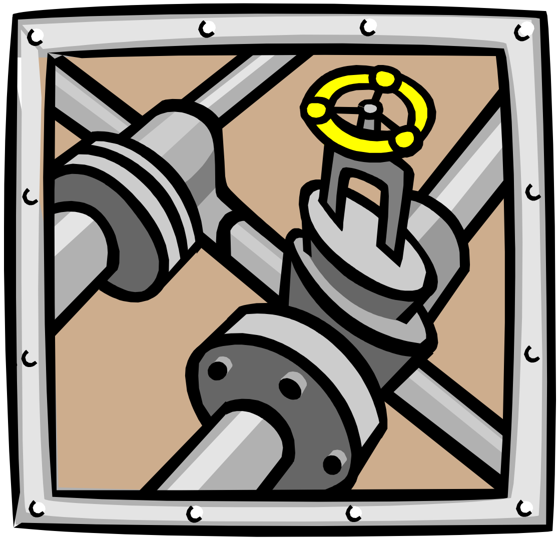
IPv6 In Depth

ICMPv6

PMTU for IPv6

NDP for IPv6

Internet Control Message Protocol version 6 (ICMPv6)



Protocol Overview

- ICMPv6 is a multipurpose protocol used for
  - Reporting errors encountered in processing packets
  - Performing diagnostics
  - Performing Neighbor Discovery
  - Reporting multicast memberships.
- ICMP messages are transported within an IPv6 packet in which extension headers can also be present.
- An ICMP message is identified by a value of **58 in the Next Header** field of the IPv6 header or of the preceding Header.

ICMPv6: Introduction

- IPv6 uses the ICMP as defined for IPv4 with a number of changes.
- The resulting protocol is called ICMPv6.
- ICMP messages, delivered in IP packets, are used for out-of-band messages related to network operation or mis-operation.
- ICMP uses IP, ICMP packet delivery is unreliable, so hosts can't count on receiving ICMP packets for any network problem.

ICMPv6: Introduction

- **The ICMPv6** is an integral part of the IPv6 architecture and must be completely supported by all IPv6 implementations.
- ICMPv6 combines functions previously subdivided among different protocols, such as
  - ICMP (Internet Control Message Protocol version 4)
  - IGMP (Internet Group Membership Protocol)
  - ARP (Address Resolution Protocol)
- It introduces some simplifications by eliminating obsolete types of messages no longer in use.

ICMP: Functions

- **Announce network errors**
  - A host or entire portion of the network being unreachable, due to some type of failure.
  - A TCP or UDP packet directed at a port number with no receiver attached is also reported via ICMP.
- **Announce network congestion**
  - When a router begins buffering too many packets, due to an inability to transmit them as fast as they are being received, it will generate **ICMP *Source Quench* messages**.
  - Directed at the sender, these messages should cause the rate of packet transmission to be slowed.
  - Generating too many Source Quench messages would cause even more network congestion, so they are used sparingly.

ICMP: Functions

- **Assist Troubleshooting**
  - ICMP supports an ***Echo*** function, which just sends a packet on a round--trip between two hosts.
  - Ping will transmit a series of packets, measuring average round--trip times and computing loss percentages.
- **Announce Timeouts**
  - If an IP packet's TTL field drops to zero, the router discarding the packet will often generate an ICMP packet announcing this fact.
  - TraceRoute is a tool which maps network routes by sending packets with small TTL values and watching the ICMP timeout announcements.

ICMPv6 Header

- **Three Fields**
  1. **Type (8 bits)**
     - Indicates the type of the message.
     - If the high order bit = 0 (0- 127)→ error message
     - if the high-order bit = 1 (128 – 255) → information message.
  2. **Code (8 bits)**
     - content depends on the message type, and it is used to create an additional level of message granularity.
  3. **Checksum (16 bits)**
     - Used to detect errors in the ICMP message and in part of the IPv6 message.

MAC header	IPv6 header	ICMPv6 header	ICMPv6 message

<table>
<tr><td>00</td><td>01</td><td>02</td><td>03</td><td>04</td><td>05</td><td>06</td><td>07</td><td>08</td><td>09</td><td>10</td><td>11</td><td>12</td><td>13</td><td>14</td><td>15</td><td>16</td><td>17</td><td>18</td><td>19</td><td>20</td><td>21</td><td>22</td><td>23</td><td>24</td><td>25</td><td>26</td><td>27</td><td>28</td><td>29</td><td>30</td><td>31</td></tr>
<tr><td colspan="8">Type</td><td colspan="8">Code</td><td colspan="16">Checksum</td></tr>
<tr><td colspan="32">ICMPv6 message
...</td></tr>
</table>

Types of ICMPv6 Messages

- ICMPv6 messages are grouped into two classes:
- **Error messages**
  - To provide feedback to a source device about an error that has occurred.
  - Generated specifically in response to some sort of action, usually the transmission of a datagram
  - Identified as such by having a zero in the high-order bit of their message
  - Type field values 0 to 127.

Informational messages
  - Used to let devices exchange information, implement certain IP-related features, and perform testing.
  - Message Types from 128 to 255.
- Many of these ICMP types have a "code" field.

Error messages

Type	Description	References
1	Destination unreachable:	RFC 2463
2	Packet too big.	RFC 2463
3	Time exceeded.	RFC 2463
4	Parameter problem.	RFC 2463

Informational messages

Type	Description	References
128	Echo request.	RFC 2463
129	Echo reply.	RFC 2463

ICMPv6 Error Messages

Type Valu e	Message Name	Summary Description of Message Type
1	Destination Unreachable	Indicates that a datagram could not be delivered to its destination. *Code* value provides more information on the nature of the error.
2	Packet Too Big	Sent when a datagram cannot be forwarded because it is too big for the MTU of the next hop in the route. This message is needed in IPv6 and not IPv4 because in IPv4, routers can fragment oversized messages, while in IPv6 they cannot.
3	Time Exceeded	Sent when a datagram has been discarded prior to delivery due to the *Hop Limit* field being reduced to zero.
4	Parameter Problem	Indicates a miscellaneous problem (specified by the *Code* value) in delivering a datagram.

ICMP Information Messages

ICMPv6 Informational Messages	128	*Echo Request*	Sent by a device to test connectivity to another device on the internetwork.	2463
	129	*Echo Reply*	Sent in reply to an *Echo (Request)* message; used for testing connectivity.	2463
	133	*Router Solicitation*	Prompts a router to send a *Router Advertisement*.	2461
	134	*Router Advertisement*	Sent by routers to tell hosts on the local network the router exists and describe its capabilities.	2461
	135	*Neighbor Solicitation*	Sent by a device to request the layer two address of another device while providing its own as well.	2461
	136	*Neighbor Advertisement*	Provides information about a host to other devices on the network.	2461
	137	*Redirect*	Redirects transmissions from a host to either an immediate neighbor on the network or a router.	2461
	138	*Router Renumbering*	Conveys renumbering information for router renumbering.	2894

Debugging ICMPv6

```
RouterA#debug ipv6 icmp
ICMPv6: Received ICMPv6 packet from 2001:410:0:1:200:86FF:FE4B:F9CE, type 128
ICMPv6: Received echo request from 2001:410:0:1:200:86FF:FE4B:F9CE
ICMPv6: Sending echo reply to 2001:410:0:1:200:86FF:FE4B:F9CE
ICMPv6: Received ICMPv6 packet from 2001:410:0:1:200:86FF:FE4B:F9CE, type 128
<output omitted>
```

Path MTU Discovery (PMTUD) for IPv6

PMTUDv6 - Overview

- To enable hosts to discover the min. MTU on a path to a particular destination.
- Fragmentation in IPv6 is not performed by intermediary routers.
- The source node may fragment packets by itself only when the path MTU is smaller than the packets to deliver
- PMTUD for IPv6 uses ICMPv6 error message
  - **Type 2 Packet Too Big**
- For detail info - http://www.ietf.org/rfc/rfc1981.txt

Differences between IPv4 & IPv6 MTU

- **Increased Default MTU**
  - In IPv4, the minimum MTU that routers and physical links were required to handle = **576 bytes**.
  - In IPv6, all links must handle a datagram size of at least **1280 bytes**.
  - improves efficiency by increasing the ratio of maximum payload to header length, and reduces the frequency with which fragmentation is required.
- **Elimination of En Route Fragmentation**
  - In IPv4, datagrams may be fragmented by either the source device, or by routers during delivery.
  - In IPv6, only the source node can fragment; **routers do not**.
  - The source must therefore fragment to the size of the smallest MTU on the route before transmission.

Differences between IPv4 & IPv6 MTU

- **MTU Size Error Feedback**
  - Since routers cannot fragment datagrams, they must drop them if they are forced to try to send a too-large datagram over a physical link.
  - A feedback process has been defined using ICMPv6 that lets routers tell source devices that they are using datagrams that are too large for the route.
- **Movement of Fragmentation Header Fields**
  - To reflect the decreased importance of fragmentation in IPv4, the permanent fields related to the process that were in the IPv4 header have been farmed out to a *Fragment* extension header, included only when needed.

