heinlein

16.03.2024 / Robert Sander

Wie funktioniert das Internet?

Heinlein Gruppe

- IT-Consulting und 24/7 Linux-Support mit ~80 Mitarbeitern
- Eigener Betrieb eines ISPs seit 1992
- Täglich tiefe Einblicke in die Herzen der IT aller Unternehmensgrößen

24/7-Notfall-Hotline: 030 / 40 50 5 – 110

- 28 Spezialisten mit LPIC-2 und LPIC-3
- Für alles rund um Linux & Server & DMZ
- Akutes: Downtimes, Performanceprobleme, Hackereinbrüche, Datenverlust
- Strategisches: Revision, Planung, Beratung, Konfigurationshilfe

heinlein

Teil 1:
Das Internet-Protokoll

Geschichte

- optische Telegrafie
  - Leuchtfeuer, schwenkbare Signalarme, Lichtzeichen, Flaggenalphabet
- 1833 elektromagnetischer Schreibtelegraf von Morse
- 1838 Morsecode
- 1861 erstes Telephon von Reis
  - „Das Pferd frisst keinen Gurkensalat“
- 1876 erstes Telefon von Bell
  - Patentstreit mit Gray
- 1969 Vernetzung von vier US-Großrechnern via IMP
- 1973 TCP von Kahn & Cerf
  - telnet und ftp sind älter
- 1978 Trennung von IP und TCP/UDP
- 1983 Internet Advisory Board
- 1986 IETF
- 1988 Morris-Wurm
  - sendmail, finger, rlogin

Leitungsvermittelte Kommunikation

Leitungsvermittelte Kommunikation

- Sender hat eine durchgeschaltete Zweidraht-Leitung bis zum Empfänger
- später elektromechanisch vermittelt
- noch später elektronisch vermittelt
- dann wurden internationale Gespräche zeitmultiplexed übermittelt
- usw. usf.

Paketvermittelte Kommunikation

- Grundidee: Nicht mehr eine reservierte Leitung zwischen Sender und Empfänger
- zu übertragender Inhalt wird in Pakete aufgeteilt und mit Adressen ausgestattet
- anhand der Adressen werden die Pakete individuell durch das Netzwerk geschickt
- von Station zu Station
- Zwischenstationen müssen sich nur die Adressen am Anfang des Paketes anschauen

Schichten-Modell
OSI oder TCP/IP?

