PONTIFÍCIA UNIVERSIDADE CATÓLICA DE GOIÁS
ESCOLA POLITÉCNICA E DE ARTES
GRADUAÇÃO EM ENGENHARIA DE COMPUTAÇÃO

Monitoramento Contínuo de Redes: Desenvolvimento de uma Solução Automatizada com Zabbix

BRENDON EVANGELISTA DOURADO DOS SANTOS

GOIÂNIA
2025

BRENDON EVANGELISTA DOURADO DOS SANTOS

Monitoramento Contínuo de Redes: Desenvolvimento de uma Solução Automatizada com Zabbix

Trabalho de Conclusão de Curso apresentado à Escola Politécnica e de Artes, da Pontifícia Universidade Católica de Goiás, como parte dos requisitos para a obtenção do título de Bacharel em Engenharia de Computação.

Orientador(a):

Prof. Dr. Ernesto Fonseca Veiga

Banca examinadora:

Prof. Me. Daniel Correa da Silva

Prof. Me. Fabrício Schlag

GOIÂNIA
2025

BRENDON EVANGELISTA DOURADO DOS SANTOS

Monitoramento Contínuo de Redes: Desenvolvimento de uma Solução Automatizada com Zabbix

Trabalho de Conclusão de Curso aprovado em sua forma final pela Escola Politécnica e de Artes, da Pontifícia Universidade Católica de Goiás, para obtenção do título de Bacharel em Engenharia de Computação, em _____/_____/_____.

_____
Orientador (a): Dr. Ernesto Fonseca Veiga

_____
Prof. Me. Daniel Correa da Silva

_____
Prof. Me. Fabrício Schlag

GOIÂNIA
2025

RESUMO

Este trabalho apresenta o desenvolvimento de uma solução completa de monitoramento contínuo de redes utilizando a plataforma Zabbix integrada ao Grafana, aplicada ao ambiente operacional de provedores de internet. O objetivo consiste em substituir práticas reativas de diagnóstico — baseadas em verificações manuais, múltiplas ferramentas desconectadas e identificação tardia de falhas — por um sistema automatizado capaz de coletar métricas em tempo real, gerar visualizações avançadas e agilizar a tomada de decisões técnicas. Para isso, foram realizados levantamentos de requisitos junto à equipe de operação, análises dos processos internos, mapeamento da arquitetura da rede e definição dos principais indicadores de desempenho e disponibilidade.

Com base nesse levantamento, foram especificados, configurados e validados dashboards personalizados no Zabbix, complementados por painéis dinâmicos do Grafana que aprimoram a visualização gráfica das métricas e facilitam análises históricas. A solução contempla monitoramento de estabilidade BGP, potência óptica, consumo de links, sessões PPPoE, ocupação de pools CGNAT e distribuição de clientes por VLAN, além da emissão de alertas automatizados via Telegram. Os resultados demonstram que a integração Zabbix–Grafana elimina a dependência de verificações manuais, amplia a precisão diagnóstica, reduz o tempo médio de resposta e melhora a previsibilidade e estabilidade operacional da rede.

A solução proposta promove maior eficiência na gestão de infraestrutura e pode ser facilmente adaptada para diferentes realidades de provedores de internet, evidenciando seu potencial de escalabilidade, automação e suporte estratégico à continuidade do serviço.

Palavras chaves: Zabbix. Grafana. Monitoramento de Redes. Provedores de Internet. Automação. Observabilidade. Infraestrutura de TI.

ABSTRACT

This work presents the development of a complete solution for continuous network monitoring using the Zabbix platform integrated with Grafana, applied to the operational environment of Internet Service Providers. The aim is to replace reactive diagnostic practices — based on manual checks, disconnected tools, and late fault detection — with an automated system capable of collecting real-time metrics, generating advanced visualizations, and accelerating technical decision-making.

To achieve this, requirement elicitation was conducted with the network operations team, followed by analysis of current processes, mapping of the infrastructure architecture, and identification of the main performance and availability indicators. Based on this analysis, customized dashboards were specified, configured, and validated in Zabbix, complemented by dynamic Grafana panels that enhance graphical visualization and support historical analyses.

The solution includes monitoring of BGP stability, optical power levels, link utilization, PPPoE sessions, CGNAT pool usage, and VLAN distribution, in addition to automated alerts delivered via Telegram. The results demonstrate that the Zabbix–Grafana integration eliminates reliance on manual checks, increases diagnostic accuracy, reduces Mean Time to Repair, and improves the predictability and operational stability of the network.

The proposed system promotes greater efficiency in infrastructure management and can be easily adapted to different ISP environments, highlighting its potential for scalability, automation, and strategic support to service continuity.

Keywords: Zabbix. Grafana. Network Monitoring. Internet Service Provider. Automation. Observability. IT Infrastructure.

SUMÁRIO

LISTA DE FIGURAS

LISTA DE TABELAS

LISTA DE ABREVIATURAS

API – *Application Programming Interface*
BGP – *Border Gateway Protocol*
BNG – *Broadband Network Gateway*
BRAS – *Broadband Remote Access Server*
CDN – *Content Delivery Network*
CGNAT – *Carrier-Grade Network Address Translation*
CPU – *Central Processing Unit*
DDoS – *Distributed Denial of Service*
DGO – Dashboard Gráfico Operacional
DHCP – *Dynamic Host Configuration Protocol*
DNS – *Domain Name System*
ECMP – *Equal-Cost Multi-Path*
GBIC – *Gigabit Interface Converter*
GPON – *Gigabit Passive Optical Network*
ICMP – *Internet Control Message Protocol*
IEEE – *Institute of Electrical and Electronics Engineers*
IP – *Internet Protocol*
IPoE – *IP over Ethernet*
IPv4 – *Internet Protocol version 4*
IPv6 – *Internet Protocol version 6*
ISP – *Internet Service Provider*
IXC – Soluções avançadas em tecnologia
LLD – *Low-Level Discovery*
MPLS – *Multiprotocol Label Switching*
MTTR – *Mean Time to Repair*
NAT – *Network Address Translation*
NOC – *Network Operations Center*
OLT – *Optical Line Terminal*
ONU – *Optical Network Unit*
PICOC – *Population, Intervention, Comparison, Outcome, Context*
PPPoE – *Point-to-Point Protocol over Ethernet*
PtP – *Point-to-Point*
PTT – Ponto de Troca de Tráfego
RF – Requisito Funcional
RNF – Requisito Não Funcional
SFP – *Small Form-factor Pluggable*
SNMP – *Simple Network Management Protocol*
SQL – *Structured Query Language*
VLAN – *Virtual Local Area Network*
VoIP – *Voice over IP*
Wi-Fi – *Wireless Fidelity*

1. INTRODUÇÃO

1.1 Contexto e Motivação

O monitoramento de redes desempenha um papel essencial na operação de provedores de internet, especialmente em ambientes distribuídos e compostos por equipamentos heterogêneos. Em infraestruturas desse tipo, falhas como quedas de sessões PPPoE, instabilidades em BGP, variações de potência óptica ou saturação de interfaces podem impactar diretamente milhares de usuários. Segundo Sebestyen, Popescu e Zmaranda (2025), redes críticas demandam mecanismos contínuos de observabilidade capazes de identificar anomalias e preservar a estabilidade do serviço.

Ferramentas como o Zabbix e o Grafana são amplamente utilizadas nesse contexto. O Zabbix é uma plataforma de monitoramento open source, voltada à coleta e análise de métricas de dispositivos e serviços de rede por meio de protocolos como SNMP e ICMP (ZABBIX, 2024). O Grafana, também open source, complementa esse processo ao permitir a criação de dashboards interativos e consolidados, facilitando a visualização do estado da infraestrutura (GRAFANA LABS, 2024). A automação de alertas por meio de bots no Telegram contribui para a notificação em tempo real de eventos críticos, reduzindo o tempo de resposta a incidentes.

No âmbito operacional, o IXC, sistema de gestão amplamente adotado por provedores de internet no Brasil, oferece funcionalidades administrativas e operacionais que podem ser integradas às plataformas de monitoramento, ampliando a correlação entre eventos técnicos e dados de negócio (IXC SOFT, 2025). Apesar da disponibilidade dessas tecnologias, muitos provedores ainda as utilizam de forma fragmentada, sem padronização entre POPs ou integração entre dashboards, o que dificulta o diagnóstico rápido de falhas e favorece uma atuação reativa (CORDEIRO; VASCONCELOS; CORREIA, 2022).

Diante desse cenário, este trabalho propõe o desenvolvimento de um modelo de monitoramento contínuo, padronizado e integrado, baseado na utilização do Zabbix, Grafana, Telegram e IXC. O objetivo é reduzir o tempo de resposta a incidentes, aumentar a previsibilidade de falhas e contribuir para uma operação mais eficiente. Trata-se ainda de um relato de experiência, que descreve a aplicação prática da solução em um ambiente real de provedor de internet.

1.2 Problema e Questão de Pesquisa

O monitoramento de redes em provedores de internet apresenta desafios particulares, especialmente devido à diversidade de equipamentos, à distribuição

geográfica dos POPs e à alta criticidade das operações. Ambientes desse tipo exigem visibilidade contínua, detecção rápida de falhas e capacidade de interpretar corretamente o comportamento da infraestrutura para evitar indisponibilidades que impactam usuários simultaneamente. Estudos e relatos técnicos mostram que, em redes complexas, a falta de padronização e de processos estruturados prejudica a identificação de anomalias e aumenta o tempo de resposta da equipe operacional Da Silva, (2021); Motta; De Oliveira; Travassos, (2020).

Quando provedores precisam estruturar seus próprios sistemas de monitoramento, surgem dificuldades relacionadas ao esforço elevado para padronizar métricas, integrar ferramentas distintas, configurar alertas confiáveis e manter coerência entre diferentes POPs, OLTs, BRAS, roteadores e servidores. Essa variabilidade torna o processo de monitoramento mais custoso, propenso a falhas e dependente de ações manuais, reduzindo a eficiência operacional Cordeiro; Vasconcelos; Correia, (2022). Nesse contexto, modelos estruturados de monitoramento — com dashboards padronizados, automações consolidadas e integrações bem definidas — tornam-se recursos essenciais para orientar equipes e garantir consistência nas análises.

Apesar da existência de ferramentas robustas como Zabbix e Grafana, muitos provedores utilizam apenas parte do potencial dessas plataformas. Em vários casos, falta padronização, integração, correlação de dados e automações avançadas, o que resulta em ambientes fragmentados e pouco eficientes. Da mesma forma que ocorre em outros domínios técnicos, o conhecimento disponível muitas vezes se encontra disperso, exigindo que cada provedor desenvolva suas próprias soluções, scripts, triggers e visualizações a partir do zero — aumentando o risco de erros e dificultando melhorias contínuas.

Dessa forma, o problema central deste trabalho é apresentado a seguir:

“A carência de um modelo padronizado e automatizado de monitoramento contínuo para provedores de internet, utilizando Zabbix, Grafana e alertas via Telegram, capaz de integrar informações, reduzir as falhas operacionais e ampliar a visibilidade da infraestrutura de rede.”

A partir do problema apresentado, o estudo busca propor uma abordagem sistemática para organizar, integrar e automatizar o monitoramento da infraestrutura, reduzindo a dependência de verificações manuais e proporcionando maior eficiência operacional. O objetivo é transformar o monitoramento atual — muitas vezes fragmentado — em um ecossistema coerente, padronizado e capaz de apoiar decisões rápidas e confiáveis durante incidentes.

1.3 Objetivo

O objetivo geral deste trabalho é **propor e desenvolver um modelo padronizado e automatizado de monitoramento contínuo para provedores de internet**, utilizando Zabbix como plataforma central de coleta, análise e automação, integrado ao Grafana e ao Telegram para ampliar a visibilidade da rede e agilizar a resposta a incidentes.

Como objetivos específicos, destacam-se:

- **Padronizar dashboards e métricas** nos POPs, BRAS, roteadores e enlaces ópticos, criando uma estrutura visual unificada no Zabbix e no Grafana;
- **Integrar dados operacionais**, combinando informações obtidas via SNMP, ICMP, scripts externos, LLD e consultas ao banco do IXC para compor uma visão completa da infraestrutura;
- **Automatizar alertas e notificações**, utilizando triggers inteligentes e envio de mensagens estruturadas via Telegram Bot;
- **Definir um conjunto de métricas essenciais**, permitindo monitorar sessões PPPoE, estabilidade BGP, saúde óptica, uso de CPU/memória, consumo de links e ocupação de pools;
- **Organizar o monitoramento em um modelo navegável**, permitindo que a equipe técnica identifique rapidamente falhas, gargalos e comportamentos anômalos;
- **Ampliar a rastreabilidade das informações**, relacionando incidentes, métricas e elementos da infraestrutura de forma clara para apoiar diagnósticos e tomadas de decisão.

1.4 Metodologia

O processo metodológico deste trabalho iniciou-se com uma análise detalhada do ambiente real de um provedor de internet, utilizando observações diretas, registros operacionais e estudo de incidentes para entender as principais necessidades do monitoramento. Essa abordagem segue princípios de pesquisa aplicada e relato de experiência, permitindo identificar limitações, fragilidades e oportunidades de melhoria a partir da vivência prática.

Em seguida, foram levantadas referências técnicas a respeito de monitoramento de redes, automação, protocolos (PPPoE, BGP, ICMP, SNMP), além de documentações oficiais do Zabbix, Grafana e IXC. O material foi organizado com o apoio do Zotero, considerando bases como IEEE Xplore, Scopus e Google Scholar, bem como fontes técnicas amplamente utilizadas no setor de telecom.

A partir dessa análise, observou-se que muitos provedores enfrentam problemas de fragmentação entre ferramentas de monitoramento, falta de padronização e necessidade constante de verificações manuais. Tais limitações comprometem a navegabilidade e a clareza dos dashboards, dificultando a eficiência operacional — situação semelhante às dificuldades relatadas na literatura sobre sistemas distribuídos e ambientes de alta complexidade (Cordeiro; Vasconcelos; Correia, 2022).

Com base nessas evidências, optou-se por adotar o Zabbix como núcleo da solução, complementado pelo Grafana para visualização avançada e pelo Telegram Bot para envio de alertas. As integrações foram modeladas com uso de triggers, LLD, itens personalizados, consultas ao banco IXC e painéis organizados por contexto (borda, BRAS, POPs, enlaces ópticos e CGNAT).

Por fim, desenvolveu-se uma proposta estruturada contendo os dashboards prototipados, o fluxo de automação dos alertas, a padronização visual das telas e o conjunto final de métricas que compõem o modelo.

É importante destacar que este trabalho se caracteriza como um estudo de caso, construído a partir da experiência direta do autor dentro de uma empresa de telecomunicações. Todo o desenvolvimento apresentado desde a análise dos problemas até a implantação das soluções reflete situações reais vivenciadas no ambiente de produção do provedor. Assim, o projeto não é meramente teórico, mas sim o relato estruturado de uma intervenção prática realizada no contexto operacional da empresa.

1.5 Organização do Text

Este trabalho está estruturado nos seguintes capítulos:

Capítulo 1 – Introdução

Apresenta o contexto do monitoramento em provedores, a motivação, o problema de pesquisa, os objetivos e a metodologia utilizada. Também é discutida a importância da padronização e automação na operação de redes.

Capítulo 2 – Fundamentos Teóricos

Traz os conceitos essenciais para compreender o ambiente monitorado. São abordados protocolos como PPPoE e BGP, fundamentos de SNMP/ICMP, princípios de monitoramento, funcionamento de OLTs e GPON, além das bases do Zabbix, Grafana e Telegram Bot.

Capítulo 3 – Estudo de Caso e Análise do Ambiente

Descreve o ambiente real do provedor analisado, os desafios enfrentados no monitoramento atual, a fragmentação dos dashboards, os incidentes recorrentes e os benefícios esperados com a solução proposta.

Capítulo 4 – Proposta de Solução

Apresenta o modelo completo de monitoramento desenvolvido. Inclui a estruturação dos dashboards, integração com IXC, criação de métricas, prototipação visual, automação via Telegram e padronização dos POPs e equipamentos.

