



Routing Security

Het voorkomen van BGP hijacks nu en in de toekomst



- Non-profit stichting: Open Source, Open Standaarden, Open Internet
- Specialisatie in DNS & Routing: Security, Stability, Privacy
- Core DNS Producten: NSD, Unbound, OpenDNSSEC
- Diensten: internet.nl – test op veilige, moderne Internetstandaarden
- *Nieuw*: RPKI Routing security toolset

The background features a network diagram with several light green circles connected by thin lines. On the left side, there are larger, overlapping abstract shapes in shades of green and white, resembling stylized leaves or petals.

Netwerk van Netwerken



Border Gateway Protocol (BGP)



"Autonomous System"



KPN = AS286

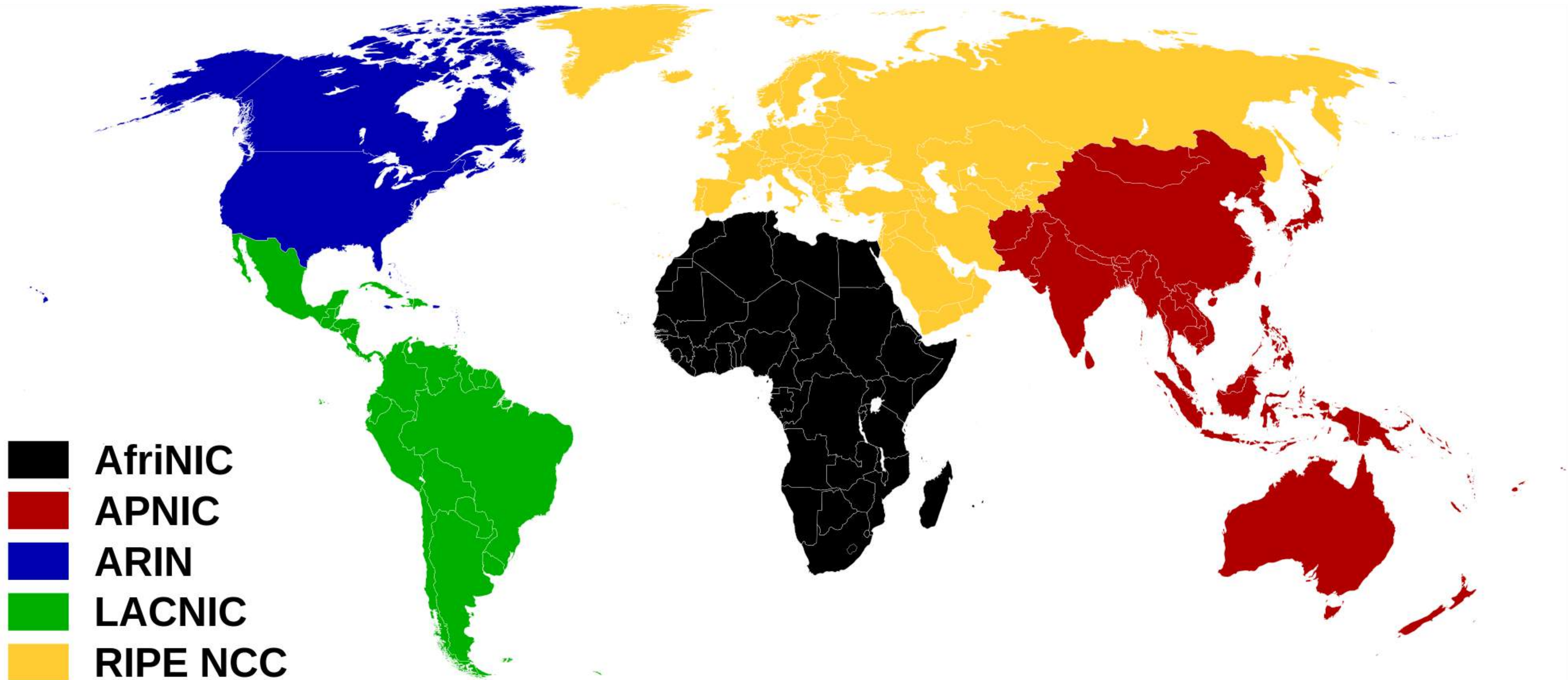


Netflix = AS2906

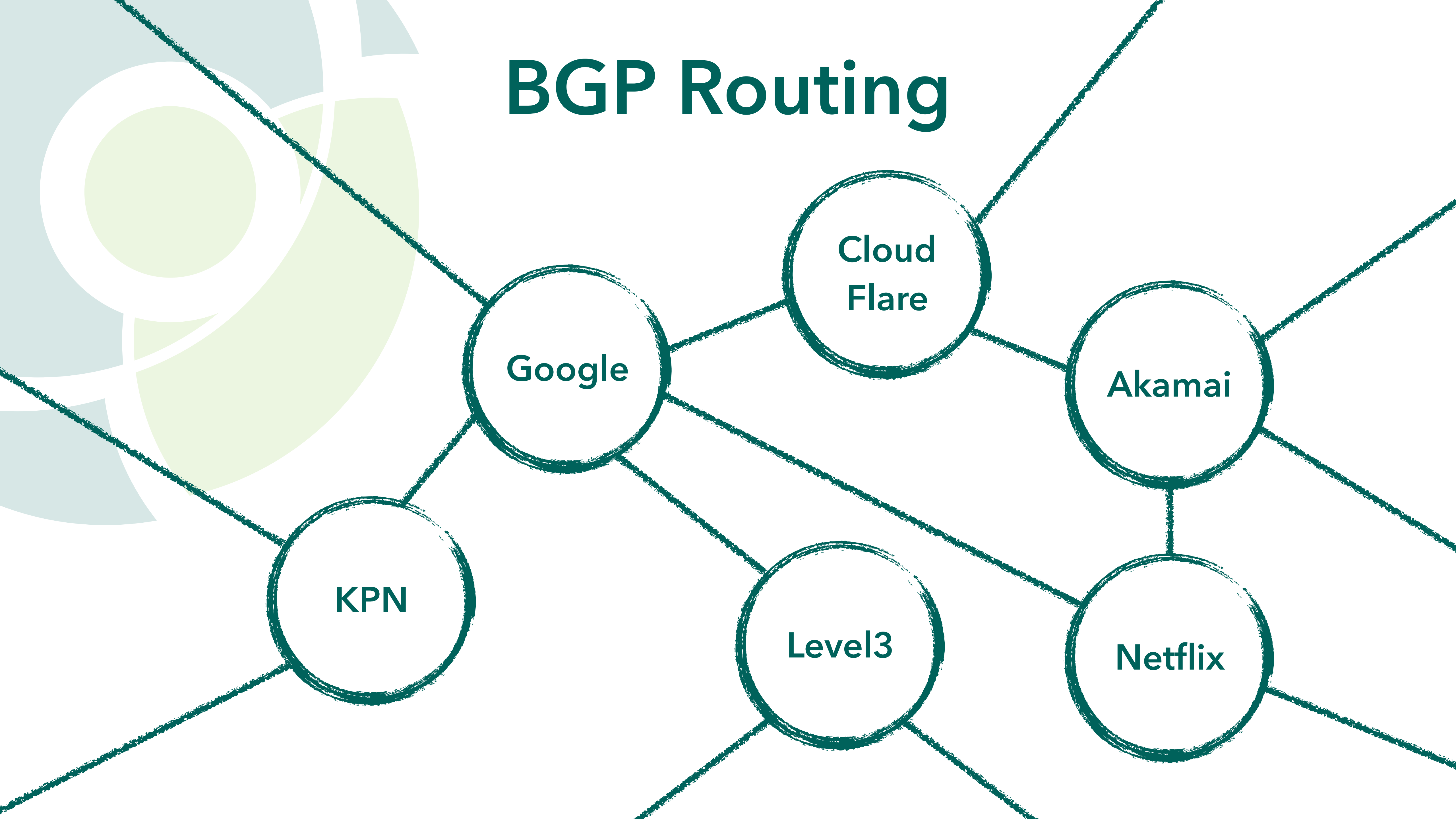


Google = AS15169

Regional Internet Registries



BGP Routing



Google

Cloud
Flare

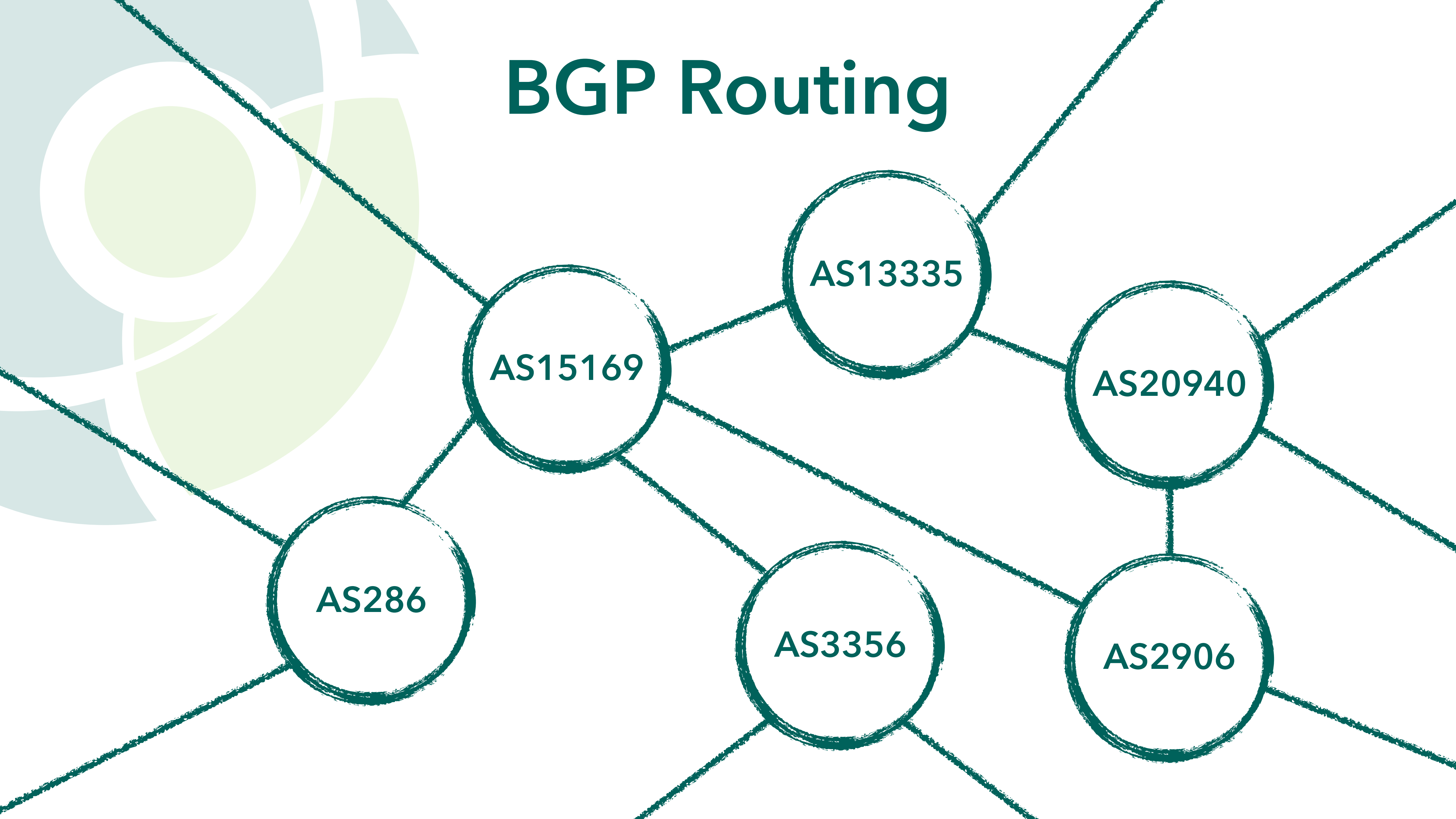
Akamai

KPN

Level3

Netflix

BGP Routing



AS15169

AS13335

AS20940

AS286

AS3356

AS2906



**Ieder AS kan ieder
IP adresblok announcen**



Internet Routing Registry (IRR)

"route" object

```
route: 185.49.140.0/22
descr: Stichting NLnet Labs
origin: AS199664
mnt-by: NLNETLABS-MNT
created: 2014-03-10T12:25:24Z
last-modified: 2015-02-23T11:56:03Z
source: RIPE
```

**Ik zal deze IP prefix announcen
vanaf dit AS**





AFRINIC, ALTDB, AOLTW, ***APNIC***, ***ARIN***, BELL, BBOI,
CANARIE, EASYNET, EPOCH, HOST, JPIRR, LEVEL3,
NESTEGG, NTTCOM, OPENFACE, OTTIX, PANIX,
RADB, REACH, RGNET, ***RIPE***, RISQ, ROGERS, TC

`irr.net/docs/list.html`



**10 IRRs hebben geen
authenticatie of validatie**



By Eduard Kovacs on August 07, 2018
[Share](#) [G+](#) [Tweet](#) [Recommend 17](#) [RSS](#)

Several payment processing companies in the United States were targeted recently in BGP hijacking attacks whose goal was to redirect users to malicious websites, Oracle reported last week.

