Netzwerksicherheit

IP Version 6

Stephen Wolthusen

Fraunhofer IGD Institut Graphische Datenverarbeitung

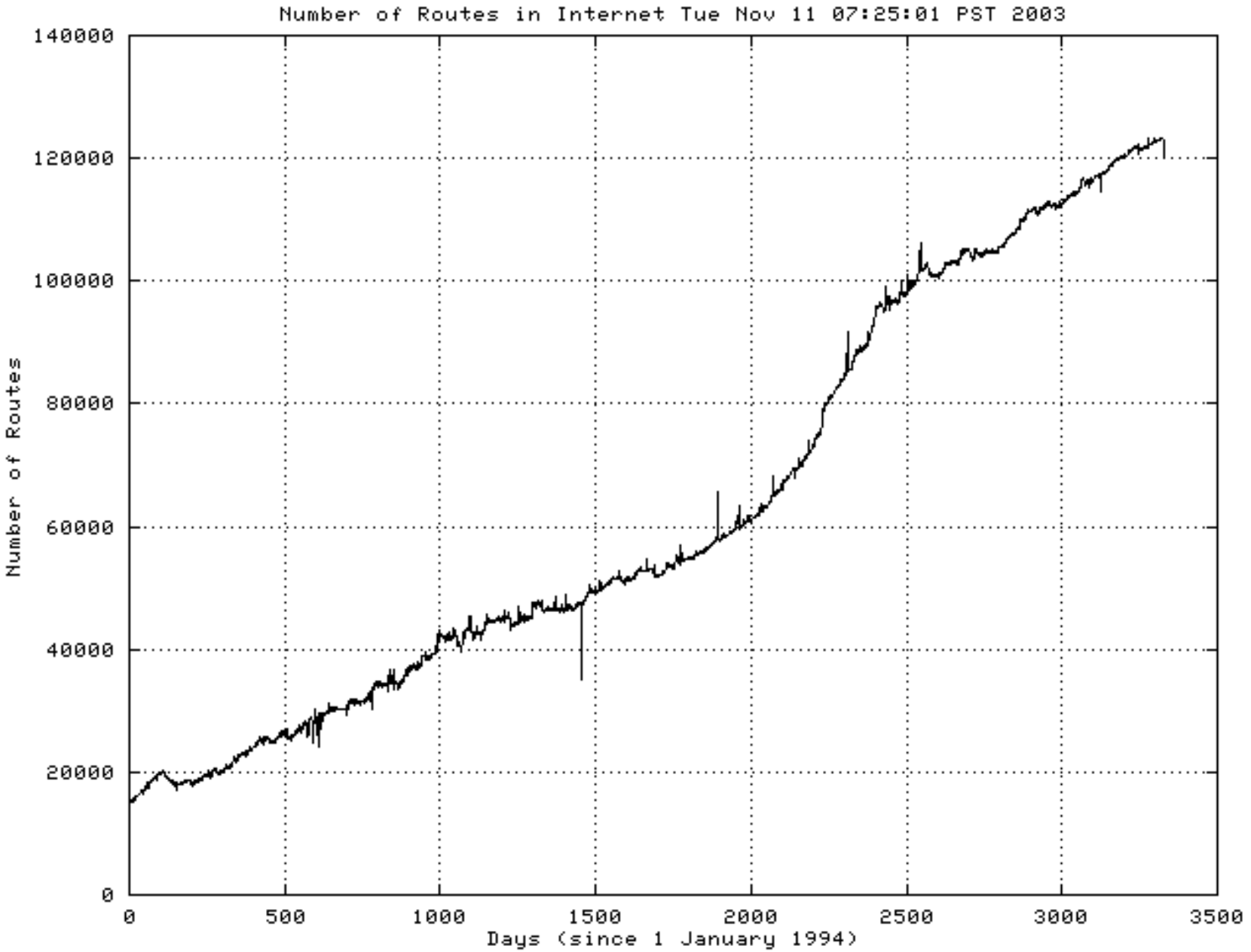
Entwicklung der Routing-Tabellen in Kernroutern

- Mai 1981: 36 Hosts und Gateways
- Allein zwischen 1988 und 1991 Verdoppelung alle 10 Monate
- Januar 1992: 4200 Routen
- Dezember 1992: 8500 Routen

