RIPE NCC
RIPE NETWORK COORDINATION CENTRE

IP Blocklisting Basics

1 hour

RIPE NCC Learning & Development

v26.1


This session is
being recorded

Goals

- Explain **why** an IP address can get blocklisted
- **Prevent** IP address blocks from being blocklisted
- **Remove** IP addresses from blocklists using specific techniques
- Implement **best practices** for preventing IP addresses from being blocklisted



Agenda

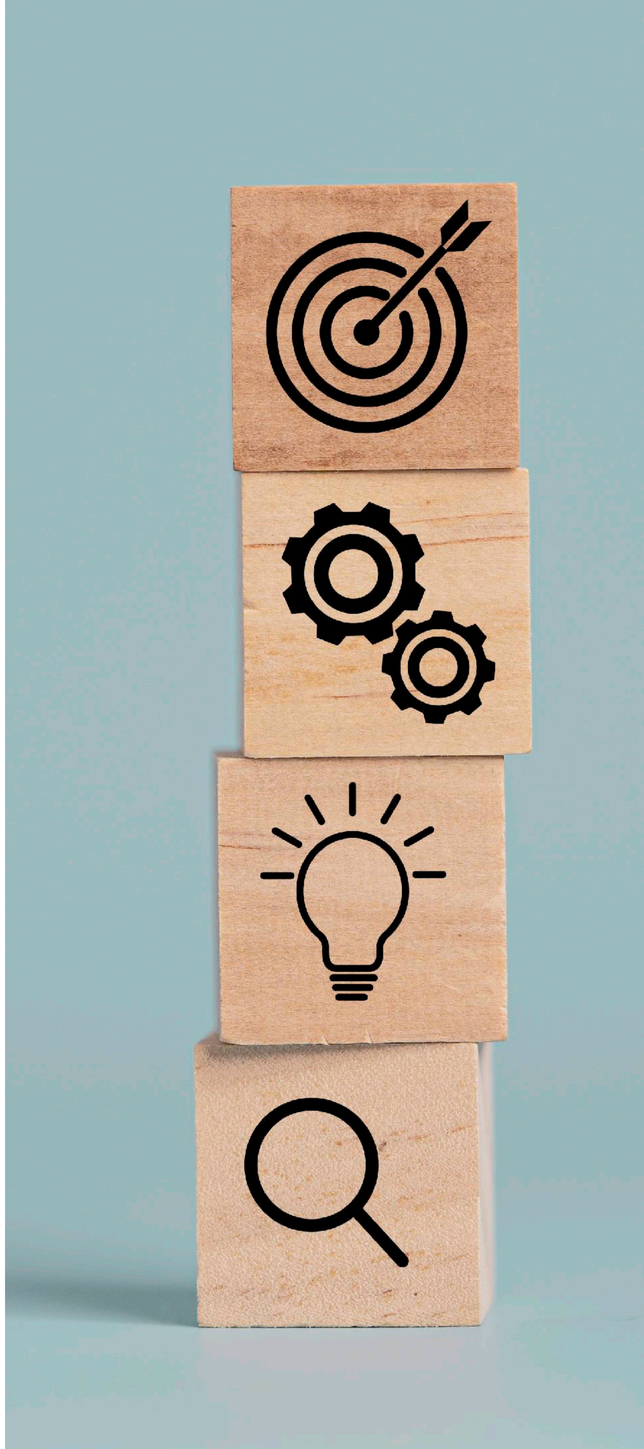
1. Internet, IPs, ASNs, Routing, etc.

2. IP and ASN Blocklists

3-7. How and why an IP prefix or ASN can be blocklisted

8-9. Best Practices:

- How to prevent IPs and ASNs from being blocklisted
- How to remove IPs and ASNs from blocklists

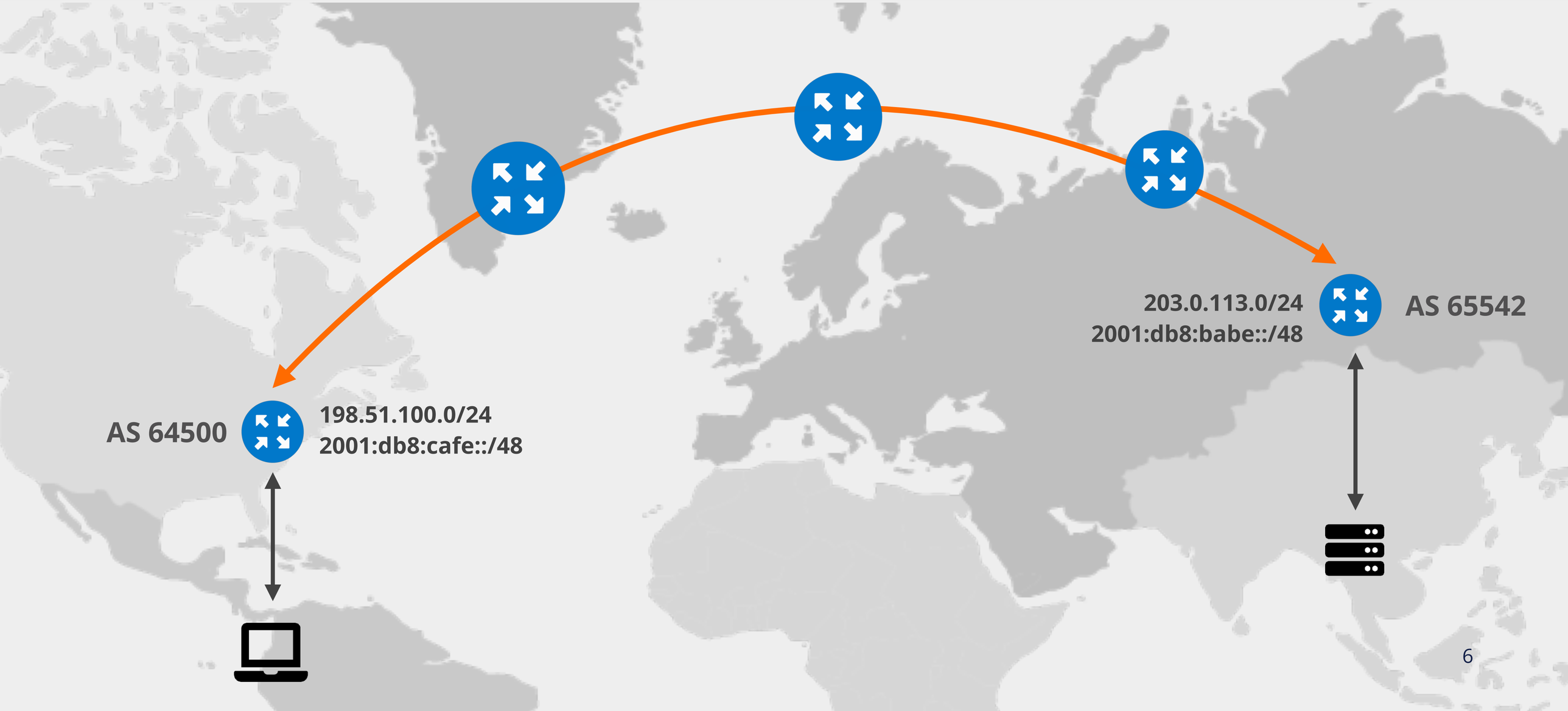




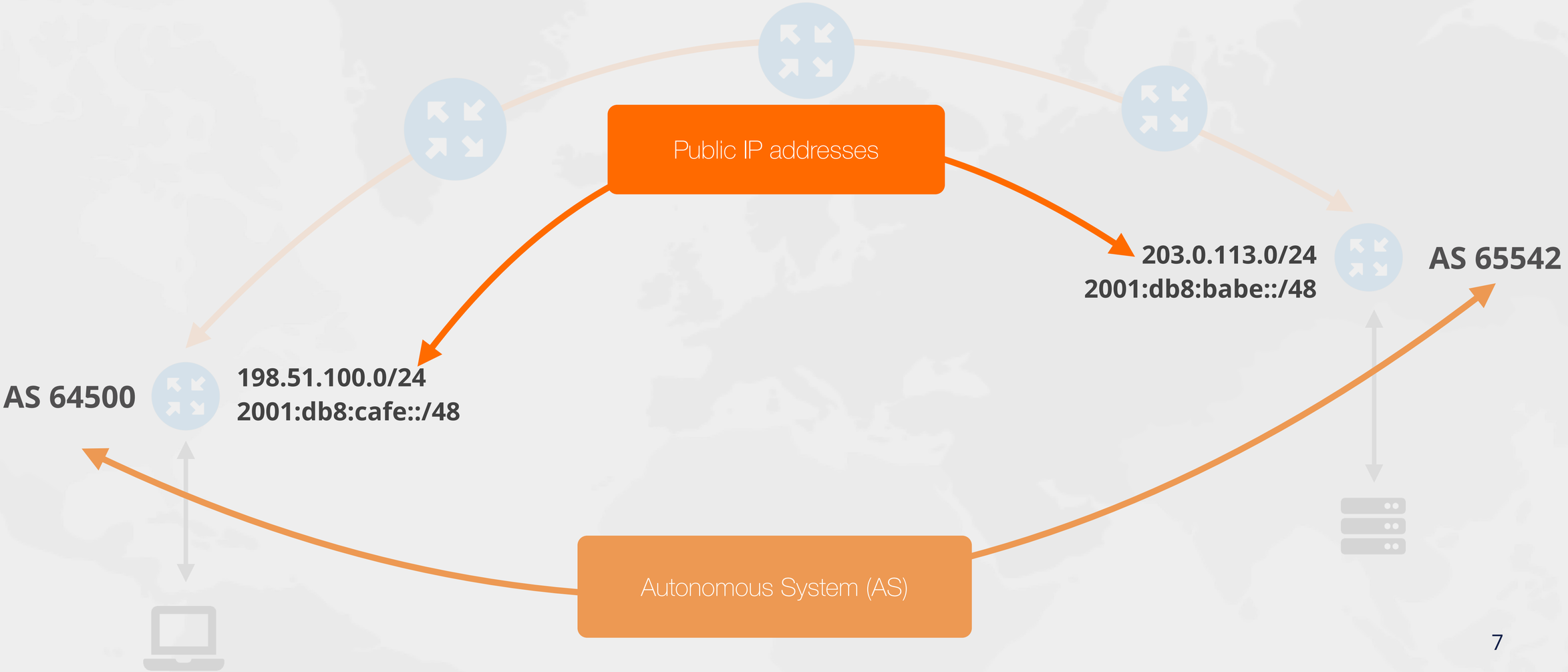
Internet, IPs, ASNs, etc.

Section 1 of 9

How do we address nodes on the Internet?



Focus on these numbers:

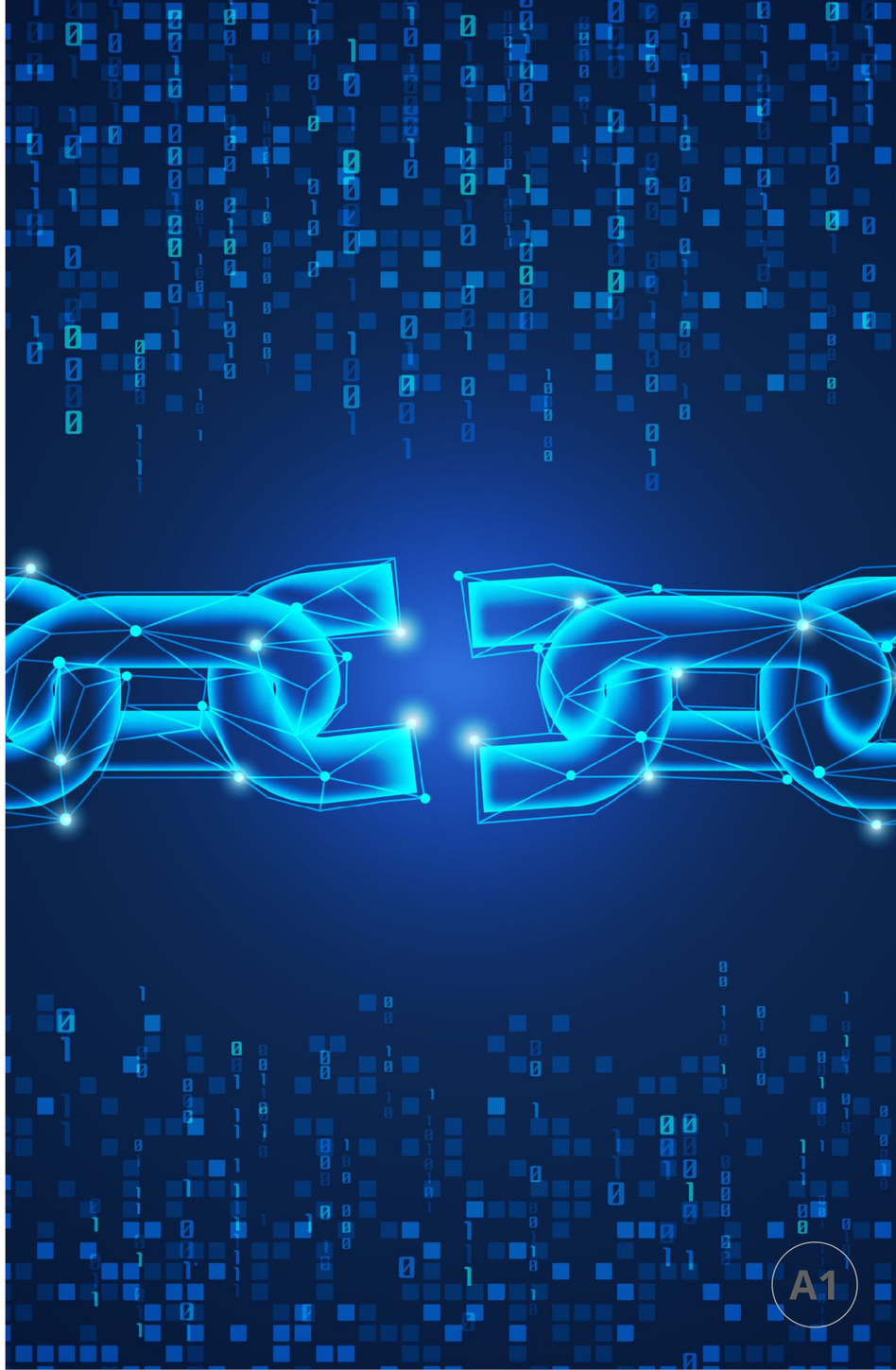


What can go wrong?

