IPv6 Courses

©G6 Association

December 20, 2010

Table of Contents

1 Associated Protocols & Mechanisms
2 IPv6 & DNS
3 Security

G6

- Group of IPv6 actors in France (researchers, engineers. . .)
- Academic & industrial partners
  - CNRS, Institut TELECOM, INRIA, Universities. . .
  - AFNIC, 6Wind, Bull. . .
- Launched in 1995 by:
  - Alain Durand
  - Bernard Tuy
- Is today a legal association under French Law (1901)
  - Laurent Toutain, President
- For further information: http://www.g6.asso.fr/

G6Charter

- Share experience gained from IPv6 experimentations and deployment
- Spread IPv6 information
  - Tutorials and trainings (ISPs, Engineers, netadmins. . .)
  - Online book (in French), "IPv6, Théorie et pratique": http://livre.g6.asso.fr/
- Initiate research activities around IPv6
- Active in RIPE & IETF working groups
- Promotion of IPv6: French Task Force

Hypertext Symbols

- Several symbols are used in this document:
  - All RFCs and Internet Drafts are hypertext links.
    - Check that there is no more recent version of the document.
  - is a link to a *Techniques de l'Ingénieur* article on the subject (in French, access may be restricted).
  - is a link to the online edition of *IPv6, Théorie et Pratique* (in French)
  - is a link to other information on the web.
- Material concerning IPv6 is taken from the G6 tutorial and copyrighted from G6.

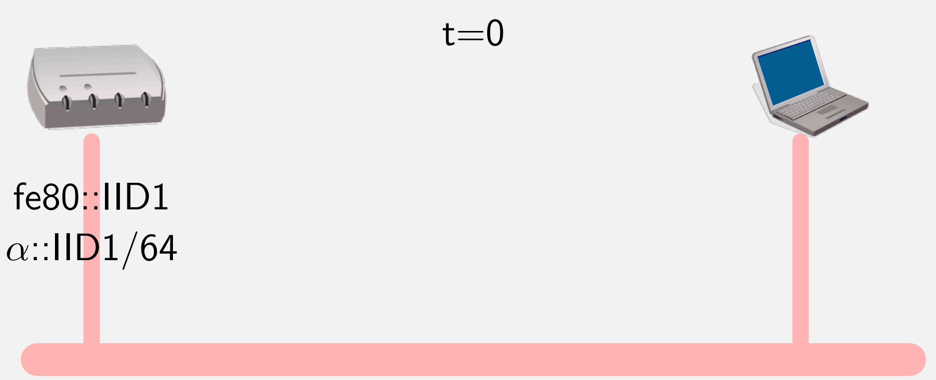
Associated Protocols & Mechanisms
Neighbor Discovery

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

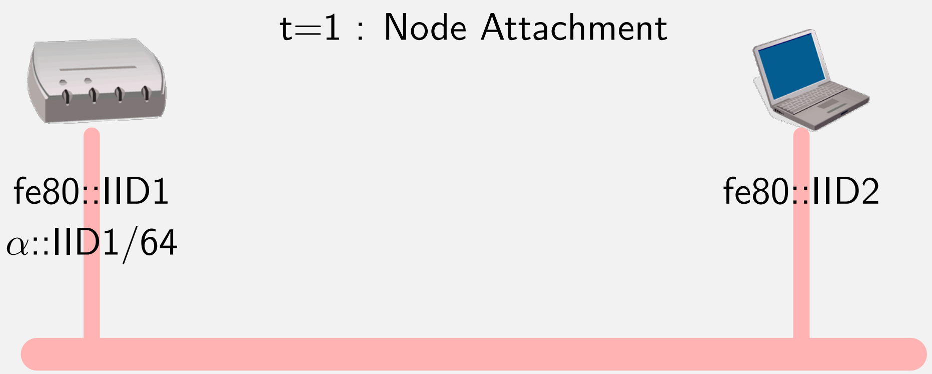
Stateless Auto-configuration: Basic Principles

Associated Protocols & Mechanisms
Neighbor Discovery
Non-Broadcast Multiple Access (NBMA) Networks
Path MTU discovery
Examples
Neighbor Discovery Security
DHCPv6
Stateless vs Stateful
IPv6 & DNS
Security



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)

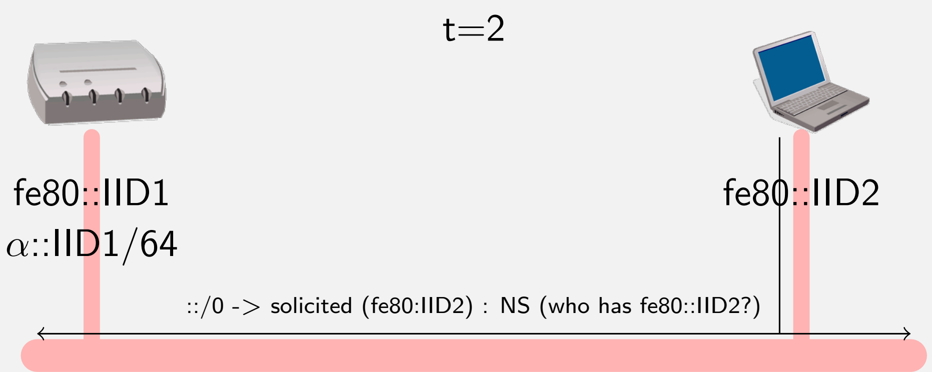
Stateless Auto-configuration: Basic Principles



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

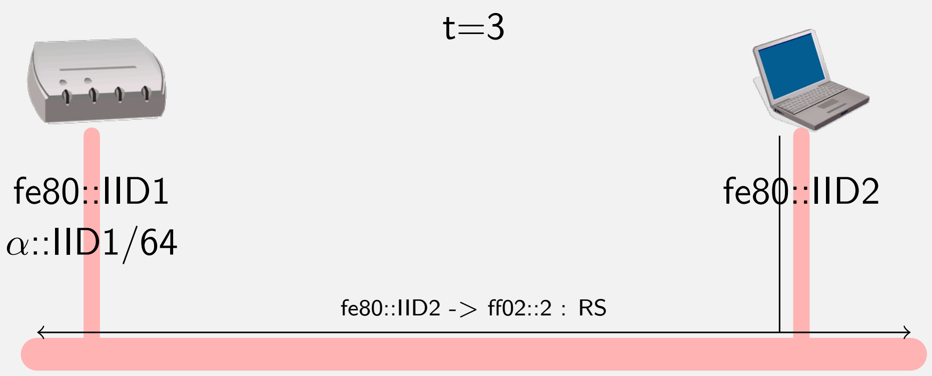
Stateless Auto-configuration: Basic Principles

Associated Protocols & Mechanisms
Neighbor Discovery
Non-Broadcast Multiple Access (NBMA) Networks
Path MTU discovery
Examples
Neighbor Discovery Security
DHCPv6
Stateless vs Stateful
IPv6 & DNS
Security



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).

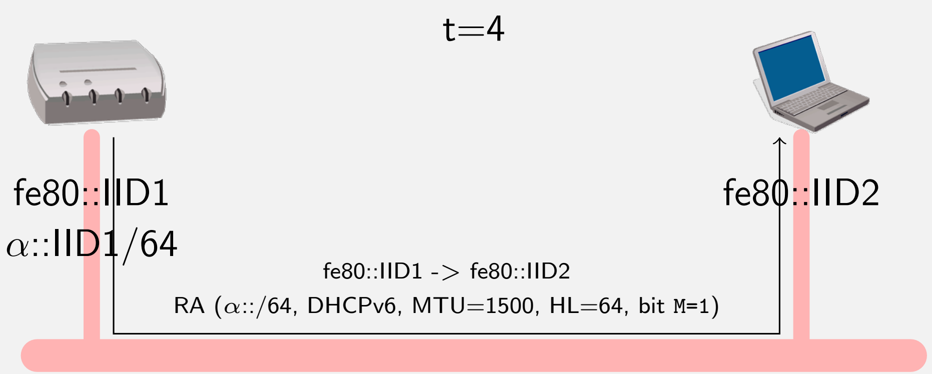
Stateless Auto-configuration: Basic Principles



