



# IPv6 Insecurity Revolutions

Marc “van Hauser” Heuse  
Hack in the Box 2012, Kuala Lumpur

Hello, my name is ...





```
graph LR; A[The Situation] --> B[Vulnerabilities]; B --> C[Pentesting]; C --> D[Hope?]
```

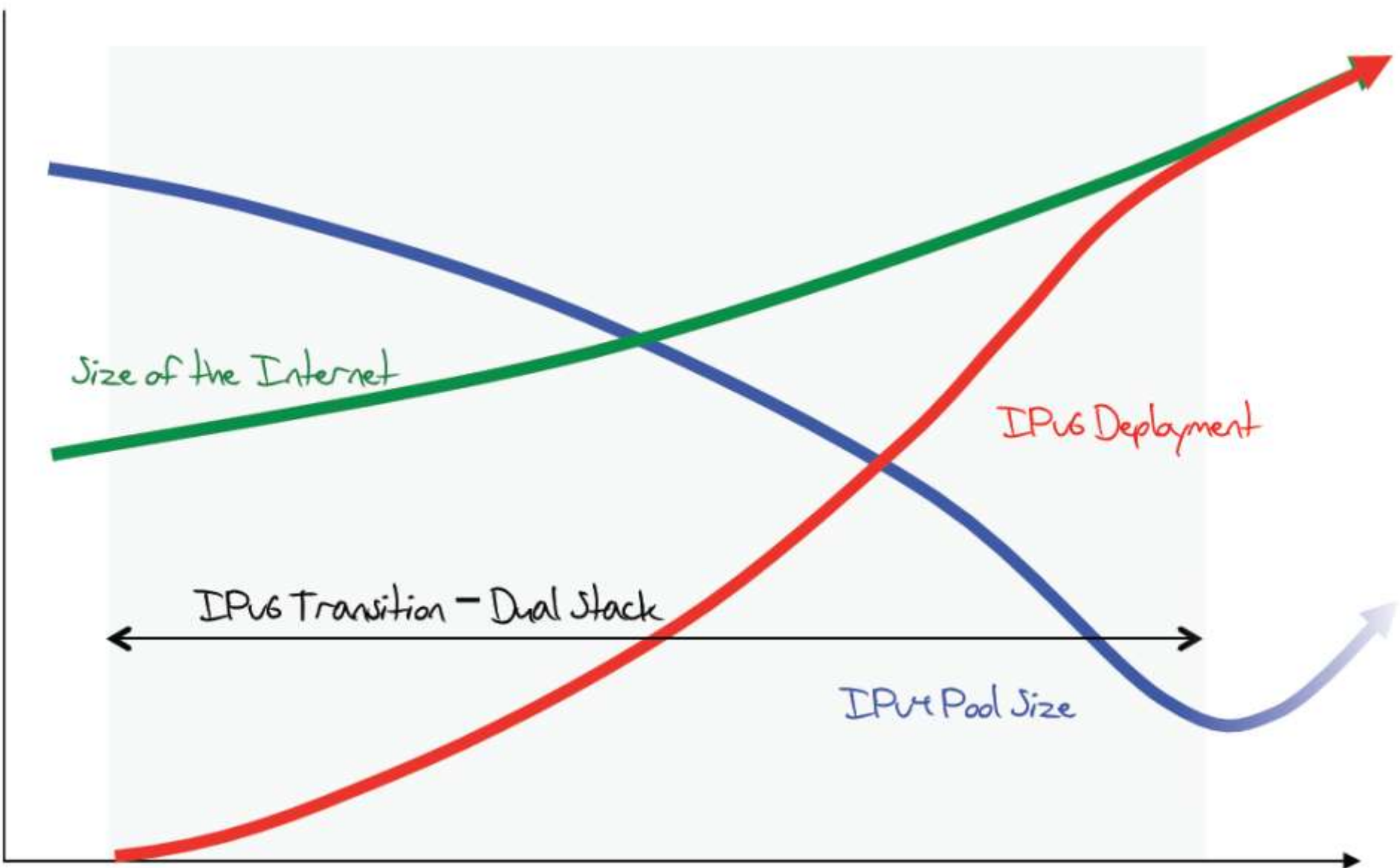
The  
Situation

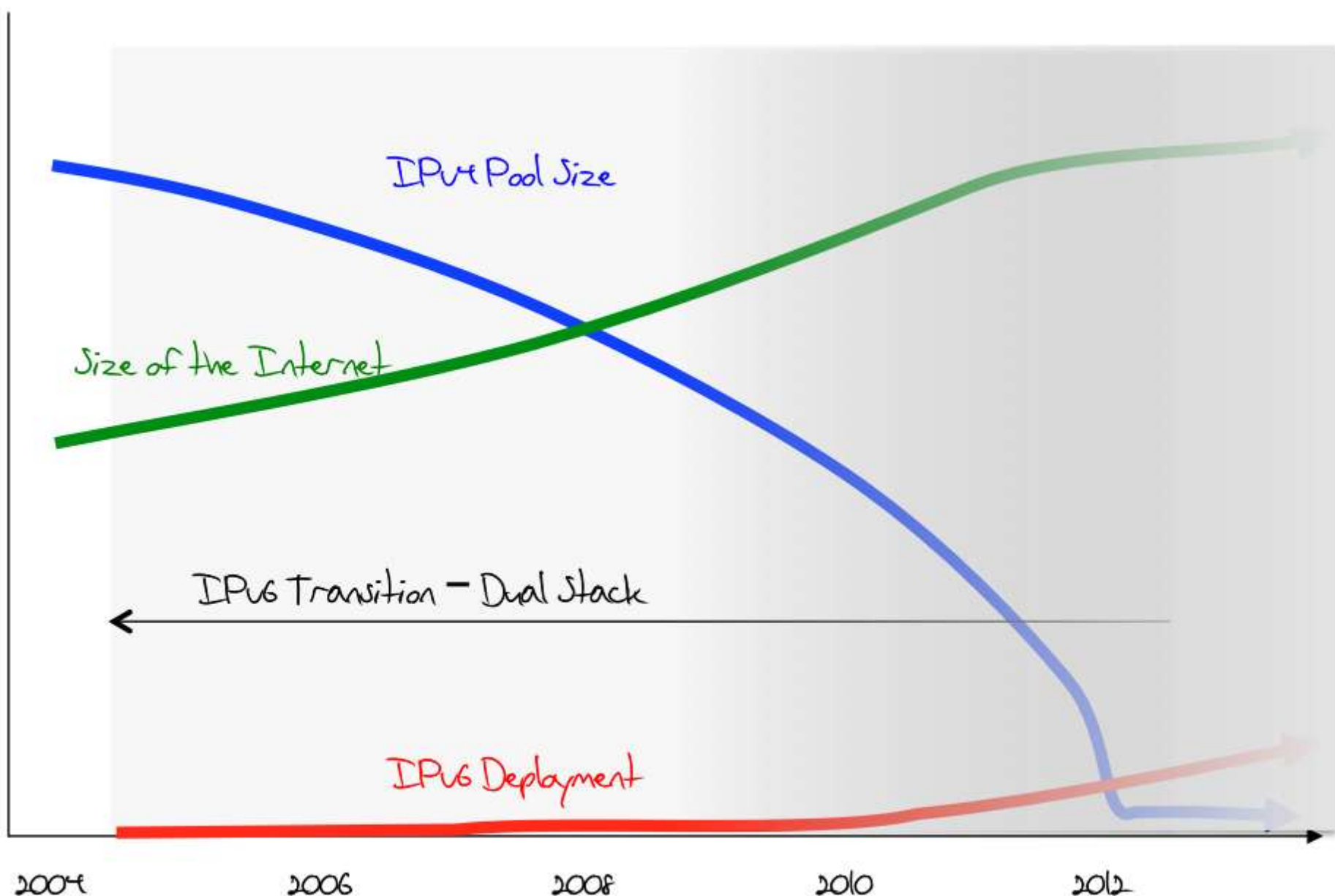
Vulnera-  
bilities

Pentesting

Hope?