How can somebody **abuse** or **misuse** resources on the Internet?

Choose all possible situations in the poll, and tell us your experience in the chat window.

1 min.



IANA and the 5 Regional Internet Registries (RIRs)



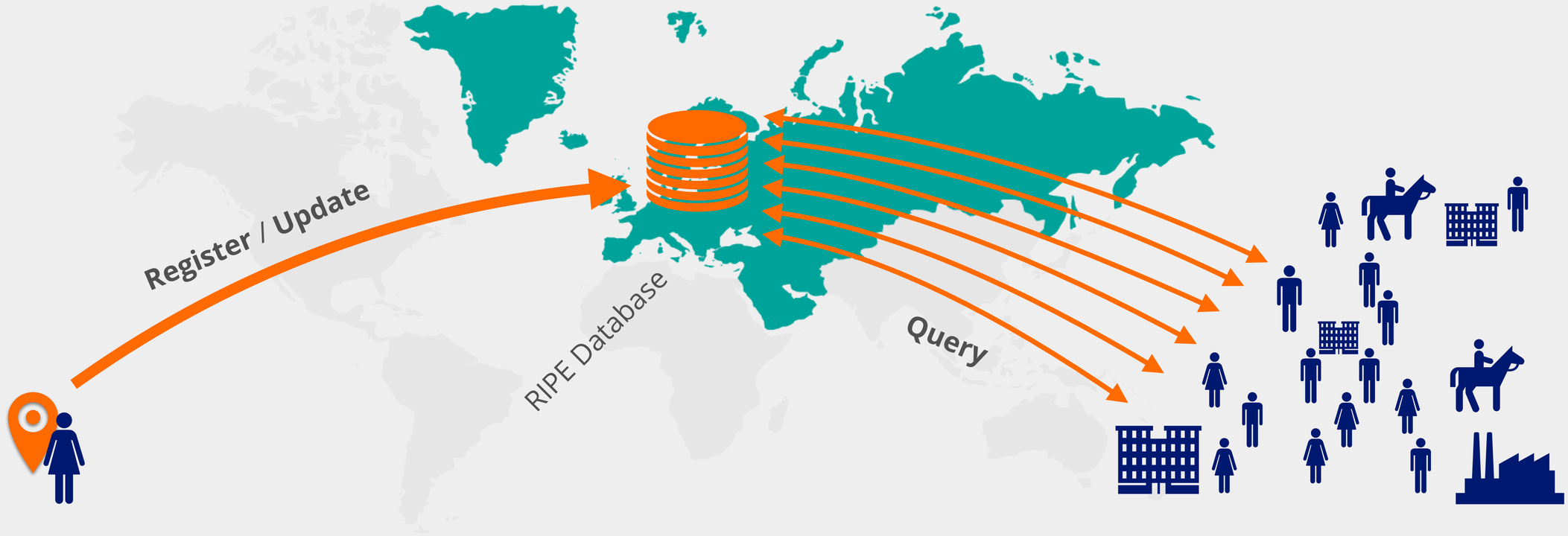
The RIPE NCC and its 20k+ LIRs



Local Internet Registries (LIRs) are responsible for:

- Distributing Internet Number resources (IP addresses and ASNs) **to End Users**
- Registering them in the **RIPE Database**
- Keeping the registry up-to-date

The Big Picture



The legitimate holder
(the RIPE NCC, LIR, etc.)
registers their assignments,
(sub)-allocations, and ASNs.

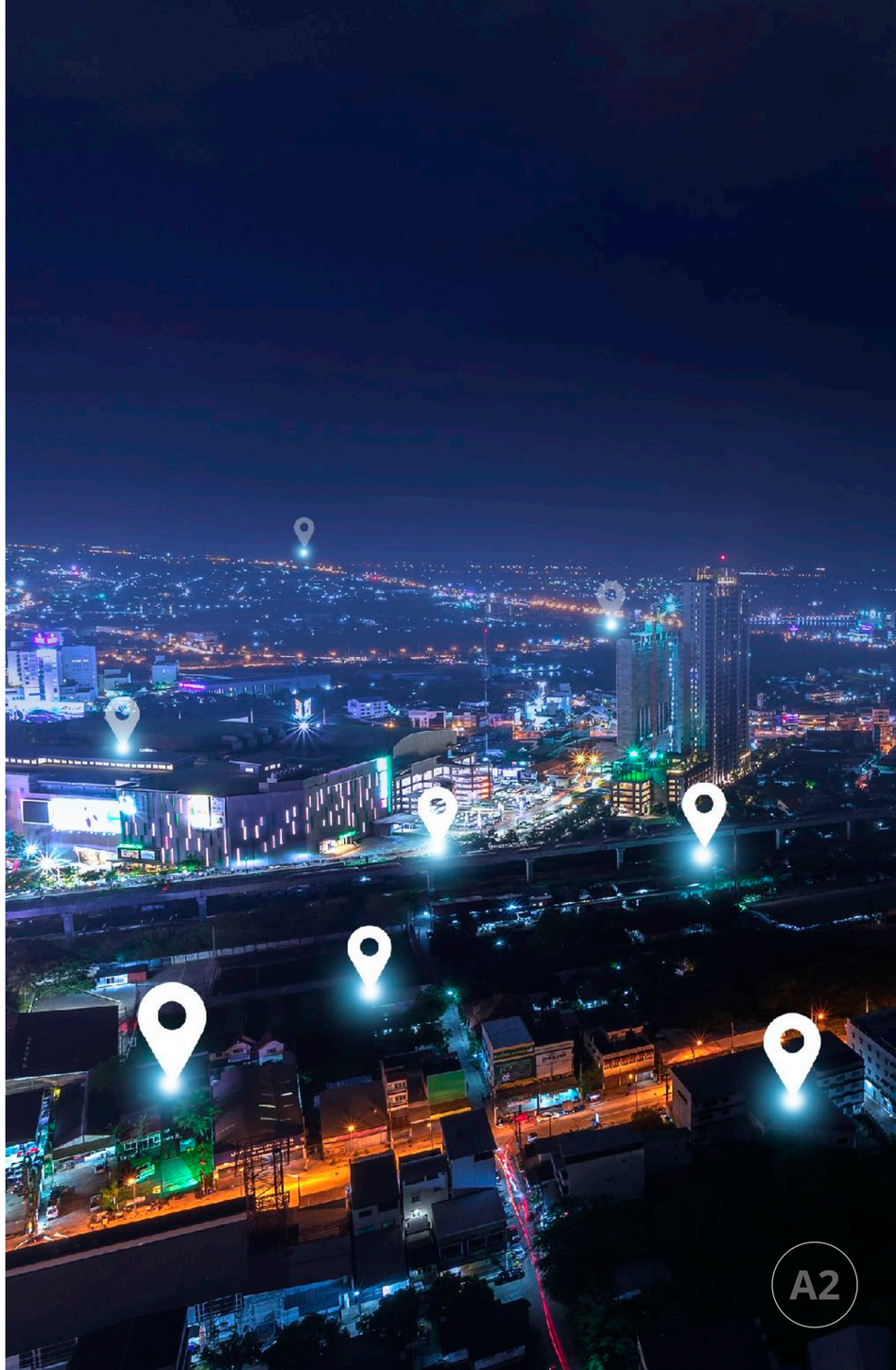
Other Internet users or ISPs
can query who is the legitimate
holder of a resource.

Can AS 3333 announce 193.0.0.0/24?

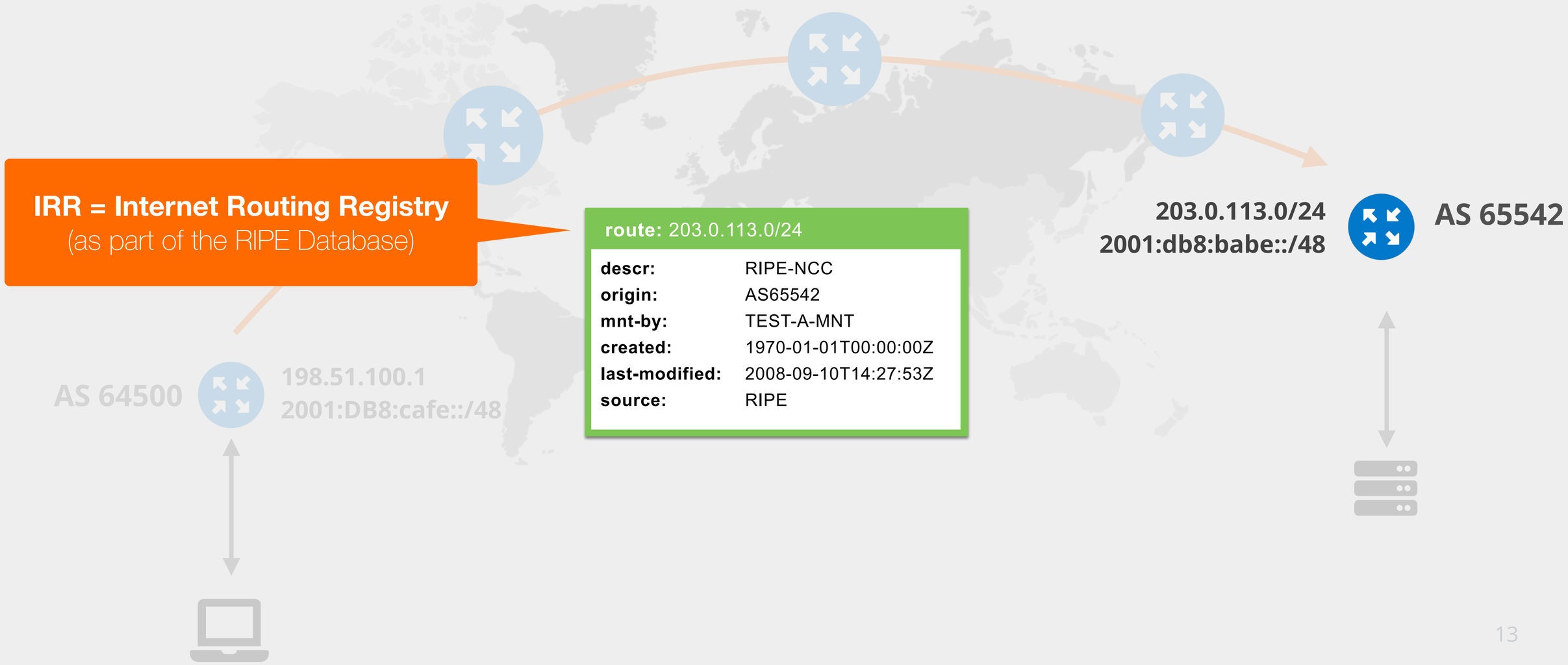
- **AS 3333** is assigned to the ORG-RIEN1-RIPE
- **193.0.0.0/24** is also assigned to ORG-RIEN1-RIPE

Please choose the correct answer.

1 min.



The prefix holder can create a ROUTE object!



For legitimate prefix holders…

Why is registering ROUTE objects **important** for the stability of the Internet?

