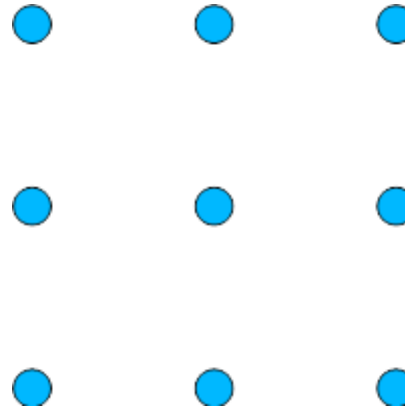


# Informationssicherheit und IT-Forensik







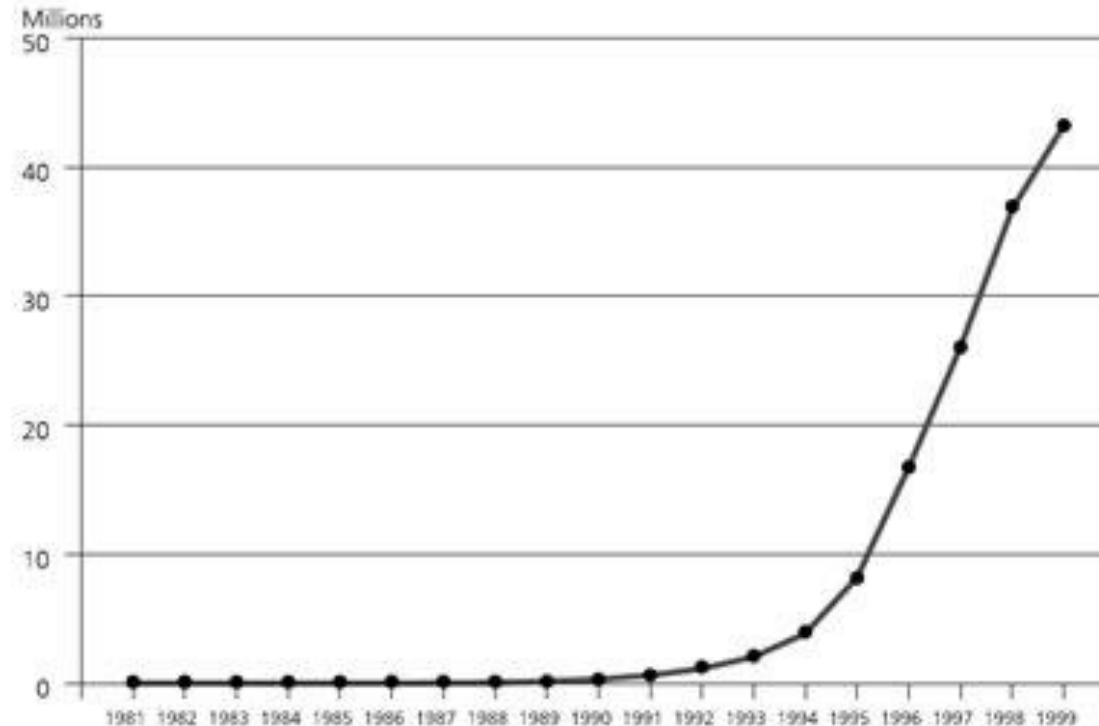


## Lernziele dieser Einheit

- Das Schichtenmodell für TCP/IP und das Prinzip der Kapselung wirklich verstanden haben und anwenden können (insb. auch Begriff und Bedeutung von „Layer“)
- Begriffe verstehen und „parat“ haben
- CIDR verstehen und anwenden können
- Alle weiteren hier genannten Verfahren und Techniken verstehen und erläutern können

## Internet Hosts IPv4 1981 bis 1999

Figure 1: Estimated Number of Internet Hosts, 1981-1999

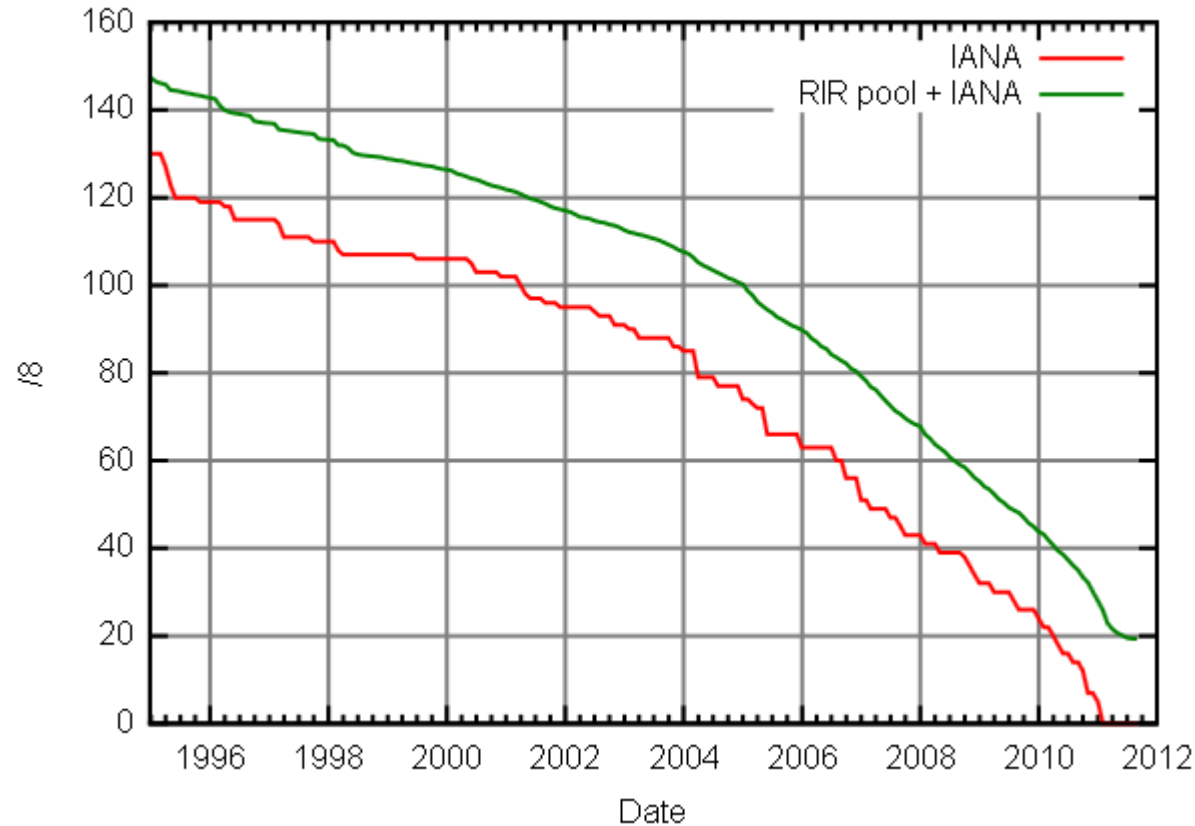


Source: Network Wizards (<http://www.nw.com>).

- Quelle: Network Wizards + <http://www.isc.org/solutions/survey/history>

## IPv4: Freie /8 Adressblöcke und vergebene /8 Adressblöcke

Free /8



Prefix	Designation	Date	Whois	Status [1]
000/8	IANA - Local Identification	1981-09		RESERVED
001/8	APNIC	2010-01	whois.apnic.net	ALLOCATED
002/8	RIPE NCC	2009-09	whois.ripe.net	ALLOCATED
003/8	General Electric Company	1994-05		LEGACY
004/8	Level 3 Communications, Inc.	1992-12		LEGACY
005/8	RIPE NCC	2010-11	whois.ripe.net	ALLOCATED
006/8	Army Information Systems Center	1994-02		LEGACY
007/8	Administered by ARIN	1995-04	whois.arin.net	LEGACY
008/8	Level 3 Communications, Inc.	1992-12		LEGACY
009/8	IBM	1992-08		LEGACY
010/8	IANA - Private Use	1995-06		RESERVED
011/8	DoD Intel Information Systems	1993-05		LEGACY
012/8	AT&T Bell Laboratories	1995-06		LEGACY
013/8	Xerox Corporation	1991-09		LEGACY
014/8	APNIC	2010-04	whois.apnic.net	ALLOCATED
015/8	Hewlett-Packard Company	1994-07		LEGACY
016/8	Digital Equipment Corporation	1994-11		LEGACY
017/8	Apple Computer Inc.	1992-07		LEGACY
018/8	MIT	1994-01		LEGACY
019/8	Ford Motor Company	1995-05		LEGACY
020/8	Computer Sciences Corporation	1994-10		LEGACY
021/8	DDN-RVN	1991-07		LEGACY

- Quelle links: Wikipediabnutzer „Mro“ | Quelle rechts: iana.org

## Netzteilnehmer (Geräte und Anschlüsse)

- Über 5 Milliarden IP Devices aktiv (IMS Research, August 2010)
- Über 1 Milliarde Computer aktiv (IMS Research, August 2010)
- 500 Millionen verkaufte Smartphones allein für 2011 erwartet; 2017: 1,5 Milliarden laut statista.com
- Über 500 Millionen Breitbandanschlüsse (ITU, Oktober 2010)

## Apple-Mobilgeräte sind voll IPv6-fähig


→ ↻ 🏠 <https://www.zdnet.com/article/apple-drops-ipv4-internet-support/> 📄 ⋮ 📌

EDITION: ▼

**ZDNet** 🔍 CENTRAL EUROPE MIDDLE EAST SCANDINAVIA AFRICA UK ITALY SPAIN MORE ▼ NEWSLETTERS


# Starting in June, Apple will require iOS apps to support IPv6

All iPhone and iPad apps must soon support IPv6. Good-bye old Internet. Hello new Internet.

By  [Steven J. Vaughan-Nichols](#) for [Networking](#) | May 5, 2016 -- 18:31 GMT (19:31 BST) | Topic: [Networking](#)

💬 0 f in 🐦 ✉ 🔔

It wasn't that long ago that most companies were still refusing to move from the Internet's ancient IPv4 networking protocol. [IPv6 was slowly catching on](#), but the vast majority of Internet users were still stuck on IPv4. Things have changed. Starting soon, Apple will require its iOS app developers not merely to use IPv6, and to mitigate IPv4 use.



