Zeitschrift: Comtec : Informations- und Telekommunikationstechnologie = information and telecommunication technology

Herausgeber: Swisscom

Band: 76 (1998)

Heft: 5

Artikel: Das Internet-Protokoll der nächsten Generation

Autor: Gisinger, Hans-Peter

DOI: https://doi.org/10.5169/seals-877300

IP Version 6

Das Internet-Protokoll der nächsten Generation

Die neue Version des Internet-Protokolls wurde nicht als radikaler Schritt weg vom aktuellen und äusserst erfolgreichen IPv4, sondern als massvolle Evolution mit vielen Verbesserungen, Vereinfachungen und Erweiterungen entworfen. Funktionen, die sich in IPv4 bewährten, wurden in IPv6 übernommen, andere wurden entfernt.

HANS PETER GISIGER, BERN

Gewisse Änderungen in IPv6 sind nicht revolutionär, bringen jedoch entscheidende Verbesserungen der Funktionalität und der Architektur:

- Einfacherer Header:
  Um trotz der vervierfachten Adresslänge die Paket-Headers so effizient wie möglich zu verarbeiten, wurden einige der IPv4-Felder weggelassen oder zur Option erklärt.
- Verbesserte Behandlung von Optionen:
  Durch die Einführung von *Extension Headers* anstelle der variablen Anzahl Optionen im Header können Optionen effizienter, flexibler und selektiver behandelt werden.
- Erweiterte Routing und Adressierungsmöglichkeiten:
  IPv6 vergrössert die IP-Adresse von 32 auf 128 Bits, wodurch eine hierarchische Adressierung mit mehreren Ebenen, eine viel grössere Anzahl von adressierbaren Knoten und eine einfachere *Autokonfiguration* von Adressen möglich wird.
  Mit *Anycast-Adressen* wird ein neuer Adresstyp definiert. Eine solche Adresse identifiziert eine Gruppe von Knoten, von denen genau ein Knoten das eintreffende Paket erhält. Die Verwendung von Anycast-Adressen in IPv6 ermöglicht *Policy Routing,* das heisst, der Pfad durch den der Verkehr fliesst, kann kontrolliert werden.
- Quality-of-Service-Unterstützung:
  Um die Zugehörigkeit von Paketen zu einem bestimmten, vom Sender für eine besondere Behandlung bestimmten Verkehrs-Fluss zu markieren, wurde das Protokoll entsprechend erweitert. Dadurch können Quality-of-Service und *Real-time* Services unterstützt werden.
- Unterstützung der Security:
  IPv6 beinhaltet Erweiterungen, welche die Authentisierung, die Datenintegrität und Vertraulichkeit unterstützen. Diese Erweiterungen sind Grundelemente jeder IPv6-Implementation.

Evolution des Internet-Protokolls

Die vierte Version des Internet-Protokolls, die «Sprache» des Internet, ist inzwischen bereits 20 Jahre alt.
Das heutige Internet hatte ursprünglich folgende Zielsetzungen:

- hohe Verfügbarkeit (militärische Anwendungen)
- Dienstevielfalt
- heterogene Teilnetze
- verteilte Verwaltung der Netz-Ressourcen
- Wirtschaftlichkeit und
- billige Anschlusstechnik.

Um hohe *Verfügbarkeit* zu erreichen, wurde die Datengrammtechnik mit wenig Zusatzinformationen im Netz und einer verteilten Verwaltung des Netzes gewählt.
Die *Dienstevielfalt* wurde durch Einführung von IP als Netzwerkprotokoll und TCP/UDP als Transportprotokolle erreicht.
Durch minimale Anforderungen an die Subnetze bezüglich Zuverlässigkeit und einer Fragmentierung in IP konnte die grosse *Heterogenität* der Teilnetze zugelassen werden.
An der Technologiefront hat sich in der Zwischenzeit viel ereignet und der Siegeszug des kommerziellen Internet mit vielen Millionen Benutzern ist nicht mehr aufzuhalten.

Der unglaubliche Erfolg des Internet ist aber heute auch sein Problem

- Der Adressbereich der *Internet-Adressen* droht auszugehen. Diese akute Gefahr beeinträchtigt das weitere Wachstum des Internet. Investitionen bisheriger Nutzer und Anbieter von Services sind durch das Fernbleiben neuer Nutzer bedroht.
- Die existierende *Adress-Architektur* verhindert ein effizientes Routing für Internet-Service-Provider.

	IPv4	IPv6
IP Adresse	4 Bytes long Addresses – gehen langsam aus – Routing nicht effizient	16 Bytes lange Adressen – gewaltiger Adressumfang – Routing effizienter
Netzwerk Adressen-Management (plug & play)	Manuell DHCP optional Router Discovery optional	*Autokonfiguration* (stateless) *DHCP* obligatorisch (stateless) *Router Discovery* obligatorisch *Neighbor Discovery* Detektion Aufdecken doppelter Adressen
Sicherheit	Retrofit, optional	Im Standard obligatorisch verlangt, integriert und flexibel
Quality-of-Service (QoS)	Optional, Zusatz	Eingebaute *Features* wie *Flow Labels* und Prioritäts-Felder zur Unterstützung der QoS
Mobilität	Retrofit, benötigt fremde und sog. home-Agents	Eingebaut als *Extension Headers* in IPv6, *Neighbor Discovery* and *Autokonfiguration*

Tabelle 1. Gegenüberstellung der Haupteigenschaften von IPv4 und IPv6.

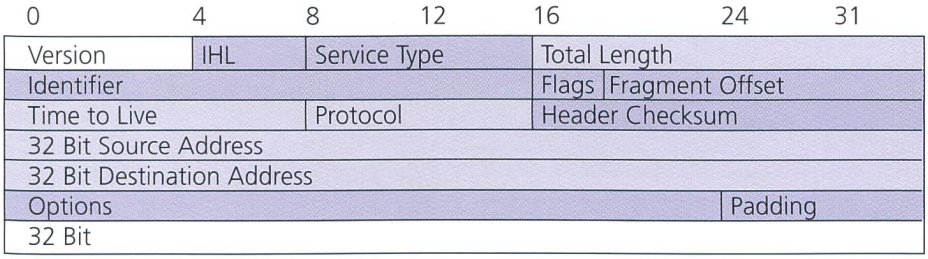


Bild 1. IPv4 Packet Header.

- Die *Systemverwaltung* ist sehr arbeitsintensiv, komplex und fehleranfällig. Zurzeit sind keine dynamischen Konfigurationsmöglichkeiten im Mobile-Bereich vorhanden.
- *Sicherheitsbedürfnisse* der Anwender sind inzwischen weit über die IPv4-Infrastruktur-Möglichkeiten hinausgewachsen.
- Die *Reservation* von Bandbreiten und Ressourcen kann in IPv4 nicht angemessen gelöst werden und verhindert dringend benötigte Real-time-Anwendungen.

