IPv6 RA DoS Attacks

Sam Bowne

gogoNET Live 4

Nov 13, 2013

Sam Bowne

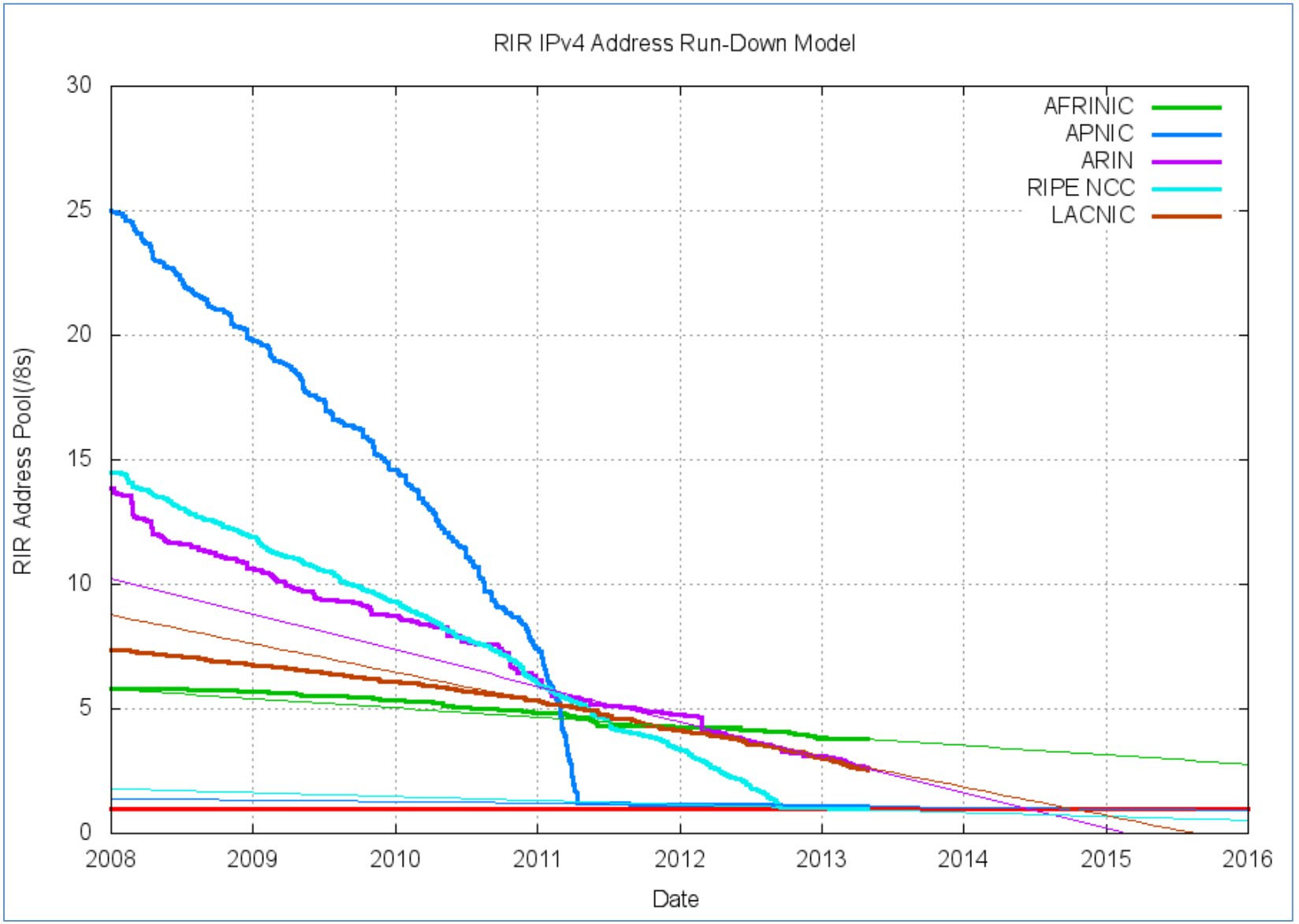
@sambowne

I teach Ethical Hacking at City College San Francisco. My statements are my own, not official positions of CCSF.

San Francisco · samsclass.info

IPv4 Exhaustion

IPv4 Exhaustion



One Year Left

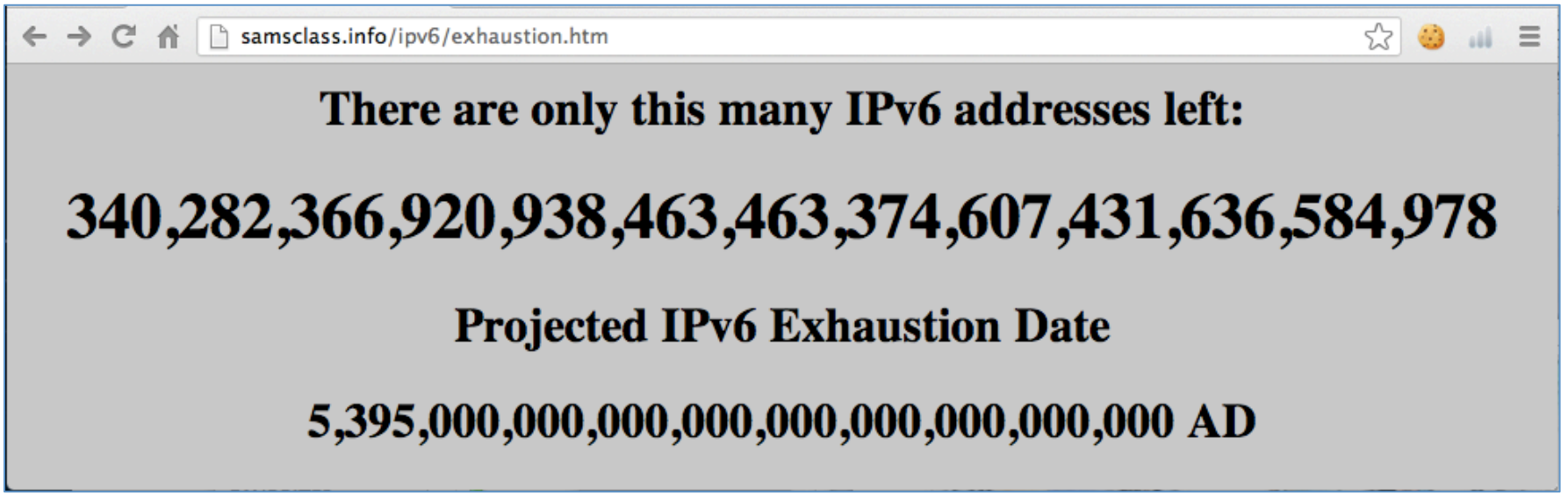
www.potaroo.net/tools/ipv4/

IANA Unallocated Address Pool Exhaustion:
03-Feb-2011

Projected RIR Address Pool Exhaustion Dates:

RIR	Projected Exhaustion Date	Remaining Addresses in RIR Pool (/8s)
APNIC:	**19-Apr-2011** (actual)	0.8694
RIPE NCC:	**14-Sep-2012** (actual)	0.9050
ARIN:	**15-Apr-2014**	2.3773
LACNIC:	**28-Aug-2014**	2.5294
AFRINIC:	**01-Aug-2020**	3.7308

