UNIVERSIDADE FEDERAL RURAL DO SEMI-ÁRIDO
PRÓ-REITORIA DE GRADUAÇÃO
DEPARTAMENTO DE CIÊNCIAS EXATAS E TECNOLOGIA DA INFORMAÇÃO
CURSO DE BACHARELADO EM SISTEMA DE INFORMAÇÃO

JOSÉ ROBERTO PEREIRA DA SILVA

UM PROTÓTIPO DE APLICAÇÃO DE MONITORAMENTO DE REDE COM ENFOQUE NO PROTOCOLO SNMP

ANGICOS
2024

JOSÉ ROBERTO PEREIRA DA SILVA

UM PROTÓTIPO DE APLICAÇÃO DE MONITORAMENTO DE REDE COM ENFOQUE NO PROTOCOLO SNMP

Monografia apresentada à Universidade Federal Rural do Semi-Árido como requisito para obtenção do título de Bacharel em Sistema de Informação.

Orientador(a): Prof. Dr. Sairo Raoni Dos Santos

ANGICOS

2024

S586p Silva, José Roberto Pereira da.
Um protótipo de aplicação de monitoramento de rede com enfoque no protocolo SNMP / José Roberto Pereira da Silva. – 2024.
46 f. : il.

Orientador: Sairo Raoni dos Santos .
Monografia (graduação) – Universidade Federal Rural do Semi-árido, Curso de , 2024.

1. Rede. 2. Monitoramento. 3. Protótipo. 4. Provedores. 5. Internet. I. , Sairo Raoni dos Santos, orient. II. Título.

Ficha catalográfica elaborada por sistema gerador automáto em conformidade com AACR2 e os dados fornecidos pelo) autor(a).
Biblioteca Campus Angicos
Bibliotecário: Helder Romero Maia Duarte
CRB: 15/673

JOSÉ ROBERTO PEREIRA DA SILVA

UM PROTÓTIPO DE APLICAÇÃO DE MONITORAMENTO DE REDE COM ENFOQUE NO PROTOCOLO SNMP

Monografia apresentada à Universidade Federal Rural do Semi-Árido como requisito para obtenção do título de Bacharel em Sistema de Informação.

Defendida em: 25/10/2024

BANCA EXAMINADORA

Prof. Dr. Sairo Raoni dos Santos (UFERSA)
Presidente

Profª Dra. Jarbele Cássia da Silva Coutinho (UFERSA)
Membro Examinador

Prof. Dr. Araken de Medeiros Santos (UFERSA)
Membro Examinador

AGRADECIMENTOS

Primeiramente quero agradecer a Deus por tudo em minha vida, agradecer aos meus pais que sempre me apoiaram, mesmo com a morte do meu pai não desanimei, pois ele tinha e tem muito orgulho de mim assim como minha mãe que sempre foi uma guerreira e sempre lutamos juntos e agradecer a todos os meus professores que sempre estiveram me auxiliando nessa trajetória.

RESUMO

O presente trabalho propõe o protótipo de ferramenta que auxiliará empresas provedores de internet por meio do monitoramento de equipamentos e da frequência de rede. Problemas relacionados a oscilações de sinal, queda de conexão e mau funcionamento de equipamento são comuns em provedores de Internet de pequeno porte. O monitoramento facilitará possíveis soluções rápidas e eficazes para resolver tais problemas. No prototipo informará também sobre as condições dos equipamentos com base na leitura do sinal de frequência, onde indicará se ele está atingindo níveis adequados para o objetivo para o qual foi implantado. O acesso à ferramenta ocorrerá por meio de uma interface web e oferecerá informações sobre ocorrências diversas relacionadas ao sistema do provedor, detectando e alertando sobre problemas, desde oscilações de rede e maus funcionamentos a possíveis acidentes envolvendo infraestrutura física. Com esta ferramenta, esperamos possibilitar que provedores de Internet respondam a problemas rotineiros de maneira eficiente e rápida.

Palavras-chave: Rede, Monitoramento, Protótipo, Provedores, Internet.

ABSTRACT

This work proposes the prototype of a tool that will help internet provider companies by monitoring equipment and network frequency. Problems related to signal fluctuations, connection drops and equipment malfunctions are common in small Internet providers. Monitoring will facilitate possible quick and effective solutions to resolve such problems. The tool will also inform you about the condition of the equipment based on the reading of the frequency signal, which will indicate whether it is reaching adequate levels for the purpose for which it was deployed. Access to the tool will occur through a web interface and will offer information on various occurrences related to the provider's system, detecting and warning about problems, from network fluctuations and malfunctions to possible accidents involving physical infrastructure. With this tool, we hope to enable Internet providers to respond to routine problems efficiently and quickly.

