

# IP Versions

- ● IPv4
  - Current Internet version
  - 32-bit addresses
  - Many incremental improvements
- ● IPv6
  - Next generation Internet
  - 128-bit addresses
  - Optimization and simplifications
  - Mobility, security are integrated parts
- ● *IPv5*
  - *ST (Stream protocol) connection oriented protocol for real-time application*

# IP datagram

**VER**- protocol version( IPv4, IPv6)

**Hlen** (4 bits) The Internet Header Length (IHL) describes how big the header is in 32-bit words. For instance, the minimum value is 5

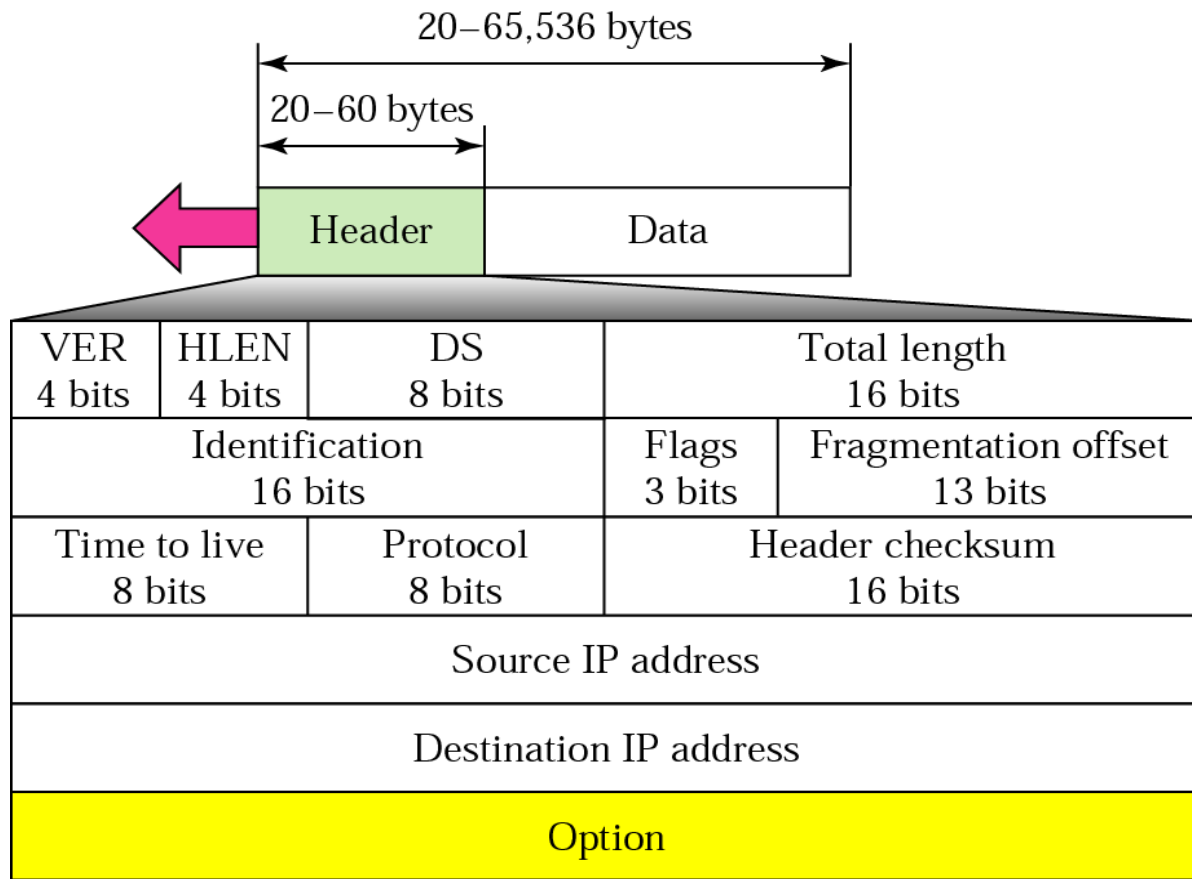
**DS** (8 bits) Type of service

**TTL** – each router decrement the value; TTL=1 the packet don't go outside of LAN

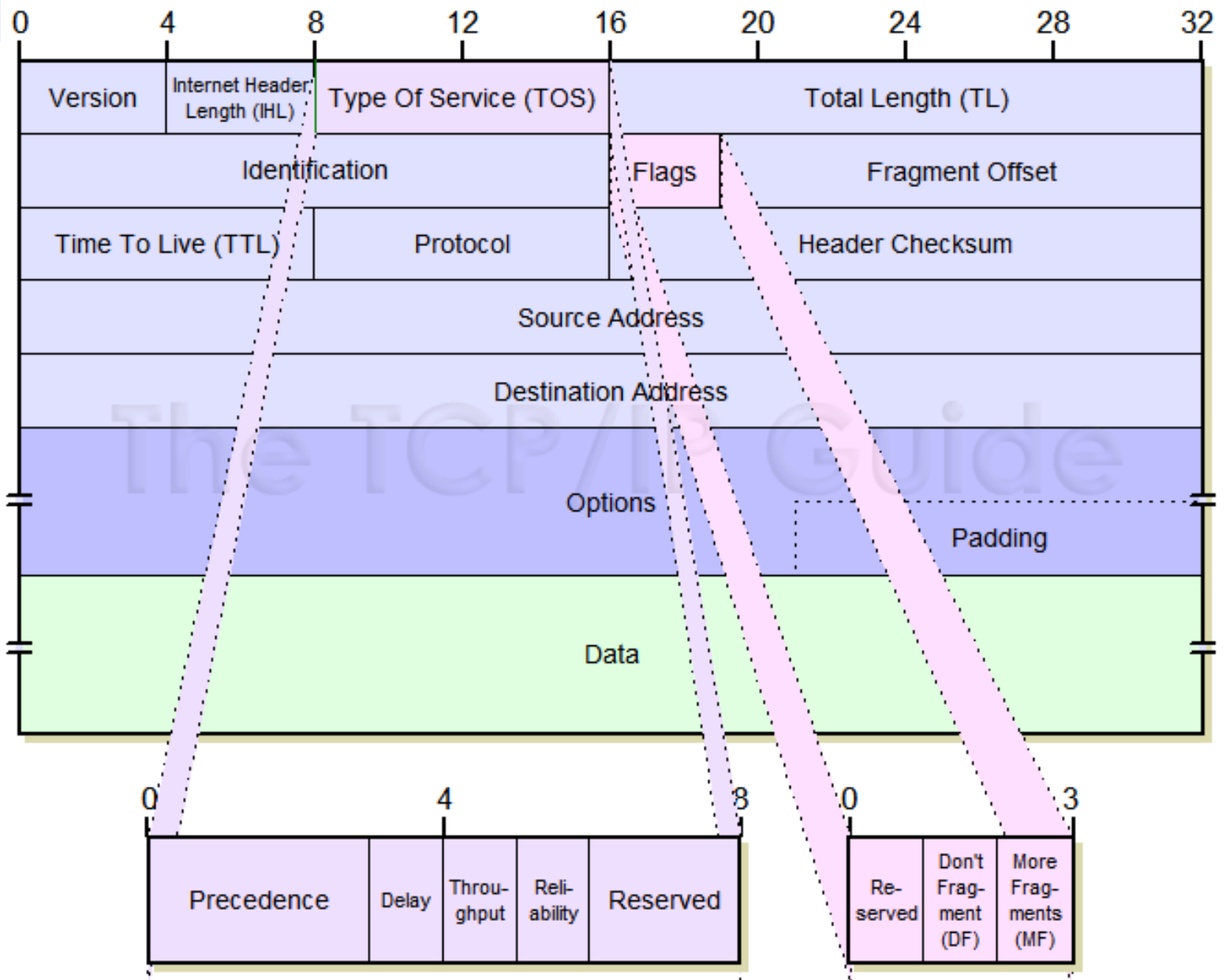
The **total length** field defines the total length of the datagram including the header.

**Protocol Field:** the values are common for IPv4 and IPv6

- 1 – ICMP for IPv4
- 2 – IGMP for IPv4
- 6 – TCP
- 17 – UDP
- 41 – IPv6
- 58 – ICMP for IPv6
- 89 - OSPF
- 132 - SCTP



# IPv4 Datagram format

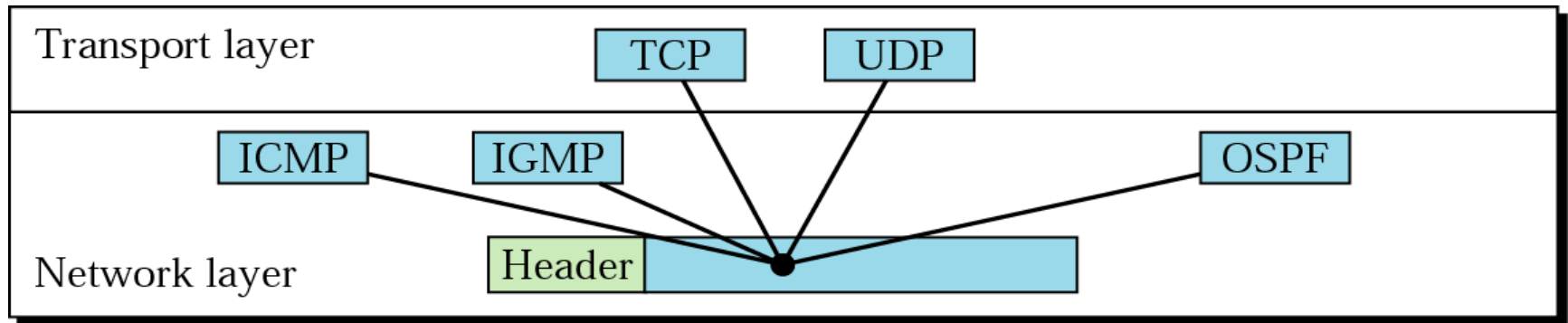


# Protocol field

*The values are common for IPv4 and IPv6*

Protocol Number	Protocol Name	Abbreviation
1	Internet Control Message Protocol	ICMP
2	Internet Group Management Protocol	IGMP
6	Transmission Control Protocol	TCP
17	User Datagram Protocol	UDP
41	IPv6 encapsulation	ENCAP
89	Open Shortest Path First	OSPF
132	Stream Control Transmission Protocol	SCTP

# Multiplexing



Address Resolution Protocol (**ARP**) uses broadcast ARP Request frames to resolve an IP address to a link-layer address.

Internet Group Management Protocol (**IGMP**) manages membership in local subnet groups.

Internet Control Management Protocol (**ICMP**) Router Discovery is used to determine the IPv4 address of the best default gateway, and it is optional.

Open Shortest Path First (**OSPF**) is a link state routing protocol.

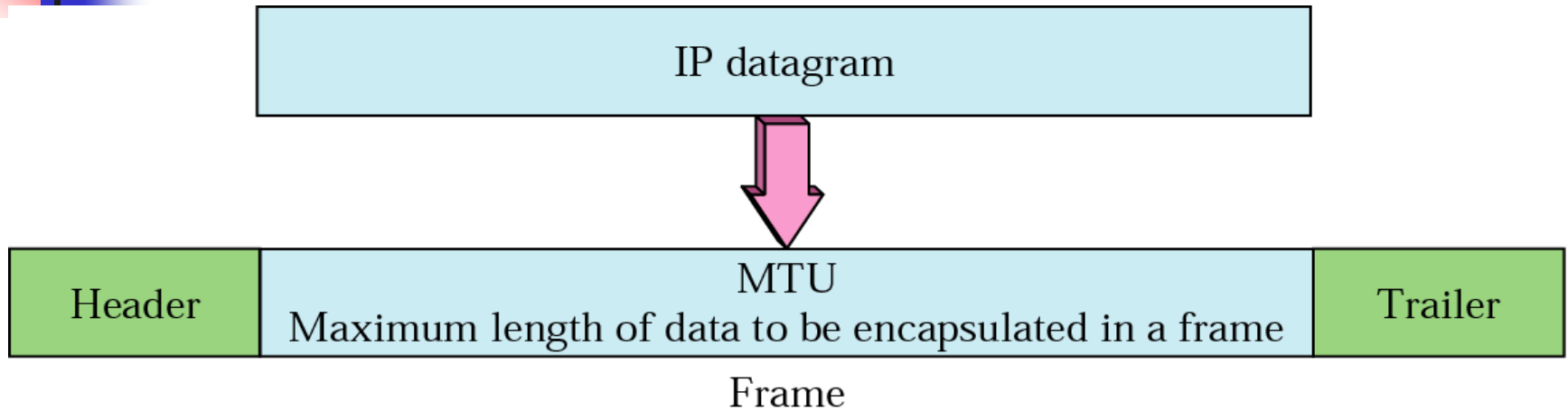
## Example of checksum calculation

4	5	0	28	
1			0	0
4	17	0		
10.12.14.5				
12.6.7.9				

4, 5, and 0 → 0100010100000000  
 28 → 00000000000011100  
 1 → 00000000000000001  
 0 and 0 → 00000000000000000  
 4 and 17 → 0000010000010001  
 0 → 00000000000000000  
 10.12 → 0000101000001100  
 14.5 → 0000111000000101  
 12.6 → 0000110000000110  
 7.9 → 0000011100001001  