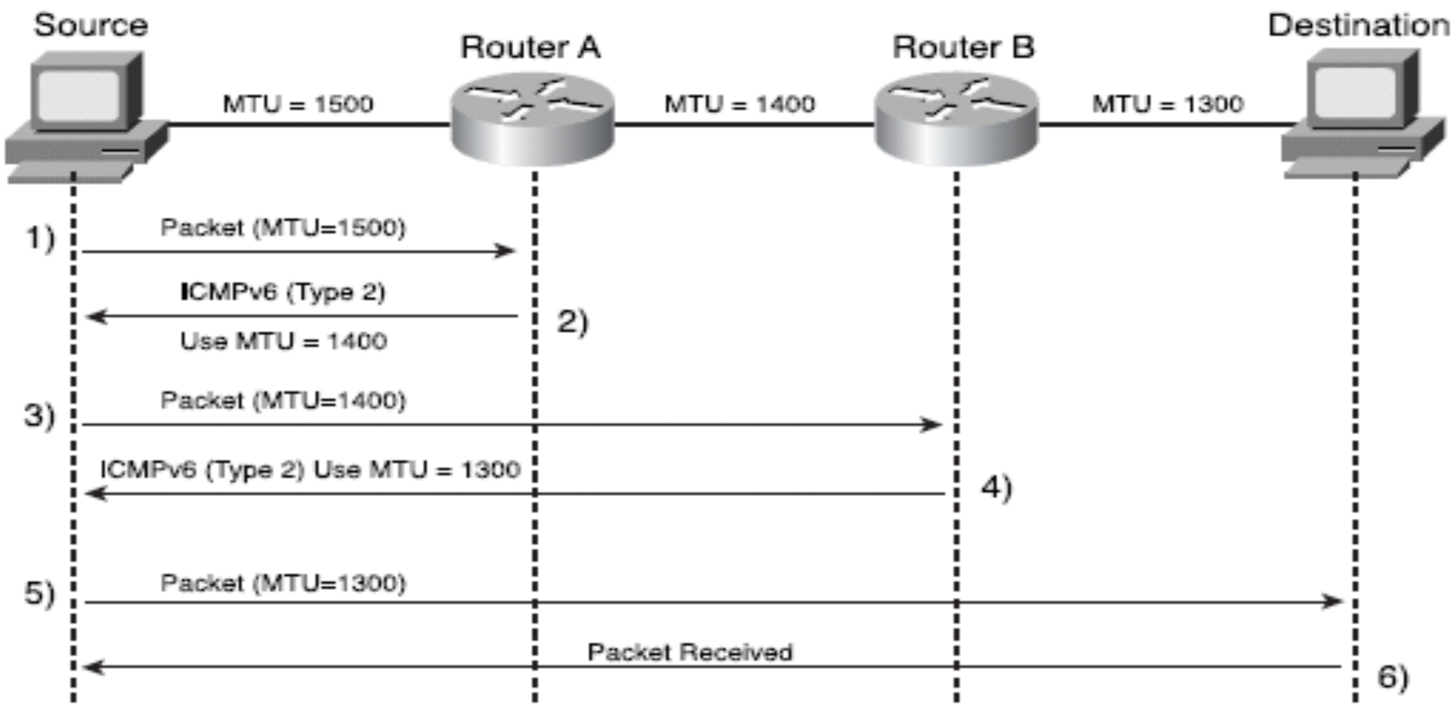
Determining the Appropriate Datagram Size

- How does the source know what size to use? It has two choices:
  1. **Use Default MTU**
     - Use the default MTU of **1280**, which all physical networks must be able to handle.
     - Good choice especially for short communications or for sending small amounts of data.
  2. **Use Path MTU Discovery feature**
     - A node sends messages over a route to determine what the overall minimum MTU for the path is, in a technique very similar to how it is done in IPv4.

Path MTU Discovery Process

1. The sending node assumes that the path MTU is the link MTU of the interface on which the traffic is being forwarded.
2. The sending node sends IPv6 packets at the **path MTU size**.
3. 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.
4. 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.
5. The sending node starts again at step 2 and repeats steps 2 through 4 for as many times as are necessary to discover the path MTU.

PMTUD uses ICMPv6 Type 2 Message

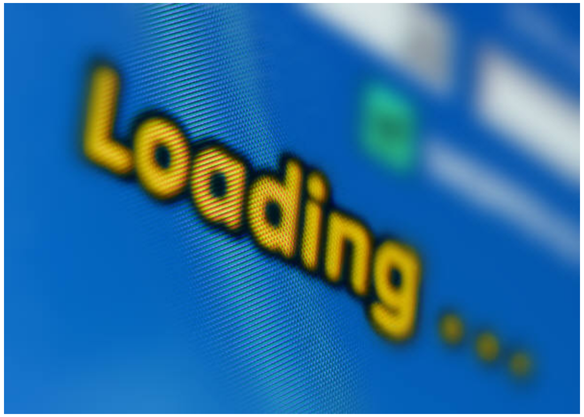


The MTU value found ICMPv6 PMTUD is cached by source node

To display:

Router#show ipv6 mtu

IPv6 Fragmentation



IPv6 Fragmentation

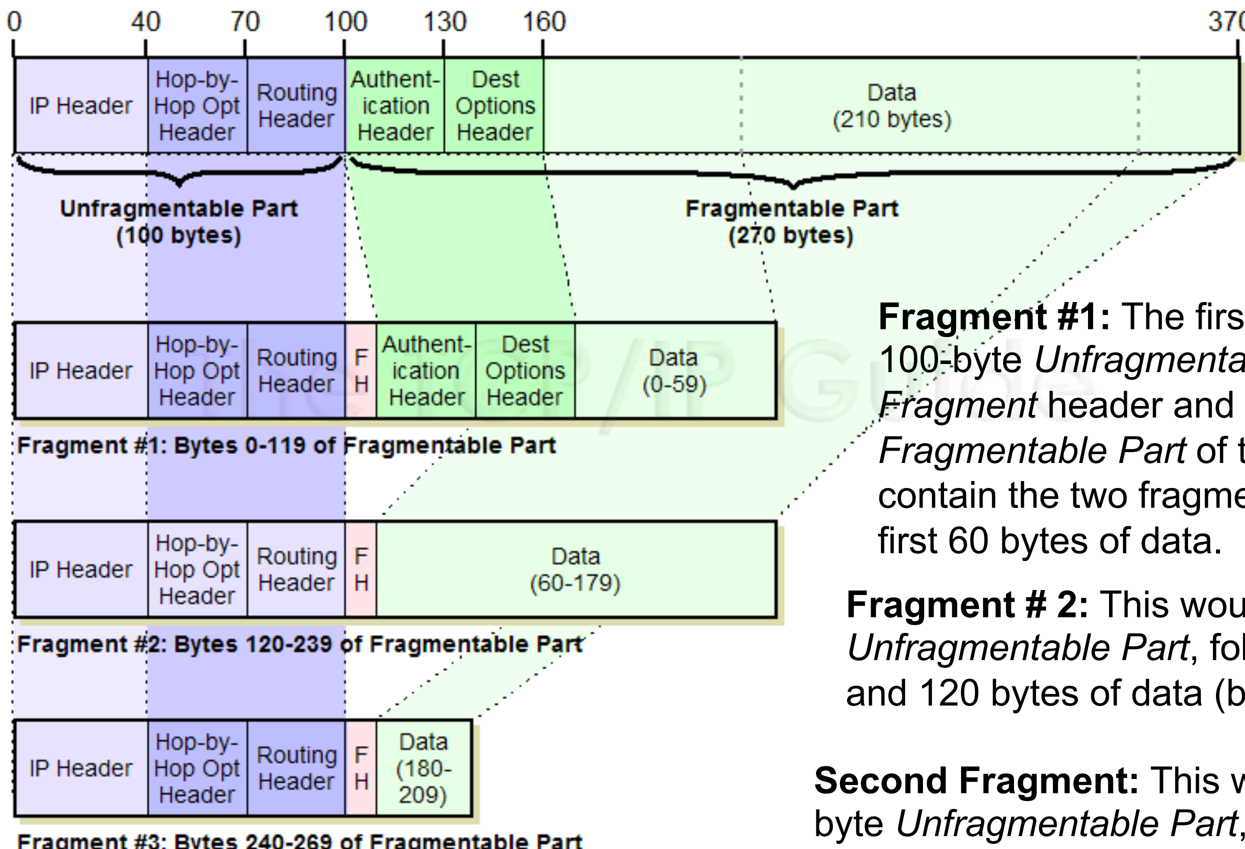
- For purposes of fragmentation, IPv6 datagrams are broken into two pieces:
- **Unfragmentable Part**
  - Includes the main header of the original datagram + any extension headers that need to be present in each fragment - ***Hop-By-Hop Options***, ***Destination Options*** (for those options to be processed by devices along a route) and ***Routing***.
- **Fragmentable Part**
  - Data portion of the datagram + other extension headers if present - *authentication Header*, *Encapsulating Security Payload* and/or *Destination Options* (for options to be processed only by the final destination).
- ***Unfragmentable Part*** must be present in each fragment, while the **fragmentable part** is split up amongst the fragments.

IPv6 Fragment Sets

- So to fragment a datagram, a device creates a set of fragment datagrams, each of which contains the following, in order:
- **Unfragmentable Part**
  - The full *Unfragmentable Part* of the original datagram, with its *Payload Length* changed to the length of the fragment datagram.
- **Fragment Header**
  - A *Fragment* header with the *Fragment Offset*, *Identification* and *M* flags set in the same way they are used in IPv4.
- **Fragment**
  - A fragment of the *Fragmentable Part* of the original datagram. Note that each fragment must have a length that is a multiple of 8 bytes, because the value in the *Fragment Offset* field is specified in multiples of 8 bytes.

IPv6 Fragmentation

Suppose we need to send this over a link with an MTU of only 230 bytes.
 We would actually require three fragments, not the two, because of the need to put the two 30-byte unfragmentable extension headers in each fragment, and the requirement that each fragment be a length that is a multiple of 8.

