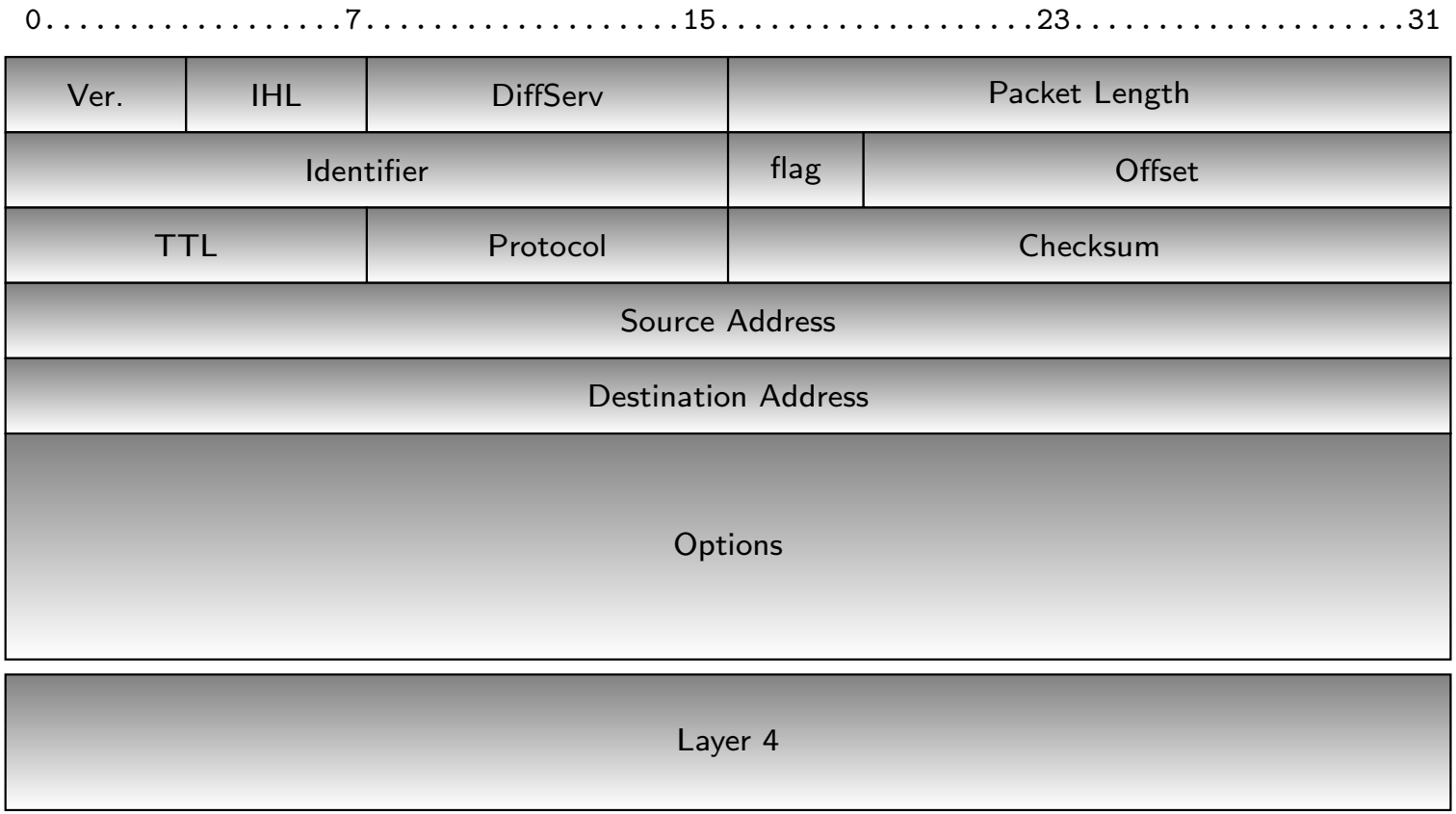
TD RNG 2

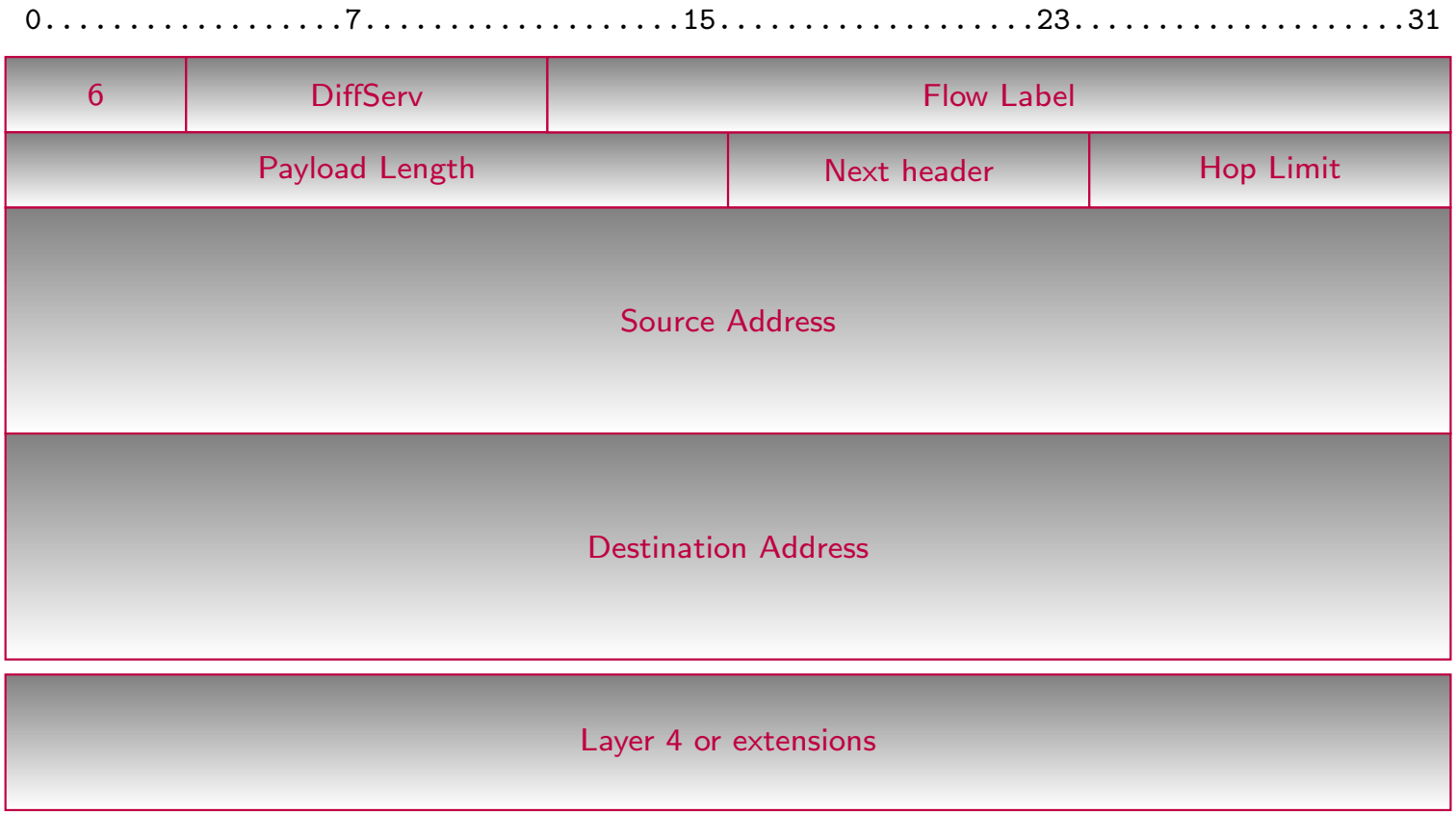
B.Stévant

En-tête des protocoles IP

IPv4 Header



IPv6 Header



Adresses IPv6

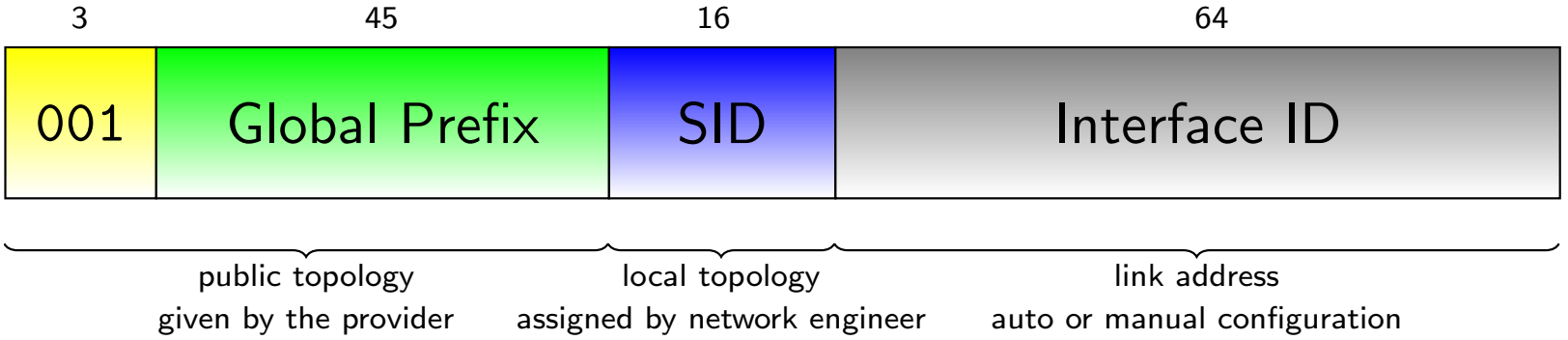
Addressing Space Utilization


```
0000::/8 Reserved by IETF [RFC4291]
0100::/8 Reserved by IETF [RFC4291]
0200::/7 Reserved by IETF [RFC4048]
0400::/6 Reserved by IETF [RFC4291]
0800::/5 Reserved by IETF [RFC4291]
1000::/4 Reserved by IETF [RFC4291]
2000::/3 Global Unicast [RFC4291]
4000::/3 Reserved by IETF [RFC4291]
6000::/3 Reserved by IETF [RFC4291]
8000::/3 Reserved by IETF [RFC4291]
a000::/3 Reserved by IETF [RFC4291]
c000::/3 Reserved by IETF [RFC4291]