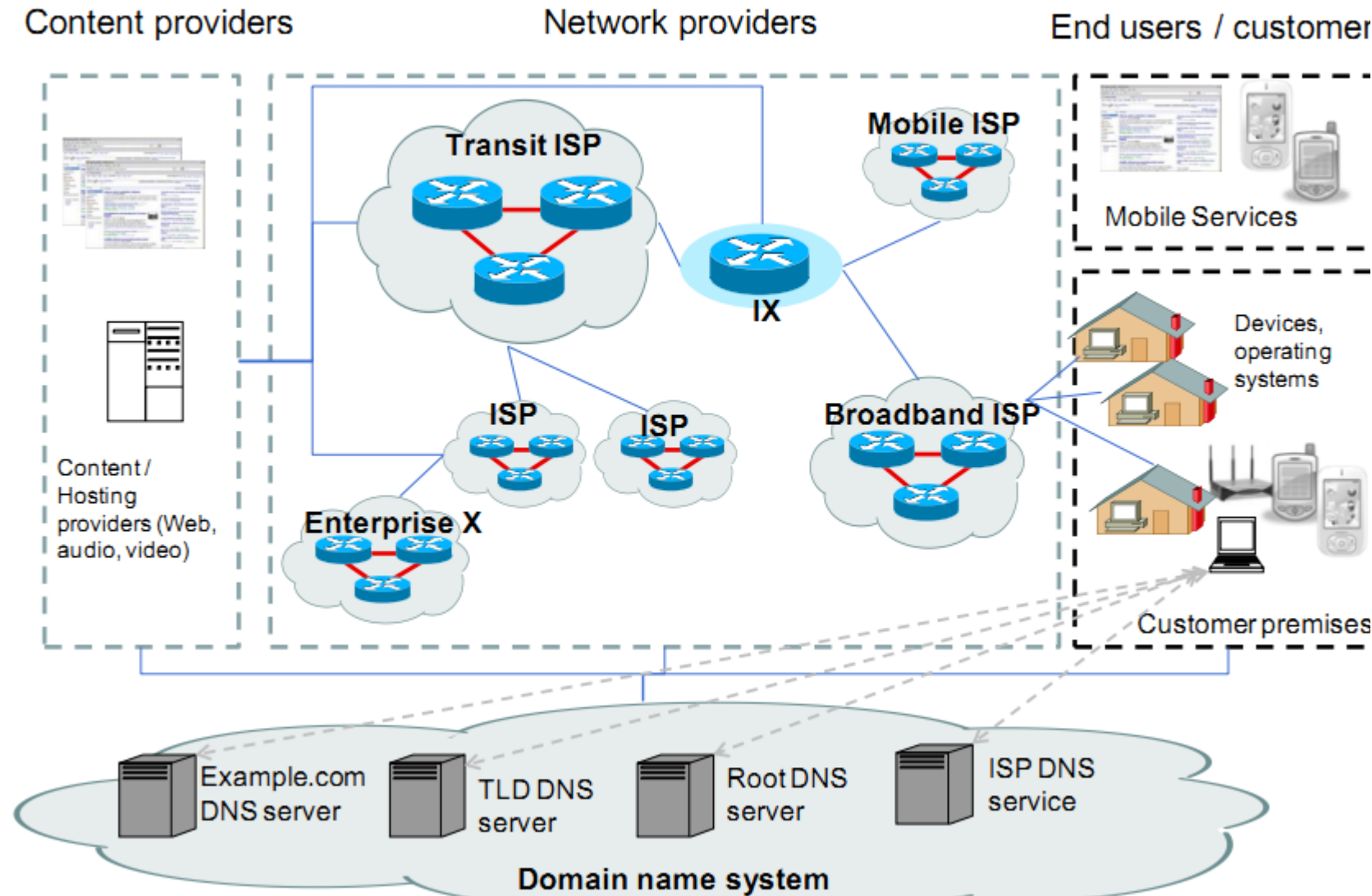
**MORE FROM STEVEN J. VAUGHAN**

- Enterprise Software  
**Ubuntu Linux 18.10 an**
- Google  
**Google Fuchsia: Here' knows about it**
- Microsoft  
**Microsoft's patent mo forward or business a**
- Microsoft  
**What does Microsoft j Open Invention Netwc you?**



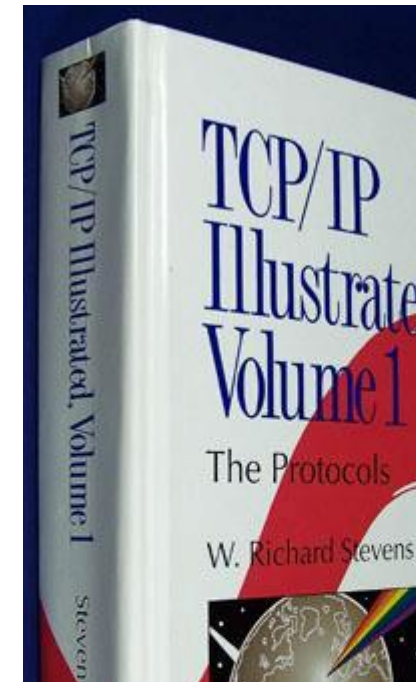
## Grober Überblick

Figure 1. Stylised view of the Internet



- Quelle: <http://www.oecd.org/dataoecd/48/51/44953210.pdf> (April 2010)

- W. Richard Stevens, TCP/IP Illustrated
  - Volume 1, **1994**
  - Volume 2, 1995
  - Volume 3, 1996
- Gutes Referenzwerk
- Allein ~100 Seiten zu TCP



## TCP/IP Schichtenarchitektur

- Auch Internetprotokollfamilie genannt
- DER dominierende Standard und Basis für Kommunikation im Internet
- TCP quasi untrennbar mit IP verbunden, daher seit Ende der 1970er gemeinsame Bezeichnung TCP/IP
- **Ziel:** Eine Vielzahl von Teilnetzen/Subnetzen zuverlässig und günstig miteinander vernetzen

## TCP/IP Schichtenarchitektur

- **Problem:** Internetworking ist Kommunikation über lokale Netzwerke hinaus und muss daher unterschiedliche Infrastrukturen und Techniken transparent und effizient überwinden
- **Idee:**
  - Bildung aufeinander aufbauender Schichten, die der jeweils oberen Schicht über Schnittstellen Kommunikationsdienste anbieten (adjacent layer interaction)
  - Jede Schicht hat eigene Adressierungsverfahren und kann verschiedene Protokolle anbieten/verwenden
  - So wird von physischen Spezifika abstrahiert
  - Einzelne Protokolle können unterschiedliche Bedürfnisse befriedigen (z.B. Geschwindigkeit vs. Korrektheit)



## TCP/IP Schichtenarchitektur

### ■ Übersicht der Ebenen Deutsch/(Englisch)

<b>TCP/IP-Schicht</b>	<b>Beispiel</b>
Anwendungen (Application)	HTTP, FTP, SMTP, IMAP
Transport (Transport)	TCP, UDP
Internet (Internet)	IP (IPv4 und IPv6), ICMP
Netzzugang (Network Access)	Ethernet, Token-Ring, FDDI

## TCP/IP Schichtenarchitektur

- **Anwendungsschicht:** Alle Protokolle, welche von Anwendungsprogrammen direkt verwendet werden und anwendungsspezifische Daten austauschen
- **Transportschicht:** Baut eine Ende-zu-Ende Verbindung auf. TCP tut dies zwischen zwei Teilnehmern mit einer “zuverlässigen“ Doppel-halbduplex-Verbindung. UDP hingegen arbeitet verbindungslos und regelt nur die Zustellung an den richtigen Dienst/Port
- **Internetschicht:** Best effort-Protokoll, das Routing-Mechanismen verwendet, um Hop-by-Hop ein Paket von der Quelle zu Ziel weiterzugeben
- **Netzzugangsschicht:** Gehört zu TCP/IP ist jedoch unterhalb dieser Protokolle. Enthält Best effort Punkt-zu-Punkt Protokolle. Regeln die Übertragung von Daten über verschiedene physische Medien/Techniken

## OSI Schichtenarchitektur

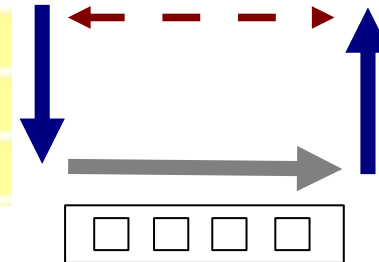
- Auch OSI-Referenzmodell genannt, von der ISO entwickelt
- Hintergrund: TCP/IP ist nicht die einzige schichtenorientierte Protokollfamilie
- Das Modell gibt die konkrete Umsetzung der einzelnen Protokolle nicht vor
- Hin und wieder existieren Probleme auch auf Schicht 8 ;-)

OSI-Schicht	TCP/IP-Schicht	Beispiel
Anwendungen (7)	Anwendungen	HTTP, FTP, SMTP, POP, Telnet, OPC UA
Darstellung (6)	(=OSI 5–7)	
Sitzung (5)		SOCKS
Transport (4)	Transport	TCP, UDP, SCTP
Vermittlung (3)	Internet	IP (IPv4, IPv6)
Sicherung (2)	Netzzugang	Ethernet, Token Bus, Token Ring, FDDI
Bitübertragung (1)	(=OSI 1–2)	

## Encapsulation and Demultiplexing/Decapsulation

### Computer 1

TCP/IP-Schicht	≈OSI-Schicht
Anwendungsschicht	5-7
Transportschicht	4
Internetschicht	3

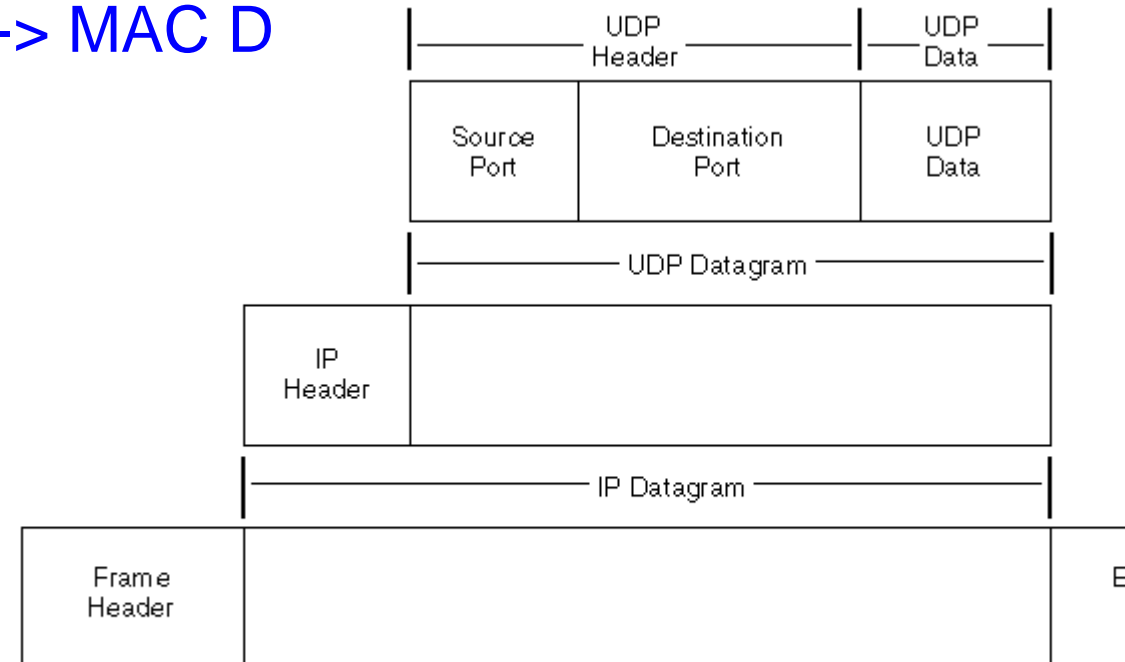


### Computer 2

TCP/IP-Schicht	≈OSI-Schicht
Anwendungsschicht	5-7
Transportschicht	4
Internetschicht	3

Ethernet-Frame: MAC A -> MAC D

- **Demultiplexing:**
- Der Weg zurück,
- jeder Layer entpackt und prüft,
- welches Protokoll des nächsten
- Layers die Daten erhalten muss