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

Associated Protocols & Mechanisms
Neighbor Discovery
Non-Broadcast Multiple Access (NBMA) Networks
Path MTU discovery
Examples
Neighbor Discovery Security
DHCPv6
Stateless vs Stateful
IPv6 & DNS
Security

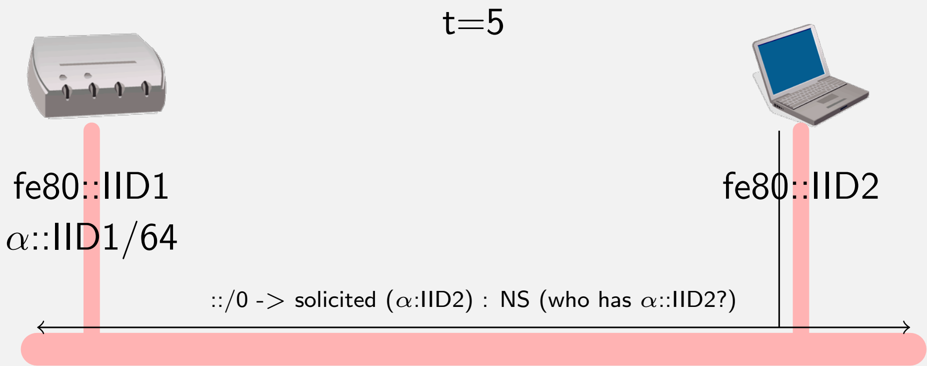


Router directly answers the host using Link-local addresses. The answer may contain a/several prefix(es). Router can also mandate hosts to use DHCPv6 to obtain prefixes (statefull auto-configuration) and/or other parameters (DNS servers. . .): Bit `M` = 1.

©G6 Association December 20, 2010 8 / 58

Stateless Auto-configuration: Basic Principles

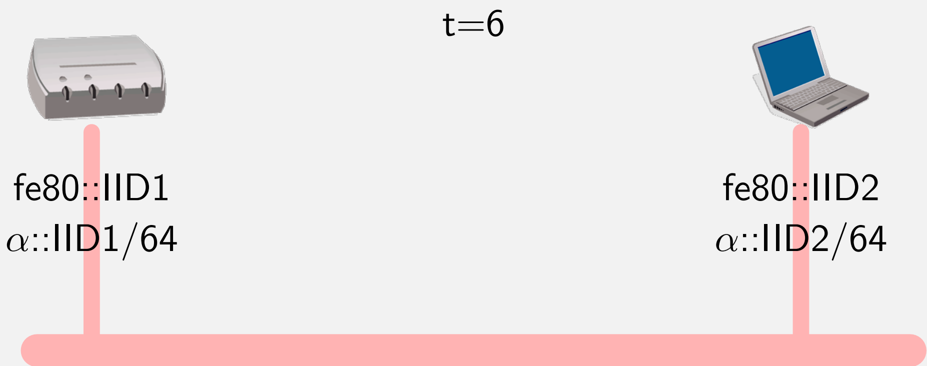
Associated Protocols & Mechanisms
Neighbor Discovery
Non-Broadcast Multiple Access (NBMA) Networks
Path MTU discovery
Examples
Neighbor Discovery Security
DHCPv6
Stateless vs Stateful
IPv6 & DNS
Security



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

Associated Protocols & Mechanisms
Neighbor Discovery
Non-Broadcast Multiple Access (NBMA) Networks
Path MTU discovery
Examples
Neighbor Discovery Security
DHCPv6
Stateless vs Stateful
IPv6 & DNS
Security



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

Associated Protocols & Mechanisms
Neighbor Discovery
Non-Broadcast Multiple Access (NBMA) Networks
Path MTU discovery
Examples
Neighbor Discovery Security
DHCPv6
Stateless vs Stateful
IPv6 & DNS
Security

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

Associated Protocols & Mechanisms
Non-Broadcast Multiple Access (NBMA) Networks

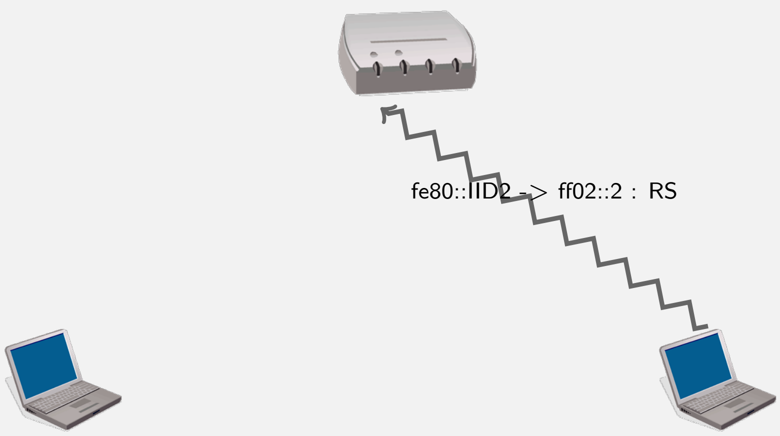
NBMA Networks

Associated Protocols & Mechanisms
Neighbor Discovery
Non-Broadcast Multiple Access (NBMA) Networks
Path MTU discovery
Examples
Neighbor Discovery Security
DHCPv6
Stateless vs Stateful
IPv6 & DNS
Security

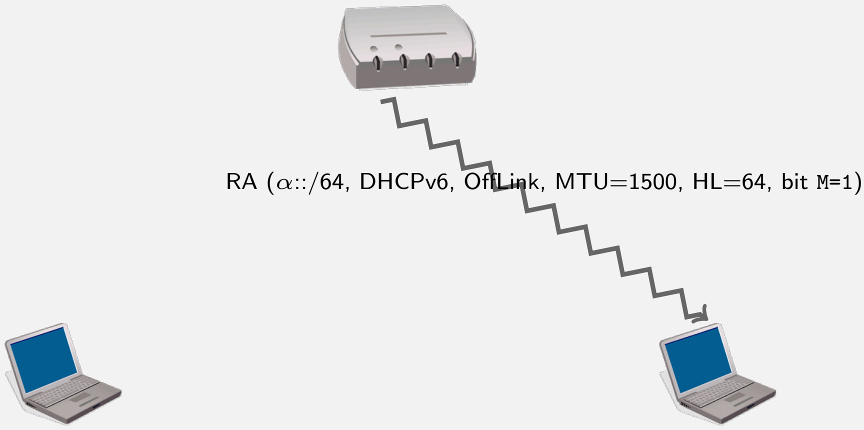
- NDP can handle efficiently NBMA networks
  - Every host can be joined separately, but no broadcast
  - Telephony network, ATM...
- Off-link bit is RA by the router to inform of a NBMA network
  - 3G, Sensor Networks (broadcast expensive)
- All packets are sent to to the router, which will forward to destination
  - No NS
  - ICMP Redirect can be used.

Off Link example Optional

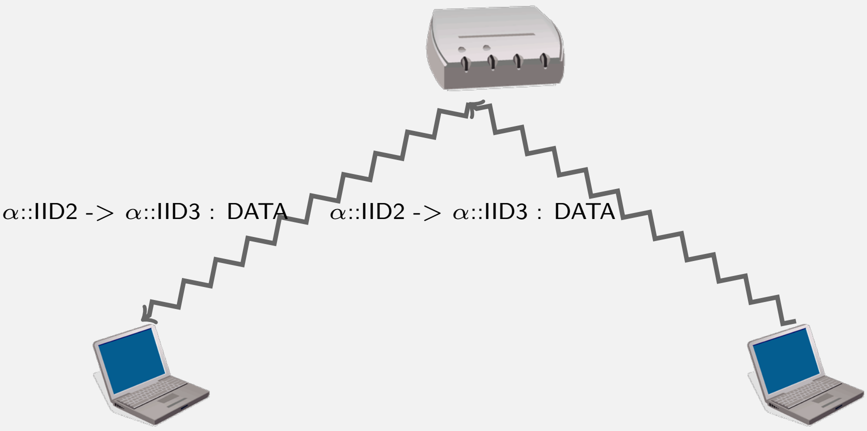
Associated Protocols & Mechanisms
Neighbor Discovery
Non-Broadcast Multiple Access (NBMA) Networks
Path MTU discovery
Examples
Neighbor Discovery Security
DHCPv6
Stateless vs Stateful
IPv6 & DNS
Security



