Hálózatok II.
IPv6

2007/2008. tanév, I. félév

Dr. Kovács Szilveszter

E-mail: szkovacs@iit.uni-miskolc.hu

Miskolci Egyetem

Informatikai Intézet 106. sz. szoba

Tel: (46) 565-111 / 21-06 mellék

IP Version 4

- **Az IPv4 címtartomány kimerülőfélben van (még a subnet maszkokkal + NAT is)**
- The current IPv4 Internet routing infrastructure is a **combination of both flat and hierarchical routing** ⇒ there are routinely **over 85,000 routes in the routing tables of Internet backbone routers .**

IP Version 4

IPv4 address allocation history:

- 1981 - IPv4 protocol published
- 1985 ~ 1/16 total space
- 1990 ~ 1/8 total space
- 1995 ~ 1/4 total space
- 2000 ~ 1/2 total space
- 2005 ~ 1 ??

Despite increasingly intense conservation efforts since 1994

- CIDR (classless inter-domain routing)
- NAT (network address translation)

Theoretical limit of 32-bit space: ~4 billion devices;

- practical limit of 32-bit space: ~250 million devices

IP Version 6

- **Az IPv6 címek 128 bitesek (16 byte), $2^{128} = 3.4 * 10^{38}$ cím**
  - **665 * 10^{21} cím per négyzetméter a földön!**
  - **Ha 10^6/μs sebességgel osztanánk ki a címeket, 20 év alatt tölthenénk be a címteret.**
  - **Könnyű subnet-eket kialakítani**
  - **Nem kell NAT**
- **Az IPv6 címek nem hoszt/node címek** (mint IPv4)**, hanem „interfész" címek**
- **Egy hosztnak lehet több interfésze (címe)**
- **IPv6 includes support for addresses of different "scope" (többes címzések – link local, site local)**
- **Unicast, multicast, anycast is lehet**
- **Ugyanakkor <u>nincs</u> „broadcast"**

További IPv6 előnyök

- New header format
- Large address space
- Efficient and hierarchical addressing and routing infrastructure
- Stateless and stateful address configuration
- Built-in security
- Better support for QoS
- New protocol for neighboring node interaction
- Extensibility

IPv6 előnyök - New header format

- Keeping header overhead to a minimum.
- By moving both non-essential fields and optional fields to extension headers.
- IPv4 headers and IPv6 headers are not interoperable. IPv6 is not a superset of functionality that is backward compatible with IPv4.
- A host or router must use an implementation of both IPv4 and IPv6 in order to recognize and process both header formats.
- The new IPv6 header is only twice as large as the IPv4 header, even though IPv6 addresses are four times as large as IPv4 addresses.

IPv6 előnyök – Hierarchical Addressing and Routing

- Efficient, hierarchical, and summarizable routing infrastructure.
- Smaller routing tables.
- “Aggregatable Global Unicast Addresses.”

IPv6 előnyök – Stateless and Stateful Address Configuration

- Supports both stateful address configuration
- Stateful: e.g. DHCP server
- Stateless: hosts on a link automatically configure themselves with IPv6 addresses for the link (called link-local addresses) and with addresses derived from prefixes advertised by local routers.
- Even in the absence of a router, hosts on the same link can automatically configure themselves with link-local addresses and communicate without manual configuration.

IPv6 előnyök – Built-in Security

- Support for IPsec is an IPv6 protocol suite requirement.
- This requirement provides a standards-based solution for network security needs and promotes interoperability between different IPv6 implementations.

IPv6 előnyök – Better Support for QoS

- **New fields in the IPv6 header define how traffic is handled and identified.**
- **Traffic identification using a Flow Label field in the IPv6 header allows routers to identify and provide special handling for packets belonging to a flow, a series of packets between a source and destination.**
- **Because the traffic is identified in the IPv6 header, support for QoS can be achieved even when the packet payload is encrypted through IPsec.**

IPv6 előnyök – New Protocol for Neighboring Node Interaction

- The Neighbor Discovery protocol for IPv6 is a series of Internet Control Message Protocol for IPv6 (ICMPv6) messages that manage the interaction of neighboring nodes (nodes on the same link).
- Neighbor Discovery replaces the broadcast-based Address Resolution Protocol (ARP), ICMPv4 Router Discovery, and ICMPv4 Redirect messages with efficient multicast and unicast Neighbor Discovery messages.

IPv6 előnyök – Extensibility

- IPv6 can easily be extended for new features by adding extension headers after the IPv6 header.
- Unlike options in the IPv4 header, which can only support 40 bytes of options, the size of IPv6 extension headers is only constrained by the size of the IPv6 packet.

IPv4 - IPv6 összevetés

IPv4	IPv6
Source and destination addresses are 32 bits (4 bytes) in length.	Source and destination addresses are 128 bits (16 bytes) in length.
IPsec support is optional.	IPsec support is required.
No identification of packet flow for QoS handling by routers is present within the IPv4 header.	Packet flow identification for QoS handling by routers is included in the IPv6 header using the Flow Label field.
Fragmentation is done by both routers and the sending host.	Fragmentation is not done by routers, only by the sending host.
Header includes a checksum.	Header does not include a checksum.

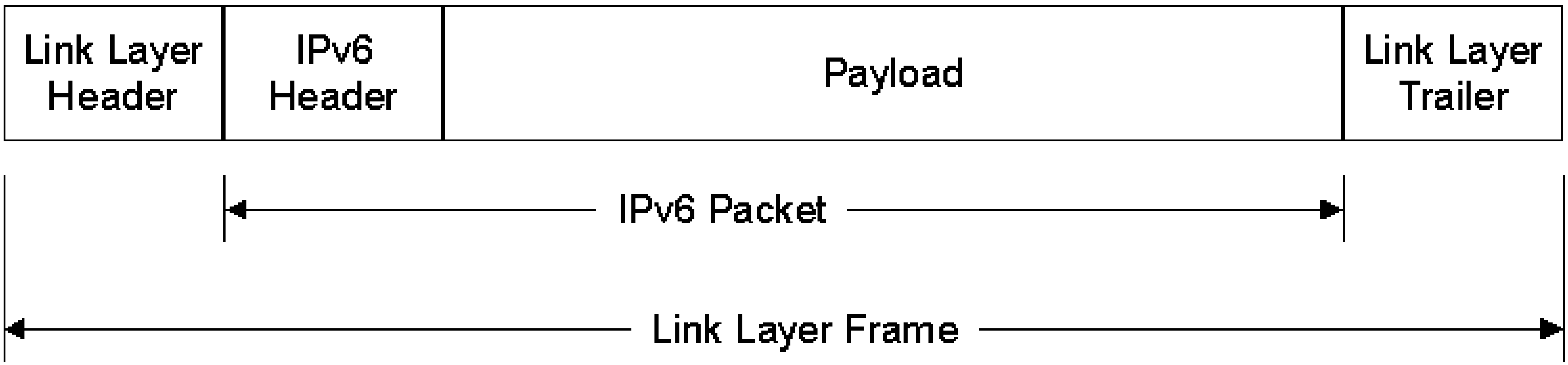
IPv4 - IPv6 összevetés

IPv4	IPv6
Header includes options.	All optional data is moved to IPv6 extension headers.
Address Resolution Protocol (ARP) uses broadcast ARP Request frames to resolve an IPv4 address to a link layer address.	ARP Request frames are replaced with multicast Neighbor Solicitation messages. “Neighbor Discovery.”
Internet Group Management Protocol (IGMP) is used to manage local subnet group membership.	IGMP is replaced with Multicast Listener Discovery (MLD) messages. “Multicast Listener Discovery.”
ICMP Router Discovery is used to determine the IPv4 address of the best default gateway and is optional.	ICMP Router Discovery is replaced with ICMPv6 Router Solicitation and Router Advertisement messages and is required. “Neighbor Discovery.”

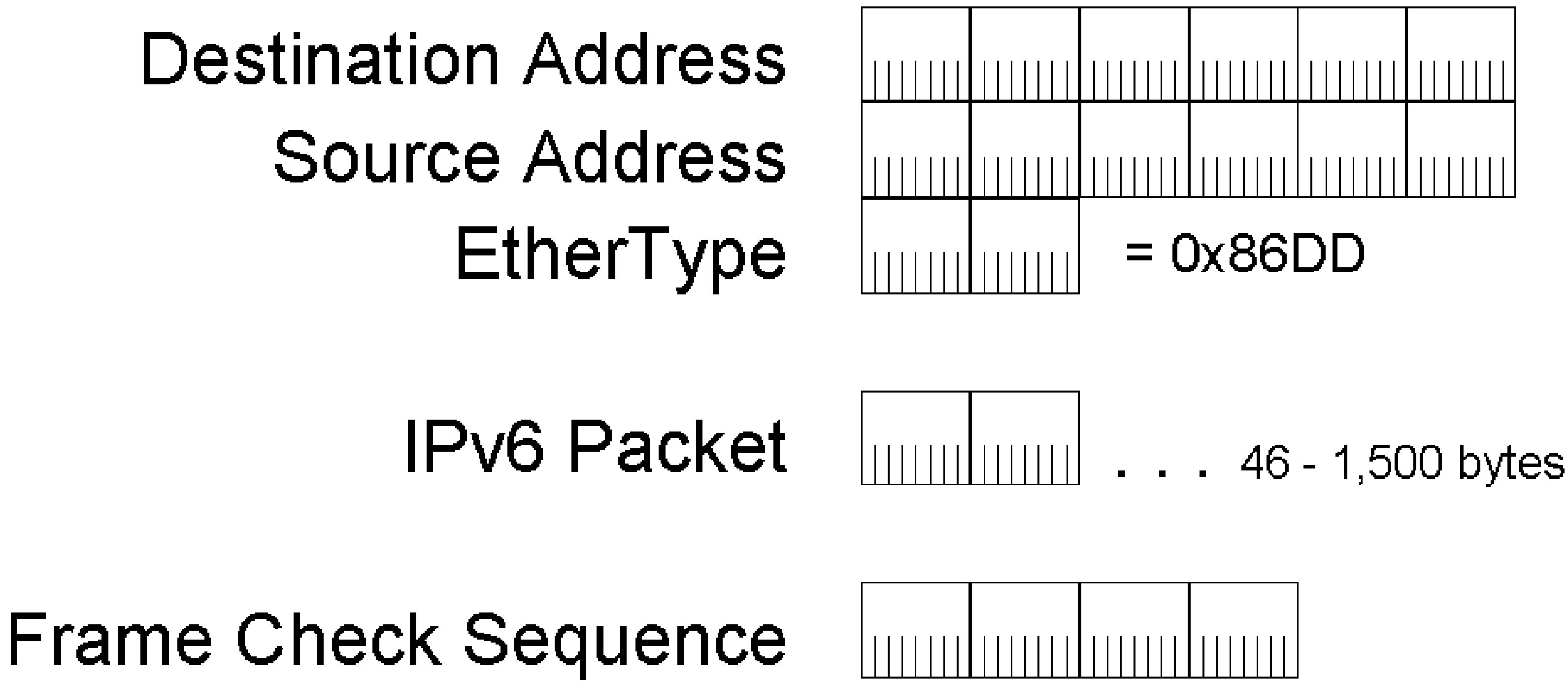
IPv4 - IPv6 összevetés

IPv4	IPv6
Broadcast addresses are used to send traffic to all nodes on a subnet.	There are no IPv6 broadcast addresses. Instead, a link-local scope all-nodes multicast address is used.
Must be configured either manually or through DHCP.	Does not require manual configuration or DHCP. “Address Autoconfiguration.”
Uses host address (A) resource records in the Domain Name System to map host names to IPv4 addresses.	Uses host address (AAAA) resource records in the Domain Name System to map host names to IPv6 addresses.
Uses pointer (PTR) resource records in the IN-ADDR.ARPA DNS domain to map IPv4 addresses to host names.	Uses pointer (PTR) resource records in the IP6.INT DNS domain to map IPv6 addresses to host names.
Must support a 576-byte packet size (possibly fragmented).	Must support a 1280-byte packet size (without fragmentation). “IPv6 MTU.”

IPv6 – Link Layer Enkapszuláció

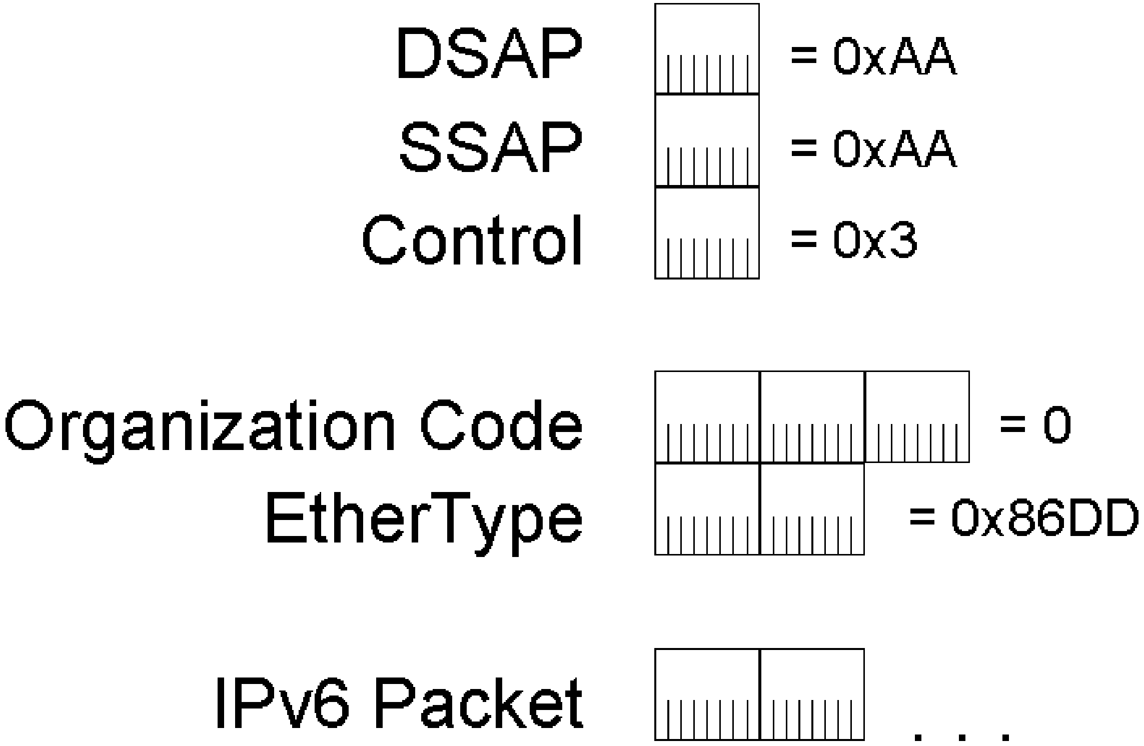


IPv6 – Ethernet II Enkapszuláció



- **EtherType field: 0x86DD (IPv4 esetén 0x800).**
- **Minimális IPv6 csomagméret: 46 byte**
- **Maximális IPv6 csomagméret: 1,500 byte**

IPv6 – IEEE 802.3 Enkapszuláció



DSAP = 0xAA

SSAP = 0xAA

Control = 0x3

Organization Code = 0

EtherType = 0x86DD

IPv6 Packet . . .

