

Internet Protokoll

Das Internet Protocol (IP) stellt die Basisdienste für die Übermittlung von Daten in TCP/IP- Netzen bereit und ist im RFC 791 spezifiziert. Hauptaufgaben des Internet Protokolls sind die Adressierung von Hosts und das Fragmentieren von Paketen. Diese Pakete werden von IP nach bestem Bemühen ("best effort") von der Quelle zum Ziel befördert, unabhängig davon, ob sich die Hosts im gleichen Netz befinden oder andere Netze dazwischen liegen. Garantiert ist die Zustellung allerdings nicht. Das Internet Protokoll enthält keine Funktionen für die Ende- zu- Ende- Sicherung oder für die Flußkontrolle.

Die Funktionen von IP umfassen:

Die Definition von Datengrammen, welche die Basiseinheiten für die Übermittlung von Daten im Internet bilden.

Definition des Adressierungsschemas.

Übermittlung der Daten von der Transportebene zur Netzwerkschicht.

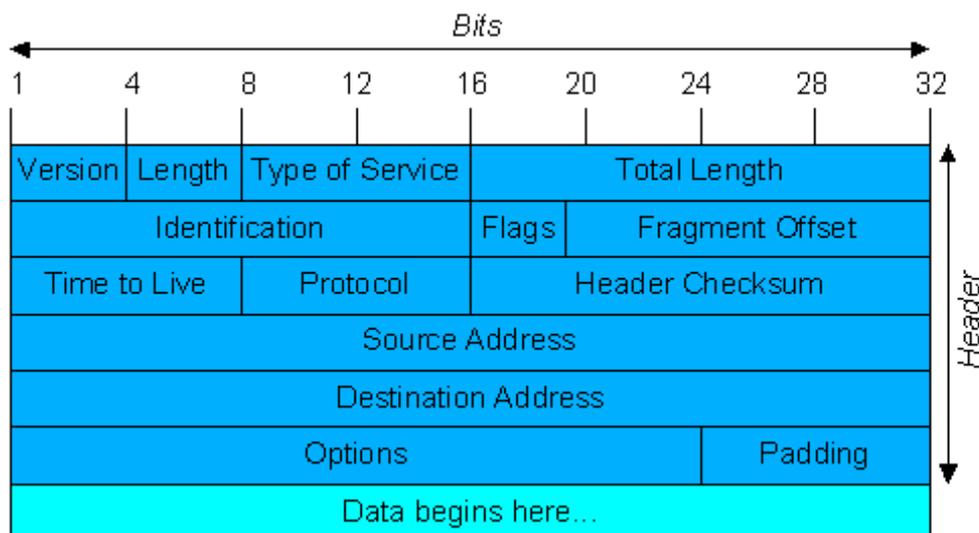
Routing von Datengrammen durch das Netz.

Fragmentierung und Zusammensetzen von Datengrammen.

IP ist ein verbindungsloses Protokoll, d.h. zur Datenübertragung wird keine Ende- zu- Ende- Verbindung der Kommunikationspartner etabliert. Ferner ist IP ein unzuverlässiges Protokoll, da es über keine Mechanismen zur Fehlererkennung und -behebung verfügt. Unzuverlässig bedeutet aber keinesfalls, daß man sich auf das IP Protokoll nicht verlassen kann. Unzuverlässig bedeutet in diesem Zusammenhang lediglich, daß IP die Zustellung der Daten nicht garantieren kann. Sind die Daten aber beim Zielhost angelangt, sind diese Daten auch korrekt.

IP- Datengramm

Die TCP/IP- Protokolle wurden entwickelt, um Daten über ein paketvermittelndes Netz (wie dem ARPANET) zu übertragen. Ein Paket ist ein Datenblock zusammen mit den Informationen, die notwendig sind, um sie dem Empfänger zuzustellen (ein Paket ist also nichts anderes als ein Paket im herkömmliche Sinn bei der Post – das Paket enthält die Daten, auf dem Paket ist die Adresse des Empfängers notiert). Das Datengramm (engl. datagram) ist das Paketformat, das vom Internet Protokoll definiert ist. Ein IP- Datengramm besteht aus einem Header und den zu übertragenden Daten. Der Header hat einen festen 20 Byte großen Teil, gefolgt von einem optionalen Teil variabler Länge. Der Header umfaßt alle Informationen, die notwendig sind, um das Datengramm dem Empfänger zuzustellen. Ein Datengramm kann theoretisch maximal 64 KByte groß sein, in der Praxis liegt die Größe ungefähr bei 1500 Byte (das hängt mit der maximalen Rahmengröße des Ethernet- Protokolls zusammen).



