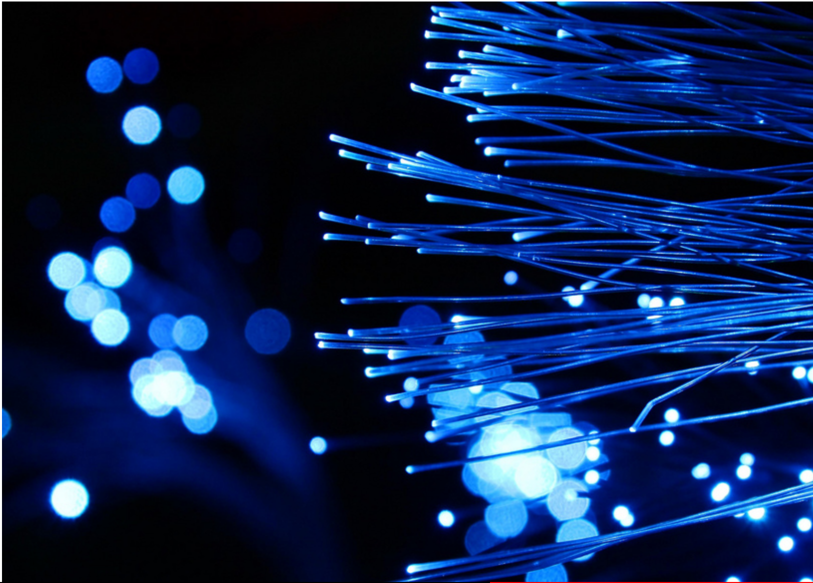
Accès IPv6 :
Pourquoi & Comment

Bruno Stévant & Laurent Toutain

June 28, 2011



Facts on Addresses

Historical view

Historical facts

- 1983 : Research network for about 100 computers
- 1992 : Commercial activity
  - Exponential growth
- 1993 : Exhaustion of the class B address space
  - Allocation in the class C space
  - Require more information in routers memory
- Forecast of network collapse for 1998!
  - 1999 : Bob Metcalfe ate his Infoworld 1995 paper where he made this prediction

Facts on Addresses

Emergency Measures

Emergency Measures: Better Addresses Management

RFC 1517 - RFC 1520 (Sept 1993)

- Ask the internet community to give back allocated prefixes (RFC 1917)
- Re-use class C address space
- CIDR (Classless Internet Domain Routing)
  - network address = prefix/prefix length
  - less address waste
  - recommend aggregation (reduce routing table length)
- Introduce private prefixes (RFC 1918)

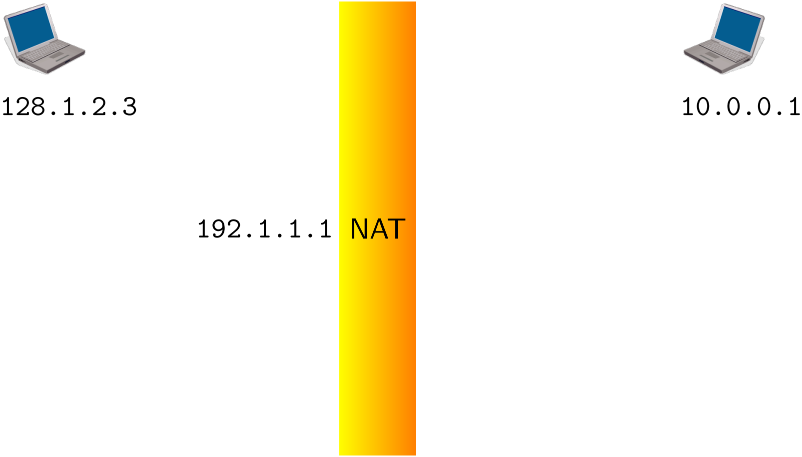
Facts on Addresses

NAT

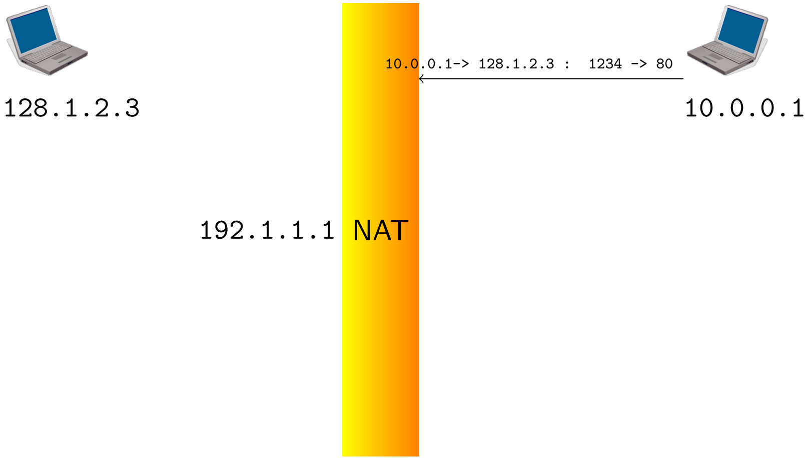
Emergency Measures: Private Addresses (RFC 1918 BCP)

- Allow private addressing plans
- Addresses are used internally
- Similar to security architecture with firewalls
- Use of proxies or NAT to go outside
  - RFC 1631, RFC 2663 and RFC 2993
- NAPT is the most commonly used of NAT variations

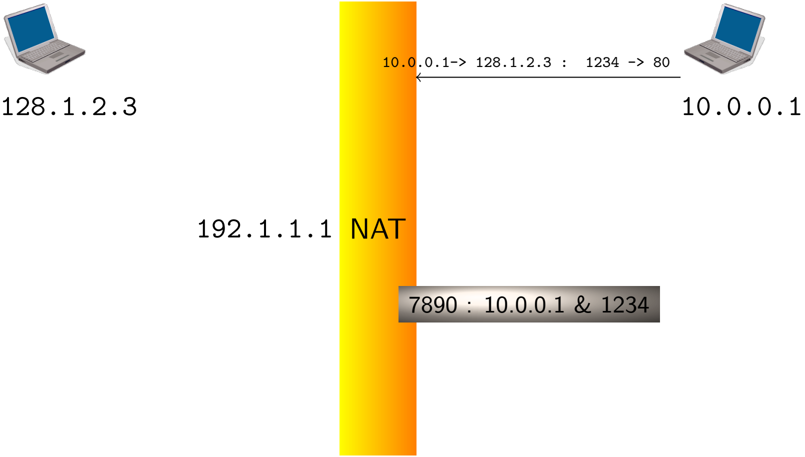
How NAT with Port Translation Works



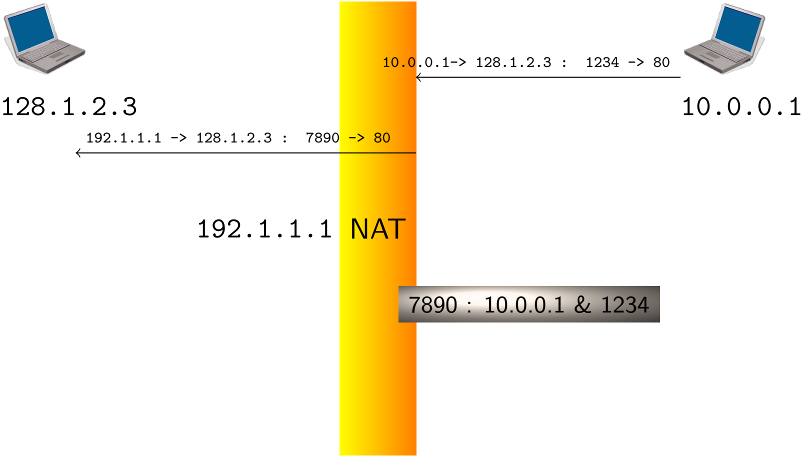
How NAT with Port Translation Works



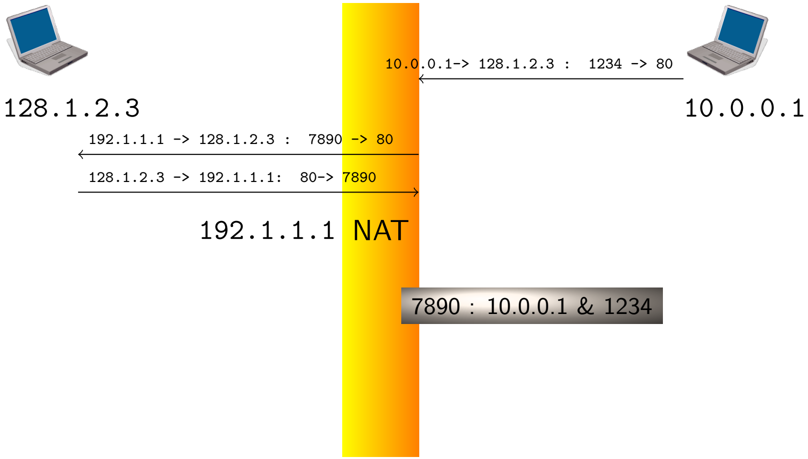
How NAT with Port Translation Works



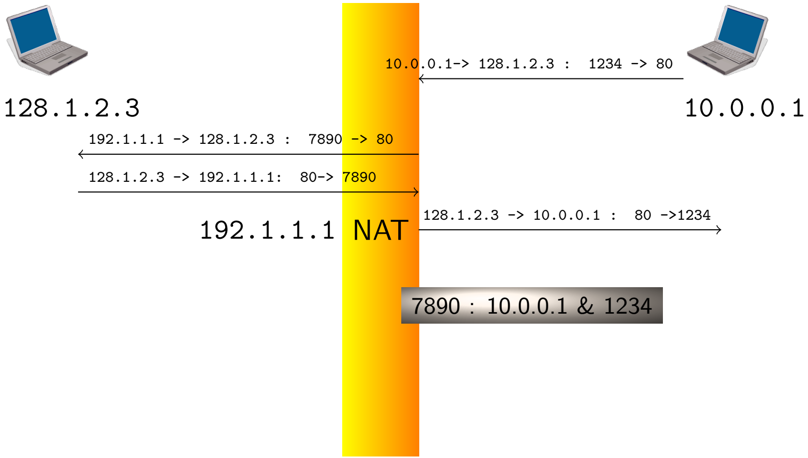
How NAT with Port Translation Works



How NAT with Port Translation Works



How NAT with Port Translation Works



NAT Impact

first consequence

The application does not know its public name.