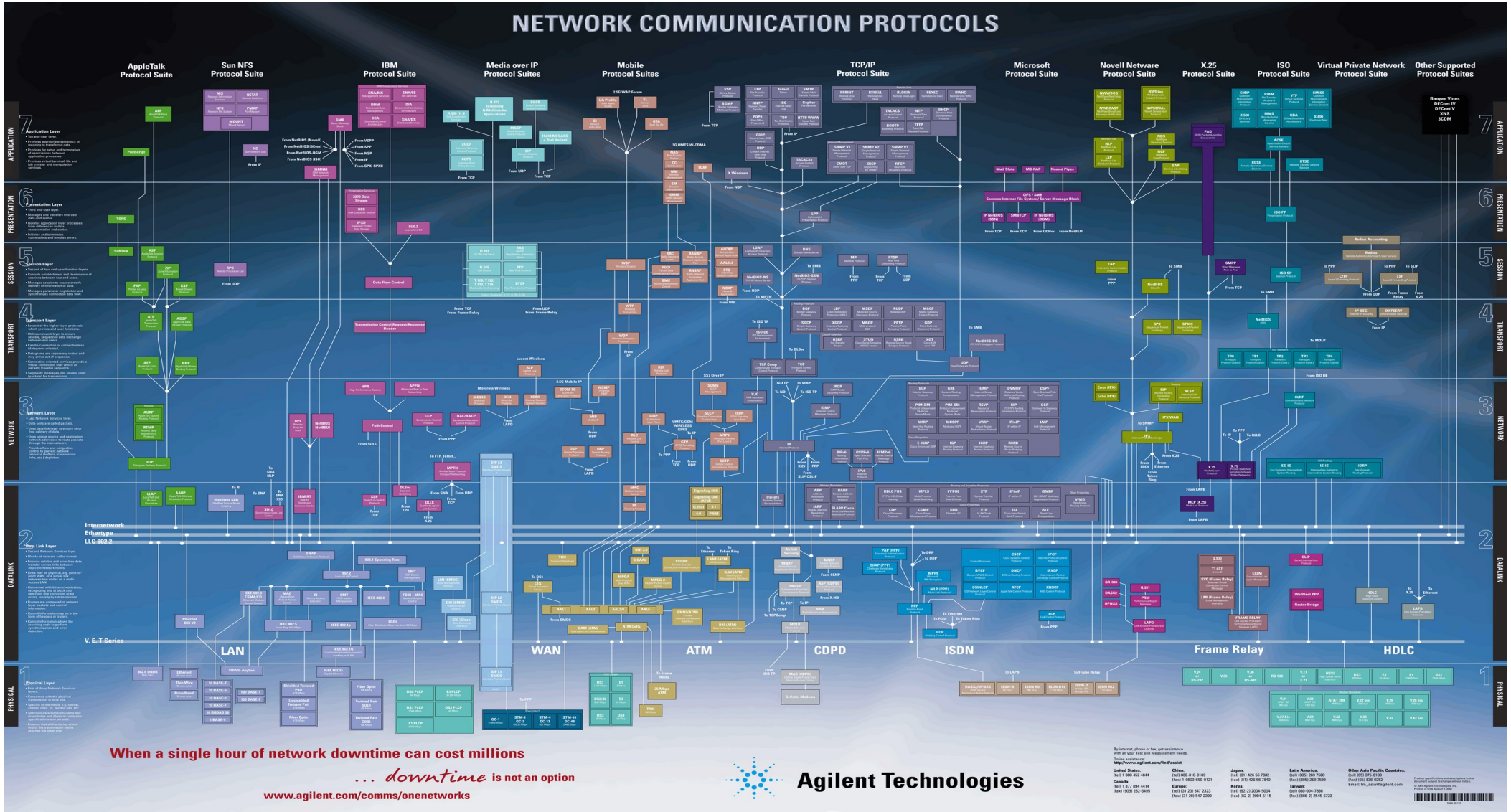
OSI

- Application
- Presentation
- Session
- Transport
- Network
- Data Link
- Physical

TCP/IP

- Application
- HTTP, FTP, SMTP, IMAP, LDAP, SSH
- Transport TCP, UDP, ESP
- Internet
- Link Layer

Jede Schicht löst ein Problem
Jede Schicht hat ein eigenes Adressierungsschema


NETWORK COMMUNICATION PROTOCOLS
AppleTalk Protocol Suite
Sun NFS Protocol Suite
IBM Protocol Suite
Media over IP Protocol Suites
Mobile Protocol Suites
TCP/IP Protocol Suite
Microsoft Protocol Suite
Novell Netware Protocol Suite
X.25 Protocol Suite
ISO Protocol Suite
Virtual Private Network Protocol Suite
Other Supported Protocol Suites
APPLICATION
PRESENTATION
SESSION
TRANSPORT
NETWORK
DATALINK
PHYSICAL
LAN
WAN
ATM
CDPD
ISDN
Frame Relay
HDLC
When a single hour of network downtime can cost millions
... downtime is not an option
www.agilent.com/comms/onenetworks
Agilent Technologies

TCP/IP Adressen

- Link-Layer: Kommt auf das Medium an, z.B. MAC-Adressen (48 Bit) bei Ethernet
- Internet: IP-Adressen IPv4: 192.0.2.24 (32 Bit), IPv6: 2001:db8::24 (128 Bit)
- Transport: Port-Nummer (16 Bit) für TCP & UDP, Typ bei ICMP
- Application: URL für HTTP, local@example.com für SMTP, etc

- Jedes Protokoll in jeder Schicht hat eigenes Paketformat

Pakete entsprechend der Schichten verpackt

- außen Ethernet
  - von 00:80:41:ae:fd:7e an 00:80:41:bc:9e:24
- dann Internet Protokoll
  - von 2001:db8:4::beef an 2001:db8:24::cafe
- dann z.B. TCP oder UDP
  - von Port 54786 an Port 80
- dann der Payload, also der eigentliche Inhalt abhängig vom Protokoll
  - HTTP-Stream
  - SNMP-Trap
  - E-Mail-Übertragung zwischen zwei MTA
- am Ende eine Folge von Bits auf der Leitung

Wie geht ein Paket auf die Reise?

