HURRICANE ELECTRIC
INTERNET SERVICES

RPKI at Hurricane Electric

Susan Forney

Hurricane Electric AS6939

RPKI Implementation at Hurricane Electric

As of February 23, 2020, the following ISPs had announced that they were filtering for RPKI validation and dropping RPKI invalids:

AT&T	AS7018
Cloudflare	AS13335
Cogent	AS174
KPN	AS286
PCCW	AS3491
Tata	AS6453
Telia	AS1299

RPKI Implementation at Hurricane Electric

As of February 24, 2020, there was one more:

HE

HURRICANE ELECTRIC
INTERNET SERVICES

AS6939

RPKI Implementation at Hurricane Electric

This is the route filtering algorithm for peers that have explicit filtering turned on:

1. Attempt to find an as-set to use for this network.

1.1 Inspect the aut-num for this ASN to see if we can extract from their IRR policy for what they would announce to Hurricane by finding export or mp-export to AS6939, ANY, or AS-ANY.

1.2 Also see if they set what looks like a valid IRR as-set name in peeringdb.com.

2. Collect the received routes for all BGP sessions with this ASN. This details both accepted and filtered routes.

2.1 If there are no received routes for this AS, perform the process below using the first 10 prefixes from their IRR policy.

RPKI Implementation at Hurricane Electric

3. For each route, perform the following rejection tests:

3.1 Reject prefix lengths less than minimum and greater than maximum. For IPv4 this is 8 and 24. For IPv6 this is 24 and 48.

3.2 Reject bogons (RFC1918, documentation prefix, default route, etc).

3.3 Reject exchange prefixes for all exchanges Hurricane Electric is connected to.

3.4 Reject routes that have RPKI status INVALID_ASN or INVALID_LENGTH based on the origin AS and prefix.

RPKI Implementation at Hurricane Electric

4. For each route, perform the following acceptance tests:

4.1 Accept routes that have RPKI status VALID based on the origin AS and prefix.

4.2 Compare the RIR handles for the prefix and the peer AS, if they match accept the prefix.

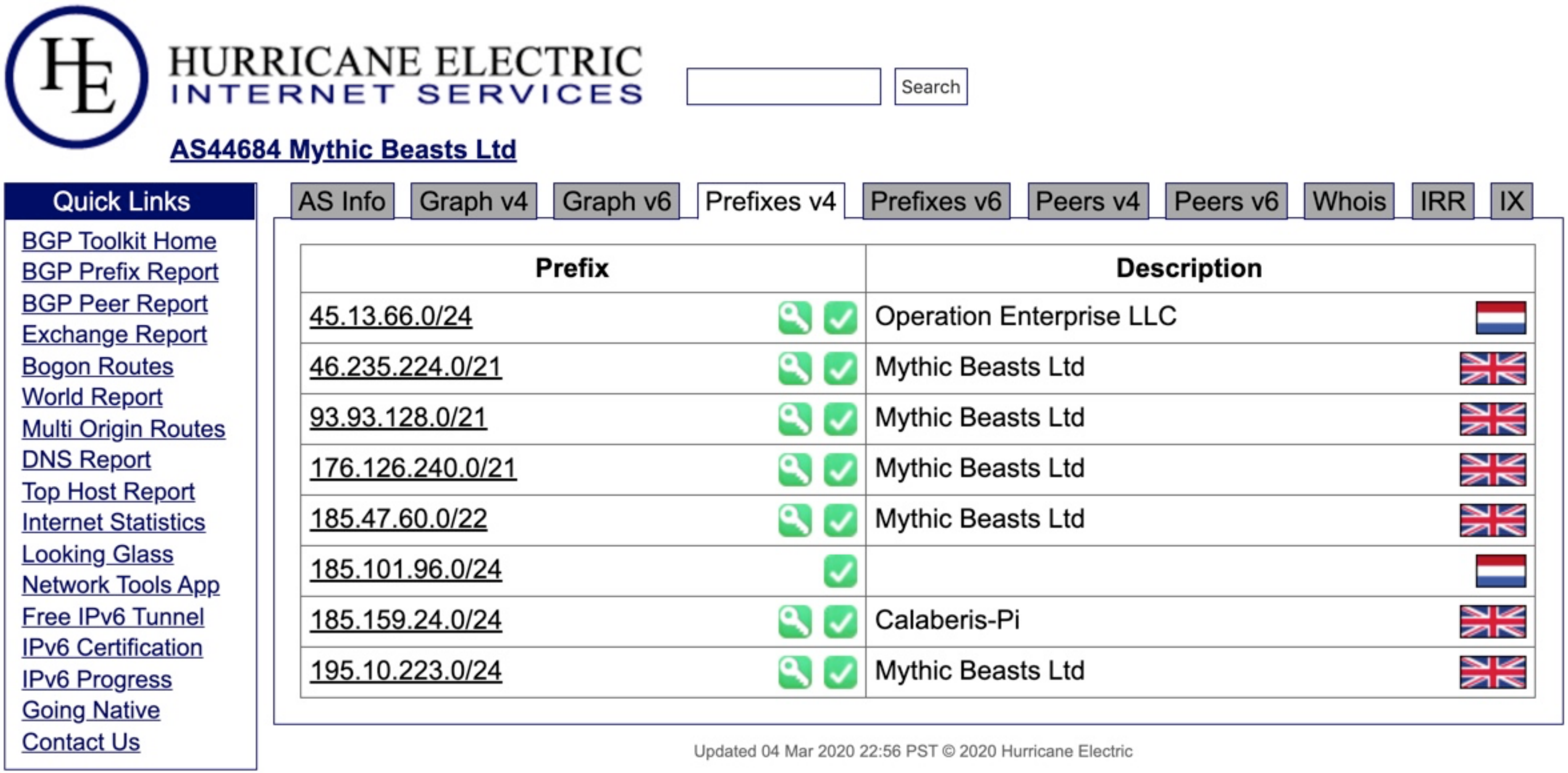
4.3 Check if this prefix exactly matches a prefix allowed by the IRR policy of this peer.

5. Reject all prefixes not explicitly accepted.

RPKI Implementation at Hurricane Electric

If you want to know at a glance how your network measures up, we have the following tools to help:

