Internet Protocol, Version 6 (IPv6)

MẠNG MÁY TÍNH NÂNG CAO

lnson@fit.hcmus.edu.vn

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

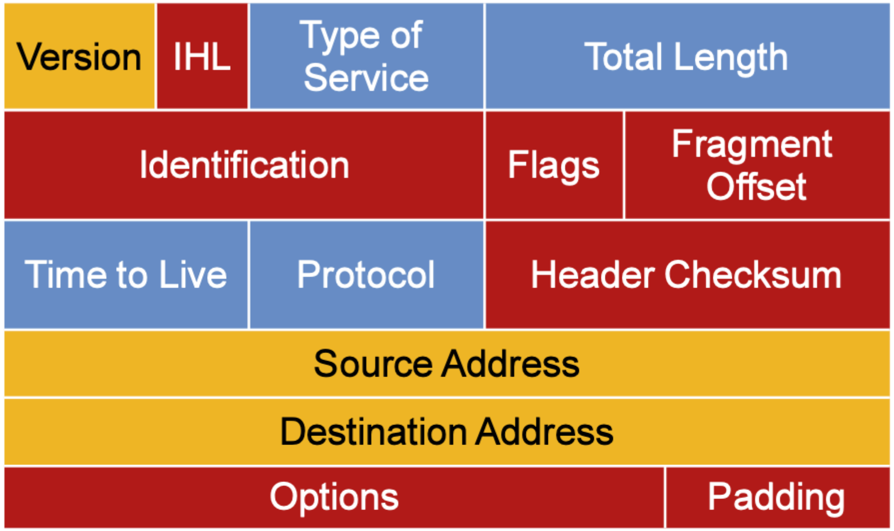
IPv6 Technology

IPv6 Features

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

IPv4 and IPv6 Header Comparison

IPv4 Header



IPv6 Header

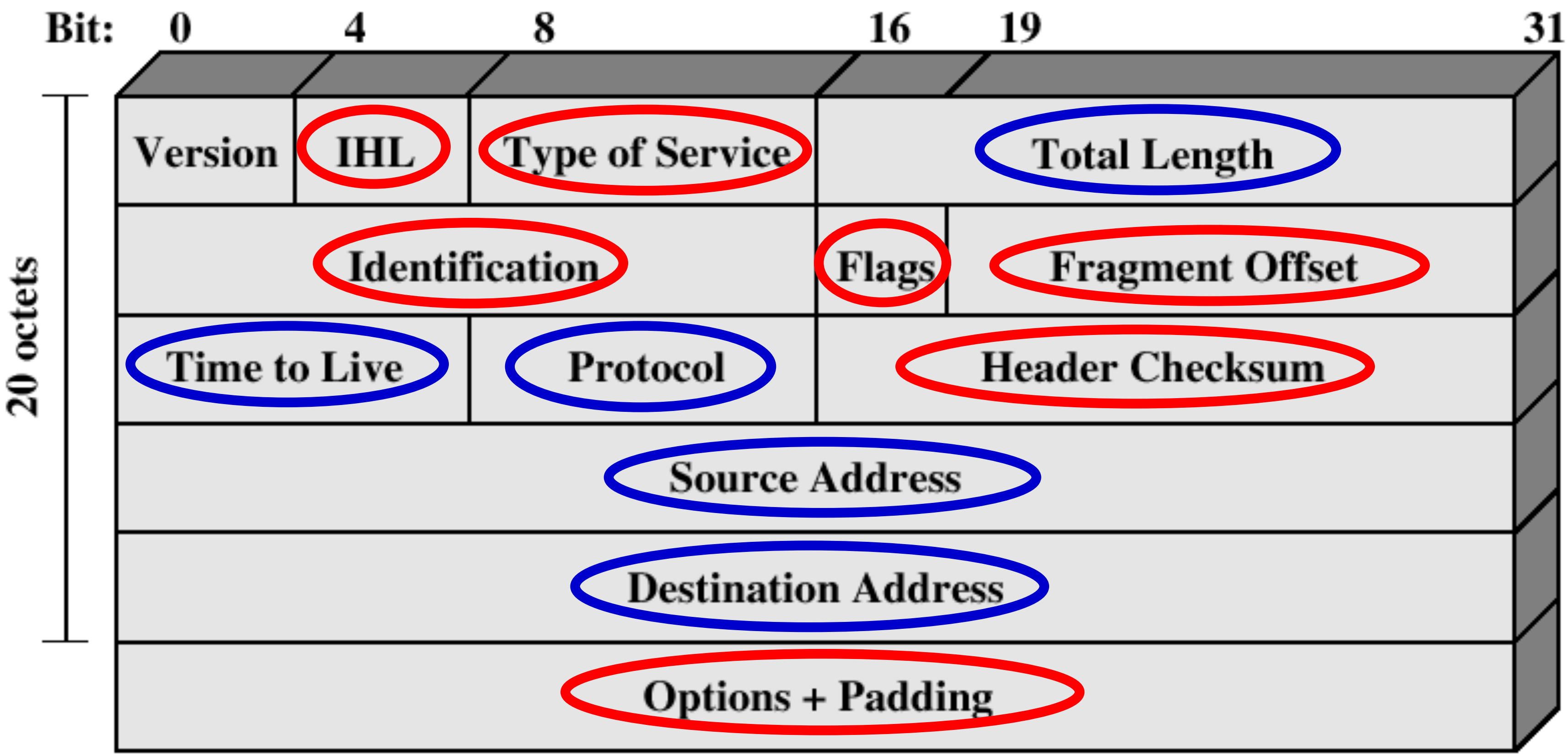
Legend

- **Field's Name Kept from IPv4 to IPv6**
- **Fields Not Kept in IPv6**
- **Name and Position Changed in IPv6**
- **New Field in IPv6**