Hint: which AS is allowed to announce **2001:67c:64::/48**?

Please choose your answer, and type in the answer for BONUS in the chat window.

1 min.

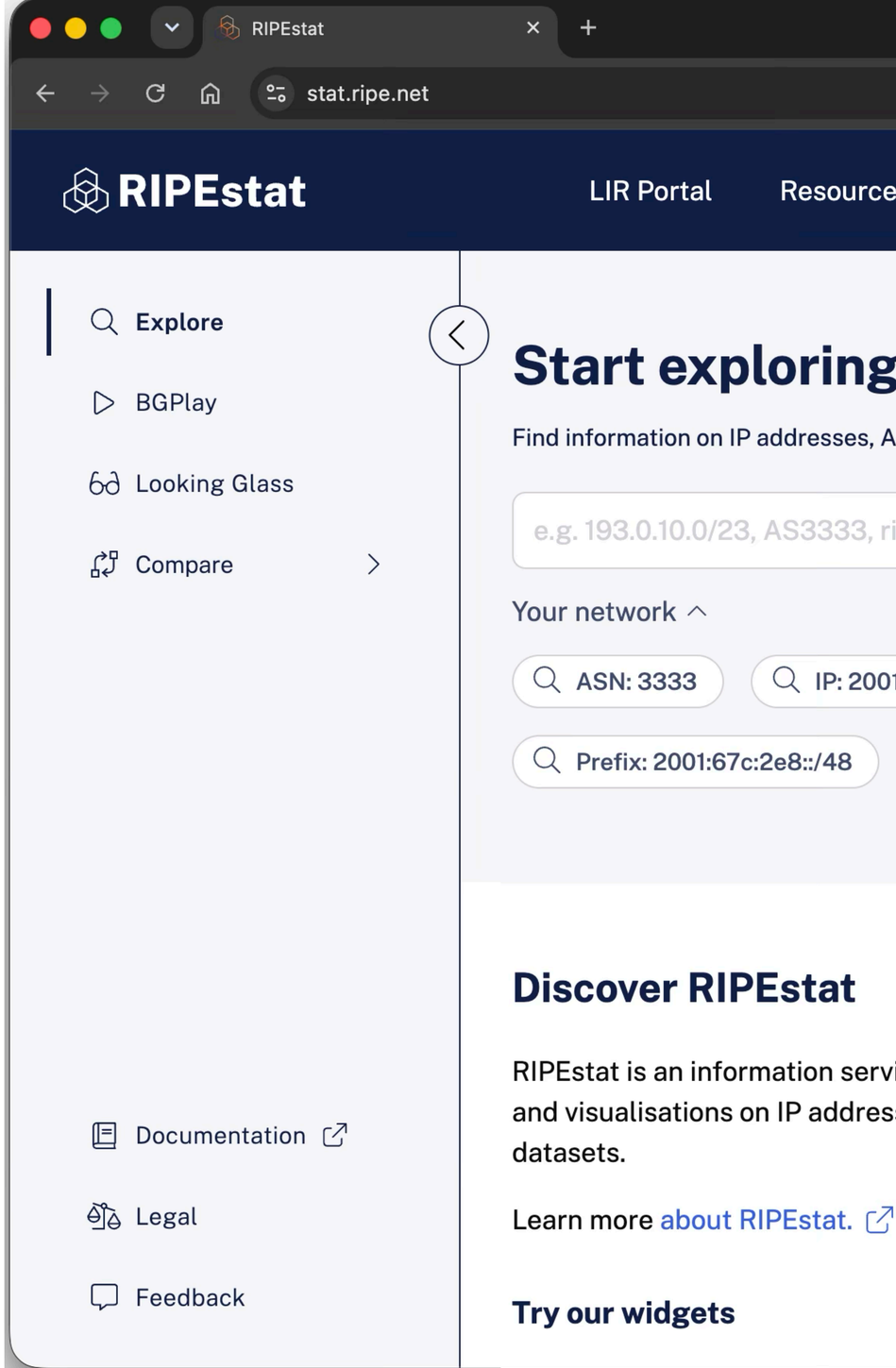


A3

Let’s investigate a prefix

Which network shall we investigate?

Demo

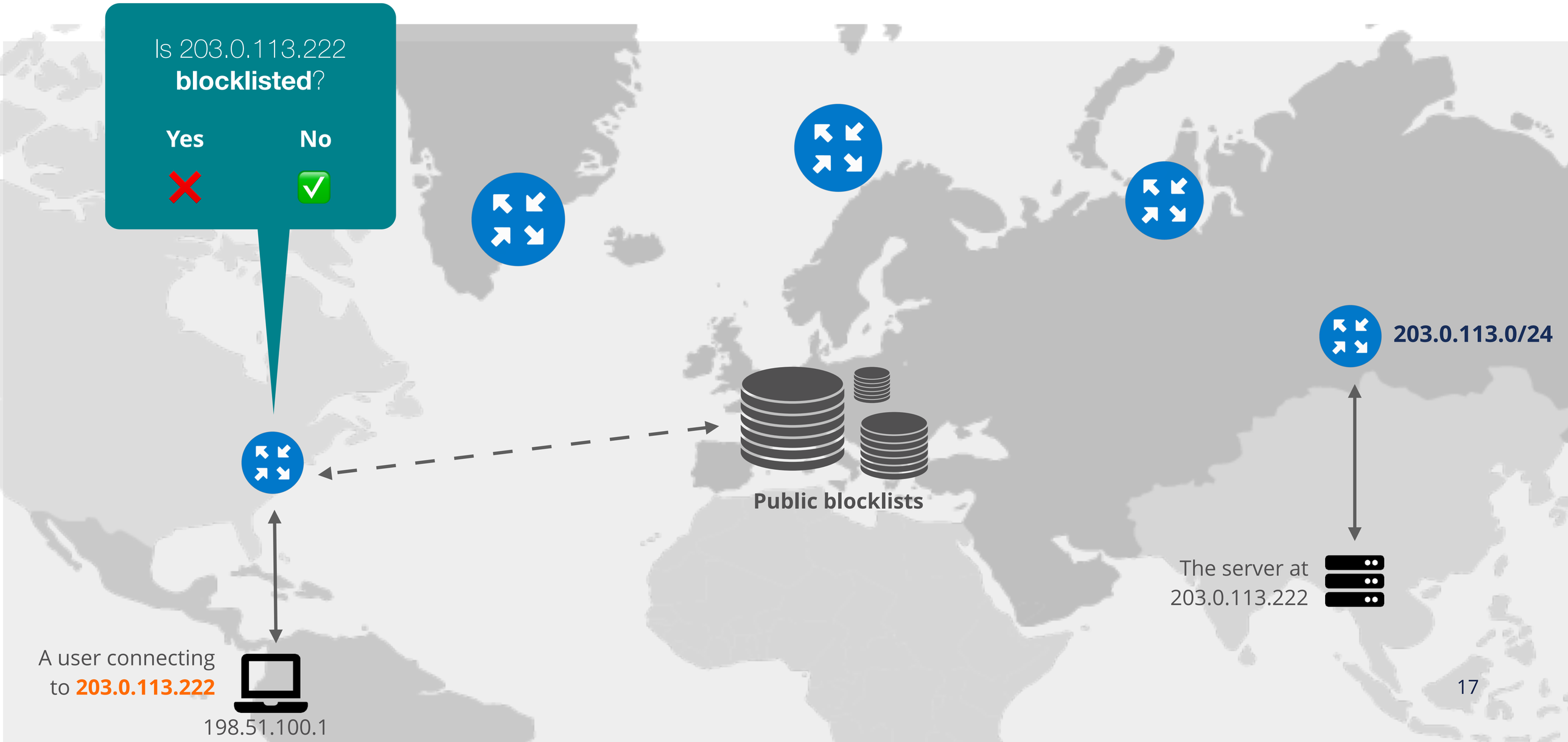




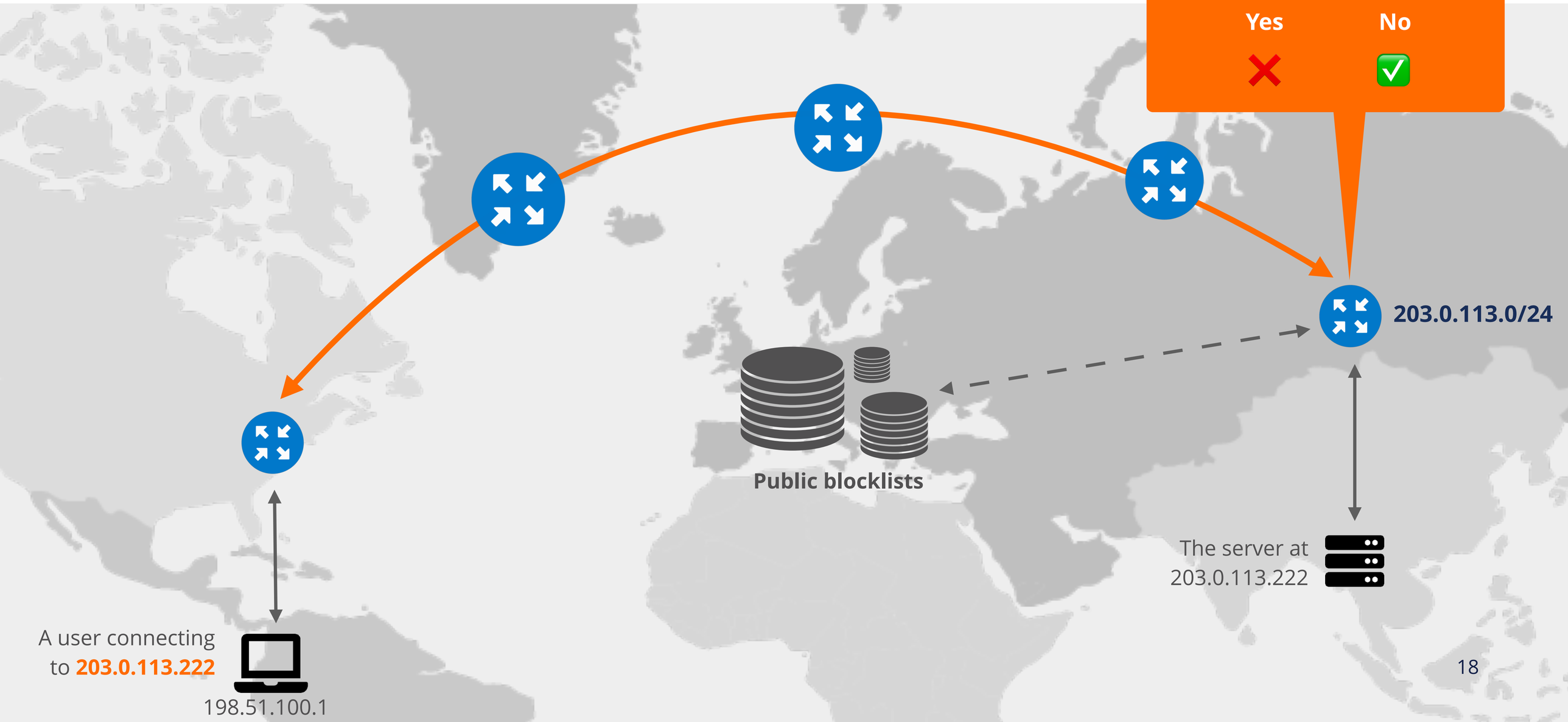
Our Focus: Blocklisting

Section 2 of 9

IP Blocklisting in Action



IP Blocklisting in Action



Tell us your experience

Have you ever **blocklisted anybody**, or were blocklisted **yourself**?

Please choose your answer, or type it in the chat window

1 min.