- Jeder Host hat eine Routing-Tabelle:

```
192.0.2.0/24 dev eth0 proto kernel scope link src 192.0.2.24 metric 100
default via 192.0.2.1 dev eth0 proto dhcp metric 100
```

- Sender schaut sich die Empfänger-Adresse an: `192.0.2.15`
- Passt sie zu einer der Routen?
  - Routen nach Netzmaske sortiert, je länger, desto spezifischer
  - default = 0.0.0.0/0
  - /24 = 255.255.255.0 = 11111111.11111111.11111111.00000000
  - Ziel-IP && Netzmaske == Netz-Adresse && Netzmaske ?
  - `192.0.2.15 && 255.255.255.0 => 192.0.2.0`
  - `192.0.2.0 && 255.255.255.0 => 192.0.2.0`

Empfänger im LAN

- LAN = direkt angeschlossenes Netzwerk
- Address Resolution Protocol (IPv4) bzw Neighbor Discovery (IPv6): IP zu MAC
- `192.0.2.15 dev eth0 lladdr 00:80:41:bc:9e:24 REACHABLE`
- Paket wird zusammengebaut:
- Ethernet-Paket von 00:80:41:ae:fd:7e an 00:80:41:bc:9e:24 enthält
- IP-Paket von 192.0.2.24 an 192.0.2.15 enthält
- TCP-Paket von Port 54786 an Port 80

