TECHNISCHE UNIVERSITÄT DRESDEN

HAW HAMBURG

DRESDEN concept

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

Amplification through IPv6 routing loops

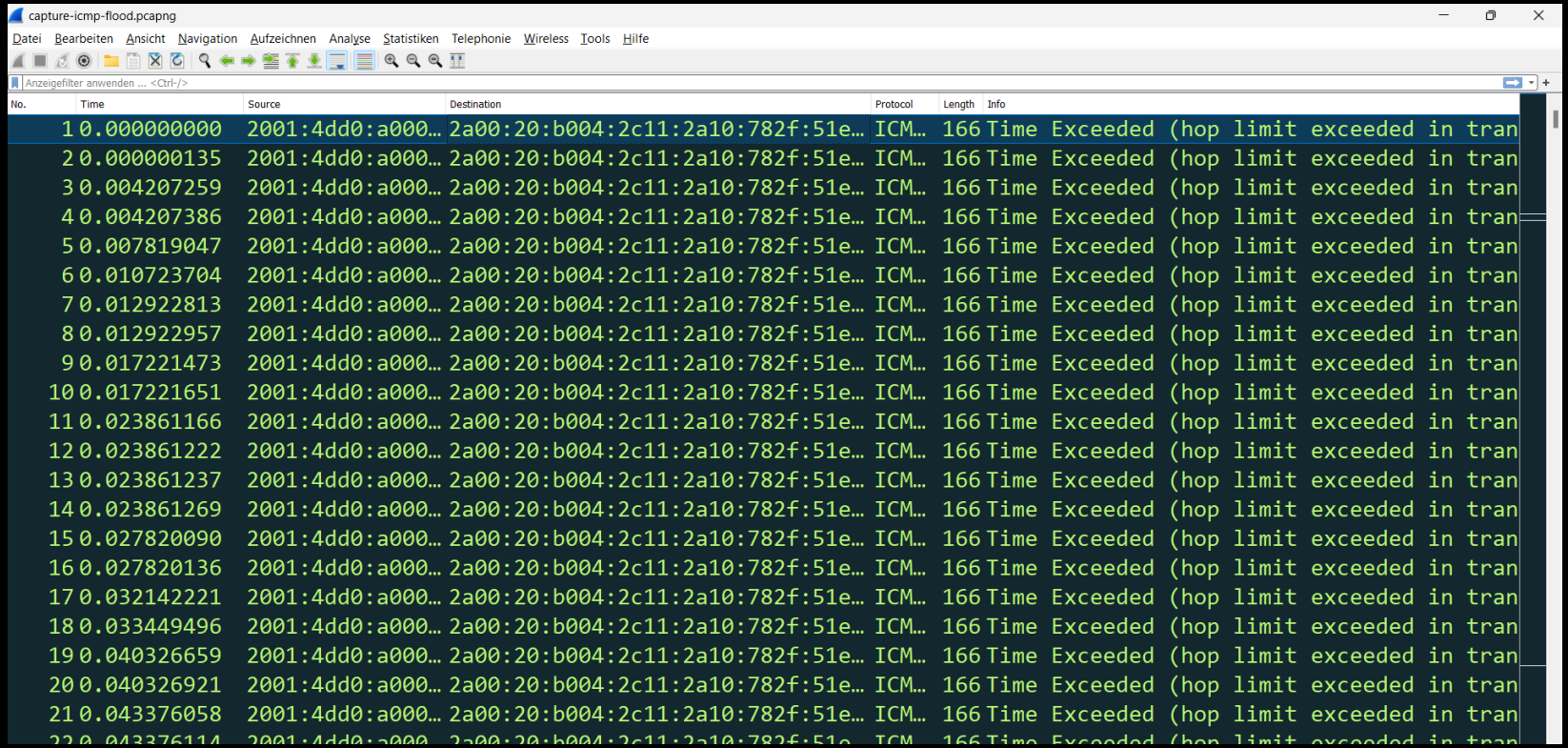
A call to fix router configurations.

