



Recent advances in IPv6 insecurities

Marc “van Hauser” Heuse
CCC Congress 2010, Berlin

Hello, my name is





Who has already

- heard my previous talk?
- played with IPv6?
- IPv6 at home?
- IPv6 at the office/university?



Episode 2

"In a distant future ...

IPv6 will come.

Maybe.

Hopefully never!"



The future is here already





Let's start with the basics



IPv4

4 octets

4.294.967.296 addresses

192.168.1.1



IPv6

16 octets

340.282.366.920.938.463.463.374
.607.431.768.211.456 addresses

2a01:2b3:4:a::1



Separated by
colons

Leading zeros
are omitted

2a01:2b3:4:a::1

2 octets each,
hexadecimal

The longest
chain of :0:0: is
replaced with ::



Subnets are /64

4.294.967.296 x the size of
the Internet!



No broadcasts



Multicasts, but they are local only



Features!

Autoconfiguration

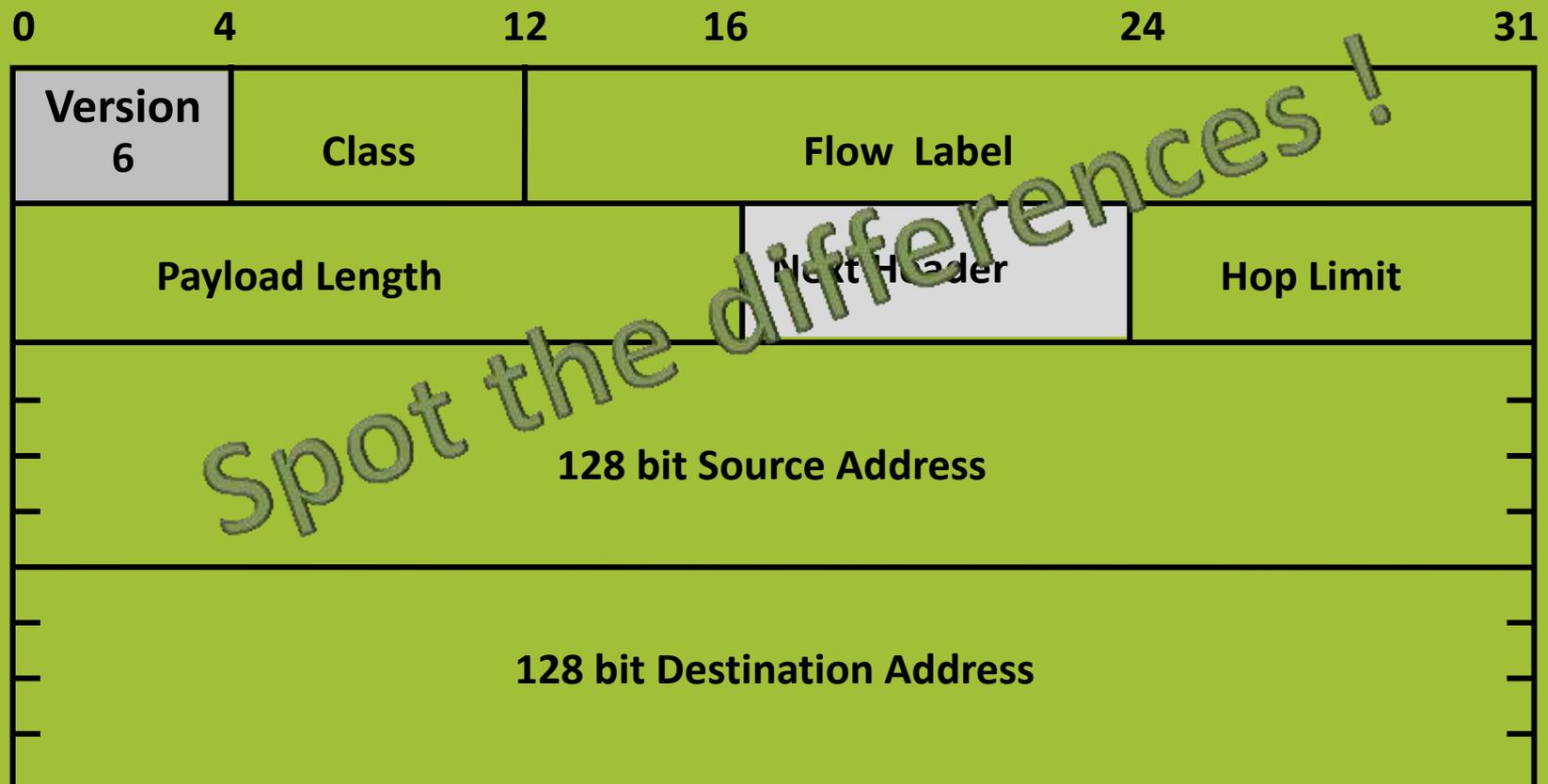
IPSEC

Mobility

Enough addresses!



