





Maynard Koch, Raphael Hiesgen, Thomas C. Schmidt, Matthias Wählisch

## **Amplification through IPv6 routing loops** A call to fix router configurations.

RIPE 90, Lisbon, Portugal // May 2025

Contact: maynard.koch@tu-dresden.de

🚄 captu	re-icmp-flood.pcapng										-	o x
<u>D</u> atei <u>B</u>	earbeiten <u>A</u> nsicht <u>N</u> avigation	n <u>A</u> ufzeichnen Anal <u>y</u> se <u>S</u> tatistiken	Telephonie Wireless Tools Hilfe									
	1 © 🗀 🖹 🗙 🙆   9, 🦛	🕨 🏓 著 🔮 📃 📃 ବ୍ ବ୍ ବ୍	**									
No.	Time	Source	Destination		Protocol	Length Info						
	10.000000000	2001:4dd0:a000	2a00:20:b004:2c1	1:2a10:782f:51e	ICM	166 Time	Exceeded	(hop	limit	exceeded	in	tran
	20.000000135	2001:4dd0:a000	2a00:20:b004:2c1	1:2a10:782f:51e	ICM	166 Time	Exceeded	(hop	limit	exceeded	in	tran
	30.004207259	2001:4dd0:a000	2a00:20:b004:2c1	1:2a10:782f:51e	ICM	166 Time	Exceeded	(hop	limit	exceeded	in	tran
	40.004207386	2001:4dd0:a000	2a00:20:b004:2c1	1:2a10:782f:51e	ICM	166 Time	Exceeded	(hop	limit	exceeded	in	tran 🔤
	50.007819047	2001:4dd0:a000	2a00:20:b004:2c1	1:2a10:782f:51e	ICM	166 Time	Exceeded	(hop	limit	exceeded	in	tran
	60.010723704	2001:4dd0:a000	2a00:20:b004:2c1	1:2a10:782f:51e	ICM	166 Time	Exceeded	(hop	limit	exceeded	in	tran
	70.012922813	2001:4dd0:a000	2a00:20:b004:2c1	1:2a10:782f:51e	ICM	166 Time	Exceeded	(hop	limit	exceeded	in	tran
	80.012922957	2001:4dd0:a000	2a00:20:b004:2c1	1:2a10:782f:51e	ICM	166 Time	Exceeded	(hop	limit	exceeded	in	tran
	90.017221473	2001:4dd0:a000	2a00:20:b004:2c1	1:2a10:782f:51e	ICM	166 Time	Exceeded	(hop	limit	exceeded	in	tran
1	00.017221651	2001:4dd0:a000	2a00:20:b004:2c1	1:2a10:782f:51e	ICM	166 Time	Exceeded	(hop	limit	exceeded	in	tran
1	10.023861166	2001:4dd0:a000	2a00:20:b004:2c1	1:2a10:782f:51e	ICM	166 Time	Exceeded	(hop	limit	exceeded	in	tran
1	20.023861222	2001:4dd0:a000	2a00:20:b004:2c1	1:2a10:782f:51e	ICM	166 Time	Exceeded	(hop	limit	exceeded	in	tran
1	30.023861237	2001:4dd0:a000	2a00:20:b004:2c1	1:2a10:782f:51e	ICM	166 Time	Exceeded	(hop	limit	exceeded	in	tran
1	40.023861269	2001:4dd0:a000	2a00:20:b004:2c1	1:2a10:782f:51e	ICM	166 Time	Exceeded	(hop	limit	exceeded	in	tran
1	50.027820090	2001:4dd0:a000	2a00:20:b004:2c1	1:2a10:782f:51e	ICM	166 Time	Exceeded	(hop	limit	exceeded	in	tran
1	60.027820136	2001:4dd0:a000	2a00:20:b004:2c1	1:2a10:782f:51e	ICM	166 Time	Exceeded	(hop	limit	exceeded	in	tran
1	70.032142221	2001:4dd0:a000	2a00:20:b004:2c1	1:2a10:782f:51e	ICM	166 Time	Exceeded	(hop	limit	exceeded	in	tran
1	80.033449496	2001:4dd0:a000	2a00:20:b004:2c1	1:2a10:782f:51e	ICM	166 Time	Exceeded	(hop	limit	exceeded	in	tran
1	90.040326659	2001:4dd0:a000	2a00:20:b004:2c1	1:2a10:782f:51e	ICM	166 Time	Exceeded	(hop	limit	exceeded	in	tran
2	00.040326921	2001:4dd0:a000	2a00:20:b004:2c1	1:2a10:782f:51e	ICM	166 Time	Exceeded	(hop	limit	exceeded	in	tran
2	10.043376058	2001:4dd0:a000	2a00:20:b004:2c1	1:2a10:782f:51e	ICM	166 Time	Exceeded	(hop	limit	exceeded	in	tran
_	0.0.040076444	2004 4 1 10 000	2-00-20-1-004-2-1	1 - 2 - 1 0 - 702 ( - 51 -	TCM	100 T	E	1	12			<b>1</b>