The Border Gateway Protocol (BGP) controls the route of data across the Web. BGP hijacking also known as prefix or route hijacking, is carried out by taking over IP address groups by corrupting the routing tables that store the path to a network.

In the past months, Oracle, which gained deep visibility into Web traffic after acquiring Dyn in 2016, has observed several instances of malicious actors trying to force users to their websites by targeting authoritative DNS servers in BGP hijacking attacks.

The attackers used rogue DNS servers to return forged DNS responses to users trying to access a certain website. They maximized the duration of an attack with long time-to-live (TTL) values in those forged responses so that DNS servers would hold the fake DNS entries in their cache for an extended period.

Turkey Hijacking IP addresses for popular Global DNS providers

Posted by Andree Toonk - March 29, 2014 - [Hijack](#), [News and Updates](#) - 26 Comments

At BGPmon we see numerous BGP hijacks every single day, some are interesting because of size and scale of the hijack or as we've seen today because of the targeted hijacked prefix. All started last weekend when the Turkish president ordered the censorship of twitter.com. It started with a block of twitter by returning false twitter IP addresses by Turk Telekom DNS servers. Soon users in Turkey discovered that changing DNS providers to Google DNS or OpenDNS was a [good method of bypassing the censorship](#). But as of around 9am UTC today

(Saturday March 29) this changed when Turk Telekom started to hijack the IP address for popular free and open DNS providers such as Google's 8.8.8.8, OpenDNS' 208.67.222.222 and 4.2.2.3's 4.2.2.2. **BGP hijack** Using the Turk Telekom looking glass we can see that AS9121 (Turk Telekom) has specific /32 routes for these IP addresses. Since this is the most specific route possible for an IPv4 address, this route will always be selected and the result is that traffic to this IP address is sent to this new bogus route.

BORDER GATEWAY PROTOCOL ATTACK —

Suspicious event hijacks Amazon traffic for 2 hours, steals cryptocurrency

Almost 1,300 addresses for Amazon Route 53 rerouted for two hours.

