# IPv4

IPv4 (Internet Protocol Version 4), vor der Entwicklung von IPv6 auch einfach IP, ist die vierte Version des Internet Protocols (IP). Es war die erste Version des Internet Protocols, welche weltweit verbreitet und eingesetzt wurde, und bildet als Teil der Internetprotokollfamilie eine wichtige technische Grundlage des Internets. Es wurde in RFC 791 im Jahr 1981 definiert und stellt einen Internetstandard der Internet Engineering Task Force dar. IPv4 verwendet 32 Bit lange IP-Adressen.

## Geschichte

IPv4 wurde als Teil der Internetprotokollfamilie für das Arpanet entwickelt und kam darin ab 1983 zum Einsatz. Damals waren nur einige hundert Rechner an das Netz angeschlossen. Das Arpanet entwickelte sich zum Internet und überschritt 1989 die Grenze von 100.000 Rechnern. Durch seine Verbreitung im Internet hat IPv4 schließlich auch LAN-Protokolle wie DECnet oder IPX verdrängt. NetWare, AppleTalk und NetBIOS wurden als neue Versionen hervorgebracht, die auf IP aufsetzen.

Am Anfang der 1990er Jahre war erkennbar, dass IP-Adressen bald knapp würden, da die damals übliche Netzklassen-basierte Adressvergabe erheblichen Verschnitt verursachte. Als kurzfristige Lösung wurde 1993 Classless Inter-Domain Routing eingeführt, das eine deutlich effizientere Adressvergabe ermöglichte. Eine weitere kurzfristige Lösung war das 1994 eingeführte Network Address Translation (NAT), das die Wiederverwendung von IP-Adressen ermöglichte. In der Variante Network Address Port Translation (NAPT) ermöglichte es die gleichzeitige Mehrfachverwendung von IP-Adressen. Mit diesen Maßnahmen konnte der Adressbedarf soweit gedämpft werden, dass der Adressraum trotz immensen Wachstums des Internet erst in den 2010er Jahren knapp wurde.

Als langfristige Lösung der Adressknappheit sollte ein neues Protokoll mit größerem Adressraum entwickelt werden. Dies führte zuerst zur Entwicklung des experimentellen Protokolls TP/IX, das die Versionsnummer 7 trug und 1993 veröffentlicht wurde. TP/IX sollte dabei einen 64-Bit-Adressbereich unterstützen, wurde dann aber zugunsten von IPv6 verworfen. Die erste Fassung von IPv6 wurde 1995 veröffentlicht und verwendete einen 128-Bit-Adressraum. Die Versionsnummer 5 wurde nicht für einen IPv4-Nachfolger verwendet, da sie bereits 1990 durch das experimentelle Internet Stream Protocol Version 2 (ST2) belegt war, einem für Streaming optimierten Protokoll.

## Adressformat

IPv4 benutzt 32-Bit-Adressen, wodurch ein Adressraum von knapp 4,3 Milliarden Adressen zur Verfügung steht. IPv4-Adressen werden meist in Dezimalpunktschreibweise dargestellt: vier Oktetts (je 8 Bit) werden durch Punkt getrennt mit vier Zahlen von 0 bis 255 dargestellt.

Beispiel: 192.0.2.155

Eine IPv4-Adresse kann in dezimal, binär, oktal und hexadezimal sowohl in der Punkt-, als auch in der Nichtpunktnotation dargestellt werden. Eine führende Null zeigt eine Oktalzahl an. Daher dürfen in der Dezimalpunktschreibweise ein- und zweistellige Zahlen nicht auf ein gleichförmiges Längenformat gebracht werden (nicht: 192.000.002.155).

Jedes der vier Oktette besteht aus 8 Bit und stellt somit 28 = 256 verschiedene Werte dar. Daraus ergibt sich eine Gesamtzahl von 256 × 256 × 256 × 256 = 2564 = 232 = 4.294.967.296 IPv4-Adressen.

## Netzanteil und Hostanteil

Eine IP-Adresse besteht aus einem Netzanteil und einem Hostanteil. Der Netzanteil identifiziert ein Teilnetz, der Hostanteil identifiziert ein Gerät (Host) innerhalb eines Teilnetzes.

Die genaue Aufteilung zwischen Netzanteil und Hostanteil wird durch eine Subnetzmaske festgelegt, beispielsweise 255.255.255.0, was in binärer Darstellung 11111111.11111111.11111111.00000000 entspricht. Die Bits der Subnetzmaske, die „1“ lauten, legen die Stellen der IP-Adresse fest, die zum Netzanteil gehören. Alle restlichen Stellen der IP-Adresse, die entsprechend in der Subnetzmaske auf „0“ gesetzt sind, gehören zum Hostanteil. In der CIDR-Notation wird die Länge des Netzanteils durch die Anzahl Bits angegeben und mit Schrägstrich getrennt als Suffix an die IP-Adresse angehängt, beispielsweise /24. Somit ist der Netzanteil 24 Bits lang, was der Subnetzmaske 255.255.255.0 entspricht. Die übrigen 8 Bits gehören somit zum Hostanteil.

