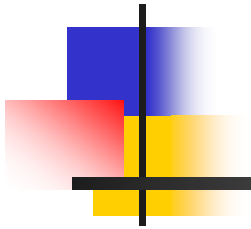
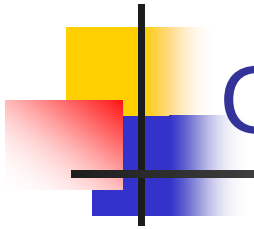


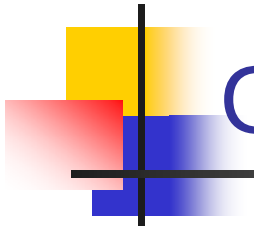
IPv6 Addressing

Dr. Whai-En Chen
Assistant Professor
Institute of Computer Science and Information Engineering
National Ilan University
wechen@niu.edu.tw
TEL: +886-3-9357400#340
http://alan.ipv6.club.tw



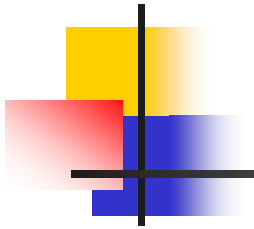
Outline

- IPv6 Addressing
  - Unicast, Multicast and Anycast
  - IPv6 Prefix and Interface ID
- IPv6 Header Format
  - IPv6 Base Header
  - IPv6 Extension Headers
- ICMPv6 Message Format
  - Error Messages
  - Informational Messages
- Neighbor Discovery Process
  - MAC Address Resolution
  - Duplicate Address Detection
  - Address Auto-configuration
  - MTU Discovery
  - Redirect



Outline

- **IPv6 Addressing**
- IPv6 Header Format
- ICMPv6 Message Format
- Neighbor Discovery Process

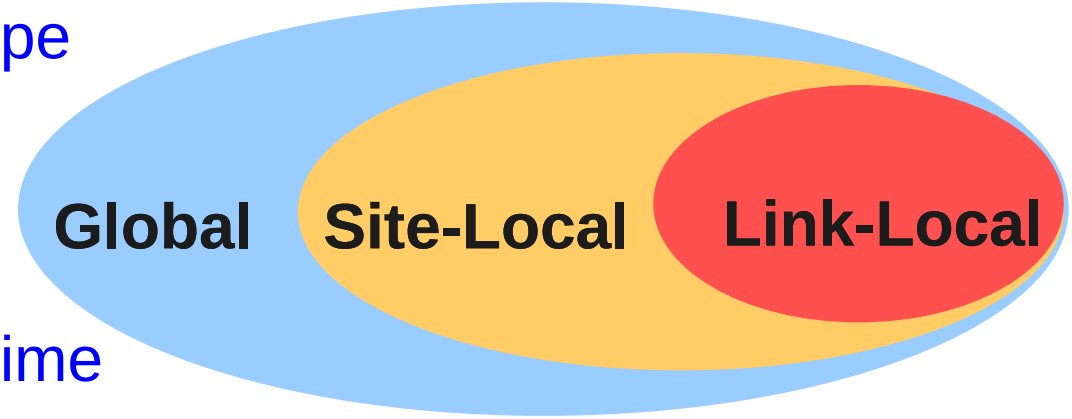


IPv6 Address Notation

- An IPv6-layer identifier for an interface or set of interfaces
- Preferred form
  - 3FFE:3600:0:FF:8:800:200C:417A
- Compressed form
  - FF01:0:0:0:0:0:0:7 becomes FF01::7
- IPv4-embedded
  - 0:0:0:0:0:0:140.113.131.3 or ::140.113.131.3
- Address prefix
  - 3FFE:3600:B:88::/64 (note: no masks in IPv6!)
  - 128-bit IPv6 Address/prefix length

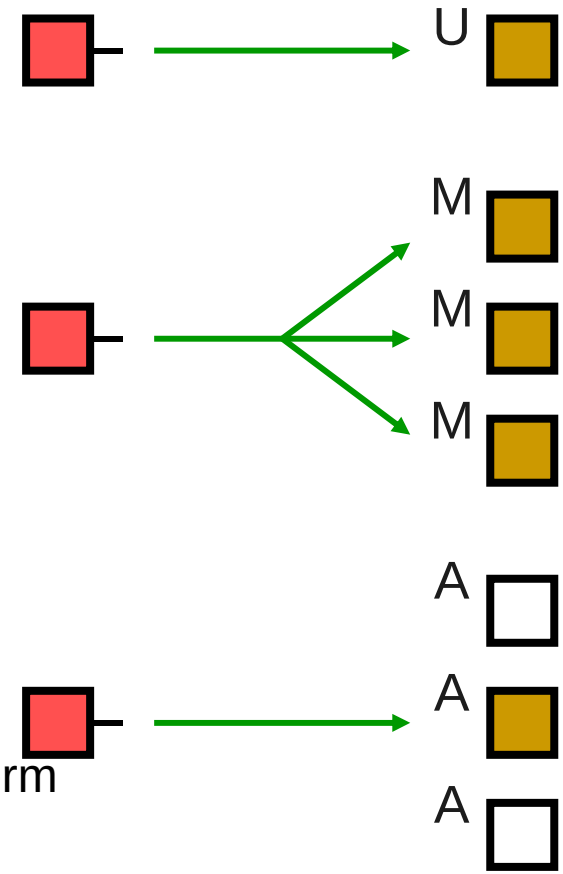
IPv6 - Addressing Model

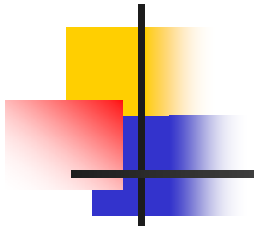
- Addresses are assigned to interfaces
  - No change from IPv4 Model
- Interface ‘expected’ to have multiple addresses
- Addresses have scope
  - Link Local
  - Site Local
  - Global
- Addresses have lifetime
  - Valid and Preferred lifetime



Basic Address Types

- Unicast
  - Address of a single interface
  - Delivery to single interface
  - for one-to-one communication
- Multicast
  - Address of a set of interfaces
  - Delivery to all interfaces in the set
  - for one-to-many communication
- Anycast
  - Address of a set of interfaces
  - Delivery to a single interface in the set
  - for one-to-nearest communication
  - Nearest is defined as being closest in term of routing distance
- No Broadcast



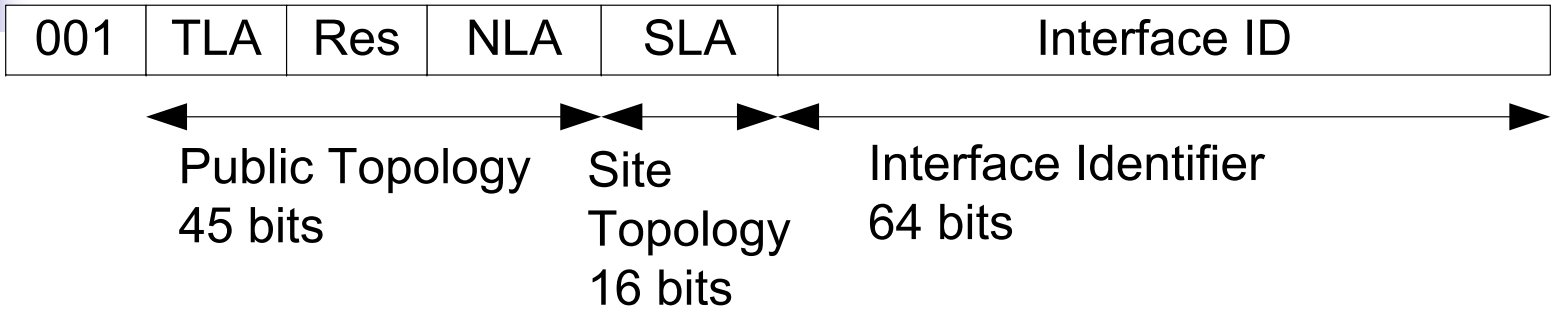


IPv6 Prefix Types

Address type	Binary prefix
IPv4-compatible	0000...0 /96 (96 zero bits)
global unicast	001/3
link-local unicast	1111 1110 10/10
site-local unicast	1111 1110 11/10
multicast	1111 1111/8

- All other prefixes reserved (approx. 7/8ths of total)
- Anycast addresses allocated from unicast prefixes

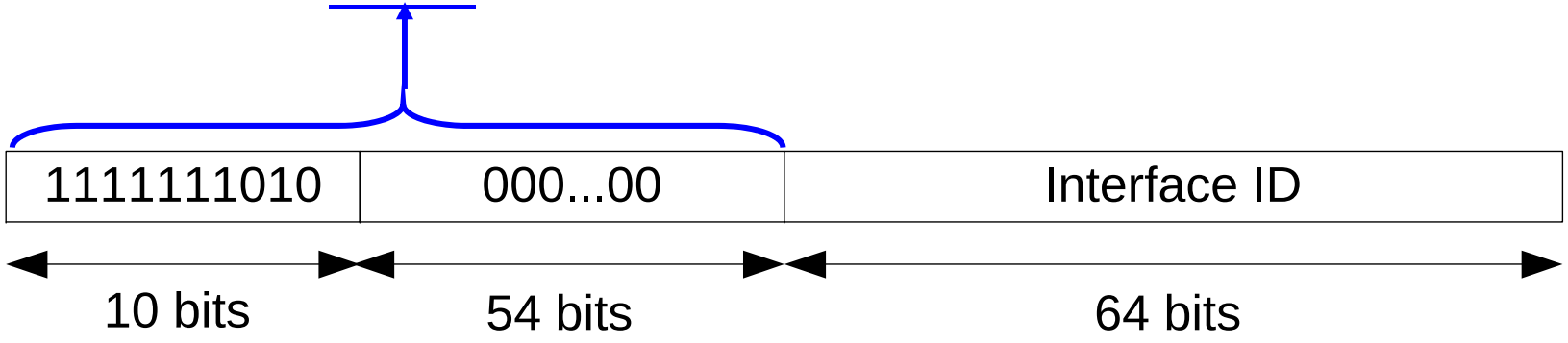
IPv6 Global Unicast Addresses



- TLA (Top Level Aggregator) = 13 bits
  - TLA routers(default-free router) do not have a default route, only route with 16 bits prefix
  - may be assigned to providers or exchanges
- Res= 8 bits
  - Reserved for future use in expanding the size of either the TLA or NLA
- NLA (Next Level Aggregator)= 24 bits
- SLA (Site level Aggregator)= 16 bits
- Public topology- Collection of larger and smaller ISP
- Site topology- Collection of subnets within an organization's site

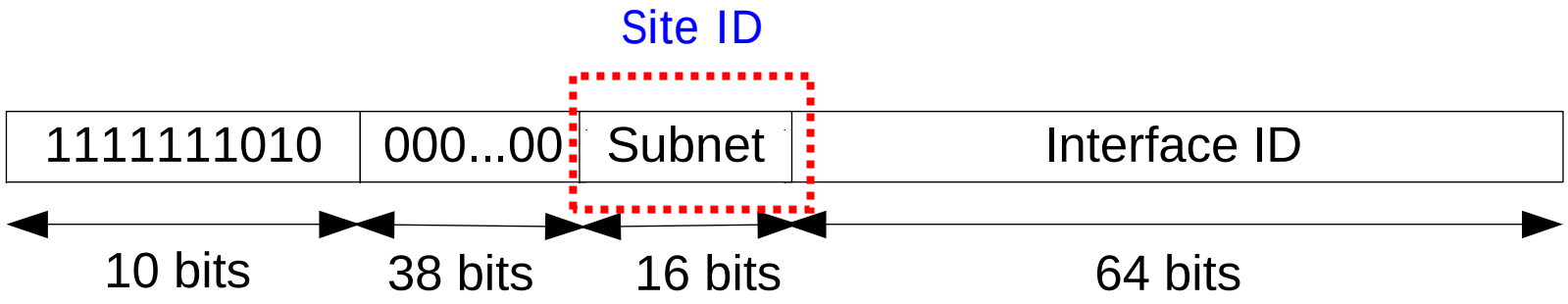
Link-Local Unicast Addresses

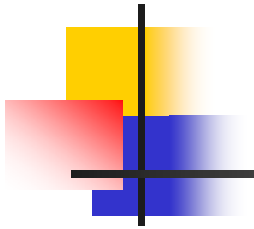
- meaningful only in a single link zone, and may be reused on other links
- Link-local addresses for use during auto-configuration and when no routers are present
- Required for Neighbor Discovery process, always automatically configuration (Interface ID+DAD)
- An IPv6 router never forwards link-local traffic beyond the link
- Prefix= FE80::/64



Site-Local Unicast Addresses

- meaningful only in a single site zone, and may be re-used in other sites
- Equivalent to the IPv4 private address space
- Address are not automatically configured and must be assigned (manually or by router)
- Prefix= FEC0::/48



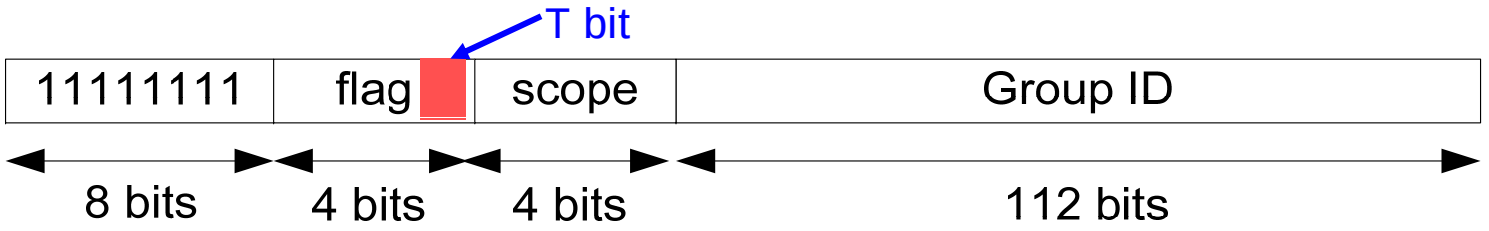


Special IPv6 address

- Unspecified address(0:0:0:0:0:0:0:0 or ::)
  - Indicate the absence of an address
  - Equivalent to IPv4 0.0.0.0
  - Never assigned to an interface or used as a destination address
- Loopback address (0:0:0:0:0:0:0:1 or ::1)
  - Identify a loopback interface
- IPv4-compatible address (0:0:0:0:0:0:w.c.x.z or ::w.c.x.z)
  - Used by dual-stack nodes
  - IPv6 traffic is automatically encapsulated with an IPv4 header and send to the destination using the IPv4 infrastructure
- IPv4 mapped address (0:0:0:0:0:FFFF:w.c.x.z or ::FFFF:w.c.x.z)
  - Represent an IPv4-only node to an IPv6 node
  - Never used as a source or destination address of IPv6 packet
- NSAP(Network Service Access Point) address(FP=0000001)
- IPX(Internetwork Packet Exchange) address (FP=0000010)

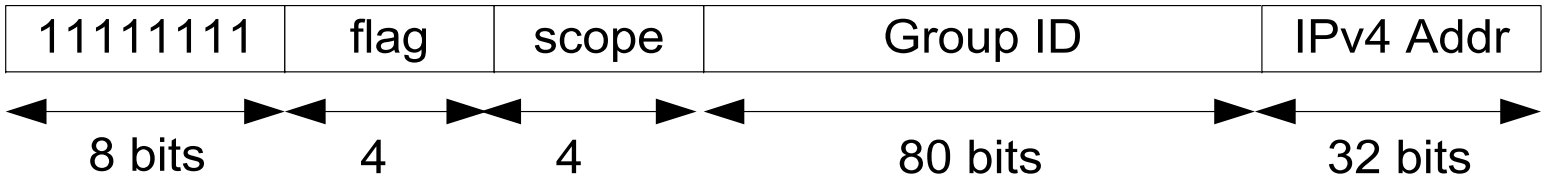
IPv6 Multicast addresses

- Multicast address can not be used as source or as intermediate destination in a Routing header
- low-order Transient(T) flag indicates permanent (T=0) / transient (T=1) group; three other flags reserved
- Scope field
  - 1: node-local
  - 2: link-local
  - 5: site-local
  - 8: organization-local
  - E: global
  - Others: reserved



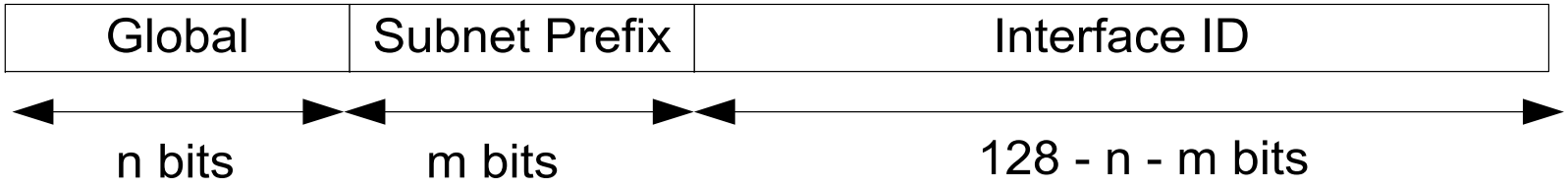
IPv6 Multicast addresses(cont.)