---

 Sum → 0111010001001110  
 Checksum → 1000101110110001

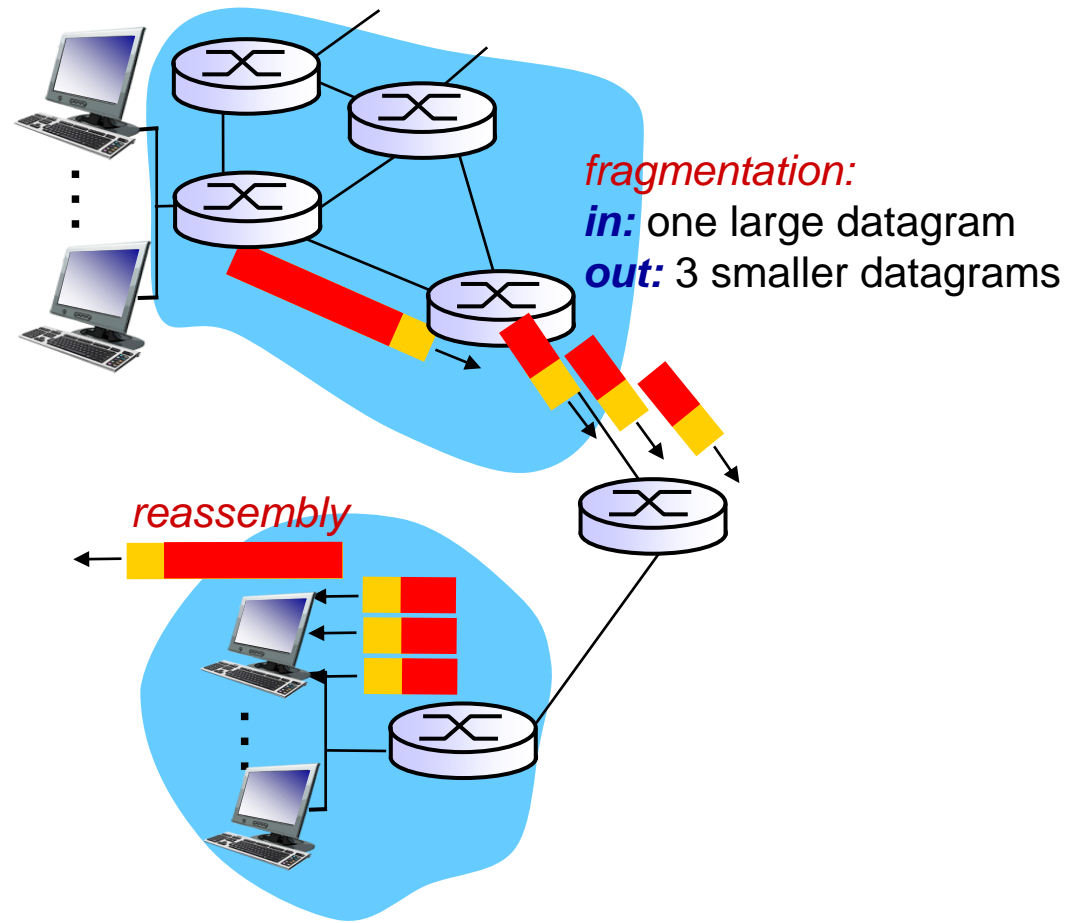


- The design accommodates networks of diverse physical nature; it is independent of the underlying transmission technology used in the Link Layer.
- Networks with different hardware usually vary not only in transmission speed, but also in the **maximum transmission unit** (MTU).
- When one network wants to transmit datagrams to a network with a smaller MTU, **it may fragment its datagrams**.
- In IPv4, this function was placed at the **Internet Layer**, and is performed in IPv4 routers, which thus only require this layer as the highest one implemented in their design.

In contrast, IPv6, does not allow routers to perform fragmentation

# IP fragmentation, reassembly

- network links have MTU (max.transfer size) - largest possible link-level frame
  - different link types, different MTUs
- large IP datagram divided (“fragmented”) within net
  - one datagram becomes several datagrams
  - “reassembled” only at final destination
  - IP header bits used to identify, order related fragments





# IP fragmentation, reassembly

## *example:*

- ❖ 4000 byte datagram
- ❖ MTU = 1500 bytes

	length	ID	fragflag	offset	
	=4000	=x	=0	=0	

*one large datagram becomes  
several smaller datagrams*

1480 bytes in  
data field

offset =  
 $1480/8$

	length	ID	fragflag	offset	
	=1500	=x	=1	=0	

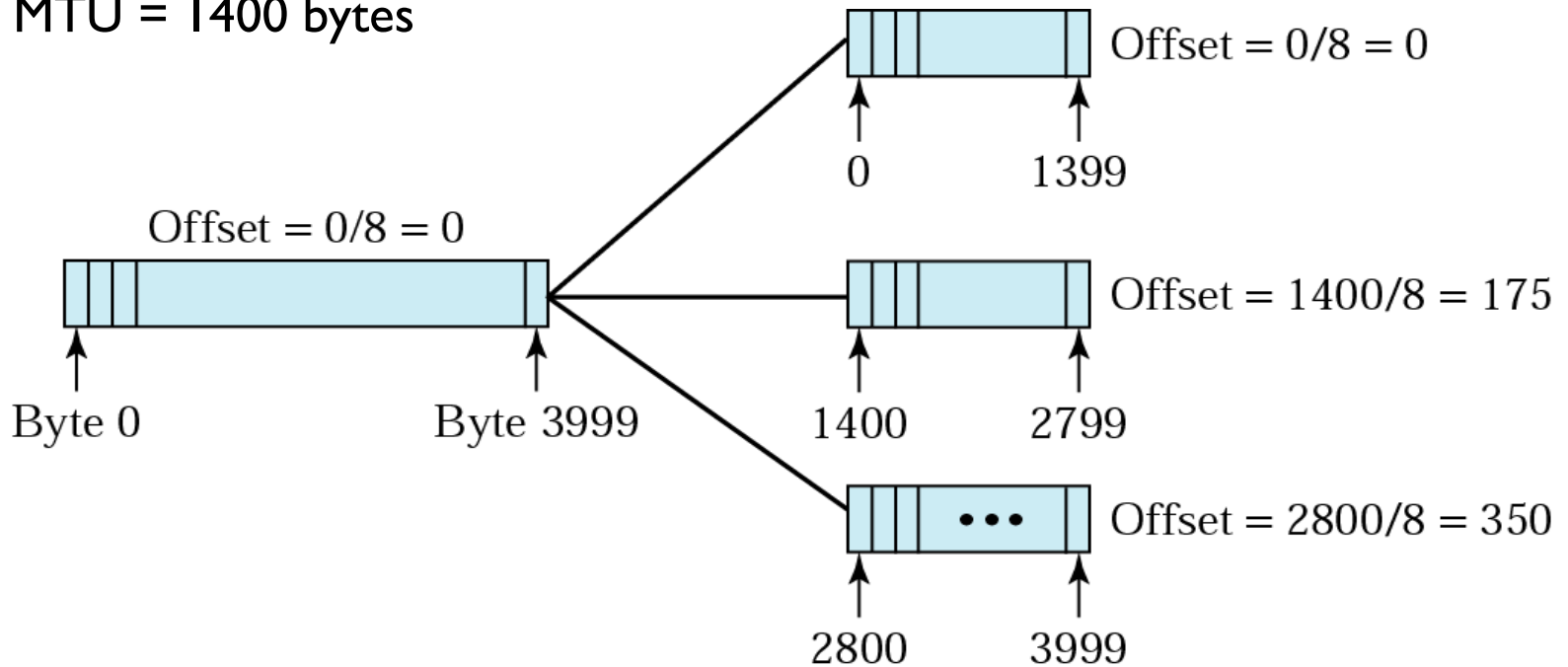
	length	ID	fragflag	offset	
	=1500	=x	=1	=185	

	length	ID	fragflag	offset	
	=1040	=x	=0	=370	

## Fragmentation example

### *example:*

- ❖ 4000 byte datagram
- ❖ MTU = 1400 bytes



# IPv4 features

## IPv4

- Source and destination addresses are 32 bits (4 bytes) in length.
- IPsec support is optional.
- IPv4 header does not identify packet flow for QoS handling by routers.
- Both routers and the sending host fragment packets.
- Header includes a checksum.
- Header includes options.
- Address Resolution Protocol (ARP) uses broadcast ARP Request frames to resolve an IP address to a link-layer address.
- Internet Group Management Protocol (IGMP) manages membership in local subnet groups.
- Internet Control Management Protocol (ICMP) Router Discovery is used to determine the IPv4 address of the best default gateway, and it is optional.
- Broadcast addresses are used to send traffic to all nodes on a subnet.
- Address must be configured either manually or through DHCP.
- Uses host address (A) resource records in Domain Name System (DNS) to map host names to IPv4 addresses.
- Uses pointer (PTR) resource records in the IN-ADDR.ARPA DNS domain to map IPv4 addresses to host names.
- Must support a 576-byte packet size (possibly fragmented).

# Technical Problems with IPv4

- • Limited number and types of addresses
  - Bad planning of address assignment gives an inefficient utilization of the address space
- • “Things that think” – auto configuration
  - Does not manage the growth. Address space full ~ 2015?
- • Address structure gives large routing tables
  - Bad address hierarchy
  - Supernetworking
- • Missing support for new services
  - No QoS guarantee
  - Mobility, multicast
- • Missing security mechanisms

# IPV6 :

- [Technet IPv6 Tutorial](#)
- [IPv6 basics pdf -Cisco](#)
- [Tutorial-ipv6-basics.pdf- from cisco](#)
- [IPV6 on Tutorials point](#)
- [IPV6 Wiki](#)

# IPv6

[https://www.tutorialspoint.com/ipv6/ipv6\\_features.htm](https://www.tutorialspoint.com/ipv6/ipv6_features.htm)

The successor of IPv4 is not designed to be backward compatible. Trying to keep the basic functionalities of IP addressing, IPv6 is redesigned entirely. It offers the following features:

- **Larger Address Space**

In contrast to IPv4, IPv6 uses 4 times more bits to address a device on the Internet. This much of extra bits can provide approximately  $3.4 \times 10^{38}$  different combinations of addresses. This address can accumulate the aggressive requirement of address allotment for almost everything in this world. According to an estimate, 1564 addresses can be allocated to every square meter of this earth.

- **Simplified Header**

IPv6's header has been simplified by moving all unnecessary information and options (which are present in IPv4 header) to the end of the IPv6 header. IPv6 header is only twice as bigger than IPv4 provided the fact that IPv6 address is four times longer.

# IPv 6 cont

- **End-to-end Connectivity**

Every system now has unique IP address and can traverse through the Internet without using NAT or other translating components. After IPv6 is fully implemented, every host can directly reach other hosts on the Internet, with some limitations involved like Firewall, organization policies, etc.

- **Auto-configuration**

IPv6 supports both stateful and stateless auto configuration mode of its host devices. This way, absence of a DHCP server does not put a halt on inter segment communication.

- **Faster Forwarding/Routing**

Simplified header puts all unnecessary information at the end of the header. The information contained in the first part of the header is adequate for a Router to take routing decisions, thus making routing decision as quickly as looking at the mandatory header.

# IPv6 cont

- **IPSec**

Initially it was decided that IPv6 must have IPSec security, making it more secure than IPv4. This feature has now been made optional.

- **No Broadcast**

Though Ethernet/Token Ring are considered as broadcast network because they support Broadcasting, IPv6 does not have any broadcast support any more.

It uses multicast to communicate with multiple hosts.

- **Anycast Support**

This is another characteristic of IPv6. IPv6 has introduced Anycast mode of packet routing. In this mode, multiple interfaces over the Internet are assigned same Anycast IP address. Routers, while routing, send the packet to the nearest destination.

- **Mobility**

IPv6 was designed keeping mobility in mind. This feature enables hosts (such as mobile phone) to roam around in different geographical area and remain connected with the same IP address. The mobility feature of IPv6 takes advantage of auto IP configuration and Extension headers.



# IPv6 cont

- **Enhanced Priority Support**

IPv4 used 6 bits DSCP (Differential Service Code Point) and 2 bits ECN (Explicit Congestion Notification) to provide Quality of Service but it could only be used if the end-to-end devices support it, that is, the source and destination device and underlying network must support it.

In IPv6, Traffic class and Flow label are used to tell the underlying routers how to efficiently process the packet and route it.

- **Smooth Transition**

Large IP address scheme in IPv6 enables to allocate devices with globally unique IP addresses. This mechanism saves IP addresses and NAT is not required. So devices can send/receive data among each other, for example, VoIP and/or any streaming media can be used much efficiently.

Other fact is, the header is less loaded, so routers can take forwarding decisions and forward them as quickly as they arrive.

- **Extensibility**

One of the major advantages of IPv6 header is that it is extensible to add more information in the option part. IPv4 provides only 40-bytes for options, whereas options in IPv6 can be as much as the size of IPv6 packet itself.

# IPv6 features

## IPv6

- Source and destination **addresses are 128 bits** (16 bytes) in length.
- **IPSec support** is required.
- IPv6 header contains Flow Label field, which identifies **packet flow for QoS** handling by router.
- Only the sending host fragments packets; routers do not.
- Header does **not include a checksum**.
- All **optional data is moved to IPv6 extension headers**.
- **Multicast Neighbor Solicitation** messages resolve IP addresses to link-layer addresses.
- Multicast Listener Discovery (MLD) messages manage membership in local subnet groups.
- ICMPv6 Router Solicitation and Router Advertisement messages are **used to determine the IP address of the best default gateway**, and they are required.
- IPv6 uses a link-local scope all-nodes multicast address.
- Does **not require manual configuration or DHCP**.
- Uses host address (AAAA) resource records in DNS to map host names to IPv6 addresses.
- Uses pointer (PTR) resource records in the IP6.ARPA DNS domain to map IPv6 addresses to host names.
- **Support a 1280-byte packet size (without fragmentation)**.

