RNP Educação, Pesquisa e Inovação em Rede

Engenharia da Rede de e-Ciência

1º Workshop de e-Ciência

GER – Gerência de Engenharia de Redes
DAERO – Diretoria Adjunta de Engenharia e Operações
DEO – Diretoria de Engenharia e Operações

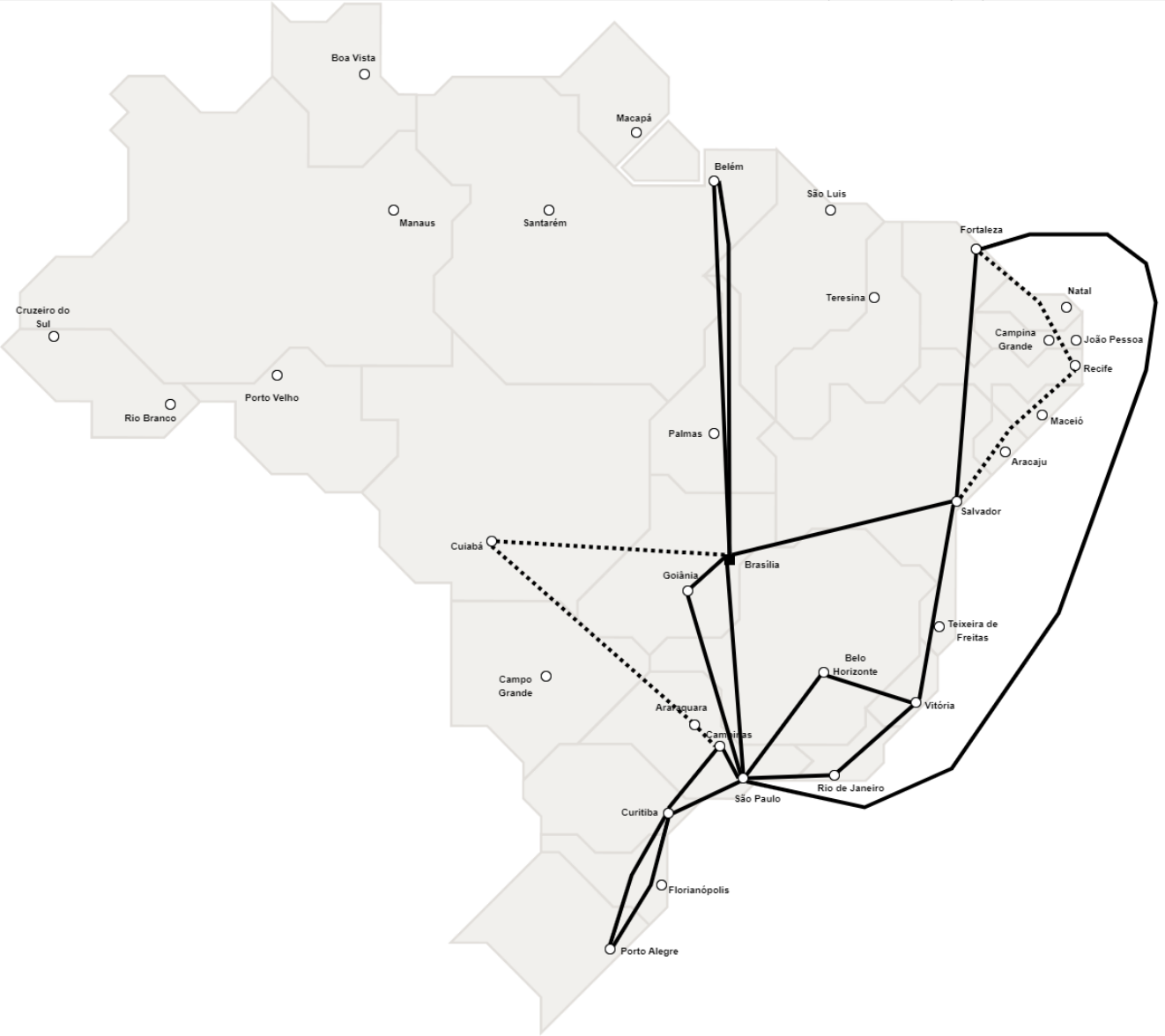
Junho/25

Objetivo

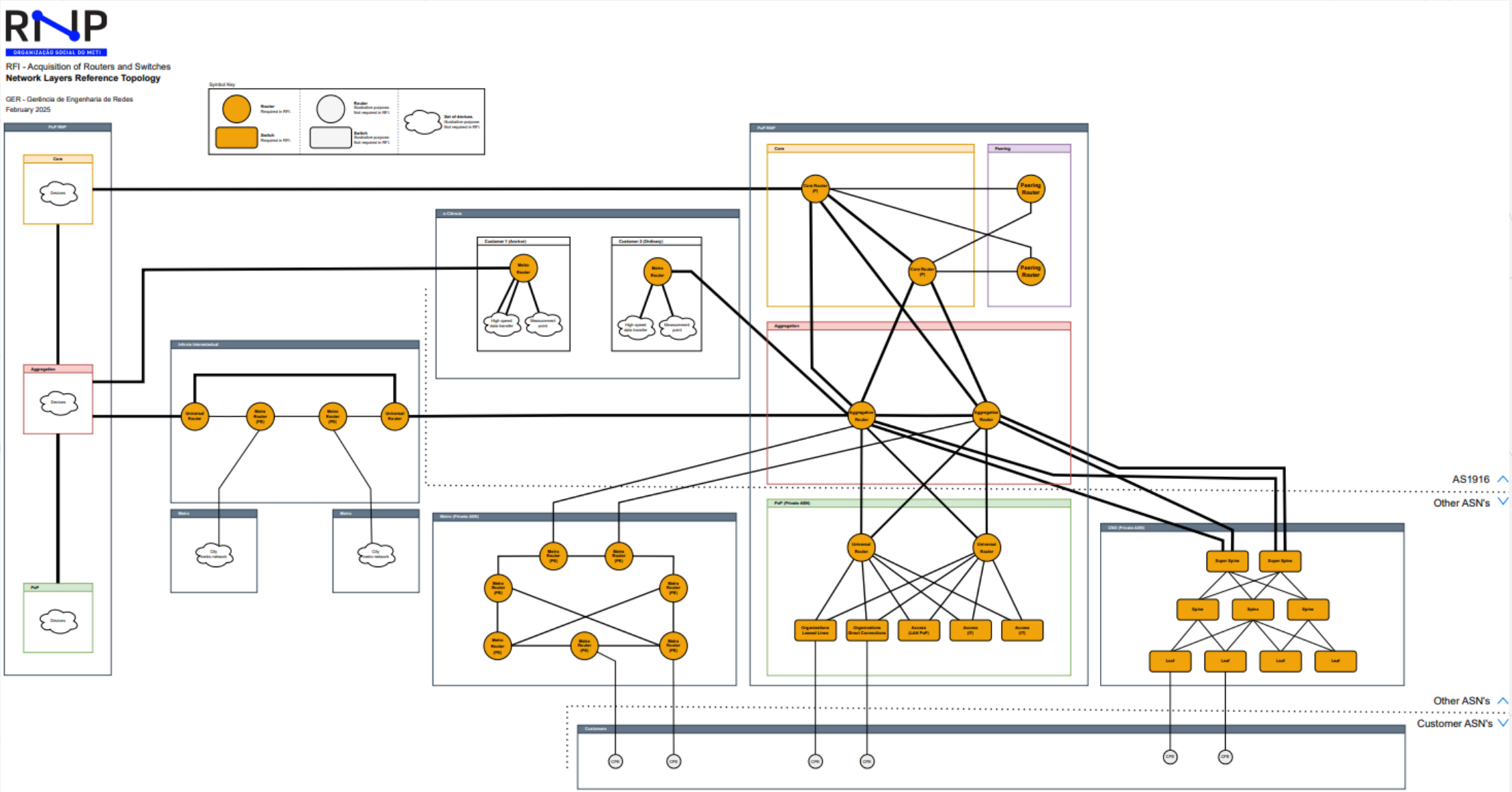
- Projetar e implantar uma rede segura de alta performance otimizada para transferências ponto a ponto de grandes volumes de dados (científicos).
  - A Rede de e-Ciência não é uma simples atualização do projeto PADEX ou REPESQ para enlaces de 100G.
  - Rede de produção (não experimental)
- Otimizar investimentos do FNDCT via Programa Conecta nos trechos de longa distância e PoPs RNP trazendo escalabilidade, simplificando ações de automação, segurança e a operação das redes.
  - Infovia Nacional
  - Rede de e-Ciência
  - Infovias Estaduais
  - CND