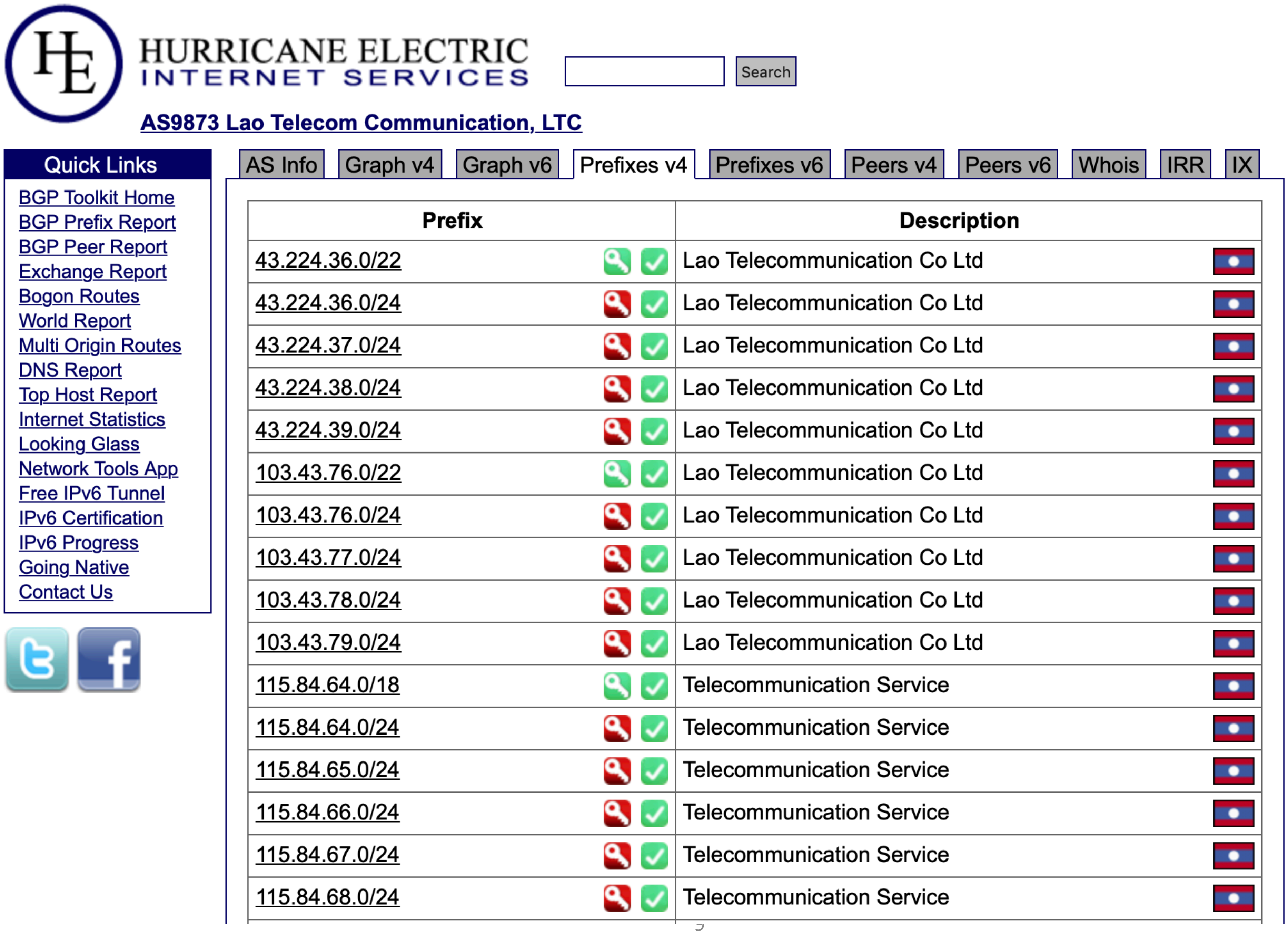
- Bgp.he.net—Our classic site featuring information from public sources about BGP and the Internet
- Routing.he.net—Our site that lets you look at any network that is in Hurricane Electric's BGP table and see how we filtered the routes.



AS44684 Mythic Beasts Ltd

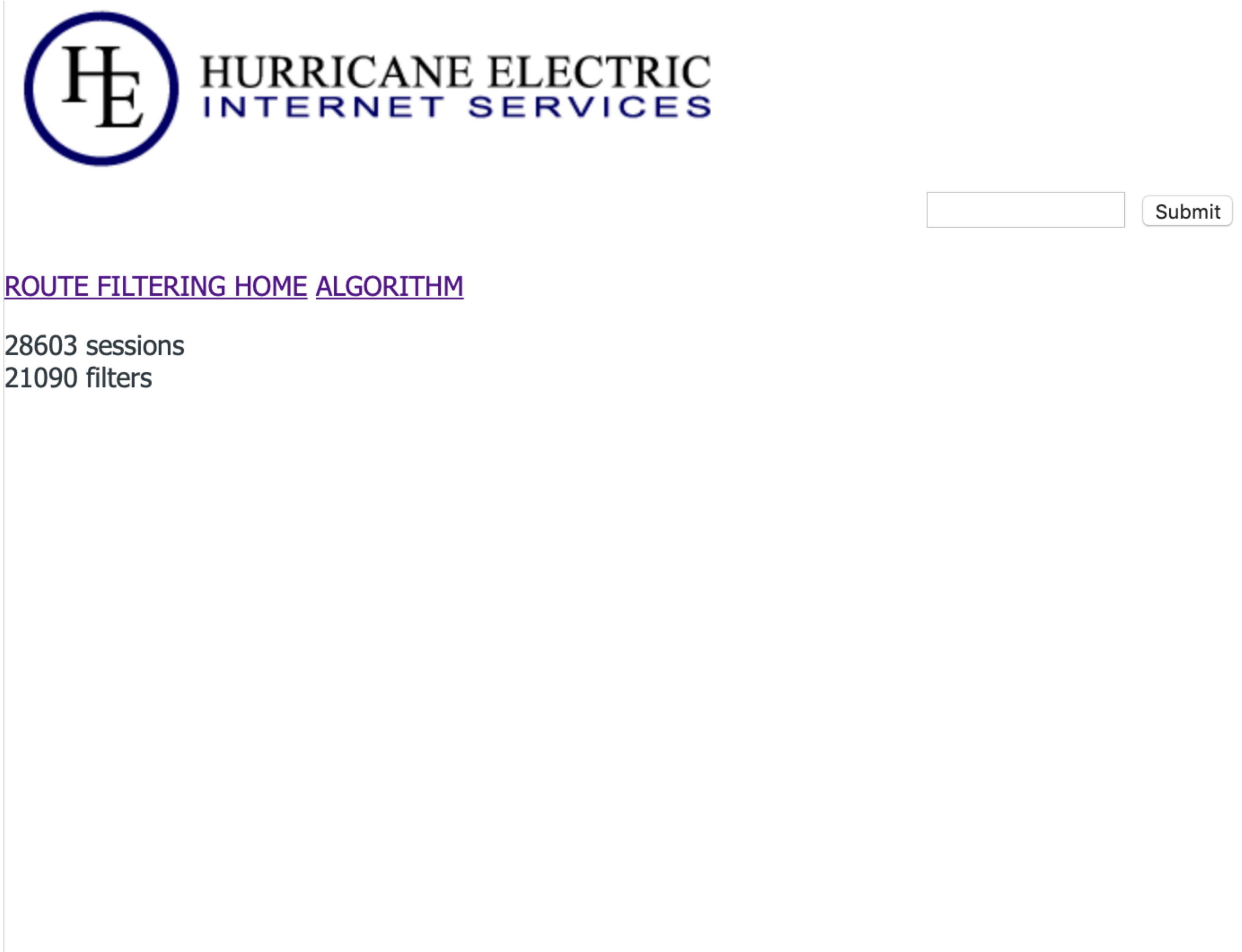
Prefix			Description	
45.13.66.0/24	🔍	✓	Operation Enterprise LLC	🇳🇱
46.235.224.0/21	🔍	✓	Mythic Beasts Ltd	🇬🇧
93.93.128.0/21	🔍	✓	Mythic Beasts Ltd	🇬🇧
176.126.240.0/21	🔍	✓	Mythic Beasts Ltd	🇬🇧
185.47.60.0/22	🔍	✓	Mythic Beasts Ltd	🇬🇧
185.101.96.0/24		✓		🇳🇱
185.159.24.0/24	🔍	✓	Calaberis-Pi	🇬🇧
195.10.223.0/24	🔍	✓	Mythic Beasts Ltd	🇬🇧