# PACKET FORMAT

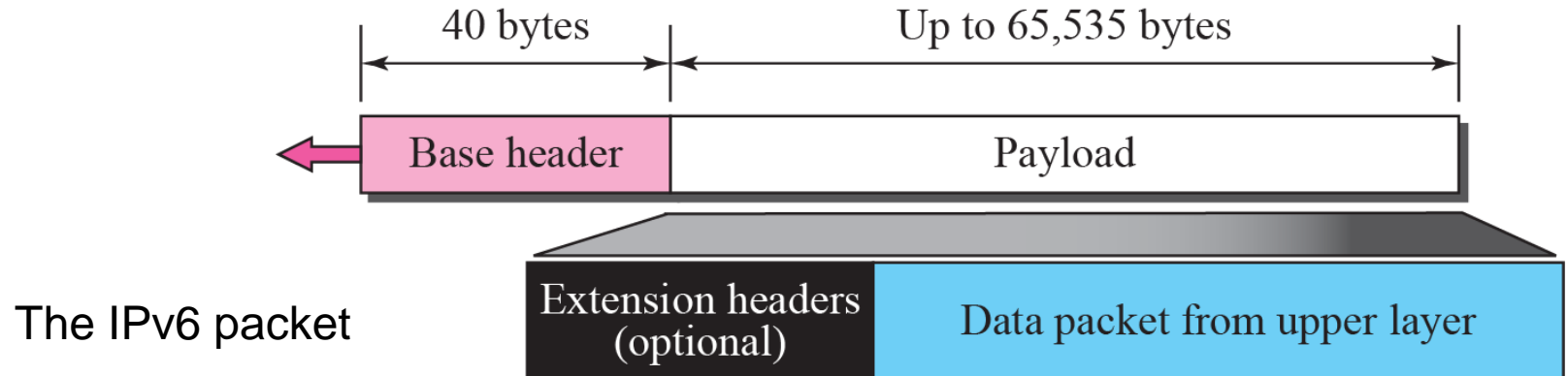
Each packet is composed of a mandatory:

**base header** followed by the **payload**.

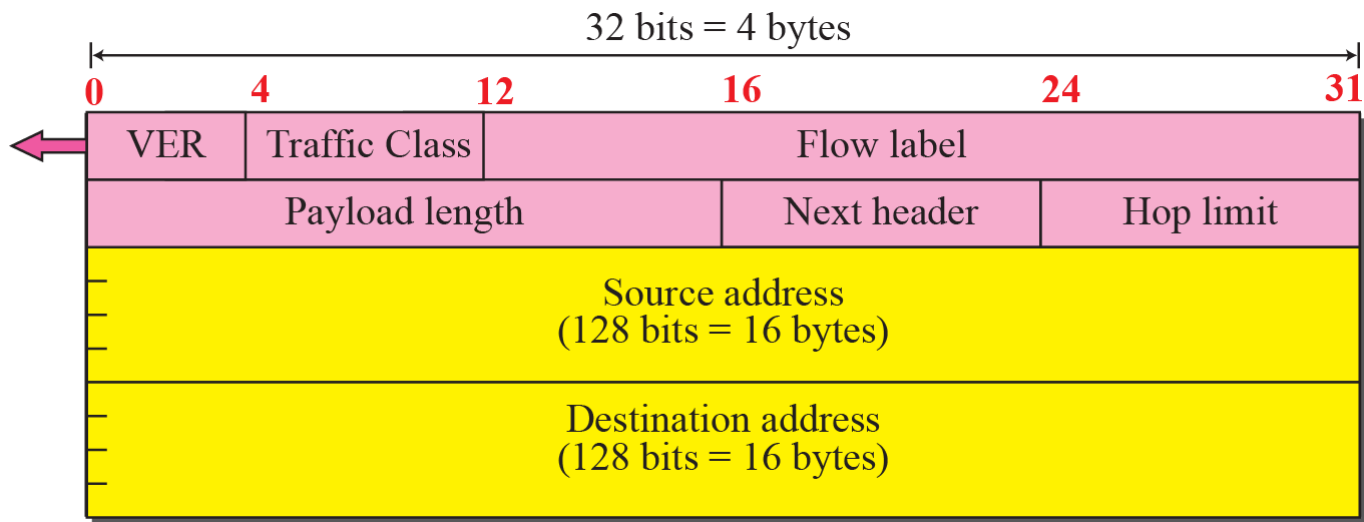
The **base header** occupies 40 bytes, whereas the extension headers and data from the upper layer contain up to 65,535 bytes of information.

The **payload** consists of two parts:

- optional extension headers and
- data from an upper layer.




# IPv6



## IPv6 base header contains the following things:

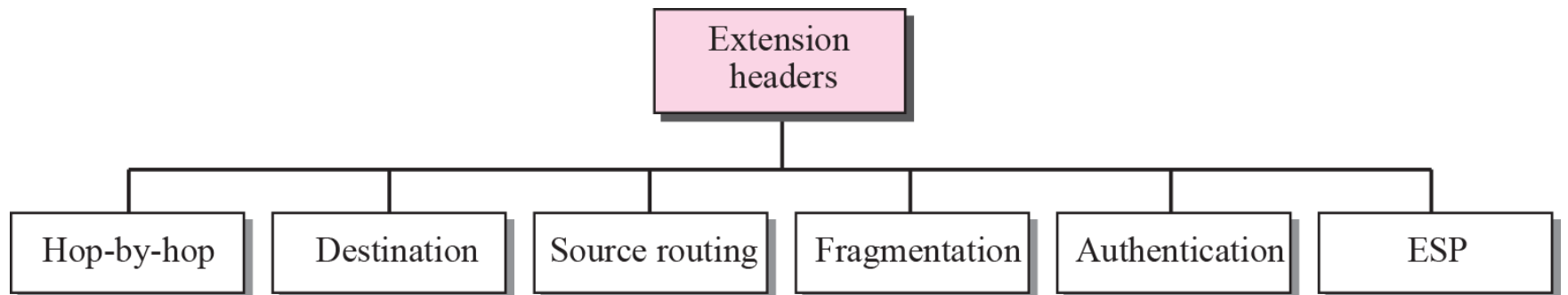
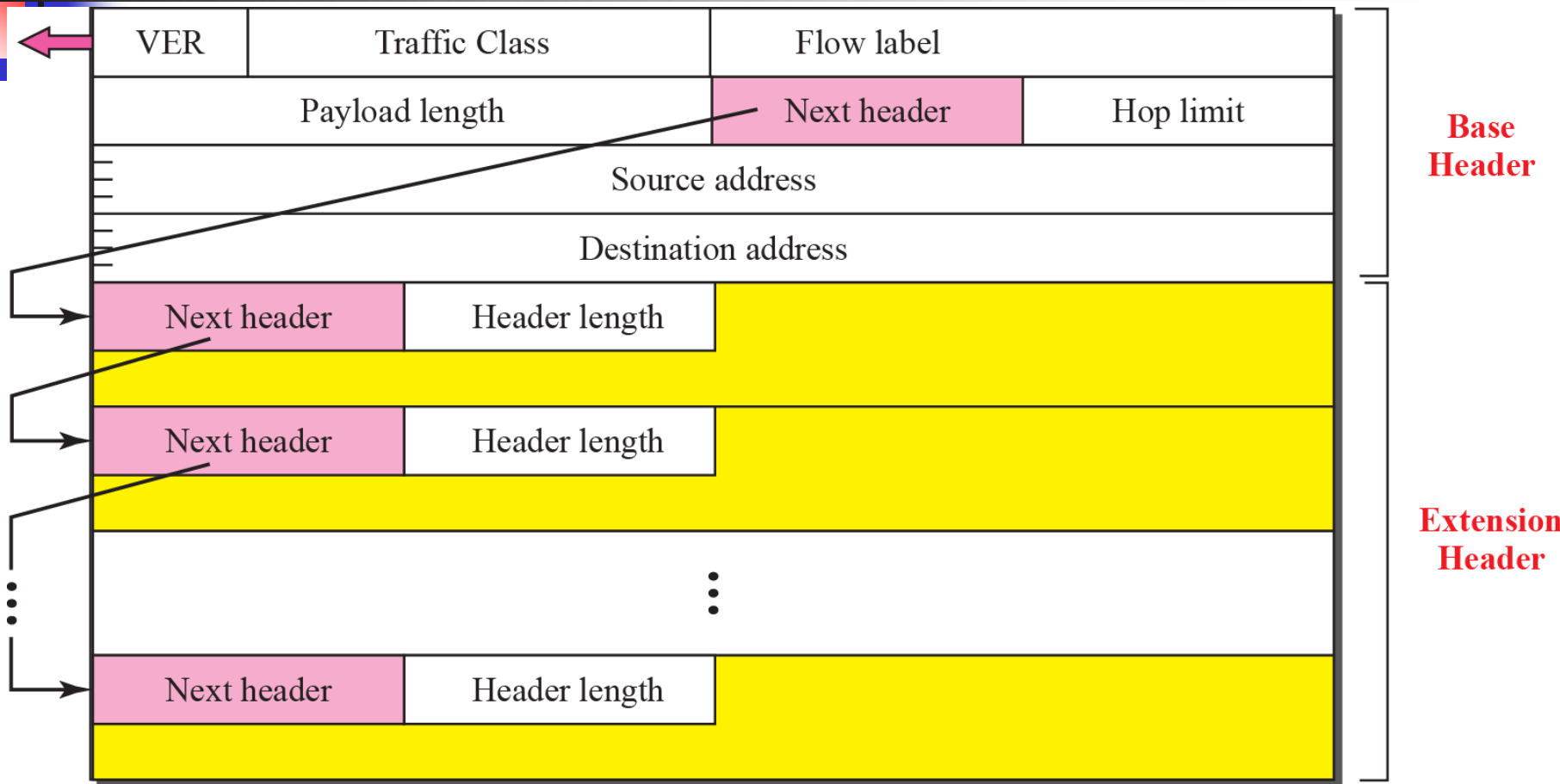
- **Version** - This field contains the version of the IP used in the packet. It is of 4-bit in IP version 6.
- **Traffic class** - This is an 8-bits field determining the **packet priority**. Priority values subdivide into ranges: traffic where the source provides congestion control and non-congestion control traffic.
- **Flow label** - This 20 bits specifies the **QoS management**. Originally created for giving real-time applications special service, but currently unused.
- **Payload length** - This 16 bits determines the **payload length in bytes**. When cleared to zero, the option is a "Jumbo payload" (hop-by-hop).
- **Next header** - This 8-bits field specifies **the next encapsulated protocol**. The values are compatible with those specified for the IPv4 protocol field.
- **Hop limit** - This is an 8-bits field **newly** introduced in IPv6. It **replaces the time to live field** of IPv4.
- **Source Address** - This 128 bits field determines the logical address of the host that is sending the packet.
- **Destination Address** - This 128 bits field determines the logical address of the host that is receiving the packet.



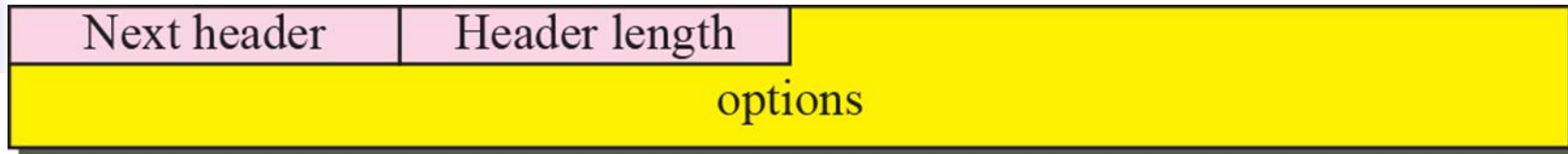
### *Next Header Codes*

<i>Code</i>	<i>Next Header</i>	<i>Code</i>	<i>Next Header</i>
0	Hop-by-hop option	44	Fragmentation
2	ICMP	50	Encrypted security payload
6	TCP	51	Authentication
17	UDP	59	Null (No next header)
43	Source routing	60	Destination option

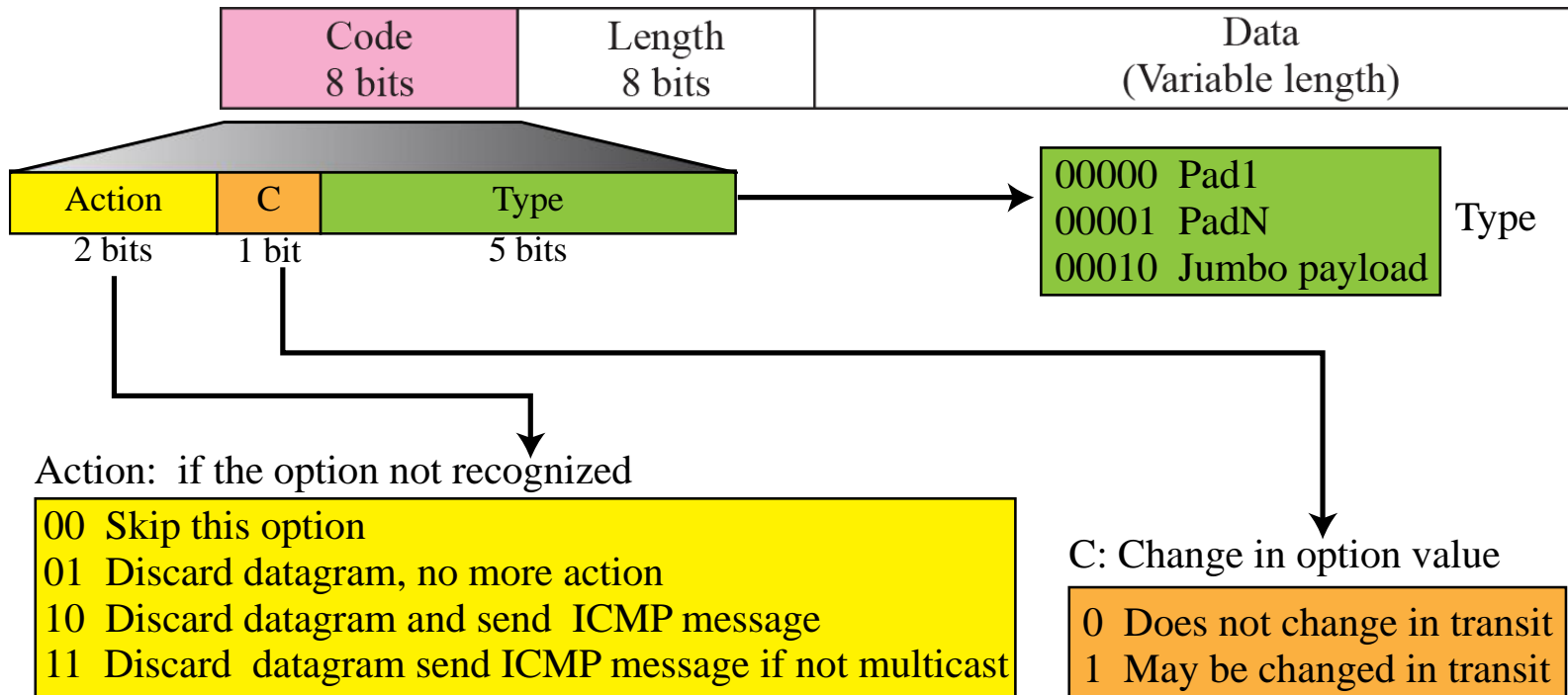
## Extension header format



*Encrypted security payload*

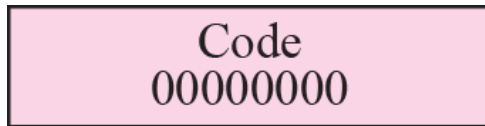


### *Hop-by-hop option header format*



### *The format of the option in a hop-by-hop option header*

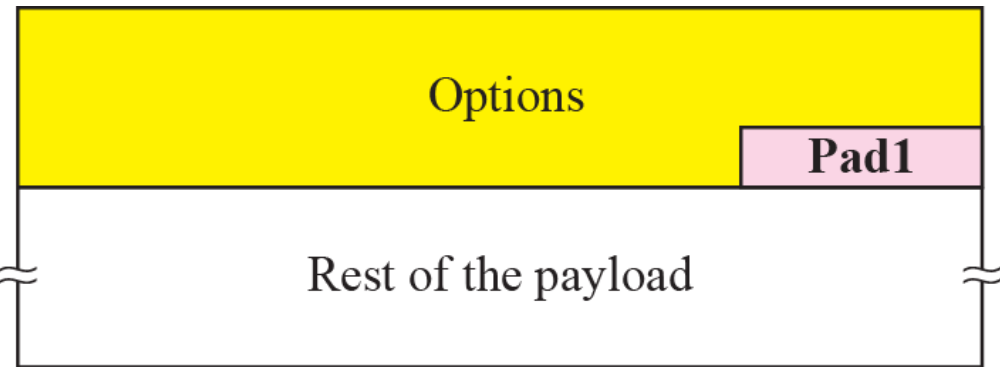
*Pad1*



a. Pad1

It is used to insert a single byte of padding so that the Hop-by-Hop Options or Destination Options headers fall on 8-byte boundaries and to accommodate the alignment requirements of options.