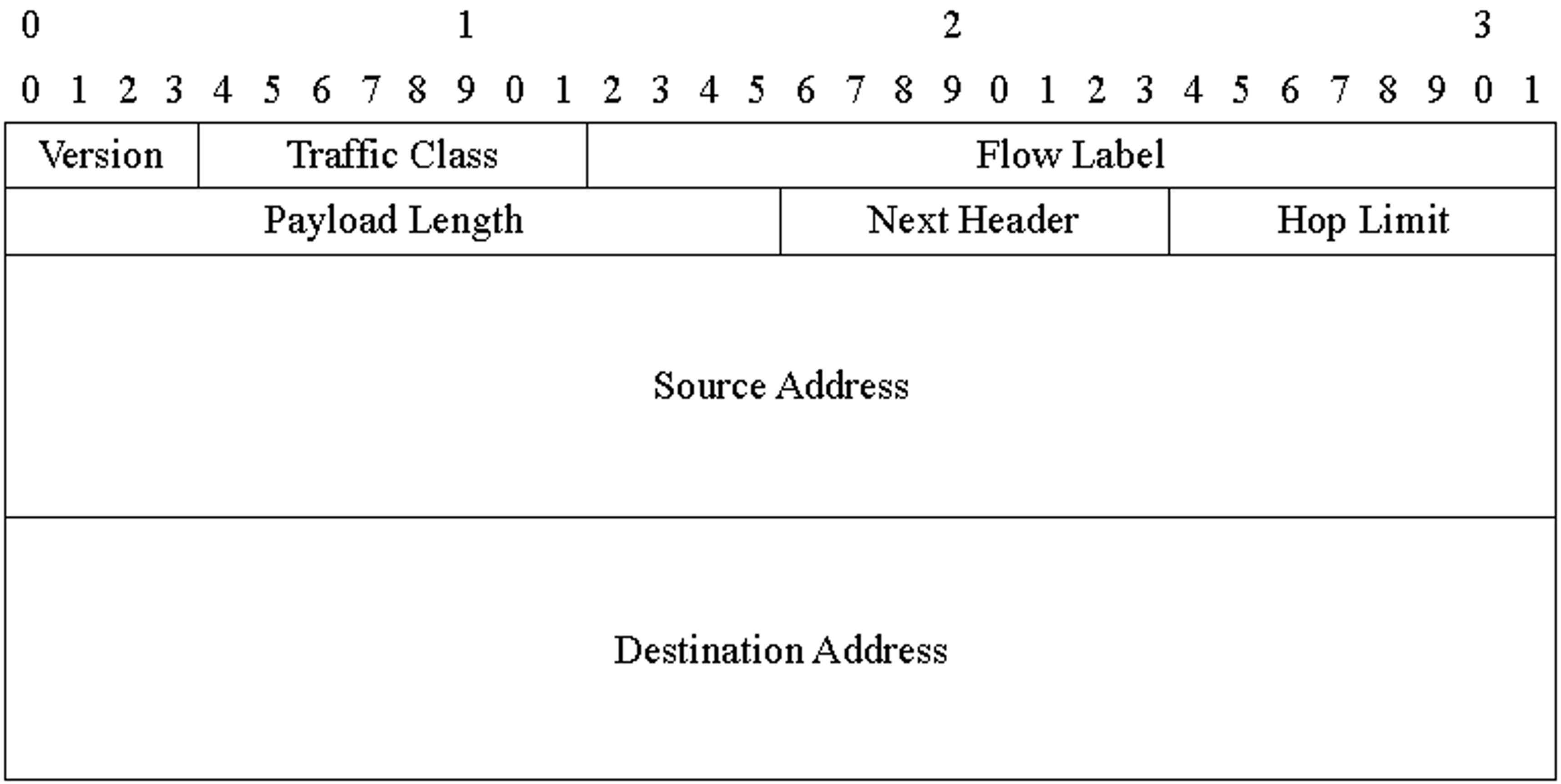
Header: from IPv4 to IPv6

Changed

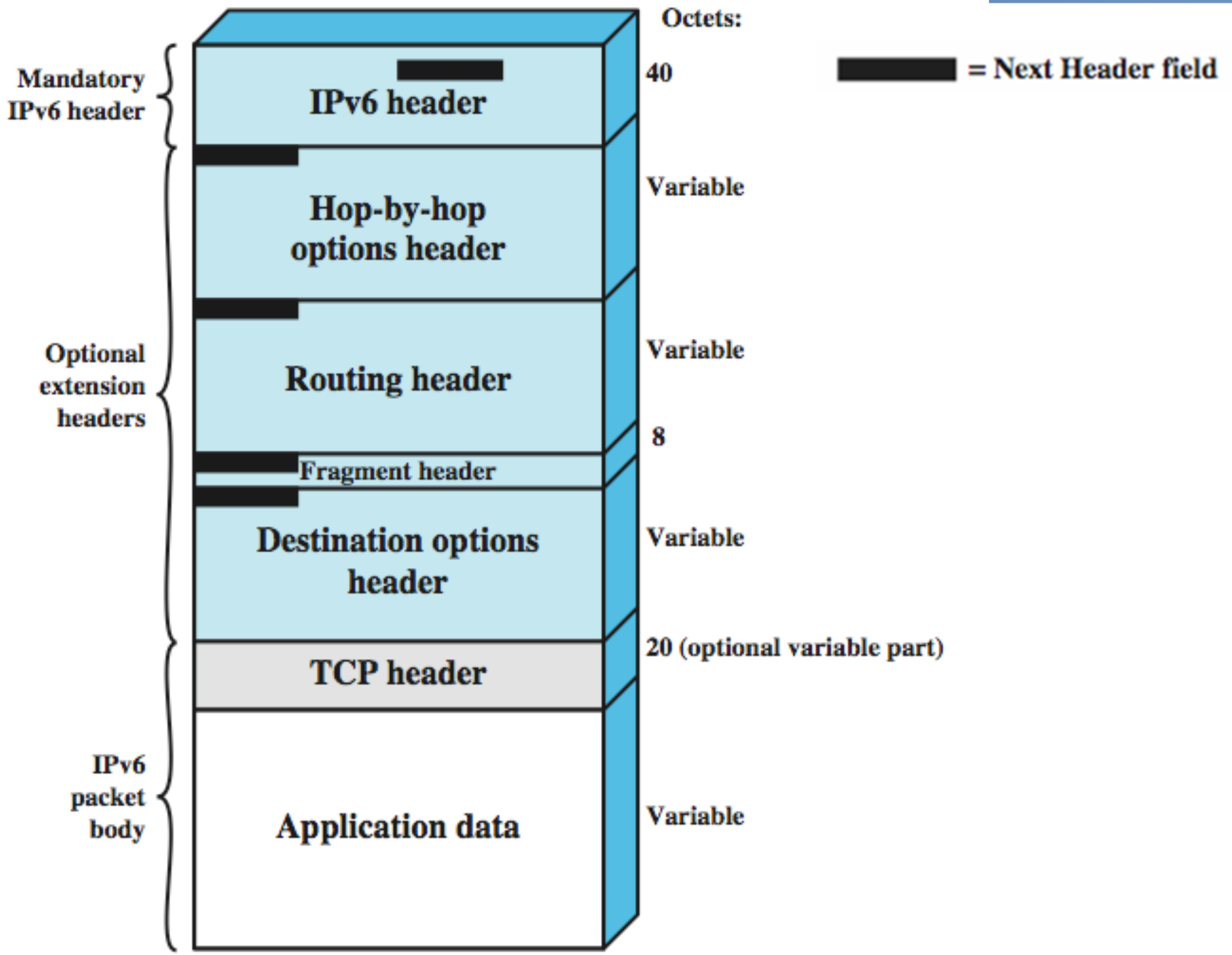
Removed



IPv6 Header Format



IPv6 Packet (PDU) Structure



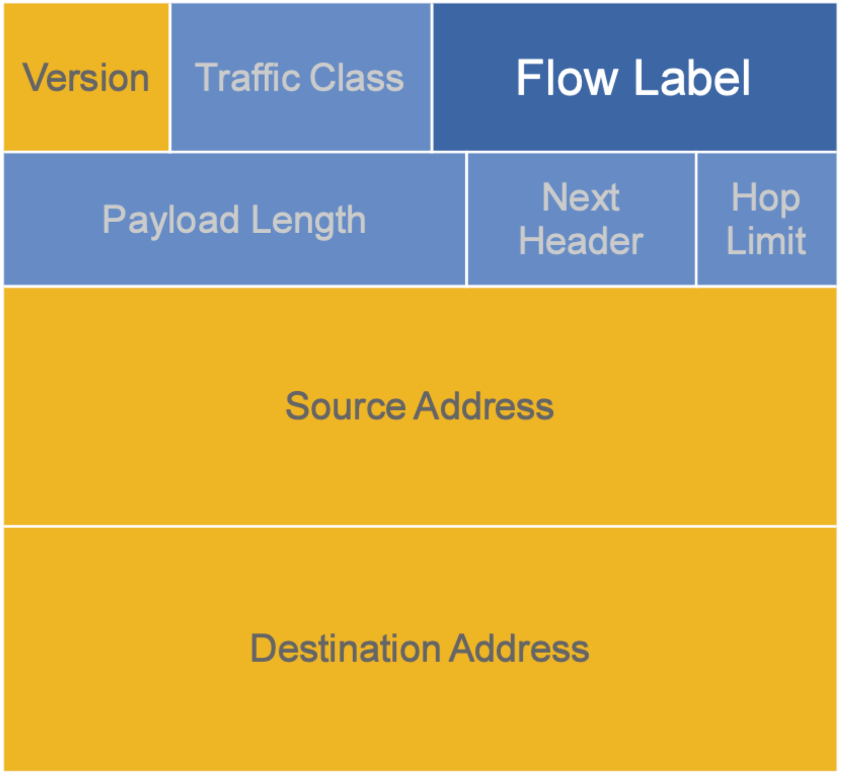
Traffic Class

- 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

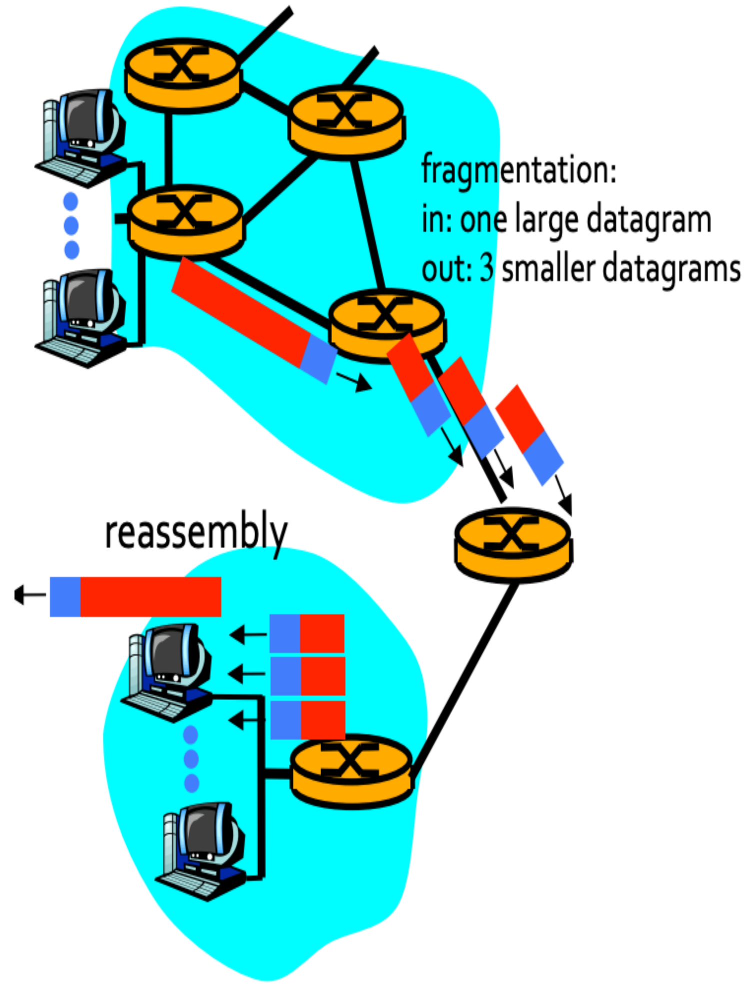
- 20-Bit Flow Label Field to Identify Specific Flows Needing Special QoS
  - Flow classifiers had been based on 5-tuple: Source/destination address, protocol type and port numbers of transport
  - With flow label, each source chooses its own flow label values; routers use source addr + flow label to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

IPv6 Header

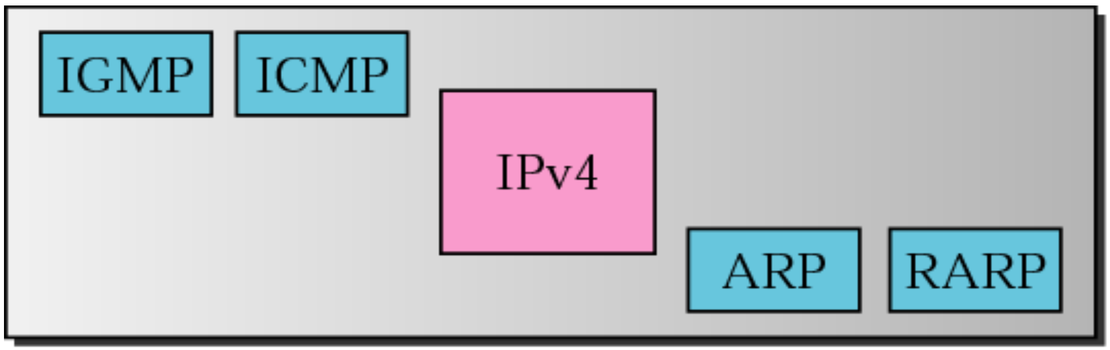


Path MTU Discovery

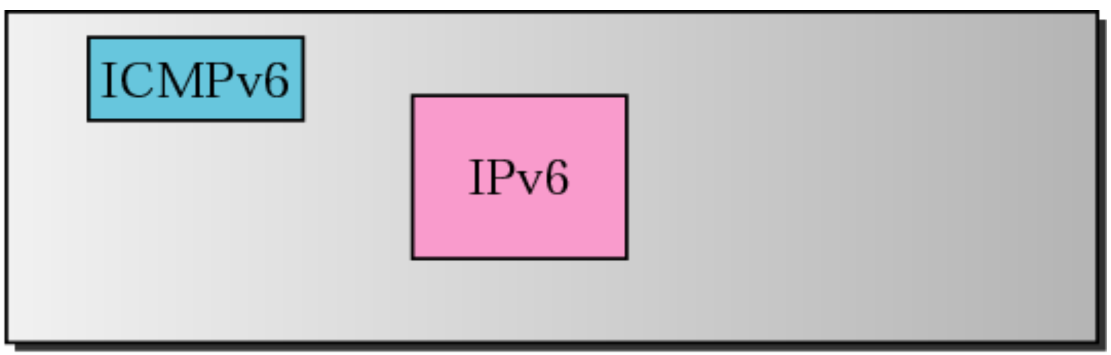
- Network links have MTU (maximum transmission unit) – the largest possible link-level frame