IPv6 Exhaustion



Link-Local DoS

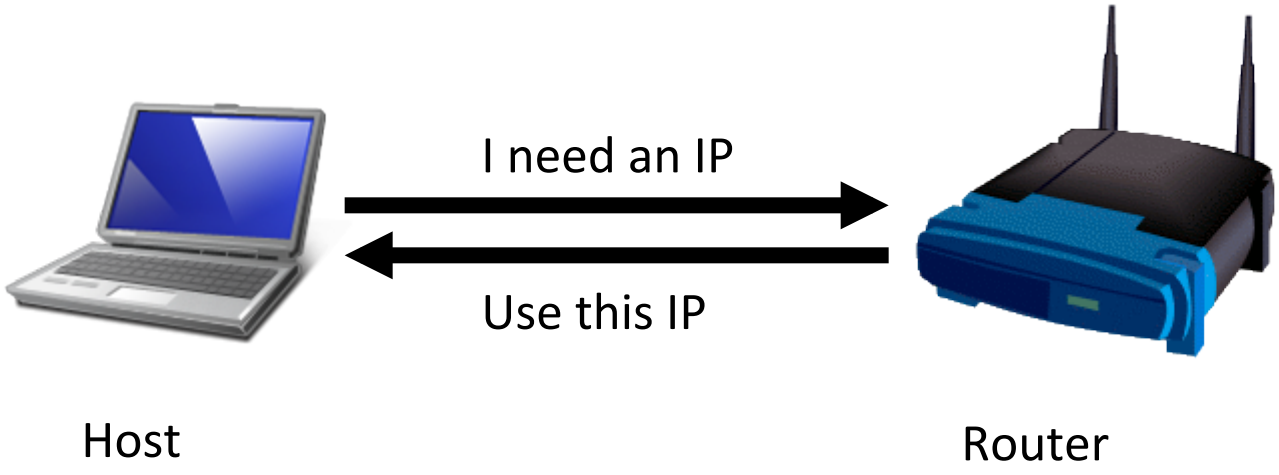
IPv6 Router Advertisements

Old Attack (from 2011)

IPv4: DHCP

PULL process

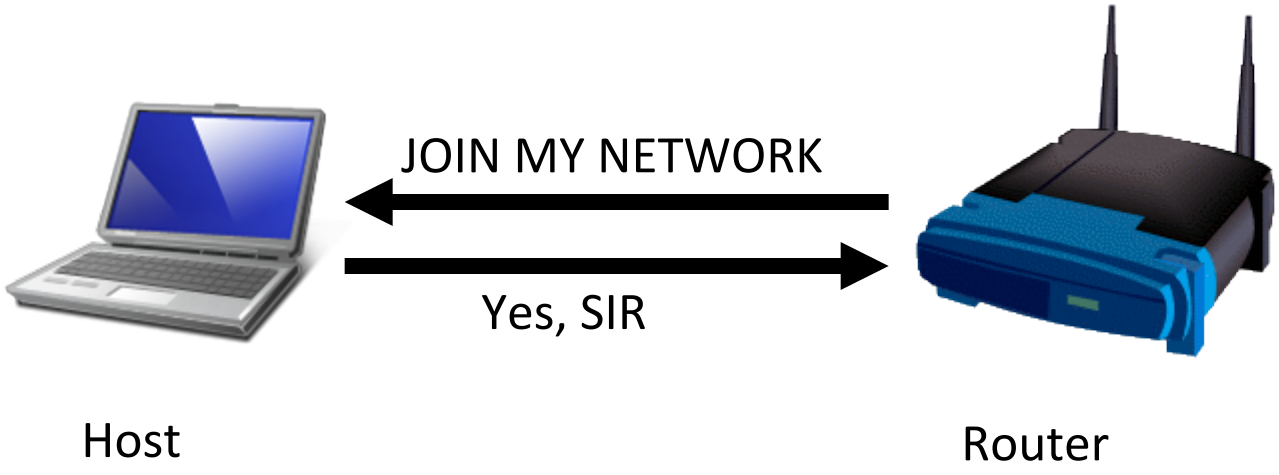
- Client requests an IP
- Router provides one