RIPE 90, Lisbon, Portugal // May 2025

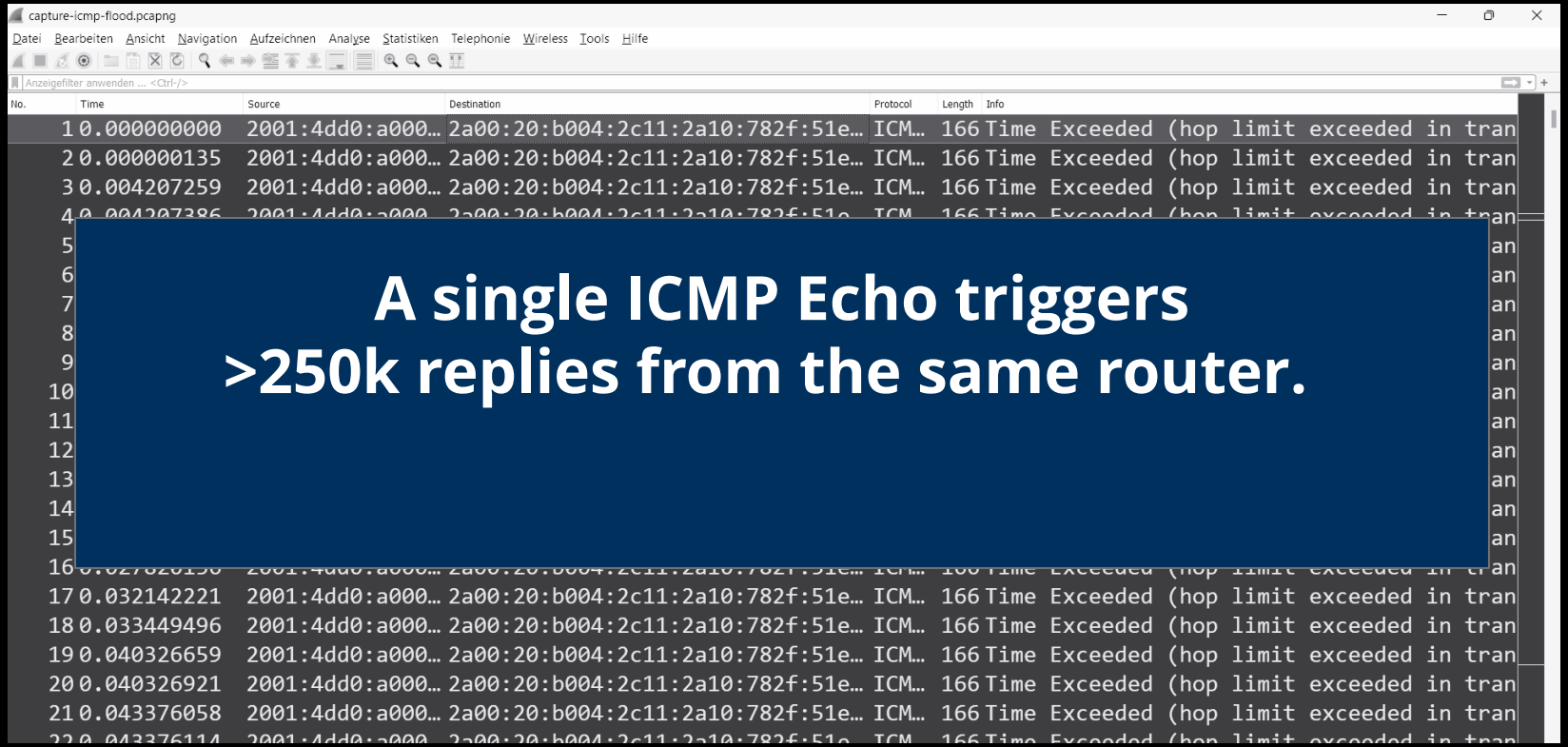
Contact: maynard.koch@tu-dresden.de

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

ping -c 1 <destination IP address>