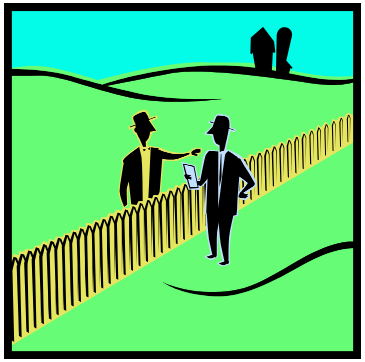


Fragment #1: The first fragment would consist of the 100-byte *Unfragmentable Part*, followed by an 8-byte *Fragment* header and the first 120 bytes of the *Fragmentable Part* of the original datagram. This would contain the two fragmentable extension headers and the first 60 bytes of data.

Fragment # 2: This would also contain the 100-byte *Unfragmentable Part*, followed by a *Fragment* header and 120 bytes of data (bytes 60 to 179).

Second Fragment: This would also contain the 100-byte *Unfragmentable Part*, followed by a *Fragment* header and 120 bytes of data (bytes 60 to 179).

IPv6 Neighbour Discovery Protocol (NDP)



IPv6 ND - Overview

- IPv6 ND is a set of messages and processes that determine relationships between neighboring nodes.
- ND replaces ARP, ICMP Router Discovery, and ICMP Redirect used in IPv4 and provides additional functionality.

IPv6 ND - Overview

- **ND is used by hosts to:**
  - Discover neighbouring 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 neighbouring node to which an IPv6 packet is being forwarded and determine when the link-layer address of a neighbouring node has changed.
  - Determine whether a neighbour is still reachable.

IPv6 ND – What is Neighbour?

- **Neighbour** is one that has been used for years in various networking standards and technologies to refer to devices that are local to each other.
- Two devices are **neighbours** if they are on the same local network, meaning that they can send information to each other directly.
- Most of the functions of the ND protocol are implemented using a set of **five special ICMPv6 control messages**.
- ND is a **messaging protocol.**
  - It doesn't implement a single specific function but rather a group of activities that are performed through the exchange of messages.
  - ND standard describes **nine specific functions** performed by the protocol.

ICMPv6 Control Messages Used By NDP

1. ***RS- Router Solicitation* Messages (ICMPv6 Type 133)**
   - Sent by hosts to request that any local routers send a *Router Advertisement* message so they don't have to wait for the next regular advertisement message.
2. ***RA - Router Advertisement* Messages (ICMPv6 Type 134)**
   - Sent regularly by routers to tell hosts that they exist and provide important prefix and parameter information to them.
3. ***NS - Neighbor Solicitation* Messages (ICMPv6 Type 135)**
   - Sent to verify the existence of another host and to ask it to transmit a *Neighbor Advertisement*.
4. ***NA - Neighbor Advertisement* Messages (ICMPv6 Type 136)**
   - Sent by hosts to indicate the existence of the host and provide information about it.
5. ***Redirect* Messages (ICMPv6 Type 137)**
   - Sent by a router to tell a host of a better method to route data to a particular destination.

ICMPv6 Messages Used by NDP

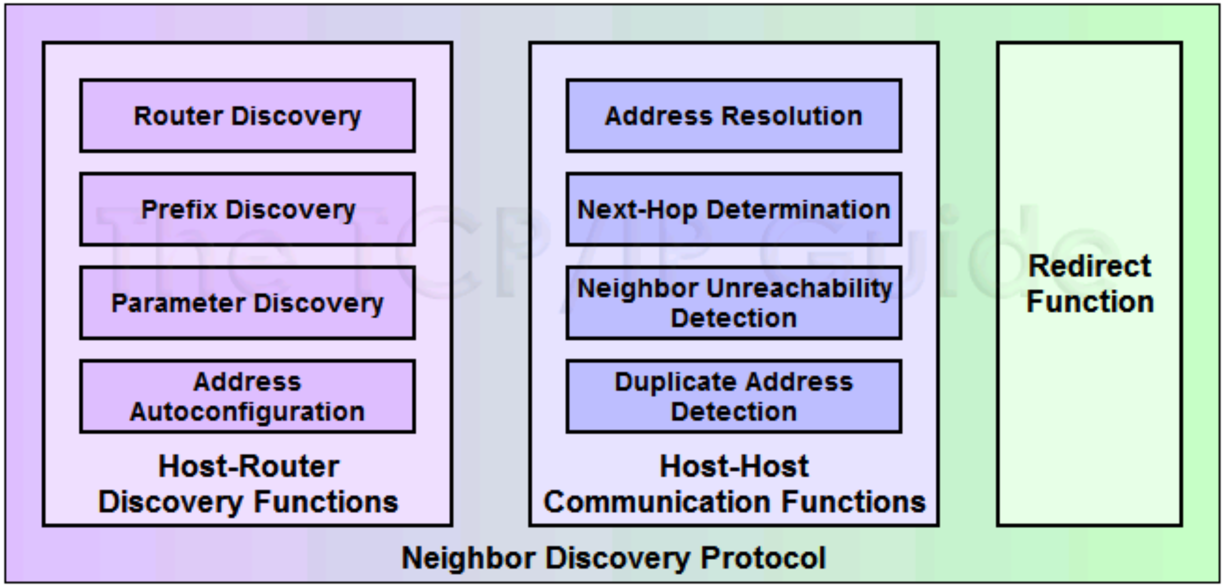
Mechanism	Type 133 (RS)	Type 134 (RA)	Type 135 (NS)	Type 136 (NA)	Type 137 (Redirect)
Replacement of ARP			X	X	
Prefix advertisement	X	X			
Prefix renumbering	X	X			
DAD			X		
Router redirection					X

IPv6 ND Functions Compared to Equivalent IPv4 Functions

- Specific improvements made in ND
  - Formalizing Of Router Discovery
  - Formalizing Of Address Resolution
  - Ability To Perform Functions Securely
  - Autoconfiguration
  - Dynamic Router Selection
  - Multicast-Based Address Resolution
  - Better Redirection

NDP Functional Groups and Functions

- Mainly three functions
  1. Host-Router Functions
  2. Host-Host Communication Functions
  3. Redirect Function



1. Host-Router Discovery Functions

- One of the two main groups of functions in ND are those that facilitate the discovery of local routers and the exchange of information between them and hosts.
- **Router Discovery**
  - Core function of this group: the method by which hosts locate routers on their local network.
- **Prefix Discovery**
  - Closely related to the process of router discovery is prefix discovery.
  - To determine what network they are on, which in turn tells them how to differentiate between local and distant destinations and whether to attempt direct or indirect delivery of datagrams.
- **Parameter Discovery**
  - A host learns important parameters about the local network and/or routers, such as the MTU of the local link.
- **Address Autoconfiguration**
  - Hosts in IPv6 are designed to be able to **automatically configure themselves**, but this requires information that is normally provided by a router.