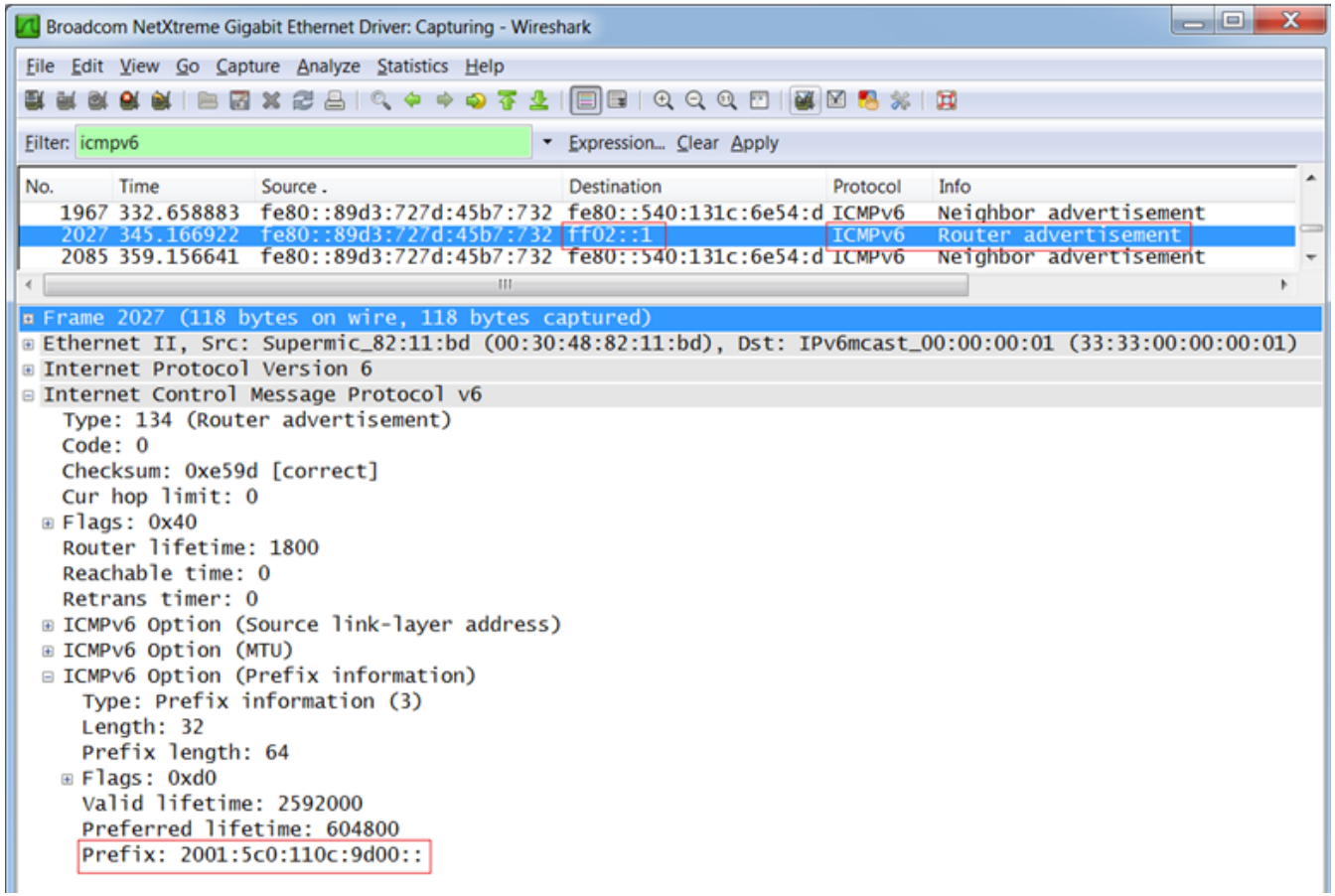
IPv6: Router Advertisements

PUSH process

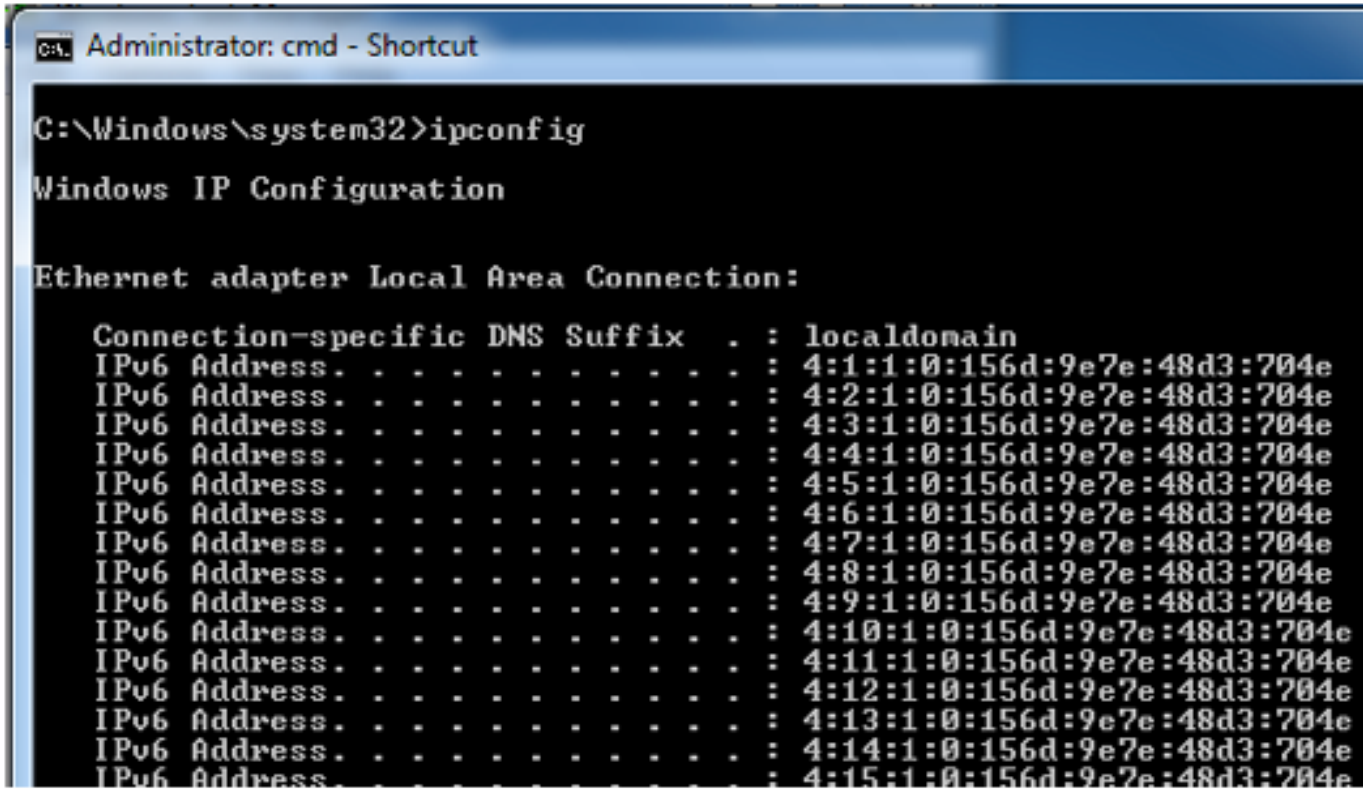
- Router announces its presence
- Every client on the LAN creates an address and joins the network



Router Advertisement Packet

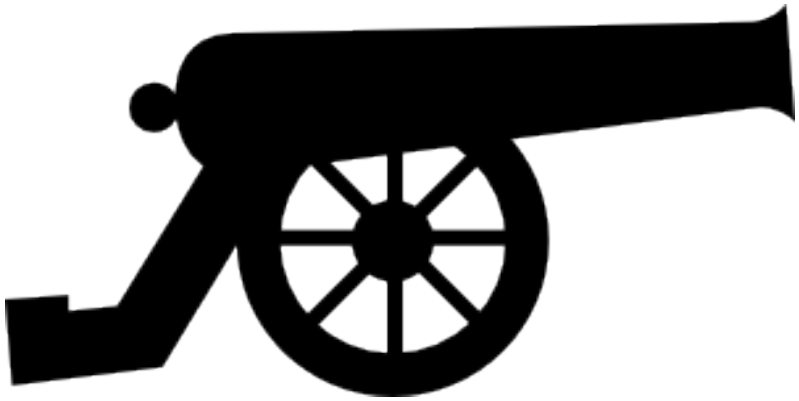


RA Flood (from 2011)
flood_router6



Effects of flood_router6

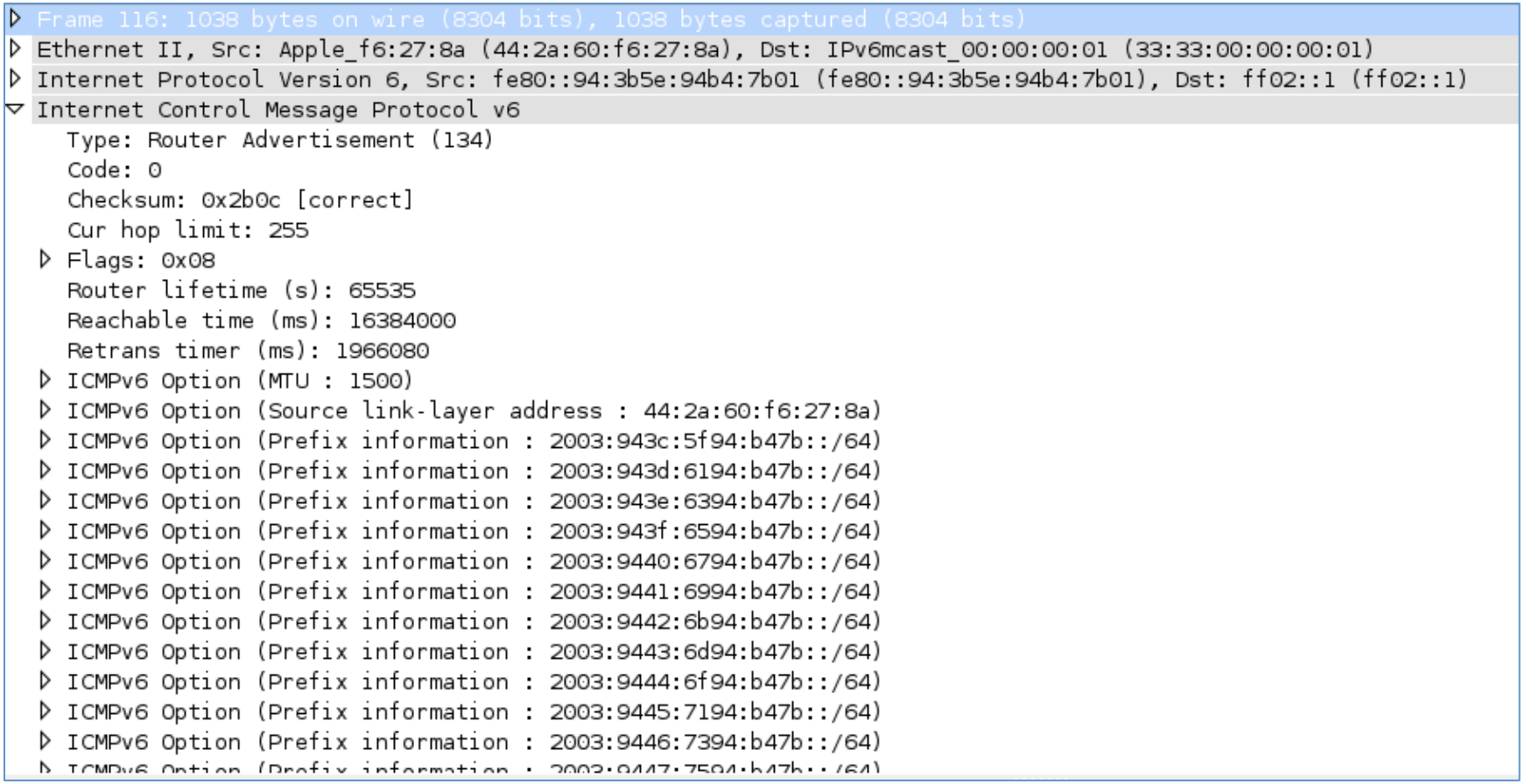
- Drives Windows to 100% CPU
- Also affects FreeBSD
- No effect on Mac OS X or Ubuntu Linux



The New RA Flood

MORE IS BETTER

- Each RA now contains
  - 17 Route Information sections
  - 18 Prefix Information sections