Backbone para a rede de e-Ciência

- Capacidade dedicada de pelo menos 100G para os PoPs com instituições selecionadas nos editais de 2024 e 2025.
  - Sub-lambdas
  - QoS
  - Flex-E
- Aproveitar, quando possível, a rede óptica escalável da RNP em parcerias com as empresas do setor elétrico (OPGW)



Proposta da nova arquitetura de rede

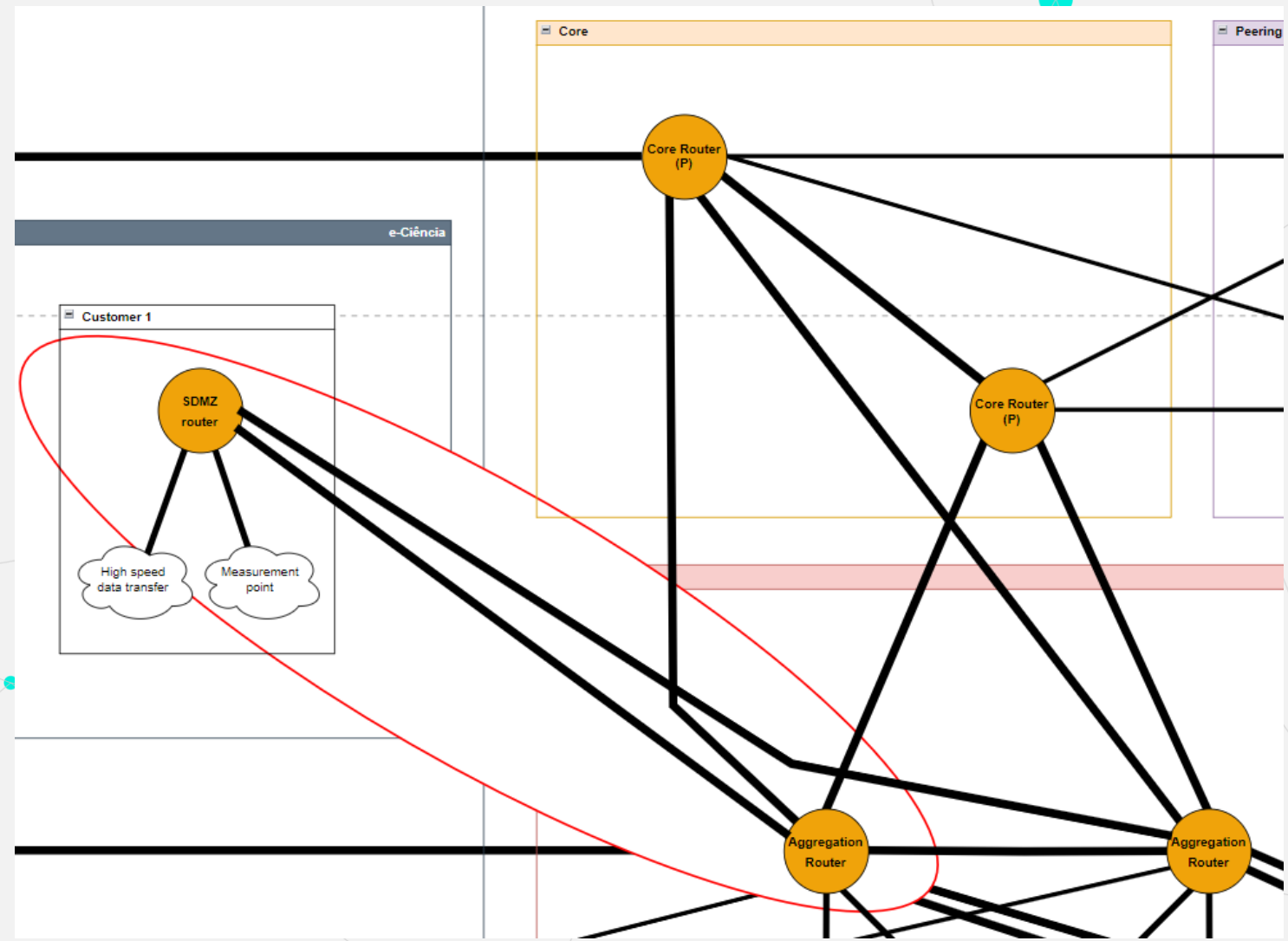


Proposta da nova arquitetura de rede

- Padronizar as topologias, protocolos e configurações das diversas redes que compõem o sistema RNP
- Aumentar a disponibilidade e minimizar impactos por eventuais incidentes/falhas
  - Equipamentos de mesma camada duplicadas (no PoP principal)
  - Segregação de funções de rede
- Convergir esforços de investimento para robustez do backbone com otimização dos recursos (sem duplicação de elementos de rede – ex. rede Ipê e e-Ciência)
- Possibilitar criação de serviços fim a fim
- Facilitar monitoramento integrado e amplo
- Facilitar jornada de automação e orquestração da rede
- Garantir a segurança da rede
- Possibilitar a escalabilidade dos serviços para os próximos 5 anos

Rede de e-Ciência nos PoPs da RNP

- Capacidade dedicada de pelo menos 100G nas interconexões internas.
  - Fração de 400G
  - Interfaces dedicadas de 100G
- Simplificação da topologia conectando as instituições diretamente na agregação.
- Planejado ambiente de alta disponibilidade nos PoPs da RNP
- RFP dos novos equipamentos será lançado no final de junho

