TECHNISCHE UNIVERSITÄT DRESDEN

HAW HAMBURG

DRESDEN concept

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

Amplification through IPv6 routing loops

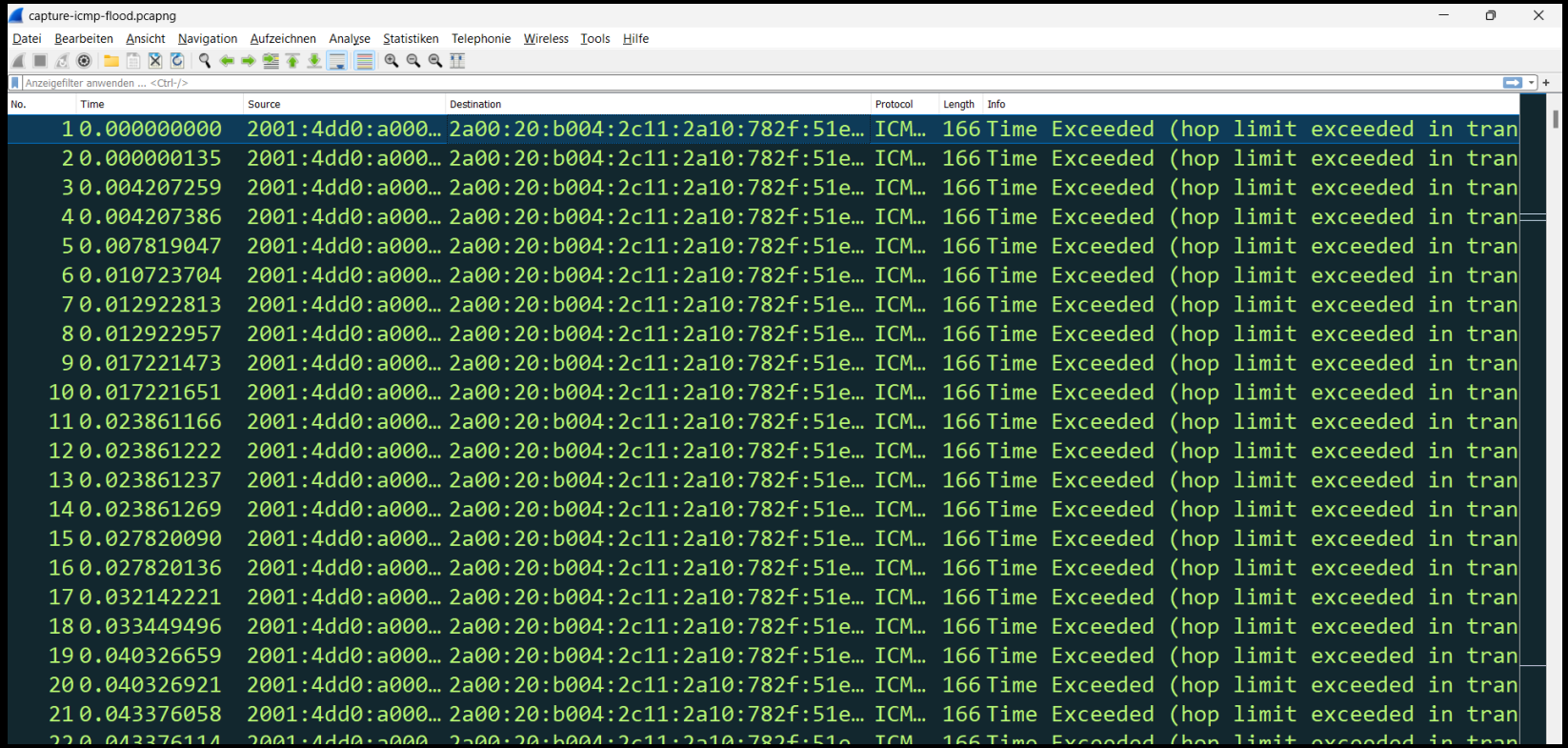
A call to fix router configurations.