Frame 116: 1038 bytes on wire (8304 bits), 1038 bytes captured (8304 bits)
Ethernet II, Src: Apple_f6:27:8a (44:2a:60:f6:27:8a), Dst: IPv6mcast_00:00:00:01 (33:33:00:00:00:01)
Internet Protocol Version 6, Src: fe80::94:3b5e:94b4:7b01 (fe80::94:3b5e:94b4:7b01), Dst: ff02::1 (ff02::1)
Internet Control Message Protocol v6
Type: Router Advertisement (134)
Code: 0
Checksum: 0x2b0c [correct]
Cur hop limit: 255
Flags: 0x08
Router lifetime (s): 65535
Reachable time (ms): 16384000
Retrans timer (ms): 1966080
ICMPv6 Option (MTU : 1500)
ICMPv6 Option (Source link-layer address : 44:2a:60:f6:27:8a)
ICMPv6 Option (Prefix information : 2003:943c:5f94:b47b::/64)
ICMPv6 Option (Prefix information : 2003:943d:6194:b47b::/64)
ICMPv6 Option (Prefix information : 2003:943e:6394:b47b::/64)
ICMPv6 Option (Prefix information : 2003:943f:6594:b47b::/64)
ICMPv6 Option (Prefix information : 2003:9440:6794:b47b::/64)
ICMPv6 Option (Prefix information : 2003:9441:6994:b47b::/64)
ICMPv6 Option (Prefix information : 2003:9442:6b94:b47b::/64)
ICMPv6 Option (Prefix information : 2003:9443:6d94:b47b::/64)
ICMPv6 Option (Prefix information : 2003:9444:6f94:b47b::/64)
ICMPv6 Option (Prefix information : 2003:9445:7194:b47b::/64)
ICMPv6 Option (Prefix information : 2003:9446:7394:b47b::/64)

Flood Does Not Work Alone

- Before the flood, you must send some normal RA packets
- This puts Windows into a vulnerable state

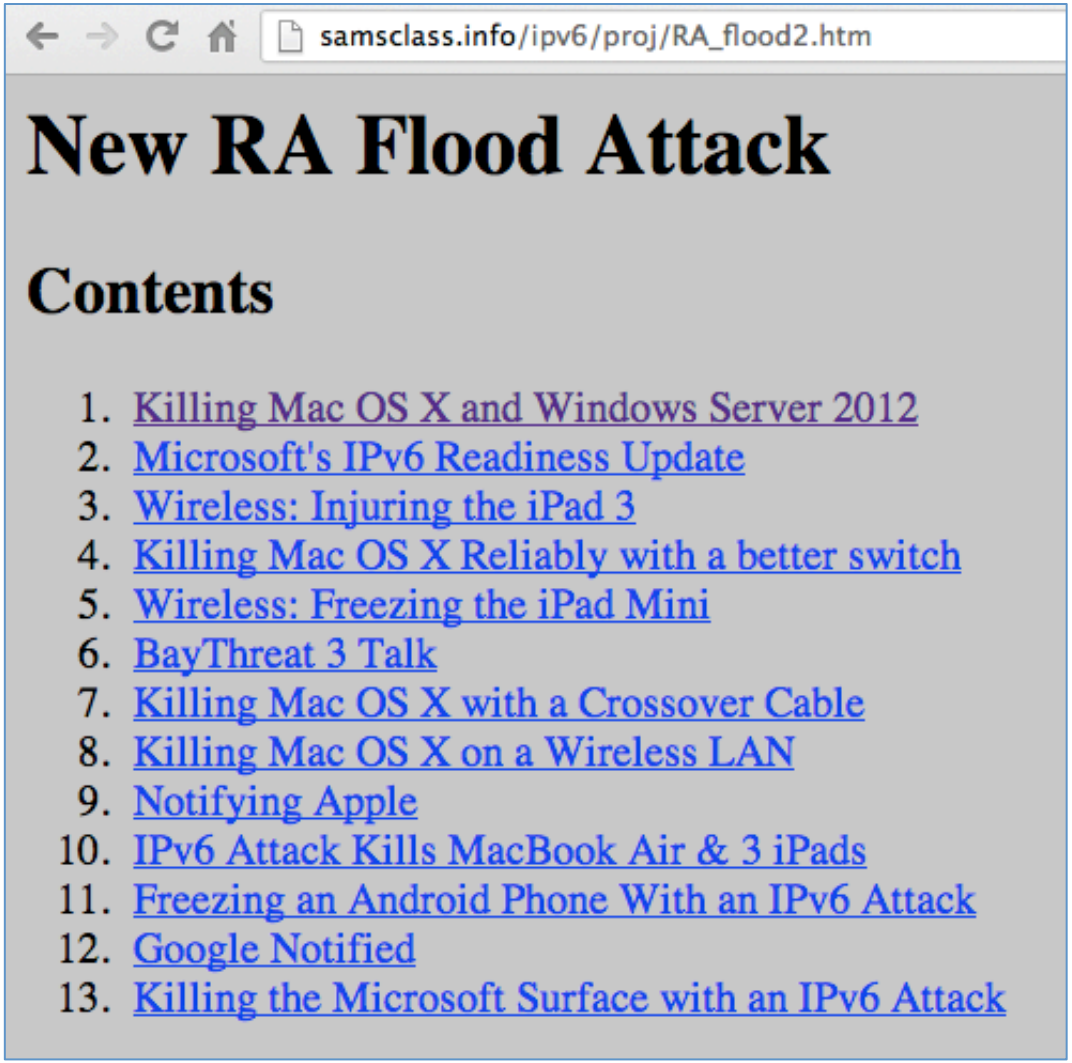
How to Perform this Attack

- For best results, use a gigabit Ethernet NIC on attacker and a gigabit switch
- Use thc-ipv6 2.3 on Kali
- Two Terminal windows:
  1. ./fake_router6 eth1 a::/64
  2. ./flood_router26 eth1
- Windows dies within 30 seconds

Effects of New RA Flood

- Win 8 & Server 2012 die (BSOD)
- Microsoft Surface RT dies (BSOD)
- Mac OS X dies
- Win 7 & Server 2008 R2, with the "IPv6 Readiness Update" freeze during attack
- iPad 3 slows and sometimes crashes
- Android phone slows and sometimes crashes
- Ubuntu Linux suffers no harm

Videos and Details



Mitigation

- Disable IPv6
- Turn off Router Discovery with netsh
- Use a firewall to block rogue RAs
- Get a switch with RA Guard
- Microsoft's "IPv6 Readiness Update" provides some protection for Win 7 & Server 2008 R2
  - Released Nov. 13, 2012
  - KB 2750841
  - ***But NOT for Win 8 or Server 2012!!***

