Computer Networks

IPv6

(bruno.quoitin@umons.ac.be)

Important note: These slides are partly based on a course by O. Bonaventure (UCLouvain) and the book "IPv6 Essentials" by S. Hagen.

IPv6

- 4. 1 Motivations
- 4.2 IPv6 Addressing Architecture
- 4.3 IPv6 Packets
- 4.4 ICMPv6
- 4.5 DNS support for IPv6
- 4.6 Transition Mechanisms

Issues with IPv4

- Late 1980s
  - Exponential growth of the Internet
- 1990
  - Other network protocols exist (*AppleTalk*, *DECnet*, *IPX*, ...)
  - Governments (esp. US) push for *ConnectionLess Network Protocol* (CLNP, ISO standard)
- 1992
  - Most class B networks have been assigned
  - Class based routing failure
  - Networking experts warn that IPv4 address space could become exhausted

Issues with IPv4 (2)

- How to solve the exhaustion of class B addresses ?

- Short term solution
  - Define *Classless Interdomain Routing* (CIDR) and introduce the related changes in routers
  - Deployment started in 1994

- Long term solution
  - Develop Internet Protocol – next generation (IPng)
    - call for proposals RFC1550 (dec 1993)
    - criteria for choice, RFC1719/1726 (dec 1994)
    - several proposed solutions
      - TUBA, PIP, CATNIP, SIP, NIMROO, ENCAPS...

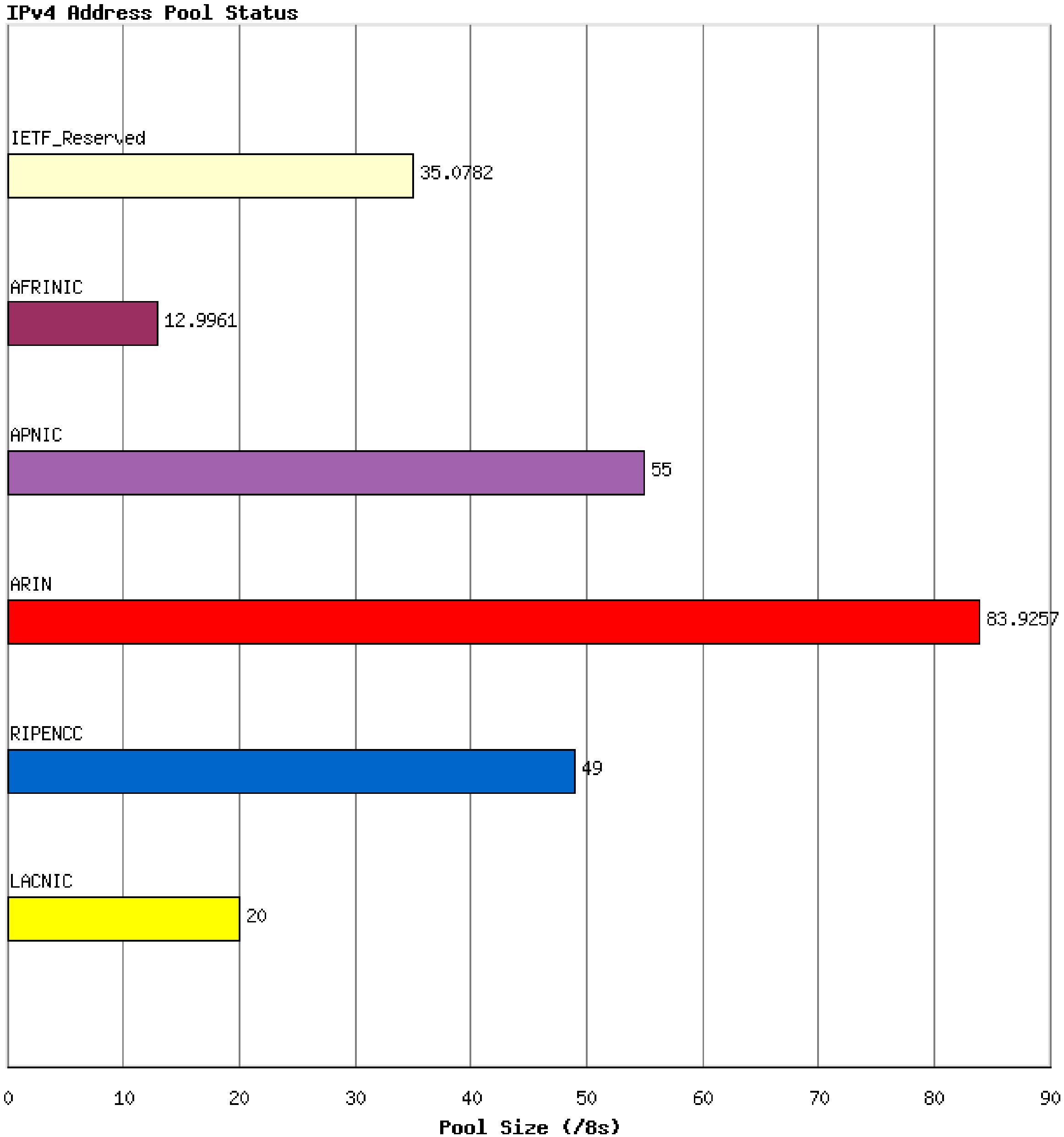
Issues with IPv4 (3)

- Implementation issues – 1990s
  - IPv4 packet format is complex
  - IP forwarding difficult to implement in hardware

- Missing functions – 1990s
  - IPv4 requires lots of **manual configuration**
    - competing protocols (CLNP, AppleTalk, IPX, ...) already supported auto-configuration in 1990s
  - How to support ***Quality of Service*** (QoS) in IP ?
    - IntServ and DiffServ did not exist then
  - How to better support **security** in IP ?
    - security problems started to appear (but less important than today)
  - How to better support **mobility** in IP ?
    - GSM started to appear and some were dreaming of mobile devices attached to the Internet...

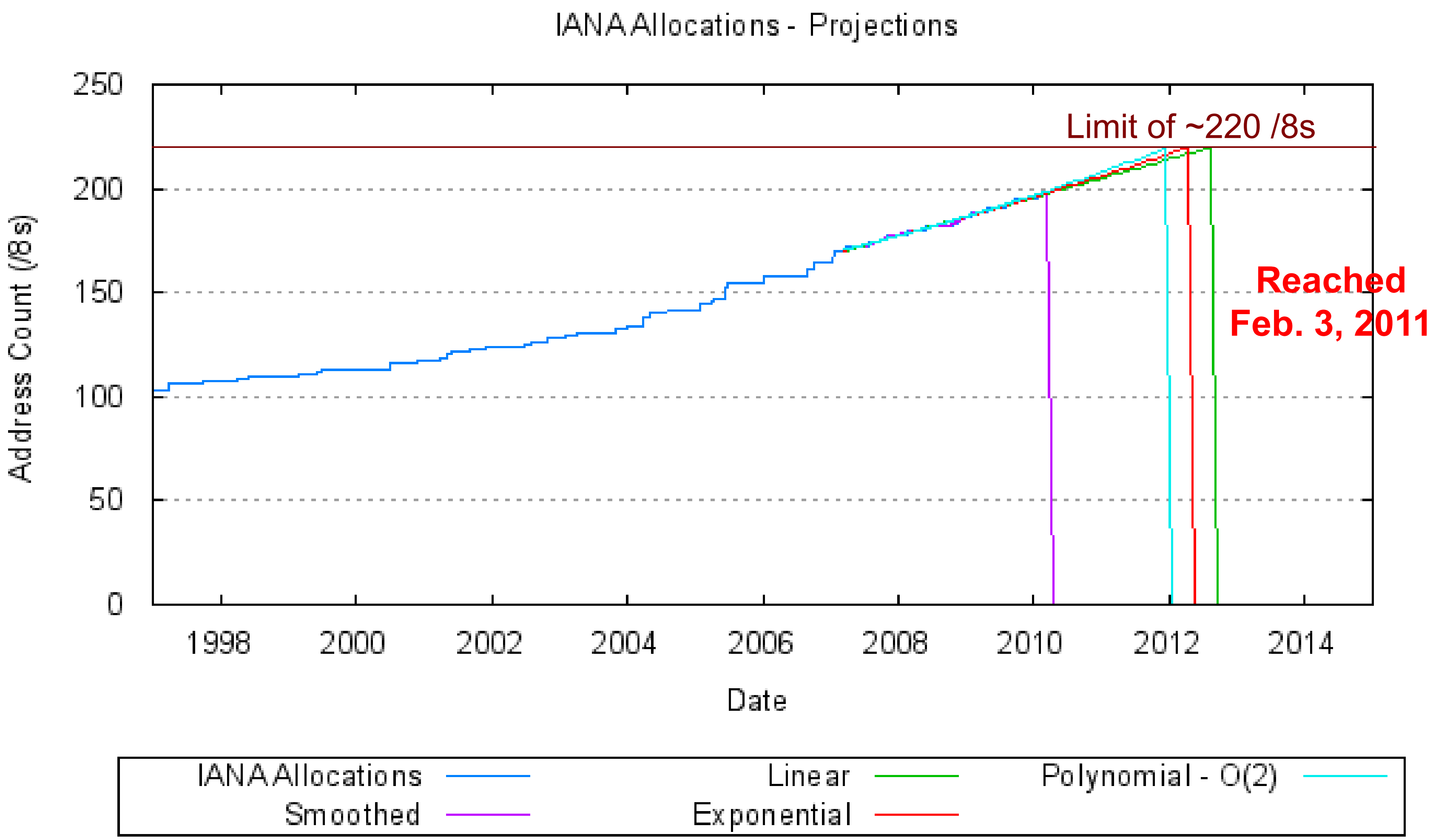
Source: http://xkcd.com/195/

IPv4 address allocation



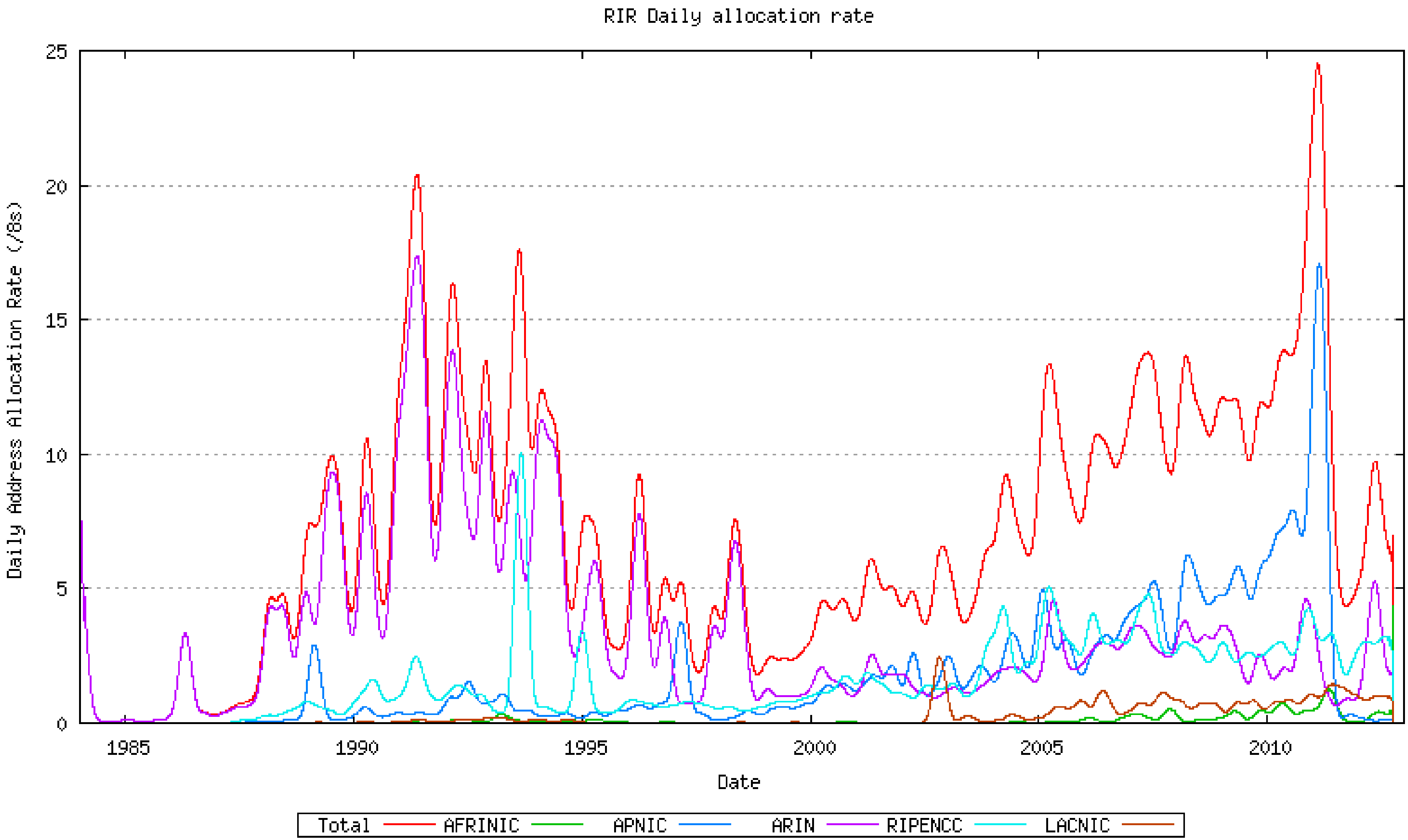
Source: http://www.potaroo.net/tools/ipv4/index.html
(retrieved on 24/10/2011)

IPv4 addr. exhaustion - prediction



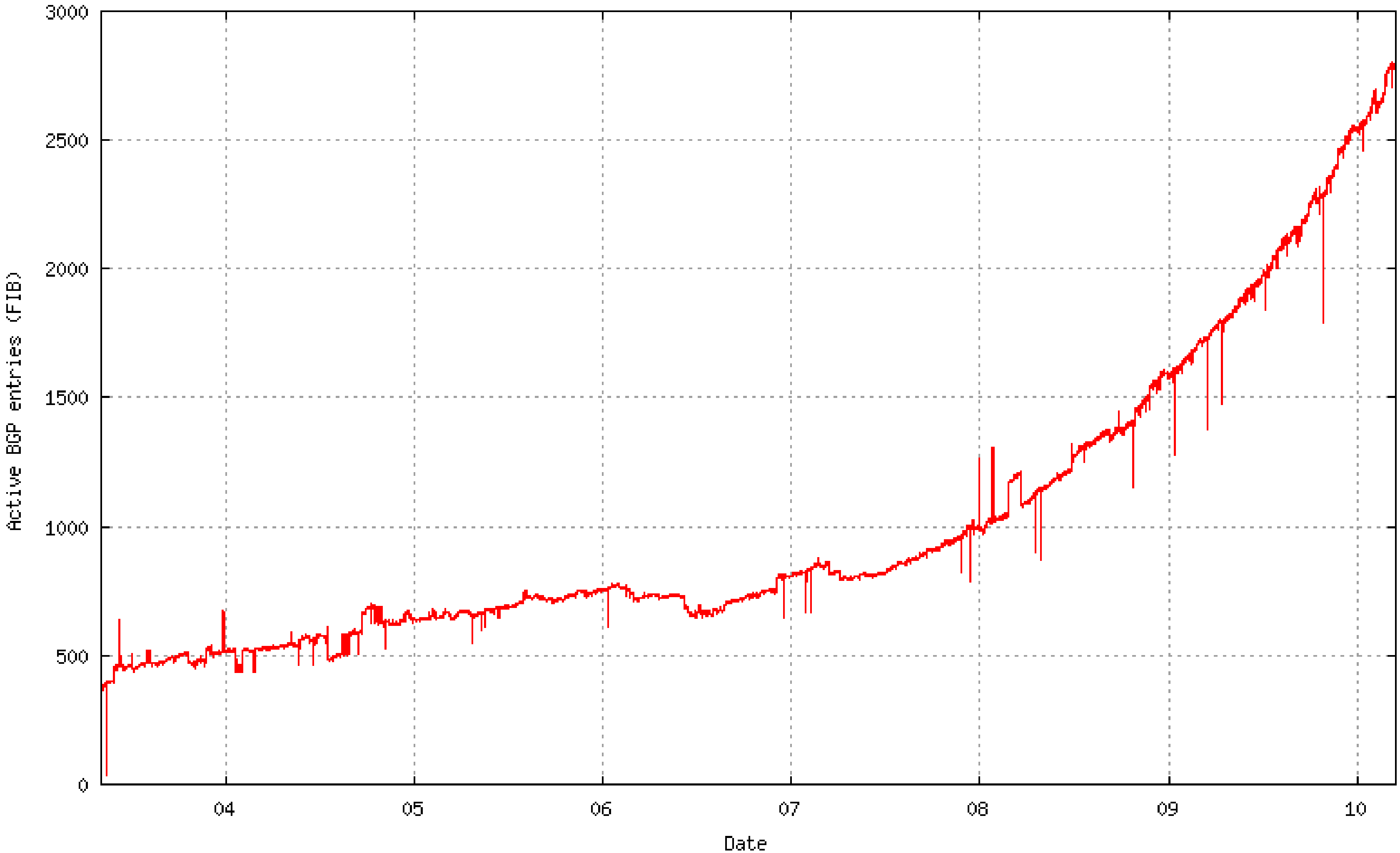
Source: http://www.potaroo.net/tools/ipv4/index.html
(retrieved on 17/03/2010)

IPv4 growth rate per region



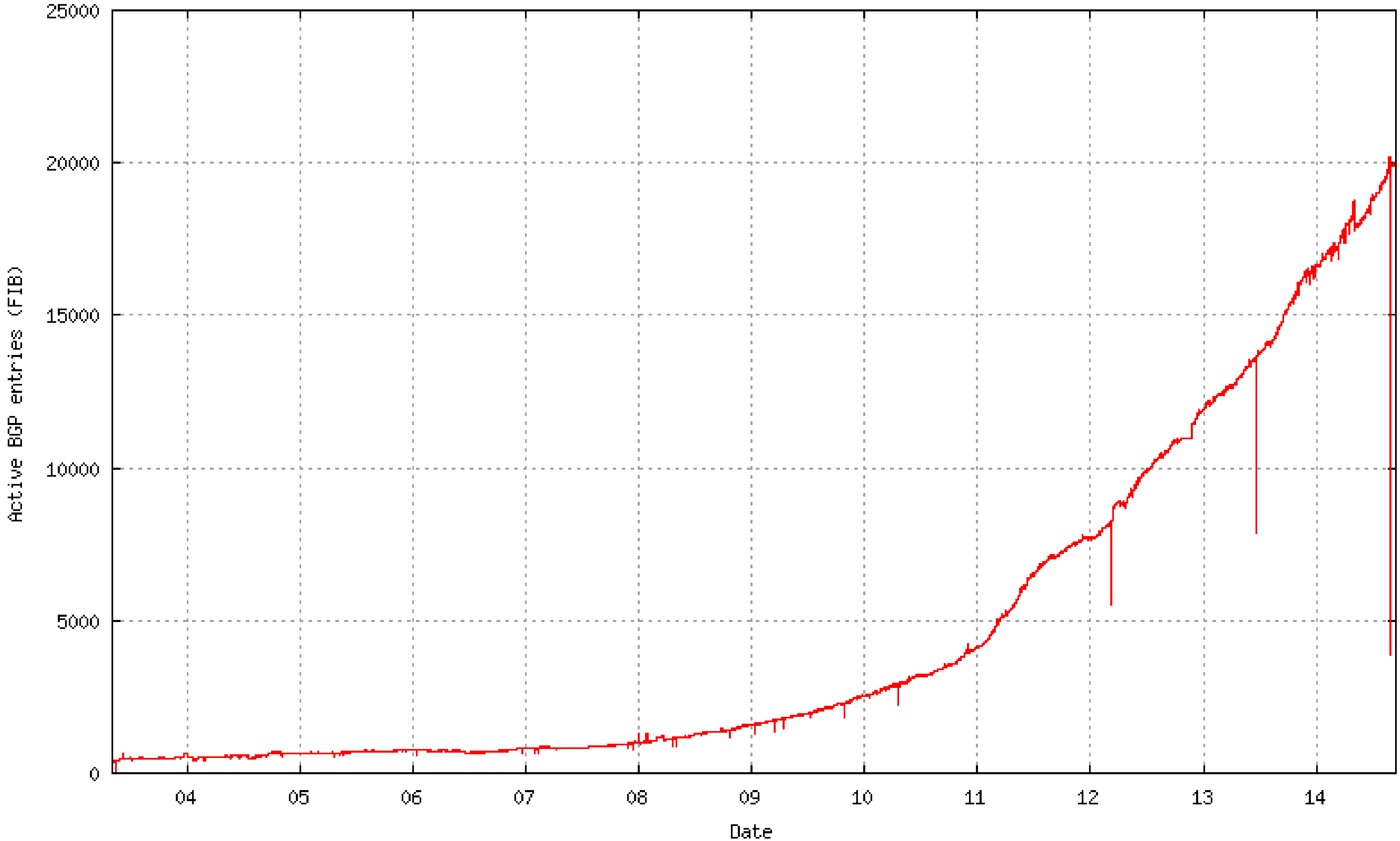
Source: http://www.potaroo.net/tools/ipv4/index.html
(retrieved on 11/10/2012)

IPv6 BGP advertisements (years ago)



Source: http://bgp.potaroo.net/v6/as6447/
(retrieved on 17/03/2010)

IPv6 BGP advertisements **today**



Source: http://bgp.potaroo.net/v6/as6447/
(retrieved on 14/09/2014)

NAT a solution ?

- Benefits
  - Reduces consumption of public IPv4 addresses
  - Hides internal IPv4 addresses inside residential and corporate networks
- Drawbacks
  - NAT traversal can be tricky
  - Goes against end-to-end principle
  - Gives a false feeling of security
  - Intermediate nodes may modify packet content
    - IP addresses
    - TCP/UDP port information
    - Some protocols encode IP addresses inside payload

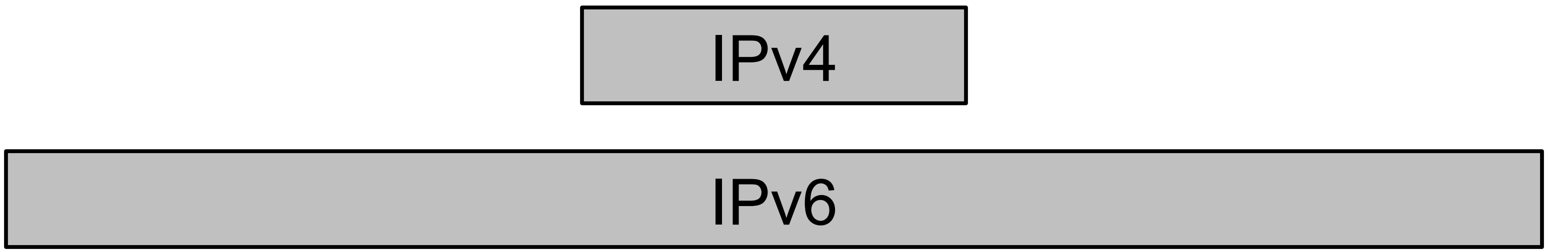
  - Carrier-Grade NAT : NAT444, LSN, ...

