KHOA CÔNG NGHỆ THÔNG TIN-ĐHKHTN
CSC11004 - MẠNG MÁY TÍNH NÂNG CAO

IPv6

Lê Ngọc Sơn

KHOA CÔNG NGHỆ THÔNG TIN
TRƯỜNG ĐẠI HỌC KHOA HỌC TỰ NHIÊN

fit@hcmus

A Need for IPv6?

- **IPv4 32 bit address = 4 billion hosts**
  The rising of Internet connected device and appliance will eventually deplete the IPv4 address space
- **IP is everywhere**
  Data, voice, audio and video integration is a reality Regional registries apply a strict allocation control
- **IETF IPv6 WG began in early 90s, to solve addressing growth issues:**

CIDR, NAT,...were developed

Why Not NAT ?

- It was created as a temp solution
- NAT breaks the end-to-end model
- Growth of NAT has slowed down growth of transparent applications
- NAT break security
- Many applications cannot work with NAT

IPv6 Technology

KHOA CÔNG NGHỆ THÔNG TIN
TRƯỜNG ĐẠI HỌC KHOA HỌC TỰ NHIÊN

fit@hcmus

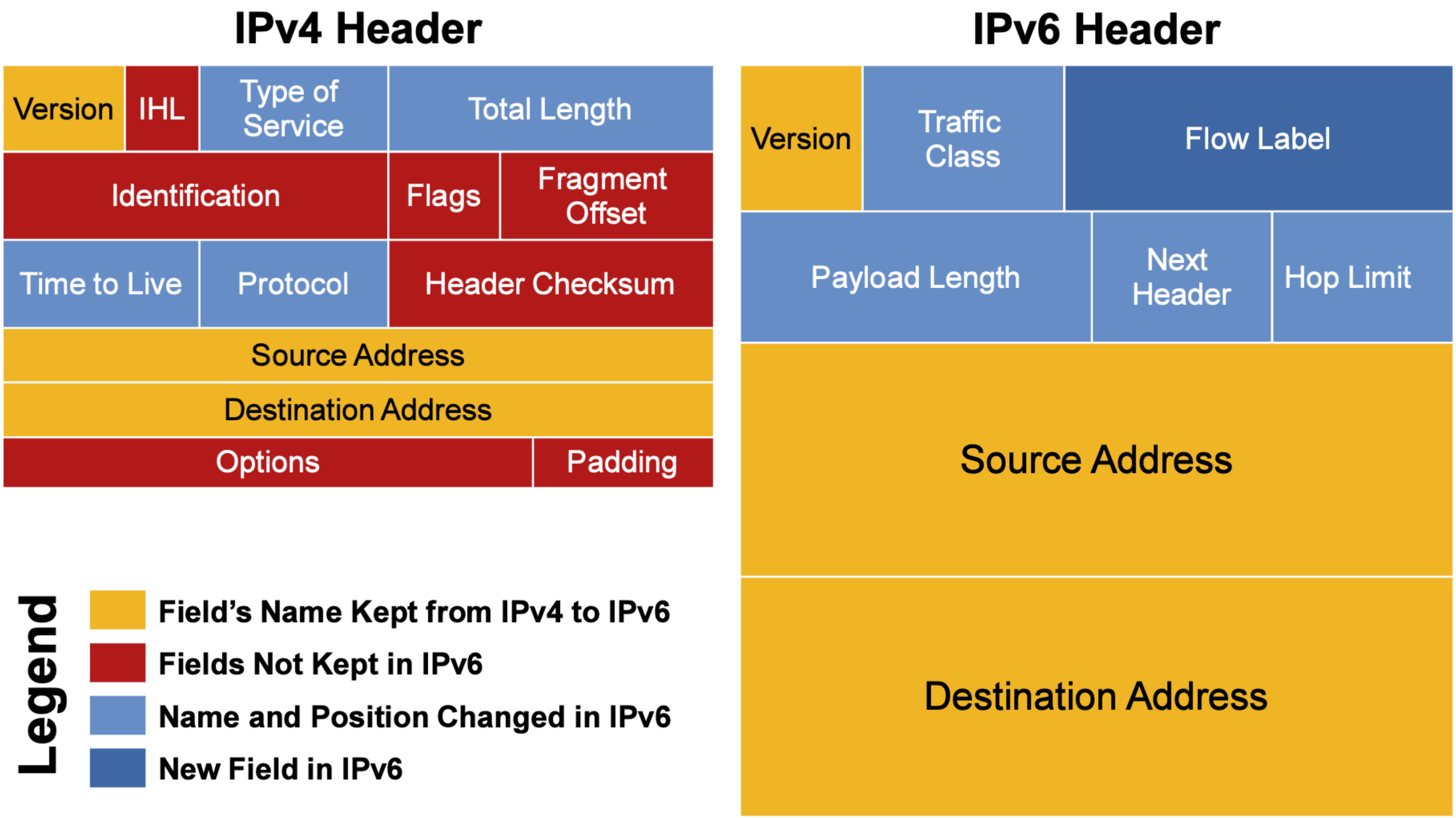
fit@hcmus

IPv6 Features

- Larger Address Space
- Simplified Header
- End-to-end Connectivity
- Auto-configuration
- Faster Forwarding/Routing
- IPSec, Mobile IP
- No Broadcast, Anycast Support
- Extensibility

fit@hcmus

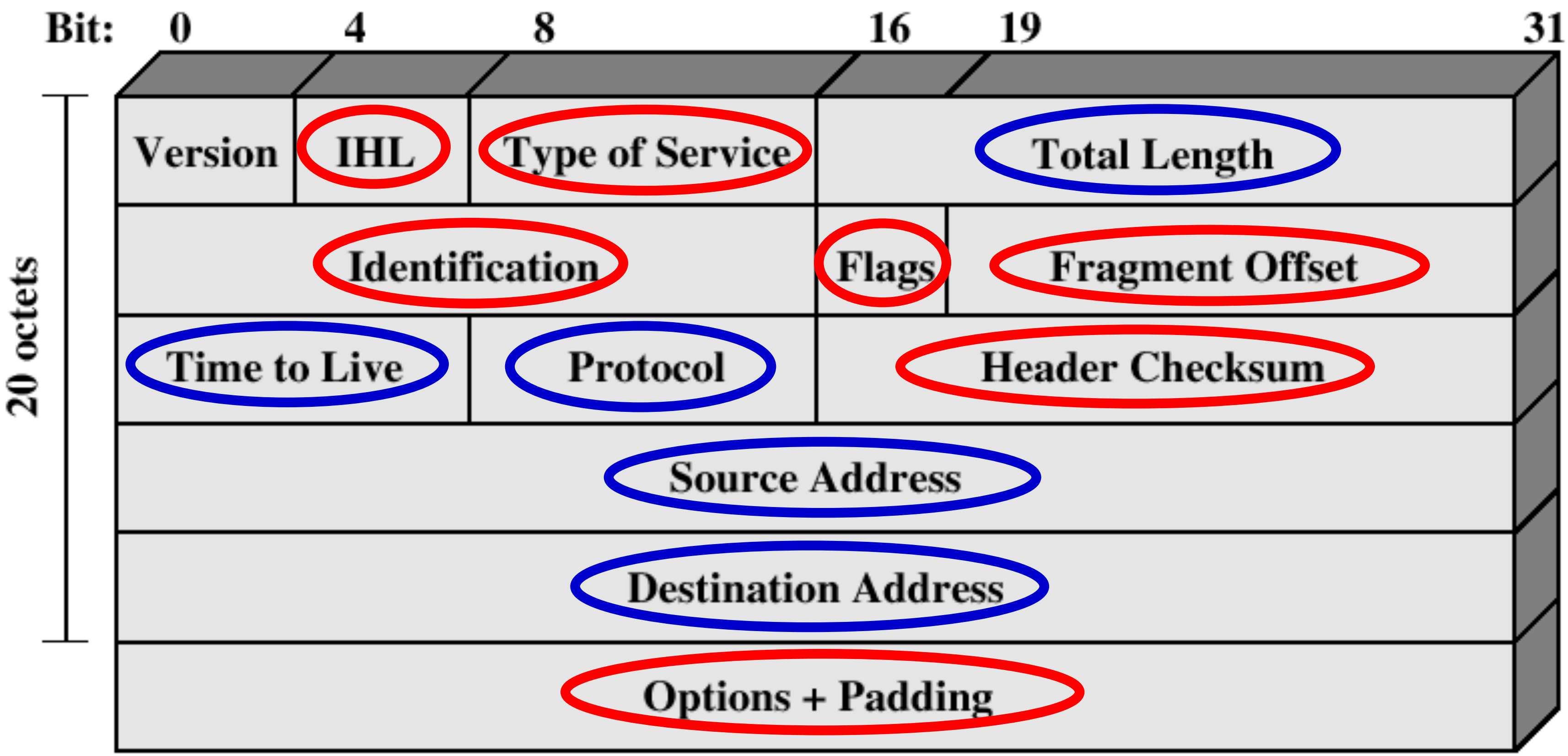
IPv4 and IPv6 Header Comparison



cdio 4.0
fit@hcmus

Header: from IPv4 to IPv6

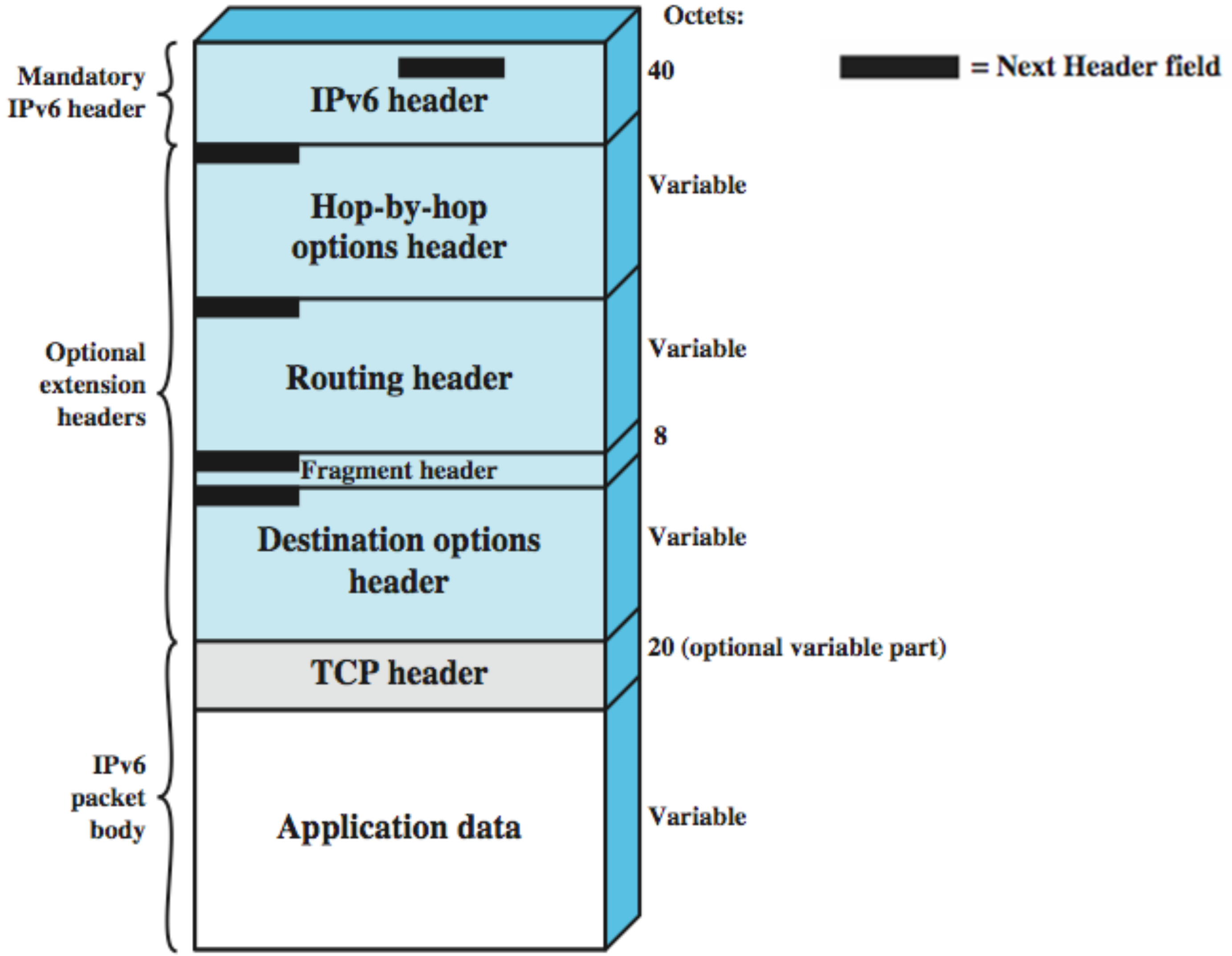
Changed
Removed



IPv6 Header Format

<table>
<tr><td colspan="8">0   1   2   3</td></tr>
<tr><td colspan="8">0 1 2 3 4 5 6 7 8 9 0 1 2 3 4 5 6 7 8 9 0 1 2 3 4 5 6 7 8 9 0 1</td></tr>
<tr><td colspan="1">Version</td><td colspan="2">Traffic Class</td><td colspan="5">Flow Label</td></tr>
<tr><td colspan="4">Payload Length</td><td colspan="2">Next Header</td><td colspan="2">Hop Limit</td></tr>
<tr><td colspan="8">Source Address</td></tr>
<tr><td colspan="8">Destination Address</td></tr>
</table>

