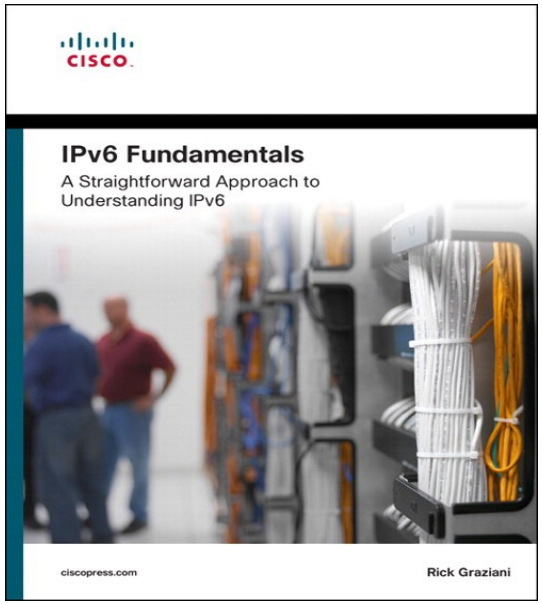
Practical Network Defense

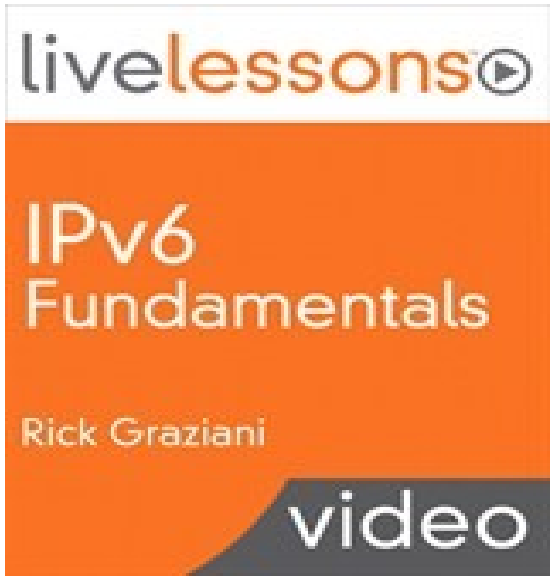
Master's degree in Cybersecurity 2024-25

IPv6: protocol overview

Angelo Spognardi
spognardi@di.uniroma1.it
Dipartimento di Informatica
Sapienza Università di Roma

Material taken from Rick Graziani IPv6 courses





IPv6 Fundamentals: A Straightforward Approach to Understanding IPv6

- By Rick Graziani
- ISBN-10: 1-58714-313-5

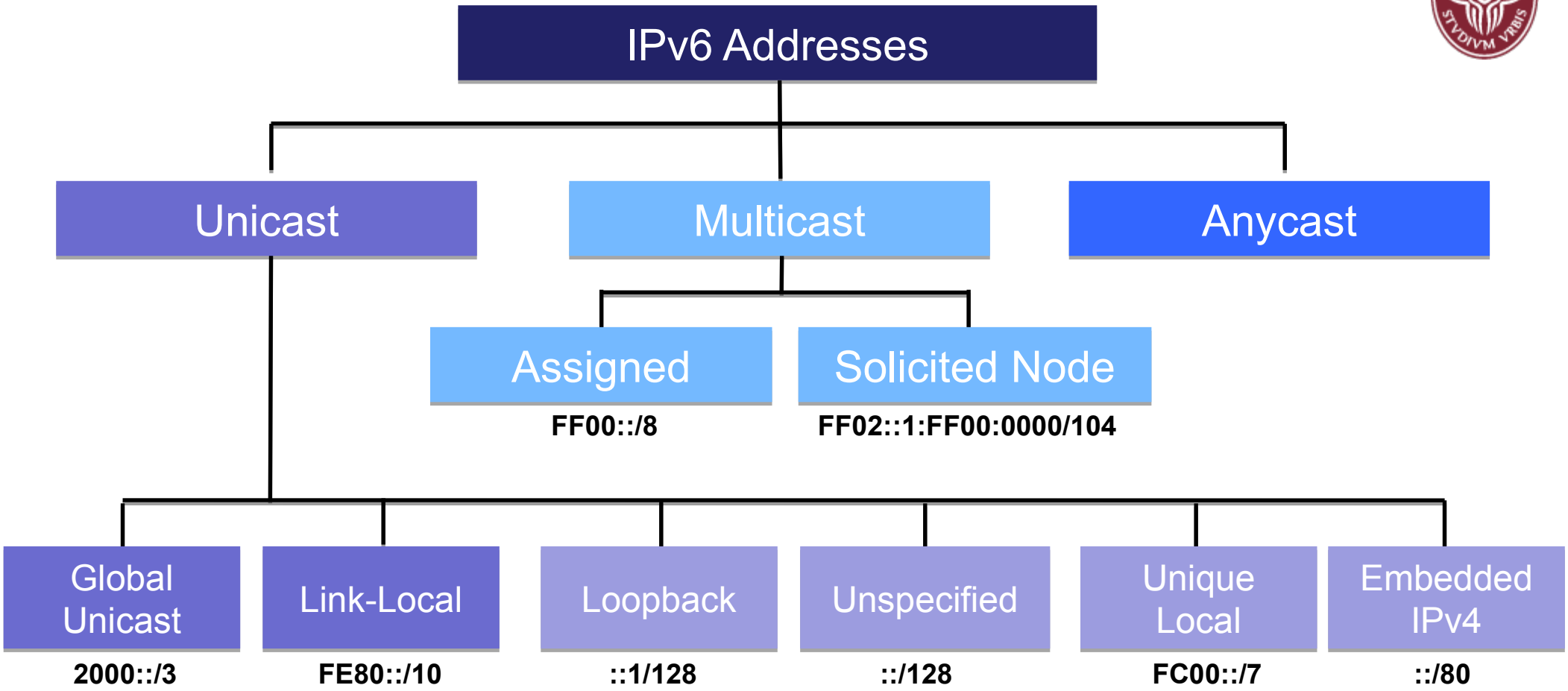
IPv6 Fundamentals LiveLessons: A Straightforward Approach to Understanding IPv6

- By Rick Graziani
- ISBN-10: 1-58720-457-6

Recap last lectures

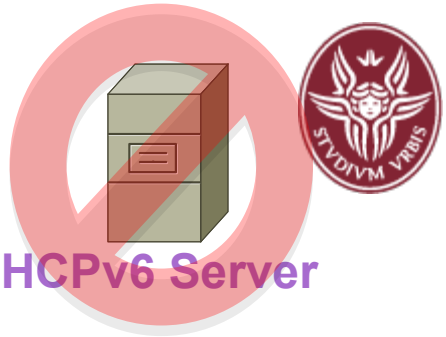
- IPv6 main features
- IPv6 address types
  - Global Unicast Address
  - Local-link unicast Address
- IPv6 dynamic assignment options
  - SLAAC
  - SLAAC+DNS via DHCPv6
  - Stateful DHCPv6
- IPv6 prefix delegation, via DHCPv6-PD

IPv6 Address Types



IPv6 does not have a "broadcast" address.

SLAAC: Random 64-bit Interface ID



/48 /64

Global Routing Prefix	16-bit Subnet ID	64-bit Interface ID

SLAAC

Operating System	EUI-64	Random 64-bit
Windows XP, Server 2003	✓	
Windows Vista and newer		✓
MAC OSX	✓	
Linux		✓

EUI-64 Process

Randomly Generated Number (Privacy Extension)

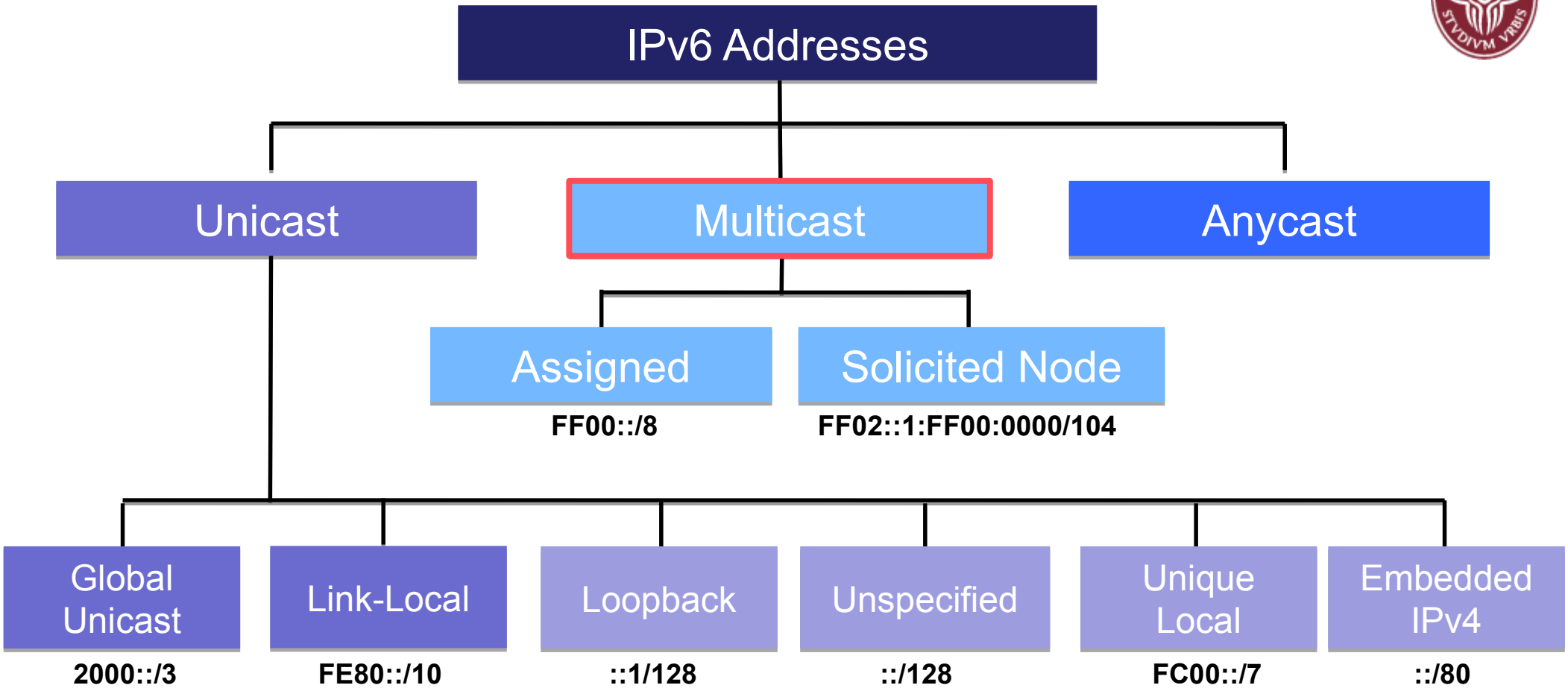
SLAAC: Temporary Addresses

- Idea: provide additional addresses that have relatively short lifetimes and are used as the source address when originating connections
- Same prefix as a public address, randomized value for the Interface ID
- Short lifetime, usually hours or days
- It is common to have multiple temporary addresses to make sure existing connections can continue while a new temporary address is created for new connections

Randomly Generated Number (Privacy Extension)

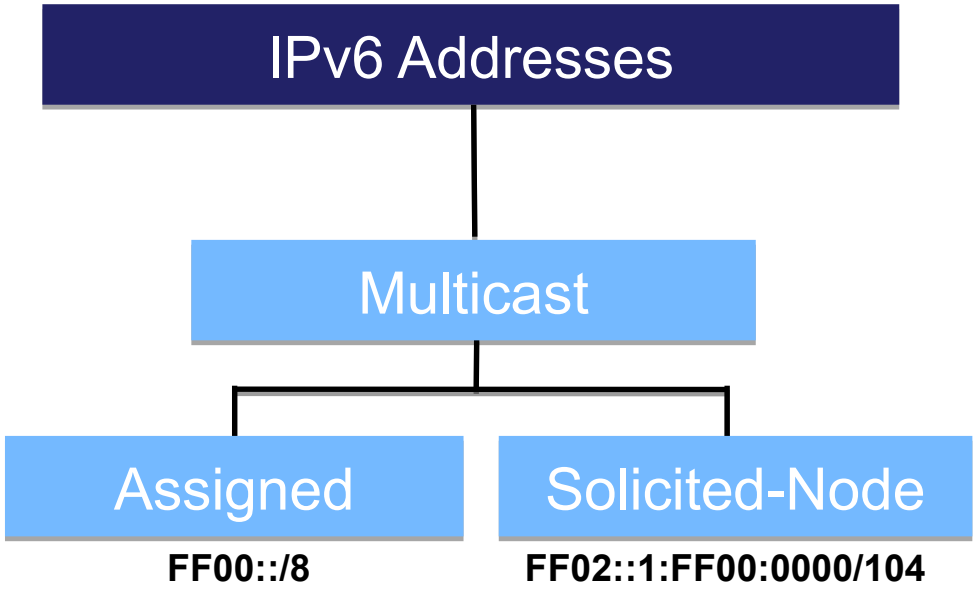
```
LinuxPC# ip -6 addr show dev eth0

2: eth0: <BROADCAST,MULTICAST,UP, LOWER_UP> mtu 1500 state UNKNOWN qlen1000
  inet6 2001:db8:cafe:4:314a:dd3e:762f:e140/64 scope global temporary dynamic
     valid_lft 604747sec preferred_lft 85747sec

  inet6 2001:db8:cafe:4:250:56ff:feaf:2524/64 scope global dynamic
     valid_lft 2591947sec preferred_lft 604747sec

 inet6 fe80::250:56ff:feaf:2524/64 scope link
     valid_lft forever preferred_lft forever
```

IPv6 Address Types



IPv6 does not have a "broadcast" address.

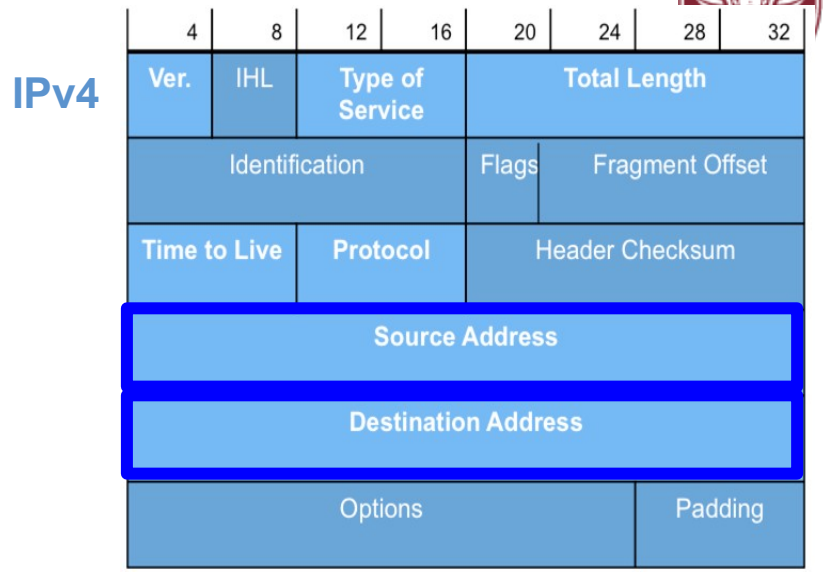
IPv6 Multicast Addresses

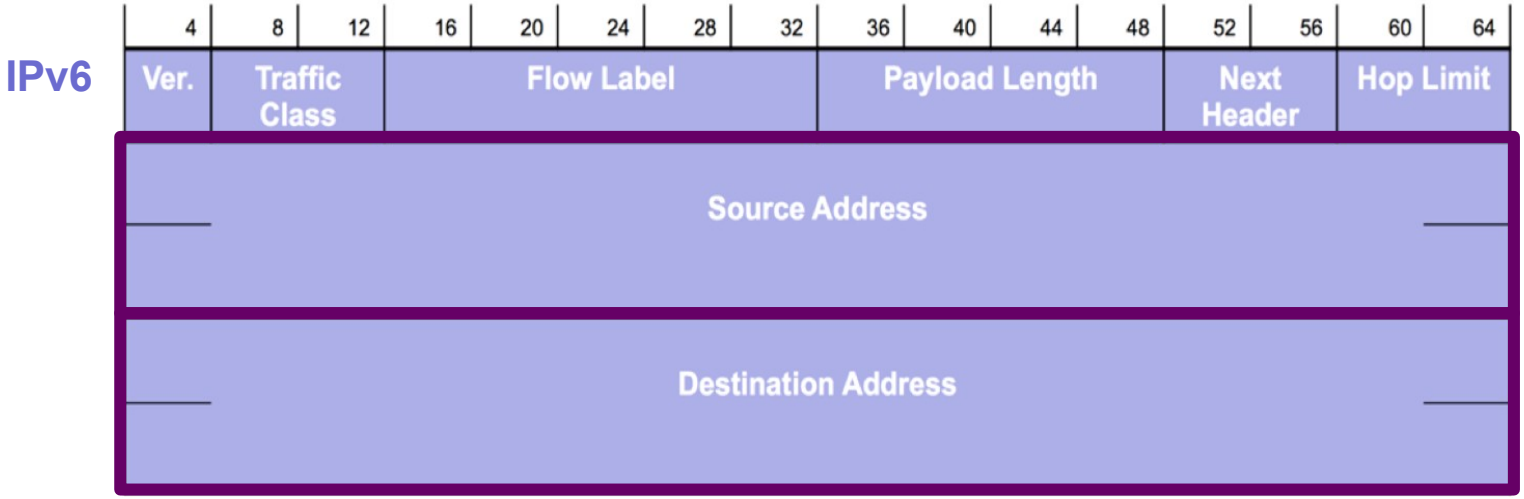


- Used by a device to send a single packet to multiple destinations simultaneously (one-to-many).
- Equivalent to 224.0.0.0/4 in IPv4.
- Two types of multicast addresses:
  - Assigned
  - Solicited-Node

IPv6 Multicast Addresses

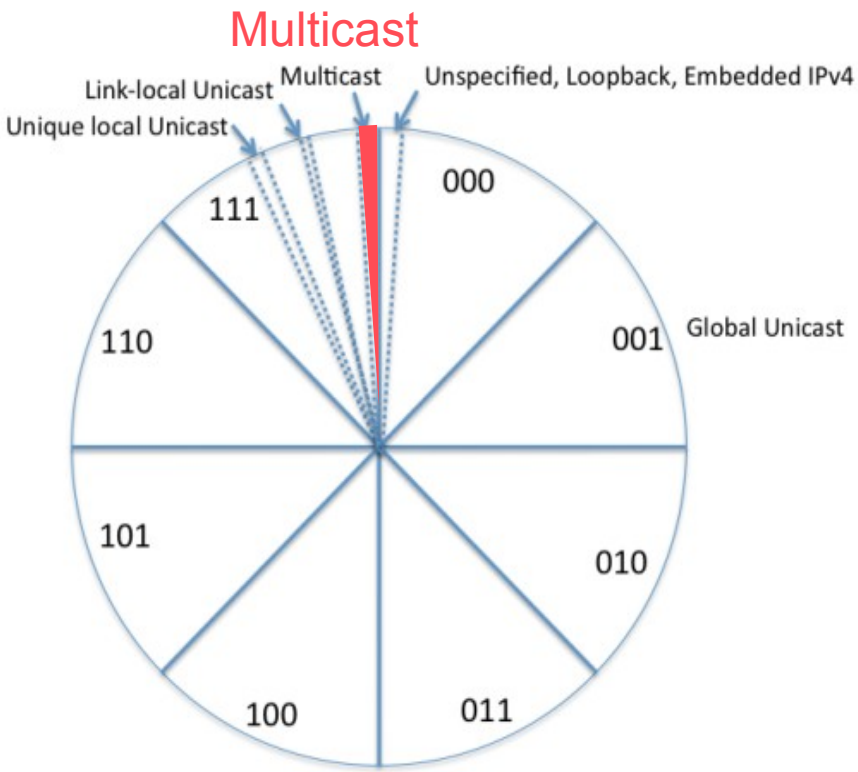
- **IPv6 Source** – Always a unicast
- **IPv6 Destination** – Unicast, ***multicast***, or anycast.





