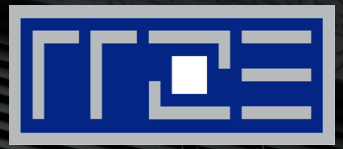
REGIONALES RECHENZENTRUM ERLANGEN [RRZE]



Handeln mit Adressen
ARP, DHCP, DNS

RRZE-Netzwerkausbildung – Praxis der Datenkommunikation

30.11.2016, Jochen Reinwand, RRZE

ORGANISATORISCHES

- Die Vorträge im Überblick
- Andere Vortragsreihen des RRZE
- Ablageorte Vortragsfolien
- RRZE-Veranstaltungskalender / Mailingliste abonnieren
- Themenvorschläge & Anregungen

Dieser Vortrag wird aufgezeichnet.

Die ersten beiden Sitzreihen befinden sich im Kameraradius.

Weitere Vorträge im Rahmen der „Netzwerkausbildung“

- immer mittwochs (ab 14 c.t.) in Raum 2.049 am RRZE

19.10.2016 – Modelle, Begriffe, Mechanismen
26.10.2016 – Lokale Netze: Switching, Routing, Strukturierung
09.11.2016 – Troubleshooting von WLAN- und VPN-Problemen
23.11.2016 – TCP-/IP-Troubleshooting
30.11.2016 – Handeln mit Adressen – ARP, DHCP, DNS
07.12.2016 – IP-FAU-6 (Teil 1)
14.12.2016 – IP-FAU-6 (Teil 2)
11.01.2017 – Elementare Sicherheitsmaßnahmen: Firewall und Netzzugriff
18.01.2017 – Anschluss von Wohnheimnetzen
25.01.2017 – Traffic Engineering: Proxy, NAT
01.02.2017 – Routingprotokolle
08.02.2017 – E-Mail-Grundlagen

Andere Vortragsreihen des RRZE

Campustreffen

- immer donnerstags ab 15 Uhr c.t.
- vermittelt Informationen zu den Dienstleistungen des RRZE
- befasst sich mit neuer Hard- & Software, Update-Verfahren sowie Lizenzfragen
- ermöglicht den Erfahrungsaustausch mit Spezialisten

Systemausbildung „Grundlagen und Aspekte von Betriebssystemen und System-nahen Diensten”

- immer mittwochs ab 14 Uhr c.t. (in den Sommersemestern)
- Ergänzung zur Netzwerkausbildung “Praxis der Datenkommunikation”
- führt in den grundsätzlichen Aufbau eines Systems sowie eingesetzte Techniken und Komponenten ein
- richtet sich primär an alle Interessierten (Studierende & Beschäftigte)

Vortragsfolien & Vortragsaufzeichnung

Die Vortragsfolien werden nach der Veranstaltung auf der Webseite des RRZE abgelegt:
http://www.rrze.fau.de/ausbildung/veranstaltungsreihen/netzwerkausbildung.shtml

Die meisten Vorträge des RRZE werden aufgezeichnet und können nach der Veranstaltung vom Videoportal der FAU heruntergeladen werden:
www.fau.tv

RRZE-Veranstaltungskalender & Mailinglisten

- Kalender abonnieren oder bookmarken
  - Alle Infos hierzu stehen auf der Webseite des RRZE unter: http://www.rrze.fau.de/news/kalender.shtml

- Mailingliste abonnieren
  - Wöchentliche Terminhinweise werden zusätzlich an die Mailingliste RRZE-Aktuelles gesendet.
  - Auch diese Liste kann man abonnieren: https://lists.fau.de/mailman/listinfo/rrze-aktuelles

Themenvorschläge & Anregungen

Themenvorschläge und Anregungen nehmen wir gerne entgegen!

Bitte schreiben Sie uns einfach eine E-Mail an: rrze-zentrale@fau.de (Betreff: Netzwerkausbildung)

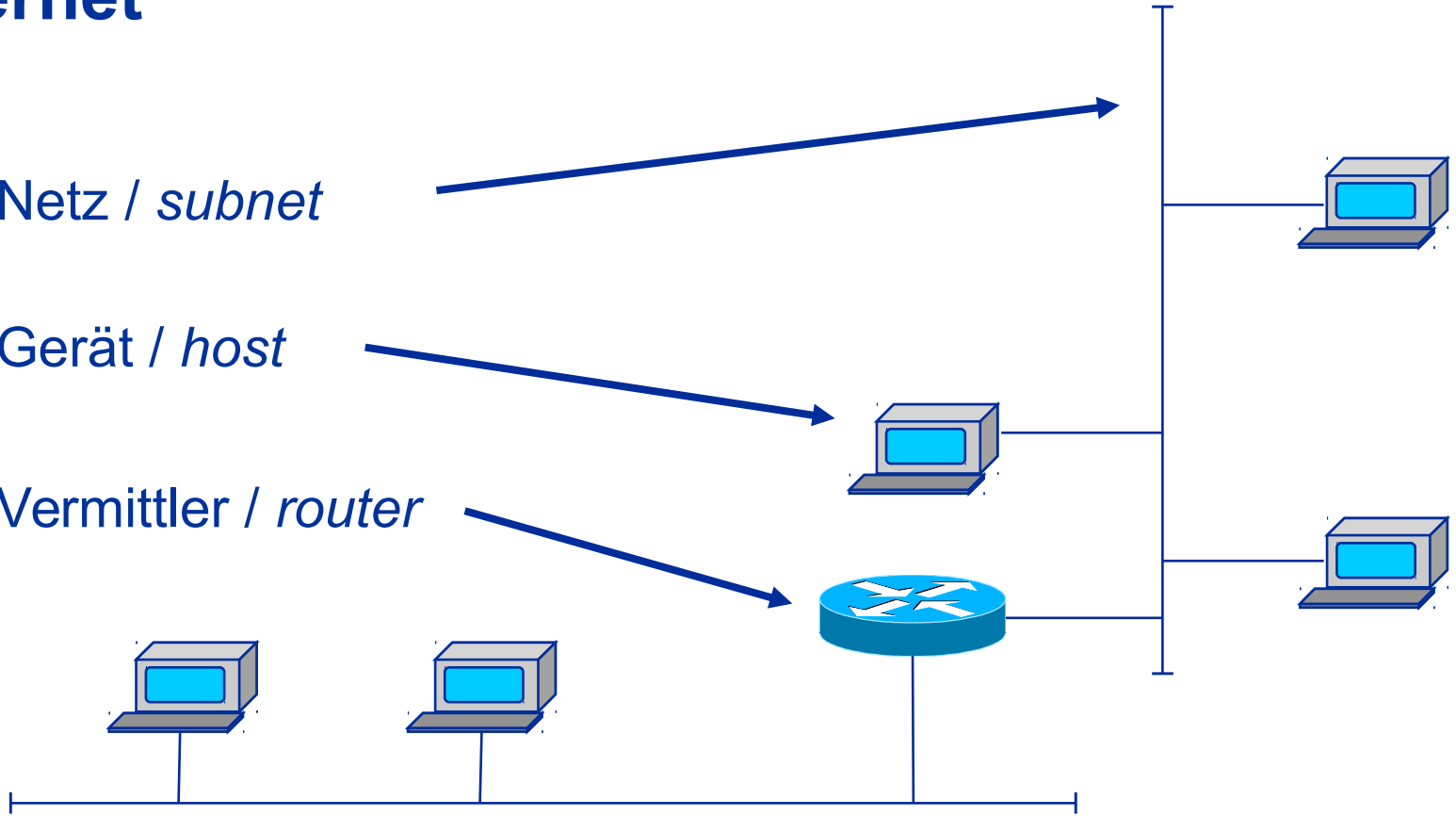
Gliederung

- Grundlagen und Theorie
  - Internet und Ethernet
- ARP
  - Ablauf
  - Erweiterungen
  - Sicherheit
  - IPv6
- DHCP
  - Ablauf
  - Windows, Linux
  - Sicherheit
- DNS
  - „Telefonbuch“
  - Einträge
  - Sicherheit
  - Werkzeuge

