Internet, Principes et Protocoles (IPP)

Peer-2-Peer(P2P), who uses it?

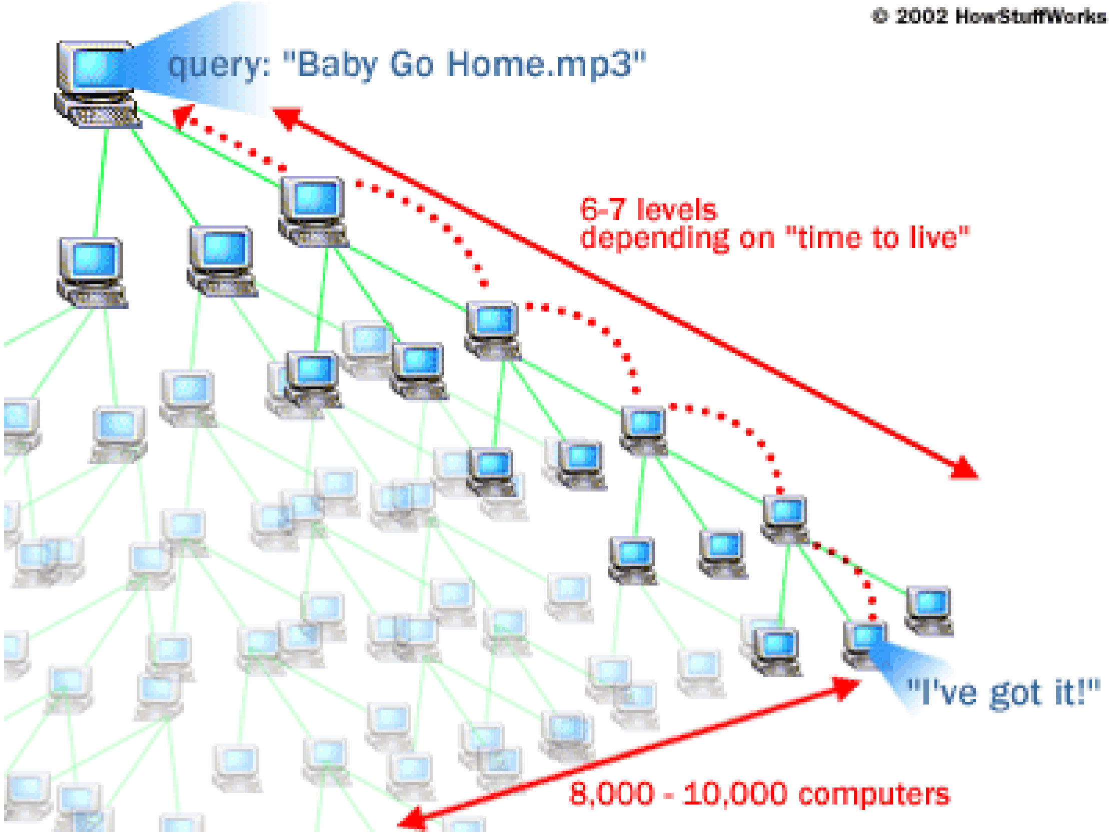
- Video-games (BF3-4, Doom, MW, ..)
- Collaborative applications (shared whiteboard/documents)
- Distributed computation (Etherium, universities, DoD)
- Windows updates
- Skype
- You know more?

Peer-2-Peer (P2)

- All nodes are both client and server (and routers)
- No centralized data source
- The loss of one node does not have an impact on the rest of the network
- Scales easily
- 2 major types: structured and un-structured

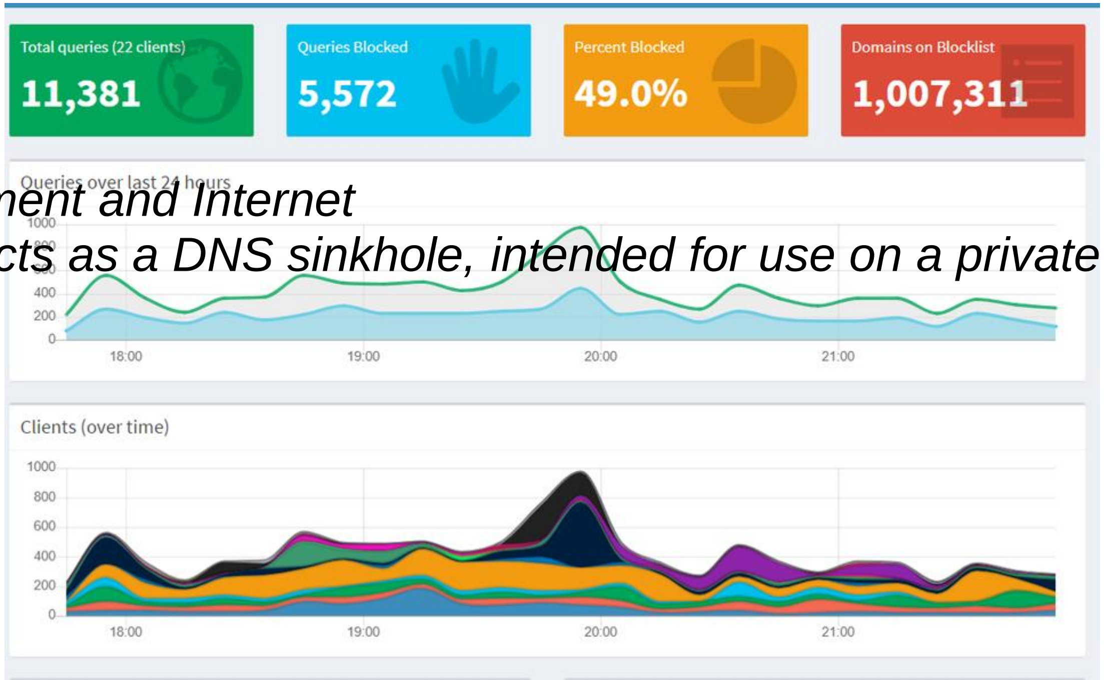
Example: Gnutella

- A way to share any files.
- Decentralized
- You ask your neighbours for a file
- Neighbours ask their neighbours, and so on
- Users with matching files reply to you



Mini-Project and how Ad blockers work

- Optional mini-project: install a pi-hole at home, or in a VM.



