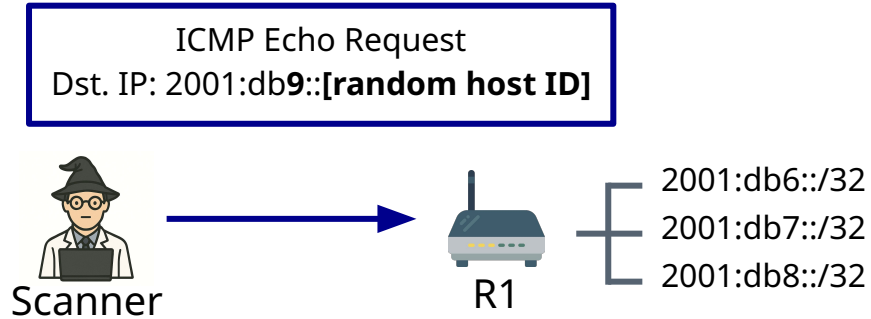


Maynard Koch, Raphael Hiesgen, Marcin Nawrocki, Thomas C. Schmidt, Matthias Wählisch

Scanning the IPv6 Internet Using Subnet-Router Anycast Probing

A common approach to analyze network topology

Send out probes to random targets and analyze ICMP error messages



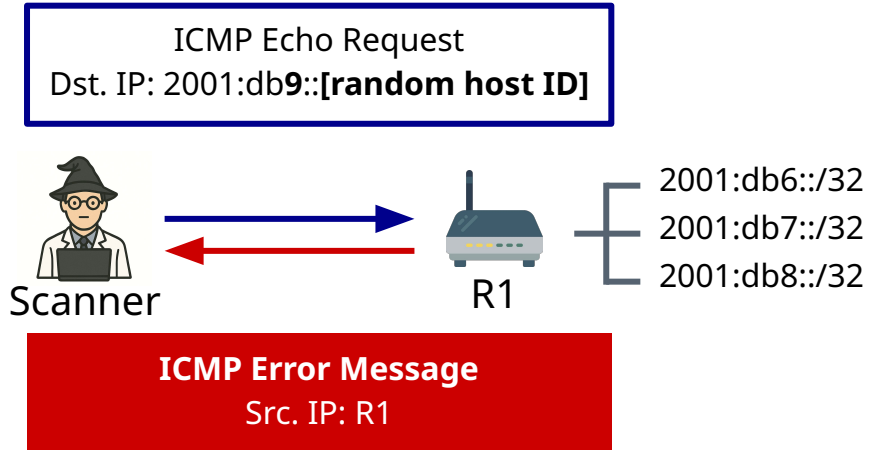
Probing technique

Router observed

Random

A common approach to analyze network topology

Send out probes to random targets and analyze ICMP error messages



Probing technique

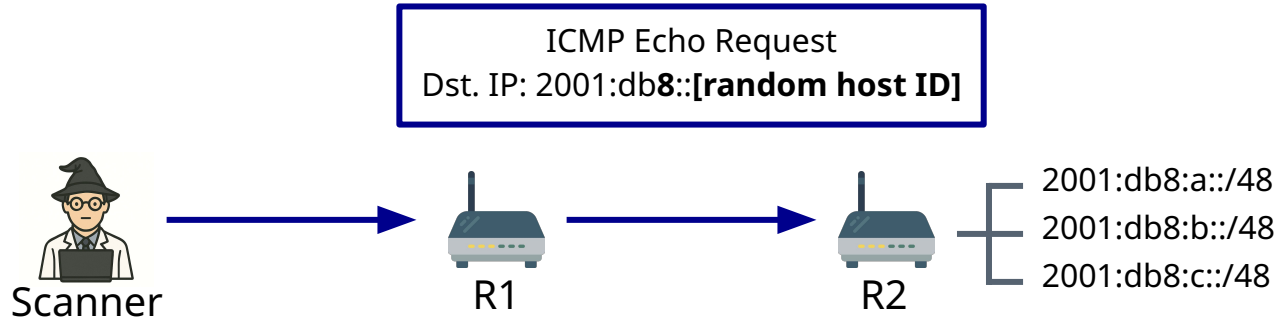
Router observed

Random



A common approach to analyze network topology

Send out probes to random targets and analyze ICMP error messages



Probing technique

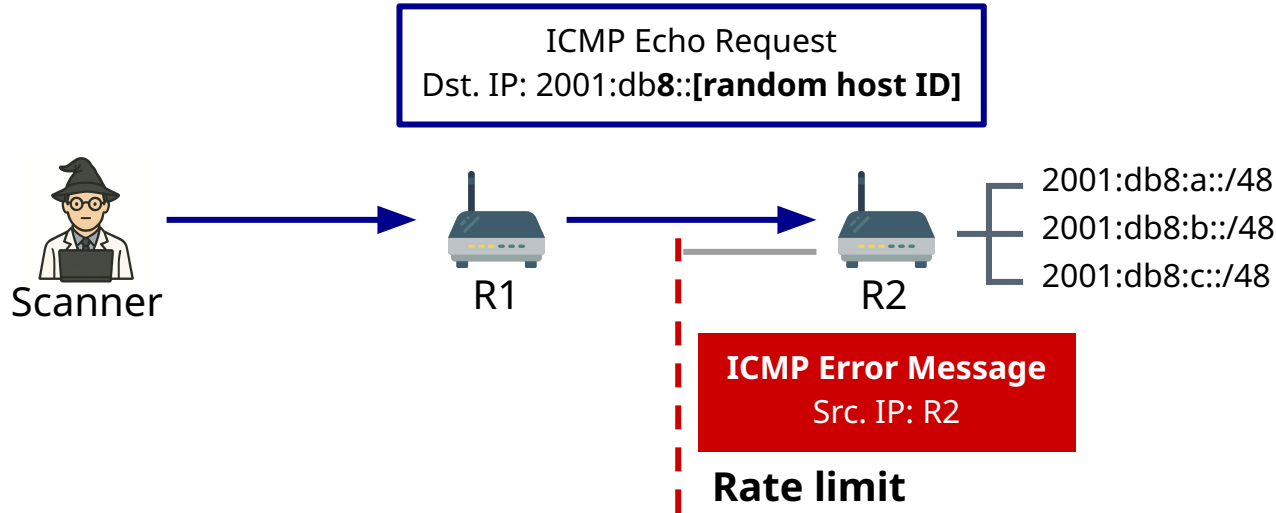
Router observed

Random



A common approach to analyze network topology

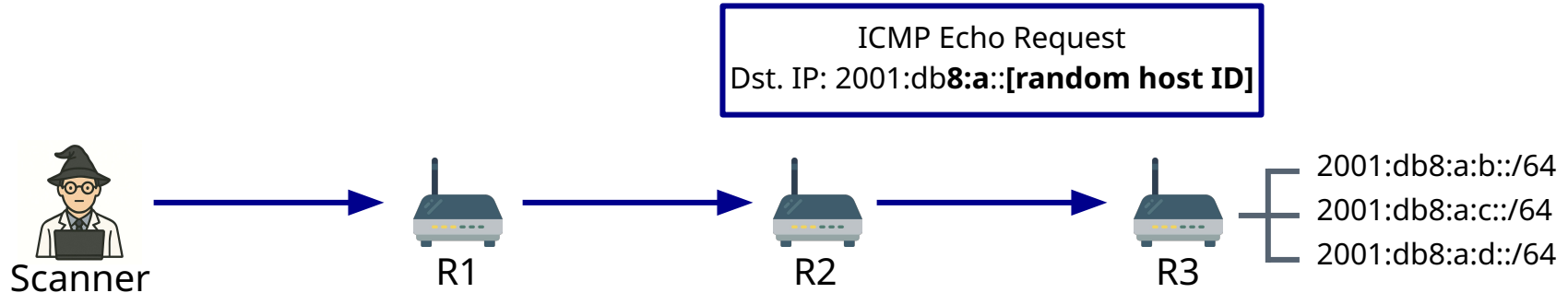
Send out probes to random targets and analyze ICMP error messages



