

DAERO / Gerência de Operações

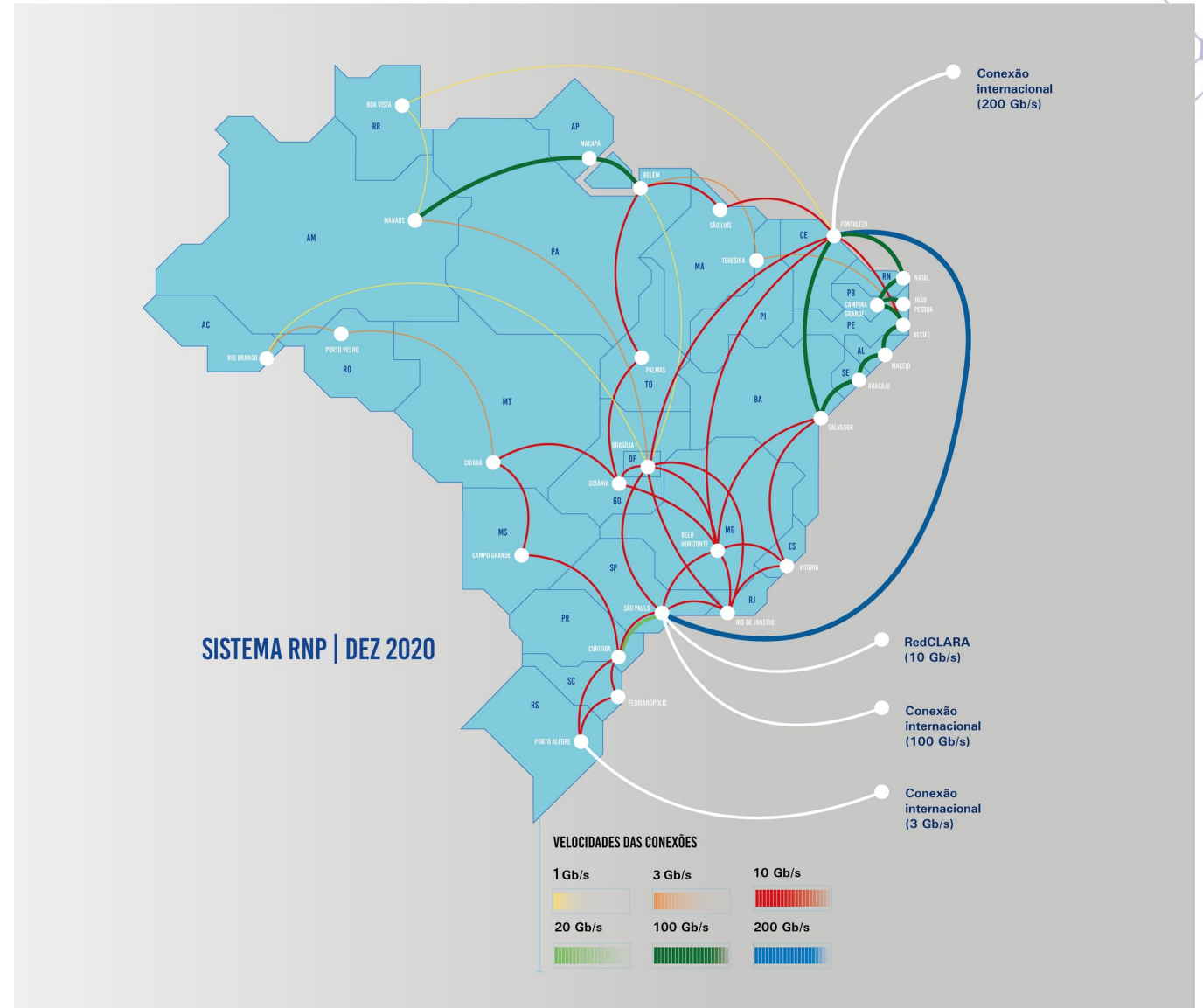
Serviço DNS Anycast recursivo da RNP
GTER 50

Agenda

- Introdução/Motivação
- IP Anycast
- Arquitetura do serviço
 - Uso de containers
 - IGP e EGP
- Automação
- Monitoramento
- Estatísticas

RNP

- Pioneira no Brasil
- OS do MCTI
- Rede para educação e Pesquisa
- Formada por
 - RedeIPê (BB)
 - PoPs
 - Redes COMEPs
 - Integração Internacional
 - Serviços
 - P&D



