Diplomarbeit

Einsatz von IP Version 6 und IP Mobility in der dritten Mobilfunkgeneration

von

Kathrin Hartwig & Jens Simon

in Zusammenarbeit mit der

Pan Dacom **Networking AG**

im Februar 2002

Inhalt

Kapitel	Seite

1 Einleitung

1.1 Hintergrund und Problemstellung

Seit einiger Zeit und vorangegangenem Zögern scheinen die Anbieter und Anwender von Netzwerken die Version 6 des Internetprotokolls zu akzeptieren. Das Internet Protokoll Version 6 (IPv6) wird als Nachfolger, des bislang implementierten und erfolgreichen Protokolls IPv4, bereits seit langem spezifiziert. In den 70er-Jahren, als das ARPA-Netz, der Vorläufer des Internets, aufgebaut wurde, war noch nicht abzusehen, dass eines Tages derart viele Adressen benötigt würden. Nach Einführung von IPv4 in den frühen 80er-Jahren schien der Adressraum für nahezu unbegrenzte Zeit auszureichen. Der rapide Wachstum des Internets seit Beginn der 90er-Jahre und die damit verbundene Verknappung und Aufteilung der IP-Adressen sowie die unüberschaubar gewachsenen Routingtabellen waren der Auslöser dafür, einen Nachfolger von IPv4 zu entwickeln. Seitdem arbeitet die Internet Engineering Task Force (IETF) am neuen Internet Protokoll der nächsten Generation.

Für uns Grund genug, das Thema aufzugreifen.

Natürlich stellt sich die Frage, ob es überhaupt notwendig ist, das gesamte Internet auf eine neue Protokollversion umzustellen, zumal es einige Jahre dauern wird bis sich IPv6 durchgesetzt hat. Portable Geräte, ob Notebooks, Handys oder digitale Assistenten, mit Internetanschluss und eigener IP-Adresse werden immer beliebter. Dadurch erlangen Schlagworte, z. B. Adressraum, Autokonfiguration, Mobility und Security völlig neue Dimensionen. Durch die geplante Einführung von UMTS im Jahr 2003 erhofft man sich, eine Killerapplikation für IPv6 zu finden. Die mobile Kommunikationsfähigkeit wird durch UMTS gefördert und durch Mobile IPv6 unterstützt. Dass ein neues Internetprotokoll von heute auf morgen funktionsfähig implementiert ist und das bisherige Protokoll ersetzt, kann man nicht erwarten. Die Nachfrage allerdings steigt. Da IPv4 nicht aufwärtskompatibel bzw. IPv6 nicht abwärtskompatibel ist, müssen zwingend Interoperationsmöglichkeiten definiert werden. Dual-Stack Verfahren und unterschiedliche Tunnelingmethoden sowie weitere Realisierungsmöglichkeiten zur Einführung von IPv6 werden daher benötigt.

1.2 Ziel der Diplomarbeit

In dieser Diplomarbeit werden die Grundlagen von IPv4 und IPv6 dargestellt, um daraus zu erkennen, auf welche Punkte während der Übergangsphase ein besonderes Augenmerk gelegt werden muss. Da die zunehmende Mobilität ein wesentlicher Faktor in der Akzeptanz von IPv6 sein wird, ist im weiteren Verlauf der Diplomarbeit auf entsprechende Möglichkeiten

in IPv6 sowie UMTS ein Schwerpunkt gelegt. Die für die Interoperabilität notwendigen Verfahren sollen im Rahmen dieser Diplomarbeit ebenfalls erläutert werden.

Ziel ist es, aus den gewonnenen Erkenntnissen sowie unter der Berücksichtigung einer sanften Migrationsphase, ein LAN-Konzept für ein Unternehmen zu entwickeln. Ebenfalls wird die Struktur eines IPv6 fähigen UMTS-Betreiber-Netzes gezeigt.

1.3 Aufbau und Terminologie

Die Diplomarbeit ist in sieben Kapitel unterteilt.

Nach dieser Einleitung folgen sechs Kapitel, die hier kurz beschrieben werden.

Neben einer ausführlichen Einleitung in die Grundlagen der Internet Protokolle und Routingverfahren, widmen wir uns im **Kapitel 2** den Spezifikationen der dritten Mobilfunkgeneration, dem Universal Mobile Telecommunications System (UMTS).

Kapitel 3, Motivation für IPv6, bietet ausführlich Informationen über die Adressräume, Konfigurationen, Mobilitätsfunktionen und Sicherheitsmerkmale von IPv6.

Eine tiefergehende und ausführlichere Untersuchung der Migration des neuen Internetprotokolls befindet sich in **Kapitel 4**.

In **Kapitel 5** widmen wir uns den Mobilitätsfunktionen von IPv6. Hier erörtern wir verschiedene Mechanismen und Arbeitsweisen von Mobile IP.

Unter IPv6 Netzwerkplanung, **Kapitel 6**, zeigen wir die mögliche Realisierung von Netzwerken anhand der bisher gewonnenen Kenntnisse.

Eine Zusammenfassung der Diplomarbeit befindet sich in **Kapitel 7**.

Der **Anhang** enthält das Abbildungs- und Tabellenverzeichnisse, Zusatzinformationen, auf die wir gegebenenfalls im jeweiligen Kapitel durch eckige Klammern [xy] verweisen, Quellenangaben, ein ausführliches Glossar sowie ein Abkürzungsverzeichnis.

Der Text der Diplomarbeit ist grundsätzlich in Deutsch gehalten. Englische Fachbegriffe wurden verwendet, soweit keine gleichwertigen deutschen Begriffe bekannt waren und die englische Ausdrucksweise die Gebräuchlichere ist.

An dieser Stelle erklären wir vier häufig verwendete Begriffe, um Missverständnisse zu vermeiden.

Ein **Router** ist ein Gerät, das unterschiedliche Netze auf IP-Ebene verbindet. Router arbeiten anhand von Protokollen, mit denen sie Informationen austauschen. Sie legen sogenannte Routingtabellen an, aufgrund derer sie Datenverkehr über angeschlossene Netzwerke verschicken.

Als **Gateway** ist eine Schnittstelle zwischen zwei verschiedenen Systemen bezeichnet, die nicht auf ein bestimmtes Protokoll festgelegt ist, sondern dem jeweiligen Bedarfsfall entsprechend ausgelegt wird. Es gibt hardware- und softwarebasierende Gateways. Router sind Gateways der Layer 3 nach dem OSI-Modell.

Ein **System** wiederum beschreibt eine Komponente oder ein Gefüge von Komponenten, das an der Kommunikation beteiligt ist. Es besitzt einen bestimmten Zweck in der Kommunikation, der hierdurch jedoch nicht genauer spezifiziert wird. Router, Gateways, Clients, Server, PCs, etc. sind Systeme.

Häufig wird allgemein der Begriff **Tunnel** verwendet. Damit ist eine virtuelle Verbindung von zwei Geräten gemeint, die aus physikalischer Sicht nicht direkt miteinander verbunden sind. Benötigt werden Tunnel dann, wenn diese Geräte Daten eines anderen Formates austauschen wollen, als das dazwischenliegende Medium verarbeiten kann. Ein Tunnel verbindet Systeme über ein Netz anderer Systeme miteinander, die keine Kenntnis der Inhalte des Tunnels benötigen.

2 Grundlagen

2.1 OSI – Modell im Vergleich zur TCP/IP-Architektur

Das von der International Standardisation Organisation (ISO) ursprünglich standardisierte Open Systems Interconnection-Modell (OSI-Modell) ist ein 7-schichtiges Referenzmodell. Es beschreibt die Struktur und die Aufgaben der für die Netzwerkdatenkommunikation verwendeten Protokolle. Nur in der untersten, der Bitübertragungsschicht, werden tatsächlich physikalische Signale ausgetauscht. In den darüber liegenden Schichten sind Dienste definiert, die die Wegefindung, Sicherung und korrekte Steuerung der Daten mittels geeigneter Protokolle ermöglichen.

Das OSI-Modell wurde aus dem älteren 4-schichtigen Modell (TCP/IP[1]-Layer) des Department of Defense (DoD) entwickelt, auf welches wir uns im folgenden beziehen. [1]

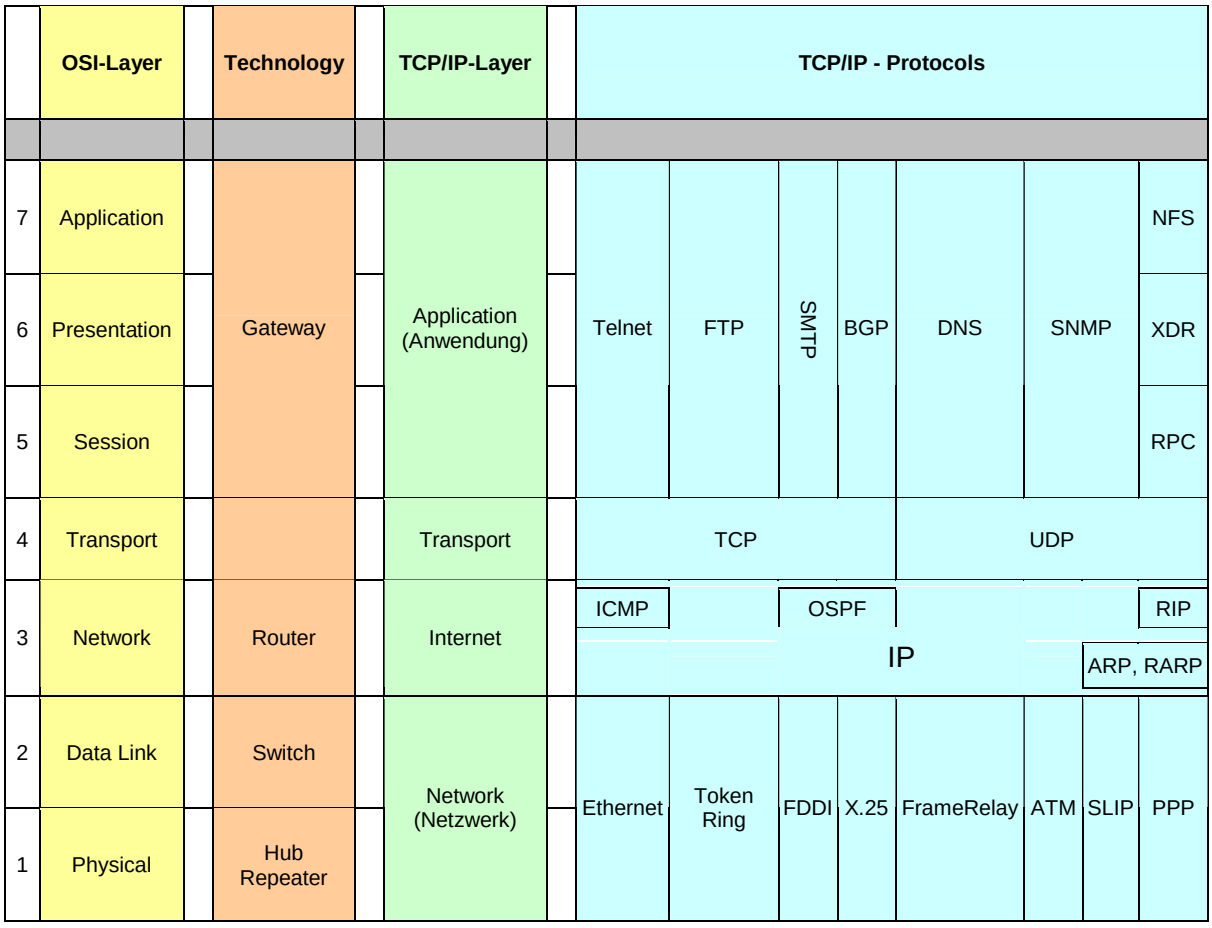


Bild 2.1 OSI-Modell im Vergleich zur TCP/IP-Architektur

[1] Transmission Control Protocol / Internet Protocol

In der untersten Schicht, der Netzwerkschicht, sind die heute genutzten Netzwerkprotokolle, wie z. B. Ethernet (IEEE 802.3[2]), Token Ring (IEEE 802.5), ATM usw. angesiedelt. Hier wird die physikalische Form der Daten und des Übertragungsmediums festgelegt. Da auch die 2. Schicht des OSI-Modells, die Sicherungsschicht, hinzugezählt wird, findet Transportsicherung und Fehlererkennung/-behebung (optional) in dieser Ebene statt.

Die Internetschicht (nach OSI-Modell Vermittlungsschicht) enthält Protokolle, die den Datenverkehr regeln, der über direkte Punkt-zu-Punkt Verbindungen hinausgeht. Dazu gehört z. B. das Internet Protocol (IP). Als Routingprotokolle werden u.a. Routing Information Protocol (RIP), Open Shortest Path First (OSPF) und Border Gateway Protocol (BGP 4) verwendet.

Das Transmission Control Protocol (TCP) und das User Datagramm Protocol (UDP) werden der Transportschicht zugeordnet. Während TCP hardwareunabhängige, fehlergesicherte Ende-zu-Ende Verbindungen in Local Area Networks (LANs) und Wide Area Networks (WANs) zur Verfügung stellt, hat das UDP keine Möglichkeit zur Fehlersicherung.

Verschiedene Protokolle, die zur Anpassung an spezielle Anwendungen und Steuerung der unteren Schichten notwendig sind, werden in der Anwendungsschicht zusammengefasst. Einige Beispiele: File Transfer Protocol (FTP), HyperText Transfer Protocol (HTTP), Domain Name Service (DNS). Eine Übersicht und Zuordnung zu den Transportschichtprotokollen befindet sich in Bild 2.1.

2.2 Internet Protocol

Ursprünglich wurde das Internet Protokoll (IP) [2] Ende der 60er Jahre für ein militärisches Netz mit dem Namen ARPANET[3], von dem US-Verteidigungsministerium gefördert, entwickelt. Die Anforderungen an dieses Netz waren vor allem, dass es auch bei Ausfällen von Teilstrecken funktionstüchtig bleibt, weswegen zum ersten Mal Paketvermittlung verwendet wurde.

Heute bildet das IP, ab 1.1.1983 als einziges Protokoll im ARPANET zugelassen, die Basis für eine weltweite Vernetzung von privaten und kommerziellen Systemen, welche ganz andere Anforderungen haben als die Forschungssysteme damals. Anforderungen an die Sicherheit waren gering und auch die Dienstqualität im heutigen Sinne war unwichtig, da

[2] IEEE steht für das Institute of Electrical and Electronic Engineers
[3] das erste Datennetz, von der Advanced Research Projects Agency entwickelt

keine Daten übertragen wurden, bei denen die Paketvermittlung ein Problem darstellte (z. B. Video, Voice over IP, etc.). Auch der Adressraum von 32 Bit war damals mehr als genug.

Mitte der achtziger Jahre wurden dann immer mehr Netze an das ARPANET angeschlossen, was dazu führte, dass das eigentliche militärische Netz aus Sicherheitsgründen ausgegliedert wurde und noch heute unter dem Namen MILNET betrieben wird.

Im Jahre 1990 wurde das eigentliche ARPANET geschlossen und sein Abkömmling, das Internet breitete sich schnell aus. Es verzeichnet immer noch einen enormen Zuwachs und das Ende des 32 Bit-Adressraumes ist in greifbare Nähe gerückt. In absehbarer Zeit werden auch andere Geräte als eigentliche Rechner (z. B. PDAs[4], Mobiltelefone, etc.) am Internet teilnehmen. Man kann heute Bestellungen und Finanztransaktionen tätigen, obwohl IPv4 (Version 4, aktuell implementiert) selbst keine hilfreiche Unterstützung für eine Verschlüsselung der Daten auf Protokollebene bietet. Diese Unzulänglichkeiten für den heutigen Gebrauch wurden erkannt und verschiedene Gremien beschäftigen sich seit 1991/92 mit der Entwicklung eines Nachfolgers für IPv4, genannt IPv6. Auf beide Protokollversionen wird im folgenden näher eingegangen.

2.2.1 IPv4

Das IPv4 ist in RFC791[5] spezifiziert und bietet einen verbindungslosen und datagrammorientierten Ende-zu-Ende Übertragungsdienst. Es ist zuständig für die Vermittlung und optional für die Aufteilung und Zusammensetzung von Benutzerdatagrammen auf deren Weg durch das Teilnetz zum Zielsystem. [2]

Die Transporteinheit im IP ist ein Datagramm. Sein Aufbau wird normalerweise in jeweils 32 Bit-Blöcken senkrecht skizziert, wobei der variable Vorspann (Header) mindestens 20 Bytes groß ist. Außerdem besitzt es keinen Nachspann (Trailer).

[4] Personal Digital Assistant
[5] Request for Comment

Folgendes Bild zeigt das Format eines IPv4-Datenpaketes mit allen Optionsfeldern.

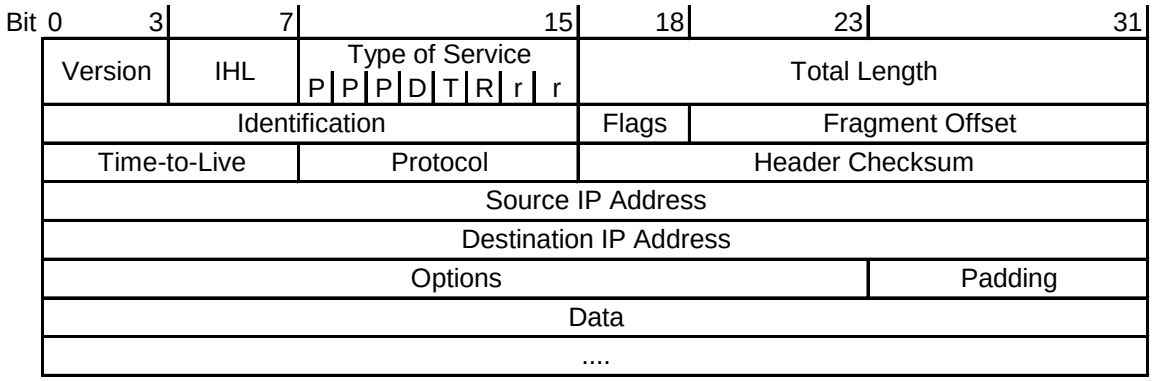


Bild 2.2 IPv4 - Datagramm

Folgende Felder sind IPv4 definiert:

Version

Beschreibt die Version des IP-Datagramms (IPv4=4; IPv6=6) und ist 4 Bit breit. IPv6 wird weiter unten ausführlich beschrieben. Datagramme verschiedener IP-Versionen lassen sich nicht zu einem Datenfluss integrieren.

IHL

Internet Header Length (IHL) gibt die aktuelle Länge des Internet-Protokollkopfes in 32-Bit-Einheiten (im Bild 2.2: 6*32 Bit=24 Bytes) an. Es hat ebenfalls eine Länge von 4 Bit und damit ist der größte Header maximal 60 Bytes groß (15*32 Bit). IHL-Wert 5 bedeutet, dass keine Optionsfelder vorhanden sind, was Standard ist und zur Folge hat, dass der Internet-Protokollkopf 5*32 Bit (20 Bytes) lang ist.

TOS

Type of Service ist ein 8 Bit langes Feld, in dem die Qualität des angeforderten Dienstes beschrieben wird. Sind alle Bits auf Null gesetzt, erfolgt eine normale Übertragung.

TOS hat folgende Aufschlüsselung:

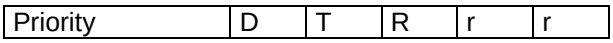


Bild 2.3 TOS Feld

Die ersten drei Bits geben den Prioritäten-Level an und haben folgende Verwendung [3]:

000	normal
001	priority
010	immediate
011	flash
100	flash override
101	critical
110	internet control
111	network control

Mit den folgenden fünf Bits werden nachstehende Eigenschaften deklariert:

00000: normaler Dienst

10000: minimiere Verzögerung (Delay D-Bit)

01000: maximiere Durchsatz (Troughput T-Bit)

00100: maximiere Zuverlässigkeit (Reliability R-Bit)

Die letzten beiden Bits sind für künftige Anwendungen reserviert.

Da das TOS-Feld nicht wie in IPv4 ursprünglich spezifiziert genutzt wird, ist es von der IETF in IPv6 nicht mehr vorgesehen. Dafür ist das Traffic Class-Feld definiert worden. Um zusätzlich für z. B. Echtzeitanwendungen entsprechende Routingmechanismen zur Verfügung zu haben, gibt es in IPv6 das Flow Label Feld. Siehe hierzu IPv6.

Momentan gibt es für IPv4 die Möglichkeit, das TOS-Feld als *Differentiated Services*- Feld (DS) zu nutzen. [10] Das DS-Feld ist auch in IPv6 bekannt und wird in RFC 3168 weitergehend definiert. Der Datenverkehr wird hierbei ein paar wenigen Klassen zugeordnet, die direkt im Paket identifiziert werden können. Die Markierung wird *Differentiated Services Code Point* (DSCP) genannt[6].

Total Length

Total Length gibt die gesamte Datagrammlänge (Header und Nutzlast) kodiert in 16 Bit an. Deshalb kann das Datagramm maximal 65535 Bytes groß werden. Die Differenz zwischen diesem Wert und dem IHL-Wert (* 4 Bytes) ergibt die Länge des Datenteils im Datagramm.

[6] vgl. [10] Seite 157ff

Identification

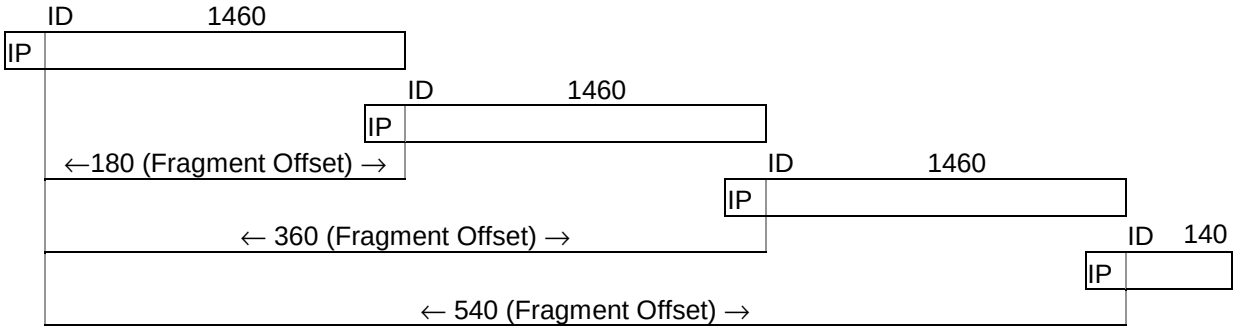
Ein Wert, der vom Sender gesetzt wird und bei dem Zusammensetzen fragmentierter Datagramme zur Identifikation dient. Das Feld hat eine Länge von 16 Bit.

Flags

In diesem 3-Bit-Feld wird die Steuerung der Fragmentierung durchgeführt. Fragmentierung ist erforderlich, wenn die zu übertragenden Daten größer als 65535 Byte sind. Das erste Bit der Flags wird nicht benutzt und muss den Wert "0" haben. Das nächste Bit ist das Don´t Fragment-flag (DF). Hier wird durch "0" eine Fragmentierung erlaubt, durch "1" nicht. Das letzte Bit ist das sogenannte More-Fragments-flag (MF), welches angibt, ob dieses das letzte Fragment (Wert "0") eines Datagramm ist oder noch weitere folgen (Wert "1").

Fragment Offset

Damit die fragmentierten Datagramme wieder korrekt zusammengeführt werden können, sind Angaben zur Position der Daten der jeweiligen Datagramm-Fragmente innerhalb des ursprünglichen Datagramms erforderlich. Dieses 13 Bit lange Feld gibt den Offset des jeweiligen Fragments in Vielfachen von 8 Bytes an. Der Offset ist bezogen auf den Paketanfang. Es folgt ein schematisches Beispiel für ein fragmentiertes Datagramm von 4500 Byte, wobei IP für den IP-Protokollkopf und ID für das Identification-Feld stehen.



Zahlenangaben in Bytes

Bild 2.4 Datagramm-Fragmente mit dargestelltem Fragment Offset

TTL

Time-to-Live (8 Bit) setzt die maximale Anzahl von Hops[7] fest. Bei jedem Hop wird der TTL-Wert um mindestens 1 dekrementiert, bis dieser Null ist. Dann muss das Datagramm verworfen werden. Diese Vorgehensweise verhindert ein endloses Kreisen eines Pakets

[7] Anzahl der Router, die durchlaufen werden

innerhalb des Netzwerkes. Die Angabe war ursprünglich für Sekunden gedacht, heute wird 1 Sekunde pro Router gezählt.

Protocol

Das 8-Bit-Protokoll-Feld gibt den Wert des Protokolls der nächsten Schicht an, welches im Datenteil verwendet wird.

Folgende Werte als Beispiele [4]:

17	UDP
6	TCP
1	ICMP
8	EGP
89	OSPF

Header Checksum

Das 16-Bit-Header-Prüfsummen-Feld befördert eine Prüfsumme, die nur über den Header berechnet wurde. Somit werden Übertragungsfehler im Header erkannt, jedoch nicht im Datenteil.

Source IP Address

Hier steht die 32 Bit IP-Adresse des Absenders. Der erste Teil der Adresse identifiziert das Netzwerk, der zweite Teil den Ziel-Host[8] in diesem Netzwerk. Genaueres folgt später. IP-Adressen werden üblicherweise als vier Dezimalzahlen geschrieben, eine je Byte. Die Zahlen werden durch einen Punkt (.) getrennt, weswegen die Schreibweise auch Dezimalnotation (Dotted Decimal Notation) genannt wird. Beispiel: 138.147.0.1

Destination IP Address

Analog zur Source IP Address steht hier die Adresse des Empfängers.

Options / Padding

Dieses Feld ist kein Pflichtbestandteil eines Datagramms und besitzt keine feste Länge, sondern kann variabel von 0 bis 40 Bytes groß sein. Es wird für die Aufnahme von Informationen zu Sicherheit, Diagnose, Routing oder Statistik genutzt. Die Füllzeichen werden eventuell gebraucht, um den Internetheader an die 32 Bit-Aufteilung anzupassen.

[8] Rechner oder Schnittstelle

Nach dem Feld Options / Padding kommt nun der Datenteil, welcher die Nutzdaten trägt, oder es folgen die Header der höheren Protokolle, wie TCP oder UDP.

Adressarchitektur in IPv4

Mit den 32 Bit IPv4-Adressen sind rein rechnerisch 4.294.967.296 Adressen möglich. Man hat 1981 sicher nicht gedacht, dass dieser Adressraum derartig schnell ausgeschöpft sein würde.

Die Adressen bestehen aus einem Netzwerkteil und einem darauf folgenden Hostteil. Das Netzwerk wurde zunächst entweder mit 8, 16 oder 24 Bit identifiziert, die jeweils folgenden Bits gehören dann zu einem Host innerhalb des angesprochenen Netzwerks. Netzwerk-Adressen, die aus 32 Bit bestehen, sind für spezielle Anwendungen reserviert.

Ursprünglich wurden fünf verschiedene Klassen zur Strukturierung der Netzwerke im Internet vorgesehen. Die Klassen A bis E sind wie folgt spezifiziert:

Class	network ID MSB[9]	decimal	host ID LSB[10]
A	0_2 + 7bit	0-127	24bit
B	10_2 + 14bit	128-191	16bit
C	110_2 + 21bit	192-223	8bit
D	1110_2 + 28bit	224-239	Multicastaddresses
E	1111_2 + 28bit	240-254	reserved

Fängt eine IP-Adresse mit dem ersten Bit "0” an, so werden noch weitere 7 Bit für die Auflösung des Netzwerks verwendet. Liegt der Dezimalwert zwischen 128 und 191, stehen insgesamt 16 Bit für die Netzwerkidentifikation zur Verfügung.

Diese Aufteilung verursachte jedoch eine zusätzliche Adressverknappung, da z. B. in großen Netzen (Class A und B) Adressen ungenutzt blieben und außerdem Adressräume wie Class D und E reserviert sind. So wird heute Classless Inter-Domain Routing (CIDR) verwendet.

[9] Most significant Bits (die höherwertigen Bits)
[10] Least significant Bits (die niederwertigen Bits)

Classless Inter-Domain Routing

CIDR wurde im September 1993 [5] entwickelt, da abzusehen war, dass der Adressraum des Class B Netzwerks bald ausgeschöpft sein würde und da der Umfang der Routingtabellen enorm zunahm. Ohne die schnelle Verbreitung von CIDR in 1994/95 hätten Internet Routingtabellen in 1996 mehr als 70.000 Routen beinhaltet, statt der tatsächlichen ca. 30.000. Aus der Sicht von 1996 war man sich nicht sicher, ob das Internet dann noch funktioniert hätte. [6] Heutzutage umfassen die Routingtabellen ca. 120.000 Einträge und die modernen Technologien ermöglichen eine Verwaltung von weitaus größeren Tabellen.

Statt der festen Netzwerkidentifizierung unter dem früheren klassenbehafteten Adressierungssystem (8, 16, oder 24 Bit) benutzen Router heute mit CIDR eine sogenannte "Netzwerk Präfix", um die Grenze zwischen Netzwerkadresse und Hostadresse zu erkennen.

Über die "Präfix-Länge", einer Zahl, die nach der IP-Adresse angegeben wird, werten Router die entsprechende Anzahl an Bits aus, die damit zur Netzwerkadresse deklariert sind. So können nun willkürlich große Netzwerke angesprochen und der unter IPv4 zur Verfügung stehende Adressraum besser ausgenutzt werden.

Hier ein paar Beispiele im Vergleich zur traditionellen Adressierung:

Classful	Classless	
Class A	12.32.27.5/22	00001100.00100000.00011011.00000101
Class B	131.16.0.0/20	10000011.00010000.00000000.00000000
Class C	204.135.128.0/18	11001100.10000111.10000000.00000000

Nach der klassenbehafteten Methode würde die erste IP-Adresse, die mit einer Null beginnt, als Class A zugehörig gewertet und nur insgesamt 8 Bit für die Netzwerkadresse ausgewertet. Da die Präfixlänge aber mit 22 angegeben ist, müssen noch 14 weitere Bits zur Berechnung der Netzadresse verwendet werden. Die Defaulteinstellung von Routern ist heute noch die klassenbehaftete Adressierung und kann manuell auf Classless umgestellt werden.

Durch die so erweiterten Möglichkeiten der Netzwerkadressierung werden Routingtabellen durch Zusammenfassung (Summarization) der Präfixe mit dem gleichen Next Hop wesentlich kompakter. Im klassenbehafteten System hatte man z. B. für mehrere Class C Netzwerke mit der Präfix 193.147.x.x, die über denselben "next hop"[11] erreichbar sind,

[11] nächster erreichbarer Router im Netz

genauso viele Einträge wie Netzwerke. CIDR braucht hierfür nur einen Eintrag mit der entsprechenden Maskierung z. B. 193.147.0.0/17.

2.2.2 IPv6

Der Nachfolger von IPv4 ⇒ IPv6, anfänglich Internet Protocol Next Generation (IPng) genannt, wird entwickelt, seit man 1991/92 abschätzen konnte, dass der zur Verfügung stehende Adressraum nicht ausreichen wird[12].

Die wichtigsten Neuerungen kurz dargestellt:

- **Neues Headerformat**

  Einige IPv4 Headerfelder werden fallen gelassen oder für optional erklärt, um den Bandbreitebedarf des Headers zu minimieren und die Weiterverarbeitung zu vereinfachen.

- **Größerer Adressbereich**

  Eine IP Adresse hat 128 Bit statt der unter IPv4 üblichen 32 Bit. Damit sind theoretisch $3{,}4*10^{38}$ Kombinationen möglich. Dies wird genutzt, um eine effizientere, hierarchische Adressierungsstruktur zur Verfügung zu stellen. Autokonfiguration wird erleichtert. Mit der "anycast address" wird ein neuer Adresstyp eingeführt. Das ebenfalls neue "scope"-Feld gibt an, wie "multicast"-Datenverkehr zu behandeln ist.

- **Integrierte Sicherheit**

  Erweiterungen ermöglichen bessere Authentifizierung, Datenintegrität und Datenvertraulichkeit.

- **Bessere QoS-Unterstützung**

  Ein Flow Label Feld ermöglicht die Kennzeichnung von Datenpaketen, die eine spezielle Behandlung erfordern, sei es in der Weiterleitung oder der Art des Quality of Service (QoS) für z. B. Echtzeitanwendungen.

[12] siehe [7] Seite 1ff

- **Neues Protokoll für Interaktion von Nachbarknoten**

  Das *Neighbor Discovery* Protokoll für IPv6 verwaltet die Interaktion von Knoten auf der gleichen Verbindung (link). Es besteht aus einer Reihe von *Internet Control Message Protocol* Meldungen für IPv6 (ICMPv6). Neighbor Discovery ersetzt das broadcast-basierte ARP (Address Resolution Protocol), ICMPv4 Router Discovery und ICMPv4 Redirect durch die effizienten Multicast- und Unicastmeldungen von Neighbor Discovery.

- **Erweiterungsfähigkeit**

  Veränderungen in der Behandlung der IP Header Optionen erlauben ein wirtschaftlicheres Weiterleiten der Datagramme. Es gibt keine strikten Begrenzungen mehr für die Länge des Optionsfeldes. So bleibt man für künftige Erweiterungen offen. [8]

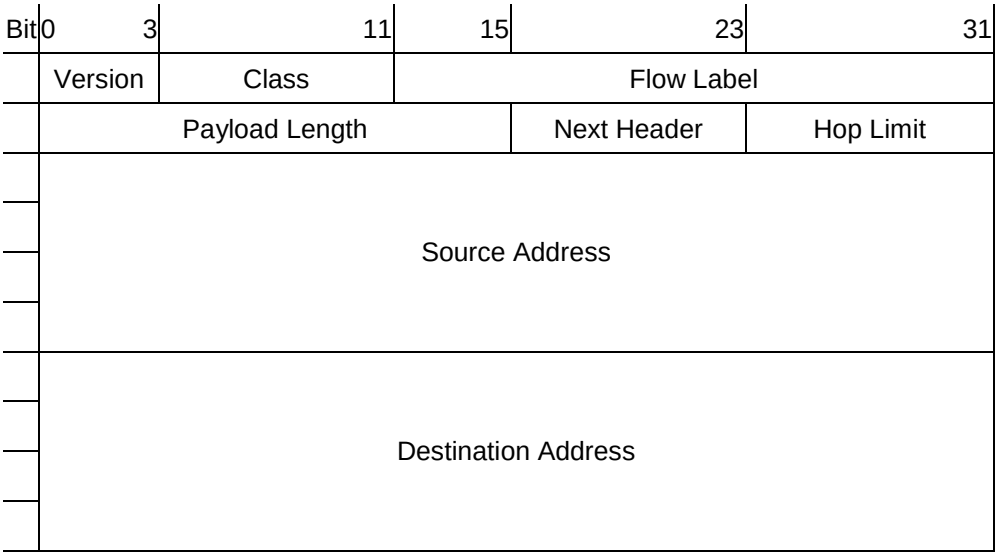


Bild 2.5 IPv6 Header

Version

Gibt wie schon unter IPv4 die Versionsnummer der folgenden Daten an und ist ebenfalls 4 Bit breit. Für IPv6 ist der entsprechende Wert 6 (0110).

Class

Ein neues und mittlerweile auf 8 Bit erweitertes Feld, das dazu dienen soll, verschiedene Klassen und Prioritäten von IPv6-Datagrammen zu unterscheiden. Zur Zeit der Erstellung dieser Diplomarbeit liefen noch etliche Untersuchungen, welche Klassifizierungen für den Datenverkehr sinnvoll seien.

Flow Label

Ein ebenfalls neues, 20 Bit breites Feld. Mit einem Flow Label sollen Datenpakete identifiziert werden, die von einer bestimmten Quelle an einen bestimmten Empfänger mit der Anforderung einer besonderen Behandlung gehen. Dies ist für Echtzeitanwendungen sinnvoll.

Payload Length

Das Feld Total Length in IPv4 gibt nun als Payload Length ("Nutz"-Daten) mit 16 Bit die Länge aller Daten nach dem Header an. Gibt es Extension Header[13], so zählen diese mit zur Payload Length.

Next Header

Ehemals das Protokollfeld, wird auch im 8 Bit Next Header der, auf den IP Header folgende, Protokolltyp angegeben. Nur kann dies jetzt zudem der Wert des Typs des ersten folgenden Erweiterungsheaders sein.

Hop Limit

Das 8 Bit Hop Limit Feld ist das frühere Time-to-Live Feld. Mit IPv6 hat man die übliche Praxis "Hops"[14] zu zählen (anstatt Sekunden) offiziell übernommen.

Source Address

128 Bit lange Quelladresse. Aufbau siehe unten.

Destination Address

128 Bit lange Zieladresse. Aufbau siehe unten.

Syntax von IPv6 Adressen

Die 128 Bit Adresse wird in Abschnitte von 16 Bit unterteilt, wobei jeder Block in eine vierstellige Hexadezimalzahl umgewandelt und durch Doppelpunkt getrennt wird. Diese Darstellung wird als Doppelpunkt-Hexadezimalformat bezeichnet.

