NANOG 69

NAT64/DNS64 experiments, warnings and one useful tool

...from go6lab.si and IPv6-lab.net

Brought to you by:

Internet Society

Jan Žorž
zorz@isoc.org

go6

Sander Steffann
sander@steffann.nl

steffann

Problem statement and real world status

(Six Degrees of Inner Turbulence)

IPv6 and IPv4 are incompatible on the wire.

- We need transition and translation mechanisms between the two protocols
- Mobile operators are massively switching devices to IPv6-only connectivity
  - millions of users
  - using 464XLAT (Android) or plain NAT64 (Apple) as a transition tool to access IPv4 content
- Some people do weird stuff while adding AAAA to their DNS records
- Important questions:
  - Do content providers know how their content will be seen from such environments?
  - Do connectivity providers know what their users' experience on IPv6-only would be?

Credits, acknowledgments and supporters

(Metropolis, Pt. 1: The Miracle and the Sleeper)

Projects like this and all the massive amount of work cannot be performed without great support of people and companies that we work with:

Internet Society - for Jan's working time and funding of the numerous travels where we got the idea of the IPv6 issues while talking to operators and also future travels where we'll talk about this topic (we are here, aren't we? :))

Go6 Institute Slovenia - for funding and running the Go6lab where we got connectivity, HW, SW and place to experiment with all this things IPv6

SJM Steffann for Sander's working time, coding skills, massive energy and also HW/SW in their ipv6-lab.net to make this tool redundant.

Corinne Pritchard for a lovely design of a tool's front-end. Hugs :)

Go6lab NAT64/DNS64 public test-bed

(The Test That Stumped Them All)

Aimed at everyone who would like to test NAT64/DNS64 functionality

4 different implementations, 4 different instructions how to direct traffic there

Used by operators

- Testing the idea of providing NAT64/DNS64 and/or 464XLAT to their users

Used by application providers

- To see how their apps works in NAT64/DNS64 environment

Used by HW/SW vendors

- Testing their solutions against multiple NAT64 vendors

Gained quite some traction and momentum this days

Instructions: https://go6lab.si/current-ipv6-tests/nat64dns64-public-test/

Go6lab NAT64/DNS64 test-bed

https://go6lab.si/current-ipv6-tests/nat64dns64-public-test/

NAT64/DNS64 public test

Go6lab is hosting a variety of NAT64/DNS64 solutions, open for general Internet public for testing.

Disclaimer: This setup is not intended for performance testing, just to see how NAT64/DNS64 operates, what applications breaks and what are differences between different implementations. If you need to do performance testing of NAT64/DNS64 send email to <zavod@go6.si> and schedule a test session in go6lab facility.

To test different NAT64/DNS64 setups you need to disable IPv4 on your device and set an IPv6 resolving DNS server, different one for each setup. Please send us your observations, specially about which applications breaks in IPv6-only/NAT64 environment. We would like to build a list of them.

A10 Networks NAT64 implementation: set your DNS to **2001:67c:27e4:15::6411**
NAT64 implementation is running on a A10 vThunder virtual appliance.
NAT64 routed prefix: 2001:67c:27e4:642::/64
Quick ping6 test if up&running: ping6 2001:67c:27e4:642::5bef:6015

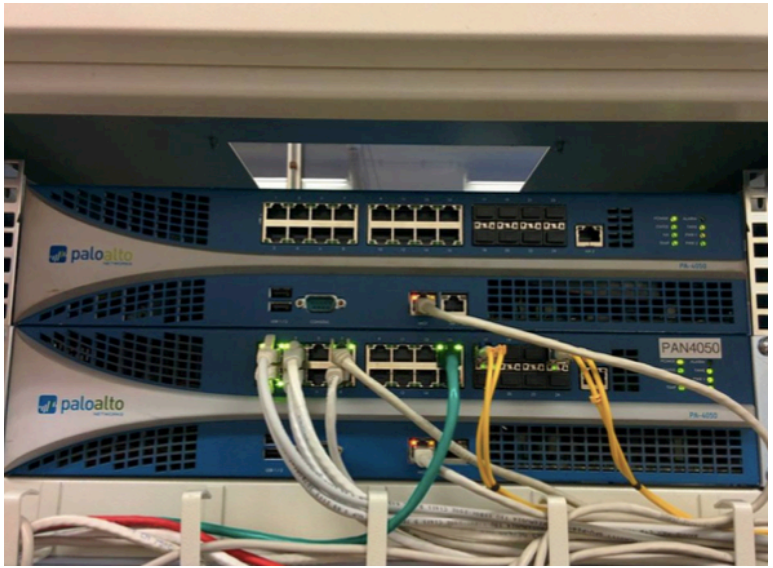
PaloAlto Networks Firewall NAT64 with BIND9.9 DNS64: set your DNS to **2001:67c:27e4::64**
NAT64 implementation is running in PAN500 firewall box.
NAT64 routed prefix: 2001:67c:27e4:64::/64
Quick ping6 test if up&running: ping6 2001:67c:27e4:64::5bef:6015

