Zusammenfassung Computernetzwerk

Inhalt

[1 Layer 1 – Medien- und Zugriffverfahren 1](#_Toc436802413)

[2 Layer 2 – Switching 1](#_Toc436802414)

[3 Layer 3 – Vermittlungsschicht 2](#_Toc436802415)

[3.1 Adressen 2](#_Toc436802416)

[3.1.1 Adressklassen 2](#_Toc436802417)

[3.2 Subnetze 2](#_Toc436802418)

[3.3 Segmentierung der Netze – Die Netzmaske 3](#_Toc436802419)

[4 DNS, DHCP, Multicast 4](#_Toc436802420)

[5 Layer 4 – Ports, Sockets, TCP, UDP, Firewall 4](#_Toc436802421)

[6 VLAN-Konzepte 4](#_Toc436802422)

[7 VPN-Konzepte 5](#_Toc436802423)

[7.1 Split Tunnels 5](#_Toc436802424)

[7.2 Verschlüsselung 5](#_Toc436802425)

[7.3 IPSec 6](#_Toc436802426)

[8 WLAN, Funknetze, VoIP 7](#_Toc436802427)

[9 Szenarien von Netzzugängen 7](#_Toc436802428)

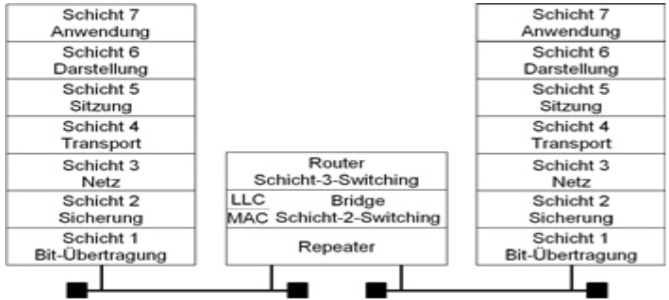
[10 IPv6 8](#_Toc436802429)

[10.1 weitere Ipv6 Protokolle 10](#_Toc436802430)

[10.2 Ipv4 to Ipv6 und umgekehrt 11](#_Toc436802431)

# Einstieg Netzwerke

**OSI-Layer Modell**



# Layer 1 – Medien- und Zugriffverfahren

# Layer 2 – Switching

# Layer 3 – Vermittlungsschicht

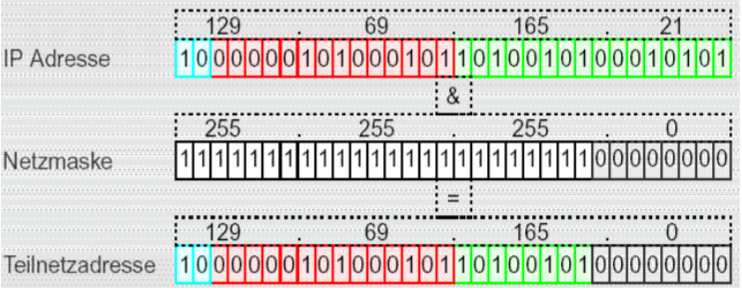
Kommunikation zwischen verschiedenen Netzwerken

## Adressen

In Layer 3 gelten andere Adressen als in Layer 2 (physische Adressen, MAC-Adressen). Durchgesetzt hat sich das IP-Adressierungssystem. IP-Adressen sind weltweit gültig und werden deshalb zentral verwaltet. Die Koordination dabei übernimmt IANA – Internet Assigned Numbers Authority.

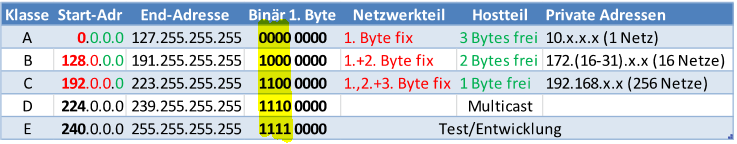
Eine IPv4 Adresse ist 32 Bit breit (IPv6 128 Bit).





