

IRR

Objetos Aut-Num Route(6) As-Set

Objetivo

Apresentar brevemente sobre a necessidade dos filtros de roteamento na internet e como podemos contribuir para este registro de roteamento pelo IRR de forma simples e escalável.

Para quem é destinada essa apresentação?

- Para toda pessoa ou empresa que tenha interesse em contribuir com os registros de roteamento da Internet.
- Detentores de ASNs.
- Fornecedores de Trânsito Internet, Clientes de Trânsito Internet, Participantes de Internet Exchange Points, e etc.

Terminologias

- BGP: Border Gateway Protocol
- ASN: Autonomous System Number
- RPSL: Routing Policy Specification Language
- IRR: Internet Routing Registry
- CDN: Content Delivery Network

Etapas da apresentação

1 – A importância dos filtros BGP e seus problemas.

- Porque precisamos filtrar os anúncios no BGP;
- Como são os métodos de filtragem;
- Como o IRR nos auxilia nisto.

2 – Como o IRR funciona.

- Como alcançar o IRR;
- Quais são os principais objetos de IRR?
- Explicar rapidamente o que significa cada atributo de IRR.

3 - Modelo hierárquico de AS-SETs.

- Sugestão de modelo de configuração!

1 - A importância dos filtros BGP e seus problemas.

Ao ativar um novo link, quais são os principais dados solicitados pela operadora?

- "Qual seu ASN e os prefixos?"

Mas qual é a intenção deles com isto?

- Com base nestas informações é feita algumas listas de permissões, garantindo uma mínima segurança de roteamento na internet.

O que é essa segurança de roteamento internet?

- Se trata de uma garantia que a operadora vai receber e repassar para a internet **apenas** as suas rotas e de seus clientes!

Um caso bem conhecido pela falta desta segurança:

Youtube 2008

18:47:00	Uninterrupted videos of Exploding jello
18:47:45	First evidence of hijacked route propagating in Asia, AS path 3491 17557
18:48:00	Several big trans-Pacific providers carrying hijacked route (9 ASNs)
18:48:30	Several DFZ providers now carrying the bad route (and 47 ASNs)
18:49:00	Most of the DFZ now carrying the bad route (and 93 ASNs)
18:49:30	All providers who will carry the hijacked route have it (total 97 ASNs)
20:07:25	YouTube, AS 36561 advertises the /24 that has been hijacked to its providers
20:07:30	Several DFZ providers stop carrying the erroneous route
20:08:00	Many downstream providers also drop the bad route
20:08:30	And a total of 40 some-odd providers have stopped using the hijacked route
20:18:43	And now, two more specific /25 routes are first seen from 36561
20:19:37	25 more providers prefer the /25 routes from 36561
20:28:12	Peers of 36561 start seeing the routes that were advertised to transit at 20:07
20:50:59	Evidence of attempted prepending, AS path was 3491 17557 17557
20:59:39	Hijacked prefix is withdrawn by 3491, who disconnect 17557
21:00:00	The world rejoices; Leeroy Jenkins online again.

https://circleid.com/posts/82258_pakistan_hijacks_youtube_closer_look

Event Timeline

- **Before, during and after Sunday, 24 February 2008:** AS36561 (YouTube) announces 208.65.152.0/22. Note that AS36561 also announces other prefixes, but they are not involved in the event.
- **Sunday, 24 February 2008, 18:47 (UTC):** AS17557 (Pakistan Telecom) starts announcing 208.65.153.0/24. AS3491 (PCCW Global) propagates the announcement. Routers around the world receive the announcement, and YouTube traffic is redirected to Pakistan.
- **Sunday, 24 February 2008, 20:07 (UTC):** AS36561 (YouTube) starts announcing 208.65.153.0/24. With two identical prefixes in the routing system, BGP policy rules, such as preferring the shortest AS path, determine which route is chosen. This means that AS17557 (Pakistan Telecom) continues to attract some of YouTube's traffic.
- **Sunday, 24 February 2008, 20:18 (UTC):** AS36561 (YouTube) starts announcing 208.65.153.128/25 and 208.65.153.0/25. Because of the longest prefix match rule, every router that receives these announcements will send the traffic to YouTube.
- **Sunday, 24 February 2008, 20:51 (UTC):** All prefix announcements, including the hijacked /24 which was originated by AS17557 (Pakistan Telecom) via AS3491 (PCCW Global), are seen prepended by another 17557. The longer AS path means that more routers prefer the announcement originated by YouTube.
- **Sunday, 24 February 2008, 21:01 (UTC):** AS3491 (PCCW Global) withdraws all prefixes originated by AS17557 (Pakistan Telecom), thus stopping the hijack of 208.65.153.0/24. Note that AS17557 was not completely disconnected by AS3491. Prefixes originated by other Pakistani ASs were still announced by AS17557 through AS3491.