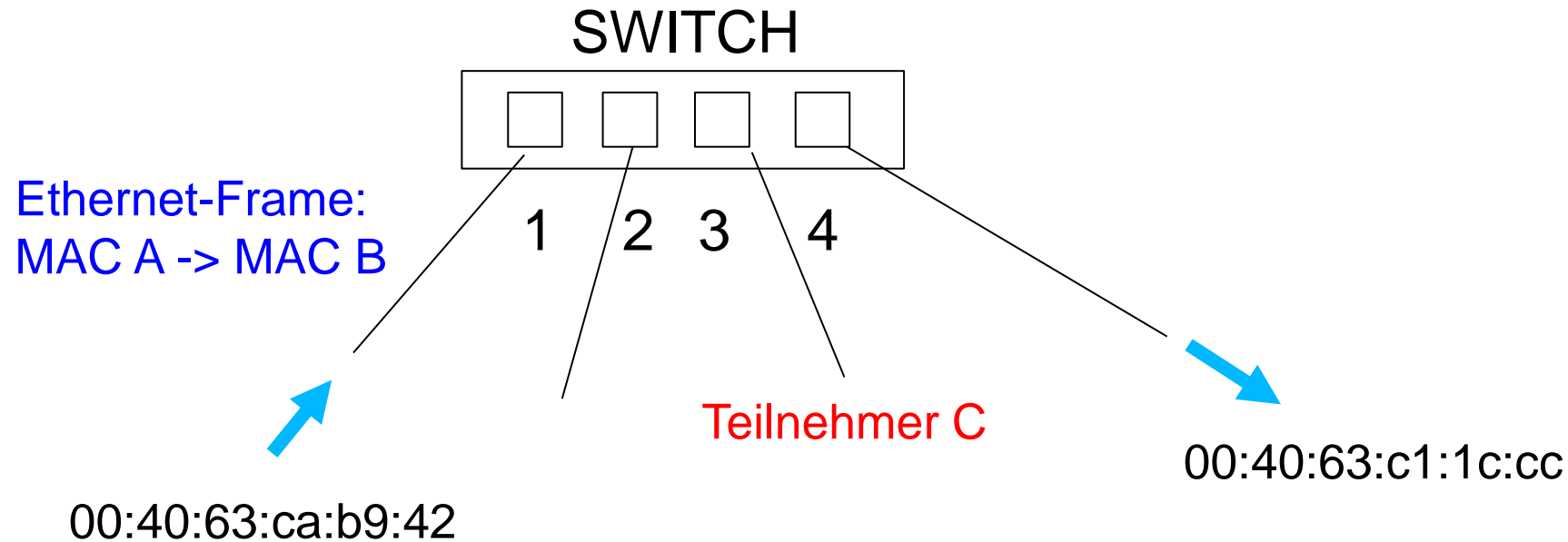
## Begriffe der einzelnen Dateneinheiten

- Netzzugang (Ethernet, PPP, FDDI, ...): **Frame**
- Internet Layer: (IP, ...): **Paket (Datagram)**
- Transport Layer: (TCP, UDP, ...): **Segment**
  
- Nicht immer ist die trennscharfe Unterscheidung notwendig, bzw. wird nicht immer aufrechterhalten. „**Paket**“ ist eine gute Allgemeinbezeichnung.
  
- Weitere Begriffe: Header, Trailer, Payload/**Data**/Body

Weitere wichtige Begriffe

- Knoten: Netzteilnehmer
- Interface: Netzwerkschnittstelle, diese ist Träger von IP-Adressen
- Host: Netzteilnehmer, z.B. PC, meist sind Diensteanbieter gemeint
- Link: Niedrigste Ebene im TCP/IP-Ebenenmodell
- Overhead: Daten, die über die Nutzdaten hinausgehen

## Die wesentlichen Punkte und Hub vs. Switch



- Physische Datenübertragung, Schnittstellen haben Hardware-Adressen (Falsche Freunde: Physical vs. Physikalisch)
- Maximale Nutzdatengröße (1492 bis 1500 Byte, PPPoE/Ethernet)
- Übertragung abgesichert durch CRC
- PPP gehört auch dazu (MTU 1492 bis 296 Byte)

Maximum Transmission Unit (MTU), Path MTU, Path MTU Discovery (PMTUD)

- Maximum Transmission Unit (MTU): Oberstes Limit der Nutzdaten pro Frame im Link Layer
- IP Paket > Frame MTU ? Fragmentierung
- Path MTU: Die kleinste MTU der an einer Kommunikation beteiligten Links (unidirektional, da Routen selbst unidirektional sind → Rückroute kann anders sein als Hinroute)
- Path MTU Discovery: Mechanismus, mit dem ein Netzteilnehmer automatisch die maximal mögliche MTU herausfinden kann
  - IPv4: Paket mit DF-Bit und Größe der lokalen MTU, Auswertung und Berücksichtigung evtl. ICMP-Rückmeldungen “kleinerer” Router

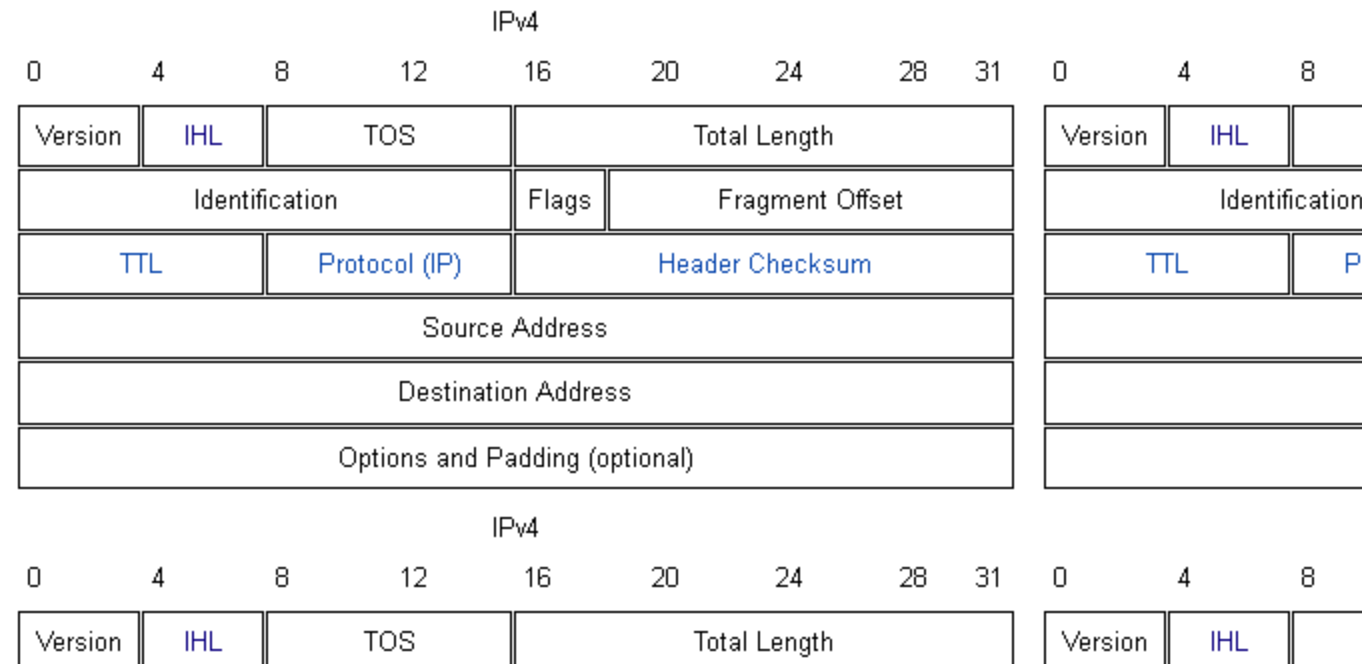


Unzuverlässiger Bursche

- IP übermittelt Pakete **verbindungslos** und **unzuverlässig**
- **Verbindungslos:** Jedes Paket völlig unabhängig von anderen. Insbesondere nicht an Routen gebunden
- **Unzuverlässig:** Best effort, aber keine Erfolgskontrolle, kein Tracking, bei Problemen: Paket entsorgen und nach Möglichkeit ICMP-Meldung zurücksenden
- Ist ein Paket zu groß für den Link Layer, **fragmentiert** IP das Paket. Fragmentierung kann auch mehrstufig/mehrfach erfolgen. Der Empfänger muss dann vor der weiteren Verarbeitung defragmentieren

## Der Header

- 20 Byte plus maximal 40 Byte optionale Felddaten (60 Byte max.)



## Adressierungsschema

- 32 Bit: 11000000 10101000 00000001 00000001
- “Decimal dotted”-Darstellung: 192.168.1.1
- Adresse hat einen **Netz-** und einen **Hostteil**. Netzteil kennzeichnet Netzwerk und Hostteil den darin enthaltenen Host
  - Traditionell: klassenbasiert (Klasse A: 8 Bit Netzwerk, Klasse B: 16 Bit Netzwerk, Klasse C: 24 Bit Netzwerk)
  - Heute: klassenlos und daher variabel
- Kennzeichnung des Netzteils über Netzmaske/Subnetzmaske:
  - 255.0.0.0 oder binär /8 (Schreibweise: 11.0.0.0/8 → **CIDR**)
  - 255.255.0.0 oder binär /16 (Schreibweise: 85.88.0.0/16)
  - 255.255.255.0 oder binär /24 (Schreibweise: 192.168.1.0/24)
  - 255.255.255.224 oder binär /27 (Schreibweise: 85.88.9.160/27)
  - 255.255.255.255 oder binär /32 (Schreibweise: 85.88.9.181/32)

## Adressierungsschema

- Niedrigstes Bit in einem Netz: Netzbezeichnung oder „ID“
  - 192.168.1.0
  - 85.88.9.160
- Höchstes Bit in einem Netz: Broadcast-Adresse
  - 192.168.1.255
  - 85.88.9.191



## Subnetting

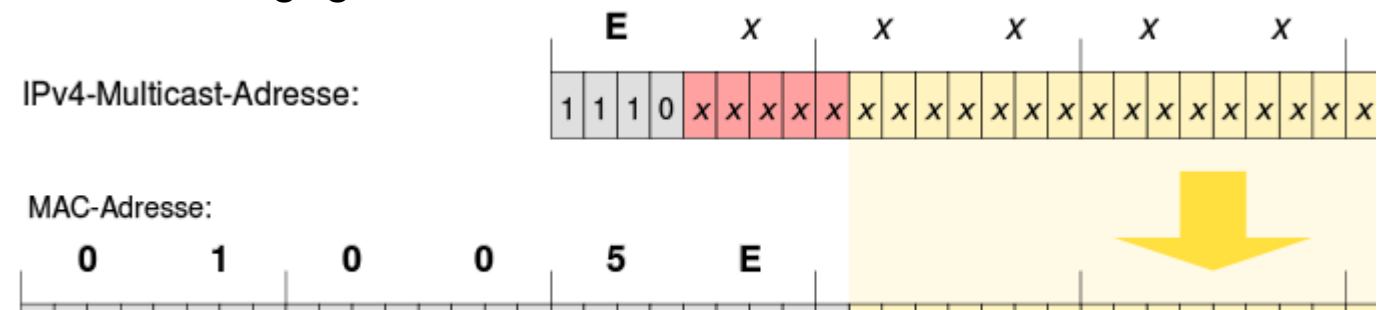
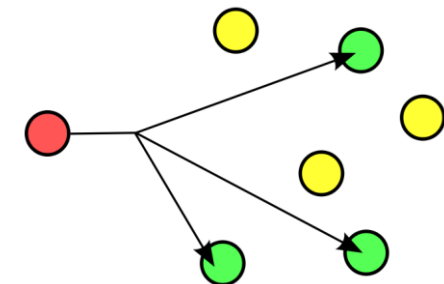
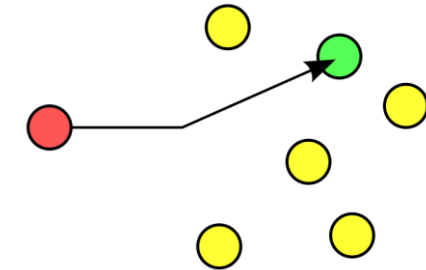
- Traditionell: Beliebig nach dem klassenbasierten Netzwerkteil
- Heute: „Beliebig nach der beliebigen Netzwerkeinteilung“ (Mehrfache Verschachtelung mit Variable Length Subnet Masking {VLSM})
- Idee: “Nach außen” ist ein Netzwerk sichtbar und es muss nur ein Netzwerk adressiert werden. „Innen“ kann dann weiter unterteilt und spezifisch zugestellt werden