📕 capt	ure-icmp-flood.pcapng										-	o x
<u>D</u> atei	<u>B</u> earbeiten <u>A</u> nsicht <u>N</u> avigation	<u>A</u> ufzeichnen Anal <u>y</u> se <u>S</u> tatistiken	Telephonie <u>W</u> ireless <u>T</u> ools	<u>H</u> ilfe								
	2 O 🗆 🗋 X 🖸 🤇 🔶	> 🕾 T 🖢 📃 📃 🔍 Q Q	2.3									
Anzei	gefilter anwenden <ctrl-></ctrl->											
No.	Time	Source	Destination		Protocol	Length Info						
	10.000000000	2001:4dd0:a000	2a00:20:b004:	2c11:2a10:782f:51e	ICM	166 Time	Exceeded	(hop	limit	exceeded	in	tran
	20.000000135	2001:4dd0:a000	2a00:20:b004:	2c11:2a10:782f:51e	ICM	166 Time	Exceeded	(hop	limit	exceeded	in	tran
	30.004207259	2001:4dd0:a000	2a00:20:b004:	2c11:2a10:782f:51e	ICM	166 Time	Exceeded	(hop	limit	exceeded	in	tran
	4 0 001202206	2001-1440-2000	2-00.20.4001.	<u>)-11.)-10.78)f.[1</u>	ТСМ	166 Timo	Excooded	(hon	limi+	aveaadad	in	±nan=
	5											an
	6	_	•			_						an
	7	Δ	single		'ho	) trie	JJAP	2				an
	0		JIIgic				58	3				20
	0	OF OL		<b>C</b>				-				all
	9	>250k r	eblies	from tr	ne s	sam	e ro		ler.			an
	10									)		an
	11											an
	12											an
	13											an
	14											an
	15											an
	16	7001.4000.0000		( <u>)     , / g   y , / y /   , /   ;</u>			LALEEVEN	1100		EALEEVEN		- an
	170 032142221	2001 · 4dd0 · a000	2a00.20.h004.	2c11·2a10·782f·51e	ТСМ	166 Time	Fyceeded	(hon	limit	exceeded	in	tran
	180 033110106	2001.4dd0.2000	2000.20.0004.	2c11.2a10.782f.51c		166 Time	Exceeded	(hop	limi+	ovcoodod	in	tran
	10 0 01033443490	2001.4000.8000	2-00.20.0004.	2 <u>c11.2a10.702</u> 1.51e		166 Time	Exceeded	(hop	1;	exceeded	-111 -111	than
	190.040326659	2001:4000:4000	2-00:20:0004:	2 <u>cii:2ai0:782</u> f:51e		100 TIMe	Exceeded			exceeded	1n	tran
	200.040326921	2001:4000:000	2a00:20:0004:	2c11:2a10:782+:51e	ICM	166 lime	Exceeded	(nop	limit	exceeded	in	tran
	210.043376058	2001:4dd0:a000	2a00:20:b004:	2c11:2a10:782f:51e	ICM	166 Time	Exceeded	(hop	limit	exceeded	in	tran
	DD 0 012276111	2001 . 1440 . 2000	2-00.20.6001.	<u>2011 • 2010 • 782 F • 510</u>	TCM	166 Timo	Evenadad	(hon	limi+	ovcoodod	in	tran