e000::/4 Reserved by IETF [RFC4291]
f000::/5 Reserved by IETF [RFC4291]
F800::/6 Reserved by IETF [RFC4291]
fc00::/7 Unique Local Unicast [RFC4193]
fe00::/9 Reserved by IETF [RFC4291]
fe80::/10 Link Local Unicast [RFC4291]
fec0::/10 Reserved by IETF [RFC3879]
ff00::/8 Multicast [RFC4291]
```

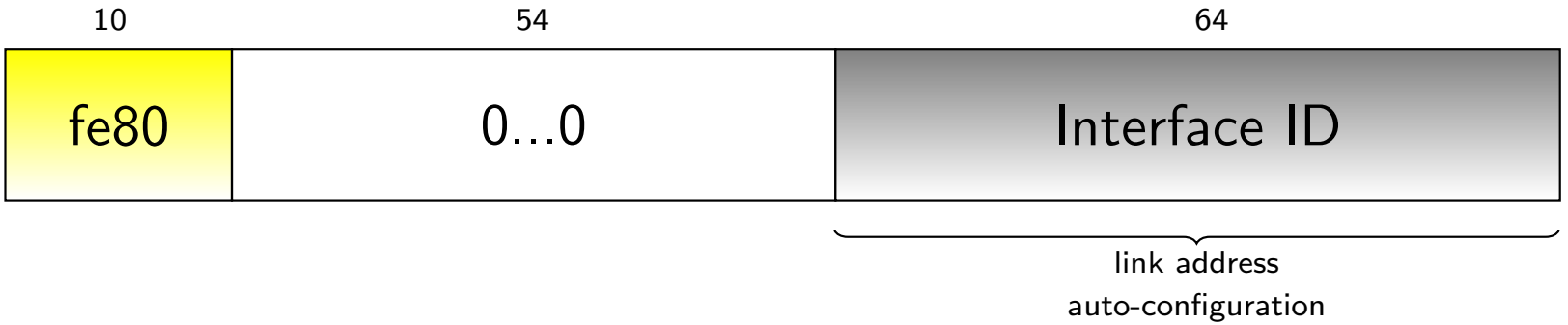
http://www.iana.org/assignments/ipv6-address-space

Address Format

Global Unicast Address:



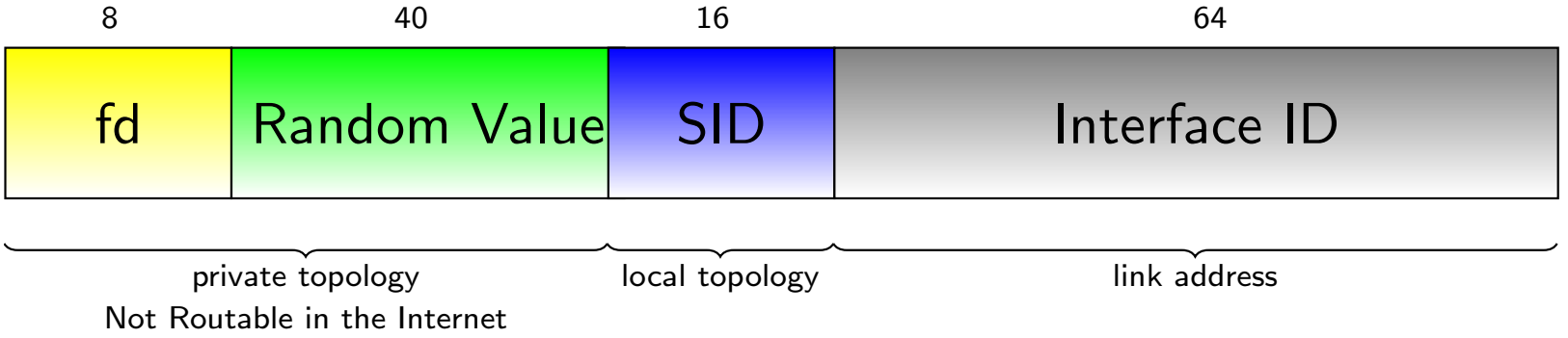
Link-Local Address:



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:

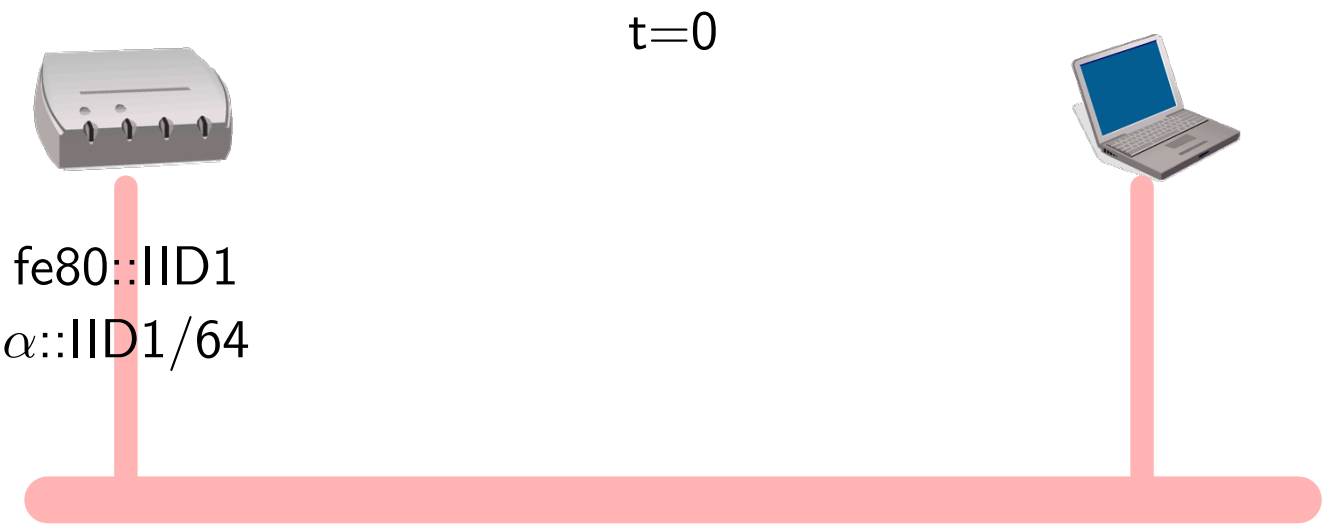


http://www.sixxs.net/tools/grh/ula/ to create your own ULA prefix.