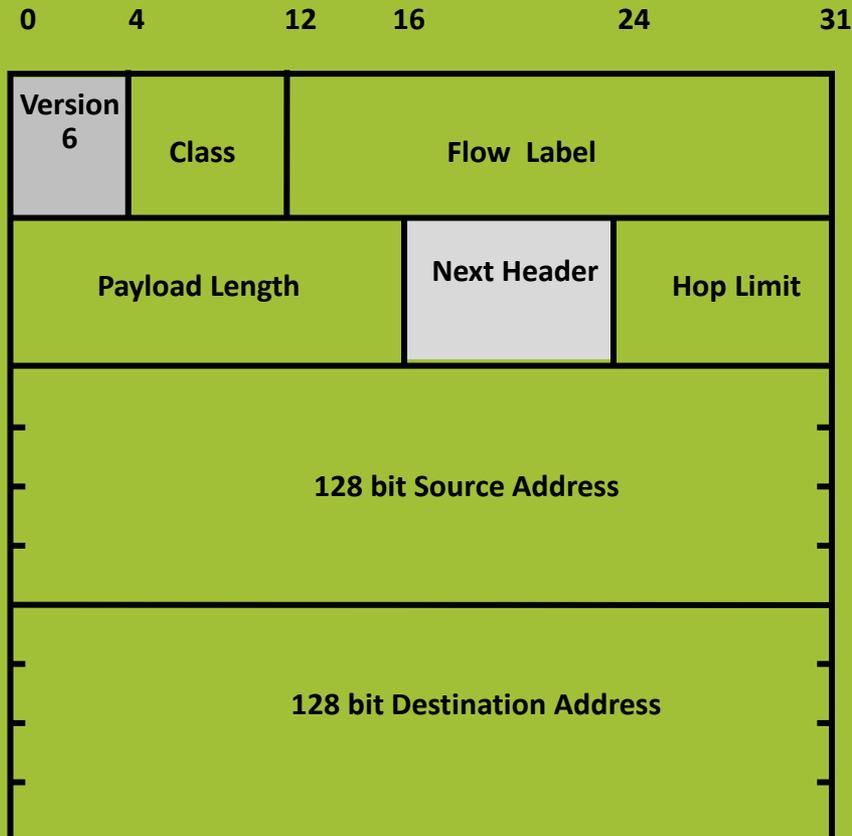
IPv6 header layout



Spot the differences!



IPv6 header layout



- No header length
- No identification
- No checksum
- No fragmentation
- No options



Every option is an extension header

Fragmentation

Source routing

IPSEC

Destination Options

...





IPv6 is much simpler than IPv4



... in theory.