second consequence

It is difficult to contact a NATed equipment from outside

- Security feeling
- Solutions for NAT traversal exist

third consequence

There is no standardized behavior for NAT yet

Facts on Addresses

Prefixes delegation

What Has Changed

Classful Addressing

1. Ensure uniqueness
2. Facilitate administrative allocation
   - One central entity

Class-Less (CIDR)

1. Facilitate administrative allocation (hierarchical)
   - Nowadays 5 regional entities
2. Facilitate host location in the network
3. Allocate the minimum pool of addresses

What Has Changed

Classful Addressing

1. Ensure uniqueness
2. Facilitate administrative allocation
    - One central entity

Class-Less (CIDR)

1. Facilitate administrative allocation (hierarchical)
    - Nowadays 5 regional entities
2. Facilitate host location in the network
3. Allocate the minimum pool of addresses

What Has Changed

Classful Addressing

1. Ensure uniqueness
2. Facilitate administrative allocation
   - One central entity

Class-Less (CIDR)

1. Facilitate administrative allocation (hierarchical)
   - Nowadays 5 regional entities
2. Facilitate host location in the network
3. Allocate the minimum pool of addresses

What Has Changed

Classful Addressing

1. Ensure uniqueness
2. Facilitate administrative allocation
   - One central entity

Class-Less (CIDR)

1. Facilitate administrative allocation (hierarchical)
   - Nowadays 5 regional entities
2. Facilitate host location in the network
3. Allocate the minimum pool of addresses

What Has Changed

Classful Addressing

1. Ensure uniqueness
2. Facilitate administrative allocation
   - One central entity

Class-Less (CIDR)

1. Facilitate administrative allocation (hierarchical)
   - Nowadays 5 regional entities
2. Facilitate host location in the network
3. Allocate the minimum pool of addresses

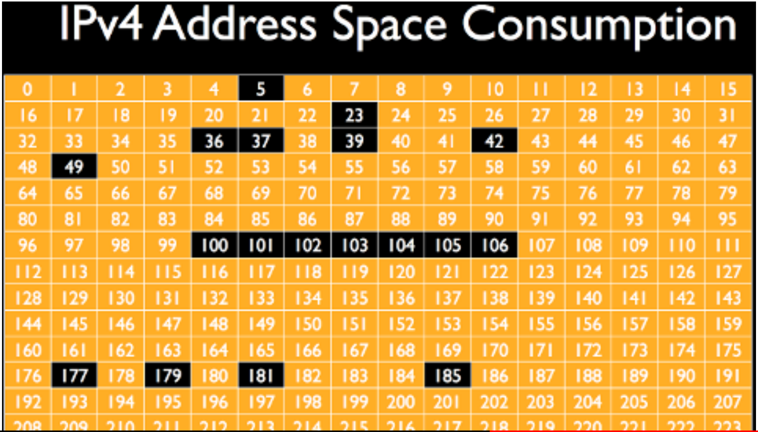
CIDR Administrative Point of View

- A hierarchy of administrative registries
  - IANA/ICANN at the top
- 5 Regional Internet Registries (RIR)
  - APNIC (Asia Pacific Network Information Centre)
  - ARIN (American Registry for Internet Numbers)
  - LACNIC (Regional Latin-American and Caribbean IP Address Registry)
  - RIPE NCC (Réseaux IP Européens - Network Coordination Center)
    - Europe, Middle east.
  - AfriNIC (Africa)
- Providers get prefixes allocation from RIR

RIR Regions

Exhaustion of IPv4 Prefix Pool

- IANA Unallocated Address Pool Depleted: February, 1st 2011
  - See: http://www.nro.net/news/ipv4-free-pool-depleted
- RIR Unallocated Address Pool Exhaustion Forecasts: Start from May 2011
  - See: http://www.potaroo.net/tools/ipv4/
  - See als: http://www.ipv4depletion.com/



IPv4 Address Space Consumption

0	1	2	3	4	**5**	6	7	8	9	10	11	12	13	14	15
16	17	18	19	20	21	22	**23**	24	25	26	27	28	29	30	31
32	33	34	35	**36**	**37**	38	**39**	40	41	**42**	43	44	45	46	47
48	**49**	50	51	52	53	54	55	56	57	58	59	60	61	62	63
64	65	66	67	68	69	70	71	72	73	74	75	76	77	78	79
80	81	82	83	84	85	86	87	88	89	90	91	92	93	94	95
96	97	98	99	**100**	**101**	**102**	**103**	**104**	**105**	**106**	107	108	109	110	111
112	113	114	115	116	117	118	119	120	121	122	123	124	125	126	127
128	129	130	131	132	133	134	135	136	137	138	139	140	141	142	143
144	145	146	147	148	149	150	151	152	153	154	155	156	157	158	159
160	161	162	163	164	165	166	167	168	169	170	171	172	173	174	175
176	**177**	178	**179**	180	**181**	182	183	184	**185**	186	187	188	189	190	191
192	193	194	195	196	197	198	199	200	201	202	203	204	205	206	207
208	209	210	211	212	213	214	215	216	217	218	219	220	221	222	223

Addresses

IPv6 Benefits

- Larger address space from 2^{32} to 2^{128}
  - Permanent address
- Stateless auto-configuration of hosts
  - Layer 3 "Plug & Play" Protocol
- Simple header $\Rightarrow$ Efficient routing
  - No checksum
  - No fragmentation by routers
  - Enhanced extension system
- Better support of mobility

Addresses

Notation

IPv6 addresses

F2C:544:9E::2:EF8D:6B7 F692:: A:1455::A:6E0 D:63:D::4:3A:55F B33:C::F2 7:5059:3D:C0::

9D::9BAC:B8CA:893F:80 1E:DE2:4C83::4E:39:F35:C875 2:: A:FDE3:76:B4F:D9D:: D6::

369F:9:F8:DBF::2 DD4:B45:1:C42F:BE6:75:: 9D7B:7184:EF::3FB:BF1A:D80 FE9::B:3

EC:DB4:B:F:F11::E9:090 83:B9:08:B5:F:3F:AF:B84 E::35B:8572:7A3:FB2 99:F:9:8B76::BC9

D64:07:F394::BDB:DF40:08EE:A79E AC:23:5D:78::233:84:8 F0D:F::F4EB:0F:5C7

E71:F577:ED:E:9DE8:: B::3 1D3F:A0AA:: 70:8EA1::8:D5:81:2:F302 26::8880:7 93:: F::9:0

E:2:0:266B:: 763E:C:2E:1EB:F6:F4:14:16 E6:6:F4:B6:A888:979E:D78:09

9:754:5:90:0A78:A1A3:1:7 2:8:: 97B:C4::C36 A40:7:5:7E8F:0:32EC:9A:D0 8A52::575

D::4CB4:E:2BF:5485:8CE 07:5::41 6B::A9:C 94FF:7B8::D9:51:26F 2::E:AE:ED:81 8241:: 5F97::

AD5B:259C:7DB8:24:58:552A:: 94:4:9FD:4:87E5:: 5A8:2FF:1::CC EA:8904:7C::

7C::D6B7:A7:B0:8B DC:6C::34:89 6C:1::5 7B3:6780:4:B1::E586 412:2:5E1:6DE5:5E3A:553:3::

7F0:: B39::1:B77:DB 9D3:1F1:4B:3:B4E6:7681:09:D4A8 61:520::E0 1:28E9:0:095:DF:F2::

1B61:4::1DE:50A 34BC:99::E9:9EFB E:EF:: BDC:672A:F4C8:A1::4:7:9CB7 C697:56AD:40:8:0::62

Notation

- Base format (a 16-octet Global IPv6 Address):
  - `2001:0db8:beef:0001:0000:0000:cafe:deca`
- Compact Format:

2001:0db8:beef:0001:0000:0000:cafe:deca

1. Remove 0 on the left of each word
2. To avoid ambiguity, substitute ONLY one sequence of zeros by `::`

- an IPv4 address may also appear : `::ffff:192.0.2.1`

Warning:

`2001:db8:3::/40` is in fact `2001:db8:0003::/40` and not `2001:db8:0300::/40`

Notation

- Base format (a 16-octet Global IPv6 Address):
  - `2001:0db8:beef:0001:0000:0000:cafe:deca`
- Compact Format:

2001:0db8:beef:0001:0000:0000:cafe:deca

1. Remove 0 on the left of each word
2. To avoid ambiguity, substitute ONLY one sequence of zeros by `::`

- an IPv4 address may also appear : `::ffff:192.0.2.1`

Warning:

`2001:db8:3::/40` is in fact `2001:db8:0003::/40` and not `2001:db8:0300::/40`

- Base format (a 16-octet Global IPv6 Address):
  - `2001:0db8:beef:0001:0000:0000:cafe:deca`
- Compact Format:

2001:db8:beef:1:0:0:cafe:deca

1. Remove 0 on the left of each word
2. To avoid ambiguity, substitute ONLY one sequence of zeros by `::`

- an IPv4 address may also appear : `::ffff:192.0.2.1`

Warning:

`2001:db8:3::/40` is in fact `2001:db8:0003::/40` and not `2001:db8:0300::/40`

- Base format (a 16-octet Global IPv6 Address):
  - `2001:0db8:beef:0001:0000:0000:cafe:deca`
- Compact Format:

2001:db8:beef:1:0:0:cafe:deca

1. Remove 0 on the left of each word
2. To avoid ambiguity, substitute ONLY one sequence of zeros by `::`

- an IPv4 address may also appear : `::ffff:192.0.2.1`

Warning:

`2001:db8:3::/40` is in fact `2001:db8:0003::/40` and not `2001:db8:0300::/40`

Notation

- Base format (a 16-octet Global IPv6 Address):
  - `2001:0db8:beef:0001:0000:0000:cafe:deca`
- Compact Format:

2001:db8:beef:1::cafe:deca

1. Remove 0 on the left of each word
2. To avoid ambiguity, substitute ONLY one sequence of zeros by `::`

- an IPv4 address may also appear : `::ffff:192.0.2.1`

Warning:

`2001:db8:3::/40` is in fact `2001:db8:0003::/40` and not `2001:db8:0300::/40`

Notation

- Base format (a 16-octet Global IPv6 Address):
  - `2001:0db8:beef:0001:0000:0000:cafe:deca`
- Compact Format:

2001:db8:beef:1::cafe:deca

1. Remove 0 on the left of each word
2. To avoid ambiguity, substitute ONLY one sequence of zeros by `::`

- an IPv4 address may also appear : `::ffff:192.0.2.1`

Warning:

`2001:db8:3::/40` is in fact `2001:db8:0003::/40` and not `2001:db8:0300::/40`

Is it enough for the future ?

