Application Layer

Domain Name System (DNS)

Standards

Das Domain Name System bildet ein verteiltes Verzeichnis zur Umwandlung von Namen und Adressen.

Der Internet Standard 13 (DOMAIN) umfaßt

- **RFC1034** Domain Names - Concepts and Facilities
- **RFC1035** Domain Names - Implementation and Specification

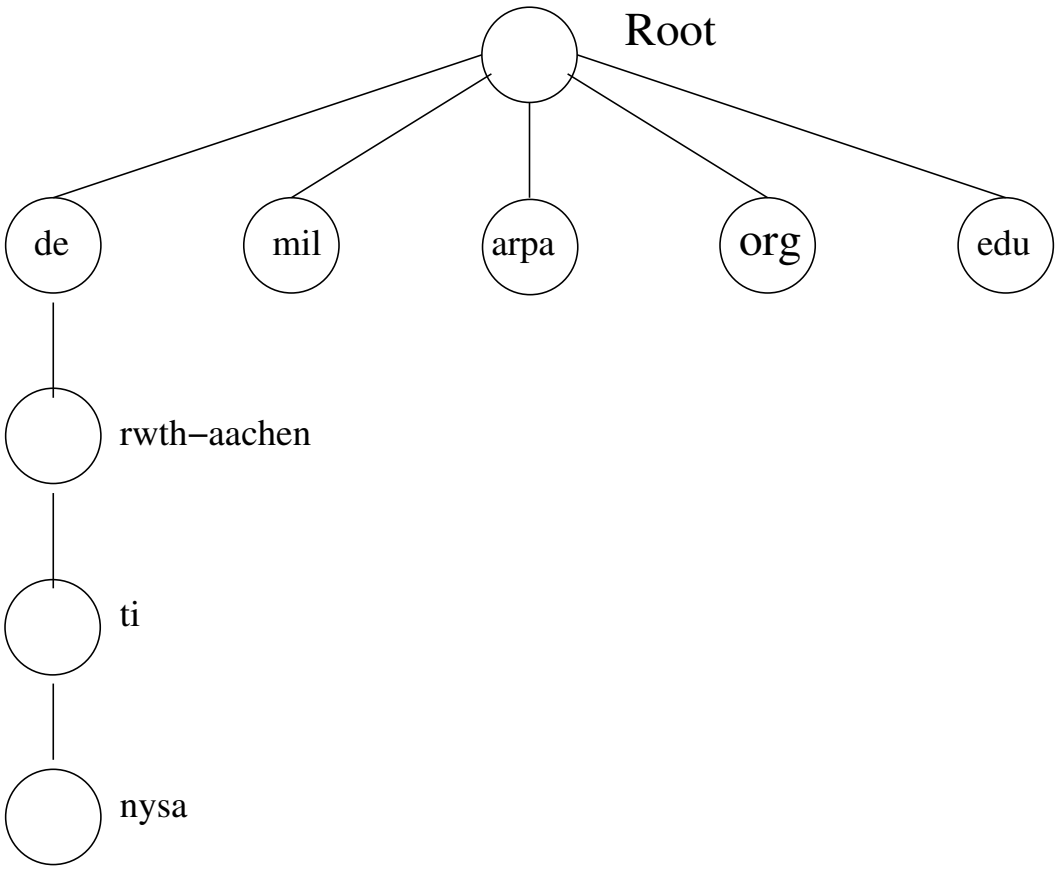
Eine Vielzahl von Erweiterungen finden sich in jüngeren RFCs (vgl. `http://www.dns.net/dnsrd/rfc/`) und sind zum Teil in aktuellen DNS Servern implementiert.

Syntax für Namen

Die dem DNS zugrunde liegende Datenbank hat einen hierarchischen Aufbau, der sich in den Namen widerspiegelt:

- Namen bestehen aus Folgen von Bezeichnern (Label), die maximal 63 Zeichen lang sind.
- Die Bezeichner werden durch einen Punkt (’.’) getrennt.
- Zwischen Groß- oder Kleinschreibung wird nicht unterschieden.
- RFC1035 empfiehlt für Label, mit einem Buchstaben (a-z oder A-Z) zu beginnen, dann Buchstaben, Ziffern oder ’-’ und nicht mit einem ’-’ zu enden.
- Namen, die mit einem Punkt (’.’) enden, werden als vollständig angenommen, andernfalls ist eine Erweiterung nötig, um zum **Fully Qualified Domain Name, FQDN** zu kommen.

Verzeichnisaufbau



Top Level Domain

Second Level Domain

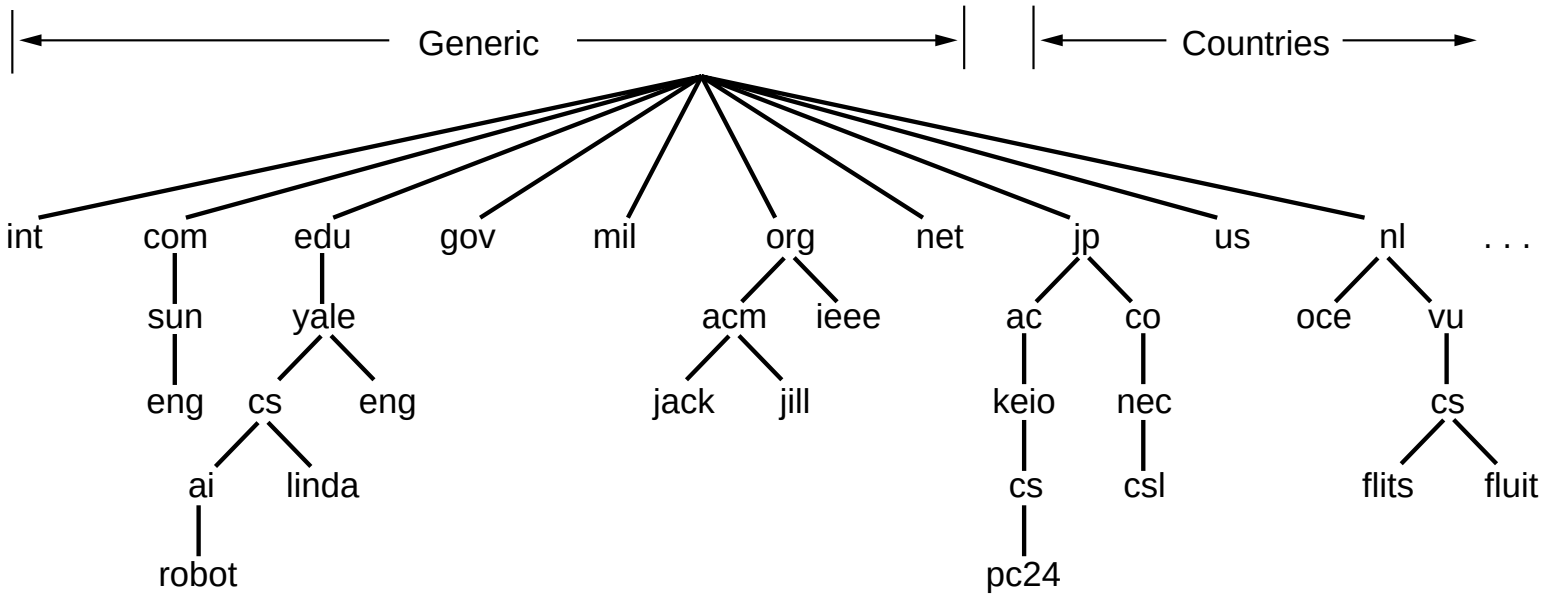
Verzeichnisaufbau

Namen werden in umgekehrter Reihenfolge des Labels geschrieben, d.h. die Top Level Domain (TLD) zuletzt.

