MENTORED

DA MODELAGEM À EXPERIMENTAÇÃO PREDIZENDO E DETECTANDO ATAQUES DDOS E ZERO-DAY

Michele Nogueira, D.Sc.
Pesquisadora Responsável
michele@dcc.ufmg.br

23 de Maio de 2022

FAPESP MCTIC cgi.br Comitê Gestor da Internet no Brasil UFMG

Panorama do Projeto

Parceiros

MENTORED

UFMG

USP

VIRTUS IMPAVIDA
UFPE

CARNEGIE MELLON UNIVERSITY
PITTSBURGH PENNSYLVANIA 1900

RNP

UNIVALI
UNIVERSIDADE DO VALE DO ITAJAÍ

INSTITUTO FEDERAL
Santa Catarina

SORBONNE UNIVERSITÉ
CRÉATEURS DE FUTURS DEPUIS 1257

Panorama do Projeto

Equipe de Concepção

MENTORED

Michele Nogueira
Pesquisadora Responsável/ Líder WP2

José Suruagy
Pesquisador Principal e Líder WP1

Aldri Santos
Pesquisador Principal e Líder WP3

Michelle Wangham
Pesquisadora Associada e Líder WP4

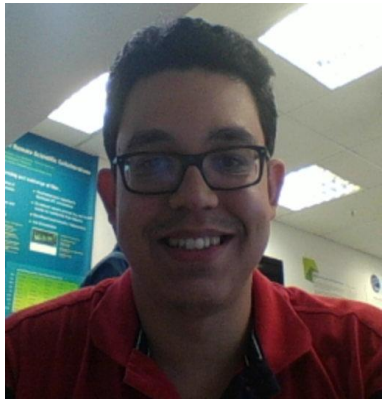
Paulo Gonçalves
Pesquisador Associado

Daniel Batista
Pesquisador Associado

Emerson Melo
Pesquisador Associado

Iara Machado
Apoio

André Marins
Apoio



Clayton Reis
Apoio

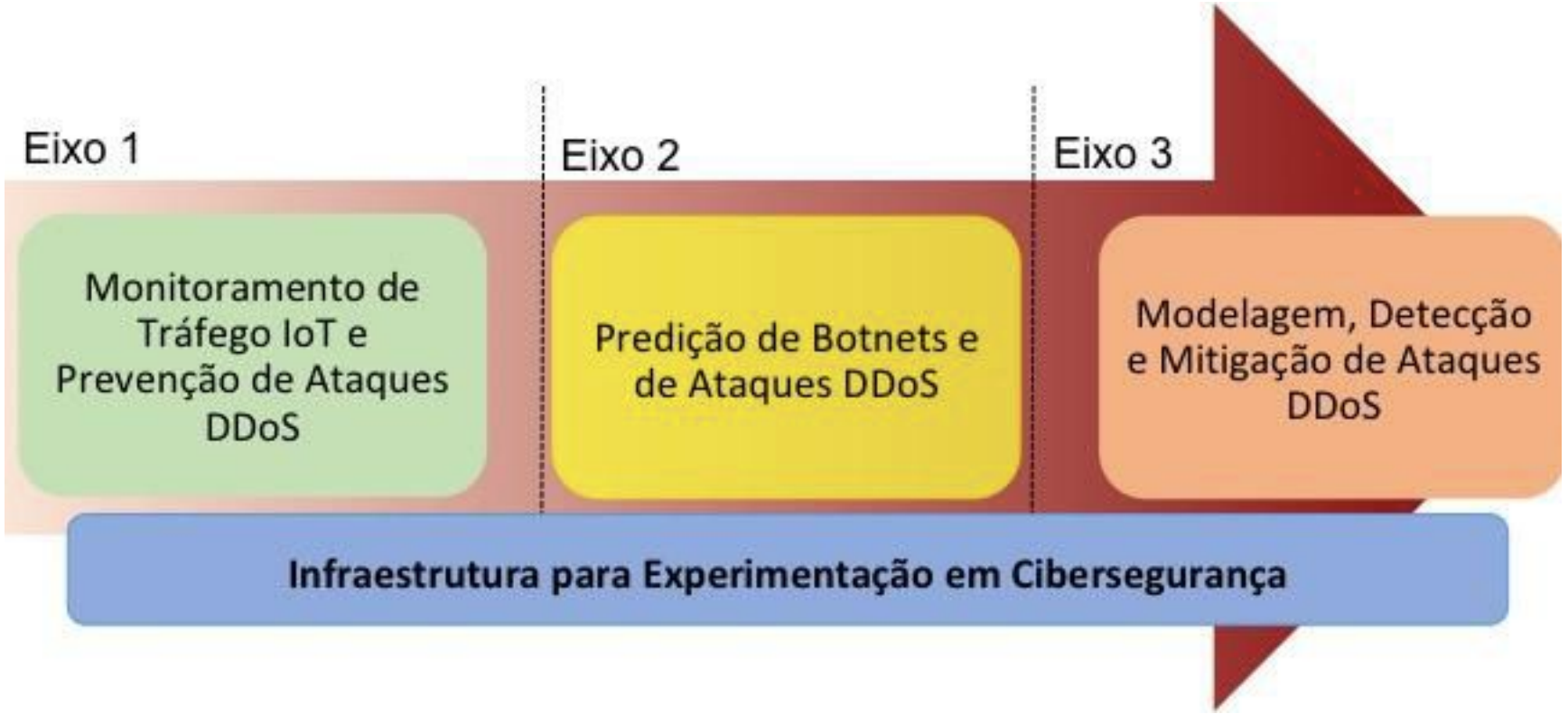
Objetivo Geral

MENTORED

Identificar, **modelar** e **avaliar** comportamentos maliciosos associados à IoT de forma a auxiliar na construção de soluções avançadas e coordenadas para possibilitar:
prevenção, **predição**, **detecção** e **mitigação**
de ataques DDoS e Zero-Day

Visão Geral
Arcabouço de Soluções

MENTORED



Visão Geral
Pacotes de Trabalho

MENTORED

WP1	WP2	WP3	WP4
José Suruagy (líder)	Michele Nogueira (líder)	Aldri Santos (líder)	Michelle Wangham (líder)
Paulo Gonçalves	Daniel Batista	Michele Nogueira	Emerson Mello
Edilson Lima	Wagner Monteverde	Edilson Lima	Iara Machado
			André Marins
			Clayton Reis

Pacote de Trabalho 4

Ambiente Experimental - Cibersegurança

Prover um ambiente controlado para experimentação (*testbed*) com cenários da IoT para avaliar propostas de cibersegurança

Quem?

- 1º Pesquisadores dos WPs
- 2º Comunidade de Segurança

Pacote de Trabalho 4

Objetivos Específicos

MENTORED

- Oferecer recursos para experimentação em cenários realistas

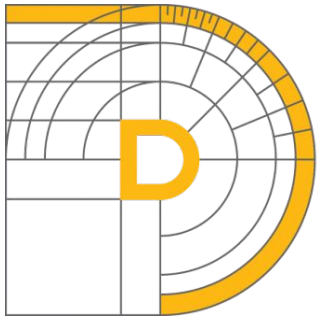
Avaliar soluções contra ataques DDoS e de botnets baseados na IoT

Desenvolver metodologias avançadas para prover pesquisa experimental em cibersegurança sob demanda

Apoiar - EaD, capacitações e disseminação (ataques e soluções de segurança)