IPv6

- 4. 1 Motivations
- 4.2 IPv6 Addressing Architecture
  - 4.2.1 Unicast Addresses
  - 4.2.2 Multicast Addresses
  - 4.2.3 Anycast Addresses
- 4.3 IPv6 Packets
- 4.4 ICMPv6
- 4.5 DNS support for IPv6
- 4.6 Transition Mechanisms

IPv6 addresses

- Each IPv6 address is encoded in 128 bits



  - 3.4*10^{38} possible addresses
    - 340,282,366,920,938,463,463,374,607,431,768,211,456 :-)
  - about 4.86*10^{28} addresses per person on the earth
  - 6.67*10^{23} addresses per square meter
  - Looks unlimited... today

- Why 128 bits ?
  - Some wanted variable size addresses
  - Some wanted 64 bits (~ to exp. CPU data path width)
  - Hardware implementers prefer fixed size addresses

IPv6 addressing architecture

- Three types of IPv6 addresses
  - Unicast addresses
    - An identifier for a single interface. A packet sent to a unicast address is delivered to the interface identified by that address.
  - Anycast addresses
    - An identifier for a set of interfaces (usually on multiple nodes). A packet sent to an anycast address is delivered to the single "nearest" interface identified by that address.
    - Works well for stateless request/reply transactions (for example over UDP). DNS over UDP can use anycast addresses.
  - Multicast addresses
    - An identifier for a set of interfaces. A packet sent to a multicast address is delivered to all interfaces identified by that address.

IPv6 Addresses Notation

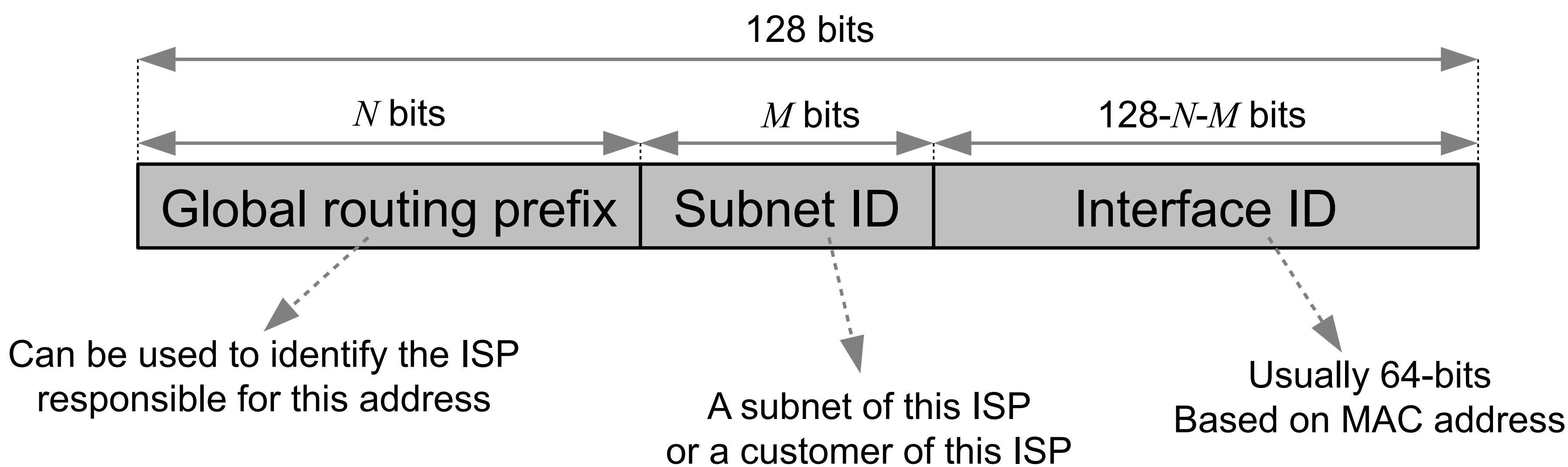
- How can we write a 128 bits IPv6 address ?
- Hexadecimal format
  - FEDC:BA98:7654:3210:FEDC:BA98:7654:3210
  - 2001:0DB8:0000:0000:0202:B3FF:FE1E:8329
    - leading zeros can be omitted → 2001:DB8:0:0:202:B3FF:FE1E:8329
- Compact hexadecimal format
  - Consecutive zeros can be replaced by a double colon. The double colon can appear only once in an address !
  - 2001:DB8::202:B3FF:FE1E:8329
  - FF01:0:0:0:0:0:0:101 → FF01::101
  - 0:0:0:0:0:0:0:1 → ::1

IPv6

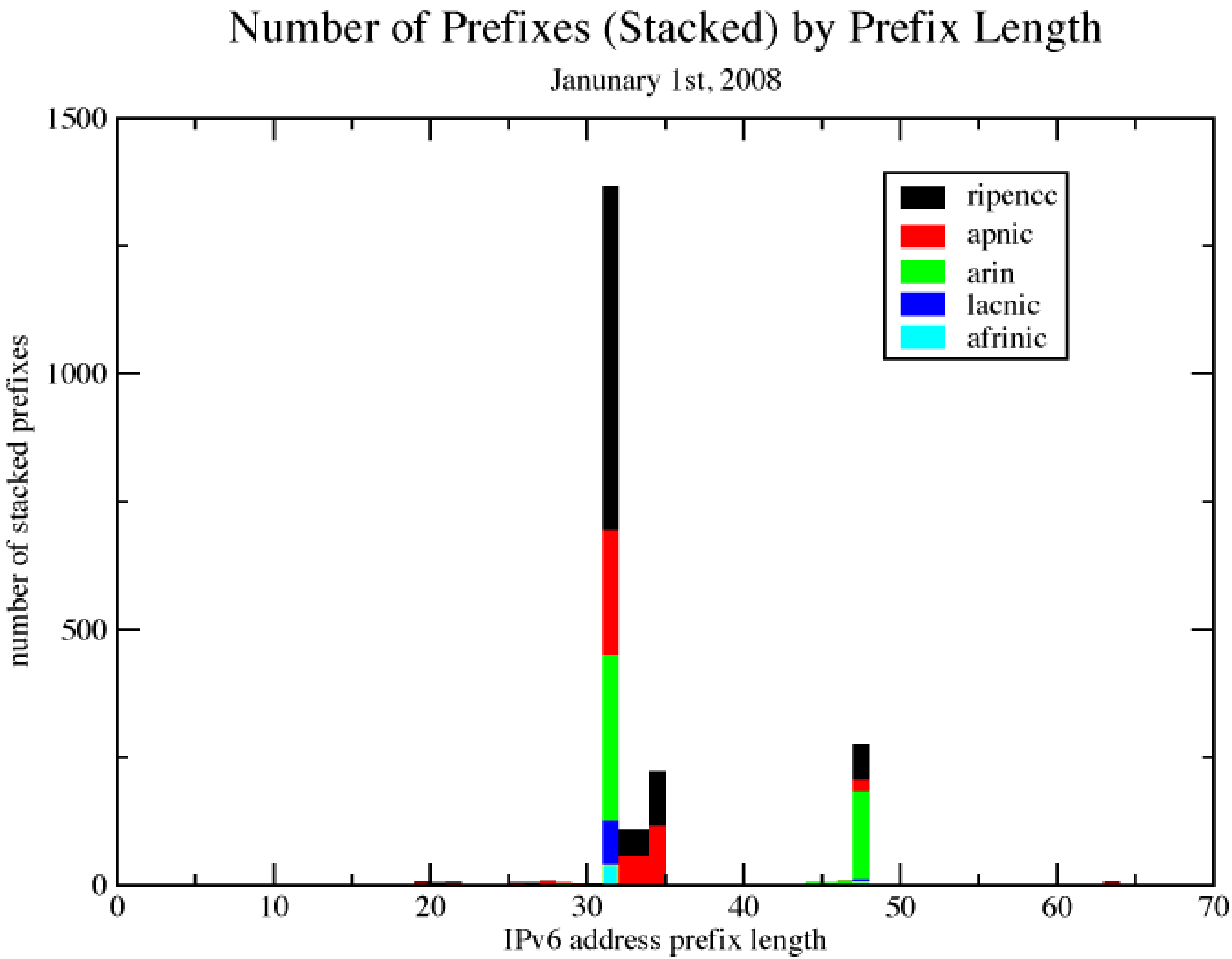
- 4. 1 Motivations
- 4.2 IPv6 Addressing Architecture
  - 4.2.1 Unicast Addresses
  - 4.2.2 Multicast Addresses
  - 4.2.3 Anycast Addresses
- 4.3 IPv6 Packets
- 4.4 ICMPv6
- 4.5 DNS support for IPv6
- 4.6 Transition Mechanisms

IPv6 Unicast Addresses

- Special addresses
  - Unspecified address: `0:0:0:0:0:0:0:0` (`::`)
  - Loopback address: `0:0:0:0:0:0:0:1` (`::1`)
- Global Unicast Addresses (RFC4291)
  - Addresses allocated hierarchically (see later)
  - N usually between 32 and 48



Allocation of IPv6 Addresses



Source: http://www.caida.org/research/topology/as_core_network/ipv6.xml
(retrieved on 17/03/2010)

Allocation of IPv6 Addresses

- IANA controls all IP addresses
  - delegates assignments of blocks to *Regional Internet Registries* (RIR): RIPE, ARIN, APNIC, AFRINIC, ...

Un client reçoit un préfixe différent pour chacun de ses fournisseurs

- An organisation can be allocated two different types of IPv6 addresses

/!\ coupure fournisseur

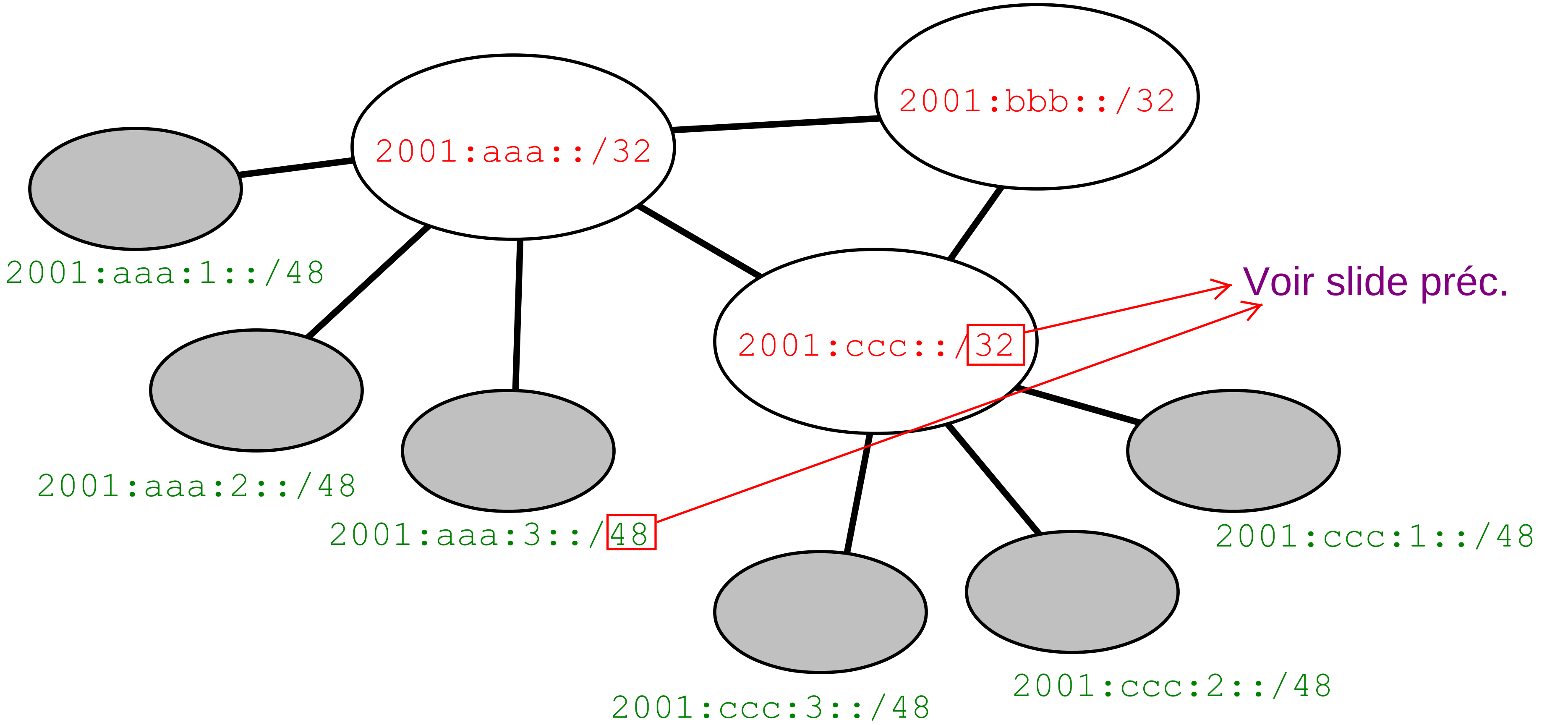
Deux types d'adresses afin d'éviter les même problème d'agrégation qu'IPv4

  - Provider Independent (PI) addresses
    - Usually allocated to ISPs or very large enterprises directly by RIRs
    - Default size is /32

Solutions possibles: entre la couche réseau et transport
¤SHIM6 => "traducteur/simulateur d'adresse"
¤HIP (mobile IP)
¤MPTCP (Multi Path TCP)

  - Provider Aggregatable (PA) addresses
    - Smaller prefixes, assigned by ISPs from their PI block
    - Size
      - /48 in the general case, except for very large subscribers
      - /64 when a single subnet is required by design
      - /128 when it is absolutely known that one and only one device is connecting

Allocation of IPv6 Addresses



Provider Independent (PI)

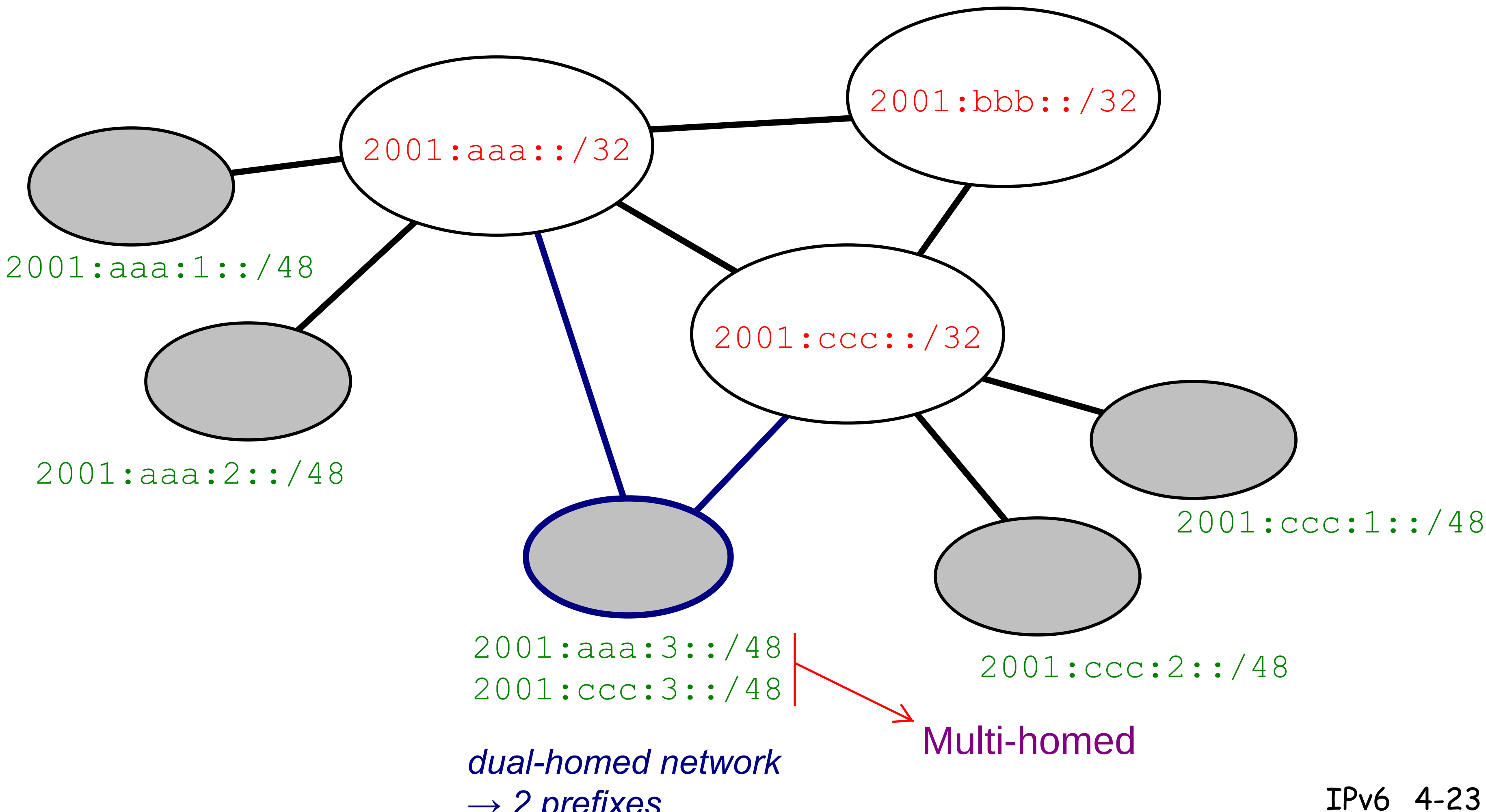
Provider Aggregatable (PA)

Allocation of IPv6 Addresses

- **Consequences of using PA addresses**
  - Better aggregation than with IPv4
    - Example: BELNET
      - with IPv4, announces several prefixes from its customers
      - with IPv6, announces a single prefix
    - Should lead to smaller global Internet routing tables
  - Provider change
    - if one network changes provider, it must re-number all its interfaces. Can be tricky and still an open research problem !
    - See for example `draft-ietf-6renum-enterprise-02.txt` (1/9/2012)
  - Multi-homed networks
    - one multi-homed network must receive a separate prefix from each of its providers and each interface will be assigned several addresses, one in each prefix.

Un préfixe agrégeable par provider

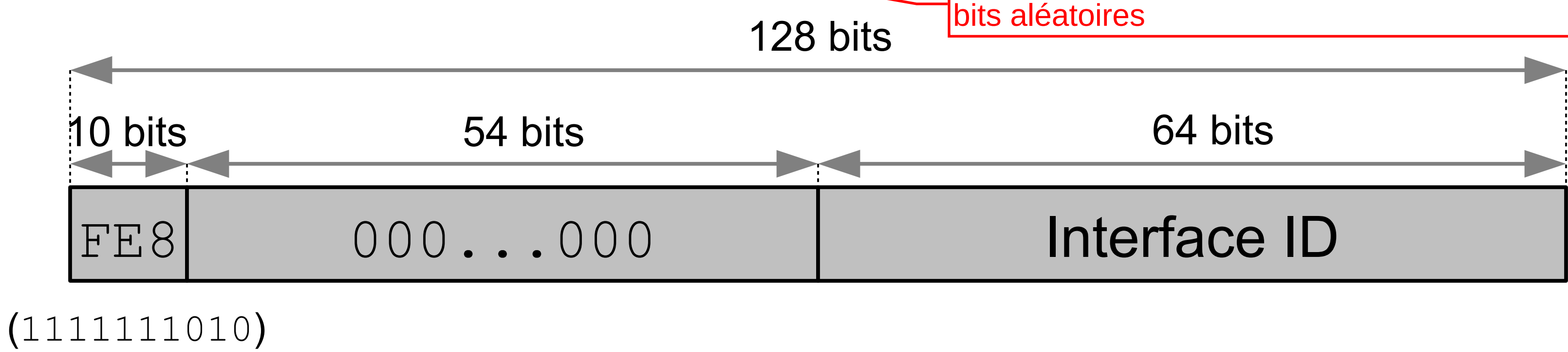
Allocation of IPv6 Addresses



Link-local IPv6 Addresses

- **Principle**
  - Used by hosts and routers attached to the same link/LAN to exchange IPv6 packets when they don't have/need globally routable addresses
  - Each host/router must generate one link local address for each of its interfaces → Each IPv6 host will use several IPv6 addresses
  - Similar to 169.254/16 addresses in IPv4

Quand DHCP ne donne pas d'adresse, 16 derniers bits aléatoires



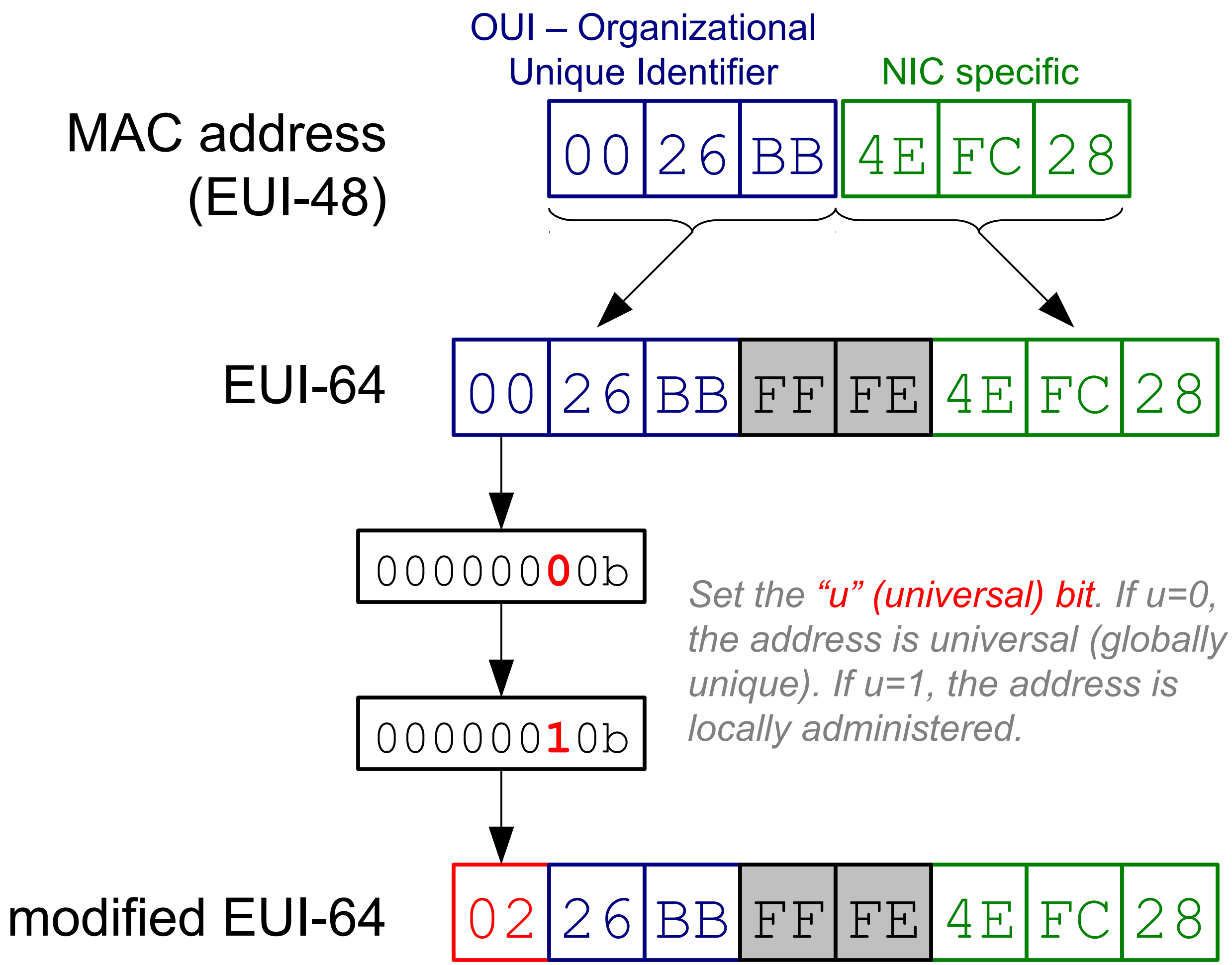
Link-local IPv6 Addresses

- **The modified EUI-64 format**
  - The *Extended Unique Identifier* (EUI) is an IEEE standard for link-layer addresses (e.g. Ethernet MAC addresses).
  - RFC2464 defines a scheme where the Interface ID of IPv6 addresses in the prefix range `001` to `111` (except for multicast) is derived from an EUI-64 address.
    - Other schemes exist, such as, for example CGA addresses (RFC3972) or IPv6 addresses in non-Ethernet networks such as IEEE 802.15.4 WPANs.
  - Example

```
bash-3.2$ ifconfig en0
en0: flags=8863<UP,BROADCAST,SMART,RUNNING,SIMPLEX,MULTICAST> mtu 1500
        inet6 fe80::226:bbff:fe4e:fc28%en0 prefixlen 64 scopeid 0x4
        inet 192.168.2.2 netmask 0xffffff00 broadcast 192.168.2.255
        ether 00:26:bb:4e:fc:28
        media: autoselect (100baseTX <full-duplex,flow-control>)
        status: active
```