- Special multicast IPv6 address
  - FF01::1
    - Node-local scope all-nodes multicast address
  - FF02::1
    - Link-local scope all-nodes multicast address
  - 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
- Use low-order 32 bits, each group ID maps to a unique Ethernet MAC address (RFC 2373)



Other IPv6 addresses

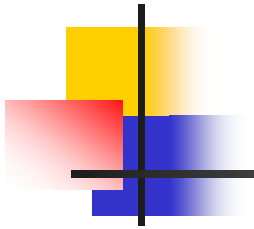
- Solicited-node address
  - Facilitates the efficient query of network node during address resolution (ICMPv6 Neighbor Discovery)
  - Prefix= FF02::1:FF00:0000/104 and the last 24-bits of IPv6 address
- Anycast IPv6 address
  - Assigned to multiple interfaces
  - Only used as destination address
  - Only assigned to router
  - Anycast addresses are indistinguishable from unicast
  - Subnet-router anycast address is predefined and requires



IPv6 Addresses for a Host

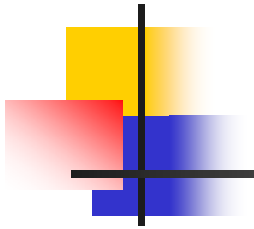
- Unicast addresses
  - A link-local address for each interface (FE80::[Interface ID])
  - Unicast address for each interface
    - Site-local, or
    - One or multiple aggregatable global unicast
  - A loopback address (::1)
- Multicast addresses
  - Node-local all-nodes multicast address (FF01::1)
  - Link-local all-nodes multicast address (FF02::1)
  - Solicited-node address for each unicast address
  - Multicast address of joined group

可以使用DOS視窗示範操作



IPv6 Addresses for a Router

- Unicast addresses
  - A link-local address for each interface
  - Unicast address for each interface
    - Site-local, or
    - One or multiple aggregatable global unicast
  - Subnet-Router anycast address
  - Additional anycast address (optional)
  - A loopback address(::1)
- Multicast addresses
  - Node-local all-nodes multicast address (FF01::1)
  - Node-local all-routers multicast address (FF01::2)
  - Link-local all-nodes multicast address (FF02::1)
  - Link-local all-routers multicast address (FF02::2)
  - Site-local all-routers multicast address (FF05:2)
  - Solicited-node address for each unicast address
  - Multicast address of joined group

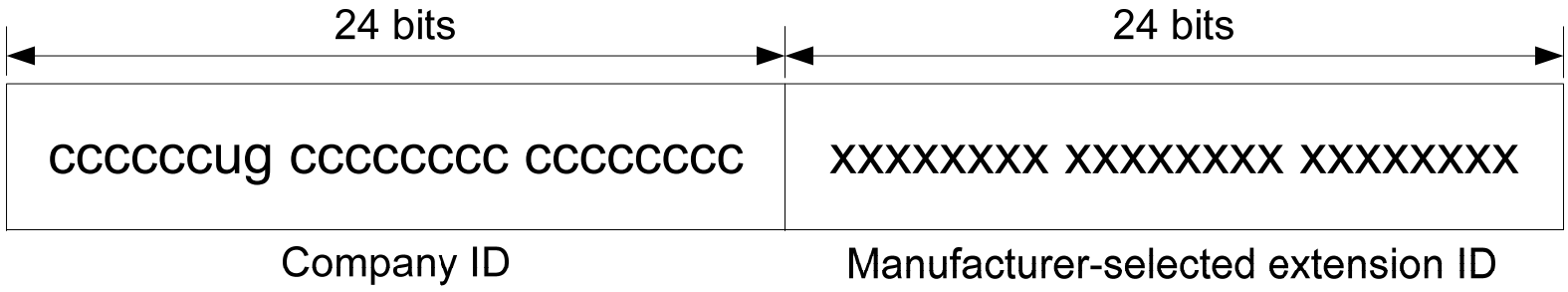


IPv6 Interface Identifier

- Lowest-order 64-bit field of unicast address
- Globally unique or locally unique within a subnet
- Future higher-layer protocols may take advantage of globally-unique interface IDs to identify nodes independently of their current location
- Configure interface identifier
  - Manual configuration
  - DHCPv6 (configures whole address)
  - automatic derivation from MAC address or other hardware serial number
  - pseudo-random generation (for client privacy)
  - the latter two choices enable "serverless" or "stateless" auto-configuration, when combined with high-order part of the address learned via Router Advertisements

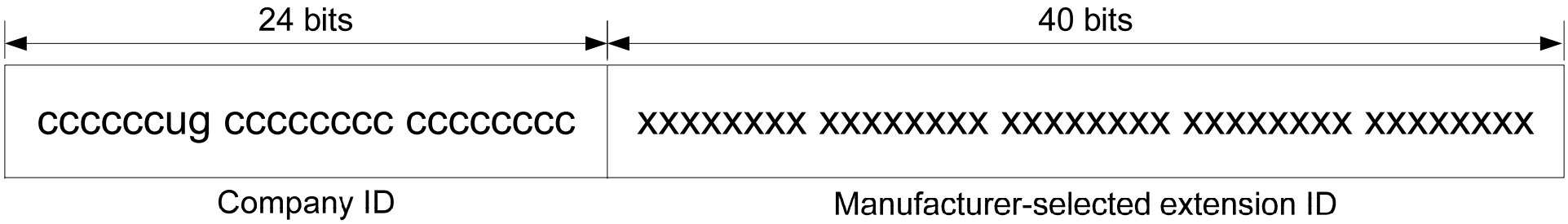
IEEE 802 Addresses

- U/L bit (u)
  - Universally (0) or Locally (1) Administration
- U/G bit (g)
  - Unicast (0) or Group (1) Address

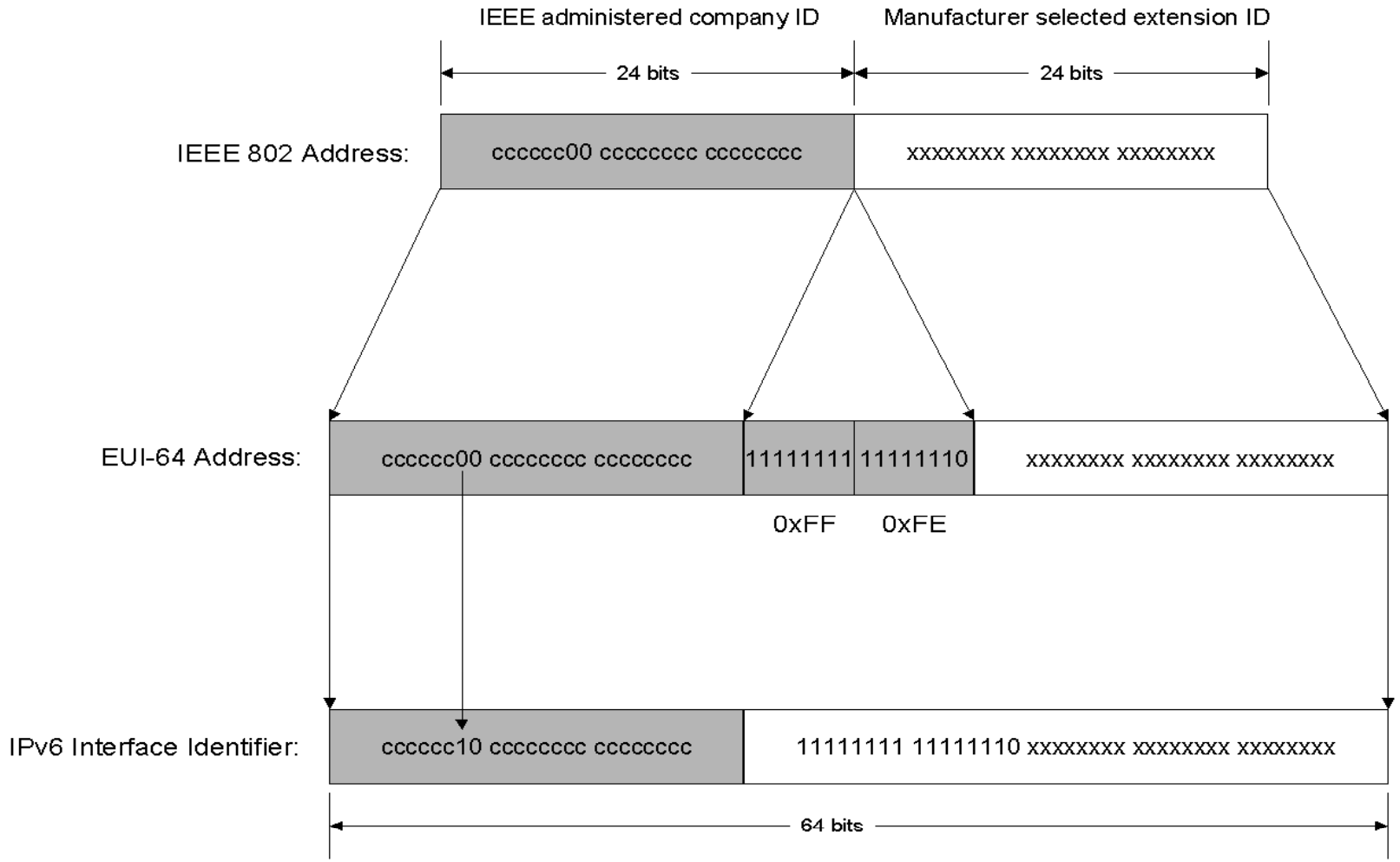


IEEE EUI-64 Addresses

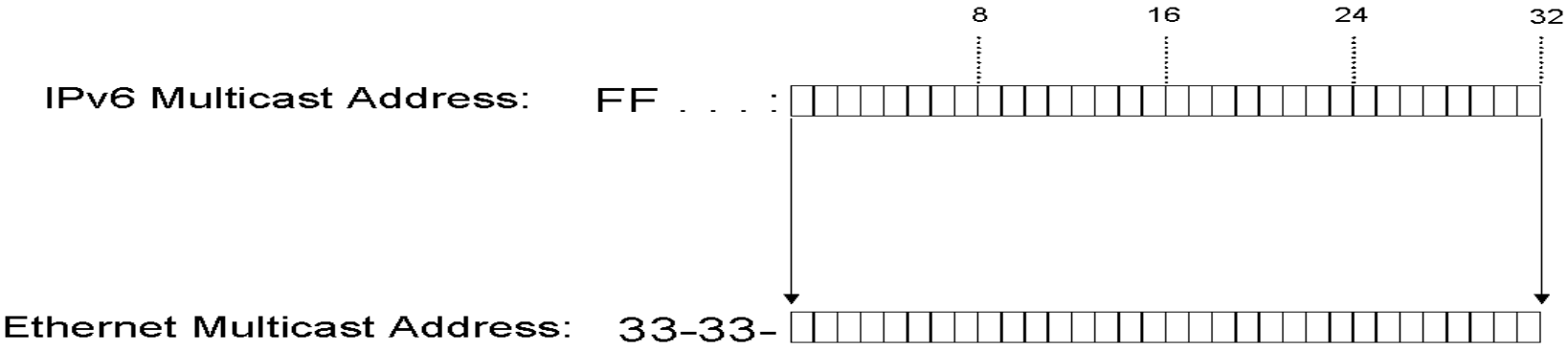
- U/L bit (u)
  - Universally (0) or Locally (1) Administration
- U/G bit (g)
  - Unicast (0) or Group (1) Address



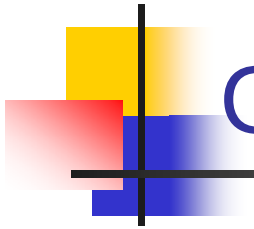
Interface ID Using IEEE EUI-64



Mapping IPv6 Multicast Address to Ethernet MAC Address



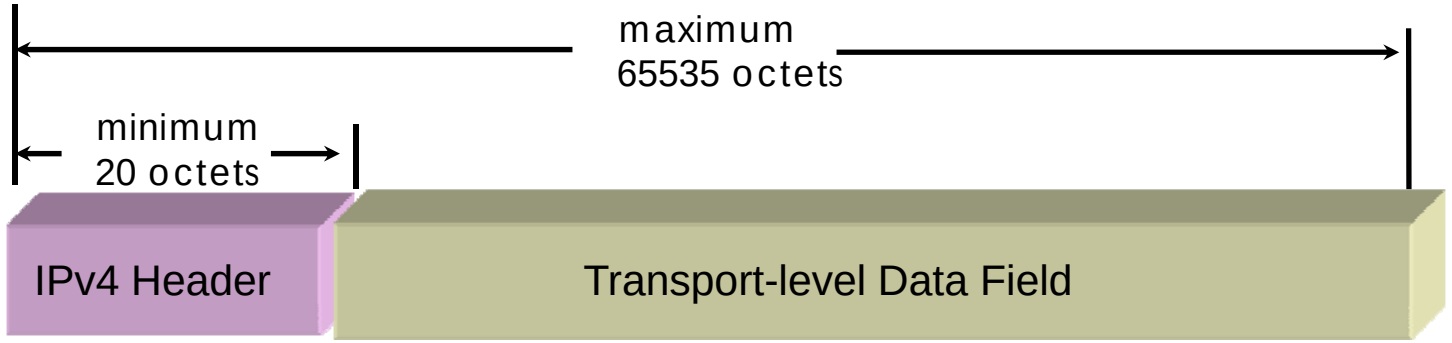
- Use specific vendor code= 33-33 for multicast use
- Avoid address duplicate in solicited-node address (lower 24-bit)
- For examples, a host with Ethernet MAC= 00-AA-00-3F-2A-1C
  - Link local address= FE80::2AA:FF:FE3F:2A1C
  - **33-33**-00-00-00-01 (link-local all-nodes multicast address FF02::1
  - **33-33**-FF-3F-2A-1C (solicited-node multicast address FF02::1:FF3F:2A1C)



