





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

Capture-icmp-flood,pcapng									-	o >			
Datei Bearbeiten Ansicht Navigation Aufzeichnen Analyse Statistiken Telephonie Wireless Iools Hilfe													
												_	
No.	Time	Source	Destination		Protocol	Length Info							ŕ
	10.000000000	2001:4dd0:a000	2a00:20:b004:2c11:2a1	l0:782f:51e	ICM	166 Time	Exceeded	(hop	limit	exceeded	in	tran	
	20.000000135	2001:4dd0:a000	2a00:20:b004:2c11:2a1	L0:782f:51e	ICM	166 Time	Exceeded	(hop	limit	exceeded	in	tran	
	30.004207259	2001:4dd0:a000	2a00:20:b004:2c11:2a1	L0:782f:51e	ICM	166 Time	Exceeded	(hop	limit	exceeded	in	tran	
	40.004207386	2001:4dd0:a000	2a00:20:b004:2c11:2a1	l0:782f:51e	ICM	166 Time	Exceeded	(hop	limit	exceeded	in	tran=	
	50.007819047	2001:4dd0:a000	2a00:20:b004:2c11:2a1	L0:782f:51e	ICM	166 Time	Exceeded	(hop	limit	exceeded	in	tran	
	60.010723704	2001:4dd0:a000	2a00:20:b004:2c11:2a1	l0:782f:51e	ICM	166 Time	Exceeded	(hop	limit	exceeded	in	tran	
	70.012922813	2001:4dd0:a000	2a00:20:b004:2c11:2a1	l0:782f:51e	ICM	166 Time	Exceeded	(hop	limit	exceeded	in	tran	
	80.012922957	2001:4dd0:a000	2a00:20:b004:2c11:2a1	L0:782f:51e	ICM	166 Time	Exceeded	(hop	limit	exceeded	in	tran	l
	90.017221473	2001:4dd0:a000	2a00:20:b004:2c11:2a1	L0:782f:51e	ICM	166 Time	Exceeded	(hop	limit	exceeded	in	tran	
	100.017221651	2001:4dd0:a000	2a00:20:b004:2c11:2a1	l0:782f:51e	ICM	166 Time	Exceeded	(hop	limit	exceeded	in	tran	l
	110.023861166	2001:4dd0:a000	2a00:20:b004:2c11:2a1	L0:782f:51e	ICM	166 Time	Exceeded	(hop	limit	exceeded	in	tran	l
	120.023861222	2001:4dd0:a000	2a00:20:b004:2c11:2a1	L0:782f:51e	ICM	166 Time	Exceeded	(hop	limit	exceeded	in	tran	l
	130.023861237	2001:4dd0:a000	2a00:20:b004:2c11:2a1	L0:782f:51e	ICM	166 Time	Exceeded	(hop	limit	exceeded	in	tran	l
	140.023861269	2001:4dd0:a000	2a00:20:b004:2c11:2a1	L0:782f:51e	ICM	166 Time	Exceeded	(hop	limit	exceeded	in	tran	l
	150.027820090	2001:4dd0:a000	2a00:20:b004:2c11:2a1	L0:782f:51e	ICM	166 Time	Exceeded	(hop	limit	exceeded	in	tran	l
	160.027820136	2001:4dd0:a000	2a00:20:b004:2c11:2a1	l0:782f:51e	ICM	166 Time	Exceeded	(hop	limit	exceeded	in	tran	
	170.032142221	2001:4dd0:a000	2a00:20:b004:2c11:2a1	l0:782f:51e	ICM	166 Time	Exceeded	(hop	limit	exceeded	in	tran	l
	180.033449496	2001:4dd0:a000	2a00:20:b004:2c11:2a1	L0:782f:51e	ICM	166 Time	Exceeded	(hop	limit	exceeded	in	tran	l
	190.040326659	2001:4dd0:a000	2a00:20:b004:2c11:2a1	L0:782f:51e	ICM	166 Time	Exceeded	(hop	limit	exceeded	in	tran_	l
	200.040326921	2001:4dd0:a000	2a00:20:b004:2c11:2a1	L0:782f:51e	ICM	166 Time	Exceeded	(hop	limit	exceeded	in	tran	I
	210.043376058	2001:4dd0:a000	2a00:20:b004:2c11:2a1	L0:782f:51e	ICM	166 Time	Exceeded	(hop	limit	exceeded	in	tran	
	220 042276114	0004 4 1 10 000	0 00 00 004 0 44 0 4	0 7005 54	TCM	1 C C T :	Free and a d	1	12		÷	4	4