Capítulo 5 – Conclusão

Traz o fechamento do trabalho, destacando os resultados alcançados, as melhorias percebidas no ambiente monitorado, limitações do estudo e sugestões para trabalhos futuros.

2.FUNDAMENTAÇÃO TEÓRICA

2.1 Sistema de Monitoramento em Provedores de Internet

Provedores de internet (ISPs) operam redes complexas compostas por diversos elementos: roteadores de borda, sistemas BRAS/BNG, OLTs, switches de agregação, enlaces ópticos, servidores internos, CGNAT, além de múltiplas rotas e sessões BGP. Diferentemente de redes pequenas ou domésticas, ambientes de provedor exigem alta disponibilidade, redundância e respostas rápidas a falhas, já que qualquer instabilidade pode afetar milhares de clientes simultaneamente. Segundo Olifer e Olifer (2023), redes de grande porte demandam arquiteturas mais robustas, mecanismos de controle distribuído e políticas de gerenciamento capazes de manter estabilidade mesmo sob alta carga e eventos inesperados.

Essas redes geralmente são divididas em:

- Backbone – onde circula o tráfego de maior volume.
- Anel de transporte (MPLS/Metro) – interliga pops e bairros.
- Rede de acesso (GPON ou PtP) – entrega o serviço ao assinante.
- Rede de autenticação (PPPoE/Hotspot/IPOe) – controla sessões.
- Serviços internos – CGNAT, DNS, DHCP, Radius, IXC.

Entender esses componentes é essencial para montar um sistema de monitoramento eficiente.

2.2 Protocolos Essenciais para Monitoramento

Antes de apresentar cada protocolo, é importante destacar que todo o sistema de monitoramento — especialmente em provedores de internet — depende diretamente da forma como os equipamentos se comunicam e disponibilizam informações para ferramentas como o Zabbix. Protocolos como SNMP, ICMP, BGP, PPPoE e CGNAT não são apenas componentes técnicos; eles representam as principais fontes de dados utilizadas para entender a saúde, o desempenho e o comportamento da infraestrutura. De acordo com Stallings (2022), a observabilidade de redes modernas depende fortemente da padronização desses protocolos e da capacidade de extrair métricas confiáveis a partir deles.

No contexto deste trabalho, que propõe um modelo de monitoramento contínuo e automatizado, esses protocolos são fundamentais porque cada um deles fornece um tipo específico de informação que afeta diretamente a experiência do cliente. Se um desses protocolos falha ou apresenta anomalias, o provedor enfrenta quedas, lentidão, aumento de chamadas no suporte e até interrupção completa do serviço. Por isso, compreender e monitorar corretamente esses protocolos é o ponto de partida para construir dashboards precisos, triggers inteligentes e alertas automatizados.

2.2.1 SNMP – Simple Network Management Protocol

O SNMP é considerado o pilar do monitoramento moderno em redes de provedores, por ser o protocolo responsável por permitir que equipamentos exponham informações internas de funcionamento. De acordo com Mauro (2021), o SNMP permanece como o principal mecanismo de gerenciamento em redes corporativas e de larga escala, fornecendo dados essenciais para diagnóstico, medição de desempenho e detecção de falhas. Através dele, o Zabbix coleta dados detalhados de switches, roteadores, OLTs, BRAS e servidores, incluindo estatísticas de tráfego, consumo de CPU, temperatura interna, potência óptica, utilização de memória, status de interfaces e condições dos módulos instalados.

Sua importância decorre do fato de que o SNMP oferece visibilidade profunda sobre o comportamento dos dispositivos, permitindo que a equipe técnica identifique problemas antes que eles se tornem indisponibilidades para o cliente final. Sem SNMP, o monitoramento ficaria restrito a informações superficiais, como disponibilidade via ping, tornando impossível detectar situações críticas como aquecimento anormal, queda gradual de potência óptica, saturação de portas ou degradação de hardware. Portanto, o SNMP viabiliza a observabilidade completa da rede, sendo essencial para qualquer solução de monitoramento profissional.

2.2.2 ICMP – *Internet Control Message Protocol*

O ICMP é amplamente utilizado para acompanhar a disponibilidade de equipamentos e a estabilidade da comunicação entre os principais pontos da rede. Segundo Feitosa e Moura (2021), protocolos de diagnóstico como ICMP são fundamentais para avaliar conectividade, latência e perda de pacotes, servindo como base para a detecção preliminar de falhas em ambientes complexos. Através de medições de latência, perda de pacotes e resposta ao echo request (ping), o protocolo permite identificar se um dispositivo está acessível, se há degradação no caminho ou se existem oscilações que possam indicar falhas físicas, congestionamentos ou problemas de roteamento.

Embora seja simples quando comparado a outros protocolos, o ICMP tem papel crítico no monitoramento porque funciona como uma espécie de “primeiro alarme” da rede. Muitas falhas começam se manifestando como pequenos aumentos de latência ou perdas intermitentes, e detectar esses sinais precocemente é essencial para reduzir o impacto ao cliente. Além disso, o ICMP fornece a visão operacional básica sobre a saúde dos enlaces, permitindo validar se as anomalias percebidas em equipamentos ou sessões estão relacionadas ao caminho físico ou lógico até eles.

2.3.4 BGP – Border Gateway Protocol

O BGP é o protocolo de roteamento que conecta o provedor à internet, permitindo a troca de rotas entre sistemas autônomos. De acordo com White e Azadi (2022), o BGP é a base do roteamento interdomínios e desempenha papel crítico na estabilidade da

internet global, exigindo monitoramento contínuo para detecção de falhas, flaps e mudanças anormais de rotas. Ele estabelece sessões (peers) com operadoras de trânsito, PTTs, CDNs e outros provedores, determinando os caminhos utilizados pelo tráfego de entrada e saída. Qualquer falha ou instabilidade no BGP pode impactar diretamente o acesso dos clientes a diversos serviços, já que mudanças repentinas nos caminhos podem provocar latência elevada, perda de rotas ou até interrupção total do tráfego.

Monitorar o BGP é fundamental para compreender a estabilidade das conexões externas do provedor. Isso envolve acompanhar o estado das sessões, o número de prefixos recebidos, a ocorrência de flaps, o uptime das conexões e o comportamento dos peers. Instabilidades nesse protocolo costumam ter efeitos amplificados, pois afetam a comunicação da rede inteira com a internet. Dessa forma, o BGP se torna um dos pontos mais críticos do monitoramento, exigindo acompanhamento rigoroso e alertas altamente confiáveis.

2.3.5 PPPoE – *Point-to-Point Protocol over Ethernet*

O PPPoE é amplamente utilizado pelos provedores brasileiros como método de autenticação e criação de sessões individuais para cada cliente. Segundo Luizelli et al. (2020), protocolos de acesso como PPPoE continuam essenciais para o controle de sessão, autenticação e gerenciamento de assinantes em redes de banda larga, especialmente em provedores regionais. O protocolo é executado no BRAS/BNG e controla a forma como os assinantes se conectam, recebem endereços IP e mantêm suas sessões ativas. Por isso, acompanhar seu funcionamento é essencial para garantir que o acesso à rede ocorra de maneira estável e previsível.

O monitoramento do PPPoE inclui a observação do número de sessões ativas, quedas simultâneas de clientes, falhas de autenticação, saturação de recursos do BRAS e variações nas VLANs de atendimento. Problemas no PPPoE costumam gerar impacto imediato e perceptível pelos usuários, resultando em chamadas em massa ao suporte e instabilidade generalizada. Assim, o PPPoE representa um dos indicadores mais importantes do estado operacional da rede, sendo indispensável sua análise contínua e detalhada.

2.3.6 CGNAT – *Carrier-Grade* NAT

Devido à escassez de endereços IPv4, o CGNAT tornou-se parte fundamental da operação de provedores. Ele permite que vários assinantes compartilhem um único IP público por meio da tradução de portas. Conforme destacam Sarrabezolles e Donnet (2021), mecanismos como CGNAT são essenciais para prolongar a vida útil do IPv4, embora introduzam desafios significativos em termos de rastreabilidade, desempenho e experiência do usuário. No entanto, essa solução traz consigo a necessidade de monitoramento rigoroso, pois seu mau funcionamento pode impedir que clientes naveguem corretamente, acessem serviços ou estabeleçam conexões necessárias para aplicações do dia a dia.

O monitoramento do CGNAT envolve acompanhar a ocupação das portas NAT, o tamanho dos pools, possíveis conflitos internos, consumo de tráfego e comportamento de cada bloco. Quando um pool atinge seu limite, os clientes passam a enfrentar erros aparentemente aleatórios, como falhas ao abrir sites, lentidão ou indisponibilidade de serviços mesmo que a conexão física esteja ativa. Por isso, o acompanhamento desse protocolo é essencial para garantir continuidade, estabilidade e qualidade na navegação dos usuários.

2.4 *Infraestrutura Óptica*

A infraestrutura óptica é um dos pilares mais importantes da operação de provedores de internet, pois é ela que sustenta o transporte de dados entre POPs, bairros e residências. Entre os modelos de acesso mais utilizados no Brasil está o GPON (Gigabit Passive Optical Network), tecnologia que permite que múltiplas unidades ópticas (ONUs) compartilhem um único feixe de fibra através de divisores passivos. Em ambientes GPON, o monitoramento é essencial para acompanhar parâmetros como potência óptica recebida e transmitida pelas ONUs, temperatura dos módulos ópticos, carga dos splitters e a utilização das portas nas OLTs. Esses indicadores são fundamentais porque a degradação gradual do nível óptico muitas vezes antecede quedas completas do cliente, permitindo que a equipe técnica aja preventivamente. Oscilações de potência, por exemplo, costumam indicar rompimentos parciais de fibra, reflexões anormais ou problemas em conectores, e podem resultar em desconexões intermitentes se não forem detectadas a tempo. Segundo Ovando e Kassler (2021), redes GPON exigem monitoramento contínuo dos parâmetros ópticos para garantir estabilidade, antecipar falhas e manter a qualidade do serviço prestado.

Além do GPON, muitos provedores utilizam enlaces ópticos ponto a ponto (PtP) para interligar POPs e expandir a rede de transporte. Esses enlaces precisam de monitoramento contínuo, especialmente no que diz respeito ao consumo de banda, estabilidade do caminho, perda de pacotes e leitura dos módulos ópticos (SFP/GBICs). Uma falha em um enlace PtP pode comprometer setores inteiros da rede, interrompendo o funcionamento de múltiplos bairros e serviços dependentes. Por isso, observar sua integridade e desempenho é essencial para manter a operação do provedor estável e resiliente.

2.5 Monitoramento de Redes

O monitoramento de redes consiste no processo contínuo de coleta, análise e visualização de informações sobre todos os componentes da infraestrutura. Ele permite identificar falhas, antecipar problemas e garantir que os serviços sejam prestados com qualidade. Em provedores de internet, essa atividade precisa operar de forma ininterrupta, 24 horas por dia, devido ao número elevado de dispositivos e à criticidade da rede. Um bom monitoramento deve ser automatizado, reduzindo a dependência de verificações manuais; centralizado, reunindo dados de diferentes POPs e equipamentos em um único

ambiente; padronizado, evitando discrepâncias entre dashboards; e visualmente claro, facilitando interpretações rápidas durante incidentes. Sem esses elementos, a equipe técnica trabalha apenas de forma reativa, detectando problemas tardiamente e comprometendo a experiência do usuário final.

2.5.1 Zabbix como Plataforma de Monitoramento

O Zabbix se consolida como uma das ferramentas mais utilizadas no setor de telecomunicações para monitoramento de redes, principalmente por ser *open source*, altamente flexível e escalável. De acordo com Koczan e Gasior (2022), o Zabbix destaca-se por sua arquitetura robusta, capacidade de integração com múltiplos protocolos e pela ampla adoção em ambientes corporativos e provedores devido à sua escalabilidade e recursos avançados de automação. Ele permite coletar informações por diferentes métodos — SNMP, ICMP, scripts personalizados e seu próprio agente — oferecendo uma visão completa do ambiente. Entre seus recursos, destacam-se as triggers inteligentes, que avaliam automaticamente condições de alerta; o sistema de automação baseado em regras; a descoberta automática (LLD) de interfaces, módulos e dispositivos; dashboards nativos personalizáveis; e integrações via API ou *webhooks*.

O Zabbix é considerado o "cérebro" do monitoramento porque centraliza a coleta, organiza os dados e aciona alertas com base em condições definidas. Sem ele, seria inviável acompanhar milhares de métricas simultaneamente ou identificar comportamentos anormais antes de uma falha crítica acontecer.

Apesar de robusto, o Zabbix apresenta limitações na construção de dashboards avançados. Sua interface gráfica possui menor flexibilidade, opções de visualização mais restritas e, muitas vezes, não é tão intuitiva para técnicos que precisam interpretar rapidamente grandes volumes de informações. Além disso, customizações visuais complexas tendem a demandar mais esforço. Por esse motivo, é comum integrar o Zabbix ao Grafana, que funciona como uma camada complementar de visualização.

2.5.2 Grafana como Ferramenta de Visualização

O Grafana é amplamente utilizado para criar dashboards mais modernos, interativos e visualmente atraentes. Ele permite gerar gráficos avançados, painéis coloridos, tabelas comparativas, mapas e elementos dinâmicos que facilitam o entendimento da situação da rede. Conforme indicado por Pires e Anderson (2023), o Grafana tornou-se uma das ferramentas mais versáteis para visualização de dados em ambientes corporativos e de telecom, permitindo criar painéis intuitivos que auxiliam na análise operacional e na tomada de decisão. Enquanto o Zabbix se concentra na coleta e análise de métricas, o Grafana organiza essas informações em layouts claros, favorecendo análises rápidas durante triagem de incidentes e monitoramento em tempo real. Essa combinação é amplamente adotada no setor porque une o melhor dos dois mundos: capacidade analítica do Zabbix e clareza visual do Grafana.

2.5.3 Automação via Telegram Bot

A automação de alertas por meio de bots no Telegram tornou-se prática comum em NOCs (Network Operation Centers), pois permite que a equipe receba notificações instantâneas sobre falhas críticas, anomalias e eventos relevantes. Os alertas chegam diretamente ao celular dos técnicos, reduzindo o tempo de detecção e aumentando a capacidade de resposta. Essa abordagem supera métodos tradicionais como e-mail ou SMS, que são mais lentos e menos eficientes. Com o bot, eventos recorrentes podem ser identificados antes de se transformarem em incidentes maiores, e a operação se torna mais ágil, colaborativa e orientada a dados.

2.5.4 Integração com o IXC

O IXC é o sistema amplamente utilizado por provedores de internet para gestão de clientes, contratos, equipamentos e VLANs. Integrar o Zabbix a esse sistema permite que o monitoramento seja complementado por informações administrativas e de cadastro, aproximando o universo técnico da gestão operacional. Com essa integração, é possível visualizar quantos clientes estão conectados por POP, quais VLANs estão em uso, o status financeiro dos assinantes, além de obter metadados de equipamentos instalados. Essa combinação torna o monitoramento mais inteligente e contextualizado, proporcionando tomadas de decisão mais precisas.

2..5.5 Importância da Padronização em POPs

A padronização é fundamental para garantir que todos os POPs operem sob um mesmo conjunto de regras, métricas, dashboards e triggers. Quando cada POP funciona como uma "ilha", com padrões distintos de configuração, aumentam as chances de incidentes não serem detectados, além de dificultar a triagem e a correção de falhas. Ao padronizar o monitoramento, o provedor reduz erros humanos, acelera o diagnóstico, melhora o treinamento da equipe e aumenta sua maturidade operacional. Dessa forma, a rede se torna mais previsível, escalável e eficiente.

