Discovering IPv6 with Wireshark

June 14, 2011

Rolf Leutert
Network Consultant & Trainer | Leutert NetServices | Switzerland

SHARKFEST ‘11
Stanford University
June 13-16, 2011
Agenda

- Address Autoconfiguration
- Neighbor discovery, Router discovery
- Host configuration with DHCPv6
- Transition technologies, ISATAP & Teredo Tunnel
IPv6 Stateless Address Autoconfiguration (SLAAC)

- An IPv6 host will **autoconfigure** a link-local address for each interface.
- Prefix for link-local address is **fe80::/64**
- Interface ID is either derived from **MAC address** or a **random value**

**IPv6 address: EUI-64 format**

```
fe 80 00 00 00 00 00 00 02 30 64 ff fe 6b 85 32
```

**IPv6 address: privacy format**

```
fe 80 00 00 00 00 00 00 9c 4a e7 8a 20 38 d4 d1
```
IPv6 Stateless Address Autoconfiguration (SLAAC)

- If a router is present, host will also autoconfigure global address
- Prefix will be obtained from router, example 2001:db8::/64
- Interface ID is either derived from MAC address or a random value
- Router indicates in advertisement if stateful configuration may be used

**Ethernet MAC address**

```
00 30 64 6b 85 32
```

**IPv6 address: EUI-64 format**

```
20 01 0d b8 00 00 00 00 02 30 64 ff fe 6b 85 32
```

**IPv6 address: privacy format**

```
20 01 0d b8 00 00 00 00 9c 4a e7 8a 20 38 d4 d1
```

random value
### Address Autoconfiguration

**Solicited Node Multicast Address (SNMA)**

- Probably the **most strange** part of IPv6 addressing
- An IPv6 host forms a SNMA for each own unicast address in use
- The SNMA address is used for Neighbor Discovery (replacement of ARP)
- The SNMA address is **derived from each unicast address in use**

<table>
<thead>
<tr>
<th>Hosts unicast address</th>
<th>Hosts SNMA address</th>
</tr>
</thead>
<tbody>
<tr>
<td>20 01:0d b8:00 00:00:00 00:02:30:64 ff:fe 6b:85 32</td>
<td>ff 02:00:00:00:00:00:00:01:ff 6b:85 32</td>
</tr>
</tbody>
</table>

**SNMA prefix** `ff02:0:0:0:1:ff00/104`  
**24 bits**

**SNMA derived from unicast address**: `ff02::1:ff6b:8532`
The initial client startup process includes the following steps:

Frame #

1. Duplicate Address Detection after Link-Local autoconfiguration
2. Router Discovery
3. Router Advertisement and global address autoconfiguration
4. Neighbor Discovery (searching for Router MAC)
5. Neighbor Advertisement (reply from Router with MAC)
6. Duplicate Address Detection with acquired global address
IPv6 Interfaces

- In Windows Vista/7, each IPv6 interface is numbered with unique ‘Zone ID’

- A link-local address is automatically configured with the address prefix \texttt{fe80::/64} for each physical or logical IPv6 interface

- If a router is available, a global address is configured on interface
## IPv6 Interfaces