RIPE 90, Lisbon, Portugal // May 2025

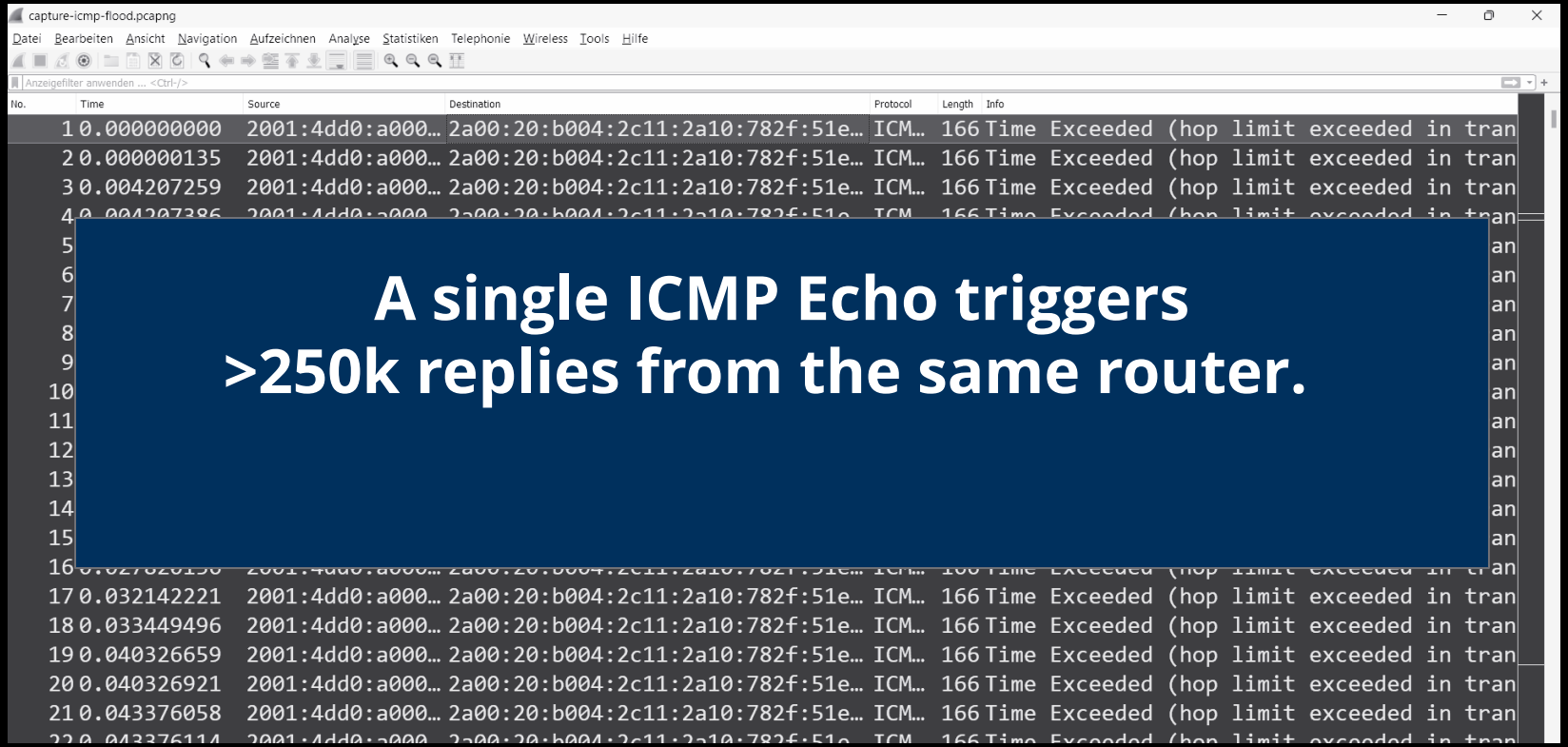
Contact: maynard.koch@tu-dresden.de

```
ping -c 1 <destination IP address>
```