[13] Erweiterungsheader, zwischen dem IPv6-header und den folgenden TCP od. UDP Nutzdaten
[14] Hop: Anzahl der durchlaufenen Router

Hier ein Beispiel einer binären 128 Bit Adresse, in 16 Bit Abschnitte unterteilt:

0011001011011110 1000000011000001 0000000001100000 0010111100111011
0000000110101010 0000000011111111 1111111000101000 1001110001111010

Nun dieselbe Adresse im Doppelpunkt-Hexadezimalformat:

32DE:80C1:0060:2F3B:01AA:00FF:FE28:9C7A

Führende Nullen in den einzelnen 16 Bit Blöcken können entfernt werden. Dabei muss jeder Block jedoch mindestens eine Ziffer aufweisen. Damit sieht obige Adresse wie folgt aus:

32DE:80C1:60:2F3B:1AA:FF:FE28:9C7A

Nun gibt es einige Adresstypen mit langen Nullfolgen. Fällt eine solche Nullfolge auf einen 16 Bit Block (und nur dann), kann sie zu "::" vereinfacht werden. Sind mehrere aufeinanderfolgende (und nur dann) 16 Bit Blöcke Nullfolgen, können diese ebenfalls durch "::" dargestellt werden. Die beiden nächsten Adressen bilden Beispiele hierfür:

FE80:0:0:0:2AA:FF:FE9A:4CA2 kann als FE80::2AA:FF:FE9A:4CA2 dargestellt werden und FF02:0:0:0:0:0:0:2 als FF02::2.

Die Komprimierung von Nullen kann in einer Adresse nur einmal angewendet werden. Es darf keine Adresse geben, die aussieht wie beispielsweise FF02::3::B. Hierbei weiß man nicht, ob sich hinter dem ersten "::" 3*16 Bit Nullfolge und hinter dem zweiten "::" 2*16 Bit Nullfolge verbirgt, oder umgekehrt.

Wie schon bei IPv4 mit CIDR eingeführt wurde, gibt es auch bei IPv6 die Möglichkeit, Präfixe anhand eines angehängten Schrägstrichs und der entsprechenden Bitanzahl zu identifizieren. Ein Beispiel für eine Präfixlänge von 22 Bit: 32DE:80C1:60:2F3B:1AA:FF:FE28:9C7A/22

IPv6 Adress Kategorien

Ein großer Unterschied zu IPv4 ist, dass jeder Schnittstelle nun mehrere Adressen zugewiesen werden können. Dies erleichtert das Adressmanagement sowie spezielle Routingfunktionen.

Die unter IPv4 bekannte *broadcast*[15] Adresse ist für IPv6 nicht mehr spezifiziert. Eine *multicast*[16] Adresse übernimmt deren Funktion. [9]

Es gibt 3 Adresstypen:

- **Unicast**

  Eine Unicastadresse bezeichnet eine einzelne Schnittstelle im Bereich des Unicastadresstyps. Mithilfe der entsprechenden Unicastroutingtopologie werden an eine Unicastadresse adressierte Pakete nur an diese einzelne Schnittstelle übermittelt.

- **Multicast**

  Mit einer Multicastadresse wird ein Satz Schnittstellen angesprochen, die typischerweise zu verschiedenen Systemen gehören. Hat ein Datagramm eine Multicastadresse als Empfänger, wird es an alle Schnittstellen mit dieser Adresse gesendet. Dies ist der Ersatz für die Broadcastadresse. Damit wird verhindert, dass ganze Netzwerke durch Broadcastmeldungen belastet werden.

- **Anycast**

  Eine Anycastadresse bestimmt einen Satz Schnittstellen, die typischerweise verschiedenen Knoten angehören. Ein an eine Anycastadresse gesendetes Datenpaket wird an einen einzigen Knoten, den "nächsten" mit dieser Anycastadresse, geliefert. Welcher als der "nächste" Knoten identifiziert wird, hängt vom verwendeten Routingprotokoll ab.

In dem riesigen Adressbereich sind spezielle Adressen spezifiziert, die oben angeführte Adresstypen identifizieren, reserviert sind für bestimmte Anwendungen oder für zukünftige Entwicklungen Raum lassen. Man muss jedoch nicht befürchten, dass dies gleich wieder zu einer Adressverknappung führt: über 70% des Adressraumes stehen weiterhin zur freien Verfügung.

[15] Rundspruch; Nachricht, die an alle am Netz angeschlossenen Schnittstellen gesendet wird
[16] Gruppenadressierung; Nachricht, die an mehrere am Netz angeschlossene Schnittstellen gesendet wird

Belegung des Adressraumes	Präfix (binär)	Anteil am Adressraum
Reserviert	0000 0000	$^1/_{256}$
Unbelegt	0000 0001	$^1/_{256}$
Reserviert für NSAP[17] Adressen	0000 001	$^1/_{128}$
Reserviert für IPX[18] Belegung	0000 010	$^1/_{128}$
Unbelegt	0000 011	$^1/_{128}$
Unbelegt	0000 1	$^1/_{32}$
Unbelegt	0001	$^1/_{16}$
Aggregatable Global Unicast Addresses	001	$^1/_{8}$
Unbelegt	010	$^1/_{8}$
Unbelegt	011	$^1/_{8}$
Reserviert für geographische Unicast Adressen	100	$^1/_{8}$
Unbelegt	101	$^1/_{8}$
Unbelegt	110	$^1/_{8}$
Unbelegt	1110	$^1/_{16}$
Unbelegt	1111 0	$^1/_{32}$
Unbelegt	1111 10	$^1/_{64}$
Unbelegt	1111 110	$^1/_{128}$
Unbelegt	1111 1110 0	$^1/_{512}$
Verbindungslokale Adressen	1111 1110 10	$^1/_{1024}$
Standortlokale Adressen	1111 1110 11	$^1/_{1024}$
Multicastadressen	1111 1111	$^1/_{256}$

Tabelle 2.1 Aktuelle Zuordnung des IPv6 Adressbereichs

Für die geographischen Unicastadressen gibt es noch keine Verwendung.

Aggregatable Global Unicast Addresses

Die zusammenfassbaren globalen Unicastadressen sind anhand der ersten drei Bits 001 erkennbar. Danach folgt ein 13 Bit langer *Top Level Aggregator* (TLA). Im Vergleich zu unserer Hierarchie im Telefonsystem entsprechen die ersten drei Bits der Länderkennzahl, z. B. +49 für Deutschland, während die folgenden 13 Bits mit der Vorwahl, z. B. 069 für Frankfurt a.M., verglichen werden können, wobei bei diesen IP-Adressen keine derartige geographische Zuordnung vorgenommen wird. Auf den TLA folgt ein 32 Bit langer *Next Level Aggregator* (NLA), der der zentralen Nummer einer Firma gleichkommt. Der darauf folgende *Site Local Aggregator* (SLA) kann der Durchwahl gleichgesetzt werden und umfasst 16 Bit. Es folgen noch 64 Bit Interface ID, die erst eine eindeutige Zuordnung zu einer Schnittstelle ermöglichen.

[17] Network Service Access Point: Zugriffspunkt zu einem Netzwerk-Dienst
[18] Internetwork Packet Exchange, ein Netzwerk Protokoll von Novell definiert

3	13	32	16	64 Bits
001	TLA	NLA	SLA	Interface ID

Tabelle 2.2 Format einer zusammenfassbaren globalen Unicastadresse

Diese Struktur dient dazu, Routingtabellen klein zu halten. Router müssen nur Tabellen führen, in denen für jeden TLA, der nicht der eigene ist, der nächste Router eingetragen ist. Für den eigenen TLA-Bereich müssen die Routingtabellen jedoch alle Einträge der NLAs führen, die zu diesem TLA zusammengefasst werden. Genauso wird mit den Einträgen für die SLAs verfahren.

Nicht spezifizierte Adresse

Die *unspecified address* besteht aus 16 Nullbytes und kann nur von einer Station benutzt werden, die noch nicht mit einer regulären Adresse konfiguriert wurde. Es gibt einige Kontrollnachrichten, die sie auch noch benutzen können, sofern keine tatsächliche Adresse verfügbar, aber erforderlich ist. Die nicht spezifizierte Adresse wird niemals eine Zieladresse sein.

Loopback Adresse

Knoten können mit der *loopback address* 0:0:0:0:0:0:0:1 IPv6 Datagramme an sich selbst senden.
Genau wie die unspecified address kann sie keiner Schnittstelle zugeordnet werden.

IPv4-basierte Adresse

Werden einer IPv4 Adresse (32 Bit) 96 Null-Bits vorangestellt, so erhält man eine gültige IPv6 Adresse. Für SIIT (siehe Kapitel 4.3) war die Einführung einer weiteren IPv6-Sonderadresse notwendig. Diese wird als IPv4-translated-address bezeichnet. Typischerweise werden solche Adressen in gemischter Schreibweise (hexadezimal und dezimal) dargestellt. So ist ::10.0.0.1 eine gültige Schreibweise für eine IPv6 Adresse, den dezimalen Teil erkennt man an der Trennung durch Punkte, den hexadezimalen an der Trennung durch Doppelpunkte.

Standortlokale Adresse

Site local addresses werden durch die Präfix 1111 1110 11 gekennzeichnet und sind für den Gebrauch zwischen 2 Stationen innerhalb einer Site[19] gedacht. Ihre Einmaligkeit ist nicht nach Außen garantiert, sie können nicht ins Internet geroutet werden.

[19] bestimmtes Informationsangebot, das unter einer gemeinsamen IP Adresse erreichbar ist

Verbindungslokale Adresse

Eine *link local address* beginnt mit der Präfix 1111 1110 10 und wird von Stationen benutzt, die weder eine Anbieter basierte (provider-based), noch eine standortlokale Adresse erhalten haben. Diese Adressen sind nur für eine Verbindung oder dasselbe lokale Netzwerk definiert und werden von Routern nicht weitergeleitet. Sie werden hauptsächlich zu Konfigurationszwecken benutzt.

Multicast Adresse

Zunächst ein wenig Allgemeines zum Multicasting:

Multimedia Anwendungen wie z. B. Audio - Videokonferenzen im Netz oder auch das Abspielen entsprechender Daten in Echtzeit erfreuen sich immer größerer Beliebtheit. Diese Anwendungen basieren jedoch auf einfachen Punkt-zu-Punkt Verbindungen. Greifen nun viele Teilnehmer gleichzeitig auf dieselben Ressourcen zu, führt dies zu einer Überlastung von Servern, Netzen oder Routern. Um dem entgegen zu wirken, wurden 1988 rein formell gesehen mit der Definition der Class D Adressen und des IGMP dem Internet Protokoll Multicastfähigkeiten hinzugefügt. Weiter verbreitet wurde diese Art der Gruppenkommunikation, als 1992 das Multicast Backbone (MBONE)[20] ins Leben gerufen wurde.

Eine Multicastadresse bezeichnet keinen einzelnen Internetknoten oder gar eine Person, sondern eine Gruppe von Schnittstellen, wie weiter oben bereits erwähnt. Ein Sender schickt nicht an jeden Teilnehmer eine Kopie seiner Daten, sondern sendet nur einmal an die Multicastadresse. Multicastpakete werden über eine Art virtuelle Baumstruktur zu den Gruppenteilnehmern geschickt. Die Daten werden nur an den Knoten zu denjenigen Ästen hin vervielfacht, an denen Empfänger vorhanden sind. Somit ist gewährleistet, dass keine Kopien der Daten unnötigerweise den gleichen Netzabschnitt durchziehen. Die Datenpakete einer Videokonferenz zwischen Europa und USA beispielsweise an jeden Zuschauer einzeln zu verschicken, hätte den Zusammenbruch der internationalen Leitungen zur Folge.

Das Deutsche Forschungsnetz (DFN), in dem das MBONE aufgesetzt wurde, hat seit April 2000 die IP Multicastfunktionalität in alle Netzknoten des Wissenschaftsnetzes integriert. Nun heißt der entsprechende Service nicht mehr "MBONE" sondern "DFN Multicast". [16]

[20] experimentelles Kernnetz aufgesetzt auf das Internet um multicast Anwendungen zu testen

Zum Aufbau einer Multicastadresse:

8	4	4	112 Bits
1111 1111	Flgs	Scop	Group ID

Tabelle 2.3 Aufbau einer Multicastadresse

Die ersten 8 Bits sind immer auf Eins gesetzt. Von den folgenden 4 Bits, *Flags* genannt, ist bisher nur das vierte Bit spezifiziert, die anderen sind Reserve und auf Null gesetzt. Das vierte Bit wird T genannt, was für *Transient*[21] steht. Ist es Eins gesetzt, zeigt es an, dass es sich um eine temporäre Adresse handelt, die bei Bedarf angefragt wird. Mit dem Schließen der entsprechenden Anwendung wird diese Adresse wieder freigegeben. Ist T = 0, so indiziert das eine fest vergebene Multicastadresse, die ständig bestehen bleibt.

Auf die Flags folgt das *Scope*-Feld mit 4 Bit, welches dazu dient, den Gültigkeitsbereich der Multicastgruppe festzulegen. Es sollen schließlich keine gruppeninternen Daten plötzlich im weltweiten Internet stehen.

Hier eine Tabelle von Werten, wie sie bereits im MBONE, also unter IPv4 genutzt werden:

0	Reserviert
1	Knotenlokale Gültigkeit
2	Verbindungslokale Gültigkeit
3	Nicht vergeben
4	Nicht vergeben
5	Standortlokale Gültigkeit
6	Nicht vergeben
7	Nicht vergeben
8	Organisationslokale Gültigkeit
9	Nicht vergeben
A	Nicht vergeben
B	Nicht vergeben
C	Nicht vergeben
D	Nicht vergeben
E	Globale Gültigkeit
F	Reserviert

Tabelle 2.4 Scope-Feld Werte einer Multicastadresse

[21] kurzzeitig

Der auf das Scope-Feld folgende 112 Bit umfassende *Group Identifier* wird aufgrund von Kompatibilitätsaspekten mit IPv4 in den ersten 80 Bit immer auf Null gesetzt, so dass die folgenden 32 Bit mit den IPv4 Adressen einhergehen können. Das beschränkt zwar den Adressraum für Multicastgruppen, ist aber notwendig, um Kollisionen zu vermeiden, solange IPv4 noch genutzt wird.[22]

Des weiteren wird dieses Feld noch in verschiedene Bereiche geteilt, um Gruppenkonflikte zu vermeiden:

- Ein Adressbereich, der von der IANA[23] registriert ist
- Ein Adressbereich, der von Neighbor Discovery Prozessen benötigt wird
- Und mehrere Adressbereiche, die für die verschiedenen Gültigkeitsbereiche der temporären Adressen zuständig sind

Im Anhang befindet sich eine komplette Liste der vergebenen Multicastadressen. [IPv6 Multicastadressen]

Um eine Multicastgruppe aufzusetzen oder daran teilzunehmen, wird im MBONE häufig das *Session Directory Tool* verwendet, welches eine temporäre Multicastadresse zuweist sowie öffentliche und private Multicastsessions listet. [17]

Das Internet Group Management Protocol (IGMP) ist ein weiteres Protokoll, das Multicastfunktionalitäten ermöglicht. Es dient Hosts und Router dazu, ihre Mitgliedschaft an Multicastgruppen im Netzwerk bekannt zu geben. [18]

Um Multicast zu betreiben, müssen die teilnehmenden Endgeräte (Hosts) sowie die entsprechenden Router multicastfähig sein. Dies ist mittlerweile bei neuen Geräten der Fall, da Multicast auch eine Funktion von IPv6 ist.

Anycast Adresse

Der Gebrauch von Anycastadressen ist immer noch ein Thema von Forschungsarbeiten, obwohl das zugrunde liegende Prinzip einfach und weiter oben bereits beschrieben ist. Eine IPv6 Adresse wird als Anycastadresse bezeichnet, wenn sie einer oder mehreren Netzwerkschnittstellen zugewiesen wird. Es gibt kein spezielles Anycastadressformat, da eine Unicastadresse, die mehreren Schnittstellen zugewiesen wird, automatisch eine Anycastadresse ist. Dies muss allerdings dem Netzknoten per Konfiguration explizit bekannt gegeben werden. [9]

[22] siehe [7] Seite 55ff
[23] Internet Assigned Numbers Authority

Mittlerweile sind von der IANA Adressen innerhalb eines jeden Subnetzes für Anycastzwecke reserviert. Dies sind die 128 höchsten Werte des Interface Identifiers, die zur Bildung von Subnet Anycast Adressen zur Verfügung stehen. [19]

n Bits	121-n Bits	7 Bits
Subnet prefix	1111111...111111	Anycast ID
	Interface Identifier Field	

Tabelle 2.5 Subnet Anycast Address Format

Folgende Anycast Identifier sind im Moment für die Subnet Anycast Adressen definiert:

Decimal	Hexadecimal	Description
127	7F	Reserved
126	7E	Mobile IPv6 Home-Agents anycast
0-125	00-7D	Reserved

Anycastadressen können z. B. genutzt werden, wenn ein bestimmter Service in Anspruch genommen wird, den mehrere Server anbieten. Es muss dann nicht bei jedem möglichen Nutzer eine Liste dieser Server manuell eingepflegt werden, sondern mittels einer Anycastadresse erreicht der Nutzer den nächsten Server mit diesem Dienst.

Oder Daten sollen über einen speziellen ISP versandt werden. Dann kann man mittels einer Anycastadresse in der *Source route* das Routing über diesen ISP erzwingen, ohne dabei den gesamten Verkehr einem einzigen Router zu zumuten.

2.2.3 TCP / UDP

2.2.3.1 Transmission Control Protocol (TCP)

Das TCP arbeitet in der Transportschicht (Schicht 4) des OSI-Referenzmodells und ist im Internet weit verbreitet. TCP ist ein verbindungsorientiertes und zuverlässiges Transportprotokoll. Verbindungsorientiert ist es, weil es vor der Übertragung der Nutzdaten eine virtuelle Verbindung zwischen den beiden End-Systemen herstellt.

Eine TCP-Übertragung erfolgt in drei Phasen:

1. **Verbindungsaufbau**
2. **Datenübertragung**
3. **Verbindungsabbau**

Seine Aufgabe ist, sicherzustellen, dass ein von der sendenden Anwendung übergebener Datenstrom zuverlässig bei der empfangenden Anwendung auf dem Zielendgerät am anderen Ende des Netzwerks abgeliefert wird. Zuverlässig bedeutet, dass der im Empfänger übergebene Datenstrom eine Kopie des Originals sein muss. Ebenso muss die korrekte Reihenfolge der Daten wiederhergestellt werden.

Damit es seine Aufgabe erfüllen kann, teilt TCP den von der Anwendung übergebenen Datenstrom in IP-Datagramme auf, versieht die Datagramme mit Ziel- und Absenderadresse, nummeriert sie, führt eine CRC Prüfung aus und fügt die CRC-Information in das jeweilige CRC-Feld im Header eines Datenpaketes ein. Mit diesen Informationen versehen, kann jedes IP-Datagramm im Netzwerk eindeutig identifiziert und auf seine Integrität geprüft werden.

Es ist wichtig zu verstehen, dass TCP eine größere Anzahl von IP-Datenpaketen hintereinander versendet, ohne auf eine Empfangsquittung zu warten. Die Anzahl der darin enthaltenen Bytes wird Fenster genannt. Sie ist ein kritischer Parameter für die optimale Funktion von TCP in einem komplexen Netzwerk.

Das empfangende TCP schickt ein Quittungs-Datagramm an den Absender. Diese Empfangsquittung enthält u.a. die Nummer des nächsten zu erwartenden Bytes, so dass das sendende TCP im Laufe der Übertragung genau informiert wird, welche Pakete erfolgreich übertragen wurden. War der ursprüngliche Datenstrom umfangreich, so durchqueren Datenpakete und Quittungen gleichzeitig und unabhängig voneinander das Netz. So wird sichergestellt, dass TCP einen hohen Datendurchsatz in einem komplexen, weltweiten Netz erzielt, bei dem die Zeit zwischen dem Senden eines bestimmten Datenpakets und dem Empfang der dazugehörenden Quittung sehr lang sein kann. Diese Zeit wird Latenz genannt.

Wenn die dem aktuellen Fenster entsprechende Retransmission Time ohne Empfang einer Quittung abgelaufen ist, d.h. nach dem Versand der im TCP-Verbindungsaufbau ausgehandelten Anzahl Datenbytes, hält TCP die Übertragung an. Das sendende TCP unterstellt dann, dass irgendwo in der Übertragungskette ein oder mehrere Bytes verloren gegangen sind und wiederholt sämtliche Datenpakete mit einer Laufnummer größer als die des letzten quittierten IP-Bytes.

TCP garantiert einen optimalen Datendurchsatz durch die automatische Anpassung von Fenstergröße und Wiederholverzögerung an den Datendurchsatz des Netzes und die Latenzzeit. Ist das Fenster zu klein, verschenkt TCP Datendurchsatz, d.h. es nützt die gegebene Bandbreite schlecht aus. Ist das Fenster zu groß, kann TCP nicht schnell genug auf Netzfehler reagieren, was ebenso zu verschenktem Datendurchsatz führt. TCP überwacht und analysiert daher ständig den Daten- und Quittungsverkehr, um die Parameter für Fenstergröße und den Retry-Timer optimal zu justieren. TCP zeigt seine beste Leistung, wenn Durchsatz und Latenz über einen größeren Zeitraum konstant bleiben.

Der TCP-Header hat eine Länge von mindestens 20 Byte, folgt unmittelbar nach dem IP-Header und hat folgenden Aufbau:

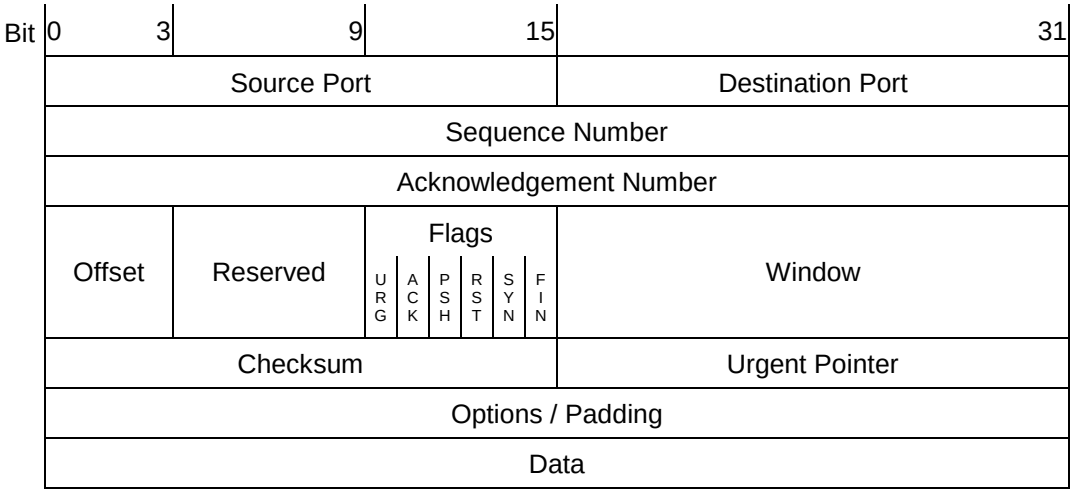


Bild 2.6 Aufbau eines TCP-Header

Die Felder haben folgende Bedeutung:

Source Port

Portnummer (Transportebene) des Absenders des TCP-Pakets. Dieses 16-Bit-Feld beinhaltet den Quell-Port der TCP-Anwendung, welche den Frame erzeugt hat.

Destination Port

Portnummer (Transportebene) des Ziels des TCP-Pakets. Hier steht der Ziel-Port der TCP-Anwendung, die den Frame empfangen soll. Es ist ebenfalls 16 Bit groß.

Sequence Number

Die Sequence Number (32 Bit) nummeriert das jeweils erste Daten-Byte innerhalb des gesamten Datenstroms und dient somit der Absicherung des Datenflusses. Beim Verbindungsaufbau wird ein zufälliger Wert für die Sequenznummer gewählt.

Acknowledgement Number

Das Feld Acknowledgement Number (32 Bit) dient zur Bestätigung eines empfangenen TCP-Pakets. Die Bestätigung wird an den Sender zurückgesendet, indem zuvor in dieses Feld die inkrementierte Sequenznummer (Sequence Number) des entsprechenden empfangenden TCP-Segments eingetragen wird. Die inkrementierte Sequenznummer setzt sich aus der letzten Sequenznummer und der Anzahl der Bytes zusammen.

Offset

Hier steht die Länge des TCP-Headers in 32-Bit-Blöcken, weil das Options-Feld im Header variabel lang sein kann. Der TCP-Header hat eine Länge von mindestens 20 Byte.

Reserved

Dieses 6-Bit-Feld wird z. Z. nicht genutzt und enthält binäre Nullen.

Flags

Flags (6 Bit) bieten die Möglichkeit, sechs definierte Ereignisse innerhalb des Headers zu kennzeichnen. Sie dienen der Kommunikationssteuerung. Sind die nachfolgenden Flags gesetzt, haben sie folgende Bedeutung: [14]

- URG: Urgent Pointer

  Markiert Vorrangdaten und zeigt an, dass das Feld im TCP Header beachtet werden muss.

- ACK: Acknowledgement

  Zeigt an, dass das Paket eine gültige Quittung enthält. Wenn keine neuen Daten von der Gegenseite empfangen wurden, so wird im neu gesendeten Paket die vorherige Quittungsnummer wiederholt. Nach Verbindungsaufbau enthält jedes Paket eine gültige Quittungsnummer.

- PSH: Push

  Teilt dem Empfänger mit, dass die Daten sofort an das höhere Protokoll weitergegeben werden müssen. Bei der Übertragung von Telnet-Parametern wird dieser Mechanismus immer eingesetzt.

- RST: Reset

  Der Sender möchte die Verbindung zurücksetzen, da er einen Fehler erkannt hat.

- SYN: Synchronisation

  Verbindungsaufbauwunsch, der quittiert werden muss. Der Verbindungsaufbau muss beidseitig erfolgen. SYN verbraucht eine Sequenznummer.

- FIN: Final

  Verbindungsabbau, der quittiert werden muss. Verbindungsabbau muss beidseitig erfolgen. FIN verbraucht eine Sequenznummer.

Window

Das Feld Window dient der Flusskontrolle. TCP steuert die Geschwindigkeit, mit der Pakete gesendet werden, indem die Anzahl der Nachrichten unterwegs durch die Fenstergröße im Header eingeschränkt wird (max. 65.535 Byte).

Checksum

16-Bit-Prüfsumme über den TCP-Header, die IP-Quell- und Ziel-Adresse, dem Protokoll-Identifizierer und der Angabe über die Länge des TCP-Segments. Während der Berechnung des Feldes ist der Wert dieses Feldes und des Datenfeldes gleich Null zu setzen.

Urgent Pointer

Der Wert im Urgent-Pointer-Feld (16 Bit) weist auf das Ende der Vorrang Daten innerhalb des TCP-Segments hin, sofern das URG-Flag gesetzt ist. Es stellt einen Offset-Wert dar, der in Addition mit der Sequencenumber die beschriebene Datenposition identifiziert.

Options / Padding

Hier wird beim Verbindungsaufbau die maximale Segmentgröße festgelegt. Diesem Feld folgen die Optionsdaten.

Wenn Optionen gesetzt sind, wird das Feld bis zu einem Vielfachen von 32 Bit aufgefüllt, sofern diese Grenze noch nicht erreicht wurde, damit im Feld Offset der Beginn des Datenfeldes korrekt angegeben werden kann.

2.2.3.2 User Datagramm Protocol (UDP)

UDP ist ein verbindungsloses und ungesichertes Transportprotokoll. Verbindungslos bedeutet, dass UDP die IP-Datagramme zu den Ports der Anwendungs-Programme weiterleitet, wobei jedes Datagramm unabhängig von den anderen zugestellt wird, d.h. ohne die Reihenfolge ihres Sendens zu beachten. Das Protokoll ist ungesichert, weil es keine Bestätigung über die korrekte Übertragung des Datagramms zum Sender schickt. Diese Aufgabe kann von höheren Protokollschichten erbracht werden.

UDP eignet sich gut für Multicast und überträgt Daten auf effiziente Weise ohne Rücksicht auf verlorengegangene Pakete zu den Zieladressen. Diese Eigenschaft ist sehr wichtig für die Übertragung in Echtzeit, bei der es meist mehr auf Schnelligkeit und weniger auf den kompletten Erhalt aller Pakete ankommt.

UDP besitzt einen Header von acht (8) Byte und hat folgenden Aufbau:

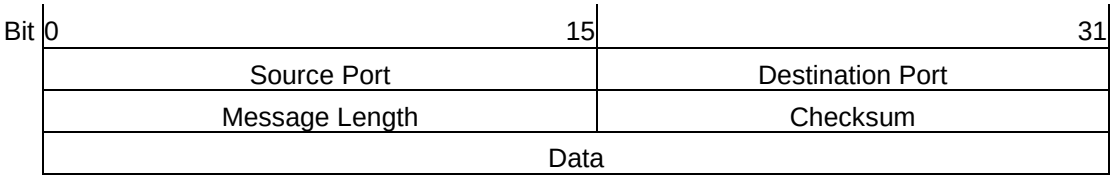


Bild 2.7 Aufbau eines UDP-Headers

Die Felder haben folgende Bedeutung:

Source Port

Portnummer des sendenden Prozesses (16 Bit), vergleiche mit TCP.

Destination Port

Portnummer des empfangenden Prozesses (16 Bit), vergleiche mit TCP.

Message Length

Der Wert dieses Feldes mit einer Länge von 16 Bit bezeichnet die UDP-Datagrammlänge inklusive Header und Daten in Byte.

Checksum

16-Bit-Checksumme der Daten und der Header, inklusive IP-Adressen (Pseudo-Header).

Nachfolgende Tabelle zeigt die Vorteile, Nachteile und Einsatzmöglichkeiten beider Protokolle im Vergleich.

	Pro	Contra	Einsatz
UDP	Schnelle Datenübertragung Einfache Implementierung	Ungesicherte Datenübertragung	Immer dann, wenn eine einfache Implementierung nötig ist und die Kontrolle von Anwendung oder User vorgenommen werden kann (SNMP,DNS)
TCP	Flusskontrolle Sichere Datenübertragung Zuverlässiges Protokoll	Aufwendige Implementierung	Immer dann, wenn Daten ohne Kontrolle der Anwendung / des Users sicher transportiert werden müssen (FTP, SMTP)

Tabelle 2.6 Vergleich von TCP / UDP

2.3 Routing im Internet

Datenpakete, die über Netzwerke ausgetauscht werden, werden durch Router vermittelt. Jeder Router führt Tabellen mit Einträgen über Nachbarstationen in anderen Netzwerken, bzw. Schnittstellen innerhalb des eigenen Netzes. Aufgrund solcher Tabellen werden Wegewahlentscheidungen getroffen. Diese Tabellen müssen deswegen ständig aktualisiert werden, da mögliche Wege wegfallen und/oder hinzukommen. Router kommunizieren mittels Routingprotokollen. Dies erzeugt administrativen Datenverkehr in Netzen.

1991/92 hat man realisiert, dass nicht nur der Adressraum des IPv4 knapp wird, sondern auch die Routingtabellen und der damit zusammenhängende Datenverkehr ungeahnte Ausmaße annimmt. Neue, effizientere Routingmechanismen werden entwickelt, um das Internet als schnelles Medium zum Datenaustausch attraktiv zu erhalten. Ganz besonders wichtig wird dies im Hinblick auf die Markteinführung des *Universal Mobile Telecommunications System* (UMTS), da dann u.a. Mobilfunk durch Netzwerke geroutet wird.

Mit CIDR[24] hat man eine zeitweilige Entspannung in der Dringlichkeit dieses Problems erreicht. Ebenso sind die neu definierten Adresstypen unter IPv6 für effizientes Routing

[24] CIDR: Classless Inter-Domain Routing

geeignet. Jüngsten Beobachtungen zufolge gibt es jedoch Bewegungen, die dieses System untergraben: *Multihoming*. Multihoming bedeutet, dass ein Kunde nicht mehr nur Serviceleistungen (Zugang zum Internet u.m.) von einem *Internet Service Provider* (ISP) erhält, sondern von mehreren. Dadurch nimmt gerade der administrative Datenverkehr, und somit die Zahl der Routingeinträge, wieder in fast exponentiellem Anstieg zu. Aktuelle Graphen dazu entnehmen wir: http://www.telstra.net/ops/bgptable.html

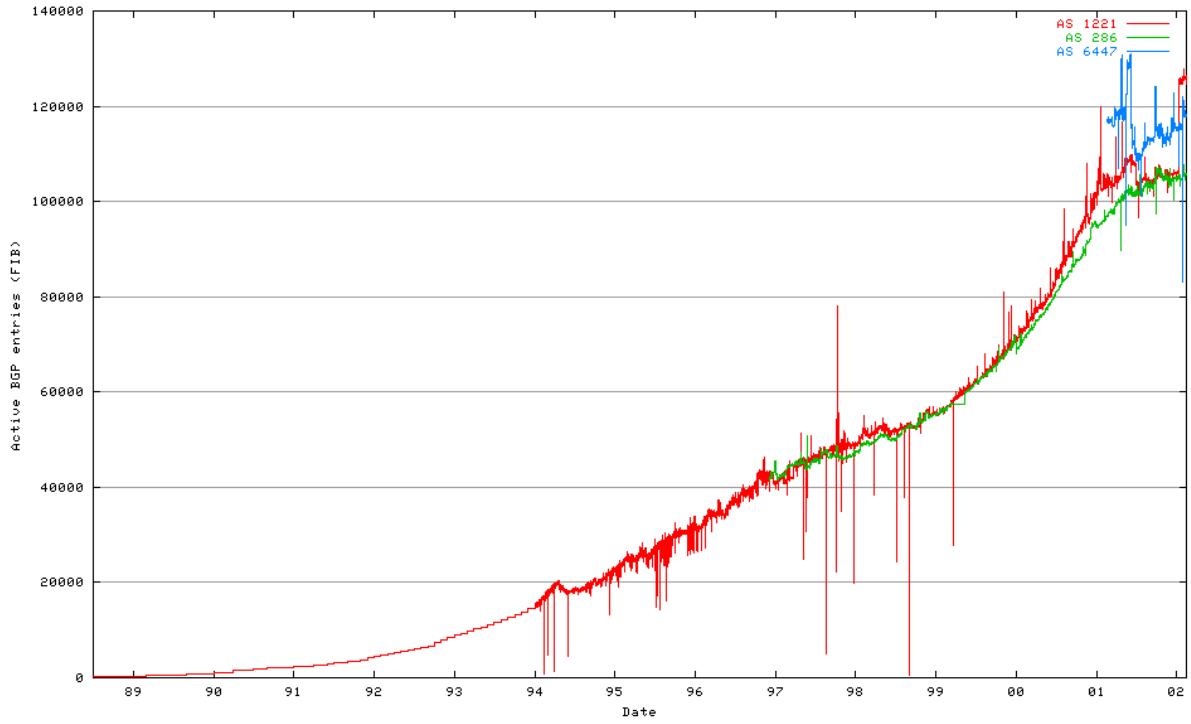


Bild 2.8 BGP-Einträge aktuell vom 14.02.2002 mit Nennung von Autonomen Systemen (AS)

AS 1221 steht für Telstra – ein Telefon und Internet Service Provider aus Australien

AS 286 steht für KPNQwest – ein Internet Service Provider aus den Niederlanden

AS 6447 steht für Route-Views.Oregon-ix.net - University of Oregon Route Views Project

Im Bild sind die BGP-Einträge des Telstra-Netzes seit 1988 dargestellt (rote Kurve). Es ist zu entnehmen, dass aktuelle Routingtabellen knapp 105.000 Einträge haben. Zu Beginn des Internetbooms 1994 betrug die Größe der Tabellen etwa ein Sechstel davon, - ca. 18000 Einträge. Die Entwicklung der Routingtabellen bei KPNQwest (grüne Kurve) weicht kaum von der des Telstra-Netzes ab. Die Entwicklung in dem Projekt der University of Oregon scheint sich momentan bei etwas über 150000 Routen einzupendeln, aber das müsste man noch weiter beobachten.

Routingprotokolle werden eingeteilt in *Interior Gateway Protocols* (IGP) für den netzwerkinternen Datenaustausch und *Exterior Gateway Protocols* (EGP) für den Datenverkehr zwischen verschiedenen Autonomen Systemen. Ein Autonomes System ist als ein Netzwerk definiert, das unter einer technischen und administrativen Kontrolle steht, was meist einer Organisation entspricht[25].

2.3.1 IGP

Zur Gruppe der *Interior Gateway Protocols* zählen Routingprotokolle wie RIP, OSPF und IS-IS. Diese Protokolle gibt es für IPv4 und sind bzw. werden noch weiter entwickelt für IPv6.

IGPs regeln den dynamischen Austausch von Routeninformationen innerhalb Autonomer Systeme (AS). Alternativ können auch statische Routen verwendet werden, welche in der Pflege aufwendig sind, da sie von Hand konfiguriert werden müssen.

2.3.1.1 RIP

Das *Routing Information Protocol* (RIP) arbeitet mit einem Bellman-Ford Algorithmus[26] auf Basis eines Distance Vector Algorithmus. Die Wegewahl wird anhand der Anzahl der Hops bestimmt, die ein Datenpaket auf seinem Weg zur Zieladresse passieren muss. Ein Router wählt für ein Paket den Weg mit der geringsten Anzahl an Hops.

