Dresden University of Technology
NETSCOUT
HAW HAMBURG

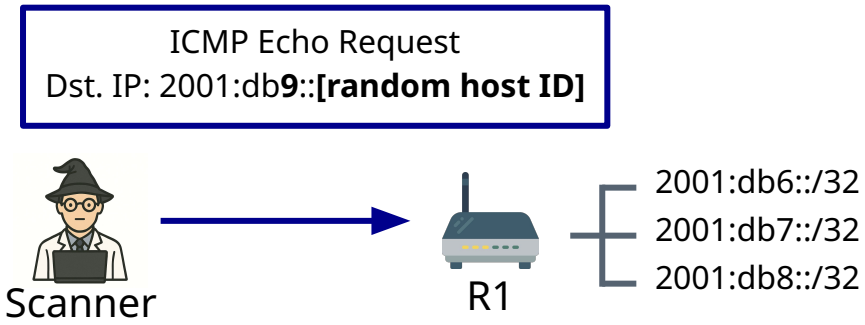
Maynard Koch, Raphael Hiesgen, Marcin Nawrocki, Thomas C. Schmidt, Matthias Wählisch

Scanning the IPv6 Internet Using Subnet-Router Anycast Probing

ACM CoNEXT, Hong Kong // December 1-4, 2025

A common approach to analyze network topology

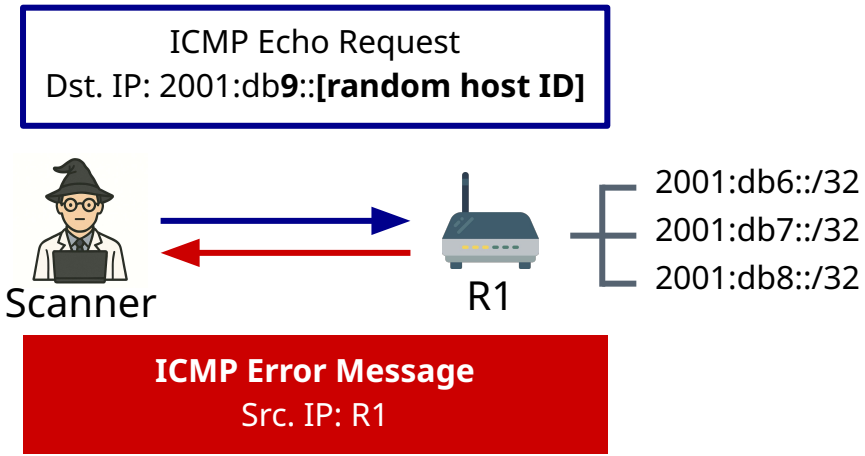
Send out probes to random targets and analyze ICMP error messages



Probing technique	**Router observed**
Random	

A common approach to analyze network topology

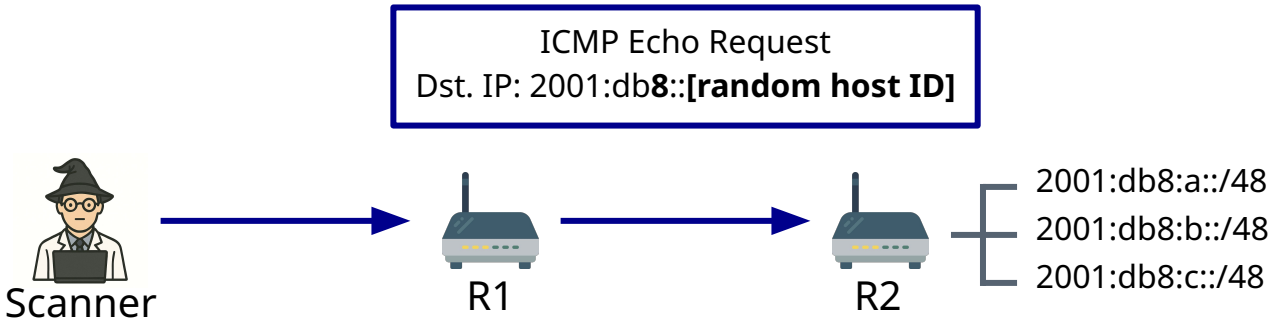
Send out probes to random targets and analyze ICMP error messages



Probing technique	Router observed
Random	✓

A common approach to analyze network topology

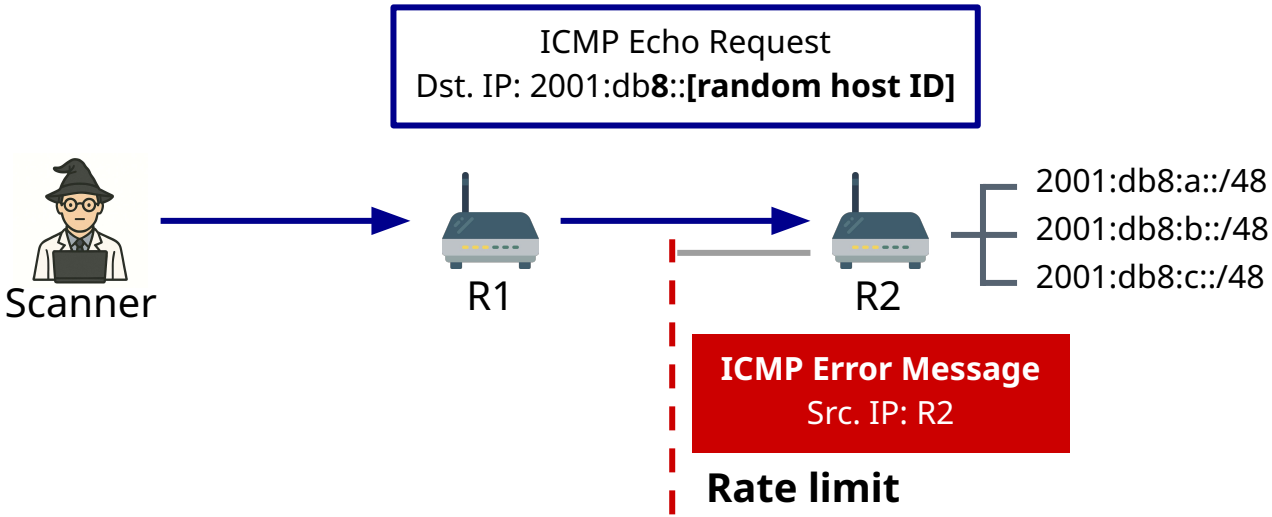
Send out probes to random targets and analyze ICMP error messages



Probing technique	Router observed
Random	✓

A common approach to analyze network topology

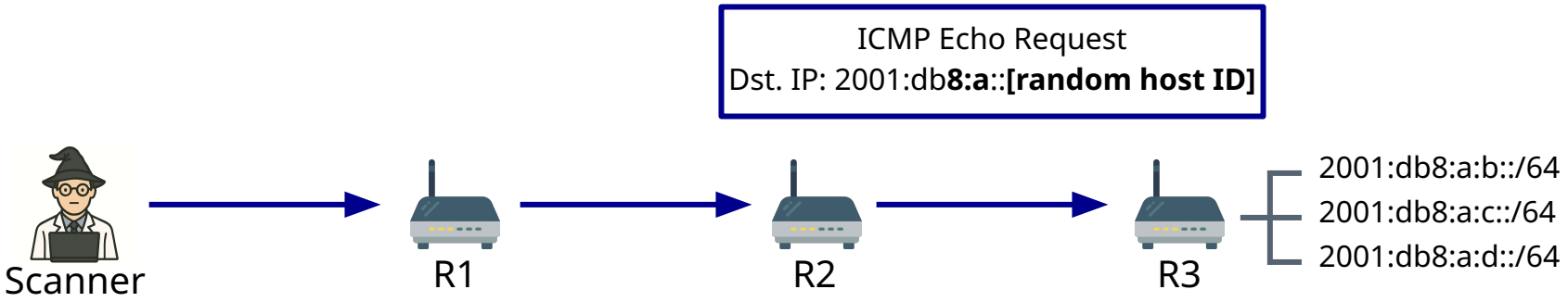
Send out probes to random targets and analyze ICMP error messages



Probing technique	Router observed	
Random	✓	✗

A common approach to analyze network topology

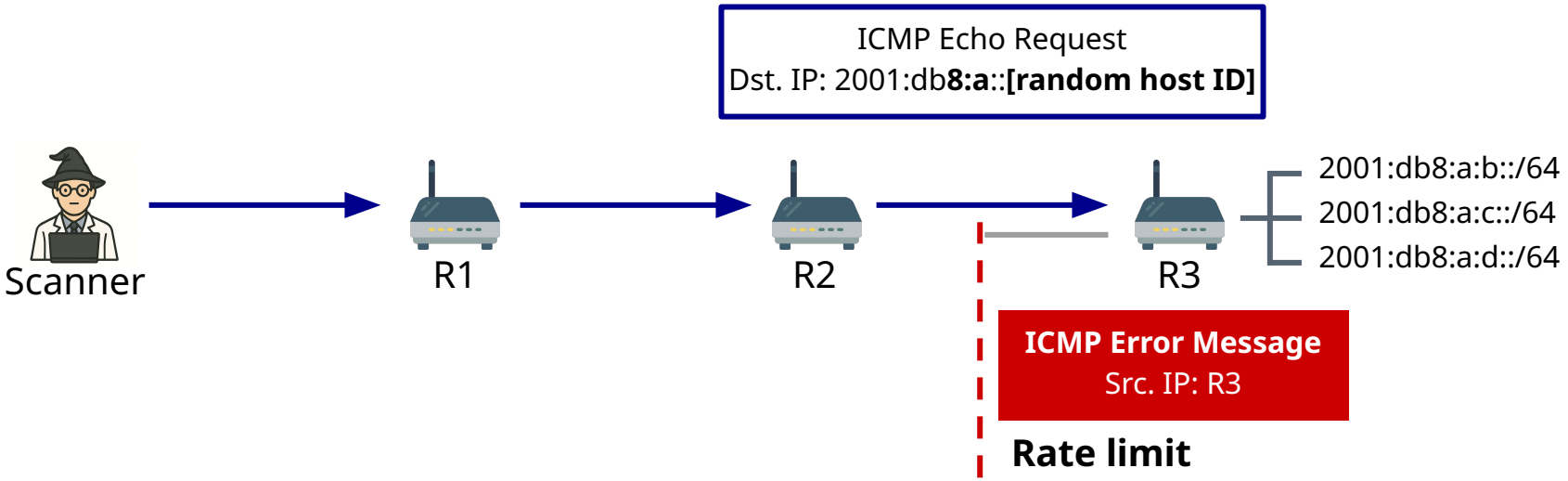
Send out probes to random targets and analyze ICMP error messages



Probing technique	Router observed	
Random	✓	✗

A common approach to analyze network topology

Send out probes to random targets and analyze ICMP error messages



Probing technique	Router observed		
Random	✓	✗	✗

A common approach to analyze network topology

Send out probes to random targets and analyze ICMP error messages

ICMP Echo Request
Dst. IP: 2001:db8:a::**[random host ID]**

Can we improve common probing methods to elicit responses from more router IP addresses?

