GTER 51

25 de Outubro de 2022 - São Paulo

IRR, RPKI, PeeringDB, Whois, rDNS, Geolocalização IP - Geofeeds, IRR Geoidx, Triangulação por latência

Autores: Douglas Fernando Fischer – fischerdouglas@gmail.com
Felipe Calebe - felipecalebe@made4it.com.br

Felipe Calebe Vicente de Araújo

- Analista de redes N2 - Made4IT
- Atua na área de redes desde 2019
- Tem contato com tecnologia desde 2006, aficionado na área desde 2012

- Made4it - http://www.made4it.com.br/
- Linkedin - https://www.linkedin.com/in/felipecalebe/

Intenções dessa apresentação?

- Apresentar, com uma linguagem SIMPLES, os principais cadastros que um provedor precisa possuir e a importância de mantê-los atualizados:
  - IRR
  - RPKI
  - PeeringDB
  - Whois
  - rDNS
- Apresentar os principais influenciadores na Geolocalização IP.
  - Geofeeds
  - IRR GeoIDX
  - Triangulação por latência

Dores dos nossos clientes que nos levaram a compreender melhor a importância dos cadastros

- Falhas nas liberações de prefixos nos Upstreams.
  - Latência para determinados destinos, mesmo que regionais.
- Problema com geolocalização.
  - Usuários finais com problemas para acesso a determinados conteúdos.
- Problemas de reputação de blocos IPs.
  - Hospedagem de sites e mail-servers.
  - Bloqueios por diversas empresas.

Intenções dessa apresentação?

- Apresentar, com uma linguagem SIMPLES, os principais cadastros que um provedor precisa possuir e a importância de mantê-los atualizados:
  - **IRR**
  - RPKI
  - PeeringDB
  - Whois
  - rDNS
- Apresentar os principais influenciadores na Geolocalização IP.
  - Geofeeds
  - IRR GeoIDX
  - Triangulação por latência

IRR

Foi criado para ser uma linguagem única de política de roteamento utilizada por qualquer sistema autônomo, prevenindo erros humanos e evitando problemas de compreensão.

O objetivo é ter a política de roteamento de uma rede publicada onde uma pessoa, seja ela no Brasil ou no Japão, consiga ver e entender a política de roteamento dessa rede.

O principal uso atualmente de IRR é na liberação automatizada de prefixos, o que reduz quase que por completo erros humanos na aplicação das liberações, além de tal tarefa se tornar muito mais simples e rápida.

IRR

Para criação de objetos IRR de seu ASN de maneira correta recomendamos o post na wiki do BPF explicando detalhadamente cada passo:
https://wiki.brasilpeeringforum.org/w/O_Minimo_que_Voce_precisa_saber_sobre_IRR

Para verificação da conformidade dos Objetos de IRR de um ASN ou prefixo, recomendamos a utilização da ferramenta IRR Explorer. Esta aponta inconsistências objetos Route[6], e facilita a identificação de objetos proxies.

https://irrexplorer.nlnog.net

IRR - https://irrexplorer.nlnog.net

Report for ASN AS65000

What does the prefix table show?

Explanation of different messages

Prefixes originated by AS65000

Prefix	RIR	BGP	RPKI	TC	Advice
10.0.0.0/22	LACNIC	65000	65000/24	65000	Expected route object in LACNIC, but only found in other IRRs

Report for ASN AS65000

What does the prefix table show?