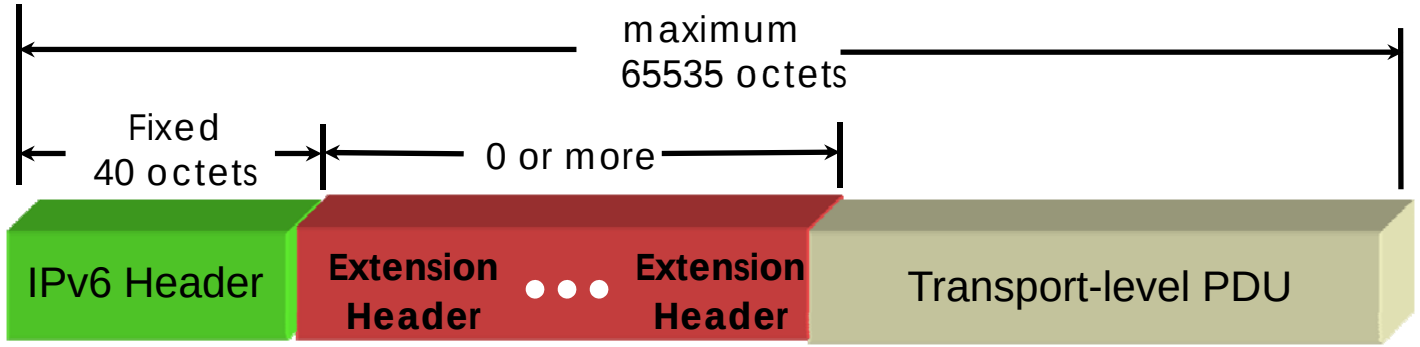
Outline

- IPv6 Addressing
- **IPv6 Header Format**
- ICMPv6 Message Format
- Neighbor Discovery Process

IPv6 vs. IPv4 Packet Data Unit



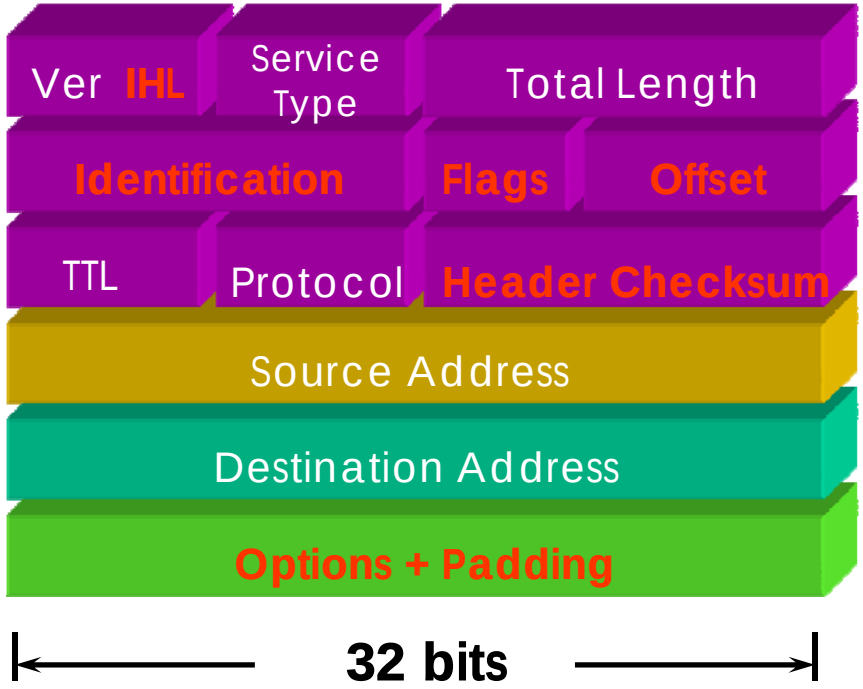
IPv4 PDU



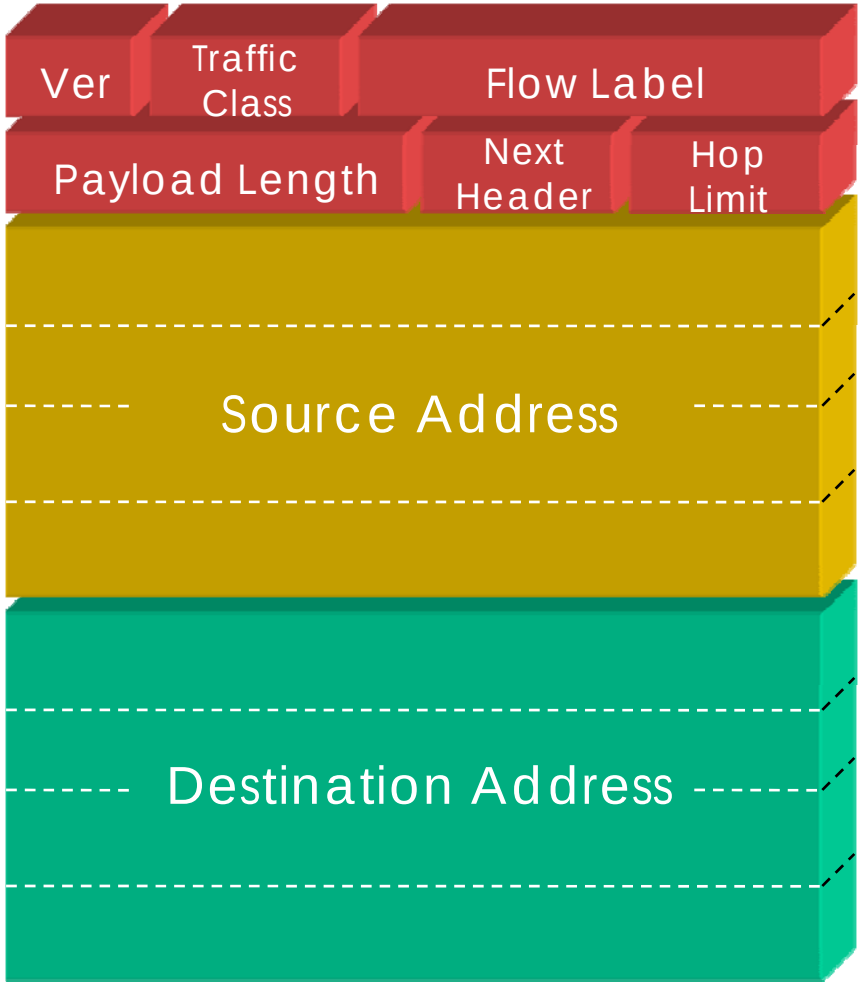
IPv6 PDU

Comparison of IPv4 and IPv6 Headers

IPv4 Packet Header



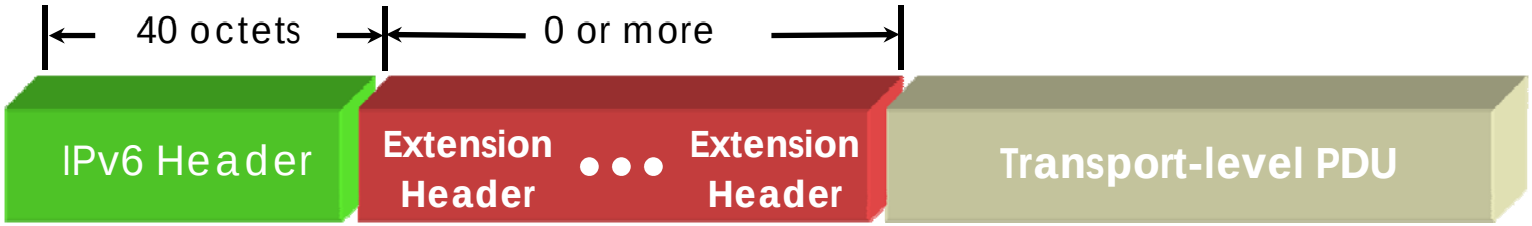
IPv6 Packet Header



Summary of Header Changes Between IPv4 & IPv6

- Streamlined
  - Fragmentation fields moved out of base header
  - IP options moved out of base header
  - Header Checksum eliminated
  - Header Length field eliminated
  - Length field excludes IPv6 header
- Revised
  - Alignment changed from 32 to 64 bits
  - Time to Live → Hop Limit
  - Protocol → Next Header
  - Precedence & TOS → Traffic Class
  - Addresses increased 32 bits → 128 bits
- Extended
  - Flow Label field added

IPv6 Extension Headers

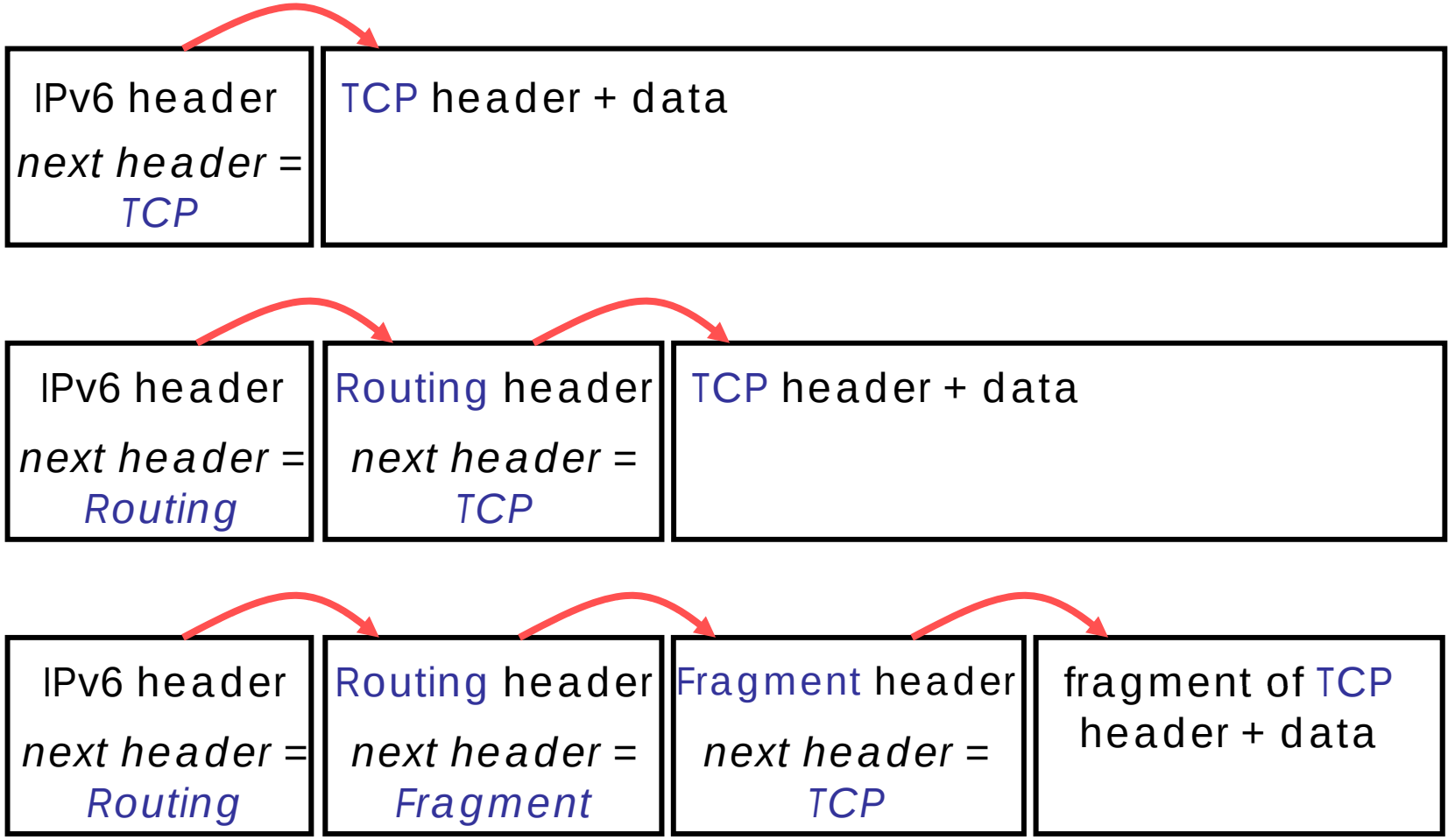


IPv6 PDU general form

Ordered

- Hop-by-hop options header
- Destination options header (*)
- Routing header
- Fragment header
- Authentication header
- Encapsulating security payload header
- Destination options header (*)

Extension Header Examples

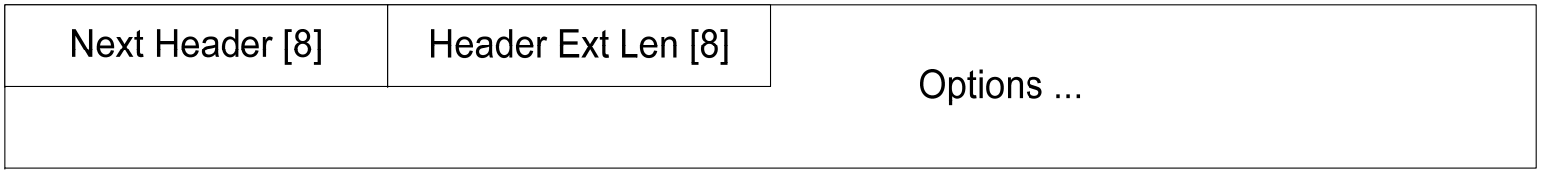


Value of Next Header Field

Value (in decimal)	Header	Value (in decimal)	Header
0	Hop-by-Hop options Header	46	RSVP
6	TCP	50	Encapsulated Security Header
17	UDP	51	Authentication Header
41	Encapsulated IPv6 header	58	ICMPv6
43	Routing Header	59	No next Header
44	Fragmentation Header	60	Destination Options header

