

TCP / IP Protokolfamilie

PascalAdam TSBE

Geschichte der TCP/IP Protokollfamilie

- 1957 Gründung der Advanced Research Project Agency (ARPA) als Teil des DoD
- 1969 ARPA eingeführt beim DoD
- 1972 Telnet
- 1973 FTP
- 1974 TCP
- 1981 IP
- 1984 DNS

Der Standardisierungsprozess im Internet

- Eine internationale Gruppe, die Internet Society, verwaltet die TCP/IP Protokollfamilie.
- Die TCP/IP-Standards werden in der Reihe von Dokumenten, RFC's (Request for Comments) veröffentlicht.
- <http://www.ietf.org/rfc.html>

RFC Status

- Informational – Hinweis, Idee, Nutzung
- Experimental – zum Experimentieren
- Proposed Standard – Vorschlag für Standard
- Draft Standard – Begutachtung von mindestens zwei unabhängigen Implementierungen
- Standard – offizieller Standard STDn
- Historic – nicht mehr benutzt

Internet Society (ISOC)

- Die Internet Society (ISOC) wurde 1992 auf der INET-Konferenz in Kōbe (Japan) gegründet und ist für die Weiterentwicklung der Internetinfrastruktur zuständig. Die ISOC hat ihren Hauptsitz in der Nähe von Washington, D.C und besteht aus mehr als 6.000 Einzelpersonen sowie ca. 150 Organisationen aus über 170 Ländern. Die Mitglieder (ca. 16.000) sind verpflichtet, zur weltweiten Verbreitung des Internets beizutragen und dessen Fortbestehen zu garantieren. Dazu zählt unter anderem die Veröffentlichung der sogenannten RFC's. Der Vorstand der ISOC (*Board of Trustees*) besteht aus 15 Mitgliedern, die von allen Mitgliedern weltweit gewählt werden.
- <http://www.isoc.org/>

Internet Architecture Board (IAB)

- Das Internet Architecture Board (IAB) ist ein Komitee, welches den architekturellen Überblick über die Standardisierungsaktivitäten der Internet Engineering Task Force (IETF) wahrt und die ISOC beratend unterstützt. Das IAB ist verantwortlich, die architekturelle Entwicklung des Internets „im Auge zu behalten“ und wacht daher über verschiedene Aktivitäten der IETF. Das IAB interessiert sich vor allem für die langfristige architekturelle Entwicklung des Internets und teilt seine Erkenntnisse oder Bedenken mit. Soll beispielsweise innerhalb der IETF eine neue Arbeitsgruppe gegründet werden, so prüft das IAB deren Charta. Das IAB überwacht außerdem den Standardisierungsprozess.
- Das IAB unterstützt und organisiert die Internet Research Task Force und lädt zu Arbeitstreffen (IAB Workshops) ein, die bestimmte architekturelle Themen des Internets detaillierter behandeln. Die Ergebnisse des Workshops werden der IETF zugänglich gemacht und meistens als RCF veröffentlicht. Das IAB äußert seine Empfehlungen der IETF und der IESG gegenüber. Das IAB hat darüber hinaus noch folgende Aufgaben:
- Genehmigt die IESG-Wahlen des NomCom
- Nimmt Beschwerden über IESG-Aktionen an und prüft diese
- Genehmigt die Ernennung der IANA
- Beaufsichtigt die Verbindungen zu anderen Standardisierungsgremien

Beziehung zwischen dem OSI-Modell und den TCP/IP-Schichten

ISO/OSI-Modell

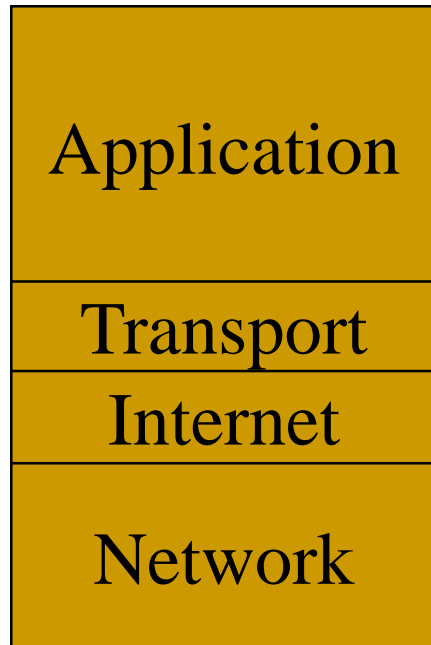
Application
Presentation
Session
Transport
Network
DataLink
Physical

TCP/IP-Schichten

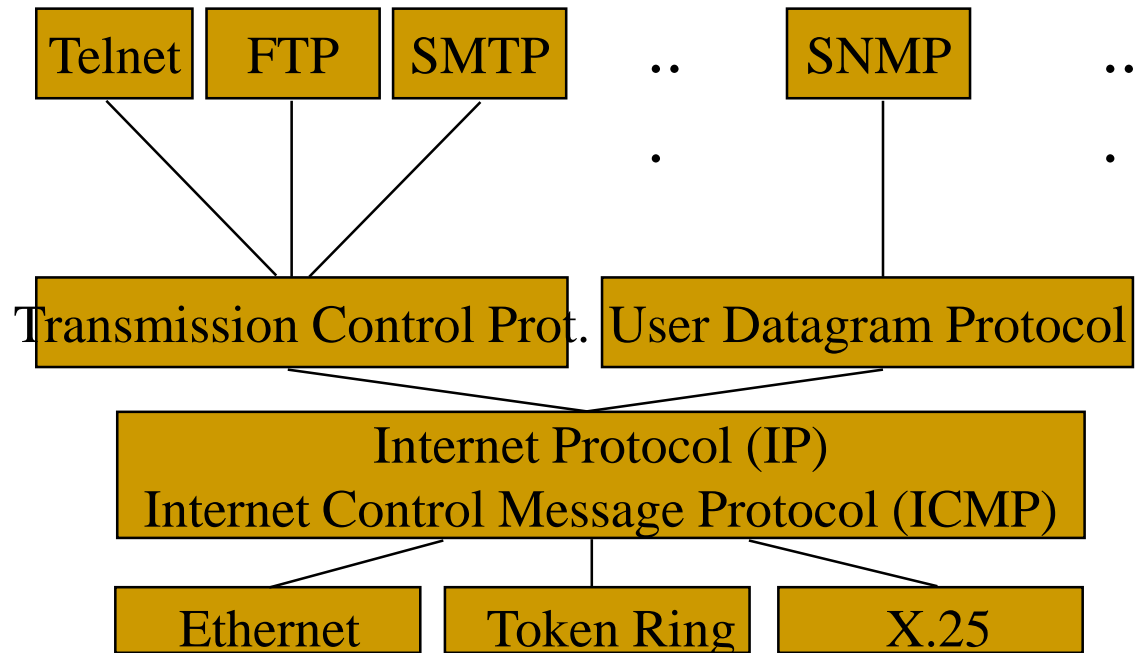
Application
Transport
Internet
Network

Beziehung zwischen den TCP/IP-Schichten und der TCP/IP-Protokollfamilie

TCP/IP-Schichten



TCP/IP-Protokolle



TCP / IP Adressen

- Die IP Adressen müssen global eindeutig sein. Die Vergabe wird durch die ICANN (Internet Corporation for Assigned Names and Numbers) vorgenommen.
- ICANN delegiert diese Verwaltung an „Regional Internet Registers (RIP). Jeder RIP erhält verschiedene Adressbereiche zugewiesen.
- Europa: RIPE, Asia-Pacific: APNIC, North America ARNI....
- Die PIR delegieren weiter an die Local Internet Registeries (LIR) oder National Internet Registeries (NIR).

Internet Netzwerkadressen

Klasse	Adressbereich	Anzahl Netze	Anzahl Hosts
A	1.0.0.0 – 127.255.255.255	127	16'777'214
B	128.0.0.0 – 191.255.255.255	16'384	65'534
C	192.0.0.0 – 223.255.255.255	2'097'152	254
D	224.0.0.0 – 239.255.255.555	Multicast Adressen	
E	240.0.0.0 – 247.255.255.255	Reserviert für zukünftige Nutzung	

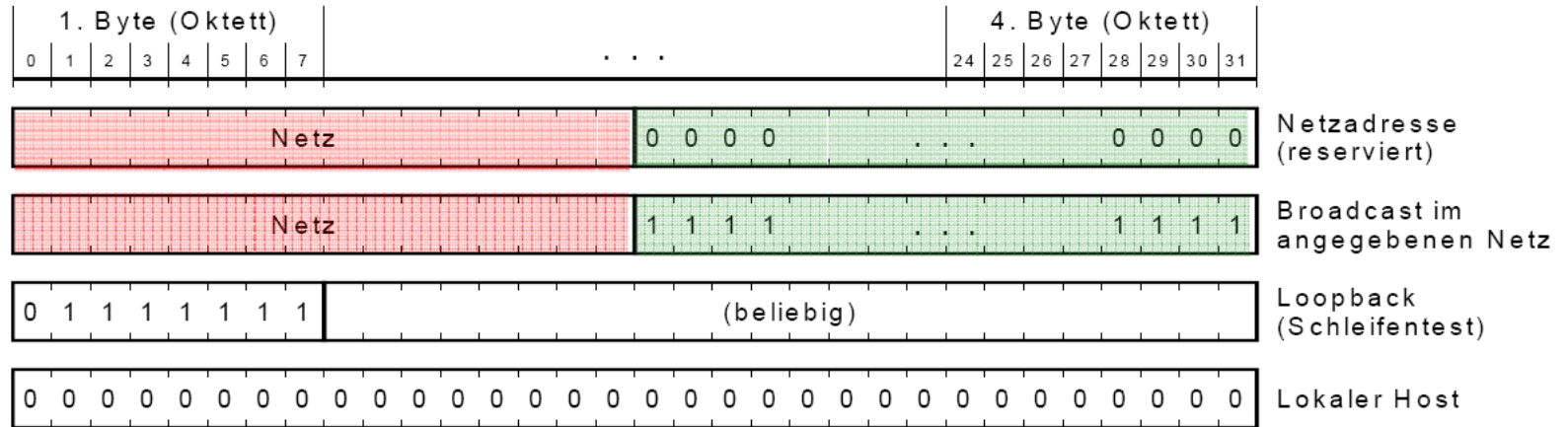
Gültige Netzwerk- und Hostadressen

- Die Netzwerk-Adresse darf nicht 127 lauten (Loopback- und Diagnose)
- Die Bits der Netzwerk- und Host-Adresse können nicht alle 1 betragen (Broadcast).
- Die Bits der Netzwerk- und Host-Adresse können nicht alle 0 betragen (Dieses Netz).
- Die Host-Adresse muss innerhalb des lokalen Netzwerk eindeutig sein.

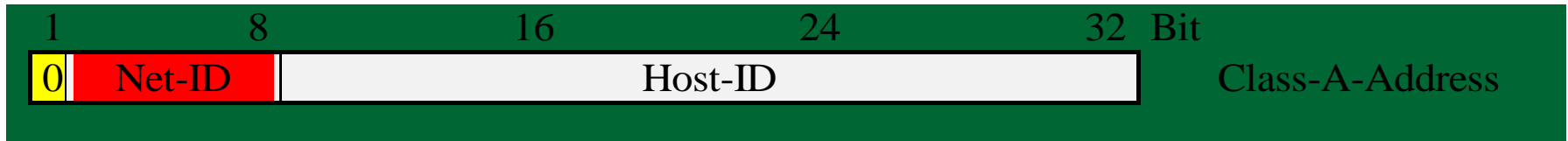
Private Netze

Klasse	Netzadresse	Subnetzmask
A	10.0.0.0	255.0.0.0
B	172.16.0.0 – 172.31.0.0	255.255.0.0
C	192.168.0.0 – 192.168.255.0	255.255.255.0

Reservierte Adressen



Internet - Adressformate



- Class-A-Adresse:

7 Bits werden hier für die Netzwerknummer und 24 Bits für die lokale Nummer (Host-Nummer) reserviert (erstes Bit zwingend '0'). Class-A-Adressen werden verwendet für sehr grosse Netzwerke mit bis zu 16 Millionen Rechner, es sind jedoch nur 128 Class-A-Netzwerke möglich (Netzwerkskennung (netid): 0-127)!