- Address length
  - About $3.4x10^{38}$ addresses
  - 60 000 trillion trillion addresses per inhabitant on earth
  - Addresses for every grain of sands in the world
  - IPv4: 6 addresses per US inhabitant, 1 in Europe, 0.01 in China and 0.001 in India
- Justification of a fixed-length address

Warning:

- An address for everything on the network and not an address for everything
- No addresses for the whole life:
  - Depends on your position on the network
  - ISP Renumbering may be possible

Addresses

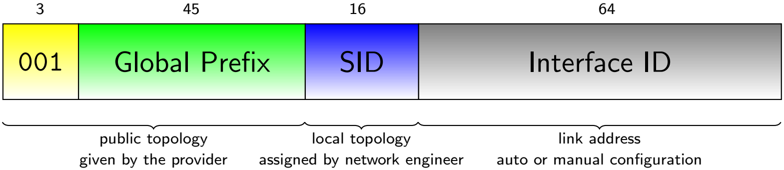
Addressing scheme

Addressing scheme

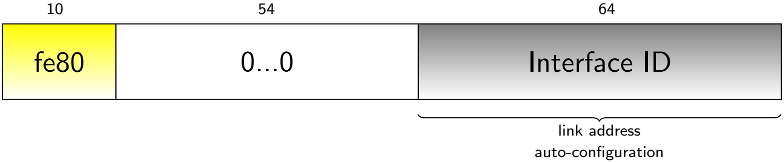
- RFC 4291 defines current IPv6 addresses
  - loopback (`::1`)
  - `link local (fe80::/10)`
  - `global unicast (2000::/3)`
  - `multicast (ff00::/8)`
- Use CIDR principles:
  - Prefix / prefix length notation
  - `2001:db8:face::/48`
  - `2001:db8:face:bed:cafe:deca:dead:beef/64`
- Interfaces have several IPv6 addresses
  - at least a link-local and a global unicast addresses

Address Format

Global Unicast Address:



Link-Local Address:



Interface ID can be selected differently

- Derived from a Layer 2 ID (I.e. MAC address) :
  - for Link Local address
  - for Global Address : plug-and-play hosts
- Assigned manually :
  - to keep same address when Ethernet card or host is changed
  - to remember easily the address
    - 1, 2, 3, ...
    - last digit of the v4 address
    - the IPv4 address (for nostalgic system administrators)
    - ...

Interface ID can be selected differently

- Derived from a Layer 2 ID (I.e. MAC address) :
  - for Link Local address
  - for Global Address : plug-and-play hosts
- Assigned manually :
  - to keep same address when Ethernet card or host is changed
  - to remember easily the address
    - 1, 2, 3, ...
    - last digit of the v4 address
    - the IPv4 address (for nostalgic system administrators)
    - ...

Interface ID can be selected differently

- Random value :
  - Changed frequently (e.g, every day, per session, at each reboot...) to guarantee anonymity
- Hash of other values (experimental) :
  - To link address to other properties
  - Public key
  - List of assigned prefixes
  - ...

Interface ID can be selected differently

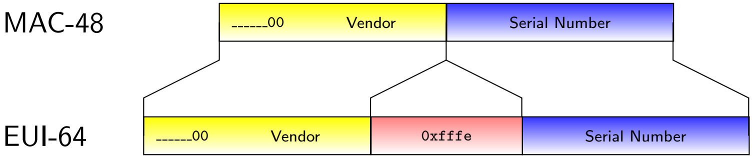
- Random value :
  - Changed frequently (e.g, every day, per session, at each reboot...) to guarantee anonymity
- Hash of other values (experimental) :
  - To link address to other properties
  - Public key
  - List of assigned prefixes
  - ...

How to Construct an IID from MAC Address

- 64 bits is compatible with EUI-64 (i.e. IEEE 1394 FireWire, ...)
- IEEE propose a way to transform a MAC-48 to an EUI-64
- U/L changed for numbering purpose
- There is no conflicts if IID are manually numbered: 1, 2, 3, ...

How to Construct an IID from MAC Address

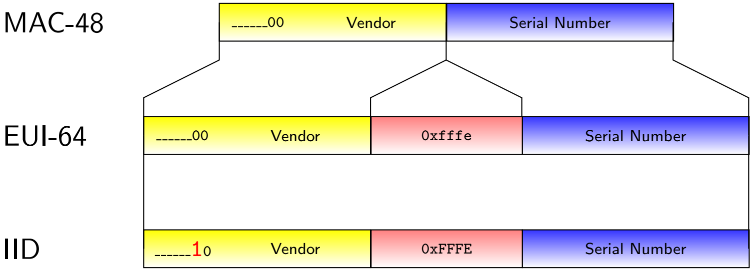
- 64 bits is compatible with EUI-64 (i.e. IEEE 1394 FireWire, ...)
- IEEE propose a way to transform a MAC-48 to an EUI-64
- U/L changed for numbering purpose



- There is no conflicts if IID are manually numbered: 1, 2, 3, ...

How to Construct an IID from MAC Address

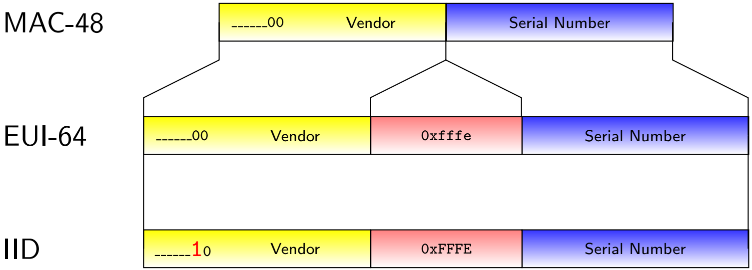
- 64 bits is compatible with EUI-64 (i.e. IEEE 1394 FireWire, ...)
- IEEE propose a way to transform a MAC-48 to an EUI-64
- U/L changed for numbering purpose



- There is no conflicts if IID are manually numbered: 1, 2, 3, ...

How to Construct an IID from MAC Address

- 64 bits is compatible with EUI-64 (i.e. IEEE 1394 FireWire, ...)
- IEEE propose a way to transform a MAC-48 to an EUI-64
- U/L changed for numbering purpose



- There is no conflicts if IID are manually numbered: 1, 2, 3, ...

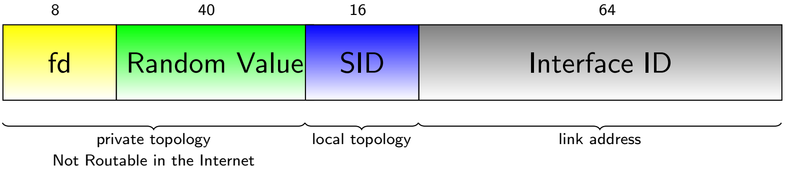
Addresses

Kind of addresses

Other kind of addresses : ULA (RFC 4193)

- Equivalent to the private addresses in IPv4
- But try to avoid same prefixes on two different sites:
  - avoid renumbering if two company merge
  - avoid ambiguities when VPN are used
- These prefixes are not routable on the Internet

Unique Local IPv6 Unicast Addresses:



http://www.sixxs.net/tools/grh/ula/ to create your own ULA prefix.

Multicast

Generic Format:

8	4	4	112
ff	xRPT	scope	Group ID

- T (Transient) 0: well known address - 1: temporary address
- P (Prefix) 1 : assigned from a network prefix (T must be set to 1)
- R (Rendez Vous Point) 1: contains the RP address (P & T set to 1)
- Scope :
  - 1 - interface-local
  - 2 - link-local
  - 3 - reserved
  - 4 - admin-local
  - 5 - site-local
  - 8 - organisation-local
  - e - global
  - f - reserved

Some Well Known Multicast Addresses

8	4	4	112
ff	0	scope	Group ID

```
ff02:0:0:0:0:0:0:1 All Nodes Address (link-local scop
ff02:0:0:0:0:0:0:2 All Routers Address
ff02:0:0:0:0:0:0:5 OSPFIGP
ff02:0:0:0:0:0:0:6 OSPFIGP Designated Routers
ff02:0:0:0:0:0:0:9 RIP Routers
ff02:0:0:0:0:0:0:fb mDNSv6
ff02:0:0:0:0:0:1:2 All-dhcp-agents
ff02:0:0:0:0:1:ffxx:xxxx Solicited-Node Address
ff05:0:0:0:0:0:1:3 All-dhcp-servers (site-local scope
```

http://www.iana.org/assignments/ipv6-multicast-addresses

Some Well Known Multicast Addresses

8	4	4	112
ff	0	scope	Group ID

```
ff02:0:0:0:0:0:0:1 All Nodes Address (link-local scop
ff02:0:0:0:0:0:0:2 All Routers Address
ff02:0:0:0:0:0:0:5 OSPFIGP
ff02:0:0:0:0:0:0:6 OSPFIGP Designated Routers
ff02:0:0:0:0:0:0:9 RIP Routers
ff02:0:0:0:0:0:0:fb mDNSv6
ff02:0:0:0:0:0:1:2 All-dhcp-agents
ff02:0:0:0:0:1:ffxx:xxxx Solicited-Node Address
ff05:0:0:0:0:0:1:3 All-dhcp-servers (site-local scope
```

http://www.iana.org/assignments/ipv6-multicast-addresses

Protocol

IPv6 Header

IPv6 Packet : Simpler

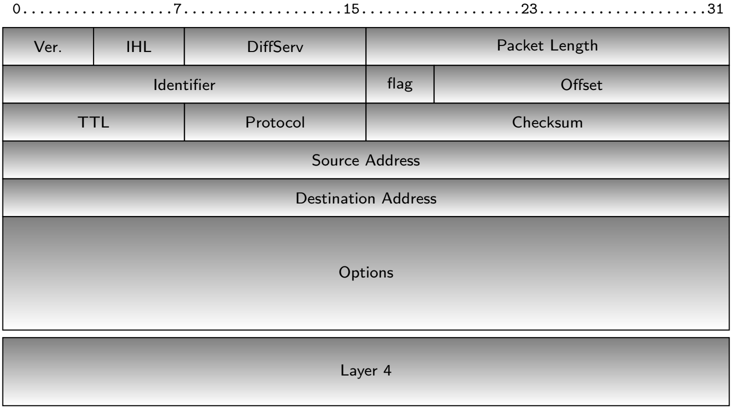
Definition

- IPv6 header follows the same IPv4 principle:
  - fixed address size ... but 4 times larger
  - alignment on 64 bit words (instead of 32)
- Features not used in IPv4 are removed
- Minimum MTU 1280 Bytes
  - If L2 cannot carry 1280 Bytes, then add an adaptation layer such as AAL5 for ATM or 6LoWPAN (RFC 4944) for IEEE 802.15.4.