<https://www.ripe.net/publications/news/industry-developments/youtube-hijacking-a-ripe-ncc-ris-case-study>

Esse ASN e prefixos são eternos?

Não!

Eles são periodicamente alterados quando temos:

- Alocação de um novo ASN ou bloco IP;
- Ativação ou remoção de algum cliente trânsito;
- Compra ou venda de blocos IP

Como podemos atualizar estes dados?

- Pode ser feita de maneira manual:

1 - Enviar email para sua operadora avisando a atualização (correndo risco de erro humano e entre os serviços de email)

2 – Podendo se passar vários dias até resolverem abrir a caixa de email... vão ler, aplicar a atualização nos filtros e repassar isso pra suas operadoras da mesma forma... (correndo risco de erro humano e nos meios de comunicação a cada etapa)

....

Até chegar em alguma operadora que realize isso de forma automática!

Como eu posso atualizar de forma automática?

Como o modelo manual já é considerado um grande problema desde a expansão da internet, em 1999 foi desenvolvido a RFC 2622 - RPSL
<https://datatracker.ietf.org/doc/html/rfc2622>

O RPSL é semelhante a uma linguagem de programação, que foi criada para padronizar de forma hierárquica essa atualização de dados e facilitar que os filtros de segurança sejam criados automaticamente a partir dela.

Estes dados em RPSL serão publicados no IRR, que é uma base de dados pública utilizada por algumas operadoras para prepararem seus filtros.

Algumas operadoras bem conhecidas que utilizam filtros RPSL-IRR:

Cogent;

NTT;

Lumen(Level3);

Internet Exchanges(DE-DIX, IX.BR, etc...);

CDNs...



2 - IRR

Como funciona o IRR?

- Existem diversas bases IRR globais, algumas delas:

TC(Só atende Brasil);

RADB;

AFRINC;

ARIN...

