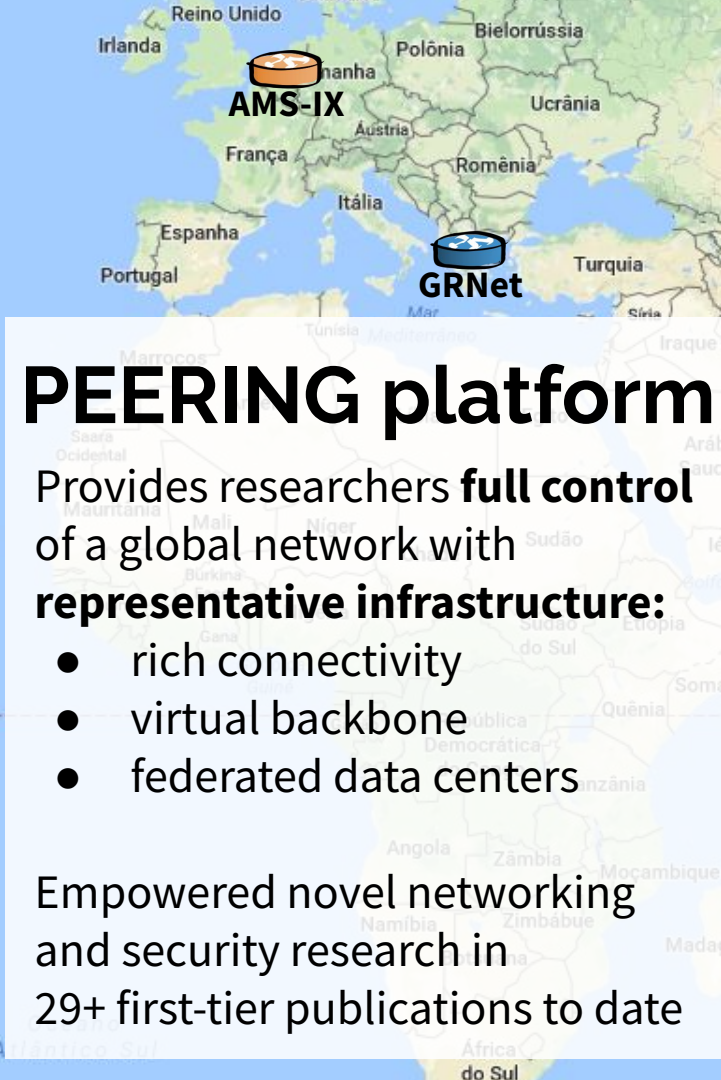
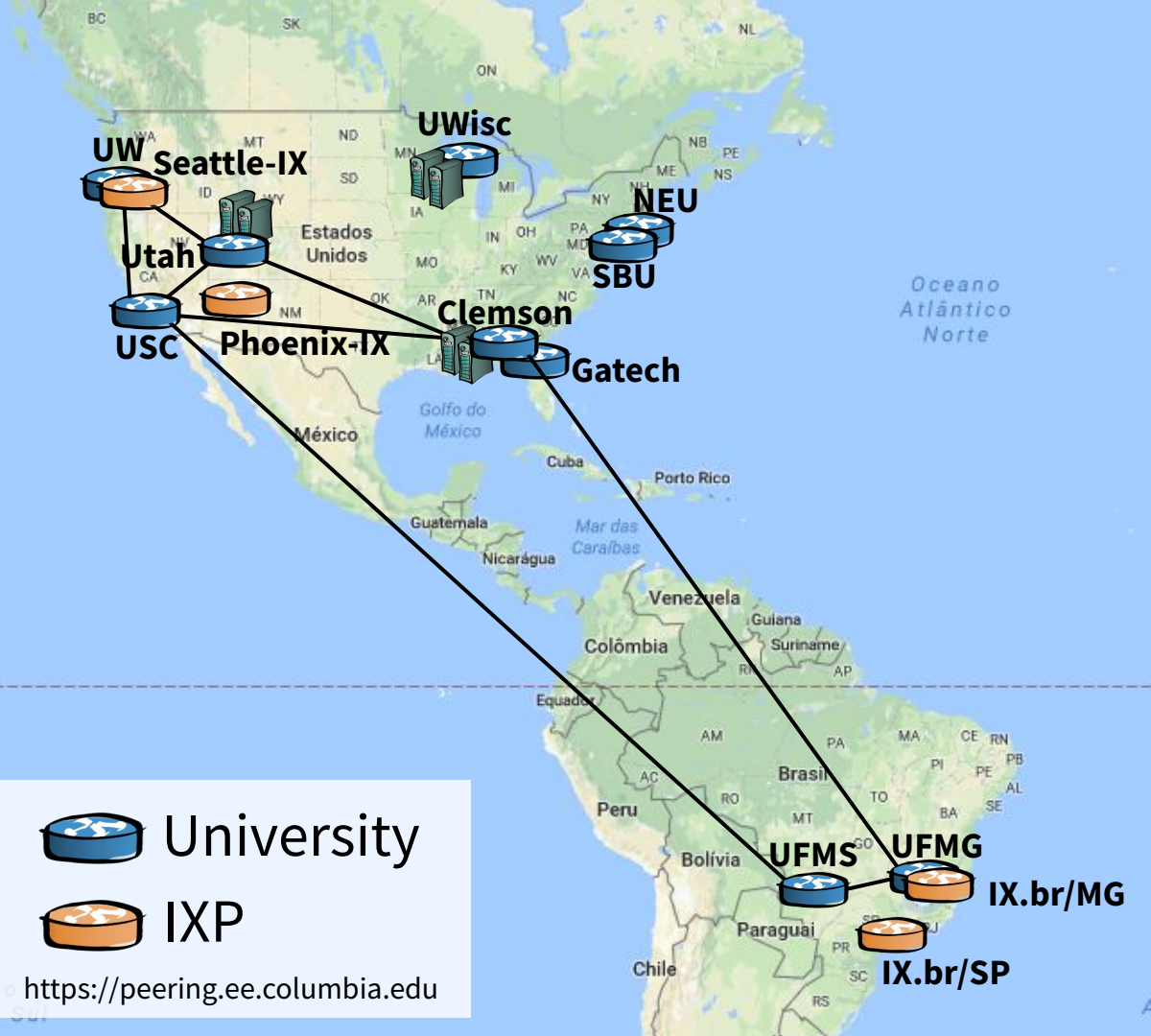


Monitoramento para Decisões Baseadas em Dados

Ítalo Cunha

Como é uma rede sem monitoramento?

- RNP não sabe: monitoramento até os dentes
- Presentes que não são da RNP não operam rede (?!)



PEERING platform

Provides researchers **full control** of a global network with **representative infrastructure:**

- rich connectivity
- virtual backbone
- federated data centers

Empowered novel networking and security research in 29+ first-tier publications to date

[PEERING] IPV4/IPV6 sessions down between AS47065 and AS10310 at Phoenix IX ➡



no-reply@peering.ee.colu... Wed, Oct 13, 4:58 PM



to peering+noc, bschlink, cunha, ta2510 ▼

AS47065 team,

We (AS10310) are currently seeing the IPV4/IPV6 sessions with you down over our peering routers at Phoenix IX as noted below. Can you please advise if there is an issue or maintenance on your end causing this or if you have an issue of some kind? appears the sessions have been down for just over two weeks now.

For your FYI our PeeringDB page can be found at <https://peeringdb.com/net/27>.