Pacote de Trabalho 4
Testbeds de Referência

MENTORED



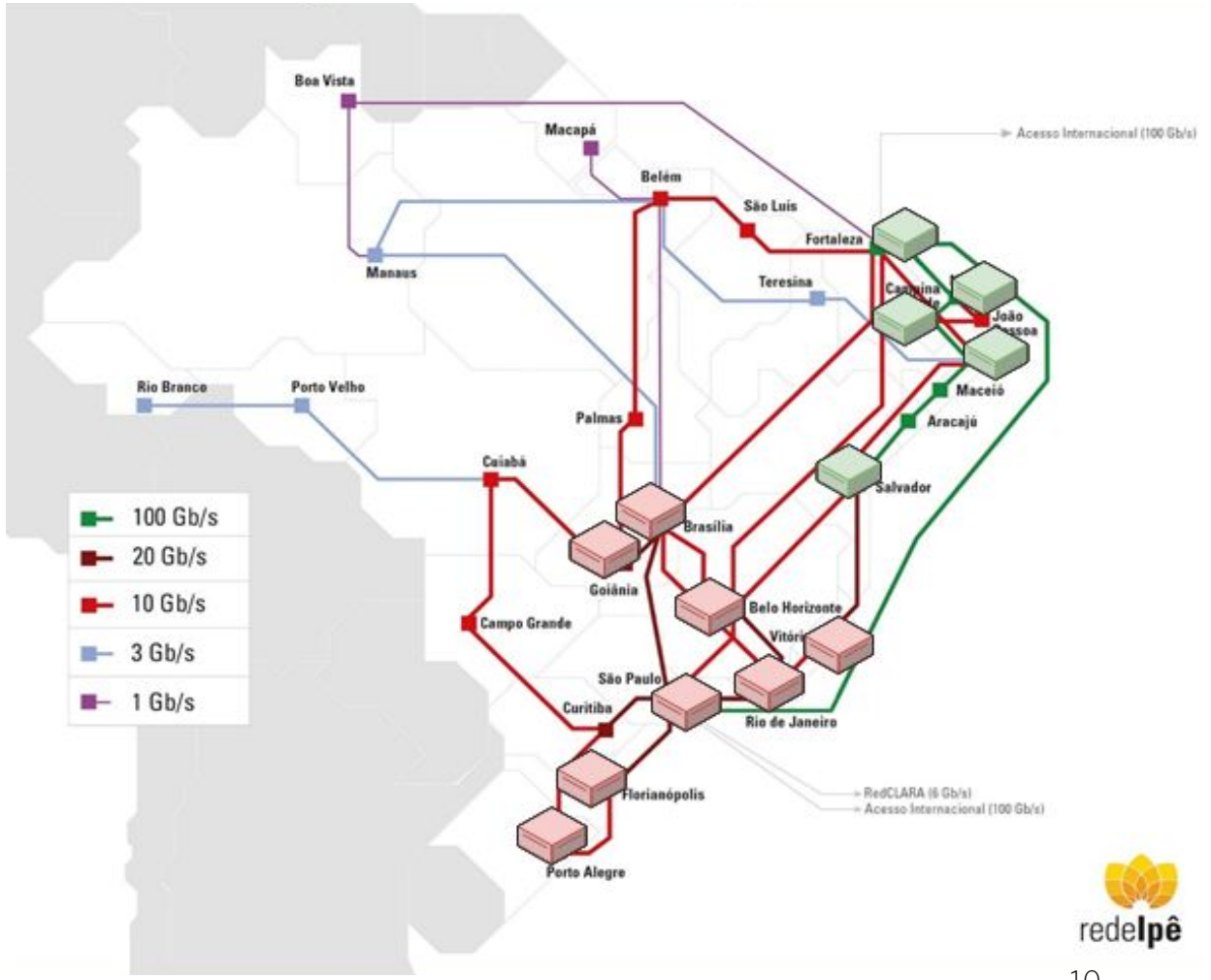
The DETER Project

- Metodologia de experimentação em cibersegurança
  - Experimentação replicável, escalável e verificável
  - Redução da complexidade ao criar experimentos de cibersegurança
- Acesso aos recursos físico como servidores e dispositivos IoT

Infraestrutura Definida por Software
Alicerce

MENTORED

- **RNP**
- **Recursos**
  - Servidores *bare metal*
  - Links de alta velocidade - 1 a 100Gbps
- **Modelo de Uso**
  - Sob demanda (requer setup inicial)
- **Propósito**
  - Infraestrutura virtualizável e programável
  - Orquestração de recursos em paradigma Cloud-Native

