



***Central Asian Workshop – Ashgabat
Turkmenistan
24 -26 April 2007***

Host Configuration (Windows XP)

Peter Kirstein, Piers O'Hanlon
<kirstein,p.ohanlon@cs.ucl.ac.uk>
Mohacsi Janos <mohacsi@niif.hu>
Nikolay Pakulin <npak@ispras.ru>

Laboratory Exercise: *Host Configuration (Windows XP)*

Objectives

In this laboratory exercise you will complete the following tasks:

- *Activate the IPv6 protocol stack on WinXP PC's*
- *Understand basic IPv6 concepts*
- *Manually add/remove IPv6 addresses on Win XP*
- *Disable 6to4 and isatap virtual interfaces*

Visual Objective

The following figure shows the topology of the current laboratory.

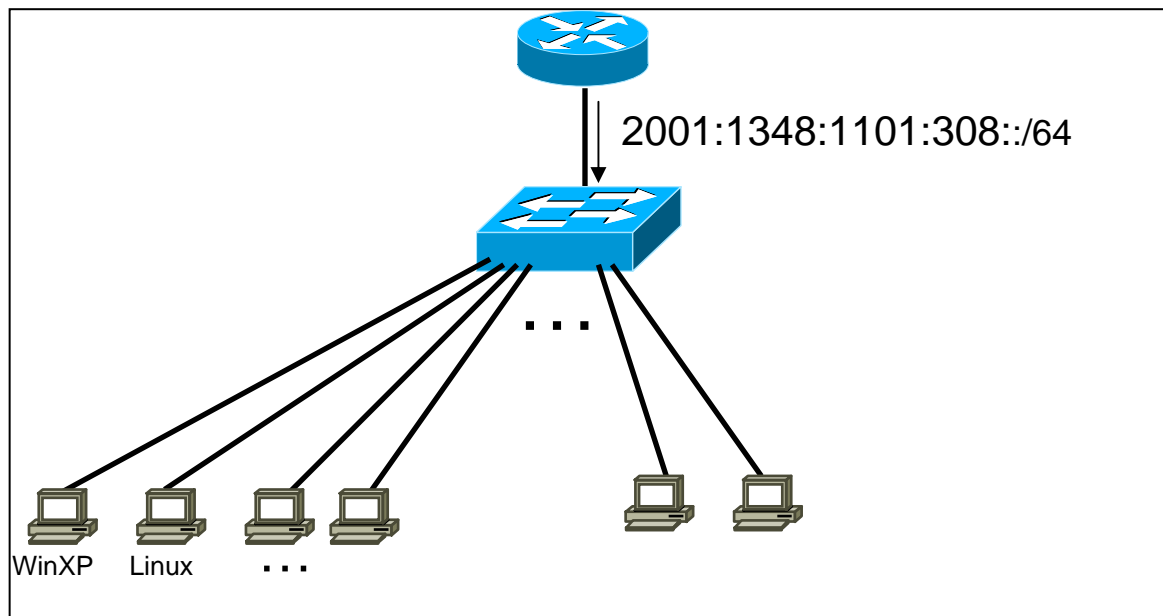


Figure 1 : Scenario topology

Scenario

The router is periodically sending router advertisement messages (see autoconfiguration session). Now that we have IPv6 support on each link, we need to activate IPv6 on our computer's Operating system, in this case, Windows XP.

Task 1: Enabling IPv6 on Windows XP

Complete the following exercise's steps

Step 1: Enable IPv6 on your Windows XP (SP2)

(**Tip:** There are two alternative methods to do it)

- Using the WinXP GUI (Install-> protocol->ipv6)