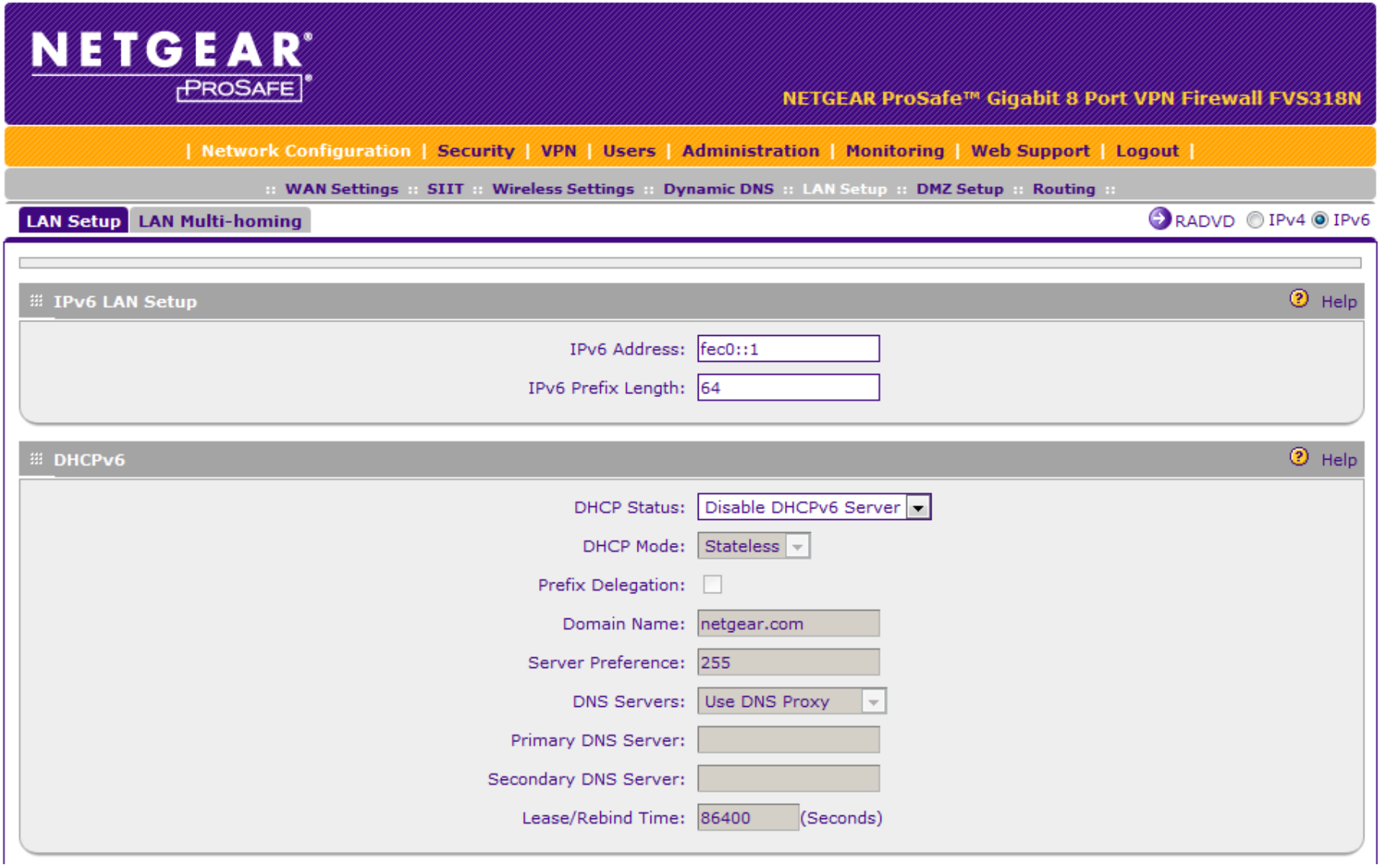
DEMO

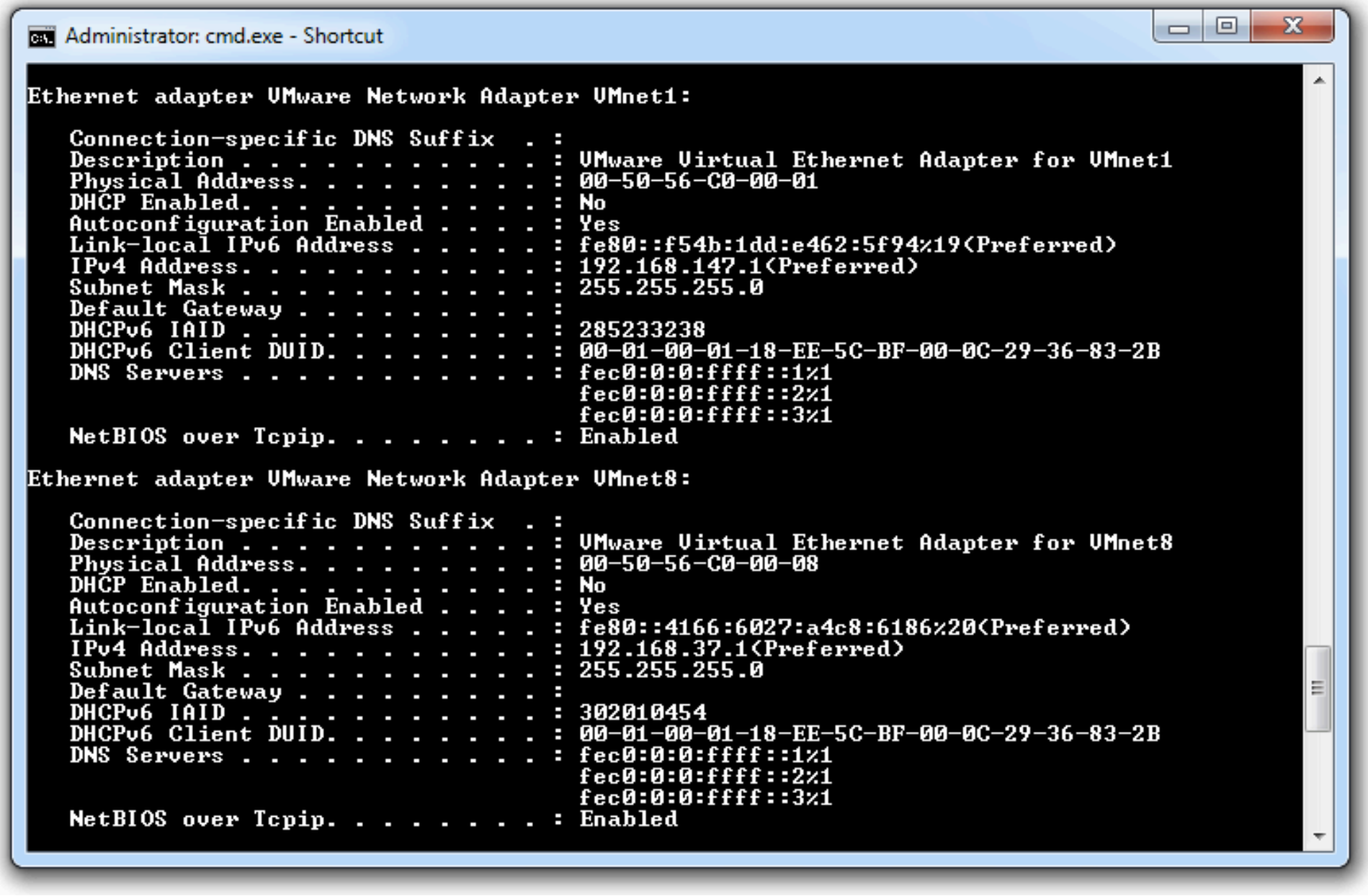
More Info

- Slides, instructions for the attacks, and more at
- Samsclass.info

Speculations

Why are Devices so Vulnerable?




Administrator: cmd.exe - Shortcut
Ethernet adapter VMware Network Adapter VMnet1:
Connection-specific DNS Suffix . :
Description . . . . . : VMware Virtual Ethernet Adapter for VMnet1
Physical Address. . . . . : 00-50-56-C0-00-01
DHCP Enabled. . . . . : No
Autoconfiguration Enabled . . . . : Yes
Link-local IPv6 Address . . . . . : fe80::f54b:1dd:e462:5f94%19(Preferred)
IPv4 Address. . . . . : 192.168.147.1(Preferred)
Subnet Mask . . . . . : 255.255.255.0
Default Gateway . . . . . :
DHCPv6 IAID . . . . . : 285233238
DHCPv6 Client DUID. . . . . : 00-01-00-01-18-EE-5C-BF-00-0C-29-36-83-2B
DNS Servers . . . . . : fec0:0:0:ffff::1%1
fec0:0:0:ffff::2%1
fec0:0:0:ffff::3%1
NetBIOS over Tcpip. . . . . : Enabled
Ethernet adapter VMware Network Adapter VMnet8:
Connection-specific DNS Suffix . :
Description . . . . . : VMware Virtual Ethernet Adapter for VMnet8
Physical Address. . . . . : 00-50-56-C0-00-08
DHCP Enabled. . . . . : No
Autoconfiguration Enabled . . . . : Yes
Link-local IPv6 Address . . . . . : fe80::4166:6027:a4c8:6186%20(Preferred)
IPv4 Address. . . . . : 192.168.37.1(Preferred)
Subnet Mask . . . . . : 255.255.255.0
Default Gateway . . . . . :
DHCPv6 IAID . . . . . : 302010454
DHCPv6 Client DUID. . . . . : 00-01-00-01-18-EE-5C-BF-00-0C-29-36-83-2B
DNS Servers . . . . . : fec0:0:0:ffff::1%1
fec0:0:0:ffff::2%1
fec0:0:0:ffff::3%1
NetBIOS over Tcpip. . . . . : Enabled

