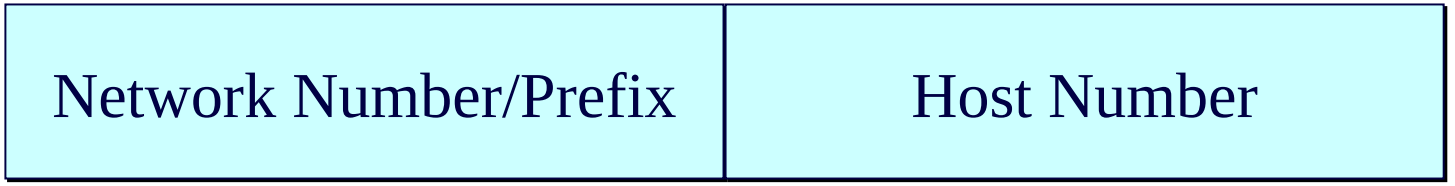
Internet Protocol – Version 6

IPv4

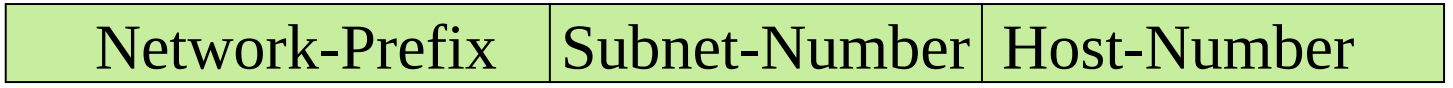
- IPv4, defines a 32-bit address - 2^{32} (4,294,967,296) IPv4 addresses available
- The first problem is the eventual depletion of the IP address space.
- Traditional model of classful addressing does not allow the address space to be used to its maximum potential.
  - When IP was first standardized in September 1981, each system attached to the IP based Internet had to be assigned a unique 32-bit address
  - The 32-bit IP addressing scheme involves a two level addressing hierarchy



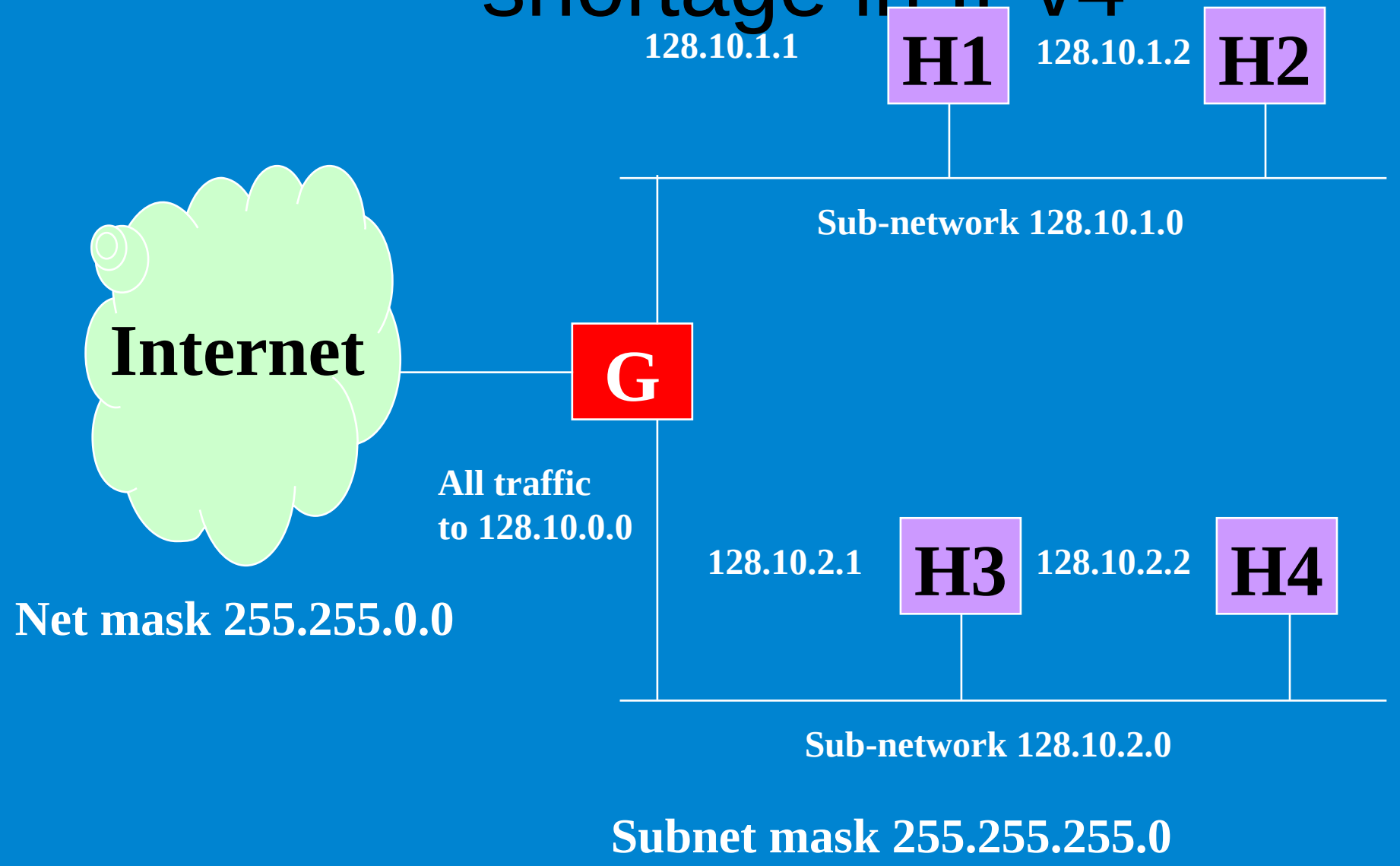
Techniques to reduce address shortage in IPv4

Subnetting

- Three-level hierarchy: network, subnet, and host.
- The extended-network-prefix is composed of the classful network-prefix and the subnet-number
- The extended-network-prefix has traditionally been identified by the subnet mask



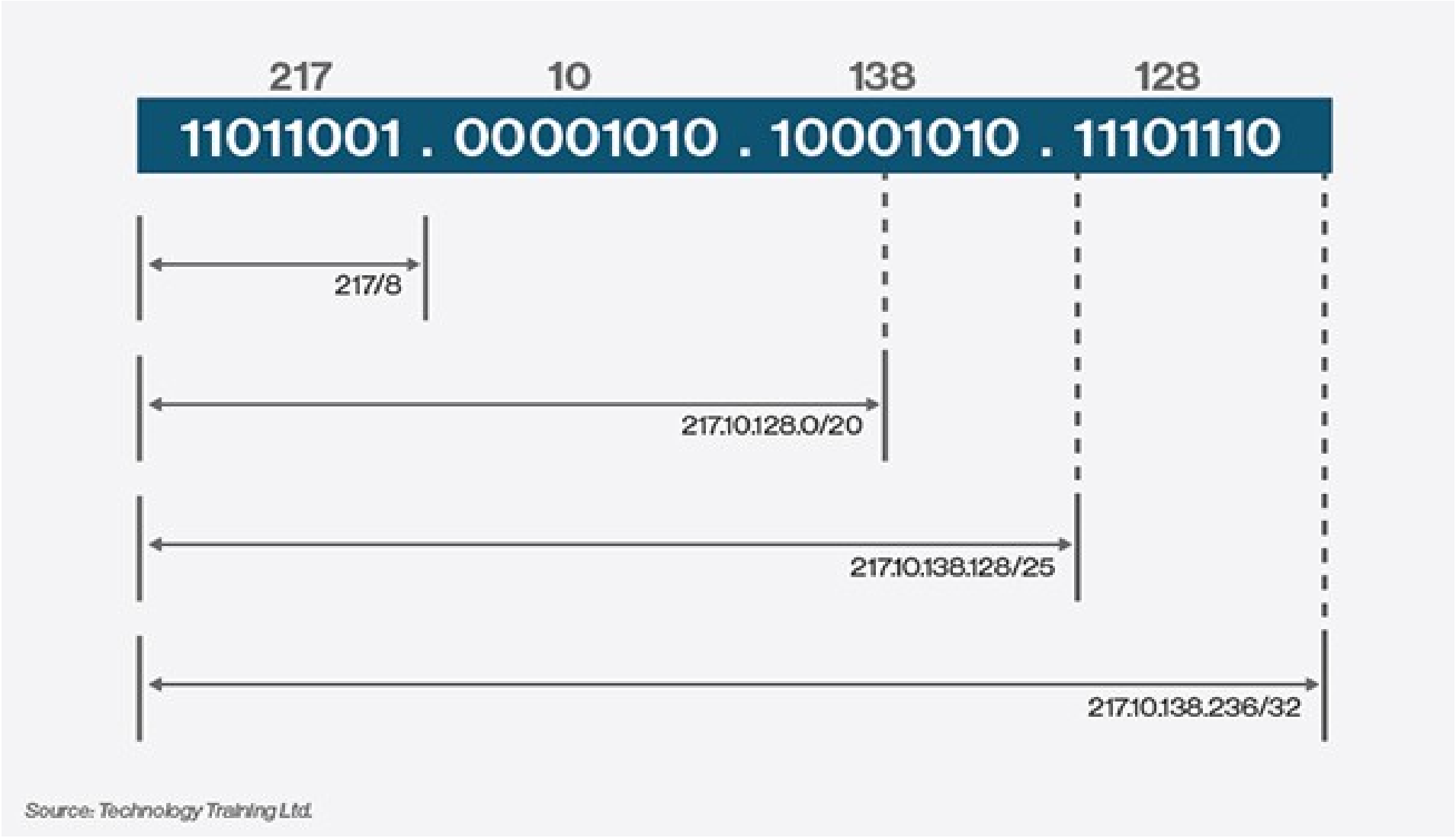
Techniques to reduce address shortage in IPv4



Classless Inter-Domain Routing

- Eliminates traditional classful IP routing.
- Supports the deployment of arbitrarily sized networks
- Routing information is advertised with a bit mask/prefix length
  - specifies the number of leftmost contiguous bits in the network portion of each routing table entry
- Example: 192.168.0.0/21
- To extract the destination IP address
  - Bit-wise AND the destination IP address with the subnet mask for each entry in the routing table.
  - The answer you get after ANDing is checked with the base address entry corresponding to the subnet mask entry with which the destination entry was ANDed.
  - If a match is obtained the packet is forwarded to the router with the corresponding base address

An Example of CIDR

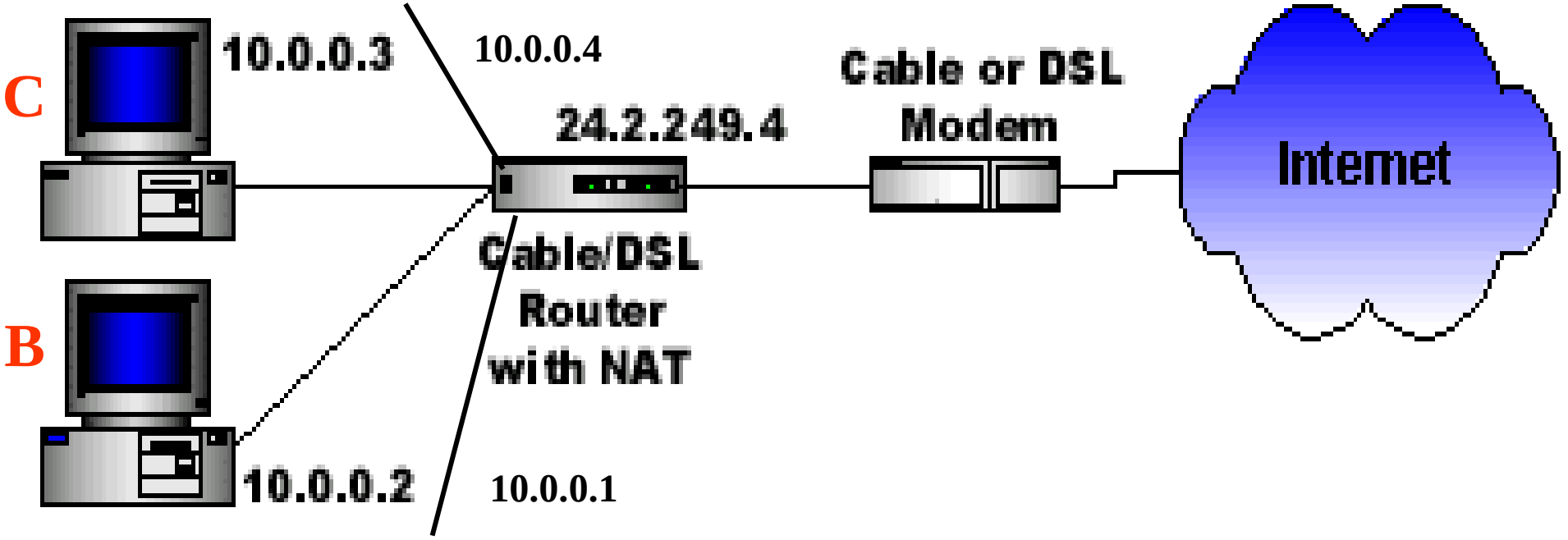


Source: Technology Training Ltd.

Network Address Translation

- Each organization- single IP address
- Within organization – each host with IP unique to the organization, from reserved set of IP addresses

NAT Example



Source Computer	Source Computer's IP Address	Source Computer's Port	NAT Router's IP Address	NAT Router's Assigned Port Number
A	10.0.0.1	400	24.2.249.4	1
B	10.0.0.2	50	24.2.249.4	2
C	10.0.0.3	3750	24.2.249.4	3
D	10.0.0.4	206	24.2.249.4	4

Why is a larger address space needed?

- Overall Internet is still growing its user base
  - ~630 million users end of 2002 – 10% of world population
  - ~1320 million users end of 2007 – 20% of world population
- Users expanding their connected device count
  - 405 million mobile phones in 2000, over 1 billion by 2005
  - ~1 Billion cars in 2010
  - 15% likely to use GPS and locality based Yellow Page services
  - Billions of new Internet appliances for Home users
  - Always-On ; Consumer simplicity required
  - US uses 6.4 IPv4 addresses per person
- Emerging population/geopolitical & economic drivers
  - Moving to an e-Economy requires Global Internet accessibility

Why not use Network Address Translation?