Total queries (22 clients) 11,381

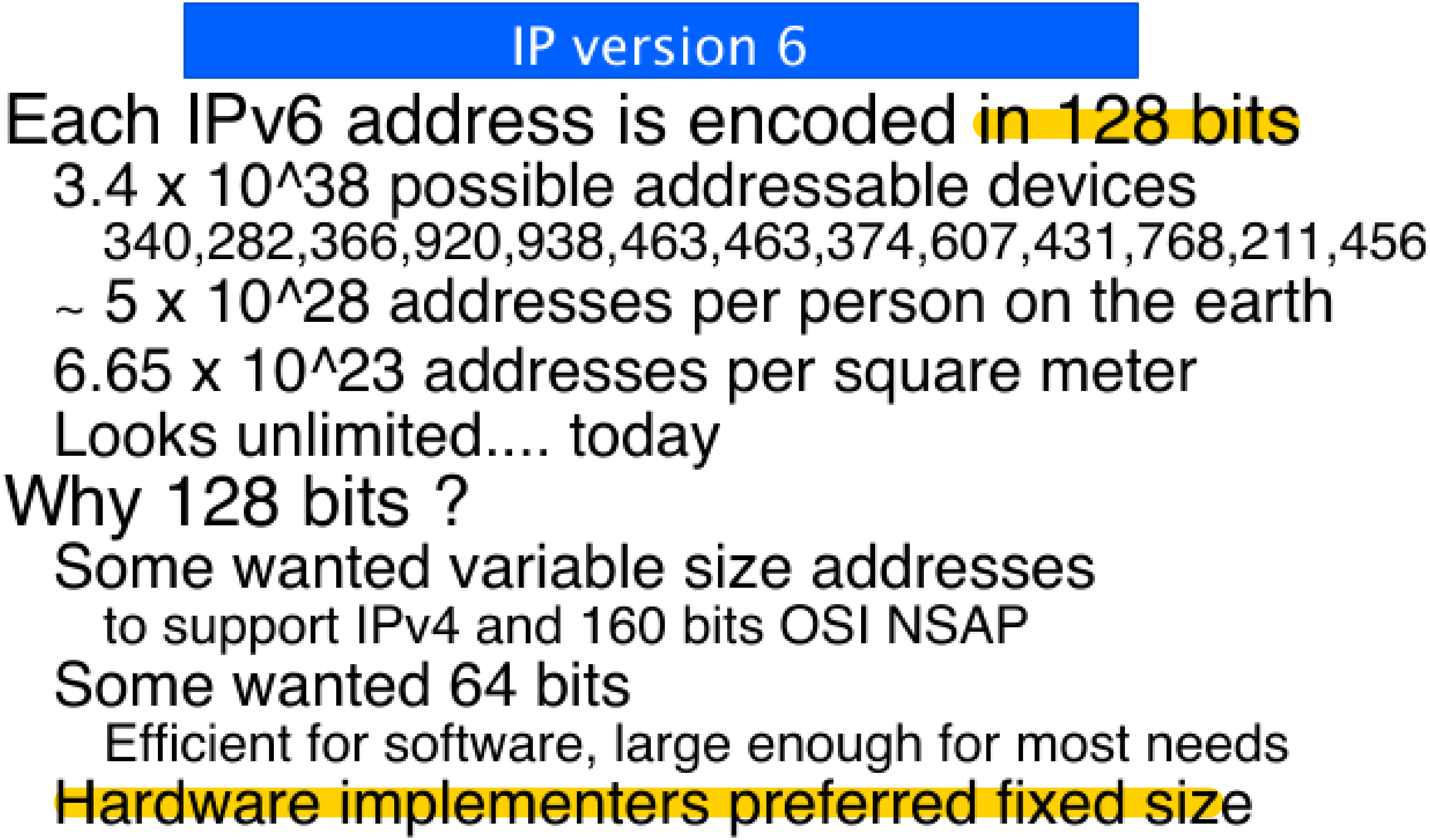
Queries Blocked 5,572

Percent Blocked 49.0%

Domains on Blocklist 1,007,311

Pi-hole is a network-level advertisement and Internet tracker blocking application which acts as a DNS sinkhole, intended for use on a private network

