

---

# Netzwerkadressen

---

## 1. Vermittlungsarten

Die Daten werden vor der Übertragung in einzelne Pakete, sog. Frames (Rahmen), aufgeteilt. Der Grund für diese Aufteilung liegt u. a. in der Vermittlungsart. Unter der Vermittlungsart versteht man die **Art und Weise, wie eine Verbindung zwischen zwei Kommunikationspartnern zustande** kommt bzw. wie der Datenfluss über diese Verbindung abläuft. Nachfolgend die zwei der wichtigsten Vermittlungsarten:

### 1.1. Leitungsvermittlung

Beim Start der Übertragung wird eine «feste» Verbindung (Leitung) zwischen zwei Kommunikationspartnern aufgebaut / geschaltet. Diese Verbindung bleibt während der gesamten Übertragung bestehen und steht exklusiv den beiden Teilnehmern (Sender und Empfänger) zur Verfügung. Die Leitung ist auch dann aktiv (online), wenn keiner der Teilnehmer Daten verschickt. Das analoge Telefonnetz basiert auf dieser Vermittlungsart. Die Leitungsvermittlung kommt in der Netzwerktechnik (LANs) nicht zum Einsatz.

### 1.2. Paketvermittlung

Alle zu übertragenden Daten werden in einzelne Pakete aufgeteilt. Diese Datenpakete werden nacheinander dem Netzwerk übergeben. Zwischen den Kommunikationspartnern besteht keine «feste» Verbindung. Daher müssen jedem Paket zwingend bestimmte Dienstinformationen hinzugefügt werden wie die Empfängeradresse und die Absenderadresse.

## 2. Netzwerkadressen

Datennetze arbeiten nach dem Prinzip der Paketvermittlung. Das bedeutet, dass jedes Datenpaket über Adressinformationen verfügen muss, damit es zum gewünschten Empfänger gesendet werden kann bzw. der Absender des Datenpakets bekannt ist. Hierbei unterscheidet man zwischen der physikalischen und der logischen Adressierung.

### 2.1. Physikalische Adressierung

Bei der physikalischen Adressierung sind diese Adressinformationen fest mit einer Netzwerkschnittstelle verknüpft und in allen Netzen einzigartig. Sie stellt so etwas wie den

Fingerabdruck einer Netzwerkschnittstelle dar. In der Praxis bedeutet dies, dass jede Netzwerkkarte oder sonstige Netzwerkschnittstelle automatisch eine eindeutige, physikalische Adresse besitzt, die sog. **MAC<sup>1</sup>-Adresse**. Diese Adresse wird nicht vom Administrator vergeben werden.

Eine MAC-Adresse besteht aus sechs Byte, die hexadezimal dargestellt wird, also zwei Hexziffern für jedes Byte. Als Trennzeichen werden oft verschiedene Zeichen verwendet wie z. B. Bindestrich, Punkt, Leerzeichen oder gar kein Zeichen. Die ersten drei Byte kennzeichnen den Hersteller (Herstellercode) und die letzten drei Byte die einzelne Karte (Kartenidentifikation).

### Beispiel

MAC-Adresse: **BC-AE-C5-12-F8-41**. Damit kann festgestellt werden:

- Herstellercode: **BC-AE-C5** (ASUSTek Computer Inc., Taiwan)
- Kartenidentifikation: **12-F8-41** (Typ, Seriennummer)

## 2.2. Logische Adressierung

Der Unterschied gegenüber der physikalischen Adressierung ist, dass die logische Adresse einer Netzwerkschnittstelle vom Administrator vergeben wird und dass diese Adresse nicht zwingend einzigartig in allen Netzen sein muss. Die gebräuchlichsten logischen Netzwerkadressen sind die **IP<sup>2</sup>-Adressen**.