## Typen von IP-Adressen

- Global/öffentlich: Alle, die keine spezielle Bedeutung haben und damit global erreichbar sind:
  - 8.8.8.8 (DNS Google)
  - 85.88.9.164 (WWW DigiTrace)
  - 85.88.9.170 (MX DigiTrace)
- Privat
  - Wichtig vorab: “Klasse A/B/C” gibt es nicht mehr -> historische Bezeichnung
    - Klasse A: 10.0.0.0/8 bis 10.255.255.255, 16M Adressen
    - Klasse B: 172.16.0.0/12 bis 172.31.255.255, 16 Netze zu 65K Adressen
    - Klasse C: 192.168.0.0/16 bis 192.168.255.255, 256 Netze zu 256 Adressen
- Link Local: 169.254.0.0/16 für APIPA (Automatic Private IP Addressing)
- ...

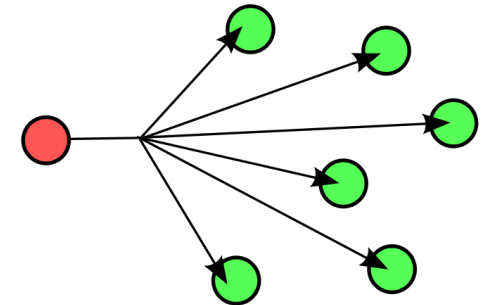
Einer oder einige

- **Unicast:** Zustellung einer Dateneinheit an einen Empfänger
  - IP: 192.168.1.1
  - Ethernet: 00:23:D7:D3:32:62
  - TCP/UDP: Port 80
- **Multicast:** Zustellung an eine Gruppe von Empfängern durch nur ein Paket (spart Bandbreite)
  - Ethernet: 01:00:00:00:00:00
  - IP: Klasse D (224.0.0.0 – 239.255.255.255)
- Grundlage: Ein Paket/Dateneinheit wird von jedem Knoten, der es erhält, ausgewertet und dann entweder im Stack weitergegeben, oder verworfen (Filtering)
- Stichwort:  
**Promiscuous Mode**



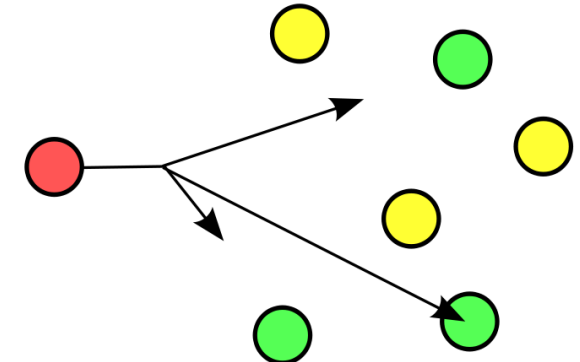
Broadcasting: Alle mal herhören!

- **Broadcasting** als zwingend nötiger und effizienter Weg, alle Teilnehmer eines Netz(teil)bereiches mit einem Datenpaket zu erreichen
- Wird z.B. verwendet von IP:
  - 192.168.1.255 (wird traditionell gerouted)
  - 255.255.255.255 (limited broadcast address für DHCP/BOOTP, wird nicht gerouted)
- Wird z.B. verwendet von Ethernet (FF:FF:FF:FF:FF:FF)
- Broadcasting kann auch von UDP verwendet werden (nicht jedoch TCP)



Einer an mehreren Orten zugleich

- **Anycast:** Eine Gruppe gleicher Server mit
- identischem Datenbestand hat jeweils
- die gleiche IP-Adresse
- Für diese Adresse wird eine BGP-Route propagiert
- Clients wählen die beste Route aus
- Völlig Transparent für Clients
- (Anycast verhält sich aus deren Sicht wie Unicast)
- Verbesserung der Performance und Verfügbarkeit
- Server sind oft für Administration/Wartung per Unicast erreichbar
- Wechselnde Routen, bzw. instabile Routen können zu Datenverlust, bzw. Streuung an verschiedene Server führen!





## Funktionsweise

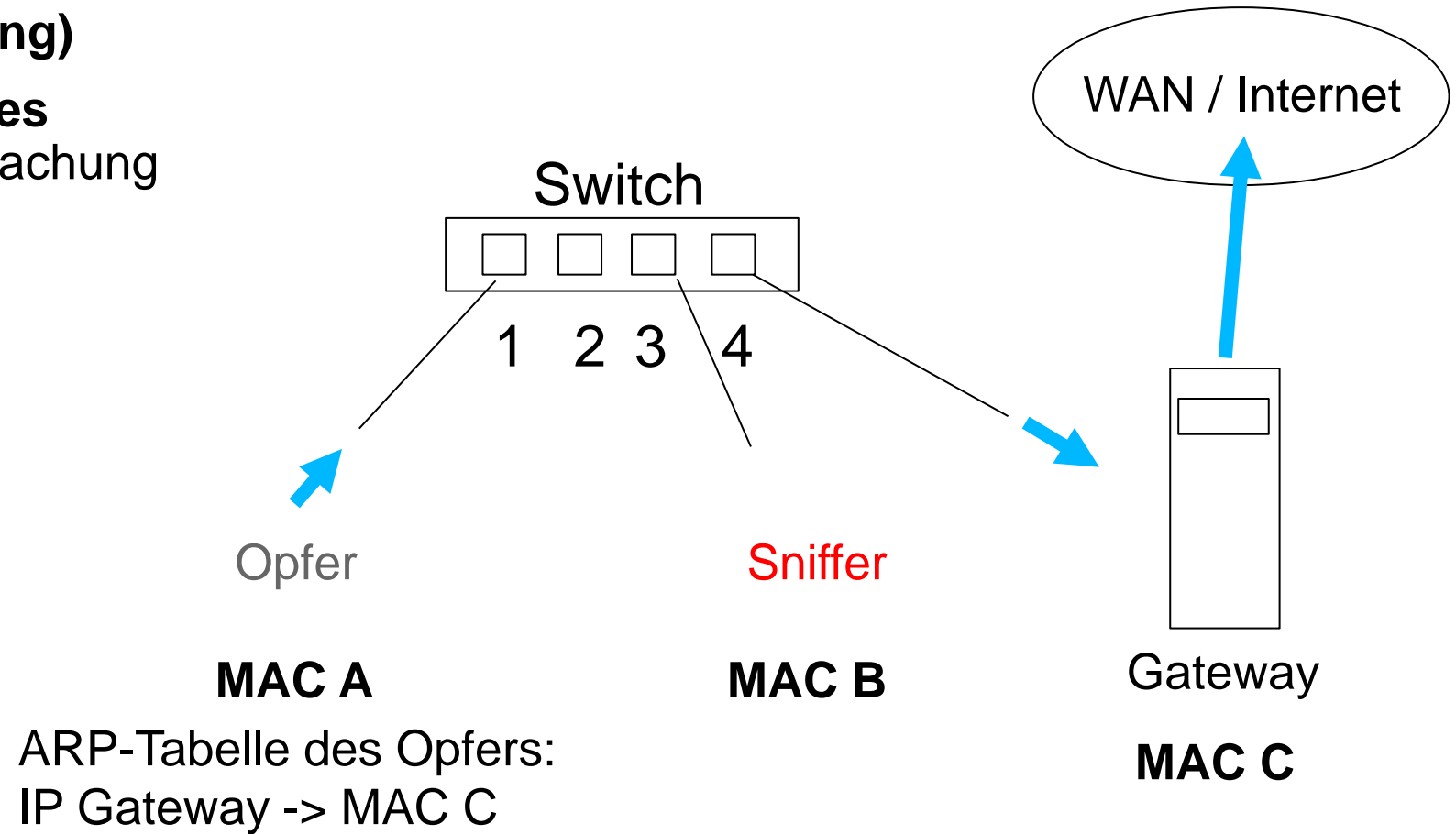
- Adjacent Layer Interaction zwischen Network Access (Layer 4) und Internet (Layer 3)
- **Notwendigkeit:**
  - An welche MAC-Adresse soll ein IP-Datenpaket gesendet werden? Wie können Teilnehmer effizient diese Angaben lernen?
- **Ablauf:**
  - Teilnehmer will zu einer IP-Adresse die MAC-Adresse erfahren und sendet einen ARP Request an die Ethernet-Broadcast-Adresse
  - Alle Teilnehmer empfangen und prüfen, der gesuchte antwortet mit einem ARP Reply (enthält seine IP + MAC) an den Anforderer
  - Anforderer macht nun Eintrag in seiner ARP-Tabelle mit Lifetime x
  - Alle Requestempfänger tragen IP<->MAC des Requesters ein
- Verbindungsloses Protokoll!

