Copyright Notice

This set of transparencies, hereinafter referred to as slides, is protected by copyright laws and provisions of International Treaties. The title and copyright regarding the slides (including, but not limited to, each and every image, photography, animation, video, audio, music and text) are property of the authors specified on page 1.

The slides may be reproduced and used freely by research institutes, schools and Universities for non-profit, institutional purposes. In such cases, no authorization is requested.

Any total or partial use or reproduction (including, but not limited to, reproduction on magnetic media, computer networks, and printed reproduction) is forbidden, unless explicitly authorized by the authors by means of written license.

Information included in these slides is deemed as accurate at the date of publication. Such information is supplied for merely educational purposes and may not be used in designing systems, products, networks, etc. In any case, these slides are subject to changes without any previous notice. The authors do not assume any responsibility for the contents of these slides (including, but not limited to, accuracy, completeness, enforceability, updated-ness of information hereinafter provided).

In any case, accordance with information hereinafter included must not be declared.

In any case, this copyright notice must never be removed and must be reported even in partial uses.
What information is needed?

- Address prefix
- Interface identifier
- Default gateway
- DNS server
- Hostname
- Domain name
- MTU (Maximum Transmission Unit)
- ...

IPv6-configuration - 3
Options

- Manual configuration
- Stateful configuration
  - All information obtained through DHCP
- Stateless configuration
  - Autogenerated
  - Address prefix obtained from router
- Hybrid (Stateless DHCP)
  - Information other than address obtained through DHCP
Interface Identifier

- Manually configured
- Obtained through DHCPv6
- Automatically generated
  - From EUI-64 MAC address
  - Privacy aware
EUI-48 to EUI-64 mapping

EUI = Extended Unique Identifier

48 bit MAC address (EUI-48 format)

OUI

“Universal” bit

manufacturer-selected

Interface ID (from EUI-64 format)

To make manually configured address (local) easier to write
Privacy Concerns

- Traceability
  - The least significant 64 bits of the IPv6 address of an interface never change when MAC address is used

- RFC 4941, “Privacy Extensions for Stateless Address Autoconfiguration in IPv6”
Privacy Extension Algorithm

(Other options are possible)

Random or previous “privacy” address

Interface ID from MAC address

MD5

111111011111111

Interface ID

Stored for next configuration
Address Usage

- A host may have several different addresses
  - “default”
  - “privacy aware”
- Usable to accept/initiate connections
- Selection of address may be available to the user/application
Address Prefix

- Manually configured
- Obtained from DHCPv6
- Automatically generated
  - Link local
- Obtained from a router
Router/Prefix Discovery

- ICMP Router Advertisement message
  - Sent by routers
- Solicited
  - Answering to Router Solicitation by host
- Unsolicited: periodic
# Router Solicitation

<table>
<thead>
<tr>
<th>Type</th>
<th>Code</th>
<th>Checksum</th>
<th>Reserved</th>
<th>Options</th>
</tr>
</thead>
</table>

Sent to the all-routers multicast address (FF01::2)
### Router Advertisement

<table>
<thead>
<tr>
<th>Type (134)</th>
<th>Code (0)</th>
<th>Checksum</th>
<th>Cur Hop Limit</th>
<th>M</th>
<th>O</th>
<th>Reserved</th>
<th>Router Lifetime</th>
</tr>
</thead>
<tbody>
<tr>
<td>Router Advertisement</td>
<td></td>
<td></td>
<td>Cur Hop Limit</td>
<td>M</td>
<td>O</td>
<td>Reserved</td>
<td>Router Lifetime</td>
</tr>
<tr>
<td>Reachable Time</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Retrans Timer</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Options</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

- **M** (Managed Address Configuration)
  - 1 – address available through DHCP
- **O** (Other configuration)
  - E.g., DNS server
Options

- General Format
- Length in multiple of 8 bytes
### Prefix Information Option

<table>
<thead>
<tr>
<th>Type (3)</th>
<th>Length</th>
<th>Prefix Length</th>
<th>L</th>
<th>A</th>
<th>Reserved</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

- **Valid Lifetime**
- **Preferred Lifetime**
- **Reserved**

- **L** – prefix is on-link
- **A** – prefix can be used for autonomous configuration
MTU Option

Ensures all hosts on-link use the same MTU value
Link Layer Address Option

<table>
<thead>
<tr>
<th>Type</th>
<th>Length</th>
<th>Link-Layer Address</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
<td>Link-Layer Address</td>
</tr>
<tr>
<td></td>
<td></td>
<td>. . .</td>
</tr>
</tbody>
</table>

IPv6-configuration - 17
ICMP Redirect

- Sent by a router to advise a host about a best first-hop
- The first-hop is always on-link, irrespective of prefix
### ICMP Redirect Message Format

<table>
<thead>
<tr>
<th>Type</th>
<th>Code</th>
<th>Checksum</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td><strong>Reserved</strong></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td><strong>Target Address</strong></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td><strong>Destination Address</strong></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td><strong>Options</strong></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
Redirect Header Option

Information about the packet being redirected

<table>
<thead>
<tr>
<th>Type (4)</th>
<th>Length</th>
<th>Reserved</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>Reserved</td>
</tr>
</tbody>
</table>

