# IPV6

## ÜBERBLICK

- Großer Unterschied zu IPv4: Jeder Host (alles was eine IP hat) ist grundsätzlich weltweit erreichbar, Firewalls begrenzen diese Zugänge (IPv4: Firewalls ermöglichen Zugänge).
- Ende-zu-Ende Kommunikation aller Teilnehmer möglich ohne Dritte
- IPv6 wird in Netzwerken gedacht (Subnetze), nicht in IPs

## NEUE EINSATZMÖGLICHKEITEN

- preiswertes WLAN über Laternenmasten vgl. teurer Mobilfunk oder Mesh Network aus Blockheizkraftwerken (derzeit über Mobilfunk)
- Sensornetzwerke aus weltweit direkt  erreichbaren Sensor-Servern
- Ablösung vieler Mobilfunk-Anwendungen durch Internet - Technik (WLANs, IPv6)

# ORGANISATION

## PROVIDER/RIPE

Kunden bekommen PA oder PI Adressblöcke,

- PA = Routing wird vom Provider übernommen, welcher IPv6 Block von RIPE bekommt
- PI = jedes Unternehmen bekommt IPv6 Block von RIPE
- Unternehmen = Sponsoring LIR (local internet registry) oder
- Unternehmen = RIPE-Mitglied 1300€ p.a.

Es liegt beim Provider, fremde (Kunden-eigene) IPv6 Netze zu routen oder nicht

## BEISPIEL DUAL UPLINK

- 2 Provider/ISPs
- Kunde nimmt aktiv am weltweiten Routing teil: teilt seinen Uplinks (ISP) mit, über welche Adressen es verfügt. Diese Information trägt der ISP wiederum zu seinen Uplinks weiter
- Kunden bekommt von seinem ISP alle Uplinks, die dieser kennt (=das Internet)
- Schnelles, automatisches Umschalten zwischen Provider im Störfall

## AS

- AS = autonomes System = ASN = 32bit Nummer von IANA vergeben
- Wikipedia: Ein **autonomes System** (**AS**) ist eine Ansammlung von IP-Netzen, welche als Einheit verwaltet werden und über ein gemeinsames internes Routing-Protokoll (IGP) (oder auch mehrere) verbunden sind. Dieses Netz

wiederum kann sich aus Teilnetzenzusammensetzen. Ein AS steht unter einer gemeinsamen Verwaltung, typischerweise von einem Internet Service Provider (ISP), einer internationalen Firma oder einer Universität. Autonome Systeme sind untereinander verbunden und bilden so das Internet.
- Netzwerk, geschlossen unter administrativer Hoheit, intern: Interior Gateway Protocol IGP, extern Exterior EGP
- diese AS-Nummer erhält ein RIPE Mitglied oder ein Sponsoring LIR, meist ein ISP
- Routing zwischen ASs per BGP = Border Gateway Protocol

---

# MIGRATION

- Können alle Geräte(Core) IPv6?
- Können alle OS IPv6 (Exchange, Windows 7 ... )
- Schulung IPv6, alle mitnehmen
- Testlabor
- Netzwerke pro Unternehmen, Standort, Gebäude  verschwenderisch und großzügige Lücken im Schema lassen
- Reihenfolge

    1. Webserver
    2. Mailserver
    3. Fernwartung/ RDG sowie VPN
    4. Neue Netzwerksegmente

---

# TECHNIK

## GENERELL

- Jedes Unternehmen bekommt /48 Netzwerk = 65535 Subnetze  = 256*256 = 65535 zusammenhängende Netzanteile in die Host geschrieben werden können, für weit entfernte Standorte evtl. nochmal

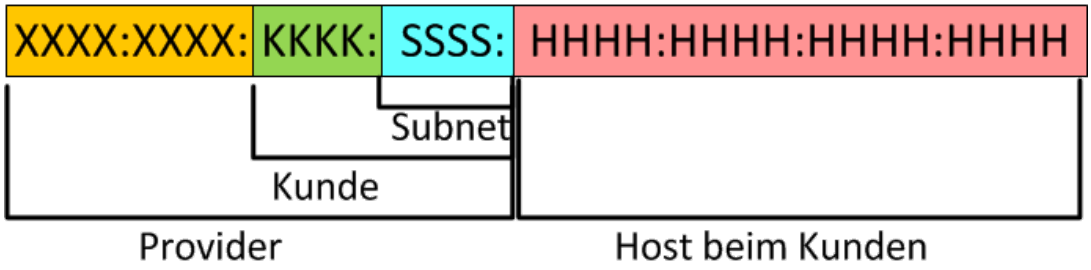
## IP SCHEMA

- IP = 128bit: 64bit Netzanteil, 64 bit Hostanteil, etwas genauer:

```
| 7 bits |1|  40 bits   |  16 bits  |          64 bits           |
+--------+-+------------+-----------+----------------------------+
| Prefix |L| Global ID  | Subnet ID |        Interface ID        |
```

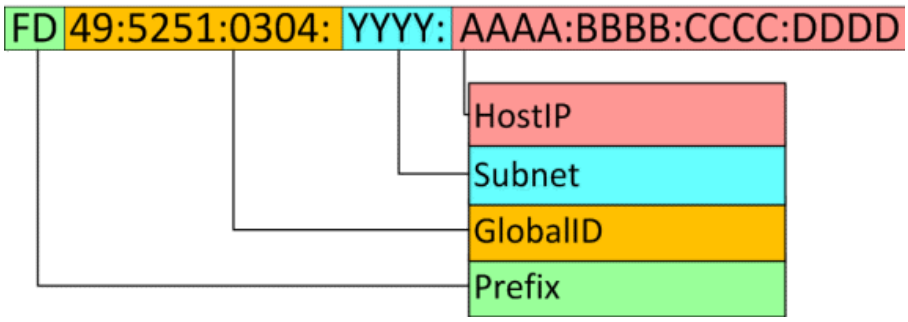
### NETZWERKANTEIL

#### ÖFFENTLICHE NETZE



### PRIVATE NETZE

Private Adressen werden im Internet nicht geroutet (verwendbar zum Beispiel für Server hinter Reverse Proxies). Beispiel von msxfaq.de: "FD ist das Präfix für private Adressen, die dann von der Länderkennung (49 = DE), dem Ortsnetz (5251 = Paderborn) und der Trunkleitung (304) gefolgt wird."