Regards

[PEERING] AS47065 <> AS13335 - Peering session removal ➡



Cloudflare Peering no-reply@peering.e... Mon, Oct 11, 1:00 PM
to bschlink, peering+noc, ta2510, cunha, peering ▼



Dear AS47065,

We are writing from Cloudflare (AS13335), we peer with you at one or more Internet Exchanges.

The following session(s) has been down for more than 2 weeks, hence we removed the related configuration from our end.

Phoenix-IX: 206.41.105.42

Phoenix-IX: 2001:504:3b::42

If you would like to peer with us again, please drop a separate email to peering@cloudflare.com.

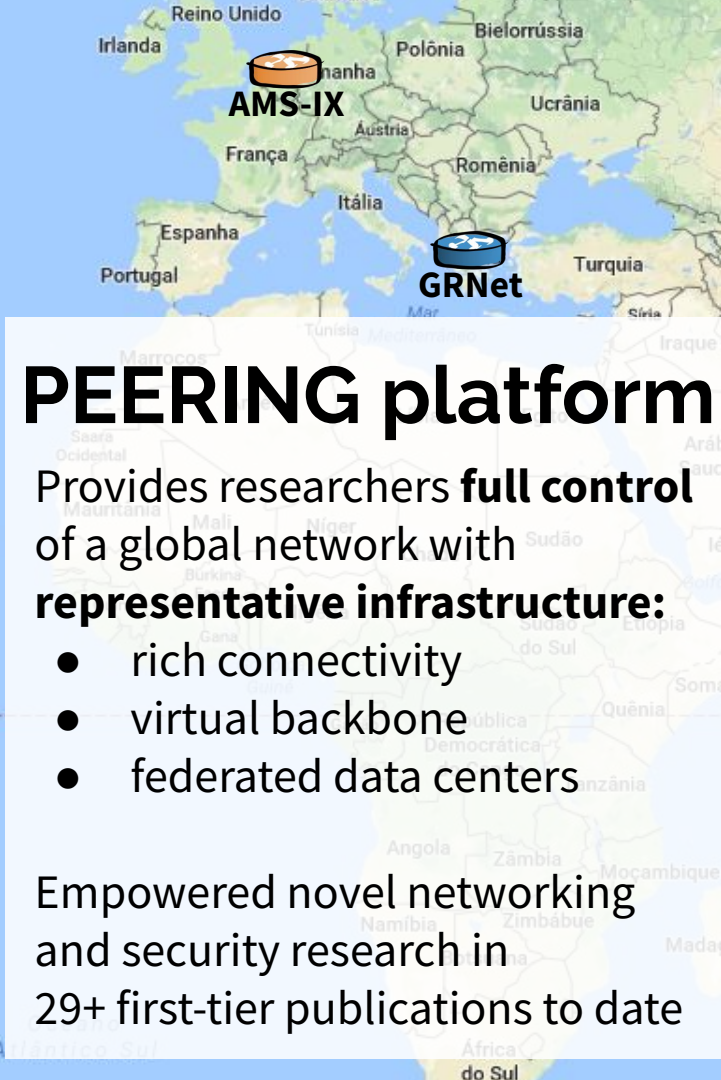
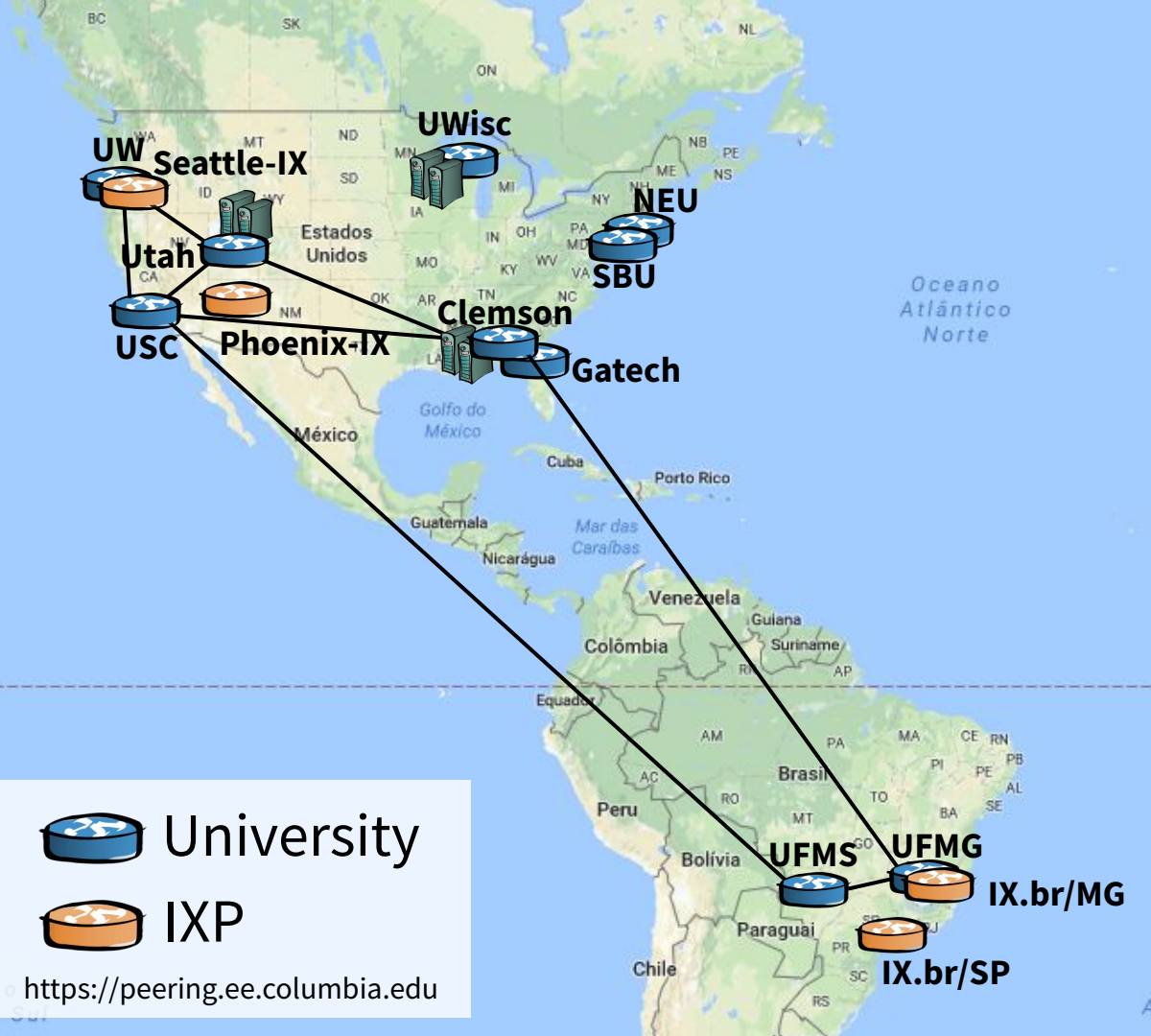
What happened?

- Server NIC died!
- 18 other peers did not seem to monitor or care :)

What happened?