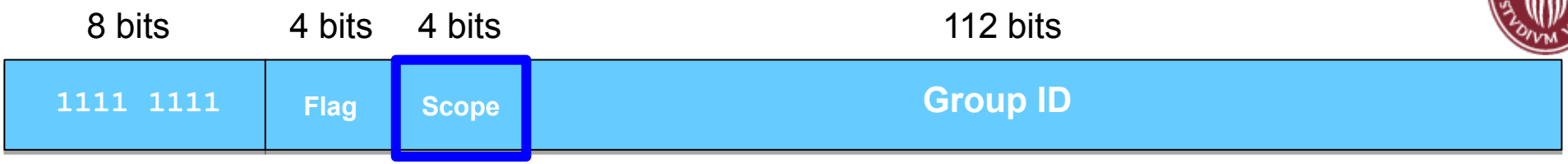
Multicast Range

IPv6 multicast addresses have the prefix **FF00::/8**

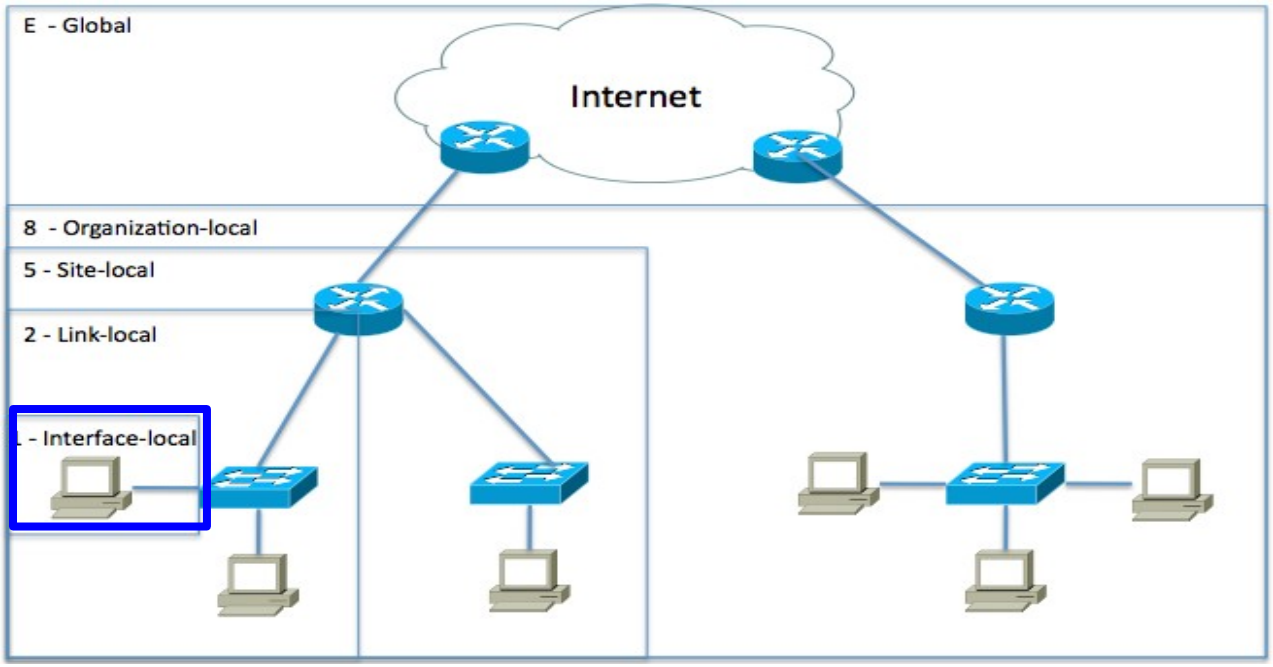


The remaining portion of IPv6 address space are reserved by IETF for future use.

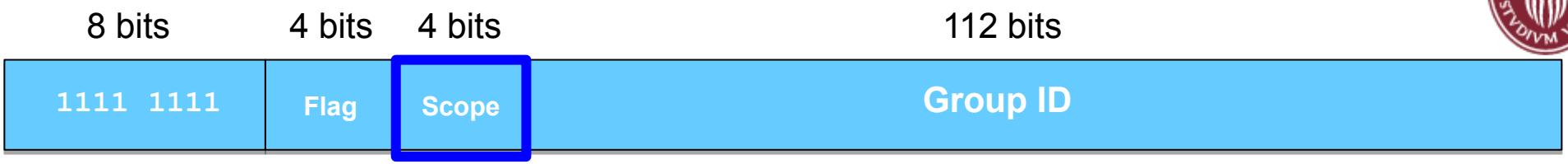
IPv6 Multicast Addresses - Scope



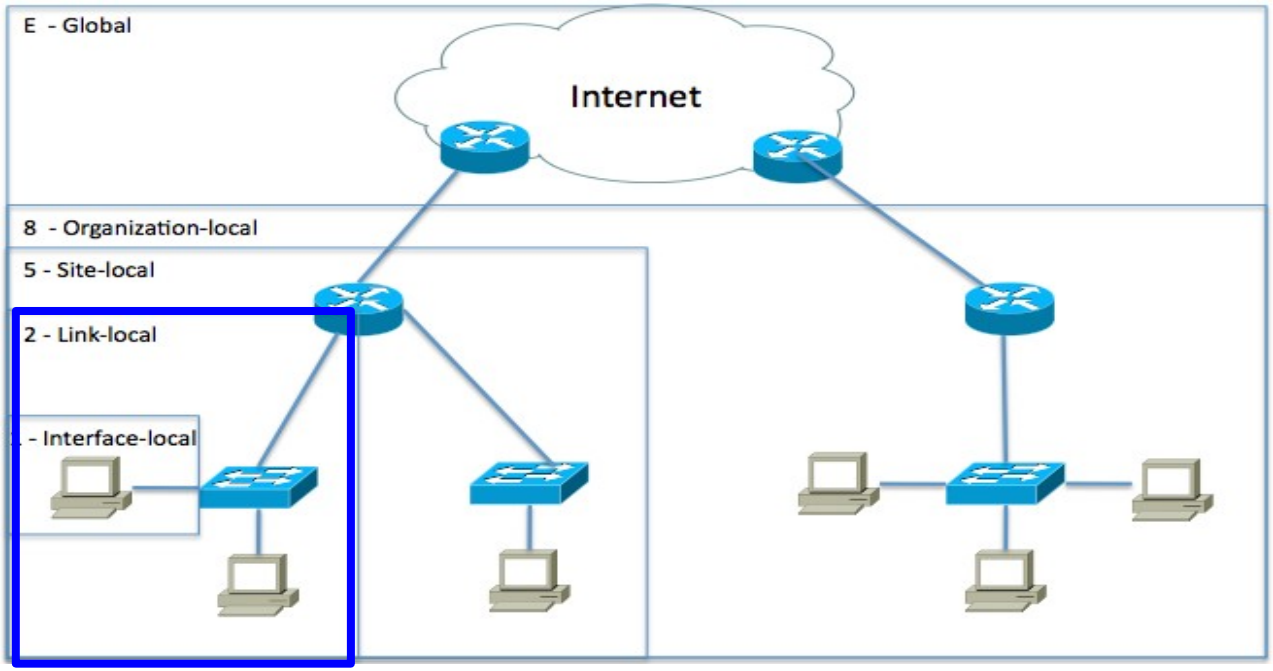
- Scope is a 4-bit field used to define the range of the multicast packet.
- **Scope** (partial list):
  - 0 Reserved
  - 1 Interface-Local scope



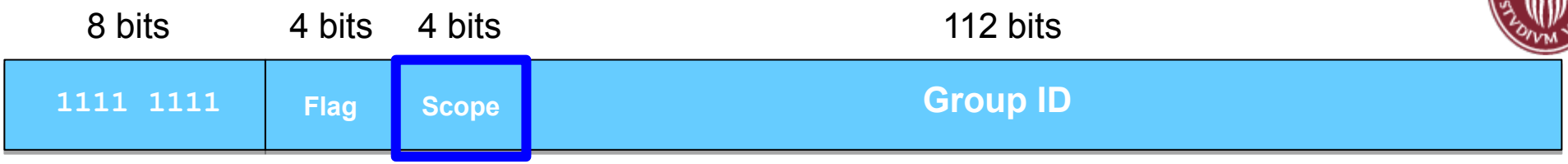
IPv6 Multicast Addresses - Scope



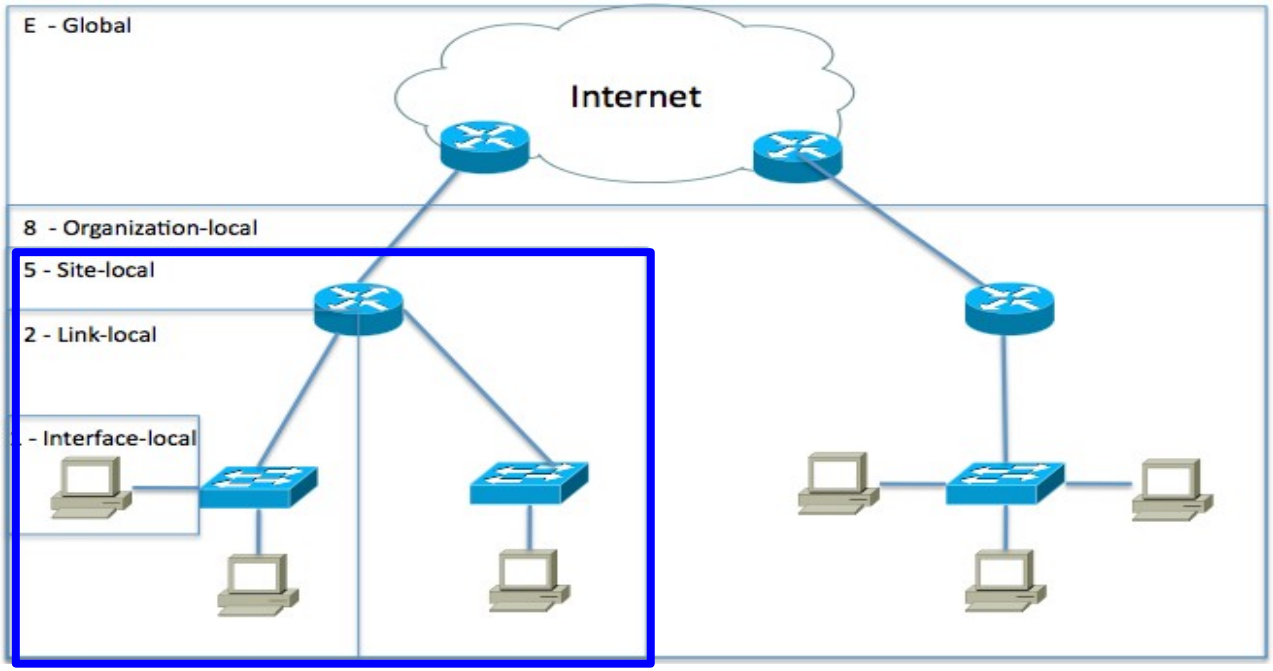
- Scope is a 4-bit field used to define the range of the multicast packet.
- **Scope** (partial list):
  - 0 Reserved
  - 1 Interface-Local scope
  - 2 Link-Local scope



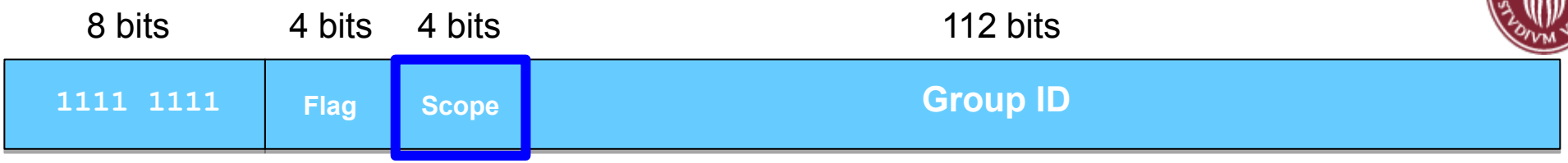
IPv6 Multicast Addresses - Scope



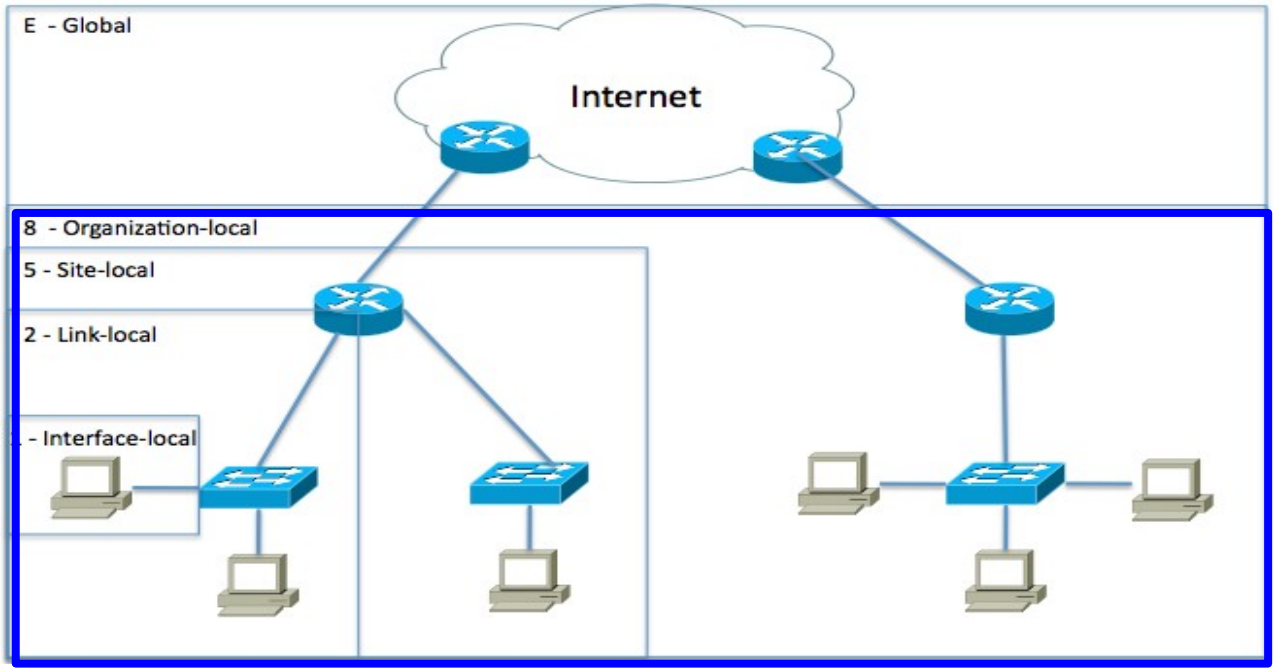
- Scope is a 4-bit field used to define the range of the multicast packet.
- **Scope** (partial list):
  - 0 Reserved
  - 1 Interface-Local scope
  - 2 Link-Local scope
  - 5 Site-Local scope