NAT has many serious issues:

- Violates end-to-end model of IP
- Not suitable for end-to-end network security
- Some applications cannot work through NATs
- Layered NAT devices
- Mandates that the network keeps the state of the connections
- How to scale NAT performance for large networks?
- Makes fast rerouting and multihoming difficult

(Multihoming - a mobile phone might be simultaneously connected to a WiFi network and a 3G network)

IPv6 Address Size

- Proposals for fixed-length, 64-bit addresses
  - Minimizes growth of per-packet header overhead
  - Efficient for software processing on current CPU hardware
- Proposals for variable-length, up to 160 bits
  - Compatible with deployed OSI NSAP addressing plans
  - Accommodates auto-configuration using IEEE 802 addresses
  - Sufficient structure for projected number of service providers
- Settled on fixed-length, 128-bit addresses
  - HOW BIG IS THAT REALLY?
  - 3.4 x 1038 possible addressable devices
  - ~ 5 x 1028 addresses per person on the planet

Features of IPv6

- Larger Address Space
- Aggregation-based address hierarchy
  - Efficient backbone routing
- Stateless Address Autoconfiguration
- Header Format Simplification
  - Fixed length, optional headers are daisy-chained
  - IPv6 header is twice as long (40 bytes) as IPv4 header without options (20 bytes)
- Efficient and Extensible IP datagram
- 64 bits aligned
- No checksum at the IP network layer

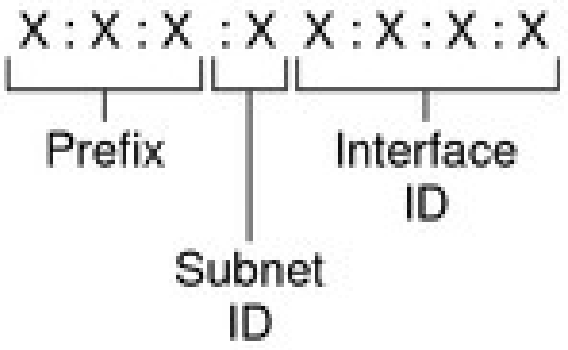
Features of IPv6

- No hop-by-hop segmentation
- Path MTU discovery
  - maximum transmission unit (**MTU**) is the largest size packet or frame, specified in octets (eight-bit bytes), that can be sent in a packet
- No more broadcast
- Security - Authentication and Privacy Capabilities (IPsec mandatory)
- Mobility

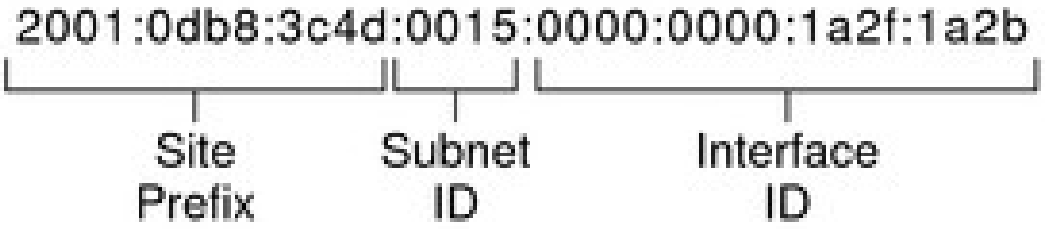
IPv6 Addressing

- IPv6 Addressing rules are covered by multiples RFC’s
  - Architecture defined by RFC 3513 (obsoletes RFC 2373)
- Address Types are :
  - Unicast : One to One (Global, Link local, Site local, Compatible)
  - Anycast : One to Nearest (Allocated from Unicast)
  - Multicast : One to Many
  - Reserved
- A single interface may be assigned multiple IPv6 addresses of any type (unicast, anycast, multicast)
  - No Broadcast Address -> Use Multicast

Basic IPv6 Address Format



Example:



Basic IPv6 Address Format

- The site prefix describes the public topology that is usually allocated to your site by an ISP or Regional Internet Registry (RIR).
- The next field is the 16-bit subnet ID, which you (or another administrator) allocate for your site. The subnet ID describes the private topology, also known as the site topology, because it is internal to your site.
- The rightmost four fields (64 bits) contain the interface ID, also referred to as a token.
- The interface ID is either automatically configured from the interface's MAC address or manually configured in EUI-64 format.

128-bit IPv6 Address

3FFE:085B:1F1F:0000:0000:0000:00A9:1234

8 groups of 16-bit hexadecimal numbers separated by “:”

Leading zeros can be removed

3FFE:85B:1F1F::A9:1234

:: = all zeros in one or more group of 16-bit hexadecimal Numbers (but only once in an address:)

IPv4-compatible address representation
0:0:0:0:0:0:192.168.30.1 = ::192.168.30.1 = ::C0A8:1E01

128-bit IPv6 Address

Prefix Format (PF) Allocation

PF = 0000 0000 : Reserved

PF = 001 : Aggregatable Global Unicast Address

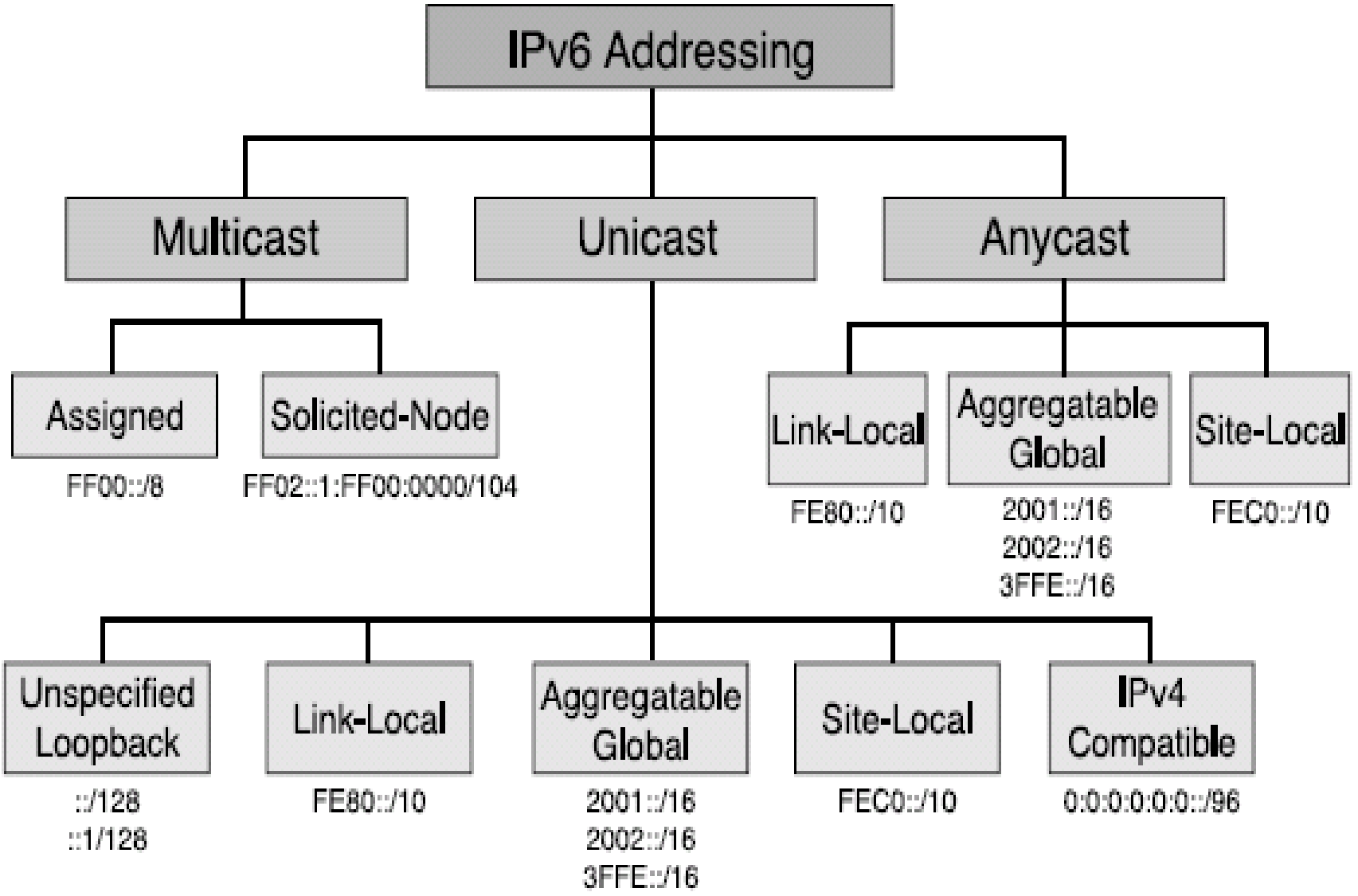
PF = 1111 1110 10 : Link Local Use Addresses (FE80::/10)

PF = 1111 1110 11 : Site Local Use Addresses (FEC)::/10)

PF = 1111 1111 : Multicast Addresses (FF00::/8)

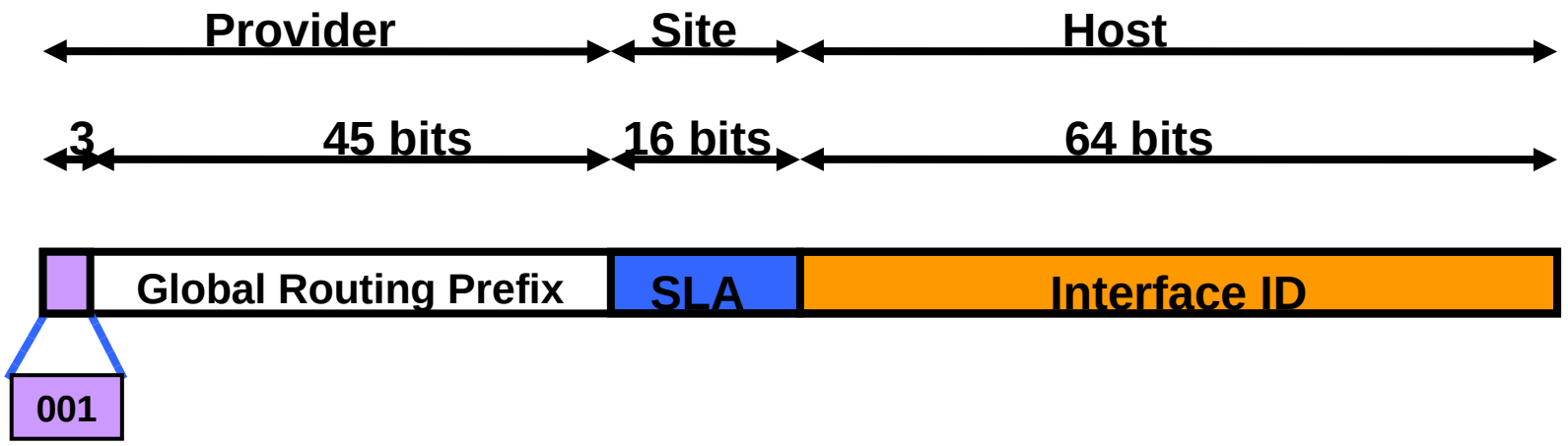
Other values are currently Unassigned (approx. 7/8th of total)

All Prefix Formats have to support EUI-64 bits Interface ID setting

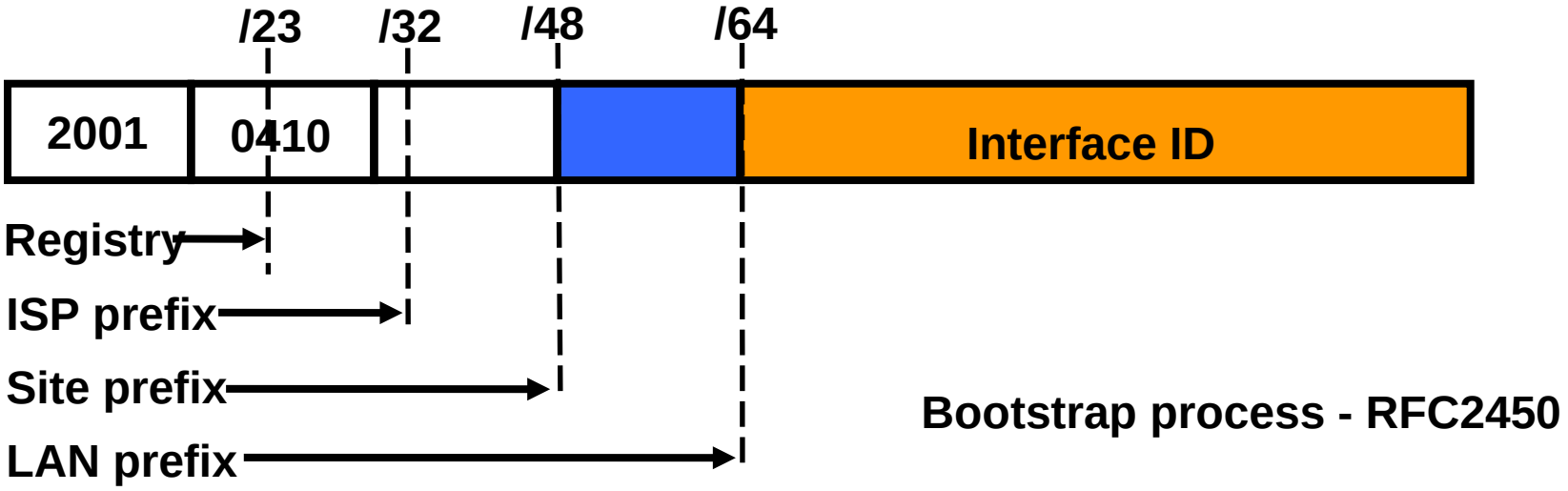

IPv6 Addressing
Multicast
Unicast
Anycast
Assigned
FF00::/8
Solicited-Node
FF02::1:FF00:0000/104
Link-Local
FE80::/10
Aggregatable Global
2001::/16
2002::/16
3FFE::/16
Site-Local
FEC0::/10
Unspecified Loopback
::/128
::1/128
Link-Local
FE80::/10
Aggregatable Global
2001::/16
2002::/16
3FFE::/16
Site-Local
FEC0::/10
IPv4 Compatible
0:0:0:0:0:0::/96

Aggregatable Global Unicast Addresses

- Aggregatable Global Unicast addresses are:
  - This address type is equivalent to IPv4's public address.
  - Global Unicast addresses in IPv6 are globally identifiable and uniquely addressable (Addresses for generic use of IPv6)
  - Structured as a hierarchy to keep the aggregation
- Ref RFC 3513



Address Allocation Policy



Bootstrap process - RFC2450

Scope of IPv6 Unicast Addresses

The scope of Link-local address is limited to the segment.

Unique Local Address are locally global, but are not routed over the Internet, limiting their scope to an organization’s boundary.

Global Unicast addresses are globally unique and recognizable. They shall make the essence of Internet v2 addressing.

IPv6 Unicast Address Scopes

Three types of scopes:

1. **Link-local scope**

   Identifies all hosts within a single layer 2 domain.

   Called as link-local addresses

2. **Unique-local scope**

   Identifies all devices reachable within an administrative site or domain typically contains multiple distinct links.

   Called as unique-local addresses (ULAs)

3. **Global scope**

   Identifies all devices reachable across the Internet.

   Called as global unicast addresses (GUAs)

Local-Use Unicast Addresses

There are two types of local-use unicast addresses:

1. **Link-local addresses**

   used between on-link neighbors and for Neighbor Discovery Processes

   required for Neighbor Discovery (NDP) processes and is always automatically configured, even in the absence of all other unicast addresses

2. **Site-local addresses** (now deprecated)

   used between nodes communicating with other nodes in the same site.

   Site local addresses have been deprecated.

   Site local addresses would cause conflicts when setting up VPNs between networks and when merging networks.

   Unique local addresses make sure that each network uses different addresses so that linking and merging won't be a problem.

Link-local Unicast Address

Used only between nodes connected on the same local link.

When an IPv6 stack is enabled on a node, one link-local address is automatically assigned to each interface of the node at boot time.