Jool NAT64 with BIND9 DNS64: set your DNS to **2001:67c:27e4:15::64**
Jool NAT64 implementation is running in a virtual container on proxmox server.
NAT64 routed prefix: 2001:67c:27e4:1064::/64
Quick ping6 test if up&running: ping6 2001:67c:27e4:1064::5bef:6015

Cisco ASR1000 NAT64 with BIND9 DNS64: set your DNS to **2001:67c:27e4::60**
NAT64 implementation is running in Cisco ASR1001.
NAT64 routed prefix: 2001:67c:27e4:11::/64
Quick ping6 test if up&running: ping6 2001:67c:27e4:11::5bef:6015

Go6lab NAT64/DNS64 test-bed HW/SW

(Systematic Chaos)



Some DNS admins put “crap” in AAAA records

(The Enemy Inside)

Have you ever seen any of this values for AAAA record?

::

::1

::ffff:[IPv4_addr]

fe80::[some_value]

64:ff9b::[some_value]

2001:DB8::[some_value]

If you have seen something like this and you know who did it, talk to that people and tell them to fix it. This sort of thing isn’t useful to anybody and severely impacts user experience.

More: http://www.employees.org/~dwing/aaaa-stats/ (courtesy of Dan Wing)

Causing confusion with or without www

(Breaking All Illusions)

```
sander@MacPro:~$ host www.firstinsight.com
www.firstinsight.com is an alias for 160569.group19.sites.hubspot.net.
160569.group19.sites.hubspot.net is an alias for
cos2mdc.hubspot.net.mdc.edgesuite.net.
cos2mdc.hubspot.net.mdc.edgesuite.net is an alias for a1711.b.akamai.net.
a1711.b.akamai.net has address 88.221.254.18
a1711.b.akamai.net has address 88.221.254.10

sander@MacPro:~$ host firstinsight.com
firstinsight.com has IPv6 address ::
firstinsight.com mail is handled by 10 mx1.emailsrvr.com.
firstinsight.com mail is handled by 20 mx2.emailsrvr.com.
```

When deploying in real life you need “fixes”

(Build Me Up, Break Me Down)

So, what can we do about it?

We can figure out who this people are, contact them, warn them about the issue, educate them and ask them to fix the problem.

Remember: If you are not part of solution, you are part of the problem.

At the same time we can protect our users from bad user experience and set the “exclude” rules in our DNS64 servers. IANA allocated 2000::/3 as global unicast address pool, so whatever else is used in AAAA - it’s by default bogus and we can safely ignore that.

When deploying in real life you need “fixes”

(Stream of Consciousness)

BIND9 example of DNS64 configuration in go6lab:

```
dns64 2001:67c:27e4:64::/96 {
        clients { any; };
        mapped { !rfc1918; any; };
        exclude { 0::/3; 4000::/2; 8000::/1; 2001:DB8::/32; };
        break-dnssec yes;
};
```

Explanation of “exclude” configuration parameter: If DNS64 server gets an AAAA record with a value of anything outside 2000::/3 - it ignores it and synthesizes the AAAA record from NAT64_prefix::IPv4_address

When deploying in real life you need “fixes”

(Moment Of Betrayal)

This fixes the most common errors and keeps your users relatively safe from bad user experience when using 464XLAT and NAT64

This also prevent issues when AAAA record contains an IPv6 documentation prefix, that is inside 2000::/3 block.

“Break-dnssec yes” configuration directive:

> By default, DNS64 module does not process queries that request DNSSEC data (DO = 1) or that have DNSSEC RRs in the answer. Setting break-dnssec yes will override this default and cause policy processing on all DNSSEC queries. However, the constructed response will not have any DNSSEC records added and therefore cannot be verified by the client (it may have the unintended consequence of looking like a bogus response or even an injection attack to the client).

Oops: website about firewalls

IPv4

NAT64

Oops: website about firewalls

Still waiting for that timeout…

IPv4

NAT64

Oops: website about firewalls

Very secure...

