschlossen.
- Damit diese Clients arbeiten können, muss zum Aufruf der jeweiligen Aktion ein Rechnername hinterlegt werden, d.h. Server1 für die Flugauskunft und Flugbuchung und Server2 für die Hotelreservierung.
- Ein Problem tritt aber auf, wenn Server1 im Laufe der Zeit überlastet ist und beschlossen wird, eine der 2 Applikationen auf einen eigenen Server auszulagern.
- Dann muss in den tausenden von Clients dieser Rechnername geändert werden.
- Benutzt man aber Aliasnamen so ist es möglich, einen neuen Rechner einzufügen und einen der Aliasnamen von Server1 auf Server3 zu übertragen.

Adresse	Name	Alias
134.108.56.60	Server1	Flugauskunft, Flugbuchung
134.108.56.61	Server2	Hotelreservierung

Domain Name System (DNS)
→ Aliasnamen (3/3)

Adresse	Name	Alias
134.108.56.60	Server1	Flugauskunft
134.108.56.61	Server2	Hotelreservierung
134.108.56.62	Server3	Flugbuchung

- Es ist kein Änderungsaufwand bei den Clients notwendig, wenn in den Clientapplikationen von Anfang an nur die Aliasnamen verwendet werden.

Inhalt

- Ziele, Einordnung und Einleitung
- Hierarchische Namen/Namensvergabe im Internet
- Abbildung der Domain-Namen auf Adressen
- Aufbau von DNS
- Kommunikation mit den Name-Servern
- Aliasnamen
- **Caching**
- Zusammenfassung

Domain Name System (DNS)
→ Caching (1/2)

- Die Kosten und auch die Netzlast für die Auflösung nicht-lokaler Namen können extrem hoch werden.
- Aus diesem Grund besitzen die meisten Implementationen eines Resolvers und der Name-Server einen Cache für häufig benutzte Namen.
- Zusätzlich zu den Namen mit entsprechenden IP-Adressen wird in diesem Cache auch noch die IP-Adresse des Name-Servers, von dem dieser Rechnername aufgelöst wurde, abgespeichert.
- Fragt eine Anwendung den lokalen Resolver ab, prüft dieser zuerst, ob der Name zu seiner eigenen Domäne gehört.
- Ist dies nicht der Fall, so wird der Cache durchsucht.
- Erst wenn der gesuchte Name auch dort nicht enthalten ist, beginnt der Resolver die Abfrage beim Name-Server.
- Der Anwendung wird mitgeteilt, wenn das Ergebnis aus dem Cache geholt wurde.

Domain Name System (DNS)
→ Caching (2/2)

- Genügt der Anwendung diese evtl. veraltete Information nicht, so kann diese den Resolver auffordern, bei dem ebenfalls noch bekannten Name-Server anzufragen, ob die Namensauflösung noch korrekt ist.
- Da aber die Zuordnung von Namen und IP-Adresse sehr selten geändert wird, ist dies kaum notwendig und die Anwendung wird im Regelfall die Abfrage aus dem Cache akzeptieren.

Domain Name System (DNS)
→ Inverse Abfragen

- Es ist neben der normalen Abfrage auch möglich, eine inverse Abfrage an einen Name-Server zu stellen. D.h. man gibt eine IP-Adresse vor und erhält einen Rechnernamen zurück.
- Diese Form der Abfrage wird auch Pointer-Query genannt.
- Um einen Pointer-Query zu generieren, muss die bekannte IP-Adresse

  aaa.bbb.ccc.ddd

  in umgekehrter Reihenfolge angegeben und anschließend der String „in-addr.arpa“ angehängt werden:

  ddd.ccc.bbb.aaa.in-addr.arpa

- Die umgekehrte Reihenfolge deshalb, da das most significant Octet im Domänen Name als letztes und in der IP-Adresse als erstes kommt.

Domain Name System (DNS)
→ Das Kommando nslookup (1/2)

- Mit dem Kommando „nslookup“ kann eine Abfrage an den Name-Server aus einer Shell des Betriebssystems durchgeführt werden.
- Das Kommando „nslookup“ hat folgende Optionen:

nslookup [-opt] [host] [server]

-opt	Setzen von Optionen
host	der gesuchte Host
server	Angabe eines anderen als den default Name-Server

- *Beispiele mit nslookup:*

```
nslookup
Default Server:  dns-pi.informatik.fh-ge.de
Address:  172.16.0.10
```

Interner Name-Server des Fachbereiches

- *Den Default-Server verlassen und einen anderen wählen*

```
> server 194.94.127.83
Default Server:  dns-pe.fh-gelsenkirchen.de
Address:  194.94.127.83
Aliases:  83.127.94.194.in-addr.arpa
```