### Adressklassen

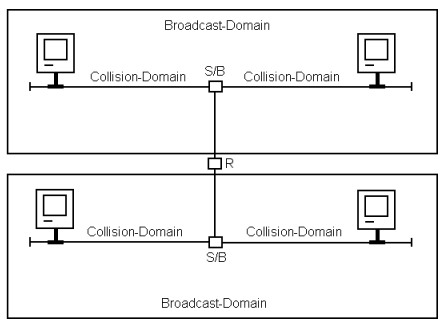
Man unterscheidet zwischen fünf Klassen von Adressen. Grosser Unterschied zwischen ihnen ist die Anzahl Hosts, welche adressiert werden können -> Grösse der möglichen Netze.



Den fixen, nicht veränderbaren Teil der IP-Adresse, nennt man Netzwerkteil.

## Subnetze

Alle 65536 Hosts einer B-Klasse Adresse auf Layer 1 oder 2 zu kommunizieren zu lassen, macht keinen Sinn. Alleine die Rundsendungen (Broadcasts) würden das Netzwerk zum Erliegen bringen. Deshalb unterteilt man die Netze in so genannte Subnetze.



|  |  |
| --- | --- |
| **1.Layer** | Hubs und Medium Konverter |
| **2.Layer** | Switches und Bridges -> trennen Kollisionsdomänen |
| **3.Layer** | Router -> trennen Broadcast-Domänen |

Die Kommunikation erfolgt innerhalb von Broadcastdomänen auf Layer 2, zwischen ihnen auf Layer.

### Spezielle Adressen

In Subnetzen gibt es auf Layer 3 (IP) fest reservierte Adressen, die keinem Host zugewiesen werden dürfen. Das sind:

|  |  |
| --- | --- |
| **Subnetzadresse** | Die kleinste Verfügbare Adresse ist die Bezeichnung des Subnetzes. |
| **Broadcast-Adresse** | Die grösste Verfügbare Adresse ist für die Rundspruchsendung.  Datenpakte für diese Adresse müssen von jedem Netzwerkgerät entgegen genommen werden. |
| **Auto Private IP Adress (APIPA)** | 169.254.0.1 – 169.254.255.255 |
| **Superprivate Adressen** | 127.x.x.x |

Wichtig: Durch die Segmentierung von Netzen gehen immer Minimum zwei Adressen für Endgeräte verloren. Beachtet man noch den benötigten Router für Netzwerk-Netzwerk Kommunikation, sind es sogar drei Adressen die „verloren“ gehen.

## Segmentierung der Netze – Die Netzmaske

Ein Router muss entscheiden können, zu welchem Teil eines Subnetzes welches Gerät gehört.

Ein Gerät möchte Daten an ein anderes Gerät schicken. Dafür muss es erst die Zieladresse auflösen. Innerhalb der Broadcast-Domäne (Layer 2) macht es deshalb einen Broadcast, einen ARP-Request (Address Resolution Protocol). Ist die Zieladresse jedoch in einem anderen Netzwerk, macht ein ARP-Request keinen Sinn. Hier kommt die Netzmaske ins Spiel.

|  |  |
| --- | --- |
| **Sub-/Netzmaske** | Definiert den Host- und den Netzwerkteil der IP-Adresse. |

(Adressbereich der Klasse C: 220.1.10.0 hat 256 Adressen zur Verfügung. Der Administrator dieses Netzwerkes bemerkt, dass die Broadcasts zunehmen und das Netzwerk somit beeinträchtigen.

Lösung: Er segmentiert das Netz weiter in Subnetze.

Problem: Alle Router im Netzt müssen automatisch wissen, dass dies passiert ist.)