IPv6 Packet (PDU) Structure

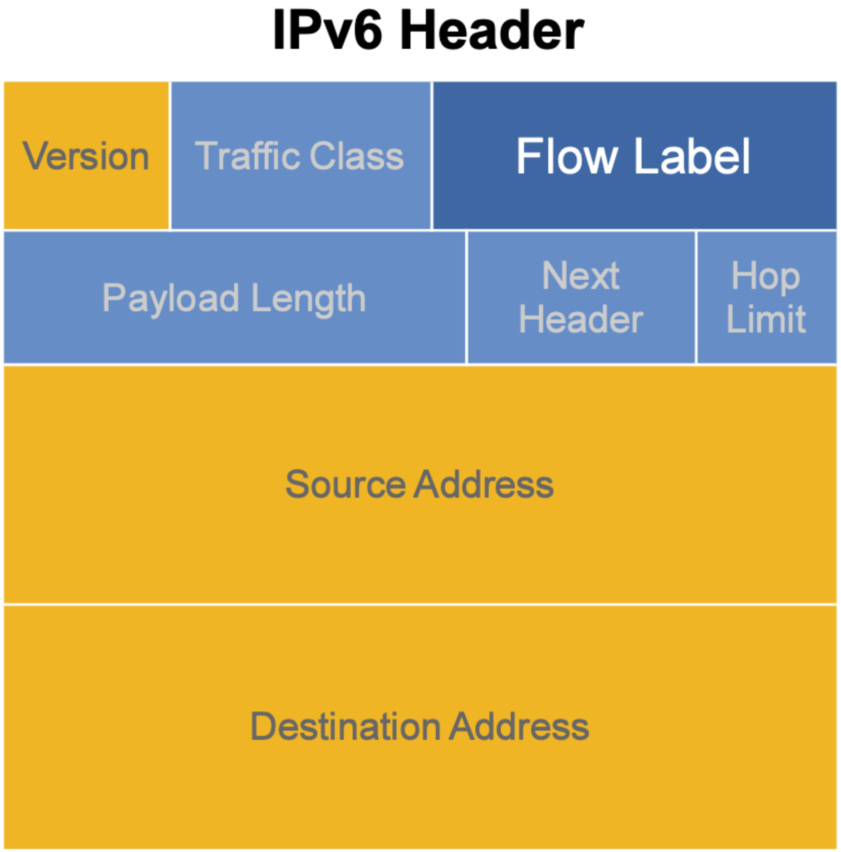


Traffic Class

- The 8-bit field in the IPv6 header is available for use by originating nodes and/or forwarding routers to identify and distinguish between different classes or priorities of IPv6 packets.
  - E.g., used as the codepoint in DiffServ
- Equivalent to IPv4's Type of Service

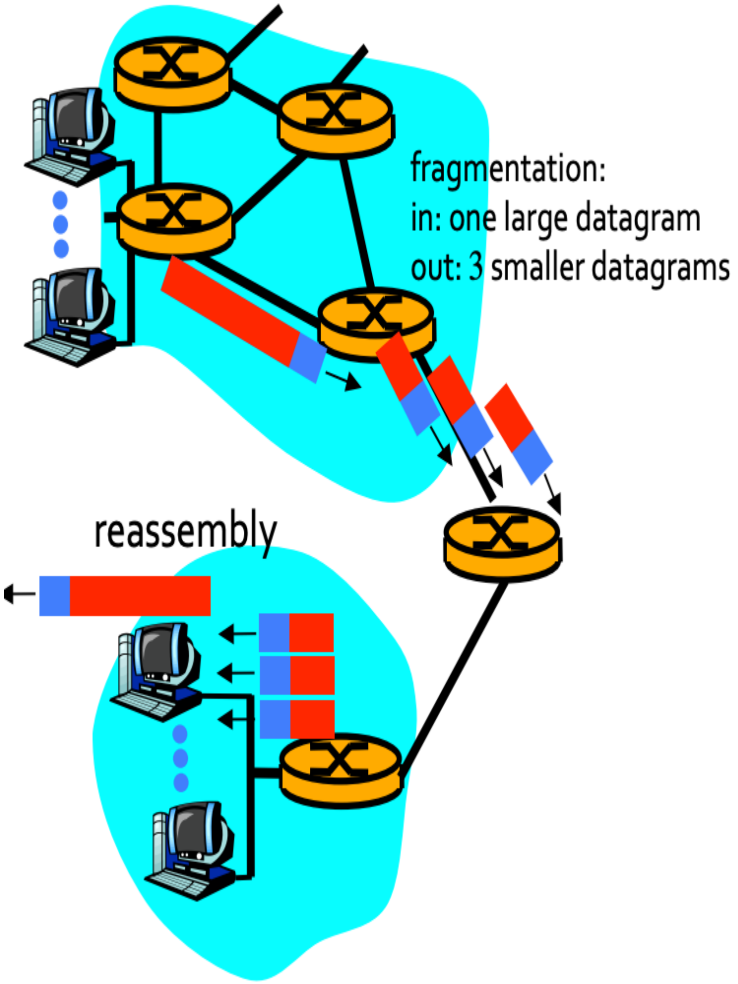
IPv6 Flow Label

- 20-Bit Flow Label Field to Identify Specific Flows Needing Special QoS
  - Flow classifiers had been based on 5-tuple: Source/destination address, protocol type and port numbers of transport
  - With flow label, each source chooses its own flow label values; routers use source addr + flow label to identify distinct flows
  - Flow label value of 0 used when no special QoS requested (the common case today)

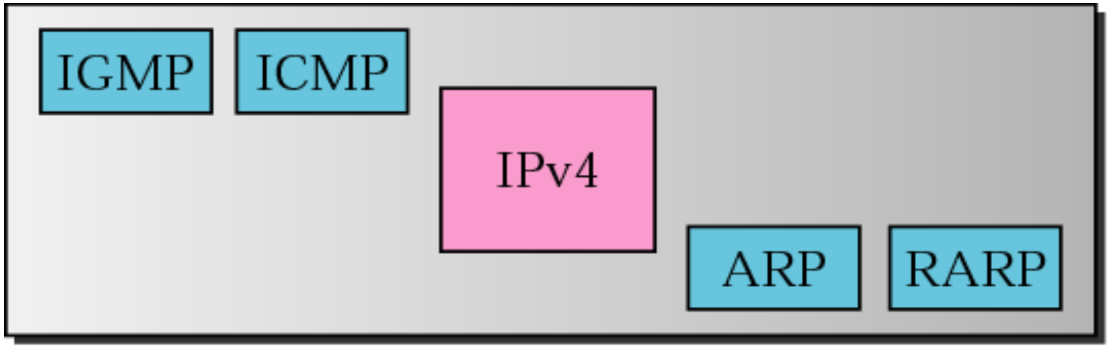


Path MTU Discovery

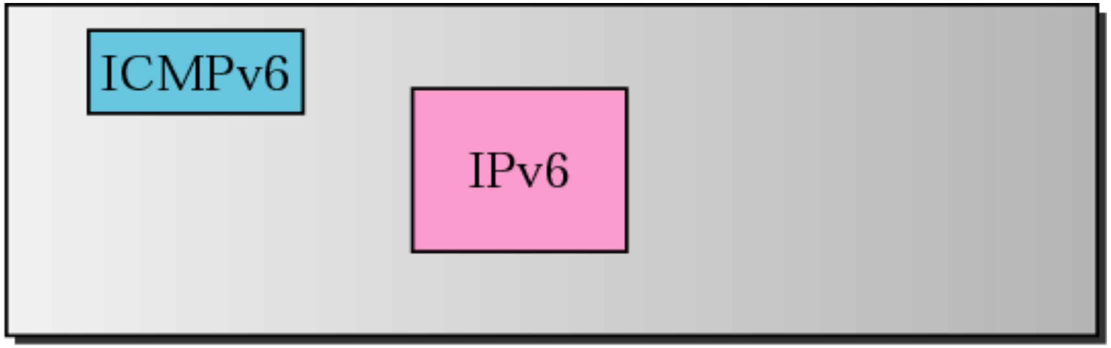
- Network links have MTU (maximum transmission unit) – the largest possible link-level frame
- As in IPv4, path MTU discovery in IPv6 allows a host to dynamically discover and adjust to differences in the MTU size of every link along a given data path.
- In IPv6, however, fragmentation is handled by the source of a packet when the path MTU of one link along a given data path is not large enough to accommodate the size of the packets.
- Having IPv6 hosts handle packet fragmentation saves IPv6 router processing resources and helps IPv6 networks run more efficiently.
- In IPv6, the minimum link MTU is 1280 octets.



Network Layer in v4 & v6



Network layer in version 4



Network layer in version 6

IPv6 Addressing

TRƯỜNG ĐẠI HỌC KHOA HỌC TỰ NHIÊN
TP. HO CHI MINH
KHTN
cdio 4.0
KHOA CÔNG NGHỆ THÔNG TIN
TRƯỜNG ĐẠI HỌC KHOA HỌC TỰ NHIÊN
fit@hcmus

Overview

IPv4 32-bits

IPv6 128-bits

2^{32} = 4,294,967,296

2^{128} = 340,282,366,920,938,463,463,374,607,431,768,211,456

$2^{128} = 2^{32} * 2^{96}$

2^{96} = 79,228,162,514,264,337,593,543,950,336 times the number of possible IPv4 Addresses (79 trillion trillion)

Overview

$$\frac{2^{128}}{6.5 \text{ Billion}} = \text{52 Trillion Trillion IPv6 addresses per person}$$

World's population is approximately 6.5 billion

$$\frac{\text{52 Trillion Trillion}}{\text{100 Billion}} = $$

523 Quadrillion (523 thousand trillion) IPv6 addresses for every human brain cell on the planet!

Typical brain has ~100 billion brain cells (your count may vary)

Overview

- Representation
  - 16-bit hexadecimal numbers
  - Numbers are separated by (:)
  - Hex numbers are not case sensitive
- Abbreviations are possible
  - Leading zeros in contiguous block could be represented by (::)
  - Double colon only appears once in the address

Addressing Format

$$\underbrace{\texttt{3FFE:085B:1F1F:0000:0000:0000:}\textcolor{red}{\texttt{00A9:1234}}}_{}$$

128bits = 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

cdio 4.0
fit@hcmus

Addressing

Prefix Representation

- Representation of prefix is just like CIDR
- In this representation you attach the prefix length like v4 address: 198.10.0.0/16
- IPv6 address is represented the same way: 2001:db8:12::/48
- Only leading zeros are omitted. Trailing zeros are not omitted

2001:0db8:0012::/48 = 2001:db8:12::/48
2001:db8:1200:adfc::/64 # 2001:db8:12:adfc::/64

Types of IPv6 Addresses

- Unicast
  - Address of a single interface
  - Delivery to single interface
- Multicast
  - Address of a set of interfaces
  - Delivery to all interfaces in the set
- Anycast
  - Address of a set of interfaces
  - Delivery to a single interface in the set
- No more broadcast addresses