Probing technique	Router observed
Random	✓ ✗

A common approach to analyze network topology

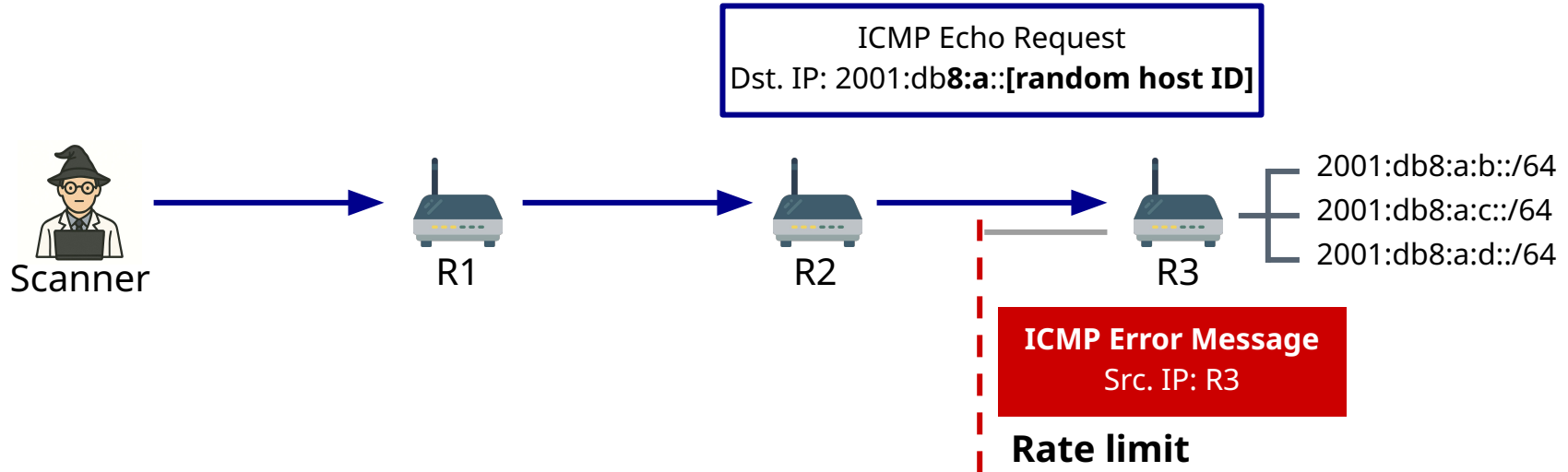
Send out probes to random targets and analyze ICMP error messages



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



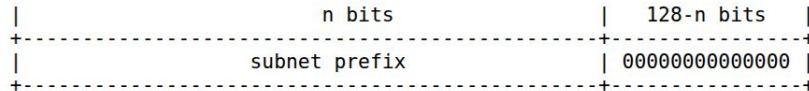
Subnet-Router Anycast (SRA) probing

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:



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

Subnet-Router Anycast (SRA) probing

Trigger ICMP Echo replies instead of error messages

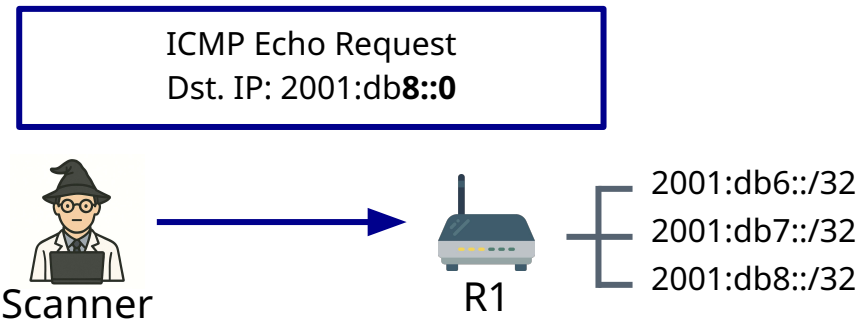
RFC 1884 (IPv6 addressing architecture):

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	0000000000000000

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		0000000000000000	
+	-----		-----	+

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

ICMP Echo Request

Dst. IP: 2001:db8::0



Scanner



R1

2001:db6::/32
2001:db7::/32
2001:db8::/32

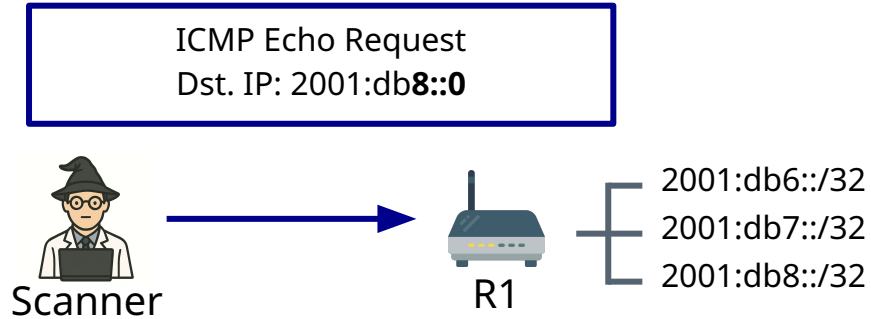
ICMP Echo Reply

Src. IP: R1

**Unaffected by rate limiting
of ICMP error messages!**

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

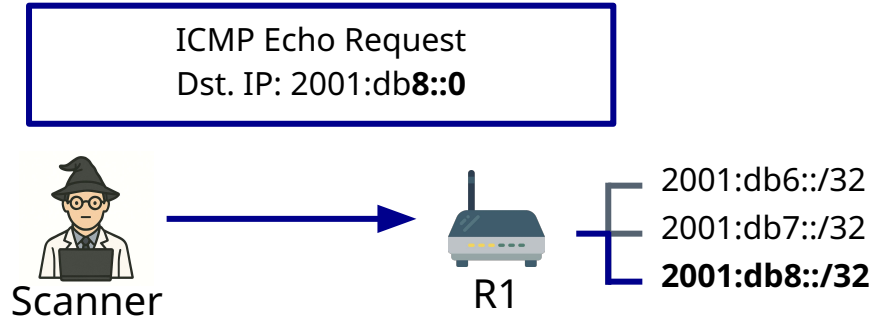
If a corresponding interface exists on that router, we trigger an Echo reply



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

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

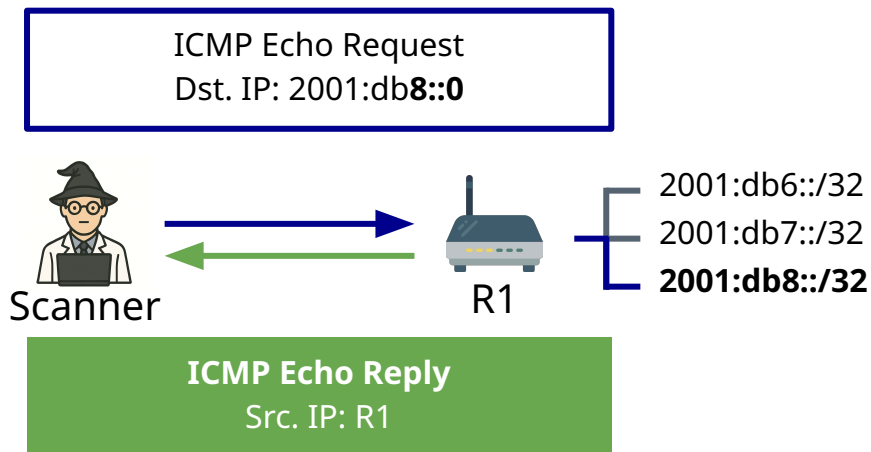
If a corresponding interface exists on that router, we trigger an Echo reply



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

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

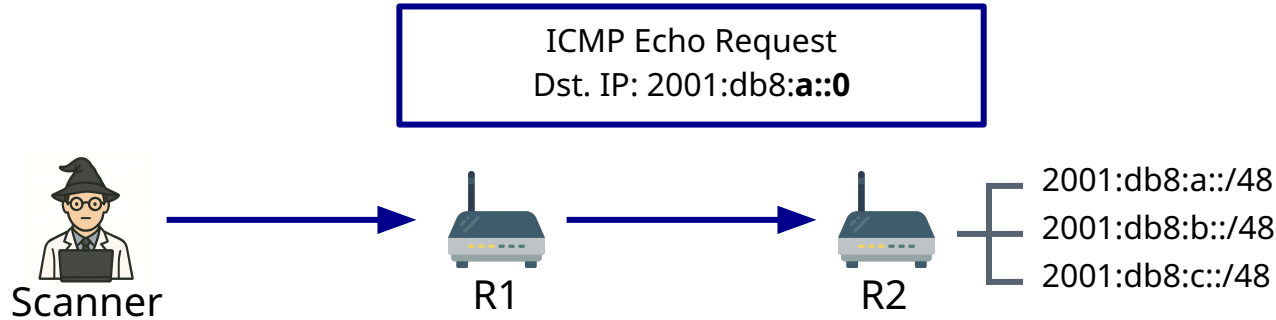
If a corresponding interface exists on that router, we trigger an Echo reply