- As in IPv4, path MTU discovery in IPv6 allows a host to dynamically discover and adjust to differences in the MTU size of every link along a given data path.
- In IPv6, however, fragmentation is handled by 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

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

$$\frac{2^{128}}{6.5 \text{ Billion}}$$

= 52 Trillion Trillion IPv6 addresses per person

World's population is approximately 6.5 billion

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

= 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

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

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

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

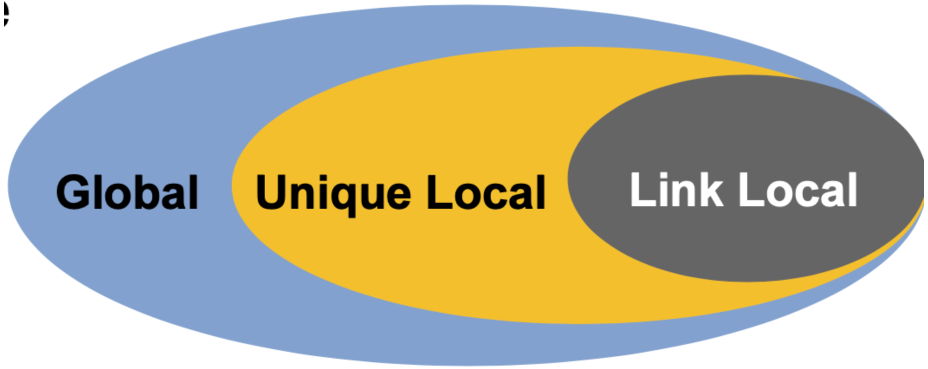
- Multicast
  - Address of a set of interfaces
  - Delivery to all interfaces in the set

- Anycast
  - Address of a set of interfaces
  - Delivery to a single interface in the set