ping -c 1 <destination IP address>

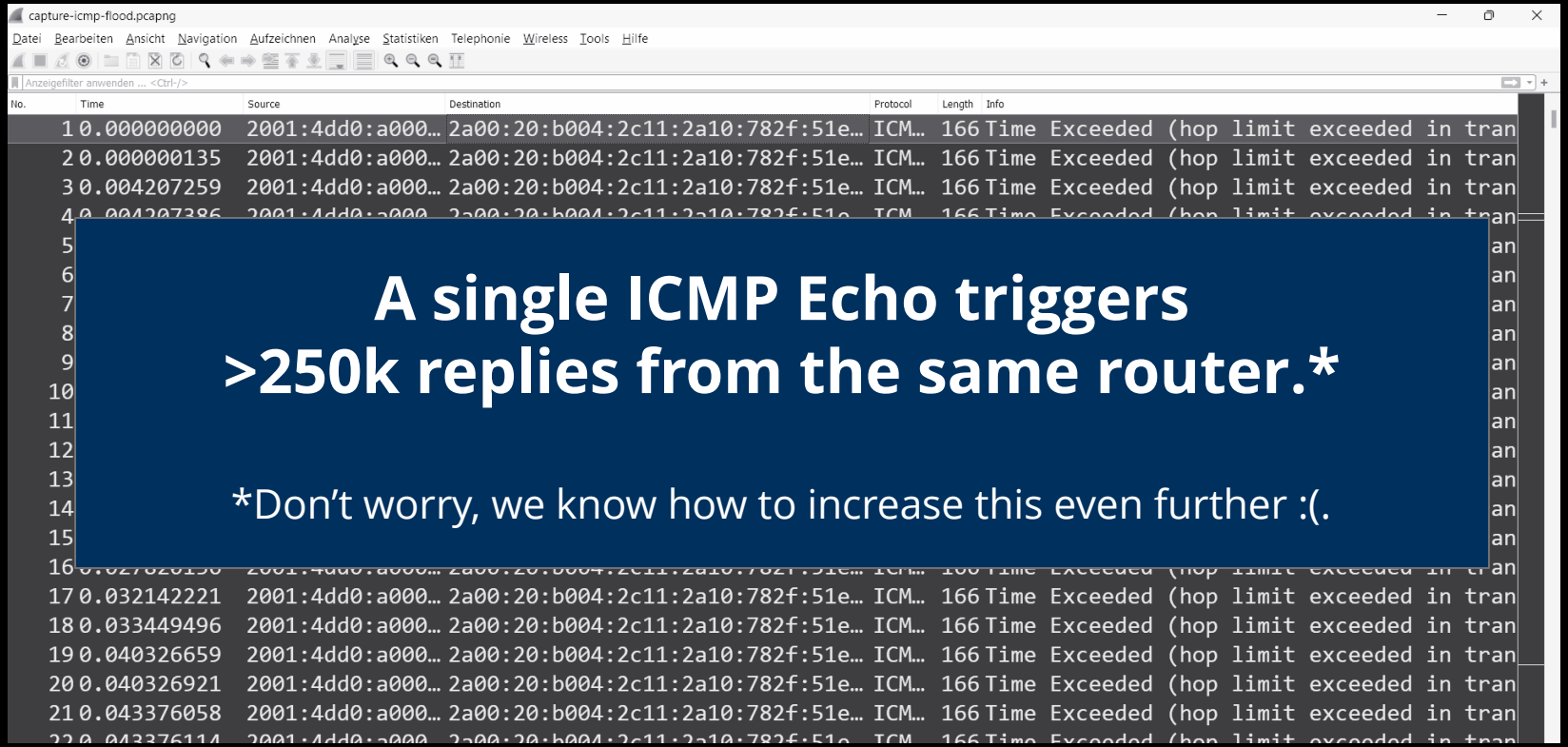


ping -c 1 <destination IP address>



A single ICMP Echo triggers
>250k replies from the same router.

ping -c 1 <destination IP address>



A single ICMP Echo triggers
>250k replies from the same router.*

*Don’t worry, we know how to increase this even further :(.

Why?

Routing Loops

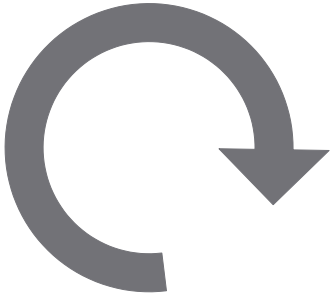
[Misconfiguration]

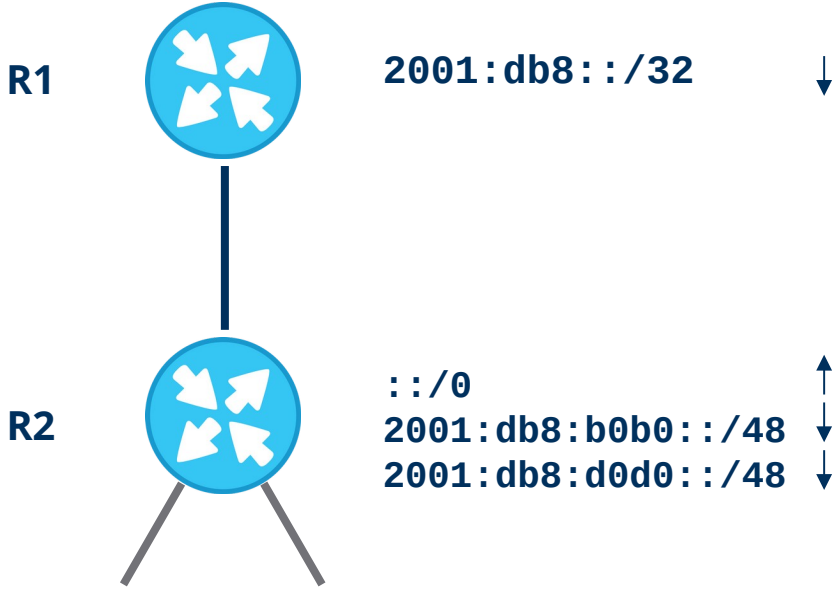
TTL Exceeded Amplification

[Software Bug]

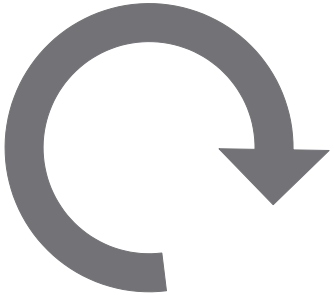
What is a routing loop?

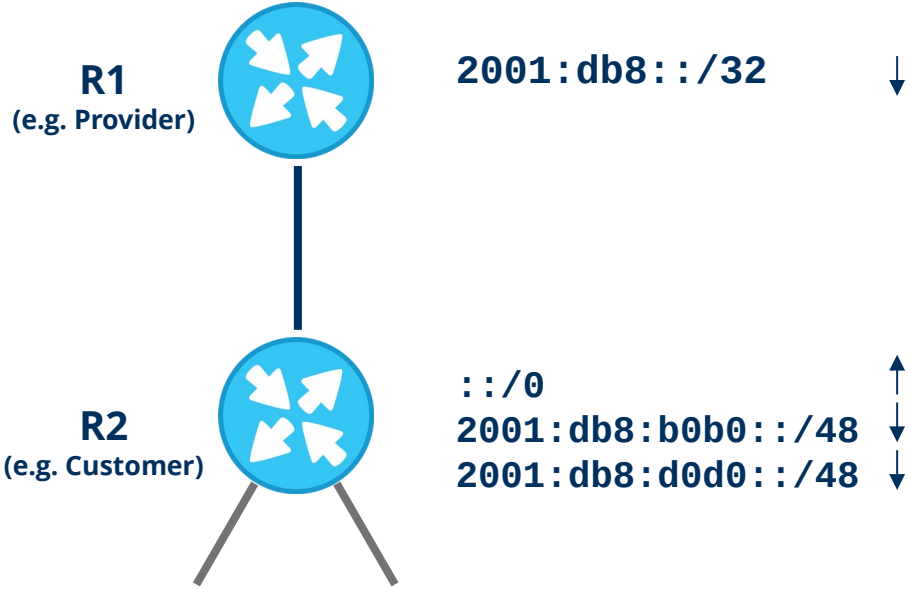
What is a routing loop?