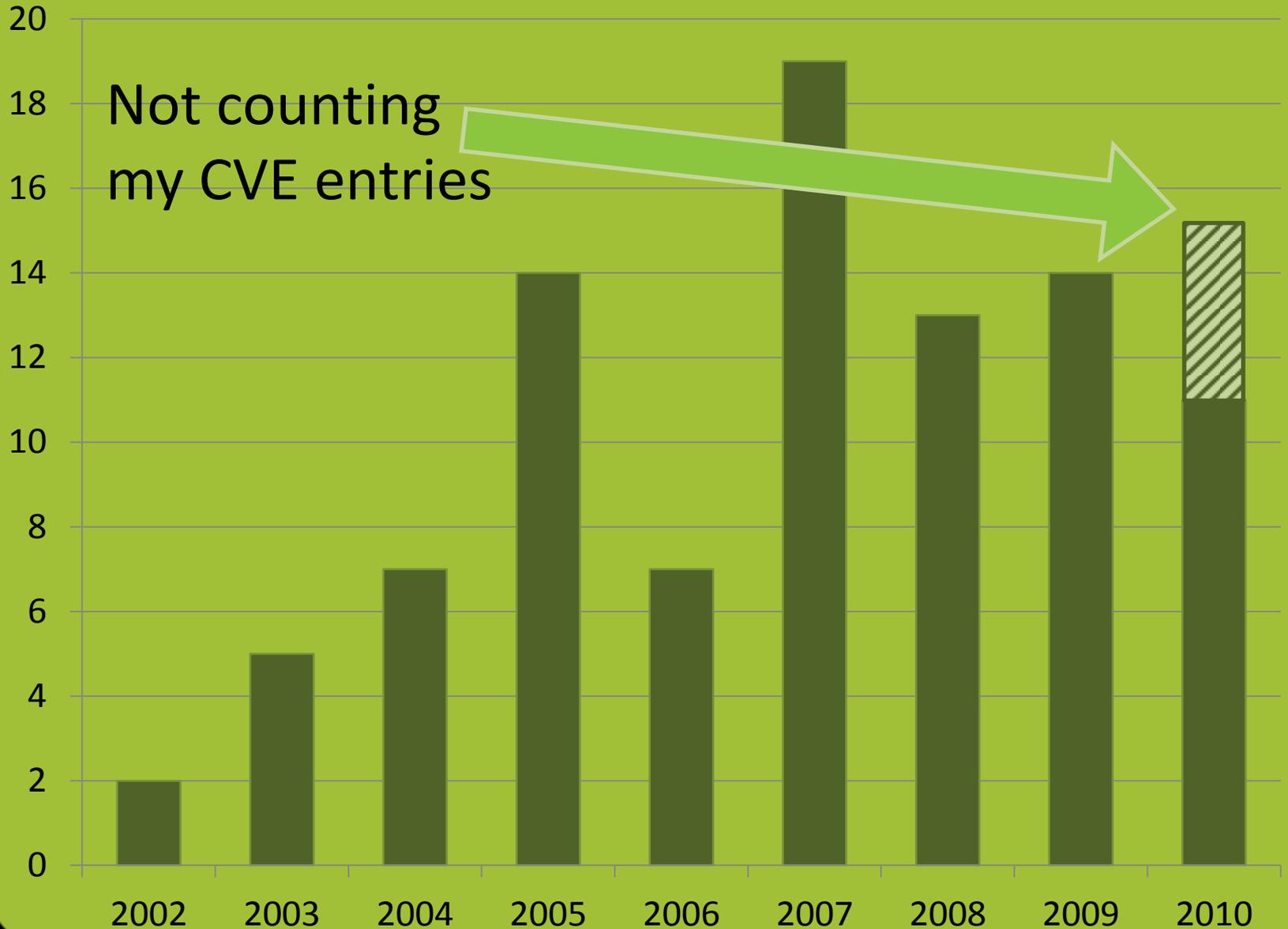
<rant>



</rant>



IPv6 Vulnerabilities (CVE)





Kids, in 2005 ...



The THC-IPv6 Attack Toolkit

ARP Spoofing => ND spoofing



1. NS:

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

parasite6:

Answers to every NS, claims to be every system on the LAN 😊

2. NA:

ICMP Type = 136
Src = B
Dst = A
Data= MAC



Duplicate Address Detection DOS



1. NS



1. NS:

ICMP Type = 135

Src = :: (unspecified)

Dst = All-Nodes Multicast
Address

query= Who-has IP A?

dos-new-ipv6:

Answer to every
NS, claim to be
every system on
the LAN 😊

2.

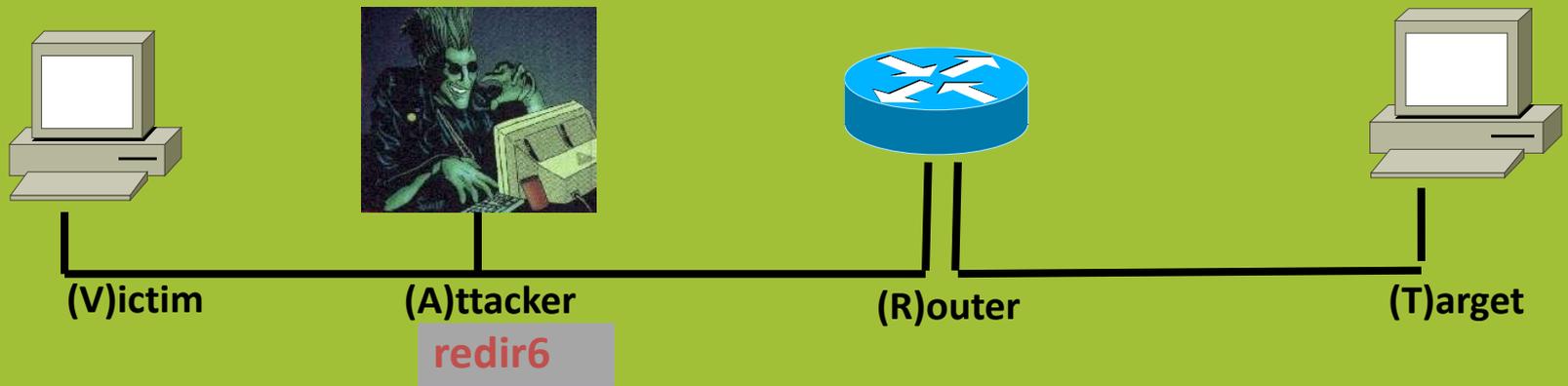
No reply if nobody owns
the IP address.



MITM with Redirects

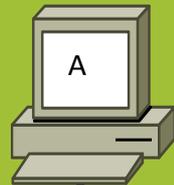


MITM with Redirects





DHCP => Autoconfiguration



1. RS



2. RA



1. RS:

ICMP Type = 133

Src = ::

Dst = FF02::2

query= please send RA

fake_router6:

Sets any IP as default router, defines network prefixes and DNS servers 😊

2. RA:

ICMP Type = 134

Src = Router Link-local Address

Dst = FF02::1

Data= options, prefix, lifetime, autoconfig flag, DNS



new and improved!

Kick the default router!



default
router



1. Send own RA



2. Spoof RA of default router with 0 lifetime



3. Resend own RA just to be sure 😊



We are getting back
to this one





Kill all routers and clients think
everything is local
(it's in the standard)



RA => Systems become dual stack

- Can be port scanned on IPv6
 - No filtering on IPv6? Full port access
- Prefer IPv6
 - Will use your tunnel / MITM



How about announcing remote
network addresses local?
(Paypal, ...)



RA flooding!

Cisco ASA/PIX, Cisco IOS
Windows 2008, 7, Vista
old Linux
more... ?