Unicast Address

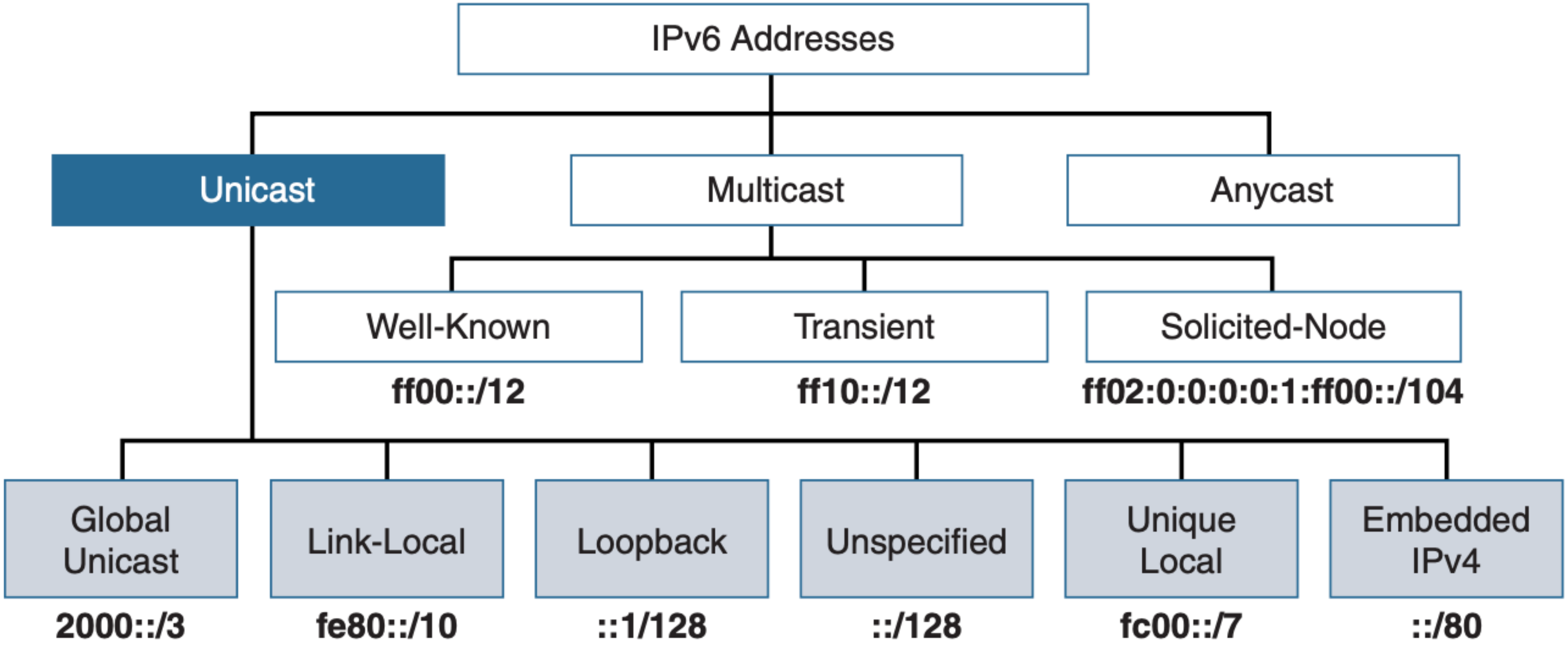
KHOA CÔNG NGHỆ THÔNG TIN
TRƯỜNG ĐẠI HỌC KHOA HỌC TỰ NHIÊN

fit@hcmus

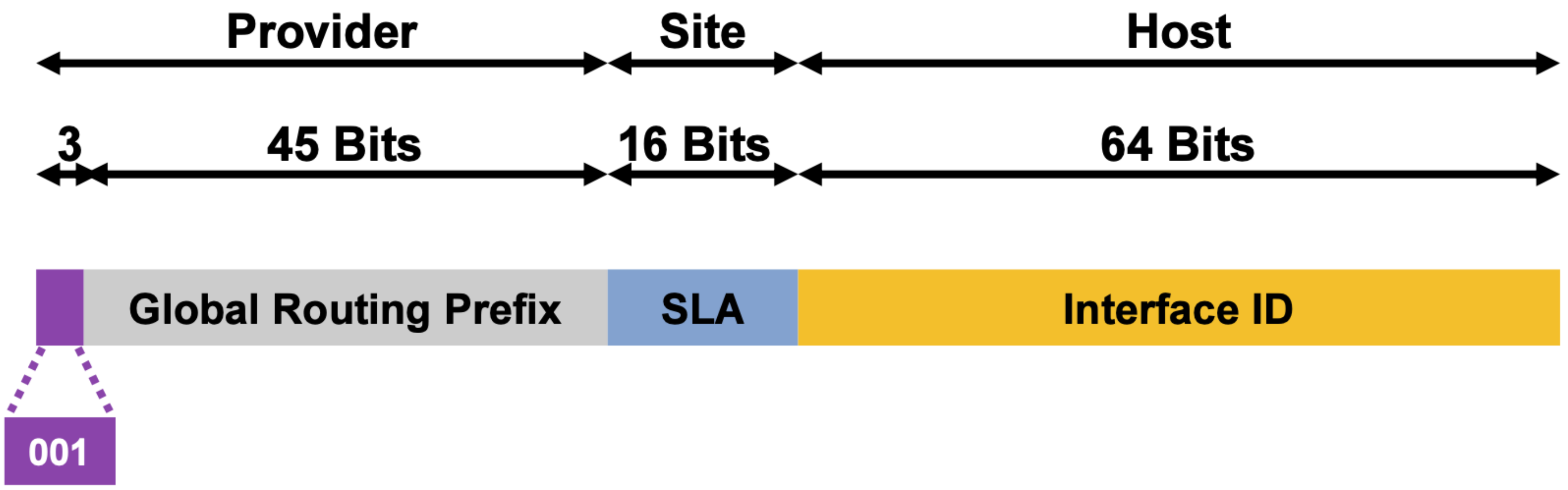
IPv6 Addressing Model

- Addresses are assigned to interfaces, not hosts
- Interface expected to have multiple addresses

Unicast Address



Global Unicast Address



- Addresses for generic use of IPv6
- Interface ID is Constructed in Modified EUI-64 format

fit@hcmus

Global Unicast Address

- There are several ways a device can be configured with a global unicast address:
  - Manually configured.
  - Stateless Address Autoconfiguration.
  - Stateful DHCPv6.

Example 4-1 *Viewing IPv6 Addresses on Windows and Mac OS*

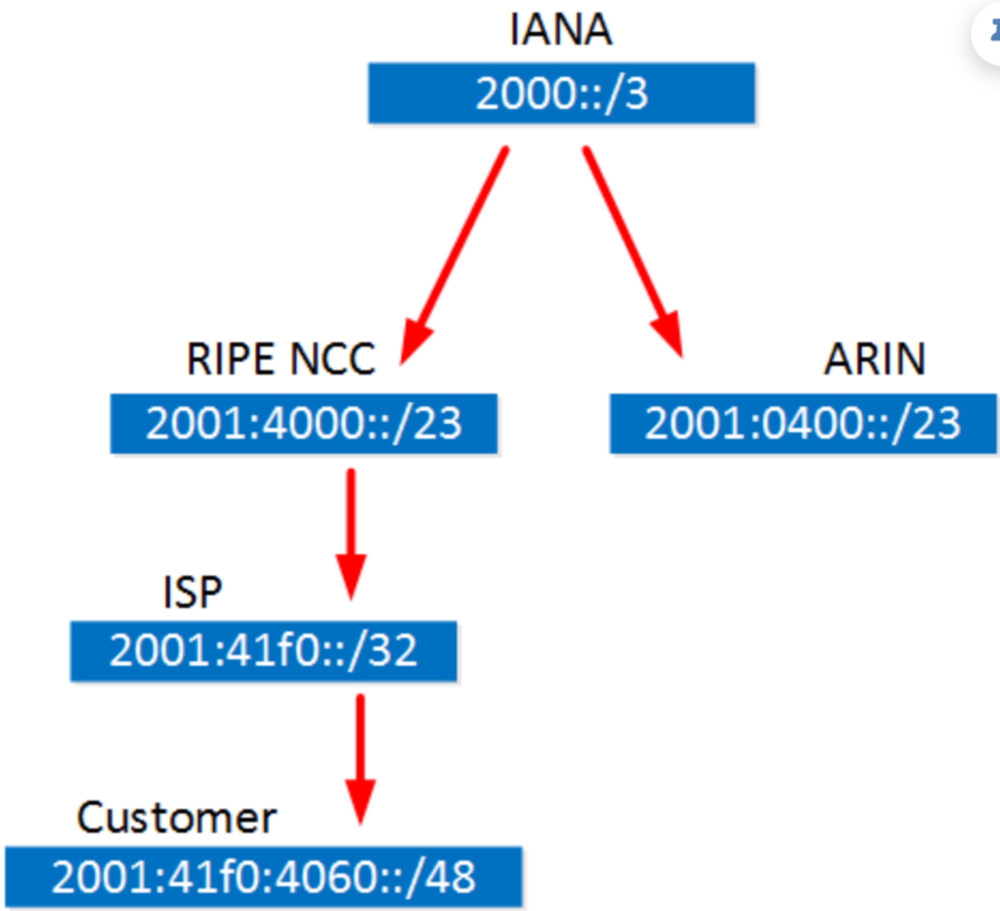
```
Windows-OS> ipconfig
Ethernet adapter Local Area Connection:
   Connection-specific DNS Suffix  . :
   ! IPv6 GUA
   IPv6 Address. . . . . . . . . . . : 2001:db8:cafe:1:d0f8:9ff6:4201:7086
   ! IPv6 Link-Local
   Link-local IPv6 Address . . . . . : fe80::d0f8:9ff6:4201:7086%11
   IPv4 Address. . . . . . . . . . . : 192.168.1.100
   Subnet Mask . . . . . . . . . . . : 255.255.255.0
   ! IPv6 Default Gateway
   Default Gateway . . . . . . . . . : fe80::1%11
                                       192.168.1.1
----------------------------------------------------------------------------------
Mac-OS$ ifconfig
en1: flags=8863<UP,BROADCAST,SMART,RUNNING,SIMPLEX,MULTICAST> mtu 1500
   ether 60:33:4b:15:24:6f
   ! IPv6 Link-Local
   inet6 fe80::6233:4bff:fe15:246f%en1 prefixlen 64 scopeid 0x5
   inet 192.168.1.111 netmask 0xffffff00 broadcast 192.168.1.255
   ! IPv6 GUA
   inet6 2001:db8:cafe:1:4bff:fe15:246f prefixlen 64 autoconf
   media: autoselect
   status: active
```

IPv6 Global Unicast Prefix Assignments

IANA “owns” the entire IPv6 address space and they assign certain prefixes to the RIRs (Regional Internet Registry). There are 5 RIRs at the moment

- AFRINIC: Africa
- APNIC: Asia/Pacific
- ARIN: North America
- LACNIC: Latin America and some Caribbean Islands
- RIPE NCC: Europe, Middle east and Central Asia