Blocklists can be private and public

1. Administrators have full control over a **private blocklist** (e.g. ACLs)
2. **Public blocklists** have different policies for how IPs/ASNs are added and removed

We're going to focus on **PUBLIC** blocklists

SPAMHAUS

spamcop.net

invaluement

CBL COMPOSITE BLOCKING LIST

Return Path

SBL Advisory

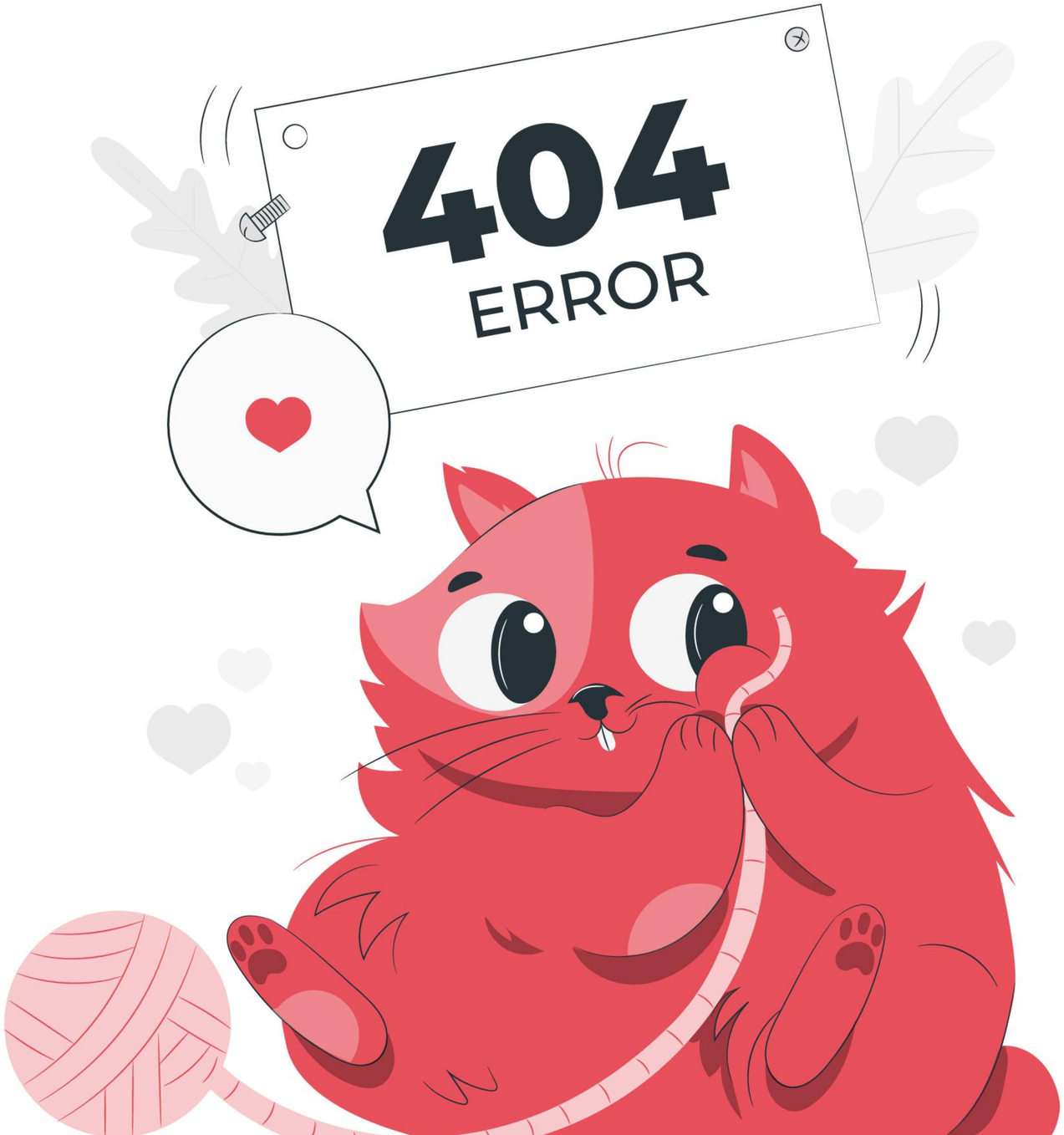
Barracuda

XBL Advisory

Passive Spam Block List (**PSBL**)

.. and many more

So… How somebody might end up on a blocklist?





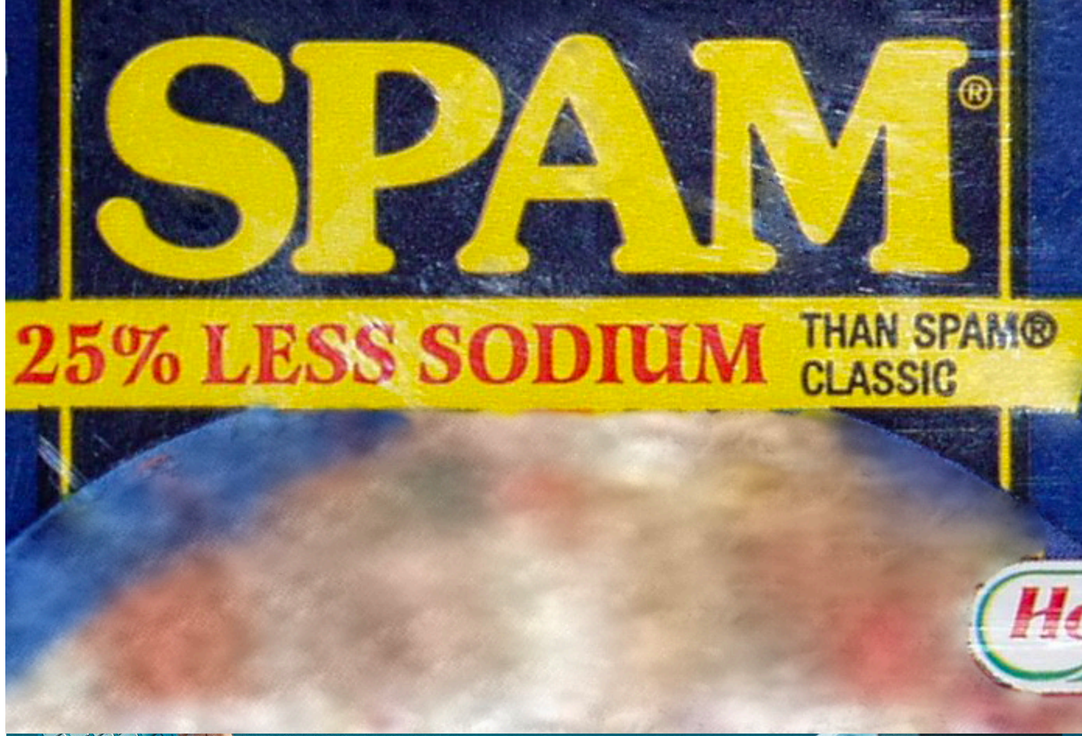
Reason #1: Spam

Section 3 of 9

What is Spam?

There are many names for **unsolicited** messages sent **in bulk by email**:

- Email **spam**
- **Junk** emails
- **UBE** = Unsolicited Bulk Email





Why spamming is unacceptable

- **Interferes** with the operation of the Internet
- Creates **unwanted traffic** for the recipients
- Creates **support overhead** for ISPs

There is no global framework regulating spamming.



What would you do?

You’re a system administrator of a small company with no extra budget to spend on IT.

One day, your colleagues start receiving **dozens of weird emails** from a foreign prince asking you for help to retrieve his fortune.

What would you do?

Please choose your answers, or type them in the chat window

1 min.



But the prince might have spoofed the sender’s IP address…

How would you check who is the **legitimate holder** of an IP address?

Please choose the correct options.

1 min.



A6



Reason #2: Misconfigurations

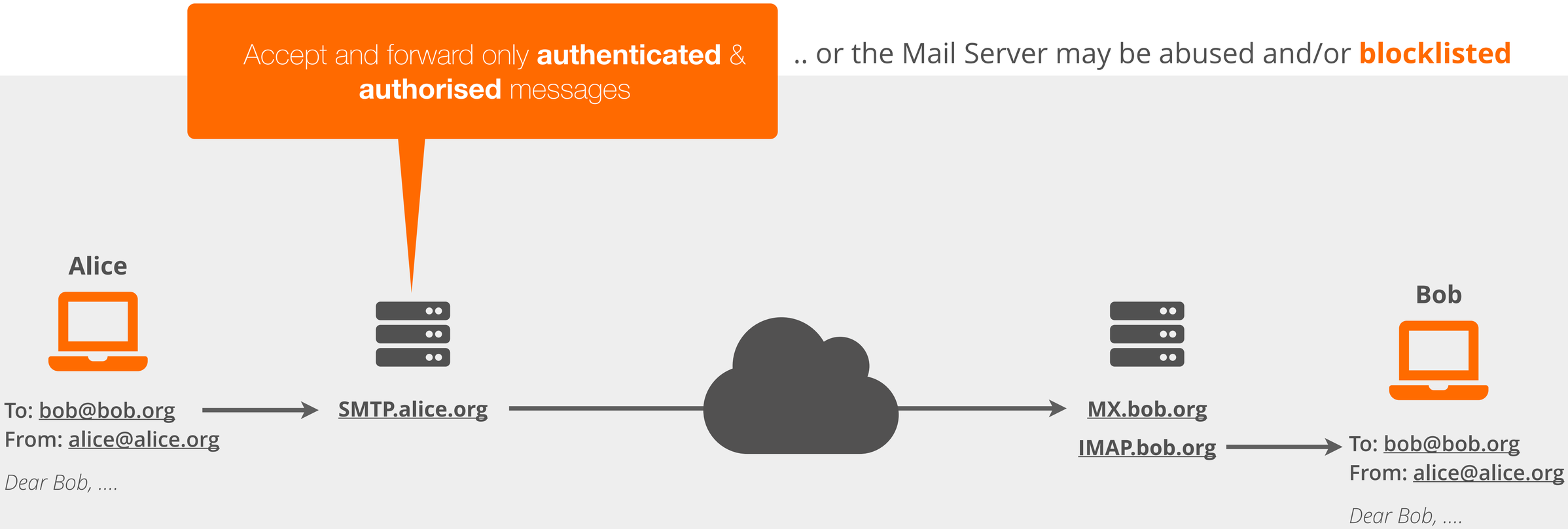
Section 4 of 9

Can wrongdoing be unintentional?



Open Mail Relay: anybody can abuse it!

- Open Mail Relays are NOT recommended by RFC 5321 (which defines SMTP)