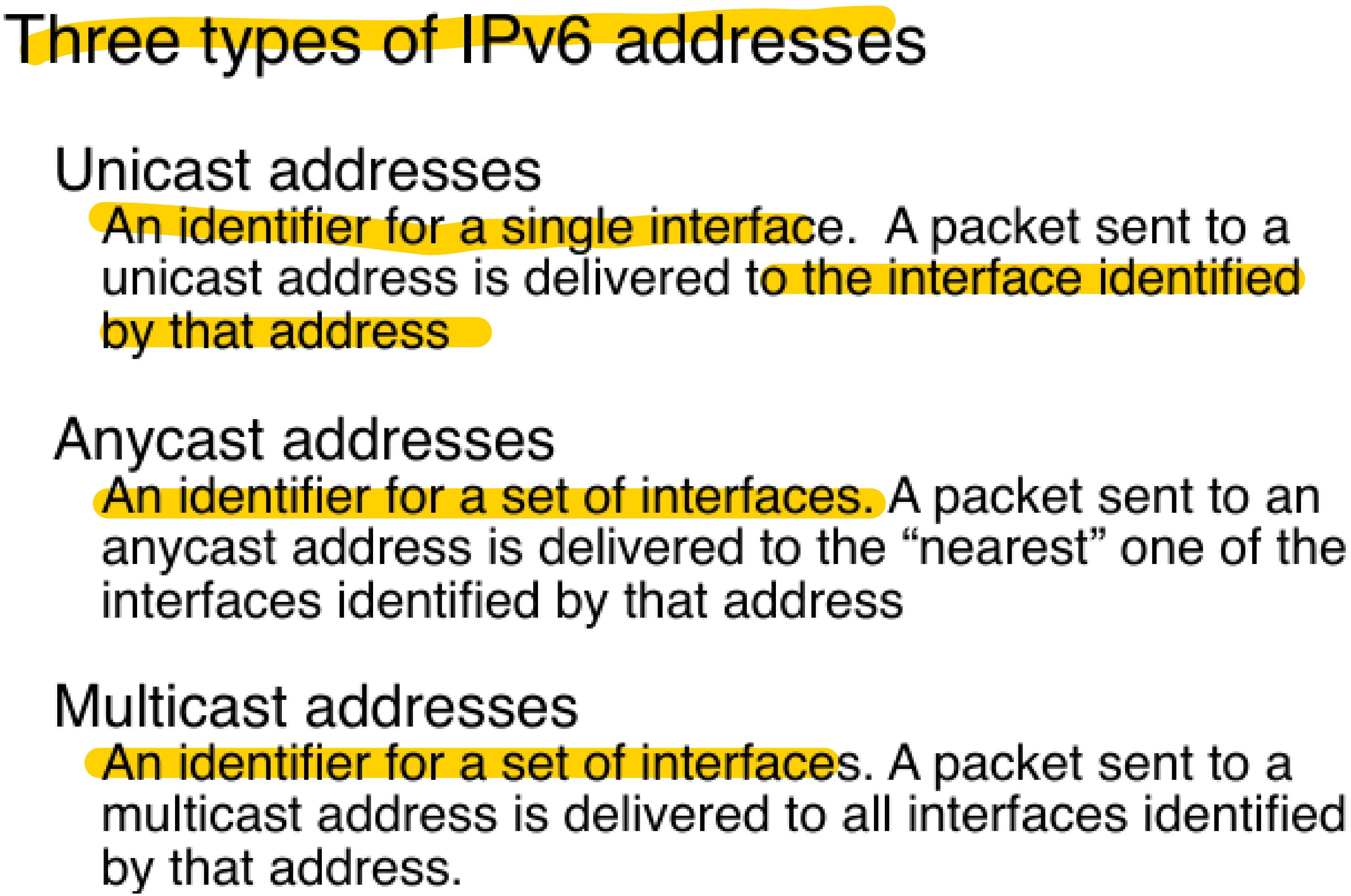
IPv6



IP version 6

- Each IPv6 address is encoded in 128 bits
  - 3.4 x 10^38 possible addressable devices
    - 340,282,366,920,938,463,463,374,607,431,768,211,456
  - ~ 5 x 10^28 addresses per person on the earth
  - 6.65 x 10^23 addresses per square meter
  - Looks unlimited.... today
- Why 128 bits ?
  - Some wanted variable size addresses
    - to support IPv4 and 160 bits OSI NSAP
  - Some wanted 64 bits
    - Efficient for software, large enough for most needs
  - Hardware implementers preferred fixed size

IPv6



Three types of IPv6 addresses

Unicast addresses

An identifier for a single interface. A packet sent to a unicast address is delivered to the interface identified by that address

Anycast addresses

An identifier for a set of interfaces. A packet sent to an anycast address is delivered to the "nearest" one of the interfaces identified by that address

Multicast addresses

An identifier for a set of interfaces. A packet sent to a multicast address is delivered to all interfaces identified by that address.

IPv6 address composition

- An IPv6 address is made of 128 bits divided into eight 16-bits blocks. Each block is then converted into 4-digit Hexadecimal numbers separated by colon symbols.
- 0010000000000001 0000000000000000 0011001000111000 1101111111100001 0000000001100011 0000000000000000 0000000000000000 1111111011111011
- **2001:0000:3238:DFE1:0063:0000:0000:FEFB**

IPv6 address composition

2001:0000:3238:DFE1:0063:0000:0000:FEFB

- Still long so:

– Rule 1: Discard leading Zero(es):

- In Block 5, 0063, the leading two 0s can be omitted

– Rule 2: If two of more blocks contain consecutive zeroes, omit them all and replace with double colon sign ::, such as (6th and 7th block). This can happen only once (If there are more, change to :0:).

– **2001:0:3238:DFE1:63::FEFB**

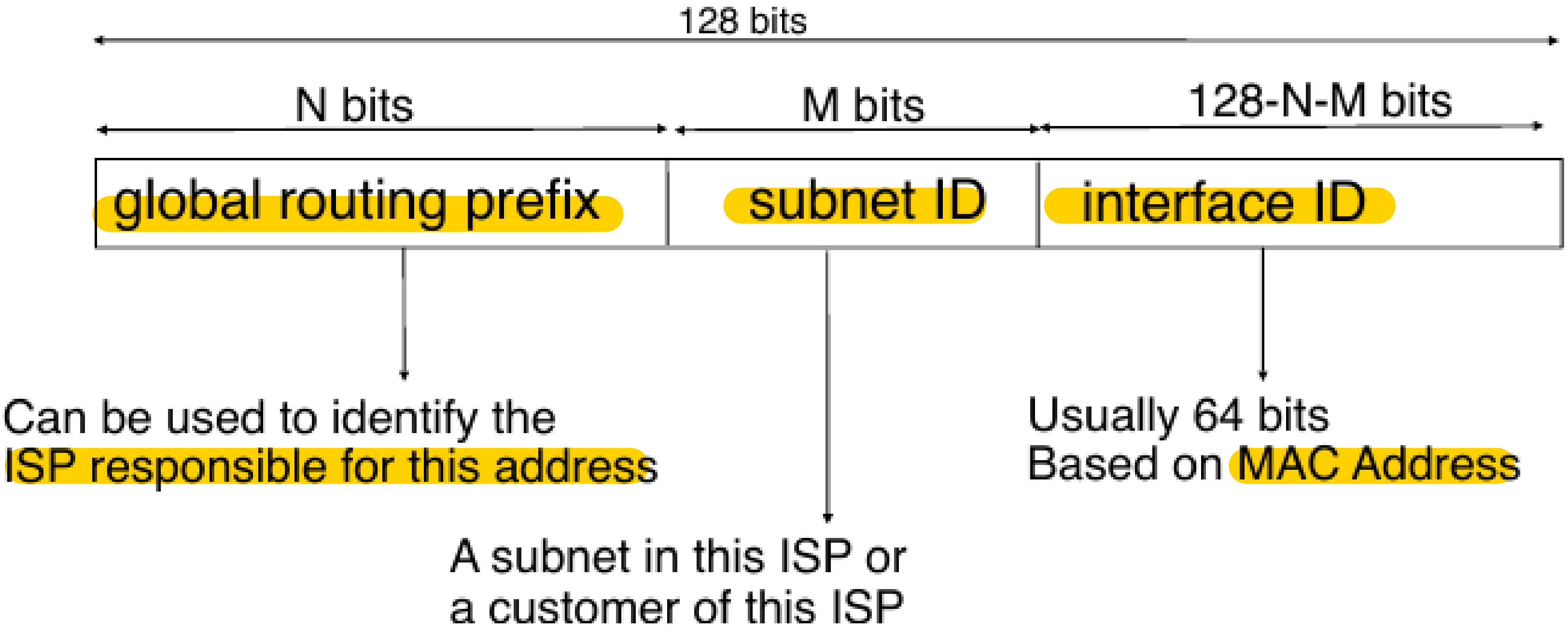
IPv6 Unicast

Special addresses

- Unspecified address : 0:0:0:0:0:0:0:0 (aka ::)
- Loopback address : 0:0:0:0:0:0:0:1 (aka ::1)

