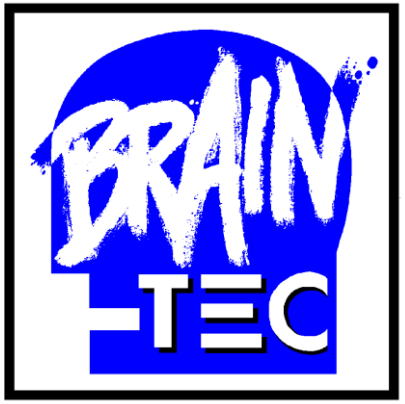


IPv6 – Historical Overview and Technical Introduction

European Conference on Applied IPv6

Köln

29. 06. 2004

Content

- History
- Who is behind IPv6
- Addresses for IP
- IPv6 - Basics
- Addresses
- Address Distribution
- Header
- Optional Headers
- ICMPv6
- Auto-Configuration
- DHCPv6
- DNS
- TCP and UDP
- Multicast and Routing
- RFCs and Links

IPv6 Tutorial

- History

Why a new IP?

- We are running out of addresses (are we really?)
- Size of routing tables explodes
- More security is requested
- Plug & play-installation
- Easier renumbering would be nice
- Quality of Service
- Other new Applications (where?)

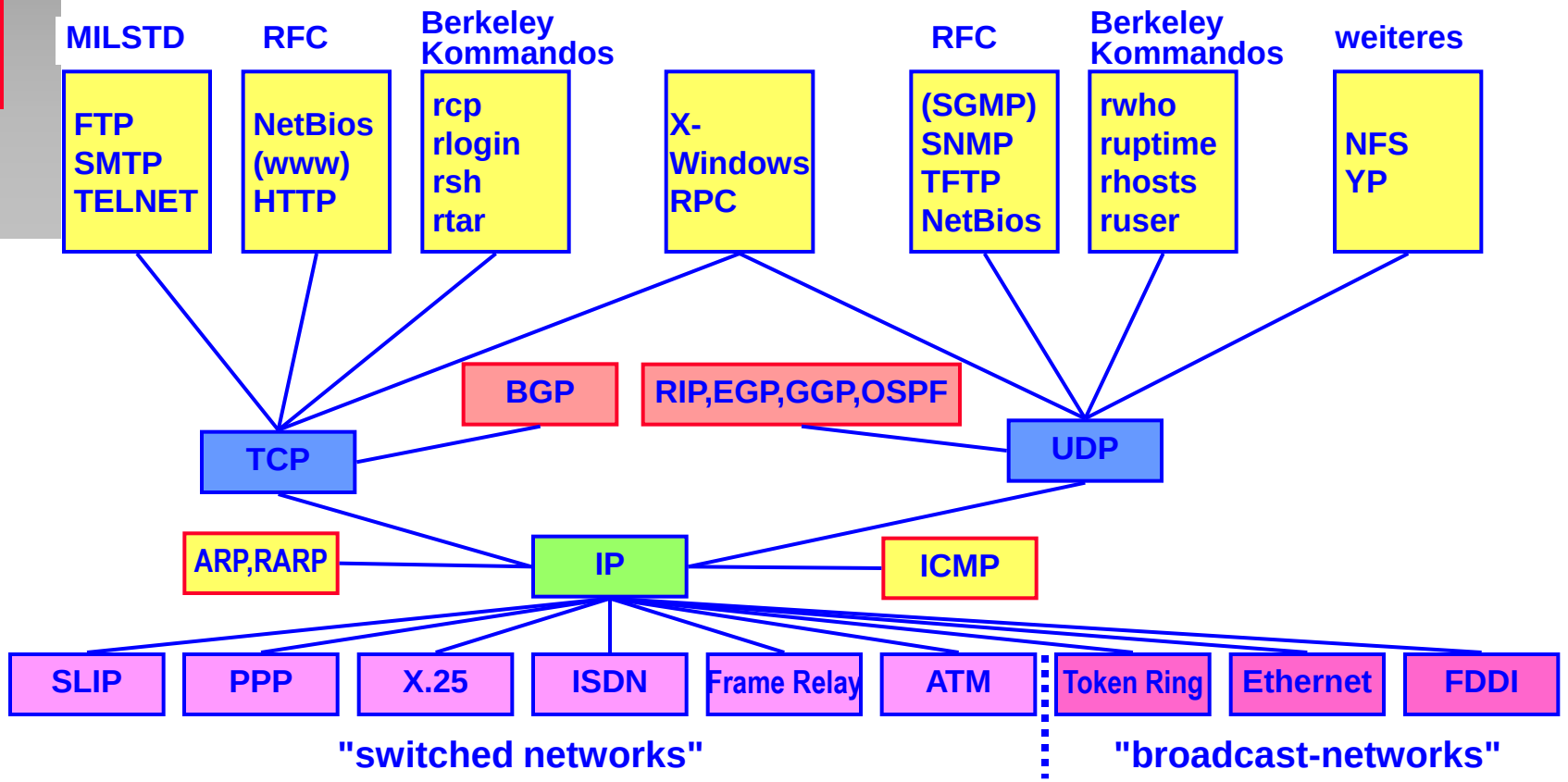
What happened with IPv5?

0–3		never used
4	IPv4	
5	ST	Stream Protocol, not a new IP
6	IPv6	used by SIP, SIPP
7	CATNIP	sometimes called IPv7 or, TP/IX; not in use anymore
8	PIP	not in use anymore
9	TUBA	not in use anymore
10-15		not yet assigned

When did it start?

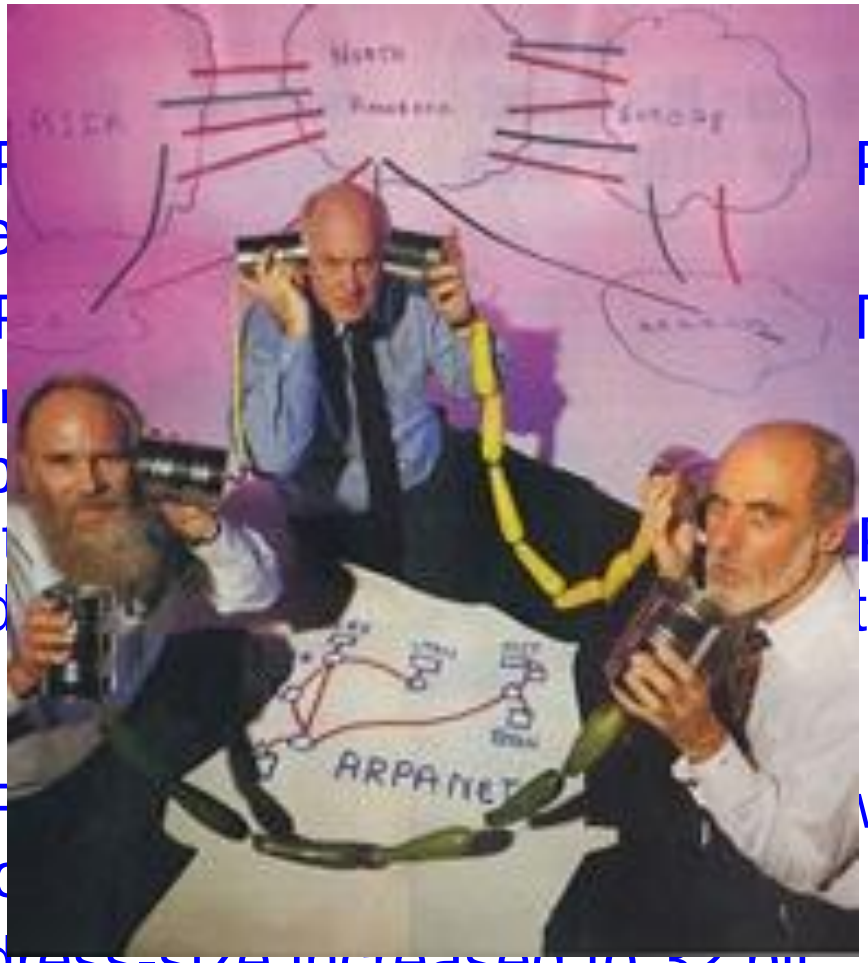
- IETF starting several projects 1991
- SIP, CATNIP, PIP and TUBA
  - IPng
  - IPv6
- Address-length 64,128, 256 or variable
- IETF recommendation of IPng area directors in 1994 called for setup of IPng working group 1995
- features, features and more features
- long discussion

What is affected?



History of the Internet

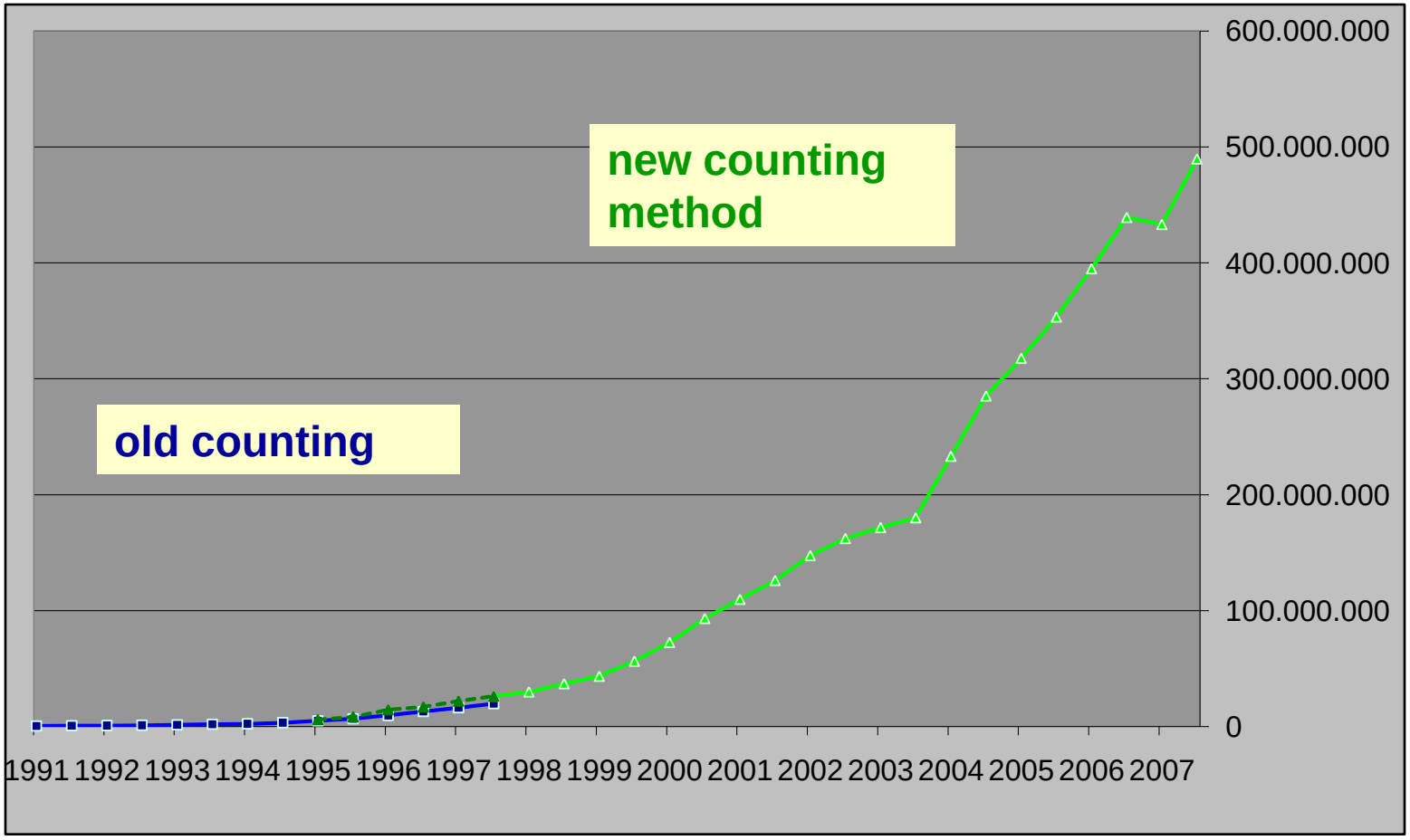
- 1969:
  - ARP Projects Age
  - ARP Twork.
  - Wor Sep Pro Program Add ts
- 1982:
  - TCP vere intro
  - Address-size increased to 32 bit