- **Sub-Network Access Protocol (SNAP) header**
- **EtherType field: 0x86DD**
- **Minimális IPv6 csomagméret: 38 byte**
- **Maximális IPv6 csomagméret: 1,492 byte**

IPv6 – Címzés: Format Prefix (FP)

Allocation	Prefix (Binary)	Fraction of Address Space
Reserved	0000 0000	1/256
Unassigned	0000 0001	1/256
Reserved for NSAP Allocation	0000 001	1/128
Reserved for IPX Allocation	0000 010	1/128
Unassigned	0000 011	1/128
Unassigned	0000 1	1/32
Unassigned	0001	1/16
Aggregatable Global Unicast Addresses	001	1/8
Unassigned	010	1/8
Unassigned	011	1/8
Unassigned	100	1/8
Unassigned	101	1/8
Unassigned	110	1/8
Unassigned	1110	1/16
Unassigned	1111 0	1/32
Unassigned	1111 10	1/64
Unassigned	1111 110	1/128
Unassigned	1111 1110 0	1/512
Link-Local Unicast Addresses	1111 1110 10	1/1024 FE80::/10
Site-Local Unicast Addresses	1111 1110 11	1/1024 FEC0::/10
Multicast Addresses	1111 1111	1/256 FF00::/8

IPv6 – Címzés: Jelölés

- **Preferred form (16 byte):**
  - – FEDC:BA98:7654:3210:FEDC:BA98:7654:3210
  - – 1080:0:0:0:0:8:800:200C:417A
- **Compressed form:**
  - – 1080::8:800:200C:417A
  - – 0:0:0:0:0:0:0:1 ==> ::1 (Unicast Loopback address)
  - – FF01:0:0:0:0:0:0:42 ==> FF01::42 (Multicast address)
  - – 0:0:0:0:0:0:0:0 ==> :: (The unspecified address)

IPv6 – Címzés: Kompatibilis címek

- IPv4-kompatibilis cím
  - 0:0:0:0:0:0:193.6.5.73 ==> ::193.6.5.73
  - 0:0:0:0:0:0:w.x.y.z ==> ::w.x.y.z
  - Csak akkor, ha IPv4/IPv6 dual stack.
  - Ha IPv4-kompatibilis címet adnak meg úgy, mint egy IPv6 cél címet, akkor az IPv6 forgalom automatikusan IPv4 fejrészt kap és az IPv4 hálózaton küldik a cél felé.
- IPv4-mapped address
  - 0:0:0:0:0:FFFF:193.6.5.73 ==> ::FFFF:193.6.5.73
  - Csak belső reprezentáció, senki sem küld ilyet.
  - Az IPv6 node jelöli így a csak IPv4 node-ot

IPv6 – Címzés: Kompatibilis címek

- **6to4 cím**
  - **2002::/16 cím 32 bites publikus IPv4 node címmel, egy 48-bites prefixet alkot.**
  - **Pl: 193.6.5.73 esetén (Hexában: C1.6.5.49) 2002:C106:0549::/48**
  - **Két IPv4 és IPv6 dual stack node között használják, ha azok IPv4 routing infrastruktúra felett kommunikálnak.**
  - **A 6to4 egy RFC 3056 szerinti tunnel technika.**
- **Az IPv6 nem használ maszkot, csak prefixet.**

IPv6 – Címzés: Cím típusok

Unicast:

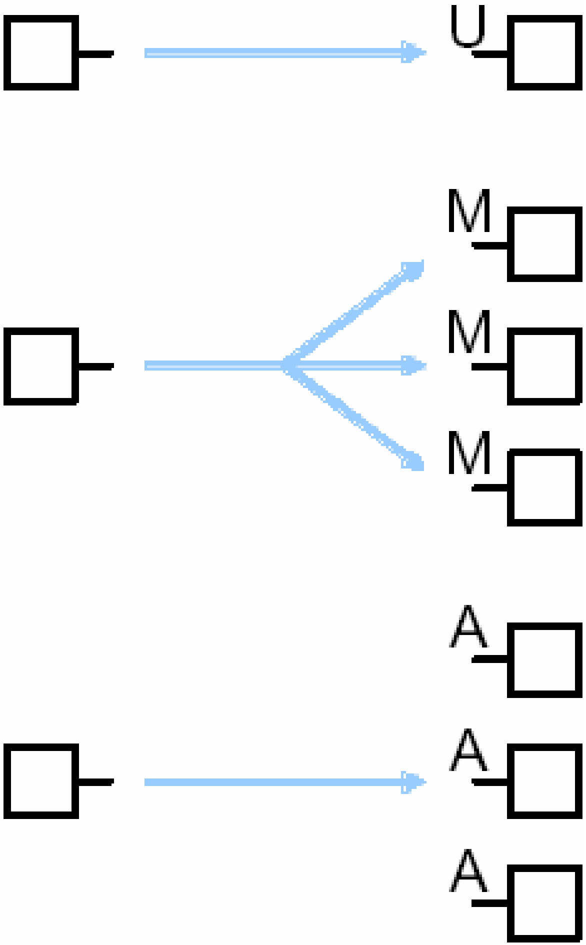
for one-to-one communication

Multicast:

for one-to-many communication

Anycast:

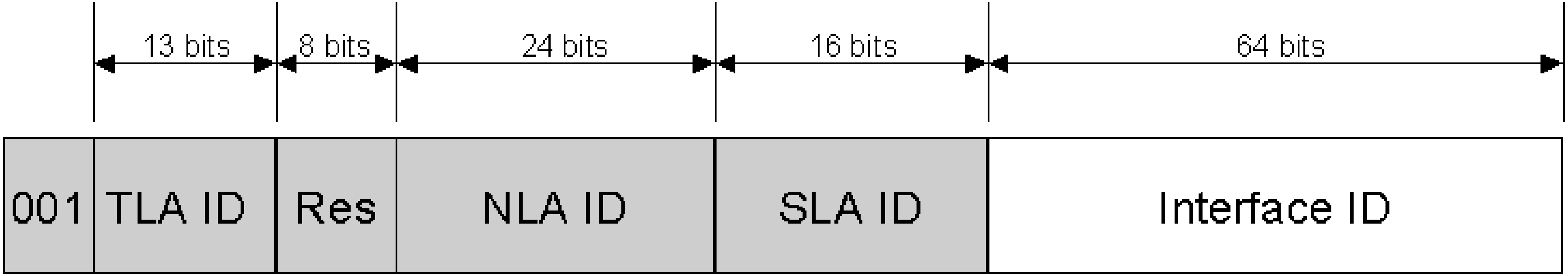
for one-to-nearest communication



IPv6 – Címzés: Unicast címek

- **Aggregatable global unicast addresses**
- **Link-local addresses**
- **Site-local addresses**
- **Special addresses**
  (loopback, unspecified compatible)

IPv6 – Aggregatable global unicast addresses



	13 bits	8 bits	24 bits	16 bits	64 bits
001	TLA ID	Res	NLA ID	SLA ID	Interface ID

- **TLA ID – Top-Level Aggregation Identifier**
  - **Highest level in the routing hierarchy (called default-free routers)**
  - **Administered by IANA for long haul Internet service providers assigned to the routing region**
- **Res – Bits that are reserved for future use**
- **NLA ID – Next-Level Aggregation Identifier.**
  - **Az intézmény azonosítására szolgál.**
- **SLA ID – Site-Level Aggregation Identifier.**
  - **Az SLA ID az intézményen belüli alhálózatok azonosítására szolgál.**
- **Interface ID – Egy alhálózaton belül az interface-t azonosítja.**

IPv6 – Miskolci Egyetem Hbone 6Net

2001:0738:6001::/48

```
inet6num:    2001:0738:6001::/48
netname:     UNI-MISKOLC
descr:       University of Miskolc
descr:       Miskolci Egyetem
descr:       H-3515 Miskolc Egyetemvaros
country:     HU
admin-c:     LB18-RIPE
tech-c:      SK38-RIPE
tech-c:      NB12-RIPE
status:      ASSIGNED
remarks:     ourid=445
mnt-by:      NIIF6-MNT
source:      RIPE
changed:     hostmaster6@iif.hu 20030103
```

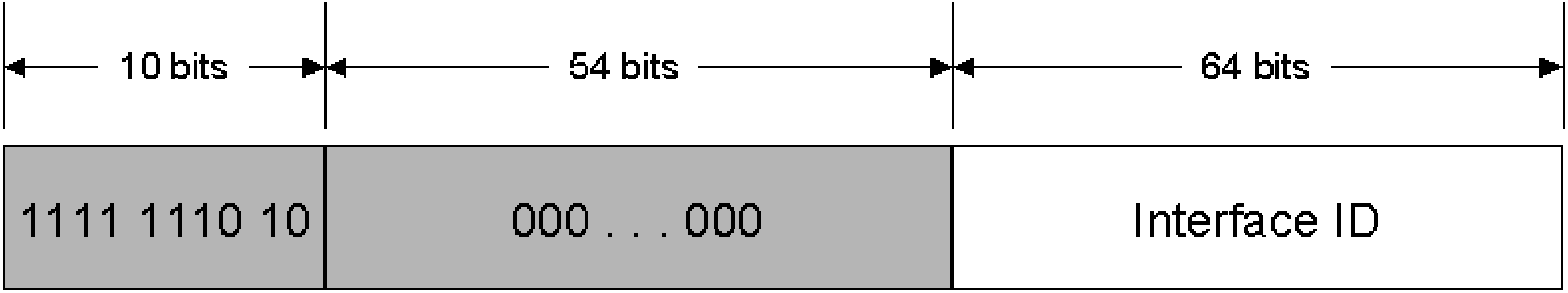
-

```
person:       Laszlo Balla
address:      University of Miskolc
address:      Miskolci Egyetem
address:      Miskolc Egyetemvaros
address:      H-3515 MISKOLC-Egytemvaros
address:      Hungary
phone:        +36 46 565111 ext. 1012
fax-no:       +36 46 363450
e-mail:       szkballa@uni-miskolc.hu
nic-hdl:      LB18-RIPE
changed:      hostmaster@iif.hu 19920705
changed:      hostmaster@iif.hu 20020103
source:       RIPE

person:       Szilveszter Kovacs
address:      University of Miskolc
address:      Miskolci Egyetem
address:      H-3515 Miskolc-Egyetemvaros
address:      Hungary
phone:        +36 46 565111 ext. 2108
fax-no:       +36 46 563450
e-mail:       szkszilv@uni-miskolc.hu
nic-hdl:      SK38-RIPE
notify:       hostmaster@iif.hu
changed:      szkszilv@uni-miskolc.hu 19960502
changed:      hostmaster@iif.hu 20020103
source:       RIPE

person:       Norbert Burmeister
address:      University of Miskolc
address:      Miskolci Egyetem
address:      H-3515 Miskolc-Egyetemvaros
address:      Hungary
phone:        +36 46 565111 ext. 1070
fax-no:       +36 46 563450
e-mail:       szkburma@uni-miskolc.hu
nic-hdl:      NB12-RIPE
notify:       hostmaster@iif.hu
changed:      hostmaster@iif.hu 19920705
changed:      hostmaster@iif.hu 20020103
source:       RIPE
```

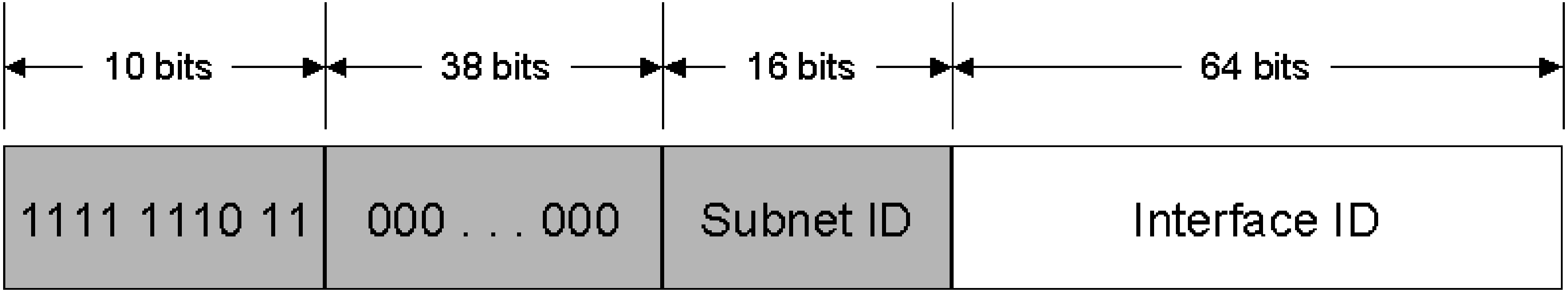
IPv6 – Link-Local unicast addresses



10 bits	54 bits	64 bits
1111 1110 10	000 . . . 000	Interface ID

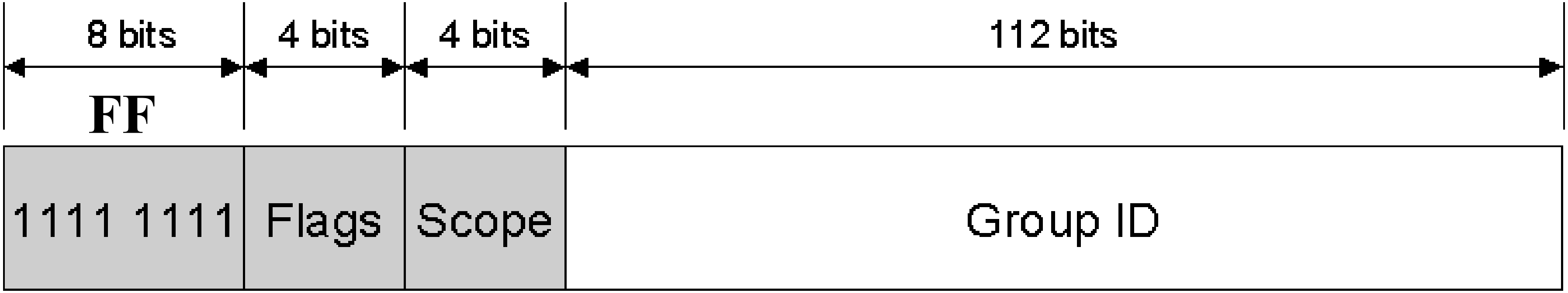
- **A link-local címek a Neighbor Discovery eljáráshoz kellenek és mindig automatikusan konfigurálódnak, még akkor is, ha semmilyen más unicast cím sem létezik.**
- **A link-local címek prefix-e mindig FE80::/64**

IPv6 – Site-Local unicast addresses



- A link-local címekkel ellentétben, a site-local címek nem automatikusan konfigurálódnak, hanem vagy állapotmentes (stateless), vagy állapot alapú (stateful) cím konfigurációval kell megadni azokat.
- A site-local címek esetén az első 48-bit mindig ugyanazzal a FEC0::/48 címmel kezdődik.
- A fix 48 bitet követi a 16-bites subnet identifier (Subnet ID field).