Hop-by-Hop option header

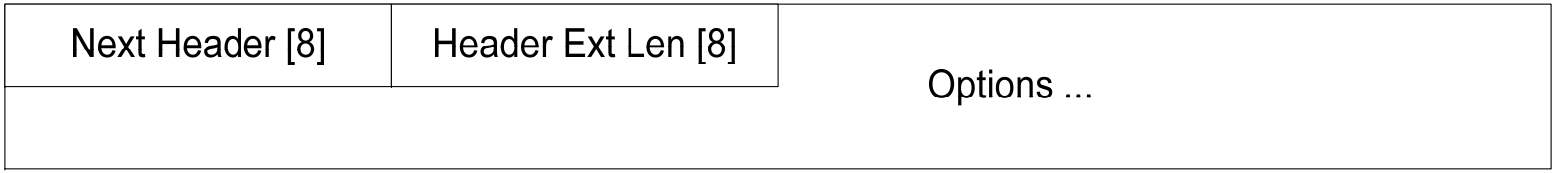
- Specify delivery parameters at each hop on the path to the destination



  - Header Extension Length
    - No of 8-byte block in Hop-by-Hop option header
    - Not including first 8 bytes
  - Option
    - Type-Length-Value (TLV) format
    - 0: Pad1– insert single byte of padding
    - 1: PadN – insert 2 or more byte of padding
    - 5: Router Alert – indicate to the router the packets require additional processing (MLD and RSVP)
    - 194: Jumbo Payload – indicate payload size over 65,535

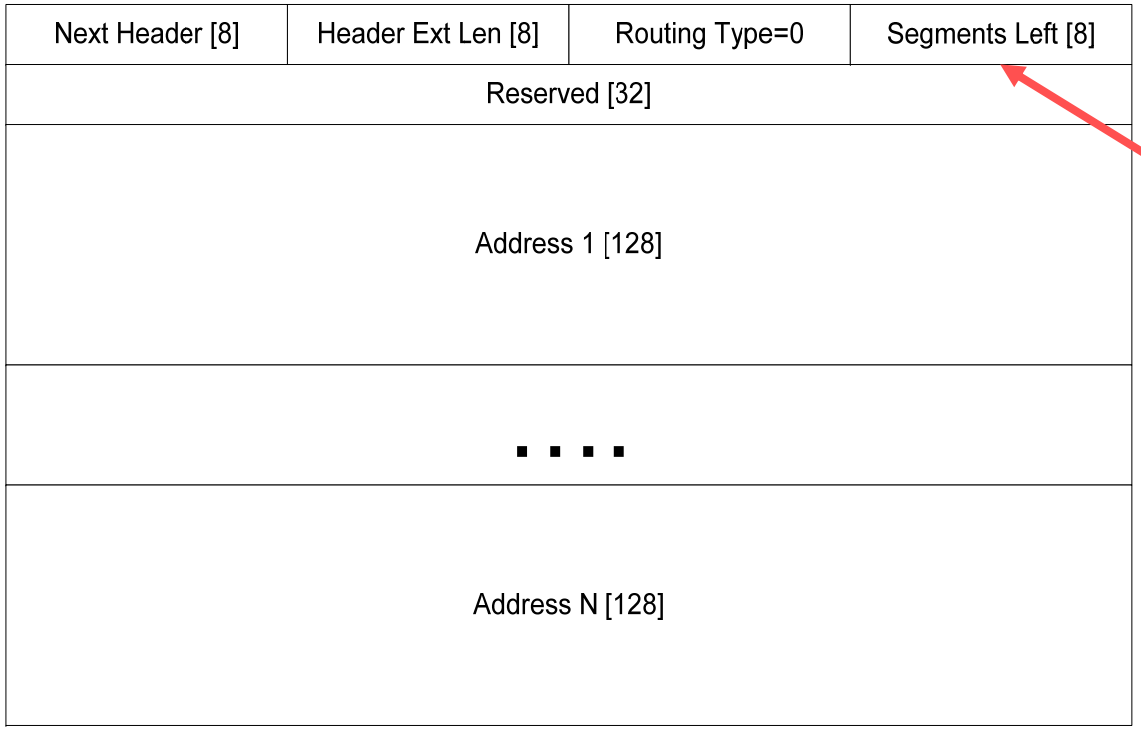
Destination Option Header

- Specify packet delivery parameter for either intermediate destinations or final destinations
- If Routing Header exists, it specifies delivery or processing options at each intermediate destination



Routing Header

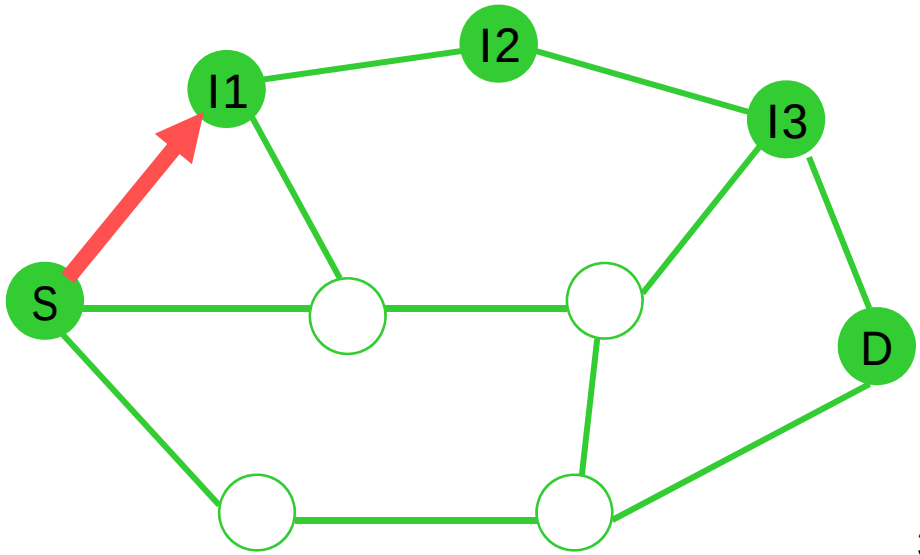
- Similar to the source routing in IPv4
- Use of Routing header with anycast addresses allows routing packets through particular regions
  - e.g., for provider selection, policy, performance, etc.



Segments Left indicates how many intermediate nodes are to be transited.

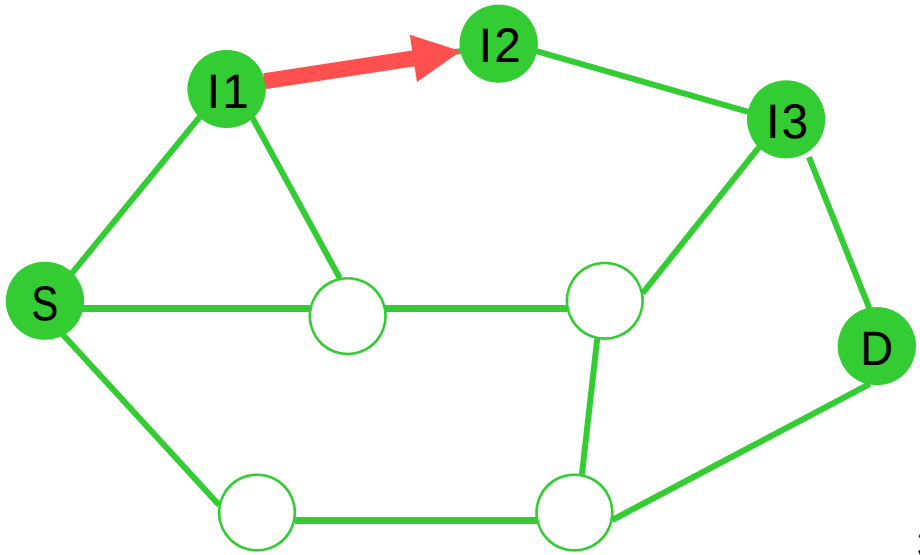
Examples of Type 0 Routing Header: S->I1->I2->I3->D

- Source Address=S
- Destination Address=I1
- Hdr Ext Len=6
- Segments Left=3
- Address[1]=I2
- Address[2]=I3
- Address[3]=D



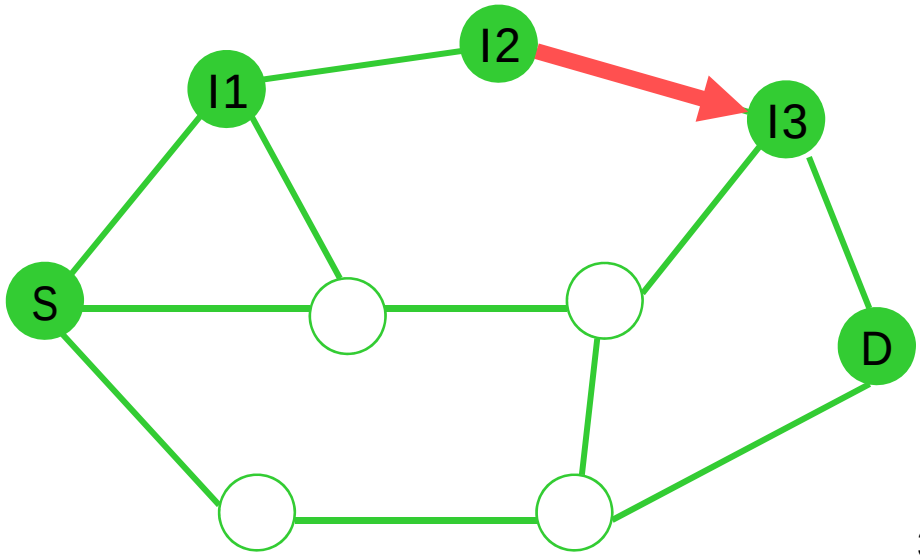
Examples of Type 0 Routing Header: S->I1->I2->I3->D

- Source Address=S
- Destination Address=I2
- Hdr Ext Len=6
- Segments Left=2
- Address[1]=I1
- Address[2]=I3
- Address[3]=D



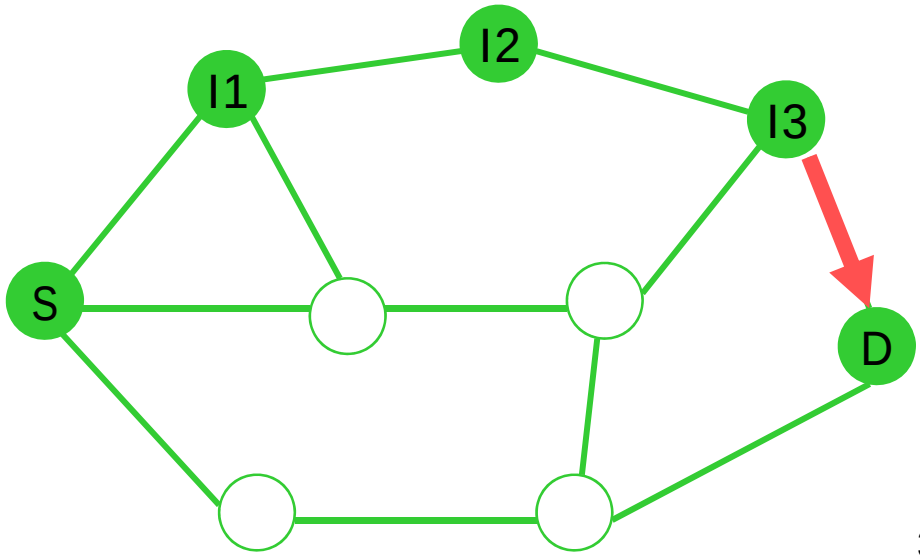
Examples of Type 0 Routing Header: S->I1->I2->I3->D

- Source Address=S
- Destination Address=I3
- Hdr Ext Len=6
- Segments Left=1
- Address[1]=I1
- Address[2]=I2
- Address[3]=D



Examples of Type 0 Routing Header: S->I1->I2->I3->D

- Source Address=S
- Destination Address=D
- Hdr Ext Len=6
- Segments Left=0
- Address[1]=I1
- Address[2]=I2
- Address[3]=I3



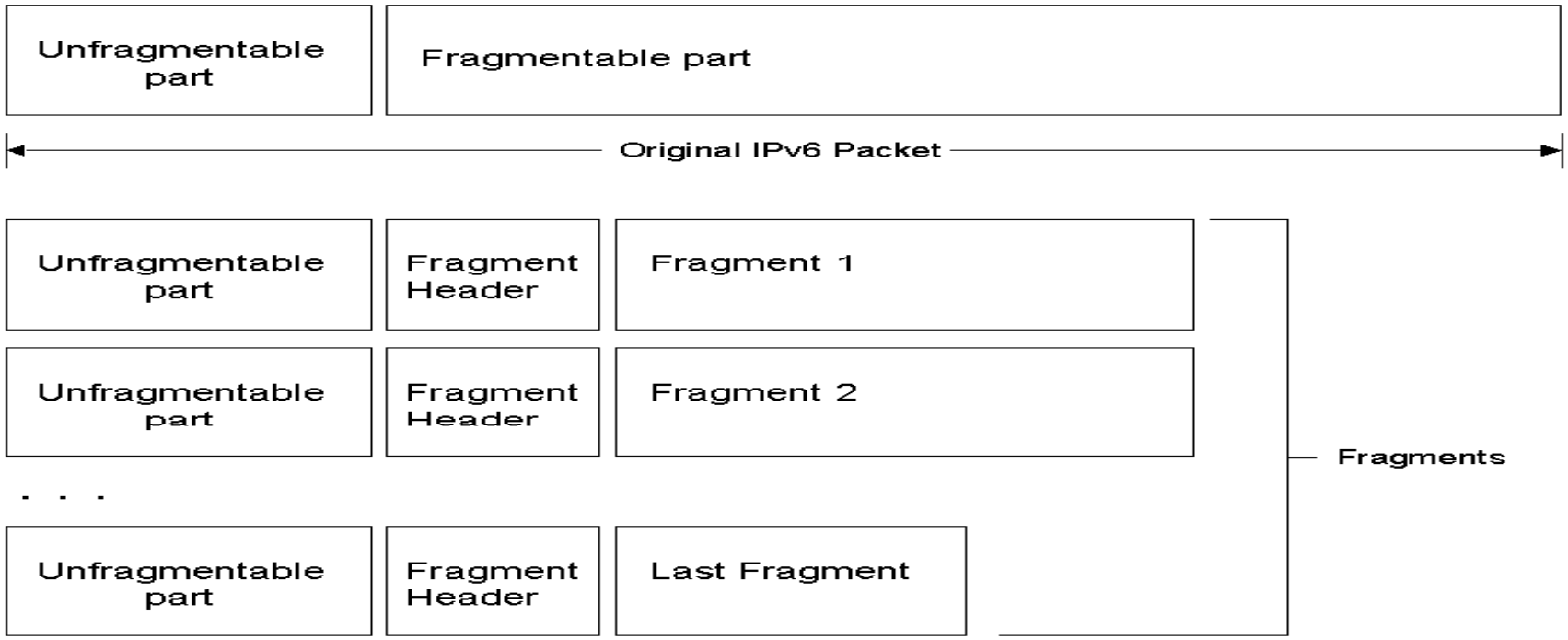
Fragment Header

- Fragmentation and reassembly services is an end-to-end function; routers do not fragment packets en-route if too big—they send ICMP "packet too big" instead
- Support only on source nodes