Format: $0NNN'NNNN'HHHH'HHHH'HHHH'HHHH'HHHH'HHHH_2$

oder Dezimal: $N.H.H.H_{10}$

(N = Netzwerkadresse, H = Hostadresse)

Beispiel: $0000'1100'0000'0000'0000'0011'1111'0001_2$

$0C'00'03'F1_H$

12.0.3.241 (Netz-ID 12, Host-ID 0.3.241; übliche Darstellung)

Internet - Adressformate (2)



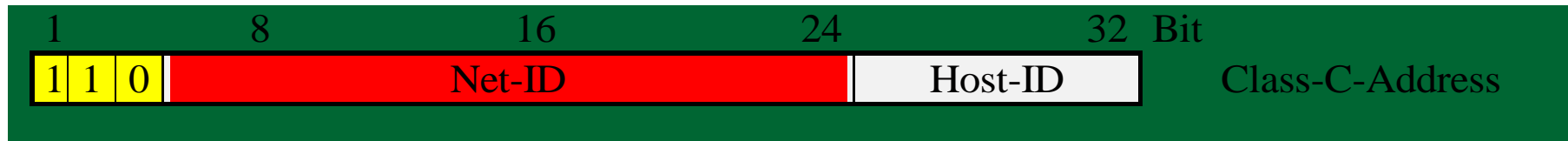
- Class-B-Adresse:

Hier werden 14 Bits für die Netzwerknummer und 16 Bits für die lokale Nummer reserviert (ersten beiden Bits zwingend '10'). Somit können 16'384 Class-B-Netzwerke mit jeweils 65'536 Knoten kreiert werden (Netzwerkskennung (netid): 128.0 bis 191.255).

Format: $10NN'NNNN'NNNN'NNNN'HHHH'HHHH'HHHH'HHHH_2$
 $N.N.H.H_{10}$

Beispiel: $1000'1100'0000'0000'0000'0011'1111'0001_2$
 $8C'00'03'F1_H$
140.0.3.241 (Netz-ID 140.0, Host-ID 3.241)

Internet - Adressformate (3)



- Class-C-Adresse:

Bei 21 Bits für die Netzwerknnummer und nur 8 Bits für lokale Adressen (ersten drei Bits zwingend '110') können ca. 2 Millionen Netze mit jeweils maximal 256 Knoten definiert werden (Netzwerkskennung (netid): 192.0.0 bis 223.255.255).

Format: $110N'NNNN'NNNN'NNNN'NNNN'NNNN'HHHH'HHHH_2$
 $N.N.N.H_{10}$

Beispiel: $1100'1100'0000'0000'0000'0011'1111'0001_2$
 $CC'00'03'F1_H$
 $204.0.3.241$ (Netz-ID 204.0.3, Host-ID 241)

Subnet-Maske für B-Adresse

B-Adresse
140.0.3.241

1100'1100'0000'0000'0000'0011'1111'0001

B-Adr-Maske
255.255.0.0

1111'1111'1111'1111'0000'0000'0000'0000

B-Class-Netzadr.
140.0

1100'1100'0000'0000

Durch die B-Adress-Maske wurde die Node-Id '3.241' vom Rest der IP-Adresse abgetrennt.

Subnet-Maske für C-Adresse

C-Adresse
204.0.3.241

1100'1100'0000'0000'0000'0011'1111'0001

C-Adr-Maske
255.255.255.0

1111'1111'1111'1111'1111'1111'0000'0000

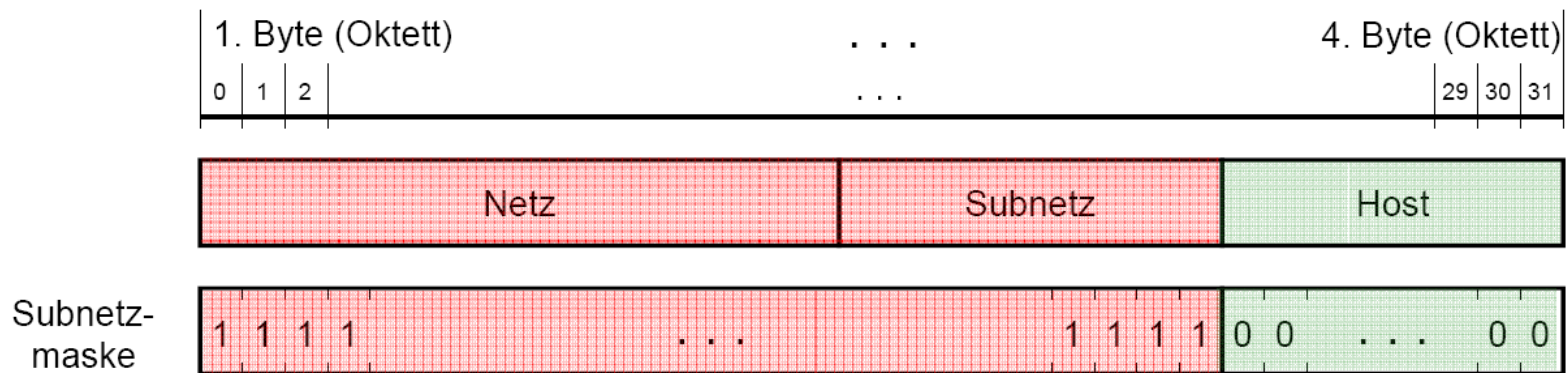
C-Class-Netzadr.
204.0.3

1100'1100'0000'0000'0000'0011

Durch die C-Adress-Maske wurde die Node-Id '241' vom Rest der IP-Adresse abgetrennt.

Subnetting

Aufteilen eines grossen Netzes in kleinere Teilnetze



Sunnetting

Die Absteckung des vom Subnetz erfassten Bereichs erfolgt durch bitweise Maskierung eines bestimmten Teils der IP-Adresse durch die Subnetzmaske. Dadurch erhält man aus einer beliebigen Adresse das Subnetz, zu dem die Adresse unter Annahme dieser Maske gehört.

Berechnung der Subnetze für Klasse C Netzwerke

Netzwerk: 192. 168. 210. 0

Netzwerk (Binär): 11000000.10101000.1010010.00000000

Subnetmask: 255. 255. 255. 0

Subnetmask (Binär): 11111111.11111111.11111111.00000000

Benötigte Subnetze: 4

Formel: $(2^n) - 2 = \text{Subnetze}$

Um vier Subnetze zu erzeugen müssen 3 Bit der Subnetmask (des Hostanteils) gestohlen werden.

$$(2^3) - 2 = 6$$

Somit werden die ersten drei Nullstellen des Hostanteils der Subnetmask auf 1 gestellt. (11111111.11111111.11111111.11100000)

Diese werden von Binär in Dezimal umgerechnet:

$$128 + 64 + 32 = 224$$

Somit lautet die neue Subnetmask: 255. 255. 255. 224

Subnetmask (Binär): 11111111.11111111.11111111.11100000

Nun zur Berechnung der Subnetze

128 64 32 = Subnetze

0 0 0 = 192.168.210.0

0 0 1 = 192.168.210.32

0 1 0 = 192.168.210.64

0 1 1 = 192.168.210.96

1 0 0 = 192.168.210.128

1 0 1 = 192.168.210.160

1 1 0 = 192.168.210.192

1 1 1 = 192.168.210.224

Hier werden die auf 1 stehenden Werte addiert um die letzte Stelle der IP-Adresse festzulegen. Die hier stehenden IP-Adressen sind die Netzwerkadressen.

Netzwerkadresse: 192.168.210.64

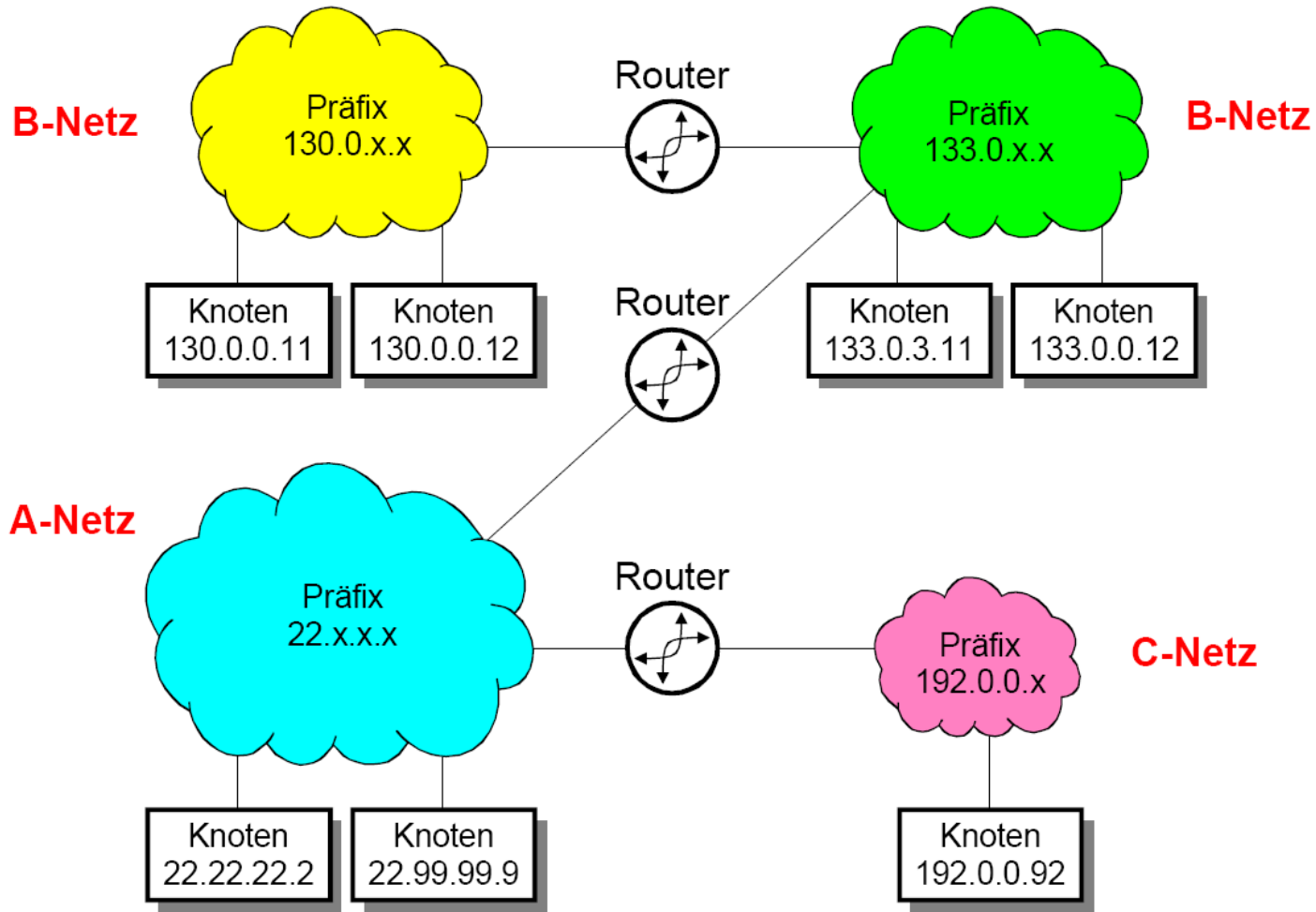
IP-Adressen: 192.168.210.65 ? 192.168.210.94

Broadcast: 192.168.210.95

Subnetmask: 255.255.255.224

Bitte auch wieder Beachten das, das Erste und Letzte Subnetz weg gestrichen werden. Somit erhalten wir 6 Subnetze.

Netzstruktur



Routing

Das Routing ist ein Vorgang, der den Weg zur nächsten Station eines Datenpakets bestimmt. Im Vordergrund steht die Wahl der Route aus den verfügbaren Routen, die in einer Routing-Tabelle gespeichert sind.

Parameter und Kriterien für Routing

Verschiedene Parameter und Kriterien können für die Wahl einer Route von Bedeutung sein:

- Verbindungskosten
- notwendige Bandbreite
- Ziel-Adresse
- Subnetz
- Verbindungsart
- Verbindungsinformationen
- bekannte Netzwerkadressen

Warum ist Routing notwendig

Vermeidung von Kollisionen und Broadcasts durch Begrenzung der Kollisions- und Broadcastdomäne

Bei der Wegfindung von Sender- zu Empfänger-Station werden häufig rundspruchbasierte Protokolle eingesetzt. Zum einen NetBIOS in Microsoft-basierten Netzwerken und ARP des TCP/IP-Stacks. Die Protokolle schicken immer wieder Broadcasts raus, um den Weg zu einer unbekannten Station zu finden. Broadcasts belasten ein Netzwerk. Router verhindern die Weiterleitung von Broadcasts, sofern sie selber nicht auf deren Verwendung angewiesen sind. Router vermindern die Belastung des Netzwerkes durch Broadcasts.

Routing über unterschiedliche Netzarchitekturen und Übertragungssysteme

Netzwerkverkabelungen sind in der Regel strukturiert angelegt. Man unterscheidet in der Primär-, Sekundär- und Tertiär-Verkabelung, die unterschiedliche Architekturen und Übertragungstechniken verwenden (Ethernet, Token Ring, FDDI, ATM, ISDN, WLAN, etc.). Ein Router kann in der Lage sein zwischen unterschiedlichen Architekturen zu vermitteln. Dazu gehört auch die Fragmentierung der Datenpakete.