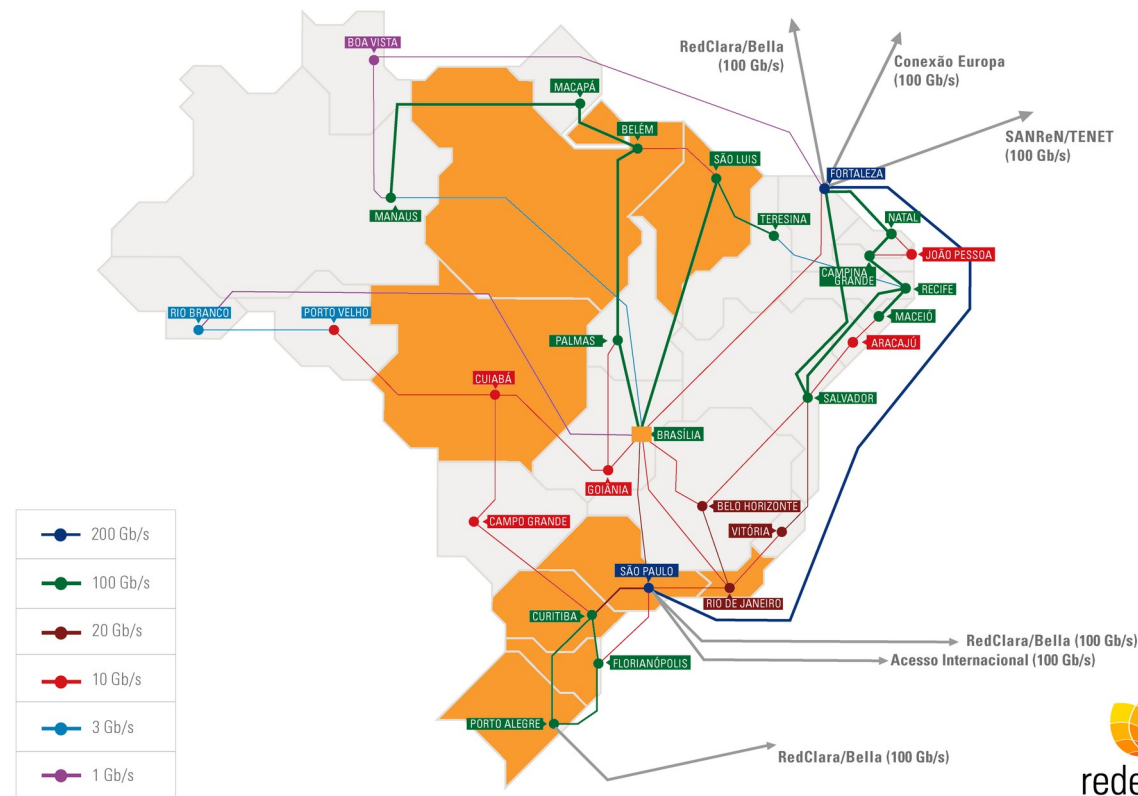
Considerações

- DNS é fundamental para o uso da Internet desde seus primórdios
- Desempenho
 - Diretamente ligado a experiência do usuário
 - Servidores DNS lentos ou falhos trazem consequências negativas para os demais serviços que dependem deles
- Segurança
 - Sua análise viabiliza a detecção de *malwares*, C&C, etc.
 - Podem ser abusados para viabilizar ataques de Man-in-the-Middle (MitM)

DNS Anycast RNP | O que é?

- É um serviço de DNS recursivo para todo o sistema RNP
- Esse serviço utiliza técnica de roteamento Anycast, permitindo que múltiplas "cópias" sejam replicadas pelo backbone da RNP
- Atualmente implantado em 9 PoPs
 - RS, SC, PR, SP, RJ, DF, MT, MA e PA*
 - *(em ativação)

Serviço DNS Anycast implantado nos PoPs da RNP (2021)



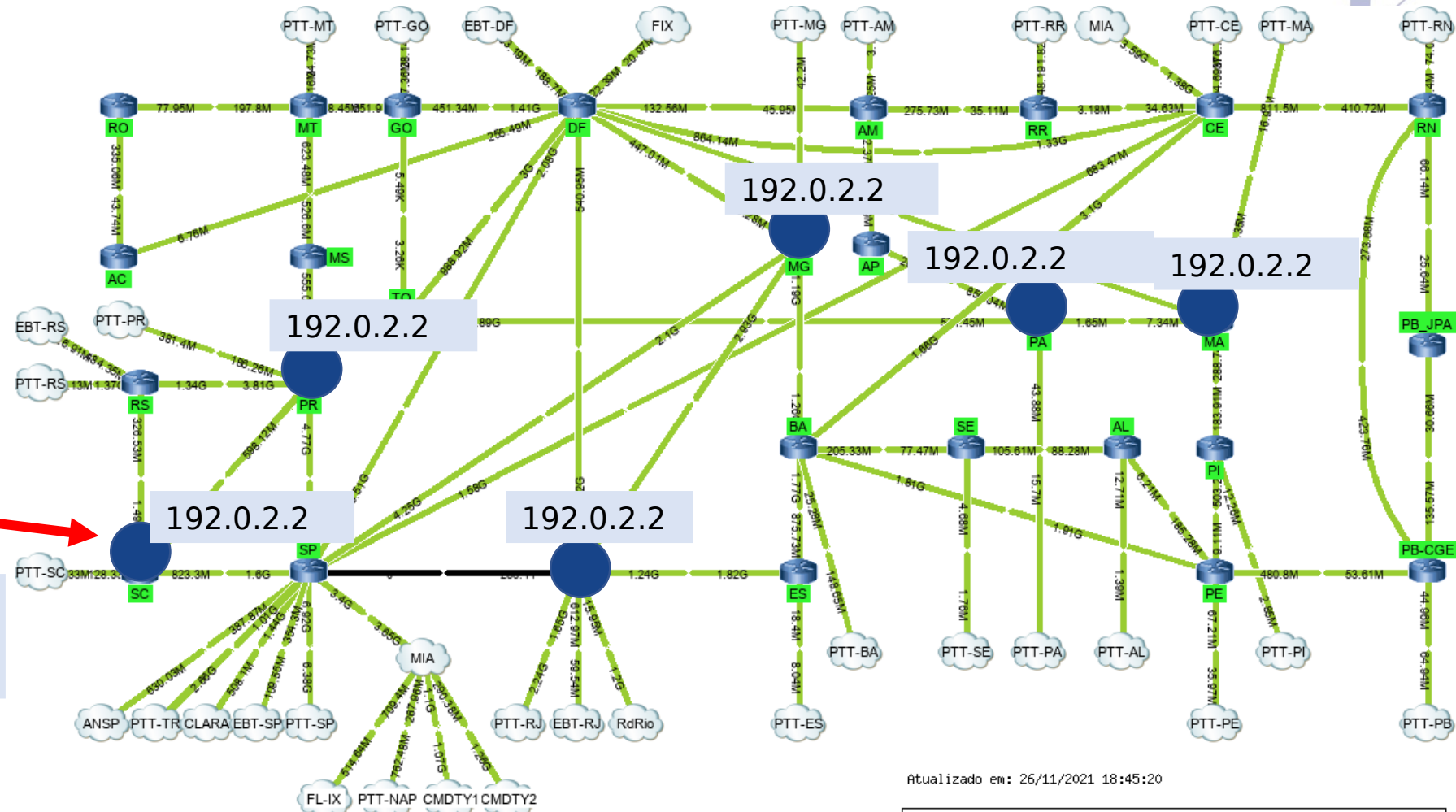
ANYCAST | Exemplo 1: Serviço operacional (up) em Santa Catarina

IP Anycast : 192.0.2.2 (*)

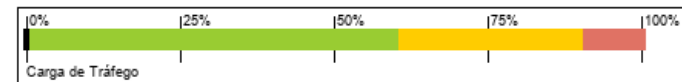
Usuário em SC

Acessando serviço Anycast no IP 192.0.2.2

Melhor caso: encontrará o serviço no PoP em que está conectado...