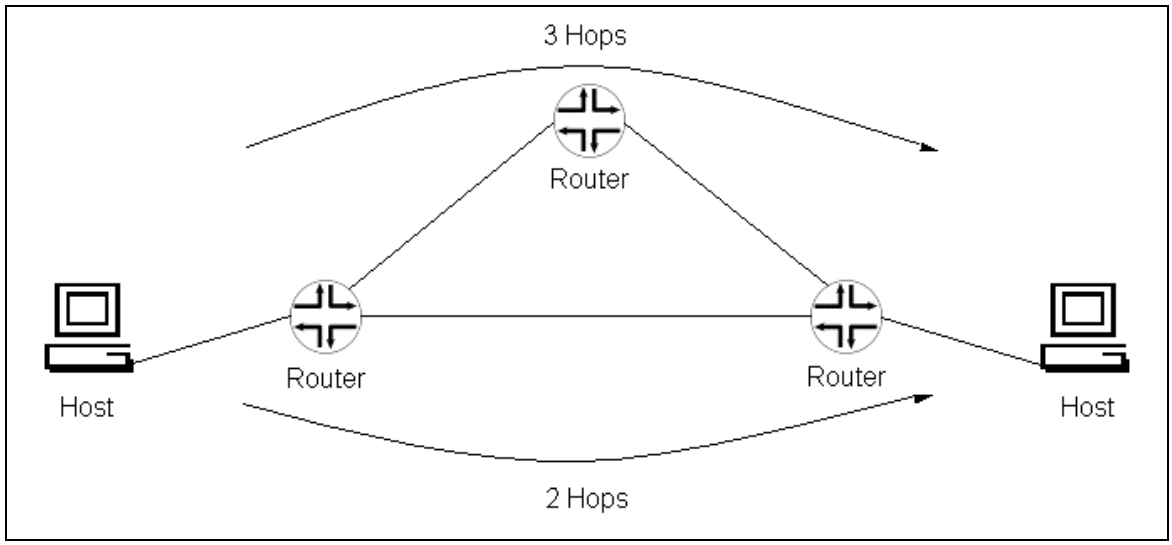


Bild 2.9 Wegewahl durch Hopcount

[25] vgl. [12] Seite 18
[26] bewertet "Entfernungen" aufgrund der Anzahl an Zwischenstationen

Bei RIP sendet jeder Router in konfigurierbaren Zeitintervallen eine Broadcast-Anfrage an alle angeschlossenen Stationen. Die anderen Router antworten darauf, indem sie ihre Routingtabellen zurücksenden. Der Router, der diese Tabellen erhält, ergänzt daraufhin mit ihnen seine eigene Routingtabelle. Antwortet ein Router nicht innerhalb einer vorgegebenen Zeit auf eine Broadcast-Anfrage, wird der Weg über diesen Router automatisch auf einen Hop-Wert von 16 gesetzt, womit er nicht mehr verfügbar ist. Bis eine Änderung der Netztopologie dann in jeder Routingtabelle eingetragen ist, können mehrere Minuten vergehen. Man spricht in diesem Zusammenhang von einem hohen Konvergenzzeitraum.

RIP eignet sich nicht für komplexe Netzwerke, da es maximal eine Distanz von 15 Hops zwischen zwei Punkten verarbeiten kann. Eine Zieladresse, die 16 oder mehr Hops entfernt ist, gilt als nicht erreichbar.

Da die Pfadkosten in Hops berechnet werden, wird immer die kürzeste Route gewählt, auch wenn es nicht die schnellste ist.

Aufgrund der Nachteile von RIP wird es immer mehr von OSPF ersetzt, welches über eine umfangreichere Funktionalität verfügt.

2.3.1.2 OSPF

Typisch für *Open Shortest Path First* (OSPF) ist, dass jeder Verbindung zwischen zwei Routern ein Kostenwert zugeordnet werden kann[27]. Anhand des *Dijkstra-Algorithmus* (siehe Glossar) wird dann für ein IP-Paket der Pfad ausgewählt, über den eine Zieladresse mit den geringsten Kosten erreichbar ist. Die Kosten für eine Verbindung werden dem Router vom Netzwerkadministrator mitgeteilt. Meist wird die Verbindungsrate als Kostengrundlage genommen (siehe Bild 2.10). Defaultmäßig ist bei Routern heute die 100Mbit/s als Berechnungsgrundlage eingestellt. Es können auch zusätzlich Lastaufkommen, Verzögerung oder Betriebskosten einer Verbindung zur Kostenberechnung hinzugezogen werden. Das könnte dann zur Folge haben, dass ein Weg gewählt wird, der über mehr Hops führt, aber geringere Kosten aufweist.

[27] mittels des sogenannten *Link State Algorithmus*

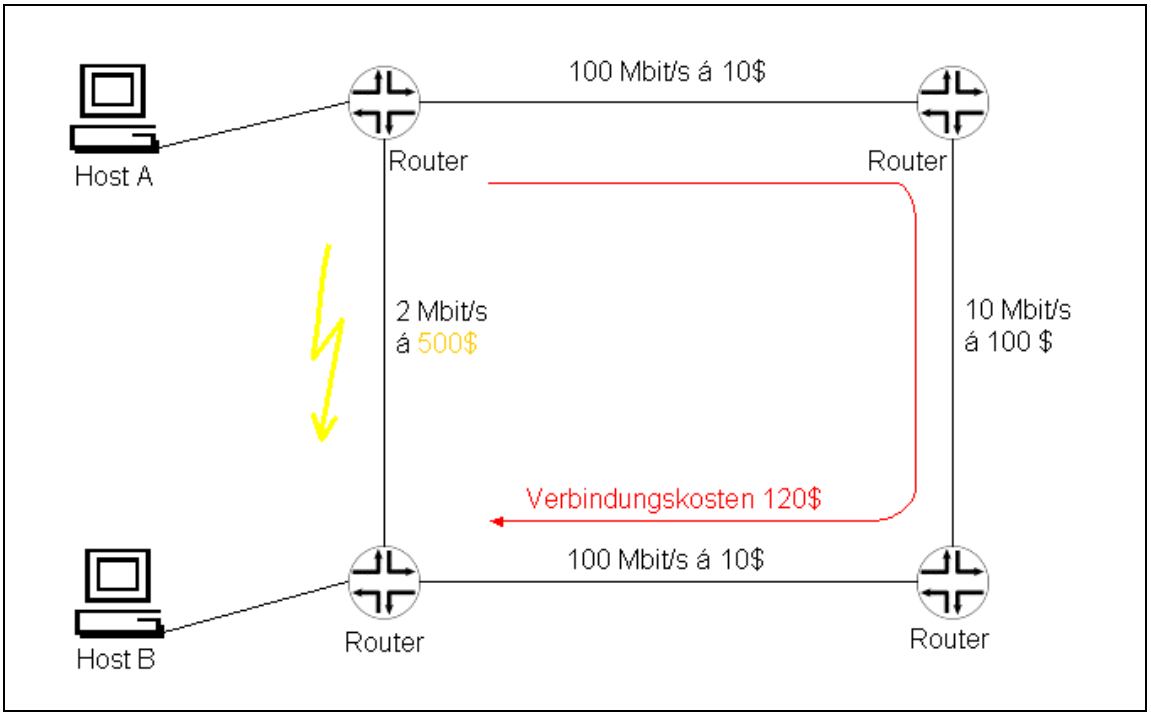


Bild 2.10 Wegewahl durch Kosten bei OSPF

In das OSPF-Protokoll wurde die Möglichkeit integriert, anhand eines jeweiligen Dienstes zu routen. Mit der OSPF-Version für IPv4 untersucht der Router das TOS-Feld im IP-Header eines zu routenden Datenpaketes und transportiert die Daten über die für diesen Dienst vorgegebene Route. Die Pakete der verschiedenen Dienste können dadurch über unterschiedliche Wege geroutet werden. Mit IPv6 werden solche Aufgaben im Flow Label- und Class-Feld übernommen.

OSPF ist verbindungsorientiert, es wird vor dem Austausch von Daten eine Verbindung zwischen Sender und Empfänger aufgebaut. Bei Veränderung der Netztopologie werden nur die Änderungen in den Routingtabellen der Router ausgetauscht. [11] Mit OSPF ist auch Loadbalancing möglich. Wenn zwei oder mehr Wege zu einem Ziel existieren, die alle die gleichen Kosten haben, wird die Datenlast mittels des *Round-Robin*-Verfahrens (siehe Glossar) auf diese Wege aufgeteilt. Diese OSPF-Funktion wird auch *Equal-Cost Multipath* genannt.

Da dieses Protokoll bereits unter IPv4 viel genutzt und immer weiter entwickelt wurde, sind für die IPv6-Fähigkeit im wesentlichen nur Änderungen notwendig, die das größere Adressformat unterstützen[28].

[28] vgl. [7], Seite 73 f

2.3.1.3 IS-IS

Intermediate System to Intermediate System (IS-IS) ist eine Alternative zu OSPF, die vor allem bei großen Service Providern und ISPs Einsatz findet. Im Sinne der OSI-Notation bezeichnet ein IS einen Router. IS-IS routet optional aufgrund von Verzögerungszeiten, Verbindungskosten und Fehlerraten. Dies befähigt das Protokoll auf QoS-Anforderungen zu reagieren. IS-IS basiert auf dem Standard DECnet Phase V, den die Digital Equipment Corporation 1991 entwickelt hat. Anfänglich lief IS-IS nur in *ConnectionLess Network Protocol* (CLNP) Netzwerken, mittlerweile unterstützt es auch IP. Beschrieben ist IS-IS im ISO Standard 10589, welcher mit RFC1142 wieder veröffentlicht wurde.

2.3.2 EGP

Zur Gruppe der EGPs zählt man Routingprotokolle, die zwischen Autonomen Systemen (AS) ablaufen. Man braucht sie, um Daten in andere Netzwerke zu verschicken. Sie haben ähnliche Funktionalitäten wie IGP-Protokolle, dienen jedoch nicht vorrangig der Pfadoptimierung. Das einzige derzeit aktuelle EGP Protokoll ist BGP in der Version 4 (BGP4). Die eindeutige Zuordnung von AS Nummern übernimmt in Europa RIPE NCC (Réseaux IP Européens - Network Coordination Centre), in Amerika ARIN (American Registry for Internet Numbers) und für Asien APNIC (Asia Pacific Network Information Center). Es ist nur selten erforderlich, im Umfeld von einfachen Unternehmensnetzen offizielle AS Nummern zu verwenden. Für IP-Carrier ist allerdings eine Registrierung bei RIPE (für Europa) mit Zuteilung einer AS Nummer obligatorisch.

2.3.2.1 BGP 4

Das BGP gibt es bereits seit 1989 und ist in RFC 1163 beschrieben. Mit dem Internetboom ab 1995 kam das BGP4 heraus, welches in RFC 1771 niedergelegt ist und seither ständig weiterentwickelt wird.

BGP-Router werden an den Grenzen zu anderen Autonomen Systemen eingesetzt. Diese Router benutzen das E-BGP (Exterior BGP), um Routinginformationen zwischen den Netzen auszutauschen. Sie sitzen an *Peering Points*[29] und haben Kenntnis von allen angeschlossenen Autonomen Systemen bzw. tauschen diese aus.

[29] Schnittstelle zu anderen Netzwerken – vornehmlich andere AS

Gibt es mehrere BGP-Router an Peering Points innerhalb eines Autonomen Systems, so können diese mittels des I-BGP (Interior BGP) virtuelle Verbindung untereinander aufnehmen, um z. B. beim Wegfall eines Routers an einem Peering Point alternative Routingwege in das Ziel-AS zu finden.

Ein großes AS kann zur besseren BGP4 Routenverteilung in sogenannte Confederation Autonomous Systems unterteilt werden, die eine Art Subadressierung darstellen. Man kann sich das vorstellen wie kleinere Autonome Systeme, die insgesamt ein tatsächliches, großes AS bilden. Sie sind untereinander ebenfalls nur durch E-BGP Router verbunden.

Alternativ können zur Organisation von BGP4 auch sogenannte *Route Reflectors* (RRs) eingesetzt werden. An einen RR sind mehrere IGP Router angebunden. Mehrere RRs in einem Autonomen System tauschen untereinander mittels I-BGP Routinginformationen aus.

Beides dient dazu, die Routingtabellen der beteiligten Router klein zu halten, um das Netzwerk nicht mit administrativem Datenverkehr zu belasten.

2.4 UMTS

UMTS steht für Universal Mobile Telecommunications System, das von dem Gremium 3GPP standardisiert wird, zu dessen Mitgliedern auch das Europäische Standardisierungsinstitut ETSI gehört. Dieser internationale Standard für die dritte Generation von Mobilfunksystemen soll neue Dienstleistungen auf mobilen Endgeräten ermöglichen.

Für die Mobilfunksysteme der dritten Generation gelten einige Vorgaben, um die Nachteile der zweiten Generation zu beseitigen:

- Verfügbarkeit der Dienste unabhängig von der Art des Zugangs (Mobilfunk, Festnetz, etc.), der Art der Dienstebereitstellung (regionale, nationale oder globale Netze, etc.) und der Art des Aufenthalts (Gebäude, im Verkehrsmittel, etc.)
- Weltweites Roaming verbunden mit der Aufnahme des schnurlosen Nahbereichs in den Leistungsumfang, an Bedarf und Umgebung angepasste Zellstrukturen sowie Integration der Satellitenanbindung in existierende Netzwerke
- Unabhängigkeit der Benutzeroberfläche vom Netzzugang, insbesondere Realisierung einer "virtuellen Heimumgebung" (VHE - Virtual Home Environment), die die Speicherung einer benutzerspezifischen Konfiguration im Netz erlaubt

- Unterstützung des UPT-Konzeptes (Universal Personal Telecommunications Service),

  d.h. jeder Teilnehmer besitzt eine persönliche Rufnummer unabhängig von

  der Netzumgebung

- Zugang zu Breitband- und Multimediadiensten
- Dynamische Bandbreitenanpassung
- Auslegung der Systemkapazität für den Massenmarkt

Nachfolgende Bilder verdeutlichen die Vorteile von UMTS:

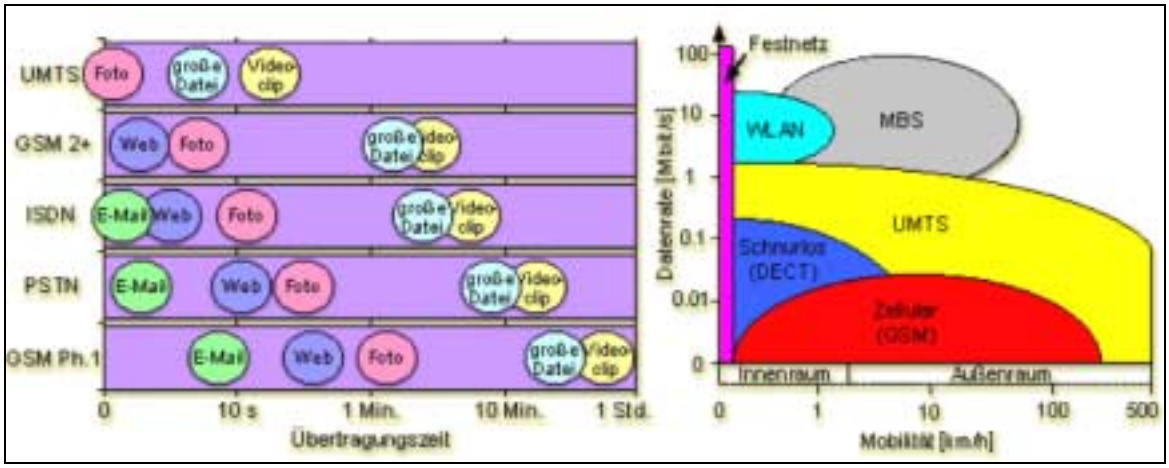


Bild 2.11 Vergleich der Übertragungszeit in Mobilfunknetzen und der Datenrate von UMTS zum Festnetz und anderen Mobilfunksystemen

Die Übertragungsraten von UMTS sollen die der Mobilfunksysteme der zweiten Generation deutlich übertreffen. Die Maximalübertragungsrate von 2 MBit/s steht aber nicht flächendeckend zur Verfügung, sondern nur in manchen Gebäuden und sogenannten Hot Spots (Flughafen, Bahnhofshalle, etc.), die im quasistationären Betrieb arbeiten. UMTS arbeitet zur Realisierung der Übertragungsraten und der Einbindung großer Gebiete mit einer mehrschichtigen Zugangsstruktur. Eine höhere Hierarchieebene versorgt geografisch ein größeres Gebiet als die jeweils darunter liegende. In der höchsten Hierarchieebene erschließen Satelliten große, möglicherweise dünn besiedelte Gebiete, ohne dort eine Infrastruktur aufbauen zu müssen und ermöglichen so eine globale Versorgung. Sie gewährleisten eine Datenrate von 144 kBit/s. Die darunter liegenden Hierarchieebenen bilden das erdgestützte Funknetz UTRAN (UMTS Terrestrial Radio Access Network). Jede Ebene besitzt einen zellularen Aufbau. Mit absteigender Hierarchieebene nimmt der Radius der Zellen ab. Kleinere Zellen erlauben eine größere Teilnehmerdichte.

Das UTRAN besteht aus Makro-, Mikro- und Pikozellen:

- Makro-Zellen (max. Datenrate: 144 kBit/s)

  Die Makro-Zellen erstrecken sich über ein größeres abgeschlossenes Gebiet z. B. eine ganze Stadt und dienen dort der flächendeckenden Grundversorgung.

- Mikro-Zellen (Datenrate: 384 kBit/s bis zu 2 Mbit/s)

  Die Mikro-Zellen decken eine Fläche von einigen Quadratkilometern ab. Sie dienen vor allem der zusätzlichen Versorgung von dicht besiedelten Gebieten.

- Piko-Zellen (max. Datenrate: 2 Mbit/s)

  Sie befinden sich im Haus des Teilnehmers, in Firmen, auf Messen, Hot Spots, etc. In Piko-Zellen bietet sich die Weiterentwicklung der schnurlosen DECT-Technologie an, die über Festnetzanschlüsse die Verbindung zum Kernnetz herstellt.

Die Integration unterschiedlicher Sendegebiete ermöglicht den Aufbau eigener unter Umständen nicht genehmigungspflichtiger UMTS-Netze in größeren Gebäuden oder abgeschlossenen Gebieten, die aber in das globale UMTS-Netz eingebunden sind.

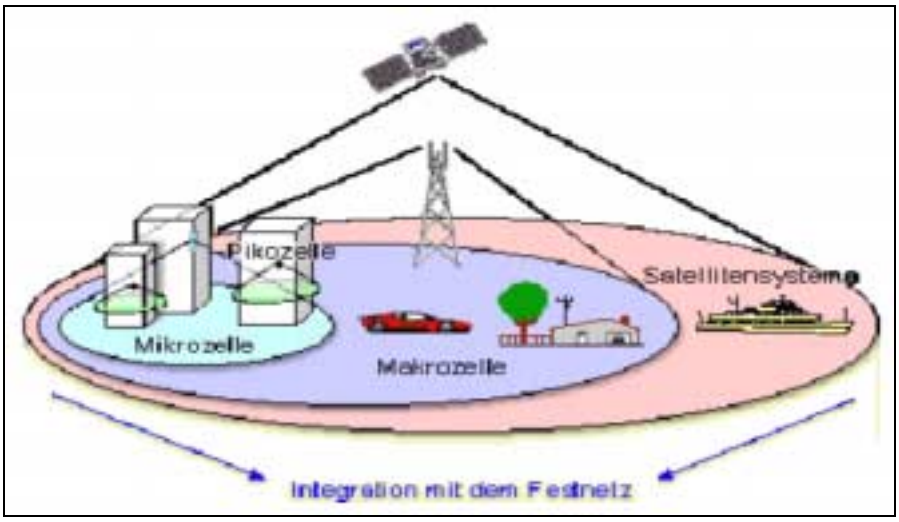


Bild 2.12 Hierarchischer Zellenaufbau zur globalen Mobilfunkversorgung (UTRAN)

Beim UMTS-Funknetz handelt es sich nicht um eine Weiterentwicklung des GSM-Funknetzes, sondern um eine Neuentwicklung. Das Funknetz umfasst die Mobilstation (Endgerät), die Basisstation (Sendeempfänger und dazugehörige Steuereinrichtung) und die Funkübertragung (Funkschnittstelle) zwischen Mobil- und Basisstation. Insbesondere bei der Methode der Funkübertragung handelt es sich um eine revolutionäre Neuentwicklung. Das UMTS-Funknetz arbeitet mit einer komplexen, hierarchischen Zellstruktur, die unterschiedliche Transfergeschwindigkeiten zulässt. Neben dem Aufbau des UMTS-

Funknetzes findet eine Weiterentwicklung und Weiterverwendung des GSM-Funknetzes statt. Das bedeutet, dass ein gemeinsames Kernnetz, aber zwei getrennt nebeneinander bestehende Funknetze für UMTS und GSM entstehen. Das UMTS-Funknetz ermöglicht dank der größeren Bandbreite der Frequenzkanäle und eines neuen Übertragungsverfahrens Multimediaanwendungen (Sprache, Daten, Text, Bilder, Audio und Video mit einer maximalen Datenrate von 2 MBit/s). Aus Kostengründen werden die Betreiber zumindest in den Anfangsjahren nach der Einführung von UMTS die reine Sprachübertragung (ohne Multimedia) weiterhin über GSM abwickeln.

Die Zellenstruktur ist flexibler als bei GSM und muss auf die Bevölkerungsdichte angepasst werden. Erste Teststrecken sind vorhanden, so wie bei D2 Vodafone mit bis zu 384 kBit/s und von der Telekom in München. Allerdings fehlen noch die dazugehörigen Endgeräte.

Bei der Gestaltung des Netzes wird es einen FDD-Mode (W-CDMA)[30] und einen TDD-Mode (TD-CDMA)[31] bei UMTS geben. Hohe Datenraten wird es nur im Piko-Zellenbereich geben. Zuerst wird es nur FDD geben, sodass es keine höheren Datenraten als bis zu 384 kBit/s geben wird. Erst TDD ermöglicht das Bündeln. Bei UMTS arbeiten alle Zellen auf der gleichen Frequenz im Gegensatz zu GSM (ca. 2-6 Frequenzpaare/Zelle). Dadurch entfällt die Gleichkanal-Interferenzfreiheit. Handover wird bei UMTS auf der gleichen oder einer anderen Frequenz stattfinden. Soft-Handover ist eine neue Funktion, um Interferenzfrei zu arbeiten, da es zu Störungen durch entfernte Basisstationen aufgrund der gleichen Frequenz kommen kann. Die Basisstationen werden über das ATM-Backbone miteinander verbunden werden. Die Zelle wird bei GSM pro Zeitschlitz exklusiv zur Verfügung gestellt. Hier ist die Zelle entweder frei oder besetzt. Bei den Datendiensten über GPRS werden allerdings die Ressourcen geteilt. Hier müssen Quality-of-Service-Merkmale angeboten werden. Bei UMTS wird die Höhe der Datenrate durch eine reduzierte Anzahl an Verschlüsselungscodes für die Signalspreizung begrenzt. Die Versorgungsreichweite ist somit abhängig von der Datenrate und der Teilnehmerzahl. Die Multimedia-Fähigkeit wird gefordert, impliziert aber nicht die notwendige Datenrate. Es werden zuerst 40 Städte mit UMTS aufgerüstet. Hamburg und Bremen werden von der T-Mobil im Jahre 2003 angebunden werden. UMTS wird mehr Basisstationen nötig machen. Dies hat eine Diskussion über die Verträglichkeit in der Öffentlichkeit ausgelöst.

[30] Frequency Division Duplex Mode (Wide Code Division Multiple Access)

[31] Time Division Duplex Mode (Time Division Multiple Access)

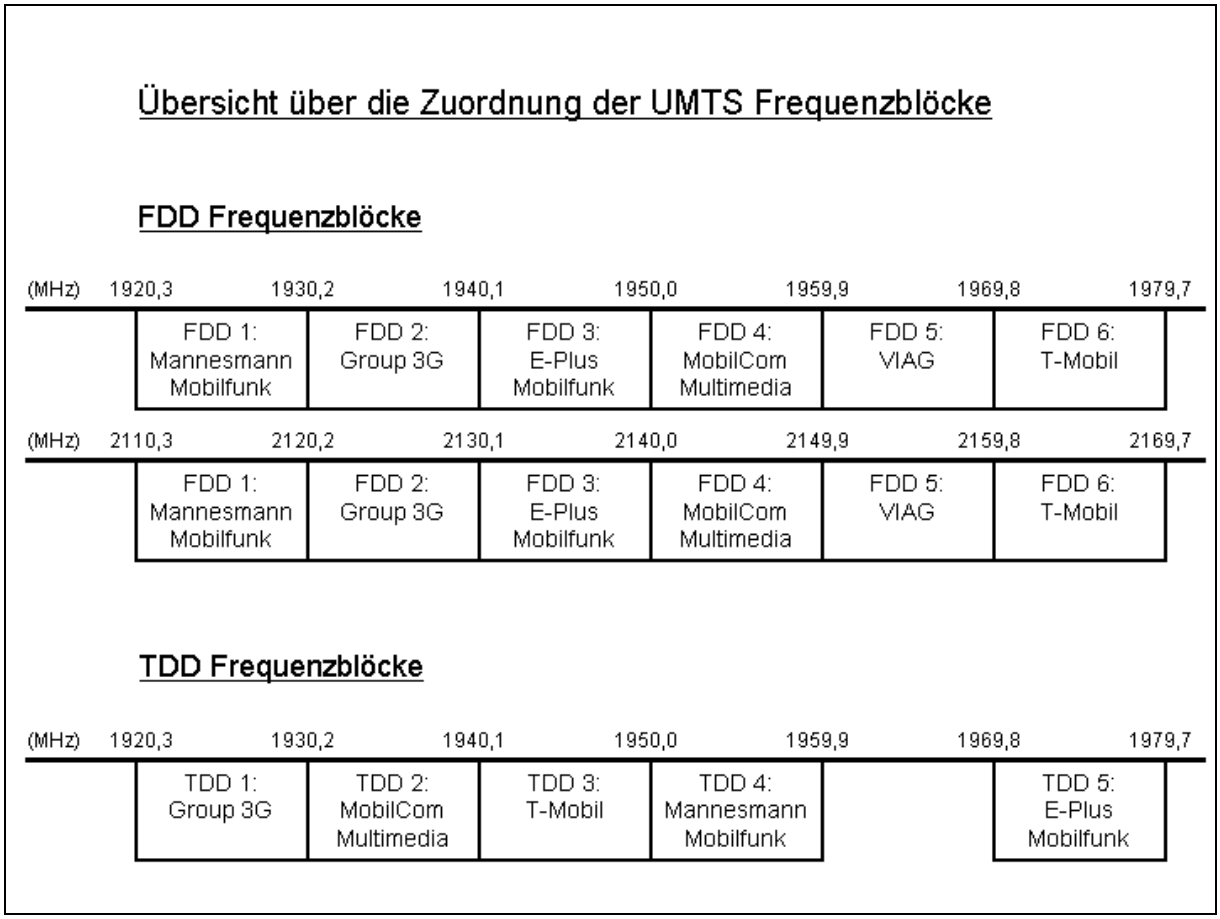


Bild 2.13 Zuordnung der UMTS Frequenzblöcke in Deutschland

2.4.1 Architektur von UMTS

Die Architektur besteht aus zwei Hauptbereichen, der User Equipment Domain, die auf Ausstattung und Funktionen der Endgeräte der Benutzer für den Zugriff auf UMTS Dienste eingeht und der Infrastructure Domain, die die benötigte physikalische Infrastruktur für die Bereitstellung der UMTS-Dienste beschreibt.

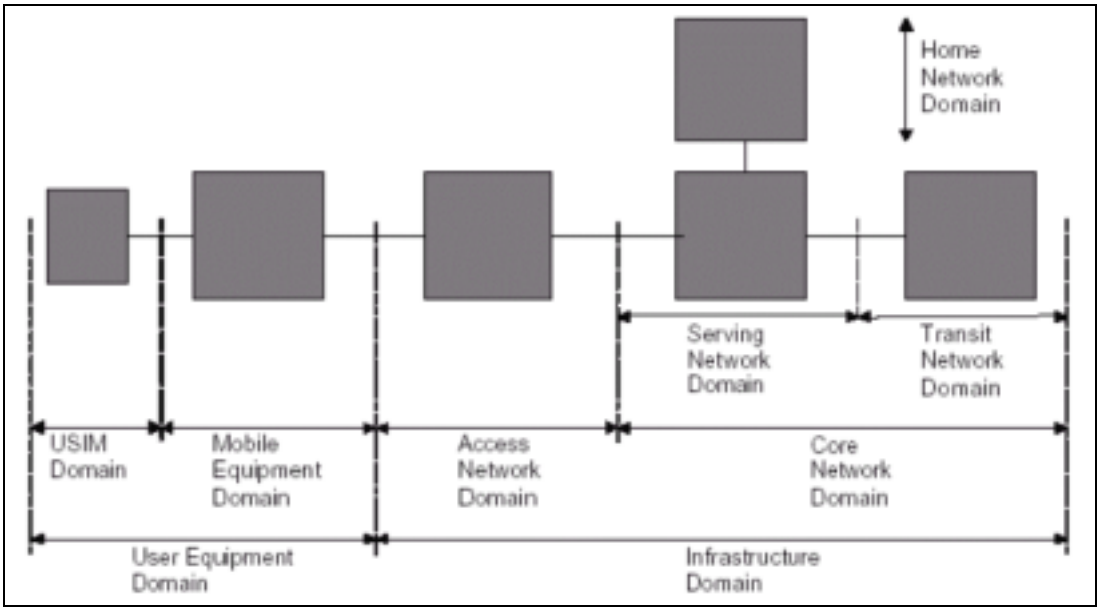


Bild 2.14 UMTS Architektur

Die User Equipment Domain umfasst wiederum die User Services Identity Module (USIM) Domain und die Mobile Equipment Domain. Die USIM-Domain beinhaltet alle Informationen und Funktionen, die das Endgerät eindeutig und sicher gegenüber dem Netz identifizieren. In der Regel befindet sich das USIM auf einer SIM-Karte, die eindeutig einem Benutzer zugeordnet ist. Die Mobile Equipment Domain führt die Funkübertragung durch und enthält alle dazu benötigten Anwendungen und Funktionen. Die Infrastructure Domain unterscheidet die Access Network Domain und die Core Network Domain. Die Access Network Domain ermöglicht den Teilnehmern den Zugang zum UMTS-Netz, indem sie die Verbindung zwischen User Equipment Domain und Core Network herstellt. Bei der Core Network Domain handelt es sich um eine aus verschiedenen Transportnetzen wie PDN- (Public Data Network), GSM- oder ISDN-Netze bestehende integrale Plattform, die über Netzübergänge miteinander verbunden sind. Sie lässt sich wiederum unterteilen in die:

- Serving Network Domain, die mit der Access Network Domain verbunden ist und alle für den Teilnehmer ortsabhängige Funktionen realisiert. Diese Funktionen folgen der Bewegung des Teilnehmers innerhalb des Netzes.
- Transit Network Domain, die für die Schnittstelle zu anderen Netzen zuständig ist.
- Home Network Domain, die vom Aufenthalt des Benutzers unabhängige benutzerspezifische Funktionalitäten beinhaltet. Dazu zählen beispielsweise die Speicherung persönlicher Daten des Benutzers oder des Benutzerprofils, also hauptsächlich Funktionen, die Service Provider zur Erbringung ihrer Dienstleistungen benötigen.

2.4.1.1 Release 3

Ein UMTS-Netz gliedert sich in das Kernnetz und das Funknetz.

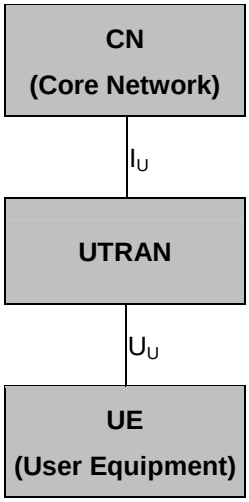


Bild 2.15 Vereinfachte UMTS-Referenzarchitektur

Das Kernnetz besteht aus Verbindungsknoten, die ein Netz miteinander verknüpft. Es verbindet die Funkübertragungseinrichtungen (Basisstationen) untereinander und schafft auch Übergänge zu ISDN-Telefonnetzen, Highspeed-Datenleitungen und Internet. Die Übertragung der Sprach-, Multimedia oder Internetdaten erfolgt konventionell über Lichtleiter, Koaxialkabel oder Richtfunkstrecken. Das Kernnetz von UMTS sollte ursprünglich (UMTS Release 3) eine evolutionäre Weiterentwicklung des bestehenden GSM-Kernnetzes sein. Diese Entscheidung beruhte hauptsächlich auf wirtschaftlichen Gründen. Bereits getätigte Investitionen in das GSM-Netz sollten erhalten bleiben und gleichzeitig das GSM-Netz weiterhin zur Verfügung stehen.

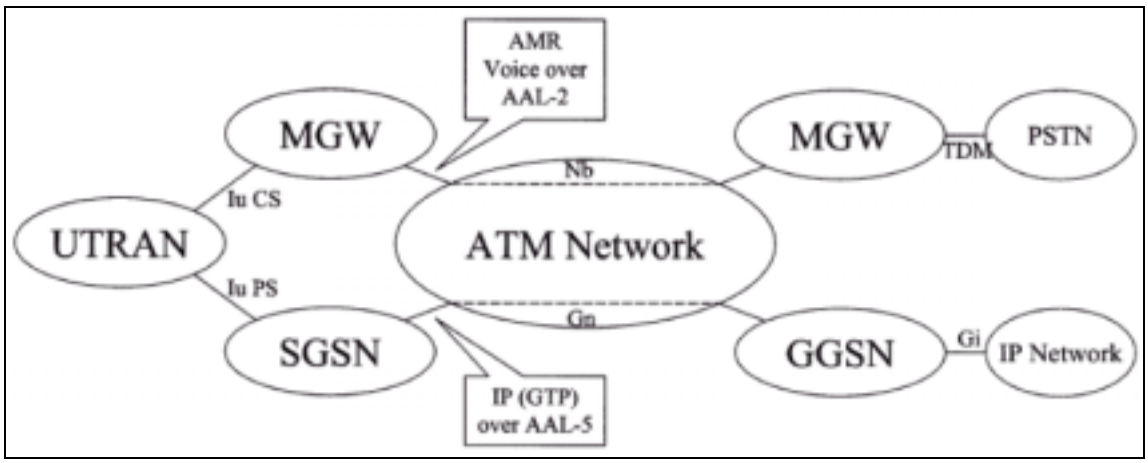


Bild 2.16 UMTS Architektur Release 3

2.4.1.2 Release 4

Eine Erweiterung erfährt das Kernnetz durch das UMTS Release 4 "All IP based Network", das eine durchgehende IP-basierte Übermittlung von Endgerät zu Endgerät bzw. zum externen Applikationsserver spezifiziert. Dabei handelt es sich um eine vollkommen neue Netzinfrastruktur, die sowohl kanalvermittelnd als auch paketvermittelnd Daten übermittelt und den Zugriff auf ERAN und URAN ermöglicht. Die All-IP-Architektur besitzt einige Erweiterungen bzgl. GSM/GPRS hinsichtlich der Funktionalitäten:

- Die Call State Control Function (CSCF) kontrolliert das gesamte Callmanagement (sowohl kanalvermittelnd als auch paketvermittelnd), verwaltet benutzerspezifische Daten, übernimmt das Adress Handling, etc.
- Der Home Subscriber Server (HSS) verwaltet alle routing- und servicerelevanten Teilnehmerdaten. Es übernimmt damit die Funktionen des Home Location Registers (HLR) des GSM-Netzes, erweitert um die Möglichkeit, über IP-Schnittstellen zu kommunizieren.
- Die Transport Signalling Gateway Function (T-SGW) und die Roaming Signalling Gateway Function (R-SGW) konvertieren die eingehende Signalisierung zu einer IP-basierenden.
- Die Media Gateway Control Function (MGCF) regelt die Protokollkonvertierung zwischen fremden PSTN/PLMN-Netzen und dem All IP based Network.
- Die Media Gateway Function (MGW) übernimmt die Verbindung zu den PSTN/PLMN-Netzen.

Der Gateway GPRS Support Node (GGSN) dient weiterhin als Schnittstelle zu externen Netzen und der Serving GPRS Support Node (SGSN) zur Zustellung der Datenpakete von und zu Mobilstationen.

Das Release 4 sieht zwei Optionen für die All-IP-Architektur vor. Option eins basiert auf einer von Release 3 völlig unabhängigen Architektur. Die auf Pakettechnologien und IP-Telefonie basierende Architektur sorgt für die Anwendung der IP-Technologie bei Diensten der dritten Generation. Option zwei unterstützt weiterhin kanalvermittelnde Geräte des Release 3 und unterstützt gleichzeitig die IP-basierten Dienste von Option eins. Dazu benötigt sie zwei weitere neue Funktionalitäten: Der MSC Server und GMSC Server bestehen hauptsächlich aus den Call Control und Mobility Control Elementen des GSM/UMTS Release 3 MSC bzw. GMSC und sind für die Signalisierung bei kanalvermittelnden Diensten zuständig.

