1.4. IPv6

PROFESSORS:

Rubén Santiago Montero

Eduardo Huedo Cuesta

OTHER AUTHORS:

Rafael Moreno Vozmediano

Juan Carlos Fabero Jiménez

Introduction: IPv4 Limitations

- Very limited addressing 10^9
  - Limited address space (32 bit addresses, ~4K millions)
  - Partial solutions:
    - Classless addressing (CIDR)
    - Private addresses and translation (NAT)
    - Dynamic addresses (DHCP)
- Complex format of the packet header
  - Variable length (option field)
  - Fragmentation information (not always needed)
- Limited security
  - No support for confidentiality or authentication
  - Solution: IPsec
- Limited support for traffic priority or service class
  - Functionality not implemented in most routers
- Limited multicast
  - Not get to be used in a full and effective way

Introduction: IPv6 Characteristics

- 128-bit addresses
  - Much bigger address space ($3.4 \cdot 10^{38}$ addresses)
- Simpler header format
  - Higher processing speed in routers
  - Improved performance of routing protocols
- Address auto-configuration capability
- Better support for additional options
  - IPv6 options are not codified in the header, but in the packet body by means of extension headers
  - More space available to codify options
  - More options can be introduced in the future
- Security options, both for authentication and encryption
- Support for real time traffic (e.g. VoIP)
- Hierarchical routing based on prefixes
- Mechanisms for transition from IPv4

Introduction: IPv4 vs. IPv6

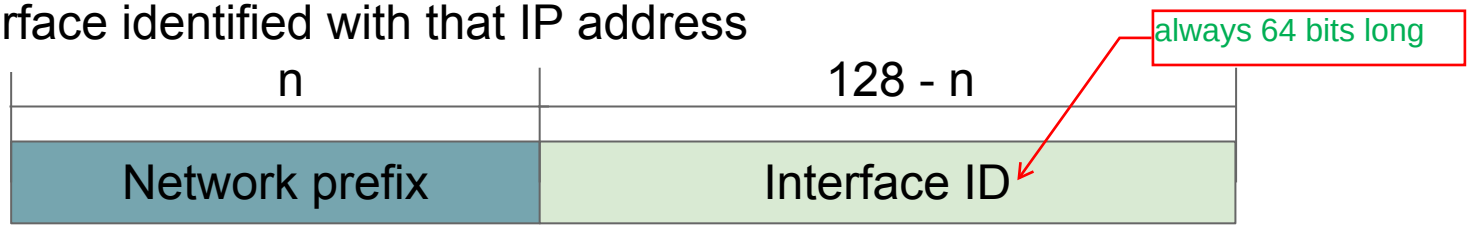
Characteristic	IPv4	IPv6
Address length	32 bits	128 bits
Address classes	Class A, B and C or CIDR	Classless
Address types	Unicast, Multicast, Broadcast	Unicast, Multicast, Anycast
Address configuration	Static (configuration files) or by DHCP	Static (configuration files), autoconfiguration (plug and play) or by DHCP
Header format	Complex. Variable length	Simple. Fixed length
Quality of service	Yes, but not fully supported by all routers	Yes
Real time traffic support	No	Yes
Security	No (IPsec extension)	Yes

Addressing

IPv6 Addresses: Address Types

Unicast

- They identify a single network interface
  - A packet addressed to a unicast address will be delivered only to the interface identified with that IP address



Multicast

- They identify a group of interfaces (assigned to more than one interface)
  - A packet addressed to a multicast address will be delivered to all interfaces identified with that IP address
- There is no broadcast address in IPv6, but a special multicast address

Anycast

- They identify a group of interfaces (assigned to more than one interface)
  - A packet addressed to an anycast address will be delivered to only one of the interfaces identified with that IP address, typically the nearest one, according to the routing protocol's definition of distance
- Assigned from the unicast address space

IPv6 Addresses: Notation

- Addresses are 128 bit (16 bytes) long
- Hexadecimal notation
  - Written as 8 groups of 4 hexadecimal digits (16 bits)
  - Groups are separated by colons (`:`)

    `FDEC:BA98:7654:3210:0123:4567:89AB:CDEF`

    `FE80:0000:0000:0000:0008:0800:200C:741A`
- Abbreviated notation
  - Leading zeroes in a group may be omitted

    `0000` → `0`

    `0074` → `74`
  - One consecutive group of zeros may be replaced with two colons (`::`)

    `FE80:0:0:0:8:800:200C:741A` → `FE80::8:800:200C:741A`
  - This two-colon replacement may only be applied once in an address

    `21AB:0:0:A:0:0:1234:5678` →

    `21AB::A::1234:5678` (incorrect, ambiguous)

    `21AB::A:0:0:1234:5678` (correct)

IPv6 Addresses: CIDR Notation

- IPv6 addresses are classless to support hierarchical addressing
- Divided in prefix and suffix
- Prefix length is denoted in CIDR notation
- Examples:

  `FDEC:BA98:7654:3210:0123:4567:89AB:CDEF/64`
  `FC80:0:0:0:8:800:200C:741A/64`

IPv6 Addresses: Scopes (RFC 4007)

- **Scope**: Specifies in which part of the network the address is valid
  - **Link-local**: The address is valid in the link where the network interface is directly attached (e.g. a LAN)
  - **Site-local (deprecated)**: The address is valid within a site, which can comprise one or more networks interconnected by routers (e.g. university campus)
  - **Global**: The address is valid in all the Internet
- **Scope zone**: Connected region of topology of a given scope
  - Address unicity is only guaranteed inside a scope zone
- Packets are never routed outside the address zone
- In case of ambiguity, zone indices are used: **<address>%<zone_id>**, e.g. `fe80::1234%1`
- Multicast addresses define their scope in a 4-bit field, e.g. interface-local (1), link-local (2), global (E)

IPv6 Addresses: Structure

- IPv4 has a one-level structure (network and host)
- IPv6 allows a flexible hierarchy, that accommodates different address types
- Each address type starts with a prefix (format prefix) of variable length

Address type	**FP (bin)**	**FP (hex)**
Reserved Address	`0000 0000`	`0000::/8`
Global Unicast Address	`001`	`2000::/3`
Link-Local Unicast Address	`1111 1110 10`	`FE80::/10`
Site-Local Unicast Address (deprecated)	`1111 1110 11`	`FEC0::/10`
Unique Local Address (ULA)	`1111 110`	`FC00::/7`
Multicast Address	`1111 1111`	`FF00::/8`