- Server NIC died!
- 18 other peers did not seem to monitor or care :)

My experience is that running a network is hard,
and monitoring is essential detect problems



PEERING platform

Provides researchers **full control** of a global network with **representative infrastructure:**

- rich connectivity
- virtual backbone
- federated data centers

Empowered novel networking and security research in 29+ first-tier publications to date

NO PROD

TRAFFIC



Univers



IXP

<https://peering.ee.columbia.edu>

Provide researchers full control of a global network with **representative infrastructure:**

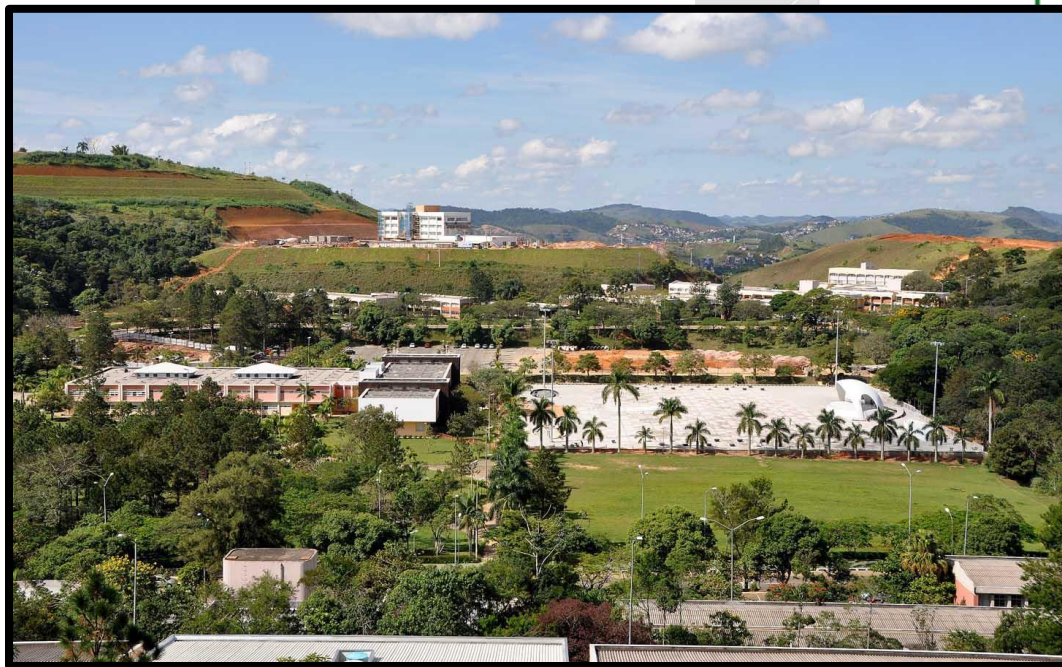
- rich connectivity
- virtual backbone
- federated data centers

Enabled global networking and security research in 29+ first-tier publications to date

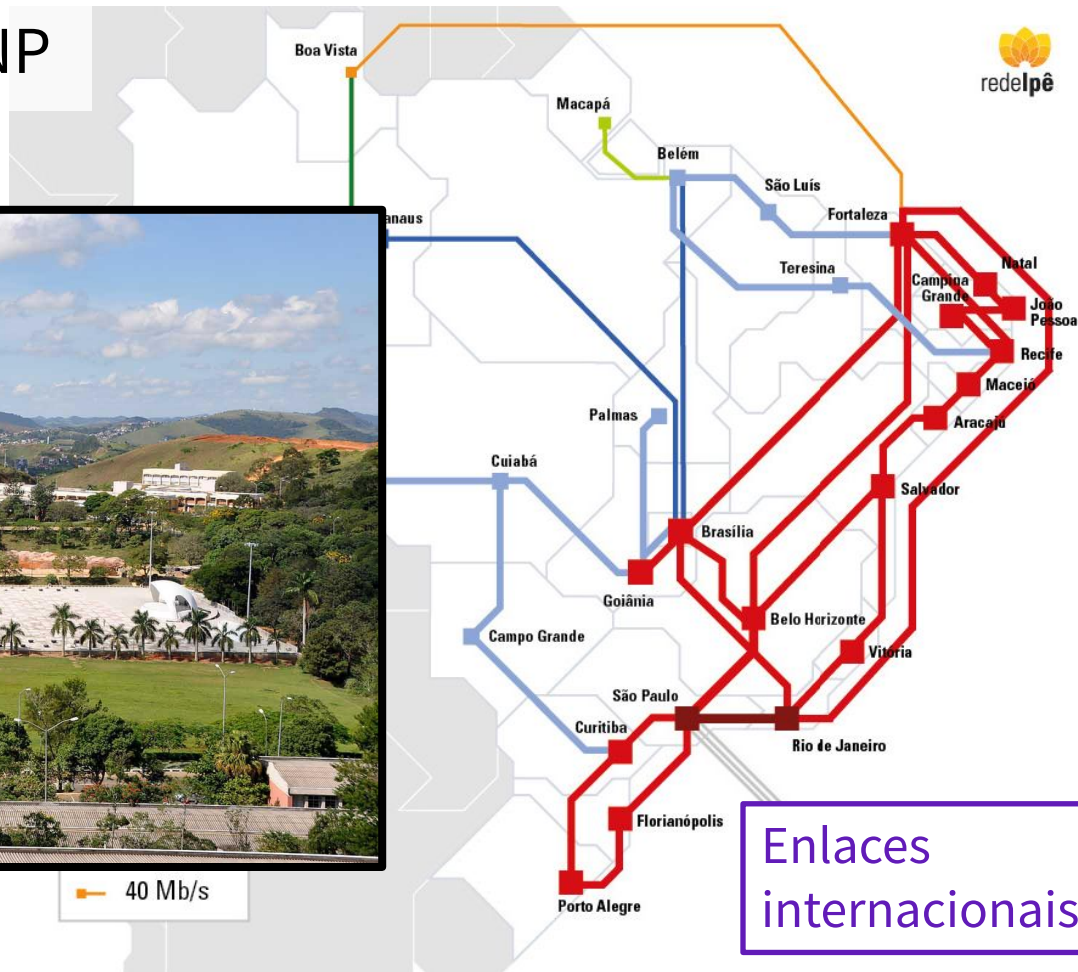
O papel da RNP

- Muitos clientes com defasagem de pessoal e capacitação (?!)
- Diversos serviços à comunidade
 - Escola Superior de Redes
 - RNP NasNuvens
- Ideias específicas relacionadas a monitoramento
 - *(Good) Entity in the Middle*
 - Soluções de monitoramento

Avaliação de falhas na RNP (em 2014)