Atualizado em: 26/11/2021 18:45:20



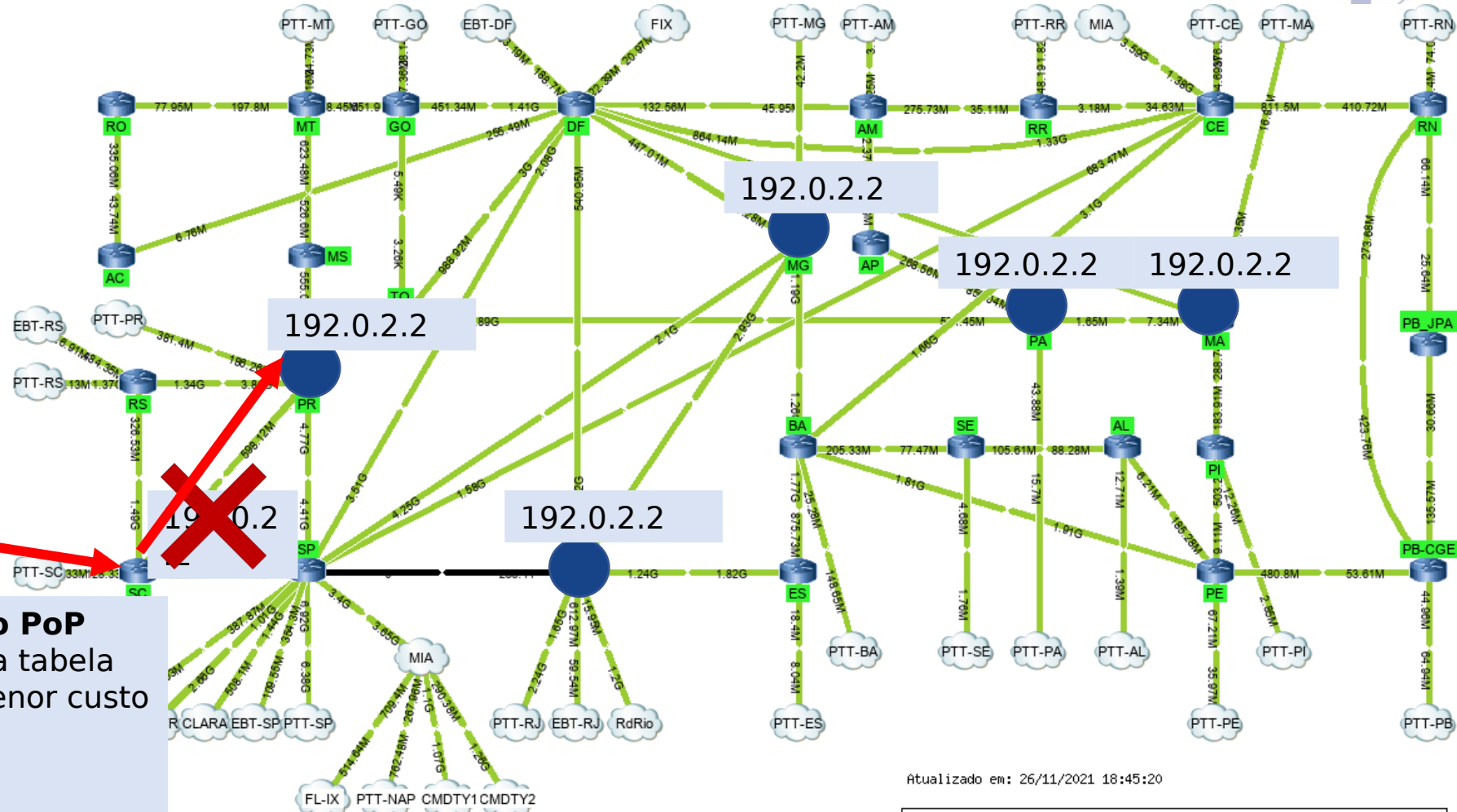
(*) RFC 5737 - reservado documentação

ANYCAST | Exemplo 2: Serviço indisponível (down) em Santa Catarina

IP Anycast : 192.0.2.2 (*)

Usuário em SC

Acessando serviço Anycast qualquer no IP 192.0.2.2



Caso: Falha do serviço dentro do PoP

- Rota Anycast local não está mais na tabela
- Será roteada para o caminho de menor custo
- Serviço entregue em PoP adjacente
- Pequeno aumento de latência
- Serviço disponível para o usuário