Updated 04 Mar 2020 22:56 PST © 2020 Hurricane Electric



AS9873 Lao Telecom Communication, LTC

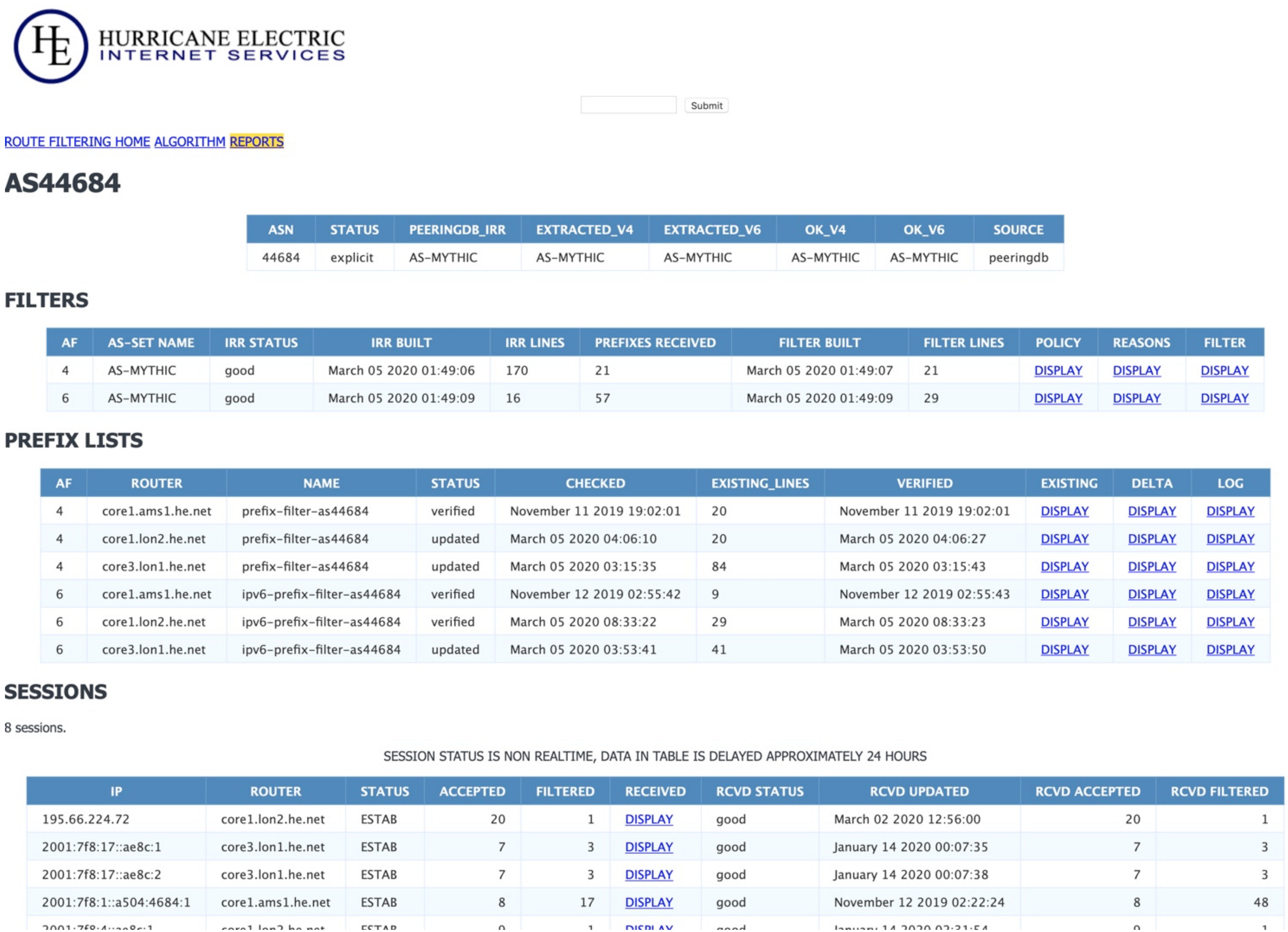
Prefix		Description
43.224.36.0/22	🔑 ✓	Lao Telecommunication Co Ltd
43.224.36.0/24	🔑 ✓	Lao Telecommunication Co Ltd
43.224.37.0/24	🔑 ✓	Lao Telecommunication Co Ltd
43.224.38.0/24	🔑 ✓	Lao Telecommunication Co Ltd
43.224.39.0/24	🔑 ✓	Lao Telecommunication Co Ltd
103.43.76.0/22	🔑 ✓	Lao Telecommunication Co Ltd
103.43.76.0/24	🔑 ✓	Lao Telecommunication Co Ltd
103.43.77.0/24	🔑 ✓	Lao Telecommunication Co Ltd
103.43.78.0/24	🔑 ✓	Lao Telecommunication Co Ltd
103.43.79.0/24	🔑 ✓	Lao Telecommunication Co Ltd
115.84.64.0/18	🔑 ✓	Telecommunication Service
115.84.64.0/24	🔑 ✓	Telecommunication Service
115.84.65.0/24	🔑 ✓	Telecommunication Service
115.84.66.0/24	🔑 ✓	Telecommunication Service
115.84.67.0/24	🔑 ✓	Telecommunication Service
115.84.68.0/24	🔑 ✓	Telecommunication Service



HURRICANE ELECTRIC
INTERNET SERVICES

ROUTE FILTERING HOME ALGORITHM

28603 sessions
21090 filters



AS44684

ASN	STATUS	PEERINGDB_IRR	EXTRACTED_V4	EXTRACTED_V6	OK_V4	OK_V6	SOURCE
44684	explicit	AS-MYTHIC	AS-MYTHIC	AS-MYTHIC	AS-MYTHIC	AS-MYTHIC	peeringdb

FILTERS

AF	AS-SET NAME	IRR STATUS	IRR BUILT	IRR LINES	PREFIXES RECEIVED	FILTER BUILT	FILTER LINES	POLICY	REASONS	FILTER
4	AS-MYTHIC	good	March 05 2020 01:49:06	170	21	March 05 2020 01:49:07	21	DISPLAY	DISPLAY	DISPLAY
6	AS-MYTHIC	good	March 05 2020 01:49:09	16	57	March 05 2020 01:49:09	29	DISPLAY	DISPLAY	DISPLAY