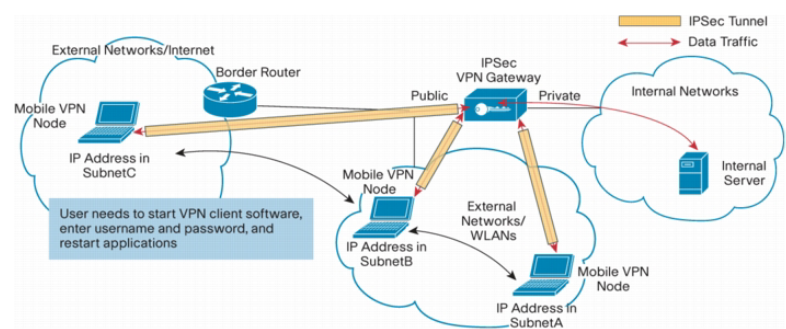
Beispiel

# DNS, DHCP, Multicast

# Layer 4 – Ports, Sockets, TCP, UDP, Firewall

# VLAN-Konzepte

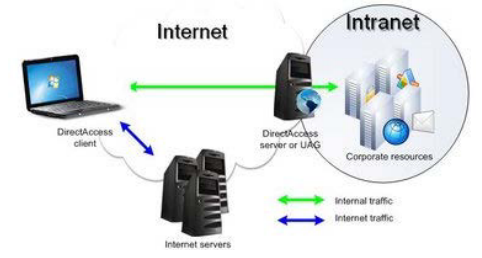
# VPN-Konzepte



VPN Gatewy (nicht Server) routet Subnetze A, B, C der Client.

Bei IP-Änderung bricht VPN-Verbindung zusammen.

## Split Tunnels



Diese geschossenen Tunnel verursachen viel Traffic.

Die Split Tunnels bieten Angriffspunkte für Angreifer aus dem Internet.

Der Client dient dabei als Hop-Node.

Als Gegenmassnahme ist nur eine Verbindung auf dem Client erlaubt.

## Verschlüsselung

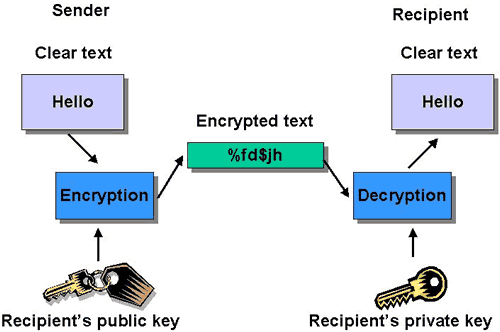
Verschüsselungsverfahren:

* DES
* 3DES
* IDEA
* AES -> aktueller Standard.

Symmetrisch:

Gleiche Schlüssel werden zum Verschlüsseln und Entschlüsseln verwendet. Problem dabei ist die Schlüsselverteilung, aso wir erhält mein Gegenüber den Schlüssel zur Entschlüsselung einer Nachricht auf sichere Art und Weise.

Asymmetrisch:



Mathematisch „verwandtes″ Schlüsselpaar (siehe Diffie-Helmann). Prinzip ist einfach, Nachrichten die mit dem öffentlichen Schlüssel verschlüsselt werden können nur mit dem Private-Key entschlüsselt werden. Verteilung des public Key ist daher unproblematisch, er kann veröffentlicht werden. Einzige Problematik ist die Frage der Authentizität (wirklich Bob’s Schlüssel?). Aus diesem Grund gibt es im Internet Certificate Authorities (CA).

Hybrid:

Mit asymmetrischem Verfahren einen symmetrischen Schlüssel für die gemeinsame Benutzung übertragen

Authentizität:

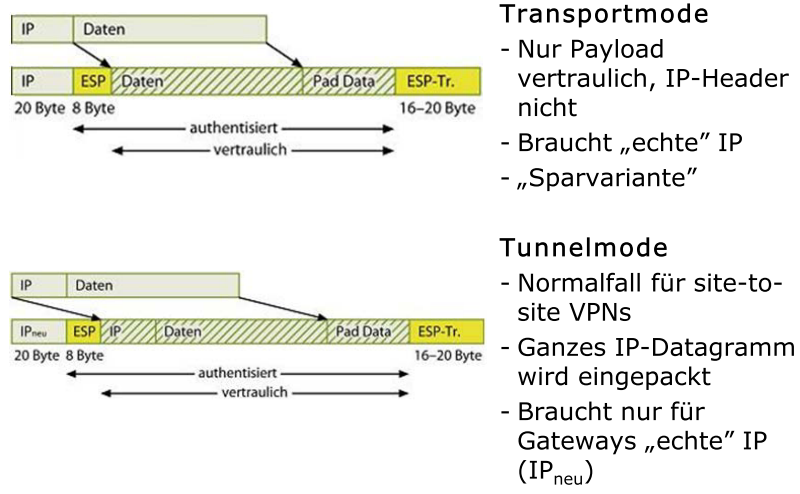
Sicherstellen, dass Gegenstelle authentisch ist, z.B. durch Prüfen der Kenntnis eines gemeinsamen Geheimnisses (PSK = Pre Shared Key)

