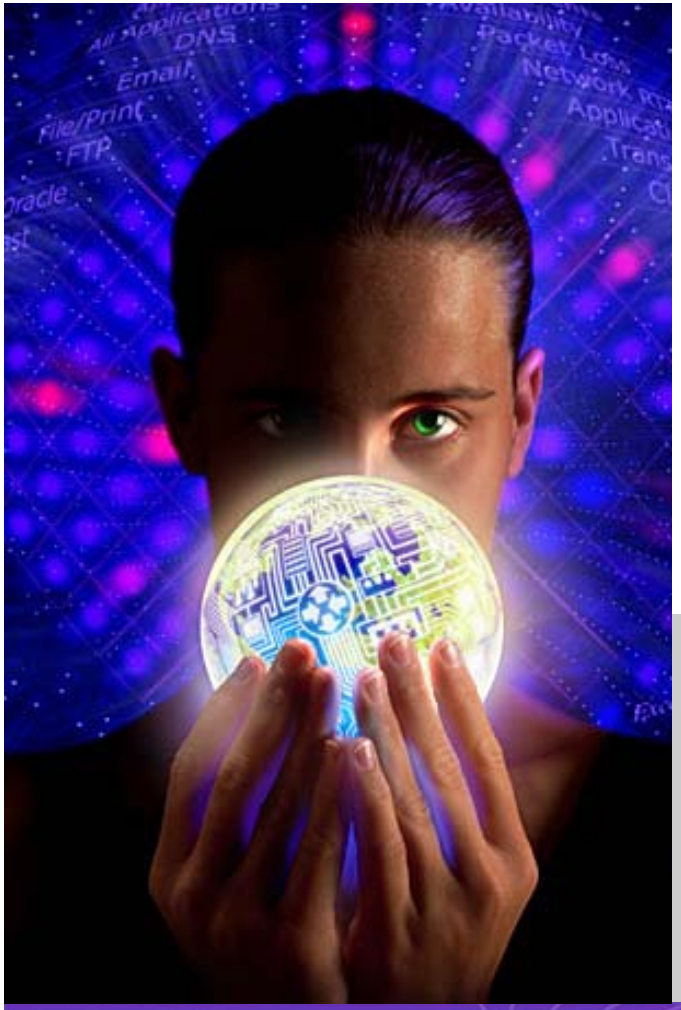
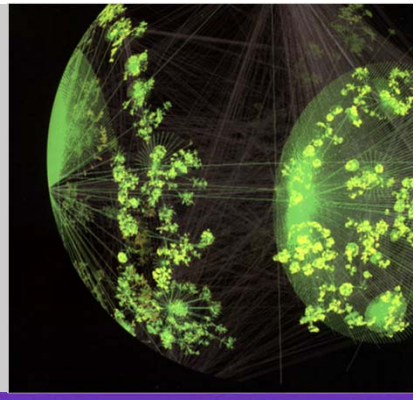


IPv6

TCP/IP Essentials

EL5373 Supplement Topic



Spring 2017

IPv6 Background

- In the early 1990s, the IETF realized that IPv4 address space was near exhaustion
  - Host density ratio (H) analysis for address assignment efficiency: RFC1715

$$H = \frac{\log(\text{number of objects})}{\text{available bits}}$$

  - Began work on the next generation of IP: IPv6
  - Incorporated many of the experiences learned from IPv4
- In addition to larger address space, IPv6 provides many enhanced capabilities
- Internet operators' approach
  - Assign private v4 address to growing IP endpoints with deployment of SP-NAT
  - Use public addresses – migrate to v6 or stay with v4 if enough address space

IPv4 Address Preservation

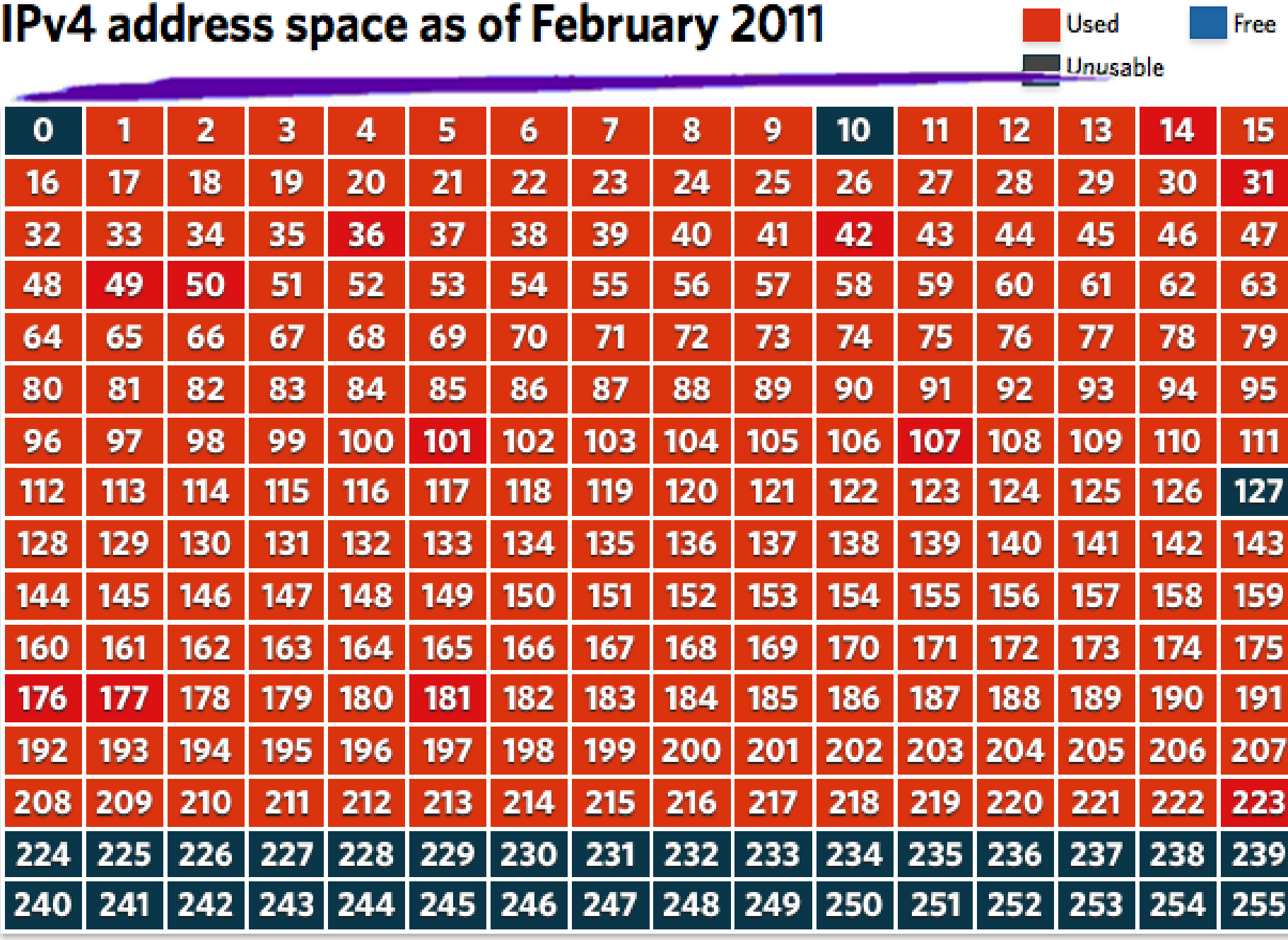
When IP v6 was being developed, there was an on-going effort to preserve IP v4 address

- CIDR (Classless Inter-domain Routing)
- DHCP (Dynamic Host Configuration Protocol)
- Allocation for private address (RFC 1918)
- NAT (Network Address Translation)
- Various tunneling technologies (MPLS, GRE)

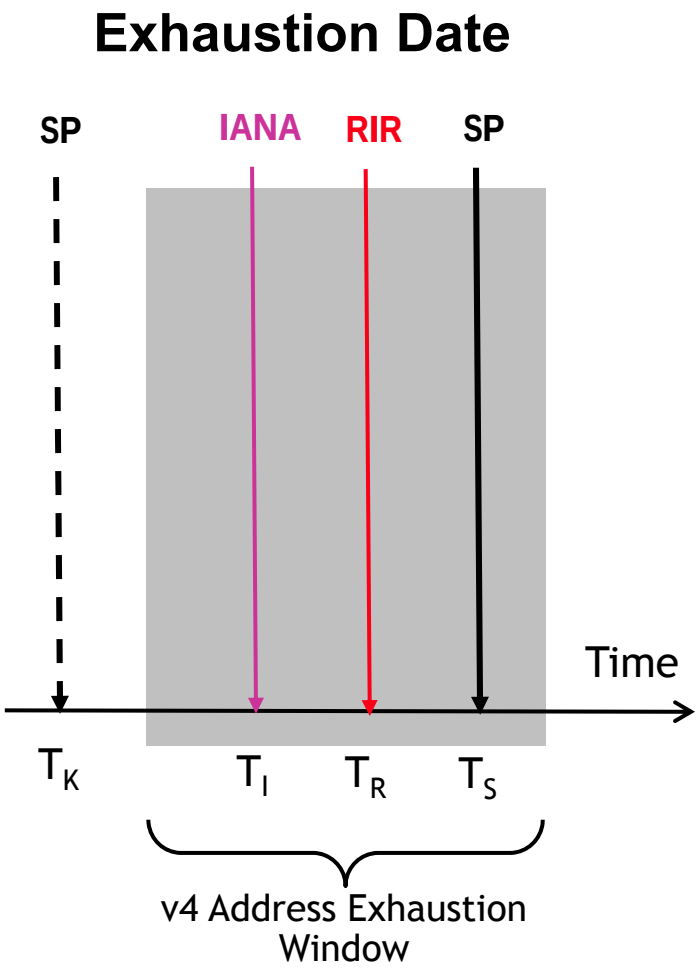
Very Successful in prolonging the life span of IPv4; however

- These interim techniques all have some drawbacks
- Experts feel that v6 deployment will reach the critical mass soon

IPv4 address space as of February 2011



v4 Address Exhaustion – A Closer Look



T_I: IANA v4 address /8 pool exhausted on 2/3/2011

T_R: RIR v4 address pool exhausted

- April15, 2011 is marked as the date, APNIC first run out of freely allocated v4 address

T_S: SP address pool exhausted/constrained

T_K: operators "kicks off" v6 migration

- T_S may be earlier or later than T_I/T_R, depending on operator's possession of v4 addresses
- T_K may be earlier or later than T_S
  - Earlier – operator starts migrating to v6 before v4 address exhaustion occurs
  - Later – operator starts with v4 private address first, then migrates to v6