Cisco:

Just fixed for IOS, ASA soon
(CSCti24526 , CSCti33534)



Microsoft

“We consider this issue to be by design. [and will not fix this]“

Even Apple got this problem right!



“Remote alive scans (ping scans) as we know them are unfeasible on IPv6”

some jerk

(OK, that was me in 2005)



How to identify remote systems?

~~Broadcasts~~

~~Scan the whole range~~

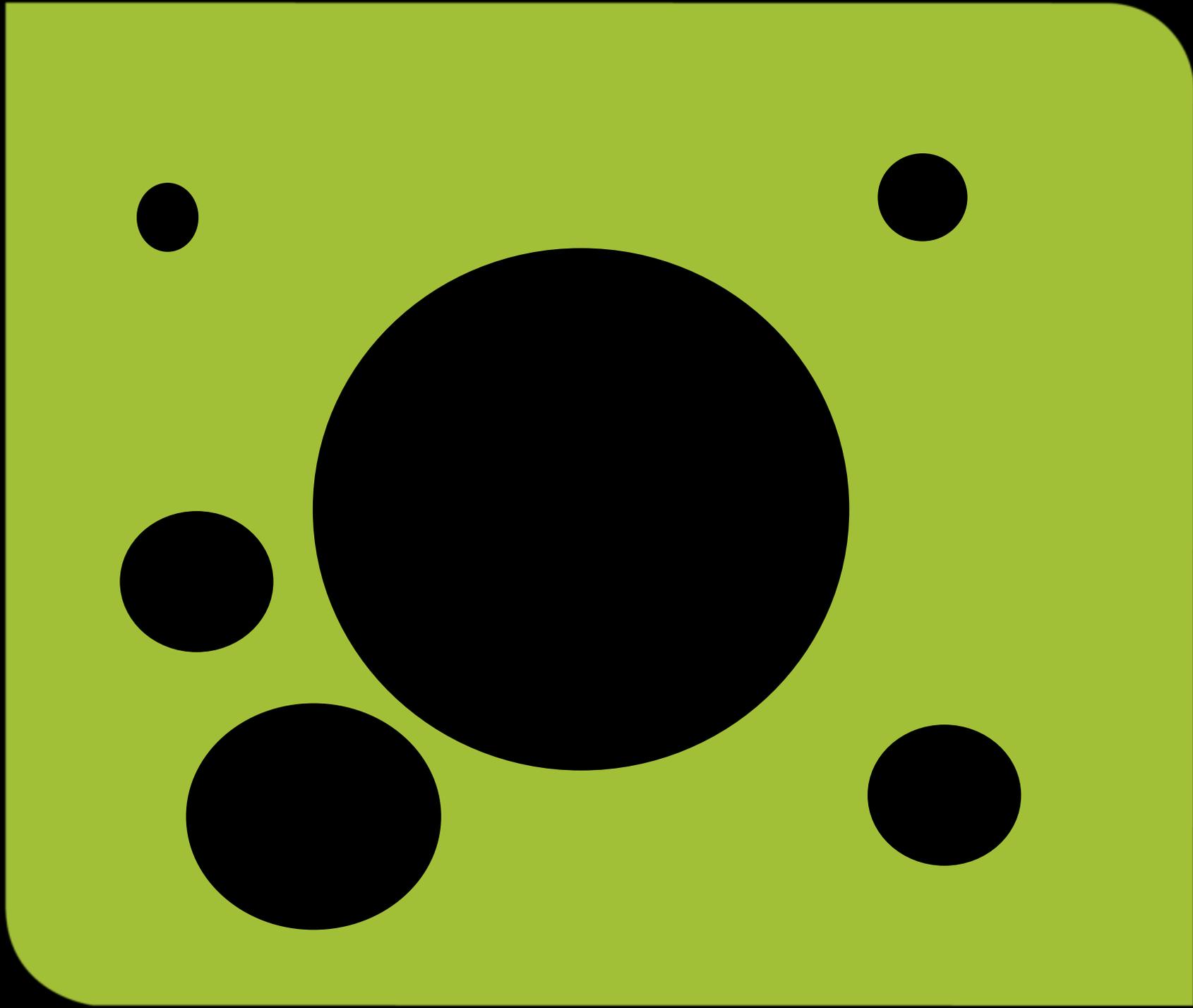
Search-engines /
databases

DNS

Combining
them

Common addresses







Search Engines

Dumped various IPv6 directories



17.000 possible domains &
subdomains identified



DNS

17.000 domains
bruteforcing 3217 hostnames



23.334 DNS entries found
(2.011 unique hostnames)



