# IPv6

Zuständig für:

* Vermittlung
* Adressierung
* Weiterleitung

Schicht 3 (OSI-Schichtenmodell), Vermittlungsschicht

Vorteile

* mehr Adressen (, weil 128 Bits)
* mehrere IPv6-Adressen pro Host (unterschiedliche Gültigkeitsbereiche):
  + lokal (Link-Lokal)
  + global
  + temporär
* Autokonfiguration SLAAC
* Multicast
* schnelleres Routing (keine Subnetzmaske berechnen)
* IPsec (Verschlüsselung)
* Quality of Service (Bandbreitengarantie 🡪 Priorität)
* Datenpaket bis 4GByte (Jumbogram)

Adressraum

128 Bit 🡪 Adressen

Address Selection

= Auswahl welche IP-Adresse (IPv4 / IPv6 link-lokal / IPv6 global / IPv6 temporär / …)

Multicast

1 Adresse für Multicast-Gruppe: z.B.: Netzwerkknoten, Router, Zeit-Server, andere Dienste/-Anbieter

NDP

Neighbor Discovery Protocol = Austausch relevanter link-lokal Nachrichten (z.B.: Router Discovery / Neighbor Discovery)

IPsec

Verschlüsselungs- / Authentifizierungsmechanismen (kryptografisch sichern)

Multihoming

Interface, welches mehrere globale IPv6-Adressen mit gleichem Präfix hat.

Renumbering

Falls Gültigkeit einer Adresse bald vorbei 🡪 neue suchen = Vorgang Renumbering

1. neue IPv6-Adresse bekommen
2. mit der Zeit alle Dienste auf neue Adresse umstellen
3. erste / alte IPv6-Adresse löschen

Über Router Advertisements kann man die neue Adresse priorisieren und die alte vermeiden, bis sie ausläuft.

Flow Labels

= Priorisierung von Paketen

mobile IPv6

zwischen verschiedenen Netzwerken (z.B.: Schule, MC, Bus, …) fluid wechseln

Jumbograms

Jumbo Payload Option ermöglich Nutzdatenlängen jenseits von 65.535 (bis 4GByte).

Segmentierung

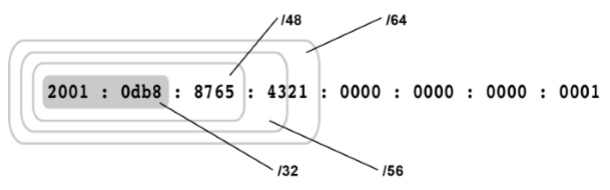
Netzanteil: immer 64Bit (fast alle Bit vom Provider vergeben, es sei denn, Provider stellt mehrere Netze zur Verfügung) 🡪 SCHNELLES ROUTING

Interface-Identifier: immer 64Bit; anfangs aus MAC-Adresse gebildet  
  
Ein Bild, das Text, Kleiderbügel enthält.

Automatisch generierte Beschreibung

Umwandlung MAC in Interface-Identifier:   
In Mitte von MAC ff:fe einfügen und siebente Bit des ersten Bytes invertieren.

Wenn Unternehmen mehrere Subnetze benötigt, gibt der Provider ein /32, /48, /56 oder /64 – Netz her. Der Netzanteil beträgt allerdings immer noch 64Bit! Das Unternehmen kann halt einen Teil des Präfix für Subnetze nutzen.



Dank dem Adressüberfluss ist es möglich, jedem Dienst eine eigene IPv6-Adresse zu geben.

Scopes (Gültigkeitsbereiche)

Der Scope ist der Teil eines Netzwerks in dem die zugehörige Adresse als gültig anerkannt und geroutet wird.