Once upon a time ...





2004 2006 2008 2010 2012

Date

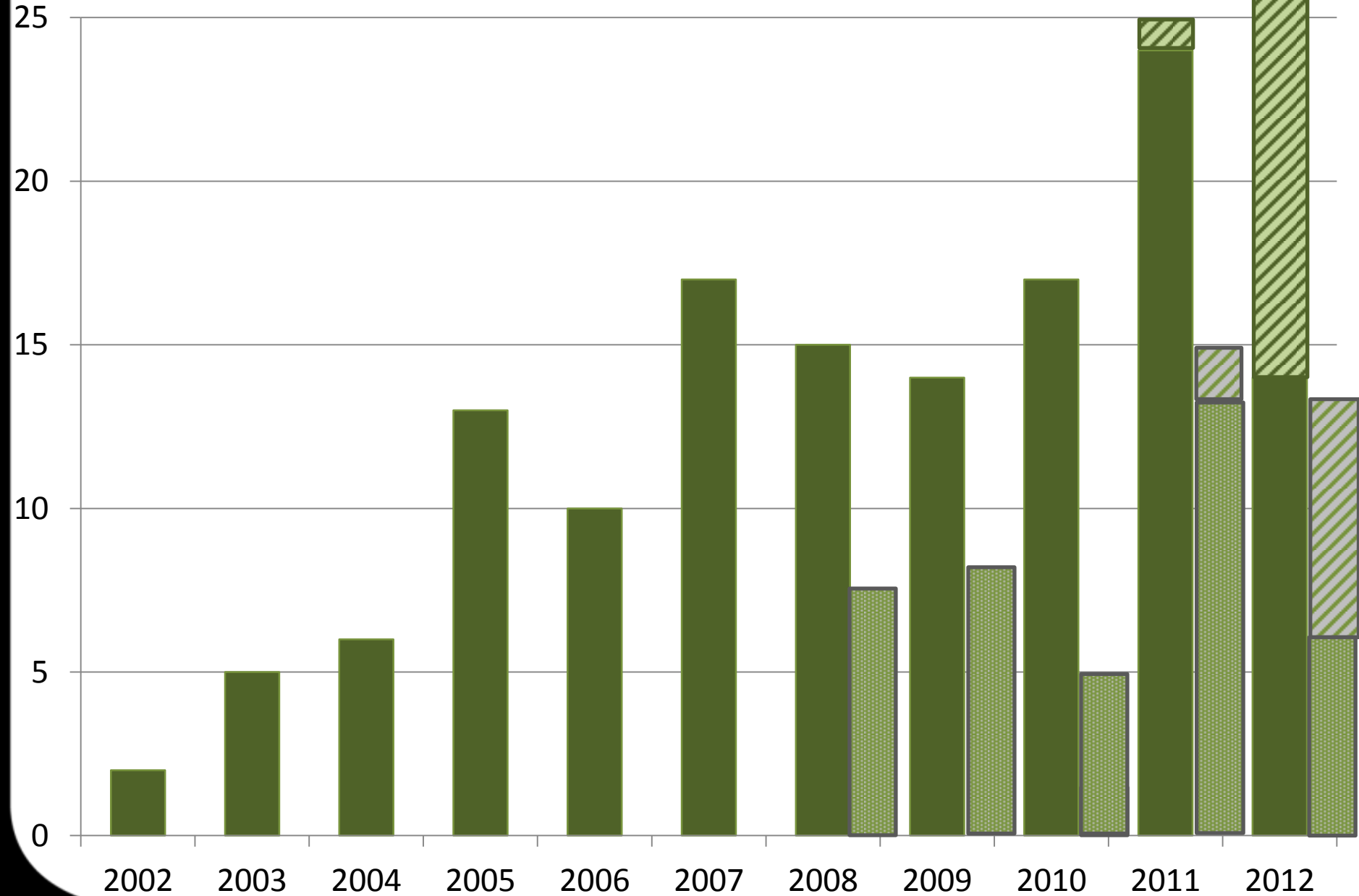
Source: Geoff Huston



THE  
END  
IS  
NEAR



# IPv6 Vulnerabilities (CVE)



# *Flooding Surprises*



# From 2010 – M\$ still didn't fix it

## Router Advertisement Flooding

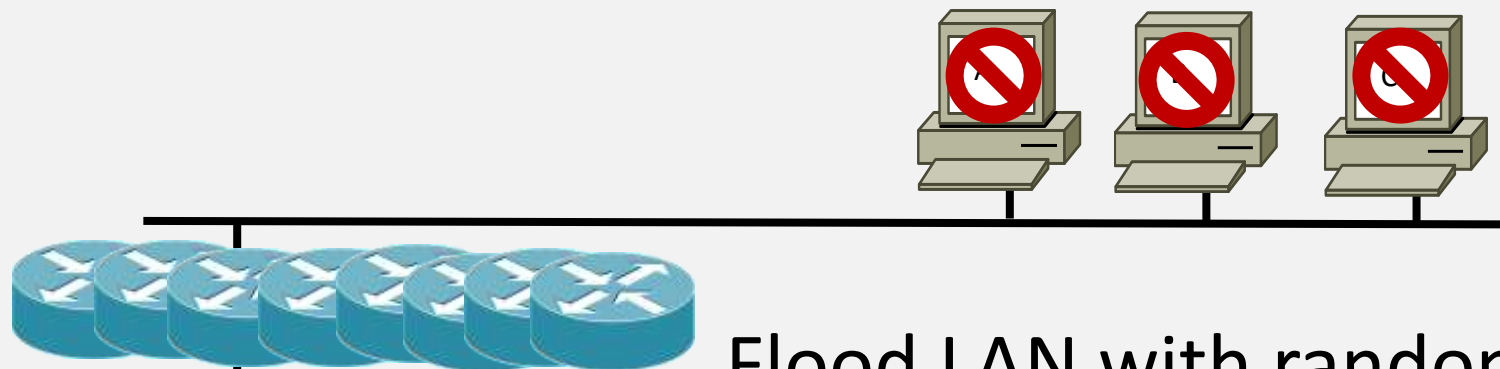


Flood LAN with random RAs.

DOS:

- Windows 7, 2008, 2003, XP
- Cisco IOS+ASA (fixed)
- Juniper Netscreen
- Free/NetBSD (fixed)

# Router Advertisement Flooding Revisited



Flood LAN with random RA with route entries.