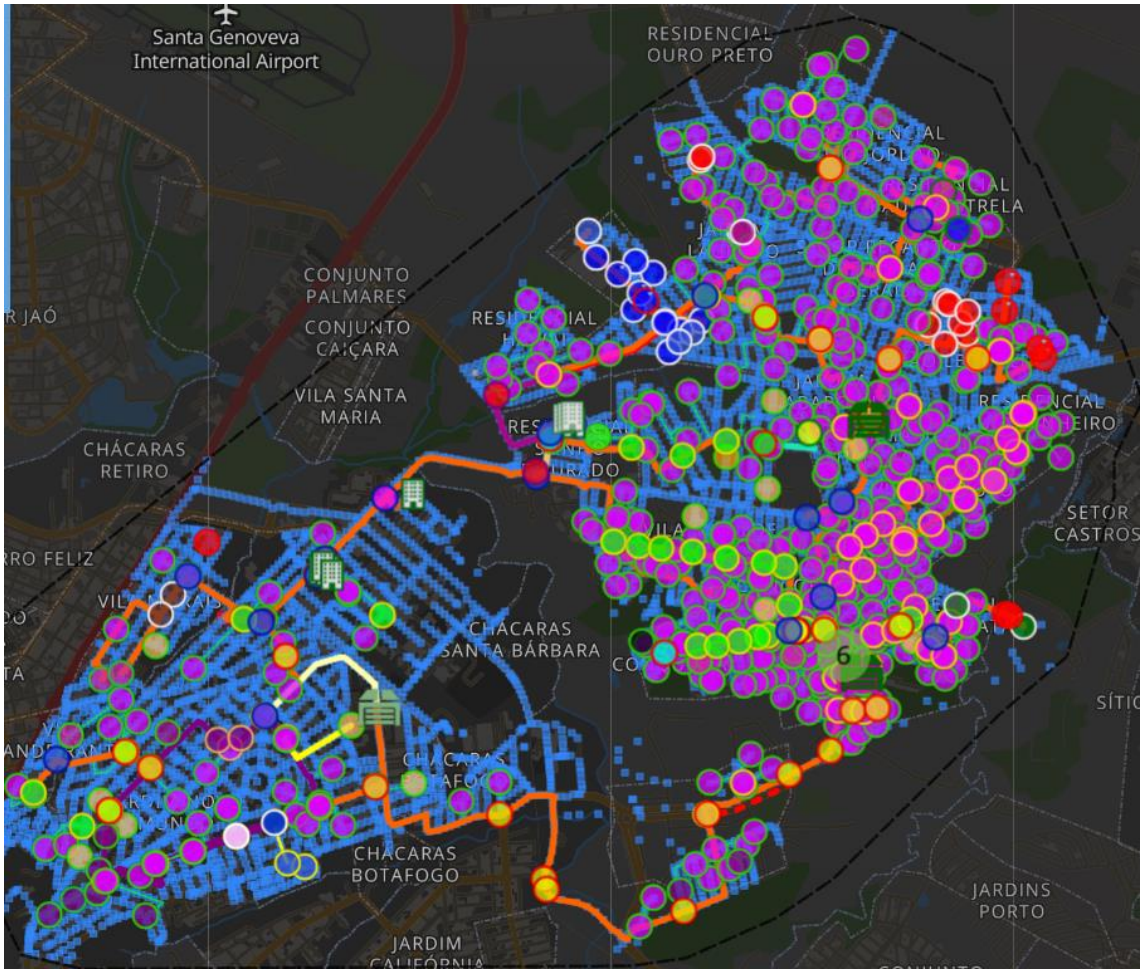
2.6 Conclusão dos Fundamentos

Todos esses conceitos fornecem a base técnica necessária para compreender a proposta desenvolvida neste trabalho. A partir deles, torna-se possível entender como cada componente — desde os protocolos de comunicação, passando pela infraestrutura óptica, até as ferramentas de coleta e visualização — contribui para formar um ecossistema de monitoramento realmente eficiente. É sobre esse alicerce conceitual que se estrutura a solução proposta, que integra Zabbix, Grafana, Telegram e IXC em um modelo unificado de monitoramento contínuo, padronizado e altamente automatizado. Ao consolidar esses elementos em uma arquitetura coerente, o provedor passa a obter maior visibilidade operacional, capacidade de identificar anomalias em tempo real e previsibilidade na gestão de incidentes, transformando o monitoramento em um processo estratégico para a estabilidade e evolução da rede.

3.ESTUDO DE CASO E ANÁLISE DO AMBIENTE

Este capítulo apresenta o ambiente analisado e descreve as etapas práticas realizadas para desenvolver o modelo de monitoramento contínuo com Zabbix. O estudo de caso foi conduzido em um provedor de internet real, considerando sua rotina operacional, os equipamentos utilizados, a estrutura de rede e os principais desafios enfrentados pela equipe técnica. A partir dessa vivência, foram identificados os pontos críticos da infraestrutura e definidos os elementos necessários para criar uma solução de monitoramento mais completa, padronizada e automatizada.

Figura 1 – Mapa da rede Óptica



Fonte – própria

3.1 Descrição Geral da Rede

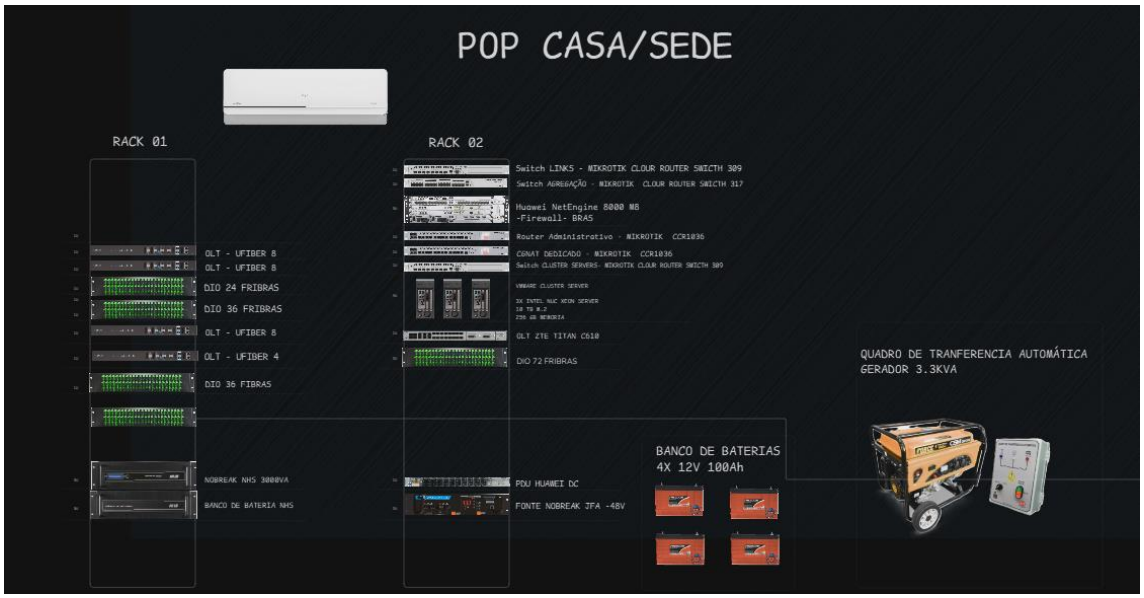
A figura representa uma visão georreferenciada da rede óptica do provedor, exibindo toda a distribuição de infraestrutura sobre o mapa da cidade. É possível observar a organização dos elementos principais do backbone e da rede de acesso, com destaque para:

- **Anéis e rotas de fibra (linhas laranjas)** que interligam bairros e garantem redundância entre POPs.
- **Caixas de terminação óptica – CTOs (círculos coloridos)** distribuídas em alta densidade na área atendida, cada uma servindo como ponto de derivação para múltiplos clientes.
- **Rede de distribuição (linhas azuis)** indicando o cabeamento que conecta CTOs, splitters e demais elementos ópticos.
- **Elementos de infraestrutura central (ícones de prédios)** que representam POPs, concentradores ou locais onde estão OLTs, switches de agregação e equipamentos de núcleo.
- **Marcadores coloridos variados**, que representam diferentes estados, grupos ou classificações das CTOs e clientes — usados internamente para indicar status operacional, ocupação, tecnologia, capacidade ou segmentação.

A visualização demonstra uma rede extensa, segmentada por bairros, com forte presença de GPON e ramificações de fibra que alimentam centenas de pontos ópticos. Observa-se também que a rede está distribuída de forma planejada, seguindo vias principais e secundárias, garantindo cobertura completa da região atendida.

3.2 POP CASA/SEDE

Figura 2 – Infraestrutura da POP



Fonte – própria

3.2.1 Descrição da POP Casa/Sede

A POP Casa/Sede representa um dos pontos de presença centrais da infraestrutura do provedor e concentra os principais equipamentos responsáveis pelo roteamento,

autenticação, distribuição óptica e operação administrativa da rede. Sua configuração foi desenvolvida para garantir alta disponibilidade, redundância e capacidade de atender simultaneamente a diferentes setores da cidade. A figura apresentada representa a organização física dos racks, a distribuição dos equipamentos e os sistemas de energia que suportam a operação.

3.2.2 Rack 01 – Infraestrutura Óptica e Equipamentos de Acesso

O primeiro rack é dedicado à camada de acesso da rede, concentrando as OLTs utilizadas para atendimento GPON e os distribuidores internos de fibra. As OLTs instaladas — organizadas em múltiplos módulos — desempenham o papel de interligar as portas PON às diversas CTOs distribuídas na área de cobertura do provedor. Associados a elas, os DIOs de 24 e 36 fibras estruturam a organização e acomodação dos cabos ópticos, facilitando manutenções, ampliações e garantindo padronização física no atendimento.

Na base do rack encontra-se o conjunto responsável por manter a continuidade da operação em eventuais falhas de energia. O nobreak, associado ao banco de baterias, fornece autonomia suficiente para que a rede GPON permaneça ativa durante interrupções na rede elétrica, evitando quedas massivas de assinantes.

3.2.3 Rack 02 – Núcleo da Rede, Roteamento e Servidores

O segundo rack concentra os elementos mais críticos do ponto de presença, incluindo equipamentos de núcleo, switches de agregação, roteadores e servidores. Os switches instalados realizam a agregação de tráfego entre as OLTs, servidores e dispositivos de borda, compondo a camada intermediária da infraestrutura.

A função de roteamento e autenticação é desempenhada pelos equipamentos de núcleo (core), que operam como BRAS, gateways de borda e concentradores de sessões PPPoE. Esses dispositivos também são responsáveis pelo processamento de rotas externas e internas, garantindo estabilidade no tráfego do provedor e integridade na comunicação com operadoras e PTTs.

Complementarmente, o rack abriga os equipamentos utilizados para o processamento administrativo e serviços internos, distribuídos em um cluster de servidores. Esses servidores suportam sistemas essenciais, como plataformas de monitoramento, bancos de dados, gerenciamento interno e aplicações corporativas, desempenhando papel fundamental na operação diária do provedor.

Também se encontra nesse rack outra OLT de maior capacidade, acompanhada de um DIO de 72 fibras, que atende setores de maior densidade populacional e amplia a capacidade de atendimento da rede de acesso.

3.2.4 Infraestrutura de Energia e Continuidade Operacional

A POP dispõe de uma estrutura de energia projetada para mitigar falhas e maximizar a disponibilidade dos serviços. O sistema é composto por PDUs dedicadas, fontes estabilizadas e um conjunto de baterias externas que fornecem autonomia estendida em caso de interrupções.

Para situações de queda prolongada de energia, o ponto de presença conta com um gerador de 3,3 kVA acoplado a um quadro de transferência automática, que entra em operação sempre que o nível de bateria atinge valores críticos. Essa arquitetura garante que os equipamentos essenciais permaneçam operantes mesmo durante longas interrupções da rede elétrica, preservando a continuidade dos serviços prestados aos assinantes.

3.2.5 Considerações Gerais

A POP Casa/Sede configura um ambiente robusto e estruturado, organizado em camadas funcionais que abrangem desde a distribuição óptica até o processamento central da rede. A disposição dos equipamentos, associada a um sistema de energia redundante, permite operação estável, resposta rápida a incidentes e capacidade de expansão. Essa infraestrutura representa um elemento estratégico para a operação do provedor, servindo como núcleo técnico e administrativo da rede.

3.3 Procedimentos Metodológicos

O desenvolvimento da solução de monitoramento proposta neste trabalho seguiu uma abordagem metodológica exploratória e aplicada, estruturada para garantir rigor na identificação, análise e integração das práticas de monitoramento contínuo utilizadas em provedores de internet. A metodologia foi organizada em etapas complementares que conectam técnicas formais de revisão da literatura, análise de métricas reais de rede e modelagem de dashboards e automações, permitindo a construção de um modelo consistente, padronizado e alinhado às necessidades operacionais de ISPs.

A primeira etapa consistiu na realização de um Mapeamento da Literatura, conduzido por meio de buscas nas bases IEEE Xplore, Scopus e Google Scholar, seguindo um protocolo de pesquisa previamente definido. Esse processo teve como objetivo identificar abordagens, desafios e boas práticas relacionadas ao monitoramento de redes, à automação de alertas, à coleta de métricas e às aplicações do Zabbix em ambientes de telecomunicações. Os resultados forneceram a base conceitual que orientou tanto a definição das métricas essenciais quanto os critérios utilizados para padronização e integração dos dashboards.

Em seguida, foi realizada uma análise técnica das principais métricas e parâmetros operacionais presentes em soluções reais de monitoramento de provedores. Essa etapa envolveu a observação direta do ambiente estudado, o levantamento de incidentes

recorrentes, o estudo de tráfego, potência óptica, sessões PPPoE, estabilidade BGP, ocupação de pools CGNAT e desempenho de enlaces. Essa análise serviu como insumo para selecionar as métricas realmente relevantes para o contexto do ISP, evitando coletas desnecessárias e priorizando itens que contribuem diretamente para a detecção precoce de falhas.

A etapa seguinte consistiu na classificação das práticas identificadas, organizando-as em categorias temáticas como desempenho, disponibilidade, estabilidade, segurança operacional e escalabilidade. Essa categorização permitiu criar um modelo de monitoramento mais claro e navegável, facilitando a definição dos painéis e das automações necessárias para suporte à equipe técnica.

3.3.1 Mapeamento da Literatura

O Mapeamento da Literatura constituiu a etapa inicial e fundamental para a consolidação da base teórica do modelo de monitoramento contínuo com Zabbix. O estudo foi conduzido utilizando bases como IEEE Xplore, Scopus e Google Scholar, sob o tema "Monitoramento Contínuo de Redes: Desenvolvimento de uma Solução Automatizada com Zabbix", com o seguinte objetivo geral:

"Busca-se aprimorar a gestão da infraestrutura de rede por meio de um monitoramento contínuo e automatizado, promovendo maior visibilidade dos ativos de rede e possibilitando a detecção ágil de falhas e anomalias, o que contribui diretamente para a redução do tempo de resposta a incidentes e para a manutenção da disponibilidade dos serviços."

Foi criado um protocolo simples e bem-organizado, definindo o que seria buscado na literatura: quais perguntas precisávamos responder, quais tipos de estudos seriam incluídos ou descartados, quais palavras-chave usar e em quais bases pesquisar. As buscas foram feitas principalmente no **IEEE Xplore**, **Scopus** e **Google Scholar**, permitindo reunir materiais realmente relevantes para o tema.

Esse processo deixou claro que ainda existem várias lacunas nas soluções de monitoramento já estudadas. A maioria dos trabalhos não apresenta um padrão claro de organização de dashboards, não integra bem ferramentas diferentes e quase nunca traz automações que realmente facilitem a vida da equipe técnica. Também foi possível perceber que muitos estudos tratam o monitoramento de forma muito isolada, sem relacionar métricas, alertas e ações práticas, o que dificulta aplicar essas ideias diretamente no dia a dia de um provedor.

Objetivo Específico:

Analisar o estado da arte das práticas e ferramentas de monitoramento contínuo de redes, mapeando metodologias, métricas essenciais, abordagens de automação com Zabbix, desafios enfrentados por provedores e lacunas ainda existentes na literatura.