ICMP Error Message
Src. IP: R3

Rate limit

Probing technique	Router observed		
Random	✓	✗	✗

Subnet-Router Anycast (SRA) probing
Trigger ICMP Echo replies instead of error messages

RFC 1884 (IPv6 addressing architecture):

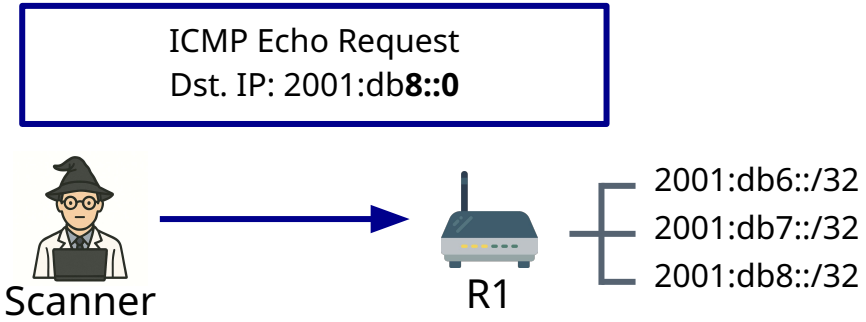
> 2.5.1 Required Anycast Address
>
> The Subnet-Router anycast address is predefined. It's format is as follows:
>
> | n bits | 128-n bits |
> |---|---|
> | subnet prefix | 00000000000000 |

Routers with interfaces to the corresponding subnet are **required** to reply!

Subnet-Router Anycast (SRA) probing
Trigger ICMP Echo replies instead of error messages

RFC 1884 (IPv6 addressing architecture):

> 2.5.1 Required Anycast Address
>
> The Subnet-Router anycast address is predefined. It's format is as follows:
>
> | n bits | 128-n bits |
> |---|---|
> | subnet prefix | 00000000000000 |



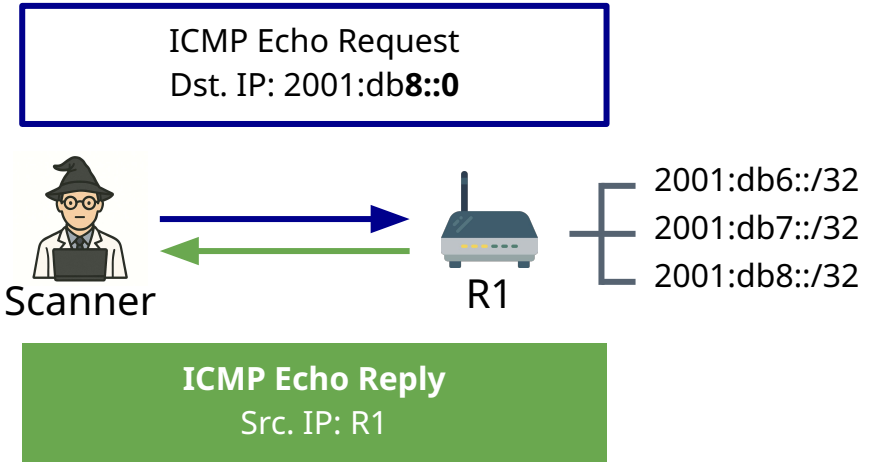
Routers with interfaces to the corresponding subnet are **required** to reply!

Subnet-Router Anycast (SRA) probing
Trigger ICMP Echo replies instead of error messages

RFC 1884 (IPv6 addressing architecture):

> 2.5.1 Required Anycast Address
>
> The Subnet-Router anycast address is predefined. It's format is as follows:
>
> | n bits | 128-n bits |
> |---|---|
> | subnet prefix | 00000000000000 |

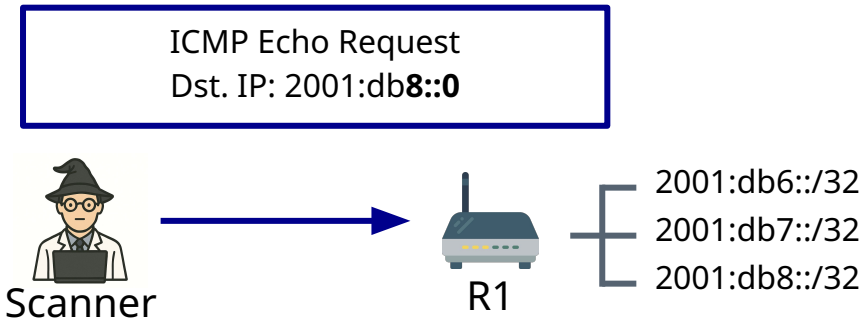
Routers with interfaces to the corresponding subnet are **required** to reply!



Unaffected by rate limiting of ICMP error messages!

Instead of probing a random address, we probe an SRA address

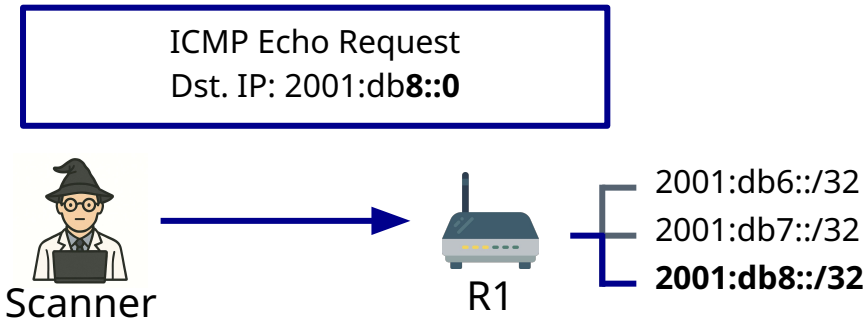
If a corresponding interface exists on that router, we trigger an Echo reply



Probing technique	Router observed
Random	✓ ✗ ✗
Subnet-Router Anycast	

Instead of probing a random address, we probe an SRA address

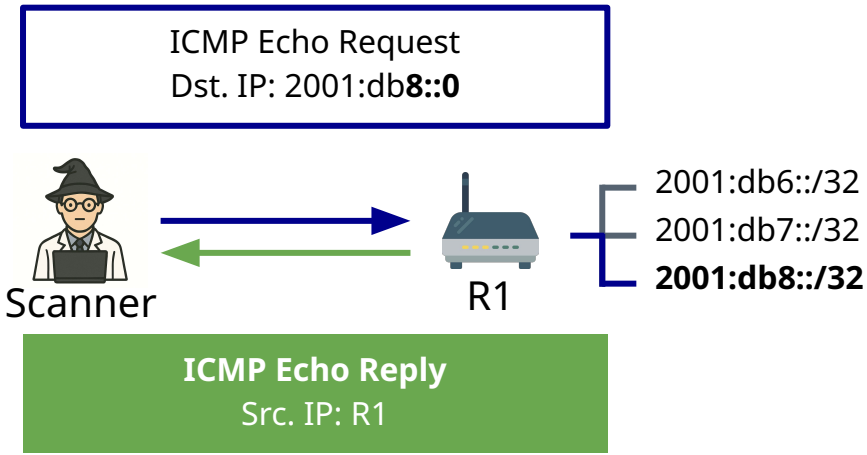
If a corresponding interface exists on that router, we trigger an Echo reply



Probing technique	Router observed		
Random	✓	✗	✗
Subnet-Router Anycast			

Instead of probing a random address, we probe an SRA address

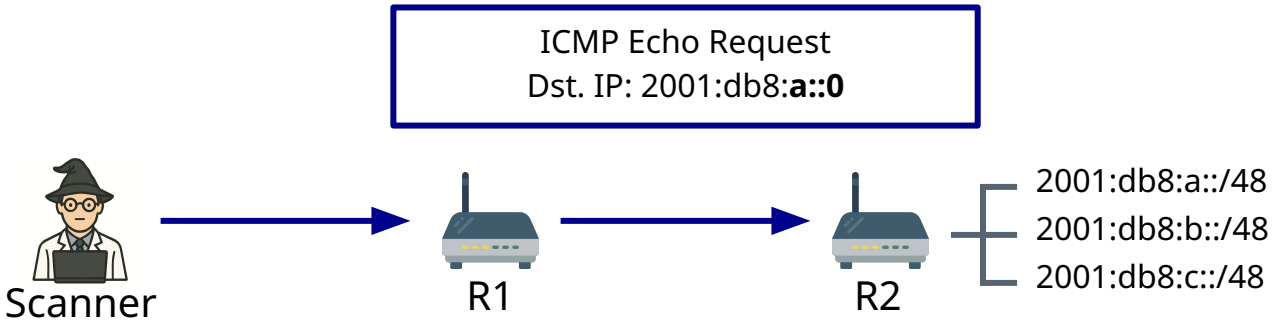
If a corresponding interface exists on that router, we trigger an Echo reply



Probing technique	Router observed		
Random	✓	✗	✗
Subnet-Router Anycast	✓		

Instead of probing a random address, we probe an SRA address

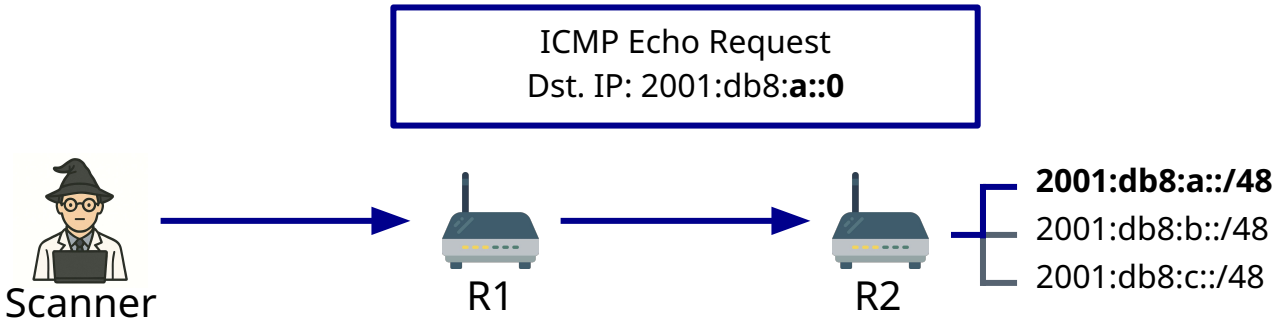
If a corresponding interface exists on that router, we trigger an Echo reply