IPv4

NAT64

Oops: website about firewalls

Very secure, running on ::ffff:
209.59.x.y…

IPv4

NAT64

Good DNS, bad server

IPv4

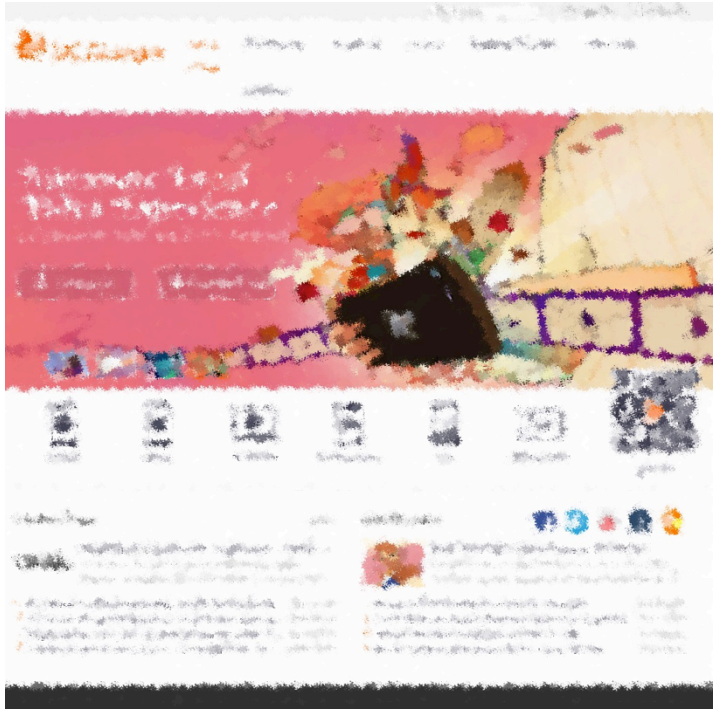
IPv6 and NAT64

Good DNS, bad geolocation tool

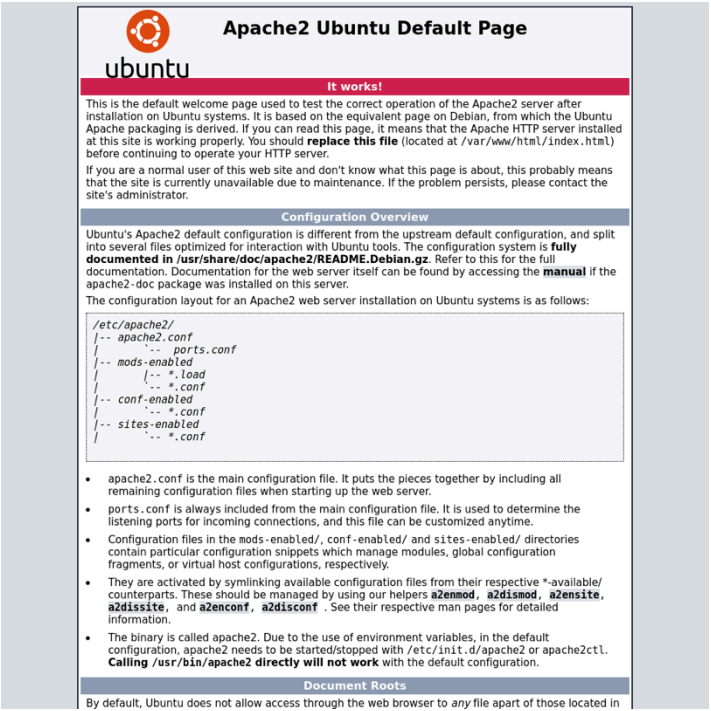
IPv4

IPv6 and NAT64

No AAAA, server still confused



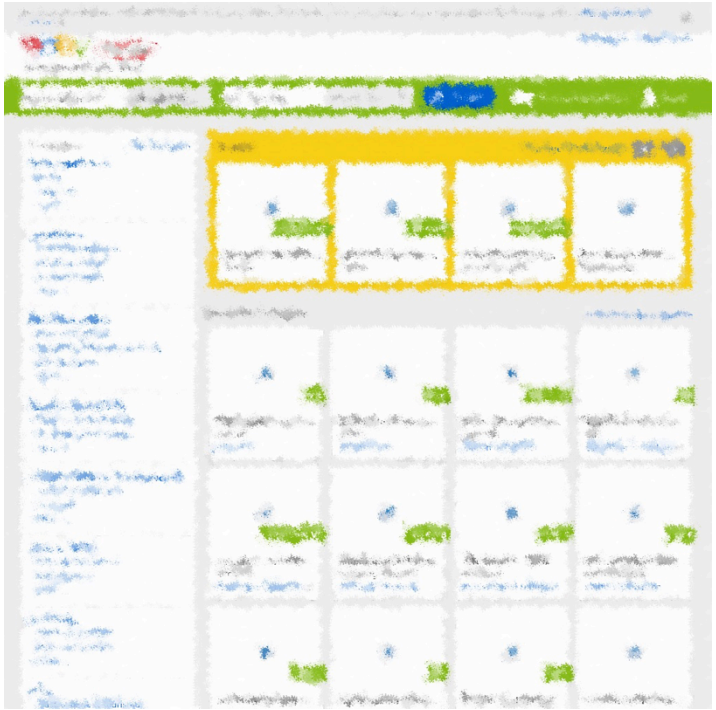
IPv4



NAT64

Good server, bad content/images

IPv4 and NAT64



IPv6

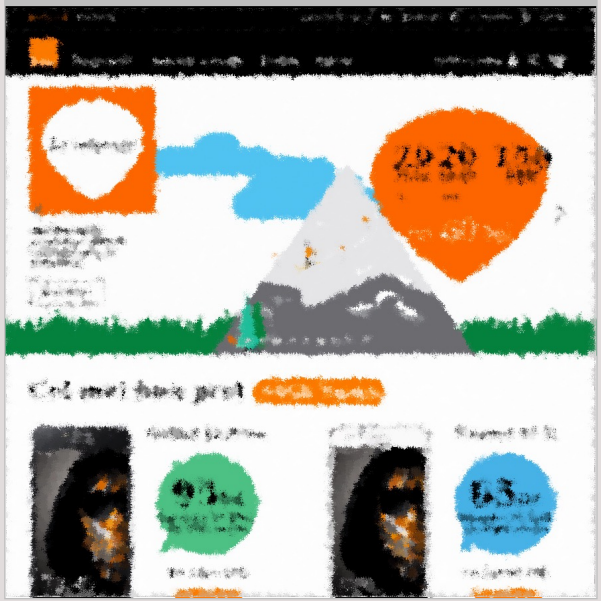
Good server, bad content/css

IPv4 and NAT64

IPv6

Non working AAAA record = broken NAT64 ☺

Image match

NAT64	IPv4-only	IPv6-only
		

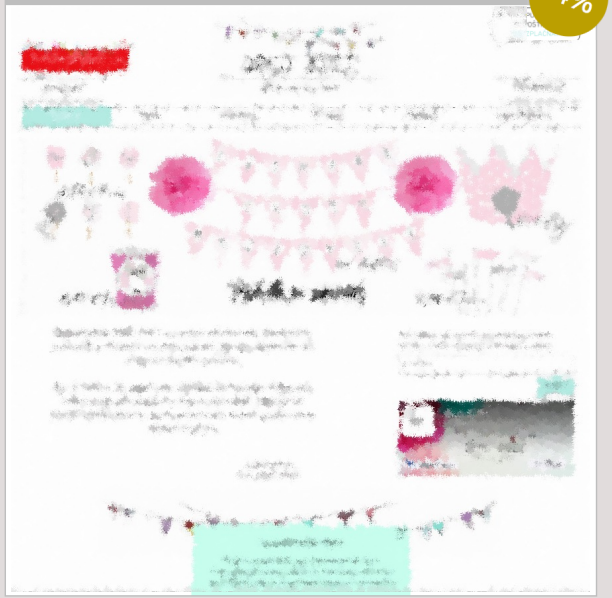
Resources match ▶

NAT64	IPv4-only	IPv6-only
Unreachable		Unreachable

DNS records	IPv4-only	IPv6-only