Die wichtigsten Erklärungen zum IP-Header:

Version:

Gibt die Versionsnummer des verwendeten IP-Protokolls an. Die derzeitige Versionsnummer ist 4, aber die Version 6 des IP-Protokolls befindet sich bereits in der Erprobung.

Length:

Gibt die Länge des Headers an (20 – 60 Bytes)

Total Length:

Enthält die gesamte Paketlänge, d.h. Header und Daten. Da es sich hierbei um ein 16-Bit-Feld handelt, ist die Maximallänge eines Datengramms auf 65.535 Bytes begrenzt.

Identification:

Über das Identifikationsfeld kann der Zielhost feststellen, zu welchem Datengramm ein neu angekommenes Fragment gehört. Alle Fragmente eines Datengramms enthalten die gleiche Identifikationsnummer, die vom Absender vergeben wird.

Protocol:

Enthält die Nummer des Transportprotokolls, an das das Paket weitergeleitet werden muß. Die Numerierung von Protokollen ist im gesamten Internet einheitlich und im RFC 1700 definiert.

Header Checksum:

Dieses Feld enthält die Prüfsumme der Felder im IP-Header.

Source Address / Destination Address:

In diese Felder werden die 32-Bit langen Internet-Adressen eingetragen.

Daten-Bereich:

Der Datenbereich enthält die zu übermittelnden Daten

Weitere Details zu den Optionen sind in RFC 791 zu finden.

Adressierung auf der Internet-Schicht

Zur Adressierung eines Kommunikationspartners in Form eines Applikationsprogramms müssen beim Durchlaufen der vier TCP/IP-Schichten auch vier verschiedene Adressen angegeben werden.

1. Eine Netzwerkadresse (z.B. eine Ethernet-Adresse)
2. Eine Internet-Adresse
3. Eine Transportprotokoll-Adresse
4. Eine Portnummer

Zwei dieser Adressen finden sich als Felder im IP-Header: die Internet-Adresse und die Transportprotokoll-Adresse.

Protokollnummern:

IP verwendet Protokollnummern, um empfangene Daten an das richtige Transportprotokoll weiterzuleiten. Die Protokollnummer ist ein einzelnes Byte im IP-Header. Die Protokollnummern sind im gesamten Internet einheitlich. Definiert sind die Protokollnummern im RFC 1700.

Empfängt IP ein Datengramm, in dessen Header als Protokollnummer 6 eingetragen ist, so werden diese Daten an das Transmission Control Protocol (TCP) weitergeleitet; ist die Nummer 17, werden die Daten an das User Datagram Protocol (UDP) weitergeleitet etc.

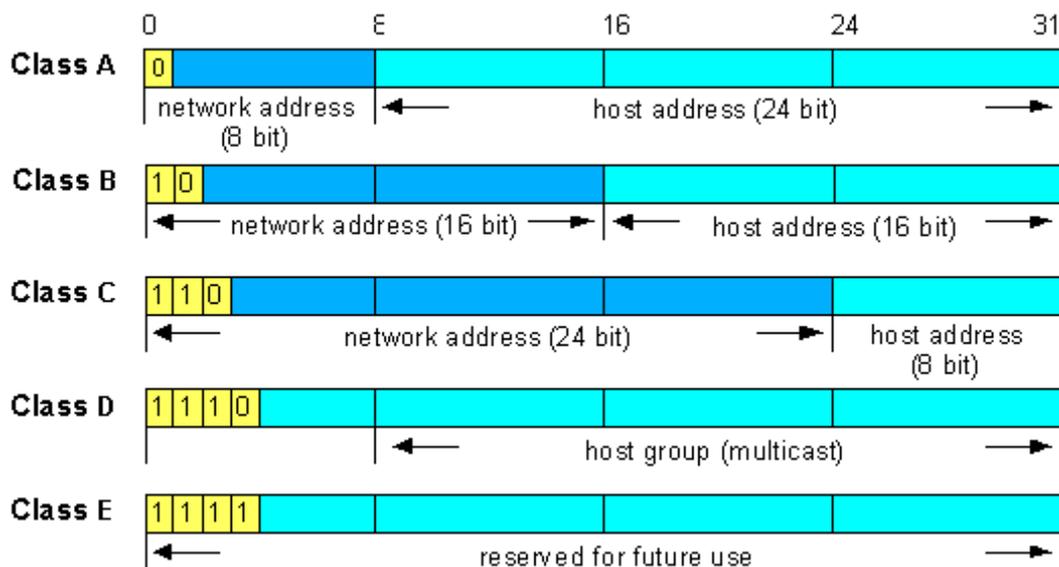
<u>Protokoll</u>	<u>Protokoll-Nr.</u>
<u>IP</u>	0

ICMP	1
IGMP	2
GGP	3
TCP	6
PUP	12
UDP	17
IDP	22
RAW	255

IP- Adressen

Jeder Host und Router im Internet hat eine 32-Bit lange IP- Adresse. Eine IP- Adresse ist eindeutig. Maschinen, die an mehrere Netze angeschlossen sind, haben in jedem Netz eine eigene IP- Adresse.

