

So funktionieren TCP/IP und IPv6

› Die Grundlage des Internet ist TCP/IP, das eine weltweite Kommunikation zwischen unterschiedlichsten Systemen ermöglicht. Wir erläutern den Aufbau der Protokollsuite und geben einen Einblick in das Protokoll IPv6.

› VON KONSTANTIN PFLIEGL

Die Protokollfamilie TCP/IP wurde erstmalig Mitte der 70er Jahre entwickelt, als bei der amerikanischen [Defense Advanced Research Agency](http://www.darpa.mil) (DARPA) das Interesse an einem Paketvermittlungsnetz aufkam, das die Kommunikation zwischen unterschiedlichen Computersystemen an Forschungseinrichtungen erleichtern würde. TCP/IP schafft ein heterogenes Netzwerk mit offenen Protokollen, die unabhängig von unterschiedlichen Betriebssystemen und Hardware-Architekturen sind. Ob Heim-PC, Großrechner oder Pocket-PC - über die Internet-Protokolle können alle Rechner miteinander kommunizieren.

Die Protokolle sind für jedermann frei verfügbar und werden als offen betrachtet. Jeder Anwender kann sie lizenzfrei für eigene Zwecke nutzen und eigene Applikationen und Dienste darauf aufsetzen. Dabei steht TCP/IP für eine ganze Reihe von Protokollen, der so genannten "Internet Protocol Suite". Die beiden wichtigsten Typen TCP und IP sind zum Synonym für diese Familie geworden.

Auf Grund des einheitlichen Adressierungsschemas kann jeder Rechner in einem TCP/IP-Netz jeden beliebigen anderen Rechner eindeutig identifizieren. Standardisierte Protokolle in den höheren Schichten stellen dem Benutzer einheitlich verfügbare Dienste zur Verfügung. Als TCP/IP Ende der 70er Jahre dem [BSD](http://www.bsd.org) -Unix beigefügt wurde, entwickelte sich daraus die Grundlage, auf der das Internet basiert.

› Protokollarchitektur

Es gibt keine generelle Übereinstimmung darüber, wie TCP/IP in einem Schichtenmodell beschrieben werden soll. Das OSI-Modell ist zwar recht nützlich, aber größtenteils sehr akademisch. Um den Aufbau von TCP/IP zu verstehen, benötigt man ein Modell, das näher an die Struktur der Protokolle angelehnt ist.

Das amerikanische Verteidigungsministerium (DoD - [Department of Defense](http://www.defenselink.mil)) hat ein 4-Schichten-Netzwerkmodell ausgearbeitet. Jede Schicht besteht aus einer Anzahl von Protokollen, die gemeinsam die TCP/IP-Protokollfamilie bilden. Die Spezifikationen für jedes Protokoll wurden jeweils in einem oder mehreren RFCs festgelegt.



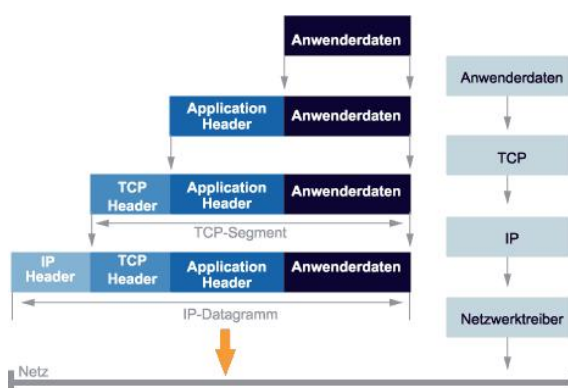
Alternative zum OSI-Modell: Das 4-Schichten-Netzwerkmodell des US-Verteidigungsministeriums.

© tecChannel.de

Die Daten werden wie im OSI-Modell beim Versenden im Stack nach unten gereicht; beim Empfang von Daten aus dem Netz führt der Weg durch den Stack nach oben. Jede Schicht fügt dabei ihre Kontrollinformationen hinzu, um eine korrekte Übertragung der Daten sicherzustellen. Diese Informationen nennt man Header, da diese den eigentlichen Daten vorangestellt werden.

› Die Kapselung von Daten

Das Hinzufügen von Kontrollinformationen nennt man Encapsulation (Kapselung). Beim Empfangen von Daten werden die Schritte der Kapselung wieder rückgängig gemacht. Jede Schicht entfernt ihren Header und reicht die restlichen Daten an die darüber liegende Schicht weiter.



Kapselung: Zahlreiche Header vergrößern die Datenmenge bei TCP/IP.

© tecChannel.de

Jede dieser Schichten verfügt über eine eigene, unabhängige Datenstruktur. In der Praxis sind aber die einzelnen Schichten so gestaltet, dass sie zu den Strukturen der benachbarten Schichten kompatibel sind. Dies dient der effizienteren Datenübertragung.

Bei der Übertragung von geringen Datenmengen kann es allerdings passieren, dass durch die Kapselung mehr Protokolldaten als Nutzdaten übertragen werden. In diesem Fall empfiehlt sich beispielsweise der Einsatz des User Datagram Protocols (UDP),

welches über nur minimale Protokollmechanismen zur Datenübertragung verfügt.

› IP: Internet Protocol

Das Internet Protocol (IP) ist die Grundlage der Protokollfamilie TCP/IP und für die Weiterleitung der Daten zuständig. Generell hat es die Aufgabe, die Datenübertragung zwischen Netzwerken sicherzustellen. Dazu muss das Protokoll diverse Aufgaben übernehmen und diese als Dienst den höheren Schichten zur Verfügung stellen. Zu den Aufgaben des IP zählen:

- › Datenpaketdienst
- › Fragmentierung von Datenpaketen
- › Wahl der Übertragungsparameter
- › Adressfunktion
- › Routing zwischen Netzwerken

Die Hauptaufgabe des IP ist die Ermittlung und Realisierung des optimalen Weges zwischen Sender und Empfänger für jedes Datenpaket. Verbindungsaufbau und Verbindungsabbau fallen nicht in den Zuständigkeitsbereich dieses Protokolls.

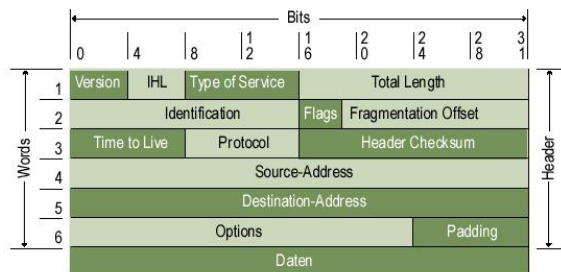
Das Internet Protocol stellt keine gesicherte Verbindung zur Verfügung und kann keine verlorenen Datenpakete erneut übertragen. Jedes IP-Datenpaket wird als unabhängiges Paket (Datagramm) durch das Netzwerk an den Empfänger übermittelt. Für die Netzwerktypen sind unterschiedliche Datenpaketlängen festgelegt. Die Größe eines Datenpakets hängt von mehreren Faktoren ab, wie Hardware- und Software-Beschränkungen.

Ist ein Datenpaket wegen seiner Überlänge nicht als eine Einheit übertragbar, so muss es in kleinere Fragmente zerlegt werden. Die Pakete werden zwar in der richtigen Reihenfolge gesendet, kommen aber nicht notwendigerweise in derselben dort an. Da die Einzelpakete verschiedene Wege gehen können, sind zusätzliche Informationen erforderlich. Diese erlauben, den Zustand des ursprünglichen Datenpakets zu rekonstruieren. Jedes Datenpaket erhält daher bei der Übertragung einen IP-Header vorangestellt.

› IP-Header im Detail

Der IP-Header verfügt über 14 Parameter und hat bei Nutzung des Feldes Options eine Länge von 32 Bytes, ansonsten 20 Bytes.

Bit für Bit: Der IP-Header im Detail.



