Caribbean Workshop - Guadeloupe

05 - 08 March '07

Stateless Auto-configuration and NDP

Bernard.Tuy@renater.fr
Simon.Muyal@renater.fr
Stig.Venaas@uninett.no
Bertus Habraken <bhabrake@cisco.com>

Laboratory Exercise: *Stateless Auto-configuration and NDP*

Objectives

In this laboratory exercise you will complete the following tasks:

- *Understand basic IPv6 concepts (NDP)*
- *Analyse messages NA/NS and RA/RS*

Visual Objective

The following figure shows the topology of the current laboratory.

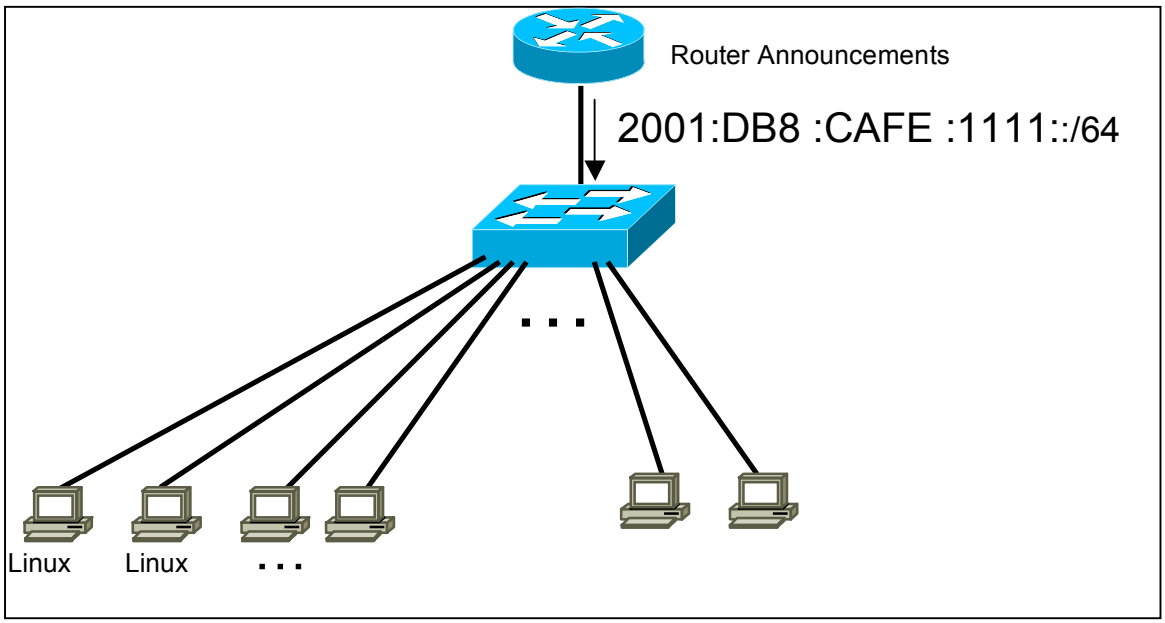

Figure 1: Scenario topology

Scenario

The router is sending periodically the correspondent router advertisement messages.
Now that we have IPv6 support on each link. We will use Linux for this hands-on to use 2 methods for analyse the packets: Ethereal and TCPDump.

Task 1: Using some IPv6 related tools

Complete the following exercise's steps:

Step1: Using *tcpdump* (`tcpdump -t -n -vv -s 512 ip6 -i <Interface>`) or `wireshark (Ethereal)`, capture neighbour advertisement and neighbour solicitation messages. To do that, retrieve the IPv6 address of your neighbour and ping this address.

- Which IPv6 addresses (source - destination) are used in this messages?

Step 2: Without looking into the router, identify the router's link-local address for your lan (**Tip:** Use the command **`ip -6 neigh …`**)

- Ping router's addresses (link-local and global addresses). Did you successfully ping router's link-local address? (**Tip:** Use the option **`-I`** in **`ping6`** command)

Step 3: Using *tcpdump* (`tcpdump -t -n -vv -s 512 ip6 -i <Interface>`) or `wireshark (Ethereal)`, capture router advertisement and router solicitation messages. If you want, look at Appendix *A* for *tcpdump* basic or Appendix B for wireshark information or use your linux manual pages.

- Which IPv6 addresses (source - destination) are used in this messages?

Step 4: ping the following multicast address ff02::1 (all the nodes in the LAN) and capture messages. Analyse the messages (**Tip:** Use the option **`-I`** in **`ping6`** command).