Goal :

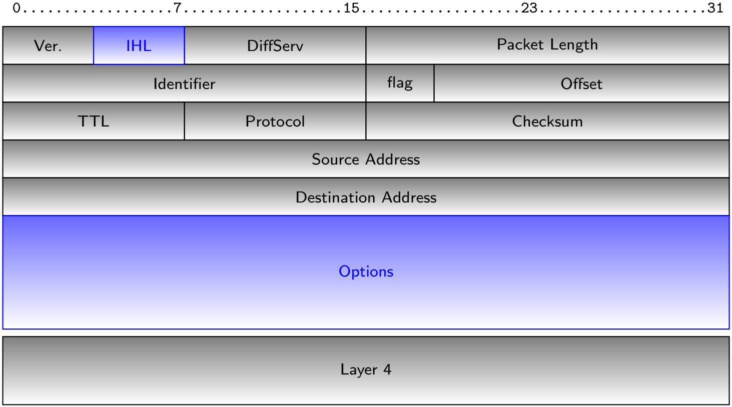
- Forward packet as fast as possible
- Less processing in routers
- More features at both ends

IPv4 Header

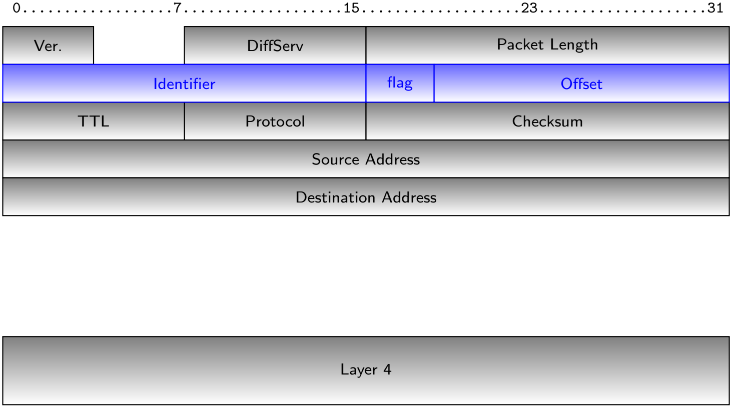


0 7 15 23 31
Ver.
IHL
DiffServ
Packet Length
Identifier
flag
Offset
TTL
Protocol
Checksum
Source Address
Destination Address
Options
Layer 4

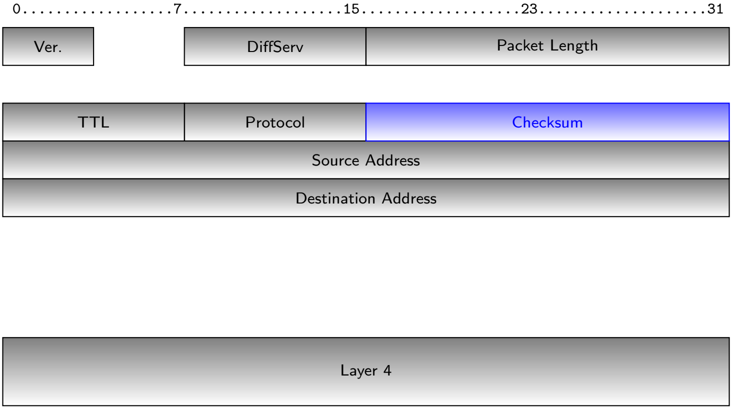
IPv4 Header


0..................7..................15..................23..................31
Ver.
IHL
DiffServ
Packet Length
Identifier
flag
Offset
TTL
Protocol
Checksum
Source Address
Destination Address
Options
Layer 4

IPv4 Header

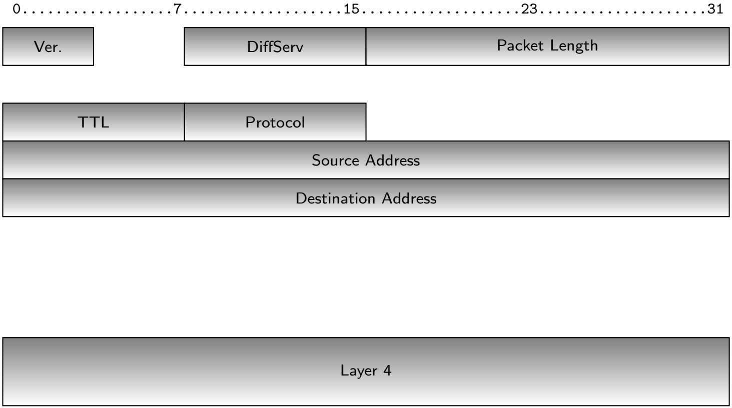

0.................7.................15.................23.................31
Ver.
DiffServ
Packet Length
Identifier
flag
Offset
TTL
Protocol
Checksum
Source Address
Destination Address
Layer 4

IPv4 Header



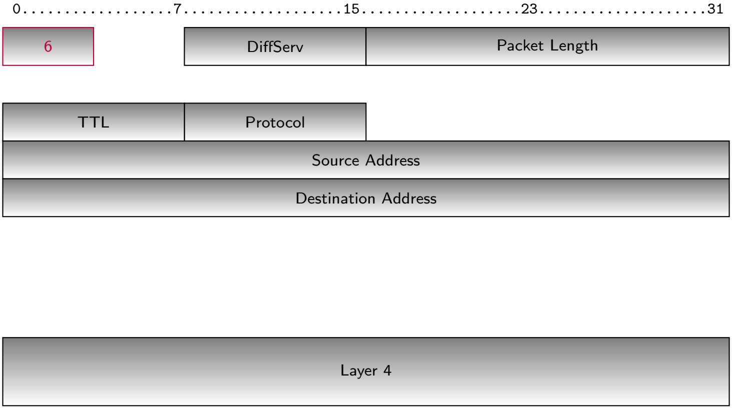
0 7 15 23 31
Ver.
DiffServ
Packet Length
TTL
Protocol
Checksum
Source Address
Destination Address
Layer 4

IPv4 Header



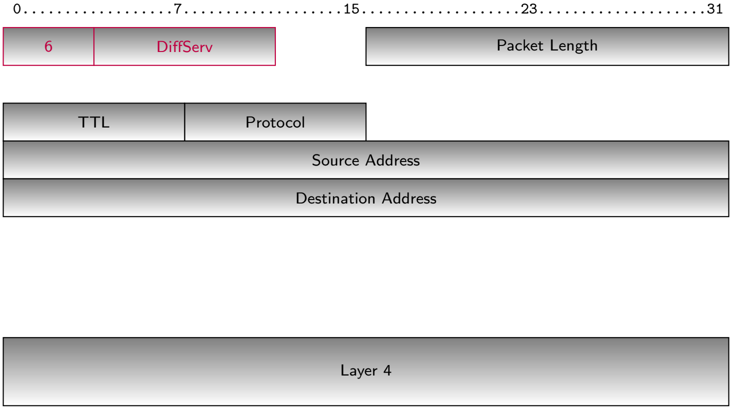
0
7
15
23
31
Ver.
DiffServ
Packet Length
TTL
Protocol
Source Address
Destination Address
Layer 4

IPv4 Header

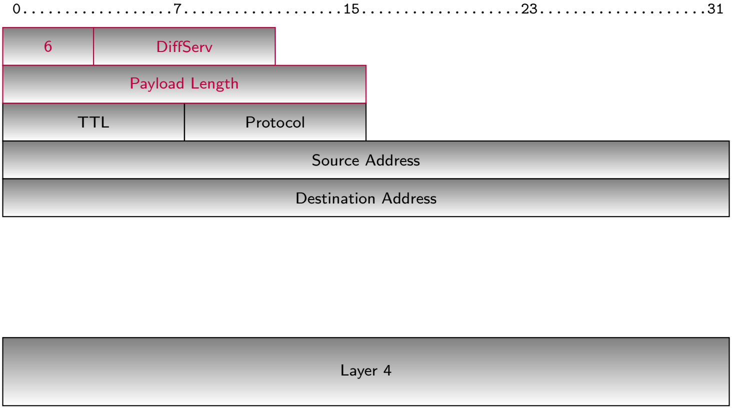


0
7
15
23
31
6
DiffServ
Packet Length
TTL
Protocol
Source Address
Destination Address
Layer 4

IPv4 Header

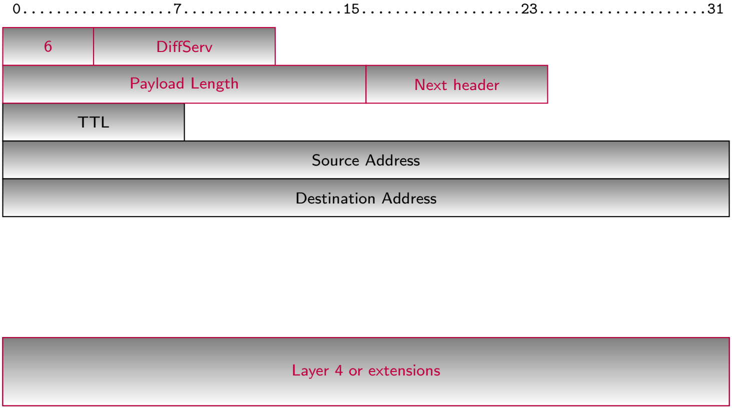

0 . . . . 7 . . . . 15 . . . . 23 31
6
DiffServ
Packet Length
TTL
Protocol
Source Address
Destination Address
Layer 4

IPv4 Header



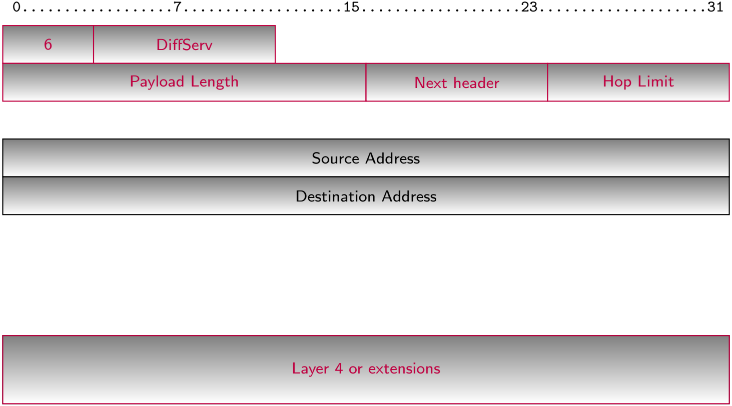
0
7
15
23
31
6
DiffServ
Payload Length
TTL
Protocol
Source Address
Destination Address
Layer 4