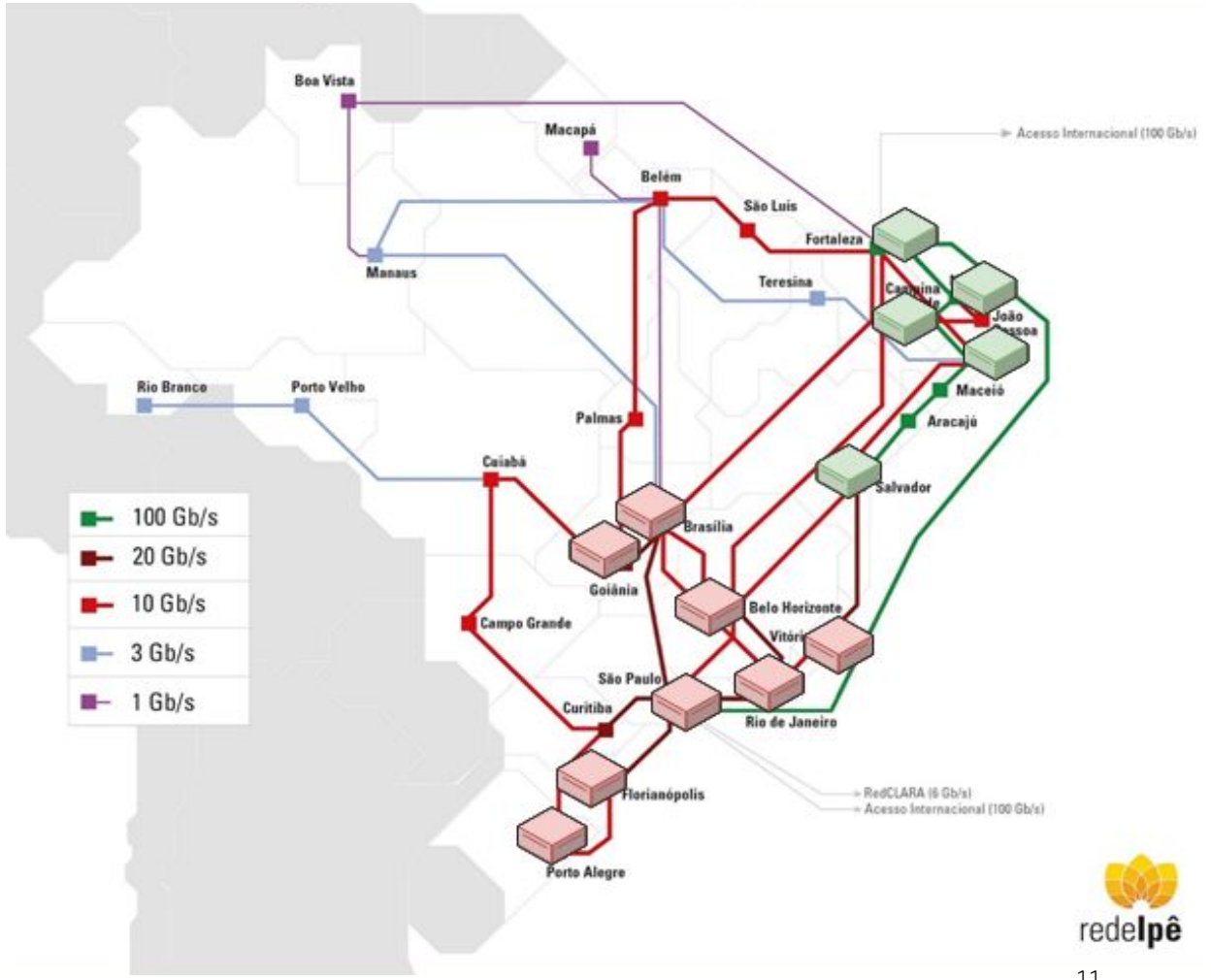


redeIpê

Infraestrutura Definida por Software (IDS-RNP)
Vantagens

MENTORED

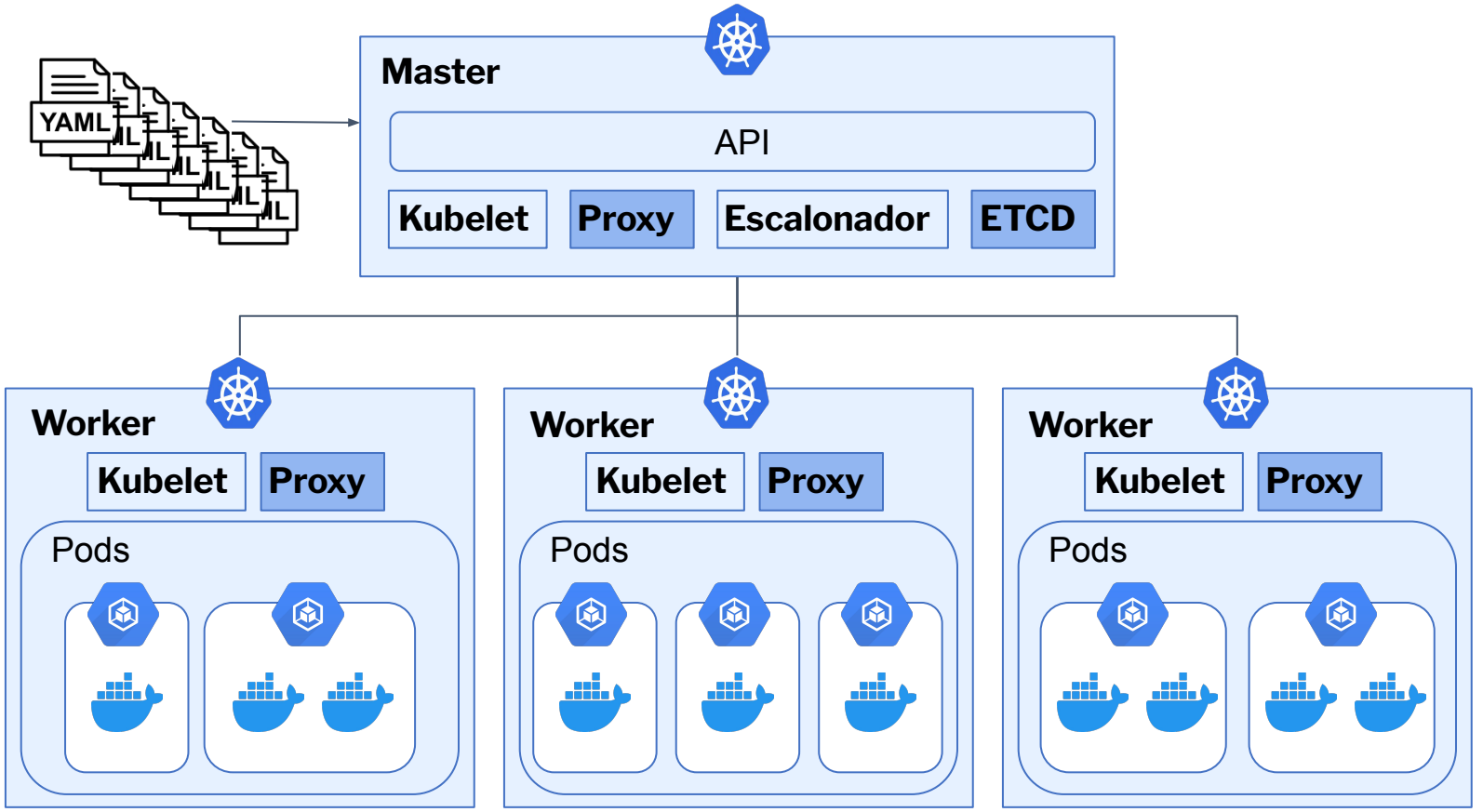
- Processamento e de armazenamento
- Rede customizável e de longa distância
- Software Livre
- Configurações sob-demanda
- Suporta a inclusão de redes de borda
- Equipe de apoio da RNP