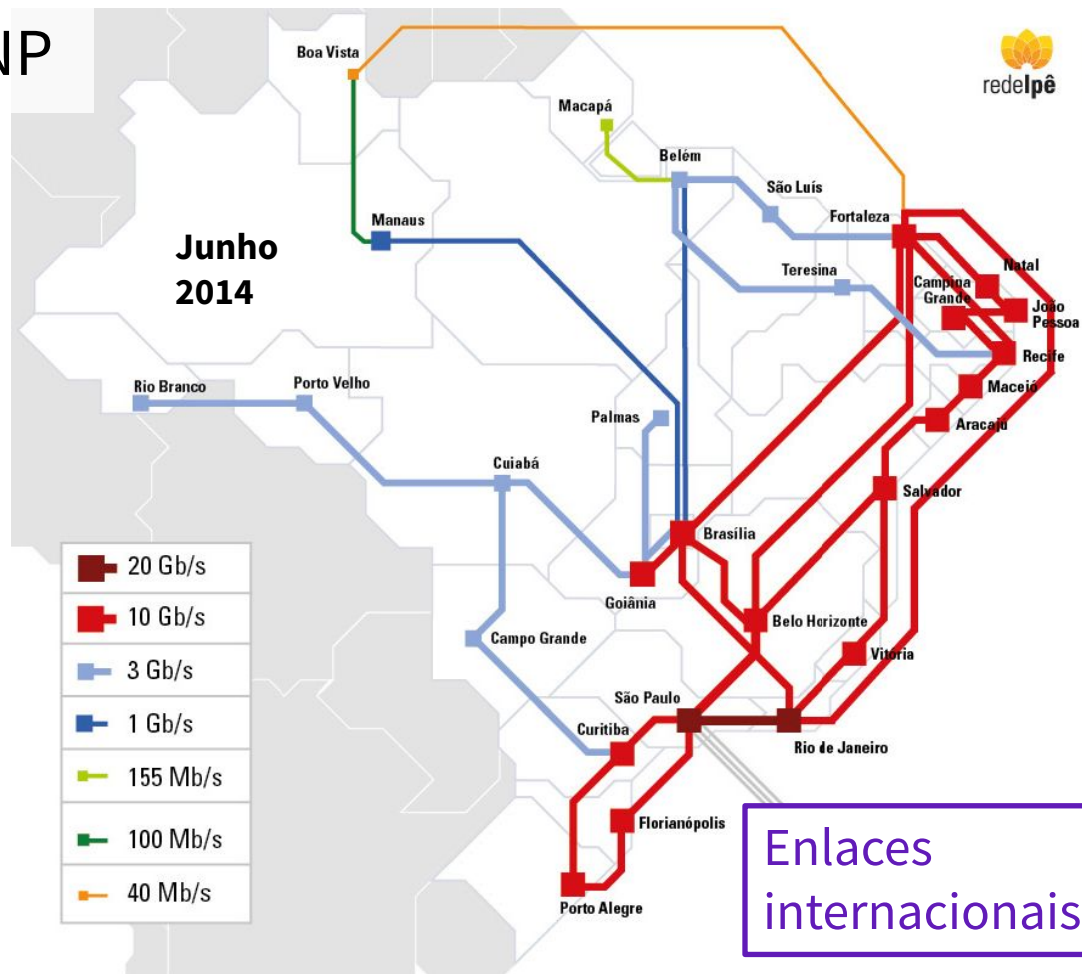
— 40 Mb/s



Enlaces
internacionais

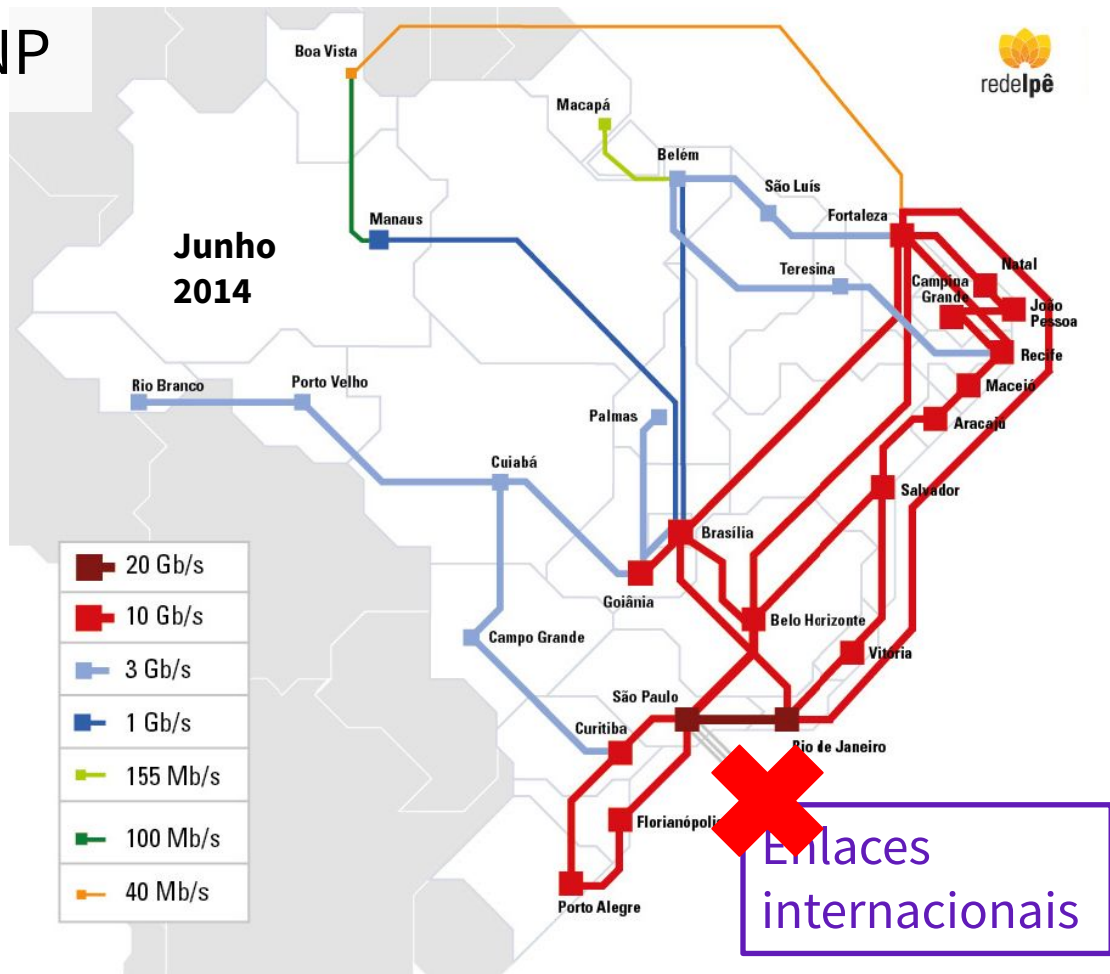
Avaliação de falhas na RNP (em 2014)