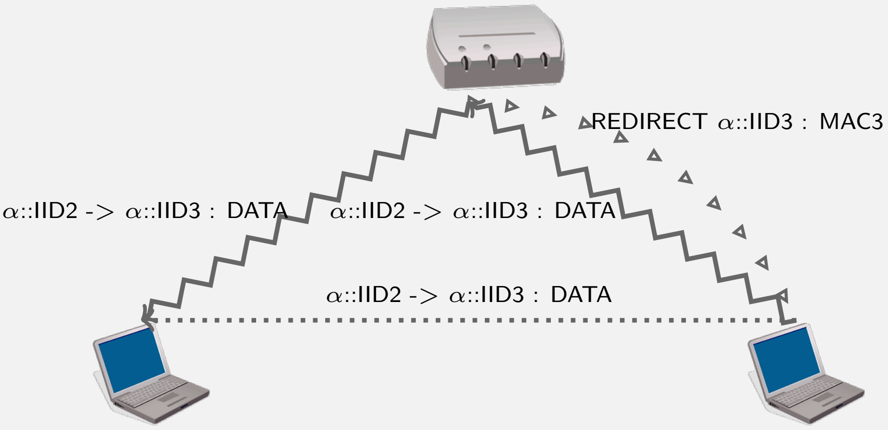
Off Link example Optional



Off Link example Optional



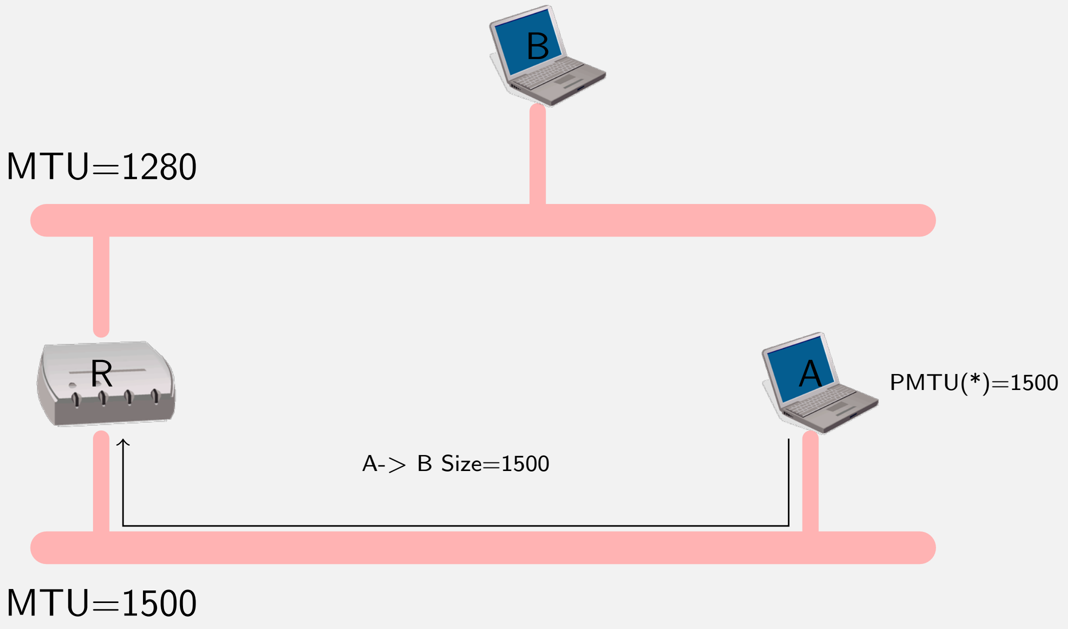
Off Link example Optional



Associated Protocols & Mechanisms

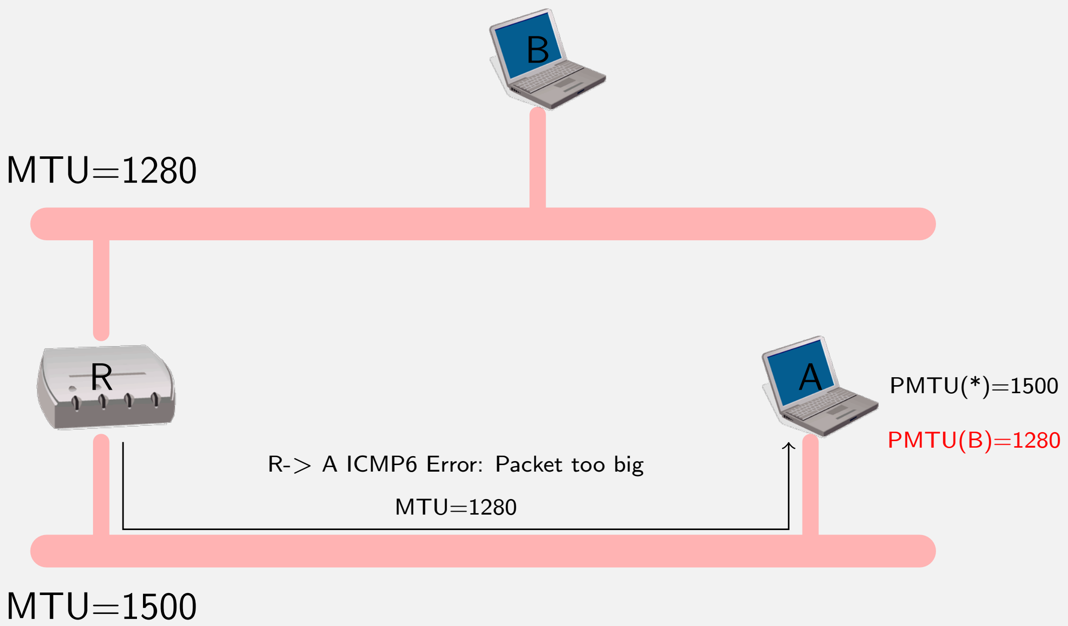
Path MTU discovery

Path MTU discovery for IPv6 (RFC 1981



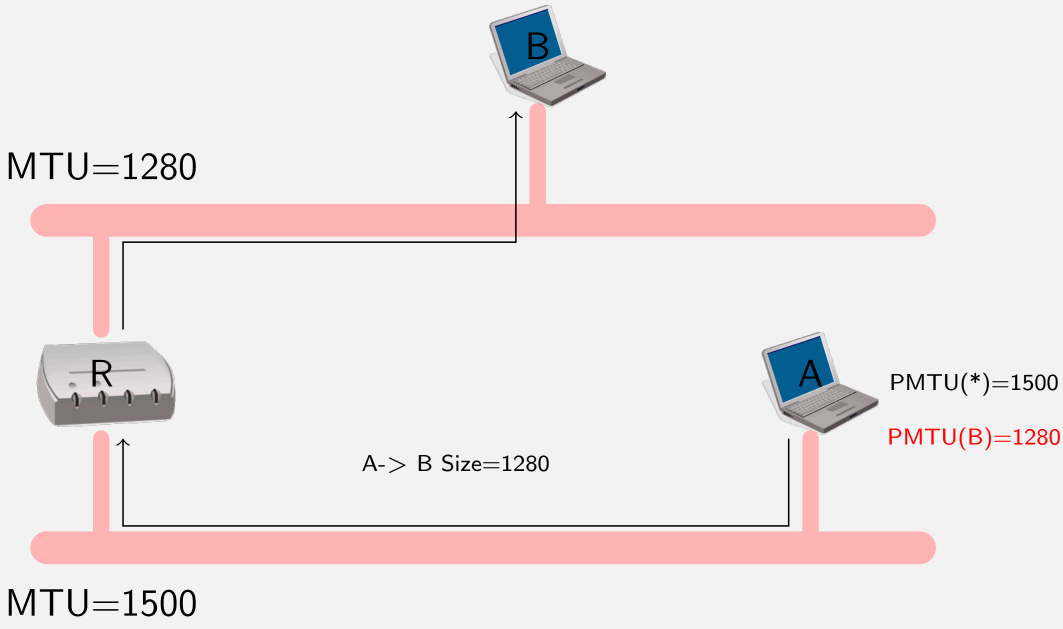
Path MTU discovery for IPv6 (RFC 1981

Associated Protocols & Mechanisms
Neighbor Discovery
Non-Broadcast Multiple Access (NBMA) Networks
Path MTU discovery
Examples
Neighbor Discovery Security
DHCPv6
Stateless vs Stateful
IPv6 & DNS
Security