Link-local addresses are only for local-link scope and must never be routed between subnets within a site.

A node having an aggregatable global unicast address on a local link uses the link-local address of its default IPv6 router rather than the router's aggregatable global unicast address.

If the unicast aggregatable global prefix is changed, the default router can always be reached using the link-local address.

Link-local addresses of nodes and routers do not change during network renumbering.

Unique-Local Address

IPv6 Unique Local addresses are the addresses which can be used inside an enterprise company at multiple sites

Defined in IETF RFC 4193

Globally unique and is intended for IPV6 local communications

Not routable over the Internet, but routable within multiple sites of the enterprise

Reserved with a range of FC00::/7

If the value of single binary bit "L" is set to 1, the Unique local IPv6 multicast address is locally assigned.

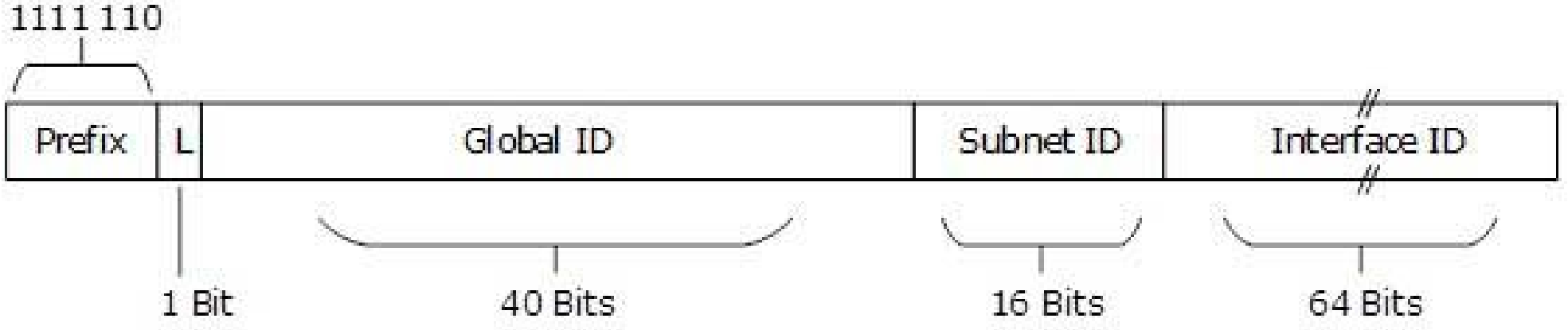
The value 0 may be defined in the future.

Link-Local Address

- Auto-configured IPv6 address is known as Link-Local address
- Always starts with FE80 (first 16 bits)
- The next 48-bits are set to 0

Unique-Local Address

- Globally unique, should be used in local communication
- The second half of this address contain Interface ID and the first half is divided among Prefix, Local Bit, Global ID and Subnet ID.



Note on IPv6 link-local vs unique local

Link local addresses are present on all interfaces and are used for many essential link protocols such as neighbor discovery, duplicate address detection and router advertisement.

Unique local addresses are the replacement for the deprecated site local address scope. ULA addresses are similar in use to RFC1918 addresses in the IPv4 world, and allow an organisation to number internal resources within their administrative domain with addresses that are unique, but not tied to routing policy, easing the pain if a change of ISP means that renumbering is required. Remember that with IPv6 there is no NAT, so you cannot simply rewrite at the border onto your ISPs address space

Site-Local Address (deprecated)

Site-local addresses are equivalent to the IPv4 private address space (10.0.0.0/8, 172.16.0.0/12, and 192.168.0.0/16).

Private intranets that do not have a direct, routed connection to the IPv6 Internet can use site-local addresses without conflicting with global unicast addresses.

Site-local addresses are not reachable from other sites, and routers must not forward site-local traffic outside the site.

Site-local addresses can be used in addition to global unicast addresses.

The scope of a site-local address is the site.

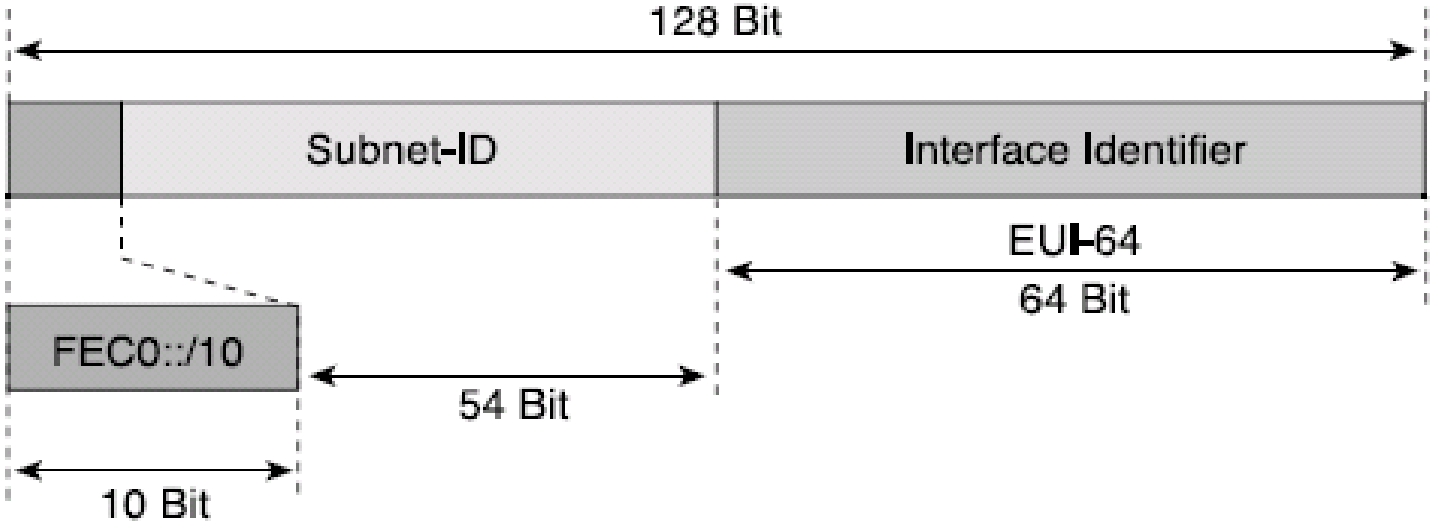
A site is an organization network or portion of an organization's network that has a defined geographical location (such as an office, an office complex, or a campus).

Site-Local Address (deprecated)

Not automatically configured

Must be assigned either through stateless or stateful address configuration processes.

May be assigned to any nodes and routers within a site.



Interface IDs

- Lowest-order 64-bit field of unicast address may be assigned in several different ways:
  - auto-configured from a 64-bit EUI-64, or expanded from a 48-bit MAC address (e.g., Ethernet address)
  - auto-generated pseudo-random number (to address privacy concerns)
  - assigned via DHCP
  - manually configured

Special IPv6 Addresses

The following are special IPv6 addresses:

Unspecified address

unspecified address (0:0:0:0:0:0:0:0 or ::) is only used to indicate the absence of an address.

equivalent to the IPv4 unspecified address of 0.0.0.0.

used as a source address for packets attempting to verify the uniqueness of a tentative address.

never assigned to an interface or used as a destination address.

Loopback address

The loopback address (0:0:0:0:0:0:0:1 or ::1) is used to identify a loopback interface, enabling a node to send packets to itself.

It is equivalent to the IPv4 loopback address of 127.0.0.1.

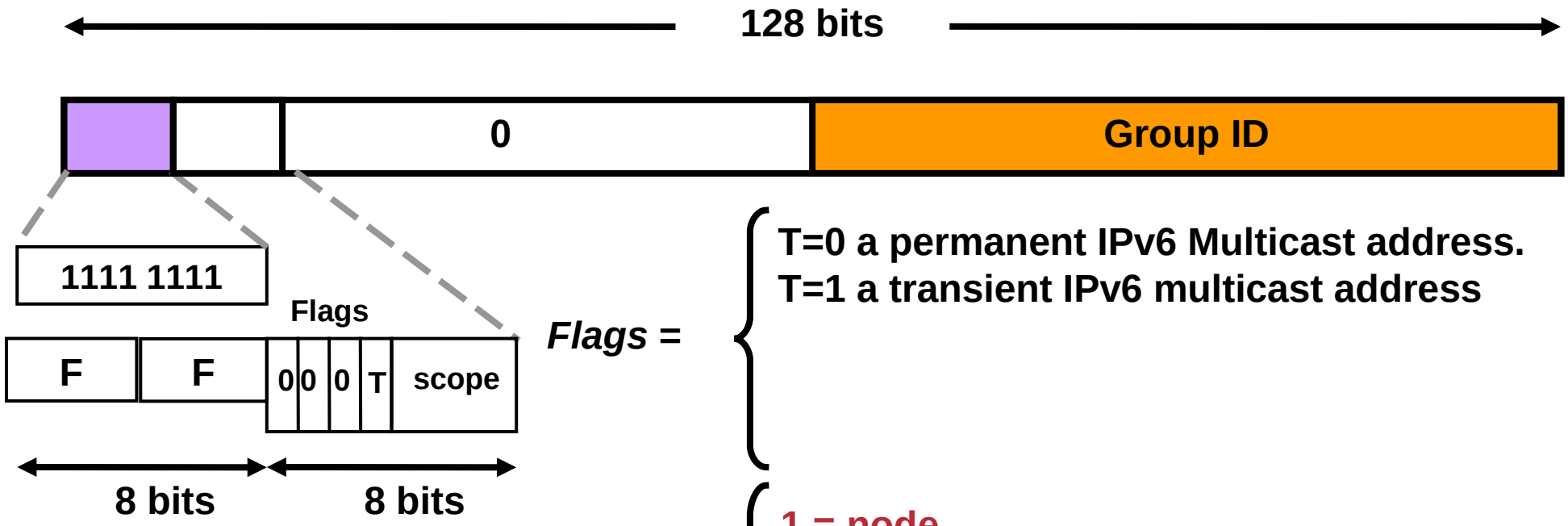
Packets addressed to the loopback address must never be sent on a link or forwarded by an IPv6 router.

Multicast Addresses

IPv6 makes heavy use of multicast addresses in the mechanisms of the protocol such as

- The replacement of Address Resolution Protocol (ARP) in IPv4
- Prefix advertisement
- Duplicate Address Detection (DAD)
- Prefix renumbering.

Expanded Address Space Multicast Addresses (RFC 3513)



IPv6 Addresses for a Host

An IPv4 host with a single network adapter typically has a single IPv4 address assigned to that adapter.

An IPv6 host, however, usually has multiple IPv6 addresses - even with a single interface.

An IPv6 host is assigned with the following unicast addresses:

1. A link-local address for each interface
2. Unicast addresses for each interface (which could be a site-local address and one or multiple global unicast addresses)
3. The loopback address (::1) for the loopback interface

IPv6 Addresses for a Router

An IPv6 router is assigned the following unicast addresses:

- A link-local address for each interface
- Unicast addresses for each interface (which could be a site-local address and one or multiple global unicast addresses)
- A Subnet-Router anycast address
- Additional anycast addresses (optional)
- The loopback address (::1) for the loopback interface

Anycast Addresses

An anycast address is an address allocated to a set of interfaces that typically belong to different routers.

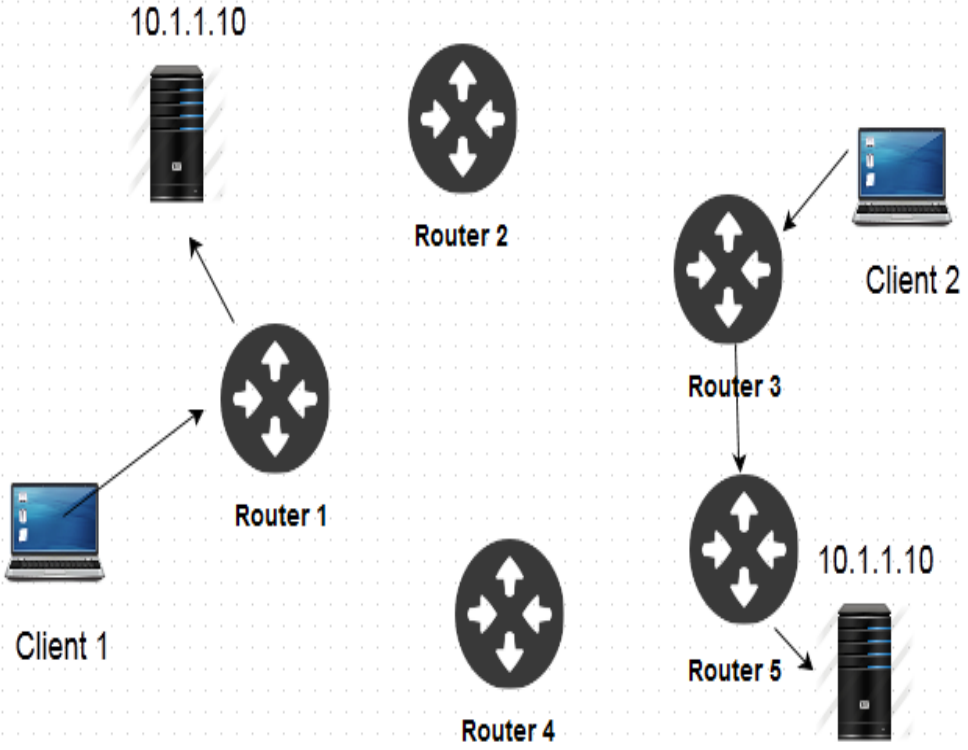
When a packet is destined to an anycast address, it is delivered to the closest interface that has this anycast address

The term “closest” is determined by the routing protocol.

An anycast address must be assigned to a router not a host and cannot be used as a source address.

One example of an anycast address is the subnet-router anycast address. This address format is formed by a subnet prefix of n bits that identifies a specific link followed by 128-n bits all set to 0. So in this example, a packet sent to the subnet-router anycast address is delivered to one of the routers on that subnet link.