Auto-configuration

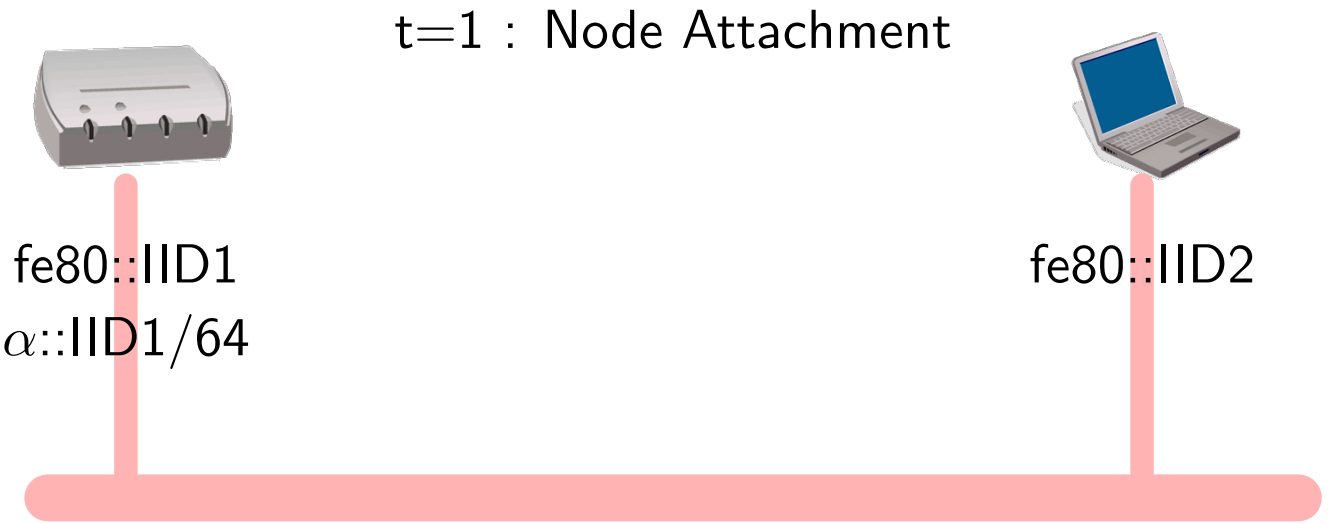
Stateless Auto-configuration: Basic Principles

Stateless Auto-configuration: Basic Principles



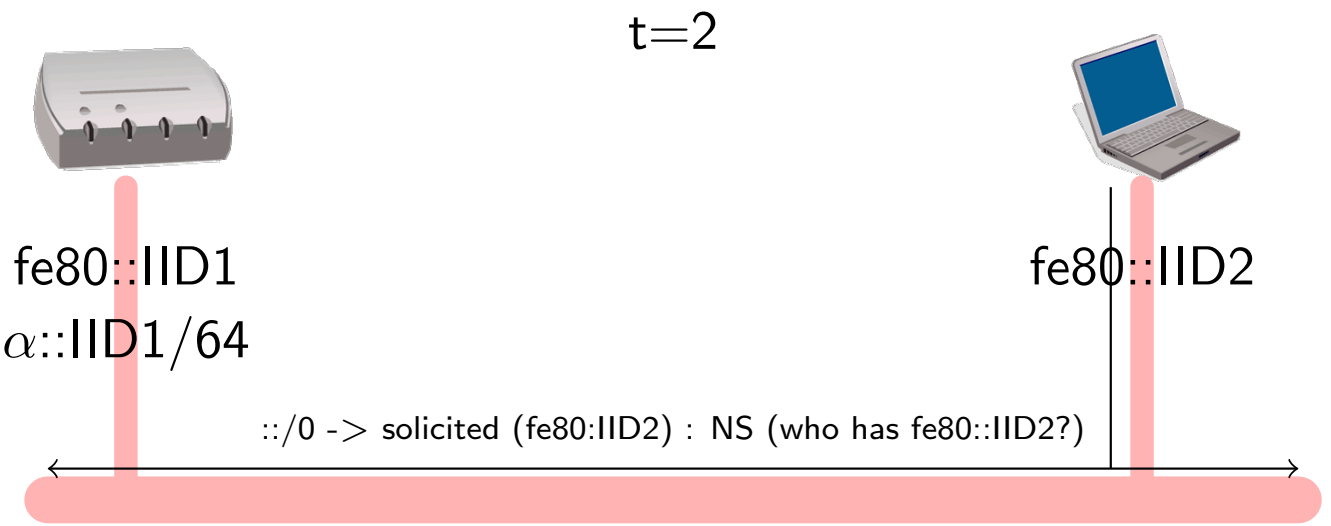
Time t=0: Router is configured with a link-local address and manually configured with a global address (α::/64 is given by the network administrator)

Stateless Auto-configuration: Basic Principles



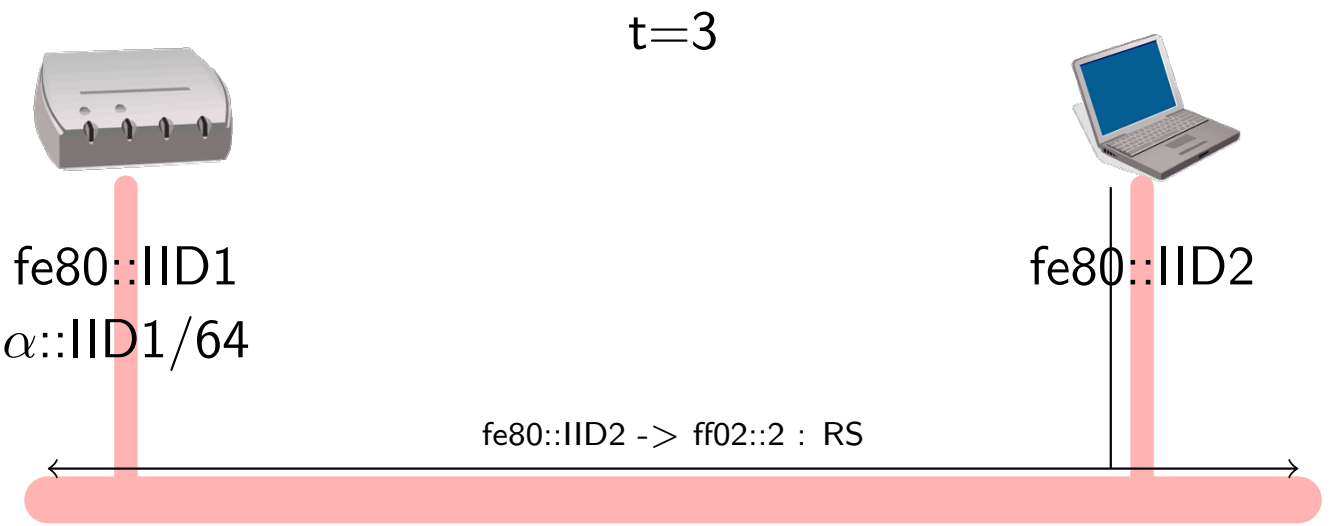
Host constructs its link-local address based on the interface MAC address