## 2.3. Aufbau und Struktur von IPv4-Adressen

Bei jeder IP-Adresse werden zwei Bestandteile unterschieden:

- Der **Netzwerkanteil**, auch: **Net-ID** genannt
- Der **Rechneranteil**, auch **Host-ID** genannt

Eine IPv4-Adresse besteht aus 4 Byte, also 32 Bit (1 Byte = 8 Bit). Die IP-Adresse verfügt somit über vier Stellen (X.X.X.X), wobei jede Stelle normalerweise als Dezimalzahl zwischen 0 und 255 dargestellt wird. Die einzelnen Stellen werden durch einen Punkt (.) getrennt. Die maximale Anzahl (Adressraum) aller IPv4-Adressen beträgt:

$2^{32} = 4\,293\,967\,296$ , also insgesamt gut 4 Milliarden Adressen.

## 2.4. Funktion der Subnetz-Maske

Die Subnetz-Maske (auch Subnet Mask, Netz-Maske oder SM) dient dazu, die Grenze zwischen dem Netzwerk- und Rechneranteil anzuzeigen. Der Ausdruck «Maskieren» bedeutet in der IT «etwas abdecken», «etwas verbergen». Und genau das macht die Subnet-Maske. Sie deckt (maskiert) den Teil der IP-Adresse ab, die den Netzwerkanteil

---

<sup>1</sup> Abkürzung für: Media Access Control (engl. für: Medienzugriffssteuerung).

<sup>2</sup> IP, Internet Protocol, dient u. a. zur Adressierung von Systemen.

(Net-ID) darstellt. Das bedeutet, dass alles, was nicht abgedeckt ist, somit zum Rechneranteil (Host-ID) gehört. Mithilfe der Subnetz-Maske kann ein Rechner feststellen, ob sich die IP-Adresse des Zielrechners (Zielhosts) im eigenen Subnetz befindet oder ob sich das Zielsystem in einem anderen, fremden Netzwerk befindet. Die SM besteht logischerweise auch aus 4 Stellen (Byte).

## 2.5. Classful IP Networks

Im Jahr 1981 wurden IP-Adressklassen eingeführt (RFC 791<sup>3</sup>). Zweck dieser Klassen war, eine bessere, situationsorientierte Vergabe von IP-Adressen vornehmen zu können. Nach der Einführung dieser Adressklassen sprach man auch von «**Classful** IP Networks». Vor Einführung der Adressklassen konnten lediglich 127 Netzwerke mit rund 16 Millionen (224) Hosts zugeteilt werden. Der Vorteil einer «Classful»-IP-Adresse ist der Umstand, dass jede Klasse über eine Default-SM verfügt. Diese SM ist starr vorgegeben und kann nicht verändert werden.

Übersicht der IP-Adressklassen gemäss RFC 791:

Klasse	Bereich	Default-Subnetz-Maske	Netze	Hosts pro Netz
A	0.0.0.0–127.255.255.255	255.0.0.0	$2^7=128$	$2^{24}-2=16777214$
B	128.0.0.0–191.255.255.255	255.255.0.0	$2^{14}=16384$	$2^{16}-2=65534$
C	192.0.0.0–223.255.255.255	255.255.255.0	$2^{21}=2097152$	$2^8-2=254$

Daneben existieren noch eine Klasse D, die aber nur für spezielle Zwecke verwendet wird (Multicastverbindungen), sowie eine Klasse E, die nicht freigegeben ist.

## 2.6. Classless IP Networks

Im Jahr 1993 wurden die IP-Adressklassen durch das sog. „**CIDR, Classless Internet Domain Routing**“ (RFC 1519) verdrängt. Bereits damals merkte man, dass die bestehenden Standards (RFCs) aus den 1970er- und 1980er-Jahren infolge der steigenden Verbreitung von TCP/IP angepasst werden mussten. CIDR ist bis heute gültig und in Verwendung. Ziel und Zweck von CIDR ist, eine flexiblere Verwendung von IP-Adressbereichen (IP-Ranges) zu ermöglichen. Dank CIDR wird die starre Beschränkung der Default-SM beseitigt. Somit kann ein bestehendes **Subnet weiter unterteilt werden**. Diesen Vorgang nennt man **Subnetting**. Obwohl die «Classful»-IP-Adressen mit den starren Subnetz-Masken seit Langem nicht mehr angewendet werden, ist der Begriff IP-Adressklassen immer noch sehr weit verbreitet.