Explanation of different messages

Prefixes originated by AS65000

Prefix	RIR	BGP	RPKI	LACNIC	RADB	Advice
192.168.0.0/24	LACNIC	65000	65000/24	65000		Everything looks good
192.168.1.0/24	LACNIC	65000	65000/24			No route objects match DFZ origin

IRR - Import e Export - AS-SETs

```
aut-num:        AS263569
as-name:        Direct-Wifi
descr:          DIRECT WIFI TELECOM LTDA. ME
admin-c:        LEDAL47-NICBR
tech-c:         LEDAL47-NICBR
mp-import:      afi any.unicast from AS263569:AS-TRANSIT accept ANY
mp-export:      afi any.unicast to AS263569:AS-TRANSIT announce AS263569:AS-DIRECT
mp-import:      afi any.unicast from AS263569:AS-CUSTOMERS accept PeerAS
mp-export:      afi any.unicast to AS263569:AS-CUSTOMERS annouce AS263569:AS-FULL
mnt-by:         MAINT-AS263569
changed:        felipecalebe@made4it.com.br 20220329
source:         TC
last-modified:  2022-03-29T12:25:49Z
```

Intenções dessa apresentação?

- Apresentar, com uma linguagem SIMPLES, os principais cadastros que um provedor precisa possuir e a importância de mantê-los atualizados:
  - IRR
  - **RPKI**
  - PeeringDB
  - Whois
  - rDNS
- Apresentar os principais influenciadores na Geolocalização IP.
  - Geofeeds
  - IRR GeoIDX
  - Triangulação por latência

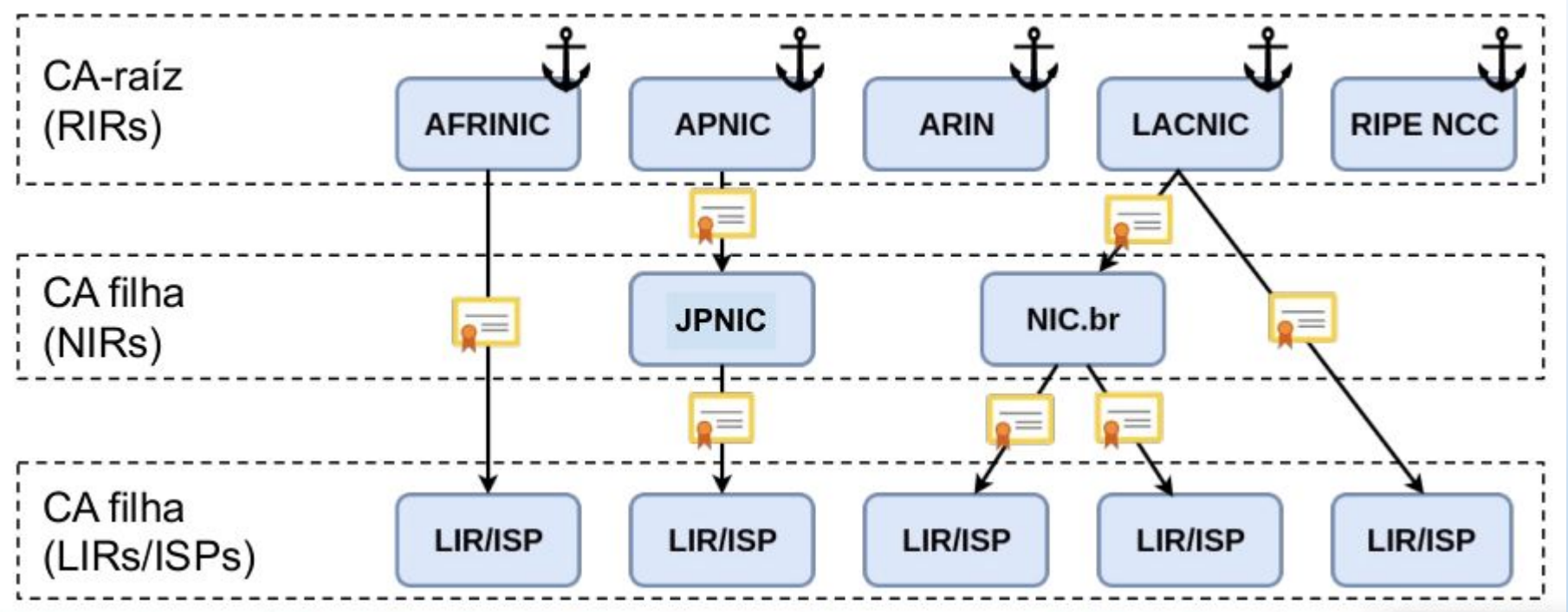
RPKI

É uma estrutura desenvolvida para validar criptograficamente rotas Internet. Ele permite a validação do ASN que originou a rota e um Prefixo.