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

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

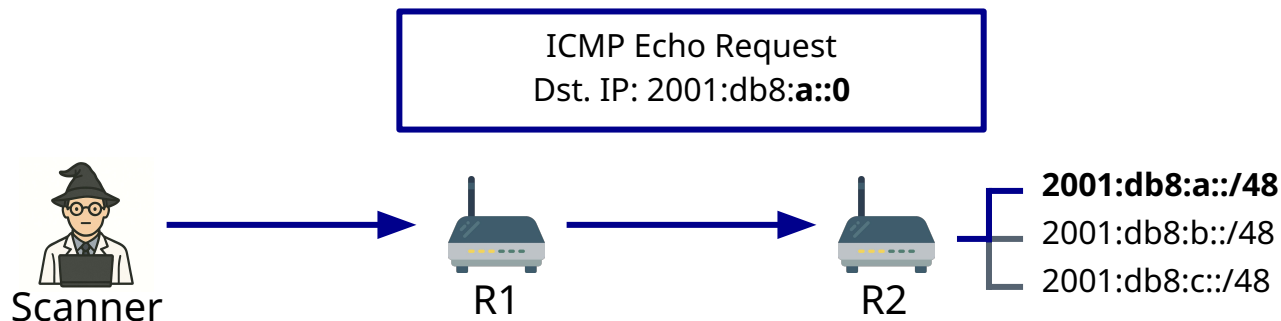
If a corresponding interface exists on that router, we trigger an Echo reply



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

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

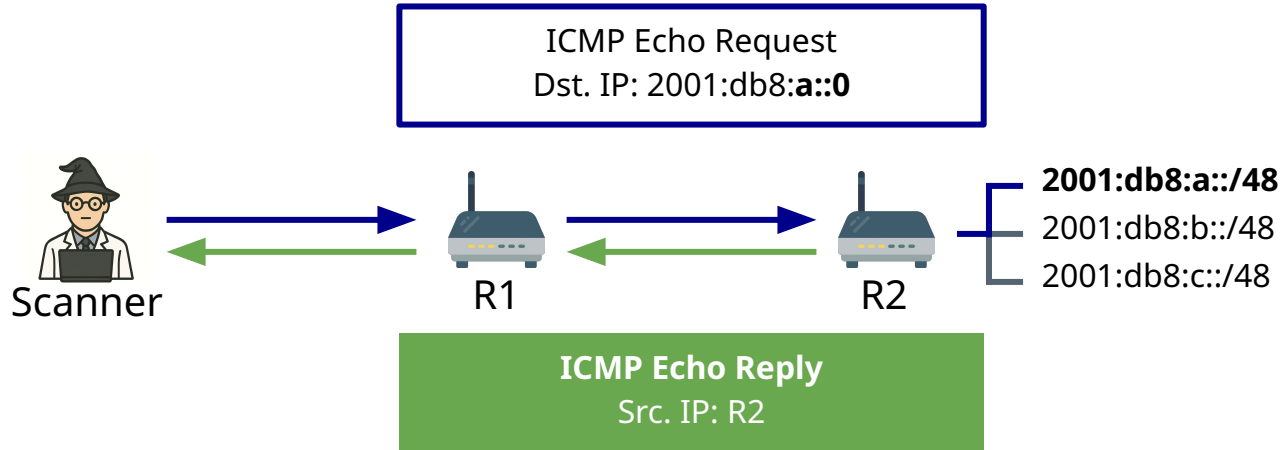
If a corresponding interface exists on that router, we trigger an Echo reply



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

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

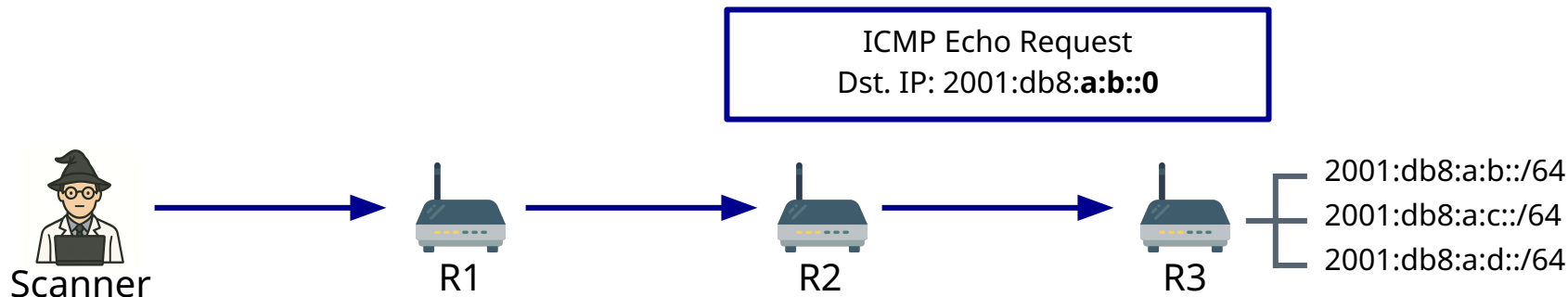
If a corresponding interface exists on that router, we trigger an Echo reply



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

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

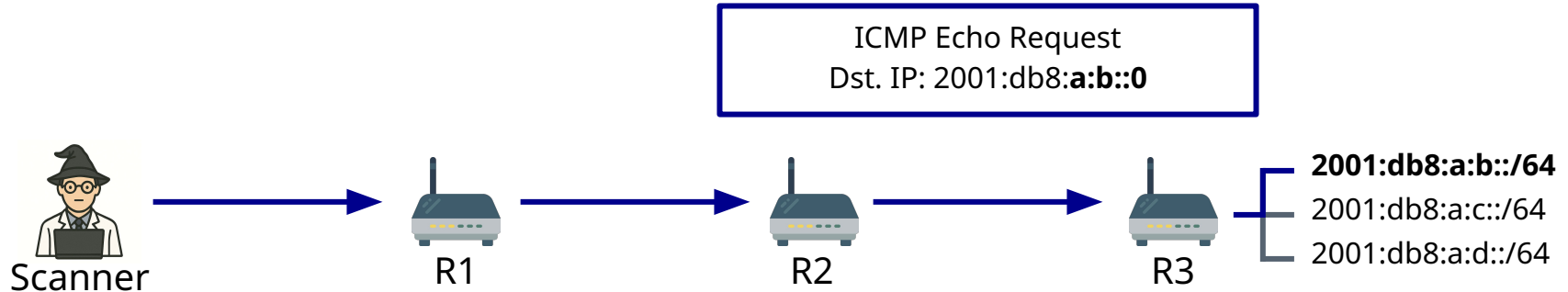
If a corresponding interface exists on that router, we trigger an Echo reply



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

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

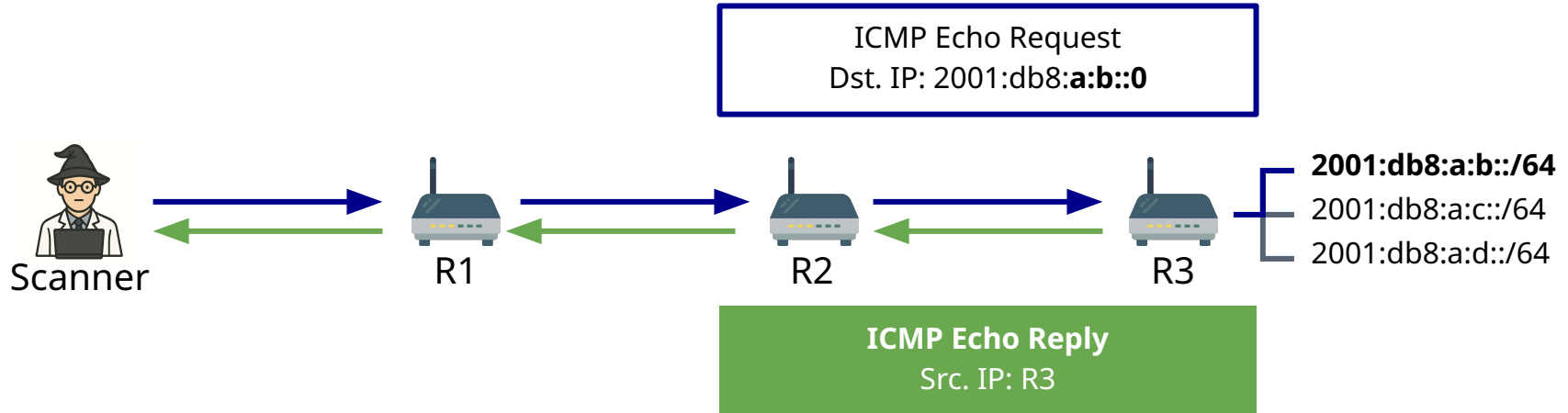
If a corresponding interface exists on that router, we trigger an Echo reply



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

ICMP Echo Request
Dst. IP: 2001:db8:a:b::0

**Challenge: How do we know the Subnet-Router
anycast addresses of these routers?**

ICMP Echo Reply
Src. IP: R3

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

Input for probing:



2001:db8::/32

Probed address
2001:db8:1::
2001:db8:a::
...
2001:db8:ffff::



2001:db8:a::/48
2001:db8:b::/48
2001:db8:c::/48

Partitioning of the routable address space into more specific subnets

Iterate through all possible subnets and probe the SRA address

Input for probing:



2001:db8::/32

Probed address
2001:db8:1::
2001:db8:a::
...
2001:db8:ffff::