- Inacessibilidade de destinos no exterior
- Congestionamento interno

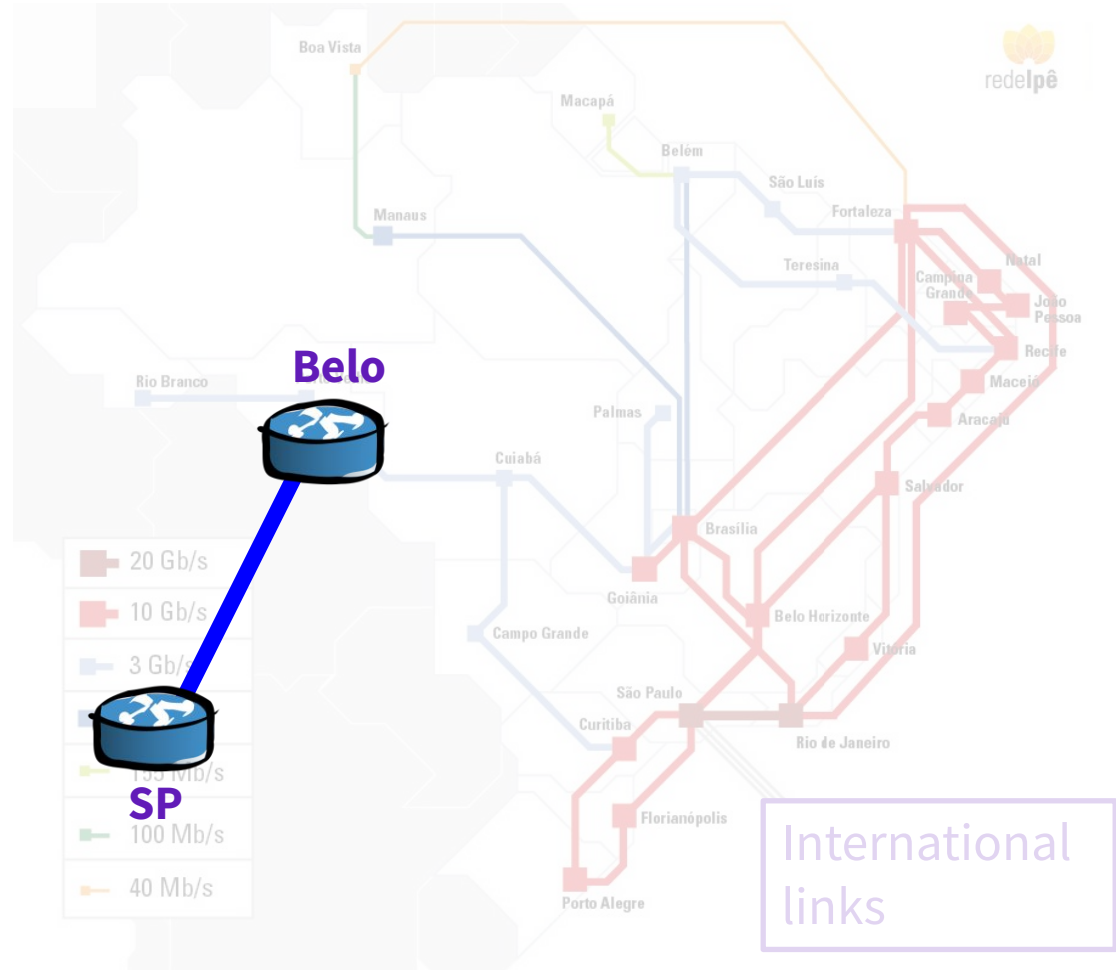


Avaliação de falhas na RNP (em 2014)

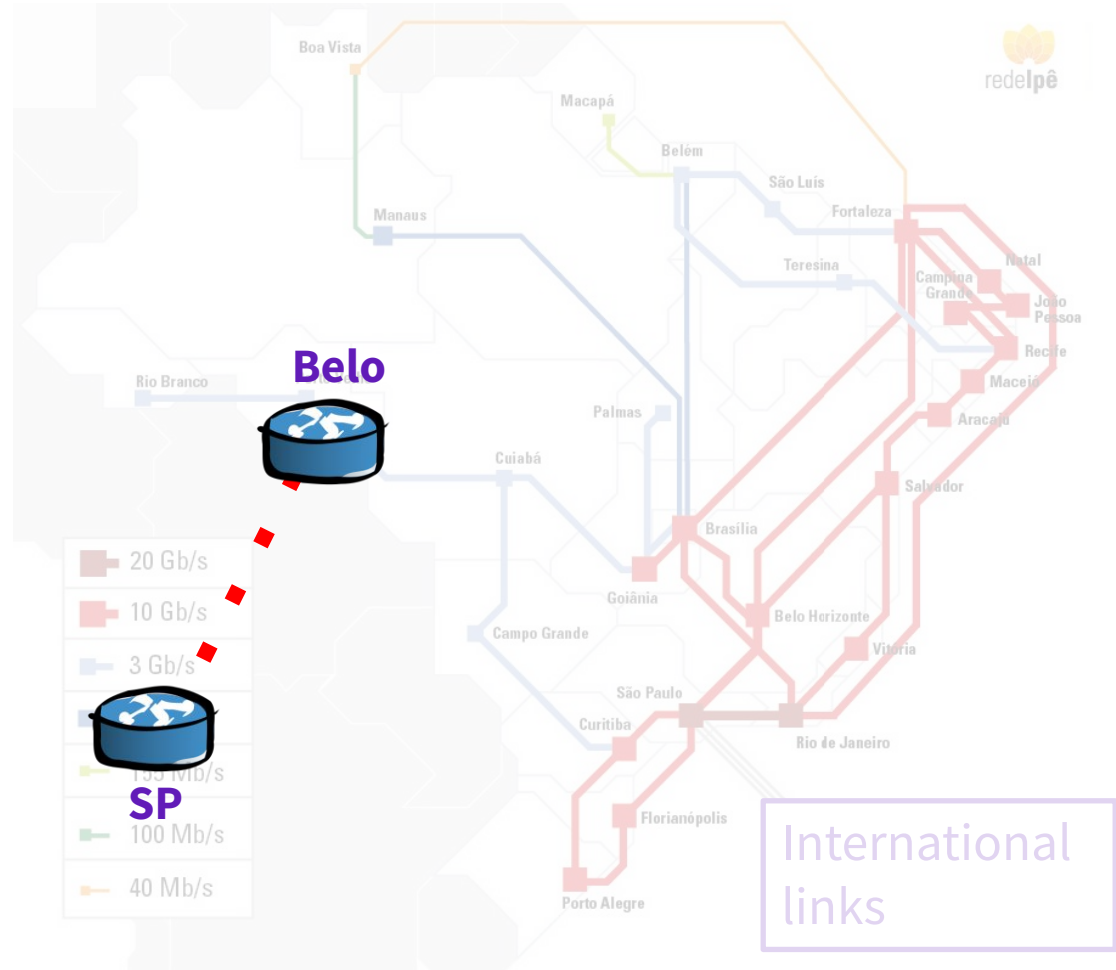
- Inacessibilidade de destinos no exterior