DNS Results

15.607 unique IPv6 addresses found

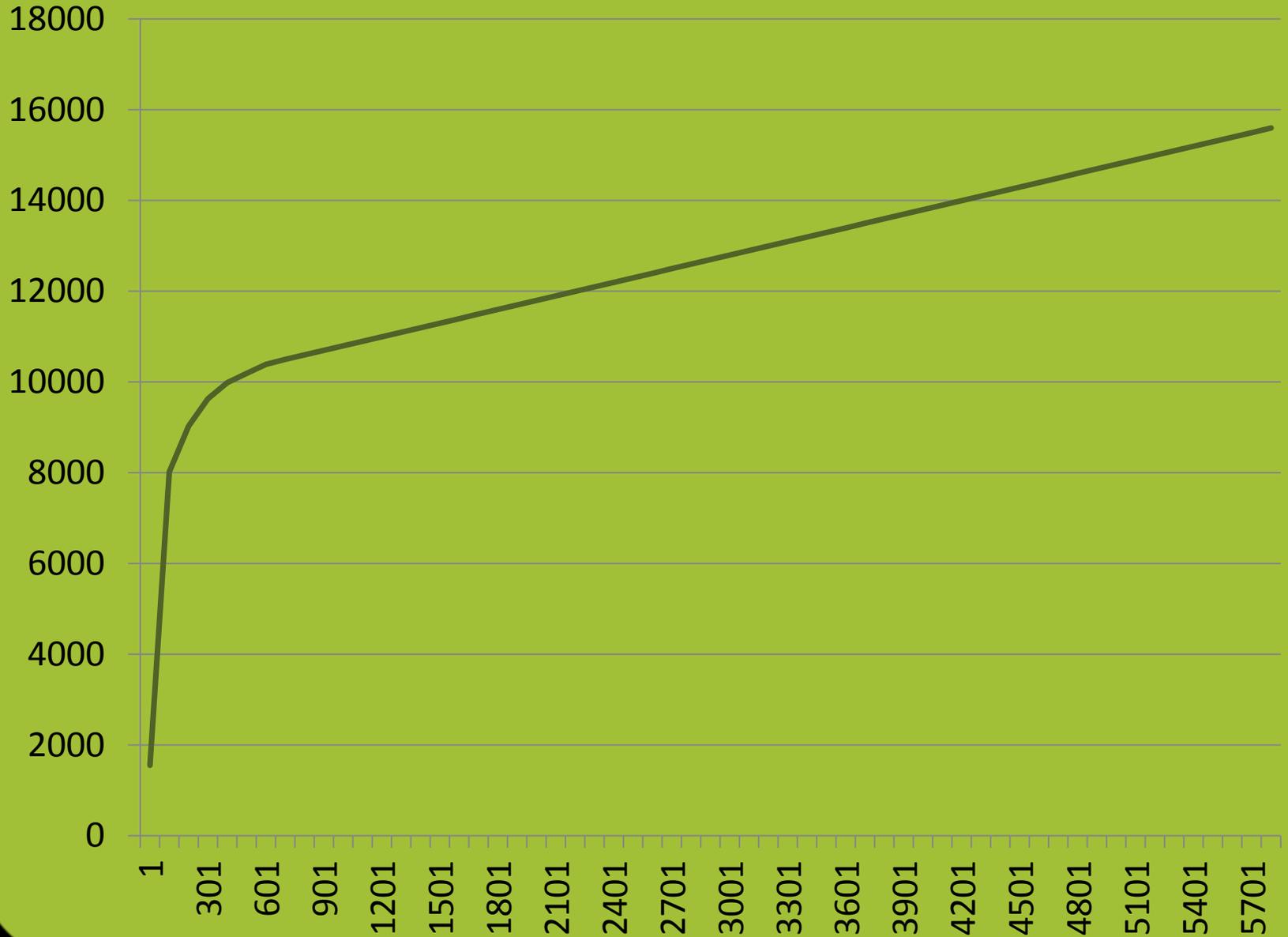


7.305 networks

5.811 unique host addresses



IPv6 Host Addresses





Host address analysis

Autoconfiguration

- MAC address \Rightarrow ~24 bit key space per vendorID
- Privacy option \Rightarrow bad luck
- Fixed random \Rightarrow bad luck

by hand

- Pattern \Rightarrow got one, got all
- Random \Rightarrow bad luck

DHCP

- Sequential
- Got one, got all
- Usually easy to find



by hand

::1, ::2, ::3, ...

::service_port

::1:service_port, ::2:service_port, ...

::service_port:1, ::service_port:2, ...

The IPv4 address

Funny stuff (::b00b:babe, etc.)

etc.