## Funktionsweise

- **Proxy ARP:** Transparenter Router, der ARP-Anfragen stellvertretend mit seiner Adresse beantwortet, da zwei seiner Netze den gleichen IP-Adressbereich verwenden
- **Gratuitous ARP:** Host sendet Request mit seiner IP-Adresse als Quelle und zugleich Ziel
  - Antwort? → Adresskonflikt
  - Sonst: Jeder Host im LAN aktualisiert den Eintrag des sendenden Hosts (z.B. Wenn ein Rechner die IP eines anderen übernommen hatte → Redundanz oder Mobile IP-Szenario)
- **ARP Spoofing:** Ein Teilnehmer in einem LAN sendet gefälschte Requests oder insbesondere gefälschte Replies und manipuliert damit den Datenverkehr (DoS oder MITM)

Ein Man in the middle Angriff (MITM)

- „**arpspoof**“ (ARP-Poisoning)
- Gezieltes Manipulieren **eines** einzelnen Hosts zur Überwachung

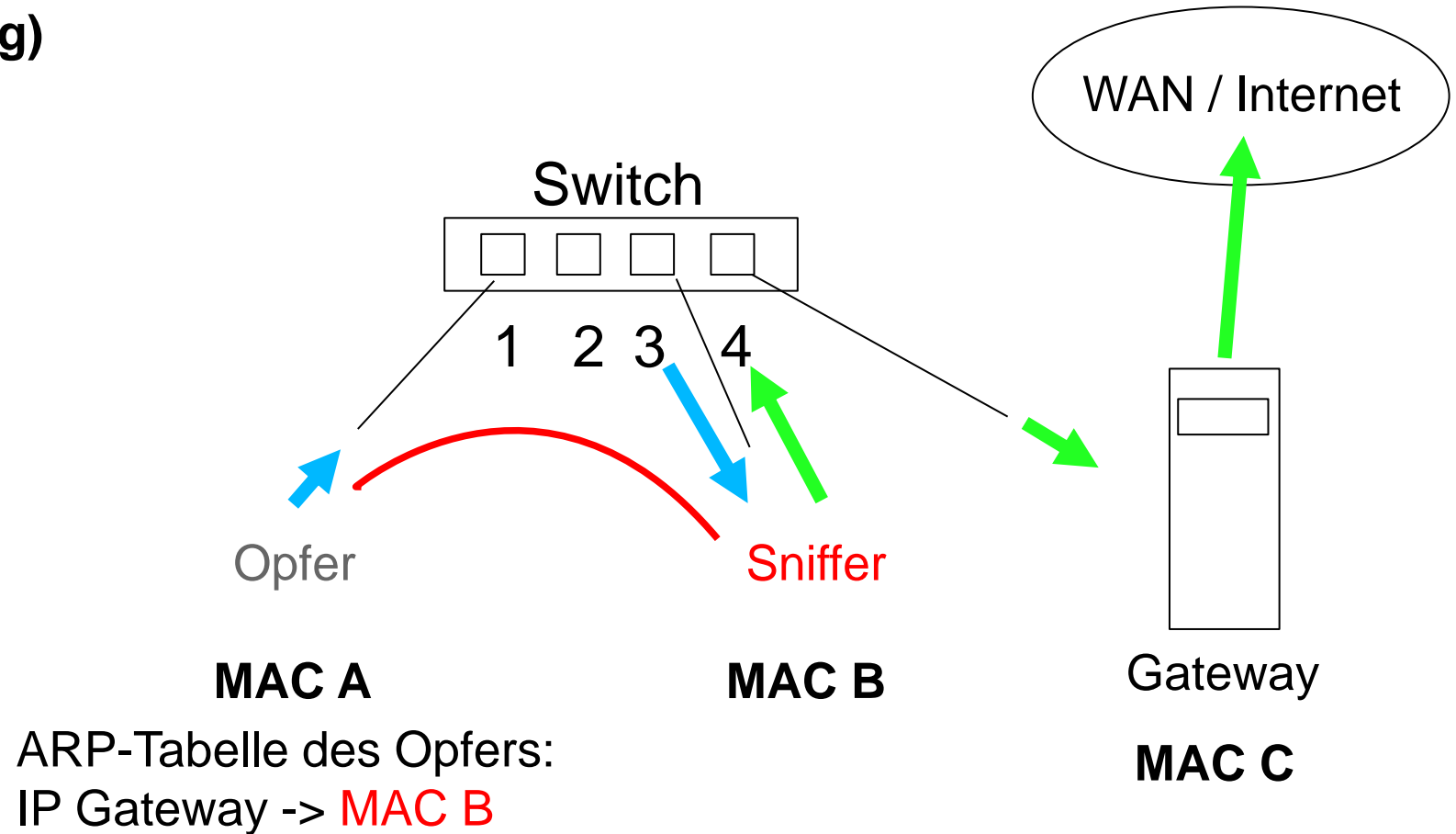


Ein Man in the middle Angriff (MITM)

## ■ „arpspoof“ (ARP-Poisoning)

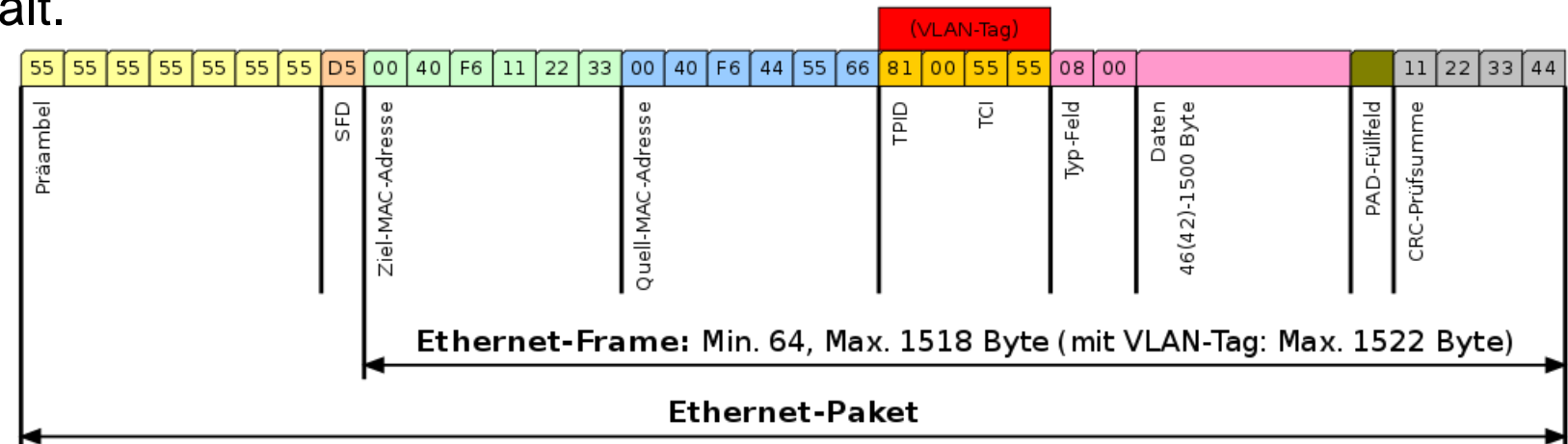
### ■ Fragen (IT-Forensik):

- Fallen Spuren an?
- Welche?
- Über welche Zeit?



## Virtual Local Area Network (VLAN)

- Technik, mit der auf Layer 2 Netztrennung erreicht wird. Dazu wird Ethernet-Paketen eine VLAN-ID hinzugefügt. Diese identifiziert das jeweilige VLAN
- Pro VLAN (analog physisch separiertem Netzwerksegment) eine eigene Broadcast-Domäne. Kommunikation zwischen den VLANs erfolgt dann geroutet auf Layer 3 (IP). Ein Layer-3-Switch kann dies direkt erledigen, sonst ist ein eigener Router nötig
- Häufige Technik: Switch ist VLAN-fähig, weist einem Port ein VLAN-“Tag“ zu, übernimmt VLAN-Stripping und leitet über einen geteilten Port (Uplink) per Multiplexing die Daten mehrerer VLANs an einen Uplink-Router weiter, der selbst VLAN-fähig ist und die Pakete daher ohne Stripping erhält.



Quelle: <https://de.wikipedia.org/wiki/Benutzer:Bluepoke>

## IEEE 802.1X: Konzept

- Standard zur Authentifizierung in Computernetzwerken
- Teilnehmer werden z.B. im WLAN oder an einem Switch-Port an einer zentralen Management-Instanz authentifiziert (Authentifizierungsserver)
- **Authenticator** prüft die übergebenen Credentials (z.B. Zertifikat oder Benutzername:Passwort) und gewährt oder verweigert Zugriff
  - Kann z.B. in einem Switch realisiert sein, der zur Prüfung mit einem zentralen Server (**Authentication Server**) kommuniziert
- Dazu brauchen Clients einen **Supplicant** als Client-Komponente
- Implementierungsbeispiel: Der Authentication Server (AS) teilt je nach Credentials dem Authenticator (hier: Switch) mit, in welches VLAN der Client konnektiert werden soll

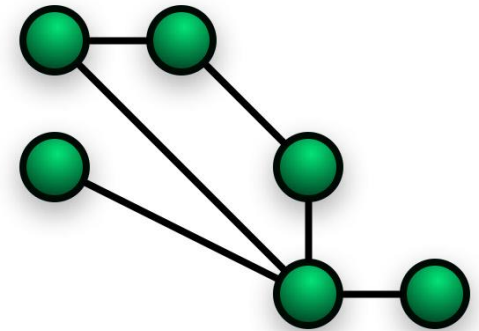


## Network Access Control (hier: Kontrolle von MAC-Adressen)

- Switches und Router werden mit einem zentralen Management-System verbunden
- Dieses führt eine Liste erwünschter MAC-Adressen (White-List)
- Nur diese werden zugelassen
- Unbekannte/Unerwünschte Systeme erhalten einen „toten“ Switch-Port oder werden z.B. einem Gäste-VLAN zugewiesen
- Network Access Control (NAC) generell meint darüber hinaus weitere Techniken, z.B.
  - Agenten auf Clients, die auf Richtlinienkonformität prüfen (aktuelle Software? Unerwünschte Software? Virenbefall?) und Systeme z.B. sperren
  - Quarantäne-Funktion
  - Rollenverteilung
  - Traffic-Analyse mittels Gateway-Appliances
- Kann mit 802.1X kombiniert werden

## Motivation

- Redundanz, Atomkrieg, die große Vision...
- Das Internet besteht aus (eigenständigen) Teilnetzen, die miteinander kommunizieren möchten
- Vermaschte Struktur, keine Vollvermaschung aber Backbones
- Hosts (insb. Router) haben Routingtabellen und verzeichnen dort über welchen Next Hop sie ein jedes relevantes Netz erreichen können
- „**Automatisches Routing**“: Ein multi-homed Host, kennt offensichtlich die Routen zu seinen unmittelbar angeschlossenen Netzen
- “**Routing des kleinen Mannes**“: Alle Pakete an Default Gateway weiterleiten
- **Forwarding**: Entscheidung eines einzelnen Knotens, an welchen seiner Links ein Paket weitergeleitet werden soll. Forwarding und Routing oft gemeinsam mit Routing bezeichnet



Die große weite Welt hinter der FritzBox! ;-)

## ■ Interior-Gateway-Protokolle (IGP)

- Kommunikation innerhalb eines Autonomen Systems
- Routing Information Protocol (RIPv1, RIPv2)
- Open Shortest Path First (OSPF)
- ...