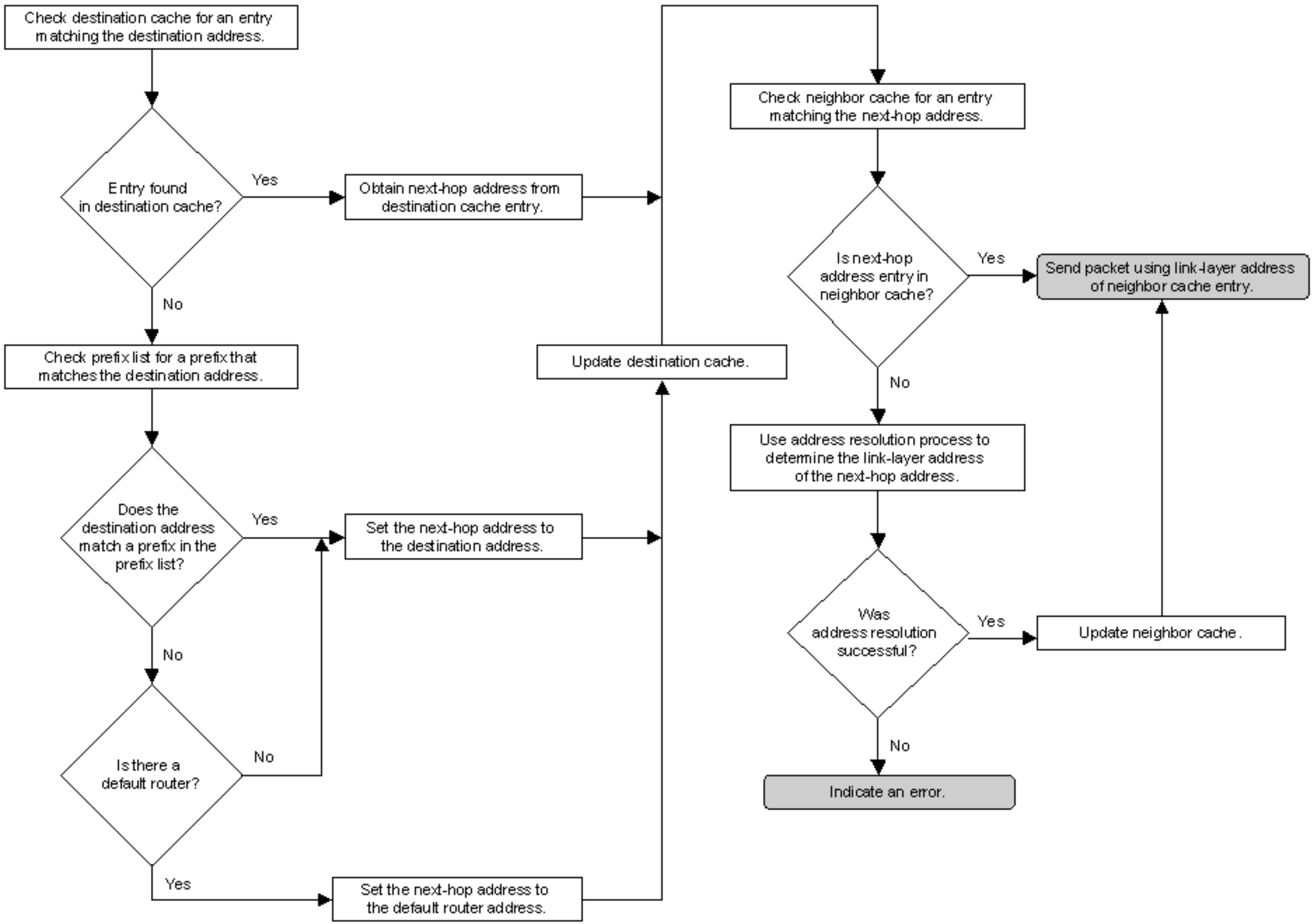
2. Host-Host Communication Functions

- **Address Resolution**
  - The process by which a device determines the layer two address of another device on the local network from that device's layer three (IP) address.
  - Performed by ARP in IP version 4.
- **Next-Hop Determination**
  - Looking at an IP datagram's destination address and determining where it should next be sent.
- **Neighbor Unreachability Detection**
  - Determining whether or not a neighbor device can be directly contacted.
- **Duplicate Address Detection (DAD)**
  - Determining if an address that a device wishes to use already exists on the network.

3. Redirect Function

- The last functional group contains just one function: *Redirect*.
- The technique whereby a router informs a host of a better next-hop node to use for a particular destination.

The Host Sending Algorithm



How Neighbour Solicitation and Neighbour Advertisement Works

- A node can use following special addresses:
  - All-node multicast address (FF02::1, destination)
  - All-routers multicast address (FF02::2, destination)
  - Solicited-mode multicast address (destination)
  - Link-local address (sources or destination)
  - Unspecified address (::, source)

Address Resolution

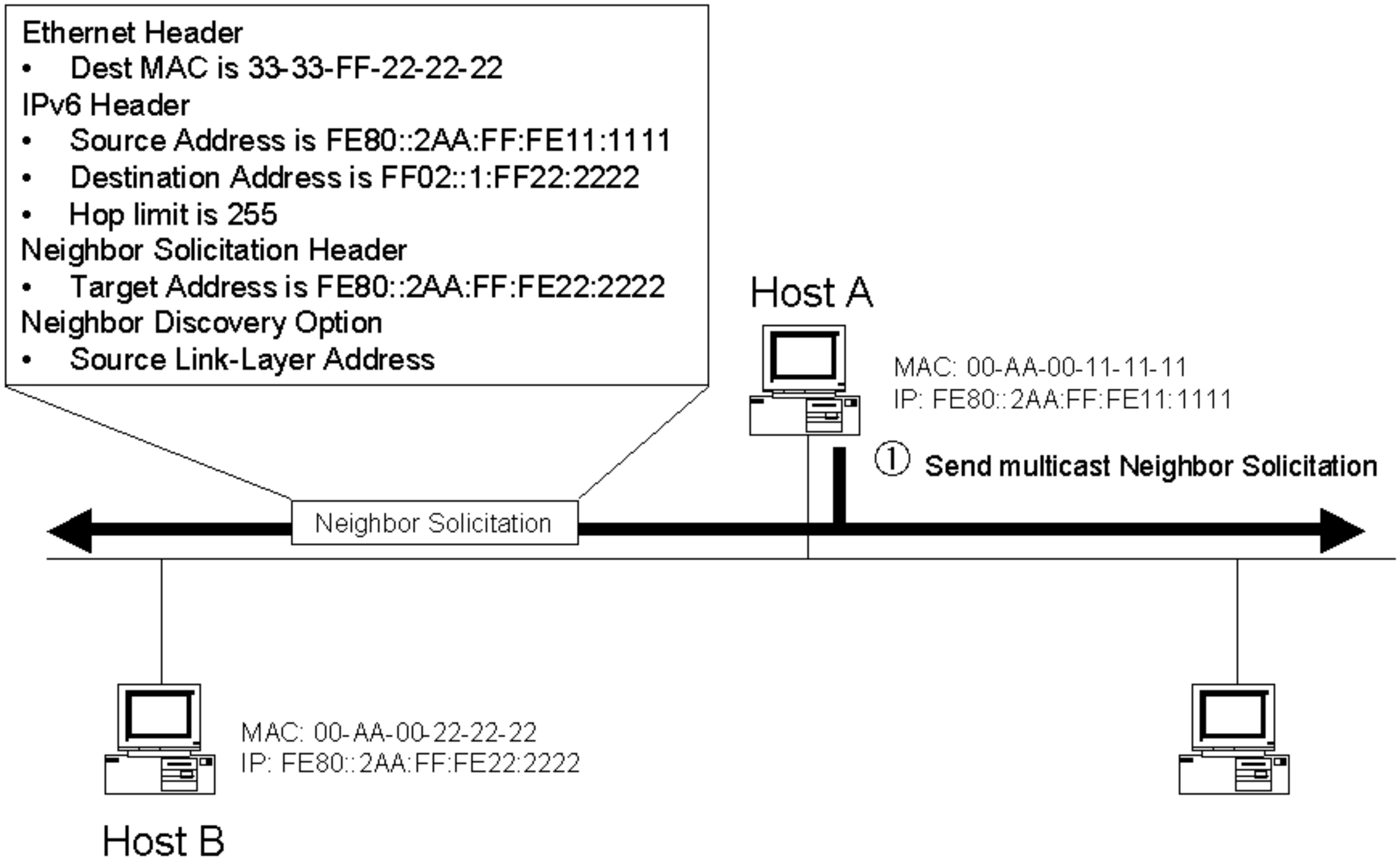
- The address resolution process for IPv6 nodes consists of an exchange of Neighbor Solicitation and Neighbor Advertisement messages to resolve the link-layer address of the on-link next-hop address for a given destination.
- The sending host sends a **multicast Neighbor Solicitation message** on the appropriate interface.
- The multicast address of the Neighbor Solicitation message is the solicited-node multicast address derived from the target IP address.
- The Neighbor Solicitation message includes the link-layer address of the sending host in the Source Link-Layer Address option.
- When the target host receives the Neighbor Solicitation message, it updates its own neighbor cache based on the source address of the Neighbor Solicitation message and the link-layer address in the Source Link-Layer Address option.

Address Resolution

- Next, the target node sends a **unicast Neighbor Advertisement** to the Neighbor Solicitation sender.
- The Neighbor Advertisement includes the Target Link-Layer Address option.
- After receiving the Neighbor Advertisement from the target, the sending host updates its neighbor cache with an entry for the target based upon the information in the Target Link-Layer Address option.
- At this point, unicast IPv6 traffic between the sending host and the target of the Neighbor Solicitation can be sent.

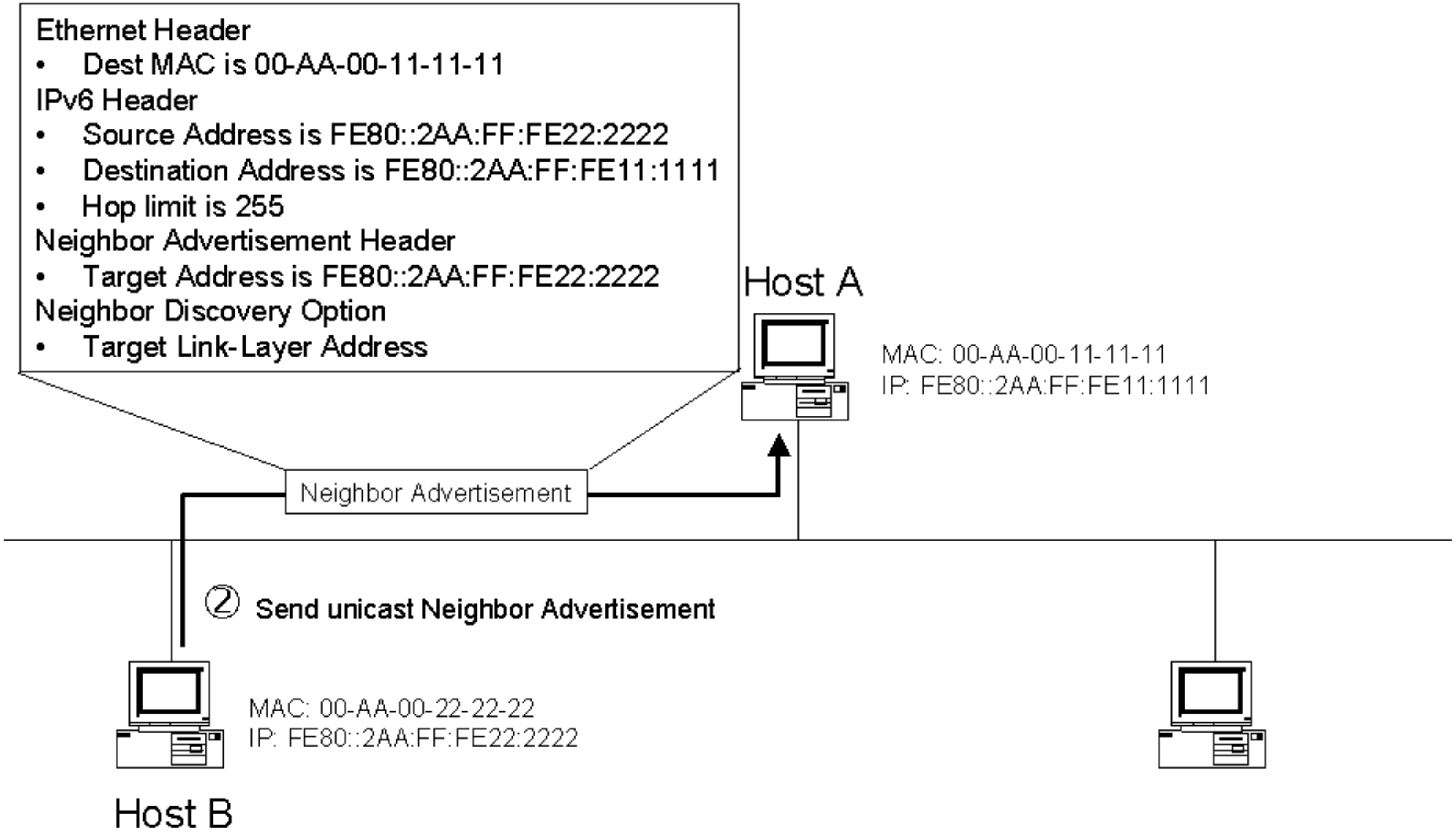
Address Resolution: Example

The multicast Neighbor Solicitation for address resolution



Address Resolution: Example contd.