IPv6 Addresses: Link Local Unicast

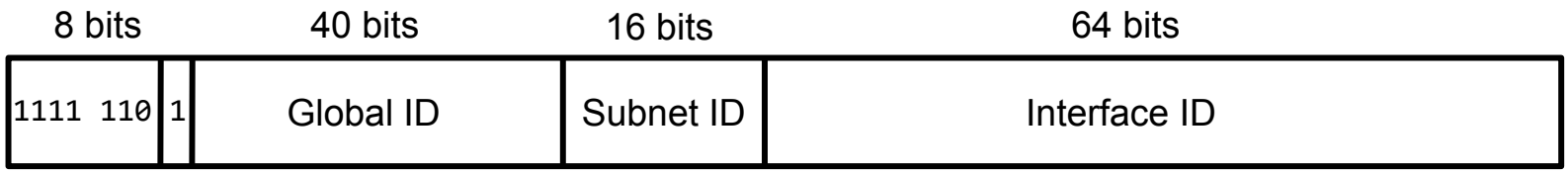
- Private unicast addresses allocated to a network link
- A link-local zone consists of a single link and all the interfaces attached to that link
- Never routed out of the link scope zone
- Plain address space
- Main use is autoconfiguration and neighbor discovery
- Format:
  - Format prefix (10 bits): `fe80::/10` (`1111 1110 10`)
  - Next 54 bits set to 0
  - Interface ID (64 bits)
- Example:

  `fe80::2e81:58ff:fee9:64bb/64`

IPv6 Addresses: Unique Local Unicast

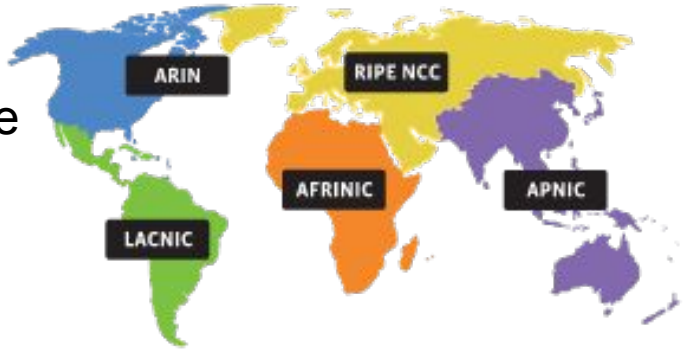
- Unique Local Addresses, defined in RFC 4193 to replace deprecated site-local addresses (RFC 3879)
- Private unicast addresses that can be used and routed in hierarchical intranets, but cannot be routed in the global IPv6 Internet
- They support autoconfiguration
- Format:
  - Format prefix (7 bits): `fc00::/7`
  - L bit: set to 1 if prefix is locally assigned (0 may be defined in the future)
  - Global ID (40 bits): For L=1, pseudo-randomly generated to avoid collisions
  - Subnet ID (16 bits): 65,536 subnets allowed per site, to create the internal network structure
  - Interface ID (64 bits)
- Example:

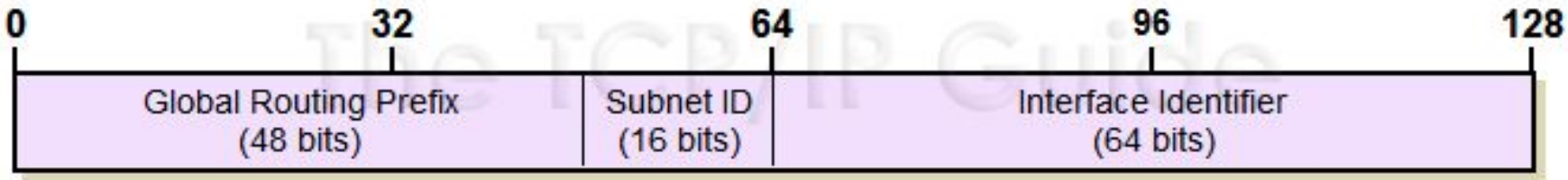
  `fd12:A128:e8e1:1:FEDC:BA98:7865:4321/64`



IPv6 Addresses: Global Unicast

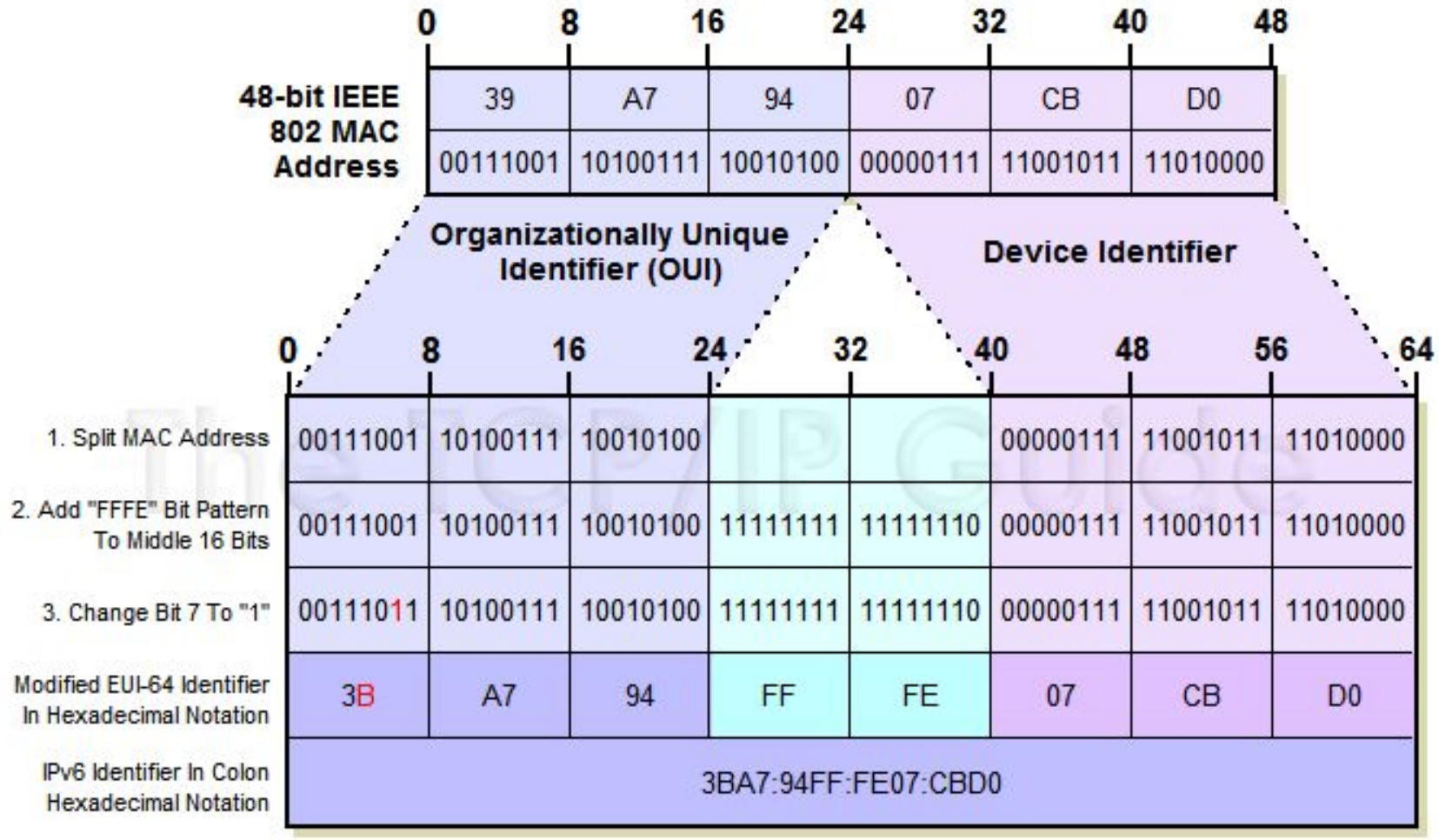
- Global unicast addresses, defined in RFC 3587
- They support autoconfiguration
- Format:
  - Global routing prefix (48 bits): Currently, IANA is assigning the `2000::/3` range (i.e. the first three bytes are `001`), allowing 2^{45} different sites
    - This prefix is the only relevant part in global routing, and can be further subdivided according to the needs of RIRs and LIRs (Regional/Local Internet Registries)
  - Subnet ID (16 bits): 65,536 subnets allowed per site, to create the internal network structure
  - Interface ID (64 bits)
- Example:
  `2004:A128::32:FEDC:BA98:7865:4321/64`