Global unicast addresses

- Addresses will be allocated hierarchically



128 bits

N bits

M bits

128-N-M bits

global routing prefix

subnet ID

interface ID

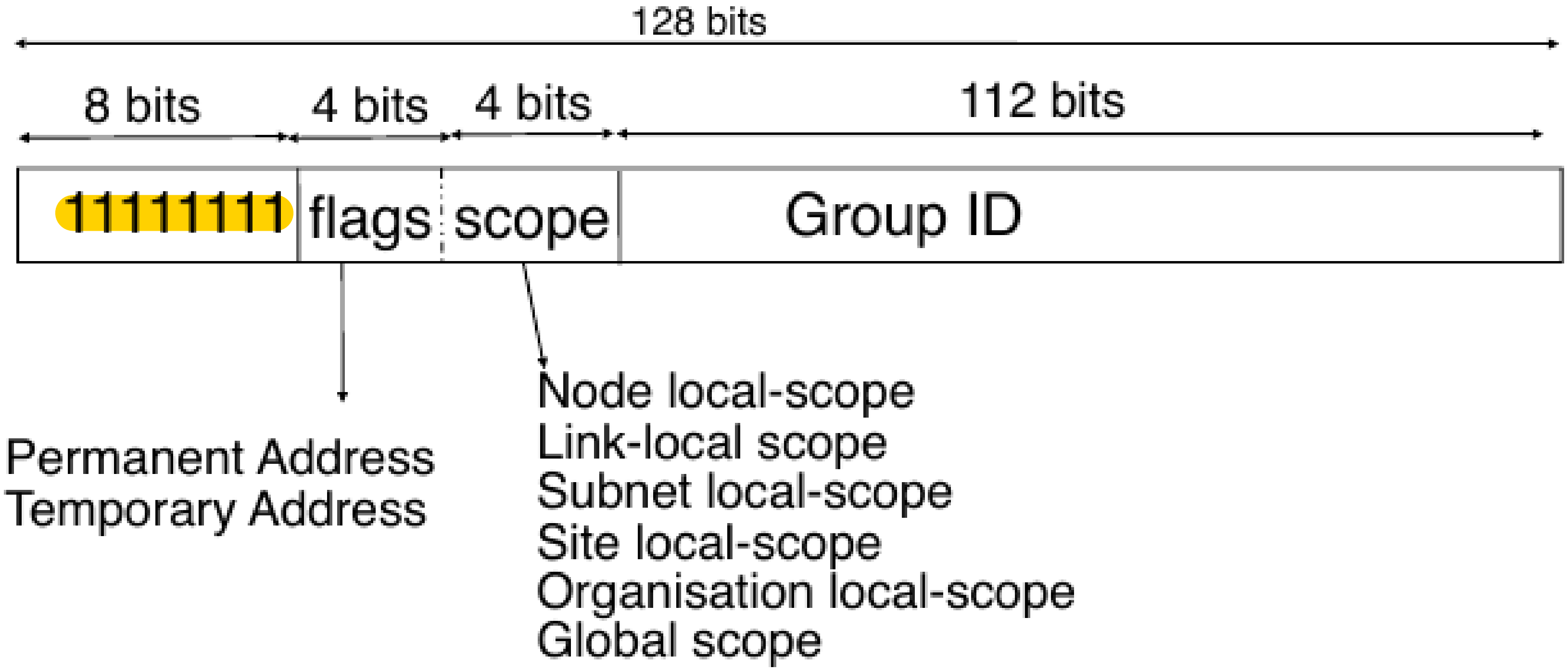
Can be used to identify the ISP responsible for this address

A subnet in this ISP or a customer of this ISP

Usually 64 bits Based on MAC Address

IPv6 Multicast

An IPv6 multicast address identifies a group a receivers



Well known groups

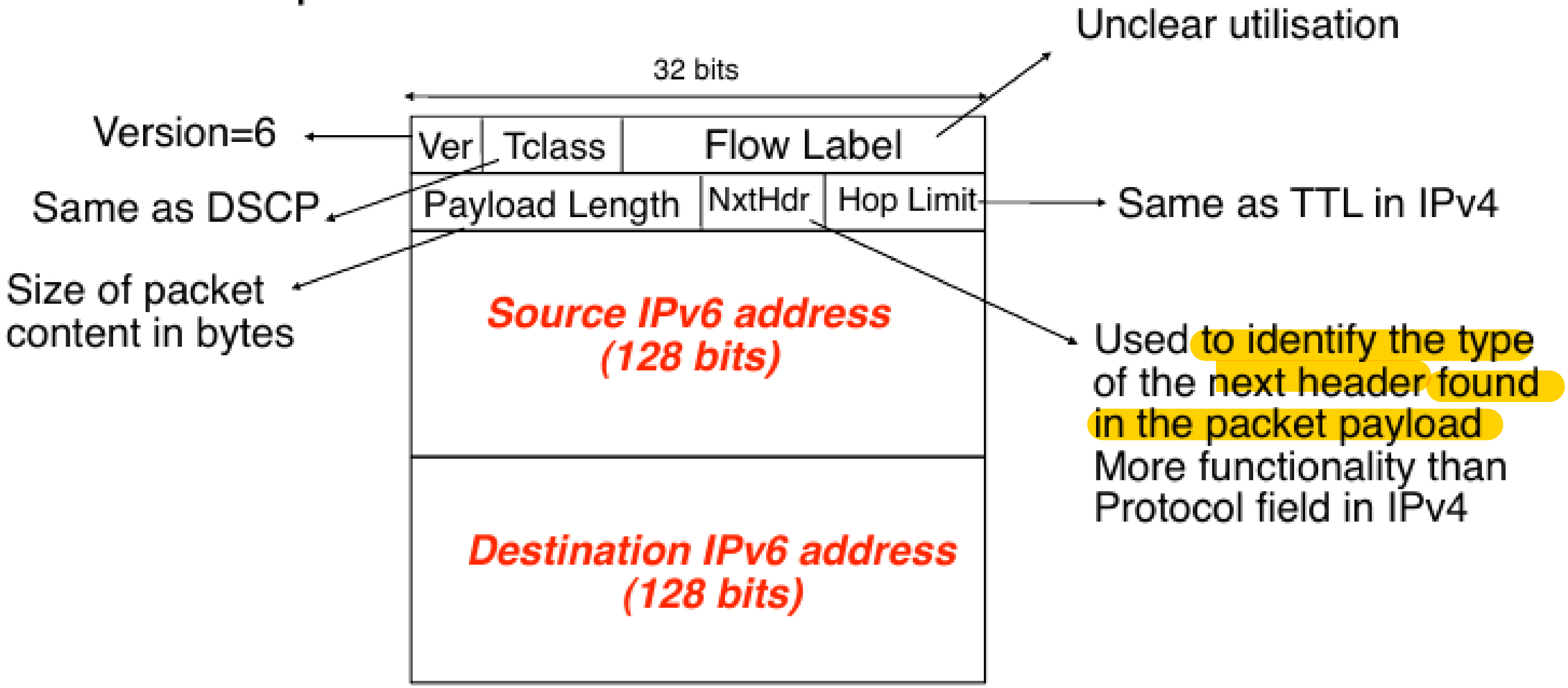
All endsystem automatically belong to the FF02::1 group