Beispiel:

| | dezimal | | | binär | |
|---|---|---|---|---|---|
| IP-Adresse | 192.0.2 | .155 | → | 11000000.00000000.00000010 | .10011011 |
| Subnetzmaske | 255.255.255 | .0 | → | 11111111.11111111.11111111 | .00000000 |
| | *Netzanteil* | *Hostanteil* | | *Netzanteil* | *Hostanteil* |
| CIDR-Notation | 192.0.2.155/24 | | | | |

Die Unterscheidung zwischen Netzanteil und Hostanteil ist erforderlich für die Entscheidung, ob sich eine Zieladresse in demselben lokalen Netz oder in einem anderen Netz befindet. Wenn der Netzanteil identisch ist, können die Endgeräte innerhalb einer Broadcast-Domäne direkt miteinander kommunizieren, beispielsweise per Ethernet oder WLAN. Im selben Teilnetz darf der Hostanteil nicht mehrfach vergeben sein, da es ansonsten zu einem IP-Adresskonflikt kommt. Für jedes Endgerät vergibt der zuständige Netzwerkadministrator den Hostanteil eindeutig durch eine manuelle oder automatische IP-Adresszuweisung.

Für die Kommunikation zwischen unterschiedlichen Netzen wird ein Router benötigt. Der Netzanteil muss ebenfalls eindeutig sein, damit es nicht zu Routing-Konflikten führt. Die Vergabe von IP-Netzbereichen erfolgt durch eine hierarchische Organisationsstruktur zwischen der Internet Assigned Numbers Authority, den Regional Internet Registrys und den Local Internet Registrys.

## Subnetting

Ein Netz kann in weitere Teil- oder Subnetze unterteilt werden. Dies erfolgt, indem ein oder mehrere höchwertige Bits des Hostanteils zur Unterscheidung des Subnetzes verwendet werden. Innerhalb eines Subnetzes wird die Subnetzmaske angepasst, um den verkleinerten Hostanteil widerzuspiegeln. Subnetting wird zur Segmentierung von Netzen verwendet. Für die Kommunikation zwischen den Subnetzen ist ein Router erforderlich.

Beispiel:

| | Netzadresse (CIDR) | Subnetzmaske | Adressbereich | Netz-, Subnetz- und Hostanteil (binär) |
|---|---|---|---|---|
| Netz | 192.0.2.0/24 | 255.255.255.0 | 192.0.2.0 – 192.0.2.255 | 11000000.00000000.00000010.xxxxxxxx |
| Subnetz | 192.0.2.0/25 | 255.255.255.128 | 192.0.2.0 – 192.0.2.127 | 11000000.00000000.00000010.0xxxxxxx |
| Subnetz | 192.0.2.128/26 | 255.255.255.192 | 192.0.2.128 – 192.0.2.191 | 11000000.00000000.00000010.10xxxxxx |
| Subnetz | 192.0.2.192/26 | 255.255.255.192 | 192.0.2.192 – 192.0.2.255 | 11000000.00000000.00000010.11xxxxxx |

Nach außen hin wird das Netz beim Routing als ein ganzes adressiert. Die innere Unterteilung in Subnetze ist nicht direkt ersichtlich. Das Gegenteil von Subnetting ist Supernetting und beschreibt die Zusammenfassung von mehreren angrenzenden Netzadressen in einer gemeinsamen Route. Der Zweck ist die Minimierung von Einträgen in einer Routingtabelle. Supernetting wird bei Classless Inter-Domain Routing als Routenaggregation bezeichnet.

## Historische Netzklassen (nicht mehr in Gebrauch seit 1993)

Ursprünglich gab es fest vorgeschriebene Einteilungen für Netzklassen mit einer festen Länge des Netzanteils. Die Größe des Netzanteils ergab sich aus den ersten Bits der Adresse; eine Subnetzmaske musste nicht angegeben werden. Da diese Einteilung sehr unflexibel ist, wird seit 1993 ausschließlich das Verfahren Classless Inter-Domain Routing angewandt, welches bitvariable Netzmasken ermöglicht. Obwohl das Konzept von Netzklassen seitdem nicht mehr im Einsatz ist, blieb der Begriff der Netzklasse über Jahre verbreitet. Hierbei steht „Klasse A“ für ein Netz der CIDR-Präfixlänge /8, „Klasse B“ für /16 und „Klasse C“ für /24. Die ursprüngliche Zuordnung zu festgelegten Adressbereichen wird für gewöhnlich ignoriert, sodass diese Begrifflichkeit nicht mit dem ursprünglichen Konzept der Netzklassen konform ist.