History

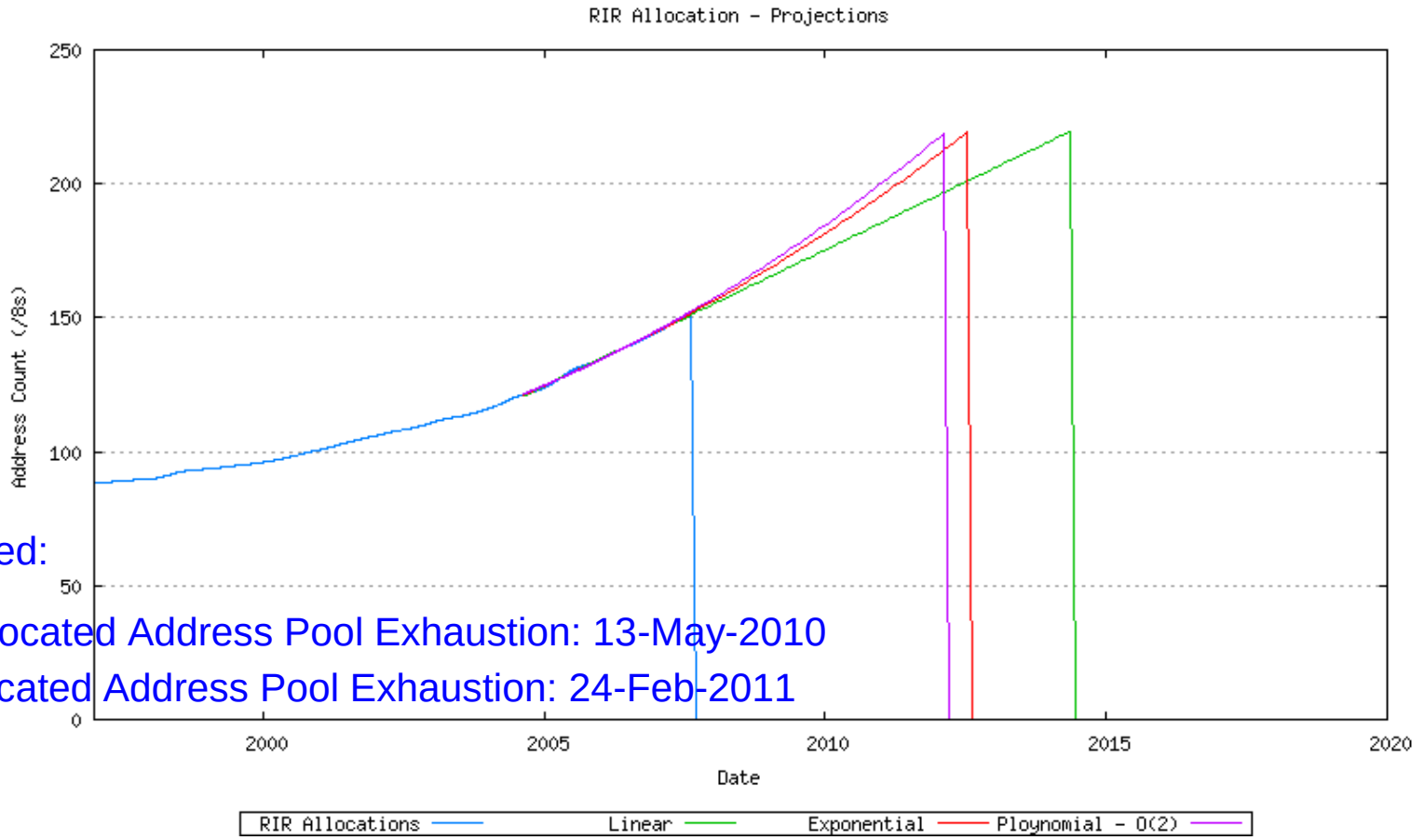
- 2007: counting more than 490 millions of hosts visible in the Internet
  - more than 11,1 millions of domains in Germany using .de
  - more than 72,5 millions using .com
  - the Internet is everywhere
  - IP-Addresses are requested for everything:
    - Computer
    - Machines
    - Telephones
    - Portable Devices
    - Cars
    - … … ..

Internet Hosts 1995-2004



Source: ISC

Usage of IPv4 Addresses



Projected:

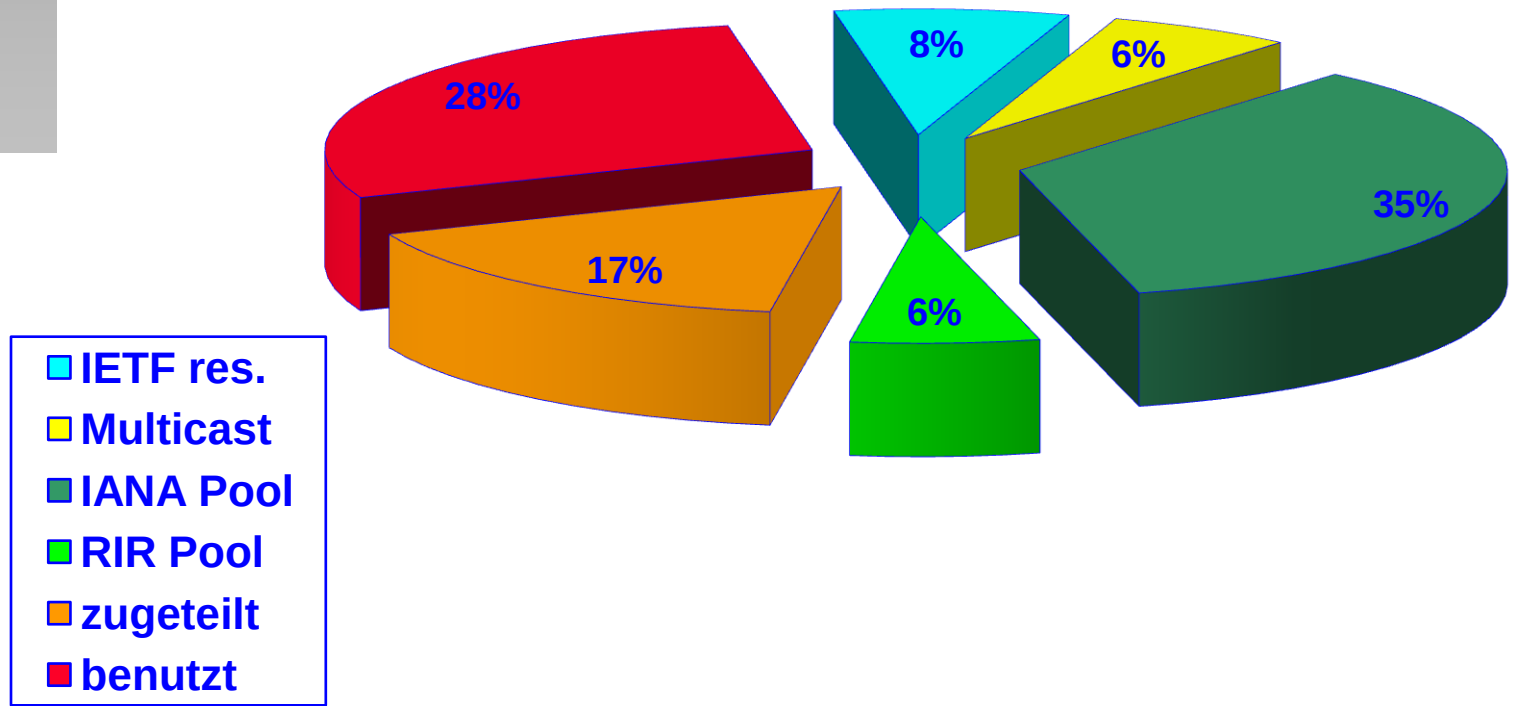
IANA Unallocated Address Pool Exhaustion: 13-May-2010

RIR Unallocated Address Pool Exhaustion: 24-Feb-2011

(Jeoff Houston http://bgp.potaroo.net/)

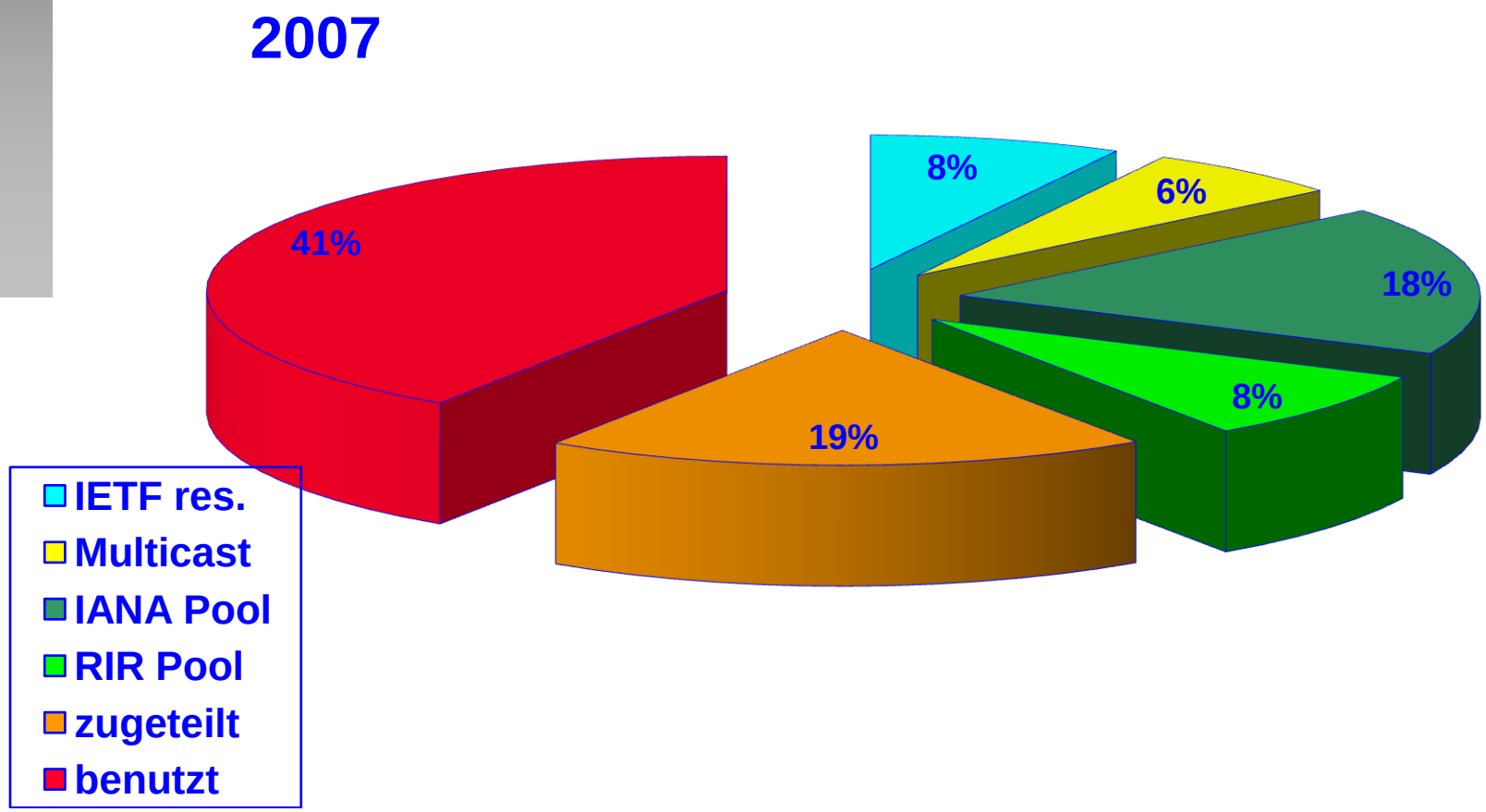
Usage of IPv4-Addresses

2003



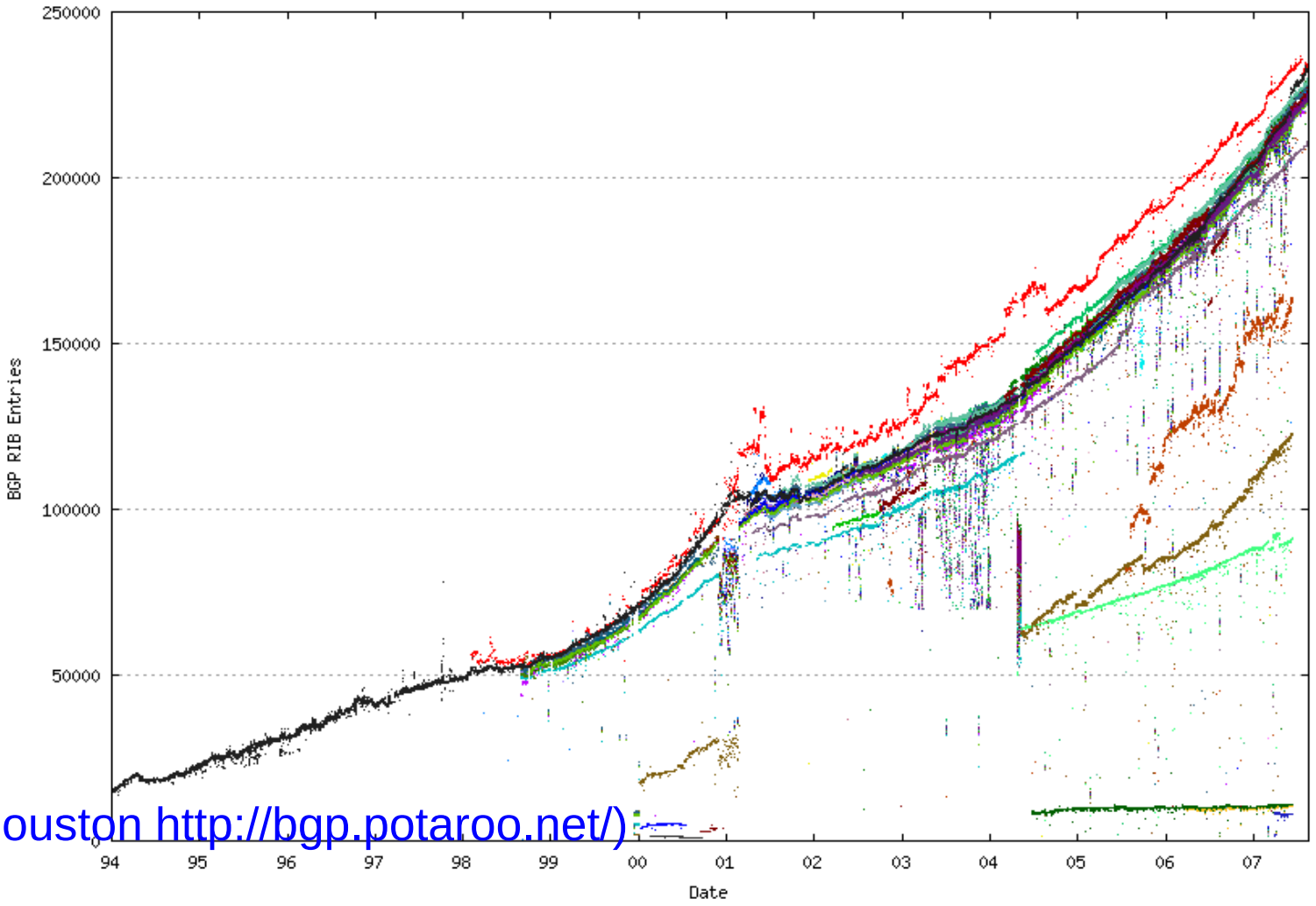
(Quelle: Geoff Houston http://bgp.potaroo.net/)

Usage of IPv4-Addresses



(Quelle: Geoff Houston http://bgp.potaroo.net/)

Increase in BGP-Routes



(Jeoff Houston http://bgp.potaroo.net/)

IPv6 Tutorial

- Who is behind IPv6

Who is the IETF?