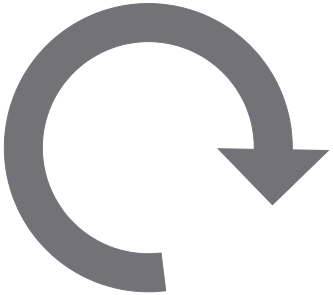


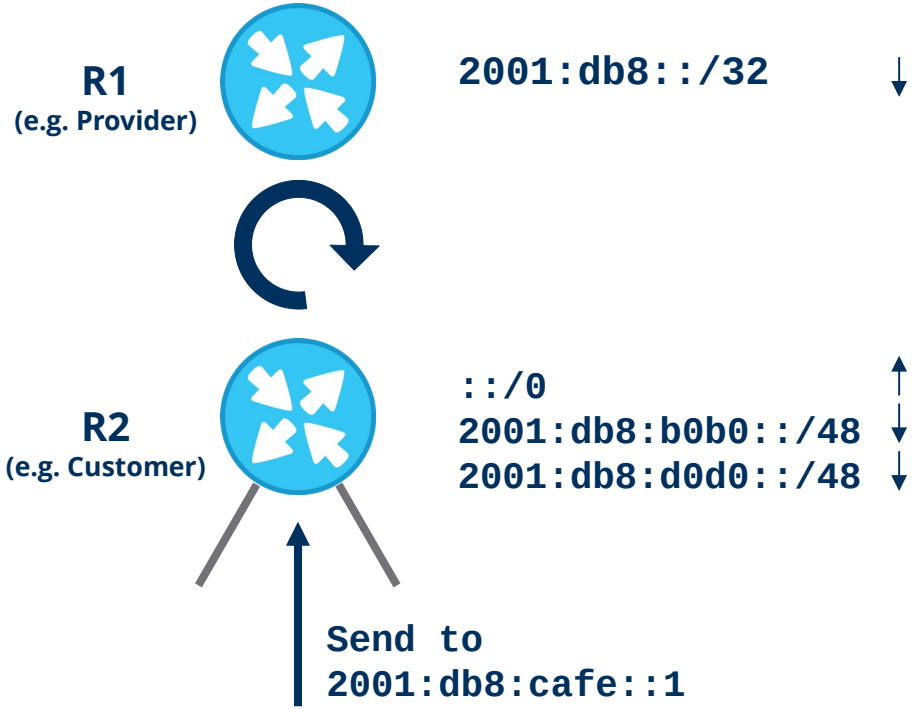
What is a routing loop?





What is a routing loop?

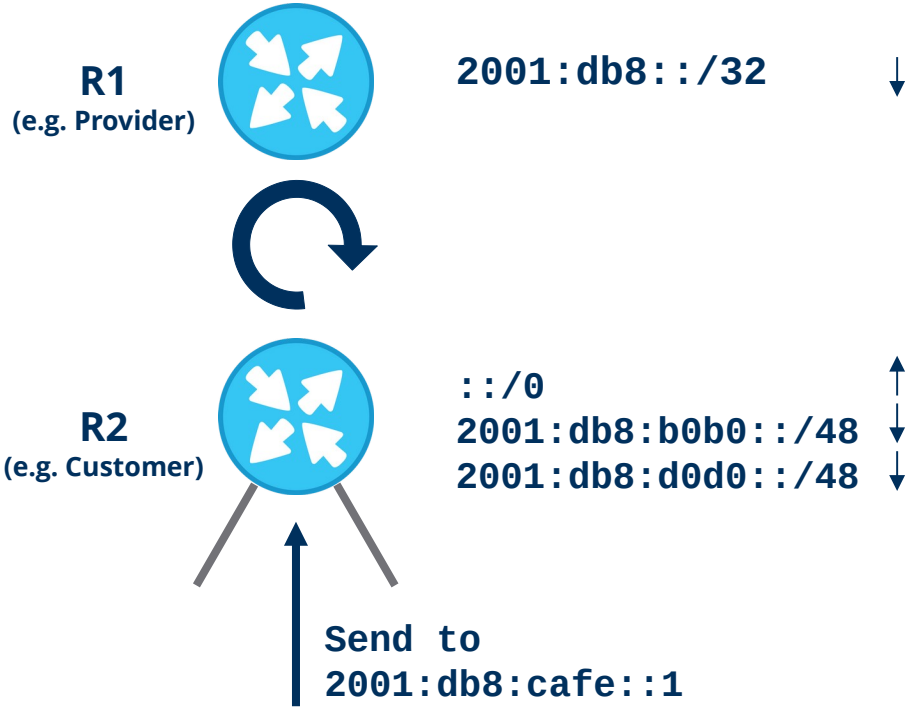




Common deployment? Yes!