Stateless Auto-configuration: Basic Principles



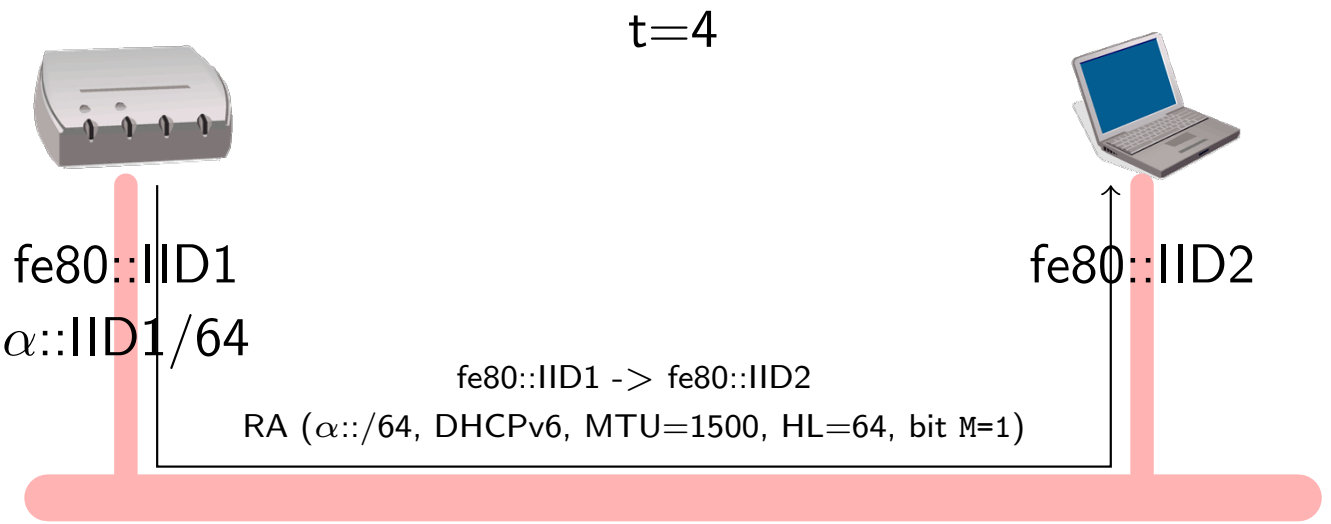
Host does a DAD (i.e. sends a Neighbor Solicitation to query resolution of its own address (tentative): no answers means no other host has this value).

Stateless Auto-configuration: Basic Principles



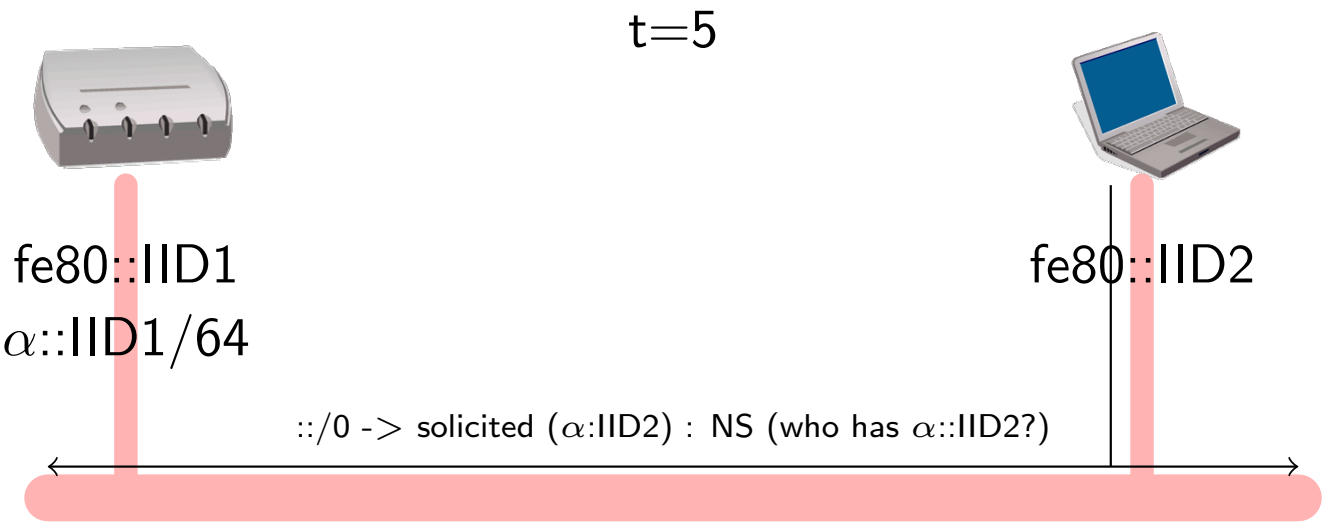
Host sends a Router Solicitation to the Link-Local All-Routers Multicast group using the newly link-local configured address

Stateless Auto-configuration: Basic Principles



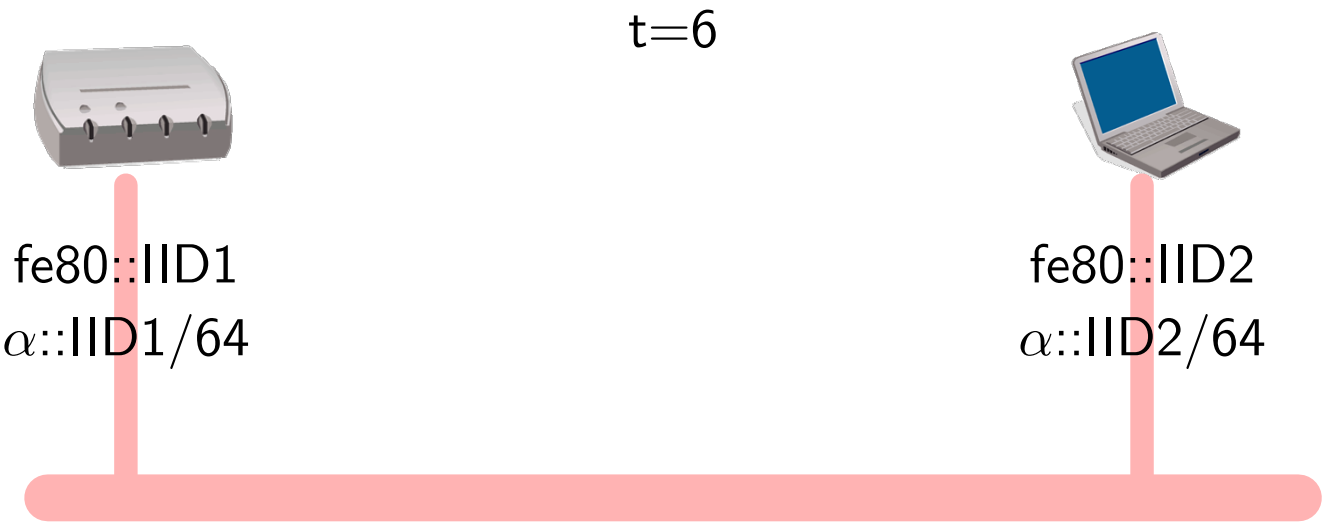
Router directly answers the host using Link-local addresses. The answer may contain a/several prefix(es). Router can also mandate hosts to use DHCPv6 to obtain prefixes (statefull auto-configuration) and/or other parameters (DNS servers...): Bit $\mathtt{M} = 1$.

Stateless Auto-configuration: Basic Principles



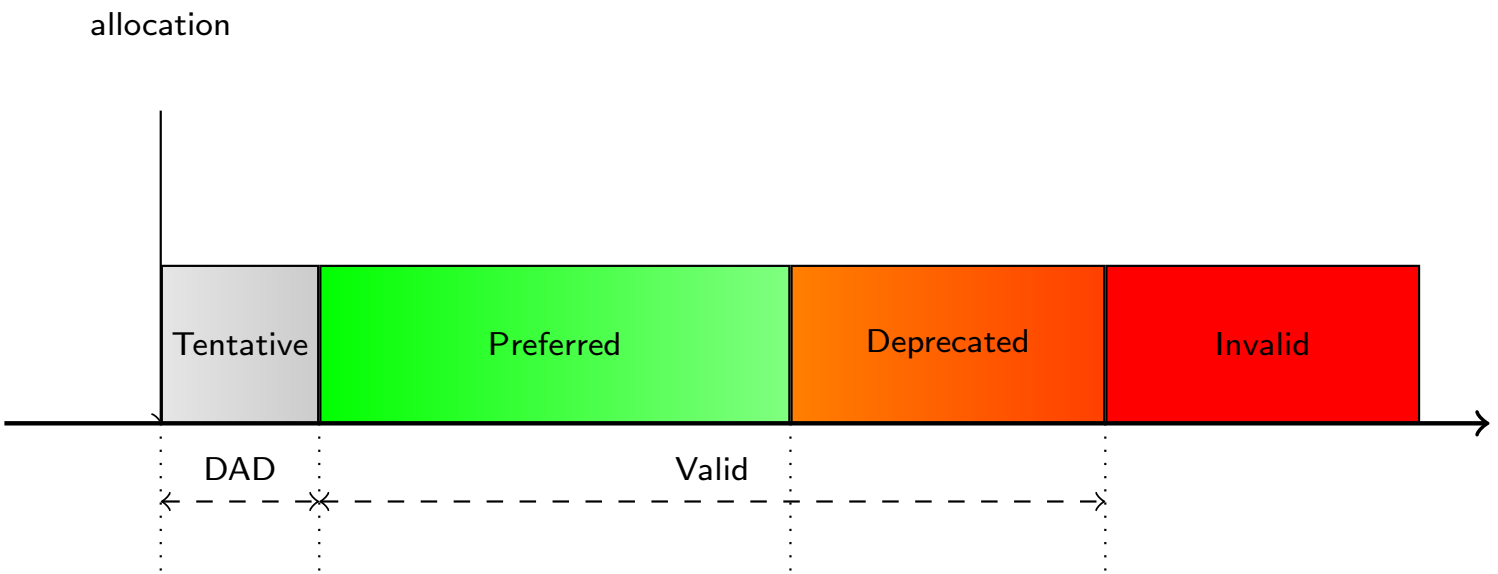
Host does a DAD (i.e. sends a Neighbor Solicitation to query resolution of its own global address: no answers means no other host as this value).