All routers automatically belong to the FF02::2 group

IPv6 Paquet Format

Simplified packet format

Fields aligned on 32 bits boundaries to ease implementation



Unclear utilisation

32 bits

Version=6

Same as DSCP

Size of packet content in bytes

Ver	Tclass	Flow Label	
Payload Length		NxtHdr	Hop Limit

Same as TTL in IPv4

Source IPv6 address (128 bits)

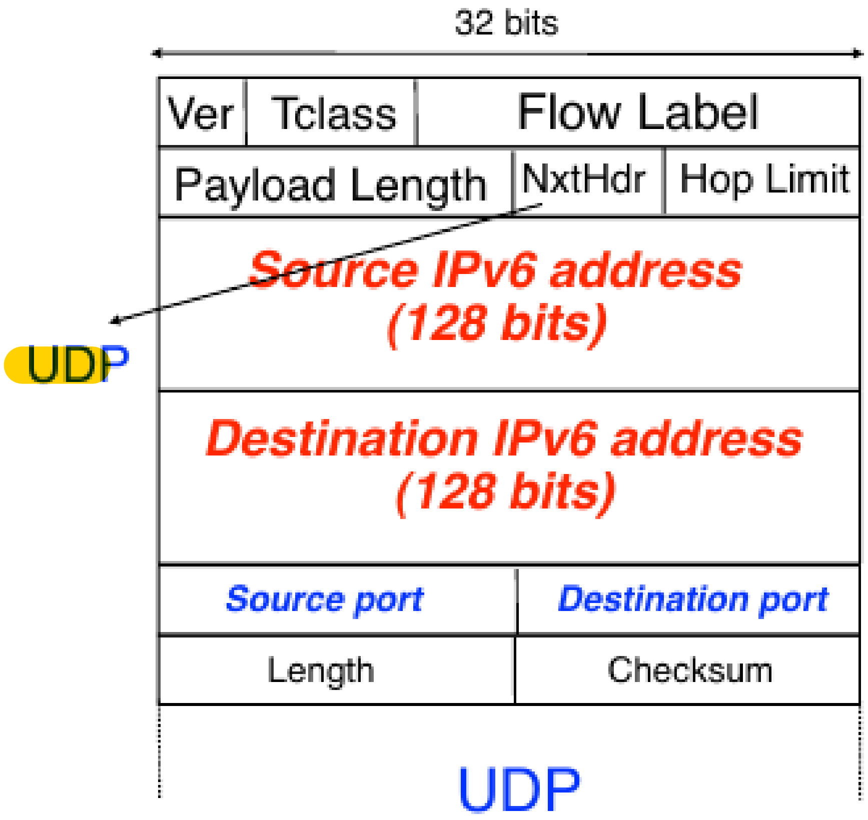
Destination IPv6 address (128 bits)

Used to identify the type of the next header found in the packet payload

More functionality than Protocol field in IPv4

No checksum in IPv6 header

IPv6 Paquet example



32 bits

Ver | Tclass | Flow Label

Payload Length | NxtHdr | Hop Limit

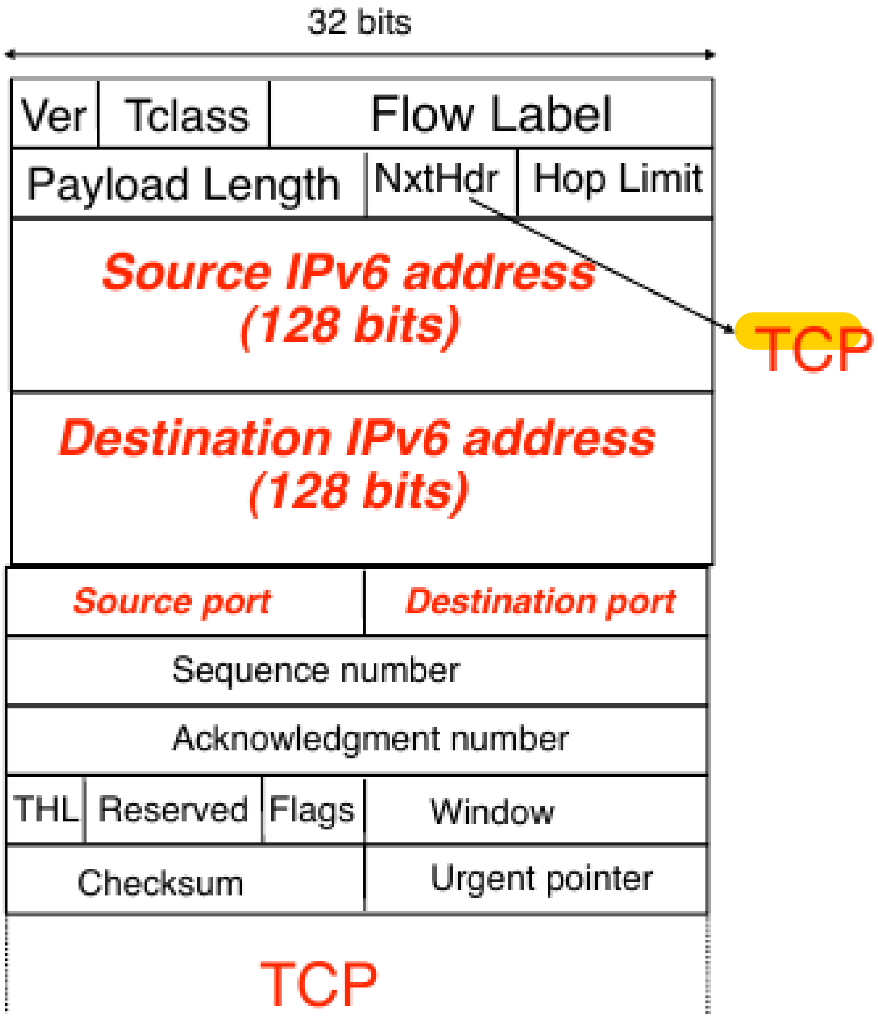
Source IPv6 address (128 bits)