IPv6 – Multicast címek



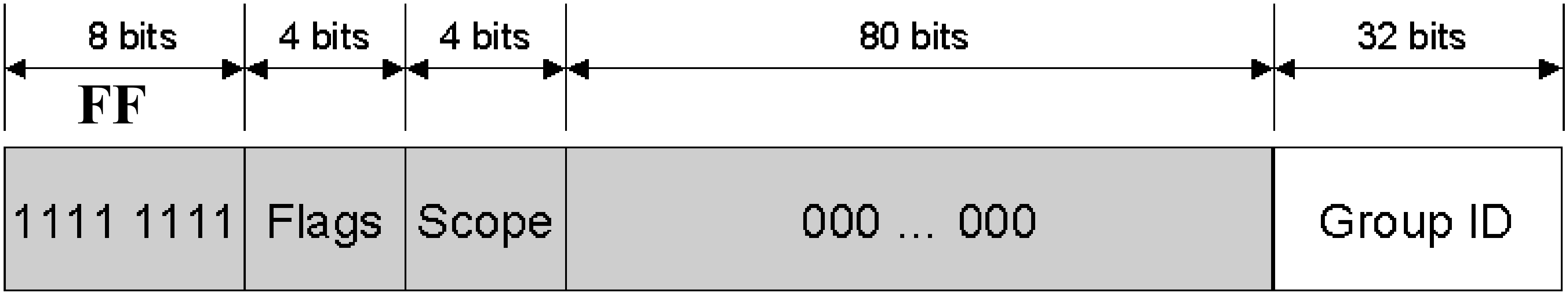
8 bits	4 bits	4 bits	112 bits
FF			
1111 1111	Flags	Scope	Group ID

- **Flags – RFC 2373, jelenleg csak: Transient (T) flag. (legalsó bit**
  - **0: multicast address is a permanently assigned (well-known) multicast address allocated by the Internet Assigned Numbers Authority (IANA). FF01:: - FF0F:: reserved, well-known addresses**
  - **1: transient (non-permanently-assigned) multicast address.**
- **Scope:**
  - **0: Reserved, 1: Node-local scope, 2: Link-local scope, 5: Site-local scope,**
  - **8: Organization-local scope, E: Global scope, F: Reserved**
  - **Pl. FF02::2 link-local scope. (Az IPv6 router-ek nem továbbítját)**
- **Group ID: A multicast csoport egyedi azonosítója**

IPv6 – Multicast címek

- **Speciális node multicast címek:**
  - **FF01::1 (node-local scope all-nodes multicast address)**
  - **FF02::1 (link-local scope all-nodes multicast address)**
- **Speciális router multicast címek:**
  - **FF01::2 (node-local scope all-routers multicast address)**
  - **FF02::2 (link-local scope all-routers multicast address)**
  - **FF05::2 (site-local scope all-routers multicast address)**

IPv6 – Multicast címek (módosítás)



8 bits	4 bits	4 bits	80 bits	32 bits
FF				
1111 1111	Flags	Scope	000 ... 000	Group ID

- However, because of the way in which IPv6 multicast addresses are mapped to Ethernet multicast MAC addresses, RFC 2373 recommends assigning the Group ID from the low order 32 bits of the IPv6 multicast address and setting the remaining original group ID bits to 0.
- By using only the low-order 32 bits, each group ID maps to a unique Ethernet multicast MAC address.

IPv6 – Solicited-Node Multicast Address

A cím felfejtés (address resolution) során elősegíti a hatékony hálózati címhez tartozó adatkapcsolati cím lekérdezést.

Az IPv6 Neighbor Solicitation üzenetet használ a cím felfejtéshez (address resolution).

Local-link scope *all-nodes* multicast címzés helyett *solicited-node* multicast címzést használ.

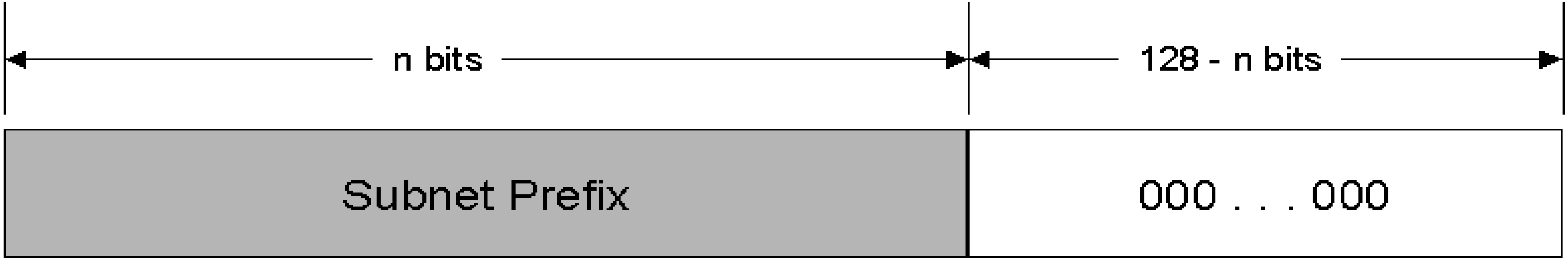
A solicited-node multicast címet az FF02::1:FF00:0/104 prefixből és a felfejtendő IPv6 cím utolsó 24-bitjébők képzi. Pl:

– Node A link-local címe FE80::2AA:FF:FE28:9C5A valamint hallgat az ehhez tartozó solicited-node multicast címre: FF02::1:FF28:9C5A

– Ha Node B keresi a Node A link-local címéhez FE80::2AA:FF:FE28:9C5A tartozó link-layer címet, akkor Neighbor Solicitation üzenetet küld a FF02::1:FF28:9C5A solicited node multicast címre.

– Mivel Node A hallgat erre a címre, megválaszolja azt B-nek az unicast Neighbor Advertisement üzenettel

IPv6 – Anycast Address



- Az anycast címeket több interfészhez is hozzá lehet rendelni.
- Packets addressed to an anycast address are forwarded by the routing infrastructure to the nearest interface to which the anycast address is assigned.
- Anycast addresses are assigned out of the unicast address space and the scope of an anycast address is the scope of the type of unicast address from which the anycast address is assigned.
- All router interfaces attached to a subnet are assigned the Subnet-Router anycast address for that subnet.
- The Subnet-Router anycast address is used for communication with one of multiple routers attached to a remote subnet

IPv6 – Addresses for a Host

- Egy IPv6 host-hoz az alábbi unicast címek vannak hozzárendelve:
  - A link-local address for each interface
  - Unicast addresses for each interface (which could be a site-local address and one or multiple aggregatable global unicast addresses)
  - The loopback address (::1) for the loopback interface
- Valamennyi host hallgat az alábbi multicast címekre:
  - The node-local scope all-nodes multicast address (FF01::1)
  - The link-local scope all-nodes multicast address (FF02::1)
  - The solicited-node address for each unicast address on each interface
  - The multicast addresses of joined groups on each interface.

IPv6 – Addresses for a Router

- Egy IPv6 router az alábbi unicast címek vannak hozzárendelve:
  - A link-local address for each interface
  - Unicast addresses for each interface (which could be a site-local address and one or multiple aggregatable global unicast addresses)
  - A Subnet-Router anycast address
  - Additional anycast addresses (optional)
  - The loopback address (::1) for the loopback interface
- Valamennyi router hallgat az alábbi multicast címekre:
  - The node-local scope all-nodes multicast address (FF01::1)
  - The node-local scope all-routers multicast address (FF01::2)
  - The link-local scope all-nodes multicast address (FF02::1)
  - The link-local scope all-routers multicast address (FF02::2)
  - The site-local scope all-routers multicast address (FF05::2)
  - The solicited-node address for each unicast address on each interface
  - The multicast addresses of joined groups on each interface

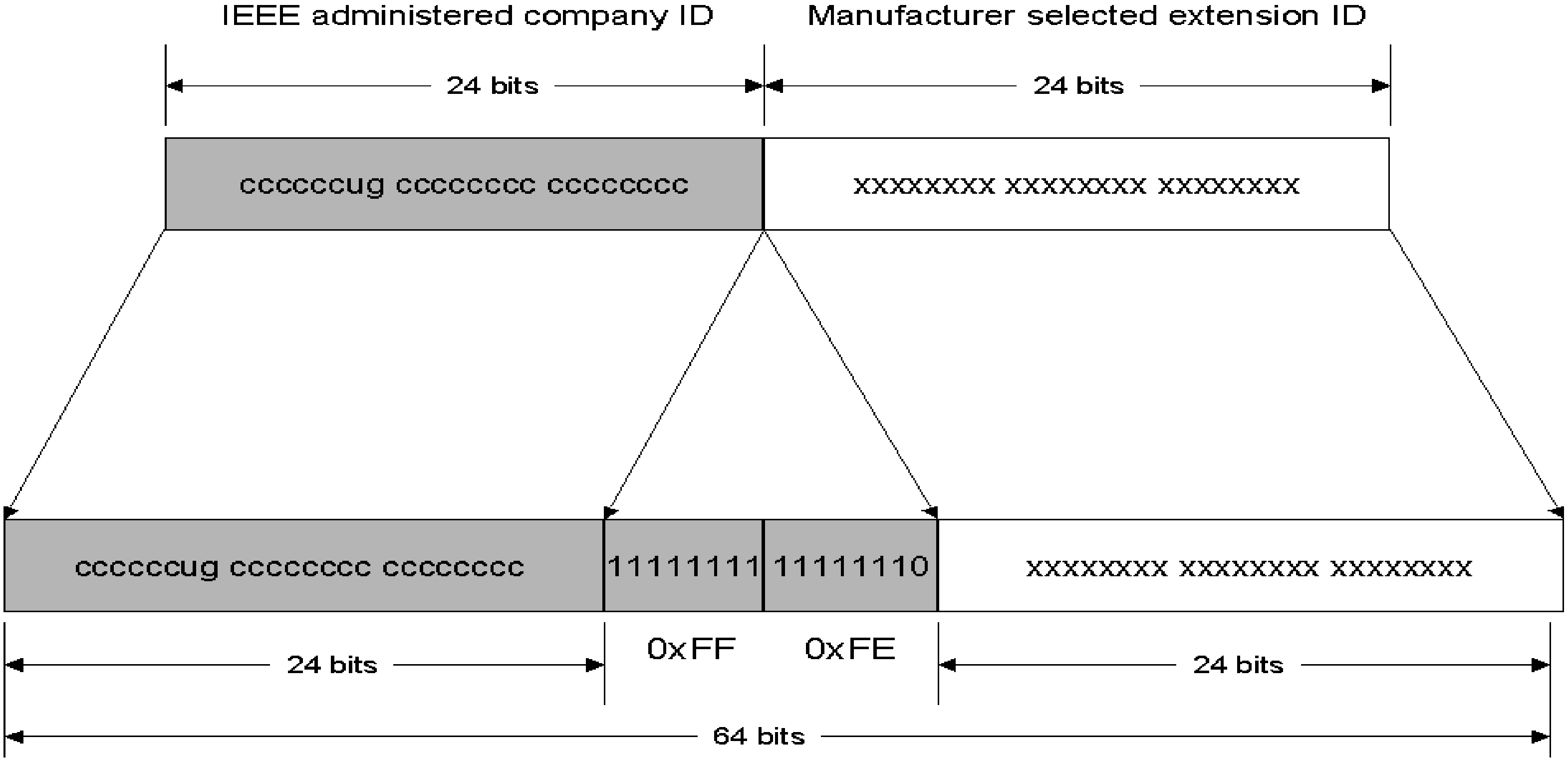
IPv6 – Interface ID

A 64 bit prefix alatti egyedi 64 bites IF cím

RFC 2373: valamennyi 001-111 prefixű unicast címnek EUI-64 (IEEE) kompatibilis IF ID címének kell lennie.