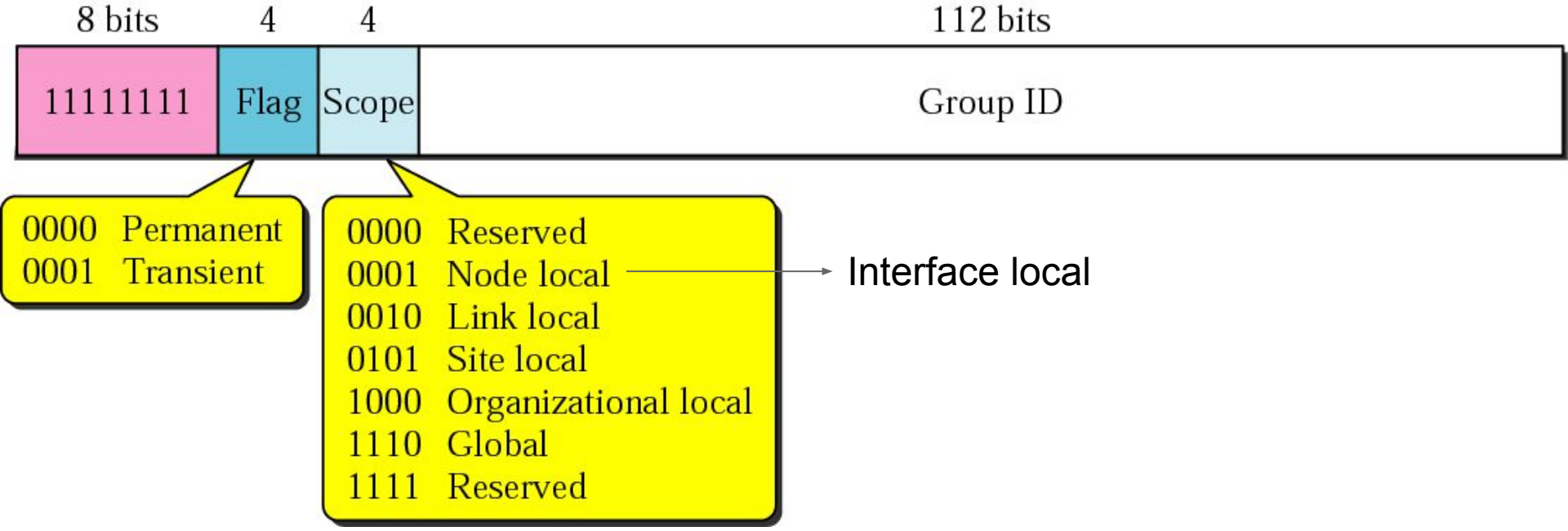
IPv6 Addresses: Interface ID

- The IEEE Modified EUI-64 (64-bit Extended Unique Identifier) format is used for the 64 less significant bits
- Network IP address related to the link MAC (EUI-48) address
  - This may pose a privacy problem for clients, as they can be tracked



IPv6 Addresses: Multicast

- Multicast addresses, defined in RFC 3306 to specify a group of hosts in a given scope
- Format:
  - Format prefix (8 bits): `FF::/8`
  - Flags (4 bits): to indicate if the address is permanent (i.e. defined by IANA) or transient for a communication (e.g. group of host in a teleconference)
  - Scope (4 bits)
  - Group ID (112 bits)



IPv6 Addresses: Multicast

- Addresses for hosts:

Address	Scope	Meaning
`FF01::1`	Interface local	Datagram sent to one interface in the node
`FF02::1`	Link local	Datagram sent to all interfaces in the local link, but it is not forwarded to other local subnetworks through internal routers

- Addresses for routers:

Address	Scope	Meaning
`FF02::2`	Link local	Datagram sent to all routers in the local link
`FF02::5`	Link local	Datagram sent to all OSPF routers in the local link
`FF02::9`	Link local	Datagram sent to all RIP routers in the local link

IPv6 Addresses: Multicast

- **Solicited-node multicast address** is used in the neighbor discovery protocol
- Calculated from the unicast address of the node (interface ID):
  `FF02:0:0:0:0:1:FF00::/104` + 24 less significant bits of the address
- Address range:
  `FF02:0:0:0:0:1:FF00:0000 - FF02:0:0:0:0:1:FFFF:FFFF`
- Example:
  Unicast address: `2037::1:800:200E:8C6C`
  Solicited-node multicast address: `FF02::1:FF0E:8C6C`

IPv6 Addresses: Other Addresses

- Unspecified address: `0:0:0:0:0:0:0:0` (`::`)
  - To indicate that the interface has no address assigned
- Loopback address: `0:0:0:0:0:0:0:1` (`::1`)
  - Analogous to IPv4 loopback address `127.0.0.1`
- Mapped IPv4 addresses:
  - To be used in architectures merging IPv4 and IPv6 stacks
  - Format:

    `::FFFF:<IPv4>`
  - Example:

    `::FFFF:192.02.13.123` (mixed notation)

How many IPv6 addresses does a host have?