<table>
<thead>
<tr>
<th>Aktive Routen</th>
<th>Gateway</th>
</tr>
</thead>
<tbody>
<tr>
<td>If Metrik Netzwerkziel</td>
<td></td>
</tr>
<tr>
<td>13 286 ::/0</td>
<td>fe80::20b:fdff:feac:c560</td>
</tr>
<tr>
<td>16 281 ::/0</td>
<td>fe80::5efe:192.168.20.1</td>
</tr>
<tr>
<td>1 306 ::/1/128</td>
<td>Auf Verbindung</td>
</tr>
<tr>
<td>14 18 2001::/32</td>
<td>Auf Verbindung</td>
</tr>
<tr>
<td>14 266 2001::d5c7:a2d6:281b:276f:3f57:ff32/128</td>
<td></td>
</tr>
<tr>
<td>13 38 2001::c::0:20::/64</td>
<td>Auf Verbindung</td>
</tr>
<tr>
<td>13 286 2001::c::0:20::/113/128</td>
<td>Auf Verbindung</td>
</tr>
<tr>
<td>13 286 2001::c::0:20::222::64ff:fe6b:8532/128</td>
<td>Auf Verbindung</td>
</tr>
<tr>
<td>13 286 2001::c::0:20::8d2d:33b4:5455:ad15/128</td>
<td>Auf Verbindung</td>
</tr>
<tr>
<td>16 33 2001::c::0:40::/64</td>
<td>Auf Verbindung</td>
</tr>
<tr>
<td>16 281 2001::c::0:40::0::5efe:192.168.0.205/128</td>
<td>Auf Verbindung</td>
</tr>
<tr>
<td>13 286 fe80::/64</td>
<td>Auf Verbindung</td>
</tr>
<tr>
<td>14 266 fe80::/64</td>
<td>Auf Verbindung</td>
</tr>
<tr>
<td>16 281 fe80::5efe:192.168.0.205/128</td>
<td>Auf Verbindung</td>
</tr>
<tr>
<td>17 296 fe80::5efe:192.168.10.100/128</td>
<td>Auf Verbindung</td>
</tr>
<tr>
<td>13 286 fe80::222::64ff:fe6b:8532/128</td>
<td>Auf Verbindung</td>
</tr>
<tr>
<td>14 266 fe80::281b:276f:3f57:ff32/128</td>
<td>Auf Verbindung</td>
</tr>
<tr>
<td>1 306 ff00::/8</td>
<td>Auf Verbindung</td>
</tr>
<tr>
<td>14 266 ff00::/8</td>
<td>Auf Verbindung</td>
</tr>
<tr>
<td>13 286 ff00::/8</td>
<td>Auf Verbindung</td>
</tr>
</tbody>
</table>

**Global Addresses**

**Link Local Addresses**
Agenda

- Address Autoconfiguration
- Neighbor discovery, Router discovery
- Host configuration with DHCPv6
- Transition technologies, ISATAP & Teredo Tunnel
Internet Control Message Protocol v6 (ICMPv6) plays an important role.
Many new ICMPv6 messages have been defined.
ICMPv6 Messages

Error and Control Messages:
- Echo Request/Reply
- Destination unreachable
- Time exceeded
- Redirect
- Parameter Problem
- Packet too big

Multicast Listener Discovery (MLD) Messages:
- Multicast Listener Query
- Multicast Listener Report
- Multicast Listener Done

Neighbor Discovery (ND) Messages:
- Neighbor Solicitation
- Neighbor Advertisement
- Router Solicitation
- Router Advertisement

IPv6

LAN, WLAN and WAN Protocols

© Leutert NetServices
The initial client startup process includes the following steps:

Frame #

1. Duplicate Address Detection after Link-Local autoconfiguration
2. Router Discovery
3. Router Advertisement and global address autoconfiguration
4. Neighbor Discovery (searching for Router MAC)
5. Neighbor Advertisement (reply from Router with MAC)
6. Duplicate Address Detection with acquired global address
Agenda

• Address Autoconfiguration
• Neighbor discovery, Router discovery
• Host configuration with DHCPv6
• Transition technologies, ISATAP & Teredo Tunnel
Despite Address Autoconfiguration, DHCP plays an important role in IPv6 environment. It is required to provide clients with additional parameters like DNS server address and many other options.