	212.56.221.5	2a01:c8cf:ffd9:1::1111

Working AAAA record and IPv4-only content

NAT64 84%



IPv4-only

IPv6-only 78%

Resources match ▼

99%

1%

URL	NAT64-only	IPv4-only	IPv6-only
GET http://deko-svet.si/	Moved	Moved	Moved
GET http://www.deko-svet.si/	Ok	Ok	Ok
GET http://frog.wix.com/bt?src=29&evid=3&pn=1&et=1&v=1.1939.13&msid=73fcc1f2-b6a4-4066-9548-5598c03d9b03&vsi=40da48dd-2df1-4f54-8951…	Ok		
GET http://frog.wix.com/bt?src=29&evid=3&pn=1&et=1&v=1.1939.13&msid=73fcc1f2-b6a4-4066-9548-5598c03d9b03&vsi=dd42d5c9-3d4d-40ef-9e0a…			Bad gateway
GET http://frog.wix.com/bt?src=29&evid=3&pn=1&et=1&v=1.1939.13&msid=73fcc1f2-b6a4-4066-9548-5598c03d9b03&vsi=d33a5027-aef3-4c98-96cc…		Ok	
GET https://static.parastorage.com/services/third-party/requirejs/2.1.15/require.min.js	Ok	Ok	-