Wie die obere Abbildung zeigt, sind IP- Adressen in verschiedene Klassen, mit unterschiedlich langer Netzwerk- und Hostadresse, eingeteilt. Die Netzwerkadresse definiert das Netzwerk, in dem sich ein Host befindet: alle Hosts eines Netzes haben die gleiche Netzwerkadresse. Die Hostadresse identifiziert einen bestimmten Rechner innerhalb eines Netzes. Ist ein Host an mehrere Netze angeschlossen, so hat er für jedes Netz eine eigene IP- Adresse.



IP- Adressen sind 32-Bit große Zahlen, die normalerweise nicht als Binärzahl, sondern in gepunkteten Dezimalzahlen geschrieben werden. In diesem Format wird die 32-Bit große Zahl in 4 Byte getrennt, die mit Punkten voneinander getrennt sind. Die Adresse 01111111111111111111111111111111 wird so z.B. als 127.255.255.255 geschrieben. Die niedrigste IP- Adresse ist 0.0.0.0., die höchste 255.255.255.255.

Wie zuvor gesagt, sind IP– Adressen in Klassen unterteilt. Der Wert des ersten Bytes gibt die Adressklasse an:

Klasse A:

Das erste Byte hat einen Wert kleiner als 128, d.h. das erste Bit der Adresse ist 0. Das erste Byte ist Netzwerknummer, die letzten drei Bytes identifizieren einen Host im Netz. Es gibt demzufolge also 126 Klasse A Netze, die bis zu 16 Millionen Host in einem Netz.

Klasse B:

Ein Wert von 128 bis 191 für das erste Byte (das erste Bit ist gleich 1, Bit 2 gleich 0) identifiziert eine Klasse B Adresse. Die ersten beiden Bytes identifizieren das Netzwerk, die letzten beiden Bytes einen Host. Das ergibt 16382 Klasse B Netze mit bis zu 64000 Hosts in einem Netz.

Klasse C:

Klasse C Netze werden über Werte von 192 bis 223 für das erste Byte (die ersten beiden Bits sind gleich 1, Bit 3 gleich 0) identifiziert. Es gibt 2 Millionen Klasse C Netze, d.h. die ersten drei Bytes werden für die Netzwerkadresse verwendet. Ein Klasse C Netz kann bis zu 254 Host beinhalten.

Klasse D:

Klasse D Adressen, sogenannte Multicast– Adressen, werden dazu verwendet ein Datagramm an mehrere Hostadressen gleichzeitig zu versenden. Das erste Byte einer Multicast– Adresse hat den Wertebereich von 224 bis 239, d.h. die ersten drei Bytes sind gesetzt und Byte 4 ist gleich 0. Sendet ein Prozeß eine Nachricht an eine Adresse der Klasse D, wird die Nachricht an alle Mitglieder der adressierten Gruppe versendet. Die Übermittlung der Nachricht erfolgt, wie bei IP üblich, nach bestem Bemühen, d.h. ohne Garantie, daß die Daten auch tatsächlich alle Mitglieder einer Gruppe erreichen.

Für das Multicasting wird ein spezielles Protokoll namens Internet Group Management Protocol (IGMP) verwendet. IGMP entspricht grob ICMP, mit dem Unterschied, daß es nur zwei Arten von Paketen kennt: Anfragen und Antworten. Anfragen werden dazu verwendet, zu ermitteln welche Hosts Mitglieder einer Gruppe sind. Antworten informieren darüber, zu welchen Gruppen ein Host gehört. Jedes IGMP– Paket hat ein festes Format und wird zur Übertragung in IP– Pakete eingekapselt. Auf IGMP wird jedoch nicht weiter eingegangen.

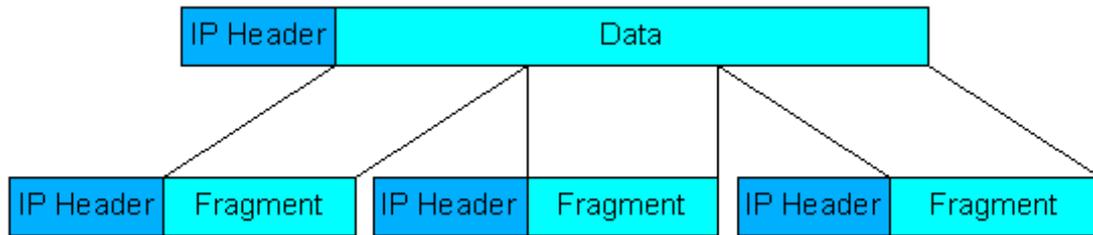
Der weitere Bereich der IP– Adressen von 240 bis 254 im ersten Byte ist für zukünftige Nutzungen reserviert. In der Literatur wird dieser Bereich oft auch als Klasse E bezeichnet.