## ■ Exterior-Gateway-Protokolle (EGP)

- Kommunikation zwischen Autonomen Systemen
- Border Gateway Protocol (BGP)

## ■ **Konvergenz** als Zielkriterium neben Redundanz und Routing-Metrik

## ■ Stichworte Classless Inter-Domain Routing (**CIDR**) und Subnetting

## Autonome Systeme (AS), Tier-Level und PI-/PA-Address Space

### ■ Autonomes System (AS)

- Eines oder mehrere IP-Netze mit einem IGP-Routing-Protokoll vernetzt und als Einheit verwaltet
- 16 Bit Identifier (seit einiger Zeit auch 32 Bit)
- Hauptsächlich ISPs, Uni's, große Unternehmen
- Kunden, Peers, Provider
- Stub-AS, Multihomed Stub AS, Multihomed AS, Transit AS

### ■ Tier-1-Provider: Haben nur Kunden und Peers, sind kein Kunde

### ■ Tier-2-Provider: Sind Kunde nur bei Tier-1-Providern, Tier-n: ...

### ■ Provider Independent Address Space (RIR direkt an Enduser)

### ■ Provider Aggregatable Address Space (RIR an LIR an Enduser)

## Netzsegmentierung

- „Flache“ Netzwerke sind häufig nicht mehr zeitgemäß
  - Große Ethernet-Broadcast-Domains
  - Unbeschränkte, direkte Erreichbarkeit von IP-Systemen (oft) unterschiedlicher Schutzstufe -> Clients, Server, Drucker, ...
- Eine Segmentierung auf Layer 2 und insbesondere Layer 3 ist daher eine sehr wirksame (passive) Schutzmaßnahme

## Einführung

- Bestandteil von TCP/IP, wird aber als eigenes Protokoll auf Layer 3 behandelt
- Wird verwendet, um Informations- und Fehlermeldungen mitzuteilen
- „Klassiker“: Ping und Traceroute (ICMP und UDP)
- Auch: Host nicht erreichbar, Port nicht erreichbar, ...
- ICMP-Nachrichten werden in den Datenteil von IP-Datagrammen eingekapselt
- Ein ICMP-Paket löst niemals ein weiteres aus (Ausnahme: ping)

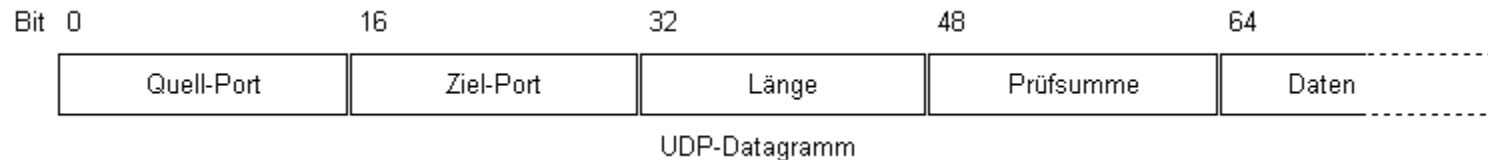


## Ping und Traceroute

- Ping
  - ICMP Echo Request (+ beliebige Daten)
  - ICMP Echo Reply (+ Teilzitat der gesendeten Daten)
  - Daten-Feld kann für ICMP-Tunneling missbraucht werden
- ICMP Traceroute mit ansteigender TTL, jeder Router bis zum Ziel sollte dann einen ICMP Time Exceeded zurück schicken

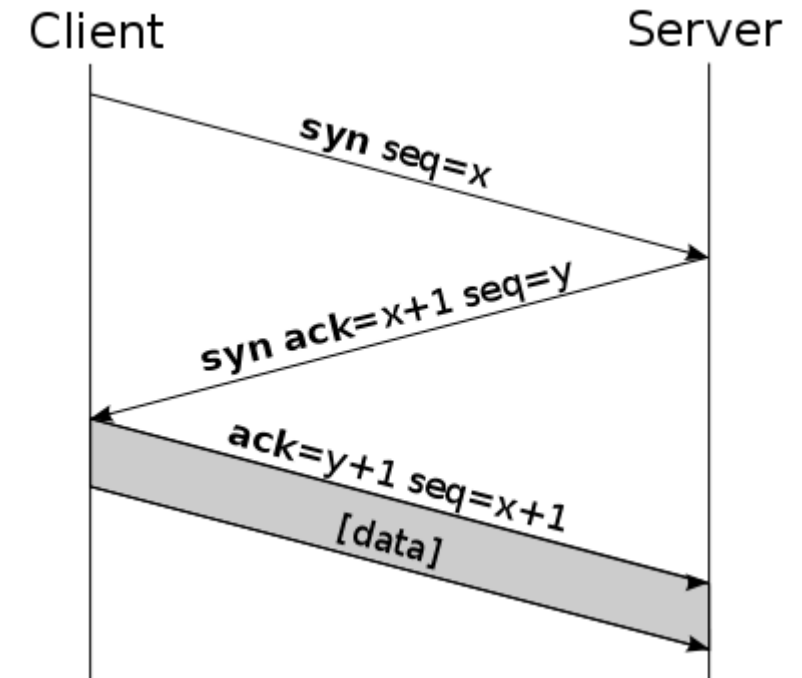
## Das „schlanke“ Paket

- UDP ist ein Protokoll der Transportebene
- Auf das Wesentliche reduziert und „nicht zuverlässig“
- Verbindungslos, es muss insbesondere keine Verbindung auf- oder abgebaut werden
- Die Datenübertragung ist nicht gesichert (Aufgabe der Anwendungsschicht)
- Wird z.B. bei VoIP und DNS verwendet



## Konzept

- Verbindungsorientiertes Protokoll für Kommunikation zwischen zwei Sockets (Zwei Endknoten einer Verbindung)
- TCP ist verbindungsorientiert, zuverlässig, paketvermittelnd und erkennt und verhindert Congestion
- Ende-zu-Ende-Verbindung in Vollduplex (Doppel-Halbduplex)
- Noch immer Gegenstand aktiver Forschung (z.B. Congestion)
- Verbindungen müssen aufgebaut und abgebaut werden
- Laufende Verbindungen werden kontinuierlich überwacht, Segmente werden bestätigt, ...



## Angriffstechniken: SYN-Flooding

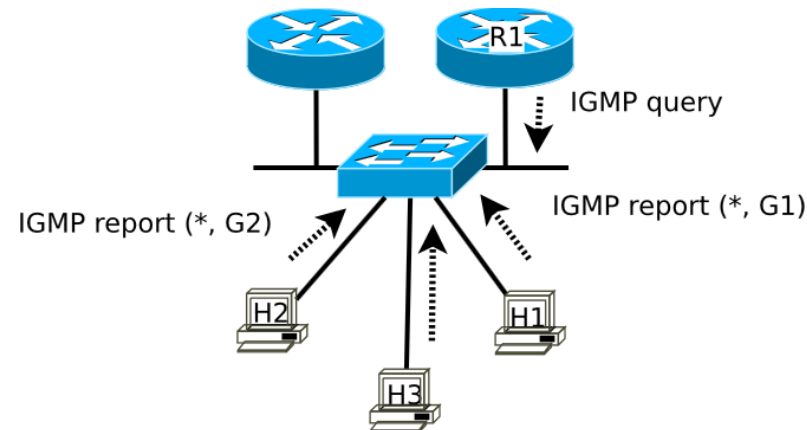
- Denial of Service-Angriff
- Angreifer greift in der Rolle des Clients einen Server an
- Client sendet ein SYN-Paket
- Server antwortet mit SYN+ACK-Paket und wartet nun auf ein ACK-Paket vom Client
- Der Client sendet kein ACK-Paket, sondern baut einfach direkt eine neue Verbindung auf
- Und wiederholt dies so oft wie möglich in kurzer Zeit parallel
- Möglicher Schutz insbesondere SYN-Cookies (Idee von Daniel Bernstein)

## Angriffstechniken: Covert Channels

- „Netzwerkverkehr lügt nicht“ – was aber, wenn ein Angreifer Informationen in einer TCP-Verbindung versteckt?
- Covert Channels ermöglichen die Ausleitung von Daten durch Einbetten in TCP-Verbindungen
- Idee z.B.: Covert channels in the TCP/IP protocol suite | Rowland | First Monday
- Idee für bi-direktionale, passive Covert channels:  
<https://events.ccc.de/congress/2004/fahrplan/files/319-passive-covert-channels-slides.pdf>
- Diese Technik funktioniert – analog der Steganographie – auch in (beliebigen) anderen Protokollen

## Kurzüberblick

- Gehört zu IP und ist „verortet“ wie ICMP
- Wird verwendet für Verwaltung/Organisation von Multicast-Gruppen
- Netzteilnehmer teilen mit IGMP Ihren Routern mit, dass sie Multicast-Traffic erhalten wollen



- Quelle: Wikipediauser „Mro“



Auflösung von Namen zu Adressen und etwas mehr

- Hierarchisches dezentrales System, zentraler und kritischer Dienst des Internet
- Weltweit gibt es tausende DNS-Server, die für einzelne oder mehrere Zonen und Domains zuständig sind
- Löste 1983 die statischen hosts-Tabellen ab
- Wesentliche Funktionalität:
  - Namensauflösung (Stichwort Fully Qualified Domain Name - FQDN)
  - Umgekehrte Auflösung (reverse DNS, RDNS)
  - Sender Policy Framework
  - MX-Server propagieren
- 13 Root Server (A bis M) sind in statischen Dateien der Netzteilnehmer fest erfasst und werden iterativ befragt (z.B. Delegation an .de-Server, dieser dann an digitrace.de-Server)

## Angriffstechniken

- DNS hat eine essentielle Bedeutung für das Internet
- Kommunikation erfolgt bis heute hauptsächlich im Klartext und ohne wirksamen Integritätsschutz
- Motivation für Angreifer z.B.: Opfer (ungerichtet/gerichtet) auf falsches Ziel umleiten, z.B. eigenen Server und dann Man-In-The-Middle-Angriff durchführen
- DoS-/DDoS-Angriffe werden durchgeführt um DNS-Server lahmzulegen
- DNS-Spoofing
- Cache Poisoning
- Ausnutzen von DNS-Servern, die unvorsichtigerweise eine komplette Zone auf Anfrage mitteilen (z.B. DNS-Server einer Firma)

## Schutztechniken

- Hauptsächlich kryptographische Absicherung, Datenübertragung z.B. per TLS gesichert
- DNSSEC
- ...

## NAT/PAT

- **Allgemein:** Funktion in Routern, die Angaben in Paketen ersetzen, damit diese Pakete bestimmte Netzwerkhürden überwinden können
- **Source NAT:** Router tauscht interne Absenderadresse gegen eigene externe Adresse und stellt das Paket zu. Antwortpaket wird zurückübersetzt
- **Destination NAT:** Router tauscht die von extern angesprochene interne Adresse gegen eine andere interne Adresse. Antwortpaket wird zurückübersetzt
- **Port Address Translation (PAT):** Meist NAT-Bestandteil (NAPT), da bei mehreren NAT-Verbindungen sonst Port-Kollisionen entstehen können
- **NAT Table:** Router halten intern eine Zuordnungsabelle
- „**Demilitarisierte Zone (DMZ)**“

## NAT/PAT

### ■ Vorteile:

- Eine/Wenige externe/globale Adressen für viele interne
- Basissicherheit

### ■ Nachteile:

- Kein Ende-zu-Ende mehr
- Schwierigkeiten mit IPSec
- „Ende-zu-Ende-NAT“ macht Schwierigkeiten

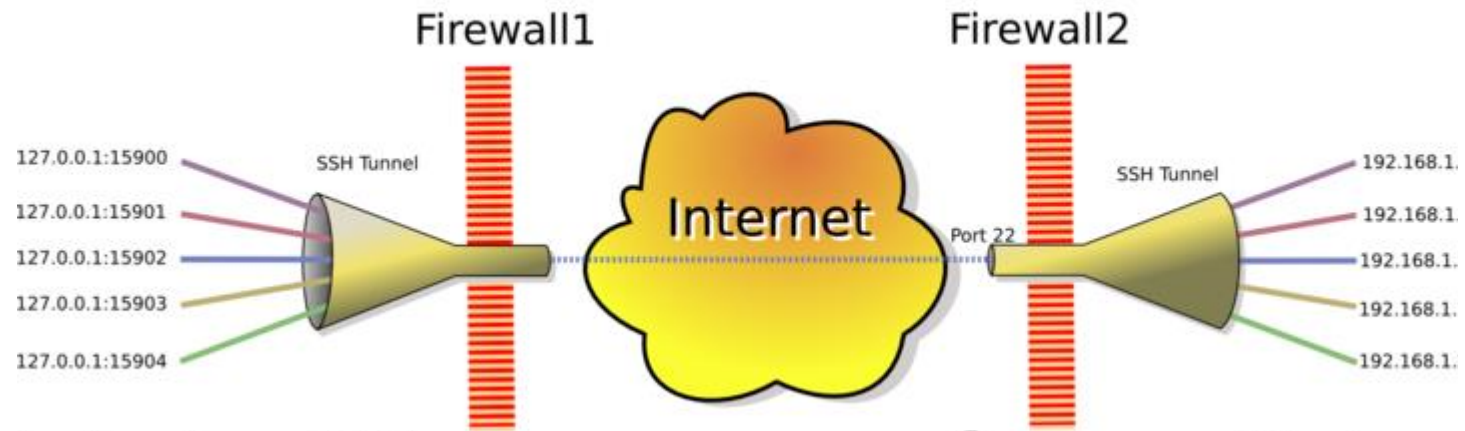
- **NAT-Traversal:** Überwindung der Schwierigkeit, wenn bei Kommunikationspartner hinter einem NAT-Gateway sind. NAT-Traversal versucht Ende-zu-Ende z.B. über einen zentralen Server im Internet durch Vermittlung zu ermöglichen

- **Hole Punching:** Verbindungsvermittlung durch externen Vermittler, dieser gibt die Sitzungsdaten an den jeweiligen Endpunkt weiter

## Tunneling

- Salopp formuliert: Das eine Protokoll wird in das andere eingebettet, der Empfänger/Gateway entpackt das innere Paket und verarbeitet es dann weiter
- Wichtig für Migration: 6to4, 6in4, Teredo, ISATAP, ... (IPv6)
- „Der“ Klassiker: Akustikkoppler
- HTTP Tunnel, OpenSSH, OpenVPN, PuTTY, Hamachi, DNSTunnel, ...