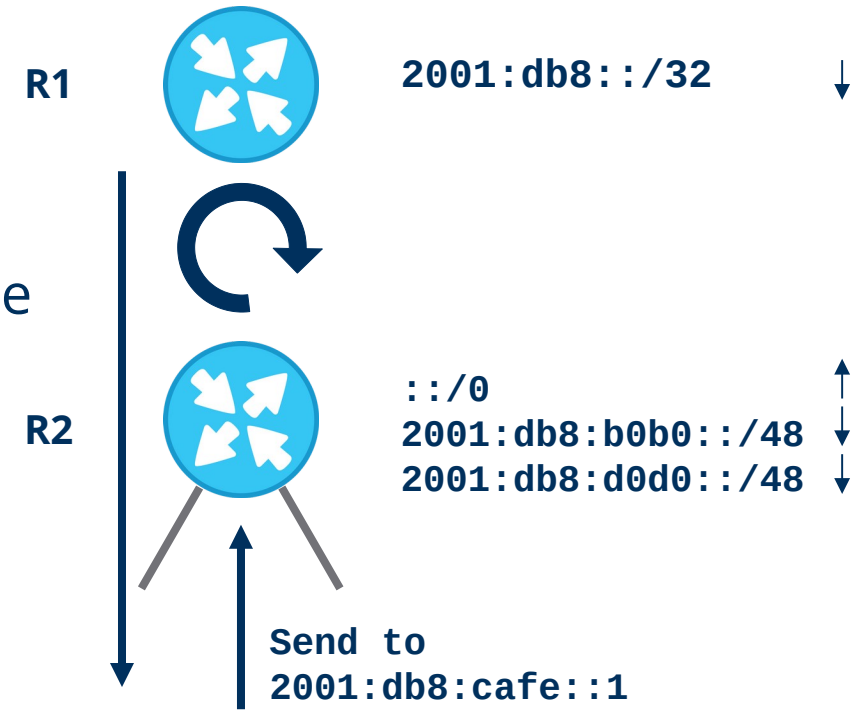
Those deployments **easily occur when providers assign PA address space** to customers.

... and there is one more problem.



A loop ultimately leads to an `ICMP TTL Exceeded`

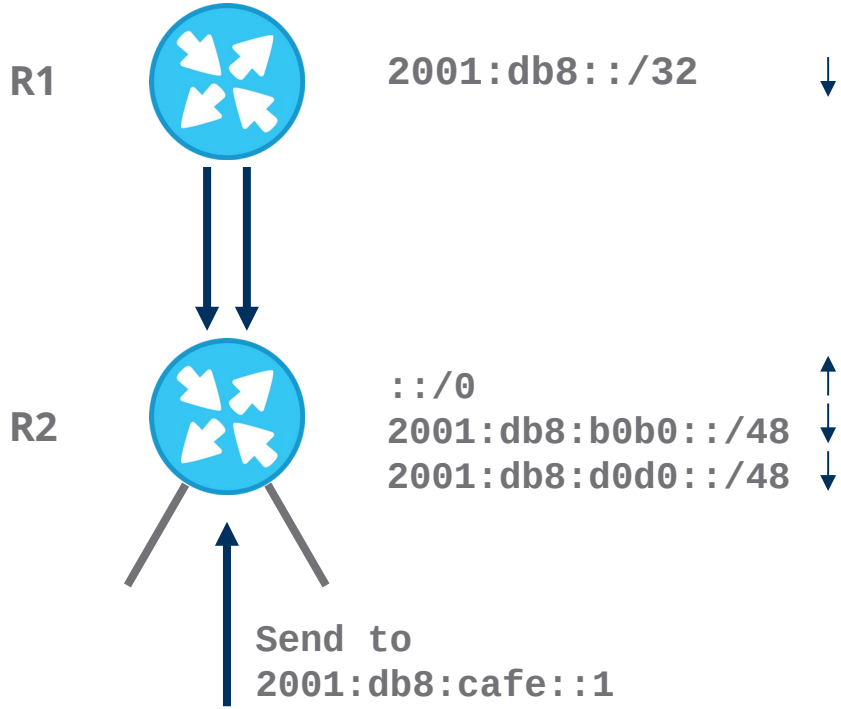
`ICMP TTL Exceeded`
send to the source of the original trigger.



A loop ultimately leads to an `ICMP TTL Exceeded`

In our case, not a single message but >250k. Why?

A router bug leads to duplication of an ICMP Echo.