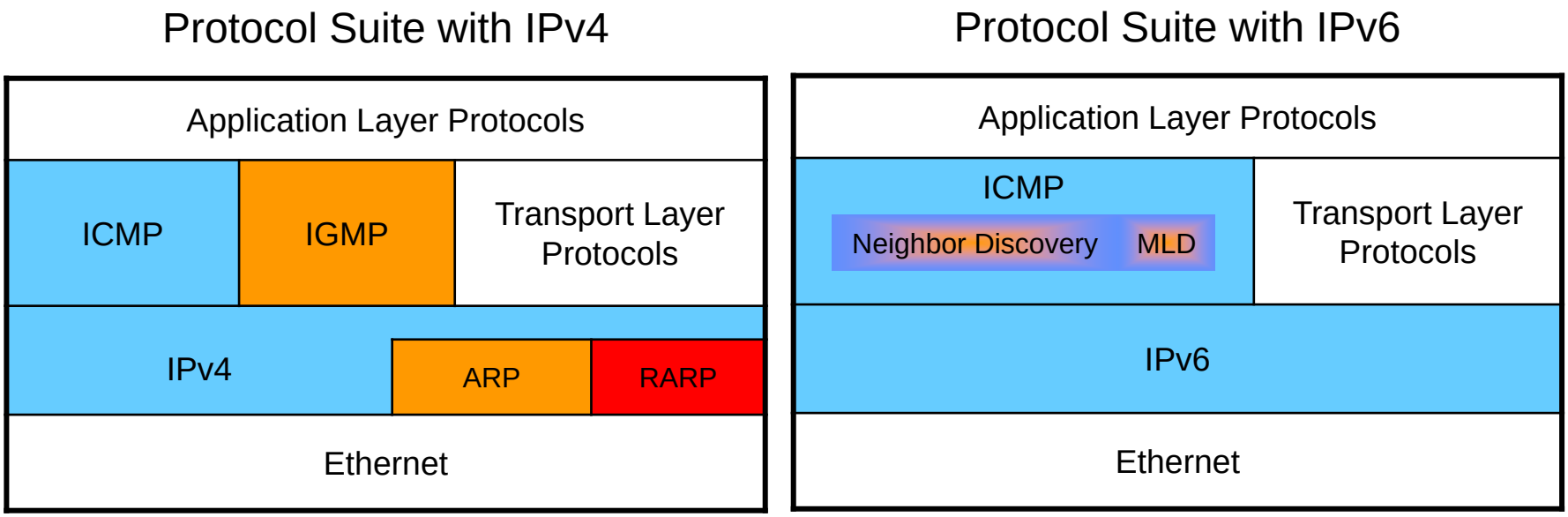
What's New with IPv6?

- Huge address space, 128 bit addresses, with expanded addressing capabilities
- Structured hierarchical address space to manage routing table growth
- Serverless auto-configuration and re-configuration: stateless (without DHCPv6) and stateful (with DHCPv6) address config.
- Streamlined header format and flow identification: less fields, better mobile IP support
- Improved neighbor discovery: e.g. ICMPv6 replaces ARP
- ICMPv6 – Multicast Listener Discovery (MLD) replaces IGMP
- Built-in security: support for authentication & payload encryption
- QoS support (?): traffic class, flow labeling, …

Key IPv6 Terminology

Node	a protocol module that implements IPv6
Router	a node that forwards IPv6 packets not explicitly addressed to itself
Host	any node that is not a router
Link	a communication facility or medium over which nodes can communicate at the link layer, i.e., the layer immediately below IPv6
Neighbors	nodes attached to the same link
Interface	a node's attachment to a link
Address	an IPv6-layer identifier for an interface or a set of interfaces

IPv6 Impact to TCP/IP Protocol Suite



Protocol enhanced

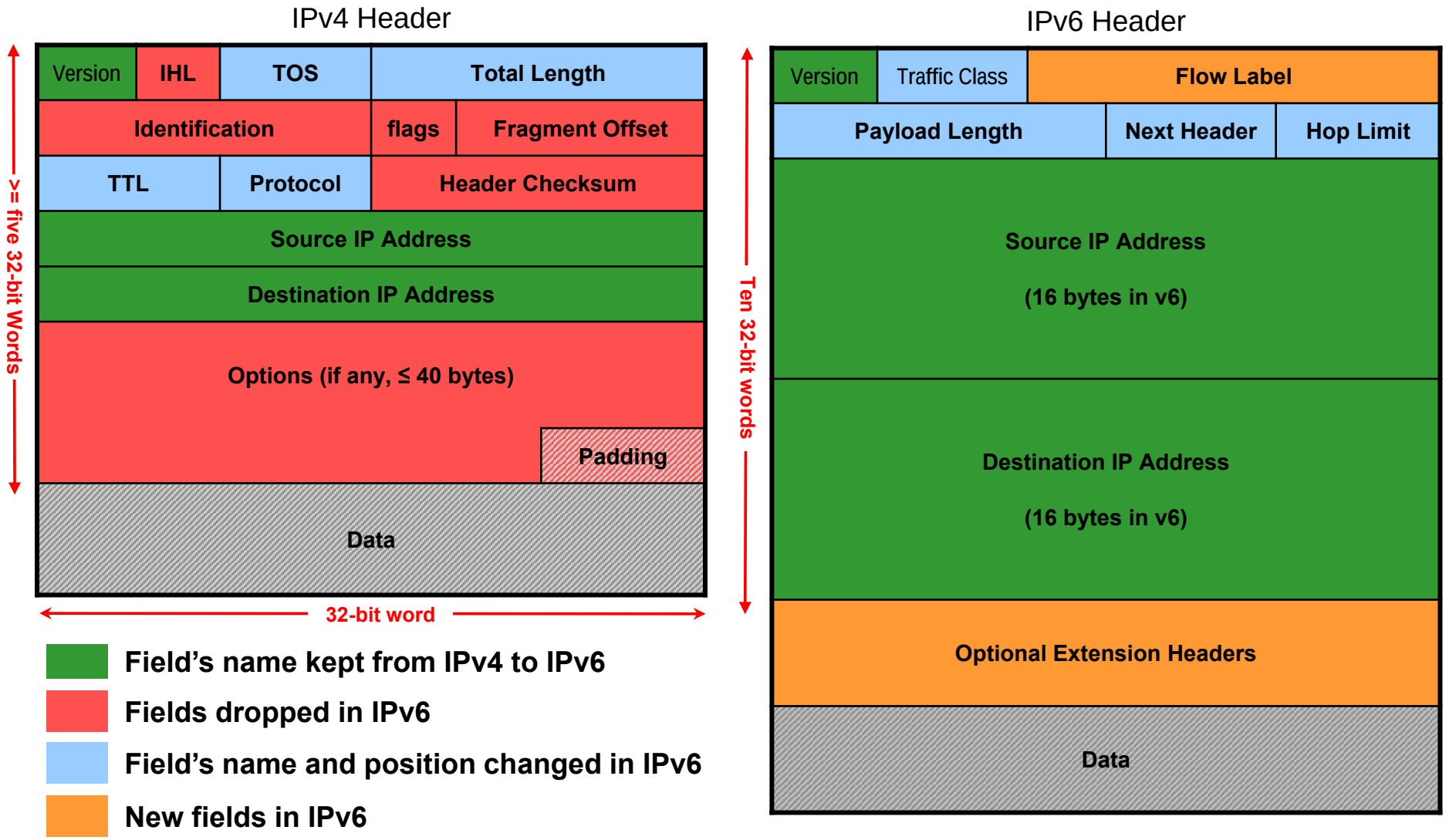
Protocol replaced

Protocol dropped

ND: Neighbor Discovery

MLD: Multicast Listener Discovery

IPv4 & IPv6 Header Comparison



Fields of the IPv6 Header

- Version: Version 6
- Traffic Class: Internet traffic priority delivery value
- Flow Label: Used for specifying special router handling from source to destination(s) for a sequence of packets
- Payload Length:
  - Number of bytes of optional extension headers and data packets from the upper layer, other than the fixed 40 bytes IPv6 header
  - When cleared to zero, the option is a hop-by-hop Jumbo payload
- Next Header: Specifies the next encapsulated protocol, compatible with those specified for the IPv4 protocol field
- Hop Limit: Renamed the TTL field in IPv4 that was originally intended to be used as a time based hop limit

Summary of Header Changes between IPv4 & IPv6

Streamlined

- Fragmentation fields moved out of base header
- IP options moved out of base header
- Header Checksum eliminated
- Header Length field eliminated
- Length field excludes IPv6 header
- Alignment changed from 32 to 64 bits

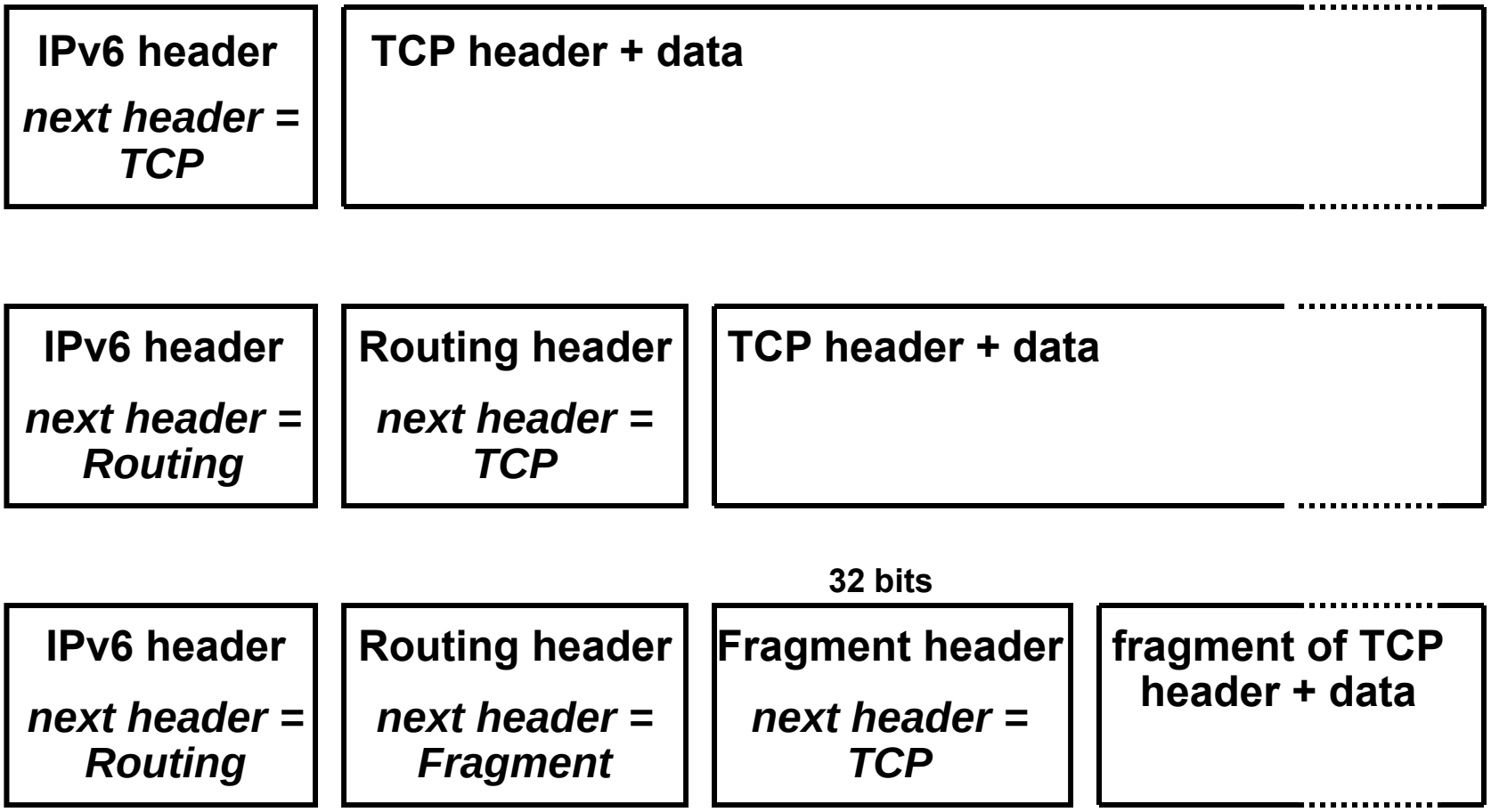
Revised

- Time to Live → Hop Limit
- Protocol → Next Header
- Precedence & TOS → Traffic Class
- Addresses increased 32 bits → 128 bits