The unicast Neighbor Advertisement for address resolution



Displaying Neighbour Discovery Table

```
RouterA#show ipv6 neighbors
IPv6 Address                  Age Link-layer Addr State Interface
FEC0::1:200:86FF:FE4B:F9CE      0 0000.864b.f9ce  REACH FastEthernet0/0
<waiting of 10 minutes>
RouterA#show ipv6 neighbors
IPv6 Address                  Age Link-layer Addr State Interface
FEC0::1:200:86FF:FE4B:F9CE      2 0000.864b.f9ce  STALE FastEthernet0/0
FE80::200:86FF:FE4B:F9CE       10 0000.864b.f9ce  STALE FastEthernet0/0
```

Adding a static entry in neighbour discovery table (Cisco feature)

```
RouterA(config)#ipv6 unicast-routing
RouterA(config)#ipv6 neighbor fec0::1:0:0:1:b fastEthernet 0/0 0080.12ff.6633
RouterA(config)#exit
RouterA#show ipv6 neighbors
IPv6 Address                     Age Link-layer Addr State Interface
FEC0::1:200:86FF:FE4B:F9CE       15 0000.864b.f9ce  STALE FastEthernet0/0
FEC0::1:0:0:1:B                   - 0080.12ff.6633  REACH FastEthernet0/0
FE80::200:86FF:FE4B:F9CE         15 0000.864b.f9ce  STALE FastEthernet0/0
```

Prefix advertisement

- It uses
  - Router Advertisement (RA) message &
  - All node mulicast address (FF02::1)
  - RA sent periodically on the local link to all node-multicast address
- Advertising an IPv6 prefix on a Cisco router:
  - As soon site-local or aggregatable global unicast address with a prefix length is configured on a network interface
  - Use command: ipv6 address
  - If multiple ip addresses with multiple prefixes to the same interface – all these advertised to hosts on the local link.

Router Advertisement Message Parameters

- IPv6 prefix
  - Multiple ipv6 prefixes can be advertised per local link
  - By default – prefix length = 64 bits
  - Nodes gets IPv6 address, they append their link-layer in EUI-format to the prefix received = 128 bit IPv6 node address.
- Life-time
  - Lifetime mat vary from 0 to infinite.
  - Two types of lifetime value per prefix:
    - Valid Lifetime: how long the node's address remains in valid state
    - Preferred Lifetime: how long the address configured by a node remains preferred. It must be <= valid lifetime

Router Advertisement Message Parameters

- Default router information
  - Information about the existence and lifetime of the default router’s ipv6 address
  - Deafult router’s address = router’s link local address
- Flags/options
  - Use flags to instruct nodes to use stateful configuration than stateless

Router Discovery

- Router discovery is the process through which nodes attempt to discover the set of routers on the local link.
- Router discovery in IPv6 is similar to ICMP Router Discovery for IPv4 described in RFC 1256.
- An important difference between ICMPv4 Router Discovery and IPv6 Router Discovery is the mechanism through which a new default router is selected when the current one becomes unavailable.
- **In ICMPv4 Router Discovery**, the Router Advertisement message includes an **Advertisement Lifetime field.**
  - It is the time after which the router, upon receiving its last Router Advertisement message, can be considered unavailable.
  - In the worst case, a router can become unavailable and hosts will not attempt to discover a new default router until the Router Advertisement time has elapsed.

IPv6 Router Discovery

- IPv6 has a Router Lifetime field in the Router Advertisement message.
- It indicates the length of time that the router can be considered a default router.
- If the current default router becomes unavailable, the condition is detected through **neighbor unreachability detection** instead of the Router Lifetime field in the Router Advertisement message.
- Because neighbor unreachability detection determines that the router is no longer reachable, a new router is chosen immediately from the default router list.

Router Discovery - parameters

- In addition to configuring a default router, IPv6 router discovery also configures the following:
  - The default setting for the **Hop Limit field** in the IPv6 header.
  - A determination of whether the node should use a **stateful address protocol, such as DHCPv6**, for addresses and other configuration parameters.
  - The **timers** used in reachability detection and the retransmission of Neighbor Solicitations.
  - The **list of network prefixes** defined for the link. Each network prefix contains both the IPv6 network prefix and its valid and preferred lifetimes.
    - If indicated, a network prefix combined with the interface identifier creates a stateless IP address configuration for the receiving interface. A network prefix also defines the range of addresses for nodes on the local link.
  - The **MTU** of the local link.

IPv6 Router Discovery Processes

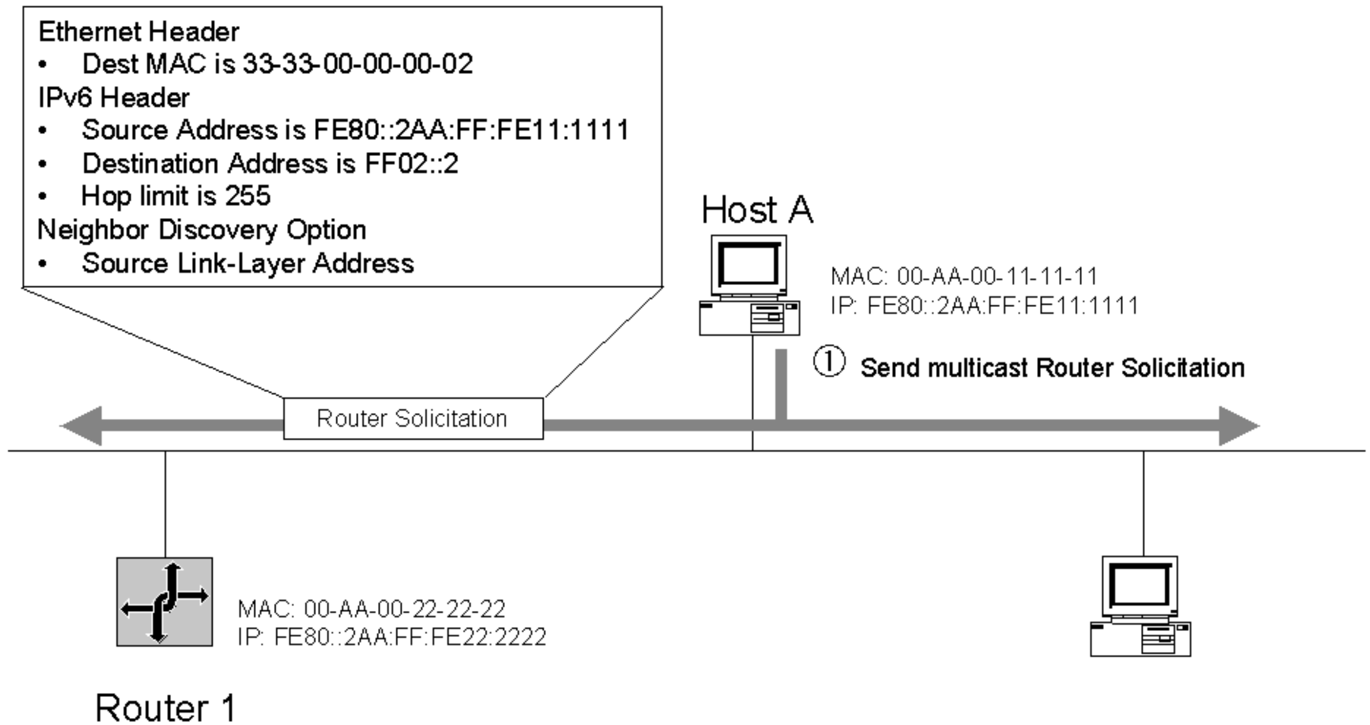
- IPv6 routers periodically send a **Router Advertisement message** on the local link advertising their existence as routers.
  - They also provide configuration parameters such as default hop limit, MTU, and prefixes.
- Active IPv6 hosts on the local link receive the Router Advertisement messages and 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.

IPv6 Router Discovery Processes

- Any node can send RS to all-routers multicast address FF02::2 on the local link
- When RS is received, a router responds with RA using all-node multicast FF02::1
- To avoid flooding of RS on the link, each node can send only three RS at boot time.