Anycast Addresses



- Primarily used for DNS
- Not suitable for TCP and connection oriented stuff
- Although, nowadays there are some uses of Anycast addresses with HTTP protocols

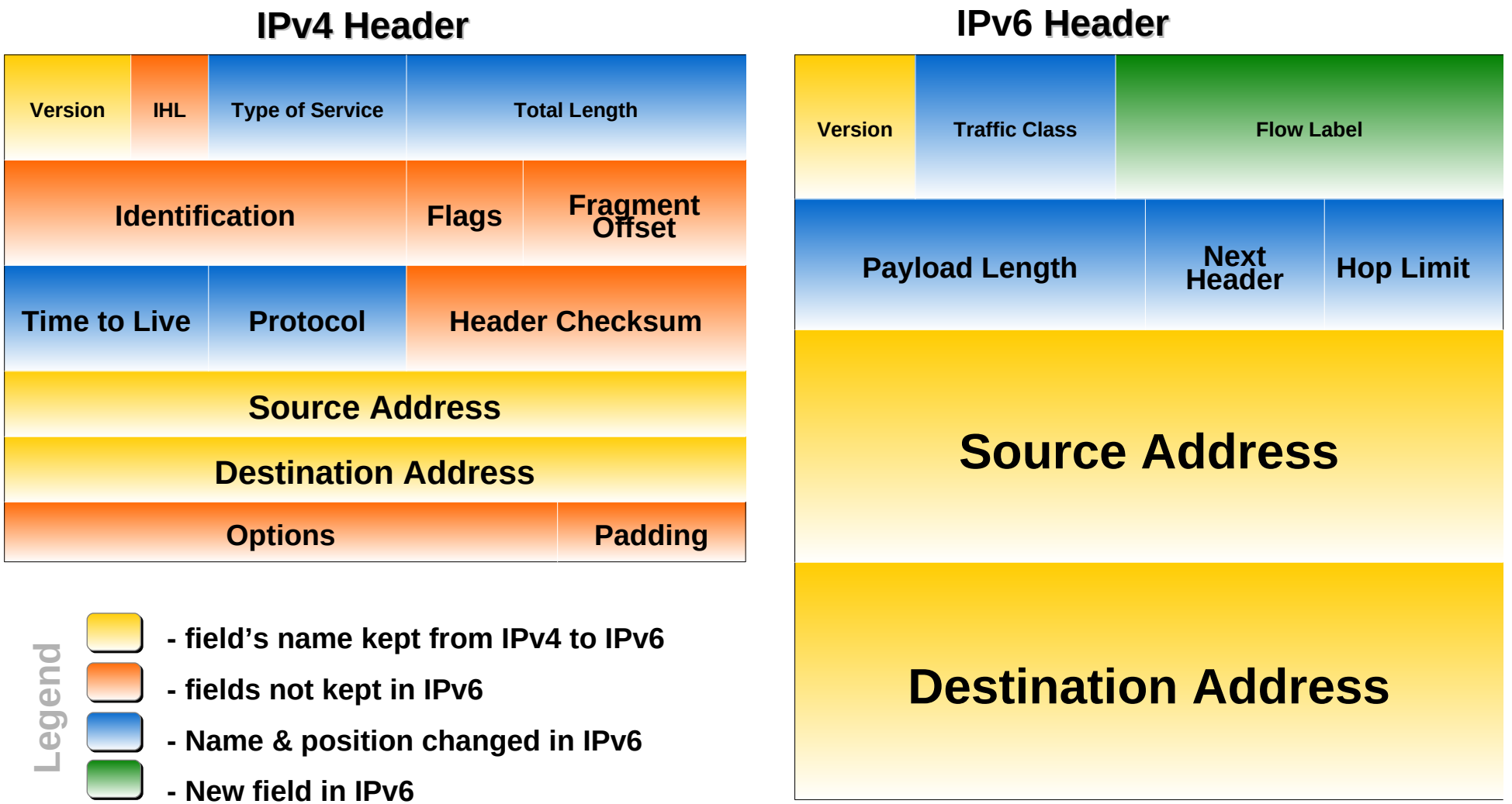
Advantages:

1.reduce latency in response

2.Higher service uptime

3.Better resistance against Distributed Denial Of Service Attacks

IPv4 & IPv6 Header Comparison



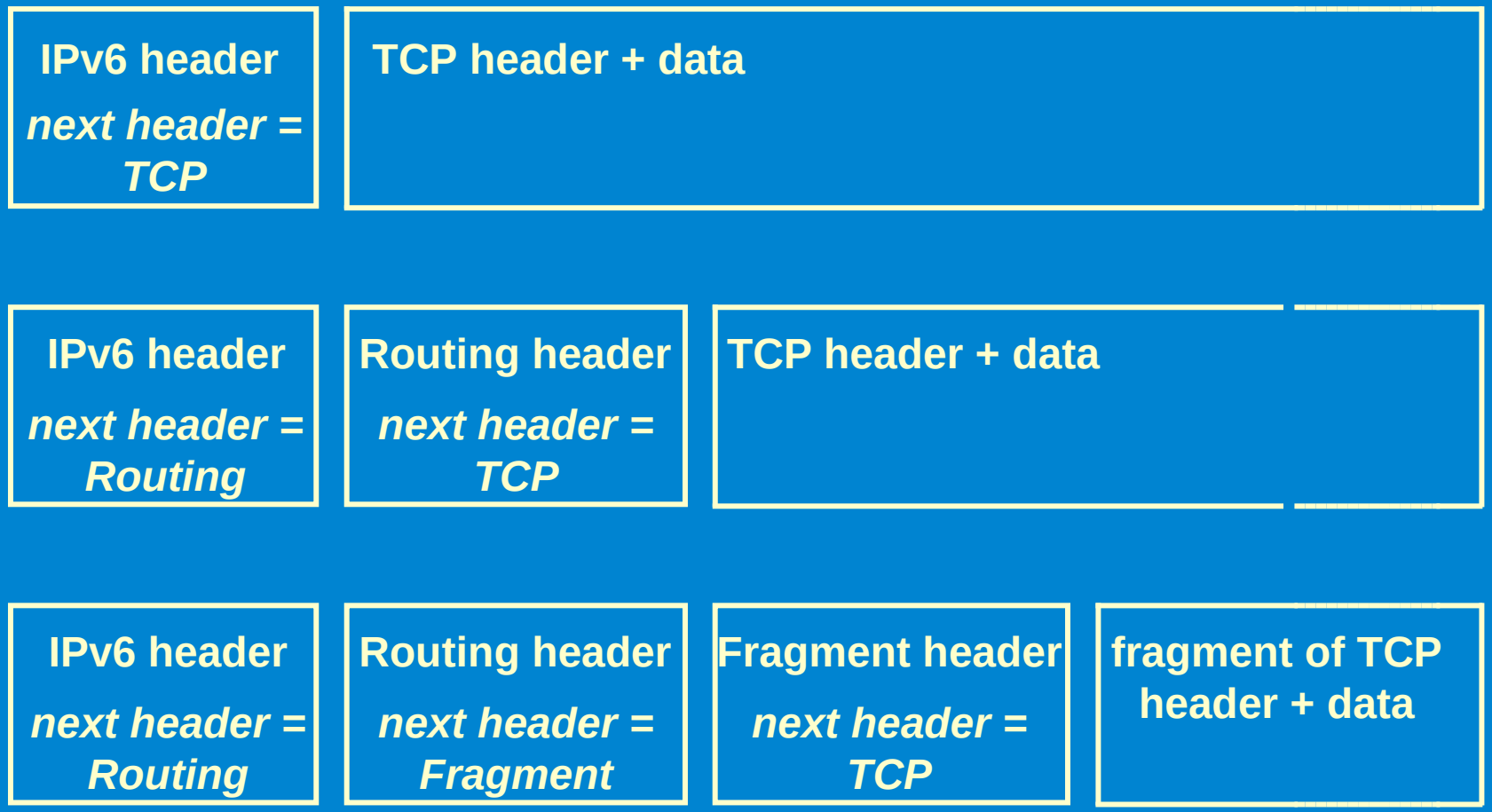
IPv4 & IPv6 Header Comparison

- 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
  - Alignment changed from 32 to 64 bits
- Revised
  - Time to Live -> Hop Limit
  - Protocol -> Next Header
  - Precedence & TOS -> Traffic Class
    - indicates the IPv6 packet’s class or priority
  - Addresses increased from 32 bits -> 128 bits

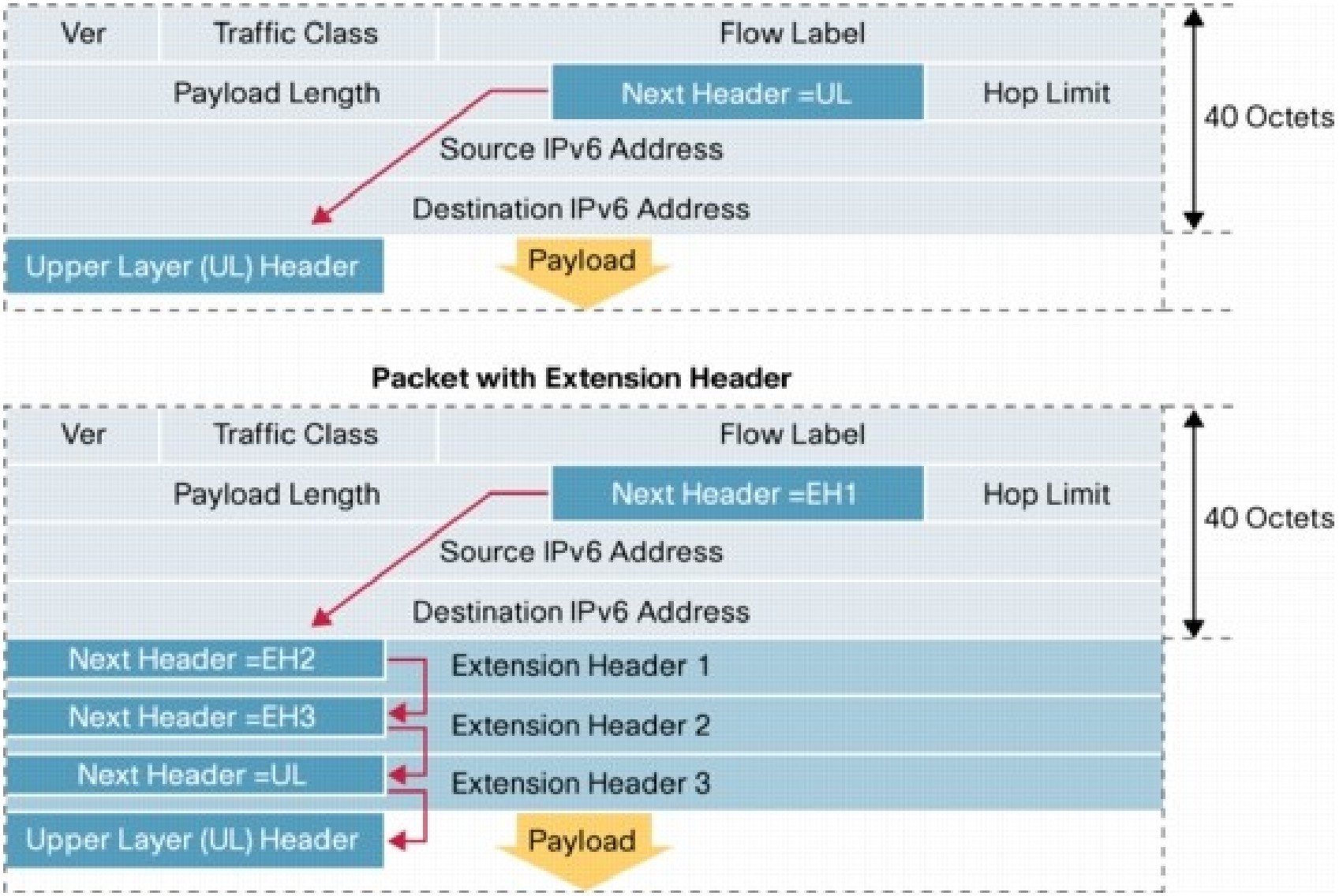
IPv4 & IPv6 Header Comparison

- Extended
  - Flow Label field added - indicates that this packet belongs to a specific sequence of packets between a source and destination
  - can be used for prioritized delivery of packets for services like voice.

Extension Headers



Chaining Extension Headers in IPv6 Packets



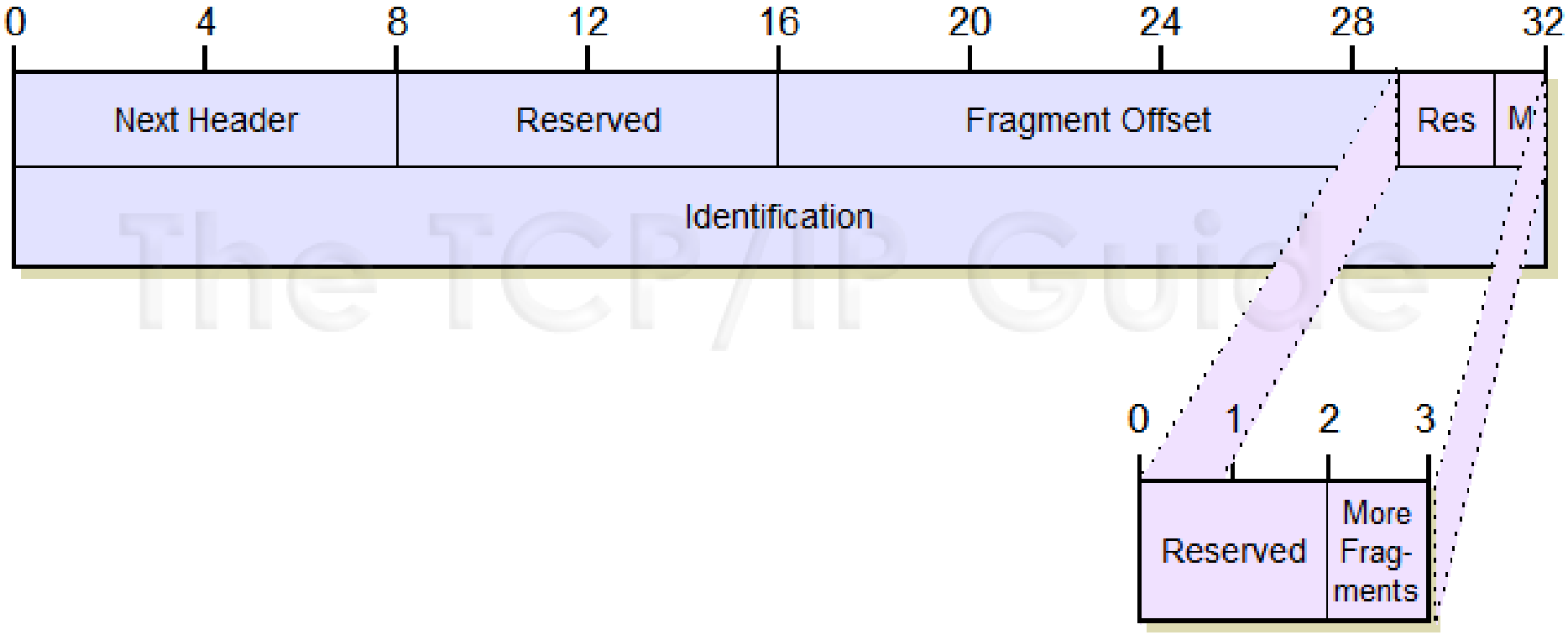
Extension Headers (cont.)