Beispiele:

- **nysa** oder **RWTH-Aachen**: Bezeichner gemäß RFC1035
- **nysa.ti.rwth-aachen.de.**: FQDN
- **nysa.ti**: Unvollständiger Name
- **182.35.130.134.in-addr.arpa.**: FQDN

Top Level Domains



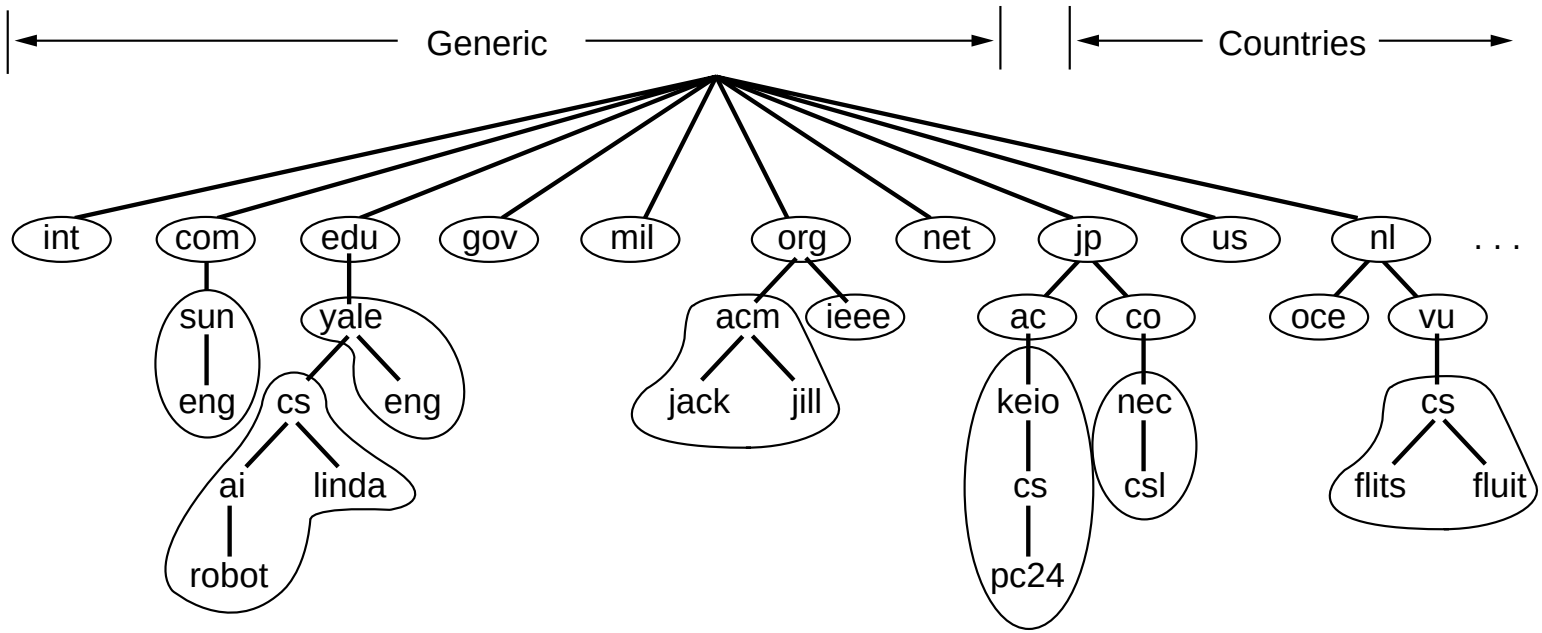
(c) Tanenbaum, Computer Networks

Top Level Domains

- **Country Coded TLD**: ISO 3166 Ländercode, Administrativer Kontakt unter `http://www.iana.org/root-whois/index.html`
- **Generic TLD**: Namen, die einer bestimmten Organisation/Verwendung zugeordnet sind, z.B. `.com`, `.edu`, Administrativer Kontakt unter `http://www.iana.org/gtld/gtld.html`
- **Infrastucture TLD**: TLD für Namen, die aus technischen Gründen benutzt werden, `.arpa` erzeugt eine separaten Baum, `.root` wird nur als Marker der Rootzone verwendet.

```
$host -t TXT \
  vrsn-end-of-zone-marker-dummy-record.root
```

DNS Zonen



(c) Tanenbaum, Computer Networks

DNS Zonen

- Zonen sind separat administrierbare Unterbäume des Verzeichnisses
- Der Administrator einer Zone ist dafür verantwortlich, DNS Server für diese Zone bereitzustellen
- Der Administrator einer Zone kann die Verwaltung von Unterbäumen an andere Administratoren delegieren.
- Primary DNS Server einer Zone ist der (ggfs. redundant aufgebaute) Server, auf dem die Konfigurationsdaten der Zone administriert werden.
- Eine Zone kann weitere Secondary DNS Server haben, die die Konfigurationsdaten vom Primary DNS Server herunterladen (sog. Zone Transfer).
- Ein DNS Server ist Authoritative, wenn er eine aktuelle Kopie der Zone hat.