© tecChannel

Der IP-Header im Detail

Name	Größe (in Bits)	Beschreibung
------	-----------------	--------------

Version	4	Legt die Version des IP-Headers fest. Momentan ist Version 4 aktuell, auch als "IPv4" bezeichnet. Mittelfristig wird diese von Version 6 (IPv6) abgelöst werden.
IHL	4	Gibt die gesamte Länge des Headers an. Die Angabe ist wegen dem Options-Feld notwendig.
Type Of Service	8	Definiert die Dienste eines IP-Datenpakets. Beispielsweise können die vorrangige Behandlung von Datenpaketen, die Durchsatzart oder die Belegung von Ressourcen in Routern festgelegt werden.
Total Length	16	Verzeichnet die Gesamtlänge des Datagramms
Identification	16	Enthält einen Kennwert von Fragmenten zu einem Datenpaket. Anhand des Feldes ermittelt der Empfänger die korrekte Reihenfolge der Datenpakete.
Flags	3	Enthält das Kontroll-Flag "Don't Fragment" (DF), wenn keine weiteren Pakete folgen und "More Fragment" (MF) wenn weitere Folgen.
Fragmentation Offset	13	Beinhaltet Informationen über die Position eines Datagramms zu anderen Datagrammen. Mit Hilfe des Fragmentation Offset kann der Empfänger die Datenpakete in der richtigen Reihenfolge zusammensetzen.
Time To Live	8	Definiert die Lebensdauer eines Datagramms im Netzwerk. Fällt der Wert auf Null, wird das Datenpaket verworfen. Die Lebensdauer eines Datenpakets beträgt maximal 255 Sekunden oder den Übergang über 255 Router. Der Wert des Feldes wird bei jedem Durchgang durch einen Router um mindestens 1 herabgesetzt.
Protocol	8	Legt fest, welches weiterverarbeitende Protokoll der höheren Schichten als nächstes das Datenpaket verarbeiten muss. Zum Beispiel "6" für TCP oder "17" für UDP.
Header Checksum	16	Enthält eine Prüfsumme, die den Header auf Fehler überprüft. Durch die Prüfsumme können Übermittlungsfehler erkannt werden.
Source Address	32	Enthält hexadezimal die Adresse des Senders
Destination Address	32	Enthält hexadezimal die Adresse des Empfängers.
Options	bis zu 96	Variables Feld, das optionale

Padding	-	Informationen wie Sicherheitsrestriktionen enthält. Enthält Füll-Bits, die sicherstellen, dass der IP-Header bei Nutzung des Options-Feldes eine Länge von 32 Bytes hat.
---------	---	---

› IP-Adressen

Jedem Host in einem TCP/IP-Netz wird eine eindeutige 32-Bit-Adresse zugewiesen, die aus zwei Hauptteilen besteht: einer Netzadresse und einer Adresse des Rechners innerhalb dieses Netzes. Allerdings ist das Format dieser beiden Teile nicht in allen IP-Adressen dasselbe. Zur einfacheren Strukturierung hat man den gesamten Adressraum in mehrere Klassen unterteilt.

Die Anzahl der Bits, die das Netzwerk identifizieren und die Anzahl der Bits, die den Rechner identifizieren, variieren mit der Klasse, der die Adresse angehört. Im Allgemeinen werden die Adressen als vier durch Punkte getrennte Dezimalzahlen geschrieben. Jede dieser vier 8-Bit-Zahlen liegt im Bereich von 0 bis 255 - die Werte die sich in einem Byte darstellen lassen.

Adressbereiche

Klasse	Adressbereich	Max. Anzahl Hosts	Einsatzbereiche
A	1.0.0.0 bis 127.255.255.255	16.777.216	Wenige Netzwerke, viele Hosts
B	128.0.0.0 bis 191.255.255.255	65.536	Mittlere Verteilung von Netzwerken und Hosts
C	192.0.0.0 bis 223.255.255.255	254	Viele Netzwerke, wenige Hosts
D	224.0.0.0 bis 239.255.255.255	-	Multicast-Adressen
E	240.0.0.0 bis 254.255.255.255	-	Nicht definiert

Allerdings werden die nur 32-Bit langen Adressen langsam knapp. Derzeit sind rund 60 Prozent aller Class-B-Adressen bereits vergeben. Diese Adressen werden daher nur noch in begründeten Fällen zugewiesen. Da erst rund 40 Prozent der Class-C-Adressen vergeben sind, geht man dazu über, statt Class-B-Adressen einen Block aufeinanderfolgender Class-C-Adressen zu vergeben.

› IP: Adressklassen und besondere Adressen

Die drei wichtigsten Adressklassen sind A, B und C. Um festzustellen, zu welcher Klasse eine Adresse gehört, liest die IP-Software die ersten Bits einer Adresse. Zur Bestimmung der Klasse, der eine Adresse angehört, wendet IP folgende Regeln an:

- › Ist das erste Bit einer Adresse "0", handelt es sich um eine Adresse der Klasse A. Das erste Bit der Adresse kodiert die Klasse, die nächsten 7 Bit identifizieren das Netzwerk. Die restlichen 24 Bits kodieren den Rechner innerhalb dieses Netzes. Insgesamt sind 127 Class-A-Netze möglich.
- › Wenn die ersten beiden Bits einer IP-Adresse "10" sind, handelt es sich um eine Adresse in einem Class-B-Netz. Die ersten beiden Bits bestimmen die Klasse, die nächsten 14 Bits identifizieren das Netz und die letzten 16 Bits den Rechner.
- › Sind die ersten drei Bits "110", handelt es sich um ein Class-C-Netz. Die ersten 3 Bits dienen zur Bestimmung der Klasse, die nächsten 21 Bits bestimmen das Netzwerk. Die letzten 8 Bits definieren den Rechner.

- › Wenn die ersten 3 Bit "111" sind, handelt es sich um eine spezielle reservierte Adresse, oft auch als Class-D-Netz bezeichnet. Diese Adressen sind so genannte Multicast-Adressen. Damit lassen sich Gruppen von Computern adressieren, die ein gemeinsames Protokoll benutzen.

Es gibt in allen Netzwerkklassen auch Rechnernummern, die für spezielle Zwecke reserviert sind. Eine IP-Adresse, in der alle Rechner-Bits auf "0" stehen, also Rechnernummer "0", identifiziert das Netzwerk selbst. Stehen alle Rechner-Bits auf "1", also Rechnernummer "255", bezeichnet man diese Adresse als Broadcast-Adresse. Diese Adresse wird benutzt, um gleichzeitig jeden einzelnen Rechner in einem Netzwerk zu adressieren.

Auch in der Klasse A gibt es zwei Adressen, nämlich "0" und "127", die für spezielle Zwecke reserviert sind. Das Netzwerk "0" bezeichnet die Default-Route (Standard- oder voreingestellte Route) und das Netzwerk "127" ist die Loopback-Adresse. Die Default-Route dient der Vereinfachung des Routing, das IP vornehmen muss. Die Loopback-Adresse vereinfacht Netzwerkanwendungen, indem der lokale Rechner genau so adressiert werden kann wie ein fremder Rechner.

› Subnetze

Durch die Verwendung von Subnetzmasken kann man den Rechneranteil der IP-Adresse in einen Subnetzteil umwandeln. Die Subnetzmaske gibt an, welche Bereiche als Subnetz- und welche als Rechneradresse interpretiert werden. Dadurch schafft man innerhalb eines großen Netzes mehrere kleine, reduziert aber gleichzeitig die Anzahl der Rechner, die zu einem Netz gehören. Diese kleinen Netze innerhalb eines großen Netzes werden als Subnetze bezeichnet.

So wird beispielsweise eine Class-A-Adresse 10.x.y.z, die eine Subnetzmaske von 255.0.0.0 hat, durch die Subnetzmaske 255.255.0.0 zu einer Class-B-Adresse, durch die Subnetzmaske 255.255.255.0 zu einer Class-C-Adresse. Die Entscheidung, Subnetze einzurichten, dient meist der Lösung topologischer oder organisatorischer Probleme. Subnetze ermöglichen es, die Verwaltung eines Rechnernetzes zu dezentralisieren.