EUI-48:
(MAC)

EUI-64:



IEEE administered company ID

Manufacturer selected extension ID

24 bits

24 bits

cccccc ug cccccccc cccccccc

xxxxxxxx xxxxxxxx xxxxxxxx

cccccc ug cccccccc cccccccc

11111111

11111110

xxxxxxxx xxxxxxxx xxxxxxxx

24 bits

0xFF

0xFE

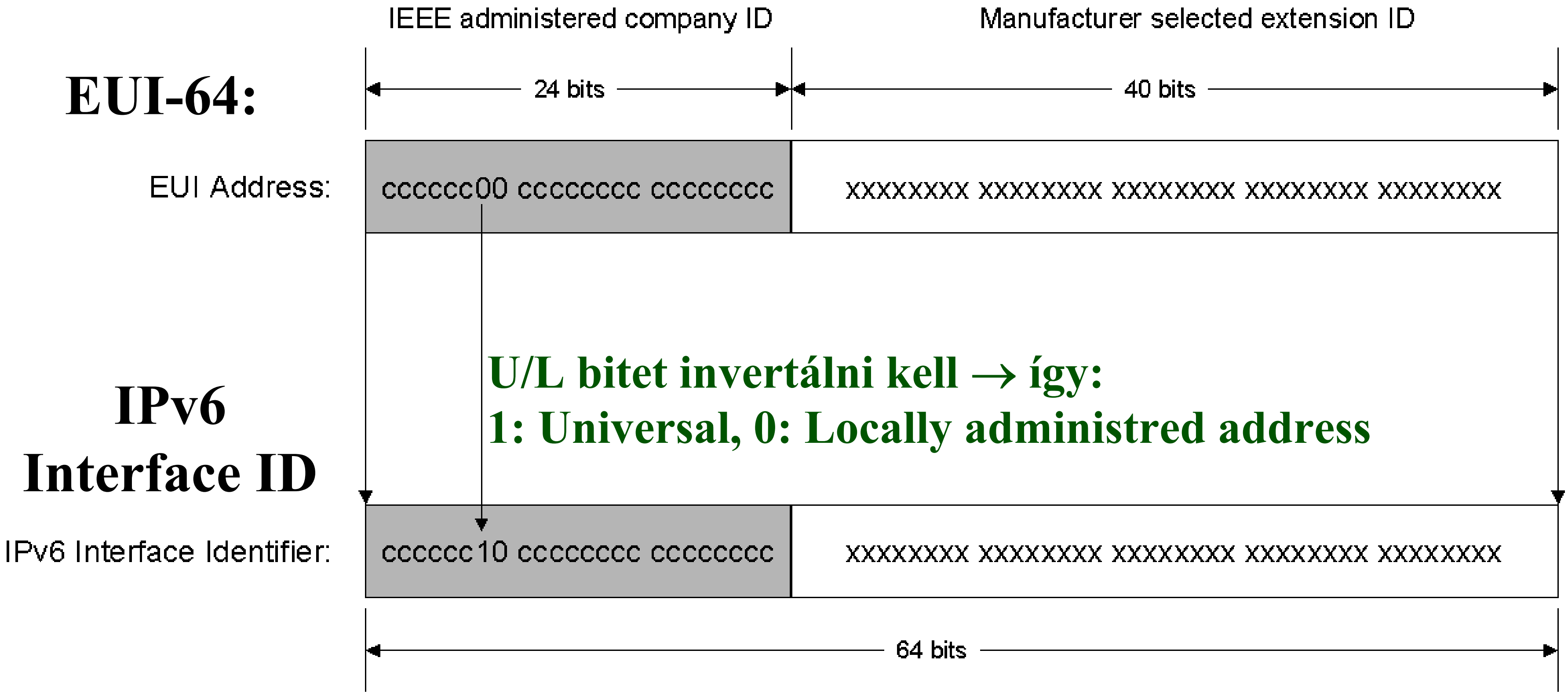
24 bits

64 bits

- U/L bit – 0: Universal, 1: Locally administred address
- I/G bit – 0: Individual (unicast), 1: Group (multicast) address

IPv6 – Interface ID

- Az Interface ID képzése az EUI-64 alapján:



EUI-64:

IEEE administered company ID

Manufacturer selected extension ID

24 bits

40 bits

EUI Address: cccccc00 cccccccc cccccccc xxxxxxxx xxxxxxxx xxxxxxxx xxxxxxxx xxxxxxxx

U/L bitet invertálni kell → így:
1: Universal, 0: Locally administred address

IPv6 Interface ID

IPv6 Interface Identifier: cccccc10 cccccccc cccccccc xxxxxxxx xxxxxxxx xxxxxxxx xxxxxxxx xxxxxxxx

64 bits

Lokálisan adminisztrált Interface ID-k esetén tehát a 7. bitnek 0-nak kell lennie ⇒

IPv6 – Miskolci Egyetem Hbone 6Net

Az IPv6 cimek kiosztasaval kapcsolatosan Burmeister Norberttel es Vitez Gaborral kozosen az alabbiakat gondoltuk ki:

A prefix, amit az egyetem kapott: 2001:0738:6001::/48

Igy ugy lehetne egyszeruen IPv6 cimeket kiosztani - a mar meglevo IPv4 cimek alapjan, hogy az egyes halozatok prefixe legyen:

2001:0738:6001:xx00::/64

ahol xx a mar meglevo IPv4 halocim utolso elotti byte-ja hexaban

pl: 193.6.5.0 eseten xx=5, 193.225.63.0 eseten 3F,

vagyis a prefix 2001:0738:6001:0500::/64,

illetve 2001:0738:6001:3F00::/64.

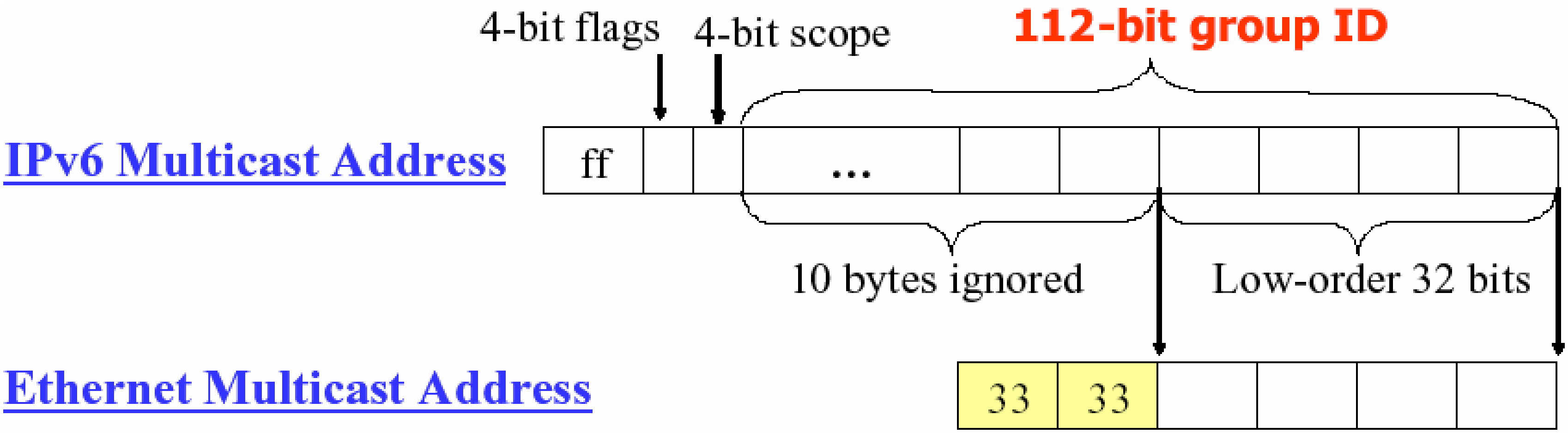
Az egyes allomascimek (Interface ID) pedig a meglevo IPv4 cim alapjan az alabbiak szerint kepezhetoek:2001:0738:6001:xx00::00yy

ahol yy az IPv4 host bitek erteke hexaban

pl: a 193.6.5.73 IPv6 cime az lehetne, hogy 2001:0738:6001:0500::49.

Ez azert is jo lehetne, mert igy az egyes epuletekre konnyeden lehet tovabbi halocimeket is kiosztani pl. xx01 stb., illetve egyszeruen lehet a kesobbiekben routing hierarchiat kialakitani /48 es /64 koze eso maszkok valasztasaval.

Mapping IPv6 Multicast Addresses to Ethernet Addresses



Pl:

- **Link-local scope all-nodes multicast address of FF02::1 ⇒ 33-33-00-00-00-01**
- **Solicited-node address of FF02::1:FF3F:2A1C ⇒ 33-33-FF-3F-2A-1C**
  - **Remember that the solicited-node address is the prefix FF02::1:FF00:0/104 and the last 24-bits of the unicast IPv6 address**

IPv6 – Header tervezési megfontolások

- **Felismerhető, egyszerűsített fejrész formátum.**
- **Csökkentse a gyakori esetek csomag-feldolgozási költségeit.**
- **A címmező méretének növekedése ellenére a fejrész overhead maradjon alacsony.**
- **Támogassa a rugalmasan bővíthető fejrész opciók használatát.**
- **A 64-bites feldolgozási architektúrára legyen optimalizálva** (Headers are 64-bit aligned)

IPv6 – Header – forma

- Fix méretű IPv6 Header
  - Az IPv4-el ellentétben – az opciók nincsenek 40 byte-ra korlátozva
- Az alap fejrészben kevesebb mező van
  - Faster processing of basic packets
- 64-bitre illesztett fejrész/opciók
- Hatékony opció feldolgozás
  - Az opció mezőket csak akkor kell feldolgozni, ha léteznek.
  - Processing of most options limited performed only at destination

IPv6 – Header – feldolgozási sebesség

- A Network Layer-ből eltűnik az ellenőrző összeg
  - Az adatkapcsolati réteg megbízhatóbbá vált
  - A felsőbb rétegekben kötelező a hibaellenőrzés
    Pl: TCP, UDP, ICMPv6
- A hálózatban nincs további csomag fregmentáció
  - Csökkenti a routerek terhelését
  - Egyszerűbb hardver implementáció
  - Könnyű Layer 3 switching of IP
- Minimum link MTU is 1280 bytes
  - Az IPv4-ben ez 68 byte volt.

IPv6 – Basic Header (RFC 2460)

IPv4

Version (4)	~~HLEN (4)~~	Type of Service (8)	Total Length(16)	
~~Identification(16)~~		~~Flags(3)~~	~~Fragment Offset(13)~~	
TTL (8)	Protocol(8)	~~Header Checksum(16)~~		
Source IP Address(32)				
Destination IP Address(32)				

20 bytes ⇒ 40 bytes

IPv6

Version (4bits)	Traffic Class (8bits)	Flow Label(20bits)	
Payload Length (16 bits)		Next Header (8bits)	Hop Limit (8bits)
Source Address(128bits)			
Destination Address (128bits)			

Version: 0110, azaz 6

Traffic Class: IPv6 Class of Priority (mint IPv4 TOS), még nincs definiálva

Flow label: adatfolyam azonosító For non-default quality of service connections. Default: Flow Label = 0.

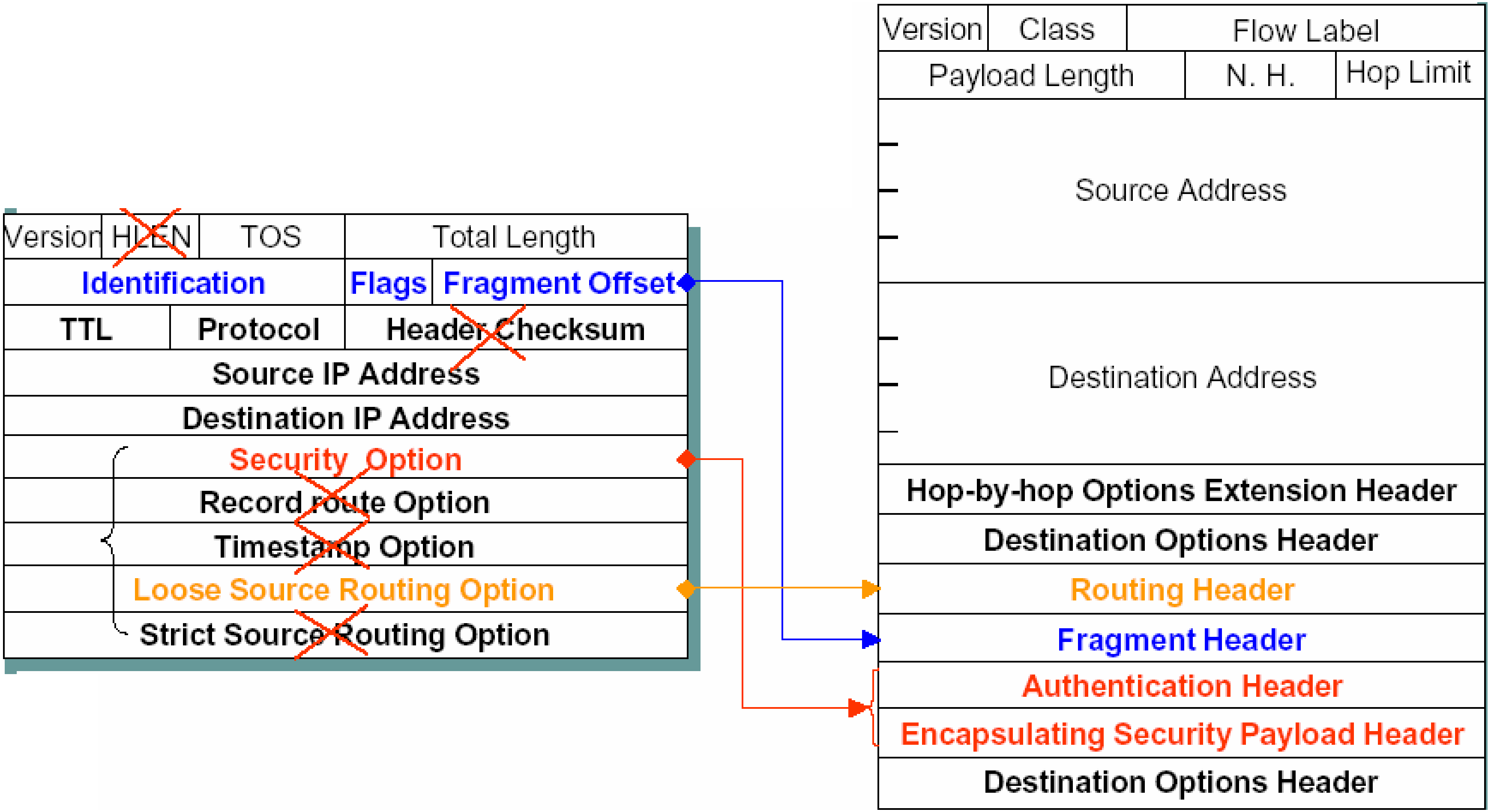
Payload Length: a csomag hasznos mérete, max. 65535 byte – ha hosszabb: Payload Length = 0 és **Jumbo Payload option** in the **Hop-by-Hop Options** **Extension Header**.