PREFIX LISTS

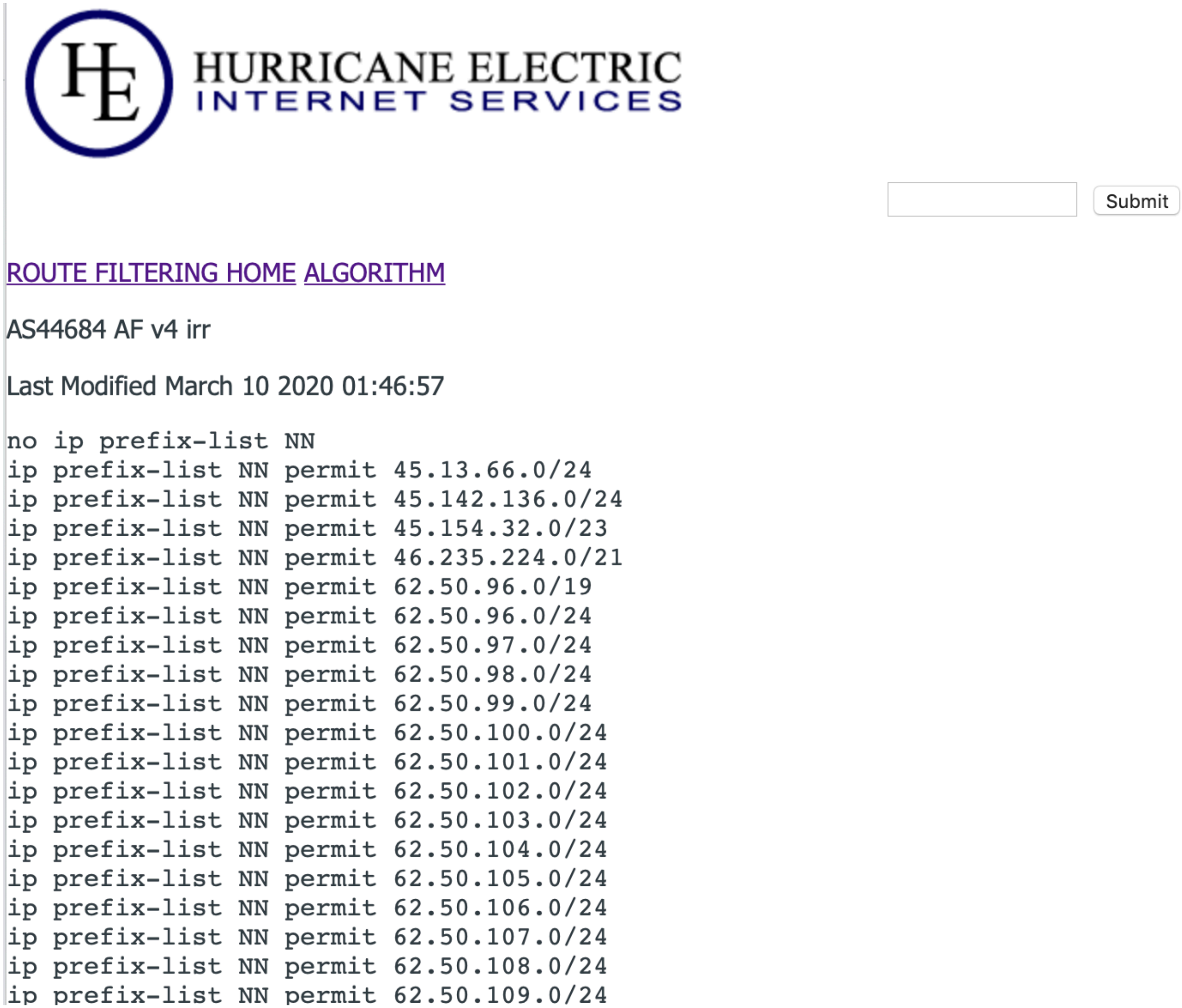
AF	ROUTER	NAME	STATUS	CHECKED	EXISTING_LINES	VERIFIED	EXISTING	DELTA	LOG
4	core1.ams1.he.net	prefix-filter-as44684	verified	November 11 2019 19:02:01	20	November 11 2019 19:02:01	DISPLAY	DISPLAY	DISPLAY
4	core1.lon2.he.net	prefix-filter-as44684	updated	March 05 2020 04:06:10	20	March 05 2020 04:06:27	DISPLAY	DISPLAY	DISPLAY
4	core3.lon1.he.net	prefix-filter-as44684	updated	March 05 2020 03:15:35	84	March 05 2020 03:15:43	DISPLAY	DISPLAY	DISPLAY
6	core1.ams1.he.net	ipv6-prefix-filter-as44684	verified	November 12 2019 02:55:42	9	November 12 2019 02:55:43	DISPLAY	DISPLAY	DISPLAY
6	core1.lon2.he.net	ipv6-prefix-filter-as44684	verified	March 05 2020 08:33:22	29	March 05 2020 08:33:23	DISPLAY	DISPLAY	DISPLAY
6	core3.lon1.he.net	ipv6-prefix-filter-as44684	updated	March 05 2020 03:53:41	41	March 05 2020 03:53:50	DISPLAY	DISPLAY	DISPLAY

SESSIONS

8 sessions.

SESSION STATUS IS NON REALTIME, DATA IN TABLE IS DELAYED APPROXIMATELY 24 HOURS

IP	ROUTER	STATUS	ACCEPTED	FILTERED	RECEIVED	RCVD STATUS	RCVD UPDATED	RCVD ACCEPTED	RCVD FILTERED
195.66.224.72	core1.lon2.he.net	ESTAB	20	1	DISPLAY	good	March 02 2020 12:56:00	20	1
2001:7f8:17::ae8c:1	core3.lon1.he.net	ESTAB	7	3	DISPLAY	good	January 14 2020 00:07:35	7	3
2001:7f8:17::ae8c:2	core3.lon1.he.net	ESTAB	7	3	DISPLAY	good	January 14 2020 00:07:38	7	3
2001:7f8:1::a504:4684:1	core1.ams1.he.net	ESTAB	8	17	DISPLAY	good	November 12 2019 02:22:24	8	48
2001:7f8:4::ae8c:1	core1.lon2.he.net	ESTAB	9	1	DISPLAY	good	January 14 2020 02:31:54	9	1