IPv6 Global Unicast Prefix Assignments



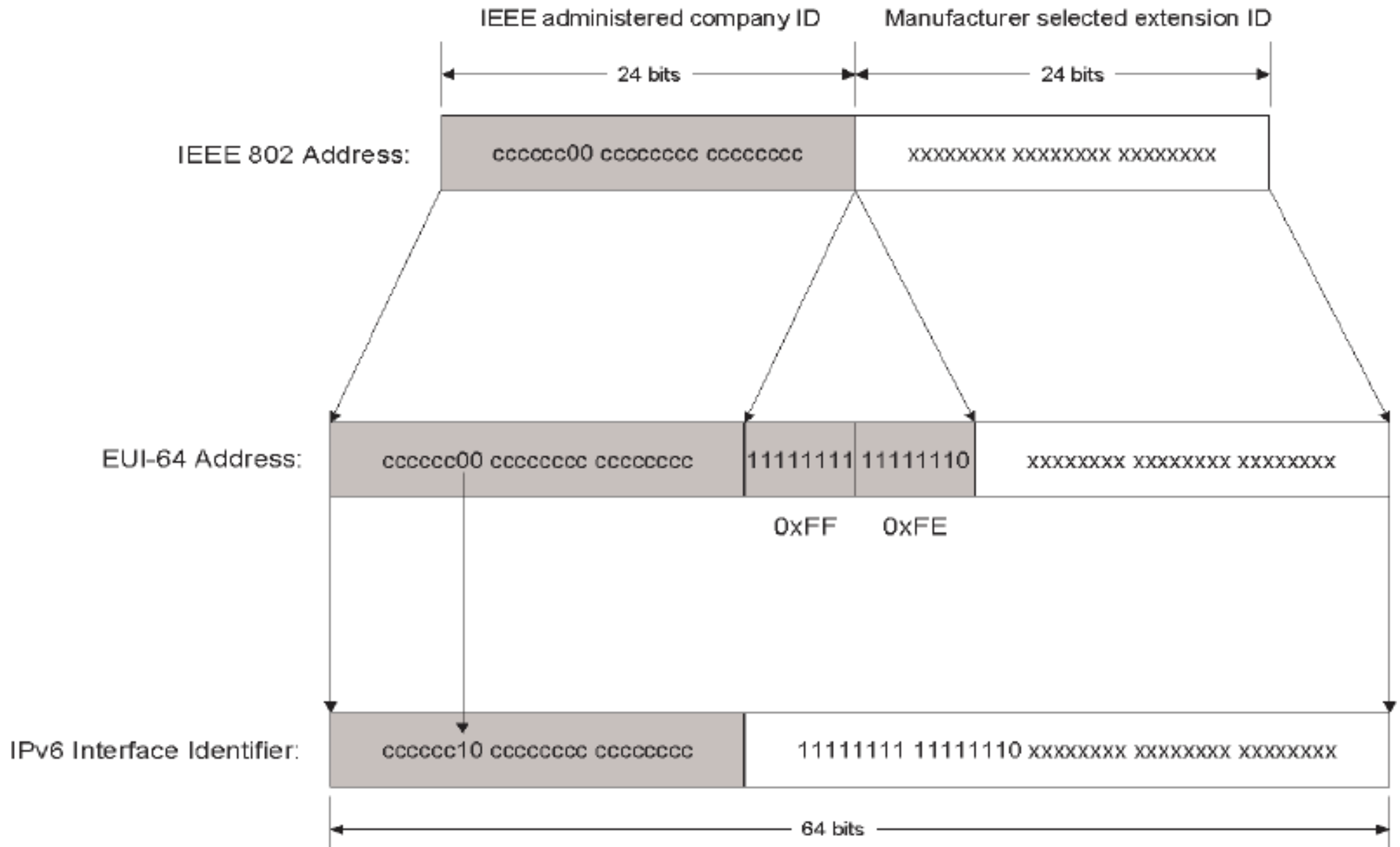
- IANA is using the 2000::/3 prefix for global unicast address space.
- According to this list, RIPE NCC received prefix 2001:4000::/23 from IANA.
- A large ISP called Ziggo in The Netherlands receives prefix 2001:41f0::/32 from RIPE NCC.
- The ISP assigns prefix 2001:41f0:4060::/48 to one of their customers.

Interface Identifier

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
- possibly other methods in the future

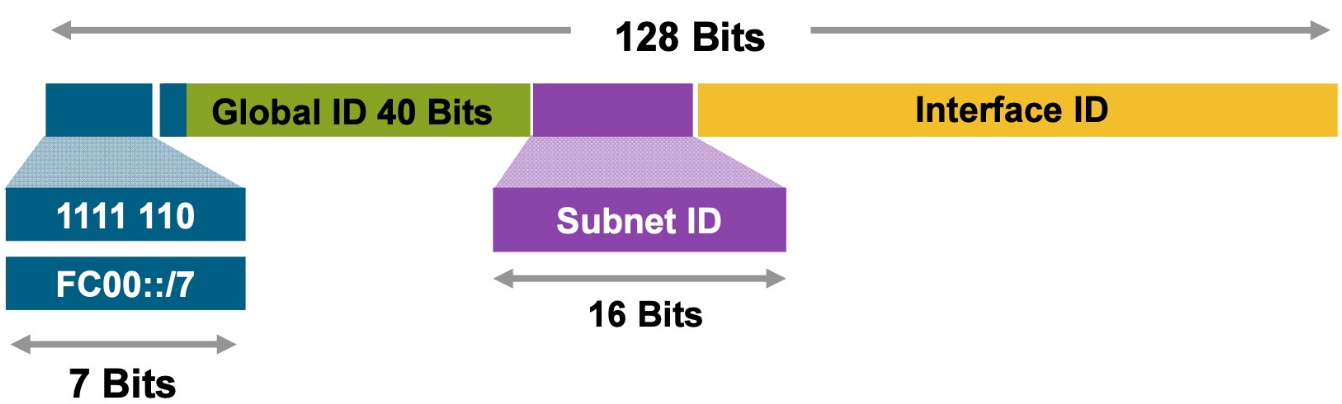
IEEE 802 → IPv6 Interface ID



fit@hcmus

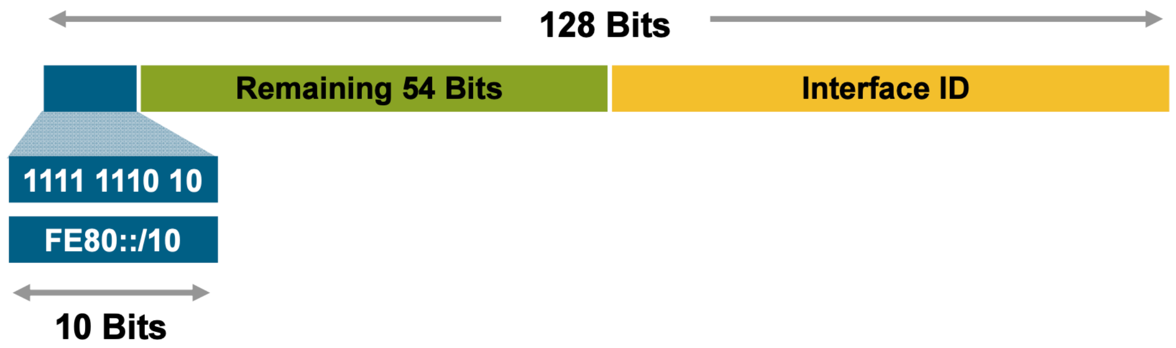
Unique Local Address

- Meaningful only in a single site zone, and may be re-used in other sites
- Equivalent to the IPv4 private address
- Manually configured by network administrators within an organization
- Prefix= FC00::/7



Link Local Address

- **Link-Local Addresses Used for:**
  - have a limited scope and are only valid and reachable within a single network segment or link. They cannot be used for communication outside of that specific network segment
  - not routable outside of the local network segment.
  - Link-local addresses are typically automatically generated by devices without the need for DHCP or manual configuration
  - Prefix is FE80::/10, remaining 54 bits could be Zero or any manual configured value



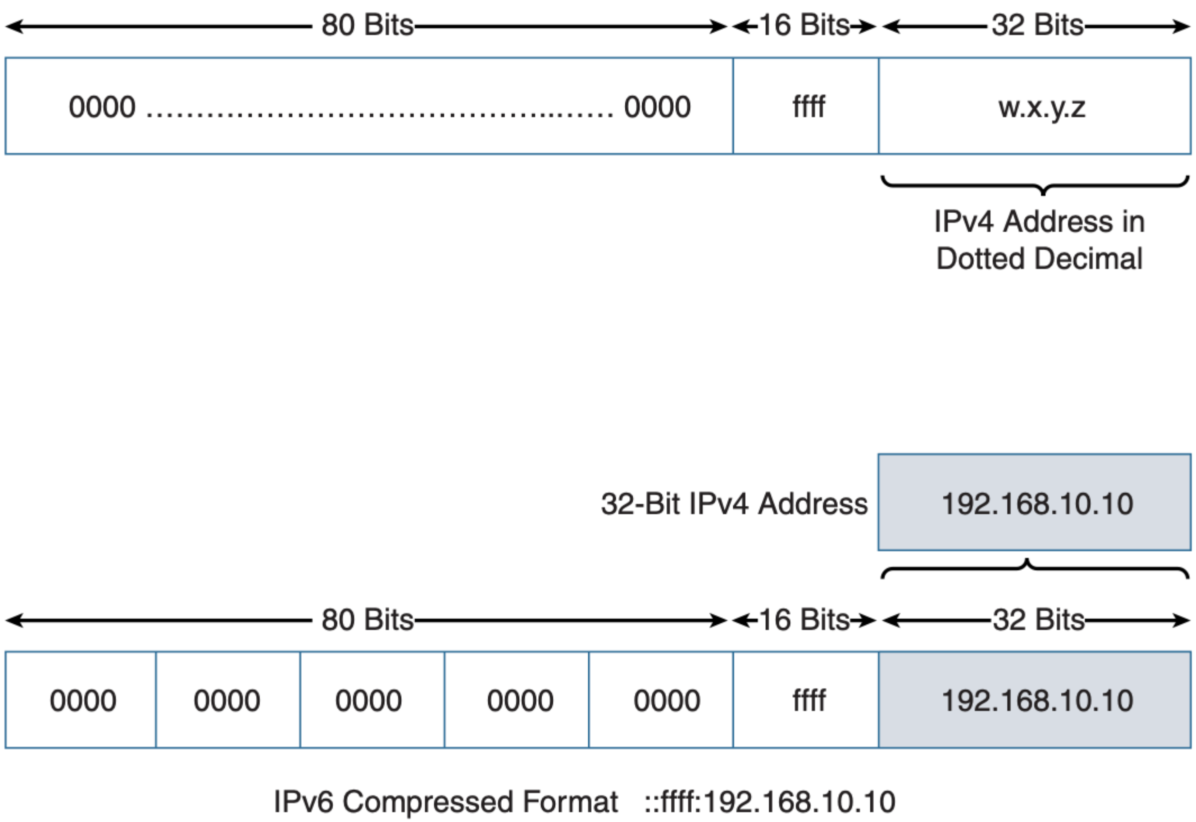
Special IPv6 Address

- **Loopback address (0:0:0:0:0:0:0:1 or ::1)**
  - An address not assigned to any physical interface that can be used for a host to send an IPv6 packet to itself
  - It is equivalent to the IPv4 address block 127.0.0.0/8, most commonly the 127.0.0.1 loopback address.
- **Unspecified Addresses ::**
  - An unspecified unicast address is an all-0s address
  - An unspecified unicast address is used as a source address to indicate the absence of an address.
    It cannot be assigned to an interface.

Special IPv6 Address

IPv4-Mapped IPv6 Addresses

IPv4-mapped IPv6 addresses can be used by a dual-stack device that needs to send an IPv6 packet to an IPv4-only device

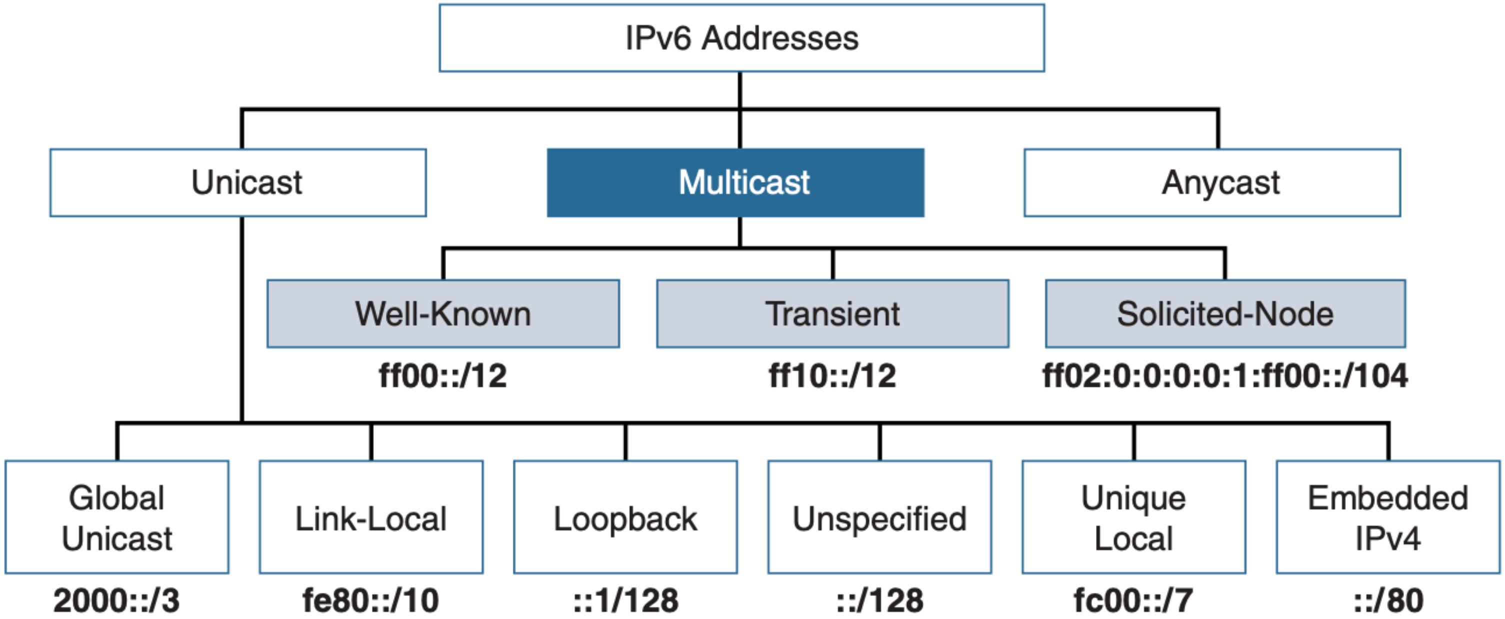


Multicast Address

KHOA CÔNG NGHỆ THÔNG TIN
TRƯỜNG ĐẠI HỌC KHOA HỌC TỰ NHIÊN

fit@hcmus

Multicast Address



fit@hcmus

IPv6 Multicast Address

Prefix FF00::/8 (1111 1111); the second octet defines the lifetime and scope of the multicast address