kubernetes docker

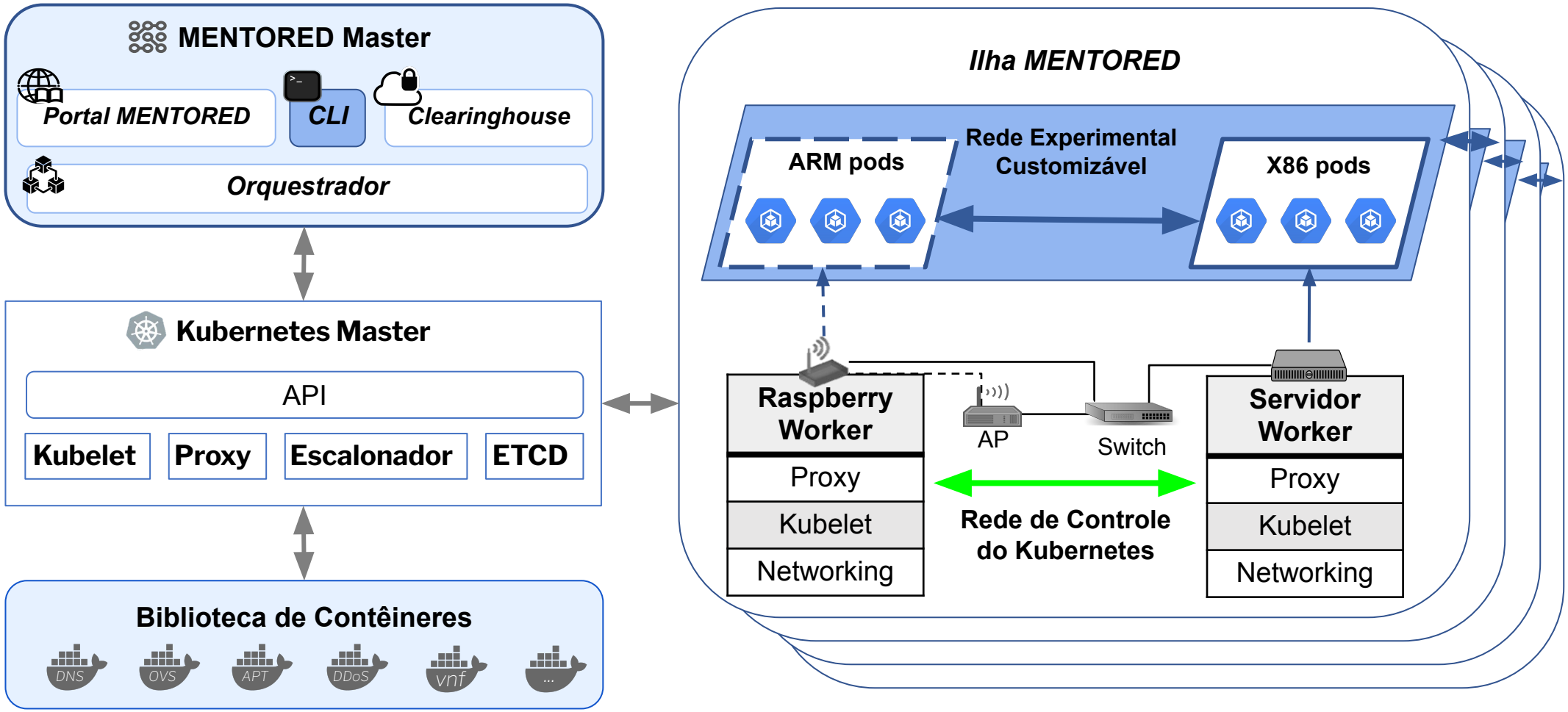
redeIpê

Infraestrutura Definida por Software
Kubernetes



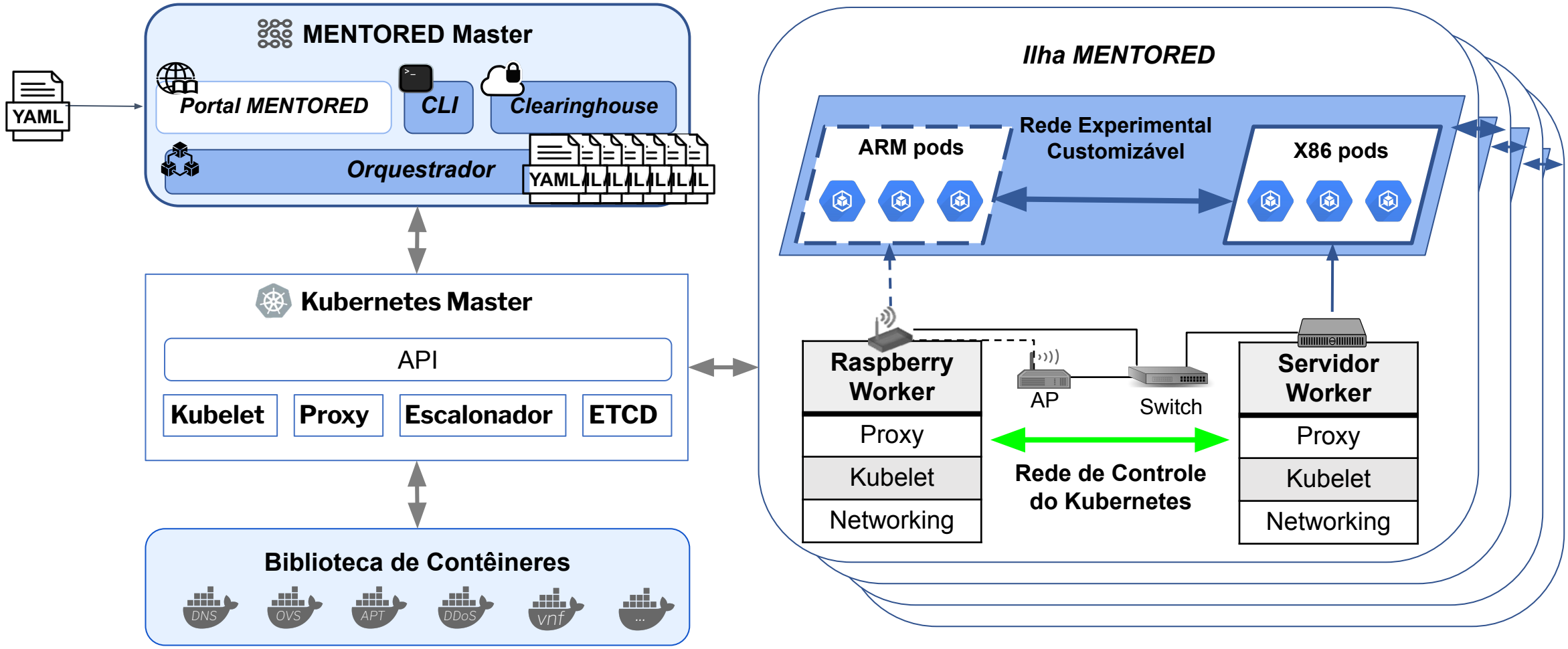
MENTORED Testbed