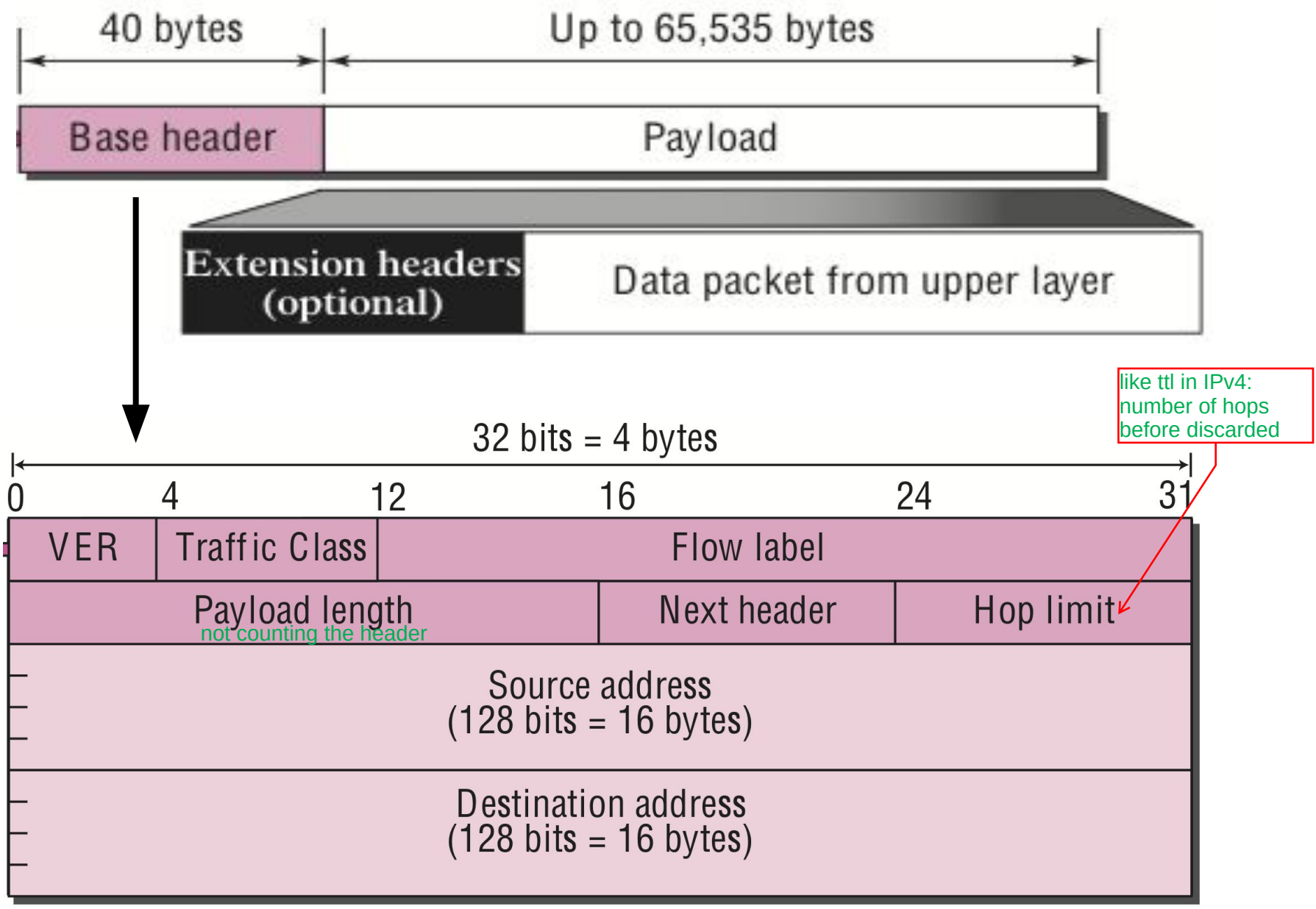
- Link local address for each interface
- Unicast or anycast addresses configured for each interface
- Loopback address

Also, it answers to the following multicast addresses:

- All nodes multicast addresses
- Solicited-node multicast address for each address configured
- Multicast addresses of other groups the host belongs to

Datagram

IPv6 Datagram: Format



IPv6 Datagram: Format

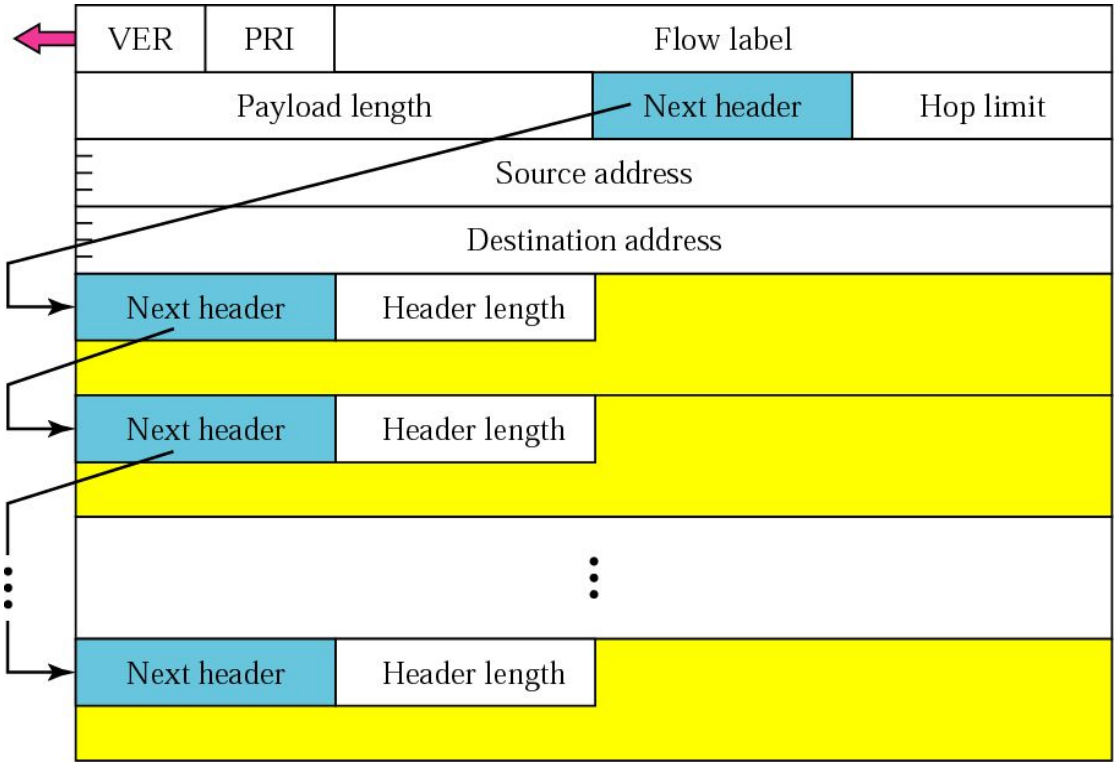
- **Version** (4 bits)**:** 6
- **Traffic Class** (8 bits): To establish different delivery requirements for the datagram, similar to the DS/ToS field in IPv4
  - DSCP (Differentiated Services Code Point, 6 bits): Traffic classification into groups with different QoS requirements
  - ECN (Explicit Congestion Notification, 2 bits): To allow routers to notify network congestion without dropping packets
- **Flow Label** (20 bits): To specify that the packet belongs to a specific sequence of packets, to improve the processing by network routers and avoid reordering
  - A flow shares the same characteristics (source/destination, requirements…)
  - Used for real time and reservation protocols (RTP/RSVP)
- **Payload Length** (16 bits): 64 Kbytes maximum
- **Hop Limit** (8 bits): Similar to the TTL field in IPv4
- **Source and Destination Addresses** (128 bits)

not very used, it's mostly experimental

IPv6 Datagram: Format

- **Next Header** (8 bits): To define the next header in the datagram, which can be:
  - A IPv6 extension header, similar to the Options field in IPv4
  - The header of the upper layer protocol, encapsulated in the data section (6=TCP, 17=UDP, 58=ICMP…)