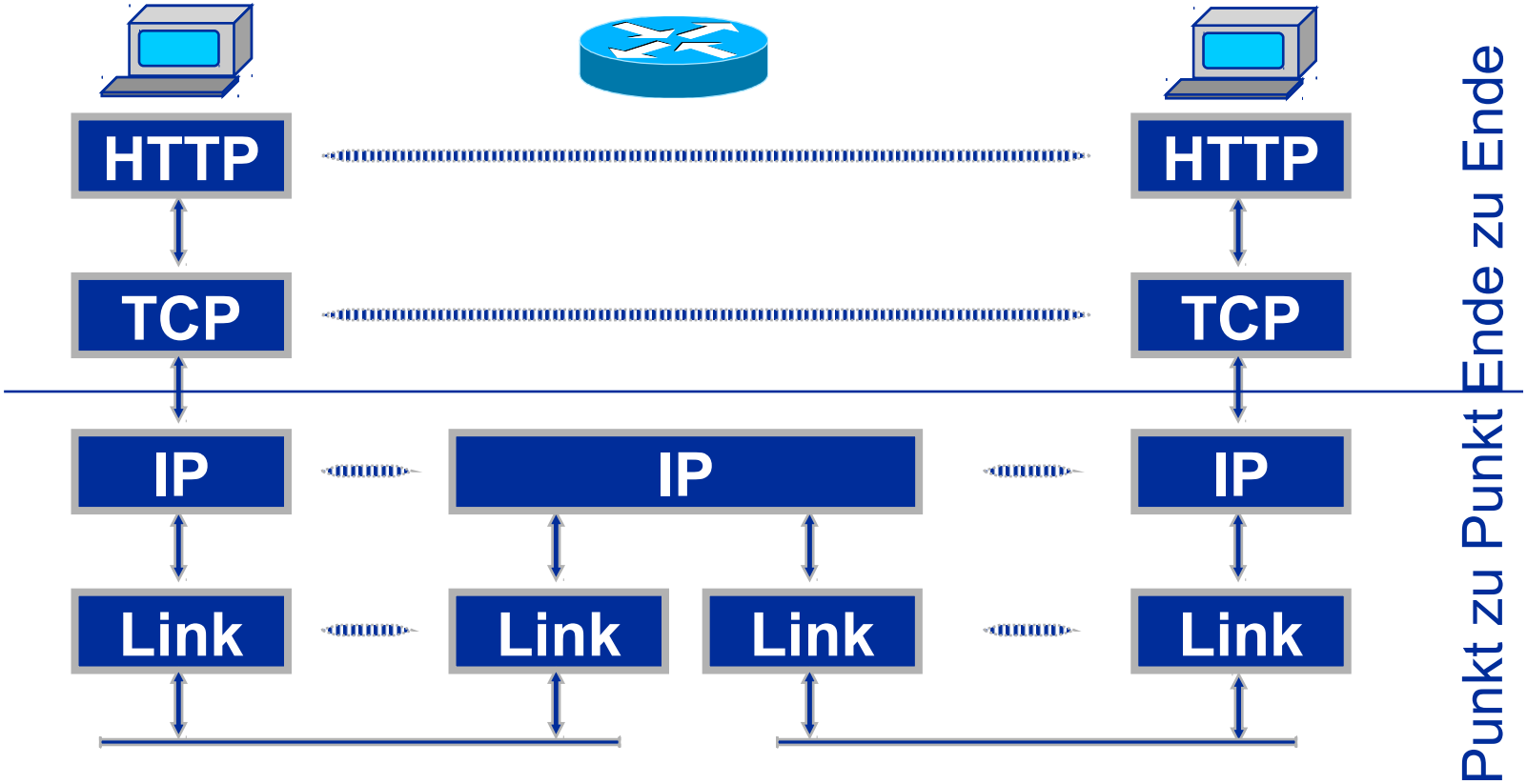
Internet und Ethernet

Internet

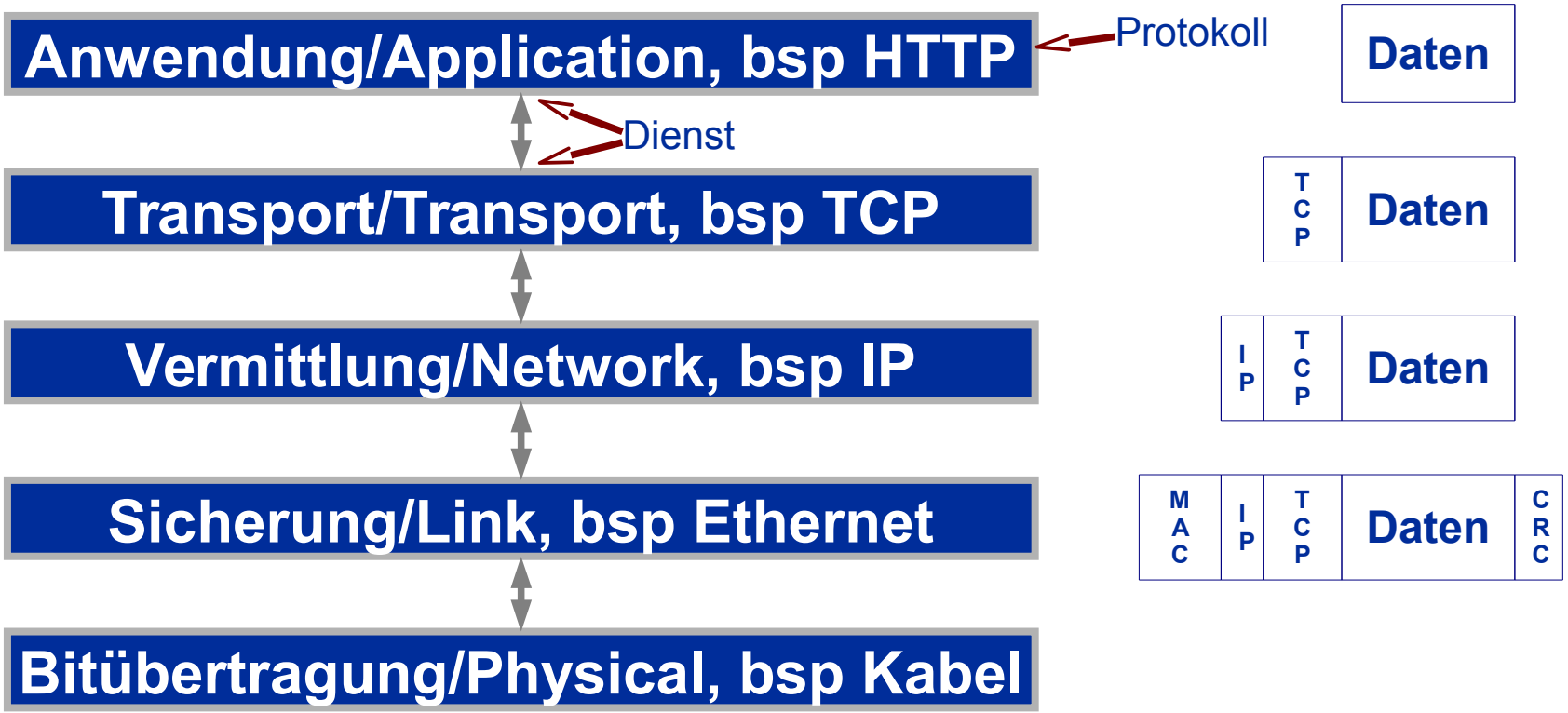
- Netz / *subnet*
- Gerät / *host*
- Vermittler / *router*



TCP/IP Schichtenmodell



TCP/IP Schichtenmodell



IP-Adressen – CIDR

131.188.79.246 im Netz 131.188.79.0/24

131.	188.	79.	246
10000011.	10111100.	01001111.	11110110
24 Bit Netz-Id			**8** Bit Host-Id

131.188.16.136 im Netz 131.188.16.128/26

131.	188.	16.	136
10000011.	10111100.	00010000. 10	001000
26 Bit Netz-Id			**6** Bit Host-Id

Nützliches Tool: http://jodies.de/ipcalc

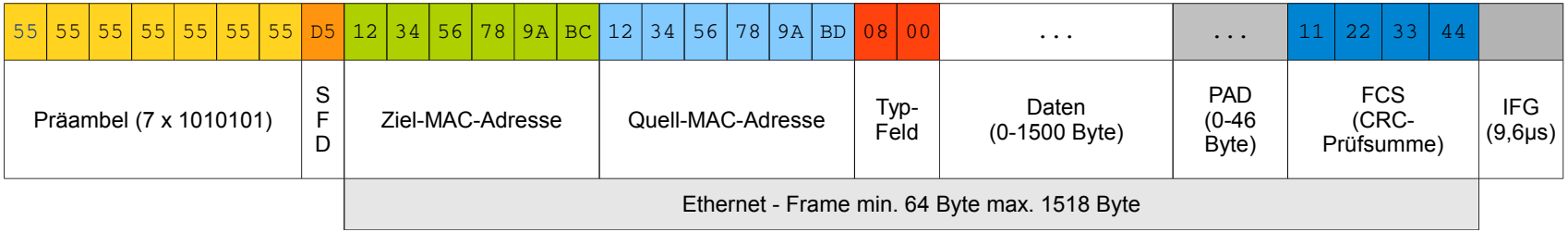
IPv4-Adressen

CIDR-Adressblock	Beschreibung	RFC
0.0.0.0/8	Aktuelles Netzwerk (nur als Quelladresse gültig)	RFC 1700
10.0.0.0/8	Privates Netzwerk	RFC 1918
14.0.0.0/8	Öffentliches Datennetzwerk	RFC 1700
39.0.0.0/8	Reserviert	RFC 1797
127.0.0.0/8[1)]	Localnet	RFC 3330
128.0.0.0/16	Reserviert	
169.254.0.0/16	Zeroconf	RFC 3927
172.16.0.0/12	Privates Netzwerk	RFC 1918
191.255.0.0/16	durch IANA reserviert	
192.0.0.0/24	durch IANA reserviert	
192.0.2.0/24	Dokumentation und Beispielcode (*TEST-NET*)	RFC 3330
192.88.99.0/24	6to4-Anycast-Weiterleitungspräfix	RFC 3068
192.168.0.0/16	Privates Netzwerk	RFC 1918
198.18.0.0/15	Netzwerk-Benchmark-Tests	RFC 2544
223.255.255.0/24	Reserviert	RFC 3330
224.0.0.0/4	Multicasts (früheres Klasse-D-Netzwerk)	RFC 3171
240.0.0.0/4	Reserviert (früheres Klasse-E-Netzwerk)	RFC 1700
255.255.255.255[2)]	Broadcast	