Stateless Auto-configuration: Basic Principles



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

Address Lifetime



Sécurité

Security issues with Neighbor Discovery

From an attacker point of view, IPv6 attacks are:

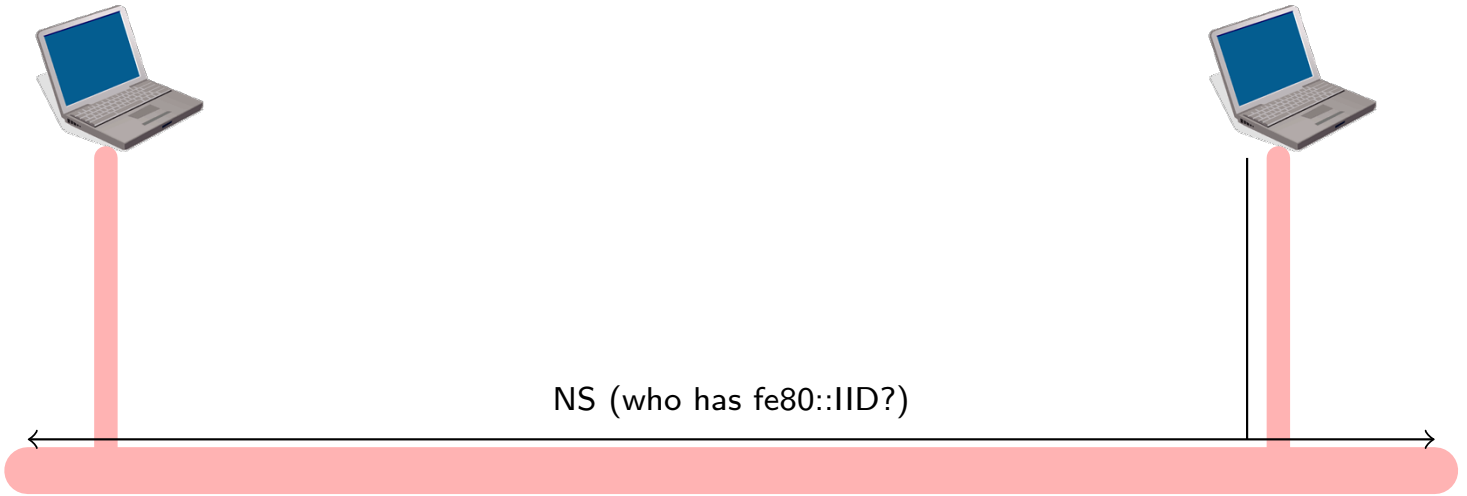
- **Difficult** from remote network:
  - Scanning IPv6 network is hard (2^{64} addresses)
    - May use random IID instead of MAC-based IID (if needed)
  - No broadcast address
  - Remote attacks would mainly target hosts exposed through the DNS
- **Easy** from local network:
  - Neighbor Discovery is basically not secured (see SEND later)
  - Attacks inspired by ARP flaws + new attacks
  - Implementations not (yet) heavily tested

Attacker toolkits already available !

See `http://www.thc.org/thc-ipv6/`

Examples of attacks using ND

Neighbor Discovery Snooping

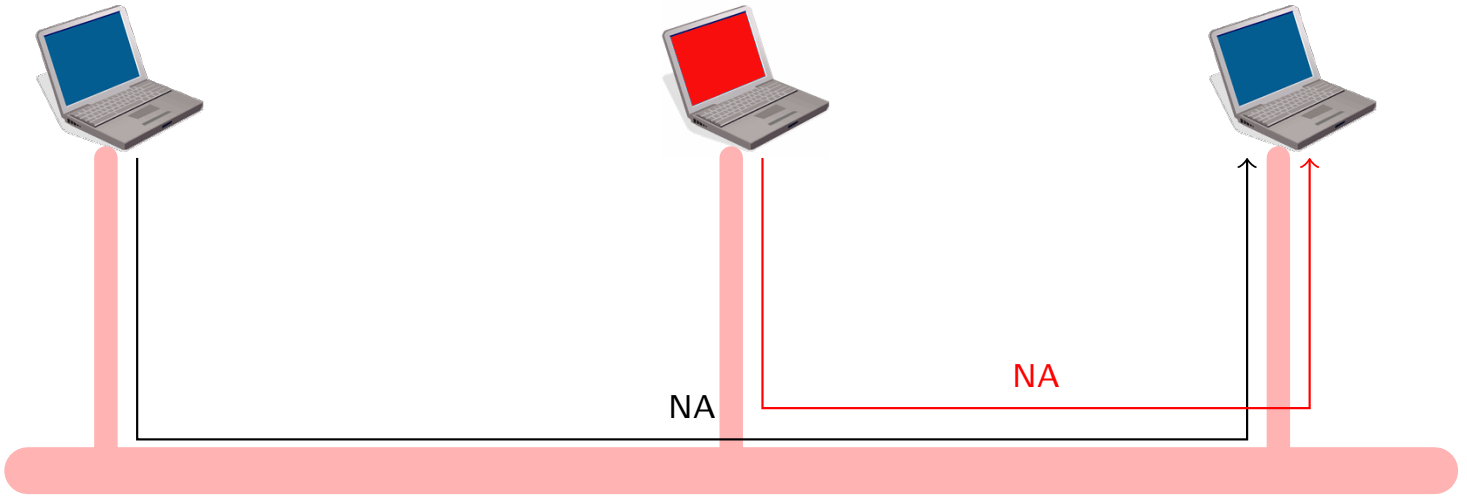


Host uses Neighbor Discovery notably in these two cases:

- To get the link-layer information (typically the MAC address) of another host (ARP-like)
- To verify address uniqueness (DAD)

Examples of attacks using ND

Neighbor Discovery Snooping

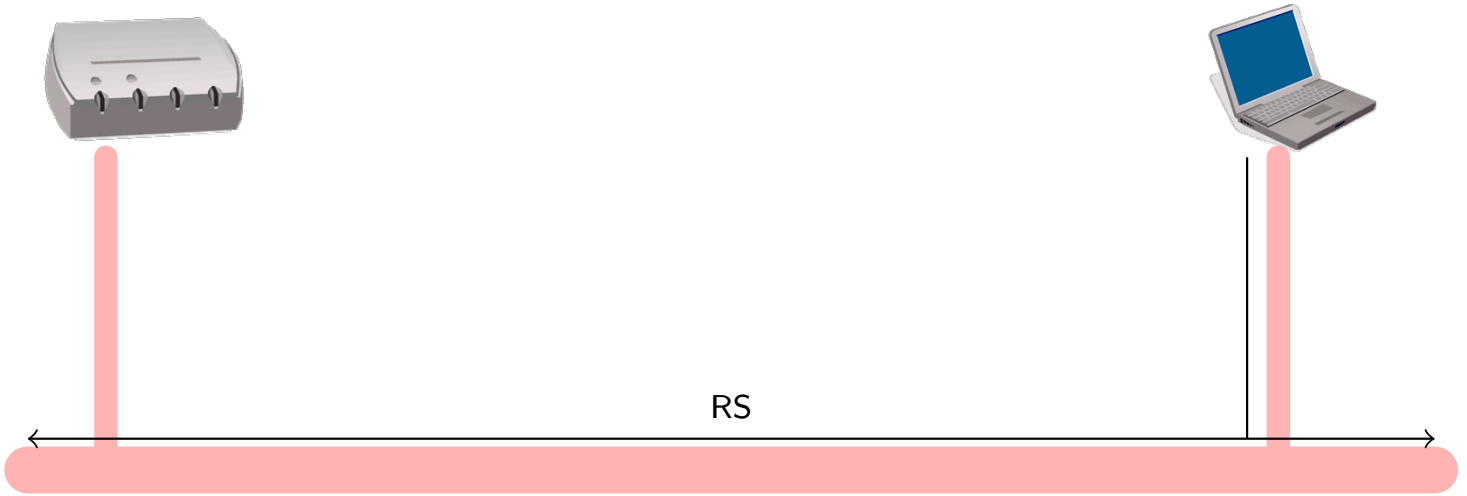


An attacker on the LAN can perform an attack by responding to ND messages

- ARP-like: Claim to be a given host on the LAN => Man in the Middle
- DAD: Claim to have any address asked for on the LAN => Deny of Service