2001:db8:a::/48
2001:db8:b::/48
2001:db8:c::/48

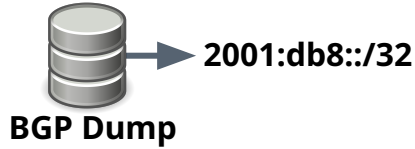
ICMP Error Message
Src. IP: R2

Rate limit

Partitioning of the routable address space into more specific subnets

Iterate through all possible subnets and probe the SRA address

Input for probing:



Probed address
2001:db8:1::
2001:db8:a::
...
2001:db8:ffff::



2001:db8:a::/48
2001:db8:b::/48
2001:db8:c::/48

Partitioning of the routable address space into more specific subnets

Iterate through all possible subnets and probe the SRA address

Input for probing:



2001:db8::/32

Probed address
2001:db8:1::
2001:db8:a::
...
2001:db8:ffff::



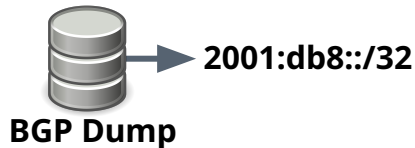
- 2001:db8:a::/48
- 2001:db8:b::/48
- 2001:db8:c::/48

ICMP Echo Reply
Src. IP: R2

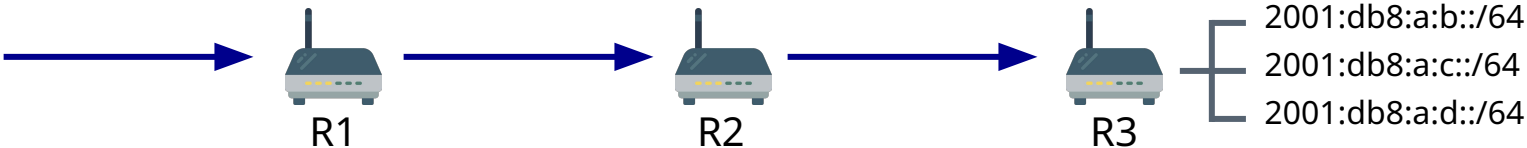
Partitioning of the routable address space into more specific subnets

Iterate through all possible subnets and probe the SRA address

Input for probing:



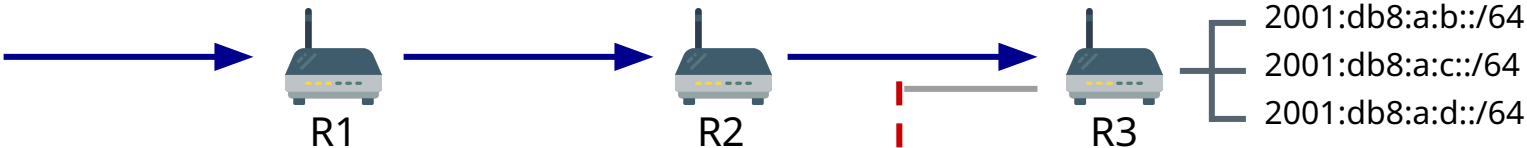
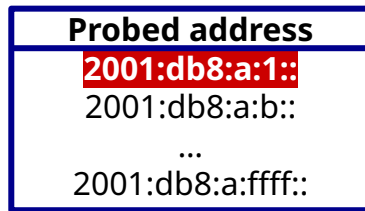
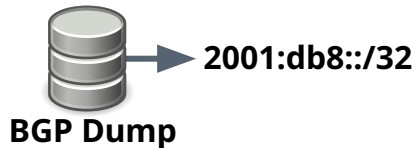
Probed address
2001:db8:a:1::
2001:db8:a:b::
...
2001:db8:a:ffff::



Partitioning of the routable address space into more specific subnets

Iterate through all possible subnets and probe the SRA address

Input for probing:



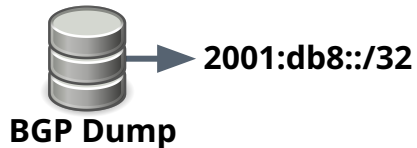
ICMP Error Message
Src. IP: R3

Rate limit

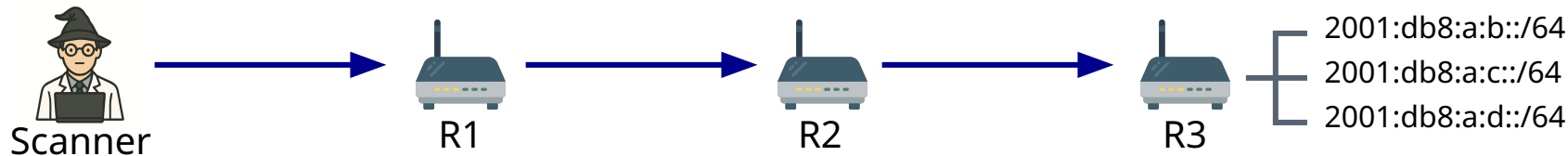
Partitioning of the routable address space into more specific subnets

Iterate through all possible subnets and probe the SRA address

Input for probing:



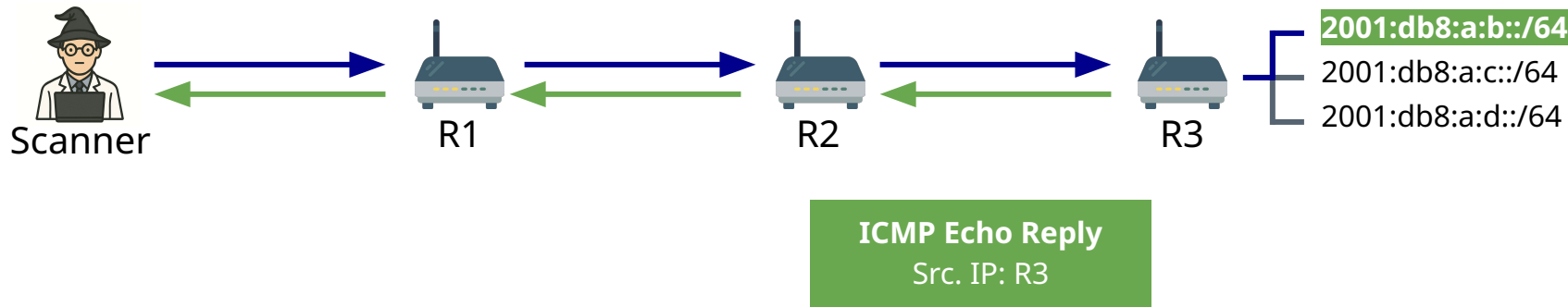
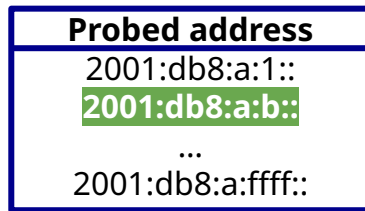
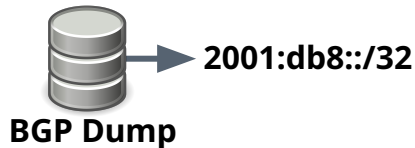
Probed address
2001:db8:a:1::
2001:db8:a:b::
...
2001:db8:a:ffff::



Partitioning of the routable address space into more specific subnets

Iterate through all possible subnets and probe the SRA address

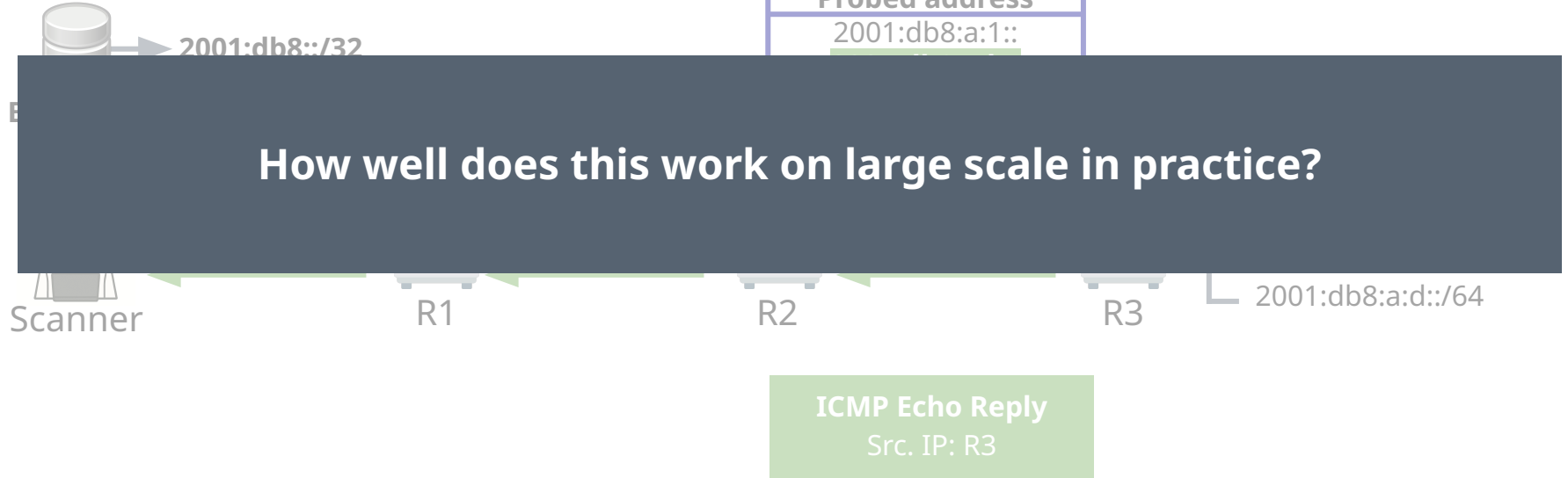
Input for probing:



Partitioning of the routable address space into more specific subnets

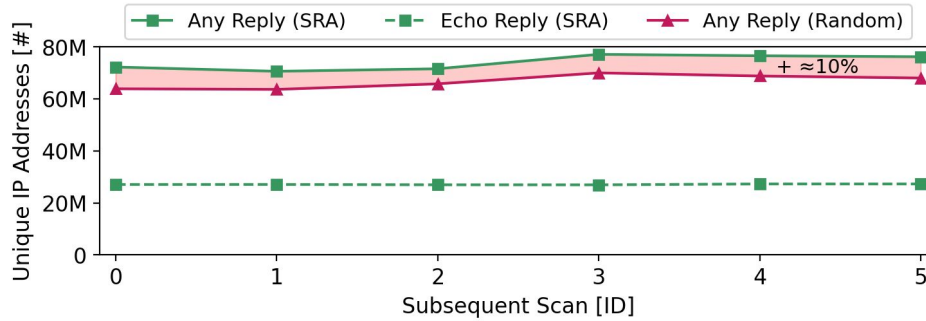
Iterate through all possible subnets and probe the SRA address

Input for probing:



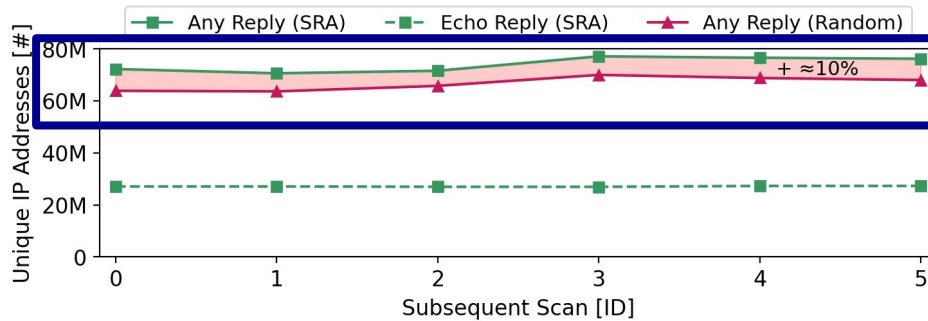
Comparison of SRA vs. Random Probing

We run our measurements every 12 hours over three days



Comparison of SRA vs. Random Probing

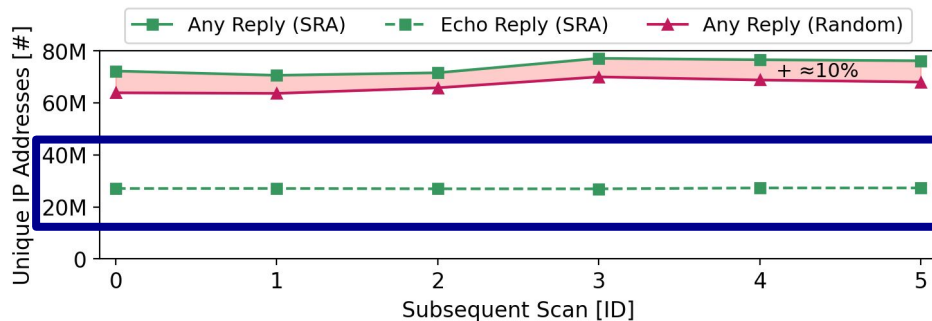
We run our measurements every 12 hours over three days



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

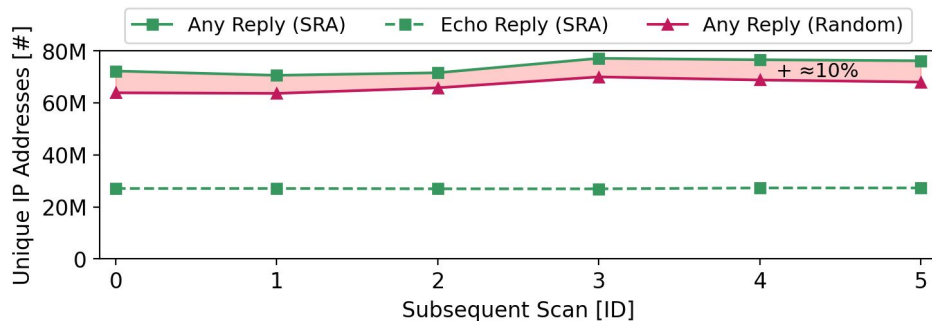


SRA probing reveals 10% more router IP addresses on average compared to random probing.

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

SRA probing reveals 10% more

Be cautious when performing active measurements ... routing loops :(

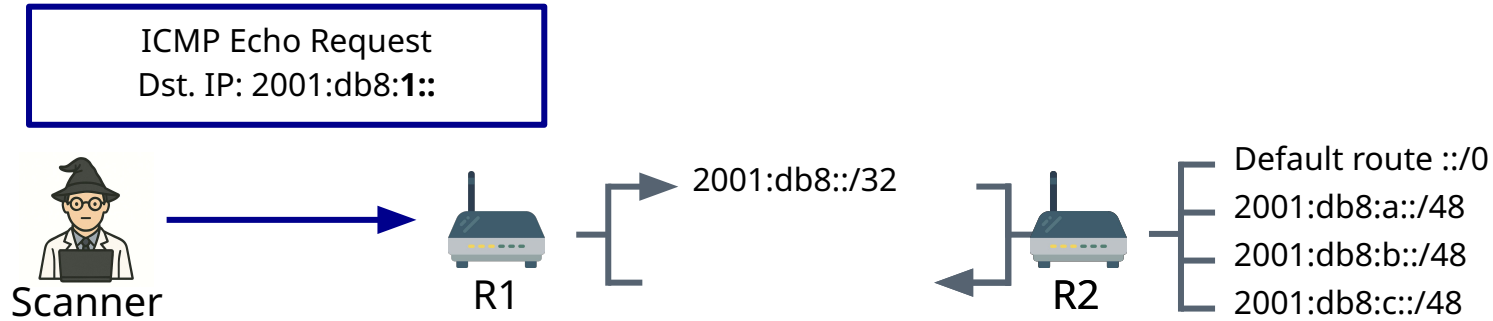
Scans are far less affected by ICMP rate limiting.

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

More results in our paper.

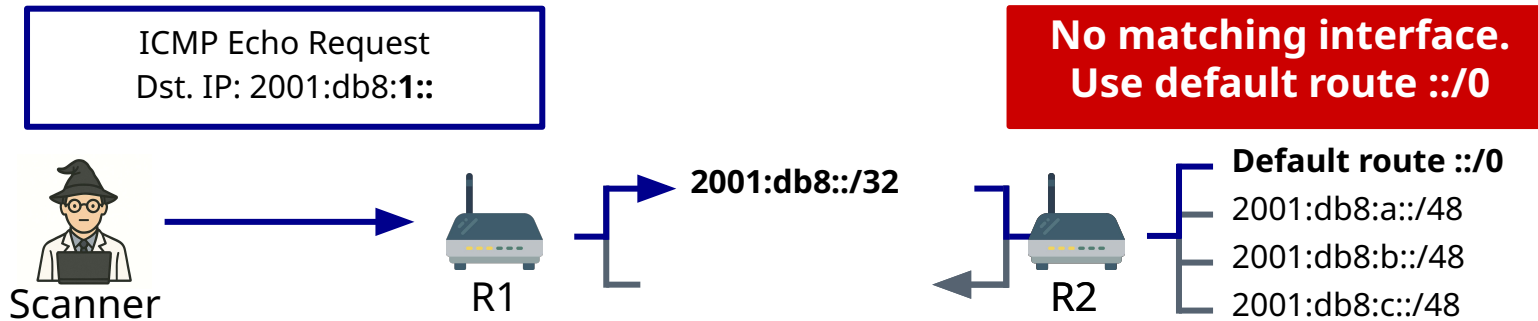
Missing NULL routes lead to routing loops