The Pad1 option has no alignment requirements.

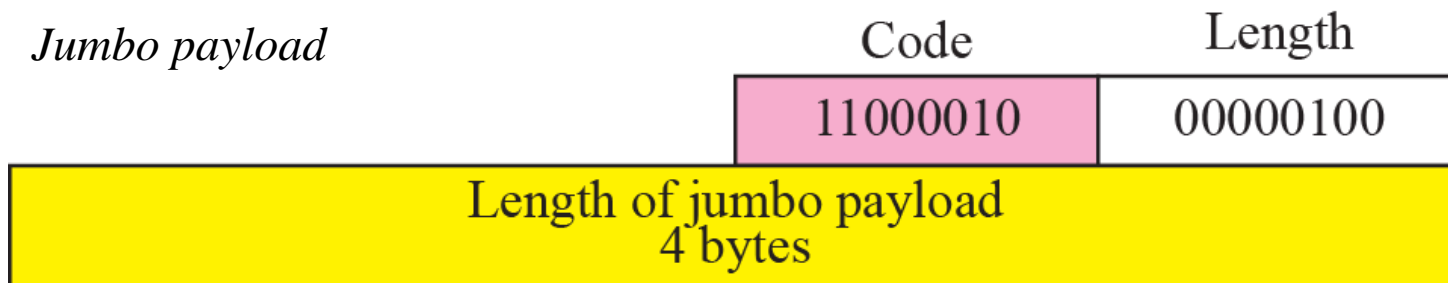


b. Used for padding

*PadN*



*Jumbo payload*





## Source routing + example

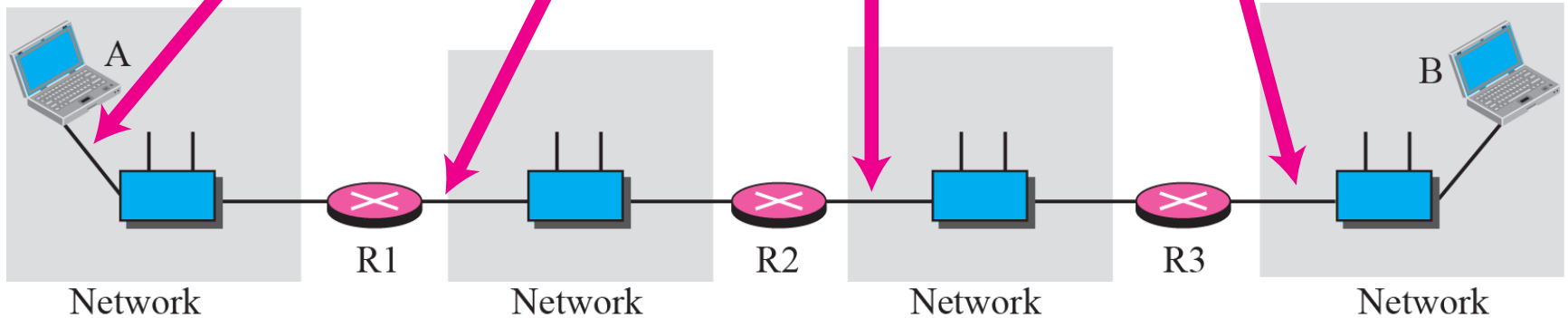
Next header	Header length	Type	Addresses left
Reserved	Strict/loose mask		
First address			
Second address			
⋮			
Last address			

Source: A
Destination: R1
Left: 3
R2
R3
B

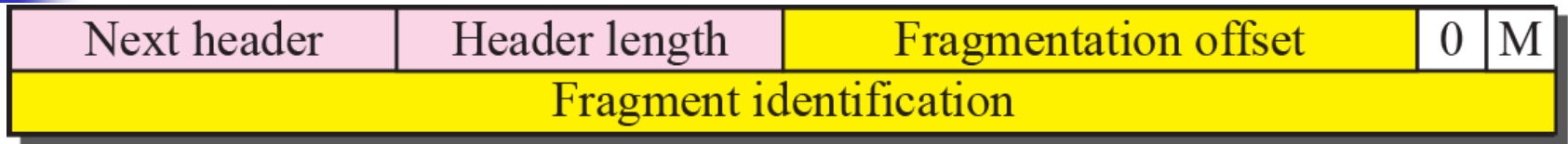
Source: A
Destination: R2
Left: 2
R1
R3
B

Source: A
Destination: R3
Left: 1
R1
R2
B

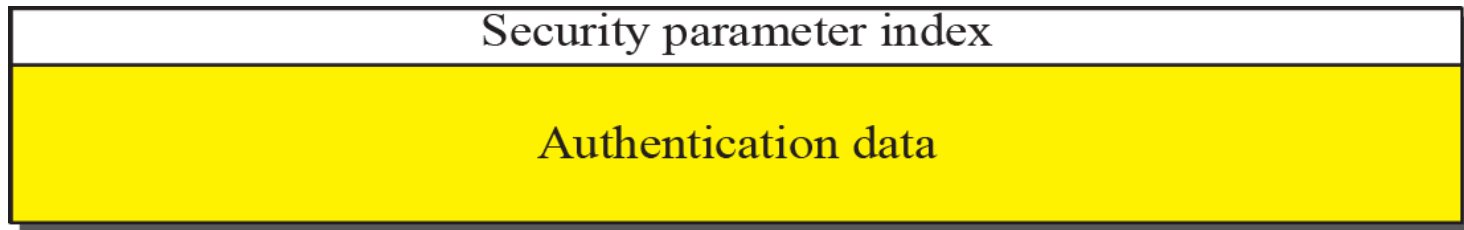
Source: A
Destination: B
Left: 0
R1
R2
R3



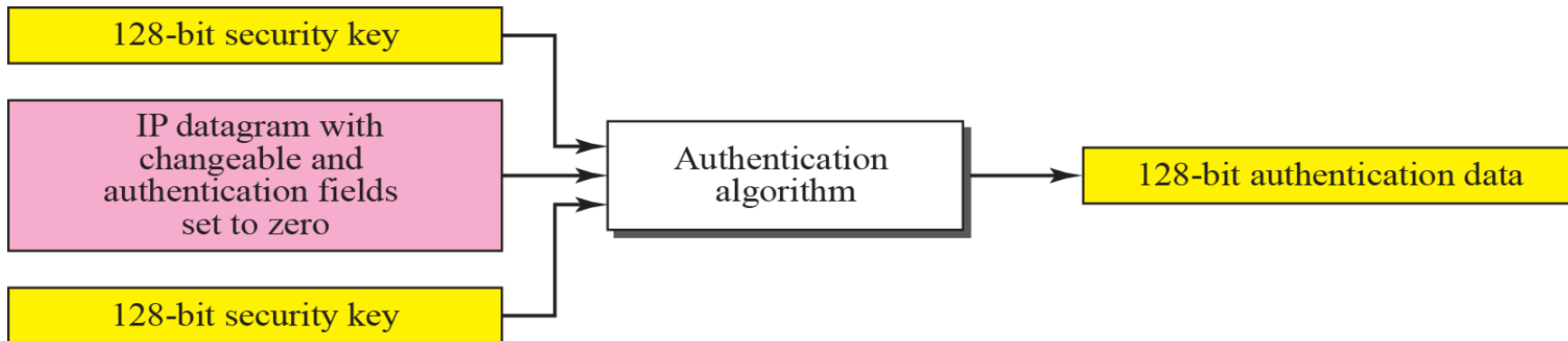
### *Fragmentation*



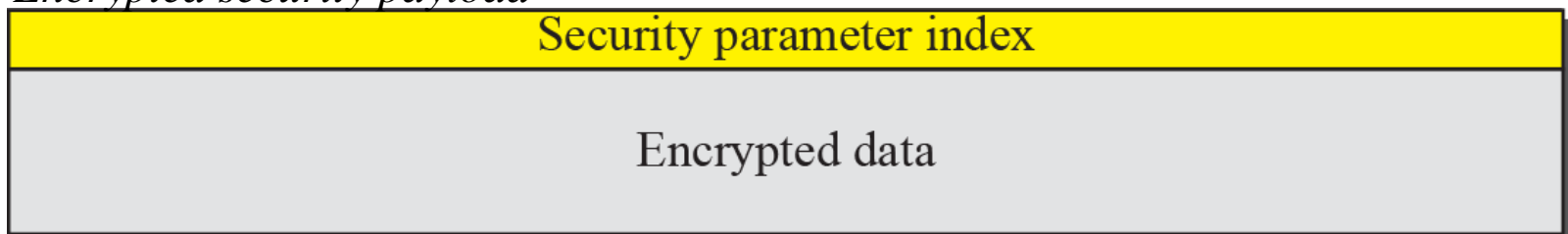
### *Authentication*



### *Calculation of authentication data*



### *Encrypted security payload*



# IPv6 Simplifications

- Fixed format headers
  - use extension headers instead of options
- Remove header checksum
  - rely on link layer and higher layers to check integrity of data
- Remove hop-by-hop segmentation
  - no fragmentation due to path MTU discovery

# IPv6 Addresses

IPv6 has three address categories:

- **unicast** - identifies exactly one interface
- **multicast** - identifies a group; packets get delivered to all members of the group
- **anycast** - identifies a group; packets normally get delivered to nearest member of the group

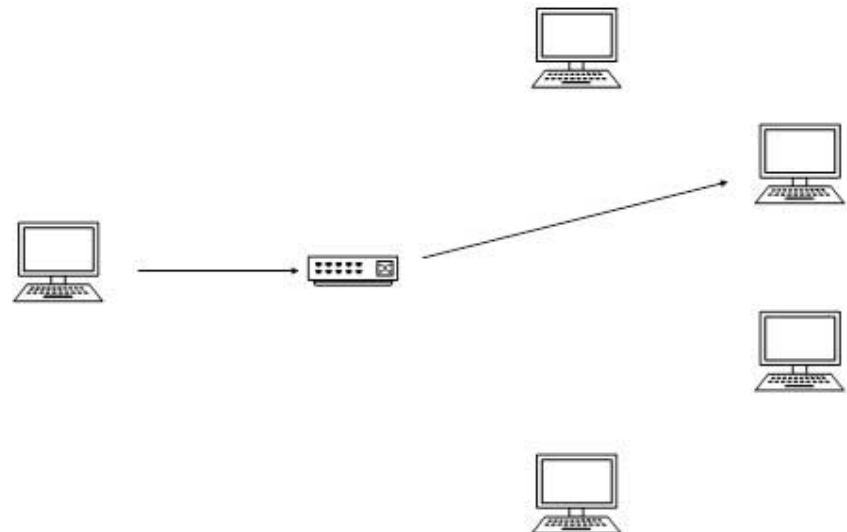
# Unicast

([https://www.tutorialspoint.com/ipv6/ipv6\\_mobility.htm](https://www.tutorialspoint.com/ipv6/ipv6_mobility.htm))

In unicast mode of addressing, an IPv6 interface (host) is **uniquely identified in a network segment**.

The IPv6 packet contains both source and destination IP addresses. A host interface is equipped with an IP address which is unique in that network segment.

When a network switch or a router receives a unicast IP packet, destined to a single host, it sends out one of its outgoing interface which connects to that particular host



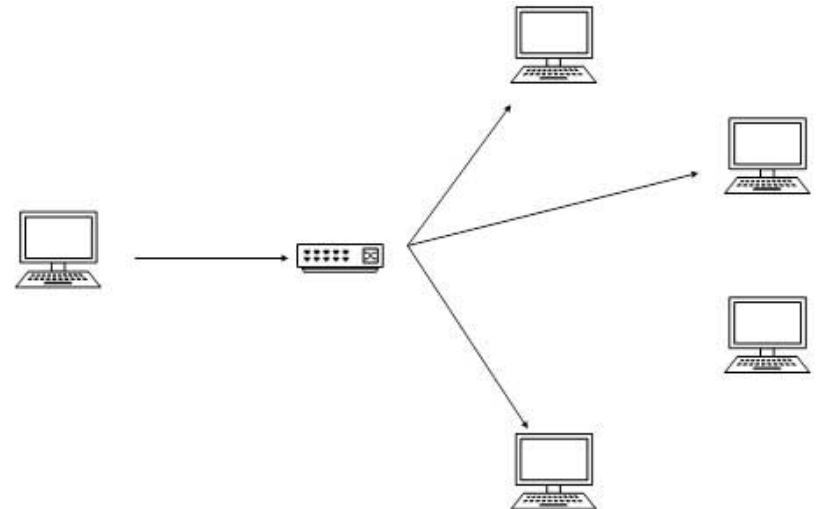
# Multicast

The IPv6 multicast mode is same as that of IPv4.

The packet **destined to multiple hosts** is sent on a special multicast address.

All the hosts interested in that multicast information, **need to join that multicast group first.**

All the interfaces that joined the group receive the multicast packet and process it, while other hosts not interested in multicast packets ignore the multicast information.



# Anycast

IPv6 has introduced a **new type of addressing**, which is called **Anycast addressing**.

In this addressing mode, **multiple interfaces (hosts)** are **assigned same Anycast IP address**.

When a host wishes to communicate with a host equipped with an Anycast IP address, it sends a Unicast message.