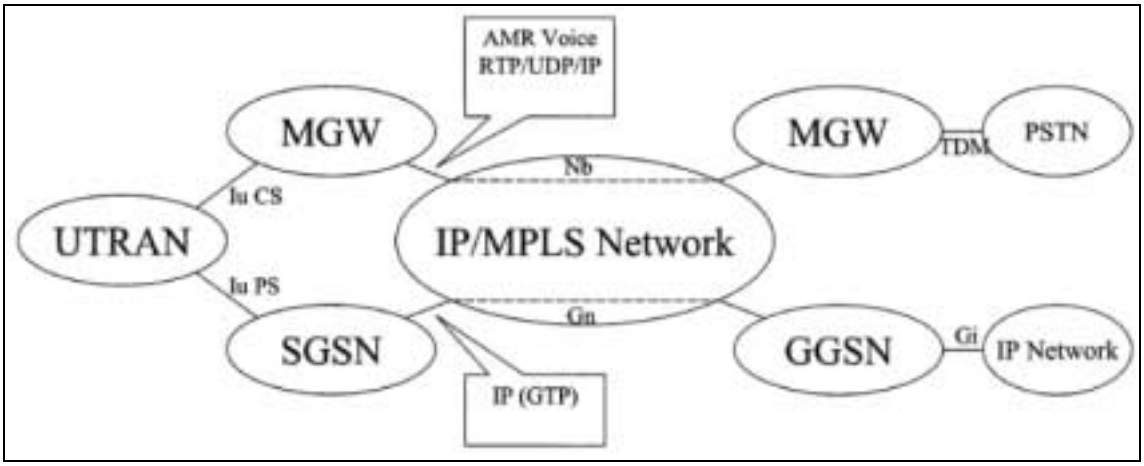


Bild 2.17 UMTS Architektur Release 4

2.4.1.3 Release 5

Das Release befindet sich zur Zeit noch in Bearbeitung und soll voraussichtlich im Jahre 2002 abgeschlossen sein. Release 5 ist nochmals eine Weiterentwicklung des bisherigen Standards und fordert ein IPv6 taugliches IP Mutimedia System im "all IP based Network". Das heißt, paketorientierte Übertragung wird in den Vordergrund gestellt werden sowie deren Anwendungsmöglichkeiten Multimedia Messaging Service (MMS) und Internet Multimedia Subsystem (IMS). MMS ist eine multimediale Erweiterung von SMS, um auf den großen Erfolg von Short Messaging Service (SMS) aufzusetzen. MMS wird also zuerst als eine Art Diashow mit Bildbeschriftung eingesetzt werden. MMS besteht dabei aus den Standards Synchronized Multimedia Integration Language (SMIL) und Multipurpose Internet Mail Extensions (MIME) [RFC 2503]. Dadurch soll eine Interoperabilität zwischen E-Mail und MMS sichergestellt werden. MMS funktioniert bereits mit GPRS, sodass UMTS hier nur eine Qualitätsverbesserung bringen würde. Bei der Nutzung interaktiver Dienste wird allerdings ein anderes Backbone benötigt. Das IMS wird paketbasierte Übertragung für den Transport von Multimediadaten nutzen. IMS nutzt das Session Initiation Protocol (SIP) für die Signalisierung. Rapid Transport Protocol (RTP) wird für die Mediendaten mit einer zusätzlichen Header-Kompression (Robust Header Compression) verwendet. Hier hat IP ein schwereres Gewicht bei der aktuellen Release erhalten, als dies vorher bei ATM der Fall war. Momentan ist keine Killerapplikation vorhanden.

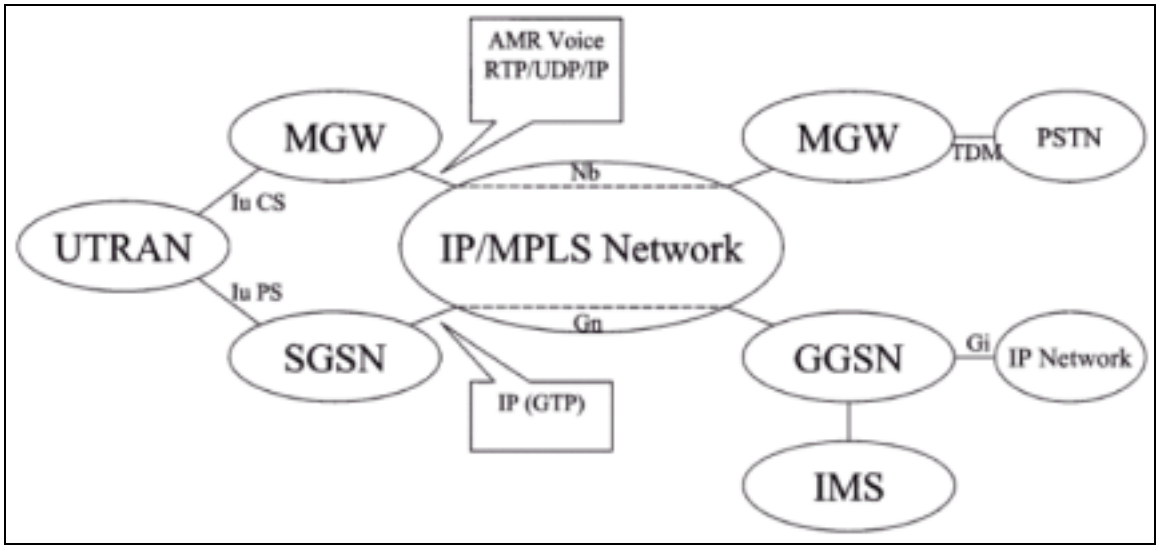


Bild 2.18 UMTS Architektur Release 5

3 Motivation für IPv6

Wozu brauchen wir überhaupt IPv6?

Wie in den vorangegangenen Kapiteln bereits mehrmals erwähnt, operieren wir heute bereits an den Leistungsgrenzen der Version 4 des Internet Protokolls, das seit mehr als zwanzig Jahren in Betrieb ist. [2] Seit 1998 liegt IPv6 als Nachfolger vor und befindet sich im Standardisierungsprozess. Die Implementierung in Testnetzen erfolgte bislang nur sehr zögerlich, was sich jedoch durch die wachsende Zahl mobiler Geräte mit eigener IP-Adresse sowie Echtzeitdienste über Mobilfunknetze ändern wird. Außerdem verdoppelt sich die Zahl der Internetuser immer noch ungefähr jährlich. Namhafte Mobilfunkhersteller wie z. B. Siemens, Nokia, Ericsson u.a. entwickeln eine völlig neue Generation von mobilen Endgeräten mit völlig neuen Nutzungsmöglichkeiten. Video-on-Demand und interaktive Spiele auf dem Handy, Internet und Multimedia im Auto, Videokonferenzen unterwegs, mobile Intranetze für Außendienstmitarbeiter sind nur einige der neuen Möglichkeiten, die durch die Interoperabilität[32] von IPv6 und Mobilfunknetzen wie UMTS ermöglicht werden. Der Bedarf an IP-Adressen steigt gewaltig, wenn man von Szenarien ausgeht, bei denen Gebäudeleitsysteme, Kühlschränke[33] und andere Haushaltsgeräte an das Internet angeschlossen sind.

IPv4 hat maßgeblich zum Erfolg des Internets beigetragen und sich aufgrund seiner Interoperabilität gut bewährt. Darauf aufbauend wird nun IPv6 entwickelt, mit der Erfahrung, die man mit IPv4 bis jetzt gemacht hat.

3.1 Adressräume

IPv4-Adressen sind relativ knapp geworden, so dass Organisationen eine NAT (Network Address Translation) verwenden müssen, mit dem mehrere private Adressen einer einzelnen öffentlichen IP-Adresse zugeordnet werden. Das erneute Verwenden von privaten Adressbereichen wird von NATs unterstützt, die standardbasierte Netzwerkschichtsicherheit oder das korrekte Zuordnen von allen höheren Protokollen jedoch nicht. Wenn zwei Organisationen verbunden werden, die den privaten Adressbereich verwenden, kann dies zu Problemen führen.

[32] Fähigkeit verschiedener Systeme (Hard- und/oder Software) miteinander zu arbeiten
[33] http://www.electrolux.com/screenfridge/

Um dem zu begegnen, sind IPv6 Adressen 128 Bit lang. Eine hierarchische Adressierungsstruktur ermöglicht das Adressieren mit begrenzter Gültigkeit. Eine Adresse kann somit zu einem einzelnen, isolierten Netzwerk oder zu einer Gruppe von Netzwerken gehören. Im 32 Bit großen Adressfeld stehen IPv4 $4{,}3*10^9$ (4,3 Milliarden) IP-Adressen zur Verfügung, die aller Voraussicht nach, da sind sich Experten einig, zwischen 2005 und 2011 komplett vergeben sein werden.

Dank der Adresslänge von 128 Bit stehen nun bei IPv6 $3{,}4*10^{38}$ IP-Adressen zur Verfügung. Legt man die momentane Erdbevölkerung auf 6 Milliarden Menschen fest, so stehen jedem Menschen $6{,}5*10^{28}$ Adressen zur Verfügung. Anders ausgedrückt stehen pro Quadratmillimeter der Erdoberfläche $667*10^{15}$ (667 Billiarden) Adressen bereit. Noch einmal anders ausgedrückt: jedes Molekül auf der Erde besitzt eine IP-Adresse. Vermutlich wird das eine ganze Weile reichen. [14]

Von diesen neuen Adressierungsmöglichkeiten profitiert auch das Routing. Hier wird eine optimierte Routinginfrastruktur bereitgestellt, da nicht mehr die komplette Adresse von den Routern ausgewertet werden muss. Momentan müssen Router im Internet-Backbone mit der Version 4 des Internet Protocol die IP-Adressierung und alle Routen der Edge-Router[34] kennen. Das Problem wurde durch CIDR mittelfristig entschärft. Mit IPv6 können Router ähnlich vorgehen wie ein Telefonnetz mit seinen hierarchisch aufgebauten Telefonnummern. Hier muss ein Knoten beim Aufbau einer Verbindung nur auf den jeweils relevanten Teil der Telefonnummer achten: Beim Weiterleiten eines Gesprächs von einem Land in ein anderes wird beispielsweise nur die Landesvorwahl analysiert. Erst wenn der Ruf im Land des Empfängers angekommen ist, finden die anderen Felder der Telefonnummer Beachtung und das Gespräch wird entsprechend weitergeleitet. Ebenso sieht ein Router im IPv6-Netz bereits aufgrund der Werte des *Format Prefix* (FP) und des *TLA* Identifiers, dass das Datagramm nicht in seine Netzstruktur gehört und wertet es somit gar nicht weiter aus. Das reduziert die Verarbeitungszeit, Routingtabellen werden kleiner und senkt die Anforderungen an den Speicher des Routers.

[34] Router an der Grenze zu einem anderen Netzwerk

3.2 Konfiguration

Die meisten aktuellen IPv4-Implementierungen müssen entweder manuell konfiguriert werden oder verwenden ein statusbehaftetes Konfigurationsprotokoll wie DHCP (Dynamic Host Configuration Protocol). Bei der zunehmenden Anzahl an Computern und Geräten, die IP verwenden, wird eine einfachere und stärker automatisierte Konfiguration von Adressen und anderen Konfigurationseinstellungen erforderlich. Laut eines Berichts in der NetworkWorld Germany[35] wird die Zahl der netzwerkfähigen Endgeräte von momentan 1,8 Milliarden in den nächsten Jahren auf 43 Milliarden steigen.

Um Hostkonfigurationen zu vereinfachen, unterstützt IPv6 sowohl statusbehaftete Adresskonfiguration, z. B. Adresskonfiguration bei Vorhandensein eines DHCP-Servers, als auch statusfreie Adresskonfiguration (Adresskonfiguration ohne DHCP-Server). Bei statusfreier Adresskonfiguration konfigurieren sich Hosts auf einer Verbindung automatisch mit IPv6-Adressen für die Verbindung (sogenannte verbindungslokale Adressen) und mit Adressen von Präfixen, die von lokalen Routern angekündigt wurden. Auch wenn kein Router vorhanden ist, können sich Hosts auf der gleichen Verbindung automatisch mit verbindungslokalen Adressen konfigurieren und ohne manuelle Konfiguration kommunizieren. Es wurde eigens für IPv6 ein neues Protokoll entwickelt, das die automatische Konfiguration erleichtern und verbessern soll: das *Neighbor Discovery Protocol* (ND), beschrieben in RFC 2461.

3.3 Mobility

Neue Impulse für IPv6 erhoffen sich seine Befürworter durch die neuen Mobilfunktechniken, insbesondere durch UMTS. Ein großer Wunsch vieler Internetbenutzer ist es, immer und überall erreichbar zu sein. Dies würde bedeuten, dass man von den unterschiedlichsten Lokalitäten aus Internetanwendungen benutzen kann, ohne sich um Konfigurationen oder IP-Adresse Gedanken machen zu müssen. Dies ist unter IPv4 nicht möglich, aber mit IPv6 ist dies realisierbar.
Die Grundidee ist, dass Pakete ihren Weg durch das Netz anhand einer IP-Adresse finden, die einem Interface zugeordnet ist. Mit Mobile-IPv6 soll es möglich sein, dass sich ein Rechner beliebig im Internet bewegt und immer unter einer fest konfigurierten IP-Adresse oder einer lokal zugewiesenen IP-Adresse erreichbar ist.

[35] Heft: 17/01, Artikel: Neuer Schwung für IPv6, Autoren: David Fraser, Bernd Reder

Durch die Interoperabilität von UMTS und IPv6 werden Mobilfunk und Internet weiter zusammengeführt und mobile Multimedia-Anwendungen möglich. Durch diese Verknüpfung und den schnellen mobilen Zugang zum Internet haben die Menschen Zugriff auf alle erdenklichen Informationen an jedem Ort und zu jeder Zeit. Musik, Fotos oder Videos mit hohen Übertragungsraten aber auch Mobile-Commerce Anwendungen sind hier nur Beispiele.

Aufgrund der Art und Weise, wie IPv4-Netzwerk-IDs bisher und momentan zugeordnet werden, enthält die Routingtabelle der Internet-Backbonerouter üblicherweise über 120.000 Routen. Bei der aktuellen Internet-Routing-Infrastruktur von IPv4 handelt es sich um eine Kombination von direktem und hierarchischem Routen. Letzteres ist durch CIDR möglich geworden.

3.4 Unterstützung von Echtzeitübermittlung

Obwohl es QoS-Standards für IPv4 gibt, basiert die Unterstützung von Echtzeit-Datenübertragung auf dem TOS-Feld (Type of Service) von IPv4 sowie auf der Nutzdatenidentifizierung. Üblicherweise wird ein UDP- oder TCP-Port zur Bestimmung der Applikation benutzt. Das TOS-Feld von IPv4 stellt nur begrenzte Funktionalität zur Verfügung. Zudem ist keine Nutzdatenkennung über einen TCP- oder UDP-Port möglich, wenn die Nutzdaten eines IPv4-Pakets verschlüsselt sind.

IPv6 stellt mit dem neuen Flow Label Feld verbesserte Möglichkeiten zur Verfügung, Daten aufgrund QoS Anforderungen zu behandeln.

3.5 Security

Während der Sicherheit früher wenig Beachtung geschenkt oder erst später hinzugefügt wurde, so müssen heute neue Protokolle bereits von Anfang an den Sicherheitsanforderungen entsprechen. Ob Sicherheit eventuell zusätzlich auf der Ebene des Transportprotokolls gelöst werden soll, ist ein eigenes Thema. Das stärkste Argument hierzu ist, dass gewisse Attacken auf IP-Ebene, wie Veränderung von Adressen oder Ausspähen von Kommunikationsbeziehungen, nur auf dieser Ebene gelöst werden können.

Bei der privaten Kommunikation über ein öffentliches Medium wie das Internet werden Verschlüsselungsdienste benötigt, die die zu sendenden Daten so schützen, dass diese bei der Übertragung nicht eingesehen oder geändert werden können.

Obwohl es derzeit einen Sicherheitsstandard für IPv4-Pakete gibt (bekannt als Internet Protocol Security oder IPSec), ist dieser optional.

Sicherheit war bereits von Anfang an neben dem erweiterten Adressraum eines der Ziele, welche mit IPv6 gelöst werden sollten. Zuerst entwickelte man eigene Sicherheitsprotokolle für IPv6. Dann wurde die Arbeitsgruppe Internet Protocol Security (IPSec) der IETF beauftragt, Sicherheitsaspekte in IPv6 einzuplanen. Alle in IPv6 verwendeten Sicherheitsfragen basieren jetzt auf den von IPSec definierten Verfahren. Obwohl IPSec ursprünglich nur für IPv6 Sicherheitsmechanismen in den Bereichen Verschlüsselung und Authentisierung entwickelte, entschloss man sich, Standards zu definieren, welche sowohl in IPv6 als auch IPv4 verwendet werden können. Diese Standards sollten alle Bedürfnisse auf den Gebieten der Verschlüsselung und Authentisierung abdecken. IPSec definiert eine Sicherheitsarchitektur [RFC 2401], welche vor allem aus IPSP (IP Security Protocol) und Verfahren zum Schlüsselmanagement besteht.
Die Sicherheitsfunktionen von IPSec sind optional und sicher sinnvoll. Die Performance könnte unter den zusätzlichen Anforderungen leiden, doch es ist zu bemerken, dass nur die Endkonten in die Verschlüsselung involviert sind und daher den Rest des Internets nicht beeinträchtigen.

3.6 Aussicht und Hindernisse

Der Trend in Richtung »Mobiles Internet« wird weiterhin für Rückenwind sorgen. Vor allem für Unternehmen, die neue Netze aufbauen und nicht durch die »Altlast« vorhandener IPv4-Infrastrukturen eingeschränkt sind, macht es Sinn, von Beginn an auf die neue IP-Version zu setzen.

Da IPv6 jedoch nicht von heute auf morgen implementiert und IPv4 abgeschaltet werden kann, ist die Interoperabilität von IPv4 und IPv6 unbedingt zu gewährleisten. Um den Nutzern, Herstellern und Carriern Zeit für die Umstellung zu geben, bleibt es jedoch weiterhin fraglich, wie lange sich die Migration von Version 4 auf 6 hinziehen wird. 75% des IPv4- Adressraumes haben die Vereinigten Staaten von Amerika (USA) erhalten, dort sind die marktführenden Hersteller im Netzwerkbereich (Cisco, Nortel, Juniper, u.a.) ansässig. Die Adressknappheit, wie wir sie hier in Europa erfahren, ist in den USA zur Zeit noch nicht gegeben, weshalb die Hersteller keine dringende Notwendigkeit zur Einführung von IPv6 zu sehen scheinen. Bislang gibt es nur ein weltweites IPv6-Testnetz (6bone)[36], das sich noch der Infrastruktur der Version 4 bedienen muss. Dies funktioniert nur durch eine Umsetzung der IPv6- in eine IPv4-Architektur. Hierzu mehr im nächsten Kapitel,

[36] http://www.6bone.net/

Interoperabilität IPv4 / IPv6. Auf diese Weise kann man sicherlich viele Fehler beim Aufbau des IPv6-Netzes vermeiden und Verbesserungen vor der eigentlichen Implementierung erzielen. Man sollte damit nicht zu lange warten, denn die Anzahl der umzustellenden Endgeräte erhöht sich von Tag zu Tag. Dennoch werden viele Anwender mithilfe von Network Address Translation, dynamischer Adressierung und ähnlichen Methoden die Migration hinauszögern. Wie lange sie das tun können, hängt nicht nur davon ab, wann der Vorrat an IP-Adressen erschöpft sein wird, sondern auch davon, wann Applikationen Fuß fassen, die Quality of Service und ausgefeiltere Sicherheitsmechanismen erfordern.

Während der Ausarbeitung der Diplomarbeit gewann IPv6 zunehmend an Bedeutung, erkennbar an den inzwischen vermehrt auftretenden Artikeln in der Fachpresse. Seit Ende 2001 bietet ein japanischer Provider IPv6-Dienste an. Des weiteren kündigt Juniper Networks im November 2001 IPv6 für seine JUNOS Software als produktiv an.

4 Interoperabilität IPv4 / IPv6

Die Internet Gemeinde hat sich entschieden, den Übergang zum neuen Internet Protokoll anhand des Dual-Stack Verfahrens durchzuführen. So wird ein IPv6 Internet parallel zum bestehenden IPv4 Netz aufgebaut, welches sich anfänglich noch der IPv4 Infrastruktur bedient[37]. Deswegen muß IPv6 unbedingt mit IPv4 interoperabel sein.

Der Parallelbetrieb von IPv4 und IPv6 Technologie wird von Mechanismen wie Dual Stack, Protokollumsetzung und / oder Tunneling gewährleistet. Letzteres ist ein Verfahren mit dem das MBone schon erfolgreich betrieben wird und das 6Bone[38] seit 1996 unter anderem den Testbetrieb realisiert.

4.1 Dual-Stack Verfahren

Router führen Tabellen, in denen sie die Adressen der ihnen angeschlossenen Geräte sowie der Next Hops ablegen. Ein möglicher Weg IPv6 parallel zu IPv4 anzubieten ist, Router mit dualem Stack auszustatten. Damit werden dann für die Netzwerkumgebung zwei verschiedene Routingtabellen geführt, - einmal im IPv4- und einmal im IPv6-Adreßformat.

Hosts können mittels eines Softwareupgrades IPv6-fähig gemacht werden. Die Entscheidung, welcher Stack letztendlich genutzt wird, basiert auf Informationen des Domain Name System (DNS), das zwingend erforderlich ist und die Umsetzung von Domain Namen in IP-Adressen bietet.

Anwendungen sollen deswegen auch *Namen* und nicht die *IP-Adressen* selbst ansprechen. DNS wurde zu diesem Zweck erweitert und verwendet jetzt einen AAAA record type[39], um IPv6-Adressen darstellen zu können. Für IPv4-Adressen war nur ein A record type notwendig. Mit dem ersten IPv6-fähigen Gerät in einem Netzwerk muß auch der DNS angeglichen werden.

[37] Vgl [7] Seite 197
[38] IPv6 Testnetz, siehe [20]
[39] Vgl [28]

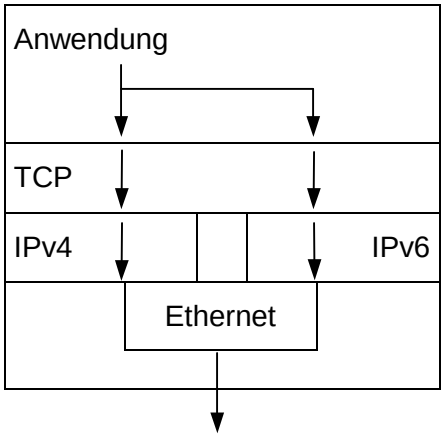


Bild 4.1 Typische Dual-Stack Konfiguration

Hosts mit dualem Stack können völlig unabhängig voneinander mit IPv4- und IPv6-Adressen konfiguriert sein oder eine IPv4-kompatible IPv6-Adresse erhalten. Das Dynamic Host Configuration Protocol (DHCP) kann weiterhin verwendet werden, um eine IPv4-Adresse zu erhalten. Für die neue IP Generation gibt es verschiedene Protokolle zur automatischen Adressvergabe, verbindungslose und statusbehaftete, wie das weiterentwickelte DHCPv6.

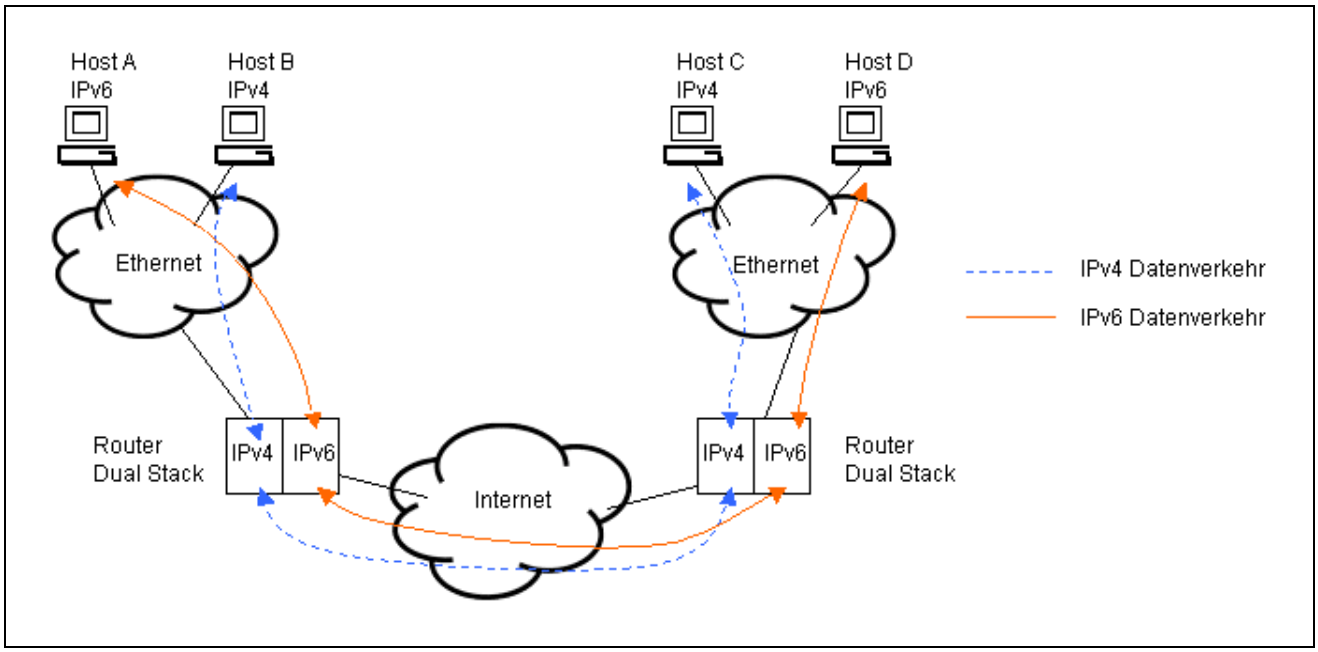


Bild 4.2 Dual-Stack Szenario

In Bild 4.2 dargestelltem Szenario wird von Host A oder D generierter Datenverkehr durch den IPv6-Stack der Router geleitet. Datenverkehr der Hosts B und C hingegen durchläuft den IPv4-Stack der Router. Nachteil bei diesem Beispiel ist zum einen, dass nur Geräte derselben Protokollversion Daten austauschen können. Zum anderen müssen auch alle

dazwischen liegenden Router Dual-Stack implementiert haben, sofern nicht zusätzlich andere Mechanismen vorgesehen sind. Werden z. B. noch IPv4-kompatible IPv6-Adressen vergeben und Tunnelmechanismen zur Verfügung gestellt, gelangt man zu einer denkbaren Lösung für die Übergangsphase.

4.2 NAT – PT Gateway

Bei der Recherche hierzu stießen wir immer wieder auf unterschiedliche Verwendung von Abkürzungen, so dass wir letztendlich beschlossen, mit der Notation von RFC 3022 konform zu gehen. [26]

Zunächst sei hier *Network Address Translation* (NAT) erwähnt, das viel genutzt wird - und nicht erst seit die IPv4 Adressen knapp werden. [25] Firmen haben damit die Möglichkeit, innerhalb ihres Netzwerkes beliebige IP-Adressen zu vergeben. Bei Änderungen in der Netztopologie sind keine aufwendigen Umkonfigurationen notwendig, da die intern verwendeten Adressen nicht global einzigartig sein müssen. Sie werden durch den sogenannten Network Address Translator in eine gültige IP-Adresse umgesetzt sobald eine Anwendung verlangt, das Firmennetz zu verlassen. Anwendungen mit IP-Adressen in der Nutzlast verlangen eine spezielle Behandlung, da die sogenannte "Payload" üblicherweise nicht ausgewertet wird. Hierfür stehen verschiedene anwendungsspezifische *Application Level Gateways* (ALG) zur Verfügung. Ist der Datenstrom außerdem noch verschlüsselt, funktioniert eine Umsetzung mittels NAT nicht mehr.

Es gibt viele Varianten von NAT und dementsprechende Notationen. Im Rahmen dieser Diplomarbeit würde es jedoch zu weit führen, auf diese einzugehen, weswegen hier nur auf RFC 2663 (IP Network Address Translator (NAT) Terminology and Considerations) verwiesen wird. [27]

Mit *Network Address Port Translation* (NAPT) werden mehrere IP-Adressen samt ihrer TCP/UDP Ports in eine einzelne Netzwerkadresse mit den entsprechenden TCP/UDP-Portnummern umgesetzt. So können gleichzeitig mehrere Knoten eines lokalen Netzes auf andere Netzwerke zugreifen, indem sie die IP-Adresse verwenden, die ihrem Access Router[40] zugewiesen wurde.

NAT und NAPT werden auch als "traditional NAT" bezeichnet. Nimmt man beide Mechanismen zusammen, erhält man die Möglichkeit, eine Anzahl interner Adressen in eine kleinere Zahl externer Adressen umzusetzen.

[40] Router, der den Zugang aus dem lokalen in andere Netzwerke ermöglicht.

Es sei hier noch erwähnt, dass bei NAT entweder die Quell- oder die Zieladressen umgesetzt werden. Wird eine Übersetzung in beide Richtungen gebraucht, z. B. bei Adresskollisionen des internen und externen Netzwerkes, kann dies mit dem sogenannten "Twice NAT" geschehen.

Da NAT verbindungsorientiert ist, wird zumeist angenommen, dass sämtlicher zusammengehörender Datenverkehr auch durch den gleichen NAT-Router laufen muss. Das wäre ein äußerst anfälliges System. Außerdem sind viele private Netzwerke nicht nur mittels eines ISPs[41] an externe Netze angebunden, sondern betreiben das sogenannte "Multihoming". Es ist z. B. denkbar, ein NAT-Gerät pro ISP in privaten Netzwerken zu verwenden. Spätestens dann macht es Sinn, die NAT-Geräte identisch zu konfigurieren, damit sie sich gegenseitig Backup gewährleisten.

Systembedingt bringen NATs Performance Engpässe ("Flaschenhälse"), geringe Skalierbarkeit und keine universellen Verbindungsmöglichkeiten mit sich.

Network Address Translation – Protocol Translation (NAT-PT) ist eine Adress- und Protokollumsetzung auf IP-Ebene, also Layer 3 nach dem OSI-Modell. Es wird in Router implementiert, die an der Grenze zwischen IPv4 und IPv6- Netzwerken beheimatet sind. Ein Vorteil ist, dass keine weitere Anpassung oder zusätzliche Software, wie z. B. Dual Stack, benötigt wird, um NAT-PT auf Endgeräten in IPv4 oder IPv6-Netzwerken zu installieren. Dadurch ist es einfach zu implementieren, zu verwalten und für die Übergangsphase IPv4 zu IPv6 ein hilfreiches Werkzeug.

Dynamisch weist NAT-PT den IPv4/IPv6-grenzübergreifenden Sessions[42] bei der Initialisierung von IPv6-Geräten ausgehend (oder zu ihnen hin), IPv4-Adressen aus einem eigens dafür vorgesehenen Adressbereich zu. Zwingend notwendig ist auch hier, dass alle zu einer Session gehörenden Datagramme denselben NAT-PT Router durchlaufen. Datenpakete, die von Dual-Stack Geräten generiert wurden oder an solche adressiert sind, müssen nicht übersetzt werden und sind dadurch von dieser Beschränkung ausgenommen.

[41] Internet Service Provider
[42] Logische Verbindung zwischen zwei adressierbaren Einheiten im Netz, um Daten auszutauschen

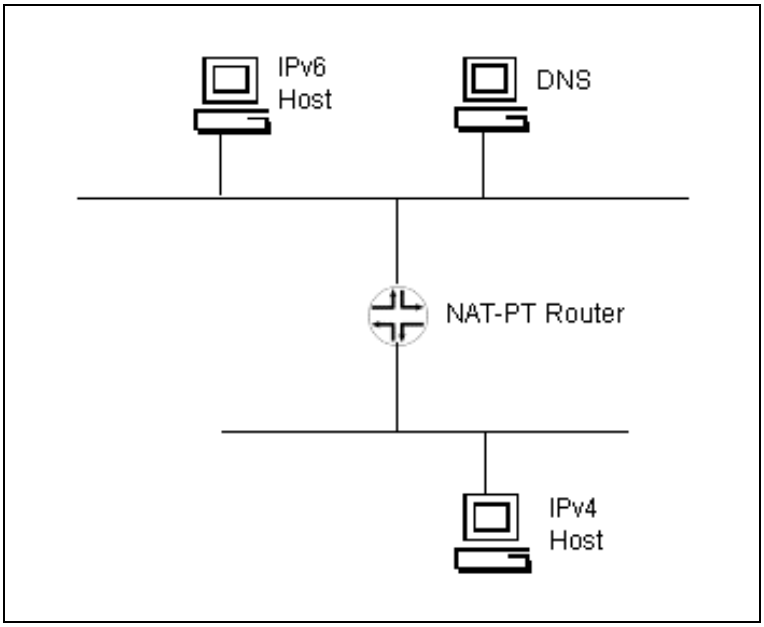


Bild 4.3 einfaches Beispielnetz mit NAT-PT

Aufgrund der Nachteile, die NAT-PT mit sich bringt, sollte es nur in der Übergangsphase von IPv4 zu IPv6 eingesetzt werden, wenn keine anderen Mechanismen zur Verfügung stehen. Zu umgehen ist eine Übersetzung z. B., wenn NAT-PT eine echte IPv6 Anbindung hat oder diese durch Tunnelmechanismen zur Verfügung gestellt wird.

Auch NAT-PT muss sich ALGs bedienen, wenn IP-Adressen von Applikationen verwendet werden, die auf Layer 3 aufsetzen.

Ein weiteres für NAT (und somit auch für NAT-PT) spezifisches Problem ist die Sicherheit innerhalb der Vermittlungsschicht. Dies trifft auch auf die Transport- und Anwendungsschicht zu, wenn Applikationen an die Anwendungsschicht IP-Adressen übermitteln.

Abgesehen davon ist eine Ende-zu-Ende Sicherheit mit IPSec nicht möglich, sobald verschiedene Adressräume durchquert werden. Die beiden Endgeräte, die IPSec Funktionalität nutzen wollen, müssen dann entweder beide IPv4 oder IPv6 unterstützen.

4.3 Stateless IP/ICMP Translation (SIIT)

Die zustandslose Protokollübersetzung von IP- und ICMP- Protokollen (Stateless IP/ICMP Translation, SIIT) ist in RFC 2765 definiert. [36] Dabei bedeutet zustandslos, dass jedes Paket für sich – ohne Speicherung eines Kontexts – übersetzbar ist. Wichtig für die Übersetzung ist, dass die IP-Adressen automatisch aufeinander abbildbar sein müssen. Für SIIT war die Einführung einer weiteren IPv6-Sonderadresse notwendig. Diese wird als IPv4-translated-Address bezeichnet und hat den in nachfolgender Abbildung gezeigten Aufbau.

0:0:0:0:FFFF:0 (96 Bit)	IPv4-Adresse (32 Bit)

Bild 4.4 IPv4-translated IPv6-Adressen

Eine IPv4-translated IPv6-Address hat somit das Format "0:0:0:0:FFFF:0:a.b.c.d", wobei "a.b.c.d" die IPv4-Adresse des IPv4 Partners darstellt. SIIT verwendet zusätzlich die bereits bekannten IPv4-mapped Adressen (0::0FF:a.b.c.d) und die kompatiblen IPv4-Adressen (0::0a.b.c.d). Mit SIIT sind nur Unicast-Pakete transformierbar, da die IPv4-Multicast-Adressen (224.x.y.z ... 239.x.y.z) mit den verwendeten Sonderadressen nicht auf die IPv6-Multicast-Adressen, die ja alle mit "FFFF:..." beginnen, abzubilden sind.

Die Funktionen der Protokollumsetzung werden in einer SIIT-Box bzw. im Translator (z. B. Zusatzsoftware in einem Router) realisiert, welcher am Rand der IPv6- Domäne am Übergang in das IPv4-Internet positioniert ist.

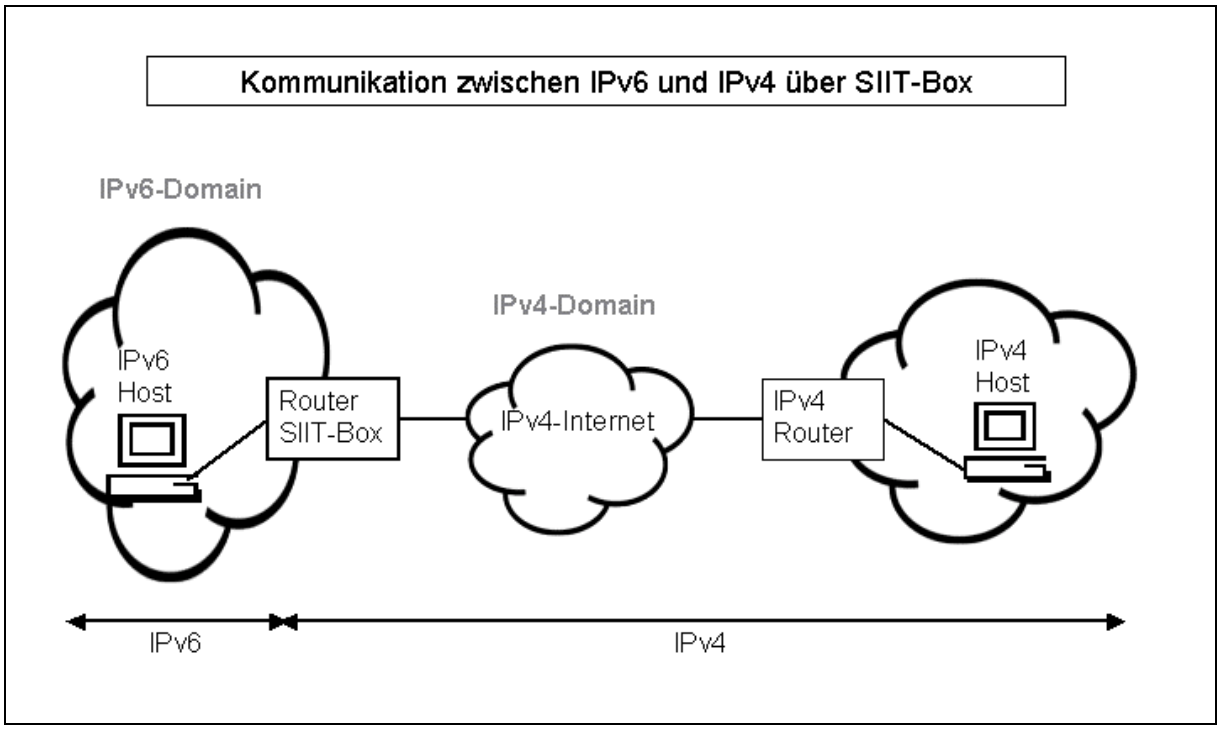


Bild 4.5 Kommunikation zwischen IPv6 und IPv4 über SIIT-Box

Voraussetzung für die Funktion von SIIT ist, dass der IPv6-Knoten, welcher mit einem IPv4-Partnerknoten IP-Pakete austauschen möchte, temporär für die Dauer einer Kommunikationsbeziehung eine IP-Adresse aus dem Bereich der öffentlichen Adressen zugewiesen bekommen muss. Dies kann ein reservierter IPv4-Adressbereich sein. Da die IPv4-Adressen nur für die Sonderanwendung der Kommunikation mit IPv4-Partnern

notwendig sind, kann ein kleiner Pool von IPv4-Adressen ausreichen. Die Zuteilung der IPv4-Sonderadresse kann z. B. über DHCPv6 erfolgen. Ebenso ist dafür zu sorgen, dass die notwendigen Einträge im DNS für diese IPv6-Sonderadressen vorgenommen werden, z. B. durch manuelle DNS-Konfiguration oder durch DNS-Updates von den DHCPv6-Instanzen aus.