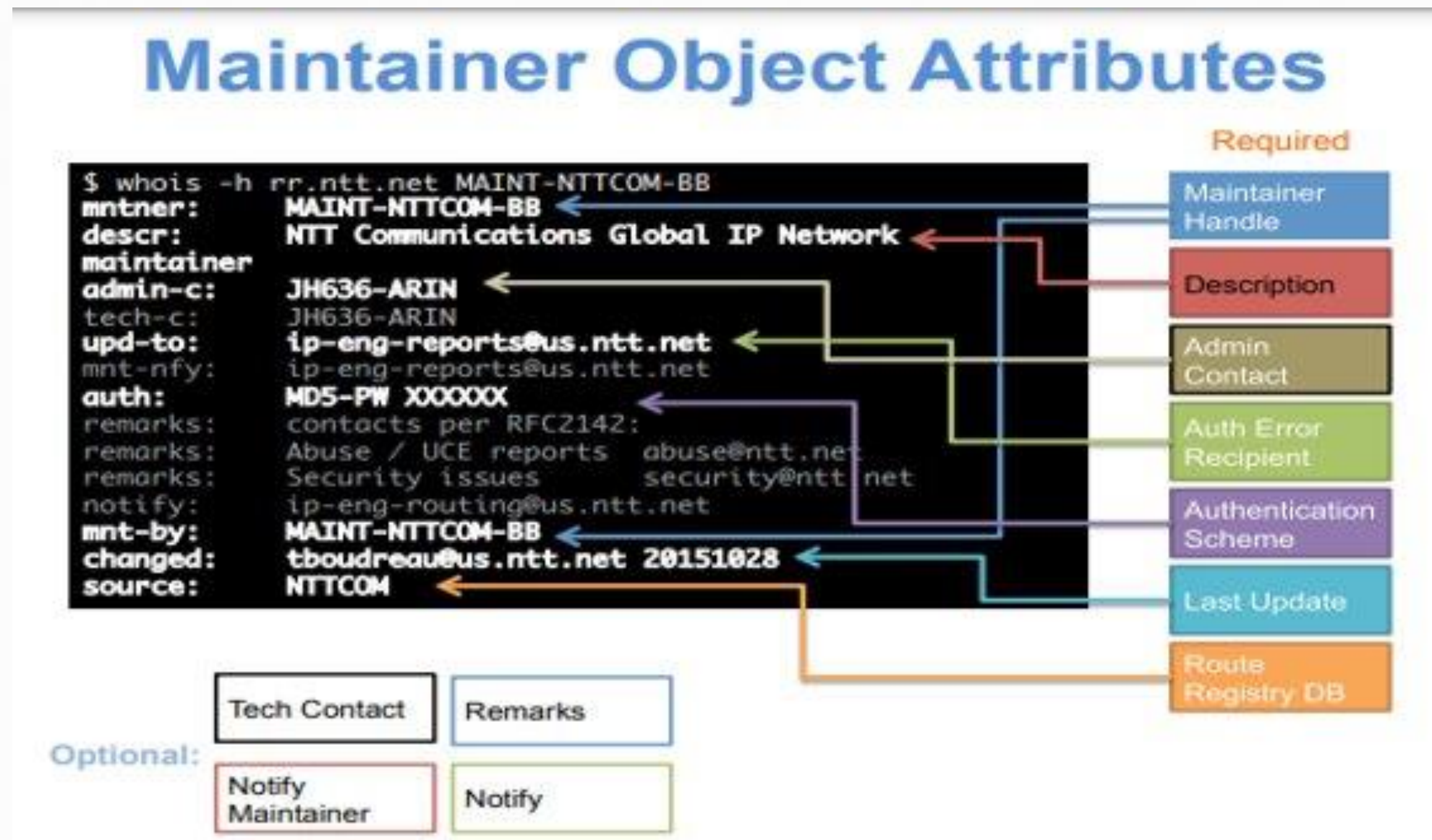
Cada uma delas são responsáveis pelos seus próprios objetos.

O que são esses Objetos?

- Orientação a objetos, que são representações digitais dos dados do dia-a-dia de roteamento internet.

Quais são os principais objetos?