### HOST/INTERFACE-ANTEIL

MAC Adresse (48bit) wird in 64 Bit Hostanteil einkodiert (Auffüllen mit "*fffe*" in der Mitte und ein Bit-Switch im zweiten `::`-Block)

```
MAC 11:22:33:44:55:66 => 1122:33ff:fe44:5566
```

### ABKÜRZUNGEN

- Von jeder :Gruppe: dürfen führende Nullen entfernt werden

```
0042 => 42
```

- Mehrere `:0:` Gruppen können als `::` zusammengefasst werden (logischerweise nur eimal in der gesamten Adresse), nicht aber einzelne `:0:` Gruppen (siehe RFC 5952)

```
:0000:0000: => ::
```

Beispiel von der IPv6 Wikipedia Seite:

```
2001:0db8:0000:0000:0000:ff00:0042:8329 => 2001:db8:0:0:0:ff00:42:8329 => 2001:db8::ff00:42:8329
```

### SPEZIELLE ADRESSEN

- siehe IANA-Liste für multicast Adressen
- **Multicast alle DHCP-Server**: `ff02::1:2`
- **Localhost** 127.0.0.1(): `::1:`
- **Multicast alle Adressen:** `ff02::1`
- **Link-Lokale Adresse**: `FE80::/10` + Host-Anteil

## NETZWERK

Siehe RFC zu DHCP/SLAAC Auslegung

### ROUTER UND FIREWALLS

- Router, Firewalls und DHCP-Server müssen feste IPs auf allen Schnittstellen haben
- Router machen sich untereinander per "Advertising" bekannt
- Router machen den Globalen IPv6-Netwerkanteil bekannt per (siehe hier):

    - Router Solicitation (Solicitation Message): Mit seiner link-lokalen IPv6-Adresse bittet der Host auf der Multicast-Adresse `ff02::2` um den globalen Präfix (optional).
    - Router Advertisement (Advertisement Message): Der Router schickt daraufhin eine Nachricht mit dem globalen Präfix für dieses Netzwerk, der MTU (Größe der IP-Pakete) und dem Flag "autonomous".

### HOSTS

- Stateless address configuration SLACC: Hosts erzeugen IPv6 Adresse selber, bekommen aber vom Router gesagt in welchem Bereich und das er das Gateway für unbekannte Addressen ist
    - aus MAC (quasi statisch) - Datenschutzprobleme, Hardwaretyp wird bekannt und Netzwerkaktivitäten können nachvollzogen werden. Gut für Server, Core, AP, SIP, Drucker, Switch
    - per Zufall - Privacy Extensions. Adresse ist im Unternehmensnetz und im Internet anonym. und wechselt ständig, Authentifizierung/ Kontrolle über Zertifikate
    - Netzwerkkarte zwei Adressen zuweisen: MAC für interne Zugriffe, Random für Internet-Kommunikation
- Jeder Host bekommt eine Link-lokale und eine globale IPv6 Adresse

Server: Zufällige "stable" Privacy-Extension Adresse vergeben, die sich erst ändert wenn das Gerät das Subnet wechseln sollte oder Autokonfiguration (SLAAC) deaktivieren bzw. serverseitig zu ignorieren und eine statische IPv6-Adressen nach dem Zufallsprinzip zu erzeugen und nicht durchnummeriert vergeben.

- TODO: http://www.elektronik-kompendium.de/...et/1902131.htm

### ROUTING

"Wenn Sie nur genau ein Subnetz haben, dann müssen sie gar nichts machen, weil alle Clients immer auch eine "Link Local" Adresse mit dem Prefix fe80 haben und damit schon kommunizieren können."

### DNS

DNS Server werden einer Multicast-Adresse zugeordnet, so das DNS clients einfach an das DNS-Server-Netz Anfragen und alle DNS Server antworten (anstelle einer Kette).

Zuweisen zusätzlicher IPv6 Adressen für DNS-Server:

```
netsh int ipv6 show interface # Ausgeben der Liste von Schnittstellen zur Verwendung
netsh interface ipv6 add address <interface> FEC0:0:0:FFFF::1
netsh interface ipv6 add address <interface> FEC0:0:0:FFFF::2
netsh interface ipv6 add address <interface> FEC0:0:0:FFFF::3
```

### AUTHENTIFIZIERUNG

- ACL anhand von IPs passt nicht besonders gut zu IPv6, da Adressen zufällig vergeben werden (können) - besser ist eine  Identifikation anhand von Schlüsseln/Zertifikaten

## IPV6 UND IPV4

- IPv6 läßt sich per GRE und MPLS in IPv4 tunneln
- 6to4 und auch Teredo kodiert IPv4 Adresse in eine IPv6 Adresse. "Der 6to4-Router nimmt die IPv4-Adresse, an der das nächste 6to4-Gateway zu finden ist, aus der IPv6-Adresse und schickt die Daten zum richtigen Ziel."