Next Header: a következő extension header típusa

Hop limit: ugrásszámláló (csökken, 0 eldob)

Next Header – 0:Hop-by-Hop Options Header, 6:TCP, 17:UDP, 43:Routing Header, 44:Fragment Header, 58:ICMPv6, 59:No next header, 60:Destination Options Header

IPv6 – Extension Headers (RFC 2460)



Version | ~~HLEN~~ | TOS | Total Length

Identification | Flags | Fragment Offset

TTL | Protocol | ~~Header Checksum~~

Source IP Address

Destination IP Address

Security Option

~~Record route Option~~

~~Timestamp Option~~

Loose Source Routing Option

~~Strict Source Routing Option~~

Version | Class | Flow Label

Payload Length | N. H. | Hop Limit

Source Address

Destination Address

Hop-by-hop Options Extension Header

Destination Options Header

Routing Header

Fragment Header

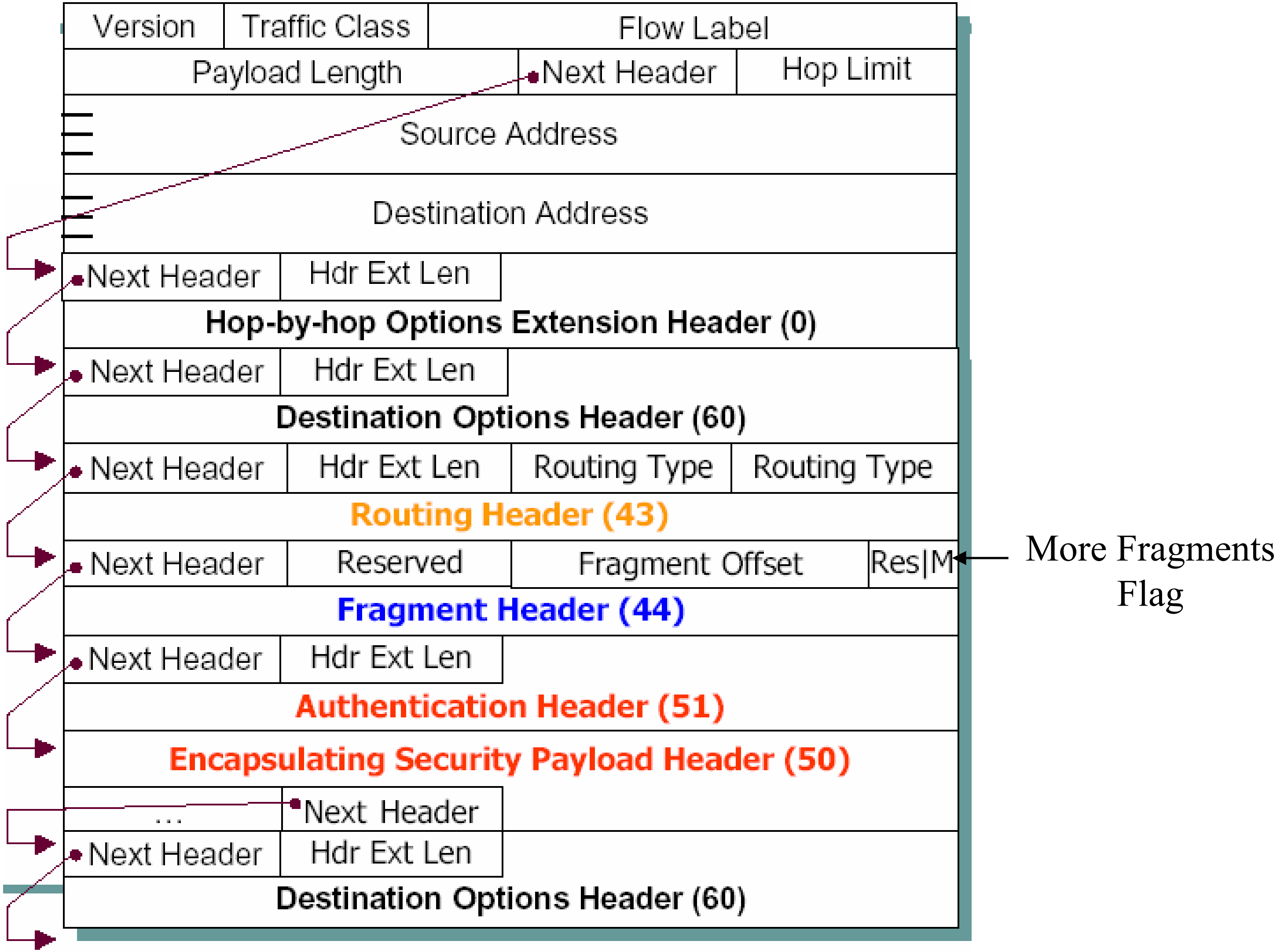
Authentication Header

Encapsulating Security Payload Header

Destination Options Header

- Delivery and forwarding options are moved to extension headers.
- The only extension header that must be processed at each intermediate router is the Hop-by-Hop Options extension header

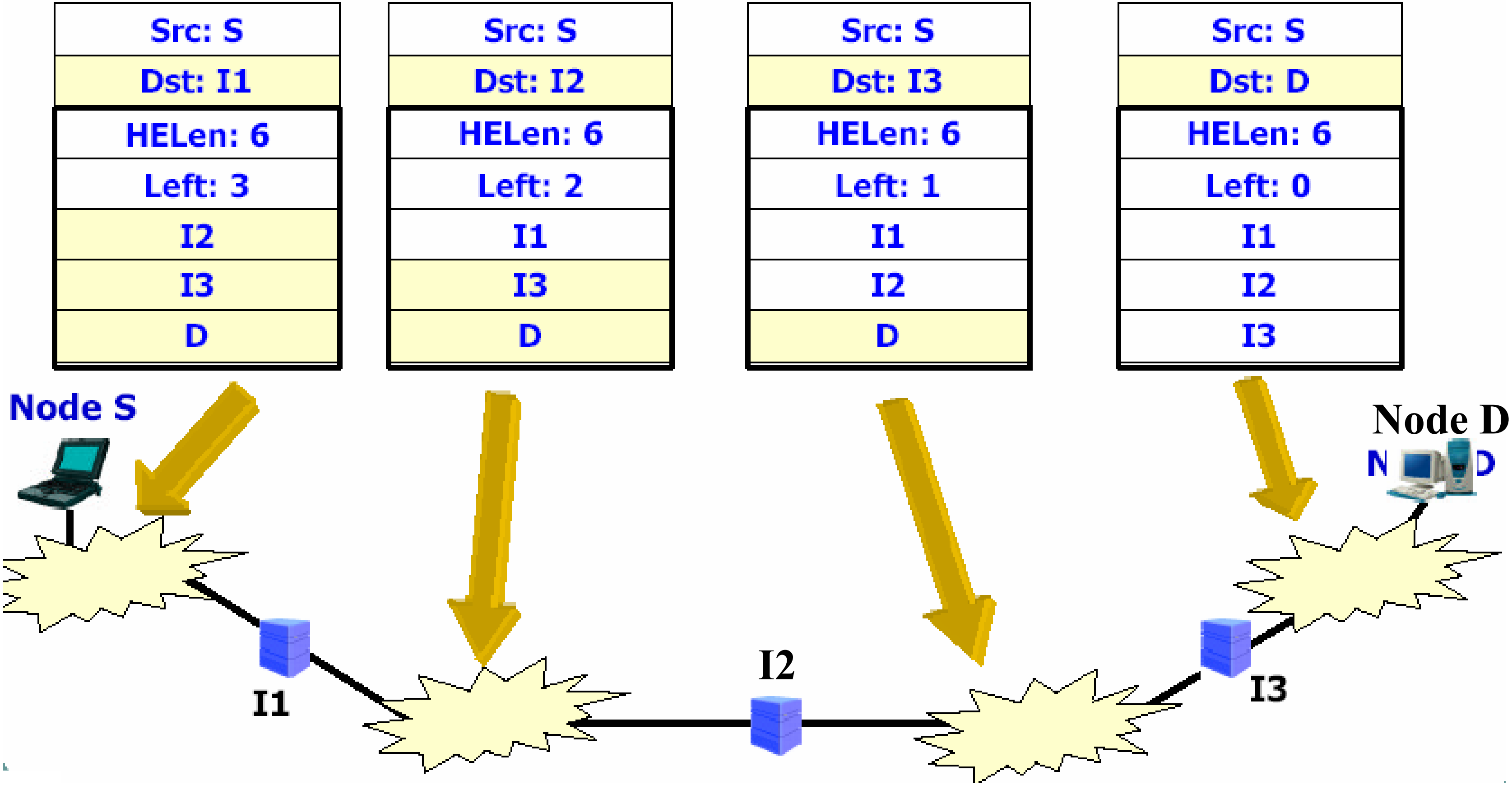
IPv6 – Extension Headers (RFC 2460)



More Fragments Flag

- **Minden Extension Header-ben van egy Next Header, ami a következő típusa.**

IPv6 – Extension Headers (pl. Routing Header)



Src: S	Src: S	Src: S	Src: S
Dst: I1	Dst: I2	Dst: I3	Dst: D
HELen: 6	HELen: 6	HELen: 6	HELen: 6
Left: 3	Left: 2	Left: 1	Left: 0
I2	I1	I1	I1
I3	I3	I2	I2
D	D	D	I3

- **A Routing extension header használható a loose source route meghatározására (az útvonal listája a célig).**

IPv6 – Extension Headers (RFC 2460)

- Hop-by-hop options header (type:0)
  - jumbo payload (csomagméret > 65535)
    → az eredeti Payload Lenght:0 – helyette a kiegészítő fejlécben 32 bit hossz (max 4 terabyte) hasznos csomagméret
  - router alert: routernek szóló információ
- Routing header
  - loose source routing (mezők a kívánt út IP címeinek)
- Fragment header
  - Az IPv6-ban, csak a forrás darabolhatja a küldendő adatokat (payload). If the payload submitted by the upper layer protocol is larger than the link or path MTU, then IPv6 fragments the payload at the source and uses the Fragment extension header to provide reassembly information.

IPv6 – ICMPv6

- IPv6 does not provide facilities for reporting errors.
- Instead, IPv6 uses Internet Control Message Protocol version 6 (ICMPv6).
- Error Messages:
  - Destination Unreachable
  - Packet Too Big
  - Time Exceeded
  - Parameter Problem
- Informational Messages:
  - Echo Request/Reply
  - De nincs forrásfolytás (Source Quench)
- Multicast Listener Discovery (MLD)
- Neighbor Discovery (ND)

ICMPv6 - Path MTU Discovery

- The sending node assumes that the path MTU is the link MTU of the interface on which the traffic is being forwarded.
- The sending node sends IPv6 packets at the path MTU size.
- If a router on the path is unable to forward the packet over a link with a link MTU that is smaller than the size of the packet, it discards the IPv6 packet and sends an ICMPV6 Packet Too Big message back to the sending node. The ICMPV6 Packet Too Big message contains the link MTU of the link on which the forwarding failed.
- The sending node sets the path MTU for packets being sent to the destination to the value of the MTU field in the ICMPv6 Packet Too Big message.

ICMPv6 - Multicast Listener Discovery

- MLD is a set of messages exchanged by routers and nodes, enabling routers to discover the set of multicast addresses for which there are listening nodes for each attached interface.

Multicast Listener Query:

- Used by a router to query a link for multicast listeners.
  - The General Query is used to query for multicast listeners of all multicast addresses.
  - Multicast-Address-Specific Query is used to query for multicast listeners of a specific multicast address.

Multicast Listener Report:

- Used by a multicast listener to either report interest in receiving multicast traffic for a specific multicast address or to respond to a Multicast Listener Query.

Multicast Listener Done:

- Used by a multicast listener to report that it is no longer interested in receiving multicast traffic for a specific multicast address.

ICMPv6 - Neighbor Discovery (ND)

ND is used by hosts to:

- Discover neighboring routers.
- Discover addresses, address prefixes, and other configuration parameters.

ND is used by routers to:

- Advertise their presence, host configuration parameters, and on-link prefixes.
- Inform hosts of a better next-hop address to forward packets for a specific destination.

ND is used by nodes to:

- Resolve the link-layer address of a neighboring node to which an IPv6 packet is being forwarded and determine when the link-layer address of a neighboring node has changed.
- Determine whether a neighbor is still reachable.