* Host-Scope (Virtualisierung)
* Link-Lokal-Scope (Autokonfiguration beim Hochfahren fe80:)
* Unique-Local-Scope
* Site-Local-Scope (veraltet)
* Global-Scope (im Internet routebar)
* Multicast-Scope

Privacy Extensions (RFC 4941)

Wenn aktiviert, bekommt jede Schnittstelle mindestens eine zusätzliche temporär globale IPv6-Adresse, deren Interface Identifier pseudozufällig erzeugt wird und regelmäßig wechselt. Somit lässt Interface Identifier (umgewandelte MAC-Adresse) keinen Rückschluss mehr auf Host zu.

Deswegen haben temporär globale IPv6-Adressen auch nur eine begrenzte Zeit Gültigkeit.

Schreibweise

1. .ToLower()
2. Nullen weglassen (z.B.: 00f4 🡪 f4; 0000 🡪 0)
3. ersten aufeinander folgenden Nullerblöcke duch :: ersetzen

z.B.: fe80::e4:0:1%eth0

URL-Pfade: [fe80::e4:0:1%25eth0]

UNC-Pfade: fe80--e4-0-1.ipv6-literal.net

Autokonfiguration

Link-Lokal-Adresse:

alle außer Windows: fe80::{Umwandlung der MAC-Adresse}

Windows: fe80::{pseudozufällig}

* SLAAC (Stateless Address Autoconfiguration) – Verfahren

Globale Adresse:

1. entweder SLAAC (per Router Advertisement),
2. DHCP (Stateful Address Autoconfiguration)
3. oder manuell (logisch)

Temporär globale Adressen:

Interface Identifier pseudozufällig, damit nicht rückverfolgbar auf MAC-Adresse.

Ein Bild, das Tisch enthält.

Automatisch generierte Beschreibung

\* Da wo SLAAC steht, muss eig. auch DHCP bzw. manuell dabeistehen…  
\* Da wo MAC steht, muss “bei Windows zufällig” dabeistehen…

Standard-Gateway:

1. SLAAC (per Router Advertisements)

DNS-Server:

1. SLAAC (per Router Advertisements)
2. DHCPv6

andere Adressen:

1. DHCPv6

Dual-Stack

Wenn ein Gerät IPv4 & IPv6 unterstützt. (Gleichzeitiger Betrieb)

NT: doppelter Administrationsaufwand 🡪 doppelte Fehlerquellen + Mitarbeiter kennen kein IPv6, weil zu neu

Stateless vs Stateful

1. Stateless: SLAAC
2. Stateful: DHCPv6

sinnvolle Szenarien der Autokonfiguration

1. komplett stateless: SLAAC vergibt per Router Advertisement link-lokal Adresse
2. stateless: SLAAC vergibt link-lokal, global und Default-Router Adressen, weiter Parameter DHCPv6
3. komplett stateful: alles DHCPv6 (außer Default-Route)

Übergangsverfahren

1. Tunneling
2. Dual-Stack
3. Protokollübersetzug

Tunneling

1. 4in6: Tunneling von IPv4 in IPv6
2. 6in4: Tunneling von IPv6 in IPv4
3. 6to4: Transport von IPv6-Paketen über IPv4-Netzwerk
4. 6over4: Transport IPv6-Pakete zwischen Dual-Stack Knoten über IPv4-Netzwerk
5. Teredo: weiterer Header über Paket

Protokollübersetzung

1. DNS64
2. NAT64

IPv6-Client will auf IPv4-Server 🡪 intern: IPv6-Adresse; extern IPv4-Adresse

Client bekommt von DNS64 IPv6-Adresse, wo IPv4-Adresse des Servers drinnen ist. Client schickt über NAT64 zu Server und umgekehrt.