---

<sup>3</sup> Englische Abk. für: Request for Comments, in der Netzwerktechnik öffentlich zugängliche Standardbeschreibungen von TCP/IP-Protokollen.

## 2.7. Adressverbrauch bei «Classful»- vs. «Classless»-Adressierung

Situation: Ein Kunde bestellt bei einem Internet-Service-Provider (ISP) 1 öffentliche, statische IP-Adresse für den Anschluss seines Netzwerks an das Internet. Dem ISP steht zur Vergabe von statischen IP-Adressen folgender IP-Adressbereich zur Verfügung: 202.12.0.0 bis 202.12.255.255. Dies umfasst rund 65 000 IP-Adressen ( $255 \times 255$ ).

Adresszuweisung mittels «Classful»-Adressierung (RFC 791):

Zugewiesene IP-Adresse	Subnet-Maske	Benötigte Adressen	Bemerkung
202.12.68.2 = 1 C-Adresse	255.255.255.0	255	Die starre SM verhindert eine Unterteilung bzw. Erweiterung des Netzanteils in weitere Subnetze, was zur «Verschwendung» von IP-Adressen führt.

Adresszuweisung mittels «Classless»-Adressierung (RFC 1519):

Zugewiesene IP-Adresse	Subnet-Maske	Benötigte Adressen	Bemerkung
202.12.68.2 = 1 C-Adresse	255.255.255.252 oder /30*	4	Dank der ermöglichten Aufteilung von Subnets (Subnetting) muss nicht der ganze Adressbereich des Netzes verwendet werden. Somit kann ein C-Netz in max. 64 Subnetze mit jeweils 4 IP-Adressen pro Subnetz aufgeteilt werden.

\*: /Zahl = CIDR-Schreibweise der SM, die Zahl gibt die Anzahl Bits an, die von der Host-ID für die Net-ID verwendet werden.

### Erklärung zu den benötigten IP-Adressen:

Auf den ersten Blick könnte man vermuten, dass für die Koppelung zweier IP-Netzwerke in jedem Netzwerk lediglich eine IP-Adresse benötigt wird. Diese Annahme ist nicht richtig, denn in jedem IP-Netzwerk – egal welcher Grösse – müssen folgende vier Adressen vorhanden sein.

Die zwingend benötigten / reservierten IP-Adressen auf ISP-Seite am Beispiel von 202.12.68.2/30:

Verwendung	IP-Adresse	Erläuterungen
Subnetzadresse	202.12.68.0	Jedes Subnetz besitzt immer auch eine eigene IP-Adresse. Die niedrigste IP-Adresse in einem Subnetz repräsentiert immer die Netzwerkadresse.
Broadcast-adresse	202.12.68.3	In jedem Subnetz muss eine IP-Adresse für den Broadcast vorhanden sein. Die höchste IP-Adresse in einem Subnetz ist für die Broadcastfunktion reserviert.
Gatewayadresse	202.12.68.1	In jedem Subnetz muss eine Adresse eingerechnet werden, an der sich ein Gateway befindet. Der Gateway oder Router ist das System zur physischen Koppelung beider Subnetze.

Verwendung	IP-Adresse	Erläuterungen
Hostadresse	202.12.68.2	Diese Adresse ist die einzig verfügbare Adresse, um auf die Systeme und Dienste in dem entsprechenden Subnetz zugreifen zu können.