Link-local IPv6 Addresses

- **The modified EUI-64 format**



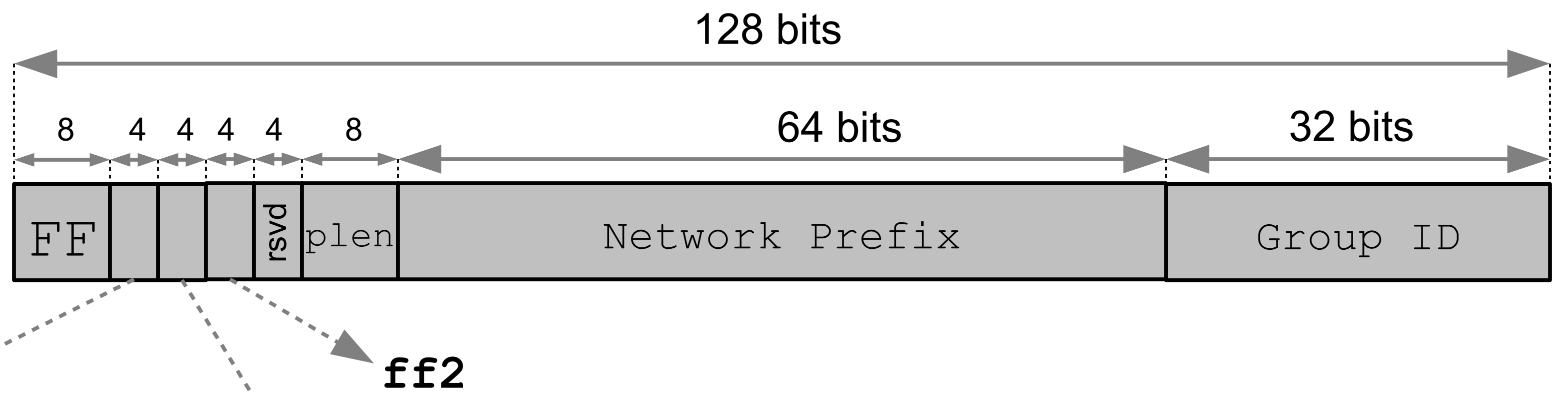
Similarités entre les deux adresses !
=> Algo permettant de dériver une adresse.

IPv6

- 4. 1 Motivations
- 4.2 IPv6 Addressing Architecture
  - 4.2.1 Unicast Addresses
  - 4.2.2 Multicast Addresses
  - 4.2.3 Anycast Addresses
- 4.3 IPv6 Packets
- 4.4 ICMPv6
- 4.5 DNS support for IPv6
- 4.6 Transition Mechanisms

Multicast IPv6 Addresses

- An IPv6 multicast address identifies a group of receivers (version RFC7371, sept. 2014)



ff1
(0RPT)
0: reserved (value=0)
R: 1=contains
rendez-vous point
T: 0=permanent
1=temporary
P: 1=assigned based
on prefix

scope
0, 3, F – reserved
1 – interface-local (a.k.a. node-local)
2 – link-local
4 – admin-local
5 – site-local
6,7 – unassigned
8 – organization-local
9, A, B, D, D – unassigned
E – global

Note: the boundaries of scopes other than interface, link and global are to be configured by network administrators !

ff1 : flag field 1
ff2 : flag field 2

Multicast IPv6 Addresses

Sert à identifier un ensemble d'utilisateur => tous les membres du groupes ciblé doivent recevoir le message

Unicast : 1 pers. => 1 pers.
Multicast : 1 pers. => groupe

host adress : unicast

group adress : multicast

- **Well-known groups**
  - Typically start with `FF0/12`
  - **Interface-local scope (loopback multicast)**
    - All-nodes address = `FF01::1`
    - All-routers address = `FF01::2`
  - **Link-local scope**
    - All-nodes address = `FF02::1`
    - All-routers address = `FF02::2`
    - Solicited-node address = `FF02::1:FF`*`xx:xxxx`*
      where *`xx:xxxx`* is formed by taking the less-significant 24 bits of an IPv6 address (more on this later)

Multicast Ethernet

- **Multicast Ethernet addresses**
  - When an IP datagram must be carried in a link-layer frame (e.g. an Ethernet frame), multicast MAC addresses could be used (if supported).
  - Ethernet supports multicast addresses. These are addresses where the least significant bit of the first byte (high order) is set to 1.
    - **00**-26-BB-4E-FC-28 is a unicast Ethernet address
    - **01**-80-C2-00-00-00 is a multicast Ethernet address
    - **FF**-FF-FF-FF-FF-FF is the broadcast Ethernet address
  - Any Ethernet controller that is registered in a multicast group should listen to frames sent to the corresponding multicast address in addition to its regular MAC address.
    - Modern Ethernet controller often provide support for multicast addresses.

IPv6 over Ethernet Multicast

- **Sending IPv6 multicast packets**
  - The **33-33-** Ethernet prefix is reserved for IPv6 multicast.
  - To send an IPv6 multicast packet over Ethernet, a node simply takes the last 32 bits of the destination IPv6 address, prepends `33-33-` and uses that as the destination Ethernet address.
  - Example
    - An IPv6 packet addressed to `FF02::1:FF4E:FC28` would be sent to the Ethernet address **33-33-**`FF-4E-FC-28`.

IPv6

- 4. 1 Motivations
- 4.2 IPv6 Addressing Architecture
  - 4.2.1 Unicast Addresses
  - 4.2.2 Multicast Addresses
  - 4.2.3 Anycast Addresses
- 4.3 IPv6 Packets
- 4.4 ICMPv6
- 4.5 DNS support for IPv6
- 4.6 Transition Mechanisms

Anycast IPv6 Addresses

Encodage similaire à unicast sauf slide suivant

- Definition
  - An IPv6 anycast address is an address that is assigned to more than one interface (typically belonging to different nodes), with the property that a packet sent to an anycast address is router to the "nearest" interface having that address, according to the routing protocols' measure of distance. This is called "*shared unicast address*"
- Usage
  - Multiple redundant servers using the same address
  - Example: DNS resolvers and DNS servers
- Representation
  - IPv6 anycast addresses are regular unicast addresses
  - Required subnet anycast address

Anycast IPv6 Addresses

- **Subnet-Router Anycast Address**
  - RFC4291
  - Subnet prefix (size n bits) + 128-n "0" for the interface part

```
|                         n bits                 |   128-n bits   |
+------------------------------------------------+----------------+
|                   subnet prefix                | 00000000000000 |
+------------------------------------------------+----------------+
```

  - A packet sent to this address will be delivered to one router on that subnet. All routers on a subnet must support the subnet-router anycast address.

Required IPv6 addresses

Pour chaque interface, on peut avoir énormément d'adresses

(pas toutes listées dans ifconfig)

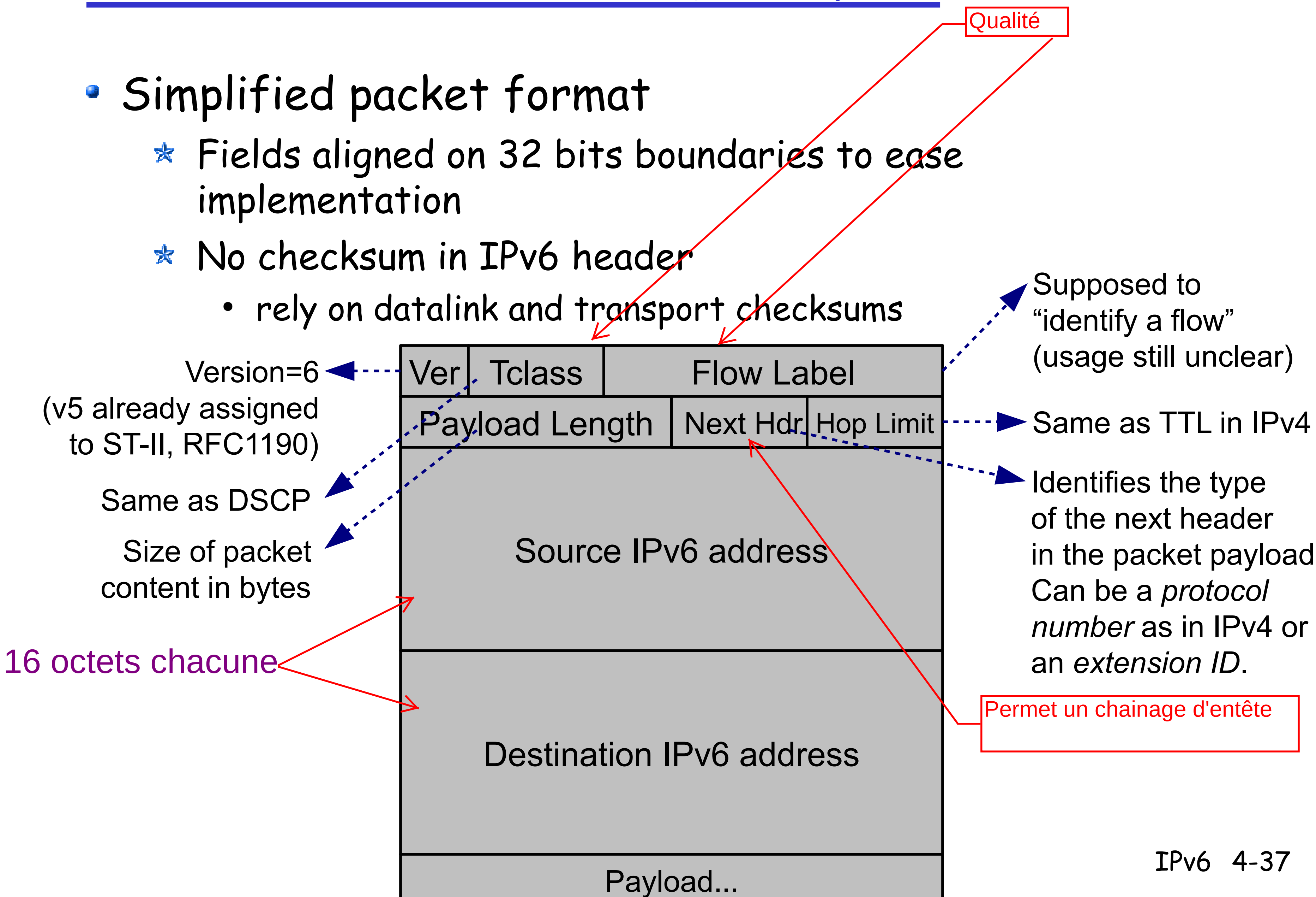
- **Summary**
  - Each **host** must consider the following addresses identify itself:
    - its link-local address for each interface i, `FE80::`$EUI_{64}(MAC_i)$
    - any assigned unicast and anycast addresses
    - the loopback address `::1`
    - the all-nodes multicast addresses `FF01::1`, `FF02::1`
    - solicited-node multicast address `FF02::1:FF`xx`:`$xxxx$
    - multicast addresses of groups to which the host belongs
  - Each **router**, in addition to the above addresses must support:
    - the all-routers multicast addresses `FF01::2`, `FF02::2`
    - multicast addresses of groups to which the router belongs
    - anycast addresses with which the router has been configured
    - subnet-router anycast addresses

IPv6

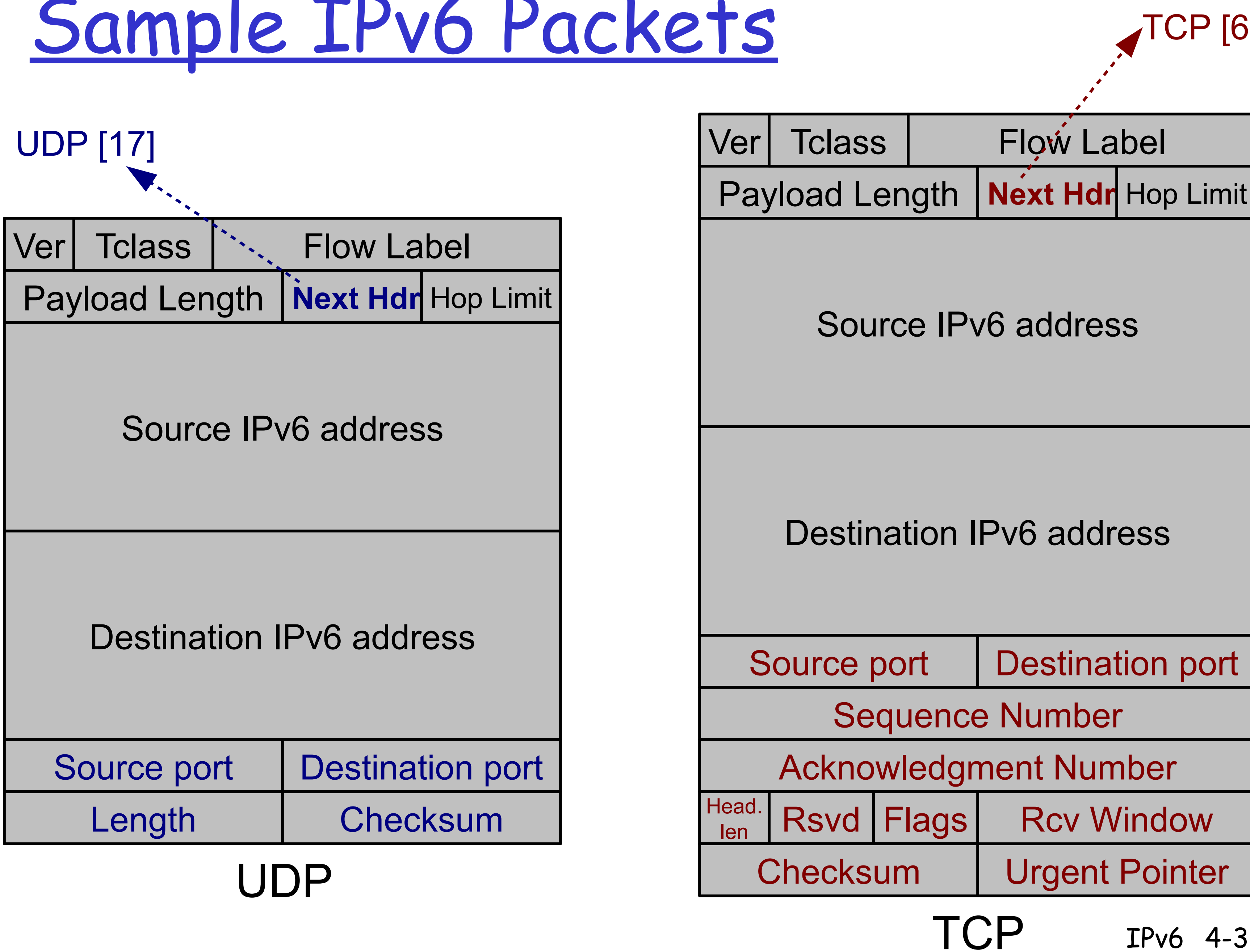
- 4. 1 Motivations
- 4.2 IPv6 Addressing Architecture
- 4.3 IPv6 Packets
  - 4.3.1 Header Format
  - 4.3.2 Extension Headers
- 4.4 ICMPv6
- 4.5 DNS support for IPv6
- 4.6 Transition Mechanisms

The IPv6 Packet Format

- Simplified packet format
  - Fields aligned on 32 bits boundaries to ease implementation
  - No checksum in IPv6 header
    - rely on datalink and transport checksums



Sample IPv6 Packets



IPv6

- 4. 1 Motivations
- 4.2 IPv6 Addressing Architecture
- 4.3 IPv6 Packets
  - 4.3.1 Header Format
  - 4.3.2 Extension Headers
- 4.4 ICMPv6
- 4.5 DNS support for IPv6
- 4.6 Transition Mechanisms

Source routing: la source décide de la route à emprunter

IPv6 Extension Headers

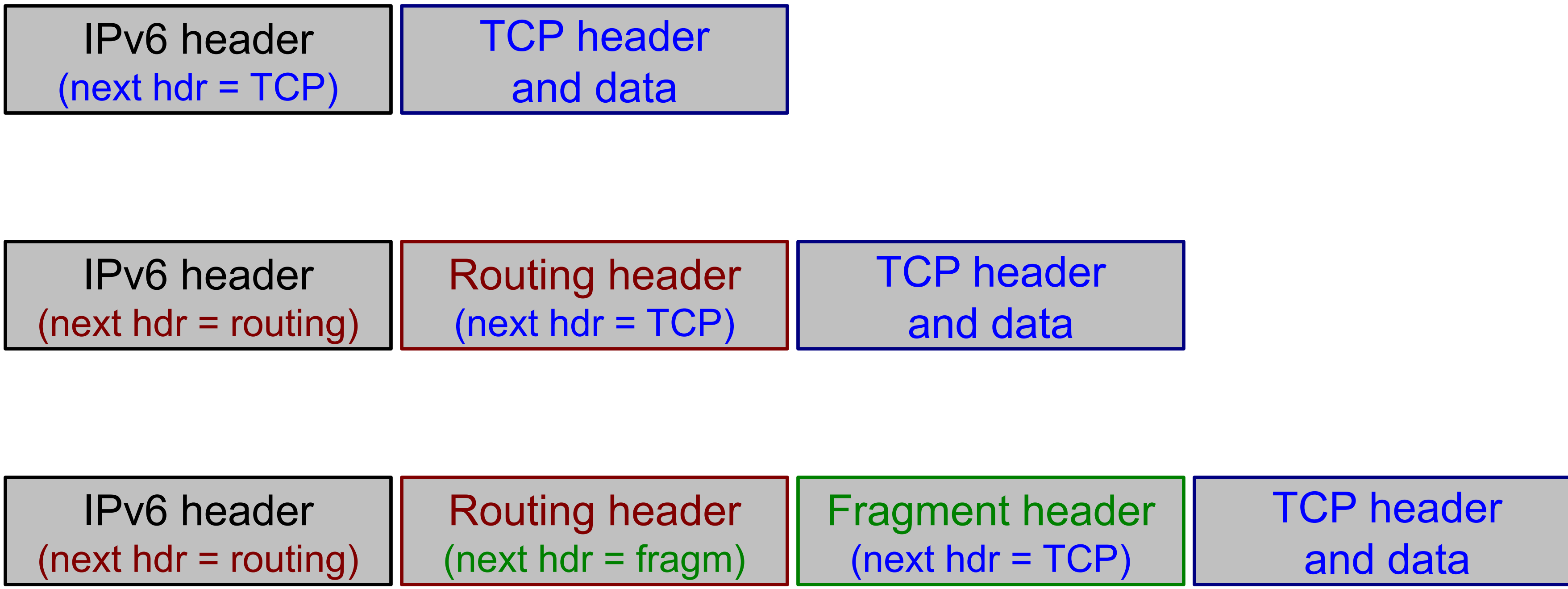
- Several types of extension headers (RFC2460)
  - Hop-by-hop Options [ID=0]
    - contains information to be processed by each hop
  - Routing header (type 0 and type 2) [ID=43]
    - contains information affecting intermediate routers
  - Fragmentation header [ID=44]
    - used for fragmentation and reassembly
  - Destination Options header [ID=60]
    - contains options only relevant to destination
  - Authentication header [ID=51]
    - for IPSec

Vérifier l'identité d'un ordinateur
(être sur que je parle à la bonne personne)

  - Encrypted Security Payload (ESP) header [ID=50]
    - for IPSec
- Each header must be encoded as a multiple of 64 bits (8 bytes)