Atualizado em: 26/11/2021 18:45:20



(*) RFC 5737 - reservado documentação

ANYCAST | Exemplo 3: Serviço indisponível (down) em múltiplos PoPs

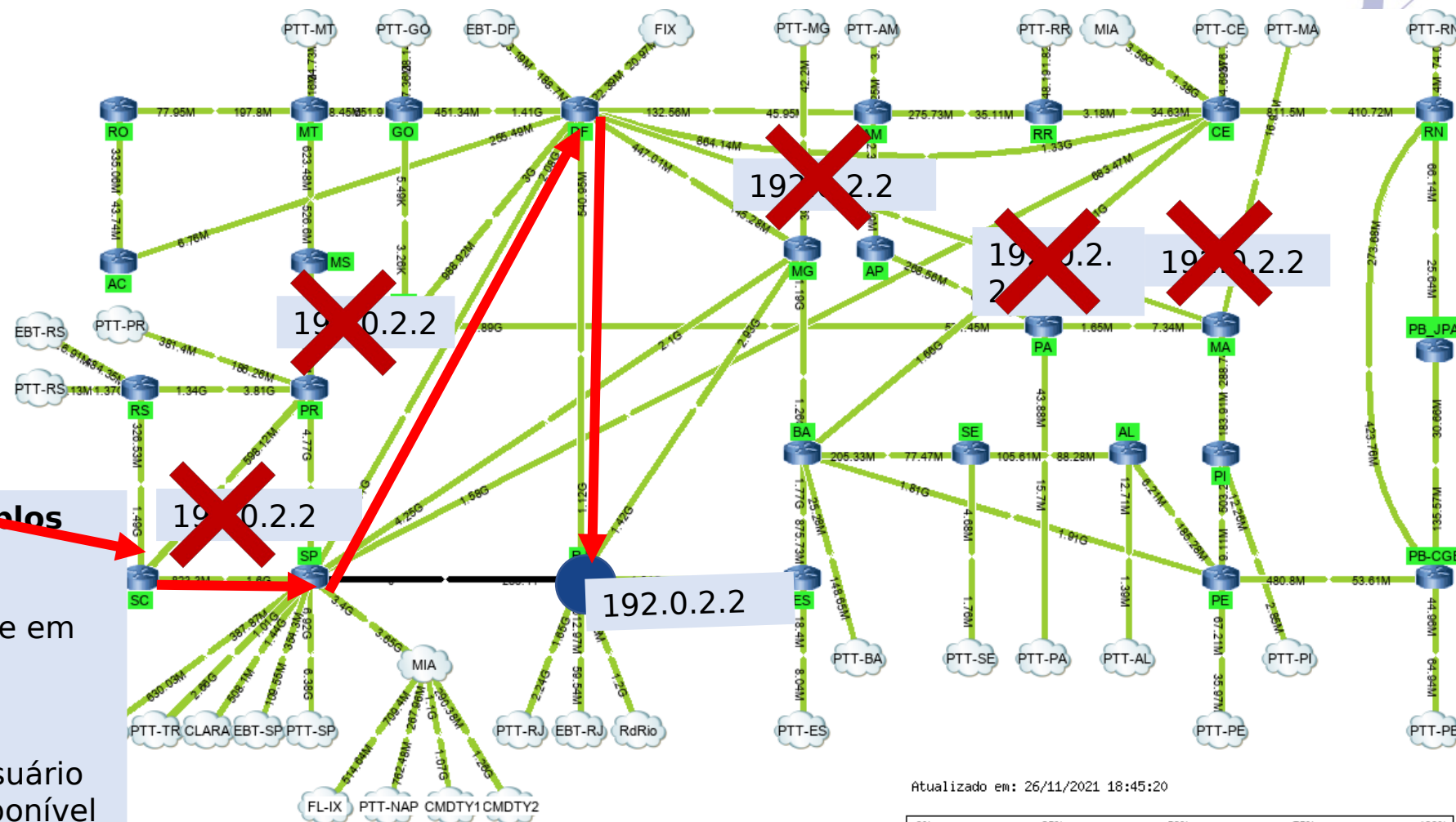
IP Anycast : 192.0.2.2 (*)

Usuário em SC

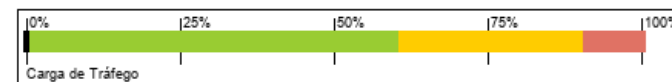
Acessando serviço Anycast qualquer no IP 192.0.2.2

Caso: Falha do serviço em múltiplos PoPs

- Temos aqui "o caos controlado"
- Rota Anycast está presente somente em um PoP
- Serviço estará disponível no PoP-RJ
- Impacto no aumento de latência
- Porém, serviço disponível para o usuário
- SD sem chamados de serviço indisponível
- A maioria dos usuários nem perceberá a mudança do servidor



Atualizado em: 26/11/2021 18:45:20



*) RFC 5737 - reservado

Prover um serviço de DNS Recursivo para o sistema RNP

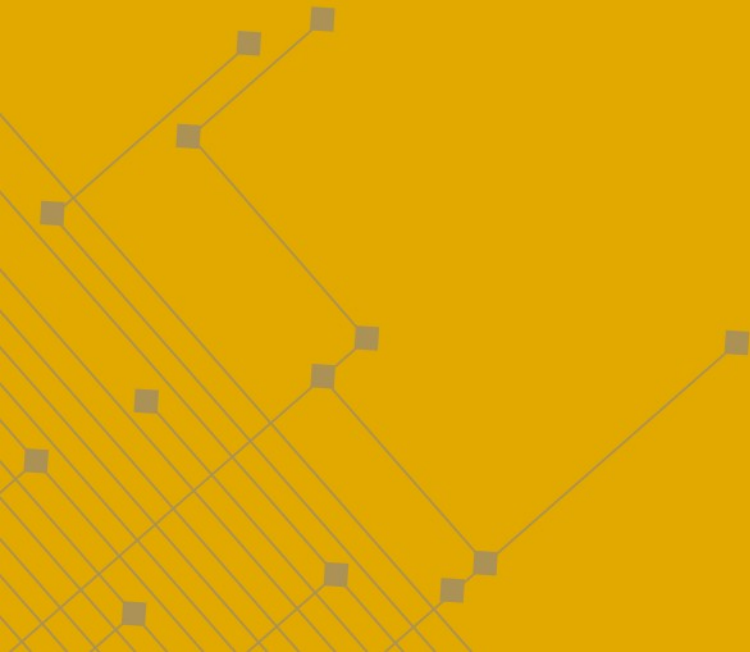
- **Baixa latência** -> Implantar nos PoPs da RNP
- **Alta disponibilidade** -> Possuir várias réplicas {locais e remotas}
- **Tolerante a falhas** -> Detectar condições de erros e tentar resolver
- **Escalável** -> Crescer conforme a demanda de uso
- **Seguro** -> Validar DNSSEC; possibilidade de aplicar requisitos de segurança e viabilidade de acoplar soluções de segurança {filtro de malware, conteúdo adulto (escolas), etc..);
- **Resolvedores únicos para todo o sistema RNP**
 - -> uso de Anycast