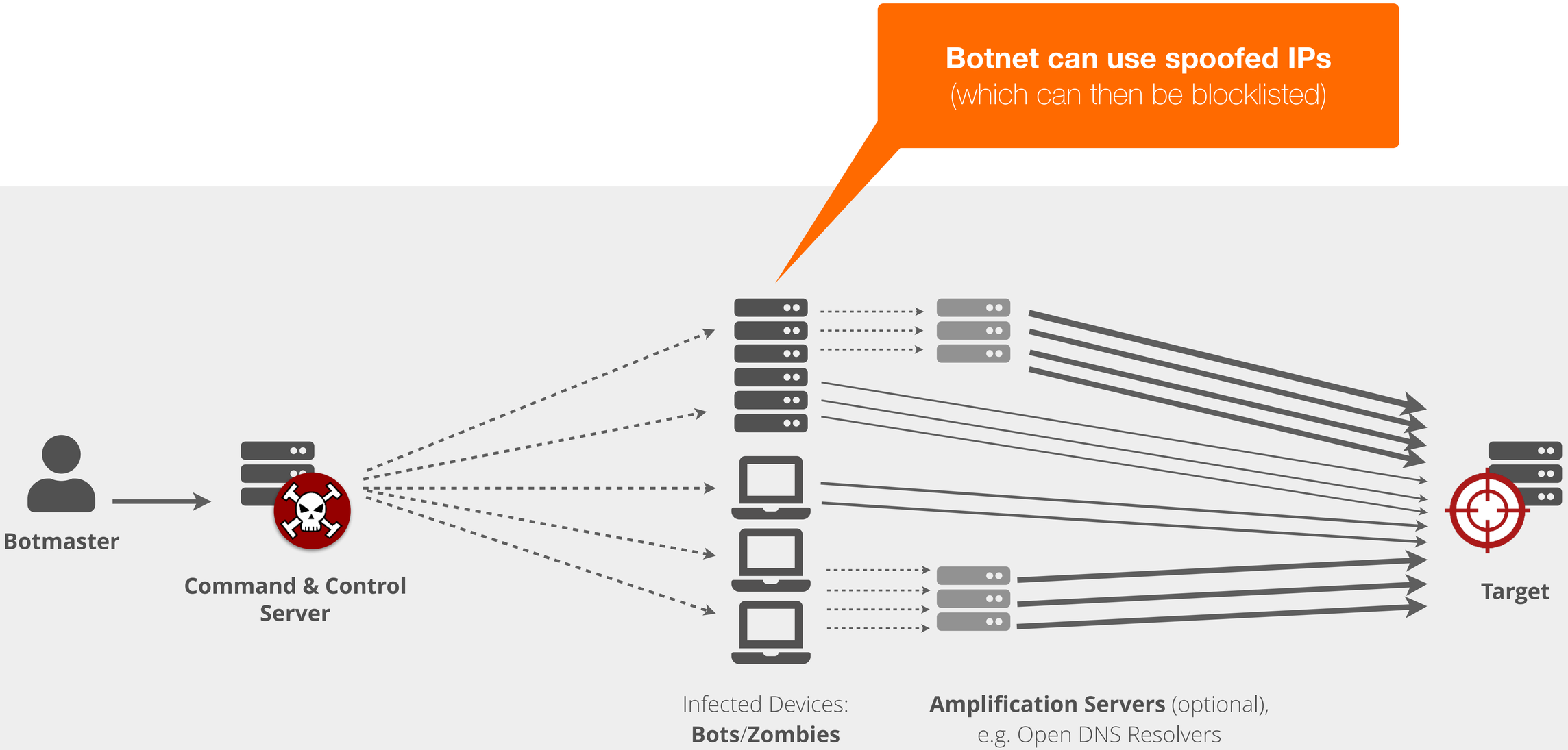




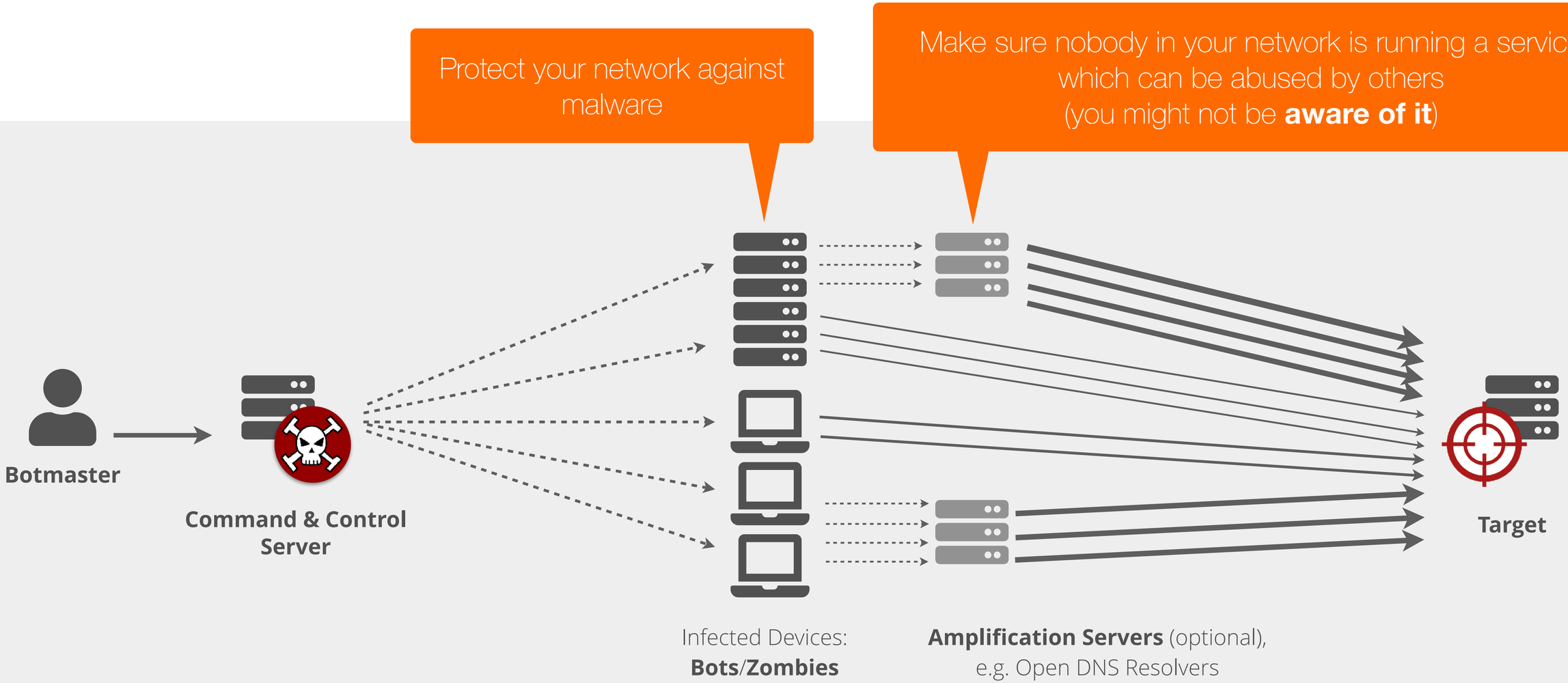
Reason #3: Malware and Botnets

Section 5 of 9

What is a botnet?



How to avoid being blocklisted?



What would you do..

.. if you were an ISP, and one of your customers insisted on running a service that could be **abused** by others?

Please choose your answer, or type in your answer in the chat widow

1 min.

```
⌥⌘1                    telnet
telnet ◂ -zsh

Last login: Wed May 19 15:15:52 on ttys000
user@computer-pro ~ % telnet smtp.example.com 25
Trying 192.168.100.25.
Connected to smtp.example.com.
Escape character is '^]'
220 smtp.example.com ESMTP Sendmail 8.12.9/8.12.9; Wed, 19 May 202
```



A7



Reason #4: Unwanted content, service or software

Section 6 of 9

Example: Open Mail Relay

- .. is an SMTP server which allows **anybody** on the Internet to send emails through it

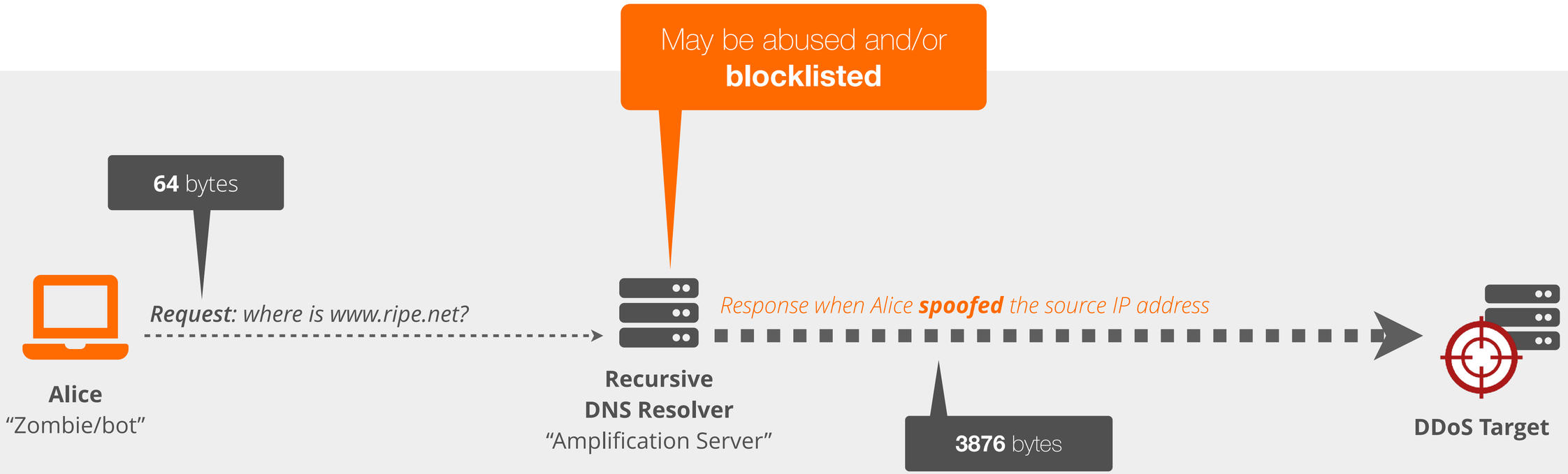


Can be abused by spammers!

- NOT recommended by RFC 5321 (defines SMTP)
- .. a valid reason for the server to be **blocklisted**

Example: Open Recursive DNS Resolver

- Can be used in a DNS amplification attack
- There are some public DNS servers: **1.1.1.1**, **8.8.8.8**, **2001:4860:4860::8888**

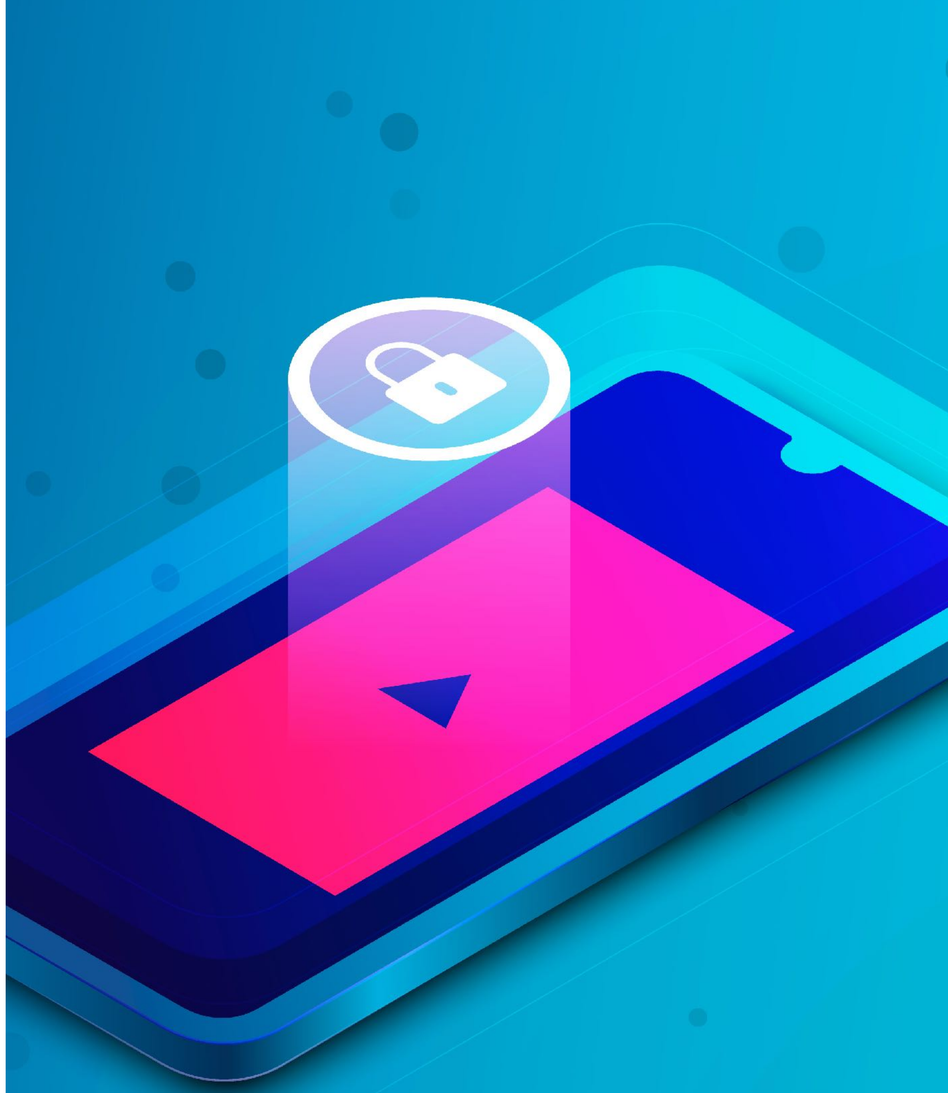


What can an ISP/LIR do...

.. to prevent IPs from being **blocklisted** due to undesirable content or services?

Please choose your answer, and share with us your experience in the chat window.

3 min.





Reason #5: IP prefix’s history

Section 7 of 9

You received a prefix …. there’re 2 options:



… all IPv4 prefixes come from **recycled** space

or

Or from **another region**
(member of another RIR)



… as a receiving LIR you might want to **investigate the prefix** before signing off the transfer

Previous holder’s actions may lead to your IP’s being **blocklisted**

How IP addresses are quarantined at the RIPE NCC

Step 1: **De-registration** → all related RIPE Database objects deleted, ROAs cleared

Step 2: **Quarantine** → for six months or as long as the space is globally routed

Step 3: **Allocation to a new LIR**

What exactly the RIPE NCC is doing during de-registration:
https://www.ripe.net/manage-ips-and-asns/resource-management/quarantine-for-returned-internet-number-resources

Resource Quality Assurance before re-allocating IP prefixes:
https://www.ripe.net/manage-ips-and-asns/resource-management/ripe-ncc-resource-quality-assistance