- Internet Engineering Task Force
- Start 1986
- Independent, not run by governments
- Open for everyone
- International audience
- Contributions from different sources
  - Science and Research
  - Manufacturer of HW
  - Manufacturer of SW
  - Provider
  - Carrier
  - User
  - Government

Working principles

- Basic rule: Consensus
- Discussions until all technical questions and open points are resolved
- Everything is public
  - use of public mailing lists
- D. Clark 1992 about the IETF:
  - „We believe in rough consensus and running code“
  - „We reject kings, presidents and voting“
- J. Postel 1982:
  - „Be liberal in what you accept, and conservative in what you send."

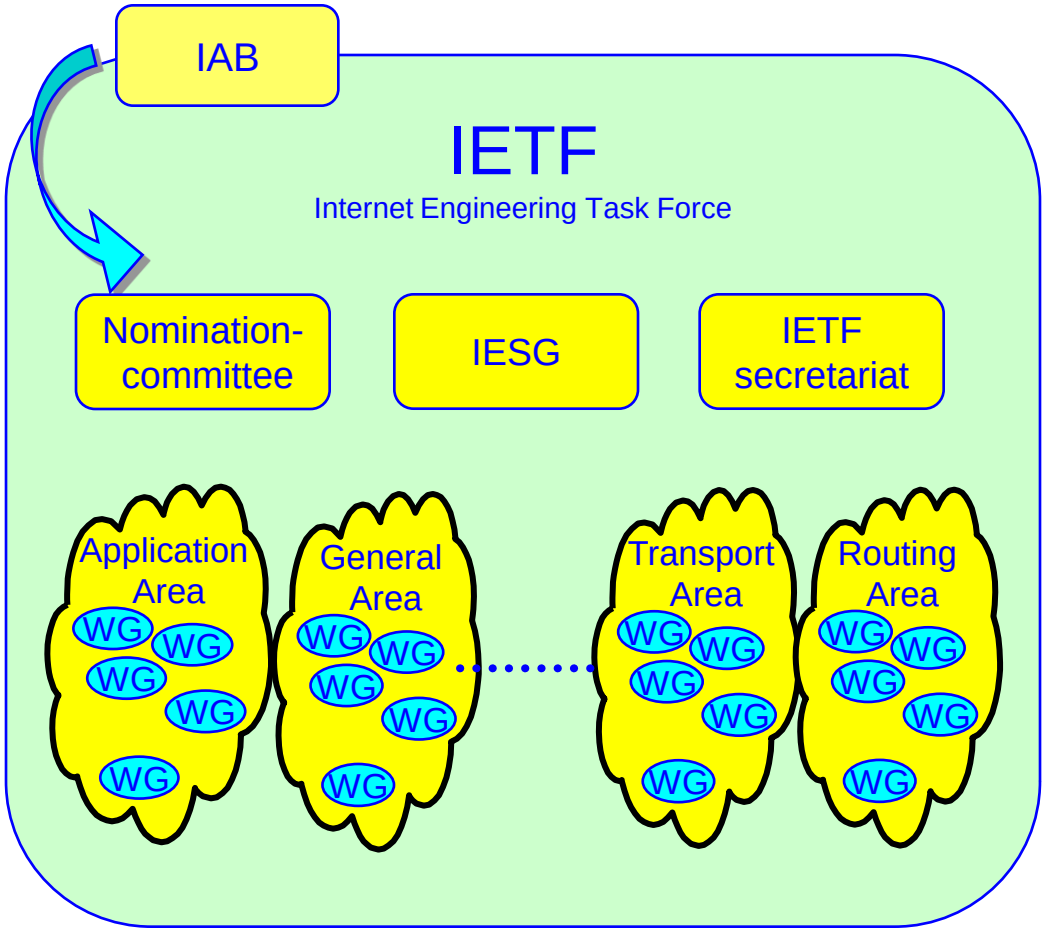
The Output of the IETF

- Internet Standards
- Documents:
  - Drafts
  - RFCs
    - Internet Standard
    - Recommendation (BCP - Best Current Practice)
    - Informative (FYI - For Your Information)

Structure of the IETF

Areas doing work in:

- Applications Area
- General Area
- Internet Area
- Operations & Management Area
- Routing Area
- Security Area
- Transport Area
- Real-time Applications & Infrastructure Area



IPv6 Tutorial

- Addresses

IPv6 – Address-Architecture

- IPv6 addresses have a fixed length of 16 bytes
- Size of addresses covered by IPv6:
  - 128 bit that is:
  - 340.282.366.920.928.463.463.374.607.431.768.211.456 addresses
  - nearly 665.570.793.348.866.943.898.599 addresses per m² of the earth
  - over 665 billiards (European! = 665 quadrillions US) addresses per mm²
  - even if addresses are used as badly as IPv4-addresses were used, more than 1.500 IPv6-addresses are available for each m² of the earth (source: Christian Huitema)

IPv6 – Address Overview

- Addresses are written using a hexadecimal notation in 16 bit groups divided by colons “ : “
- leading zeroes in each group my be omitted
- Exactly one sequence of zeroes may be replaced by the shortcut “::”

- Examples:
  - 2001:DB80:2341:AB12:654F:0800:200C:F17A
  - 2001:DB80:0:0:0:800:200C:F17A
  - 2001:DB80::800:200C:F17A

- Prefix is used to indicate the network part:
  - 2001:DB80::/32
  - 2001:DB80:2241:1231::/64
  - 2001:DB80:1231:0:0:0:0:0/48

Types of IPv6 Addresses

- Addressing modes:
  - unicast — directed to one node
    - global
    - link-local
    - ~~site-local~~ — site-locals are removed from all standards
  - anycast — to the first (nearest) node of a group sharing one prefix (used in MOBILEIP)
  - multicast — to all in a group

  - an interface has always a link-local unicast address
  - an interface has always one or more multicast addresses
  - an interface may have several global addresses

  additional hint:
  - IPv6 has no broadcast-addresses . This function from IPv4 was completely replaced by multicast

Usage of IP - Addresses

- IPv6 - addresses are supposed to identify interfaces and not nodes
  - a node (computer) may be identified by any of its interfaces
- IPv6 unicast addresses are unique for each interface
- one interface may have as many unicast addresses as needed
  - in a multi-homed network, an interface has a unique global IPv6-address for each upstream connection
  - every interface has an automatically defined link-local address
- Exceptions:
  - in a load sharing environment a single IPv6-address may be used to identify several physical interfaces which shall be presented as “one” interface to the next layer
  - router may use interfaces without IPv6-addresses on unnumbered point-to-point links

IPv6 - Addresstypes

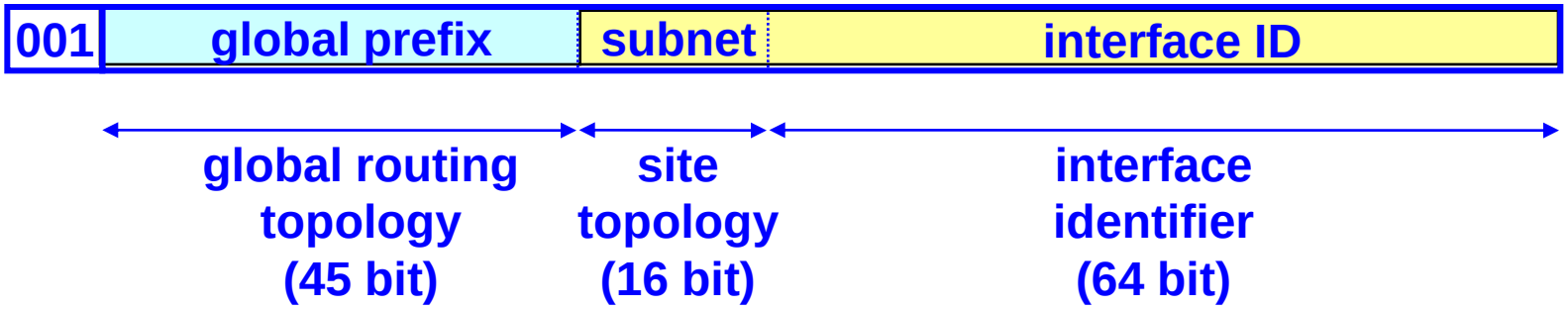
- using the first bits the format prefix (FP) defines the usage of the IPv6-address
- 0000 0000 — special usage
  - ::/128 — unspecified address
  - ::1/128 — loopback
- 1111 1110 10 — FE80::/10 — link-local
- 1111 1111 — FF00::/8 — multicast:
  - all nodes — in a node: FF01::1 — on a link: FF02::1
  - all routers — in a node: FF01::2 — on a link: FF02::2
  - 8 bits used for flags and scope
- all others — unicast as defined by IANA
- 001 — this is the FP used by all IPv6-unicast-addresses available at the moment now
  other FP may be used in future
- 0000 001 — reserved for NSAP addressing

IPv6 - Addresses

- Scope
  if several addresses may be in conflict (like FF02::1 all nodes on this link on a machine with several links) an additional zone identifier may be added:
  - FF01::1%1 means all nodes on all links with the manually defined zone value 1 and FF01::1%23 means all nodes in zone 23

- private addresses
  - FC00::/7 proposed solution for unique local addresses
  - 7 bit FP
  - FC00::/8 using a 40 bit centrally allocated global identifier
  - FD00::/8 using a 40 bit locally defined identifier
  - 16 bit subnet
  - 64 bit interface ID

Global Unicast Addresses



- alle fields are variable
- global prefix are given out in chunks from IANA to the RIRs
- RIRs give prefixes to providers, exchanges and carriers
- field delimiter between global prefix an subnet is variable and defined by RIR policy
- delimiter between subnet and interface is up to the user and/or implementer of software

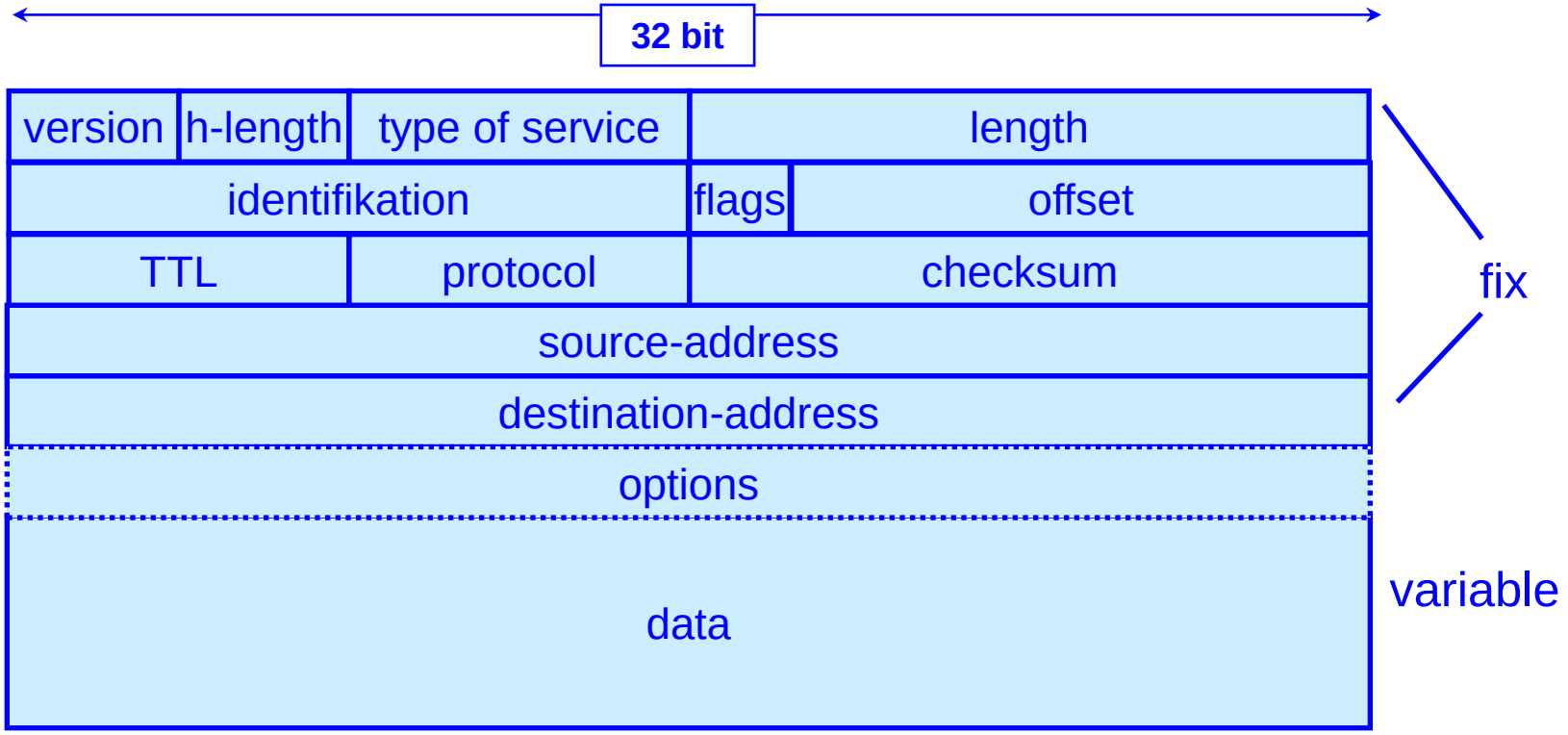
Interface IDs

- the lower 64 bit of an IPv6-address may be defined using several methods:
  - automatically by auto-configuration computing the 64 bit of the ID from the 48 bit MAC-address as described in EUI-64
  - automatically from a DHCP-server, either using EUI-64 identifier or preset values from the network manager
  - manually defined at the node
  - generated at system-start (or triggered by time, data volume or manual trigger) using a random (pseudo-random) 64 bit value (for privacy reasons in dial-up situations)
  - other methods are up to the wild dreams of system designers