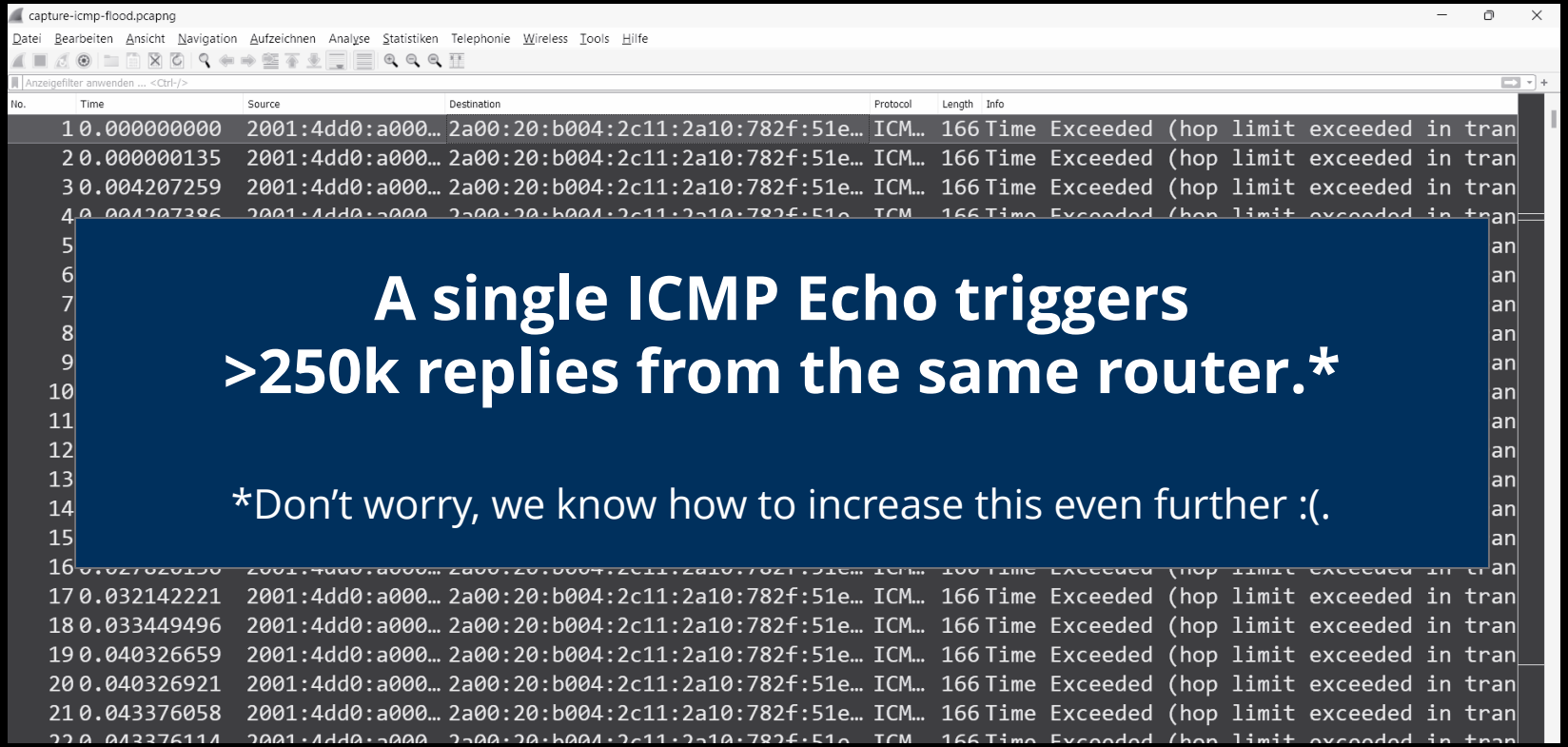


ping -c 1 <destination IP address>



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

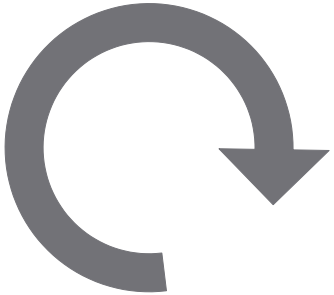
[Misconfiguration]