IPv6 Router Discovery Processes -

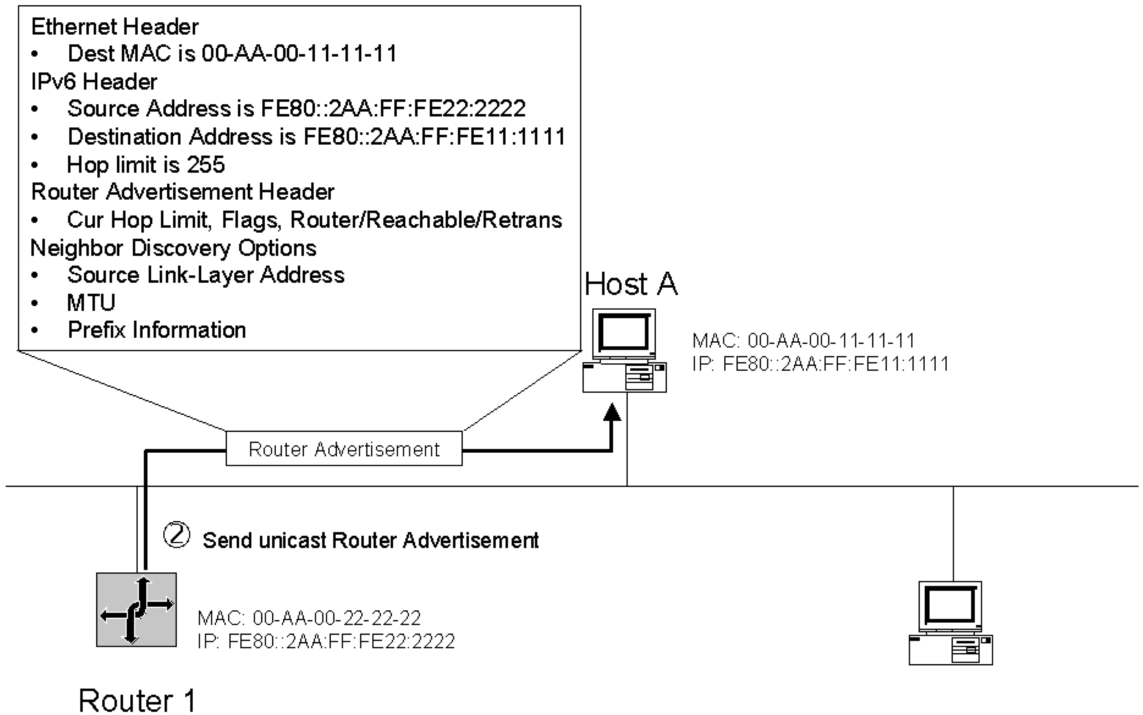
The multicast Router Solicitation for router and prefix discovery



- To forward packets to off-link destinations, Host A must discover the presence of Router 1.
- Host A sends a multicast Router Solicitation to the address FF02::2

IPv6 Router Discovery Processes –

The unicast Router Advertisement for router and prefix discovery



- Router 1, having registered the multicast address of 33-33-00-00-00-02 with its Ethernet adapter, receives and processes the Router Solicitation.
- Router 1 responds with a unicast Router Advertisement message containing configuration parameters and local link prefixes

Duplicate Address Detection (DAD)

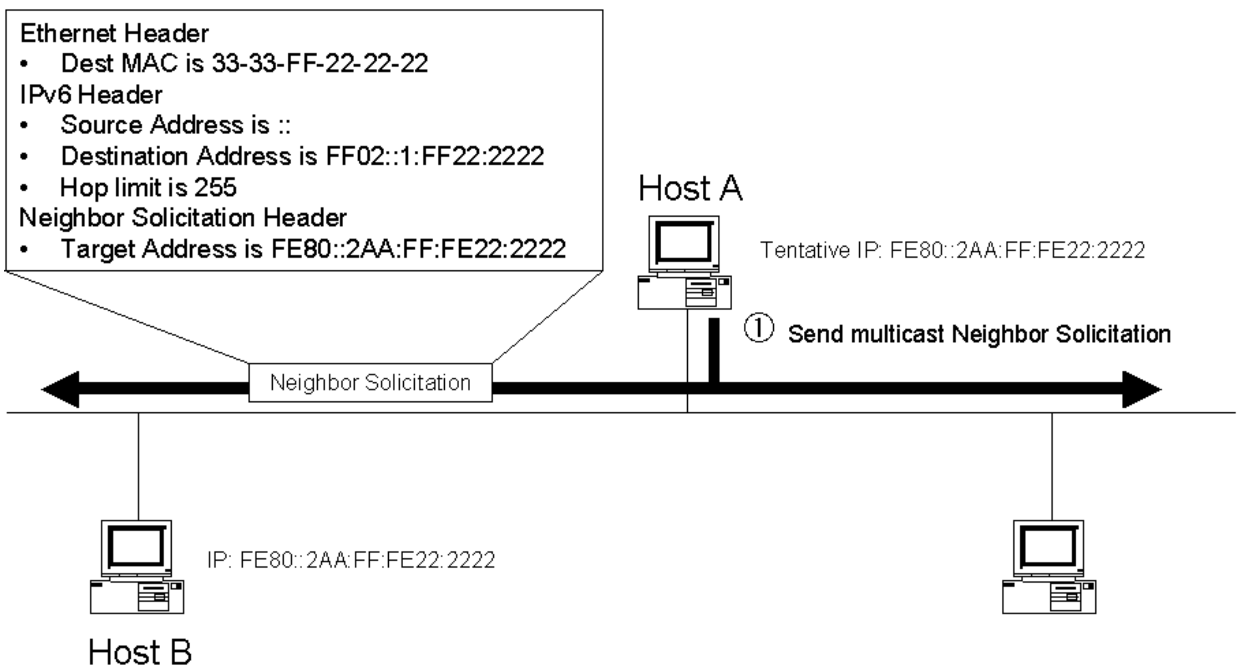
- IPv4 nodes use ARP Request messages and a method called gratuitous ARP to detect a duplicate IP address on the local link.
- Similarly, IPv6 nodes use the **Neighbor Solicitation message** to detect duplicate address use on the local link.
- Before a node can configure its IPv6 address using stateless autoconfiguration, it must verify on the local link that the tentative address it wants to use is unique and not already in use by another mode.
- Node sending a Neighbour Solicitation (NS) on the local link using **unspecified address (::)** as its source address and **solicited-node multicast** of the tentative unicast address as the destination address.
- If a duplicate address – no assignment of this unicast address

DAD – Example

The multicast Neighbor Solicitation for duplicate address detection

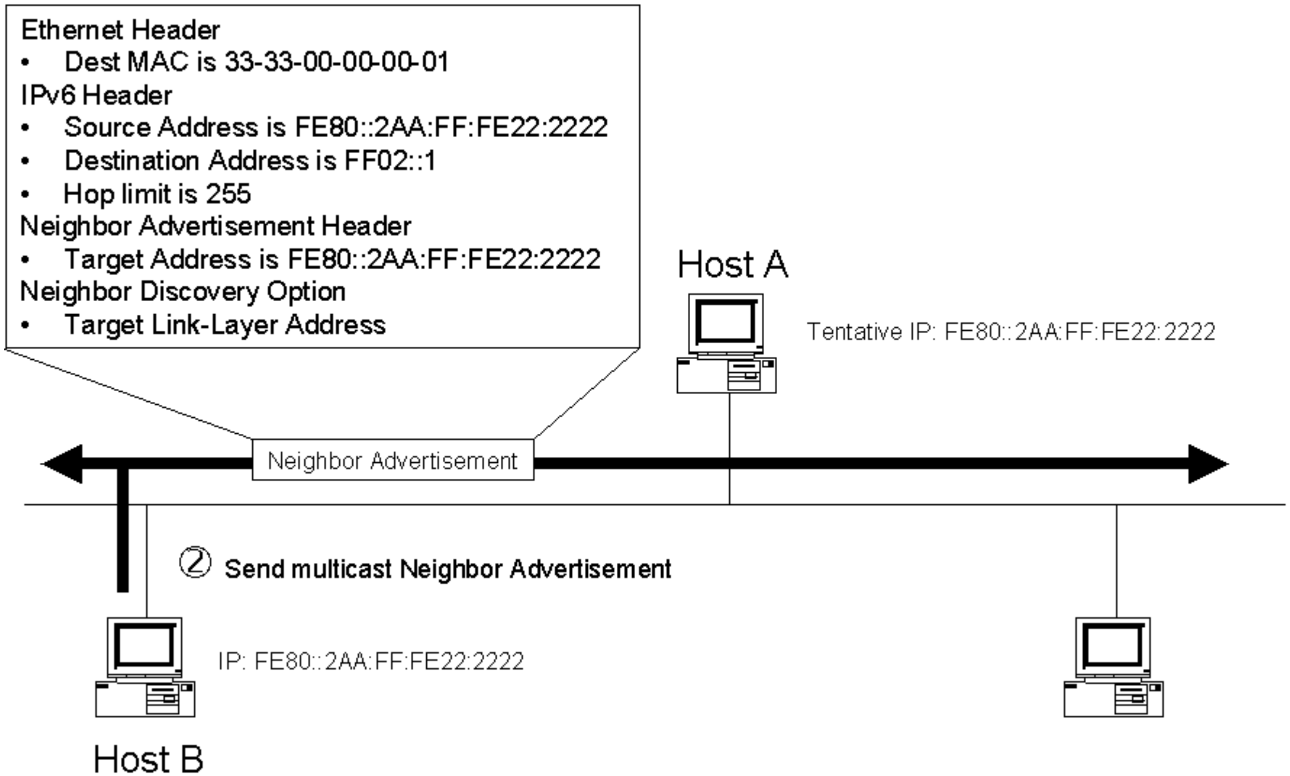
- Host B has a link-local address of FE80::2AA:FF:FE22:2222.
- Host A is attempting to use the link-local address of FE80::2AA:FF:FE22:2222.
- Before Host A can use this link-local address, it must verify its uniqueness through duplicate address detection.