8-bit	4-bit	4-bit	112-bit
1111 1111	Lifetime	Scope	Group-ID

Lifetime	
0	If Permanent
1	If Temporary

Scope	
1	Node
2	Link
5	Site
8	Organization
E	Global

cdio 4.0
fit@hcmus

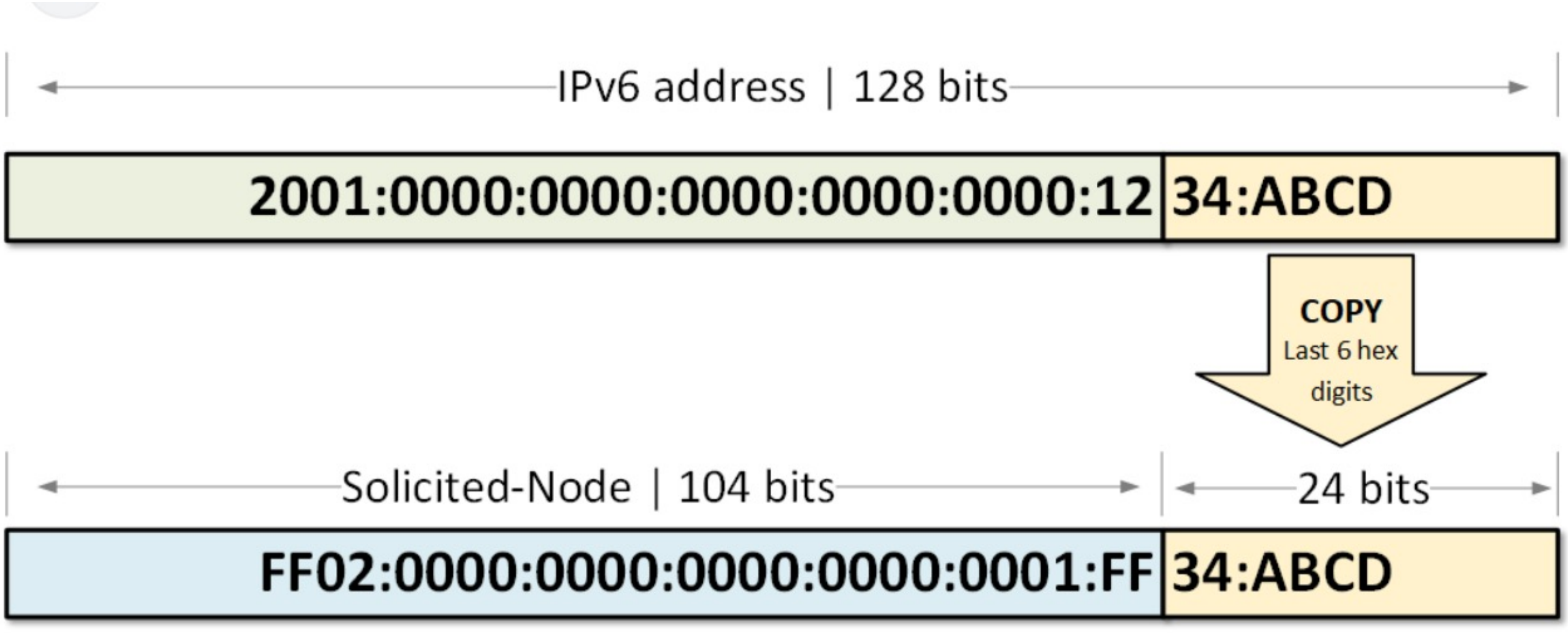
Some Common Multicast Addresses

- FF02::1 – all nodes on local network segment.
- FF02::2 – all routers on local network segment.
- FF02::5 – all OSPFv3 routers.
- FF02::6 – all OSPFv3 DR routers.
- FF02::9 – RIPng routers
- FF02::A – EIGRP routers

cdio 4.0
fit@hcmus

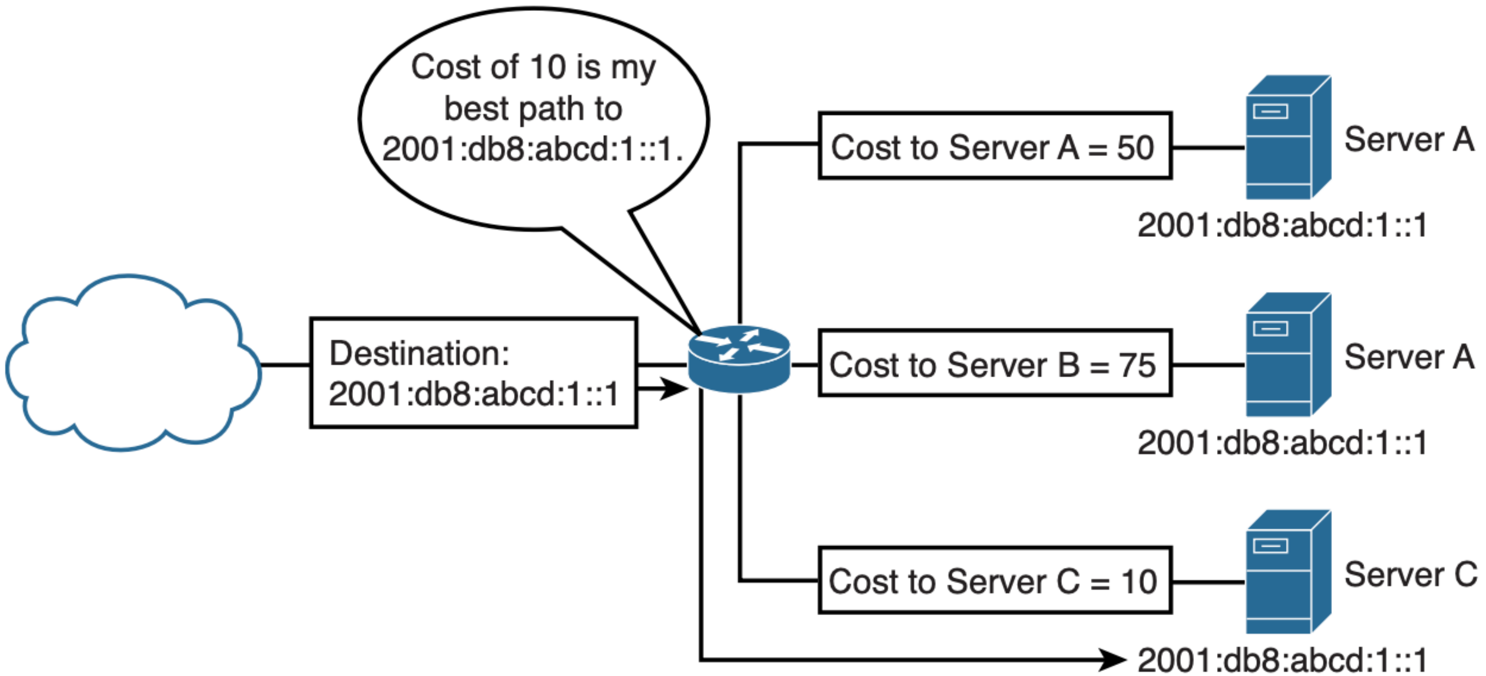
IPv6 Solicited Node Multicast Address

Every device that uses an IPv6 address will also compute and join a solicited node multicast group address. This address is used for layer two address discovery.



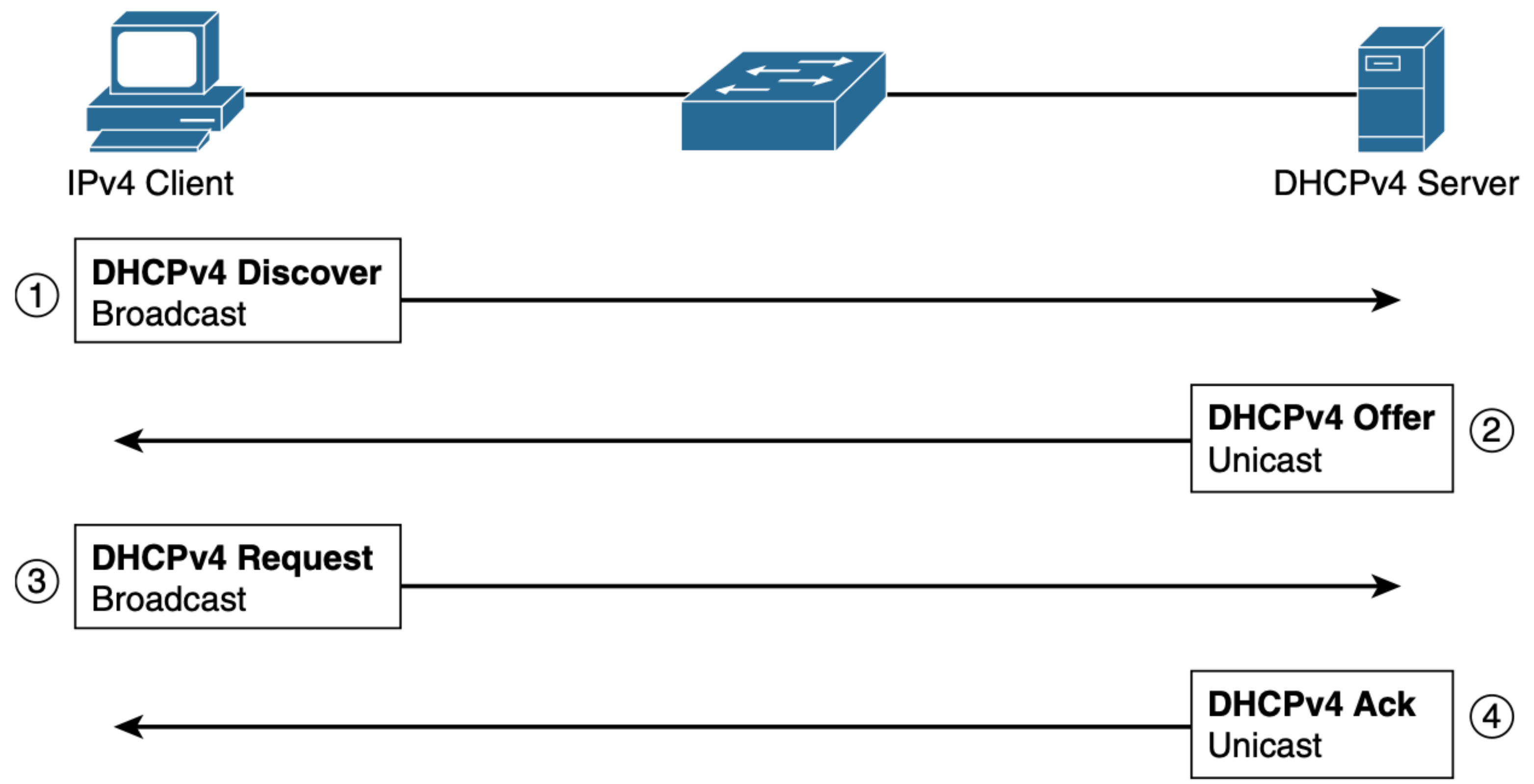
Anycast Address

- An IPv6 anycast address is an address that can be assigned to more than one interface (typically different devices)
- A packet sent to an anycast address is routed to the "nearest" interface having that address, according to the router's routing table