- M indicates more fragments
- Fragment Offset in units of 8 bytes
- Identification is a 32-bit label used to identify the fragment

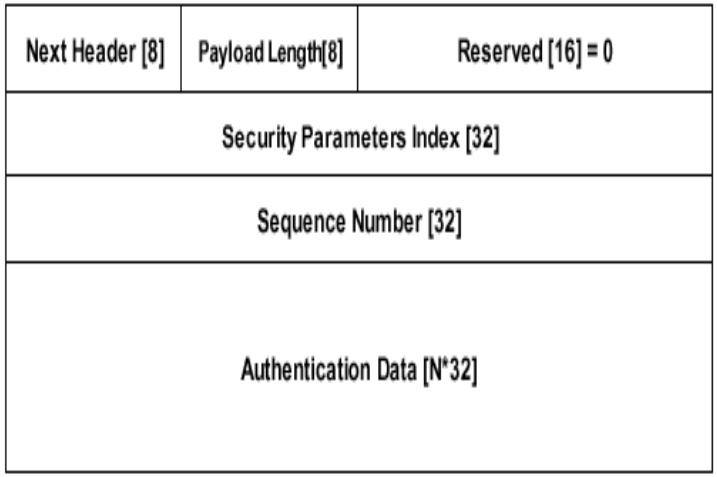
Fragmentation process

- Unfragmentable part must be processed by each intermediate node and destination
- Fragmentable part must only processed at final destination



Authentication Header

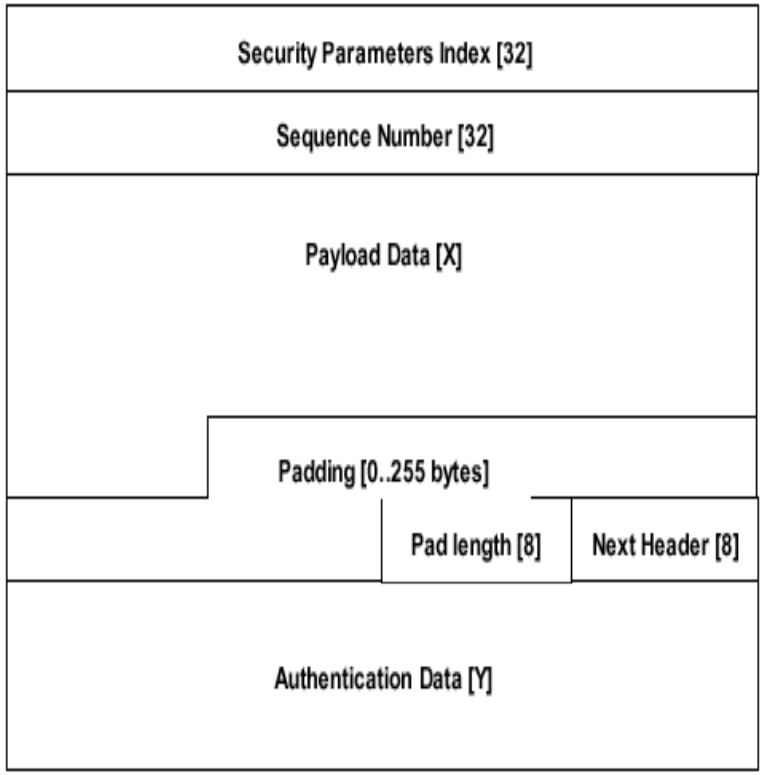
- Provide data authentication
  - verification of the node that sent the packet
- Provide data integrity
  - verification that the data was not modified in transit
- Provide anti-replay protection
  - assurance that captured packets cannot be retransmitted and accepted as valid data



- SPI identifies the security association.
- Sequence Number is incremented by sender for every packet.
- Authentication Data is the integrity check data.

Encapsulating Security Payload(ESP) Header and Trailer

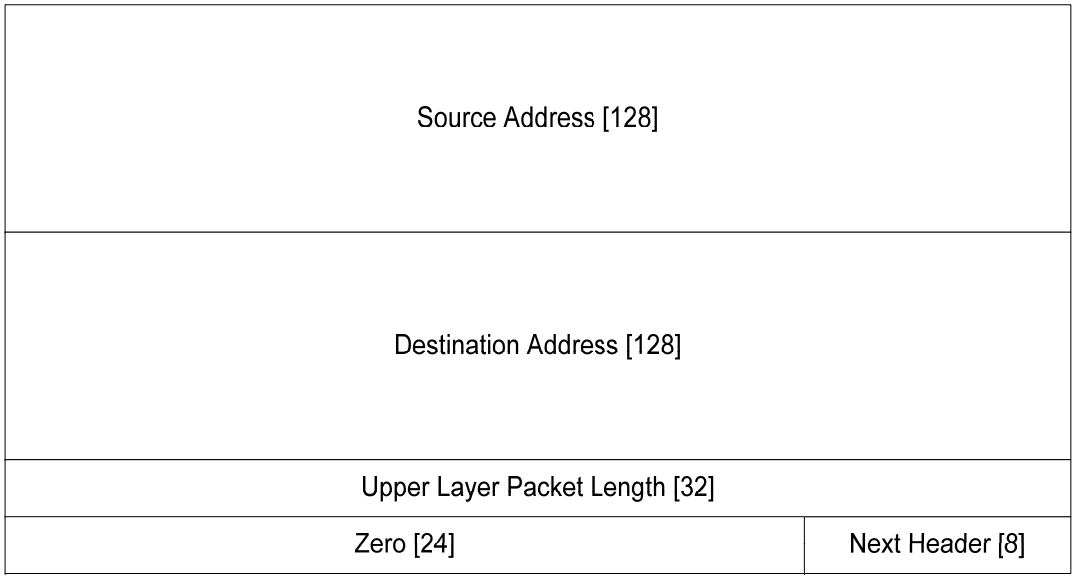
- Provides data confidentiality, data authentication, and data integrity



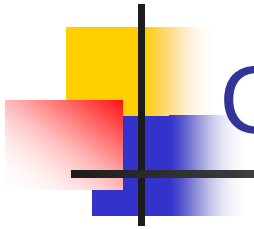
Field Name	Bit Length	Description
Security Parameters Index	32	Used as for the AH.
Sequence Number	32	Used as for the AH
Payload Data.	X	The encrypted payload along with any data required for decryption (e.g. initialization data)
Padding.	0-256	Added to the header to ensure that the payload data ends on the appropriate byte boundary
Pad length	8	The number of padding bytes added
Next header	8	As for all other options headers
Authentication Data	Y	Used as for the AH.

Upper Layer Checksums

- TCP/UDP "Pseudo-Header" for IPv6

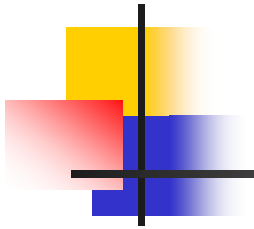


- ICMPv6 includes the above pseudo-header in its checksum computation
  - Protect ICMP from misdelivery or corruption of IPv6 header
  - Next header field in pseudo-header for ICMP = 58 (ICMP)



Outline

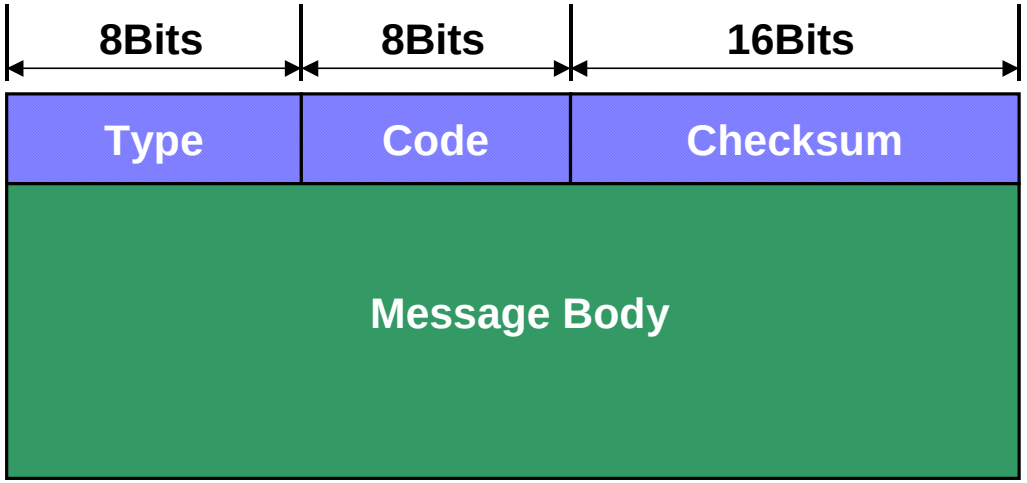
- IPv6 Addressing
- IPv6 Header Format
- **ICMPv6 Message Format**
- Neighbor Discovery Process



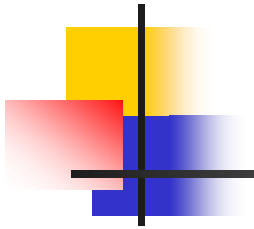
Features of ICMPv6

- An integral part of IPv6 and MUST be fully implement by every IPv6 node (RFC 2463)
- Next Header value= 58
- Report delivery or forwarding errors
- Provide simple echo service for troubleshooting
- Multicast Listener discovery(MLD) – 3 ICMPv6 messages (defined in RFC 2710)
- Neighbor Discovery(ND) – 5 ICMPv6 messages (defined in RFC 2461)

ICMPv6 Message Format



Field Name	Bit Length	Description
Checksum	16	The checksum is a 16 bit CRC check calculated over the entire ICMPv6 message, including an IPv6 "Pseudo Header" as defined in Section 8.1 of [IPv6].
Code	8	The code field further defines the message content
Type	8	The Type field identifies the message contents. ICMPv6 messages are divided into two classes; Error messages and Informational messages. The Type values of Error messages go from 0 to 127. Informational messages have type values from 128 to 255.
Message Body	N*32	The message body depends on the message type. Every ICMPv6 error message includes as much of the offending packet as can be accommodated without exceeding the minimum IPv6 MTU (1280 bytes).

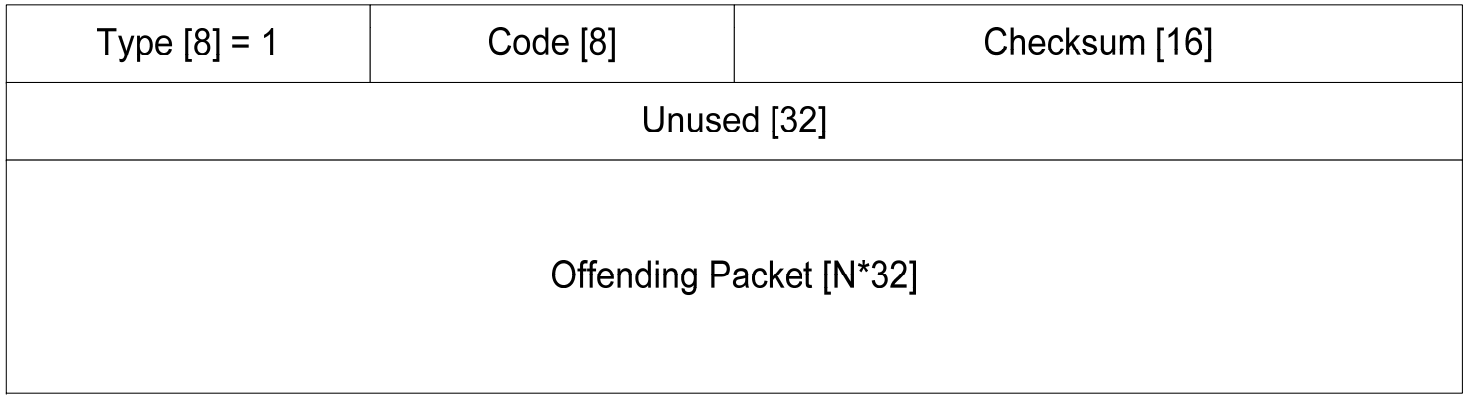


Two Types of ICMP Messages

- Error messages
  - Report error in the forwarding or delivery
  - Type 1 (Destination Unreachable)
  - Type 2 (Packet Too Big)
  - Type 3 (Time Exceeded)
  - Type 4 (Parameter Problem)
- Informational messages
  - Provide diagnostic function, MLD, and ND
  - Type 128 (Echo Request)
  - Type 129 (Echo Reply)

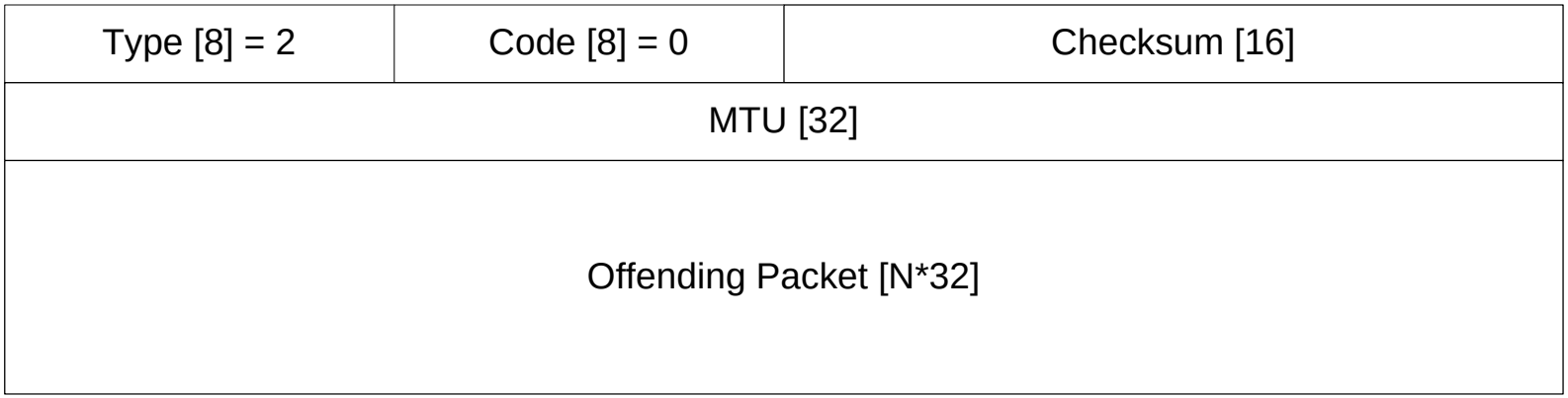
Error Message
(Destination Unreachable)

- Sent by router or destination host
  - Type Value = 1
  - Code 0 (No route to destination)
  - Code 1 (Communication with destination prohibited)
  - Code 2 (Not Assigned)
  - Code 3 (Address unreachable)
  - Code 4 (Port unreachable)



Error message (Packet Too Big)

- Sent when link MTU is smaller than the size of packet
- Used for IPv6 Path MTU Discovery process
  - Type Value=2
  - Code 0