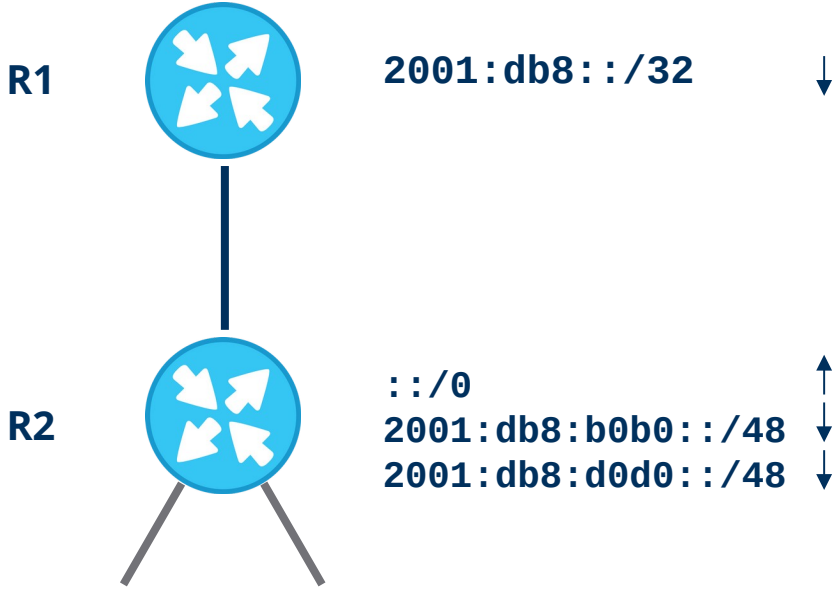
TTL Exceeded Amplification

[Software Bug]

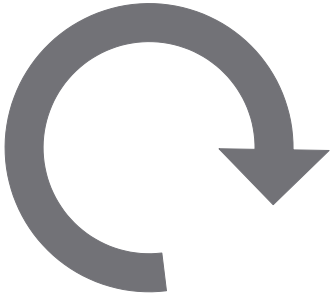
What is a routing loop?

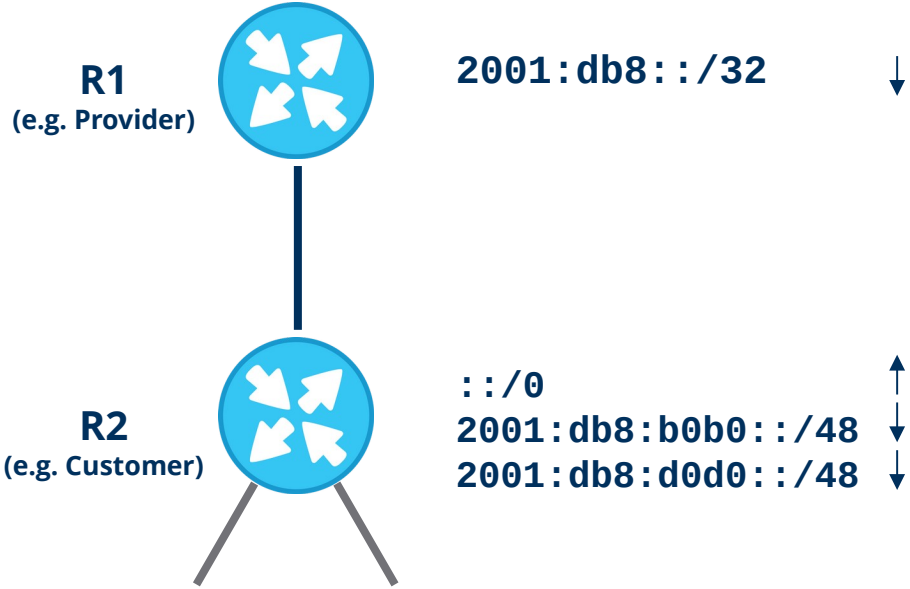
What is a routing loop?