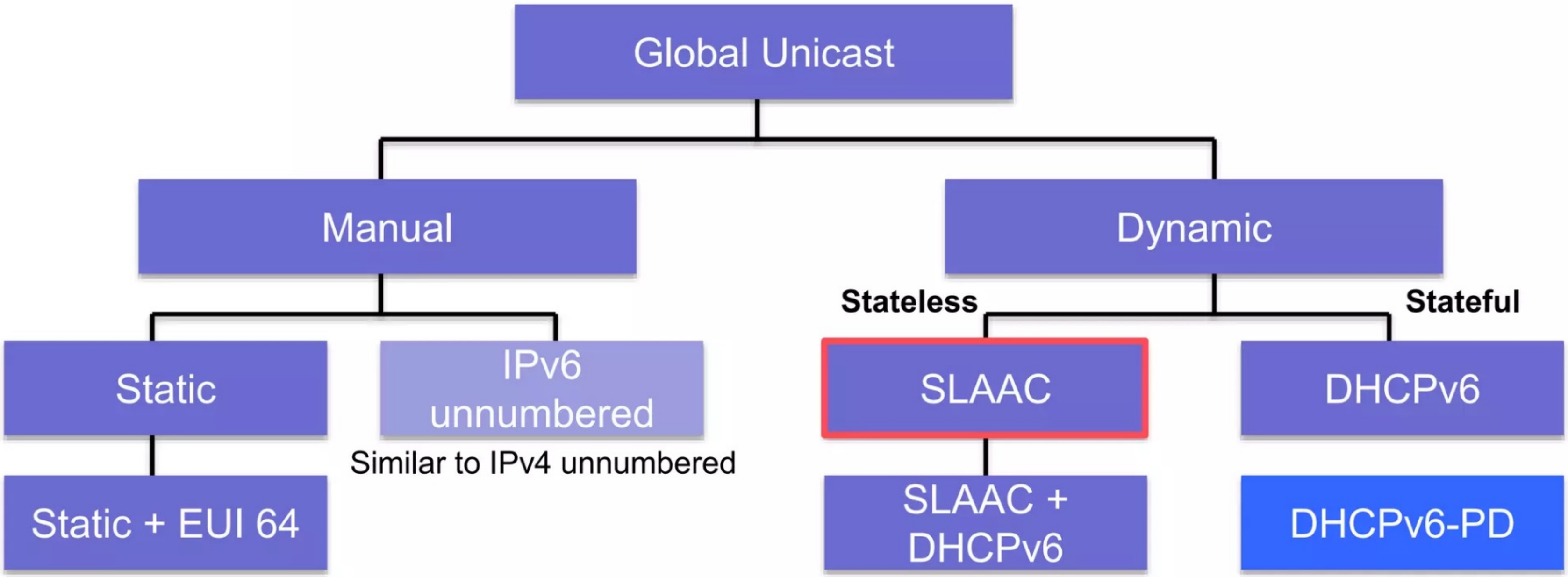


Dynamic Addressing

Dynamic IPv4 Address Allocation: DHCPv4



Dynamic IPv6 Address Allocation



Option 1: SLAAC – No DHCPv6 (Default on Cisco routers)

"I'm *everything* you need (Prefix, Prefix-length, Default Gateway)"

Option 2: SLAAC + Stateless DHCPv6 for DNS address

"Here is my information but you need to get other information such as DNS addresses from a **DHCPv6 server**." (DNS can be in RA)

Option 3: All addressing except default gateway use DHCPv6

"I can't help you. Ask a **DHCPv6** server for all your information."

Introducing ICMPv6 Neighbor Discovery

- Node (Hosts and Routers) use ND to determinate the link-layer addresses for neighbors known to reside on attached links and quick purge cached valued that become invalid. Hosts also use ND to find neighboring router that willing to forward packets on their behalf
- Neighbor Discovery uses five ICMPv6 messages:
  - Router–device messages used for dynamic address allocation:
    - **Router Solicitation (RS)** message
    - **Router Advertisement (RA)** message
  - Device–device messages used for address resolution:
    - **Neighbor Solicitation (NS)** message
    - **Neighbor Advertisement (NA)** message
  - Router–device messages used for better first-hop selection:
    - **Redirect message**

Router Solicitation and Advertisement

1—ICMP Type = 133 (RS)

Src = link-local address (FE80::1/10)

Dst = all-routers multicast address (FF02::2)

Query = please send RA

2—ICMP Type = 134 (RA)

Src = link-local address (FE80::2/10)

Dst = all-nodes multicast address (FF02::1)

Data = options, subnet prefix, lifetime, autoconfig flag

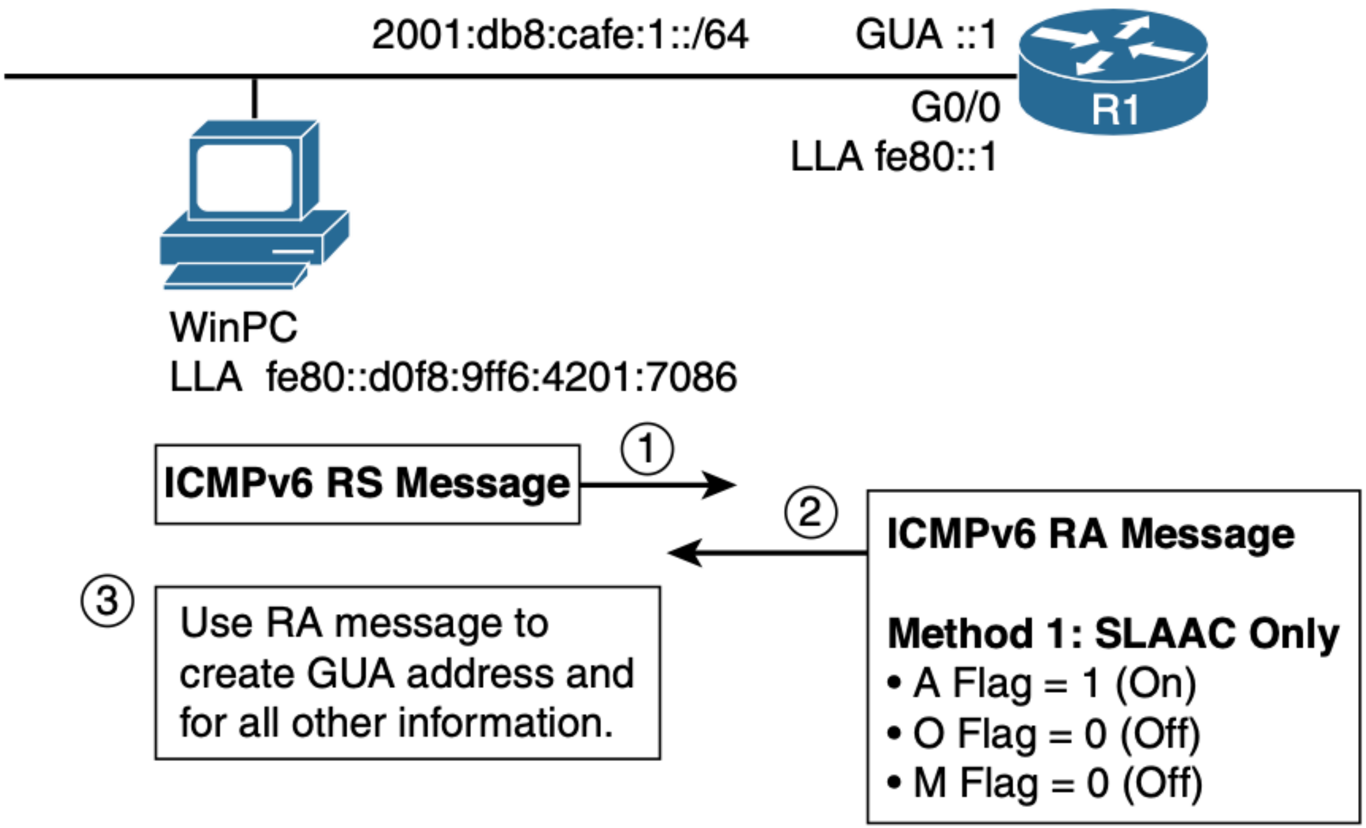
- Router solicitations (RS) are sent by booting nodes to request RAs for configuring the interfaces
- Routers send periodic Router Advertisements (RA) to the all-nodes multicast address

Router Advertisment Method and the A,O, M flag

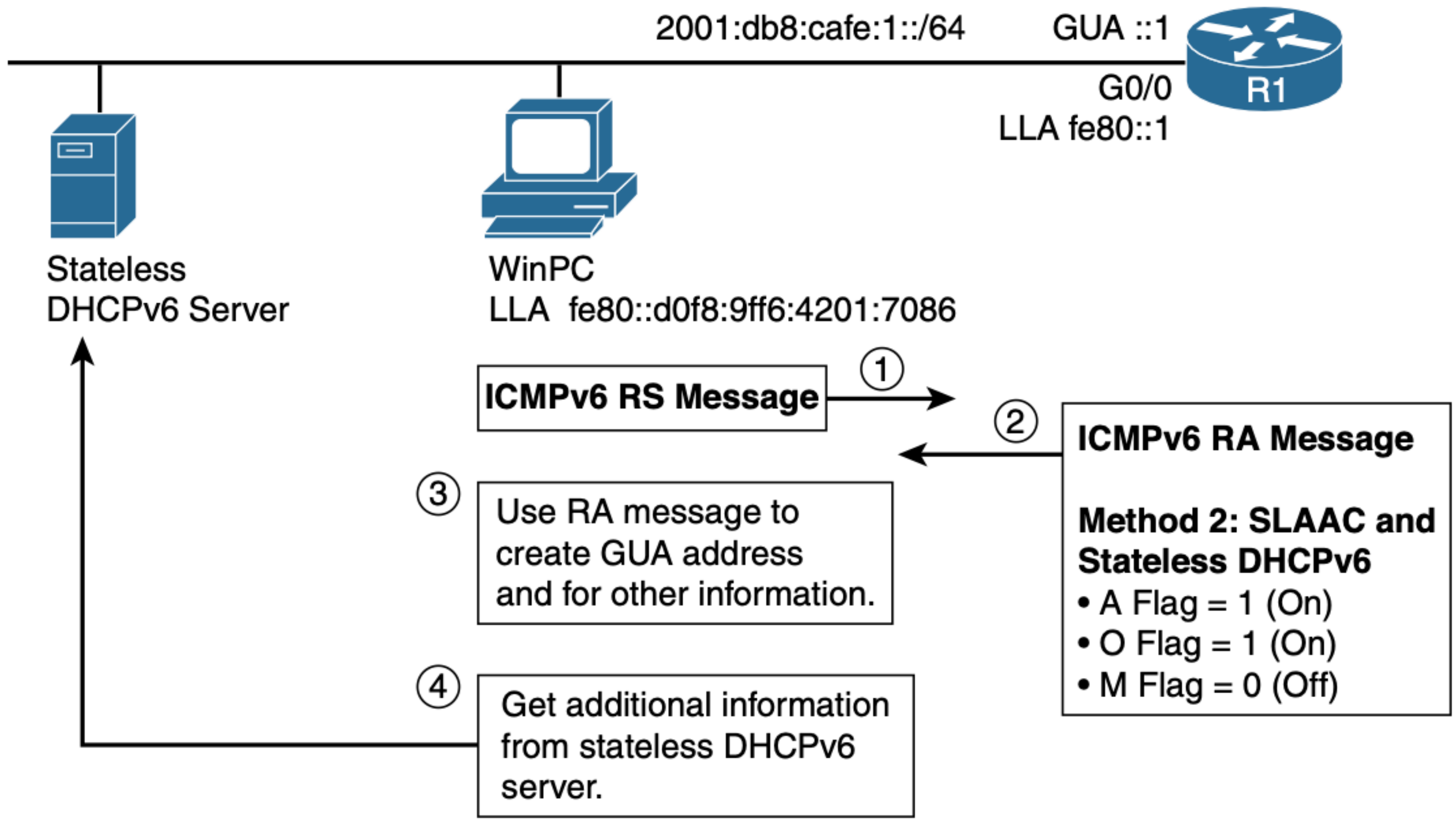
- **M (Managed Address Configuration)**:The M flag indicates whether a host should use DHCPv6 (Dynamic Host Configuration Protocol for IPv6) for address configuration.
- **O (Other Configuration)** flag indicates whether other (non-address) configuration information is available from DHCPv6.
- **A (Autonomous Address Configuration):** flag indicates whether a host should perform Stateless Address Autoconfiguration (SLAAC) to generate its own IPv6 addresses.