Datenintegrität:

Den einzelnen Datenpaketen wird ein MAC (Message Authentication Code) angehängt, eine komplizierte Prüfzahl, die am Ziel erneut berechnet wird und den Originalwert ergeben muss. Ein HMAC kombiniert das Verfahren mit dem Hashwert eines gemeinsamen Geheimnisses (Authentizität)

## IPSec

IPSec kann in zwei verschienden Modis betrieben werden.

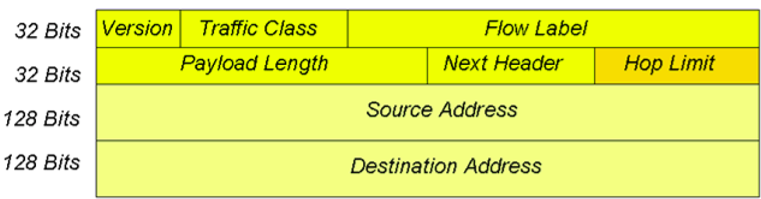


# WLAN, Funknetze, VoIP

# Szenarien von Netzzugängen

# IPv6

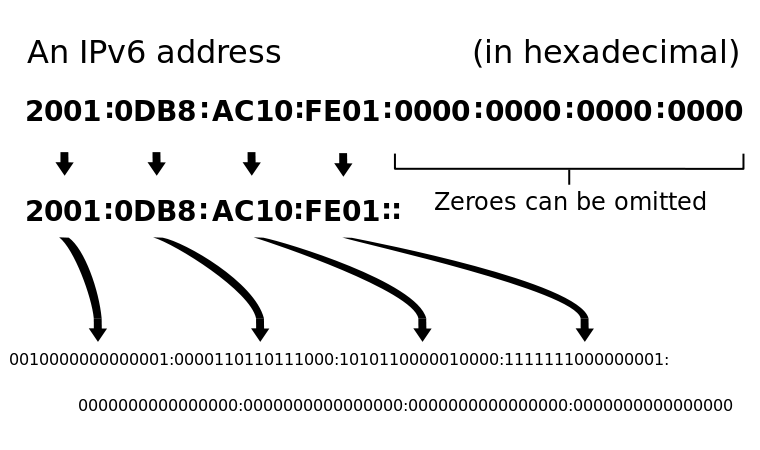
* Grösserer Adressraum: 2^128
* Variable und minimaler Header



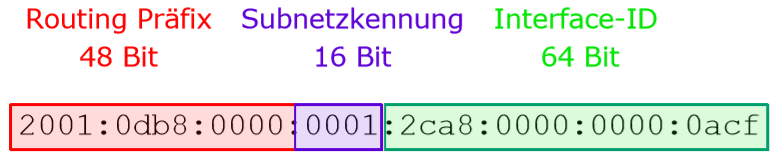
* Provider-Hierarchie in der Adresse ist Konzeptionellunverändert
* Routing Präfix und Host Suffix

**Adresse**

Ipv6 Adressen sind weitaus komplizierter als Ipv4 Addressen.



Bestimmte Felder in der Adresse haben unterschiedliche Funktionen.



Service Priovider erhalten 32 Bit Präfixe. Diese geben 48 Bit Netze weiter an die Kunden.