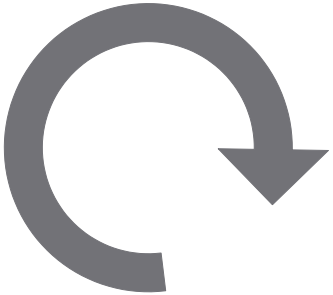


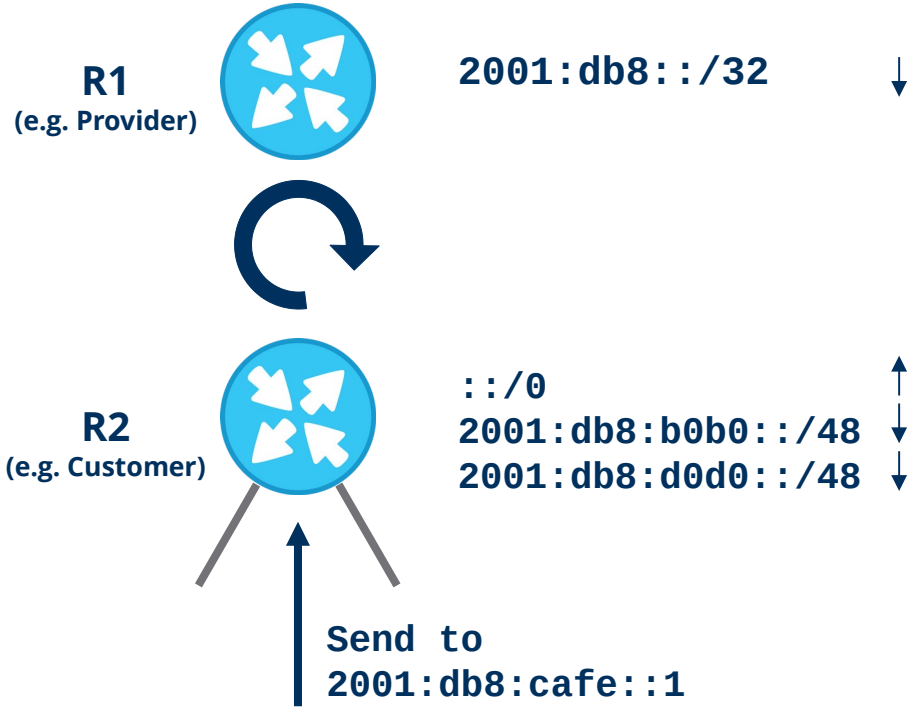
What is a routing loop?





What is a routing loop?

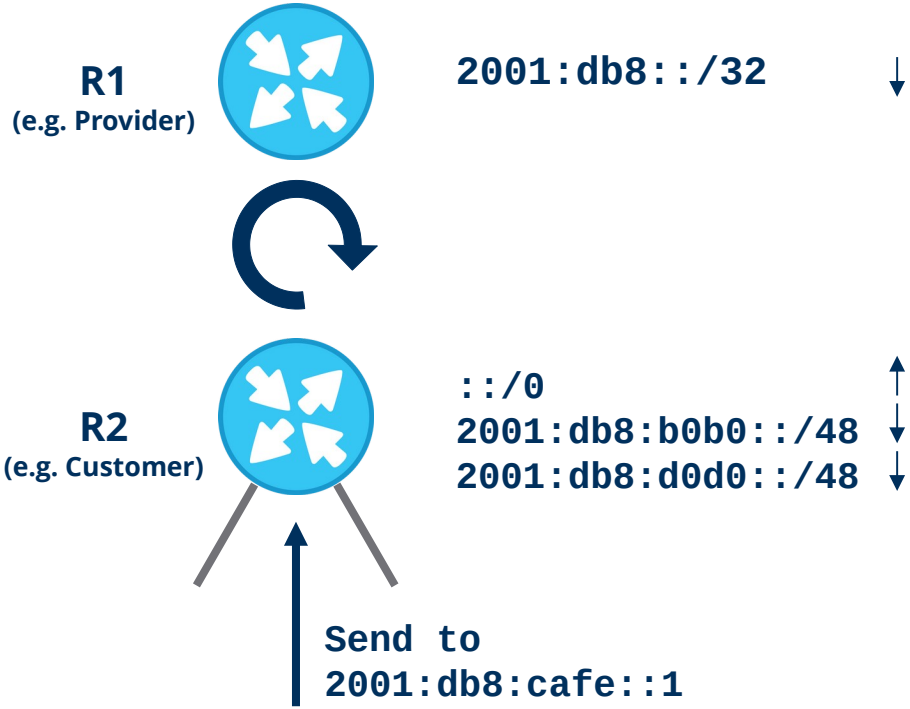




Common deployment? Yes!