### 3. Private IP-Adressbereiche

Auch mit der Einführung von CIDR war vorauszusehen, dass der Adressraum von IPv4 früher oder später erschöpft sein würde. Deshalb wurden 1994 die «privaten IP-Adressbereiche» eingeführt (RFC 1597). Mittels privater IP-Adressen will man verhindern, dass Privatpersonen oder Firmen für ihre privaten Netzwerke auch sog. öffentliche IP-Adressen benutzen. Vor der Einführung der privaten IP-Adressen waren alle vorhandenen IP-Adressen öffentlicher Natur. Eine öffentliche IP-Adresse darf weltweit nur 1× vergeben bzw. vorhanden sein. Private IP-Adressen im Gegensatz dürfen mehrfach vorhanden sein, da diese Adressen nur in einem privaten Netzwerk verwendet werden können. Jeder darf so viel private IP-Adressen verwenden, wie er will, da dieser «private Adressraum» im Grunde unerschöpflich ist. Dies aufgrund der Tatsache, dass ein Router zwischen einem privaten und einem öffentlichen Netzwerk (z. B. Internet) alle Datenpakete mit privaten IP-Adressen in Richtung öffentliches Netz blockiert. Datenpakete mit öffentlichen IP-Adressen hingegen werden von Routern ohne Einschränkungen in beide Richtungen weitergeleitet.

Netztyp	Private Adressbereiche	CIDR-Notation
Klasse A	10.0.0.0–10.255.255.255	10.0.0.0/8
Klasse B	172.16.0.0–172.31.255.255	172.16.0.0/16
Klasse C	192.168.0.0–192.168.255.255	192.168.0.0/24

## 4. IPv6 – The Next Generation IP

Wie bereits erwähnt, beträgt die Anzahl möglicher Adressen bei IPv4 rund 4.3 Milliarden ( $2^{32}$ ). Dies ist zwar viel, aber angesichts der Tatsache der rasant wachsenden Anzahl an Geräten, die via Internet kommunizieren, wird der Adressraum von IPv4 in absehbarer Zeit erschöpft sein. Genau hier setzt IPv6 oder IPnG (IP Next Generation) neue Grenzen. IPv6 hat einen Adressraum von  $2^{128}$  (> 340 Sextillionen). Die Gesamtzahl der IP-Adressen unter IPv6 würde ausreichen, um auf jedem  $\text{mm}^2$  der Erdoberfläche inklusive Wüsten und Ozeanen rund 600 Milliarden IP-Adressen zu vergeben. Der neue IP-Standard wurde Ende 1998 verabschiedet (RFC 2460). Natürlich bietet IPv6 neben dem immensen Adresspool noch weitere wichtige, zeitgemässe Eigenschaften, die IPv4 in den letzten Jahren dringend gebraucht hätte.

- **Keine privaten Adressen mehr nötig:** Jede Adresse unter IPv6 ist im Grunde eine einzigartige, öffentliche IP-Adresse. Lediglich durch die Verwendung eines bestimmten Präfixes am Anfang der Adresse kann bestimmt werden, dass eine IP-Adresse nicht ins Internet geroutet werden soll, fe80:: bedeutet z. B. «link local». «Link local»- Adressen können nur im lokalen LAN verwendet werden, da ein Router Datenpakete mit diesen Adressen nicht in ein öffentliches Netz routet.
- **Effizientes Routing:** Durch zahlreiche Anpassungen im IP-Header von IPv6 kann das Routing extrem vereinfacht werden, was eine spürbare Beschleunigung der Datenkommunikation im Internet bedeutet.
- **Plug-And-Play:** Die Autokonfigurationsfunktion von IPv6 ist in der Lage, die gesamte IP-Adressierung in einem Netze selbstständig und fehlerfrei durchzuführen.

Obwohl IPv6 noch eine ganze Reihe weiterer Verbesserungen bereithält, wird dieses neue Protokoll in den nächsten Jahren in privaten Netzwerken noch keine grosse Rolle spielen. Die internationalen Carriernetzwerke hingegen arbeiten meist bereits mit IPv6. Auch alle Betriebssysteme unterstützen seit Jahren IPv6.

Quellen:

- Modul 117: Informatik- und Netzinfrastruktur für ein kleines Unternehmen realisieren, Compendio Bildungsmedien AG, Zürich, Auflage: 4., überarbeitete Auflage 2014, Attila Mathé und Simon Roggli