Working AAAA record and IPv4-only content

URL	NAT64-only	IPv4-only	IPv6-only
[redacted]	Moved	Moved	Moved
[redacted]	Ok	Ok	Ok
[redacted]&pn=1&et=1&v=1.1939.13&msid=73fcc1f2-b6a4-4066-9548-5598c03d9b03&vsi=40da48dd-2df1-4f54-8951…	Ok		
[redacted]&pn=1&et=1&v=1.1939.13&msid=73fcc1f2-b6a4-4066-9548-5598c03d9b03&vsi=dd42d5c9-3d4d-40ef-9e0a…			Bad gateway
[redacted]&pn=1&et=1&v=1.1939.13&msid=73fcc1f2-b6a4-4066-9548-5598c03d9b03&vsi=d33a5027-aef3-4c98-96cc…		Ok	
[redacted]/third-party/requirejs/2.1.15/require.min.js	Ok	Ok	-
[redacted]/santa/1.1939.13/app/main-r.min.js	Ok	Ok	-
[redacted]/santa/1.1939.13/static/css/viewer.css	Ok	Ok	-
[redacted]/web/2.1229.56/javascript/wysiwyg/viewer/deprecatedbrowsers/UpgradeBrowser.js	Ok	Ok	-
[redacted]0946736314&evid=361&src=42&majorVer=3&server=app-jvm14c&did=98a027aa-433e-4874-8e6b-9197c3fa…	Ok		
[redacted]3_1685ea46e831627d8b2fee6a28075065_726.json.z?v=3	Ok	Ok	
[redacted]0946736315&evid=351&src=42&majorVer=3&server=app-jvm14c&did=98a027aa-433e-4874-8e6b-9197c3fa…	Ok		
[redacted]323&evid=3&src=29&pn=1&isp=1&url=deko-svet.si%2F&v=1.1939.13&dc=app-jvm14c&sid=98a027aa-433e-…	Ok		
[redacted]0946736130&evid=361&src=42&majorVer=3&server=app-jvm12a&did=98a027aa-433e-4874-8e6b-9197c3fa…		Ok	
[redacted]0946736131&evid=351&src=42&majorVer=3&server=app-jvm12a&did=98a027aa-433e-4874-8e6b-9197c3fa…		Ok	
[redacted]139&evid=3&src=29&pn=1&isp=1&url=deko-svet.si%2F&v=1.1939.13&dc=app-jvm12a&sid=98a027aa-433e-…		Ok	
[redacted]/santa/1.1939.13/packages-bin/wixCodeInit/wixCodeInit.min.js	Ok	Ok	
[redacted]/third-party/lodash/3.10.1/lodash.min.js	Ok	Ok	
[redacted]/santa/1.1939.13/packages-bin/coreUtils/coreUtils.min.js	Ok	Ok	
[redacted]/santa/1.1939.13/packages-bin/skins/skins.min.js	Ok	Ok	
[redacted]/santa/1.1939.13/packages-bin/components/components.min.js	Ok	Ok	
[redacted]/santa/1.1939.13/packages-bin/core/core.min.js	Ok	Ok	
[redacted]/third-party/tweenmax/1.18.2/minified/TweenMax.min.js	Ok	Ok	
[redacted]/santa/1.1939.13/packages-bin/animations/animations.min.js	Ok	Ok	
[redacted]/third-party/react/0.14.3/react-with-addons.min.js	Ok	Ok	
[redacted]/santa/1.1939.13/packages-bin/layout/layout.min.js	Ok	Ok	
[redacted]/santa/1.1939.13/packages-bin/wixappsCore/wixappsCore.min.js	Ok	Ok	
[redacted]/santa/1.1939.13/packages-bin/wixappsClassics/wixappsClassics.min.js	Ok	Ok	
[redacted]/santa/1.1939.13/packages-bin/wixappsBuilder/wixappsBuilder.min.js	Ok	Ok	
[redacted]/santa/1.1939.13/packages-bin/tpa/tpa.min.js	Ok	Ok	
[redacted]/santa/1.1939.13/packages-bin/dataFixer/dataFixer.min.js	Ok	Ok	
[redacted]/santa/1.1939.13/packages-bin/siteUtils/siteUtils.min.js	Ok	Ok	
[redacted]/santa/1.1939.13/packages-bin/translationsUtils/translationsUtils.min.js	Ok	Ok	
[redacted]/third-party/hammerjs/2.0.8/hammer.min.js	Ok	Ok	

How to test for all of these things?

(The Looking Glass)

There are many things to test:

- Test on NAT64
- Test on IPv6-only
- Did all resources (images, stylesheets, scripts) load ok?
- Does it look good to the user?
- Do we see any pMTUd issues?

One service to test them all: **NAT64Check !!!**

(Caught in a web)

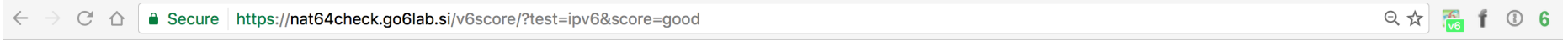
nat64check

Check: http://www.example.com/

Internet Society go6 steffann

Search NAT64 IPv6 Poor Mediocre Good

	URL	When	NAT64	IPv6-only
Details	http://dehumida.si	Nov. 27, 2016, 10:27 p.m.	100%	Unreachable
Details	http://osvelikadolina.si	Nov. 27, 2016, 10:27 p.m.	100%	Unreachable
Details	http://puhar.si	Nov. 27, 2016, 10:27 p.m.	100%	Unreachable
Details	http://vkf-renzel.si	Nov. 27, 2016, 10:27 p.m.	100%	Unreachable
Details	http://domstarejsihidila.si	Nov. 27, 2016, 10:27 p.m.	100%	Unreachable
Details	http://mirza.si	Nov. 27, 2016, 10:27 p.m.	100%	Unreachable
Details	http://program-za-trgovino.si	Nov. 27, 2016, 10:27 p.m.	100%	Unreachable
Details	http://fitness-epicenter.si	Nov. 27, 2016, 10:27 p.m.	100%	Unreachable
Details	http://vrtuoz.si	Nov. 27, 2016, 10:27 p.m.	100%	Unreachable
Details	http://chill.si	Nov. 27, 2016, 10:27 p.m.	100%	Unreachable