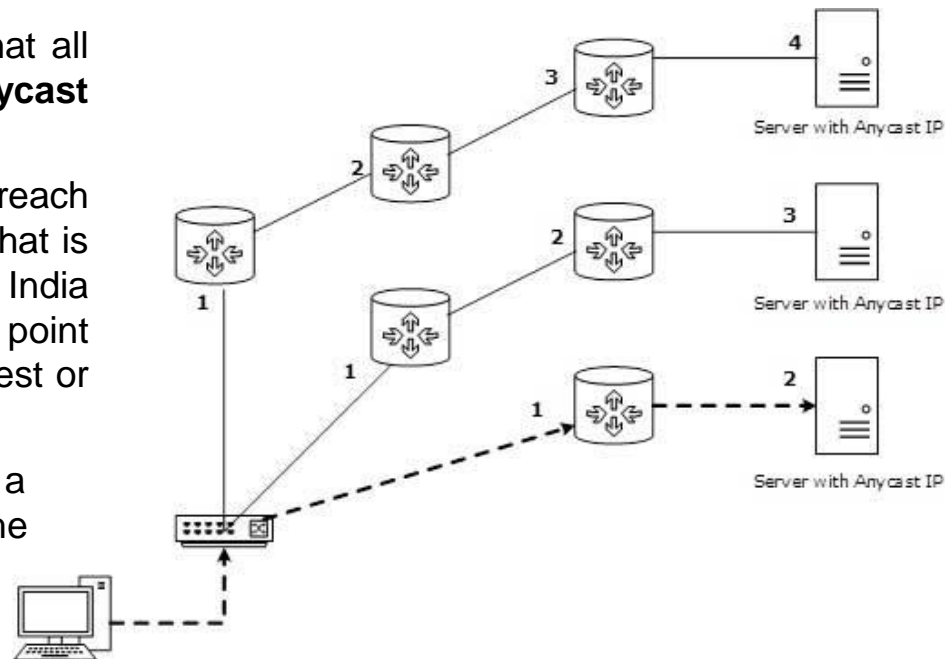
With the help of **complex routing mechanism**, that Unicast message is delivered to the host closest to the Sender in terms of Routing cost.

Let's take an example of **TutorialPoints.com**

Web Servers, located in all continents. Assume that all the **Web Servers are assigned a single IPv6 Anycast IP Address**.

Now when a user from Europe wants to reach **TutorialsPoint.com** the DNS points to the server that is physically located in Europe itself. If a user from India tries to reach Tutorialspoint.com, the DNS will then point to the Web Server physically located in Asia. Nearest or Closest terms are used in terms of Routing Cost.

In the picture, when a client computer tries to reach a server, the request is forwarded to the server with the **lowest Routing Cost**.



# IPv6 Addresses

- An IPv6 unicast address identifies an interface connected to an IP subnet (as is the case in IPv4)
- One big difference between IPv6 and IPv4 is that IPv6 routinely allows each interface to be identified by several addresses



# IPv6 Addresses

- 128 bits results in  $2^{128}$  addresses
- Distributed over the Earth:
- 665,570,793,348,866,943,898,599
- Pessimistic estimate with hierarchies:  
~1,564 addresses/m<sup>2</sup>

# How real is IPv6 in the future?

- IPv6 as a catalyst to expand the functionality in IPv4
- IPv4 can extend towards IPv6 functionality with/by
  - – Network Address Translation
  - – Dynamical configuration of addresses
  - – RSVP combined with IP-«switching»
  - – CIDR - Classless InterDomain Routing
  - – IPSEC as an addition for IPv4, default for IPv6
- IPv6 is still needed to
  - – **Manage the future lack of addresses**
  - – Better utilization in the network

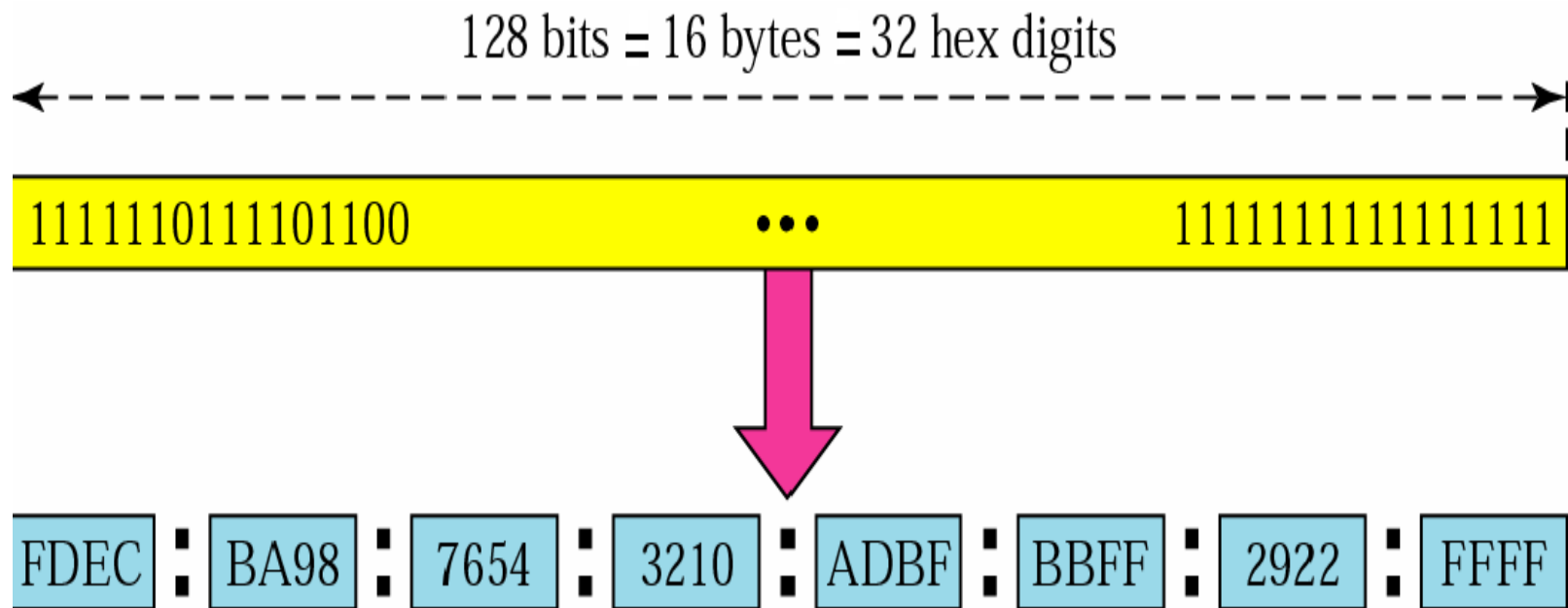
# Writing IPv6 Addresses

- Hexadecimal notation (eight 16 bit hexadecimal integers)
  - 68E8:1480:0022:0000:ABC1:0000:0000:01FE
- Leading zeros may be oppressed
  - 68E8:1480:22:0:ABC1:0:0:1FE
- Zero compression: one of a series of zeros may be replaced by ::
  - 68E8:1480:22:0:ABC1:0:0:1FE replaced by
  - 68E8:1480:22:0:ABC1::1FE

## IPv6 address

### Address Structure

An IPv6 address is made of 128 bits divided into eight 16-bits blocks. Each block is then converted into 4-digit Hexadecimal numbers separated by “:” symbols.



Abbreviated address

Unabbreviated

FDEC ■ BA98 ■ 0074 ■ 3210 ■ 000F ■ BBFF ■ 0000 ■ FFFF



FDEC ■ BA98 ■ 74 ■ 3210 ■ F ■ BBFF ■ 0 ■ FFFF

Abbreviated

**CIDR  
address**

FDEC ■ 0 ■ 0 ■ 0 ■ 0 ■ BBFF ■ 0 ■ FFFF/60

Abbreviated

FDEC ■ 0 ■ 0 ■ 0 ■ 0 ■ BBFF ■ 0 ■ FFFF

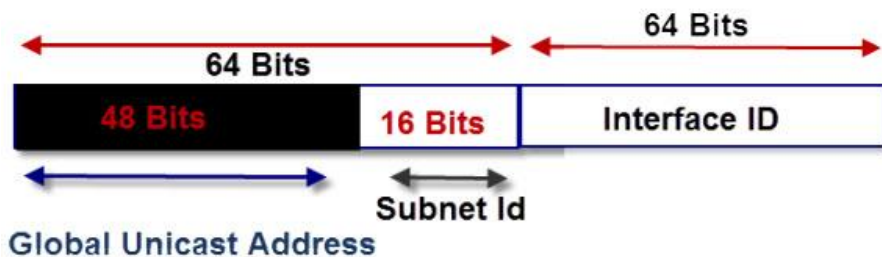


FDEC ■ ■ BBFF ■ 0 ■ FFFF

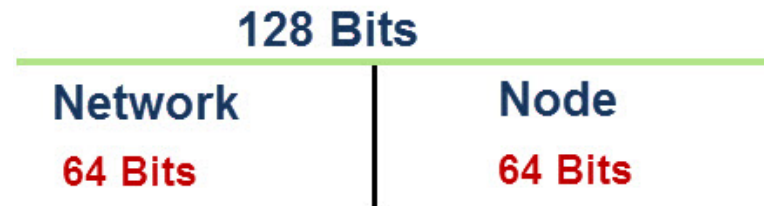
More Abbreviated

# Network And Node Addresses

- In IPv4 an address is split into two components a **network component** and a **node component**.
- This was done initially using **Address classes** and later using **subnet masking**.
- In IPv6 we do the same. **The first step is to split the address into two parts.**
- The address is split into two **64 bit** segments
- the top 64 bits is the **network part** and
- the lower 64 bits the **node part**:



IPv6 Address Structure



IPv6 Address Network and Node

The upper 64 bits are used for **routing**.

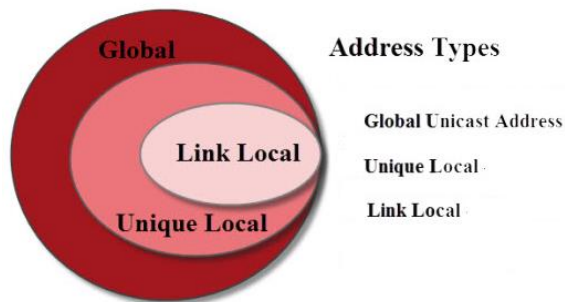
# Scope of IPv6 Unicast Addresses:

IPv6 addresses have three types:

**Global Unicast** Address –Scope Internet- routed on Internet

**Unique Local** — Scope Internal Network or VPN internally routable, but Not routed on Internet

**Link Local** – Scope network link- Not Routed internally or externally.



Features	Global Unicast Address	Unique Local Address	Link Local Address
Scope	Internet	Internal network	Single link (inside an internal network)
Prefix	2001	•fd00 is the manually assigned address by an organization. •fc00::/8 •fd00::/8	fe80
IPv4 equivalent	Public addresses of IPv4 networks.	•10.0.0.0/8 •172.16.0.0/12 •192.168.0.0/16	169.254.0.0/16 (allocated on an IPv4 network when no DHCP server is found.)

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.

# Link-Local Address

Auto-configured IPv6 address is known as **Link-Local** address. This address always starts with **FE80**. The first 16 bits of link-local address is always set to 1111 1110 1000 0000 (FE80). The next 48-bits are set to 0, thus:

1111 1110 1000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000	Interface ID
---	--------------

Link-local addresses are used for communication among IPv6 hosts on a link (broadcast segment) only.

In IPv4 internal addresses use the reserved number ranges 10.0.0.0/8, 172.16.0.0/12 and 192.168.0.0/16 and 169.254.0.0/16.

These addresses are not routed on the Internet and are reserved for internal networks.

These addresses **are not routable**,

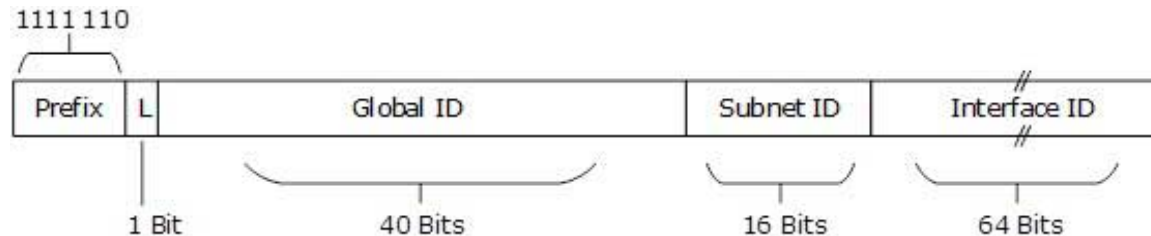
so a Router **never forwards these addresses outside the link**.

- These are meant **to be used inside an internal network**, and again they are not routed on the Internet.
- It is equivalent to the IPv4 address **169.254.0.0/16 which is allocated on an IPv4 network when no DHCP server is found**.
- They are restricted to a link and are not routed on the Internal network or the Internet.
- **Link Local addresses are self assigned** i.e. they **do not require a DHCP server**.
- A link local address is required on every IP6 interface even if no routing is present.



## Unique-Local Address

This type of IPv6 address is **globally unique**, but it **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**.



Prefix is always set to 1111 110. L bit, is set to 1 if the address is locally assigned. So far, the meaning of L bit to 0 is not defined. **Therefore, Unique Local IPv6 address always starts with 'FD'.**

- **fc00::/8** for globally assigned addressing.
- **fd00::/8** for locally assigned addressing.

Unique Local are meant to be used **inside an internal network**.

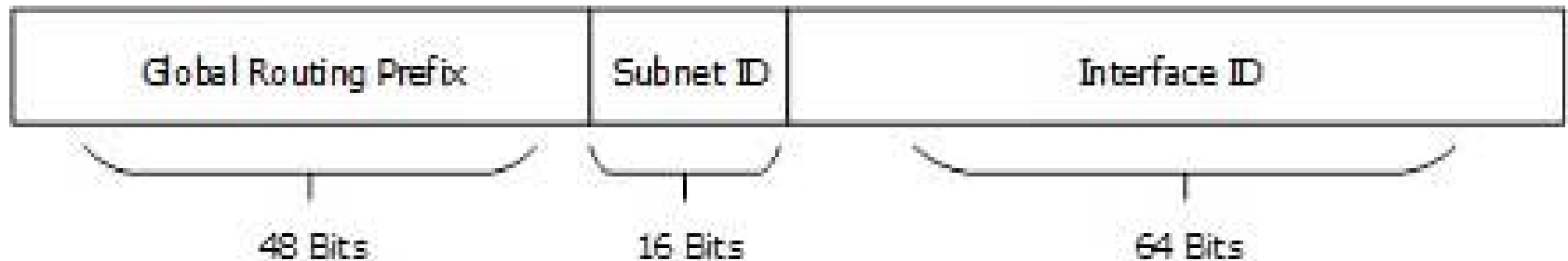
They are **routed on the Internal network but not routed on the Internet**.