Ethernet-Adressen

- MAC-Adressen
- 6 Byte `12-34-56-78-9a-bc`
  `12:34:56:78:9a:bc`
  `1234:5678:9abc`
- `12-34-56-xx-xx-xx` — Hersteller
- `yy-xx-xx-xx-xx-xx` (yy: LSB=1) — Broadcast/Multicast
  `ff-ff-ff-ff-ff-ff` — Broadcast
  `01-00-5e-xx-xx-xx` — IPv4-Multicast
  `33-33-xx-xx-xx-xx` — IPv6-Multicast
- `yy-xx-xx-xx-xx-xx` (yy: 2. Bit=1) — Lokal administriert

Ethernet-Paket

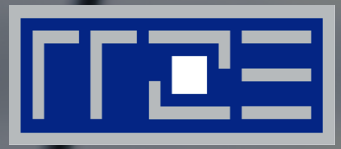


SFD Start Frame Delimiter
PAD Padding
FCS Frame Check Sequence
IFG Inter Frame Gap

Typ-Feld	Protokoll
0x0800	Internet Protocol Version 4 (IPv4)
0x0806	Address Resolution Protocol (ARP)
0x8035	Reverse Address Resolution Protocol (RARP)
0x8100	VLAN Tag
0x8138	Novell
0x86DD	Internet Protocol Version 6 (IPv6)

Vereinfachte Darstellung!

ARP



Ablauf, Erweiterungen, Sicherheit, IPv6

ARP (Address Resolution Protocol)

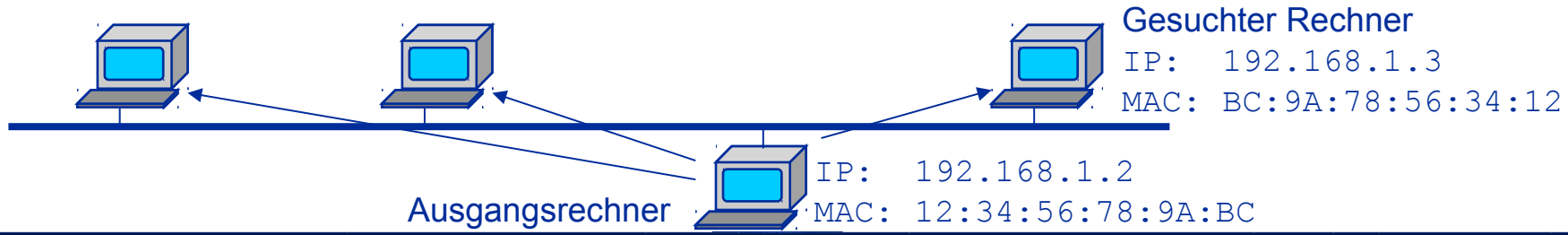
- *Address Resolution Protocol*
- Welche MAC gehört zu einer IP-Adresse (im selben Subnetz)?
- Gelöst per *Broadcast*
- *ARP-Request* wird gesendet an FF:FF:FF:FF:FF:FF

  Quell-MAC: `12:34:56:78:9A:BC`

  Quell-IP: `192.168.1.2`

  Ziel-MAC: `???`

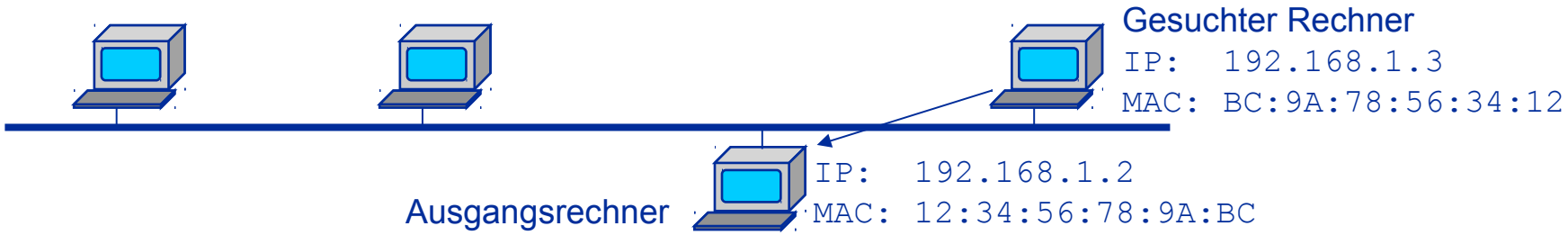
  Ziel-IP: `192.168.1.3`



ARP (Address Resolution Protocol)

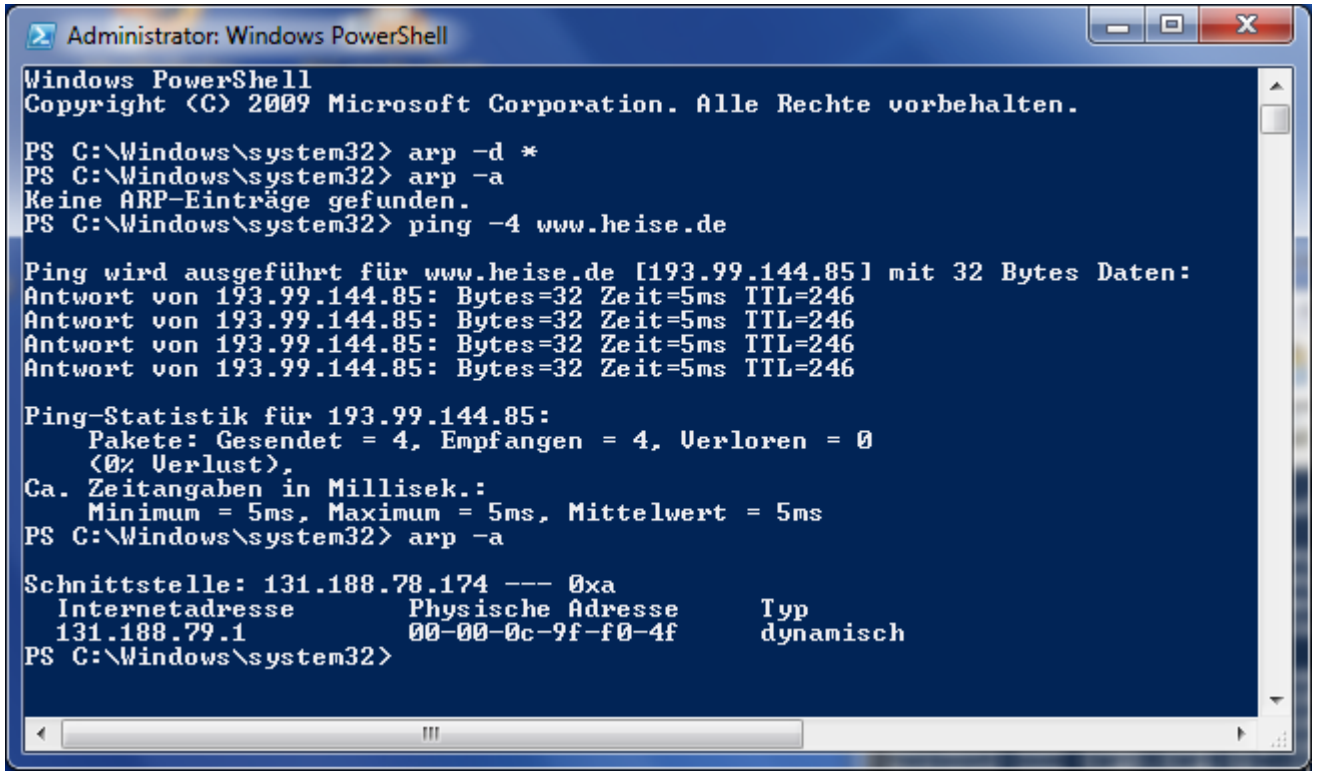
- *ARP-Reply* wird gesendet an anfragende MAC

  Quell-MAC: `BC:9A:78:56:34:12`
  Quell-IP: `192.168.1.3`
  Ziel-MAC: `12:34:56:78:9A:BC`
  Ziel-IP: `192.168.1.2`