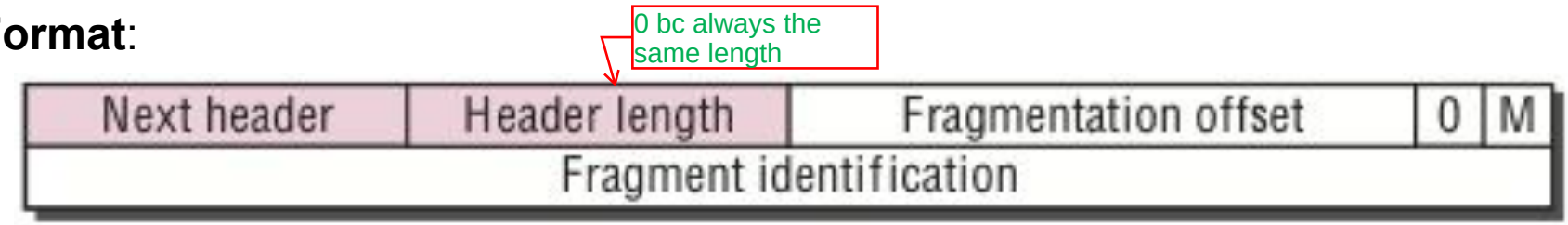
Code	Next Header
0	Hop-by-hop Options
43	Routing
44	**Fragment**
50	Encapsulating Security Payload
51	Authentication
59	Null (no next header)
60	Destination Options



  - Header length (8 bits): length in 8-byte units

IPv6 Datagram: Fragmentation Header

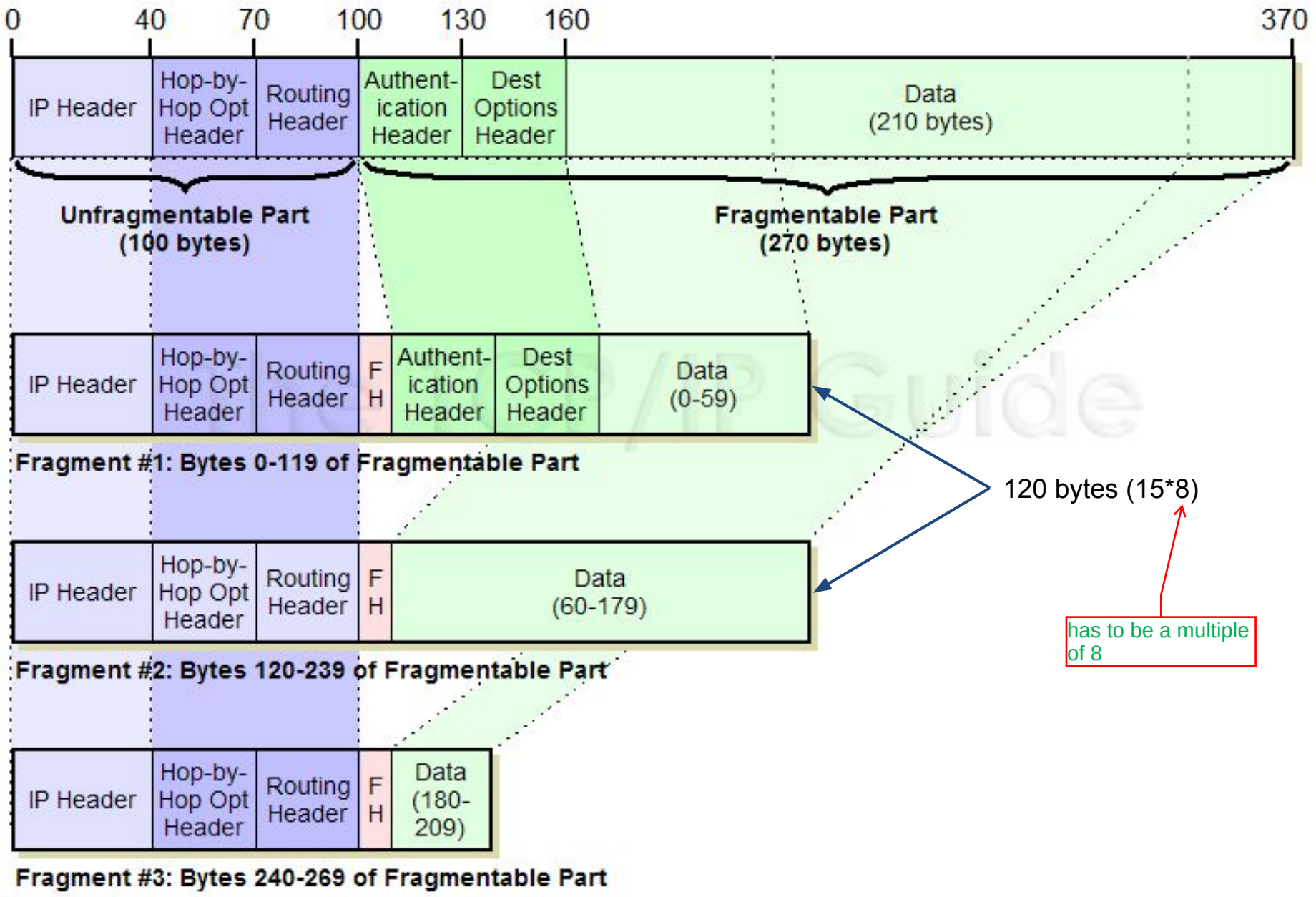
- In IPv6, fragmentation is always done at origin (routers never fragment)
  - It is strongly recommended that IPv6 nodes implement Path MTU Discovery (PMTUD, RFC 1981), in order to discover and take advantage of path MTUs (the minimum link MTU of all the links in the path) greater than 1280 octets (the minimum MTU for links conveying IPv6, while 1500 is recommended)
  - The upper-layer protocol is expected to limit the payload size according to the path MTU. However, if it is unable to do so and generates a packet that is larger than the path MTU, the sender will split the packet into fragments
- **Format**:



  - **Header length** (8 bits): Reserved, set to 0s
  - **Offset** (13 bits): The offset, in 8-byte units, of the data following this header, relative to the start of the Fragmentable Part of the original packet (i.e. the offset of the first fragment is 0)
  - **M**: Flag indicating if there are more fragments or not
  - **Identification**: Number identifying fragments belonging to the same datagram

IPv6 Datagram: Fragmentation

MTU=230 Bytes



IPv6 Datagram: IPv4 Comparison

- The Header Length field is removed, since header length is fixed
- The ToS field is replaced by Traffic Class field (in IPv4, it was also replaced by the Differentiated Services field)
- The Flow Label field is added still not used
- The Payload Length field does not include the header
- The TTL field is replaced by the Hop Limit field mostly the same
- The Checksum field is removed, since it is done by upper layer protocols
- The Option field is replaced by extension headers in payload not in header
- The Identification, Flag and Offset fields, for fragmentation, are removed from the header and included in a Fragmentation extension header, if needed
- The Protocol field is replaced by the Next Header field ^last