DHCP

::1000-2000

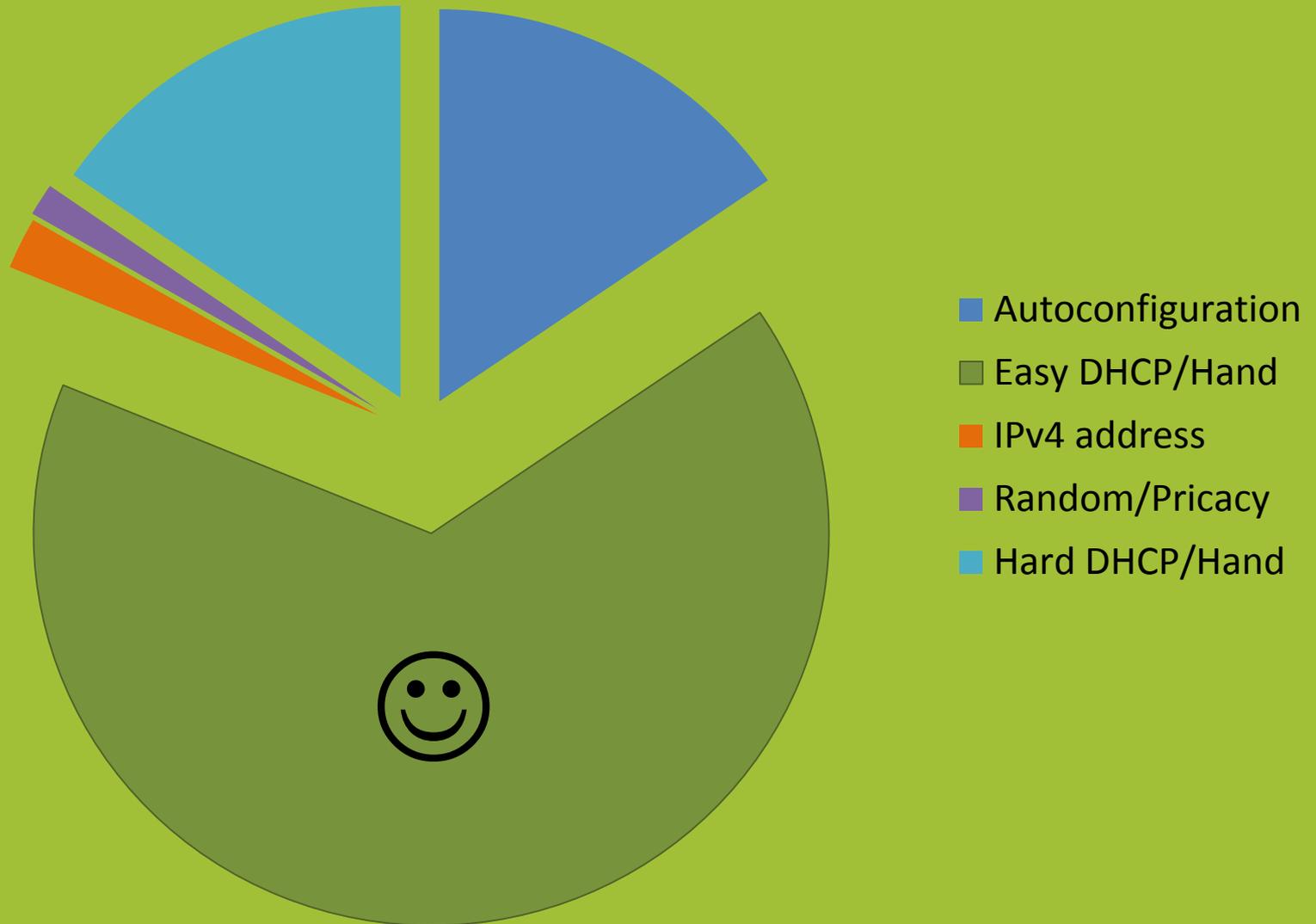
::100-200

::1:0-1000

::1:1000-2000



IPv6 Host Address Distribution





Alive Scanning

7.305 networks

bruteforcing 3000 host addresses



380.766 alive systems

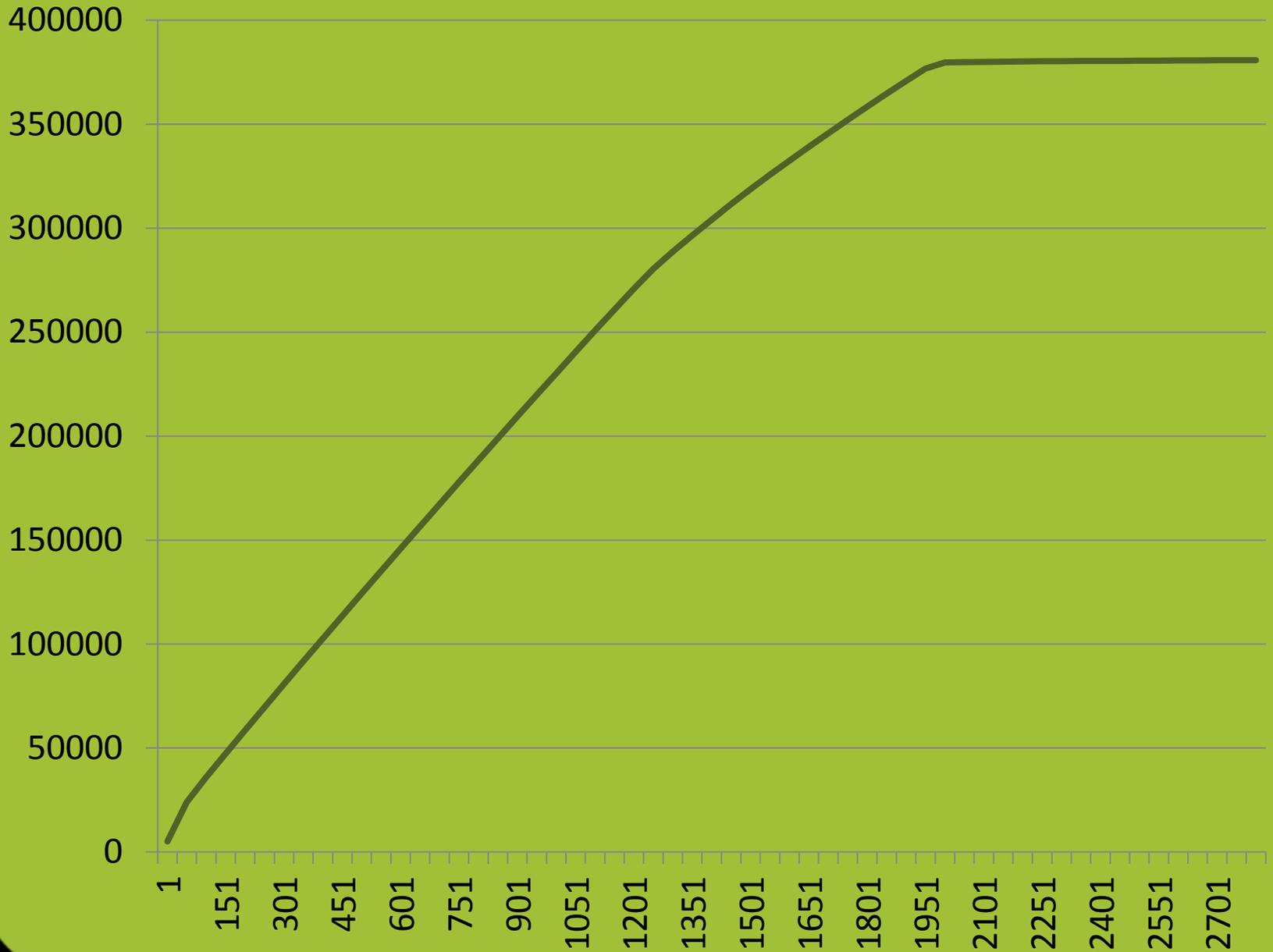


8.160 networks

2.779 unique host addresses



Alive Host Addresses





Alive Scanning

380.776 alive systems



17.154 reverse DNS entries

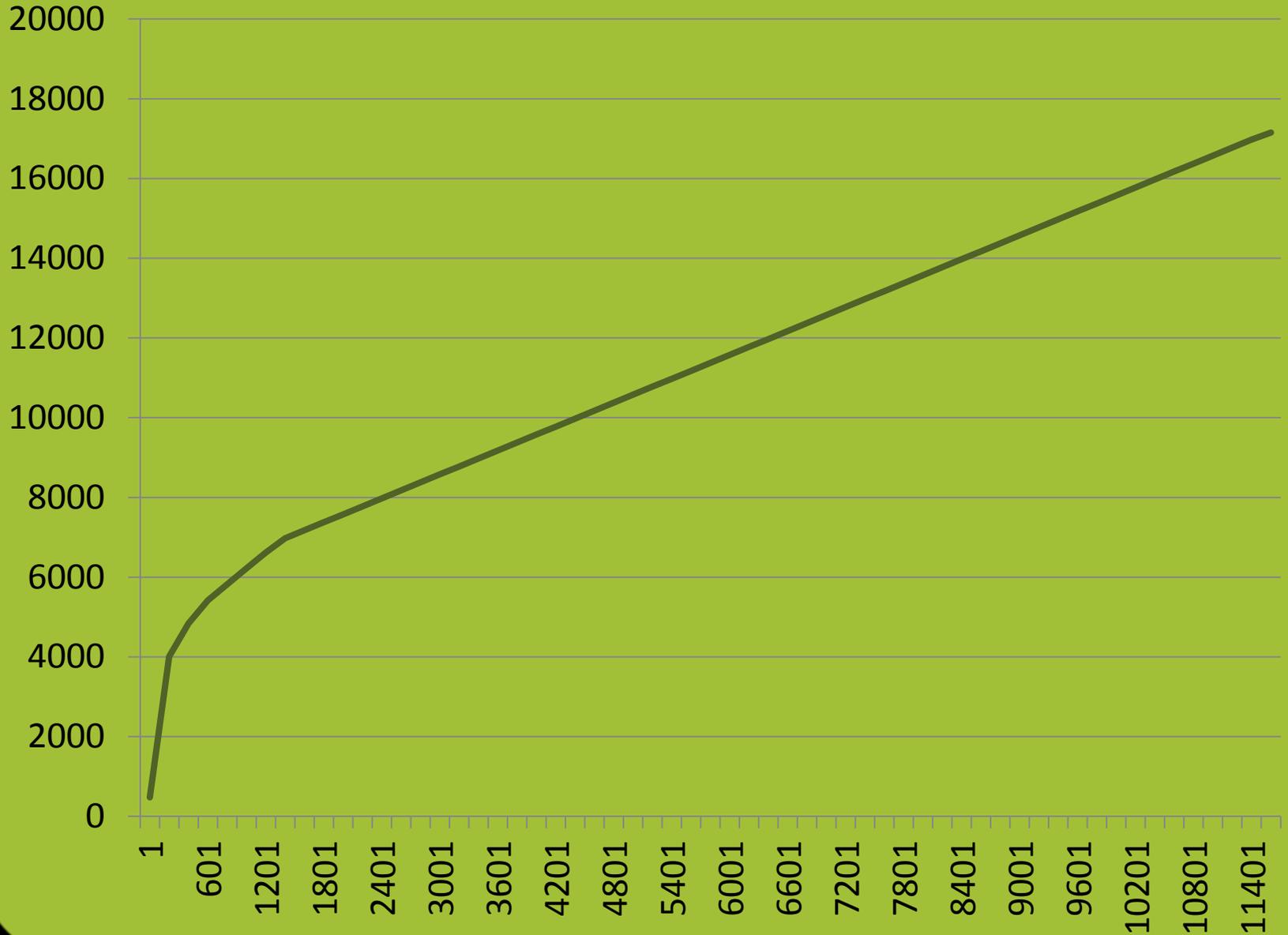


5.357 unique domains

11.578 unique hostnames



DNS Reverse Hostnames





```
do {  
    new_dns=dns_brute(new_alive);  
    new_alive=alive_brute(new_dns);  
} while (new_dns || new_alive)
```



Conclusion

DNS bruteforcing: 90% of systems
in DNS with 1900 words



Conclusion

Alive bruteforcing: 66% of systems
with 2000 addresses
scanned in 1-20 seconds



Conclusion

Combined (and use of brain)
~90-95% of **servers** are found



THERE IS MORE!



Taking over the Multicast Listener
Discovery Protocol for fun and
denying multicast traffic



How does MLD work?



Sends periodically MLD general query messages

MLD Report: "I am a multicast DNS server" to all routers

DNS multicast traffic flows to the network

Sends specific address query message

MLD Report: "I am (still) a multicast DNS server"



Spoofs "A" MLD Done message





First we want to become the MLD
query router

```
if (router1 < router2)  
    master(router1);
```



Sends periodically MLD general query messages