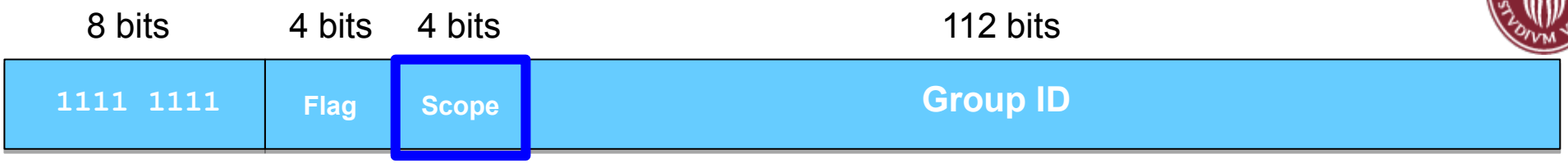
IPv6 Multicast Addresses - Scope



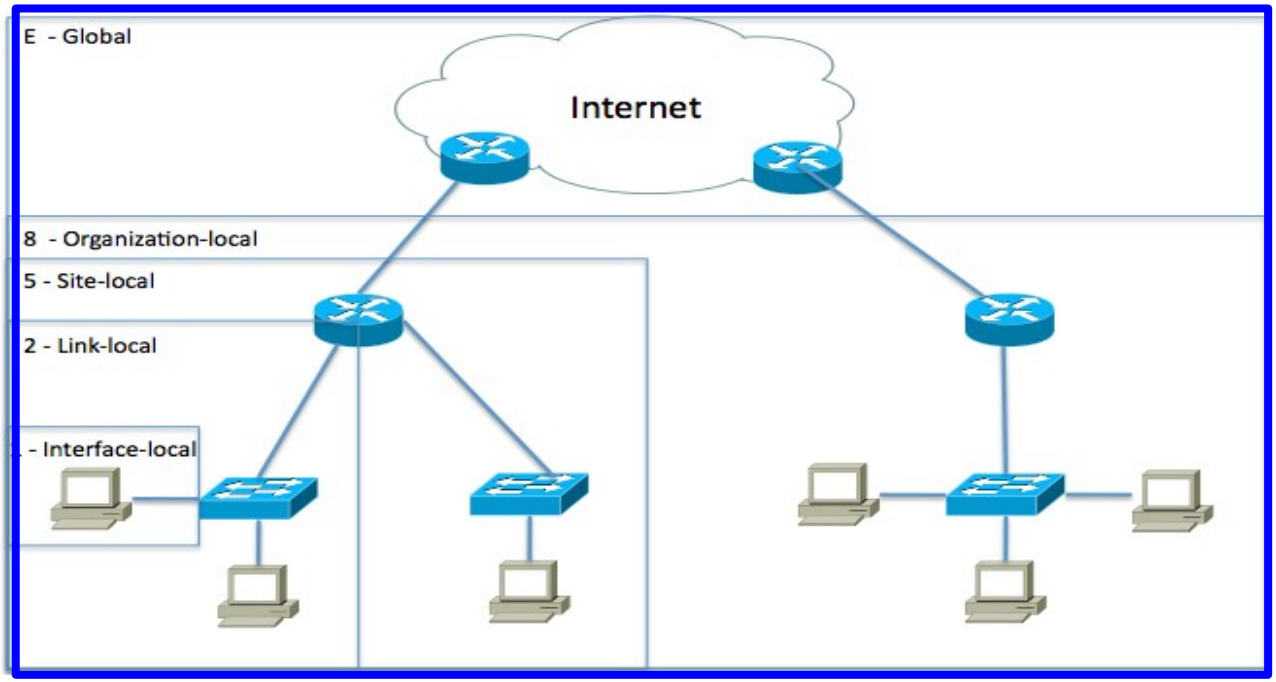
- Scope is a 4-bit field used to define the range of the multicast packet.
- **Scope** (partial list):
  - 0 Reserved
  - 1 Interface-Local scope
  - 2 Link-Local scope
  - 5 Site-Local scope
  - 8 Organization-Local scope



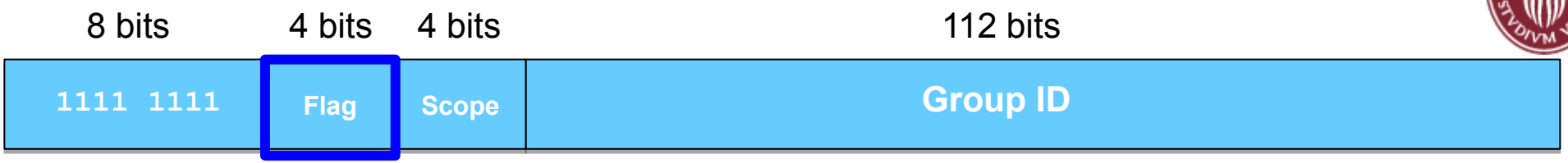
IPv6 Multicast Addresses - Scope



- Scope is a 4-bit field used to define the range of the multicast packet.
- **Scope** (partial list):
  - 0 Reserved
  - 1 Interface-Local scope
  - 2 Link-Local scope
  - 5 Site-Local scope
  - 8 Organization-Local scope
  - E Global scope

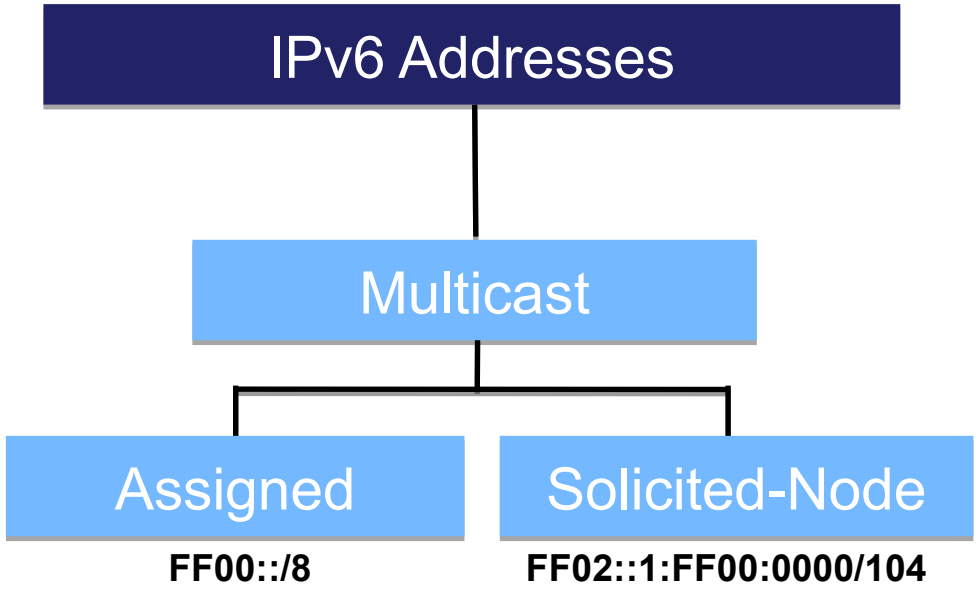


IPv6 Multicast Addresses - Flag



- **Flag**
  - **0** - Permanent, well-known multicast address assigned by IANA.
    - Includes both assigned and solicited-node multicast addresses.
  - **1** - Non-permanently-assigned, “dynamically" assigned multicast address.
    - An example might be FF18::CAFE:1234, used for a multicast application with organizational scope.

Assigned IPv6 Multicast Addresses



IPv6 Multicast Address Space Registry

Last Updated
2014-08-17

Expert(s)
Stig Venaas

Note

IPv6 multicast addresses are defined in "IP Version 6 Addressing Architecture" [RFC4291]. This defines fixed scope and variable scope multicast addresses.

IPv6 multicast addresses are distinguished from unicast addresses by the value of the high-order octet of the addresses: a value of 0xFF (binary 11111111) identifies an address as a multicast address; any other value identifies an address as a unicast address.

The rules for assigning new IPv6 multicast addresses are defined in [RFC3307]. IPv6 multicast addresses not listed below are reserved.

Available Formats

XML HTML Plain text

Registries included below

- IPv6 Multicast Address Scopes
- Node-Local Scope Multicast Addresses
- Link-Local Scope Multicast Addresses
- Site-Local Scope Multicast Addresses
- Variable Scope Multicast Addresses
- Source-Specific Multicast block

- RFC 2375, IPv6 Multicast Address Assignments, defines the initial assignment of IPv6 multicast addresses that have permanently assigned Global IDs.
- Reference for assigned multicast addresses:
  - (IANA) IPv6 Multicast Address Space Registry - http://www.iana.org/assignments/ipv6-multicast-addresses/ipv6-multicast-addresses.xhtml

Assigned Multicast Addresses with Link-local Scope

Flag = 0, Assigned multicast
Scope = 2, Link-local scope

Prefix	Flag	Scope	Predefined Group ID	Compressed Format	Description (IPv6 assumed)
FF	**0**	2	0:0:0:0:0:0:1	FF02::1	All-devices
FF	**0**	2	0:0:0:0:0:0:2	FF02::2	All-routers
FF	**0**	2	0:0:0:0:0:0:5	FF02::5	OSPF routers
FF	**0**	2	0:0:0:0:0:0:6	FF02::6	OSPF DRs
FF	**0**	2	0:0:0:0:0:0:9	FF02::9	RIP routers
FF	**0**	2	0:0:0:0:0:0:A	FF02::A	EIGRP routers
FF	**0**	2	0:0:0:0:0:1:2	FF02::1:2	DHCP servers/relay agents

Assigned Multicast Addresses with Site-local Scope

Flag = 0, Assigned multicast
Scope = 5, Site-local scope

Prefix	Flag	Scope	Predefined Group ID	Compressed Format	Description (IPv6 assumed)
FF	**0**	5	0:0:0:0:0:0:2	FF05::2	All-routers
FF	**0**	5	0:0:0:0:0:1:3	FF05::1:3	All DHCP servers

- Used to communicate within a “site”, possibly routed within the site.
- Must have IPv6 multicast routing enabled:

```
Router(config)# ipv6 multicast-routing
```

- *DHCPv6, relay agents and DHCPv6 multicast addresses are included in Lesson 8.*

DHCPv6 without and with relay agents

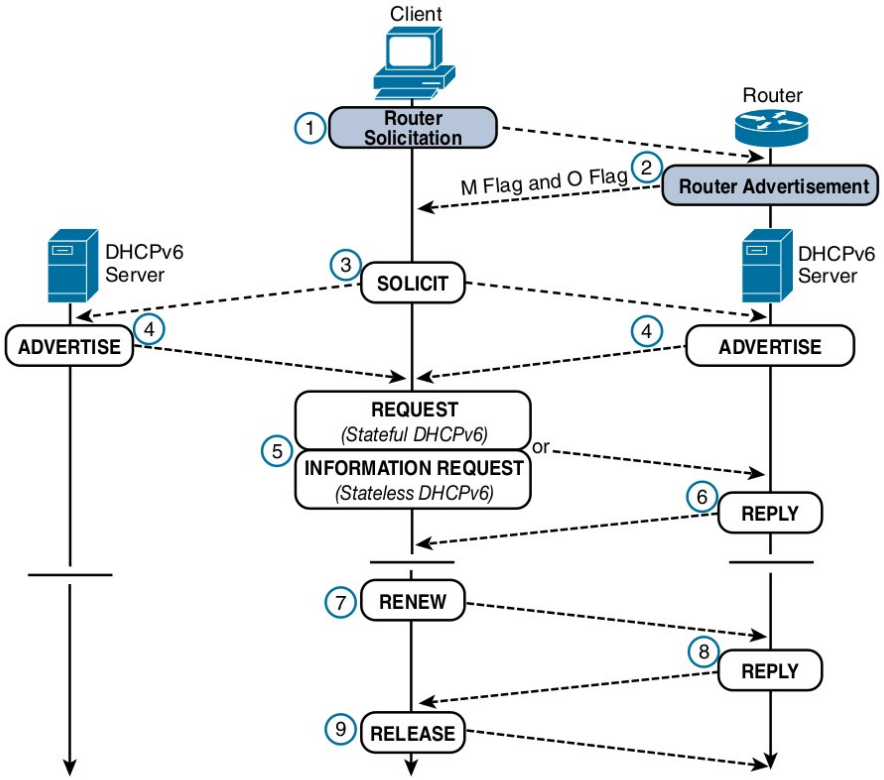


Figure 8-9 *Stateless and Stateful DHCPv6 Operations*

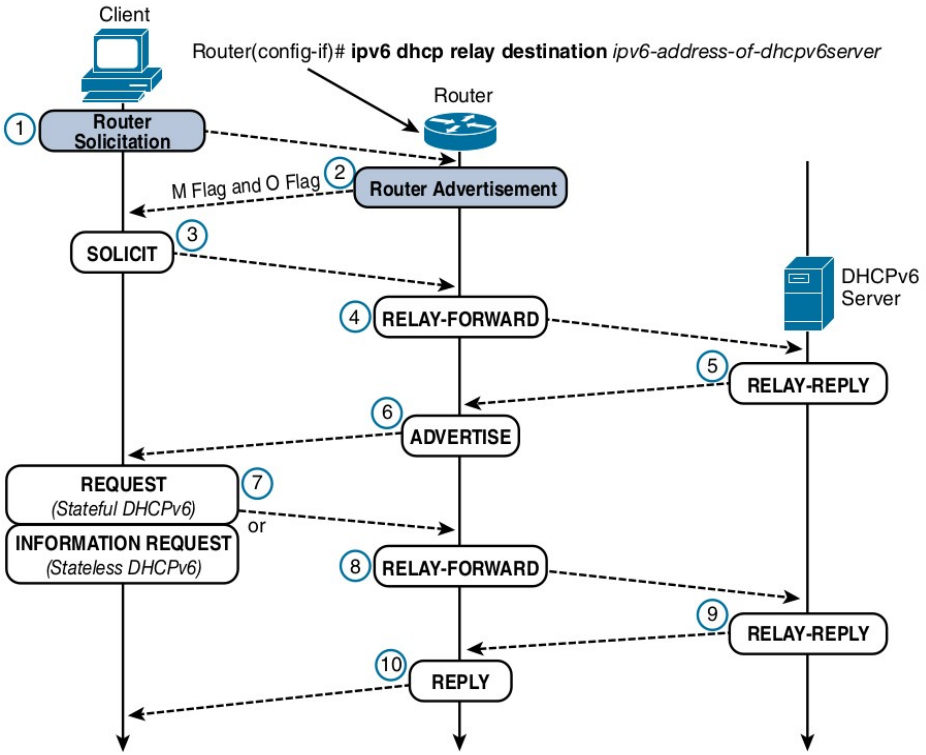


Figure 10-4 *DHCPv6 Relay Agent Communications*

Figures taken from the book **IPv6 Fundamentals: A Straightforward Approach to Understanding IPv6,** by Rick Graziani, Ciscopress

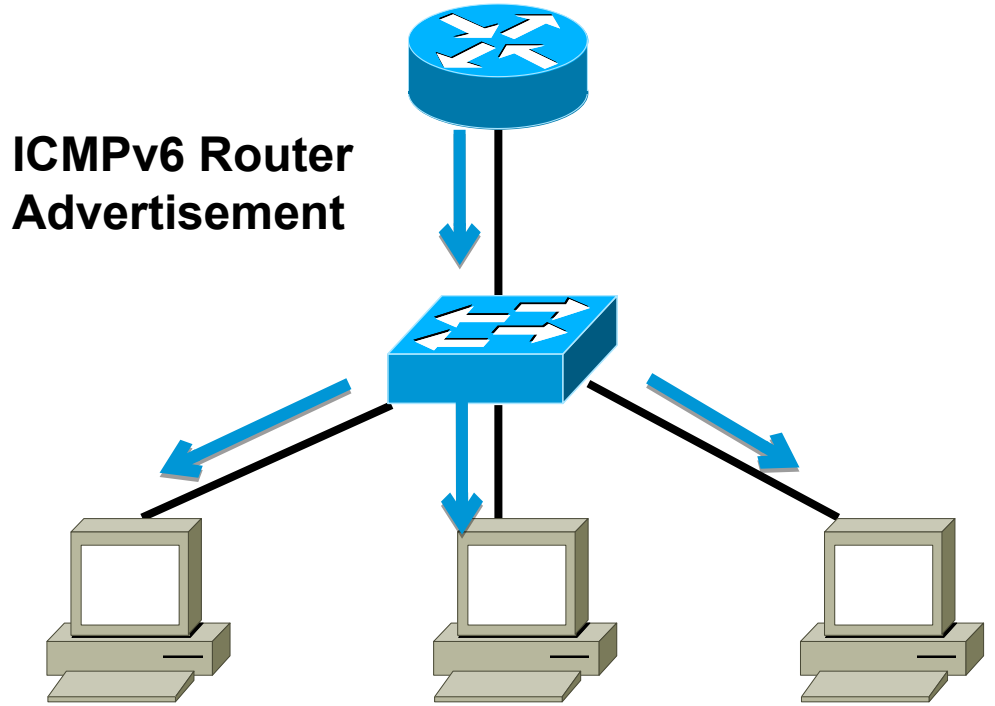
“All IPv6 Devices” Assigned Multicast Address

ICMPv6 Router Advertisement

FF02::1	FE80::1	Rest of IPv6 Packet
Destination IPv6 Address	**Source IPv6 Address**	

```
Router(config)# ipv6 unicast-routing
```

- **FF02::1 – All IPv6 Devices**
- All IPv6 devices, including the router, belong to this group.
- Every IPv6 device will listen and process packets to this address.
- Isn’t this the same as a broadcast?
- No, because it maps to a Layer 2 MAC address which is more efficient… coming soon!



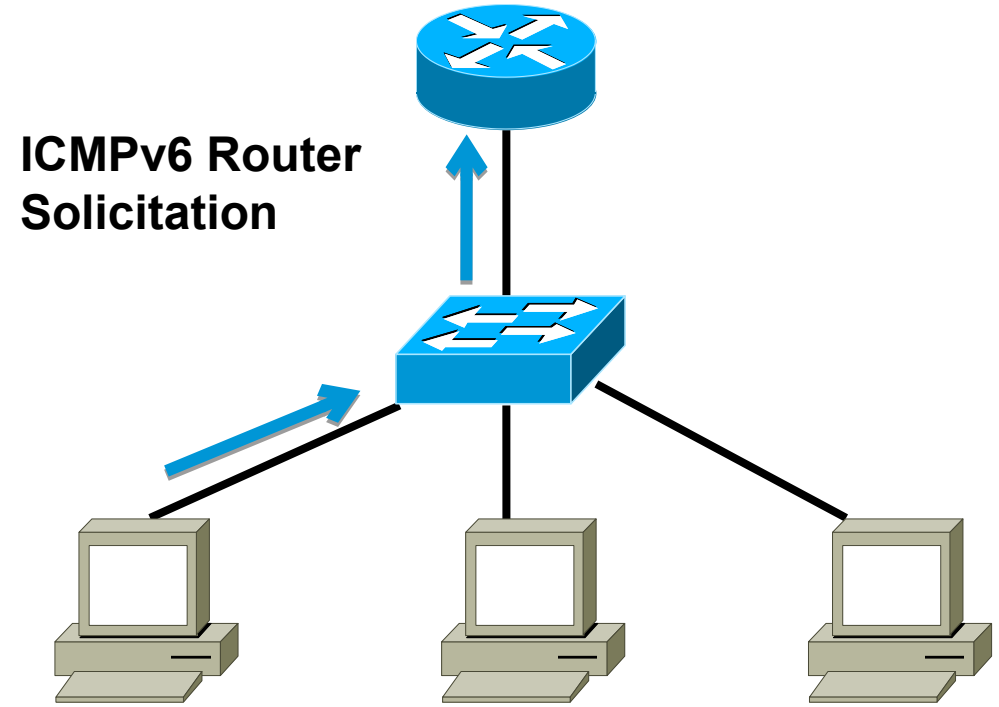
“All IPv6 Routers” Assigned Multicast Address

ICMPv6 Router Solicitation

FF02::2	FE80::12:3456:7890:ABCD	Rest of IPv6 Packet
Destination IPv6 Address	**Source IPv6 Address**	

```
Router(config)# ipv6 unicast-routing
```

- **FF02::2 – All IPv6 Routers**
- All IPv6 routers belong to this group. (Process these packets.)
- Used by devices to communicate with an IPv6 Router.