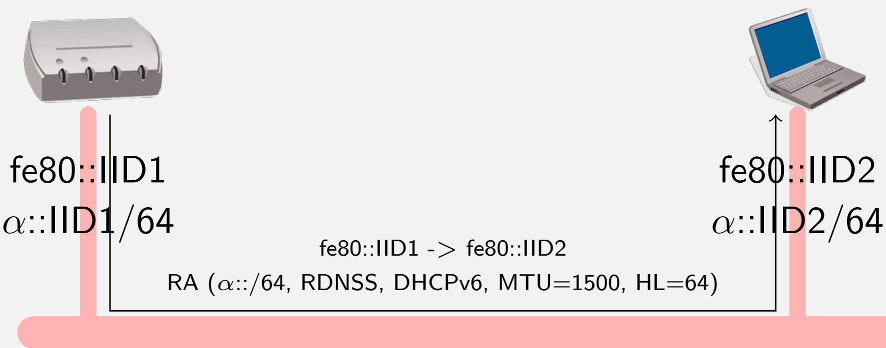
©G6 Association December 20, 2010 14 / 58

Path MTU discovery for IPv6 (RFC 1981



Experimental solution : RDNSS option in RA

Associated Protocols & Mechanisms
Neighbor Discovery
Non-Broadcast Multiple Access (NBMA) Networks
Path MTU discovery
Examples
Neighbor Discovery Security
DHCPv6
Stateless vs Stateful
IPv6 & DNS
Security



RFC 6106 : IPv6 Router Advertisement Options for DNS Configuration proposes a new option for RA. It allows IPv6 routers to advertise a list of DNS recursive server addresses and a DNS Search List to IPv6 hosts.

Associated Protocols & Mechanisms

Examples

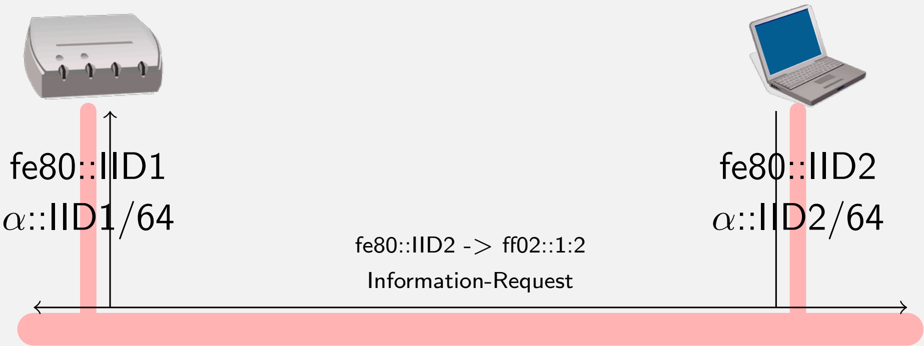
Router Configuration Example

Associated Protocols & Mechanisms
Neighbor Discovery
Non-Broadcast Multiple Access (NBMA) Networks
Path MTU discovery
Examples
Neighbor Discovery Security
DHCPv6
Stateless vs Stateful
IPv6 & DNS
Security

```
interface Vlan5
 description reseau C5
 ip address 192.108.119.190 255.255.255.128
...
 ipv6 address 2001:660:7301:1::/64 eui-64
 ipv6 enable
 ipv6 nd ra-interval 10
 ipv6 nd prefix-advertisement 2001:660:7301:1::/64 2592000\
 604800 onlink autoconfig
```

Stateless DHCPv6 (RFC 3736): With static parameters

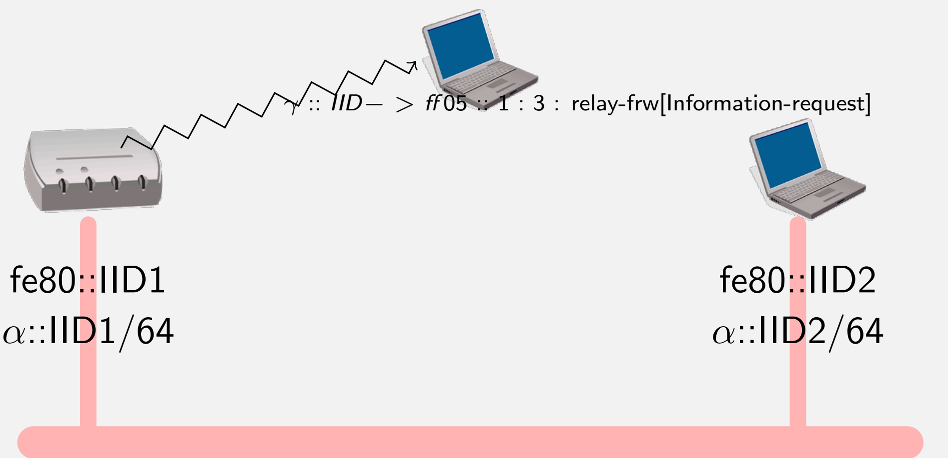
Associated Protocols & Mechanisms
Neighbor Discovery
Non-Broadcast Multiple Access (NBMA) Networks
Path MTU discovery
Examples
Neighbor Discovery Security
DHCPv6
Stateless vs Stateful
IPv6 & DNS
Security



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.

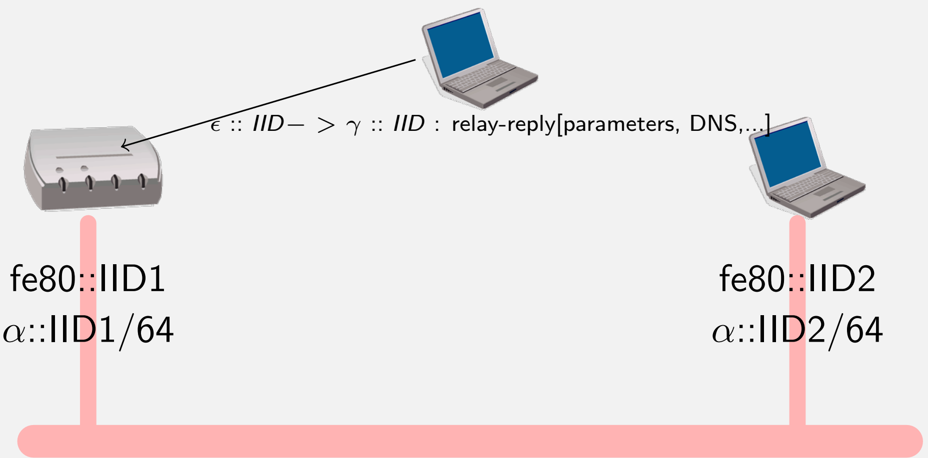
Stateless DHCPv6 (RFC 3736): With static parameters

Associated Protocols & Mechanisms
Neighbor Discovery
Non-Broadcast Multiple Access (NBMA) Networks
Path MTU discovery
Examples
Neighbor Discovery Security
DHCPv6
Stateless vs Stateful
IPv6 & DNS
Security



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.*

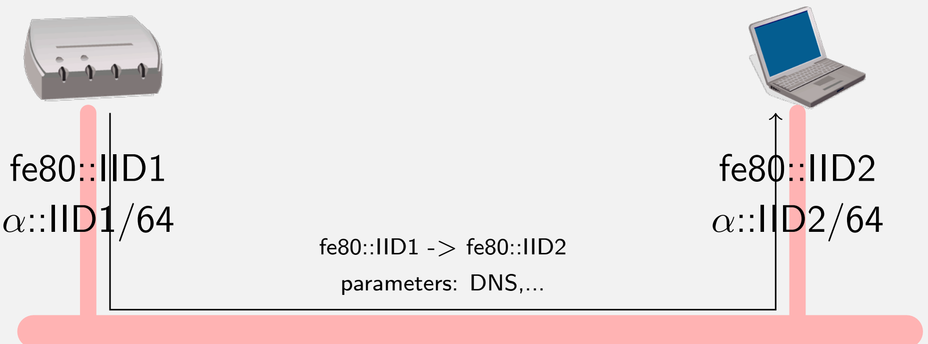
Stateless DHCPv6 (RFC 3736): With static parameters