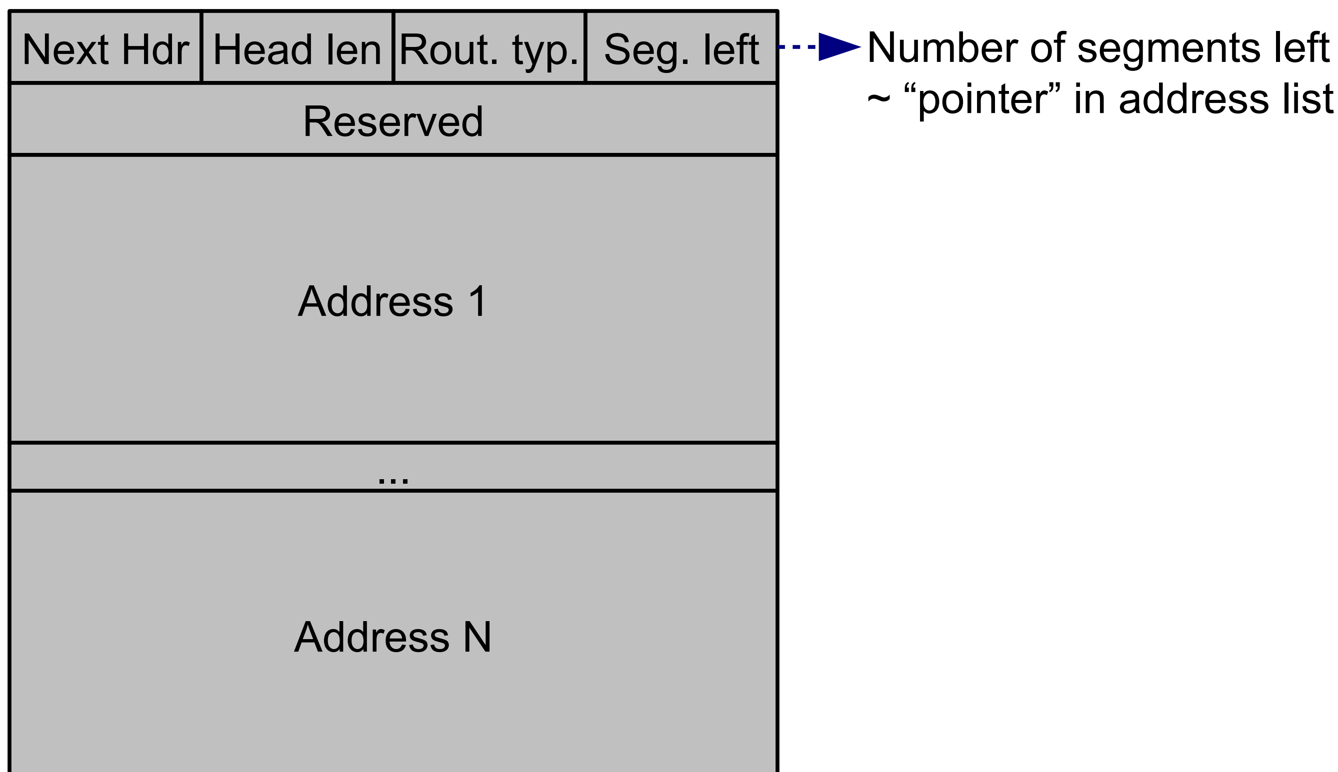
IPv6 Extension Headers

- Extension headers can be chained together



Type 0 Routing header

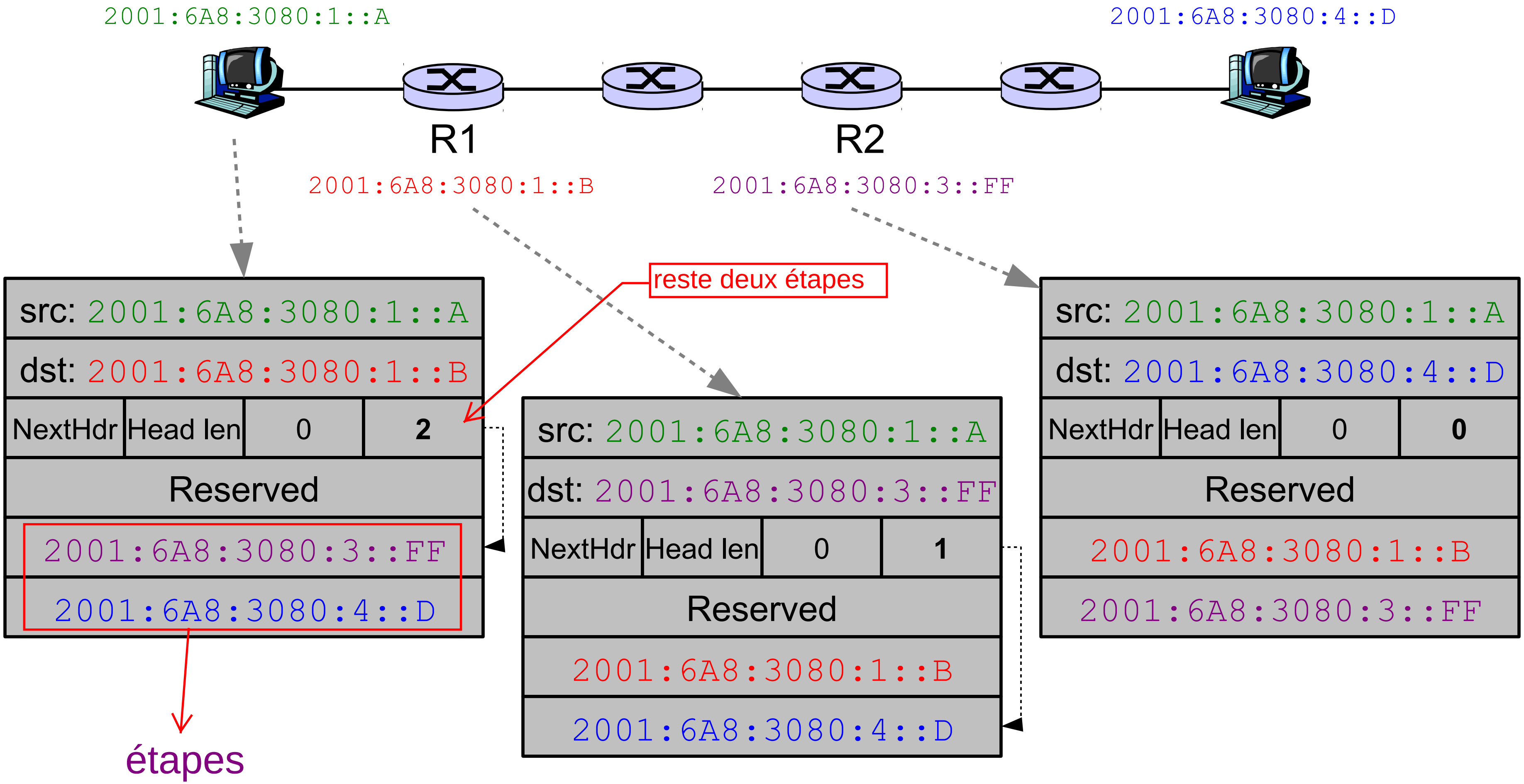
- Defines "*a mean for a source to list one or more intermediate nodes to be visited on the way to a packet's destination*"
  - similar to loose source routing in IPv4



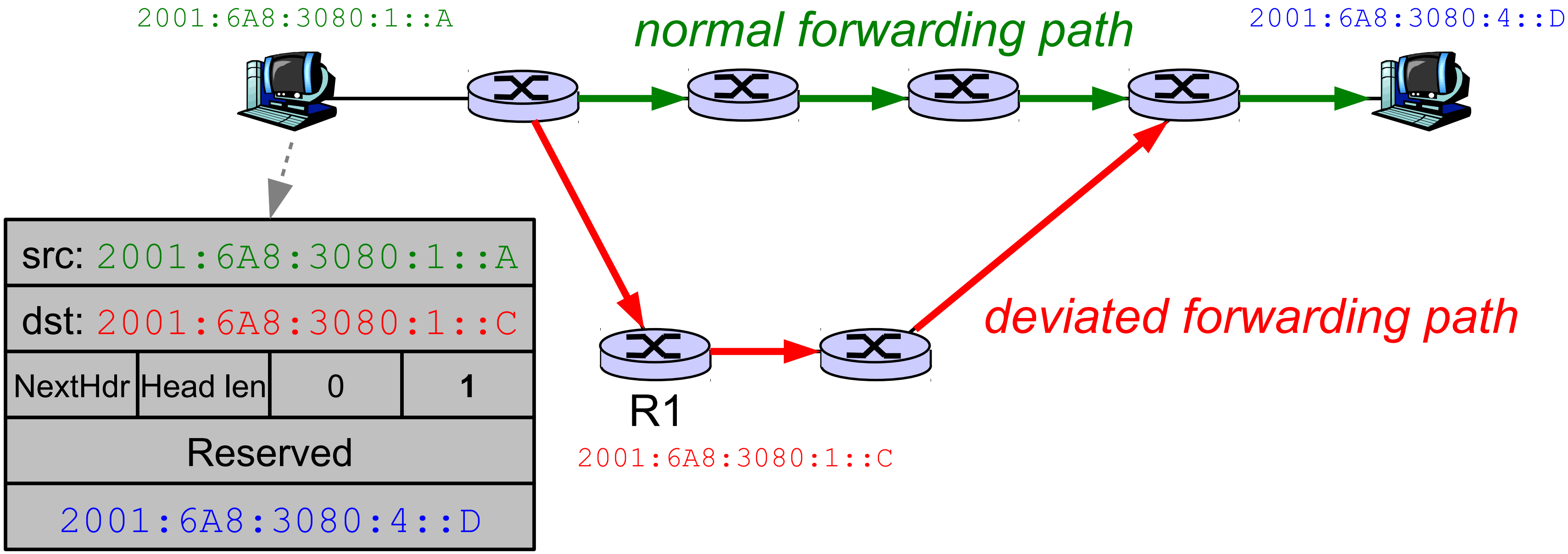
Type 0 Routing header

=> Afin d'avoir un contrôle plus fin de la topologie

=> Système prévu pour pouvoir dump les adresses "étapes"

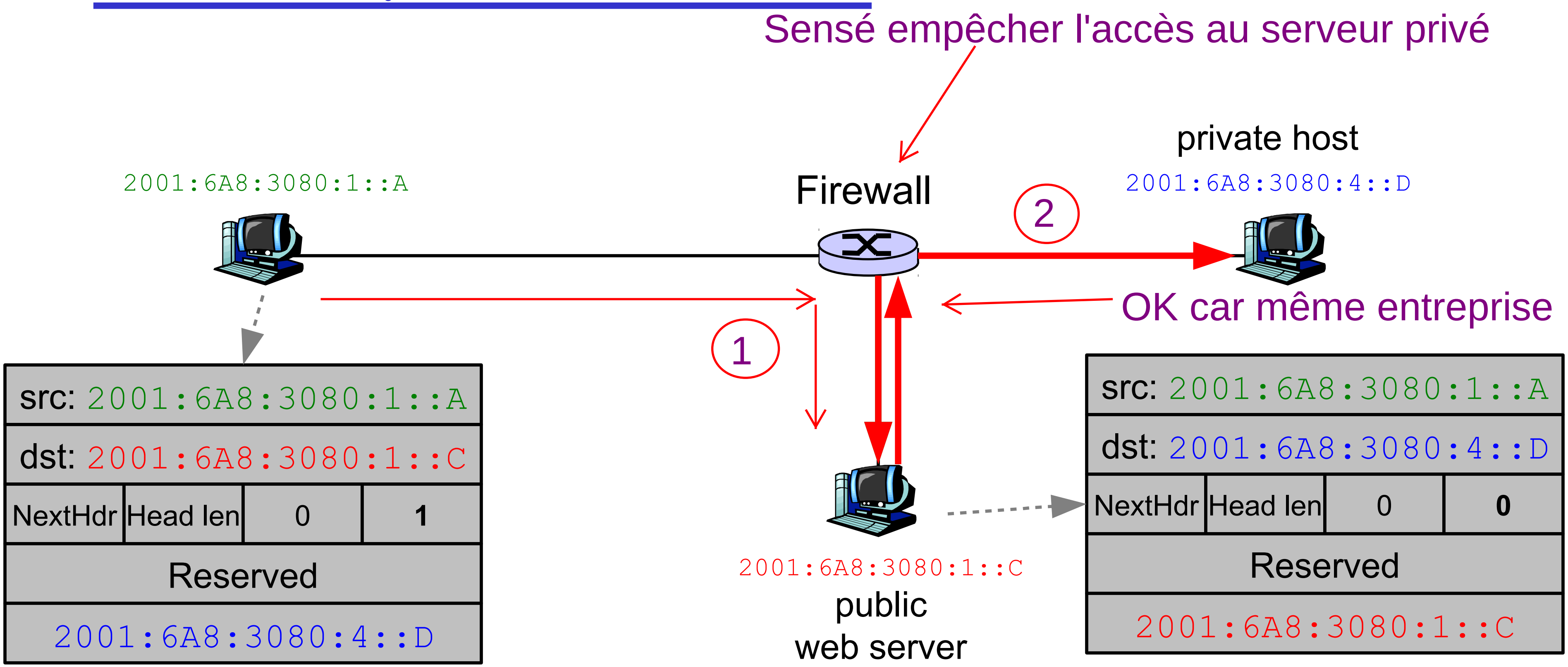


Type 0 Routing header



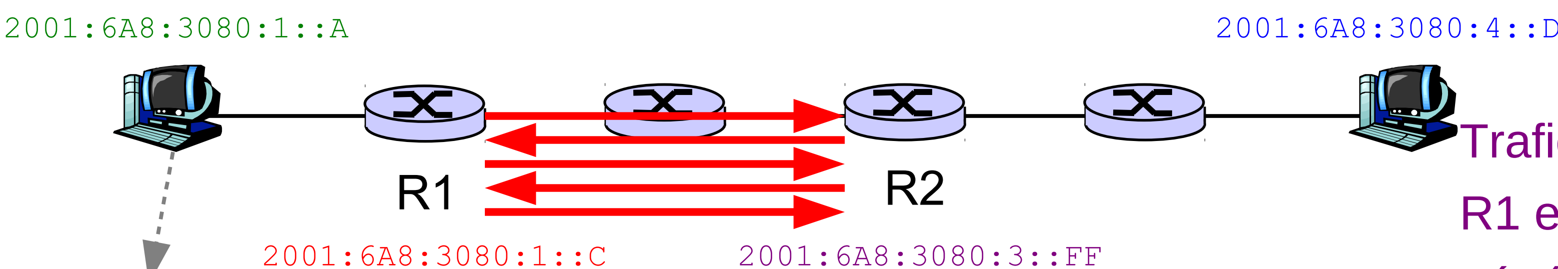
- The IPv6 specification is unclear: "*IPv6 nodes must accept and attempt to process extension headers in any order and occurring any number of times in the same packet, . . .*" => N'importe quel noeud peut être traversé pour atteindre le but final
- what are IPv6 nodes ? routers ? end-hosts ?

Problems with RH0



- The IPv6 specification is unclear: "*IPv6 nodes must accept and attempt to process extension headers in any order and occurring any number of times in the same packet, . . .*"
- In practice, a lot of end-host OS support it.

Amplification Attack using RH0



Trafic entre R1 et R2 généré par le paquet

src: 2001:6A8:3080:1::A			
dst: 2001:6A8:3080:1::C			
NextHdr	Head len	0	**73**
Reserved			
2001:6A8:3080:3::FF			
2001:6A8:3080:1::C			
2001:6A8:3080:3::FF			
2001:6A8:3080:1::C			
2001:6A8:3080:3::FF			
2001:6A8:3080:1::C			
2001:6A8:3080:3::FF			

77 : nombre d'adresses possible dans le datagramme pour l'attaque

Vitesse du lien

- A single packet can generate tens of packets between two routers/hosts
  - every IPv6 implem. must support at least 1280 bytes datagrams
  - (1280-40-8)/16=~77
  - 10Mbit/s → 770 Mbit/s

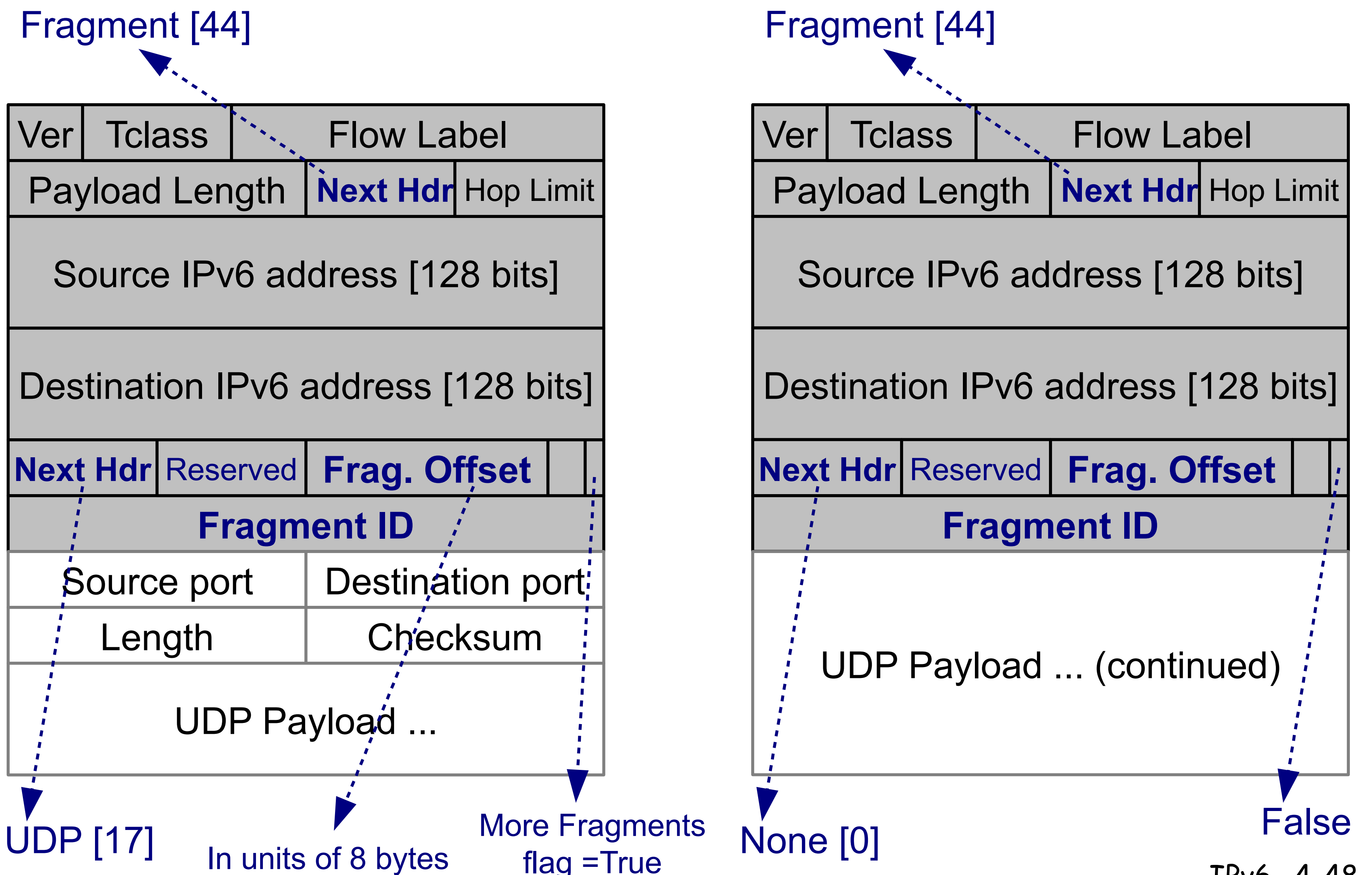
Packet Fragmentation

- **IPv4 supported packet fragmentation on routers**
  - All hosts must be able to handle packets that are at least 576 bytes (minimum MTU for IPv4)
  - Experience has shown that fragmentation is costly for routers and difficult to implement in hardware
  - PathMTU discovery is now widely implemented

- **IPv6**
  - Minimum MTU of 1280 bytes required
    - Otherwise, link-specific fragmentation and reassembly must be provided (IPv6 should not be aware of this)
  - Routers do not perform fragmentation
    - Only end hosts perform fragmentation and reassembly by using the fragment extension header
    - But PathMTU discovery should avoid fragmentation most of the time

Revient à l'hôte => à lui à le fragmenter

Packet Fragmentation



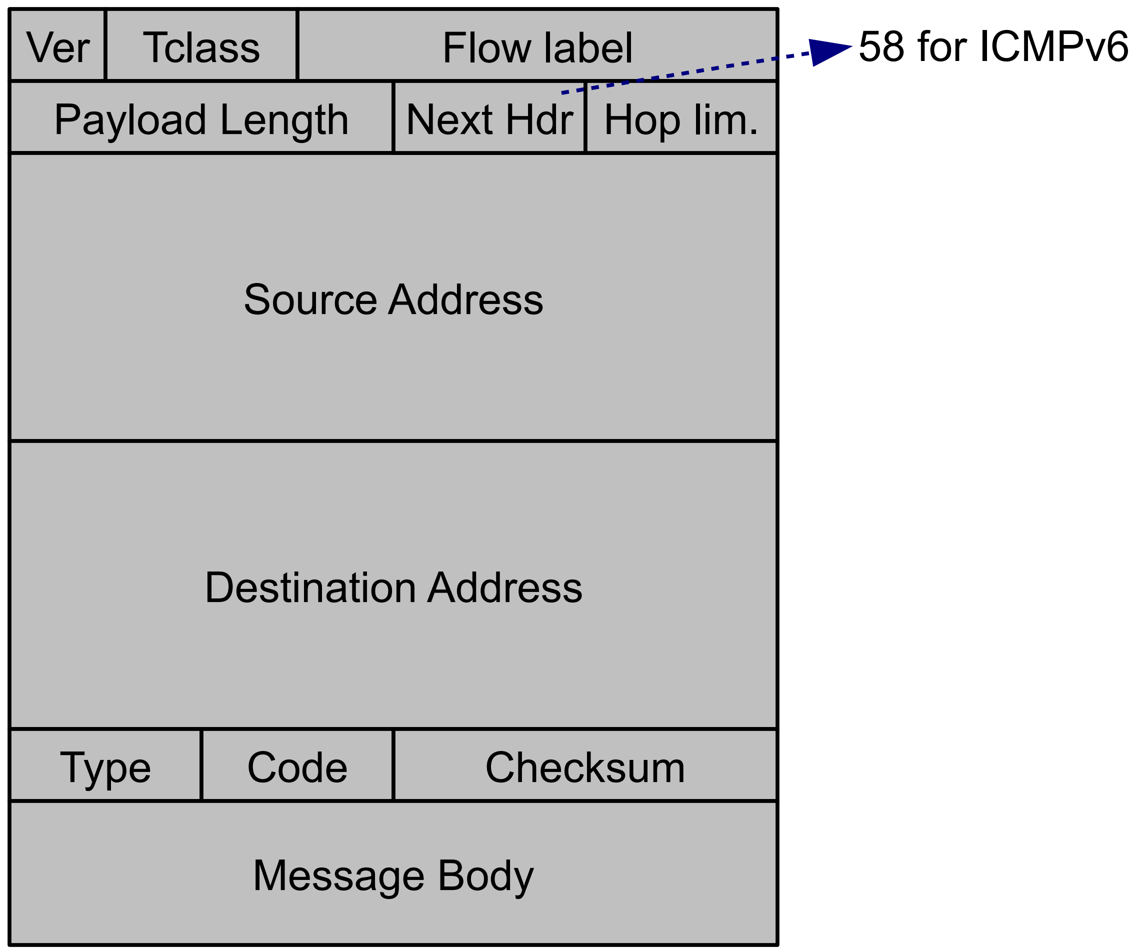
IPv6

- 4. 1 Motivations
- 4.2 IPv6 Addressing Architecture
- 4.3 IPv6 Packets
- 4.4 ICMPv6
  - 4.4.1 Introduction and Packet Format
  - 4.4.2 Auto-configuration
  - 4.4.3 Security
- 4.5 DNS support for IPv6
- 4.6 Transition Mechanisms

ICMPv6

- Provides the same functions as ICMPv4, IGMP and ARP
- Types of ICMPv6 messages
  - Error: Destination unreachable [type=1]
  - Error: Packet too big [type=2]
    - used for PathMTU Discovery
  - Error: Time Exceeded (Hop limit exhausted) [type=3]
    - traceroute v6
  - Info: Echo request and echo reply [types=128,129]
    - ping v6
  - Info: Multicast group membership [types=130..132]
    - equivalent to IPv4's IGMP
  - Auto-configuration, Router advertisements, Neighbor discovery

ICMPv6 Packet Format

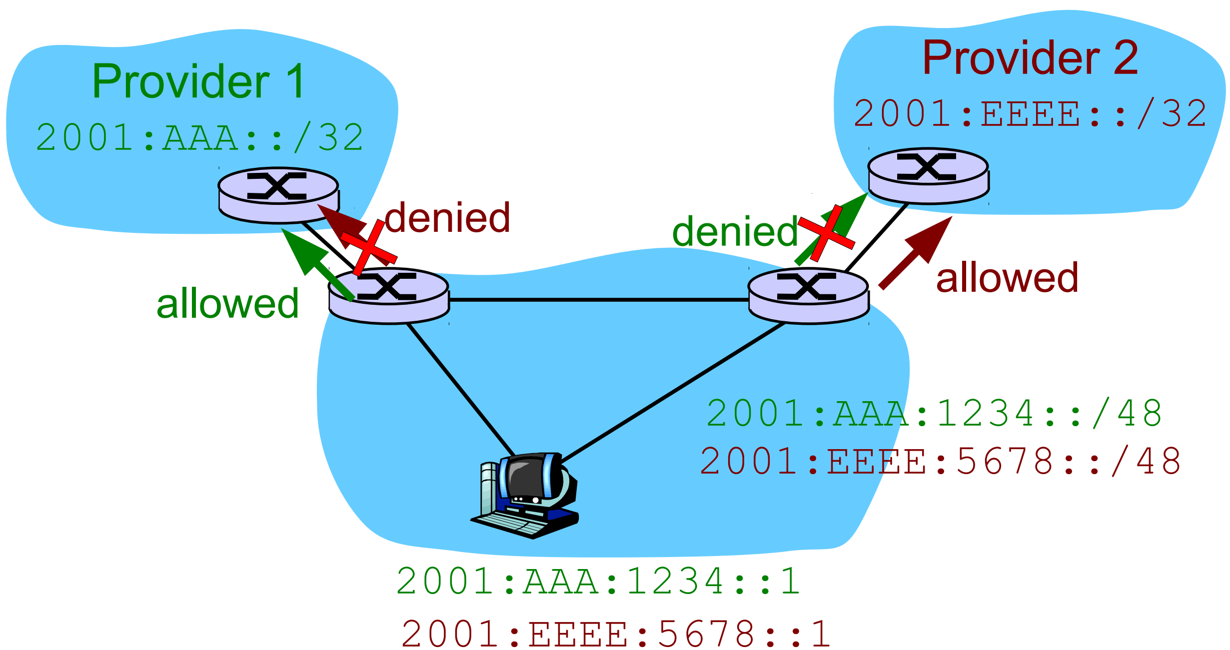


ICMPv6 Destination unreachable

- Destination Unreachable [type=1]
  - no route to destination [code=0]
    - no route for destination in forwarding table
  - communication with destination administratively prohibited [code=1]
    - typically sent by a firewall upon a "reject" action
  - beyond scope of source address [code=2]
  - address unreachable [code=3]
    - typically IPv6 address unknown on destination LAN
  - port unreachable [code=4]
    - transport-layer port not listening
  - source address failed ingress/egress policy [code=5]
    - see next slide :-)
  - reject route to destination [code=6]

Ingress and Egress Policies

- For security reasons, a provider should only accept packets from sources belonging to allocated prefixes.
  - Prevents IP spoofing
  - Typically implemented using *Reverse Path Forwarding* (RPF) checks in IPv4.