Extended

- Flow Label field added

Extension Header Examples

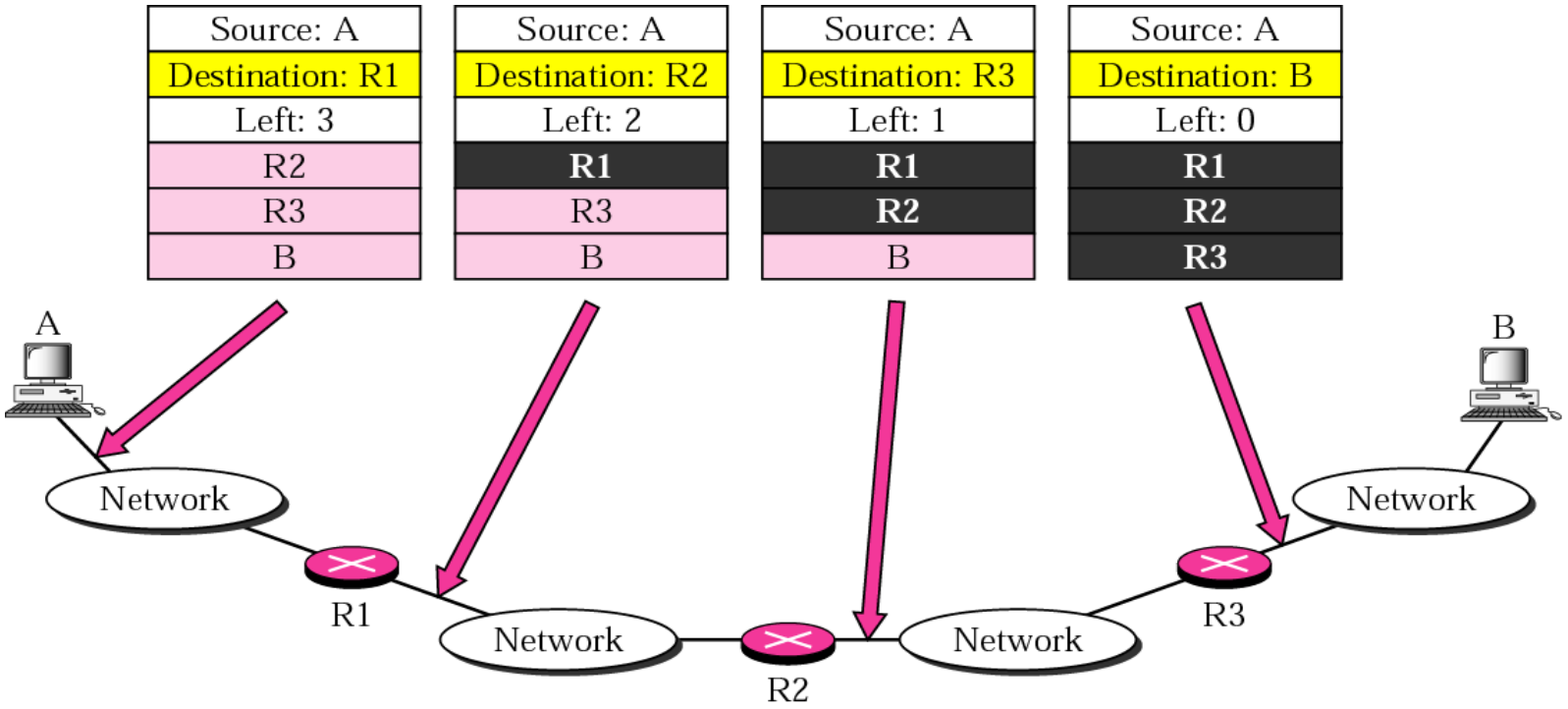


Extension Header Types – defined by the value in Next Header

Order	Header Type	Description	Next Header Code
1	Basic IPv6 Header		
2	Hop-by-Hop Options	Special options that require hop-by-hop processing	0
4	Routing header	Source routing	43
5	Fragment header	Supports fragmentation of IPv6 datagrams at source	44
6	Authentication header	Integrity and authentication	51
7	Encapsulation Security Payload header	Confidentiality w/ encrypted data	50
8	Destination Options	Optional information to be examined by the destination node	60
9	Mobility header	Signaling information of the Mobile IPv6 protocol	135
	No Next header (Null)	No header after the current one	59
	Upper layer: TCP, UDP, ICMP, OSPF		6, 17, 58, 89

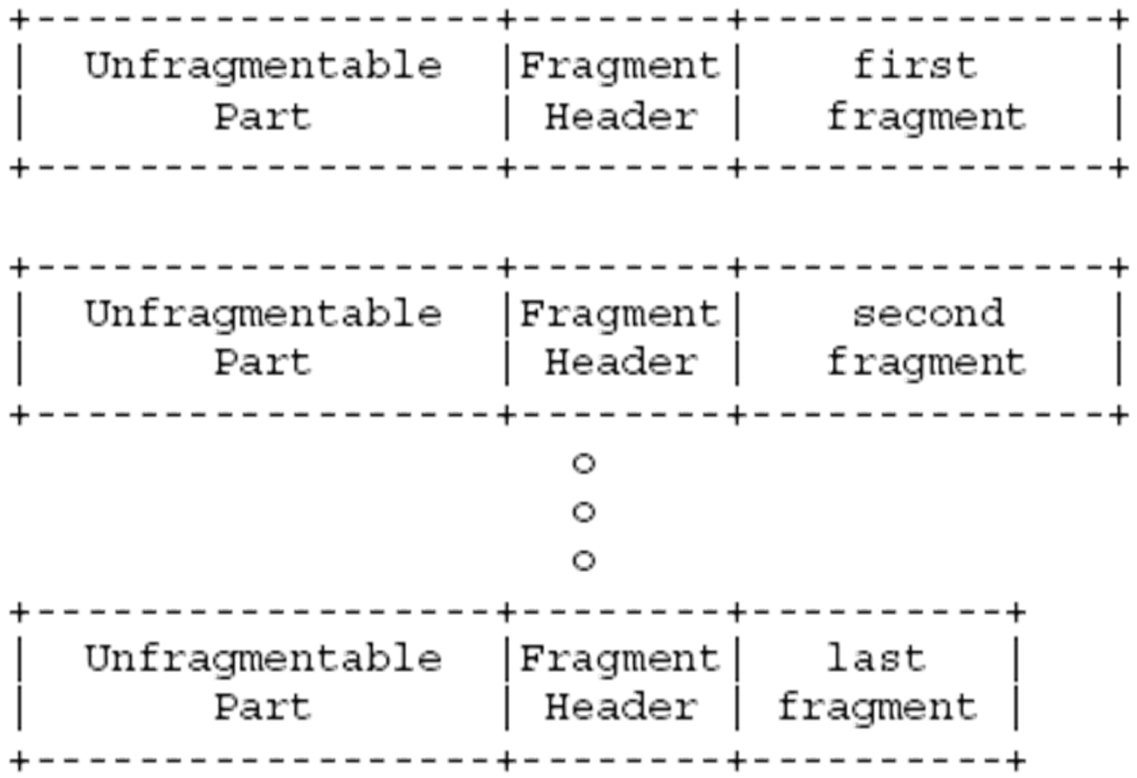
Routing Header
– Source Routing Example

- Routing header type 0 specifies Source Routing
  - List of one or more intermediate nodes to visit
  - Provide a simple but effective to alunch DoS attack, thus is deprecated
- Type 2 defines a limited version of type 0 and is used for Mobile IPv6



Fragment Header

- Used by source to send packets to accommodate path MTU
- Unfragmentable part: IPv6 header + any extension headers that must be processed by nodes en route
- Fragment Offset, Identification, MF fields are kept
- The offset of the data following this header, in 8-byte units, relative to the start of Fragmentable Part of the original packet



IPv6 Address

- Uses 128 bits to support at least one billion networks
- Addresses are assigned to interfaces - no change from IPv4 Model
- Interface is ‘expected’ to have multiple addresses
- Address scope: Link Local, Site Local, Global
- Addresses have preferred and valid lifetime

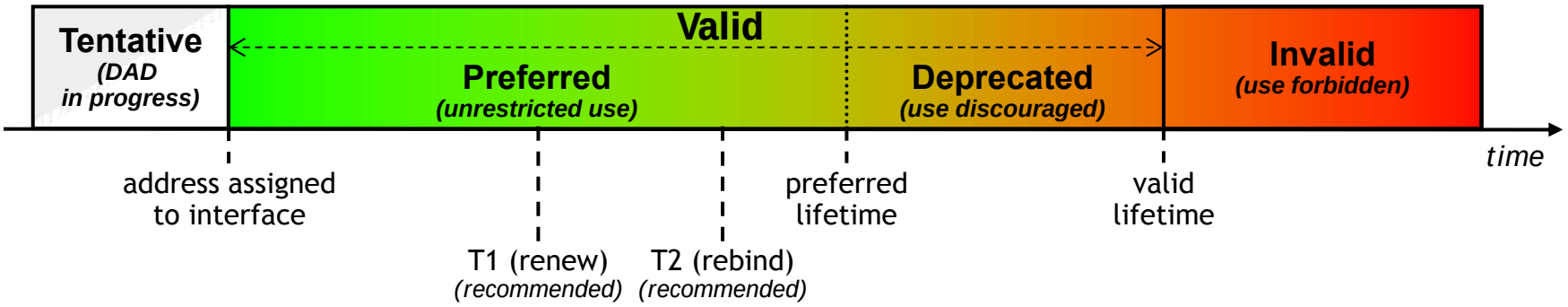
IPv6 Address Type Description

- 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

Address Lifetime

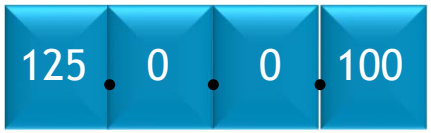
Two timers are associated with graceful degradation of v6 address bindings:

- Preferred Lifetime – the length of time that a valid address is preferred (i.e., the time until deprecation). When the preferred lifetime expires, the address becomes deprecated.
- Valid Lifetime - the length of time an address remains in the valid state (i.e., the time until invalidation). The valid lifetime must be greater than or equal to the preferred lifetime. When the valid lifetime expires, the address becomes invalid.