The server responds to the relay

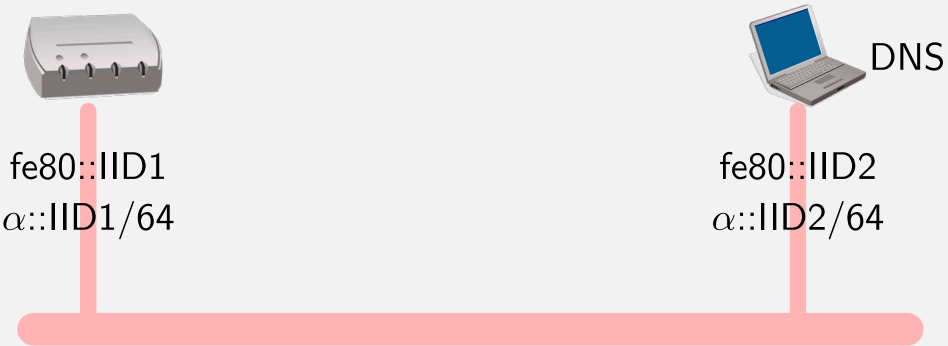
Associated Protocols & Mechanisms
Neighbor Discovery
Non-Broadcast Multiple Access (NBMA) Networks
Path MTU discovery
Examples
Neighbor Discovery Security
DHCPv6
Stateless vs Stateful
IPv6 & DNS
Security

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

Router Solicitation

0..................7..................15..................23...................31

Type=133	Code =0	Checksum
Reserved		
Options: - Source link-layer address		

- Sent by a host at bootstrap to receive information from the/a router
- Source Address: Link Local address of the interface
- Destination Address: ff02::2 (All-Routers link-local multicast group)
- Common option is:
    - Source link-layer address: physical (MAC) address of the host

Source/Target Link Layer Option

Generic: (type 1: source – 2:Target)

0.................7..................15..................23...................31

Type=1/2	length	Link Layer Address

MAC-48 (Ethernet, Wi-Fi,...) RFC 2464

Type=1/2	length =1	MAC...
...Address		

MAC-16 (IEEE 802.15.4 6LoWPAN) RFC 4944

Type=1/2	length =1	Address
Reserved		

MAC-64 (IEEE 802.15.4 6LoWPAN) RFC 4944

Type=1/2	length =2	
Address		
Reserved		

Router Advertisement

0.................7..................15..................23...................31

Type=134				Code =0	Checksum
Cur. Hop Lim.	M	O	H	reserved	Router Lifetime
Reachable Time					
Retrans Time					
Options: Source link-layer address MTU Prefix Information (may be repeated)					

Router Advertisement (continued)

- Source Address: Link Local address of the router's interface
- Destination Address:
  - Sent in point-to-point in response to a RS (Link-Local address of the Solicitation) or
  - Sent periodically to ff02::1
- Current Hop Limit: The Value a host should set as Hop Limit
- Flags: `M`: 1 use DHCPv6 for address allocation ; `O`: 1 use DHCPv6 for other information ; `H` (RFC 3775) The router is also a Home Agent.
- Router Lifetime: How long this router will be running
- Reachable Time: Time in ms an host is supposed reachable (kept in ND table)
- Retransmission Time: Time in ms between two non solicited RA
- Common options are:
  - Source link-layer address: physical (MAC) address of the router
  - MTU: Maximum size used on the link
  - Prefix Information (may be repeated)

MTU, Prefix Information

MTU:

0.................7..................15..................23...................31

Type=5	length =1	Reserved
MTU		

Prefix Information:

0.................7..................15..................23...................31

Type=3	length =4	Prefix Length	L	A	R	Reserved
Valid Lifetime						
Prefered Lifetime						
Reserved						
Prefix						

RDNSS option (RFC 6106)

0.................7..................15..................23....................31

Type=25	length ⩾ 3	Reserved
Lifetime		
Prefix		
Prefix		

Neighbor Solicitation

Associated Protocols & Mechanisms
Neighbor Discovery
Non-Broadcast Multiple Access (NBMA) Networks
Path MTU discovery
Examples
Neighbor Discovery Security
DHCPv6
Stateless vs Stateful
IPv6 & DNS
Security

0.................7..................15..................23....................31

Type=135	Code =0	Checksum
Reserved		
Target Address		
Options: Source link-layer address		

Neighbor Advertisement

Associated Protocols & Mechanisms
Neighbor Discovery
Non-Broadcast Multiple Access (NBMA) Networks
Path MTU discovery
Examples
Neighbor Discovery Security
DHCPv6
Stateless vs Stateful
IPv6 & DNS
Security

0..................7..................15..................23...................31

Type=136			Code =0	Checksum	
R	S	O	Reserved		
Target Address					
Options: Source link-layer address					

Redirect

Associated Protocols & Mechanisms
Neighbor Discovery
Non-Broadcast Multiple Access (NBMA) Networks
Path MTU discovery
Examples
Neighbor Discovery Security
DHCPv6
Stateless vs Stateful
IPv6 & DNS
Security

0..................7..................15..................23...................31

Type=137	Code =0	Checksum
Reserved		
Target Address		
Target Address		
Options: Target link-layer address, Redirected Header		

Associated Protocols & Mechanisms
Neighbor Discovery
Non-Broadcast Multiple Access (NBMA) Networks
Path MTU discovery
Examples
Neighbor Discovery Security
DHCPv6
Stateless vs Stateful
IPv6 & DNS
Security

Redirect Header

0.................7..................15..................23..................31

Type=5	length =1	Reserved
Reserved		
IPv6 Header and Data		

ICMPv6 redirect:

- Optimize routing inside a network
- Substitute to NS/NA in NBMA Networks

Associated Protocols & Mechanisms

Neighbor Discovery Security

Security issues with Neighbor Discovery

Associated Protocols & Mechanisms
Neighbor Discovery
Non-Broadcast Multiple Access (NBMA) Networks
Path MTU discovery
Examples
Neighbor Discovery Security
DHCPv6
Stateless vs Stateful
IPv6 & DNS
Security

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

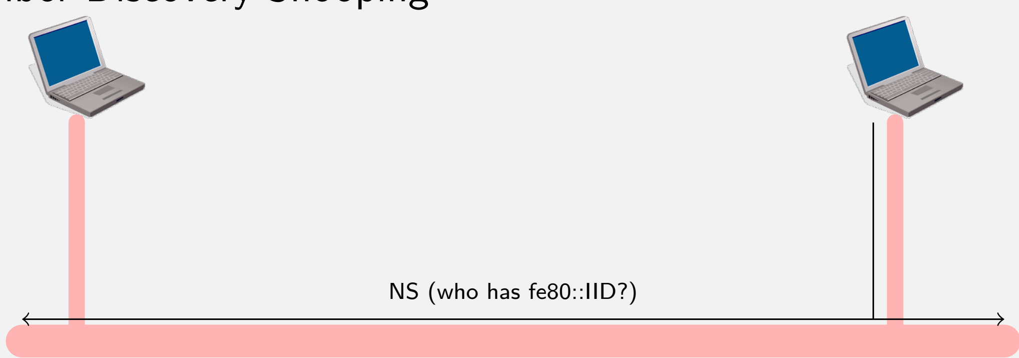
Attacker toolkits already available !