- Generally processed only by node identified in IPv6 Destination Address field
  - much lower overhead than IPv4 options processing
  - exception: Hop-by-Hop Options header
- Eliminates IPv4's 40-byte limit on options
  - in IPv6, limit is total packet size, or Path MTU in some cases
- Currently defined extension headers:
  - Hop-by-Hop Options, Routing, Fragment, Authentication, Encryption, Destination Options

Fragment Header

- In order to send a packet larger than the PMTU, an IPv6 node may fragment a packet at the source and have it reassembled at the destination
- In IPv6, only hosts can fragment
- In IPv4, both hosts and routers can fragment
- IPv6 fragment & reassembly is an end-to-end function
- IPv6 Fragmentation has always been discouraged
  - Reassembly is computationally expensive and inefficient
  - Security concerns
- Routers do not fragment packets en-route if too big—they send ICMP “packet too big” instead

Fragment Header



Fragment

Fragment Header

Next Header: Contains the protocol number of the next header after the Fragment header

Reserved: Not used; set to zeros

Fragment Offset: Specifies the offset, or position, in the overall message where the data in this fragment goes (specified in units of 8 bytes (64 bits)

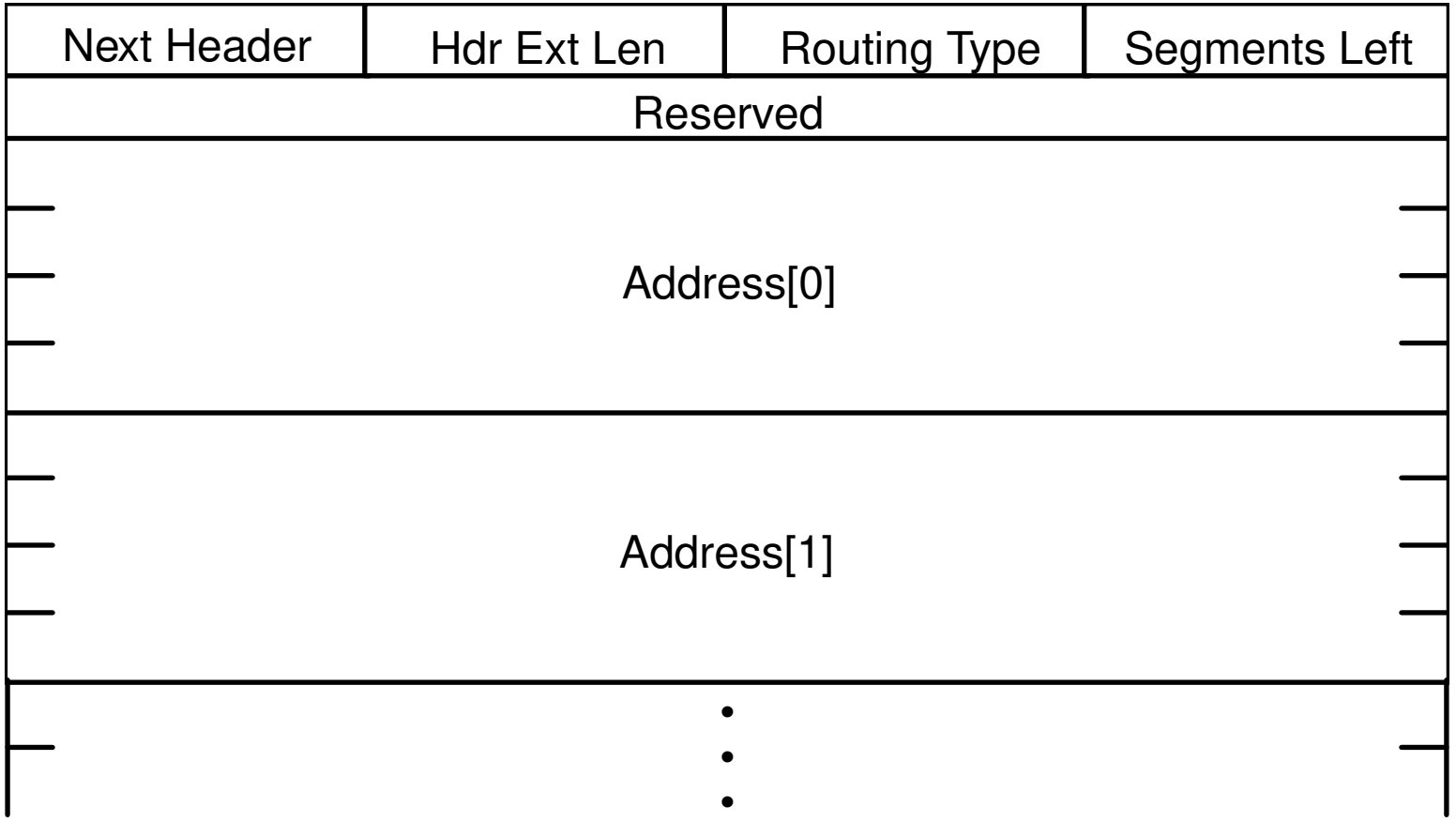
M Flag: when set to 0, indicates the last fragment in a message; when set to 1, indicates that more fragments are yet to come in the fragmented message

Identification: expanded to 32 bits. Contains a specific value that is common to each of the fragments belonging to a particular message, to ensure that pieces from different fragmented messages are not mixed together.

Routing Header

- Same “longest-prefix match” routing as IPv4 CIDR
- Straightforward changes to existing IPv4 routing protocols to handle bigger addresses
  - unicast: OSPF, RIP-II, IS-IS, BGP4+, …
  - multicast: MOSPF, PIM, …
- Use of Routing header with anycast addresses allows routing packets through particular regions
  - e.g., for provider selection, policy, performance, etc.

Routing Header



Routing Header

Hdr Ext Len: 8-bit unsigned integer. Length of the Routing header

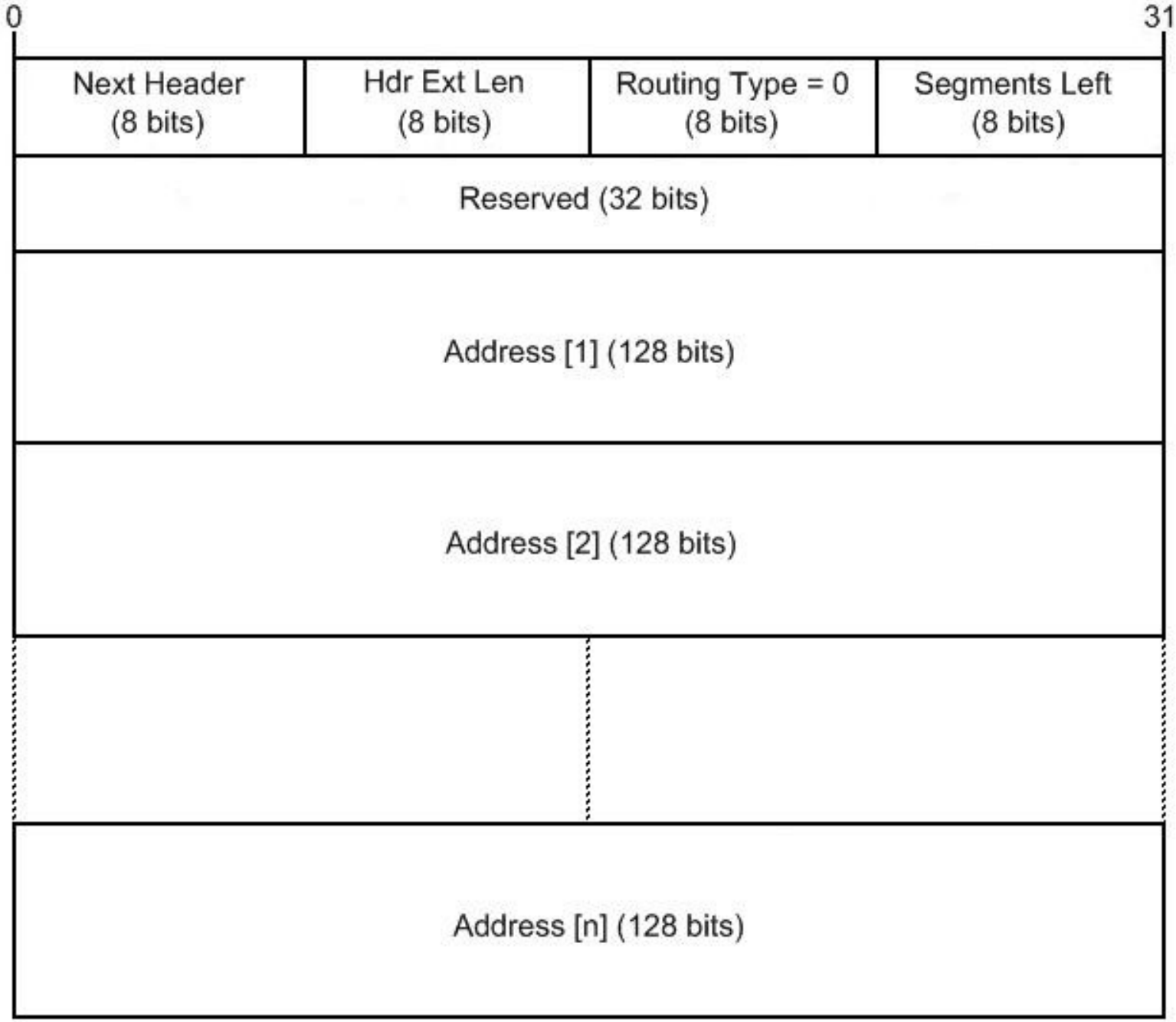
Routing Type: 8-bit identifier of a particular Routing header variant

Segments Left: Number of explicitly listed intermediate nodes still to be visited before reaching the final destination.

Type-specific data: Variable-length field, of format determined by the Routing Type, and of length such that the complete Routing header is an integer multiple of 8 octets long

Type 0 Routing header

- Used by an IPv6 source to list one or more intermediate nodes to be "visited" on the way to a packet's destination
- The IPv6 Type 0 Routing header is similar in function to the IPv4 (RFC 791) “Loose Source and Record Route” IP options.


0
31
Next Header
(8 bits)
Hdr Ext Len
(8 bits)
Routing Type = 0
(8 bits)
Segments Left
(8 bits)
Reserved (32 bits)
Address [1] (128 bits)
Address [2] (128 bits)
Address [n] (128 bits)

Type 0 Routing header

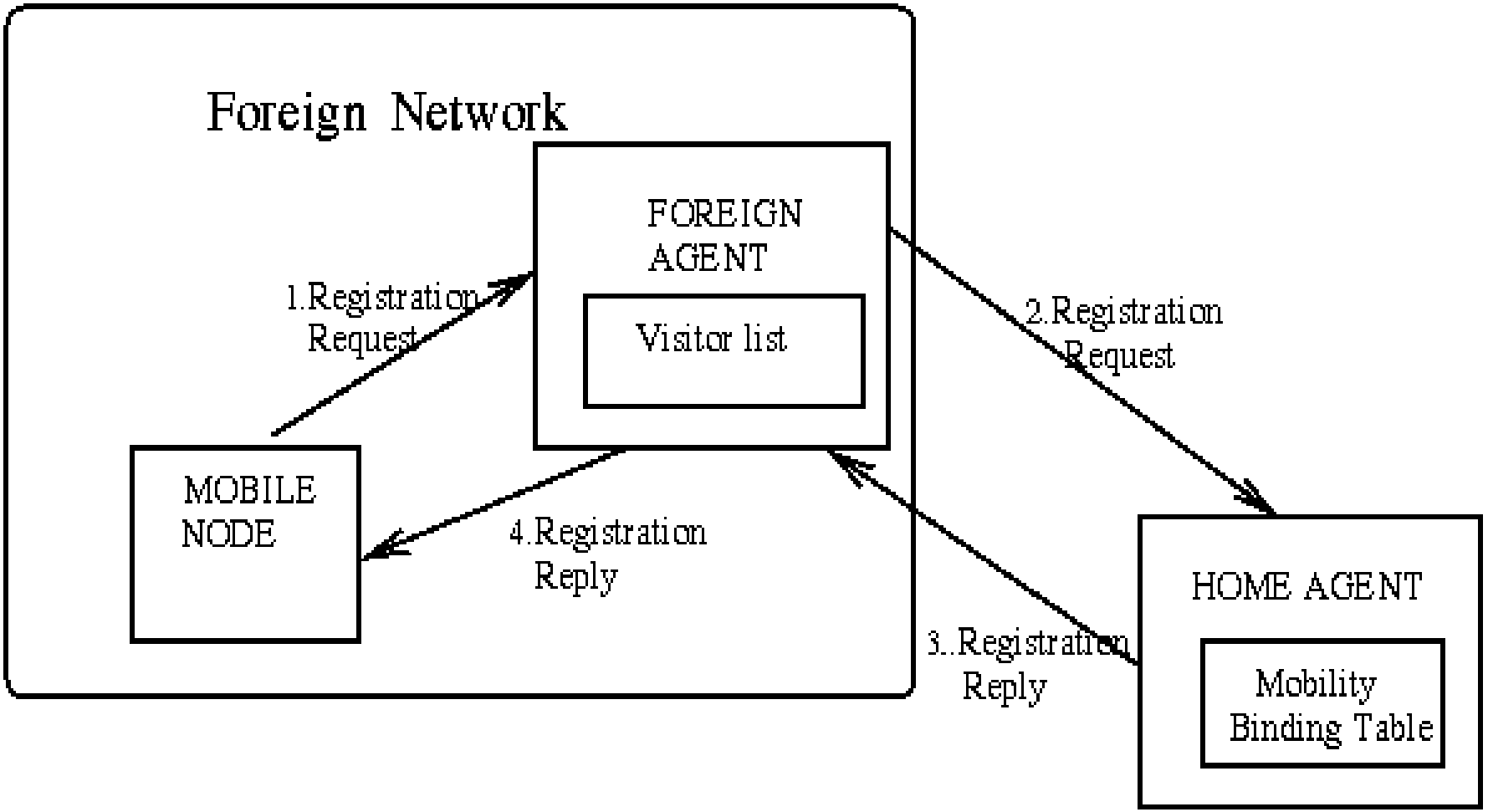
The functionality provided by IPv6's Type 0 Routing Header can be exploited in order to achieve traffic amplification over a remote path for the purposes of generating denial-of-service traffic.

RFC 5095 updates the IPv6 specification to deprecate the use of IPv6 Type 0 Routing Headers, in light of this security concern.

Other extension headers

- Authentication – Integrity and authentication, security
- Encapsulation – Confidentiality
- Hop-by-Hop Option – Special options that require hop-by-hop processing
- Destination Options – Optional information to be examined by the destination node
- Mobility Header is a newly defined Extension Header
  - It is an extension header used by mobile nodes, correspondent nodes and home agents in all messaging related to the creation and management of bindings.

Mobile IP (before IPv6)



Mobility in IPv6

- The base IPv6 was designed to support Mobility - Mobility is not an “Add-on” features
  - All IPv6 Networks are IPv6-Mobile Ready
  - All IPv6 nodes are IPv6-Mobile Ready
  - All IPv6 LANs/Subnets are IPv6 Mobile Ready
- Route Optimization is a fundamental goal of Mobile IPv6
- Foreign Agents are not needed in Mobile IPv6
  - MNs can function at any location without the services of any special router in that location
- Security
  - Nodes are expected to employ strong authentication and encryption

Mobility in IPv6

- When the mobile node is away from home it acquires a care-of address through the use of "Address Autoconfiguration"
- There may be more than one care-of addresses, such as when it is moving but still reachable at the previous link.
- The association between a mobile node's home address and care-of-address is known as a "binding" for the mobile node.
- While away from home, a mobile node registers its primary care-of address with a router on its home link
- This router functions as the "home agent" for the mobile node.

