Data Communication
(DC)

Lecture 8a

Overview of the contents

- **IPv6 Addressing**
- **IPv6 Protocol**
- **ICMPv6 Protocol**
- **Transition from IPv4 to IPv6**

IPv6 Addressing

Network Layer

IPv6 Addressing

The main reason for migration from IPv4 to IPv6 is **the address depletion of IPv4.**

IPv6 example:

Binary (128 bit)	**1111111011110110 ... 1111111100000000**
Hex-notation	**FEF6:BA98:7654:3210:ADEF:BBFF:2922:FF00**

Abbreviated notation:

FDEC:0:0:0:0:BBFF:0:FFFF	**->**	**FDEC::BBFF:0:FFFF**

A method of shortening a IPv6 address by eliminating 0s, for example:

- **0074** is written as **74**
- **000F** is written as **F**
- **0000** is written as **0**
- If multiple sections are **0000**, then they can be replaced by a double colon **::**

Note that only the leading 0s can be removed, not the trailing 0s.

Network Layer

IPv6 Addressing: **CIDR** (**C**lassless **I**nter-**D**omain **R**outing) notation

- IPv6 uses hierarchical addressing.
- Therefore, one can use CIDR notation. That is, IPv6 address consists of a prefix and a suffix.

An example of how we can define an IPv6 address with a prefix of 60 bits.

FDEC::BBFF:0:FFFF/60

Network Layer

IPv6 Address space

IPv6 has a very large address space: 2^{128} addresses. This address space is 2^{96} times the IPv4 address space

$$3{,}40282366920938463463374607431 77e+38$$

Definitely no address depletion anymore!

Network Layer

IPv6 Three types of addresses

In the IPv6 address system, a destination address can belong to one of the following three types:

- Unicast
- Anycast
- Multicast

Unicast: Such an address defines a single interface (computer or router). The packets sent to a unicast address are sent to only one receiver.

Anycast: Such an address defines a group of computers that all share one address. A packet sent to anycast address is only delivered to one member of the group, the easiest one to reach.

- Anycast communication is used e.g., when multiple servers can respond to an inquiry.
- The request is sent only to the one who is easiest to reach.
- Hardware and software generate only one copy of the request.
- This copy reaches only one of the servers.
- IPv6 does not designate a special block for Anycast addresses, the address is taken from the Unicast block.

Network Layer

IPv6 Three types of addresses

Multicast: Such an address also defines a group of computers, all of which share one address.
But unlike Anycast, where only one copy of a packet was sent to only one member of the group, each members in the group will receive a copy of the packet.
IPv6 has a special block for Multicasting, from which the same address is assigned to all members of a group.

Note that IPv6 does not define Broadcasting. IPv6 considers broadcasting as a special case of Multicasting.

Network Layer

IPv6 Address space allocation

Prefix for IPv6 addresses			
Block prefix	**CIDR (Classless Inter-Domain Routin)**	**Block assignment**	**Fraction**
0000 0000	0000::/8	Special address	1/256
001	**2000::/3**	**Global unicast address**	**1/8**
1111 110	FC00::/7	Unique local address	1/128
1111 1110 10	FE80::/10	Link local address	1/1024
1111 1111	FF00::/8	Multicast address	1/256

Global unicast addresses

Let's take a closer look at the block used for unicast (one-on-one) communication. The block is called **Global Unicast Address Block.** CIDR for the block is **2000::/3**.

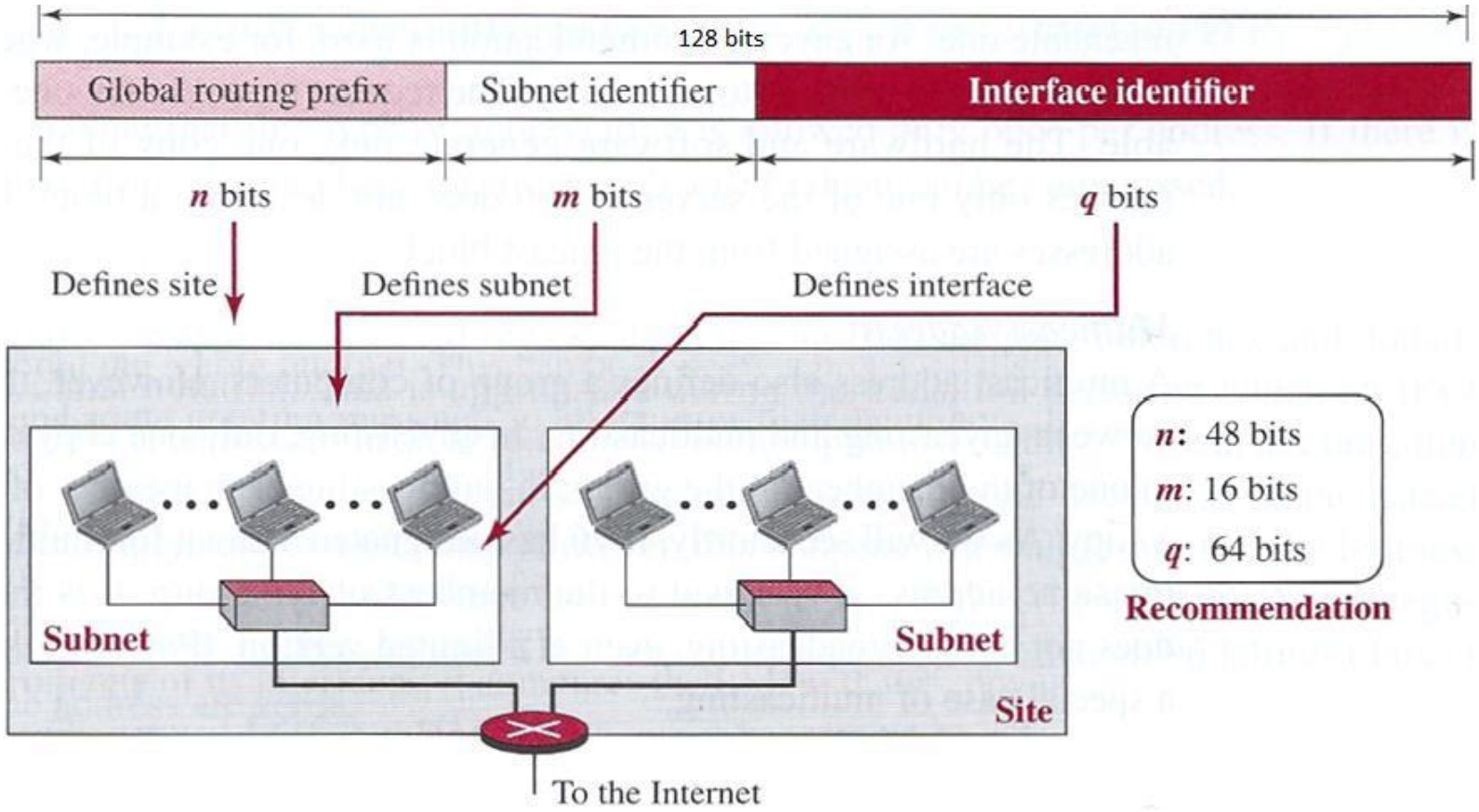
This means that the 3 MSB bits are the same for the whole block (001).

This means that there are 2^{125} addresses in a block (***4,25352958651173079329218259289 71e+37***).

That should be more than enough for Internet expansion for many years to come.