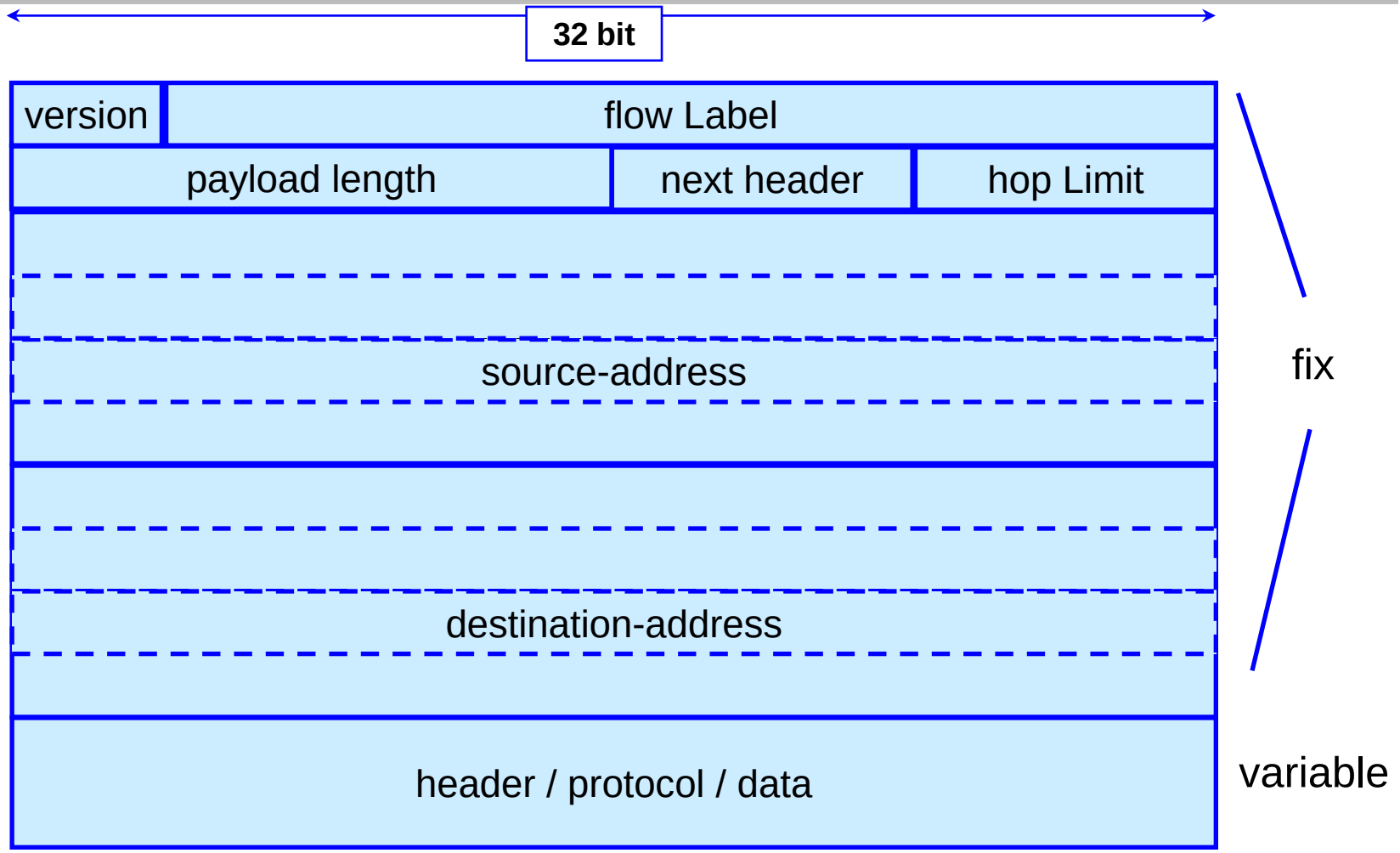
IPv6 – Tutorial

- Header

IPv4 Header Format



IPv6 Header


32 bit
version
flow Label
payload length
next header
hop Limit
source-address
destination-address
header / protocol / data
fix
variable

IPv6 - Header

field	size	content
version	4 bit	version (always = 6)
flow Label.	28 bit	define packets in one stream or flow of data

- usage and format of flow label is still under discussion
- several groups (DIFFSERV, INTSERV) define usage possibilities of the flow label
- flow labels may either be unchanged from end-to-end or may be interpreted and changed on a hop-by-hop base

IPv6 - Header

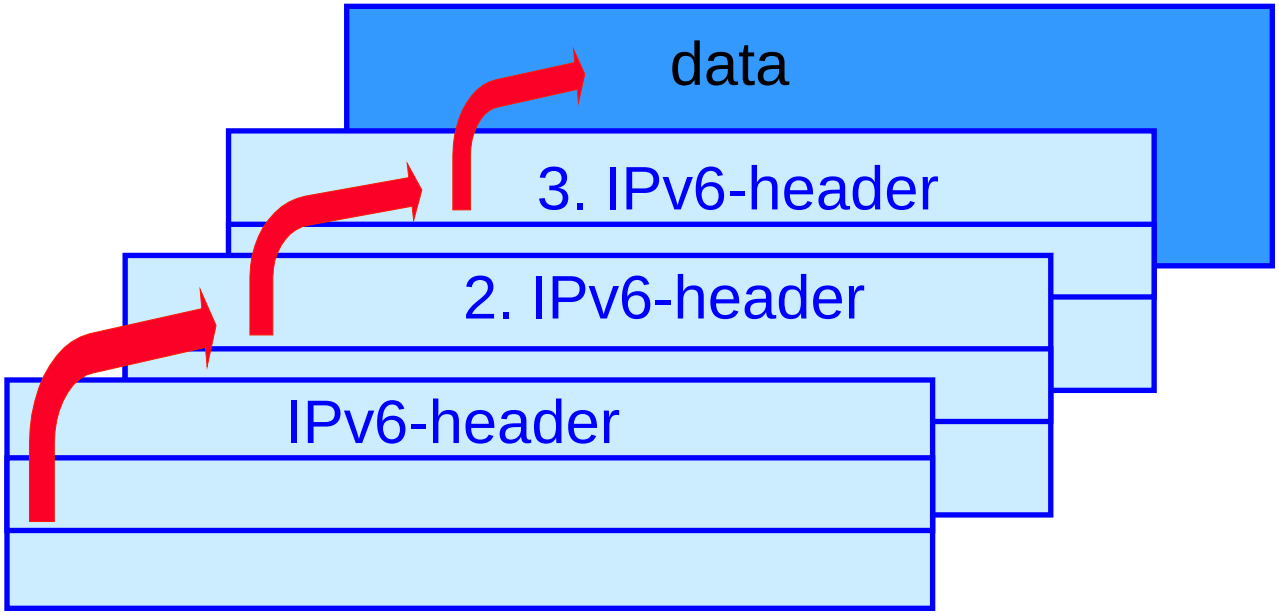
field	size	content
hop limit	8 bit	= IPv4 TTL decremented by each router packet discarded if counter reaches zero in transit
source address	128 bit	address of sender
destination address	128 bit	address of the destination of the packet. May be only the address of the next hop, if an explicit route is defined by a routing-option-header

IPv6 - Header

field	size	content
payload length	16 bit	length of the data section following all IPv6-headers counted in octets, if set to zero the Jumbo-Packet-Option is used to define values larger than 64 k bytes.
next header	8 bit	header-type of the following IPv6-header this may be another option-header or a protocol header like TCP all values defined for IPv4 may be used, additional IPv6-secific values are defined

IPv6 - Header - Linkage

The field “next header“ defines the chaining of one or several option-headers between them main IPv6-header and the final data part.



Header-Types

0	IPv6 hop-by-hop-options
60	IPv6 destination-options
43	IPv6 header for routing
44	IPv6 header for fragmentation
51	header for authentication (IPSEC)
50	header for encryption (IPSEC)
59	IPv6 no more header
1	ICMP (Internet Control Message Protocol)
4	IPv4-data in a IPv6-tunnel
6	TCP (Transmission Control Protocol)
17	UDP (User Datagram Protocol)
41	IPv6-data in a tunnel

Header-Ordering

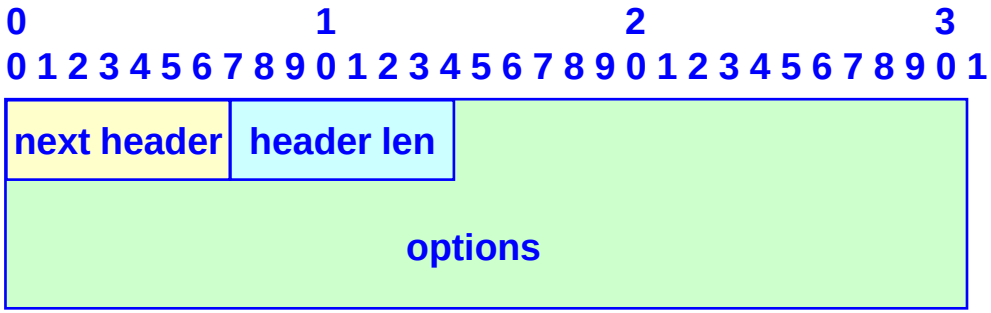
IPv6-Basis-header
Hop-by-Hop-options (0)
destination-options (60) for any router
Header for routing (43)
Header for fragmentation (44)
Header for authentication (51)
Header for encryption (50)
destination-options (60) for receiving end-node
TCP / UDP / other payload data

IPv6 – Tutorial

- Optional Headers

Hop-by-Hop Option Header

- carries optional information
- indicated by next header = 0 in previous header
- is read and interpreted by any node passed by this packet



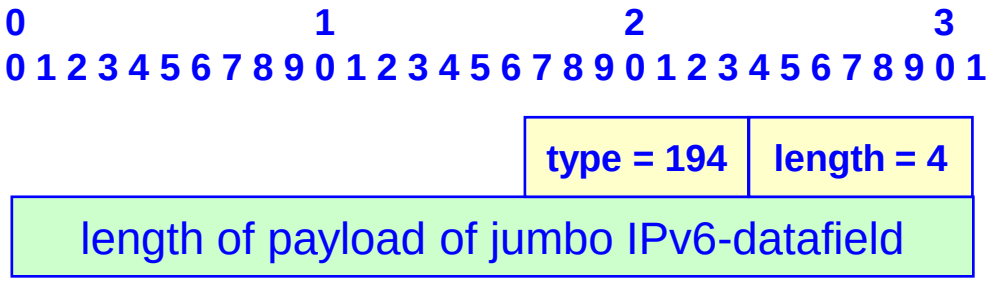
- next header — type of the following header (another IPv6 – option-header or next protocol like TCP or UDP)
- header len — length of this header counted in chunks of 8 octets
- options — one or more fields coded as TLV (type-length-value) to carry the optional parameters

Type of IPv6-Options

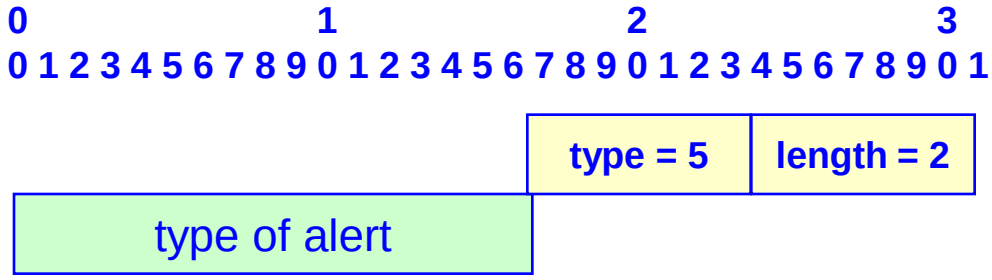
- 2 bit action
  - 00 ignore unknown option
  - 01 ignore whole packet with unknown option
  - 10 ignore whole packet with unknown option and send ICMP-error
  - 11 ignore whole packet with unknown option and send ICMP-error if destination is a unicast-address
- 1 bit change
  - 0 – no change during transit allowed
  - 1 – may be changed during transit
- 5 bit option number
  - defines desired function

Hop-by-Hop Options

- jumbo-payload
  - enables Packets carrying up to 2^128 (= 4.294.967.295) bytes



- router-alert
  - example: triggers router to read additional options



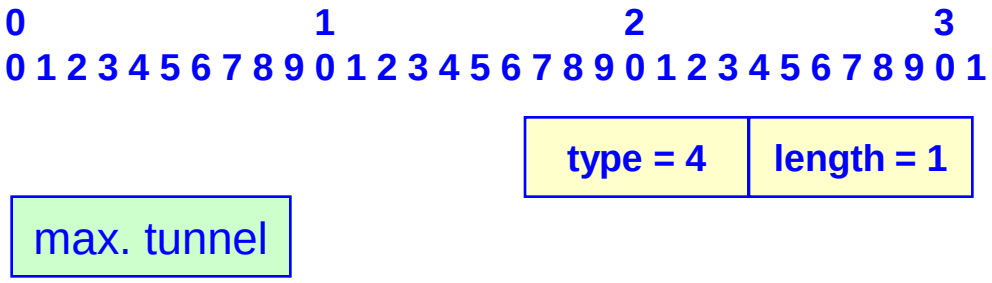
End-to-End Option Header

- carries optional information to last node
- is only read by the final destination node
- is indicated by type 60 (0x3C) in the next header field
- uses the same format as the hop-by-hop option header

There were no options defined in the base standard. First usage was with automatic setup of tunnels and options are defined there.
MOBILEIP defines several more options using this format.