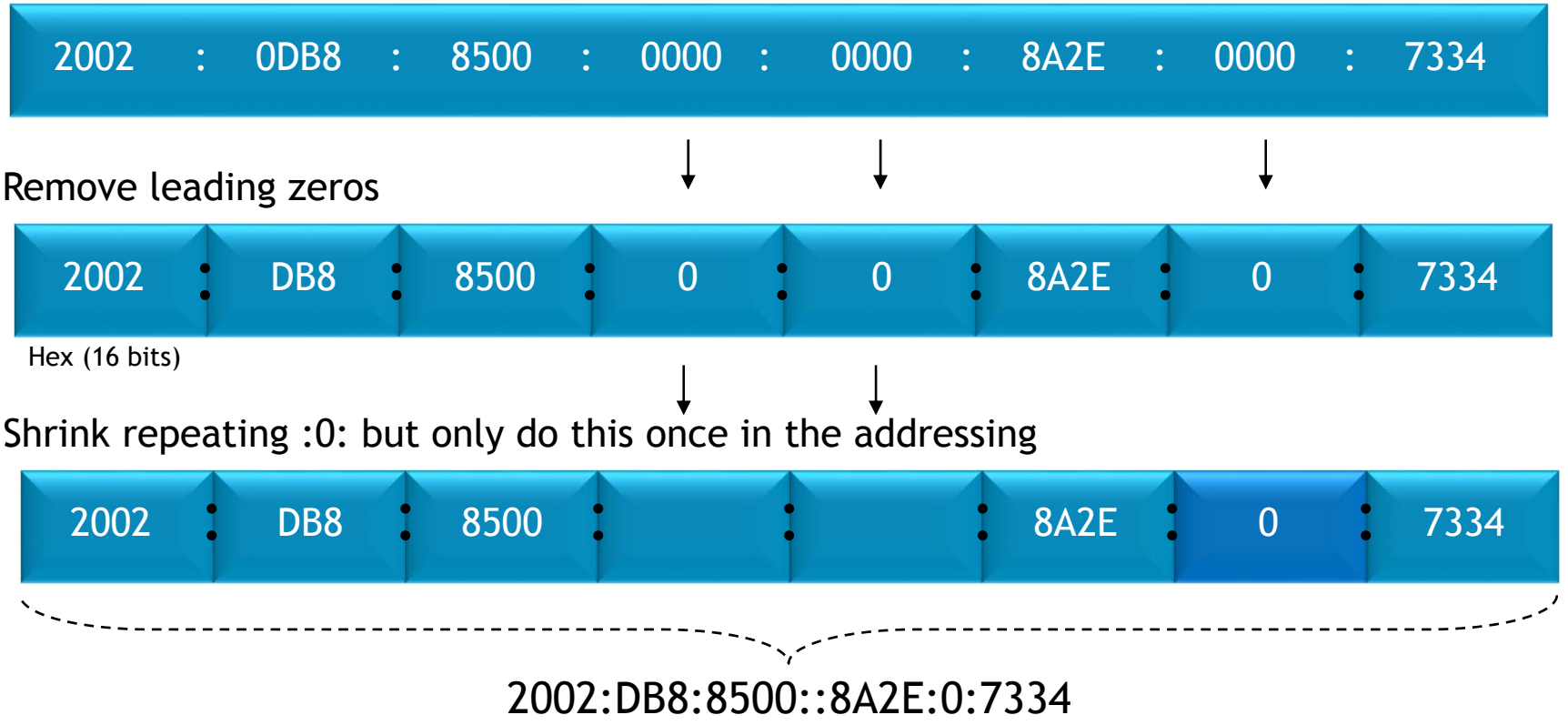


IPv6 Address Notation

- 32 bit IPv4 address notation: **dotted decimal**



- 128 bit IPv6 address notation: **colon hexadecimal** - each colon to separate 16 bits



IPv6 Address Types

Ref: RFC4291 & http://www.iana.org/assignments/ipv6-address-space

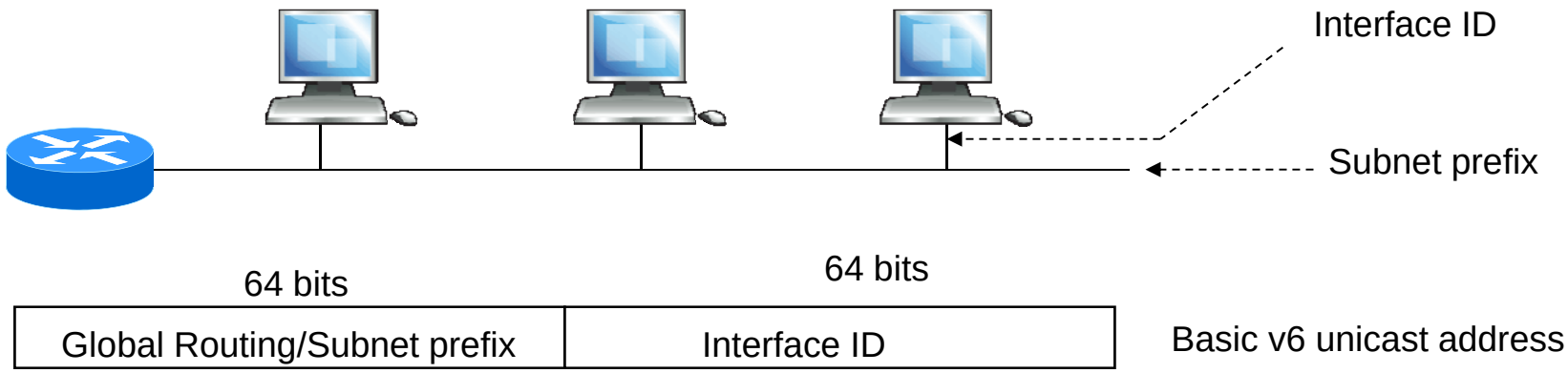
- An IPv6 address can be identified by the high-order bits as below
  - Unspecified – : : /128, i.e. 00…0, used by an initializing host to obtain IP address
  - Loopback – : :1/128, i.e. 00…1
  - Multicast addresses – FF00: : /8, i.e. binary prefix 11111111, also used to replace broadcasting
  - Link Local Unicast – FE80: : /10, like 169.254/16 in IPv4
  - Unique Local Unicast – FC00: : /7, routable only within a private IPv6 network (RFC4193)
  - Global Unicast – all others

Global Routing Prefix (n bits)	Subnet Prefix (m bits)	Interface ID (128-n-m bits)

  - Anycast addresses are included in the unicast spaces
- IPv6 still uses the concept of Subnet Prefix (network) and Interface ID (host); through hosts and very simple routers may have no knowledge of the internal structure of an IPv6 unicast address

IPv6 Unicast Address Basic Structure

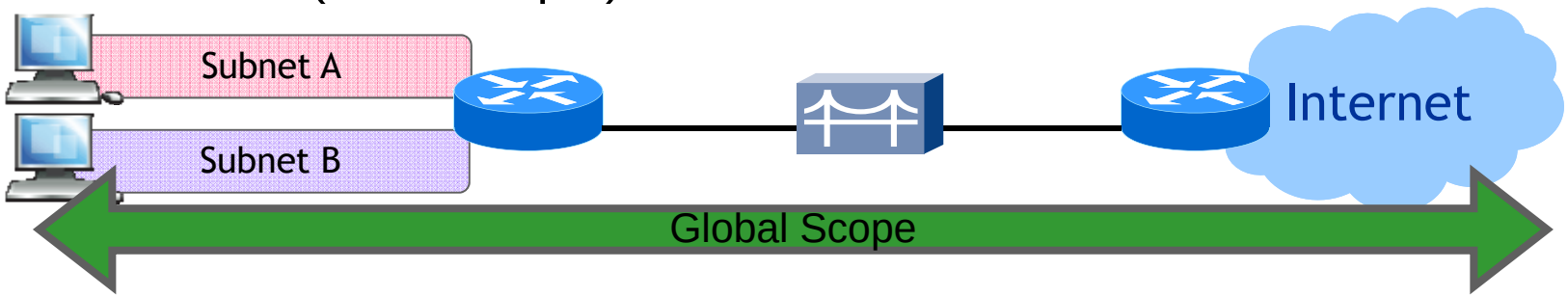
- Current address structure is as follows:
  - 64 bits for subnet prefix and 64 bits for interface ID (may use MAC address)



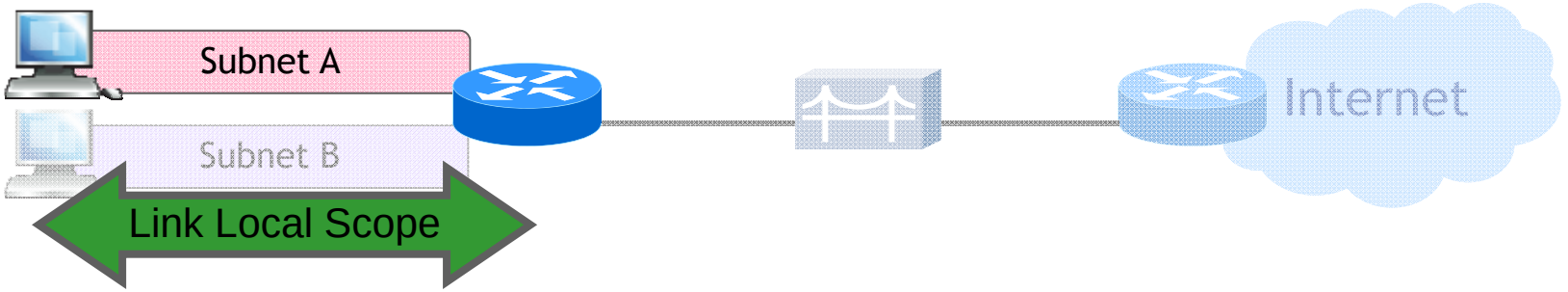
  - The only exceptions to the 64/64 split are addresses with embedded IPv4 address
    - The first 3 bits of these addresses are 000