Paket-Filter durch eine Firewall

Sicherheitsaspekte gehen auch an Routern nicht vorbei. Ungewünschter oder unsicherer Datenverkehr kann anhand von IP-Adressen oder TCP- und UDP-Ports gefiltert und unterbunden werden. Häufig kommen spezielle Firewall-Router oder Router mit Firewall-Funktionen zum Einsatz.

Routing über Backup-Verbindungen bei Netzausfall

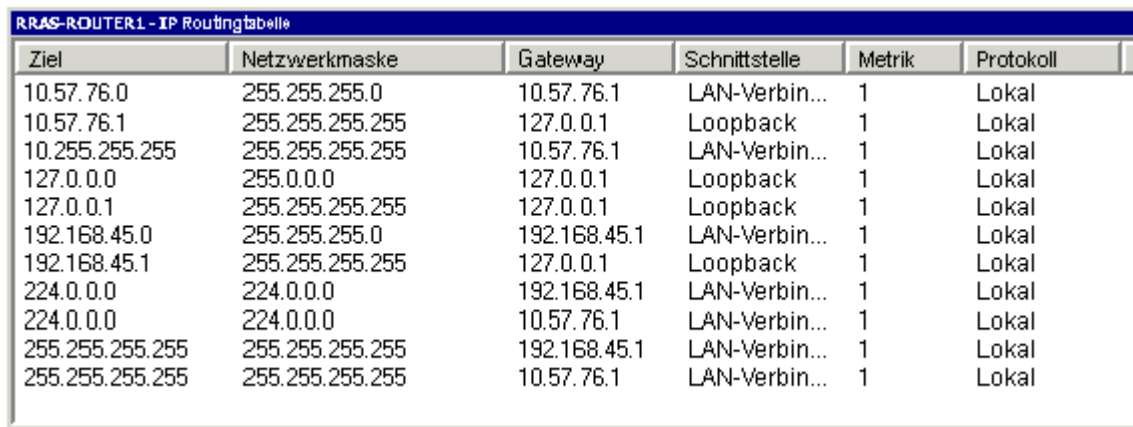
Durch den Einsatz von Routern entsteht häufig ein engmaschiges Netz, dass dem Datenpaket zum Ziel mehrere Wege zum Ziel bietet. Fällt ein Router aus, verständigen sich die Router untereinander und die Datenpakete nehmen einfach einen anderen Weg zu ihrem Ziel. Fällt eine Leitung zwischen zwei Routern aus, können diese z. B. eine Backup-Verbindung herstellen. Zum Beispiel eine Wählverbindung über das Telefonnetz.

In großen und modernen Netzwerken spielt die Fehlererkennung und -behandlung eine große Rolle. Router können den Netzwerkverkehr protokollieren und über SNMP Meldungen an eine Netzwerk-Management-Station senden oder Befehle des Netzwerk-Administrators ausführen.

Grundlegendes zu IP-Routingtabellen

Bei der Behandlung von Routingproblemen ist das Verständnis der Routingtabelle unerlässlich. Auf jedem Computer, auf dem TCP/IP ausgeführt wird, werden anhand der IP-Routingtabelle Routingentscheidungen getroffen.

In der folgenden Abbildung wird ein Beispiel für eine Routingtabelle dargestellt.
Die IP-Routingtabelle enthält Informationen in den folgenden Spalten:



Ziel	Netzwerkmaske	Gateway	Schnittstelle	Metrik	Protokoll
10.57.76.0	255.255.255.0	10.57.76.1	LAN-Verbin...	1	Lokal
10.57.76.1	255.255.255.255	127.0.0.1	Loopback	1	Lokal
10.255.255.255	255.255.255.255	10.57.76.1	LAN-Verbin...	1	Lokal
127.0.0.0	255.0.0.0	127.0.0.1	Loopback	1	Lokal
127.0.0.1	255.255.255.255	127.0.0.1	Loopback	1	Lokal
192.168.45.0	255.255.255.0	192.168.45.1	LAN-Verbin...	1	Lokal
192.168.45.1	255.255.255.255	127.0.0.1	Loopback	1	Lokal
224.0.0.0	224.0.0.0	192.168.45.1	LAN-Verbin...	1	Lokal
224.0.0.0	224.0.0.0	10.57.76.1	LAN-Verbin...	1	Lokal
255.255.255.255	255.255.255.255	192.168.45.1	LAN-Verbin...	1	Lokal
255.255.255.255	255.255.255.255	10.57.76.1	LAN-Verbin...	1	Lokal

Routing

Ziel

Das Ziel ist ein Zielhost, eine Subnetzadresse, eine Netzwerkadresse oder die Standardroute. Das Ziel der Standardroute ist 0.0.0.0.

Netzwerkmaske

Die Netzwerkmaske wird zusammen mit dem Ziel verwendet, um zu ermitteln, wann eine bestimmte Route verwendet werden soll. Hostrouten besitzen die Maske 255.255.255.255, die Standardroute besitzt die Maske 0.0.0.0, und Subnetz- bzw. Netzwerkrouen besitzen Masken zwischen diesen beiden Extremwerten.

Die Maske 255.255.255.255 bedeutet, dass die Route nur bei genauer Übereinstimmung des Zieles verwendet wird. Die Maske 0.0.0.0 bedeutet, dass die Route für beliebige Ziele verwendet wird. Wenn die Maske in binärer Schreibweise ausgedrückt wird, ist eine **1** signifikant (muss übereinstimmen), und eine **0** ist nicht signifikant (muss nicht übereinstimmen).

So verfügt z. B. das Ziel 172.16.8.0 über eine Netzwerkmaske 255.255.248.0. Diese Netzwerkmaske bedeutet, dass die ersten beiden Oktette genau übereinstimmen müssen, die ersten 5 Bit des dritten Oktetts übereinstimmen müssen (248 = 1111000) und das letzte Oktett nicht von Bedeutung ist. Das dritte Oktett von 172.16.8.0 (also 8) entspricht **00001**000 in binärer Schreibweise. Ohne die ersten 5 Bit (der **fett** dargestellte maskierte Teil) zu ändern, kann bis 15 hochgezählt werden (dies entspricht **00001**111 in binärer Schreibweise). Eine Route mit dem Ziel 172.16.8.0 und der Maske 255.255.248.0 gilt also für alle Datenpakete mit den Zielen 172.16.**8**.0 bis 172.16.**15**.255.

Routing

Gateway

Das Gateway ist die IP-Adresse des nächsten Routers, an den Datenpakete übermittelt werden müssen. Bei LAN-Verbindungen (z. B. Ethernet oder Token Ring) muss das Gateway von diesem Router unter Verwendung der in der Spalte **Schnittstelle** angegebenen Schnittstelle direkt erreichbar sein. Bei LAN-Verbindungen bestimmen sowohl das Gateway als auch die Schnittstelle, wie der Router den Datenverkehr weiterleitet. Bei Schnittstellen für Wählen bei Bedarf kann keine Gatewayadresse eingestellt werden. Bei Punkt-zu-Punkt-Verbindungen bestimmt die Schnittstelle, wie der Router den Datenverkehr weiterleitet.

Schnittstelle

Die Schnittstelle gibt die LAN-Schnittstelle oder die Schnittstelle für Wählen bei Bedarf an, die zum Erreichen des nächsten Routers verwendet werden soll.

Metrik

Die Metrik stellt die relativen Kosten dar, die bei der Verwendung dieser Route zum Erreichen des Zieles anfallen. In der Regel wird dies in Abschnitten (Hops) ausgedrückt, die Anzahl der Router, die bis zum Ziel durchlaufen werden müssen. Wenn mehrere Routen mit demselben Ziel vorliegen, gilt die Route mit der niedrigsten Anzahl als die beste Route.

Protokoll

Das Protokoll zeigt an, wie die Route ausfindig gemacht wurde. Wenn in der Spalte **Protokoll** der Eintrag **RIP**, **OSPF** oder ein beliebiger Eintrag außer **Lokal** angezeigt wird, empfängt der Router Routen. OSPF (Open Shortest Path First) ist für Windows XP 64-Bit Edition (Itanium) und die 64-Bit-Versionen der Windows Server 2003-Produktfamilie nicht verfügbar.

Routenwahl Methoden

Der Aufbau einer Routing-Tabelle entscheidet, welche Routenwahlmethode verwendet wird. Diese Methode ist ein Algorithmus, der die Einträge in der Routing-Tabelle benutzt um die Route zu berechnen. Die häufigsten Routenwahlmethoden sind der Distance-Vector-Algorithmus (DVA) und der Link-Status-Algorithmus (LSA).

LSA - Link-Status-Algorithmus

Der LSA bestimmt die Route anhand dem Status der Verbindungen, also deren Verfügbarkeit und Geschwindigkeit. Ein spezieller Sortieralgorithmus ermittelt dann z. B. den kürzesten Weg (Shortest Path) zum Ziel.

Beim Link-Status-Routing (LSR) werden die Änderungen in der Routing-Tabelle per Multicast zwischen den Routern ausgetauscht. In der Routing-Tabelle ist deshalb die gesamte Netzstruktur abgebildet. Der Router kennt deshalb jede erdenkliche Route.

Protokolle nach LSA werden als externe oder exterior Routing Protokolle bezeichnet, die netzübergreifend genutzt werden.

DVA - Distance-Vector-Algorithmus

Jede Route wird anhand einiger Kriterien klassifiziert. Aus allen Routen wird dann die mit den optimalen Voraussetzungen gewählt. Besonders bei weit entfernten Zielen mit vielen Routen, lässt sich so die optimale Route ermitteln.

Beim Distance-Vector-Routing (DVR) werden die Routing-Tabellen mit dem direkten Nachbar-Router ausgetauscht. Die Routing-Tabelle wird in periodischen Abständen ausgetauscht. Das führt zu zusätzlichem Datenverkehr zwischen den Routern.

DVR-Protokolle werden als interne oder interior Routing Protokolle bezeichnet, die in lokalen Netzen genutzt werden.

Routing Protocol

Routing-Protokolle für dynamisches Routing

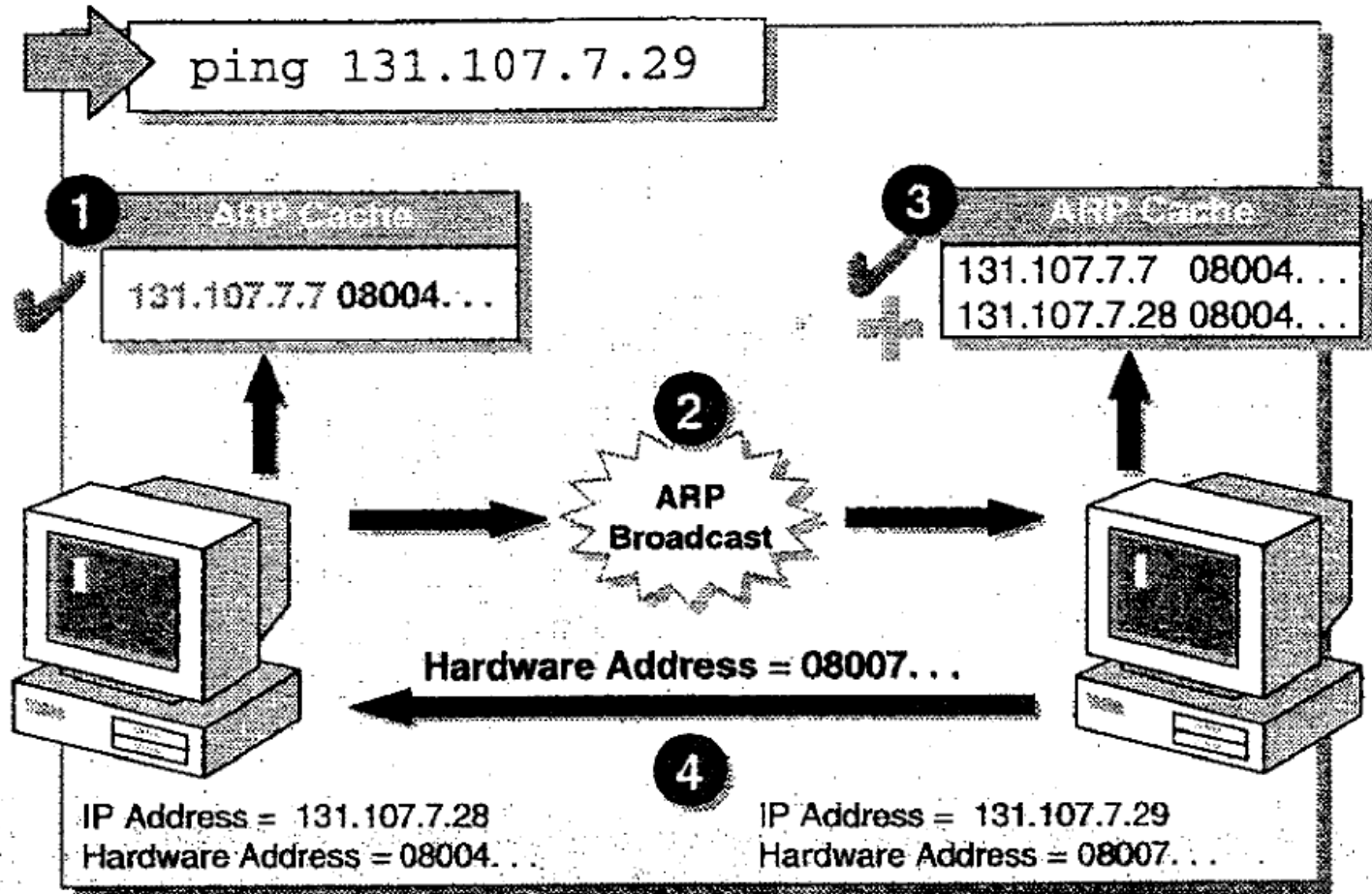
BGP - Border Gateway Protocol
EGP - Exterior Gateway Protocol
IGP - Interior Gateway Protocol
OSPF - Open Shortest Path First
RIP - Routing Information Protocol
DRP - DECnet Routing Protocol
IGRP - Interior Gateway Routing Protocol
EIGRP - Enhanced Interior Gateway Routing Protocol