Use RIPEstat for transfers

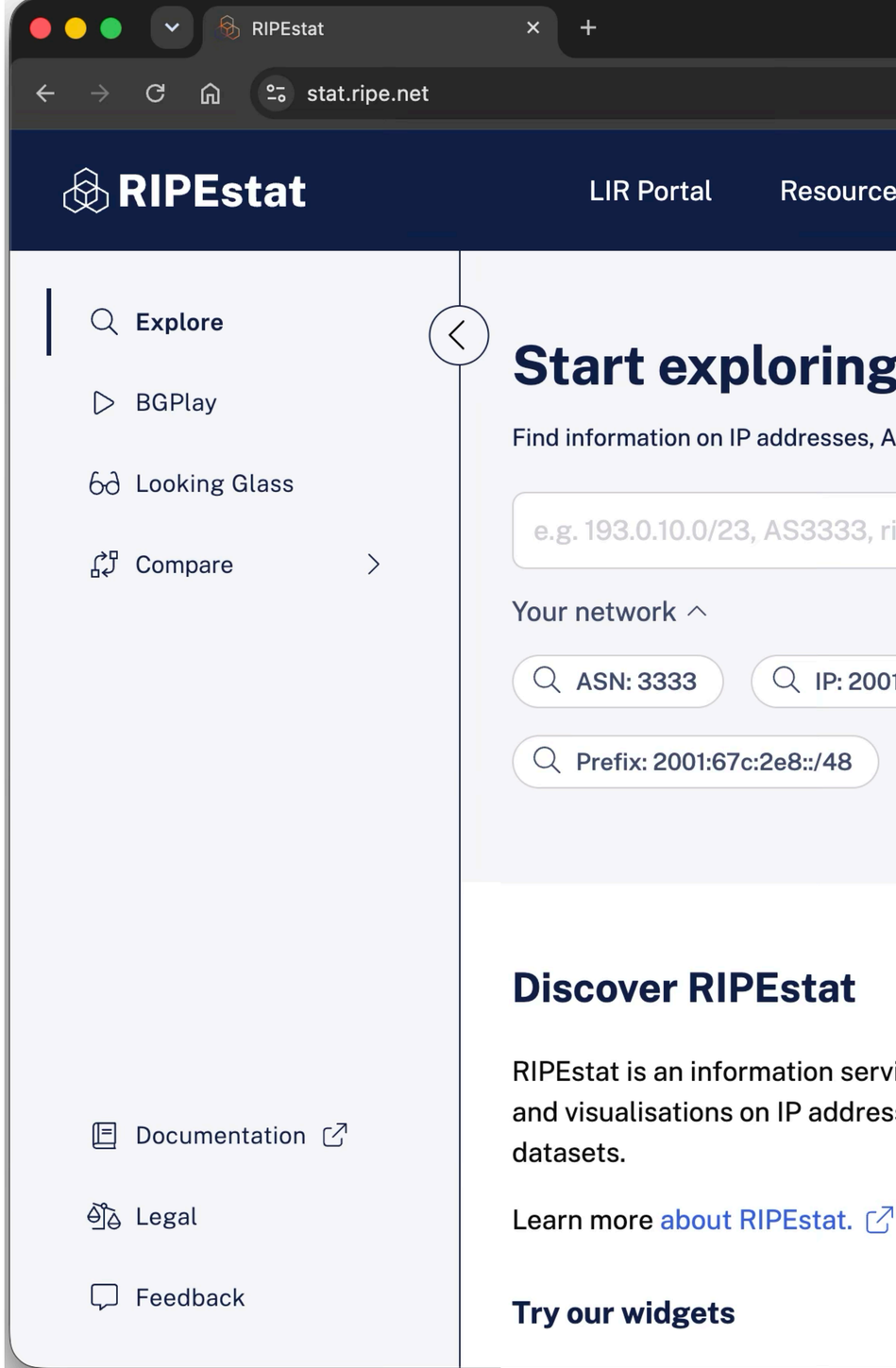
One of the services to use when investigating **the previous usage** of a prefix or ASN:

- Who was the legitimate holder in the past?
- Who was announcing the prefix in the past?

...

But there is **NO GUARANTEE**
that no changes will be detected after the transfer,
or after you just finished investigating

Demo



Questions



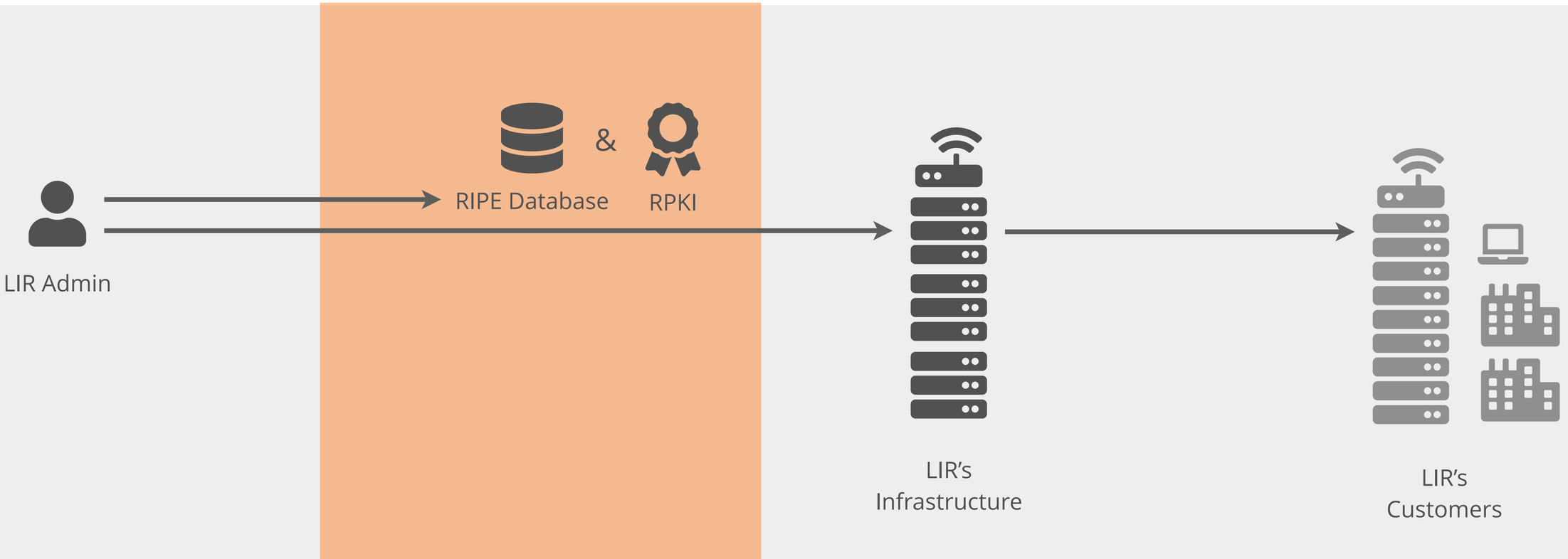


How to prevent IPs and ASNs from being blocklisted

Section 8 of 9

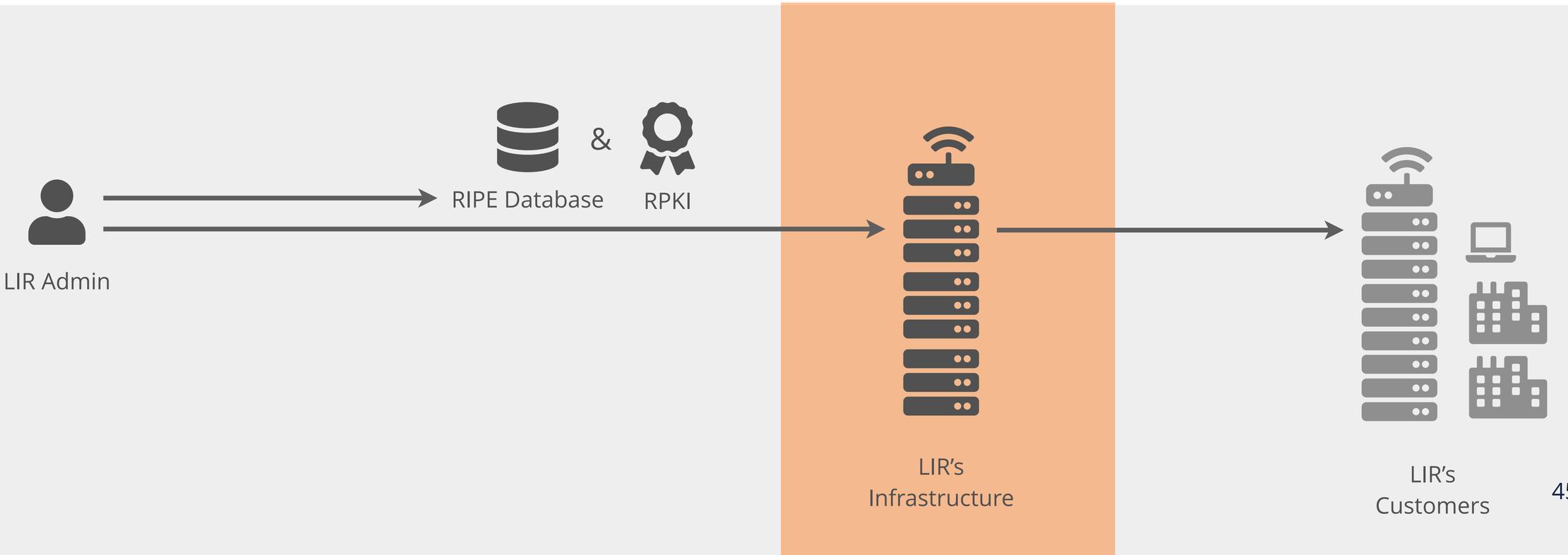
1. Know your infrastructure and customers

- Separate prefixes used for different services/networks/customers
- Separate the LIR’s prefix from the customer’s resources



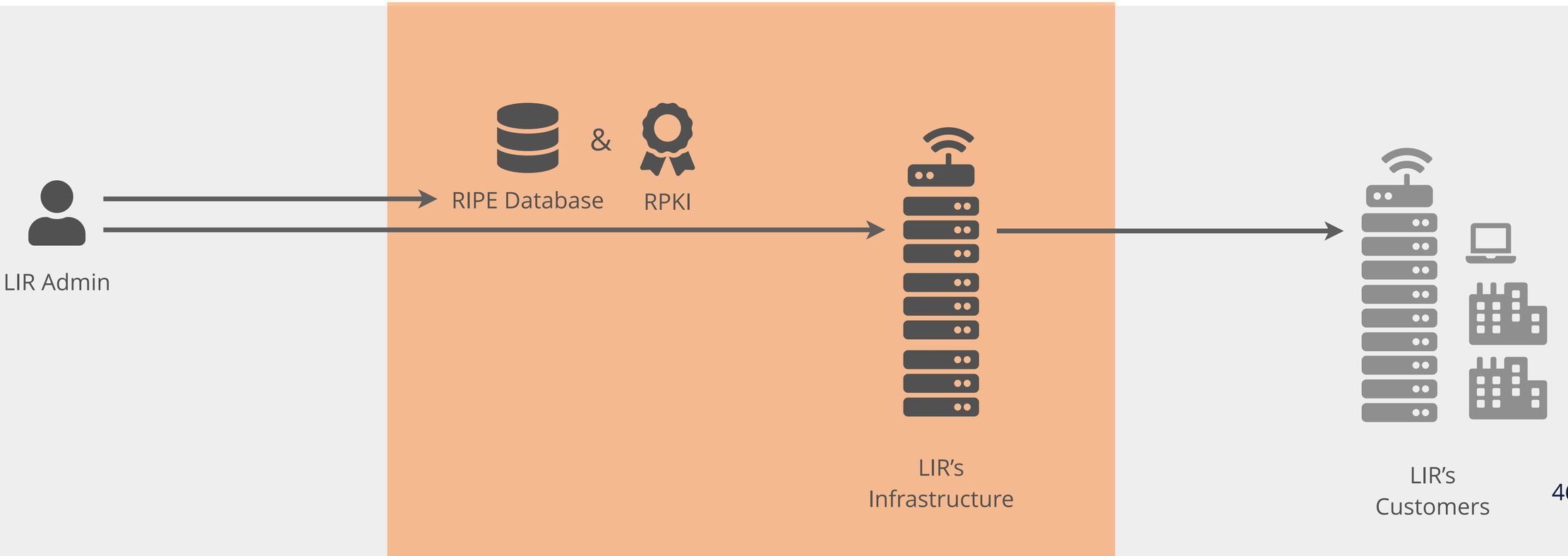
2. Implement proper security measures

- Follow RFC 5321 for mail servers
- Do not operate open DNS resolvers if possible
- Implement measures against amplification attacks, e.g. response rate-limiting