## Nutzbare Adressen

Die jeweils erste und letzte Adresse eines Subnetzes haben eine besondere Bedeutung und stehen üblicherweise nicht zur Vergabe an Hosts zur Verfügung. Die maximale Anzahl der zu vergebenen Hostadressen in einem Netz beträgt somit effektiv:

$2^{\text{Anzahl Bits der Hostadresse}} - 2.$

Diese Einschränkung geht auf die Praxis zurück, Adressen mit „0“ an allen Stellen als „dieses Netz“ und Adressen mit „1“ an allen Stellen als „alle Hosts“ zu interpretieren. Die erste Adresse eines Subnetzes (zum Beispiel 192.0.2.0) bezeichnet das Netz selbst. Die letzte Adresse (zum Beispiel 192.0.2.255) bezeichnet die Broadcast-Adresse, unter der alle Hosts im Netz angesprochen werden können. Ein Versuch, diese Einschränkung aufzuheben, hat sich nicht durchgesetzt, sodass auch heute noch in praktisch jedem Netz beide Adressen reserviert sind. Gängig ist außerdem, das Default Gateway auf die zweite oder die vorletzte IP-Adresse im Netz zu legen (zum Beispiel 192.0.2.1 oder 192.0.2.254), wobei es dafür keinerlei Vorgaben gibt.

## Besondere Netzadressen

Einige Netzadressen sind für spezielle Zwecke reserviert:

| Adressblock (Präfix) | Verwendung | Referenz |
|---|---|---|
| 0.0.0.0/8 | Das vorliegende Netzwerk | RFC 1122 |
| 10.0.0.0/8 | Private Netze | RFC 1918 |
| 100.64.0.0/10 | Shared Transition Space | RFC 6598 |
| 127.0.0.0/8 | Loopback (Lokaler Computer) | RFC 1122 |
| 169.254.0.0/16 | Automatische Adresskonfiguration (link local), APIPA | RFC 3927 |
| 172.16.0.0/12 | Private Netze | RFC 1918 |
| 192.0.0.0/24 | IETF Protocol Assignments | RFC 6890 |
| 192.0.2.0/24 | Dokumentationszwecke | RFC 6890 |
| 192.88.99.0/24 | IPv6 zu IPv4 Relay (Veraltet) | RFC 7526 |
| 192.168.0.0/16 | Private Netze | RFC 1918 |
| 198.18.0.0/15 | Netzwerk-Benchmark-Tests | RFC 2544 |
| 198.51.100.0/24 | Dokumentationszwecke | RFC 6890 |
| 203.0.113.0/24 | Dokumentationszwecke | RFC 6890 |
| 224.0.0.0/4 | Multicasts | RFC 5771 |
| 240.0.0.0/4 | Reserviert | RFC 1700 |
| 255.255.255.255/32 | Limited Broadcast | RFC 919, RFC 922 |

## Private IP-Adressen

Bestimmte IP-Adressbereiche stehen zur freien Verfügung und können ohne vorherige Registrierung für private Netze verwendet werden. Im Internet werden diese IP-Adressbereiche nicht geroutet. Historisch befand sich jeder der Adressbereiche in einer anderen Netzklasse. Aus Gewohnheitsgründen ist es gängig für Subnetze im Adressblock 172.16.0.0/12 die Präfixlänge /16 und im Adressblock 192.168.0.0/16 die Präfixlänge /24 zu verwenden. Eine Vorgabe existiert diesbezüglich nicht.

## Paketformat

Ein IP-Paket besteht aus einem Header und den eigentlichen Nutzdaten. Der IPv4-Header ist normalerweise 20 Bytes lang, kann aber durch zusätzliche Optionen in jeweils 4-Byte-Schritten auf bis zu 60 Bytes verlängert werden. Die Optionen sind größtenteils ungenutzt und IPv4-Pakete mit Optionen werden oft blockiert.

IPv4 dient als Grundlage, um darüber andere Protokolle zu transportieren. In dem Datenteil eines IP-Pakets werden der Header, die Nutzdaten und ein eventueller Trailer eines anderen Netzwerkprotokolls gekapselt. Typische Beispiele sind TCP, UDP oder ICMP. Um welches Protokoll es sich handelt, wird durch eine Nummer im Protokoll-Feld des IP-Headers festgelegt. Die Internet Assigned Numbers Authority verwaltet eine Liste der registrierten Protokollnummern.