IPv6

- 4. 1 Motivations
- 4.2 IPv6 Addressing Architecture
- 4.3 IPv6 Packets
- 4.4 ICMPv6
  - 4.4.1 Introduction and Packet Format
  - 4.4.2 Auto-configuration
  - 4.4.3 Security
- 4.5 DNS support for IPv6
- 4.6 Transition Mechanisms

Autoconfiguration

- **Introduction**
  - IPv6 provides support for *StateLess Address Auto-Configuration* (SLAAC)
  - Based on ICMPv6 messages
  - Components of SLAAC
    - Neighbor Discovery (ND): similar to ARP in IPv4
    - Duplicate Address Detection (DAD)
    - Router Discovery
    - Link parameters and prefixes discovery

ICMPv6 Neighbor Discovery

- Replacement for IPv4's ARP

Question

- Neighbor Solicitation [type=135]
  - usually sent to solicited-node multicast address `FF02::1:FFxx:xxxx`

Type=135	Code=0	Checksum
Reserved		
Target IPv6 Address		

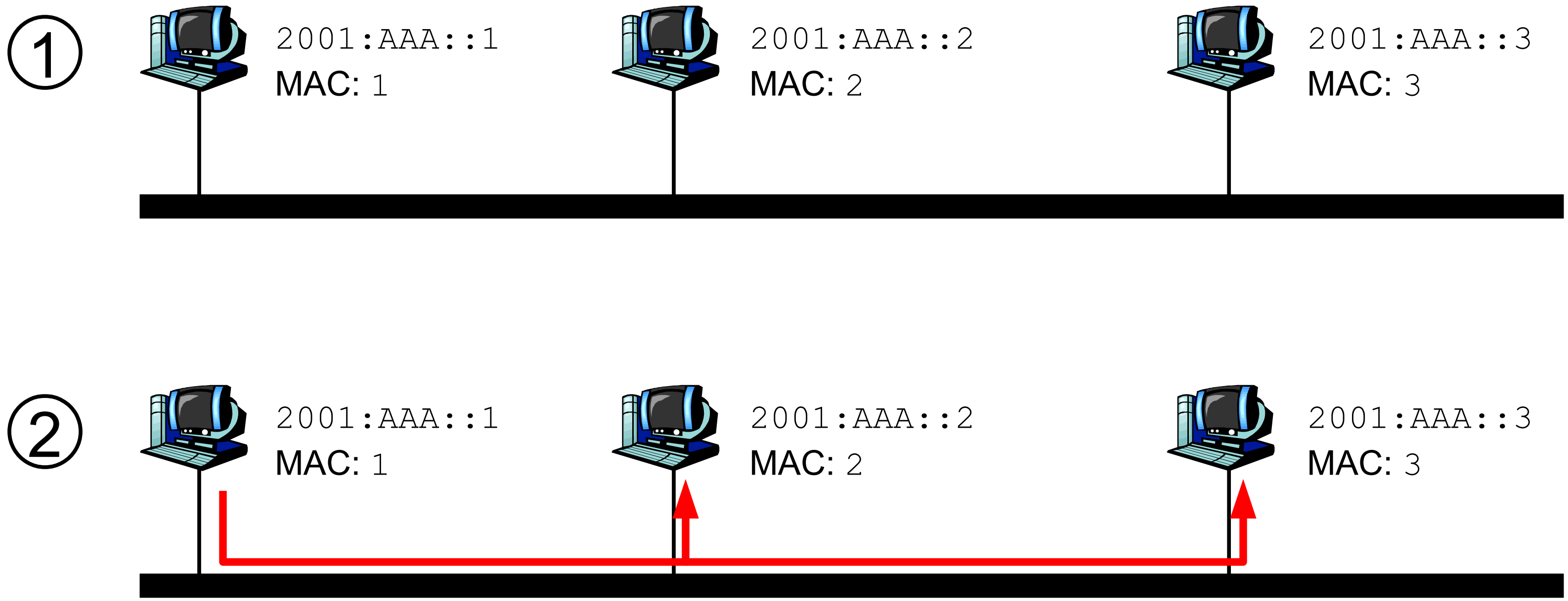
Réponse

- Neighbor Advertisement [type=136]
  - sent to requesting node (if source address of solicitation is not the unspecified address ::)
  - sent to all-nodes multicast address (if src of neighbor solicitation was ::)

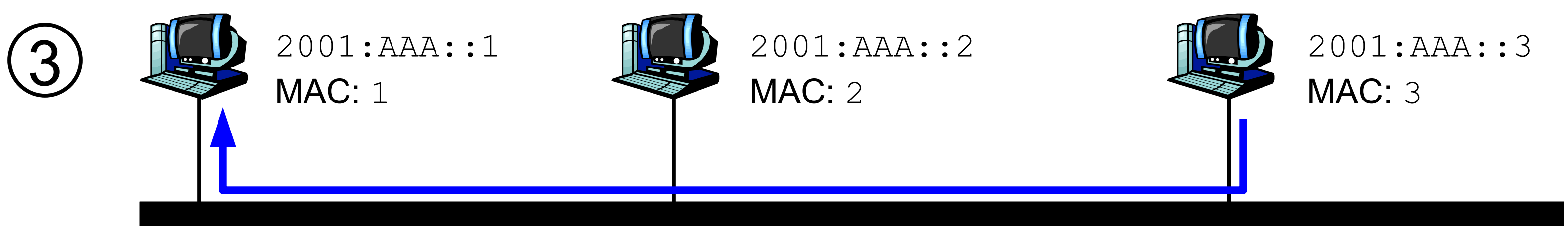
Type=136	Code=0	Checksum
Flags	Reserved	
Target IPv6 Address		
Target Link Layer Address		

R: Router
S: Solicited
O: Override

IPv6 over Ethernet



Neighbor Solicitation: `2001:AAA::3` sent to multicast address `FF02::1:FF00:3`

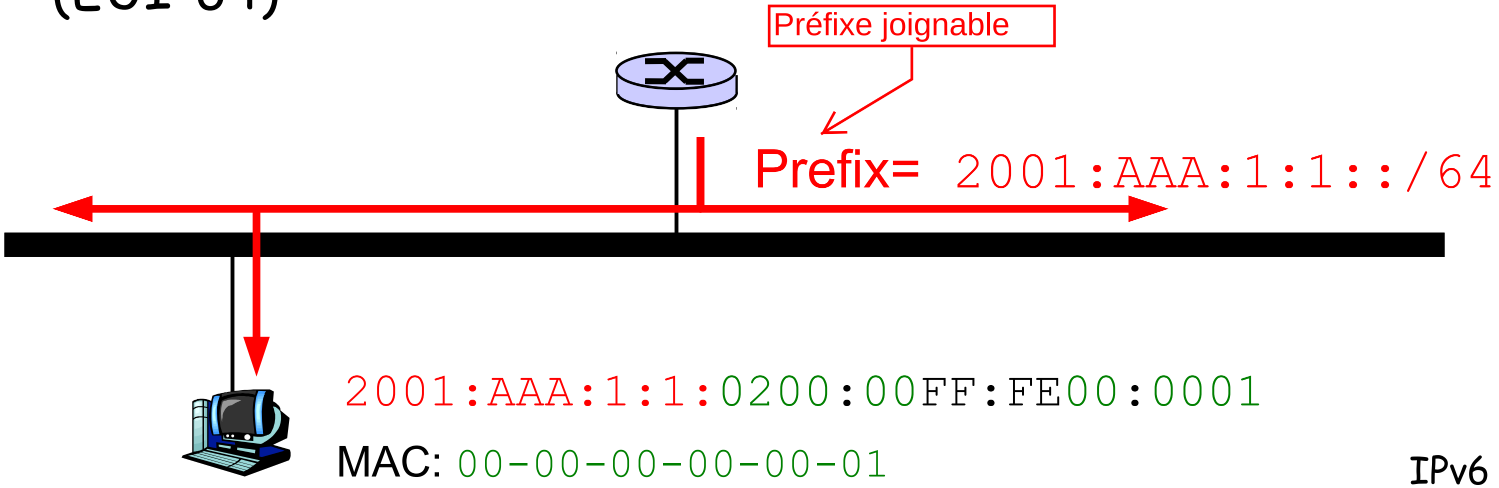


Neighbor Advertisement: (`2001:AAA::3`, `3`) sent to `2001:AAA::1`

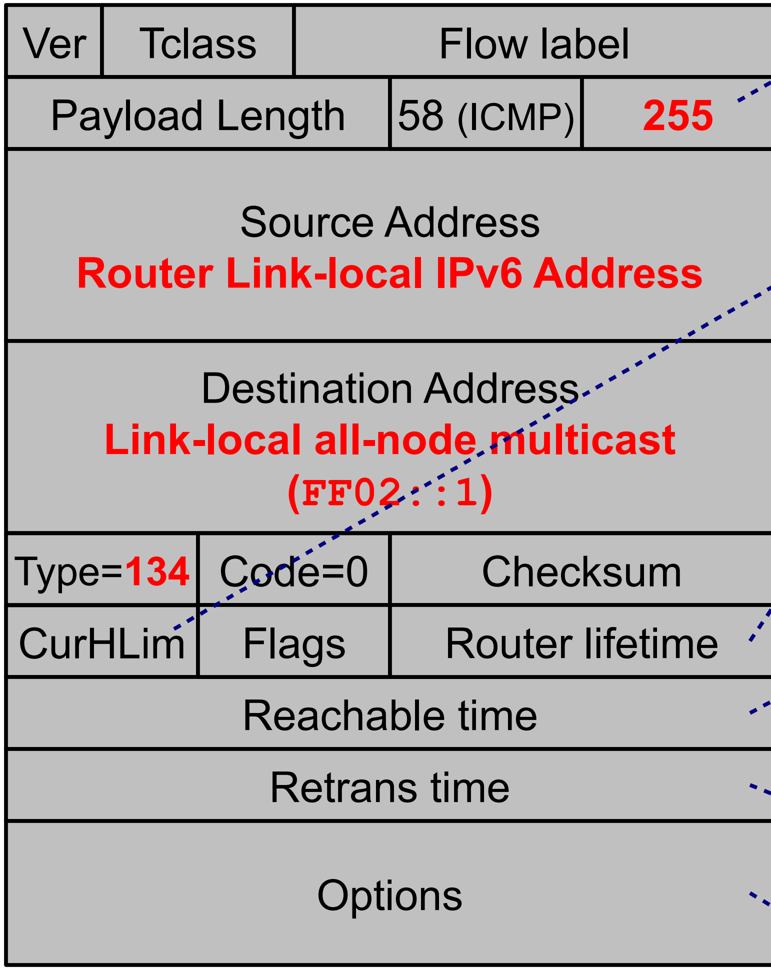
IPv6 Autoconfiguration

Si on connaît une IPv6 locale, on peut se demander l'adresse globale correspondante

- How can a node obtain its IPv6 address ?
  - Manual configuration
  - From a server by using DHCPv6 as in IPv4
- Automatically
  - Router advertises prefix on LAN by sending ICMPv6 messages to "all IPv6 hosts" multicast address (`FF02::1`)
  - Hosts build their address by concatenating the prefix with their MAC address converted in 64 bits format (EUI-64)



Router Advertisements



Maximum hop limit to avoid spoofed packets from outside of LAN

Value of hop limit to be used by hosts when they send IPv6 packets

The lifetime associated with the default router in seconds. If the router is not a default router, lifetime = 0.

The time (in ms) that a node can assume a neighbor is reachable after having received a reachability confirmation (see *Neighbor Unreachability Detection* algorithm, NUD).

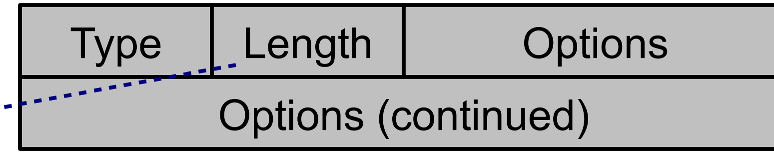
The time (in ms) between retransmitted *Neighbor Solicitation* messages.

Prefix information
MTU to be used on the LAN

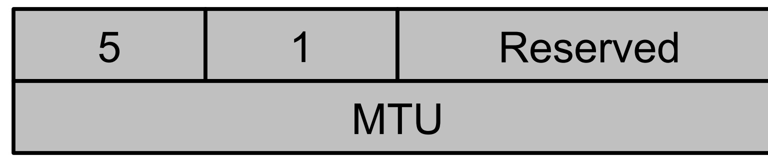
Router Advertisement Options

- General Option format

Length in units of 8 bytes



- MTU Option

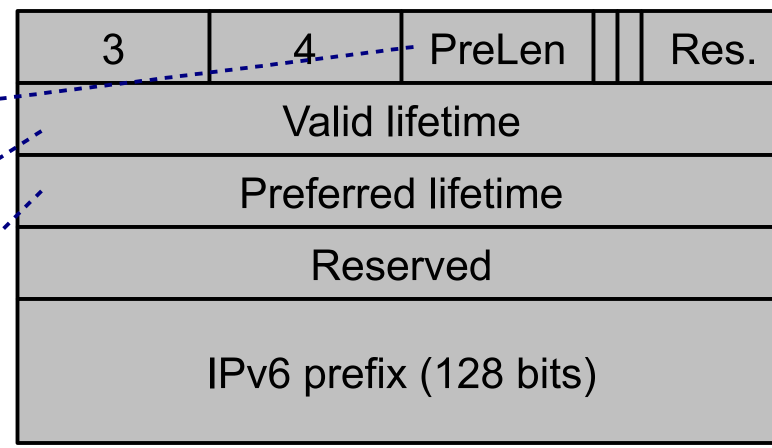


- Prefix option

Number of bits in IPv6 prefix that identify subnet

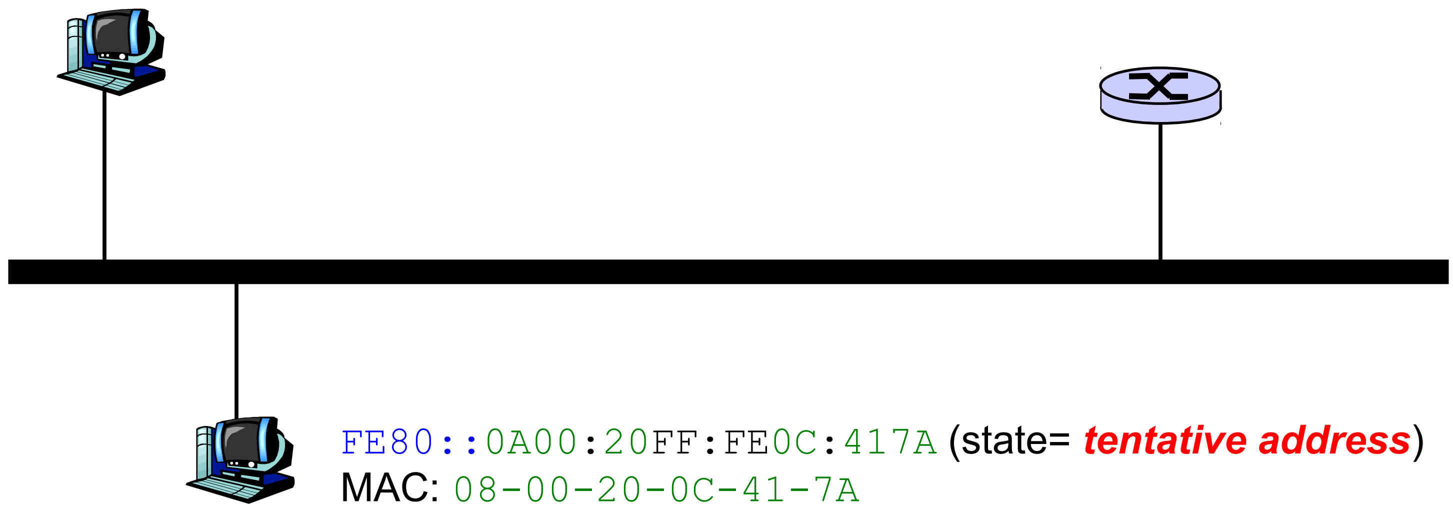
The validity period of the prefix (in seconds)

The duration (in seconds) that addresses generated from the prefix via stateless address autoconfiguration remain preferred



IPv6 Stateless Autoconfiguration (1)

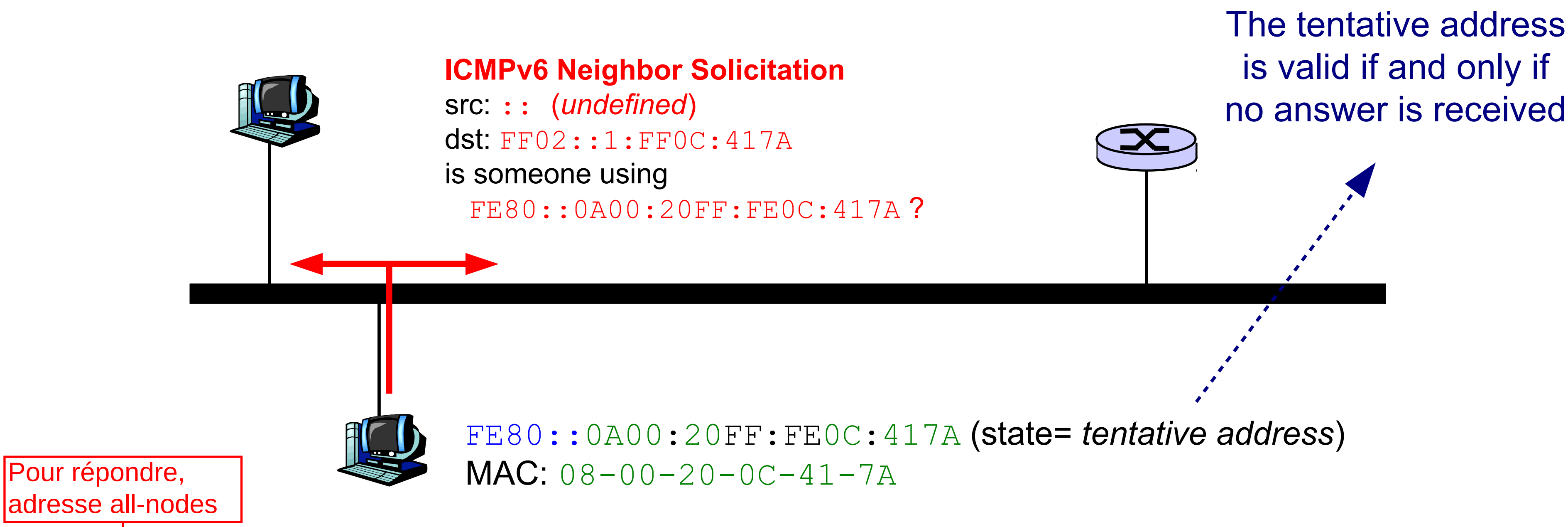
- What happens when an end-system boots ?
  - It knows nothing about its current network
    - but needs an IPv6 address to send ICMPv6 messages



  - Use Link-local IPv6 address (FE80::/64)
    - Each host, when it boots, has a link-local IPv6 address
    - But another node might have chosen the same address !
      - Ethernet cards with same MAC address or manually configured

IPv6 Stateless Autoconfiguration (2)

- ***Duplicate Address Detection*** **(DAD)**
  - Send a Neighbor solicitation message to the tentative address's solicited-node multicast address.