PICOC	
Elementos	Descrição
População:	Projetos que utilizam Zabbix e automatização em tempo real
Intervenção:	Métodos e Técnicas de Avaliação
Comparação:	Matéria relacionada ao controle e à análise exploratória
Resultado:	Visão abrangente sobre a aplicação de monitoramento de redes automatizado
Contexto:	Aplicação para a área de redes

Tabela 1 - Estrutura PICOC utilizada para definição das questões de pesquisa

Questões de Pesquisa:

1. Quais métodos são usados para detecção de falhas?
2. Quais são os principais desafios e dificuldades encontrados durante a implementação?
3. Quais métodos de avaliação foram aplicados para avaliar os resultados obtidos?
4. Quais são os requisitos de rede para operar o Zabbix?
5. Quais ferramentas são compatíveis ou integráveis com o Zabbix?

String de Busca:

- V1: ("Monitoring" OR "Control" OR "Supervision" OR "Network Management" OR "Fault Detection")

AND

- V2: ("Network Infrastructure" OR "Computer Networks" OR "IT Infrastructure" OR "Communication Systems")

AND

- V3: ("Zabbix" OR "Open-source monitoring tools")

Bases de Dados:

- IEEE Xplore
- Google Scholar
- Scopus

3.3.2 Levantamento dos Pontos Críticos da Rede

A primeira etapa consistiu em entender como a rede do provedor funciona na prática: quais são os equipamentos essenciais, onde ocorrem os principais incidentes e quais métricas são realmente importantes para a operação diária. Foram analisados BRAS, sessões PPPoE, enlaces ópticos, rotas BGP, CGNAT, switches de agregação, OLTs e POPs distribuídos.

Esse levantamento permitiu identificar gargalos, quedas recorrentes, instabilidades e pontos da rede que exigiam monitoramento mais preciso. Foi nessa fase que surgiram os elementos prioritários da solução, como monitoramento de VLANs, potência óptica, uso de links e estabilidade de sessões PPPoE.

3.3.3 Construção de Templates Padronizados no Zabbix

Com os pontos críticos mapeados, iniciou-se a padronização do monitoramento. Foram criados templates específicos para BRAS, roteadores, OLTs, switches e enlaces ópticos. Esses templates continham:

- itens SNMP padronizados,
- triggers ajustadas,
- macros para adaptação entre equipamentos,
- regras LLD para descoberta automática,
- organização de métricas por categoria (tráfego, CPU, potência, PPPoE).

A padronização eliminou configurações manuais, reduziu erros e garantiu uniformidade entre os POPs.

3.3.4 Implementação de Triggers Inteligentes e Scripts Automatizados

Nessa fase, o Zabbix começou a ganhar "inteligência". Foram implementadas triggers que levam em conta histórico, tendência e severidade. O objetivo foi reduzir falsos positivos e alertas irrelevantes.

Também foram criados scripts que automatizam ações como:

- coleta de informações adicionais,
- formatação de alertas,
- envio de dados complementares ao Telegram,
- validações rápidas que antes eram feitas manualmente.

Isso trouxe mais precisão aos alertas e diminuiu o tempo de resposta dos técnicos.

3.3.5 Integração com Grafana e Criação dos Painéis Operacionais

Após consolidar os dados no Zabbix, os dashboards foram construídos no Grafana para facilitar a visualização. Os painéis foram organizados em categorias:

- BGP e tráfego de borda

- PPPoE e BRAS
- CGNAT e uso de pools
- Interfaces críticas e backbone
- GPON e potência óptica
- VLANs e distribuição de clientes

O Grafana trouxe clareza visual e facilitou análises rápidas durante incidentes.

3.3.6 Otimização do Bot no Telegram

A integração do Zabbix com o Telegram foi aprimorada para que os alertas chegassem de forma clara, organizada e com todas as informações necessárias para que a equipe técnica pudesse agir rapidamente. O formato das mensagens foi padronizado com base nas necessidades reais da operação e no comportamento dos incidentes analisados.

Na figura 11 apresentada, é possível observar como os alertas chegam ao grupo: cada mensagem segue um padrão visual e informativo que facilita a leitura e reduz o tempo de diagnóstico. As notificações incluem:

- O tipo de alerta e sua severidade, indicado por ícones visuais (❌ para problema e ✅ para resolução);
- O serviço afetado, como PPPoE, VLAN específica ou instabilidade em sessões;
- O equipamento envolvido, como o BRAS NE8000 e seu respectivo IP;
- A causa técnica que disparou o alerta, como ausência de clientes na VLAN ou queda em massa;
- O valor que acionou a trigger e o valor atual no momento da notificação;
- O horário exato em que o evento ocorreu, permitindo auditoria precisa;
- A duração total do incidente, quando o alerta é finalizado;
- Links diretos do Zabbix, que levam o técnico para a tela do problema ou do equipamento monitorado.

Essa padronização tornou os alertas muito mais úteis no dia a dia. A equipe não precisa mais abrir vários dashboards ou cruzar informações manualmente — tudo chega pronto, seguindo um padrão que facilita a identificação do que está acontecendo e a rapidez da resposta.

Além disso, o bot foi configurado para evitar mensagens repetitivas e reduzir ruídos operacionais, enviando apenas alertas realmente relevantes. Isso contribuiu para diminuir o tempo médio de resposta (MTTR) e deixou o processo de monitoramento mais fluido e confiável.

3.3.7 Trigger

Uma trigger no Zabbix é uma regra de detecção de problema. Ela funciona como uma condição lógica que o Zabbix avalia o tempo todo para saber se algo na rede está fora do normal.

Pense na trigger como um "sensor inteligente": se algum valor monitorado ultrapassar o limite definido, ela dispara um alerta.

Como funciona uma trigger?

O Zabbix coleta dados o tempo todo (CPU, tráfego, potência óptica, sessões PPPoE, BGP).
A trigger analisa esses dados com base em regras, como:

- "se a potência óptica for menor que –20 dBm"
- "se a interface usar mais de 90% da banda por 5 minutos"
- "se não houver clientes na VLAN"
- "se o ping passar de 100 ms"
- "se o equipamento parar de responder"

Quando a condição seja falha, o Zabbix dispara:

Quando a condição volta ao normal:

3.3.8 Integração dos DGOs

Os DGOs (Dashboards Gráficos Operacionais) foram integrados ao modelo como uma camada visual complementar. Eles exibem:

- mapas dos POPs,
- distribuição de clientes,
- status por região,
- ativos mais utilizados,
- visão geral do comportamento da rede.

Essa integração permitiu unir as informações numéricas do Zabbix com uma representação visual da topologia do provedor.

3.3.9 Testes, Validação e Análise Comparativa

Por fim, a solução foi testada no ambiente real do provedor. Foram avaliados:

- tempo de detecção de falhas,
- precisão dos alertas,
- estabilidade das sessões PPPoE,
- comportamento do BGP,
- uso de banda e potência óptica,
- MTTR (Mean Time to Repair).

A comparação entre o antes e o depois mostrou ganho significativo na visibilidade da rede, maior rapidez na identificação de incidentes e redução de erros operacionais.

3.4 Implementação e Teste da Solução de Monitoramento

A implementação da solução de monitoramento foi estruturada para integrar diferentes ferramentas já utilizadas pelo provedor, unificando dados de rede, métricas operacionais e informações extraídas diretamente do sistema de gestão IXC. Diferente do desenvolvimento tradicional de software, este projeto não consistiu na criação de um sistema do zero, mas sim na configuração, integração e evolução de um ecossistema composto por Zabbix, Grafana, Telegram Bot, DGOs e consultas ao banco de dados do IXC.

A solução foi implementada considerando as características específicas do provedor e os problemas recorrentes observados no ambiente real, como instabilidade em sessões PPPoE, saturação de CGNAT, divergência de cadastro de clientes e falta de padrão nos dashboards. Para garantir uma implementação eficiente e escalável, as ferramentas foram organizadas em camadas, cada uma com responsabilidades específicas:Java: Linguagem de programação orientada a objetos amplamente usada em aplicações corporativas por sua portabilidade e robustez (Oracle, 2025).

- **Zabbix Server:** É responsável por coletar métricas via SNMP, scripts e API, processar dados e acionar triggers.

  No caso da integração com o IXC, foram criados itens que consultam diretamente o banco de dados para extrair informações complementares, como número de clientes conectados por ONU/POP ou VLANs em uso.

- **Grafana:** Além de consumir dados do Zabbix, o Grafana também pode ler consultas SQL diretamente do banco do IXC, permitindo criar painéis híbridos.

  Essa camada desempenha um papel equivalente ao “frontend” de um sistema tradicional.

- **IXC – Banco de Dados:** O IXC armazena informações comerciais e operacionais do provedor — como clientes, contratos, planos, OLTs cadastradas e vínculos com setoriais.

- **API IXC:** Foram criados scripts e consultas SQL para extrair dados do IXC e enviar para o Zabbix, automatizando processos.

- **SNMP, ICMP e Coletas de Rede:** Continuam sendo responsáveis pelas métricas técnicas.

- **Telegram Bot:** Usado para enviar alertas automáticos.

- **DGOs – Dashboards Gráficos Operacionais:** Fornecem visão rápida e organizada por POP, usando dados combinados do IXC + Zabbix.

3.4.1 Teste da Solução de Monitoramento

A etapa de testes tem papel essencial na garantia de qualidade de qualquer solução tecnológica, pois verifica se o sistema funciona conforme o esperado e atende às

necessidades do ambiente operacional. Embora este trabalho não envolva a construção de um software tradicional, os princípios de teste se aplicam diretamente à solução de monitoramento proposta, assegurando que o comportamento do sistema seja consistente, confiável e adequado ao uso diário.

Segundo Pressman e Maxim (2016), os testes têm como objetivo principal identificar falhas, validar comportamentos e garantir que o sistema esteja alinhado às necessidades dos usuários.

No contexto deste projeto — que também se caracteriza como um **relato de experiência** no ambiente real de um provedor — os testes são entendidos como o conjunto de verificações necessárias para confirmar a integridade dos dados, a consistência dos dashboards, a precisão das métricas coletadas e a confiabilidade dos alertas de monitoramento. Em outras palavras, trata-se de definir **como o sistema deverá ser validado**, considerando os desafios observados diariamente na operação da rede.

Com base na experiência prática no provedor, os testes foram organizados em três categorias fundamentais:

3.4.2 Testes de Coleta e Integridade dos Dados

Nesta etapa são verificados todos os pontos que alimentam o monitoramento, garantindo que as informações coletadas representem fielmente o ambiente da rede. A partir da vivência no provedor, sabe-se que métricas incorretas podem gerar diagnósticos equivocados ou mascarar falhas importantes.

Os testes considerados essenciais incluem:

- verificação do retorno correto das coletas SNMP em switches, OLTs, BRAS e roteadores;
- conferência de leituras de potência óptica e utilização de interfaces;
- validação das consultas realizadas ao banco de dados do IXC, que fornecem informações administrativas importantes (clientes ativos, contratos, VLANs, vínculos com pops);
- análises de ping, latência e perda de pacotes para confirmar estabilidade de enlaces.

Essas verificações asseguram que o monitoramento reflita a realidade do provedor, reduzindo o risco de interpretações erradas.

3.4.3 Testes de Dashboards e Visualizações

A etapa de visualização é fundamental em qualquer solução de monitoramento. A partir da experiência cotidiana na operação, ficou evidente a importância de painéis claros e atualizados. Portanto, os testes desta categoria envolvem:

- comparação dos dados exibidos com valores coletados diretamente dos equipamentos;
- análise da atualização dos gráficos no Zabbix e no Grafana;
- verificação da organização dos dashboards por POP;

- confirmação de que os gráficos de BGP, PPPoE, CGNAT e fibra mostram valores consistentes;
- revisão da clareza visual, cores, padrões e disposição das informações.

Esses testes permitem validar se os dashboards realmente ajudam no trabalho diário da equipe técnica.

3.4.4 Testes de Alertas e Comportamento das Triggers

Alertas precisos são fundamentais para reduzir tempo de identificação e resposta a falhas. Com base na prática dentro do provedor, sabe-se que alertas mal configurados geram ruídos, enquanto alertas bem definidos aumentam a eficiência operacional.

Portanto, os testes previstos incluem:

- simulação de condições que acionem triggers (quedas de interface, instabilidade de BGP, variações de potência óptica etc.);
- verificação se o Telegram Bot envia notificações com informações corretas;
- confirmação de que os alertas possuem severidade adequada;
- análise para evitar alertas duplicados ou desnecessários;
- validação da lógica geral das triggers conforme definido nos requisitos.

3.4.5 Conclusão da Etapa de Testes

A etapa de testes, no contexto deste relato de experiência, consiste em documentar claramente os critérios necessários para validar a solução de monitoramento, assegurando que ela funcione de forma confiável ao ser implantada. Essa definição baseia-se na vivência diária dentro do provedor, observando como os técnicos utilizam os dados, quais métricas são mais críticas e quais verificações são indispensáveis para garantir estabilidade.

Dessa forma, os testes descritos fornecem um guia completo do que precisa ser verificado para que a solução de monitoramento atenda plenamente às demandas operacionais, refletindo não apenas teoria, mas a realidade prática observada no ambiente de trabalho.

3.4.6 Desafios Enfrentados pelo Provedor

Durante a vivência cotidiana na operação, foi possível observar que os desafios enfrentados por um provedor não estão apenas na parte técnica, mas também na forma como as informações são organizadas e utilizadas pela equipe. A falta de padronização e de visibilidade consolidada sobre os elementos da rede gera um conjunto de problemas que prejudica o atendimento, a identificação de falhas e o tempo de resposta.

Os principais desafios identificados foram:

- **Falta de padronização nos dashboards e POPs:** Cada POP possuía dashboards montados de maneiras diferentes, o que dificultava a identificação de padrões de comportamento da rede.
- **Ausência de integração entre Zabbix, Grafana e IXC:** Sem integração, dados importantes ficavam isolados VLANs, contratos e setoriais não apareciam no monitoramento.
- **Alertas inconsistentes:** triggers disparavam sem contexto;

O cenário observado revela que o provedor enfrentava dificuldades semelhantes às de muitos negócios que utilizam ferramentas sem padronização: perda de eficiência, falta de organização, falta de visibilidade e aumento do risco operacional.

3.4.7 Benefícios Esperados com a Implementação do Sistema

Diante dos desafios levantados, tornou-se evidente a necessidade de uma solução estruturada que unificasse o monitoramento, organizasse as informações e tornasse o diagnóstico mais rápido e eficiente. A solução proposta — envolvendo Zabbix, Grafana, integração com o banco de dados do IXC e padronização dos POPs — busca atender exatamente a essa demanda.

- **Padronização dos dashboards:** Com a organização visual e estrutural.
- **Visibilidade completa do ambiente:** A unificação dos dados traz relação entre clientes ativos e conectados.
- **Redução do tempo de diagnóstico:** Com dados organizados são identificadas as falhas ópticas rapidamente.
- **Automação de alertas mais precisos:** Alertas inteligentes priorizam eventos realmente críticos.