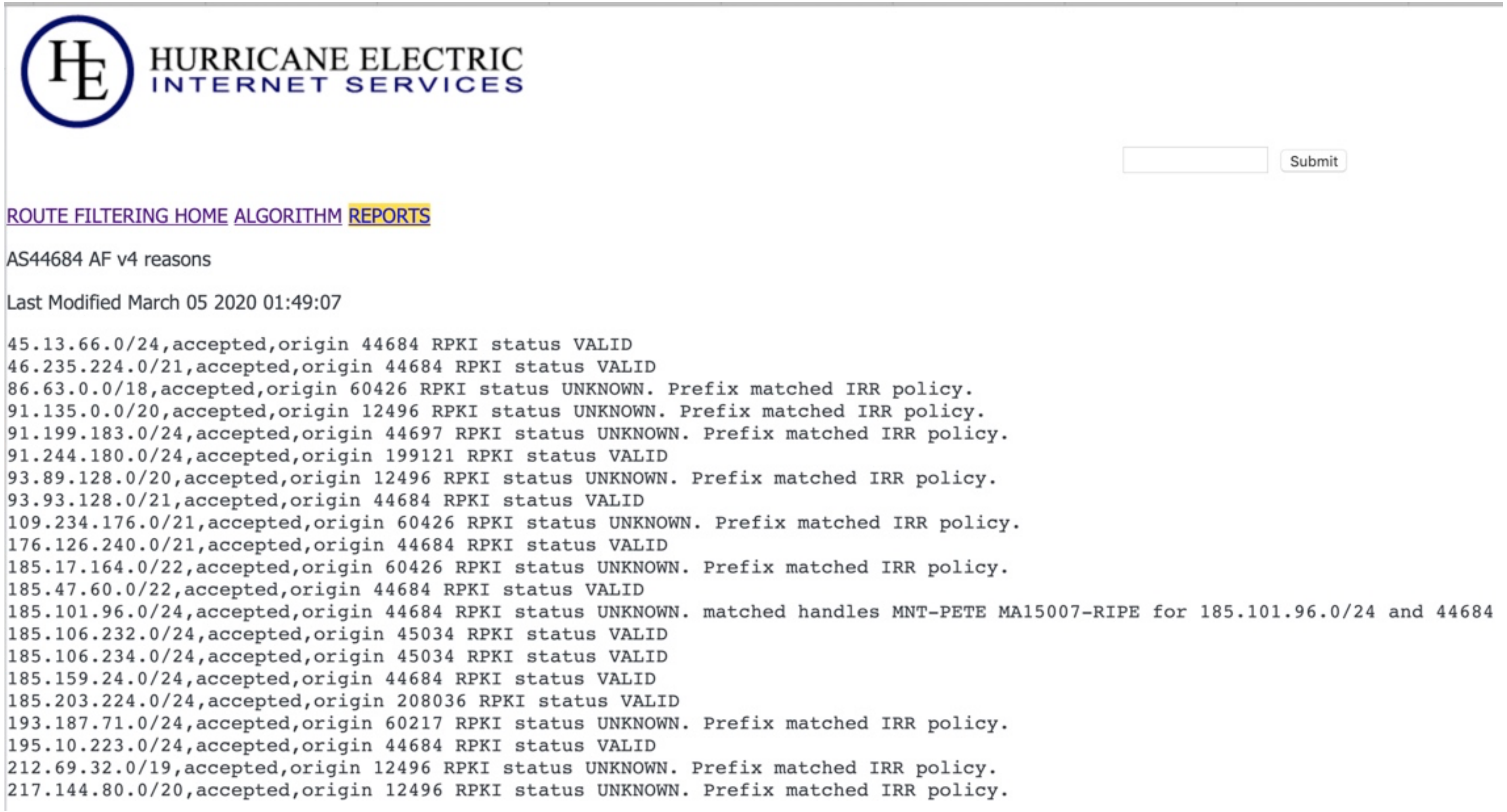


ROUTE FILTERING HOME ALGORITHM

AS44684 AF v4 irr

Last Modified March 10 2020 01:46:57

```
no ip prefix-list NN
ip prefix-list NN permit 45.13.66.0/24
ip prefix-list NN permit 45.142.136.0/24
ip prefix-list NN permit 45.154.32.0/23
ip prefix-list NN permit 46.235.224.0/21
ip prefix-list NN permit 62.50.96.0/19
ip prefix-list NN permit 62.50.96.0/24
ip prefix-list NN permit 62.50.97.0/24
ip prefix-list NN permit 62.50.98.0/24
ip prefix-list NN permit 62.50.99.0/24
ip prefix-list NN permit 62.50.100.0/24
ip prefix-list NN permit 62.50.101.0/24
ip prefix-list NN permit 62.50.102.0/24
ip prefix-list NN permit 62.50.103.0/24
ip prefix-list NN permit 62.50.104.0/24
ip prefix-list NN permit 62.50.105.0/24
ip prefix-list NN permit 62.50.106.0/24
ip prefix-list NN permit 62.50.107.0/24
ip prefix-list NN permit 62.50.108.0/24
ip prefix-list NN permit 62.50.109.0/24
```