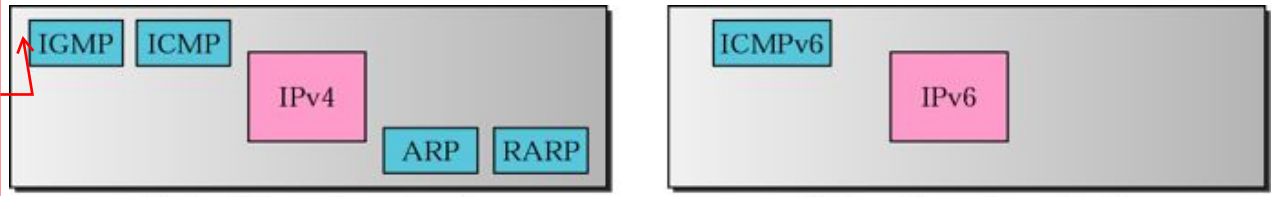
bc fragmentation should be avoided when possible

ICMPv6

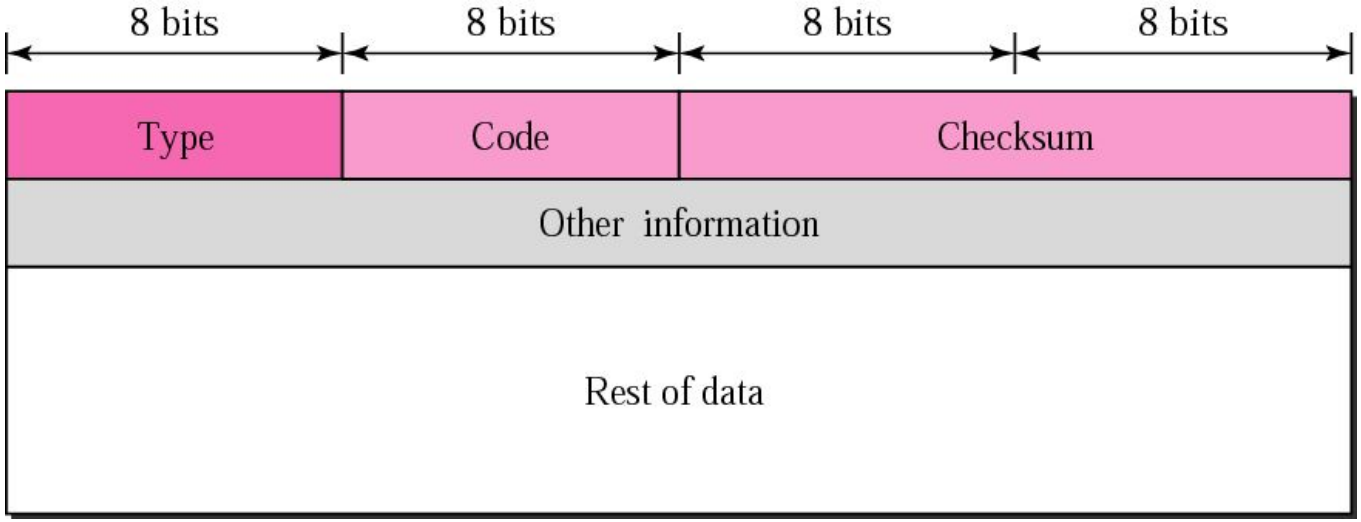
Introduction

- ICMPv6 (RFC 4443), or ICMP for IPv6, takes the role of several IPv4 protocols:

internet group management protocol: to subscribe to a multicast addres and create a temporary multicast group

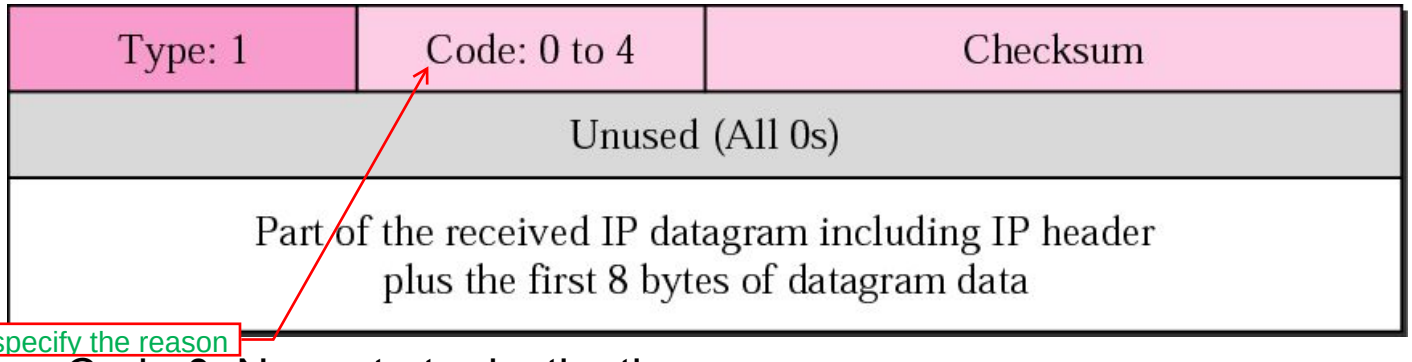


- Message-oriented protocol
  - Error messages
  - Informational messages
  - Neighbor Discovery (ND) protocol (RFC 4861), similar to ARP
  - Multicast Listener Discovery (MLD) protocol (RFC 3810), similar to IGMP
- All ICMPv6 messages have a common format:



Error Messages

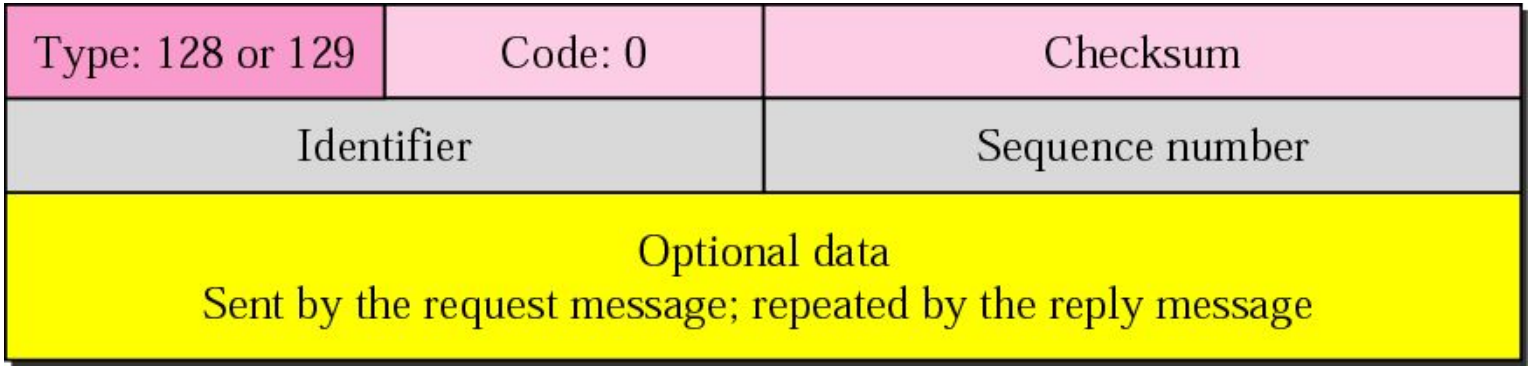
- To indicate an error condition (types from 0 to 127):
  - Destination unreachable (1)
  - Packet too big (2) → Path MTU Discovery (includes the MTU)
  - Time exceeded (3)
  - Parameter problem (4)
- Example: Destination unreachable
  - If a packet cannot be delivered to its destination address (for reasons other than congestion), the datagram is discarded and an ICMP message is sent