4. SOLUÇÃO PROPOSTA

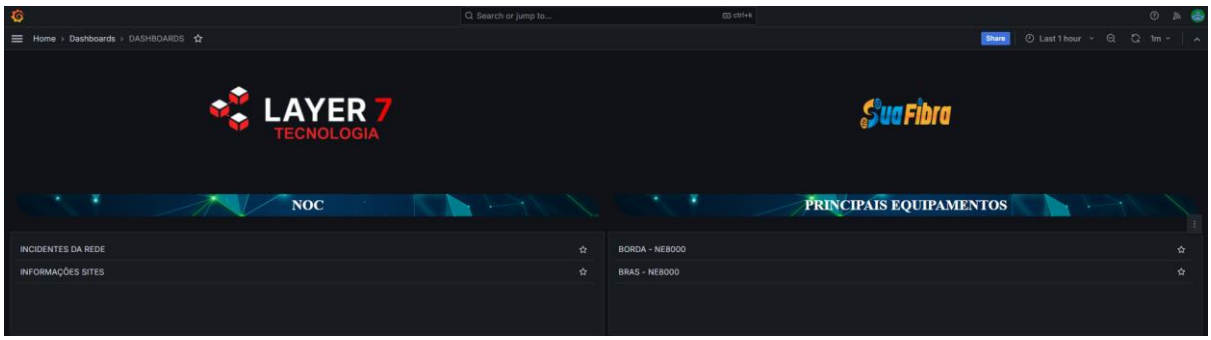
Este capítulo apresenta a solução proposta para melhorar e padronizar o monitoramento da rede do provedor. A ideia foi construída a partir do estudo de caso, das necessidades observadas no dia a dia e da experiência prática dentro da operação. Aqui são detalhados como as métricas serão organizadas, como os dashboards devem ser estruturados, de que forma os dados do IXC serão integrados e como os protótipos dos painéis vão orientar a implantação da solução.

4.1 Projeto Visual dos Dashboards

O projeto visual dos dashboards consistiu em desenvolver representações organizadas das telas que integrarão a solução de monitoramento. Esses projetos cumprem a função de validar o layout, priorização de métricas e estrutura geral das informações. A construção foi guiada pelos requisitos coletados e pela experiência prática na operação do provedor, facilitando a visualização antecipada de como os dados serão apresentados.

4.1.1 Tela Inicial

Figura 3- Tela inicial.



Fonte: Própria

Essa tela apresenta o “painel principal” do sistema de monitoramento. É o primeiro lugar que qualquer técnico ou analista vê quando abre o Grafana, servindo como uma espécie de portal central para os dashboards mais importantes do provedor.

Logo no topo aparecem os logotipos da empresa e do provedor, reforçando a identidade visual e organizando o ambiente do NOC (Network Operations Center). A ideia dessa home é deixar o acesso rápido e intuitivo, sem que a equipe precise ficar navegando por menus ou procurando dashboards no meio de dezenas de pastas.

4.1.1.1 A tela é dividida em duas grandes seções principais

NOC — Incidentes e Informações Gerais

No lado esquerdo fica a parte destinada aos incidentes da rede e às informações dos sites/POPs.
Aqui o técnico consegue visualizar rapidamente:

- alertas em aberto,
- status dos POPs,
- indisponibilidades recentes,
- eventos pendentes,
- situações que precisam de intervenção imediata.

Essa área funciona como uma espécie de "caixa de entrada" da rede. Tudo o que está errado aparece aqui.

4.1.1.2 Principais Equipamentos

No lado direito estão os atalhos para os dashboards dos equipamentos críticos, como:

- Borda — NE8000
- BRAS — NE8000

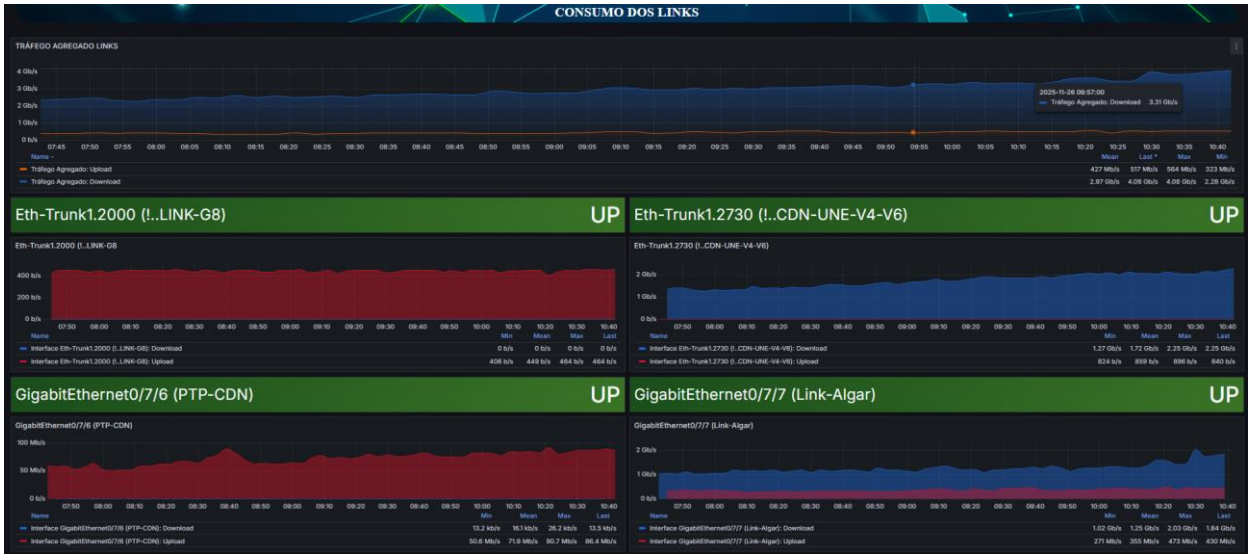
4.1.1.3 Esses equipamentos normalmente são os "corações" do provedor, pois concentram

- sessões PPPoE,
- BGP,
- roteamento principal,
- tráfego de borda,
- autenticação dos clientes.

Ter atalhos diretos torna a operação muito mais rápida. O técnico consegue abrir o painel certo com um clique, sem precisar navegar em várias páginas.

4.2 Dashboard do Consumo dos Links

Figura 4 - Consumo dos Links.



Fonte: Própria

O objetivo é identificar rapidamente o volume total de dados que entra e sai da rede.

Isso ajuda a perceber horários de pico, possíveis saturações e comportamentos anormais.

4.2.1 Gráfico superior — Tráfego Agregado dos Links

A primeira parte do painel apresenta o tráfego total da rede, somando todos os enlaces principais.
Esse gráfico mostra:

- Download (linha azul)
- Upload (linha laranja)

O objetivo é identificar rapidamente o volume total de dados que entra e sai da rede.
Isso ajuda a perceber horários de pico, possíveis saturações e comportamentos anormais.

4.2.2 Blocos individuais — Status dos Links

Cada bloco abaixo do gráfico geral representa um link específico e contém:

✓ Nome do enlace (ex.: *Eth-Trunk1.2000 (I. LINK-G8)*)

Mostra qual equipamento ou rota está sendo monitorado.

✓ Status do link (“UP”)

Informa se a interface está ativa e operando normalmente.

✓ Indicadores mínimos, médios e máximos

Para cada link, o painel exibe valores como:

- Min → menor tráfego registrado
- Mean → média do período
- Max → maior tráfego
- Last → valor atual

Esses números ajudam a comparar o desempenho ao longo do tempo.

4.2.3 Este painel permite que o técnico

- visualize rapidamente a saúde dos principais links;
- identifique saturações antes que causem lentidão;
- compare tráfego entre diferentes operadoras e enlaces;
- entenda o comportamento diário da rede;
- tome decisões sobre upgrade e balanceamento;
- identifique quedas ou oscilações imediatamente.

4.3 Dashboard do Hardware Equipamento

Figura 5 - Hardware Equipamento.

Fonte: Própria

Este dashboard reúne os principais indicadores operacionais do roteador responsável pelas sessões BGP do provedor. Por concentrar boa parte das rotas de entrada e saída da rede, esse equipamento é um dos elementos mais críticos da infraestrutura. O painel permite avaliar, de maneira rápida e integrada, se o roteador está funcionando com estabilidade ou se apresenta sinais de risco, como travamentos, quedas ou degradação do desempenho.

O BGP é o protocolo encarregado de realizar a troca de rotas entre sistemas autônomos. Cada vez que um pacote avança de um roteador para outro, esse processo é chamado de *hop*. Quanto menor o número de *hops*, mais eficiente é o caminho percorrido até o destino. Por isso, estabelecer sessões BGP com peers adequados pode melhorar significativamente a latência, a redundância e a qualidade geral da navegação oferecida aos clientes.

4.3.1 Status Geral do BGP

Figura 6 – Histórico BGP

Fonte - Propria.

No canto superior esquerdo, o painel apresenta o status consolidado das sessões BGP.

Quando o indicador aparece como **online**, significa que todas as sessões configuradas estão ativas e operando corretamente.

Qualquer queda ou instabilidade é refletida nessa área, acionando alertas imediatos.

Essa visualização é essencial, pois uma sessão BGP inapta pode comprometer o recebimento de prefixos e gerar perda de rotas, afetando diretamente o tráfego dos clientes.

4.3.2 Peers do BGP

Os *peers* são os roteadores vizinhos com os quais o provedor mantém sessões BGP. São esses equipamentos que trocam rotas, anunciam prefixos e permitem que as redes se comuniquem entre si. Um peer pode representar:

- um provedor de trânsito;
- um ponto de troca de tráfego (PTT/IX);
- uma CDN;
- uma conexão privada com outra rede (PNI).

Além de fornecer rotas, um bom peer pode **reduzir a quantidade de hops até o destino**, melhorando o tempo de resposta e a eficiência do tráfego.

4.3.3 Latência do BGP

Figura 7 – Histórico de Latência BGP

Fonte – Própria

O painel apresenta também a latência entre o roteador e seus peers. No exemplo analisado, o valor de **0,195 ms** indica excelente estabilidade e uma conexão extremamente eficiente.

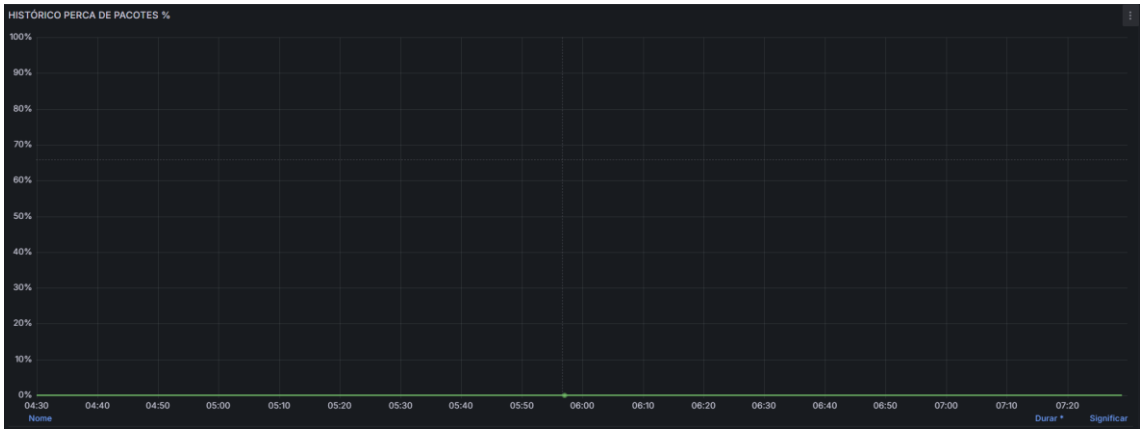
Elevações anormais na latência costumam indicar:

- congestionamento no caminho;
- problemas de rota;
- oscilação na rede interna;
- sobrecarga no próprio roteador.

Monitorar esse indicador é essencial para diagnosticar falhas que ainda não impactaram os usuários, mas que já sinalizam desgaste.

4.3.4 Perda de Pacotes

Figura 8 – Histórico de Perda de Pacote



Fonte - Própria

O dashboard exibe também o percentual de perda de pacotes das sessões BGP. No caso analisado, o índice é **0%**, o que representa um cenário ideal.

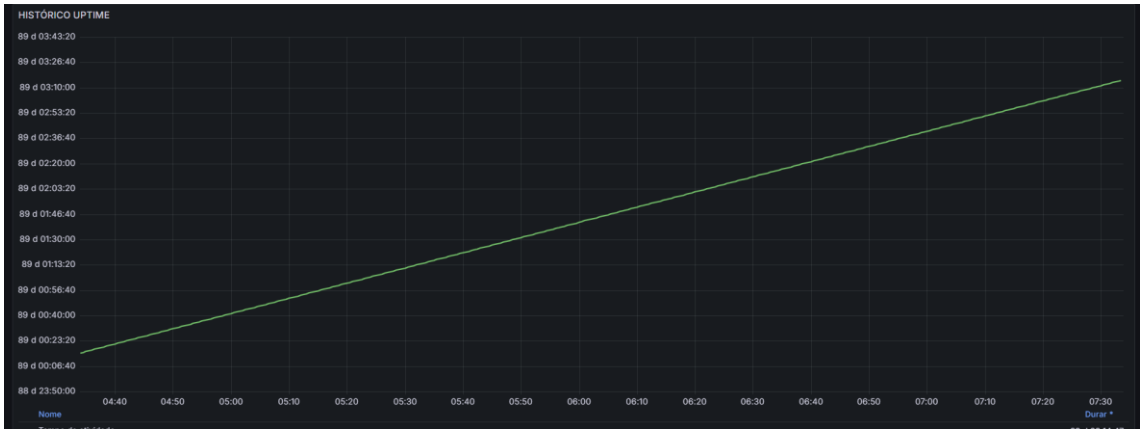
Qualquer taxa de perda é preocupante, pois pode afetar diretamente:

- a estabilidade do BGP;
- o tempo de resposta;
- processos PPPoE;
- a navegação dos clientes.

Perda de pacotes nesse ponto da rede tende a repercutir em toda a operação.

4.3.5 Uptime do Equipamento

Figura 9- Histórico UPtime



Fonte - Própria

Outro indicador importante é o uptime — o tempo que o roteador permanece ligado sem reinicializações.

O valor de **84 dias, 6 horas e 25 minutos** indica um equipamento estável, sem quedas recentes.

Uptimes muito baixos podem significar:

- falhas físicas;
- travamentos;
- problemas elétricos;
- reinicializações indevidas

4.3.6 Status do SNMP

Figura 10 - HISTÓRICO STATUS SNMP

Fonte - Própria

O status SNMP informa se o Zabbix está coletando dados trafegados pelo roteador. A indicação monitorando confirma que as métricas estão sendo recebidas corretamente. Caso apareça “Sem coleta SNMP”, isso significa que o roteador está ativo, porém sem enviar dados — o que compromete a capacidade de análise e correlação de eventos.

4.3.7 Indicadores de Hardware

Na parte inferior do painel, encontram-se métricas diretamente relacionadas ao hardware do equipamento — essenciais para prever falhas físicas e evitar interrupções inesperadas.

4.3.8 Uso de CPU

A CPU aparece com **46% de utilização**, valor adequado para a função desempenhada.
Utilização constante acima de 80% pode causar:

- travamentos;
- lentidão no processamento de rotas;

- flaps de BGP;
- falhas no PPPoE.

4.3.9 Histórico de CPU

Permite identificar picos anormais ao longo do dia e períodos com maior carga de processamento.

4.3.10 Voltagem do Equipamento

A leitura de **760 V** corresponde à tensão interna do equipamento, comum em roteadores de grande porte com fontes high-power.
Variações acentuadas podem indicar:

- falha na fonte;
- instabilidade elétrica;
- defeito no nobreak;
- risco de desligamento.

4.3.11 Uso de Memória

A memória aparece com **60% de uso**, dentro de limites normais. Valores próximos de 90% podem gerar travamentos ou reinicializações automáticas.

4.3.12 Temperatura do Equipamento

Com **46 °C**, a temperatura do hardware está dentro da faixa ideal. Acima de 65–70 °C, o risco de falhas aumenta consideravelmente.

4.3.13 Status da FAN

O painel exibe **FAN OK**, indicando que as ventoinhas estão funcionando normalmente.
A velocidade em 35% demonstra funcionamento estável.

4.3.14 Status das Fontes

As fontes **#1** e **#3** aparecem como **online**, garantindo redundância. A perda de uma das fontes não impactaria o funcionamento, desde que outra esteja ativa — fator crucial para evitar quedas durante falhas elétricas.

4.4 Dashboard de BGP

Figura 11 – Sessões BGP IPv4 e IPv6

Fonte: Própria

Este dashboard foi projetado para monitorar o estado das sessões BGP do provedor, tanto em IPv4 quanto em IPv6. Como o BGP é o protocolo responsável por anunciar e receber rotas da internet, qualquer oscilação nessas sessões afeta diretamente a navegação dos clientes e a disponibilidade do serviço. Por esse motivo, o painel oferece uma visão objetiva e centralizada que auxilia o time técnico na identificação rápida de falhas, instabilidades e comportamentos inesperados no roteamento.