DNS Rahmen

Identification	Flags
Number of Questions	Number of RRs
Number of Authority RRs	Number of Additional RRs
Questions	
Answer RRs	
Authority RRs	
Additional RRs	

Felder im DNS Rahmen

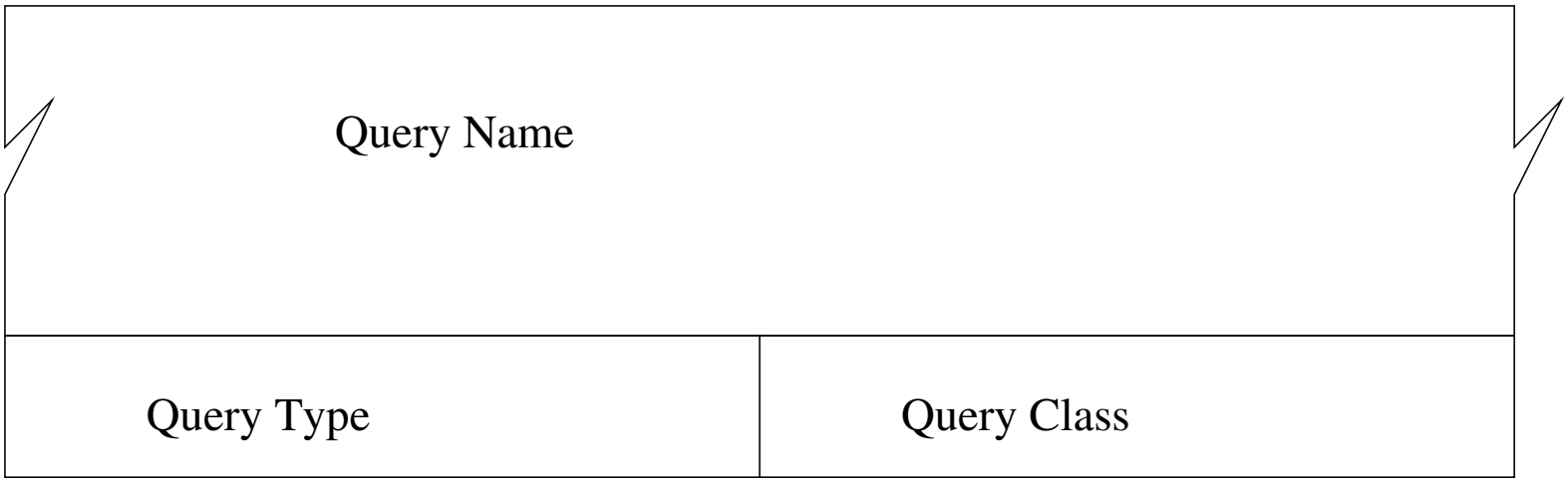
- **Identification**: 16 Bit Code, mit dem die Antwort einem Request zugeordnet werden kann.
- **Flags**: 16 Bit, beschreibt Art der Antwort, Fehlerstatus, ...
- **Number of Questions**: 1 für DNS Anfragen, 0 für Antworten
- **Number of RRs**: Anzahl Resource Records (Antworten auf eine Anfrage)
- **Number of Authority RRs**: Anzahl Authority Records (DNS Server, die die gesuchte Information sicher haben)
- **Number of Additional RRs**: Anzahl Additional Records (Zusatzinformation, z.B. die Adressen der DNS Server aus den Authority Records)

Flags

QR	opcode	AA	TC	RD	RA	empty (0)	RCode

- **QR**: 0: Anfrage, 1: Antwort
- **opcode**: 0: Default, 1: Inverse Abfrage, 2: Server Status
- **AA**: Antwort ist “authoritative”
- **TC**: (Truncated) Paket enthält nur 512 Bytes der Antwort
- **RD**: 1: Server soll Anfrage rekursiv bearbeiten
- **RA**: 1: Server bietet Rekursion an
- **RCode**: Fehlerstatus, 0: Kein Fehler, 3: Name nicht gefunden

Question Datensatz



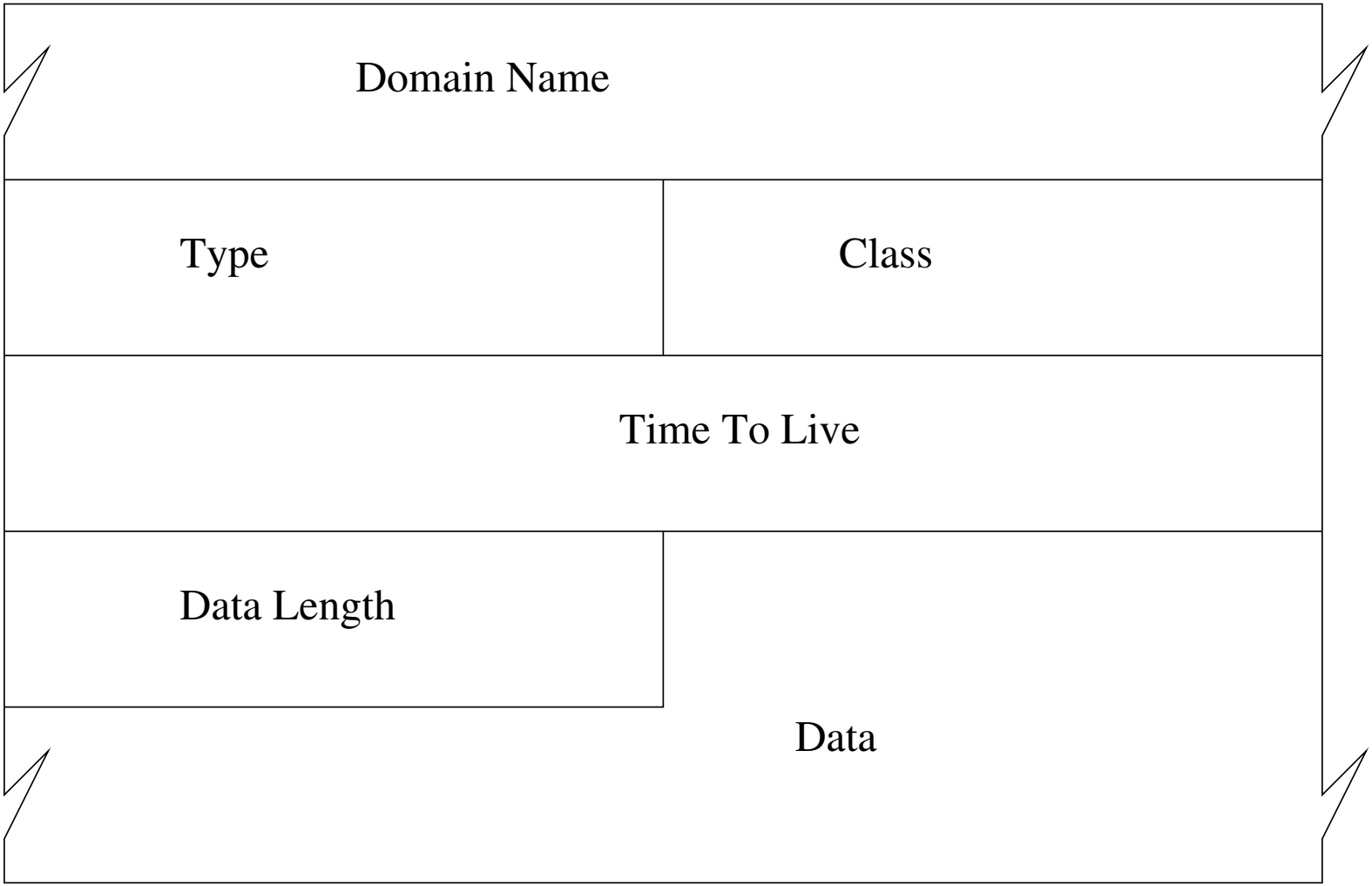
- **Query Name**: Name, der abgefragt wird
- **Query Type**: Typ der Anfrage, entweder Standardtyp oder
  - **ANY**: Jeder Standardtyp
  - **AXFR**: Zonentransfer
- **Query Class**: 1 für Internet (IN)