VT: Client weiß nichts von IPv4-Server

NT: öffentliche IPv4-Adressen mög.w. nicht verfügbar

DS-Lite

hat nichts mit Dual-Stack zu tun, weil Tunneltechnik

Router globale IPv6-Adresse und privat IPv4-Netzwerk

# TCP

= Transmission Control Protocol

Schicht 4 Osi-Schichtenmodell (Transportschicht)

Aufgaben

* Segmentierung: Dateien in Segmente teilen, Riehenfolge wiederherstellen und wieder zusammensetzen
* Verbindungsmanagement: Auf- / Abbau d. Verbindung
* Fehlerbehandlung: Bestätigung + Zeitüberwachung
* Flusssteuerung: Dynamische Auslastung d. Übertragungsstreche
* Anwendungsunterstützung: Adressierung spezifischer Anwendungen durch Port-Nummern

Data Segmenting

Jedes Segment wird mit Header versehen, damit wieder in richtiger Reihenfolge zusammengebastelt werden kann (mittels fortlaufenden Sequenznummern).

Connection Establishment and Termination

Ende-zu-Ende-Kommunikation 🡪 Sender & Empfänger ständig in Kontakt zueinander.

Falls nach einiger Zeit nichts mehr kommuniziert wird, schickt TCP ein Bestätigungsprotokoll, damit die Verbindung nicht abbricht.

Error Detection

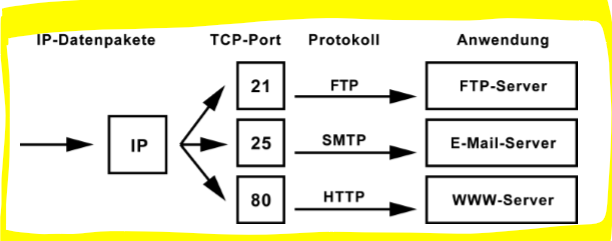
ständig Kontrollmeldungen 🡪 Empfänger bestätigt jedes 1-4 Datenpaket. Falls dies nicht der Fall ist, wird das Paket / die Pakete noch einmal verschickt.

Flow Control

TCP hat keine Information über die verfügbare Bandbreite. Flow Control reagiert auf langsame / schnelle Verbindungen bzw. unerwartete Engpässe oder Verzögerungen. Flow Control lastet diese Verbindung immer dynamisch aus.

Application Support

Jede Anwendung hat einen Port, sodass der Host auch weiß, zu welcher Anwendung dieses Paket gehört.



Ports

* 0 – 1.023: well-known Ports: fest zugeordnet
* 1.024 – 49.151: registered Ports: jeder kann Port reservieren
* 49.152 – 65.535: dynamically-allocated Ports: werden dynamisch zugewisen (ausgehende Verbindung (Source-Port)

Die wichtigsten Port finden Sie hier: <https://schneider-it.at/docs/netzwerktechnik/grundlagen.html#well-known_Ports>

Ports können mehrere Zustände haben:

* Open: Anwendung dahinter
* Closed: keine Anwendung dahinter bzw. drop (Firewall)
* Filtered: reject (Firewall)

# UDP

= verbindungsloses Transport-Protokoll

Schicht 4 (Transportschicht)

Vorteile

* Header viel kleiner

Verwendung

* DNS-Abfragen
* VPN-Verbindugnen
* Audio & Video

Unterschiede

* keine Methoden, die sicherstellen, dass Pakete irgendwie ankommen
* keine Methoden, die sicherstellen, dass Pakete in richtiger Reihenfolge zusammengesetzt werden
* Anwendung ist für sichere Datenübertragung zuständig

# RTP

= Realtime Transport Protocol

Daten in Echtzeit übertragen, speziell für Audio & Video  
kein Quality of Service (garantiert keine Dienstqualität der Übertragung)

Sinn hinter RTP: Paketverluste sollen bis zu bestimmten Grad akzeptabel seien!