RIP - Routing Information Protocol

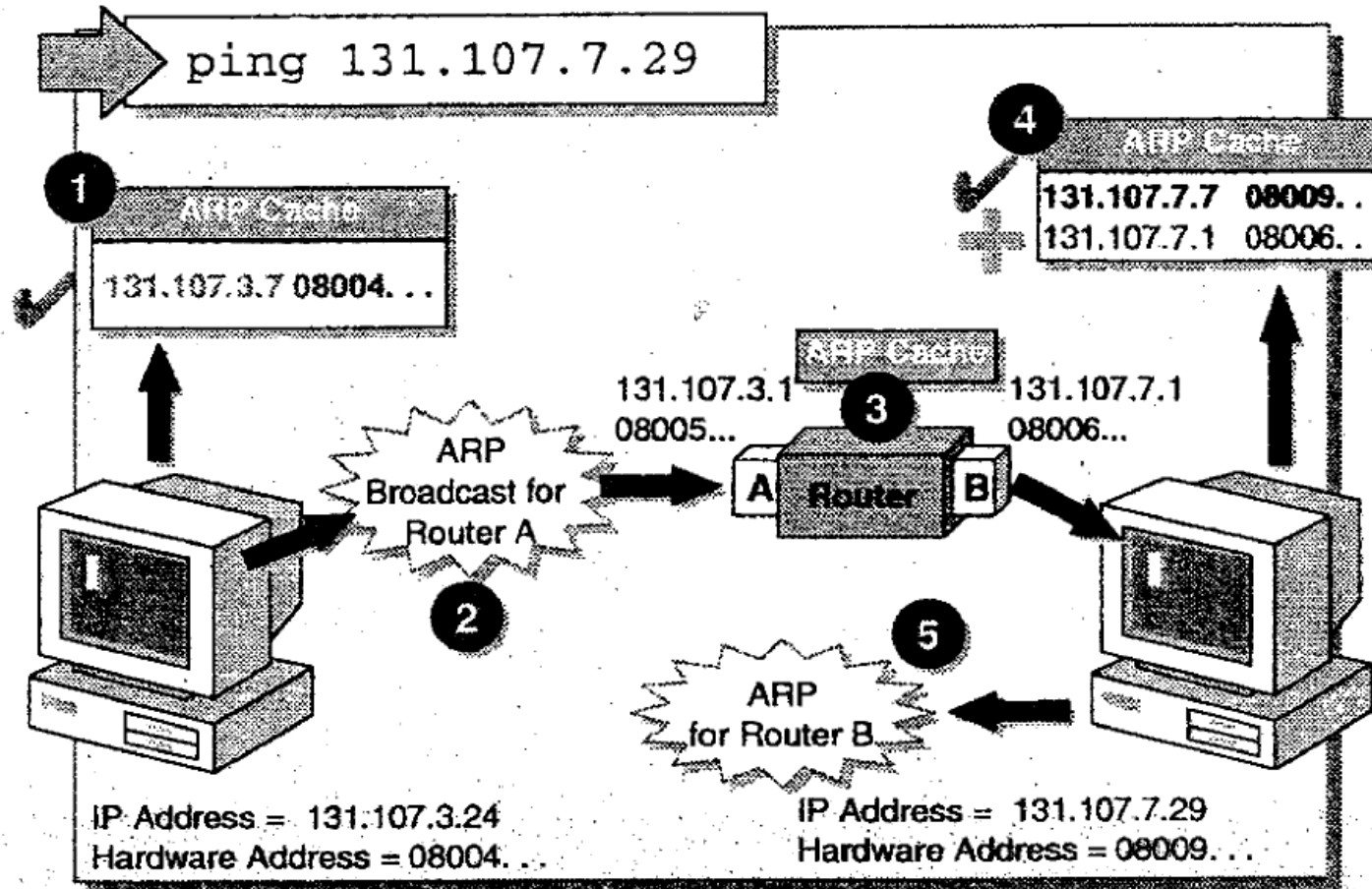
Das RIP ist ein Distance-Vector-Algorithmus, also ein Distance-Vector-Routing-Protokoll. Es ist das einfachste und meist genutzte Routing-Protokoll. Die Fähigkeiten moderner Netze werden von RIP allerdings nicht berücksichtigt. Im einfachsten Fall speichert RIP in seiner Routing-Tabelle neben Netzwerkadresse und abgehende Schnittstelle nur die Anzahl der Stationen (Hops) die ein Datenpaket bis zum Zielnetz überwinden muss. Ein Hop-Eintrag von 16 gilt als unendlich und bedeutet, dass dieses Netz nicht erreichbar ist. Deshalb ist RIP in Netzwerken mit mehr als 15 Zwischenstationen nicht geeignet. Es wird daher auch nur in lokalen Netzwerken eingesetzt, wo die Netzübergänge (Router) von gleicher Qualität sind und die Netzwerkstruktur nur selten verändert wird.

Die Routing-Tabellen werden von den Routern alle 30 Sekunden mit dem benachbarten Router ausgetauscht. Dies führt zu einem erhöhten Datenverkehr zwischen den Routern. Fällt ein Router aus, kann es mehrere Minuten dauern, bis diese Information und die entsprechend geänderte Routing-Tabelle übermittelt wurden.

ARP lokal



ARP Remonte



Portnummer

- Die Portnummer ist eine mehrstellige Ziffer, mit der Dienste eines Rechners gekennzeichnet werden. Erreicht ein Datenpaket einen Zielrechner, dann vermittelt dieser es an das entsprechende Programm. Aus diesem Grund ist in den Protokoll-Headern ein Datenfeld für die Portnummer.
- <http://www.iana.org/assignments/port-numbers>

Portnummer

Portnummer	Protokoll
20	FTP (Daten)
21	FTP (Befehle)
22	Secure Shell
23	Telnet
25	SMTP
53	DNS-Server
79	Finger
80	HTTP (Proxy-Server)
110	POP3
119	NNTP
143	IMAP
194	IRC
210	WAIS
256 - 1023	UNIX-spezifische Services
540	UUCP
1024 - 49151	Registered Ports
49152 - 65535	Dynamic / Private Ports

ausgewählte Ports:

Filesharing-Protokolle

<input type="checkbox"/> KaZaA	1214
<input type="checkbox"/> eDonkey	4661 bis 4665
<input type="checkbox"/> Gnutella	6346, 6347
<input type="checkbox"/> Napster	6699

SNMP-Abfragen 161,162

Netbios 139

Simple Mail Transfer 25

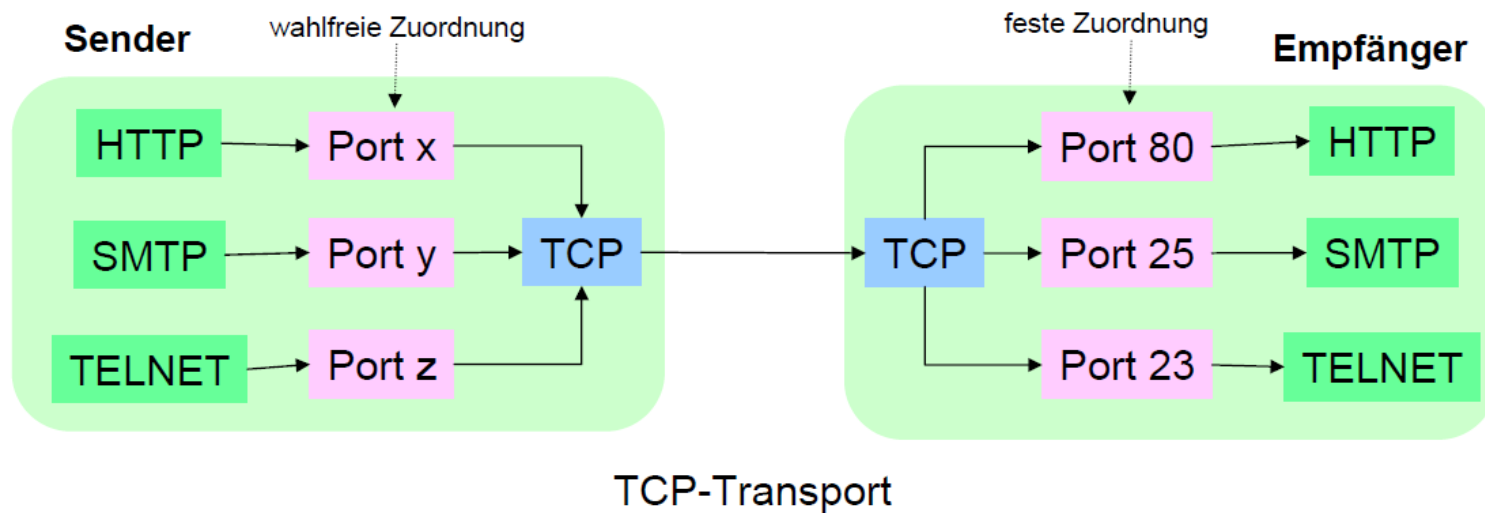
z.Z am WiN-Zugang des MWN gesperrt

Liste der Port-Nummern

<http://www.iana.org/assignments/port-numbers>

Portnummer

● TCP-Ports



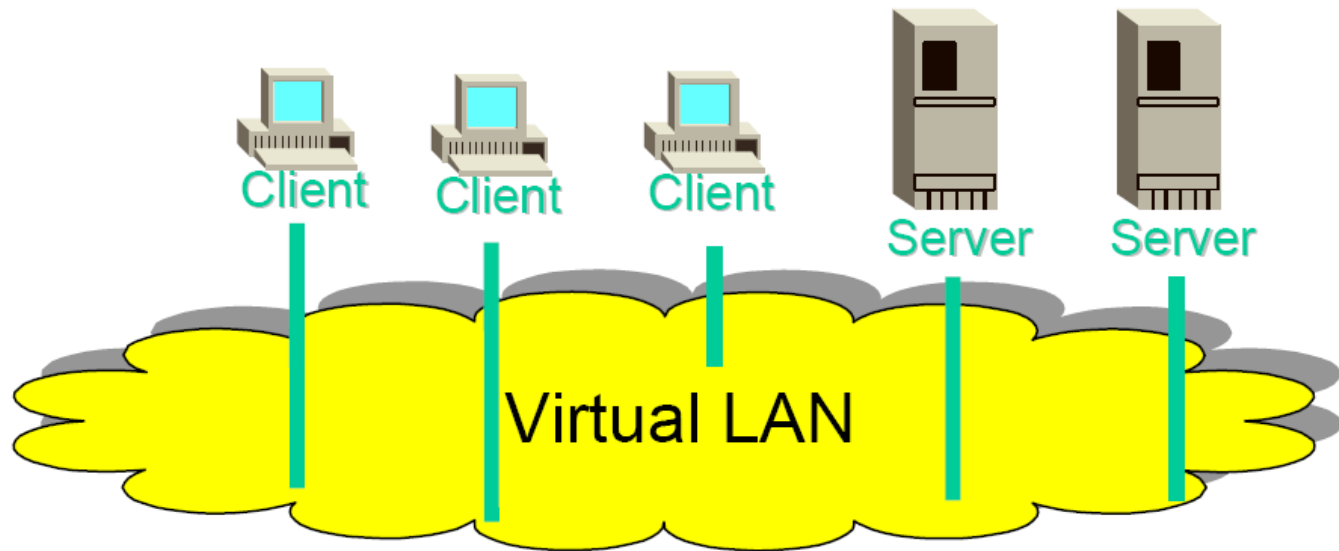
Portnummer

● TCP-Ports

- TCP-Verbindung kann über Socket-Nummern
 - (IP-Adresse + Portnummer)
- auf Sender und Empfängerseite eindeutig identifiziert werden
- **Empfänger assoziiert über die angegebene Portnummer die zugehörige Anwendung**, mit der kommuniziert werden soll
- Empfänger überwacht ständig alle Ports auf eingehende Verbindungen
- Offene Ports stellen oft ein **Sicherheitsrisiko** dar
 - können gesperrt werden