Probing technique	Router observed		
Random	✓	✗	✗
Subnet-Router Anycast	✓		

Instead of probing a random address, we probe an SRA address

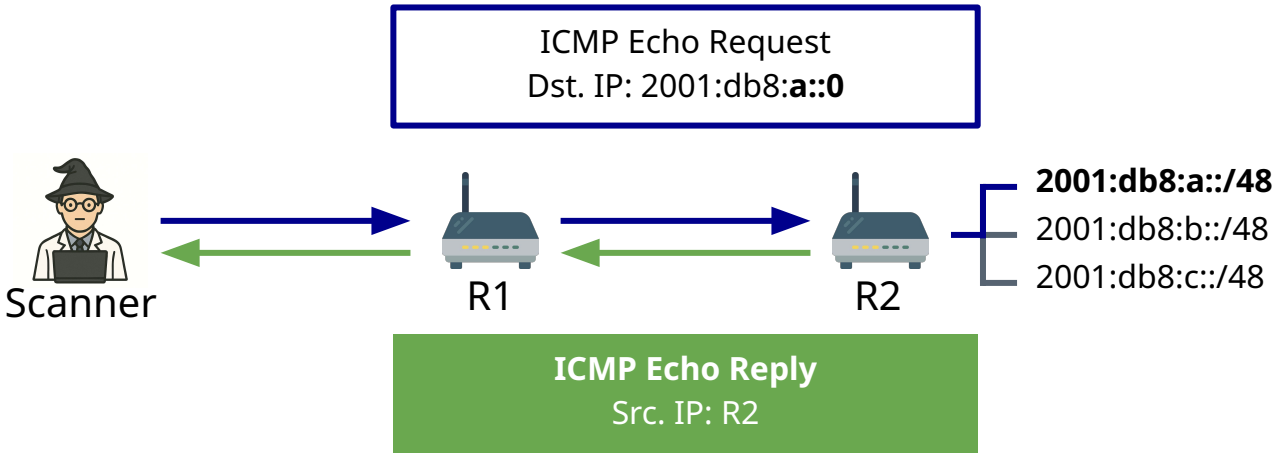
If a corresponding interface exists on that router, we trigger an Echo reply



Probing technique	**Router observed**		
Random	✓	✗	✗
Subnet-Router Anycast	✓		

Instead of probing a random address, we probe an SRA address

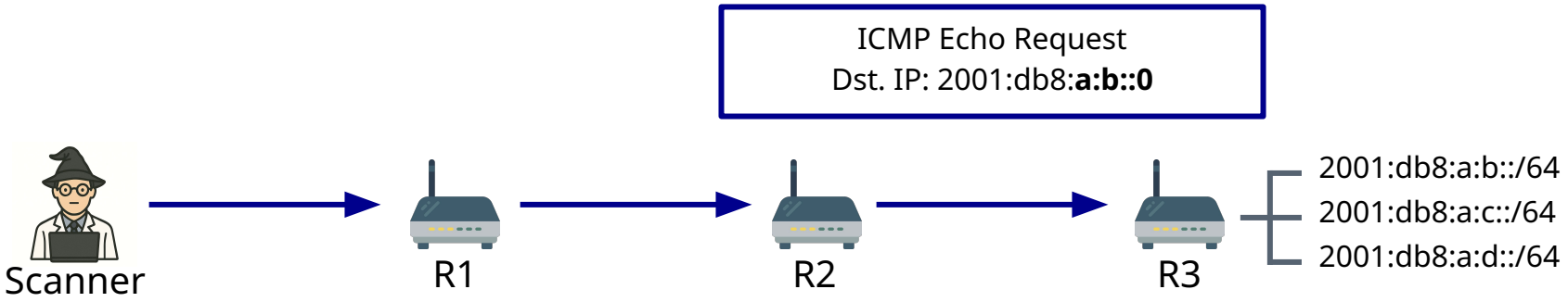
If a corresponding interface exists on that router, we trigger an Echo reply



Probing technique	**Router observed**		
Random	✓	✗	✗
Subnet-Router Anycast	✓	✓	

Instead of probing a random address, we probe an SRA address

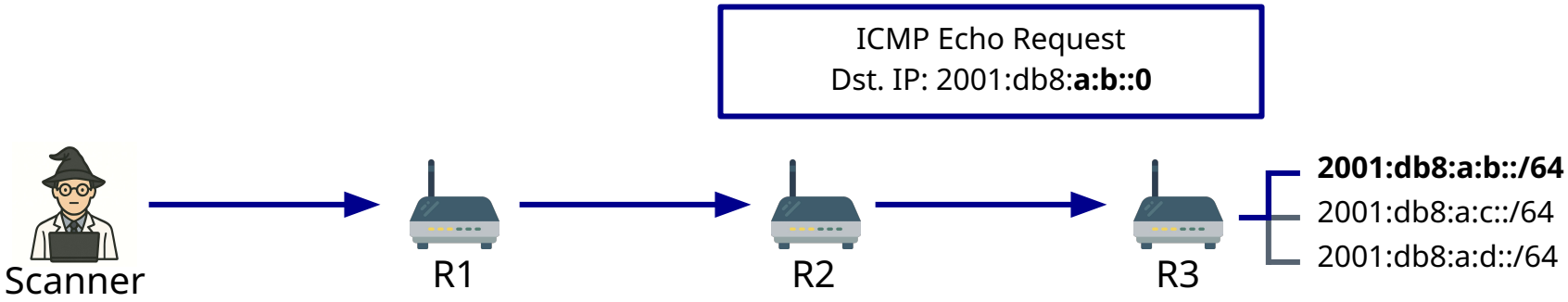
If a corresponding interface exists on that router, we trigger an Echo reply



Probing technique	**Router observed**		
Random	✓	✗	✗
Subnet-Router Anycast	✓	✓	

Instead of probing a random address, we probe an SRA address

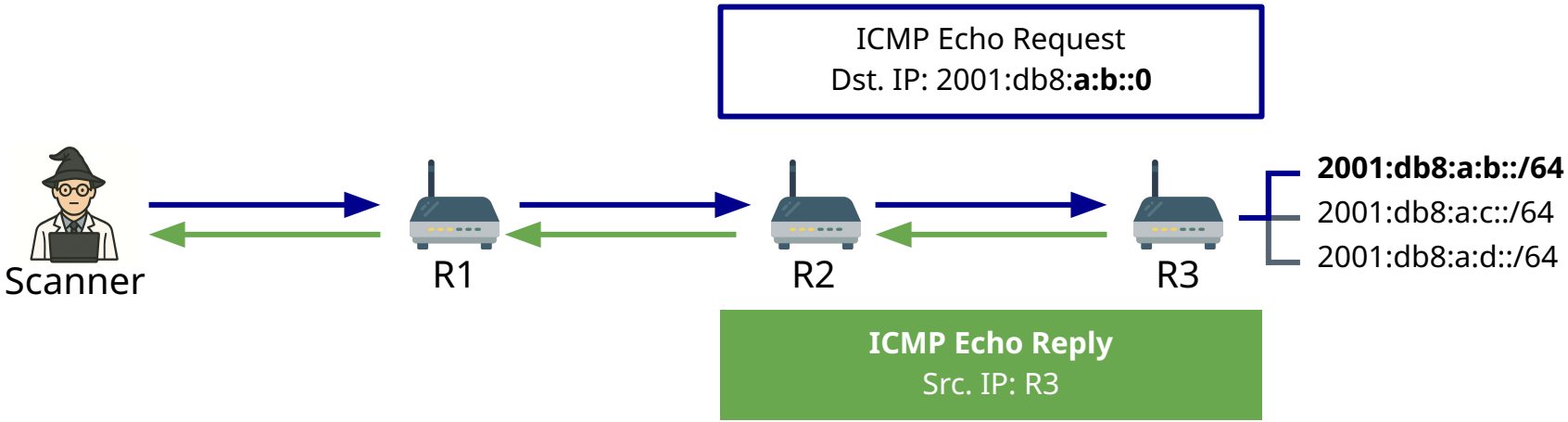
If a corresponding interface exists on that router, we trigger an Echo reply



Probing technique	**Router observed**		
Random	✓	✗	✗
Subnet-Router Anycast	✓	✓	

Instead of probing a random address, we probe an SRA address

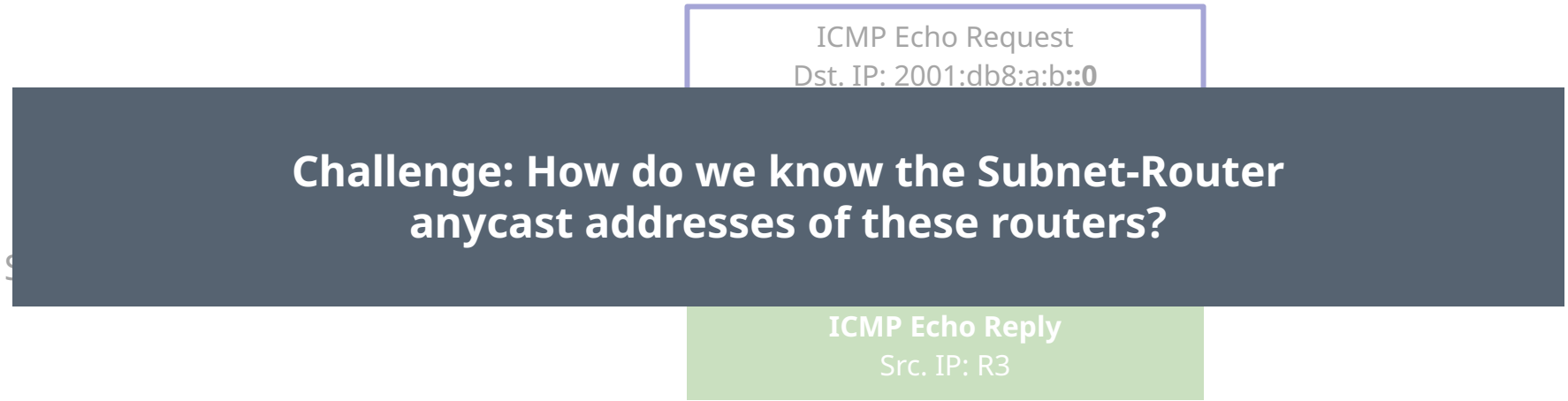
If a corresponding interface exists on that router, we trigger an Echo reply