O ASN “assina” digitalmente o seu bloco através de uma estrutura de certificados (que vem do RIR/NIR/LIR, ex: Registro.BR). Essa “assinatura” é chamada de ROA - Route Origin Authorization. Nas ROAs constam os prefixos, suas máscara de rede, e tamanho máximo de máscara, que pode ser originados por um ASN específico.

Os dados de RPKI podem então ser utilizados nos roteadores para filtrar rotas inválidas. Geralmente BGP Hijacking.

RPKI



- No Brasil - Modo Delegated - Server com Krill
- Demais RIR/NIR/LIR - Modo Hosted - No próprio portal
- Blocos com ROA tem significativa melhora de reputação

Intenções dessa apresentação?

- Apresentar, com uma linguagem SIMPLES, os principais cadastros que um provedor precisa possuir e a importância de mantê-los atualizados:
  - IRR
  - RPKI
  - **PeeringDB**
  - Whois
  - rDNS
- Apresentar os principais influenciadores na Geolocalização IP.
  - Geofeeds
  - IRR GeoIDX
  - Triangulação por latência

PeeringDB

O PeeringDB é um banco de dados de Peering entre sistemas autônomos. A manutenção das informações é feita pelos responsáveis pelo ASN. Esses dados ajudam a interconexão global de redes nos centros de dados, instalações de interconexão e IXPs - Internet Exchange Points (PTTs).

Possui uma API aberta através da qual empresas consultam de forma automatizada as informações para configuração de Filtros BGP. Limite de Prefixos, e AS-SET do IRR.

Também é utilizado como fonte de dados para contatos de Abuse e acordos de Peering.

A criação de uma organização e ASN no PeeringDB depende diretamente dos contatos de e-mail registrados no WHOIS.

PeeringDB

Direct WiFi Telecom

Some of the data on this page is incomplete, please update the fields marked with ❗ to improve data quality.

Also Known As	Direct Internet
Long Name	Direct Wifi Telecom Ltda
Website	http://www.directwifi.com.br
Address 1	Rua Rosa Sedoski Valenga, 515, Jardim Novos Horizontes
Address 2	
Floor	
Suite	
Location	Campo Magro, , 83535-000
Country Code	BR
Geocode	-25.375424, -49.42221
Last Updated	2022-10-19T13:07:42Z
Notes ❓	
Logo ❓	

Direct WiFi Telecom

Organization	Direct WiFi Telecom
Also Known As	Direct Internet
Long Name	Direct Internet
Company Website	http://www.directwifi.com.br
ASN	263569
IRR as-set/route-set ❓	TC::AS263569:AS-DIRECT
Route Server URL	
Looking Glass URL	
Network Type	Cable/DSL/ISP
IPv4 Prefixes ❓	150
IPv6 Prefixes ❓	50
Traffic Levels	200-300Gbps
Traffic Ratios	Mostly Inbound
Geographic Scope	Regional
Protocols Supported	✓ Unicast IPv4 ○ Multicast ✓ IPv6 ○ Never via route servers ❓
Last Updated	2022-07-28T22:55:15Z
Public Peering Info Updated	2022-09-22T20:19:40
Peering Facility Info Updated	2017-03-29T17:32:25Z
Contact Info Updated	2022-02-02T17:18:33
Notes ❓	
RIR Status	ok
RIR Status Updated	2022-07-28T22:55:09

PeeringDB

Peering Policy Information

Peering Policy	
General Policy	Open
Multiple Locations	Not Required
Ratio Requirement	No
Contract Requirement	Not Required
Health Check	