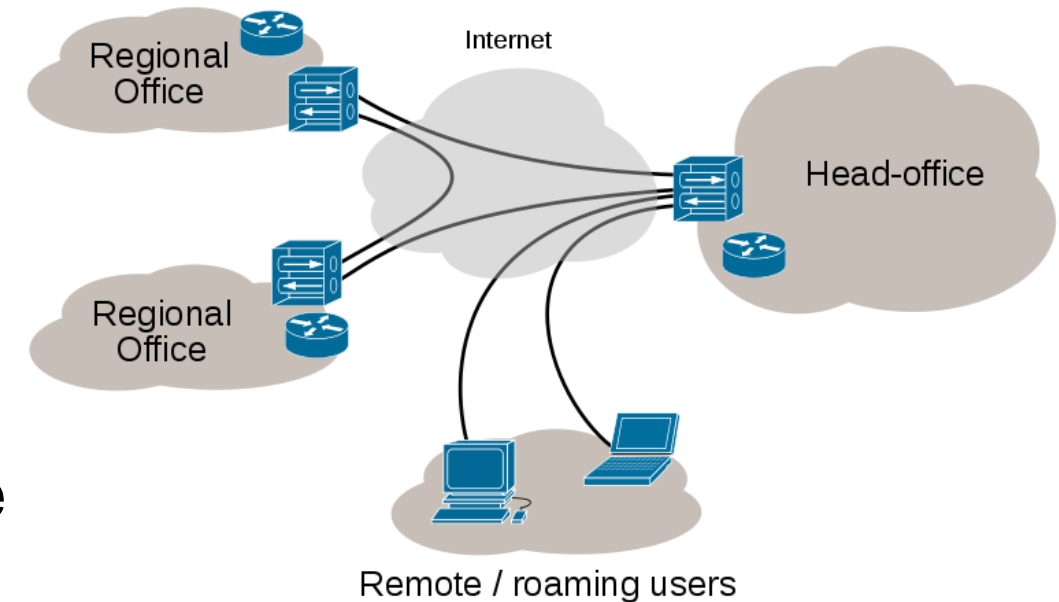
## Veranschaulichung SSH Tunnel



Quelle: Wikipediabbenutzer "Christian Mueller h07bc10@gmail.com"

## Grundüberlegungen

- Technik, die ein abgegrenztes Netzwerk transparent über ein anderes Netzwerk legt
- Teilnehmer des abgegrenzten Netzwerks erfahren u.U. nichts vom Trägernetz (“Verlängerungskabel”)
- Verschlüsselungstechniken werden verwendet, um die VPN-Daten abhör- und manipulationssicher durch ein (unsicheres) Trägernetz zu tunneln
- Durch vollständige Kapselung kann die Kommunikation an sich „versteckt“ werden, ansonsten nur die Nutzdaten
- Site-to-Site, End-to-Site, End-to-End



- Quelle: Wikipediabnutzer „Ludovic.ferre“



## Definition

- Virtual Private Network (Virtuelles Privates Netzwerk)
- Es handelt sich um ein Netzwerk, welches ein anderes (öffentliches) Netzwerk nutzt, um durch dieses private Daten zu transportieren
- Eigenschaften wie Vertraulichkeit oder Integrität sind streng genommen optional
- Öffentliches Netz:
  - Ist jedem zugänglich
- Privates Netz:
  - Sind nur einem definierten Kreis zugänglich
  - Gemietete Netze und Verbindung jedoch unter der Kontrolle des Dienstleisters

## Definition

- Die logische Verbindung des privaten Netzes durch das öffentliche wird Tunneling genannt
- Die Kernaufgabe eines VPN ist also, sicherzustellen, dass die Pakete vom richtigen Sender zum richtigen Empfänger gelangen

## Motivation

- Kostengünstige Möglichkeit bestehende (öffentliche) Netze für vertrauliche, geschäftskritische Bedürfnisse zu nutzen
- Sichere, vertrauliche Anbindung externer Teilnehmer an eigene Netze (B2B, Filialen, SOHO, Mobilgeräte, ...)
- Steigerung der Sicherheit und Vertraulichkeit gegenüber Festverbindungen/Standleitungen

## VPN-Tunneling

- Wie kann eine private und sichere Kommunikation erreicht werden?
  - Alternative 1:
    - Gesamtes Paket verschlüsseln
    - Router können Informationen im Paket-Header nicht mehr einsehen und daher nicht mehr passend forwarden
  - Alternative 2:
    - Gesamtes Paket bis auf Header verschlüsseln
    - Quell- und Ziel-Adresse können jetzt von Routern für Routing eingesehen werden...
    - ...aber auch von Angreifern
  - Lösung:
    - Das gesamte Paket verschlüsseln und in ein neues Paket mit neuen Transit-IPs einbetten -> Tunneling

## VPN-Split-Tunneling

- Split-Tunneling ermöglicht Datenverkehr an dem (sicheren) Tunnel vorbei ins Internet
- Sollte im VPN-Client nicht vom Endanwender konfigurierbar sein
- Denn der Client stellt sonst eine Brücke zwischen internem (VPN-)Netz und dem Internet her.
- Datenaustausch sollte also ausschließlich über den Tunnel laufen
- Ausnahme: Kommunikation des Clients mit dessen internen Netzgeräten (z.B. Druckserver)

## Grundlagen

- IPSec ist ein Verschlüsselungs- bzw. allgemein Sicherheitsprotokoll der TCP/IP-Familie im Internet Layer
- Fester Bestandteil von IPv6 und „Backport“ in IPv4
- *„IPsec war eine große Enttäuschung für uns. In Anbetracht der Qualifikation der Leute, die daran gearbeitet haben, und der Zeit, die dafür aufgebracht wurde, haben wir ein viel besseres Ergebnis erwartet.“*

Bruce Schneier, Niels Ferguson : A Cryptographic Evaluation of Ipsec (S. 1, Abs. 2)

- **Transportmodus:**
  - Für Host-to-Host und Host-to-Router
  - IPSec-Header zwischen IP-Header und Payload
- **Tunnelmodus:**
  - Besonders sinnvoll bei Gateway-zu-Gateway (P2P auch möglich)
  - Vollständige Kapselung des ursprünglichen Pakets

## Grundlagen

- **Authentication Header (AH):** Sichert das gesamte Paket durch Hash gegen Manipulation
- **Encapsulated Security Payload (ESP):** Sichert die Payload (incl. TCP) mit einem Hash, zusätzlich wird verschlüsselt
- **Internet Key Exchange (IKE):** Regelt den Schlüsselaustausch
- Probleme bei NAT



## Grundlagen

- Software (Client und Server) zur Erstellung eines VPN und zum Verbinden mit einem VPN
- Open-Source
- Nutzt TLS (z.B. mittels openssl)
- Entwickler: OpenVPN Technologies, Inc.
- Bietet Authentifizierung mittels Pre-shared Key oder Zertifikaten



**Zitat:**

```
<Elch> Du kennst dich ja voll mit Rechner aus.  
<bitchchecker> halts maul ich hack dich  
<Elch> ok, ich bin ja schon ruhig, nicht dass du uns zeigst was für  
ein toller Hacker du bist ^^  
<bitchchecker> sag mir deine netzwerk nummer man dann bist du  
tot  
<Elch> öhm die ist 129.0.0.1  
<Elch> oder war es 127.0.0.1  
<Elch> ja genau die war es: 127.0.0.1 Ich warte dann mal auf einen  
dollen Hackerangriff  
<bitchchecker> in fünf minuten ist deine fest platte gelöscht  
<Elch> Da habe ich jetzt aber Angst  
<bitchchecker> halts maul du bist gleich weg  
<bitchchecker> ich hab hier ein program da gebe ich deine ip ein  
und du bist tot  
<bitchchecker> sag schon mal auf wieder sehen  
<Elch> zu wem?  
<bitchchecker> zu dir mann  
<bitchchecker> buy buy  
<Elch> Ich zitter schon förmlich vor einem so krassen Hack0r wie du  
einer bist  
* bitchchecker (~java@euirc-61a2169c.dip.t-dialin.net) Quit  
(Ping timeout#)
```

Quelle: <http://www.stophiphop.com/modules/news/article.php?storyid=184>

## Was ist neu?

- Wer IPv4 kennt, kommt auch mit IPv6 zurecht!
- Neue, größere Adressen
- Kein Broadcast mehr, stattdessen viele Typen von Multicast
- Kein ARP mehr, stattdessen Neighbor Discovery
- Autokonfiguration
- Interface-ID enthält Hardware-ID oder Zufalls-ID
- Änderungen am Header, ICMPv6, leichte Änderungen an UDP und anderen Upper Layer Protokollen, DHCP ziemlich umgekrempelt
- Mobile IPv6
- Umfangreiche Tunnelingmechanismen für Übergang von v4 zu v6
- IPSec und Quality of Service (QoS) bereits in IPv4 enthalten/möglich

## Entwicklungsgeschichte

- Anfang der 1990er: Internet Engineering Task Force (IETF) beginnt mit der Entwicklung eines Nachfolgeprotokolls (mehrere Ansätze parallel)
- **Januar 1995:** RFC 1752 „The Recommendation for the IP Next Generation Protocol“
- Bezeichnung: IPng (Internet Protocol next Generation)
- 1994: Untersuchung, ob Zeit für Entwicklung eines Protokolls mit neuer Funktionalität, oder ob Zeit zu knapp und daher dringende Notwendigkeit für Protokoll mit lediglich größerem Adressraum
- Vermutung: **Adressen reichen bis 2005 oder 2011** → Gründliche Neuentwicklung
- 1996-2006: 6Bone als ältestes v6-(Test)-Netzwerk mit 1.000 Hosts in 50 Ländern
- **1998: Standardisierung der IPv6 Core-Funktionalität**
- 2001: 6to4, Nokia präsentiert erstmalig Mobile IPv6
- 2003: DHCPv6
- 2004: Mobile IPv6, Nokia zeigt erstes Videotelefonat über Mobile IPv6