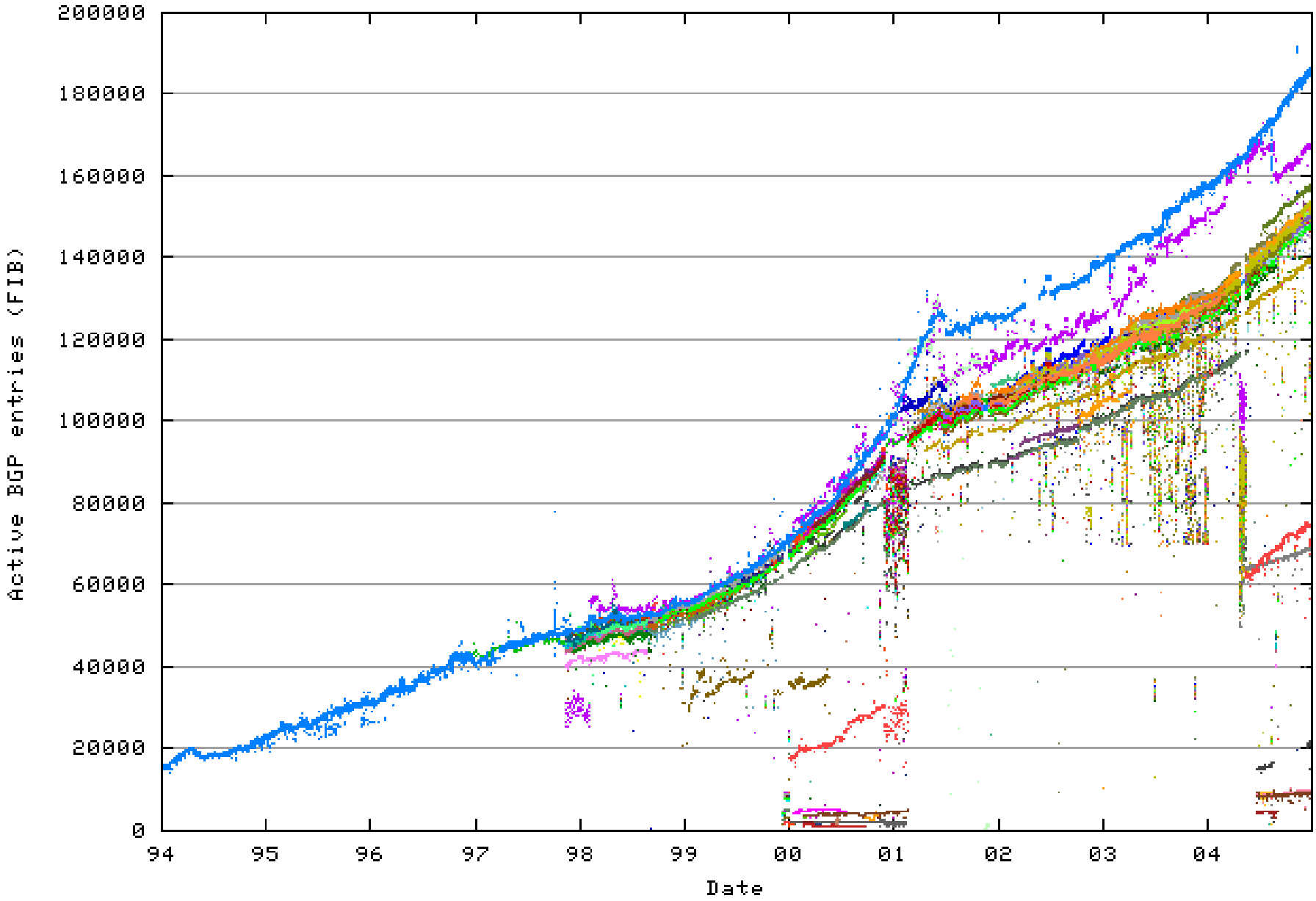
Adreßerschöpfung ?

- Einführung von CIDR 1993
  - Adreßbereich-Konsolidierung bei ISPs
  - Zwischen 1993 und 2000 konnte das Wachstum fast linear gehalten werden
- Wachstum ist mittlerweile wieder (schwach) exponentiell
  - Stand Dezember 2004: Erschöpfung der nicht zugewiesenen IPv4-Adreßbereiche im August 2018, Erschöpfung aller IPv4-Adressen im April 2040
- Dennoch: Änderungen und Anpassungen sind notwendig, aufwendig, kostspielig und brauchen vor allem Zeit