Mobility in IPv6

- The home agent defends the mobile node’s addresses

(in case another node configures an address that collides with a mobile node’s home address (or addresses))

- Mobile IPv6 specification prohibits the home agent from tunneling packets addressed to the mobile node’s link-local address
- Site-local addresses SHOULD NOT be used as home or care-of addresses
- The mobile node performs binding registration by sending a "Binding Update" message to the home agent.
- The home agent replies to the mobile node by returning a "Binding Acknowledgement" message.

Mobility in IPv6

- Two possible modes for communications between Mobile Node (MN) and Correspondent Node (CN)

  1. Bidirectional tunneling

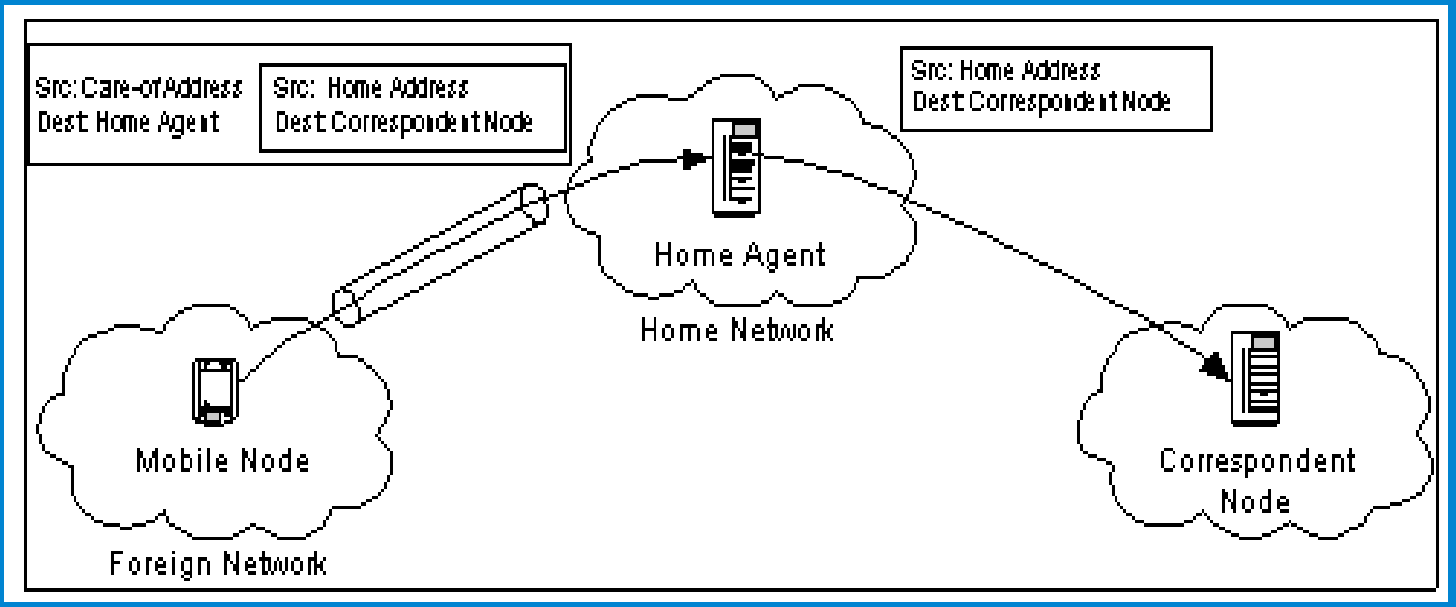
  -(does not require Mobile IPv6 support from the CN)

  -available even if the mobile node has not registered its current binding with the CN

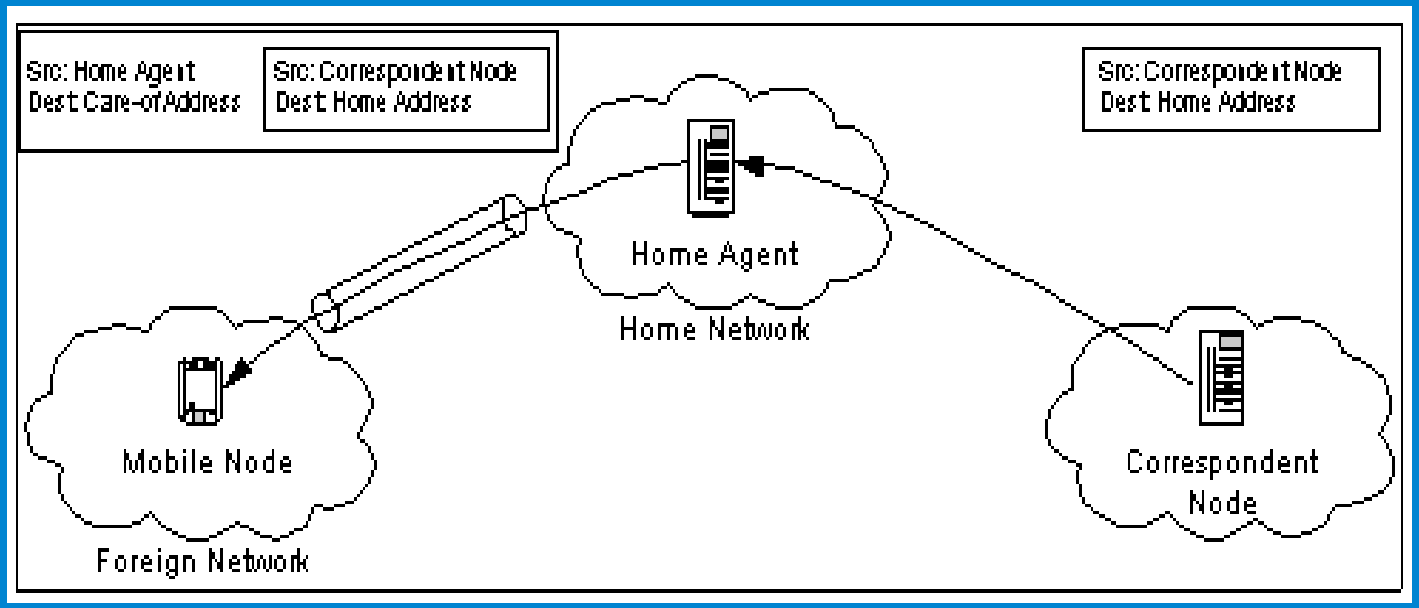
  -Packets from the CN are routed to the home agent and then tunneled to the MN.

  -Packets to the CN are tunneled from the MN to the home agent ("reverse tunneled") and then to the CN

  -The home agent uses proxy Neighbor Discovery



Data Path: Mobile Node to Correspondent Node in Basic Operation



Data Path: Correspondent Node to Mobile Node in Basic Operation

Mobility in IPv6

- Two possible modes for communications between MN and CN

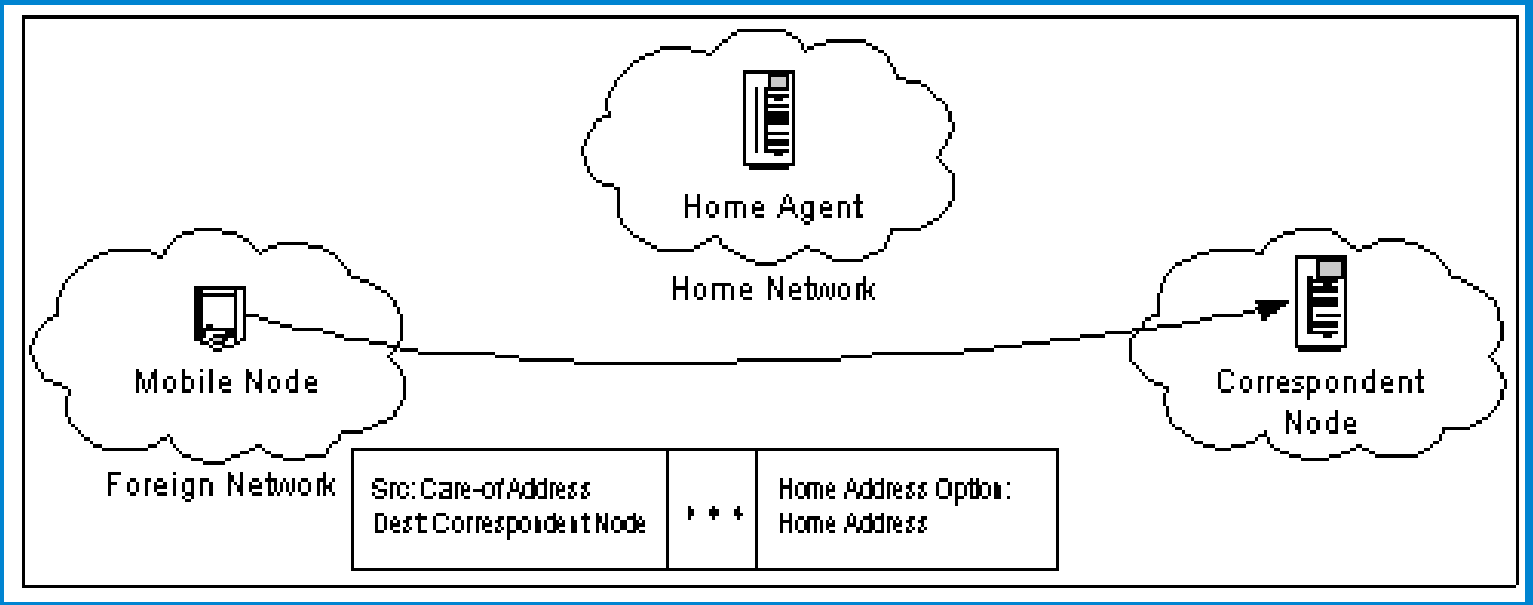
  2. Route optimization

  -The MN registers its current binding at the CN

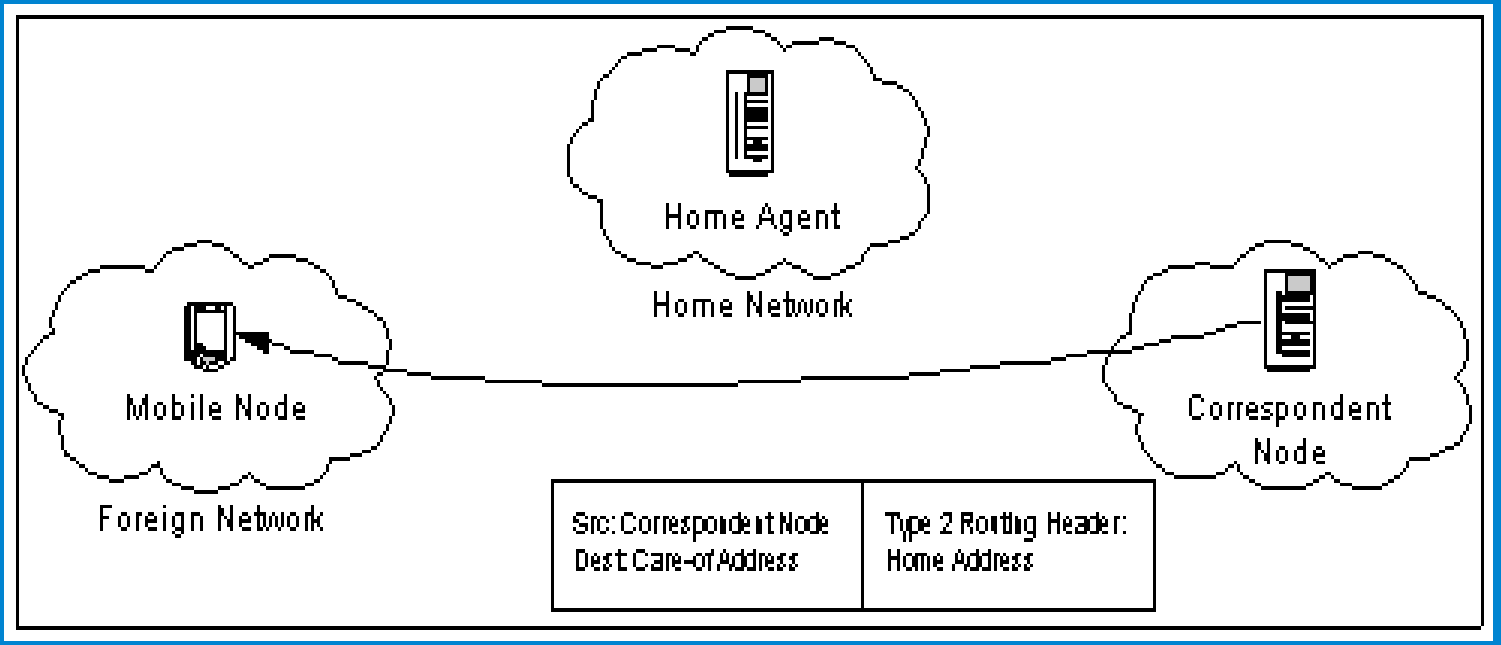
  -Packets from the CN can be routed directly to the care-of address of the MN

  -When sending a packet to any IPv6 destination, the CN checks its cached bindings for an entry for the packet's destination address

  -If a cached binding for this destination address is found, the node uses a type 2 IPv6 routing header (a type of extension header) to route the packet to the MN using the address indicated in this binding