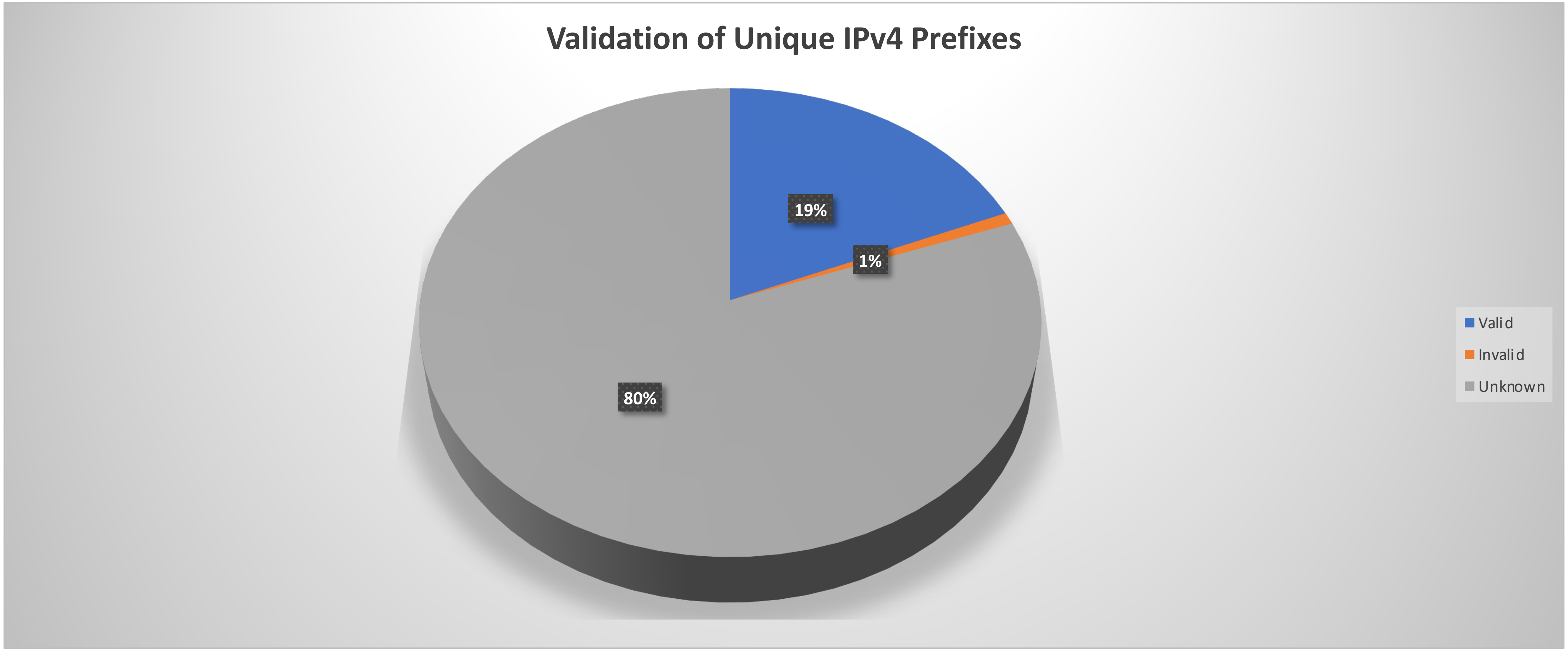


AS44684 AF v4 reasons

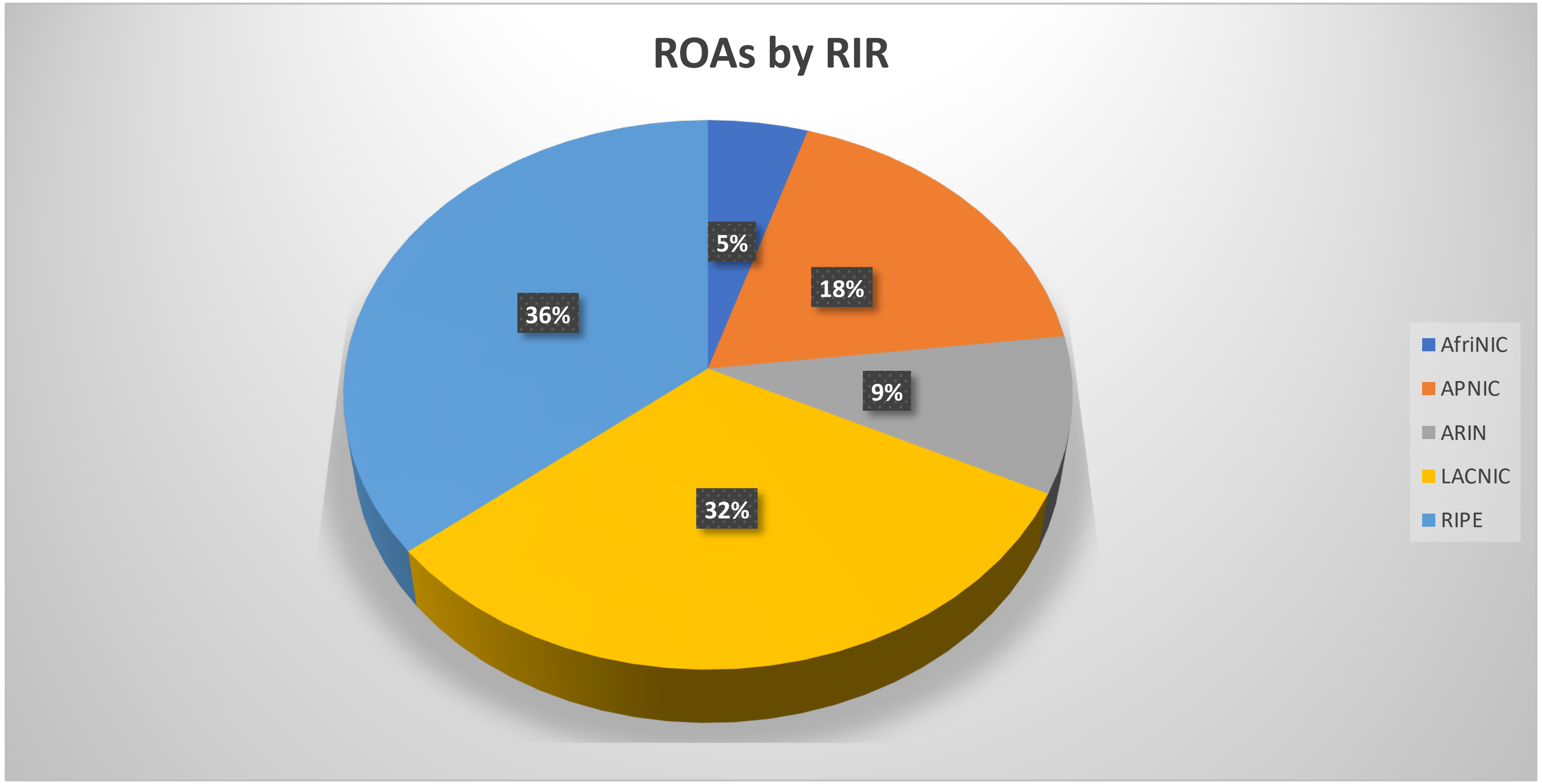
Last Modified March 05 2020 01:49:07

```
45.13.66.0/24,accepted,origin 44684 RPKI status VALID
46.235.224.0/21,accepted,origin 44684 RPKI status VALID
86.63.0.0/18,accepted,origin 60426 RPKI status UNKNOWN. Prefix matched IRR policy.
91.135.0.0/20,accepted,origin 12496 RPKI status UNKNOWN. Prefix matched IRR policy.
91.199.183.0/24,accepted,origin 44697 RPKI status UNKNOWN. Prefix matched IRR policy.
91.244.180.0/24,accepted,origin 199121 RPKI status VALID
93.89.128.0/20,accepted,origin 12496 RPKI status UNKNOWN. Prefix matched IRR policy.
93.93.128.0/21,accepted,origin 44684 RPKI status VALID
109.234.176.0/21,accepted,origin 60426 RPKI status UNKNOWN. Prefix matched IRR policy.
176.126.240.0/21,accepted,origin 44684 RPKI status VALID
185.17.164.0/22,accepted,origin 60426 RPKI status UNKNOWN. Prefix matched IRR policy.
185.47.60.0/22,accepted,origin 44684 RPKI status VALID
185.101.96.0/24,accepted,origin 44684 RPKI status UNKNOWN. matched handles MNT-PETE MA15007-RIPE for 185.101.96.0/24 and 44684
185.106.232.0/24,accepted,origin 45034 RPKI status VALID
185.106.234.0/24,accepted,origin 45034 RPKI status VALID
185.159.24.0/24,accepted,origin 44684 RPKI status VALID
185.203.224.0/24,accepted,origin 208036 RPKI status VALID
193.187.71.0/24,accepted,origin 60217 RPKI status UNKNOWN. Prefix matched IRR policy.
195.10.223.0/24,accepted,origin 44684 RPKI status VALID
212.69.32.0/19,accepted,origin 12496 RPKI status UNKNOWN. Prefix matched IRR policy.
217.144.80.0/20,accepted,origin 12496 RPKI status UNKNOWN. Prefix matched IRR policy.
```