Keywords: Network, Monitoring, Tool, Providers, Internet.

LISTA DE ABREVIAÇÕES

ASN.1	Abstract Syntax Notation One
ASCII	American Standard Code for Information Interchange
CMIP	Common Management Information Protocol
CNPJ	Cadastro Nacional de Pessoas Jurídicas
CSS	Cascading Style Sheets
HTML	HyperText Markup Language
HTTP	Hypertext Transfer Protocol
IETF	Internet Engineering Task Force
IP	Internet Protocol
ITU	International Telecommunication Union
MIB	Management Information Base
NMS	Network Management Systems
OID	Object Identifier
PDU	Protocol Data Unit
RF	Requisitos Funcionais
RFC	Request for Comments
RN	Rio Grande Do Norte
RNF	Requisitos Não-Funcionais
RMON	Remote Monitoring
RPC	Remote Procedure Call
SGMP	Simple Gateway Monitoring Protocol
SGML	Standard Generalized Markup Language
SNMP	Simple Network Management Protocol
SMS	Short Message Service
SMI	Structure of Management Information
TCC	Trabalho de Conclusão de Curso
TCP	Transmission Control Protocol
TI	Tecnologia da Informação
UDP	User Datagram Protocol
VSCode	Visual Studio Code

LISTA DE FIGURAS

LISTA DE TABELAS

SUMÁRIO

1 INTRODUÇÃO

No início dos anos 70, as redes de computador tinham crescido de uma organização simples de redes pequenas e separadas, para uma outra organização, com redes maiores e interconectadas. Estas redes maiores foram chamadas internets e o seu tamanho cresceu a uma taxa exponencial. Quanto maior estas redes se tornavam, mais difícil elas ficavam para administrar, e logo ficou evidente que um protocolo de administração de rede precisava ser desenvolvido.

O primeiro protocolo usado foi o Simple Network Management Protocol (SNMP), proposto em 1989. Inicialmente era considerado uma solução temporária, projetada para contornar dificuldades de administração de internetworking, enquanto outros, maiores e melhores protocolos estavam sendo projetados.

Destes projetos de protocolos dos anos 80 emergiram dois protocolos de administração de rede diferentes. O primeiro era SNMPv2, que incorporou muitas das características do SNMP original (que ainda hoje é o mais utilizado) como também alguns características somadas ao protocolo original, para consertar algumas falhas. O segundo era o Common Management Information Protocol (CMIP) que era melhor organizado e conteve muitos mais características que SNMPv1 ou v2.

O protocolo SNMP só começou realmente a ser largamente utilizado com a expansão das redes, na década de 90.

1.1 OBJETIVOS

Nesta seção são apresentados os objetivos do trabalho, agrupados em objetivo geral e objetivos específicos.

1.1.1 Objetivo Geral

Desenvolver um protótipo de uma ferramenta de monitoramento de rede que auxilie na manutenção para a eficiência, segurança e disponibilidade dos recursos de uma rede de computadores, por meio de atividades de coleta, análise e interpretação de dados relacionados ao tráfego de rede, desempenho, utilização de recursos e eventos de segurança.

1.1.2 Objetivos Específicos

- Elaborar fundamentação teórica a respeito do protocolo a ser analisado.
- Elaborar questionários.
- Aplicar um questionário com o profissional de rede a respeito de problemas de rotina que sofrem.
- Aplicar um questionário com clientes a respeito da qualidade de internet obtida por eles, buscando entender sua necessidade.
- Analisar os resultados.
- Definir escopo e requisitos.
- Desenvolver um protótipo do sistema projetado.

2 REFERENCIAL TEÓRICO

2.1 SNMP (*SIMPLE NETWORK MANAGEMENT PROTOCOL*)

De acordo com Mauro (2005), o SNMP (*Simple Network Management Protocol*) é um protocolo de gerência de redes cujo objetivo é disponibilizar uma forma simples e prática de realizar o controle dos equipamentos de uma rede de computadores. Definido ao nível de aplicação, o SNMP utiliza os serviços do protocolo de transporte UDP (*User Datagram Protocol*) para enviar suas mensagens através da rede.

Nos últimos anos, o SNMP tem dominado o mercado de sistemas de gerenciamento de redes devido, principalmente, a sua simplicidade de implementação, pois consome poucos recursos de redes e de processamento, o que permite a sua inclusão em equipamentos bastante simples (MAURO, 2005).