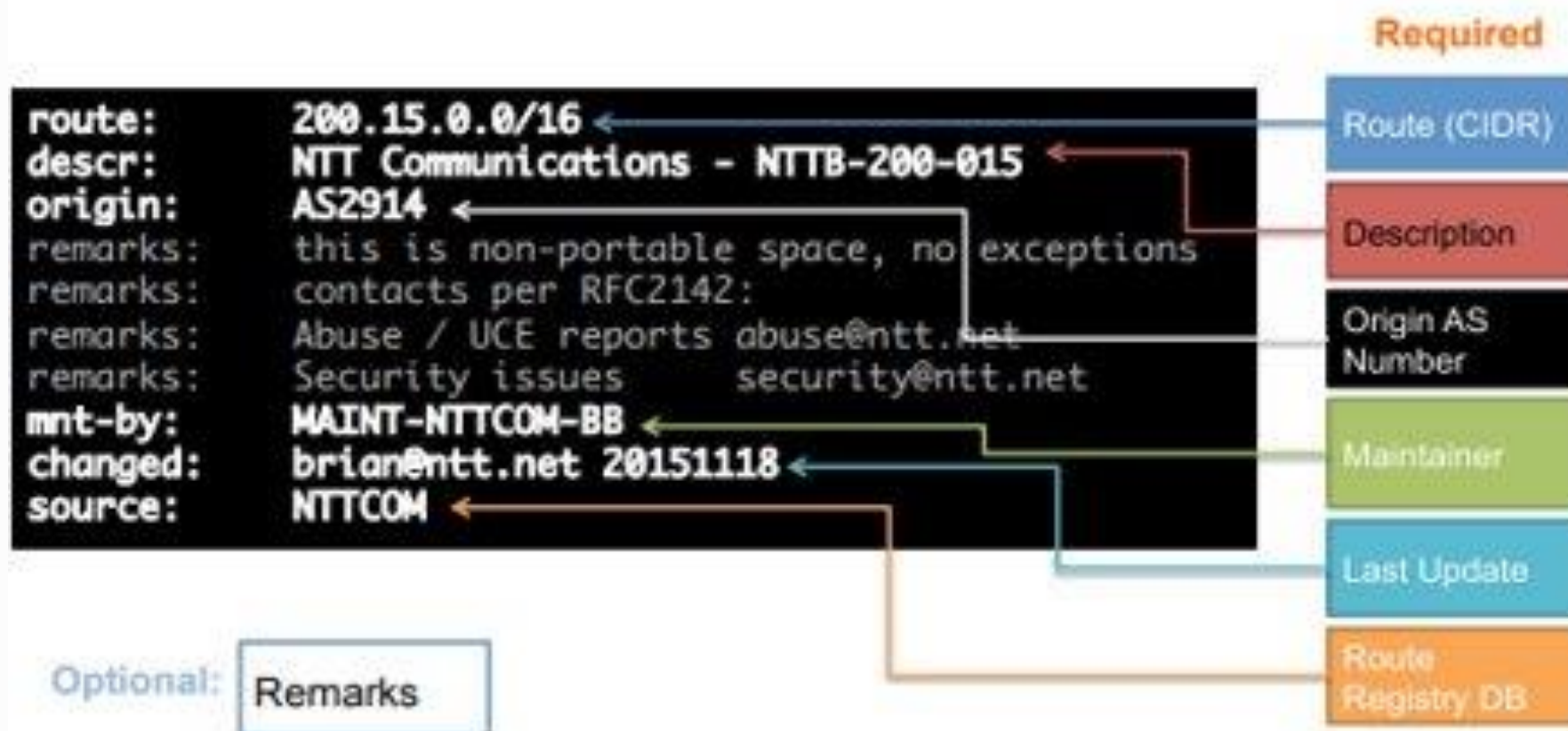
Maint -> Mantainer são as empresas ou pessoas que são responsáveis pelos objetos criados ou alterados no IRR.



Quais são os principais objetos?

Route/Route6; -> Apresentam o blocos IPv4 e IPv6 que o ASN é responsável pelo anúncio.

Route Object Attributes



Basic Route Objects

IPv4

```
route: 200.15.248.0/24
descr: ABC Corporation
origin: AS97
mnt-by: MAINT-NTTCOM-RA
changed: brian@ntt.net 20151118
source: NTTCOM
```

IPv6

```
route6: 2001:418:FFAA::/48
descr: ABC Corporation
origin: AS97
mnt-by: MAINT-NTTCOM-RA
changed: brian@ntt.net 20151118
source: NTTCOM
```

Note: "route6" is used for IPv6 objects

Quais são os principais objetos?