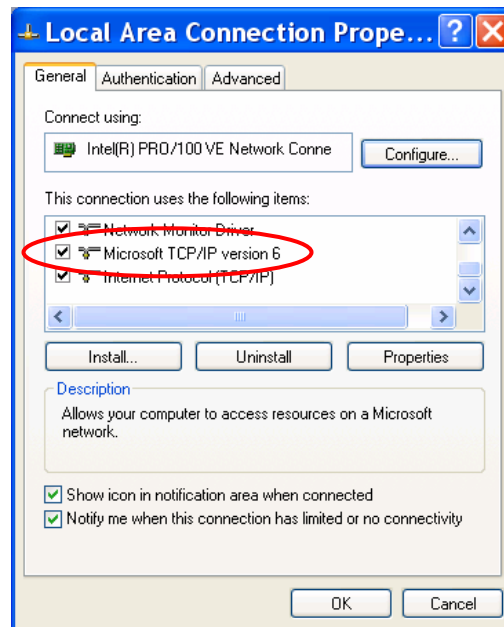


Figure 2: IPv6 GUI installation

- Or from a CLI (cmd.exe) run `ipv6 install`

Task 2: Display and identify existing IPv6 addresses

Complete the following exercise's steps

Step 1: Identify the different interfaces at your PC. Which ones are related to IPv6 transition mechanisms?

From a CLI run the following commands:

- `ipconfig /all`
- `netsh interface ipv6 show interface` (look at the end of the document for `netsh` basic information).
- `ipv6 -v if`

Step 2: Identify different types of IPv6 addresses (Note! You already have IPv6 addresses and you didn't have to make any configuration on your host machine)

- Link local (**Tip:** Search for `fe80::...`)

- auto-configuration IPv6 address (**Tip:** Search for ...ff:fe...)
- IPv6 address due to privacy extension
- multicast addresses
- validity of addresses (**Tip:** Use the command `netsh interface ipv6 show address <interface>`)

Task 3: Using some IPv6 related tools

Step 1: Ping local IPv6 addresses

- Ping6 the IPv6 localhost address (::1)
- Ping6 your host's link-local and global addresses

Step 2: Without looking into the router, identify the router's link-local address

- What's the appropriate command?
 - `Tracert6`?
 - `Netsh interface ipv6 show neighbors`?
 - `ipconfig`?
- Ping router's addresses (link-local and global addresses). Did you successfully ping router's link-local address?

Step 3: Using *wireshark/ethereal*, capture router advertisement and router solicitation messages. (Look at the end of the document for wireshark/ethereal basic information).

- Which IPv6 addresses (source - destination) are used in these messages?
- In `netsh` command prompt, renew your IPv6 address (**Tip:** `netsh interface ipv6 ?`). Did you capture any router solicitation message? Then, look at the first router advertisement message after the RS message. What's the source/destination address? Are they equal to the previous RA message? Why?

Step 4: Display your current IPv6 routing table (**Tip:** Use command `netsh interface ipv6 show routes level=verbose`).

Task 4: Add/Remove IPv6 addresses

Complete the following exercise's steps

Step 1: Manually add an IPv6 address

- On your local area connection, add, for example, the following address: 2001:1348:1101:308::10 (Note: WinXP doesn't allow setting of prefixlen, though this is fixed in Vista/2003)

- Duplicate Address Detection (DAD) counter should indicate if more than one machine has same address. (Tip1: see interface stats: nets hint ipv6 show int <interface_num>)
(Tip 1: `netsh interface ipv6 add ...`)
(Tip 2: <interface -> interface number or name>)

Step 2: Manually remove an IPv6 address

- Remove the address created on the previous step (Tip: `netsh ipv6 interface delete ...`)

Step 3: Disable privacy extensions (RFC3041). (Tip: Use the command `netsh interface ipv6 set privacy`)

- Check your current addresses
- What could be the problems in terms of security if you enable/disable privacy extension?

Step 4: Disable 6to4 and isatap virtual interfaces.

(Tip 1: Use the command `netsh interface ipv6 6to4 set state ...`)

(Tip 2: Use the command `netsh interface isatap set ...`)

Check your current interfaces.

Summary

After completing these exercises, you should be able to:

- *Enable and configure IPv6 addresses on windows XP*
- *Identify different address types*
- *Manually add/remove IPv6 addresses*
- *Disable 6to4 and isatap virtual interfaces*

Appendix A

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).