IPv6 vs. IPv4

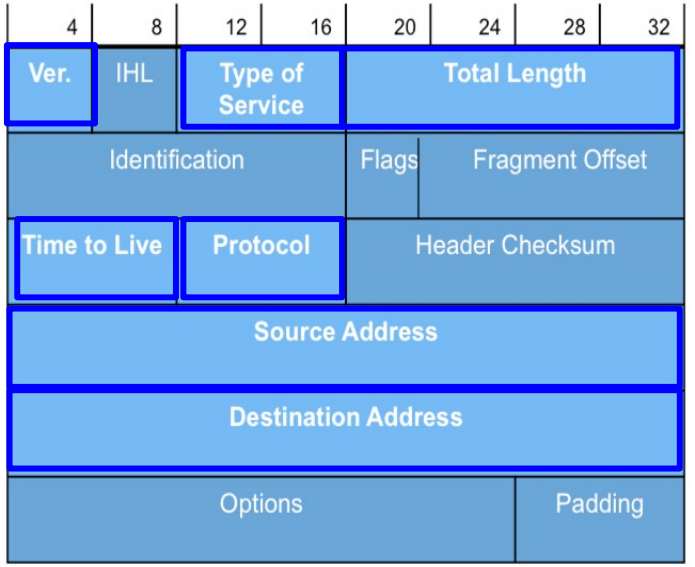
IPv6 Header

- Understanding IPv6 begins with the IPv6 header.
- IPv6 takes advantage of 64-bit CPUs.
- Several differences between IPv4 and IPv6 headers.

- Simpler IPv6 header.
- Fixed 40 byte IPv6 header.
- Lets look at the differences…

Similar fields

IPv4

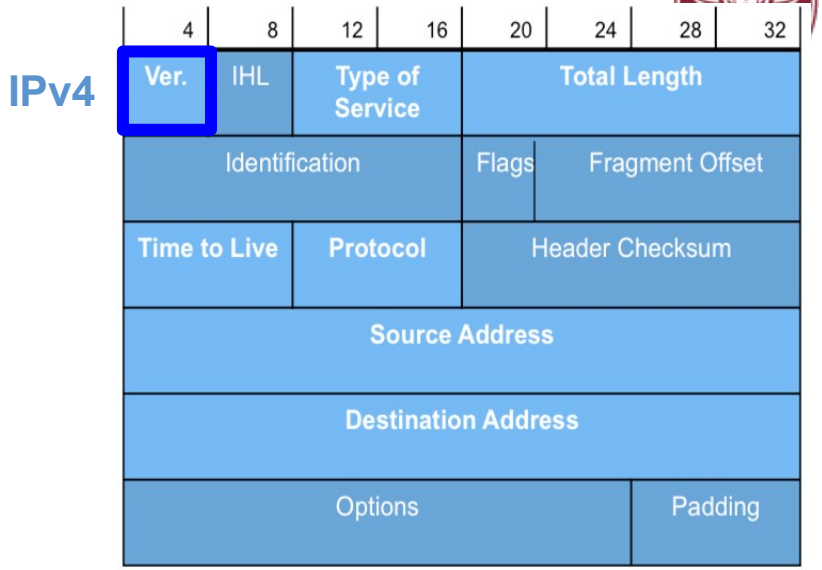


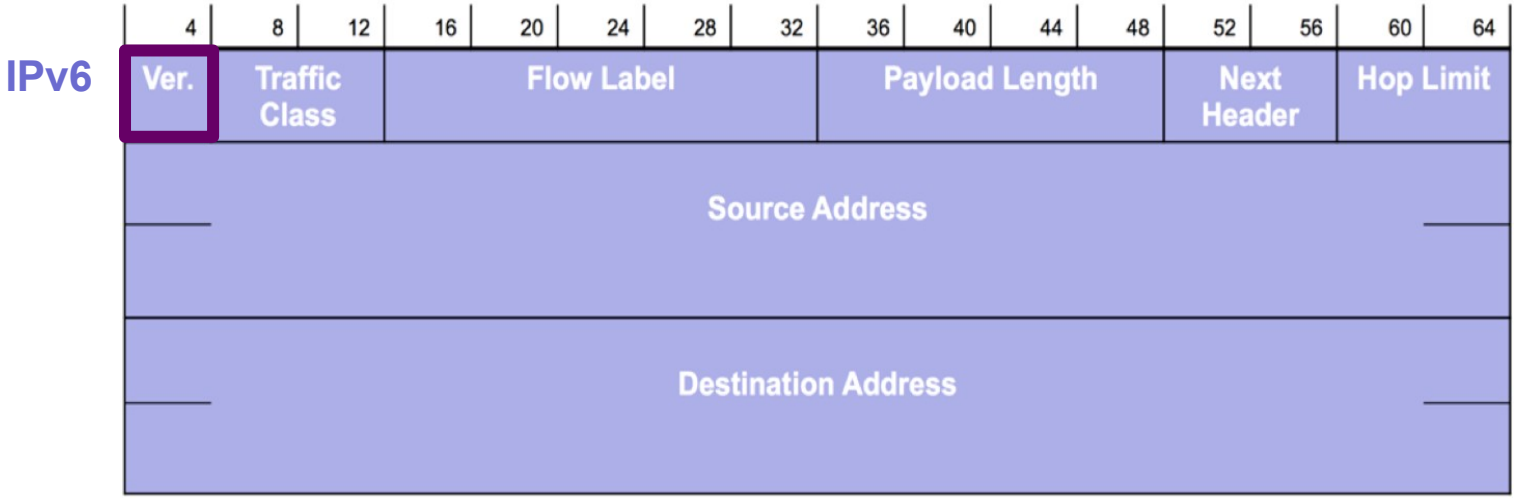
64-bit memory word

IPv6

IPv6 Version

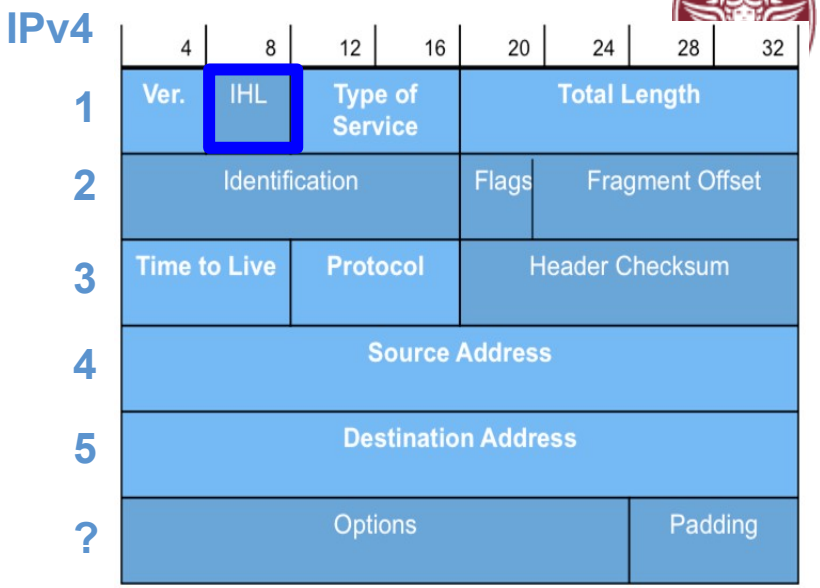
- **IPv4 Version** contains 4.
- **IPv6 Version** contains 6.
- Version 5: Internet Stream Protocol (ST2)

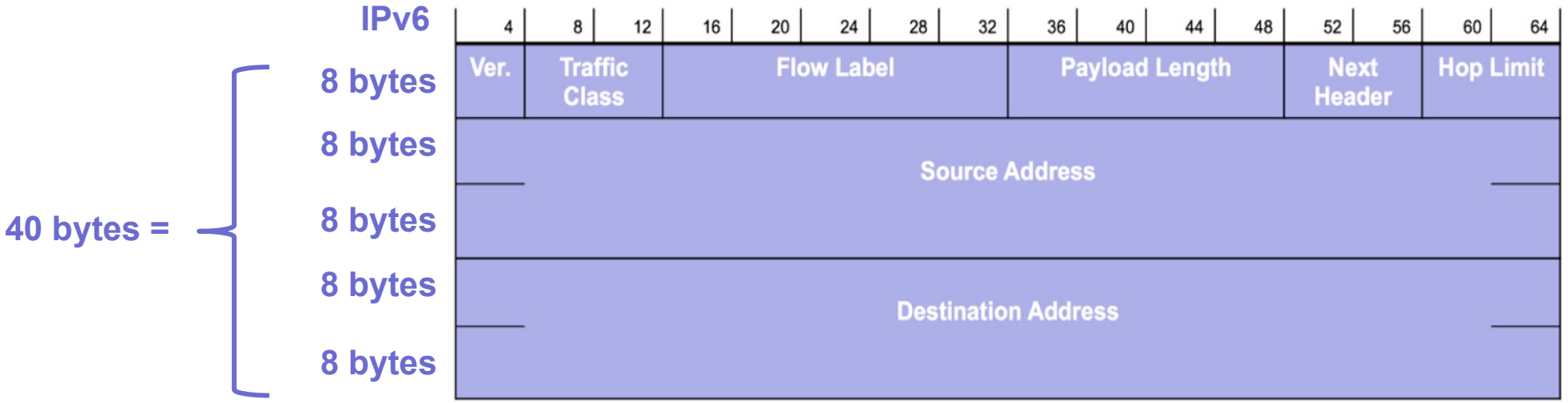




IPv4 Internet Header Length

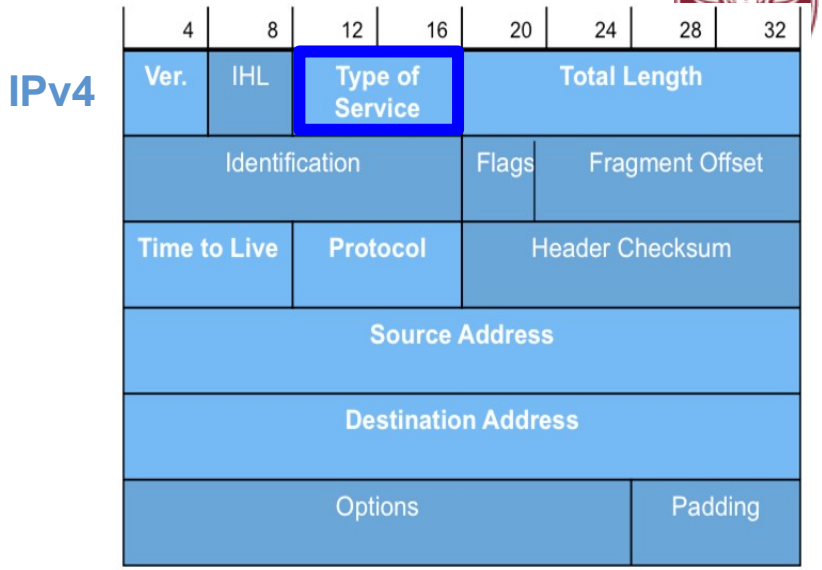
- **IPv4 Internet Header Length (IHL)**
  - Length of IPv4 header in 32-bit words including any Options or Padding.
- **IPv6**
  - IHL for IPv6 is not needed.
  - IPv6 header is fixed at 40 bytes.

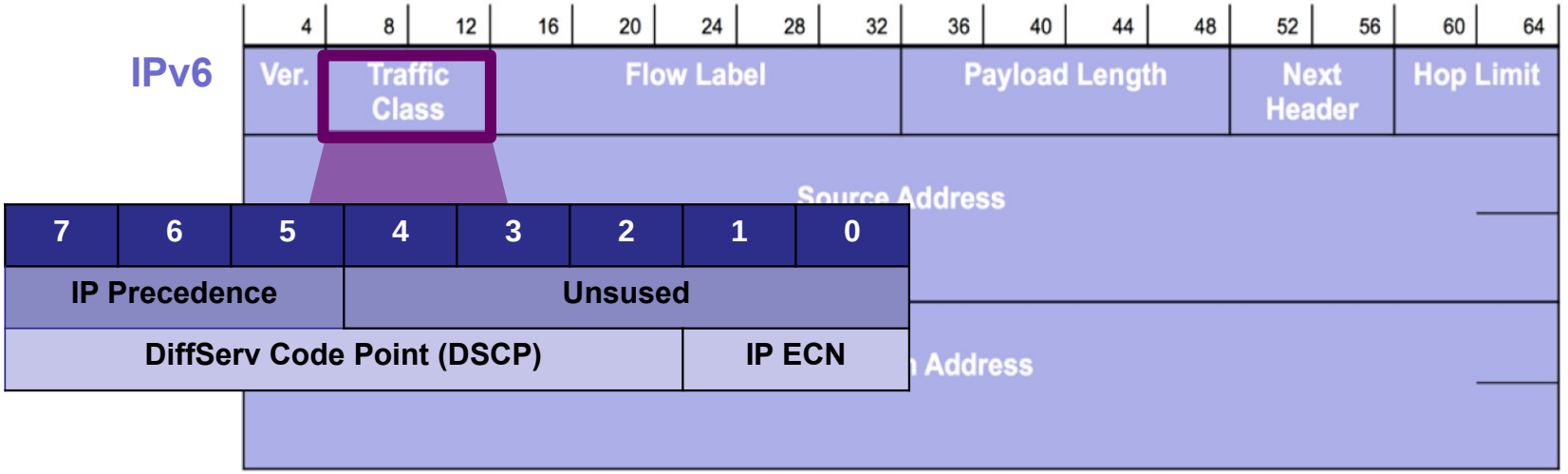




IPv6 Traffic Class

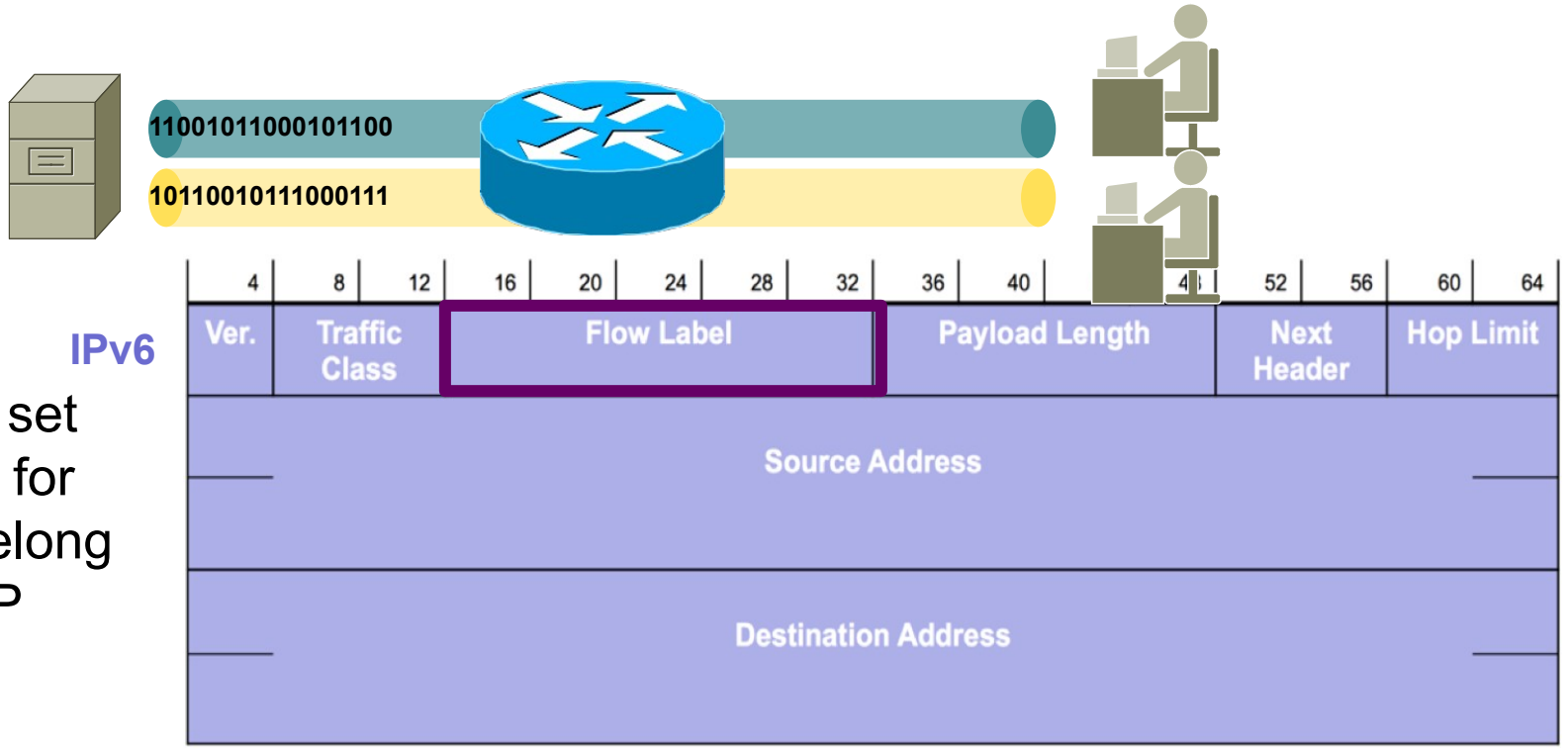
- **IPv4 Type of Service**
- **IPv6 Traffic Class**
  - Not mandated by any IPv6 RFCs.
  - Same functionality as IPv4.
  - Uses same Differentiated Services technique (RFC 2474) as IPv4.