**DHCPv6 offers different level of control over the workstations:**

<table>
<thead>
<tr>
<th>Client parameters</th>
<th>Stateless Auto Address Config. RFC2462</th>
<th>Stateless DHCP Service for IPv6 RFC3736</th>
<th>Stateful DHCPv6 RFC3315</th>
</tr>
</thead>
<tbody>
<tr>
<td>Subnet Prefix &amp; Mask</td>
<td>From Router Advertisements (O-Flag=0 M-Flag=0)</td>
<td>From Router Advertisements (O-Flag=1 / M-Flag=0)</td>
<td>From Router Advertisements (O-Flag=1 / M-Flag=1)</td>
</tr>
<tr>
<td>Interface Identifier</td>
<td>Auto Configuration</td>
<td>Auto Configuration</td>
<td>From DHCPv6 Server</td>
</tr>
<tr>
<td>DNS, NTP address etc.</td>
<td>Manual Configuration</td>
<td>From DHCPv6 Server</td>
<td>From DHCPv6 Server</td>
</tr>
</tbody>
</table>

O = Other Flag / M = Managed Flag
During this phase, the client is supplied with additional parameters:

Frame #

2. Router Discovery
3. Router Advertisement with ‘Other Flag’ set
6. Client contacts DHCP server
7. DHCP server delivers additional parameter like DNS, suffixes etc.
Host configuration with DHCPv6

DHCP server reply

Client

Subnet 2001:cafe:0:20::

Router

Subnet 2001:cafe:0:30::

DHCP Server

2001:cafe:0:30::199

DHCP Reply

DHCP Relay-reply

IPv6_DHCP_Relay_01.pcap - Wireshark

File Edit View Go Capture Analyze Statistics Help

Filter:  

<table>
<thead>
<tr>
<th>No.</th>
<th>Time</th>
<th>IPv6 Source</th>
<th>IPv6 Destination</th>
<th>Protocol</th>
<th>Info</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>0.000000</td>
<td>2001:cafe:0:30::3</td>
<td>2001:cafe:0:30::199</td>
<td>DHCPv6</td>
<td>Relay-forward</td>
</tr>
<tr>
<td>2</td>
<td>0.000676</td>
<td>2001:cafe:0:30::199</td>
<td>ff02::1:ff00::3</td>
<td>ICMPv6</td>
<td>Neighbor solicitation</td>
</tr>
<tr>
<td>3</td>
<td>0.001176</td>
<td>2001:cafe:0:30::3</td>
<td>2001:cafe:0:30::199</td>
<td>ICMPv6</td>
<td>Neighbor advertisement</td>
</tr>
<tr>
<td>4</td>
<td>0.000041</td>
<td>2001:cafe:0:30::199</td>
<td>2001:cafe:0:30::3</td>
<td>ICMPv6</td>
<td>Neighbor solicitation</td>
</tr>
<tr>
<td>5</td>
<td>4.998115</td>
<td>fe80::20b:fdff:feac::c60</td>
<td>2001:cafe:0:30::199</td>
<td>ICMPv6</td>
<td>Neighbor solicitation</td>
</tr>
<tr>
<td>6</td>
<td>0.000245</td>
<td>fe80::20e:a::d4:cf:1963::571f</td>
<td>ff02::1::ffac::c60</td>
<td>ICMPv6</td>
<td>Neighbor solicitation</td>
</tr>
<tr>
<td>7</td>
<td>0.001314</td>
<td>fe80::20b:fdff:feac::c60</td>
<td>fe80::20e:a::d4:cf:1963::571f</td>
<td>ICMPv6</td>
<td>Neighbor advertisement</td>
</tr>
<tr>
<td>8</td>
<td>0.000051</td>
<td>2001:cafe:0:30::199</td>
<td>fe80::20b:fdff:feac::c60</td>
<td>ICMPv6</td>
<td>Neighbor advertisement</td>
</tr>
<tr>
<td>9</td>
<td>2.248004</td>
<td>2001:cafe:0:20::222:64ff:fe6b:8532</td>
<td>2001:cafe:0:30::199</td>
<td>DNS</td>
<td>Standard query A wpad.1</td>
</tr>
<tr>
<td>10</td>
<td>0.000274</td>
<td>2001:cafe:0:30::199</td>
<td>2001:cafe:0:20::222:64ff:fe6b:8532</td>
<td>DNS</td>
<td>Standard query response</td>
</tr>
<tr>
<td>11</td>
<td>1.696142</td>
<td>2001:cafe:0:20::222:64ff:fe6b:8532</td>
<td>2001:cafe:0:30::199</td>
<td>DNS</td>
<td>Standard query SRV _ldap...</td>
</tr>
</tbody>
</table>
Host configuration with DHCPv6