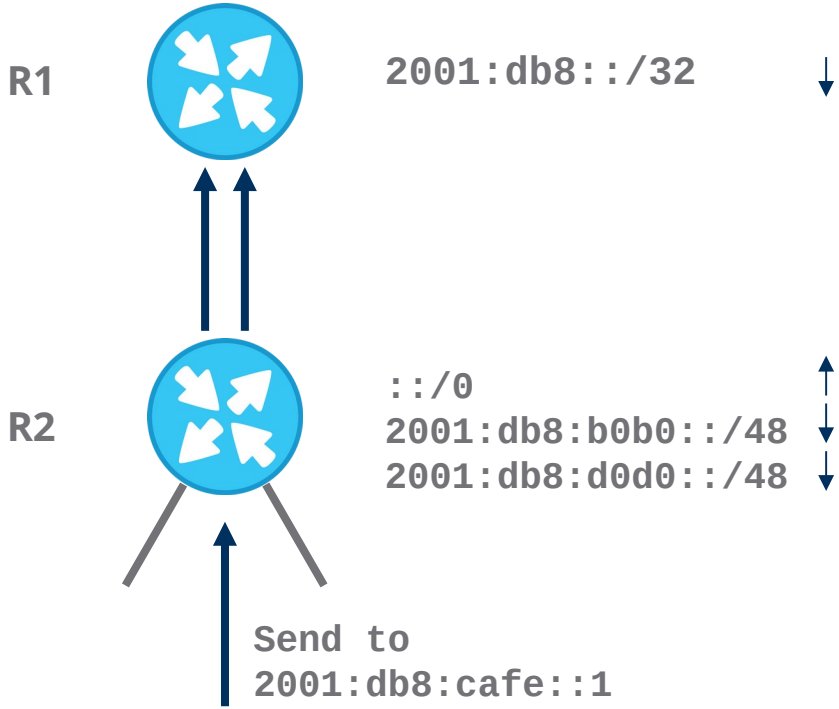


A loop ultimately leads to an `ICMP TTL Exceeded`

In our case, not a single message but >250k. Why?

A router bug leads to duplication of an ICMP Echo.

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

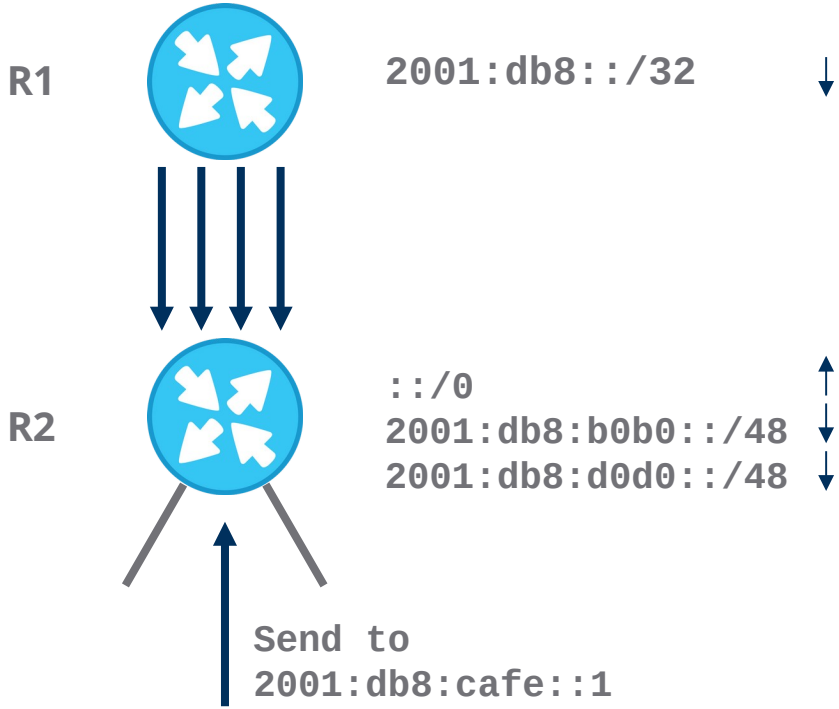


A loop ultimately leads to an `ICMP TTL Exceeded`

In our case, not a single message but >250k. Why?

A router bug leads to duplication of an ICMP Echo.

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



A loop ultimately leads to an `ICMP TTL Exceeded`

In our case, not a single message but >250k. Why?

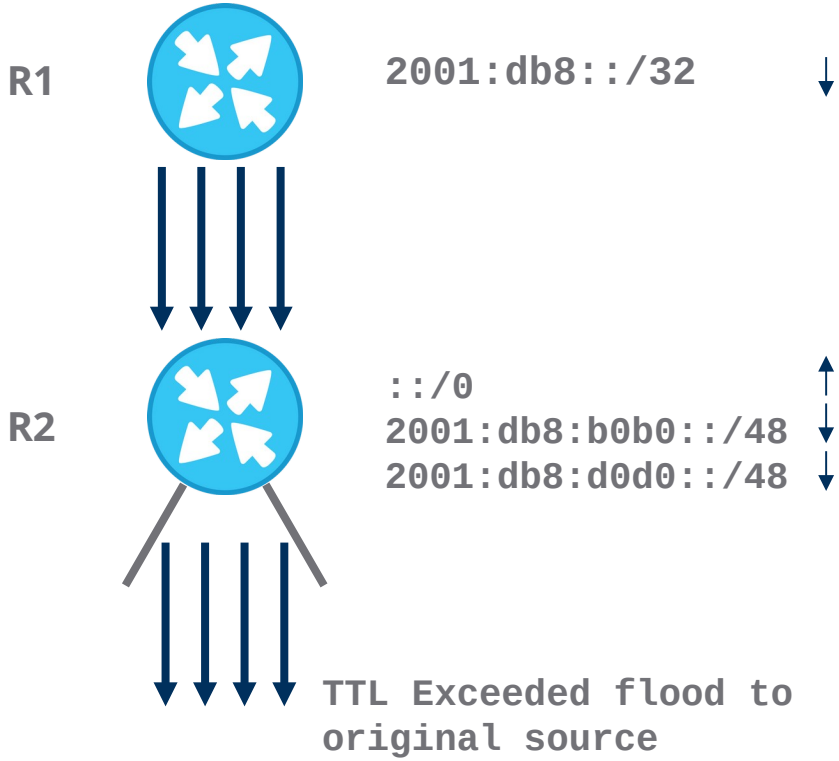
A router bug leads to duplication of an ICMP Echo.