Destination Options

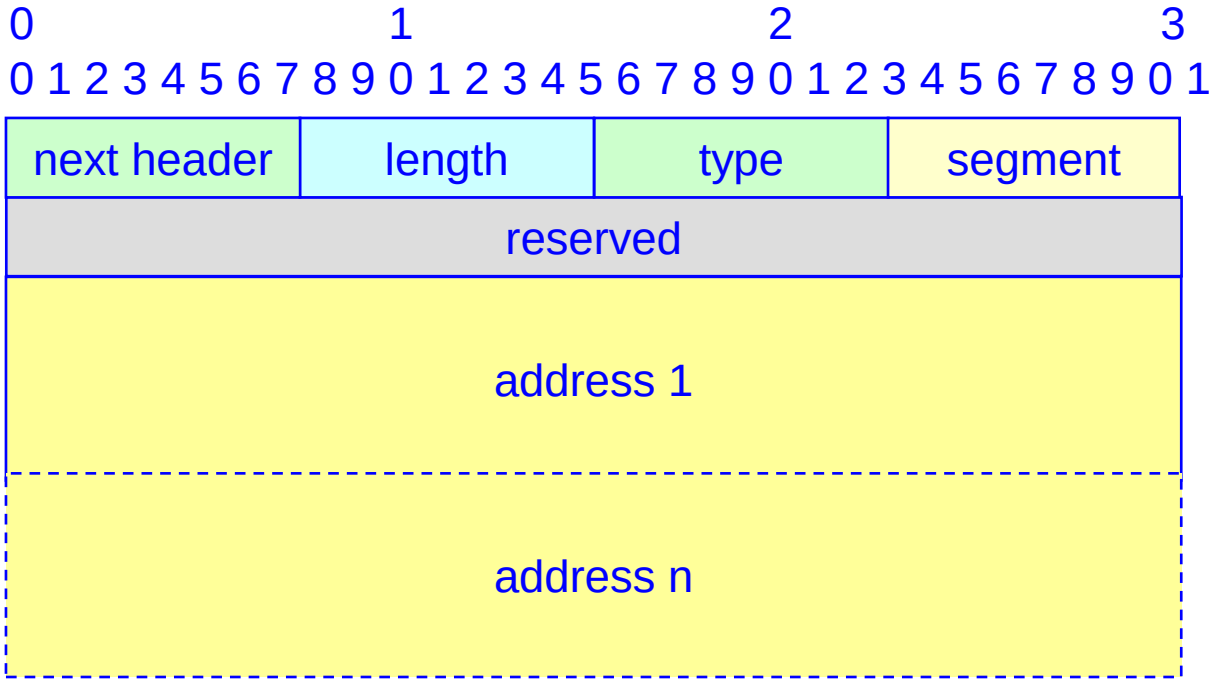
- maximum number of encapsulation recursions for a tunnel



- more options for MOBILEIP
  - 198 - Binding Update
  - 7 - Binding Acknowledgment
  - 8 - Binding Request
  - 201 - Home Address

Routing Header

- carries a list of nodes which shall be used to forward the packet
- is announced using protocol id 43 in the next-header field
- is designed to implement SDRP (source Demand Routing Protocol)
- replaces old source routing options from IPv4



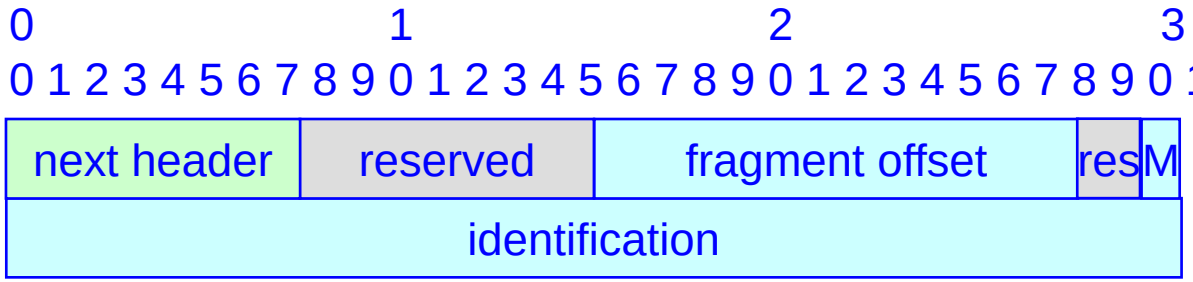
Routing Header

field	size	content
next header	8 bit	type of next header in chain
length	8 bit	length of header using 8-octet-groups not counting the header self so one route -> 2, 2 routes -> 4 …
type	8 bit	set to zero (for later extensions)
reserved	32 bit	not used in this revision
segment	8 bit	index pointing to the next field in the list of routes which shall be used. The routes are used from last to first, so the index may be as well taken as counter of routes which are still to be used
route	128 bit	list of IPv6-addresses which define the path for this packet

Whenever a node finds a routing header holding its own address, the segment count is decremented and the destination address switches places with the address from the routing header pointed by segment

Fragmentation Header

- is used to indicate payloads larger than the allowed MTU on the used transport path
- fragmentation is only allowed at the sending node
- fragmentation on the path, as used with IPv4 is no longer possible

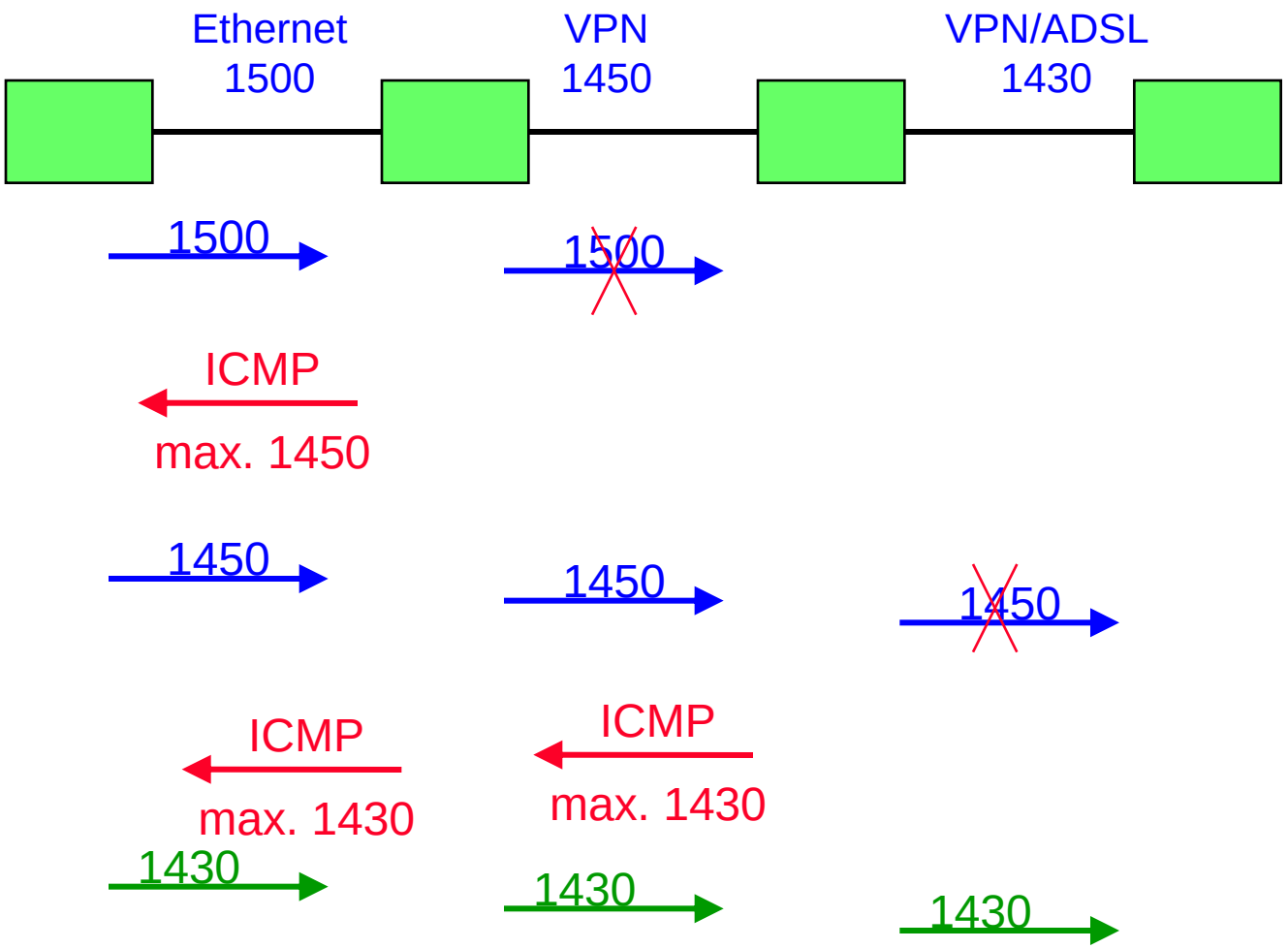


field	size	content
next header	8 bit	type of the following header
reserved	8+2 bit	not used – set to zero
fragment offset	13 bit	the position of this payload counting from the initial start of the original payload using units of 8 octets
M flag	1 bit	1 = more fragments to follow, 0 = last fragment
identification	32 bit	is a unique identifier used by the final destination to identify all fragments from a single packet

Selection of Packetsize

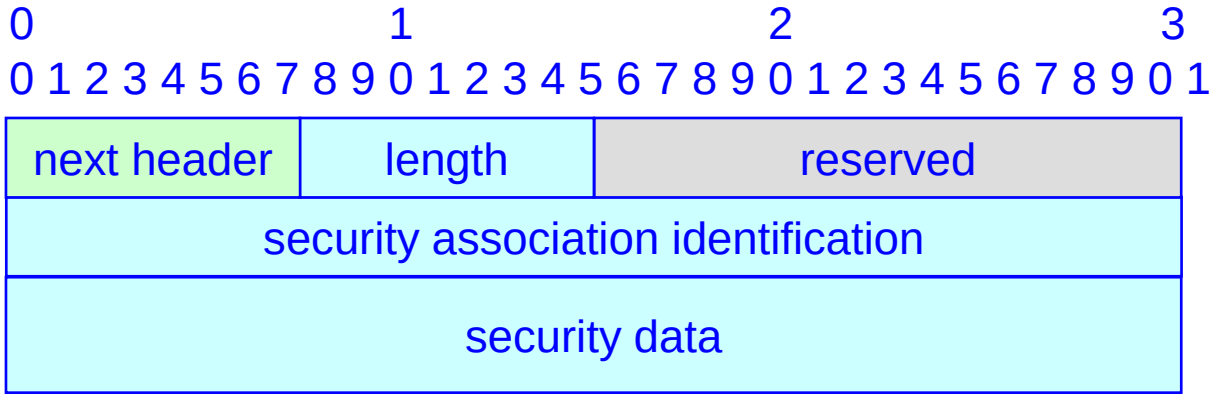
- the smallest MTU-value (maximum transport unit) for a given link is defined with 1280 bytes (576 in early RFCs)
  - old value with IPv4 = 68 bytes
  - packets may be smaller, it must only be guaranteed that packets with fewer than 1280 bytes can be transported without undergoing fragmentation
  - if a link (example ATM) has smaller transport units, either the link-layer or a layer between link layer and IP must do the fragmentation and reassembly hiding it from IPv6
- all IPv6 nodes must be able to do MTU-discovery to find out the MTU of a given link
- nodes which are absolutely sure that all their data fits into packets smaller than 1280 bytes may skip MTU-detection
  - may be suitable for embedded devices sending only alarms
  - may be usable in voice applications
  - not optimal for normal server or client usage

Cascaded MTU-Discovery



IPv6 Authentication Header

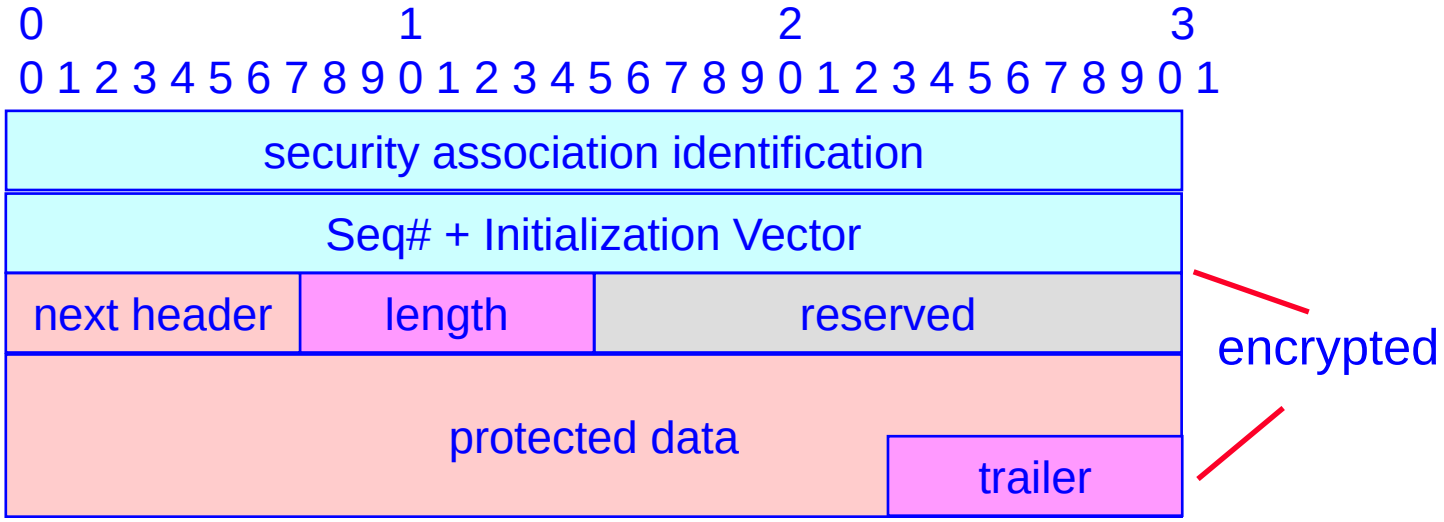
- defines authentication and validation by checksum for the content



field	length	content
next header	8 bit	type of next headers
length	8 bit	length of security data using 8 octets units
reserved	16 bit	set to 0
security a. i.	32 bit	pointer to a security association which is used by this data flow
security data	variable	security information, content depends on the hashing algorithm defined in the SAI starts always with a 4 byte sequence-number