IPv6 Address Scopes

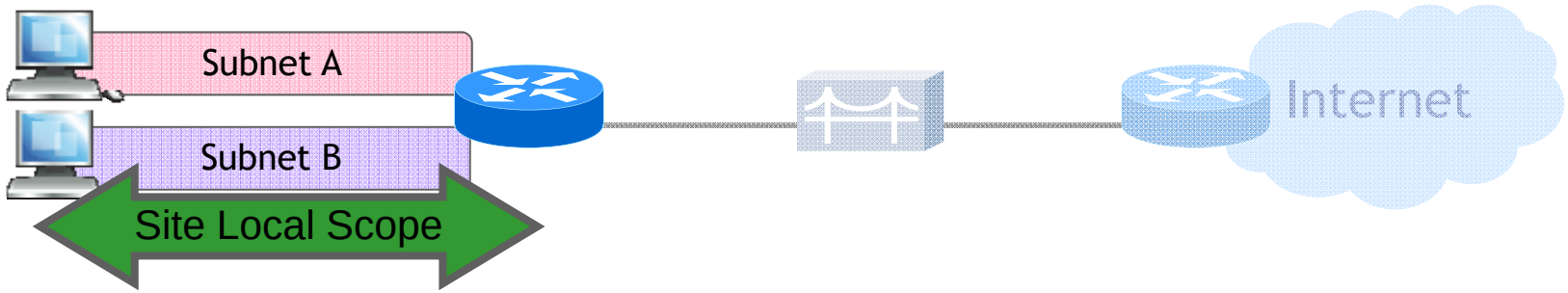
Global unicast (/48 example)



Link local (FE80::/10)



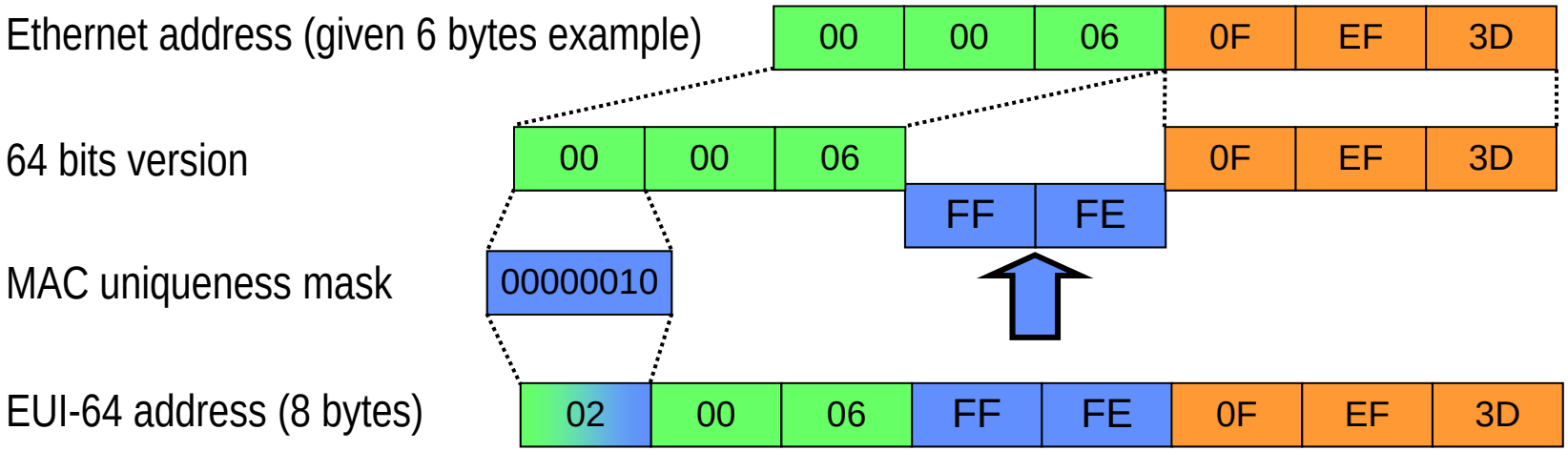
Unique local addresses (FC00::/7, e.g. FD00::/8 for /48 prefixes)



Interface ID Encoding

Recommend to use modified EUI-64 format addresses except for those with embedded IPv4 address

- EUI-64 is extended unique identifier managed by IEEE
- Current 48 bits Ethernet address can be embedded into the 64 bit-format
- EUI-64 address is formed by inserting FFFE and OR'ing a bit identifying the uniqueness of the MAC address



Common IPv6 Multicast Addresses

IPv6 multicast addresses – FF00: : /8

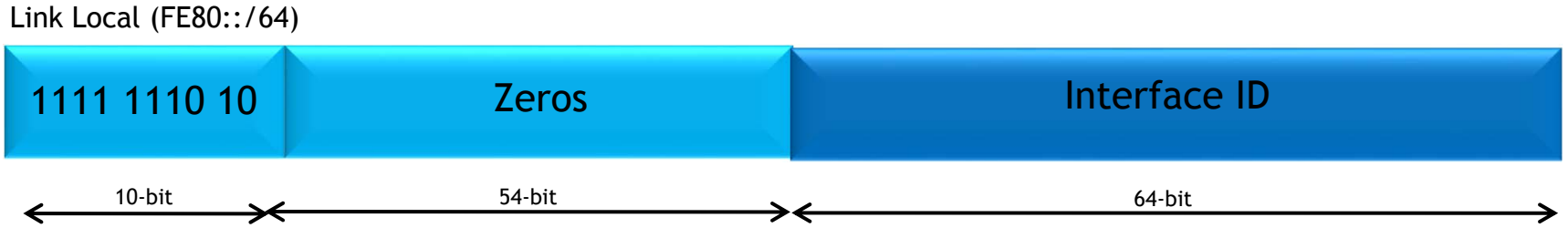
Address	Description
FF01::1	All IPv6 nodes within the node-local scope
FF01::2	All IPv6 routers within the node-local scope
FF02::1	All IPv6 nodes within the link-local scope
FF02::2	All IPv6 routers within the link-local scope
FF02::5	All OSPFv3 routers within the link-local scope
FF02::6	All OSPFv3 designated routers within the link-local scope
FF02::9	All RIPng routers within the link-local scope
FF02::A	All EIGRP routers within the link-local scope
FF02::D	All PIM routers within the link-local scope
FF02::16	ALL MLDv2 routers within the link-local scope
FF02::1:2	All DHCPv6 agents (servers and relays) within the link-local scope
FF05::2	All IPv6 routers within the site-local scope
FF05::1:3	All DHCPv6 servers within the site-local scope
FF02::1:FF00:0/104	IPv6 solicited-node multicast address within the link-local scope

Assigning IPv6 Addresses

- IPv6 hosts normally have more than one IPv6 address
- Stateless Address Auto-Configuration (SLAAC) is based on ICMPv6 and mandatory
  - Hosts choose their own IPv6 address by appending their Interface ID to any /64 prefix
  - SLAAC is supported by every IPv6 host and cannot be disabled
- DHCPv6 is optional: not used by all hosts
  - Works like DHCPv4 for address assignment, but
  - Does not provide any information about routers!
  - Does not replace SLAAC

IPv6 Link-Local Address

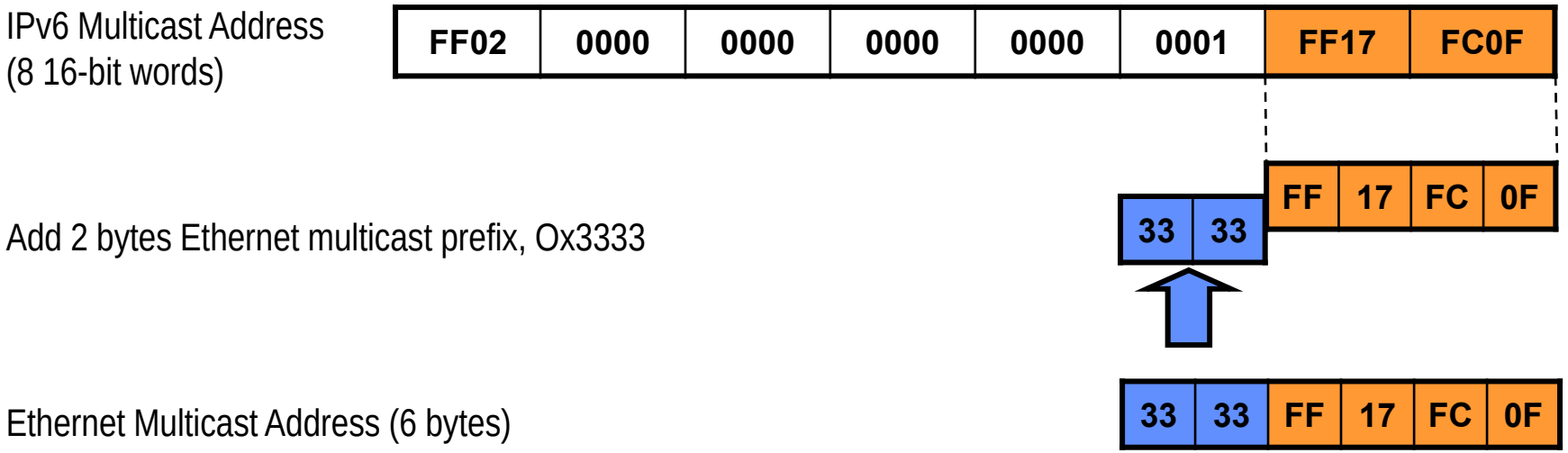
- Assigned automatically when an interface is enabled and auto configured using the Interface ID (e.g. EUI-64)
- Infinite preferred and valid lifetime
- Used to reach nodes on the same link (for auto configuration, discovery, …)
- IPv6 interfaces must have at least one Link-local address.
- Routers must not forward any packets with source address or destination address equal to Link-Local to other links.