Características

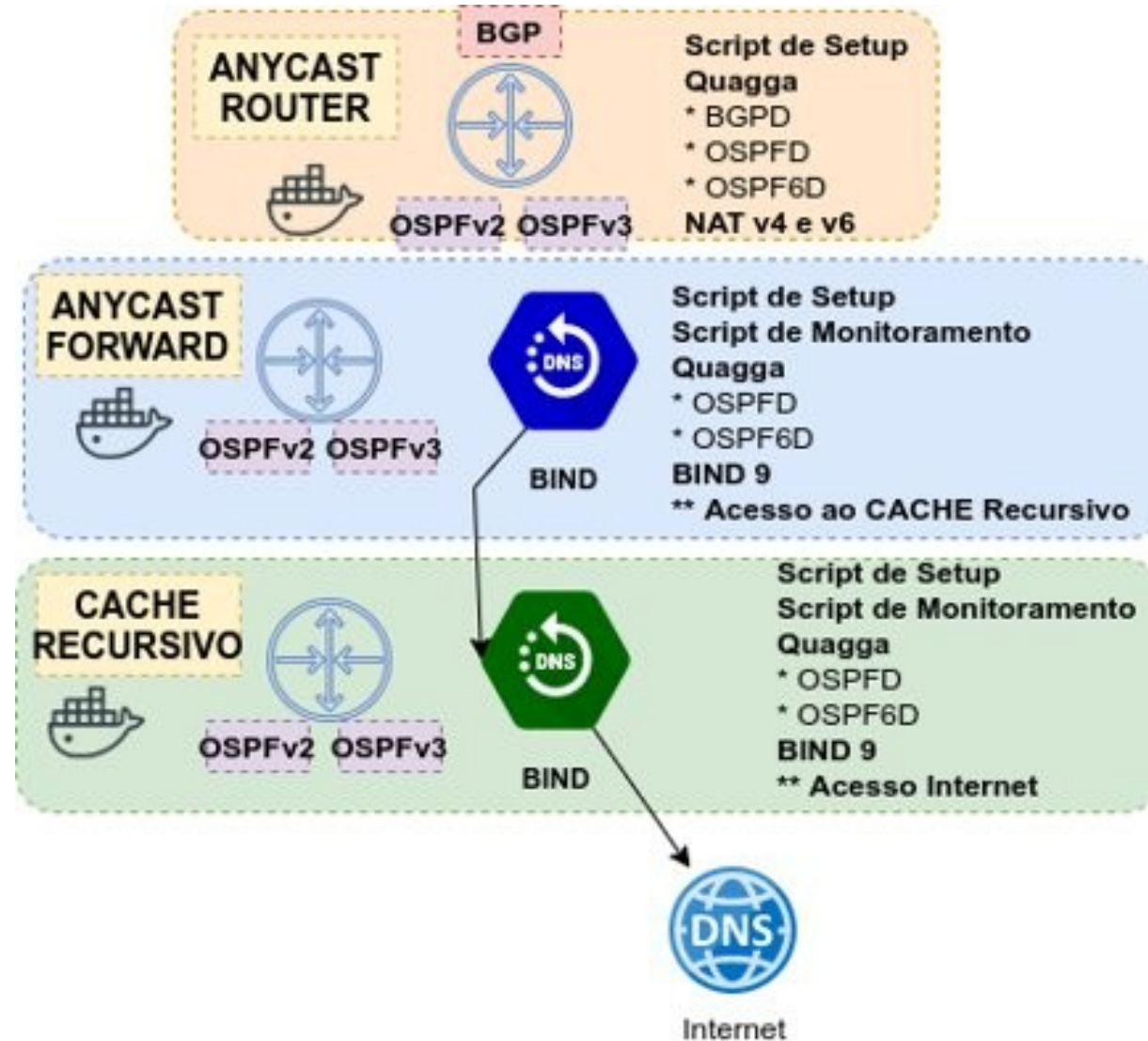
- Objetivo principal é proporcionar melhor experiência no uso da rede IPÊ
- Alta disponibilidade
- Baixa latência - Implantado localmente nos PoPs
- Hyperlocal
- Validação de DNSSEC
- RPZ disponível
- DNSTAP
- Logs legais e de aplicação centralizados
- Deploy automatizado (servidores)
- Serviço Monitorado pelo SD & Estatísticas por nó
- Em conformidade com MCI e LGPD
- Otimiza o uso das CDNs implantadas no backbone da RNP