MLD Report: "I am a multicast DNS server" to all routers

DNS multicast traffic flows to the network

Spoofs MLD general query message as fe80::

Spoofs "A" MLD Done message



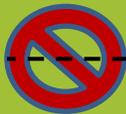


Problem: We must send an MLD
general query message regularly



Solution:

Spoof query message with
multicast all-router MAC address!



Spoof MLD general query message as fe80::

Spoofs "A" MLD Done message

Send general query as fe80:: with special MAC





Anybody sniffing?





Send a ping to the target with an unused multicast MAC address

(Windows, Linux, more?)



Side channels in IPv6?

IPv6 **is** a side channel.



Don't be scared.



IPv6

complex

intellectual challenge

tired ... ?

be an explorer!



Join researching IPv6!



How to get IPv6 to your home (1/4)

1. Create an account at Sixxs:
<http://www.sixxs.net/>
2. Request tunnel (static if possible for you, heartbeat otherwise)
3. Request a subnet (a week later)



How to get IPv6 to your home (2/4)

4. a) Configure a static tunnel:

```
ip tunnel add sixxs mode sit local [Your  
IPv4 Endpoint] remote [Sixxs IPv4  
Endpoint]  
  
ip link set sixxs up  
  
ip link set mtu 1280 dev sixxs  
  
ip tunnel change sixxs ttl 64  
  
ip -6 addr add [Your IPv6  
Endpoint]/[Prefix Length] dev sixxs  
  
ip -6 ro add default via [Your IPv6  
endpoint] dev sixxs
```



How to get IPv6 to your home (3/4)

4. b) Configure a heartbeat tunnel:

a) Install aiccu

b) Configure aiccu.conf:

```
username xxxx-SIXXS  