Destination IPv6 address (128 bits)

Source port | Destination port

Length | Checksum

UDP



32 bits

Ver | Tclass | Flow Label

Payload Length | NxtHdr | Hop Limit

Source IPv6 address (128 bits)

Destination IPv6 address (128 bits)

Source port | Destination port

Sequence number

Acknowledgment number

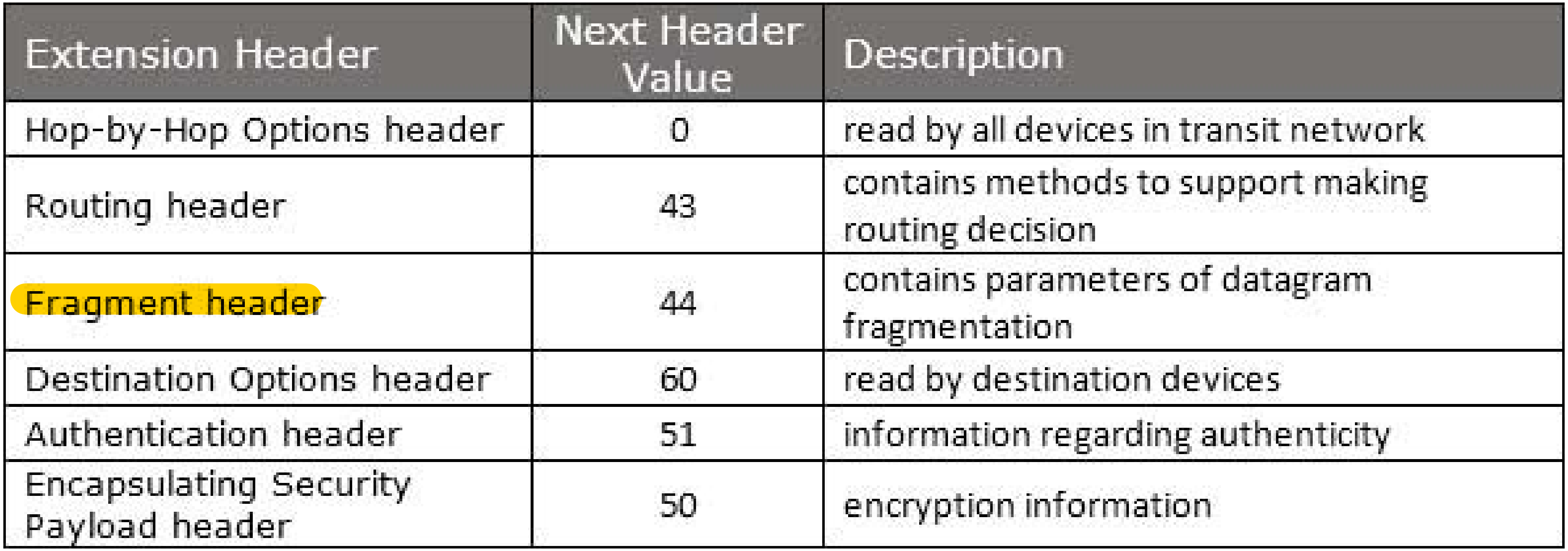
THL | Reserved | Flags | Window

Checksum | Urgent pointer

TCP

IPv6 Extension Headers

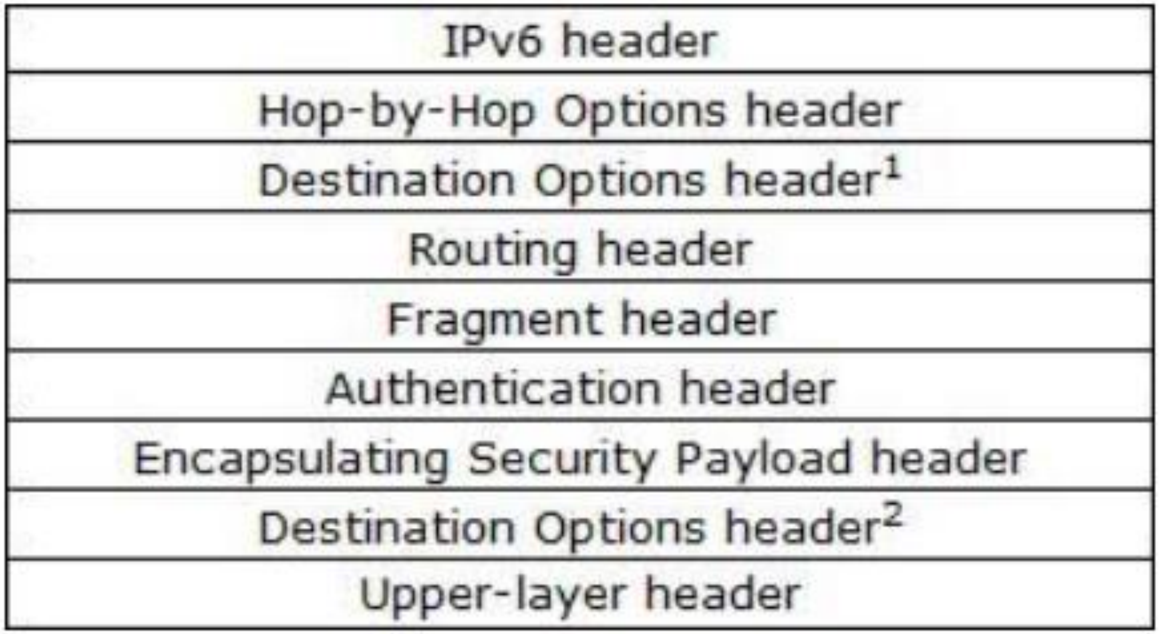
As you can see, The IPv6 fixed header is short. IPv6 supports header extensions, that hold more info.