IPv6 Privacy Header

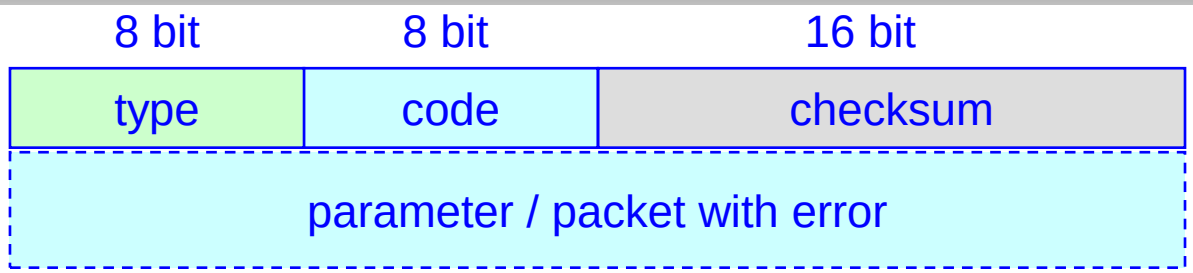
- provides encryption of the payload data
- may be used to encrypt header-information including addresses in tunnel mode
- is always the last visible unencrypted part of a IPv6 - packet



IPv6 – Tutorial

- ICMPv6

ICMPv6

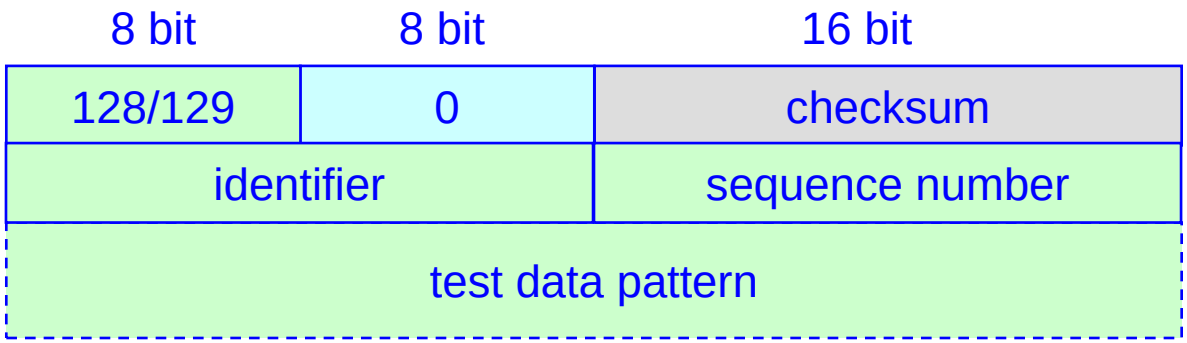


type	meaning	
1	Destination Unreachable	error-messages
2	Packet Too Big	
3	Time Exceeded	
4	Parameter Problem	
128	Echo Request	control and information
129	Echo Reply	
130	Group Membership Query	
131	Group Membership Report	
132	Group Membership Reduction	
133	Router Request	
134	Router Announcement	
135	Neighbour Discovery	
136	Neighbour Announcement	
137	Redirection	
141	Reverse Neighbour Discovery	
142	Reverse Neighbour Announcement	

Error Messages

type	code	meaning
1	0	no route to destination
1	1	communication with destination administratively prohibited
1	2	not a neighbor
1	3	address unreachable
1	4	port unreachable
2	0	Message > MTU size
3	0	hop limit exceeded in transit
3	1	fragment reassembly time exceeded
4	0	erroneous header field encountered
4	1	unrecognized next header type encountered
4	2	unrecognized IPv6 option encountered

ICMPv6 - Echo

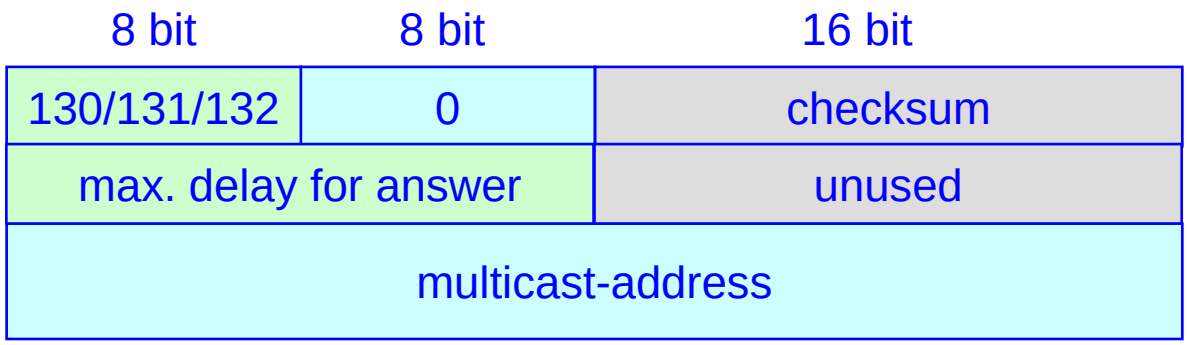


Ping:

ICMP Echo Request (128)

ICMP Echo Reply (129)

ICMPv6 Group Membership



- Control of multicast-groups:
  - ask if the system addressed in the IPv6-destination-address is member of the group defined in this ICMP-packet (type = 130)
  - indication that the system with source-IP-address in the packet-header is member of the multicast-group defined here (type = 131)
  - announce the leaving of a multicast-group (type= 132)

IPv6 Seminar

- Auto-Configuration

Auto-Configuration

- Start with a link-local address
  - well-known "unique token" like MAC-address
  - + link local prefix
  - FE 80 : 0 : 0 : 0 : 0 : xxxx : xxxx : xxxx
    the first link-local address of an interface
- make sure this address is not yet in use:
  - send ICMP neighbor discovery (135) to the address created just before
    - no answer – everything is OK, use this address
    - answer received with an ICMP neighbor announcement (136) – someone already uses this address ➡ error handling
- enter all necessary multicast groups:
  - FF02 :: 1 all nodes on the link
  - FF02 :: 2 all routers on the link

Auto-Configuration

- solicit router (ICMP router request 133)
  - destination-address: FF02 :: 2 (all routers on this link)
  - source-address: local-link address
- answer from router (ICMP router announcement 134)
  - no answer received: network not connected to a router, network not connected to global Internet, so continue working with the link-local address
  - router advertisement received carrying all information needed: setup unicast addresses using prefixes from router, start using global unicast addresses
  - router advertisement received with DHCP bit set: use router prefixes if available, ask DHCP-server for further values and use both (still some discussion how to combine information from both sources)

Neighbor Solicitation

- requests the MAC-address of a neighbor

8 bit	8 bit	16 bit
type (= 135)	0	checksum
not used		
IPv6-address of the machine searched for		
option (= 1)	length (= 1)	MAC-address (upper 16 bit)
MAC-address of sender (lower 32 bit)		

  - replaces IPv4-ARP

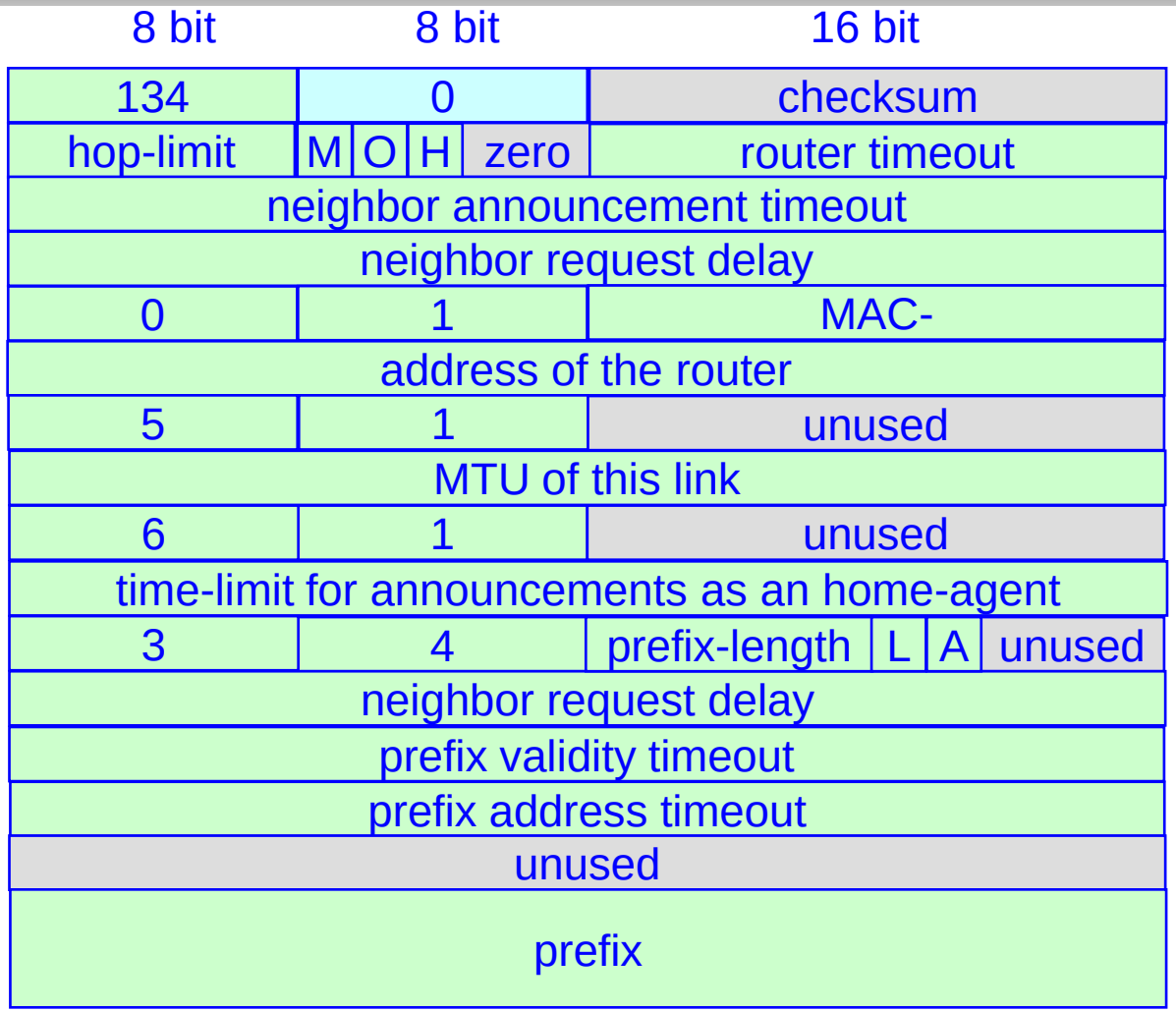
Neighbor Announcement

- shows the IPv6-address used by a MAC-address

8 bit			8 bit	16 bit
type (= 136)			0	checksum
R	S	O	frei	
associated IPv6-destination-address				
option (= 2)			length (= 1)	MAC-address
MAC-address				

  - R = router, S = answer, O = override

Router Advertisement



Router Advertisement

information to setup the IPv6-system:

- M-bit = 0 ➡ use router advertisement (stateless)
- M-bit = 1 ➡ use DHCP (stateful)
- O-bit = 1 ➡ use router advertisement für address, DHCP for other information and configuration data
- H-bit = 1 ➡ router is a home-agent für MOBILEIP

- hop-limit ➡ router defines this hop-limit
- router announcement timeout
  neighbor announcement timeout
  home-agent announcement timeout ➡ defines lifetimes for announcements
- neighbor request delay ➡ minimum time between requests

- MAC-address ➡ to avoid an additional neighbor-solicit cycle
- MTU ➡ indicate MTU for this link

Router Advertisement

- prefix (may be included several times in one announcement)
  - the network prefix and the number of bits to be used (length)
  - The time (duration) how long this prefix may be used to construct new addresses
  - the time (duration) of the usability of addresses using this prefix
  - an indication if this prefix is locally connected (L=1)
  - an indication that this prefix may be used to construct global unicast addresses
- there is still some discussion about additional parameters to be included like DNS-server
- there is still some discussion about handling of changed parameter-values especially shortened time-limits or changeover from DHCP to RA only and vice versa

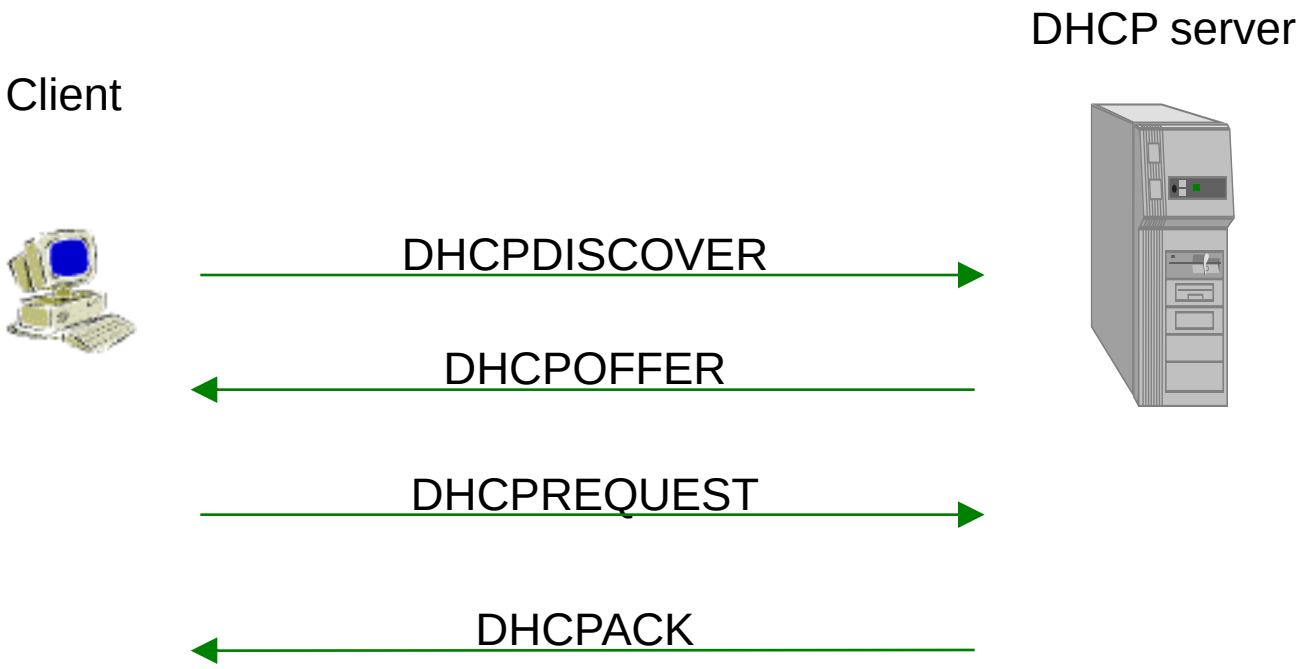
Selection of Source-Address

- A node may have several (many) addresses on every interface
- still under discussion, current proposal:
  - using the destination-address all prefixes of possible source-addresses will be checked for a longest match and this address shall be used.
  - are several candidates available, a manually configurable routing-weight should decide. Other proposals favor rules using local addresses first
- There are still drafts on the table, which define fixed ordering of priorities on address-types

IPv6 – Tutorial

- DHCPv6

flow of DHCP-Boot using IPv6



the same procedure as being used with IPv4….