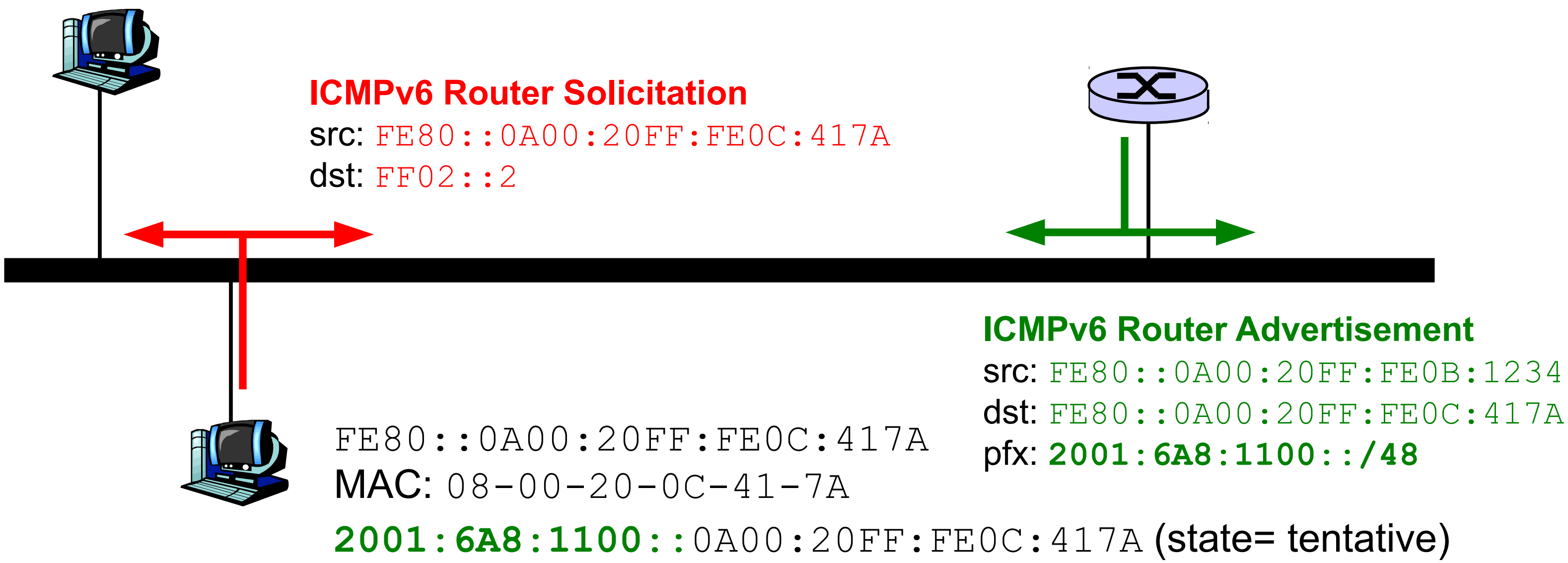
  - Before sending the Neighbor Solicitation, the node must register on the *all-node multicast* address (`FF02::1`) and the *solicited-node multicast* address (`FF02::1:FFxx:xxxx`) for the tentative address

IPv6 Stateless Autoconfiguration (3)

- **DAD Algorithm**
  1. Node X is going to assign address A on interface I
  2. Interface I first joins the following multicast groups:
     - `FF02::1` (all-nodes link-local)
     - `FF02::1:FF`*xx*:*xxxx* (solicited-node)
  3. If X receives a *Neighbor Solicitation* for address A (on the solicited node address), then another node is performing DAD for address A. STOP
  4. X sends a *Neighbor Solicitation* for address A
     - to the corresponding solicited-node address and with the undefined source address
  5. If X receives a *Neighbor Advertisement* for A (on the all-nodes address), then another node has selected address A. STOP
  6. Address A is not in use.

IPv6 Stateless Autoconfiguration (4)

- How to obtain the IPv6 prefix of the subnet ?
  - Wait for Router Advertisements (e.g. 30 seconds)
  - Solicit Router Advertisement



  - Need to perform DAD for newly created address(es)

Privacy Issues with IPv6 Autoconfiguration

- **Issue**
  - Autoconfigured IPv6 addresses contain the MAC address of the hosts
    - MAC addresses are "fix and unique"
    - A laptop/user could be identified by tracking the lower 64 bits of its IPv6 addresses
- **How to maintain privacy with IPv6 ?**
  - Use DHCPv6 and configure server to never reallocate the same IPv6 address
  - Allow hosts to use random host IDs in lower 64 bits of their IPv6 addresses
    - algorithms have been implemented to generate such random hosts IDs on nodes with and without stable storage

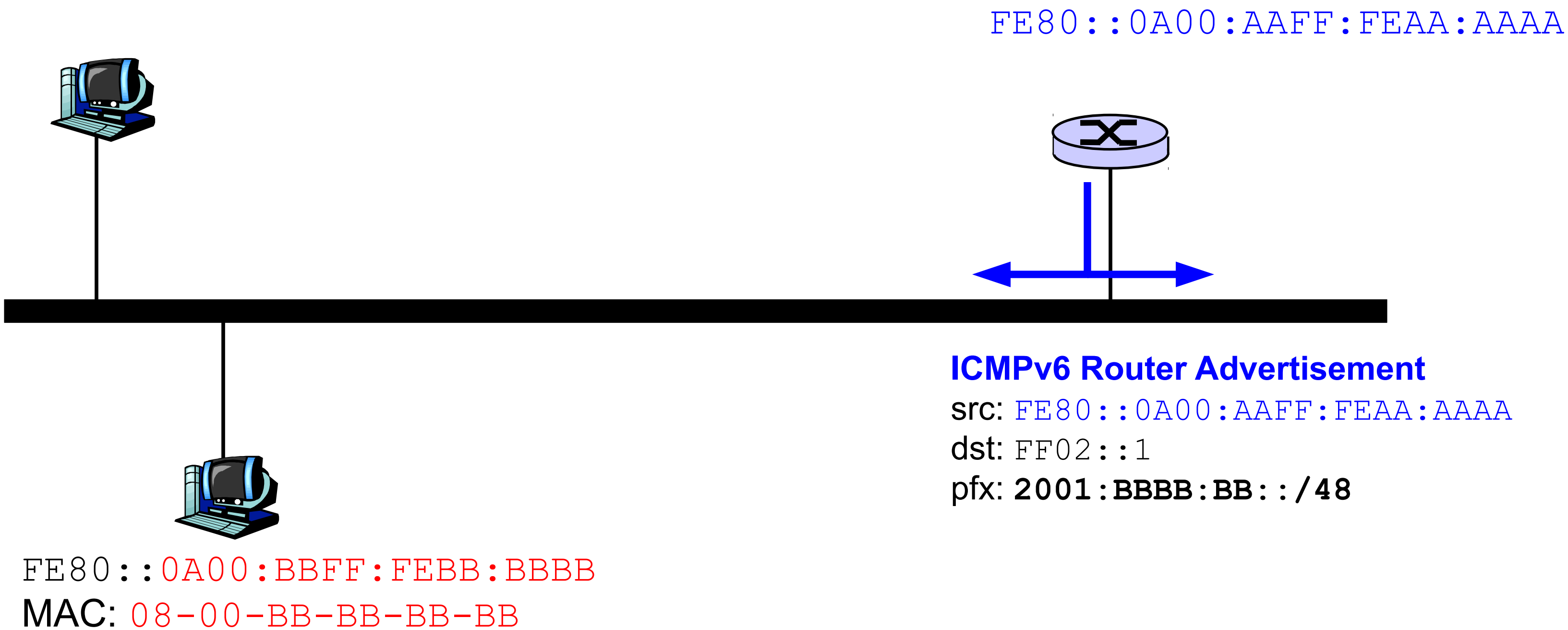
IPv6

- 4. 1 Motivations
- 4.2 IPv6 Addressing Architecture
- 4.3 IPv6 Packets
- 4.4 ICMPv6
  - 4.4.1 Introduction and Packet Format
  - 4.4.2 Auto-configuration
  - 4.4.3 Security
- 4.5 DNS support for IPv6
- 4.6 Transition Mechanisms

Security Risks

- What happens if an attacker sends **fake router advertisements** on LAN ?

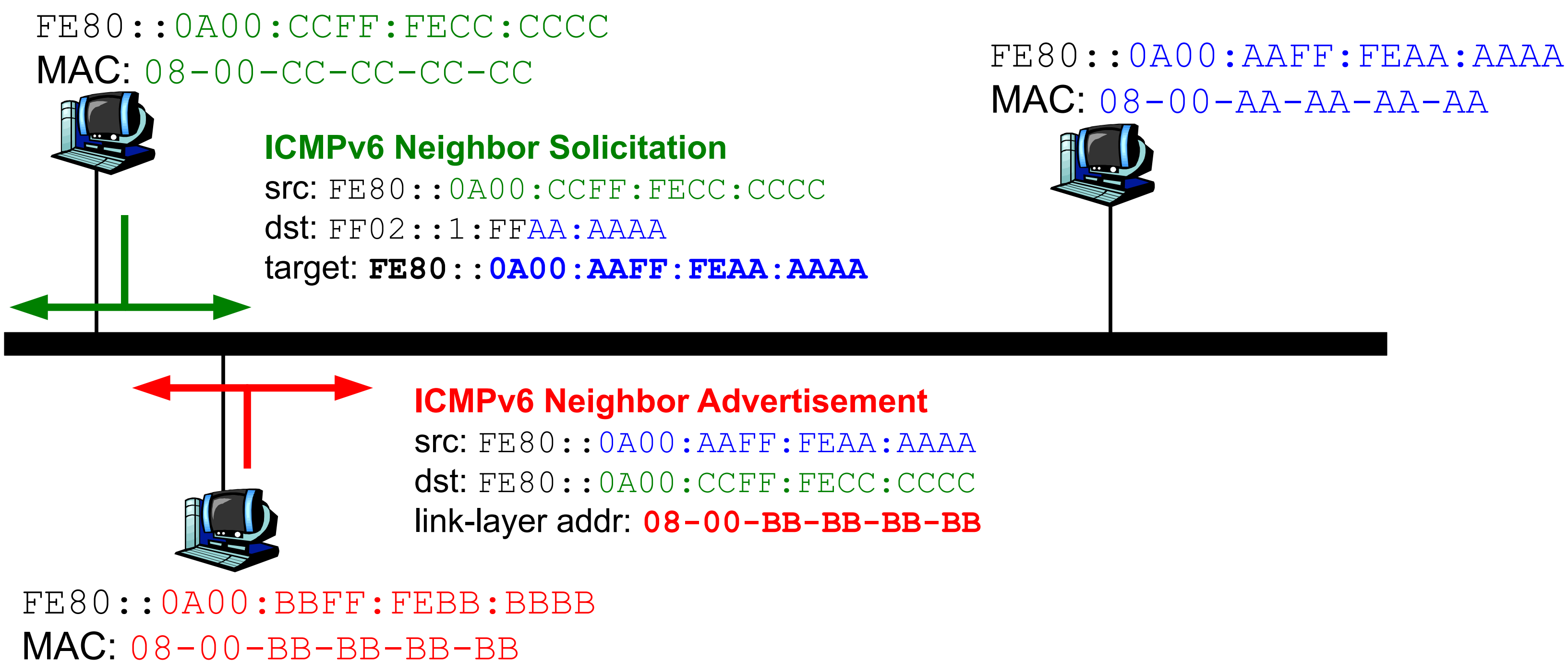
Man in the middle



Solution : Crypter l'adresse (SEND)

Security Risks

- What happens if an attacker sends **fake neighbor advertisements** on LAN ?



Securing ICMPv6

Pas vu

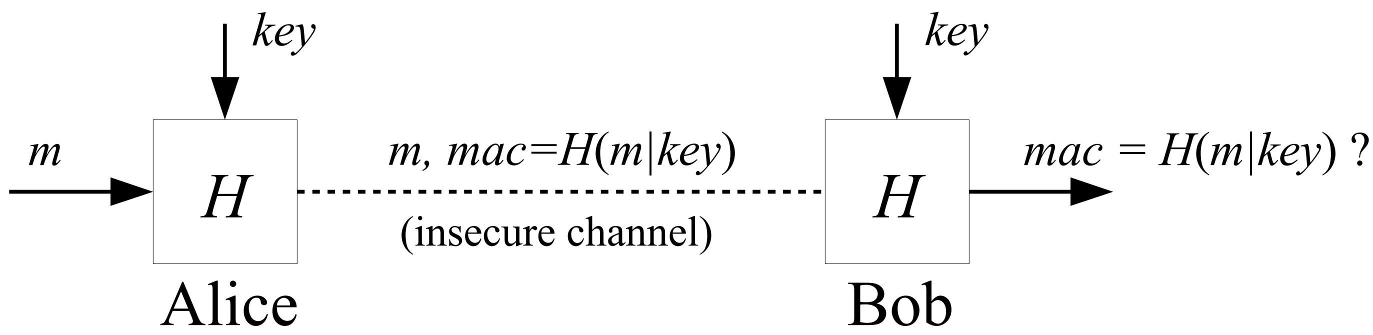
- **Principle of the solution**
  - Need to secure *Router Advertisements* and *Neighbor Advertisements*
    - A host that replies to an ICMPv6 *Neighbor Solicitation* should be able to prove that it owns the corresponding IPv6 address
    - A router that sends ICMPv6 *Router Advertisements* should be able to prove that it is authorized to serve as a router **and** that is authorized to announce the advertised prefixes

- **Issues**
  - How to exchange these proofs and authorizations ?
  - Is IPSec a solution ?

Cryptographical building blocks

Pas vu

- **Hash functions**



- Properties
  - Easy to compute $H(\mathrm{m})$
  - Very difficult to invert, i.e. find m_2 such that

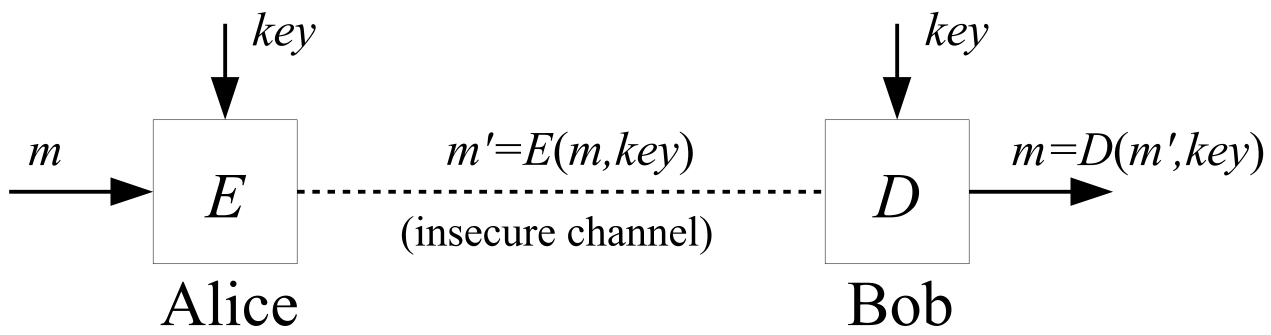
    $H(\mathrm{m}) = H(m_2)$
  - Used to provide *Message Authentication Codes* (MAC)

- Example hash functions
  - MD5, MD4, SHA-1

Cryptographical building blocks

Pas vu

- **Secret-key Cryptography**

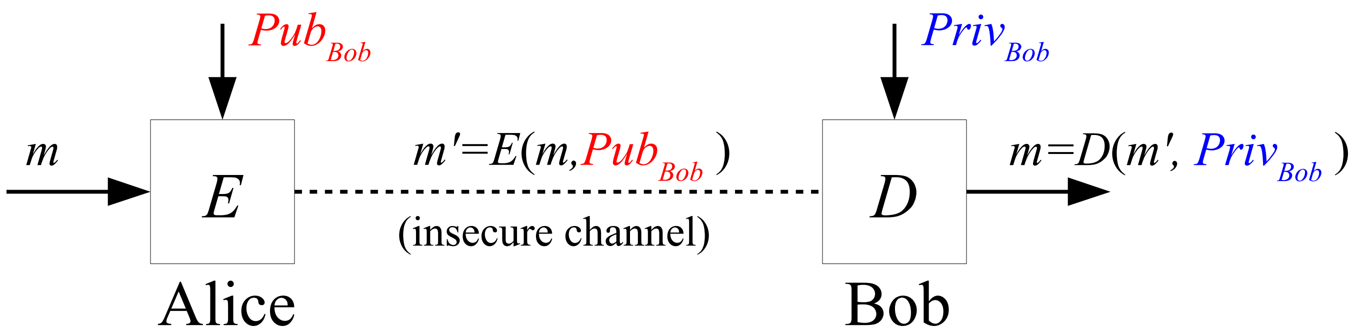


- Advantages
  - Efficient algorithms exist
  - Security is function of implementation and key size
- Drawbacks
  - Key must be distributed securely
  - Does not provide any authentication scheme
- Examples
  - DES, AES, RC-4, IDEA, ...

Cryptographical building blocks

Pas vu

- **Public-key Cryptography**



- Each user maintains two keys
  - A public key ($Public_{Key}$) which can be made public and can be used by any user to send him/her encrypted messages
  - A private key ($Private_{Key}$) which is kept secret and can be used to decrypt information encrypted with the public key.

Cryptographical building blocks

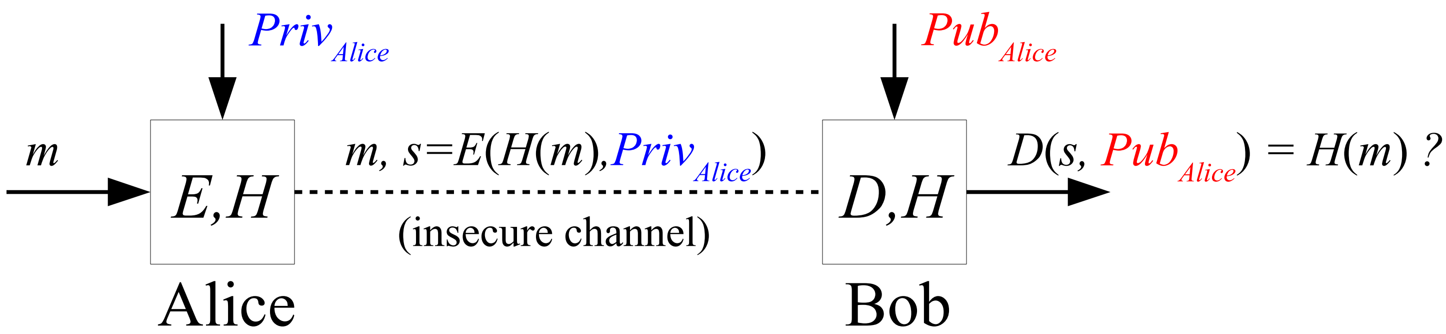
Pas vu

- **Public-key Cryptography**
  - Advantages
    - Users do not need to share a secret key to be able to encrypt messages
    - Public-key cryptography allows signatures
    - Security is function of implementation and key size
    - Can be used to sign messages (using private key)
  - Drawbacks
    - Public-key cryptography is 10 or 100 times slower than secret-key cryptography
  - Examples
    - RSA, DSS

Cryptographical building blocks

Pas vu

- **Digital Signature**



- Property of public-key cryptography
  - public-key and private-key can be exchanged in the encryption and decryption processes. This still works!
  - Basis for digital signatures
- Note
  - Digital signature only proves that message was originated by owner of private key used for signature. Not sufficient for authentication.

First Solution: Certificates

Pas vu

- **Principle**
  - Each router has a public/private key pair
  - A certificate is generated for each router to confirm
    - that the key pair belongs to the router
    - that the owner of the key pair is a valid router
  - Certificates must be anchored on an authority that is trusted by both routers and hosts
  - ICMPv6 router advertisement messages are signed by the router

- **Protocol issues**
  - Need to extend ICMPv6 to support signatures and certificates

Cryptographically Generated Addresses (CGA)

Pas vu

- **Observations**
  - Placing certificates on all hosts is too difficult
  - We usually don't need to prove that a host is a host

Can we verify the validity of signed messages without relying on a PKI ?

- **Principle of the solution**
  - Assume that IPv6 addresses are variable-length and unlimited length
  - Generate IPv6 addresses as follows

Global prefix + subnet ID	Host's public Key

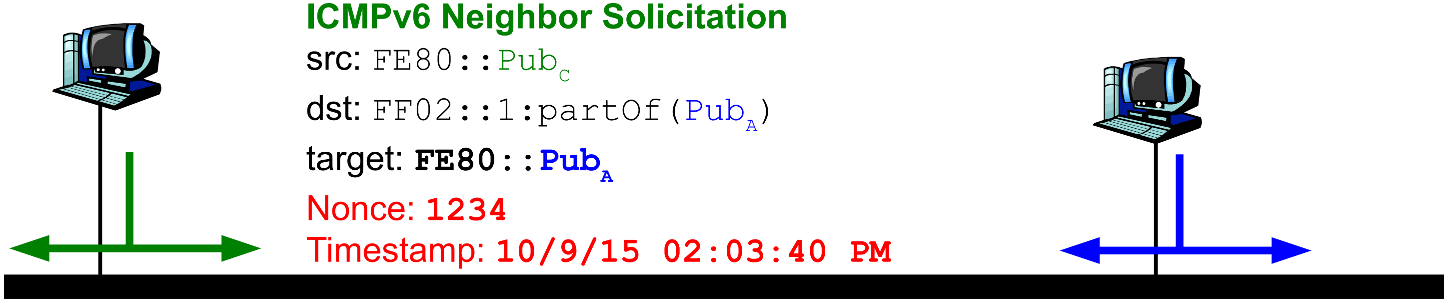
  - Use private key to sign ICMPv6 neighbor advertisement messages

Principles of Secure Neighbor Discovery

Pas vu

FE80::Pub_C
Public key: Pub_C
MAC: 08-00-CC-CC-CC-CC

FE80::Pub_A
Public key: Pub_A
MAC: 08-00-AA-AA-AA-AA



ICMPv6 Neighbor Solicitation
src: FE80::Pub_C
dst: FF02::1:partOf(Pub_A)
target: **FE80::Pub_A**
Nonce: **1234**
Timestamp: **10/9/15 02:03:40 PM**

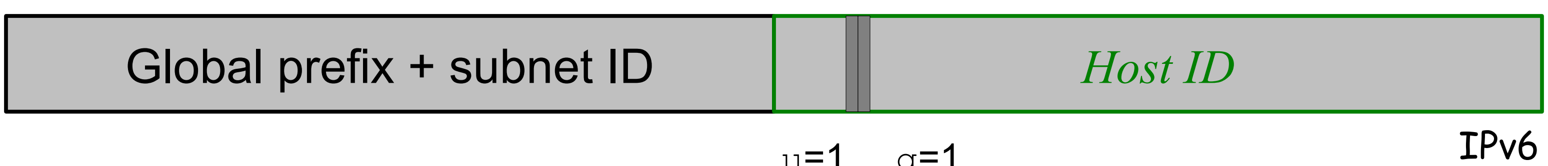
ICMPv6 Neighbor Advertisement
src: FE80::Pub_A
dst: FE80::Pub_C
target: **FE80::Pub_A**
link addr: **08-00-AA-AA-AA-AA**
Nonce: **1234**
CGA Parameter: **Pub_A**
Timestamp:
Signature: signed with **$Priv_A$**

Cryptographically Generated Addresses (CGA)

Pas vu

- **IPv6 addresses have a fixed size**
  - The Host ID is 64 bits and 2 bits (`u`,`g`) are reserved in (MEUI-64) → only 62 bits remain.
  - A 62 bits RSA public-key is not secure
    - NIST recommends > 1024 bits

- **Solution**
  - To secure a binding between a MAC address and an IPv6 address, each host
    - generates its (Pub_{Key}, $Priv_{Key}$) key pair
    - uses a special $HostId$ = $Hash_{64}(Pub_{Key})$, ignore (`u`,`g`) bits
    - signs its Neighbor Advertisements by using its $Priv_{Key}$



Cryptographically Generated Addresses (CGA)

Pas vu

- **Simplified version**

1). **host A** picks $(Pub_A, Priv_A)$
address' $HostId_A = Hash_{64}(Pub_A)$

2). later, **host B** sends *Neighbor Solicitation* (NS) for address $Prefix{:}HostID_A$