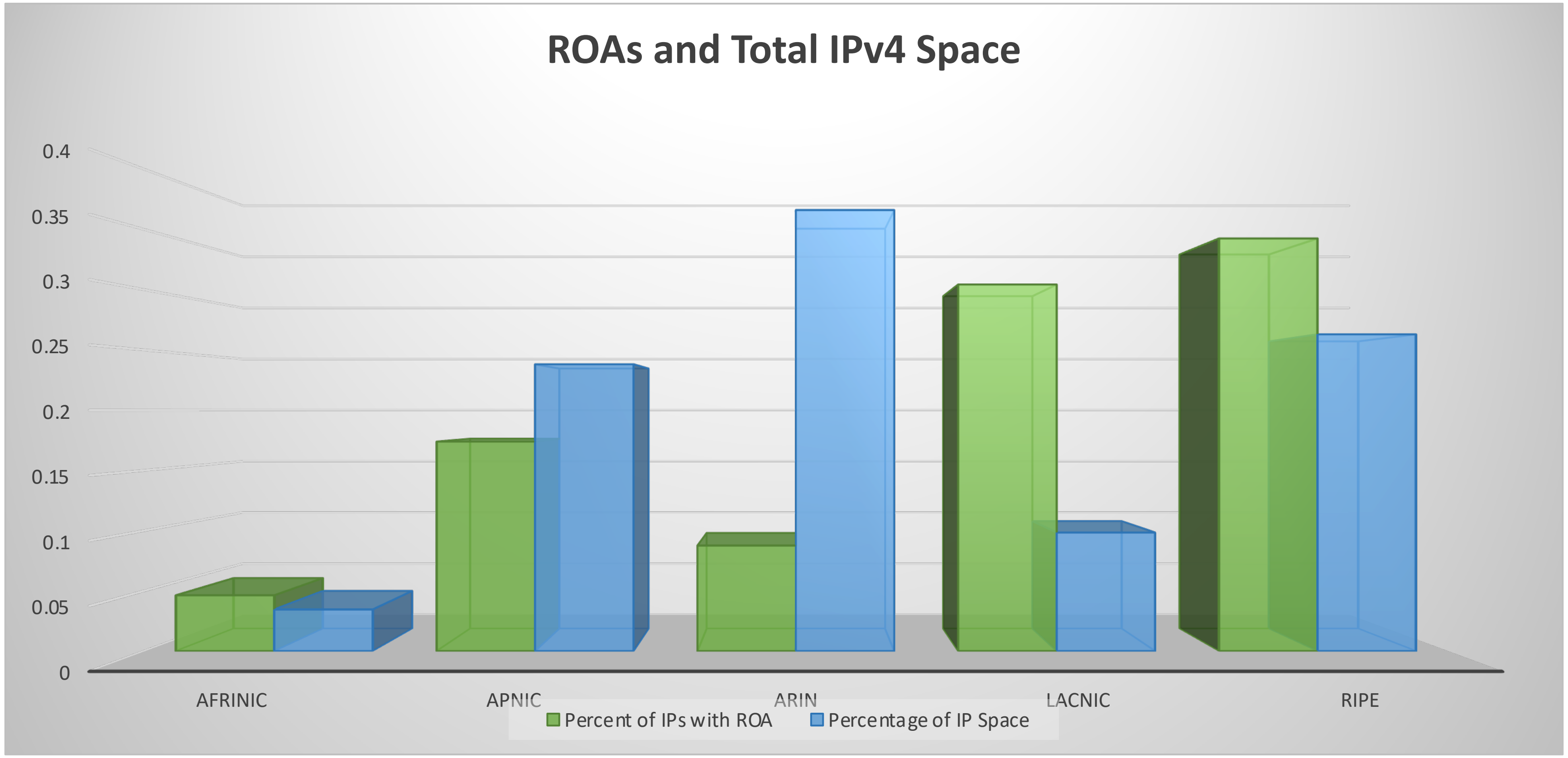
The Current State of RPKI



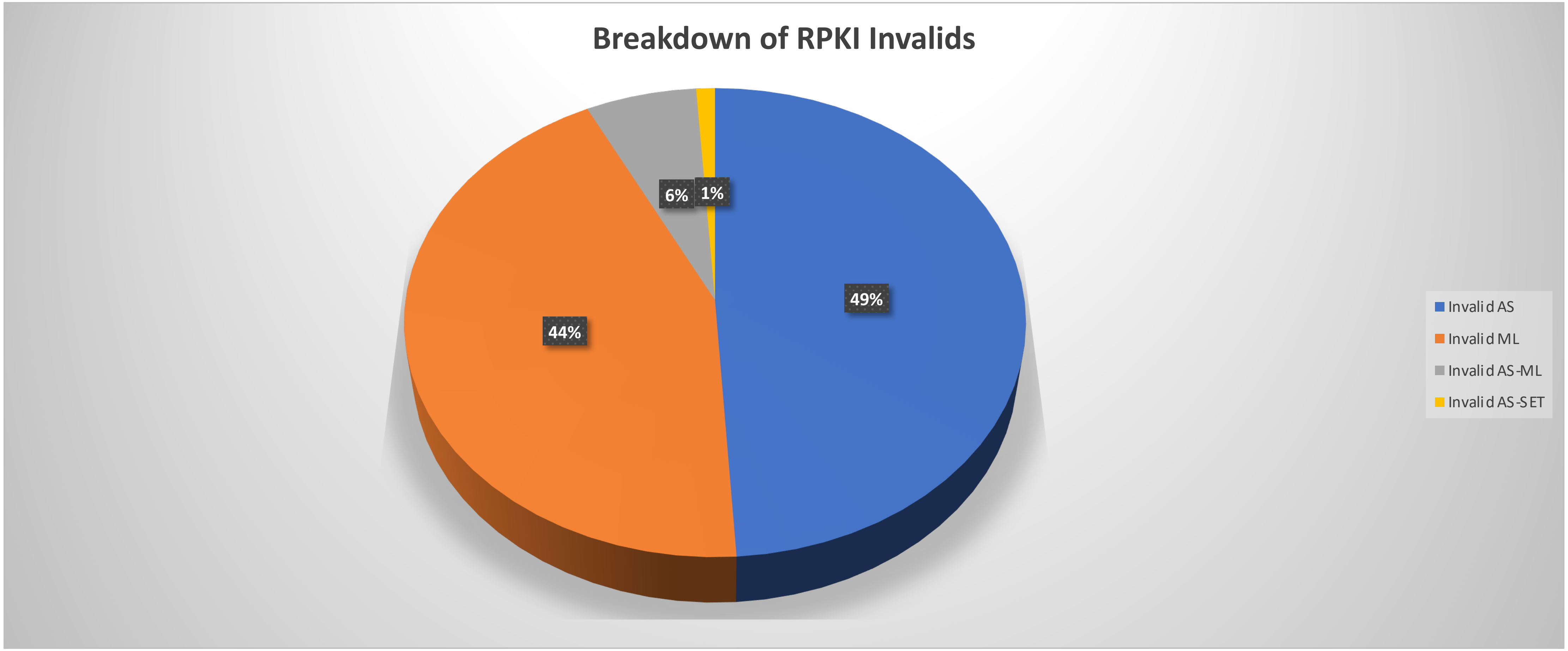
The Current State of RPKI



The Current State of RPKI



The Current State of RPKI



What RPKI Can Do for Your Network

RPKI has advantages, even if you maintain your IRR records.

- ROAs protect you against bad IRR records that might make it possible for another AS to advertise your prefix.
- ROAs are digitally signed.
- Only the RIRs, who have the allocations in the first place, have trust anchors that can sign the ROAs.

What RPKI Can’t Do for Your Network

RPKI definitely is worth implementing, but don’t stop there.