Network Layer

IPv6 Address space allocation



An address in this block is divided into three parts:

- Global routing prefix (recommended length: 48 bit)
- Subnet identifier (recommended length: 16 bit)
- Interface identifier (recommended length: 64 bit)

Network Layer

IPv6 Address space allocation

Global routing prefix: here the 3 MSB bits go for the block prefix, then there are 45 bits left. This global routing prefix is used to send packets through the Internet to reach a specific ISP or organization.
2^{45} or ***35.184372088832e+12*** different ISPs or organizations **(e.g., SDU)**.

Subnet ID: Once the packet has reached the ISP or organization, it can itself have ***2^{16}*** or ***65,536*** different subnets, which should be enough!
(could correspond to faculties at SDU)

Interface ID: Each subnet can have ***2^{64}*** or ***18.446744073709551616e+18*** different addresses.

Note that in IPv6 it is called an ***Interface ID*** and in IPv4 we call it a ***Host ID***.
It is actually more correct to call it Interface ID because ff you move a host to another connection on the Internet, it must also have a new IP address.

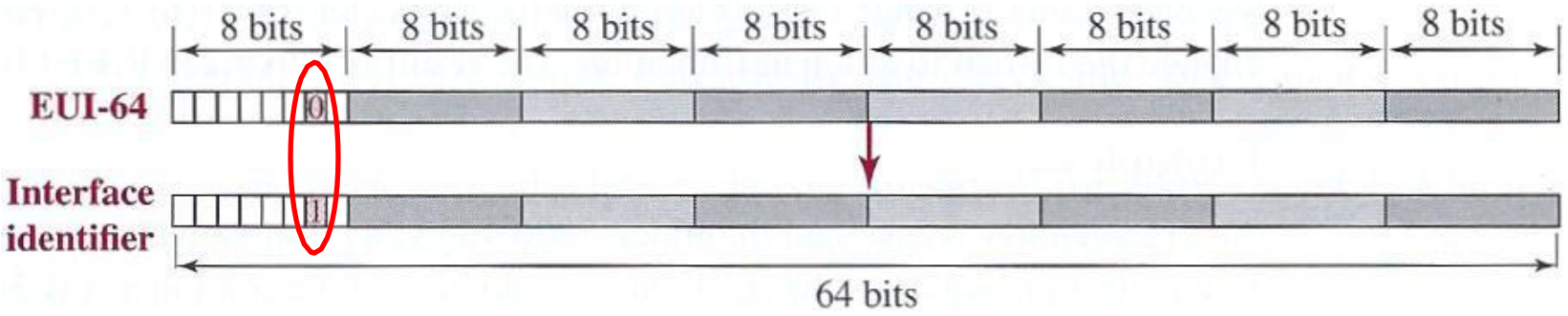
Network Layer

IPv6 Address Mapping

IPv6 allows a relationship between the IP address and the link-layer address.

Two common link layer addressing methods can be considered for this purpose:

- 64-bit **E**xtended **U**nique **I**dentifier (**EUI-64**), defined by the IEEE
- 48-bit MAC address defined by Ethernet

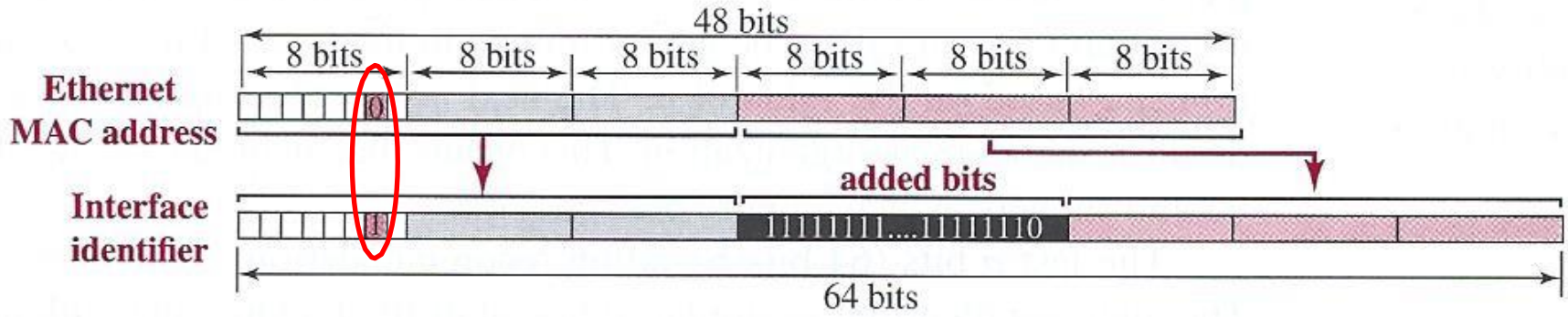


EUI-64 mapping

To relate a 64-bit link-layer address to an Interface ID, the global/local bit must be changed from 0 to 1 (local to global)

Network Layer

IPv6 Address mapping



Mapping of Ethernet MAC addresses

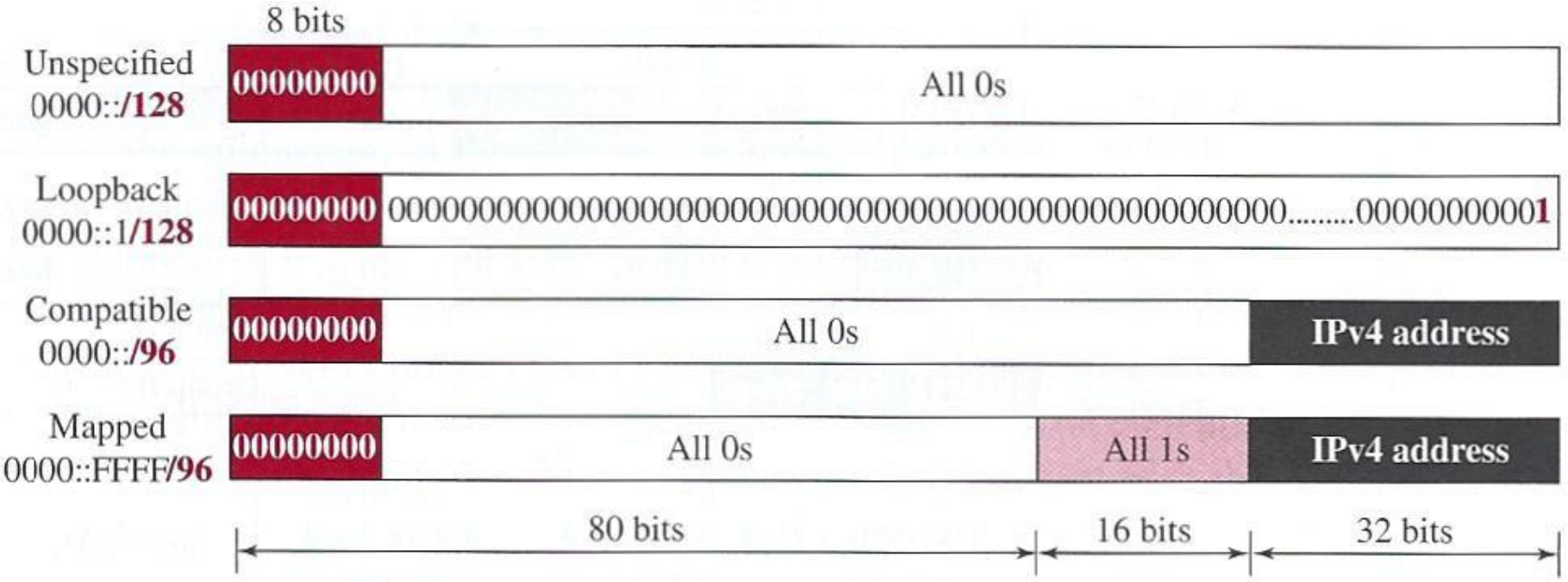
To relate a 48-bit MAC address to an Interface ID, the global/local bit must be changed from 0 to 1, and 16 more bits must be added, consisting of 15 1-digits and a 0 digit: ***FFFE*$_{16}$**.