🚄 capture-icmp-flood.pcapng										-	o x
<u>D</u> atei <u>B</u> earbeiten <u>A</u> nsicht <u>N</u> avigatio	n <u>A</u> ufzeichnen Anal <u>y</u> se <u>S</u> tatistiken	Telephonie <u>W</u> ireless <u>T</u> ools <u>H</u> ilfe									
	• 🔿 🕾 🚡 📃 🔍 Q, Q										
Anzeigefilter anwenden <ctrl-></ctrl->											
		Destination		Protocol		Twoodod	(hen	1::+	avaaadad	1	±
10.00000000	2001:4000:2000.	2a00:20:0004:2C11	.:2a10:782f:51e	1CM	166 Time	Exceeded	(nop	limit	exceeded	1n	tran
20.000000135	2001:4dd0:a000.	2a00:20:b004:2c11	:2a10:782f:51e	ICM	166 Time	Exceeded	(hop	limit	exceeded	in	tran
30.004207259	2001:4dd0:a000	2a00:20:b004:2c11	:2a10:782f:51e	ICM	166 Time	Exceeded	(hop	limit	exceeded	in	tran
4 0 001202286	2001 • 1440 • 2000	2-00.20.h001.2-11	· 2-10.702f.51-	тсм	166 Timo	Evended	(hon	limi+	avcoadad	in	±nan —
5											an
6	_	• • •			_ •						an
7	$\Delta$	single (	MP Fc	ho	) tria	JJAP	5				an
,						58	5				an
0	AFAL						-		<b>.</b>		an
9	>250K r	enlies f	rom fh	<b>e</b> 9	sam	e ro	UIT	er.	<b>*</b>		an
10							GIG		)		an
11											an
12											an
13	•		•				_	-			an
14	*Don't wor	rv. we know	how to inc	reas	se this	event	furt	her	:(.		an
15		<i>, , , , , , , , , , , , , , , , , , , </i>							~~~		an
16											20
170 021020130	2001.4440000	2-00.20.6004.2011	· 2a10· 7021· 510·	TCM	100 1100	Evended	(100	12	exceeded	±	trall
1/0.032142221	2001:4000:2000.	2a00:20:0004:2c11	.:2a10:782†:51e	1CM	166 lime	Exceeded	(nop	limit	exceeded	in	tran
180.033449496	2001:4dd0:a000	2a00:20:b004:2c11	:2a10:782f:51e	1CM	166 Time	Exceeded	(hop	limit	exceeded	in	tran
190.040326659	2001:4dd0:a000	2a00:20:b004:2c11	:2a10:782f:51e	ICM	166 Time	Exceeded	(hop	limit	exceeded	in	tran
200.040326921	2001:4dd0:a000.	2a00:20:b004:2c11	:2a10:782f:51e	ICM	166 Time	Exceeded	(hop	limit	exceeded	in	tran
210.043376058	2001:4dd0:a000	2a00:20:b004:2c11	:2a10:782f: <u>51e</u>	ICM	166 Time	Exceeded	(hop	limit	exceeded	in	tran
220 012276111	2001.1440.2000	2-00.20.4001.2c11	·2-10.782f.51	TCM	166 Timo	Excooded	(hon	limi+	avcoodod	in	tran



#### Routing Loops [Misconfiguration]



TTL Exceeded Amplification

[Software Bug]









#### **Common deployment? Yes!**

Those deployments easily occur when providers assign PA address space to customers.

... and there is one more problem.



#### A loop ultimately leads to an ICMP TTL Exceeded



2001:db8::/32 **R1** A router bug leads to duplication of an ICMP Echo. ::/0 **R2** 2001:db8:b0b0::/48 2001:db8:d0d0::/48 b8:cafe::1

**R1** 

A router bug leads to duplication of an ICMP Echo.

Each duplicated ICMP Echo is duplicated again. Exponential increase of ICMP Echos between routers.



**R1** 

**R2** 

A router bug leads to duplication of an ICMP Echo.

**Each duplicated ICMP Echo is duplicated again.** Exponential increase of ICMP Echos between routers.



**R1** 

A router bug leads to duplication of an ICMP Echo.