4.4.1 Status dos Peers IPv4

A primeira coluna do dashboard apresenta o estado das sessões BGP em IPv4. Cada peer é exibido com um indicador visual que reflete sua condição atual:

- **Verde (Estabilizado)** — a sessão está ativa e funcionando normalmente.
- **Vermelho (Down)** — a sessão caiu ou não está respondendo.
- **Amarelo/Azul (Conectado)** — a sessão está ativa, mas ainda não atingiu estabilidade completa.

No painel analisado, vemos diversos peers em estado estabilizado, como LINKIP-UNE-AQUARIUS, LINKIP-UNE-EUROBACKUP e CDN-UNE, enquanto outros, como TRÂNSITO-RD e CDN-RD, aparecem como Down. Essa diferenciação é fundamental para identificar rapidamente quais operadoras estão fornecendo rotas e quais estão indisponíveis.

4.4.2 Uptime dos Peers IPv4

A coluna seguinte indica o *uptime* de cada sessão — ou seja, há quanto tempo o peer permanece estável.

Exemplos observados incluem sessões com **21 dias de estabilidade**, indicando funcionamento contínuo e confiável, e sessões marcadas com **00:00:00**, que representam quedas recentes ou tentativas de conexão sem sucesso.

Essa informação permite identificar:

- instabilidades recorrentes;
- flutuação de rotas de operadoras;
- possíveis quedas físicas (fibra rompida, porta defeituosa);
- reinicialização de equipamentos;
- falhas pontuais na negociação da sessão.

Um uptime zerado é um sinal claro de que o peer não está funcionando como esperado.

4.4.3 Prefixos IPv4 Recebidos

A terceira coluna mostra o volume de prefixos recebidos por cada peer. Esse número representa a quantidade de rotas repassadas ao provedor.

Valores elevados — como **1.022.387 prefixos** — indicam que a sessão está operando normalmente e recebendo toda a tabela de rotas do BGP.
Já valores **zerados** apontam para uma sessão inoperante ou para a ausência de anúncios por parte da operadora ou servidor remoto.

É importante destacar que **sem prefixos, a rota deixa de existir** para o provedor, o que resulta em falhas de acesso a determinados destinos.

4.4.4 Status dos Peers IPv6

A quarta coluna funciona de maneira semelhante, mas voltada para sessões BGP IPv6. Esse painel destaca um cenário comum em muitos ISPs: a coexistência de peers IPv4 estáveis com peers IPv6 indisponíveis ou parcialmente ativos.

Na imagem analisada, por exemplo:

- *TRANSITO-ALGAR-V6* aparece como **Down**,
- *LINKIP-UNE-AQUARIUS-V6* aparece como **conectado**,
- *LINKIP-UNE-EUROBACKUP-V6* está **estabilizado**.

A distinção entre IPv4 e IPv6 é essencial porque algumas operadoras fornecem suporte mais completo para IPv4, enquanto o IPv6 ainda está em ampliação ou transição gradual.

4.4.5 Uptime dos Peers IPv6

Assim como nas sessões IPv4, o uptime das sessões IPv6 mostra o tempo de estabilidade das conexões. Valores como **21 dias** reforçam que o peer está funcionando corretamente. Em contrapartida, sessões com **00:00:00** indicam problemas de estabelecimento, erros nas configurações de roteamento ou até bloqueio em firewalls intermediários.

Monitorar essa métrica ajuda a identificar falhas exclusivas do IPv6, que muitas vezes não aparecem no operacional do IPv4.

4.4.6 Prefixos IPv6 Recebidos

A última coluna apresenta a quantidade de prefixos IPv6 recebidos. Um exemplo positivo observado é o peer *LINKIP-UNE-EUROBACKUP-V6*, fornecendo **230.642 prefixos**, o que evidencia a operação normal da sessão.

Outros peers exibem **0 prefixos**, indicando sessões desconectadas ou sem anúncios — cenário comum na fase inicial de adoção de IPv6 ou em operadoras que ainda não distribuem rotas completas.

Manter prefixos IPv6 ativos é cada vez mais relevante devido ao esgotamento dos endereços IPv4 e à expansão do protocolo em nível mundial.

4.5 Dashboard dos Dados GBIC

Figura 12 – Dados GBIC

Fonte: Própria

Este dashboard reúne as principais informações relativas aos módulos ópticos (GBICs/SFPs) instalados nos equipamentos do provedor. Esses módulos têm papel fundamental na infraestrutura de rede, pois são responsáveis por converter o sinal elétrico em sinal óptico e vice-versa. Por isso, acompanhar seus parâmetros operacionais é essencial para garantir a estabilidade dos enlaces evitar problemas como perda de pacotes, quedas inesperadas ou degradação do desempenho.

O objetivo do painel é oferecer uma visão clara e centralizada das condições da fibra, exibindo valores de potência óptica recebida (RX), potência transmitida (TX), temperatura do módulo e a leitura interna do laser. Essas informações permitem identificar anomalias de forma antecipada, facilitando intervenções preventivas antes que algum link se torne instável.

4.5.1 Interfaces Monitoradas

A primeira seção do dashboard apresenta a lista de interfaces associadas aos módulos ópticos monitorados, como:

- **GigabitEthernet0/7/6 (PTP-CDN)**
- **GigabitEthernet0/7/7 (Link-Algar)**

Em geral, essas interfaces representam enlaces ponto a ponto (PtP), conexões com operadoras, interligações entre POPs ou links dedicados de CDN.
Manter essa identificação explícita é importante porque facilita a correlação entre o módulo monitorado e seu papel na rede. Assim, caso algum parâmetro esteja fora do esperado, o técnico sabe exatamente qual link deve ser inspecionado ou priorizado.

4.5.2 Sinal da Fibra – RX

O valor de **RX (Receive Power)** representa a potência óptica recebida pelo módulo. No painel apresentado, os valores são:

- **–6.93 dBm**
- **–7.18 dBm**

Esses números indicam níveis de potência excelentes para enlaces típicos em ISPs. A interpretação segue padrões amplamente utilizados na prática:

- Entre **–5 dBm e –15 dBm** → sinal considerado normal ou ótimo.
- Entre **–18 dBm e –22 dBm** → faixa de atenção, podendo indicar perda gradual ou sujeira no conector.
- Abaixo de **–24 dBm** → risco real de queda, especialmente em enlaces longos ou com múltiplas fusões.

No caso do dashboard analisado, os valores estão dentro de uma faixa segura, indicando que os enlaces não apresentam degradação significativa.

4.5.3 Sinal da Fibra – TX

A potência **TX (Transmit Power)** indica o nível de sinal óptico enviado pelo módulo. Os valores exibidos no painel incluem:

- **3.90 dBm**
- **–4.40 dBm**

A variação entre potências positivas e negativas é normal e depende do tipo de módulo, distância suportada e design óptico da porta:

- Módulos de longa distância (10–20 km) costumam operar com TX entre **+1 e +5 dBm**.
- Módulos de curta distância (até 2 km) operam entre **–1 e –5 dBm**.

Mais importante do que o número absoluto é saber se a potência TX está dentro da especificação do fabricante. Valores muito altos podem saturar o receptor equipamento remoto; valores muito baixos podem indicar defeito no laser ou atenuação excessiva.

4.5.4 Temperatura do Módulo Óptico

A temperatura é um dos parâmetros mais críticos para o bom funcionamento do GBIC. No dashboard analisado, os valores são:

- **38 °C**
- **42 °C**

Ambos são totalmente normais para módulos instalados em equipamentos que permanecem ligados 24/7.
Como referência:

- **20 °C a 55 °C** → faixa segura e esperada
- **55 °C a 70 °C** → faixa de atenção
- **> 70 °C** → risco de travamentos, erros de leitura, perdas de sinal e até queima do módulo

Monitorar essa métrica ajuda a prevenir falhas como microquedas, perda de rotas BGP e interrupção de enlaces que dependem do módulo.

4.5.5 Voltagem Interna do Laser (Leitura do Fotodiodo)

A última coluna do dashboard exibe a chamada "voltagem do laser", com valores como:

- **3.37 kV**
- **3.33 kV**

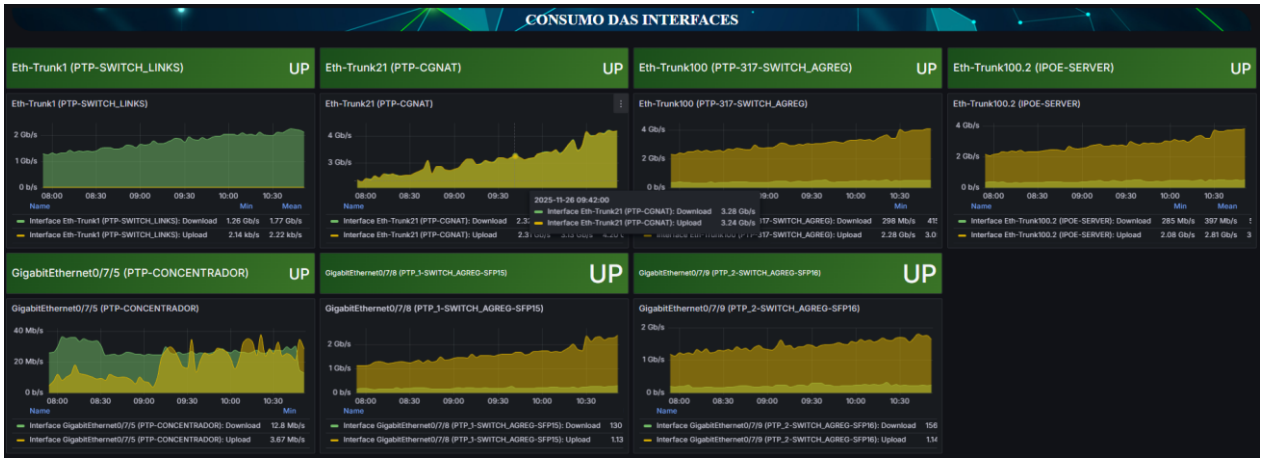
Apesar do uso da sigla "kV", esses valores **não correspondem a quilovolts reais**. Essa representação é apenas uma escala interna utilizada pelo firmware para expressar a intensidade luminosa medida pelo fotodiodo do módulo. Como cada fabricante utiliza um método próprio de conversão do sinal óptico em valor numérico, essa "voltagem" não tem relação com tensão elétrica real e não deve ser interpretada literalmente.

O importante é observar **variações bruscas**, que podem indicar:

- desgaste do laser,
- contaminação nos conectores,
- perda progressiva de potência,
- módulos próximos à falha.

4.6 Dashboard do Consumo das Interfaces

Figura 13 – Consumo das Interfaces



Fonte: Própria

Este dashboard apresenta uma visão consolidada do uso das principais interfaces de rede do provedor, permitindo acompanhar em tempo real o comportamento do tráfego nos enlaces que compõem o backbone e os POPs. Ele funciona como um indicador da "respiração" da rede ao longo do dia, ajudando a identificar rapidamente situações de saturação, padrões anormais ou tendências que possam comprometer o desempenho geral da infraestrutura.

Cada bloco do painel corresponde a uma interface relevante — como troncos LACP, enlaces ponto a ponto, portas de agregação ou ligações com servidores — e exibe a evolução do tráfego de upload e download. Essa visualização contínua é fundamental para compreender a dinâmica da rede, permitindo que o técnico antecipe problemas e intérprete variações de comportamento de forma clara e objetiva.

4.6.1 Eth-Trunk1 (PTP-SWITCH_LINKS)

Essa interface representa um tronco que interliga equipamentos centrais do provedor.

O gráfico mostra um crescimento gradual ao longo da manhã, com tráfego variando entre **1,2 Gb/s e 1,7 Gb/s**.

O upload permanece baixo — comportamento típico em redes assimétricas. Aqui, o principal objetivo é observar se o link está se aproximando do limite operacional para evitar gargalos futuros.

4.6.2 Eth-Trunk21 (PTP-CGNAT)

Um dos enlaces mais críticos da operação, pois transporta o tráfego processado pelo CGNAT.

O gráfico evidencia consumo acima de **3 Gb/s**, chegando próximo a **4 Gb/s**, com crescimento constante no período analisado.

Por transportar um grande volume de clientes simultaneamente, qualquer saturação nessa interface pode gerar:

- aumento de latência,
- perda de pacotes,
- reclamações de lentidão.

É uma interface que exige monitoramento contínuo.

4.6.3 Eth-Trunk100 (PTP-317-SWITCH_AGREG)

Outro tronco de agregação essencial para o backbone.

O download permanece entre **3 e 4 Gb/s**, com comportamento estável e sem variações abruptas.

O tráfego evolui de forma uniforme, indicando operação saudável e sem indícios de saturação ou falhas.

4.6.4 Eth-Trunk100.2 (IPOE-SERVER)

Interface diretamente ligada ao servidor PPPoE/BRAS.

Os gráficos mostram tráfego entre **2,5 Gb/s e 3,5 Gb/s**, com crescimento natural ao longo do dia e sem sinais de anomalia.

Qualquer saturação nessa porta afeta diretamente a autenticação e navegação dos clientes PPPoE, tornando-a um ponto crítico do painel.

4.6.5 GigabitEthernet0/7/5 (PTP-CONCENTRADOR)

Trata-se de uma interface responsável por conectar concentradores ou um POP específico.

O tráfego é baixo (entre **10 Mb/s e 40 Mb/s**) e apresenta oscilações leves, compatíveis com a operação local.

É uma interface tranquila, com ampla folga de banda.

4.6.6 GigabitEthernet0/7/9 (PTP_2-SWITCH_AGREG-SFP16)

Enlace interno que alimenta switches de agregação.

O tráfego varia entre **1 e 2 Gb/s**, com crescimento suave e consistente.

A ausência de picos bruscos ou quedas indica funcionamento estável.

Por alimentar equipamentos que distribuem conexões para diversos clientes, a

saturação dessa interface poderia comprometer toda a árvore de atendimento associada a ela.

4.6.7 Problemas Detectáveis pelo Consumo de Interfaces

O dashboard permite identificar diversos tipos de falhas que impactam diretamente o desempenho da rede. O principal deles é a saturação dos enlaces: quando o tráfego se aproxima do limite da interface, surgem efeitos como latência elevada, perda de pacotes e degradação perceptível pelos usuários.

Além disso, o painel facilita a detecção de gargalos internos causados por sobrecarga em links que interligam switches, agregadores, BRAS ou CGNAT — situações que podem gerar microquedas e instabilidades em regiões inteiras.

A análise gráfica também permite identificar:

- **picos abruptos de tráfego**, possivelmente associados a ataques DDoS, loops de rede ou flaps de roteamento;
- **quedas rápidas ou flutuações (flaps)**, que costumam indicar problemas em SFPs, conectores ópticos, fibra danificada ou renegociação de porta;
- **desbalanceamento entre enlaces**, quando um link opera muito acima dos demais devido a falhas em LACP, hashing ou políticas de roteamento.

Com essas informações em mãos, o técnico consegue agir de forma proativa, corrigindo falhas antes que se tornem incidentes de maior impacto.

4.7 Dashboard das Conexões PPPoE

Figura 14 – Conexões PPPoE

Fonte: Própria

Este dashboard mostra, de forma bem clara, como o BRAS está funcionando. Como ele é o equipamento que autêntica todas as conexões PPPoE, qualquer problema ali vira problema para todo mundo. O painel junta informações sobre a "saúde" do equipamento com a quantidade de clientes conectados em tempo real. Isso ajuda bastante a perceber instabilidades, quedas em massa, lentidão ou até sinais de que alguma peça do hardware pode estar falhando.