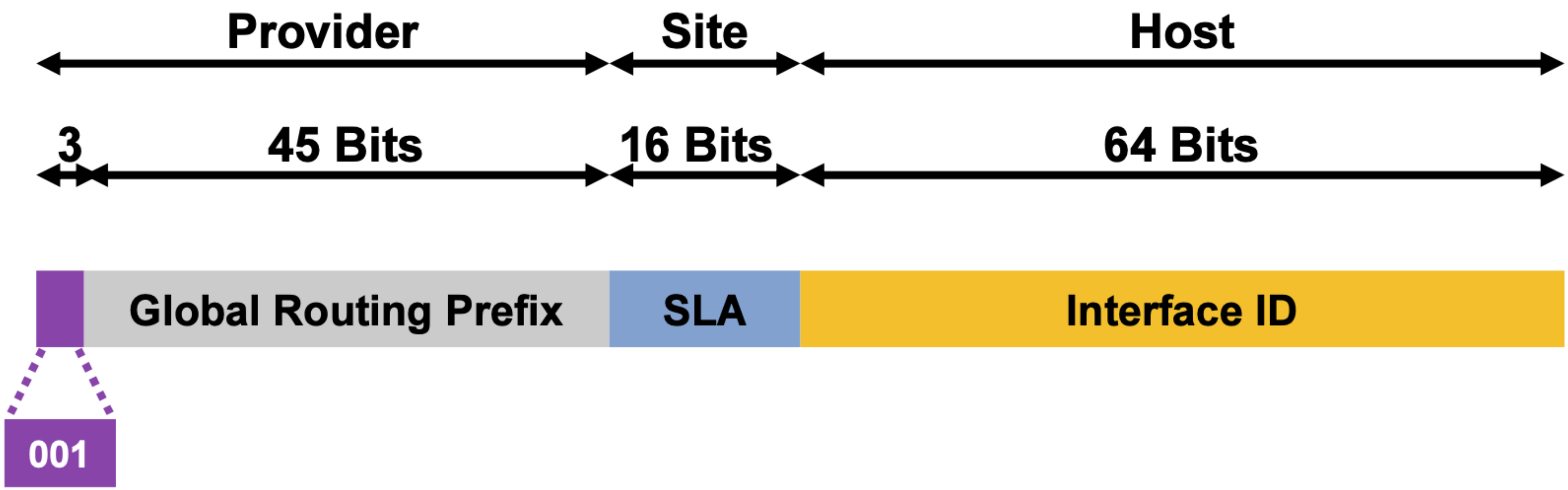
- No more broadcast addresses

IPv6 Addressing Model

- Addresses are assigned to interfaces, not hosts
- Interface expected to have multiple addresses
- Addresses have scope
  - Link-Local
  - Site-Local → Unique Local
  - Global



Global Unicast Address



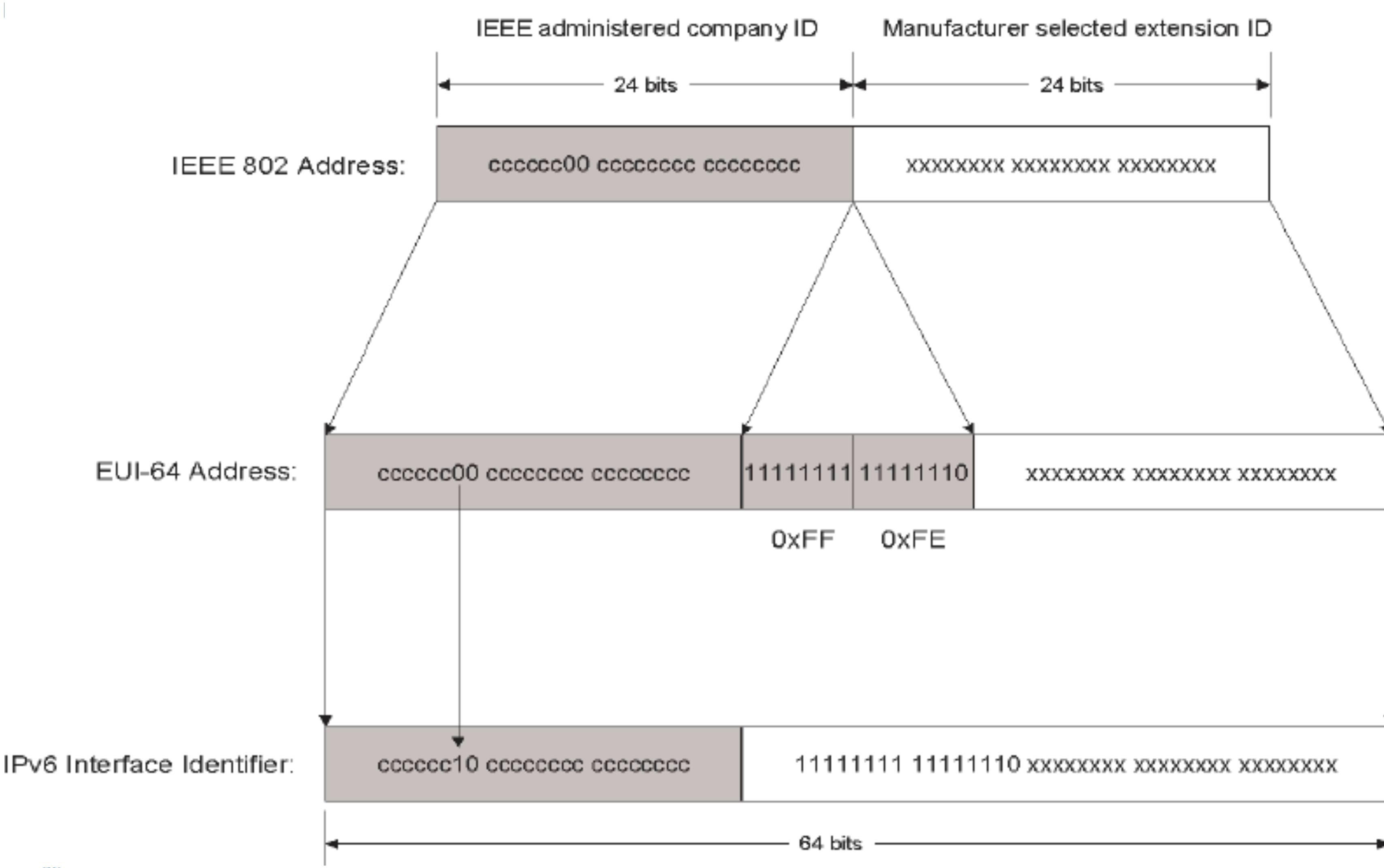
- Addresses for generic use of IPv6
- Interface ID is Constructed in Modified EUI-64 format

Interface Identifier

may be assigned in several different ways:

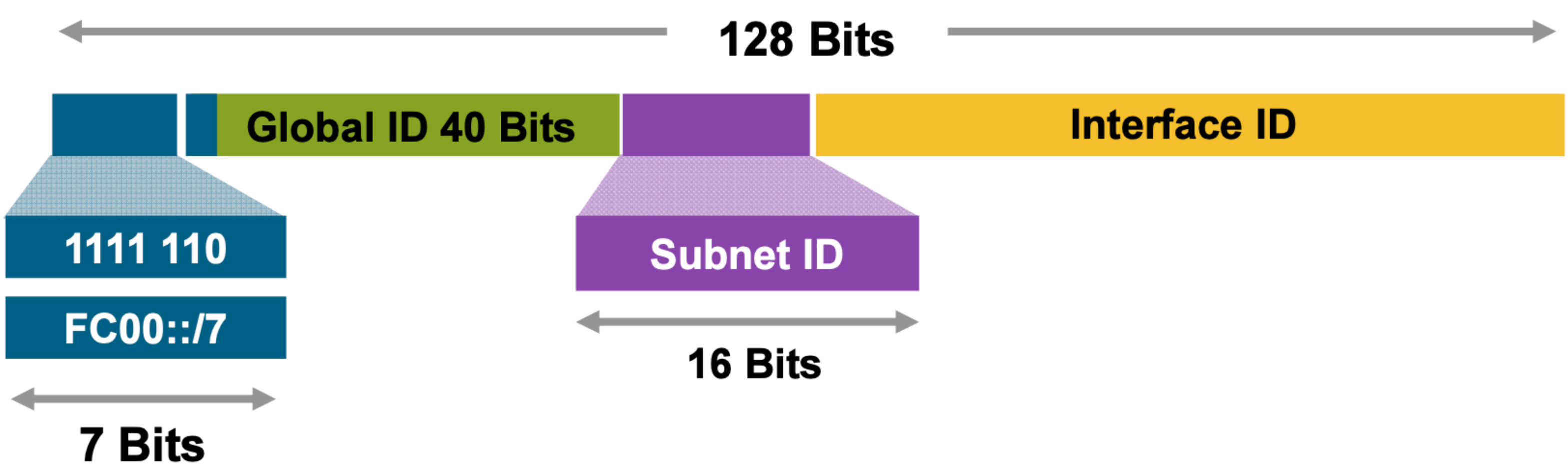
- auto-configured from a 64-bit EUI-64, or expanded from a 48-bit MAC address (e.g., Ethernet address)
- auto-generated pseudo-random number (to address privacy concerns)
- assigned via DHCP
- manually configured
- possibly other methods in the future

IEEE 802 → IPv6 Interface ID



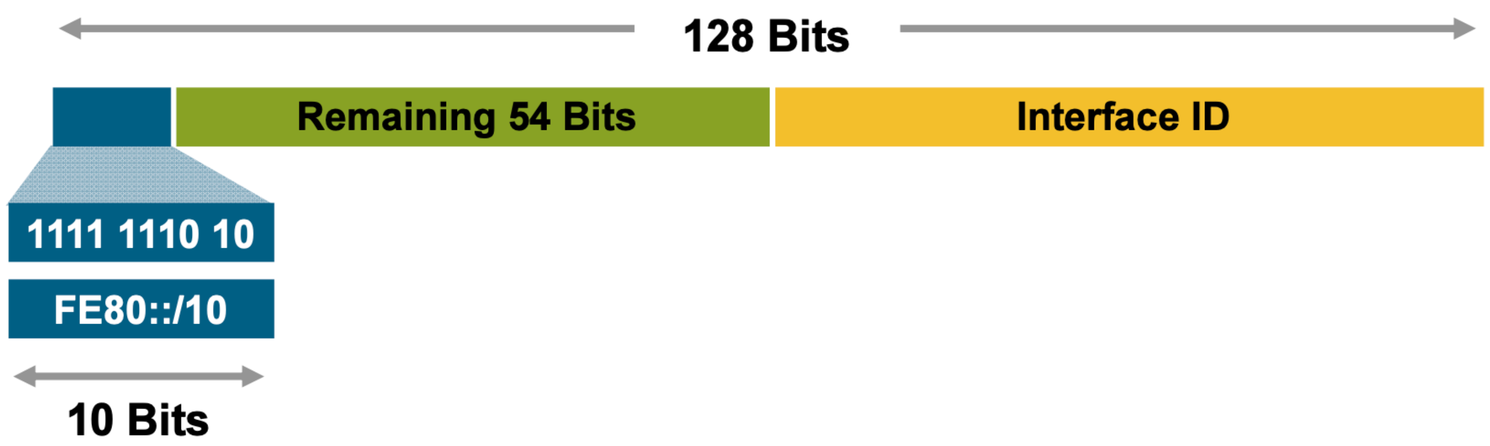
Unique Local Address

- Meaningful only in a single site zone, and may be re-used in other sites
- Equivalent to the IPv4 private address
- Prefix= FC00::/7



Link Local Address

- **Link-Local Addresses Used for:**
  - Mandatory Address for Communication between two IPv6 devices (like ARP but at Layer 3)
  - Automatically assigned by Router as soon as IPv6 is enabled
  - Also used for Next-Hop calculation in Routing Protocols
  - Only Link Specific scope
  - 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)
  - Identify a loopback interface
- ❑ IPv4-compatible address (0:0:0:0:0:0:w.c.x.z or ::w.c.x.z)
  - Used by dual-stack nodes
  - IPv6 traffic is automatically encapsulated with an IPv4 header and send to the destination using the IPv4 infrastructure
- ❑ IPv4 mapped address (0:0:0:0:0:FFFF:w.c.x.z or ::FFFF:w.c.x.z)
  - Represent an IPv4-only node to an IPv6 node
  - Only use a single listening socket to handle connections from client via both IPv6 and IPv4 protocols.
  - Never used as a source or destination address of IPv6 packet
  - Rarely implemented

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

Some Well Known Multicast Addresses

Address	Scope	Meaning
FF01::1	Node-Local	All Nodes
FF02::1	Link-Local	All Nodes
FF01::2	Node-Local	All Routers
FF02::2	Link-Local	All Routers
FF05::2	Site-Local	All Routers
FF02::1:FFXX:XXXX	Link-Local	Solicited-Node

Address Autoconfiguration

- Allow plug and play
- BOOTP and DHCP are used in IPv4
- DHCPng will be used with IPv6
- Two Methods: Stateless and Stateful
- Stateless:
  - A system uses link-local address as source and multicasts to "All routers on this link"
  - Router replies and provides all the needed prefix info
  - All prefixes have a associated lifetime
  - System can use link-local address permanently if no router