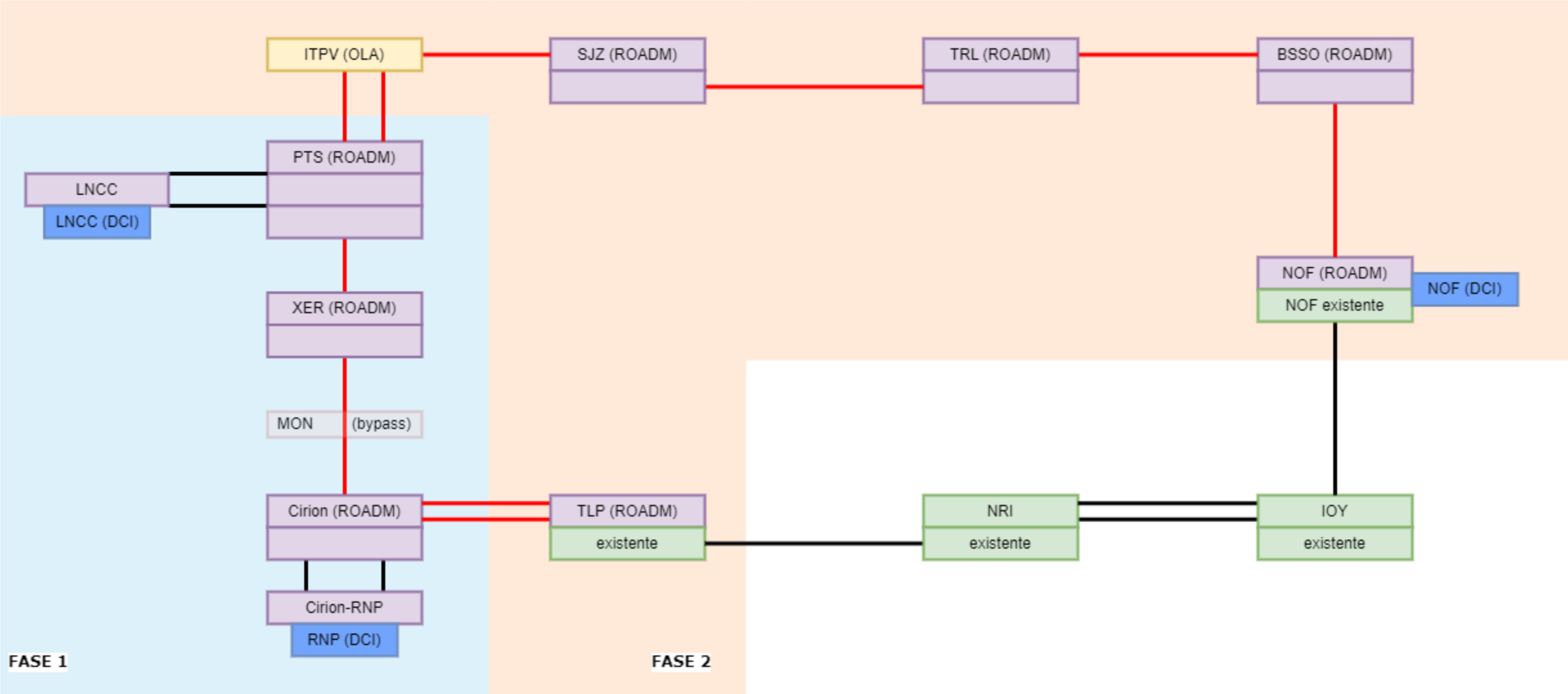


Acessos para a rede de e-Ciência

- Várias modalidades de conexão mapeadas - exemplos:
  - Conexão local no PoP-RNP (ex: UFMG e UFES)
  - Conexão via fibra de rede metropolitana da RNP (ex: Embrapa-BSB e UFG)
  - Conexão via rede óptica intermunicipal (ex: INPE/CPTEC e LNCC)