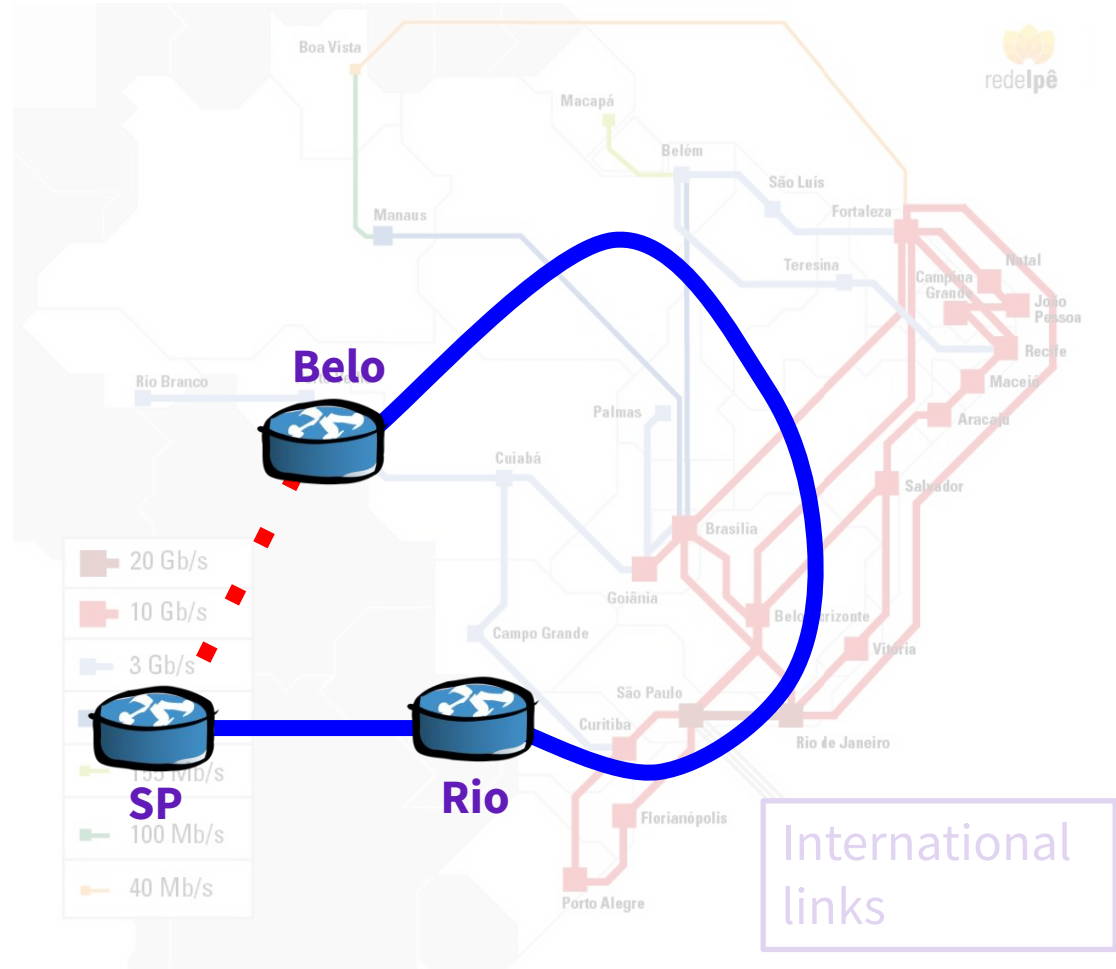
Congestionamento interno na RNP



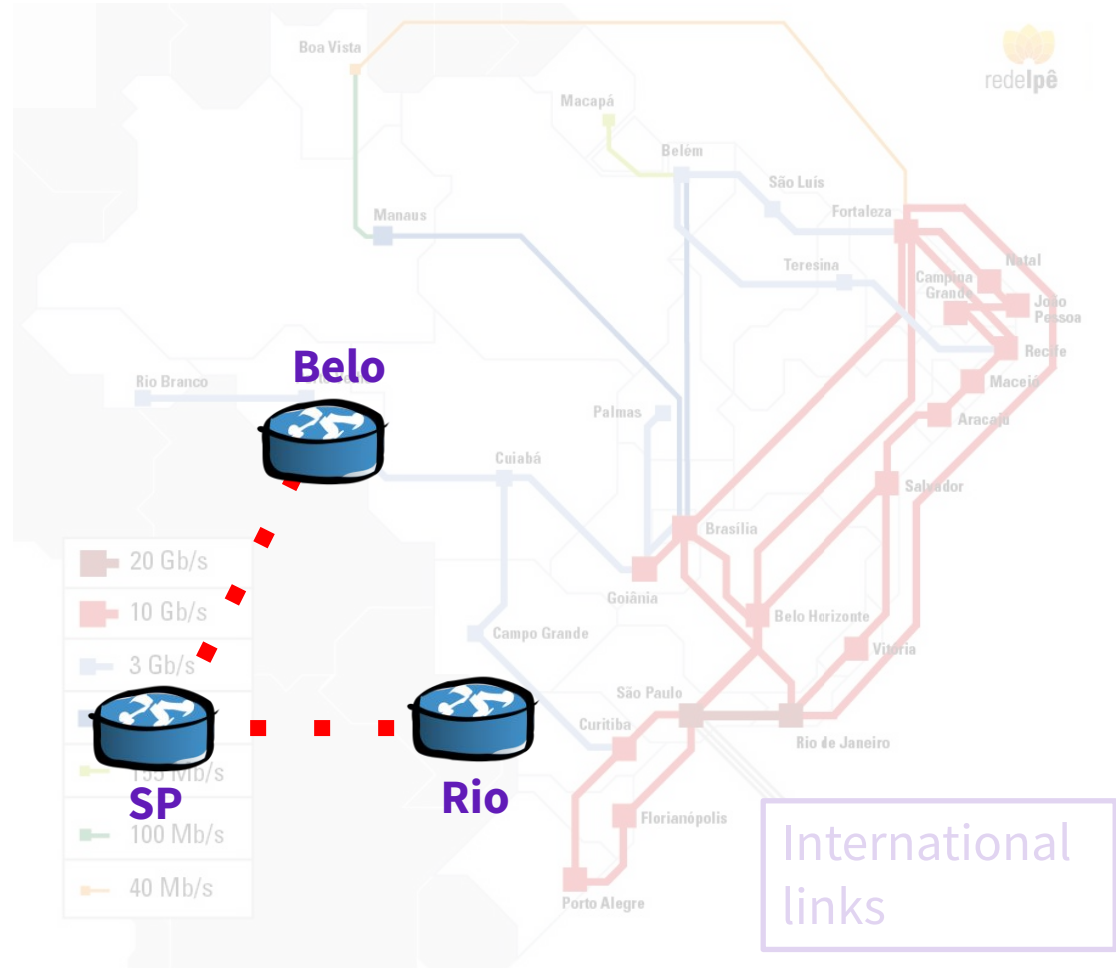
Congestionamento interno na RNP



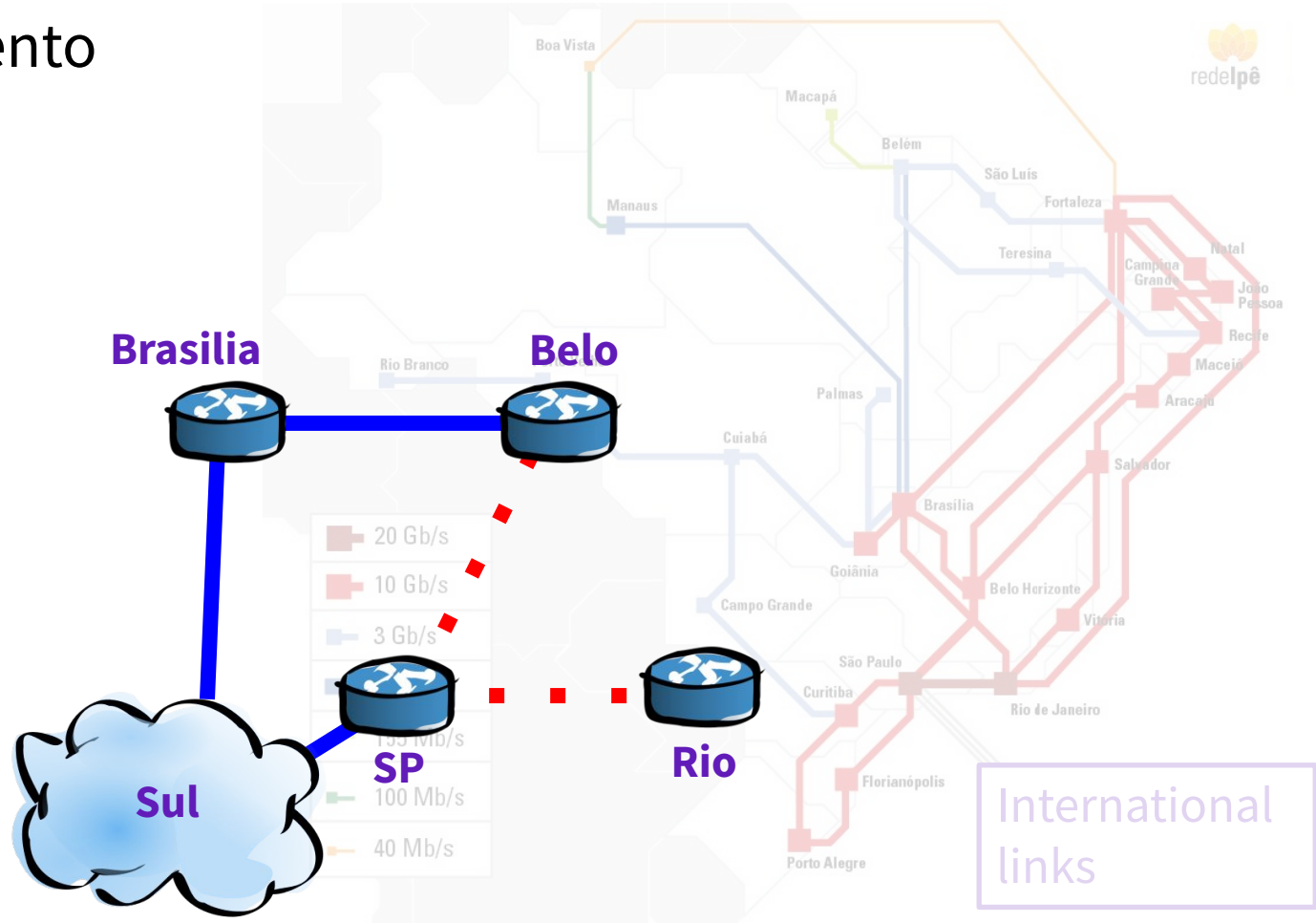
Congestionamento interno na RNP



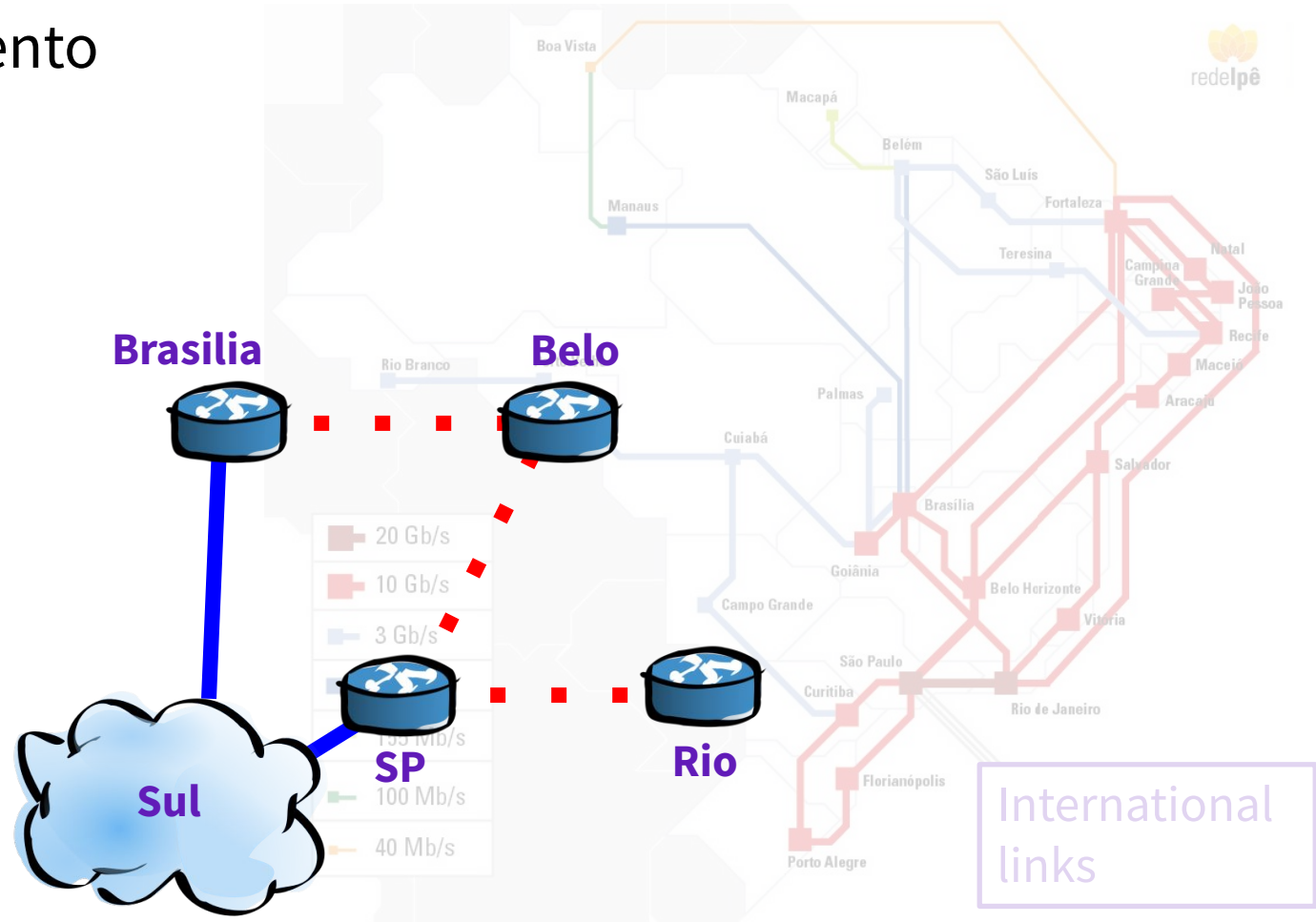
Congestionamento interno na RNP



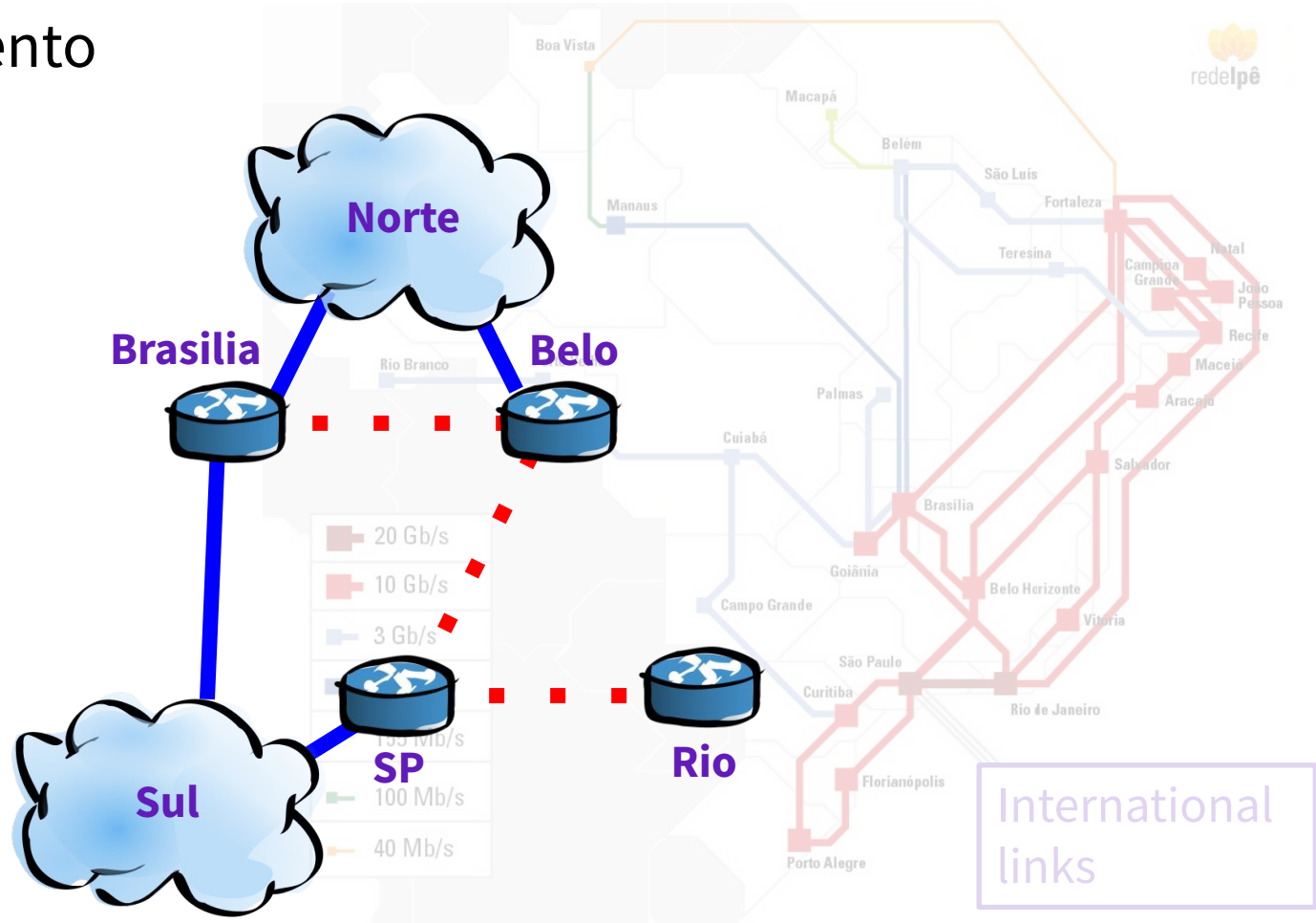
Congestionamento interno na RNP



Congestionamento interno na RNP



Congestionamento interno na RNP



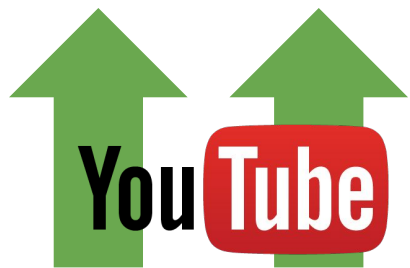
Princípio da conservação da procrastinação

Durante inaccessibilidade de destinos no exterior

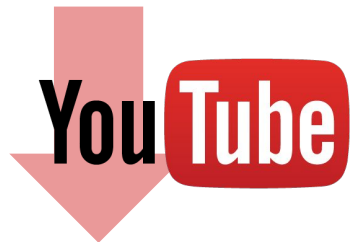


Princípio da conservação da procrastinação

Durante inaccessibilidade de destinos no exterior



Durante congestionamento interno



Requisitos do monitoramento

- Dados ricos, informações complementares
 - Nosso trabalho utilizou informações do tráfego e de rotas
 - Suporte a análises complexas, validação
 - Metadados

Requisitos do monitoramento

- Dados ricos, informações complementares
 - Nosso trabalho utilizou informações do tráfego e de rotas
 - Suporte a análises complexas, validação
 - Metadados
 - Configuração de ferramentas de medição
 - Falhas na infraestrutura de monitoramento ou medição
 - Descrição de como alvos para medição foram selecionados

Requisitos do monitoramento

- Dados ricos, informações complementares
 - Nosso trabalho utilizou informações do tráfego e de rotas
 - Suporte a análises complexas, validação
 - Metadados
 - Configuração de ferramentas de medição
 - Falhas na infraestrutura de monitoramento ou medição
 - Descrição de como alvos para medição foram selecionados
- Monitoramento contínuo
 - Monitoramento precisa esteja ativo durante a falha
 - “Monitoramento” da infraestrutura de monitoramento

Requisitos operacionais

- Respeito à privacidade e atendimento às leis
 - Informações de rede são sensíveis

Requisitos operacionais

- Respeito à privacidade e atendimento às leis