Note that, the 16 extra bits are inserted in the middle of the Interface ID. The MAC address itself is split into two parts on the two sides of this Interface ID.

Network Layer

IPv6 Special addresses

Addresses that use the prefix (0000::/8) are reserved, but part of this block is used to define some special addresses.



Network Layer

IPv6 Special addresses

Unspecified: is a block with only one address (all bits are 0).
This address is used during booting when a host does not yet know its own address
(we have seen this in the **DHCP** **D**ynamic **H**ost **C**onfiguration **P**rotocol)

Loopback: is a block with only one address (all bits 0 except LSB, which is 1).
when this IP address is applied, the packet does not leave the host and is used for testing purposes.
NOTE: For IPv4, there are many addresses in this block while in IPv6 there is only one!

Network Layer

IPv6 Special addresses

Compatible address: is an address of 96 bits of zero followed by 32 bits of ***IPv4*** address. It is used when an ***IPv6*** host wants to communicate with another ***IPv6*** host (can be used in the transition phase from IPv4 to IPv6)

Mapped address: is an address of 80 bits of zero followed by 16 bits of one and 32 bits of ***IPv4*** addresses. It is used when an ***IPv6*** host wants to communicate with an ***IPv4*** host (can be used in the transition phase from IPv4 to IPv6)

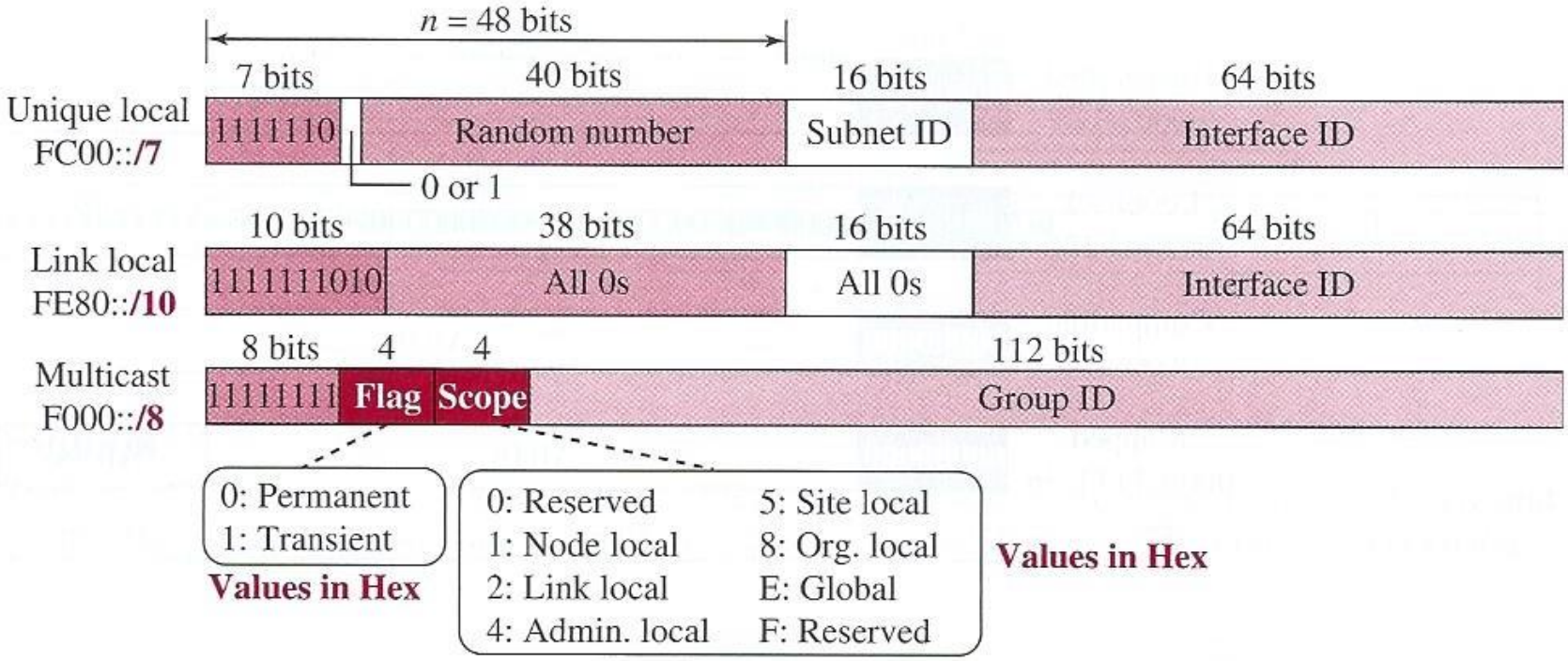
The smart thing about the last two blocks of Compatible and mapped addresses is that a calculation of the checksum can either be done on the entire ***IPv6*** address or only the ***IPv4*** address, it does not change the result of the checksum.
If 0 or 1 digits appear in multiples of 16, then it does not change the checksum.

This is important for UDP and TCP, which use a pseudoheader to calculate the checksum, because the checksum calculation is not affected if the address of the packet is changed from IPv6 to IPv4 by a router.

Network Layer

IPv6 Blocks for other purposes

IPv6 uses two large blocks for private addressing and one large block for multicasting.



Network Layer

IPv6 Blocks for other purposes

Unique local unicast block: Addresses in this block can be freely selected by the organization. Note that packets with a destination address in this block are not expected to leave the organization.
The 40 bits of random number must help minimize the probability of two identical addresses.
(used for private communication in the same LAN)

Link local block: Addresses in this block can be used as private addresses on the organization's network. (used e.g., for autoconfiguration)

Multicast block: An address from this block is used to define a group of hosts and not just one host.
As we can see, the group can be permanent (***0 for the flag***), if it is, then the address is defined by the internet authorities.
The group can also be transient or temporary (***1 for the flag***), and the address does not have to be defined by the internet authorities.
Scope field tells something about the domains within which the group appears.

Network Layer

IPv6 Autoconfiguration

We have seen how we can use DHCP to configure a host in IPv4.
we can still do that in IPv6.
BUT a host can also configure itself in IPv6, which is called **Autoconfiguration**

The following steps are followed for the autoconfiguration in IPv6:

1. First, the host creates a link local address for itself. This is done as follows:
   first 10-bit = **1111 1110 10**
   then 54-bit with 0s is added.
   finally, the Interface ID, which can be extracted from the network card, is used.

Network Layer

IPv6 Autoconfiguration

2. The host tests whether the generated link local address is unique. Since the Interface ID from the network card must be assumed to be unique, the local link address is unique with a high probability.

   but to be sure, the host sends a ***neighbor solicitation message*** (does anyone have my ID?) and waits for a ***neighbor advertisement message*** (yes I have!) If there are others, the configuration fails and DHCP has to used for instance.

Network Layer

IPv6 Autoconfiguration

3. If the uniqueness of the link local address is passed, the host stores this address as its link local address for private communication.
   But it still lacks a ***Global unicast address***.
   Now a ***router solicitation message*** is sent to a local router.
   If there is a running router on the network, it sends a ***router advertisement message*** back to the host***.***
   The message contains the Global prefix and the Subnet ID that the host needs to add to its interface identifier in order to generate its Global unicast address.

   If the router cannot help the host with the Global unicast address, then the process fails and then DHCP must be used.