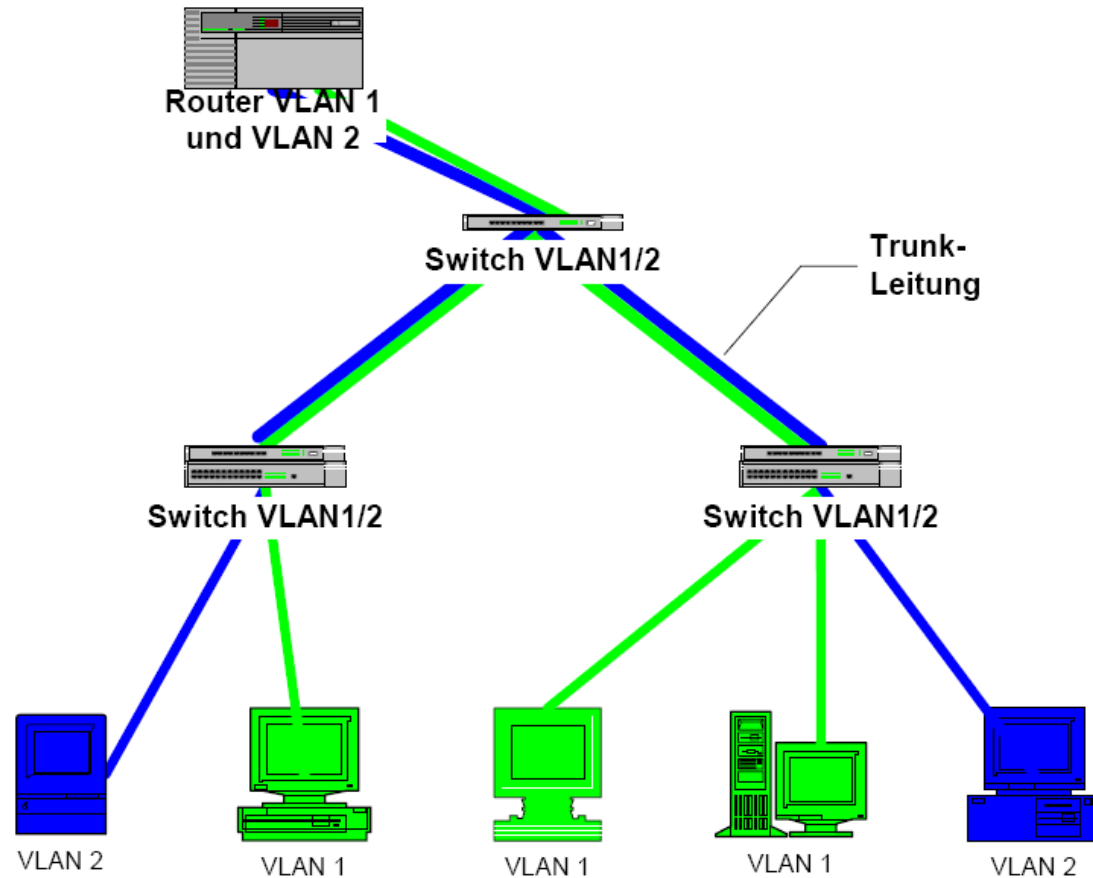
VLAN

- ❑ Orts- / Topologie-unabhängige Zusammenfassung von Rechnern, die miteinander kommunizieren, wie wenn sie sich auf einem gemeinsamen, physischen LAN befänden



- ❑ ein VLAN = eine Broadcast-Domain, ein “klassisches LAN”
- ❑ zwischen Geräten in einem VLAN wird geswitched
- ❑ zwischen verschiedenen VLANs wird geroutet

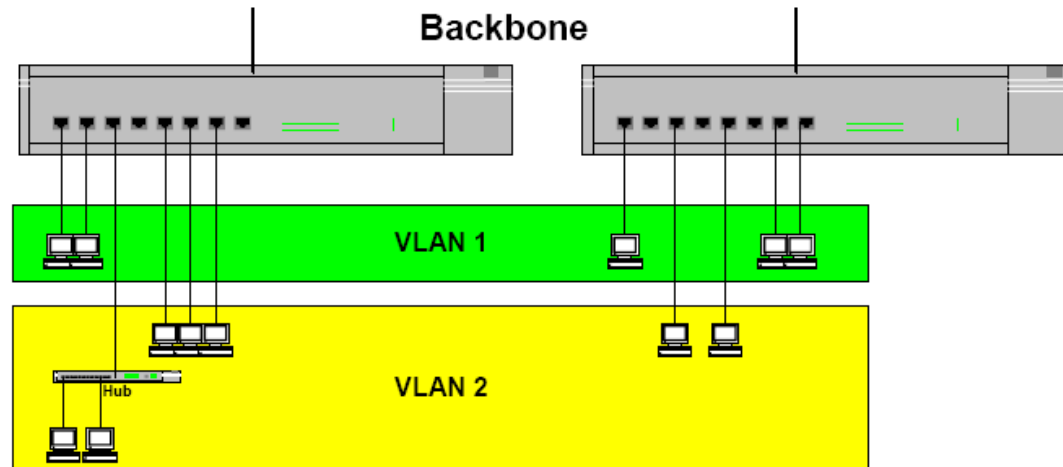
VLAN



VLAN

- ☐ weniger Komponenten notwendig
- ☐ keine parallelen physischen Infrastrukturen notwendig, wenn mehrere Institutionen / Arbeitsgruppen im gleichen Gebäude
- ☐ Segmentierung, kleinere Collisionsdomänen
- ☐ verteilte Arbeitsgruppen
- ☐ Sicherheit, Zugriffskontrolle (Firewalls)

VLAN



- ☐ Für jeden Switch-Port wird festgelegt, in welches VLAN die angeschlossenen Geräte gehören
- ☐ Switch wird aufgeteilt in mehrere Netze
- ☐ entspricht weitgehend herkömmlichen Installationen
- ☐ Hubs können problemlos eingesetzt werden
- ☐ Standard 802.1Q (Kennzeichnung der Pakete mit sog. Tag`s (12 Bit VLAN))
- ☐ Hoher Konfigurations- und Dokumentationsaufwand
- ☐ schwierige Fehlersuche

DHCP Dynamic Host Configuration Protocol

DHCP ist ein Protokoll, um IP-Adressen in einem TCP/IP-Netzwerk zu verwalten und an die Stationen zu verteilen. Mit DHCP ist jede Netzwerk-Station in der Lage sich selber vollautomatisch zu konfigurieren.

Warum DHCP?

Um ein Netzwerk per TCP/IP aufzubauen ist es notwendig jede einzelne Station zu konfigurieren. Für ein TCP/IP-Netzwerk müssen folgende Einstellungen bei jeder Station vorgenommen werden:

- Vergabe einer eindeutigen IP-Adresse
- Zuweisen einer Subnetzmaske (Subnetmask)
- Zuweisen des Default- bzw. Standard-Gateways
- DNS-Serveradressen

In den ersten IP-Netzen wurden IP-Adressen noch von Hand vergeben und fest in die Systeme eingetragen. Die dazu erforderliche Dokumentation war jedoch nicht immer fehlerfrei und schon gar nicht aktuell und vollständig. Der Ruf nach einer einfachen und automatischen Adressverwaltung wurde deshalb besonders bei Betreibern großer Netze lauter. Hier war sehr viel Planungs- und Arbeitszeit notwendig. Um dem zu entgehen, wurde DHCP entwickelt.

Mit DHCP kann jede Netzwerk-Station die Adresskonfiguration von einem DHCP-Server anfordern und sich selber automatisch konfigurieren. So müssen IP-Adressen nicht mehr manuell verwaltet und zugewiesen werden.

DHCPv6

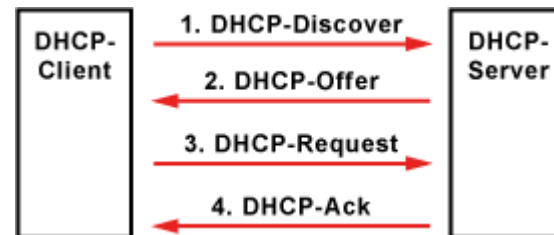
Bei IPv6 gibt es die Stateless Autoconfiguration. Doch diese berücksichtigt keine Informationen über Host-, Domainnamen und DNS. Diese Angaben und noch mehr können durch den Einsatz eines DHCPv6-Servers ergänzt werden. Dieser liefert die gewünschten Zusatzinformationen, kümmert sich dabei aber nicht um die Adressvergabe. Man spricht von Stateless DHCPv6.

DHCP Funktionsweise

DHCP ist eine Client-Server-Architektur. Der DHCP-Server verfügt über einen Pool von IP-Adressen, die er den DHCP-Clients zuteilen kann. Bei größeren Netzen muss der DHCP-Server zudem wissen, welche Subnetze und Standard-Gateway es gibt. In der Regel ist der DHCP-Server ein Router.

Wird eine Station gestartet und ist dort ein DHCP-Client aktiviert, wird ein in seiner Funktion eingeschränkter Modus des TCP/IP-Stacks gefahren. Dieser hat keine gültige IP-Adresse, keine Subnetzmaske und kein Standard-Gateway. Das einzige, was der Client machen kann, ist IP-Broadcasts verschicken. Der DHCP-Client verschickt ein UDP-Paket mit der Ziel-Adresse 255.255.255.255 und der Quell-Adresse 0.0.0.0. Dieser Broadcast dient als Adressanforderung an alle verfügbaren DHCP-Server. Im Optimalfall gibt es nur einen DHCP-Server. So vermeidet man Konflikte bei der Adressvergabe.

Der DHCP-Server antwortet auf den Broadcast mit einer freien IP-Adresse und weiteren Parametern. Danach wird die Datenübergabe bestätigt.



DHCP

Mit DHCP werden nicht nur die IP-Adressen verteilt. Bei der Gelegenheit werden weitere Parameter übergeben, um die IP-Konfiguration im Client zu vervollständigen. Jeder angesprochene DHCP-Server schickt ein UDP-Paket mit folgenden Daten zurück:

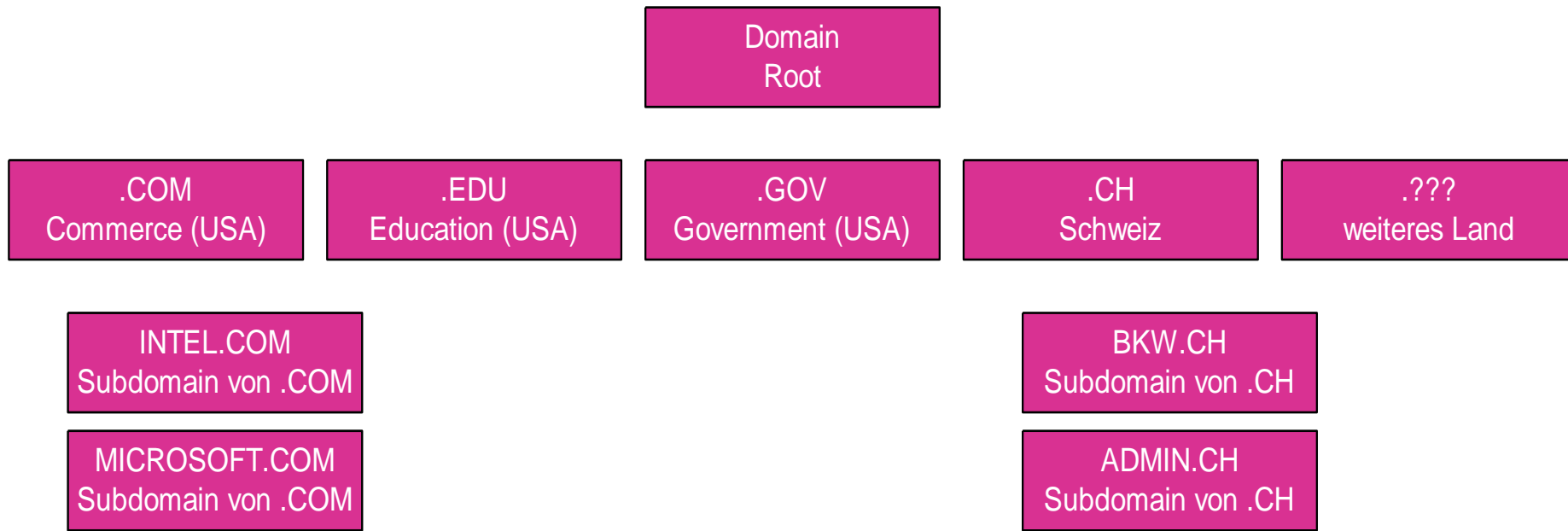
- MAC-Adresse des Clients
- mögliche IP-Adresse
- Laufzeit der IP-Adresse
- Subnetzmaske
- IP-Adresse des DHCP-Servers / Server-ID

Aus der Auswahl von evt. mehreren DHCP-Servern sucht sich der DHCP-Client eine IP-Adresse heraus. Daraufhin verschickt er eine positive Meldung an den betreffenden DHCP-Server. Alle anderen Server erhalten die Meldung ebenso und gehen von der Annahme der IP-Adresse zugunsten eines anderen Servers aus. Anschließend muss die Vergabe der IP-Adresse vom DHCP-Server bestätigt werden. Sobald der DHCP-Client die Bestätigung erhalten hat, speichert er die Daten lokal ab. Abschließend wird der TCP/IP-Stack vollständig gestartet.