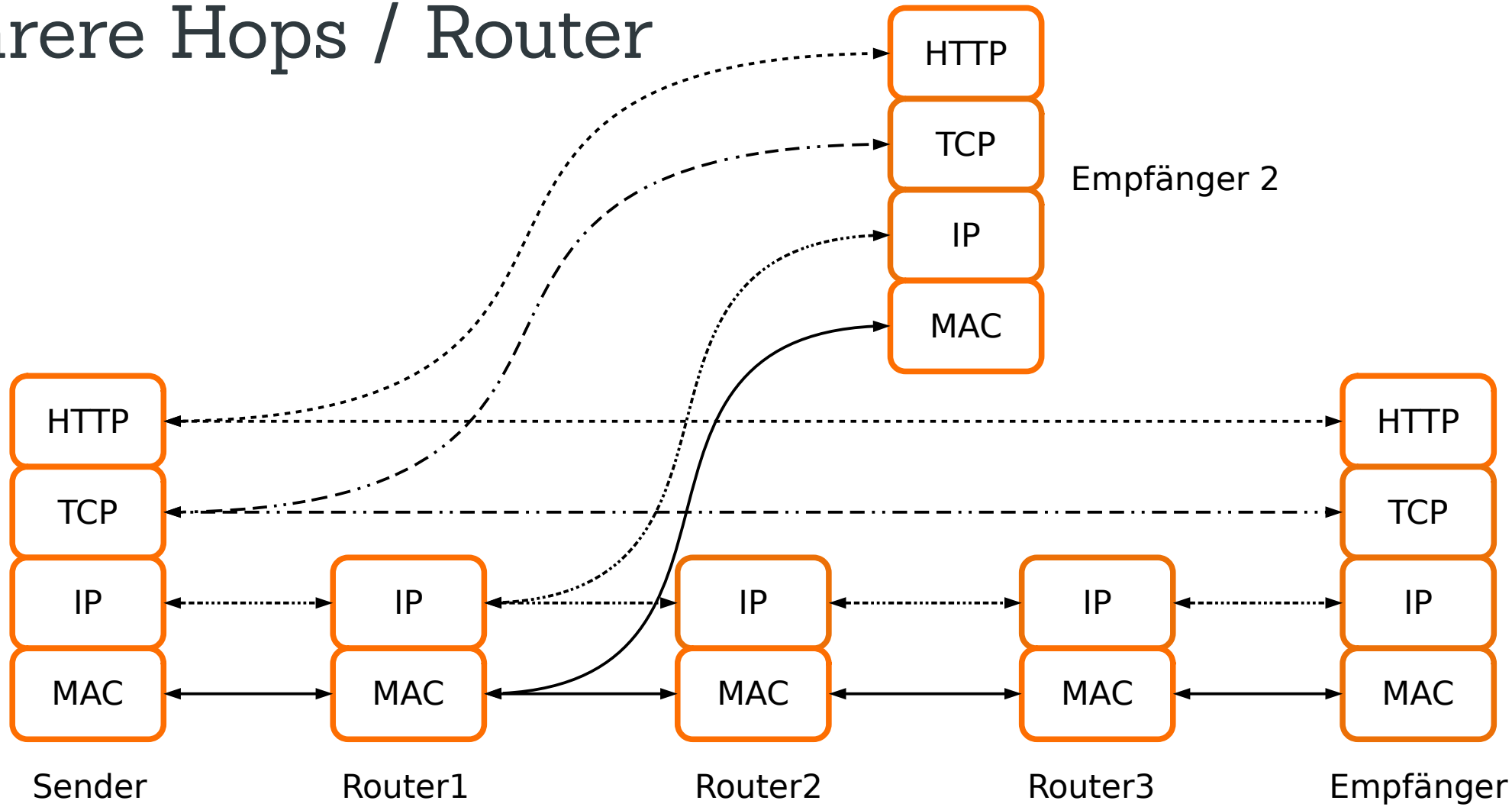
Empfänger nicht im LAN

- Empfänger ist 198.51.100.42
- `198.51.100.42 && 0 == 0.0.0.0 && 0 == 0 =>` default Route greift als letztes
- via 192.0.2.1 ist der Gateway
- MAC Adresse von `192.0.2.1 ist 00:80:41:43:af:14` (ARP)
- Paket wird zusammengebaut:
- Ethernet-Paket von 00:80:41:ae:fd:7e an 00:80:41:43:af:14 enthält
- IP-Paket von 192.0.2.24 an 198.51.100.42 enthält
- TCP-Paket von Port 34516 an Port 22

Empfänger nicht im LAN

- Gateway 00:80:41:43:af:14 erhält IP-Paket an Empfänger 198.51.100.42
- keine der eigenen IP-Adressen => weiterleiten
- Gateway 00:80:41:43:af:14 schaut in eigene Routing-Tabelle
- usw. usf.