Probing technique	**Router observed**		
Random	✓	✗	✗
Subnet-Router Anycast	✓	✓	✓

Instead of probing a random address, we probe an SRA address

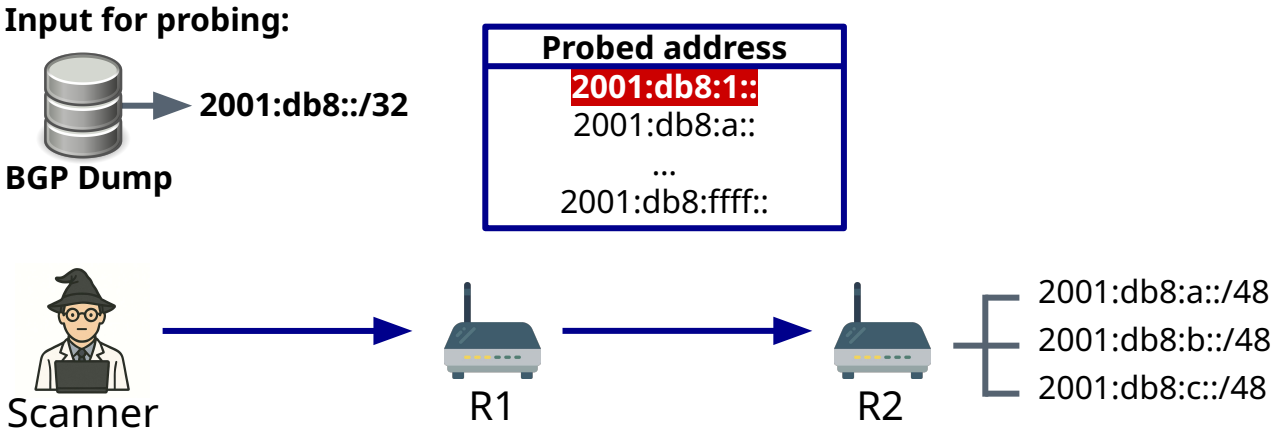
If a corresponding interface exists on that router, we trigger an Echo reply



Probing technique	Router observed		
Random	✓	✗	✗
Subnet-Router Anycast	✓	✓	✓

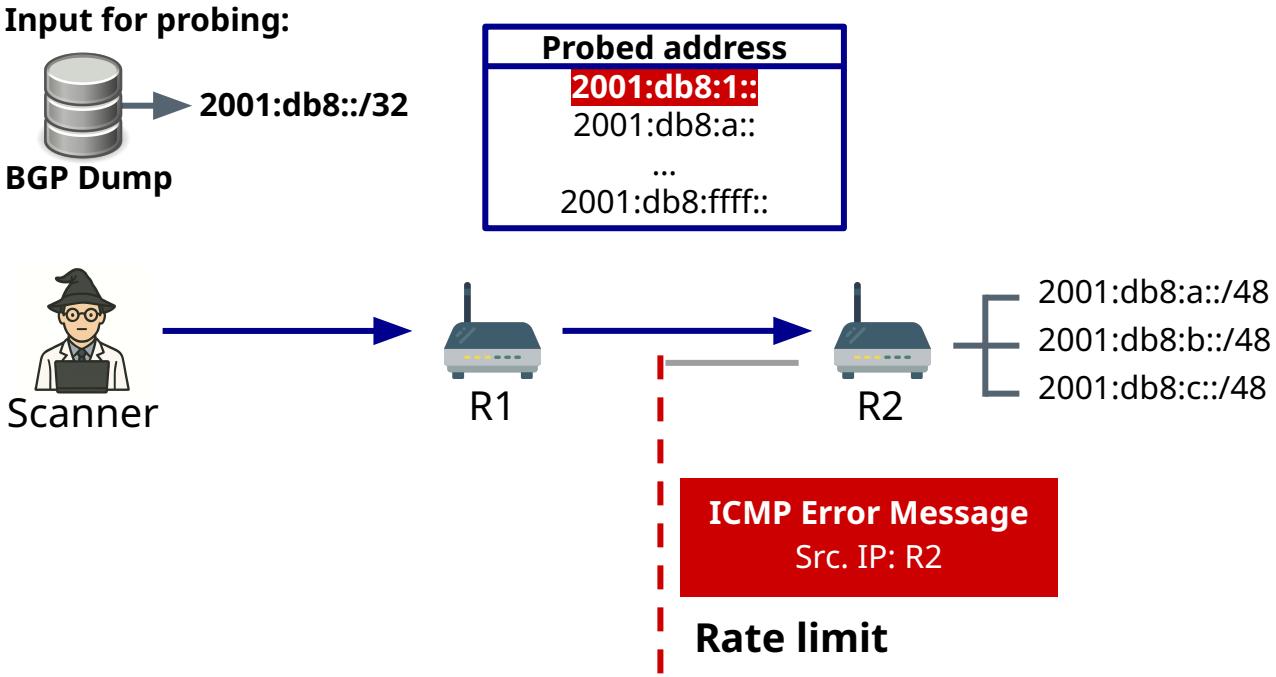
Partitioning of the routable address space into more specific subnets

Iterate through all possible subnets and probe the SRA address



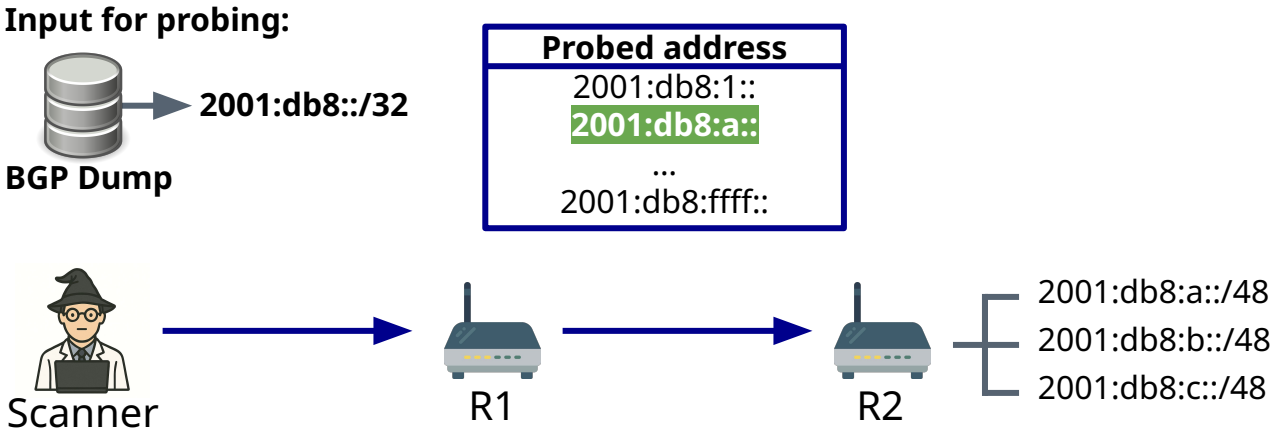
Partitioning of the routable address space into more specific subnets

Iterate through all possible subnets and probe the SRA address



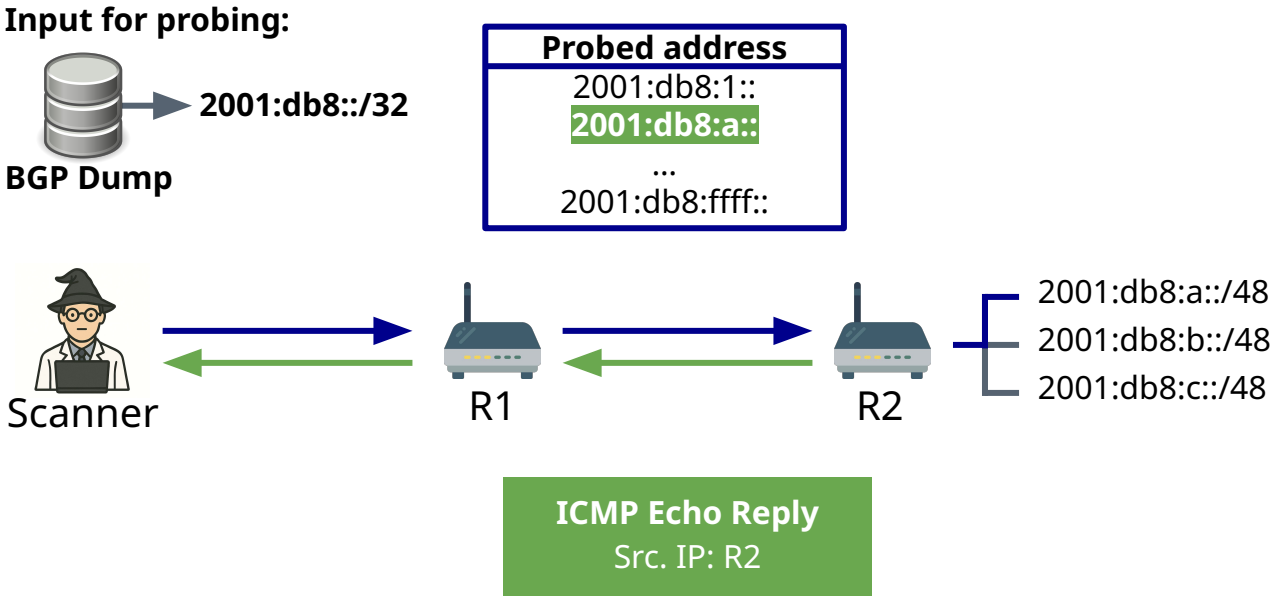
Partitioning of the routable address space into more specific subnets

Iterate through all possible subnets and probe the SRA address



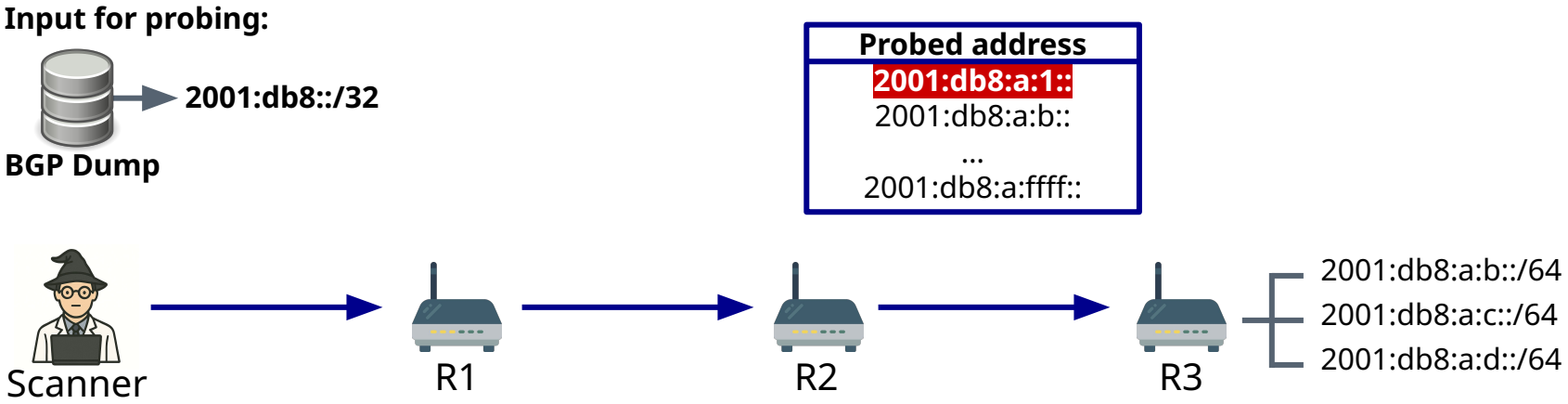
Partitioning of the routable address space into more specific subnets