Step 5: Disable autoconfiguration for eth0 and configure the static address corresponding to your laptop number NN (modify /etc/network/interfaces):

```
                iface eth0 inet6 static
turn off autoconf:   up sysctl -q -w net.ipv6.conf.eth0.autoconf=0
                     address 2001:DB8:CAFE:1111::1
                     netmask 64
```

Summary

After completing these exercises, you should be able to:

- *Understand basic IPv6 concepts (NDP)*
- *Analyse messages NA/NS and RA/RS*

Appendix A

Using "IPv6 tcpdump"

On Linux, *tcpdump* is the major tool for packet capturing. Below you can find some examples. IPv6 support in tcpdump is available since version 3.6. tcpdump uses expressions for filtering packets to minimize the "noise":

- **icmp6:** filters native ICMPv6 traffic
- **ip6:** filters native IPv6 traffic (including ICMPv6)
- **proto ipv6:** filters tunneled IPv6−in−IPv4 traffic
- **not port ssh:** to suppress displaying SSH packets for running *tcpdump* in a remote SSH session

Some more command line options are very useful to catch and print more information in a packet, mostly interesting for digging into ICMPv6 packets:

- **-s 512**: increase the snap length during capturing of a packet to 512 bytes
- **-n**: don't convert host addresses to names.
- **-i**: Listen on <interface>
- **-vv:** Even more verbose output

Example: IPv6 ping to 2001:DB8:CAFE:22::1 native over a local link

```
tcpdump □t □n □vv -s 512 ip6 □i eth0

tcpdump: listening on eth0
2001:db8:cafe:22:2e0:18ff:fe90:9205 > 2001:db8:cafe:22::1: icmp6: echo
¬ request (len 64, hlim 64)
2001:db8:cafe:22::1 > 2001:db8:cafe:22:2e0:18ff:fe90:9205: icmp6: echo
¬ reply (len 64, hlim 64)
```

Appendix *B*
Compact "Ethereal/Wireshark" documentation

Ethereal is used by network professionals around the world for troubleshooting, protocol analysis, software and protocol development. Its open source license allows talented experts in the networking community to add enhancements. It runs on all popular computing platforms, including Linux, and Windows. See further information at http://www.wireshark.com/.

In order to capture packets, use the menu (***Capture*** -> ***Interfaces…***). Then choose the interface you want to use and click on the correspondent ***Prepare*** button. In the ***Capture Options*** window check both "***Update list of packets in real time***" and "***Automatic scrolling in live capture***". Then uncheck both "***Enable transport name resolution***" and "***Enable MAC name resolution***" (see figure 3).

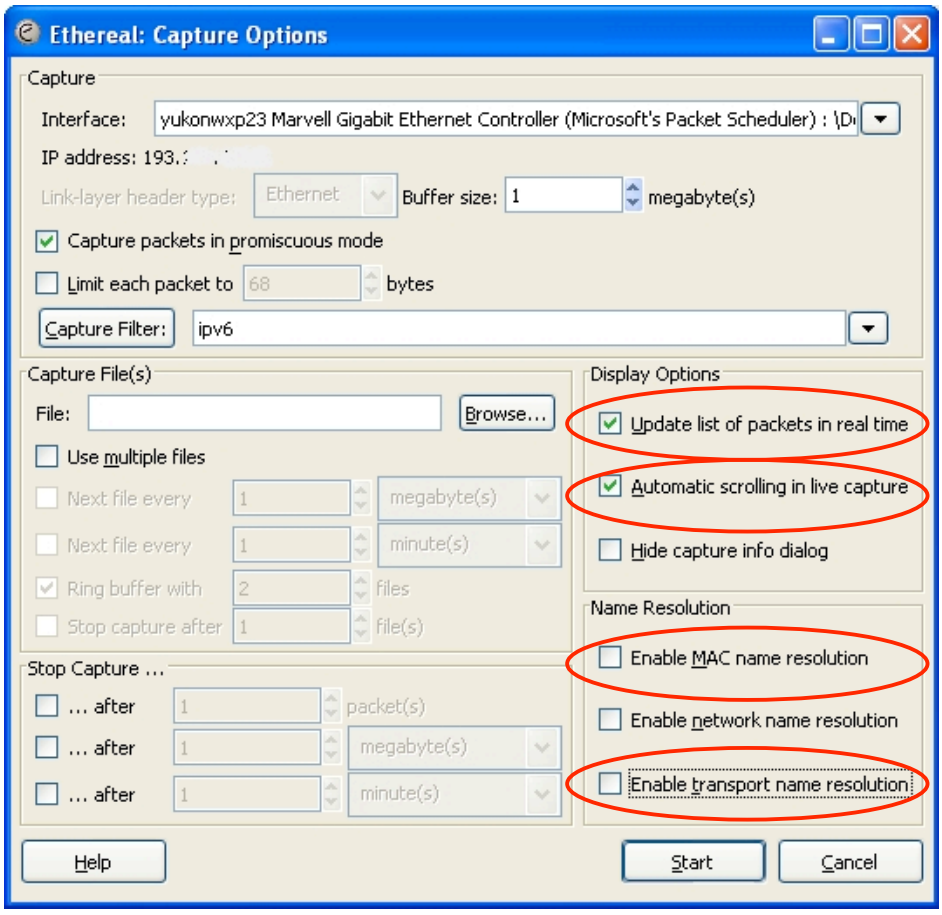

Figure 2: Ethereal capture options

If you want to capture only a specific set of packets, use ***Capture Filter*** option (in the ***Capture Options*** window), as shown in Figure 4. Use the capture filter ***`ipv6`*** (some Ethereal versions use ***ip6***) to capture only IPv6 packets or ***`icmpv6`*** to capture only ICMPv6 packets.