Como o serviço foi formatado

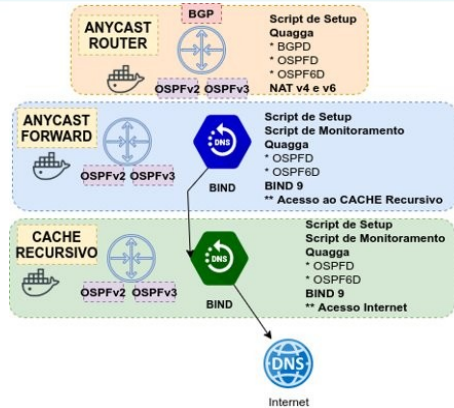




Serviço DNS RNP



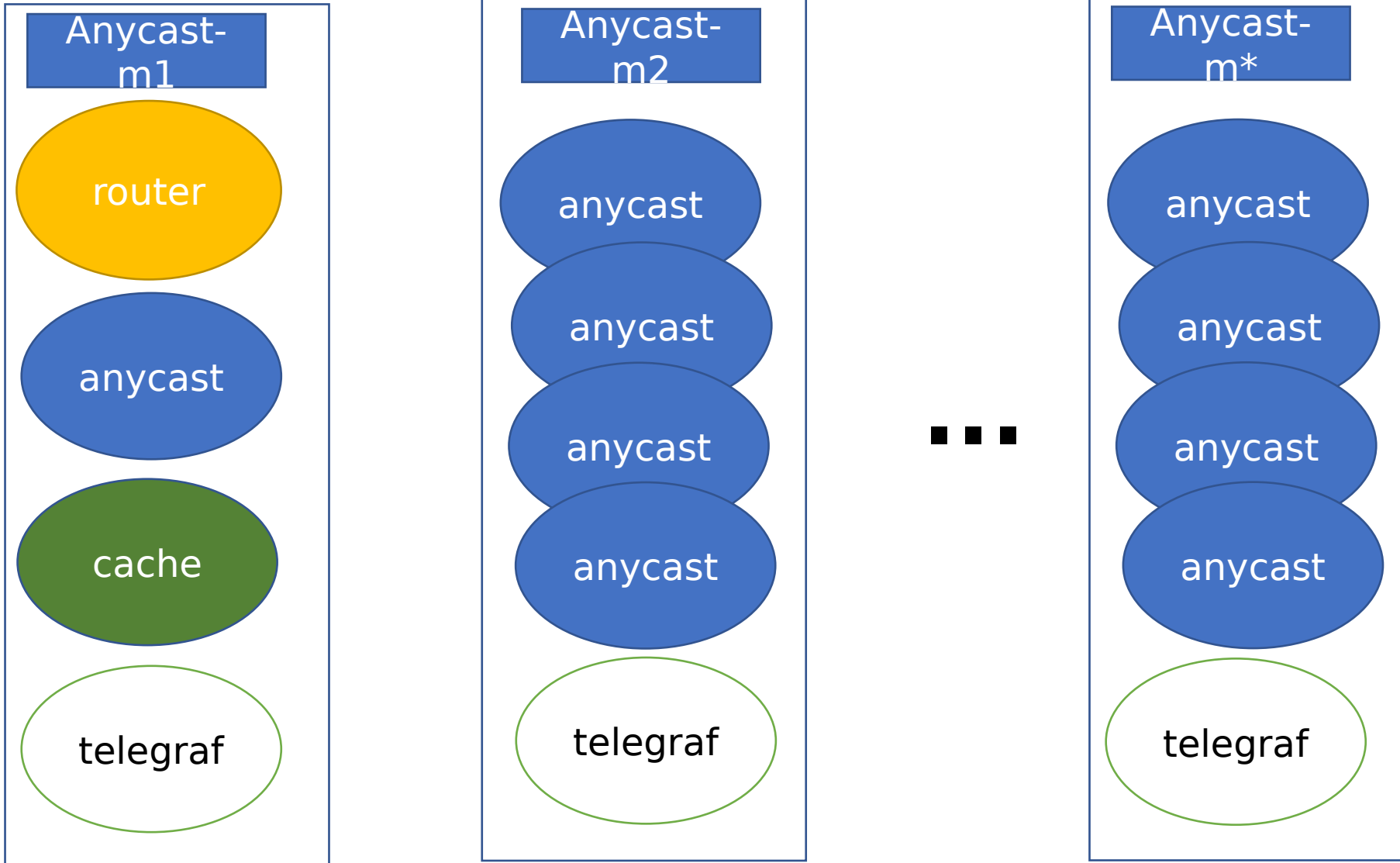
**INFRA DNS
ANYCAST**



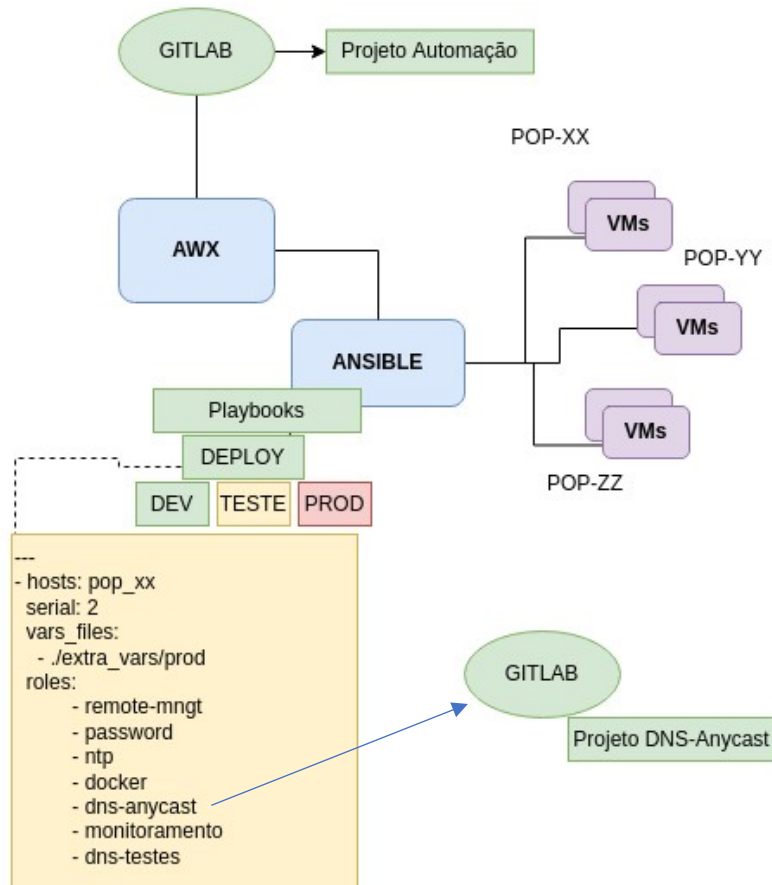
INFRA DNS
ANYCAST
PoP-SG
v2
Jun/2020

DOCKER

- **Virtualização VMs, com:**
- **REDE**
 - 3 camadas
 - Gerenciamento OOB (VM)
 - IGP (intracluster, p/ OSPFv2 e v3)
 - EGP (BGP p/ o PoP)
- **Imagem**
 - Alpine linux / Quagga /bind + scripts
 - ~ 123MB