## Adressierungsschema

- 2001:4dd0:f9cd:1:5d0:8a59:38bb:83f9
- Definiert in RFC 4291
- Adressraum von  $2^{128}$  = 128 Bit = 16 Byte = 8 “2-Byte-Päckchen”
  - 340.282.366.920.938.463.463.374.607.431.768.211.456
  - $\approx$  340 Sextillionen mögliche Adressen
  - Zum Vergleich IPv4: 4.294.967.296
  - Davon rund 74% im Besitz der USA
  - Die University of California besaß 2004 so viele IPv4-Adressen wie ganz China...  
([http://www.chinadaily.com.cn/english/doc/2004-12/27/content\\_403512.htm](http://www.chinadaily.com.cn/english/doc/2004-12/27/content_403512.htm))

## Adressierungsschema

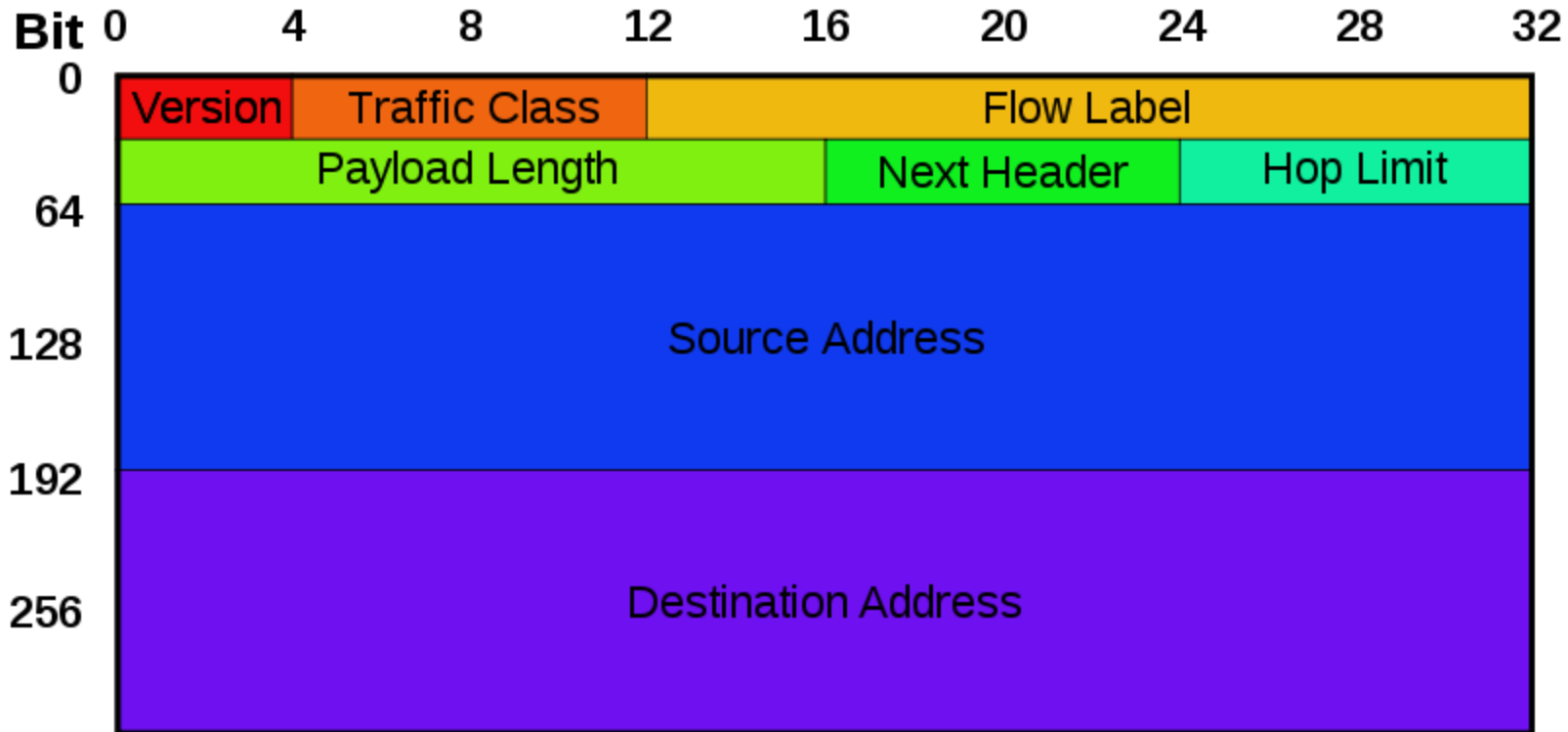
- **2001:4dd0:f9cd:0001:5d0:8a59:38bb:83f9**
- **Provider** bekommen von ihrer RIR (meist) ein /32er-Netz
- Und geben ihren **Kunden** davon /48er-, /56er- oder /64er-Netze
  - Ein /48er Netz ermöglicht dem Kunden, selbst 65.000 **Subnetze** zu bilden
- Die letzten 64 Bit sind **immer** die **Interface-ID**

## Adressierungsschema

- Hex-Schreibweise, Case InSeNsITivE (aber Konvention [RFC5952]: Kleinschreibung)
- 8 Blöcke mit je 16 Bit, bzw. je 2 Byte
  - **2001:4dd0:f9cd:1:5d0:8a59:38bb:83f9**
  - Trennung durch Doppelpunkt
  - mehrere aufeinander folgende Null-Blöcke können ausgelassen und durch einen zweifachen Doppelpunkt ersetzt werden
  - Die Verkürzung darf jedoch nur einmal durchgeführt werden
    - 2001:0db8:0000:0000:1234:0000:0000:2342 =
    - 2001:0db8::<1234:0000:0000:2342 **oder**
    - 2001:0db8:0000:0000:1234::<0350:2342 (nicht RFC5952-konform)
  - Führende Nullen in einem Block dürfen weggelassen werden
    - 2001:0db8:0000:0000:0000:0000:0350:2342 =
    - 2001:db8::350:2342



## Header



Quelle: Wikipediabnutzer Mro

- Feste Größe von 40 Byte (v4: 20 – 60 Byte)
- Auslagerung seltenerer Optionen in “Extension Headers”,
- etwa Fragmentierung (v4: Direkt im Header)
- Keine Header Checksum (v4: Ja, historisch)

## Interface-ID

- **Globale Unicast-Adresse:** 2001:4dd0:f9cd:1::100/64
- [ n Bit: Global Routing Präfix ] [ 64 – n Bit: Subnet ID ] [ 64 Bit: Interface ID ]
- Als ISP-Kunde erhält man oft /48er-Adressbereiche und damit ~65.000 Subnetze
- **Interface-ID:**
  - Muss eindeutig sein
  - EUI-64, modified EUI-64 (invertiertes 7tes Bit)
  - kann dazu die MAC-Adresse enthalten, **muss aber nicht**
  - Erstellung:
    - MAC: 00:05:A8:C5:42:23
    - Interface ID: 02:05:A8:FF:FE:C5:42:23 (modified EUI-64)
  - **Address Privacy** als Schutzmaßnahme → Zufällige ID-Generierung (RFC 4941)
  - → per default aktiv seit Windows Vista, also eigentlich überall!

## Wesentliche Neuerungen in Upper-Layer-Protokollen

- IPv6-Auswirkungen auf höhere Protokolle sind **insgesamt minimal**
- Wesentliche Änderungen dort, wo Upper Layer direkt IP-Adressen und IP-Spezifika verwenden
- **UDP**: Prüfsumme nicht mehr optional, sondern Pflicht; zur Berechnung ein neuer IPv6-Pseudoheader
- **DHCP**-Konfiguration nun „Stateful Address Autoconfiguration“ genannt. Nicht kompatibel zu DHCPv4. Deutliche Anpassungen (geht über diesen Workshop hinaus).
  - Aber Bedeutung für **IT-Forensik**: Jeder DHCP-Client und jeder DHCP-Server hat eine „DHCP Unique Identifier Number“ (**DUID**)
- **FTP**: EPRT statt PORT, EPSV statt PASV
- **Browser**: `http://[2001:4dd0:f9cd:1::100]`

## Integration mittels Dual-Stack

- Moderne Systeme verfügen parallel über IPv4-Stack + IPv6-Stack
- Programme sind dann dual-fähig (z.B. Web-Server)
- Oft: IPv4-Konfiguration inkl. DNS-Server per DHCPv4 und IPv6 per Router Advertisement
- Je eine Firewall/Firewall-Ruleset pro Protokoll notwendig
- Frage: welche (grundsätzlichen) IT-Sicherheitsrisiken drohen bei Einführung eines weiteren Netzwerkstacks auf einem Host?

## Translation- und Proxytechniken

- Carrier Grade NAT64 und NAT46 (unvermeidlich und problematisch → insbesondere Sippenhaft-Effekte bei Missbrauch; Multichannel-Protokolle mit eingebetteten Ports und Adressen funktionieren nicht mehr; Latenz!; Multicast; Geolocation; **eingehende Verbindungen**; FTP und P2P funktionieren nicht mehr, Skalierungsprobleme, ...)
- Carrier Grade NAT44 (Sippenhaft-Effekte, wird schon bei Mobilfunk Providern gemacht und Vergleichbar bei Zwangsproxys, ...)
- Dual-Stack lite: v6-Adresse + private v4-Adresse und CG-NAT44 auf öffentlichen v4-Adresspool
- Web-Gateways
  - ~~Beispiel SixXS-Web-Gateway (<http://www.sixxs.net/tools/gateway/>)~~

## Sicherheitsaspekte bei Integrationszenarien

- Viele Netze sind noch ausschließlich auf IPv4 eingestellt (insbesondere SOHO-LANs)
- Win Vista/7/8/10 können durch aktive IPv6-Funktionen (warten auf Router Advertisements, Tunnel) plötzlich und unvorbereitet ein IPv6-Loch in ein Netzwerk schlagen
- Zwei parallele „Welten“ müssen übereingebracht werden
- Zwei Firewalls/Firewall-Sets notwendig (IPv4 + IPv6)
- Vorteil: Subnet-Scanning deutlich bis unendlich schwieriger (IPv4 Klasse C: 254 Hosts, IPv6: 64 Bit für /64er Netz)

Wiederkehrende, vorlesungs- und übungsbegleitende Übungsaufgabe

- Überarbeiten Sie (als Hausaufgabe) Ihre Planung für die Errichtung einer „smarten“ Einbruchmeldeanlage 2.0 für das Handwerksunternehmen Ihrer Eltern
- Beantworten und begründen Sie unter eigenen Annahmen z.B. folgende Fragen:
  - Ändern Sie Ihre bisherige Planung?
  - Mit welcher Technik werden Sie Ihre EMA wie vernetzen? Anschluss an das LAN? Von Außen erreichbar? Wenn ja: wie?
  - Wie wollen Sie Ihre EMA auf Netzwerkebene absichern?
  - Skizzieren Sie mögliche Problemstellen. Wo könnten Probleme lauern?

Mittels ARP-Spoofing einen Denial-Of-Service-Angriff durchführen

- arpspoof
- ACHTUNG:
  - Verwendung ist grundsätzlich illegal
  - Z.B. Erschleichen von Leistungen