Microsoft, 2005

technet.microsoft.com/en-us/library/cc783049(v=ws.10).aspx

IPv6 configuration items

7 out of 11 rated this helpful – Rate this topic

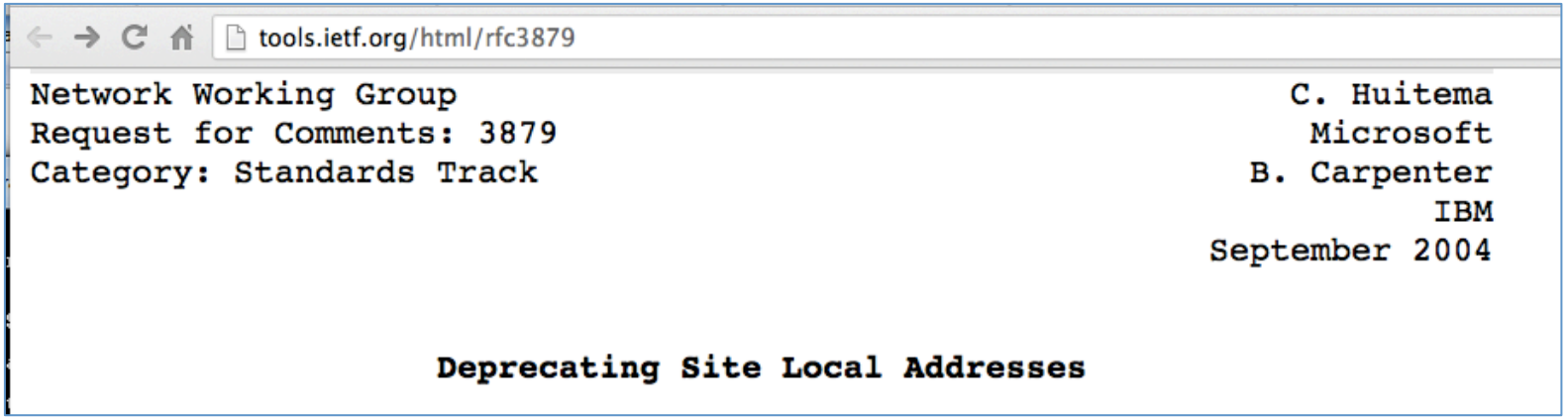
Updated: January 21, 2005

Applies To: Windows Server 2003, Windows Server 2003 R2, Windows Server 2003 with SP1, Windows Server 2003 with SP2

To configure the DNS server with one of the three IPv6 addresses that are available on IPv6 client computers by default, use the **netsh interface ipv6 add address** command. The three default DNS server addresses are:

- FEC0:0:0: FFFF::1
- FEC0:0:0: FFFF::2
- FEC0:0:0:FFFF::3

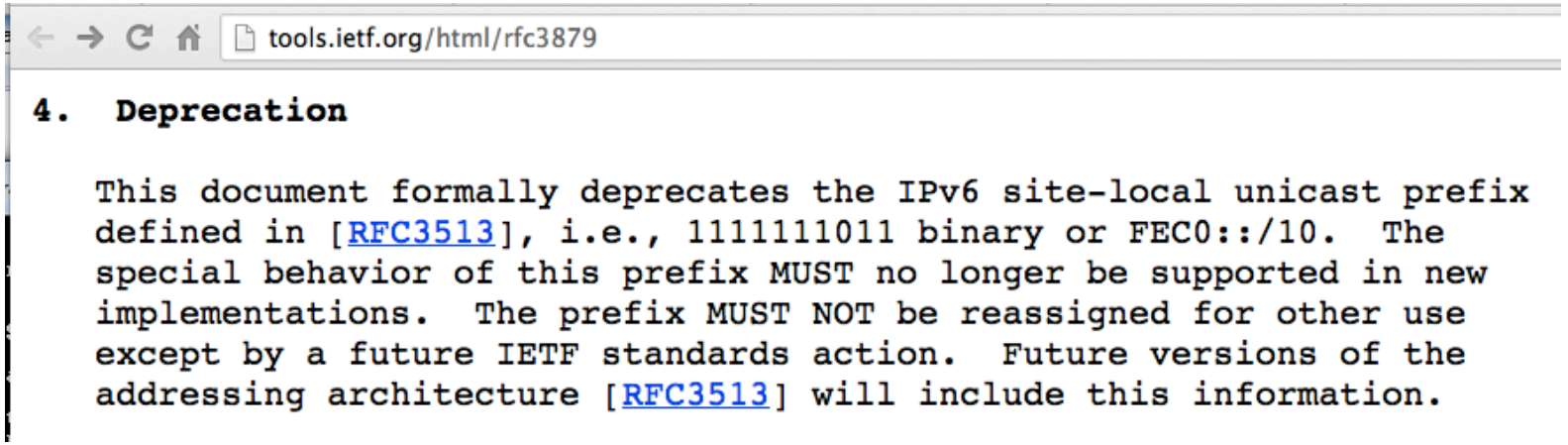
Microsoft, 2004



tools.ietf.org/html/rfc3879

Network Working Group — C. Huitema, Microsoft
Request for Comments: 3879
Category: Standards Track — B. Carpenter, IBM
September 2004

Deprecating Site Local Addresses



tools.ietf.org/html/rfc3879

4. Deprecation

This document formally deprecates the IPv6 site-local unicast prefix defined in [RFC3513], i.e., 1111111011 binary or FEC0::/10. The special behavior of this prefix MUST no longer be supported in new implementations. The prefix MUST NOT be reassigned for other use except by a future IETF standards action. Future versions of the addressing architecture [RFC3513] will include this information.

Patching

Microsoft Timeline

- Marc Hause informed them of the original RA flood vuln on July 10, 2010
- In March, 2011, I also warned Microsoft

IPv6 Router Advertisement DoS on Windows [jt] Inbox x

Microsoft Security Response Center <secure@microsoft.com> 3/25/11

to me

Hello Sam,

My name is Jeremy and I'm a program manager here in the Microsoft Security Response Center (MSRC). I was forwarded your mail regarding the DoS in Windows. Thank you very much for reporting this vulnerability to us, however we are already aware of it. This vulnerability is actually public and documented in CVE-2010-4669. The only way to fix this issue is to implement the SeND protocol, which we are looking into for future versions of Windows.