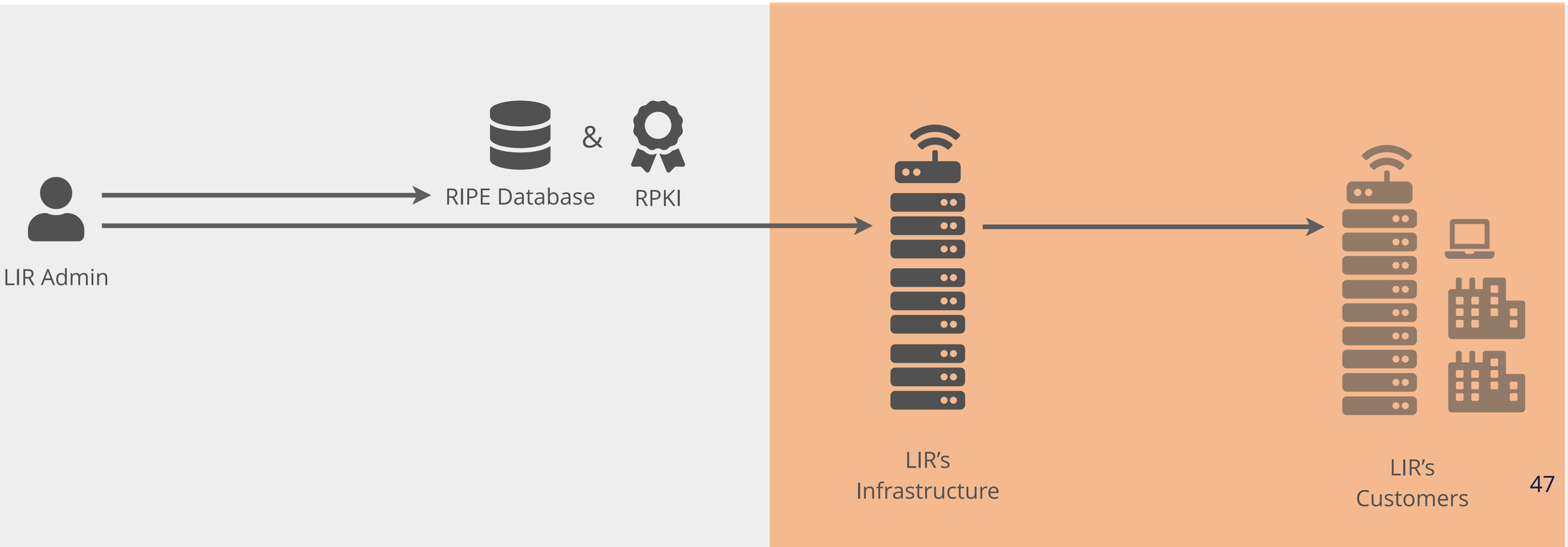
3. Prevent address space hijacking

- Maintain RIPE Database objects and keep them **up-to-date**
- Create **ROAs** for your prefixes
- Detect spoofed IP addresses in the ingress traffic: implement **BCP-38**



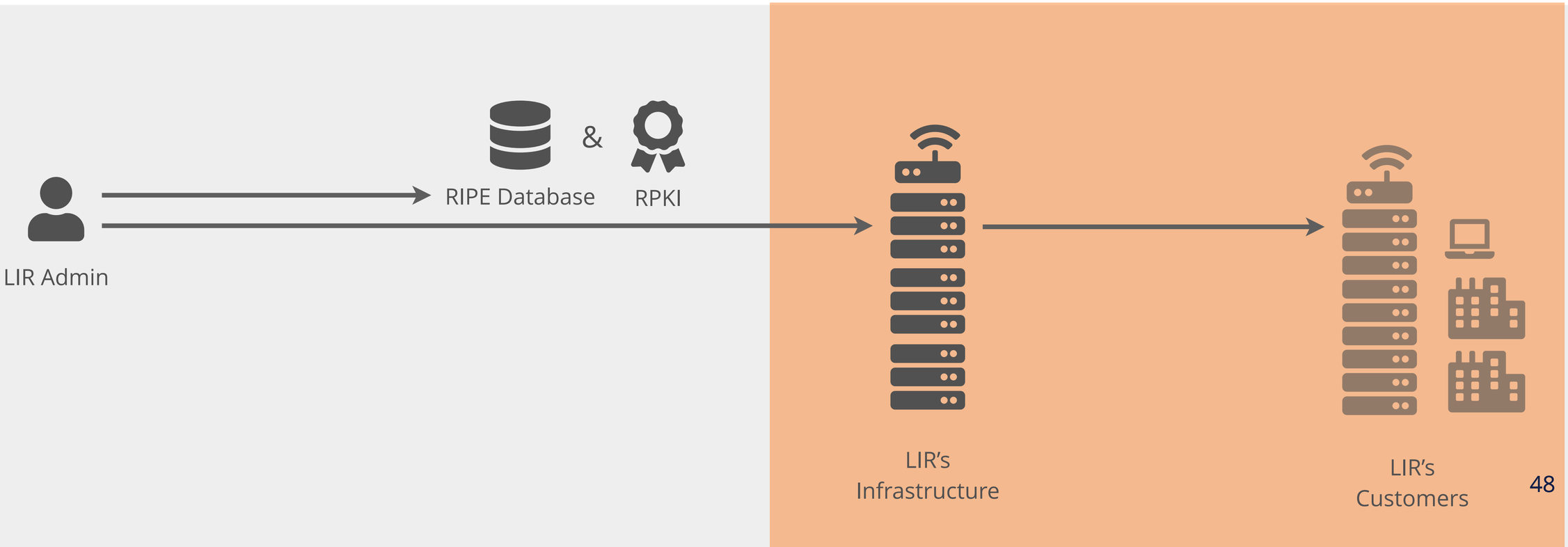
4. Investigate the prefix

- Investigate how the prefix was used in the past before assigning it to a critical service



5. Monitor your reputation

- **Monitor** how your prefixes are used
- Look for **abnormalities** in the traffic



How to prevent your IPs from being blocklisted:

What is **the most important** measure?

Please choose an option or type in your answer in the chat window.



1 min.

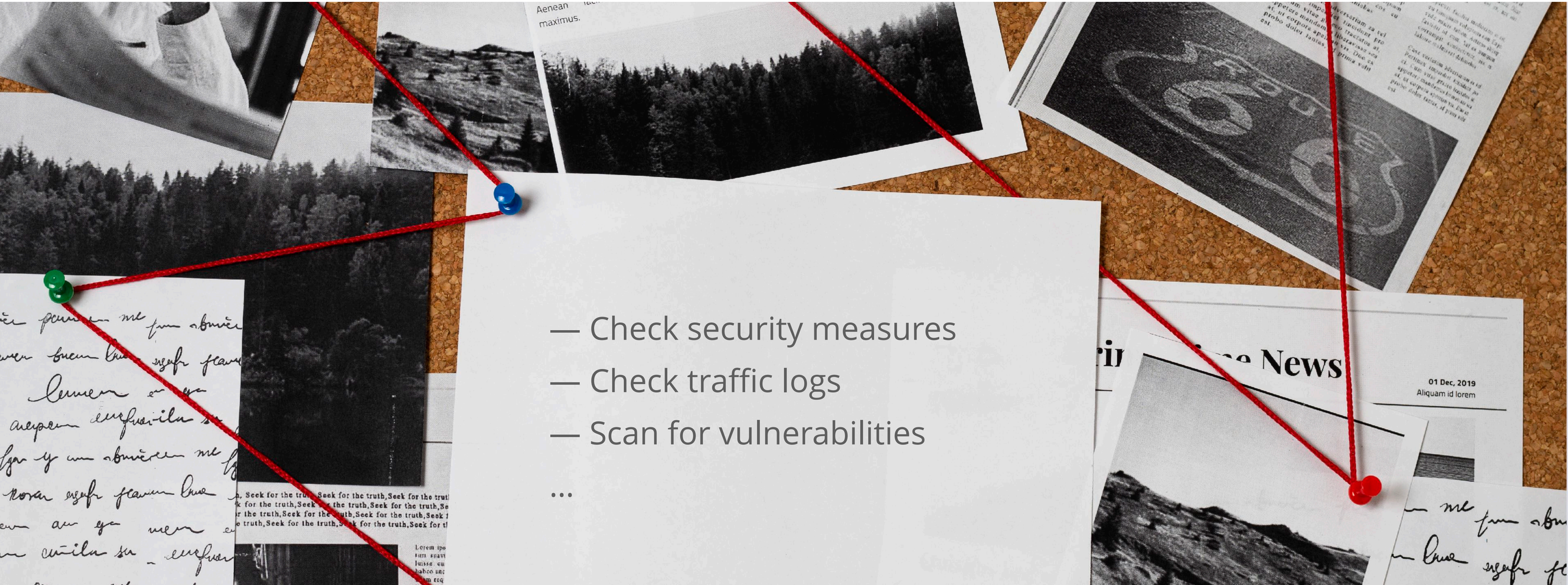


How to remove IPs and ASNs from blocklists

Section 9 of 9

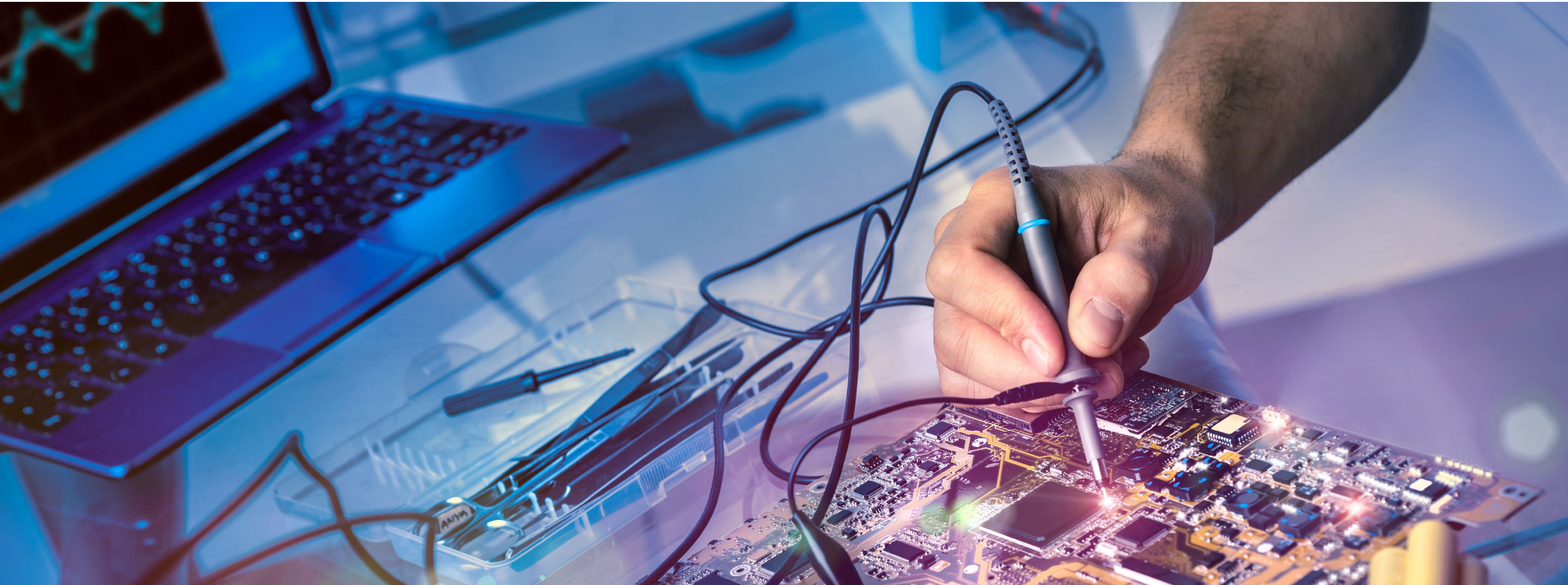
1. Don’t panic, investigate first

Find out **where** you’re blocklisted, and **for what**.



2. Take care of the reasons and contact blocklists

Remove malware, fix misconfiguration, etc, and **explain** to blocklists what was done.



How to remove your IPs from public blocklists:

What is **the most challenging** thing to do?

Please choose an option or type in your answer in the chat window.

1 min.



Wrap-Up

1. Stay **up-to-date**: sign up for mailing lists
2. **Know** the services you and your customers are providing
3. Implement **security measures** for infrastructure and services
4. Create and update assignments in the **RIPE Database**
5. Prevent address space hijacking: use BGP security measures for your prefixes



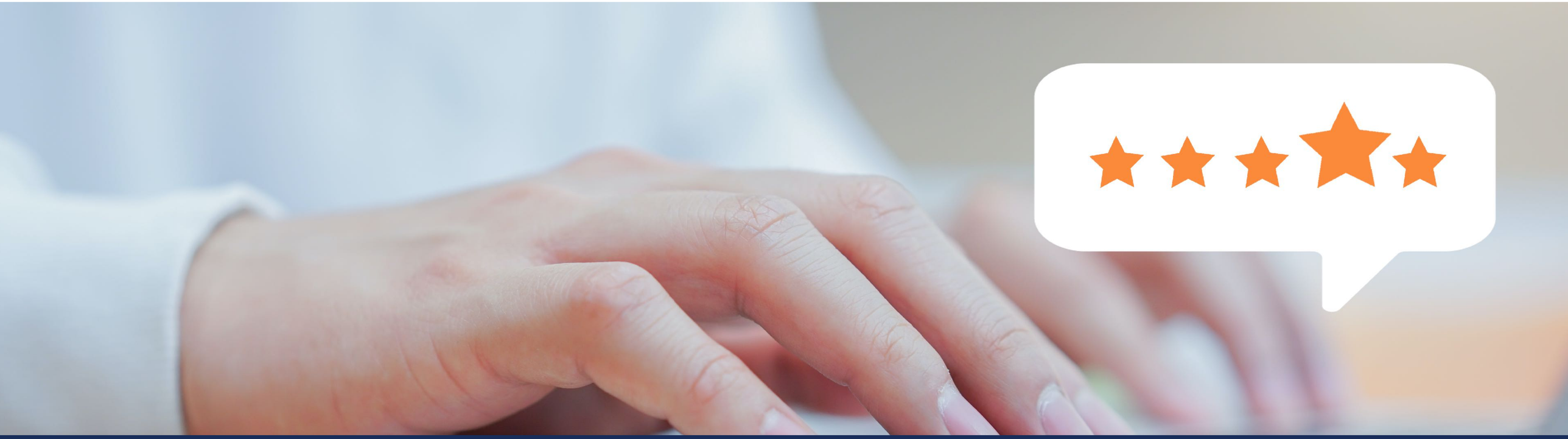
Questions



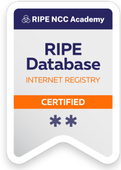
We want your feedback!