- AS-SET -> Grupo de ASNs, dentro desse grupo podem existir ASNs e também outros AS-SET(Grupo de grupos)

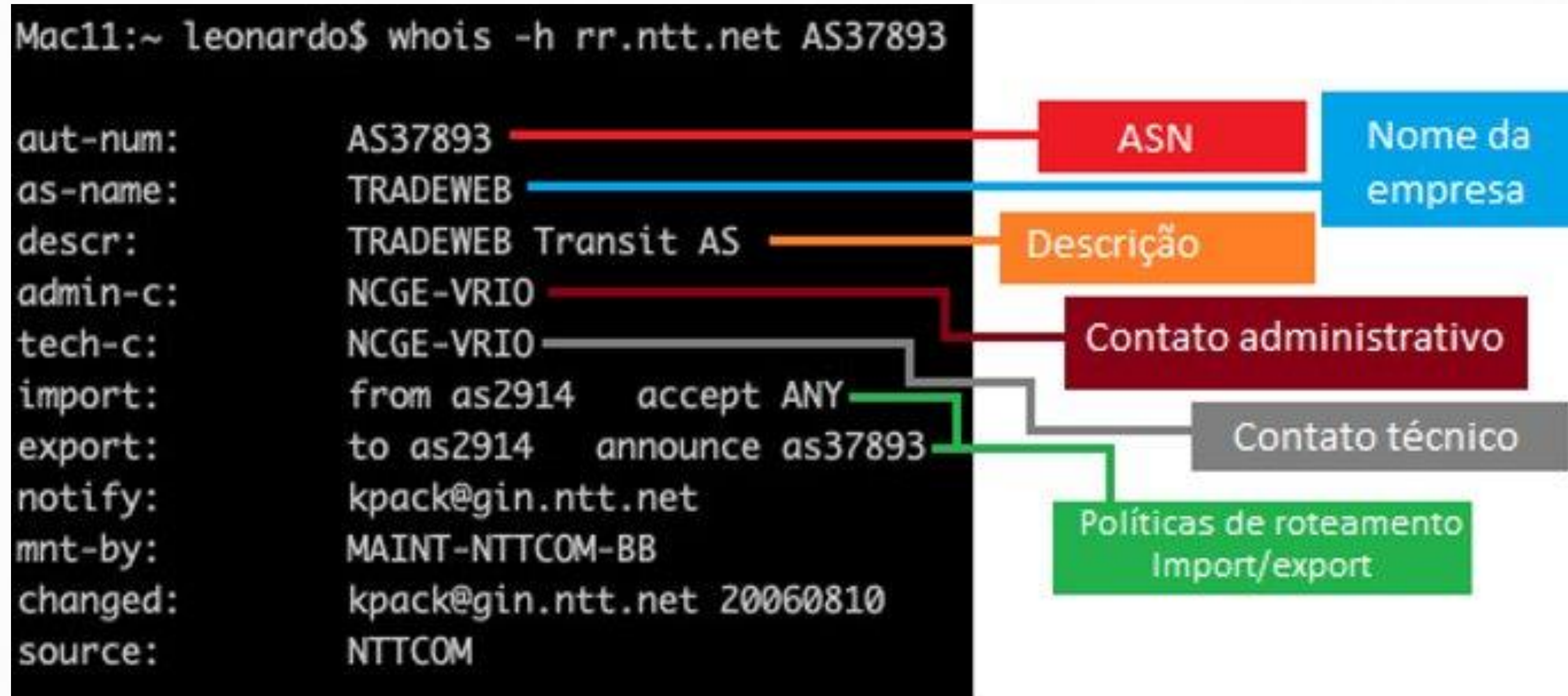
Basic AS-SET Object

```
as-set:      AS97:AS-GLOBAL
descr:      ABC Corporation Customers
members:    AS97, AS3939:AS-GLOBAL
admin-c:    NCGE-VRIO
tech-c:     NCGE-VRIO
mnt-by:     MAINT-NTTCOM-RA
changed:    brian@ntt.net 20151118
source:     NTTCOM
```

Members can be a combination of AS Numbers and AS-SET

Quais são os principais objetos?

ASN(Aut-Num); -> Contém o ASN e podemos adicionar a política de roteamento.



3 – Modelos Hierárquicos de as-set

Se apenas seguirmos a configuração básica, adicionando/removendo os ASNs como membros um atrás do outro de qualquer forma... até vai SIM funcionar. Mas trazendo uma gestão desnecessariamente extensa de diversos objetos

Um exemplo:

Na Made4it, que mantemos o IRR de diversas empresas, que muitas das vezes estão conectadas entre elas, a cada entrada ou saída de algum cliente, alteração nos recursos alocados... Teríamos que alterar esse único dado em DIVERSOS objetos de DIVERSOS maintainers.