IP-Router können physikalisch verschiedene Netzwerke miteinander verbinden. Allerdings nur, wenn jedes einzelne Netz seine eigene, eindeutige Netzwerkadresse bekommt. Durch das Subnetz teilt man eine einzige Netzwerkadresse in viele eindeutige Subnetz-Adressen aus. So bekommt jedes physikalische Netz seine eigene Adresse.

Subnetzmasken sind Bit-orientiert und bieten die Möglichkeit Zwischenklassen festlegen. Zum Beispiel ergibt eine Subnetzmaske 255.128.0.0 eine Class-A-Adresse. Das zweite Byte unterscheidet zwischen den beiden Netzen 0 bis 127 und 128 bis 255. Ein Class-A-Netzwerk wird damit in zwei Subnetze gegliedert.

› Routing: So kommen die Daten ans Ziel

Der Sender eines IP-Datenpakets kennt zwar die Zieladresse, nicht aber den Weg dorthin. Jede Station auf dem Weg des Datagramms zum Empfänger muss eine Entscheidung über die Wahl des weiteren Weges fällen. Dieser Vorgang wird als Routing bezeichnet. Die Wahl einer bestimmten Route ist von verschiedenen Kriterien abhängig. Der Sender übergibt diese Aufgabe einem Standard-Router, der für die Zustellung von Datenpaketen in andere Netze zuständig ist.

Zwischen zwei Hosts liegen in der Regel mehrere Router. Jeder dieser Router verfügt über eine so genannte Routing-Tabelle. Auf Grund derer wird die nächste Station für das Datagramm bestimmt. Jeder Eintrag in der Routing-Tabelle ist durch folgende Informationen spezifiziert:

Routing-Tabelle im Detail

Feld	Beschreibung
Destination	Zielnetzwerk; dabei kann es sich um eine IP-Adresse oder ein Subnetz handeln
Gateway	Die Adresse des Standard-Gateways, über den das Ziel

	erreicht werden kann
Flags	Bestimmen die Charakteristika dieser Route: H: Route zu einem Rechner und nicht zu einem Netzwerk. G: Route benutzt einen Gateway U: Route existiert und kann benutzt werden
Refcnt	Gibt an, wie häufig die Route zum Verbindungsaufbau benutzt wurde.
Interface	Gibt den Namen des Netzwerk-Interfaces für die Route an.
Metric	Entspricht der Anzahl von Gateways, die zwischen Absender und Ziel der Daten liegen. Diese Angabe ist vor allem beim dynamischen Routing von Bedeutung.

› Routing-Verfahren

Prinzipiell unterscheidet man zwischen drei Routing-Verfahren:

- › Statisches Routing über feste Tabelleneinträge
- › Default-Routing über einen festen Tabellen-Eintrag
- › Dynamisches Routing über ein automatisches Update der Routing-Tabellen

Beim statischen Routing wird für jedes Netzwerk der zuständige Router in die Routing-Tabelle des Rechners eingetragen. So kann man genau nachvollziehen, welchen Weg ein Datenpaket genommen hat. Bei größeren Netzen ist dieses Vorgehen aber nicht sinnvoll, da zu viele Einträge gewartet werden müssten.

Beim Default-Routing wird in die Routing-Tabelle des Rechners eine Adresse eingetragen, an die alle Datenpakete gesendet werden, die nicht aus dem eigenen Netzwerk-Adressbereich stammen.

Beim dynamischen Routing tauschen sowohl Rechner als auch Router Informationen untereinander aus. Dadurch "weiß" jeder Rechner, welcher Weg aktuell der beste ist. Die Routing-Tabellen müssen nicht von Hand gepflegt werden. Jedes Datenpaket wird über den derzeit optimalen Weg geschickt. Die Kommunikation zwischen den Routern erfolgt über spezielle Router-Protokolle wie RIP (Routing Information Protocol) oder IGRP (Interior Gateway Routing Protocol).

› Routing am Beispiel

Eine Routing-Tabelle könnte beispielsweise wie folgt aussehen:

```

kpf% netstat -rn
Routing tables
Destination Gateway      Flags  Refcnt  Use    Interface  Metric
127.0.0.1   127.0.0.1   UR     1       0     lo0        0
default    192.168.12.1 UG     0       0     eth0       0
192.168.12.0 192.168.12.2 U      0       0     eth0       0

```

Beispiel: Routing-Tabelle im Detail.

Der erste Tabelleneintrag kennzeichnet die Loopback-Route für diesen Rechner. Alle Systeme nutzen diese Route, um Datagramme an sich selbst zu senden. Daher findet sich dieser Eintrag in jeder Routing-Tabelle. Da es sich um eine Route zu einem Rechner und nicht zu einem Netzwerk handelt, ist das "H"-Flag gesetzt.

Der zweite Eintrag kennzeichnet die Default-Route. Der Gateway in diesem Eintrag ist der Default-Gateway. Dieser wird immer dann benutzt, wenn für eine Zieladresse keine bestimmte Route in der Tabelle enthalten ist.

Aus der Routing-Tabelle kann man ablesen, dass dieser Rechner direkt an das Netz 192.168.80.0 angeschlossen ist. Der Tabelleneintrag für dieses Netz benennt keinen externen Gateway, da das "G"-Flag nicht gesetzt ist. Daraus folgt, dass der Rechner direkt mit diesem Netz verbunden sein muss.

› Private IP-Adressen

Für die Verwaltung von IP-Adressen ist in erster Linie die [IANA](http://www.iana.org) (Internet Assigned Numbers Authority) zuständig. Diese hat wiederum die Vergabe weltweit an drei regionale Organisationen abgegeben. Für Nord- und Südamerika ist [ARIN](http://www.arin.net) (American Registry for Internet Numbers), für Europa [RIPE NCC](http://www.ripe.net) (Réseaux IP Européens) und für Asien [APNIC](http://www.apnic.net) (Asia-Pacific Network Information Center) zuständig.

Details für die Vergabe von IP-Adressen sind in [RFC 2050](http://www.isi.edu/in-notes/rfc2050.txt) definiert. Die Reservierung von einer oder mehreren IP-Adressen erfolgt immer über einen Internet-Provider. Nicht alle TCP/IP-Netze sind untereinander über das Internet verbunden. Daher sind in [RFC 1918](http://www.isi.edu/in-notes/rfc1918.txt) drei Adressbereiche in den Netzwerkclassen A, B und C speziell für isolierte, lokale TCP/IP-Netzwerke reserviert:

Netzwerkclassen

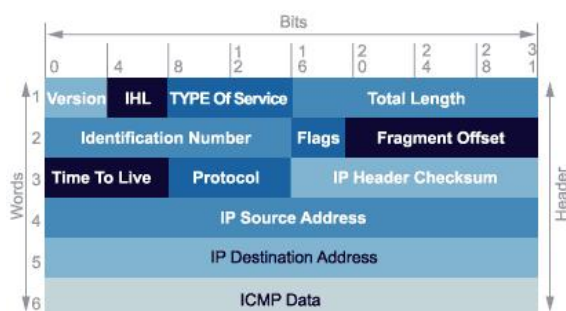
Adressbereich	Klasse
10.0.0.0 bis 10.255.255.255	Class-A-Netz
172.16.0.0 bis 172.31.255.255	Class-B-Netz
192.168.0.0 bis 192.168.255.255	Class-C-Netz

Hosts mit diesen Adressen können nicht direkt an das Internet angeschlossen werden. So stehen diese Adressbereiche für beliebig viele lokale Netze gleichzeitig zur Verfügung.