IPv4 Header

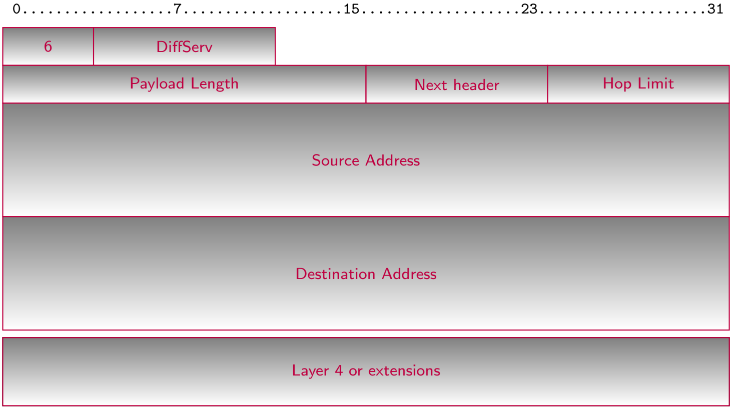


0 . . . . 7 . . . . 15 . . . . 23 31
6
DiffServ
Payload Length
Next header
TTL
Source Address
Destination Address
Layer 4 or extensions

IPv4 Header

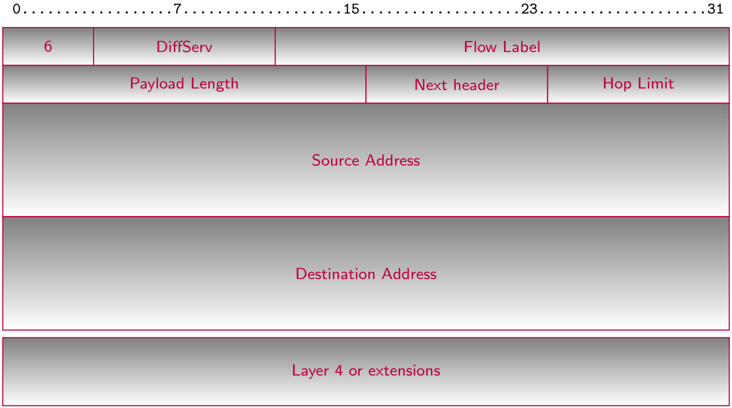

0..................7..................15..................23..................31
6
DiffServ
Payload Length
Next header
Hop Limit
Source Address
Destination Address
Layer 4 or extensions

IPv4 Header



0.................7..................15..................23...................31
6
DiffServ
Payload Length
Next header
Hop Limit
Source Address
Destination Address
Layer 4 or extensions

IPv6 Header



0..................7..................15..................23..................31
6
DiffServ
Flow Label
Payload Length
Next header
Hop Limit
Source Address
Destination Address
Layer 4 or extensions

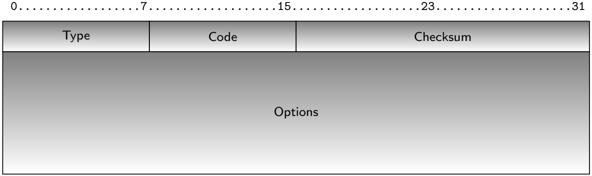
Protocol

ICMPv6

ICMPv6

- ICMPv6 is different from ICMP for IPv4 (RFC 4443)
  - IPv6 (or extension): 58
- Features are extended and better organized
- Never filter ICMPv6 messages blindly, be careful to what you do (see RFC 4890)

Format :



Precision

type code nature of the message ICMPv6
code specifies the cause of the message ICMPv6
mandatory *checksum* used to verify the integrity of ICMP packet

ICMPv6 : Two Functions

- Error occurs during forwarding (*value* < 128)

1	Destination Unreachable
2	Packet Too Big
3	Time Exceeded
4	Parameter Problem

- Management Applications (*value* > 128)

128	Echo Request
129	Echo Reply
130	Group Membership Query
131	Group Membership Report
132	Group Membership Reduction
133	Router Solicitation
134	Router Advertisement
135	Neighbor Solicitation
136	Neighbor Advertisement
137	Redirect

Associated Protocols & Mechanisms

Neighbor Discovery

Neighbor Discovery (RFC 4861)

- IPv6 nodes sharing the same physical medium (link) use Neighbor Discovery (ND) to:
  - determine link-layer addresses of their neighbors
    - IPv4 : ARP
  - Address auto-configuration
    - Layer 3 parameters: IPv6 address, default route, MTU and Hop Limit
    - Only for hosts !
    - IPv4 : impossible, mandate a centralized DHCP server
  - Duplicate Address Detection (DAD)
    - IPv4 : gratuitous ARP
  - maintain neighbors reachability information (NUD)
- Mainly uses multicast addresses but also takes into account NBMA Networks (eg., ATM)
- Protocol packets are transported/encapsulated by/in ICMPv6 messages:
  - Router Solicitation: 133 ; Router Advertisement: 134 ; Neighbor Solicitation: 135 ; Neighbor Advertisement: 136 ; Redirect: 137

Neighbor Discovery (RFC 4861)

- IPv6 nodes sharing the same physical medium (link) use Neighbor Discovery (ND) to:
  - determine link-layer addresses of their neighbors
    - IPv4 : ARP
  - Address auto-configuration
    - Layer 3 parameters: IPv6 address, default route, MTU and Hop Limit
    - Only for hosts !
    - IPv4 : impossible, mandate a centralized DHCP server
  - Duplicate Address Detection (DAD)
    - IPv4 : gratuitous ARP
  - maintain neighbors reachability information (NUD)
- Mainly uses multicast addresses but also takes into account NBMA Networks (eg., ATM)
- Protocol packets are transported/encapsulated by/in ICMPv6 messages:
  - Router Solicitation: 133 ; Router Advertisement: 134 ; Neighbor Solicitation: 135 ; Neighbor Advertisement: 136 ; Redirect: 137

Neighbor Discovery (RFC 4861)

- IPv6 nodes sharing the same physical medium (link) use Neighbor Discovery (ND) to:
  - determine link-layer addresses of their neighbors
    - IPv4 : ARP
  - Address auto-configuration
    - Layer 3 parameters: IPv6 address, default route, MTU and Hop Limit
    - Only for hosts !
    - IPv4 : impossible, mandate a centralized DHCP server
  - Duplicate Address Detection (DAD)
    - IPv4 : gratuitous ARP
  - maintain neighbors reachability information (NUD)
- Mainly uses multicast addresses but also takes into account NBMA Networks (eg., ATM)
- Protocol packets are transported/encapsulated by/in ICMPv6 messages:
  - Router Solicitation: 133 ; Router Advertisement: 134 ; Neighbor Solicitation: 135 ; Neighbor Advertisement: 136 ; Redirect: 137

Neighbor Discovery (RFC 4861)

- IPv6 nodes sharing the same physical medium (link) use Neighbor Discovery (ND) to:
  - determine link-layer addresses of their neighbors
    - IPv4 : ARP
  - Address auto-configuration
    - Layer 3 parameters: IPv6 address, default route, MTU and Hop Limit
    - Only for hosts !
    - IPv4 : impossible, mandate a centralized DHCP server
  - Duplicate Address Detection (DAD)
    - IPv4 : gratuitous ARP
  - maintain neighbors reachability information (NUD)
- Mainly uses multicast addresses but also takes into account NBMA Networks (eg., ATM)
- Protocol packets are transported/encapsulated by/in ICMPv6 messages:
  - Router Solicitation: 133 ; Router Advertisement: 134 ; Neighbor Solicitation: 135 ; Neighbor Advertisement: 136 ; Redirect: 137

Neighbor Discovery (RFC 4861)

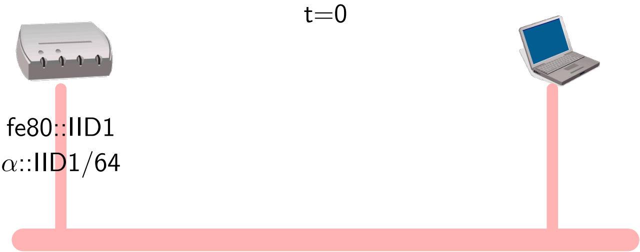
- IPv6 nodes sharing the same physical medium (link) use Neighbor Discovery (ND) to:
  - determine link-layer addresses of their neighbors
    - IPv4 : ARP
  - Address auto-configuration
    - Layer 3 parameters: IPv6 address, default route, MTU and Hop Limit
    - Only for hosts !
    - IPv4 : impossible, mandate a centralized DHCP server
  - Duplicate Address Detection (DAD)
    - IPv4 : gratuitous ARP
  - maintain neighbors reachability information (NUD)
- Mainly uses multicast addresses but also takes into account NBMA Networks (eg., ATM)
- Protocol packets are transported/encapsulated by/in ICMPv6 messages:
  - Router Solicitation: 133 ; Router Advertisement: 134 ; Neighbor Solicitation: 135 ; Neighbor Advertisement: 136 ; Redirect: 137

Neighbor Discovery (RFC 4861)

- IPv6 nodes sharing the same physical medium (link) use Neighbor Discovery (ND) to:
  - determine link-layer addresses of their neighbors
    - IPv4 : ARP
  - Address auto-configuration
    - Layer 3 parameters: IPv6 address, default route, MTU and Hop Limit
    - Only for hosts !
    - IPv4 : impossible, mandate a centralized DHCP server
  - Duplicate Address Detection (DAD)
    - IPv4 : gratuitous ARP
  - maintain neighbors reachability information (NUD)
- Mainly uses multicast addresses but also takes into account NBMA Networks (eg., ATM)
- Protocol packets are transported/encapsulated by/in ICMPv6 messages:
  - Router Solicitation: 133 ; Router Advertisement: 134 ; Neighbor Solicitation: 135 ; Neighbor Advertisement: 136 ; Redirect: 137

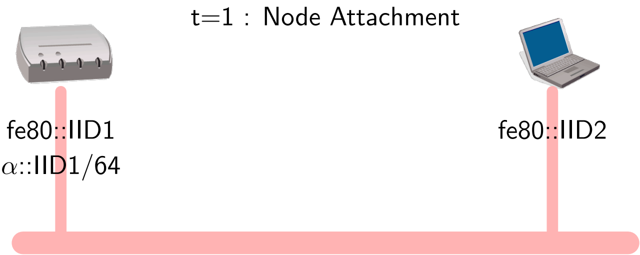
Stateless Auto-configuration: Basic Principles