What did you think about this session? Take our survey at:

https://www.ripe.net/feedback/ip-blocklisting-basics

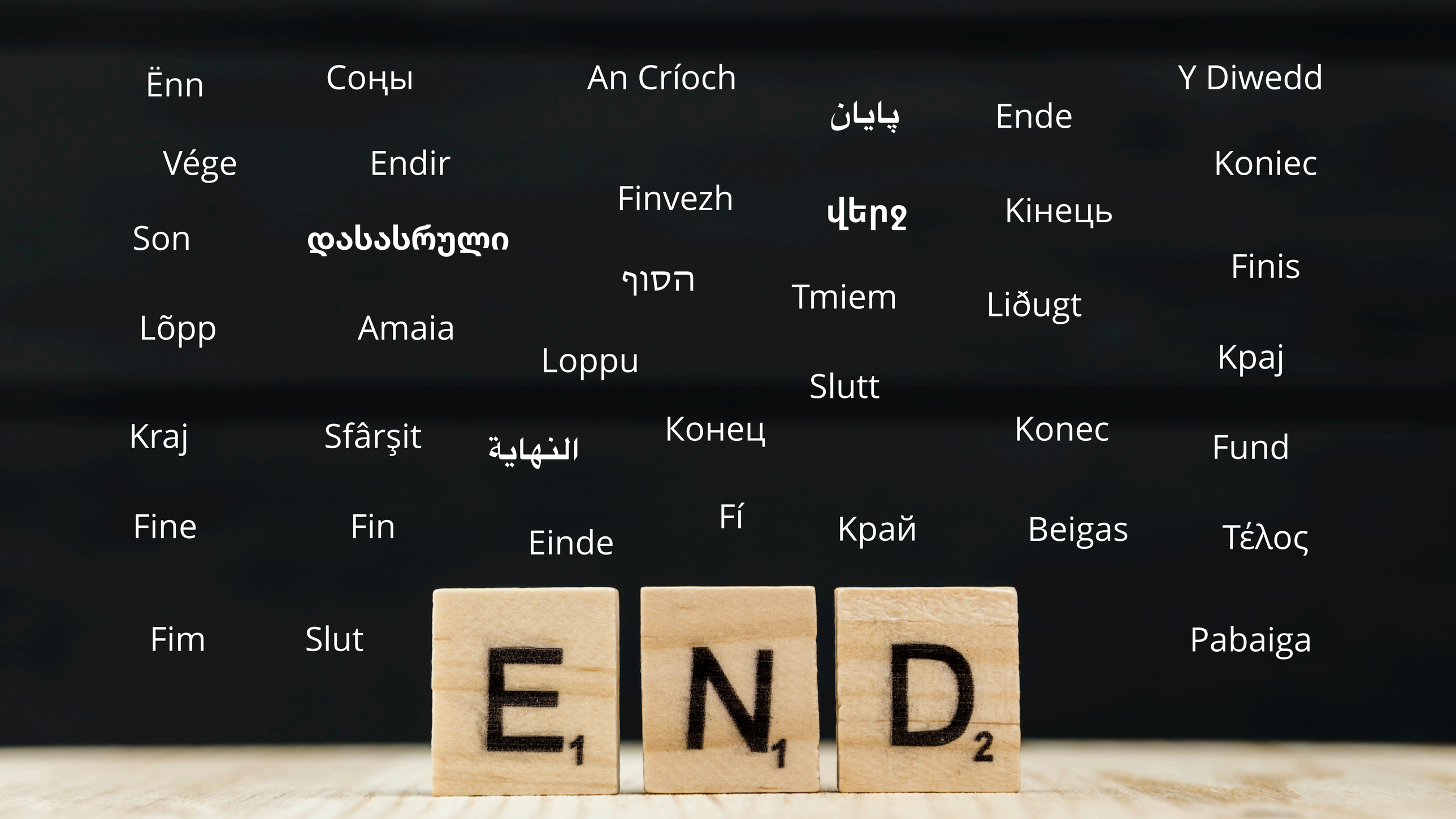


What else can you learn about?

	Fundamentals	Advanced	Expert
Internet Registry	**Internet Registry Fundamentals**	**Internet Registry Advanced**	
Routing	**E-learning course** Local Internet Registry Fundamentals 3h **Certification exam** Local Internet Registry Fundamentals  **In-person course** Local Internet Registry Fundamentals 8h **Webinars** Welcome to the RIPE NCC 1h IP Blocklisting Basics 1h Anti Abuse 1.5h	**E-learning course** RIPE Database 16h **Certification exam** RIPE Database  **In-person course** RIPE Database 8h **Webinars** RIPE Database Basics 2h RIPE Database Applications 2h	
IPv6			
Measurements & Tools			
Internet Governance			

Still have technical questions? Email us at academy@ripe.net

Check all our training & certifications at academy.ripe.net


Ënn
Соңы
An Críoch
پایان
Ende
Y Diwedd
Vége
Endir
Finvezh
վերջ
Кінець
Koniec
Son
დასასრული
הסוף
Tmiem
Liðugt
Finis
Lõpp
Amaia
Loppu
Slutt
Kpaj
Kraj
Sfârşit
النهاية
Конец
Konec
Fund
Fine
Fin
Einde
Fí
Край
Beigas
Τέλος
Fim
Slut
Pabaiga
E1 N1 D2

Fighting Spam

Good Practice In Minimising Email Abuse: https://www.ripe.net/publications/docs/ripe-409

The History of Spam: https://www.internetsociety.org/wp-content/uploads/2017/08/History20of20Spam.pdf

Combating Spam: Policy, Technical and Industry Approaches: https://www.internetsociety.org/resources/doc/2012/combating-spam-policy-technical-and-industry-approaches/

Anti-Spam Recommendations for SMTP MTAs: https://datatracker.ietf.org/doc/html/rfc2505

Email Submission Operations: Access and Accountability Requirements (BCP-134): https://datatracker.ietf.org/doc/html/rfc5068

Botnets Prevention

Botnet Remediation Overview & Practices: https://www.internetsociety.org/wp-content/uploads/2017/10/ota_2013_botnet_remediation_best_practices.pdf

Preventing Use of Recursive Nameservers in Reflector Attacks (BCP-140): https://www.ietf.org/rfc/rfc5358.txt

Prevent hijacking

Maintain the RIPE DB objects up-to-date: https://apps.db.ripe.net/db-web-ui/myresources/overview

Create ROAs and an ASPA: https://dashboard.rpki.ripe.net/#overview

Network Ingress Filtering: Defeating Denial of Service Attacks which employ IP Source Address Spoofing (BCP-38): https://www.rfc-editor.org/info/bcp38

Join the MANRS: https://www.manrs.org/isps/

RIPE NCC procedures

Reusing Recovered Internet Number Resources:
https://www.ripe.net/manage-ips-and-asns/resource-management/quarantine-for-returned-internet-number-resources

Resource Quality Assurance before re-allocating IP prefixes:
https://www.ripe.net/manage-ips-and-asns/resource-management/ripe-ncc-resource-quality-assistance

Useful tools for investigation

RIPEstat Historical Whois: https://stat.ripe.net/widget/historical-whois

RIPEstat Allocation History: https://stat.ripe.net/widget/allocation-history

RIPEstat Routing History: https://stat.ripe.net/widget/routing-history

Transfer Statistics: https://www.ripe.net/manage-ips-and-asns/resource-transfers-and-mergers/transfer-statistics

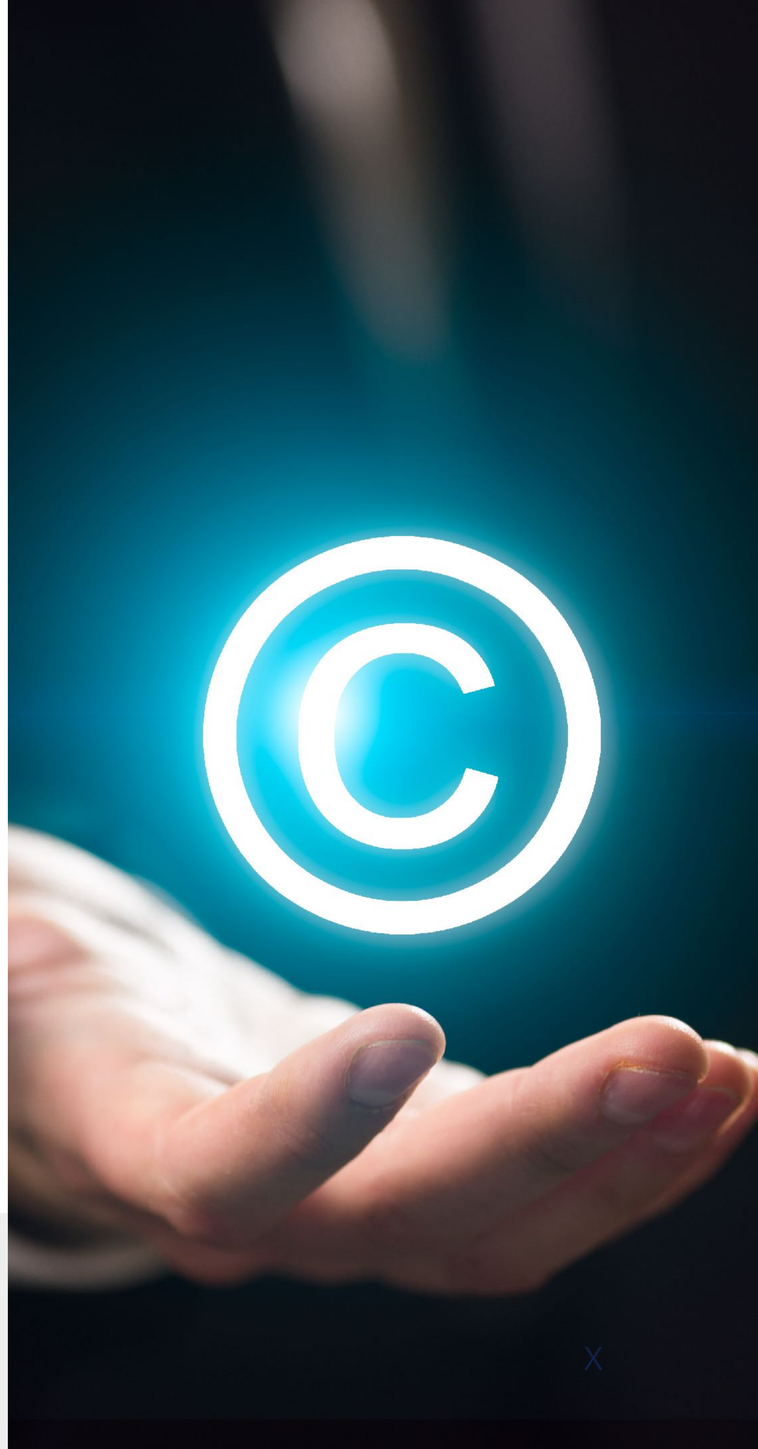
Anti-Abuse Working Group (WG): https://www.ripe.net/participate/ripe/wg/active-wg/anti-abuse

Copyright Statement

[...]

The RIPE NCC Materials may be used for **private purposes, for public non-commercial purpose, for research, for educational or demonstration purposes**, or if the materials in question specifically state that use of the material is permissible, and provided the RIPE NCC Materials are not modified and are properly identified as RIPE NCC documents. Unless authorised by the RIPE NCC in writing, any use of the RIPE NCC Materials for advertising or marketing purposes is strictly forbidden and may be prosecuted. The RIPE NCC should be notified of any such activities or suspicions thereof.

[...]



Find the full copyright statement here:
https://www.ripe.net/about-us/legal/copyright-statement