IPv6 over Ethernet

- IPv6 has a specific protocol ID for Ethernet Type field

- IPv6 multicast address is mapped to Ethernet with a specific prefix



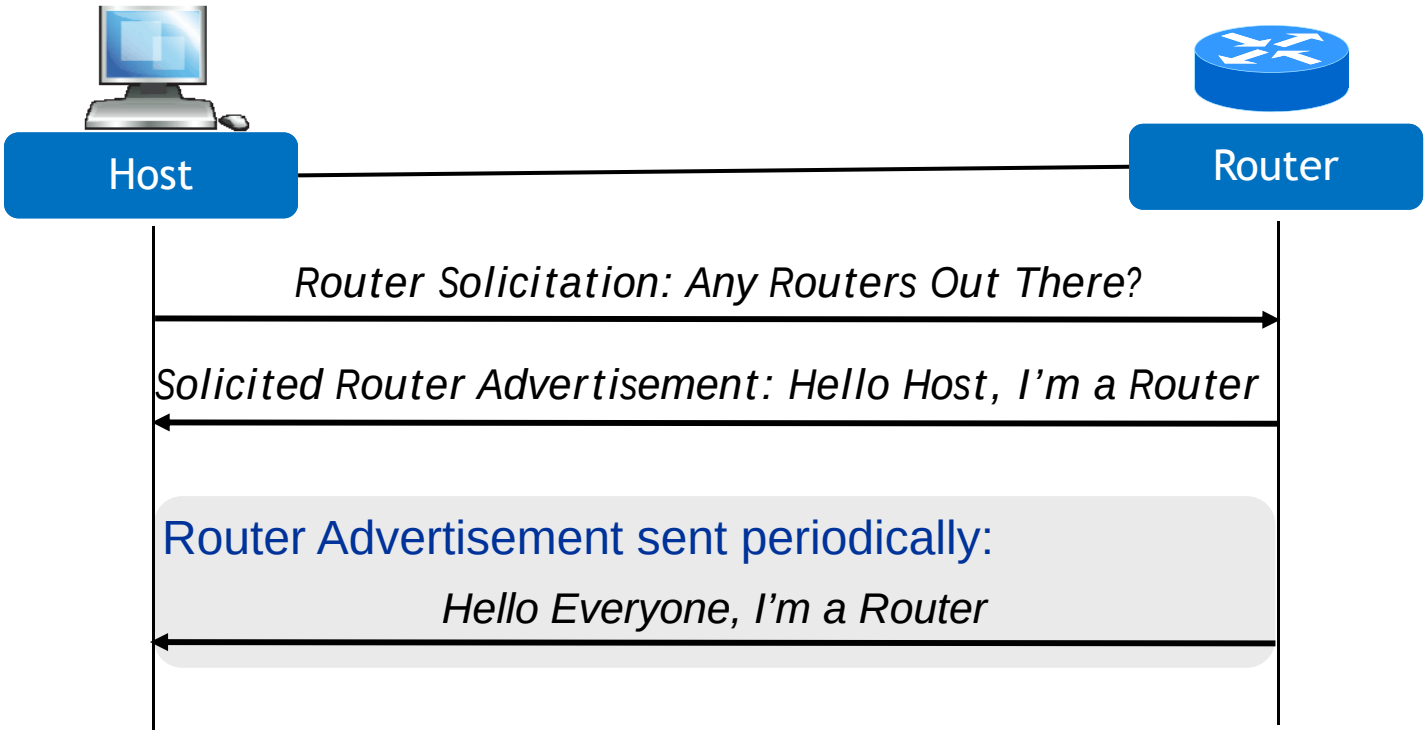
ICMPv6 & IPv6 Routing

- IPv6 a.k.a. IPng (next generation)
- ICMP is modified into ICMPv6 (RFC2463)
  - ARP and IGMP are incorporated into ICMPv6
  - RARP is deleted
  - 5 ICMPv6 packet types: Router Solicitation / Router Advertisements, Neighbour Solicitation / Neighbour Advertisements, Redirect
- Routing in IPv6 is not changed much from IPv4
  - IPv6 has 2 types of routing protocols: IGP and EGP
  - IPv6 still uses the longest-prefix match routing algorithm
  - Routing protocols are enhanced for IPv6: RIPng, OSPFv3, MP-BGP, …

ICMPv6 Router Discovery

An IPv6 host must discover a router using ICMPv6 Router Advertisements

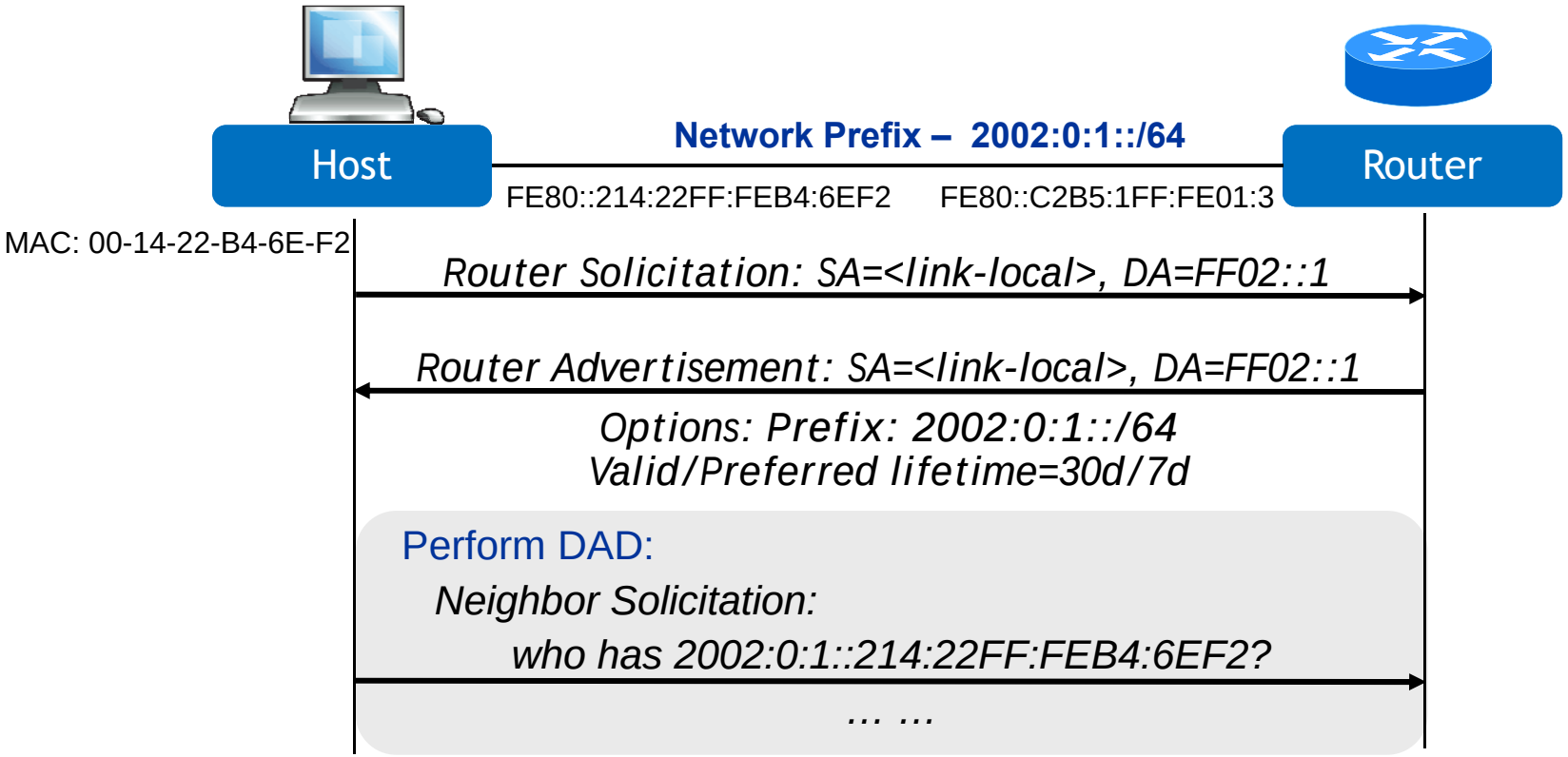
- Every host needs to find a router first
- Unlike IPv4 which assigning a default gateway to host



ICMPv6 SLAAC – RFC2462

StateLess Address Auto-Configuration steps on an active interface:

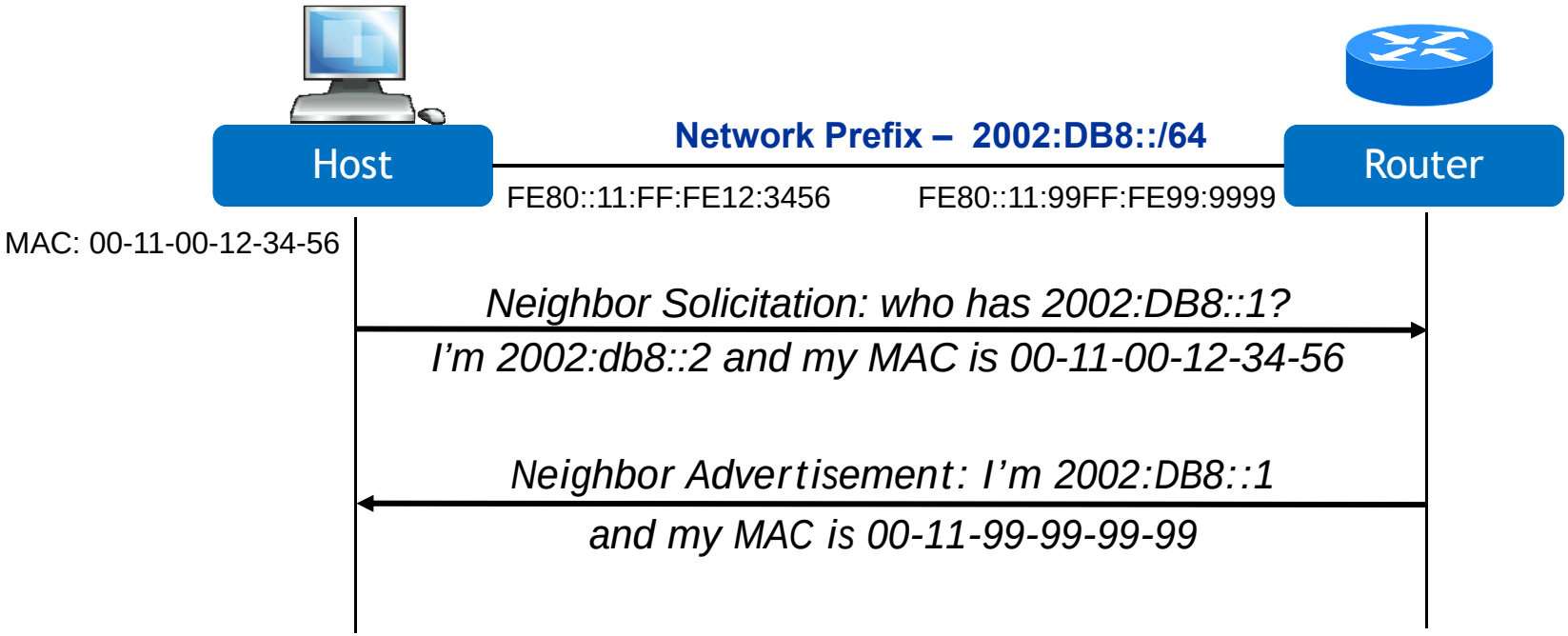
1. Discover prefix on link through RA messages
2. Verify address uniqueness by carrying Duplicate Address Detection (DAD)
3. Assign the address to the interface after passing DAD check