Anzahl der Routen im Internet



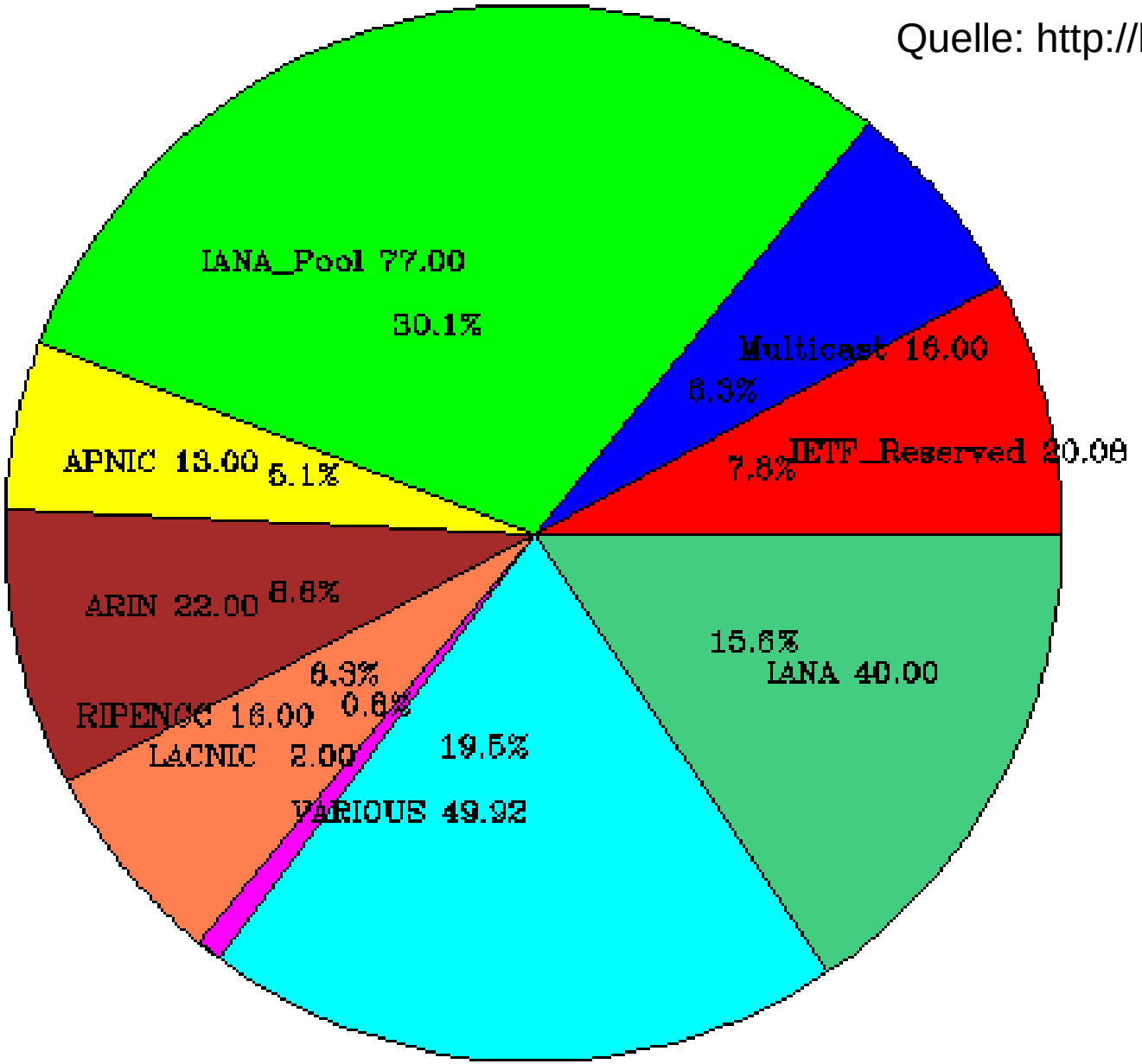
Aktive BGP-Routen



Quelle: http://bgp.potaroo.net/index-bgp.html

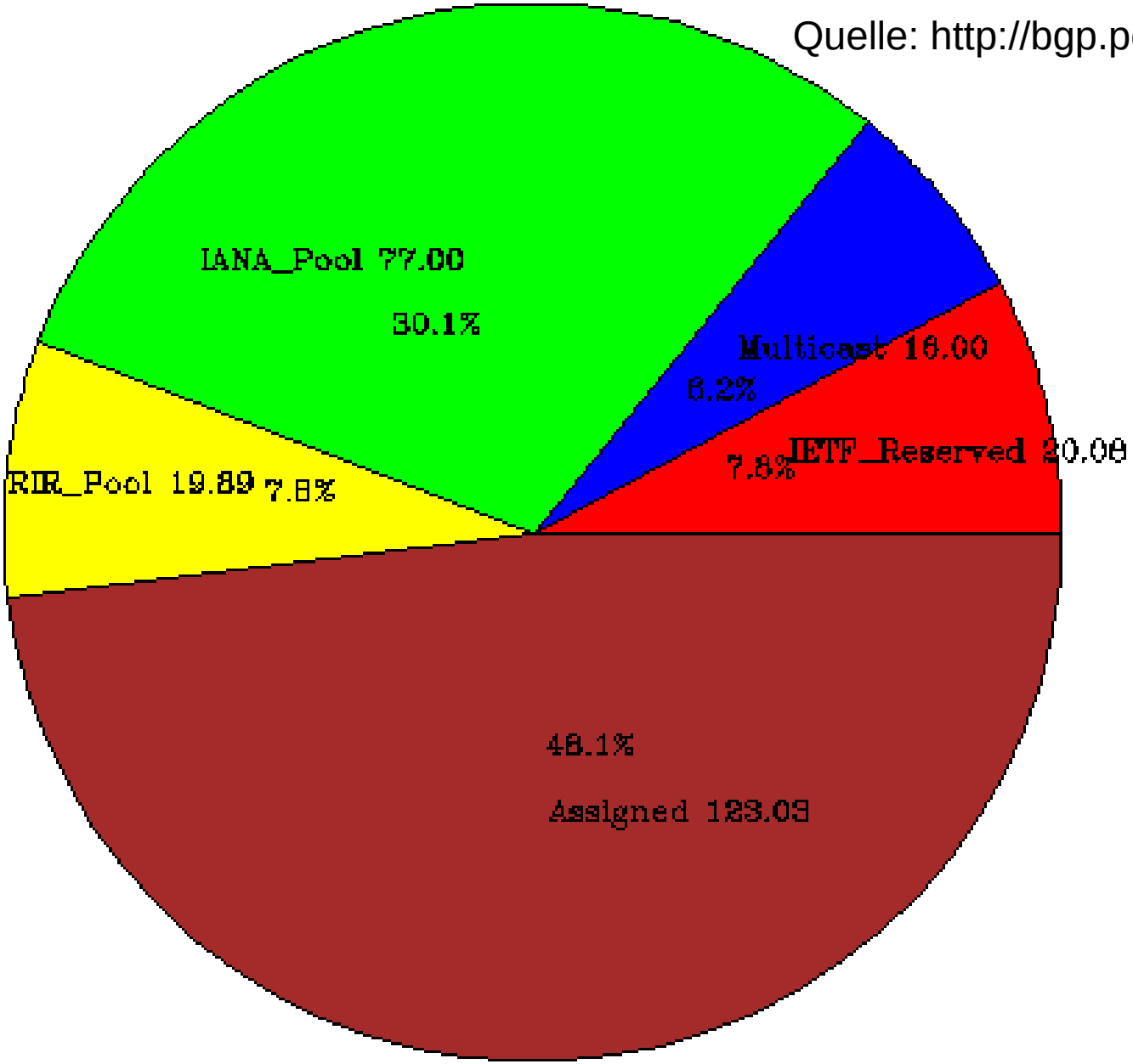
IPv4-Adreßbereich-Zuteilung der IANA

Quelle: http://bgp.potaroo.net/ipv4/

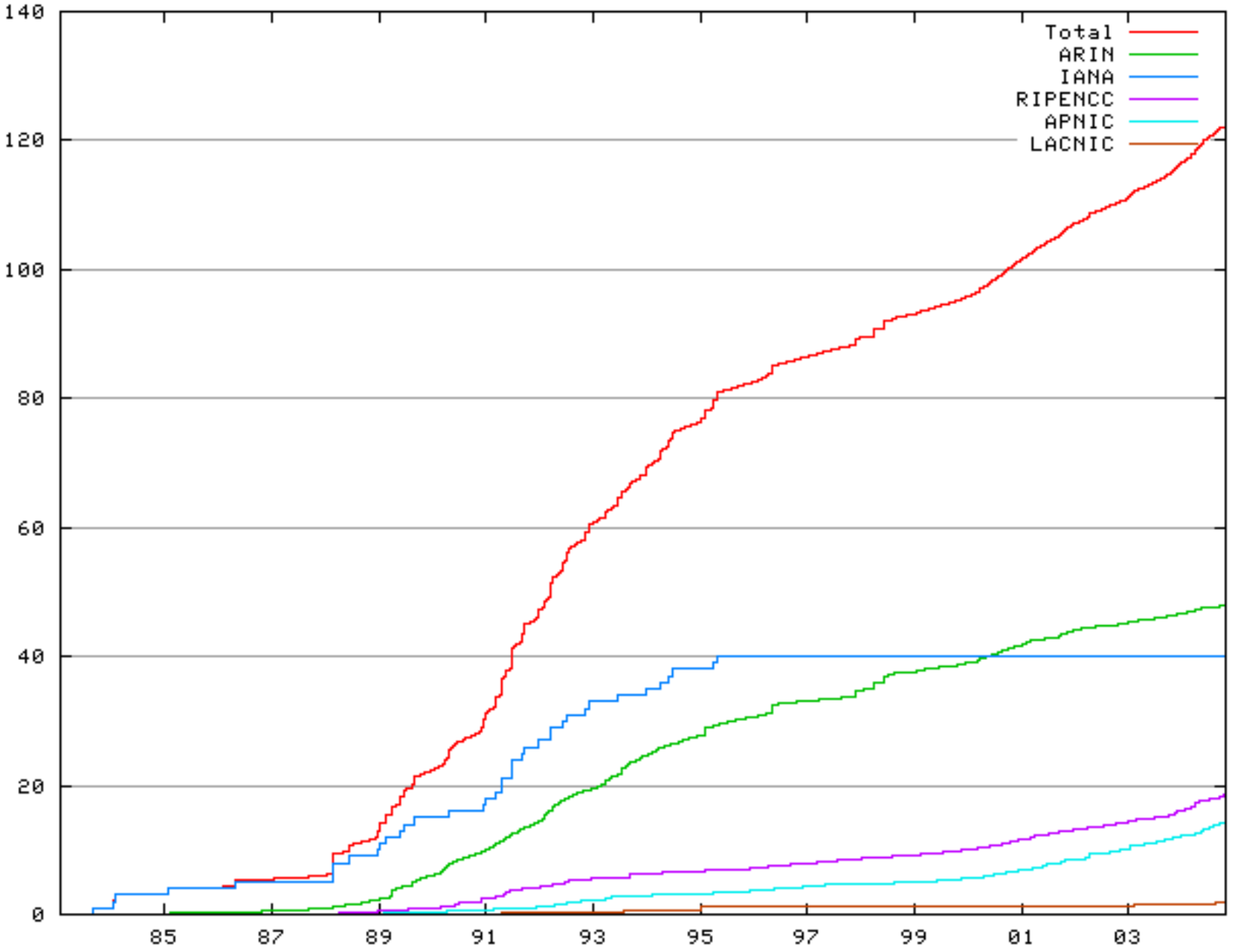


IPv4-Adreßbereich-Nutzung

Quelle: http://bgp.potaroo.net/ipv4/

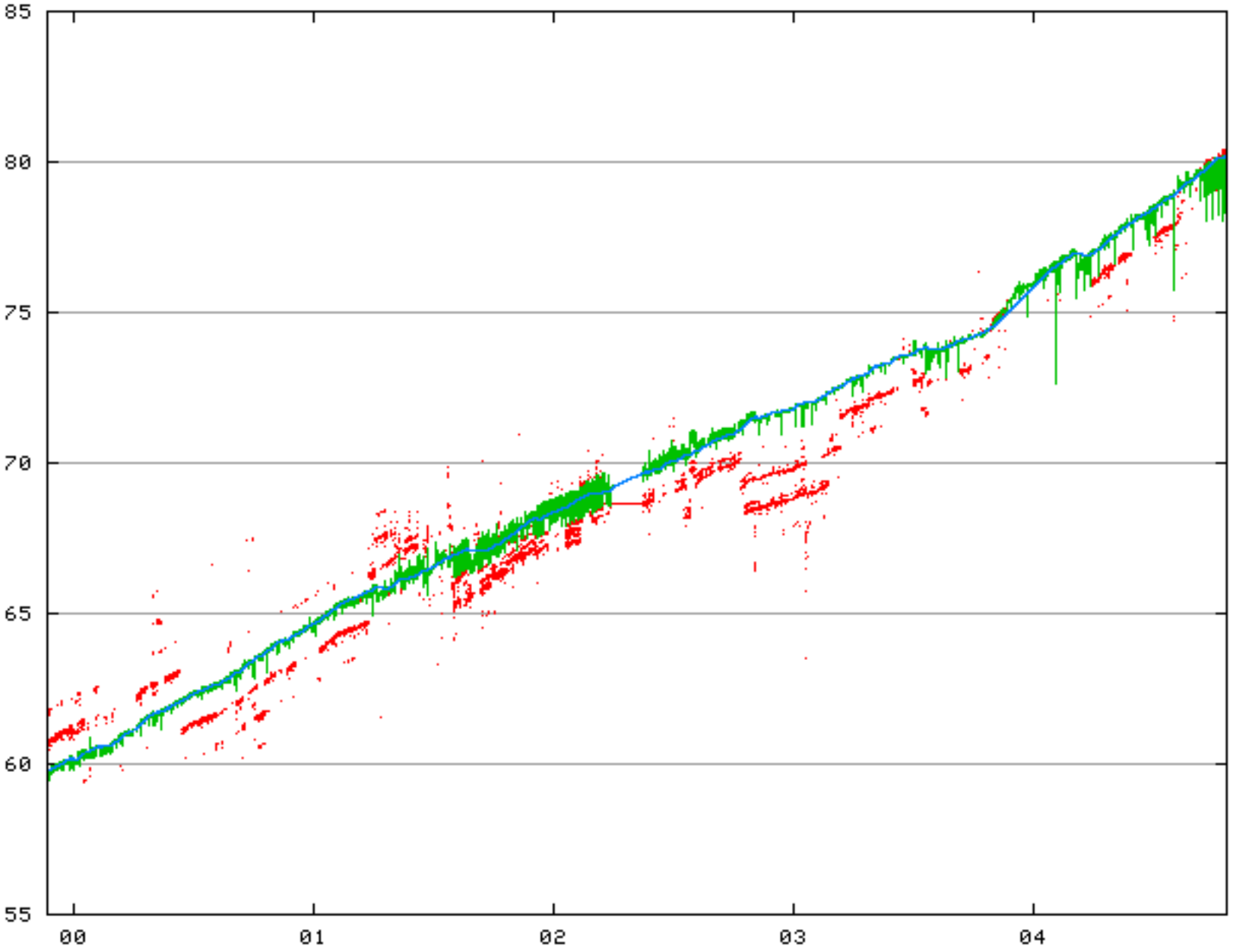


IPv4-Adreßzuweisungen seitens RIRs



Quelle: http://bgp.potaroo.net/ipv4/

Tatsächlich sichtbare IPv4-Adreßbereiche



Quelle: http://bgp.potaroo.net/ipv4/

Entstehung von IPng

- Gründung der IETF-Arbeitsgruppe ROAD (Routing and Addressing) 1990