Beispiel 1

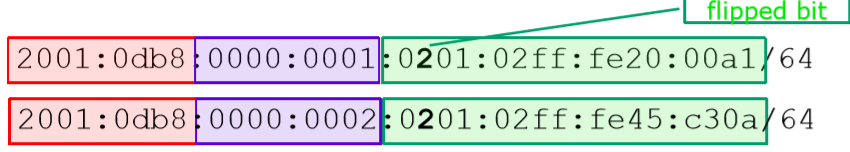
Kunde erhält das Netz 2001:0db8:0002/48 und definiert einen Host im subnetz 0001



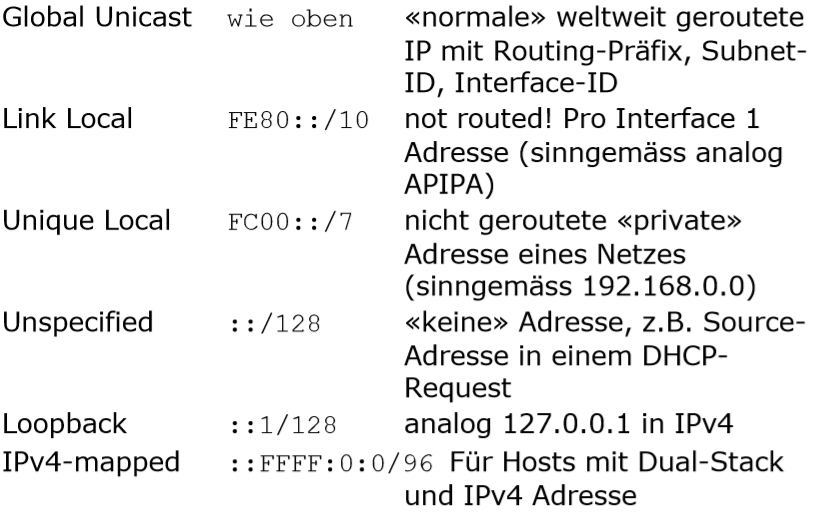
Das Minimum für eine Kunde-IP sind 64 Bit. 64 Bit weil der Kunde kein Subnetting machen darf.

Beispiel 2

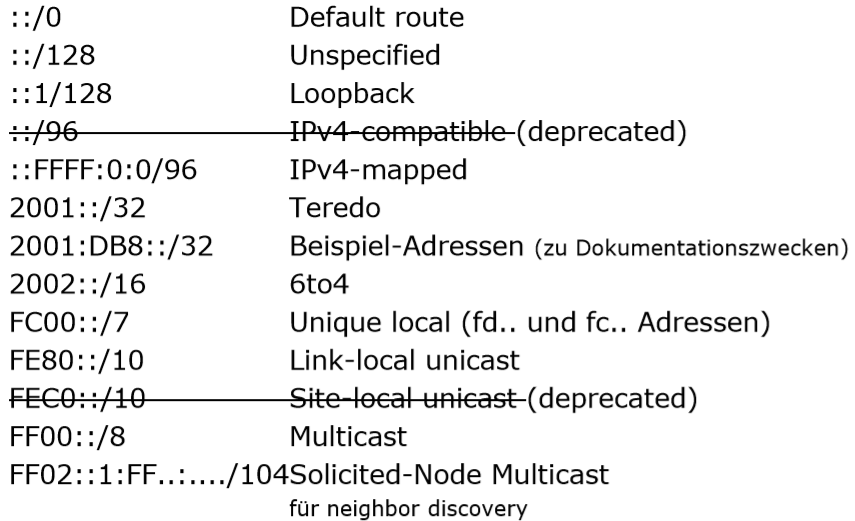
benachbarte /64er Kunden mit NICs von 3Com mit Herstellercode 00:01:02



**Unicast Adressen**



**Reservierte Adressen**



**Beispiel**

Lösung für oben mit «EUI Formation»:

Loopback: ::1

Link-Local: fe80::250:56ff:fec0:8

Global Unicast:2001:620:110: c101:250:56ff:fec0:8

All nodes Multicast: ff02::1 (link local wegen «im LAN»)

Solicited Node Multicast: ff02::1:ffc0:8

Weitere Multicast: ff00::/8 (diese Antwort könnte auch für die oberen 2 gegeben werden!)