Auf jeden Fall wird bei SIIT für die Dauer einer Kommunikationsbeziehung zwischen einem IPv6-Knoten und einem IPv4-Knoten je IPv6-Knoten eine eigene IPv4-Adresse benötigt. Bei IPv6 ist eine minimale MTU[43] (Maximum Transfer Unit) von 1280 Bytes immer garantiert.

4.3.1 Fragmentierung

Bei IPv6 ist die Feststellung der minimalen MTU (Path-MTU) zwischen zwei Endknoten, die über IPv6 miteinander kommunizieren, zwingend vorgeschrieben und mit ICMPv6 zu realisieren. Bei IPv4 ist die Feststellung der Path-MTU jedoch nicht zwingend vorgeschrieben, sondern optional.

Wenn nun ein IPv4-Knoten, welcher über einen SIIT-Translator mit einem IPv6-Knoten kommunizieren will, die Path-MTU feststellen will, so sieht dies der SIIT-Translator, da er ja auf der Strecke zwischen beiden Endknoten liegt. In diesem Fall muss im IPv6-Netz nur dann ein Fragmentierungserweiterungsheader eingefügt werden, wenn das Paket bereits auf der IPv4-Seite fragmentiert ist. Falls ein IPv4-Knoten jedoch auf die nicht zwingend vorgeschriebene Prozedur zur Feststellung der Path-MTU verzichtet, so muss der sendende IPv4-Knoten sicherstellen, dass die minimale IPv6-MTU von 1280 Bytes nicht überschritten wird. Er darf nur IPv4-Pakete mit einer maximalen Länge von 1232 Bytes (ohne IPv4-Header) senden, welche nach Umwandlung in IPv6-Pakete (zusätzlich 40 Bytes für den IPv6-Header) und Hinzufügung des IPv6-Fragmentierungsheaders (8 Bytes) dann insgesamt 1280 Bytes lang sind. Es könnte sein, dass eine der IPv6-Strecken nur diese MTU hat. Da IPv6-Router unterwegs aber nicht mehr fragmentieren, darf der sendende IPv4-Knoten diese MTU nicht überschreiten. Außerdem muss – sofern der IPv4-Knoten nicht die Path-MTU feststellt – der Translator auf der IPv6-Seite in jedem Fall einen Fragmentierungserweiterungsheader einfügen, da der sendende IPv4-Knoten Fragmentierung erlaubt. Ohne diesen Erweiterungsheader könnte ein empfangender IPv6-Knoten empfangene Pakete nicht wieder zusammensetzen.

[43] Die größte Frame-Länge, die über ein bestimmtes physikalisches Medium verschickt werden kann.

Wenn ein IPv4-Paket allerdings die Path-MTU nicht überschreiten würde (z. B. ein Paket mit weniger als 1232 Bytes ohne IPv4-Header) und das DF-Bit im IPv4-Paket gesetzt ist, d.h. dass das Paket kein Fragment ist, so kann es auch auf IPv6-Seite ohne Fragmentierungserweiterungsheader übertragen werden.

4.3.2 Übersetzung der IP-Header

4.3.2.1 IPv4 nach IPv6

Bei der Übersetzung der IP-Header von IPv4 nach IPv6 können folgende Felder direkt übersetzt werden:

IPv4	IPv6
Version (4)	Version (6)
TOS	Traffic Class
-	Flow Label
Total Length	Payload Length (=Total Length – Header Length)
Protocol	Next Header
TTL	Hop Limit
Source Address	Source Address[44]
Destination Address	Destination Address[42]

Sofern auf IPv6-Seite ein Fragmentierungsheader eingefügt werden muss, sind im IPv6-Header folgende Modifikationen notwendig:

IPv4	IPv6
Total Length	Payload Length (=Total Length – Header Length + 8 Bit)
Fragment Header	Next Header

[44] je nach verwendetem Mechanismus (SIIT, NAT-PT, etc.) umgesetzte Adressen

Im IPv6-Fragmentierungserweiterungsheader müssen folgende Felder angepasst werden:

IPv4	IPv6
Protocol	Next Header
Fragment Offset	Fragment Offset
More Fragment Bit	More Fragment Bit
Identification	Identification

IPv4-Optionen werden ignoriert und erscheinen nicht mehr im IPv6-Paket.

UDP-Pakete können – sofern bei UDP mit IPv4 eine Checksum im Paket enthalten ist – ohne Sonderbehandlung übersetzt werden. Wenn allerdings keine UDP-Checksum vorliegt – sie ist bei IPv4 optional und bei IPv6 obligatorisch -, muss der SIIT-Translator die UDP-Checksum für das IPv6-Paket selbst erzeugen.

4.3.2.2 IPv6 nach IPv4

Bei der Übersetzung von IPv6 nach IPv4 kann der IPv4-Header, sofern das IPv6-Paket keinen Fragmentierungsheader enthält, in folgenden Feldern angepasst werden:

IPv6	IPv4
Version (6)	Version (4)
Header Length	Header Length
Traffic Class	TOS
Payload Length + 20 Bit[45]	Packet Length
-	Identification (=0)
-	Fragment Flag (=0)
-	Fragment Offset (=0)
Hop Limit	TTL
Next Header	Protocol
-	Header Checksum (wird nach Erzeugung des Ipv4-Headers berechnet)
Source Address	Source Address
Destination Address	Destination Address

[45] IPv4 Header Length = 20 Bit

Enthält das IPv6-Paket IPv6-Optionen, werden diese ignoriert, d.h. die Länge der Erweiterungsheader ist von der Paketlänge abzuziehen und das Protokollfeld für den IPv4-Header ist aus dem letzten IPv6-Header zu kopieren. Ist kein Fragmentierungserweiterungsheader im IPv6-Paket enthalten, sind folgende Felder anzupassen:

IPv6	IPv4
Packet Length	Payload Length – 8 Bit[46] + 20 Bit
Identification	Untere 16 Bit der IPv6 Identification
More Fragment Bit	More Fragment Bit
Fragment Offset	Fragment Offset
Protocol	Next Header

4.3.3 Übersetzung der ICMP-Header

Die ICMP-Felder sind nur sehr eingeschränkt oder gar nicht übersetzbar. In den nachfolgenden beiden Tabellen sind jeweils die Abbildungen der ICMP-Nachrichten zwischen den beiden Protokollversionen prinzipiell dargestellt, ohne die Details der jeweiligen Anpassungen. Die ICMP-Checksum-Werte sind immer zu korrigieren, da bei ICMPv6 die Pseudoheader wie bei der TCP- und UDP-Prüfsumme mit in die ICMP-Prüfsummenberechnung einzubeziehen sind.

Eine Tabelle mit ICMP Nachrichten vom Type 0 bis 36 befindet sich unter dem Kapitel Anhänge. [RFC 792] [RFC 2463] [www.feuerwallshop.de]

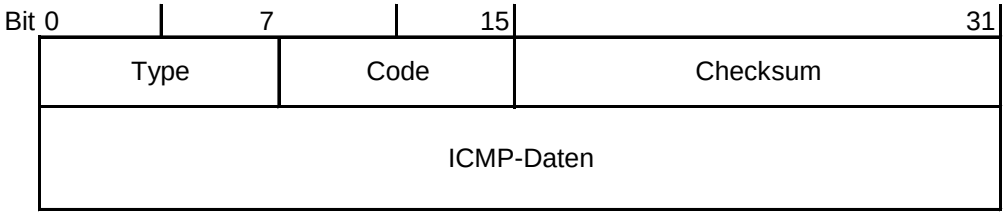


Bild 4.6Grundsätzlicher Aufbau des IPv6-ICMP-Pakets

[46] minus 8 Bit wegen IPv6 Fragment Header

Bedeutung der Felder:

Type: Typ des IP-Paketes, Fehlermeldungen haben dabei Werte von 0-127, Steuerungs- und Statusmeldungen haben Werte von 128-255.

Code: Unterfunktion innerhalb des gegebenen Typs, abhängig vom Feld Type

Checksum: Prüfsumme über das gesamte ICMP-Paket inklusive IP-Pseudoheader

ICMPv4 (Eingang)	ICMPv6 (Ausgang)
Echo Request / Reply (Typ 8 und 0)	Echo Request / Reply (Typ 128 und 129)
Timestamp Request / Reply (Typ 13 und 14)	Wird verworfen
Address Mask Request / Reply (Typ 17 und 18)	Wird verworfen
Destination Unreachable (Typ 3)	Destination Unreachable (Typ 1) Übersetzung des Code-Feldes für ICMPv6
Redirect (Typ 5)	Wird verworfen
Source Quench (Typ4)	Wird verworfen
Time Exceeded (Typ 11)	Time Exceeded (Typ 3) Code-Feld unverändert
Parameter Problem (Typ 12)	Parameter Problem (Typ 4)

Tabelle 4.1 Abbildung von ICMPv4- auf ICMPv6- Nachrichten

ICMPv6 (Eingang)	ICMPv4 (Ausgang)
Echo Request / Reply (Typ 128 und 129)	Echo Request / Reply (Typ 8 und 0)
ICMP-Multicast-Messages (Typ 130, 131 und 132)	Werden verworfen
Neighbor- and Router-Solicitation (Typ 133, 134, 135,136 und 137)	Werden verworfen
Destination Unreachable (Typ 1)	Destination Unreachable (Typ 3) Übersetzung des Code-Feldes für ICMPv4
Paket to big (Typ 2)	Destination Unreachable (Typ 3) mit Code = 4
Time Exceeded (Typ 3)	Time Exceeded (Typ 11) Code-Feld unverändert
Parameter Problem (Typ 4)	wenn Code = 4: Time Exceeded (Typ 3) andere Codes: Parameter Problem (Typ 12)

Tabelle 4.2 Abbildung von ICMPv6- auf ICMPv4- Nachrichten

4.4 Tunneling

Wozu braucht man Tunnel?

Wenn zwei reine IPv6-Rechner aus unterschiedlichen Netzen versuchen, miteinander Daten auszutauschen, aber auf dem Weg liegen Router, die nur IPv4 beherrschen, so würden die Daten nicht ankommen. Ein Tunnel hat nun die Aufgabe, die Daten an das dazwischenliegende Medium anzupassen. Die Daten werden so verpackt, dass sie auch im IPv4 Netz richtig weitergeleitet werden. Am Tunnel-Endpunkt in einer IPv6 Umgebung werden die Daten wieder in den Ausgangszustand transferiert und können den Zielrechner erreichen.

Damit können ISPs Ende-zu-Ende IPv6 Service anbieten, ohne dass größere Umrüstungen der vorhandenen Infrastruktur vonnöten wären.

Mittlerweile stehen verschiedene Tunnelmechanismen zur Verfügung. Es gibt manuell konfigurierte IPv6 Tunnel, wie in RFC 2893 beschrieben [31] und IPv6 over IPv4 GRE[47] Tunnel, halbautomatisch aufgesetzte Tunnel, wie Tunnel Broker sie verwenden, aber auch rein automatisch konfigurierte Tunnel, wie bei 6to4 und IPv4-kompatiblen. Bei den manuell aufzusetzenden und den GRE Tunneln müssen Anfangs- und Endpunkt des Tunnels konfiguriert werden, im Gegensatz zu den automatisch konfigurierten Tunneln, die nur aktiviert werden müssen. Letztere werden dann nur für die jeweilige Kommunikation aufgesetzt und wieder deaktiviert, sobald alle Daten ausgetauscht sind.

Für Router gilt ein Tunnel immer als ein Hop, egal, wieviele IPv4 Zwischenstationen passiert werden. Im allgemeinen sollten Tunnel eher vermieden werden, da sich die zusätzliche Paketbearbeitung negativ auf die Performance der involvierten Router auswirkt.

Tunnelmechanismus	Einsatzbereich	Vorzüge	Einschränkungen	Anforderungen
IPv6 manuell konfigurierter Tunnel	Stabile, sichere Verbindung für übliche Kommunikation Verbindung zum 6Bone	Verlangt kein DNS das auf IPv6 aufgerüstet wurde	Nur Tunnel zwischen 2 Endpunkten Großer Verwaltungsaufwand Kein unabhängig verwaltetes NAT	Vom ISP registrierte IPv6 Adressen Dual-Stack Router
IPv6 over IPv4 Tunnel	ISP mit IPv6 Service Angebot Enterprise[48] mit IPv6 Bedarf Stabile, sichere Verbindung für übliche Kommunikation	Bekannte standard Tunneltechnik Geringe Kosten, geringes Risiko Einfach zu implementieren	Nur Tunnel zwischen 2 Endpunkten Großer Verwaltungsaufwand Kein unabhängig verwaltetes NAT Nicht für Verbindung zum 6Bone geeignet	Vom ISP registrierte IPv6 Adressen Dual-Stack Router Wird verlangt von i/IS-IS für IPv6
Tunnel Broker	Autonome isolierte IPv6 Endsysteme	Tunnel wird vom ISP aufgesetzt und verwaltet	Mögliche Sicherheits-auswirkungen	Tunnel Broker Service muss proprietäre Protokolle kennen
Automatischer IPv4-kompatibler Tunnel	Einzelne Hosts oder kleine Standorte Unregelmäßige Kommunikation		Kommunikation nur mit anderen IPv4-kompatiblen Standorten Skaliert nicht gut Kein unabhängig verwaltetes NAT	IPv6 Präfix (0::/96) Dual-Stack Router

[47] Generic Routing Encapsulation
[48] Unternehmen

Automatischer 6to4 Tunnel	Verbindung mehrfacher remote IPv6 Domains Häufige Kommunikation	Einfach aufzusetzen ohne Verwaltungsaufwand	Kein unabhängig verwaltetes NAT	IPv6 Präfix (2002::/16) Dual-Stack Router
6over4 Tunnel	Übergang von Standorten ohne Router			

Tabelle 4.3 Überblick über verschiedene Tunnelmechanismen mit Einsatzbereich [34]

4.4.1 Layer Two Tunneling Protocol

Das Layer Two Tunneling Protocol (L2TP) unterstützt ein transparentes Tunneln von PPP[49]-Paketen durch ein dazwischenliegendes Netzwerk. [32] Das Point-to-Point Protokoll dient zur Kopplung von LANs über WANs und wird mittlerweile sehr häufig für Internetzugänge verwendet. Dabei bekommt der Benutzer eine Schicht Zwei Verbindung zu einem Zugangsserver (NAS - Network Access Server) durch Einwahl (z. B. mittels Modem, ISDN, ADSL), um dann über die Verbindung PPP zu betreiben. Die Endpunkte der Schicht Zwei Verbindung und der PPP Sitzung liegen hierbei auf demselben physikalischen Gerät, z. B. dem NAS.

L2TP ermöglicht, dass diese Endpunkte auf verschiedenen Geräten liegen können, welche über ein paketvermitteltes Netzwerk verbunden sind. Der Benutzer hat eine Verbindung zu einem Zugangskonzentrator (z. B. DSLAM), welcher die PPP Pakete zum NAS tunnelt.

Für den Benutzer macht es keinen großen Unterschied, außer, dass er mit L2TP nicht für eine überregionale Verbindung zahlen muss, da der Layer Two Endpunkt lokal ist. Ein weiterer Vorteil von L2TP liegt im Einsatz von Multilink PPP[50]. Dabei müssten alle Kanäle, die zu einer Multilink Verbindung gehören, auf *einem* NAS angesiedelt sein. Ist dies nicht der Fall, können mittels L2TP alle Kanäle dennoch auf einem einzigen NAS abgeschlossen werden.

[49] Point-to-Point Protocol
[50] wird zur Zusammenfassung von ISDN B Kanälen verwendet; siehe auch RFC 1990

4.4.2 Point-to-Point Tunneling Protocol

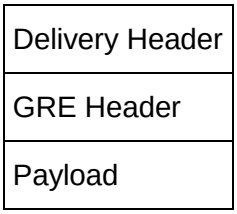
Mit dem Point-to-Point Tunneling Protocol (PPTP) kann das PPP durch IP-Netzwerke getunnelt werden. Eine Client-Server Architektur ist definiert worden, um Funktionen, die bei aktuellen Zugangsservern bestehen, zu entkoppeln und um VPNs[51] zu unterstützen. Der PPTP Netzwerk Server (PNS) läuft auf einem normalen Betriebssystem, während der Client, der PPTP Access Concentrator (PAC), auf einer Einwahl-Plattform arbeitet. Der PNS kann den Zugang von leitungsvermittelten Einwahl-Verbindungen, die von PSTN oder ISDN stammen, kontrollieren oder leitungsvermittelte Verbindungen nach außen aufbauen.

PPTP verwendet einen erweiterten GRE Mechanismus um einen Datagramm-Service zur Verfügung zu stellen, der gekapselte PPP Pakete transportiert und sowohl fluss- als auch lastgesteuert ist.

Benutzer, die sich in verschiedene PACs einwählen, können eine einzige IP-Adresse erhalten, sofern sie von einem gemeinsamen PNS bedient werden. Genauso werden in einem Firmennetz, das nicht registrierte IP-Adressen verwendet, von einem zugehörigen PNS Adressen zugewiesen, die nur für das private Netzwerk gelten. IP-fremde Protokolle, wie z. B. Appletalk und IPX, können durch einen nur-IP Provider getunnelt werden, ohne dass der PAC diese Protokolle weiterleiten können muss. In Bezug auf Multilink PPP bringt PPTP denselben Vorteil, wie schon unter L2TP beschrieben.

4.4.3 Generic Routing Encapsulation

Generic Routing Encapsulation (GRE), beschrieben in RFC 1701, ist ein Weg Daten zu kapseln, um sie auch mithilfe anderer Protokolle weiterleiten zu können. [29] Dabei werden die Daten als "Payload" in ein sogenanntes GRE-Paket gekapselt, welches einen Pfad beinhalten kann. Das so entstandene Paket wird dann in ein anderes Protokoll eingebunden und weitergeleitet. Dieses "äußere" Protokoll wird *delivery protocol* genannt. Hieraus ergibt sich folgende Form:



[51] Virtual Private Network

Im GRE Header sind Informationen enthalten, wie z. B. welchen Protokolltyp die Payload hat, Routinginformationen, Authentifizierung, Sequenznummer.

In RFC 1702 ist GRE im Zusammenhang mit IPv4 dargestellt. [30] Fungiert IP als Delivery Protocol, so steht im Protokollfeld des GRE Headers die 47 für IPv4. Ist die Payload IPv4, so steht 0x800 im Protokollfeld. Dann wird im Routing Feld eine Liste von IP-Adressen oder Autonomous System Nummern enthalten sein.

4.4.4 Automatischer 6to4 Tunnel

Diese Variante des automatischen Tunneling beschreibt die Möglichkeit, jeder Site mit einer eindeutigen IPv4-Adresse einen eindeutigen IPv6-Adresspräfix zuzuweisen. Die mit einem solchen Präfix ausgestatteten IPv6-Pakete werden dann über das IPv4-Netz transportiert. Ein 6to4-Router, welcher sich normalerweise zwischen der IPv6-Site und dem IPv4-WAN befindet, leitet die Pakete anhand des IPv6 Präfixes an das korrekte Ziel.

4.4.5 IPv6 over IPv4 Tunnel

Der Versand des IPv6-Pakets geschieht bei 6 over 4 in einem IPv4-Multicast-Paket, so dass jeder Host der Multicast-Gruppe das Paket empfängt und ggf. an den IPv6-Stack weiterleitet. Bei Übereinstimmung der Paketadresse mit der IPv6-Empfängeradresse wird es vom IPv6-Stack bearbeitet. Dieses Verfahren eignet sich für denn Fall einzelner IPv6-Hosts in einem IPv4-LAN. [RFC 2529]

4.4.6 MPLS

Multiprotocol Label Switching (MPLS) besteht aus einer Reihe von Protokollen, die Schicht 2 Switching Technologien und Schicht 3 Routing Strategien miteinander vereinen. [33] Dadurch hat es Vorzüge in Sachen Vorhersagbarkeit des Verkehrsaufkommens, Skalierbarkeit und Management. Einsatzmöglichkeiten bestehen bei der Bildung von VPNs, Traffic Engineering (TE), QoS und Tunneling. Ein Verkaufsargument für MPLS ist, dass bestehende Investitionen nicht umsonst getätigt wurden, sondern nur ein Aufrüsten und eventuell Ergänzen vorhandener Netztopologien notwendig wird.

Mit MPLS werden den Datenpaketen sogenannte *Label*[52] vergeben, anhand derer ein modifizierter Switch oder Router die Wegewahlentscheidung für das Weiterleiten im Netzwerk trifft, statt nach der längsten Übereinstimmung in der Routingtabelle zu suchen. Damit ist ersichtlich, dass beteiligte Geräte MPLS implementiert haben müssen.

[52] Etikett; in diesem Zusammenhang ein Wert (Nummer)

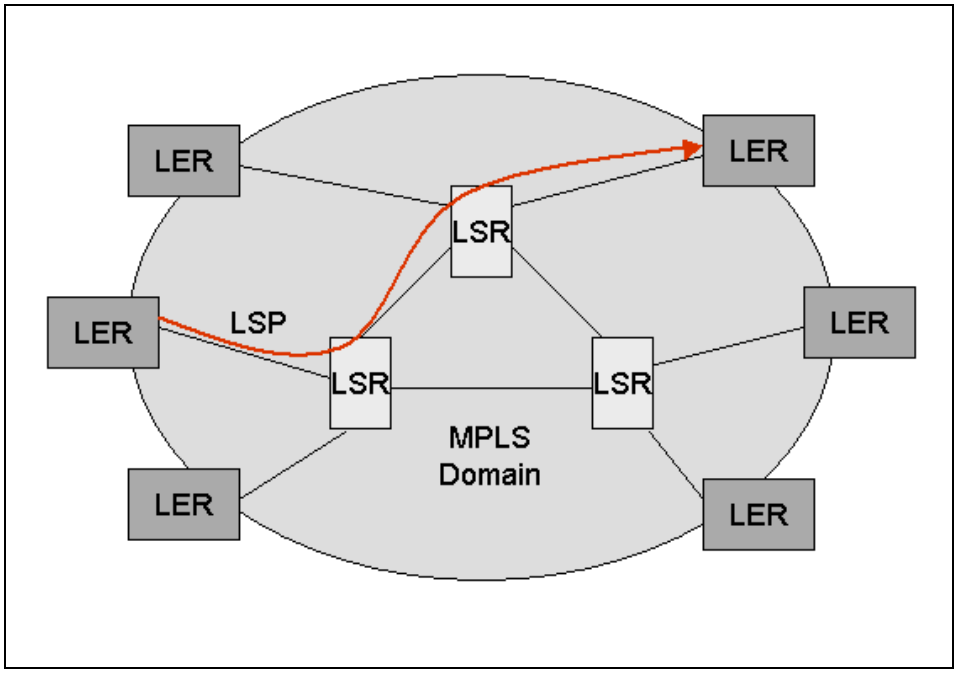


Bild 4.7 MPLS Terminologie

Im Bild ist schematisch ein Netzaufbau mit MPLS dargestellt, um die Terminologie einzuführen:

- **LER**
  Label Edge Router sitzt am Rand einer MPLS Domain und vergibt aufgrund der Routinginformationen die Label, anhand derer innerhalb der Domain weitergeleitet wird.
- **LSP**
  Label Switched Path ist der Pfad, den ein Datagramm aufgrund seines Labels innerhalb des Netzes nimmt.
- **LSR**
  Label Switching Router sitzen innerhalb der MPLS Domain und können Datagramme aufgrund ihrer Label weiterleiten.
- **MPLS Domain**
  Teil eines Netzwerks der MPLS-fähige Geräte enthält.

Die Label werden zwischen dem Netzwerkschicht-Header und dem Internetschicht-Header (nach dem TCP/IP Layer Modell) eingefügt und sind 4 oder 8 Byte lang.

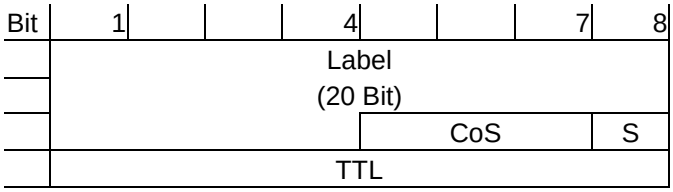


Bild 4.8 MPLS Label Stack

- **Label**

  Das 20 Bit Label enthält einen bestimmten Wert, anhand dessen zusammengehörender Datenverkehr entsprechend weitergeleitet wird

- **CoS**

  Im 3 Bit breiten *Class of Service* Feld werden Werte abgelegt, die die Art der Weiterleitung der Pakete beeinflussen.

- **S**

  Dieses Bit markiert den letzten Eintrag im Label Stack, wenn es gesetzt ist.

- **TTL**

  Das Time to Live Feld markiert die Lebensdauer eines Pakets mit 8 Bit.

Die Technologie der Labelvergabe prädestiniert MPLS zum Aufbau von VPNs, macht es aber auch denkbar, dass es während der Übergangsphase von IPv4 zu IPv6 statt anderer Tunnelmechanismen eingesetzt wird. Arbeitsgruppen der IETF befassen sich immer noch mit der Weiterentwicklung von MPLS.

4.4.7 Tunnel Broker

Ein Tunnel Broker ist ein Service, der es ermöglicht, von einem IPv6 Einwahl PC mit Dual-Stack oder einem an einen Dual-Stack Router angeschlossenen IPv6 Rechner Zugang zu einem IPv6 Backbone zu erhalten. Der Unterschied zu anderen Tunnelmechanismen ist, dass dies ein Service ist, der von ISPs angeboten wird. Der Tunnelab- und aufbau wird von dem Service übernommen und ist für den Endnutzer transparent. Hierzu muss sich der Endnutzer bei dem Service Provider registrieren, um ein Skript zu erhalten, dass den Tunnel zum IPv6 Netzwerk aufbaut. Der ISP ordnet dem Endsystem eine IPv6 Adresse zu und dem Router eine Netzwerk Präfix, um Zugang zum Rest der Site zu erlauben.

Ein Nachteil des Tunnel Brokers ist, dass das Endsystem (oder der Router) eine Änderung der Konfiguration durch einen Einwahl Server akzeptieren muss, was ein potentielles Sicherheitsrisiko darstellt. Nicht alle ISPs bieten diesen Dienst an und die Skriptdatei muss kompatibel zu den verwendeten Geräten sein.

4.5 Technische Realisierung

Es werden die für die Übergangsphase bereits angebotenen Lösungen namhafter Hersteller von Netzwerkkomponenten aufgezeigt.

- **Cisco**

  Cisco vertritt die Ansicht, dass es besser sei, bestehende Netzwerke von den äußeren Grenzen an in Richtung Kernnetz zu migrieren. So kann man die Umstellungskosten gut überwachen und sich auf die Anforderungen der Anwendungen konzentrieren, statt ein komplettes reines IPv6 Netzwerk auf einmal erschaffen zu müssen. Ihre IPv6 Router Produkte bieten für diese Strategie die entsprechenden Funktionen.

  Im Mai 2001 hat Cisco offiziell bekannt gegeben, dass IPv6 in seiner IOS Software verfügbar ist und damit mannigfaltige Systemplattformen unterstütze. Im Moment würde sich der Service jedoch hauptsächlich an erste Kunden aus der Funk-, Spiel- und Heimnetzwerkindustrie wenden. Die weitere Entwicklung von IPv6 und seinen Applikationen wird, wie Cisco versichert, auch in Zukunft von ihnen unterstützt. [37] So ist in der Network World Germany im Dezember 2001 zu lesen, dass Cisco nun den Dual-Stack Betrieb und MPLS durch die IOS Software zur Verfügung stellt. Es wird angekündigt, dass eine hardwaregestützte Weiterleitung ab Mitte 2002 unterstützt wird.

- **Nortel Networks**

  Bereits im Oktober 1997 hat Nortel in seiner BayRS Software in der Release 12.0 IPv6-Funktionalitäten eingebaut. IPv6 RIP, statische Routen und TCP wurden damit schon unterstützt. Es können sowohl statische Tunnel (IPv6- Adressen) als auch automatische Tunnel mit IPv4- kompatiblen Adressen verwendet werden.

Folgende Auflistung von Nortelprodukten, die IPv6 unterstützen, steht im Internet[53], - leider ohne Aktualitätshinweis:

- Baystack AN/ANH Routers
- ARN Router (Advanced Remote Node)
- ASN (Access Stack Node)
- Passport 5430
- BN Backbone Node

- **Juniper**

  Anfang November 2001 hat Juniper Networks IPv6 in Junos 5.1 integriert, wodurch alle Router der M-Serie mittels eines Software-Upgrades IPv6-fähig werden. Diese Router werden vornehmlich im Backbonebereich, sowie auch im Zugangs- und in den Randbereichen eingesetzt. Junipers Lösung basiert ebenfalls auf der Dual-Stack Strategie, um "einen unterbrechungsfreien Übergang ohne Performanceprobleme" [38] zu gewährleisten. Router können IPv6-Pakete mit Wirespeed aufgrund von ASICs (Application Specific Integrated Circuits) weiterleiten. Drei Kunden werden genannt, die IPv6 testen, bzw. bereits produktiv nutzen:

  - Gip Renator (internationales Forschungsnetz aus Frankreich)
  - 6Tap (Betreiber eines IPv6-Exchange-Points in Palo Alto)
  - France Telecom

- **Foundry Networks**

  Foundrys Routing-Switches unterstützten IPv6 in VLANs bereits im Dezember 2001, der Hardwaresupport soll Anfang 2002 hinzukommen. Bis Mitte 2002 soll die IPv6-Software "ZebOS" von IP Infusion integriert werden. Bobby Johnson, Präsident und CEO von Foundry Networks, ist jedoch der Meinung, dass sich IPv6 in Amerika nicht in naher Zukunft durchsetzen wird, da die ISPs viel Geld in die IPv4 Ausstattung gesteckt haben und sich dies erst rechnen muss. [39]

[53] www.nortelnetworks.com Suchbegriff: IPv6

- **Redback Networks**

  Anlässlich der Exponet im November 2001 in Köln hatte Pan Dacom die Ehre Ravi Chandra auf ihrem Stand begrüßen zu dürfen. Dabei ergab sich die Gelegenheit, diese Koryphäe in Sachen Routing Protokolle interviewen zu können. Zum Thema IPv6 befragt, wies er auf die geringe Notwendigkeit für die USA hin.

  Mit dem SmartEdge 800 Router steht jedoch MPLS- und IPv6- Unterstützung zur Verfügung. [40]

5 Mobility – Funktionen in IPv6

Mit der ständigen Verkleinerung von elektronischen Geräten und Bauteilen finden mobile Geräte in zunehmendem Maß Verbreitung. Handys, Laptops und Organiser bringen meist die Fähigkeit zur Kommunikation mit Bürocomputern (zumindest optional) mit. Diese müssen dazu aber oft mit sehr spezieller Funktionalität aufgerüstet werden, was bedeutet, dass der Zugriff der mobilen Geräte auf Ressourcen des Netzes ortsgebunden ist. Manche Funktionalität, die sonst dem heimischen Computer vorbehalten ist, möchte man aber gerne mitnehmen. Dabei müssen allerdings Authentizität des Gerätes bzw. Benutzers sowie Zuverlässigkeit der Datenübertragung gewährleistet sein.

Denkbar sind mobile Anwendungen für

- Administration (Fernwartung / -bedienung)
- Web-Surfen
- eMail
- Up- / Downloads
- Multimedia-Dienste u.v.m.
- Videoconferencing

Für die schnellen Strukturänderungen, die die Mobilität von Rechnern mit sich bringt, ist die ursprüngliche Architektur des Internet nicht gedacht gewesen. Zwar wurden durch einige Protokolle, wie z. B. ARP (Address Resolution Protocol), BOOTP (Bootstrap Protocol), DHCP (Dynamic Host Configuration Protocol), die bei Strukturänderungen erforderlichen Umkonfigurationen automatisiert, aber das meiste muss jedoch immer noch per Hand getan werden. Die angebotenen Dienste müssen daher im Zusammenhang mit Mobilität überdacht und gegebenenfalls angepasst oder neu implementiert werden. Mobile IP z. B. ergab sich als eine solche Anpassung des durch IP festgelegten Vermittlungsdienstes (Routing). Beim Transportdienst (TCP) ist man sich einig, dass angepasst werden muss, man weiß aber noch nicht wie.

Schließlich ergeben sich durch Mobilität auch Anforderungen für gänzlich neue Dienste. Ein Beispiel ist die Aufenthaltsbestimmung, die eine Voraussetzung für die Anpassung des Vermittlungsdienstes und daher in Mobile IP integriert ist. Ein anderes Beispiel ist die

Identifikation von Diensten, also das Herausfinden ihrer IP-Adressen. Das neue Protokoll SLP (Service Location Protocol) wird dies weitgehend automatisieren.

Nachfolgend werden Begriffe erklärt, die für Mobility Funktionen von besonderer Bedeutung sind:

Mobile Node (MN)

- mobiles Gerät mit fester IP-Adresse (Home Address)
- mit wechselnden Anschlusspunkten zum Netz

Home Network

- Subnetz, in dem sich die Home Address befindet

Home Agent (HA)

- verwaltet aktuellen Standort des Mobile Node
- befindet sich im Home Network

Visited Network

- fremdes Subnetz, in dem sich der Mobile Node gerade befindet

Foreign Agent (FA)

- bietet Internetanschluss für Mobile Node an
- vergibt die jeweilige Care-of Address

Care-of Address (CoA)

- IP-Adresse, über die der Mobile Node erreichbar ist
- entweder IP-Adresse des Foreign Agent
- oder "eigene" IP-Adresse für den Mobile Node

Correspondent Node (CN)

- Kommunikationspartner des Mobile Node

Agent Advertisement

- Anbieten von Diensten zur Mobilkommunikation in einem Subnetz
- Aushandeln von Modalitäten

Agent Solicitation

- Anfordern von Diensten zur Mobilkommunikation in einem Subnetz

Register Request

- Anfrage eines MN nach Registrierung der COA
- muss authentifiziert sein

Register Reply

- Bestätigung der Registrierung der COA
- muss authentifiziert sein

5.1 DHCP

DHCP (Dynamic Host Configuration Protocol) ist per Definition zur dynamischen Konfiguration von IP-Netzen fähig. Jeder DHCP-Client kann dabei jederzeit einen gegebenenfalls inzwischen geränderten Parameter der IP-Konfiguration erneuern. Dazu muss er lediglich eine DHCP-Request-Meldung an den DHCP-Server senden. Die Neuvergabe von IP-Adressen wird mit Renumbering bezeichnet. Die Notwendigkeit für Renumbering tritt zum Beispiel auf, wenn ein anderer ISP die Versorgung eines Netzes übernimmt. Zwar ist DHCP zum Teil von sich aus in der Lage, das Renumbering zu bewerkstelligen, das gilt jedoch nur, wenn ein DHCP-Client einen bestehenden Lease zu verlängern sucht. In diesem Fall kann der DHCP-Server den Client mittels eines "DHCPNAK" (DHCP negative acknowledgement) auffordern, sich eine neue IP-Adresse zuteilen zu lassen. Jedoch stellt Renumbering keinen offiziellen Bestandteil der DHCPv4-Spezifikationen dar, daher muss man gegebenenfalls den DHCP-Server veranlassen, diese Funktion zu unterstützen. DHCPv4 sieht ebenfalls nicht vor, dass ein DHCP-Server seine Clients zu einer Rekonfiguration auffordert. Dieses Manko wurde bei DHCPv6/IPv6 beseitigt. Bei IPv4 musste sich der Server für das Renumbering auf die Anfrage der Clients zur Lease-Verlängerung stützen.