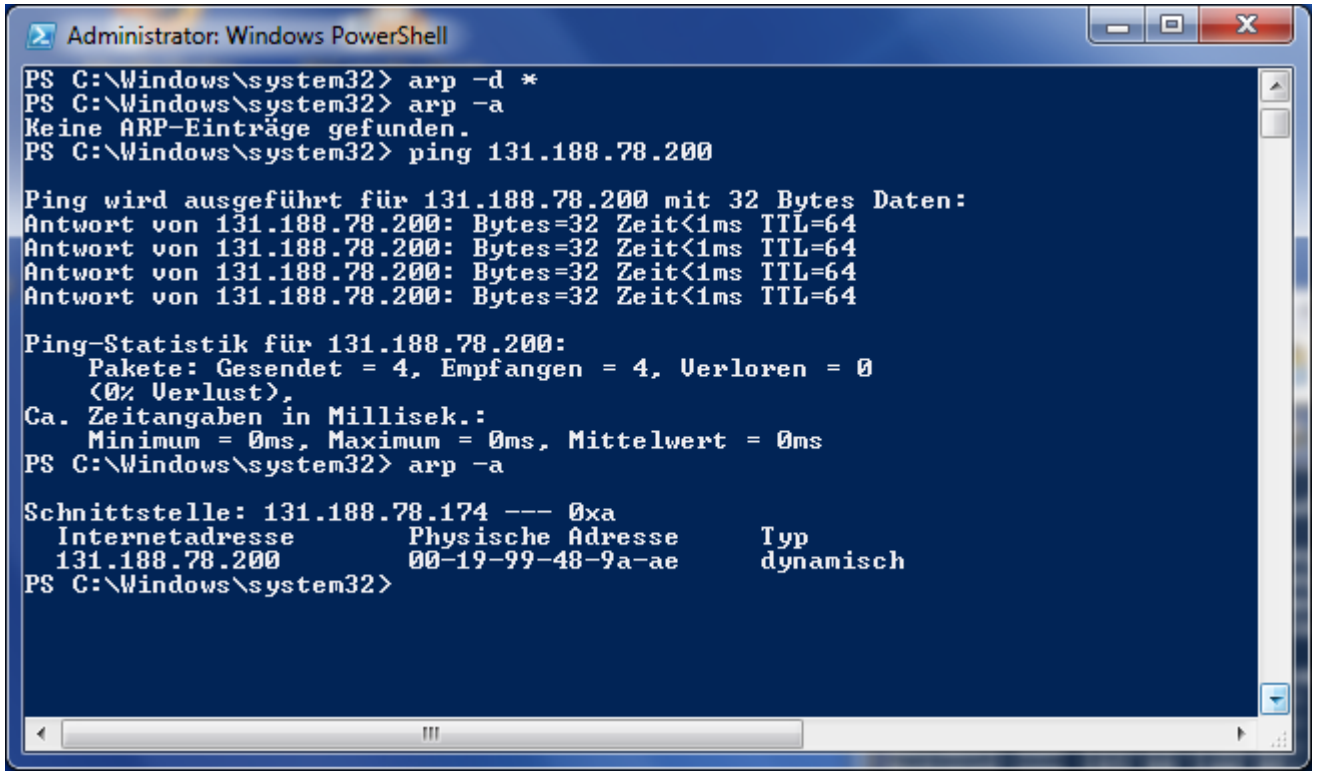


- Informationen landen auf beiden Rechnern im *ARP-Cache*
- Auch andere Stationen können Informationen (über anfragenden Rechner) in ARP-Cache speichern

ARP – Windows


Administrator: Windows PowerShell
Windows PowerShell
Copyright (C) 2009 Microsoft Corporation. Alle Rechte vorbehalten.
PS C:\Windows\system32> arp -d *
PS C:\Windows\system32> arp -a
Keine ARP-Einträge gefunden.
PS C:\Windows\system32> ping -4 www.heise.de
Ping wird ausgeführt für www.heise.de [193.99.144.85] mit 32 Bytes Daten:
Antwort von 193.99.144.85: Bytes=32 Zeit=5ms TTL=246
Antwort von 193.99.144.85: Bytes=32 Zeit=5ms TTL=246
Antwort von 193.99.144.85: Bytes=32 Zeit=5ms TTL=246
Antwort von 193.99.144.85: Bytes=32 Zeit=5ms TTL=246
Ping-Statistik für 193.99.144.85:
Pakete: Gesendet = 4, Empfangen = 4, Verloren = 0
(0% Verlust),
Ca. Zeitangaben in Millisek.:
Minimum = 5ms, Maximum = 5ms, Mittelwert = 5ms
PS C:\Windows\system32> arp -a
Schnittstelle: 131.188.78.174 --- 0xa
Internetadresse Physische Adresse Typ
131.188.79.1 00-00-0c-9f-f0-4f dynamisch
PS C:\Windows\system32>

ARP – Windows


Administrator: Windows PowerShell
PS C:\Windows\system32> arp -d *
PS C:\Windows\system32> arp -a
Keine ARP-Einträge gefunden.
PS C:\Windows\system32> ping 131.188.78.200
Ping wird ausgeführt für 131.188.78.200 mit 32 Bytes Daten:
Antwort von 131.188.78.200: Bytes=32 Zeit<1ms TTL=64
Antwort von 131.188.78.200: Bytes=32 Zeit<1ms TTL=64
Antwort von 131.188.78.200: Bytes=32 Zeit<1ms TTL=64
Antwort von 131.188.78.200: Bytes=32 Zeit<1ms TTL=64
Ping-Statistik für 131.188.78.200:
Pakete: Gesendet = 4, Empfangen = 4, Verloren = 0
(0% Verlust),
Ca. Zeitangaben in Millisek.:
Minimum = 0ms, Maximum = 0ms, Mittelwert = 0ms
PS C:\Windows\system32> arp -a
Schnittstelle: 131.188.78.174 --- 0xa
Internetadresse Physische Adresse Typ
131.188.78.200 00-19-99-48-9a-ae dynamisch
PS C:\Windows\system32>

ARP – Spezialfälle

- Gratuitous („unaufgefordertes“) ARP
  - Host teilt eigene MAC-Adresse unaufgefordert durch ARP-Anfrage mit seiner IP-Adresse als Quelle und Ziel mit
  - Fehleranalyse (es darf keine Antwort kommen!)
  - Hardware-Änderungen / Booten
  - High Availability („Umbiegen“ auf Standby-Maschine)
  - Mobile IP
- Proxy ARP
  - Router beantwortet ARP-Anfragen für Hosts aus anderen Netzen
  - „Routen ohne Wissen“
- Reverse ARP (RARP)
  - MAC-Adresse → IP-Adresse
  - Anderer Anwendungsbereich
  - Ähnelt DHCP und wird kaum noch verwendet

ARP – Sicherheit

- ARP-Spoofing
  - Angriffe
    - Sniffing
    - Man-In-The-Middle
  - Sinnvolle Anwendungen
    - Verkehrsanalyse zwischen zwei beliebigen Hosts
    - Hochverfügbarkeitscluster
  - Gegenmaßnahmen
    - Verschlüsselung (mit Zertifikaten!)
    - Kontrolle und Überwachung der Infrastruktur (arpwatch, Intrusion Detection Systeme)
    - Proprietäre Lösungen (z.B. via DHCP-Snooping)

ARP – IPv6

- ARP nicht verwendet in IPv6
- *Neighbor Discovery Protocol* (NDP)
  - Basiert auf ICMPv6
  - Verwendet IPv6 statt MAC-Adressen (Link-Local-Unicast und Multicast)
  - Automatische Adressvergabe
  - Konfiguration der Default-Routen
  - „Bruch“ des Schichtenmodells verkleinert

DHCP

Ablauf, Windows, Linux, Sicherheit

DHCP

- Dynamic Host Configuration Protocol (RFC 2131)
- Automatische Konfiguration für Netzwerkteilnehmer
- RARP → BOOTP → DHCP
- Optionen:
  - IP-Adresse, Netzmaske, Router, Domain-Name-Server
  - Viele weitere Möglichkeiten
  - http://www.iana.org/assignments/bootp-dhcp-parameters
- UDP
  - Port 67 – BOOTP Server – Anfrage
  - Port 68 – BOOTP Client – Antwort