  - Conexão via PoA-RNP (ex: CNPEM)
  - Conexão própria da instituição e/ou rede parceira (ex: UNESP)
  - Conexão não dedicada via rede metro (ex: SENAI/Cimatec e UFRJ?)

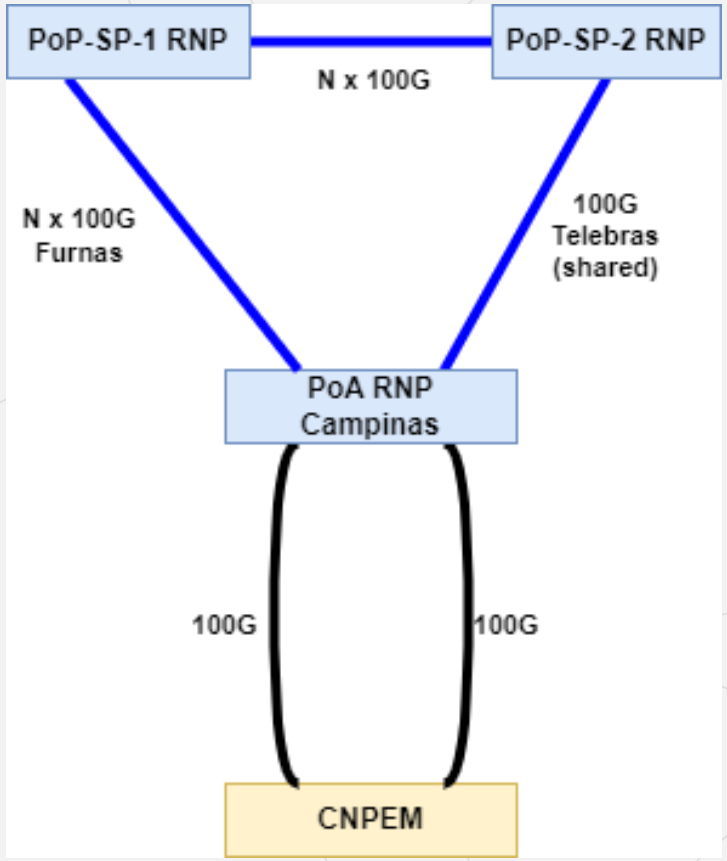
- Sempre que viável, o acesso ao PoP-RNP contará com redundância física.