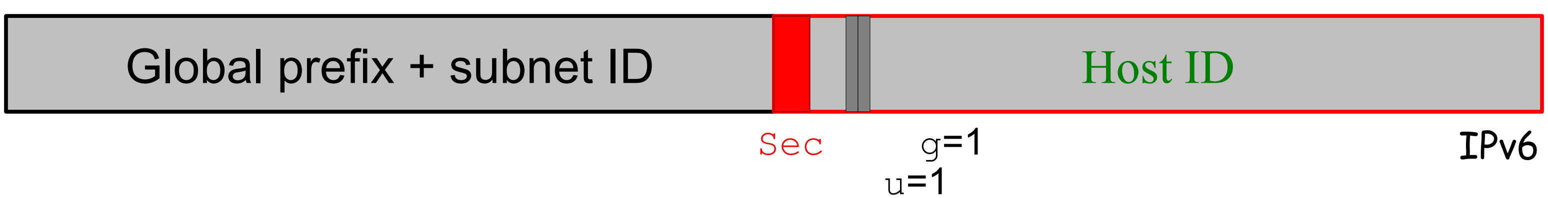
3). **host A** answers with *Neighbor Advertisement* (NA), signed with
$s = E(H(\mathrm{NA}), Priv_A)$
In addition, it provides the public key Pub_A and its link-layer address

4). **host B** checks that
a). $Hash_{64}(Pub_A) = HostID_A$
b). $D(s, Pub_A) = H(\mathrm{NA})$

Cryptographically Generated Addresses (CGA)

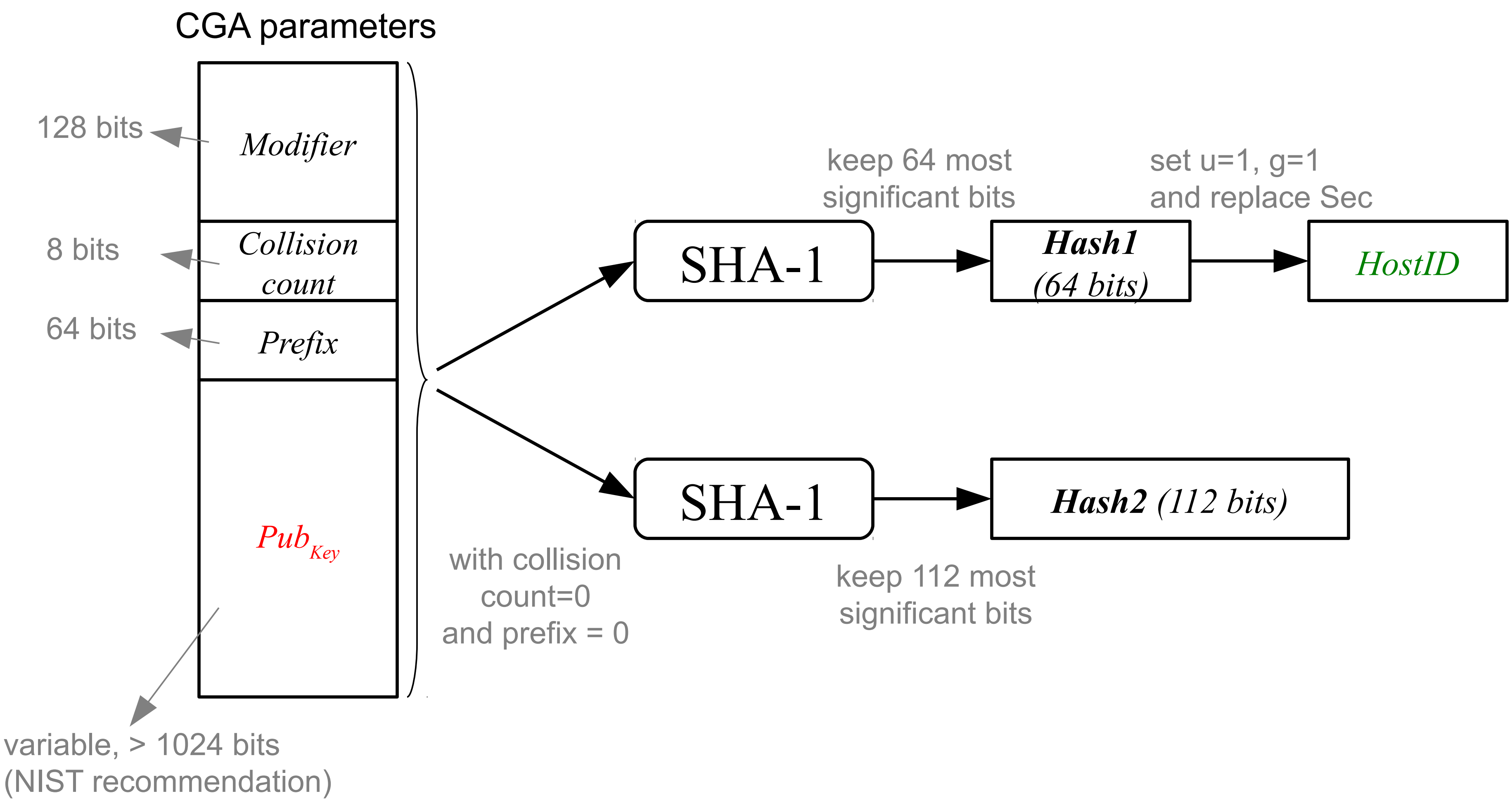
Pas vu

- **Issue with CGA**
  - A 62 bits hash is not very secure
    - an attacker could use brute-force to find a public-key whose hash is equal to a given value (dictionary attack)
- **Improving CGA security beyond 62 bits (RFC3972)**
  - Objective: Increase the difficulty for an attacker of computing the Host Id.
  - Basic idea: compute a large hash value and transmit only a part of this hash value, the remaining part being known (0).
    - $HostId = Low_{64}(Hash_{80}(Modifier \mid Pub_{Key}))$ and such that $High_{16}(Hash_{80}(Modifier \mid Pub_{Key}))=0$
    - Random $Modifier$ value generated iteratively
    - Security level (Sec) encoded in Host Id



Cryptographically Generated Addresses (CGA)

Pas vu



CGA Generation

Pas vu

- **Algorithm (RFC3972)**
  1. Pick a random *modifier*
  2. Set the *collision count* to 0
  3. Hash the concatenation of CGA parameters with *collision count* and *prefix* set to 0

     $$Hash2 = Left_{112}(\text{ SHA-1}(\ modifier \mid \text{coll. count} \mid \text{prefix} \mid Pub_{Key}\ )\ )$$
  4. Compare the $16{*}Sec$ leftmost bits of *Hash2* with 0. If they differ, increment *modifier* and go back to step (2).
  5. Hash the concatenation of *modifier*, *collision count*, *prefix* and Pub_{Key}

     $$Hash1 = Left_{64}(\text{ SHA-1}(\ modifier \mid \text{coll. count} \mid \text{prefix} \mid Pub_{Key}\ )\ )$$
  6. Obtain the *HostID* by setting the “u” and “g” bits to 1 and the *Sec* bits.
  7. Perform DAD. If there is a collision, increment the *collision count* and go back to step 5.

CGA Verification

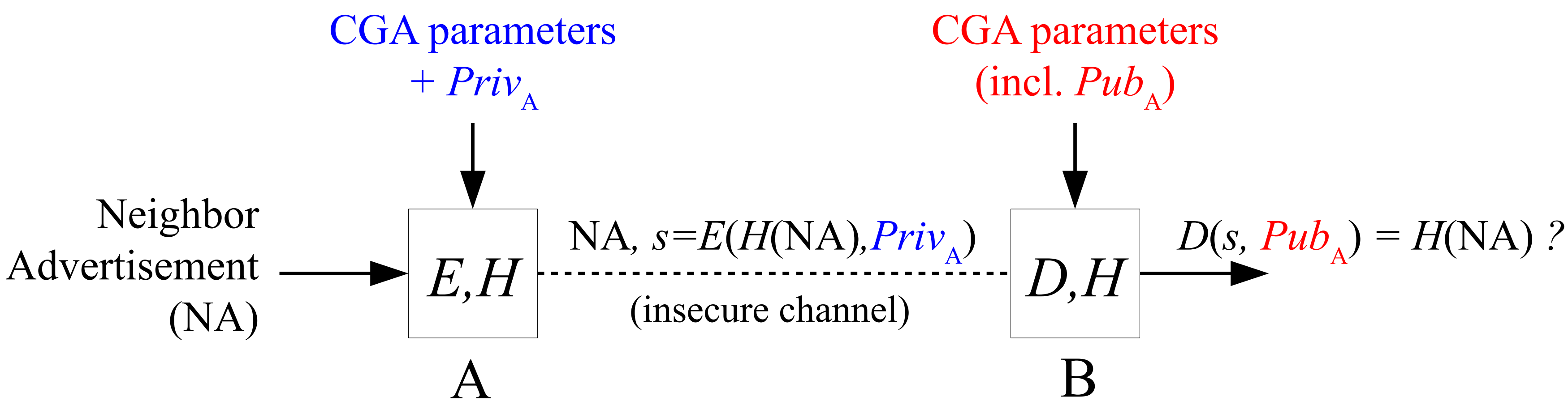
Pas vu

- **Algorithm (RFC3972)**
  1. Hash the concatenation of modifier, subnet prefix, collision count and PubKey obtained from the CGA parameters. The 64 leftmost bits are $Hash1$.
  2. Compare $Hash1$ with the HostID, ignoring the "u", "g" and Sec bits. If the comparison fails, the verification fails.
  3. Hash the concatenation of the CGA parameters (*collision count* and prefix set to 0). The 112 leftmost bits are $Hash2$.
  4. Compare the $16*Sec$ leftmost bits of $Hash2$ with zero. If the comparison fails, the verification fails.

CGA Signature

Pas vu

- **Generation and Verification**

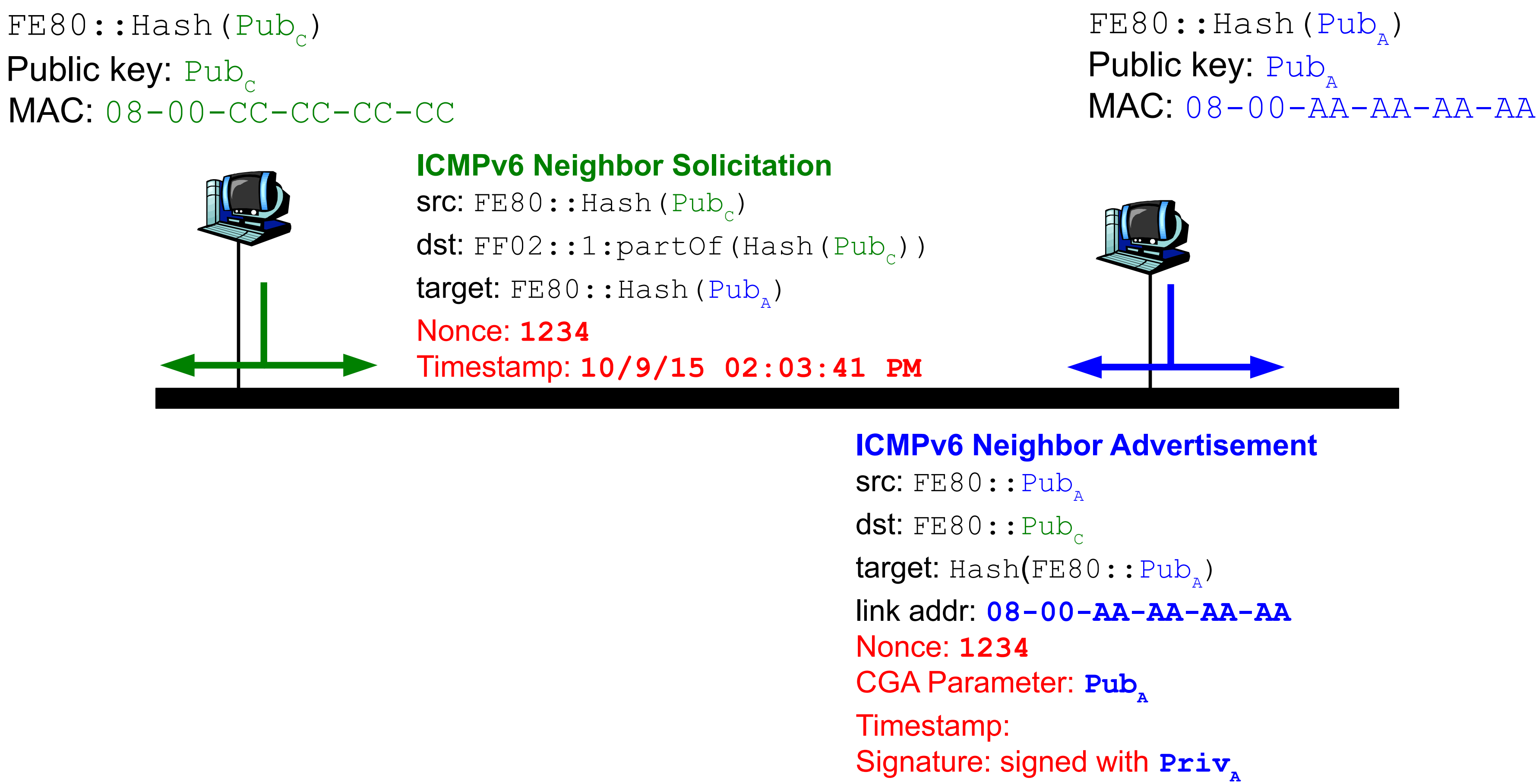


- The receiver must
  - first verify the CGA address, i.e. check that the CGA parameters would lead to the same HostId
  - then check the digital signature

Extensions to ICMPv6

- **SEcure Neighbor Discovery (SEND)**
  - RFC3971
  - RSA Signature option
    - 128 most significant bits of SHA-1 of PubKey used to sign
    - digital signature computed over (random message tag, source address, destination address, ICMPv6 type, code and checksum, NDP header and options)
  - Timestamp option
    - used to avoid replay attacks
  - Nonce option
  - CGA parameter option
    - used to exchange CGA generation parameters: Modifier, collision count, subnet prefix and Pub_{Key}.

Secure Neighbor Discovery (SEND)



CGA

- **The attacker's perspective**
  - To steal a CGA address, a malicious host should be able to either
    - find the private key used
    - or find a public/private key pair that hashes to the same target hostId
  - Both problems are now very difficult.

- **Note**
  - CGA addresses are also extended for use beyond SEND. See RFC4581

IPv6

- 4. 1 Motivations
- 4.2 IPv6 Addressing Architecture
- 4.3 IPv6 Packets
- 4.4 ICMPv6
- 4.5 DNS support for IPv6
- 4.6 Transition Mechanisms

DNSv6

Car UDP : taille minimale : 512 octets
=> certains routeurs rejetaient les paquets

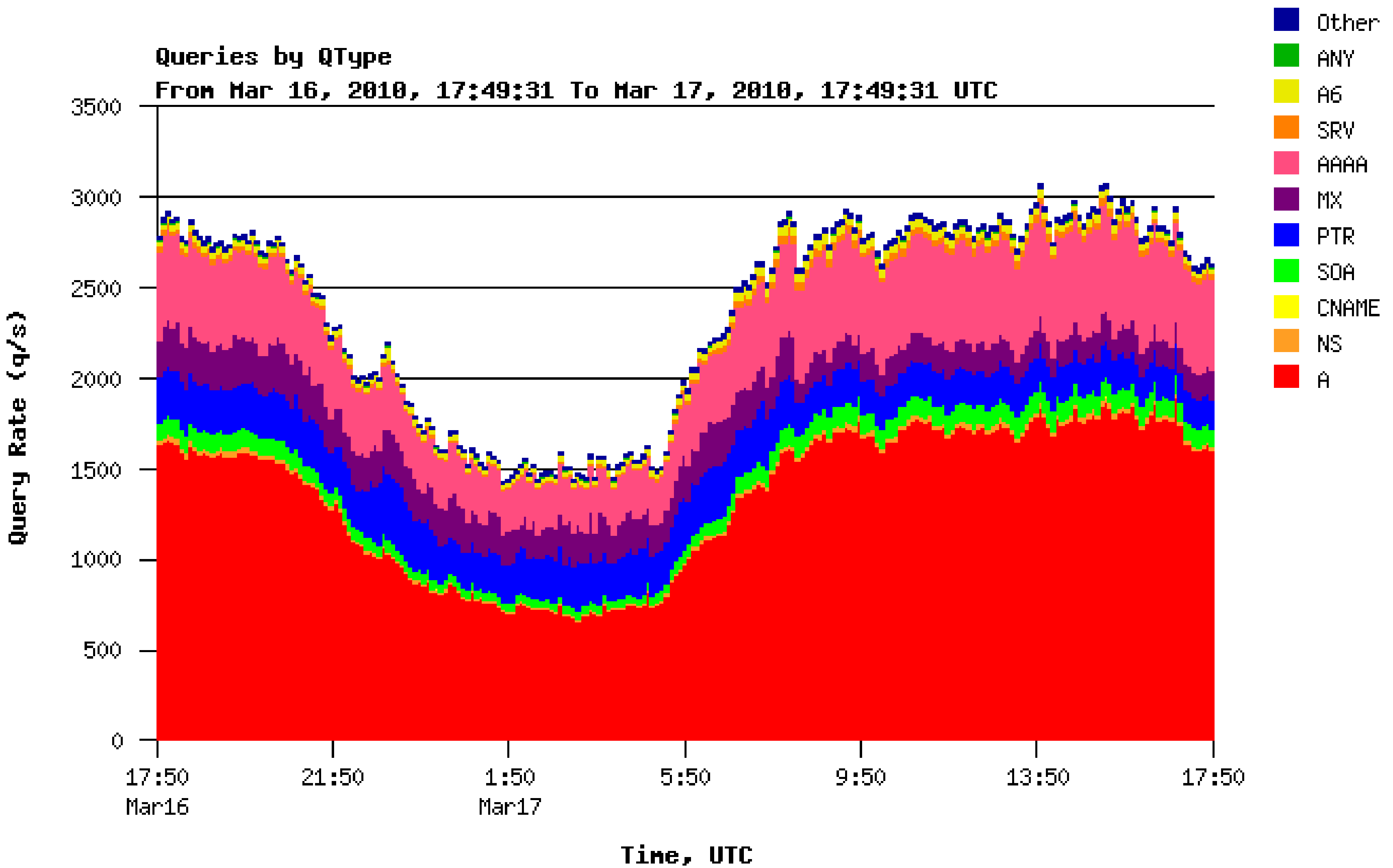
- Three problems to solve
  - How to encode IPv6 addresses in the DNS ?
  - How to support reverse DNS ?
  - How to perform all DNS requests by using only IPv6 ?

DNSv6

- Each DNS message is composed of *Resource Records* (RR) encoded as *Type-Length-Value* (TLV) <Name, Value, Type, TTL>

- Types of RR
  - A (IPv4 Address)
    - Name is a hostname and Value an IPv4 address
  - **AAAA (IPv6 Address)**
    - Name is a hostname and Value an IPv6 address
  - NS (NameServer)
    - Name is a domain name and Value is the hostname of a DNS server responsible for this domain
  - MX (Mail eXchange)
    - Name is a domain name and Value is the name of an SMTP server that must be contacted to send emails to this domain
  - CNAME (Canonical Name)
    - Alias

DNSv6



Source: http://k.root-servers.org/statistics/denic/daily/
(retrieved on 17/03/2010)

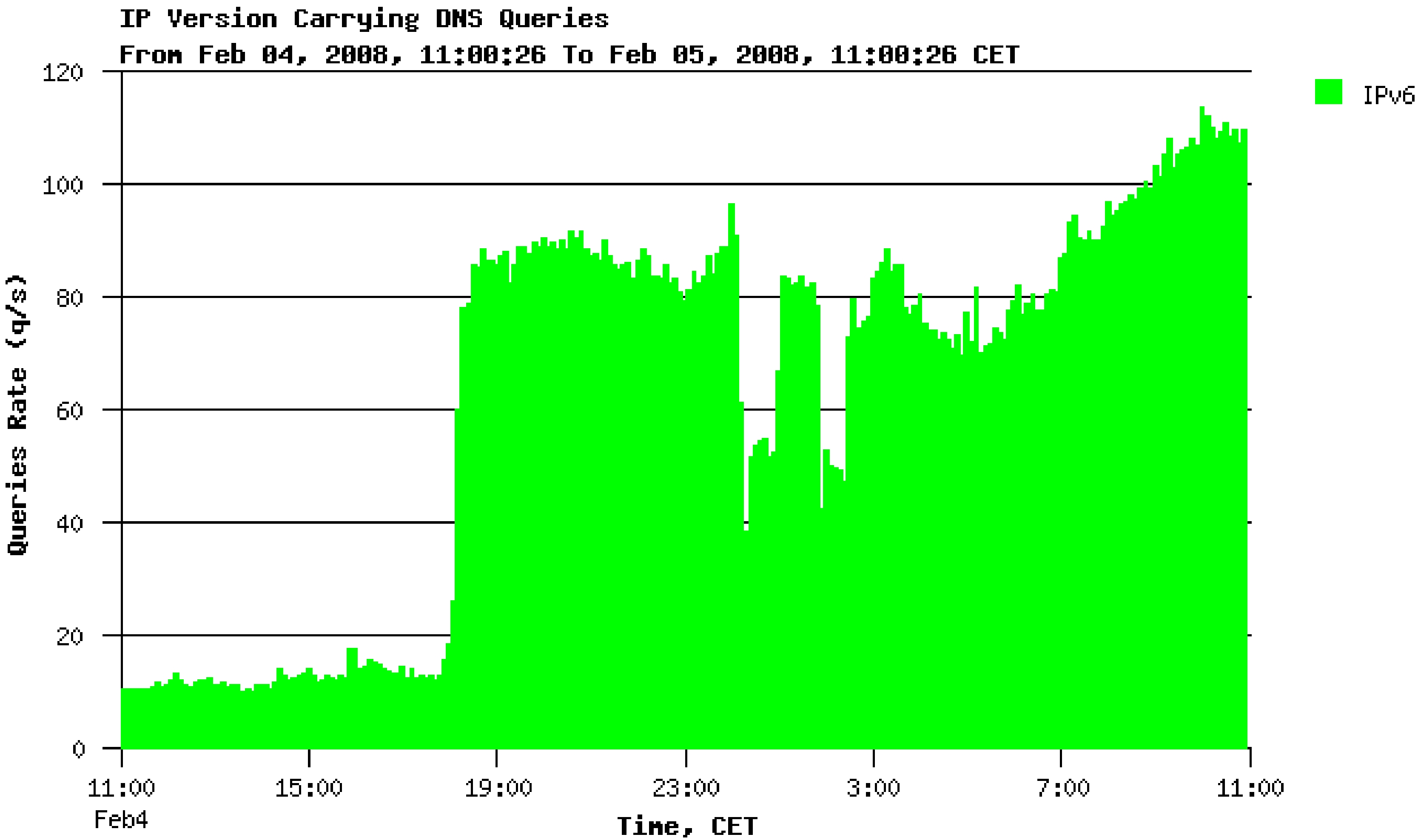
Supporting Reverse DNS

- Solution: special domain IP6.ARPA
  - Encode IPv6 address in reverse order, one character per group of 4 bits
  - perform classical DNS query
  - Example
    - `4321:0:1:2:3:4:567:89AB`
    - `b.a.9.8.7.6.5.0.4.0.0.0.3.0.0.0.2.0.0.0.1.0.0.0.0.0.0.0.1.2.3.4.IP6.ARPA.`