Host A sends a solicited-node multicast Neighbor Solicitation to the address FF02::1:FF22:2222



DAD – Example

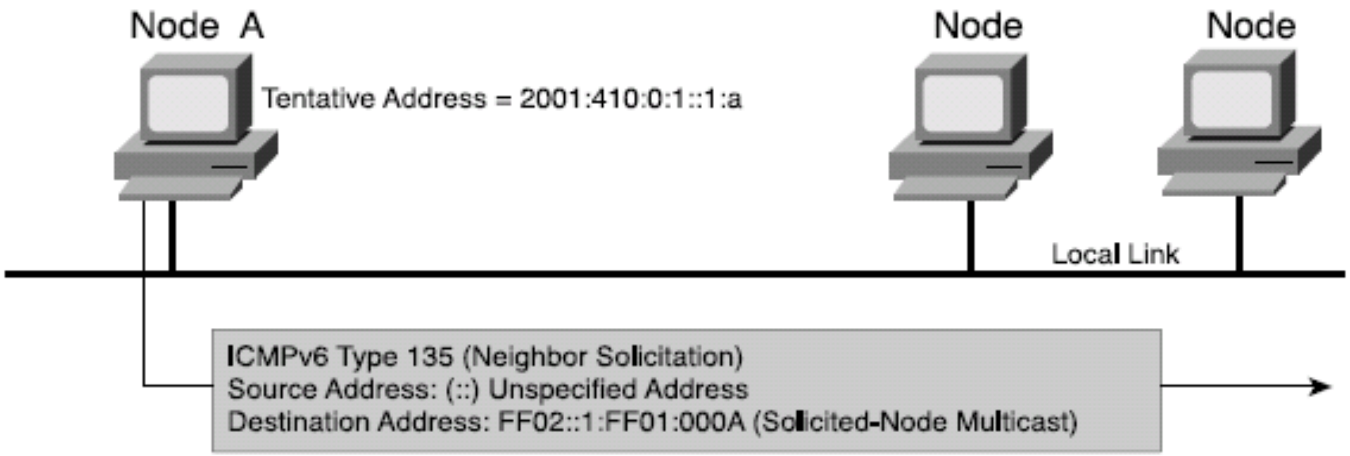
The multicast Neighbor Advertisement for duplicate address detection



- Host B, having registered the solicited-node multicast address of 33-33-FF-22-22-22 with its Ethernet adapter, receives and processes the Neighbor Solicitation.
- Host B notes that the source address is the unspecified address.
- Host B then responds with a multicast Neighbor Advertisement message

Duplicate Address Detection

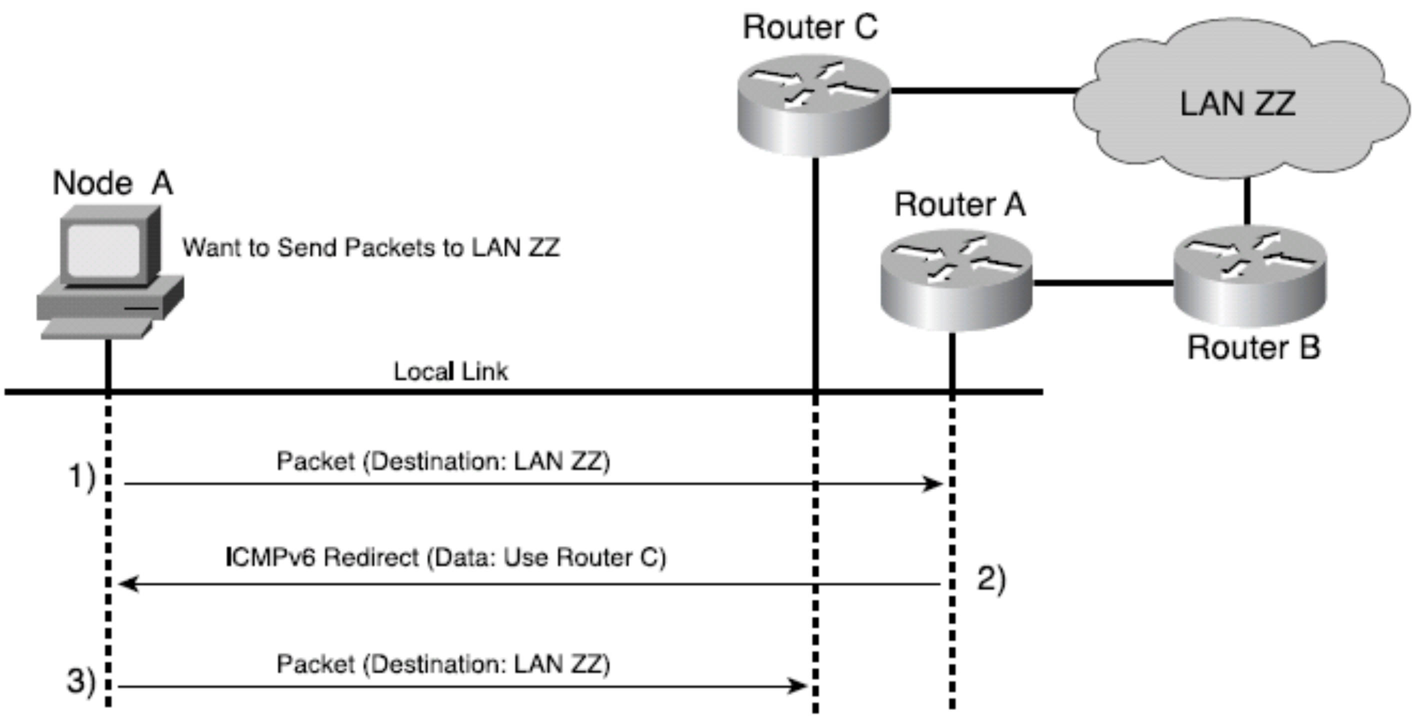
- By default, DAD is enabled on Cisco routers



Command	Description
Router(config-if)# **ipv6 nd dad attempts** *number*	Defines the number of router solicitation messages for DAD to send on the link before considering an IPv6 address unique.
Example RouterA(config-if)# **ipv6 nd dad attempts 3**	DAD sends three neighbor solicitation messages on the link before considering the IPv6 address unique.
Example RouterA(config-if)# **ipv6 nd dad attempts 0**	The value 0 disables DAD on an interface.

Router Redirect

- 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.
- Nodes receiving it may modify its routing table according to the new router address.



Router Redirect

- There are two instances where redirect is used:

1. **A router informs an originating host of the IP address of a router available on the local link that is "closer" to the destination.**
   - "Closer" is routing metric function used to reach the destination network segment.
   - This condition can occur when there are multiple routers on a network segment and the originating host chooses a default router and it is not the best one to use to reach the destination.
2. **A router informs an originating host that the destination is a neighbor (it is on the same link as the originating host).**
   - This condition can occur when the prefix list of a host does not include the prefix of the destination.
   - Because the destination does not match a prefix in the list, the originating host forwards the packet to its default router.

Router Redirect Process

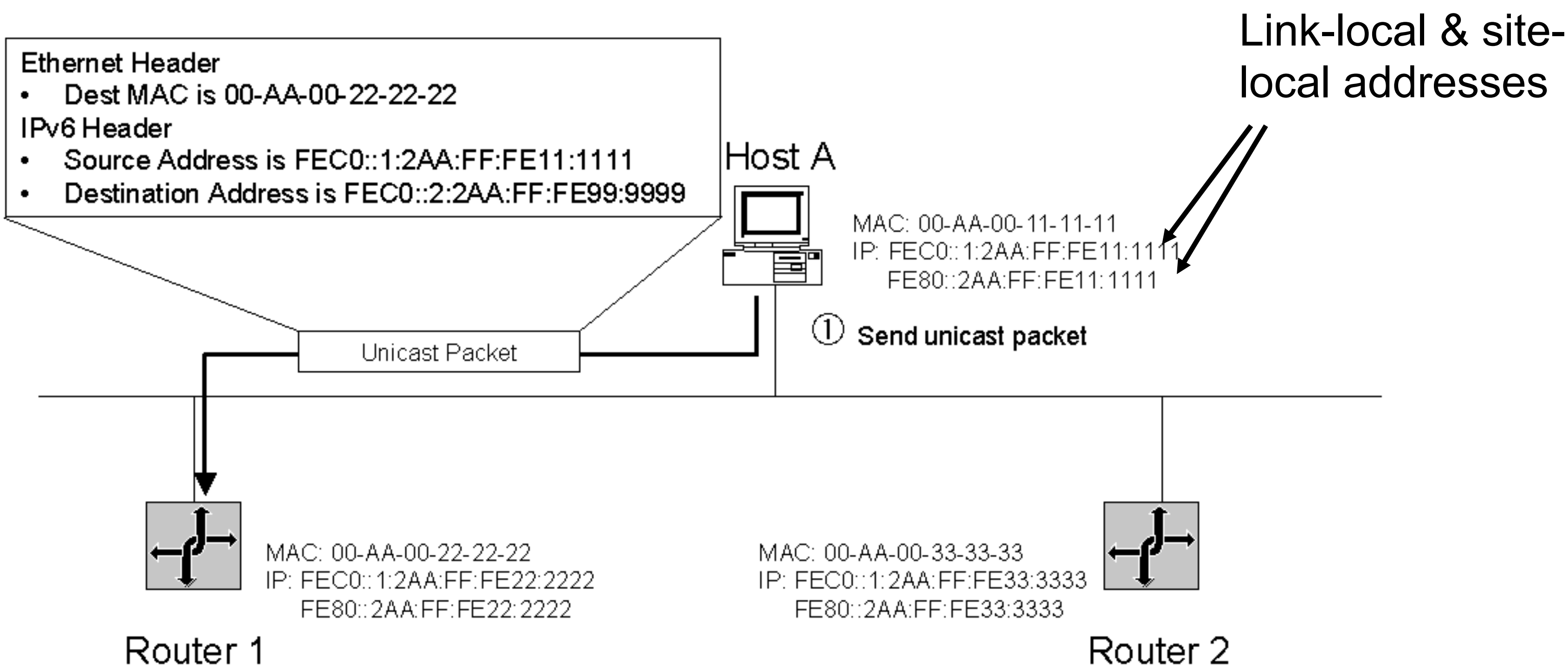
1. The originating host forwards a unicast packet to its default router.
2. The router processes the packet and notes that the address of the originating host is a neighbor.
   - Additionally, it notes that the addresses of both the originating host and the next-hop are on the same link.
3. The router forwards the packet to the appropriate next-hop address.
4. 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.