- 1992 Vorschlag zur Migration von TCP/IP zu CLNP (ConnectionLess Network Protocol) der OSI-Gruppe
  - Hierarchisches Adreßschema entlang administrativer Hierarchien
  - Löste in der IETF massiven Protest aus
- 1993 Ausschreibung des IPv4-Nachfolgers in RFC 1550
  - Termin für Einreichung Februar 1994
  - 21 Vorschläge wurden eingereicht

Anforderungen an IPng-Vorschläge

- Skalierbarkeit
- Fehlertoleranz
- Flexibilität der Topologie
- Erweiterte Routing-Kriterien
- Datenströme und Ressourcen-Reservierung
- Unterstützung mobiler Systeme
- Sicherheit
- Zeitrahmen für Umstellung, Planung des Übergangs

Aussichtsreiche Bewerber 1994

- TUBA (TCP and UDP with Bigger Addresses)
- CATNIP (Adaptierung von OSI CLNP)
- SIPP (Simple Internet Protocol Plus)
  - Basiert auf SIP (Dezember 1992)
    - Deutliche Vereinfachung der Header-Struktur
  - Integration mit PIP (Dezember 1992)
    - Adressen dynamischer Länge
    - Unterstützung mobiler Systeme
    - Baumartiges Multicasting-Modell

Auswahl des IPng-Protokolls

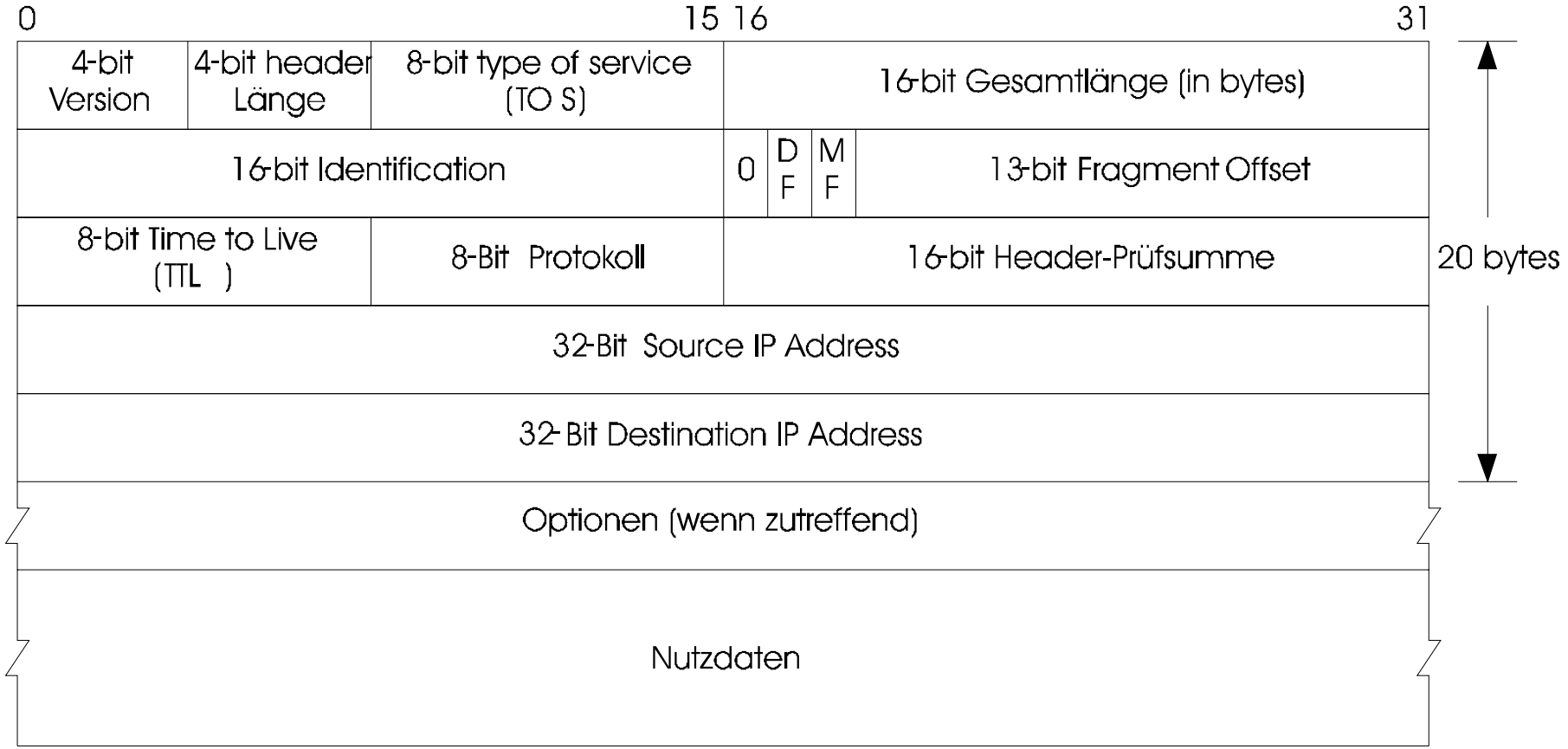
- SIPP wurde mit Änderungen (Übergangsplan, Routing-Modell) als IPv6 übernommen (RFC 1752, Januar 1995)
  - Adreßlänge 128 Bit (SIPP: 64 Bit)
  - Optionen werden ausgelagert und gruppiert
- Erste RFCs Ende 1995, Ergänzungen und Stabilisierung zu Draft Standards im August 1998