IPv6 Flow Label

- New field in IPv6 – not part of IPv4.
- Flow label is used to identify the packets in a common stream or flow.
- Traffic from source to destination share a common flow label.
- RFC 6437 IPv6 Flow Label Specification



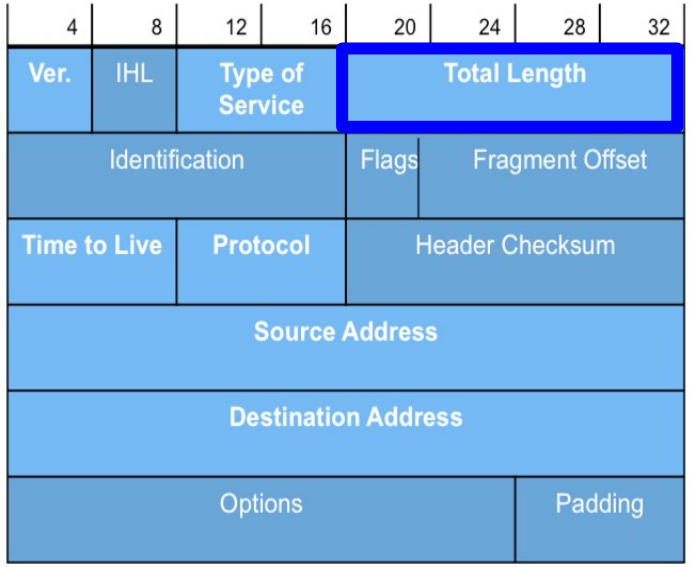
IPv6

- Many systems set the Flow Label for packets that belong to different TCP sessions

IPv6 Payload Length

- **IPv4 Total Length** – Number of bytes of the IPv4 header (options) + data.

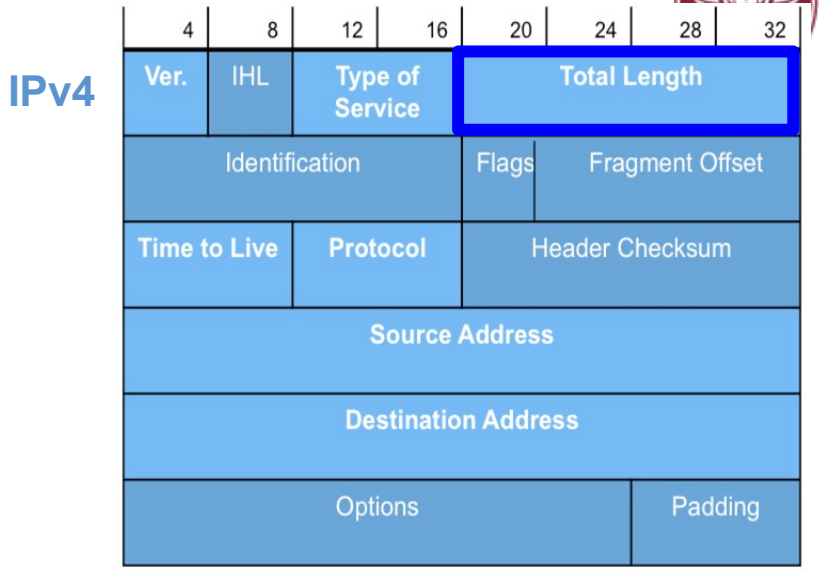
IPv4

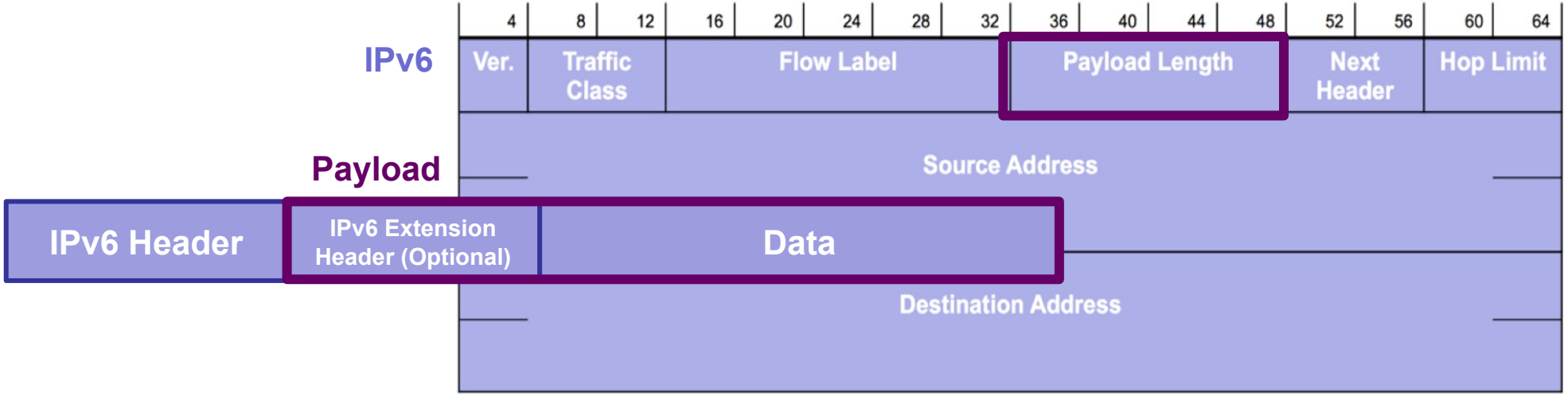


IPv6

IPv6 Payload Length

- **IPv4 Total Length** – Number of bytes of the IPv4 header (options) + data.
- **IPv6 Payload Length** – Number of bytes of the payload.
  - Does not include the main IPv6 header.
  - Includes extension headers + data

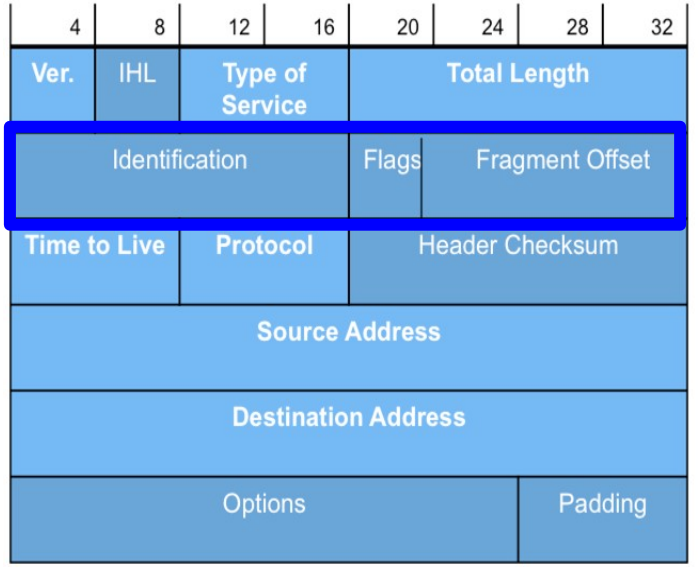




IPv4 Fragmentation

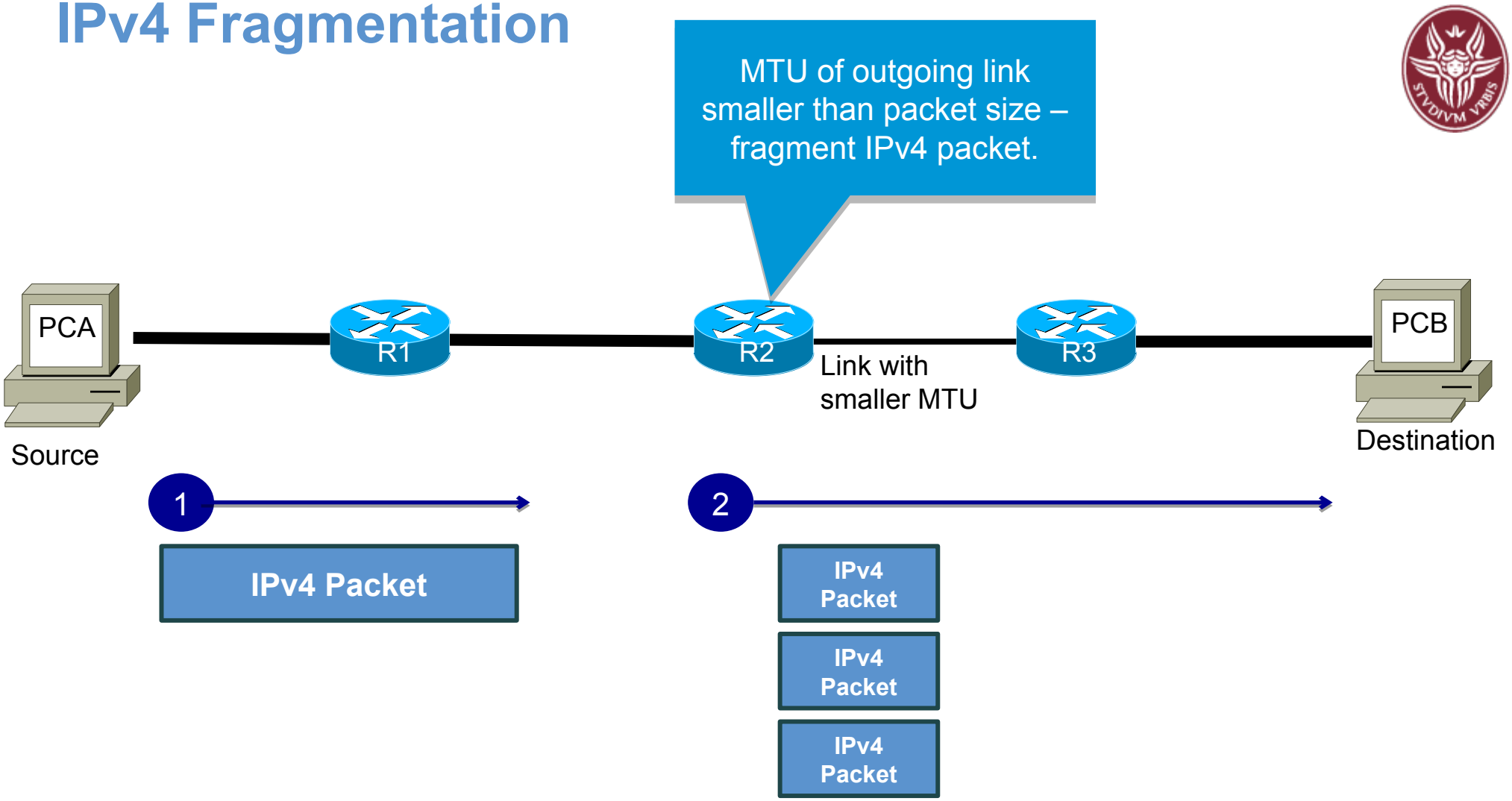
- IPv4 fields used for fragmentation and reassembly.
- Intermediate devices such as IPv6 routers do not perform fragmentation.
- Any fragmentation needed will be handled by the source using an extension header.