(Caught in a web)

nat64check

Check: http://www.example.com/

Internet Society go6 steffann

Search NAT64 IPv6 Poor Mediocre Good

	URL	When	NAT64	IPv6-only
Details	http://www.sdeval.si	Nov. 27, 2016, 10:25 p.m.	100%	100%
Details	http://myunikat.si	Nov. 27, 2016, 10:21 p.m.	100%	100%
Details	http://korsic.si	Nov. 27, 2016, 10:19 p.m.	100%	100%
Details	http://igraj-tenis.si	Nov. 27, 2016, 10:16 p.m.	100%	97%
Details	http://www.vrtecosbos.si	Nov. 27, 2016, 10:08 p.m.	100%	100%
Details	http://69.si	Nov. 27, 2016, 10:06 p.m.	100%	100%
Details	http://renovatio.si	Nov. 27, 2016, 10:02 p.m.	100%	100%
Details	http://ki-ki-do.si	Nov. 27, 2016, 10:02 p.m.	100%	100%
Details	http://projekt-it.si	Nov. 27, 2016, 9:58 p.m.	100%	100%
Details	http://lenstime.si	Nov. 27, 2016, 9:56 p.m.	100%	97%

Secure https://nat64check.go6lab.si/v6score/measurement-19037/

nat64check

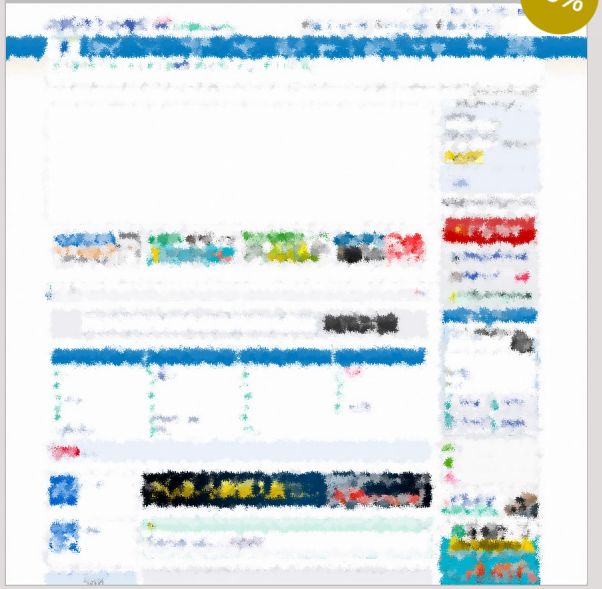
(The Mirror)

www.netbk.co.jp Test again

Last test finished:
23 November 2016, 01:21 CET

Image match

NAT64	IPv4-only	IPv6-only
85%		



Resources match ▶

nat64check

(The Shattered Fortress)

www.netbk.co.jp

Test again

Last test finished:
23 November 2016, 01:21 CET

Image match

NAT64	IPv4-only	IPv6-only
85%		

Resources match

We don’t “fix” brokenness

(Lines in the Sand)

For NAT64/DNS64 implementations in go6lab, we try to avoid AAAA bogus records and all our DNS64 configs are tuned like we have shown in previous slides.

For NAT64 Check tool, however, we don’t exclude anything. We are trying to show how it is in reality and not mask problems. Those people, causing problems needs to find out the situation and fix it.