Doch nicht nur die Daten zum TCP/IP-Netzwerk kann DHCP an den Client vergeben. Sofern der DHCP-Client weitere Angaben auswerten kann, übermittelt der DHCP-Server weitere Optionen:

- Time Server
- Name Server
- Domain Name Server (Alternative)
- WINS-Server
- Domain Name
- Default IP TTL
- Broadcast Address
- SMTP Server
- POP3 Server

Internet Domain Name Struktur



- Die Domain Name Struktur ist streng hierarchisch aufgebaut
- In den USA gibt es die Bereiche COM, EDU, GOV und MIL (Militär)
- Normalerweise kennzeichnet die Master-Domain das jeweilige Land (.CH)
- Für die Domain Name Vergabe gibt es nationale Clearing-Stellen (SWITCH)

Geografische Top-Level-Domains (TLD)

Domain (ccTLD)	Land
.at	Österreich
.au	Australien
.cc	Kokos-Inseln
.ch	Schweiz
.de	Deutschland
.fr	Frankreich
.gb	Großbritannien
.ie	Irland
.it	Italien
.li	Lichtenstein
.nl	Niederlande
.no	Norwegen
.ru	Russland
.to	Tonga
.uk	Vereinigtes Königreich
...	

Organisatorische Top-Level-Domains (TLD)

Domain (gTLD)	Organisationsform
.aero	Lufttransportindustrie
.arpa	Alte Arpanet Domäne
.biz	Business, für große und kleinere Unternehmen
.com	Kommerzielle Domain
.coop	Kooperationen, Genossenschaften
.edu	Schulen, Universitäten, Bildungseinrichtungen
.gov	Regierungsstellen der Vereinigten Staaten von Amerika
.info	Informationsdienste
.int	International tätige Institutionen
.mil	Militär der Vereinigten Staaten von Amerika
.museum	Museen
.name	Privatpersonen
.net	Netzspezifische Dienste und Angebote
.org	Nichtkommerzielle Unternehmungen und Projekte
.pro	Professionals, spezielle Berufsgruppen
...	

DNS Server

Ein DNS-Server tritt niemals alleine auf. Es gibt immer einen Primary und einen Secondary Nameserver. Sie sind voneinander unabhängig und redundant ausgelegt, so dass mindestens immer ein Server verfügbar ist. Der Secondary Nameserver gleicht in regelmäßigen Abständen seine Daten mit dem Primary Nameserver ab und dient so als Backup-Server.

Damit nicht bei jeder DNS-Anfrage das Netzwerk belastet werden muss, hat jeder DNS-Server einen Cache, in dem er erfolgreiche DNS-Anfragen speichert. Bei wiederholtem Aufruf holt er bereits erfolgreich aufgelöste Domain-Namen aus dem Cache. Die gespeicherten Daten haben eine Lebensdauer (Time-To-Live, TTL) von ca. 2 Tagen. Wird eine IP-Adresse durch den Umzug eines Domain-Namens geändert, ist die Domain nach spätestens 2 Tagen wieder im ganzen Internet erreichbar.

Neben den ganz normalen DNS-Servern gibt es auch die Root-Server, von denen es weltweit nur 13 Stück gibt. 10 davon stehen in den USA. Die 3 anderen befinden sich in London, Stockholm und Tokio.

Resolver / DNS-Client

Der DNS-Client (Resolver) ist direkt in TCP/IP integriert und steht dort als Software-Bibliothek für die DNS-Namensauflösung zur Verfügung. Der DNS-Client wird als Resolver bezeichnet und ist der Mittler zwischen DNS und dem Anwendungsprogramm. Der Resolver wird mit den Funktionen "gethostbyname" und "gethostbyaddr" angesprochen. Er liefert die IP-Adresse eines Domain-Namens bzw. dem Haupt-Domain-Namen einer IP-Adresse zurück.

Damit der Resolver arbeiten kann benötigt er die IP-Adresse von einem, besser von zwei DNS-Server, die in den TCP/IP-Einstellungen eingetragen oder über DHCP angefordert werden müssen

Namesauflösung

Namensauflösung

Im TCP/IP-Netzwerk werden Stationen mit ihrer IP-Adresse angesprochen. Die IP-Adresse in binärer Form ist eine 32-Bit-Folge von 1en und 0en. Dadurch können digital arbeitenden elektronischen Schaltungen und Programmen die IP-Adressen schneller verarbeiten. Doch weder die 32-Bit-Folge, noch die IP-Adresse sind für das menschliche Gehirn einfach zu erfassen und zu merken. Der Mensch verwendet lieber Namen um eine Sache zu benennen und zu identifizieren. Diese Tatsache ist in den 70er-Jahren in das ARPANET, dem ursprünglichen Vorgänger des Internets, mit eingeflossen. Statt der IP-Adressen wurden Namen zur Adressierung von Computern verwendet. Diese waren für Menschen leichter zu merken und zu verstehen. Bis heute ist es jedoch nicht möglich, einen Computer direkt mit seinem Namen über das Netzwerk anzusprechen. Für ihn besteht die Welt immer noch aus Bit und Byte. Und deshalb braucht er immer eine binäre Adresse. Aus diesem Grund wurden mehrere Methode entwickelt, um eine Namensauflösung von Namen in numerische Adressen zu realisieren.

hosts

Jedes TCP/IP-Betriebssystem hat eine Datei mit dem Namen hosts. In ihr sind die IP-Adressen und Namen tabellenartig aufgelistet.

lmhosts

Die Datei lmhosts ist ausschließlich in Windows-Betriebssystemen zu finden. Neben den IP-Adressen sind dort NetBIOS-Namen enthalten.

DNS - Domain Name System

DNS ist eine servergestützte Struktur zur Auflösung von Namen in IP-Adressen. Der Client, der einen DNS-Namen in eine IP-Adresse aufgelöst haben will, stellt eine Anfrage an den DNS-Server. Der DNS-Server verwaltet IP-Adressen und die dazugehörigen Namen in einer Datenbank. Ist ein Name dort nicht enthalten, befragt er einen übergeordneten DNS-Server, bis eine IP-Adresse an den anfragenden Client zurück geliefert werden kann.

WINS - Windows Internet Name Service

WINS ist ein plattformabhängiges, auf Windows-basierendes, System zur Namensauflösung. Es baut auf den NetBIOS-Dienst der Windows-Betriebssysteme auf. WINS wurde eingeführt, um die NetBIOS-Rundsprüche zur Namensauflösung zu reduzieren. Wie bei DNS greift der Client auf den WINS-Server zu, um einen Namen in eine IP-Adresse umzuwandeln.

Ablauf einer Namensauflösung

Als erstes prüft der Client in seinem lokalen Cache, ob eine Adresse für den Namen vorliegt.

Wenn nicht, sieht er in der Datei hosts nach.

Findet er auch dort den Namen nicht stellt er eine Anfrage an den DNS-Server.

Zusätzliche Namensauflösung in Windows

Findet die Suche über den DNS-Server die IP-Adresse nicht, wird der WINS-Server befragt.

Kennt auch dieser den Namen nicht, wird ein NetBIOS-Rundspruch abgesetzt.

Als letzter Strohalm bei der NetBIOS-Namensauflösung ist die lmhosts-Datei.

DynDNS

DynDNS oder DDNS ist ein System, das in Echtzeit Domain-Name-Einträge aktualisieren kann. Unter DynDNS versteht man in der Regel einen DNS-Host-Dienst, der die ständig wechselnden IP-Adressen einem festen Domain-Namen bereithält. Unter DDNS versteht man in der Regel einen Aktualisierungsmechanismus für DNS-Einträge.

Wie funktioniert DynDNS?

Möchte man über den eigenen DSL-Zugang einen Server-Dienst zugänglich machen, dann scheitert das in der Regel an der dynamischen IP-Vergabe durch den Internet-Provider. Gemeint ist, dass der eigenen Internet-Anschluss regelmäßig eine neue IP-Adresse bekommt. Das bedeutet, diese IP-Adresse kann nicht als Ziel-Adresse genutzt werden. Will man das eigene Netzwerk doch aus dem Internet dauerhaft erreichbar machen, braucht man eine ständig gültige einmalige Adresse. Da man in der Regel mit Domain-Namen und nicht mit IP-Adressen bei der Adressierung arbeitet, benötigt man einen Dienst, der die IP-Adresse ständig aktualisiert und einem Domain-Namen zuordnen kann. Die Zuordnung der Domain-Namen und IP-Adressen im regulären DNS sind in der Regel statisch. Das heißt, sie ändern sich in der Regel nicht.

Um einen Server mit einem festen Domain-Namen, aber ständig wechselnden IP-Adressen, dauerhaft erreichbar zu machen, gibt es Dienste, wie zum Beispiel DynDNS.org. Dort kann man sich eine Subdomain kostenlos zuweisen lassen. Die wird im eigenen Internet-Zugangs-Router eingetragen. Immer dann, wenn sich die IP-Adresse des Routers ändert, meldet der Router die IP-Adresse an DynDNS.org. Von diesem Dienst wird bei einer DNS-Anfrage mit dem eigenen Domain-Namen immer die aktuelle IP-Adresse zurückgeliefert.

DynDNS eignet sich zum Beispiel zum Verbindungsaufbau eines VPN-Zugangs zu einem LAN, welches über keine eigene feste IP-Adresse verfügt. Ebenso kann über den Domain-Name ein Web- oder FTP-Server erreichbar sein. Die Möglichkeiten sind vielfältig.

Host - Tabelle

Beispiel einer Host-Tabelle:

~~local~~ local network host addresses

127.0.0.1	local	localhost	
192.10.100.301	ch1	CH1	
192.10.100.302	ch2	CH2	
0xC0.0x09.0x96.0x01	ch7		hexadecimal
0300.011.0226.02	tsbe4		octal

IP - Protokollkopf

Version	Länge	Servicetypen	Paketlänge			
Identifikation			0	DF	MF	Fragmentabstand
Lebenszeit		Transportprot. ID	Kopfprüfsumme			
Senderadresse						
Empfängeradresse						
Optionen					Füllzeichen (PAD)	

TCP - Protokollkopf

1	4	10	16	24	32			
Sender-Port				Empfänger-Port				
Sequenznummer								
Quittungsnummer								
Daten- abstand	Reserviert	U	P	S	A	R	F	Fenstergrösse
		R	S	Y	C	S	I	
		G	H	N	K	T	N	
Prüfsumme				Urgent-Zeiger				
Optionen				Füllzeichen				

ICMP - Protokollkopf

ICMP - Protokollkopf:

1	16	17	32
Typ	Code	Prüfsumme	
Verschiedenes			
IP-Kopf und 8 weitere Bytes oder Testdaten			

Typenfeld: Spezifiziert die Art der ICMP-Nachricht. Eine Auswahl davon:

Typenfeld	Funktion	Typenfeld	Funktion
0	Echo Reply	11	Time Exceeded for a Datagramm
3	Destination Unreachable	12	Parameter Problem on a Datagram
5	Redirect	13	Timestamp Request
8	Echo Request	14	Timestamp Reply

UDP - Protokollkopf

1		16 17		32	
Sender-Port			Empfänger-Port		
Länge			Prüfsumme		

Sender- und Empfänger-Portnummer: Wie im TCP-Protokoll sind auch hier die Portnummern die Referenz zu den Transportprotokollbenutzern.

Länge: Enthält die Länge des gesamten Datagramms, inklusive des Protokollkopfs.

Prüfsumme: Enthält die Internet-Prüfsumme der Daten und des Protokollkopfs. Wenn dieses Feld den Wert 0 enthält, hat der Absender keine Prüfsumme eingetragen und es findet im Empfänger-UDP keine Prüfung statt.