Common in IPv6 because of large amounts of unassigned subnets



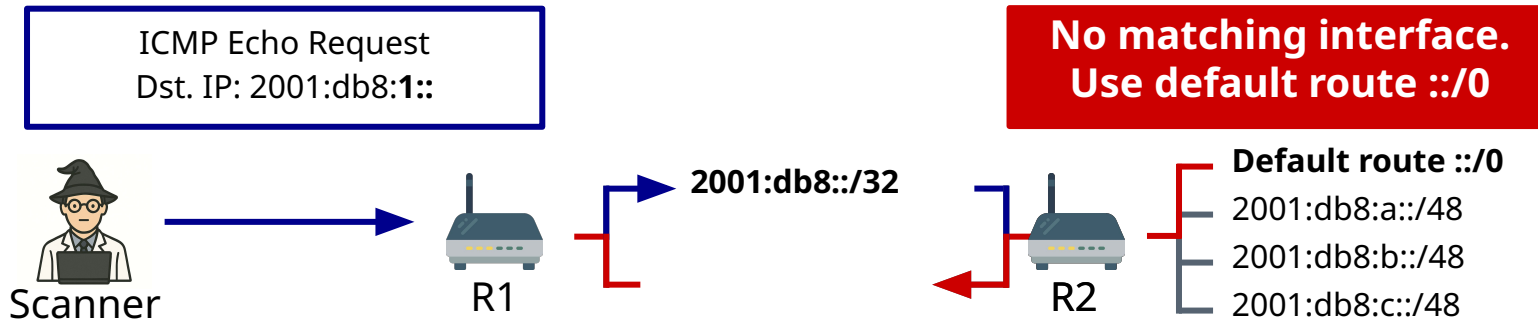
Missing NULL routes lead to routing loops

Common in IPv6 because of large amounts of unassigned subnets



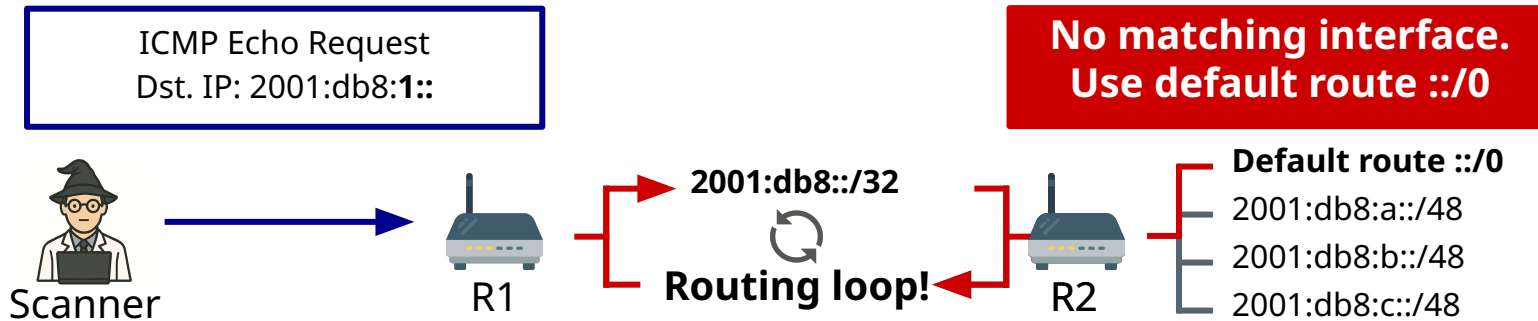
Missing NULL routes lead to routing loops

Common in IPv6 because of large amounts of unassigned subnets



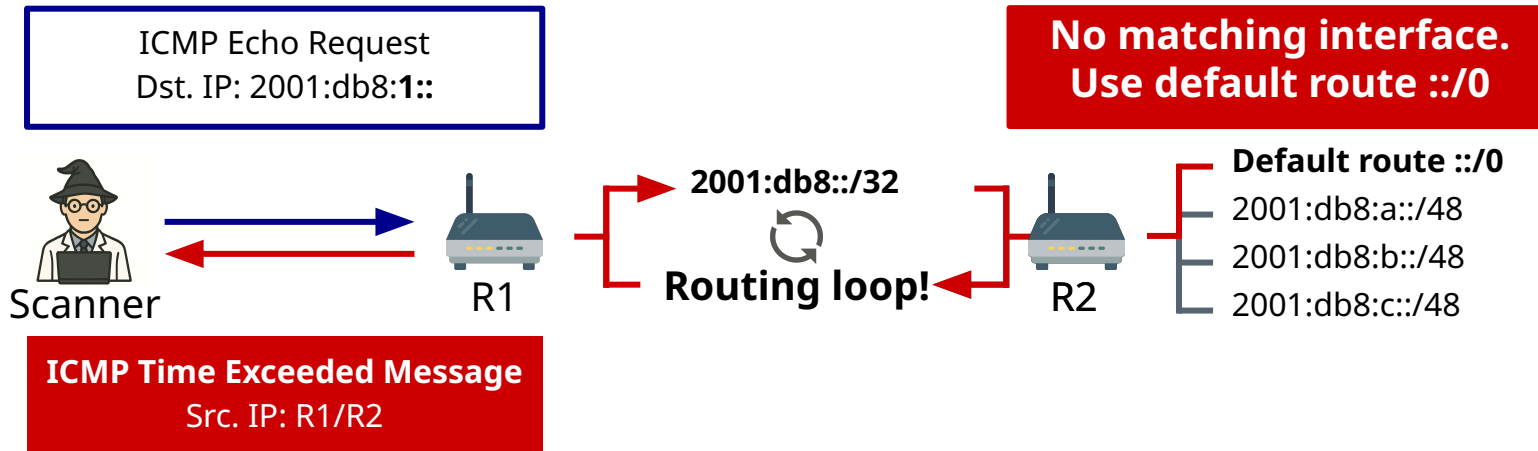
Missing NULL routes lead to routing loops

Common in IPv6 because of large amounts of unassigned subnets



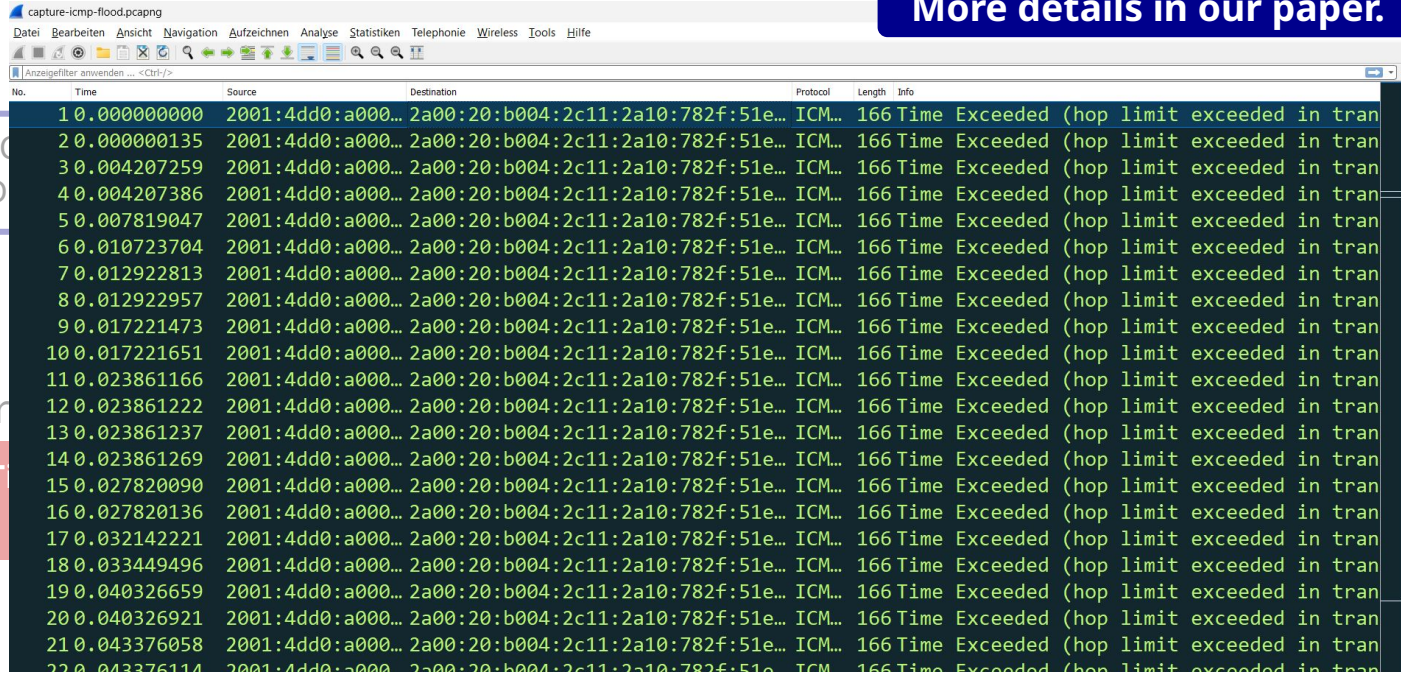
Missing NULL routes lead to routing loops

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.