    - Code 0: No route to destination
    - Code 1: Communication with destination administratively prohibited
    - Code 2: Beyond scope of source address
    - Code 3: Address unreachable
    - Code 4: Port unreachable
    - Code 5: Source address failed ingress/egress policy
    - Code 6: Reject route to destination

Informational Messages

- To provide diagnostic information (types from 128 to 255):
  - Echo request (128)
  - Echo reply (129)
- Format:



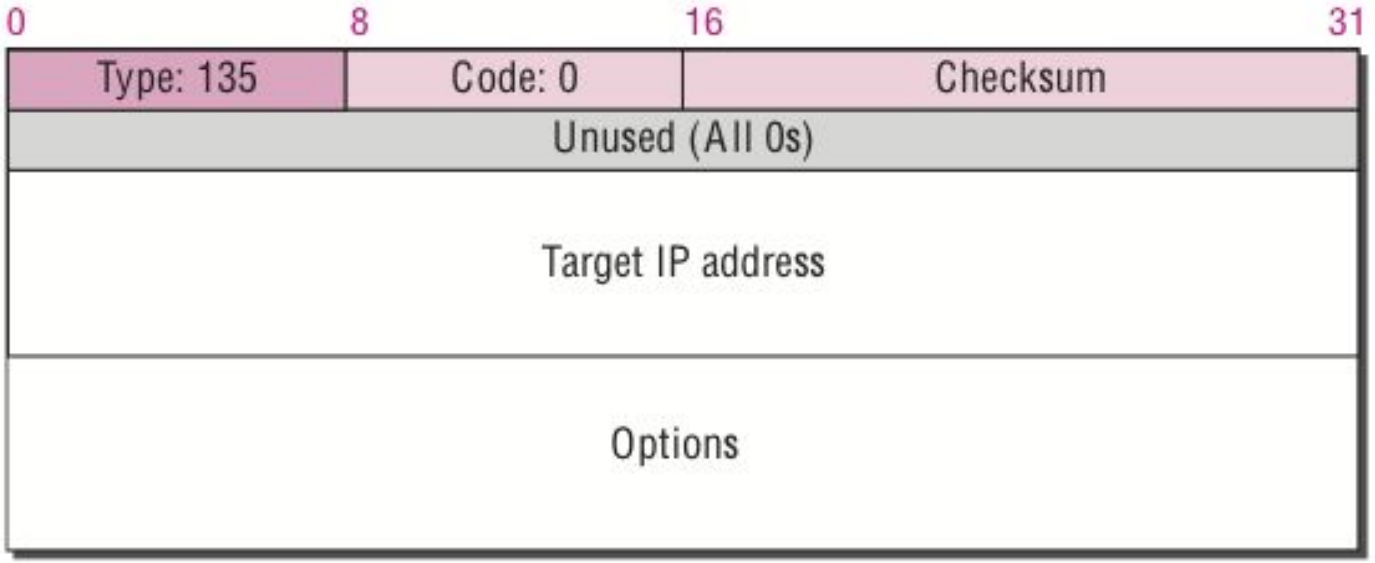
  - Identifier and Sequence number (16 bits): Used to match replies to request (actual numbers are implementation dependent)
  - Data: It must be copied in the reply

Neighbor Discovery Protocol

- Multifunction protocol that allows performing configuration operations
- It operates on hosts and routers in the same link
- **Neighbor Discovery**
  - Address resolution (equivalent to ARP in IPv4)
  - Detection of duplicate address
  - Detection of unreachable neighbor
  - Messages: Neighbor Solicitation (135) and Neighbor Advertisement (136)
- **Router Discovery**
  - Announcement of routers
  - Announcement of prefixes and other network configuration information
  - Messages: Router Solicitation (133) and Router Advertisement (134)
- **Redirection**
  - Notification of a more appropriate route to reach a given destination
  - Messages: Redirect (137)

Neighbor Solicitation

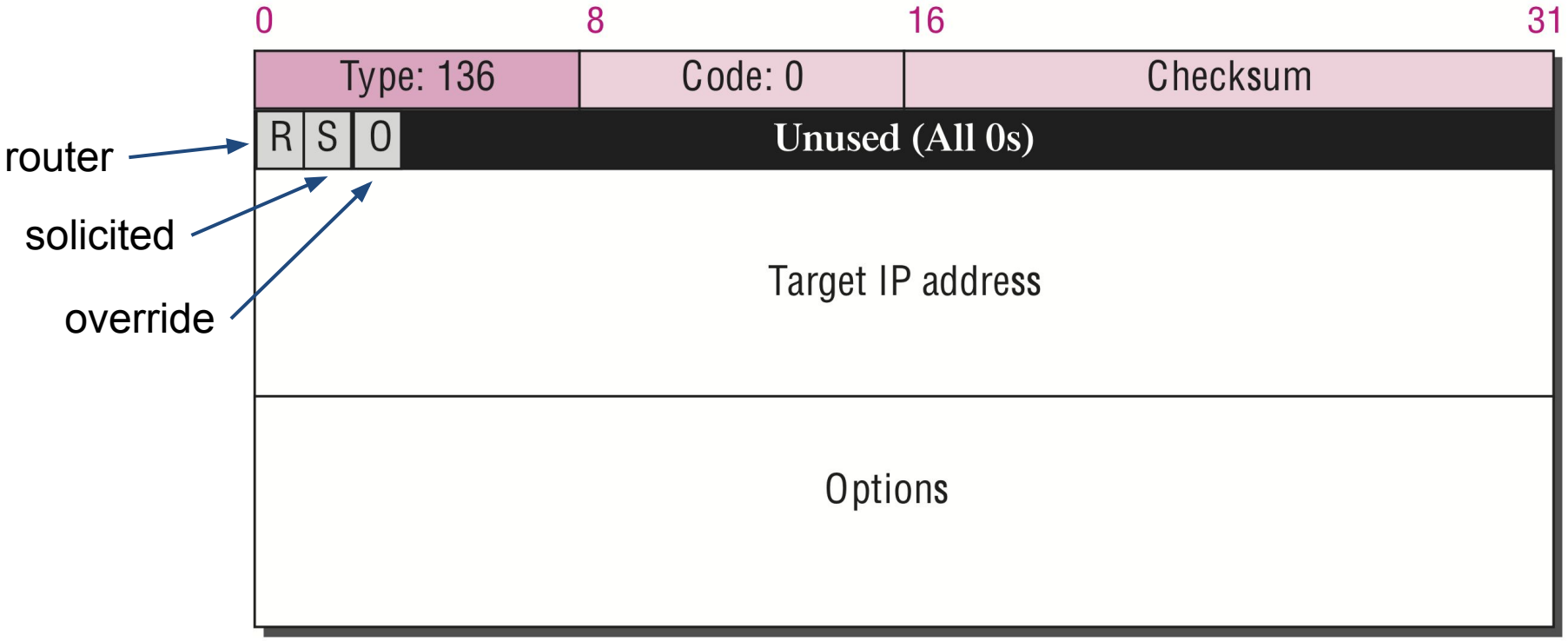
- This message is sent in the following situations:
  - To get the link-layer address associated to an IP address (similar to an ARP request in IPv4), with the multicast solicited-node address as destination
  - To determine if a neighbor host is still reachable, with the host's unicast address as destination
  - To detect if the IP address is already in use, during the autoconfiguration process
- Format:



  - Options: Source link-layer address (1)

Neighbor Advertisement

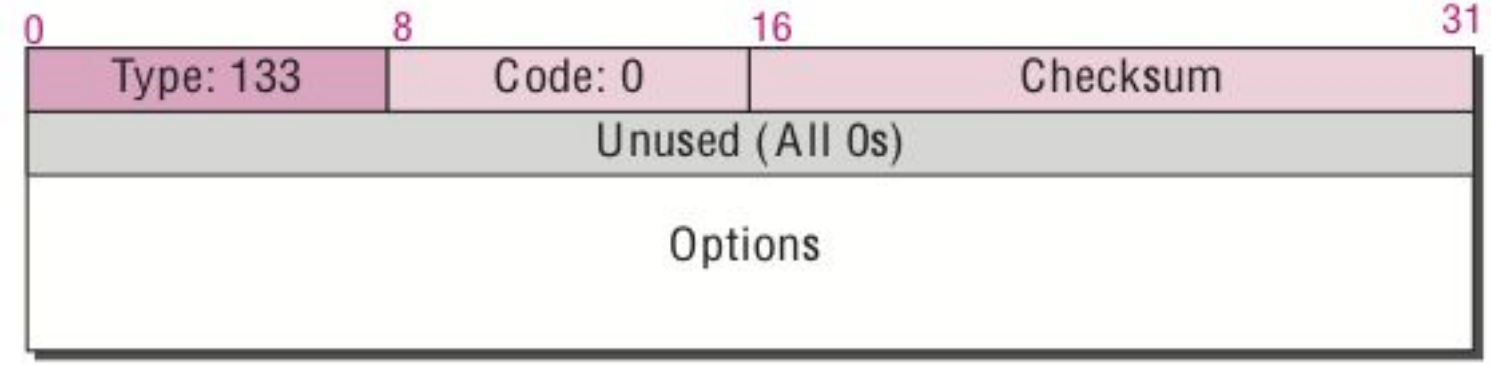
- This message is sent in the following situations:
  - To reply a Neighbor Solicitation message from a host (similar to an ARP reply in IPv4), with the host's unicast address as destination
  - To notify a change in the link-layer address of an interface, with multicast address `FF02::1` (all hosts, link local) as destination
- Format:



  - Options: Target link-layer address (2)

Router Solicitation

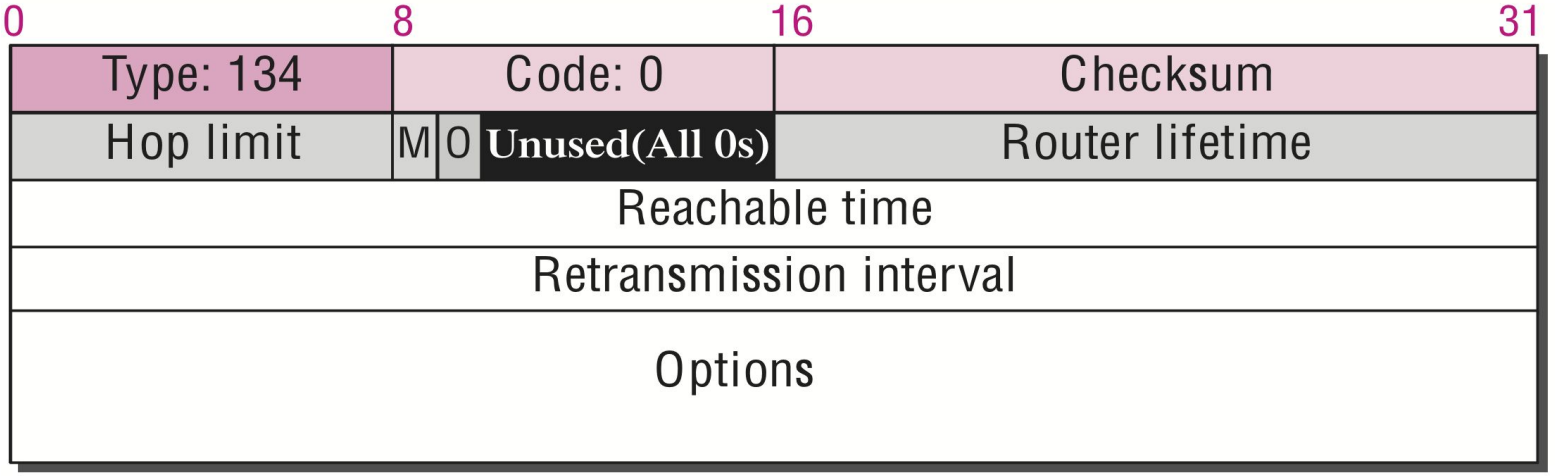
- This message is sent after an interface is enabled:
  - To quickly detect routers and perform autoconfiguration, with multicast address `FF02::2` (all routers, link local) as destination
- Format:



  - Options: Source link-layer address (1)

Router Advertisement

- This message is sent by routers to announce their presence in the network:
  - Periodically, with multicast address `FF02::1` (all hosts, link local)
  - To reply a Router Solicitation message from a host, with multicast address `FF02::1` as destination
    - They may also use the host's unicast address as destination
- Format:



  - M: Addresses are available via DHCPv6
  - O: Other configuration information is available via DHCPv6 (e.g. DNS or other servers)
  - Options: Source (i.e. router's interface) link-layer address (1), MTU (5) and prefix information (3)

Autoconfiguration

- StateLess Address AutoConfiguration (SLAAC)
- Interface autoconfiguration combines:
  - The Interface ID, generated according to the Modified EUI-64 format
  - The network prefix announced by the router
- Options in Router Advertisement messages can also include DNS information
- Privacy problems for clients → generation of pseudo-random temporary Interface IDs (privacy extensions, defined in RFC 4941)
- DHCPv6: DHCP for IPv6