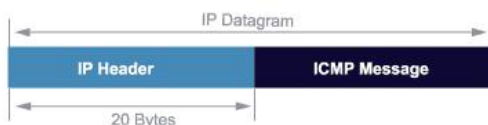
› Kontrollmechanismus für IP: ICMP

Treten bei der Übertragung des IP Fehler auf, kommt das Internet Control Message Protocol (ICMP) zum Einsatz. ICMP kennt dabei Fehler- und Statusmeldungen. Ist beispielsweise ein Host nicht erreichbar, sendet ein Host oder Router die Fehlermeldung "Destination Unreachable" zum Absender.

Die Interpretation der Nachricht ist vom Absender der Fehlermeldung abhängig: Wurde die Nachricht von einem Router generiert, ist der Zielhost nicht erreichbar. Die gleiche Nachricht vom Zielrechner bedeutet, das ein angegebener Port nicht ansprechbar ist. Neben der Fehlerübermittlung dient ICMP zur Kontrolle: So verwendet der Ping-Befehl ICMP-Pakete, um die Laufzeit von Datagrammen zwischen zwei Hosts zu ermitteln.



ICMP: Header und Datagramm im Detail.



© tecChannel.de

Die Übermittlung von ICMP-Nachrichten erfolgt innerhalb von IP-Datagrammen. Sie bestehen aus drei Headerfeldern und dem Datenblock. Das Headerfeld "Type" gibt den Nachrichtentyp an. Man unterscheidet dabei zwischen Fehler- und Statusmeldungen. Im Feld "Code" sind die Fehlercodes für das jeweilige Datagramm enthalten. Die Interpretation ist dabei vom Nachrichtentyp abhängig. Das Headerfeld "Checksum" enthält eine Prüfsumme.

› ICMP-Meldungen

Man unterscheidet zwei Klassen von ICMP-Meldungen:

ICMP-Fehlermeldungen

Meldung	Beschreibung
Destination Unreachable	Der Code teilt dem Sender mit, warum das Datenpaket nicht übermittelt werden konnte, z.B. Rechner nicht erreichbar.
Redirect	Durch den Code in der Redirect-Meldung wird dem Sender mitgeteilt, über welchen Router das Datenpaket geschickt werden muss.
Source Quench	Die Meldung besagt, dass das Datenpaket auf Grund fehlender Ressourcen nicht übermittelt werden konnte.
Time Exceeded	Das Paket konnte wegen Überschreitung der maximalen Zeit nicht übermittelt werden, wenn beispielsweise der Fragmentierungsprozess zu lange dauerte.
Parameter Problem	Der Pointer im ICMP-Header zeigt auf das Byte im Datenpaket, das bei der Übermittlung ein Fehler verursacht hat.

ICMP-Informationsmeldungen

Meldung	Beschreibung
Echo	An den Sender eines Echo-Requests werden vom Empfänger alle im Datenpaket enthaltenen Daten zurückgeschickt.
Information	Durch die Information-Meldung kann der Sender die Netzadresse des Netzes erfragen, an das er angeschlossen ist.
Timestamp	Dem Sender eines Timestamp Request-Datenpakets werden vom Empfänger Sende- und Empfangszeit sowie die Sendezeit des Timestamp Reply-Datenpakets übermittelt.

› TCP: Transmission Control Protocol

Anwendungen, die darauf angewiesen sind, dass ihre Daten zuverlässig ihr Ziel erreichen, benutzen das Transmission Control Protocol (TCP). Es stellt sicher, dass die Daten korrekt und in der richtigen Reihenfolge über das Netz transportiert werden. Dabei wird das IP-Protokoll nicht ersetzt, sondern dessen Fähigkeiten werden zum Versand und Empfang genutzt.

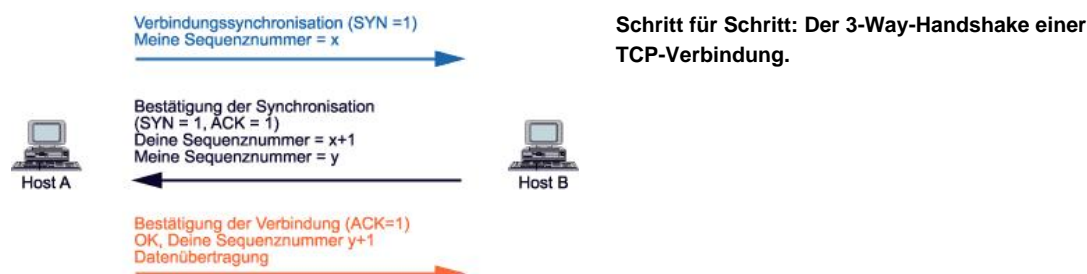
TCP ist ein zuverlässiges, verbindungsorientiertes Protokoll. Ein Rechner sendet die Daten nach einer bestimmten Zeit noch einmal, bis er von der Gegenstelle die Bestätigung erhält, dass sie korrekt empfangen wurden. Die Dateneinheit, die TCP-Module bei der Kommunikation untereinander verwendet, wird als Segment bezeichnet. Dabei enthält jedes Segment eine Prüfsumme, die auf der Empfängerseite

ausgewertet wird. Damit wird getestet, ob die Daten korrekt empfangen wurden.

TCP arbeitet verbindungsorientiert. Das Protokoll stellt also eine logische Rechner-zu-Rechner-Verbindung her. Zu diesem Zweck übermittelt TCP vor der Übertragung der Nutzdaten einige Kontrollinformationen, Handshake genannt. Das von TCP benutzte Handshake wird als 3-Way-Handshake bezeichnet, weil dazu drei Segmente ausgetauscht werden. Der Verbindungsaufbau beginnt damit, dass beide Rechner einen Anfangswert für die Sequenznummer (Initial Sequence Number / ISN) festlegen. Die Nummern werden in einem Dialog zwischen den beteiligten TCP-Systemen ausgetauscht und bestätigt.

› 3-Way-Handshake

Der Verbindungsaufbau mit dem 3-Way-Handshake lässt sich an einem Verbindungsdiagramm aufzeigen. Ausgangspunkt ist ein ruhender Service (Closed-Modus). Er stellt den Anfangswert einer Verbindung dar. Die Verbindung wird befehls gesteuert in den Listen-Modus gesetzt. Dies ist der Zustand, bei dem zum anderen TCP-System eine Verbindung aufgebaut werden kann.



© tecChannel.de

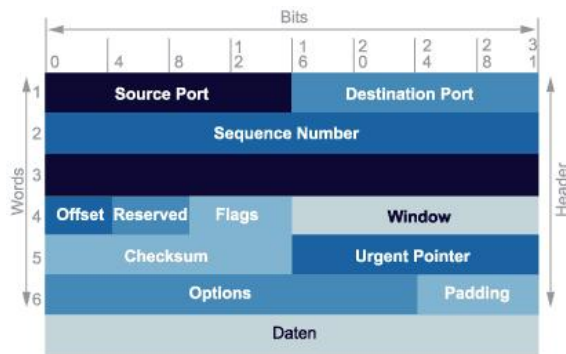
Befindet sich das System im Listen-Modus, wartet es auf ankommende Syn-Zeichen, um nach dem Eintreffen mit einem weiteren Syn-Zeichen zu antworten und in den "Syn Received"-Modus zu gehen. Wurde ein Syn-Zeichen gesendet, wechselt die Verbindung in den "Syn Send"-Modus. In diesem Modus bleibt das TCP-System, bis es vom Partnersystem als Antwort ein Syn-Zeichen erhält.

Wird auf dieses Syn-Zeichen positiv geantwortet, so gelangt das TCP-System in den "Syn Received"-Modus. Nach der positiven Quittierung des Syn-Zeichens (ACK auf SYN) gelangen Sender und Empfänger in den Established-Modus: Daten können nun zwischen den Rechnern übertragen werden. Nachdem alle Daten übertragen worden sind, nehmen die beteiligten Rechner einen weiteren 3-Way-Handshake vor. Dabei werden Segmente mit dem Bit "No more data from sender" ausgetauscht, um die Verbindung zu schließen.