Standardtypen

Hier ist eine Auswahl der gebräuchlichsten Datensätze

Typ	Wert	Name
A	1	IPv4 Adresse
NS	2	Name Server Name
CNAME	5	Canonical Name (Alias)
SOA	6	Start of Authority, Administrative Daten einer Domain
PTR	12	Pointer Record (Verweis)
HINFO	13	Host Info (Informationen über den Rechner)
MX	15	Mail Exchange (Zuständiger E-Mailserver)
AAAA	28	IPv6 Adresse (RFC1933)
SRV	32	Server Record (Host:Port des Servers)
NAPTR	35	Naming Authority Pointer (RFC2915)

Resource Records



Felder eines Resource Records

- **Domain Name**: Name, zu dem die Daten gehören
- **Type**: Standardtyp der Daten
- **Class**: 1 für IN
- **Time To Live**: Zeit in Sekunden, die der Eintrag von einem DNS Server oder Client aus dem Cache verwendet werden darf.
- **Data Length** Länge in Byte der folgenden Daten
- **Data**: Daten und Kodierung abhängig vom Typ.

Transport

- Üblicherweise werden DNS Anfragen per UDP gestellt
- Zeitüberschreitungen und Wiederholungen werden von den Clients gesteuert.
- Zonentransfers finden über TCP statt (aber nur zu den Secondary DNS Servern)
- DNS Server binden sich üblicherweise auf Port 53
- Der Quellport bei Anfragen ist beliebig.
- Sind mehr als 512 Byte zu übertragen, muß der Client via TCP erneut nachfragen (TC Flags ist in der Antwort gesetzt).

Beispiel

Abfrage eines SRV Records (TTL und Query Class):

```
$ dig -t SRV _xmpp-client._tcp.jabber.org
;; QUESTION SECTION:
;_xmpp-client._tcp.jabber.org.   SRV
;; ANSWER SECTION:
_xmpp-client._tcp.jabber.org.    SRV   5222 jabber.org.
;; AUTHORITY SECTION:
jabber.org.                       NS   ns2.jeremie.com.
jabber.org.                       NS   ns1.jeremie.com.
;; ADDITIONAL SECTION:
jabber.org.                        A   208.245.212.98
ns1.jeremie.com.                   A   208.245.212.29
```

Auflösung von Namen

- Ein Host stellt die Anfrage bei den (bis zu 3) konfigurierten Nameservern (RD ist üblicherweise 1)
- Hat ein DNS Server die Antwort im Cache, sendet er die zugehörigen Daten
- Kann er die Anfrage nicht lokal beantworten, fragt er (nicht rekursiv) einen der konfigurierten ROOT Server.
- Antwort ist eine Liste der Authoritative DNS Server der zugehörigen Zone in den Authority RRs.
- Eine Anfrage bei einem dieser DNS Server führt entweder zum Ergebnis, oder zu einer weiteren Liste von DNS Servern einer untergeordneten Zone.
- Dies wird fortgesetzt, bis ein Server die Anfrage beantworten kann.

Beispiel mit Rekursion

```
$ dig www.heise.de
;; QUESTION SECTION:
;www.heise.de.                  IN   A
;; ANSWER SECTION:
www.heise.de.           74272   IN   A   193.99.144.85
;; AUTHORITY SECTION:
heise.de.               74272   IN   NS  ns.pop-hannover.d
heise.de.               74272   IN   NS  ns.heise.de.
heise.de.               74272   IN   NS  ns2.pop-hannover.
;; ADDITIONAL SECTION:
ns.pop-hannover.de.     10562   IN   A   193.98.1.200
ns2.pop-hannover.net.   75522   IN   A   62.48.67.66
ns.heise.de.            85574   IN   A   193.99.145.37
```

Beispiel ohne Rekursion

```
$ dig +norec www.heise.de @198.41.0.4
;; QUESTION SECTION:
;www.heise.de.                  IN    A
;; AUTHORITY SECTION:
de.                     172800  IN    NS    Z.NIC.de.
de.                     172800  IN    NS    A.NIC.de.
de.                     172800  IN    NS    C.DE.NET.
;; ADDITIONAL SECTION:
A.NIC.de.               172800  IN    A     194.0.0.53
C.DE.NET.               172800  IN    A     208.48.81.43
Z.NIC.de.               172800  IN    A     194.246.96.1
Z.NIC.de.               172800  IN    AAAA  2001:628:453:4905::53
```

Beispiel ohne Rekursion (2)

```
$ dig +norec www.heise.de @194.246.96.1
;; QUESTION SECTION:
;www.heise.de.                  IN   A
;; AUTHORITY SECTION:
heise.de.               86400   IN   NS   ns.heise.de.
heise.de.               86400   IN   NS   ns.pop-hannover.de.
heise.de.               86400   IN   NS   ns2.pop-hannover.ne
;; ADDITIONAL SECTION:
ns.heise.de.            86400   IN   A    193.99.145.37
ns.pop-hannover.de.     86400   IN   A    193.98.1.200
```

Beispiel ohne Rekursion (3)

```
$ dig +norec www.heise.de @193.99.145.37
;; QUESTION SECTION:
;www.heise.de.          IN   A
;; QUESTION SECTION:
;www.heise.de.  IN      A
;; ANSWER SECTION:
www.heise.de.   86400  IN   A   193.99.144.85
;; AUTHORITY SECTION:
heise.de.       86400  IN  NS   ns.pop-hannover.de.
heise.de.       86400  IN  NS   ns2.pop-hannover.net.
heise.de.       86400  IN  NS   ns.heise.de.
;; ADDITIONAL SECTION:
ns.heise.de.    86400  IN   A   193.99.145.37
```

Reverse Lookup

- IP Adressen in Dotted Notation bilden Namen im DNS Verzeichnis
- Die TLD ist arpa, die Second Level Domain ist in-addr.
- Eine IP Adresse a.b.c.d wird in der Zone administriert als **d.c.b.a.in-addr.arpa**
- Der Typ eines in-addr.arpa Eintrages ist PTR, der Wert ist der FQDN des Hosts mit der entsprechenden Adresse.
- Die Auflösung des Namens **d.c.b.a.in-addr.arpa** erfolgt wie für alle FQDN