Contact Information

Role	Name	Phone E-Mail
Abuse	Direct Internet Team	noc@directwifi.com.br
NOC	NOC	+5544985003834 noc@directwifi.com.br
Technical	Leandro Dias de Almeida	+5541999231521 leandro@directwifi.com.br
Technical	Made4it	+5543999526000

Public Peering Exchange Points

Filter

Exchange IPv4	ASN IPv6	Speed	RS Peer
IX.br (PTT.br) Curitiba 200.219.140.176	263569 2001:12f8:0:4::176	100G	○
IX.br (PTT.br) Curitiba 200.219.140.152	263569 2001:12f8:0:4::152	100G	○
IX.br (PTT.br) São Paulo 187.16.222.36	263569 2001:12f8::222:36	100G	○
IX.br (PTT.br) São Paulo 187.16.222.198	263569 2001:12f8::222:198	20G	○
IX.br (PTT.br) São Paulo 187.16.211.161	263569 2001:12f8::211:161	10G	○

Private Peering Facilities

Filter

Facility ASN	Country City

No filter matches.
You may filter by **Facility**, **ASN**, **Country** or **City**.

Intenções dessa apresentação?

- Apresentar, com uma linguagem SIMPLES, os principais cadastros que um provedor precisa possuir e a importância de mantê-los atualizados:
  - IRR
  - RPKI
  - PeeringDB
  - **Whois**
  - rDNS
- Apresentar os principais influenciadores na Geolocalização IP.
  - Geofeeds
  - IRR GeoIDX
  - Triangulação por latência

Whois

O WHOIS é um protocolo usado para consultar informações de um determinado recurso de rede, nomes ou números. Podendo conter, dentre outras informações, os owner ou registrantes de um prefixo e/ou domínio.

Em outras palavras, o WHOIS funciona como um local público no qual você pode descobrir informações sobre um prefixo ou domínio.

Para os ASNs, quem mantém essas bases de dados são o RIR/NIR/LIR (ex: Registro.BR). As informações lá contidas podem ser atualizadas por um "handle" responsável pelo ASN e/ou prefixo.

Whois

AS26162

TITULAR	Núcleo de Inf. e Coord. do Ponto BR - NIC.BR
DOCUMENTO	05.506.560/0001-36
RESPONSÁVEL	Demi Getschko
PAÍS	BR
CONTATO DO TITULAR	FAN
CONTATO DE ROTEAMENTO	ROPTT
CONTATO DE ABUSO	ABPTT
CRIADO	29/04/2009
ALTERADO	06/03/2013

Razão Social
vs
Nome Fantasia

Bloco 187.16.192.0/19

ASN	AS26162
CONTATO DE ABUSO	ABPTT
TITULAR	Núcleo de Inf. e Coord. do Ponto BR - NIC
DOCUMENTO	05.506.560/0001-36
RESPONSÁVEL	Demi Getschko
PAÍS	BR
CONTATO DO TITULAR	FAN
CONTATO TÉCNICO	ROPTT
CRIADO	13/12/2010
ALTERADO	07/03/2013

Contato (ID) FAN

NOME	Frederico Augusto de Carvalho Neves
EMAIL	fneves@registro.br
PAÍS	BR
CRIADO	17/12/1997
ALTERADO	02/07/2020

Contato (ID) ABPTT

NOME	Abuse PTT.br
EMAIL	abuse@ptt.br
PAÍS	BR
CRIADO	08/06/2011
ALTERADO	08/06/2011

Contato (ID) ROPTT

NOME	Routing PTT.br
EMAIL	bgp@ptt.br
PAÍS	BR
CRIADO	08/06/2011
ALTERADO	07/12/2017

Intenções dessa apresentação?