4.7.1 Perda de Pacotes e Latência

Ao lado, estão dois indicadores essenciais para avaliar a estabilidade geral do equipamento:

- **0% de perda de pacotes** — sinal de que todo o tráfego ICMP está sendo respondido corretamente.
- **0,20 ms de latência** — demonstra uma operação extremamente estável.

Alterações nesses valores normalmente antecedem problemas perceptíveis pelos usuários, como lentidão, falhas PPPoE ou erros de autenticação.

4.7.2 Uptime

O painel também mostra que o BRAS está em funcionamento contínuo há **84 dias**, sem reinicializações. Um uptime longo indica estabilidade, ausência de falhas críticas e um ambiente saudável. Caso o tempo de operação fosse baixo ou houvesse reinicializações frequentes, isso seria um forte indicativo de instabilidade ou problemas de hardware/software.

4.7.3 Status SNMP

O status do SNMP informa se o equipamento está efetivamente enviando métricas ao sistema de monitoramento.

- **Monitorando** → Coletas normais.
- **Sem coleta SNMP** → O equipamento está ativo, mas sem transmitir dados, o que compromete análises e correlações.

4.7.4 Indicadores Históricos

O dashboard apresenta também gráficos históricos essenciais:

- **Disponibilidade (ICMP)**: demonstra que o BRAS permaneceu 100% disponível no período analisado.
- **Histórico de perda de pacotes**: linha completamente zerada, indicando operação estável.
- **Histórico de latência**: pequenas oscilações naturais, sempre abaixo de 1 ms.

Esses históricos ajudam a identificar instabilidades que podem não aparecer visualmente em um único momento.

4.7.5 Condições de Hardware

Na parte inferior do painel estão os indicadores que representam a saúde física do equipamento:

- **CPU**: atualmente em 41%, um nível considerado excelente. Uso contínuo acima de 80% pode resultar em lentidão, queda de sessões ou falhas de autenticação.
- **Histórico de CPU**: permite verificar se ocorreram picos incomuns ao longo do tempo.
- **Temperatura**: com 46 °C, dentro do padrão de operação. A partir de 65 °C já se considera uma faixa de atenção.
- **Memória**: uso em 59%, dentro do limite seguro. Valores próximos de 90% podem causar travamentos e reinicializações automáticas.
- **Status das ventoinhas (FAN)**: exibe **FAN OK**, indicando que o sistema de resfriamento está funcionando adequadamente.
- **Status das fontes de energia**: Fonte #1 e Fonte #3 estão online, garantindo redundância energética — fundamental para evitar quedas por falha elétrica.

4.7.6 Conexões PPPoE

O painel também apresenta informações sobre os clientes atualmente conectados ao BRAS:

- **Total de clientes conectados**: 2.854 conexões ativas, número extraído diretamente do equipamento. Esse dado permite identificar quedas em massa, picos de demanda e variações ao longo do dia.
- **Clientes IPv4 conectados**: mesmo número — demonstrando que todos estão utilizando IPv4.
- **Clientes Dual-Stack (IPv4 + IPv6)**: 0 conexões, indicando que o provedor ainda não autêntica clientes utilizando IPv6 ou está em fase inicial de implantação.

4.7.7 Históricos de Clientes

Os gráficos exibem a evolução dos clientes conectados ao longo do tempo, permitindo identificar:

- quedas abruptas (indicando falhas ou quedas de energia),
- aumentos repentinos (recuperação de energia ou reconexões em massa),
- horários de maior pico de autenticação.

4.8 Dashboard do Total de VLAN por clientes

Figura 15 – Total de Clientes por VLAN

Fonte: Própria

Este dashboard apresenta um panorama abrangente da distribuição de clientes conectados em cada VLAN do provedor. Nas operações de ISP, cada VLAN costuma representar um bairro, região, POP ou setor específico da cidade, tornando essa visualização essencial para compreender a carga de usuários em diferentes partes da rede. Com esses dados, é possível identificar áreas mais demandadas, regiões estáveis e setores com pouca utilização, permitindo ao time técnico ter uma percepção clara do comportamento geral da rede.

Na parte superior do painel, cada bloco colorido indica a quantidade de clientes conectados em determinada VLAN. No exemplo analisado, observam-se valores como **1664 clientes na VLAN 801**, **497 na VLAN 802** e **689 na VLAN 811**, enquanto outras VLANs aparecem com números reduzidos ou próximos de zero. Essa representação direta possibilita a avaliação imediata da pressão exercida sobre cada segmento da rede e facilita o reconhecimento de padrões de uso por região.

4.8.1 Gráfico de Evolução dos Clientes (Linha)

O gráfico de linha, exibido no lado esquerdo, apresenta a evolução temporal dos clientes conectados em cada VLAN. As VLANs com maior número de usuários — como a 801 — tendem a permanecer nas posições superiores do gráfico, enquanto VLANs com menor quantidade de clientes, como a 802 e a 811, surgem em curvas mais baixas. VLANs sem clientes aparecem totalmente zeradas.

Essa visualização temporal é fundamental para detectar:

- quedas em massa de clientes;
- falhas em concentradores (BRAS/BNG);
- instabilidades em OLTs, switches de agregação ou enlaces PtP;
- problemas de autenticação PPPoE;
- padrões de uso conforme horários de pico.

Se uma VLAN, por exemplo, passa abruptamente de centenas de clientes para zero, isso indica um problema claro na infraestrutura daquela região — como uma falha de energia no POP, degradação óptica na OLT ou ruptura de fibra.

4.8.2 Gráfico de Proporção (Pizza)

O gráfico à direita, exibe a porcentagem de clientes conectados em cada VLAN em relação ao total de assinantes ativos. No exemplo visualizado:

- a **VLAN 801 concentra cerca de 58% dos clientes**,
- a **VLAN 811 aparece com 24%**,
- a **VLAN 802 representa 17%**,
- as demais apresentam participação mínima.

Esse tipo de análise facilita a identificação de regiões de alto consumo, auxilia no planejamento de expansão, permite o balanceamento de tráfego entre POPs e possibilita compreender o impacto potencial de falhas regionais. Quando uma única VLAN concentra mais de 60% dos clientes ativos, qualquer instabilidade naquela área tende a gerar um volume elevado de chamados e impacto significativo no atendimento.

4.8.3 Problemas que a Distribuição de Clientes por VLAN Pode Indicar

Além de apresentar o cenário de uso da rede, este dashboard permite identificar problemas operacionais críticos. Entre os principais, destacam-se:

4.8.4 Sobrecarga em POPs ou Concentradores

VLANs com muitos clientes podem indicar que a região está operando acima da capacidade planejada, causando latência elevada, perda de pacotes, saturação das portas de agregação e instabilidade no BRAS.

4.8.5 Gargalos na Infraestrutura Óptica

Grande concentração de clientes pode indicar sobrecarga em splitters, potência óptica insuficiente ou excesso de ONUs em uma mesma porta da OLT, resultando em microquedas ou degradação de desempenho.

4.8.6 Quedas em Massa (Mass Logout)

Quando uma VLAN despenca de centenas de clientes para zero, isso sugere falha grave, como ruptura de fibra, queda de OLT, problema elétrico no POP ou falha no BRAS.

4.8.7 Problemas de Autenticação PPPoE

Flutuações repetitivas no gráfico podem indicar falhas no RADIUS, loops de autenticação ou instabilidade no servidor PPPoE.

4.8.8 VLANs Subutilizadas

VLANs constantemente zeradas podem sinalizar portas desativadas, falhas de cadastro no IXC, problemas no provisionamento de ONUs ou falhas físicas em enlaces internos.

4.8.9 Desbalanceamento na Rede

Uma distribuição desigual, com grande concentração de clientes em poucas VLANs, pode gerar saturação localizada e reduzir a eficiência global da rede, exigindo redistribuição manual ou revisão das políticas de engenharia.

4.80.10 Impacto Direto na Qualidade do Serviço

Regiões mais carregadas tendem a apresentar maior quantidade de chamados, maior uso de CPU no BRAS, ocupação intensa de NAT e maior sensibilidade a quedas regionais.

4.8.11 Conclusão da Análise

A distribuição de clientes por VLAN é um dos indicadores mais importantes para a operação do provedor. Ela permite visualizar rapidamente o comportamento da rede, identificar falhas, compreender padrões regionais e antecipar problemas antes que afetem uma grande parcela dos usuários. O uso combinado de blocos numéricos, gráfico de linha e gráfico de pizza torna este painel uma ferramenta indispensável para tomada de decisões operacionais e planejamento de capacidade.

4.9 Dashboard Informação da Pool

Figura 16 – Informação da Pool

Fonte: Própria

Este dashboard apresenta uma visão detalhada do estado dos pools de IP utilizadas pelo provedor, incluindo faixas internas, pools públicos, pools específicos de autenticação e o bloco destinado ao CGNAT. Como a atribuição correta de endereços IP é essencial para o funcionamento do PPPoE e para a navegação dos clientes, esse painel se torna indispensável para monitorar o crescimento do consumo, prever esgotamentos e identificar conflitos que podem comprometer a operação.

A principal finalidade do dashboard é oferecer uma visão centralizada e imediata sobre a disponibilidade e o uso dos pools. Com isso, torna-se possível detectar rapidamente quando uma faixa de IP está prestes a atingir seu limite, quando há desperdício de recursos, quando existe subutilização ou quando aparecem conflitos que podem gerar erros de conexão. A visualização contínua desse painel evita que um pool "estoure" sem aviso, evento que costuma resultar em falhas de autenticação PPPoE, indisponibilidade de navegação e, em casos mais graves, quedas em massa de clientes.

4.9.1 Tamanho da Pool

A primeira coluna do dashboard indica o tamanho total de cada pool, ou seja, quantos endereços IP estão disponíveis para uso. No exemplo analisado, temos:

- **CGNAT – 100.81.16.0/20 → 4093 IPs**
- **Pool Pública → 61 IPs**
- **pool_aviso_atraso → 253 IPs**
- **pool_bloqueio → 509 IPs**
- **radius-server-suafibra → 245 IPs**
- **pool-privada-pppoe-teste → 1021 IPs**

Esses números representam a capacidade máxima de cada bloco e servem de referência para determinar se o dimensionamento está adequado à quantidade de clientes e ao tráfego demandado.

4.9.2 IPs em Uso

A segunda coluna mostra quantos IPs estão sendo utilizados naquele exato momento.
No exemplo, observa-se:

- **2.826 IPs do CGNAT em uso**
- Pools menores com uso momentaneamente zerado

Quando o consumo de IPs se aproxima da capacidade disponível, aumenta o risco de esgotamento do pool, o que resulta em falhas de navegação, erros de autenticação e instabilidade na abertura de sessões PPPoE. Por esse motivo, acompanhar esse número em tempo real é fundamental para evitar interrupções.

4.9.3 Percentual de Uso

A terceira coluna apresenta a porcentagem de ocupação de cada pool. No painel analisado:

- **CGNAT → 69% de uso**
- **Pool pública → 49%**
- Demais pools → 0%

A porcentagem é um dos indicadores mais importantes, pois mostra, de forma clara, a proximidade de saturação.
Quando um pool ultrapassa **80%**, já é considerado um nível crítico que exige atenção.
Acima de **90%**, o provedor corre risco real de:

- falta de endereços para novos clientes;
- falhas intermitentes de autenticação PPPoE;
- navegação instável;
- impossibilidade de renovar sessões PPPoE já existentes;
- aumento brusco de chamados no suporte.

Esse dashboard permite prever esgotamentos com antecedência e programar upgrades de maneira segura.

4.9.4 IPs em Conflito

A última coluna indica quantos endereços IP estão apresentando conflito.
No exemplo:

- **7 conflitos no CGNAT**
- **30 conflitos no pool público**
- Demais pools zerados

Conflitos de IP são eventos comuns em ambientes de grande escala e podem ocorrer por diversos motivos, como:

- clientes com roteadores mal configurados reutilizando IP antigo;
- redes internas sem NAT adequado;
- equipamentos com DHCP duplicado;
- falhas no CPE do cliente;
- bugs em firmware;
- conflitos na própria rede interna do ISP.

A detecção imediata desses conflitos facilita o trabalho do suporte e reduz o tempo de indisponibilidade percebida pelo usuário.

4.9.5 Problemas que o Consumo das Pools Pode Causar

Além de apresentar dados operacionais, o dashboard permite identificar problemas que, se não tratados, afetam diretamente a qualidade do serviço. Os principais são:

Esgotamento do Pool de IP

Quando um pool chega ao limite, o cliente não recebe IP. Isso resulta em:

- falha total de navegação;
- impossibilidade de autenticar PPPoE;
- desconexão de sessões já existentes;
- quedas em massa.

O esgotamento do CGNAT é particularmente crítico, pois afeta praticamente toda a base de clientes residenciais.

4.9.6 Lentidão e Instabilidade no CGNAT

Pools muito avançadas no uso podem gerar:

- lentidão ao estabelecer conexões;
- falhas em serviços que dependem de múltiplas portas;
- NAT insuficiente para novas conexões simultâneas;
- quedas de chamadas VoIP e interrupções em aplicativos.

CGNAT saturado costuma ser um dos problemas mais difíceis para o usuário identificar, mas um dos mais impactantes para o provedor.

4.9.7 Falhas de Autenticação PPPoE

Quando um pool pública ou privada está perto de esgotar:

- a cliente autêntica, mas não consegue navegar;
- sessões começam a abrir e fechar repetidamente;
- múltiplos usuários ficam sem internet.

Isso gera chamadas massivas no suporte.

4.9.8 Conflitos de IP

Conflitos podem causar:

- perda de conectividade;
- instabilidade intermitente;
- quedas de sessão;
- problemas específicos de clientes corporativos.

É um dos motivos mais comuns de “internet cai só em um equipamento”.

4.9.9 Problemas de Roteamento e Overlapping

Pools configuradas incorretamente podem conflitar com redes internas, gerando:

- rotas sobrepostas;
- perda de pacotes;
- lentidão em sites;
- falhas no CGNAT ou nos servidores PPPoE.

4.9.10 Dimensionamento inadequado

Se o provedor não acompanha o crescimento do consumo:

- a rede não escala;
- aumenta o risco de indisponibilidade;
- upgrades emergenciais se tornam mais caros.

4.9.11 Conclusão da Análise

O dashboard de pools de IP é uma das ferramentas mais importantes para garantir estabilidade operacional. Ele permite prever esgotamentos, identificar conflitos, dimensionar corretamente o crescimento da rede e evitar falhas críticas. Sem esse tipo de monitoramento, qualquer sobrecarga nos pools pode se transformar rapidamente em quedas generalizadas, afetando milhares de clientes simultaneamente.

4.10 Monitoramento de Latência para Redes Sociais e Jogos Online

Figura 17 – Latência nas Redes Sociais e Jogos Online

Fonte: Própria

Este dashboard foi desenvolvido para monitorar a latência dos principais serviços utilizados pelos clientes do provedor, com foco em **redes sociais** e **jogos online**. Esses dois grupos de aplicações representam boa parte do tráfego diário dos assinantes e estão diretamente relacionados à experiência de navegação, já que latência elevada é percebida imediatamente pelo usuário final como lentidão, travamento, delay ou instabilidade.

O painel oferece uma visão clara e comparativa do tempo de resposta para cada serviço monitorado, permitindo à equipe técnica identificar rapidamente anomalias, oscilações e queda na qualidade de conexão especialmente importante para jogos, onde alguns milissegundos fazem diferença.

4.10.1 Latência das Redes Sociais

Na parte superior do dashboard, cada bloco exibe a latência atual medida até os principais serviços:

- WhatsApp → 11.9 ms
- Instagram → 11.8 ms
- Facebook → 11.9 ms
- Twitter → 12.6 ms
- Discord → 12.1 ms
- TikTok → 12.1 ms
- YouTube → 21.6 ms
- Pinterest → 12.0 ms
- LinkedIn → 11.8 ms
- Skype → 12.0 ms

Esses valores mostram que, no momento analisado, quase todas as plataformas apresentam latência excelente, abaixo de 15 ms, exceto o YouTube, que aparece com tempo mais alto (21.6 ms), algo comum por conta da CDN e do volume de requisições.