Beispiel

Der Host `www.heise.de` hat die IP Adresse `193.99.144.85`

```
$ dig -t PTR 85.144.99.193.in-addr.arpa
;; QUESTION SECTION:
;85.144.99.193.in-addr.arpa.          PTR
;; ANSWER SECTION:
85.144.99.193.in-addr.arpa.   PTR   www.heise.de.
;; AUTHORITY SECTION:
144.99.193.in-addr.arpa.      NS    ns.s.plusline.de.
144.99.193.in-addr.arpa.      NS    ns.heise.de.
144.99.193.in-addr.arpa.      NS    ns.plusline.de.
;; ADDITIONAL SECTION:
ns.heise.de.                  A     193.99.145.37
ns.s.plusline.de.             A     212.19.40.14
ns.plusline.de.               A     212.19.48.14
```

Reverse Lookups und CIDR

- Die Segmente eines FQDN geben die Ebenen der Administrativen Kontrolle an.
- Dieser Mechanismus funktioniert nicht beim Reverse Lookup, wenn Netze eine Netzmaske haben, die nicht auf einer Bytegrenze endet.
- RFC2317 beschreibt eine mögliche Konfiguration des Parent DNS Servers, der die Kontrolle an untergeordnete Server weiterleitet.
- Einige DNS Server haben eigene Lösungen, die Delegation zu implementieren (z.B. BIND9 $GENERATE).

Beispiel

Unterhalb der Domain `test.net` mit Adressbereich `1.2.3.0/24` wird eine Domain `sub.test.net` mit Adressen `1.2.3.128/25` angelegt.
Auszug aus dem Zonenfile der `test.net` Domain (RFC1035):

```
$ORIGIN test.net
@     NS      ns.test.net.
ns    A       1.2.3.1
sub   NS      ns.sub.test.net.
```

```
$ORIGIN 3.2.1.in-addr.arpa
1     PTR     ns.test.net.
128   CNAME   128.3.2.1.sub.test.net.
129   CNAME   129.3.2.1.sub.test.net.
```

Beispiel Fortsetzung

Das Zonenfile der `sub.test.net` Domain:

```
$ORIGIN sub.test.net
@       NS    ns.sub.test.net.
ns      A     1.2.3.129
host2   A     1.2.3.130
129     PTR   ns
130     PTR   host2
```

DNS Load Balancing

- Server können nur eine begrenzte Anzahl paralleler Verbindungen bedienen.
- Viele Dienste erfordern/erlauben, daß Verbindungen lange geöffnet bleiben (z.B. IMAP IDLE, vgl. RFC2177).

Die Lösung besteht darin, auf den Clients den Namen (nicht die IP) des Servers zu konfigurieren. Bei jedem Verbindungsaufbau wird der Name in eine Adresse umgewandelt, wobei die TTL des Eintrages beachtet wird. Dadurch kann der Administrator später weitere Server hinzuschalten.

Beispiel: Round Robin DNS

```
$ host www.google.de
 www.google.de      CNAME  www.google.com
 !!! www.google.de CNAME record has zero ttl
 www.google.com     CNAME  www.l.google.com
 !!! www.google.com CNAME record has zero ttl
 www.l.google.com     A    209.85.135.104
 www.l.google.com     A    209.85.135.147
 www.l.google.com     A    209.85.135.99
 www.l.google.com     A    209.85.135.103
```

Bei weiteren Anfragen ist die Reihenfolge der Resource Record möglicherweise anders.

Hypertext Transport Protocol
HTTP

HTTP 0.9

Die Urversion des Hypertext Transport Protocols bietet ein einfaches Request-Response Modell aufbauend auf einer TCP Verbindung.

- Client baut eine TCP Verbindung auf, der Default für den Zielport ist 80.
- Er sendet eine Anfragezeile der Form
  GET Path?Search, abgeschlossen durch ein CRLF (ASCII Codes 13, 10, Carriage Return Line Feed)
- Der Server antwortet mit einem Textdokument mit HTML Markup (`http://www.w3c.org/MarkUp/`).
- Das Ende des Dokuments wird durch Schließen der Verbindung angezeigt.

Aktueller Standard

Aktuell ist HTTP in der Version 1.1 (RFC2616). Die Änderungen zur ersten Version machen es zu einem vielseitig verwendbaren Transport Protokoll.

- Neben Text mit HTML Markup werden andere Datentypen und Formate unterstützt.
- Gegenseitige Authentifizierung der Kommunikationspartner ist möglich.
- Virtual Hosting ermöglicht verschiedene, unabhängige Dienste auf einem Server hinter einer einzigen IP Adresse.
- Für den Nutzer transparente Daten- und Transportkodierungen bieten effiziente Nutzung der Serverresourcen.
- HTTP unterstützt Infrastruktur, die den Einsatz aus privaten Netzen ermöglicht.

SMTP Header (RFC822)

Das Format einer HTTP Nachricht entspricht weitgehend einer E-Mail (SMTP, Simple Mail Transfer Protocol), d.h. nach der Anfragezeile folgen Name-Wert Paare (sog. Header), dann - durch eine Leerzeile getrennt - die Nutzdaten. Zeilenumbrüche bestehen immer aus CRLF (ASCII Codes 13, 10).

- Namen und Werte der Header sind durch Doppelpunkt und Leerzeichen voneinander getrennt.
- Bei den Namen wird nicht zwischen Groß- und Kleinschreibung unterschieden.
- Mehrere Header mit gleichem Namen sind möglich, wenn die Syntax für den Wert eine Folge von durch Komma getrennten Werten vorschreibt.
- Die Reihenfolge von Headern ist nur von Bedeutung, wenn es Header mit gleichem Namen sind.

Header Folding

Lange Zeilen (mehr als 72 Zeichen) sollen zur Verbesserung der Lesbarkeit vermieden werden. Header Zeilen müssen dazu umgebrochen werden. Dazu wird an LWSP (Linear White SPace), d.h. Leerzeichen (SPACE) oder Tabulator (HT) getrennt.

- Enthält der Wert eines Headers ein LWSP, kann es durch CRLF + LWSP ersetzt werden (Folding).
- Beginnt umgekehrt eine Headerzeile mit einem LWSP, ist es die Fortsetzung der vorausgehenden Zeile. Dann muß vor der weiteren Verarbeitung das vorausgehende CRLF entfernt werden.

Beispiel

```
GET /Test HTTP/1.1
Host: localhost:8080
Accept: text/html, text/plain, text/css,
  text/sgml, */*;q=0.01
Accept-Encoding: gzip
Accept-Language: en
User-Agent: Lynx/2.8.6rel.4 libwww-FM/2.14
  SSL-MM/1.4.1 GNUTLS/1.6.2
```

Statuscodes

HTTP benutzt wie SMTP Statuscodes bestehend aus 3 Ziffern mit folgender Interpretation:

Code	Bedeutung
100-199	Information
200-299	Erfolg
300-399	Wiederhole mit anderen Daten
400-499	Client Fehler
500-599	Server Fehler

Hex/Base16 Kodierung (RFC3548)

RFC822 (SMTP) erlaubt nur den (7 Bit) ASCII Zeichensatz. Um Binärdaten in Headern zu übertragen, müssen diese daher auf Zeichenketten aus dem ASCII Alphabet abgebildet werden.