- Apresentar, com uma linguagem SIMPLES, os principais cadastros que um provedor precisa possuir e a importância de mantê-los atualizados:
  - IRR
  - RPKI
  - PeeringDB
  - Whois
  - **rDNS**
- Apresentar os principais influenciadores na Geolocalização IP.
  - Geofeeds
  - IRR GeoIDX
  - Triangulação por latência

rDNS

O Sistema de Nomes de Domínio Reverso (rDNS) é o protocolo usado para traduzir o endereço IP em um nome de host.

Ao traduzir o endereço IP do servidor de envio em um nome de host, a verificação do rDNS frequentemente é usada para validar a vinculação entre um endereço IP e um domínio.

rDNS

Observa-se significativa melhora de reputação de IPs contidos em blocos que tiveram a devida correção de seus NS de rDNS.

É requisito quase imprescindível a correta configuração de rDNS para certos tipos de serviços, como por exemplo Mail-Server.

Existem implementações legadas de atualização de informação de geolocalização de IPs através de registro LOC nos rDNS

Para que se possa fazer alterações e ajustes referentes aos apontamentos dos servidores de DNS autoritativos sobre o reverso do bloco, é necessário o acesso ao portal do RIR/NIR/LIR

Intenções dessa apresentação?

- Apresentar, com uma linguagem SIMPLES, os principais cadastros que um provedor precisa possuir e a importância de mantê-los atualizados:
  - IRR
  - RPKI
  - PeeringDB
  - Whois
  - rDNS
- Apresentar os principais influenciadores na Geolocalização IP.
  - **Geofeeds**
  - IRR GeoIDX
  - Triangulação por latência

Geofeeds

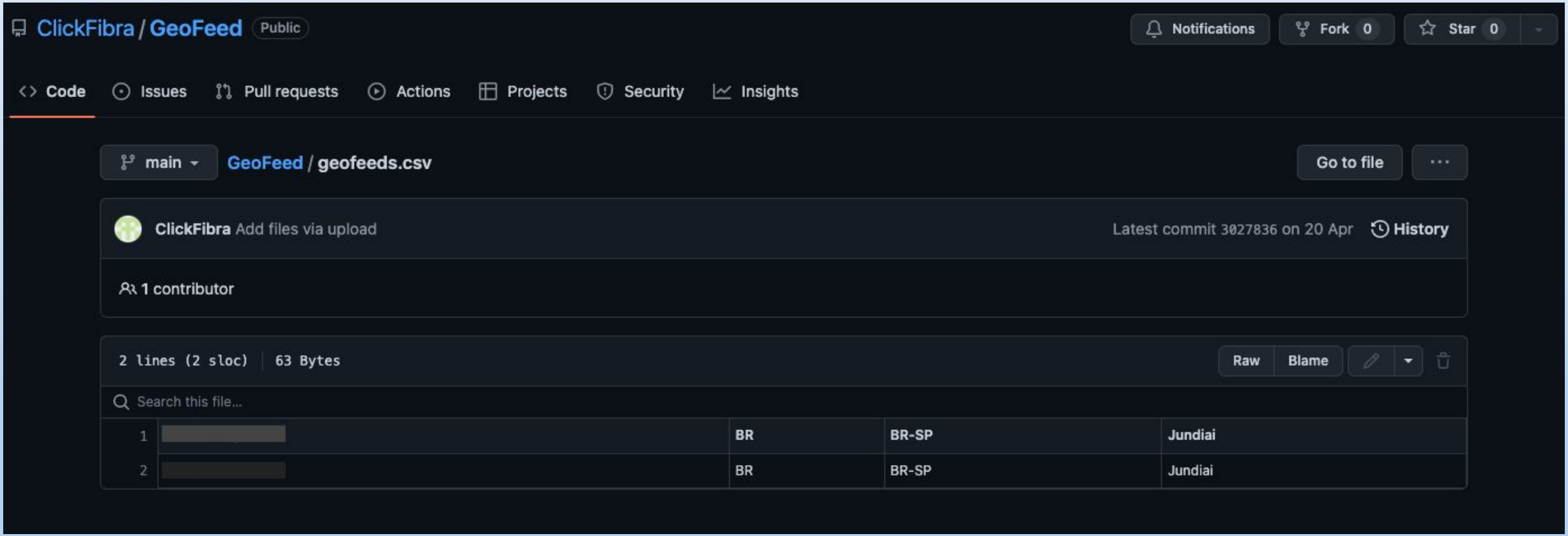
O Geofeeds é uma sintaxe utilizada para criar uma base própria de geolocalização, definida pela RFC 8805.

