IP-Adressen

Was ist eine IP-Adresse?

Eine IP-Adresse (kurz: IP, das steht für Internet Protocol) ist die eindeutige Adresse eines Geräts in einem Netzwerk. Ähnlich einer postalischen Adresse ermöglicht sie den gerichteten Datenaustausch zwischen Netzwerkkomponenten. So wird sichergestellt, dass Datenpakete zuverlässig ihr Ziel erreichen, ohne Verwechslungen. Heutzutage gibt es IPv4 und IPv6-Adressen. Das v4 bzw. v6 steht tatsächlich für die Versionsnummer. Mit v5 wurde nur experimentiert, diese Version wurde nie veröffentlicht.

Aufbau einer IPv4-Adresse

Eine IPv4-Adresse ist eine 32 Bit lange Zahl, aufgeteilt in vier Byte (oder auch vier Oktette). Jedes Oktett kann die Zahlen 0 bis 255 (Binär: 00000000 - 11111111) annehmen. Wir haben also 2^{32} oder knapp 4,3 Milliarden IPv4-Adressen.
IPv4-Adressen setzen sich immer aus einem Netzwerkanteil und einem Hostanteil zusammen. Wo der Netzwerkanteil aufhört und der Hostanteil anfängt, bestimmt die Subnetzmaske.

Klassen von IPv4-Adressen

Klasse	Bereich	Netzwerkanteil	Anwendungsbeispiel
A	**1.0.0.0 - 126.255.255.255**	Erstes Oktett	Große Unternehmen / Provider
B	**128.0.0.0 - 191.255.255.255**	Ersten beiden Oktette	Mittlere Netzwerke wie z.B. Unis
C	**192.0.0.0 - 223.255.255.255**	Ersten drei Oktette	Kleine Netzwerke wie z.B. LAN
D	**224.0.0.0 - 239.255.255.255**		Multicast (Gruppenkommunikation)
E	**240.0.0.0 - 255.255.255.255**		Reserviert (Experimente)

Besondere IPv4-Adressen

0.0.0.0	Standartroute (Default route) / "Alle Adressen"
127.0.0.1	Loopbackadresse (lokaler Rechner)
255.255.255.255	Broadcast alle Geräte im Internet

Funfakt
127.0.0.1 ist nicht die einzige Loopbackadresse. Vielmehr ist es **127.0.0.0/8** oder der IP-Bereich **127.0.0.1 - 127.255.255.254**, also gute 16 Millionen Möglichkeiten sich selbst zu "pingen".

Private IPv4-Adressbereiche

Es gibt drei private Adressbereiche bei IPv4-Adressen, die nur für den privaten Bereich vorgesehen sind und nicht im Internet geroutet werden können.

10.0.0.0	-	10.255.255.255	Klasse A
172.16.0.0	-	172.31.255.255	Klasse B
192.168.0.0	-	192.168.255.255	Klasse C

IPv4-Adressen sind knapp!

IPv4 wurde in den 1980er-Jahren eingeführt. Mit seinen 32-Bit und über 4 Milliarden Adressen hat man gedacht, das wäre mehr als ausreichend. Deshalb waren die Erfinder anfangs sehr großzügig und vergaben Klasse-A-Netzwerke mit jeweils ca. 16,7 Millionen Adressen an großen Firmen und Institutionen, wie General Electric, IBM, HP, das MIT, sowie an das Militär und Geheimdienste.
Als dann in den 1990er-Jahren allmählich klar wurde, dass die Adressen knapp werden, begann man gegenzusteuern. Eine der wichtigsten Maßnahmen war die Einführung von Classless Inter-Domain Routing (CIDR), wodurch die starre Einteilung in Klassen aufgehoben wurde und Adressräume flexibler genutzt werden konnten. Einige Unternehmen gaben ihre Klasse-A-Netze sogar freiwillig zurück, um die Lebensdauer von IPv4 zu verlängern.