Ändert sich in einer IPv6/DHCPv6-Umgebung etwa die Adress-Situation (etwa durch den Umzug eines Netzwerkdruckers in eine andere Abteilung), so kann DHCPv6 die notwendigen Änderungen für die DHCP-Clients von sich aus mit Hilfe der DHCP

Reconfigure-PDU (Protocol Data Unit)[54] durchführen. Sobald eine Änderung in der Netzkonfiguration der Clients erforderlich wird, prüft der Server in seinem Datenbestand für die zu versorgenden Clients, welche Clients von der Änderung betroffen sind und schickt an sämtliche in Frage kommenden Clients ein "DHCP Reconfigure". Dazu fügt er die zu verändernden Parameter als Extensions bei. Die Clients empfangen das Reconfigure vom Server und senden ihrerseits einen neuen DHCP Request an den Server, wiederum mit den gewünschten Parametern als Extensions. Der weitere Ablauf der Rekonfiguration entspricht dem oben geschilderten Verhalten des Clients. [21]

5.2 Tunneling über HLR (GPRS) mit IPv4

GPRS (General Packet Radio Service) ist ein paketvermitteltes Datenübertragungssystem, das für GSM Mobilfunksysteme vorgesehen ist. GPRS-Systeme benutzen eine eigene Infrastruktur, die zum GSM-Teil über einen sogenannten SGSN (Serving GPRS Support Node) und zum Internet hin über einen GGSN-Router (Gateway GPRS Support Node-Router) angebunden ist. HLR (Home Location Register) ist ein Standortverzeichnis für Mobilfunk.

Für die Weiterleitung der Daten, die für ein entferntes Gerät bestimmt sind, verpackt der jeweilige Router die Pakete, indem er sie mit einem neuen Header versieht, und schickt sie an den aktuellen Aufenthaltsort des Empfängers. Dort wird das Paket angenommen und der zusätzliche Header wieder entfernt. In Mobile IP sind verschiedene Arten dieser Kapselung vorgesehen.

Man unterscheidet zur Zeit drei Tunneling Techniken:

- IP-in-IP-Kapselung

Verpflichtend sieht der RFC eine IP-in-IP-Kapselung vor, bei der das komplette IP-Paket, also Nutzdaten und Header als neues Datagramm mit einem neuen IP-Header versehen werden. Dies stellt die einfachste Art der Adressierung für das Tunneling dar. Die neue Source Address ist die des Home Agents, die Destination Address ist die registrierte Care-of Address des Mobile Nodes. Andere Felder des Headers werden einfach kopiert.

- Minimale Kapselung

Optional kann der neue Header durch eine Ergänzung des alten mit den unbedingt nötigen Informationen erzeugt werden. Unwichtige Header-Felder werden dabei weggelassen. Dabei

[54] Protokolldateneinheit einer Schicht im OSI Modell

nicht kopierte Header-Felder sind u.a. Fragment Offset und Flags, weshalb fragmentierte Datagramme nicht minimal gekapselt werden können.

- Generic Routing Encapsulation (GRE)

Ebenfalls optional ist die Implementierung der Generic Routing Encapsulation, die entwickelt wurde, um Daten mit verschiedenen Protokollen in IP-Paketen zu verpacken. U.a. werden die Protokolle OSI Network Layer, Vines und Apple Talk unterstützt. Beim Einsatz mit Mobile IP entsteht durch diese größere Funktionalität aber auch ein größerer Overhead.

Nachfolgendes Bild verdeutlicht den Kommunikationsablauf durch Tunnel bei Mobile IPv4:

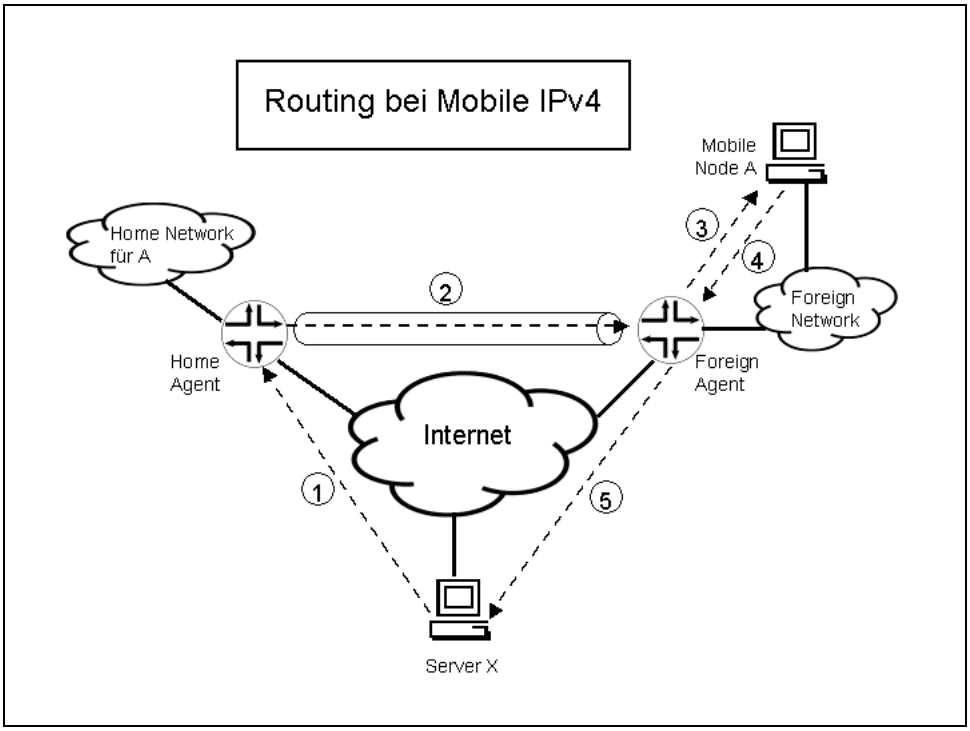


Bild 5.1 Triangular Routing bei Mobile IPv4

- (1) Ein Server X sendet Daten an den Mobile Node A. Diese werden in das Home Network von A übertragen.

- (2) Im Heimatnetz fängt der Home Agent die Daten für A ab, packt sie als Nutzlast in neue IP-Pakete und trägt als Ziel die Care-of Address des Mobile Node A ein. Dieses Verfahren heißt »Tunneling«.

- (3) Der Foreign Agent im Fremdnetz empfängt die IP-Pakete, packt die Nutzlast aus und schickt diese über den Link-Layer zum Mobile Node.

- (4) Will der Mobile Node A Daten an den Server X senden, kann er das direkt aus dem Fremdnetz heraus tun. Er versieht dazu die IP-Pakete mit der Zieladresse von X und der Adresse, die er im Home Network besitzt.

- (5) Das IP-Paket wird über das Internet zum Server X übertragen.

Die Anforderung der Kompatibilität zu IPv4 bringt nicht nur Vorteile mit sich. Dadurch, dass vermittelnde Geräte auf dem Datenpfad Mobile IP nicht unterstützen, muss die Funktionalität in den involvierten Agenten gebündelt sein. Es entstehen Umwege, daher ist eine Optimierung nur begrenzt möglich.

Eine Möglichkeit ist das "*Triangular Routing*".

Alle Pakete werden zunächst vom Correspondent Node zum Home Agent gehen und erst von dort zum Mobile Node getunnelt (Triangular Routing). Es entsteht außer dem Protokoll-Overhead durch den längeren Datenpfad eine Verzögerung und eine größere Netzlast. Als Verbesserung könnte der Home Agent die Care-of Address an den Correspondent Node übermitteln. Dieser muss mit der Information aber umgehen können, wovon keinesfalls ausgegangen werden kann. Darüber hinaus kann es aus Fragen der Sicherheit unerwünscht sein, dass Kommunikationspartner über den aktuellen Aufenthaltsort des Mobile Nodes (und dessen Benutzers) informiert werden.

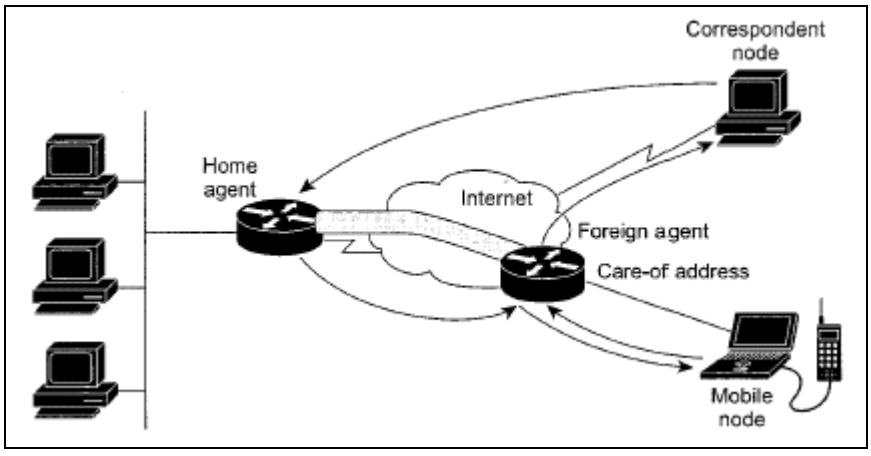


Bild 5.2 Triangular Routing

Eine weitere Möglichkeit ist das "*Reverse Tunneling*".

Es ist vorgesehen, dass der Mobile Node Daten an den Correspondent Node direkt versendet. U.a. aus dem vorgenannten Grund gibt er aber als Source Address seine IP-Adresse (die Home Address) an, welche aber im Fremdnetz topologisch inkorrekt ist. Router können die Weitergabe solcher Pakete verweigern. Abhilfe schafft das in RFC 2344 beschriebene Reverse Tunneling. Hierbei tunnelt der Mobile Node die Daten unter Angabe der Care-of Address als Source Address zunächst zum Home Agent, welcher die Pakete entpackt und korrekt adressiert an den Correspondent Node weitersendet. Das führt allerdings wiederum zu Verzögerung, erhöhter Netzlast und geringer Skalierbarkeit.

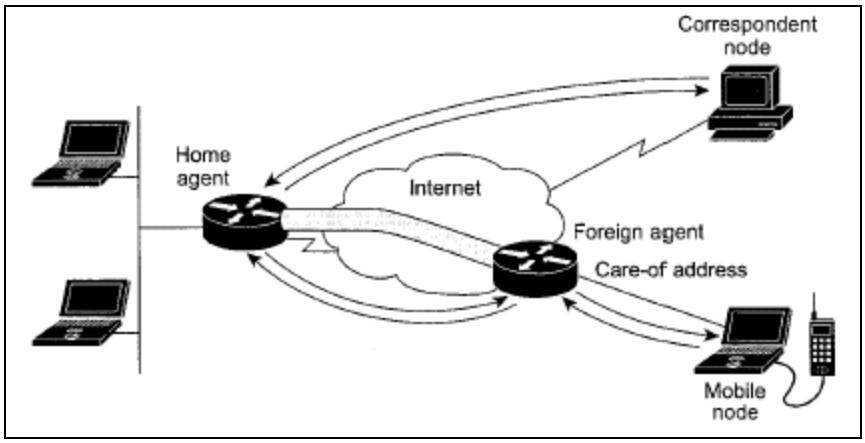


Bild 5.3 Reverse Tunneling

5.3 Autokonfiguration / Mechanismus

Sobald ein IPv6-Interface gestartet wird, sucht dieses selbstständig nach einem Router, der ihm eine gültige IPv6-Adresse zuweisen kann. Nachfolgend gehen wir hierzu detaillierter ein:

Damit sich das Interface vom kontaktierten Router überhaupt ansprechen lässt, generiert es zunächst selbstständig und automatisch eine vorläufige Adresse aus dem Link-Local-Bereich, also FE8.... Dabei kommt ein speziell festgelegtes Verfahren zum Einsatz, das die MAC-Adresse des Interfaces benutzt, um die Eindeutigkeit der lokalen Verbindung zu garantieren. Bei der EUI64-Spezifikation wird in der Mitte der 48 Bit langen MAC-Adresse die 16-Bit-Folge FFFE eingeschoben, sodass eine derart generierte Link-Local-Adresse zum Beispiel so aussieht: FE80::XZXX:XXFF:FEYY:YYYY/64, wobei X und Y aus der Ethernet-MAC-Adresse übernommen werden. Zur Eindeutigkeit führt diese Konstruktion erst dadurch,

dass das zweitletzte Bit des ersten Bytes der MAC-Adresse auf 1 gesetzt wird, das heißt, das Halbbyte Z muss gerade sein.

Ist das IPv6-Interface aktiviert, sendet dieses zunächst sogenannte Router Solicitations (RS) an eine spezielle Multicast-Adresse, nämlich FF02::2. Diese Adresse symbolisiert sämtliche erreichbaren Router. Sofern dadurch ein Router angesprochen wird, antwortet er mit einem Router Advertisement (RA). Dieses Verfahren wird auch "Stateless Autoconfiguration" genannt, da der Administrator nicht vorab festlegen muss, welche IP-Adressen vergeben werden.

Der Router selbst muss lediglich das Präfix und dessen Länge konfigurieren. Wenn dabei ein Präfix aus dem Bereich der global eindeutigen IPv6-Adressen zum Einsatz kommt, kann sich das IPv6-Interface damit seine Adresse selbst ausrechnen. Dabei braucht das Interface lediglich die ersten 64 Bit (Präfix FE80::/64) mit dem im RA verschickten Präfix. Aus dem RA kann das Interface zudem den Default Gateway auslesen, so dass theoretisch die Konfiguration am Endgerät entfällt.

Es gibt noch eine weitere Methode zur Autokonfiguration, die sogenannte Neighbor Discovery. Diese gewährleistet die Eindeutigkeit dadurch, dass das Interface eine so genannte "Neighbor Solicitation" an die spezielle Multicast-Adresse FF02::1 schickt, mit der eben generierten Adresse als Absender. Falls es genau diese Adresse bereits gibt, kann der betroffene Doppelgänger darauf antworten und das Interface nimmt dann einen erneuten Anlauf mit anderer Adresse.

"Stateful Autoconfiguration" bezeichnet die zentrale Konfiguration der möglichen Adressen sowie zusätzlicher Informationen über das DHCPv6-Protokoll (Dynamic Host Configuration Protocol). Bei der DHCP-Erweiterung für IPv6 lassen sich auch aufwändige Konfigurationen zentral verwalten.

Stateful- und Stateless Autoconfiguration schließen sich gegenseitig nicht aus, sondern ergänzen sich. So kann beispielsweise einem Host mit Hilfe von Stateless Autoconfiguration eine firmenweite Adresse zugewiesen werden, mit der sich dann dieser Rechner selbstständig bei einem zentralen DHCPv6-Server eine globale Adresse mit DNS-Konfiguration holt. Dabei wird der Rechner gleichzeitig im DNS-Server eingetragen. [23]

5.4 Mobile IP

Da in Zukunft die Anzahl der mobilen Internetnutzer, welche von einem Ort zum anderen reisen und dort immer unter ihrer Heimatadresse erreichbar sein wollen, stark wachsen wird, wurde unter dem Namen "Mobility Support in IPv6" eine spezielle Unterstützung für diese Fälle definiert. [24]

Mobile IP ist ein Protokoll, das aus drei Komponenten besteht:

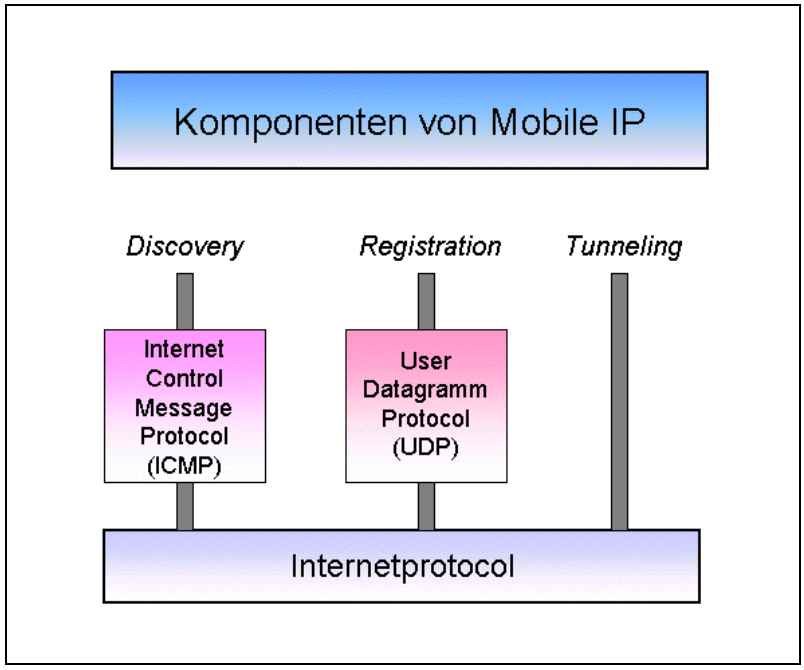


Bild 5.4 Komponenten von Mobile IP

Als Ergänzung des z.Zt. eingesetzten IPv4 werden an Mobile IP laut RFC 2002 folgende Anforderungen gestellt:

- Kommunikation mit mobilen Endgeräten

  Angeschlossene bewegliche Geräte sollen den Kontakt zum Netz behalten.

- gleichbleibende IP-Adresse

  Um die bisherige Funktionalität des Gerätes nicht zu beeinträchtigen, muss dieses weiterhin über dieselbe Adresse erreichbar sein.

- Abwärtskompatibilität zu IP

  Der Datenverkehr von und zu mobilen Geräten muss auch über Stationen gehen können, die nur IPv4-Funktionalität besitzen. Das Finden des Pfades zum Empfänger muss für sie transparent sein.

- authentifizierte Registrierung

  Der derzeitige Aufenthaltsort eines Gerätes muss von einem speziellen Modul verwaltet werden. An- und Abmeldungen müssen gesichert sein.

- Skalierbarkeit

  Mit sinkenden Preisen steigt die allgemeine Verfügbarkeit von netzfähigen mobilen Geräten, deshalb muss die Erweiterbarkeit von Teilnetzen mit Mobilfunktionalität in besonderem Maße gewährleistet sein.

IP-Adressen erfüllen zwei Aufgaben: Sie dienen zum einen dazu, IP-Pakete weiterzuleiten (Forwarding). Dazu wird der Netzwerkteil der Adresse ausgewertet. Zum anderen kennzeichnen sie ein Endgerät in einem Netz. Eine TCP-Verbindung zu einem Gerät, die über Mobile IP hergestellt wurde, soll auch dann weiterbestehen, wenn das mobile System in ein anderes IP-Netz wechselt. Das ist etwa beim Übergang zwischen zwei Zugangspunkten innerhalb eines UTRANs der Fall, die im selben Gebäude liegen, jedoch unterschiedlichen IP-Subnetzen angehören. Um diese Terminal-Mobilität auf IP-Ebene sicherzustellen, musste IP um Funktionen eines Netzwerkprotokolls erweitert werden. Bereits 1996 stellte die IETF eine solche Lösung für IPv4 vor: Mobile IPv4 (siehe 5.2). [24]

Ein mobiles Endgerät, also ein Mobile Node, ist normalerweise in einem Home Network (Heimatnetz) angesiedelt und hat eine entsprechende Home Address (Heimat-IP-Adresse). Hält sich ein Mobilsystem im Heimatnetz auf, teilt es das seinem Home Agent mit. Wechselt das Mobilsystem in ein anderes Netz (Foreign Network), meldet es sich dort bei einem Foreign Agent an. Das kann beispielsweise ein lokaler Router sein. Hat sich der Mobile Node beim Foreign Agent registriert, teilt er dem Home Agent in seinem Heimatnetz seine Care-of Address mit, unter der er im fremden Netz zu erreichen ist. Die Care-of Address ist meist die IP-Adresse desjenigen Foreign Agent, der die eingehenden Pakete an den mobilen Knoten weiterreicht.

Mithilfe der Agent Discovery stellt ein Mobilgerät fest, in welchem Netz es sich gerade befindet. Es nutzt dazu die ICMP-Agent-Advertisement-Nachrichten[55], die Heimat- oder mobile Agenten versenden. Ein Agent Advertisement enthält Informationen darüber, ob ein Agent als Foreign oder Home Agent zur Verfügung steht, ob sich der mobile Knoten beim Agenten registrieren muss, welche Tunneling-Verfahren der Agent unterstützt und welche Care-of Address für diesen Foreign Agent verwendet werden soll. Allerdings kann es vorkommen, dass der Mobile Node in einem Netzwerk landet, das keinen Foreign Agent unterstützt. Dann kann der Mobile Node selbst einspringen und eine Co-located-Care-of Address verwenden, die direkt beim Mobile Node angesiedelt ist. Der Standard bei Mobile IP lässt offen, auf welche Weise ein Mobile Node seine Care-of Address erhält - ob er sie dynamisch über einen DHCP-Server oder über eine fest zugewiesene Adresse für die Zeit seines Aufenthalts im Fremdnetz zugewiesen bekommt.

Nach dem Discovery-Prozess registriert sich der Mobile Node in einem fremden Netz beim Foreign Agent. Der leitet die Registrierung an den Home Agent weiter. Die Nachricht enthält unter anderem die Heimatadresse des mobilen Knotens, die Adresse des Home Agent des Mobile Node sowie dessen Care-of Address. Zudem gibt sie das Tunneling-Verfahren an. Der mobile Knoten kann sich auch bei mehreren Foreign Agents gleichzeitig anmelden. Dann wird ein Paket an mehrere Care-of Adressen gesendet, das die Ausfallsicherheit erhöht. Ferner lassen sich mit der Registrierungsnachricht auch Erweiterungen (Extensions) angeben. Die wichtigste ist die Security Extension. Sie definiert einen Security Context zwischen zwei Knoten. Vorgeschrieben ist eine Authentifizierung zwischen dem Mobilknoten und dem Home Agent, optional hingegen eine Security Association zwischen dem Mobile Node und dem Foreign Agent sowie dem Foreign Agent und dem Home Agent. Die Authentifizierung verhindert, dass sich ein Angreifer als Mobile Node ausgibt und den Datenstrom zu sich umleitet.

Hat sich ein Mobilknoten im Fremdnetz bei seinem Heimatagenten angemeldet, kann dieser IP-Pakete an ihn weiterleiten. Ähnlich wie bei der Postnachsendung werden die Daten an die Care-of Address des mobilen Gerätes übermittelt. Zuvor nimmt der Home Agent die Pakete quasi als Treuhänder in Empfang. Ein Home Agent kann sich beispielsweise als Proxy[56]-ARP für einen Mobilknoten ausgeben und den an diesen adressierten ARP-Request beantworten. Bei einem anderen Verfahren filtert der Home Agent die Pakete für den Mobile Node. Dazu muss er jedoch die Verbindung zwischen dem Internet und dem Mobile Node

[55] ICMP: Internet Control Message Protocol
[56] Der Router übernimmt die Verantwortung für die Weiterleitung der Datenpakete an den wirklichen Empfänger.

überwachen können. Das ist etwa dann der Fall, wenn der Home Agent der Zugangsrouter zu einem Netzwerk ist.

5.5 Arbeitsweise von Mobile IPv6

Neben den beiden Kommunikationspartnern (Mobile Node und Node B) ist der Home Agent (HA) als dritter zwingend für die Funktion von Mobile IPv6 erforderlich. Bei Mobile IPv4 hätte im Gastnetz noch der Foreign Agent (FA) vorhanden sein müssen.

Wenn der Mobile Node (MA) außerhalb seines Heimatnetzes ist, geht die Kommunikation zunächst nur über den Home Agent, welcher zunächst Stellvertreterfunktionen für den Mobile Node übernimmt.

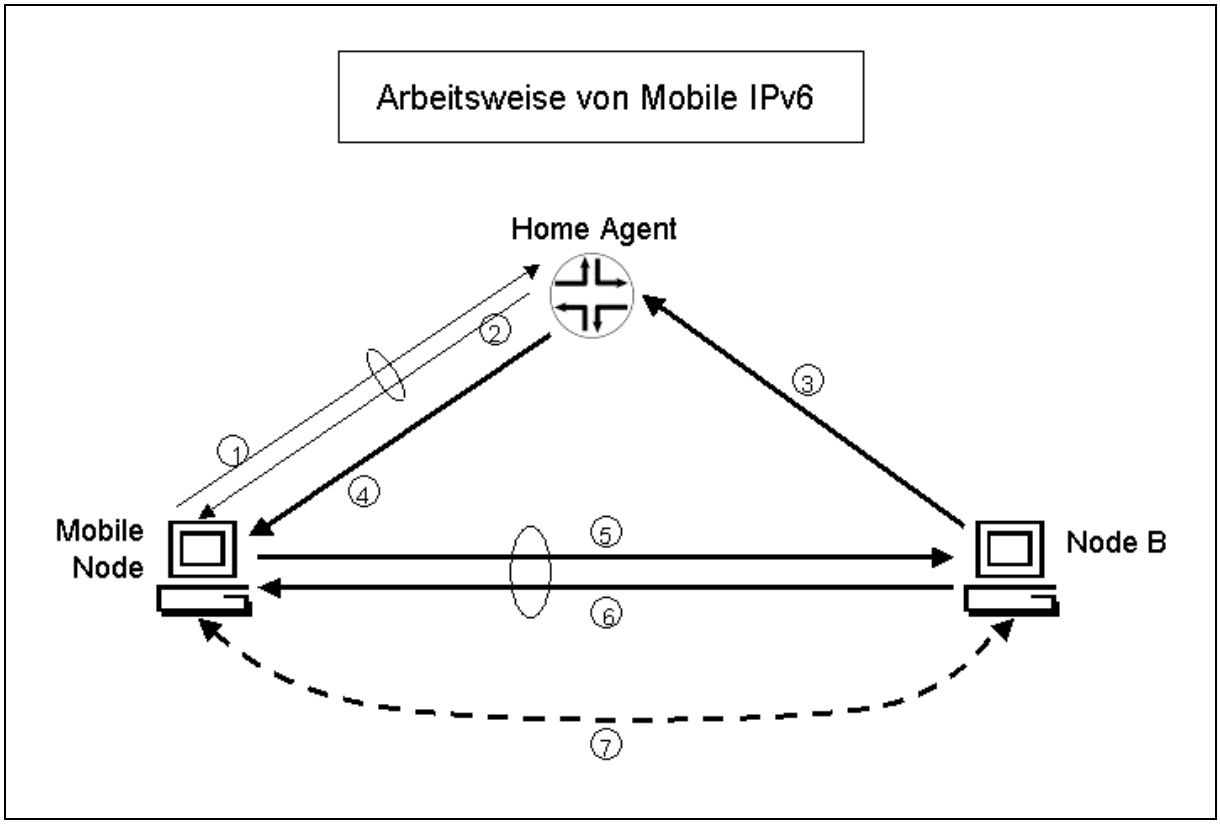


Bild 5.5 Arbeitsweise von Mobile IPv6

- (1) Der Mobile Node meldet sich aus einem fremden Netz bei seinem Home Agent und teilt ihm seine Care-of Address mit. Die zum Home Agent gesendete Nachricht wird als IP-Paket mit der Binding-Update-Option gesendet.

- (2) Der Home Agent sendet nun eine Binding-Acknowledge-Option im IP-Paket. Das Herstellen der Beziehung zwischen Home Address und Care-of Address wird als "Binding" bezeichnet.

- (3) Der Node B möchte mit dem Mobile Node IP-Pakete austauschen, er weiß zunächst nicht, wo sich der Mobile Node gerade befindet. Der Node B sendet nun das Paket an den Home Agent vom Mobile Node.

- (4) Dort nimmt jetzt der Home Agent das Paket entgegen, packt das empfangene Paket in ein neues IPv6-Paket mit der Care-of Address als Zieladresse ein und leitet es an die Care-of Address des Mobile Node weiter (-> Tunneling).

- (5) Nach Auspacken des getunnelten Pakets durch den Mobile Node sieht dieser die ursprüngliche Absenderadresse von Node B und sendet nun eine Antwort direkt an den Node B mit seiner Care-of Address als Absender.

- (6) Der Node B übernimmt diese Binding-Information und speichert so die Care-of Address des Mobile Node für nachfolgende direkte Kommunikation. Er sendet eine Antwort an den Mobile Node mit der Binding-Acknowledge-Option im IP-Paket.

- (7) Beide Kommunikationspartner können nun direkt miteinander Pakete austauschen, wobei jedoch in jedes Paket folgende Header-Optionen eingefügt werden müssen:

Mobile Node --> Node B: Home-Address-Option

Node B --> Mobile Node: Routing Header-Option

- Home-Address-Option:

  Die Home-Address-Option wird in jedem Paket benutzt, welches zum Partnerknoten gesendet wird. Im äußeren IP-Header ist die Care-of Address des Mobile Node als Absenderadresse eingetragen. Erhält ein Knoten ein Paket mit dieser Option, so ersetzt er die Absenderadresse im äußeren Header durch die Heimatadresse und liefert dann das Paket an die höhere Schicht (z. B. TCP oder UDP) weiter, allerdings ist die Home-Address-Option aus dem Paket entfernt. Für die über der IP-Schicht liegende Ebene sieht das Paket dann genauso aus, als ob es direkt vom Mobile Node aus dessen Heimatnetz gekommen wäre.

- Routing Header-Option:

  Die Routing Header-Option dient zur Festlegung einer Reihe von Routern, welche auf dem Weg eines Pakets von der Quelle zum Ziel besucht werden sollen. Nur diejenigen Router, die in einer Routingtable aufgelistet sind, müssen diese Routing Header-Option bearbeiten. [RFC 2460]

5.6 Ausblick

Gegenwärtig kommt Mobile IP meist in Verbindung mit IPv4 zum Einsatz. Diese Kombination weist jedoch etliche Einschränkungen auf. So muss in jedem Subnetz eine Home- und Foreign-Agent-Infrastruktur vorhanden sein. Hinzu kommt, dass das Routing sich strikt auf die Zieladresse der IP-Pakete stützt. Es darf also kein Source-Routing erfolgen. Ferner dürfen in den Mobile IP Netzen keine Ingress- oder Reverse-Path-Forwarding-Filter konfiguriert sein, die verhindern, dass der Mobile Node im Fremdnetz Pakete mit der Quelladresse aus dem Heimatnetz verschicken kann. Auch das Tunneling von Paketen muss gestattet sein. Diese Faktoren haben bislang verhindert, dass Mobile IP auf breiter Basis eingesetzt wird. Das soll nun mit der IP-Version 6 anders werden.

Das Ziel von Mobile IPv6 ist das gleiche: Ein mobiler Knoten soll permanent unter seiner Heimatadresse zu erreichen sein. Der Mobile Node erhält auch bei Mobile IPv6 eine IP Care-of Address im Fremdnetz. Diese kann jedoch zusätzlich mithilfe von Neighbor Discovery ermittelt werden, wodurch sich die Unterstützung von Mobile IP deutlich vereinfacht. Im Foreign Network teilt der mobile Knoten wie bei IPv4 dem Home Agent im Heimatnetz seine Care-of Address mit. Der Home Agent schickt die Pakete dann über einen Tunnel an die Care-of Address des mobilen Knotens.

Der wesentliche Unterschied zu Mobile IPv4 liegt darin, dass der Mobile Node bei IPv6 der Gegenseite über eine spezielle Address-Binding-Option im Destination Option Extension Header seine neue Adresse mitteilen kann. Die Gegenseite hat damit die Möglichkeit, alle folgenden Pakete direkt an den mobilen Knoten weiterzuleiten. Das aufwändige und ineffiziente Dreiecks-Routing über den Home Agent bei Mobile IPv4 entfällt somit.

Bei IPv6 kann das mobile Gerät auch seine Care-of Address als Absenderadresse verwenden. Dies beseitigt das Problem des Ingress Filtering bei Internet-Service-Providern. Der Home Agent und das Netzwerk insgesamt werden damit vom IP-Verkehr entlastet und der Transport zwischen Mobile Node und anderen Rechnern im Netz erfolgt wegen des direkten Datenversands schneller. Ein weiteres Plus sind die besseren Sicherheitsmechanismen von IPv6 (siehe Kapitel Security). [22]

6 IPv6 Netzwerkplanung

Bevor eine Netzwerkplanung angegangen wird, gibt es Klärungsbedarf zu folgenden Punkten:

- Größe des zu planenden Netzes
  - Anzahl der Knoten (Router)
  - Datenvolumen
  - Anzahl der Nutzer
  - Räumliche Verteilung der Nutzer
- Zweck des Netzwerkes
  - in Anspruch genommene Dienste (Web, Mail, Datenbanken...)
  - zum Einsatz kommende Protokolle
    - IP- Adressplanung
  - verwendete Systeme / Betriebssysteme
- Ausgangsvoraussetzungen
  - aktive oder passive Infrastruktur
    - vorhanden – kaufen oder mieten - bei wem
- Einzufügende Redundanzen
  - Zweck
  - an welcher Stelle
  - wie realisiert (1:N / 1:1)
- Rechtestrukturen (Firewall, AAA[57])
  - wer darf was
  - wohin

[57] Authentication, Authorisation, Accounting

- Management
  - nötiges Know-how
  - Automation
  - Protokolle / Mechanismen
- Kosten
  - Investitionen
  - Art der Anbindung
  - eigene Durchführung oder Outsourcing
  - Schulungskosten

Wir gehen in unserer Beispielplanung nicht explizit auf jeden dieser Punkte ein. Unser Hauptaugenmerk liegt bei der Einführung von IPv6, dem gemeinsamen Betrieb beider Internet Protokollversionen während der Übergangsphase sowie neuer Anwendungsmöglichkeiten durch Mobilityfunktionen.

6.1 Prinzipielles Netzdesign

Der prinzipielle Aufbau eines **WANs** (Wide Area Network) lässt sich mit einem Zwiebelmodell verdeutlichen. In den einzelnen Schichten werden, entsprechend unterschiedlicher Anforderungen, verschiedene Techniken eingesetzt.

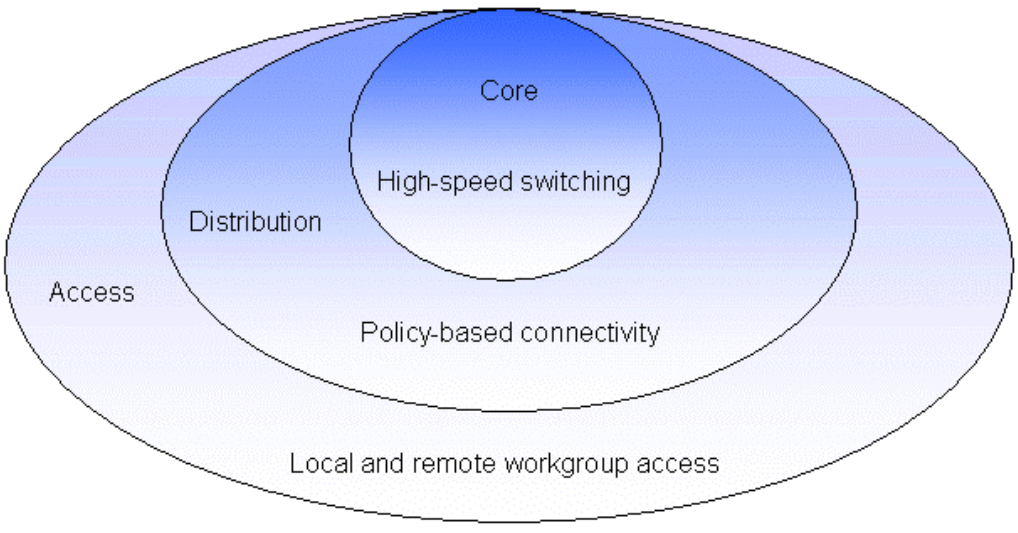


Bild 6.1 Prinzipielles Netzwerkdesign

- Funktion des Core Layer (Kernschicht)

Ein Core Layer ist ein High-Speed Switching Backbone und sollte so designed sein, dass Pakete so schnell als möglich übertragen werden können. In diesem Zusammenhang wird oft von "over-engineered" gesprochen, d. h. das Netz besitzt mehr Kapazität als benötigt. Diese Schicht des Netzwerks sollte keine Paketmanipulation (z. B. Access-Listen, Filter) unterstützen, sonst würde das die Paketweiterleitung verlangsamen.

- Funktion des Distribution Layer (Verteilungsschicht)

Der Distribution Layer des Netzwerks ist die Schicht zwischen dem Access- und Core Layer. Sie grenzt diese beiden Schichten voneinander ab und dient zur Vorkonzentration von Datenverkehr, Wegewahl, Filterung und Klassifizierung.

In der lokal begrenzten Umgebung kann der Distribution Layer folgende Funktionen beinhalten:

- Vorkonzentration des Access Layers
- Broadcast / Multicast Domain Definition
- VLAN Routing beim Routing zwischen Subnetzen
- Medien Übergänge (z. B. Ethernet – ATM)
- Klassifikation, Kennzeichnung und Warteschlangenzuordnung (Queuing) für Class of Service (CoS) / Quality of Service (QoS) (z. B. DiffServ)

In der regionalen Umgebung kann der Distribution Layer ein Netzknoten zwischen Routing Domains oder eine Abgrenzungsschicht zwischen statischen und dynamischen Routing Protokollen sein. Außerdem kann diese Schicht der Zugangspunkt für Fernzugriff (Remote Access) im Netzwerk sein. Der Distribution Layer kann zusammenfassend als die Schicht bezeichnet werden, die auf bestimmten Regeln basierende Verbindungen zur Verfügung stellt.

- Funktion des Access Layer (Zugangsschicht)

Der Access Layer ist der Zugangspunkt in das Netzwerk für lokale Endnutzer. Hier sind Geräte angesiedelt, die die Einwahlverbindungen ermöglichen, z. B. Remote Access Server und Router.

In einer regionalen Umgebung werden an dieser Stelle Zugangsberechtigungen für zusammengehörige Netzwerke über Wide Area Netzwerke (z. B. Frame Relay, ISDN oder Standleitungen) vergeben.

Die einzelnen Schichten sind als Hilfe dazu definiert, um ein Netzwerk technisch einwandfrei zu designen und die Funktionsfähigkeit des Netzwerks zu gewährleisten. Die technische Ausführung eines jeden Layers kann in ausgewählten Routern oder Switches, in physikalischen Medien oder in einem Endgerät kombiniert, realisiert werden. Inwieweit die einzelnen Schichten im Netzwerk Verwendung finden, liegt an der Struktur des Netzdesigns. Um das Netzwerk optimal ausnutzen zu können, sollte man sich an die Hierarchiestruktur halten.