Der IPv6-Basis-Header

Version	Traffic Class	Flow Label	
Payload Length		Next Header	Hop Limit
Source Address			
Destination Address			

Zum Vergleich: v4

IP Header Version 4



Elemente des IPv6-Basis-Headers (1)

- Version (4 Bit)
- Traffic Class (8 Bit, entspricht etwa Type of Service, Precedence)
- Flow Label (20 Bit)
  - Identifikation von Datenströmen, z.B. mit festgelegter QoS
- Payload Length (16 Bit)
- Next Header (8 Bit)
  - Header-Typ, der auf den IPv6-Header folgt, entspricht etwa IPv4-“Protocol“

Elemente des IPv6-Basis-Headers (2)

- Hop Limit (8 Bit)
  - Anzahl Hops (nicht mehr Sekunden wie in IPv4)
- Source Address (128 Bit)
- Destination Address (128 Bit)
- Header ist auf 64-Bit-Ausrichtung hin optimiert
- Weitere Optionen sind nicht Bestandteil des Basis-Headers, sondern werden in Extension Headers ausgelagert
  - Ermöglicht schnelle Verarbeitung mit ASIC-basierten Routern

Extension Headers - Sequenzierung

- 1) IPv6 Basis-Header
- 2) Hop By Hop Options
- 3) Destination Options für Knoten entlang der in (4) angegebenen Route
- 4) Routing Header
- 5) Fragment Header
- 6) Authentication
- 7) Encapsulated Security Payload
- 8) Destination Options ausschließlich für den Ziel-Knoten

Generelle Optionsdaten

- Option Type
  - Bestimmt welche Aktion ein Knoten auszuführen hat, wenn Option nicht verarbeitet werden kann
    - 00 Überspringen der Option, Fortsetzung der Verarbeitung
    - 01 Verwerfen des Datagramms
    - 10 Verwerfen des Datagramms, in jedem Fall Rückmeldung eines ICMP Typ 4 Code 2
    - 11 Verwerfen des Datagramms, Rückmeldung eines ICMP Typ 4 Code 2 wenn kein Multicast-Datagramm
- Option Length (8 Bit)

Option Headers (1)

- Hop by Hop
  - Next Header (8 Bit)
  - Header Extension Length (8 Bit)
  - Optionen (variabel)
- Destination
  - Next Header (8 Bit)
  - Header Extension Length (8 Bit)
  - Optionen (variabel)
- Header (d.h. Optionsdaten) müssen immer an 64-Bit-Grenzen ausgerichtet werden.

Adressierung in IPv6

- Unicast
  - Genau ein Knoten wird angesprochen
- Multicast
  - Menge von Schnittstellen, Datagramm wird an alle Adressen versandt, die durch Multicast-Adresse identifiziert werden
- Anycast
  - Menge von Schnittstellen, Datagramm wird an gemäß Routing-Protokoll nächstliegende Adresse ausgeliefert

Adreßerzeugung: Interface Identifier

- Stateless Address Autoconfiguration ersetzt DHCP
- MACs oder Zufallszahlen werden als eindeutige Merkmale verwendet (z.B. bei Ethernet, FDDI)
  - 48 MAC-Bits werden in 64 Bits gepackt (EUI-64): OUI-Präfix gefolgt von FF:FE und Rest, Beispiel:
  - **`08:00:20:93:47:E4`** wird zu **`08:00:20:FF:FE:93:47:E4`**
- RFC 3041 erlaubt zufällige Erzeugung zum Schutz vor Identifikation anhand des eindeutigen Merkmals selbst wenn ein IEEE-Identifier vorliegt
- Resultat: Interface Identifier

Adreßerzeugung: LLA, SLA, Globale Adressen

- LLA (Link Local Address)
  - Präfix **`FE:80:00:00:00:00:00:00`**
  - Dürfen von Routern nicht weitergereicht werden
  - Jede Schnittstelle muß mindestens eine LLA besitzen
- SLA (Site Local Address)
  - Präfix **`FE:C0:00:00:00:00:00:00/46`**, 16 Bit Subnet-ID
  - Dürfen von Routern nicht weitergereicht werden
- Globale aggregierbare Adressen
  - Präfix **`0b001`**

Adressierung: Aggregierung

- Ziel der IPv6-Adressierung ist eine möglichst kleine globale Routing-Tabelle
- Hierarchie von Aggregatoren
  - Routing erfolgt aufgrund des längsten gefundenen Präfixes (wie in IPv4)
  - 13 Bits Adreßraum für Top Level Aggregation
  - 13 Bits Adreßraum für Next Level Aggregation, nur diese werden von IANA in kleinen Blocks (64 IDs) vergeben
  - 19 Bits Next-Level Aggregation Identifier
    - Werden an Organisationen vergeben

Multicast-Adressen in IPv6

- Präfix (8 Bit) 0xFF
- Flags (4 Bit) 3 MSB reserviert (0)
  - LSB=0: permanente Adresse LSB=1: vorübergehend
- Scope (4 Bit)
  - Knoten- (=1), Link- (=2), Site- (=5), Organisations- (=8), oder globale (=14) Adresse.