Die maximale Länge eines IP-Pakets beträgt 65535 Bytes ($2^{16}-1$) und die maximale Datenlänge 65515 Bytes (Paketlänge – minimale Headerlänge von 20 Byte). Die Paketlänge wird jedoch normalerweise von dem zugrundeliegenden Netzwerkprotokoll auf Netzzugangsschicht weiter eingeschränkt, woraus sich eine für das Netz spezifische maximale IP-Paketlänge ergibt, die Maximum Transmission Unit (MTU) genannt wird. Bei Ethernet beispielsweise beträgt die MTU 1500 Bytes. Die MTU reduziert sich, wenn ein IP-Paket über einen Tunnel oder ein Virtual Private Network transportiert wird. Die minimale Frame-Länge von Ethernet hat hingegen keine Auswirkung auf IPv4, da durch das Längenfeld im IPv4-Header ein beliebig kurzes IPv4-Paket transportiert werden kann, selbst wenn der Ethernet-Frame mit Nullbytes aufgefüllt werden muss.

Eine spezielle Bedeutung kommt in modernen Implementierungen dem früheren Feld Type of Service (ToS) im zweiten Oktett des IPv4-Headers zu. Ursprünglich diente dieses Feld bei der Vermittlung eines Datenpaketes als Entscheidungshilfe für die beteiligten Router bei der Wahl der Übertragungsparameter. In modernen Implementierungen wird dieses Feld im Zusammenhang mit der network congestion avoidance (Vermeidung von Überlastungen) verwendet. Das ToS-Feld wurde durch das DS-Feld (differentiated services) ersetzt, dessen erste sechs Bits als differentiated services code point (DSCP) und dessen letzte beiden Bits als explicit congestion notification (ECN) benutzt werden.

## Routing

IPv4 unterscheidet nicht zwischen Endgeräten (Hosts) und Vermittlungsgeräten (Router). Jeder Computer und jedes Gerät kann gleichzeitig Endpunkt und Router sein. Ein Router verbindet dabei verschiedene Netze. Die Gesamtheit aller über Router verbundenen Netze bildet das Internet.

IPv4 ist für LANs und WANs gleichermaßen geeignet. Ein Paket kann verschiedene Netze vom Sender zum Empfänger durchlaufen, die Netze sind durch Router verbunden. Anhand von Routingtabellen, die jeder Router individuell pflegt, wird der Netzteil einem Zielnetz zugeordnet. Die Einträge in die Routingtabelle können dabei statisch oder über Routingprotokolle dynamisch erfolgen. Die Routingprotokolle dürfen dabei sogar auf IP aufsetzen.

Bei Überlastung eines Netzwerks oder einem anderen Fehler darf ein Router Pakete auch verwerfen. Pakete desselben Senders können bei Ausfall eines Netzes auch alternativ „geroutet“ werden. Jedes Paket wird dabei einzeln „geroutet“, was zu einer erhöhten Ausfallsicherheit führt.

Beim Routing über IP können daher

- einzelne Pakete verlorengehen,
- Pakete doppelt beim Empfänger ankommen,
- Pakete verschiedene Wege nehmen,
- Pakete fragmentiert beim Empfänger ankommen.

Wird TCP auf IP aufgesetzt (d. h. die Daten jedes IP-Pakets enthalten ein TCP-Paket, aufgeteilt in TCP-Header und Daten), so wird neben dem Aufheben der Längenbeschränkung auch der Paketverlust durch Wiederholung korrigiert. Doppelte Pakete werden erkannt und verworfen. Die Kombination TCP mit IP stellt dabei eine zuverlässige bidirektionale Verbindung eines Datenstroms dar.

## Paketfragmentierung

Auf dem Weg vom Sender zum Empfänger kann es vorkommen, dass ein IP-Paket ein Netz durchlaufen muss, bei dem das Paket länger ist als die vom Netz maximal unterstützte Paketlänge (MTU). In einem solchen Fall kann der Router entweder eine Fehlermeldung zurücksenden oder das Paket in Fragmente aufteilen und in separaten IP-Paketen weiter versenden. Jedes der Fragmente trägt dieselbe Identifikationsnummer im Header, mit denen der Empfänger eine Zusammensetzung vornehmen kann. Die Fragmentierung erfolgt in folgenden Schritten:

- Aufteilen der Nutzdaten an einer 8-Byte-Grenze (das letzte Fragment enthält dann nicht unbedingt ein Vielfaches von 8 Byte Daten).
- Kopieren der IP-Headerdaten des Originalpakets in die neuen Header der Fragmente.
- Setzen des Felds „More Fragments“ auf den Wert 1 bei allen bis auf das letzte Fragment.
- Beim letzten Fragment wird der Wert von „More Fragments“ aus dem Originalpaket kopiert. Im Regelfall ist der Wert 0, kann aber auch 1 sein, falls das Originalpaket bereits ein Fragment ist.
- Setzen der Längen-Felder und des Fragment-Offsets in den Headern. Das Fragment-Offset gibt die Position eines Datenfragments im Originalpaket an (als Vielfaches von 8 Bytes).