Ein **LAN** (Local Area Network) hingegen wird heutzutage meist nach folgendem Grundkonzept entworfen:

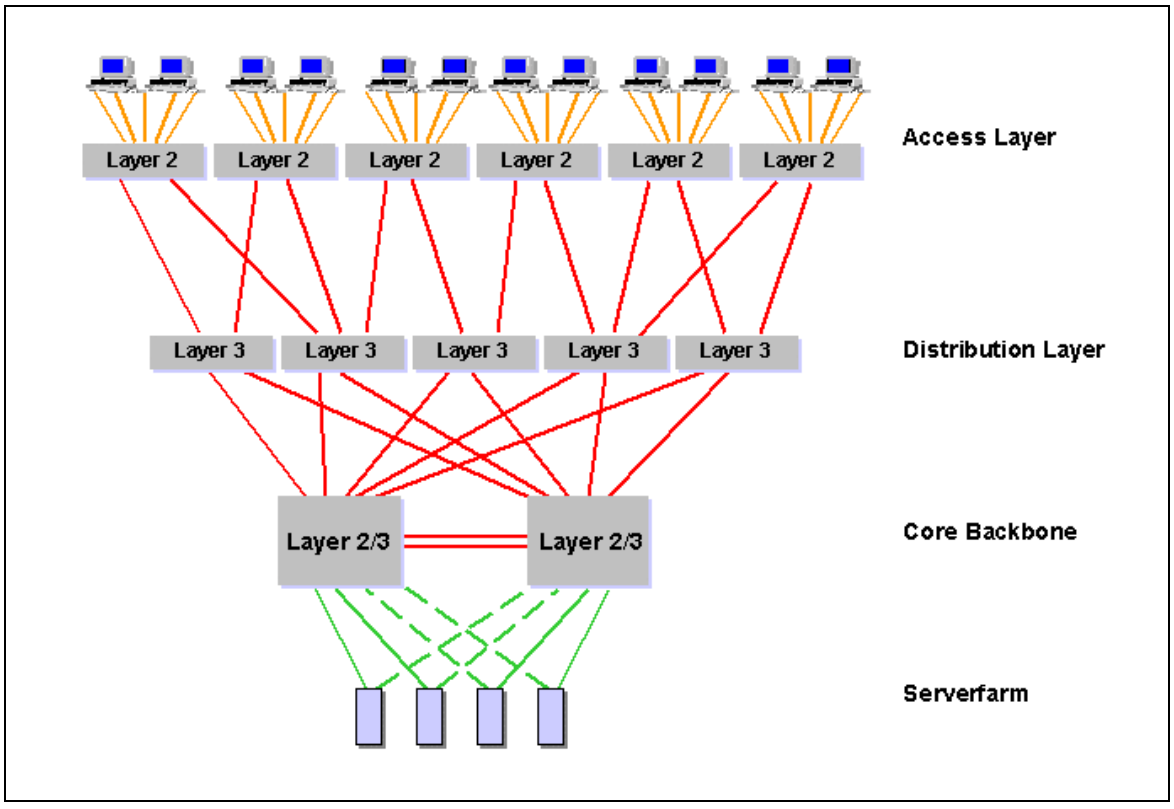


Bild 6.2 Grundkonzept eines LAN Netzes mit Multilayer Switching

Dieser Entwurf wird üblicherweise für Netzwerke verwendet, die ca. 100 bis etliche 10.000 Endgeräte integrieren. Wird das Netzwerk ein paar tausend Endgeräte nicht übersteigen, so entfällt der Distribution Layer.

- **Core Backbone**

Das Core Backbone besteht aus mindestens zwei Switches, die Layer 2 und Layer 3 Funktionalitäten aufweisen, und dient hauptsächlich zur Vermittlung der Daten. Sie sind redundant miteinander verbunden, um Ausfallsicherheit zu gewährleisten und reibungslose Wartung zu ermöglichen. Innerhalb des Backbones ist es üblich, Gigabit Ethernet (GE) Verbindungen einzusetzen. Die Switches sind mit mehreren GE Verbindungen zusammengeschaltet, um *Loadsharing*[58] betreiben zu können. Diese Verbindungen werden zu einem sogenannten Trunk[59] zusammengefasst. Logisch gesehen stellt der Trunk eine einzige Verbindung dar. Das bedeutet, wenn eine GE Verbindung des Trunks ausfällt, wird der Datenverkehr durch die restlichen Verbindungen des Trunks nahtlos weiter betrieben, ohne dass dies nach außen sichtbar wird.

Direkt an das Core Backbone werden die Server und die Geräte der Distribution Layer (falls vorhanden) angeschlossen.

- **Distribution Layer**

Der Distribution Layer wird bei größeren Netzwerken eingesetzt (mehrere 1.000 bis einige 10.000 Endgeräte), zur Vorkonzentration des Datenverkehrs und eventuell Bereitstellung erster Dienste. Häufig werden Switches mit Layer 3 Funktionalität verwendet, die ebenfalls mit Gigabit Ethernet angebunden sind. Die Switches werden so angeschlossen, dass auch hier die Ausfallsicherheit der redundanten Core Komponenten an den Access Layer weitergegeben wird.

- **Access Layer**

Der Access Layer bildet die Anschlussebene für die Endgeräte. Diese werden meist über Fast Ethernet[60] (FE) an Layer 2 Switches angebunden. Wie der Access Layer dann tatsächlich realisiert wird, variiert stark aufgrund der räumlichen und technischen Gegebenheiten des zu planenden Netzwerkes.

- **Serverfarm**

Verschiedene Dienste, wie z. B. Web, Email u. v. m., werden nicht durch einen einzigen Server zur Verfügung gestellt, sondern durch eine sogenannte Serverfarm. Die Server sind üblicherweise dienstmäßig strukturiert, das bedeutet, dass je nach Bedarf verschiedene Dienste auf verschiedenen Servern implementiert sind. [35]

---

[58] Lastausgleichsverfahren
[59] "Stamm" – logische Zusammenfassung mehrerer physikalischer Verbindungen
[60] 100Mbit/s

6.2 LAN Netzwerkentwurf

Wir gehen davon aus, das ein Softwareunternehmen, welches Anwendungen für UMTS Netze entwickelt, sein Netzwerk IPv6-fähig machen möchte. Folgende **Ausgangssituation** liegt unserer Planung zugrunde:

- 1.000 Angestellte = Rechnerplätze
- 15 Stockwerke je mit einem Stockwerksverteiler
- ein redundant ausgelegtes Rechenzentrum
- einen Internetzugang
- 64 IPv4-Adressen mit einer Netzwerkpräfix von /26, Provider assigned[61] (PA)
- eine DMZ (Demilitarized Zone)
- reines IPv4 Netzwerk mit privaten Adressen [41]
- NAPT für IPv4

Nun zum **Design** des aufgerüsteten Netzwerkes:

- Access Layer - Stockwerksverteiler

  Bei 1.000 Angestellten, auf 15 Etagen verteilt, kommen durchschnittlich 67 Arbeitsplätze auf jedes Stockwerk. Es werden daher 2 Switches mit je 48 freien Ports als Stockwerksverteiler eingesetzt. Aus Kostengründen sind dies Layer 2 Switches.

- VLANs / Subnetze (logische Sicht)

  Geswitchte LANs werden üblicherweise pro 250 bis 500 Endgeräte in *Virtual Local Area Networks* (VLAN) unterteilt. Unser Firmennetz bekommt ein Server VLAN und sämtliche Endgeräte werden auf 2 weitere VLANs logisch verteilt. Der Administrationsaufwand wächst mit der Anzahl der VLANs. Jedem VLAN wird ein IPv6 Subnetz zugeordnet, um die IPv6 Funktionalität mittels Dual-Stack zu nutzen. Damit ergibt sich folgendes Konstrukt:

[61] vom Provider zugewiesene Adressen, sogenannte PA Adressen

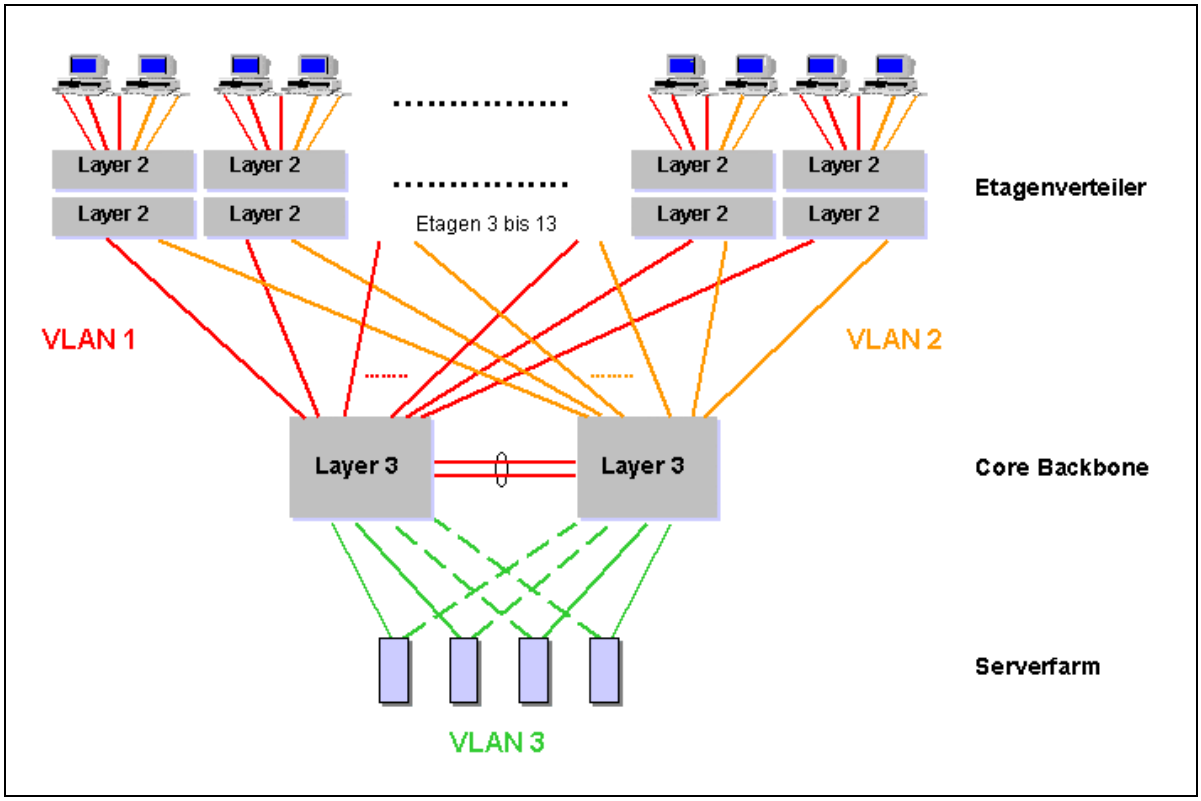


Bild 6.3 VLAN- Struktur des Netzbeispiels

- Routing – Layer 3 Switching

  Im Core-Bereich sind zwei redundant angebundene Layer 3 Switches angesiedelt. Layer 3 Switching unterscheidet sich vom Layer 2 Switching durch die Weiterleitung der Daten. Bei Letzterem entscheidet die MAC Adresse, wohin das Datagramm geleitet wird, bei Ersterem ist es die Zieladresse auf Netzwerkschichtebene (nach dem OSI Modell Layer 3, IP-Adresse). Eine Lasttrennung wird bereits durch die VLANs der Layer 2 Switches erreicht.

  An die Switches im Core Backbone sind die Stockwerksverteiler angeschlossen, sowie die Server der Serverfarm. Der Router, der das Netzwerk mit dem Internet verbindet, ist ebenfalls im Rechenzentrum über eine Firewall an einen Layer 3 Switch angeschlossen. Hier geschieht die Trennung zwischen privaten und öffentlichen IP-Adressen. Es wird eine DMZ eingerichtet, eine sogenannte neutrale Zone zwischen dem internen Netz des Unternehmens und dem öffentlichen Netz. Hierdurch wird verhindert, dass Benutzer von außen direkt auf einen Server mit Unternehmensdaten zugreifen können.

- IP-Adressvergabe

  Es sind 64 IPv4-Adressen im CIDR-Format, mit einer Netzwerkpräfix von /26, vorhanden. Diese wurden dem Unternehmen vom ISP aus dessen Adresspool zugewiesen.

  Server und Switches erhalten fest zugewiesene IPv4-Adressen, wobei die Server in der DMZ öffentlich gültige erhalten, während die restlichen nur lokale Gültigkeit besitzen, da sie von außen nicht direkt erreichbar sein sollen. In unserem Beispiel werden für die DMZ 16 global gültige IPv4-Adressen reserviert. Die übrigen stehen dann für Erweiterungen während der Übergangsphase zur Verfügung.

  Zur Verdeutlichung hier noch einmal die Struktur unseres Netzwerkes, vervollständigt um die DMZ und Internetanbindung.

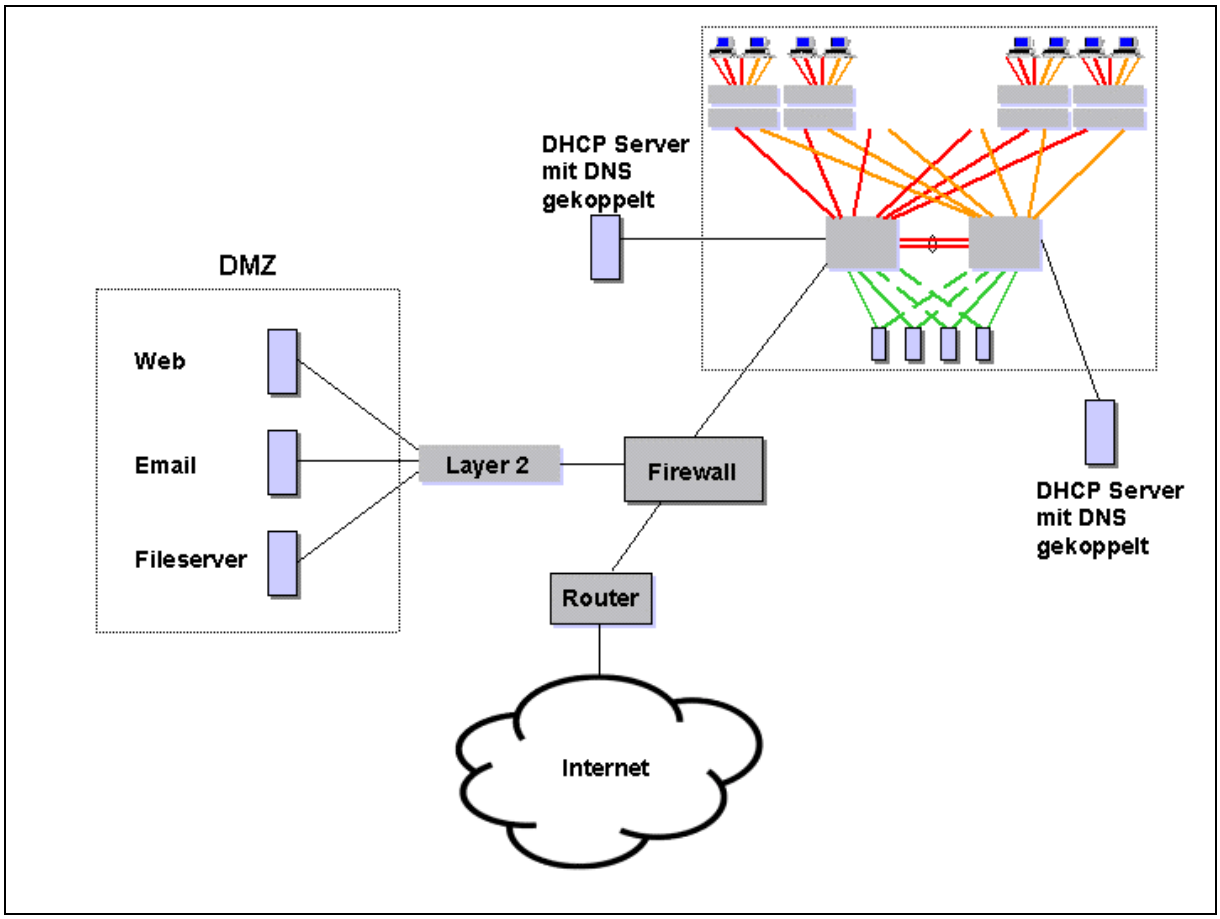


Bild 6.4 Netzwerkbeispiel mit Internetzugang und DMZ

Des weiteren muss das Softwareunternehmen bei seinem ISP IPv6-Adressen beantragen. Bei der Erstvergabe von IPv6-Adressräumen gelten zunächst auf

technischen Erwägungen basierende[62] Regeln. Zusätzliche Adressräume werden später aufgrund der Nutzung der zuerst vergebenen Adressen zugewiesen. [42] Regionale, von der IANA anerkannte Internet Registraturen[63], vergeben Top-Level Aggregation Identifier (TLA, siehe auch Kapitel IPv6) an Organisationen, welche ihrerseits den ISPs oder auch Endnutzern Adressräume zuweisen. Die Organisationen geben zusammen mit den TLAs Next Level Aggregation Identifier (NLA) an die anfragenden Unternehmen weiter. Eine Tabelle, mit den bisher aus dem aggregatable global unicast address Bereich allokierten TLAs befindet sich im Anhang.

Hat der ISP des Unternehmens noch keinen IPv6-Adressraum zugewiesen bekommen, so muss ein anderer ISP gewählt werden. (Siehe eben erwähnte Tabelle im Anhang).

Da die Dual-Stack Strategie in diesem Beispiel umgesetzt wird, werden den Servern und Switches global gültige IPv6-Adressen zugewiesen. Die DHCP Server mit DNS sind ebenfalls mittels Upgrades IPv6-fähig. Dadurch kann die IPv6-Subnetzstruktur mittels statusbehafteter Konfiguration (DHCPv6) durch standortlokale Adressen (Format Prefix FEC0, siehe Kapitel IPv6) aufgesetzt werden.

- Dual-Stack

  Um die Dual-Stack Strategie durchgängig im Unternehmen einsetzen zu können, müssen als erstes die DNS und DHCP Server durch Upgrades Dual-Stacks erhalten. Dann ist es sinnvoll, die anderen Server, Switches, Router, als auch Clients mit Dual-Stacks auszustatten. Die zum Testen der entwickelten Software vorgesehenen Arbeitsplätze werden als reine IPv6-Rechner aufgesetzt und haben nur einen IPv6-Stack. Es steht ein Server zur Verfügung, der nur für IPv6-Testzwecke ohne Dual-Stack aufgesetzt wird.

- Netzübergänge

  Soll über das Internet eine direkte Verbindung von unserem Beispielunternehmen zu seinem Kunden, einem UMTS-Netzbetreiber, hergestellt werden, um die entwickelte Software live zu testen, müssen Tunnelmechanismen eingesetzt werden, da die Daten momentan durch ein reines IPv4-Netz transportiert werden müssen. Dabei

[62] "Bootstrap Phase" beschrieben in Ripe-196 [42]
[63] z. B. ARIN, RIPE NCC, APNIC

bedeutet "reines" IPv4-Netz, dass innerhalb dieses Netzes nur mit IPv4-Netzprotokollen gearbeitet und nur für IPv4 eine Routing-Infrastruktur aufgebaut wird.

Das schlecht skalierende NAT-PT wird aufgrund der Kombination von Dual-Stack und Tunnelmechanismen nun nicht mehr benötigt.

Wie bereits im Kapitel Interoperabilität dargestellt, gibt es eine Vielzahl verschiedener Tunnelmechanismen. Für unser Netzbeispiel kommen nur Tunnelmechanismen in Frage, die IPv6-Datenverkehr durch eine IPv4-Netzstruktur leiten, da aufgrund der Dual-Stack Auslegung der IPv4-Datenverkehr direkt ablaufen kann. Der Fall, dass IPv4-Daten durch eine IPv6-Netzstruktur getunnelt werden muss, tritt nicht auf.

Zu klären ist nur noch, ob der ISP die Tunnelarchitektur bereitstellt und damit die Kontrolle über die Tunnelendpunkte hat, oder ob das Unternehmen dies selbst übernimmt. Anbieten würden sich Tunnelverfahren, wie IPv6 over IPv4 Tunnel oder automatische 6to4 Tunnel. Für letztere sind IPv6-Adressen notwendig, die mit dem Präfix 2002 beginnen. Da momentan nur Adressen mit dieser Präfix vergeben werden, ist diese Bedingung erfüllt.

6.3 Netzwerkentwurf für einen UMTS-Lizenznehmer

Als nächstes Beispiel stellen wir einen Netzwerkentwurf eines UMTS-Lizenznehmers dar. Unter Berücksichtigung der am Anfang dieses Kapitels aufgelisteten Punkte planen wir dieses Netz, um dem UMTS-Betreiber die im Release 5 der 3GPP geforderte IPv6 Tauglichkeit bereitzustellen.

Die **Ausgangssituation** ist folgende: der UMTS-Betreiber möchte den Endverbrauchern in seinem Netz, das die Bevölkerung zu einem großen Teil abdecken soll, echte Mobilitätsfunktionen anbieten. Der UMTS-Betreiber möchte seine Kunden neben dem bisherigen IPv4-Service auch die Möglichkeit geben, IPv6-Dienste in Anspruch zu nehmen. Um diese Dienste wiederum reibungslos mit einer möglichst hohen Geschwindigkeit im Netz zu übertragen, bedarf es einem IPv6 tauglichen IP Mutimedia System im "all IP based Network". Die bereits vorhandene Infrastruktur basiert auf einem GPRS-Core, welches für die Anwendungen auf ein Dual-Stack IP-Core aufgerüstet wird. Das UTRAN ist ebenfalls grundlegender Bestandteil für den Netzaufbau.

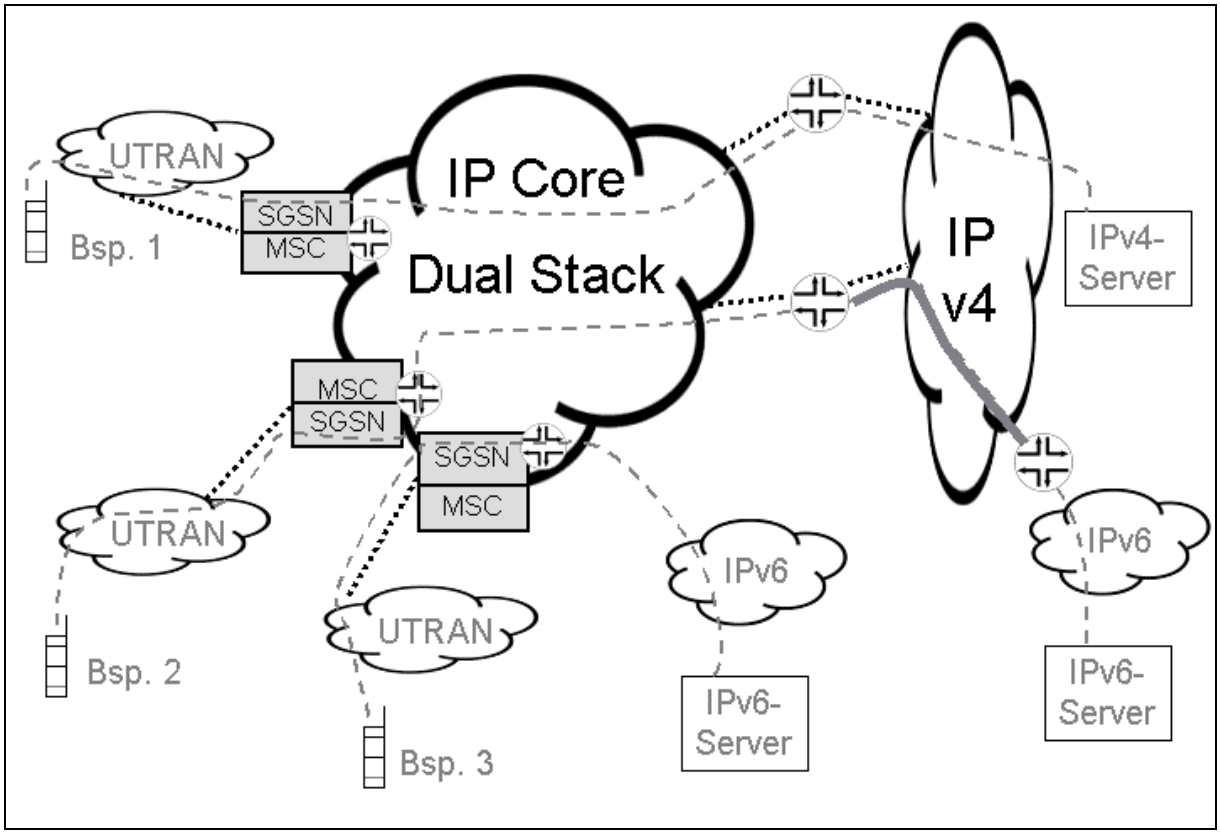


Bild 6.5 Netzstruktur eines UMTS-Betreibers (Beispiel)

Der dargestellte **Netzaufbau** eines UMTS-Betreibers wird nachfolgend beschrieben.

- Router mit Dual-Stack

  Als erstes ist auch hier wichtig, dass das zugrunde liegende Kernnetz mit Dual-Stack für IPv4 und IPv6 ausgestattet wird, um die Migration zu IPv6 überhaupt zu ermöglichen. Dual Stack findet bei den Routern und Servern im IP-Core Verwendung, so benötigen wir kein Dual Stack beim Client. Mit Beispiel 3 im o. a. Bild wird ein Anwendungsfall für reine Dual-Stack Strategie dargestellt. Es muss auf keinen anderen Mechanismus der Migrationsphase zurückgegriffen werden, da ein Mobile IPv6 Gerät auf einen IPv6-Server zugreift. Hier wird ausschließlich der IPv6-Stack des Dual-Stacks genutzt.

- NAT-PT

  Am Übergang vom Access Netz (UTRAN) zum IP Dual-Stack Core wird NAT-PT auf den Routern eingesetzt. Die Identifikation einer Kommunikationsbeziehung bei Einrichten der Kommunikation wird im NAT-PT Gateway gespeichert und später für die Protokollübersetzung immer benötigt. Zur Identifikation einer

Kommunikationsbeziehung gehören mindestens die beiden IP-Adressen der Kommunikationspartner. Ein- und ausgehender Datenverkehr muss immer über dasselbe NAT-PT Gateway laufen, da der Kontext nur dort gespeichert ist.

Durch das Einbringen von NAT-PT Routern an der Grenze vom UTRAN zum Core Netzwerk[64], lässt sich die NAT-PT wesentlich höher skalieren, da eine begrenzte Anzahl von mobilen Teilnehmern auf dieses Gateway zugreift. Würde das Gateway am Übergang zwischen IPv6 Core und dem Internet stehen, würden erheblich mehr Teilnehmer darüber geroutet. Die Nutzung ein- und desselben NAT-PT Gateways, das an der Grenze von Access zu Core sitzt, kann dort für den Hin- und Rückweg gesteuert werden, da es unabhängig vom Internet Routing, nämlich innerhalb des eigenen Autonomen Systems, also in IGP geschieht.

Das Beispiel 1 im o. a. Bild zeigt ein Szenario, bei dem ein IPv6-Client auf einen IPv4-Server zugreift und somit NAT-PT nutzen muss..

- Tunneling

  Tunneling wird verwendet, um Daten an ein reines IPv6-Netz, das nicht direkt erreichbar ist, zu versenden. Siehe hierzu Beispiel 2 in o. a. Bild. Das Paket muss über ein IPv4-Netz eines Peering[65] Partners getunnelt werden. Über diesen Mechanismus werden sich die Anbieter der IPv6-Dienste über das Internet virtuell vernetzen. Vermutlich werden Service Provider ohne eigenes Netz ebenfalls eigene Server aufsetzen, die mit den UMTS-Netzen verbunden werden müssen. Weitere Anbieter, die e-commerce- bzw. m-commerce- Dienste anbieten, werden den Vorteil von unübersetzter IPv6-Kommunikation, die zum Teil für Verschlüsselungen notwendig ist, ebenfalls erkennen und daran teilhaben.

Durch die weitere Verbreitung der IPv6-basierenden Dienste, werden zunächst die globalen und überregionalen, dann auch die regionalen ISPs ihre Netze IPv6-fähig machen, um den Anforderungen ihrer Kunden nach ungetunnelten IPv6-Diensten nachzukommen.

---

[64] am SGSN. Es ist davon auszugehen dass mindestens ein SGSN pro größerer Stadt bzw. Ballungsgebiet existiert. Für Deutschland sind dies die ca. 15 größten Städte.

[65] Zusammenschaltung von ISP-Datenleitungen für den Datenaustausch untereinander

7 Zusammenfassung / Ergebnisse

Zu Beginn dieser Diplomarbeit im August 2001 war IPv6 noch kein öffentlich diskutiertes Thema. Die Väter der Internetgemeinde entwickelten im stillen Kämmerlein an dem Protokoll, das hierzulande wegen des begrenzten IPv4-Adressraumes schon wesentlich dringender benötigt wurde als in den USA, wo die marktführenden Netzwerkhersteller beheimatet sind. Häufig war die Meinung zu hören, dass IPv6 sich gar nicht durchsetzen wird.

Inzwischen hat sich die Situation grundlegend geändert. Die Standardisierung von IPv6 sowie die Standardisierung von Übergangsstrategien ist weitgehend abgeschlossen. Bei Mobile IPv6 und DHCPv6 ist die Spezifikation zwar noch im Draft-Status, aber weit fortgeschritten. RFCs für diese beiden Einsatzgebiete sind in Bälde zu erwarten. In allen einschlägigen Fachmagazinen sind Artikel zu IPv6 zu finden. Die marktführenden Hersteller wie Cisco, Juniper und Nortel haben produktiv einsetzbare IPv6-Funktionalitäten für ihre Geräte angekündigt oder sogar schon implementiert.

Es hat sich herausgestellt, dass nicht der enorme Adressraum der "driving factor" für IPv6 ist, sondern seine Mobilitätsfunktionen. Das Zusammenspiel mit UMTS wird eine große Rolle spielen. Insbesondere werden UMTS-Betreiber auf die Einführung von IPv6 drängen. Sobald UMTS-Betreiber ihre Migration vollzogen haben, werden global agierende ISPs mit IPv6-fähigen Diensten nachziehen. Regionale, kleinere ISPs folgen mit ihren Lösungen später.

Dadurch ist oberstes Gebot für IPv6-Funktionalitäten, dass stark hierarchische Strukturen zugrunde liegen, die verbesserte Routingmechanismen ermöglichen. Eine hohe Skalierbarkeit ist ein zwingendes Muss.

NAT-PT, Dual-Stack und Tunneling sind Mechanismen, die geschaffen werden mussten, um die Zeit der parallelen Existenz des alten und des neuen Protokolls zu überbrücken. Alle drei sind keine Techniken, die im normalen, reinen IPv6-Betrieb noch wünschenswert sind, da sie zusätzlichen Managementaufwand und Systembegrenzungen bedeuten. Leider sind die Netzwerkhersteller so spät auf den Zug aufgesprungen, dass die Standardisierung von Tunnelmechanismen z. B. noch nicht weit genug fortgeschritten war, als sie bereits im IPv6-Testnetz, dem 6Bone, benötigt wurden. Aus diesem Grund haben Hersteller wieder proprietäre Tunnelmethoden entwickelt, die nicht miteinander kompatibel sind. Eine Schwachstelle, die es bei der Netzwerkplanung während der Übergangsphase zu beachten gilt. Aufgrund der Skalierbarkeit, haben sich Verfahren wie Dual-Stack und Tunneling anstelle von NAT-PT durchgesetzt.

Dr. Vint Cerf, Chairman of the Internet Society and known as one of the fathers of the Internet: "IPv6 is here and now, so take the Internet where no other network has gone before!"

8 Anhang

A Abbildungsverzeichnis

B Tabellenverzeichnis

C1 IPv6 Multicastadressen

Die folgende Auflistung stammt von der IANA und enthält alle reservierten und registrierten Multicastadressen. Die aktuelle Version kann im Internet unter www.iana.org abgerufen werden. Zum Zeitpunkt der Erstellung dieser Diplomarbeit ist die folgende aktuelle Version vom Stand des 21.05.2001.

INTERNET PROTOCOL VERSION 6 MULTICAST ADDRESSES

Fixed Scope Multicast Addresses

These permanently assigned multicast addresses are valid over a specified scope value.

Node-Local Scope

FF01:0:0:0:0:0:0:1	All Nodes Address
FF01:0:0:0:0:0:0:2	All Routers Address

Link-Local Scope

FF02:0:0:0:0:0:0:1	All Nodes Address
FF02:0:0:0:0:0:0:2	All Routers Address
FF02:0:0:0:0:0:0:3	Unassigned
FF02:0:0:0:0:0:0:4	DVMRP Routers
FF02:0:0:0:0:0:0:5	OSPFIGP
FF02:0:0:0:0:0:0:6	OSPFIGP Designated Routers
FF02:0:0:0:0:0:0:7	ST Routers
FF02:0:0:0:0:0:0:8	ST Hosts
FF02:0:0:0:0:0:0:9	RIP Routers
FF02:0:0:0:0:0:0:A	EIGRP Routers
FF02:0:0:0:0:0:0:B	Mobile-Agents
FF02:0:0:0:0:0:0:D	All PIM Routers
FF02:0:0:0:0:0:0:E	RSVP-ENCAPSULATION
FF02:0:0:0:0:0:1:1	Link Name
FF02:0:0:0:0:0:1:2	All-dhcp-agents
FF02:0:0:0:0:1:FFXX:XXXX	Solicited-Node Address

Site-Local Scope

FF05:0:0:0:0:0:0:2	All Routers Address
FF05:0:0:0:0:0:1:3	All-dhcp-servers
FF05:0:0:0:0:0:1:4	All-dhcp-relays

FF0X:0:0:0:0:0:1:1000 Service Location, Version 2
-FF0X:0:0:0:0:0:1:13FF

Variable Scope Multicast Addresses

These permanently assigned multicast addresses are valid over all scope ranges. This is shown by an "X" in the scope field of the address that means any legal scope value.

Note that, as defined in [RFC2373], IPv6 multicast addresses which are only different in scope represent different groups. Nodes must join each group individually.

The IPv6 multicast addresses with variable scope are listed below.