Each duplicated ICMP Echo is duplicated again. Exponential increase of ICMP Echos between routers.

Each duplicate triggers an individual TTL Exceeded.

**Amplification at its best!** 

[Confirmed by Juniper.]



### What is a routing loop? **Solution: Null route.**



### How many IPv6 routing loops occur?

#### November 2024

141M /48 subnets

#### **April 2025**

162M (+15%) /48 subnets

#### How many IPv6 routing loops occur?



**5411 ASes in 155 countries** are affected by routing loops.

**18% of all looping** /48 subnets concentrate in only 5 ASes.

**55% of all looping** /48 subnets concentrate in only 5 countries.

#### How many /48 allow for TTL Exceeded amplifications?

#### November 2024

7.4M /48 subnets

#### **April 2025**

10M (+35%) /48 subnets

#### How many /48 allow for TTL Exceeded amplifications?



**1885 ASes in 102 countries** show amplifying router behavior.

**9% of all amplifying** /48 subnets concentrate in 10 ASes.

**82% of all amplifying** /48 subnets concentrate in only 5 countries with Brazil alone accounting for 72%.

## **Amplification Factors by TTL Exceeded messages**



**Maximum packet size** of ICMPv6 error message is 1280 bytes.

**99% of the amplification** factors are below 6.

**8 routers** operated by a single German ISP reach amplification factors of more than 250K.

**Juniper L3 switches** of the EX production line, e.g. EX3400 are affected by the amplification bug.

#### We reached out to operators of affected networks and created a lot of noise. Sorry for that!

We ran an email campaign to get in contact with operators of affected networks.

**To motivate operators to reply**, we kept the initial mail intentionally vague without any specific details of affected devices.

We received >1000 replies, including phone calls.

While the majority appreciated our work (so did we your reply, thanks a lot!), we also received a lot of complains about spreading panic by not sharing specific information at first hand.

#### We reached out to operators of affected networks and created a lot of noise. Sorry for that!

**Promise:** In the future, we will include all important details in the first email.

We ran an email campaign to get in contact with operators of affected networks.

**To motivate operators to reply**, we kept the initial mail intentionally vague without any specific details of affected devices.

We received >1000 replies, including phone calls.

While the majority appreciated our work (so did we your reply, thanks a lot!), we also received a lot of complains about spreading panic by not sharing specific information at first hand.

### We reached out to operators of affected networks and created a lot of noise. Sorry for that!

**Promise:** In the future, we will include all important details in the first email.

But please reply, even if the email helped fixing the issue. We rely on your help.

We ran an email campaign to get in contact with operators of affected networks.

**To motivate operators to reply**, we kept the initial mail intentionally vague without any specific details of affected devices.

We received >1000 replies, including phone calls.

While the majority appreciated our work (so did we your reply, thanks a lot!), we also received a lot of complains about spreading panic by not sharing specific information at first hand.

## **Impact of the Email campaign** Thank you for your support!

**Fewer loops.** Reduced number of routing loops for /48 in **263** ASes by a total of **-7.7M** loops (of which **134** ASes have no more routing loops).

## **Impact of the Email campaign** Thank you for your support!

**Fewer loops.** Reduced number of routing loops for /48 in **263** ASes by a total of **-7.7M** loops (of which **134** ASes have no more routing loops).

Less amplification. Reduced number of /48 subnets that allow for amplification in **54** ASes by -380K (of which **32** ASes have no more amplification).

## **Impact of the Email campaign** Thank you for your support!



**Fewer loops.** Reduced number of routing loops for /48 in **263** ASes by a total of **-7.7M** loops (of which **134** ASes have no more routing loops).

**Less amplification.** Reduced number of /48 subnets that allow for amplification in **54** ASes by **-380K** (of which **32** ASes have no more amplification).

**But still ... a lot to do**, in particular given that loops+amplification have been discovered first in 2021.

#### Conclusion

Loops are bad, amplification is worse.

**IPv6 deployments make routing loops more likely than in IPv4** since PA address space is more likely partially used.

Some IPv6 router implementations duplicate looping ICMPv6 Echo requests.

We can expect an increasing threat potential with ongoing IPv6 deployment.