TCP betrachtet die übertragenen Daten als ununterbrochenen Datenstrom und nicht als eine Reihe unabhängiger Pakete. Das Protokoll ist auch dafür verantwortlich, dass die von IP empfangenen Daten an die richtige Anwendung zugestellt werden. Die Anwendungen werden durch eine 16-Bit lange Portnummer identifiziert.

› TCP-Header im Detail

Der TCP-Header verfügt über 12 Parameter und hat bei Nutzung des Feldes Options eine Länge von 32 Bytes, ansonsten 20 Bytes.



© tecChannel.de

Bit für Bit: Der TCP-Header im Detail.

TCP-Header im Detail

Name	Größe (in Bits)	Beschreibung
Source Port	16	Enthält die Portnummer der Quelldaten.
Destination Port	16	Bestimmt den Ziel-Port der Daten. Dieser bleibt für die Dauer der Verbindung gleich.
Sequence Number	32	Gibt beim Verbindungsaufbau eine Zufallszahl als "Initial Sequence Number" (ISN) an. Das erste Segment erhält so den Wert ISN+1.
Acknowledge Number	32	Bestätigungsnummer für Empfangsquittungen an den Sender.
Data Offset	4	Gibt die Anzahl der 32-Bit-Worte im TCP-Header an. Der Eintrag in diesem Feld ist für die Berechnung des Datenteils relevant.
Reserved	6	Für zukünftige Anwendungen reserviert; muss immer auf Null gesetzt werden.
Control Flags	6	Enthält eine Reihe von so genannten Ein-Bit-Indikatoren, die zum Aufbau, zur Beendigung und zur Aufrechterhaltung von Verbindungen dienen.
Windows Size	16	Dient zur Flusskontrolle zwischen Sender und Empfänger. Die Flusskontrolle basiert auf der fortlaufenden Nummerierung der übertragenen Datenpakete.
Checksum	16	Enthält eine Prüfsumme, die aus dem TCP-Header und einem 96-Bit-Pseudo-Header gebildet wird.
Urgent Pointer	16	Gibt an, dass die TCP-Segmente Informationen mit großer Dringlichkeit transportieren. Solche Segmente werden durch das URG-Flag gekennzeichnet.
Options	96	Definiert Dienstoptionen, Optionenart und Optionenlänge. Die aktuellen Optionen bestimmen

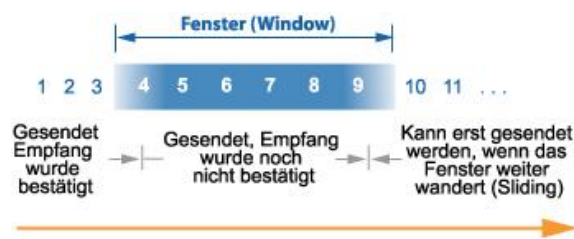
Padding	-	die Länge des Feldes. Enthält eine variable Bit-Zahl, die sicherstellt, dass der TCP-Header bei Benutzung des Options-Feldes immer im 32-Bit-Format endet.
---------	---	---

Alle weiteren Informationen, die zum Senden und Empfangen nötig sind, enthält der gekapselte IP-Header.

› TCP: Sliding Window

Das Sliding Window Protocol ist eine Methode zur Datenflusskontrolle, bei der ein Empfänger dem Sender die Übertragung von mehreren Segmenten auf einmal ermöglicht. Dies erlaubt eine schnellere Datenübertragung und senkt das Datenvolumen, da der Sender nicht nach jedem Segment auf eine Bestätigung warten muss.

Um also eine höhere Effizienz zu erreichen, wird nicht ein Segment nach dem anderen gesendet, sondern es werden gleich alle Segmente innerhalb eines sogenannten Fensters (Window) gesendet. Auf der Empfängerseite existiert analog dazu ebenfalls ein Fenster, in dem die Pakete aufgenommen und wieder zu einem Strom zusammengesetzt werden.



Sliding Window: Datenflusskontrolle für eine höhere Effizienz einer TCP-Verbindung.

© tecChannel.de

Trifft nun die Bestätigung für das erste Segment im Fenster beim Sender ein, so wird das Fenster um ein Segment weiterschoben (Sliding), und das nächste Segment wird gesendet. Alle Segmente links vom Fenster sind somit bereits bestätigt, alle im Fenster sind gesendet aber noch nicht bestätigt, und Segmente rechts davon sind noch nicht gesendet. Das erste Segment im Fenster ist also das letzte noch nicht bestätigte Paket. Die Größe des Fensters richtet sich nach dem TCP-Puffer des Empfangsrechners, kann aber vom Administrator eines Servers manuell geändert werden.

› UDP: User Datagramm Protocol

Das User Datagram Protocol (UDP) bietet höheren Protokollen einen definierten Dienst zum transaktionsorientierten Versand von Datenpaketen. UDP verfügt nur über minimale Protokollmechanismen zur Datenübertragung. Es setzt unmittelbar auf dem Internet Protocol auf. Da es im Gegensatz zu TCP keine Ende-zu-Ende-Kontrolle garantiert, sind weder die Ablieferung eines Datenpakets beim Empfänger, das Erkennen von Duplikaten oder die reihenfolgerichtige Übermittlung gewährleistet.

Es gibt dennoch eine Reihe von guten Gründen, die dafür sprechen, UDP als Datentransportdienst zu wählen. Wenn nur geringe Datenmengen zu übertragen sind kann es passieren, dass der Verwaltungsaufwand für die Herstellung einer Verbindung und das Sicherstellen einer korrekten Übertragung größer wären als der Aufwand für eine erneute Übertragung der gesamten Daten.

Minimale Protokollmechanismen: Der UDP-Header im Detail.



© tecChannel

UDP-Header im Detail

Name	Größe (in Bits)	Beschreibung
Source Port	16	Enthält die optionale Adresse des Sende-Ports. Bei Antworten auf Datenpakete kann durch die Portadresse der jeweilige Prozess unmittelbar wieder angesprochen werden. Wird vom Sender kein Sende-Port definiert, so wird dieses Feld mit dem Wert "0" übertragen.
Destination Port	16	Enthält die Adresse des Empfänger-Ports.
Length	16	Definiert die Gesamtlänge des Datenpakets, inklusive Header und Nutzdaten.
Checksum	16	Enthält eine optionale Prüfsumme. Der Wert "0" weist darauf hin, dass keine Berechnung erfolgt ist. Die Prüfsumme wird aus dem UDP-Header und einem 96-Bit-Pseudo-Header errechnet.

Alle weiteren Informationen, die zum Senden und Empfangen nötig sind, enthält der gekapselte IP-Header.

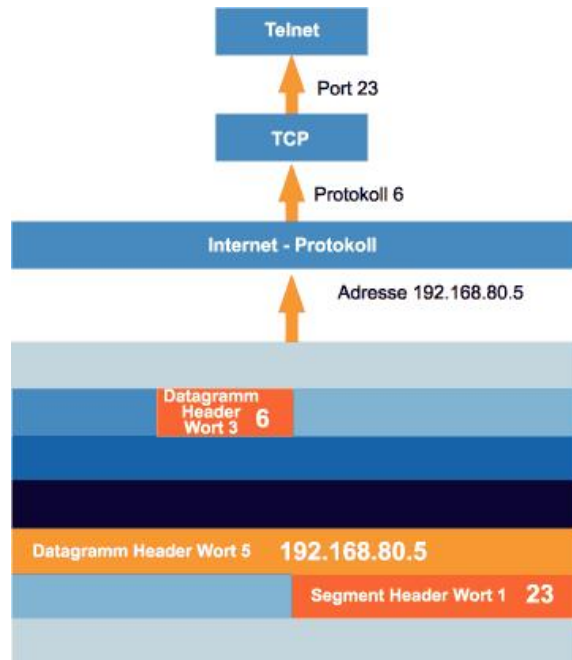
› Nebenstellen: Protocols, Ports und Sockets

Sind die Daten am Zielrechner angekommen, müssen diese noch an den richtigen Anwendungsprozess ausgeliefert werden. Beim Transport der Daten durch die einzelnen TCP/IP-Schichten benötigt man einen Mechanismus, der die Übergabe der Daten an das jeweilige richtige Protokoll sicherstellt. Das Zusammenlegen von Daten aus mehreren Quellen zu einem einzigen Datenstrom nennt man Multiplexen.