📕 cap	ture-icmp-flood.pcapng										-	o x
<u>D</u> atei	Bearbeiten Ansicht Navigation	Aufzeichnen Analyse Statistiken	Telephonie <u>W</u> ireless <u>T</u> ools	<u>H</u> ilfe								
Anze	igefilter anwenden <ctrl-></ctrl->											
No.	Time	Source	Destination		Protocol	Length Info						
	10.000000000	2001:4dd0:a000.	_2a00:20:b004:2	2c11:2a10:782f:51e.	. ICM	166 Time	Exceeded	(hop	limit	exceeded	in	tran
	20.000000135	2001:4dd0:a000.	2a00:20:b004:2	2c11:2a10:782f:51e.	. ICM	166 Time	Exceeded	(hop	limit	exceeded	in	tran
	30.004207259	2001:4dd0:a000	2a00:20:b004:2	2c11:2a10:782f:51e.	ICM	166 Time	Exceeded	(hop	limit	exceeded	in	tran
	4 0 001207286	2001-1440-2000	2-00.JU. PO01.	0-11.0-10.780f.51a	тсм	166 Timo	Evenadad	(hon	limi+	avcoadad	in	±nan=
	5											an
	6	_	•			-						an
	7	Δ	single		ho	, trio	JJAP	2				an
	0		JIIgic				58	3				20
	0			e				_				an
	9	>250k r	enlies	from th	e 9	sam	e ro	UT	er.			an
	10)		an
	11											an
	12											an
	13											an
	14											an
	15											an
	16	/ 18/1 - 4 10.07 - 010.07.										an
	170 0301/02010	2001 • 1 dd0 • 2000	2-00.20.0001.	$2c_{11} \cdot 2a_{10} \cdot 782f \cdot 51c_{10}$	тсм	166 Time	Exceeded	(hon	limi+	exceeded	in	tran
	190 022142221	2001.400.000	2200.20.0004.2	11.2a10.7021.51c.		166 Time	Exceeded	(hop	1;;+	exceeded	111 10	than
	180.033449490			CII:Zal0:/82T:51e.		100 11me	Exceeded	(nop	11M1C	exceeded	111 •	tran
	190.040326659	2001:4000:a000.	2a00:20:0004:2	2C11:2a10:782+:51e.	. ICM	166 lime	Exceeded	(nop	limit	exceeded	in	tran
	200.040326921	2001:4dd0:a000.	2a00:20:b004:2	2c11:2a10:782f:51e.	. ICM	166 Time	Exceeded	(hop	limit	exceedded	in	tran
	210.043376058	2001:4dd0:a000.	2a00:20:b004:2	c11:2a10:782f:51e.	. ICM	166 Time	Exceeded	(hop	limit	exceeded	in	tran
	220 012376111	2001.1440.000	2-00.20.0001.	$10-11 \cdot 2-10 \cdot 782 + 510$	TCM	166 Timo	Excooded	(hon	limi+	ovcoodod	in	tran

🚄 capture-icmp-flood.pcapng										-	o ×	
Datei Bearbeiten Ansicht Navigation Aufzeichnen Analyse Statistiken Telephonie Wireless Tools Hilfe												
Anzeigefilter anwenden <ctrl-></ctrl->												
		Destination		Protocol		Twoodod	(hen	1:	avaaadad	1	tuon	
10.00000000	2001:4000:2000.	2a00:20:0004:2C11	.:2a10:782f:51e	1CM	166 lime	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	+ŋan 💳	
5											an	
6	_	• • •			_ •						an	
7	Δ	single (MP Fc	ho) tria	JJAP	5				an	
,						58	5				20	
0	AFAL						-		.		an	
9	>250K r	enlies f	rom fh	e 9	sam	e ro	UIT	er.	*		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	±	turan	
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

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

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

on Thursda

How many /48 allow for TTL Exceeded amplifications?

November 2024

7.4M /48 subnets

April 2025

10M (+35%) /48 subnets

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 routers! b8:cafe::1