Iterate through all possible subnets and probe the SRA address



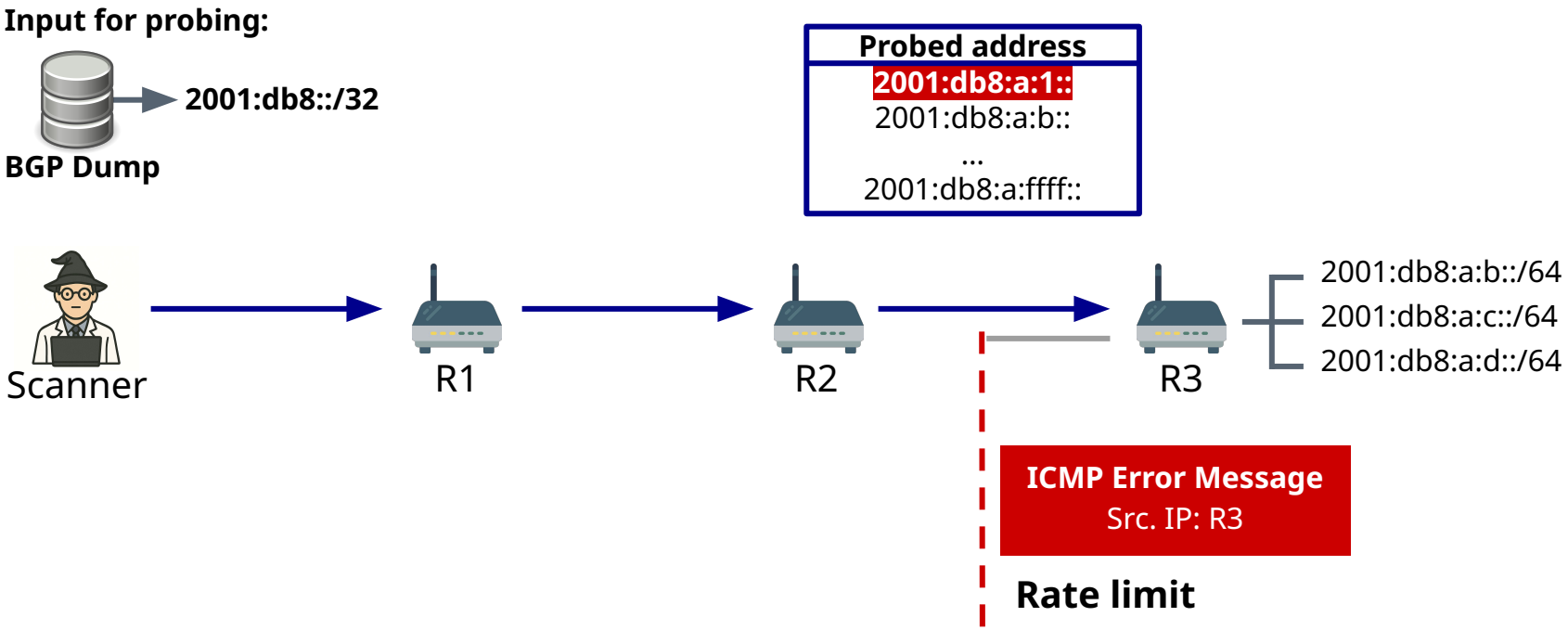
Partitioning of the routable address space into more specific subnets

Iterate through all possible subnets and probe the SRA address



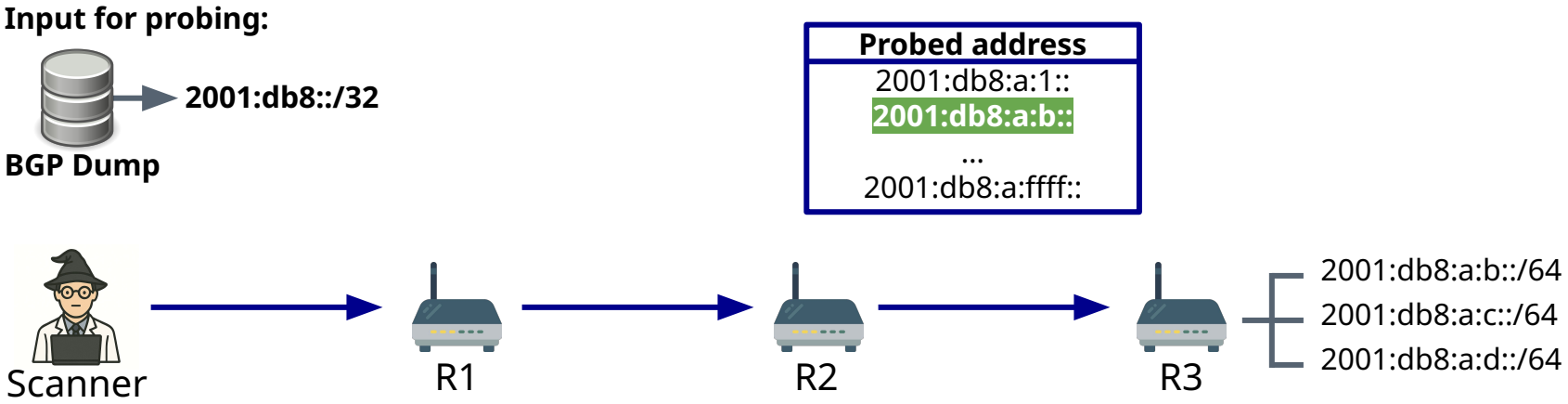
Partitioning of the routable address space into more specific subnets

Iterate through all possible subnets and probe the SRA address



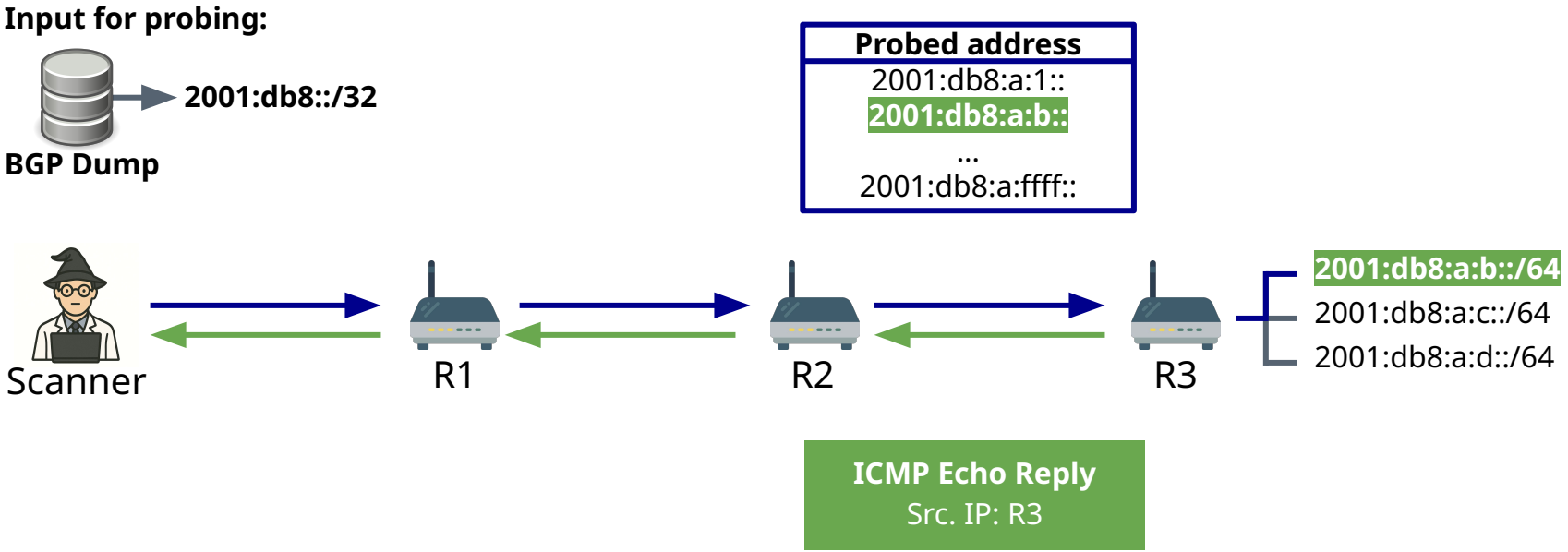
Partitioning of the routable address space into more specific subnets

Iterate through all possible subnets and probe the SRA address



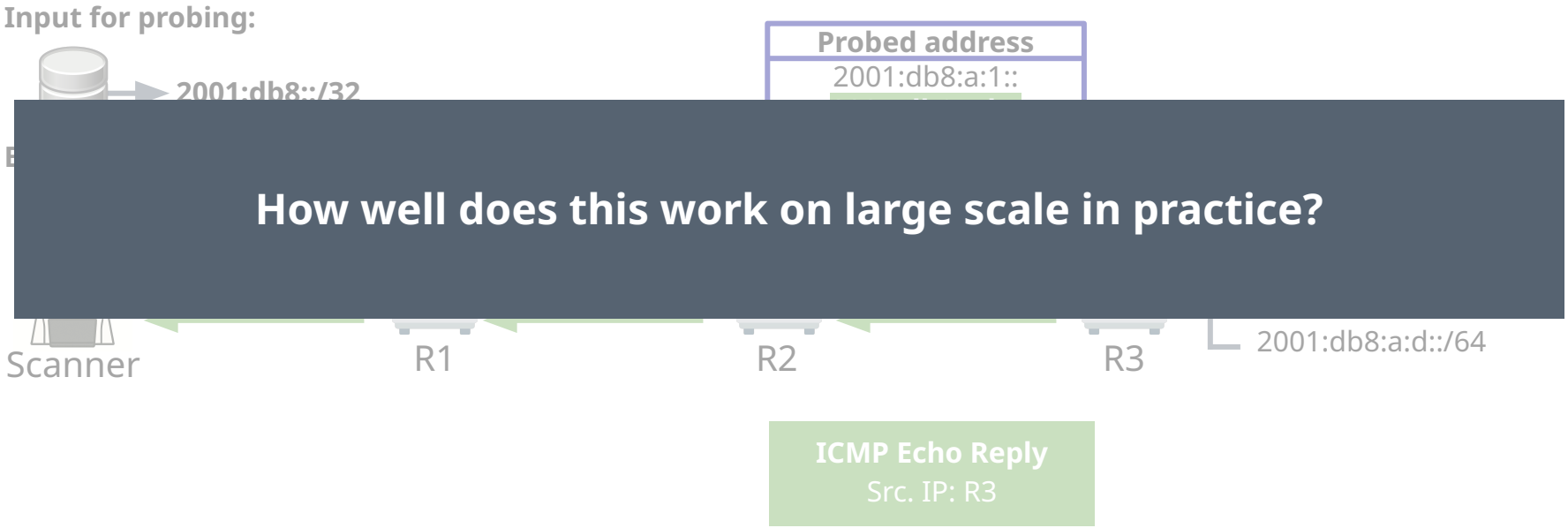
Partitioning of the routable address space into more specific subnets