Bei der Hex Kodierung werden die 16 möglichen Werte einer 4 Bit Folge abgebildet auf die 16 Zeichen 0123456789abcdef.

Damit wird jedes Byte dargestellt als 2 ASCII Zeichen.
Beispiel: Die Bytes 127, 62 werden dargestellt als `7F 3E`

Beim Dekodieren wird nicht zwischen Groß- und Kleinschreibung unterschieden.

Base64 Kodierung (RFC3548)

Base16 Kodierung ist bei großen Datenmengen ineffizient, da sie die Datenmenge (gemessen in Byte) verdoppelt. Die Base64 Kodierung ist in diesem Fall um 33% besser.

- Je 6 Bit werden als ein Zeichen kodiert.
- Zielalphabet sind die Zeichen A-Z, a-z, 0-9 und “+”, “/” in dieser Reihenfolge (z.B. $27_{10} = 011011_2 = b_{64}$).
- Da immer je 24 Bit kodiert werden müssen, werden Bytefolgen mit 0 Bits aufgefüllt.
- 6 Füllbits werden durch ’=’ dargestellt.

Beispiel: Die Bytes 127, 62 werden dargestellt als `fz4=`, denn: 127,62 entspricht den Bits 011111 110011 1110`00` `000000`. Die je 6 Bit entsprechen den Zahlen 31(f), 51(z), 56(4) und Füller(=).

Aufbau von Nachrichten

HTTP implementiert ein Request-Response Modell.
Eine Nachricht hat den Aufbau:

```
Anfragezeile/Statuszeile
Headerzeilen
Leerzeile
optionaler Datenblock
```

Eine Anfragezeile hat die Form

```
Methode ' ' URI ' ' HTTP-Version
```

(' ' Leerzeichen, URI, Uniform Resource Identifier)

Eine Statuszeile hat die Form

```
HTTP-Version Status-Code Reason-Phrase
```

HTTP 1.1 Methoden

Folgende Methoden sind standardisiert:

Name	Zweck
OPTIONS	Lesen von Transportoptionen, z.B. `Allow`
GET	Lesen von Daten vom Server
HEAD	Wie GET, Server sendet keinen Datenblock
POST	Senden von Daten zum Server
PUT	Speichern von Daten unter dem URI
DELETE	Löschen von Daten unter dem URI
TRACE	Server sendet den Request als Response
CONNECT	Nur für SSL/TLS Proxies

Ein Server muß nicht alle diese Methoden implementieren, Erweiterungen sind möglich.

Uniform Resource Identifier (vgl. RFC2396)

Die HTTP URL (Uniform Resource Locator) hat die Form:
`"http://" host [ ":" port ] [ path [ "?" query ]]`
Dabei sind Teile in eckigen Klammern "[]" optional.

- **Host**: Hostname des Dienstes.
- **Port**: Portnummer, 80, falls weggelassen.
- **path**: Pfad zur Resource, jeder Pfad startet mit "/"
- **query**: Serverspezifische Parameter, üblicherweise Name "=" Wert Paare, getrennt durch "&" (sog. Formkeys)

IP Adresse statt Hostname ist in URIs zu vermeiden. Falls eine IPv6 Adresse angegeben werden muß, wird sie in eckige Klammern geschrieben.

Schreibweise für URIs

Da URIs auch über andere Transportwege als Computernetze weitergegeben werden, dürfen sie nur druckbare Zeichen enthalten.

Im Pfad einer URI sind mindestens die folgenden Zeichen US-ASCII Zeichen zu ersetzen:

- Codes 0-31 und 127: Control Character
- Code 32: Space
- < > # % ¨: Begrenzer
- { } | \ ˆ [] ‘: Diese Zeichen können von bestimmten Transportmechanismen verändert werden.

Escape Sequenz in URIs

Einige Zeichen haben an bestimmten Stellen der URI eine spezielle Bedeutung und müssen dann ebenfalls ersetzt werden (z.B. im Query Anteil):

- ; / ? : @ & = + $,

Spezielle Zeichen und nicht druckbare Zeichen werden durch ihre Hexadezimaldarstellung, eingeleitet durch ein %-Zeichen, angegeben.

Beispiel: Host `a.b.c`, Port 80, Path `/a_b/c` und Formkeys M=a+b, N="a=b" wird geschrieben als:
`http://a.b.c/a_b/c?M=a%2Bb&N=%22a%3Db%22`

Minimaler HTTP 1.1 Request

Die URL wird vom Client in einen HTTP 1.1 Request umgesetzt. Dazu wird die Serverinformation, d.h. Hostname und Port in den `Host` Header kopiert. Die Anfragezeile enthält im Normalfall als URI nur Path, Query und HTTP-Version. Ausnahme ist der Proxy Request.
Beispiel: Ein `GET` Request auf
`http://localhost:8080/test`
führt zu

```
GET /test HTTP/1.1
Host: localhost:8080
```

Der Header mit Namen `Host` ist bei HTTP 1.1 verbindlich.

HTTP 1.1 Header

In Request und Response sind unterschiedliche Header üblich. Prinzipiell können beiden Nachrichten beliebige Header hinzugefügt werden (sog. extension-header).

Für Requests sind die folgenden Headergruppen standardisiert:

- General Header
- Request Header
- Entity Header

Für Responses entsprechend:

- General Header
- Response Header
- Entity Header

General Header

Ein Auszug aus der Liste der standardisierten General Header:

- **Cache-Control**: Legt fest, was beim Caching der Daten zu beachten ist. (z.B. no-cache, max-age)
- **Connection**: Zeigt an, ob die TCP Verbindung für weitere Anfragen verwendet werden kann (z.B. keep, close)
- **Date**: Zeitpunkt, zu dem die Nachricht erzeugt worden ist.
- **Pragma**: Implementationsspezifische Parameter (z.B. no-cache)
- **Trailer**: Bei Chunked-Encoding können die angegebenen Header am Ende der Nachricht im Datenblock auftauchen.
- **Transfer-Encoding**: Legt fest, wie der Datenblock übertragen wird (z.B. chunked).
- **Via**: Wird von Systemen zwischen Quelle und Ziel eingesetzt, um Schleifen zu entdecken.

Transfer-Encodings

RFC2616 erwähnt folgende Kodierungen:

- **identity**: Die Nachricht wird nicht speziell kodiert.
- **gzip**: Transparente Komprimierung mit Lempel-Ziv Algorithmus.
- **compress**: Unix `compress` LZW Format.
- **deflate**: zlib Format (RFC1950 + RFC1951)
- **chunked**: Der Datenblock besteht aus Länge-Wert kodierten Segmenten.
  - Jedes Segment beginnt mit einer Zeile mit Länge in Hexadezimaldarstellung und optionalem Kommentar
  - Es folgt die angegebene Anzahl Bytes.
  - Das letzte Segment hat die Länge 0
  - Auf das letzte Segment können HTTP Header folgen.