Stateless Auto-configuration: Basic Principles



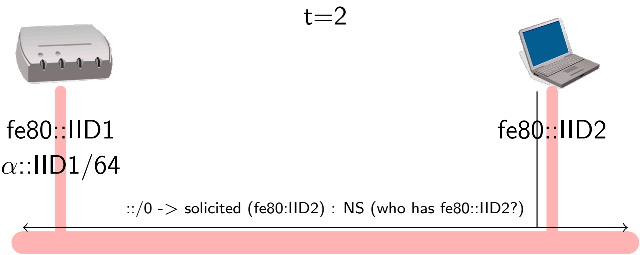
Time t=0: Router is configured with a link-local address and manually configured with a global address (α::/64 is given by the network administrator)

Stateless Auto-configuration: Basic Principles



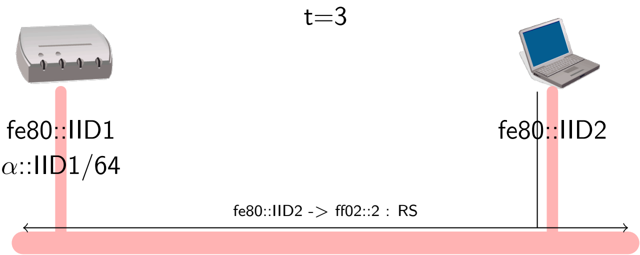
Host constructs its link-local address based on the interface MAC address

Stateless Auto-configuration: Basic Principles



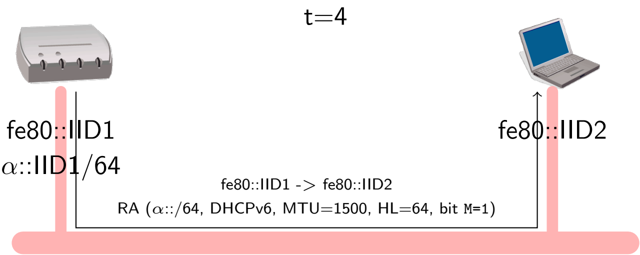
Host does a DAD (i.e. sends a Neighbor Solicitation to query resolution of its own address (tentative): no answers means no other host has this value).

Stateless Auto-configuration: Basic Principles



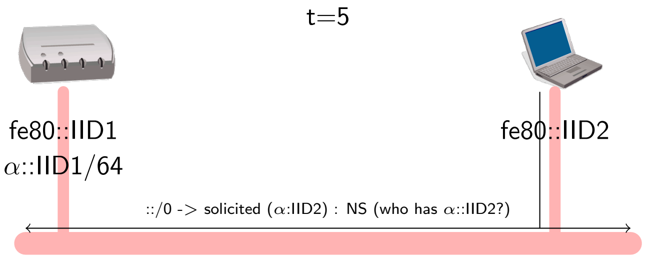
Host sends a Router Solicitation to the Link-Local All-Routers Multicast group using the newly link-local configured address

Stateless Auto-configuration: Basic Principles



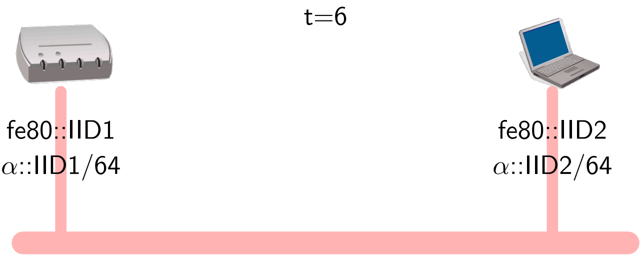
Router directly answers the host using Link-local addresses. The answer may contain a/several prefix(es). Router can also mandate hosts to use DHCPv6 to obtain prefixes (statefull auto-configuration) and/or other parameters (DNS servers...): Bit `M` = 1.

Stateless Auto-configuration: Basic Principles



Host does a DAD (i.e. sends a Neighbor Solicitation to query resolution of its own global address: no answers means no other host as this value).

Stateless Auto-configuration: Basic Principles

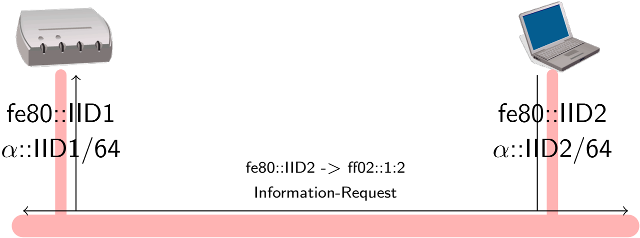


Host sets the global address and takes answering router as the default router.

Optimistic DAD RFC 4429

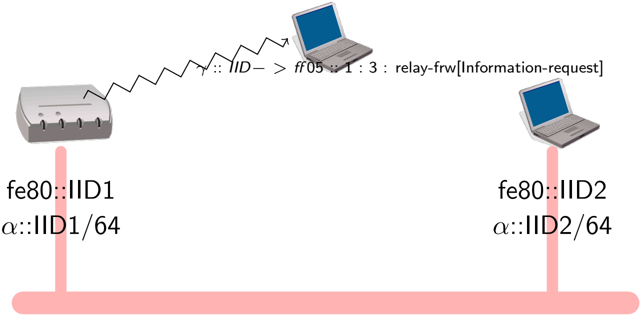
- DAD is a long process:
  - Send NS
  - Timeout
  - May be repeated
- For Link-Local and Global addresses
- Mobile nodes are penalized
  - Discover Network
  - Authentication
  - DAD, RS/RA, DAD
- oDAD allows a host to use the address before DAD
- If no answer to DAD then the address becomes a valid one

Stateless DHCPv6 (RFC 3736): With static parameters



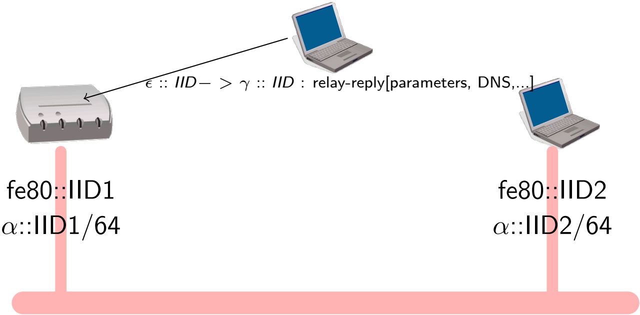
Host needs only static parameters (DNS, NTP,...). It sends an Information-Request message to All_DHCP_Agents multicast group. The scope of this address is link-local.

Stateless DHCPv6 (RFC 3736): With static parameters



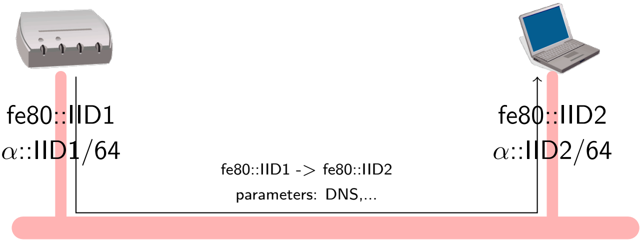
A relay (generally the router) encapsulates the request into a *Forward message and sends it either to the All_DHCP_Servers site-local multicast group or to a list of pre-defined unicast addresses.*

Stateless DHCPv6 (RFC 3736): With static parameters



The server responds to the relay

Stateless DHCPv6 (RFC 3736): With static parameters



The router extracts information from the message to create answer and sends information to the host

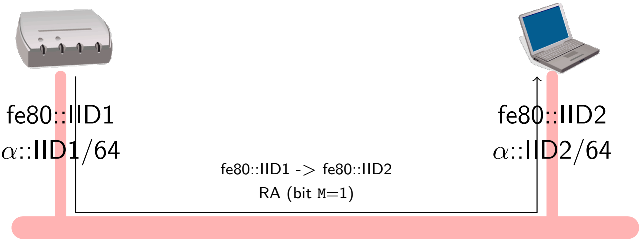
Stateless DHCPv6 (RFC 3736): With static parameters

Host is now configured to resolve domain names through the DNS

Associated Protocols & Mechanisms

DHCPv6

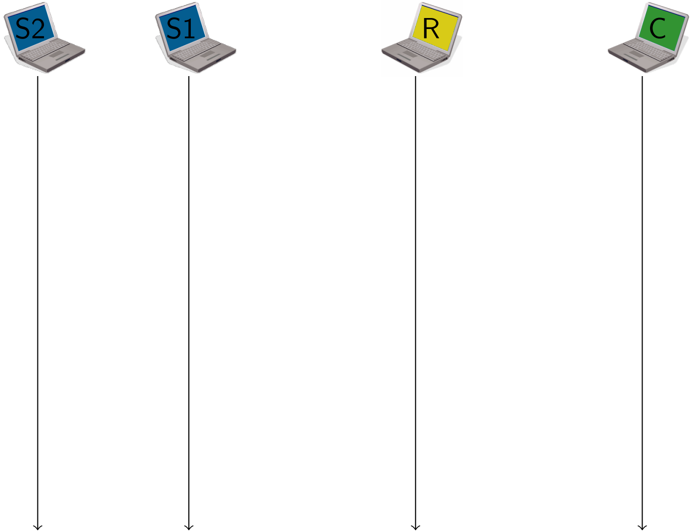
DHCPv6 : Stateful Auto-Configuration



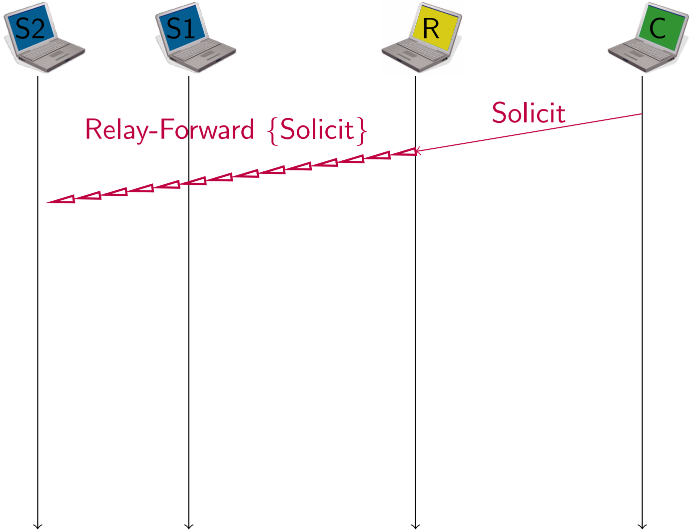
Router responds to RS with a RA message with bit `M` set to 1. Host should request its IPv6 address from a DHCPv6 server.