At this state, the client is configured with all required parameters:

C:\windows\system32>ipconfig /all

Ethernet-Adapter LAN-Verbindung:

Verbindungsspezifisches DNS-Suffix: ipv6.ch
Beschreibung: Marvell Yukon 88E8072 PCI-E Gigabit Ethernet
Physikalische Adresse: 00-22-64-6B-85-32
DHCP aktiviert: Ja
Autoconfiguration aktiviert: Ja
IPv6-Adresse: 2001:cafe:0:20:222:64ff:fe6b:8532 (Bevorzugt)
Verbindungslokale IPv6-Adresse: fe80::222:64ff:fe6b:8532%13 (Bevorzugt)
Lease läuft ab: Sonntag, 1. März 2009 11:46:03
Standardgateway: fe80::20b:fdff:feac:c561%13
DHCPv6-IAID: 251667044
DHCPv6-Client-DUID: 00-01-00-01-10-D2-B9-65-00-22-64-6B-85-32
DNS-Server: 2001:cafe:0:30:199
Suchliste für verbindungsspezifische DNS-Suffixe:
yourdomain.ch
ipv6.ch
dummy.ch
• Address Autoconfiguration
• Neighbor discovery, Router discovery
• Host configuration with DHCPv6
• Transition technologies, ISATAP & Teredo Tunnel
ISATAP (Intra-Site Automatic Tunnel Addressing Protocol)

- ISATAP enables easy deployment of IPv6 in existing IPv4 infrastructure
- ISATAP hosts do not require any manual configuration
- IPv6 address contains an embedded IPv4 source or destination address
- ISATAP clients use locally assigned IPv4 address (public or private) to create the 64-bit interface identifier

**IPv6 Transition Technologies**
ISATAP (Intra-Site Automatic Tunnel Addressing Protocol)

- ISATAP interface is created at the same time the IPv6 stack is installed

- Local interface ID # (%17) must be appended to destination address

  Ping fe80::5efe:192.168.30.199%17
IPv6 Transition Technologies

ISATAP (Intra-Site Automatic Tunnel Addressing Protocol)

Frame 1 (118 bytes on wire, 118 bytes captured)


Internet Protocol Version 6
  0110 .... = Version: 6
  .... 0000 0000 .... .... .... .... .... .... = Traffic class: 0x00000000
  .... .... .... 0000 0000 0000 0000 = Flowlabel: 0x00000000
  Payload length: 40
  Next header: ICMPv6 (0x3a)
  Hop limit: 128
  Source: fe80::5efe:c0a8:1464 (fe80::5efe:c0a8:1464)
  Destination: fe80::5efe:c0a8:1ec7 (fe80::5efe:c0a8:1ec7)

© Leutert NetServices
SHARKFEST ‘11 | Stanford University | June 13–16, 2011
ISATAP (Intra-Site Automatic Tunnel Addressing Protocol)

- ISATAP can also be used to access **native IPv6 destinations**
- Client resolves **ISATAP router IPv4 address** through internal DNS
- Client requests **IPv6 global unicast prefix** from ISATAP router
- Client sends **IPv6 in IPv4 embedded packets** to ISATAP router

- **ISATAP router unpacks embedded packets and forwards them**
IPv6 Transition Technologies

ISATAP (Intra-Site Automatic Tunnel Addressing Protocol)
IPv6 Transition Technologies

ISATAP (Intra-Site Automatic Tunnel Addressing Protocol)

- Client received prefix 2001:c0afe:0:40:: from ISATAP router

- Client installs address of Default Gateway
IPv6 Transition Technologies

ISATAP (Intra-Site Automatic Tunnel Addressing Protocol)