ICMPv6 - Address Resolution Example

- Host A has an Ethernet MAC address of 00-AA-00-11-11-11
  and a corresponding link-local address of FE80::2AA:FF:FE11:1111.
- Host B has an Ethernet MAC address of 00-AA-00-22-22-22
  and a corresponding link-local address of FE80::2AA:FF:FE22:2222.
- To send a packet to Host B, Host A must use address resolution to resolve Host B's link-layer address.
- Based on Host B's IP address, Host A sends a solicited-node multicast Neighbor Solicitation to the address of FF02::1:FF22:2222

ICMPv6 - Address Resolution Example

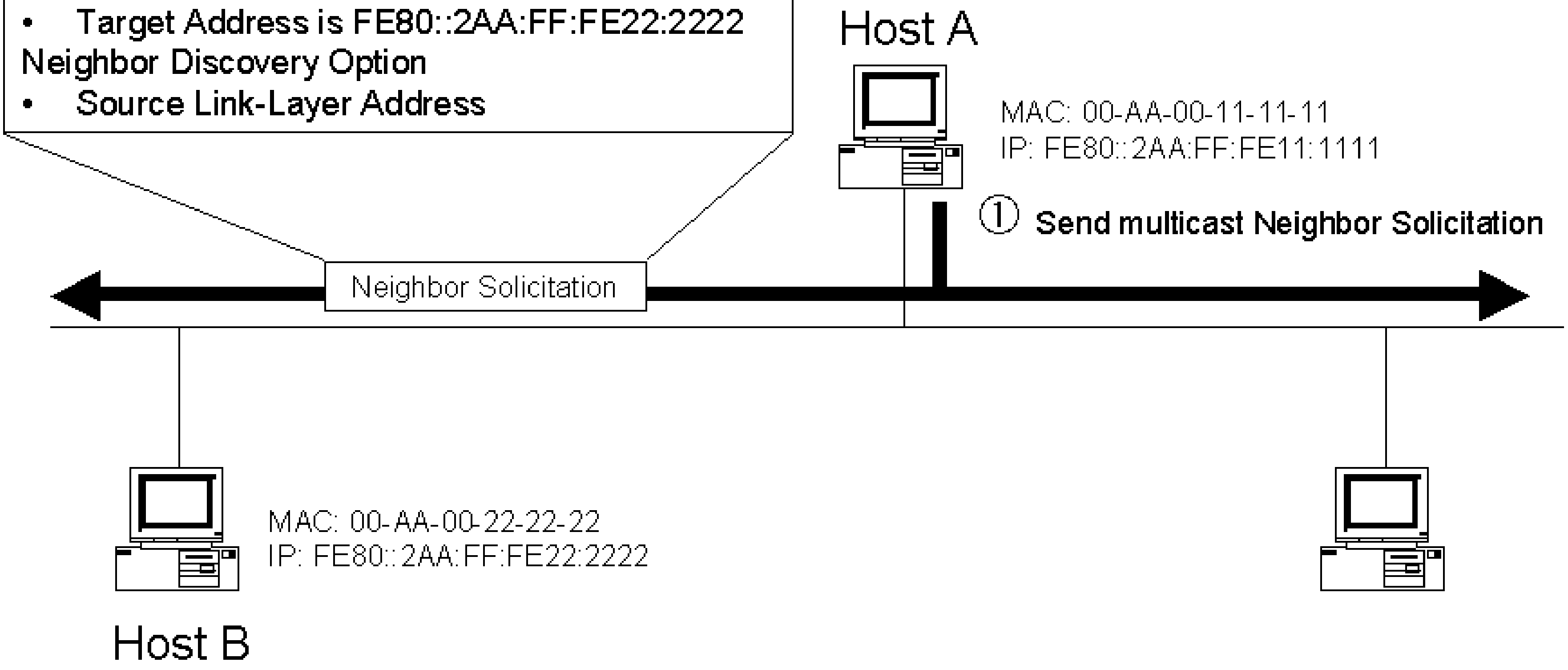
Ethernet Header
- Dest MAC is 33-33-FF-22-22-22

IPv6 Header
- Source Address is FE80::2AA:FF:FE11:1111
- Destination Address is FF02::1:FF22:2222
- Hop limit is 255

Neighbor Solicitation Header
- Target Address is FE80::2AA:FF:FE22:2222

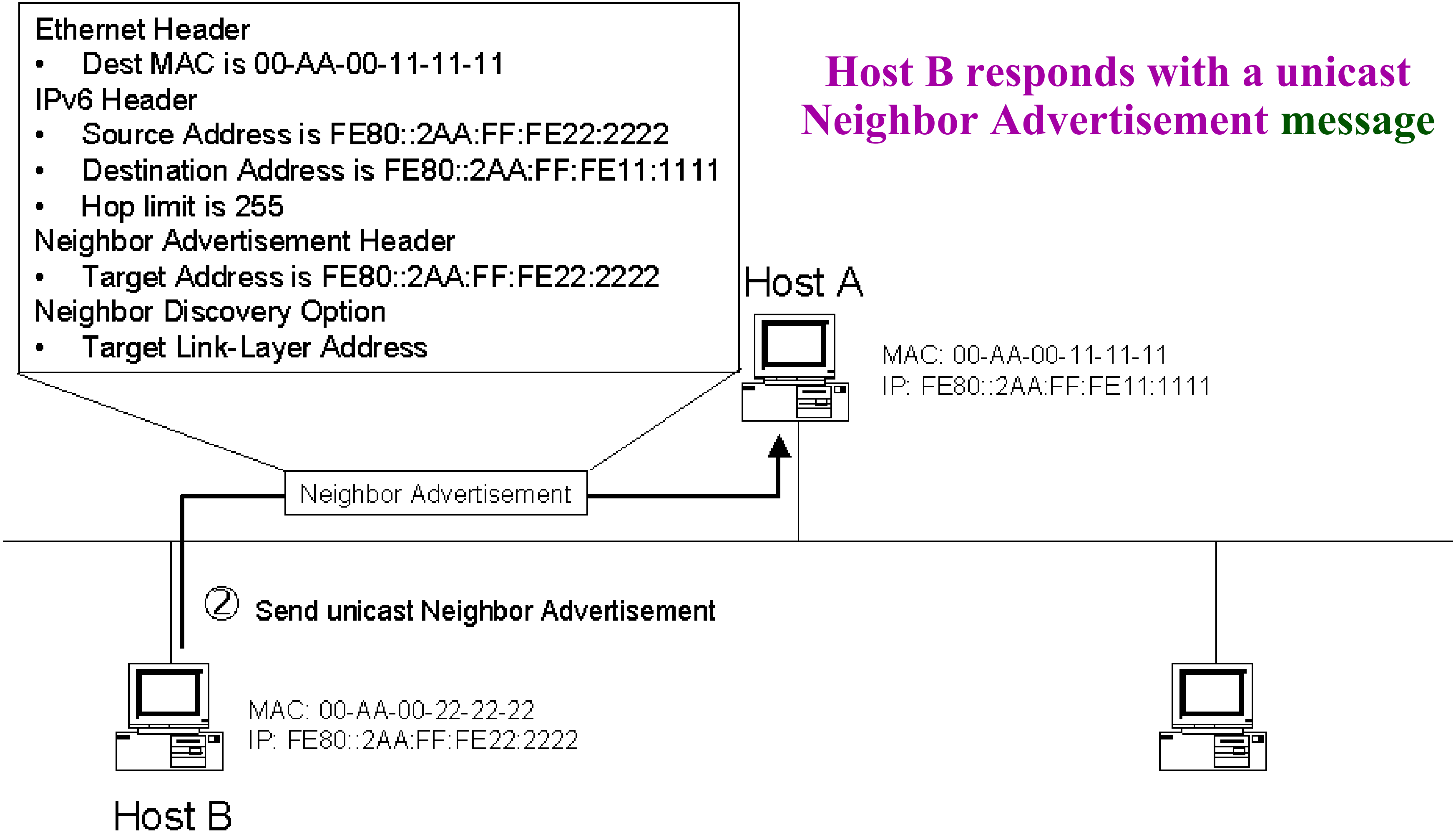
Neighbor Discovery Option
- Source Link-Layer Address

Based on Host B’s IP address, Host A sends a solicited-node multicast Neighbor Solicitation to the address of FF02::1:FF22:2222


Host A
MAC: 00-AA-00-11-11-11
IP: FE80::2AA:FF:FE11:1111
① Send multicast Neighbor Solicitation
Neighbor Solicitation
MAC: 00-AA-00-22-22-22
IP: FE80::2AA:FF:FE22:2222
Host B

ICMPv6 - Address Resolution Example

Host B responds with a unicast Neighbor Advertisement message



Ethernet Header
- Dest MAC is 00-AA-00-11-11-11

IPv6 Header
- Source Address is FE80::2AA:FF:FE22:2222
- Destination Address is FE80::2AA:FF:FE11:1111
- Hop limit is 255

Neighbor Advertisement Header
- Target Address is FE80::2AA:FF:FE22:2222

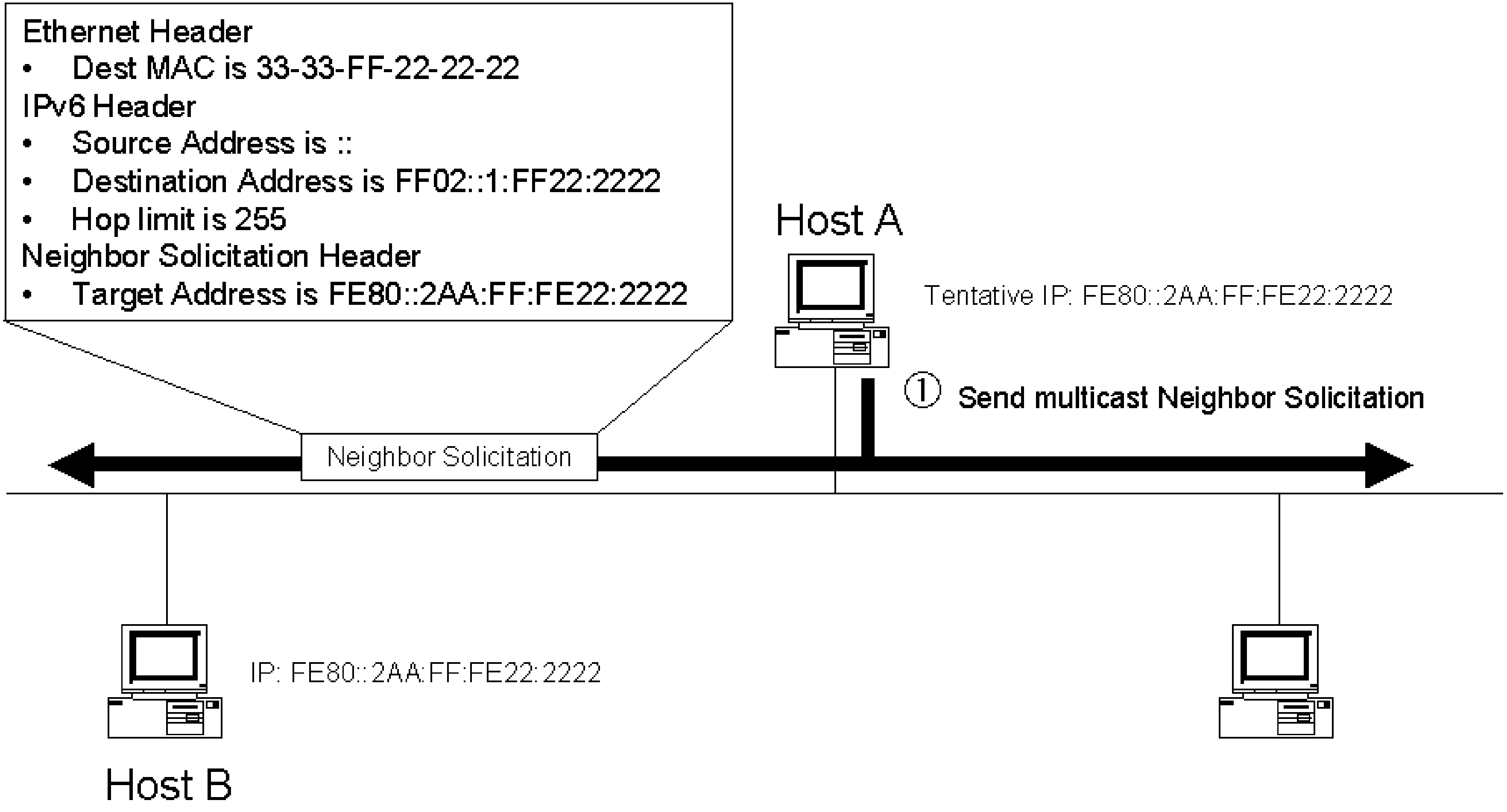
Neighbor Discovery Option
- Target Link-Layer Address

Host A
MAC: 00-AA-00-11-11-11
IP: FE80::2AA:FF:FE11:1111
Neighbor Advertisement
② Send unicast Neighbor Advertisement
MAC: 00-AA-00-22-22-22
IP: FE80::2AA:FF:FE22:2222
Host B

ICMPv6 - Duplicate Address Detection

- IPv6 nodes use the Neighbor Solicitation message to detect duplicate address use on the local link.
- In the duplicate address detection Neighbor Solicitation message, the Source Address field in the IPv6 header is set to the unspecified address (::).
  - The address being queried for duplication cannot be used until it is determined that there are no duplicates.
- In the Neighbor Advertisement reply to a duplicate address detection Neighbor Solicitation message, the Destination Address in the IP header is set to the link-local scope all-nodes multicast address (FF02::1).
  - The Solicited flag in the Neighbor Advertisement message is set to 0.
  - Because the sender of the duplicate address detection Neighbor Solicitation message is not using the desired IP address, it cannot receive unicast Neighbor Advertisements.
  - Therefore, the Neighbor Advertisement is multicast.
- Duplikáció esetén a Node nem használja a duplikált címet

ICMPv6 - Duplicate Address Detection Pl:



Ethernet Header

- Dest MAC is 33-33-FF-22-22-22

IPv6 Header

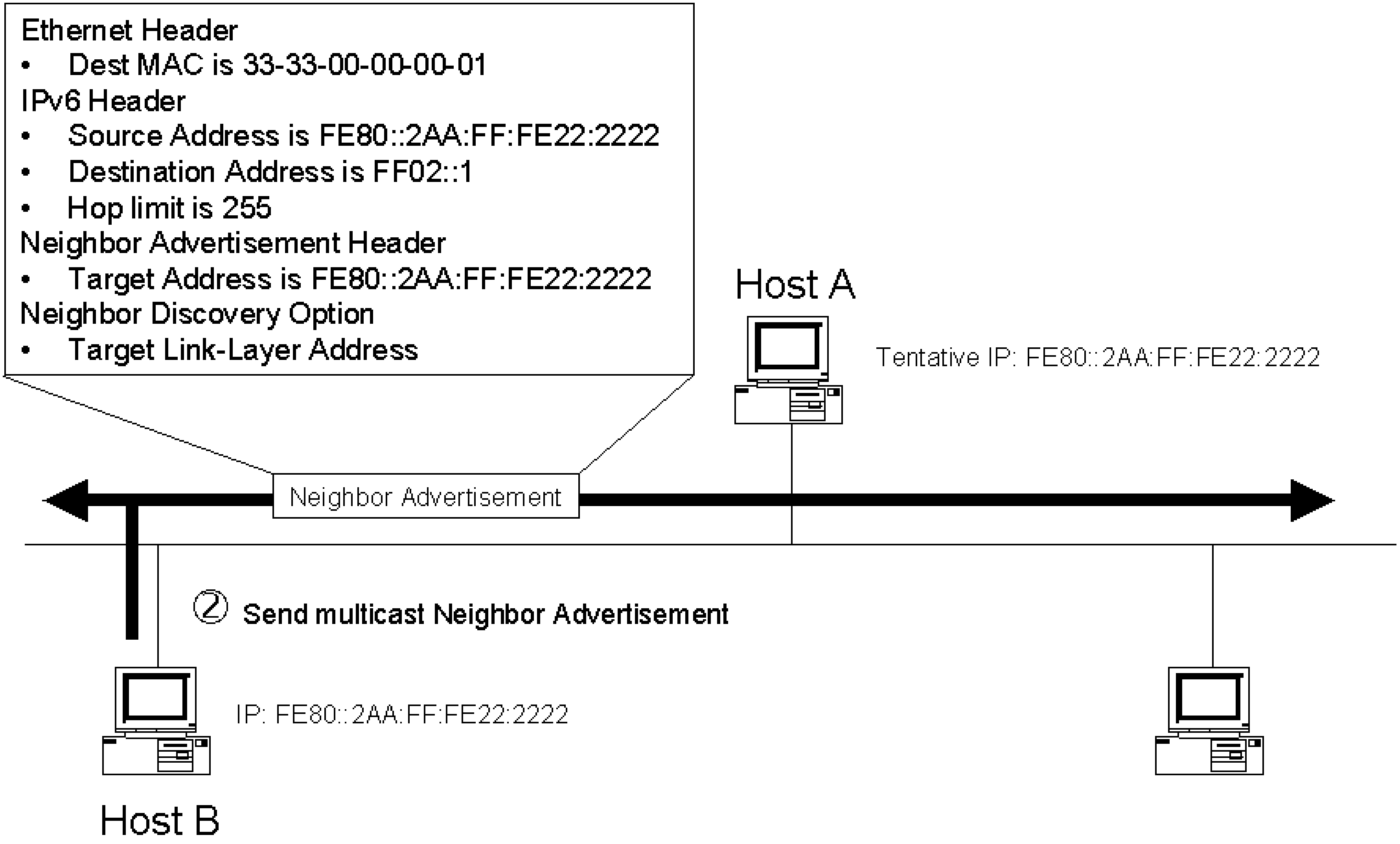
- Source Address is ::
- Destination Address is FF02::1:FF22:2222
- Hop limit is 255

Neighbor Solicitation Header

- Target Address is FE80::2AA:FF:FE22:2222

Host A
Tentative IP: FE80::2AA:FF:FE22:2222
① Send multicast Neighbor Solicitation
Neighbor Solicitation
IP: FE80::2AA:FF:FE22:2222
Host B

ICMPv6 - Duplicate Address Detection Pl:



Ethernet Header
- Dest MAC is 33-33-00-00-00-01

IPv6 Header
- Source Address is FE80::2AA:FF:FE22:2222
- Destination Address is FF02::1
- Hop limit is 255

Neighbor Advertisement Header
- Target Address is FE80::2AA:FF:FE22:2222

Neighbor Discovery Option
- Target Link-Layer Address

Host A

Tentative IP: FE80::2AA:FF:FE22:2222

Neighbor Advertisement

② Send multicast Neighbor Advertisement

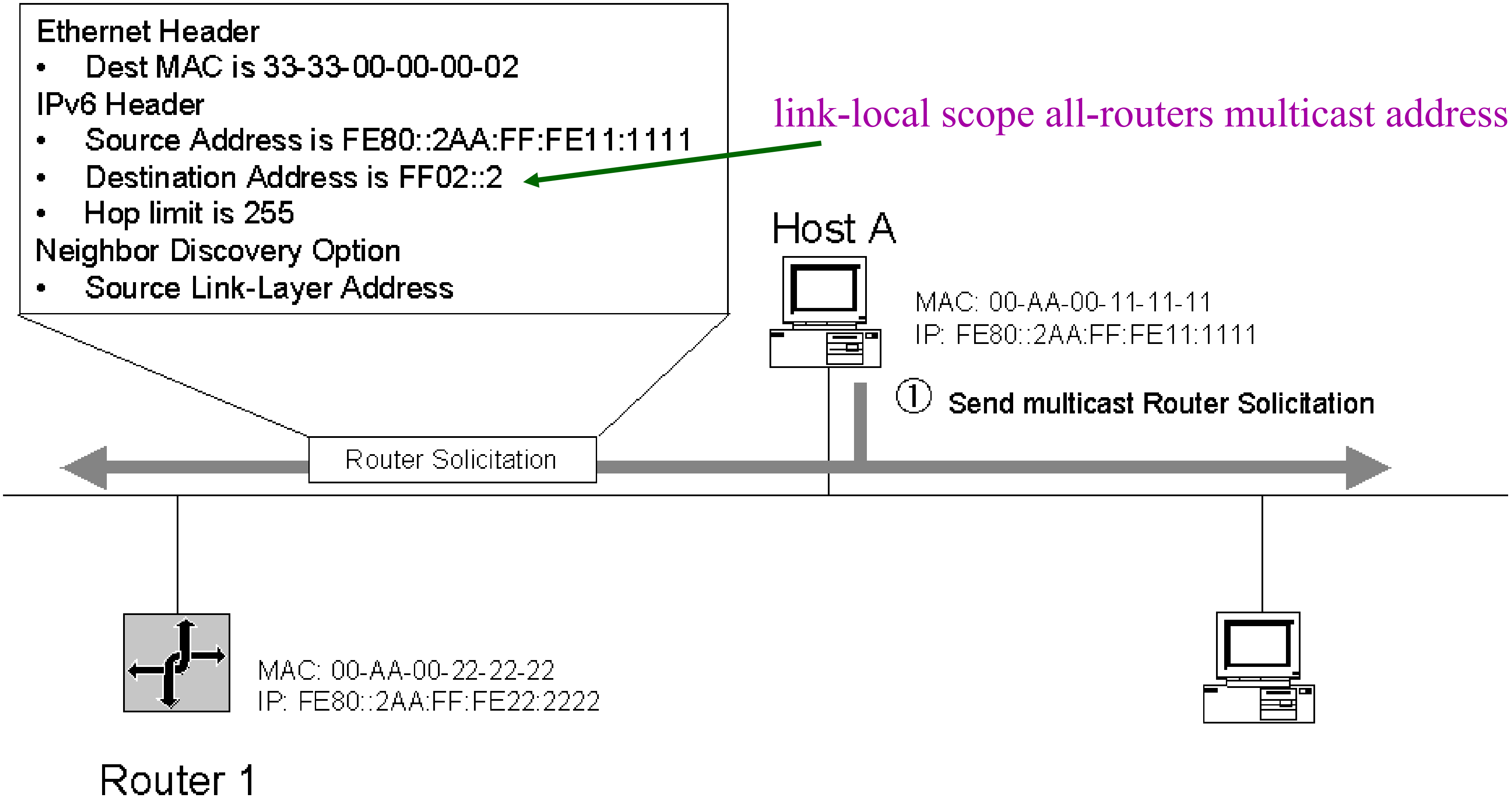
IP: FE80::2AA:FF:FE22:2222

Host B

ICMPv6 - Router Discovery

- Router discovery is the process through which nodes attempt to discover the set of routers on the local link.
- IPv6 routers periodically send a Router Advertisement message on the local link advertising their existence as routers.
  - They also provide configuration parameters such as default hop limit, MTU, and prefixes.
- Active IPv6 hosts on the local link receive the Router Advertisement messages and use the contents to maintain the default router list, the prefix list, and other configuration parameters.
- A host that is starting up sends a Router Solicitation message to the link-local scope all-routers multicast address (FF02::2).
- Upon receipt of a Router Solicitation message, all routers on the local link send a unicast Router Advertisement message to the node that sent the Router Solicitation.
- The node receives the Router Advertisement messages and uses their contents to build the default router and prefix lists and set other configuration parameters.

ICMPv6 - Router Discovery Pl:



Ethernet Header
- Dest MAC is 33-33-00-00-00-02

IPv6 Header
- Source Address is FE80::2AA:FF:FE11:1111
- Destination Address is FF02::2
- Hop limit is 255

Neighbor Discovery Option
- Source Link-Layer Address

link-local scope all-routers multicast address

Host A

MAC: 00-AA-00-11-11-11
IP: FE80::2AA:FF:FE11:1111

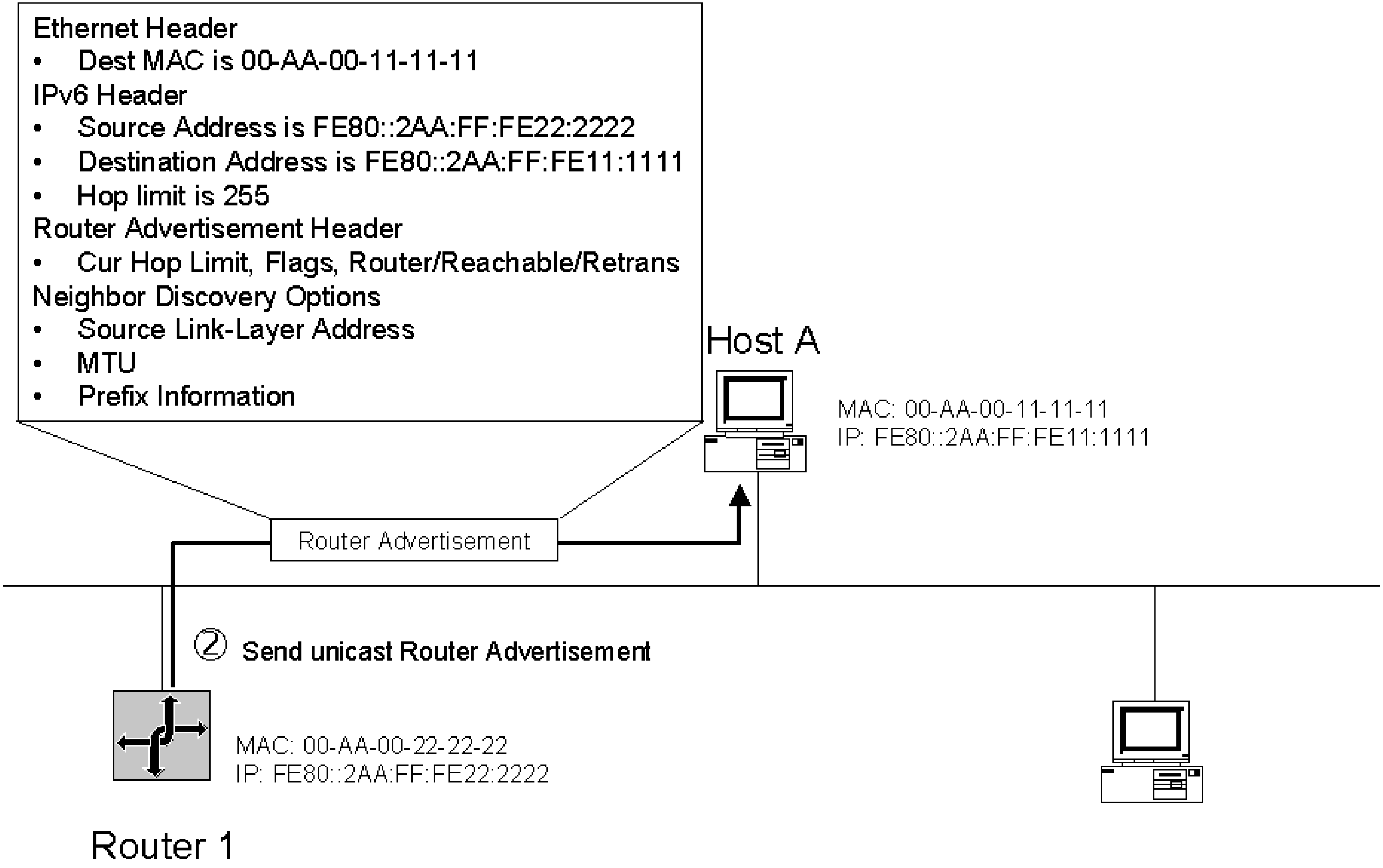
① Send multicast Router Solicitation

Router Solicitation

MAC: 00-AA-00-22-22-22
IP: FE80::2AA:FF:FE22:2222

Router 1

ICMPv6 - Router Discovery Pl:



Ethernet Header
- Dest MAC is 00-AA-00-11-11-11

IPv6 Header
- Source Address is FE80::2AA:FF:FE22:2222
- Destination Address is FE80::2AA:FF:FE11:1111
- Hop limit is 255

Router Advertisement Header
- Cur Hop Limit, Flags, Router/Reachable/Retrans

Neighbor Discovery Options
- Source Link-Layer Address
- MTU
- Prefix Information