Lösung für «von Hand» zugewiesene fixe IP: 2001:638:d:c101:acdc:1979:3:1008 (AAAA Eintrag von www.dfn.de)

Loopback: ::1

Link-Local: fe80::acdc:1979:3:1008

Global Unicast: 2001:638:d:c101:acdc:1979:3:1008

All nodes Multicast: ff02::1 (link local wegen «im LAN»)

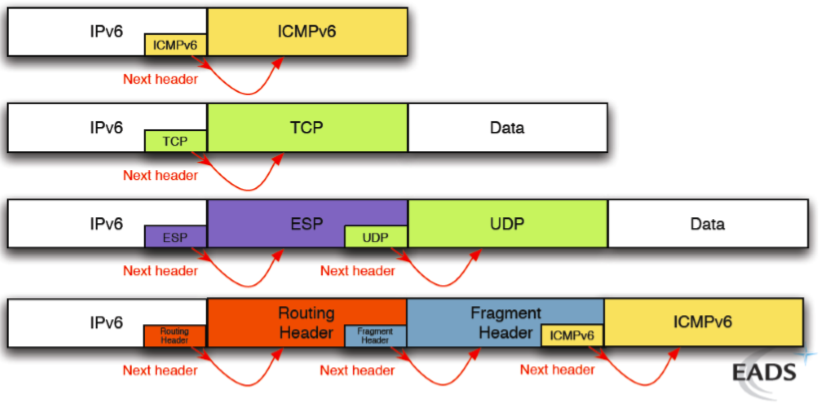
Solicited Node Multicast: ff02::1:ff03:1008

Weitere Multicast: ff00::/8 (diese Antwort könnte auch für die oberen 2 gegeben werden!)

**Extension Header**

Der Header von Ipv6 hat im Vergleich zu Ipv4 viel weniger Felder.

Der Extension-Header gibt an welchers Protokoll folgt.



## weitere Ipv6 Protokolle

**Stateless Address Autoconfiguration – SAA**

Netzwerkkonfiguration von Hand.

1. Link-Local mit EUI-64 Formation erzeugen
2. Die zugehörige Solicited-Node Multicast auf Einmaligkeit prüfen
3. Router Solicitation an FF02::2
4. Router Advertiment mit Netzparametern empfangen
5. Neighbor-Advertisment an FF02:1

Stateful Autoconfiguration mit DHCPv6

1. Nach SAA DHCPv6 Request via UDP an Port 546; Identifiziert durch DUID und IAIDs (eindeutige IDs, die bei Neustart nicht ändern = Rolle der MAC-Adresse in IPv4)
2. Antwort enthält DNS, NTP, SIP, NIS, … mit Ablaufdatum

**Neighbor Detection Protocol**

Ipv4 equivalent ist ARP

1. Neighbor Solicitation Message an Solicited Multicast Adresse des Partners z.B. FF02::1:ff12:3456 senden
2. Diese Solicitation enthält die Layer-2 Adresse des Absenders
3. Partner antwortet mit Neighbor Advertisment, das seine Layer-2 Adresse enthält
4. Beide können im lokalen Netz via MAC auf Layer 2 kommunizieren

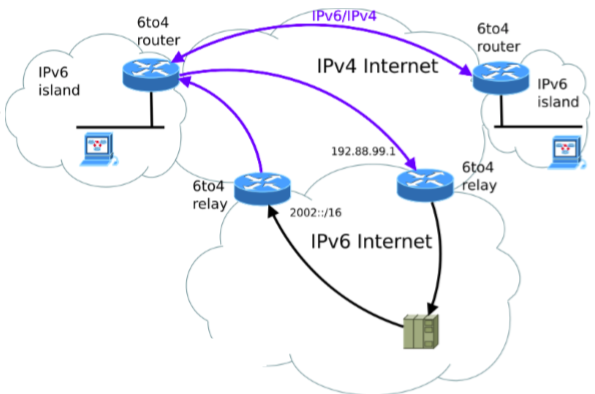
Wenn ein Host seine IP ändert, teilt er das allen Hosts über die All-Nodes Multicast Adresse (FF02::1) mit. Alle aktiven Hosts im Netz übernehmen diese Änderung und können die neue IP der MAC Adresse richtig zuordnen.