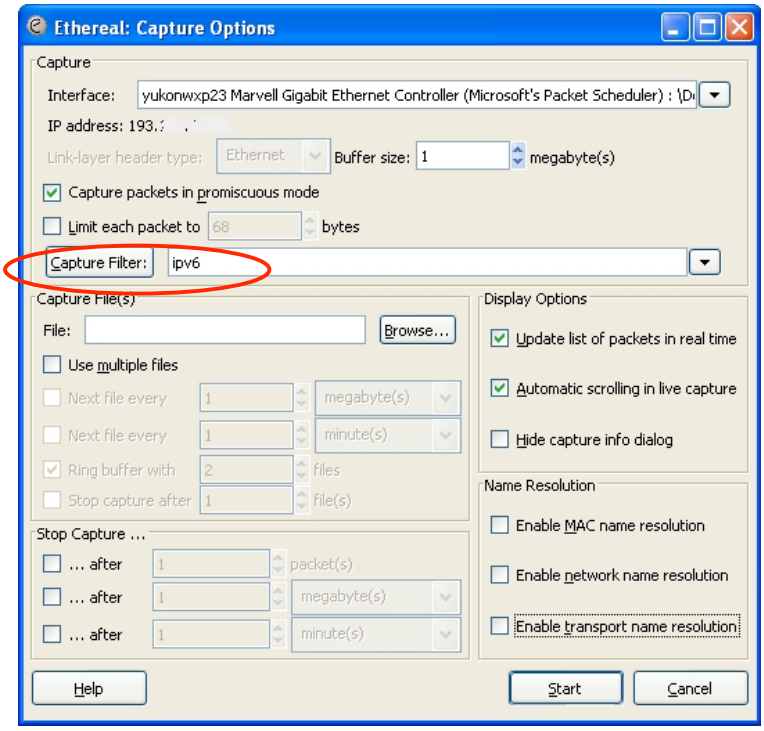

Figure 3: Ethereal packet capture filters

After having captured some traffic, you can also filter the results using the ***Filter*** option, as shown in the Figure 5.

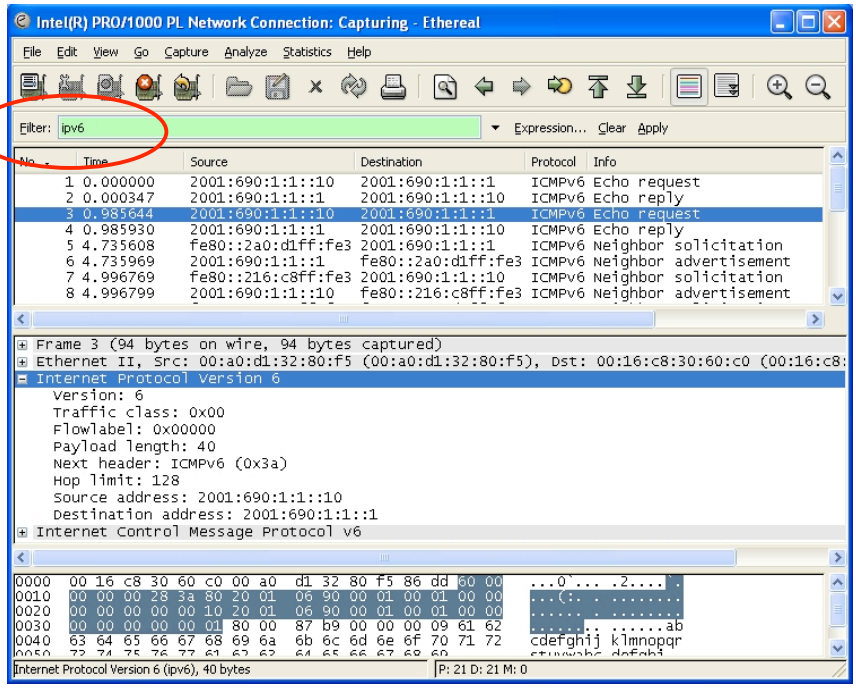

Figure 4: Ethereal interface

(**Tip:** Use the filter ***ipv6*** (some Ethereal/Wireshark's versions uses ***ip6***) to show only IPv6 packets, ***icmpv6.code==0*** to show ICMP packets of specific code or ***http*** to show HTTP traffic.)