- Maintain your IRR records as accurately as you possibly can.
- Filter for bogons.
- Use AS Path filters, or what some people call Peer Lock.
- Announce all of your IP space.
- Set prefix limits.

What RPKI Can't Do for Your Network

Let's look at the 12 November 2018 Google Route Leak— Google and a number of other services experienced a 74-minute outage. Due to a configuration mistake, a small ISP re-advertised about 500 Google prefixes that it had learned from an IX route server.

- RPKI can't help here.
- AS Path filters would not have been useful.
- IRR Path filters would have helped.
- Maximum prefix limits might have helped.

What RPKI Can’t Do for Your Network

Let’s look at the June 24 Verizon outage caused by a route leak. Recall that Verizon listened to routes from a small company in Northern Pennsylvania’s route optimizer, making this downstream the preferred path of a large quantity of Internet routes transiting Verizon (AS701).

- RPKI would have dropped any invalid origin routes or prefixes with invalid lengths, possibly more efficiently than the current IRR method.
- The bad paths still would have been a problem.
- Max prefix limits would have shut down the sessions before they could have done any damage.

What Could Make RPKI Even Better

While RPKI certainly can solve some issues, the system still is capable of creating them.

The second week into our implementation of RPKI, I found the answer to the Internet’s routing woes could also cause them.

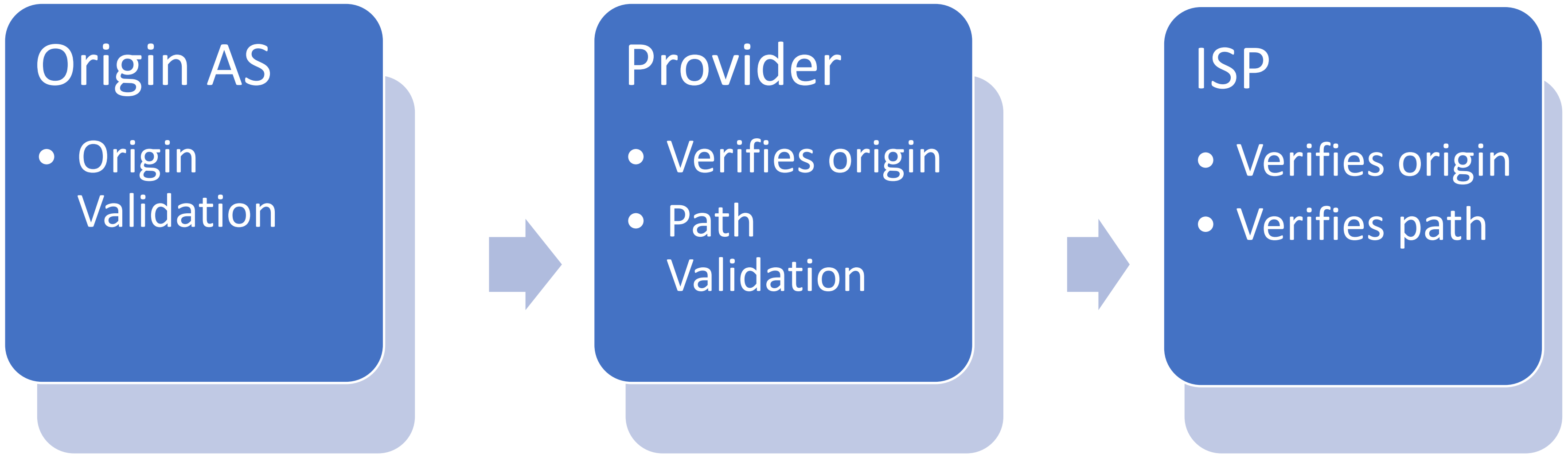
What Could Make RPKI Even Better

This leads into the second thing that could make RPKI even better, which is path validation.

- IRR path validation suffers from some of the same issues that its origin validation does: not current, not secure.
- IRR path validation only prevents against accidental route announcements.

What Could Make RPKI Even Better

Today, networks tell you what downstreams or peers they want to advertise to other networks.



Origin AS

- Origin Validation

Provider

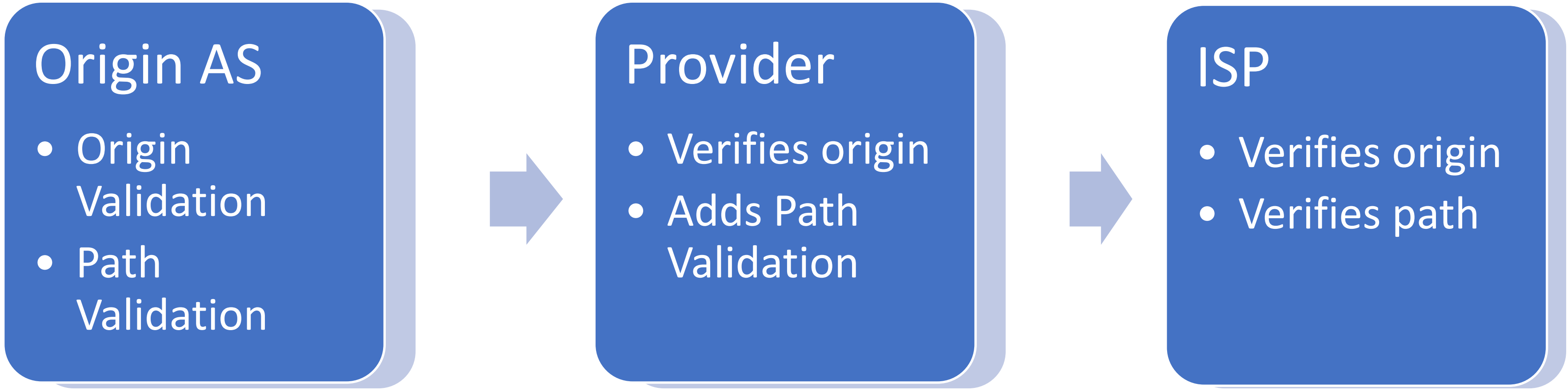
- Verifies origin
- Path Validation

ISP

- Verifies origin
- Verifies path

What Could Make RPKI Even Better

What if the advertising network had to specify which networks could advertise its routes?



Origin AS

- Origin Validation
- Path Validation

Provider

- Verifies origin
- Adds Path Validation

ISP

- Verifies origin
- Verifies path

What Could Make RPKI Even Better

An example of how this might work at Hurricane Electric with a network like Cloudflare that is widely connected.

- AS6939 would accept prefixes with AS13335 origins that were ^13335$.
- If Cloudflare were to identify Telia as an upstream, we also would accept ^1299_13335$.
- All other AS paths would be dropped as invalid.

What Could Make RPKI Even Better

I don’t have all the answers, but as a community, we definitely can find them.

- We should discuss this with the community and work together to devise simple, practical solutions.
- Who wants to collaborate?

Thank you!

Questions?

Resources

- RPKI Status Data
  https://bgp.he.net

- Routing Filter information
  http://routing.he.net

- Global Prefix/Origin Validation using RPKI
  https://rpki-monitor.antd.nist.gov