DOS:

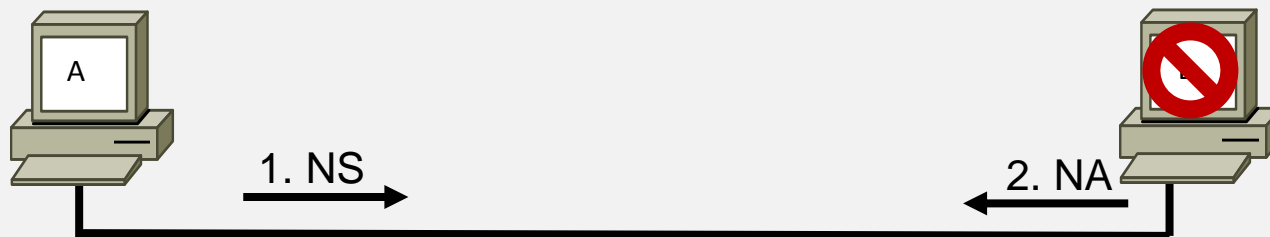
- Windows 7, 8, 20xx, XP
- Free-/NetBSD
- OS X

flood\_router26 eth0

# Neighbor Solicitation Flooding

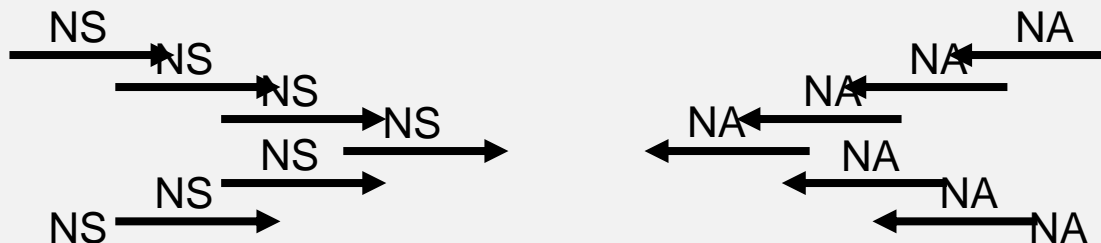


`flood_solicitat6`



1. NS:  
ICMP Type = 135  
Src = A  
Dst = All-Nodes Multicast  
Query= Who-has IP B?

2. NA:  
ICMP Type = 136  
Src = B  
Dst = A  
Data= MAC



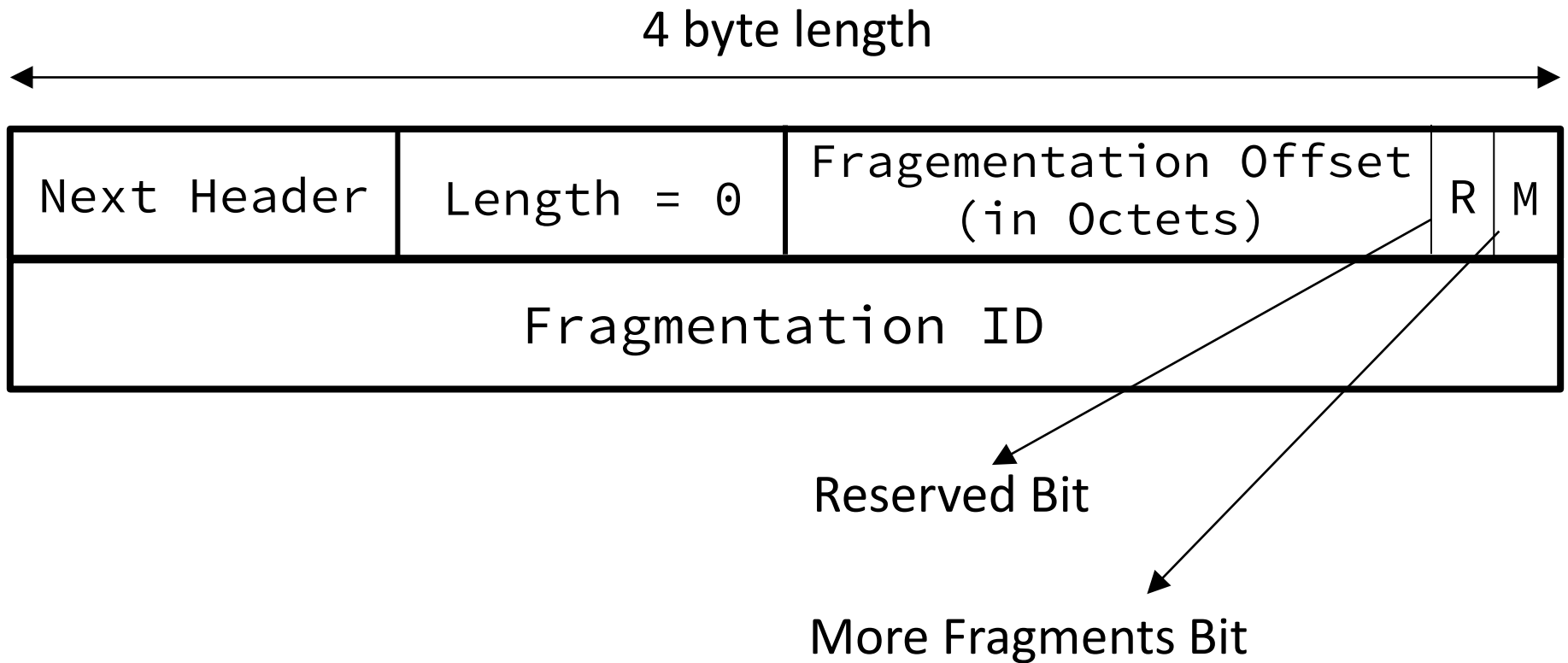
Affected:

- Windows (all)
- Solaris
- OS X
- FreeBSD/NetBSD

# ***Fragmentation Surprises***

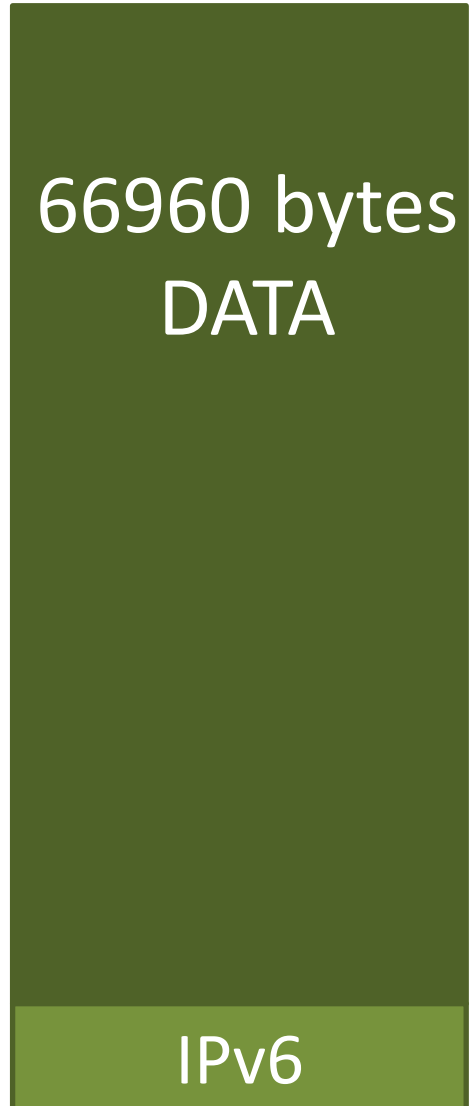
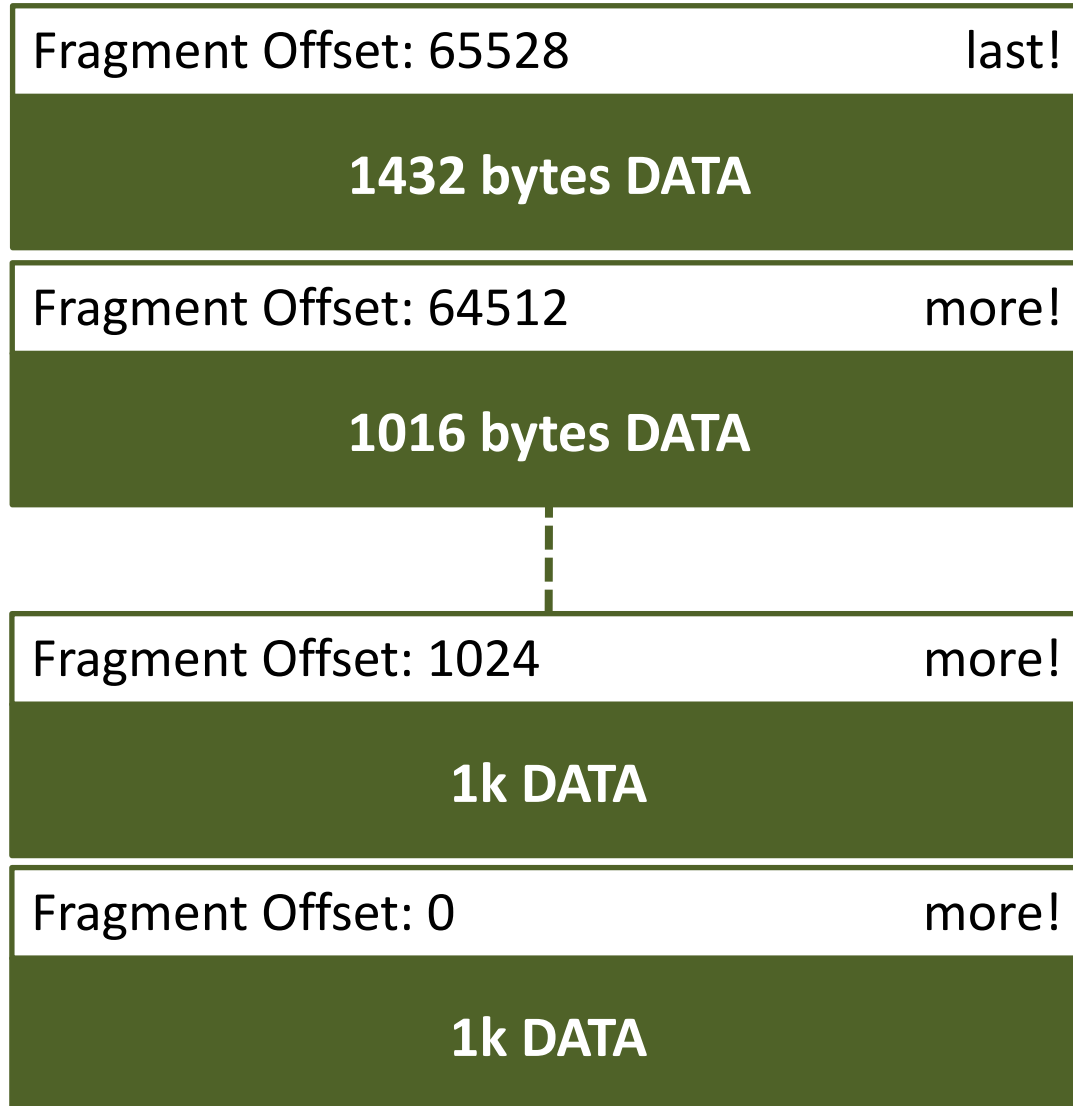


# Fragmentation Header





# Fragmentation Surprises



# Avira Personal Firewall 2012

A problem has been detected and windows has been shut down to prevent damage to your computer.

IRQL\_NOT\_LESS\_OR\_EQUAL

If this is the first time you've seen this stop error screen, restart your computer. If this screen appears again, follow these steps:

Check to make sure any new hardware or software is properly installed. If this is a new installation, ask your hardware or software manufacturer for any windows updates you might need.

If problems continue, disable or remove any newly installed hardware or software. Disable BIOS memory options such as caching or shadowing. If you need to use Safe Mode to remove or disable components, restart your computer, press F8 to select Advanced startup options, and then select Safe Mode.

Technical information:

\*\*\* STOP: 0x0000000A (0x000000B0, 0x00000002, 0x00000000, 0x8302D7AF)

Collecting data for crash dump ...

Initializing disk for crash dump ...

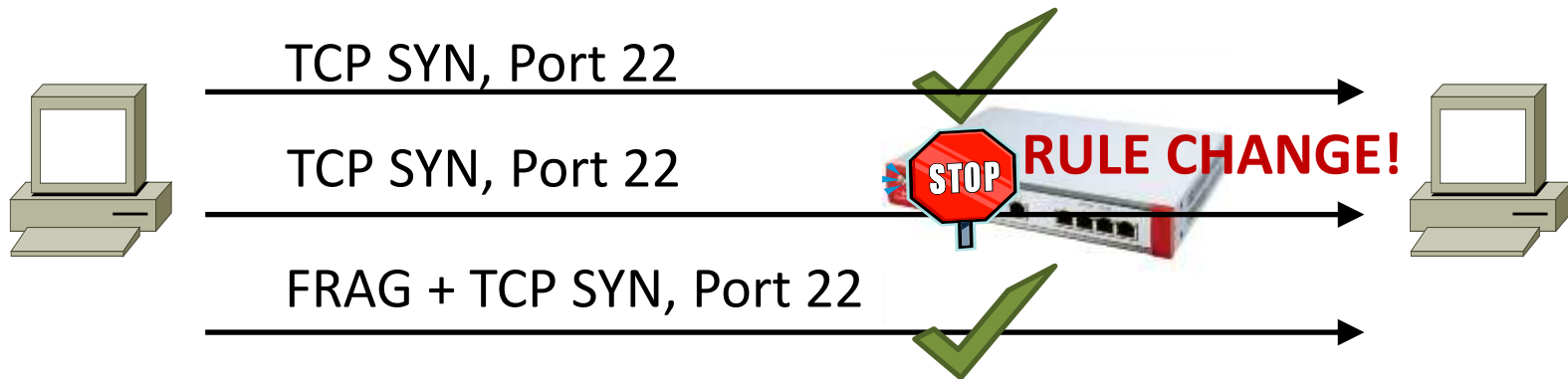
Beginning dump of physical memory.

Dumping physical memory to disk: 100

Physical memory dump complete.

Contact your system admin or technical support group for further assistance.

# Fragmentation Surprises II



Zyxel does not consider this a bug ...