Mehrere Hops / Router



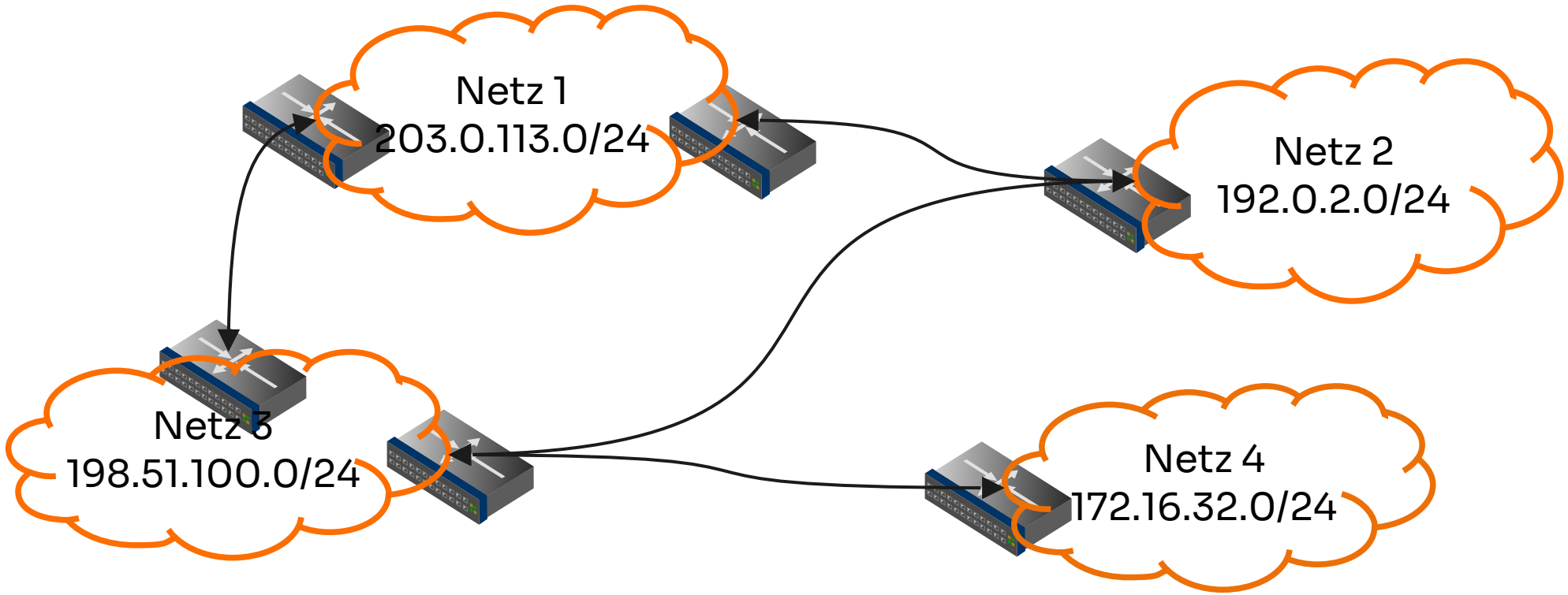
Router

- Netzwerkgerät mit mindestens 2 Schnittstellen
  - intern (LAN)
  - extern (WAN)
  - Verbindungen zu anderen Routern
- Router-ID
  - IPv4-Adresse
  - Auf Loopback-Interface
- Interface-Adressen

heinlein

Teil 2:
Woher wissen Router, wohin mit den Paketen?

Internet
Netz aus Netzen



Autonomous System

- Sammlung von gemeinsam verwalteter IP-Netze
- „Autonome Systeme sind untereinander verbunden und bilden so das Internet.“
- Eindeutig identifiziert über AS-Nummer (32 bit)
- In Europa: RIPE http://ripe.net/
- Voraussetzung für eigene AS-Nummer
  - Verbindung zu zwei anderen AS über BGP

RIPE NCC
Réseaux IP Européens Network Coord. Centre

- Objekte in der RIPE-Datenbank