ICMPv6 Neighbor Discovery: Address Resolution

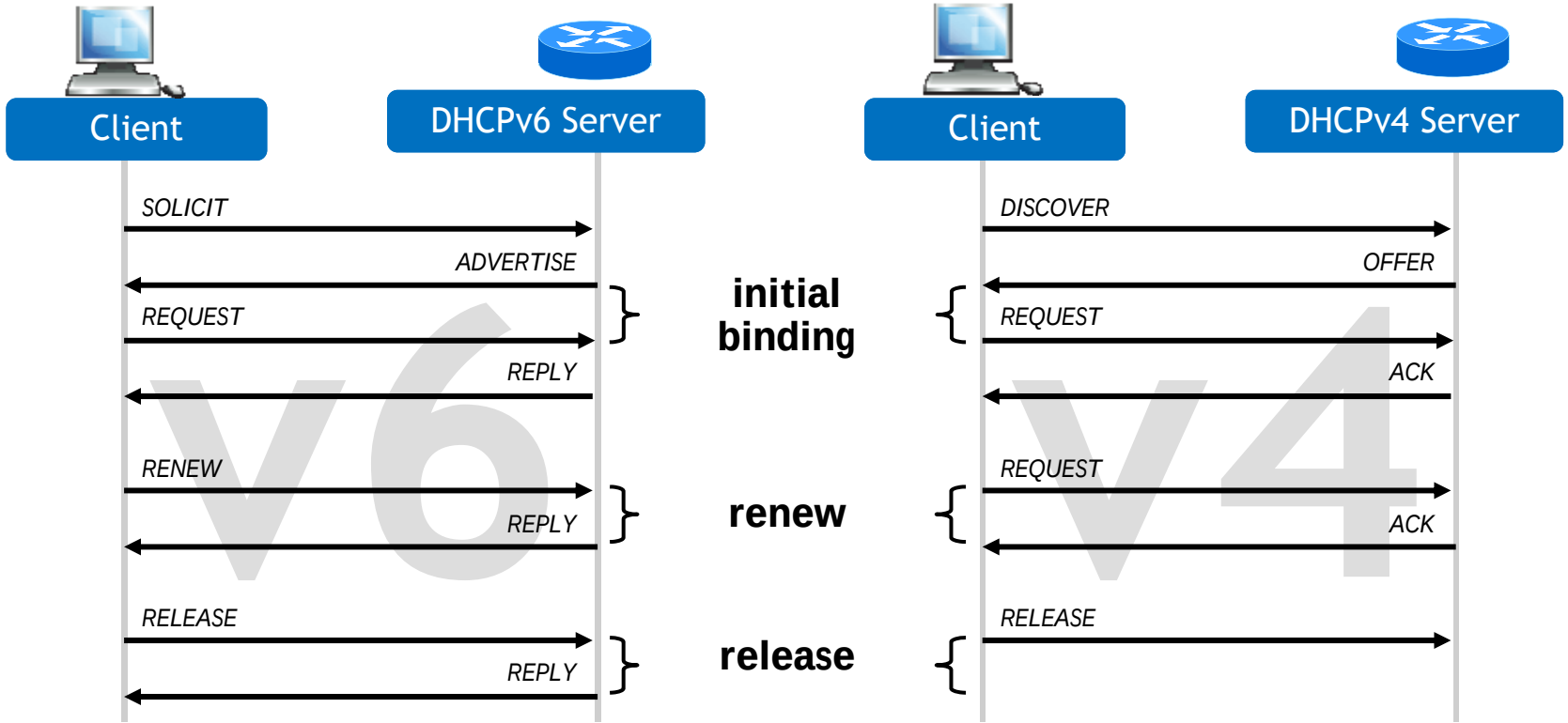
Neighbor Discovery Example:

- A host wants to send traffic to 2002:db8::1
- The host knows that 2002:db8::/64 is on-link, learnt about this from the Router Advertisement



DHCPv6 and DHCPv4

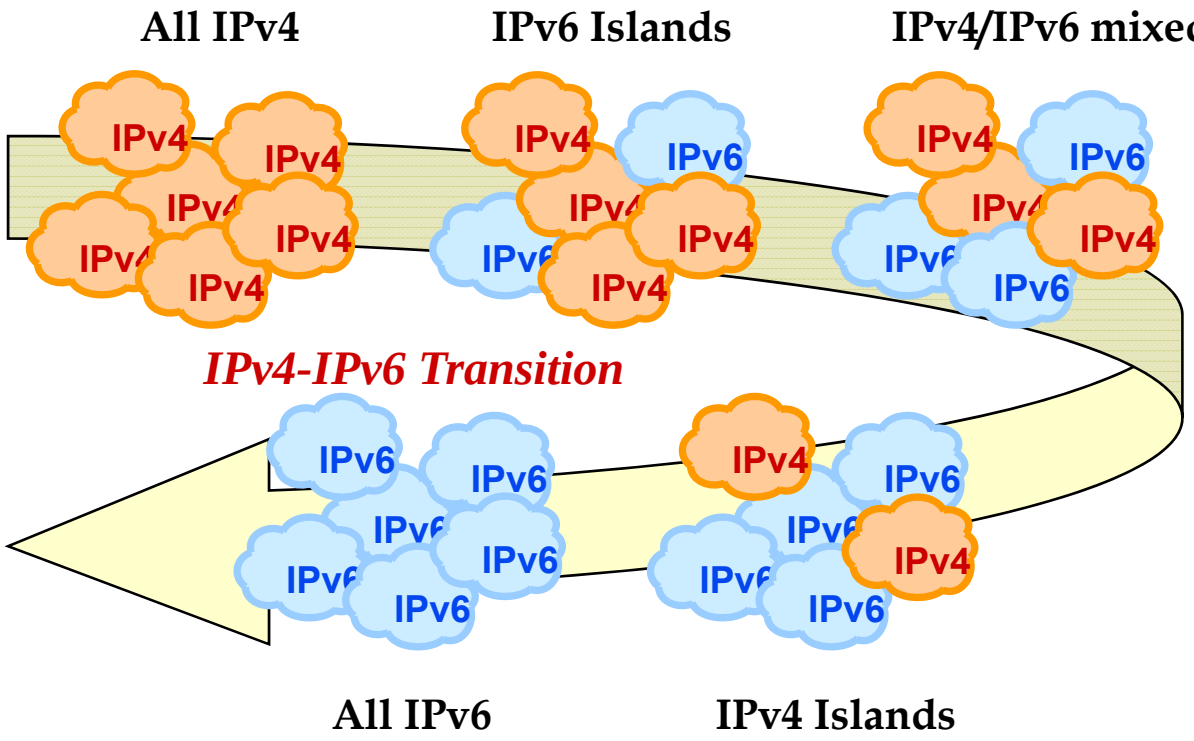
- Stateful DHCPv6 keeps state of client lease
- Provides additional information (e.g. DNS server, domain, etc.)
- Conceptually similar to IPv4 DHCP (some message types have changed)
- Clients send messages to “All DHCP Relay agents and Servers” multicast address (FF02::1:2)
- Servers send messages in unicast to the client link local address



IPv6 Neighbor Discovery

IPv6 ND feature	Description	IPv4
Router discovery	Allows hosts to locate routers on attached links	Usually done via DHCP
Prefix discovery	Allows hosts to learn prefixes on attached links	Usually done via DHCP
Parameter discovery	Enables nodes to learn parameters such as link MTU and hop limit	PMTU discovery (RFC1191)
Address auto-configuration	Enables hosts to automatically configure an IP address	N/A
Address resolution	Allows hosts to determine the link-layer address for on-link destinations	ARP
Next-hop determination	Enables hosts to determine next-hop for given destination	ARP cache for on-link prefixes, default router otherwise
Neighbor Unreachability Detection (NUD)	Allows nodes to detect that a neighbor is no longer reachable	Dead gateway detection (RFC816, RFC1122)
Duplicate Address Detection (DAD)	Enables hosts to determine addresses already in use	ARP with SA=0

Transport Network Transition Phases



The transition method may differ for the different phases e.g. whether one has universal v4 connectivity, or v6 connectivity

Diagram reproduced from: "IPv4 to IPv6 Transition, Interoperability and Issues", Shiao-Li Charles Tsao

Basic idea is to migrate subnet by subnet

- Use dual stack as much as possible
- Use translator/gateway as proxies for simple devices not capable of dual stack (e.g. SIP phones)
- Tunnel IP v6 traffic over IPv4 infra-structure first; v4 over v6 later

IPv4 to IPv6 Transition Techniques

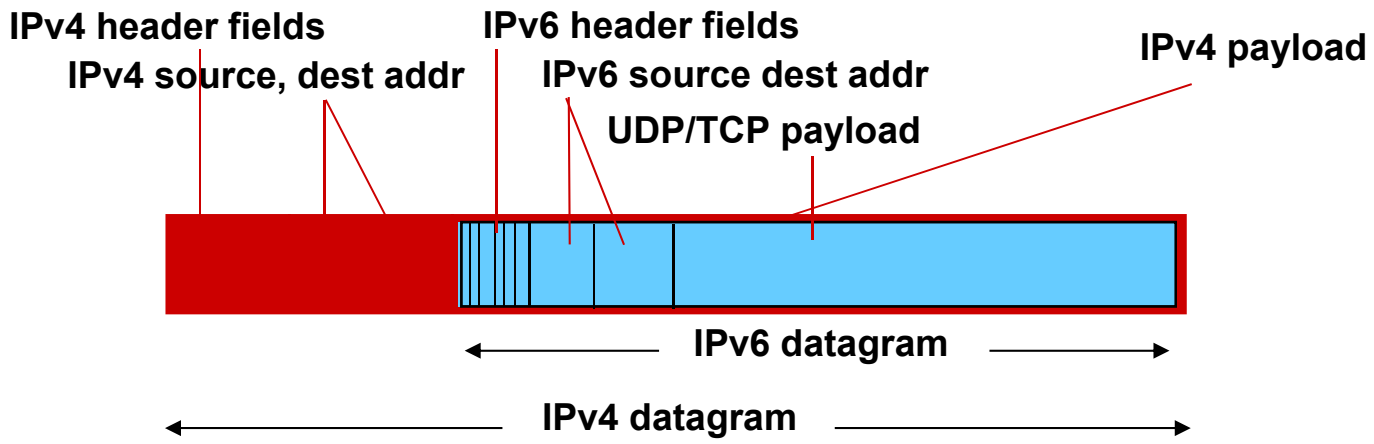
- Dual Stack (RFC4213): both protocols running in hosts and routers until all of the Internet uses IPv6
  - Queries to DNS to determine IP address version
  - Often use IPv4-mapped address
- Tunneling
  - 6over4 (RFC2 2529): put IPv6 into IPv4 packets like Ethernet emulation and run that tunnels between two pre-configured end points
  - 6to4 (RFC 3056): use v6 prefix 2002::/16 to connect v6 sub-networks via a pair of 6to4 router through v4 network
  - Teredo Server (RFC4380): use v6 prefix 2001::/32 to support remote access of v6 network through v4 network with NAT
  - Tunnel brokers: e.g. FreeNet6 at http://www.freenet6.net/
- ISATAP (RFC4214, Intra-Site Automatic Tunnel Addressing Protocol): use v4 tunnel a an L2 link to connect a host to v6 network via an ISATAP server.
- NAT-PT (RFC2766, Network Address Translation–Protocol Translation): used for v6 only host to communicate with v4 host