DAN GOODIN - 4/24/2018, 9:00 PM



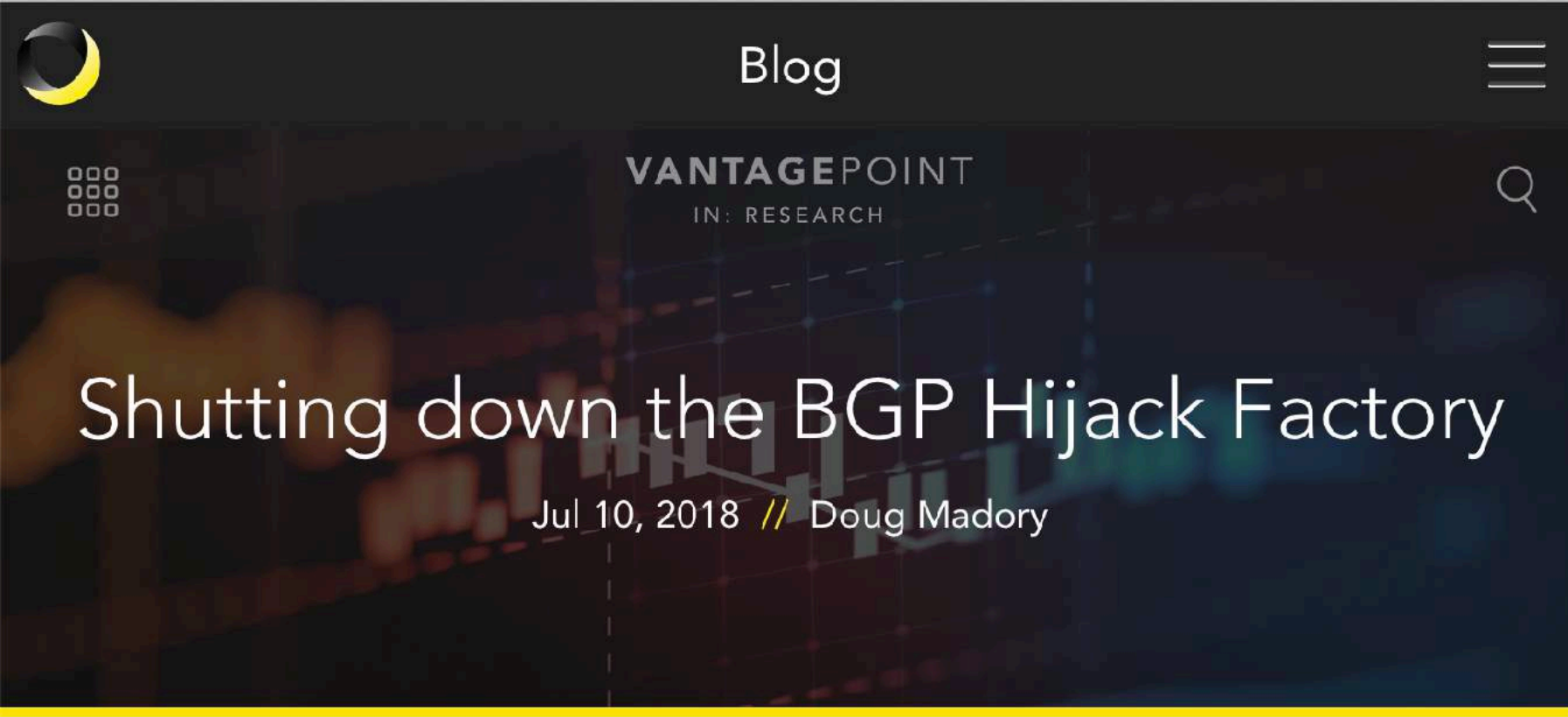
Amazon lost control of a small number of its cloud services IP addresses for two hours on Tuesday morning when hackers exploited a known Internet-protocol weakness that let them to redirect traffic to rogue destinations. By subverting Amazon's domain-resolution service, the attackers managed to steal cryptocurrency website MyEtherWallet.com and stole about \$150,000 in digital coins from unwitting end users. They may have targeted other Amazon customers as well.

December 18, 2017 By [Pierluigi Paganini](#)

Traffic for Google, Apple, Facebook, Microsoft and other tech giants routed through Russia, experts believe it was an intentional BGP Hijacking.

Last week a suspicious event routed traffic for major tech companies (i.e. Google, Facebook, Apple, and Microsoft) through a previously unknown Russian Internet provider. The event occurred on Wednesday, researchers who investigated it believe the traffic was intentionally hijacked.

The incident involved the Internet's Border Gateway Protocol that is used to route traffic among Internet backbones, ISPs, and other large networks.



It started with a [lengthy email](#) to the NANOG mailing list on 25 June 2018: independent security researcher Ronald Guilmette detailed the suspicious routing activities of a company called [Bitcanal](#), whom he referred to as a "Hijack Factory." In his post, Ronald detailed some of the Portuguese company's most recent BGP hijacks and asked the question: why Bitcanal's transit providers continue to carry its BGP hijacked routes on to the global internet?

This email kicked off a discussion that led to a concerted effort to kick this bad actor, who has hijacked with impunity for many years, off the internet.



3

How Pakistan knocked YouTube offline (and how to make sure it never happens again)

YouTube becoming unreachable isn't the first time that Internet addresses were hijacked. But if it spurs interest in better security, it may be the last.



by **Declan McCullagh**
Updated: February 25, 2008 4:28 PM PST



100.000+ BGP hijacks
per jaar




De Oplossing?