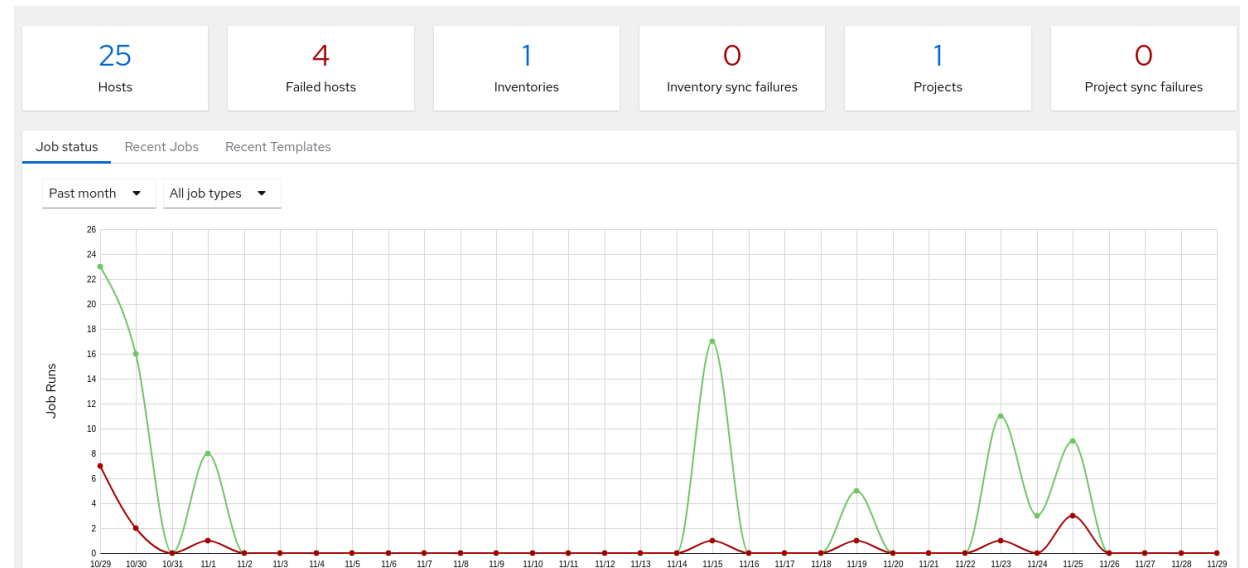


Workflow simplificado



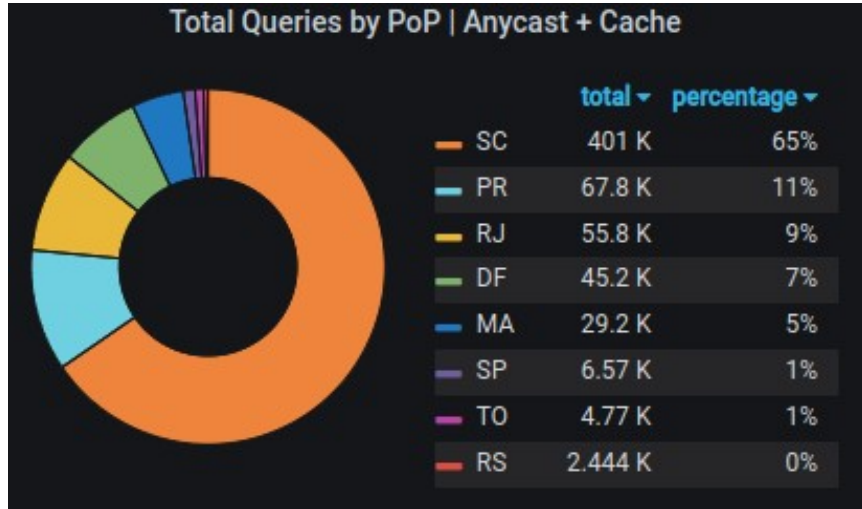
Dashboard AWX

Dashboard



Monitoramento e estatísticas

<https://ajuda.rnp.br/dns-anycast>



November 16, 2021 6:20 PM

Home > Custom Views

SERVICOS ANYCAST

Hosts ANYCAST

-- More actions -- Export

<input type="checkbox"/>	Host Name - Host Alias	Status	Last Check	Duration	Status information
<input type="checkbox"/>	GTI-DF-ANYCAST-POP-DF-M1 - ANYCAST-POP-DF-M1	UP	2m 26s ago	1d 15h ago	OK - 200.19.119.78 rta 0.950ms lost 0%
<input type="checkbox"/>	GTI-DF-ANYCAST-POP-DF-M2 - ANYCAST-POP-DF-M2	UP	2m 31s ago	5d 1h ago	OK - 200.19.119.79 rta 1.072ms lost 0%
<input type="checkbox"/>	GTI-MA-ANYCAST-POP-MA-M1 - ANYCAST-POP-MA-M1	UP	4m 5s ago	7h 54m ago	OK - 200.137.129.14 rta 0.278ms lost 0%
<input type="checkbox"/>	GTI-MA-ANYCAST-POP-MA-M2 - ANYCAST-POP-MA-M2	UP	3m 45s ago	7h 54m ago	OK - 200.137.129.15 rta 0.304ms lost 0%
<input type="checkbox"/>	GTI-PR-ANYCAST-POP-PR-M1 - ANYCAST-POP-PR-M1	UP	2m 46s ago	1M 1w ago	OK - 200.134.255.10 rta 1.659ms lost 0%
<input type="checkbox"/>	GTI-PR-ANYCAST-POP-PR-M2 - ANYCAST-POP-PR-M2	UP	2m 51s ago	1M 1w ago	OK - 200.134.255.11 rta 0.241ms lost 0%
<input type="checkbox"/>	GTI-RJ-ANYCAST-POP-RJ-M1 - ANYCAST-POP-RJ-M1	UP	3m 17s ago	2M 3w ago	OK - 200.159.252.16 rta 0.510ms lost 0%
<input type="checkbox"/>	GTI-RJ-ANYCAST-POP-RJ-M2 - ANYCAST-POP-RJ-M2	UP	3m 17s ago	2M 3w ago	OK - 200.159.252.17 rta 0.787ms lost 0%
<input type="checkbox"/>	GTI-RS-ANYCAST-POP-RS-M1 - ANYCAST-POP-RS-M1	UP	4m 10s ago	2M 2w ago	OK - 200.132.1.120 rta 0.340ms lost 0%
<input type="checkbox"/>	GTI-RS-ANYCAST-POP-RS-M2 - ANYCAST-POP-RS-M2	UP	4m 10s ago	2M 2w ago	OK - 200.132.1.121 rta 0.496ms lost 0%
<input type="checkbox"/>	GTI-SC-ANYCAST-POP-SC-M1 - ANYCAST-POP-SC-M1	UP	1m 20s ago	2w 3d ago	OK - 200.237.203.98 rta 0.571ms lost 0%
<input type="checkbox"/>	GTI-SC-ANYCAST-POP-SC-M2 - ANYCAST-POP-SC-M2	UP	1m 20s ago	2w 3d ago	OK - 200.237.203.99 rta 0.617ms lost 0%
<input type="checkbox"/>	GTI-SC-ANYCAST-POP-TO-M1 - ANYCAST-POP-TO-M1	UP	3m 25s ago	2M 2w ago	OK - 200.139.26.27 rta 0.418ms lost 0%
<input type="checkbox"/>	GTI-SC-ANYCAST-POP-TO-M2 - ANYCAST-POP-TO-M2	UP	3m 30s ago	2M 2w ago	OK - 200.139.26.28 rta 0.343ms lost 0%
<input type="checkbox"/>	GTI-SP-ANYCAST-POP-SP-M1 - ANYCAST-POP-SP-M1	UP	2m 21s ago	2d 8h ago	OK - 200.132.102.20 rta 1.217ms lost 0%

services ANYCAST

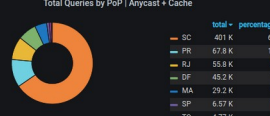
Anycast RNP

2021-09-29 05:00:00 to 2 hours ago

Pop: ma Host: All Tipo: anycast Container: All

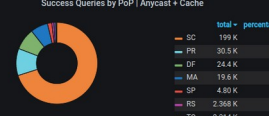
Visão Geral

Total Queries by PoP | Anycast + Cache



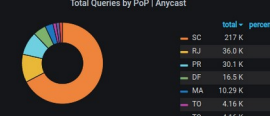
PoP	total	percentage
SC	401 K	65%
PR	67.8 K	11%
RJ	55.8 K	9%
DF	45.2 K	7%
MA	29.2 K	5%
SP	6.57 K	1%
TO	4.77 K	1%
RS	2.444 K	0%