Reserved

IP header + data
Duplicate Address Detection (DAD)

- Probe uniqueness of an IPv6 address
- Neighbor solicitation with address being probed as target
  - Sent to corresponding IPv6 Solicited Node Multicast Address
  - Corresponding MAC multicast address
- Wait for a response for at least 1 sec
  - If no answer is received, the address is considered valid
Stateless Configuration: Basic Step

- Generate a link local address
- Probe for its uniqueness (DAD)
- Subscribe to the corresponding IPv6 Solicited Node Multicast Address
  - Configure reception of corresponding multicast MAC
  - Send ICMP Multicast Listener Report
- On-link communication enabled
Stateless Configuration: With Router

- Possibly send Router Solicitation
- Listen to Router Advertisements
- Create address from advertised prefix
- Probe for its uniqueness (DAD)
- Subscribe to the corresponding IPv6 Solicited Node Multicast Address
  - Configure reception of corresponding multicast MAC
  - Send ICMP Multicast Listener Report
Stateless Configuration: Renumbering

- Keep listening to Router Advertisements
  - Host can be re-configured any time
- State of addresses
  - Preferred
  - Deprecated
- Easier renumbering
  - Possible to switch from a previous (ISP) global address to a new one
Stateful Configuration: Dynamic Host Configuration Protocol

- Client/server model
- M flag = 1 in Router Advertisement
- Messages:
  - Solicit (to all-agents address: FF02::1:2)
  - Advertise
  - Request (all-agents address: FF02::1:2)
  - Reply
  - Release
  - Reconfigure
DHCP Stateless Configuration

- M flag = 0 in Router Advertisement
  - Address autoconfigured from prefix in Router Advertisement
- O flag = 1 in Router Advertisement
  - Other information configured through DHCP
Autoconfiguration for routers

- Router Renumbering (RFC 2894)
- Router Renumbering packets
  - they include PCOs (Prefix Control Operations)
    - Match-Prefix: specifies the operation
    - Use-Prefix
  - They are transported in ICMPv6 packets
- Two types of Router Renumbering messages
Scoped Addresses
Why is a scope required?

fe80::0237:00ff:fe02:a7fd

socket

Application

TCP/UDP

IPv6

DL

PHY

fe80::0237:00ff:fe02:a7fd
Sintax

- A scoped address is composed of an IPv6 address followed by a % and a number identifying the interface

Example:
- FE80::0237:00FF:FE02:a7FD%19

The choice of the actual value of the scope is implementation-specific
Examples of Scoped Addresses

c:\>netsh interface ipv6 show address
Interface 1: Loopback Pseudo-Interface 1
Addr Type  DAD State  Valid Life  Pref. Life  Address
---------  ---------  -----------  -----------  ----------------------------
Other  Preferred  infinite  infinite  ::1

Interface 10: Wireless Network Connection
Addr Type  DAD State  Valid Life  Pref. Life  Address
---------  ---------  -----------  -----------  --------------------------------=
Other  Preferred  infinite  infinite  fe80::9832:45b1:96e9:f444:10

Interface 9: Local Area Connection
Addr Type  DAD State  Valid Life  Pref. Life  Address
---------  ---------  -----------  -----------  --------------------------------=
Other  Deprecated  infinite  infinite  fe80::9158:6fc2:4155:356e%9

Interface 12: Local Area Connection* 12
Addr Type  DAD State  Valid Life  Pref. Life  Address
---------  ---------  -----------  -----------  --------------------------------=
Public  Preferred  infinite  infinite  2001:0:5ef5:79fd:14b0:f4d:f50d:a9a9
Other  Preferred  infinite  infinite  fe80::14b0:f4d:f50d:a9a9%12

Interface 27: Bluetooth Network Connection
Addr Type  DAD State  Valid Life  Pref. Life  Address
---------  ---------  -----------  -----------  --------------------------------=
Other  Deprecated  infinite  infinite  fe80::9061:aca4:ff3:337-27

Interface 31: Local Area Connection* 25
Addr Type  DAD State  Valid Life  Pref. Life  Address
---------  ---------  -----------  -----------  --------------------------------=
Other  Deprecated  infinite  infinite  fe80::5efe:10.242.86.86%31
Security and IPv6 addresses

- Network scanning
  - More difficult, from a theoretical point of view, because the larger number of combinations available (64 bits per LAN)
  - In reality, it is possible to use tricks to shrink the address space to be scanned
    - Addresses are assigned sequentially (from ::1 on)
    - Stateless address autoconfiguration (48 bits to be scanned)
    - Hosts with sequential MAC addresses (once one is found, all the others have similar MACs)
    - Start scanning with known OUI (NIC manufacturers → 24 bit)
    - IPv6 addresses derived from IPv4 ones
    - Often, an IPv6 host uses dual stack, hence it is possible to scan the IPv4 space
  - Address harvesting, used to find addresses to be used as "seeds"
    - Host published in DNS
    - Analysis of log files of an host (e.g. tracker P2P, web server)

- DDoS
  - An attacker may use several different addresses from the same machine (potentially, a whole /64)