

Central America Workshop - Guatemala City Guatemala 30 January - 1 February '07

Host Configuration (Windows XP)

Miguel Baptista(miguel.baptista@fccn.pt) Piers O'Hanlon (p.ohanlon@cs.ucl.ac.uk) Pedro Lorga (lorga@fccn.pt) Simon Muyal (muyal@renater.pt)

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)

Local Area Connection Prope?
This connection uses the following items:
Install Uninstall Properties
Description Allows your computer to access resources on a Microsoft network.
 Show icon in notification area when connected Notify me when this connection has limited or no connectivity
OK Cancel

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?
 - O Tracert6?
 - O Netsh interface ipv6 show neighbors?
 - o 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)

IPv<mark>6DISS</mark>emination and Exploitation

• 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).

C Ethereal: Captur	e Options		
Capture			
Interface: yukonw	xp23 Marvell Gig	abit Ethernet Controllei	r (Microsoft's Packet Scheduler) : \D
IP address: 193.3			
Link-layer header type	;; Ethernet	V Buffer size: 1	🗢 megabyte(s)
🔽 Capture packets in	promiscuous ma	de	
📃 Limit each packet to	68	🗘 bytes	
Capture Filter: ipve	5		
Capture File(s)			Display Options
File:		Browse	Update list of packets in real time
Use <u>m</u> ultiple files			
Next file every	1	megabyte(s) 🗸	Automatic scrolling in live capture
Next file every	1	minute(s) 🗸	Hide capture info dialog
💌 Ring buffer with	2	files	Name Recolution
Stop capture after	1	file(s)	
Stop Capture			Enable MAC name resolution
🔲 after 🛛 1	🔶 P	acket(s)	Enable network name resolution
🔲 after 1	÷	megabyte(s) 🗸 🗸	
🔲 after 🛛 1	\$	minute(s) 🗸 🗸	Enable transport name resolution
			<u>S</u> tart <u>C</u> ancel

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.



C Ethereal:	Capture Opti	ons	
Capture			
Interface:	yukonwxp23 Ma	rvell Gigabit Ethernet Controlle	er (Microsoft's Packet Scheduler) : \D
IP address: 1	.93./		
Link-layer he	ader type; Eth	ernet 💉 Buffer size: 1	🗢 megabyte(s)
Capture p	ackets in promisc	uous mode	
Limit each	nacket to 68	a hytes	
Cashing Tille			
	r: Ipv6	>	\
Capture File(s)			Display Options
File:		Browse	Update list of packets in real time
Use <u>m</u> ultip	le files		
Next file a	every 1	🗘 megabyte(s) 🗸	Automatic scrolling in live capture
Next file a	every 1	🗘 minute(s) 🗸	Hide capture info dialog
🗹 Ring buffe	er with 2	🗘 files	New Perchas
Stop capt	ure after 1	🗘 file(s)	Name Resolution
Stop Capture .			Enable MAC name resolution
🔲 after	1	packet(s)	Enable petwork name resolution
📃 after	1	🗘 megabyte(s) 🗸 🗸	
🔲 after	1	🗘 minute(s) 🗸 🗸	Enable transport name resolution
Help	٦		Start Cancel

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.

© In	tel(R)	PRO	/100	00 P	L N	etw	ork	c Co	опп	eci	tio	n: (Ca	ptu	irii	ng	- E	the	ere	al																		<
Eile	Edit	⊻iew	Gο	⊆a	aptu	re	Ana	alyze	•	Stat	isti	cs	Ħ	elp																								
Ð	<u>Å (</u>	Ø		M, I	<u>)</u>	. [2	Э)	×		R	Ş	ļ	3		Q	Ì			¢	>	Ċ)	1		1	-				44		Ð		Q	
Eilter	ipv6)																	•	Ē×	pre	ssio	n	9	lea	r į	3pp	ly							_	
Alo -		ime	/		S	ourc	е							De	stin	atio	n						Pro	toc	ol	In	fo											^
	10	0.00	0000 0347) 7	2	001	.:6 :6	90 90	:1:	1	:1	.0		20	01	:6 :6	90):1):1	:1	::	1 10		IC	MP MP	ν6 ν6	E	ch ch		neo neo	que nlv	≥st ∕	-						
	3 (.98	5644		2	001	:6	90	:1	1	:1	.0		20	01	:6	90	1:1	:1	::	1		IC	MP	v6	E	ch	0 1	rec	que	est							
	4 ().98 .73	5930 5608) 3	f	001 e8(.:6)::	90 2a	:1: 0:0	1 11f	f	fe	3	20	01	.:6	90 90	(1)	1		10 1		IC	MP MP	ν6 v6	E N	ch ei	o i ghl	nep 100	ply n s	/ 501	lic	it	at '	ion			
	64	.73	5969	9	2	001	:6	90 21	:1:	:1:	:1	fr		fe	80	::	2 a	0:	d1	ff	:fe	23	IC	MP MD	V6	N	ei	ğhl	100	r a	adv	/en	ti	sen	ient	t		
	84	.99	6799	3	2	001	:6	90	:1	:1:	:1	.0	:5	fe	80	:::	21	6:	<8	ff	:fe	≘3	IC	MP	v6	N	ei	ghl	100	n a	adv	/er	ti	sen	1en1	t		~
<																																					>	
	rame therr Ners Traf Flow Pavl	iet ion fic labe oad	94 c II, Prot : 6 cla el: ler	יאדנ Sr כככ נss נss טא(25 1 0 0 0 0 0 0 0 0 0 0	on 00: Ver x00 00 40	w1 :a0 :si	re :d	, 1:3 6	94 32:	8(/τε):f	5	Ca	10:	a0	ec):d	1)	32	:8	0:1	f5)),	DS	t:	0	0:	16	:c	8:	30	:60):c	:0	(00	:1)	6:C	3
	Next Hop Sour	hea limi ce a	ader it: addr	128 128 ess	:⊂M } ::	PV6)1:	0x: 69: 20:	3a) 0:1)	. : :	10	1.	• • 1																								
±Ι	nterr	iet (Iont	ro	M	ess	ag	e	Pro	oto)CO	1	ve	5																								
<																																						2
0000 0010 0020 0030 0040) 00) 00) 00) 00) 63) 72	16 00 00 00 64 74	C8 00 00 00 65 75	30 28 00 00 66 76	60 3 a 00 00 67 77	C0 80 10 01 68 61	0(2(2(8(6) 6)		10)1)1)0 ja	0 0 8 6 4	1 6 7 b	32 90 90 60 60	00000	0 0 0 0 0	F5 01 01 00 6e	800000	6 0 0 f	dd 01 01 09 70	6 0 6 7	0 0 1 1	00 00 00 62 72			.0 .(ef	gh	 : ;;	kr	2. 1mi	nor	. al								
Intern	et Prot	ocol Ve	ersion	6 (ip	v6),	40	oyte	s										P:	21	D:	21 🕅	1: 0																
]	Fi	gı	ır	e	5	:]	Et	h	er	ea	ıl	in	te	rf	ac	e													

(**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
```