RA Address Allocation Method	A Flag (SLAAC)	O Flag (Stateless DHCPv6)	M Flag (Stateful DHCPv6)
Method 1: SLAAC (default)	1 (on)	0 (off)	0 (off)
Method 2: SLAAC and stateless DHCPv6	1 (on)	1 (on)	0 (off)
Method 3: Stateful DHCPv6	0 (off)	N/A	1 (on)

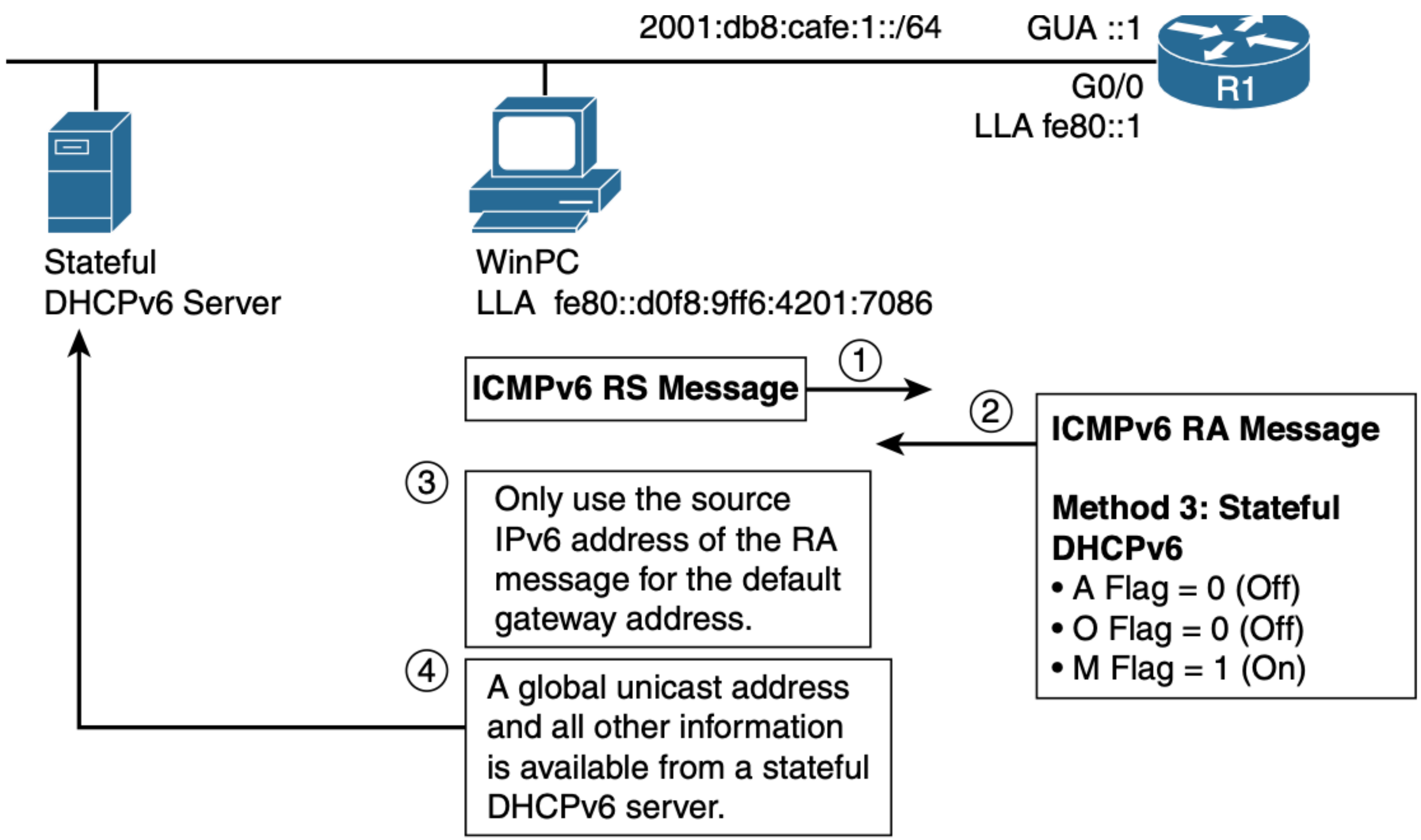
Method 1: SLAAC



Method 2: SLAAC + Stateless DHCPv6



Method 3: Statefull DHCPv6



ICMPv6 and Neighbor Discovery

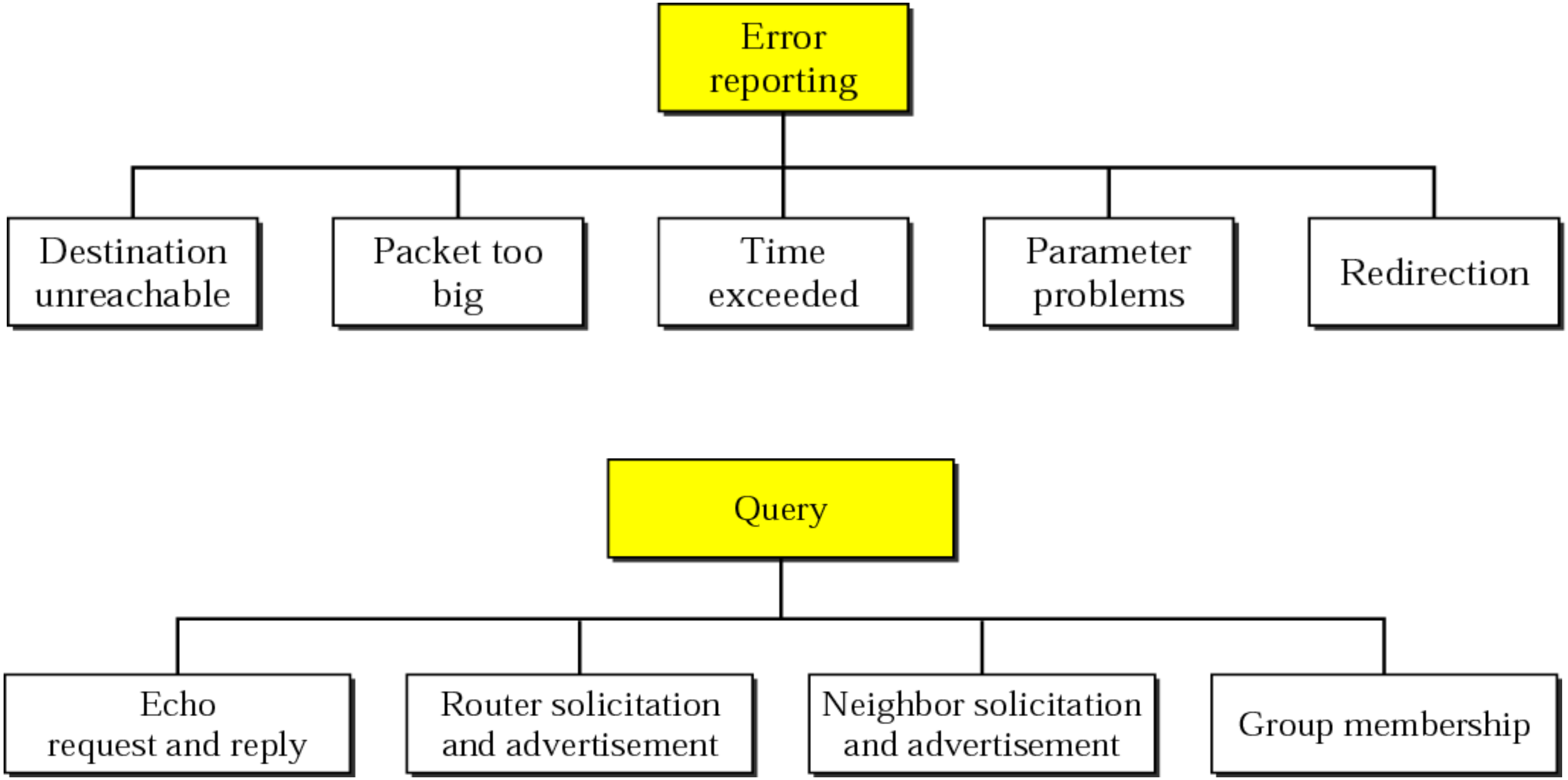
KHOA CÔNG NGHỆ THÔNG TIN
TRƯỜNG ĐẠI HỌC KHOA HỌC TỰ NHIÊN

fit@hcmus

ICMPv6

- Modification of ICMP from IPv4
- Next Header value= 58
- Report delivery or forwarding errors
- Provide simple echo service for troubleshooting
- Neighbor Discovery (ND): 5 ICMP messages
- Multicast Listener Discovery (MLD): 3 ICMP messages

ICMPv6 Messages



Neighbor Discovery (ND)

- Node (Hosts and Routers) use ND to determinate the link-layer addresses for neighbors known to reside on attached links. Hosts also use ND to find neighboring router that willing to forward packets on their behalf
- Neighbor Discovery uses five ICMPv6 messages:
  - Router–device messages used for dynamic address allocation:
    - **Router Solicitation (RS)** message
    - **Router Advertisement (RA)** message
  - Device–device messages used for address resolution:
    - **Neighbor Solicitation (NS)** message
    - **Neighbor Advertisement (NA)** message
  - Router–device messages used for better first-hop selection:
    - **Redirect message**

Neighbor Solicitation and Advertisement

Neighbor Solicitation
ICMP type = 135

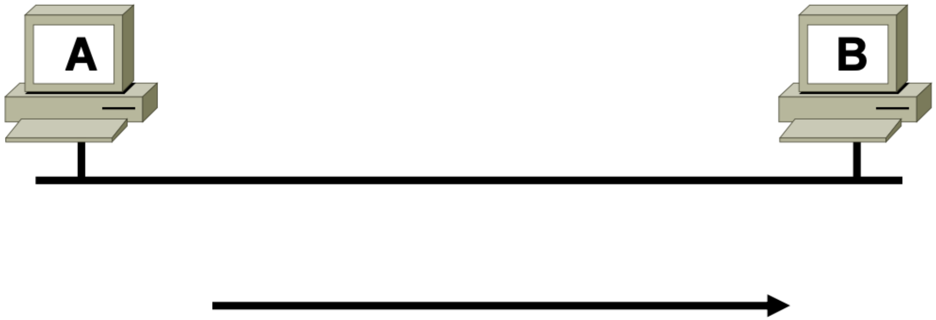
Src = A
Dst = Solicited-node multicast of B
Data = link-layer address of A
Query = what is your link address?

Neighbor Advertisement
ICMP type = 136
Src = B
Dst = A
Data = link-layer address of B

A and B can now exchange packets on this link

Duplicate Address Detection

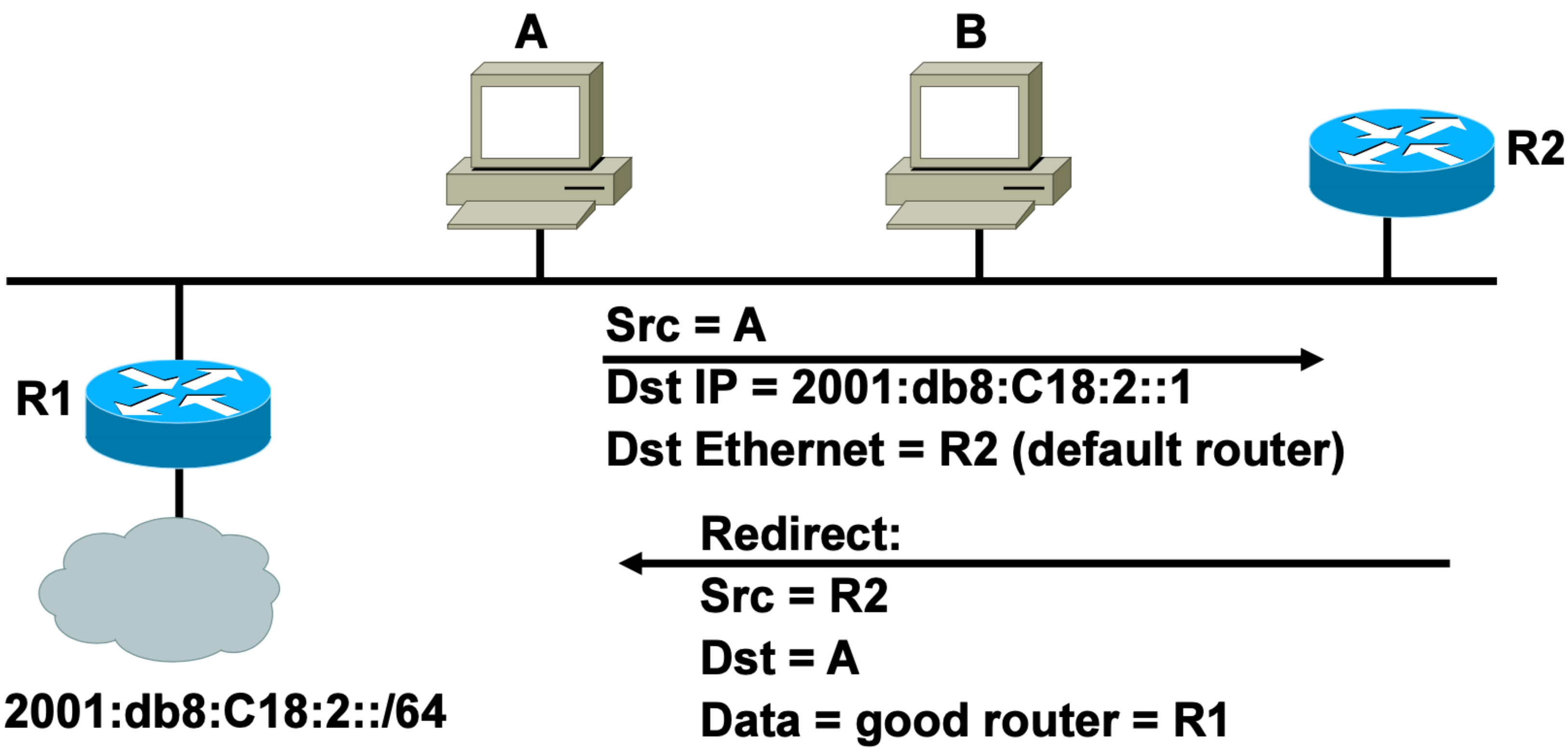
fit@hcmus




```
ICMP type = 135
Src = 0   (::)
Dst = Solicited-node multicast of A
Data = link-layer address of A
Query = what is your link address?
```