Request Header

Ein Auszug aus der Liste der Request Header:

- **Accept, Accept-Charset, ...**: Liste der Mediatypen, Kodierungen und Sprachen, die der Client akzeptiert
- **Authorization, Proxy-Authorization**: Übergabe von Daten und Anforderung der Authentifizierung.
- **Host**: Servername (eventuell mit Port)
- **If-Match, If-Modified-Since, ...**: Anforderung von Daten nur unter gegebener Bedingung.
- **Max-Forwards**: Maximale Anzahl von Proxies in der Kette.
- **Referer**: URI, von der aus die aktuelle URI angewählt worden ist.
- **TE**: Liste der möglichen Transfer-Encodings
- **User-Agent**: Identifikation des Clients

Response Header

Ein Auszug der Liste der Response-Header:

- **Age**: Alter eines Dokumentes (im Cache)
- **ETag**: Dokumentversion
- **Location**: URI des Dokumentes (benutzt im `201 Created` und z.B. im `302 Redirect`)
- **Proxy-Authenticate, WWW-Authenticate**: Authentifizierungsdaten des Clients
- **Retry-After**: Im `503 Service Unavailable` und bei `3xx Redirect`, wann die Daten verfügbar sein werden.
- **Server**: Identifikation (Typ, Version) des Servers
- **Vary**: Liste der Request-Header, die die Antwort festlegen, nötig für Proxies, um zu entscheiden, ob die Antwort aus dem Cache benutzt wird.

Entity Header

- **Allow**: Methoden, die der Server erlaubt
- **Content-Encoding**: Kodierung, die für die Daten verwendet worden ist (z.B. gzip)
- **Content-Language**: ausgewählte Sprache
- **Content-Length**: Anzahl Bytes im Datenblock, falls nicht `Transfer-Encoding: chunked`.
- **Content-Location**: URI des Dokuments
- **Content-MD5**: Hash der Daten, Prüfsumme des (dekodierten) Datenblocks
- **Content-Range**: gelieferter Bereich in der Antwort `206 Partial Content`
- **Content-Type**: Medientyp
- **Expires**: Wann Daten im Cache veraltet sind
- **Last-Modified**: Zeitpunkt der letzten Änderung

Content-Type Header

- Der Content-Type gibt den Medientyp im Datenblock an.
- Format ist stets `Type "/" Subtype*(";" Parameter)`
- Die standardisierten Medientypen finden sich unter `http://www.iana.org/assignments/media-types/`
- Parameter dienen zur weiteren Festlegung der Interpretation, z.B. `text/plain; charset=utf8`.
- Der Typ `multipart/form-data` (vgl. RFC1867) dient der Übertragung von Formkeys mit Zusatzinformationen wie Zeichensatz oder Medientyp bei Dateiübertragung.

Viele Clients (z.B. MS Windows, Mobiltelefone) benutzen zur Feststellung des Medientyps nicht den Content-Type Header, sondern eventuell vorhandene Dateiheader.

HTTP Proxies

Proxies sind integraler Bestandteil einer HTTP Infrastruktur. Haupteinsatzzwecke sind:

- **Effizienzsteigerung**: Zwischenspeichern von statischen Daten reduziert den Netzwerkverkehr
- **Zugriffskontrolle**: Netzwerkbereiche können nur über Proxies erreicht werden, die Authentifizierung vorschreiben.
- **Protokollierung/Abrechnung**: Proxies können Datenvolumen und Zugriffszeiten protokollieren.
- **Routing**: Zugriff aus privaten Netzen kann über die öffentliche Adresse eines Proxies ermöglicht werden.
- **Sicherheit**: Komplexe Webserver werden durch einfache Proxies vom Internet isoliert.

HTTP Proxies

Man unterscheidet folgende Typen von Proxies:

- **Vorwärtsproxies**: Der Client muß konfiguriert werden, um den Proxy zu benutzen.
- **Rückwärtsproxies**: Dem Client gegenüber verhalten sie sich wie Server. Sie blenden Pfade fremder Server in den eigenen Bereich ein.
- **Transparente Proxies**: Die TCP Verbindung von Clients wird abgefangen und auf den Proxy umgeleitet. Dieser baut bei Bedarf eine eigene Verbindung zum Server auf.

Die Anfragezeile bei Vorwärtsproxies enthält nicht nur den Pfad, sondern die komplette URL.

HTTP Authentifizierung

Soll mittels HTTP auf geschützte Bereiche sowohl auf einem Server als auch hinter einem Proxy zugegriffen werden, erlaubt der Standard, daß Authentifizierungsdaten abgefragt werden.

Wird der Zugriff verweigert, sendet ein Server eine Response mit Statuscode 401, ein Proxy eine Response mit Statuscode 407.

In der Response findet sich der `WWW-Authenticate` oder `Proxy-Authenticate` Header, der festlegt, wie der Client auf den geschützten Bereich zugreifen kann.

Der Client muß dann die Authentifizierungsdaten im `Authorization` bzw. `Proxy-Authorization` Header liefern.

Basic Authentication (RFC2617)

Basic Authentication funktioniert dadurch, daß beim Zugriff auf den geschützten Bereich Benutzername und Kennwort im Klartext übertragen werden.

Findet ein Zugriff ohne gültige Authentifizierung statt, folgt vom Server eine Antwort mit Status 401 und `WWW-Authenticate` Header mit Parametern `basic` und dem Namen des Bereiches.

Der Client wiederholt den Request und sendet den Header `Authorization: Credentials`, wobei Credentials Benutzername ":" Kennwort in Base64 Kodierung ist.

Beispiel Basic Authentication, erster Versuch

```
GET //scripts/Literaturliste.pdf HTTP/1.0
Host: www.comnets.rwth-aachen.de


HTTP/1.1 401 Authorization Required
WWW-Authenticate: Basic
realm=ßcript-downloads"
Content-Type: text/html; charset=iso-8859-1

HTML Fehlertext
```

Beispiel Basic Authentication, erfolgreich

```
GET //scripts/Literaturliste.pdf HTTP/1.0
Host: www.comnets.rwth-aachen.de
Authorization: Basic dXNlcjpwYXNzd29yZA==


HTTP/1.1 200 OK
Content-Length: 34544
Content-Type: application/pdf

PDF Dokument
```

Digest Access Authentication (RFC2617)

Der entscheidende Nachteil der Basic-Authentication ist, daß jeder, der die Datenübertragung abhört, Benutzernamen und Kennwort erfährt. Dies wird bei der Digest-Authentication vermieden.

Der `WWW-Authenticate` oder `Proxy-Authenticate` Header hat die Form: `Digest Challenge`, wobei Challenge eine Folge von Name "=" Wert Paaren ist, die durch "," getrennt werden.