3 – Modelos Hierárquicos de as-set

Como solução, desenvolvemos um modelo que aproveita a função recursiva do as-set (grupo de grupos) do objeto as-set! De forma que precisamos apenas atualizar alguns poucos objetos apenas no maintainer que sofreu a alteração:

Considerando que no exemplo somos o AS65000, PescadorNet, um fornecedor de trânsito e temos as seguintes conexões:

1 - Fornecedores de trânsito (UPSTREAM)

AS174 - Cogent

AS3356 - Level3

AS1299 - Telia

2 - Parceiros de peering

AS-AMAZON - Amazon (já é as-set porquê utilizam diversos asns para isso)

AS-GOOGLE - Google (já é as-set porquê utilizam diversos asns para isso)

AS-CLOUDFLARE - Cloudflare (já é as-set porquê utilizam diversos asns para isso)

AS64999 - Robson

3 - Clientes trânsito (DOWNSTREAM)

AS65123 Darwinet - (Ele próprio possui 8 Downtreams)

AS65456 HumertoNet

AS65389 SennaNet - (Ele próprio possui 1 Downtream e o as-set AS-SENNANET alinhado)

3 – Modelos Hierárquicos de as-set

Respeitando o protocolo RPSL, utilizando "ASN:AS-XXX" para as-sets macro, vamos preparar um as-set para cada grupo:

#1 - Fornecedores de trânsito (UPSTREAM)

as-set: AS65000:AS-TRANSIT
descr: List of Transit Providers of PescadorNet Internet Transit Provider
members: AS174
members: AS3356
members: AS1299
mnt-by: MAINT-AS65000
changed: registro@pescador.net.br 20211125
source: TC

#2 - Parceiros de peering

as-set: AS65000:AS-PEERING
descr: List of Peering Partner of PescadorNet Internet Transit Provider
members: AS-AMAZON
members: AS-GOOGLE
members: AS-CLOUDFLARE
members: AS64999
mnt-by: MAINT-AS65000
changed: registro@pescador.net.br 20211125
source: TC

3 – Modelos Hierárquicos de as-set

#3 - Clientes trânsito (DOWNSTREAM)

Agora que chegamos no principal!

Antes de criar um grupo para todos clientes, vamos criar um as-set para CADA cliente transito nosso adicionando seus clientes ou as-set como membro.

```
as-set: AS65000:AS-65123
descr: ASNs in cone of Darwismonet Internet Transit Provider
members: AS65123
members: AS65xx1
members: AS65xx2
members: AS65xx3
members: AS65xx4
members: AS65xx5
members: AS65xx6
members: AS65xx7
members: AS65xx8
admin-c: ADMIN-DARWINET-NICBR
tech-c: TECH-DARWINET-NICBR
mnt-by: MAINT-AS65000
changed: registroIRR@pescador.net.br 20211125
source: TC
```

```
as-set: AS65000:AS-65456
descr: ASNs in cone of HumertoNet Internet Transit Provider
members: AS65456
admin-c: ADMIN-HUMBERTONET-NICBR
tech-c: TECH-HUMBERTONET-NICBR
mnt-by: MAINT-AS65000
changed: registroIRR@pescador.net.br 20211125
source: TC
```

```
as-set: AS65000:AS-65456
descr: ASNs in cone of HumertoNet Internet Transit Provider
members: AS65456
admin-c: ADMIN-HUMBERTONET-NICBR
tech-c: TECH-HUMBERTONET-NICBR
mnt-by: MAINT-AS65000
changed: registroIRR@pescador.net.br 20211125
source: TC
```