IPv6 ist als Internet Protocol (Version 6) für die Vermittlung von Daten durch ein paketvermittelndes Netz, die Adressierung von Netzknoten und -stationen, sowie die Weiterleitung von Datenpaketen zwischen Teilnetzen (Routing) zuständig. Mit diesen Aufgaben ist IPv6 der Schicht 3 des OSI-Schichtenmodells zugeordnet. IPv6 ist der direkte Nachfolger von IPv4 und Teil der Protokollfamilie TCP/IP. Der Grund für die Einführung des Internet Protocols Version 6 (IPv6) und Ablösung von IPv4 ist die Adressknappheit von nur 4 Milliarden IP-Adressen (Version 4), die bald aufgebraucht sind. Da weltweit immer mehr Menschen, Maschinen und Geräte an das Internet mit einer eindeutigen Adresse angeschlossen werden wollen, reichen die IPv4-Adressen nicht mehr lange aus.

Internet Protocol Version 5?

IPv5 hieß offiziell ST-2 (Internet Stream Protocol Version 2) und war ein experimentelles Protokoll für Echtzeit-Datenströme. ST-2 wurde von RSVP (Resource Reservation Protocol) zur Bandbreitenanforderung bei Routern abgelöst. ST-2 sollte ursprünglich Audio und Video per Multicast übertragen. Dadurch sollten die Bandbreitenreservierungsvorteile von ATM in die IP-Netze gelangen. Zur Serienreife hat es nicht gereicht. Deshalb gab es auch kein IPv5 im praktischen Einsatz.

IPv6

Die nächste Generation von IP, das IP Version 6, erhöht den Adressumfang auf 2¹²⁸. Damit wäre es möglich, jeden Quadratmillimeter der Erde mit rund 600 Billionen Adressen zu belegen. Doch nicht nur das, obendrein soll IPv6 Erleichterung bei der Rechnerkonfiguration und Betrieb bringen.

IPv6-Adressen bestehen aus 128 Bit. Wegen dieser unhandlichen Länge hat man sich für Hexadezimalzahlen als Schreibweise entschieden. 16 Bit sind jeweils durch einen Doppelpunkt (":") getrennt. Führende Nullen können in den Blöcken wegfallen. Eine Folge von Nullen kann man durch zwei Doppelpunkte ("::") ersetzen. Da in URLs der Doppelpunkt mit der Portangabe kollidiert, sind IPv6-Adressen in eckige Klammern gesetzt. Die Netzwerkmasken fallen ersatzlos weg. Den Adressbereich bzw. das Subnetz hängt man an und trennt ihn vom Rest der Adresse durch ein "/". In IPv6 adressieren die ersten 64 Bit das Netz und die restlichen 64 Bit den Host.

Adresse nach

IPv4	127.0.0.1
IPv6	FE80::0211:22FF:FE33:4455
IPv6-URL	http://[FE80::0211:22FF:FE33:4455]:80/

IPv6

IPv6 schafft die Adressknappheit und damit viele Netzwerkprobleme aus der Welt. IPv4 sieht nur 232 Adressen vor. Das sind rund 4,3 Milliarden IP-Adressen. IPv6 hat einen Adressraum von 2^{128} . Das sind 340.282.366.900.000.000.000.000.000.000.000, also rund 340,28 Sextillionen Adressen. Das reicht aus, um umgerechnet jeden Quadratmillimeter der Erdoberfläche inklusive der Ozeane mit rund 600 Billionen Adressen zu pflastern. Weil man mit dieser großen Menge an Adressen verschwenderisch umgehen darf, spart man sich eine aufwendige Verwaltung, wie es bei IPv4-Adressen notwendig ist. Der große Adressraum, also die hohe Anzahl an Präfixen, macht das Wegfallen von NAT möglich. Wobei das nicht bedeutet, dass es nicht doch irgendwann eine Implementierung für NAT in IPv6 geben wird. Bei IPv6 hat man sich nicht nur um die Adresserweiterung gekümmert, sondern auch gleich eine Generalüberholung des Protokolls vorgenommen. Zählte zur Hauptaufgabe der heutigen IPv4-Routern das Prüfen von Checksummen und Fragmentieren von Daten, so ist die Arbeit für IPv6-Router sinnvoll minimiert worden. IPv6 führt keine Prüfsumme mehr im Header mit. Stattdessen wird dem übergeordneten Transport-Protokoll TCP die Aufgabe überlassen, kaputte Pakete zu erkennen und neu anzufordern. Dieser Vorgang wird komplett beim Empfänger bearbeitet. Zu große Datenpakete werden von IPv6-Routern nicht mehr selber fragmentiert. Ist ein Paket zu groß wird dem Absender eine Fehlermeldung geschickt. Dieser muss dann die maximale Paketlänge (MTU - Maximum Transmissin Unit) anpassen. Dieses Verfahren nennt sich Path MTU Discovery und existiert in ähnlicher Form auch in IPv4. Dort muss im Datenpaket das Don't-Fragment-Flag (DF) gesetzt werden. War in IPv4 dieses Verfahren optional, ist es in IPv6 Pflicht. Kommt es zum Verlust eines Datenpakets oder kommt es zu Fehlern bei der Fragmentierung, schlägt das Path MTU Discovery fehl. In IPv4 wurde der MTU dann auf 68 Byte abgesenkt. Das führte zu einer höheren Paketanzahl und einem unwirtschaftlichen Protokoll-Overhead. IPv6 hat als kleinste einstellbare MTU 1280 Byte. Dadurch werden die Router nicht mehr unnötig belastet. Selbstverständlich können auch kleinere Pakete als 1280 Byte übertragen werden.

IPv4-Router müssen Checksummen prüfen und Pakete fragmentieren. Das erfordert Rechenleistung und reduziert den Datendurchsatz. Um das Routing zu beschleunigen wird auf Fragmentierung und Checksummen verzichtet. Die Prüfsumme bleibt höheren Protokolle überlassen. Zum Beispiel TCP. Und für das Prüfen der Pakete auf IP-Ebene ist nur noch der Empfänger zuständig. Ist ein Paket zu groß, wird es nicht mehr fragmentiert. Dafür wird es generell verworfen und der Sender per ICMP-Nachricht informiert. Der Sender setzt dann die maximale Paketgröße für diese Route herab (MTU, Maximal Transmission Unit).

Aufteilung des IPv6-Adressraums

Man unterscheidet grob gesehen zwischen globalen Adressen (Global Scope) und lokalen Adressen (Local Scope). Pakete mit globale Adressen werden außerhalb des lokalen Netzwerks geroutet. Link-lokale Adressen sind nur innerhalb des lokalen Netzwerks gültig. Sie werden nicht extern, sondern nur intern geroutet. Hinter Link-Local Scope stecken Mechanismen wie Neighbor Discovery, das das Address Resolution Protocol (ARP) ablöst oder Stateless Address Autoconfiguration (SAC oder SAA) als Alternative zu DHCP. Neighbor Discovery zeichnet sich vor allem durch Unabhängigkeit von der Übertragungstechnik aus. Für private lokale Netze gibt es in IPv6 reservierte Adressbereiche (Unique Local Adressses, ULA). Sie haben eine ähnliche Funktion, wie die lokalen IPv4-Adressen. Die privaten IPv6-Adressen sind weltweit eindeutig, werden aber nicht geroutet.

Adressvergabe und Autokonfiguration

IPv6 kennt zwei verschiedene Wege, wie Clients an ihre eigene IP-Adresse kommen. Entweder über DHCPv6 oder Autokonfiguration. Letzteres hat den Nachteil, dass damit nur die Kommunikation im lokalen Netz möglich ist. Standard-Gateway und DNS-Server müssen immer noch manuell konfiguriert werden oder per DHCPv6 abgefragt werden.

Stateful Address Configuration (DHCPv6)

Stateless Address Configuration (Autokonfiguration)

Anders als bei IPv4 müssen die IP-Adressen im lokalen Netzwerk nicht zentral vergeben werden. Die Adressvergabe erfolgt automatisch und die Stationen prüfen selbständig, ob ihre Adresse im Netz schon vergeben ist. Unter IPv6 gibt es keine Netzwerkmaske und Broadcast-Adressen mehr. Die Einrichtung eines Netzwerks ist dadurch viel einfacher.

Stateless Address Configuration

Wird eine Station mit IPv6 gestartet, dann weist sie sich als erstes eine lokale Adresse zu. Die ersten 64 Bit sind fest vorgegeben. Davon bestehen die ersten 16 Bit aus dem Prefix "fe80". Die restlichen 48 Bit werden mit Nullen aufgefüllt. Die zweiten 64 Bit werden als Suffix bezeichnet und bestehen aus der MAC-Adresse des Netzwerkadapters, die in das Nummerierungssystem EUI-64 des IEEE umgewandelt wird. Da MAC-Adressen in der Regel weltweit einmalig sind ist die lokale IP-Adresse es ebenso.

Bevor der PC diese Adresse nutzen kann, schickt er eine Anfrage ins lokale Netz (Neighbor Solicitation). Falls eine andere Station die Adresse bereits nutzt (Neighbor Advertisement), muss die IP-Adresse manuell umgeändert werden. In der Regel ist das nicht notwendig, weil jeder Netzwerkadapter in der Regel eine einmalig MAC-Adresse hat. Sollte doch einmal eine Doppelung vorkommen, dann sollte man das Netzwerk überprüfen. Dann könnte es sein, dass jemand eine MAC-Adresse gekapert hat und per MAC-Spoofing ins Netzwerk eingedrungen ist.

Mit seiner lokalen Adresse kann die Station nur im lokalen Netzwerk kommunizieren. Für das Internet braucht sie eine zusätzliche Adresse, die sie sich ebenfalls selber generiert. Dazu muss die Station beim Standard-Gateway (Router) nachfragen, welche Netzwerk-Adresse sie verwenden soll (Prefix des öffentlichen Adressblocks). Mit der lokalen Adresse bittet (Solicitation Message) die Station auf der Multicast-Adresse "FF02::2" um den IPv6-Präfix. Der Router schickt daraufhin eine Ankündigung (Advertisement Message) mit einem Adress-Präfix für dieses Netzwerk und die Größe der Pakete (MTU). Aus dem Präfix und Suffix erzeugt die Station ihre öffentliche IPv6-Adresse. Der Suffix ist eine EUI-64-Adresse, die aus der Hardware-Adresse (MAC-Adresse) erzeugt wird. Danach prüft die Station, ob diese Adresse im lokalen Netzwerk schon vergeben ist (Duplicate Address Detection). Wenn sie frei ist, weist sie die Adresse ihrer Netzwerkschnittstelle zu.

Die IP-Autokonfiguration ist allerdings nicht ganz vollständig. Es werden keine Adressen für DNS- oder NTP-Server erzeugt. Auch ein Hostname wird nicht zugewiesen. An diese Informationen kommt ein PC beispielsweise über Bonjour (Apple), PNRP (Microsoft) oder DHCPv6.

Privacy Extensions / Vorteile von IPv6

Der Interface Identifier wird aus der MAC-Adresse errechnet. Weil die globale MAC-Adresse und die IPv6-Adressen durch den Interface Identifier nachverfolgbar ist wurden die Privacy Extensions entwickelt. Damit wird ein Teil der Anonymität, wie es bei IPv4 möglich ist, wieder hergestellt werden, in dem die Kopplung von Interface Identifier und MAC-Adresse aufgehoben wird.

Privacy Extensions erzeugt ständig wechselnde Interface Identifiers, statt diesen aus der MAC-Adresse zu errechnen. Privacy Extensions erzeugt zusätzlich zu der festen IP-Adresse periodisch eine neue Adresse, bei der der hintere Teil verändert ist. Anschließend werden mit diesen wechselnden Adressen ausgehende Verbindungen hergestellt. Auf diese Weise wird auf IP-Ebene die Erstellung von Bewegungsprofilen verhindert.