Extension Header	Next Header Value	Description
Hop-by-Hop Options header	0	read by all devices in transit network
Routing header	43	contains methods to support making routing decision
Fragment header	44	contains parameters of datagram fragmentation
Destination Options header	60	read by destination devices
Authentication header	51	information regarding authenticity
Encapsulating Security Payload header	50	encryption information

IPv6 Extension Headers

The sequence of Extension Headers should be:



IPv6 header
Hop-by-Hop Options header
Destination Options header[1]
Routing header
Fragment header
Authentication header
Encapsulating Security Payload header
Destination Options header[2]
Upper-layer header

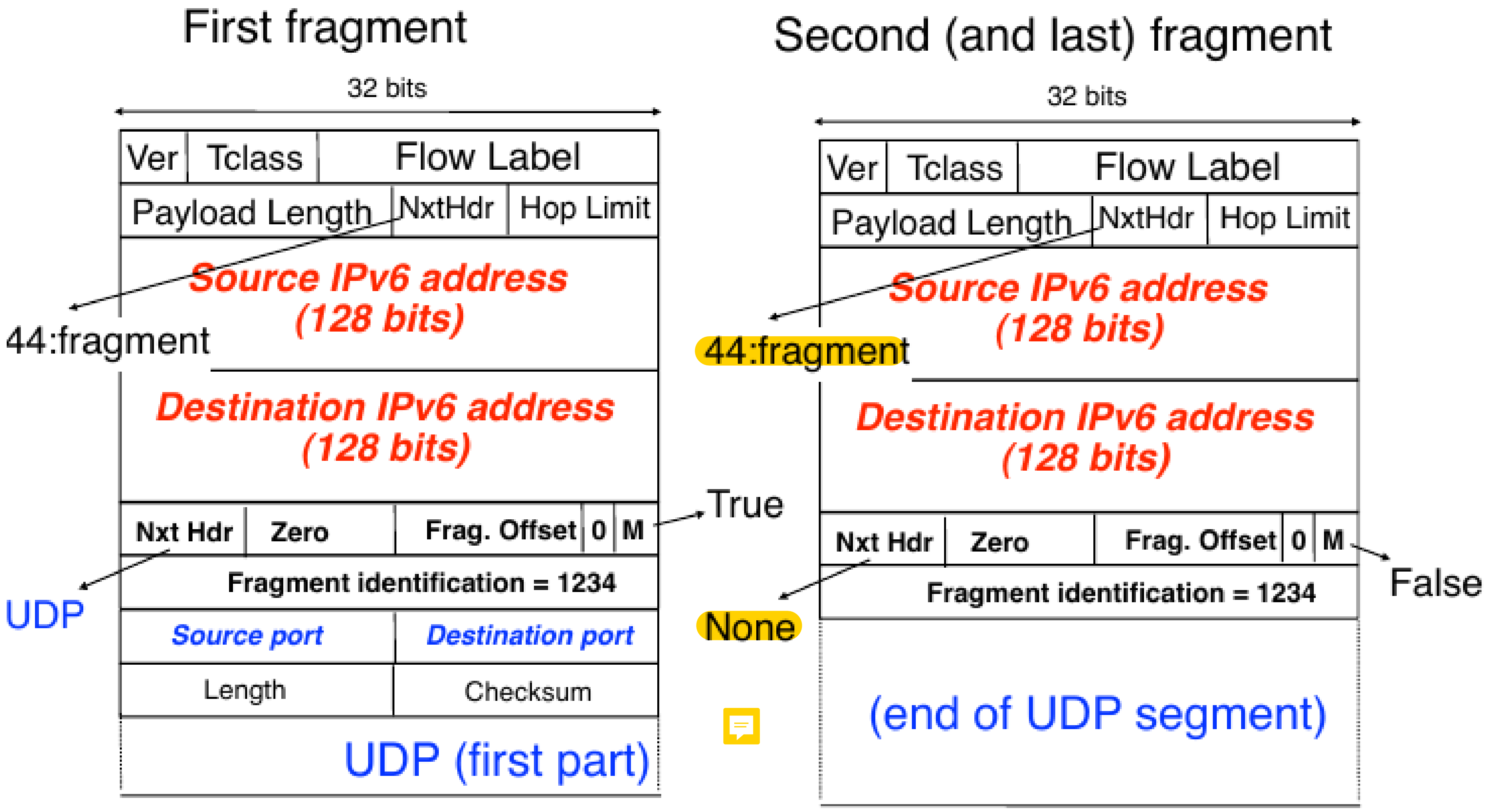
IPv6 Paquet Fragmentation

- IPv4 used packet fragmentation on routers
  - All hosts must handle 576+ bytes packets
  - experience showed fragmentation is costly for routers and difficult to implement in hardware
  - PathMTU discovery is now widely implemented
- IPv6
  - IPv6 requires that every link in the internet have an MTU of 1280 octets or more
    - otherwise link-specific fragmentation and reassembly must be provided at a layer below IPv6
  - Routers do not perform fragmentation
    - Only end hosts perform fragmentation and reassembly by using the fragmentation header
    - But PathMTU discovery should avoid fragmentation most of the time

Path MTU Discovery

- The approach is to send packets with the Don’t-Fragment-bit set. Where a router on the path is unable to forward the packet because it is too large for the next hop, the Don’t Fragment field directs the router to discard the packet and send a Destination Unreachable ICMP message with a code of “Fragmentation Required and DF set” to the source, thus informing it of the MTU (Maximum Transmition Unit).
- If the source node does not perform PMTU discovery, it must send packets no larger than the minimum IPv6 MTU size of 1,280 bytes.