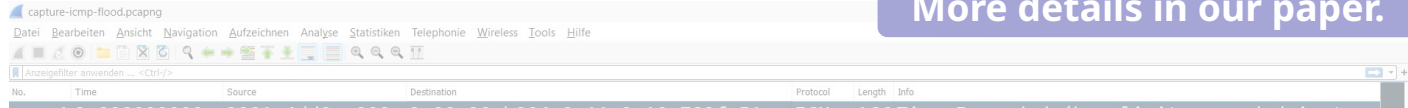


The image shows a Wireshark packet capture titled 'capture-icmp-flood.pcapng'. The interface includes a menu bar (Datei, Bearbeiten, Ansicht, Navigation, Aufzeichnen, Statistiken, Telephonie, Wireless, Tools, Hilfe) and a toolbar. A search filter 'Anzeigefilter anwenden ... <Ctrl-F>' is visible. The packet list pane shows 22 packets, all of which are ICMP Time Exceeded messages. The packet details pane shows the structure of an ICMP Time Exceeded message, including the hop limit and the reason for exceeding the limit.

No.	Time	Source	Destination	Protocol	Length	Info
1	0.000000000	2001:4dd0:a000...	2a00:20:b004:2c11:2a10:782f:51e...	ICMP...	166	Time Exceeded (hop limit exceeded in tran
2	0.000000135	2001:4dd0:a000...	2a00:20:b004:2c11:2a10:782f:51e...	ICMP...	166	Time Exceeded (hop limit exceeded in tran
3	0.004207259	2001:4dd0:a000...	2a00:20:b004:2c11:2a10:782f:51e...	ICMP...	166	Time Exceeded (hop limit exceeded in tran
4	0.004207386	2001:4dd0:a000...	2a00:20:b004:2c11:2a10:782f:51e...	ICMP...	166	Time Exceeded (hop limit exceeded in tran
5	0.007819047	2001:4dd0:a000...	2a00:20:b004:2c11:2a10:782f:51e...	ICMP...	166	Time Exceeded (hop limit exceeded in tran
6	0.010723704	2001:4dd0:a000...	2a00:20:b004:2c11:2a10:782f:51e...	ICMP...	166	Time Exceeded (hop limit exceeded in tran
7	0.012922813	2001:4dd0:a000...	2a00:20:b004:2c11:2a10:782f:51e...	ICMP...	166	Time Exceeded (hop limit exceeded in tran
8	0.012922957	2001:4dd0:a000...	2a00:20:b004:2c11:2a10:782f:51e...	ICMP...	166	Time Exceeded (hop limit exceeded in tran
9	0.017221473	2001:4dd0:a000...	2a00:20:b004:2c11:2a10:782f:51e...	ICMP...	166	Time Exceeded (hop limit exceeded in tran
10	0.017221651	2001:4dd0:a000...	2a00:20:b004:2c11:2a10:782f:51e...	ICMP...	166	Time Exceeded (hop limit exceeded in tran
11	0.023861166	2001:4dd0:a000...	2a00:20:b004:2c11:2a10:782f:51e...	ICMP...	166	Time Exceeded (hop limit exceeded in tran
12	0.023861222	2001:4dd0:a000...	2a00:20:b004:2c11:2a10:782f:51e...	ICMP...	166	Time Exceeded (hop limit exceeded in tran
13	0.023861237	2001:4dd0:a000...	2a00:20:b004:2c11:2a10:782f:51e...	ICMP...	166	Time Exceeded (hop limit exceeded in tran
14	0.023861269	2001:4dd0:a000...	2a00:20:b004:2c11:2a10:782f:51e...	ICMP...	166	Time Exceeded (hop limit exceeded in tran
15	0.027820090	2001:4dd0:a000...	2a00:20:b004:2c11:2a10:782f:51e...	ICMP...	166	Time Exceeded (hop limit exceeded in tran
16	0.027820136	2001:4dd0:a000...	2a00:20:b004:2c11:2a10:782f:51e...	ICMP...	166	Time Exceeded (hop limit exceeded in tran
17	0.032142221	2001:4dd0:a000...	2a00:20:b004:2c11:2a10:782f:51e...	ICMP...	166	Time Exceeded (hop limit exceeded in tran
18	0.033449496	2001:4dd0:a000...	2a00:20:b004:2c11:2a10:782f:51e...	ICMP...	166	Time Exceeded (hop limit exceeded in tran
19	0.040326659	2001:4dd0:a000...	2a00:20:b004:2c11:2a10:782f:51e...	ICMP...	166	Time Exceeded (hop limit exceeded in tran
20	0.040326921	2001:4dd0:a000...	2a00:20:b004:2c11:2a10:782f:51e...	ICMP...	166	Time Exceeded (hop limit exceeded in tran
21	0.043376058	2001:4dd0:a000...	2a00:20:b004:2c11:2a10:782f:51e...	ICMP...	166	Time Exceeded (hop limit exceeded in tran
22	0.043376114	2001:4dd0:a000...	2a00:20:b004:2c11:2a10:782f:51e...	ICMP...	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.



The image shows a Wireshark packet capture window titled 'capture-icmp-flood.pcapng'. The interface includes a menu bar (Datei, Bearbeiten, Ansicht, Navigation, Aufzeichnen, Analyse, Statistiken, Telephonie, Wireless, Tools, Hilfe) and a toolbar. Below the toolbar is a search bar with the text 'Anzeigefilter anwenden ... <Ctrl-F>'. The main display area shows a table of network traffic with columns: No., Time, Source, Destination, Protocol, Length, and Info. The table contains multiple entries, all showing ICMP messages from source 2001:4dd0:a000... to destination 2a00:20:b004:2c11:2a10:782f:51e... with a protocol of ICMP and a length of 166. The 'Info' column for these packets indicates 'Time Exceeded (hop limit exceeded in tran'.

No.	Time	Source	Destination	Protocol	Length	Info
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
22	0.043376114	2001:4dd0:a000...	2a00:20:b004:2c11:2a10:782f:51e...	ICM...	166	Time Exceeded (hop limit exceeded in tran

Implications for active scanning:



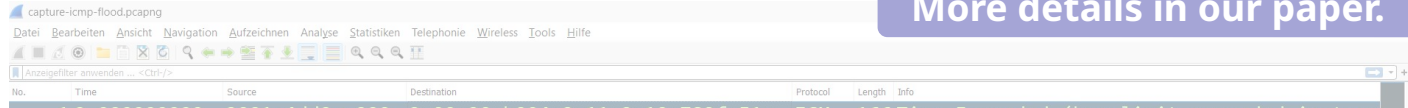
The image shows a diagram of a scanner (represented by a laptop icon) sending ICMP traffic to a network. The network is represented by a series of nodes connected by lines. The traffic is shown as a series of packets, each with a source and destination address. The source address is 2001:4dd0:a000... and the destination address is 2a00:20:b004:2c11:2a10:782f:51e... The traffic is labeled 'ICMP T'.

No.	Time	Source	Destination	Protocol	Length	Info
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
22	0.043376114	2001:4dd0:a000...	2a00:20:b004:2c11:2a10:782f:51e...	ICM...	166	Time Exceeded (hop limit exceeded in tran

Probed BGP Prefix: 2001:db8::/32

**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.](#)

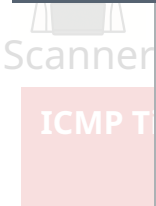


The image shows a Wireshark packet capture window titled 'capture-icmp-flood.pcapng'. The interface includes a menu bar (Datei, Bearbeiten, Ansicht, Navigation, Aufzeichnen, Analyse, Statistiken, Telefonie, Wireless, Tools, Hilfe) and a toolbar. Below the toolbar is a filter bar with 'Anzeigefilter anwenden ... <Ctrl-F>'. The main packet list table has columns for No., Time, Source, Destination, Protocol, Length, and Info. The first few rows of the table are visible, showing ICMP Echo (ping) requests from various sources to 2001:db8::32.