Address Autoconfiguration

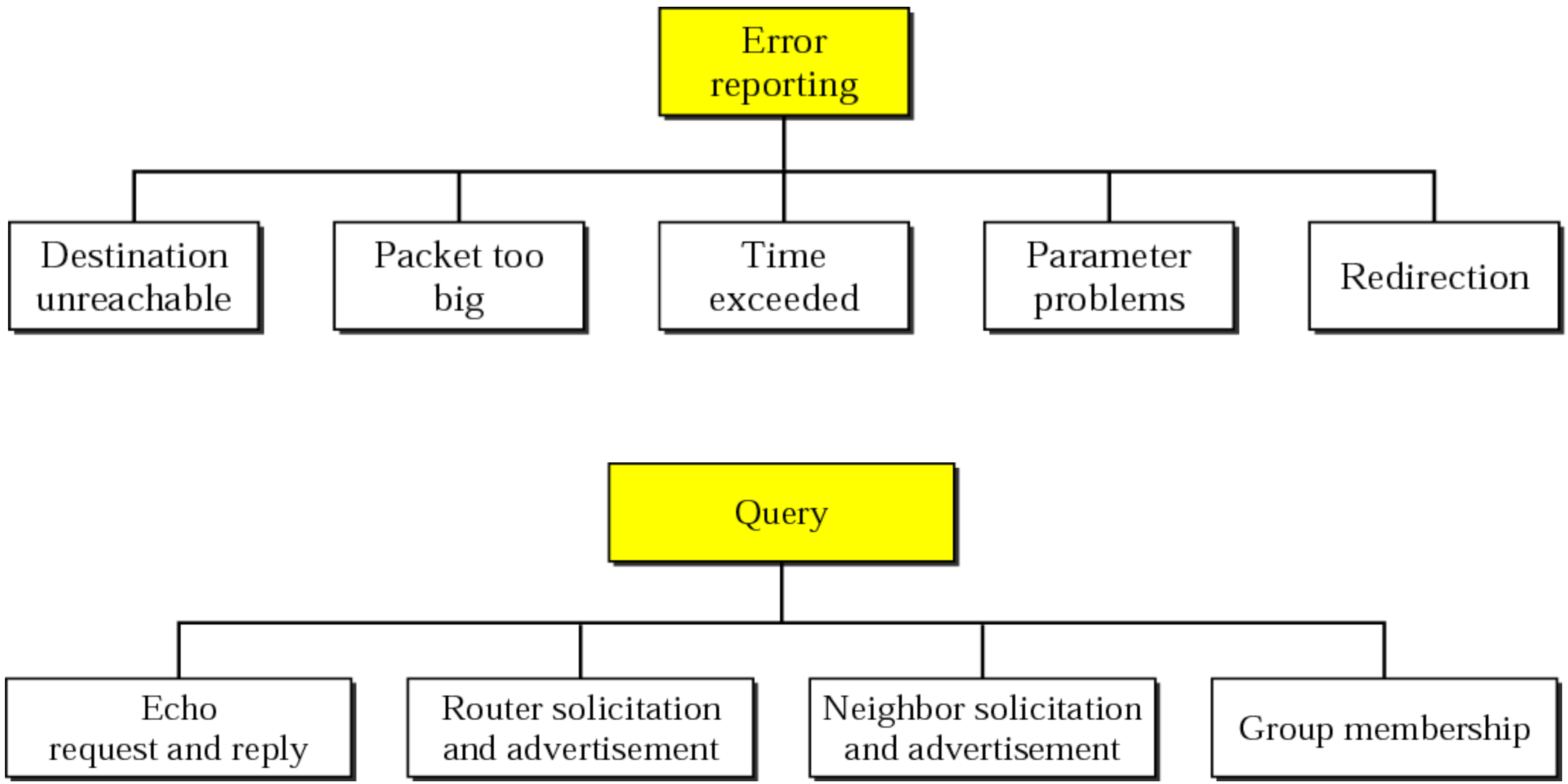
- Stateful:
  - Problem w/ stateless: Anyone can connect
  - Routers ask the new system to go DHCP server (by setting managed configuration bit)
  - System multicasts to "All DHCP servers"
  - DHCP server assigns an address

ICMPv6 and Neighbor Discovery

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 and quick purge cached valued that become invalid
- Hosts also use ND to find neighboring router that willing to forward packets on their behalf
- Five neighbor discovery messages
  1. Router solicitation (ICMPv6 type133)
  2. Router advertisement (ICMPv6 type134)
  3. Neighbor solicitation (ICMPv6 type135)
  4. Neighbor advertisement (ICMPv6 type136)
  5. Redirect (ICMPV6 type137)