# Fragmentation Surprises III



FRAG ID A, Offset 0

FRAG ID A, Offset 20.000

FRAG ID A, Offset 60.000

FRAG ID B, Offset 0

FRAG ID B, Offset 20.000

FRAG ID B, Offset 60.000

FRAG ID C, Offset 0

FRAG ID C, Offset 20.000

FRAG ID C, Offset 60.000

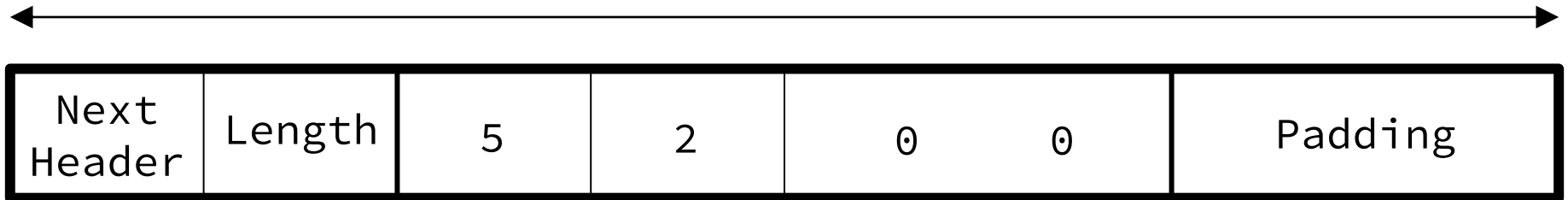
# *Router Alert Magic*



# Router Alert Option

## Hop-by-Hop Extension Header

8 byte length

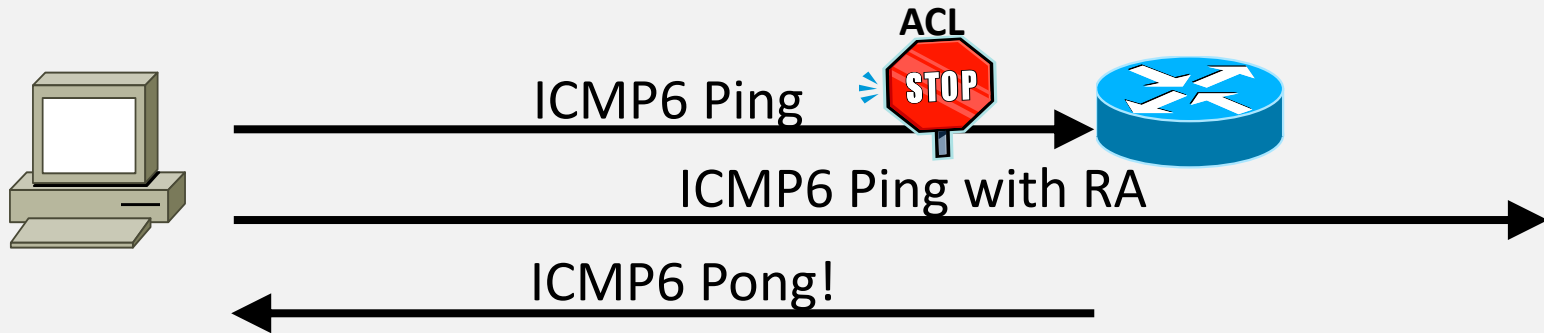


Router  
Alert  
Option

Option  
Length

Value:  
Multicast  
Listener  
Discovery

# Cisco ICMP ACL Bypass



**RA**

YOU  
**RANG?**

***Speeeeeeeeeeeeeeed***





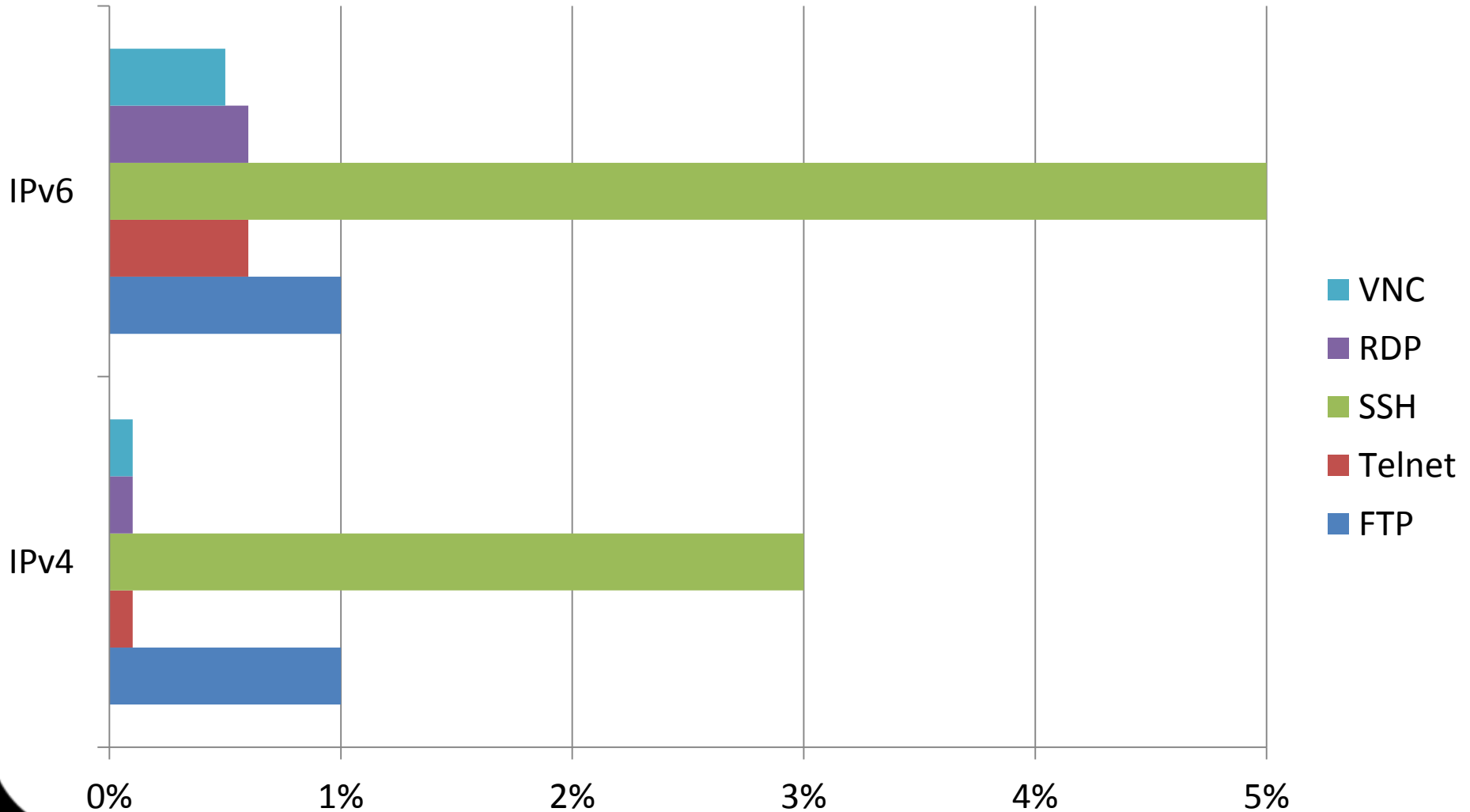


*Nothing can happen  
on IPv6, right?*

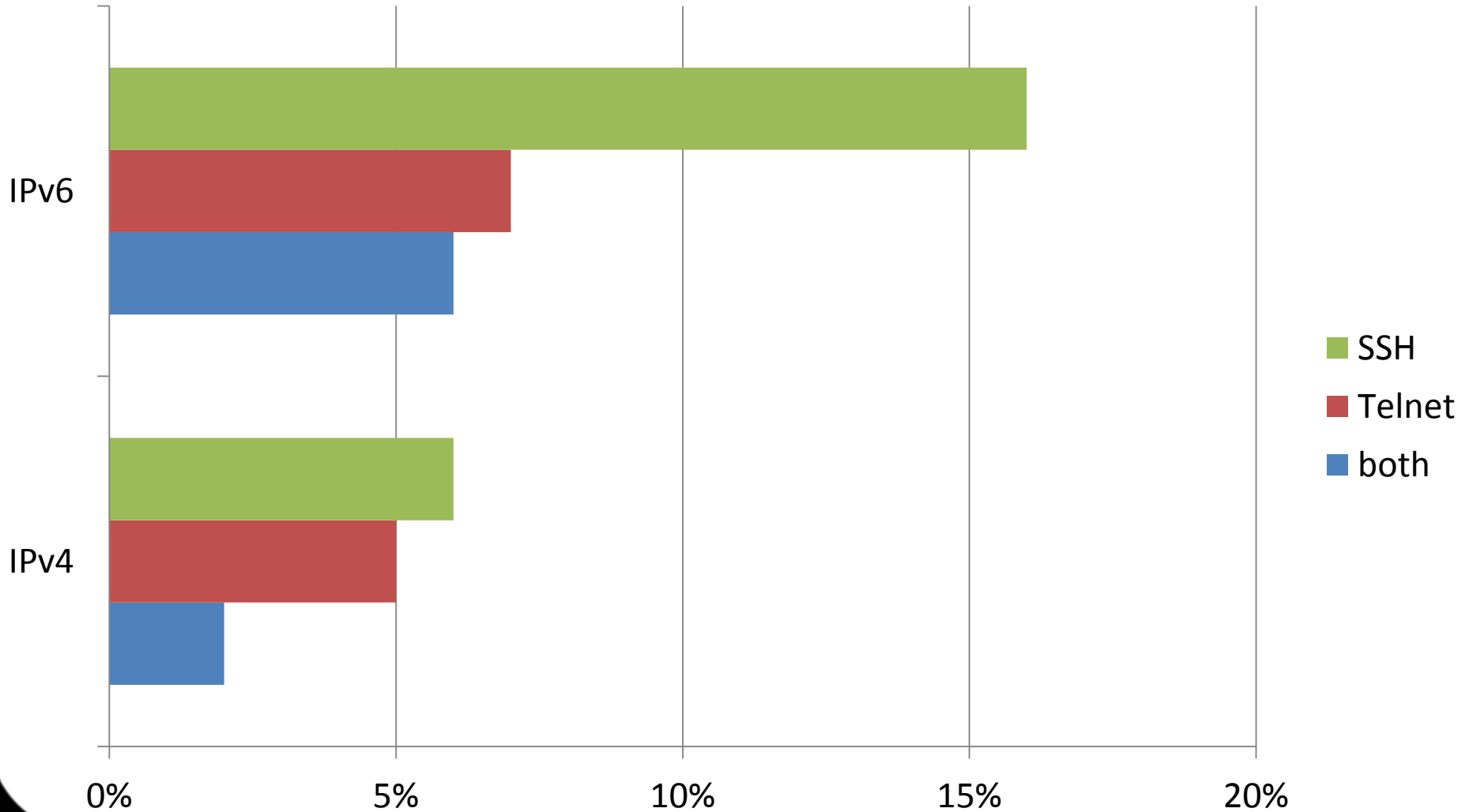
A nighttime aerial photograph of Singapore's skyline. The city is illuminated with various lights, reflecting on the water in the foreground. The number '2500' is overlaid in a large, white, sans-serif font in the center of the image. The background shows a dark blue sky and the city's dense urban landscape.

*2500*

# Company Server protection



# ISP Router protection



A close-up portrait of a man with a mustache and glasses, looking directly at the camera with a wide-eyed, surprised expression. He is wearing a dark red, vertically striped shirt. The background is a solid light blue color.

***So, how do I  
pentest IPv6?***

***Thank you RIPE!***



# Find the AS for the target

## Full Text Search

RIPE Database text search:

All     Any     Exact Match

By submitting this form you explicitly express your agreement with the [RIPE Database Terms and Conditions](#)

[Basic Search](#)

Search only within the following objects:    Search only within the following fields:

as-block	admin-c
as-set	as-name
aut-num	aut-num
domain	default
filter-set	descr
inet-rtr	export
inet6num	import
inetnum	member-of
irt	mnt-by
key-cert	mnt-lower
mntner	mnt-routes
organisation	mp-default
peering-set	mp-export
route	mp-import
route-set	notify
route6	org
rtr-set	remarks
	tech-c

[Reset](#)

<https://apps.db.ripe.net/search/full-text.html>

## Search results

This is the RIPE Database full text search service.  
The RIPE Database is subject to Terms and Conditions.  