DHCP – Normaler Ablauf

- DHCPDISCOVER

  `0.0.0.0 (12:34:56:78:9A:BC) → 255.255.255.255 (FF:FF:FF:FF:FF:FF)`

- DHCPOFFER

  `10.188.12.19 (BC:9A:78:56:34:12) → [192.168.1.10] (12:34:56:78:9A:BC)`

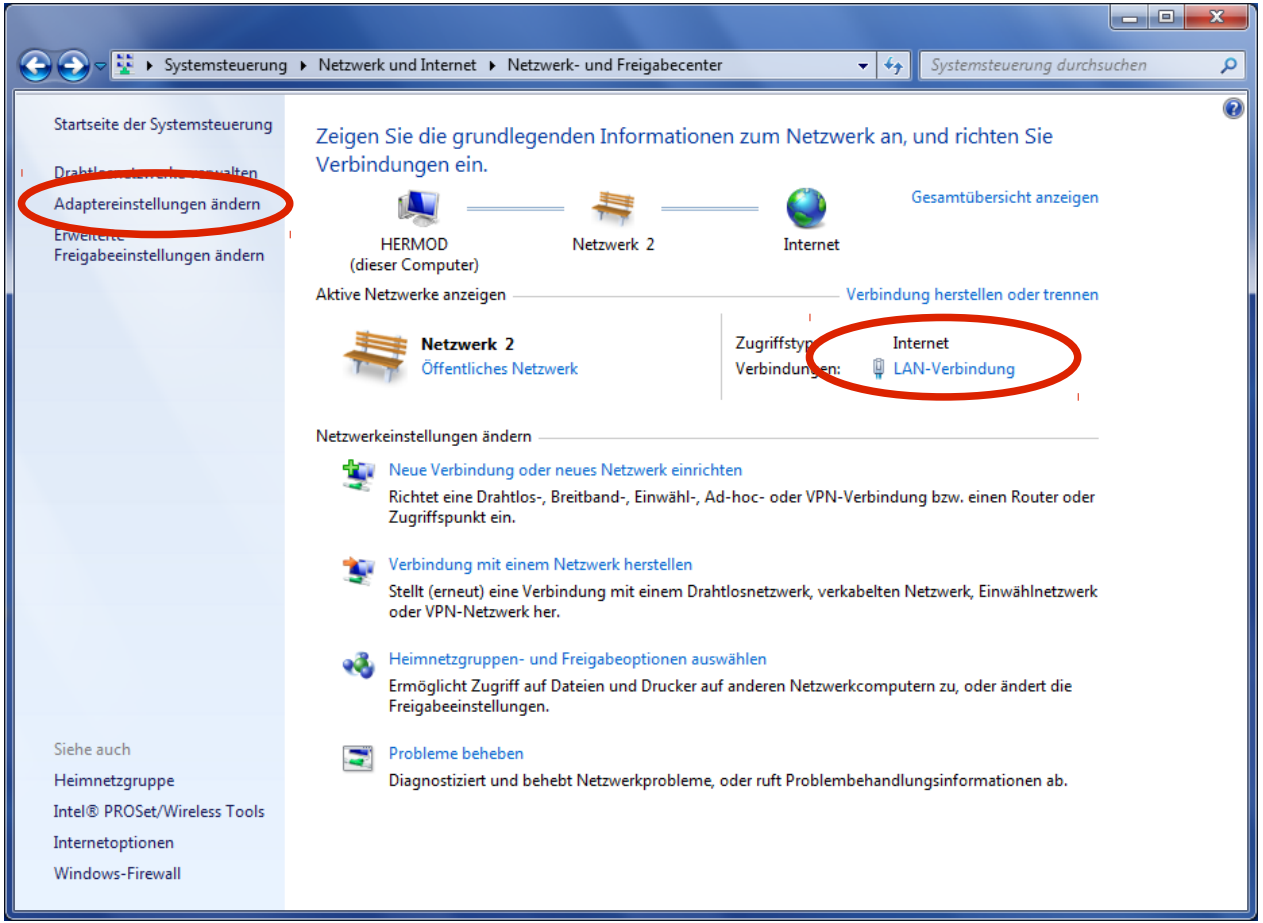
- DHCPREQUEST

  `0.0.0.0 (12:34:56:78:9A:BC) → 255.255.255.255 (FF:FF:FF:FF:FF:FF)`

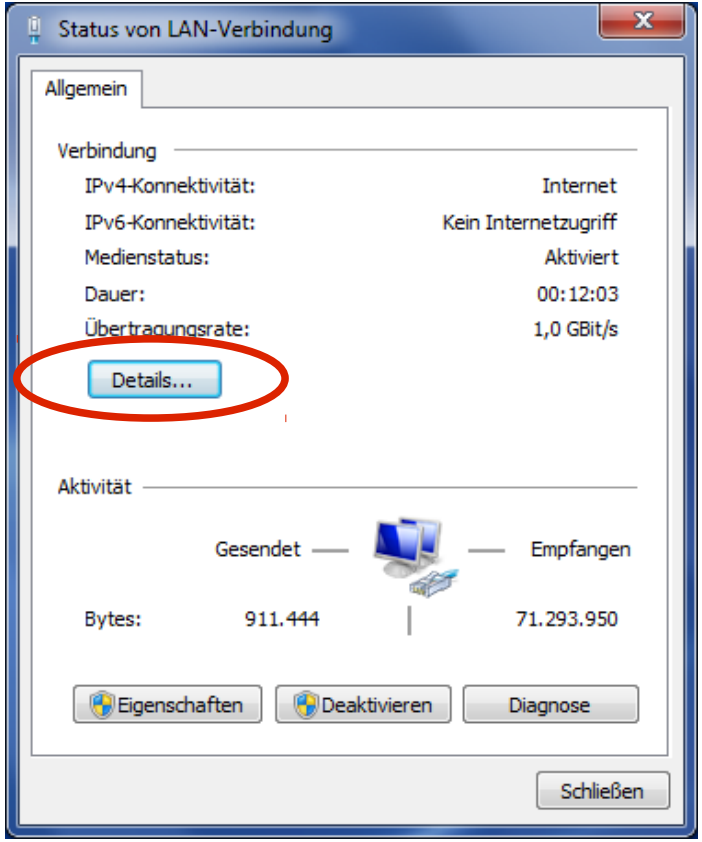
- DHCPACK

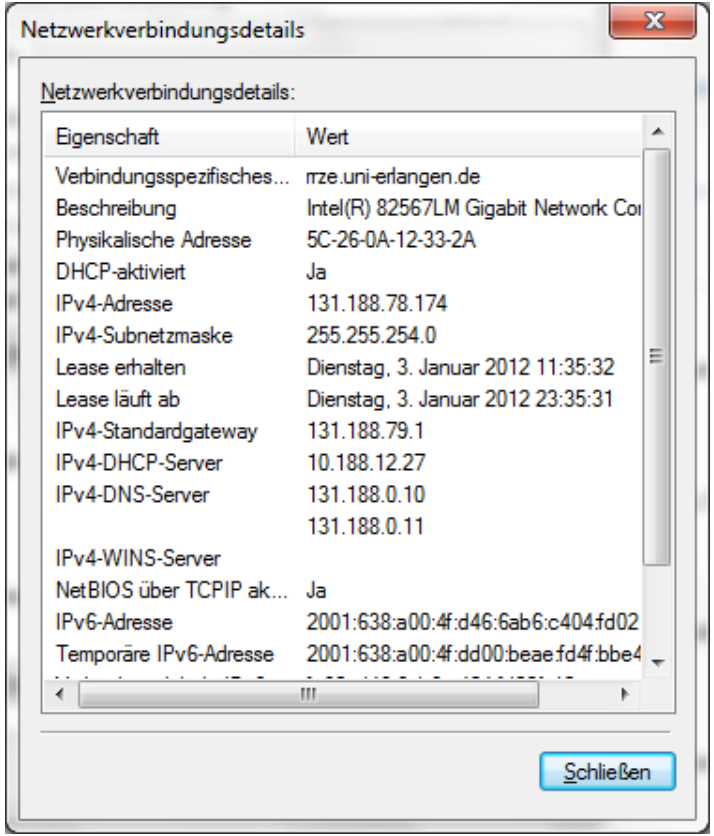
  `10.188.12.19 (BC:9A:78:56:34:12) → [192.168.1.10] (12:34:56:78:9A:BC)`

DHCP
Windows



DHCP – Windows





DHCP – Linux

- Verschiedene Varianten der Netzwerkkonfiguration!
  Nicht nur wegen unterschiedlichen Distributionen!
- Im Wesentlichen zwei Tools im Hintergrund:
  - dhcpcd (DHCP Client Daemon)
    Aktuelle Lease-Informationen gibt es beispielsweise hier:
    `/var/lib/dhcpcd/dhcpcd-eth0.info`
  - dhclient (Client des Internet Systems Consortium)
    Aktuelle Lease-Informationen gibt es beispielsweise hier:
    `/var/lib/dhcp/dhclient.leases`
- In der Regel heute moderne grafische Werkzeuge
- Oft läuft der NetworkManager im Hintergrund
  - Kommandozeilen-Tool: `nm-tool`

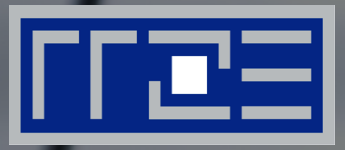
DHCP – Sicherheit

- DHCP basiert auf Broadcasts von Rechnern, die keine Kenntnis von ihrer Umgebung haben
- Verschiedene Angriffsszenarien
- Abwehr ähnlich schwierig wie bei ARP
- Kontrolle und Überwachung der gesamten Infrastruktur
- Meist proprietäre Lösungen (Cisco DHCP Snooping)
- Satire: Peg DHCP (http://de.wikipedia.org/wiki/Peg_DHCP)

DHCP an der FAU

- Oft lokal „vor Ort“ betrieben
- DHCP-Dienst des RRZE
  - Basiert auf DHCP-Relay (= Router)
  - Administration:
    - NEU: dhcp@fau.de
    - alt: dhcp-admin@rrze.fau.de