3 – Modelos Hierárquicos de as-set

E agora sim vamos adicionar estes as-sets em um novo as-set de clientes!

```
as-set:      AS65000:AS-CUSTOMERS
descr:      ASNs in cone of PescadorNet ITP
members:    AS65000:AS-65123
members:    AS65000:AS-65456
members:    AS65000:AS-65389
mnt-by:     MAINT-AS65000
changed:    registrolrr@pescador.net.br 20211125
source:     TC
```

3 – Modelos Hierárquicos de as-set

Desta forma, qualquer atualização vamos precisar mexer apenas no AS-SET referente, exemplo:

1 - Cancelamos o peering com o AS64999 - Robson. Vamos precisar apenas remove-lo do AS65000:AS-PEERING

```
as-set: AS65000:AS-PEERING
descr: List of Peering Partner of PescadorNet Internet Transit Provider
members: AS-AMAZON
members: AS-GOOGLE
members: AS-CLOUDFLARE
mnt-by: MAINT-AS65000
changed: registrolRR@pescador.net.br 20211125
source: TC
```

2 - Nosso querido AS65123 - Darwinet fez jus ao seu nome e resolveu criar um as-set contendo seu ASN e de seus clientes! AS-DARWINISMO. Vamos precisar alterar apenas no AS65000::AS-65123

```
as-set: AS65000:AS-65123
descr: ASNs in cone of Darwinismoet Internet Transit Provider
members: AS-DARWINISMO
admin-c: ADMIN-DARWINET-NICBR
tech-c: TECH-DARWINET-NICBR
mnt-by: MAINT-AS65000
changed: registrolRR@pescador.net.br 20211125
source: TC
```

Até agora só vimos como seria a casa arrumada e se fossemos utilizar os as-sets sem a recursividade ou um padrão?



Provavelmente teríamos algo como

```
as-set: AS-CUSTOMERS
descr: ASNs in cone of Darwinet Internet Transit Provider
members: AS65123
members: AS65xx1
members: AS65xx2
members: AS65xx3
members: AS65xx4
members: AS65xx5
members: AS65xx6
members: AS65xx7
members: AS65xx8
members: AS65456
members: AS65389
members: AS65xx9
admin-c: ADMIN-DARWINET-NICBR
tech-c: TECH-DARWINET-NICBR
mnt-by: MAINT-AS65000
changed: registroIRR@pescador.net.br 20211125
source: TC
```

Desta forma teríamos alguns casos problemas que trariam dores de cabeça e desorganização:

- E se o cliente AS65456 resolve ativar alguns downstreams nele?

Vamos precisar jogar eles no final da lista embaralhando tudo ou no meio dela?

- E se algum destes downstream ter link com 2 ou mais de nossos clientes?

Vamos repetir o ASN dele várias vezes na lista?

- E se algum de nossos clientes cancelar nosso link e resolvemos apagar todo ASN ligado a ele e conflitar com o caso acima?

...

E se nem usarmos as-set? Jogarmos direto para as políticas do aut-num?



Com sorte teríamos algo como

1

```
aut-num: AS65000
as-name: PescadorNet
descr: PescadorNet
admin-c: PESCADORNET-NICBR
tech-c: PESCADORNET-NICBR
import: from AS65123 accept AS65123
import: from AS65123 accept AS65xx1
import: from AS65123 accept AS65xx2
import: from AS65123 accept AS65xx3
import: from AS65123 accept AS65xx4
import: from AS65123 accept AS65xx5
import: from AS65123 accept AS65xx6
import: from AS65123 accept AS65xx7
import: from AS65123 accept AS65xx8
export: to AS65123 announce ANY
import: from A65456 accept A65456
export: to AS65456 announce ANY
import: from AS65389 accept AS-SENNANET
export: to 65389 announce ANY
export: to 65389 announce
export: to AS174 announce AS65000
export: to AS174 announce AS65123
export: to AS174 announce AS65xx1
export: to AS174 announce AS65xx2
export: to AS174 announce AS65xx3
```

```
export: to AS174 announce AS65xx4
export: to AS174 announce AS65xx5
export: to AS174 announce AS65xx6
export: to AS174 announce AS65xx7
export: to AS174 announce AS65xx8
export: to AS174 announce A65456
export: to AS174 announce AS-SENNANET
export: to AS3356 announce AS65000
export: to AS3356 announce AS65123
export: to AS3356 announce AS65xx1
export: to AS3356 announce AS65xx2
export: to AS3356 announce AS65xx3
export: to AS3356 announce AS65xx4
export: to AS3356 announce AS65xx5
export: to AS3356 announce AS65xx6
export: to AS3356 announce AS65xx7
export: to AS3356 announce AS65xx8
export: to AS3356 announce A65456
export: to AS3356 announce AS-SENNANET
export: to AS1299 announce AS65000
export: to AS1299 announce AS65123
export: to AS1299 announce AS65xx1
export: to AS1299 announce AS65xx2
export: to AS1299 announce AS65xx3
export: to AS1299 announce AS65xx4
```