IPv6 Protocol

Network Layer

The IPv6 protocol - benefits

Many more addresses: As we have seen, there are far more addresses in IPv6 (2^{128}) than in IPv4 (2^{32}): 2^{96}, or 79,228,162,514,264,337,593,543,950,336 or 7.9×10^{27} times.

- **Better header format**: IPv6 uses a new header format, where options are separated from the base header and inserted between the base header and the data section when needed. This simplifies and speeds up the routing process as most of the options do not need to be checked by the routers.

- **New options**: IPv6 has new options to allow for additional functionality.

- **Possibility of extension**: IPv6 is designed to allow the extension of the protocol if required by new technologies or applications.

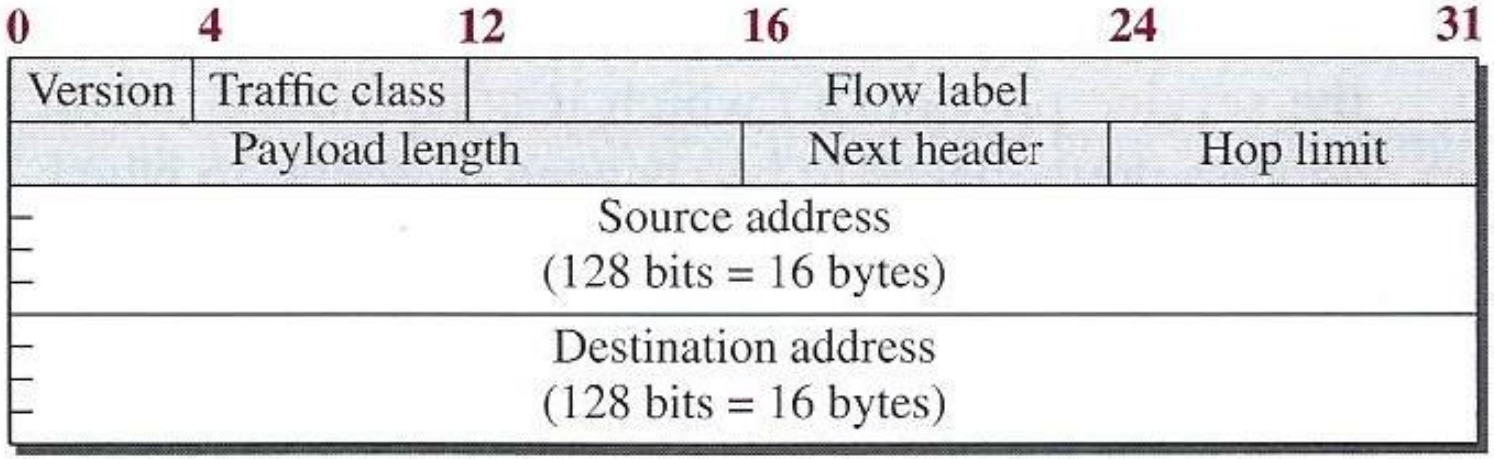
- **Resource allocation support**: In IPv6, the "type-of-service" field has been removed, but two new fields, traffic class and flow label, have been added to enable the sender to request special handling of the packet. This mechanism can be used to support traffic such as real-time audio and video.

- **Support for more security**: The encryption and authentication options in IPv6 provide confidentiality and integrity of the packet.

Network Layer

IPv6 protocol - Packet format

a. IPv6 packet



b. Base header

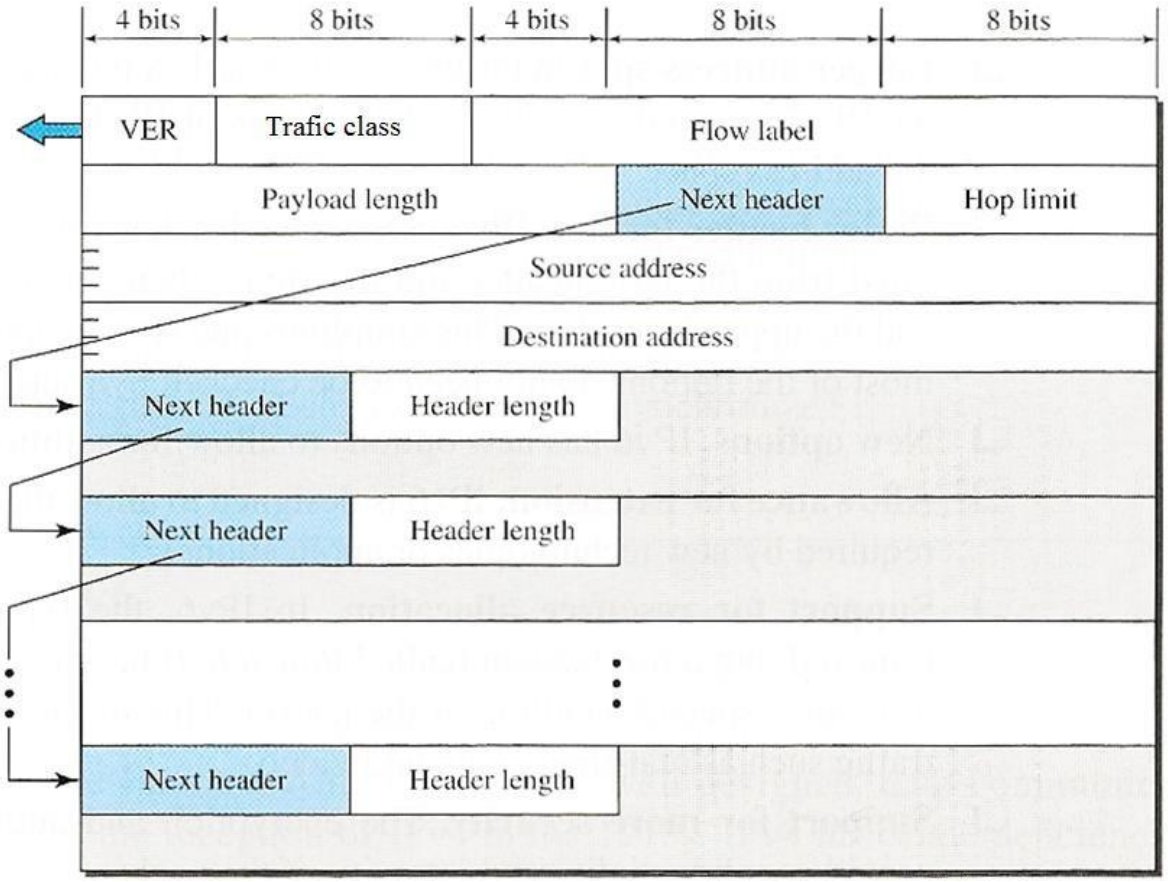
The payload consists of two parts:

- Optional extension header(s).
- Data from the upper layer.

Network Layer

IPv6 protocol - Packet format

Compared to IPv4, the payload field in IPv6 has a different format and meaning. The payload in IPv6 is a combination of zero or more extension headers (options) followed by the data from other protocols (UDP, TCP, and so on). **Options as part of the header in IPv4 are designed as extension headers In IPv6.**



Network Layer

IPv6 protocol – Packet format

- **Version (VER)**: this 4-bit field indicates the version number of the IP. For IPv6, this value is 6.
- **Traffic Class**: this 8-bit field is used to distinguish different payloads with different delivery requirements. It replaces the type-of-service field in IPv4.
- **Flow label**: this 20-bit field is designed to provide special handling for a particular flow of data.
- **Payload length**: This 2-byte field indicates the length of the datagram excluding the base header (40 bytes).