DNS



„Telefonbuch“, Einträge, Sicherheit, Werkzeuge

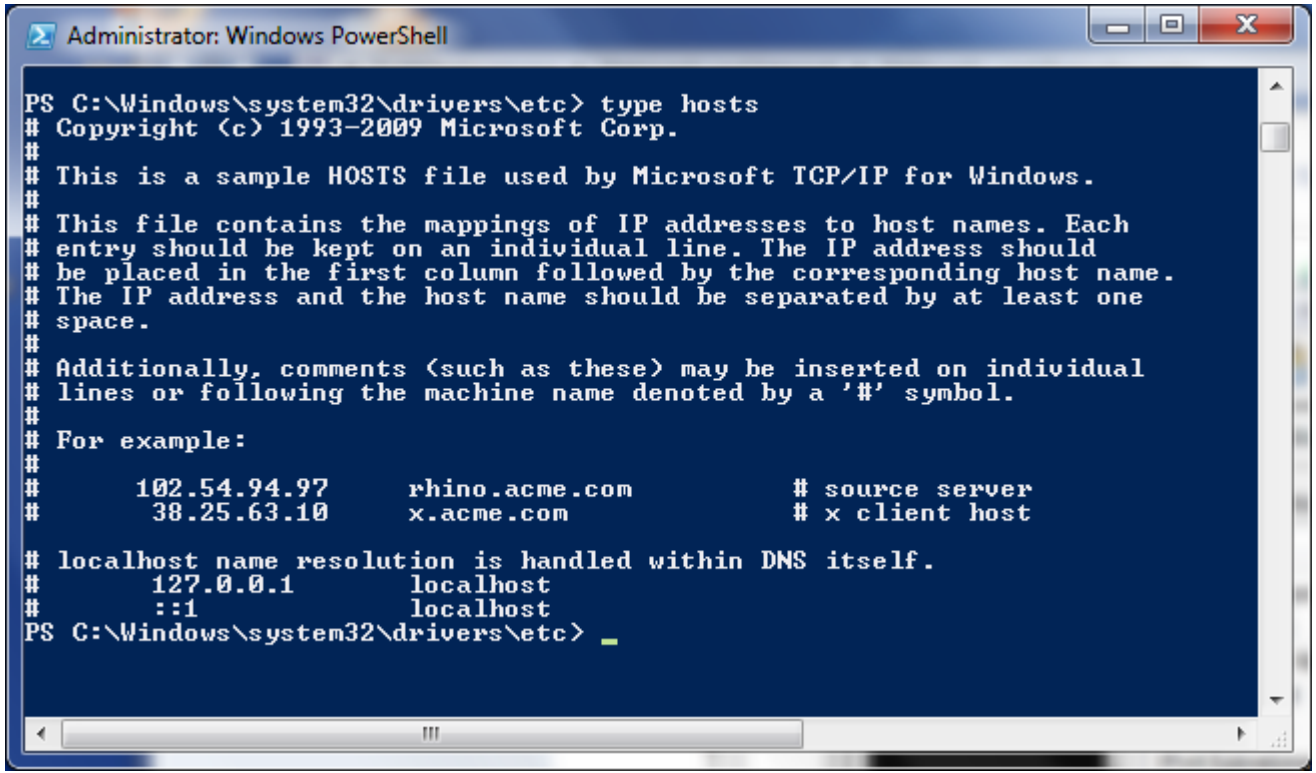
IP-Adresse – Domain-Name

- IP-Adressen: *131.188.97.34*
  - sind schwer zu merken
  - ändern sich (zwangsläufig)
  - → Namen für IP-Adressen sehr hilfreich
- Die Datei hosts
  - Historisch
  - Verteilung per FTP
  - Unix: `/etc/hosts`
    Windows: `C:\WINDOWS\system32\drivers\etc\hosts`

IP-Adresse – Domain-Name

- Domain Name System (DNS): www.uni-erlangen.de
  - Nameserver (NS); oft eingesetzte Implementation: BIND
  - Hierarchisch und verteilt
  - Zonen, Delegationen und Weiterleitungen
  - Autoritative NS, Primary / Secondary NS, Caching NS
  - FQDN (Fully Qualified Domain Name)

hosts – Windows



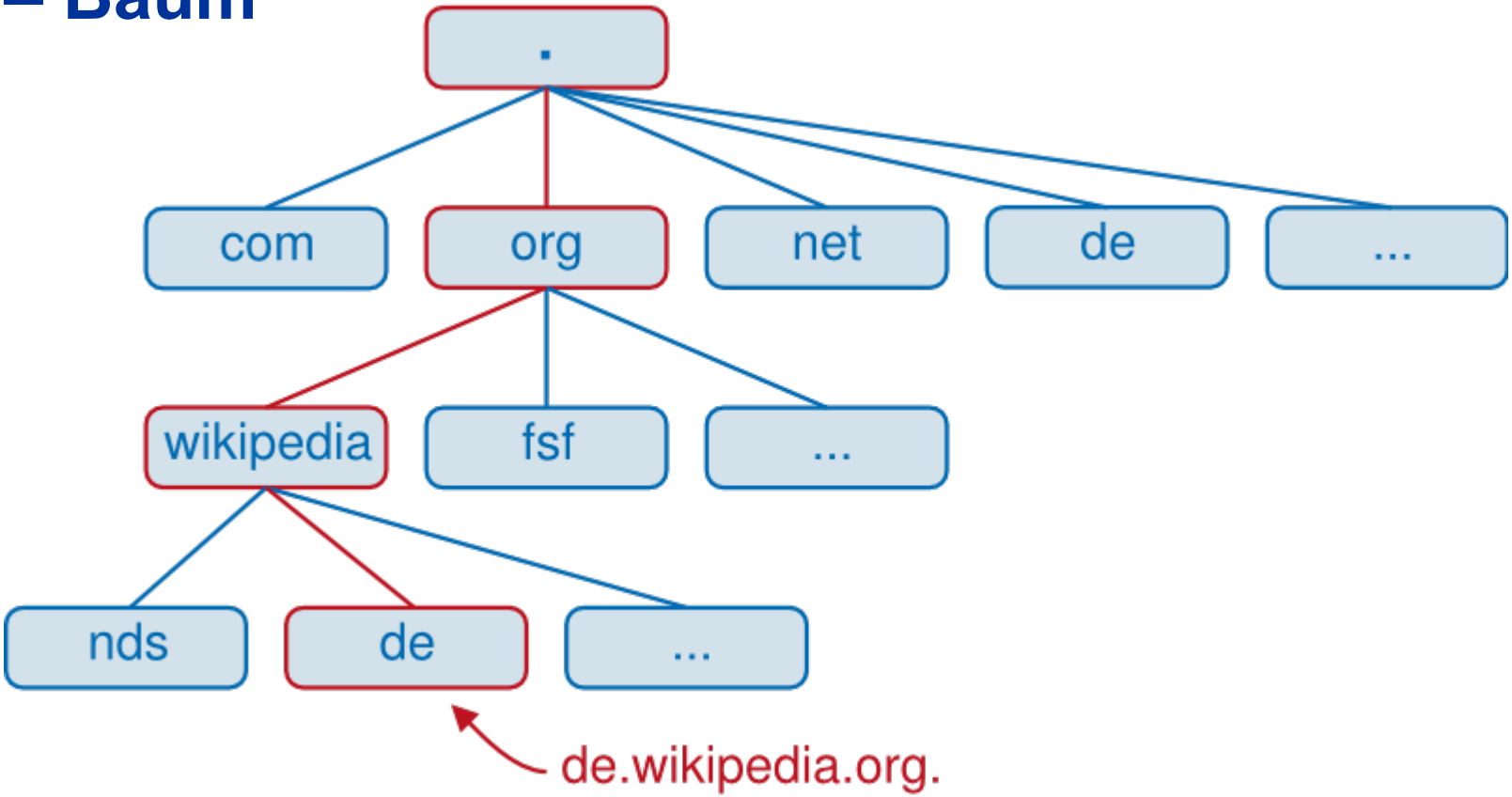
hosts – Linux

```
#
# hosts         This file describes a number of hostname-to-address
#               mappings for the TCP/IP subsystem.  It is mostly
#               used at boot time, when no name servers are running.
#               On small systems, this file can be used instead of a
#               "named" name server.
# Syntax:
#
# IP-Address  Full-Qualified-Hostname  Short-Hostname
#

127.0.0.1       localhost

# special IPv6 addresses
::1             localhost ipv6-localhost ipv6-loopback

fe00::0         ipv6-localnet

ff00::0         ipv6-mcastprefix
ff02::1         ipv6-allnodes
ff02::2         ipv6-allrouters
ff02::3         ipv6-allhosts
```