Examples of attacks using ND

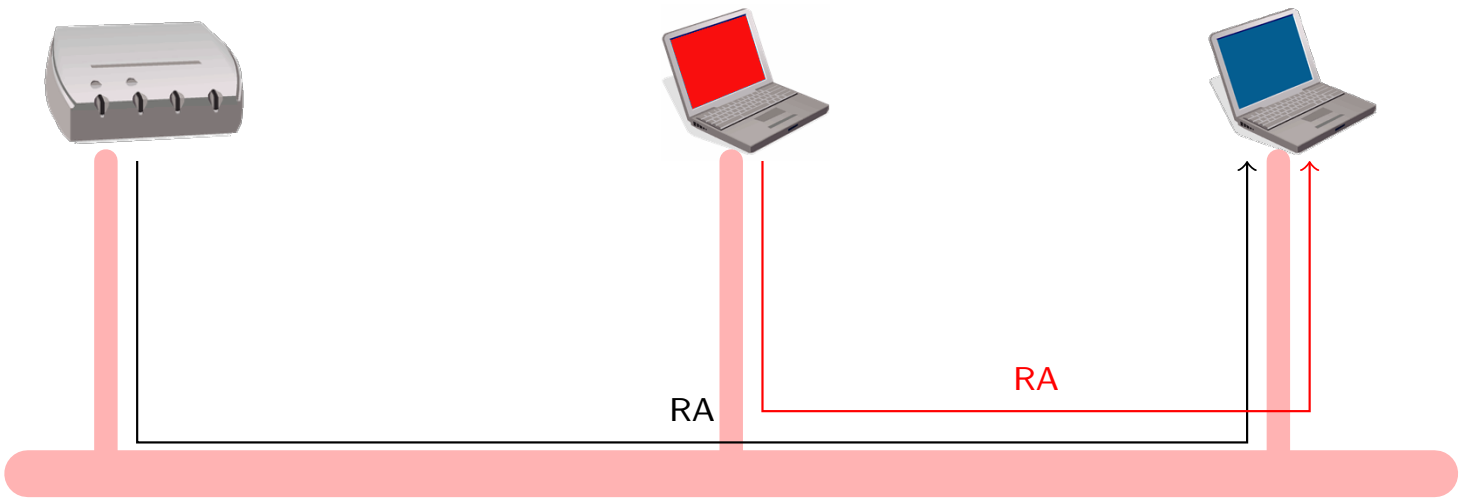
Rogue router



Host uses the Router Solicitation to get the address of the exit router and the prefix used on the LAN.

Examples of attacks using ND

Rogue router



An attacker on the LAN can perform an attack by responding to RS messages

- Claim to be the exit router => Man in the Middle
- Claim to route another prefix on the LAN => Deny of Service

Example: Interface during an IETF meeting


```
en3: flags=8863<UP,BROADCAST,SMART,RUNNING,SIMPLEX,MULTICAST> mtu 1500
   inet6 fe80::223:6cff:fe97:679c%en3 prefixlen 64 scopeid 0x6
   inet6 2002:8281:1c8c:d:223:6cff:fe97:679c prefixlen 64 autoconf
   inet6 2002:c15f:2011:d:223:6cff:fe97:679c prefixlen 64 autoconf
   inet6 fec0::d:223:6cff:fe97:679c prefixlen 64 autoconf
   inet6 2001:df8::24:223:6cff:fe97:679c prefixlen 64 autoconf
   inet 130.129.28.215 netmask 0xfffff800 broadcast 130.129.31.255
   inet6 2002:8281:1ccb:9:223:6cff:fe97:679c prefixlen 64 autoconf
   inet6 fec0::9:223:6cff:fe97:679c prefixlen 64 autoconf
   ether 00:23:6c:97:67:9c
   media: autoselect status: active
   supported media: autoselect
```

Solutions to mitigate or prevent attacks?

Prevention of attacks:

- SEND (Secure Neighbor Discovery)
  - IETF proposed solution: RFC 3971 (note: too complex to deploy for an average site!)
  - Use signed ND messages, with a trust relationship
- Level-2 Filtering
  - Filter ND on switch port (ex. only one port allowed to send RA)
  - A few switch still implements it ... (Cisco ?)

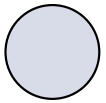
Detection of attacks: ndpmon

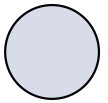
- Similar to ARP-watch
- Detect Snooping and Denial of Services
- `http://ndpmon.sf.net`

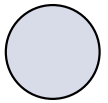
Routage par la source

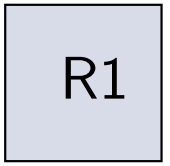
- Utilise l'extension d'en-tête « Routing » de type 0, contenant tous les points à traverser avant d'arriver à la destination