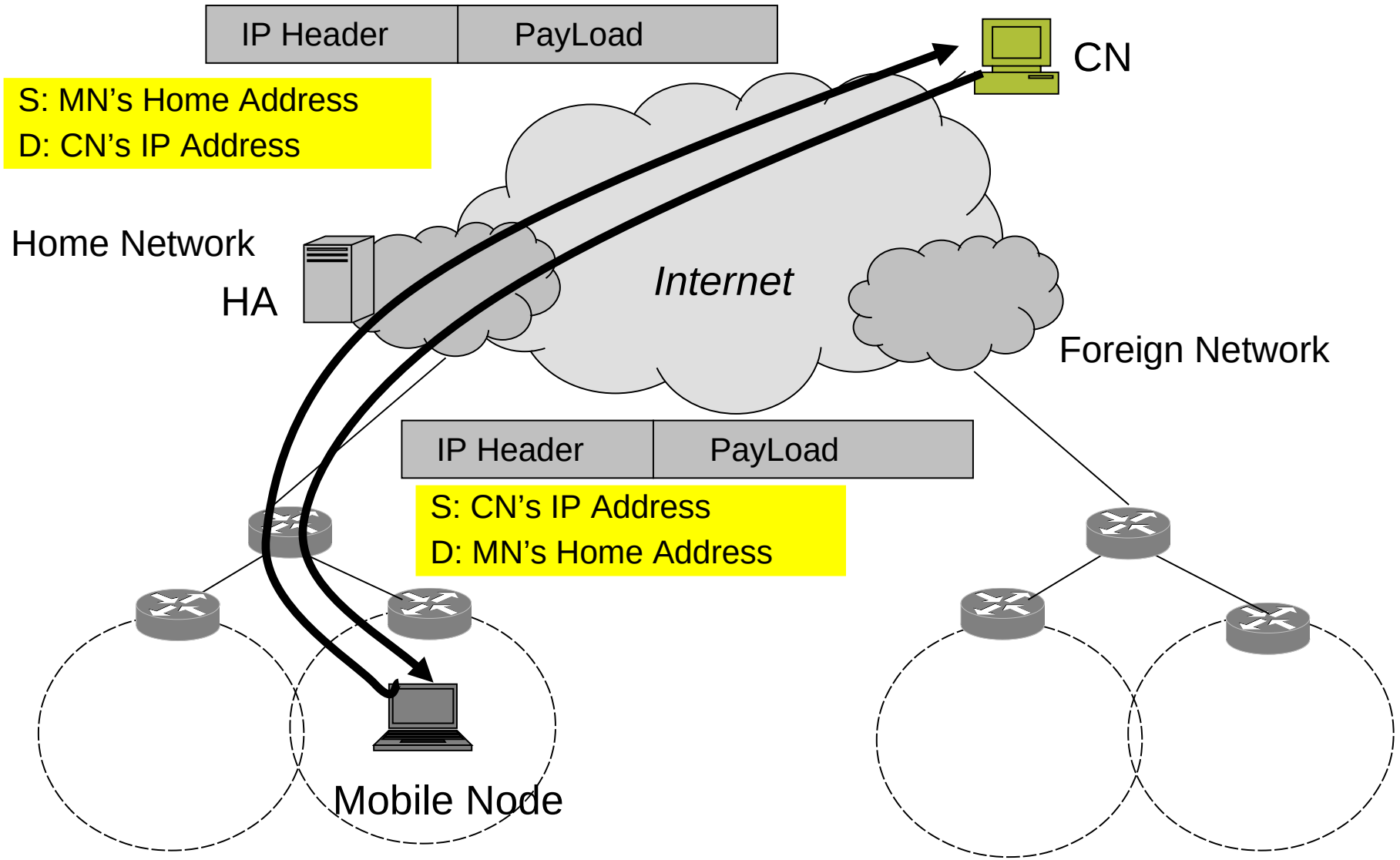


Data Path: Mobile Node to Correspondent Node in Route Optimization

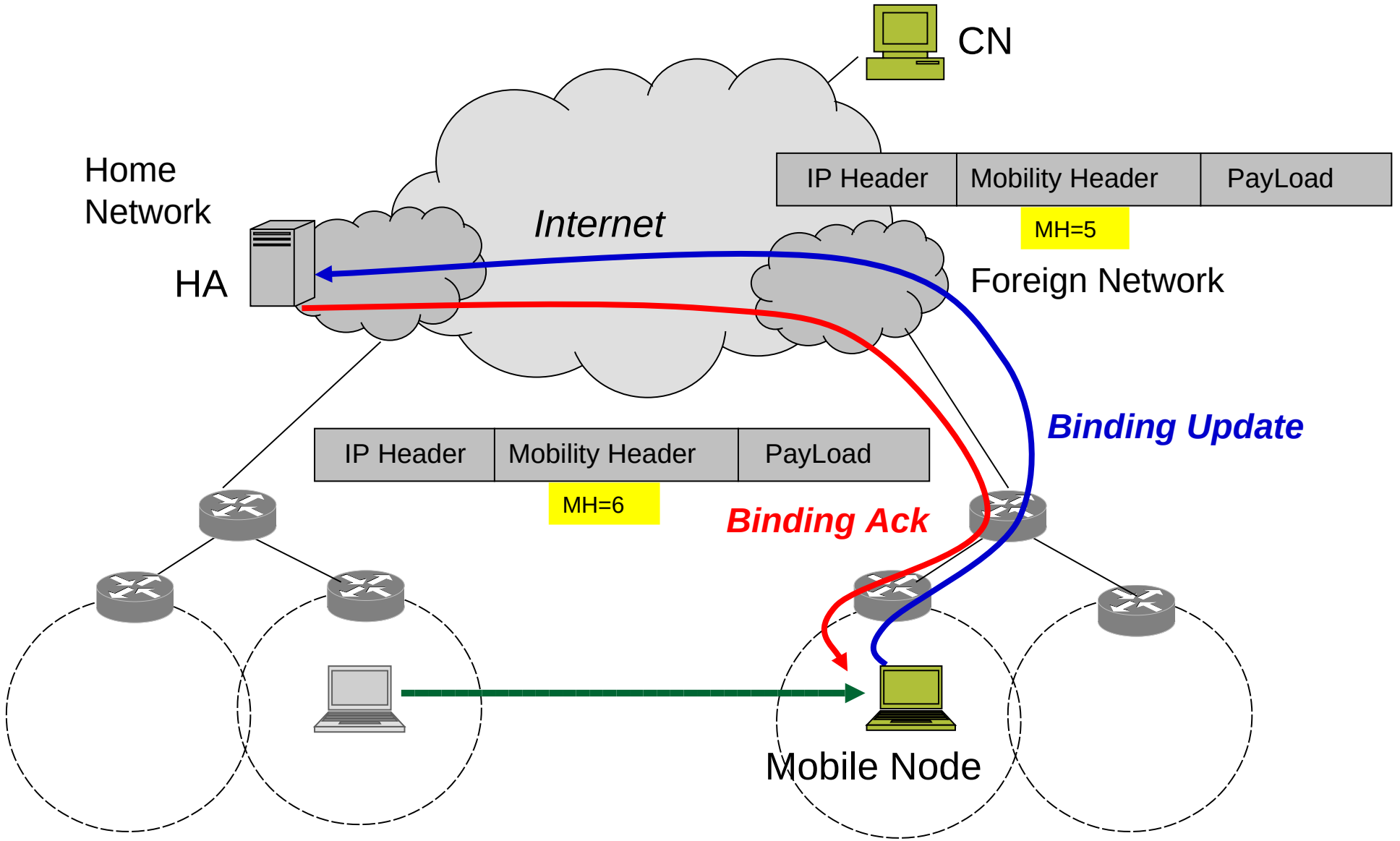


Data Path: Correspondent Node to Mobile Node in Route Optimization

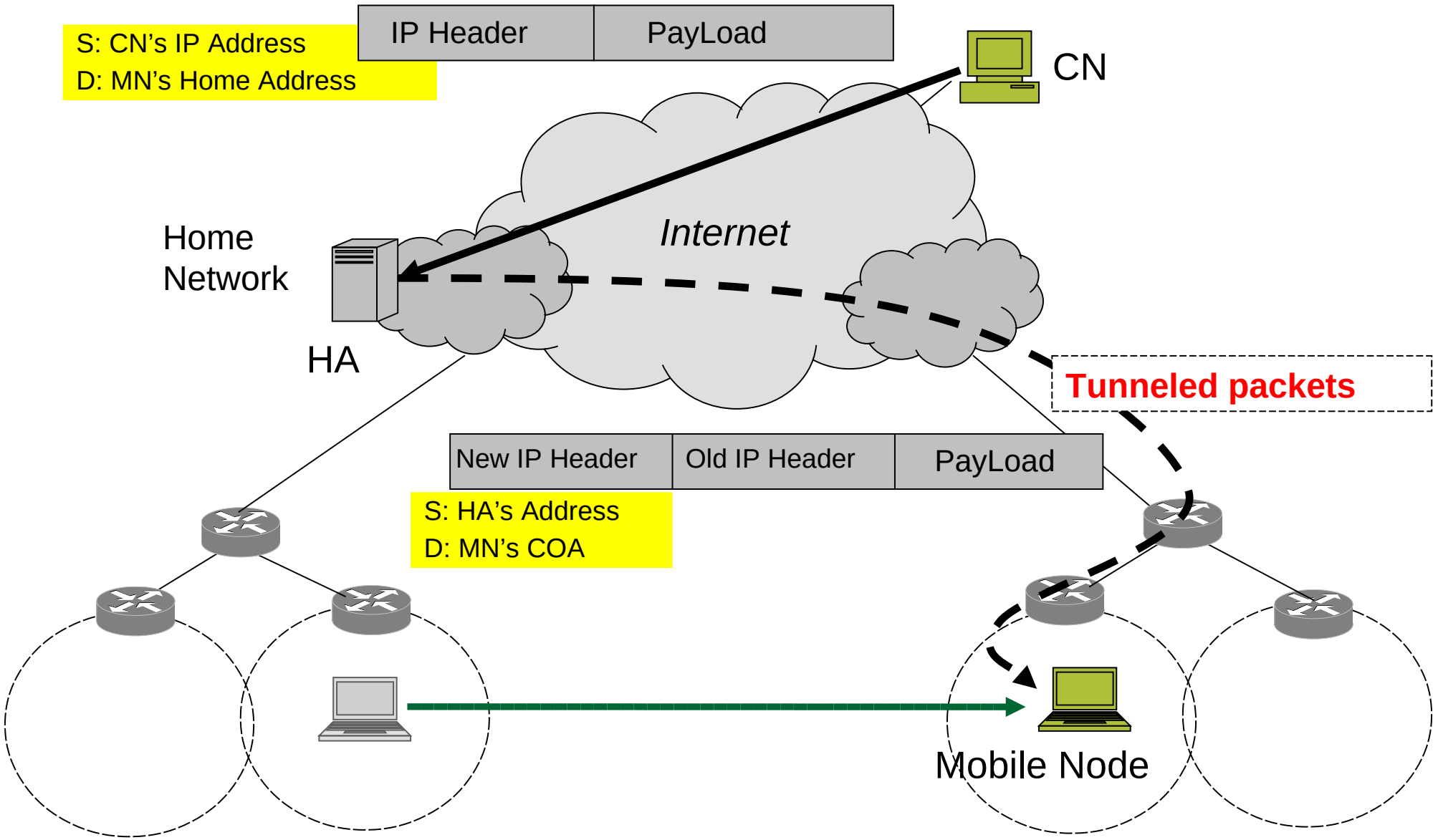
MIPv6 Basic Operation (1)



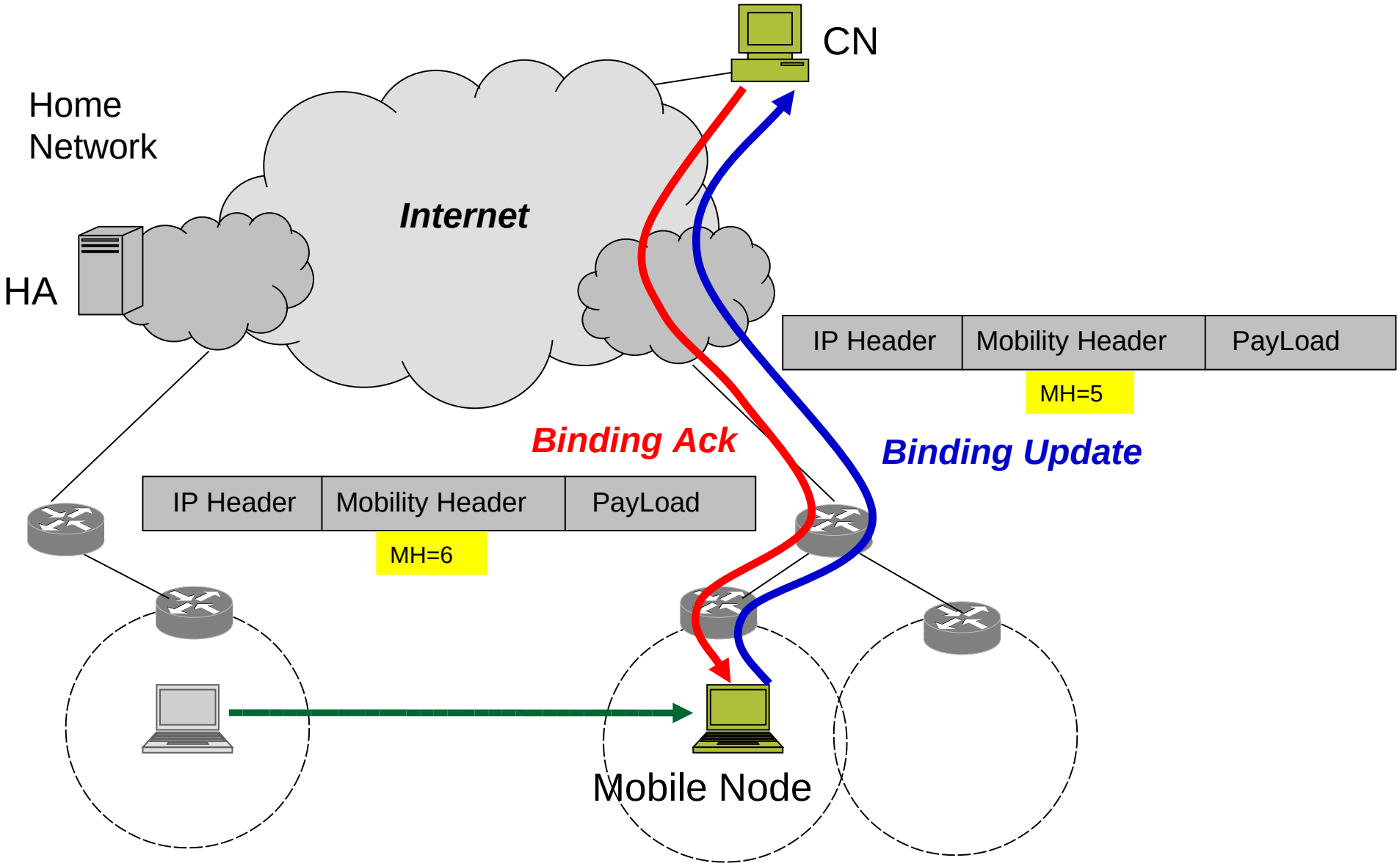
MIPv6 Basic Operation (2)