ICMP in IPv6

- Type (8 Bit)
- Code (8 Bit)
- Checksum (16 Bit, analog zu IP-Prüfsumme)
- Aufbau ist analog zu ICMPv4, alle Nachrichten müssen an 64-Bit Grenzen ausgerichtet sein.
- Sofern Daten zurückgeschickt werden, wird das Datagramm nur bis zur absoluten MTU (1280 Bytes) aufgefüllt

ICMPv6-Codes (1)

- Typ 1: Destination Unreachable
  - 0 Keine Route zum Zielsystem
  - 1 Kommunikation administrativ verboten
  - 2 unbelegt
  - 3 Adresse kann nicht erreicht werden
  - 4 Port kann nicht erreicht werden
- Typ 2: Packet Too Big
  - Rückgabe enthält als 32-Bit Wert die MTU auf der Route (eingehendes Interface), Anfang der verursachenden Nachricht

ICMPv6-Codes (2)

- Typ 3: Time Exceeded
  - 0: Hop Count hat bei Durchlauf den Wert 0 erreicht
  - 1: Maximalzeit für Zusammensetzung von Fragmenten überschritten
- Typ 4: Parameter Problem
  - 0: Fehlerhaftes Header-Feld
  - 1: Unbekannter Wert im Next Header Feld
  - 2: Unbekannte IPv6-Option
  - Code ist gefolgt von 32-Bit Wert, der ein Zeiger auf die Problemstelle in kopiertem Fragment der Antwort ist

ICMPv6-Codes (3)

- Typ 128: Echo Request („Ping“)
  - Nach Prüfsumme folgt ein 16 Bit Identifier, um Anfragen trennen zu können sowie weitere 16 Bit Sequenznummern für Anfragen zwischen denselben Knoten
- Typ 129: Echo Reply („Ping-Antwort“)
  - Nach Prüfsumme folgt ein 16 Bit Identifier, um Anfragen trennen zu können sowie weitere 16 Bit Sequenznummern für Anfragen zwischen denselben Knoten, jeweils unmodifiziert aus der Typ 128-Nachricht.

ICMPv6-Codes (4)

- Typ 138: Router Renumbering
  - 0: Router Renumbering Command
  - 1: Router Renumbering Result
  - 255: Sequence Number Reset
  - Erlaubt Renumerierung von Routern (bei Änderung von Adreßpräfixen, z.B. Providerwechsel, Multihoming)
  - IPSec ist bei Einsatz von RR zwingend
    - Spoofing
    - Replay Attacks

Neighborhood Discovery (1)

- Erkennung von Hosts, die an direkt angeschlossenen Interfaces erreichbar sind
  - Ersetzt ARP, ICMP RDISC, ICMP Redirect aus IPv4.
- Funktionen:
  - Router Discovery (Solicitation, Advertisement)
    - ICMP Type 133, 134
  - Prefix Discovery
    - Implizit in Router Discovery, Neighbor Discovery
      Grundlage für Routing-Entscheidungen (ohne Präfix: Default-Router), enthalten als Optionsfeld

Neighborhood Discovery (2)

- Funktionen
  - Parameter Discovery
    - Als Optionsfeld in Router, Neighbor Discovery: PMTU, Hop Limit
  - Address Autoconfiguration
    - In Router Advertisement: Stateless Autoconfig oder DHCPv6 (d.h. vorgegebene Adressen)
  - Address Resolution
    - In Neighbor Discovery (Network / Data Link)

Neighborhood Discovery (3)

- Funktionen
  - Next-Hop-Determination
    - Unterscheidung direkt erreichbar, via Router
  - Neighbor Unreachability Detection
    - Implizit in Neighbor Discovery
  - Duplicate Address Detection
    - via Neighbor Solicitation (muß 1. Nachricht sein)
  - Redirect
    - Umleitung auf günstigere (auch direkte) next hops

Neighborhood Discovery (4)

- Aber: Immer noch recht komplex und unsicher
- Neighborhood Discovery sollte zur Absicherung IPSec verwenden … aber IKE benötigt seinerseits eine gültige IPv6-Adresse für die Aushandlung von IPSec-Schlüsseln
  - Secure Neighbor Discovery (SEND) und andere Vorschläge: IETF-Arbeitsgruppe, RFC 3756 „IPv6 Neighbor Discovery Trust Models and Threats“
- Seit ca. 2003 Gegenstand intensiver Diskussionen in der IETF, Bestrebungen hin zu radikaler Vereinfachung

IPSec (1)

- Als separate RFCs definiert, besteht aus mehreren Komponenten
  - Enthalten im IP-Stack
    - Integritätsschutz/Authentisierung: Authentication Header
    - Vertraulichkeit: Encapsulated Security Payload
    - Auch unter IPv4 realisierbar, abwärtskompatibel
  - Parallel dazu
    - Mechanismen zum Austausch von Schlüsselmaterial und zur Authentisierung von Parteien mittels kryptographischer Verfahren

IPSec (2)

- Von IPSec gebotene Leistungen
  - Zugriffskontrolle
  - Schutz der Integrität von Daten
  - Schutz vor Wiedereinspielung (Replay Attacks)
  - Vertraulichkeit der Daten
  - Vertraulichkeit des Datenflußverhaltens
- Realisierungsmöglichkeiten
  - Direkte Implementierung im Stack
  - Einfügen einer Schicht auf OSI-Ebene 2 („bump in the stack“)
  - Externe Realisierung (Coprozessor, „bump in the wire“)

Security Association (SA)

- Prädikat über unidirektionale Verbindung (3-Tupel):
  - Security Parameter Index
  - IP Destination Address
  - Security Protocol Identifier
- Jede SA spezifiziert genau ein Protokoll; wenn mehrere Protokolle benötigt werden: SA-Bündel
- Wird verwaltet in der SAD (Security Association Database)

Security Policy Database (SPD)

- Spezifiziert, welche Dienste für IP-Pakete angeboten werden
  - Liste von Policy Entries, auf der vollständige Ordnung definiert ist
  - Selektoren geben an, welche SAs anzuwenden sind:
    - IP-Zieladresse
    - IP-Quelladresse
    - Name (Nutzer, DNS-Eintrag, X.500-Name,...)
    - Data Sensitivity Level (Sensitivity Label)
    - Transport Layer Protocol
    - Quell-Port
    - Ziel-Port