O SNMP ajuda o administrador a localizar e corrigir erros ou problemas de uma rede. Por meio de agentes SNMP, o administrador da rede consegue visualizar estatísticas de tráfego da rede e após analisar esses dados o administrador pode atuar na rede, alterando a sua configuração (MAURO, 2005).

2.1.1 Histórico

Segundo Stallings (2006), o SNMP foi desenvolvido no final dos anos 80 por um grupo da IETF (*Internet Engineering Task Force*) e teve sua origem em um protocolo para monitoração de gateways IP, o SGMP (*Simple Gateway Management Protocol*). O modelo SNMP possui uma abordagem genérica, podendo ser utilizado para gerenciar diferentes tipos de sistemas. Sua especificação está contida no RFC 1157 (Request for Comments).

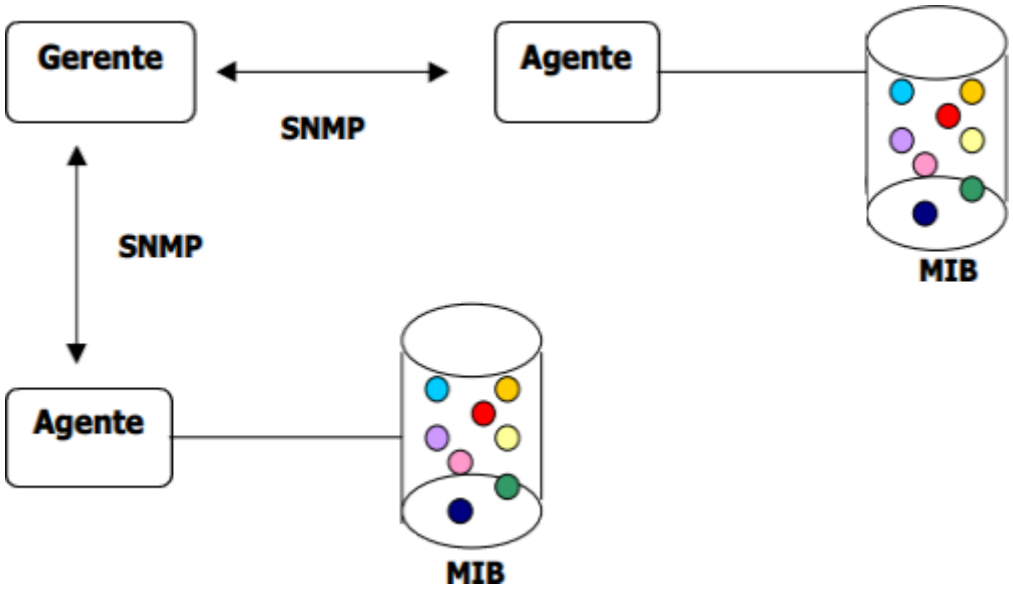
- 1989: SNMP v1
- 1992: Remote Monitoring – RMON
- 1993: SNMPv2
- 1996: SNMP v2c (Community Security)
- 1996: MIB RMON v2
- 1998: SNMP v3 (User Security Model)

2.1.2 Estrutura e Funcionamento

Stallings (2006) explica que o modelo de gerenciamento consiste em um esquema centralizado, isto é, uma estação (*host*) é configurada como gerente e os demais elementos da rede desempenham o papel de agentes. Um agente serve de procurador para aqueles equipamentos que não implementam o SNMP (*Simple Network Management Protocol*). Cada agente possui uma MIB (*Management Information Base)* que contém as variáveis relativas aos objetos gerenciados. O modelo genérico compreende três componentes:

- um conjunto de objetos gerenciados, correspondente a um agente e uma MIB (*Management Information Base)* associada;
- uma estação de gerenciamento de rede;
- um protocolo de gerenciamento de rede usado pela estação gerente e pelos agentes na troca de informações de gerenciamento.

Figura 1 – Modelo de Gerenciamento SNMP



Fonte: Telcomanager (2022).

2.1.3 Protocolo de Gerenciamento

De acordo com Kurose (2013), o protocolo de gerenciamento é visto sob o paradigma de observação remota, isto é, ele não transporta simplesmente

operações de gerenciamento que devem ser executadas pelos objetos gerenciados; cada objeto é visto como uma coleção de variáveis MIB (*Management Information Base)*, cujo valor pode ser lido ou alterado, possibilitando, assim, a monitoração e o controle de cada elemento da rede.