- Command ‘route print -6’ displays clients routing table
IPv6 Transition Technologies

Teredo Tunnel

- Tunneling method named after Teredo Navalis (shipworm)
- Teredo encapsulates IPv6 packets within UDP/IPv4 datagram
- Most NAT Routers can forward these packets properly
- Teredo allows a client to communicate with a native IPv6 server
- Teredo Server and Teredo Relay in the Internet care for transitions

- Teredo tunnels are set up automatically, no configuration is needed.
Teredo Tunnel interface

- In WIN Vista clients, the Teredo Tunneling I/F is created automatically.
- The IPv6 prefix of all Teredo clients is `2001:0::/32`.
- The client resolves `teredo.ipv6.microsoft.com` to build the `/64` prefix.
- The value `5ef5:79fd` is the IPv4 Teredo server address: `94.245.121.253`.
- `Miredo` is the open-source Teredo tunneling software for Linux, BSD etc.
IPv6 Transition Technologies

Teredo Tunnel initialization (File IPV6_Teredo/www_six_heise_de)
IPv6 Transition Technologies

Teredo Tunnel initialization (File IPV6_Teredo_www_six_heise_de)

Step 1
ICMP Echo Request
Bubble Packet (with IP and UDP Port of Teredo Relay)

Step 2
Forwarding Echo Request to Server
Responds with Bubble packet

Step 3
Server IPv6 (SRV)
www.six.heise.de
Echo Reply to Relay

Step 4
IPv6 Internet

Step 5
Teredo Relay (TR)

Step 6
Teredo Server (TS)
IPv4 Internet

Step 7
Teredo Client (TC)

IPv4 Subnets
Enterprise IPv4 Subnets

Step 8
NAT-Router (NR)

IPv4 Internet

Step 9
TCP SYN

© Leutert NetServices
SHARKFEST ‘11 | Stanford University | June 13–16, 2011
Teredo Tunnel

• When starting, a Windows-based computer using Teredo resolves the IPv4 address of the Teredo server teredo.ipv6.microsoft.com
• By the Router solicitation/advertisement dialog through Teredo, the client receives a valid IPv6 prefix
• When activated, the Teredo client contacts Teredo server to obtain information such as the type of NAT that the client is behind
• If the client has only link-local or Teredo IPV6 addresses assigned, then the DNS Client will send only queries for A records
• The client needs at least one valid IPv6 address configured (may be manually) in order to query for AAAA records
• Windows Vista Client computers will always use IPV6 over IPV4
• A default route may have to be configured on Teredo interface:
  
  netsh interface ipv6 add route ::/0 14 ← Teredo Interface ID
IPv6 Transition Technologies

Teredo commands & settings

- `netsh interface teredo show state`
- `netsh interface teredo set state disabled`
- `netsh interface teredo set state client`
- `netsh interface teredo set state enterpriseclient`
- `netsh int ipv6 set teredo client teredo.remlab.net`
- `netsh int ipv6 set teredo client teredo.ipv6.microsoft.com`
- `netsh interface ipv6 show address`
- `netsh interface ipv6 add address "Local Area Connection 2" fd00:0:0:1::1`
- `netsh interface ipv6 add route ::/0 14`
- **Windows firewall must be activated to enable Teredo!**
IPv6 Session Summary

• Verify IPv6 readiness of your suppliers
• Verify IPv6 readiness of your applications
• IPv6 can perfectly coexist with IPv4
• Start experimenting using ISATAP and Teredo
• Network migration can be done smoothly
• Train yourself and your people
• Wireshark is the perfect tool to learn and train
• Interesting IPv6 references:


  www.ipv6forum.com World-wide consortium of Internet vendors aiming to promote IPv6. Includes mailing lists, event listings, technical information, and links

Thanks for visiting

Rolf Leutert, Leutert NetServices, [www.wireshark.ch](http://www.wireshark.ch)