See <http://www.ripe.net/db/support/db-terms-conditions.pdf>

### [aut-num: AS3333](#)

*as-name=RIPE-NCC-AS, mnt-by=RIPE-NCC-END-MNT RIPE-NCC-MNT, remarks=:  
+-----+ | AS3333 RIPE-NCC-AS | | RIPE NCC (Network  
Coordination Centre, descr=Reseaux IP Europeens Network Coordination Centre (RIPE NCC)*

### [aut-num: AS12654](#)

*as-name=RIPE-NCC-RIS-AS, mnt-by=RIPE-NCC-END-MNT RIPE-NCC-RIS-MNT, remarks=RIPE NCC RIS project  
<http://www.ripe.net/ris/> The RIPE NCC RIS collects routing data using several, descr=Reseaux IP Europeens Network  
Coordination Centre (RIPE NCC)*

### [aut-num: AS197000](#)

*as-name=RIPE-NCC-AUTHDNS-AS, mnt-by=RIPE-NCC-END-MNT RIPE-GII-MNT, remarks=remarks:  
+-----+ | RIPE NCC anycast DNS, descr=Reseaux IP Europeens Network  
Coordination Centre (RIPE NCC)*

### [aut-num: AS196615](#)

*as-name=RIPE-NCC-RIS-4BYTE-AS, mnt-routes=RIPE-NCC-RIS-MNT, mnt-by=RIPE-NCC-END-MNT RIPE-NCC-RIS-MNT,  
remarks=RIPE NCC RIS beacon from a 4-byte AS asdot to asplain conversion, descr=Reseaux IP Europeens Network  
Coordination Centre (RIPE NCC)*





# Do the AS announce IPv6?

## AS3333 Reseaux IP Europeens Network Coordination Centre (RIPE NCC)

### Quick Links

[BGP Toolkit Home](#)  
[BGP Prefix Report](#)  
[BGP Peer Report](#)  
[Bogon Routes](#)  
[World Report](#)

[AS Info](#) [Graph v4](#) [Graph v6](#) [Prefixes v4](#) [Prefixes v6](#) [Peers v4](#) [Peers v6](#) [Whois](#) [IRR](#)



Prefix	Description
<a href="#">2001:067c:02e8::/48</a> 	Reseaux IP Europeens Network Coordination Centre (RIPE NCC) 

## AS197000 Reseaux IP Europeens Network Coordination Centre (RIPE NCC)

### Quick Links

[BGP Toolkit Home](#)  
[BGP Prefix Report](#)  
[BGP Peer Report](#)  
[Bogon Routes](#)  
[World Report](#)

[AS Info](#) [Graph v4](#) [Graph v6](#) [Prefixes v4](#) [Prefixes v6](#) [Peers v4](#) [Peers v6](#) [Whois](#) [IRR](#)

Prefix	Description
<a href="#">2001:067c:00e0::/48</a> 	Reseaux IP Europeens Network Coordination Centre (RIPE NCC) 

## AS196615 Reseaux IP Europeens Network Coordination Centre (RIPE NCC)

### Quick Links

[BGP Toolkit Home](#)  
[BGP Prefix Report](#)  
[BGP Peer Report](#)  
[Bogon Routes](#)  
[World Report](#)