- aut-num: AS-Nummer
  - Mit Import und Export (BGP-Partner)
- inetnum / inet6num: zugeteilter IP-Addressbereich
  - Wem gehören die IP-Adressen?
- route / route6:
  - Welches AS darf den IP-Prefix annoncieren?
  - IP-Prefix ggfs kleiner als inetnum / inet6num
- domain:
  - Welche Nameserver sind für die PTR-Records zuständig?

Border Gateway Protocol

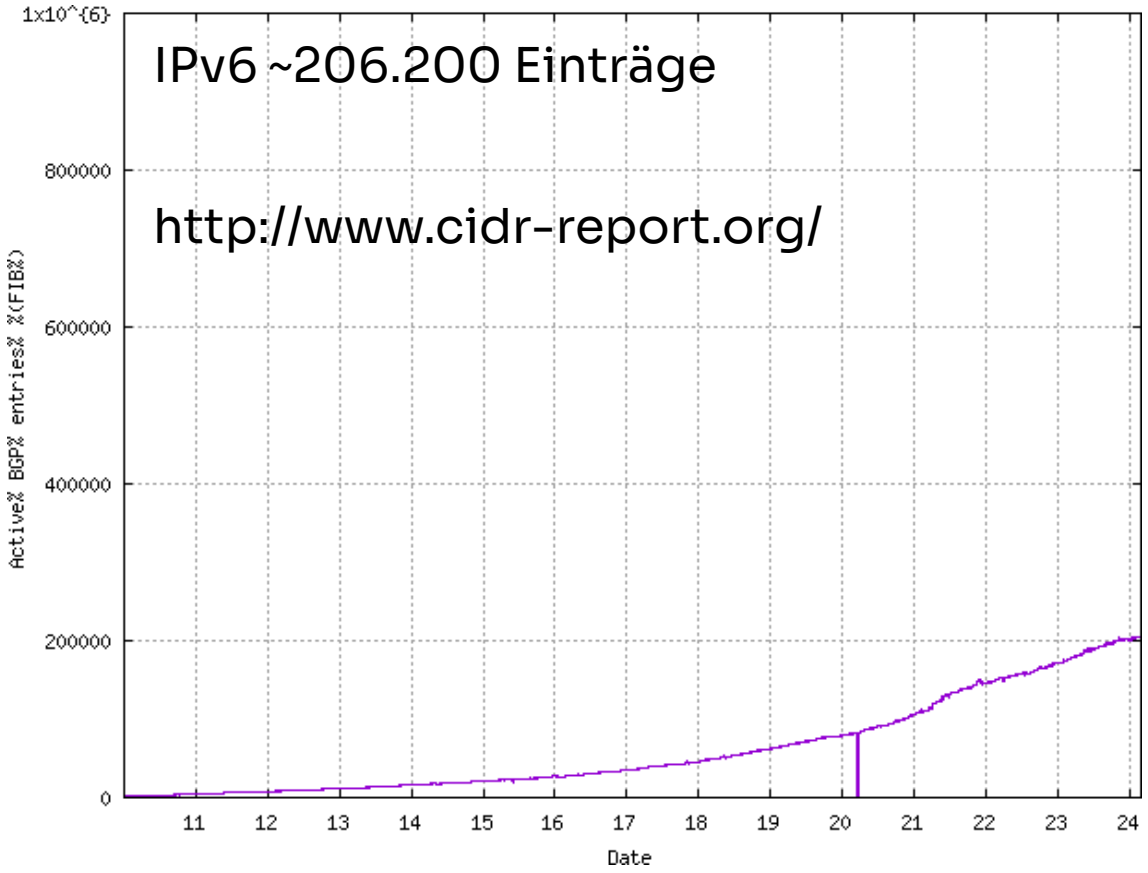
- Exterior Gateway Protocol / Routing Protokoll
- Router tauschen IP-Routen untereinander aus
- Router A sagt Router B
  - Du erreichst a.b.c.0/24 über mich
- Router B sagt Router A
  - Du erreichst y.z.0.0/16 und u.v.w.0/24 über mich
- Wird die Defaultroute übergeben, dann Provider → Kunde
- Empfänger kann entscheiden, ob er einzelne Routen akzeptiert