Um diese und ähnliche Probleme zu lösen, wurde von der Internet Engineering Task Force (IETF), der verantwortlichen Instanz in der Internet-Standardisierung, im Jahre 1991 die Arbeit für ein neues Internet-Protokoll in Angriff genommen. 1993 wurde von der IETF eine Arbeitsgruppe ins Leben gerufen, mit dem Ziel, ein neues Protokoll zu definieren. IPv6, eine sinnvolle Kombination verschiedener früherer Vorschläge, wurde als zukünftiger Ersatz von IPv4 ausgewählt. Eine wichtige Rolle bei der Wahl von IPv6 als zukünftiges Protokoll spielte die Möglichkeit einer sanften Migration von IPv4 auf IPv6 und der möglichen Koexistenz beider Protokolle und deren Interoperation über lange Zeit. Tabelle 1 stellt die wichtigsten Eigenschaften beider Protokolle, IPv4 und IPv6, gegenüber.

Ist IPv6 ein Mythos oder Realität?

Will man nicht riskieren, erst zu reagieren, wenn das Internet (IPv4) zusammenbricht, muss man sich heute mit IPv6 beschäftigen. Seit mehr als fünf Jahren wird an IPv6 entwickelt, und seit einem Jahr befindet sich ein *Public Domain Network* im Test. Um zu überprüfen, womit sich die IT-Industrie heute befasst, können die Aktivitäten im 6Bone konsultiert werden. Der 6Bone ist ein öffentliches *Testbed* zur Unterstützung der Entwicklung von IPv6. IPv6-Sites sind mit dem 6Bone über IPv4-Tunnels verbunden. Zurzeit existieren rund 175 registrierte IPv6-Sites – verteilt über 30 Staaten – auf dem 6Bone. Auf dem 6Bone stehen inzwischen bereits 28 verschiedene Implementationen, seien es Host-Implementationen oder Router-Implementationen, zur Verfügung.
Um alle Teile von IPv6 vollständig zu definieren, reife Produkte zu entwickeln und zu vertreiben, braucht die Entwicklung von IPv6 jedoch noch eine gewisse Zeit. Einzelne Teile von IPv6 sind jedoch bereit, eingesetzt zu werden.

Eine Protokollübersicht

IPv6-Header contra IPv4-Header

Die Grösse des IPv4-Header mit seinen 13 Feldern ist *variabel,* das heisst er benötigt 20 Bytes und zusätzlichen Platz für eine variable Anzahl von *Optionen.* Das Header-Format von IPv6 hingegen ist bedeutend einfacher. Er umfasst nur noch 8 Felder und benötigt mit 40 Bytes eine *feste* Grösse. Obwohl IPv6-Adressen viermal länger sind als IPv4-Adressen, ist der IPv6-Header bloss doppelt so gross wie der IPv4-Header. Die Bilder 1 und 2 geben einen Vergleich der beiden IP-Header. Verschiedene Felder wurden im neuen Header weggelassen, andere neu definiert oder umbenannt. Neue Felder in IPv6 sind:

- Das Feld *Class* ermöglicht einer Quelle, ihren Paketen eine gewünschte Übertragungs-Priorität zuzuordnen.
- Das Feld *Flow Label* wird beim Routing zur Unterstützung der *Packet Forwarding Decisions* verwendet. Es handelt sich dabei um eine Zufallszahl. Ein Flow (Fluss) wird dadurch zu einer Sequenz von Paketen, die speziell behandelt werden. Eine eindeutige Flusskennung setzt sich zusammen aus der Quell-Adresse und dem Flow-Label: Unique Flow = Source Address + Flow Label.
- Das *Payload-Length*-Feld bestimmt die Länge des Teils eines Pakets, der dem IPv6-Header folgt und ist in Octets definiert.
- Der *Next Header* entspricht dem *Protocol*-Feld aus IPv4 und bestimmt den Beginn des nächsten Headers (vgl. auch Extension Headers).
- Das *Hop-Limit*-Feld entspricht dem *Time-to-Live*-Feld des IPv4-Protokolls und wird durch jeden Knoten dekrementiert. Das Paket wird verworfen, wenn das Hop-Limit zu Null wird; dadurch wird die Lebensdauer eines Paketes bestimmt.

Extension Headers

Da die Optionen aus dem IPv6-Header entfernt wurden, sind als Ersatz dafür sog. *Extension Headers* eingeführt worden. Extension Headers können über das Feld *Next Header* verkettet werden (Bild 3). Die Reihenfolge der Extension Headers ist wichtig, da die Header in der entsprechenden Reihenfolge abgearbeitet werden. Diese Reihenfolge ist in der IPv6-Spezifikation wie folgt definiert:

- *Hop-by-Hop Options (Jumbo Payload):* Tragen Informationen, die bei jedem Hop gelesen werden (z. B. RSVP's Resource Reservation Message). Deshalb muss diese Option unmittelbar dem IPv6-Header folgen. Die Hop-by-Hop-Option trägt auch die *Payload-Length*-Information von *Jumbo*-Paketen.
- *(Source) Routing:* Die Routing Extension enthält *Source Routing* Information. Diese Information besteht aus einer geordneten Liste von IPv6-Adressen, die das Paket besuchen muss.

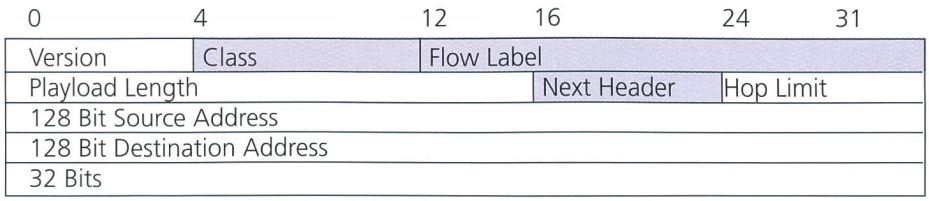


Bild 2. IPv6 Packet Header.

IPv6 Header Next = TCP	TCP Header	Application Data	
IPv6 Header Next = Routing	Routing Hdr Next = TCP	TCP Header	Application Data
IPv6 Header Next = Routing	Routing Hdr Next = Frag	Fragmentation Hdr Next = TCP	TCP Header	Application Data

Bild 3. Beispiele von Header-Verkettungen.