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

Examples of attacks using ND

Associated Protocols & Mechanisms
Neighbor Discovery
Non-Broadcast Multiple Access (NBMA) Networks
Path MTU discovery
Examples
Neighbor Discovery Security
DHCPv6
Stateless vs Stateful
IPv6 & DNS
Security

Neighbor Discovery Snooping

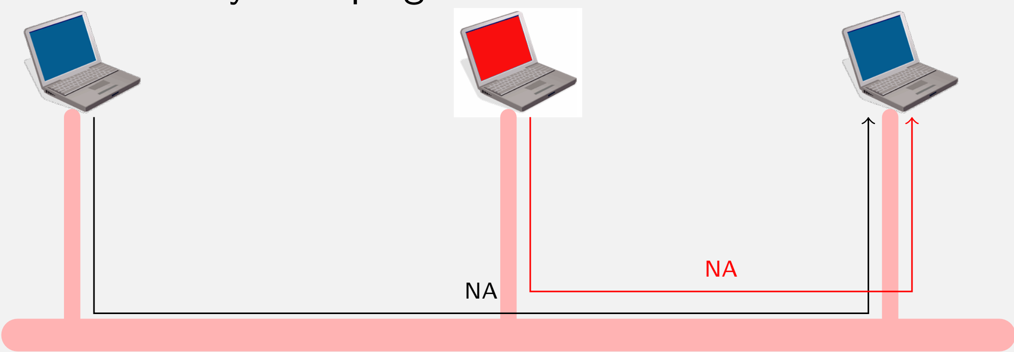


Host uses Neighbor Discovery notably in these two cases:

- 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

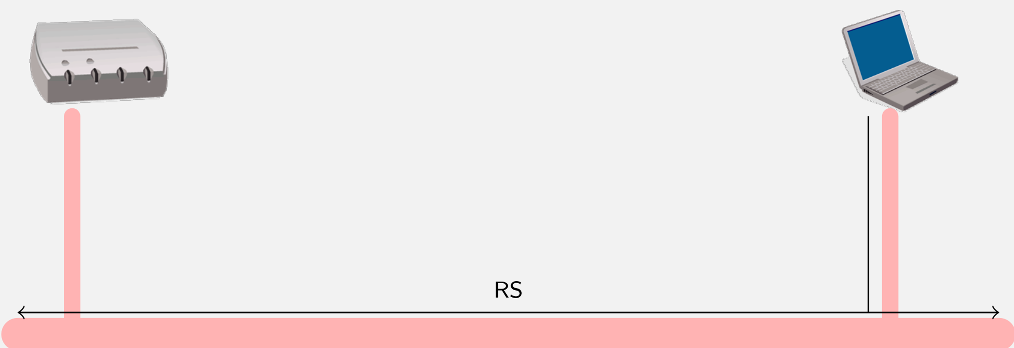


An attacker on the LAN can perform an attack by responding to ND messages

- 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

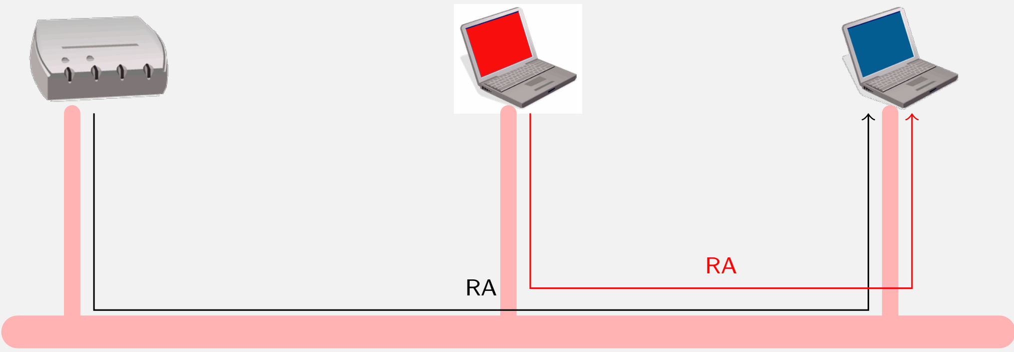
Rogue router



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

Solutions to mitigate or prevent attacks?

Associated Protocols & Mechanisms
Neighbor Discovery
Non-Broadcast Multiple Access (NBMA) Networks
Path MTU discovery
Examples
Neighbor Discovery Security
DHCPv6
Stateless vs Stateful
IPv6 & DNS
Security

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`

Example: Interface during an IETF meeting

Associated Protocols & Mechanisms
Neighbor Discovery
Non-Broadcast Multiple Access (NBMA) Networks
Path MTU discovery
Examples
Neighbor Discovery Security
DHCPv6
Stateless vs Stateful
IPv6 & DNS
Security

```
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
```


How to solve wrong RA

Associated Protocols & Mechanisms
Neighbor Discovery
Non-Broadcast Multiple Access (NBMA) Networks
Path MTU discovery
Examples
Neighbor Discovery Security
DHCPv6
Stateless vs Stateful
IPv6 & DNS
Security

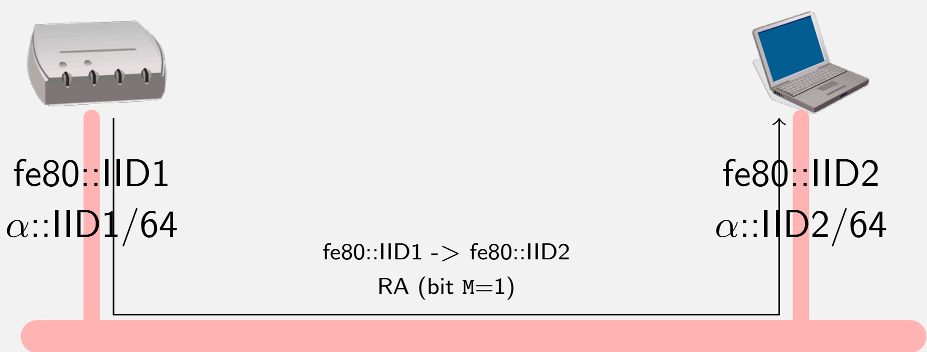
- SeND: Secure Neighbor Discovery
  - Use of cryptography to protect and authenticate announcements
  - Protect against bad guys
  - Complex and not verify flexible
- SAVI : Source Address Validation
  - : Work in Progress: see http://tools.ietf.org/html/draft-ietf-savi-framework-01
  - Implement in switches functions to control announcements
  - Flexible, but not a strong protection
  - Under experimentation
- Otherwise filter announcements with a firewall

Associated Protocols & Mechanisms

DHCPv6

DHCPv6 : Stateful Auto-Configuration

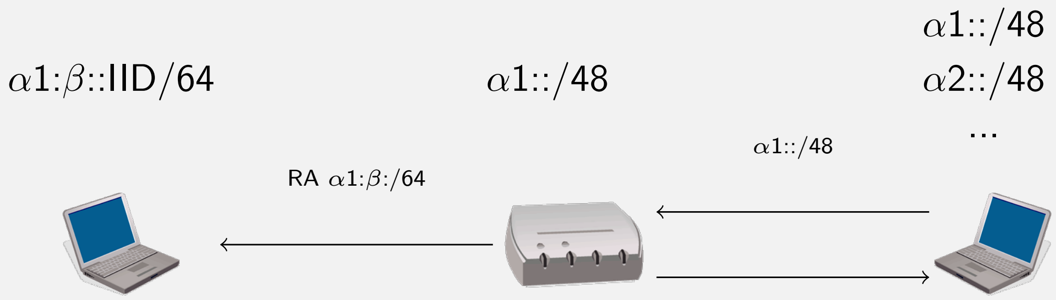
Associated Protocols & Mechanisms
Neighbor Discovery
Non-Broadcast Multiple Access (NBMA) Networks
Path MTU discovery
Examples
Neighbor Discovery Security
DHCPv6
Stateless vs Stateful
IPv6 & DNS
Security



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 : Prefix Delegation

- Dynamic configuration for routers
- ISP solution to delegate prefixes over the network