Iterate through all possible subnets and probe the SRA address



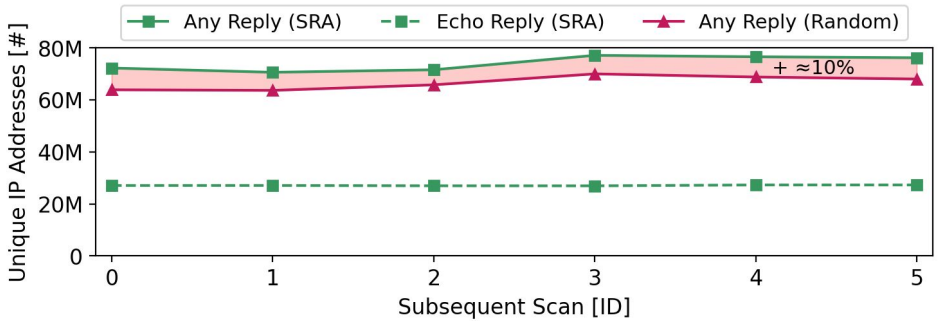
Partitioning of the routable address space into more specific subnets

Iterate through all possible subnets and probe the SRA address



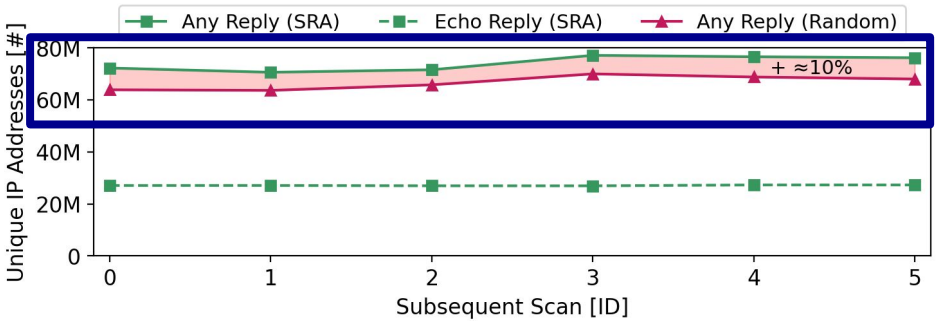
Comparison of SRA vs. Random Probing

We run our measurements every 12 hours over three days



Comparison of SRA vs. Random Probing

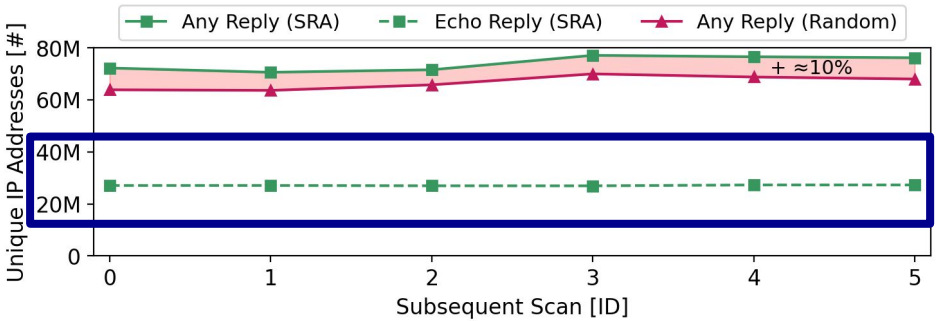
We run our measurements every 12 hours over three days



SRA probing reveals 10% more router IP addresses on average compared to random probing.

Comparison of SRA vs. Random Probing

We run our measurements every 12 hours over three days

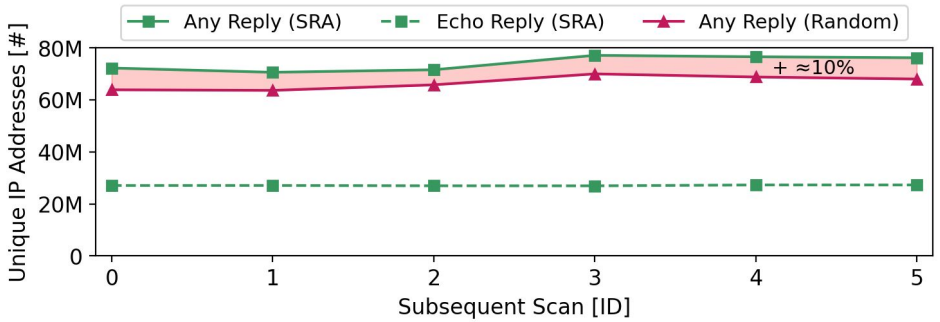


SRA probing reveals 10% more router IP addresses on average compared to random probing.

The number of Echo replies remains stable over time, SRA scans are far less affected by ICMP rate limiting.

Comparison of SRA vs. Random Probing

We run our measurements every 12 hours over three days



SRA probing reveals 10% more router IP addresses on average compared to random probing.

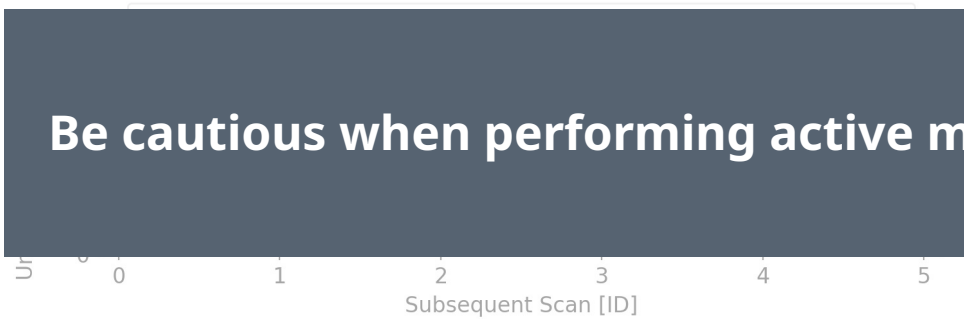
The number of Echo replies remains stable over time, SRA scans are far less affected by ICMP rate limiting.

We find ~9M router IP addresses exclusively with SRA probing.

More results in our paper.

Comparison of SRA vs. Random Probing

We run our measurements every 12 hours over three days



Be cautious when performing active measurements … routing loops :(

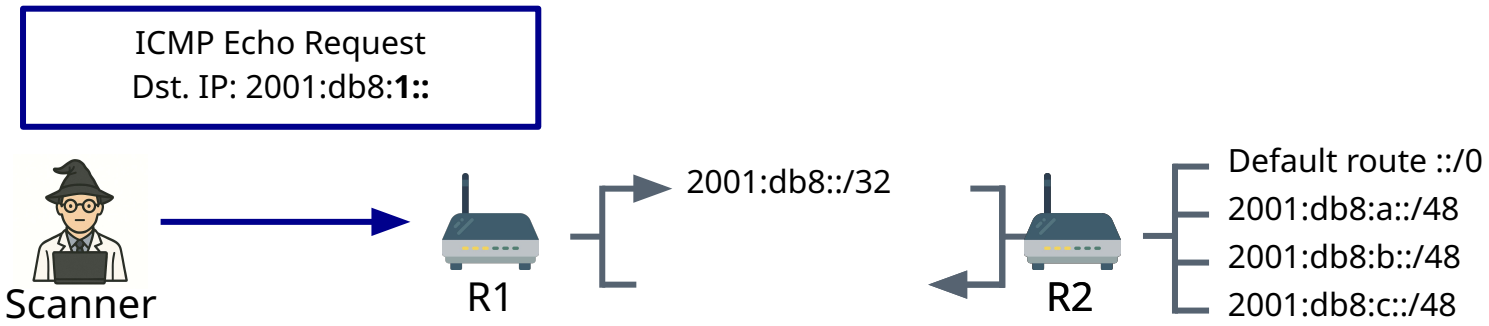
SRA probing reveals 10% more

scans are far less affected by ICMP rate limiting.

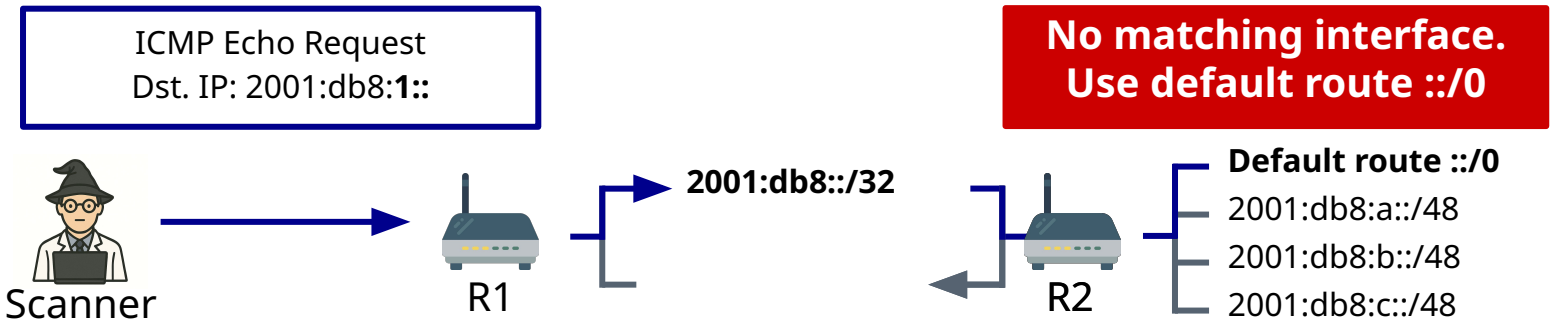
We find ~9M router IP addresses exclusively with SRA probing.