- *Fragmentation:*
  Da IPv6 nur noch End-zu-End-Fragmentierung kennt, enthält diese Extension Felder, die eine Gruppe von Fragmenten eines Pakets identifizieren und weist ihnen Sequenznummern zu.
- *Destination Options* (Mobile Binding Update, Anycast Address Dynamic Update):
  Trägt Informationen für die Destination des Pakets.
- *Authentication:*
  Der IPv6-Authentication-Header garantiert auf Transport-Ebene, dass empfangene Pakete auch wirklich von der richtigen Quelle stammen.
- *Encapsulation Security Payload:*
  Garantiert durch Verschlüsselung Privacy und Integrität der Daten auf Transport-Ebene.

Ein Router muss dabei nur die beiden ersten Header (Hop-by-Hop, Routing) bearbeiten.

IPv6-Adress-Architektur

Wie im IPv4-Modell werden Adressen auch im IPv6-Modell Schnittstellen (Interfaces) zugeordnet. Schnittstellen können dabei mehrere Adressen tragen, sie müssen aber nicht unbedingt eine Adresse haben. Beispiele zu Schnittstellen ohne Adresse sind Router-Punkt-zu-Punkt-Verbindungen. Einem einzelnen Link können in IPv6 einzelne oder auch mehrere Subnetze zugeordnet werden.
Der IPv6-Adressbereich kann hierarchisch in einen *globalen,* einen *site-local* und in eine *link-lokal* Bereich unterteilt werden. IPv6-Adressen sind entweder *Unicast-, Multicast-* oder *Anycast-Adressen.* Unicast-Adressen sind Adressen an einzelne Interfaces. Da Multicast-Adressen eine Gruppe von Interfaces umfassen, wird ein Paket, das an eine Multicast-Adresse geschickt wird, allen Interfaces, die dieser Adresse zugeordnet sind, weitergegeben. Eine Multicast-Gruppe muss somit zuvor definiert sein. Anycast-Adressen umfassen ebenfalls eine Gruppe von Interfaces, wobei Pakete, die an eine Anycast-Adresse geschickt werden, genau einem Interface dieser vordefinierten Gruppe ausgeliefert werden.

IPv6-Adressen

IPv6-Adressen lassen sich textuell durch 8 Gruppen von 16-Bit-Hex-Werten darstellen:
5F15:ABCD:1234:5678:9ABC:1234:4567:8901.
Durch Unterdrückung führender Nullen und durch Ersatz von Nullen durch "::" (nur einmal erlaubt pro Adresse) lassen sich IPv6-Adressen kompakter darstellen:
FF01:0000:0000:0000:0000:0000:0000:0043
wird zu FF01:0:0:0:0:0:0:43
und wird zu FF01::43.
IPv6 unterstützt verschiedene Adresstypen, wobei die führenden Bits (Format Prefix) auf den Adresstypen hinweisen. Tabelle 2 gibt dazu eine Übersicht.

Legacy-IPv4-Adressen

Legacy-IPv4-Adressen können in IPv6 entweder als *IPv4 Compatible Addresses* oder als *IPv4 Mapped Addresses* dargestellt werden. IPv4 Compatible Addresses sind *echte* IPv6-Knoten mit IPv4 kompatiblen Adressen:
0:0:0:0:0:0:16.36.16.118 oder
::16.36.16.118.
IPv4 Mapped Addresses sind *nur IPv6-Darstellungen* von IPv4-Only-Knoten. Diese Knoten verstehen *kein* IPv6, d. h. diese Adressen erscheinen *nie* auf einer Verbindung:
0:0:0:0:0:FFFF:192.3.4.1 oder
::FFFF:192.3.4.1.

Aggregatable Global Unicast Address

Das wohl wichtigste Adressformat ist die *Aggregatable Global Unicast Address.* Dieses Adressformat wird im 6Bone verwendet. Es unterstützt eine sinnvolle Adress-Aggregation. Bild 3 zeigt dieses Adressformat.
Der Format Prefix (001) definiert das Format *Aggregatable Global Unicast Address.* Die TLA-ID (Top-level-Aggregation) identifiziert grosse Telcos, die untereinander sog. Peering-Verträge aushandeln und den Backbone des IP-Netzes betreiben. Die NLA-ID (Next-level-Aggregation) wird vom TLA administriert und zugeteilt und dient dazu, Adresshierarchien aufzubauen. Die 32-Bit der NLA-ID können in mehrere Ebenen unterteilt werden. Die SLA-ID (Site-level-Aggregation) wird ISPs zugeteilt, um eine eigene lokale Adresshierarchie aufzubauen und Subnetze zu identifizieren. Die Interface-ID identifiziert das Interface eines typischen Host (Bild 4).
Die mögliche Adress-Hierarchie mit Aggregatable Global Unicast Address ist in Bild 5 dargestellt.

IPv6-Interface-ID

Eine IPv6-Interface-ID basiert auf den Standard EUI-64 und wird sowohl in Unicast- als auch in Anycast-Adressen verwendet. Ein EUI-64 basierte Interface-ID wird aufgebaut aus der IEEE 48-Bit-MAC-Adresse, die in der Mitte aufgespaltet (zwischen Company-ID und Manufacturer-Data) und mit FFFE aufgefüllt wird. Bild 6 zeigt die zusammengesetzte 64-Bit-IPv6-Interface-ID.
Eine IPv6-Adresse lässt sich somit als Kombination eines *Prefix* und einer *Interface-ID,* wie in Bild 7 dargestellt, verstehen.
Die Prefix-Darstellung lässt sich auch wie folgt beschreiben:
3FFE:0301:DEC1::/64.

3 Bits	13 Bits	32 Bits	16 Bits	64 Bits
FP	**TLA ID**	**NLA ID**	**SLA ID**	**Interface ID**
001	1FFE	0301:DEC1	0000	0A00:2BFF:FE36:701EE

3FFE: 0301:DEC1:0000:
Public Topology

0A00:2BFF:FE36:701EE
Site Topology

Bild 4. Aggregatable Global Unicast Address.