Um painel como esse permite identificar rapidamente:

- Aumento repentino de latência em algum serviço específico;
- Possíveis falhas na rota até a CDN;
- Problemas regionais em plataformas populares;
- Instabilidades no provedor de trânsito.

4.10.2 Gráfico de Histórico (Redes Sociais)

O gráfico à direita mostra a evolução da latência ao longo do tempo. Ele ajuda a identificar:

- Oscilações;
- Picos súbitos;
- Períodos de degradação;
- Quedas de rota.

Como redes sociais têm tráfego intensivo, picos de latência podem indicar saturação do backbone ou instabilidade em operadoras upstream.

4.10.3 Proporção de Latência – Redes Sociais

A pizza ao lado exibe a participação média de cada plataforma no total de latência registrada no período.
No exemplo analisado:

- YouTube concentra maior média (18.27%)
- Twitter (10.62%)
- Discord (10.26%)
- TikTok (10.22%)
- Skype (10.21%)
- WhatsApp (10.08%)
- Instagram (10.03%)

Essa análise ajuda a entender **quais serviços são mais sensíveis à latência** e podem causar mais impacto no atendimento caso apresentem problemas.

4.10.4 Latência dos Jogos Online

A seção inferior do painel é dedicada exclusivamente aos jogos — um dos segmentos onde a latência é mais crítica.

Valores observados:

- CS:GO → 12.1 ms
- Fortnite → 12.2 ms
- PUBG → 11.9 ms
- Valorant → 15.3 ms
- League of Legends → 15.4 ms
- FIFA 23, GTA V, Steam e Xbox → entre 11.7 e 12.3 ms

Jogos são extremamente sensíveis ao delay, e valores acima de 40 ms já começam a gerar reclamações de "lag" ou travamentos.

Este dashboard permite ao NOC detectar:

- Se um jogo específico está com rota ruim;
- Se há problema em servidores externos;
- Se o provedor está entregando baixa latência de forma consistente;
- Desbalanceamento ou saturação nos enlaces.

4.10.5 Histórico de Latência – Jogos

O gráfico mostra se a latência se manteve estável ao longo do dia. Picos podem indicar:

- DDoS contra servidores de jogo
- Problemas de rota internacional
- Sobrecarga de tráfego em horários de pico
- Saturação momentânea em PTTs ou transitos

4.10.6 Pizza de Latência – Jogos

A pizza exibe a participação de cada jogo na média de latência.

Exemplo da imagem:

- League of Legends → 11.02%
- Valorant → 10.95%
- Free Fire → 9.82%
- Fortnite → 8.27%
- CS:GO → 8.78%
- Steam → 8.42%
- Xbox → 8.29%

Essa distribuição ajuda a identificar quais jogos têm variação maior e, portanto, precisam de atenção especial.

4.10.7 Principais problemas que esse dashboard ajuda a identificar

Rota degradada para um serviço específico

Ex.: apenas o TikTok ou apenas o LoL ficando com latência alta.
→ Sinal de problema entre o provedor do ISP e a CDN específica.

Instabilidade generalizada

Vários serviços com picos simultâneos.
→ Indica falha no backbone, trânsito ou saturação interna.

Picos de latência em jogos

→ Geralmente associados a problemas externos, congestionamento internacional ou ataques aos servidores de jogo.

4.10.8 Desbalanceamento de tráfego

Quando apenas alguns serviços apresentam latência mais alta.
→ Pode indicar falha em hashing, ECMP, ou saturação em um tronco específico.

4.10.9 Problemas em operadoras de trânsito

Se todos os serviços dependentes de uma operadora ficam instáveis.
→ Diagnóstico rápido de falha no trânsito.

4.10.10 Detecção de anomalias ao longo do dia

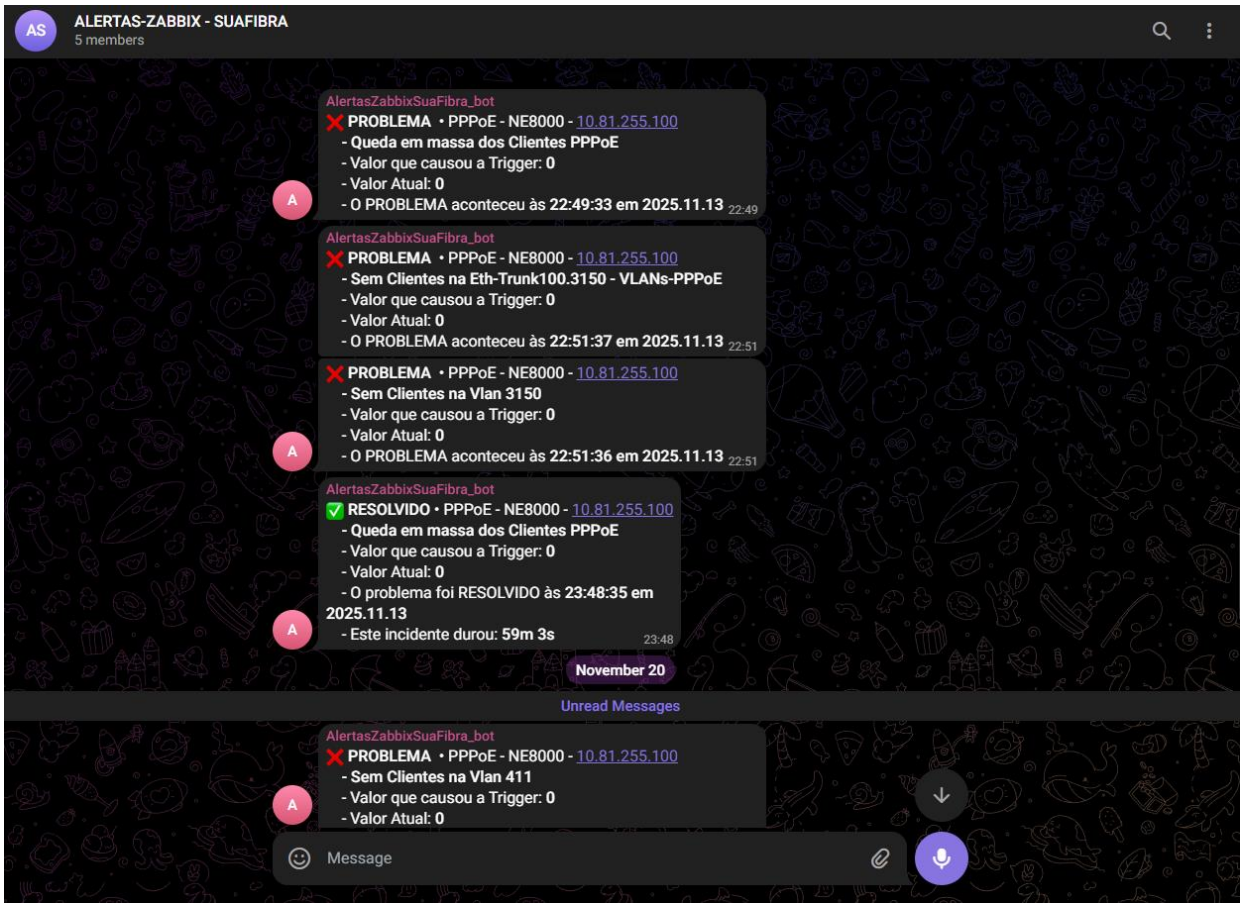
Gráficos permitem identificar:

- Horários de pico;
- Momentos de degradação;
- Oscilações repetitivas.

Esses padrões ajudam no planejamento de capacidade e na prevenção de falhas.

4.11 Interface de Alertas – Notificações Automáticas via Telegram

Figura 18 – Interface para Alertas



Fonte: Própria

A interface de alertas via Telegram constitui um dos componentes mais relevantes do sistema de monitoramento, pois é por meio dela que a equipe técnica recebe notificações imediatas sobre incidentes ou comportamentos anormais na rede. Diferentemente dos dashboards, que exigem acompanhamento constante, os alertas são enviados automaticamente para o celular ou computador dos técnicos, garantindo que a equipe seja informada quase em tempo real sempre que algum parâmetro crítico atinge um estado de risco. Esse mecanismo reduz drasticamente o tempo de detecção de falhas e, na prática, permite que muitos incidentes sejam identificados antes mesmo que os clientes percebam a instabilidade.

A imagem analisada demonstra como essas mensagens são apresentadas ao grupo de operação. Cada alerta contém informações completas e objetivas sobre o incidente detectado, incluindo o tipo de problema (como queda de PPPoE, perda de clientes por VLAN, instabilidade em BRAS ou rompimento de um enlace), o equipamento afetado, o valor exato que acionou a trigger e o horário preciso do início do evento. Em vez de um

aviso superficial, o bot fornece dados suficientes para que o técnico compreenda rapidamente a situação e possa tomar decisões assertivas.

Além de informar quando o problema ocorre, o bot também envia alertas indicando que o incidente foi resolvido. Nessas mensagens, são exibidos detalhes como o tempo total de duração do evento, o status normalizado do equipamento e a confirmação de que o serviço voltou a operar dentro dos padrões aceitáveis. Esse registro automatizado é extremamente valioso para relatórios internos, auditorias, controle de incidentes e identificação de falhas recorrentes.

Na rotina do provedor, esse tipo de alerta desempenha papel essencial na redução do tempo de indisponibilidade. Em muitos casos, a equipe técnica já está atuando no incidente antes mesmo do primeiro chamado de cliente chegar ao suporte, o que evidencia o impacto direto dessa ferramenta na agilidade da resposta operacional. Para quedas em massa, interrupções em POPs inteiros, travamentos de BRAS, instabilidades PPPoE ou flutuações inesperadas de clientes em VLANs específicas, a automação de alertas via Telegram torna-se indispensável para manter a rede estável e minimizar os impactos ao usuário final.

5. CONCLUSÃO

5.1 Considerações Finais

Este trabalho teve como propósito organizar, padronizar e aprimorar o monitoramento da rede do provedor, trazendo maior clareza, eficiência e automação para o ambiente operacional. Através de um estudo de caso baseado na experiência prática dentro da empresa, foi possível identificar desafios reais como dashboards inconsistentes, dificuldade em visualizar métricas críticas e ausência de integrações relevantes entre as ferramentas utilizadas.

Ao longo do desenvolvimento, ficou evidente que monitorar uma rede não se resume a "observar gráficos". É necessário estruturar a informação, garantir métricas confiáveis, padronizar visualizações, criar históricos consistentes e, principalmente, configurar alertas inteligentes que realmente auxiliem na tomada de decisão. A solução construída integrando Zabbix, Grafana, banco IXC e Telegram demonstrou que é possível transformar um ambiente fragmentado em um sistema unificado, claro e eficiente.

A prototipação dos painéis contribuiu para visualizar a disposição ideal das informações, beneficiando tanto a operação atual quanto o treinamento de novos técnicos. A definição de requisitos e critérios de validação trouxe segurança ao processo de implantação, reduzindo improvisos e garantindo funcionamento adequado.

Além disso, a melhoria no monitoramento impacta diretamente o provedor: reduzindo tempo de resposta a incidentes, prevenindo falhas maiores, diminuindo indisponibilidades e proporcionando uma experiência superior ao cliente final. O monitoramento, quando bem estruturado, torna-se uma ferramenta estratégica, não apenas operacional.

5.2 Contribuições

As principais contribuições deste trabalho são:

5.2.1 Padronização dos dashboards

Criação de modelos visuais consistentes para POPs, BGP, BRAS, GPON, CGNAT, interfaces e serviços externos.

5.2.2 Integração entre ferramentas

União de dados do Zabbix, Grafana e IXC para formar um ecossistema monitorado centralizado.

5.2.3 Alertas automáticos

Implementação de notificações via Telegram, reduzindo o tempo de detecção e resposta a incidentes críticos.

5.2.4 Organização da informação

Estruturas mais claras, intuitivas e fáceis de interpretar, tanto para técnicos experientes quanto para novos colaboradores.

5.3 Limitações da Pesquisa

5.3.1 Dependência do ambiente real

A pesquisa foi baseada em um único provedor, podendo haver variações significativas em ambientes com arquiteturas diferentes.

5.3.2 Volume de dados

Algumas integrações dependem do desempenho das APIs ou do banco IXC, o que pode gerar atrasos em redes maiores.

5.3.3 Restrições de hardware

O desempenho do monitoramento pode variar de acordo com capacidade de processamento e memória dos servidores Zabbix/Grafana.

5.3.4 Tempo disponível

Alguns aprimoramentos desejáveis não foram implementados devido ao escopo e cronograma do TCC.

5.3.5 Trabalhos Futuros

A partir da base desenvolvida, diversas melhorias podem ser implementadas em versões futuras do sistema:

5.3.6 Ampliação dos dashboards

Incluir novos POPs, novas métricas e mais detalhamento de redes Wi-Fi, VoIP, Core e Serviços Internos.

5.3.7 Predição de falhas

Aplicação de inteligência artificial para prever quedas de potência, saturação de enlaces e instabilidade de BGP.

5.3.8 Automação avançada

Criação de scripts que realizem ações corretivas automáticas, como reiniciar serviços, reestabelecer sessões ou ajustar limite.

REFERÊNCIAS

ABDULHAMID, S. M. et al. Network traffic monitoring and analysis: Challenges, solutions and future directions. IEEE Access, v. 11, p. 14523–14540, 2023.

CORDEIRO, M.; VASCONCELOS, A.; CORREIA, R. Challenges in monitoring distributed network infrastructures: A systematic review. Computer Networks, v. 212, p. 108–125, 2022.

PAPOUTSAKIS, M. et al. Operational challenges in large-scale ISPs: Monitoring, automation and incident response. Journal of Network and Systems Management, v. 29, p. 1–18, 2021.

SEBESTYEN, G.; POPESCU, D.; ZMARANDA, D. Methods and architectures for modern network monitoring in telecom environments. Sensors, v. 25, n. 4, p. 1120–1138, 2025.

DA SILVA, R. Network Monitoring in Distributed Environments: Challenges and Approaches. Journal of Network Systems, v. 14, n. 2, p. 45–59, 2021.

MOTTA, E.; DE OLIVEIRA, L.; TRAVASSOS, G. H. Network observability and failure detection in large-scale infrastructures: A systematic review. Information and Software Technology, v. 131, p. 106–118, 2020.

CORDEIRO, M.; VASCONCELOS, A.; CORREIA, R. Challenges in monitoring distributed network infrastructures: A systematic review. Computer Networks, v. 212, p. 108–125, 2022.

ZABBIX SIA. Zabbix Documentation 7.0 LTS. Disponível em: https://www.zabbix.com/documentation. Acesso em: 28 nov. 2025.

PIRES, Ricardo; ANDERSON, Chris. Grafana: Visualizing Metrics, Logs, and Traces. O’Reilly Média, 2023.

KOCZAN, Lukasz; GASIOR, Pawel. Zabbix 6 IT Infrastructure Monitoring Cookbook. Packt Publishing, 2022.

OVANDO, Luís; KASSLER, Andreas. Fiber Optic Communication Systems and GPON Networks. Springer, 2021.

SARRABEZOLLES, Valentin; DONNET, Benoît. Measuring NAT Behaviour in the Internet. Springer, 2021.

LUIZELLI, Marcelo et al. Broadband Access Networks: Technologies and Protocols. Springer, 2020.

WHITE, Russ; AZADI, Alvaro. Practical BGP. Addison-Wesley Professional, 2022.

FEITOSA, Emanoel; MOURA, Aline. Redes de Computadores: Fundamentos, Protocolos e Aplicações. 2. ed. LTC, 2021.

MAURO, Douglas R. Essential SNMP. 3. ed. O'Reilly Media, 2021.

STALLINGS, William. Foundations of Modern Networking: SDN, NFV, QoE, IoT, and Cloud. 2. ed. Pearson, 2022.

OLIFER, Natalia; OLIFER, Victor. Computer Networks: Principles, Technologies and Protocols for Network Design. 2. ed. Wiley, 2023.