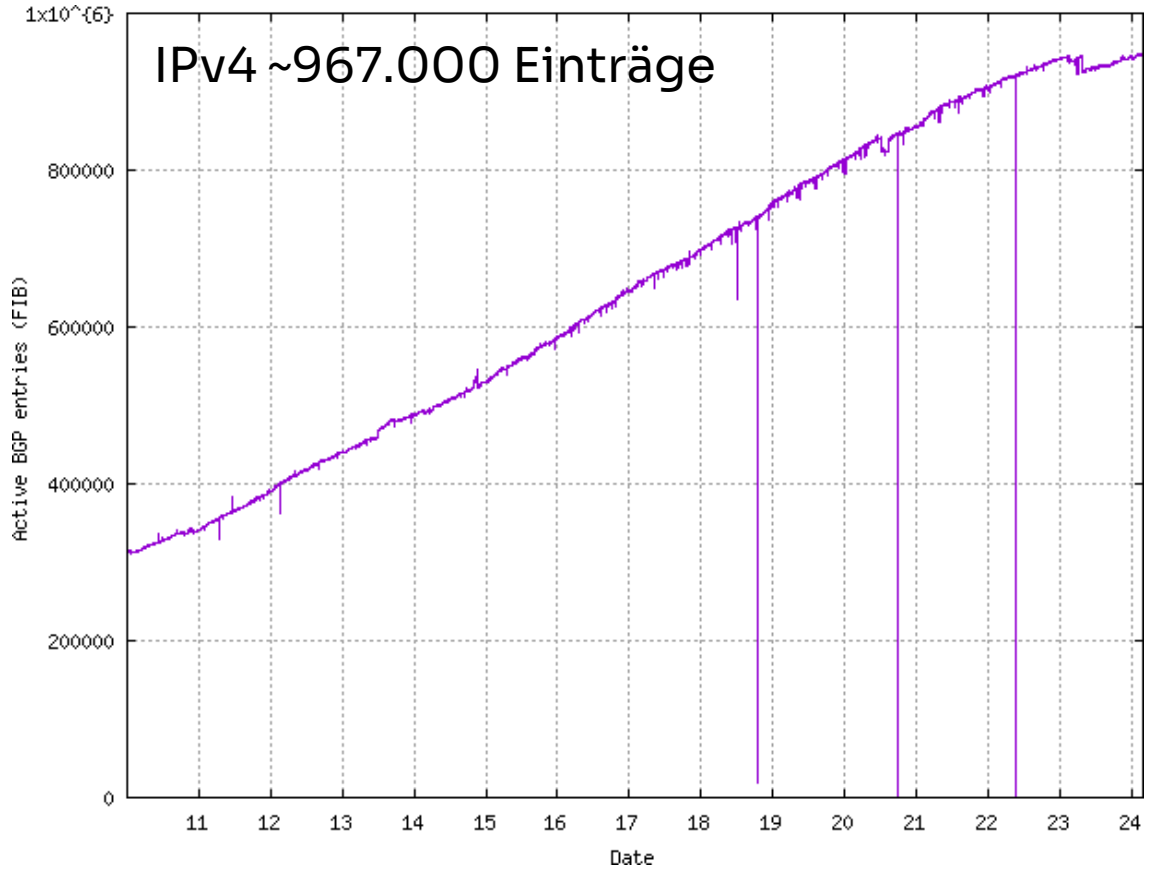
- IPv4 + IPv6

BGP Updates

- Announcement oder Withdrawal von Routen
- AS Path
  - über welche AS ist der IP-Prefix erreichbar
- IGP-Metrik
  - wie teuer ist es bei mir dorthin
- Multi-Exit Discriminator (MED)
  - Priorität bei parallelen Peerings zwischen zwei AS
- Local Preference
  - bevorzugt AS-Pfade mit höherem Wert
- Next Hop
  - IP-Adresse des Next-Hop-Routers zum annoncierten Prefix
- Auswahl der aktiven Route anhand der Prioritäten
- Auswahl über Filter beeinflussbar

Full Routing Table





heinlein

Teil 3:
Wie funktioniert das mit Linux?

Packet Forwarding

- echo 1 > /proc/sys/net/ipv4/ip_forward
- echo 1 > /proc/sys/net/ipv6/conf/all/forwarding
- oder in /etc/sysctl.conf
  - net.ipv4.ip_forward=1
  - net.ipv6.conf.all.forwarding=1
- Redirects ausschalten
  - net.ipv4.conf.all.accept_redirects = 0
  - net.ipv6.conf.all.accept_redirects = 0

Routing Software

- Quagga (Fork von Zebra)
  - verschiedene Daemonen für Protokolle BGP, OSPFv2, OSPFv3, RIP, Kernel
  - vtysh ähnlich zu IOS von Cisco
  - Weiterentwicklung: FRR (https://frrouting.org/)
- XORP
  - aktuelles Release von Januar 2012...
- OpenBGPD
  - BGP und OSPF, Teil von OpenBSD
- BIRD
  - Entwickelt in Prag von nic.cz
  - an vielen europäischen IXPs genutzt (DE-CIX, AMS-IX, LINX, ECIX)
  - Linux, FreeBSD, NetBSD und OpenBSD
  - http://bird.network.cz/

heinlein

Fragen und Diskussionen

Linux höchstpersönlich.