Fragmentierung

Damit Datagramme über jede Art von Netzwerk verschickt werden können, muß das Internet Protokoll dazu in der Lage sein, die Größe der Datagramme dem jeweiligen Netz anzupassen. Jedes Netzwerk besitzt eine sogenannte maximale Paketgröße (Maximum Transfer Unit – MTU), die bezeichnet, daß nur Pakete bis zu dieser Größe über das Netz verschickt werden können. So dürfen z.B. Pakete, die über ein X.25–Netz verschickt werden sollen nicht größer als 128 Byte sein. Ein Ethernet–Paket darf die Größe von 1500 Byte nicht überschreiten. Falls die MTU eines Übertragungsmediums kleiner ist als die Größe eines versendeten Pakets, so muß dieses Paket in kleinere Pakete aufgeteilt werden.

Es genügt allerdings nicht, daß die Protokolle der Transportschicht nun von sich aus einfach kleinere Pakete versenden. Ein Paket kann auf dem Weg vom Quell– zum Zielhost mehrere unterschiedliche Netzwerke mit unterschiedlichen MTUs durchlaufen. Aus diesem Grund muß ein flexibleres Verfahren angewendet werden, daß bereits auf der Internet–Schicht kleiner Pakete erzeugen kann. Dieses Verfahren wird Fragmentierung genannt.

Unter Fragmentierung wird verstanden, daß das IP– Protokoll eines jeden Netzwerkknotens in der Lage ist empfangene Pakete gegebenenfalls zu zerteilen, um sie weiter über ein Teilnetz bis zum Zielhost zu übertragen. Jedes empfangende IP muß dazu in der Lage sein, diese Fragmente wieder zum ursprünglichen Paket zusammenzusetzen.



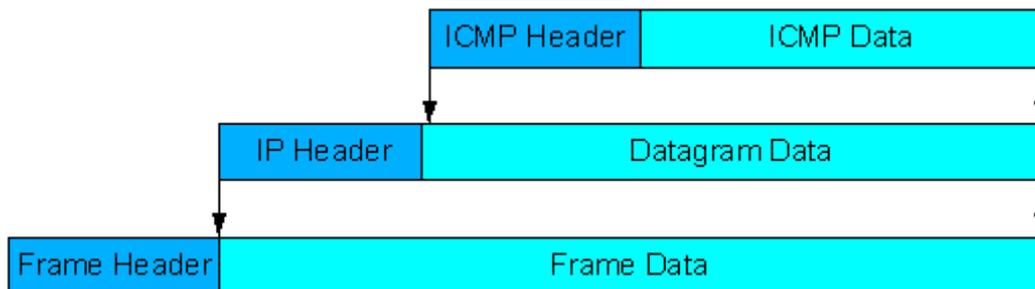
Jedes Fragment eines zerteilten Pakets erhält einen eigenen, vollständigen IP-Header. Über das Identifikationsfeld im Header können alle Fragmente eines Pakets wiedererkannt werden. Die einzelnen Fragmente eines Pakets können durchaus unterschiedliche Wege auf dem Weg zum Zielhost nehmen. Die Lage der Daten eines Fragments innerhalb der Gesamtnachricht wird mit Hilfe des Fragment Offset-Feldes ermittelt.

Internet Control Message Protocol

Das Internet Control Message Protocol (ICMP) ist Bestandteil jeder IP-Implementierung und hat die Aufgabe Fehler- und Diagnoseinformationen für IP zu transportieren. ICMP ist im RFC 792 spezifiziert.

ICMP hat sehr unterschiedliche Informationen zu transportieren. Deshalb ist nur der Grundaufbau des ICMP-Headers immer gleich, die Bedeutung der einzelnen Felder im Protokollkopf wechselt jedoch. Jeder ICMP-Nachrichtentyp wird in einem IP-Datengramm eingekapselt.

IP verwendet ICMP zum versenden von Fehler- und Diagnosemeldungen, während ICMP zur Übertragung seiner Nachrichten IP benutzt. Das bedeutet, wenn eine ICMP-Nachricht verschickt werden muß, wird ein IP-Datengramm erzeugt und die ICMP-Meldung in den Datenbereich des IP-Datengramms eingekapselt.



Als Quellen dienten mir verschiedene Internetseiten.

Von Stephan Burghartz