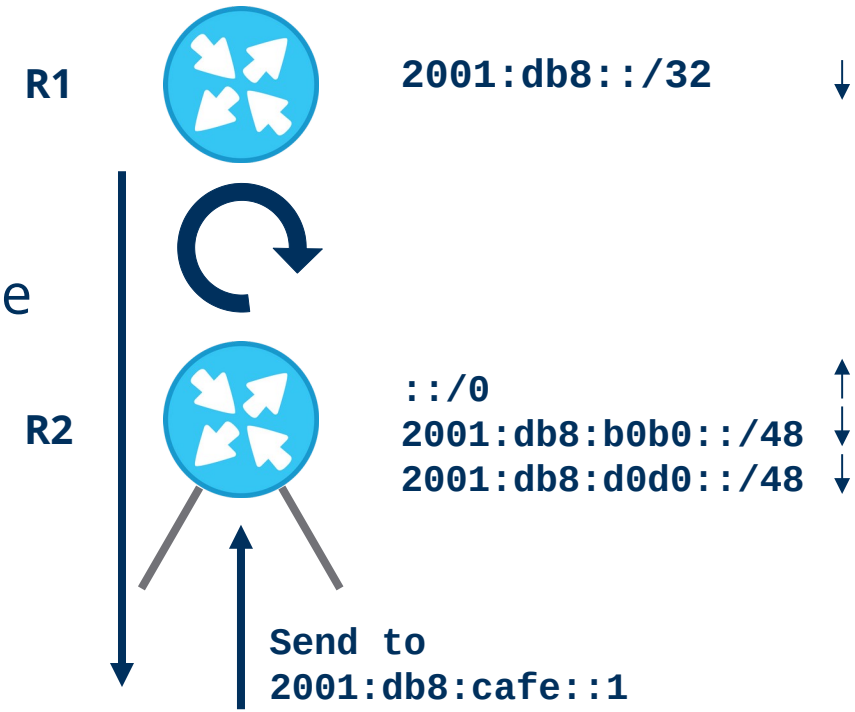
Those deployments **easily occur when providers assign PA address space** to customers.

... and there is one more problem.



A loop ultimately leads to an `ICMP TTL Exceeded`

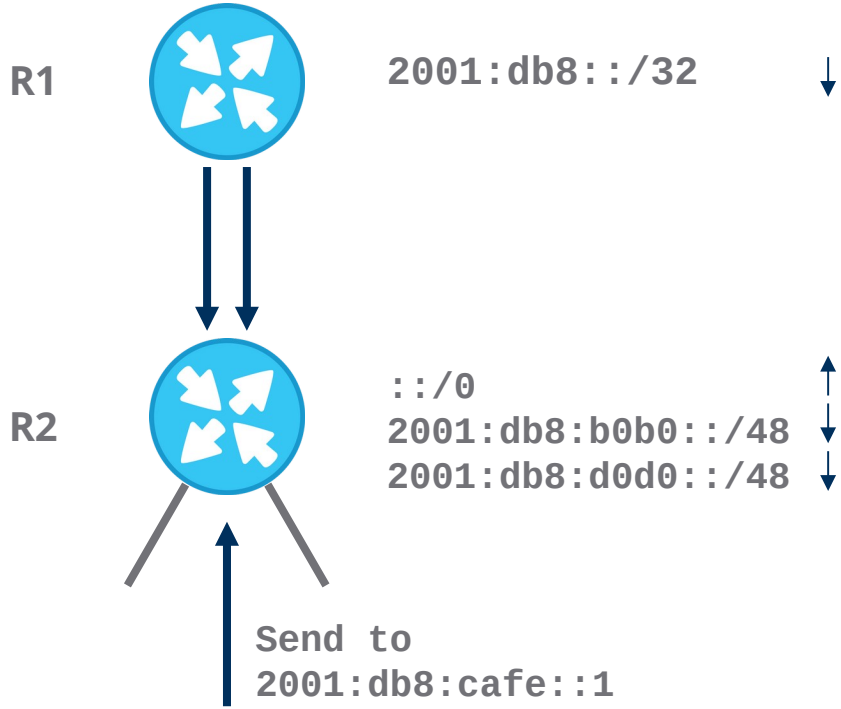
`ICMP TTL Exceeded`
send to the source of the original trigger.



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.