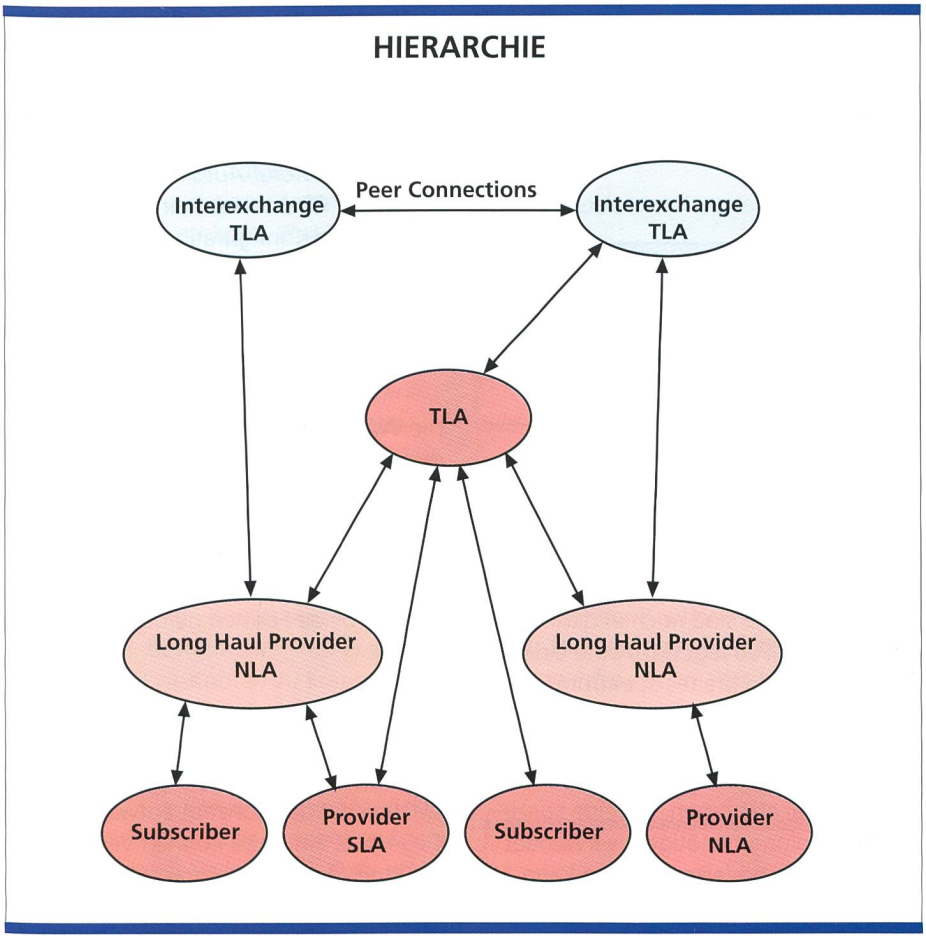


Bild 5. Adress-Hierarchie.

Die Unterscheidung zwischen Prefix und Interface-ID mit je 64 Bits in einer IPv6-Adresse ermöglicht, das *Routing* auf die oberen 64 Bits zu beschränken.

Unicast-Adressen
Die Unicast-Adress-Struktur (Bild 8) mit 128 Bits kann entweder als *global* ohne *innere Struktur* oder *mit innerer Struktur,* d. h. unterteilt in Prefix und Interface-ID, betrachtet werden:
Link-local-Adressen (Prefix: FE80::) werden als einzelne Verbindungen verwendet. Sie setzen sich zusammen aus dem Prefix und der entsprechenden Interface-ID:

FE80::0A00:2BFF:FE36:701E.

Diese Adressen können bei der *Autokonfiguration* und in *kleinen Sites* mit einem *einzigen Link* verwendet werden.
Site-local-Adressen (Prefix: FEC0::) werden innerhalb *einer Site* verwendet:

FEC0::9876:0A00:2BFF:FE36:701E.

Diese Adresse enthält *Site-level-Subnet-Informationen* (z. B. 9876). Site-local-Adressen werden ausserhalb der Site weitergegeben, sind jedoch für Sites gedacht, die aktuell nicht mit dem globalen Internet verbunden sind. Beide lokalen Adressen sind leicht in globale Internet-Adressen zu konvertieren. FE80:: oder FEC0:: sind durch einen globalen Prefix zu ersetzen, wobei beispielsweise die Adresse:

3FFE:0301:DEC1::
0A00:2BFF:FE36:701E

entsteht.

Anycast- und Multicast-Adressen
Anycast-Adressen werden vom Anycast-Adress-Space (Tabelle 2) alloziert und zwei oder mehr Interfaces zugeordnet (üblicherweise auf unterschiedlichen Knoten). Der Verkehr wird dabei dem «nächsten» Interface übermittelt. Multicast-Adressen identifizieren eine Gruppe von Knoten.

Sicherheit
Das Fehlen eines standardisierten Sicherheitsschemas auf dem Netzwerk-Layer ist ein offensichtlicher Mangel in IPv4. *Hacker Spoofing* und *Snooping Data Streams* können IP-basierten Corporate Networks enormen Schaden zufügen. IPv6 begegnet diesem Problem mit Hilfe zweier Extension-Headers, einer unterstützt die *Authentisierung* des IP-Verkehrs, und der andere *verschlüsselt* IP-Pakete teilweise oder vollständig. Die Implementation der Sicherheit auf der Ebene von IP unterstützt sowohl Applikationen, die von einem sicheren Netzwerk ausgehen, als auch Applikationen, die sich nicht explizit um Sicherheit kümmern.
Der IPv6-Authentication-Header garantiert Applikationen, dass empfangene Pakete auch wirklich von einer authentischen Quelle stammen. Mit IPv6-Authentication-Headers können Hosts eine standard-basierte Sicherheitsgemeinschaft aufbauen, die auf dem Austausch von algorithmen-unabhängigen *Secret Keys* basiert.
Authentication-Headers eliminieren eine Reihe von *Host-Spoofing- und Paket-Modification-Hacks,* sie verhindern jedoch nicht das unterbrechungsfreie *Lesen* (Sniffing, Snooping) der Inhalte der Pakete, die das Internet oder den Corporate Backbone traversieren. Mit Hilfe des *Encapsulating Security Payload Service* (ESP) in IPv6, einem optionalen Extension Header, kann dieses Problem gelöst werden. Pakete, geschützt durch ESP-Verschlüsselungstechniken, geniessen ein hohes Mass an *Privacy* und *Integrität,* was im aktuellen Internet zurzeit nur mit einzelnen sicheren Applikationen (z. B. Private Electronic Mail usw.) erreicht werden kann. ESP unterstützt Verschlüsselung auf dem Netzwerk-Layer, wodurch dieser Service für alle Applikationen in einer standardisierten Weise zur Verfügung steht.
IPv6-ESP kann so verwendet werden, dass entweder der Transport-Layer-Header und die Nutzlast (z. B. TCP, UDP), oder das ganze IP-Datagramm verschlüsselt werden. Beide Methoden verwenden einen ESP-Extension-Header, der die Ver-

Company ID			Filler		Manufacturer ID		
08	00	2B	**FF**	**FE**	36	70	1E

Bild 6. 64-Bit-IPv6-Interface-ID.