No.	Time	Source	Destination	Protocol	Length	Info
11	0.023861166	2001:4dd0:a000::2	2001:db8::32	ICMP	166	Time Exceeded (hop limit exceeded in transi...
12	0.023861222	2001:4dd0:a000::2	2001:db8::32	ICMP	166	Time Exceeded (hop limit exceeded in transi...
13	0.023861237	2001:4dd0:a000::2	2001:db8::32	ICMP	166	Time Exceeded (hop limit exceeded in transi...
14	0.023861269	2001:4dd0:a000::2	2001:db8::32	ICMP	166	Time Exceeded (hop limit exceeded in transi...
15	0.027820090	2001:4dd0:a000::2	2001:db8::32	ICMP	166	Time Exceeded (hop limit exceeded in transi...
16	0.027820136	2001:4dd0:a000::2	2001:db8::32	ICMP	166	Time Exceeded (hop limit exceeded in transi...
17	0.032142221	2001:4dd0:a000::2	2001:db8::32	ICMP	166	Time Exceeded (hop limit exceeded in transi...
18	0.033449496	2001:4dd0:a000::2	2001:db8::32	ICMP	166	Time Exceeded (hop limit exceeded in transi...
19	0.040326659	2001:4dd0:a000::2	2001:db8::32	ICMP	166	Time Exceeded (hop limit exceeded in transi...
20	0.040326921	2001:4dd0:a000::2	2001:db8::32	ICMP	166	Time Exceeded (hop limit exceeded in transi...
21	0.043376058	2001:4dd0:a000::2	2001:db8::32	ICMP	166	Time Exceeded (hop limit exceeded in transi...
22	0.043376114	2001:4dd0:a000::2	2001:db8::32	ICMP	166	Time Exceeded (hop limit exceeded in transi...

Implications for active scanning:

1. Exclude networks that lead to routing loops



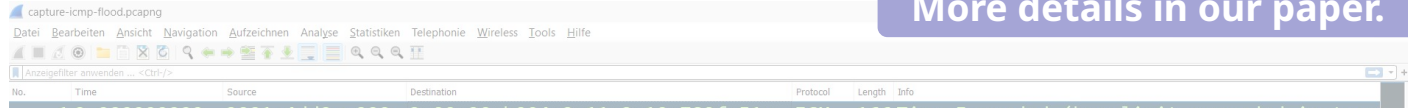
The diagram shows a 'Scanner' connected to a router. The router is labeled 'ICMP T' and has a red box next to it. The router is connected to a network of nodes, represented by a grid of dots. The nodes are labeled with IP addresses and the text 'Time Exceeded (hop limit exceeded in transi...'. The router is also labeled 'Probed BGP Prefix: 2001:db8::/32'.

```
11 0.023861166 2001:4dd0:a000::2 2001:db8::32 ICMP... 166 Time Exceeded (hop limit exceeded in tran
12 0.023861222 2001:4dd0:a000::2 2001:db8::32 ICMP... 166 Time Exceeded (hop limit exceeded in tran
13 0.023861237 2001:4dd0:a000::2 2001:db8::32 ICMP... 166 Time Exceeded (hop limit exceeded in tran
14 0.023861269 2001:4dd0:a000::2 2001:db8::32 ICMP... 166 Time Exceeded (hop limit exceeded in tran
15 0.027820090 2001:4dd0:a000::2 2001:db8::32 ICMP... 166 Time Exceeded (hop limit exceeded in tran
16 0.027820136 2001:4dd0:a000::2 2001:db8::32 ICMP... 166 Time Exceeded (hop limit exceeded in tran
17 0.032142221 2001:4dd0:a000::2 2001:db8::32 ICMP... 166 Time Exceeded (hop limit exceeded in tran
18 0.033449496 2001:4dd0:a000::2 2001:db8::32 ICMP... 166 Time Exceeded (hop limit exceeded in tran
19 0.040326659 2001:4dd0:a000::2 2001:db8::32 ICMP... 166 Time Exceeded (hop limit exceeded in tran
20 0.040326921 2001:4dd0:a000::2 2001:db8::32 ICMP... 166 Time Exceeded (hop limit exceeded in tran
21 0.043376058 2001:4dd0:a000::2 2001:db8::32 ICMP... 166 Time Exceeded (hop limit exceeded in tran
22 0.043376114 2001:4dd0:a000::2 2001:db8::32 ICMP... 166 Time Exceeded (hop limit exceeded in tran
```

Probed BGP Prefix: 2001:db8::/32

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.](#)



The image shows a Wireshark packet capture window titled 'capture-icmp-flood.pcapng'. The interface includes a menu bar (Datei, Bearbeiten, Ansicht, Navigation, Aufzeichnen, Analyse, Statistiken, Telefonie, Wireless, Tools, Hilfe) and a toolbar. Below the toolbar is a filter bar with 'Anzeigefilter anwenden ... <Ctrl-F>'. The main packet list table has columns for No., Time, Source, Destination, Protocol, Length, and Info. The first few rows of the table are visible, showing ICMP Echo (ping) requests from various sources to 2001:db8::32.

No.	Time	Source	Destination	Protocol	Length	Info
11	0.023861166	2001:4dd0:a000::2	2a00:20:b004:2c11:2a10:782f:51e...	ICMP...	166	Time Exceeded (hop limit exceeded in tran
12	0.023861222	2001:4dd0:a000::2	2a00:20:b004:2c11:2a10:782f:51e...	ICMP...	166	Time Exceeded (hop limit exceeded in tran
13	0.023861237	2001:4dd0:a000::2	2a00:20:b004:2c11:2a10:782f:51e...	ICMP...	166	Time Exceeded (hop limit exceeded in tran
14	0.023861269	2001:4dd0:a000::2	2a00:20:b004:2c11:2a10:782f:51e...	ICMP...	166	Time Exceeded (hop limit exceeded in tran
15	0.027820090	2001:4dd0:a000::2	2a00:20:b004:2c11:2a10:782f:51e...	ICMP...	166	Time Exceeded (hop limit exceeded in tran
16	0.027820136	2001:4dd0:a000::2	2a00:20:b004:2c11:2a10:782f:51e...	ICMP...	166	Time Exceeded (hop limit exceeded in tran
17	0.032142221	2001:4dd0:a000::2	2a00:20:b004:2c11:2a10:782f:51e...	ICMP...	166	Time Exceeded (hop limit exceeded in tran
18	0.033449496	2001:4dd0:a000::2	2a00:20:b004:2c11:2a10:782f:51e...	ICMP...	166	Time Exceeded (hop limit exceeded in tran
19	0.040326659	2001:4dd0:a000::2	2a00:20:b004:2c11:2a10:782f:51e...	ICMP...	166	Time Exceeded (hop limit exceeded in tran
20	0.040326921	2001:4dd0:a000::2	2a00:20:b004:2c11:2a10:782f:51e...	ICMP...	166	Time Exceeded (hop limit exceeded in tran
21	0.043376058	2001:4dd0:a000::2	2a00:20:b004:2c11:2a10:782f:51e...	ICMP...	166	Time Exceeded (hop limit exceeded in tran
22	0.043376114	2001:4dd0:a000::2	2a00:20:b004:2c11:2a10:782f:51e...	ICMP...	166	Time Exceeded (hop limit exceeded in tran

Implications for active scanning:

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

Scanner

ICMP T

```
11 0.023861166 2001:4dd0:a000::2 2a00:20:b004:2c11:2a10:782f:51e... ICMP... 166 Time Exceeded (hop limit exceeded in tran
12 0.023861222 2001:4dd0:a000::2 2a00:20:b004:2c11:2a10:782f:51e... ICMP... 166 Time Exceeded (hop limit exceeded in tran
13 0.023861237 2001:4dd0:a000::2 2a00:20:b004:2c11:2a10:782f:51e... ICMP... 166 Time Exceeded (hop limit exceeded in tran
14 0.023861269 2001:4dd0:a000::2 2a00:20:b004:2c11:2a10:782f:51e... ICMP... 166 Time Exceeded (hop limit exceeded in tran
15 0.027820090 2001:4dd0:a000::2 2a00:20:b004:2c11:2a10:782f:51e... ICMP... 166 Time Exceeded (hop limit exceeded in tran
16 0.027820136 2001:4dd0:a000::2 2a00:20:b004:2c11:2a10:782f:51e... ICMP... 166 Time Exceeded (hop limit exceeded in tran
17 0.032142221 2001:4dd0:a000::2 2a00:20:b004:2c11:2a10:782f:51e... ICMP... 166 Time Exceeded (hop limit exceeded in tran
18 0.033449496 2001:4dd0:a000::2 2a00:20:b004:2c11:2a10:782f:51e... ICMP... 166 Time Exceeded (hop limit exceeded in tran
19 0.040326659 2001:4dd0:a000::2 2a00:20:b004:2c11:2a10:782f:51e... ICMP... 166 Time Exceeded (hop limit exceeded in tran
20 0.040326921 2001:4dd0:a000::2 2a00:20:b004:2c11:2a10:782f:51e... ICMP... 166 Time Exceeded (hop limit exceeded in tran
21 0.043376058 2001:4dd0:a000::2 2a00:20:b004:2c11:2a10:782f:51e... ICMP... 166 Time Exceeded (hop limit exceeded in tran
22 0.043376114 2001:4dd0:a000::2 2a00:20:b004:2c11:2a10:782f:51e... ICMP... 166 Time Exceeded (hop limit exceeded in tran
```

Probed BGP Prefix: 2001:db8::/32

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>