[AS Info](#) [Graph v4](#) [Prefixes v4](#) [Peers v4](#) [Whois](#) [IRR](#)

Updated 02 Oct 2012 07:43 PST © 2012 Hurricane Electric






















[http://bgp.he.net/ASxxxx#\\_prefixes6](http://bgp.he.net/ASxxxx#_prefixes6)

## AS12654 Reseaux IP Europeens Network Coordination Centre (RIPE NCC)

### Quick Links

[BGP Toolkit Home](#)  
[BGP Prefix Report](#)  
[BGP Peer Report](#)  
[Bogon Routes](#)  
[World Report](#)  
[Multi Origin Routes](#)  
[DNS Report](#)  
[Top Host Report](#)  
[Internet Statistics](#)  
[Looking Glass](#)  
[Free IPv6 Tunnel](#)  
[IPv6 Certification](#)  
[IPv6 Progress](#)  
[Going Native](#)  
[Contact Us](#)


[AS Info](#)
[Graph v4](#)
[Graph v6](#)
[Prefixes v4](#)
[Prefixes v6](#)
[Peers v4](#)
[Peers v6](#)
[Whois](#)
[IRR](#)

Prefix	Description
<a href="#">2001:07fb:fd02::/48</a>	Reseaux IP Europeens Network Coordination Centre (RIPE NCC) 
<a href="#">2001:07fb:fd03::/48</a>	Reseaux IP Europeens Network Coordination Centre (RIPE NCC) 
<a href="#">2001:07fb:fe00::/48</a>	Reseaux IP Europeens Network Coordination Centre (RIPE NCC) 
<a href="#">2001:07fb:fe05::/48</a>	Reseaux IP Europeens Network Coordination Centre (RIPE NCC) 
<a href="#">2001:07fb:fe0a::/48</a>	Reseaux IP Europeens Network Coordination Centre (RIPE NCC) 
<a href="#">2001:07fb:fe0b::/48</a>	Reseaux IP Europeens Network Coordination Centre (RIPE NCC) 
<a href="#">2001:07fb:fe0c::/48</a>	Reseaux IP Europeens Network Coordination Centre (RIPE NCC) 
<a href="#">2001:07fb:fe0e::/48</a>	Reseaux IP Europeens Network Coordination Centre (RIPE NCC) 
<a href="#">2001:07fb:fe0f::/48</a>	Reseaux IP Europeens Network Coordination Centre (RIPE NCC) 
<a href="#">2001:07fb:fe10::/48</a>	Reseaux IP Europeens Network Coordination Centre (RIPE NCC) 
<a href="#">2001:07fb:ff00::/48</a>	Reseaux IP Europeens Network Coordination Centre (RIPE NCC) 
<a href="#">2001:07fb:ff01::/48</a>	Reseaux IP Europeens Network Coordination Centre (RIPE NCC) 
<a href="#">2001:07fb:ff03::/48</a>	Reseaux IP Europeens Network Coordination Centre (RIPE NCC) 
<a href="#">2001:07fb:ff04::/48</a>	Reseaux IP Europeens Network Coordination Centre (RIPE NCC) 
<a href="#">2001:07fb:ff05::/48</a>	Reseaux IP Europeens Network Coordination Centre (RIPE NCC) 
<a href="#">2001:07fb:ff07::/48</a>	Reseaux IP Europeens Network Coordination Centre (RIPE NCC) 
<a href="#">2001:07fb:ff0a::/48</a>	Reseaux IP Europeens Network Coordination Centre (RIPE NCC) 
<a href="#">2001:07fb:ff0b::/48</a>	Reseaux IP Europeens Network Coordination Centre (RIPE NCC) 
<a href="#">2001:07fb:ff0c::/48</a>	Reseaux IP Europeens Network Coordination Centre (RIPE NCC) 
<a href="#">2001:07fb:ff0e::/48</a>	Reseaux IP Europeens Network Coordination Centre (RIPE NCC) 
<a href="#">2001:07fb:ff10::/48</a>	Reseaux IP Europeens Network Coordination Centre (RIPE NCC) 

63% ::1

76% ::1, ::2

79% ::0, ::1, ::2

(statistic based on 8200 networks)

```
# alive6 -p eth0 2001:67c:238::0-ffff::0-2
```

```
Alive: 2001:67c:238:1::2 [ICMP echo-reply]
```

```
Alive: 2001:67c:238:3::1 [ICMP echo-reply]
```

```
Alive: 2001:67c:238:3::2 [ICMP echo-reply]
```

```
Alive: 2001:67c:238:300::1 [ICMP echo-reply]
```

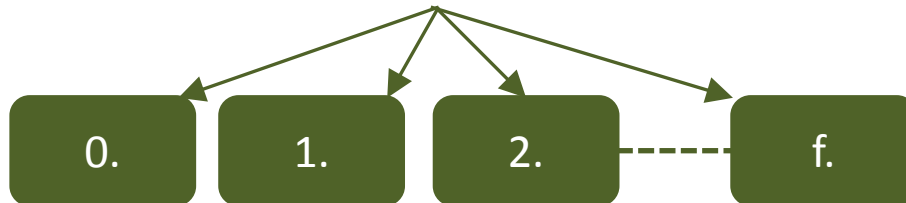
```
Scanned 65536 systems in 29 seconds and found 4  
systems alive
```

# Reverse DNS Enumeration

8.e.2.0.c.7.6.0.1.0.0.2.ip6.arp



**NXDOMAIN**    **NOERROR**    **NXDOMAIN**    **NXDOMAIN**



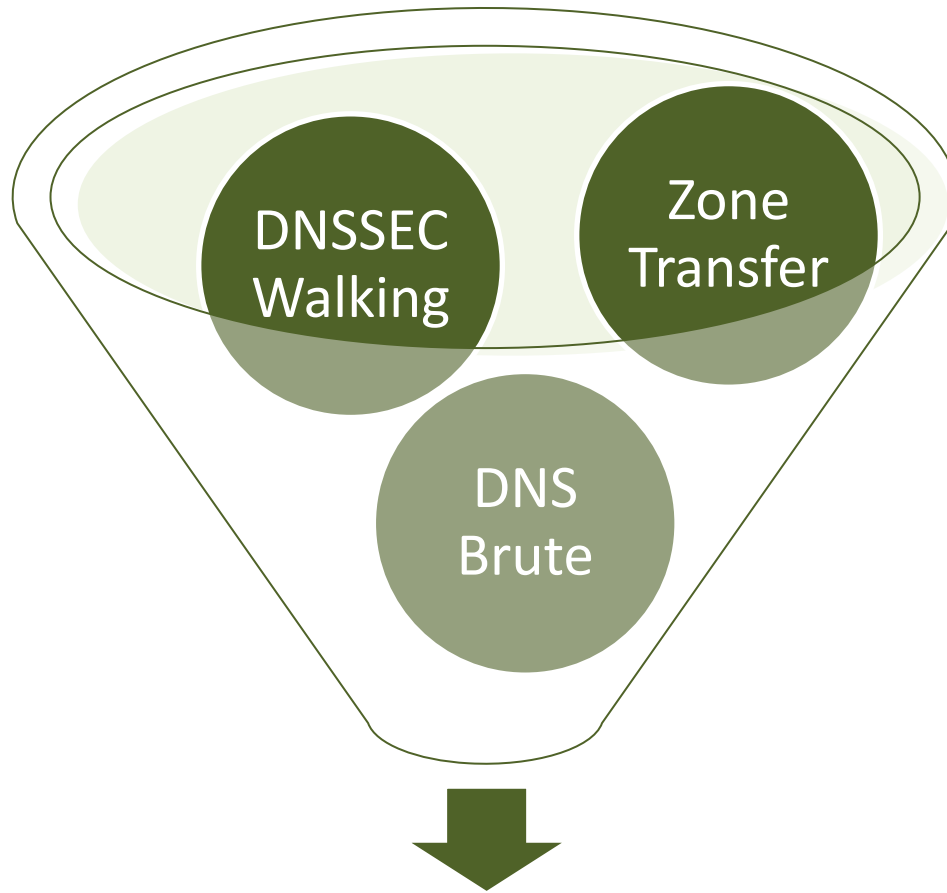
e.6.1.0.0.0.1.c.0.0.0.0.0.0.0.0.1.0.0.0.8.e.2.0.c.7.6.0.1.0.0.2.ip6.arp  
PTR db-int.ipv6.ripe.net. (2001:67c:2e8:1::c100:16e)