IPv4

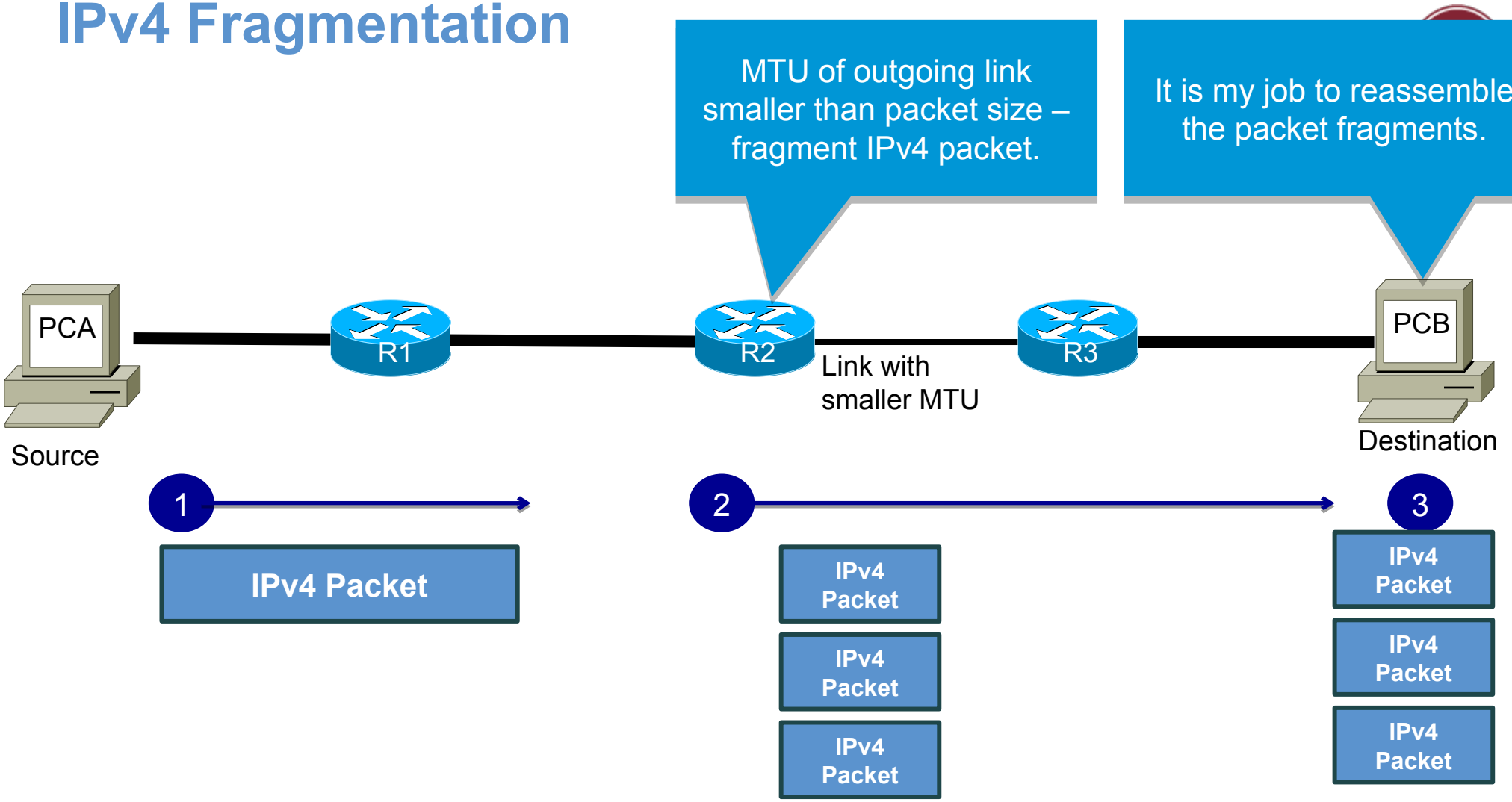


IPv6

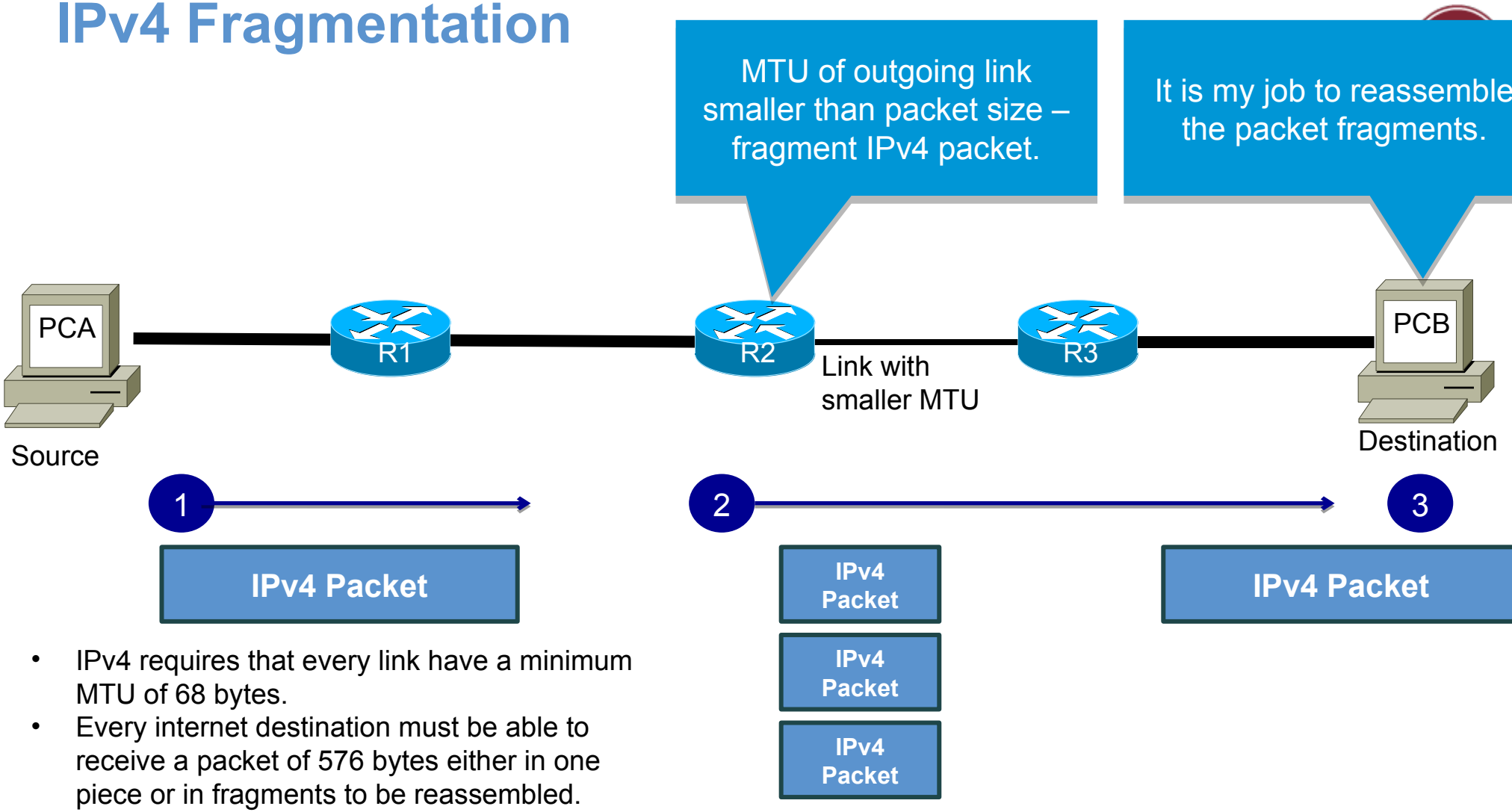
IPv4 Fragmentation



IPv4 Fragmentation

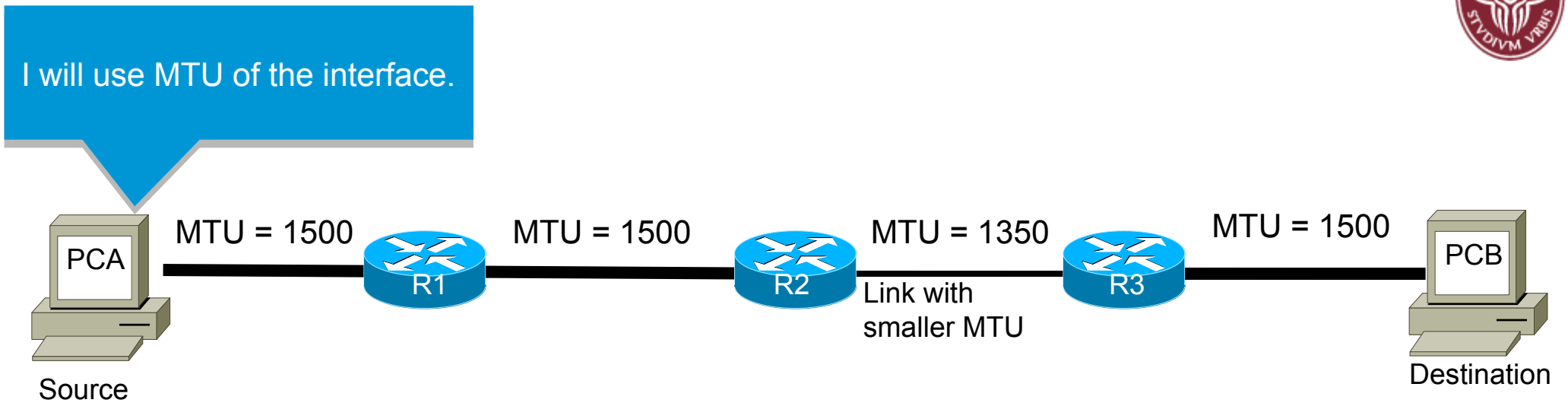


IPv4 Fragmentation

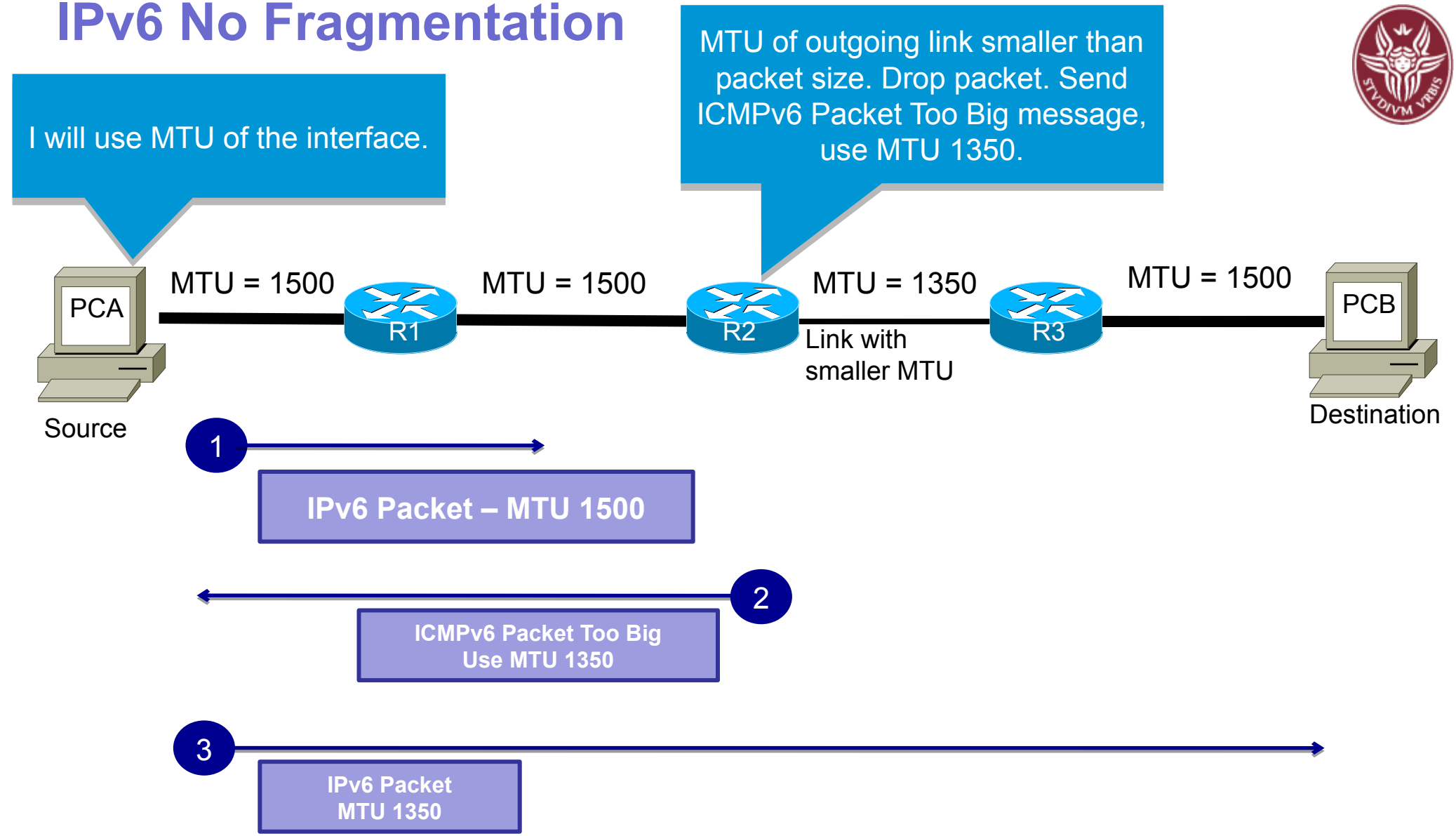


- IPv4 requires that every link have a minimum MTU of 68 bytes.
- Every internet destination must be able to receive a packet of 576 bytes either in one piece or in fragments to be reassembled.

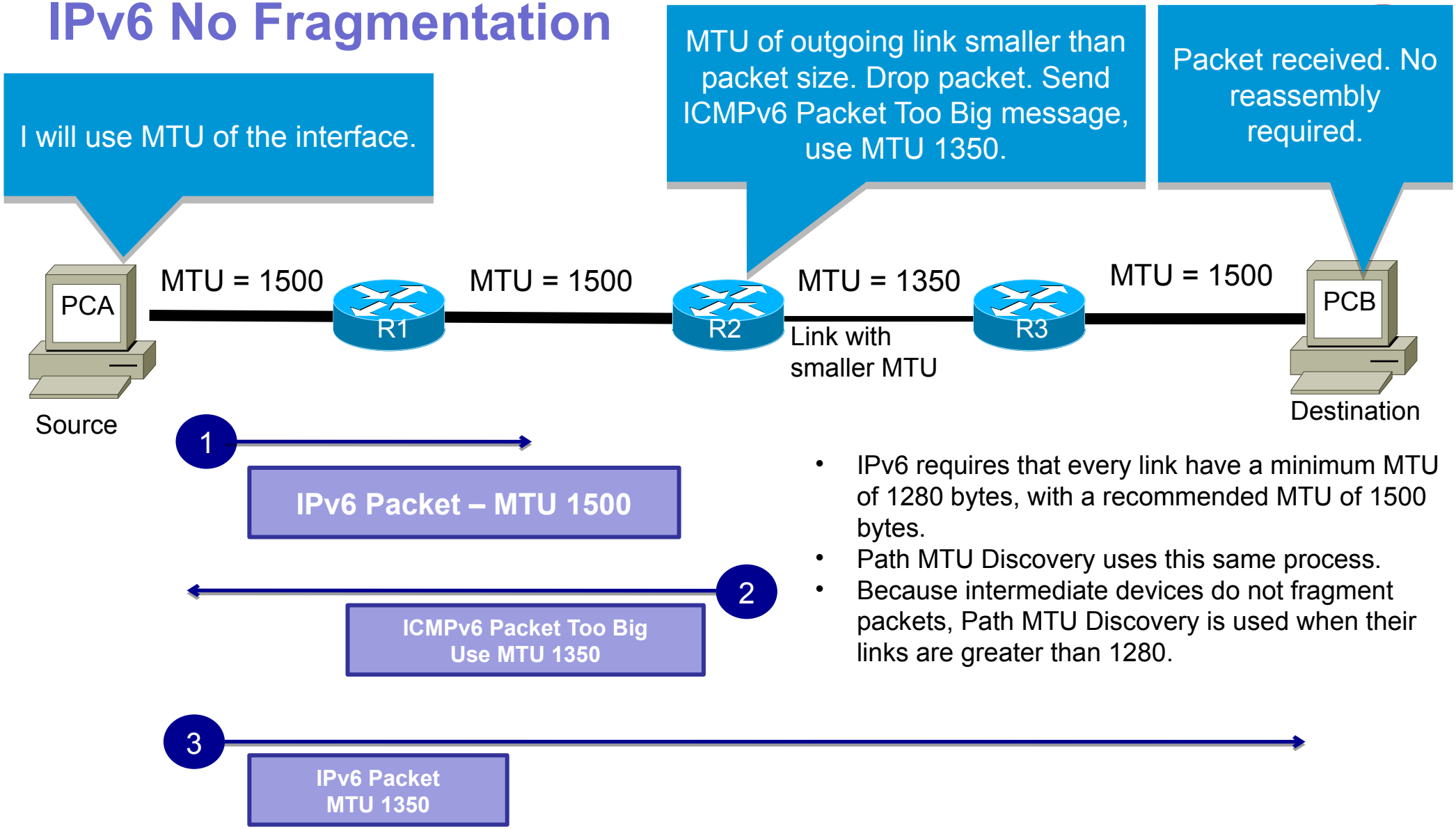
IPv6 No Fragmentation



IPv6 No Fragmentation



IPv6 No Fragmentation

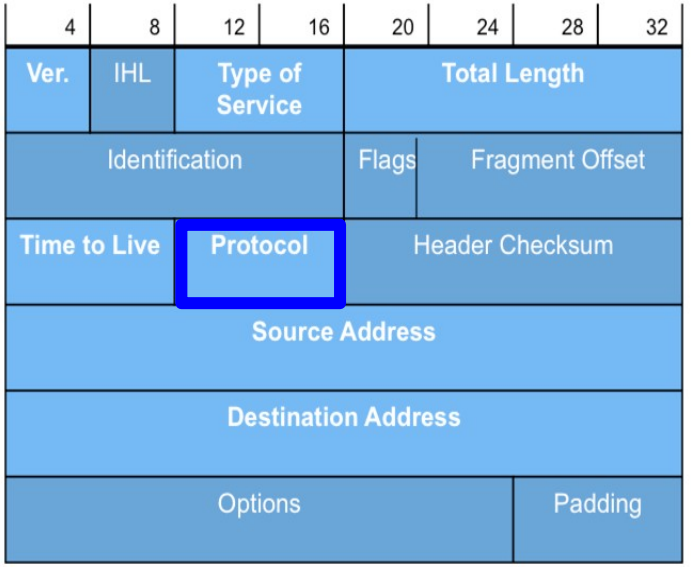


- IPv6 requires that every link have a minimum MTU of 1280 bytes, with a recommended MTU of 1500 bytes.
- Path MTU Discovery uses this same process.
- Because intermediate devices do not fragment packets, Path MTU Discovery is used when their links are greater than 1280.

IPv6 Next Header

- **IPv4 Protocol**
- **IPv6 Next Header**
- For both protocols, the field indicates the type of header following the IP header.

IPv4

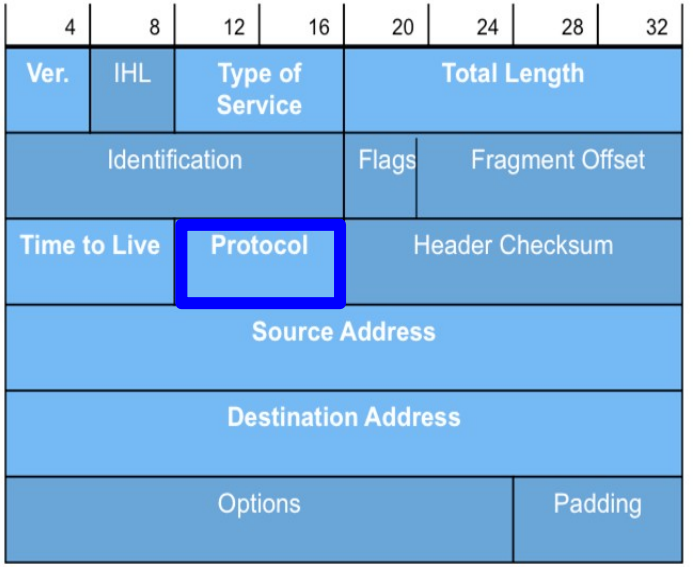


IPv6

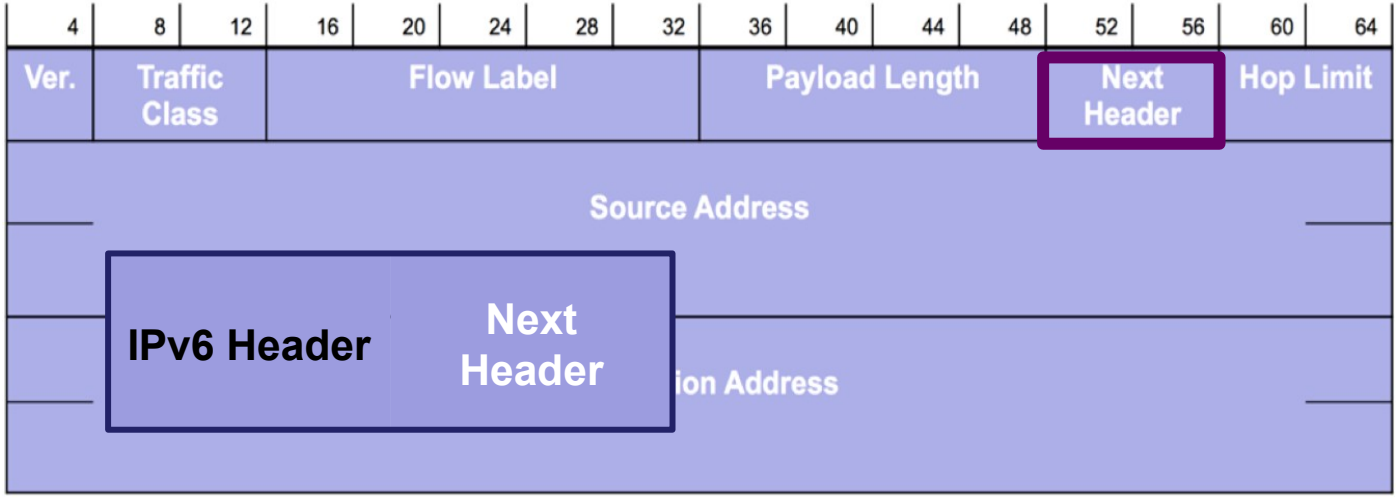
IPv6 Next Header

- **IPv4 Protocol**
- **IPv6 Next Header**
- For both protocols, the field indicates the type of header following the IP header.

IPv4



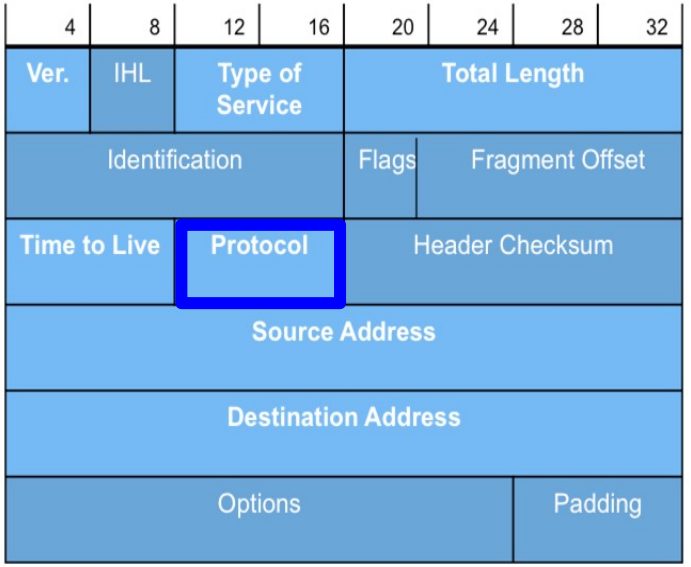
IPv6



IPv6 Next Header

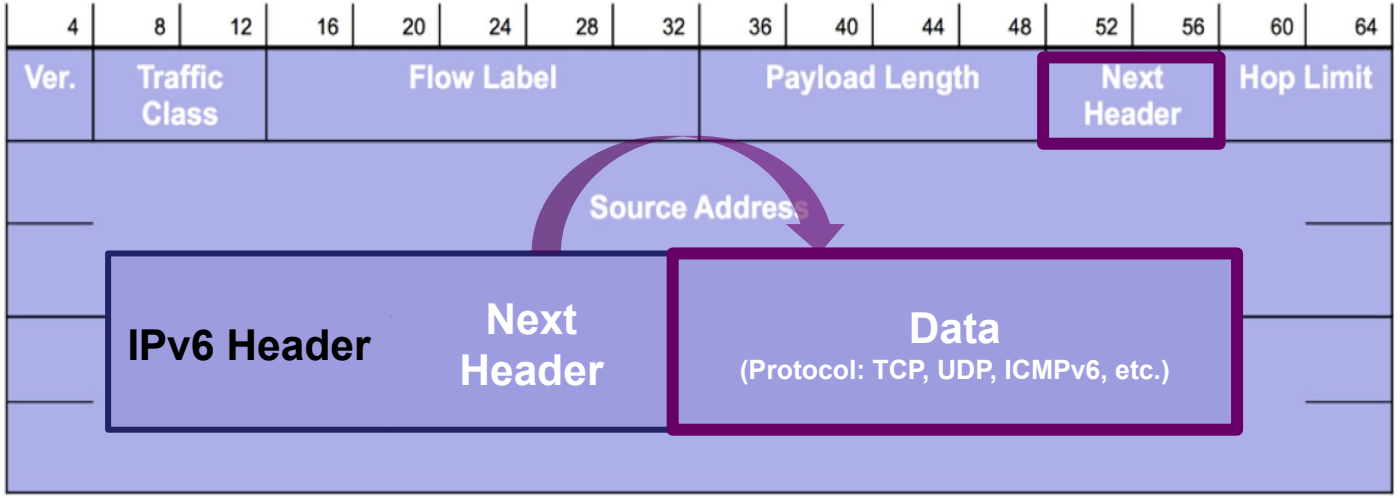
- **IPv4 Protocol**
- **IPv6 Next Header**
- For both protocols, the field indicates the type of header following the IP header.