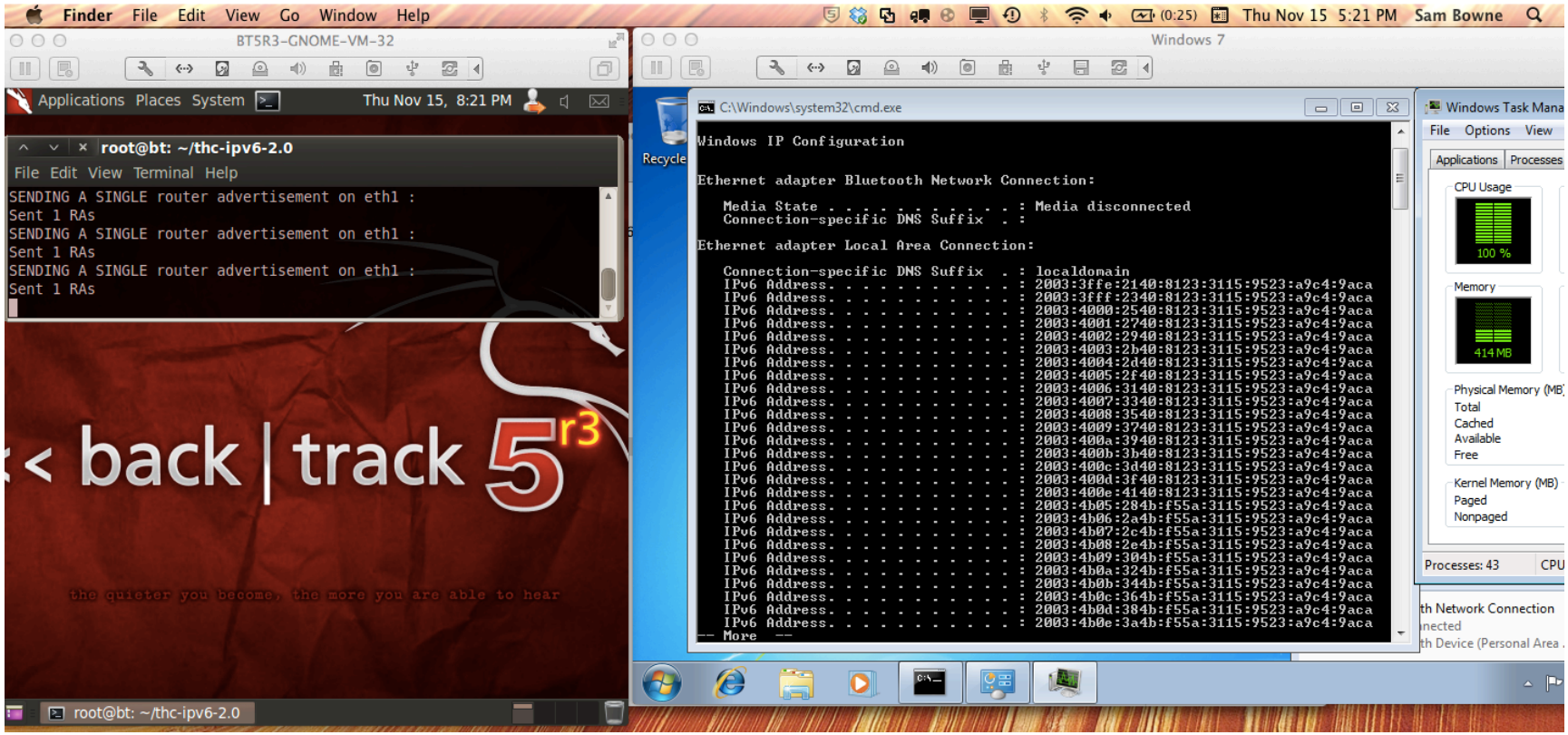
In the future, if you find any other vulnerabilities, feel free to send them to secure@microsoft.com and we will investigate.