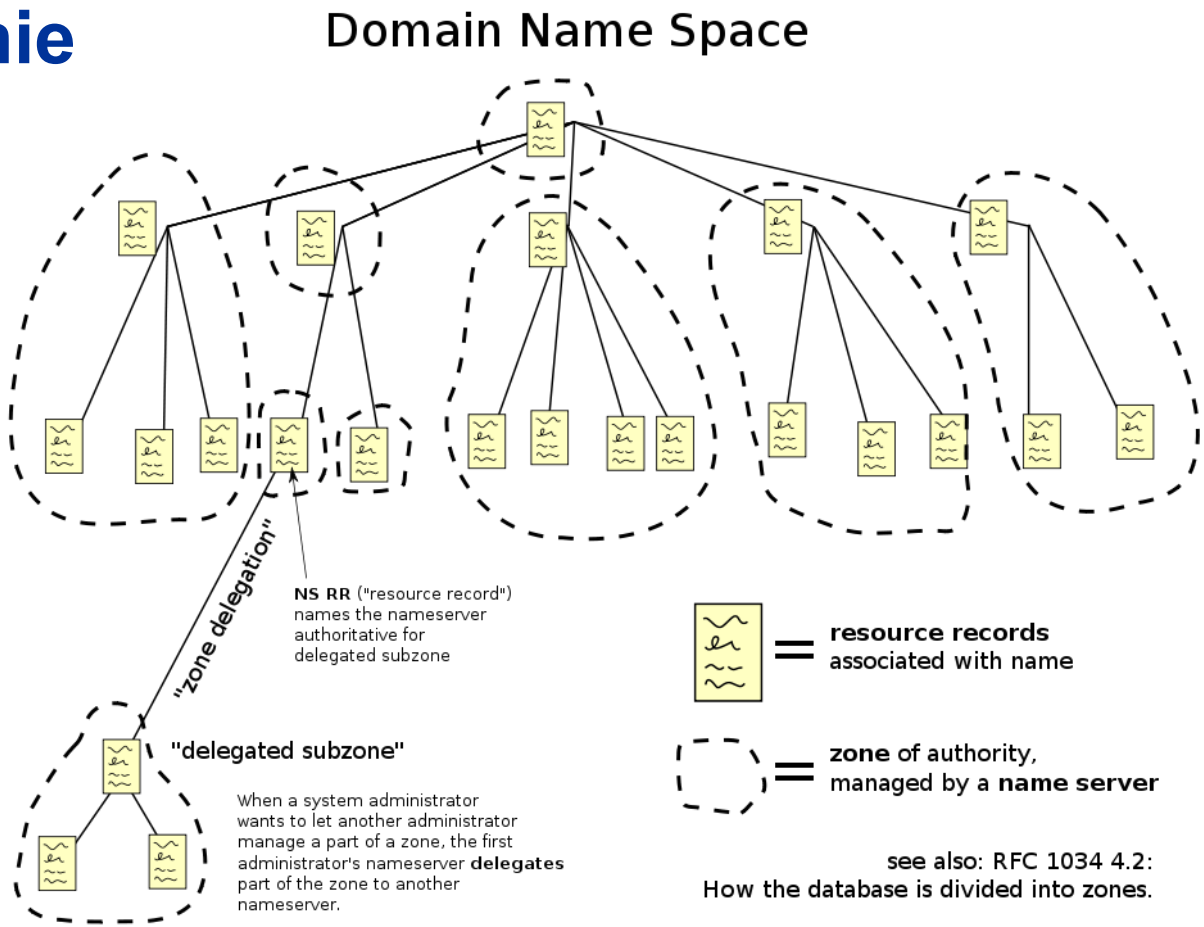
DNS – Resource Record

- A – IPv4-Adressen
- AAAA – IPv6-Adressen
- SOA (Start of Authority) – Zonen-Beschreibung
- NS – Autoritative NS und Delegation von Sub-Zonen
- MX – Mail-Exchanger
- CNAME (Canonical Name) – Alias
- PTR (Pointer) – Rückwärts-Abbildung (IP → Name)
- SRV (Service) – Zuständiger Server (allgemeiner als MX)

DNS – Baum



DNS – Hierarchie

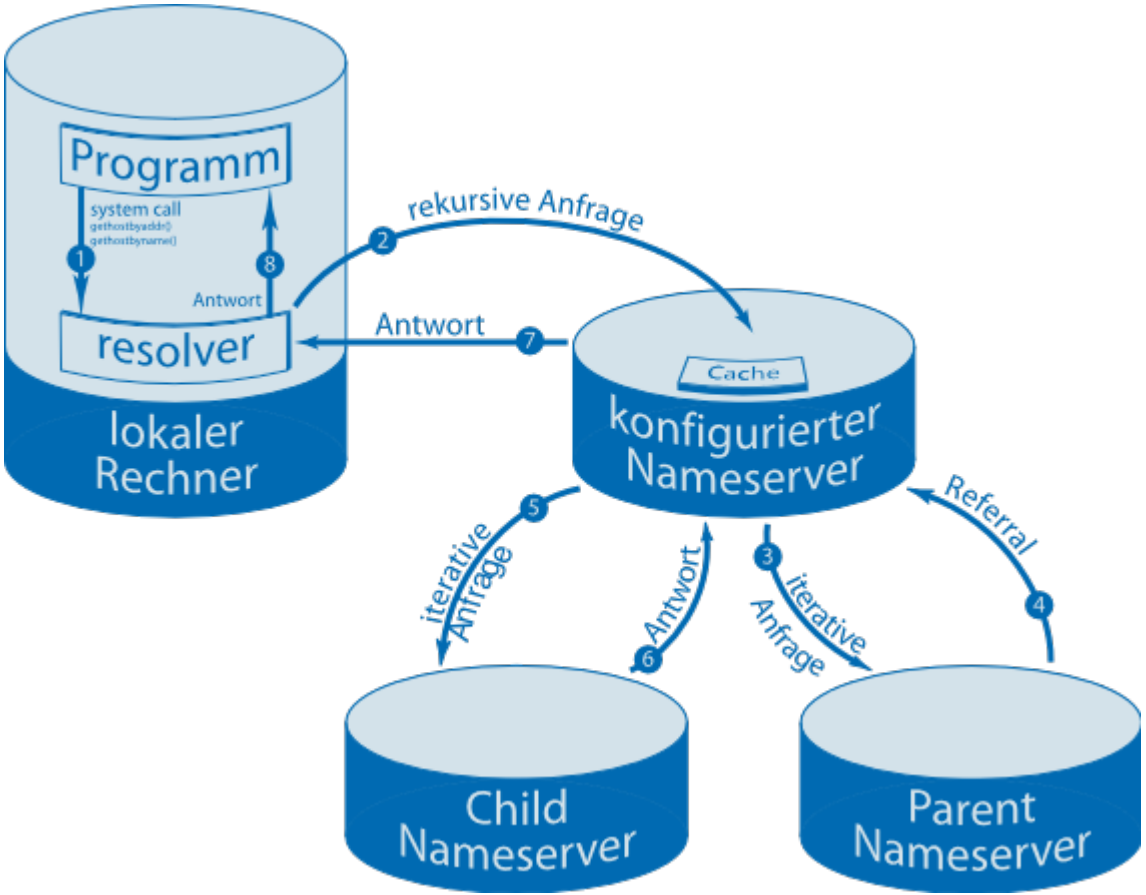


DNS – Top Level Domains (TLD)

.com	commercial	.berlin	Berlin	.de	Deutschland
.org	organisation	.bayern	Bayern	.us	USA
.net	network	.xxx	Sex	.uk	United Kingdom
.edu	education	.app	Apps (Google)	.at	Österreich
.gov	goverment	.kinder	Kinder (Ferrero)	.ch	Schweiz
.mil	military	.kaufen	Einkaufen	.tv	Tuvalu
.info	information	.gmx	GMX (1&1)	.to	Königreich Tonga

- ccTLD (Country-Code)
- gTLD (Generic) – sTLD (sponsord), uTLD (unsponsored)
- Akzeptanz der neuen gTLD (2000, 2004, 2013+) immer noch fraglich

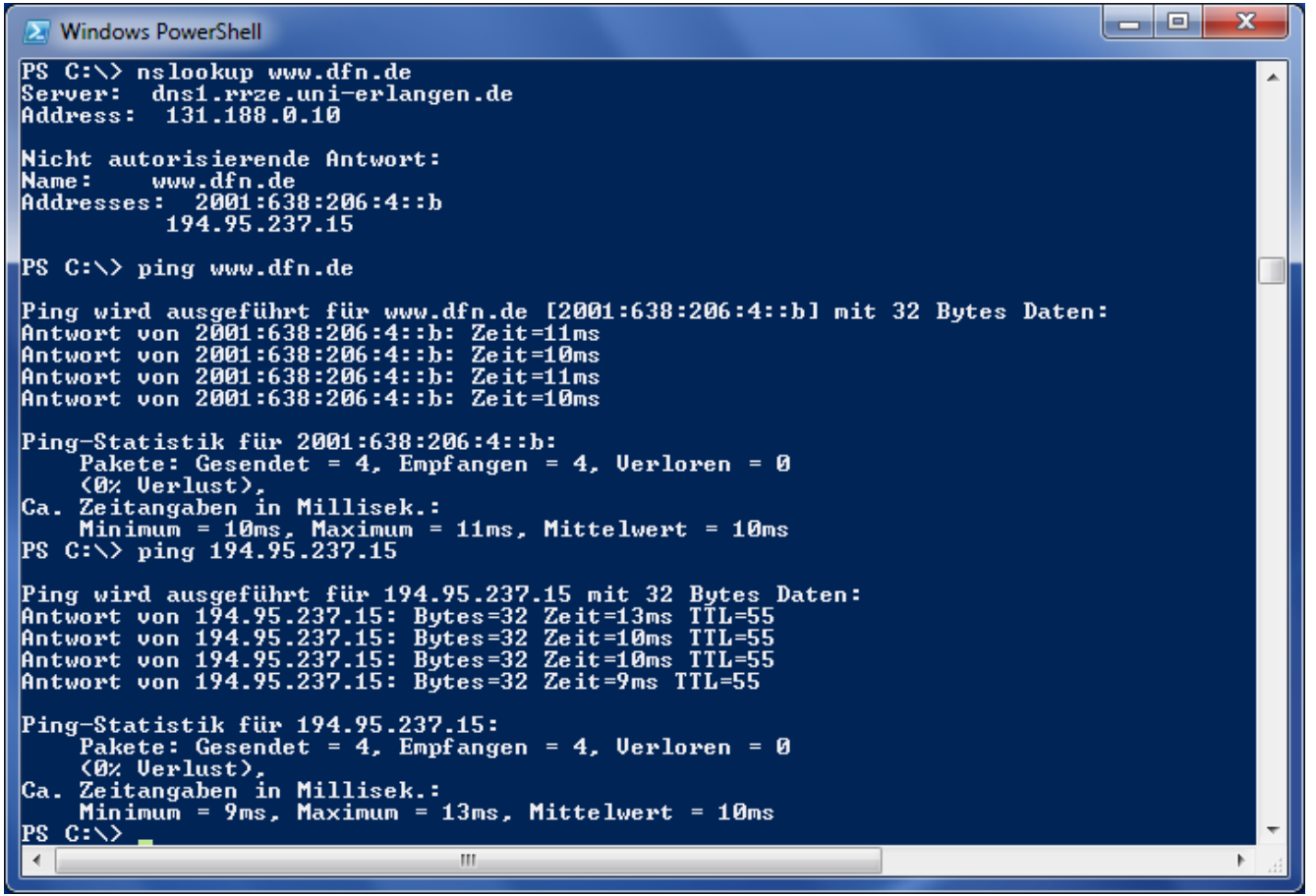
DNS – Anfrage


Programm
system call
gethostbyaddr()
gethostbyname()
1
8
Antwort
resolver
lokaler Rechner
rekursive Anfrage
2
Antwort
7
Cache
konfigurierter Nameserver
5
iterative Anfrage
6
Antwort
3
iterative Anfrage
4
Referral
Child Nameserver
Parent Nameserver