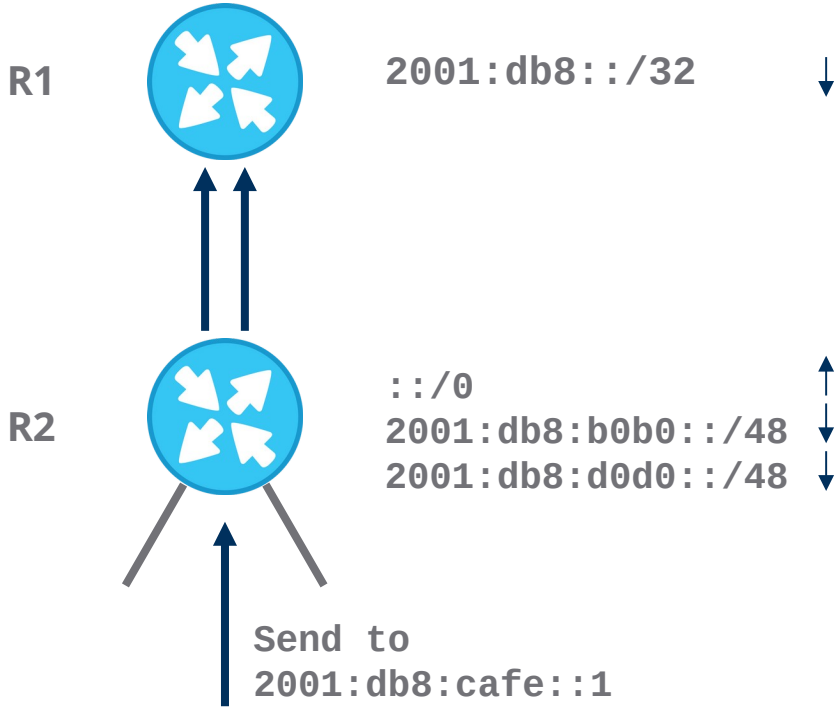


A loop ultimately leads to an `ICMP TTL Exceeded`

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.

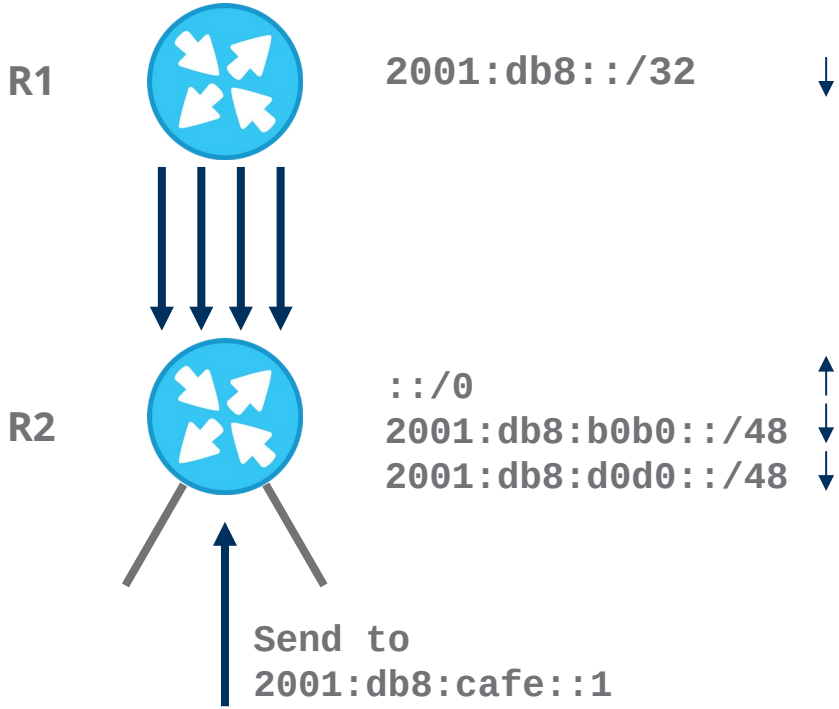


A loop ultimately leads to an `ICMP TTL Exceeded`

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?