Um ein Paket wieder zusammenzusetzen, kombiniert der Empfänger alle Fragmente, welche die gleiche Identifikationsnummer, den gleichen Absender, Empfänger und das gleiche Protokoll haben. Die Reihenfolge der Fragmente ergibt sich aus dem jeweiligen Fragment-Offset im Header. Das letzte Fragment erkennt der Empfänger daran, dass das Feld „More Fragments“ auf 0 gesetzt ist.

## ICMP

IP ist eng verknüpft mit dem Internet Control Message Protocol (ICMP), das zur Fehlersuche und Steuerung eingesetzt wird. ICMP setzt auf IP auf, das heißt ein ICMP-Paket wird im Datenteil eines IP-Pakets abgelegt. Eine IP-Implementierung enthält stets auch eine ICMP-Implementierung. ICMP besteht aus verschiedenen Pakettypen, die unterschiedlichen Funktionen dienen. Ein prominentes Beispiel sind „Echo Request“ und „Echo Reply“, was für das Diagnosewerkzeug Ping verwendet wird. Auch Traceroute verwendet ICMP.

ICMP kann zusammen mit dem Don’t-Fragment-Bit des IP-Pakets auch eingesetzt werden, um die maximale Paketgröße eines Übertragungsweges zu einer Zieladresse zu ermitteln. Dies wird als Path MTU Discovery bezeichnet und ermittelt die kleinste MTU aller passierten Netze. Dadurch kann auf IP-Fragmentierung verzichtet werden, wenn der Sender nur Pakete mit der maximalen Größe der PMTU erzeugt.

## Netzzugangsschicht

IPv4 kann auf verschiedene Übertragungsmedien und Protokolle in der Netzzugangsschicht aufsetzen, zum Beispiel das Point-to-Point Protocol oder Serial Line Internet Protocol. In lokalen Netzen wird überwiegend Ethernet oder WLAN eingesetzt. Beide verwenden eine 48 Bit lange MAC-Adresse zur Adressierung von Netzwerkkarten. Ein Sender muss die MAC-Adresse des Ziels kennen, bevor ein IP-Paket gesendet werden kann. Um für eine gegebene IP-Adresse des Ziels die zugehörige MAC-Adresse zu ermitteln, wird das Address Resolution Protocol (ARP) verwendet. Unbekannte MAC-Adressen fragt der Sender mittels einer ARP-Anfrage an, die er als Broadcast an alle Netzwerkgeräte im lokalen Netz sendet. Das Ziel sendet daraufhin eine ARP-Antwort zurück, die die gesuchte MAC-Adresse enthält. Die Kommunikationsteilnehmer speichern die gelernten Zuordnungen von IP-Adresse zu MAC-Adresse in einem Cache zwischen.

## Adressknappheit

Aufgrund des unvorhergesehenen Wachstums des Internets herrscht heute Adressknappheit. Im Januar 2011 teilte die IANA der asiatisch-pazifischen Regional Internet Registry APNIC die letzten zwei /8-Adressblöcke nach der regulären Vergabepraxis zu. Gemäß einer Vereinbarung aus dem Jahr 2009 wurde am 3. Februar 2011 schließlich der verbliebene Adressraum gleichmäßig auf die regionalen Adressvergabestellen verteilt: jeweils ein /8-Adressblock pro Vergabestelle. Seitdem hat die IANA auf der globalen Ebene keine weiteren /8-Adressblöcke mehr zu vergeben.

Auf der regionalen Ebene verschärften die Regional Internet Registrys ihre Vergabepraktiken, um aus dem letzten /8-Adressblock möglichst lange schöpfen zu können. Bei der APNIC traten diese am 15. April 2011 in Kraft, da die zuvor erhaltenen beiden /8-Adressblöcke bereits nach drei Monaten aufgebraucht waren. Am 14. September 2012 folgte dann RIPE NCC mit der letzten regulären Zuteilung in der Region Europa/Naher Osten. Mit der neuen Vergabepraxis hatten APNIC- und RIPE-NCC-Mitglieder jeweils nur noch Anspruch auf Zuteilung eines /22-Adressbereichs, selbst wenn sie einen größeren Bedarf nachweisen konnten.

Am 25. November 2019 hat RIPE NCC ihren /8-Adressblock endgültig aufgebraucht. Seitdem werden nur noch /24-Kleinstblöcke per Warteliste aus Rückläufern vergeben.

## Adressfragmentierung

Die historische Entwicklung des Internets wirft ein weiteres Problem auf: Durch die mit der Zeit mehrmals geänderte Vergabepraxis von Adressen des IPv4-Adressraums ist dieser inzwischen stark fragmentiert, d. h., häufig gehören mehrere nicht zusammenhängende Adressbereiche zur gleichen organisatorischen Instanz. Dies führt in Verbindung mit der heutigen Routingstrategie (Classless Inter-Domain Routing) zu langen Routingtabellen, auf welche Speicher und Prozessoren der Router im Kernbereich des Internets ausgelegt werden müssen. Zudem erfordert IPv4 von Routern, Prüfsummen jedes weitergeleiteten Pakets neu zu berechnen, was eine weitere Prozessorbelastung darstellt.