Arquitetura



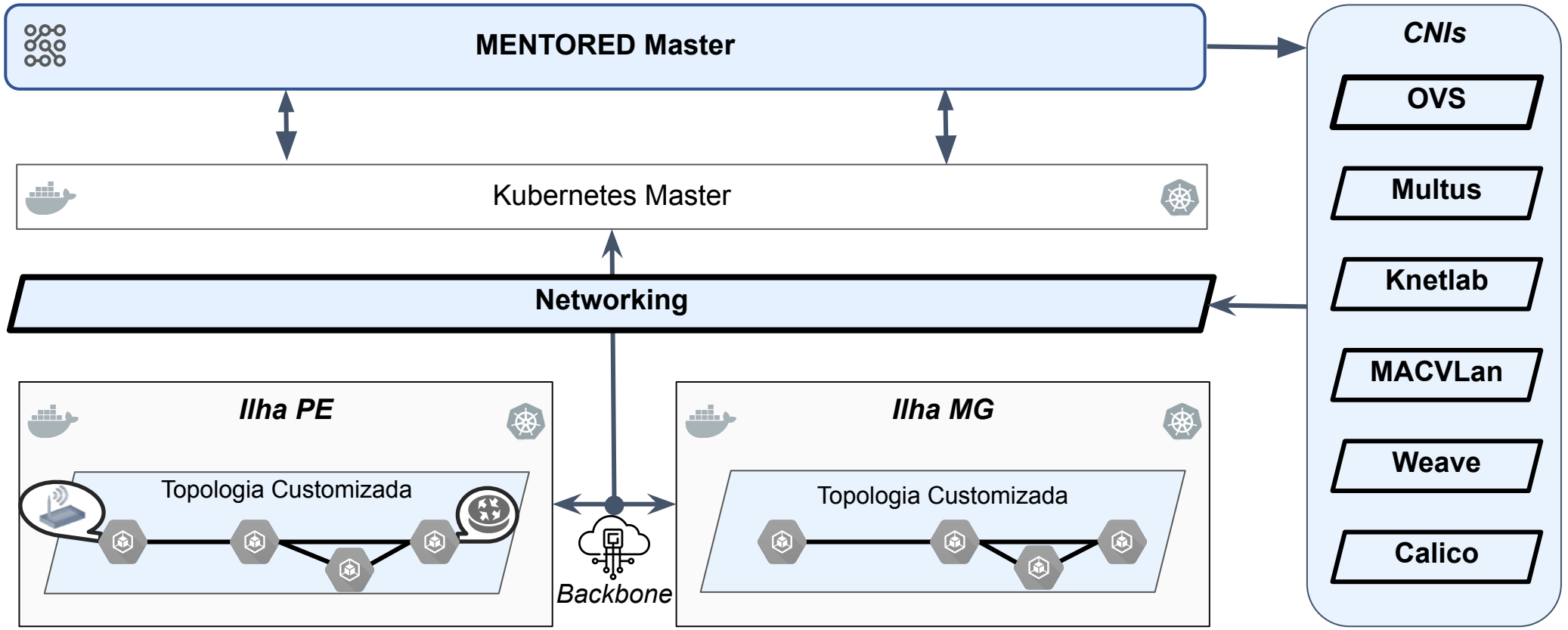
MENTORED Testbed

Arquitetura



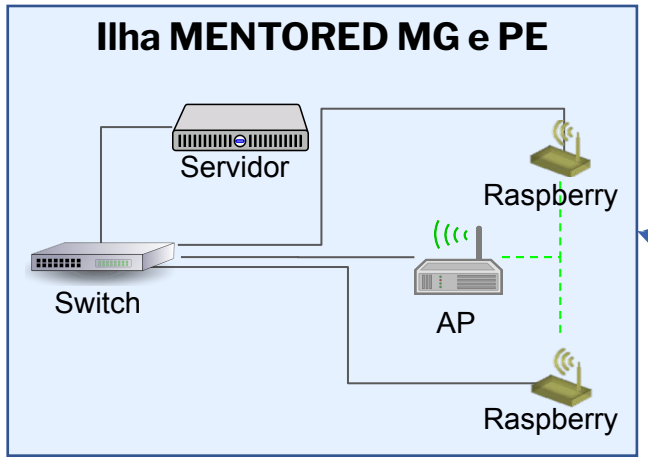
MENTORED Testbed

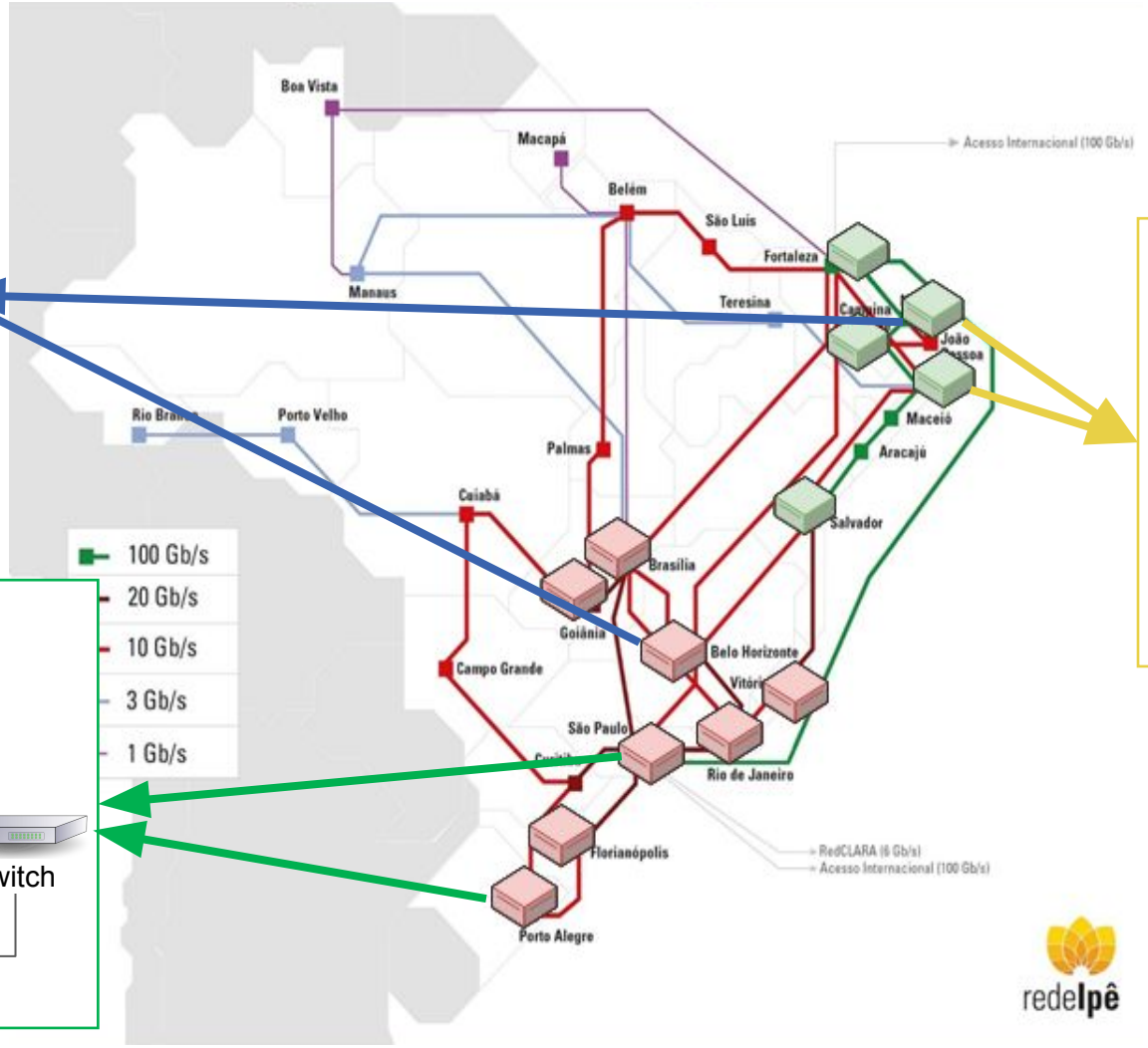