3

```
export: to AS1299 announce AS65xx5
export: to AS1299 announce AS65xx6
export: to AS1299 announce AS65xx7
export: to AS1299 announce AS65xx8
export: to AS1299 announce A65456
export: to AS1299 announce AS-SENNANET
export: to AS65123 announce AS65000
export: to AS65123 announce AS65123
export: to AS65123 announce AS65xx1
export: to AS65123 announce AS65xx2
export: to AS65123 announce AS65xx3
export: to AS65123 announce AS65xx4
export: to AS65123 announce AS65xx5
export: to AS65123 announce AS65xx6
export: to AS65123 announce AS65xx7
export: to AS65123 announce AS65xx8
export: to AS65123 announce A65456
export: to AS65123 announce AS-SENNANET
export: to AS65456 announce AS65000
export: to AS65456 announce AS65123
export: to AS65456 announce AS65xx1
export: to AS65456 announce AS65xx2
export: to AS65456 announce AS65xx3
export: to AS65456 announce AS65xx4
export: to AS65456 announce AS65xx5
```

4

```
export: to AS65456 announce AS65xx6
export: to AS65456 announce AS65xx7
export: to AS65456 announce AS65xx8
export: to AS65456 announce A65456
export: to AS65456 announce AS-SENNANET
export: to AS65389 announce AS65000
export: to AS65389 announce AS65123
export: to AS65389 announce AS65xx1
export: to AS65389 announce AS65xx2
export: to AS65389 announce AS65xx3
export: to AS65389 announce AS65xx4
export: to AS65389 announce AS65xx5
export: to AS65389 announce AS65xx6
export: to AS65389 announce AS65xx7
export: to AS65389 announce AS65xx8
export: to AS65389 announce A65456
export: to AS65389 announce AS-SENNANET
mnt-by: MAINT-AS65000
changed: registro@PESCADORNET.net.br
20211125
source: TC
```

BÔNUS!

Um exemplo de aut-num
com políticas de rotas definidas
utilizando os as-sets recursivos

BÔNUS!

Seguindo o modelo recursivo, vai depender dos serviços utilizados e da criatividade para criar os as-sets e representa-los nas politicas de roteamento.

```
aut-num: AS65000
as-name: PescadorNet
descr: PescadorNet
admin-c: PESCADORNET-NICBR
tech-c: PESCADORNET-NICBR
mp-import: afi any.unicast from AS65000:AS-TRANSIT accept ANY
mp-export: afi any.unicast to AS65000:AS-TRANSIT announce AS65000:AS-PESCADORNET
mp-import: afi any.unicast from AS65000:AS-PEERING accept PeerAS
mp-export: afi any.unicast to AS65000:AS-PEERING announce AS65000:AS-PESCADORNET
mp-import: afi any.unicast from AS65000:AS-CUSTOMERS accept PeerAS
mp-export: afi any.unicast to AS65000:AS-CUSTOMERS announce AS65000:AS-FULL
mnt-by: MAINT-AS65000
changed: registro@PESCADORNET.net.br 20210830
source: TC
```

Obrigado!

Agradeço a presença de todos!

Contato: noc@made4it.com.br

 @made4it

 Made4it soluções em ti

 Made4it