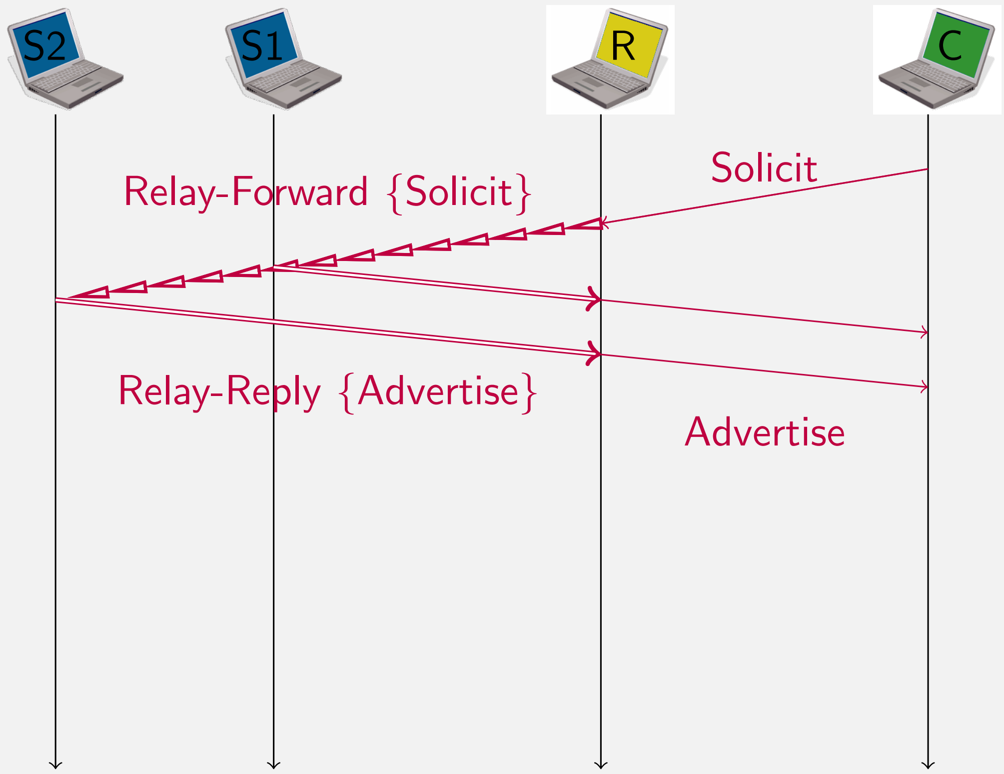


DHCPv6 Full Features

Associated Protocols & Mechanisms
Neighbor Discovery
Non-Broadcast Multiple Access (NBMA) Networks
Path MTU discovery
Examples
Neighbor Discovery Security
DHCPv6
Stateless vs Stateful
IPv6 & DNS
Security

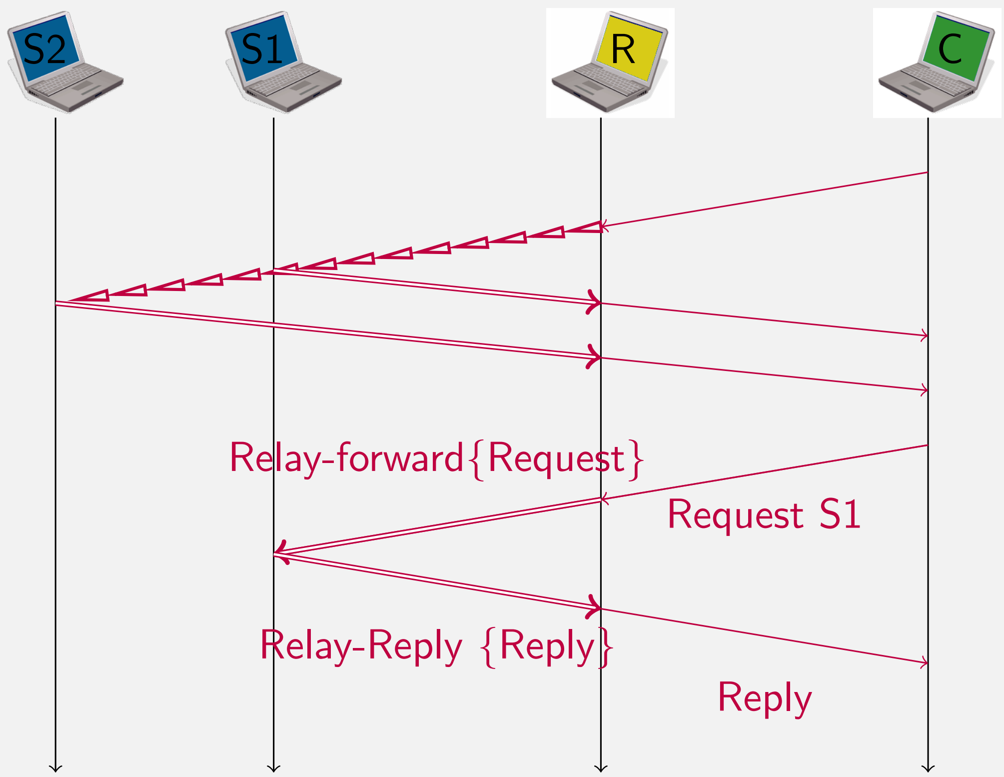
- For address or prefix allocation information form only one DHCPv6 must be taken into account. Four message exchange :
  - Solicit : send by clients to locate servers
  - Advertise : send by servers to indicate services available
  - Request : send by client to a specific server (could be through relays)
  - 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

DHCPv6 Scenarii



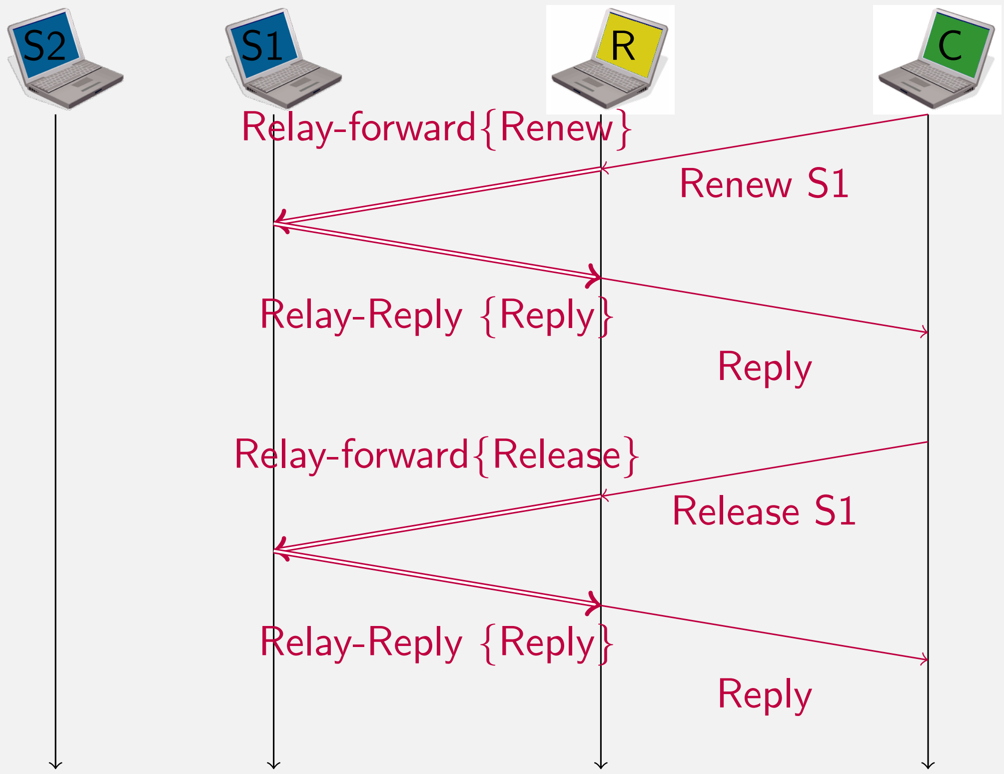
DHCPv6 Scenarii

Associated Protocols & Mechanisms
Neighbor Discovery
Non-Broadcast Multiple Access (NBMA) Networks
Path MTU discovery
Examples
Neighbor Discovery Security
DHCPv6
Stateless vs Stateful
IPv6 & DNS
Security



©G6 Association December 20, 2010 40 / 58

DHCPv6 Scenarii



DHCPv6 Identifiers

Associated Protocols & Mechanisms
Neighbor Discovery
Non-Broadcast Multiple Access (NBMA) Networks
Path MTU discovery
Examples
Neighbor Discovery Security
DHCPv6
Stateless vs Stateful
IPv6 & DNS
Security