Router Advertisement

② Send unicast Router Advertisement

Host A

MAC: 00-AA-00-11-11-11
IP: FE80::2AA:FF:FE11:1111

Router 1

MAC: 00-AA-00-22-22-22
IP: FE80::2AA:FF:FE22:2222

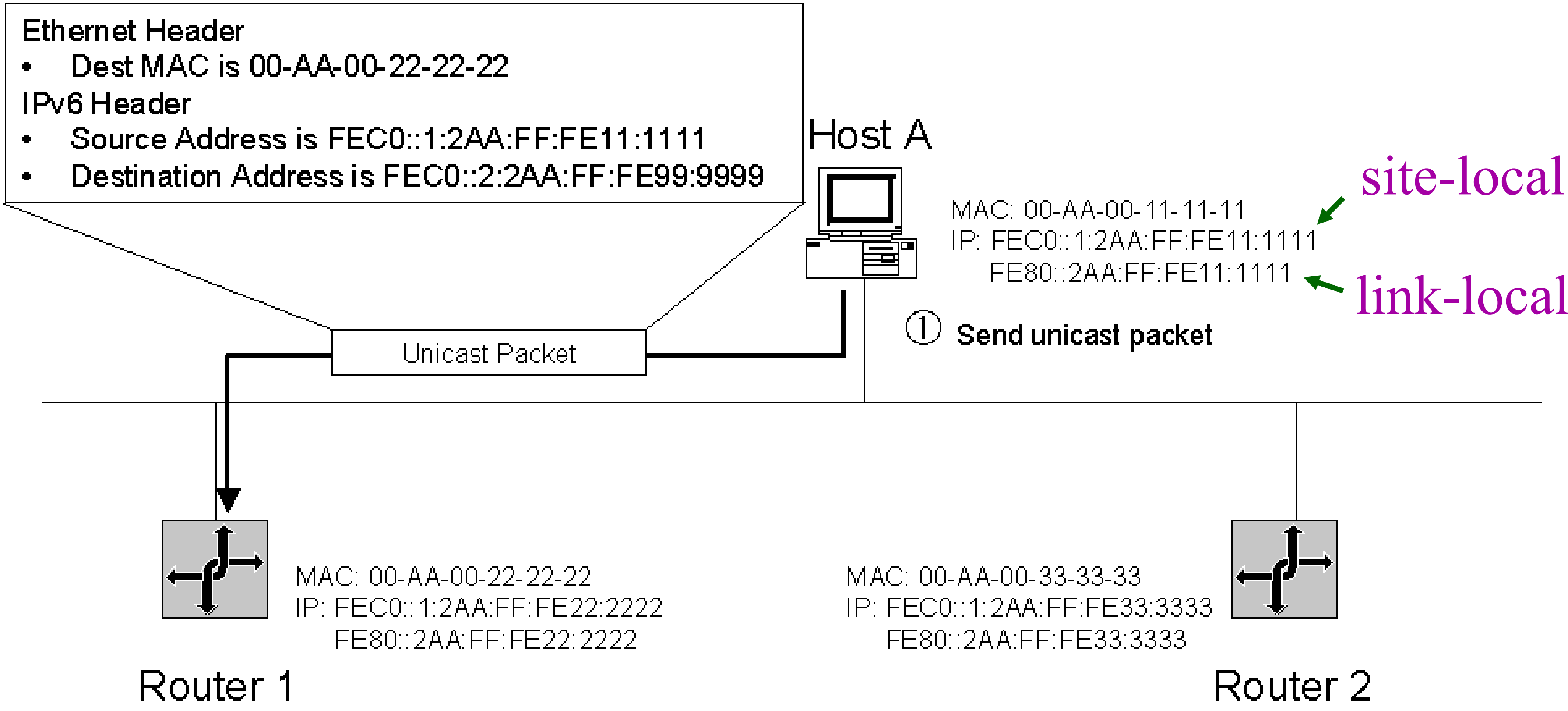
ICMPv6 – Redirect Function

- Routers use the redirect function to inform originating hosts of a better first-hop neighbor to which traffic should be forwarded for a specific destination.
- Redirect messages are only sent by the first router in the path between the originating host and the destination and like ICMPv6 error messages are rate limited.
- Hosts never send Redirect messages and routers never update routing tables based on the receipt of a Redirect message

ICMPv6 – Redirect Function

- The originating host forwards a unicast packet to its default router.
- The router processes the packet and notes that the address of the originating host is a neighbor. Additionally, it notes that the addresses of both the originating host and the next-hop are on the same link.
- The router forwards the packet to the appropriate next-hop address.
- The router sends the originating host a Redirect message. In the Target Address field of the Redirect message is the next-hop address of the node to which the originating host should send packets addressed to the destination.
- For packets redirected to a router, the Target Address field is set to the link-local address of the router. For packets redirected to a host, the Target Address field is set to the destination address of the packet originally sent.
- The Redirect message includes the Redirected Header option. It might also include the Target Link-Layer Address option.
- Upon receipt of the Redirect message, the originating host updates the destination address entry in the destination cache with the address in the Target Address field. If the Target Link-Layer Address option is included in the Redirect message, its contents are used to create or update the corresponding neighbor cache entry.

ICMPv6 – Redirect Function Pl:



Ethernet Header

- Dest MAC is 00-AA-00-22-22-22

IPv6 Header

- Source Address is FEC0::1:2AA:FF:FE11:1111
- Destination Address is FEC0::2:2AA:FF:FE99:9999

Host A

MAC: 00-AA-00-11-11-11
IP: FEC0::1:2AA:FF:FE11:1111
FE80::2AA:FF:FE11:1111

site-local

link-local

① Send unicast packet

Unicast Packet

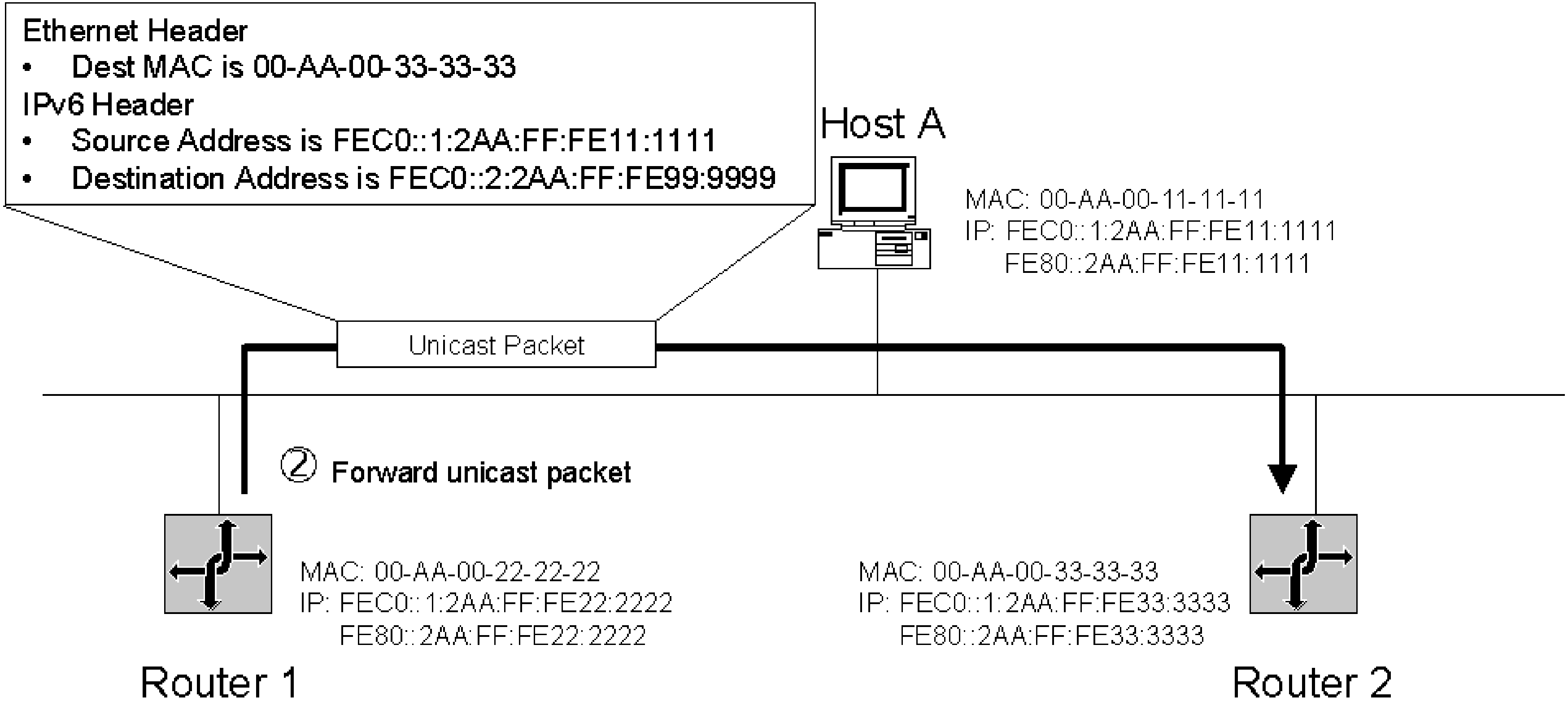
MAC: 00-AA-00-22-22-22
IP: FEC0::1:2AA:FF:FE22:2222
FE80::2AA:FF:FE22:2222

Router 1

MAC: 00-AA-00-33-33-33
IP: FEC0::1:2AA:FF:FE33:3333
FE80::2AA:FF:FE33:3333

Router 2

ICMPv6 – Redirect Function Pl:



Ethernet Header
- Dest MAC is 00-AA-00-33-33-33

IPv6 Header
- Source Address is FEC0::1:2AA:FF:FE11:1111
- Destination Address is FEC0::2:2AA:FF:FE99:9999

Unicast Packet

Host A

MAC: 00-AA-00-11-11-11
IP: FEC0::1:2AA:FF:FE11:1111
FE80::2AA:FF:FE11:1111

② Forward unicast packet

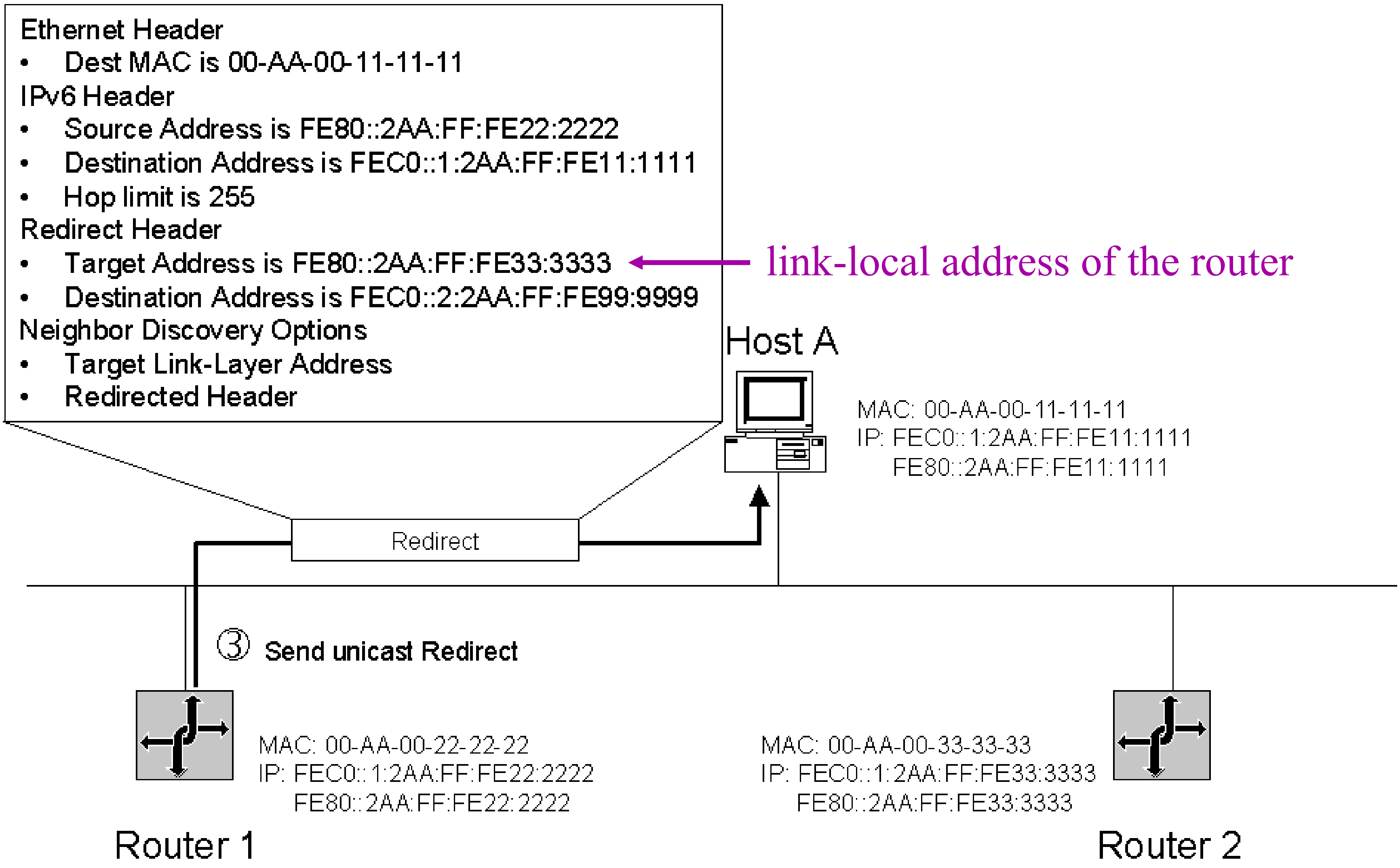
Router 1

MAC: 00-AA-00-22-22-22
IP: FEC0::1:2AA:FF:FE22:2222
FE80::2AA:FF:FE22:2222

Router 2

MAC: 00-AA-00-33-33-33
IP: FEC0::1:2AA:FF:FE33:3333
FE80::2AA:FF:FE33:3333

ICMPv6 – Redirect Function Pl:



Ethernet Header

- Dest MAC is 00-AA-00-11-11-11

IPv6 Header

- Source Address is FE80::2AA:FF:FE22:2222
- Destination Address is FEC0::1:2AA:FF:FE11:1111
- Hop limit is 255

Redirect Header

- Target Address is FE80::2AA:FF:FE33:3333 ← link-local address of the router
- Destination Address is FEC0::2:2AA:FF:FE99:9999

Neighbor Discovery Options

- Target Link-Layer Address
- Redirected Header