Vorteile von Ipv6

IP-Autokonfiguration anhand der MAC-Adresse der Netzwerkkarte

schnelleres Routing

Punkt-zu-Punkt-Verschlüsselung mit IPsec

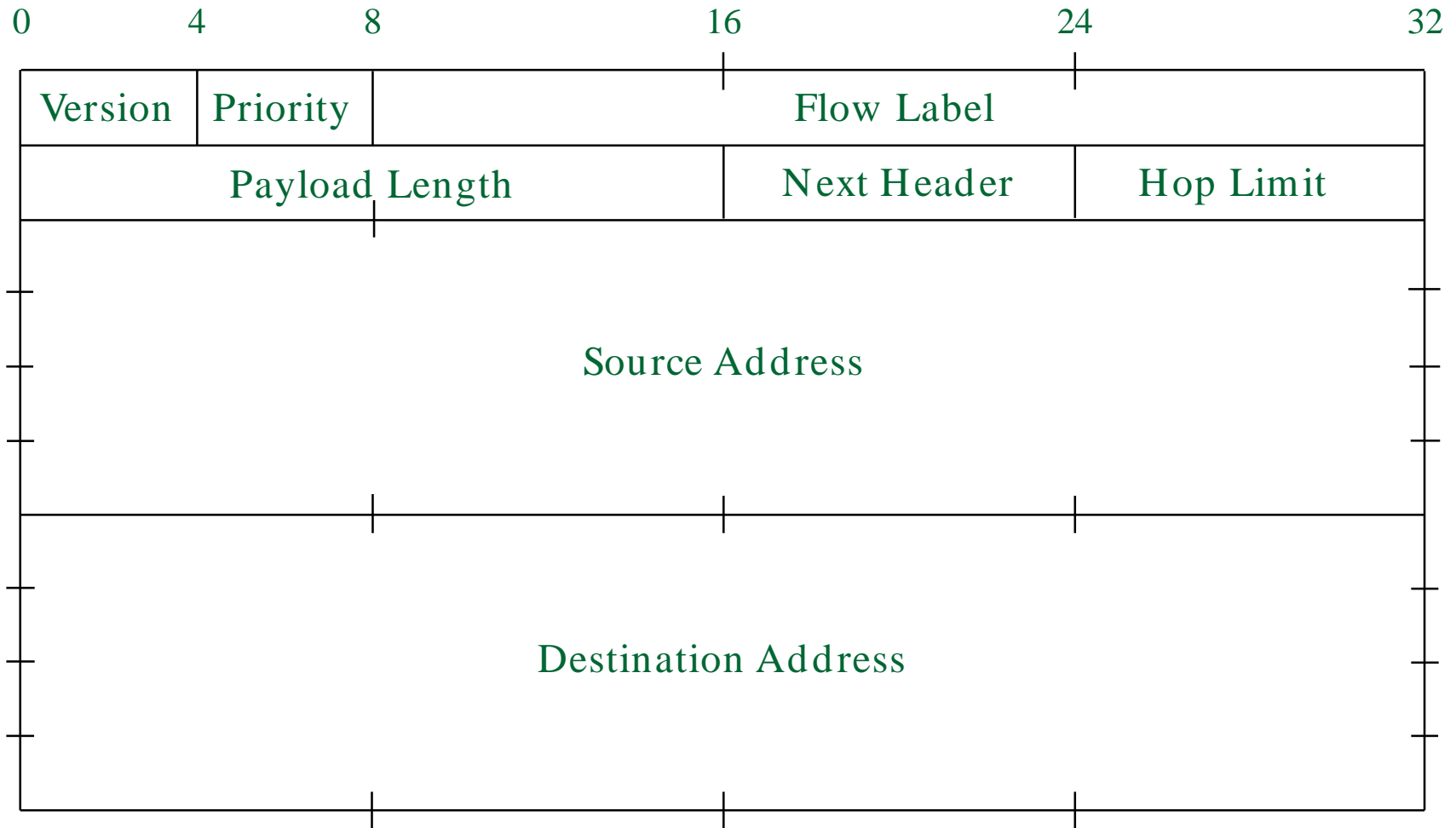
gleiche Adresse in wechselnden Netzen

Multicast

Quality of Service

Datenpakete bis 4 GByte Größe

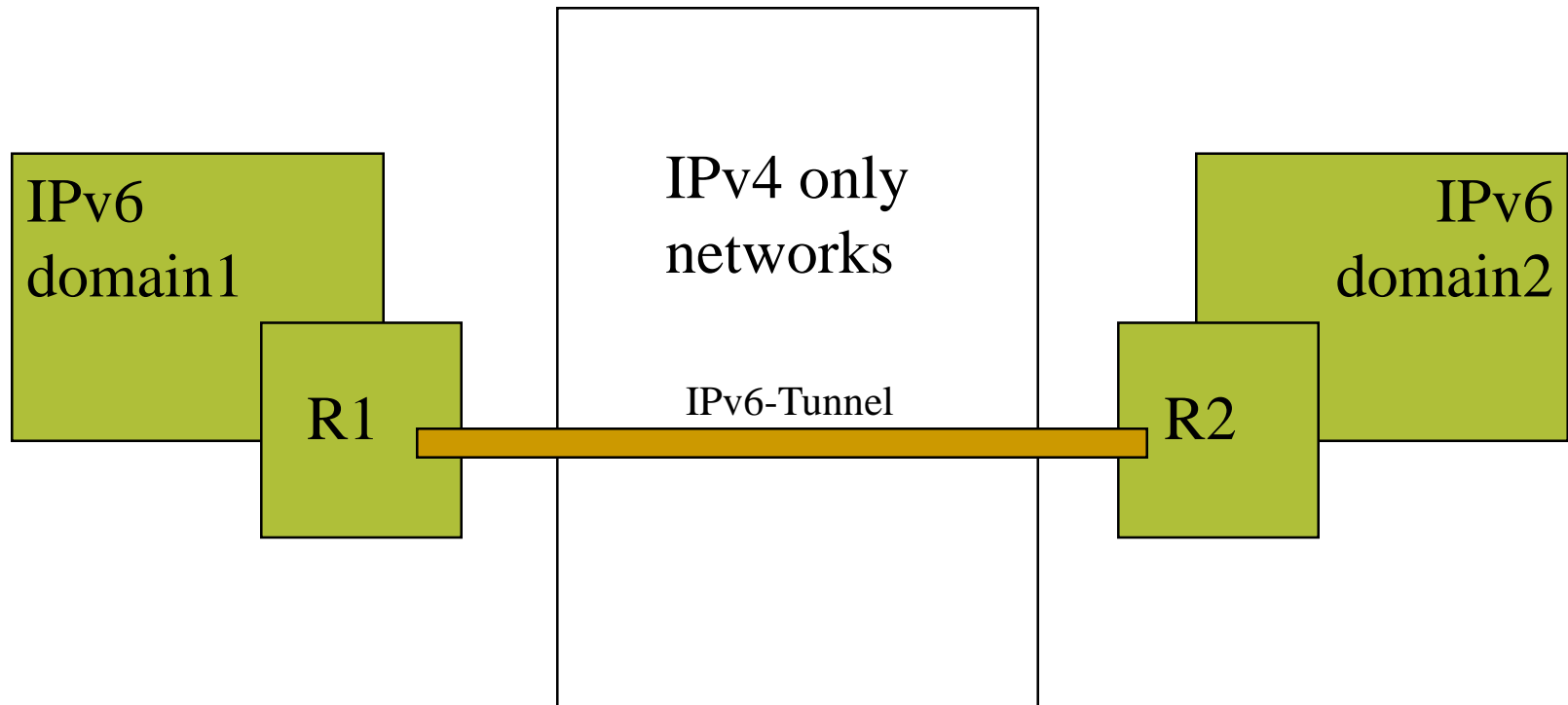
IPv6 - Header



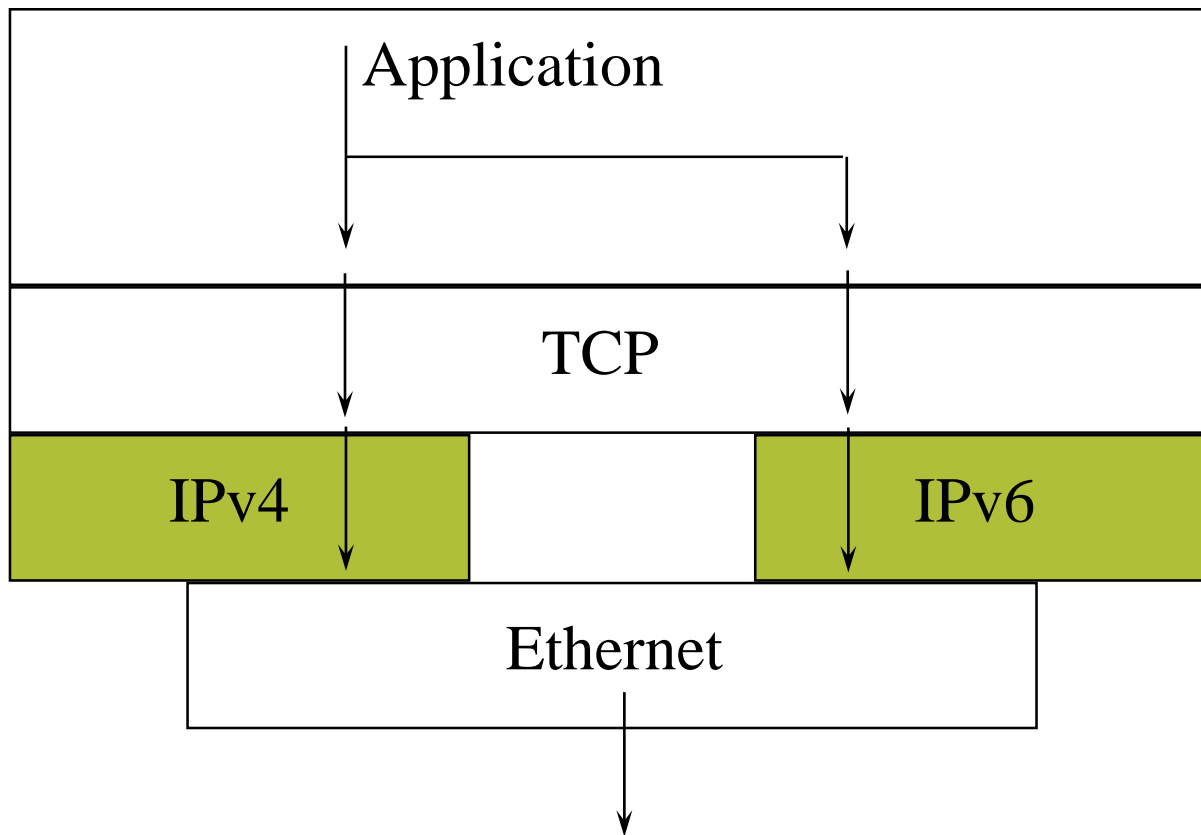
Bedeutung der Felder im IPv6-Header

Feldinhalt	Bit	Beschreibung
Version	4	Hier ist die Version des IP-Protokolls abgelegt, nach der das IP-Paket erstellt wurde.
Traffic Class	8	Der Wert des Feldes definiert die Priorität des Paketes.
Flow Label	20	Das Flow Label kennzeichnet Pakete für ein viel schnelleres Routing. Das MPLS macht dieses Verfahren allerdings überflüssig.
Payload Length	16	Hier steht die im IP-Paket transportierten Daten in Byte. Bisher musste der Wert aus dem Feld Paketlänge abzüglich dem Feld IHL ermittelt werden.
Next Header	8	Hier ist das übergeordnete Transportprotokoll angegeben. Bei IPv4 hieß das Feld einfach Protokoll.
Hop Limit / TTL	8	Dieses Feld enthält die Anzahl der verbleibenden weiterleitenden Stationen, bevor das IP-Paket verfällt. Es entspricht dem TTL-Feld von IPv4. Jede Station, die ein IP-Paket weiterleitet, muss von diesem Wert 1 abziehen.
Source-Address	128	An dieser Stelle steht die IP-Adresse der Station, die das Paket abgeschickt hat (Quell-IP-Adresse).
Destination-Address	128	An dieser Stelle steht die IP-Adresse der Station, für die das Paket bestimmt ist (Ziel-IP-Adresse).
IPv6-Header-Erweiterungen jeweils 64 Bit (8 Byte)		Im IPv6-Header können optional Informationen im separaten Header dem IP-Kopf angehängt werden. Bis auf wenige Ausnahmen werden diese Header-Erweiterungen von IP-Routern nicht beachtet.

IPv6 / IPv4 - Tunneling



IPv6 Dual-Stack-Implementierung



TCP/IP - Protokollszenarien

Verbindungsaufbau in TCP

TCP A		TCP B
→	(SEQ=100), (FLAGS=SYN)	
	(SEQ=300) ,(ACK= 101) ,(FLAGS=SYN, ACK)	←
→	(SEQ=101), (ACK=301), (FLAGS=ACK)	

Datenaustausch in TCP

TCP A		TCP B
→	(SEQ=101), (ACK=301), (FLAGS=ACK), (DATA=5)	
	(SEQ=301) ,(ACK= 106) ,(FLAGS=ACK) ,(DATA=10)	←
→	(SEQ=106), (ACK=311), (FLAGS=ACK)	

TCP/IP - Protokollszenarien (2)

Verbindungsabbau in TCP

TCP A

TCP B

→ (SEQ=106), (FLAGS=FIN, ACK)

(SEQ=311), (ACK=107), (FLAGS=ACK) ←

(SEQ=311), (ACK=107), (FLAGS=ACK), (DATA=5) ←

→ (SEQ=107), (ACK=316), (FLAGS=ACK)

(SEQ=316), (ACK=107), (FLAGS=FIN, ACK) ←

→ (SEQ=107), (ACK=317), (FLAGS=ACK)

Weitere Informationsquellen

- TCP/IP und NFS / M.Santifaller / Addison-Wesley
- Lexikon der Datenkommunikation / K.Lipinski / Datacom
- TCP/IP / Othmar Kays / Datacom
- Internet / Othmar Kays / Datacom