Container Network Interfaces - CNIs

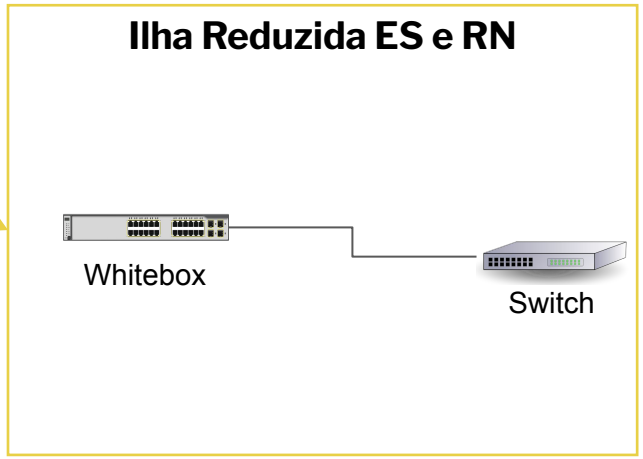


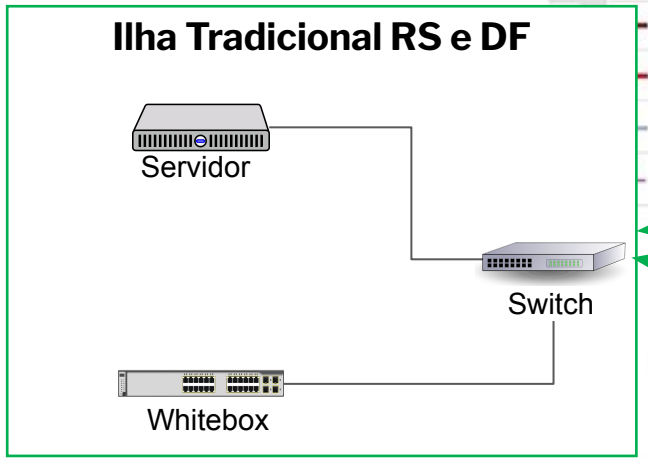
Estudo de caso - botnets
Infraestrutura

MENTORED









MENTORED

Perguntas?
www.mentoredproject.org

Michele Nogueira, D.Sc.
Pesquisadora Responsável
michele@dcc.ufmg.br

23 de Maio de 2022

FAPESP MCTIC cgi.br Comitê Gestor da Internet no Brasil UFMG