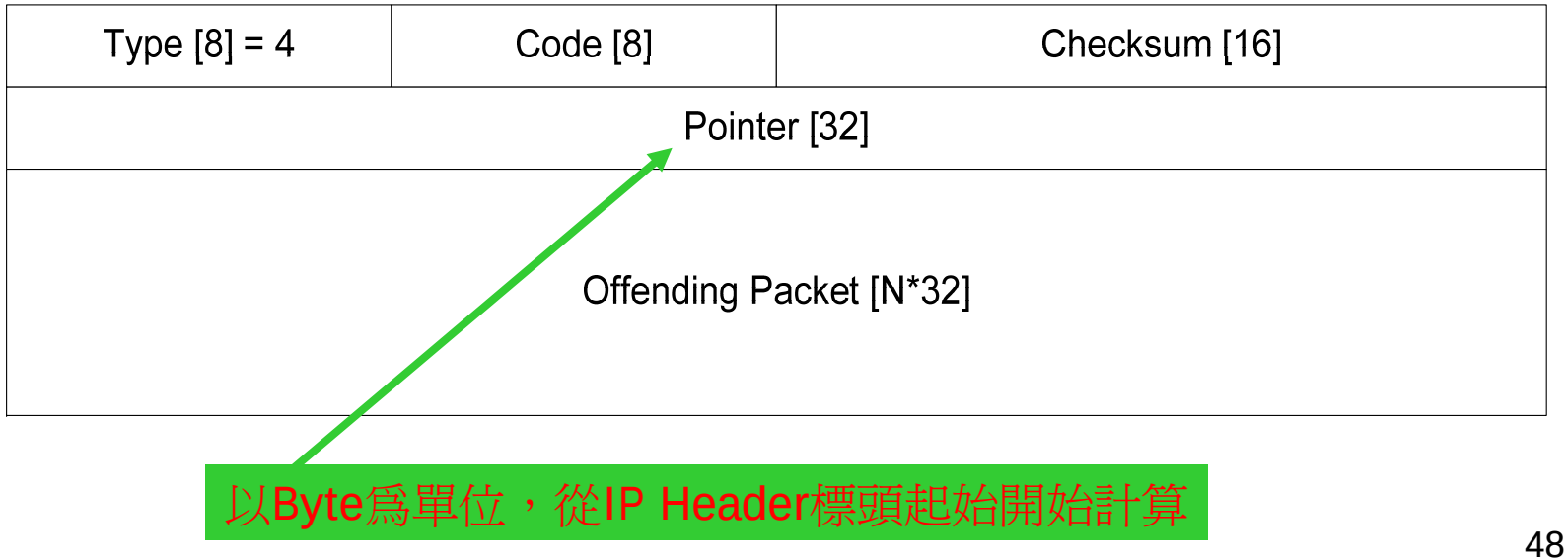
Error message (Time Exceeded)

- Sent by router when Hop limit field is zero
  - Type Value=3
  - Code 0
    - Hop limit= 0
    - Hop limit of outgoing packets is not large enough to reach destination, or routing loop exist
  - Code 1
    - fragmentation reassembly time of destination host is exceeded

Type [8] = 3	Code [8]	Checksum [16]
Unused [32]		
Offending Packet [N*32]		

Error message (Parameter Problem)

- Sent by router or destination host when errors of IPv6 header or extension header
  - Type Value=4
  - Code 0 (Erroneous header field)
  - Code 1 (Unrecognized Next Header type)
  - Code 2 (Unrecognized IPv6 Option)



Informational message

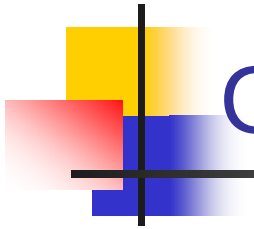
- Echo Request message

Type [8] = 128	Code [8] = 0	Checksum [16]
Identifier [16]		Sequence Number [16]
Data [N*32]		

- Echo Reply message

Type [8] = 129	Code [8] = 0	Checksum [16]
Identifier [16]		Sequence Number [16]
Data [N*32]		

- Identifier and Sequence Number are send by host and used to match incoming Echo Reply with corresponding Echo Request(same as IPv4)
- Multicast Listener Query messages:
  - Query, Report, done (like IGMP for IPv4)
  - Does not include in this presentation



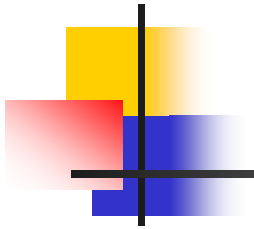
Outline

- IPv6 Addressing
- IPv6 Header Format
- ICMPv6 Message Format
- **Neighbor Discovery Process**

Neighbor Discovery (ND) Process

Reference RFC 2461

- Router discovery
  - Discover the local hosts on an attached link
  - Equivalent to ICMPv4 Router Discovery
- Prefix discovery
  - Discovery the network prefix
  - Equivalent to ICMPv4 Address Mask Request/Reply
- Parameter discovery
  - Discovery additional parameter(ex: link MTU, default hop limit for outgoing packet)
- Address auto-configuration
  - Configure IP address for interfaces
- Address resolution
  - Equivalent to ARP in IPv4



IPv6 ND Process (cont.)

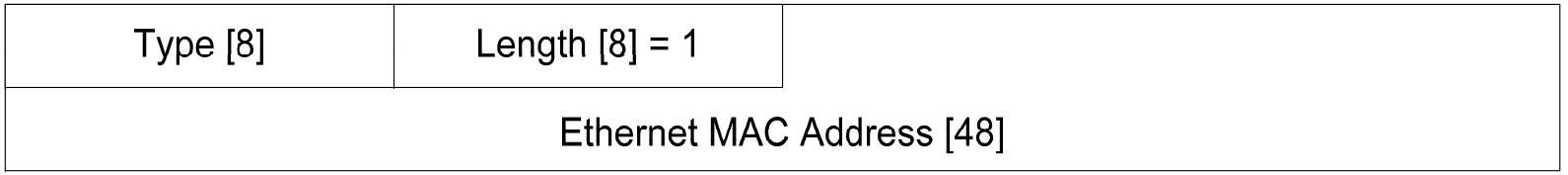
- Next-hop Determination
  - Destination address, or
  - Address of an on-link default router
- Neighbor Unreachable Detection (NUD)
- Duplicate Address Detection (DAD)
  - Determine that an address considered for use is not already in use by a neighboring node
- First-hop Redirect Function
  - Inform a host of a better first-hop IPv6 address to reach a destination
  - Equivalent to ICMPv4 Redirect

ND Message Format

- 5 ND messages:
  - Type 133 Code 0 (Router Solicitation)
  - Type 134 Code 0 (Router Advertisement)
  - Type 135 Code 0 (Neighbor Solicitation)
  - Type 136 Code 0 (Neighbor Advertisement)
  - Type 137 Code 0 (Redirect)
- All ND message are send with hop limit= 255
  - If it is not set to 255, the message is silently discarded
  - Provide protection from ND-based network attacks launched from off-link nodes
  - Router can not have forwarded the ND message from an off-link node

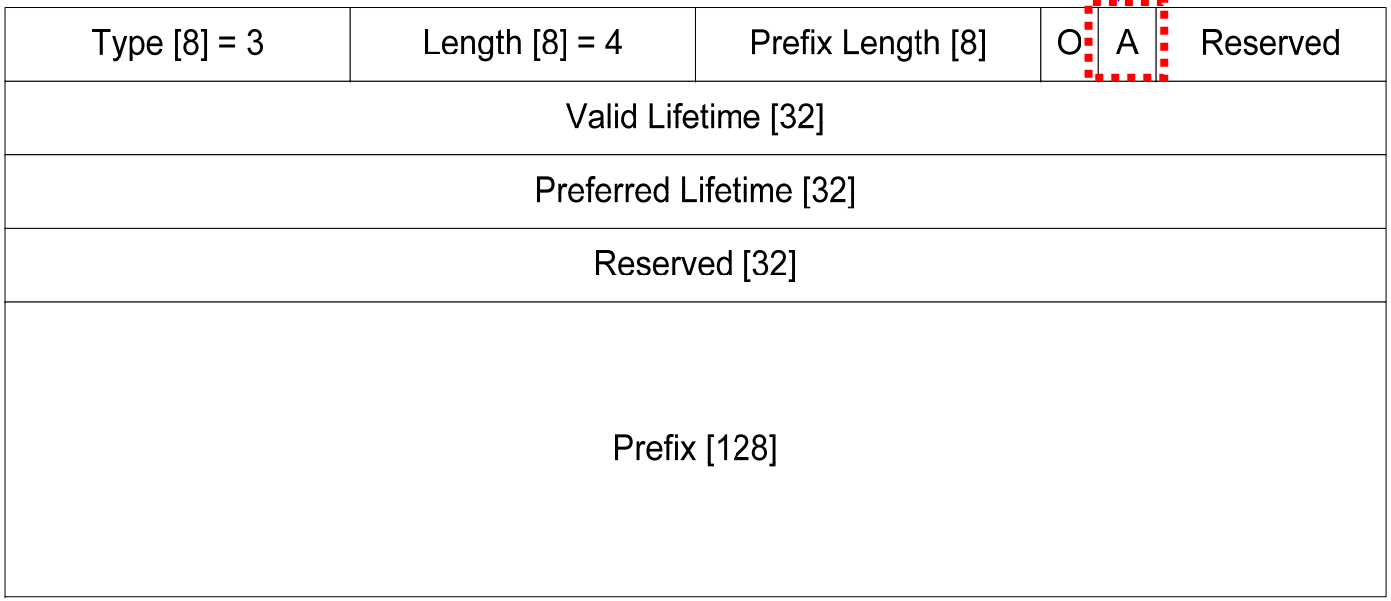
Neighbor Discovery Options

- Source/Target link-layer address option
  - Source link-layer address
    - Indicate the link-layer address of the ND sender
    - Included in Neighbor Solicitation, Router Solicitation, and Router Advertisement
    - Type = 1
  - Target link-layer address
    - Indicate the link-layer address of the neighbor node
    - Included in Neighbor Advertisement and Redirect
    - Type = 2
  - Example for Ethernet



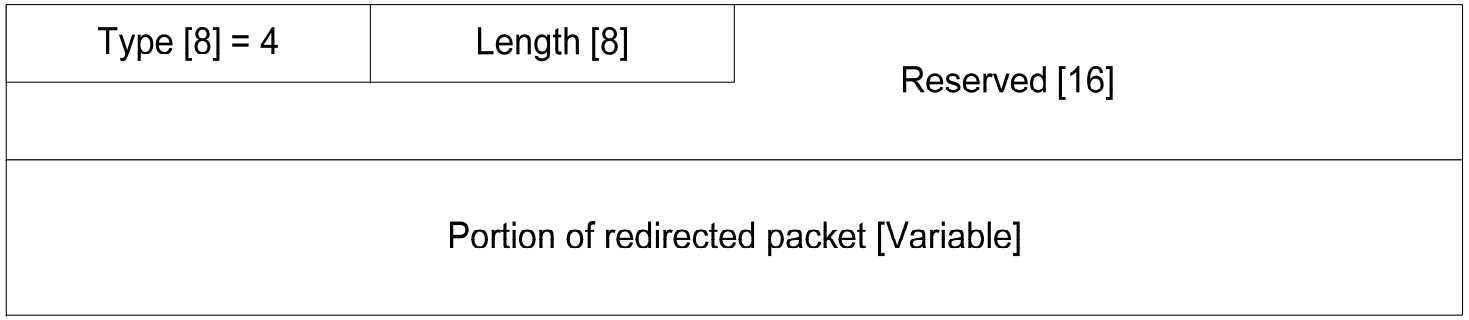
Neighbor Discovery Options(cont.)

- Prefix information option
  - Indicate both address prefixes and information about address auto-configuration
  - Included in Router Advertisement
  - Can be multiple prefix information options in Router Advertisement message
  - Autonomous flag: stateless address configuration

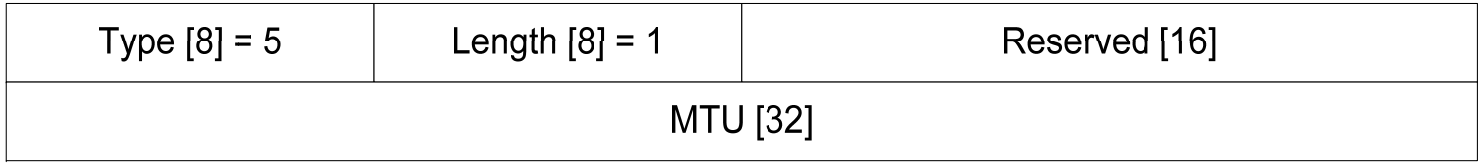


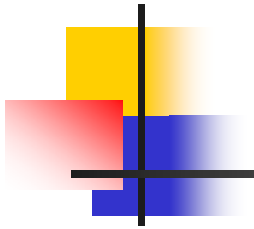
Neighbor Discovery Options (cont.)

- Redirect header option



- MTU option

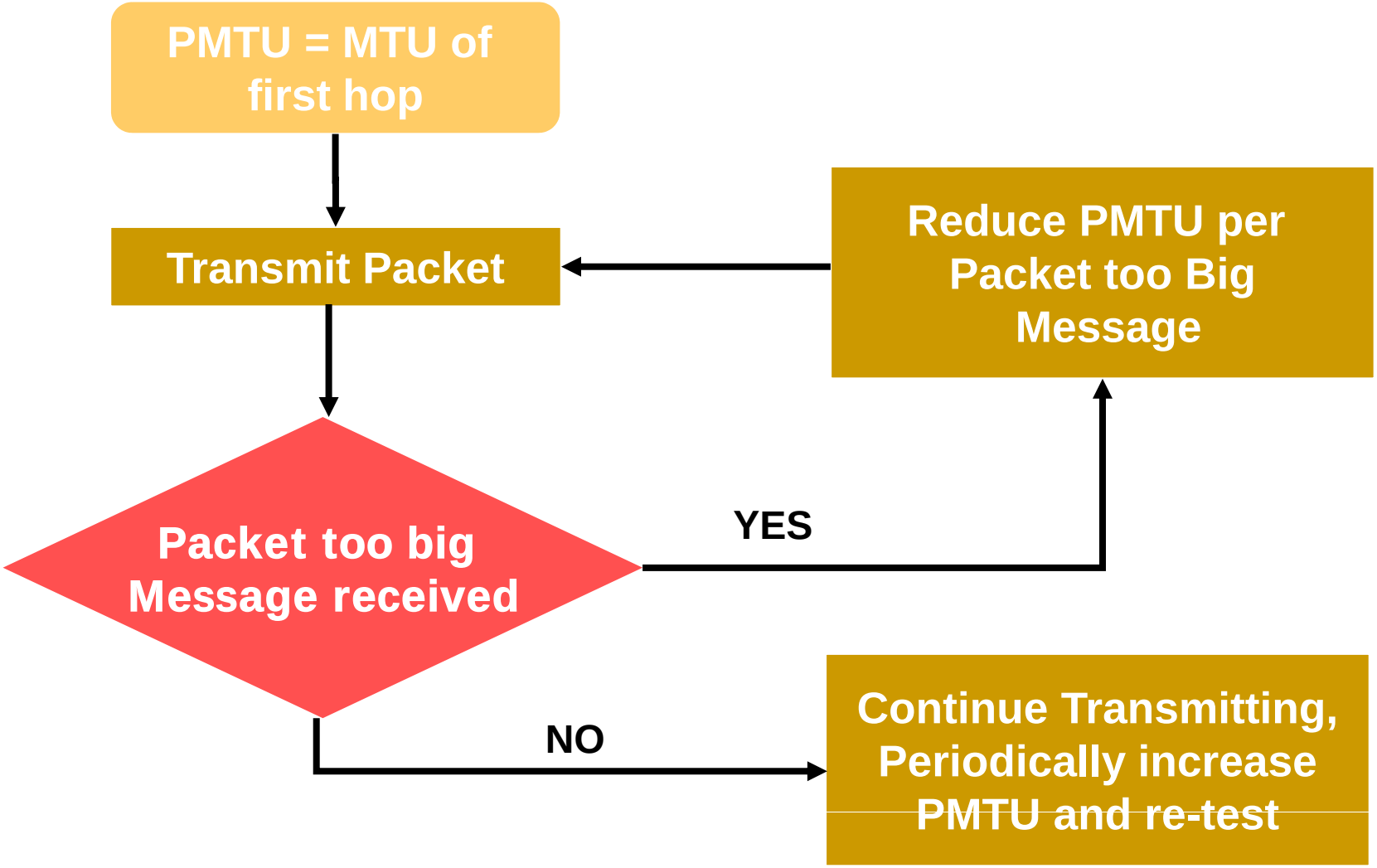




Path MTU (= Min{ link MTUs })