Bleiben wir im Kontakt

Robert Sander

Tel. +49 30 40 50 51-43
r.sander@heinlein-support.de

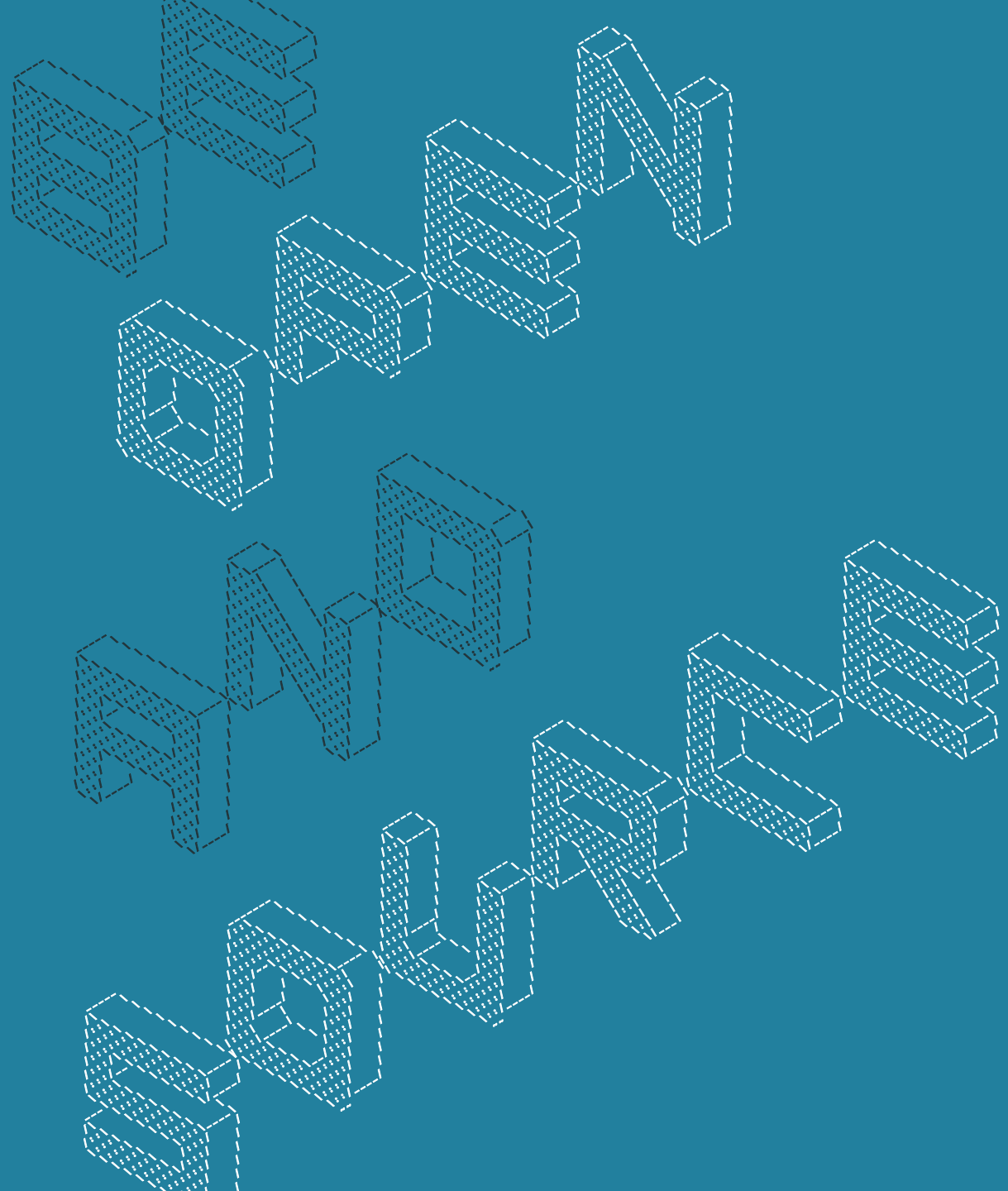
Heinlein Support GmbH
Schwedter Straße 8/9 | 10119 Berlin
www.heinlein-support.de

Wenn's brennt: CompetenceCall

Das Backup für Ihre Server-Administration.

Nutzen Sie unsere SLA-Verträge und sichern Sie sich den 24/7-Support unserer Linux-Consultants.

- Kontinuierliche Absicherung mit garantierten Reaktionszeiten und festen SLAs
- Rückendeckung im Notfall: mindestens LPIC-2 zertifizierte Profis mit jahrelanger, täglicher' Admin-Erfahrung
- Projektunterstützung: maßgeschneiderte Lösungen, die Flexibilität, Sicherheit, Administrierbarkeit und Hochverfügbarkeit vereinen
- Services: Performanceanalyse, Serverhärtung, Netzwerkanalyse, Konfigurationshilfe, Datenrestaurierung



SLAC 2024

06.–08. Mai 2024 | Berlin

www.slac-2024.de

Die Heinlein-Gruppe: Gemeinsam für digitale Souveränität

Heinlein Support

- Akademie: Für die oberen 10% des Wissens – unsere Linux-Schulungen für IT-Experten.
- Consulting: Security- und Strategieberatung, Projektumsetzung und umfassender Support für IT-Administratoren
- Services: SLA-Verträge, Hosting und Lizenzen als Unterstützung & Absicherung Ihrer kritischen IT-Infrastruktur

Weitere Marken

- mailbox.org: E-Mail, Online-Office, Cloud-Speicher und Videokonferenzen nach neuesten Sicherheitsstandards und mit grüner Energie.
- OpenTalk: Videocalls, wie sie sein sollten – mit unserer sicheren, benutzerfreundlichen und skalierbaren Videokonferenz für Behörden, Provider, Unternehmen und Schulen.

Werde Teil des Teams

Wir suchen:

- Admins, Consultants, Supporter, Trainer

Wir bieten:

- Spannende Projekte, Kundenlob, eigenständige Arbeit, ein tolles Team, Work-Life-Balance

- ...und natürlich: Linux, Linux, Linux...

- https://www.heinlein-support.de/jobs