 - Informações de rede são sensíveis
- Disponibilidade dos dados
 - Dados abertos motivam e facilitam a pesquisa

Requisitos operacionais

- Respeito à privacidade e atendimento às leis
 - Informações de rede são sensíveis
- Disponibilidade dos dados
 - Dados abertos motivam e facilitam a pesquisa
- Automatização, implantação em produção e sustentabilidade
 - GTs para automatização do processamento e catalogação de dados
 - Sobrecarga em técnicos da RNP
 - Até GTs têm dificuldade de obter dados
 - SSH para copiar datasets

Expansão da coleta e análise de dados

- Automatização e operacionalização da disponibilização
 - *Deploy and forget*
- Reconhecimento da sobrecarga técnica e alocação de RH
 - Alocação de pessoal
- Repasse da sobrecarga técnica aos requisitantes de dados
 - Desenvolvimento de código para processamento de dados privados
 - Disponibilização

Decisões baseadas em dados

- Análise dos dados pode levar a melhorias de processos
 - Segurança
 - Identificação de tráfego malicioso
 - Identificação de dispositivos vulneráveis
 - Exemplos: classificação de fluxos, detecção de anomalia

Decisões baseadas em dados

- Análise dos dados pode levar a melhorias de processos
 - Segurança
 - Identificação de tráfego malicioso
 - Identificação de dispositivos vulneráveis
 - Exemplos: classificação de fluxos, detecção de anomalia
 - Desempenho
 - Planejamento de capacidade
 - Alocação de recursos
 - Exemplos: Detecção de congestionamento, controladores de tráfego

Decisões baseadas em dados

- Análise dos dados pode levar a melhorias de processos
 - Segurança
 - Identificação de tráfego malicioso
 - Identificação de dispositivos vulneráveis
 - Exemplos: classificação de fluxos, detecção de anomalia
 - Desempenho
 - Planejamento de capacidade
 - Alocação de recursos
 - Exemplos: Detecção de congestionamento, controladores de tráfego
 - Disponibilidade
 - Resposta a incidentes