Transition from IPv4 to IPv6

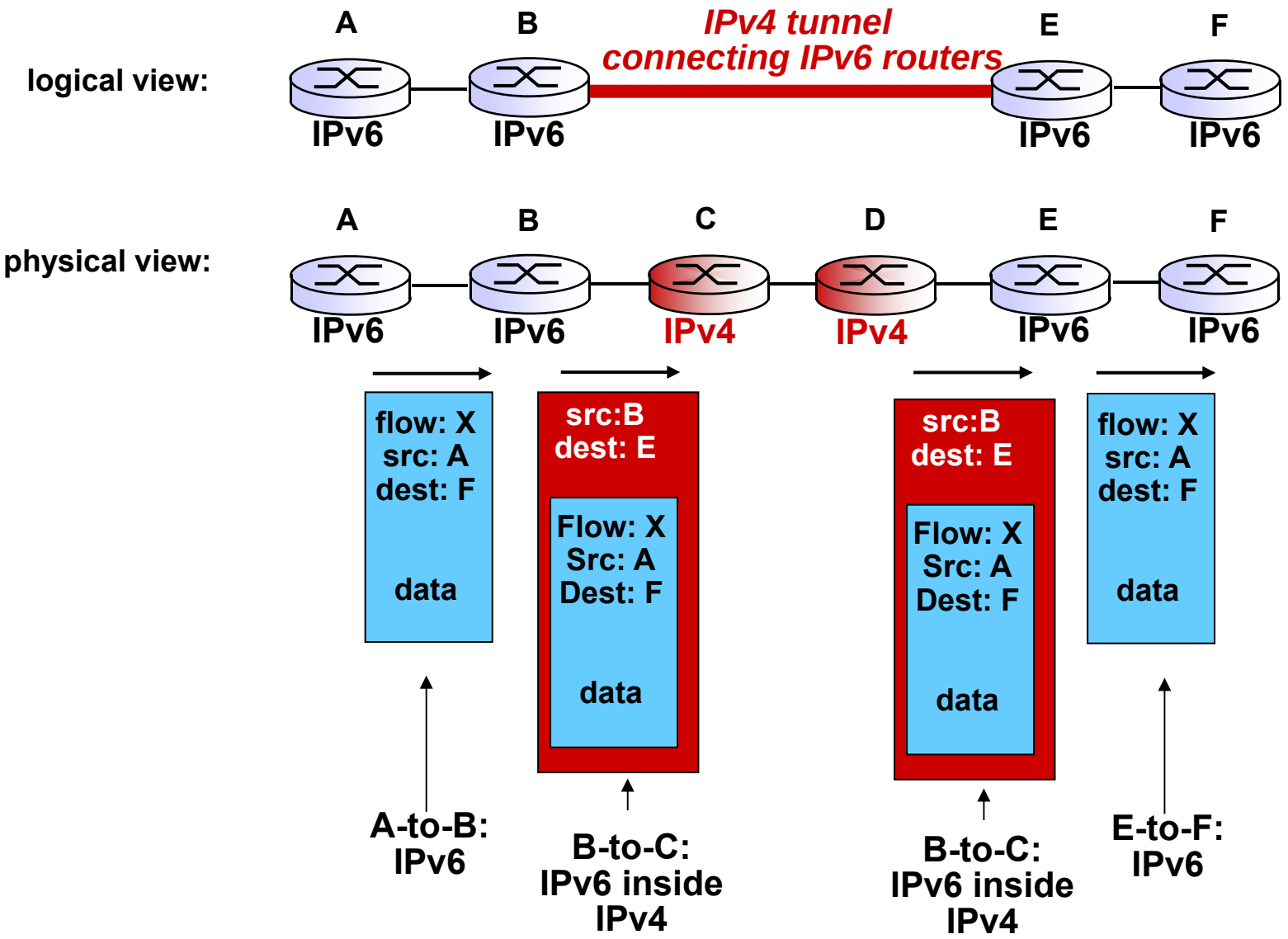
Not all routers can be upgraded simultaneously

- 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

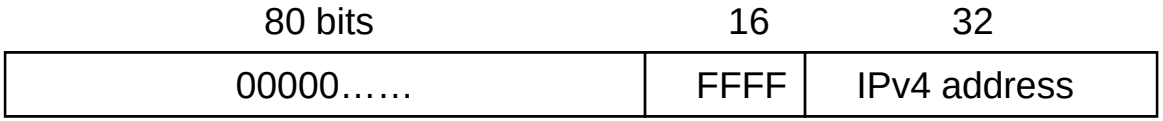


6over4 Tunneling

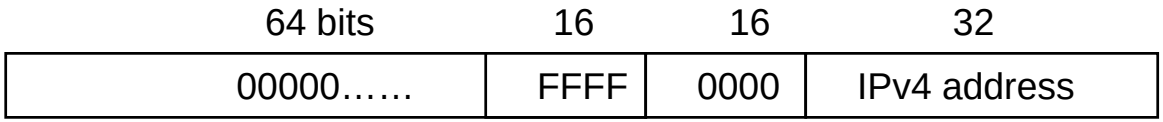


IPv6 Addresses with Embedded IPv4 Address

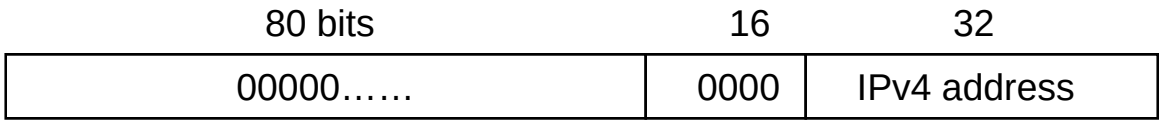
- **IPv4-Mapped IPv6 address**
  - **Represents an IP v4 address in IP v6 format (i.e. the end-point is a v4 node)**
  - **Allows a host that support both IPv4 and IPv6 to communicate with a host that supports only IPv4.**
  - **The IP v4 address must be a globally unique IPv4 unicast address**



- **v4 translated address (SIIT, RFC 2765)**



- **IPv4-Compatible IPv6 address**
  - **To be deprecated as not used in current IPv6 transition**

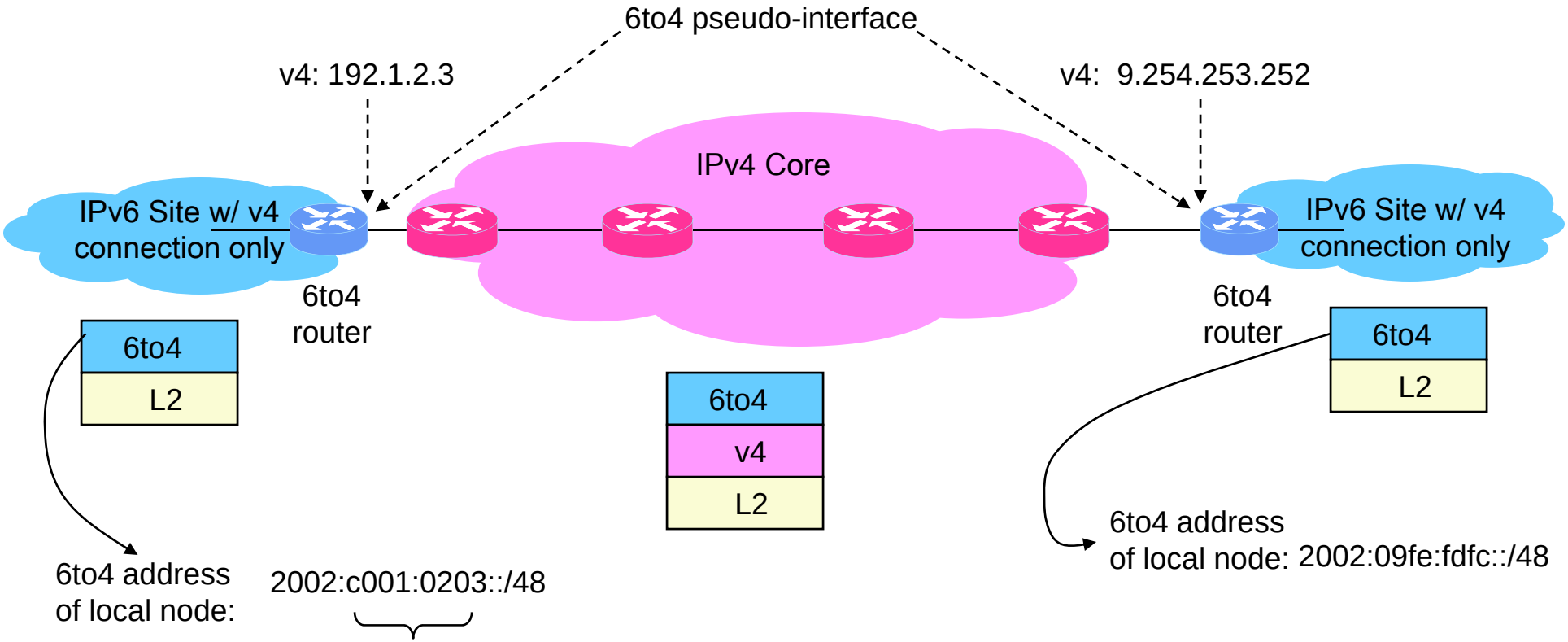


RFC3056 – 6to4 Tunneling
Connection of IPv6 Domains via IPv4 Clouds

- 6to4 is a special class of v6 unicast address, used when v6 sub-networks are connected via a v4 network
  - 6to4 Prefix 2002::/16 used to allocate 6to4 Addresses
- The v6 packet is encapsulated within a v4 address through v4 network
  - Encapsulation done by 6to4 Border Router with protocol type 41
  - Host is required to have address selection rule
  - Minimum impact on routing table
    - > No IPv4 routing information is imported into IPv6 routing (nor vice versa)
- The v4 address of the point of attachment (at 6to4 Router) is encoded as part of the v6 6to4 address
  - The v4 address must be a public v4 address
  - TLS: Top Level Aggregation

FP 001	TLS 0x0002	v4 Address (pt. of attach.)	Sub-network ID	Host Interface ID
3	13	32	16	64 bits

6to4 Configuration



192.1.2.3 → 1100 0000 → c0010203
0000 0001
0000 0002
0000 0003

RFC5569: IPv6 Rapid Deployment on IPv4 Infrastructures (6rd)

Note: The v4 network must be contiguous