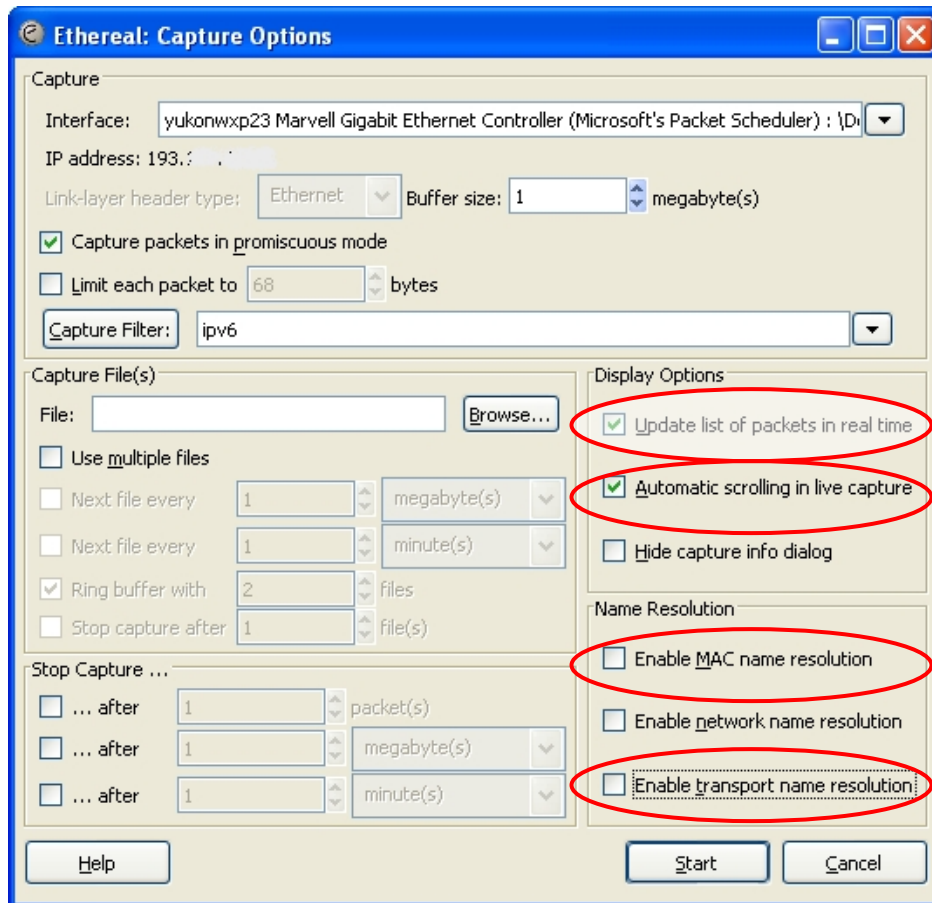


Figure 3: Ethereal capture options

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.