Network Layer

IPv6 protocol - Packet format

- **Next header**: this 8-bit field indicates the type of headers that come after the base header. Next header can either be type of the option headers (extension headers) if present, or the type of the encapsulated data in the datagram, e.g., ***UDP*** or ***TCP*** (see figure and table below). Note that the field is called protocol in IPv4.

Code	Next Header
0	Hop-to-hop option
2	**I**nternet **C**ontrol **M**essage **P**rotocol (**ICMP**)
6	**T**ransmission **C**ontrol **P**rotocol (**TCP**)
17	**U**ser **D**atagram **P**rotocol (**UDP**)
43	Source routing
44	Fragmentation
50	Encrypted security payload
51	Authentication
59	Null (no more next header)
60	Destination options

Network Layer

IPv6 protocol - Packet format

- **Hop limit**: This 8-bit field serves the same purpose as the TTL (Time-To-Live) field in IPv4.
- **Source address**: This 16-byte (128 bits) field indicates the Internet address of the sender.
- **Destination address**: This 16-byte (128 bits) field indicates the Internet address of the receiver.
- **Payload**: This field contains all the data coming from the upper protocols and all the possible next headers.

Network Layer

IPv6 Protocol - Flow Label

A sequence of packets, that are sent from a specific sender to a specific receiver and that needs a special handling by the routers along the way, are called a "**flow**" of packets.

Seen from a router, "a flow" is a sequence of packets that have the same characteristics as e.g.

- They travel the same path on the Internet.
- They use the same resources on their way.
- They have the same kind of security.

and so on

A router that supports the handling of flow labels (flow sequences) has a **flow label table**.

This table has an entry for each active flow sequence, which defines what service is required for that particular sequence of packets.

Note that it is not the Flow Label itself that determines which services should be provided for the flow sequence. **The flow label table is filled in by others**: e.g., information from the option section (located between the base header and the data section) or other routing protocols.

Network Layer

IPv6 Protocol - Flow Label

Flow label table can increase the router's handling speed: instead of having to look up the regular routing table and then run a routing algorithm to find the address of the next hop. Then the address of the next hop is found directly by looking up the flow label table.

A process (a sender) can reserve in advance various resources such as:

- high bandwidth
- large buffers
- dedicated paths through routers

It is then guaranteed that real-time data will not be delayed due to lack of resources.

The use of real-time data and advance reservation of resources requires other protocols e.g.,

- Real-time Transport Protocol (**RTP**)
- Resource Reservation Protocol (**RSVP**)

Network Layer

IPv6 Protocol - Flow Label

To allow efficient use of flow labels, there are 3 rules:

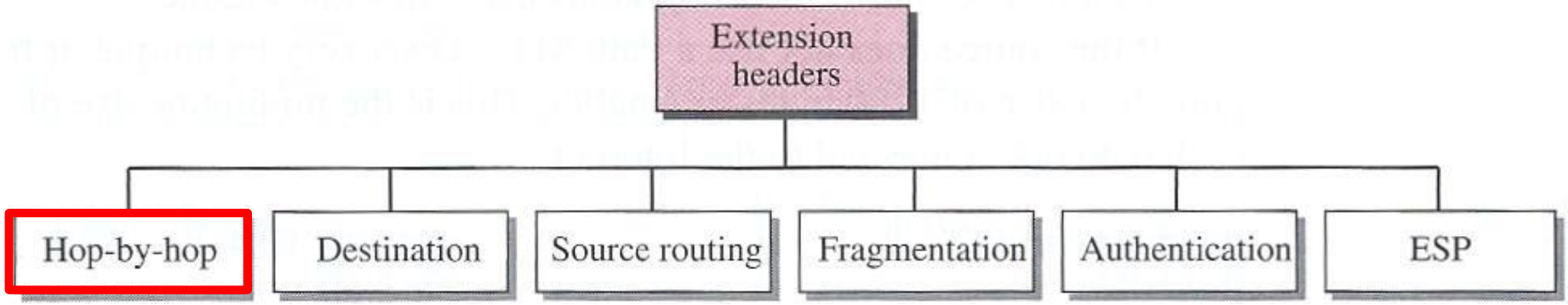
1. Flow labels are assigned to the packets by the sender. The label is a random number between ***1*** and $\boldsymbol{2^{20}-1}$.
   The sender must not reuse flow labels in a new flow sequence if they have been used in an ongoing sequence.

2. If the sender does not support flow sequences, then the flow label field is set to 0.
   If a router does not support flow sequences, then the field is ignored.

3. All packets belonging to the same flow sequence must have the same sender, receiver, security level and options.

Network Layer

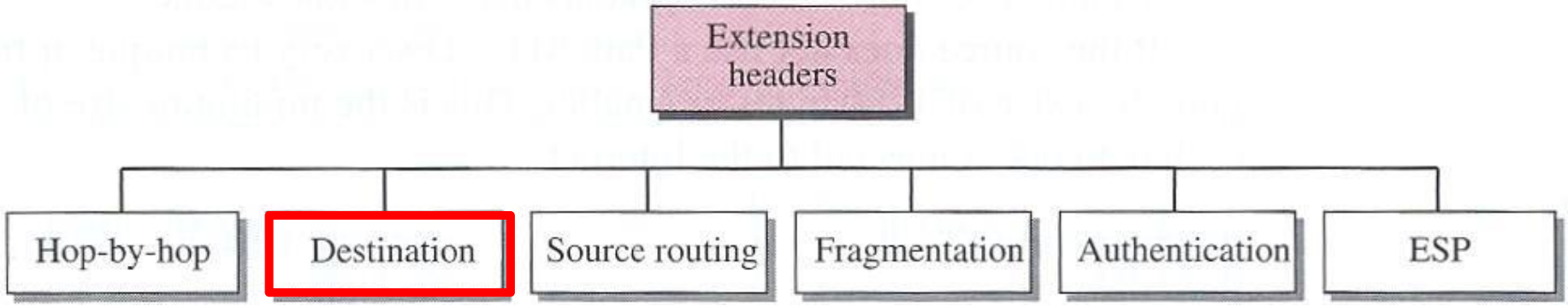
IPv6 Protocols - Extension Headers



- **Hop-by-hop option**: This extension header is used when a sender needs to provide information to all the routers visited by its datagram.
  So far, only 3 options have been defined:
  - Pad1: This option is 1 byte long and is designed for alignment purposes. Some options need to start at a specific bit of the 32-bit word. If an option falls short of this requirement by exactly one byte, Pad1 is added.
  - PadN: similar to Pad1 but used when 2 or more bytes are needed for alignment.
  - Jumbo payload: This option is used to define payloads longer than 65,535 bytes.

Network Layer

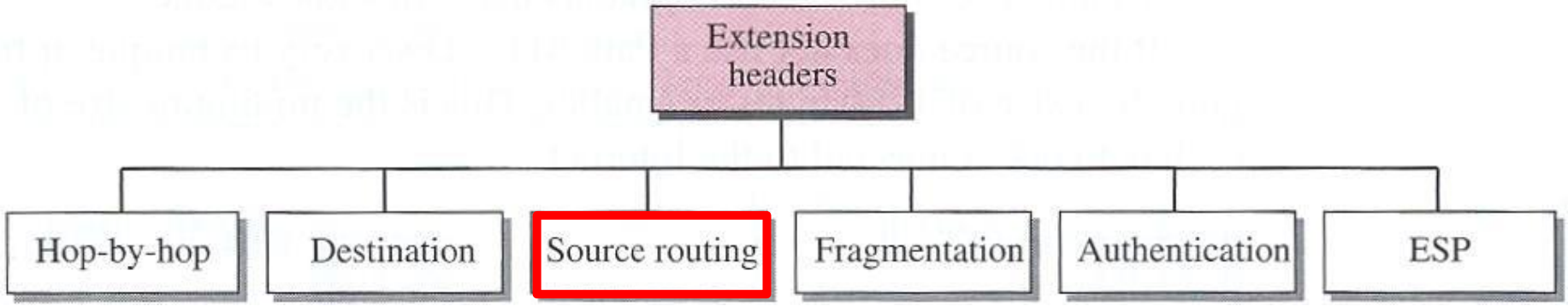
IPv6 Protocols - Extension Headers



- **Destination option**: This option is used when the sender wants to pass information only to the receiver. This means that routers are not allowed to access this information.