password xxxxxxxxxxx  
tunnel_id T<your tunnel id>  
daemonize true  
automatic true  
ipv6_interface sixxs
```

c) Start aiccu



How to get IPv6 to your home (4/4)

5. Configure your local network card

```
ip -6 addr add [Your IPv6  
subnet]::1/[Prefix Length] dev eth0
```

6. Use fake_router6 for your local subnet:

```
fake_router6 eth0 <Your IPv6  
subnet>::/<Prefix Length>  
2a01:4f8:100:2283::2
```



What is new in thc-ipv6 since the 2005-2007 release?

- DNS6 bruteforcer
- More payloads for fake_router6
- Implementation test-case tool
- Fast traceroute6
- Fuzzer for IPv6
- Flood tools for RA and NA
- Several library bugfixes & enhancements



What is new in the current thc-ipv6 source state?

- alive6 rewritten with 250% new functionality
- Flood & spoofing for all multicast protocols
- DHCPs6 spoofer
- DHCPc6 flooder
- DNS6 spoofer
- ... more new tools than fit the slide
- Enhancements for all previous tools
- Several library bugfixes & enhancements



How to get access to the current
thc-ipv6 source code state?

Send in patches and new tools!

Small and limited updates will still get
into the public version.

Complete public release in ~2011.



<http://www.thc.org/thc-ipv6>



Central information resource for
IPv6 security (wiki, forum, news):



www.ipv6security.info

www.ipv6hacking.info

(Online end of January 2011)



Contact

Send an email to
vh@thc.org
(add “antispam” to
the subject line)



Thanks!

And have fun exploring IPv6!