Ankommende Daten aus dem Netz muss IP also demultiplexen. Dazu kennzeichnet IP die Transportprotokolle mit Protokollnummern. Die Transportprotokolle selber nutzen Portnummern zur Identifizierung von Anwendungen. Einige dieser Protokoll- und Portnummern sind so genannte "Well-known services" - reservierte Nummern für Standardservices wie FTP oder Telnet. Also Dienste, die im gesamten Internet verbreitet sind.

Die IP-Protokollnummer steht in einem Byte im dritten Wort des Datagramm-Headers. Dieser Wert bestimmt die Übergabe an das jeweilige Protokoll in der Transportschicht,

beispielsweise "6" für TCP oder "17" für UDP. Das Transportprotokoll muss nach Empfang der Daten diese an den richtigen Anwendungsprozess übergeben. Anwendungsprozesse werden anhand einer 16-Bit langen Portnummer identifiziert. Im ersten Wort jedes TCP- und UDP-Headers sind sowohl die "Source Port"-Nummer als auch die "Destination Port"-Nummer enthalten.



Nebenstellen: Nach Empfang der Daten werden diese an den richtigen Anwendungsprozess übergeben.

© tecChannel.de

TCP und UDP können dabei die selben Portnummern vergeben. Erst die Kombination aus Protokoll und Portnummer ist eindeutig. Somit ist die Portnummer 53 in TCP nicht identisch mit der Portnummer 53 in UDP. Man unterscheidet zwischen unterschiedlichen Port-Typen:

- › Well-known ports: Bei diesem Typ handelt es sich um reservierte und standardisierte Port-Nummern zwischen 1 und 1023. Dies vereinfacht den Aufbau einer Verbindung, weil sowohl Absender und Empfänger bereits wissen, dass Daten für einen bestimmten Prozess an einen bestimmten Port gesendet werden müssen. So nutzen beispielsweise alle Systeme für Telnet den Port 23.
- › Dynamically allocated ports: Diese dynamisch zugewiesenen Ports werden nicht vorab vergeben, sondern erst, wenn ein Prozess einen Port benötigt.

Die Kombination aus IP-Adresse und Port-Nummer wird als Socket bezeichnet. Ein Socket kann einen einzelnen Netzwerkprozess innerhalb des gesamten Internet eindeutig identifizieren. Zwei Sockets, einer für den Ausgangs- und einer für den Zielrechner, definieren eine Verbindung für verbindungsorientierte Protokolle wie TCP/IP.

Die [Liste](http://www.iana.org/assignments/port-numbers) (<http://www.iana.org/assignments/port-numbers>) der aktuell vergebenen Portnummern wird von der [IANA](http://www.iana.org) (<http://www.iana.org>) verwaltet.

› PPP: Point-to-Point Protocol

Das Point-to-Point-Protokoll (PPP) kam ursprünglich als Kapselungs-Protokoll für die Übertragung von IP-Datenverkehr über Punkt-zu-Punkt-Verbindungen auf. Es löste das ältere Serial Line Interface Protocol (SLIP) ab. Heute wird es hauptsächlich bei Internet-Providern zur Einwahl benutzt. PPP besteht aus drei Komponenten:

- › Die Fähigkeit IP-Datagramme auf einer seriellen Verbindung zu kapseln. PPP

unterstützt asynchrone und Bit-orientierte synchrone Verbindungen.

- › Einem Link Control Protocol (LCP) zum Aufbau, Konfigurieren und Testen einer Datenverbindung.
- › Einer Familie von Network Control Protocols (NCP) zur Unterstützung verschiedener Protokolle der Netzwerkschicht.

Bevor über PPP Daten ausgetauscht werden können, muss ein Verbindungsaufbau stattgefunden haben. Dazu einigen sich beide Endpunkte auf die wesentlichen Merkmale der aufzubauenden Verbindung, wie Komprimierungsverfahren oder Frame-Größe. Wird die Verbindungskonfiguration von beiden Rechnern akzeptiert, kann ein Zugangsberechtigungsverfahren mittels PAP- oder CHAP-Protokoll starten.

Das Password Authentication Protocol (PAP) war das erste Zugangsberechtigungsprotokoll für PPP. Wenn ein Rechner eine Verbindung zu einem Router aufbaut, sendet er wiederholt den PAP-Benutzernamen und das Passwort, bis die Verbindung aufgebaut ist oder abgebrochen wird. Dies schützt allerdings nicht vor einem so genannten Modem-Playback. Bei diesem Verfahren klemmt sich der Eindringling in die Telefonverbindung ein und zeichnet die Datenübertragung auf. Benutzername und Passwort lassen sich so leicht herausfinden.

Das Challenge Handshake Authentication Protocol (CHAP) ist ein verbessertes Zugangsverfahren. Mit CHAP baut der entfernte Rechner die Verbindung auf und erhält vom Router eine "Herausforderung" (Challenge) in Form eines kryptographischen Schlüssels. Der entfernte Rechner verschlüsselt Benutzername und Passwort vor der Übertragung. Nach dem Empfang entschlüsselt der Router Benutzername und Passwort mit demselben Schlüssel. Nach Erhalt der Zugangsberechtigung legen beide Rechner die Protokolle fest, die für PPP verkapselt werden sollen.

› IPv6: Internet Protocol Version 6

Die rund vier Milliarden möglichen IP-Adressen werden dem Boom im Internet nicht mehr gerecht. Da demnächst praktisch jede Kaffeemaschine über eine eigene Internet-Adresse verfügen soll, stößt der derzeit verwendete Protokolltyp IPv4 an seine Grenzen. Zudem kennt IPv4 keine Sicherheitsfunktionen oder Verschlüsselung. Auch Streaming-Anwendungen wird das Protokoll nicht gerecht.

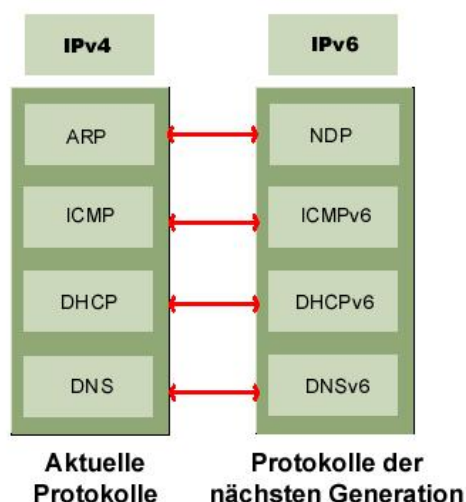
Daher ist ein neues Protokoll mit größerem Adressraum notwendig. Der Nachfolger steht bereits in den Startlöchern. Er trägt die Bezeichnung Internet Protocol Version 6 (IPv6) und wurde Anfang der 90er Jahre von der Internet Engineering Task Force (IETF (<http://www.ietf.org>)) empfohlen. Die IETF ist die zentrale Organisation zur technischen Entwicklung und Standardisierung des Internet. Die Spezifikationen wurden in RFC1883 (<ftp://ftp.isi.edu/in-notes/rfc1883.txt>) festgelegt. IPv6 soll viele Unzulänglichkeiten seines Vorgängers beseitigen.

Seitdem haben viele Unternehmen, Organisationen und Netzwerker damit begonnen, erste Implementierungen zu entwickeln. Insbesondere Hersteller von Routern haben ihren Produkten eine IPv6-Unterstützung verpasst. Aber auch Entwickler sind auf den IPv6-Zug aufgesprungen. Mit 6Bone (<http://www.6bone.net>) existiert bereits ein entsprechendes globales Netzwerk.