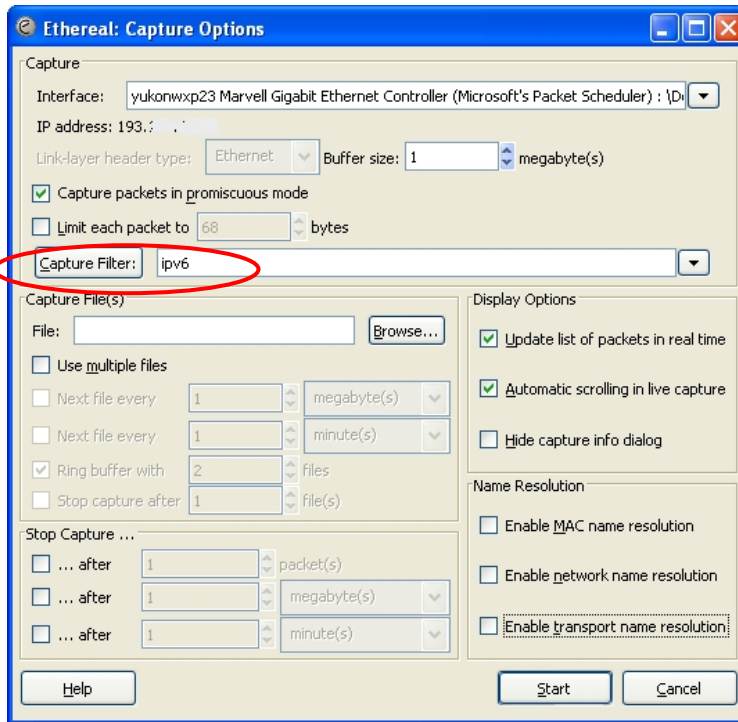


Figure 4: Ethereal packet capture filters

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

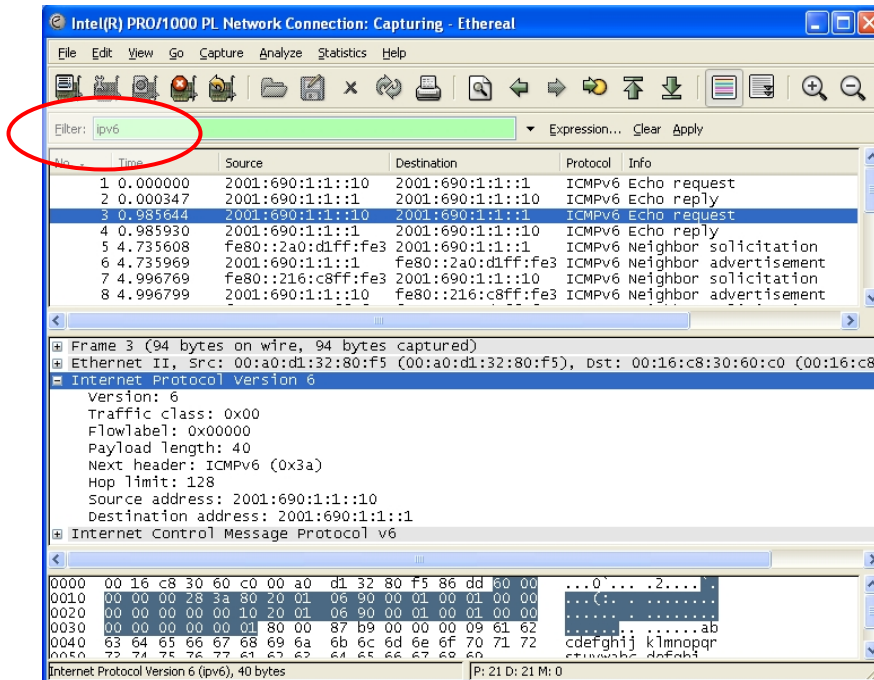


Figure 5: Ethereal interface

(**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.)

Appendix B

Using Netsh

Netsh is a command-line scripting utility, for the Windows Operating System, which allows you to display or modify a computer's network configuration currently running.

Netsh contexts

To run a **netsh** command, you must start **netsh** from the CLI prompt and change to the context that contains the command you want to use. The contexts that are available to you depend on which networking components you have installed. For example, if you type **dhcp** at the **Netsh** command prompt, you change to the DHCP context, but if you do not have DHCP installed the following message appears:

The following command was not found: dhcp.

Running Netsh commands from the Netsh.exe command prompt

Netsh uses the following standard commands in all contexts that you can run from a Netsh.exe command prompt (that is, netsh>). There might be functional differences between Netsh context commands on Windows 2003 and Windows XP.

1. To view the command syntax, click a command.
2. **..** Moves to the context that is one level up.
3. **{/?|?|help|h}** Displays help at the command prompt.
4. **Abort** Discards any changes made in offline mode. **Abort** has no effect in online mode.
5. **quit** Exits Netsh.exe

Example

The following sample script changes a context from the root context to the **interface ipv6** context and adds an IPv6 address:

```
C:\> netsh
netsh>
netsh> interface ipv6
netsh interface ipv6>
netsh interface ipv6> add address interface=7 address=2001:ABBA::1
```