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

Neighbor Solicitation and Advertisement

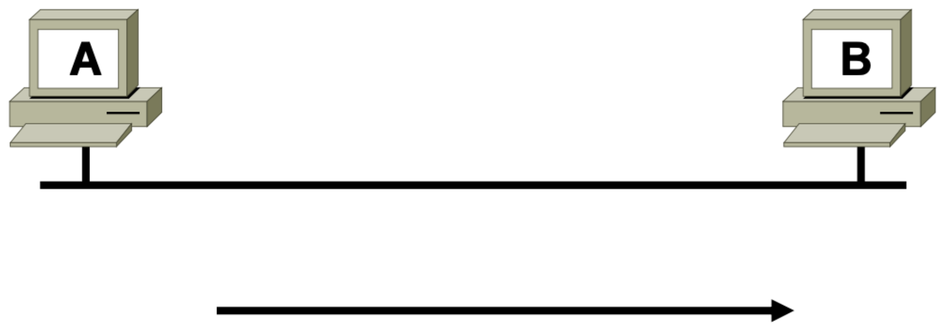
Neighbor Solicitation
ICMP type = 135

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

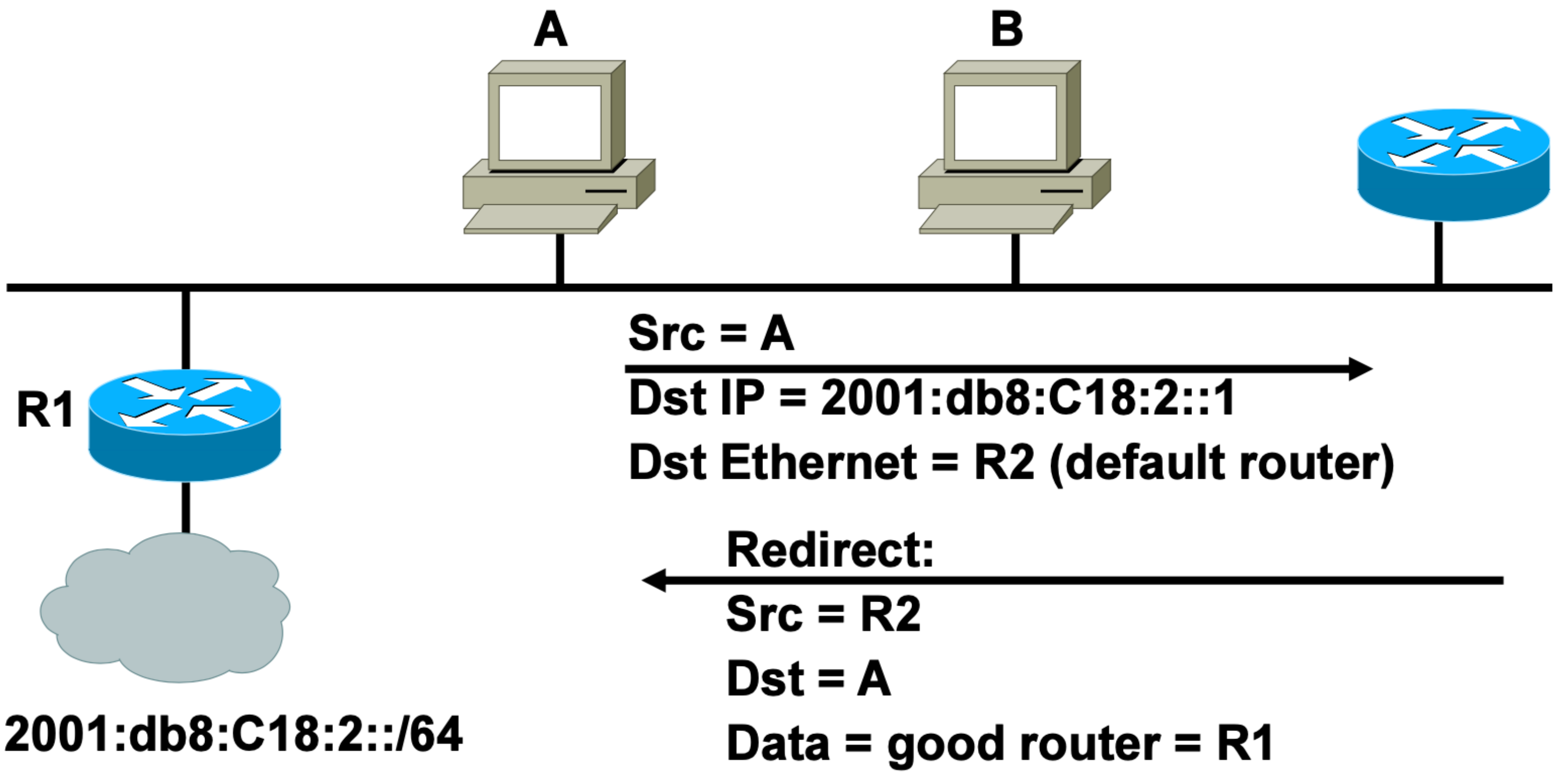
Duplicate Address Detection




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

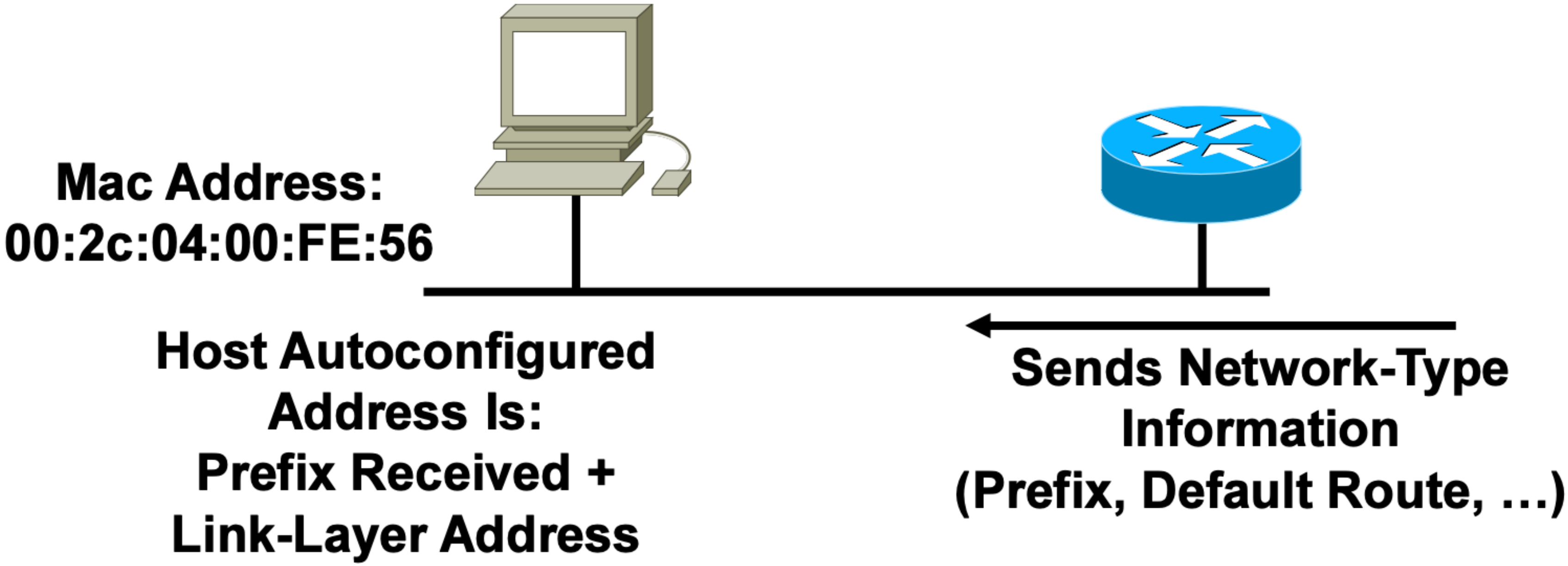
Duplicate Address Detection (DAD) uses neighbor solicitation to verify the existence of an address to be configured

Redirect



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

Address Autoconfiguration

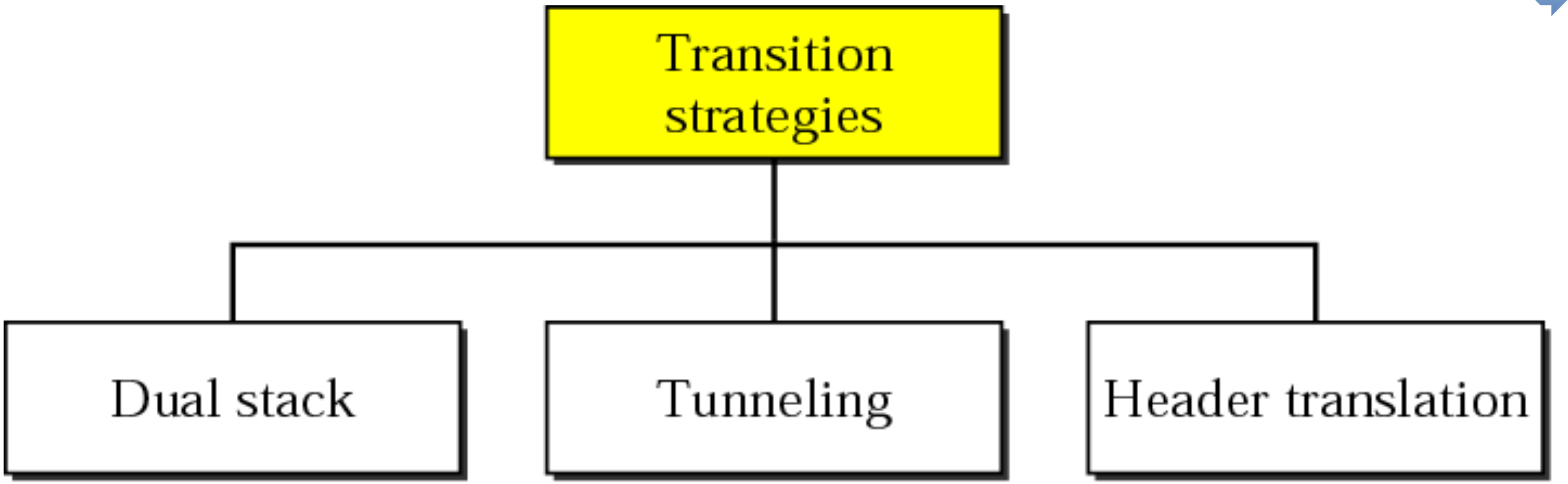


Routing in IPv6

- 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)