They are equivalent to the **IPv4 addresses** are **10.0.0.0/8, 172.16.0.0/12 and 192.168.0.0/16**

# Global Unicast Address

This address type is equivalent to IPv4's public address.

**Global Unicast** addresses in IPv6 are globally identifiable and uniquely addressable.



## Global Routing Prefix:

The most significant 48-bits are designated as **Global Routing Prefix** which is assigned to specific autonomous system.

The three most significant bits of Global Routing Prefix is **always set to 001**.

- These addresses are known as global Unicast addresses and are the **equivalent of the public addresses of IPv4 networks**.
- The **Internet authorities allocate address blocks to ISPs who in turn allocate them to their customers**

# Using IPv6 Addresses in URLs

- On IPv4 networks you can access a network resource e.g. a web page using the format
- `http://192.168.1.21/webpage`
- However IPv6 addresses contains a colon as separator and so must be enclosed in square brackets.
- `http:[IPv6 address]/webpage.`

# IPv6 Loop Back

- The IPv6 **loopback address** is **::1**. You can ping it as follows:
- **ping ::1**

■ C:\mos>ping ::1 -6



**Force IPv6**

Pinging ::1 with 32 bytes of data:

Reply from ::1: time<1ms

Reply from ::1: time<1ms

Reply from ::1: time<1ms

Reply from ::1: time<1ms

Ping statistics for ::1:

Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),

Approximate round trip times in milli-seconds:

Minimum = 0ms, Maximum = 0ms, Average = 0ms

**Ping Loopback IPv6**

<https://support.hp.com/hr-en/document/c06431186>

# Special Address Formats

IPv6 Address	Meaning
::/128	Unspecified Address
::/0	Default Route
::1/128	Loopback Address

- As shown in the table, the address 0:0:0:0:0:0:0:0/128 does not specify anything and is said to be an **unspecified address**. After simplifying, all the 0s are compacted to ::/128.
  - **only used as source address during bootstrap by a computer that has not yet learned its address**
- In IPv4, the address 0.0.0.0 with netmask 0.0.0.0 represents the default route. The same concept is also applied to IPv6, address 0:0:0:0:0:0:0:0 with netmask all 0s **represents the default route**. After applying IPv6 rule, this address is compressed to ::/0.
- Loopback addresses in IPv4 are represented by 127.0.0.1 to 127.255.255.255 series. But in IPv6, only 0:0:0:0:0:0:0:1/128 represents the **Loopback address**. After loopback address, it can be represented as ::1/128.
  - **used for testing software** (compare with **IPv4 loopback address 127.0.0.1**)

# Reserved Multicast Address for Routing Protocols

The reserved multicast addresses used by interior routing protocol. The addresses are reserved following the same rules of IPv4

IPv6 Address	Routing Protocol
FF02::5	OSPFv3
FF02::6	OSPFv3 Designated Routers
FF02::9	RIPng
FF02::A	EIGRP

## Reserved Multicast Address for Routers/Node

IPv6 Address	Scope
FF01::1	All Nodes in interface-local
FF01::2	All Routers in interface local
FF02::1	All Nodes in link-local
FF02::2	All Routers in link-local
FF05::2	All Routers in site-local

These addresses help routers and hosts to speak to available routers and hosts on a segment without being configured with an IPv6 address. Hosts use EUI-64 based auto-configuration to self-configure an IPv6 address and then speak to available hosts/routers on the segment by means of these addresses.

# Neighbor Discovery Protocol

In IPv6, there are no broadcast mechanisms. It is not a must for an IPv6 enabled host to obtain an IP address from DHCP or manually configured, but it can auto-configure its own IP.

- ARP has been replaced by ICMPv6 Neighbor Discovery Protocol.

A host in IPv6 network is capable of auto-configuring itself with a unique link-local address. As soon as host gets an IPv6 address, it joins a number of multicast groups. All communications related to that segment take place on those multicast addresses only. A host goes through a series of states in IPv6:

- **Neighbor Solicitation:** After configuring all IPv6's either manually, or by DHCP Server or by auto-configuration, the host sends a Neighbor Solicitation message out to FF02::1/16 **multicast address for all its IPv6 addresses in order to know that no one else occupies the same addresses.**
- **DAD (Duplicate Address Detection):** When the host does not listen from anything from the segment regarding its Neighbor Solicitation message, it assumes that no duplicate address exists on the segment.
- **Neighbor Advertisement:** After assigning the addresses to its interfaces and making them up and running, **the host once again sends out a Neighbor Advertisement message telling all other hosts on the segment, that it has assigned** those IPv6 addresses to its interfaces.

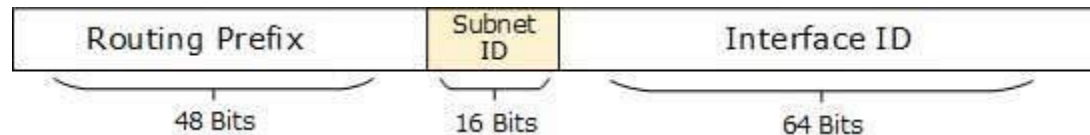
Once a host is done with the configuration of its IPv6 addresses, it does the following things:

- **Router Solicitation:** A host sends a Router Solicitation multicast packet (FF02::2/16) out on its segment **to know the presence of any router on this segment.** It **helps the host to configure the router as its default gateway.** If its default gateway router goes down, the host can shift to a new router and makes it the default gateway.
- **Router Advertisement:** When a router receives a Router Solicitation message, it response back to the host, advertising its presence on that link.
- **Redirect:** This may be the situation where a Router receives a Router Solicitation request but **it knows that it is not the best gateway for the host.** In this situation, the **router sends back a Redirect message telling the host that there is a better 'next-hop'** router available. Next-hop is where the host will send its data destined to a host which does not belong to the same segment.



# Subnetting

- IPv6 addresses use 128 bits to represent an address which includes bits to be used for subnetting. The second half of the address (least significant 64 bits) is always used for hosts only. Therefore, there is no compromise if we subnet the network.



**16 bits of subnet is equivalent to IPv4's Class B Network.** Using these subnet bits, an organization can have another 65 thousands of subnets which is by far, more than enough.

Thus routing prefix is /64 and host portion is 64 bits. We can further subnet the network beyond 16 bits of Subnet ID, by borrowing host bits; but it is recommended that 64 bits should always be used for hosts addresses because auto-configuration requires 64 bits.

**IPv6 subnetting works on the same concept as Variable Length Subnet Masking in IPv4.**

/48 prefix can be allocated to an organization providing it the benefit of having up to /64 subnet prefixes, which is 65535 sub-networks, each having  $2^{64}$  hosts. A /64 prefix can be assigned to a point-to-point connection where there are only two hosts (or IPv6 enabled devices) on a link.

# Mobility

IPv6 mobility provides a mechanism for the host to roam around different links without losing any communication/connection and its IP address.

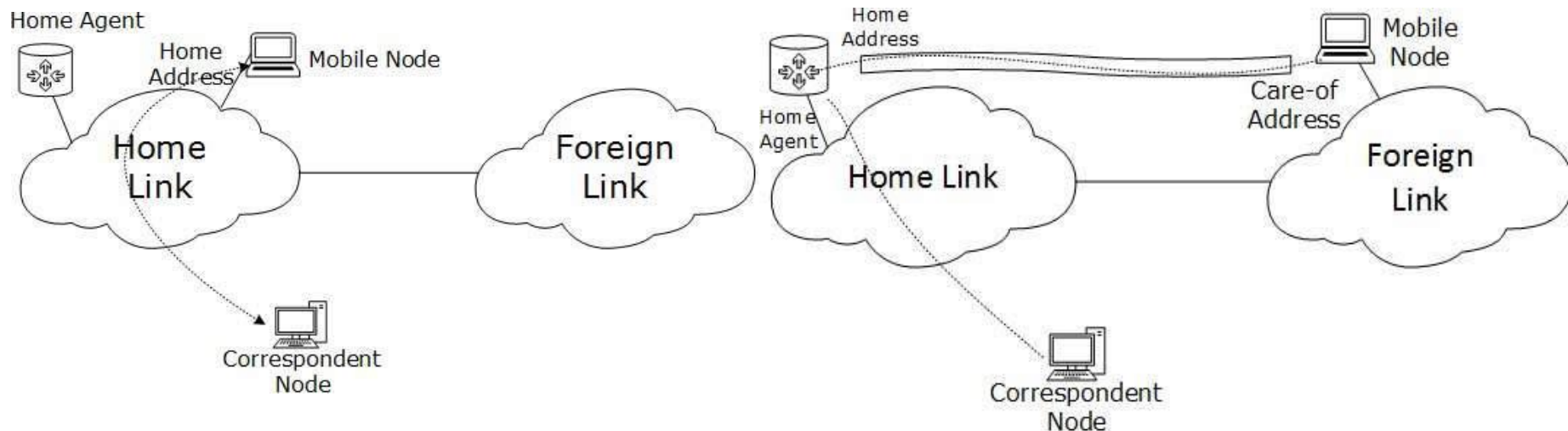
Multiple entities are involved in this technology:

- **Mobile Node:** The device that needs IPv6 mobility.
- **Home Link:** This link is configured with the home subnet prefix and this is where the Mobile IPv6 device gets its Home Address.
- **Home Address:** This is the address which the Mobile Node acquires from the Home Link. This is the permanent address of the Mobile Node. If the Mobile Node remains in the same Home Link, the communication among various entities take place as usual.
- **Home Agent:** This is a **router that acts as a registrar for Mobile Nodes**. Home Agent is connected to Home Link and maintains information about all Mobile Nodes, their Home Addresses, and their present IP addresses.
- **Foreign Link:** Any other Link that is not Mobile Node's Home Link.
- **Care-of Address:** When a Mobile Node gets attached to a Foreign Link, it acquires a new IP address of that Foreign Link's subnet. **Home Agent maintains the information of both Home Address and Care-of Address.** Multiple Care-of addresses can be assigned to a Mobile Node, but at any instance, only one Care-of Address has binding with the Home Address.
- **Correspondent Node:** Any IPv6 enabled device that intends to have communication with Mobile Node.

# Mobility Operation

[https://www.tutorialspoint.com/ipv6/ipv6\\_mobility.htm](https://www.tutorialspoint.com/ipv6/ipv6_mobility.htm)

- When Mobile Node stays in its Home Link, all communications take place on its Home Address as shown below:



When a Mobile Node leaves its Home Link and is connected to some Foreign Link, the Mobility feature of IPv6 comes into play. After getting connected to a Foreign Link, the **Mobile Node acquires an IPv6 address from the Foreign Link. This address is called Care-of Address.** The Mobile Node sends a binding request to its Home Agent with the new Care-of Address. **The Home Agent binds the Mobile Node's Home Address with the Care-of Address, establishing a Tunnel between both.**

Whenever a Correspondent Node tries to establish connection with the Mobile Node (on its Home Address), the Home Agent intercepts the packet and forwards to Mobile Node's Care-of Address over the Tunnel which was already established.

# Route Optimization

When a Correspondent Node initiates a communication by sending packets to Mobile the Node on the Home Address, these packets are tunneled to the Mobile Node by the Home Agent.

**In Route Optimization mode, when the Mobile Node receives a packet from the Correspondent Node, it does not forward replies to the Home Agent. Rather, it sends its packet directly to the Correspondent Node using Home Address as Source Address. This mode is optional and not used by default.**

Routing concepts remain same in case of IPv6 but almost all routing protocols have been redefined accordingly. **Routing is a process to forward routable data choosing the best route among several available routes or path to the destination.** A router is a device that forwards data that is not explicitly destined to it.

There exists two forms of routing protocols:

- **Distance Vector Routing Protocol:** A router running distance vector protocol advertises its connected routes and learns new routes from its neighbors. The routing **cost to reach a destination is calculated by means of hops between the source and destination.** A router generally relies on its neighbor for best path selection, also known as “routing-by-rumors”. RIP and BGP are Distance Vector Protocols.
- **Link-State Routing Protocol:** This protocol acknowledges the state of a Link and advertises to its neighbors. Information about new links is learnt from peer routers. After all the routing information has been converged, the Link-State Routing Protocol uses its **own algorithm to calculate the best path to all available links.** OSPF and IS-IS are link state routing protocols and both of them use **Dijkstra’s Shortest Path First** algorithm.

# Routing protocols can be divided in two categories:

- **Interior Routing Protocol:** Protocols in this categories are used within an autonomous system or organization to distribute routes among all routers inside its boundary. Examples: RIP, OSPF.
- **Exterior Routing Protocol:** An Exterior Routing Protocol distributes routing information between two different autonomous systems or organization. Examples: BGP.

# Routing protocols

- **RIPng**

- RIPng stands for Routing Information Protocol Next Generation. This is an **Interior Routing Protocol** and is a Distance Vector Protocol. RIPng has been upgraded to support IPv6.
- The RIPng IGP uses the Bellman-Ford distance-vector algorithm to determine the best route to a destination, using hop count as the metric. RIPng allows hosts and routers to exchange information for computing routes through an IP-based network. RIPng is intended to act as an IGP for moderately-sized autonomous systems.

- **OSPFv3**

- Open Shortest Path First version 3 is an **Interior Routing Protocol** which is modified to support IPv6. This is a Link-State Protocol and uses Dijkstra's Shortest Path First algorithm to calculate best path to all destinations. It was designed for use in an autonomous system such as a local area network.
- OSPF was developed so that the shortest path through a network was calculated based on the cost of the route, taking into account bandwidth, delay and load.

# Routing protocols

- **BGPv4**

- BGP stands for Border Gateway Protocol. It is the only open standard **Exterior Gateway Protocol** available. BGP is a Distance Vector protocol which takes Autonomous System as calculation metric, instead of the number of routers as Hop. BGPv4 is an upgrade of BGP to support IPv6 routing.
- The Border Gateway Protocol makes routing decisions based on paths, network policies, or rule-sets configured by a network administrator and is involved in making core routing decisions.

# Protocols Changed to Support IPv6

- **ICMPv6:** Internet Control Message Protocol version 6 is an upgraded implementation of ICMP to accommodate IPv6 requirements. This protocol **is used for diagnostic functions, error and information message, statistical purposes.** ICMPv6's Neighbor Discovery Protocol replaces ARP and helps discover neighbor and routers on the link.
- ICMPv6 is defined in RFC 4443.
- Similar to ICMPv4, describes two types of messages:
  - Informational
  - Error
- Much more robust than ICMP for IPv4.
- Contains new functionality and improvements.
- More than just “messaging” but “how IPv6 conducts business”.