 - Exemplos: Detecção de tíquetes improcedentes, anexar metadados a tíquetes

Atribuições e Tarefas no Monitoramento de Redes



Atribuições e Tarefas no Monitoramento de Redes



Manutenção do monitoramento;
Monitoramento clássico



Atribuições e Tarefas no Monitoramento de Redes



Manutenção do monitoramento;
Monitoramento clássico

Disponibilização de dados



Atribuições e Tarefas no Monitoramento de Redes



Manutenção do monitoramento;
Monitoramento clássico

Disponibilização de dados



Atribuições e Tarefas no Monitoramento de Redes



Manutenção do monitoramento;
Monitoramento clássico



Disponibilização de dados



Atribuições e Tarefas no Monitoramento de Redes



Manutenção do monitoramento;
Monitoramento clássico



Disponibilização de dados



Atribuições e Tarefas no Monitoramento de Redes



Manutenção do monitoramento;
Monitoramento clássico



Disponibilização de dados



Expansão do monitoramento;
Novas técnicas/ferramentas



Atribuições e Tarefas no Monitoramento de Redes



Manutenção do monitoramento;
Monitoramento clássico



Disponibilização de dados



Expansão do monitoramento;
Novas técnicas/ferramentas



Atribuições e Tarefas no Monitoramento de Redes



Manutenção do monitoramento;
Monitoramento clássico



Disponibilização de dados



Expansão do monitoramento;
Novas técnicas/ferramentas



Avanços utilizando dados de
monitoramento



Atribuições e Tarefas no Monitoramento de Redes



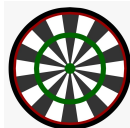
Manutenção do monitoramento;
Monitoramento clássico



Disponibilização de dados



Expansão do monitoramento;
Novas técnicas/ferramentas



Avanços utilizando dados de
monitoramento



Atribuições e Tarefas no Monitoramento de Redes



Manutenção do monitoramento;
Monitoramento clássico



Disponibilização de dados



Expansão do monitoramento;
Novas técnicas/ferramentas



Avanços utilizando dados de
monitoramento



Atribuições e Tarefas no Monitoramento de Redes