Die Antwort hat die Form `Digest Response`, wobei Response dasselbe Format wie Challenge hat.

Challenge Parameter

- **realm**: Name des Sicherheitsbereiches
- **domain**: Liste von URI Präfixen, für die die Credentials gelten
- **nonce**: Eindeutige Challenge
- **opaque**: Wert, der vom Client zum Server zurückgeschickt wird
- **stale**: Zeigt an, daß der vorherige Nonce abgelaufen ist.
- **algorithm**: Zu verwendender Hash Algorithmus, z.B. MD5, SHA1
- **qop**: angebotene Sicherheitsstufen, z.B. Authentizität (auth), Integrität (auth-int)
- **auth-param**: z.Zt nicht benutzt

Response Parameter

- **username**: Name, unter dem der Client sich anmeldet
- **realm, nonce, algorithm, opaque**: die Werte der Challenge.
- **uri**: URI, die zur Challenge geführt hat (die Anfragezeile könnte von einem Proxy verändert worden sein)
- **response**: Hash, der aus Nonce, Benutzername, Kennwort und möglicherweise weiteren Bestandteilen der Nachricht berechnet wurde.
- **cnonce**: Zufälliger Text des Clients, der in den Hash einbezogen wird und Chosen Plaintext Angriffe verhindert.
- **qop**: gewählte Sicherheitsstufe
- **nonce-count**: Zähler, wie oft der nonce in Requests verwendet worden ist
- **auth-param**: z.Zt. nicht benutzt

Digest Auth Beispiel

```
GET /apache2-default/ HTTP/1.1
User-Agent: Mozilla/5.0 (X11; U; Linux i686; en-US)
Host: localhost
Accept: text/html;q=0.9,text/plain;q=0.8,*/*;q=0.5
Accept-Language: en
Accept-Encoding: gzip,deflate
Accept-Charset: ISO-8859-1,utf-8;q=0.7,*;q=0.7
Connection: close
If-Modified-Since: Sat, 20 Nov 2004 20:16:24 GMT
Cache-Control: max-age=0
```

Digest Auth Beispiel

```
HTTP/1.1 401 Authorization Required
Date: Sun, 09 Dec 2007 15:07:31 GMT
Server: Apache/2.2.6 (Debian)
WWW-Authenticate: Digest realm="my-realm",
  nonce="6by31ttABAA=1b869666ab4d0c05c785475d376797a
  algorithm=MD5, qop="auth"
Content-Length: 475
Connection: close
Content-Type: text/html; charset=iso-8859-1

475 Bytes Fehlertext
```

```
GET /apache2-default/ HTTP/1.1
User-Agent: Mozilla/5.0 (X11; U; Linux i686; en-US)
Host: localhost
Accept: text/html;q=0.9,text/plain;q=0.8,*/*;q=0.5
Accept-Language: en
Accept-Encoding: gzip,deflate
Accept-Charset: ISO-8859-1,utf-8;q=0.7,*;q=0.7
Connection: close
If-Modified-Since: Sat, 20 Nov 2004 20:16:24 GMT
Cache-Control: max-age=0
Authorization: Digest username="username",
  realm="my-realm",
  nonce="6by31ttABAA=1b869666ab4d0c05c785475d376797ac126
  uri="/apache2-default/", algorithm=MD5,
  response="6f8e48f7d00453d12f63405b53984537",
  qop=auth, nc=00000001, cnonce="de371d3080a00b58"
```

Cookies

HTTP bietet im Protokoll keine Möglichkeit, Zustandsinformationen zwischen verschiedenen Requests zu transportieren. Zwar gibt es eine Vielzahl von Ansätzen, dieses Problem zu lösen, die jedoch alle anwendungsabhängig sind oder nur eingeschränkte Möglichkeiten bieten (z.B. HTML Hidden Felder oder Session ID in der URL).

Netscape hat daher HTTP um sogenannte Cookies erweitert:

- Die originale Spezifikation findet sich unter `http://wp.netscape.com/newsref/std/cookie_spec.h`
- RFC2109 erweitert den Vorschlag von Netscape so, daß bisherige Server und Clients interoperieren können.
- RFC2965 führt einen neuen Header ein, um die Zustandsinformation zu speichern.

Austausch von Cookies

Cookies werden in der Response vom Server im “Set-Cookie” oder “Set-Cookie2” (RFC2965) Header gesetzt. Sie bestehen aus Segmenten, die durch Semikolon voneinander getrennt sind. Erstes Segment ist ein Name “=” Wert Paar, das den Namen des Cookies festlegt.

In weiteren Requests sendet der Client das Cookie im “Cookie” Header an den Server zurück, sofern im Cookie enthaltene Bedingungen erfüllt sind.

Der Server kann über das Cookie verschiedene Requests demselben Client zuordnen.

Felder im Cookie

- **Comment**: Für Menschen lesbarer Kommentar zum Cookie
- **Domain**: Domain (oder ein Suffix beginnend mit .), für den das Cookie gilt.
- **Max-Age**: Nach dieser Zeit in Sekunden soll der Client das Cookie nicht mehr benutzen.
- **Path**: Pfad (oder ein Präfix), für den das Cookie gilt. Nur für URIs mit einem Pfad unterhalb des Attributes wird das Cookie benutzt.
- **Secure**: Versende das Cookie nur bei ausreichend hoher Sicherheit (z.B. bei verschlüsselter Verbindung).
- **Version**: Version des Cookies (verbindlich = 1 für RFC2109, nicht benutzt für Netscape)

RFC2965 benutzt einige weitere Felder. Version ist ebenfalls 1.

Verarbeitung auf Clientseite

- Ist **Domain** nicht angegeben, wird der FQDN der URI benutzt.
- Ist **Max-Age** nicht angegeben, wird das Cookie bei Beenden des Clients verworfen.
- Der Standardwert für **Path** ist der Path der aktuellen URI bis zum letzten “/”.
- Ein fehlendes **Secure** wird als nicht gesetzt angenommen.

Cookies werden vom Client verworfen, wenn

- **Path** kein Präfix des aktuellen Path ist.
- der Host nicht zur **Domain** gehört.
- **Domain** keinen eingeschlossenen Punkt enthält.
- Falls das Präfix, das zusammen mit **Domain** den FQDN des Hosts ergibt, einen Punkt enthält.

Beispiel

```
GET http://www.google.de/ HTTP/1.0
Host: www.google.de


HTTP/1.0 200 OK
Content-Type: text/html; charset=ISO-8859-1
Set-Cookie:
PREF=ID=112381d8e7dc6b1e:TM=1197301885:...;
  path=/; domain=.google.de
Via: 1.0 localhost.localdomain:3128
(squid/2.6.STABLE17)
Proxy-Connection: close
Connection: close

...HTML Text...
```