A ideia do Geofeeds é que você mantenha as informações de geolocalização dos seus blocos IP em uma base própria, mantendo-a sempre atualizada e disponibilizando publicamente essa base. Segundo RFC 9092, a URL para essa base de dados deve ser apontada no WHOIS do bloco IP.

O Geofeeds busca corrigir um problema comum, no caso, bases de geolocalização desatualizadas, de uma maneira mais simples e também eficiente.

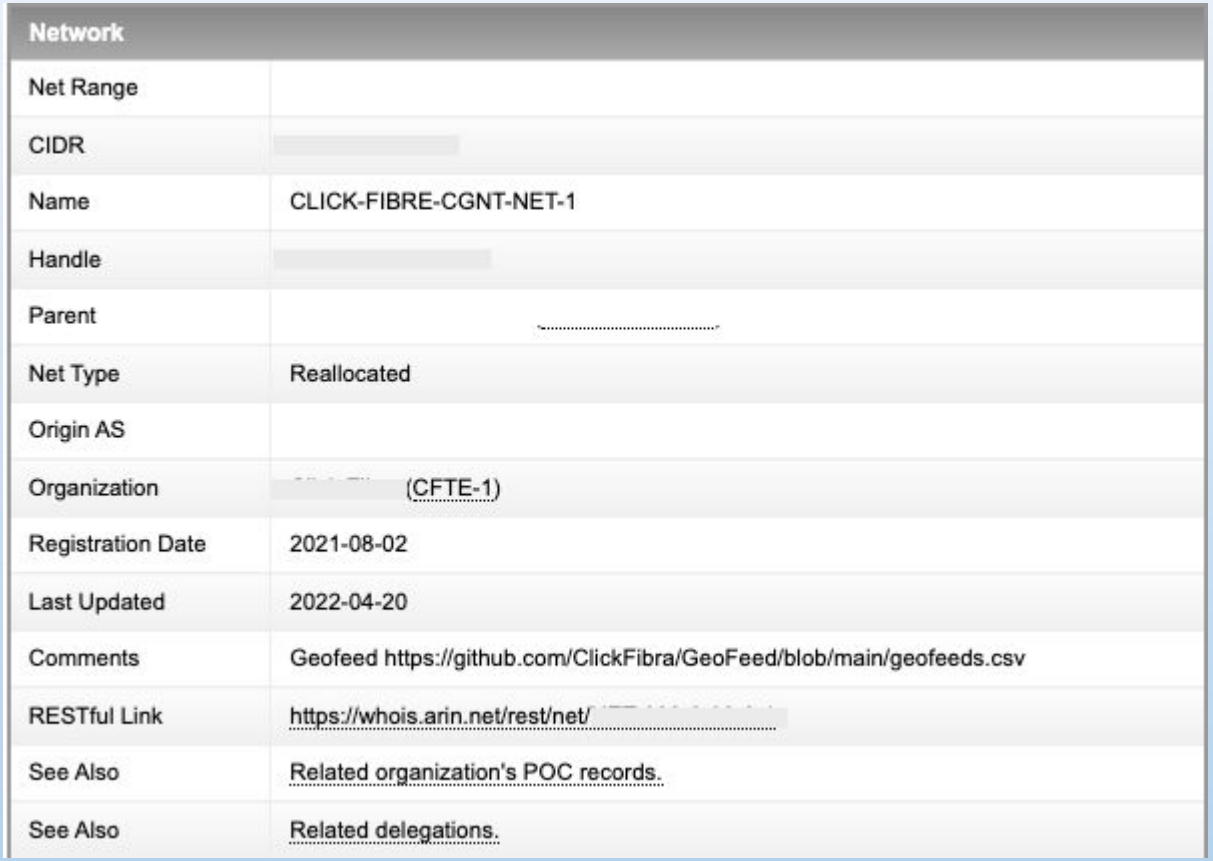