Format Prefix (FP)	Zuteilung des Adressbereiches
0000 001	NSAP Address Allocation
0000 010	IPX Address Allocation
001	*Aggregatable Unicast Addresses*
1111 1110 10	*Link Local*
1111 1110 11	*Site Local*
1111 1111	*Multicast Addresses*
Special Addresses	
0:0:0:0:0:0:0:0	= :: Unspecified Address
nicht zugewiesene Adressen	während Konfiguration als Source verwendet
0:0:0:0:0:0:0:1	= ::1 Loopback Address

Tabelle 2. Prefixes der Adresstypen.

schlüsselungs-Parameter und Schlüssel von Endpunkt zu Endpunkt trägt. Wenn nur die Transport-Nutzlast verschlüsselt wird, wird der ESP-Header direkt vor dem Transport-Header eingefügt, und die Headers vor dem ESP-Header werden nicht verschlüsselt. Diese Methode wird als *Transport-Mode* bezeichnet. Wenn das ganze IP-Datagramm verschlüsselt werden soll, wird ein neuer IPv6- und ESP-Header vorangestellt und alle Felder eingepackt. Diese Methode wird als *Tunnel-Mode* bezeichnet, da der Inhalt des Datagramms nur an den Endpunkten des Sicherheitstunnels (Steel Pipe) sichtbar wird (Bild 9). Vollständig verschlüsselte Datagramme sind sicherer, da die Headers nicht zur Analyse des Verkehrs verwendet werden können.
Die Authentisierungs- und Verschlüsselungs-Services von IPv6 arbeiten Hand in Hand und schaffen so eine flexible und leistungsfähige Lösung. Normalerweise wird der Authentication-Header vor den verschlüsselten Teil des Pakets plaziert, da die Authentisierung beim Empfänger vor der Entschlüsselung erfolgt. Zusammen bilden diese beiden Services einen robusten, standard-basierten Sicherheits-Mechanismus, der in Zukunft eine wichtige Rolle spielen wird.

Quality-of-Service

Das IPv6-Paket-Format enthält ein 24-Bit-Feld zur Identifikation des *Traffic-Flow,* das für die Implementierung der Quality-of-Service von grosser Bedeutung sein wird. Netzwerk-Layer-basierte Quality-of-Service Produkte sind noch in der Planungsphase. IPv6 legt dazu eine Grundlage, so dass ein breites Spektrum von QoS-Funktionen in einer offenen und interoperablen Weise verfügbar sein wird. IPv6-Flow-Labels können zur Identifizierung von Paketströmen, die eine spezielle Behandlung benötigen, verwendet werden. Fluss-basiertes Routing kann dem Internet gewisse deterministische Charakteristiken ermöglichen, die sonst verbindungs-orientierten Switching-Technologien und der Telephonie vorbehalten sind. Damit wird Desktop-Video oder Audio-Strömen ein Flow Label zugeteilt, das Routern mitteilt, dass eine kontrollierte End-zu-End-Latenz benötigt wird. Flow Labels können auch dazu benutzt werden, Verkehrsflüssen eine spezifische Stufe an Sicherheit, Ausbreitungsverzögerung oder Kosten zuzuordnen.

Prefix	Interface ID
3FFE:0301:DEC1::	0A00:2B**FF**:**FE**36:701E

Bild 7.
Zusammensetzung der IPv6-Adresse.

Adress-Autokonfiguration

Die Autokonfiguration ist für Hosts entworfen worden – Router müssen anders konfiguriert werden. Sie ermöglicht *plug 'n' play*-Möglichkeiten, so dass kein manuelles Adressieren von Hosts mehr notwendig ist. Durch die Autokonfiguration werden «routbare» Adressen generiert. Ebenso kann die Neunummerierung ganzer Subnetze automatisiert werden. Jeder Host lernt dabei seine eigene Adresse und führt den Verzeichnisdienst (DNS) nach. Wenn kein Router oder Server benötigt wird, erhält ein Host seine Link-local-Adresse. Im anderen Fall kann zwischen *Statefull-* und *Stateless-Autokonfiguration* unterschieden werden:

- Bei der *Stateless-Autokonfiguration* macht der Router die Prefixes desjenigen Subnetzes bekannt, mit dem ein Host verbunden ist. Hosts generieren dann ein «Interface Token», das ein Interface in einem Subnetz eindeutig identifiziert. Die Adresse wird dann aus diesen beiden Teilen aufgebaut.
- Bei der *Stateful-Autokonfiguration* erhält der Client (Host) eine Adresse oder eine Konfiguration von einem DHCP-Server. DHCP-Server unterhalten die Datenbank und haben eine strenge Kontrolle über die vergebenen Adressen.

Die Wahl der Autokonfiguration kann durch den Administrator erfolgen und hängt von der Stufe der gewünschten Kontrolle über die Adressvergabe und vom gewünschten/erlaubten Aufwand der Adressverwaltung ab. Grundsätzlich können beide Formen gemeinsam existieren.

Mobilität

Um den wachsenden Bedarf nach *Mobile IP* zu unterstützen, wurde in IPv6 ein entsprechendes Konzept entwickelt. IPv6-Hosts auf Reise können Verbindung mit ihrer «home»-IP-Adresse aufrecht erhalten. Bevor man auf die Reise geht, können Benutzer ihren lokalen Router anweisen, den gesamten Verkehr mit ihrer home-IP-Adresse zu einer temporären *Care of Address* weiterzuleiten. Die Care-of-Adresse kann per Autokonfiguration zusammengesetzt werden (Adapter ID + Prefix des fremden Netzes). Bei jedem Reisehalt kann dem Router ein neuer Prefix übermittelt werden.
Dieser Ansatz reduziert die Komplikationen, die beim Ändern des DNS-Eintrages (Zuordnung von Adresse zu Namen) eines Mobilen Computers auftreten. Mit dem IP-forwarding-Feature bleiben DNS-Einträge im wesentlichen unberührt. Bei längerem Verweilen können die Partner (Correspondant Node) über die neue Adresse des mobilen Hosts informiert werden (Binding Update), was dann auch einen Eintrag ins DNS erfordert. Bild 10 zeigt dazu ein typisches Szenario.

Transition zu IPv6

Nicht bekannt ist heute, wie schnell der Übergang von IPv4 nach IPv6 geschehen wird. Einzelne erwarten eine gross ange-

Subnet Prefix	Interface ID
n Bits	128-n Bits

Bild 8. Unicast-Adress-Struktur.

legte Anpassung an IPv6 bereits in naher Zukunft, andere ziehen es vor zu warten, bis der Adressbereich ausgeschöpft ist, und erhoffen dadurch eine Beschleunigung des Übergangs.
Beim Umfang dieser Umstellung ist es klar, dass während einer längeren Zeitspanne beide Protokolle, IPv4 und IPv6, koexistieren müssen. Aus diesem Grund ist es notwendig, dass Hosts und Router in beliebiger Reihenfolge inkrementell aufgerüstet werden können. Um dieses Ziel zu erreichen, wurden verschiedene spezielle Funktionen in den IPv6-Standard eingebaut wie beispielsweise *Dual-Stack*-Hosts und -Routers wie auch *Tunneling*-IPv6 über Ipv4.