IPv4



- Common values:
- 6 = TCP
- 17 = UDP
- 58 = ICMPv6
- 88 = EIGRP
- 89 = OSPF

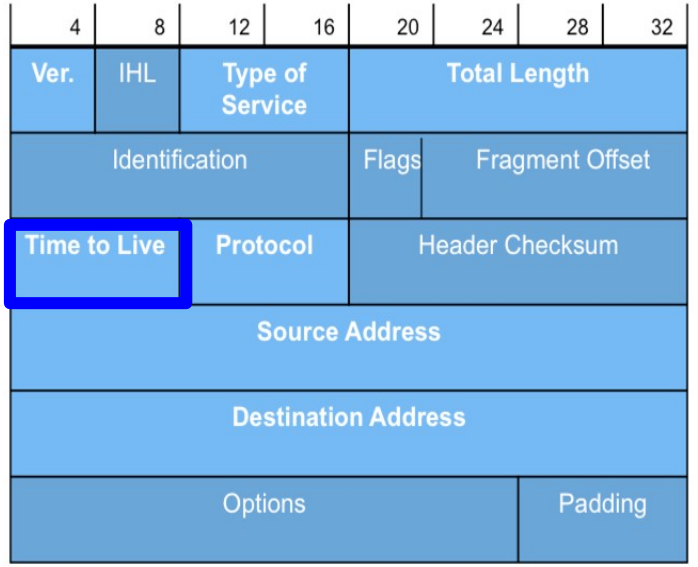
IPv6



IPv6 Hop Limit

- **IPv4 TTL (Time to Live)**
- **IPv6 Hop Limit**
- Renamed to more accurately reflect process.
- Set by source, every router in path decrements hop limit by 1.

IPv4



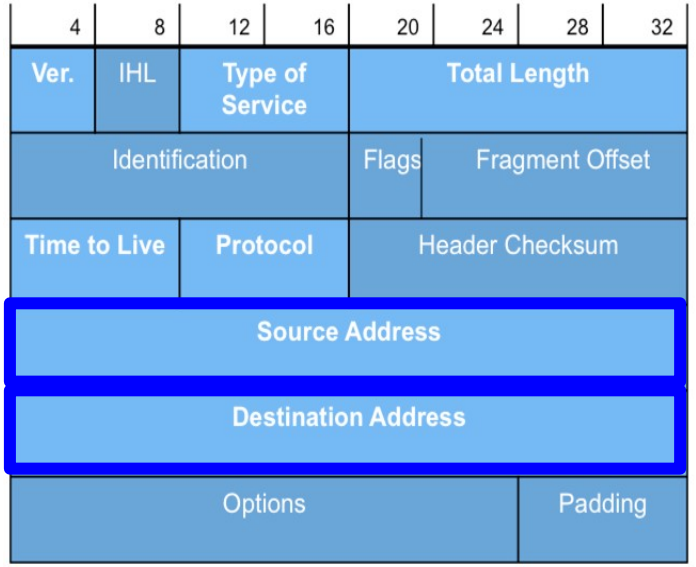
- When 0, drop packet.

IPv6

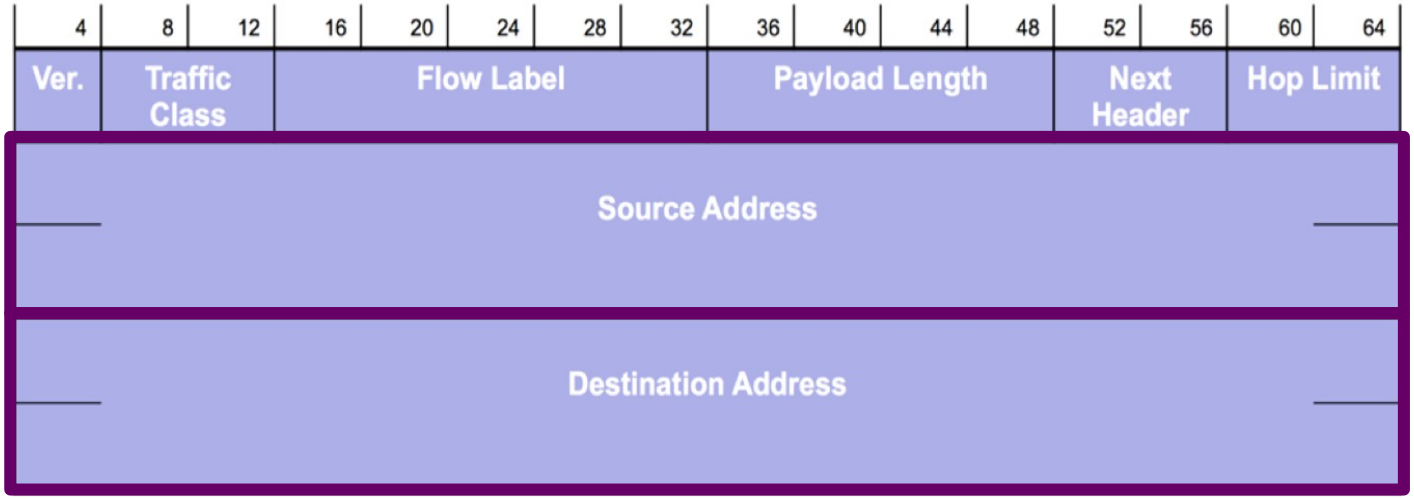
IPv6 Source and Destination Addresses

- **IPv6 Source** and **Destination** addresses have the same basic functionality as IPv4.
- IPv4 – 32-bit addresses.
- IPv6 – 128-bit addresses.
- Some significant changes in IPv6.

IPv4



IPv6

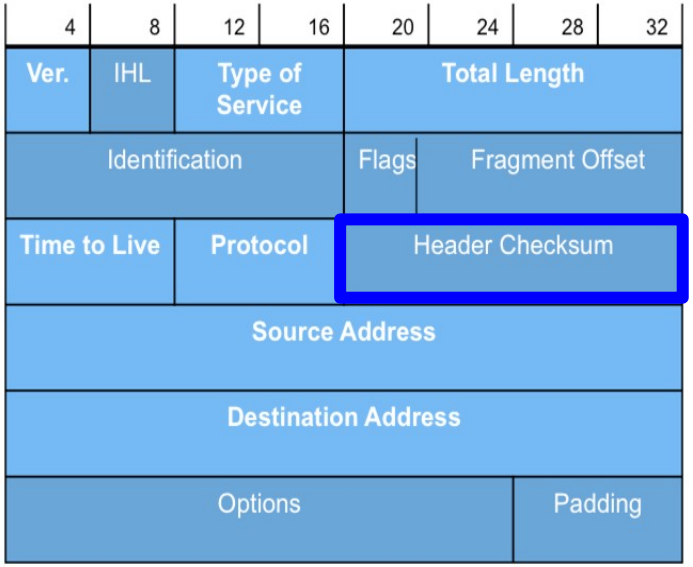


IPv4 Header Checksum

- **IPv4 Header Checksum**
- Not used in IPv6.
- Upper-layer protocols generally have a checksum (UDP and TCP).
- So, in IPv4 the UDP checksum is optional.

- Because it's not in IPv6, the UDP checksum is now mandatory.

IPv4

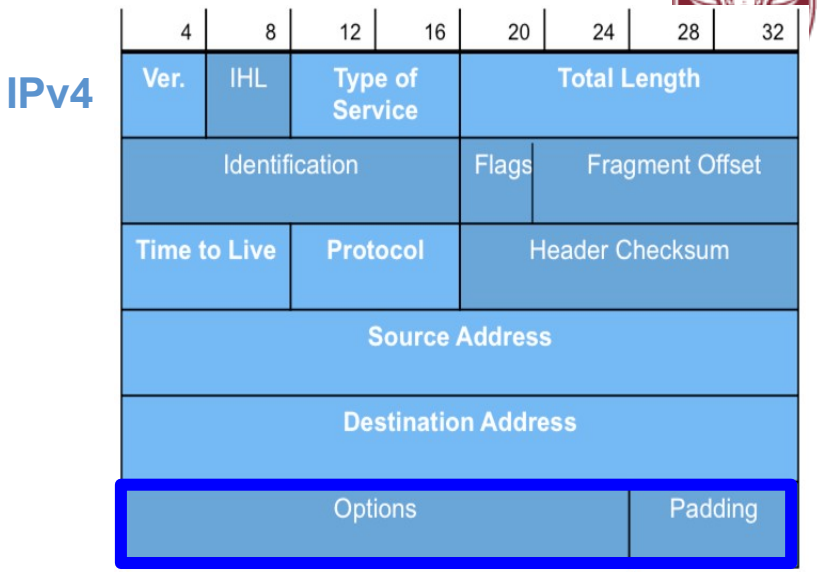


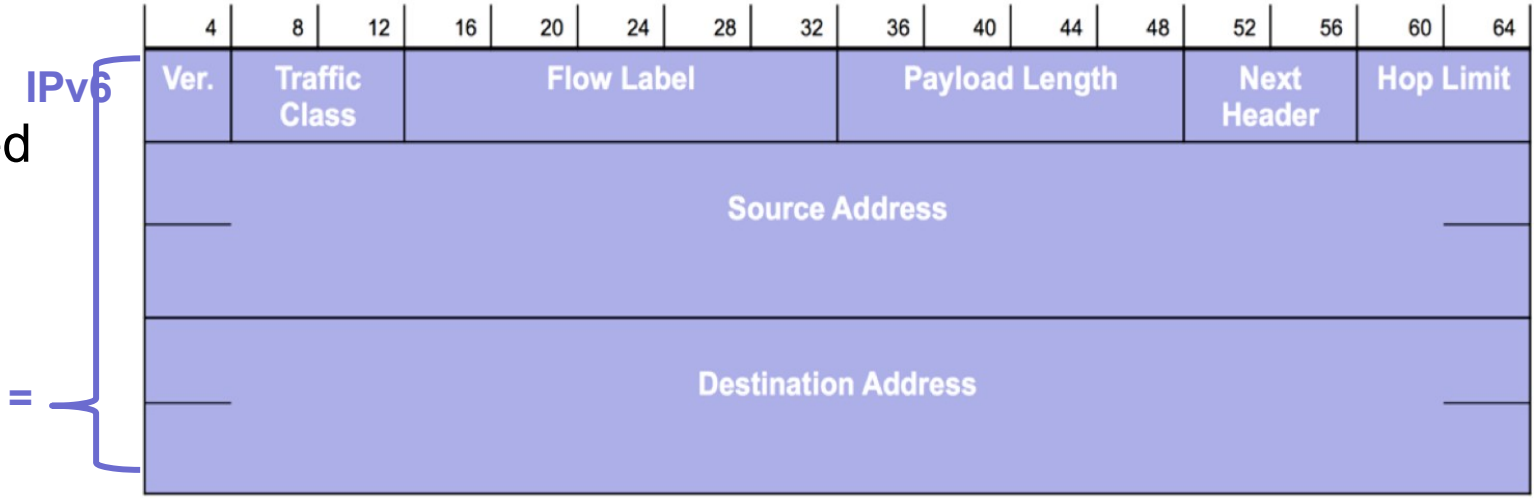
IPv6

IPv4 Options and Padding

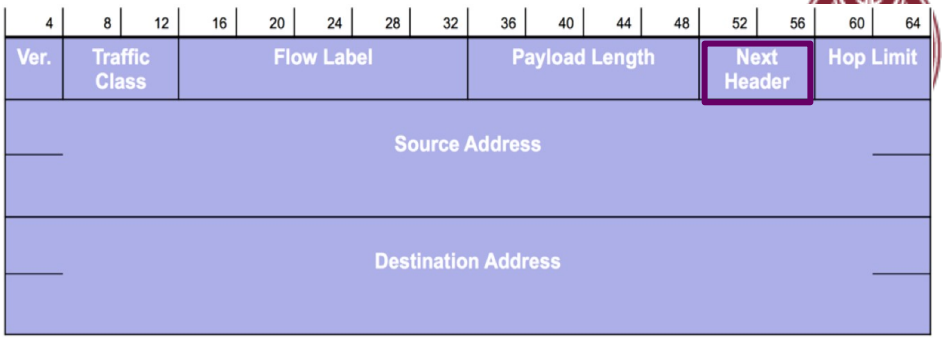
- **IPv4 Options** and **Padding**
- Not used in IPv6.
- Variable length, optional.
- **IPv4 Options** are handled using extension headers in IPv6.

- **Padding** makes sure IPv4 options fall on a 32-bit boundary.
- IPv6 header is fixed at 40 bytes.

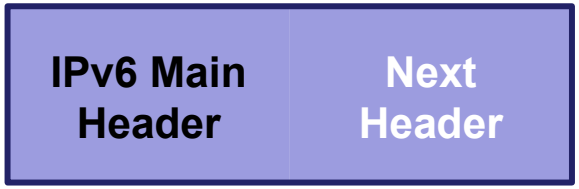




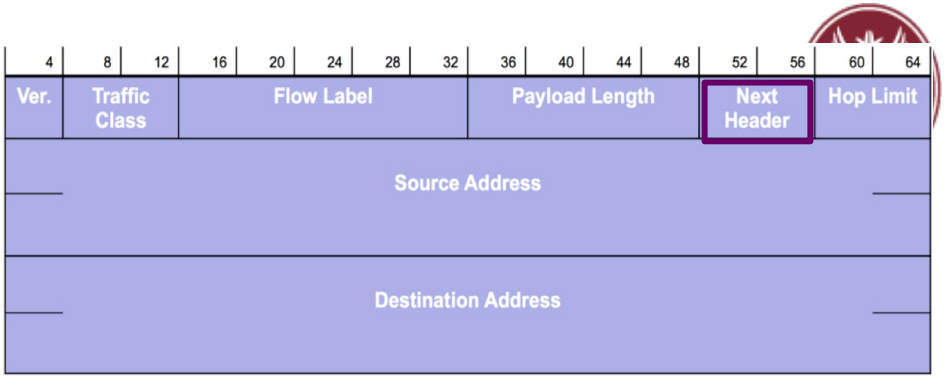
IPv6 Extension Header



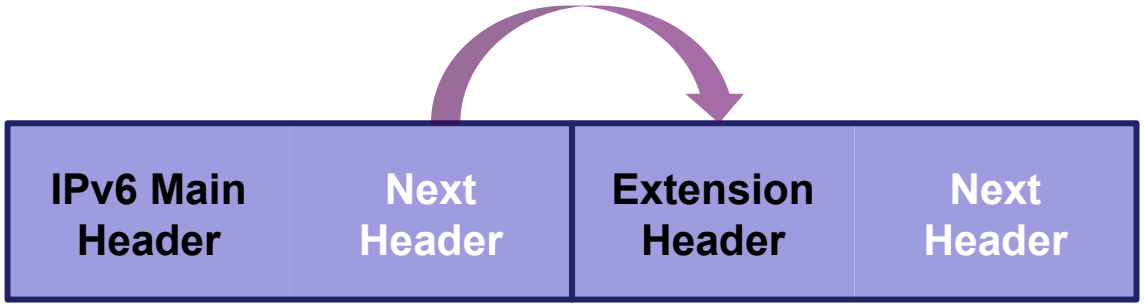
- **Next Header** identifies:
  - The protocol carried in the data portion of the packet.
  - The presence of an extension header.



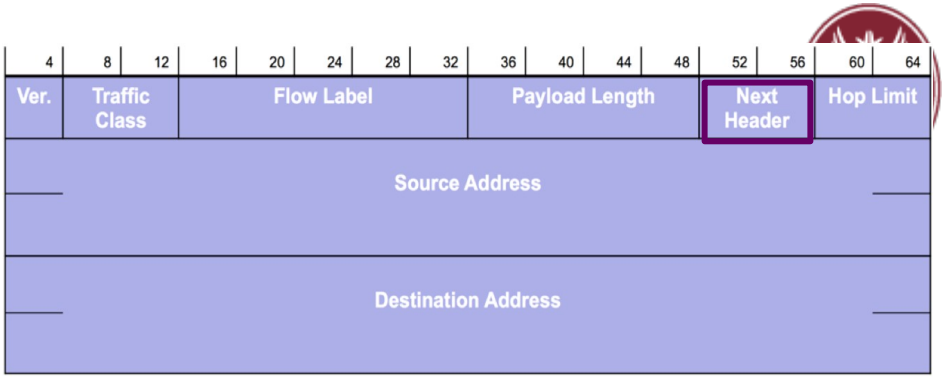
IPv6 Extension Header



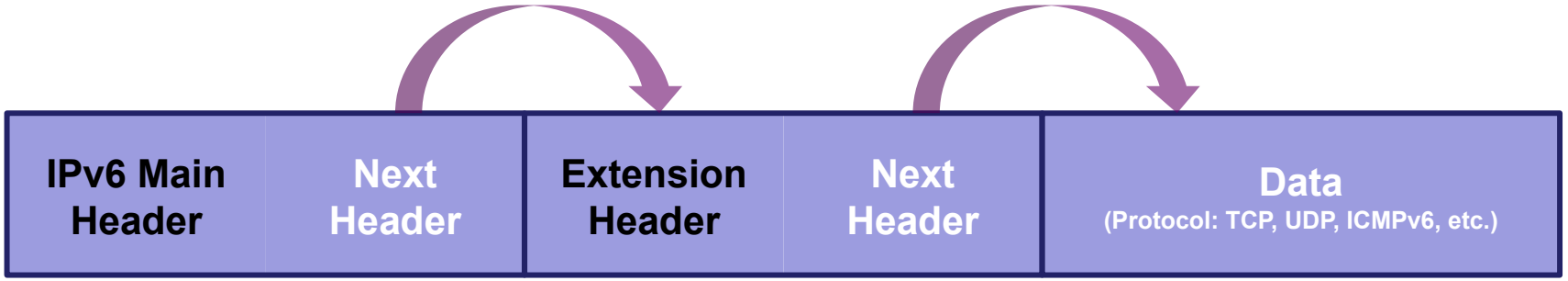
- **Next Header** identifies:
  - The protocol carried in the data portion of the packet.
  - The presence of an extension header.