Acessos para a rede de e-Ciência: LNCC

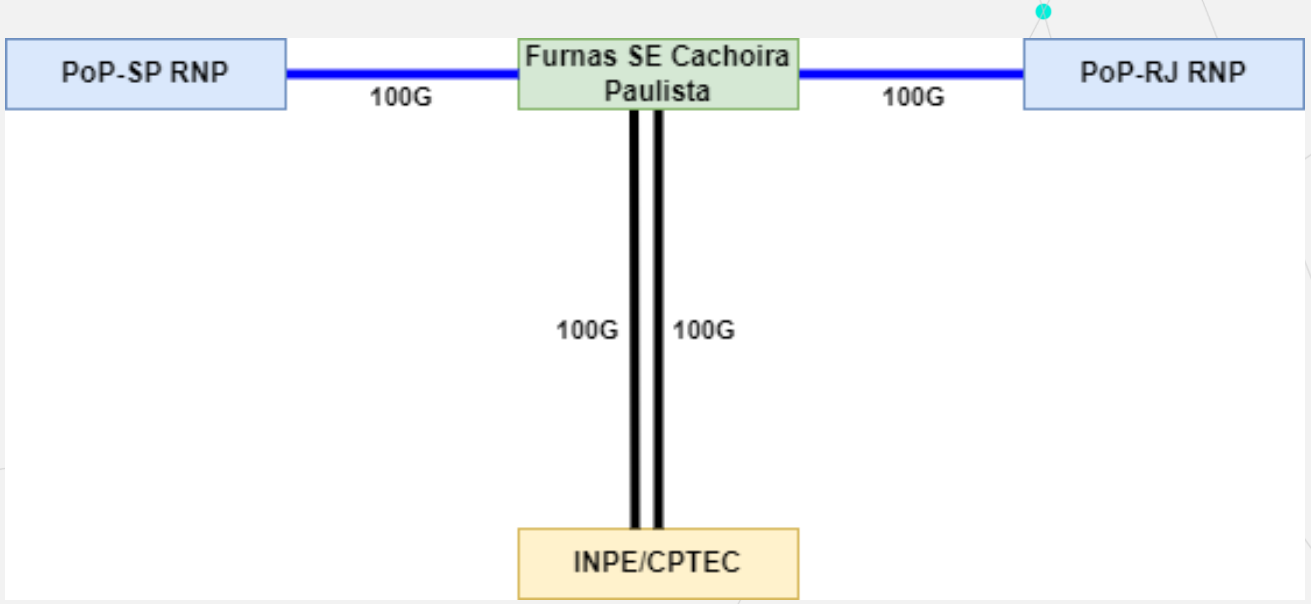


Projeto óptico de conexão Rio – Petrópolis para atendimento ao LNCC com benefício para outras instituições do estado.

Acessos para a rede de e-Ciência: CNPEM e INPE



Topologia para acesso ao CNPEM



Topologia para acesso ao INPE

Rede de e-Ciência: conectividade lógica

- Rede isolada da Internet
- Circuitos protegidos (1+1) ponto a ponto de camada 2 com caminhos determinísticos
  - Isolamento do tráfego entre as diferentes demandas científicas
- Aprovisionamento multi-domínio segregado (ao menos inicialmente)
  - Em redes metro, será solicitado *service* vlan para flexibilidade de criação de circuitos de forma transparente do ponto de vista do operador da rede.
- Criptografia fim a fim – DTN a DTN (ainda necessário validação)
  - MACsec tunelado em VPWS
  - IPsec
- Plano de controle/gerência isolado do plano de dados
- Configuração e equipamentos padronizados para simplificação de roadmap e operação.