DHCPv6

- format for request

8 bit	8 bit		8 bit	8 bit
type (= 3)	C S R	res.	transaction-ID	
address of the client				
address of the relay agent (S = 0) or server (S = 1)				
address of the server (only if previous field contains a relay)				
DHCP-extensions (variable in number and length; may be omitted) enumerates options which shall be re-confirmed or extended by the server				

R = 0: reset done, C = 0: return address to pool

DHCPv6

- answer

8 bit	8 bit		8 bit	8 bit
type (= 4)	L	state	transaction-ID	
address of the clients (only present if L = 1, otherwise this place is occupied by the address of the relay)				
extensions (variable in number and length) DHCP-parameter				

  - additional packet-types for information, release and request of a complete re-configuration are also defined

DHCPv6-Parameter

- IP-address

8 bit	8 bit	8 bit	8 bit
type (= 1)		length	
state	C L Q A P	reserved	prefix-length
IP-address (may be omitted, C = 1 if present)			
preferred life-time (may be omitted, L = 1 if present)			
valid life-time (may be omitted, L = 1 if present)			
DNS-name (may be omitted)			

Q: this option is required by the client

A: address shall be entered into DNS using an AAAA-record

P: server shall create a PTR-record in DNS for this address

DHCPv6-Parameter

- many other options are defined:
  - 2 – time-offset
  - 3 – time
  - 6 – DNS-server
  - 10 – domain-name
  - 16 – directory-service
  - 18 – NTP-server
  - 19 + 20 – NIS-server
  - 32 – TCP-keep-alive-time
  - 40 – IPv6-message-size (MTU)
  - 48 – private vendor extensions
  - 66 – multicast-address
  - 67 – DHCP-server-address to be used after a hand-over
  - 68 – ICMP-error-message created by the relay-agent
  - 84 + 86 – DHCP-authentication
  - more parameters and options are defined as needed

IPv6 – Tutorial

- DNS

DNS and IPv6

- IPv6 in DNS is a simple extension to IPv4-rules:

myv4host	IN	A	1.2.3.4
myv6host	IN	AAAA	2001:DB80:1:2:3:4:56:789a
mypc	IN	AAAA	2001:DB80::4567:89ab

second DNS-Format

- proposed version using recursion

my6host	IN	AAAA	2001:DB80:1:2:3:4:56:789a
-			
mynet	IN	A6	2001:DB80:1:2::
my6host	IN	A6	::3:4:56:789a 64 mynet
mypc2	IN	A6	::1:9:7654:fedc 64 mynet

This solution is now depreciated and removed from the standards track because of implementation problems and load problems caused by complex recursion especially in caching environments.

Reverse DNS

- To find names from addresses the IPv4-PTR was only extended:
  - who has: 2001:DB8::12:3:4:567:89ab

    DNS entry:

b.a.9.8.7.6.5.0.4.0.0.0.3.0.0.0.2.1.0.0.0.0.0.0.0.8.B.D.1.0.0.2.ip6.arpa. IN PTR my6host

- Hint:
  at the start of the standardization (still found in some machines) the DNS-tree .int instead of .arpa was proposed for this functionality

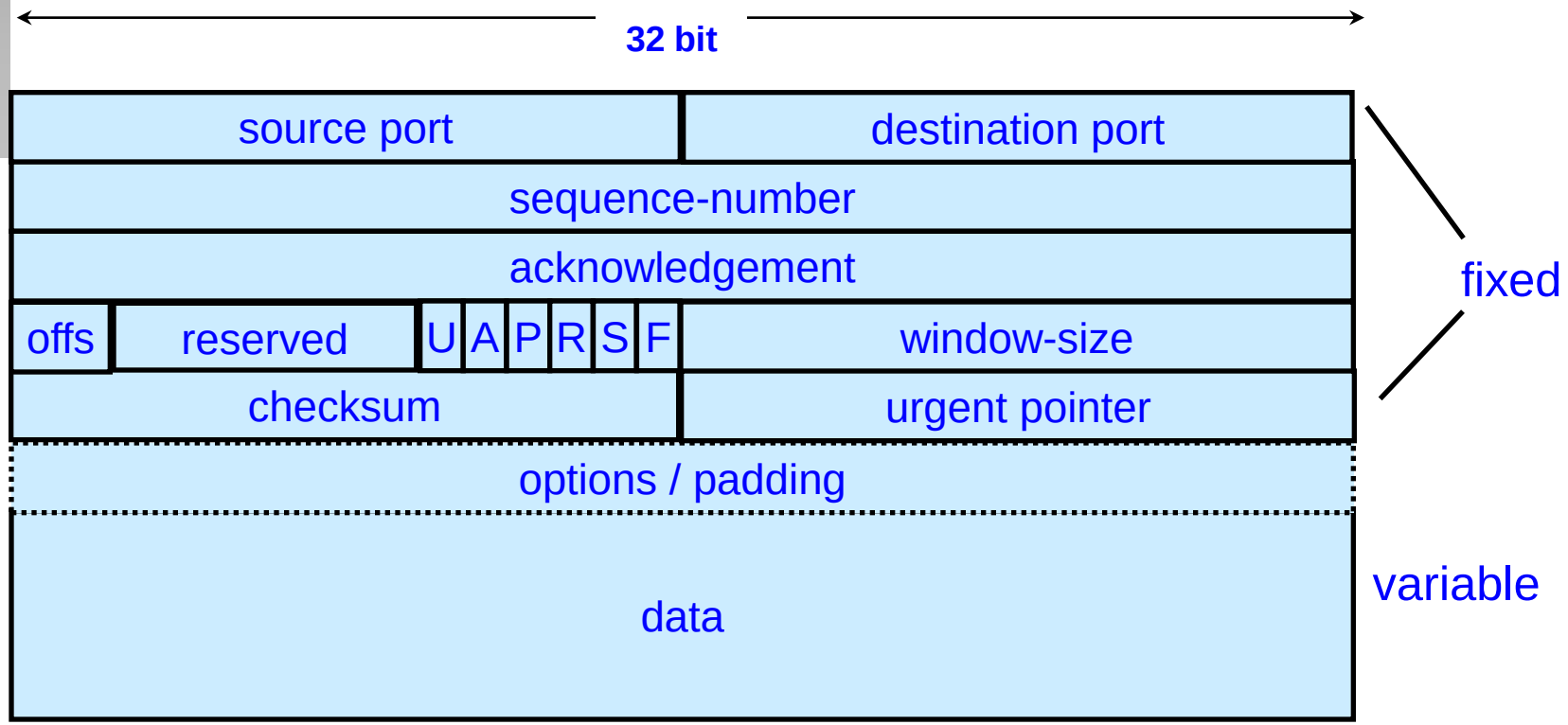
Problems with DNS

- DNS is a hierarchical tree
  - not all combinations of IPv4-servers and IPv4-forwarders are working seamlessly with IPv6-based resolvers and clients
  - a standard for gateways is still under discussion
- ICANN has approved IPv6-Service for DNS-root-servers
  - this has not yet been fully rolled out to all servers
  - not all TLD-servers are running IPv6-DNS
  - not all registries are accepting IPv6-addresses

IPv6 – Tutorial

- TCP and UDP

TCP Header Format

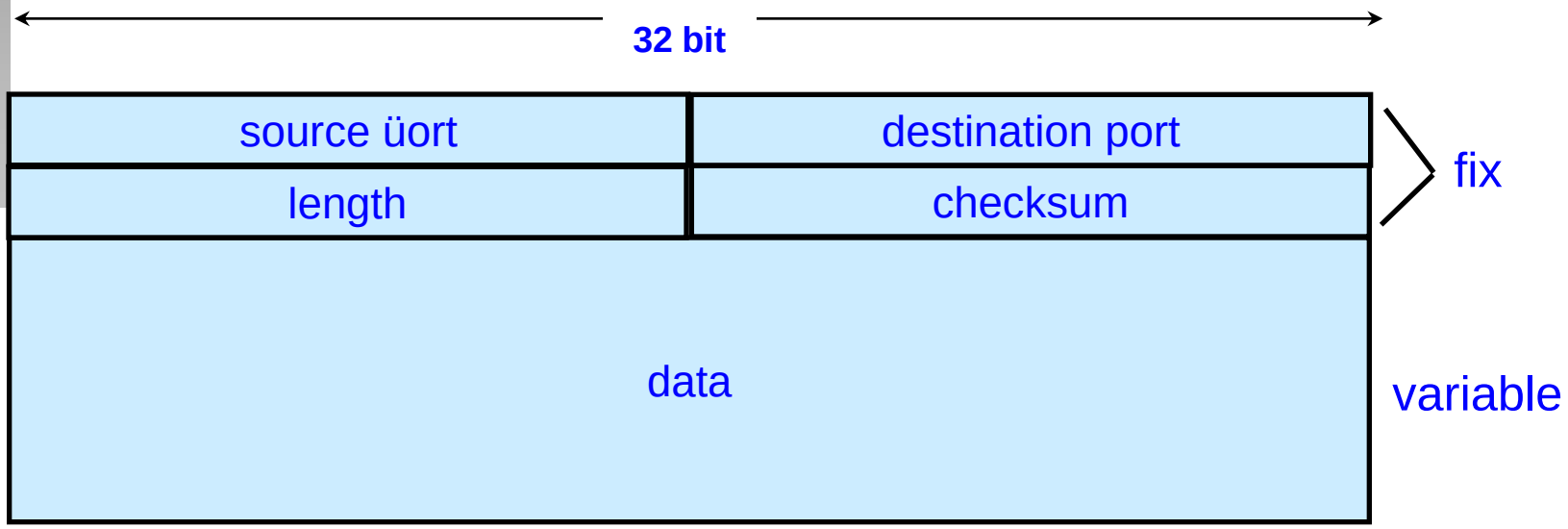


Changes in TCP

- only calculation of checksum has been adapted to IPv6 :

16 bit	8 bit	8 bit
128 bit IPv6-source-address		
128 bit IPv6-destination-address		
lenght over all		
0		protocol (= 6)
source-port	destination-port	
sequence-number		
acknowledge-number		
length	U A P R S	window
checksum		priority-pointer
options		
data		

UDP Header


32 bit
source üort
destination port
length
checksum
data
fix
variable

Changes in UDP

- checksum calculation adapted to new address size
- checksum is no longer optional
  - this requirement is atill under heavy discussion in VoIP and UMTS working groups, because checksums add only delay to voice transmission without being used for re-transmission in case of errors

IPv6 – Tutorial

- Multicast und Routing

Multicast

- Multicast has a much more central role with IPv6
- Multicast (and Anycast) in LAN-environments replace Broadcasts used by IPv4
- Multicast over WAN or the global Internet are nearly identical from IPv4 to IPv6:
  - Multicast-protocols were adapted (PIM)
  - additional ICMPv6-protocol elements are used for better control of multicast-groups

Routing

- All existing routing-protocols must be adopted for IPv6
  - RIP - done
  - BGP - done
  - OSPF - done
  - new versions carry longer address-fields
  - implementation and availability still varies from manufacturer to manufacturer

IPv6 – Tutorial

- RFCs and Links

Current RFCs

- RFC 1887 An Architecture for IPv6 Unicast Address Allocation
- RFC 1883 Internet Protocol, Version 6 (IPv6) Specification obsoleted by RFC 2460
- RFC 1884 IP Version 6 Addressing Architecture obsoleted by RFC 2373
- RFC 1885 Internet Control Message Protocol (ICMPv6) for the Internet Protocol Version 6 (IPv6) obsoleted by RFC 2463
- RFC 1886 DNS Extensions to support IP version 6
- RFC 1888 OSI NSAPs and IPv6
- RFC 1897 IPv6 Testing Address Allocation obsoleted by RFC 2471
- RFC 1970 Neighbor Discovery for IP Version 6 (IPv6) obsoleted by RFC 2461
- RFC 1972 A Method for the Transmission of IPv6 Packets over Ethernet Networks obsoleted by RFC 2464
- RFC 1981 Path MTU Discovery for IP version 6
- RFC 2019 Transmission of IPv6 Packets Over FDDI obsoleted by RFC 2467
- RFC 2023 IP Version 6 over PPP obsoleted by RFC 2472
- RFC 2073 An IPv6 Provider-Based Unicast Address Format obsoleted by RFC 2374
- RFC 2133 Basic Socket Interface Extensions for IPv6 obsoleted by RFC 2553
- RFC 2147 TCP and UDP over IPv6 Jumbograms obsoleted by RFC 2675
- RFC 2292 Advanced Sockets API for IPv6 obsoleted by RFC 3542
- RFC 2373 IP Version 6 Addressing Architecture obsoleted by RFC 3513
- RFC 2374 An IPv6 Aggregatable Global Unicast Address Format obsoleted by RFC 3587
- RFC 2375 IPv6 Multicast Address Assignments
- RFC 2450 Proposed TLA and NLA Assignment Rules