More results in our paper.

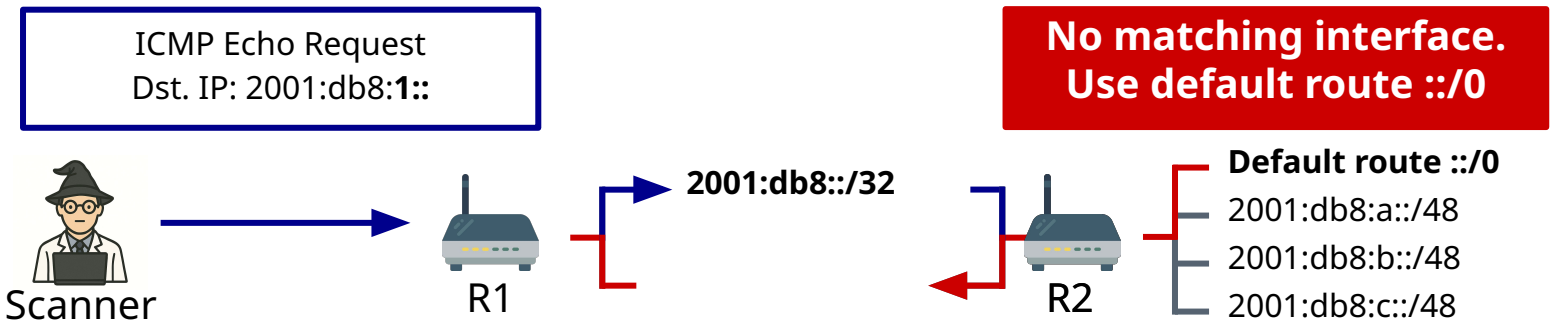
Missing NULL routes lead to routing loops
Common in IPv6 because of large amounts of unassigned subnets



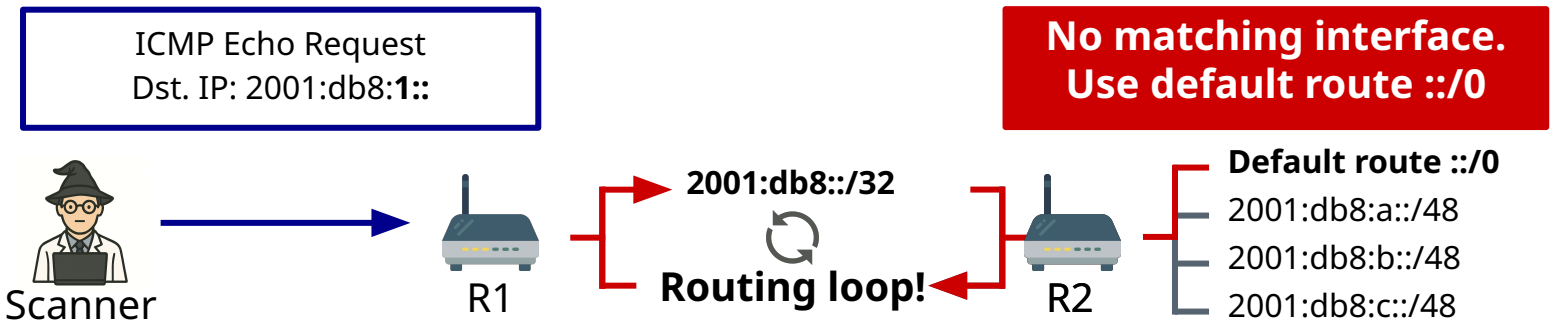
Missing NULL routes lead to routing loops
Common in IPv6 because of large amounts of unassigned subnets



Missing NULL routes lead to routing loops
Common in IPv6 because of large amounts of unassigned subnets

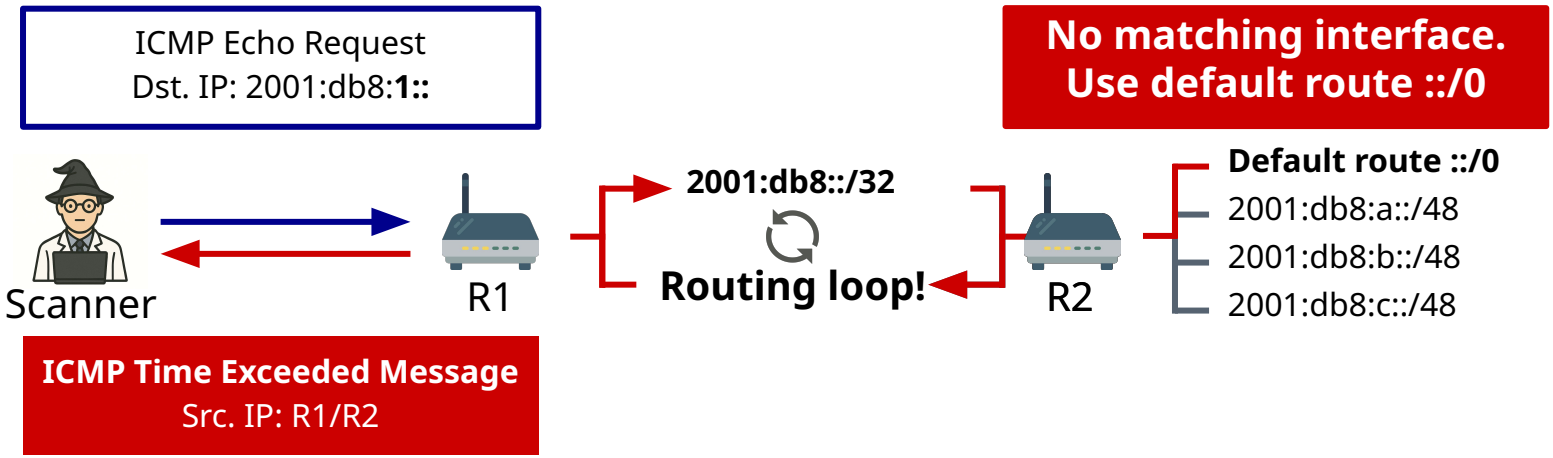


Missing NULL routes lead to routing loops
Common in IPv6 because of large amounts of unassigned subnets



Missing NULL routes lead to routing loops

Common in IPv6 because of large amounts of unassigned subnets



In our case not a single ICMP time exceeded message but >250k!

A router bug may trigger amplification of ICMP messages.

More details in our paper.

Scanner

ICMP T

capture-icmp-flood.pcapng

Datei Bearbeiten Ansicht Navigation Aufzeichnen Analyse Statistiken Telephonie Wireless Tools Hilfe