Rede de e-Ciência: rede L2 vs L3

- Camada 2
  - Permite estender o MACsec fim a fim
  - Maior isolamento do tráfego entre as demandas científicas
  - Simplicidade de monitoramento do tráfego por demanda científica
  - Engenharia de tráfego simplificada considerando demandas p2p

- Camada 3
  - Simplificação da configuração da DTN
  - Facilidade de conexão com múltiplos participantes da ReC
  - Complexidade de roteamento é totalmente transferido para a rede.
  - Menos opções no mercado para criptografia com alta performance

Rede de e-Ciência: monitoramento da performance

- Telemetria de todos os nós da rede
- Perfsonar com testes contínuos no mesmo lsp de transporte da DTN
- Circuitos protegidos (1+1) ponto a ponto de camada 2 com caminhos determinísticos
- Aprovisionamento multi domínio segregado (ao menos inicialmente)
  - Em redes metro, será solicitado service vlan para flexibilidade de criação de circuitos de forma transparente do ponto de vista do operador da rede.
- Criptografia fim a fim – DTN a DTN (ainda necessário validação da solução proposta)
  - MACsec tunelado em VPWS
  - IPsec

Rede de e-Ciência: transição

- No backbone da RNP:
  - QoS com garantia de 50G de capacidade nos enlaces da rede Ipê
  - Enlaces dedicados serão agregados assim que disponíveis
  - Aprovisionamento dos circuitos com EVPN VPWS (sem multihoming)
- Nos equipamentos nos PoPs da RNP
  - Atualização das conexões para suporte das capacidades necessárias
  - Possível by-pass de camadas para contornar ausência de porta física (casos do JMX204)
  - EVPN VPWS para o switch da SDMZ

- Independente da transição, todas as configurações serão padronizadas
- Expectativa de início da implantação de novos equipamentos apenas no Q1-2026

Automação/orquestração da rede

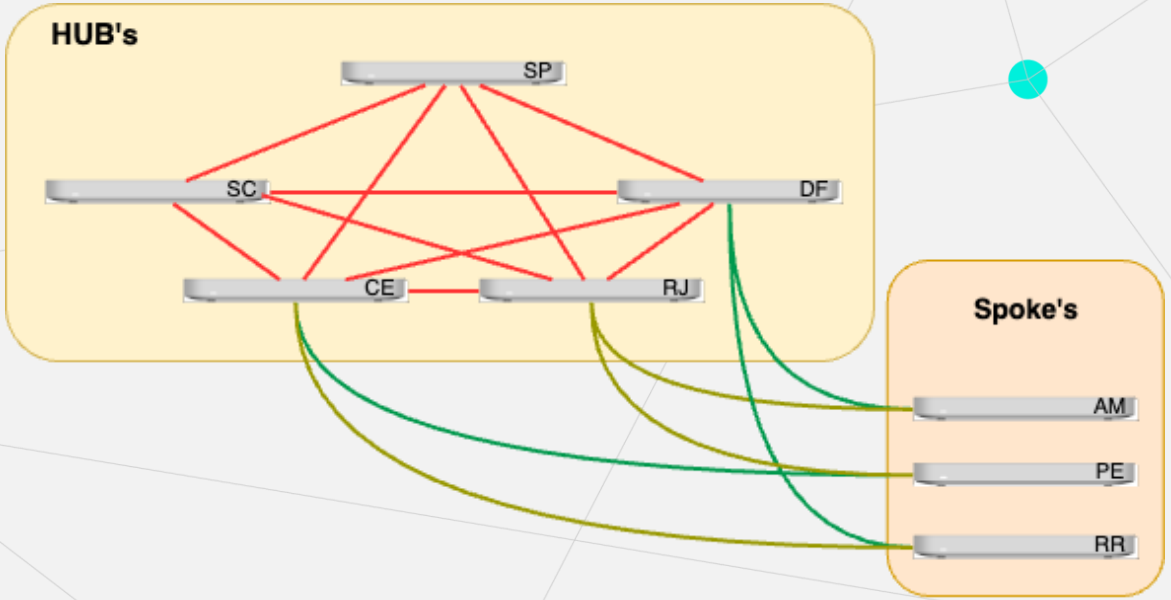
- Ambiente de transferências simplificado por ferramenta gráfica para os usuários finais (piloto Globus)
- Dados de monitoramento como insumos para comutação de rotas com baixo desempenho (testes PS-2-PS)
- Inicialmente não teremos agendamento para transferências, mas é algo que estamos estudando implementar mais a frente.
- Possibilidade de implementação de algum "profile tuning" nas DTNs para atualizar otimizações

Rede de Missão Crítica

- A RNP está desenvolvendo um projeto de uma rede de controle e gerência de missão crítica
- Teve como base a implantação bem sucedida da nova rede de gerência fora de banda (OoB) e discussões internas após visitas realizadas ao NOC e SOC da RNP
- Monitoramento sempre acessível (alta disponibilidade e HW e conectividade) integrado às ferramentas das equipes de operação de redes e segurança da RNP
- Acessos para equipes de engenharia, operações e P&D, incluindo portas consoles, quando aplicável.