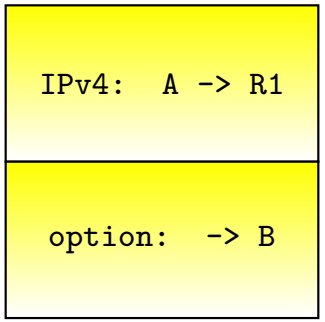
Extension Superiority

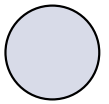


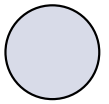




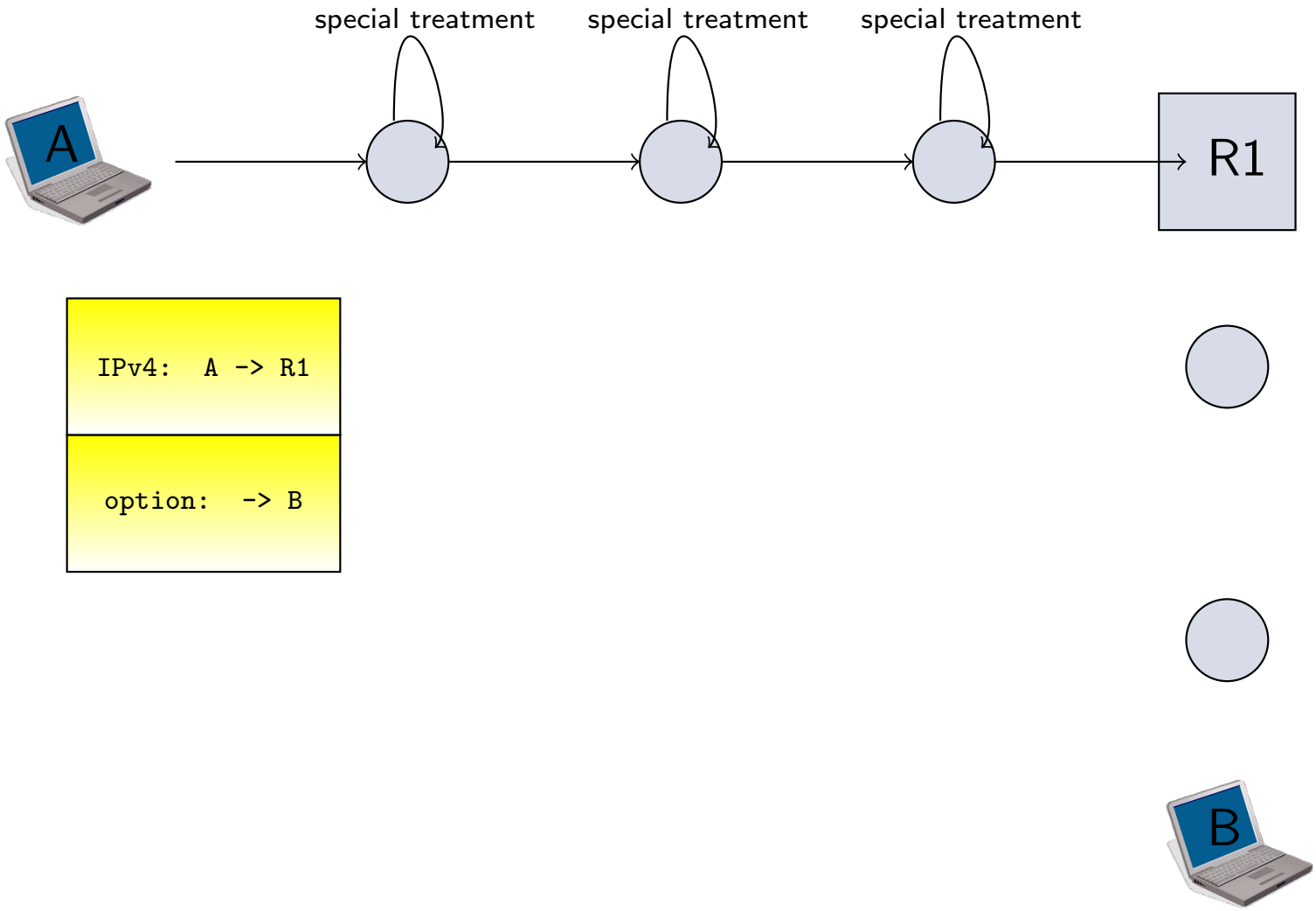




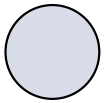


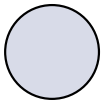


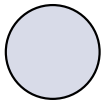
Extension Superiority

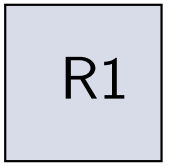


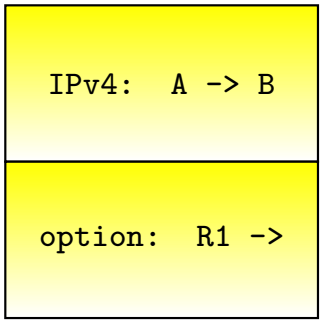
Extension Superiority

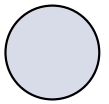


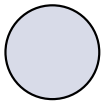




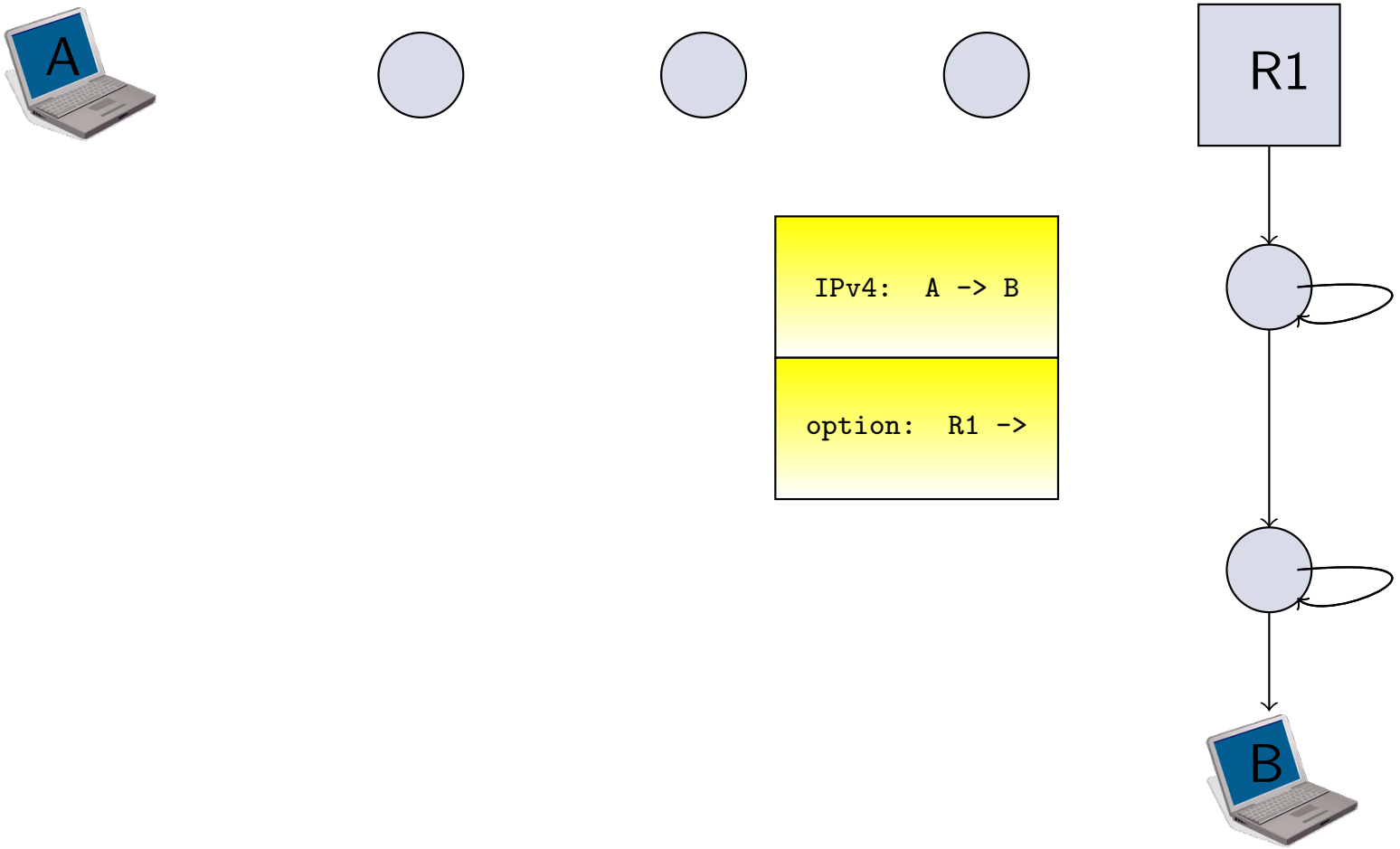




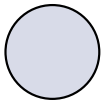


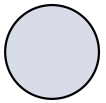


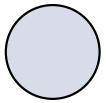
Extension Superiority

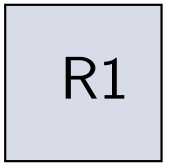


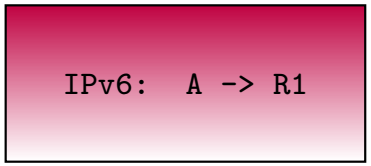
Extension Superiority

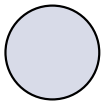


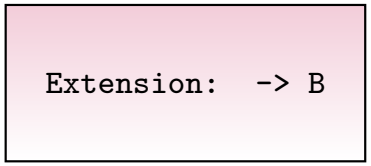


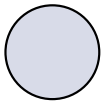




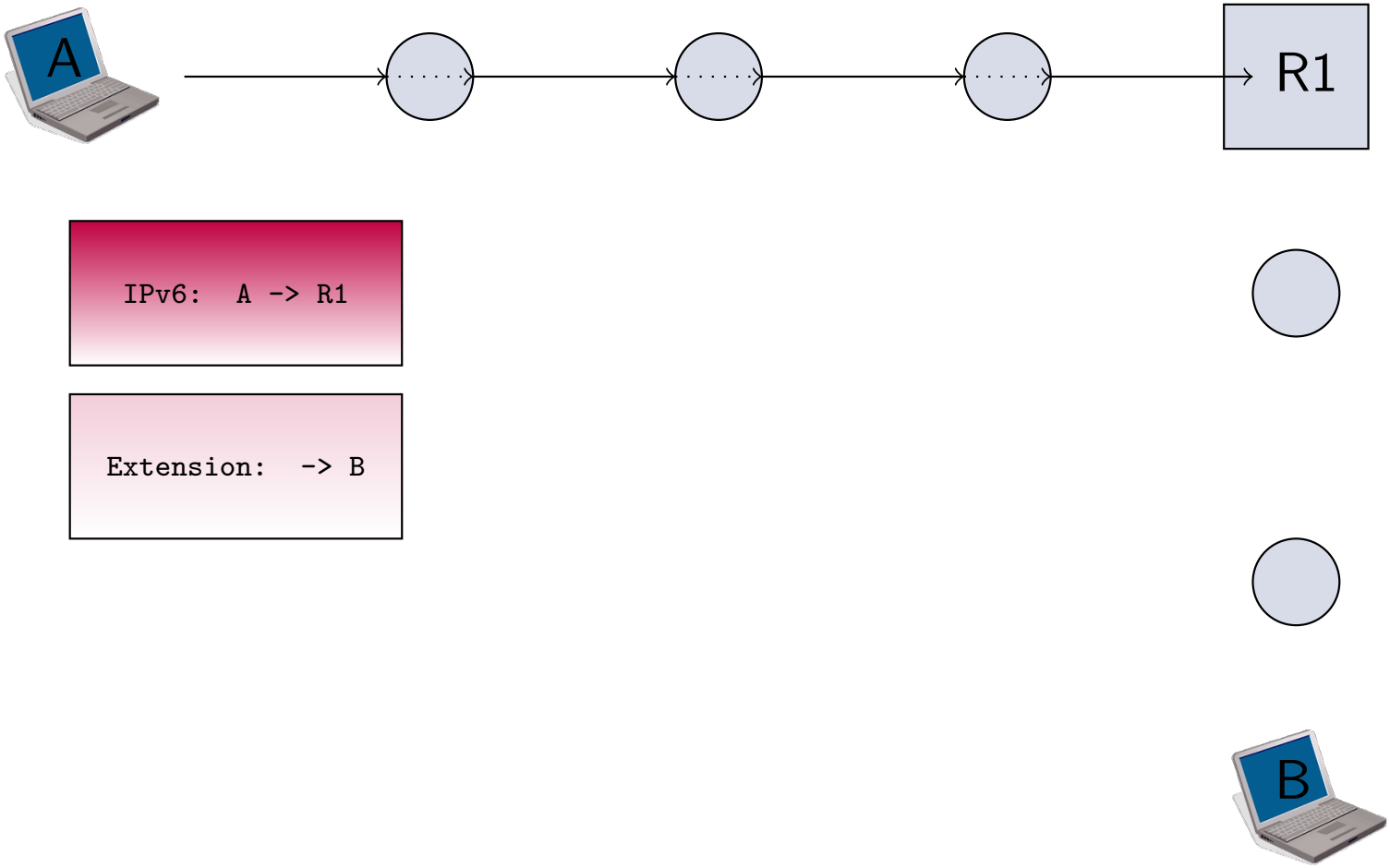




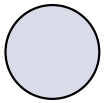


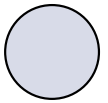


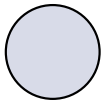
Extension Superiority

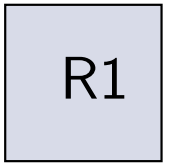