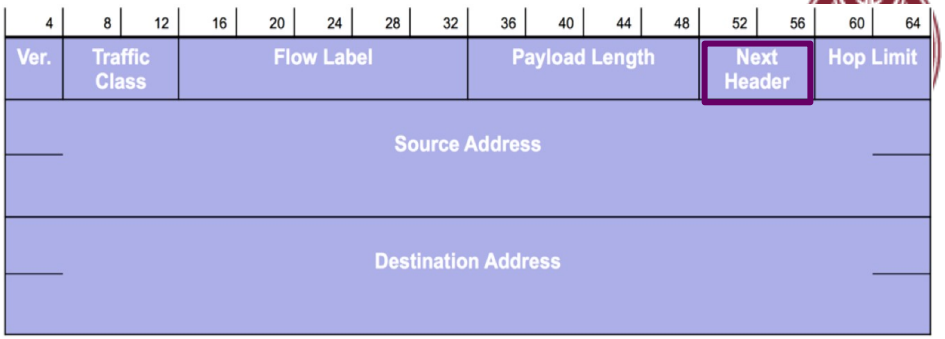
IPv6 Extension Header



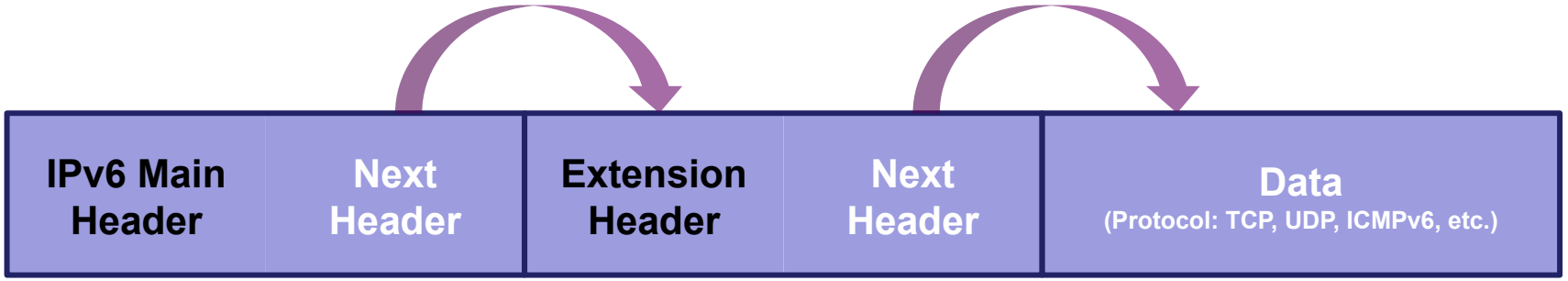
- **Next Header** identifies:
  - The protocol carried in the data portion of the packet.
  - The presence of an extension header.
- **Extension headers** are optional and follow the main IPv6 header.
- Provide flexibility and features to the main IPv6 header for future enhancements without having to redesign the entire protocol.



IPv6 Extension Header

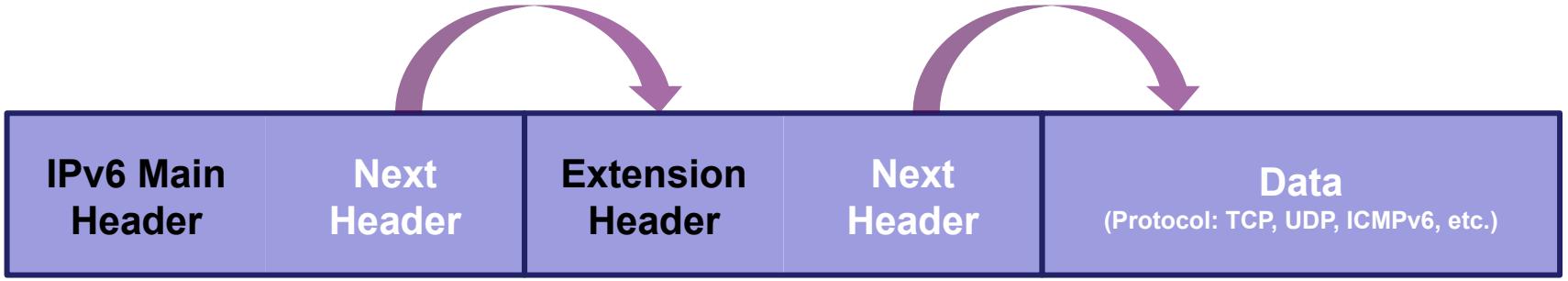


- **Next Header** identifies:
  - The protocol carried in the data portion of the packet.
  - The presence of an extension header.
- **Extension headers** are optional and follow the main IPv6 header.
- Provide flexibility and features to the main IPv6 header for future enhancements without having to redesign the entire protocol.
- Allows the main IPv6 header to have a fixed size for more efficient processing.



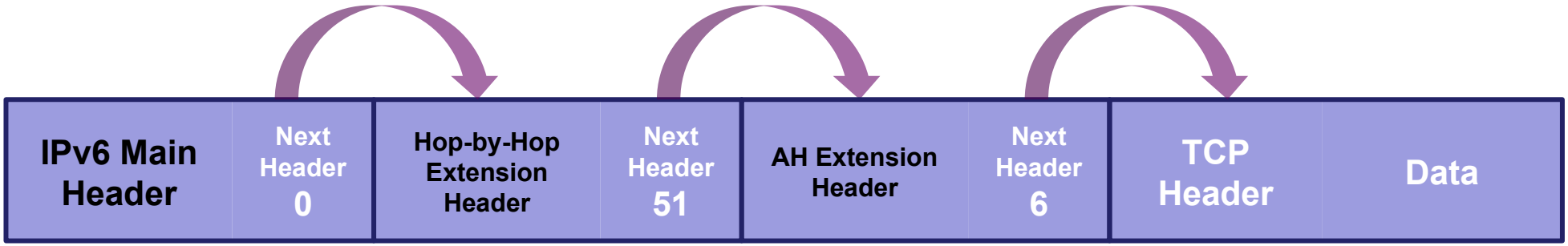
IPv6 Extension Header Properties

- **Flexible** (normally there are no EHs in IPv6 packets)
  - The use of EHs is optional, providing a powerful and flexible mechanism for IPv6
  - In the Basic IPv6 header, the EHs and the upper layer header (if used), are linked using the Next Header field. This is called the "**IPv6 Header Chain**"
- **Fixed** (Types and order)
  - The number of Extension Header types is fixed and standardised.
- **Processed only at endpoints** (Except Hop-by-Hop and Routing)
  - Packet processing complexity moved from the core to the edge of the Internet for improved IPv6 performances.

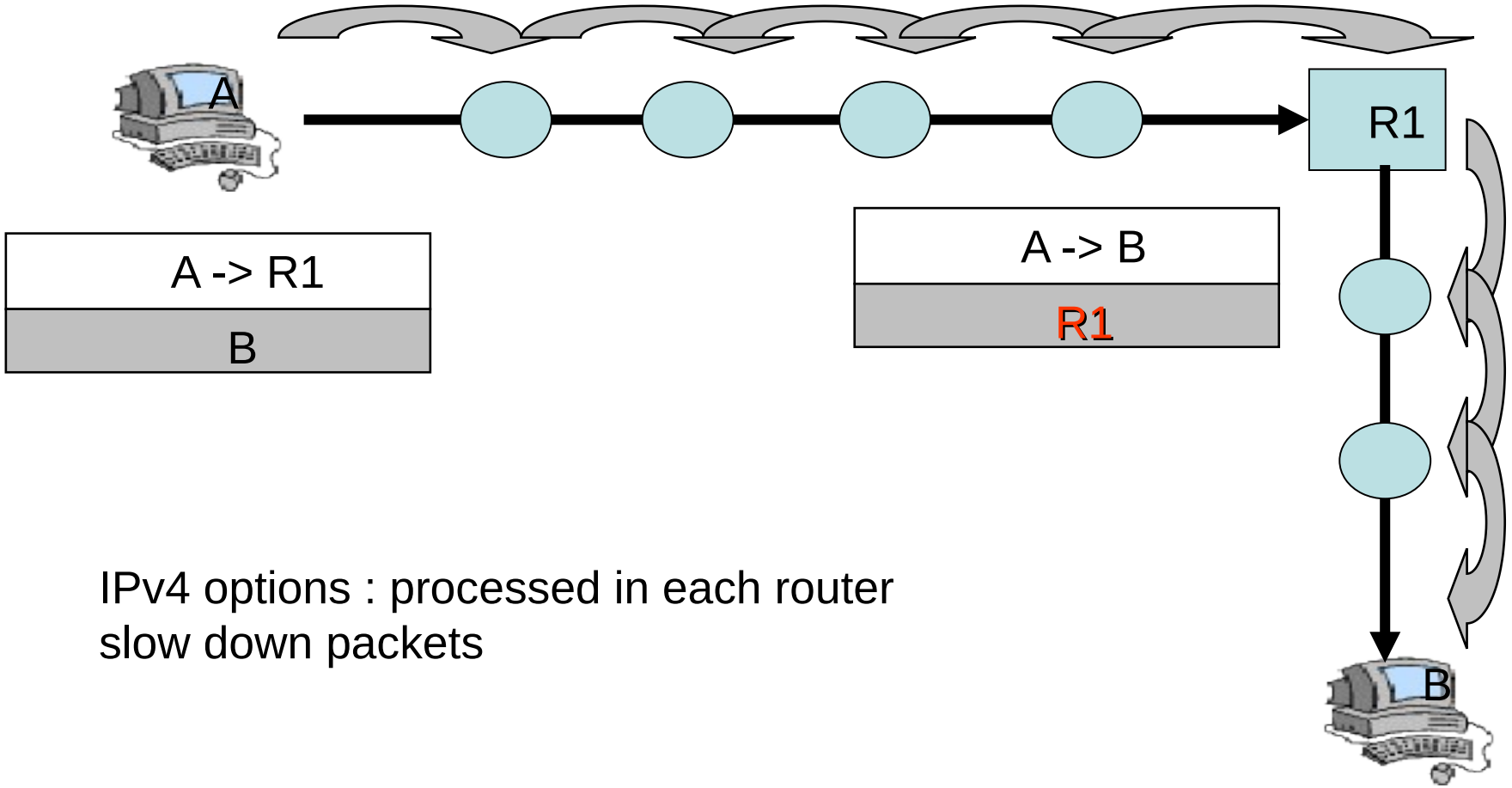


IPv6 Extension Header

Next Header Value (Decimal)	Extension Header Name	Extension Header Description
0	Hop-by-Hop Options	Used to carry optional information, which must be examined by every router along the path of the packet.
43	Routing	Allows the source of the packet to specify the path to the destination.
44	Fragment	Used to fragment IPv6 packets.
50	Encapsulating Security Payload (ESP)	Used to provide authentication, integrity, and encryption.
51	Authentication Header (AH)	Used to provide authentication and integrity.
60	Destination Options	Used to carry optional information that only needs to be examined by a packet's destination node(s).

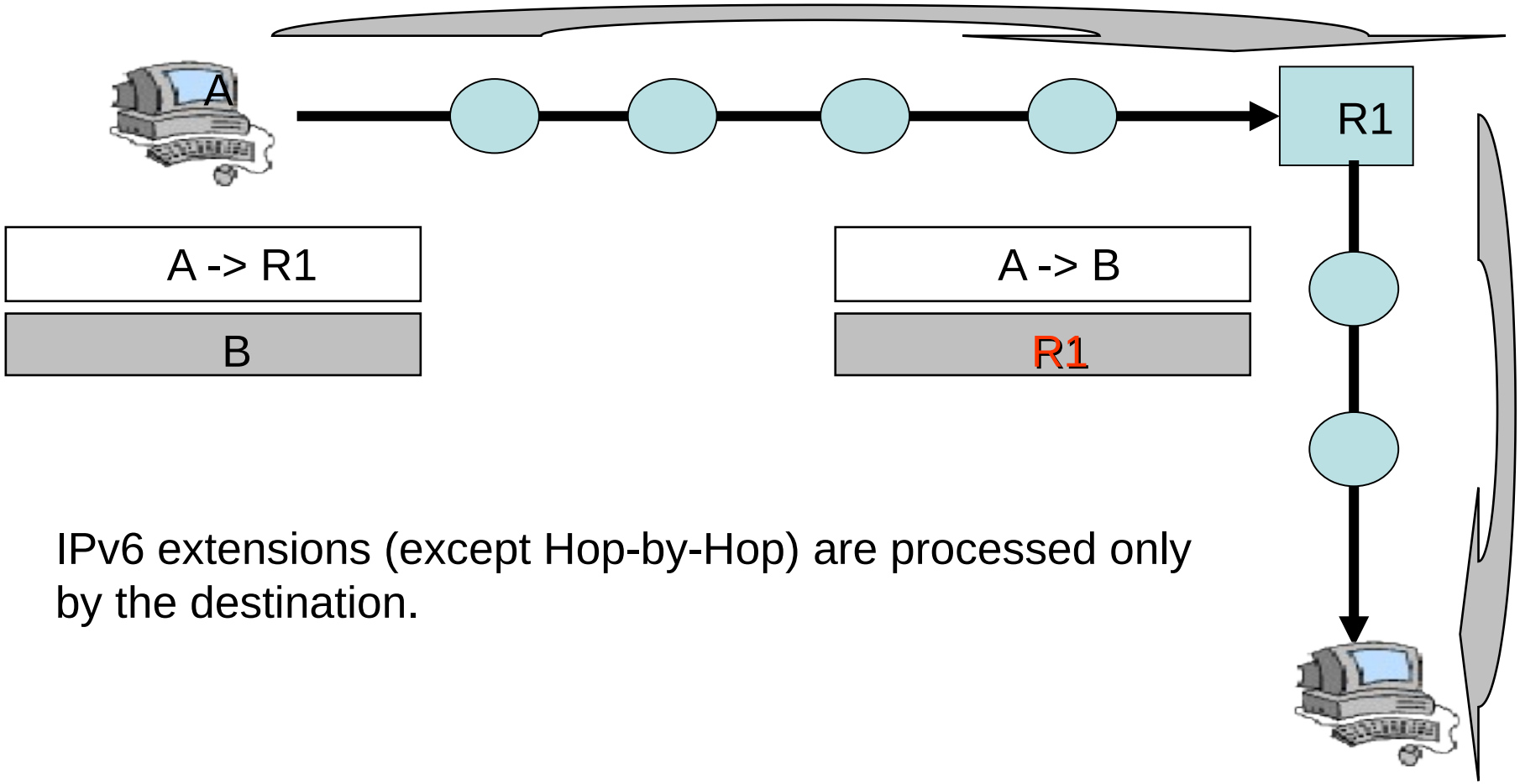


IPv4 options vs. IPv6 extensions



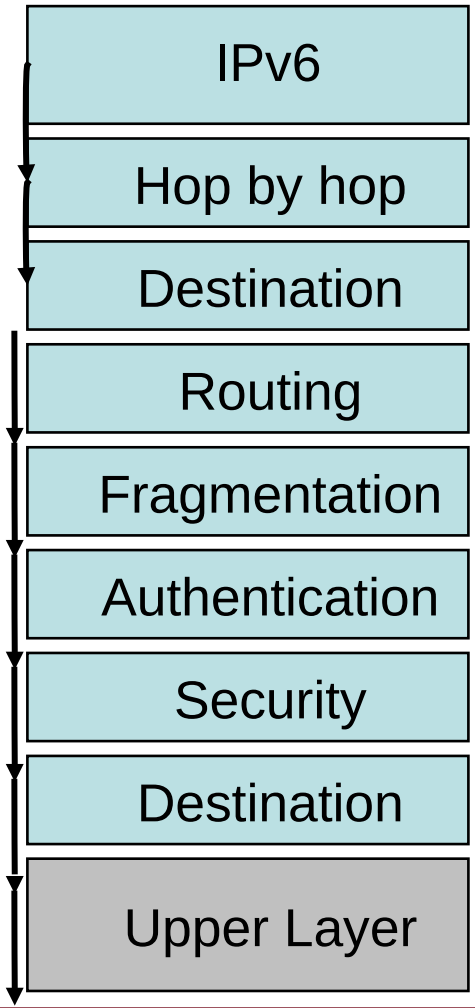
IPv4 options : processed in each router
slow down packets

IPv4 options vs. IPv6 extensions



IPv6 extensions (except Hop-by-Hop) are processed only by the destination.

Order is important (RFC 8600 Section 4)



Processed by every router

Processed by routers listed in Routing extension

List of routers to cross

Processed by the destination

After reassembling the packet

Cipher the content of the remaining information

Processed **only** by the destination

That's all for today

- **Questions?**
- See you next lecture!!
- References:
  - TCP-IP guide
    - http://www.tcpipguide.com/free/t_InternetProtocolVersion6IPv6IPNextGenerationIPng.htm
  - IPv6 Dissemination and Exploitation (6diss) European project
    - http://6diss.6deploy.eu/
  - Cabrillo's publications
    - http://www.cabrillo.edu/~rgraziani/ipv6-presentations.html
  - RIPE NCC Academy: *IPv6 Fundamentals (free course)*
    - https://academy.ripe.net/course/view.php?id=13
  - Networkacademy *(free course)*
    - https://www.networkacademy.io/ccna/ipv6
  - Book chapter 11 (even if quite obsoleted)