Best Regards
Jeremy

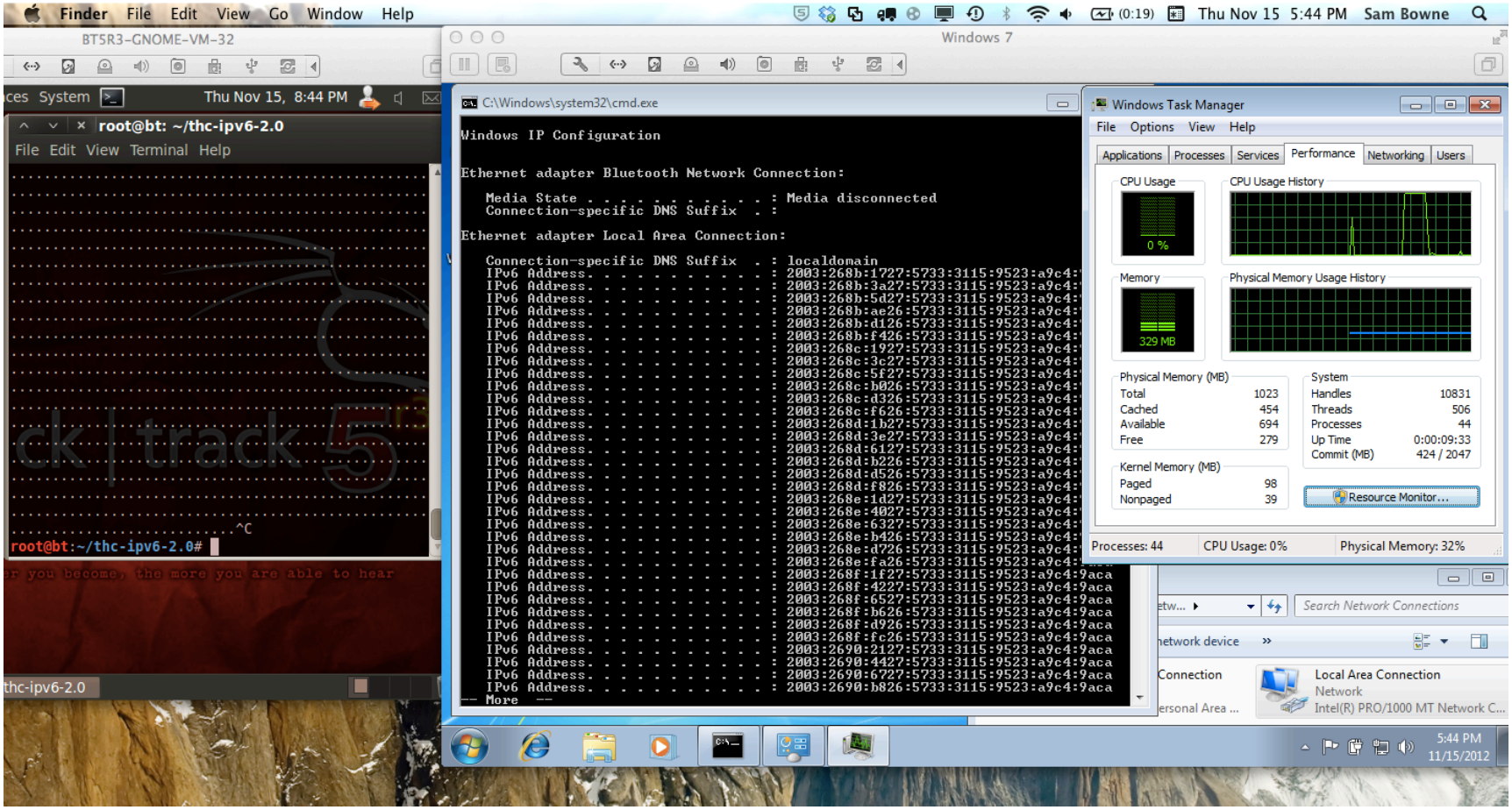
Microsoft IPv6 Readiness Update

- Released in Nov., 2012

Windows 7
Without the IPv6 Readiness Update



Windows 7
With the IPv6 Readiness Update

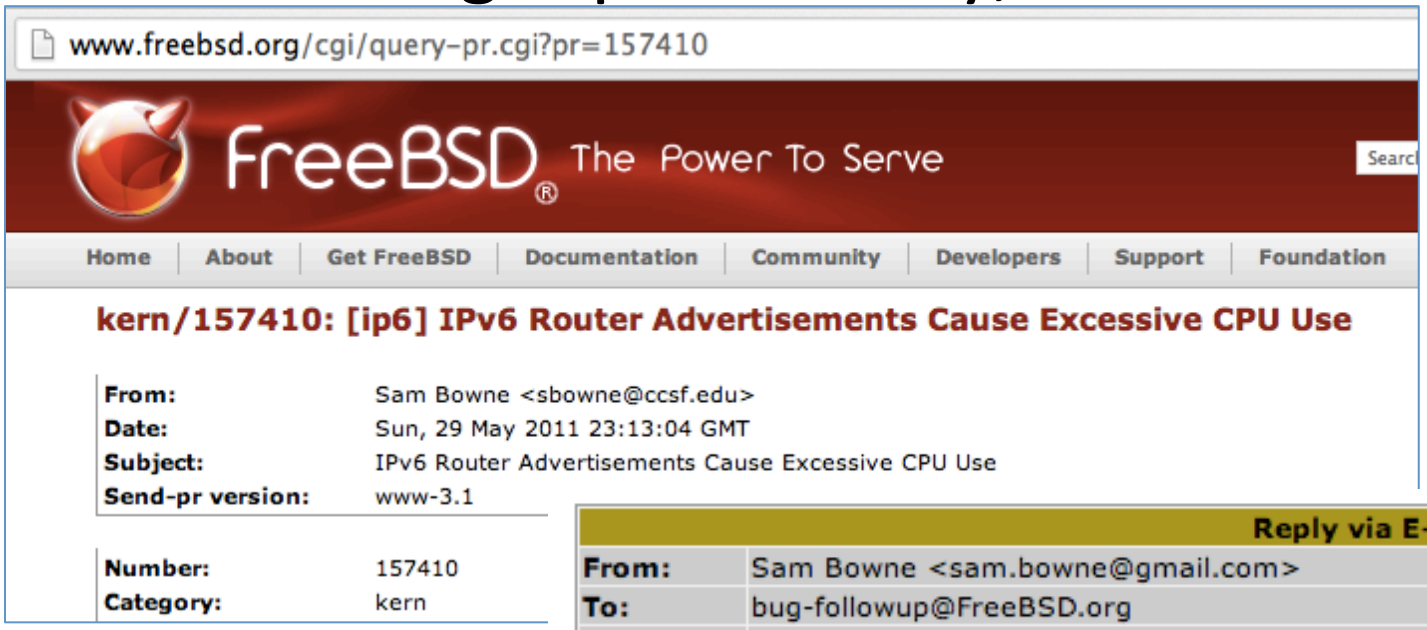


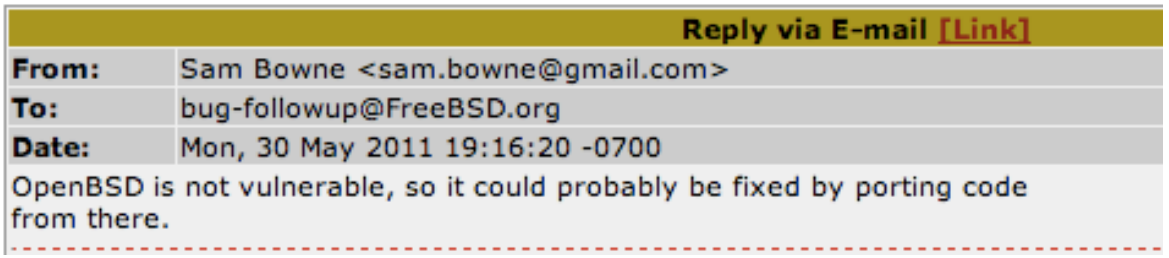
Limitations of the IPv6 Readiness Update

- Does not eliminate the DoS
- Windows 7 freezes during the attack, but recovers quickly when it stops
- Only available for Win 7 and Server 2008 R2
- Windows Server 2012 and Windows 8 are vulnerable to flood_router26 when preceded by a few normal RAs

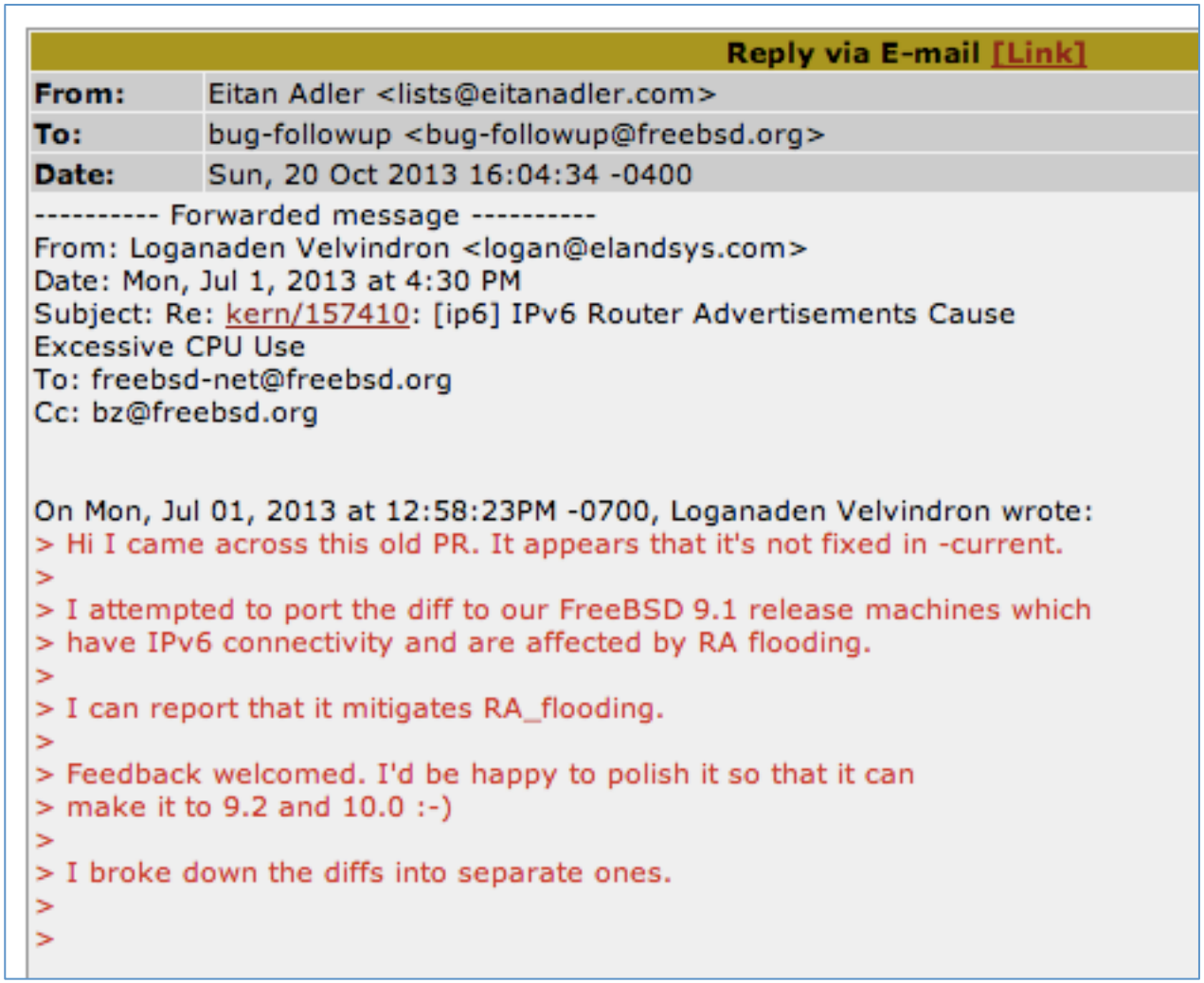
FreeBSD Timeline

- Feb 5, 2011: Marc Hause warned them of the original RA vulnerability
- I filed a bug report in May, 2011





Possibly Patched in 2013



Reply via E-mail [Link]

From:	Eitan Adler <lists@eitanadler.com>
To:	bug-followup <bug-followup@freebsd.org>
Date:	Sun, 20 Oct 2013 16:04:34 -0400

---------- Forwarded message ----------
From: Loganaden Velvindron <logan@elandsys.com>
Date: Mon, Jul 1, 2013 at 4:30 PM
Subject: Re: kern/157410: [ip6] IPv6 Router Advertisements Cause Excessive CPU Use
To: freebsd-net@freebsd.org
Cc: bz@freebsd.org

On Mon, Jul 01, 2013 at 12:58:23PM -0700, Loganaden Velvindron wrote:
> Hi I came across this old PR. It appears that it's not fixed in -current.
>
> I attempted to port the diff to our FreeBSD 9.1 release machines which
> have IPv6 connectivity and are affected by RA flooding.
>
> I can report that it mitigates RA_flooding.
>
> Feedback welcomed. I'd be happy to polish it so that it can
> make it to 9.2 and 10.0 :-)
>
> I broke down the diffs into separate ones.
>
>