- Link MTU
  - A link's maximum transmission unit (ex: the max IP packet size that can be transmitted over the link)
- Path MTU
  - The minimum MTU of all the links in a path between a source and a destination
- Minimum link MTU for IPv6 is 1280 octets vs 68 octets for IPv4
- On links with MTU < 1280, link-specific fragmentation and reassembly must be used
- On links that have a configurable MTU, it's recommended a MTU of 1500 bytes

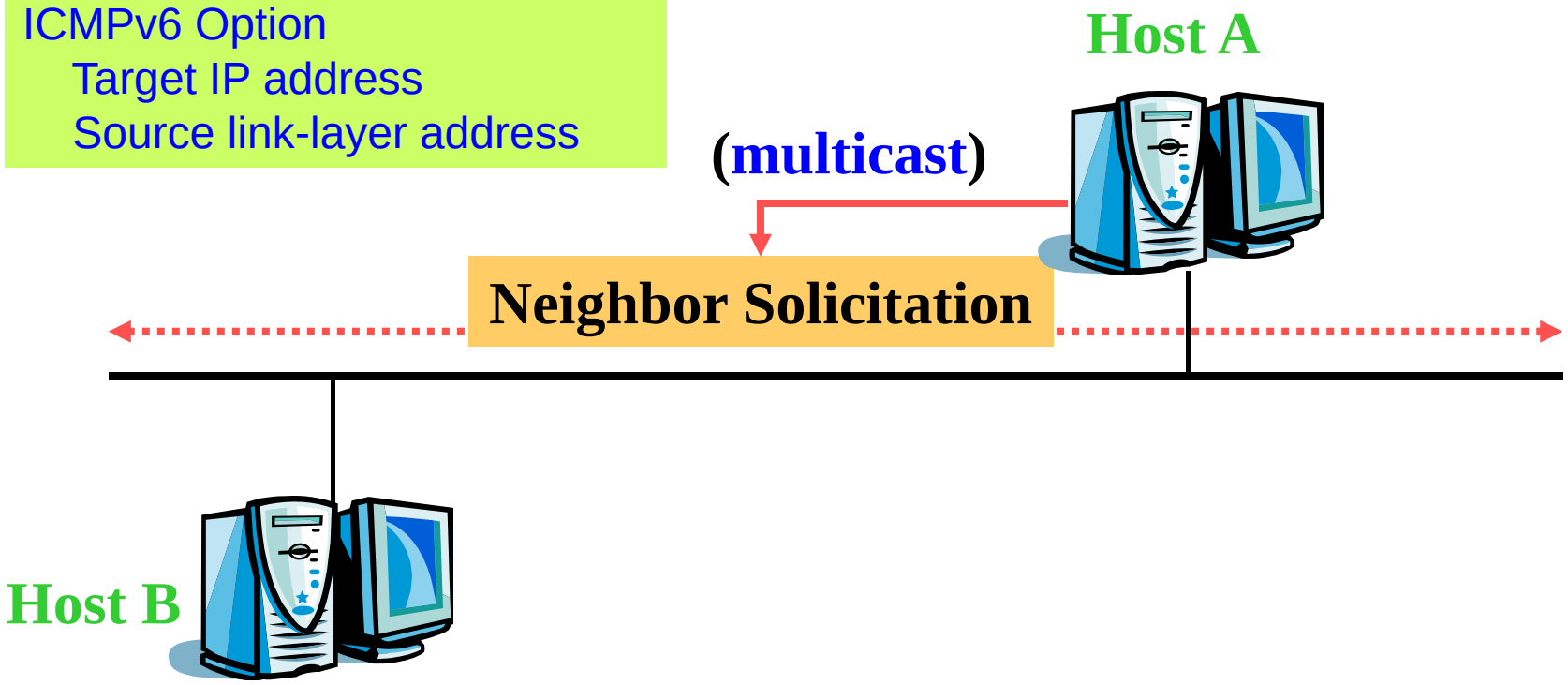
Path MTU Discovery (RFC 1981)



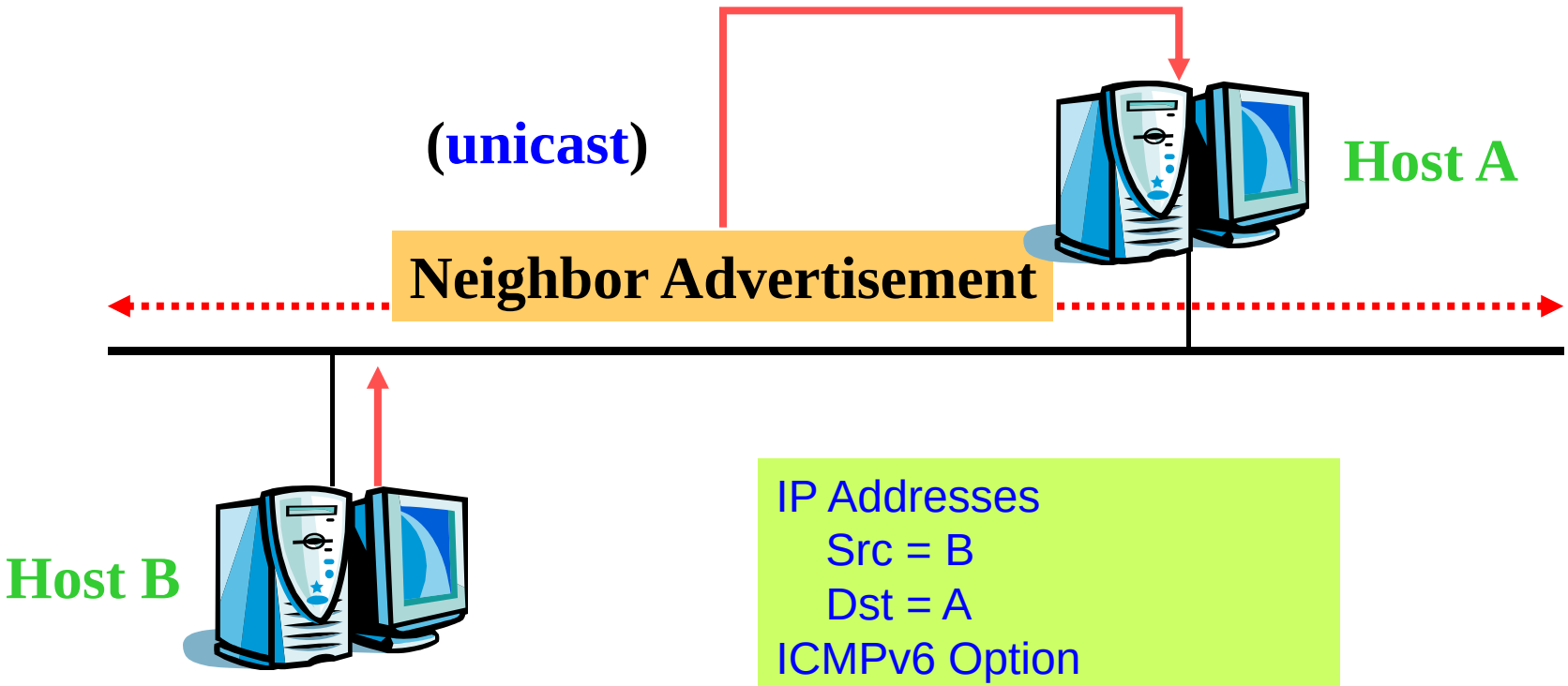
MAC Address Resolution (1)

IP Addresses
- Src = A
- Dst = Solicited-node address

ICMPv6 Option
- Target IP address
- Source link-layer address



MAC Address Resolution (2)



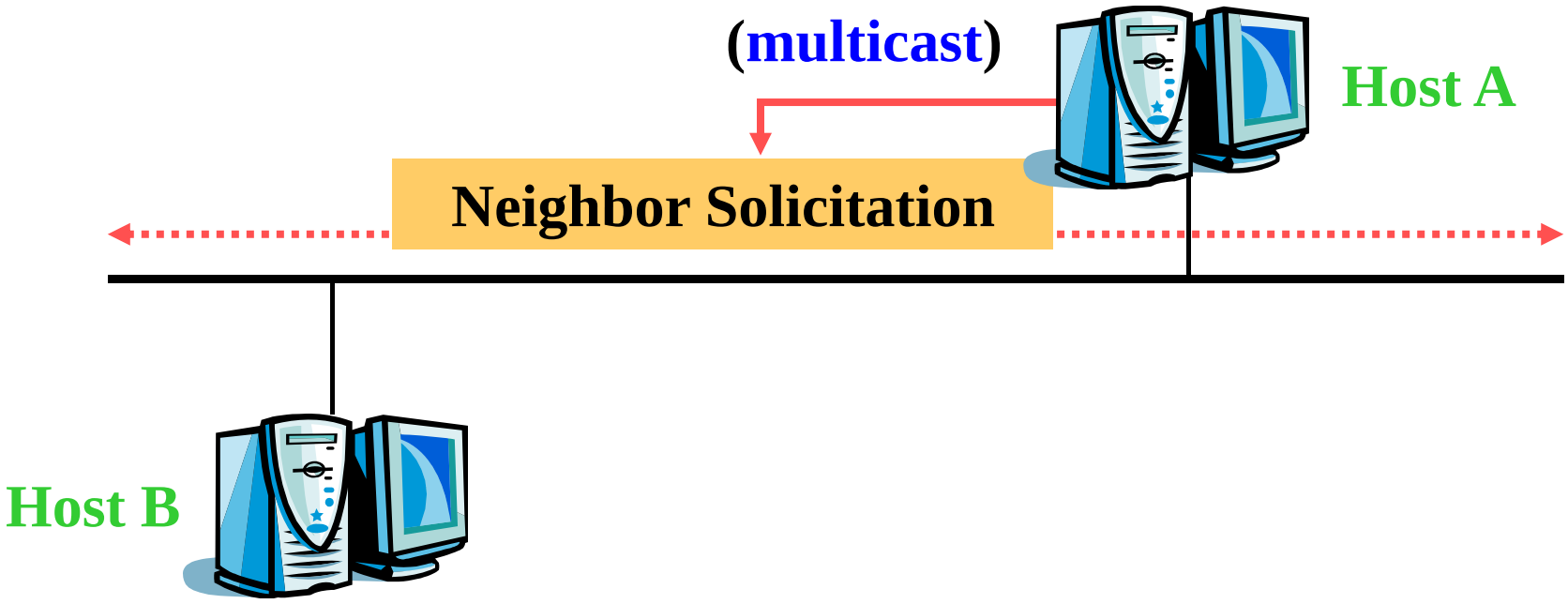
IP Addresses
- Src = B
- Dst = A

ICMPv6 Option
- Target IP address
- Target link-layer address

Duplicate Address Detection (1)