Network Layer

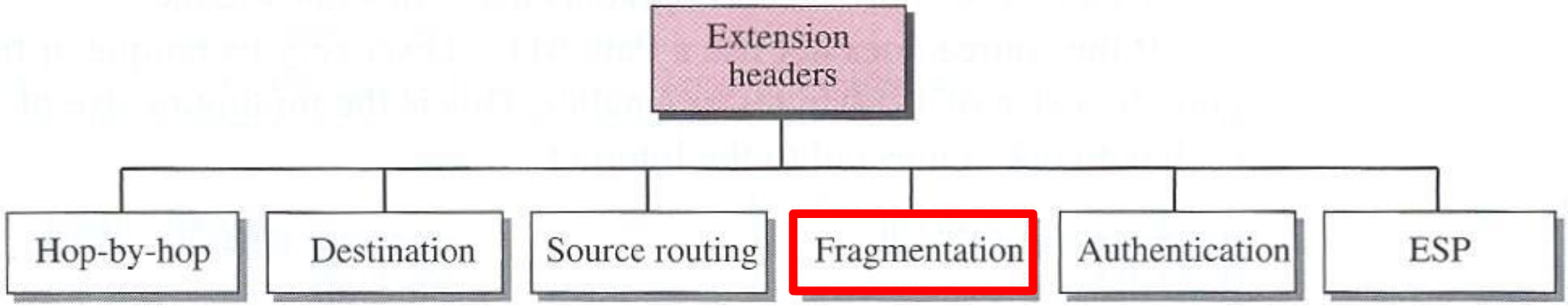
IPv6 Protocols - Extension Headers



- **Source Routing**: This Extension combines the concepts of Strict Source Route and Loose Source Route from the IPv4 protocol.

Network Layer

IPv6 Protocols - Extension Headers

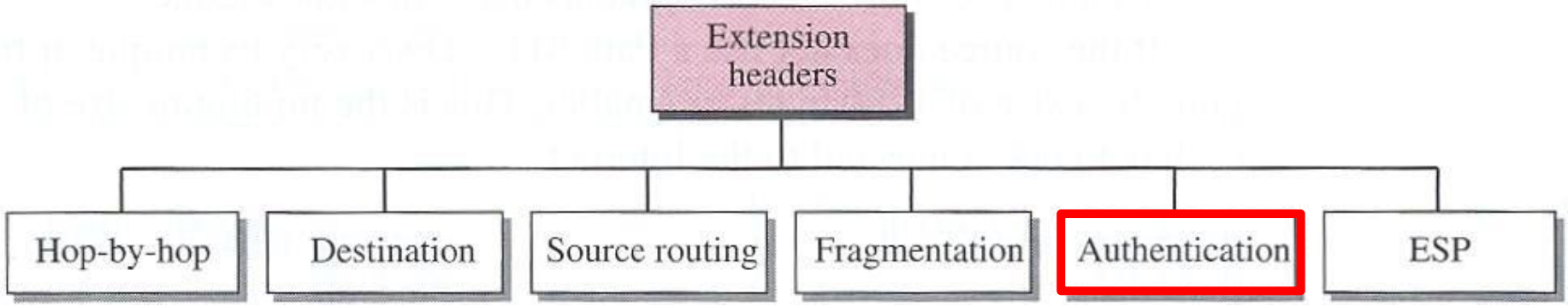


- **Fragmentation**: This extension is used when fragmentation is needed.
  Unlike IPv4, where it was either the sender itself or a given router on the way to the receiver that was responsible for the fragmentation if the MTU (Max. Transfer unit) for the network used was less than the datagram size.
  In IPv6, only the sender can perform this fragmentation.
  The sender must use a **path MTU discovery technique** to find the smallest MTU supported by any network on the path and use it to fragment the datagram after.

  If the source does not use a Path MTU Discovery technique, it fragments the datagram to a size of 1280 bytes or smaller. This is the minimum size of MTU required for each network connected to the Internet.

Network Layer

IPv6 Protocols - Extension Headers

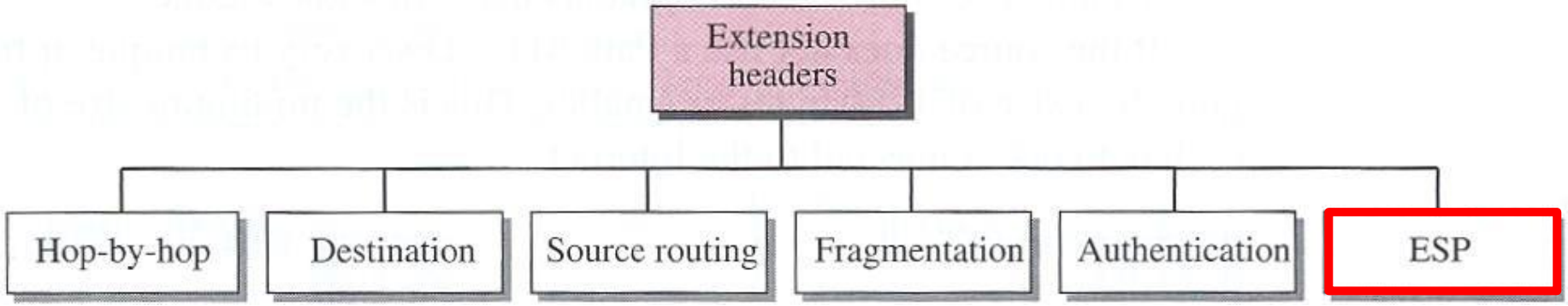


- **Authentication**: This extension has a dual purpose: it validates the sender and ensures the integrity of the received data.

  The former is needed so the receiver can be sure that a message is from the genuine sender and not from an imposter. The latter is needed to check that the data is not altered in transition by some hacker.

Network Layer

IPv6 Protocols - Extension Headers



- **Encrypted Security Payload**: (**ESP**) is an extension that offers confidentiality and guards against eavesdropping.

ICMPv6 Protocol

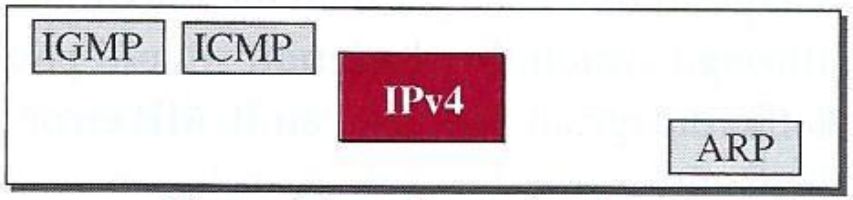
Network Layer

ICMPv6 protocol

ICMP has been modified in version 6 as well. This new version, Internet Control Message Protocol version 6 (ICMPv6), follows the same strategy and purposes of version 4.

The **ARP** , **ICMP** and **IGMP** protocols in version 4 have been merged into **ICMPv6**

ICMPv6 performs error reporting and diagnostic functions.