Dual-Stack-Transitions-Methode

Auch wenn einige Knoten auf IPv6 umgestellt sind, besteht noch immer das Bedürfnis, mit IPv4-Knoten zu kommunizieren. Diesem Bedürfnis kann mit dem *Dual-Stack-Ansatz* begegnet werden. Dabei hat ein Host Zugriff sowohl auf IPv4- als auch auf IPv6-Ressourcen. Router, die beide Protokolle unterstützen, können dadurch Verkehr von IPv4- und IPv6-Knoten weiterleiten. Dual-Stack-Maschinen können vollständig unabhängige IPv4- und IPv6-Adressen verwenden oder mit IPv4-kompatiblen IPv6-Adressen konfiguriert werden. Um IPv4-Adressen zu erhalten, können Dual-Stack-Knoten konventionelle IPv4-Services (DHCP) verwenden. IPv6-Adressen können manuell in der 128-Bit-lokalen Host-Tabelle konfiguriert oder automatisch via IPv6-*Stateless* resp. -*Statefull* erhalten werden.
Es wird erwartet, dass die meisten Server auf beliebig lange Zeit (oder bis alle Knoten auf IPv6 umgestellt sind) im Dual-Stack-Mode werden arbeiten können.

IPv6 Domain Name Service

Der aktuelle 32-Bit-Name-Service kann die von IPv6 verlangte Namensauflösung mit 128-Bit-Adressen nicht behandeln. Um diesen Mangel zu beheben, haben IETF-Designer einen IPv6-DNS-Standard (RFC 1886, *DNS Extensions to Support IP Version 6)* definiert.
Ist mal ein IPv6-fähiger DNS installiert, können Dual-Stack-Hosts austauschbar mit IPv6-Knoten zusammenarbeiten. Wenn ein Dual-Stack-Host einen DNS abfragt und eine 32-Bit-Adresse zurückerhält, wird IPv4 verwendet; erhält er eine 128-Bit-Adresse, dann wird IPv6 verwendet.

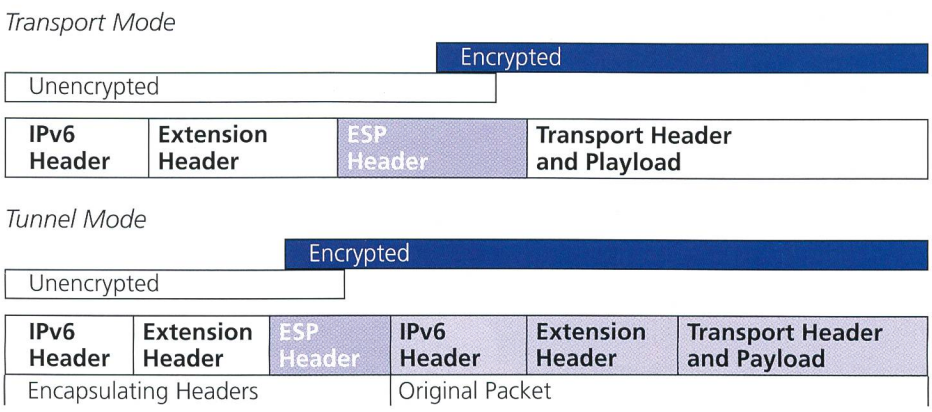


Bild 9. Tunnel Mode und Transport Mode durch IPv6 Encryption.

Routing in IPv6/IPv4-Netzwerken

Router mit IPv4 und IPv6 können in IPv4-Netze administriert werden. IPv6-Versionen populärer Routing-Protokolle wie *Open Shortest Path First* (OSPF) und *Routing Information Protocol* (RIP) sind bereits in Entwicklung.

In vielen Fällen versuchen Administratoren die IPv6-Topologie logisch vom IPv4-Netz zu trennen, auch wenn beide auf der selben physikalischen Infrastruktur laufen. Dadurch können die beiden Versionen getrennt verwaltet werden. Andererseits ist es in gewissen Fällen vorteil-

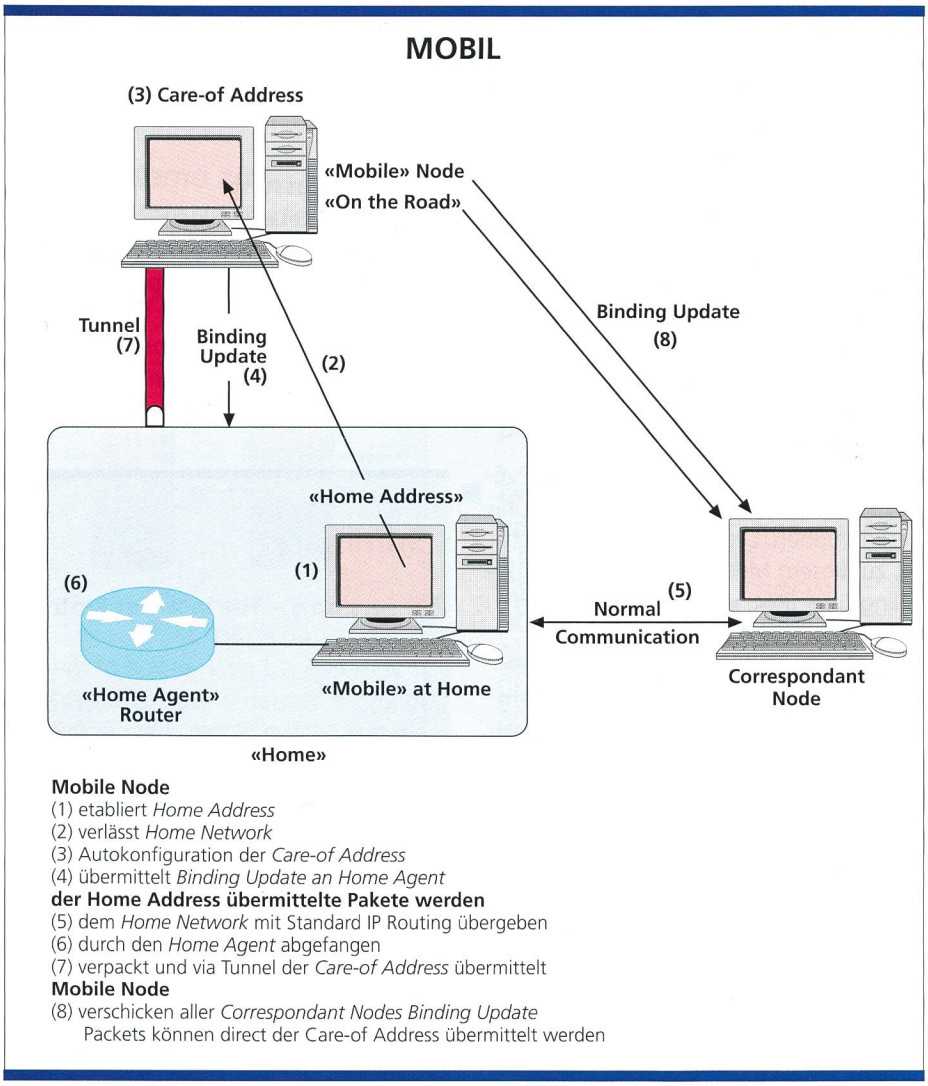


Bild 10. Mobile IP.