IP Addresses
- Src = ::
- Dst = Solicited-node address

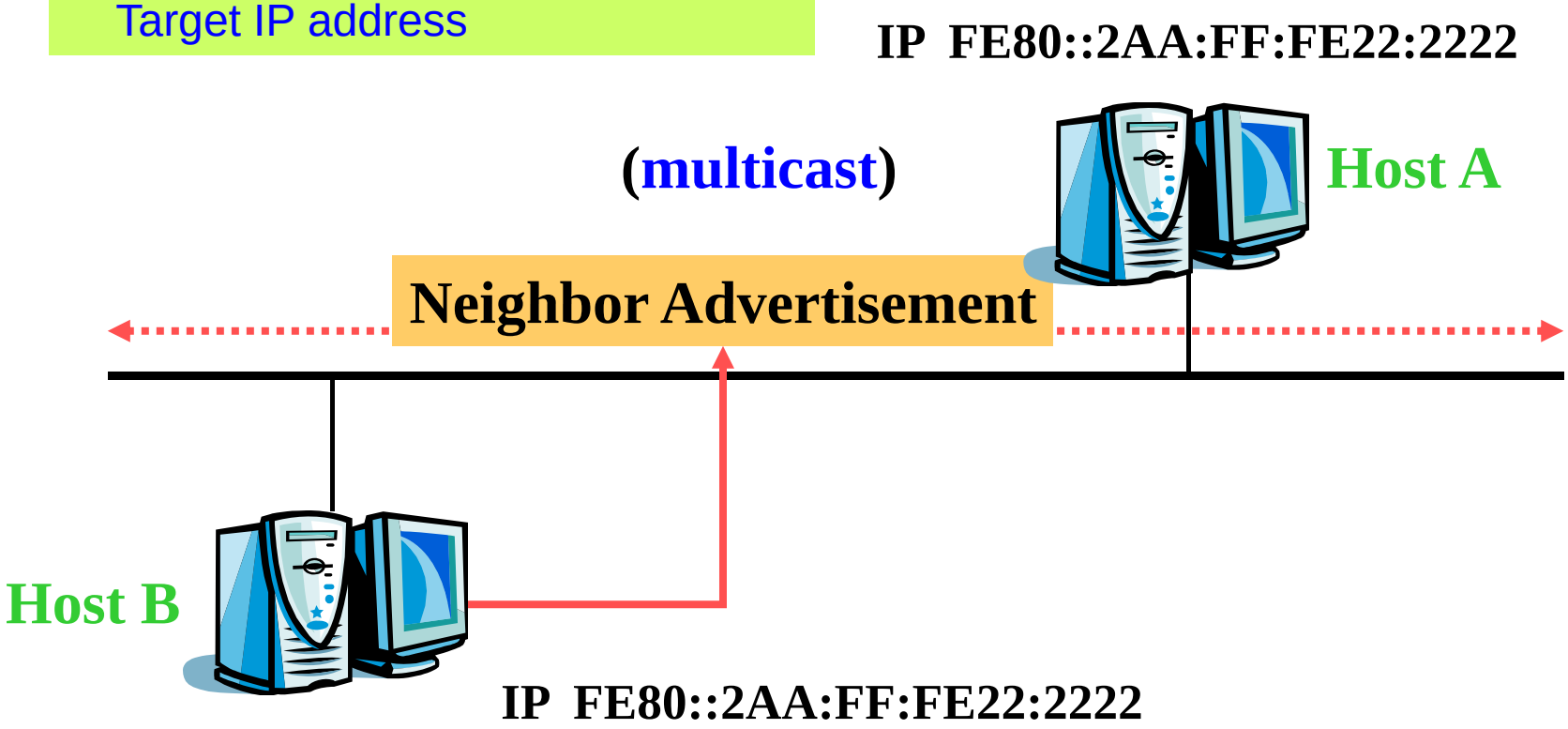
ICMPv6 Option
- Target IP address



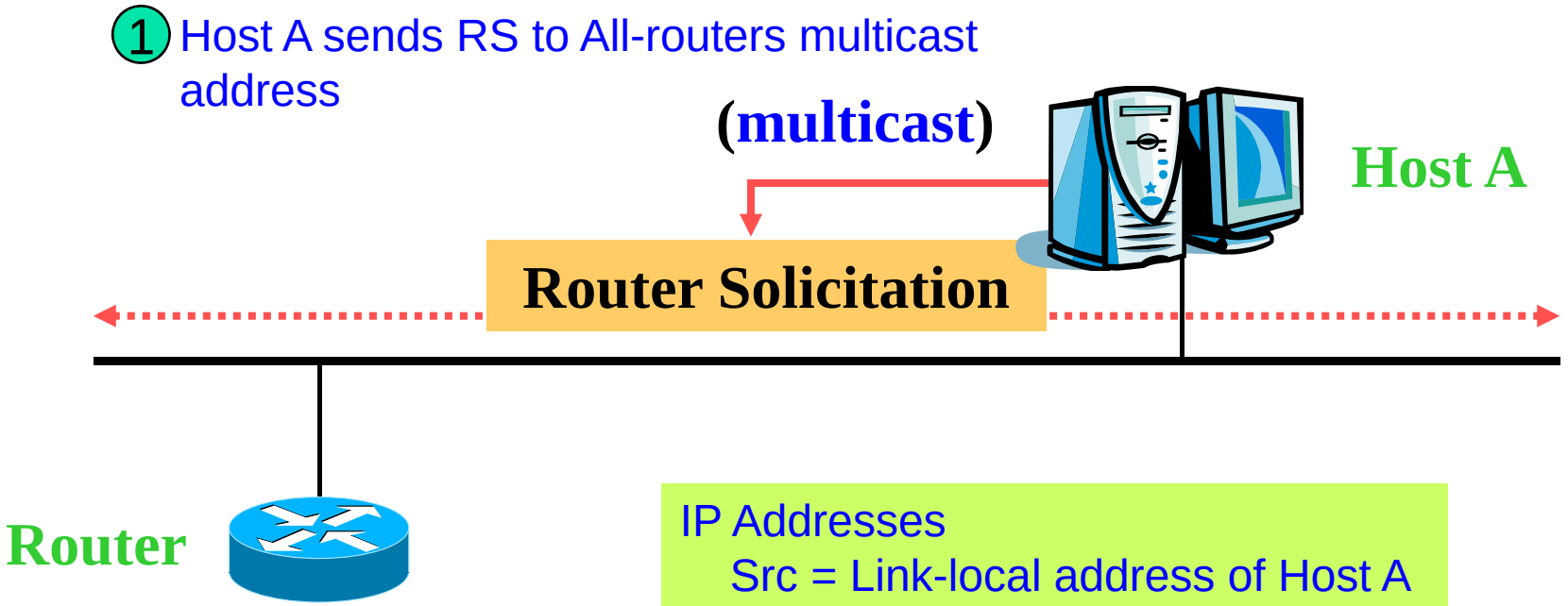
Duplicate Address Detection (2)

IP Addresses
- Src = Link-local address of Host B
- Dst = Solicited-node address

ICMPv6 Option
- Target IP address



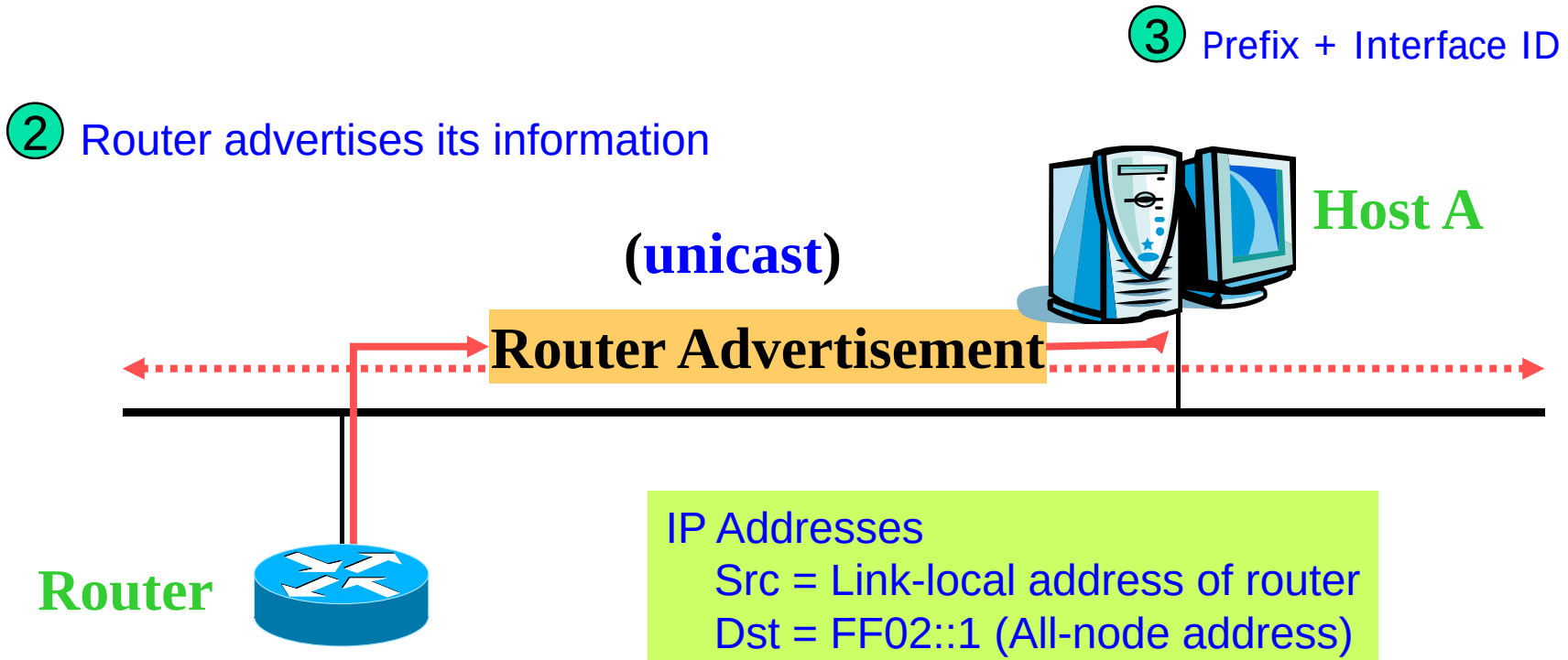
Address Auto-configuration (1)



IP Addresses
- Src = Link-local address of Host A
- Dst = FF02::2 (All-routers address)

ICMPv6 Option
- Empty

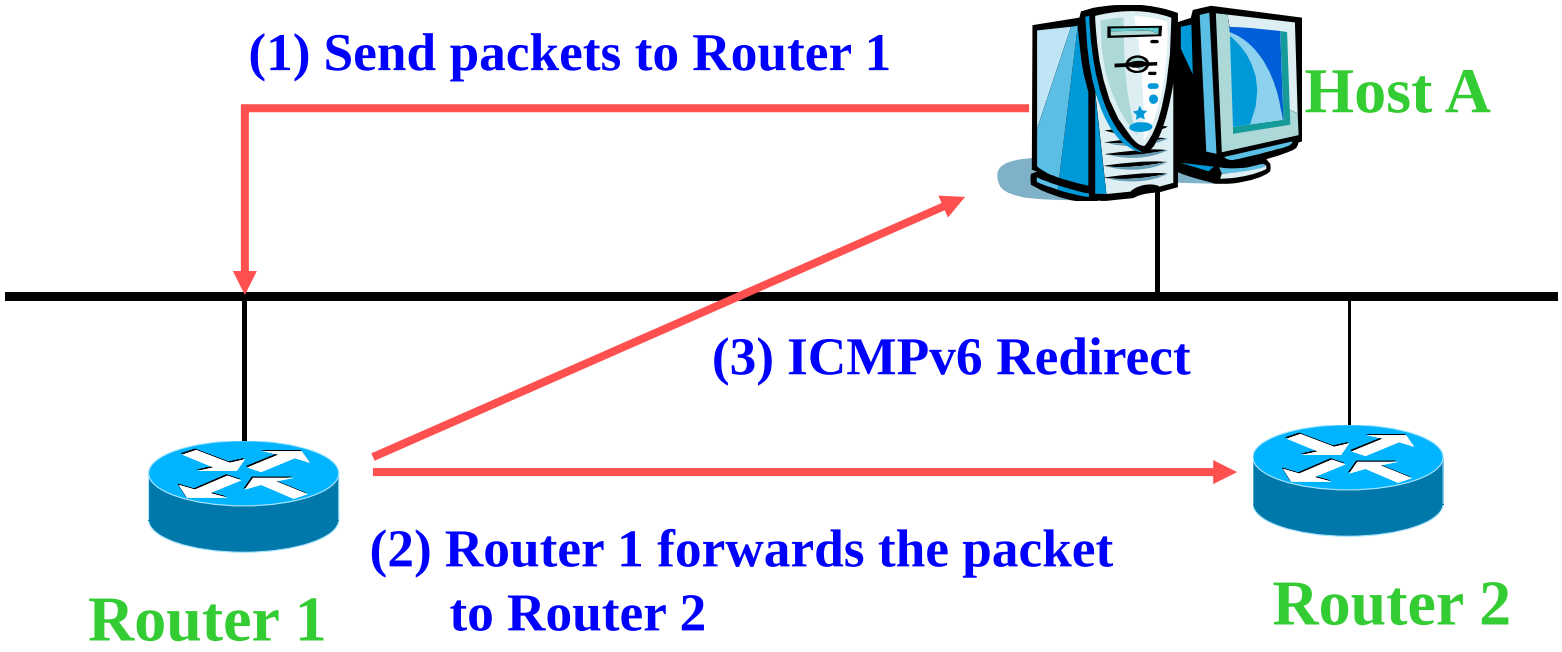
Address Auto-configuration (2)



IP Addresses
- Src = Link-local address of router
- Dst = FF02::1 (All-node address)

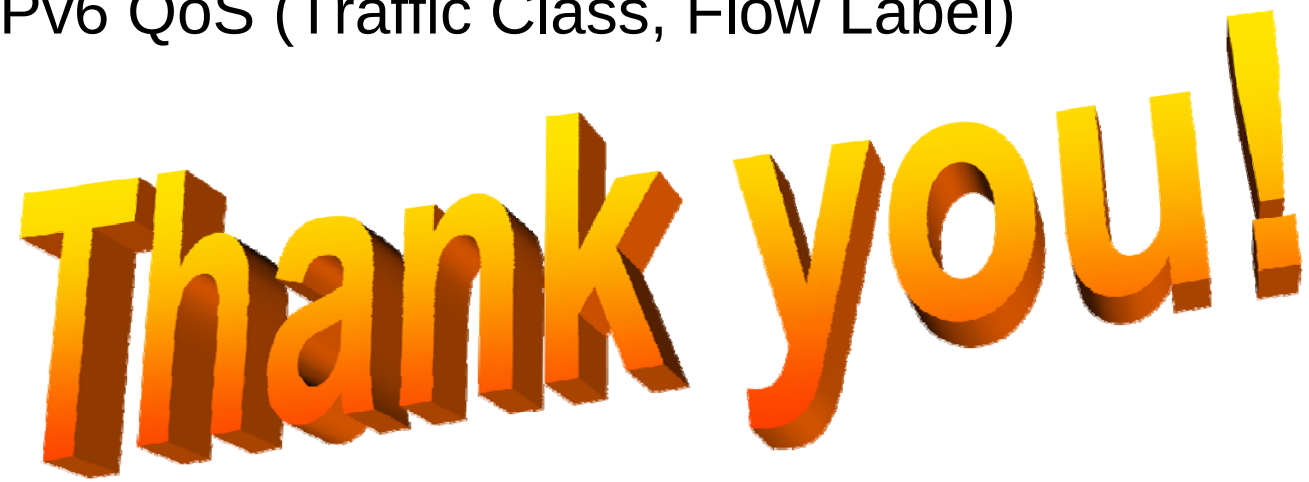
ICMPv6 Option
- Link-layer address
- MTU
- Prefix Information

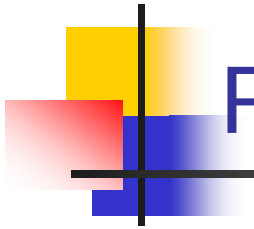
Redirect


(1) Send packets to Router 1
Host A
(3) ICMPv6 Redirect
(2) Router 1 forwards the packet
to Router 2
Router 1
Router 2

Future Topics

- IPv6 Auto-configuration (IPv6, ICMPv6)
- IPv6 Routing (RIPng, OSPF, BGP4+)
- IPv6 Security (AH and ESP headers, For MIPv6)
- Mobile IPv6 (HMIPv6 and Fast Handover for MIPv6)
- IPv6 Anycast Address
- IPv6 Multihoming
- IPv6 QoS (Traffic Class, Flow Label)





Reference

- RFC2460. Internet Protocol, Version 6 (IPv6) Specification. S. Deering, R. Hinden. December 1998. (PS)
- RFC3513. Internet Protocol Version 6 (IPv6) Addressing Architecture. R. Hinden, S. Deering. April 2003. (PS)
- RFC2463. Internet Control Message Protocol (ICMPv6) for the Internet Protocol Version 6 (IPv6) Specification. A. Conta, S. Deering. December 1998. (DS)
- RFC2461. Neighbor Discovery for IP Version 6 (IPv6). T. Narten, E. Nordmark, W. Simpson. December 1998. (DS)
- 謝佳男、朱永正、陳懷恩. “IPv6解析”. 台灣歐萊禮.
- 2002巡迴演講講義. “IPv6 Addressing”. http://www.ipv6.org.tw/Tutorial_IPv6inSummer02.htm
- IPv6 文章(陳懷恩等提供). http://alan.ipv6.club.tw/IPv6.htm