Externer Name-Server des Fachbereiches

Domain Name System (DNS)
→ Das Kommando nslookup (2/2)

- *Nach dem Mail-Server einer Domäne fragen*

```
> set querrytype=mx
> informatik.fh-gelsenkirchen.de.
Server:  dns-pe.fh-gelsenkirchen.de
Address:  194.94.127.83
Aliases:  83.127.94.194.in-addr.arpa

informatik.fh-gelsenkirchen.de  preference = 10, mail exchanger = mail1.informatik.fh-gelsenkirchen.de
informatik.fh-gelsenkirchen.de  preference = 20, mail exchanger = mail2.informatik.fh-gelsenkirchen.de
informatik.fh-gelsenkirchen.de  nameserver = dns-se.informatik.fh-gelsenkirchen.de
informatik.fh-gelsenkirchen.de  nameserver = dns-pe.informatik.fh-gelsenkirchen.de
dns-pe.informatik.fh-gelsenkirchen.de   internet address = 194.94.127.83
dns-se.informatik.fh-gelsenkirchen.de   internet address = 194.94.127.27
```

Der Mail-Server mit der kleineren „Preference“ soll bevorzugt werden

- *Nach dem Mail-Server einer weiteren Domäne fragen*

```
> gmx.de.
Server:  dns-pe.fh-gelsenkirchen.de
Address:  194.94.127.83
Aliases:  83.127.94.194.in-addr.arpa

Non-authoritative answer:
gmx.de  preference = 10, mail exchanger = mx0.gmx.net
gmx.de  preference = 10, mail exchanger = mx0.gmx.de

Authoritative answers can be found from:
gmx.de  nameserver = ns.schlund.de
gmx.de  nameserver = dns.gmx.net
mx0.gmx.de      internet address = 213.165.64.100
ns.schlund.de   internet address = 195.20.224.97
dns.gmx.net     internet address = 213.165.64.1
```

Wahrscheinlich zwei SMTP-Proxies, der eigentliche Mail-Server steht im geschützten Bereich

Domain Name System (DNS)
→ Andere Anwendungen

- **Realtime Blocking Lists (RBL)**
  - Z.B. um das Problem der Spam-Mails zu reduzieren.

- **Loadbalancing**
  - Wenn ein Hostname aufgelöst wird, dann ist die Antwort nicht auf einen Eintrag beschränkt.
  - Es ist möglich mit mehreren Adressen zu antworten, deren Reihenfolge zufällig vom Name-Server bestimmt wird.
  - Da ein Resolver im Allgemeinen nur den ersten Eintrag weitergibt, bekommen unterschiedliche Anfragen verschiedene Ergebnisse.
  - Bei der Verwendung von mehreren Servern (z.B. Webserver), die die gleiche Aufgabe erfüllen, lässt man einen Namen auf alle Adressen dieser Server auflösen.
  - Stellen nun viele Benutzer eine Verbindung auf diesen Namen her, so werden sie etwa gleichmäßig auf die verschiedenen Server verteilt.

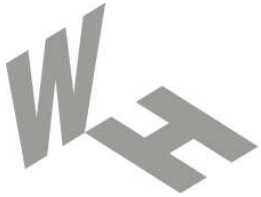
Inhalt

- Ziele, Einordnung und Einleitung
- Hierarchische Namen/Namensvergabe im Internet
- Abbildung der Domain-Namen auf Adressen
- Aufbau von DNS
- Kommunikation mit den Name-Servern
- Aliasnamen
- Caching
- **Zusammenfassung**

Domain Name System (DNS)
→ Zusammenfassung

- **Konzept:**
  - DNS ist ein **hierarchisches domänenorientiertes** Namenssystem und
  - ein **verteiltes Dateisystem (Ressourcen Records)** zur Realisierung dieses Namenssystems.
  - Ohne DNS - keine Kommunikation!

- **Ziele:**
  - DNS wird hauptsächlich benutzt, um Rechnernamen auf IP-Adressen abzubilden.
  - Anwendungen, die den DNS Service nutzen, sind z.B. HTTP, SMTP, FTP.



Westfälische Hochschule
Gelsenkirchen Bocholt Recklinghausen
University of Applied Sciences

Domain Name System (DNS)

Vielen Dank für Ihre Aufmerksamkeit
Fragen ?

Prof. Dr. (TU NN)
Norbert Pohlmann

Institut für Internet-Sicherheit – if(is)
Westfälische Hochschule, Gelsenkirchen
http://www.internet-sicherheit.de