***Hans Peter Gisiger**, Dr. sc. techn., Dipl. El.-Ing. und Informatik-Ing. ETH, diplomierte 1982 zum Elektroingenieur und 1986 zum Informatik-Ingenieur an der ETH Zürich. Anschliessend arbeitete er mehrere Jahre als Assistent/Wissenschaftlicher Mitarbeiter und Oberassistent am Institut für Technische Informatik und Kommunikationsnetze (TIK) an der ETH, wo er 1992 auch zum Dr. sc. techn. an der Abteilung für Informatik der ETHZ promovierte. Seit 1995 arbeitet Hans Peter Gisiger bei Swisscom Corporate Technology (früher Forschung und Entwicklung) als Projektleiter, wo er sich intensiv mit objektorientierten Technologien und New LAN Technologies befasst.*

haft, die beiden Architekturen auf die selben Grenzen, Bereiche und Subnetze auszurichten. Beide Ansätze haben ihre Vor- und Nachteile: eine separate IPv6-Architektur schafft die Gelegenheit für einen Neuanfang mit einem hierarchischen Netzwerk-Adressplan, der die Verbindung zu einem oder mehreren ISPs stark vereinfacht. Dies legt auch die Grundlage für eine effiziente Neunummerierung, für Route Aggregation und andere Ziele einer Advanced-Internetwork-Routing-Hierarchie.
In vielen Organisationen, in denen IPv6 inkrementell eingeführt wird, werden Inseln von IPv6-Topologien in einem Ozean von IPv4 entstehen. Glücklicherweise haben IPv6-Designer die Transitions-Mechanismen so ausgestattet, dass IPv6-Hosts über das IPv4-Netzwerk kommunizieren können. Die entscheidende Technik zu diesem Mechanismus ist IPv6-Tunneling über IPv4, wobei IPv6-Pakete in IPv4-Pakete eingepackt werden.
Tunneling ermöglicht frühen IPv6-Implementationen, die Vorteile der bestehenden IPv4-Infrastruktur ohne Änderungen der IPv4-Komponenten zu nutzen. Ein Dual-Stack-Router oder -Host am Rand einer IPv6-Topologie ergänzt ein IPv6-Paket um einen IPv4-Header und verschickt es als ursprünglichen IPv4-Verkehr über die existierenden Links. IPv4-Router leiten diesen Verkehr mit Wissen um IPv6 weiter. An der anderen Seite des Tunnels packt ein anderer Dual-Stack-Router das IPv6-Paket aus und leitet es mit Standard-IPv6-Protokoll an die eigentliche Destination weiter.

Konfiguriertes und Automatisches Tunneling

Um *konfiguriertes Tunneling* zu realisieren, müssen Administratoren manuelle IPv6-zu-IPv4 Adress-Abbildungen und Tunnel-Endpunkte definieren. Auf beiden Seiten des Tunnels wird der Verkehr mit 128-Bit-Adressen weitergeleitet. Am Tunnel-Eingangspunkt wird ein Router-Tabelleneintrag manuell konfiguriert.
Automatische Tunnels verwenden IPv4-kompatible Adressen. Wenn Verkehr mit kompatiblen Adressen weitergeleitet wird, kann das Device am Tunneleingang automatisch den eingekapselten Verkehr adressieren, indem die IPv4-kompatible 128-Bit-Adresse in 32-Bit-Ipv4-Adressen konvertiert wird. Auf der anderen Seite des Tunnels wird der IPv4-Header entfernt und die ursprüngliche IPv6-Adresse wieder hergestellt. Automatisches Tunneling ermöglicht IPv6-Hosts, dynamisch IPv4-Netze zu nutzen.
Mit IPv4-kompatiblen Adressen können Vorteile des erweiterten Adressraums jedoch nicht genutzt werden, andere Verbesserungen wie Flow Labels, Authentisierung, Verschlüsselung, Multicast und Anycast hingegen bringen die IPv6-Vorteile.

Zusammenfassung

IPv6 ist eine neue Version des Internet-Protokolls, entworfen als Nachfolger des heutigen IPv4. Will man Experten glauben, gibt es über kurz oder lang keine Alternative zu diesem Protokoll. Einige Änderungen sind revolutionär, andere sind grundlegende Verbesserungen der Funktionen und der Architektur. Die wichtigsten Eigenschaften von IPv6 sind
- der erweiterte Adressbereich,
- die Plug-and-play-Möglichkeiten der Autokonfiguration,
- die inhärenten Möglichkeiten für Netzwerk-Mobility,
- der vollständige Sicherheitsstandard, der zu IPv6 gehört, und
- das Potential für Quality-of-Service-Möglichkeiten.

Dank seiner Rückwärts-Kompatibilität mit IPv4 ist eine sinnvolle und inkrementelle Transitionsstrategie von IPv4 nach IPv6 möglich.
Erste Produkte von IPv6 sind in der zweiten Hälfte dieses Jahres zu erwarten. [1, 7]

Literatur

[1] Hinden, R. M.: *IP Next Generation Overview,* http://playground.sun.com/pub/ipng/html/INET-IPng-Paper-html, 1995.
[2] Bay Networks, *The Case for IPv6,* White Paper, 1997.
[3] Bradner, S. O., Mankin, A.: *IPng: Internet Protocol Next Generation,* Addison-Wesley, IPng Series, 1996.
[4] *IP Next Generation Homepage:* http://playground.sun.com/pub/ipng/html/ipng-main.html
[5] *6Bone Homepage:* http://www.6bone.net/