Blockchain

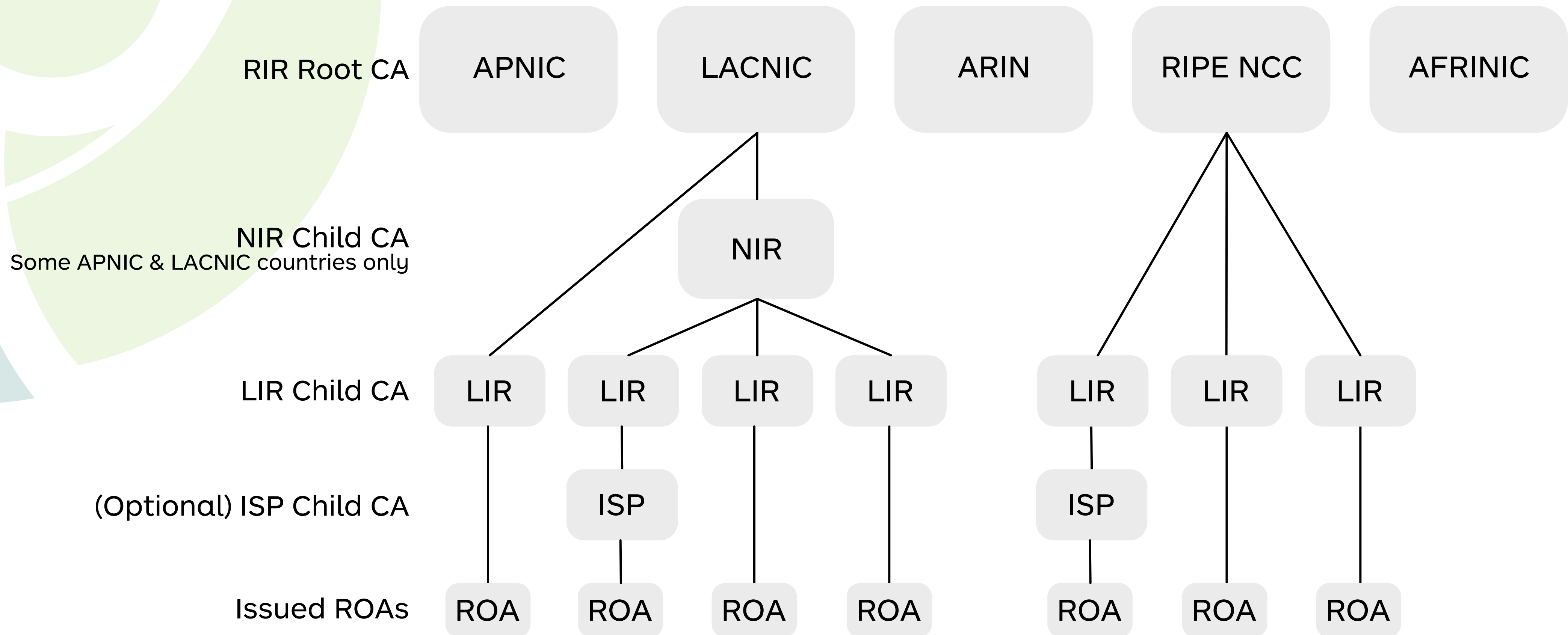


~~Blockchain~~



Resource Public Key Infrastructure (RPKI)

RPKI Structuur





Route Origin Authorisation (ROA)



**Ik autoriseer dit AS
om deze IP prefix met
deze lengte te
announcen**

 **Was getekend...**



Creëer ROAs

my.ripe.net

Resources ⇨ RPKI Dashboard



You are here: [Home](#) > [Manage IPs and ASNs](#) > LIR Portal

You are editing

Stichting NLnet Labs

[My LIR](#) >

Resources ▾

[My Resources](#)

[Request Resources](#)

[Request Transfer](#)

[IPv4 Transfer Listing Service](#)

[RPKI Dashboard](#)

[RIPE Database](#) >

RPKI Dashboard

2 CERTIFIED RESOURCES

ALERTS ARE SENT TO 1 ADDRESS

2 BGP Announcements

2 Valid 0 Invalid 0 Unknown

2 ROAs

2 OK 0 Causing problems

BGP Announcements

Route Origin Authorisations (ROAs)

History

Search...