https://nat64check.go6lab.si/
https://nat64check.ipv6-lab.net/

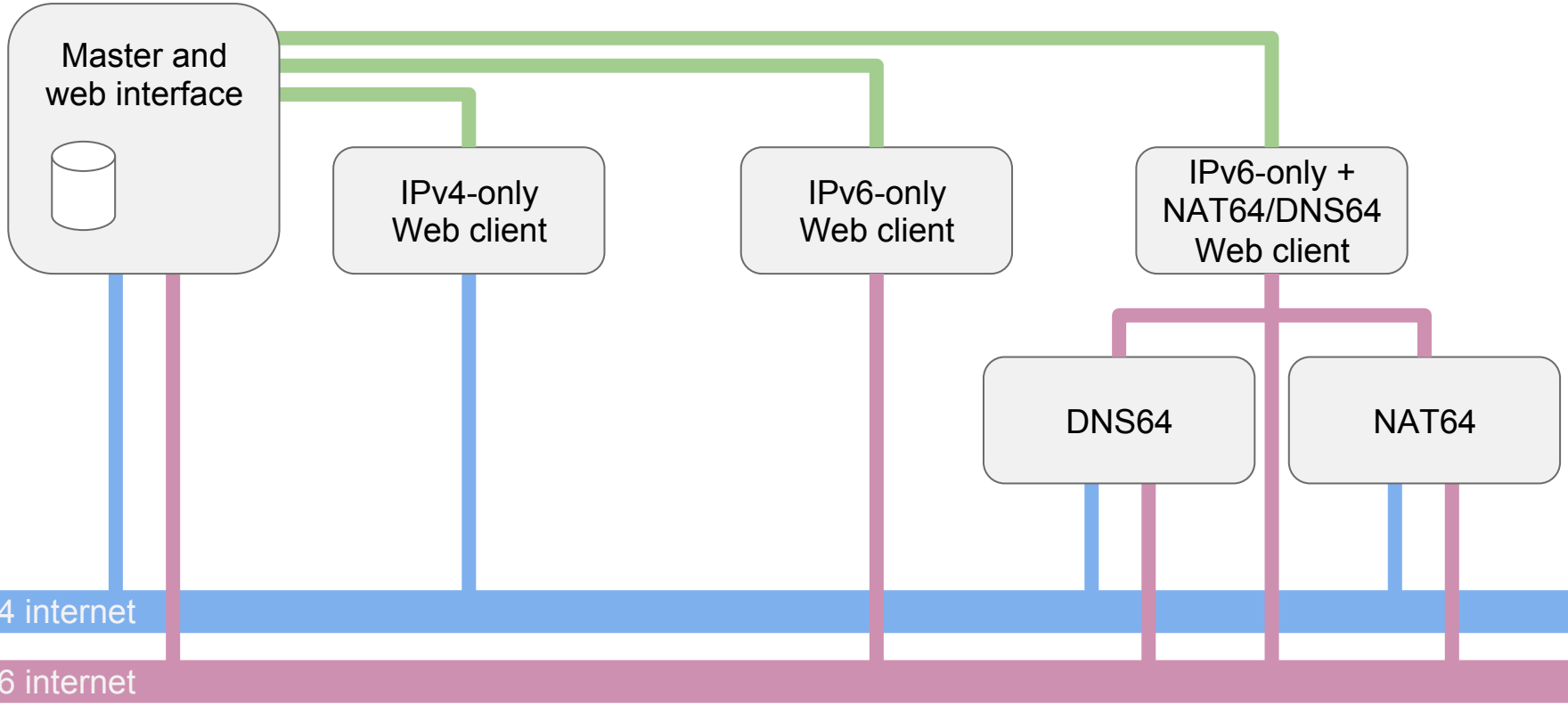
How does this work?

(Illumination Theory)

- Four servers:
  - Management server and web interface
  - Server with only IPv4
  - Server with only IPv6
  - Server with NAT64
  - Go6lab specific: All servers are virtual machines (LIX) on Proxmox 4.2 virtualization cluster
  - IPv6-lab.net specific: All running on virtual machines (Ubuntu) on a VMware cluster
- Using phantomjs as a command-line browser
  - Keep track of all loaded (or not) resources
  - Make a screenshot when the page has loaded
- Compare images with each other
- Check for resources that could not be loaded

How does this work?

(Images and Words)



Run the test and calculate the score

(Take the Time)

Enter the domain name or URL that you would like to test and submit it to the system.

The process of starting all needed browsers, get the results, grab the screen and calculate/compare all the results takes some time, so please be patient.

Run the test and calculate the score

(Take the Time)

You'll see something like this for some time after you start the measurement...

Measurement #15784

Website:	www.afrinic.net
Test requested:	Nov. 18, 2016, 3:59 p.m.
Test started:	Nov. 18, 2016, 3:59 p.m.
Test finished:	None

Back to overview

The system will show you when the test was requested, when test was started and will also show you the result in the same page after some time.

No need to hit the "Back" button, it will happen, just give it some time. We promise. Scout's word of honor. :)

Wash, rinse and repeat

(Lifting Shadows of a Dream)

Test your website

Are you sure all the images, analytics scripts etc. load over IPv6?

If you don't have IPv6 on your server:

Did you hard-code any IPv4 addresses in your HTML code? In this case NAT64/DNS64 will fail. You might get away with it on 464XLAT, but don't count on it.

Why you don't have IPv6 on your server yet?

If things fail - make sure you are persistent enough to find the issues. There are millions of potential viewers of your content on IPv6-only connection at this precise moment, make sure you don't mess it up and that our tool shows the 100% good result.

Test again

Repeat until your website is no longer broken

If you are fixing a DNS misconfiguration - it might take some time before our tool gets and sees the new and fixed AAAA value. DNS propagation is slow.

Non properly working target domain = no content!