# DHCPv6

- **DHCPv6:** Dynamic Host Configuration Protocol version 6 is an implementation of DHCP.
- IPv6 enabled hosts do not require any DHCPv6 Server to acquire IP address as they can be auto-configured.
- Neither do they need DHCPv6 to locate DNS server because DNS can be discovered and configured via ICMPv6 Neighbor Discovery Protocol.
- Yet DHCPv6 Server can be used to provide these information.

# DHCPv6 versus DHCPv4 Message Types

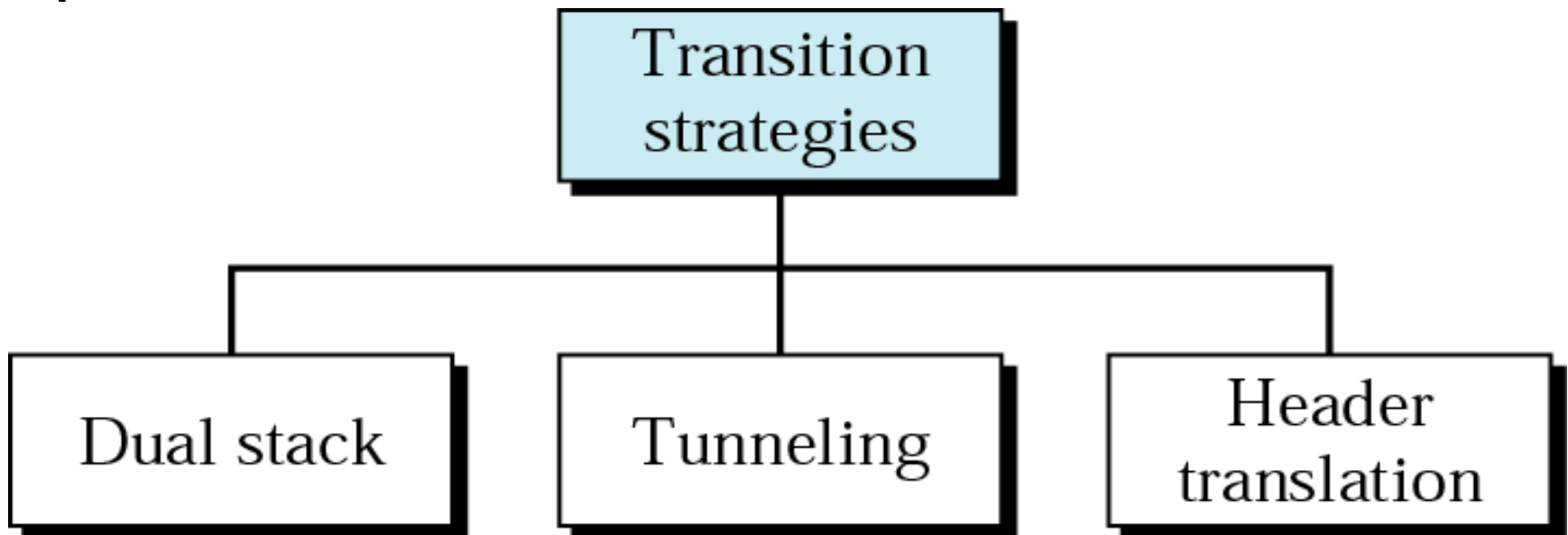
DHCPv6 Message Type	DHCPv4 Message Type
Solicit (1)	DHCPDISCOVER
Advertise (2)	DHCPOFFER
Request (3), Renew (5), Rebind (6)	DHCPREQUEST
Reply (7)	DHCPACK / DHCPNAK
Release (8)	DHCPRELEASE
Information-Request (11)	DHCPINFORM
Decline (9)	DHCPDECLINE
Confirm (4)	none
Reconfigure (10)	DHCPFORCERENEW
Relay-Forw (12), Relay-Reply (13)	none

# IPv6 and DNS

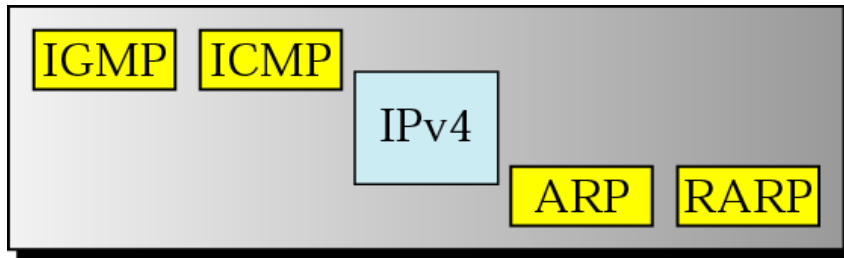
	IPv4	IPv6
Hostname to IP address	A record: www.abc.test. A 192.168.30.1	AAAA record: www.abc.test AAAA 2001:db8:C18:1::2
IP address to hostname	PTR record: 1.30.168.192.in-addr.arpa. PTR www.abc.test.	PTR record: 2.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.1.0.0.0.8.1.c.0. 8.b.d.0.1.0.0.2.ip6.arpa PTR www.abc.test.

**DNS:** There has been no new version of DNS but it is now equipped **with extensions to provide support for querying IPv6 addresses**. A new AAAA (quad-A) record has been added to reply IPv6 query messages. Now the DNS can reply with both IP versions (4 & 6) without any change in the query format.

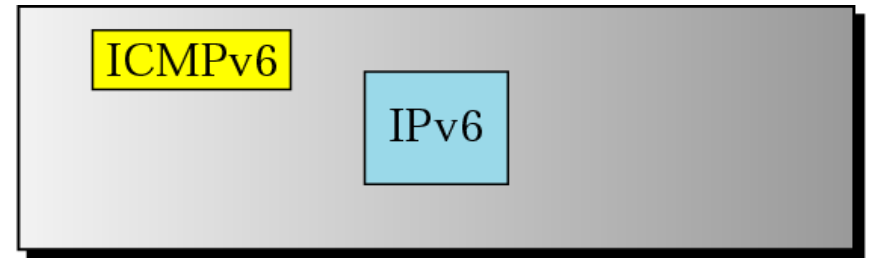
- Because of the large number of systems on the Internet, the transition from IPv4 to IPv6 cannot happen suddenly
- Transition should be smooth to prevent problems



## Comparison of network layers in version 4 and version 6



Network layer in version 4



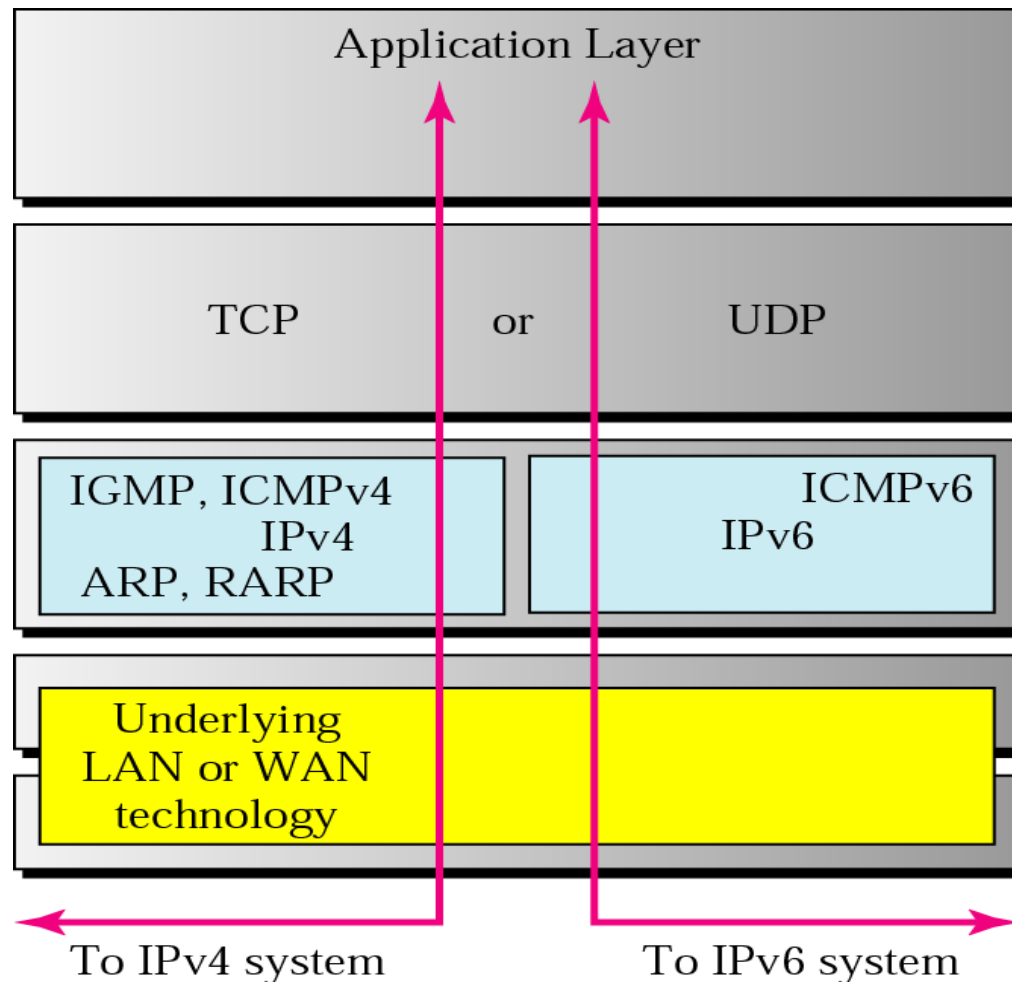
Network layer in version 6

- ICMPv4 has been modified to be more suitable for IPv6, and thus updated to ICMPv6
- ARP and ICMP in version 4 are now part of ICMPv6
- RARP has been dropped due to limited use (BOOTP does the job of RARP)
- As in ICMPv4, ICMPv6 messages are divided into 2 categories:
  - Error-reporting (somewhat different messages)
  - Query (rather different messages in v6 vs v4)

## Dual stack

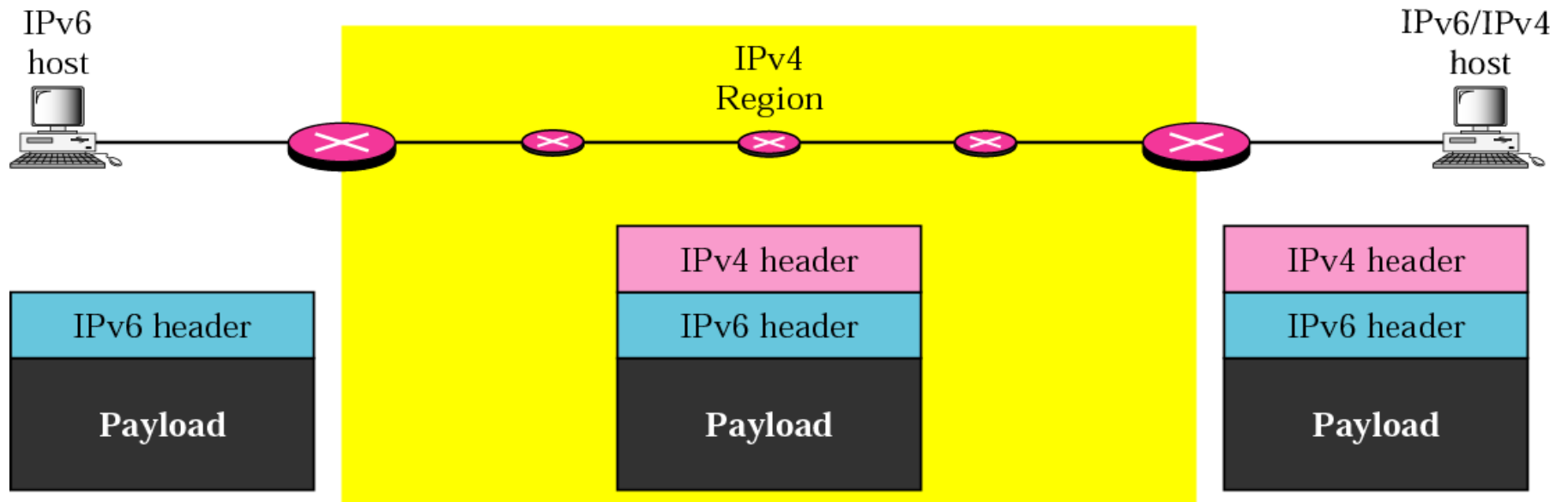
Recommended that all hosts have dual stack of protocols until all of the Internet runs IPv6

To determine which version to use, the source host queries the DNS



- It is recommended that all hosts, before migrating completely to version 6, have a dual stack of protocols.
- ***In other words, a station must run IPv4 and IPv6 simultaneously until all the Internet uses IPv6.***
- To determine which version to use when sending a packet to a destination, the source host queries the DNS.
- If the DNS returns an IPv4 address, the source host sends an Ipv4 packet.
- If the DNS returns an IPv6 address, the source host sends an IPv6 packet.