Adding IPv6 addresses to the DNS root

- Took a much longer time than expected
  - Initially DNS root was only reachable via IPv4
    - List of DNS root servers is encoded in one DNS reply
    - All DNS implementations must support DNS replies of 512 bytes, but encoding of the 13 IPv4 DNS root servers already consumes 400 bytes. Adding IPv6 for all DNS root servers requires 811 bytes in the reply
  - Several TLD moved quickly to IPv6
    - One IPv6 authoritative server for `.be` since sept. 2004
  - DNS was extended to support larger replies
  - February 2008
    - 6 root DNS servers support IPv6
    - IPv6-only hosts can at last use the DNS
    - Today (9/2014), 11 among 13 root servers

Adding IPv6 addresses to the DNS root



Source: k-root server (retrieved on 17/03/2010)

IPv6

- 4. 1 Motivations
- 4.2 IPv6 Addressing Architecture
- 4.3 IPv6 Packets
- 4.4 ICMPv6
- 4.5 DNS support for IPv6
- 4.6 Transition Mechanisms

Transition From IPv4 To IPv6

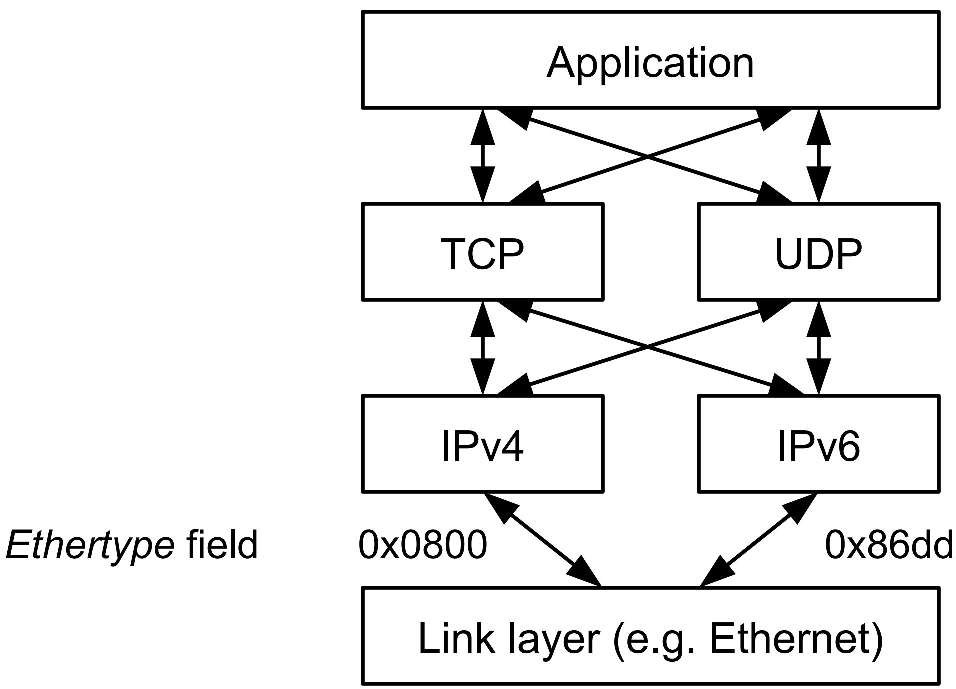
- Not all routers and end-hosts can be upgraded simultaneously
  - There will be no "flag days"
  - How will the network operate with mixed IPv4 and IPv6 routers?

- Several techniques have been proposed
  - *Dual-stack*
  - *Tunneling:* IPv6 carried as payload in IPv4 datagram among IPv4 routers
  - Translation

Dual Stack Techniques

TCP/UDP légèrement modifiés pour IPv6
=> interpretation du pseudo header

- **Dual-stack node**
  - has support for both protocol versions
    - behaves as an IPv6 node when in communication with another IPv6 node
    - behaves as an IPv4 node when in communication with another IPv4 node



Application need to be updated to support IPv6 addresses
+ slight changes in socket API

Dual Stack Techniques

- **Dual-stack node**
  - Most end-host OS today (linux, FreeBSD, Mac OS X, and even Windows) support IPv6 !
  - Usually, the DNS is used to detect if the remote host supports IPv4 and/or IPv6.
  - Very often, the local OS has a priority for the IP version to use.
    - For example, Mac OS X used to first try the IPv6 address.
  - Benefit:
    - straightforward
  - Drawbacks:
    - need to store state for both network protocol stacks (i.e. routing table, ...); some v4/v6 commands/options differ; ...
    - People don't know IPv6 enabled on their machine → don't configure firewall accordingly → Danger !

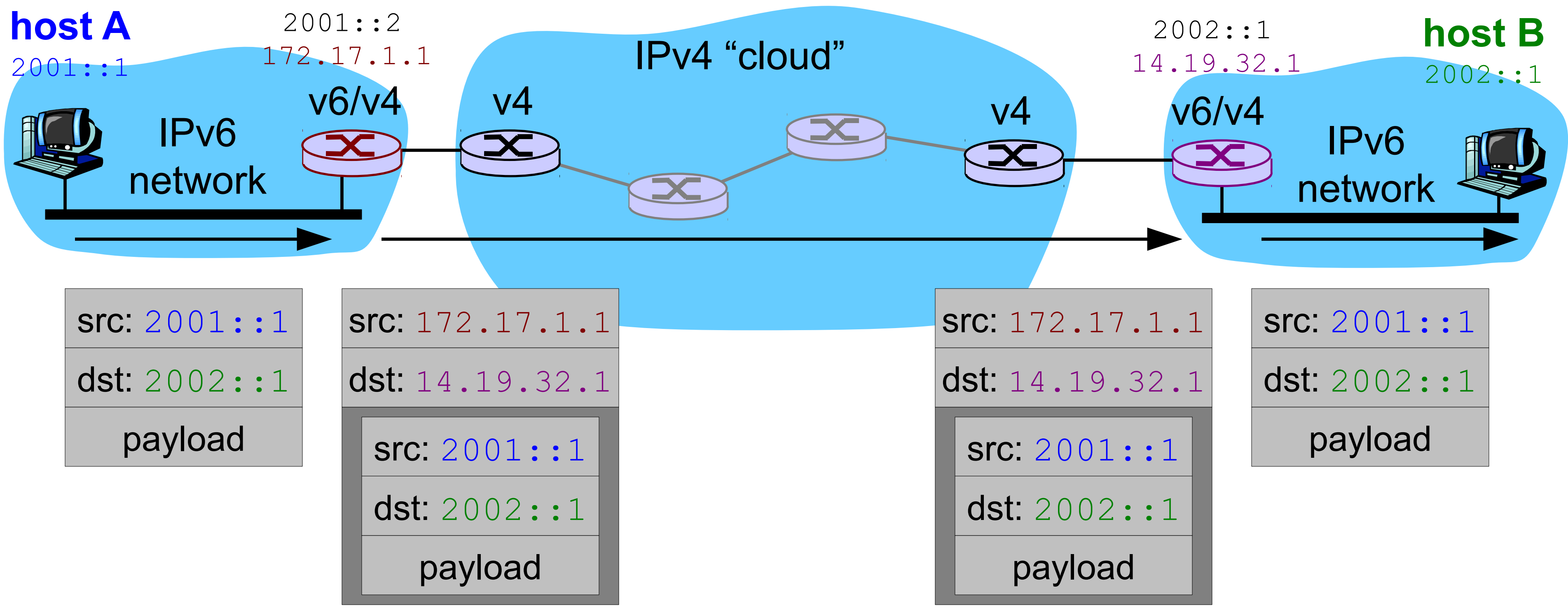
Dual Stack Techniques

- **Dual-stack network**
  - Need to update core devices so that they can support IPv6
  - **Switches**
    - operate at layer 2 (below v6) → should be transparent
    - But most switches have a management layer (using IP)
    - But IP Multicast help from switches (IGMP snooping)
  - **Routers**
    - routing protocols need to be updated
      - RIP → RIPng
      - OSPF → OSPFv3
      - BGP → Multi-Protocol BGP (MP-BGP)
    - Need to support hardware based IPv6 forwarding (in particular IPv6 lookup)
  - Other infrastructure services
    - Security (firewalls, DPI), DNS, NAT, ...

Afin de connaître à quel groupe appartient quel routeur afin d'éviter le broadcast inutile

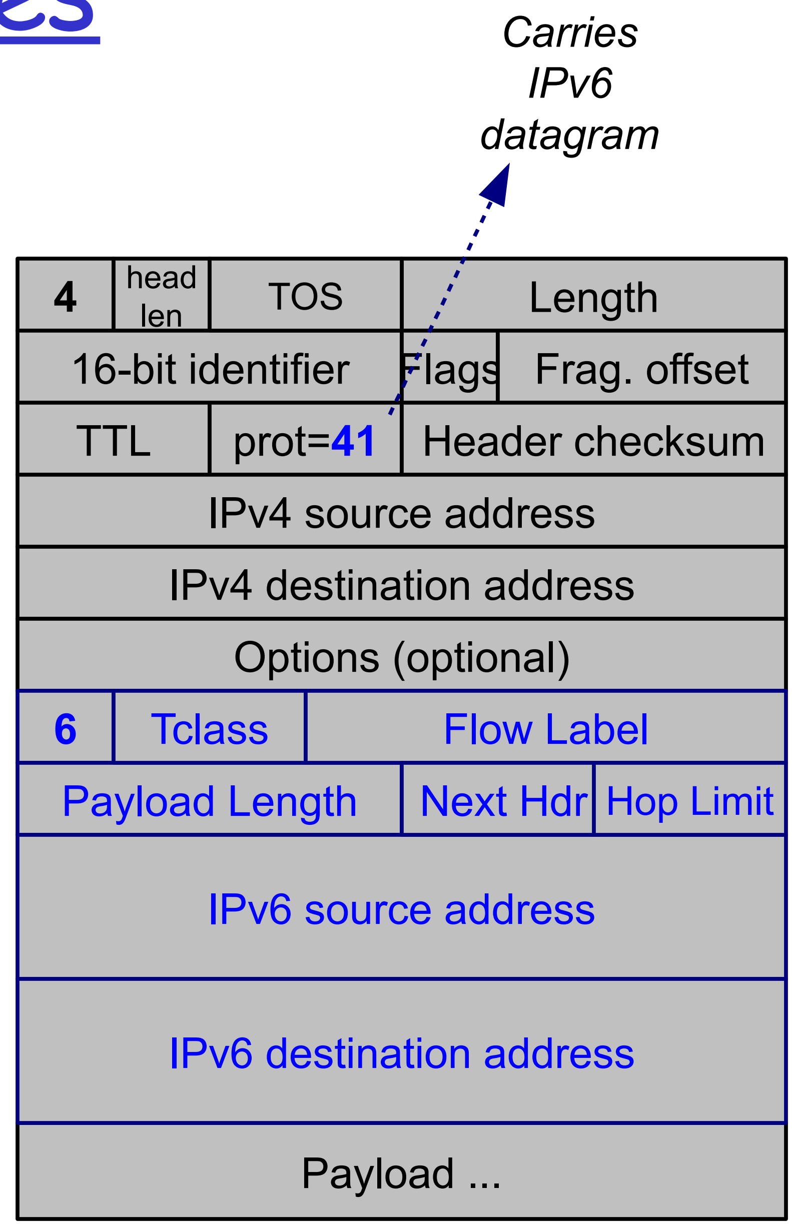
Tunneling Techniques

- **Objective**
  - Typically deploy an IPv6 forwarding infrastructure over the existing IPv4 infrastructure.



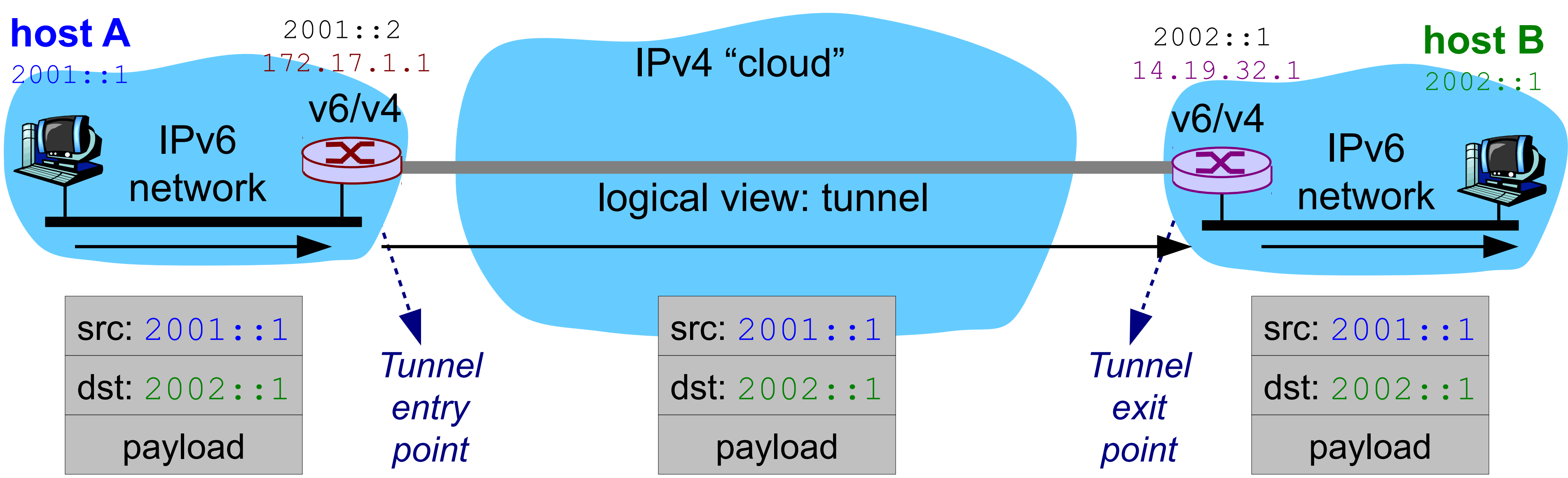
Tunneling Techniques

- Different encapsulation standards
  - IP in IP
  - *Generic Routing Encapsulation* (GRE), IPSec, …
- Issues
  - MTU
    - IPv6 requires 1280 bytes
    - IPv4 requires 576 bytes
  - TTL
    - what value to use ? (implementation dependent)
  - ICMPv4 errors within tunnel



Tunneling Techniques

- **Objective**
  - Typically deploy an IPv6 forwarding infrastructure over the existing IPv4 infrastructure.
  - Tunneling = encapsulation



Tunneling Techniques

- **Two general types of tunneling**
  - Manually configured
    - tunnels head- and tail- ends are configured manually
  - Automatic tunneling
    - relies on the use of special addresses, such as 6to4 or ISATAP addresses, to dynamically tunnel IPv6 packets over an IPv4 routing infrastructure. The special IPv6 addresses embed an IPv4 address.

Tunneling Techniques

- **6to4** (RFC3056)
  - transition mechanism that allows IPv6 islands to communicate with each other over an IPv4 infrastructure without explicit setup
  - 6to4 routers/gateways
  - Special IPv6 prefix assigned by IANA: `2002::/16`
    - 32 bits after prefix represent IPv4 address of gateway

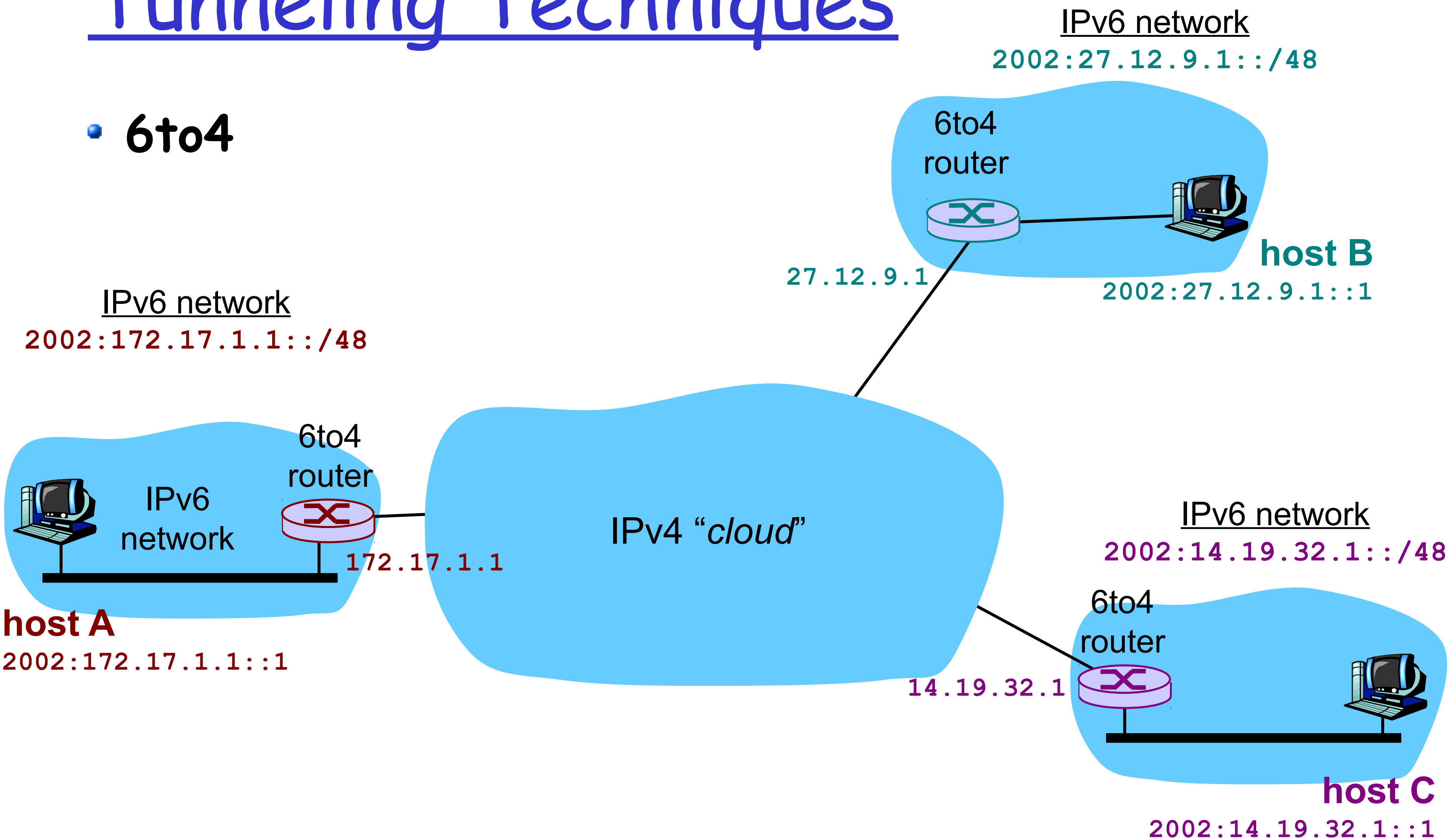
`2002:0`	IPv4 addr	Subn. ID	Interface ID

    - Example prefix of a 6to4 network: `2002:172.17.1.1::/48`

  - for some statistics, see also ***Observations of IPv6 Traffic on a 6to4 Relay***, Pekka Savola, ACM SIGCOMM Computer Communications Review, Volume 35, Number 1: January 2005

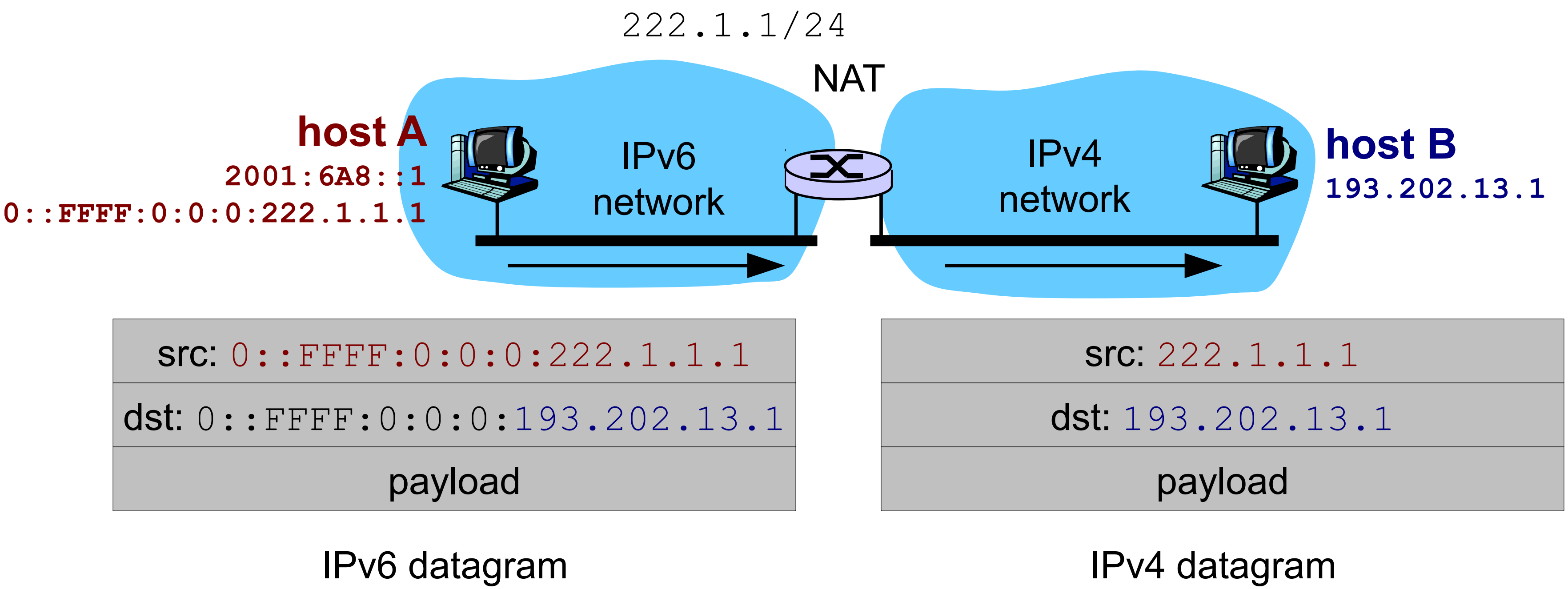
Tunneling Techniques

- **6to4**



Translation

- Stateless IP/ICMP Translation (SIIT, RFC2765)
  - Special IPv6 addresses in prefix `0::FFFF:0:0:0/96`
  - Host ID part is an IPv4 address



Translation

Teredo => encapsuler IPv6 par UDP
Microsoft Vista => par défaut sur serveur Teredo Microsoft

- NAT-PT (RFC2766)
  - Uses translation defined by SIIT
  - Uses pool of IPv4/IPv6 addresses to allocate to the other side
  - Keep mapping in translation table (same as classical NAT)

- Issues with translation
  - some fields have no counterpart, IPv6 options, fragmentation vs PMTUD, ...
  - translation is expensive (CPU, memory)
  - constraints on topology (replies have to come through same NAT)
  - breaks applications with IP addresses in the payload
  - you don't want NAT in IPv6