(Learning To Live)

```
Dec 02 12:01:21 nat64check-core named[42328]: REFUSED unexpected RCODE resolving 'supersaver.si/AAAA/IN': 2a0b:8e00::10#53
Dec 02 12:01:21 nat64check-core named[42328]: REFUSED unexpected RCODE resolving 'supersaver.si/AAAA/IN': 2a0b:8e00:1::10#53
Dec 02 12:07:08 nat64check-core named[42328]: REFUSED unexpected RCODE resolving 'everlast.si/AAAA/IN': 192.241.255.25#53
Dec 02 12:07:08 nat64check-core named[42328]: REFUSED unexpected RCODE resolving 'everlast.si/AAAA/IN': 176.62.8.3#53
Dec 02 12:07:08 nat64check-core named[42328]: REFUSED unexpected RCODE resolving 'everlast.si/AAAA/IN': 176.62.8.3#53
Dec 02 12:07:08 nat64check-core named[42328]: REFUSED unexpected RCODE resolving 'everlast.si/AAAA/IN': 192.241.255.25#53
Dec 02 12:09:34 nat64check-core named[42328]: DNS format error from 173.255.195.189#53 resolving ns3.dnserv.com/AAAA: Name dnserv.com (SOA) not subd
main of zone ns3.dnserv.com -- invalid response
Dec 02 12:09:34 nat64check-core named[42328]: FORMERR resolving 'ns3.dnserv.com/AAAA/IN': 173.255.195.189#53
Dec 02 12:09:34 nat64check-core named[42328]: REFUSED unexpected RCODE resolving 'strojno-vezenje.si/AAAA/IN': 173.255.195.189#53
Dec 02 12:10:18 nat64check-core named[42328]: REFUSED unexpected RCODE resolving 'biomasanaklik.si/A/IN': 185.53.12.52#53
Dec 02 12:18:59 nat64check-core named[42328]: success resolving 'g-ns-1485.awsdns-10.co.uk/AAAA' (in 'awsdns-10.co.uk'?) after disabling EDNS
Dec 02 12:18:59 nat64check-core named[42328]: success resolving 'g-ns-453.awsdns-04.net/AAAA' (in 'awsdns-04.net'?) after disabling EDNS
Dec 02 12:19:00 nat64check-core named[42328]: success resolving 'g-ns-163.awsdns-35.org/AAAA' (in 'awsdns-35.org'?) after disabling EDNS
Dec 02 12:19:00 nat64check-core named[42328]: success resolving 'g-ns-596.awsdns-20.com/AAAA' (in 'awsdns-20.com'?) after disabling EDNS
Dec 02 12:37:40 nat64check-core named[42328]: DNS format error from 203.205.147.152#53 resolving ns1.qq.com/AAAA: Name qq.com (SOA) not subdomain of
zone ns1.qq.com -- invalid response
Dec 02 12:37:40 nat64check-core named[42328]: FORMERR resolving 'ns1.qq.com/AAAA/IN': 203.205.147.152#53
Dec 02 12:37:40 nat64check-core named[42328]: DNS format error from 203.205.147.152#53 resolving ns3.qq.com/AAAA: Name qq.com (SOA) not subdomain of
zone ns3.qq.com -- invalid response
Dec 02 12:37:40 nat64check-core named[42328]: FORMERR resolving 'ns3.qq.com/AAAA/IN': 203.205.147.152#53
Dec 02 12:37:40 nat64check-core named[42328]: DNS format error from 182.254.16.102#53 resolving ns-cnc1.qq.com/AAAA: Name qq.com (SOA) not subdomain
of zone ns-cnc1.qq.com -- invalid response
Dec 02 12:37:40 nat64check-core named[42328]: FORMERR resolving 'ns-cnc1.qq.com/AAAA/IN': 182.254.16.102#53
Dec 02 12:37:40 nat64check-core named[42328]: DNS format error from 182.254.16.102#53 resolving ns-cmn1.qq.com/AAAA: Name qq.com (SOA) not subdomain
of zone ns-cmn1.qq.com -- invalid response
Dec 02 12:37:40 nat64check-core named[42328]: FORMERR resolving 'ns-cmn1.qq.com/AAAA/IN': 182.254.16.102#53
Dec 02 12:37:40 nat64check-core named[42328]: DNS format error from 182.254.16.102#53 resolving ns-tel1.qq.com/AAAA: Name qq.com (SOA) not subdomain
of zone ns-tel1.qq.com -- invalid response
Dec 02 12:37:40 nat64check-core named[42328]: FORMERR resolving 'ns-tel1.qq.com/AAAA/IN': 182.254.16.102#53
Dec 02 12:37:40 nat64check-core named[42328]: DNS format error from 182.254.16.102#53 resolving ns1.qq.com/AAAA: Name qq.com (SOA) not subdomain of
one ns1.qq.com -- invalid response
Dec 02 12:37:40 nat64check-core named[42328]: FORMERR resolving 'ns1.qq.com/AAAA/IN': 182.254.16.102#53
Dec 02 12:37:40 nat64check-core named[42328]: DNS format error from 182.254.16.102#53 resolving ns-os1.qq.com/AAAA: Name qq.com (SOA) not subdomain
```

Conclusions, questions, suggestions?

(Act II: Scene Eight: The Spirit Carries On)

If you are content provider: test how people sees your content from different environments

If you are connectivity provider: test how IPv6-only and 464XLAT/NAT64-DNS64 users sees content

If both: all of the above :)

You might be surprised. Well, you probably will be surprised.

https://nat64check.go6lab.si/
https://nat64check.ipv6-lab.net/

Internet Society

Jan Žorž
zorz@isoc.org

go6

Sander Steffann
sander@steffann.nl

steffann