Geofeeds

O Geofeeds pode ser hospedado em um servidor próprio, porém recomendamos, pensando em alta disponibilidade, que seja hospedado no Github ou serviço similar.



Geofeeds

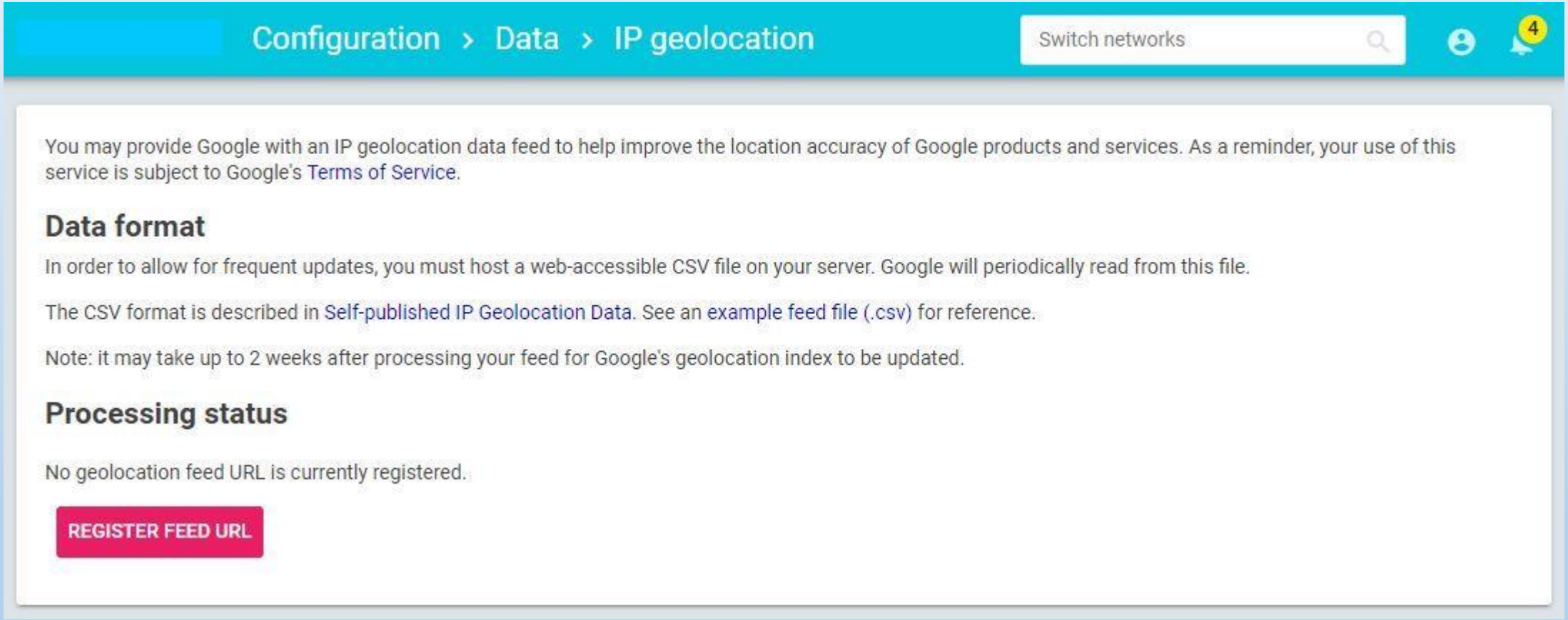
Observação: Atualmente não é possível adicionar o geofeeds no whois de prefixos do Registro.BR, porém para prefixos de outros RIRs, conseguimos adicionar utilizando os campos "remarks" ou "comments".