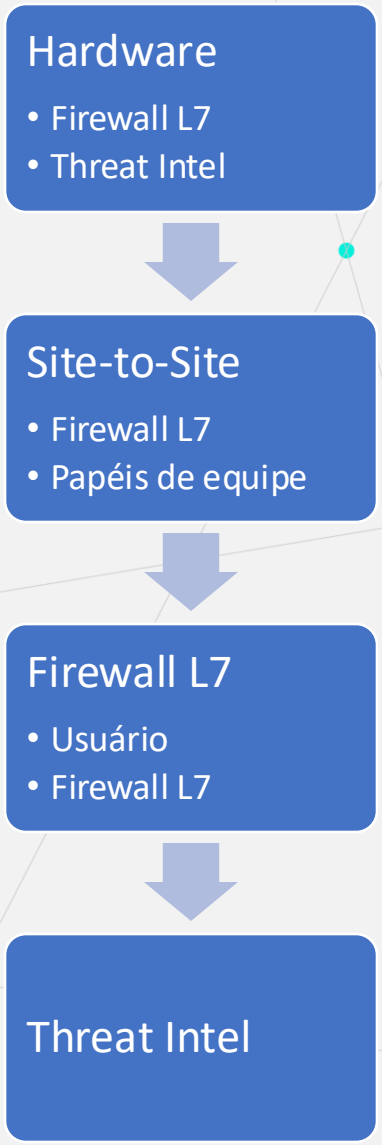
Arquitetura da rede de Missão Crítica

- Rede Ipsec VPN tipo HUB and Spoke
- Mínimo de 2 Hubs por Spoke
- Múltiplos Hubs
- HA (warm-spare)
- Tecnologia SD-WAN para gerenciamento dos acessos in-band e out-of-band (fixo e móvel)



Segurança da rede de Missão Crítica

- FW leste-oeste e norte-sul
  - Granularidade por dispositivo/cliente
- IPS com solução Cisco Talos Intel
- Bloqueios
  - ToR Exit nodes
  - Malware/Phishing
  - DNS
  - AntiSpoofing
- Relatórios
- Export dos logs para ferramenta de segurança com monitoramento do SOC



Automação na rede de Missão Crítica

- **Para a rede de missão crítica:**
  - **Garantir o compliance nas configurações aplicadas**
  - **Pipelines CI/CD com fluxo operacional de alteração**
  - **Aprovisionamento efetuado via API**
- **Para os componentes do e-ciência**
  - **Garantir túneis seguros e disponíveis**
  - **Aplicar hardering**
  - **Alteração de profile tuning**
  - **Export dos dados para o SOC e ferramentas auxiliares**

Desafios

- Atender as demandas científicas em que a ponta B não esteja na rede de e-Ciência da RNP (instituições nacionais ou internacionais)
- No longo prazo queremos expandir a rede de e-Ciência para qualquer instituição/laboratório conectada via Infovia Estadual ou com possibilidade de conexão via rede metropolitana ou fibra própria
- Desafios vão muito além da conectividade de alta velocidade. Eles incluem:
  - Operação de rede e segurança especializada
  - Aquisição e implantação de um kit SDMZ por instituição (modelo atual). Queremos testar possibilidade de DTN em PoPs.
  - Manutenção da padronização no caso de aquisições por organizações usuárias

Outros projetos na ENG com outras áreas da DAERO contribuem para a Rede de e-Ciência

- AAA unificado
- Documentação unificada
- Rede de gerência e controle de missão crítica
- Monitoramento unificado e expandido

Obrigado!