IPv6 Paquet Fragmentation



First fragment

32 bits

Ver	Tclass	Flow Label		
Payload Length		NxtHdr	Hop Limit	

Source IPv6 address (128 bits)

Destination IPv6 address (128 bits)

Nxt Hdr	Zero	Frag. Offset	0	M

Fragment identification = 1234

Source port	Destination port
Length	Checksum

UDP (first part)

44:fragment

UDP

True

Second (and last) fragment

32 bits

Ver	Tclass	Flow Label		
Payload Length		NxtHdr	Hop Limit	

Source IPv6 address (128 bits)

Destination IPv6 address (128 bits)

Nxt Hdr	Zero	Frag. Offset	0	M

Fragment identification = 1234

(end of UDP segment)

44:fragment

None

False

IPv6 Jumbograms

- In IPv4, the max MTU is 1500 bytes
- In IPv6, the ‘lenght’ field of the standard header is 16 bits longs, which allows for a maximum MTU of 65 536 bytes.
- Jumbograms are IPv6 paquets bigger than 65 536 bytes. IPv6 jumbograms are defined as an IPv6 hop-by-hop option (in the extension header), called the “Jumbo Payload” option, that carries a 32-bit length field in order to allow transmission of IPv6 packets with payloads between 65,536 and 4,294,967,295 bytes (almost 4Gb).
- Routers and links must be able to support this to use it.

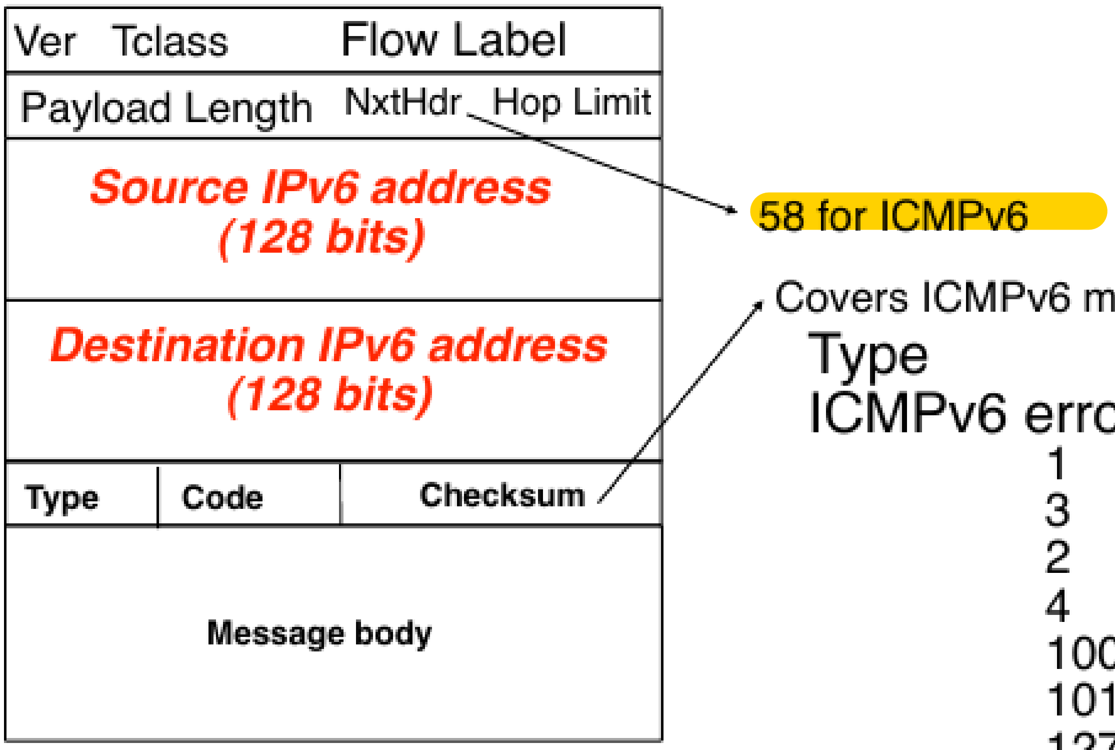
ICMPv6

Provides the same functions as ICMPv4, and more

Types of ICMPv6 messages

- Destination unreachable
- Packet too big
  - Used for PathMTU discovery
- Time expired (Hop limit exhausted)
  - Traceroute v6
- Echo request and echo reply
  - Pingv6
- Multicast group membership
- Router advertisments
- Neighbor discovery
- Autoconfiguration

ICMPv6



Covers ICMPv6 message and part of IPv6 header

Type

ICMPv6 error messages (0<type<127)

1	Destination Unreachable
3	Time Exceeded
2	Packet Too Big
4	Parameter Problem
100	Private experimentation
101	Private experimentation
127	Reserved for expansion

ICMPv6 informational messages:

128	Echo Request
129	Echo Reply
200	Private experimentation
201	Private experimentation
255	Reserved for expansion

Neighbor Discovery Protocol

- ARP, translates MAC address to IP address. Uses broadcasts (not possible in IPv6).
- DHCP, gives IP address to the machines on the network that request it.
- Since an IPv6 is composed of the MAC address and subnet, a newly connected machine could auto-configure its IPv6 (network + subnet + MAC).
- Uses ND protocol to advertise/choose an IP

Neighbor Discovery Protocol – Setting the IP

Neighbor Solicitation: After configuring his IPv6's either manually, or by DHCP Server or by auto-configuration, the host sends a Neighbor Solicitation message out to FF02::1/16 multicast address for its IPv6 addresses in order to know that no one else occupies the same addresses. When the host does not hear anything back regarding its Neighbor Solicitation message, it assumes that no duplicate address exists on the segment.

- **Neighbor Advertisement**: After assigning the addresses to its interfaces the host sends out a Neighbor Advertisement message telling all other hosts on the segment that it has assigned those IPv6 addresses to its interfaces.

ND Protocol – Getting a router/gateway

- **Router Solicitation**: A host sends a Router Solicitation multicast packet out to know the presence of any router on this segment. It helps the host to configure the router as its default gateway.
- **Router Advertisement:** When a router receives a Router Solicitation message, it response back to the host, advertising its presence on that link.

IPv4 to IPv6 Transition

- IPv6 is not backwards compatible. A domain/network either uses one or the other.
- Solutions:
  - Dual-stack routers
  - Tunneling (ISATAP, Teredo, 6over4 or 4over6)
  - NAT-PT (Network Address Translation – Protocol Translation), already obsolete. DSTM is the new sexy.

IPv6 secuirty and privacy concerns

secuirty and privacy concerns

Food for thought

- Why is the EU/US slower to adopt IPv6 than the rest of the world, for example Asia?
- Compare the ipv6 header and the ipv4 header, and for each field that is different in IPv6 (added, removed, new), explain what is/was it used for.

Questions