Router Redirect Process

- **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.

Router Redirect Process - Example

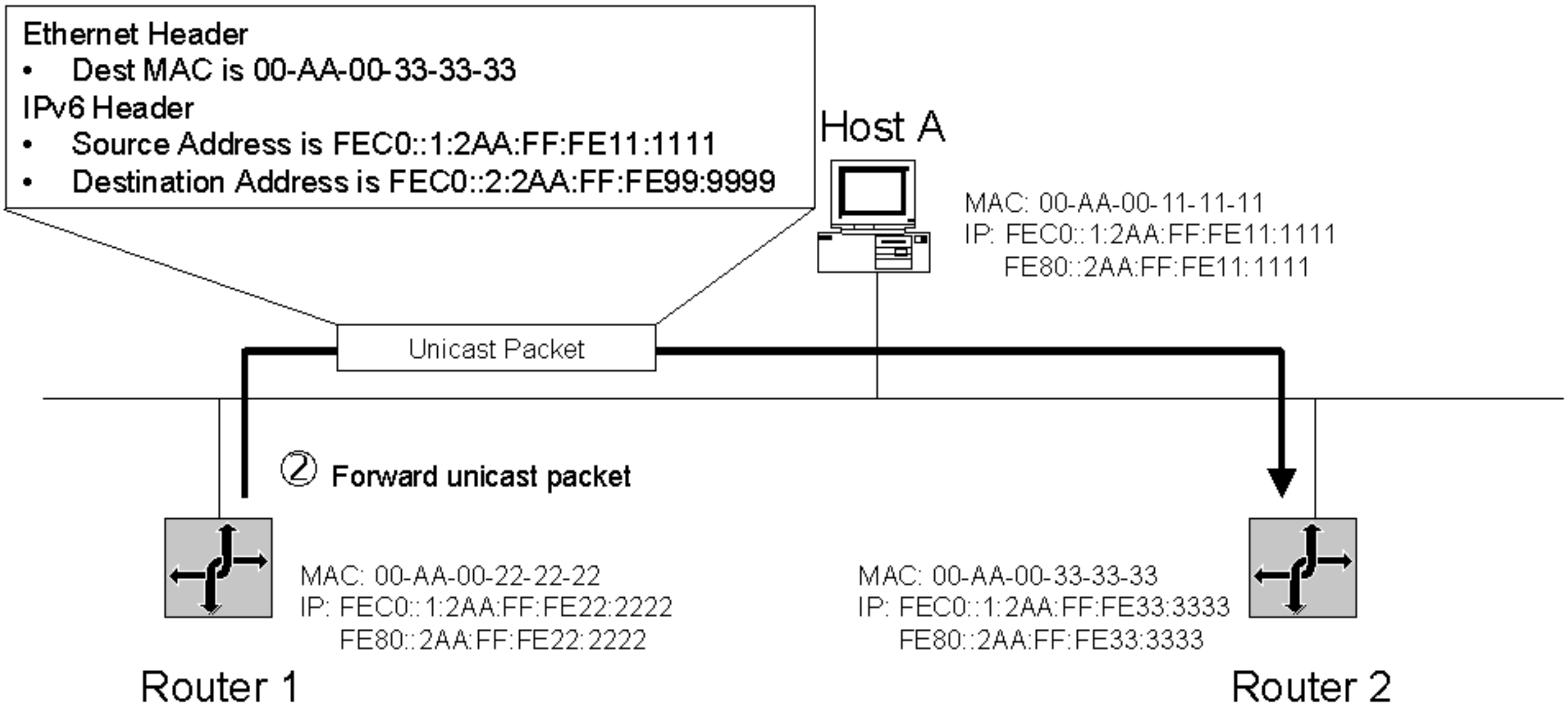
The unicast packet forwarded by the originating node



Host A is sending a packet to an off-link host at FEC0::2:2AA:FF:FE99:9999 (not shown) and is using Router 1 as its current default router.
However, Router 2 is the better router to use to reach this destination.
Host A sends the packet destined to FEC0::2:2AA:FF:FE99:9999 to Router 1

Router Redirect Process - Example

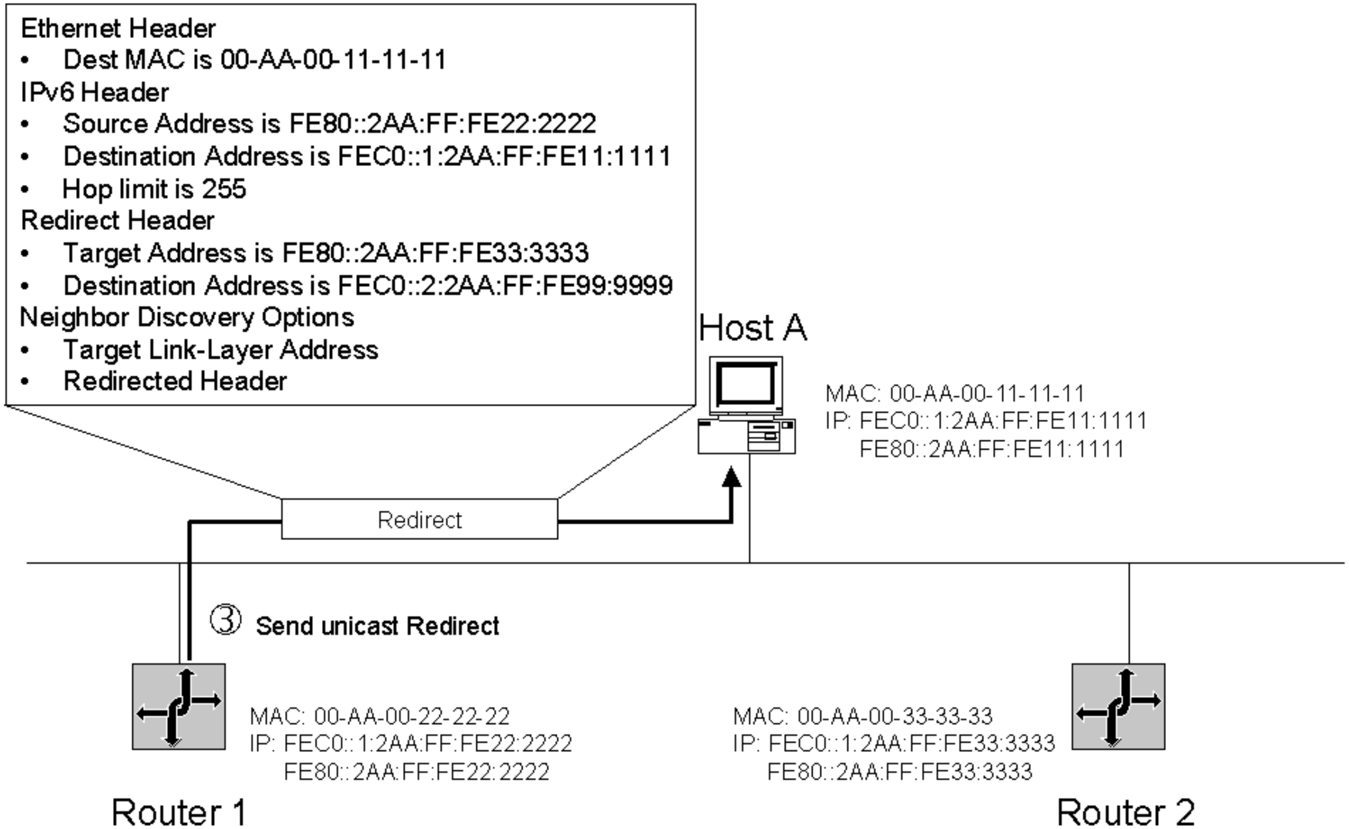
The unicast packet forwarded by the router



- Router 1 receives the packet from Host A and notes that Host A is a neighbor.
- It also notes that Host A and the next-hop address for the destination are on the same link. Based on the contents of its local routing table, Router 1 forwards the unicast packet received from Host A to Router 2

Router Redirect Process - Example

The Redirect message sent by the router



- To inform Host A that subsequent packets to the destination of FEC0::2:2AA:EE:FE99:9999 should be sent to Router 2, Router 1 sends a Redirect message to Host A