Darüber hinaus wurde NAT (Network Address Translation, auf Deutsch: Netzwerkadressübersetzung) eingeführt, ebenso wie die Definition der heute gängigen privaten IPv4-Adressbereiche.

Was macht CIDR?

Das Classless Inter-Domain Routing (Deutsch: Klassenloses Inter-Domain-Routing) verwendet eine flexible Präfixnotation (z.B. /24), um Netzwerke beliebiger Größe zu definieren, statt fixer und starrer Klassen. Dadurch können Adressen passgenauer vergeben und große Blöcke zusammengefasst werden, was die Größe der globalen Routing-Tabellen reduziert. Dieser Präfix gibt an, wie viele Bits der Adresse, von links nach rechts gezählt, unveränderlich fest stehen. Bei dem Netzwerk **192.168.0.0/24** zum Beispiel bleibt die **192.168.0.** immer gleich und nur die hinterste Zahl ist veränderlich. **192.168.1.x** ist dann ein anderes Netzwerk.

Was macht NAT?

In Heim- und Firmennetzwerken werden IP-Adressen aus den privaten IPv4-Bereichen verwendet. Der Zugang zum Internet erfolgt dabei in der Regel über einen Router. Dieser Router erhält vom Internetanbieter (ISP - Internet Service Provider) eine öffentliche IP-Adresse. Der Router verwendet NAT, um die privaten IPs des lokalen Netzwerks in die öffentliche IP des Routers zu übersetzen, wenn Daten ins Internet gesendet werden, und umgekehrt, wenn Daten aus dem Internet empfangen werden. So können mehrere Geräte im lokalen Netzwerk gleichzeitig das Internet nutzen, ohne jeweils eine eigene öffentliche IP-Adresse zu benötigen. Sie teilen sich alle die IP des Routers und dieser sorgt dafür, dass alle Daten zu den richtigen Empfängern gelangen.

NAT nur als Übergangslösung?

Die Einführung von NAT war ein wichtiger Schritt, um der IPv4-Adressknappheit kurzfristig entgegenzuwirken. Da jedoch die Zahl der internetfähigen Geräte förmlich explodierte und NAT gewisse Nachteile mit sich bringt - wie erhöhte Komplexität bei Anwendungen wie Peer-to-Peer-Kommunikation - wurde schließlich IPv6 eingeführt.

Aufbau einer IPv6-Adressen

Eine IPv6-Adresse ist eine 128-Bit lange Zahl, die in acht Böcke von jeweils 16-Bit, getrennt durch Doppelpunkte, aufgeteilt ist. Ein Block wird oft Hextett genannt, aber auch Segment, Quartett, oder 16-Bit-Block, aber eigentlich haben die einzelnen Blöcke noch keinen einheitlichen Namen. Jedes Hextett hat vier hexadezimale Ziffern und kann die Werte **0000 - ffff (0 - 65535)** annehmen, wobei letztendlich jede Ziffer wieder für eine 4-Bit Binärzahl steht **(0000 - 1111)**. Eine typische IPv6-Adresse sieht wie folgt aus: **2001:0db8:85a3:0000:0000:8a2e:0370:7334**.
Mit dieser Version vom Internet Protokoll haben wir jetzt $\mathbf{2^{128}}$ IPv6-Adressen. Ausgeschrieben: **340.282.366.920.938.463.463.374.607.431.768.211.456**. Das sind mehr als $\mathbf{10^{28}}$ IPs pro Mensch auf der Erde (Bei aktuell 8 Milliarden Menschen)

IPv6-Adressabkürzungen

Führende Nullen in einem Hextett dürfen weggelassen werden. Aus der obigen IPv6 wird also: **2001:db8:85a3:0000:0000:8a2e:370:7334**.
Des Weiteren dürfen Blöcke, welche ausschließlich mit Nullen gefüllt sind, ebenfalls weggelassen werden (aber nur ein Mal pro Adresse), stehen bleiben müssen dann die Doppelpunkt vor und nach den weggelassenen Nullen: **2001:db8:85a3::8a2e:370:7334**.