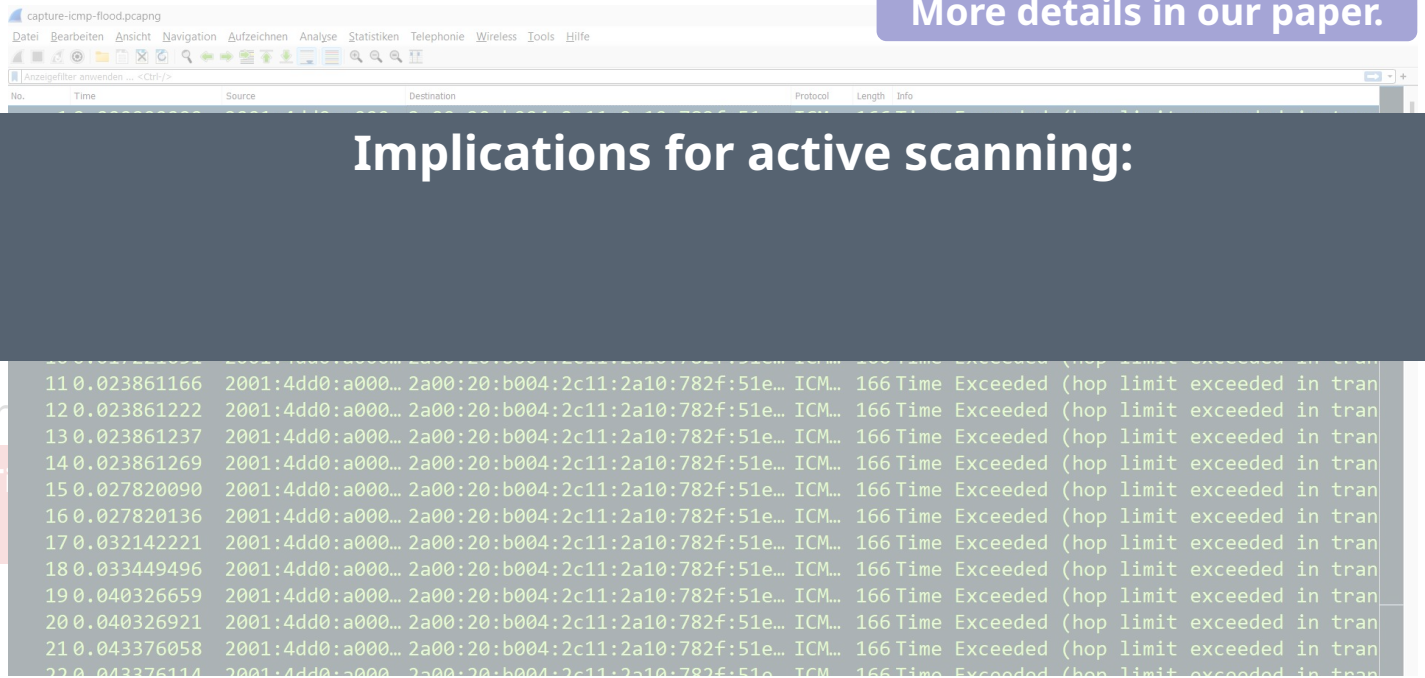
Anzeigefilter anwenden … <Ctrl-/>

No.	Time	Source	Destination	Protocol	Length	Info
1	0.000000000	2001:4dd0:a000…	2a00:20:b004:2c11:2a10:782f:51e…	ICM…	166	Time Exceeded (hop limit exceeded in tran
2	0.000000135	2001:4dd0:a000…	2a00:20:b004:2c11:2a10:782f:51e…	ICM…	166	Time Exceeded (hop limit exceeded in tran
3	0.004207259	2001:4dd0:a000…	2a00:20:b004:2c11:2a10:782f:51e…	ICM…	166	Time Exceeded (hop limit exceeded in tran
4	0.004207386	2001:4dd0:a000…	2a00:20:b004:2c11:2a10:782f:51e…	ICM…	166	Time Exceeded (hop limit exceeded in tran
5	0.007819047	2001:4dd0:a000…	2a00:20:b004:2c11:2a10:782f:51e…	ICM…	166	Time Exceeded (hop limit exceeded in tran
6	0.010723704	2001:4dd0:a000…	2a00:20:b004:2c11:2a10:782f:51e…	ICM…	166	Time Exceeded (hop limit exceeded in tran
7	0.012922813	2001:4dd0:a000…	2a00:20:b004:2c11:2a10:782f:51e…	ICM…	166	Time Exceeded (hop limit exceeded in tran
8	0.012922957	2001:4dd0:a000…	2a00:20:b004:2c11:2a10:782f:51e…	ICM…	166	Time Exceeded (hop limit exceeded in tran
9	0.017221473	2001:4dd0:a000…	2a00:20:b004:2c11:2a10:782f:51e…	ICM…	166	Time Exceeded (hop limit exceeded in tran
10	0.017221651	2001:4dd0:a000…	2a00:20:b004:2c11:2a10:782f:51e…	ICM…	166	Time Exceeded (hop limit exceeded in tran
11	0.023861166	2001:4dd0:a000…	2a00:20:b004:2c11:2a10:782f:51e…	ICM…	166	Time Exceeded (hop limit exceeded in tran
12	0.023861222	2001:4dd0:a000…	2a00:20:b004:2c11:2a10:782f:51e…	ICM…	166	Time Exceeded (hop limit exceeded in tran
13	0.023861237	2001:4dd0:a000…	2a00:20:b004:2c11:2a10:782f:51e…	ICM…	166	Time Exceeded (hop limit exceeded in tran
14	0.023861269	2001:4dd0:a000…	2a00:20:b004:2c11:2a10:782f:51e…	ICM…	166	Time Exceeded (hop limit exceeded in tran
15	0.027820090	2001:4dd0:a000…	2a00:20:b004:2c11:2a10:782f:51e…	ICM…	166	Time Exceeded (hop limit exceeded in tran
16	0.027820136	2001:4dd0:a000…	2a00:20:b004:2c11:2a10:782f:51e…	ICM…	166	Time Exceeded (hop limit exceeded in tran
17	0.032142221	2001:4dd0:a000…	2a00:20:b004:2c11:2a10:782f:51e…	ICM…	166	Time Exceeded (hop limit exceeded in tran
18	0.033449496	2001:4dd0:a000…	2a00:20:b004:2c11:2a10:782f:51e…	ICM…	166	Time Exceeded (hop limit exceeded in tran
19	0.040326659	2001:4dd0:a000…	2a00:20:b004:2c11:2a10:782f:51e…	ICM…	166	Time Exceeded (hop limit exceeded in tran
20	0.040326921	2001:4dd0:a000…	2a00:20:b004:2c11:2a10:782f:51e…	ICM…	166	Time Exceeded (hop limit exceeded in tran
21	0.043376058	2001:4dd0:a000…	2a00:20:b004:2c11:2a10:782f:51e…	ICM…	166	Time Exceeded (hop limit exceeded in tran

In our case not a single ICMP time exceeded message but >250k!

A router bug may trigger amplification of ICMP messages.

More details in our paper.

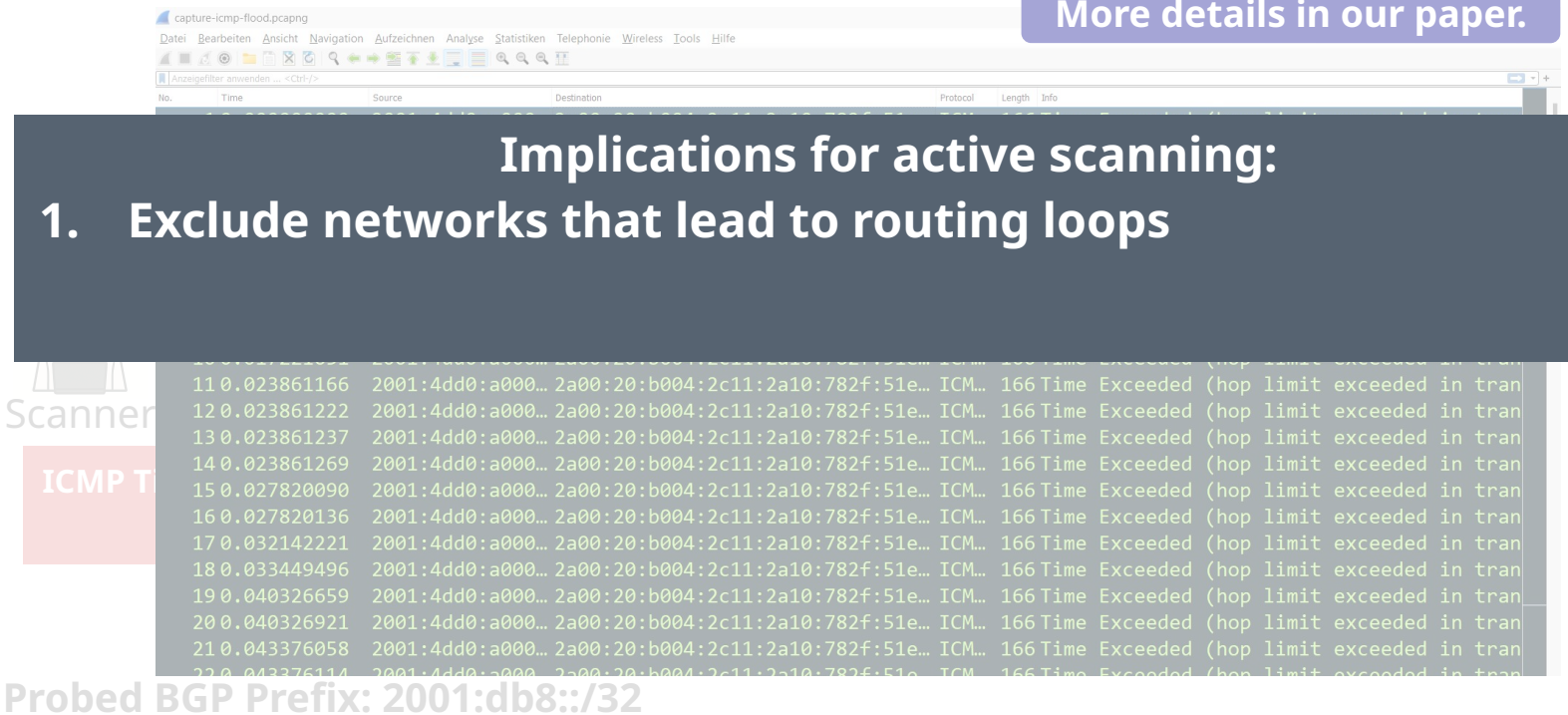


Implications for active scanning:

In our case not a single ICMP time exceeded message but >250k!

A router bug may trigger amplification of ICMP messages.

More details in our paper.



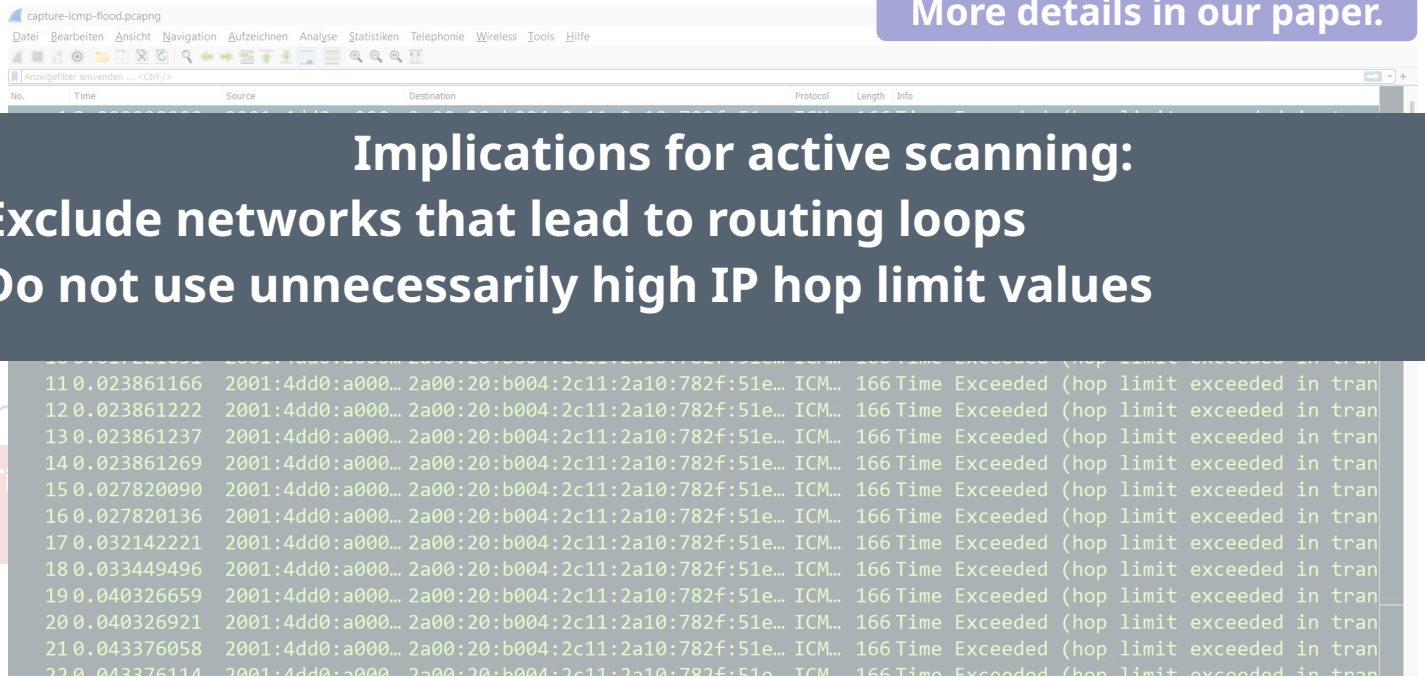
Implications for active scanning:

1. Exclude networks that lead to routing loops

In our case not a single ICMP time exceeded message but >250k!

A router bug may trigger amplification of ICMP messages.

More details in our paper.



Implications for active scanning:

1. Exclude networks that lead to routing loops
2. Do not use unnecessarily high IP hop limit values

Conclusion

Exploring the active IPv6 address space is challenging.

Conclusion

Exploring the active IPv6 address space is challenging.

SRA probing is a valid approach to complement existing hitlists and replace random probing.

Be aware of IPv6 routing loops!

Conclusion

Exploring the active IPv6 address space is challenging.

SRA probing is a valid approach to complement existing hitlists and replace random probing.

Be aware of IPv6 routing loops!

More details can be found in the paper!
All artifacts of this paper are available under
https://doi.org/10.5281/zenodo.17210253