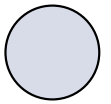
Extension Superiority



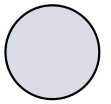




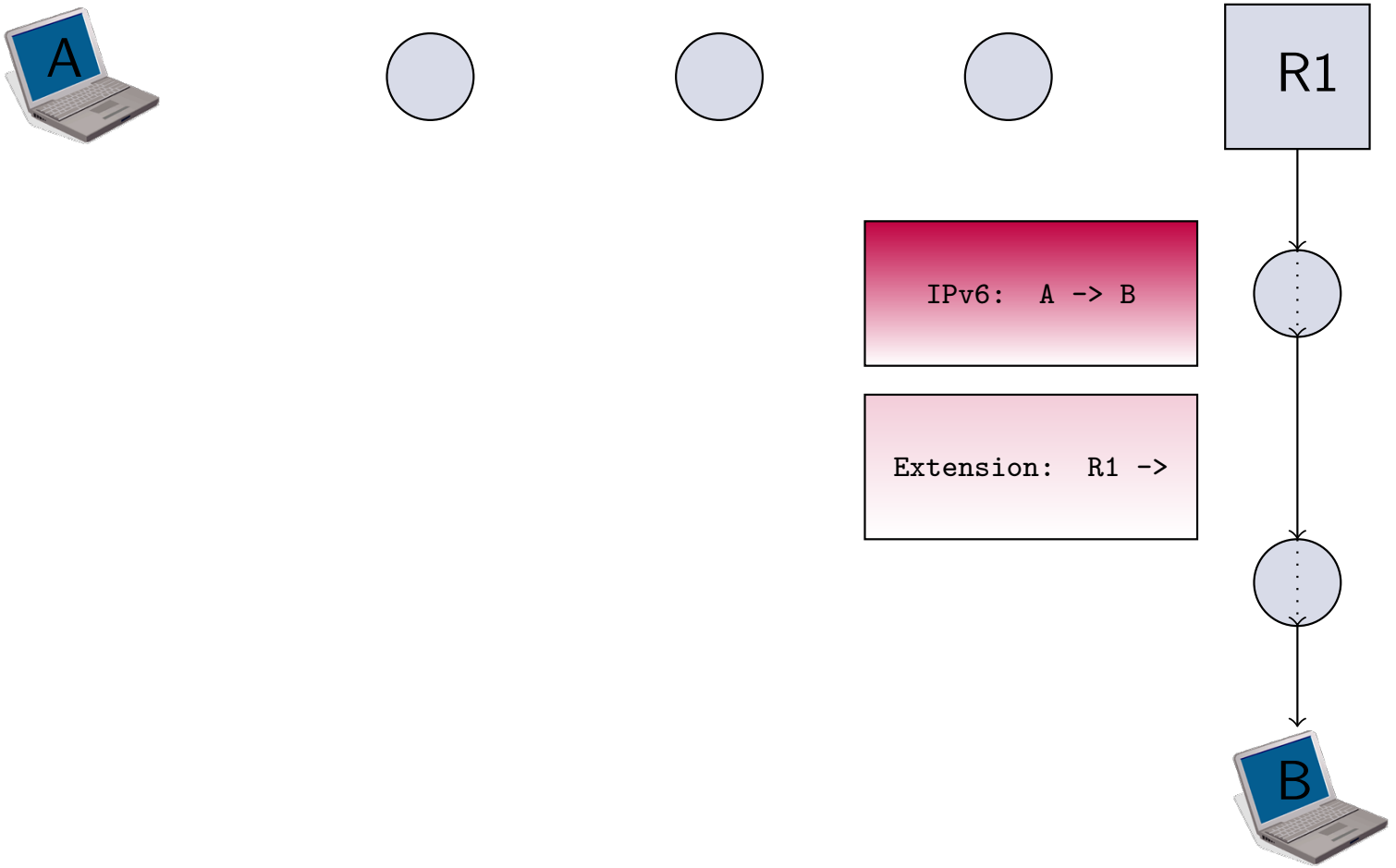




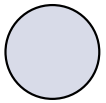
R1 is the destination, packet is sent to Routing Extension layer which swaps the addresses and forwards the packet.

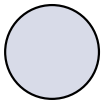


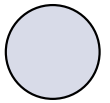
Extension Superiority

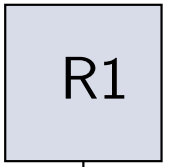


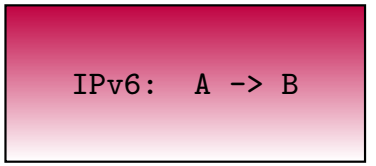
Extension Superiority

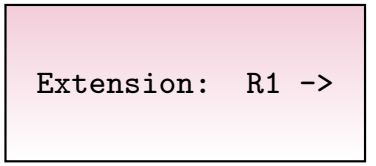


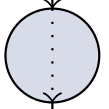


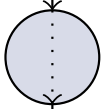












B is the destination, packet is sent to Routing Extension layer which sends it to upper layer protocol. ULP will see a packet from A to B.

Routage par la source

- Problèmes de sécurité :
  - Contournement de règles de pare-feu
    L'extension de routage peut contenir une adresse qui n'est pas dans le même plan de sécurité que l'adresse de destination du paquet
  - Amplification d'attaque, type DoS
    L'extension de routage peut spécifier des aller-retour entre 2 nœuds, surchargeant les liens

Voir http://www.secdev.org/conf/IPv6_RH_security-csw07.pdf