Current RFCs

- RFC 2452 IP Version 6 Management Information Base for the Transmission Control Protocol
- RFC 2454 IP Version 6 Management Information Base for the User Datagram Protocol
- RFC 2460 Internet Protocol, Version 6 (IPv6) Specification
- RFC 2461 Neighbor Discovery for IP Version 6 (IPv6)
- RFC 2462 IPv6 Stateless Address Autoconfiguration
- RFC 2463 Internet Control Message Protocol (ICMPv6) for the Internet Protocol Version 6 (IPv6) Specification
- RFC 2464 Transmission of IPv6 Packets over Ethernet Networks
- RFC 2465 Management Information Base for IP Version 6: Textual Conventions and General Group
- RFC 2466 Management Information Base for IP Version 6: ICMPv6 Group
- RFC 2467 Transmission of IPv6 Packets over FDDI Networks
- RFC 2470 Transmission of IPv6 Packets over Token Ring Networks
- RFC 2471 IPv6 Testing Address Allocation obsoleted by RFC 3701
- RFC 2472 IP Version 6 over PPP
- RFC 2473 Generic Packet Tunneling in IPv6 Specification
- RFC 2497 Transmission of IPv6 Packets over ARCnet Networks
- RFC 2507 IP Header Compression
- RFC 2526 Reserved IPv6 Subnet Anycast Addresses
- RFC 2529 Transmission of IPv6 over IPv4 Domains without Explicit Tunnels
- RFC 2553 Basic Socket Interface Extensions for IPv6 obsoleted by RFC 3493
- RFC 2675 IPv6 Jumbograms

Current RFCs

- RFC 2710 Multicast Listener Discovery (MLD) for IPv6
- RFC 2711 IPv6 Router Alert Option
- RFC 2732 Format for Literal IPv6 Addresses in URL's
- RFC 2874 DNS Extensions to Support IPv6 Address Aggregation and Renumbering
- RFC 2894 Router Renumbering for IPv6
- RFC 2928 Initial IPv6 Sub-TLA ID Assignments
- RFC 3041 Privacy Extensions for Stateless Address Autoconfiguration in IPv6
- RFC 3019 IP Version 6 Management Information Base for the Multicast Listener Discovery Protocol
- RFC 3056 Connection of IPv6 Domains via IPv4 Clouds
- RFC 3089 A SOCKS-based IPv6/IPv4 Gateway Mechanism
- RFC 3111 Service Location Protocol Modifications for IPv6
- RFC 3122 Extensions to IPv6 Neighbor Discovery for Inverse Discovery Specification
- RFC 3142 An IPv6-to-IPv4 Transport Relay Translator
- RFC 3146 Transmission of IPv6 Packets over IEEE 1394
- RFC 3162 RADIUS and IPv6
- RFC 3175 Aggregation of RSVP for IPv4 and IPv6 Reservations
- RFC 3177 IAB/IESG Recommendations on IPv6 Address Allocations to Sites
- RFC 3178 IPv6 Multihoming Support at Site Exit Routers
- RFC 3146 Transmission of IPv6 Packets over IEEE 1394 Networks
- RFC 3178 IPv6 multihoming support at site exit routers
- RFC 3226 DNSSEC and IPv6 A6 aware server/resolver message size requirements

Current RFCs

- RFC 3266 Support for IPv6 in Session Description Protocol (SDP)
- RFC 3306 Unicast-Prefix-based IPv6 Multicast Addresses
- RFC 3307 Allocation Guidelines for IPv6 Multicast Addresses
- RFC 3314 Recommendations for IPv6 in Third Generation Partnership Project (3GPP) Standards
- RFC 3315 Dynamic Host Configuration Protocol for IPv6 (DHCPv6)
- RFC 3316 Internet Protocol Version 6 (IPv6) for Some Second and Third Generation Cellular Hosts
- RFC 3363 Representing Internet Protocol version 6 (IPv6) Addresses in the Domain Name System (DNS)
- RFC 3364 Tradeoffs in Domain Name System (DNS) Support for Internet Protocol version 6 (IPv6)
- RFC 3484 Default Address Selection for Internet Protocol version 6 (IPv6)
- RFC 3493 Basic Socket Interface Extensions for IPv6
- RFC 3513 Internet Protocol Version 6 (IPv6) Addressing Architecture
- RFC 3531 A Flexible Method for Managing the Assignment of Bits of an IPv6 Address Block
- RFC 3542 Advanced Sockets Application Program Interface (API) for IPv6
- RFC 3572 Internet Protocol Version 6 over MAPOS (Multiple Access Protocol Over SONET/SDH)
- RFC 3574 Transition Scenarios for 3GPP Networks
- RFC 3582 Goals for IPv6 Site-Multihoming Architectures
- RFC 3587 IPv6 Global Unicast Address Format

Current RFCs

- RFC 3590 Source Address Selection for the Multicast Listener Discovery (MLD) Protocol
- RFC 3595 Textual Conventions for IPv6 Flow Label
- RFC 3633 IPv6 Prefix Options for Dynamic Host Configuration Protocol (DHCP) version 6
- RFC 3646 DNS Configuration options for Dynamic Host Configuration Protocol for IPv6 (DHCPv6)
- RFC 3697 IPv6 Flow Label Specification
- RFC 3701 6bone (IPv6 Testing Address Allocation) Phaseout
- RFC 3736 Stateless Dynamic Host Configuration Protocol (DHCP) Service for IPv6
- RFC 3750 Unmanaged Networks IPv6 Transition Scenarios
- RFC 3756 IPv6 Neighbor Discovery (ND) Trust Models and Threats
- RFC 3769 Requirements for IPv6 Prefix Delegation
- RFC 3775 Mobility Support in IPv6
- RFC 3776 Using IPsec to Protect Mobile IPv6 Signaling Between Mobile Nodes and Home Agents
- RFC 3810 Multicast Listener Discovery Version 2 (MLDv2) for IPv6
- RFC 3831 Transmission of IPv6 Packets over Fibre Channel
- RFC 3849 IPv6 Address Prefix Reserved for Documentation
- RFC 3879 Deprecating Site Local Addresses
- RFC 3898 Network Information Service (NIS) Configuration Options for Dynamic Host Configuration Protocol for IPv6 (DHCPv6)

Current RFCs

- RFC 3901 DNS IPv6 Transport Operational Guidelines
- RFC 3904 Evaluation of IPv6 Transition Mechanisms for Unmanaged Networks
- RFC 3919 Remote Network Monitoring (RMON) Protocol Identifiers for IPv6 and Multi Protocol Label Switching (MPLS)
- RFC 3956 Embedding the Rendezvous Point (RP) Address in an IPv6 Multicast Address
- RFC 3963 Network Mobility (NEMO) Basic Support Protocol
- RFC 3974 SMTP Operational Experience in Mixed IPv4/v6 Environments
- RFC 4007 IPv6 Scoped Address Architecture
- RFC 4029 Scenarios and Analysis for Introducing IPv6 into ISP Networks
- RFC 4038 Application Aspects of IPv6 Transition
- RFC 4057 IPv6 Enterprise Network Scenarios
- RFC 4068 Fast Handovers for Mobile IPv6
- RFC 4074 Common Misbehavior Against DNS Queries for IPv6 Addresses
- RFC 4076 Renumbering Requirements for Stateless Dynamic Host Configuration Protocol for IPv6 (DHCPv6)
- RFC 4135 Goals of Detecting Network Attachment in IPv6
- RFC 4140 Hierarchical Mobile IPv6 Mobility Management (HMIPv6)
- RFC 4147 Proposed Changes to the Format of the IANA IPv6 Registry
- RFC 4159 Deprecation of ip6.int
- RFC 4177 Architectural Approaches to Multi-homing for IPv6
- RFC 4192 Procedures for Renumbering an IPv6 Network without a Flag Day
- RFC 4193 Unique Local IPv6 Unicast Addresses

Current RFCs

- RFC 4213 Basic Transition Mechanisms for IPv6 Hosts and Routers
- RFC 4215 Analysis on IPv6 Transition in Third Generation Partnership Project (3GPP) Networks
- RFC 4218 Threats Relating to IPv6 Multihoming Solutions
- RFC 4219 Things Multihoming in IPv6 (MULTI6) Developers Should Think About
- RFC 4241 A Model of IPv6/IPv4 Dual Stack Internet Access Service
- RFC 4242 Information Refresh Time Option for Dynamic Host Configuration Protocol for IPv6 (DHCPv6)
- RFC 4260 Mobile IPv6 Fast Handovers for 802.11 Networks
- RFC 4283 Mobile Node Identifier Option for Mobile IPv6 (MIPv6)
- RFC 4285 Authentication Protocol for Mobile IPv6
- RFC 4293 Management Information Base for the Internet Protocol (IP)
- RFC 4294 IPv6 Node Requirements
- RFC 4295 Mobile IPv6 Management Information Base
- RFC 4301 Security Architecture for the Internet Protocol
- RFC 4302 IP Authentication Header
- RFC 4303 IP Encapsulating Security Payload (ESP)
- RFC 4305 Cryptographic Algorithm Implementation Requirements for Encapsulating Security Payload (ESP) and Authentication Header (AH)
- RFC 4311 IPv6 Host-to-Router Load Sharing
- RFC 4330 Simple Network Time Protocol (SNTP) Version 4 for IPv4, IPv6 and OSI
- RFC 4338 Transmission of IPv6, IPv4, and Address Resolution Protocol (ARP) Packets over Fibre Channel

Current RFCs

- RFC 4339 IPv6 Host Configuration of DNS Server Information Approaches
- RFC 4380 Teredo: Tunneling IPv6 over UDP through Network Address Translations (NATs)
- RFC 4392 IP over InfiniBand (IPoIB) Architecture
- RFC 4429 Optimistic Duplicate Address Detection (DAD) for IPv6
- RFC 4443 Internet Control Message Protocol (ICMPv6) for the Internet Protocol Version 6 (IPv6) Specification
- RFC 4449 Securing Mobile IPv6 Route Optimization Using a Static Shared Key
- RFC 4472 Operational Considerations and Issues with IPv6 DNS
- RFC 4477 Dynamic Host Configuration Protocol (DHCP): IPv4 and IPv6 Dual-Stack Issues
- RFC 4487 Mobile IPv6 and Firewalls: Problem Statement
- RFC 4489 A Method for Generating Link-Scoped IPv6 Multicast Addresses
- RFC 4554 Use of VLANs for IPv4-IPv6 Coexistence in Enterprise Networks
- RFC 4580 Dynamic Host Configuration Protocol for IPv6 (DHCPv6) Relay Agent Subscriber-ID Option
- RFC 4584 Extension to Sockets API for Mobile IPv6
- RFC 4607 Source-Specific Multicast for IP
- RFC 4620 IPv6 Node Information Queries
- RFC 4640 Problem Statement for bootstrapping Mobile IPv6 (MIPv6)
- RFC 4649 Dynamic Host Configuration Protocol for IPv6 (DHCPv6) Relay Agent Remote-ID Option
- RFC 4651 A Taxonomy and Analysis of Enhancements to Mobile IPv6 Route Optimization

Current RFCs

- RFC 4659 BGP-MPLS IP Virtual Private Network (VPN) Extension for IPv6 VPN
- RFC 4668 RADIUS Authentication Client MIB for IPv6
- RFC 4669 RADIUS Authentication Server MIB for IPv6
- RFC 4670 RADIUS Accounting Client MIB for IPv6
- RFC 4671 RADIUS Accounting Server MIB for IPv6
- RFC 4692 Considerations on the IPv6 Host Density Metric
- RFC 4704 The Dynamic Host Configuration Protocol for IPv6 (DHCPv6) Client Fully Qualified Domain Name (FQDN) Option
- RFC 4727 Experimental Values In IPv4, IPv6, ICMPv4, ICMPv6, UDP, and TCP Headers
- RFC 4773 Administration of the IANA Special Purpose IPv6 Address Block
- RFC 4779 ISP IPv6 Deployment Scenarios in Broadband Access Networks
- RFC 4798 Connecting IPv6 Islands over IPv4 MPLS Using IPv6 Provider Edge Routers (6PE)
- RFC 4818 RADIUS Delegated-IPv6-Prefix Attribute
- RFC 4835 Cryptographic Algorithm Implementation Requirements for Encapsulating Security Payload (ESP) and Authentication Header (AH)
- RFC 4843 An IPv6 Prefix for Overlay Routable Cryptographic Hash Identifiers (ORCHID)
- RFC 4852 IPv6 Enterprise Network Analysis - IP Layer 3 Focus
- RFC 4864 Local Network Protection for IPv6

Current RFCs

- RFC 4866 Enhanced Route Optimization for Mobile IPv6
- RFC 4877 Mobile IPv6 Operation with IKEv2 and the Revised IPsec Architecture
- RFC 4882 IP Address Location Privacy and Mobile IPv6: Problem Statement
- RFC 4890 Recommendations for Filtering ICMPv6 Messages in Firewalls
- RFC 4891 Using IPsec to Secure IPv6-in-IPv4 Tunnels
- RFC 4919 IPv6 over Low-Power Wireless Personal Area Networks (6LoWPANs): Overview, Assumptions, Problem Statement, and Goals
- RFC 4968 Analysis of IPv6 Link Models for 802.16 Based Networks

- Sources for RFCs and Drafts
  - www.ietf.org
  - www.ripe.net

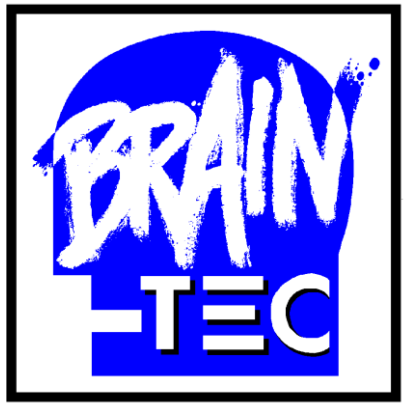
URLs for IPv6

- playground.sun.com
- www.ipv6forum.com
- www.ipv6tf.org
- www.kame.net

Dipl. Inform. Hans Peter Dittler

- 72 - 77 Computer Science at University of Karlsruhe
- 77 - 79 Research Fellow at University of Karlsruhe
- 80 - 89 Engineer for Data Communication Products at Conware Computer Consulting
- 90 - 94 CEO of Conware
- 95 - 96 BRAINTEC Consultant
- since 97 CEO of BRAINTEC Netzwerk-Consulting GmbH

- since 86 active in various groups at IEEE and IETF
- Vize-Chair of ISOC.DE



BRAINTEC Netzwerk-Consulting GmbH

Hans Peter Dittler

www.braintec-consult.de
hpdittler@braintec-consult.de
dittler@isoc.de

Herstellerunabhängige Beratung für
Vernetzung und Kommunikation
Karlsruhe