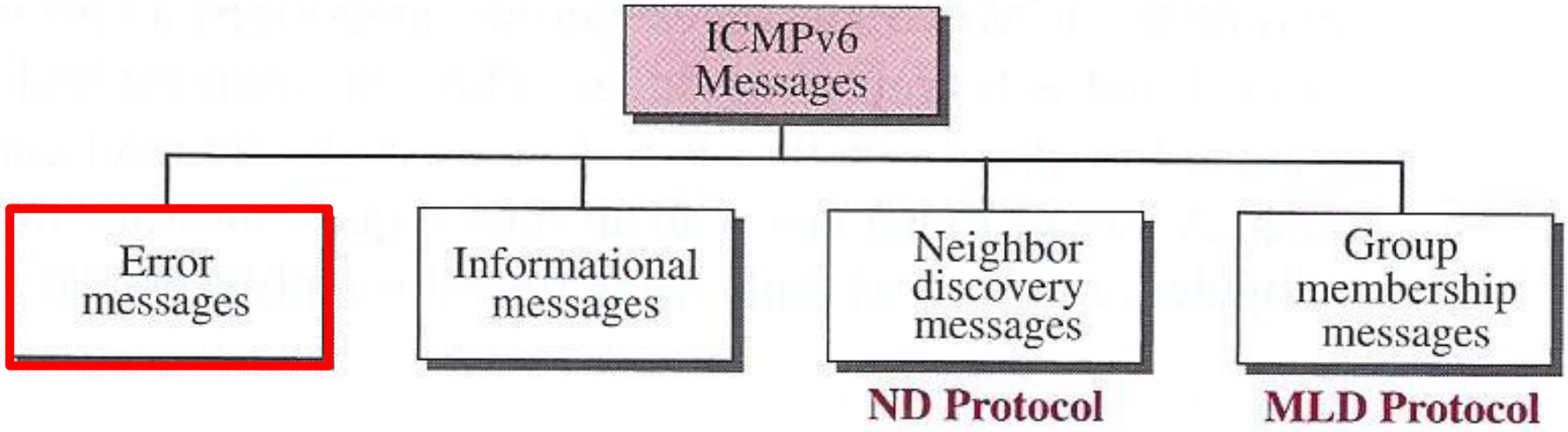


Network layer in version 4

Network layer in version 6

Network Layer

ICMPv6 protocol

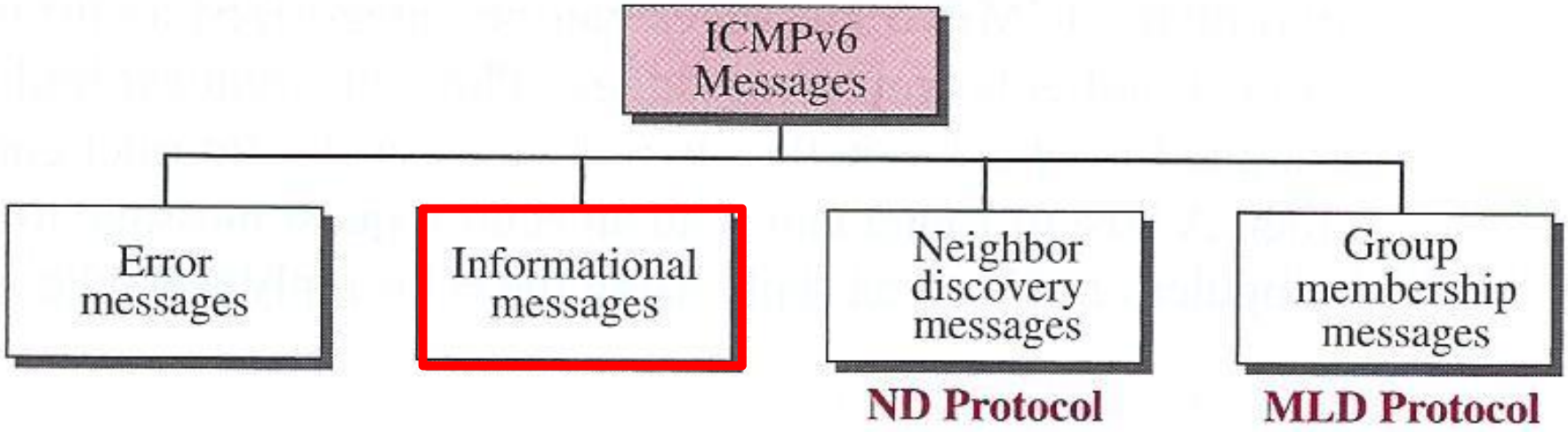


ICMPv6 forms an error packet, which is encapsulated in an IPv6 datagram and sent back to the original sender of the failed datagram.

- **Destination-Unreachable message**: same as in version 4. There is no protocol on the receiver that will receive the datagram, therefore a host cannot deliver the content of the datagram to the upper layer protocol.
- **Packed-Too-Big message**: new in version 6. If a router receives a packet larger than its MTU (Max. Transfer unit), the packet is discarded and an ICMP message is sent back to the sender (packet too large).
- **Time-Exceeded message**: same as in version 4. Either if the time-to-live counter reaches zero or if not all fragments of a datagram have arrived on time.
- **Parameter-problem message**: same as in version 4. used when a router or the destination host discovers any ambiguous or missing value in any field of the header.

Network Layer

ICMPv6 protocol



Here are two informative messages:

- Echo-request: same as in IPv4
- Echo-reply: same as in IPv4

The echo-request and echo-reply messages are designed to check whether two devices on the Internet can communicate with each other.

Network Layer

ICMPv6 protocol

Two new **ND** (**N**eighbor-**D**iscovery) and **IND** (**I**nverse **N**eighbor-**D**iscovery protocols clearly define the functionality of these group messages. The two protocols are used for three purposes:

1. Hosts use the ND protocol to find routers in the neighborhood that will forward packets for them.
2. Nodes use the ND protocol to find the link-layer addresses of neighbors (nodes attached to the same network).
3. Nodes use the IND protocol to find the IPv6 addresses of neighbors.

Network Layer

ICMPv6 protocol

Router-Solicitation message

A host finds a router in the network that can forward IPv6 datagram. (same as in IPv4)

Router-Advertisement message

It is a response to a router solicitation message.

Neighbor-Solicitation message

In version 6, the ARP protocol is eliminated. This functionality (acquire the MAC address by knowing the IP address) is now part of ICMPv6, and can be implemented by this type of messages. (now there is a relationship between IP and MAC addresses in ver6)

Neighbor-Advertisement message

It is a response to a neighbor solicitation message

Redirection message

same as in version 4, used to inform the host of the IP address of a better router for data transmission.
(but now the host can also get the MAC address of the better router)

Network Layer

ICMPv6 protocol

Inverse-Neighbor-Solicitation message

If a node knows the data link address of its neighbor and wants to know the IP address. The message is encapsulated in an IPv6 datagram which has an all-node multicast address. The sender must send in the option field:

- Own link-layer address
- Desired neighbor link-layer address

In addition, the sender can insert:

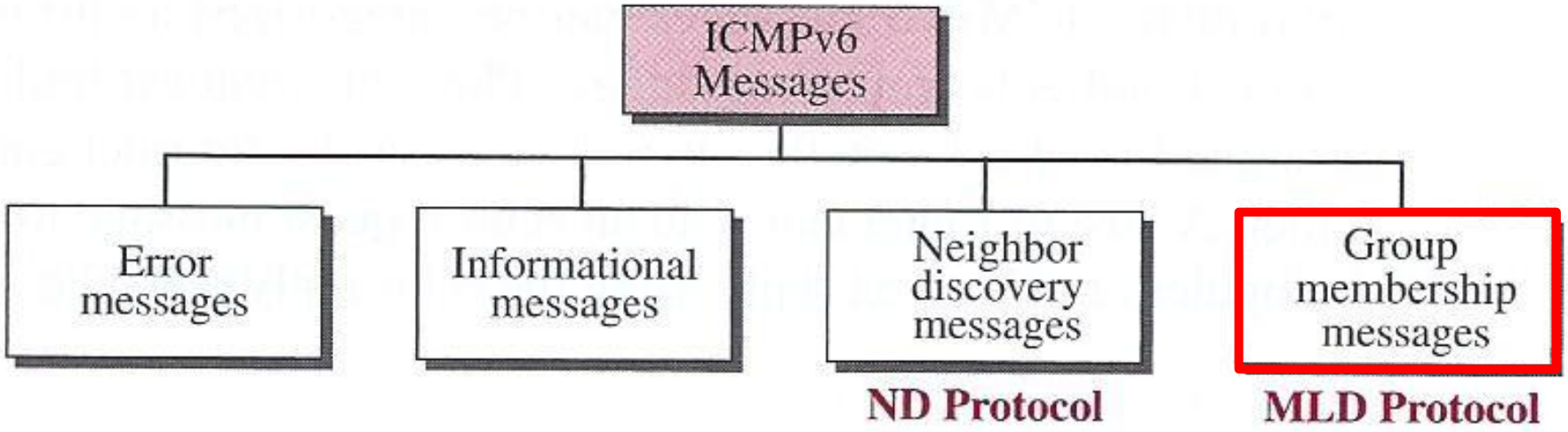
- Own IP address
- MTU (Max Transfer Unit) for the network

Inverse-Neighbor-Advertisement message

It is a response to the inverse-neighbor-solicitation message

Network Layer

ICMPv6 protocol



Group membership message

In version 6, the IGMP protocol is eliminated. This functionality is now part of ICMPv6 and can be accessed with this message type.

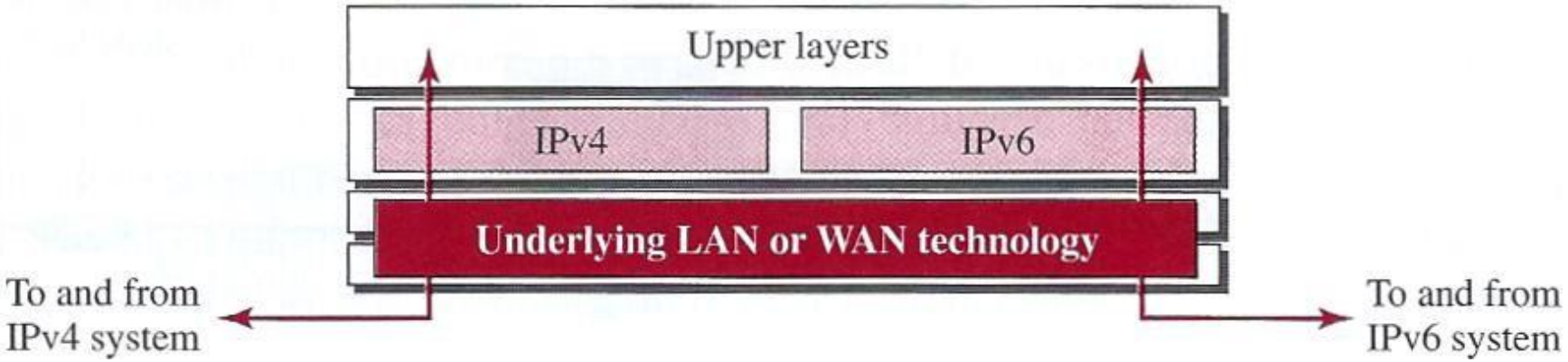
Transition from IPv4 to IPv6

Network Layer

Transition from IPv4 to IPv6

The transition from IPv4 to IPv6 should preferably take place smoothly.
Therefore, the **IETF** (**I**nternet **E**ngineering **T**ask **F**orce) recommends 3 strategies that can support this transition:

Dual Stack: It is recommended that all hosts, before the transition is complete, have a **dual stack of protocols**. This means that the host must run IPv4 and IPv6 simultaneously.
To determine which version to use when sending a packet to a destination, the source host queries the **DNS** (**D**omain **N**ame **S**ystem).
If an IPv4 address is returned, then an IPv4 packet (datagram) is sent and if an IPv6 address is returned, then an IPv6 packet (datagram) is sent.

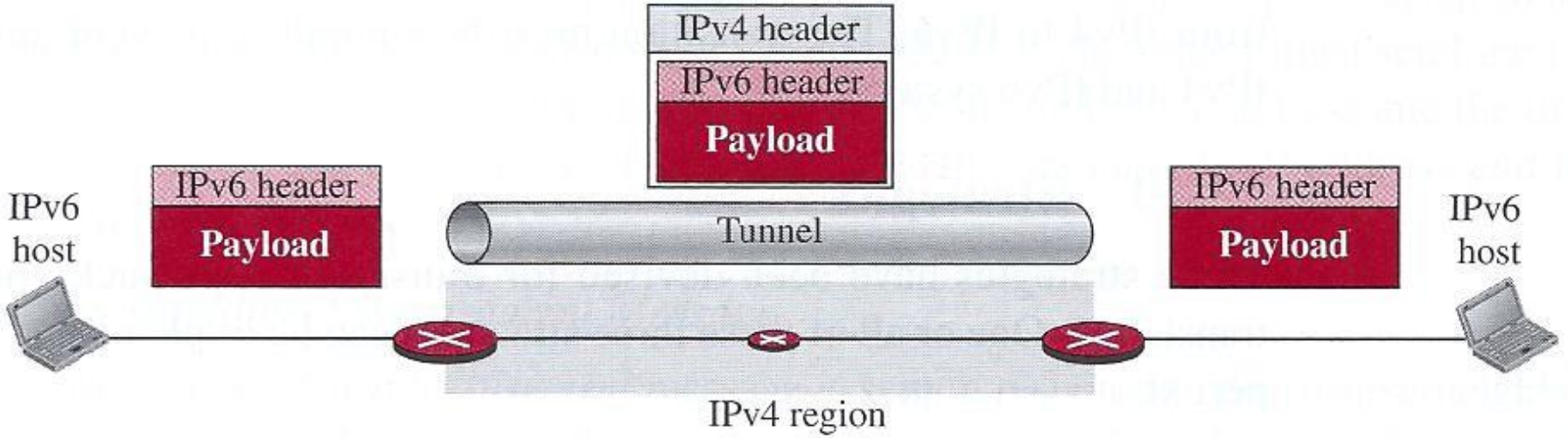


Network Layer

Transition from IPv4 to IPv6

Tunneling: When two computers using IPv6 want to communicate, and the packets must pass a region using IPv4. Then the packets need to have an IPv4 address in this region.

This is done by encapsulating the IPv6 packets in IPv4 packets when they arrive in the IPv4 region and unpacking them to have IPv6 packets when they leave the region. It seems as if the IPv6 packet enters a tunnel at one end and emerges at the other end.



Network Layer

Transition from IPv4 to IPv6

Header Translation: Header translation is required when the majority of the Internet has moved to IPv6, but some systems still use IPv4. The sender wants to use IPv6, but the receiver does not understand IPv6.

Tunneling does not work in this situation because the packet must be in the IPv4 format to be understood by the receiver. In this case, the header format must be totally changed through header translation. The header of the IPv6 packet is converted to an IPv4 header.