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

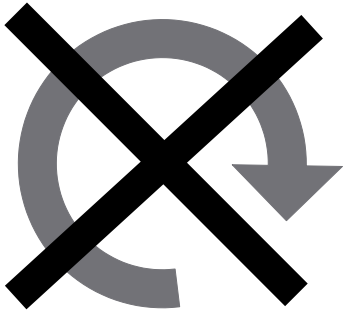
Each duplicate triggers an individual TTL Exceeded.

Amplification at its best!

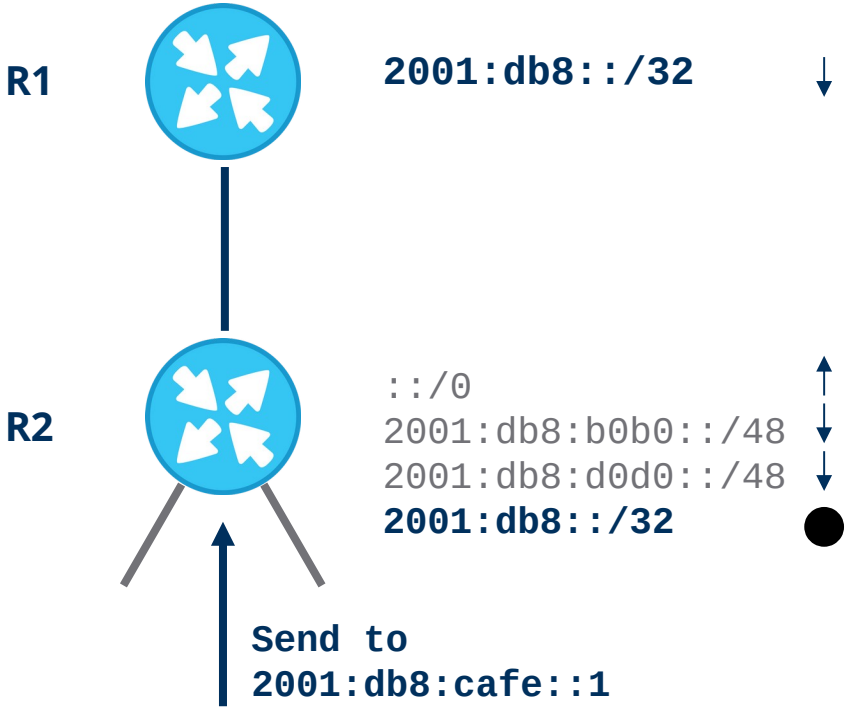
[Confirmed by Juniper.]



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



Please, stop this nonsense!



How many IPv6 routing loops occur?

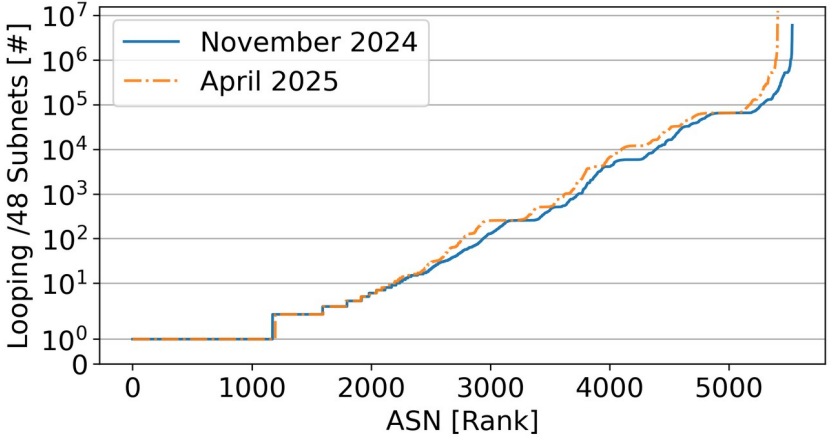
November 2024

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?

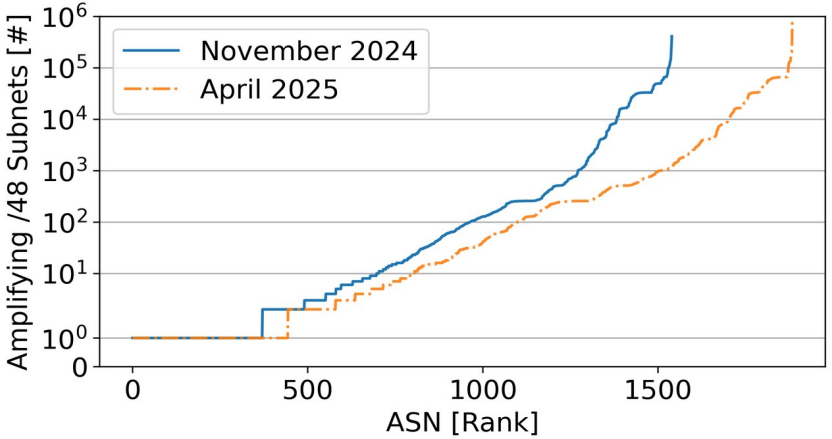
November 2024

7.4M /48 subnets

April 2025

10M (+35%) /48 subnets

How many /48 allow for TTL Exceeded amplifications?