# Reverse DNS Enumeration

```
# dnsrevenue6 pri.authdns.ripe.net. 2001:67c:2e8::/48
```

```
2001:67c:2e8:1::1 is gw.ipv6.office.nsrp.ripe.net.  
2001:67c:2e8:1::c100:102 is alfresco.ripe.net.  
2001:67c:2e8:1::c100:10c is pademelon.ipv6.ripe.net.  
2001:67c:2e8:1::c100:114 is otter.ipv6.ripe.net.  
2001:67c:2e8:1::c100:11c is int.db.ipv6.ripe.net.  
2001:67c:2e8:1::c100:115 is jaguar.ipv6.ripe.net.  
2001:67c:2e8:1::c100:117 is cougar.ipv6.ripe.net.  
2001:67c:2e8:1::c100:123 is db-apps.ipv6.ripe.net.  
2001:67c:2e8:1::c100:128 is coral.ipv6.ripe.net.  
2001:67c:2e8:1::c100:12b is tarsier.ipv6.ripe.net.  
...
```

# Extract DNS Information



DNS Name → IPv6 Addresses

# Try it

```
# dig @pri.authdns.ripe.net. ripe.net. axfr
ripe.net. 3600 IN SOA      pri.authdns.ripe.net.
ripe.net. 2160 IN A       193.0.6.139
ripe.net. 300  IN AAAA    2001:67c:2e8:22::c100:68b
...
```



# Try it

```
# dnssecwalk pri.authdns.ripe.net.  ripe.net.  
Found: 256cns.ripe.net.  
Found: _jabber._tcp.ripe.net.  
Found: _xmpp-client._tcp.ripe.net.  
Found: _xmpp-server._tcp.ripe.net.  
Found: access.ripe.net.  
Found: addax.ripe.net.  
Found: ox.admin.ripe.net.  
Found: adp.ripe.net.  
Found: albatross.ripe.net.  
...
```

# Try it

```
# dnsdict6 ripe.net.  
access.ripe.net. => 2001:67c:2e8:22::c100:685  
atlas.ripe.net. => 2a01:4f8:121:30a3::78:16  
calendar.ripe.net. => 2a00:1450:4008:c01::79  
cgi.ripe.net. => 2001:67c:2e8:1::c100:117  
dns.ripe.net. => 2001:67c:e0::6  
eagle.ripe.net. => 2001:67c:2e8:1::c100:159  
eb.ripe.net. => 2001:67c:2e8:11::c100:1333  
fax.ripe.net. => 2001:67c:2e8:11::c100:1310  
falcon.ripe.net. => 2001:67c:2e8:16::c100:58a  
...
```

# Scan all addresses found

```
# alive6 -i found.txt -D -M -F eth0
```

↓  
All addresses found from alive6,  
dnsrevenue6 and DNS information

↙  
Perform common address scan on  
each network in the input file

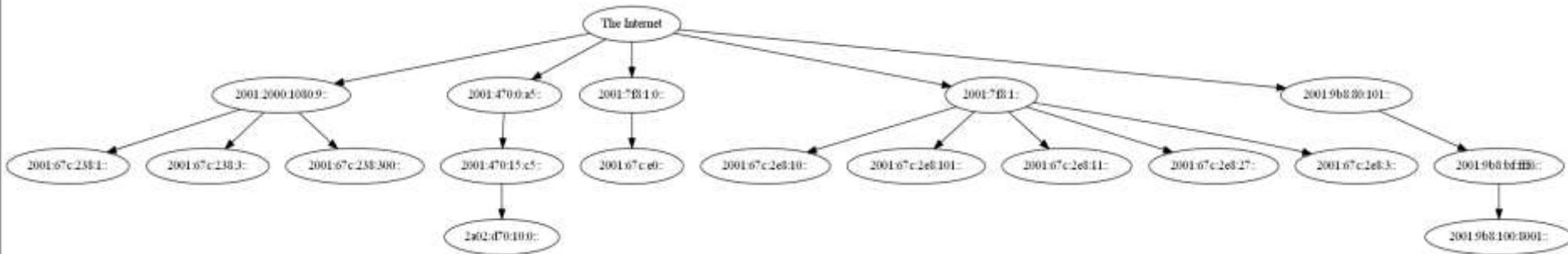
↓  
Perform MAC address scan on each  
SLAAC address in the input file

↓  
Firewall piercing mode

# Alive systems ...

```
# alive6 -i found.txt -D -M -F eth0
Alive: 2001:67c:238:1::2 [ICMP echo-reply]
Alive: 2001:67c:238:1::a [ICMP echo-reply]
Alive: 2001:67c:238:1::b [22/TCP ACK]
Alive: 2001:67c:238:3::1 [22/TCP ACK]
Alive: 2001:67c:238:300::1 [ICMP echo-reply]
Alive: 2001:67c:2e8:10::1 [ICMP echo-reply]
Alive: 2001:67c:2e8:10::1:1 [ICMP parameter problem]
Alive: 2001:67c:2e8:10::1:2 [ICMP echo-reply]
Alive: 2001:67c:2e8:101::1 [ICMP echo-reply]
Alive: 2001:67c:2e8:101::1:2 [ICMP echo-reply]
Alive: 2001:67c:2e8:13::14 [22/TCP SYN-ACK]
...
Scanned 553212 addresses and found 671 systems alive
```

# Nice maps possible too ...





IP v6



all tools at [www.thc.org/thc-ipv6](http://www.thc.org/thc-ipv6)

# Contact

Marc Heuse



+49 (0)177 961 15 60



+49 (0)30 37 30 97 26



mh@mh-sec.de



www.mh-sec.de



winsstrasse 68

d-10405 berlin



# Picture Credits

- Potpourri – [sxc.hu/profile/saflora](http://sxc.hu/profile/saflora)
- The end is near – [furiousideas.deviantart.com](http://furiousideas.deviantart.com)
- Dam – [sxc.hu/profile/linder6580](http://sxc.hu/profile/linder6580)
- Broken brick – [www.sxc.hu/profile/guitargoa](http://www.sxc.hu/profile/guitargoa)
- Magician – [mrpunto @ Flickr](#)
- Flash Hero – [Maggie Osterberg @ Flickr](#)
- Admin – [astragony @ Flickr](#)
- Nerd – [pitadel @ Flickr](#)



End