DHCPv6 Full Features

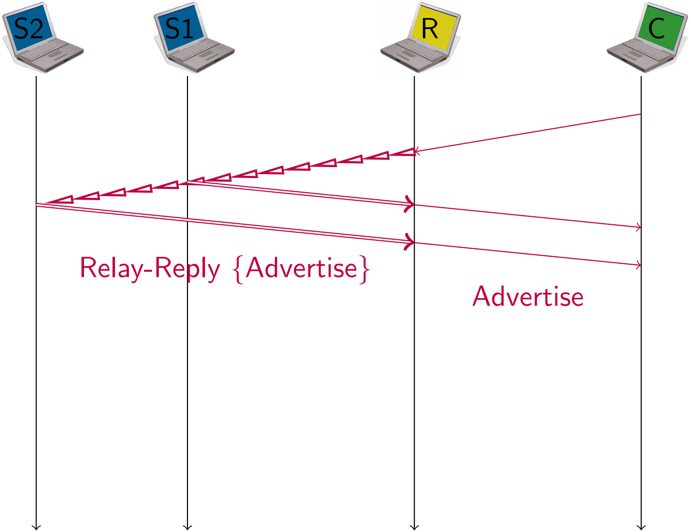
- For address or prefix allocation information form only one DHCPv6 must be taken into account. Four message exchange :
  - Solicit : send by clients to locate servers
  - Advertise : send by servers to indicate services available
  - Request : send by client to a specific server (could be through relays)
  - Reply : send by server with parameters requested
- Addresses or Prefixes are allocated for certain period of time
  - Renew : Send by the client tells the server to extend lifetime
  - Rebind : If no answer from renew, the client use rebind to extend lifetime of addresses and update other configuration parameters
  - Reconfigure : Server informs availability of new or update information. Clients can send renew or Information-request
  - Release : Send by the client tells the server the client does not need any longer addresses or prefixes.
  - Decline : to inform server that allocated addresses are already in use on the link


S2
S1
R
C

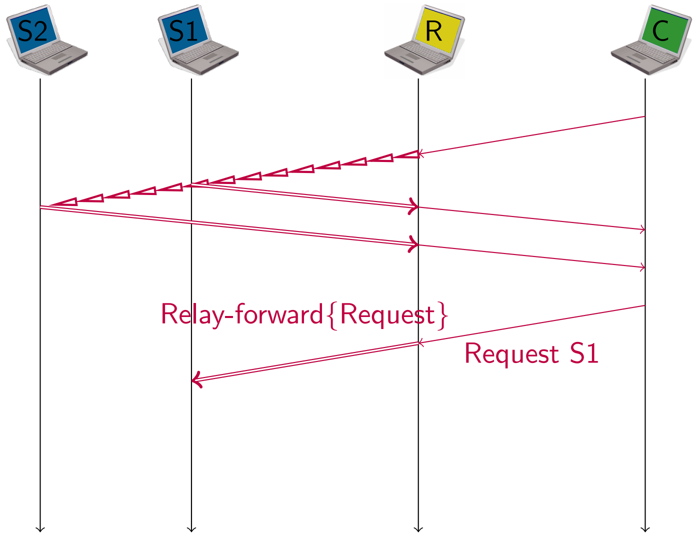
DHCPv6 Scenarii



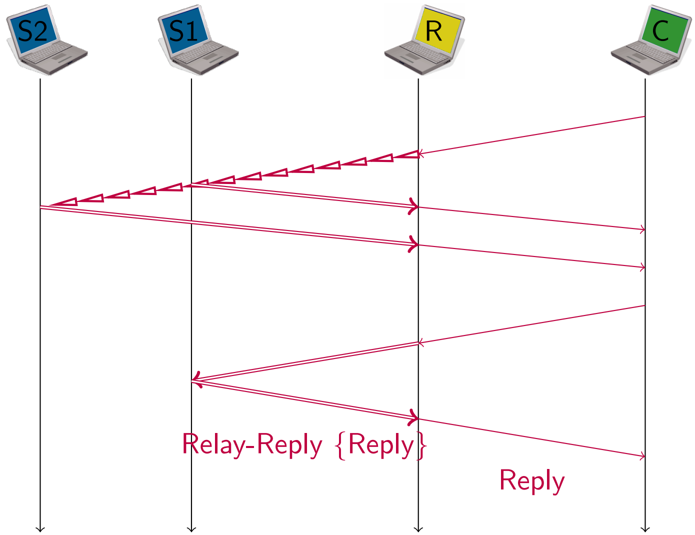
DHCPv6 Scenarii



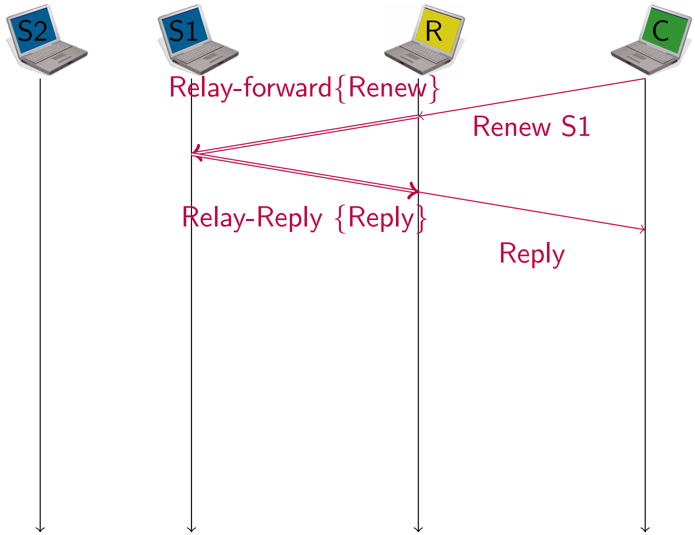
DHCPv6 Scenarii



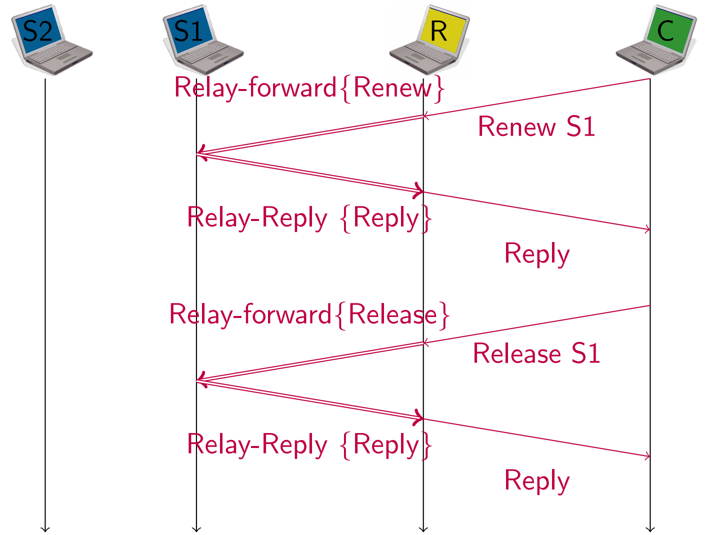
DHCPv6 Scenarii



DHCPv6 Scenarii



DHCPv6 Scenarii



Strategy

How to introduce IPv6 ?

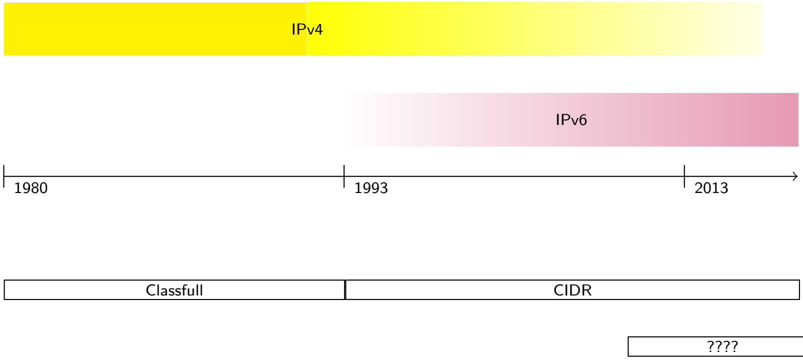
How to introduce IPv6?

- Renater: native
- Free: 6rd
- but why ?
  - No services
  - But no more IPv4 addresses for services
  - Use IPv6 in provider network and tunnel IPv4 packets inside IPv6 packets
  - Put NAT inside provider network
  - One IPv4 address can be shared among several users ?
  - How many users ?
- More difficult to install a server
  - No wellknow port
  - New services with IPv6?

Change Security

IPv6 Format Versus Addresses

Addresses versus Packet Format



Change Security

Devil is in details

What is changing?

- In theory
  - minor changes
  - Use CIDR rules
    - No Multi-Homing
    - Use PI
    - One Prefix per site
  - Same routing protocols
  - Same Firewalls
    - Extensions not used
    - Blocking incoming traffic
    - Too restrictive ?
- In practice
  - New implementation $\Rightarrow$ New bugs
  - Transition mechanisms $\Rightarrow$ Tunneled traffic
  - System administrator does not manage addresses but prefixes
  - New protocol: Neighbor Discovery

What is changing?

- In theory
  - minor changes
  - Use CIDR rules
    - No Multi-Homing
    - Use PI
    - One Prefix per site
  - Same routing protocols
  - Same Firewalls
    - Extensions not used
    - Blocking incoming traffic
    - Too restrictive ?
- In practice
  - New implementation ⇒ New bugs
  - Transition mechanisms ⇒ Tunneled traffic
  - System administrator does not manage addresses but prefixes
  - New protocol: Neighbor Discovery

What is changing?

- In theory
  - minor changes
  - Use CIDR rules
    - No Multi-Homing
    - Use PI
    - One Prefix per site
  - Same routing protocols
  - Same Firewalls
    - Extensions not used
    - Blocking incoming traffic
    - Too restrictive ?
- In practice
  - New implementation ⇒ New bugs
  - Transition mechanisms ⇒ Tunneled traffic
  - System administrator does not manage addresses but prefixes
  - New protocol: Neighbor Discovery

Eduroam

- Charter:

```
L'établissement doit garder les traces nécessaires
à l'identification d'un usager à partir de l'adresse
IP utilisée en cas d'abus constaté :
accounting RADIUS, logs DHCP, NAT,...
Ces traces doivent comporter un horodatage fiable.
```

- No more NAT, No more DHCP
  - RADIUS will authorize users, but does not know the source IID
  - Works now but limit IPv6 flexibility.
  - Everything is in . . .