Security Association Database (SAD) (1)

- Enthält zu jeder SA gehörige Parameter
- Für ausgehende Pakete existieren Verweise aus SPD in SAD, wenn für einen SPD-Eintrag kein SAD-Eintrag existiert, muß er angelegt werden.
- Eingehender Datenverkehr wird einer SA zugeordnet anhand:
  - Äußerer IP-Header
  - IPSec-Protokoll
  - Security Parameter Index (SPI)

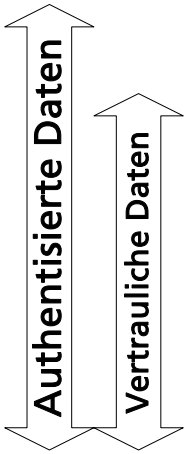
Security Association Database (SAD) (2)

- Eine SAD-Implementierung muß für jede SA verwalten
  - Sequence Number Counter (32 Bit)
  - Sequence Counter Overflow (1 Bit, Flag)
  - anti replay window (32 Bit + Bitmaske)
  - AH-Authentisierungs-Parameter (Algorithmen, Schlüssel,...)
  - ESP-Verschlüsselungs-Parameter (Algorithmen, Schlüssel,...)
  - ESP-Authentisierungs-Parameter (Algorithmen, Schlüssel,...)
  - Lebensdauer der SA (Zeit, Datenvolumen, Zertifikate)
  - Modus (Tunnel, Transport mode)
  - Path MTU

Encapsulated Security Payload

- Extension Header-Format

Security Parameters Index (SPI)		
Sequence Number Field		
Payload Data (variable Länge)		
Padding (0-255 Bytes)	Padding Länge	Next Header
Payload Data (variable Länge)		



Authentication Header

- Extension Header-Format

Next Header	Payload Length	RESERVIERT
Security Parameters Index (SPI)		
Sequence Number Field		
Authentication Data (variable Länge)		

Mobile IPv6

- Derzeit noch im Internet-Draft-Status
- Unterstützung von Hosts, die sowohl unter einer (semi)permanenten als auch temporären lokalen Adresse erreichbar sein sollen.
- Weiterentwicklung von Mobile IPv4, RFC 2002/RFC3344 deutlich eleganter
- Definiert eine Reihe von neuen Destination Options und ICMP-Typen und Modifikationen an Optionen
  - müssen von allen Hosts unterstützt werden
  - problematisch durch umfangreiche Semantik

Optionen in Mobile IPv6

- Home Address
  - Mobiler Knoten verwendet „care-of address“, eigentliche „home address“ ist in Destination Option vermerkt
  - Transparente Handhabung des Transports zum Heimatnetz
  - „home agent“ sorgt für eingekapselte Weiterreichung/redirect zu „care-of address“
- Binding Update/Binding Acknowledgment
  - Mobiler Knoten sendet neue „care-of address“
- Binding Request
  - Aufforderung eines mobilen Knotens zum erneuten binding

ICMP-Erweiterungen in Mobile IPv6

- Home Agent Address Discovery Request
  - Suche eines mobilen Knotens nach einer Liste von „home agent“-Routern
  - Quelle ist aktuelle „care-of address“
  - Ziel ist „Mobile IPv6 Home Agents“-Anycast-Adresse im Präfix des Heimatnetzes
- Home Agent Address Discovery Reply
  - Liefert als Antwort eine Liste von Routern, die als „home agent“ operieren können

Erweiterungen des Domain Name System

- RFC 1886: AAAA (deprecated)
  - neuer Record-Typ im DNS
  - Adressen im RFC 1884-Format
  - IP6.INT-Lookup-Domain
- RFC 2874: A6
  - A6-Format, Unterstützung für Umleitung (z.B. Prefix Delegation)
  - IP6.ARPA-Lookup-Domain
  - DNAME-Records zur Umleitung anstelle von NS-Einträgen für IPv4
  - Strukturierte Records für IPv6-Adressen
    - Unterstützt Multi-Homing mit Record-Ketten
  - AAAA-Records können automatisch erzeugt werden: AAAA wird leider noch oft benutzt...

API-Anpassungen

- Notwendigkeit der Ergänzung von Datenstrukturen und neuer Leistungsmerkmale in APIs
  - Primär BSD-Sockets, mit Modifikationen auch unter Win32 etc. - SVR4 TLI spielt de facto kaum eine Rolle
- Basic Sockets API in RFC 3493 (war: RFC 2553,2133)
  - Adreßdatenstrukturen, Adreßumsetzungen, ansonsten kaum Änderungen
  - Dennoch: Anpassungen sind nicht immer einfach, ein „`int`“ kann leider ein Schleifenzähler oder eine IPv4-Adresse sein…
- Advanced Sockets API (RFC 3542, war RFC 2292)
  - Zugriff auf Interna wie Raw Sockets, Header-Daten

Existierende Implementierungen (Beispiele)

- Digital/Compaq OpenVMS, Tru64 Unix
- Sun Solaris (IPSec aus rechtlichen Gründen separat)
- Free/Open/NetBSD, BSDI: KAME
- Hewlett-Packard HP-UX
- IBM AIX, OS/390
- Linux
- Microsoft Windows (ab XP SP1, 2003 Server)
- Cisco IOS (Seit 12.3 (S/T))

Anwendungen und Migration

- *„IPv6 ist das Protokoll der Zukunft und wird es auch noch ein paar Jahre bleiben“*
- Derzeit schon im Carrier-Backend im Einsatz (z.B. auch für UMTS, UWB)
- Anforderungen seitens Bundeswehr, DoD, etc. für integrierte universelle Vernetzung bis hin zu Sensoren und Funkgeräten
- Kosten für Umrüstung (Hardware, IPv6/v4-Gateways, Software-Anpassung)… meist noch geringer Leidensdruck