## IPv6

Weil die IPv4-Adressen auszugehen drohten, wurde IPv6 als 128-Bit-Adressen entwickelt. Diese werden in acht hexadezimale 4er-Gruppen dargestellt und die Gruppen durch Doppelpunkte getrennt. Damit können $2^{128} = 65.5368 \approx 340$ Sextillionen IPv6-Adressen vergeben werden, eine extrem hohe Zahl. Zusätzlich wurde die Systematik der Adress-Struktur wesentlich verbessert. Verfügbar sind die Adressen seit 2017.

IPv6-Beispiel: 2001:0db8:85a3:08d3:1319:8a2e:0370:7344

# IPv6

IPv6 (Internet Protocol Version 6) ist eine IP-Protokollversion, die von der Internet Engineering Task Force (IETF) erarbeitet wurde. Diese Protokollversion soll das bisher verwendete IP-Protokoll Version 4 (IPv4) ablösen und stellt ein standardisiertes Verfahren zur Übertragung von Datenpaketen in Rechnernetzen dar. Zentrale Funktionen von IPv6 sind die Adressierung von Netzwerkelementen über sogenannte IPv6-Adressen sowie die Paketweiterleitung zwischen Teilnetzen (Routing). Einer der Hauptgründe für die Entwicklung von IPv6 ist die Knappheit an öffentlichen Internetadressen. IPv4 verwendet 32-Bit-Adressen. Daraus ergibt sich ein Adressraum mit ca. 4,3 Milliarden Adressen. IPv6 verwendet dahingegen IPv6-Adressen mit einer Länge von 128 Bit. Diese Adresslänge erlaubt eine unvorstellbare Menge von 2^ 128 oder 3,4 x 10^38 IPv6-Adressen.

## Aufbau einer IPv6-Adresse

IPv6-Adressen bestehen aus 8 Blöcken zu 16 Bit mit jeweils vierstelligen hexadezimalen Zahlen. Diese Blöcke werden jeweils durch einen Doppelpunkt getrennt. Beispiel:

- 2001:0620:0000:0000:0211:24FF:FE80:C12C

Die vorderen 64-Bit werden für das Routing verwendet und bezeichnen das Netzwerkpräfix. Das Netzwerkpräfix kennzeichnet das Netzwerk, das Subnetz bzw. den Adressbereich. Die hinteren 64-Bit werden als Interface Identifier (IID) bezeichnet. Der Interface Identifier kennzeichnet einen Host in diesem Netz und wird aus der 48-Bit-MAC-Adresse des Interfaces gebildet und in eine 64-Bit-Adresse umgewandelt. Hierbei handelt es sich um das modifizierte EUI-64-Format. Somit ist das Interface unabhängig vom Netzwerkpräfix eindeutig identifizierbar.

Die von IPv4 bekannte Netz- bzw. Subnetzmaske fällt bei IPv6 ersatzlos weg. Um trotzdem eine Segmentierung durchführen zu können, wird die Präfixlänge definiert und mit einem "/" (Slash) an die eigentliche IPv6-Adresse angehängt. Beispiel:

Ein Subnetzwerk mit den IPv6-Adressen 2001:0820:9511:0000:0000:0000:0000:0000 bis 2001:0820:9511:FFFF:FFFF:FFFF:FFFF:FFFF kann mit der Notation 2001:0820:9511::/48 beschrieben werden.

## Adresszuweisung

In der Regel bekommen Internetprovider (ISP) von der RIR /32-Netze zugeteilt, die diese wiederum in Subnetze gliedern. An Endkunden werden entweder /48-Netze oder /56-Netze vergeben.

## Privacy Extensions

Eine IPv6-Adresse, die auf dem modifizierten EUI-64-Format beruht, lässt Rückschlüsse auf die zugrundeliegende MAC-Adresse zu. Da dies bei Nutzern Bedenken bezüglich des Datenschutzes hervorrufen könnte, wurde mit Privacy-Extensions ein Verfahren entwickelt, um den Hostanteil der IPv6-Adressen zu anonymisieren. Zu diesem Zweck hebt Privacy Extensions die Kopplung von Interface Identifier und MAC-Adresse auf und generiert temporäre Interface Identifier für ausgehende Verbindungen.