Discard Changes

Delete ROAs

Causing Problems

Not Causing Problems

+ New ROA

<input type="checkbox"/>	AS number	Prefix	Most specific length allowed	Affects	
	<input type="text" value="AS Number"/>	<input type="text" value="Prefix"/>	<input type="text" value="Max length"/>		
<input type="checkbox"/>	AS199664	2a04:b900::/29	29	1	
<input type="checkbox"/>	AS199664	185.49.140.0/22	22	1	

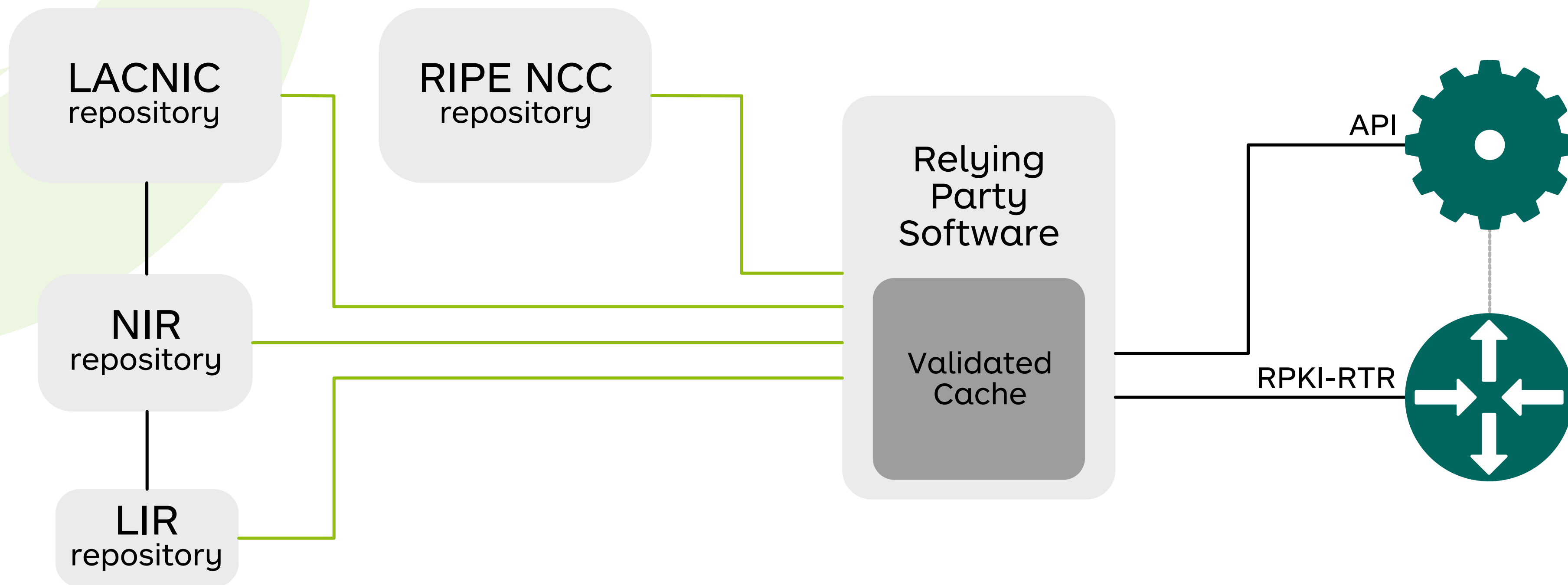
Show 25 of 2 items

A map of Europe where the Netherlands is highlighted in a darker shade of green. A white callout box with a grey border is positioned over the Netherlands, containing the text 'NL' and '%: 53.75'. The rest of Europe is shown in a light beige color.

NL

%: 53.75

Relying Party Software





<https://nlnetlabs.nl/projects/rpki/project-plan/>



ROUTINATOR

<https://github.com/nlnetlabs/routinator>



INVALID = DROP

INVALID = DROP



Binnenkort...





CLOUDFLARE®



<https://blog.cloudflare.com/rpki/>

Huiswerk

- Besluit op management niveau of RPKI een Goed Idee™ is
- Zet RPKI aan in de RIPE NCC LIR Portal – my.ripe.net
- Maak ROAs voor al je BGP announcements (en onderhoud ze!)
- Installeer validatie-software ([NLnet Labs Routinator](#) of [RIPE NCC RPKI Validator](#))
 - Vergeet niet de [ARIN Trust Anchor Locator](#) te downloaden!
- Besteed wat tijd aan dit onderwerp met eerste-lijn support personeel
- Configureer je routers en DROP invalid BGP announcements

Operationele Ervaringen



<https://nlnog.net/nlnog-day-2018/>

Interesse?

 Ik ben hier de rest van de dag

 <https://rpki.nl>

 <https://github.com/nlnetlabs/routinator>

 rpki@nlnetlabs.nl

 [@alexander_band](https://twitter.com/alexander_band)