› Der Weg zu IPv6

Das neue Protokoll IPv6 wird innerhalb der IETF (<http://www.ietf.org>) zentral im Bereich Internet in der Gruppe IPNGWG behandelt. Bestimmte Teile werden aber auch in anderen Gruppen und Bereichen standardisiert, wie zum Beispiel die Migration von IPv4 zu IPv6 im Bereich NGTRANS.

Einige Zeit, bevor die Entscheidung zur Entwicklung von IPv6 gefallen war, wurde ein anderes Protokoll als Alternative zu IPv4 vorgeschlagen: IPv5. Dieses Protokoll wurde jedoch nur experimentell implementiert und fand keinerlei Verbreitung in kommerziellen Produkten.



Großer Umstieg: Mit IPv6 ändern sich auch viele Dienste und Protokolle im IP-Umfeld.

© tecChannel

Bei der Entwicklung des Nachfolgers für IPv4 standen drei Vorschläge konkurrierend nebeneinander: [Simple Internet Protocol Plus](http://www.ietf.org/html.charters/OLD/sipp-charter.html) (SIPP), [Common Architecture for the Internet \(CATNIP, RFC1707\)](http://www.ietf.org/html.charters/OLD/catnip-charter.html) (<ftp://ftp.isi.edu/in-notes/rfc1707.txt>) und [The TCP/UDP over CLNP-Addressed Networks](http://www.ietf.org/html.charters/OLD/tuba-charter.html) (TUBA). Erst im Jahre 1993 erarbeitete eine eigene Arbeitsgruppe (IPNG) einen gemeinsamen Vorschlag. Die ersten Entwürfe führte man unter der Bezeichnung Internet Protocol next Generation (IPnG). Unter dem Namen Internet Protocol Version 6 (IPv6) entstanden im Laufe der Jahre 1995 und 1996 zahlreiche Entwürfe. Im Jahre 1997 wurde IPv6 zum "Draft Standard".

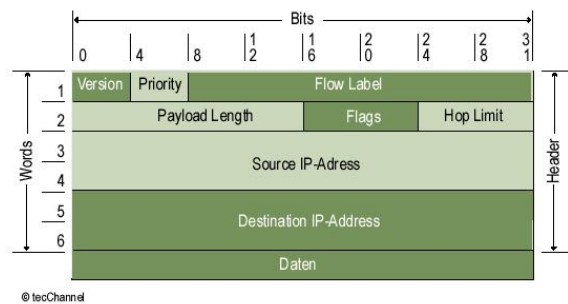
› IPv6 im Überblick

IPv6 ist wie sein Vorgänger IPv4 ein Transportprotokoll, das einzelne Pakete durch ein Netz transportiert. Zur Sicherstellung der vollständigen Übertragung kann IPv6 Protokolle auf einer höheren Schicht, zum Beispiel TCP, verwenden. Die wesentlichen funktionalen Elemente des neuen Protokolls sind:

- › 128 Bit lange IP-Adressen.
- › Vereinfachte Struktur des Headers.
- › Verkettete Header für den Transport von Optionen.
- › Optionen für Verschlüsselung und Authentisierung auf IP-Ebene.
- › Neue Klassifizierung von Datenströmen (Flows) für einen optimierten Transport von Audio- und Video-Daten.
- › Vereinfachung der manuellen Konfiguration.
- › Verbesserung der Flusskontrolle und der Erkennung von Engpässen.
- › Spezielle Mechanismen zur Entdeckung und Überwachung von Nachbarn beim Einsatz auf Routern.

› IPv6-Header im Detail

Die Vereinfachung der Header-Struktur zählt zu den bedeutendsten Neuerungen der IPv6-Spezifikation. Im Gegensatz zum Vorgänger IPv4 wurde der Header auf das unbedingt notwendige Minimum gekürzt. Dies ermöglicht eine schnellere Bearbeitung und somit einen schnelleren Transport über Router.



Übersichtlicher: Der IPv6-Header ist gegenüber dem alten IPv4-Header deutlich vereinfacht.

Der IPv6-Header im Detail

Name	Größe (in Bits)	Beschreibung
Version	4	Enthält bei IPv6 stets den Wert 6. Dieses Feld verwendet die Software zur Unterscheidung verschiedener IP-Versionen. Dies ermöglicht die parallele Verwendung unterschiedlicher Versionen des Protokolls.
Class	8	Gibt an, mit welcher Priorität die Daten auf dem Weg zum Ziel behandelt werden.
Flow-Label	20	Kennzeichnet einen Datenstrom zwischen Sender und Empfänger. Hierzu tragen alle Pakete, die zu einem bestimmten Datenstrom gehören, in diesem Feld den gleichen Wert.
Payload Length	16	Gibt die Länge des Datenpakets nach dem ersten Header an. Es werden die reinen Nutzdaten sowie alle vorhandenen optionalen Header berücksichtigt.
Next	8	Kennzeichnet den Typ des nächsten Header. Der Eintrag "59" bedeutet, dass weder weitere Header noch Daten folgen.
Hop-Limit	8	Legt fest, nach wie vielen Durchgängen durch einen Router das Datenpaket zur Vermeidung von Schleifen verworfen werden soll. Der Maximalwert in diesem Feld beträgt 255.
Source Address	128	Beinhaltet die Absenderadresse.
Destination Address	128	Beinhaltet die Adresse des Empfängers.

Da man alle bisher bereits benutzten Funktionen und auch neue Features des Protokolls verwenden möchte, ist eine Erweiterung des IPv6-Headers notwendig. Dies geschieht nicht mehr wie in IPv4 mit Hilfe eines variabel langen Optionsfeldes, sondern durch die Verkettung von zusätzlichen Headern. Jeder Header hat eine bestimmte Funktion und wird nur bei Bedarf verwendet.

› Neue Adressen

Die wohl wichtigste Änderung, die IPv6 mit sich bringt, ist die Vergrößerung des IP-Adressraums. Die Entscheidung, welche Anzahl von Bytes letztendlich benötigt wird, blieb lange offen. Erfahrungen bei der Zuteilung der IPv4-Adressen zeigen, dass nur ein Bruchteil der möglichen Adressen tatsächlich Verwendung findet. Der Grund hierfür liegt in der veralteten Einteilung in feste Klassen. In einem Class-B-Netz werden in der Praxis lediglich rund 2.500 Adressen der rund 65.000 Adressen tatsächlich genutzt.

Durch die Erweiterung der Adresslänge von 32 auf 128 Bit ergeben sich 2^{128} mögliche IP-Adressen. Ausgeschrieben sind das astronomische 340.282.366.920.938.463.463.374.607.431.768.211.456 verschiedene Werte. Da diese Zahl von Normalsterblichen kaum zu fassen ist, haben sich findige Rechenkünstler einen nicht minder beeindruckenden Vergleich ausgedacht: Die Adressvielfalt reicht aus, um jeden Quadratkilometer der Erdoberfläche mit 665.570.793.348.866.943.898.599 Adressen abzudecken. Damit dürfte auch jede Waschmaschine problemlos eine eigene IP-Adresse abbekommen.

› IPv6-Adressformat

Der Anwender kommt auch in Zeiten des Domain Name System (DNS) gelegentlich mit den IP-Adressen in Berührung. Für eine vereinfachte Schreibweise werden bei IPv4 vier Bytes einer Adresse als normale Zahlen zur Basis zehn notiert. Die einzelnen Bytes werden durch einen Punkt voneinander getrennt, zum Beispiel 127.0.0.1. Bei den neuen 128-Bit-Adressen von IPv6 führt dies jedoch zu einer äußerst unpraktischen Darstellung.