#### **Call for action**

**If you operate an IPv6 network and use a default route, install null routes, too!** Providers should talk to their customers.

If you do IPv6 scanning, exclude networks that lead to routing loops! We can provide data.

**Do not use unnecessarily high IP TTL values when scanning.** A value of 64 should be sufficient in most cases.



2001:db8::/32 **R1** The higher your IP TTL value, the higher the amplification. ::/0 **R2** 2001:db8:b0b0::/48 We confirmed exponential 2001:db8:d0d0::/48 growth for some few routers! b8:cafe::1

#### **How many IPv6 routing loops occur?** Top-10 countries

#### Scan 11-2024:

Country	Looping /48 subnets [#]
BRA	37,081,970
DEU	13,273,666
CZE	10,444,197
USA	7,613,551
NLD	7,241,713
ITA	5,587,495
UKR	4,754,099
TUR	4,441,823
GBR	4,216,438
FRA	3,588,092

#### Scan 03-2025:

Country	Looping /48 subnets [#]
BRA	35,674,251
DEU	18,952,139
GBR	15,815,809
CZE	12,352,542
USA	8,016,203
NLD	6,717,473
TUR	5,422,390
FRA	5,009,856
ITA	4,407,476
CHN	3,961,245

### **How many IPv6 routing loops occur?** Top-10 countries

#### Scan 11-2024:

Country	Looping /48 subnets [#]
BRA	37,081,970
DEU	13,273,666
CZE	10,444,197
USA	7,613,551
NLD	7,241,713
ITA	5,587,495
UKR	4,754,099
TUR	4,441,823
GBR	4,216,438
FRA	3,588,092

#### Scan 03-2025:

Country	Looping /48 subnets [#]
BRA	35,674,251
DEU	18,952,139
GBR	15,815,809
CZE	12,352,542
USA	8,016,203
NLD	6,717,473
TUR	5,422,390
FRA	5,009,856
ITA	4,407,476
CHN	3,961,245

**Germany** shows an increase in routing loops of **~5.7M (+43%)**.

## **How many IPv6 routing loops occur?** Top-10 countries

#### Scan 11-2024:

Country	Looping /48 subnets [#]
BRA	37,081,970
DEU	13,273,666
CZE	10,444,197
USA	7,613,551
NLD	7,241,713
ITA	5,587,495
UKR	4,754,099
TUR	4,441,823
GBR	4,216,438
FRA	3,588,092

#### Scan 03-2025:

Country	Looping /48 subnets [#]
BRA	35,674,251
DEU	18,952,139
GBR	15,815,809
CZE	12,352,542
USA	8,016,203
NLD	6,717,473
TUR	5,422,390
FRA	5,009,856
ITA	4,407,476
CHN	3,961,245

**Germany** shows an increase in routing loops of **~5.7M (+43%)**.

**Great Britain** tripled its routing loop amount to ~15.8M, an increase of **11.6M (+275%)**.

### **How many IPv6 routing loops occur?** Top-5 ASes with highest increase

AS-Number	Organization	Туре	Looping /48 subnets [#]	Δ to first scan [#]
3170	VELOXSERV	Hosting	12,652,406	+12,652,400
3214	xTom GmbH	Hosting	7,864,367	+7,864,367
16019	VODAFONE-CZ-AS	ISP	5,291,388	+467,355
43260	DGN Teknoloji A.S.	Hosting	2,518,892	+341,521
29119	AireNetworks	ISP	1,598,563	+537,516

**Two hosting providers** are responsible for the majority of newly occurred routing loops.

#### **How many /48 allow for TTL Exceeded amplifications?** Top-5 countries with highest increase of amplifying subnets

Country	Amplifying /48 subnets [#]	Δ to first scan [#]
BRA	7,148,496	+2,473,809
GBR	182,821	+172,129
PRY	128,312	+73,947
RUS	73,011	+63,154
HKG	63,793	+62,499

**Brazil** shows an increase of **~2.5M** amplifying /48 subnets (+53%).

Widely distributed in Brazil. These subnets are assigned to routers from over **789** ASes.

**Amplification factors still low in Brazil.** We only observe 7 routers with an amplification factor  $\geq$ 10 and max. amplification is **36**.