## Notationsregeln

Weil IPv6-Adressen sehr lang sein können, werden sie in der Regel gekürzt. In RFC 5952 wurden diesbezüglich verbindliche Notationsregeln definiert. Diese beinhalten unter Anderem folgende Regeln:

- Führende Nullen innerhalb eines Blockes dürfen ausgelassen werden.
- Ein einzelner Block aus 4 Nullen wird zu einer Null zusammengefasst.
- Aufeinanderfolgende Blöcke deren Wert 0 bzw. 0000 beträgt, werden durch zwei Doppelpunkte ("::") gekürzt. Diese Kürzung darf jedoch nur einmal in einer Adresse vorgenommen werden, da sonst die Eindeutigkeit verloren geht. Beispiel:
  - Die Adresse 2001:0dc8:0:0:8d5:0:0:0 muss somit wie folgt gekürzt werden: 2001:0dc8:0:0:8d5:0:: oder 2001:0dc8:0::8d5:0:0:0
- Sind mehrere Null-Sequenzen in der Adresse enthalten, darf nur die am weitesten links stehende Sequenz ersetzt werden.

## URL-Notation

In einer URL werden IPv6-Adressen in eckige Klammern eingeschlossen. Beispiel:

http://[2001:0db8:83a3:08d3::0380:7344]/

Portnummern müssen hinter der schließenden Klammer stehen. Diese werden mit einem Doppelpunkt abgetrennt.

http://[2001:0db8:83a3:08d3::0380:7344]:8080/

Das Prozentzeichen (%) wird weiterhin für die Kennzeichnung der hexadezimalen Zeichencodierung in URLs verwendet. Innerhalb der URL muss das Prozentzeichen durch seinen eigenen Hex-Code "%25" ersetzt werden (RFC 6874). Dies ist notwendig, wenn man die Verbindung über eine bestimmte Schnittstelle erzwingen will.

## IPv6-Adresstypen

Wie bei IPv4 wurden auch bei IPv6 verschiedene Adressbereiche mit speziellen Aufgaben und Eigenschaften definiert. Diese wurden in RFC 4291 und RFC 5156 spezifiziert und lassen sich bereits durch die ersten Bits einer IPv6-Adresse, das sogenannte Formatpräfix, identifizieren.

### Loopback-Addressen:

Die Adresse 0:0:0:0:0:0:0:1 (auch ::1/128) wird Loopback-Adresse genannt. Es handelt sich um die Adresse des eigenen Standorts.

### Link-Local-Adressen:

Link-Local-Adressen sind nur innerhalb von lokalen Netzwerken gültig und beginnen mit dem Formatpräfix FE80::/10. Diese Adressen werden zur Adressierung von Elementen innerhalb eines lokalen Netzwerks sowie zur Autokonfiguration oder für die Neighbour-Discovery verwendet. In der Regel reicht der Geltungsbereich einer Link-Local-Adresse bis zum nächsten Router, sodass jedes an das Netzwerk angebundene Gerät in der Lage ist, mit diesem zu kommunizieren, um sich eine globale IPv6-Adresse zu generieren. Dieser Prozess wird Neighbor Discovery genannt.

Unique-Local-Adressen: Für private lokale Netze wurden für das IPv6-Protokoll reservierte Adressbereiche definiert. Diese werden in RFC 4193 beschrieben und haben eine ähnliche Funktion wie die privaten Adressebereiche, die im IPv4-Protokoll festgelegt sind. Unique-Local-Adressen befinden sich im Adressbereich "fc00::/7" (fc00… bis fdff…) und werden nicht im Internet geroutet. Vielmehr sind sie nur inerhalb eines definierten Netzwerkbereichs gültig. Unterscheiden muss man zwischen dem Präfix "fc" und "fd", da diese unterschiedliche Bedeutungen haben. Während IPv6-Adressen mit dem Präfix fc vom Provider vergeben werden, können IPv6-Adressen mit dem Präfix fd im eigenen lokalen Netzwerk verwendet werden.

Global-Unicast-Adressen: Bei Global-Unicast-Adressen handelt es sich um weltweit einmalige Adressen, die weltweit geroutet werden. Diese werden von einem Netzwerkgerät benötigt, um eine Verbindung zum Internet aufzubauen. Ein Host kann mehrere dieser IPv6-Adressen besitzen. Diese werden vom Host mittels Autokonfiguration bezogen.

Multicast-Adressen: Mit Multicast-Adressen kann man eine Eins-zu-viele-Kommunikation realisieren. Pakete, die an eine Multicast-Adresse gesendet werden, erreichen alle Netzwerkgeräte, die Teil der Multicast-Gruppe sind. Hierbei kann ein Gerät parallel mehreren Multicast-Gruppen angehören. Wird für ein Netzwerkgerät eine IPv6-Unicast-Adresse erstellt, wird dieses automatisch Mitglied von bestimmten Multicast-Gruppen, die für die Erkennung, Erreichbarkeit und Präfixermittlung benötigt werden. Multicast-Adressen sind durch das Präfix "ff::/8" gekennzeichnet. Danach folgen 4 Bit für Flags und weitere 4 Bit für die Angabe des Multicast Scopes.