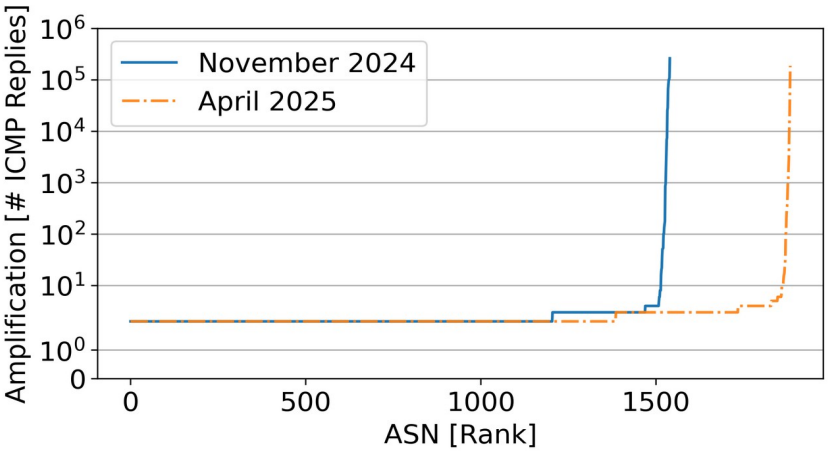


1885 ASes in 102 countries show amplifying router behavior.

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

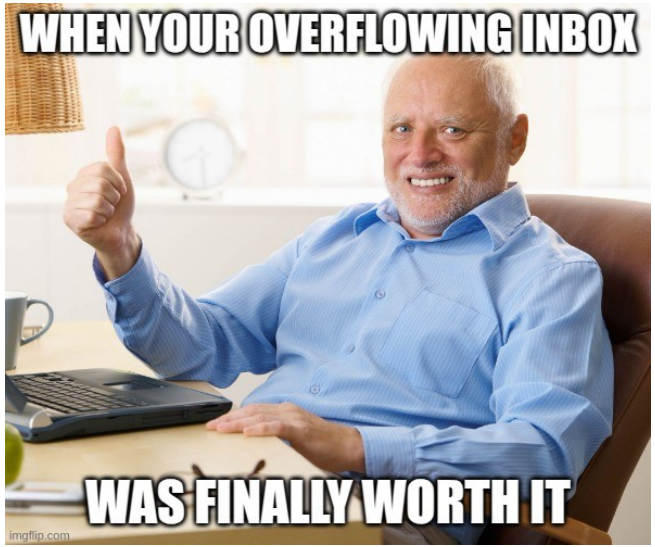
Thank you for your support!

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.

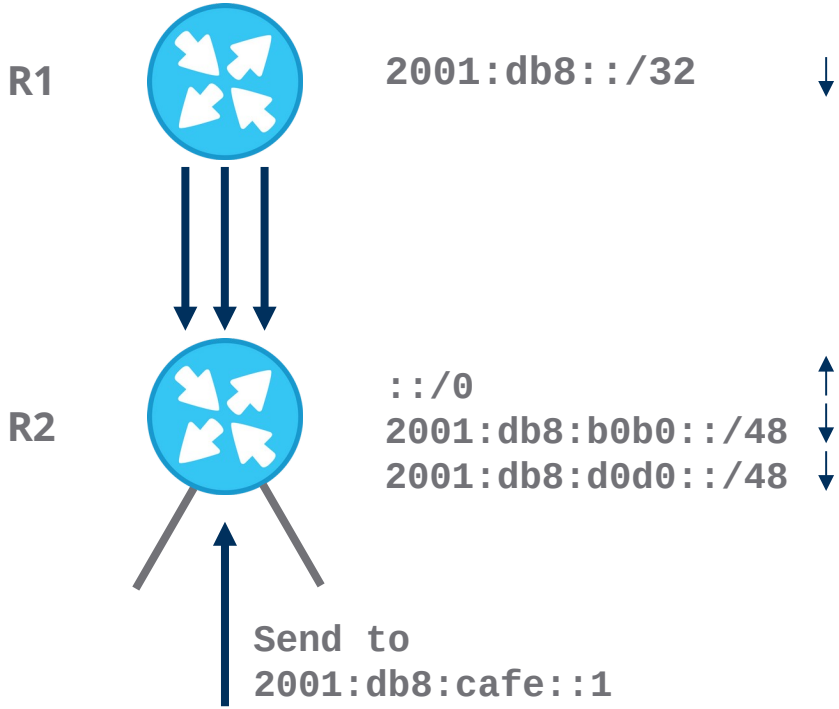
Backup

A loop ultimately leads to an `ICMP TTL Exceeded`

In our case not a single message but >250k.

The higher your IP TTL value, the higher the amplification.

We confirmed exponential growth for some few routers!



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	Type	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 ≥10 and max. amplification is **36.**