Duplicate Address Detection (DAD) uses neighbor solicitation to verify the existence of an address to be configured

Redirect



Redirect is used by a router to signal the reroute of a packet to a better router

Routing in IPv6

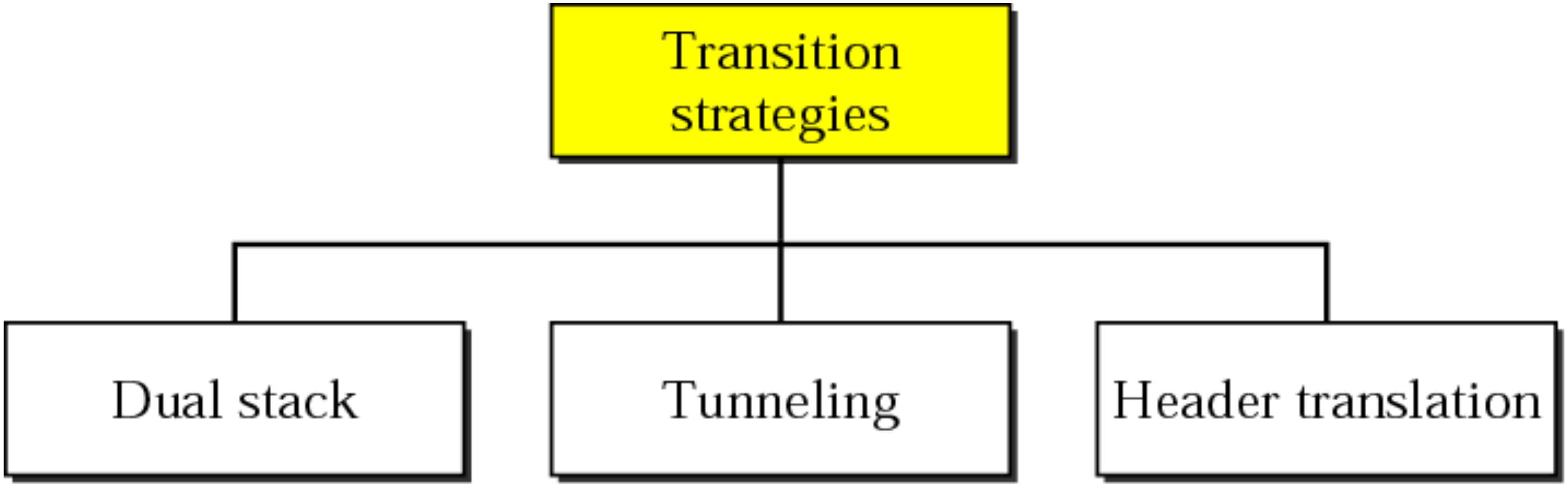
- As in IPv4, IPv6 has 2 families of routing protocols: IGP and EGP, and still uses the longest-prefix match routing algorithm
- IGP
  - RIPng (RFC 2080)
  - Cisco EIGRP for IPv6
  - OSPFv3 (RFC 2740)
  - Integrated IS-ISv6 (draft-ietf-isis-ipv6-02)
- EGP : MP-BGP4 (RFC 2858 and RFC 2545)

ICMPv6 Deployment

KHOA CÔNG NGHỆ THÔNG TIN
TRƯỜNG ĐẠI HỌC KHOA HỌC TỰ NHIÊN

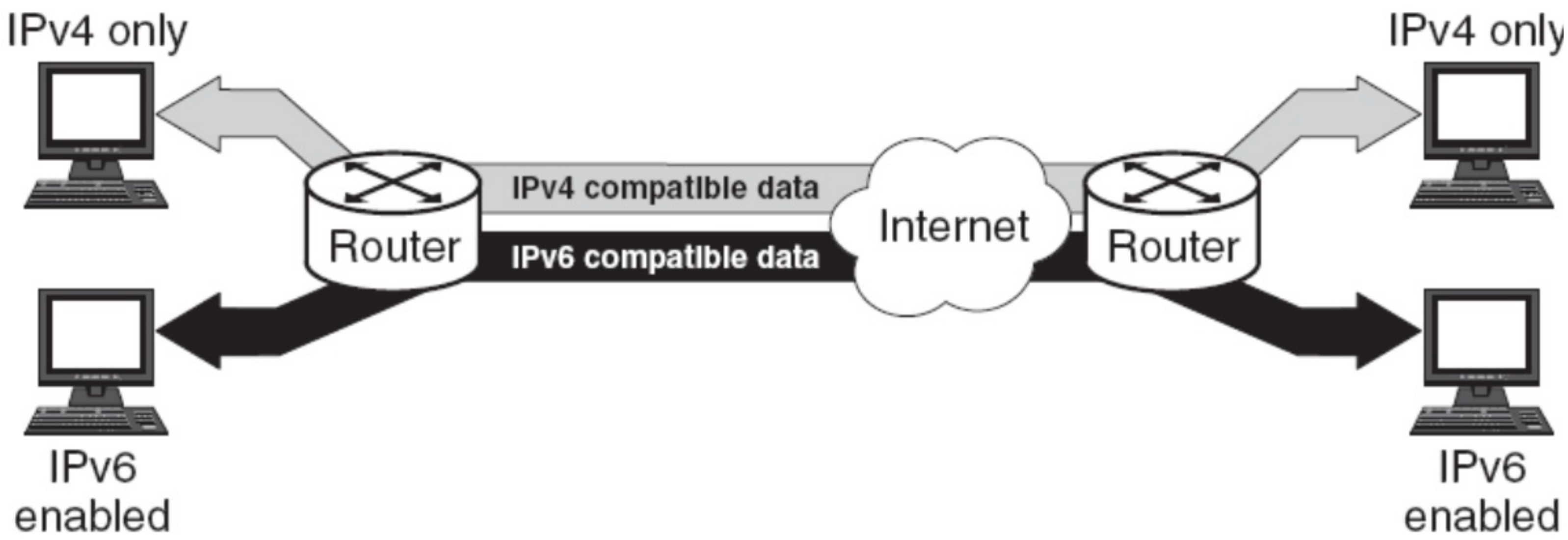
fit@hcmus

Transition from IPv4 to IPv6



- **Dual-stack techniques**
  - to allow IPv4 and IPv6 to co-exist in the same devices and networks
- **Tunneling techniques**
  - to avoid order dependencies when upgrading hosts, routers, or regions
- **Translation techniques**
  - to allow IPv6-only devices to communicate with IPv4-only devices

Dual Stack

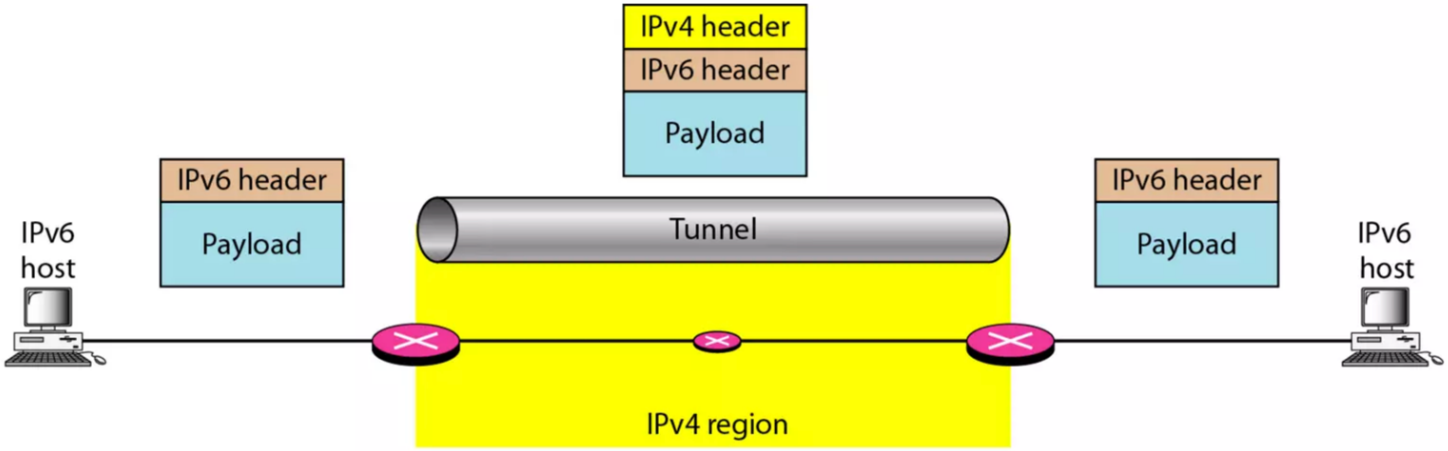


- Both IPv4 and IPv6 stacks enabled
- Applications can talk to both
- Choice of the IP version is based on name lookup and application preference

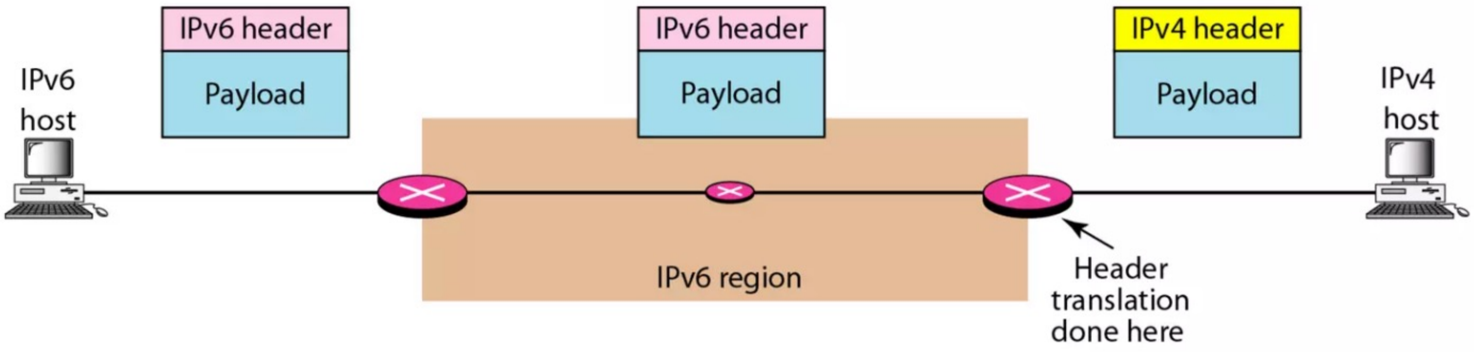
Tunneling

There are several tunneling types for IPv6:

- **6to4 tunnel**
- **ISATAP (Intra-Site Automatic Tunnel Addressing Protocol) tunnel**
- **GRE (Generic Routing Encapsulation) tunnel**
- **IPv6 Rapid Deployment (6rd) tunnels**



Header Translation



Q&A