Multicast-Adressen enden mit einer Nummer, die für eine Multicast-Gruppe steht. Eine Liste der Multicast-Gruppen finden Sie unter https://www.iana.org/assignments/ipv6-multicast-addresses/ipv6-multicast-addresses.xhtml

Anycast-Adressen: Adressen dieses Typs können an Gruppen von Empfängergeräten adressiert werden. Die Datenpakete werden hierbei nur an das Gerät gesendet, das dem Sender am nächsten ist. Anycast-Adressen kommen daher im Rahmen der Lastenverteilung und Ausfallsicherheit zum Einsatz.

## IPv6-Paketformat

Das IPv6-Protokoll zeichnet sich durch ein vereinfachtes Paketformat aus. Der Header verfügt über eine feste Länge von 40 Bytes. Optionale Informationen werden in Extension Headers zwischen dem IPv6-Kopfdatenbereich und der eigentlichen Nutzlast ausgelagert. So können Optionen eingefügt werden, ohne dass sich der Header verändert. Zu den Informationen, die IPv6-Kopferweiterungen beinhalten können, zählen unter anderem Knoten-zu-Knoten-Optionen, Zieloptionen, Routing-Optionen sowie Optionen zu Fragmentierung, Authentifikation und Verschlüsselung. Weitere Informationen zum IPv6-Paketformat finden Sie in RFC 2460.

## Stateless Address Autoconfiguration

Die Stateless Address Autoconfiguration (SLAAC) ist ein Verfahren zur zustandslosen und automatischen Konfiguration von IPv6-Adressen an einem Netzwerk-Interface. Mittels dieses Verfahrens kann ein Host vollautomatisch eine funktionsfähige Internetverbindung aufbauen. Stateless bedeutet in diesem Zusammenhang, dass die jeweilige IPv6-Adresse nicht zentral vergeben und gespeichert wird. Vielmehr erzeugt der Host zur initialen Kommunikation mit dem Router eine link-lokale IPv6-Adresse und weist sich diese zu. Mit dieser link-lokalen IPv6-Adresse kann ein Gerät mittels des Neighbour Discovery

Protocols (NDP) nach den Routern in seinem Netzwerksegment suchen. Dies geschieht durch eine Anfrage an die Multicast-Adresse, über die alle Router eines Segments erreichbar sind.

Nach dem Erhalt einer solchen Anfrage versendet ein Router Informationen zu verfügbaren Präfixen. Um die doppelte Vergabe von IPv6-Adressen zu vermeiden, führt der Host bei einer neu generierten IPv6-Adresse eine Duplicate Address Detection (DAD) durch. Dazu schickt der Host eine Anfrage an die generierte Adresse ins lokale Netz. Als Antwort-Adresse dient eine Multicast-Adresse. Wenn eine andere Station die IPv6-Adresse bereits nutzt, kommt eine Antwort zurück. Wenn keine Antwort von dieser Adresse zurückkommt, verwendet der Host die IPv6-Adresse für die Kommunikation.

## Neighbour Discovery Protocol

Das Neighbour Discovery Protocol (NDP) ist ein IPv6-Protokoll. Es wird unter anderem verwendet, um IPv6-Adressen in Link-Layer-Adressen (MAC-Adressen) aufzulösen. Darüber hinaus wird es zum Aktualisieren der gecachten Adressen verwendet. Wenn sich ein Knoten nicht im gleichen Netzwerk befindet, wird NDP verwendet, um einen Router zu finden, der die Pakete weiterleiten kann. Ferner erfüllt dieses Protokoll unter anderem noch folgende Aufgaben:

- Parameterermittlung
- Stateless Address Autoconfiguration
- Adressauflösung (Address Resolution mit Neighbor Discovery)
- Erkennung der Nichterreichbarkeit des Nachbarn (Neighbor Unreachability Detection, NUD)
- Erkennung doppelter Adressen (Duplicate Address Detection, DAD)
- Umleitung (Redirect)

## DHCP6

DHCP ist ein Protokoll, das für die Verwaltung der IP-Konfiguration in einem TCP/IP-Netzwerk verwendet wird. Dieses ermöglicht es, angeschlossene Clients ohne manuelle Konfiguration der Netzwerkschnittstelle in ein bestehendes Netzwerk einzubinden. In einem IPv6-Netzwerk wird DHCP6 eigentlich nicht benötigt, da diese Aufgabe durch die Stateless Address Autoconfiguration (SLAAC) übernommen wird. Es können jedoch gute Gründe für die Verwendung von DHCP6 sprechen. Dies trifft z. B. zu, wenn der IPv6-Client die Optionen der IP-Konfiguration nicht mittels Stateless Address Autoconfiguration entgegen nehmen kann. In diesem Fall können mittels Stateless Address Autoconfiguration die IP-Adresse und mittels DHCP6 die restlichen Konfigurationsparameter zugeteilt werden.