IPv6-Adressaufteilung

Eine IPv6-Adresse besteht typischer Weise aus zwei Teilen, dem 64-Bit langen Netzwerkpräfix, der vergleichbar ist mit dem Netzanteil bei IPv4-Adressen, gefolgt von dem ebenfalls 64-Bit langen Interface-Identifier (Schnittstellenidentifizierer), was die eindeutige Kennung eines Host im Netzwerk ist. Der Interface-Identifier wird oft aus der MAC-Adresse generiert, oder ist zufällig.

IPv6-Adressarten

Es gibt unterschiedliche Arten von IPv6-Adressen, die sich teilweise an ihrem Präfix erkennen lassen.
Zum Einen gibt es die Unicast-Adressen, welche sich aufteilen in Global Unicast, Link-Local und Unique Local.
Es gibt aber auch noch die Multicast- und Anycast-Adressen.

Unicast-Adressen

Global Unicast	Öffentlich routbar im Internet. Adressbereich: **2000:: - 3fff:ffff:ffff:ffff:...** Kurz: **2000::/3** Aktuell noch fast ausschließlich **2000::/4**
Link-local	Nur im lokalen Netzwerk gültig. Adressbereich: **fe80:: - febf:ffff:ffff:ffff:...** Kurz: **fe80::/10** In der Praxis meist **fe80::/64**
Unique local	Ähnlich privaten IPv4-Adressen. Adressbereich: **fc00:: - fdff:ffff:ffff:ffff:...** Kurz: **fc00::/7** **fd00::/8** ist als Standard festgelegt.

Multicast

Multicast ist ein zentrales Konzept von IPv6 und ersetzt die IPv4-Broadcast-Adressen durch eine effizientere und flexiblere Gruppenkommunikation. Im Gegensatz zu Broadcasts, welche alle Hosts im Netzwerk belasten, oder Unicast (1:1 Kommunikation) ermöglicht Multicast die gezielte Ansprache von Empfängergruppen (1:n oder m:n), die sich explizit für bestimmte Dienste oder Nachrichten "interessieren".

Multicast-Adressformat

Der theoretische Adressbereich von Multicast ist: **ff00::/8**, das dritte "Hex" (oder die dritte Stelle, also die Bits 9-12) ist hier allerdings eine Flag (im Sinne von "Signalflagge"), die zusätzliche Informationen über die Multicast-Adresse gibt, und das vierte "Hex" (also die vierte Stelle, oder die Bits 13-16) ein Scope (Bereich), welches den Gültigkeitsbereich definiert.

8-Bit	4-Bit	4-Bit	112-Bit
ff	Flag	Scope	Gruppen ID

Flags 4-Bit

Wert	Bedeutung	Beschreibung
0	Permanent (well-known)	Von der IETF* definiert. (* siehe Anmerkung Unten)
1	Transient (temporär)	Dynamisch, wird z.B. durch Anwendungen erzeugt.
2	Nicht verwendet	Reserviert
4	Rendezvous Point (RPL)	Speziell für Routingprotokolle.

Die Flags 3 und 5 - F sind nicht dokumentiert, also frei oder für zukünftige Zwecke reserviert.

Anmerkung: Die Internet Engineering Task Force (IETF) - auf Deutsch etwa Arbeitsgruppe für Internettechnik - ist eine bedeutende Organisation, welche sich mit der technischen Weiterentwicklung des Internets beschäftigt, mit dem Ziel Internetstandards und sogenannte "Best Practices" zu entwickeln. Sie setzt sich zusammen aus Netzwerktechnikern, Herstellern, Netzbetreibern, Forschern und Anwendern - jeder kann mitwirken. Bei Regelmäßigen Treffen werden Arbeitsgruppen zu spezifischen Themen, wie Protokolle, Sicherheit oder Netzwerktechnologie, gebildet.
Die Ergebnisse der IETF-Arbeit werden in sogenannten RFCs (*Requests for Comments*) veröffentlicht. Dabei gibt es sowohl rein informelle RFCs als auch solche mit verbindlichem Charakter, die als Standard anerkannt sind (sogenannte Standards-Track RFCs). Diese sind zwar nicht gesetzlich vorgeschrieben, doch wer sich nicht an sie hält, läuft Gefahr, mit etablierten Systemen nicht kompatibel zu sein.
Beispielsweise wurde IPv4 in der verbindlichen RFC 791 im Jahr 1981 definiert, während IPv6 mit RFC 2460 im Jahr 1998 eingeführt wurde.