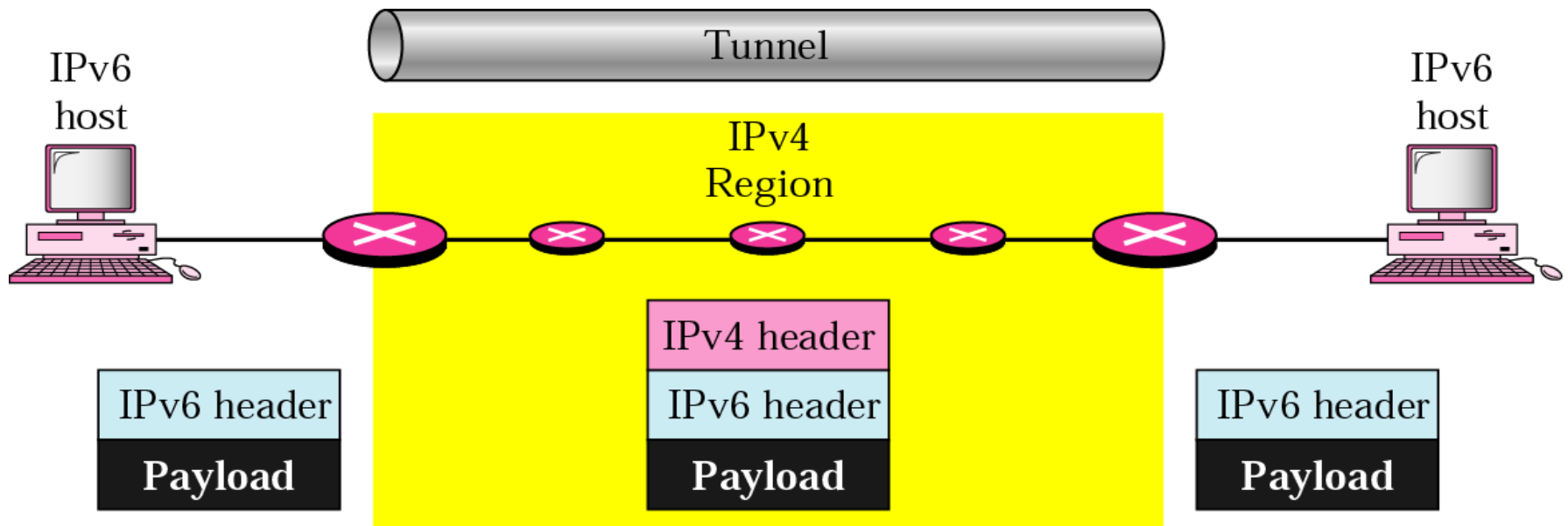
# Automatic tunneling





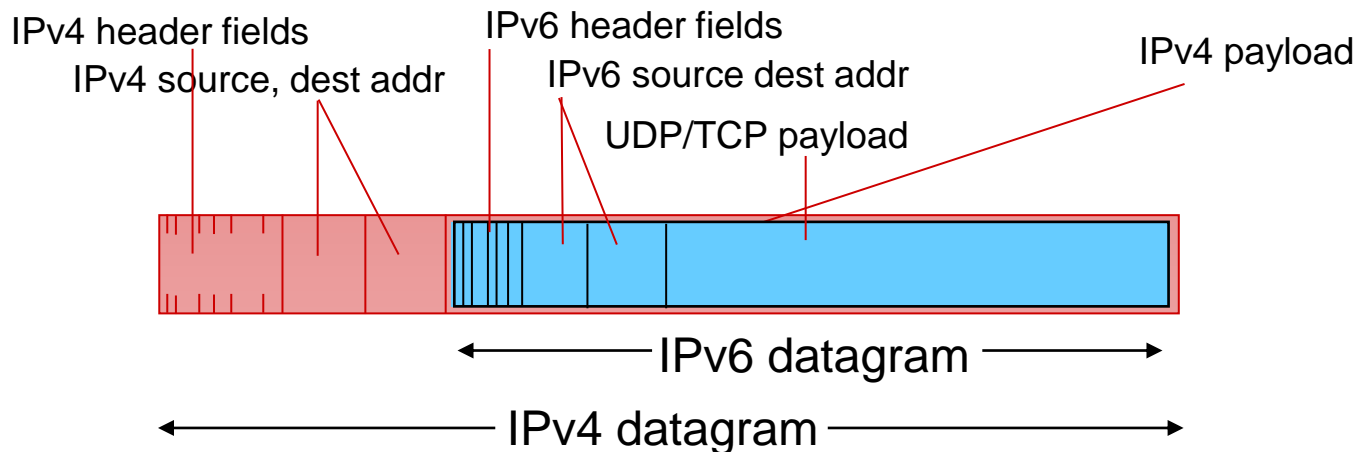
## *Configured Tunneling*

- The IP packets are encapsulate again
- The purpose of tunneling is to transport the information from the original IP as data
- The initial heading is keeping original
- Will be attached a new heading with the addresses the addresses of beginning respectively the end of tunnel



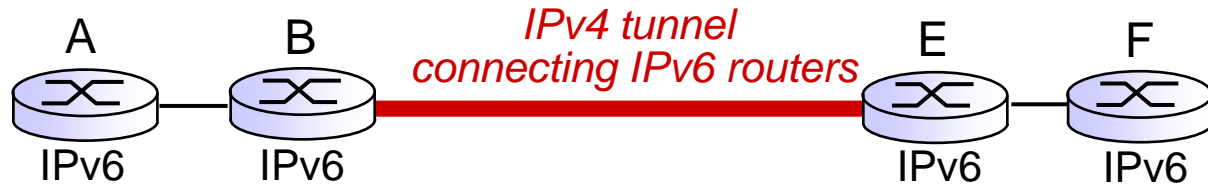
# Transition from IPv4 to IPv6

- not all routers can be upgraded simultaneously
  - no “flag days”
  - how will network operate with mixed IPv4 and IPv6 routers?
- *tunneling*: IPv6 datagram carried as *payload* in IPv4 datagram among IPv4 routers

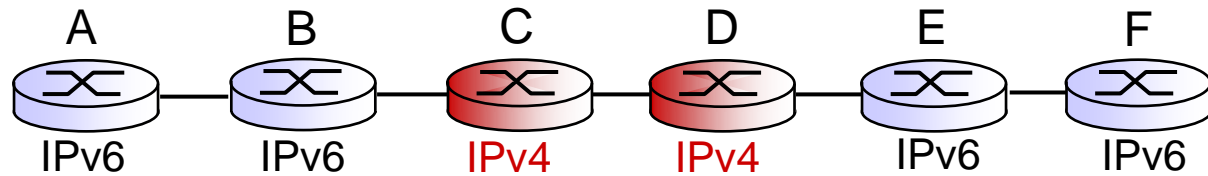


# Tunneling

logical view:

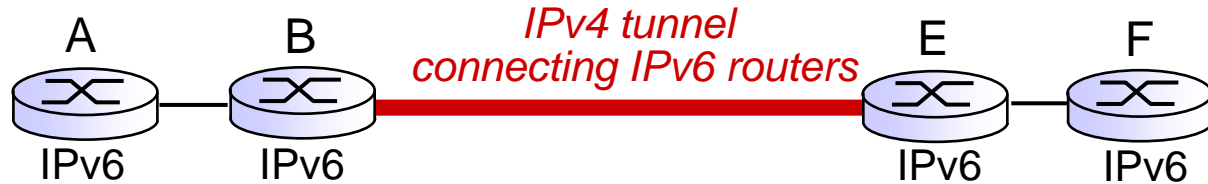


physical view:

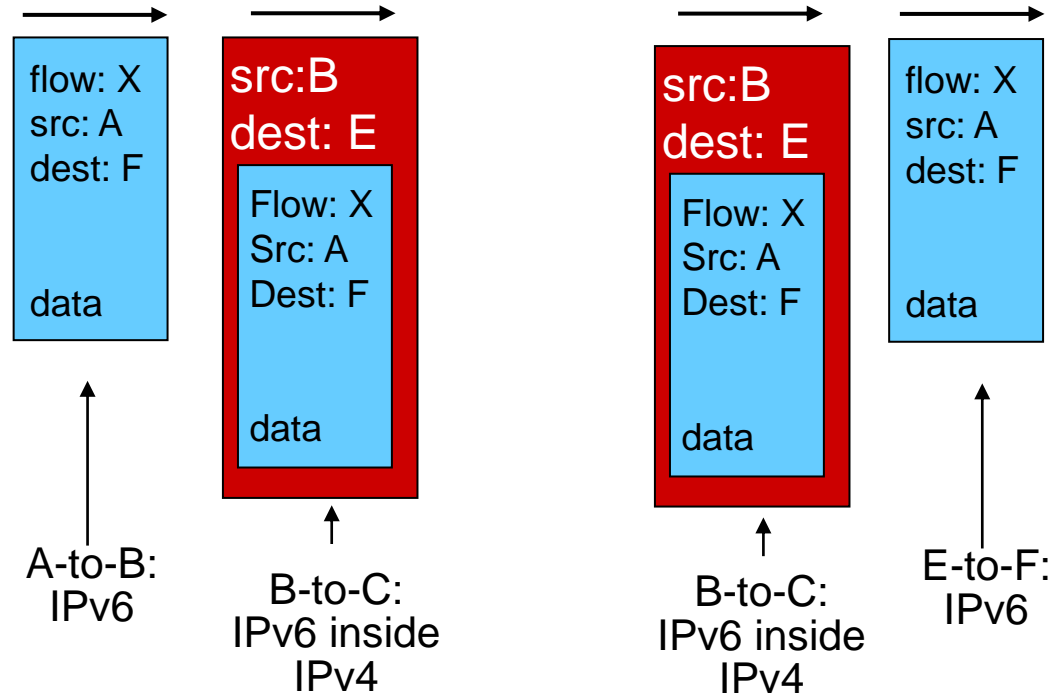
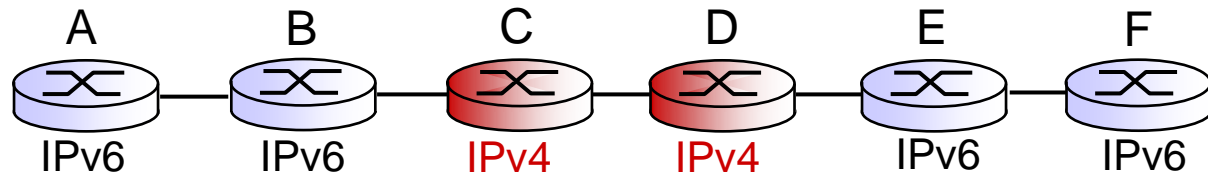


# Tunneling

logical view:

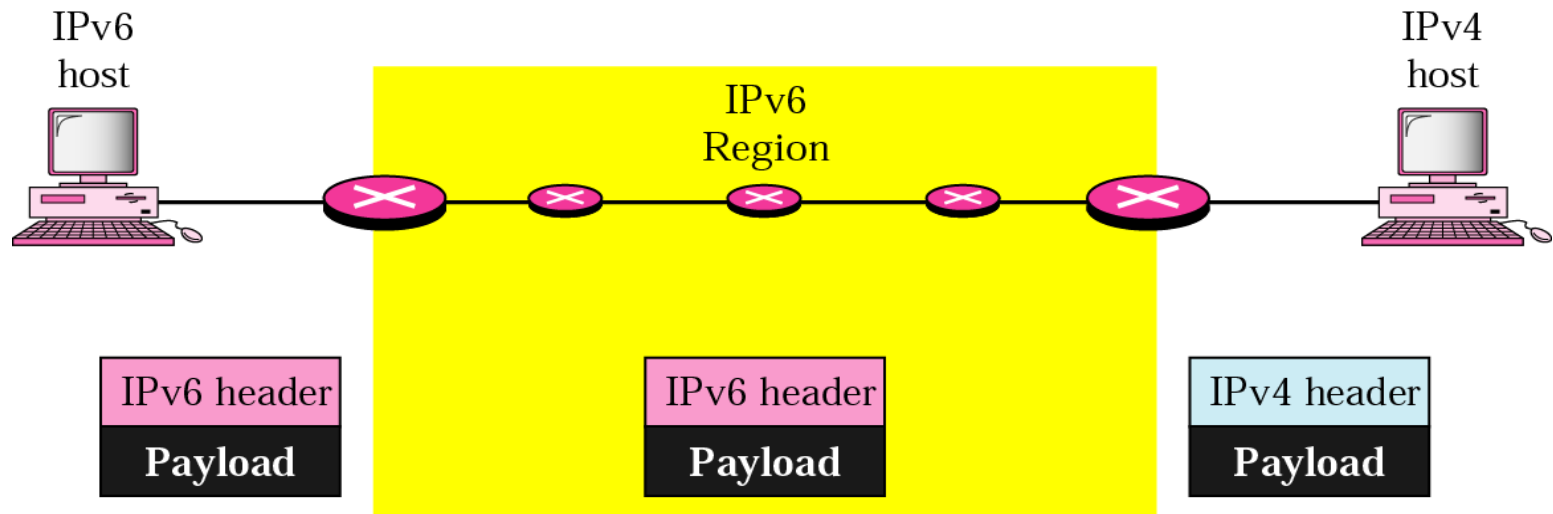


physical view:



## Header translation

- Used when majority of the Internet has moved to IPv6, but some systems still use IPv4
- Sender wants to use IPv6, but receiver does not understand IPv6
- Tunneling does not work, and the header must be changed
- Header translation uses the IPv4-mapped IPv6 address to translate an IPv6 address to an IPv4 address



# Header Translation Procedure

## *Header Translation Procedure*

1. The IPv6 mapped address is changed to an IPv4 address by extracting the rightmost 32 bits.
2. The value of the IPv6 priority field is discarded.
3. Set the type of service field in IPv4 to zero.
4. The checksum for IPv4 is calculated and inserted in the corresponding field.
5. The IPv6 flow label is ignored.
6. Compatible extension headers are converted to options and inserted in the IPv4 header.
7. The length of IPv4 header is calculated and inserted into the corresponding field.
8. The total length of the IPv4 packet is calculated and inserted in the corresponding field.

# IPv4 and IPv6 Header Comparison

## IPv4 Header

Version	IHL	Type of Service	Total Length	
Identification			Flags	Fragment Offset
Time to Live	Protocol		Header Checksum	
Source Address				
Destination Address				
Options			Padding	

## IPv6 Header

Version	Traffic Class	Flow Label		
Payload Length		Next Header	Hop Limit	
Source Address				
Destination Address				

### Legend

- Field name kept from IPv4 to IPv6
- Fields not kept in IPv6
- Name and position changed in IPv6
- New field in IPv6

## *Comparison between IPv4 options and IPv6 extension headers*

<i>Comparison</i>	
1.	The no-operation and end-of-option options in IPv4 are replaced by Pad1 and PadN options in IPv6.
2.	The record route option is not implemented in IPv6 because it was not used.
3.	The timestamp option is not implemented because it was not used.
4.	The source route option is called the source route extension header in IPv6.
5.	The fragmentation fields in the base header section of IPv4 have moved to the fragmentation extension header in IPv6.
6.	The authentication extension header is new in IPv6.
7.	The encrypted security payload extension header is new in IPv6.



# IPv6 Summary

- 128-bit address space
- revised header format
- new options
- allowance for extension
- support for special handling of packet flows
- increased security measures
- IPv6 uses hexadecimal notation with abbreviation methods
- IPv6 has 3 types of addresses: unicast, anycast, and multicast
- IPv4, ICMPv4, ARP, RARP, and IGMP replaced with IPv6 and ICMPv6
- IPv4 to IPv6 transition strategies are dualstack, tunneling, and header translation

# IPv4 vs IPv6 Header

- 1. Header length removed
- 2. ToS Class + Flow label
- 3. Total length Payload Length
- 4. Identification, flags and offset are removed
  - Fragmentation extension
- 5. TTL Hop limit
- 6. Protocol Next Header
- 7. Header checksum removed
- 8. Options Extension headers