- DHCPv6 defines several stable identifiers
- After a reboot, the host can get the same information.
- DUID (DHCPv6 Unique IDentifier) :
  - Identify the client
  - Variable length:
    - Link-layer address plus time
    - Vendor-assigned unique ID based on Enterprise Number
    - Link-layer address
- For instance:

```
>od -x /var/db/dhcp6c_duid
0000000 000e 0100 0100 5d0a 5233 0400 9e76 0467
```

DHCPv6 Identifier : IA and IA_PD

Associated Protocols & Mechanisms
Neighbor Discovery
Non-Broadcast Multiple Access (NBMA) Networks
Path MTU discovery
Examples
Neighbor Discovery Security
DHCPv6
Stateless vs Stateful
IPv6 & DNS
Security

- IA and IA_PD are used to link Request and Reply
  - IA is used for Address Allocation and is linked to an Interface
  - IA_PD is used for Prefix Delegation and can be shared among interfaces
- They must be stable (e.g. defined in the configuration file)

Associated Protocols & Mechanisms
Stateless vs Stateful

Auto-configuration: Stateless vs. Stateful

Associated Protocols & Mechanisms
Neighbor Discovery
Non-Broadcast Multiple Access (NBMA) Networks
Path MTU discovery
Examples
Neighbor Discovery Security
DHCPv6
Stateless vs Stateful
IPv6 & DNS
Security

Stateless

Pro:

- Reduce manual configuration
- No server, no state (the router provides all information)

Cons:

- Non-obvious addresses
- No control on addresses on the LAN

Stateful (DHCPv6)

Pro:

- Control of addresses on the LAN
- Control of address format

Cons:

- Requires an extra server
- Still needs RA mechanism
- Clients to be deployed

- Stateless: Typically, for Plug-and-Play networks (Home Network)
- Stateful: Typically, for administrated networks (enterprise, institution)

IPv6 & DNS

Reminder: The two faces of the DNS

The DNS seen as a TCP/IP application

- The service is accessible in either transport modes (UDP/TCP) and over either IP versions (v4/v6)
- If IPv6 transport is not supported yet, then it's highly time!
- *Caution: Information given over either IP version MUST BE CONSISTENT!*

The DNS seen as a database

- Stores different types of resource records (RR), including those related to IPv4 and IPv6 addresses: SOA, NS, A, AAAA, MX, PTR, TXT
- IPv6 nodes & services become visible as soon as their related resources are published in the DNS database
- *Caution: DNS database is IP transport version agnostic!*

DNS Extensions for IPv6 Support (RFC 3596)

Forward lookup ('Name → IPv6 Address')

- A new Resource Record (RR) : **AAAA**
- The "AAAA" RR is for IPv6 what the "A" RR is for IPv4

Example:

```
www.afnic.fr.        IN        A         192.134.4.20
                     IN        AAAA      2001:660:3003:2::4:20
```

Reverse lookup ('IPv6 Address → Name')

- A new and dedicated reverse tree: **ip6.arpa**
- The IPv6 equivalent to the IPv4 dedicated *in-addr.arpa* tree
- PTRs labels follow a *nibble-boundary* (4 bits)

Example:

```
0.2.0.0.4.0.0.0.0.0.0.0.0.0.0.0.2.0.0.0.3.0.0.3.0.6.6.0.1.0.0.2.ip6.arpa. PTR www.afnic.fr.
```

Recursive Name Servers Information Discovery

A Stub Resolver needs a Recursive Name Server **address** to which it sends **name resolution** queries

In the IPv4 world, this DNS information is:

- Either configured manually in the stub resolver (e.g. `/etc/resolv.conf for Unix stations`)
- Or discovered via DHCPv4

In the IPv6 world: RFC 4339 (IPv6 Host Configuration of DNS Server Information Approaches)

- Via stateful DHCPv6: RFC 3315
- Via stateless DHCPv6: RFC 3736, "DHCPv6-light"
- RA-based: RFC 6106 ("IPv6 Router Advertisement Options for DNS Configuration", obsoletes RFC 5006)
- Manual configuration as for IPv4
- If IPv4 is supported, than run a DHCPv4 client

DNSv6 Operational Requirements, Recommendations & Issues

RFC 3901: "DNS IPv6 Transport Operational Guidelines"

- For DNS service continuity across a mixture of v4/v6 networks: Recursive Name Servers SHOULD be dual-stack → Use dual-stack forwarders if necessary
- DNS zones SHOULD be served by at least one v4-reachable Authoritative Name Server → Avoid v6-only servers

Bear in mind

- During the long v4-v6 transition period: some systems will stay v4-only, others will be dual-stack and others v6-only

RFC 4472 "Operational Considerations and Issues with IPv6", among others:

- Misbehavior of some DNS servers and Load-balancers
- Handling special (e.g. limited-scope) IPv6-addresses (published vs reachable)
- Service name *vs* Node name
- IPv6 and Dynamic DNS Update (RFC 2136)

Security

Announcement Filtering

Solutions in a closed environment

- Link Layer is protected either physically or by cryptographic
- Attacks/Misconfiguration comes from inside
  - Misconfiguration is more important to solve than attacks
  - Attacks are almost the same than in IPv4
  - Auto-configuration leads to catastrophic behavior in case of misconfiguration
- Auto-configuration looks more dangerous than in IPv4:
  - A centralized DHCPv4 server allows IPv4 addresses allocation
  - Does not avoid to forge a IPv4 address
- Authentication has not to be done at IPv6 level
  - IEEE 802.1X, IEEE 802.11i (WPA), PANA authenticates users, not MAC addresses
  - If allowed them auto-configuration.

NDP filtering

- Switches should understand IPv6
  - MLD Snooping (like IGMP snooping)
  - Only port assigned to routers may send RA
    - More complex than in IPv4
    - No Layer 2 type for NPD, `IPv6|ICMPv6|RA`
    - With extensions, information may be at different places
  - Should be able to register IPv6 addresses per port
    - To monitor network
- This can also be done in IEEE 802.11 architecture
  - Only specific MAC addresses can send RA
  - MAC address can be spoofed
    - No Wep
    - WPA
  - Do not work in ad hoc mode

Security

Firewalls

Concept of firewalling

- What is a firewall: a border equipment between different policy areas
- What are the roles of a firewall ?
  - Filter packets according rules
  - Alter packets (i.e. NAT)
  - Route packets between policy areas (in/out/DMZ)
- What does IPv6 change ?
  - New rules to filter IPv6
  - Need of NAT in IPv6 not yet identified
  - Routing should handle IPv6

IPv6 Filtering rules: Address scope

- Need to filter invalid scopes of addresses
- See RFC 5156
- What should be filtered as source/destination :
  - Link-local Unicast (`fe80::/10`)
  - Host-scoped addresses (`::1`)
  - Host,Link,Site-local multicast as source/destination and global multicast as source
  - ULA addresses (in site border)
  - IPv4 compatible/mapped addresses

IPv6 Filtering rules: Other principles

- ICMPv6 MUST NOT be handled the same way as ICMPv4
  - Be careful when filtering: RFC 4890 ("Recommendations for Filtering ICMPv6 Messages in Firewalls")
  - For instance, ICMPv6 is needed (Path MTU disc, Error reporting)
- IPv6 extensions need to be considered
  - Should be allowed: Fragmentation, IPSec
  - Should be considered with care : Hop-by-Hop, Destination (IPv6 Mobility), Routing
- Stateful rules are needed for a NAT-like filtering
- Beware of tunnels (6to4, Teredo) that can be backdoors

IPv6 Filtering rules: Application Headers

- Filter needs to inspect Application header (HTTP, SIP, etc.)
- IPv6 addresses may be present inside these headers (cf. SIP)
- Requirements:
  - Firewall need to handle presence of these IPv6 addresses
  - Filter need to check validity of these addresses (scope, etc.)

IPv6 Firewalls implementations

Implementation	IPv6 Support	Stateful Filter	Extension support
pf (*BSD)	X	X	X
iptables (Linux)	X	X	X
MS Vista	X	X	X
Cisco PIX/ASA	X	X	?
Cisco ACL	X	X	?
Juniper ScreenOS	X	X	?
CheckPoint	X	X	?