# NetBIOS

= Network Basic Input/Output System

Fakten

* von IBM
* Schicht 5 (Kommunikationsschicht)
* Schnittstelle für Anwedungen zum Windows-basierten Netzwerk (dient als Application Programming Interface / API)
* soll für Kommunikation in kleinen Netzwerken dienen (max. 80 Hosts)
* Dienste:
  + Name-Service (137/udp): Auflösung der NetBIOS-Namen
  + Datagram-Service (138/udp): Statusmeldungen
  + Session-Service (445/tcp und 139/tcp): Nutzdaten & Steuerungsinfos mit SMB und CIFS

# Zeroconf / Bonjour / Avahi

= selbstkonfigurierende Verfahren für IPv4 und IPv6 (Sammlung bestehender Protokolle 🡪 IP, DNS, NAT)

* IPv4: 224.0.0251
* IPv6: ff02::fb
* Port: 5353

geht nicht über Subnetze hinweg! (DNS-übliche Unicasts als Lösung 🡪 WAB / Wide Area Bonjour)

Aufgaben

* IP-Adressen zuweisen (IPv4: Bonjour [169.254.0.0/16]: per Broadcast an ARP-Cache verteilt, IPv6: SLAAC)
* Namen zuweisen: mDNS
* Dienste bekannt machen: über Adresse oben kann z.B.: Netzwerk-Drucker Dienst anbieten

Annoncierung

Dienstanbieter teilt Dienst von sich aus mit 🡪 andere Stationen können diesen dann finden

# WWW

= Sammlung von Servern mit Informationen  
Zugriff mittels Browser; Links machen Informationen zugänglich

HTTP-Request: z.B.: <https://schneider-it.at> (vom Client zum Server)  
HTTP-Response: Texte, Bilder, Video, Audio (vom Server zum Client)

HTTP-Client

* Chrome (Google)
* Safari (Apple)
* Edge (Microsoft)
* Opera
* Firefox (Mozilla)

HTTP-Server

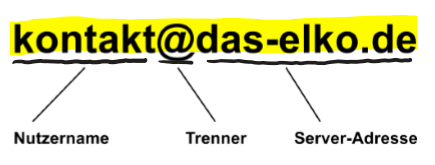
* Apache
* Nginx
* Internet Information Server (Microsoft)
* Lighttpd

HTML

Hypertext Markup Language = Beschreibungssprache für plattformübergreifende Dokumente

E-Mail

zentrales Kommunikationsmittel



“das-elko.de” = eig. eine Domain; mittels DNS MX-Record (Mail Exchanger) in IP-Adresse umgewandelt

Ein Bild, das Text enthält.

Automatisch generierte Beschreibung

* MUA – Mail User Agent (E-Mail-Client)
* MTA – Mail Transfer Agent (Postausgangsserver)
* MDA – Mail Delivery Agent (Posteingangsserver)

Vorgang: Sendender E-Mail-Client schicht zu seinem Ausgangsserver (per SMTP). Diese E-Mail wird per SMTP zum MTA des Empfängers weitergeleitet. Weil der empfangende E-Mail-Client nicht da ist, wird die E-Mail in den Posteingangsserver verschoben. Von dort kann sich der empfangende E-Mail-Client mittels POP oder IMAP abholen.

DNS-Server: wandelt Domainnamen mittels MX-Record in IP-Adresse um.

SMTP – Simple Mail Transfer Protocol

Ports: 25, 465, 587

Überträgt E-Mails vom Sender zu dessen Ausgangsserver und weiter zu Empfängers Ausgangsserver.

POP – Post Office Protocol

Ports: 110, 995

Ladet alle E-Mails von Posteingangsserver herunter.

Nachteile:

* Falls Nutzer auf mehreren Geräten arbeitet, sieht er Nachrichten doppelt (immer ungelesen, die er schon gelesen hat)
* nicht für mobile Geräte gedacht
* keine Verwaltung von E-Mails (Verschieben, Kopieren, Löschen) in Ordnerstrukturen

IMAP – Internet Mail Access Protocol

Ports: 143, 993

Bearbeitet E-Mails immer online am Server, sodass auf anderen Geräten immer aktueller Stand ist…

E-Mail immer aus 3.Teilen: Header, Body, Attachement