DNS – Werkzeuge

- `host`
  - einfaches Werkzeug (BIND)
- `dig`
  - Domain Information Groper; mächtiges Werkzeug (BIND)
- `nslookup`
  - mächtig; alt; Quasi-Standard (Windows)
- `getent`
  - Un*x; nicht direkt Zugriff auf NS, sondern „Systemdatenbank“/Resolver (`/etc/hosts` !)
- `/proj/dns/etc/DOMAINS`
  - FAU spezifisch (alle Zonendateien in einer Datei)
- `/etc/resolv.conf`, `/etc/nsswitch.conf`
  - Resolver Konfiguration unter Uni*x

DNS – Werkzeuge unter Windows



DNS – Werkzeuge

```
> dig www.heise.de

; <<>> DiG 9.7.4-P1 <<>> www.heise.de
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 63302
;; flags: qr rd ra; QUERY: 1, ANSWER: 1, AUTHORITY: 5, ADDITIONAL: 5

;; QUESTION SECTION:
;www.heise.de.                  IN      A

;; ANSWER SECTION:
www.heise.de.           1239    IN      A       193.99.144.85

;; AUTHORITY SECTION:
heise.de.               1239    IN      NS      ns.pop-hannover.de.
heise.de.               1239    IN      NS      ns.plusline.de.
heise.de.               1239    IN      NS      ns2.pop-hannover.net.
heise.de.               1239    IN      NS      ns.heise.de.
heise.de.               1239    IN      NS      ns.s.plusline.de.

;; ADDITIONAL SECTION:
ns2.pop-hannover.net.   31568   IN      A       62.48.67.66
ns.plusline.de.         42      IN      A       212.19.48.14
ns.s.plusline.de.       42      IN      A       212.19.40.14
ns.heise.de.            1706    IN      A       193.99.145.37
ns.pop-hannover.de.     10279   IN      A       193.98.1.200

;; Query time: 0 msec
;; SERVER: 131.188.0.10#53(131.188.0.10)
;; WHEN: Wed Jan  4 11:17:44 2012
;; MSG SIZE  rcvd: 252
```

DNS – Werkzeuge

```
> dig @8.8.8.8 www.heise.de

; <<>> DiG 9.7.4-P1 <<>> @8.8.8.8 www.heise.de
; (1 server found)
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 30625
;; flags: qr rd ra; QUERY: 1, ANSWER: 1, AUTHORITY: 0, ADDITIONAL: 0

;; QUESTION SECTION:
;www.heise.de.                  IN      A

;; ANSWER SECTION:
www.heise.de.           67      IN      A       193.99.144.85

;; Query time: 5 msec
;; SERVER: 8.8.8.8#53(8.8.8.8)
;; WHEN: Wed Jan  4 11:25:54 2012
;; MSG SIZE  rcvd: 46

> dig @8.8.8.8 +nocmd +nocomment +nostats +noquestion www.heise.de aaaa
www.heise.de.           142     IN      AAAA    2a02:2e0:3fe:100::7

> dig +nocmd +nocomment +nostats +noquestion +noauthority +noadditional +nottlid
  ftp.uni-erlangen.de
ftp.uni-erlangen.de.    IN      CNAME   ftp.rrze.uni-erlangen.de.
ftp.rrze.uni-erlangen.de. IN    A       131.188.12.212

> dig +nocmd +nocomment +nostats +noquestion +noauthority +noadditional +nottlid
  rrze.uni-erlangen.de mx
rrze.uni-erlangen.de.   IN      MX      10 mx-rz-3.rrze.uni-erlangen.de.
rrze.uni-erlangen.de.   IN      MX      10 mx-rz-1.rrze.uni-erlangen.de.
rrze.uni-erlangen.de.   IN      MX      10 mx-rz-2.rrze.uni-erlangen.de.
```

DNS – Werkzeuge

```
> nslookup 193.99.144.85
Server:         131.188.0.10
Address:        131.188.0.10#53

Non-authoritative answer:
85.144.99.193.in-addr.arpa      name = www.heise.de.

Authoritative answers can be found from:
144.99.193.in-addr.arpa nameserver = ns.heise.de.
144.99.193.in-addr.arpa nameserver = ns.s.plusline.de.
144.99.193.in-addr.arpa nameserver = ns.plusline.de.
ns.heise.de     internet address = 193.99.145.37
ns.plusline.de  internet address = 212.19.48.14
ns.s.plusline.de        internet address = 212.19.40.14

> nslookup 193.99.144.85 8.8.8.8
Server:         8.8.8.8
Address:        8.8.8.8#53

Non-authoritative answer:
85.144.99.193.in-addr.arpa      name = www.heise.de.

Authoritative answers can be found from:

> dig +nocmd +nocomment +nostats +noquestion +noauthority +noadditional +nottlid
  -x 193.99.144.85
85.144.99.193.in-addr.arpa. IN  PTR     www.heise.de.

> dig +nocmd +nocomment +nostats +noquestion +noauthority +noadditional +nottlid
  85.144.99.193.in-addr.arpa ptr
85.144.99.193.in-addr.arpa. IN  PTR     www.heise.de.
```

DNS – Werkzeuge

```
> getent hosts www.sparkasse.de
212.34.69.3     www.sparkasse.de
```

Einfügen einer Zeile in Datei `/etc/hosts`:
`123.123.123.123 www.sparkasse.de`

```
> getent hosts www.sparkasse.de
123.123.123.123 www.sparkasse.de

> dig +nocmd +nocomment +nostats +noquestion +noauthority +noadditional +nottlid
  www.sparkasse.de
www.sparkasse.de.       IN      A       212.34.69.3

> nslookup www.sparkasse.de
Server:         131.188.0.10
Address:        131.188.0.10#53

Non-authoritative answer:
Name:   www.sparkasse.de
Address: 212.34.69.3
```

Hinweis zu `dig`:

Parameter `+trace` erlaubt Analyse der DNS-Server-Hierarchie

DNS – Sicherheit

- Denial of Service (DoS)
  - Distributed-Denial-of-Service (DDoS) – Angriff auf DNS
  - DNS Amplification – Missbrauch von DNS für Angriff
- Zone Walking
  - „Abziehen“ aller DNS-Daten zur Angriffsvorbereitung
- DNS-Spoofing / Cache-Poisoning / DNS-Hijacking
  - Pharming (Weiterentwicklung von Phishing)
  - Zensur (China, Zugangserschwerungsgesetz)

DNS – Sicherheit

- Modifikation der Datei hosts durch Viren und Würmer
  - „Umgehung“ des DNS
  - Effektive Umleitung von unerwünschten Adressen, wie z.B. die der Update-Server von Antiviren-Programmen
- DNS-Anfragen sind unverschlüsselt
  → Datenschutz nicht gewährleistet!
- Verdeckte Kommunikation in DNS-Payload (Steganografie)
  - Umgehung von Sperren
  - Kontakt zwischen Malware und Command-and-Control-Servern
    http://heise.de/-2923909

DNS – Sicherheit – Absicherung von DNS

- TSIG (Transaction Signatures)
  - Sichere Verbindung zwischen DNS-Servern
  - Eher selten im Einsatz
- DNSSEC (DNS Security)
  - Signierung der DNS-Daten - Keine Verschlüsselung!
  - Absicherung aller Verbindungen (Server-Server und Server-Client)
  - Wird gerade ausgerollt (*uni-erlangen.de* und *fau.de* seit 20.9.2016)
  - Erhöhung der Sicherheit des gesamten Internets (DANE, SSL/Zertifikate, SSH-Keys, …)
- DNS-Privacy
  - Verschlüsselung der Anfragen (ähnlich TSIG; mit Hilfe von DNSSEC)

DNS an der FAU

- Caching Nameserver (Anycast)
  - dns1/2: 131.188.0.10 / 131.188.0.11
  - Alle anderen Adressen sind veraltet!
- Autoritative Name-Server
  - ns1: 131.188.3.2
  - ns2: 131.188.12.100
  - ns3: 131.188.3.4
  - Hidden Primary
- Administration
  - NEU: dns@fau.de
  - alt: dns-admin@rrze.fau.de

Vielen Dank für Ihre Aufmerksamkeit!

Regionales RechenZentrum Erlangen [RRZE]
Martensstraße 1, 91058 Erlangen
http://www.rrze.fau.de