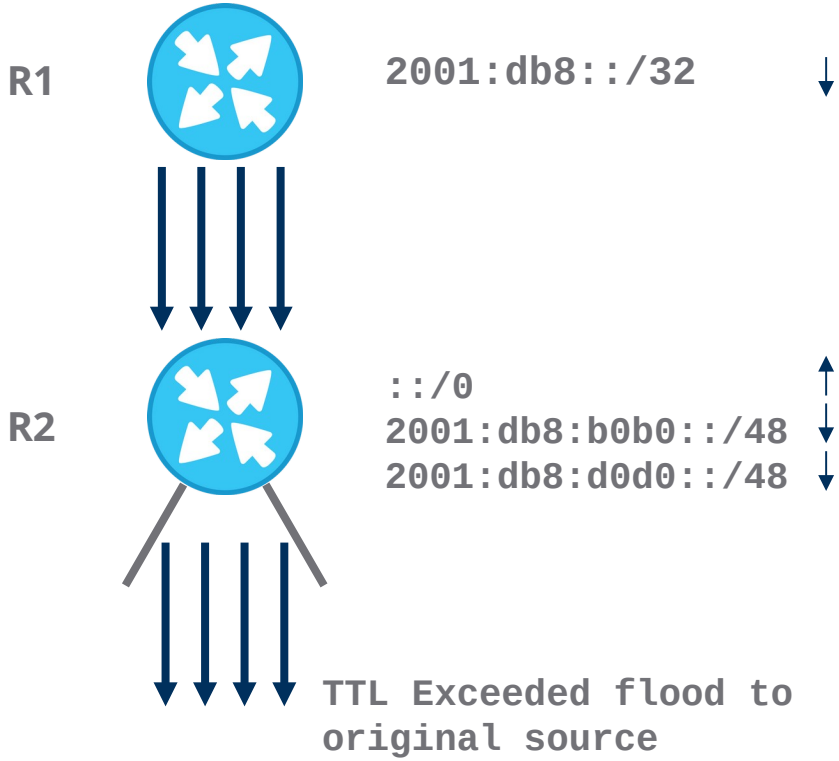
A router bug leads to duplication of an ICMP Echo.

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

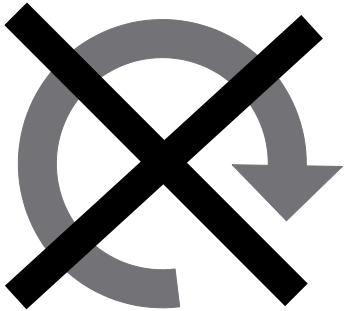
Each duplicate triggers an individual TTL Exceeded.

Amplification at its best!

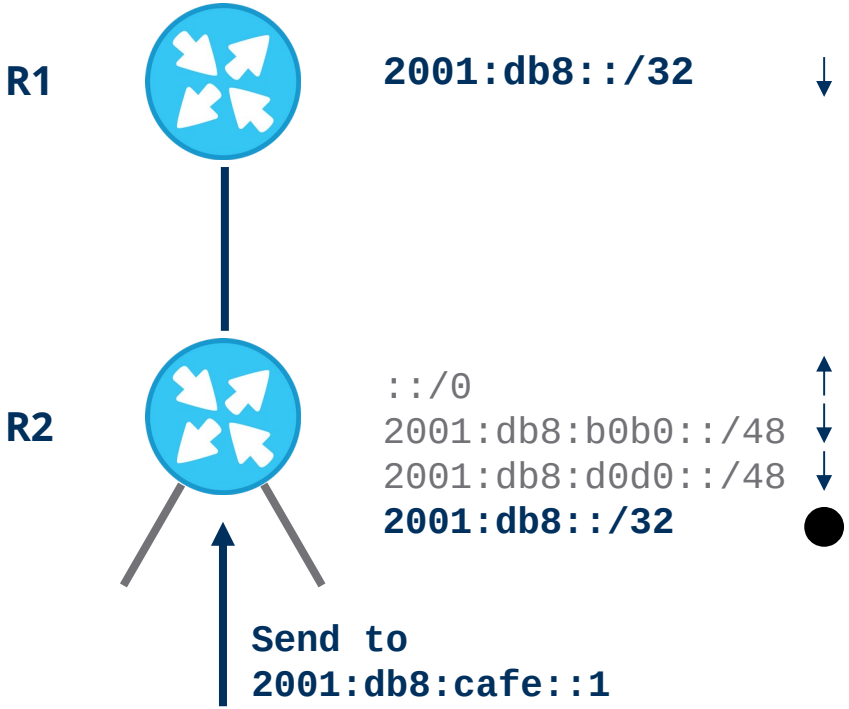
[Confirmed by Juniper.]



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

Interested in more details? Join the IPv6 Working Group session on Thursday morning!

How many /48 allow for TTL Exceeded amplifications?

November 2024

7.4M /48 subnets

April 2025

10M (+35%) /48 subnets

Interested in more details? Join the IPv6 Working Group session on Thursday morning!

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 routers!