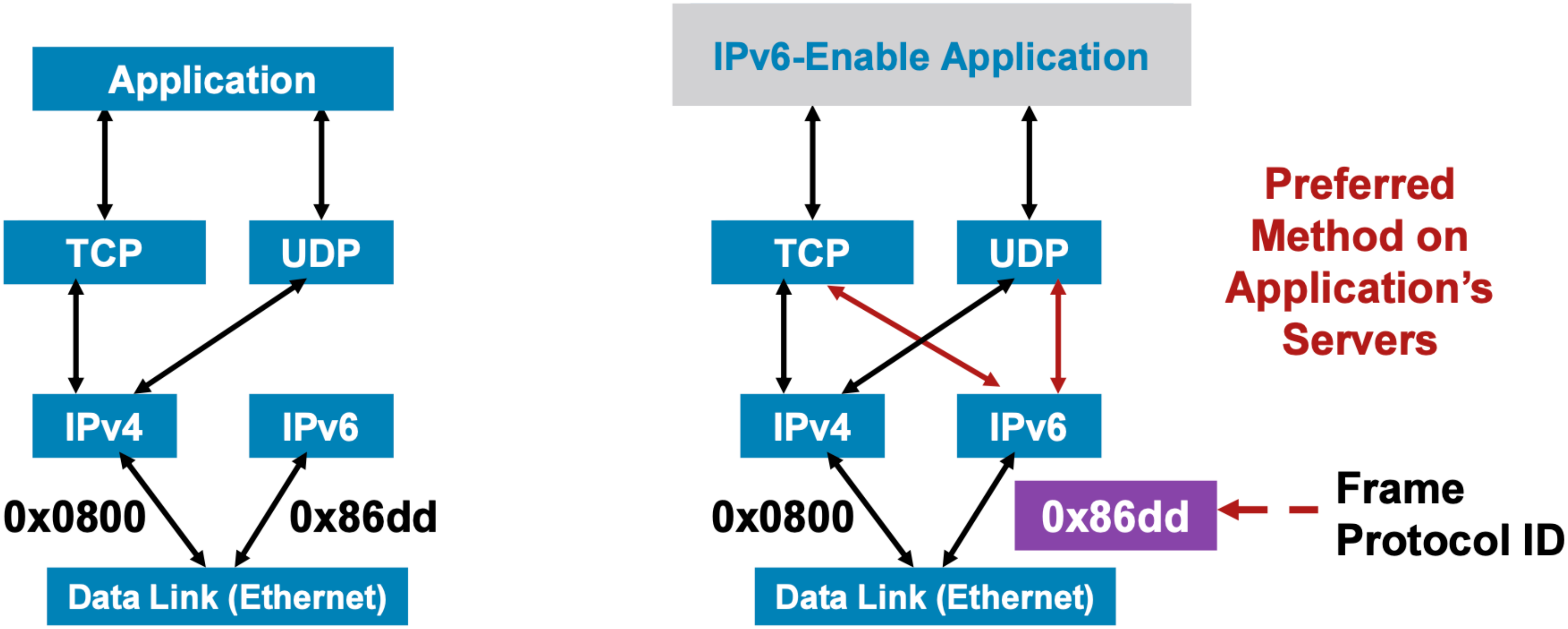
ICMPv6 Deployment

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

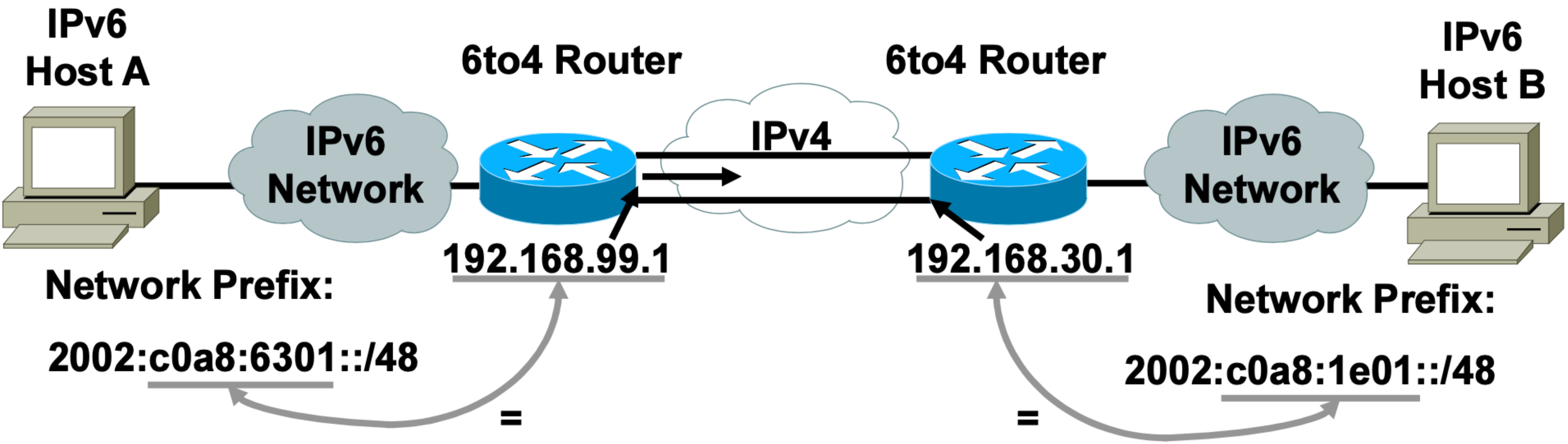


- Both IPv4 and IPv6 stacks enabled
- Applications can talk to both
- Choice of the IP version is based on name lookup and application preference

Tunneling

- Many Ways to Do Tunneling
  - Some ideas same as before GRE, MPLS, IP
  - Native IP over data link layers
    ATM PVC, dWDM Lambda, Frame Relay PVC, Serial,
  - Sonet/SDH, Ethernet
  - Some new techniques
    Automatic tunnels using IPv4 , compatible IPv6 address, 6to4, ISATAP

Automatic 6to4 Tunnel (RFC 3056)



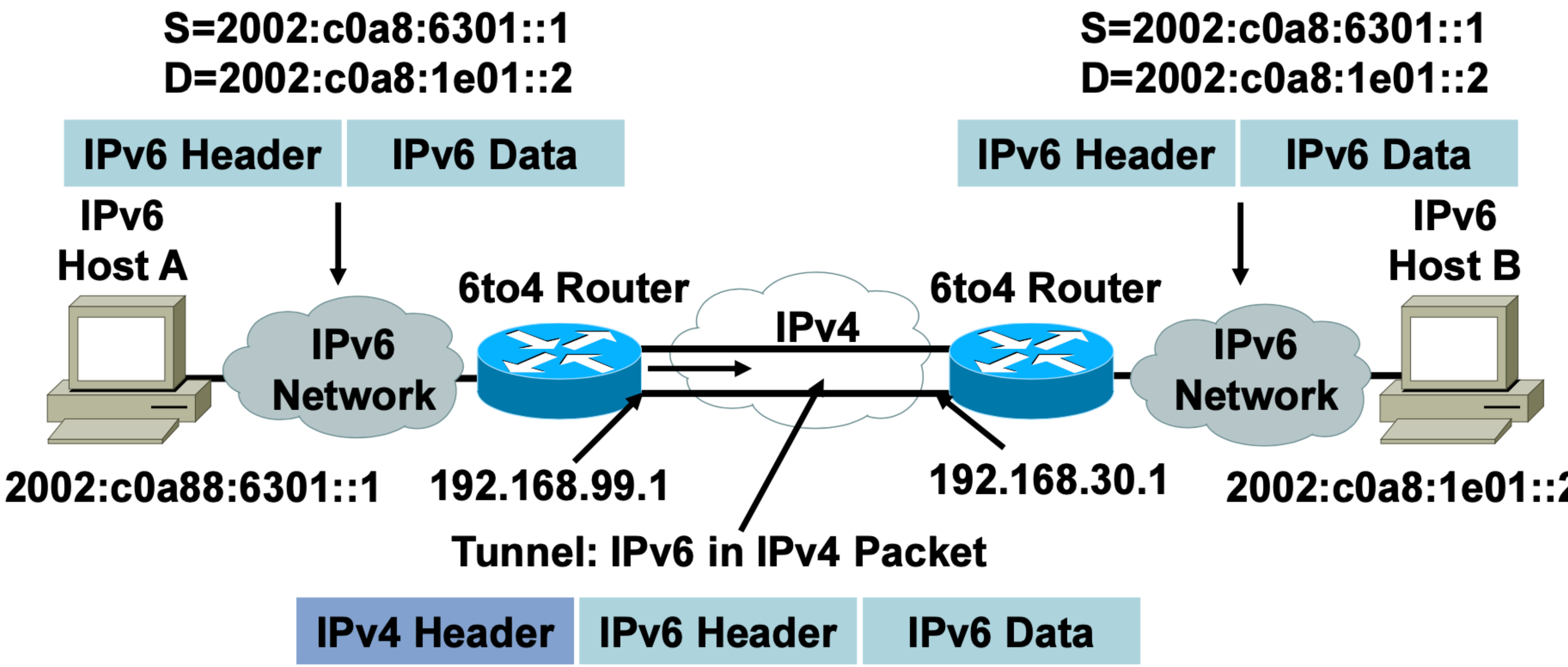
6to4:

- Is an automatic tunnel method
- Gives a prefix to the attached IPv6 network

2002	Public IPv4 Address	SLA	Interface ID

/16 /48 /64

Automatic 6to4 Tunnel (RFC 3056)



S(v4)=192.168.99.1
D(v4)=192.168.30.1
S(v6)=2002:c0a8:6301::1
D(v6)=2002:c0a8:1e01::2

Hỏi & Đáp