FF0X:0:0:0:0:0:0:0	Reserved Multicast Address
FF0X:0:0:0:0:0:0:100	VMTP Managers Group
FF0X:0:0:0:0:0:0:101	Network Time Protocol (NTP)
FF0X:0:0:0:0:0:0:102	SGI-Dogfight
FF0X:0:0:0:0:0:0:103	Rwhod
FF0X:0:0:0:0:0:0:104	VNP
FF0X:0:0:0:0:0:0:105	Artificial Horizons - Aviator
FF0X:0:0:0:0:0:0:106	NSS - Name Service Server
FF0X:0:0:0:0:0:0:107	AUDIONEWS - Audio News Multicast
FF0X:0:0:0:0:0:0:108	SUN NIS+ Information Service
FF0X:0:0:0:0:0:0:109	MTP Multicast Transport Protocol
FF0X:0:0:0:0:0:0:10A	IETF-1-LOW-AUDIO
FF0X:0:0:0:0:0:0:10B	IETF-1-AUDIO
FF0X:0:0:0:0:0:0:10C	IETF-1-VIDEO
FF0X:0:0:0:0:0:0:10D	IETF-2-LOW-AUDIO
FF0X:0:0:0:0:0:0:10E	IETF-2-AUDIO
FF0X:0:0:0:0:0:0:10F	IETF-2-VIDEO
FF0X:0:0:0:0:0:0:110	MUSIC-SERVICE
FF0X:0:0:0:0:0:0:111	SEANET-TELEMETRY
FF0X:0:0:0:0:0:0:112	SEANET-IMAGE
FF0X:0:0:0:0:0:0:113	MLOADD
FF0X:0:0:0:0:0:0:114	any private experiment
FF0X:0:0:0:0:0:0:115	DVMRP on MOSPF
FF0X:0:0:0:0:0:0:116	SVRLOC
FF0X:0:0:0:0:0:0:117	XINGTV
FF0X:0:0:0:0:0:0:118	microsoft-ds
FF0X:0:0:0:0:0:0:119	nbc-pro
FF0X:0:0:0:0:0:0:11A	nbc-pfn
FF0X:0:0:0:0:0:0:11B	lmsc-calren-1
FF0X:0:0:0:0:0:0:11C	lmsc-calren-2
FF0X:0:0:0:0:0:0:11D	lmsc-calren-3
FF0X:0:0:0:0:0:0:11E	lmsc-calren-4

FF0X:0:0:0:0:0:0:11F ampr-info

FF0X:0:0:0:0:0:0:120 mtrace
FF0X:0:0:0:0:0:0:121 RSVP-encap-1
FF0X:0:0:0:0:0:0:122 RSVP-encap-2
FF0X:0:0:0:0:0:0:123 SVRLOC-DA
FF0X:0:0:0:0:0:0:124 rln-server
FF0X:0:0:0:0:0:0:125 proshare-mc
FF0X:0:0:0:0:0:0:126 dantz
FF0X:0:0:0:0:0:0:127 cisco-rp-announce
FF0X:0:0:0:0:0:0:128 cisco-rp-discovery
FF0X:0:0:0:0:0:0:129 gatekeeper
FF0X:0:0:0:0:0:0:12A iberiagames

FF0X:0:0:0:0:0:0:201 "rwho" Group (BSD) (unofficial)
FF0X:0:0:0:0:0:0:202 SUN RPC PMAPPROC_CALLIT

FF0X:0:0:0:0:0:2:0000
-FF0X:0:0:0:0:0:2:7FFD Multimedia Conference Calls
FF0X:0:0:0:0:0:2:7FFE SAPv1 Announcements
FF0X:0:0:0:0:0:2:7FFF SAPv0 Announcements (deprecated)
FF0X:0:0:0:0:0:2:8000
-FF0X:0:0:0:0:0:2:FFFF SAP Dynamic Assignments

C2 ICMP Nachrichten

Typ (dezimal)	**Meldung**	**Bedeutung**
0	Echo Reply	Echo Antwort (auf eine Echo Anfrage Anforderung)
1	Frei	--
2	Frei	--
3	Destination Unreachable	Ziel nicht erreichbar
4	Source Quench	Überlastung durch den Sender (“Packet to Big”)
5	Redirect	Umleitung, umadressieren (über andere Router)
6	Address	Alt-Hauptrechneradresse
7	Frei	--
8	Echo Request	Echo Anfrage Anforderung einer "Echo"-Antwort
9	Router Advertisement	Router Anzeige
10	Router Solicitation	Router Auswahl

11	Time Exceeded	Zeitüberschreitung bei Hop Limit oder bei der Wiederzusammensetzung von fragmentierten Paketen
12	Parameter Problem	Falsche Einstellungen
13	Timestamp Request	Umlaufzeit-Anfrage
14	Timestamp Reply	Umlaufzeit-Antwort
15	Information Request	Informations-Anfrage
16	Information Reply	Informations-Antwort
17	Address Mask Request	Address Format Request Subnet-Mask-Anfrage
18	Address Mask Reply	Address Format Request Subnet-Mask-Antwort
19	Reserviert	--
20	Reserviert	--
21	Reserviert	--
22	Reserviert	--
23	Reserviert	--
24	Reserviert	--
25	Reserviert	--
26	Reserviert	--
27	Reserviert	--
28	Reserviert	--
29	Reserviert	--
30	Traceroute	Paketverfolgung
31	Datagram Error	Datagramm-Konvertierungsfehler
32	Mobile Host Rerouting	Umleitung mobiler Host
33	IPv6 Where-are-you	Ipv6 Anfrage
34	IPv6 I-am-here	Ipv6 Antwort
35	Mobile Host Register Request	Mobile Host Registrierungsanfrage
36	Mobile Host Register Reply	Mobile Host Registrierungsantwort

C3 Bereits von den Registraturen vergebene TLAs

Global IPv6 allocations made by the Regional Internet Registries:
-APNIC
-ARIN
-RIPENCC

APNIC (whois.apnic.net)	
WIDE-JP-19990813	2001:0200::/35
NUS-SG-19990827	2001:0208::/35
CONNECT-AU-19990916	2001:0210::/35
NTT-JP-19990922	2001:0218::/35
KT-KR-19991006	2001:0220::/35
JENS-JP-19991027	2001:0228::/35
ETRI-KRNIC-KR-19991124	2001:0230::/35
HINET-TW-20000208	2001:0238::/35
IIJ-JPNIC-JP-20000308	2001:0240::/35
IMNET-JPNIC-JP-20000314	2001:0248::/35
CERNET-CN-20000426	2001:0250::/35
INFOWEB-JPNIC-JP-2000502	2001:0258::/35
BIGLOBE-JPNIC-JP-20000719	2001:0260::/35
6DION-JPNIC-JP-20000829	2001:0268::/35
DACOM-BORANET-20000908	2001:0270::/35
ODN-JPNIC-JP-20000915	2001:0278::/35
KOLNET-KRNIC-KR-20000927	2001:0280::/35
TANET-TWNIC-TW-20001006	2001:0288::/35
HANANET-KRNIC-KR-20001030	2001:0290::/35
SONYTELECOM-JPNIC-JP-20001207	2001:0298::/35
TTNET-JPNIC-JP-20001208	2001:02A0::/35
CCCN-JPNIC-JP-20001228	2001:02A8::/35
KORNET-KRNIC-KR-20010102	2001:02B0::/35
NGINET-KRNIC-KR-20010115	2001:02B8::/35
INFOSPHERE-JPNIC-JP-20010207	2001:02C0::/35
OMP-JPNIC-JP-20010208	2001:02C8::/35
ZAMA-AP-20010320	2001:02D0::/35
SKTELECOMNET-KRNIC-KR-20010406	2001:02D8::/35
HKNET-HK-20010420	2001:02E0::/35
DTI-JPNIC-JP-20010702	2001:02E8::/35
MEX-JPNIC-JP-20010801	2001:02F0::/35
SINET-JPNIC-JP-20010809	2001:02F8::/35
PANANET-JPNIC-JP-20010810	2001:0300::/35
HTCN-JPNIC-JP-20010814	2001:0308::/35
CWIDC-JPNIC-JP-20010815	2001:0310::/35
STCN-JPNIC-JP-20010817	2001:0318::/35

KREONET2-KRNIC-KR-20010823	2001:0320::/35
MANIS-MY-20010824	2001:0328::/35
UNITEL-KRNIC-KR-20010920	2001:0330::/35
U-NETSURF-JPNIC-JP-20011005	2001:0338::/35
FINE-JPNIC-JP-20011030	2001:0340::/35
QCN-JPNIC-JP-20011031	2001:0348::/35
MCNET-JPNIC-JP-20011108	2001:0350::/35
MIND-JPNIC-JP-20011115	2001:0358::/35
V6TELSTRAINTERNET-AU-20011211	2001:0360::/35
MEDIAS-JPNIC-JP-20011212	2001:0368::/35
GCTRJP-NET-20011212	2001:0370::/35
THRUNET-KRNIC-KR-20011218	2001:0378::/35
OCN-JP-20020115	2001:0380::/35
AARNET-IPV6	2001:0388::/35
HANINTERNET-KRNIC-KR-20020207	2001:0390::/35
Allocated Prefixes:	51 /35

ARIN (whois.arin.net)	
ESNET-V6	2001:0400::/35
VBNS-IPV6	2001:0408::/35
CANET3-IPV6	2001:0410::/35
VRIO-IPV6-0	2001:0418::/35
CISCO-IPV6-1	2001:0420::/35
QWEST-IPV6-1	2001:0428::/35
DISN-LES-V6	2001:0430::/35
ABOVENET-IPV6	2001:0438::/35
SPRINT-V6	2001:0440::/35
UNAM-IPV6	2001:0448::/35
GBLX-V6	2001:0450::/35
STEALTH-IPV6-1	2001:0458::/35
NET-CW-10BLK	2001:0460::/35
ABILENE-IPV6	2001:0468::/35
HURRICANE-IPV6	2001:0470::/35
EP-NET	2001:0478::/35
DREN-V6	2001:0480::/35
AVANTEL-IPV6-1	2001:0488::/35
NOKIA-1	2001:0490::/35
ITESM-IPV6	2001:0498::/35
IPV6-RNP	2001:04A0::/35

AXTEL-IPV6-1	2001:04A8::/35
AOLTIMEWARNER	2001:04B0::/35
WAYPORT-IPV6	2001:04B8::/35
Allocated Prefixes:	24 /35

RIPE (whois.ripe.net)	
EU-UUNET-19990810	2001:0600::/35
DE-SPACE-19990812	2001:0608::/35
NL-SURFNET-19990819	2001:0610::/35
UK-BT-19990903	2001:0618::/35
CH-SWITCH-19990903	2001:0620::/35
AT-ACONET-19990920	2001:0628::/35
UK-JANET-19991019	2001:0630::/35
DE-DFN-19991102	2001:0638::/35
RU-FREENET-19991115	2001:0640::/35
GR-GRNET-19991208	2001:0648::/35
DE-ECRC-19991223	2001:0650::/35
DE-TRMD-20000317	2001:0658::/35
FR-RENATER-20000321	2001:0660::/35
EU-NACNET-20000403	2001:0668::/35
EU-EUNET-20000403	2001:0670::/35
DE-JIPPII-20000426	2001:0678::/35
DE-XLINK-20000510	2001:0680::/35
FR-TELECOM-20000623	2001:0688::/35
PT-RCCN-20000623	2001:0690::/35
SE-SWIPNET-20000828	2001:0698::/35
PL-ICM-20000905	2001:06A0::/35
BE-BELNET-20001101	2001:06A8::/35
SE-SUNET-20001218	2001:06B0::/35
IT-CSELT-20001221	2001:06B8::/35
SE-TELIANET-20010102	2001:06C0::/35
DK-TELEDANMARK-20010131	2001:06C8::/35
RU-ROSNIIROS-20010219	2001:06D0::/35
PL-CYFRONET-20010221	2001:06D8::/35
NL-INTOUCH-20010307	2001:06E0::/35
FI-TELIVO-20010321	2001:06E8::/35
SE-DIGITAL-20010321	2001:06F0::/35
UK-EASYNET-20010322	2001:06F8::/35
NO-UNINETT-20010406	2001:0700::/35

FI-FUNET-20010503	2001:0708::/35
UK-INS-20010518	2001:0710::/35
CZ-TEN-34-20010521	2001:0718::/35
ES-REDIRIS-20010521	2001:0720::/35
UK-VERIO-20010717	2001:0728::/35
AT-TELEKABEL-20010717	2001:0730::/35
HU-HUNGARNET-20010717	2001:0738::/35
DE-VIAG-20010717	2001:0740::/35
DE-ROKA-20010817	2001:0748::/35
IT-EDISONTEL-20010906	2001:0750::/35
UK-NETKONECT-20010918	2001:0758::/35
IT-GARR-20011004	2001:0760::/35
DE-CYBERNET-20011008	2001:0768::/35
IE-HEANET-20011008	2001:0770::/35
LT-LITNET-20011115	2001:0778::/35
DE-NORIS-20011203	2001:0780::/35
FI-SONERA-20011231	2001:0788::/35
EU-CARRIER1-20020102	2001:0790::/35
EU-DANTE-20020131	2001:0798::/35
Allocated Prefixes:	52 /35

Total Allocated for the 3 RIRs: 127 /35

Quelle: www.ripe.net

Datum: keines angegeben

D Quellenangaben

[1] "TCP/IP und Internet"; Skript zum Unterricht V 1.0; 24.11.1998; Autor: Martin Gafner; Hochschule für Technik und Architektur Bern

[2] IETF (Internet Engineering Task Force) RFC 791 (09/1981): "Internet Protocol"

[3] IETF RFC 795 (9/1981): "Service Mappings"

[4] IANA (Internet Assigned Numbers Authority) RFC 1700 (10/1994): "Assigned Numbers"

[5] Network Working Group RFC 1519 (09/1993): "Classless Inter-Domain Routing (CIDR)"

[6] "Understanding IP Addressing: Everything you ever wanted to know" Autor: Chuck Semeria, 26.April 1996

[7] "IPv6 second edition" Autor: Christian Huitema, 1998, ISBN: 0-13-850505-5

[8] Network Working Group RFC 2460 (12/1998): "Internet Protocol, Version 6 (IPv6) Specification" *Draft Status*

[9] Network Working Group RFC 2373 (07/1998): "IP Version 6 Addressing Architecture" *Proposed Status*

[10] Network Working Group RFC 2474 (12/1998): "Definition of the Differentiated Services Field (DS Field) in the IPv4 and IPv6 Headers" *Standards Track*

[11] "MPLS Technology and Applications" Autoren: Bruce Davie and Yakov Rekhter, ISBN: 1-55860-656-4

[12] Network Working Group RFC 2453 (11/1998): "RIP Version 2" *Standards Track*

[13] "BGP4 Inter-Domain Routing in the Internet" Autor: John W. Stewart III, 1998 ISBN: 0-201-37951-1

[14] Seminar "Kommunikationssysteme" an dem Institut für Informatik der Universität Zürich, Sommersemester 2000, Thema: "IPv6", Autoren: Engel, Habicht, Király, Müller http://www.ifi.unizh.ch/ikm/Vorlesungen/KommSeminar00/KommSeminar00.data/Site%20Trash/IPv6.pdf

[15] "TCP/IP light" Autoren: Mathias Hein und Marie-Christine Billo, ISBN: 3-931959-04-X

[16] "Was ist Mbone, IP Multicast, etc. ..?" Autor: Peter Heiligers (Mitarbeiter der Geschäftsstelle Stuttgart des Deutschen Forschungsnetzes (DFN), www.dfn.de) http://www.mbone.de/allgemeines.html

[17] "Session Directory", http://www-mice.cs.ucl.ac.uk/multimedia/software/sdr/

[18] Network Working Group RFC 2236 (11/1997): "Internet Group Management Protocol, Version 2" *Standards Track*

[19] Network Working Group RFC 2526 (03/1999): "Reserved IPv6 Subnet Anycast Addresses" *Standards Track*

[20] www.6bone.de; IPv6 Testnetz

[21] Network Working Group RFC 2131 (03/1997): "DHCP" *Draft Status*

[22] NetworkWorld 21-01: "Das mobile Internet rückt näher" Autor: Dr. André Zehl

[23] www.internetnews.ch; Autokonfiguration

[24] Network Working Group RFC 2002 (10/1996): "IP Mobility Support" *Standards Tr*ack

[25] Network Working Group RFC 1631 (05/1994): "The IP Network Address Translator (NAT)" *Informational*, obsoleted by RFC 3022

[26] Network Working Group RFC 3022 (01/2001): "Traditional IP Network Address Translator (Traditional NAT)" *Informational*

[27] Network Working Group RFC 2663 (08/1999): "IP Network Address Translator (NAT) Terminology and Considerations" *Informational*

[28] Network Working Group RFC 1886 (12/1995): "DNS Extensions to support IP version 6" *Standards Track*

[29] Network Working Group RFC 1701 (10/1994): "Generic Routing Encapsulation (GRE)" *Informational*

[30] Network Working Group RFC 1702 (10/1994): "Generic Routing Encapsulation over IPv4 networks" *Informational*

[31] Network Working Group RFC 2893 (08/2000): "Transition Mechanisms for IPv6 Hosts and Routers" *Standards Track*

[32] Network Working Group RFC 2661 (08/1999): "Layer Two Tunneling Protocol "L2TP"" *Standards Track*

[33] "Layer 3 Switching Using MPLS" Whitepaper von NetPlane Systems, Inc. www.netplane.com

[34] "IPv6 Deployment Strategies" by Cisco, Version 1, 10/15/2001 www.cisco.com

[35] Manuskript "IP-Netzwerke" Autor: Kai Steuernagel, Pan Dacom Networking AG

[36] Network Working Group RFC 2765 (02/2000): "Stateless IP/ICMP Translation Algorithm (SIIT)" *Standards Track*

[37] "Cisco Delivers Industry´s Most Comprehensive IPv6 Solution" SAN JOSE, California, May 14, 2001; http://newsroom.cisco.com

[38] "Juniper führt IPv6 ein" Network World Germany 29.11.2001

[39] "IPv6 gewinnt an Fahrt" Network World Germany 23/24-01

[40] "IP Edge Aggregation", Redback Networks, www.redback.com

[41] Network Working Group RFC 1918 (02/1996): "Address Allocation for Private Internets" *Best Current Practice*

[42] RIPE NCC, Document ID ripe-196, "Provisional IPv6 Assignment and Allocation Policy Document", 20. July 1999

E Glossar

Adressen	1) In der Datenverarbeitung kennzeichnet eine physikalische Adresse den Ort, an dem sich Daten in Speichermedien befinden. 2) In Netzwerken sind Adressen festgelegte Bitfolgen zur eindeutigen Kennzeichnung von Stationen, damit sie im Netz angesprochen werden können.
Anycast	Ein Anycast ist eine Adressierungsart, bei der man genau eine Adresse aus einer ganzen Gruppe von Rechnern erreicht. Es antwortet der Rechner, der am besten (schnellsten) erreichbar ist.
ATM	ATM ist eine Technologie für vermittelte, verbindungsorientierte LANs und WANs. Sie ermöglicht einer theoretisch unbegrenzten Anzahl von Netzbenutzern dedizierte Hochgeschwindigkeitsfestverbindungen sowohl untereinander als auch mit Servern.
Bandbreite	Beschreibt den Frequenzbereich eines Datenübertragungskanals. Je größer die Bandbreite ist, desto mehr Informationen können pro Zeiteinheit übertragen werden. Die Bandbreite gibt aber nur die theoretische Obergrenze vor.
Broadcast	Rundruf, Nachricht, die an alle am Netz angeschlossenen Stationen (Empfänger) übertragen wird.
CIDR	Methode, um bei IPv4-Netzen auf IP-Netzklassen verzichten und damit die IP-Adressen effektiver ausnutzen zu können. CIDR erlaubt durch "Supernetting" mehrere Netzwerke logisch zusammenzufassen.
CSMA/CD	Zugriffsverfahren in LANs, bei dem die teilnehmenden Stationen physikalisch den Verkehr auf der Leitung abhören.

Datenpaket	Eine durch das Netz vorgeschriebene Anzahl von Zeichen, die als Einheit über das Netz weitergeleitet wird. Datenpakete enthalten Informationen und Steuerzeichen.
Destination Address	Zieladresse
Dijkstra Algorithmus	Von Dijkstra entwickelter mathematischer Algorithmus, der die Grundlage für den Link State Algorithmus bildet.
Distance Vector Algorithmus	Auch Bellman-Ford-Algorithmus genannt. Algorithmus, der von Routern in Routing-Protokollen beim dynamischen Routing eingesetzt wird.
Ebene 3	Schicht 3 des ISO/OSI-Modells der offenen Kommunikation beschäftigt sich mit der Steuerung des Subnetz-Betriebes. Seine wichtigste Aufgabe ist die Bestimmung von Paketleitwegen vom Ursprungs- zum Bestimmungsort (Routing).
Ethernet	Sammelbezeichnung für eine ganze Reihe von Basisbandnetzen unterschiedlicher Topologie, die alle mit dem CSMA/CD-Zugriffsverfahren arbeiten.
EUI-64	Adressformat, von der IEEE definiert. Bestehend aus einem 24 Bitfeld, dessen Wert für eine Firma registriert ist, und 40 Bit, die die Firma willkürlich vergeben kann.
Extension Header	Erweiterungs-Header in IPv6. Übernimmt Funktionalitäten des Option Headers von IPv4 und stellt neue Nutzungsmöglichkeiten zur Verfügung. Falls vorhanden wird er an den eigentlichen IPv6 Header angehängt. Das wird dort im Next Header Feld vermerkt.
FDD	FDD ist ein Verfahren zur Realisierung von Duplex - Verbindungen über Funkkanäle. Bei diesem Verfahren, das beispielsweise bei GSM und UMTS eingesetzt wird, werden das Uplink und das Downlink auf zwei verschiedenen Frequenzen realisiert.

FDDI	Genormtes Token-Passing-Glasfaser-Netz mit Doppel-Ring-Topologie.
Flow label	Ein Flow Label ist ein Feld im Header von IPv6-Datenpaketen. Es dient der Vereinfachung und Beschleunigung des Routings.
Fragment	Teil eines Datenpaketes
Fragmentierung	Prozess des Zerlegens eines Datenpaketes in kleinere Einheiten (Fragmente) zur Weiterleitung über eine Netzwerk, das die originale Größe nicht unterstützt. Das Paket muss dann im Zielsystem wieder zusammengefügt werden (Reassembly). Fragmentation ist eine Aufgabe der Vermittlungsschicht.
Frame	Datenpaket der Sicherungsschicht , das die Header - und Trailer -Informationen enthält, die die Bitübertragungsschicht für die Übertragung benötigt. Frames sind also verkapselte Datenpakete der Vermittlungsschicht.
Frame Relay	Technik und Übertragungsprotokoll zur paketvermittelten Datenkommunikation im WAN-Bereich. Es soll höhere Übertragungsleistungen als X.25 ermöglichen.
Gateway	Hard- und/oder Softwarelösung, die eine Verbindung von inkompatiblen Netzwerken schafft.
Header	Ein den Nutzdaten vorangestellter Bereich eines Datentelegramms, das wichtige Informationen zur Steuerung der Datenübertragung enthält. Unterschiedliche Protokolle besitzen unterschiedliche Header, aber Ziel- und Absenderadresse sind fast immer Bestandteil der Haderinformationen.
Hop	Anzahl der Router die durchlaufen werden.
Host	Ein zentraler Großrechner, auf den von anderen Systemen aus zugegriffen werden kann. Die vom Host bereitgestellten Dienstleistungen können über Lokal- und Fernabfrage

	abgerufen werden. Die Verbindung zum Host wird über Terminals aufgebaut. Daten können an den Host gesendet und von ihm empfangen werden.
Hub	Sternkoppler, an dem sternförmig LAN-Stationen angeschlossen werden.
ICMP	Das ICMP-Protokoll ist ein Protokoll zur Übertragung von Statusinformationen und Fehlermeldungen der Protokolle IP, TCP und UDP zwischen IP-Netzknoten. Besonders Gateways und Hosts benutzen ICMP, um Berichte über Probleme mit Datagrammen zur Originalquelle zurückzuschicken.
Interoperabilität	Beschreibt die Fähigkeit verschiedener Systeme (Hardware und / oder Software) miteinander zu arbeiten. Herstellerunabhängig.
ISDN	ISDN ist ein digitales, leitungsvermitteltes Netz, das Übertragung von Sprache und Daten gleichermaßen ermöglicht.
ISO	Internationaler Zusammenschluss der nationalen Normungsausschüsse der Datenkommunikationstechnik.
ISO/OSI-Modell	Referenzmodell der ISO für Netzwerke mit dem Ziel der Herstellung einer offenen Kommunikation. Es definiert die Schnittstellenstandards zwischen Computerherstellern in den entsprechenden Soft- und Hardwareanforderungen.
LAN	Ein räumlich eng begrenztes Netzwerk. Räumlich eng bedeutet in der Praxis meist ein Gebäude oder ein Teil eines Gebäudes (Etage), der sich unter Kontrolle eines Besitzers befindet. Aufgrund ihrer geringen Ausdehnung sind LANs optimal für die Bereitstellung hoher Bandbreiten geeignet.
Link State Algorithmus	Algorithmus, der beim dynamischen Routing angewendet wird.

MIME	Standard für mehrteilige, Multi-Media-EMail-Messages und WWW-Hypertext-Dokumente im Internet. Unterstützt die verschiedensten Nicht-Text-Formate wie Grafik, Audio und Fax.
MTU	Größtmögliche Dateneinheit bzw. Frame -Länge, die über ein vorhandenes physikalisches Übertragungsmedium bzw. über einen LAN - oder WAN -Pfad gesendet werden kann.
Multicast	Bezeichnung für einen Gruppenruf (Gruppenadressierung). Adressierungsmöglichkeit, bei der eine Nachricht an einen logischen Verband von Teilnehmern verschickt wird.
Multihoming	Ein Host oder ganzes Netzwerk bezieht Dienstleistungen von mehreren Internet Service Providern.
NAT	Verfahren, das als Alternative zu IPv6 die Knappheit an IP-Adressen im Internet überwinden helfen soll. Damit soll es möglich werden, innerhalb eines Firmennetzes Adressen zu verwenden, die nur in Richtung Internet eindeutig gemacht werden. Innerhalb von unterschiedlichen Firmennetzen können aber durchaus Adressen doppelt verwendet werden.
Neighbor Discovery	Das Neighbor-Discovery-Protocol dient dem IPv6-Protokoll für die schnelle Ermittlung der IPv6-Link -Layer -Adressen . Darüber hinaus wird dieses Protokoll von Routern und Rechnern genutzt, um am Netz angeschlossene Router zu ermitteln und den aktuellen Netzzustand sowie Änderungen im Netz automatisch zu erkennen.
Netzklassen	Art der Unterteilung einer IP-Adresse in einen Netz- und einen Host-Anteil. Die Netzklasse ist abhängig von der Anzahl der in einer Firma an das Internet anzuschließenden Computer.
Netzwerk	auch Netz, Network oder Net. Ein Telekommunikationsnetz umfasst die Gesamtheit der netz-, vermittlungs- und übertragungstechnischen

	Einrichtungen sowie die Verbindungsmöglichkeiten zwischen diesen Systemelementen.
Path-MTU	maximale Paketlänge auf einem Pfad
Peering	Zusammenschaltung von ISP-Datenleitungen für den Datenaustausch untereinander.
Protokoll	Definierte Vereinbarung über die Art und Weise des Informationsaustauschs zwischen zwei Systemen. Damit sind alle Regeln, Formate, Parameter und Eigenschaften gemeint, die zu einer vollständigen, fehlerfreien und effektiven Datenübertragung beitragen.
Quality-of-Service	Die ITU und das ATM-Forum haben die Dienstgüte (QoS) klassifiziert und damit die Dienste in bestimmte QoS-Klassen eingeteilt. Die Klassifizierung der ITU unterscheidet zwischen drei Klassen, die des ATM -Forums zwischen vier.
Reassembly	Wiederzusammensetzen von Datenpaketen, die entweder im Quell- oder einem Durchgangssystem fragmentiert wurden.
Request	Diensteanfrage
Reply	Diensteantwort
Round Robin	Ein Verfahren für Switches , bei dem die ankommenden Verbindungswünsche der Reihe nach an die einzelnen Server weitergeleitet werden.
Route	Optimaler Weg vom Sender zum Empfänger.
Router	Geräte, das unterschiedliche Netze auf der Ebene 3 des ISO/OSI-Modells verbindet. Router sind nicht protokolltransparent, sondern müssen in der Lage sein, alle verwendeten Informationsblöcke zu erkennen. Die logischen Adressen in einem Netzwerk werden vom Router ausgewertet. Damit werden Routing-Tabellen angelegt, um den optimalen Weg vom Sender zum Empfänger zu finden. Um die Routing-Tabellen auf dem Laufenden zu halten,

	tauschen die Router untereinander Informationen mit Hilfe von Routing-Protokollen aus (z.B. OSPF, RIP, etc.).
Routing	Prozess der optimalen Wegwahl von Datenpaketen vom Sender zum Empfänger über einzelne Netzwerke. Beim statischen Routing werden die Routen in den Routern fest eingestellt. Zwischen zwei Endstationen nehmen Datenpakete daher immer den selben Weg. Damit kann nicht automatisch auf Überlastungen oder Ausfälle von Routen reagiert werden. Die Router benötigen keine Routing-Protokolle. Beim dynamischen Routing bilden die Router Metriken, die durch Routing-Algorithmen errechnet werden. Außerdem benutzen sie Routing-Protokolle, um die so gewonnenen Weg- und Wichtungsinformationen auszutauschen und in Routing-Tabellen abzulegen. Auf diese Weise wird erreicht, dass sich die Wegwahl automatisch an die aktuelle Situation im Netz anpasst. Ausgefallene oder neu hinzugekommene Verbindungen werden dynamisch berücksichtigt.
Routine-Algorithmus	Algorithmus mit dem bei dynamischen Routine-verfahren die Wegwahl getroffen wird. Ein solcher Algorithmus verrechnet für jeden möglichen Weg die Entscheidungskriterien (Metriken) mit Wichtungsfaktoren. Der so errechnete Wert ist ein Maß für die Optimalität der Route. Über die beste Route wird das Paket weitergeleitet.
Routing-Protokolle	Protokoll, das Router beim dynamischen Routing einsetzen, um untereinander Informationen über angeschlossene Netzwerke auszutauschen und in Routing-Tabellen abzulegen.
Routing-Tabelle	Werden in einem Netzwerk mehrere Router mit dynamischem Routing eingesetzt, so kommunizieren die Router untereinander über Routing-Protokolle und bauen Routing-Tabellen auf. Über die Routing-Tabelle weiß ein Router, über welchen anderen Router er ein Datenpaket am günstigsten zu einem Zielsystem routen kann.

Server	Rechner im Netzwerk, der spezielle Aufgaben abwickelt. Z.B.: Bereitstellung von Daten und Programmen, Verwaltung aller im Netz verfügbaren Drucker, Bereitstellung und Überwachung von Kommunikations-Verbindungen, Ausführung von netzübergreifend genutzten Anwendungsprogrammen.
Session	Logische Verbindung zwischen zwei adressierbaren Einheiten im Netz, um Daten auszutauschen
Site	wörtlich: Stelle, Stätte. Internet: bestimmtes Informationsangebot, das unter einer gemeinsamen IP Adresse zu erreichen ist.
SMIL	Spezifikation einer Skriptsprache für fernsehähnliche Anwendungen im Internet bzw. World Wide Web. SMIL ermöglicht eine einfache, textgesteuerte Synchronisation von Multimedia-Anwendungen wie etwa gleichzeitiges Abspielen von Audio- und Videodateien verschiedener Quellen. Hauptvorteil ist jedoch die Reduzierung der Bandbreite von Videodaten auf den Umfang bisheriger "low-bandwidth media" wie Text und Grafik.
Standleitung	Feste Verbindung zwischen zwei Teilnehmern, die somit weder Verbindungsauf- und -abbau noch eine Rufnummer benötigt.
Subnetting	Unterteilung eines Netzwerkes in logische Unternetzwerke.
Subnetz	Unternetzwerk. Sinn ist meist die bessere Verwaltbarkeit oder das Abgrenzen von Routing-Domains zur Lasteingrenzung.
Supernetting	Gegenteil von Subnetting. Beim Supernetting werden Netzwerke logisch zusammengefasst.
Switch	Gerät zur Vermittlungstechnik für Datenpakete (Zellen) in Hochgeschwindigkeitsnetze wie ATM.
TDD	Bei dem TDD-Verfahren handelt es sich um ein Zeitmultiplex -Verfahren für Funkübertragungen. Bei diesem Verfahren werden für den Uplink und den Downlink die gleichen

	Übertragungsfrequenzen benutzt, allerdings im Zeitmultiplex mit periodischer Umschaltung.
Telnet	Terminal-Emulations-Protokoll, das in TCP/IP standardmäßig integriert ist. Es erlaubt einem Rechner, sich in einen anderen Rechner über eine Netzverbindung einzuloggen.
Terminal	Datenein- und Ausgabegerät (Tastatur, Bildschirm), das die Arbeit mit Programmen erlaubt, die auf einem Server ablaufen.
Token Ring	Ringnetzwerk, das aus Sicherheits-, Fehlertoleranz- und Redundanzgründen aus einer Reihe ringförmig gekoppelter Sterne gebildet wird, sich logisch aber wie ein Ring verhält.
Token-Passing	Zugriffsverfahren, das mit Hilfe eines speziellen Bitmusters die Sendeberechtigung vergibt.
Topologie	1) Anordnung in der Rechner beim Aufbau eines LAN miteinander verbunden werden. Es gibt Bus-, Ring- und Sterntopologie sowie Mischformen. 2) Allgemein die Struktur eines Netzwerkes.
Trailer	Endteil eines Datenpaketes
Translator	Leistet die erforderliche Umsetzung der Signale von der Sende- auf die Empfangsfrequenz
Unicast	Datentransfer zwischen einem Sender und einem Empfänger. Adressierung eines einzelnen Empfängers.
WAN	WANs bestehen aus mehreren LANs, die über Fernleitungen miteinander gekoppelt sind. Solche Verbindungen können z.B. per Wählverbindung, ISDN, oder verschiedensten Arten von Standleitungen hergestellt werden.
X.25	Beschreibt den synchronen Betrieb einer paketfähigen DTE an einem PDN und umfasst sowohl den zeitlichen Ablauf, als auch das Datenformat.

Zelle	1) Übertragungseinheit (Datenblock) fester Länge, der durch eine Cell-Switching-Vermittlungstechnik weitergeleitet wird. 2) Im Mobil- und Bündelfunk eine räumliche Untereinheit des Gesamtnetzes.

F Abkürzungsverzeichnis

3GPP	Third Generation Partnership Project
AAL	ATM-Adaption-Layer
AH	Authentication Header
ALG	Application Level Gateway
AMR	Adaptive Multi Rate
ARP	Address Resolution Protocol
ARPANET	Advanced Research Projects Agency Network
AS	Autonomes System
ASIC	Application Specific Integrated Circuit
ATM	Asynchronous Transfer Mode
BGP	Border Gateway Protocol
BOOTP	Bootstrap Protocol
CDMA	Code Division Multiple Access
CIDR	Classless Inter-Domain Routing
CLNP	Connection-Less Network Protocol
CN	Core Network
CoA	Care-of Address
CRC	Cyclic Redundancy Check
CSCF	Call State Control Function
CSMA/CA	Carrier Sense Multiple Access / Collision Avoidance
CSMA/CD	Carrier Sense Multiple Access / Collision Detection
DECT	Digital European Cordless Telephone
DES	Data Encryption Standard
DFN	Deutsches Forschungsnetz www.dfn.de
DHCP	Dynamic Host Configuration Protocol
DHCPv6	Dynamic Host Configuration Protocol version 6
DMZ	Demilitarized Zone
DNS	Domain Name System (Internet)
DNS	Domain Name Service (IP)
DoD	Department of Defence
DTE	Data Terminal Equipment

E-BGP	Exterior Border Gateway Protocol
EGP	Exterior Gateway Protocol
EDGE	Enhanced Data Rates for GSM Evolution
EMS	Enhanced Messaging Service
ERAN	EDGE Radio Access Network
ESP	Encapsulating Security Payload
ETSI	European Telecommunications Standard Institute
EUI-64	Extended Unique Identifier 64 Bit
FA	Foreign Agent
FDD	Frequency Division Duplex
FDDI	Fiber Distributed Data Interface
FE	Fast Ethernet
FP	Format Prefix
FTP	File Transfer Protocol
GE	Gigabit Ethernet
GGSN	Gateway GPRS Support Node
GMSC	Gateway Mobile Switching Center
GPRS	General Paket Radio Service
GRE	Generic Routing Encapsulation
GSM	Global System for Mobile Communications
GTP	GPRS Tunneling Protocol
HA	Home Agent
HLR	Home Location Register
HSS	Home Subscriber Server
HTTP	Hyper Text Transfer Protocol
IAB	Internet Architecture Board
IANA	Internet Assigned Numbers Authority
I-BGP	Interior Border Gateway Protocol
ICMP	Internet Control Message Protocol
ICMPv6	Internet Control Message Protocol for IPv6
IEEE	Institute of Electrical and Electronic Engineers
IESG	Internet Engineering Steering Group

IETF	Internet Engineering Task Force
IGMP	Internet Group Management Protocol
IGP	Interior Gateway Protocol
IHL	Internet Header Length
IKE	Internet Key Exchange
IMS	Internet Multimedia Subsystem
IOS	Internet Operating System (Cisco Software)
IP	Internet Protocol
IPng	Internet Protocol Next Generation
IPSec	Internet Protocol Security
IPSP	Internet Protocol Security Protocol
IPv4	Internet Protocol Version 4
IPv6	Internet Protocol Version 6
IPX	Internetwork Packet Exchange
ISDN	Integrated Services Digital Network
IS-IS	Intermediate System to Intermediate System
ISO	International Standardisation Organisation
ISP	Internet Service Provider
L2TP	Layer 2 Tunneling Protocol
LAN	Local Area Network
MAC	Media Access Control
MAC-Adresse	Media Access Control Adresse
MBONE	Multicast Backbone www.mbone.de
MGCF	Media Gateway Control Function
MGW	Media Gateway Function
MIME	Multipurpose Internet Mail Extensions
MLD	Multicast Listener Discovery
MMS	Multimedia Messaging Service
MN	Mobile Node
MPLS	Multiprotocol Label Switching
MSC	Mobile Switching Center
MTU	Maximum Transmission Unit
MVPN	Mobile Virtual Private Network
NAT	Network Address Translation

NAT-PT	Network Address Translation – Protocol Translation
ND	Neighbour Discovery
NFS	Network File System
NLA	Next Level Aggregator
NLA ID	Next-Level Aggregation Identifier
NSAP	Network Service Access Point
OSI	Open Systems Interconnection
OSPF	Open Shortest Path First
PDA	Personal Digital Assistant
PDN	Public Data Network
PDU	Protocol Data Unit
PLMN	Public Land Mobile Network
PPP	Point-to-Point Protocol
PSTN	Public Switch Telephone Network
QoS	Quality of Service
RARP	Reverse Address Resolution Protocol
Res	Reserviert
RFC	Request for Comments
RIP	Routing Information Protocol
RPC	Remote Procedure Call
R-SGW	Roaming Signalling Gateway Function
RTP	Real-time Transport Protocol
SDH	Synchronous Digital Hierarchy
SGSN	Serving GPRS Support Node
SIP	Session Initiation Protocol
SLA	Service Level Agreement
SLA ID	Site-Level Aggregation Identifier
SLIP	Serial Line over IP
SLP	Service Location Protocol
SMIL	Synchronized Multimedia Integration Language
SMS	Short Messaging Service
SMTP	Simple Mail Transfer Protocol

SNAP	Sub-Network Access Protocol
SNMP	Simple Network Management Protocol
Stack	Stapelspeicher
TCP	Transmission Control Protocol
TCP/IP	Transmission Control Protocol / Internet Protocol
TD-CDMA	Time Division Code Division Multiple Access
TDD	Time Division Duplex
TDMA	Time Division Multiple Access
TLA	Top Level Aggregator
TLA ID	Top-Level Aggregation Identifier
TOS	Type of Service
T-SGW	Transport Signalling Gateway Function
TTL	Time to Live
UDP	User Datagram Protocol
UE	User Equipment
UMTS	Universal Mobile Telecommunication System
UPT	Universal Personal Telecommunications
URAN	UMTS Radio Access Network
USIM	Universal Subscriber Identity Module
UTRAN	UMTS Terrestrial Radio Access Network
VHE	Virtual Home Environment
VPN	Virtual Private Network
WAN	Wide Area Network
W-CDMA	Wide Code Division Multiple Access
XDR	External Data Representation Standard