Network	
Net Range	
CIDR	
Name	CLICK-FIBRE-CGNT-NET-1
Handle	
Parent	
Net Type	Reallocated
Origin AS	
Organization	(CFTE-1)
Registration Date	2021-08-02
Last Updated	2022-04-20
Comments	Geofeed https://github.com/ClickFibra/GeoFeed/blob/main/geofeeds.csv
RESTful Link	https://whois.arin.net/rest/net/
See Also	Related organization's POC records.
See Also	Related delegations.

Geofeeds - isp.google.com

Alguns fornecedores de conteúdo já aceitam o Geofeeds. (ex: Google)



Intenções dessa apresentação?

- Apresentar, com uma linguagem SIMPLES, os principais cadastros que um provedor precisa possuir e a importância de mantê-los atualizados:
  - IRR
  - RPKI
  - PeeringDB
  - Whois
  - rDNS
- Apresentar os principais influenciadores na Geolocalização IP.
  - Geofeeds
  - **IRR GeoIDX**
  - Triangulação por latência

IRR GeoIDX

Seu objetivo é o mesmo que o do Geofeeds, porém, utilizando essas informações no IRR.

O GeoIDX de maneira resumida é a geolocalização dos prefixos associada ao objeto route no IRR, facilitando automações e consultas.

```
route:          45.172.252.0/22
descr:          DIRECT WIFI TELECOM LTDA. ME
origin:         AS263569
notify:         leandro@directwifi.com.br
mnt-by:          MAINT-AS263569
changed:         felipecalebe@made4it.com.br 20220803
source:         TC
geoidx:         BR
geoidx:         BR-PR
geoidx:         Campina Grande do Sul
last-modified:  2022-08-03T12:20:45Z
rpki-ov-state:  valid
```

Exemplo de objeto Route utilizando GeoIDX

Intenções dessa apresentação?

- Apresentar, com uma linguagem SIMPLES, os principais cadastros que um provedor precisa possuir e a importância de mantê-los atualizados:
  - IRR
  - RPKI
  - PeeringDB
  - Whois
  - rDNS
- Apresentar os principais influenciadores na Geolocalização IP.
  - Geofeeds
  - IRR GeoIDX
  - **Triangulação por latência**

Triangulação por latência

É uma técnica para triangular a localização de um determinado IP através da latência medida a partir de diversos pontos de origem com geolocalização conhecida.

São realizadas diversas medições a partir de origens diferentes, levando-se em conta geolocalização das origens dos testes, traceroutes também a partir dos mesmos pontos, e estado da tabela de rotas Internet.

Recomendamos a instalação de probes do RIPE-Atlas, e se possível anchors, o mais perto o possível dos hosts em que os IPs que necessitam de ajuste de geolocalização. Também evitar o bloqueio de ICMP echo, traceroutes(entre outros).

IRR - RADB/TC/ALTDB - Ativação depende dos contatos do Whois

RPKI - Depende do acesso ao portal do RIR/NIR/LIR

PeeringDB - Ativação depende dos contatos do Whois

Whois - Depende do acesso ao portal do RIR/NIR/LIR

rDNS - Depende do acesso ao portal do RIR/NIR/LIR

Geofeeds - Publicação da URL depende do Whois

IRR GeoIDX - Inserção depende do IRR

Triangulação por latência - Xô obscuridade!

Perguntas?
Sugestões?

“A escolha é possível, em certo sentido, porém o que não é possível é não escolher. Eu posso sempre escolher, mas devo estar ciente de que, se não escolher, assim mesmo estarei escolhendo.”

Jean-Paul Sartre