Scopes 4-Bit

Hex	Name	Beschreibung
1	Interface-Local	Nur auf dem Gerät selbst.
2	Link-Local	Innerhalb des lokalen Netzwerksegments.
3	Subnet-Local	Innerhalb des selben Subnetzes. (veraltet und kaum genutzt)
4	Admin-Local	Innerhalb einer administrativen Domain.
5	Site-Local	Innerhalb einer gesamten Site. (z.B. Campus, Firma)
8	Organization-Local	Innerhalb einer Organisation.
E	Global	Weltweit gültig, also internetweit.

Die Scopes 0, 6, 7, 9 - D und F werden nicht verwendet und/oder sind für zukünftige Zwecke reserviert.

Anmerkung: ff02::1 erreicht alle Knoten (Nodes) im lokalen Netzwerk, wobei ein Knoten jedes Gerät ist, welches eine oder mehrere IP-Adressen benutzen kann, wie Drucker, Server, IP-Telefone, IoT-Geräte, während sich das Interface nur auf die Schnittstelle des Knotens bezieht.

Anycast

Bei Anycast wird, wie bei Unicast, eine einzelne IPv6-Adresse vergeben, allerdings an mehrere Geräte, meist Server oder Router, gleichzeitig. Diese Geräte befinden sich an unterschiedlichen Orten im Netzwerk oder weltweit verteilt.
Wenn ein Gerät ein Paket an eine solche Anycast-Adresse sendet, wird es immer an den, aus Routing-Sicht, "nächstgelegenen" Knoten weitergeleitet. Was als "nächstgelegen" gilt, entscheidet das Routingprotokoll, basierend auf Kriterien wie Hop-Anzahl, Latenz oder administrative Kosten.

Wichtig: Die Adresse sieht aus wie eine normale Unicast-Adresse. Anycast wird durch das Routingverhalten bestimmt, nicht durch einen speziellen Adressbereich oder Präfix.

Vorteile von Anycast

- **Hohe Verfügbarkeit:** Fällt ein Knoten aus, übernimmt automatisch der Nächstbeste.
- **Lastverteilung:** Anfrage werden auf mehrere Server verteilt, ohne dass der Client es merkt.
- **Niedrige Latenz:** Clients erreichen automatisch den "nächstgelegenen" Server.
- **Einfache Adressierung:** Ein Dienst, wie DNS, ist immer unter der selben IP erreichbar, weltweit.

Einschränkungen von Anycast

Anycast eignet sich besonders gut für zustandslose Protokolle wie UDP, z.B. bei DNS.
Bei TCP-Verbindungen können Probleme auftreten, wenn im Verlauf der TCP-Verbindung die Verbindung auf einen anderen Anycast-Knoten weitergeleitet wird, was beispielsweise bei Verbindungsabbrüchen oder Routingänderungen der Fall sein kann. Dies kann auch z.B. bei HTTPS, SSH oder FTP zu Instabilitäten führen.

Beispiele für Anycast in der Praxis

Public DNS-Dienste
Die DNS-Server von Google haben die IP: **2001:4860:4860::8888**
Die von Cloudflare haben folgende IP: **2606:4700:4700::1111**
Diese IPv6-Adressen sind weltweit erreichbar, aber es antwortet immer der nächste Knoten.

Content Delivery Networks (CDNs)
Dienste wie Akamai, Cloudflare oder Fastly nutzen Anycast, um Webseiteninhalte schnell und redundant auszuliefern.