## Ipv4 to Ipv6 und umgekehrt

**6to4**

Verbindung von Ipv6 Netzen über ein Ipv4 Netz.

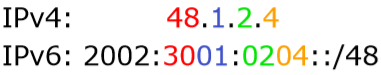
2002::/16 ist der Präfix für 6to4 Adressen, bei 6in4 globale Präfixe.



**6in4**

IPv6 wird auf IPv4-Strecke encapsulated

Beispiel der Zuweisung:



**Intra-Site Automatic Tunnel Addressing Protocol - ISATAP**

* In erster Linie für die Kommunikation reiner IPv6 Hosts in einem IPv4 Subnetz gedacht
* Die IPv4 Adresse wird direkt in die Interface-ID eingebaut: Interface ID = 0000:5EFE:<IPv4-Adresse>
* Sie ist automatisch Unique, wenn echte (ebenfalls eindeutige) IPv4 Adressen benutzt werden
* Das Präfix der IPv6 Adresse des Hosts kann global oder linklocal sein
* Bei globalen Präfixen ist Routing (oder relaying) ins IPv6 Internet möglich

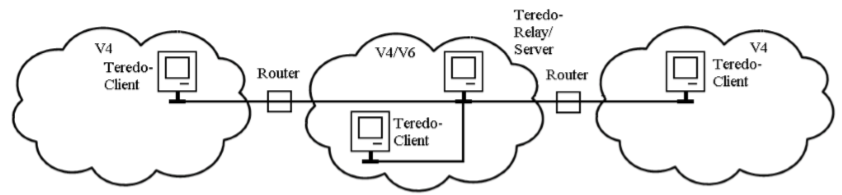
Beispiel:

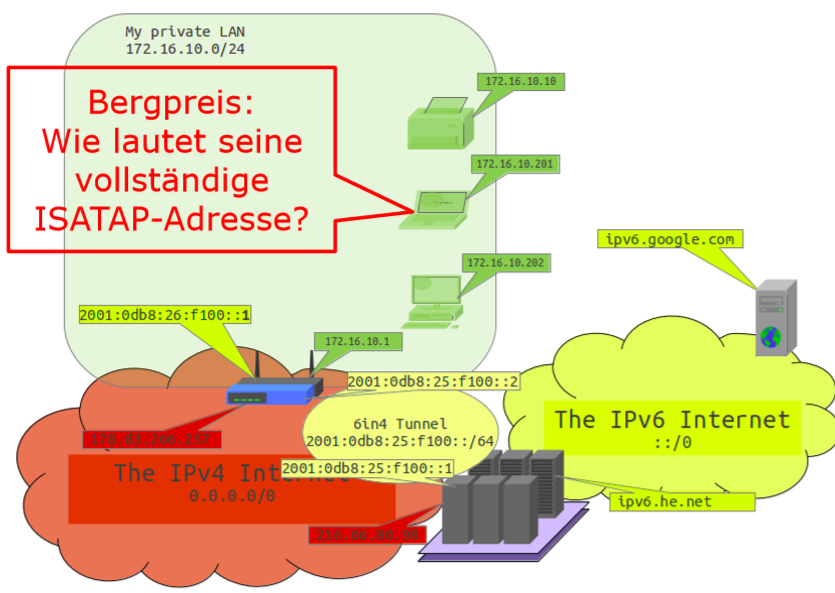
HSLU Adresse: 147.88.210.185

Interface-ID: 0000:5EFE: 9358D2B9

**Teredo**

* Workaround bei «dual-stack» Konfiguration, wenn z.B. 6to4 wegen NAT nicht möglich ist
* Der Protokolltyp 41 (IPv6 in IPv4 getunnelt) wird von den meisten NAT-Routern nicht geroutet (in der Payload befindet sich nämlich kein eigentliches IPv4)
* Der Transport durchs IPv4 Internet geschieht bei Teredo über UDP, wobei alle NAT-Infos mitgegeben werden. Es braucht allerdings einen Teredo Relay Server (3544/udp)!



Beispiel Tunnel Broker

Antwort:

Interface ID: 2001:0db8:26:f100::