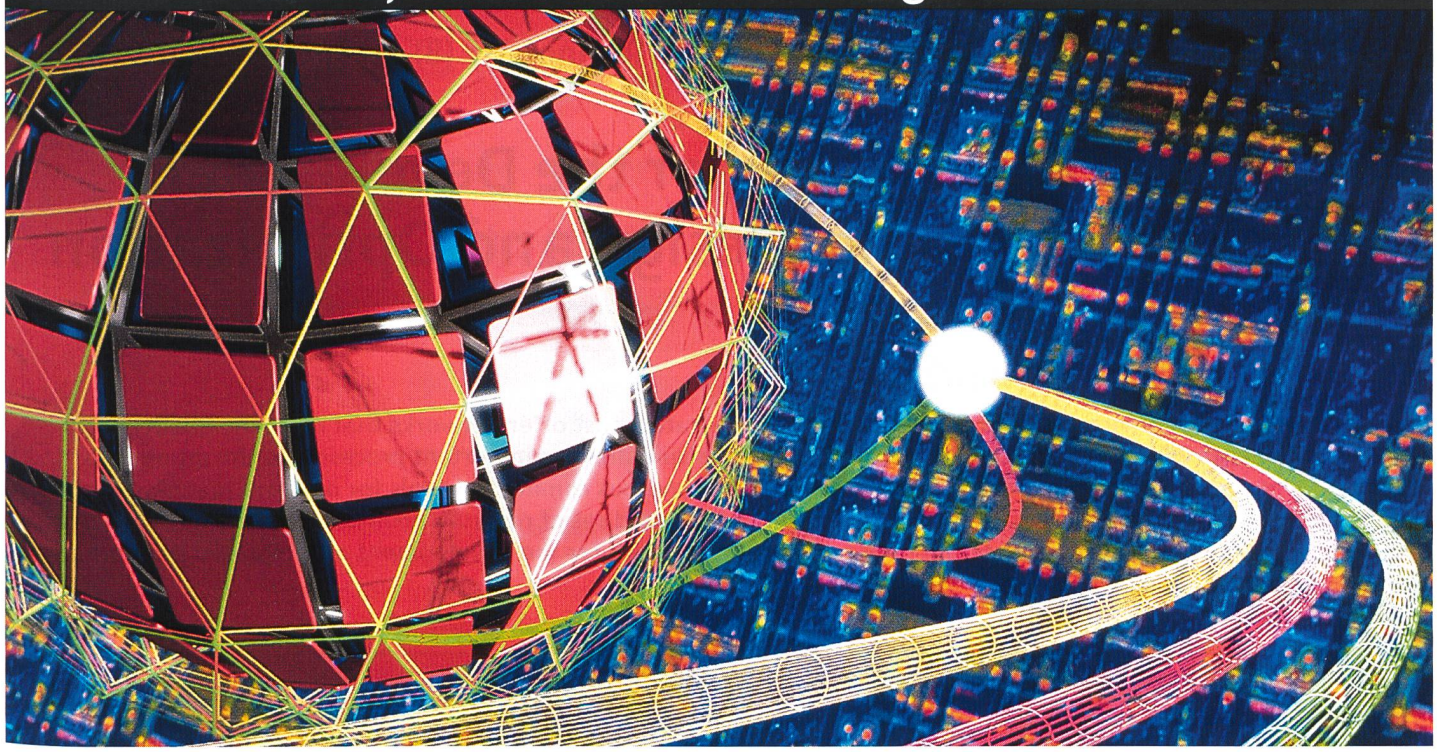
Summary

IP version 6 – The Internet Protocol of the Next Generation

IP version 6 is a new version of the Internet protocol, designed as the successor of today's IP version 4. Experts say that there will be no alternative to IPv6 in a longer perspective. Some changes in this new protocol are revolutionary, others are basic and important enhancements of functionality and architecture. The most important features of IPv6 are:
– the enormous address range,
– the plug-'n'-play features of the autoconfiguration,
– all the inherent potential for network mobility,
– the complete and mandatory security standard of IPv6, and
– the potential for quality-of-service.

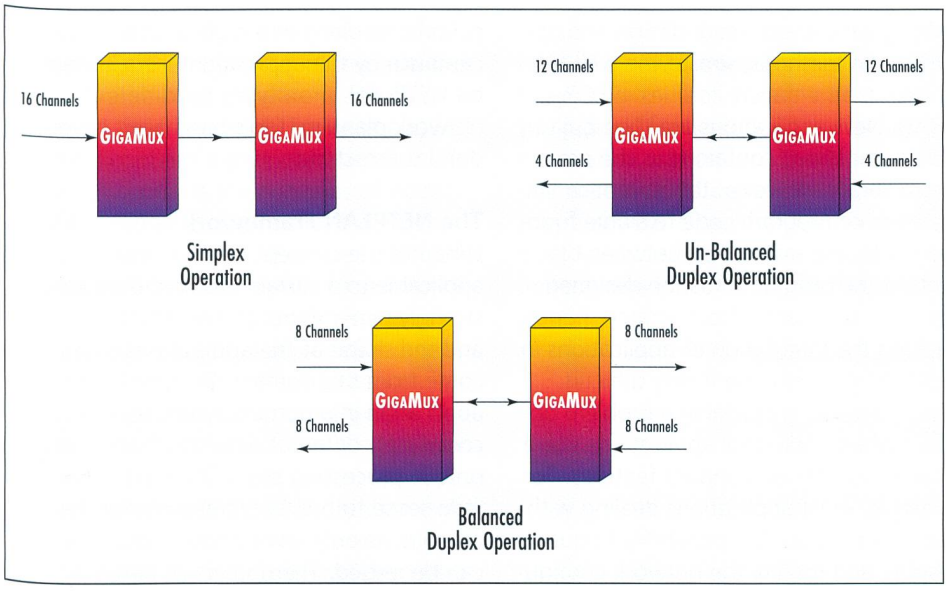
Due to the backward-compatibility with IPv4 an incremental transition strategy from IPv4 to IPv6 is possible. First products of IPv6 are available soon.

16 x 2,5 GB/s über eine einzige Glasfaser



GigaMux – neues Leben für Ihre Glasfaser!

Kommunikationstechnologie erfordert immer mehr Leistung und Fortschritte in sämtlichen Bereichen.
Dies gilt auch für die Entwicklung neuer Systeme zur Beseitigung von Engpässen im WAN. Im Mittelpunkt steht dabei die kostengünstige Überwindung der Einschränkungen bei knappen Glasfaserverbindungen im Fernbereich.



- GigaMux die Alternative zum Verlegen zusätzlich teurer Fasern
- Drastische Erhöhung der Kapazität von Glasfasern (Dark Fiber)
- DWDM-Technologie ermöglicht die Bildung von 16 «virtuellen» Glasfasern, je mit einer Übertragungskapazität von bis zu 2.5 GB/s (OC-48)
- Der GigaMux von Osicom ist vollkommen protokolltransparent: ATM OC-1 bis OC-48, GB-Ethernet, FDDI, ESCON, SONET/SDH oder proprietäre Bitstreams werden miteinander über eine Distanz von bis zu 80 km auf einer einzigen Glasfaser übertragen.

Magirus
Value Added Distribution

DeltaNet Communications

Alle reden von MEGA, wir reden von GIGA!

TeleNetCom 26.-29. Mai 1998 Halle 6 / Stand 6.180

DeltaNet AG, Riedstrasse 8, CH-8953 Dietikon, Tel. 01 - 742 05 00, Fax 01 - 742 05 55, http://www.deltanet.ch