Success Queries by PoP | Anycast + Cache




PoP	total	percentage
SC	199 K	70%
PR	30.5 K	11%
RJ	24.4 K	9%
DF	19.6 K	7%
MA	10.29 K	3%
SP	4.80 K	2%
TO	2.368 K	1%
RS	1.16 K	1%

Total Queries by PoP | Anycast



PoP	total	percentage
SC	217 K	67%
RJ	38.0 K	17%
PR	30.1 K	9%
DF	16.6 K	5%
MA	10.29 K	3%
TO	4.16 K	1%
RS	1.16 K	1%
RJ	863	1%

Success Queries by PoP | Anycast




PoP	total	percentage
SC	108.4 K	73%
PR	18.50 K	16%
DF	11.57 K	8%
MA	8.73 K	6%
SP	3.20 K	2%
TO	2.288 K	2%
RS	1.16 K	1%
RJ	863	1%

ALL PoPs | Anycast + Cache Totals

Total Queries	Success Queries	Rejected Recursive Queries	Rejected Authoritative Queries
612727	284504	6.6	0.067

ALL PoPs | Queries RTT Total (Anycast + Cache)

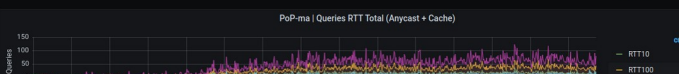


RTT	current	total
RTT10	235	185312
RTT100	249	224357
RTT500	208	165584

PoP-ma | Anycast + Cache Totals

Total Queries	Success Queries	Rejected Recursive Queries	Rejected Authoritative Queries
29193	19577	0	0

PoP-ma | Queries RTT Total (Anycast + Cache)



RTT	current	total
RTT10	20	9388
RTT100	43	20913
RTT500	16	7139

- Teste de resolução com origem em 27 PoPs realizado de forma paralela

Dados coletados em 27/09/2021 - infra daero-pops

Pol	DNS Recursivos					
	Públicos				ANYCAST RNP	
AC	78,8	62,6	61,2	157,9	36	36
AL	40,9	58,1	22,2	119,1	39,1	50,1
AM	59	62	71	163	42	NA
AP	131	74,3	85,5	193,2	56,1	56,4
BA	30,9	46,5	13,2	84,5	30,1	49,2
CE	44,9	45,5	1,1	80,1	45,1	45,2
DF	38,6	18,4	17,9	123,3	1	0,2
ES	58,6	19,7	11,6	96,7	10	10
GO	34,1	21,9	23,2	129,6	3,1	3
MA	41,3	40,8	39,6	155,4	5,4	0,6
MG	27,7	24,4	14,8	115,2	13,1	13,1
MS	46,3	30,5	28,5	134,6	20	20
MT	37,9	40,4	38,6	167,2	19	18,7
PA	45,6	42,2	41,7	138,5	16	16
PB	52,5	56,4	11,1	88,2	52	53,7
PE	74,2	56,5	23,1	105,1	40	49,6
PI	45,6	46,5	47,1	132,4	7,1	6,7
PR	9,5	10,7	9,7	150,7	2,8	0,1
RJ	2,5	16,8	1,7	135,7	0,9	0,4
RN	50,3	51	8,7	108,6	49,2	51,6
RO	52,6	54,3	52,1	143,3	33	33
RR	108,3	109,8	63,2	142	52	52,2
RS	17,5	19,3	20,2	151,3	3,6	0,9
SC	13,4	13,8	13,1	153,7	1,1	0,9
SE	35,9	51,3	18,4	115,8	35,1	41,7
SP	49,7	2,7	3,3	116,7	1	1
TO	28,4	26,8	27	128,2	4,4	0,1

Estado atual:

- Cache Implantado em 8 PoPs



PA* Em implantação

DF	8
SP	8
RJ	3
MA	2
PR	2
TO	2
RS	1
SC	1

Ex: dados PoP-MA

Dados coletados em 27/09/2021 - infra daero-pops						
DNS Recursivos						
Públicos				ANYCAST RNP		
PoP						
MA						
MA: ICMP	41,93	39,068	39,565	115,506	0,671	0,652
MA: QDNS	41,3	40,8	39,6	155,4	5,4	0,6
MA: ANYCAST					MA	MA

Influência do DNS na escolha da CDN

DNS	NOME	RTT_MÉDIO
Recursos Públicos	star.c10r.facebook.com	38,809
		38,767
		38,868
		132,811
Recursos RNP		38,86
		38,819
Recursos Públicos	www.americanas.com.br	66,224
		66,241
		261,703
		138,357
Recursos RNP		64,271
		63,492

DNS Anycast RNP

- Recursão disponível para todo sistema RNP
 - IPs RNP e seus ASNs membros
 - ACL de serviço alimentada pelo RA-DB
 - Acesso de outras redes NEGADO
- Usuário final:
 - Basta configurar o IP em seu equipamento
- Organização usuária:
 - Pode entregar os IPs diretamente
 - Recomenda-se configurar o "forward" de seu DNS local
- Como posso saber qual cache está respondendo:
 - `dig @dns.rnp.br ch txt version.bind +short`

<https://ajuda.rnp.br/dns-anycast>

```
-----~$ dig chaos txt version.bind @dns.rnp.br +short  
"RNP ANYCAST - MA 94e9efea65c6"
```

PoP que está respondendo

Trabalhos futuros

- Aumento da malha
 - Dependem da troca de roteador do PoP (padronização)
- Aumento da privacidade no transporte
 - DoT - DNS-over-TLS
 - DoH - DNS-over-HTTPS
- Proteção premium de segurança

GO / DAERO / RNP

Guilherme Rhoden

**Áreas envolvidas:
GO, PoPs, GTI, CAIS ENG**

Apoio GCC e DPD



MINISTÉRIO DO
TURISMO

MINISTÉRIO DA
DEFESA

MINISTÉRIO DA
SAÚDE

MINISTÉRIO DAS
COMUNICAÇÕES

MINISTÉRIO DA
EDUCAÇÃO

MINISTÉRIO DA
CIÊNCIA, TECNOLOGIA
E INOVAÇÕES