Eduroam

- Charter:

```
L'établissement doit garder les traces nécessaires
à l'identification d'un usager à partir de l'adresse
IP utilisée en cas d'abus constaté :
accounting RADIUS, logs DHCP, NAT,...
Ces traces doivent comporter un horodatage fiable.
```

- No more NAT, No more DHCP
  - RADIUS will authorize users, but does not know the source IID
  - Works now but limit IPv6 flexibility.
  - Everything is in . . .

Two approaches:

- Try to mimic IPv4 behavior
  - Mandate DHCPv6 for addresses allocation
- Adapt to IPv6
  - Development of new tools and protocols around IPv6 for management.
- What to do with stateless auto-configuration?
  - It is not a new security problem
    - Any node can announce wrong prefixes
    - in IPv4, any node can be a DHCP Server
  - but lead to configuration problems.
    - How to block wrong prefix announcement ?
    - Use Cryptographic Certificats (SEND)?
    - Good in a very control environment
    - To complex and not enough flexible in company network.

Best Current Practice

- In IPv4:
  - centralize management
  - DHCP server linked with a DNS
  - Is it realy secure ?
- In IPv6:
  - Authentication at Layer 2 ?
    - IEEE 802.1X, WPA, PANA,...
  - Who has this address ?
    - A new group SAVI allows switches to log IPv6 addresses associated to switch port.
    - IEEE 802.1 ⇒ identity/port & PANA ⇒ address/port
  - Filter RA on switch port not connected to routers

DNS registration

- In IPv4
  - DHCP server register host name and address in the DNS
  - direct and reverse
- In IPv6
  - The host cannot register easily in the DNS
    - Common key is incompatible with auto-configuration
- Do we need to register a IPv6 client in the DNS ?
  - Some applications require it
  - Is it really the good principle ? (security, confidentiality)

Next Steps ?

Change application architecture

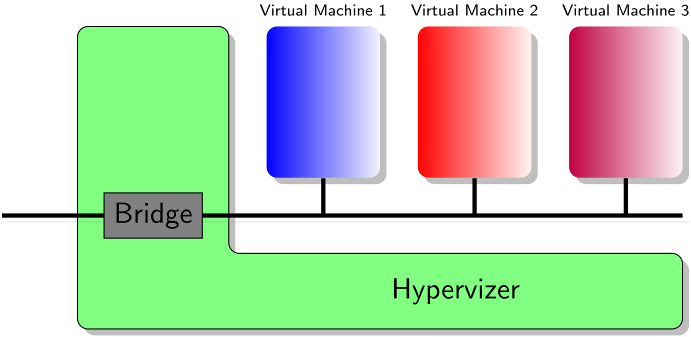
Change application architecture

- Applications are based on Client/Server paradigm.
  - Due to NAT, servers must be located in the core network.
- With IPv6, servers can be located anywhere
  - keep data localy
  - manage identity/authentication
  - make links between data
- Better control of the information
- Need for better throughput for uplinks
  - Optical fiber ?

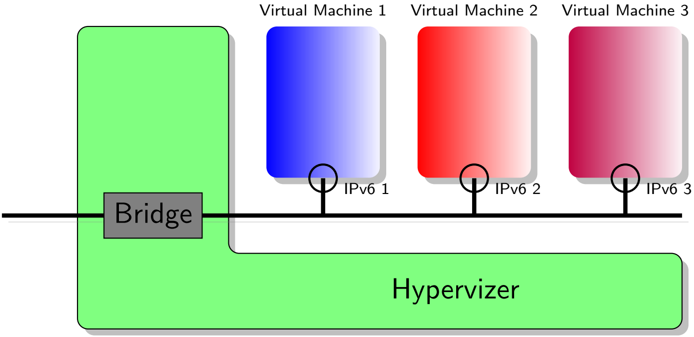
Next Steps ?

What is an address ?

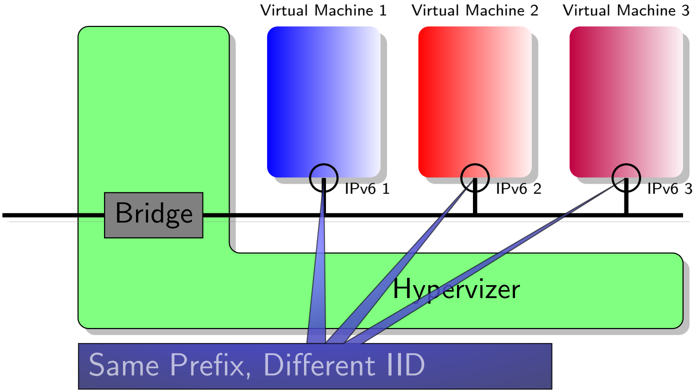
Virtualization



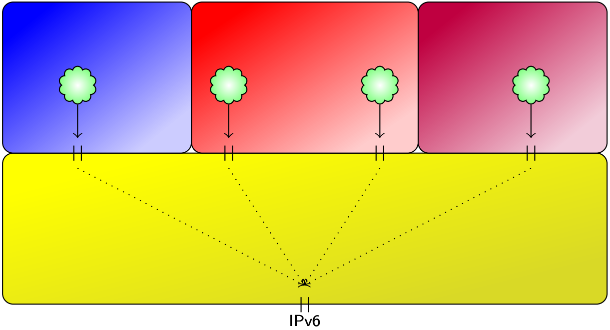
Virtualization



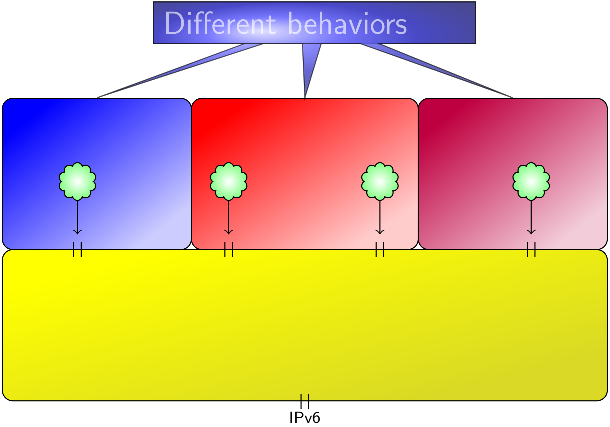
Virtualization



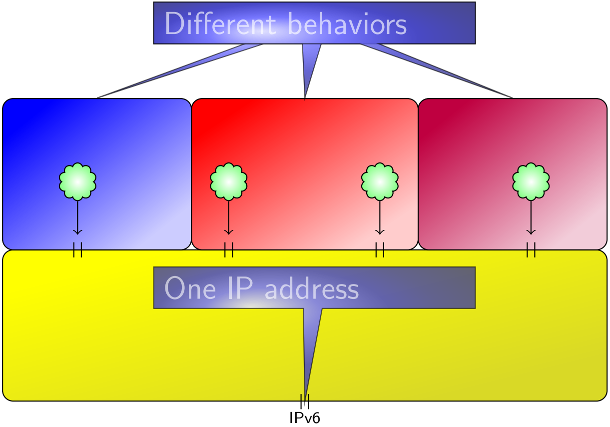
Without virtualization



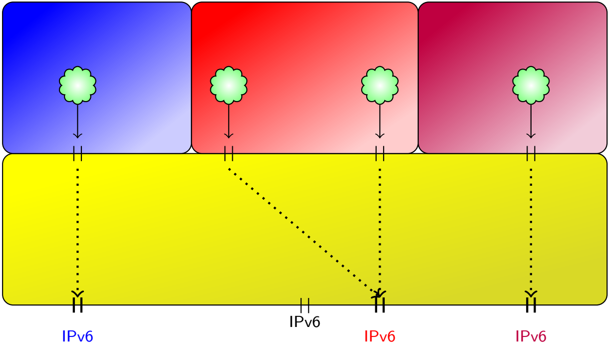
Without virtualization



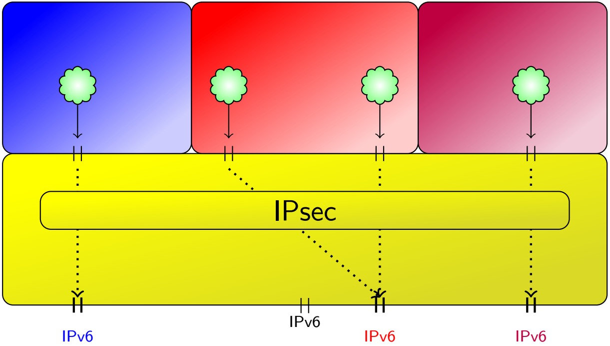
Without virtualization



Without virtualization



Without virtualization



Generalization to Identification

- Address is no more a host property, but is linked to applications
  - Use rights as for file system
- Step to separate localization and identification.
  - Prefix part used for mobility or multi-homing
  - IID: used by applications
- Identification will not be unique:
  - trade-off between Authenticated (not unique) and Anonymous.
    - Authenticated with the bank.
    - Authenticated with the IRS.
    - Authenticated with a VoIP provider.
    - Anonymous on the web.

Conclusion

Conclusion

1. IPv6 is coming
   - There is no other alternative
2. Program applications using IPv6 compatible API
   - If addresses are sent in payload, take care of IPv6
3. Think differently:
   - Servers are not always far-away
4. Internet v4 evolution was blocked by the address space
   - Everything become possible with IPv6

http://G6.asso.fr/livre

Conclusion

Facts on Addresses
Addresses
Protocol
Associated Protocols & Mechanisms
Strategy
Change Security
Next Steps ?
Conclusion

1. IPv6 is coming
   - There is no other alternative
2. Program applications using IPv6 compatible API
   - If addresses are sent in payload, take care of IPv6
3. Think differently:
   - Servers are not always far-away
4. Internet v4 evolution was blocked by the address space
   - Everything become possible with IPv6

http://G6.asso.fr/livre

Conclusion

1. IPv6 is coming
   - There is no other alternative
2. Program applications using IPv6 compatible API
   - If addresses are sent in payload, take care of IPv6
3. Think differently:
   - Servers are not always far-away
4. Internet v4 evolution was blocked by the address space
   - Everything become possible with IPv6

http://G6.asso.fr/livre

Conclusion

1. IPv6 is coming
   - There is no other alternative
2. Program applications using IPv6 compatible API
   - If addresses are sent in payload, take care of IPv6
3. Think differently:
   - Servers are not always far-away
4. Internet v4 evolution was blocked by the address space
   - Everything become possible with IPv6

http://G6.asso.fr/livre