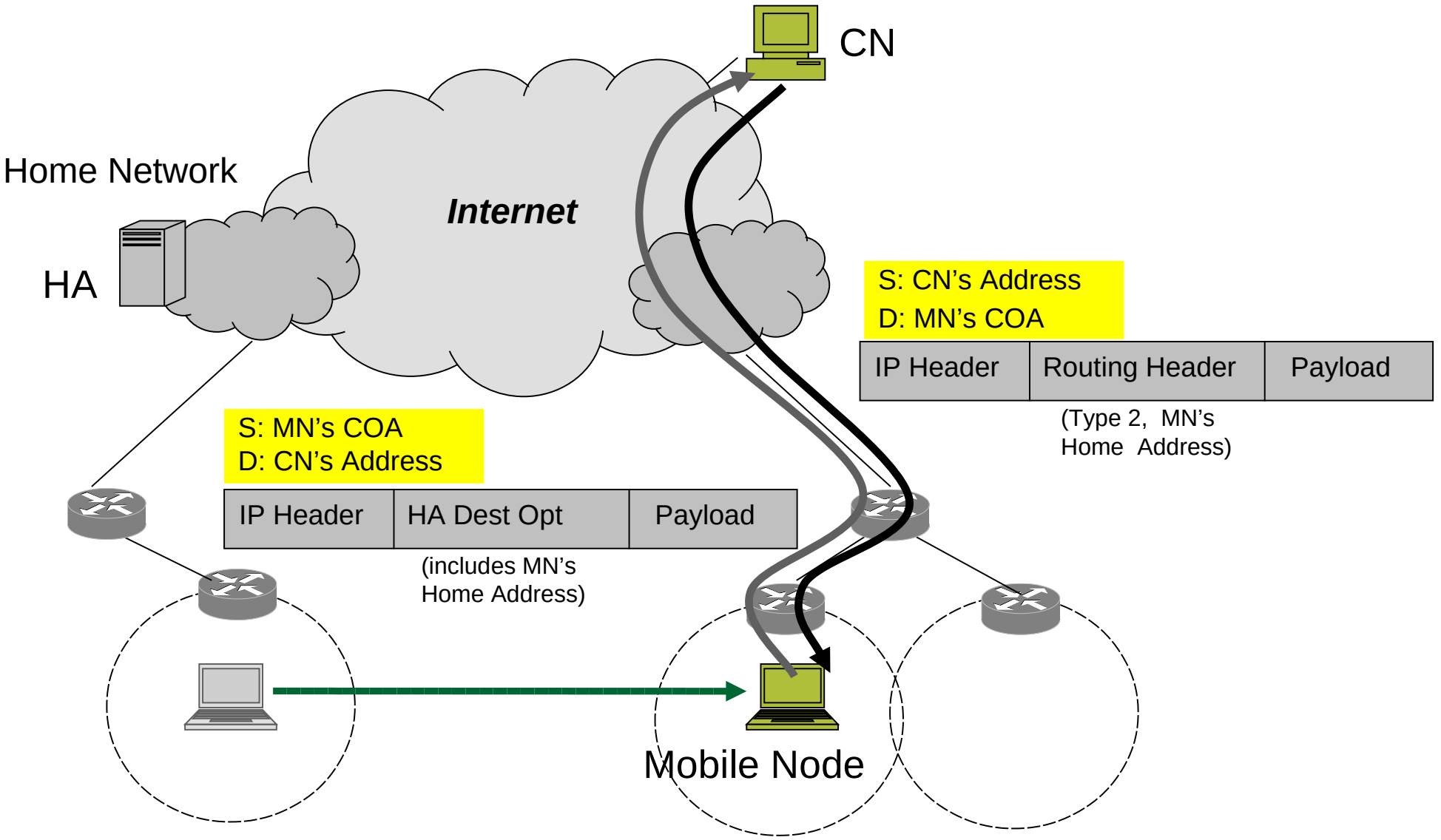
MIPv6 Basic Operation (3)

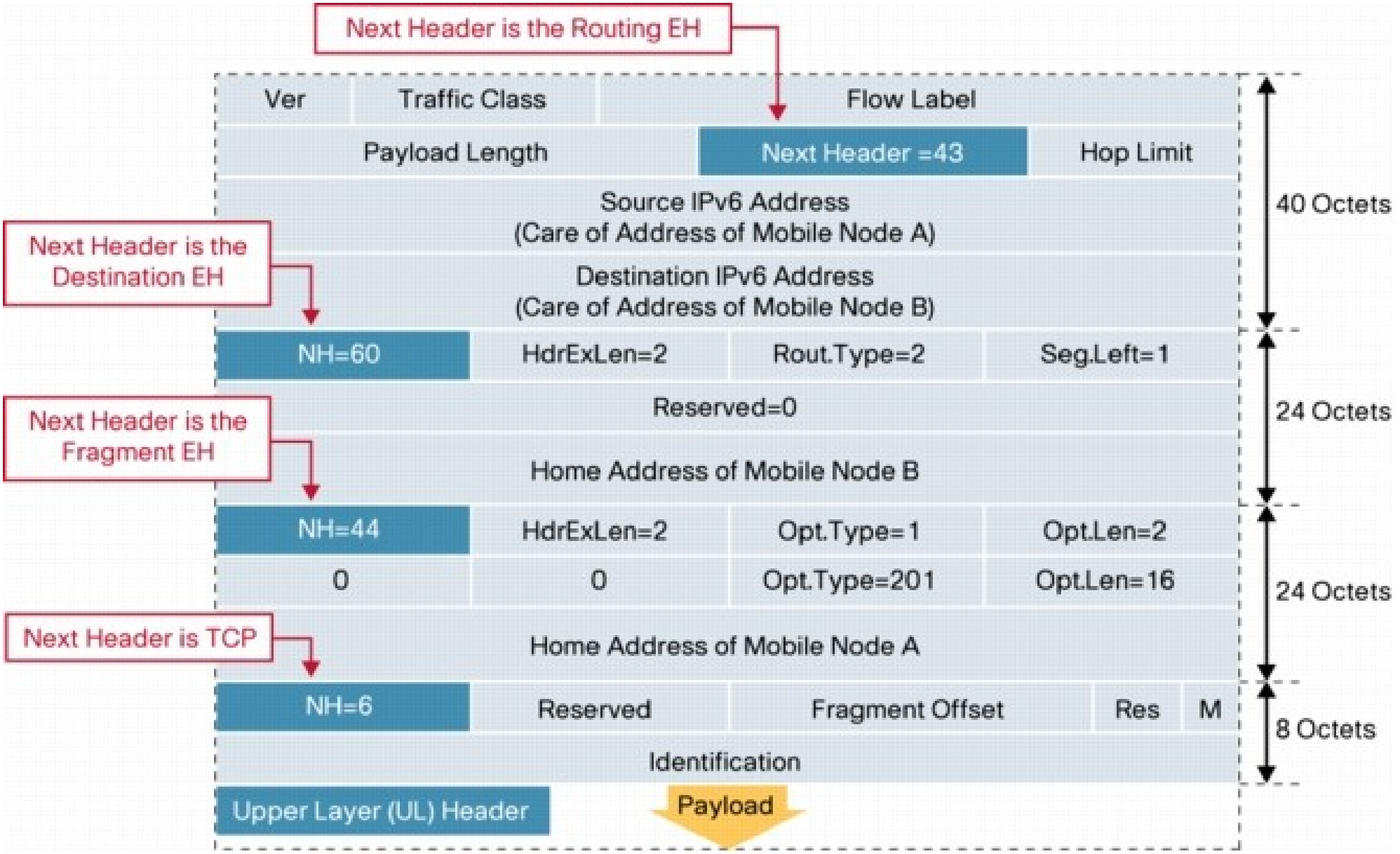


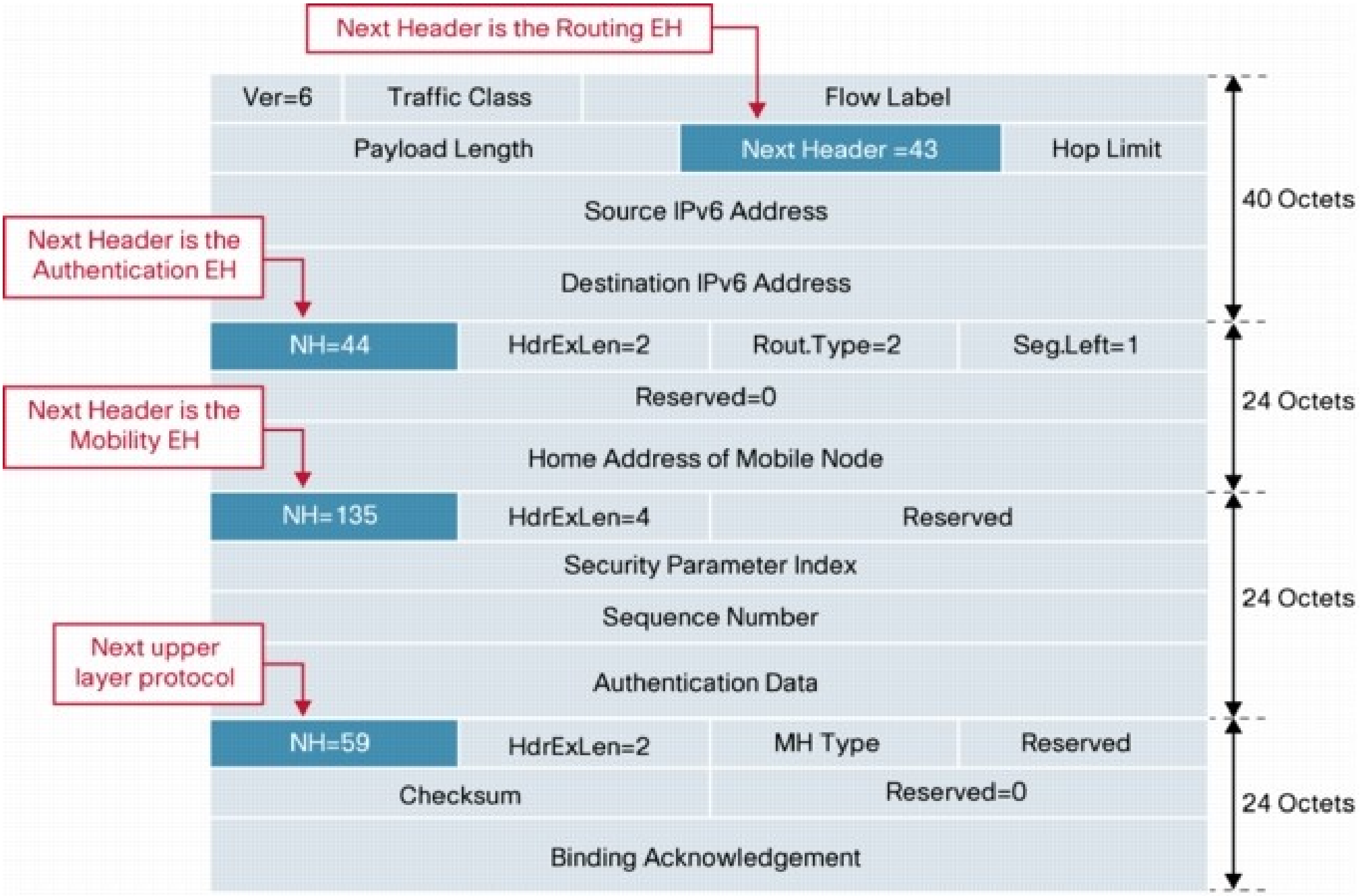
MIPv6 Basic Operation (4)



MIPv6 Basic Operation (5)




Next Header is the Routing EH
Ver
Traffic Class
Flow Label
Payload Length
Next Header =43
Hop Limit
Source IPv6 Address
(Care of Address of Mobile Node A)
Destination IPv6 Address
(Care of Address of Mobile Node B)
40 Octets
Next Header is the Destination EH
NH=60
HdrExLen=2
Rout.Type=2
Seg.Left=1
Reserved=0
Home Address of Mobile Node B
24 Octets
Next Header is the Fragment EH
NH=44
HdrExLen=2
Opt.Type=1
Opt.Len=2
0
0
Opt.Type=201
Opt.Len=16
Home Address of Mobile Node A
24 Octets
Next Header is TCP
NH=6
Reserved
Fragment Offset
Res
M
Identification
8 Octets
Upper Layer (UL) Header
Payload



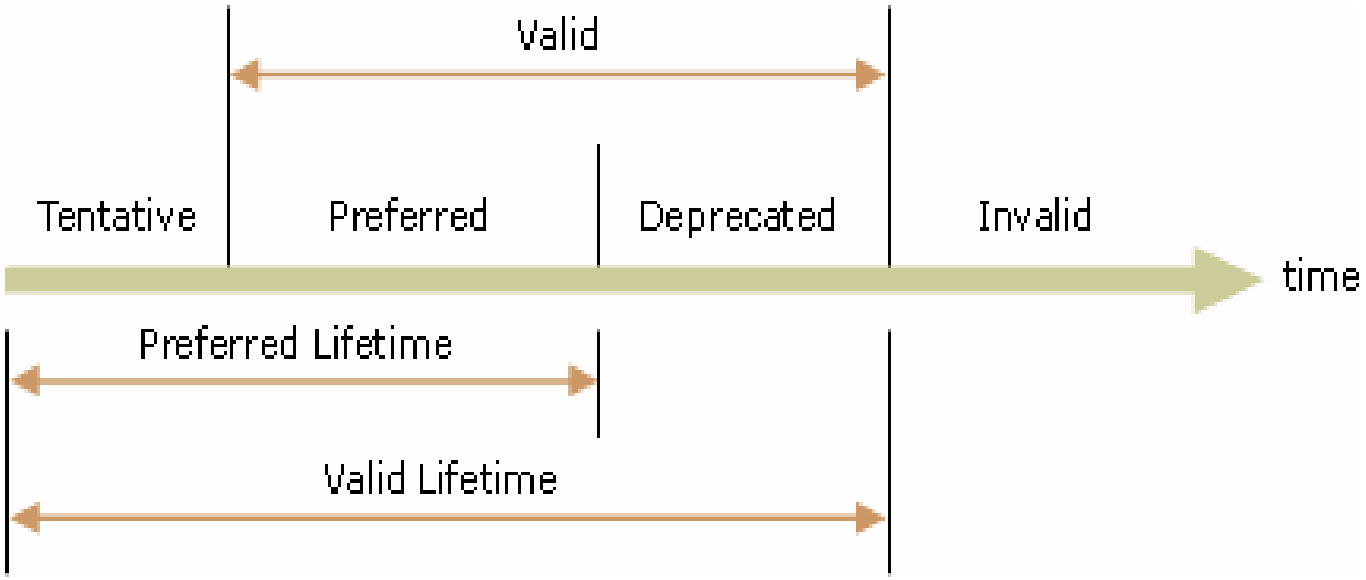
IPv6 does not allow data to be piggy-backed to the binding maintenance messages

Autoconfiguration

- The host sends a Router Solicitation message
- If a Router Advertisement message is received, the information is set on the host
  - This includes prefix and default route
  - RFC6106 adds DNS server option
- For each stateless autoconfiguration address prefix that is included, the following processes occur:
  - The address prefix and the appropriate 64-bit interface identifier are used to derive a tentative address
  - Duplicate address detection is used to verify the uniqueness of the tentative address
  - Valid and preferred lifetimes are set based on information included in the Router Advertisement message

Autoconfiguration

States



Steps for Autoconfiguration

Link-Local Address Generation -

The device is assigned a link-local address comprising '1111111010' as the first ten bits followed by 54 zeroes and a 64 bit interface identifier

Link-Local Address Uniqueness Test -

The networked device ensures that the link-local address generated by it is not already used by any other device (the address is tested for its uniqueness)

Link-Local Address Assignment -

Once the uniqueness test is cleared, the IP interface is assigned the link local address. The address becomes usable on the local network but not over the Internet

Steps for Autoconfiguration

Router Contact -

The networked device makes contact with a local router to determine its next course of action in the auto configuration process

Router Direction -

The node receives specific directions from the router on its next course of action in the auto configuration process.

Global Address Configuration -

The host configures itself with its globally unique Internet address. The address comprises a network prefix provided by the router together with the device identifier

Advantages of Stateless Auto Configuration

Does not require support of a DHCP server

Allows hot plugging of network devices

Suitable for applications requiring secure connection without additional intermediaries in the form of a proxy or a DHCP server

Cost effective

Suitable for wireless networks

Renumbering

- To allow sites to change the service provider,
  - Built into IPv6 addressing
  - If the site changes the provider, the address prefix needs to be changed
  - A router to which the site is connected can advertise a new prefix
  - The site continues to use the old prefix for a while before disabling it
  - During the transition period, a site has two prefixes

20/08/19 – 26, 20, 28, 10, 32, 11, 15, 57