Aus diesem Grund verwendet IPv6 das Hexadezimalsystem. Dieses ermöglicht es, auch längere Zahlenreihen einigermaßen kompakt darzustellen. Man bildet Gruppen von je zwei Bytes und trennt sie durch einen Doppelpunkt, zum Beispiel 0000:0000:0000:3210:0123:4567:89AB:CDEF. Innerhalb einer Gruppe kann man auf führende Nullen verzichten. Um die noch immer langen Adressen weiter abzukürzen, darf man innerhalb einer Adresse eine Gruppe aufeinander folgender Nullen durch zwei Doppelpunkte ersetzen.

Laut Spezifikation von IPv6 können bestehende IPv4-Adressen innerhalb des Adressraums von IPv6 beibehalten werden. In diesem Fall kommt eine gemischte Schreibweise zum Einsatz: `::FFFF:127.0.0.1` entspricht also `0:0:0:0:FFFF:7F00:0001`.

› Arten von IPv6-Adressen

Die Internet Engineering Task Force ([IETF](http://www.ietf.org) (<http://www.ietf.org>)) legte mit anderen Internet-Gremien wie dem Internet Architecture Board ([IAB](http://www.iab.org) (<http://www.iab.org>)) und der Internet Society ([ISOC](http://www.isoc.org) (<http://www.isoc.org>)) fest, dass die IPv6-Adressen von der Internet Assigned Numbers Authority ([IANA](http://www.iana.org) (<http://www.iana.org>)) zentral verwaltet werden. Im Gegensatz zu den IPv4-Adressen ist die Vergabe der IPv6-Adressen nicht endgültig. Die neuen Adressenblöcke können wieder zurückgerufen werden, falls dies aus technischen Gründen oder wegen Missbrauchs erforderlich ist.

Bei IPv6 unterscheidet man zwischen drei Arten von Adressen:

- › Unicast-Adressen: Dieser Adresstyp stellt einen Identifikator für ein Interface an einem Rechner oder Router dar. Ein Datagramm an eine Unicast-Adresse wird an das durch die Adresse identifizierte Interface zugestellt.
- › Anycast-Adressen: Identifikator für eine Gruppe von Interfaces an einem Gerät oder an mehreren Geräten.
- › Multicast-Adressen definieren eine Gruppe. Sendet man ein Datagramm an eine Multicast-Adresse, empfangen alle Interfaces, die der Gruppe angehören, diese Nachricht.

› Sicherheit und ICMP

Der Sicherheitsaspekt stand bei der Entwicklung von IPv6 von Anfang an im Mittelpunkt. Es wurden Sicherheitsstandards definiert, die sowohl für IPv6 als auch für IPv4 verwendet werden können. Auf Grund der neuen Standards ist es möglich, Angriffe zu verhindern, die sich auf Adressänderungen beziehen oder die Kommunikation ausspähen. Die einzelnen Sicherheitsverfahren gliedert man in folgende Bereiche:

- › Verschlüsselung zur Sicherung gegen Mitlesen.
- › Authentisierung der Nachricht durch Prüfsumme zum Beweis der Unverfälschtheit.
- › Authentisierung der Absenders durch eine digitale Signatur.

Damit will man verhindern, dass ein Unbefugter den Inhalt der Nachricht auf dem Weg vom Sender zum Empfänger mitliest. Eine komplette Verschlüsselung stellt zudem sicher, dass die Nachricht nicht verändert werden kann. Der zweite Ansatz kommt ohne Verschlüsselung der Daten aus. Es wird eine Prüfsumme über den Datenblock erzeugt, der mit einem Schlüssel gesichert wird. Die Verwendung einer Prüfsumme mit einem nur dem Absender bekannten Wert ermöglicht gleichzeitig ein sicheres Verfahren zur Identifikation des Absenders.

IPv6 nutzt das Internet Control Message Protocol (ICMP) für IPv6 mit einigen Erweiterungen. Auf ICMP-Protokollelemente wird in Version 6 mit dem Wert 58 im Feld "Next" hingewiesen. Die wesentlichen Änderungen bei ICMP sind:

- › Neue Formate für die Übertragung der Adressauflösung, die das bisherige Address Resolution Protocol (ARP) ablösen.
- › Elemente zur Definition der maximalen zulässigen Datensatzlänge (MTU).
- › Neue Elemente zur Steuerung von Multicast-Gruppen. Diese ersetzen das Internet Group Management Protocol (IGMP, RFC2236 (<ftp://ftp.isi.edu/in-notes/rfc2236.txt>)) von IPv4.

› Sanfte Migration

Die Umstellung auf eine neue Technik bedeutet für einen Netzwerkadministrator immer eine enorme Gefahr: Netzabschaltungen, Störungen und folgende Betriebsunterbrechungen gehen für eine Firma nicht selten mit großen finanziellen Einbußen einher.

Für den Übergang auf IPv6 hat man sich daher viele Gedanken über eine "sanfte" Migration gemacht. Innerhalb der Internet Engineering Task Force (IETF (<http://www.ietf.org>)) gründete man hierfür eine eigene Arbeitsgruppe. Diese soll verschiedene Modelle für den Übergang und die Einführung ausarbeiten.

In RFC1933 (<ftp://ftp.isi.edu/in-notes/rfc1933.txt>) wurde ein Mechanismus definiert, der für den "sanften" Umstieg von einer Protokollversion zur nächsten sorgt. DNS-Server müssen mit den in RFC 1886 (<ftp://ftp.isi.edu/in-notes/rfc1886.txt>) definierten Erweiterungen auf IPv6 vorbereitet sein.

› Implementierungen

Was bedeutet IPv6 nun für den Anwender? Kann oder muss man sich bald um einen neuen TCP/IP-Stack für seinen Rechner kümmern? Oder muss man womöglich gar auf eine neue Betriebssystemversion umsteigen?

Derzeit kann man sich noch in Geduld üben. Das Internet wird nach wie vor von IPv4 beherrscht. Und das wird wohl auch noch einige Zeit so bleiben. Erste Implementierungen von IPv6 gibt es zwar, doch sind die wichtigsten Komponenten, DNS-Server und Router, längst noch nicht umgerüstet.

Als Anwender muss man sich um diese Dinge praktisch nicht kümmern: Ein Dual-Stack-Mechanismus automatisiert die Kommunikation mit neuen IPv6- und alten IPv4-Hosts - zumindest in der Theorie. Ist IPv6 sauber implementiert, sollten keine

Probleme auftreten. Doch da wird es noch manche Überraschungen geben. (kpf)

› Weitere Themen zu diesem Artikel:

So funktioniert HTTP (<http://www.tecchannel.de/internet/208/index.html>)

So funktioniert FTP (<http://www.tecchannel.de/internet/207/index.html>)

So funktioniert DHCP (<http://www.tecchannel.de/internet/206/index.html>)

So funktioniert das Domain Name System (<http://www.tecchannel.de/internet/205/index.html>)

WML-Grundlagen (<http://www.tecchannel.de/internet/258/index.html>)

Copyright © 2001
IDG Interactive GmbH

Alle Rechte vorbehalten. Jegliche Vervielfältigung oder Weiterverbreitung in jedem Medium in Teilen oder als Ganzes bedarf der schriftlichen Zustimmung der IDG Interactive GmbH. DPA-Texte und Bilder sind urheberrechtlich geschützt und dürfen weder reproduziert noch wiederverwendet oder für gewerbliche Zwecke verwendet werden. Für den Fall, dass in tecChannel unzutreffende Informationen veröffentlicht oder in Programmen oder Datenbanken Fehler enthalten sein sollten, kommt eine Haftung nur bei grober Fahrlässigkeit des Verlages oder seiner Mitarbeiter in Betracht. Die Redaktion übernimmt keine Haftung für unverlangt eingesandte Manuskripte, Fotos und Illustrationen. Für Inhalte externer Seiten, auf die von tecChannel aus gelinkt wird, übernimmt die IDG Interactive GmbH keine Verantwortung.