Quando recebe uma solicitação do gerente, um agente encaminha as informações ou altera valores das variáveis que representam os objetos gerenciados. O agente pode, ainda, avisar o gerente da ocorrência de algum evento não-previsto, encaminhando esses avisos na forma de *traps* (KUROSE, 2013).

2.1.4 O Gerente

De acordo com Walsh (2008), o gerente compreende um tipo de software que permite a obtenção e o envio de informações de gerenciamento junto aos mecanismos gerenciados mediante comunicação com um ou mais agentes.

As informações de gerenciamento podem ser obtidas com o uso de requisições efetuadas pelo gerente ao agente, como também, mediante envio automático disparado pelo agente a um determinado gerente. Tipicamente, um gerente está presente em uma estação de gerenciamento de rede (WALSH, 2008).

Devido à natureza de consumo intenso de recursos de processamento pelos componentes, a aplicação gerente costuma ser implementada em uma estação de trabalho rodando um sistema operacional multitarefa, como Unix ou Windows NT. Muitas vezes o dispositivo destinado a abrigar a aplicação gerente deverá disponibilizar bastante memória RAM, um considerável espaço em disco, além de outros mecanismos de armazenamento secundário e dispositivo de backup (WALSH, 2008).

2.1.5 O Agente

Para Perkins (1996), o agente utiliza as chamadas de sistema para realizar o monitoramento das informações do nodo e utiliza as chamadas de procedimento remoto (*Remote Procedure Call* - RPC) para controlar informações do nodo. Caso ocorra alguma exceção no nodo gerenciado, o agente fica responsável de notificar o gerente por meio de uma interrupção *trap*. Também compete ao agente efetuar a interface entre os diferentes mecanismos usados na instrumentação das

funcionalidades de gerenciamento inseridos em um determinado dispositivo gerenciado.

2.1.6 MIB (*Management Information Base*)

Perkins (1996) explica que a MIB (*Management Information Base*) é uma árvore hierárquica, dividida por tipos de informações onde se encontra nos nodos agentes que ficam organizadas em bases de informações de gerência chamadas MIB (*Management Information Base)* definidas em uma estrutura chamada SMI (*Structure of Management Information)*. A SMI (*Structure of Management Information)* especifica como as informações de gerência serão agrupadas e denominadas, definindo os tipos de dados e a sintaxe utilizada na MIB (*Management Information Base*) para evitar depender de detalhes de implementação dos equipamentos utilizados em rede.

Segundo Walsh (2008), a identificação e a forma de representação dos objetos contidos na MIB são definidos na linguagem abstrata ASN.1 (*Abstract Syntax Notation One*), desenvolvida pelo órgão ITU (*International Telecommunication Union*). Ela se caracteriza por representar as informações sem levar em consideração as estruturas e restrições dos equipamentos utilizados no sistema. Dessa maneira, a linguagem ASN.1 visa fornecer uma forma de representação genérica para a definição do formato das PDU (*Protocol Data Unit*) trocadas pelo protocolo e dos objetos que são gerenciados. A identificação do objeto é referida por OID (*Object Identifier*) e uma vez que o objeto é registrado com um determinado OID (*Object Identifier*) ele não poderá ser eliminado nem sua definição alterada.

A MIB pode ter 3 classificações possíveis:

- MIB Padrão: possui um conjunto de objetos bem definidos, conhecidos e aceitos pelos grupos e padrões Internet;
- MIB Experimental: podem conter informações específicas sobre outros elementos da rede e gerenciamento de dispositivos que são considerados importantes. Este termo “experimental” é como se fosse um ensaio para a MIB se tornar padrão;

- MIB Privada: projetadas por empresas individuais exclusivamente para seus dispositivos de rede.

Figura 2 – Estrutura Hierárquica da MIB.

Fonte: Telcomanager (2022).

2.1.7 Formato SNMP

Segundo Stallings (2006), O SNMP é um protocolo da camada de aplicação agindo na troca de informações de gerenciamento entre dispositivos de rede, as funções básicas do SNMP são:

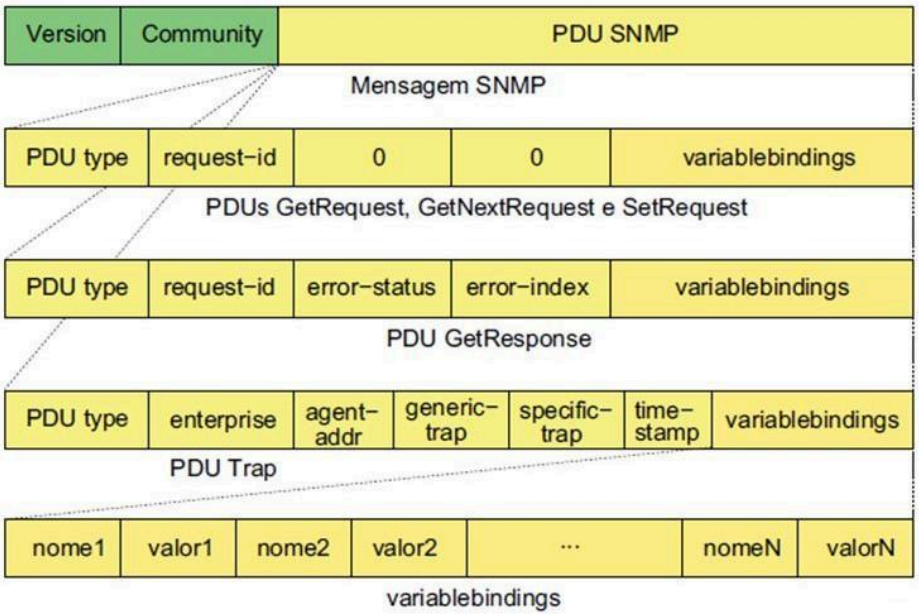
- *Get*: utilizado para se obter um valor do objeto escalar de um agente;
- *Set*: utilizado para se atribuir um valor a um objeto escalar de um agente;
- *Trap*: utilizado pelo agente para encaminhar um evento (objeto) não solicitado para uma estação de gerenciamento da rede.

O SNMP (*Simple Network Management Protocol*) utiliza como serviço de autenticação e controle de acesso uma forma primitiva e limitada chamada de comunidade SNMP (Community). Cada mensagem SNMP (*Simple Network Management Protocol*), ao ser encaminhada para o agente, contém a Community que será utilizada como parâmetro de identificação (STALLINGS, 2006).

Walsh (2008) fala que, através da definição de uma Community, um agente pode limitar o acesso a um conjunto selecionado de estações gerentes, à visão de um subconjunto de objetos de uma MIB (*Management Information Base*) e ao modo de acesso *read-only* (somente leitura) ou *read-write* (leitura e escrita).

As mensagens trocadas durante a comunicação entre os agentes e os gerentes são divididas em cinco tipos. Os possíveis formatos de mensagem são ilustrados na Figura 3.

Figura 3 – Formatos de mensagens SNMP.



Fonte: Mundo TI Brasil (2012).

No SNMP, informações são trocadas entre uma estação de gerenciamento e um agente na forma de uma mensagem SNMP (*Simple Network Management Protocol*). Cada mensagem inclui o número da versão SNMP, o nome da community para ser usado para esta troca e um de cinco tipos do Protocolo de Unidade de Dados (PDUs) (WALSH, 2008).

Perkins (1996) explica que a estrutura é descrita na figura 3 e os campos que a constituem estão definidos na Tabela 1. Nota-se que o GetRequest, GetNextRequest e SetRequest PDU tem o mesmo formato que o GetResponse PDU

Tabela 1 – Campos de Mensagem SNMP.

Campo	**Descrição**
version	Versão SNMP; RFC 1157 é versão 1.

community	Uma PAIring de um agente SNMP com alguns conjuntos arbitrários de entidades de aplicação SNMP.
request-id	Usados para distinguir entre requests OUStanding provendo cada request com um ID único.
error-status	Usados para indicar que uma exceção ocorreu enquanto processava um request.
error-index	Quando um error-status é não 0, error-index pode prover informações adicionais indicando qual variável na lista causou a exceção.
variable-bindings	Uma lista de nomes de variáveis e valores correspondentes.
enterprise	Tipo do objeto gerador do trap.
generic-trap	Tipo genérico do trap.
specific-trap	Código específico do trap.
time-stamp	Tempo ocorrido entre a última reinicialização da entidade da rede e a geração do trap.

Fonte: Mundo TI Brasil (2012).

2.1.8 Transmissão de uma mensagem SNMP

Walsh (2008) explica que uma entidade SNMP (*Simple Network Management Protocol*) pode transmitir cinco tipos diferentes de PDU para outra entidade SNMP. São os cinco tipos:

- *GetRequest* – solicita a informação sobre um objeto escalar;
- *GetNextRequest* – solicita informação sobre o próximo objeto escalar;
- *GetResponse* – resposta da solicitação;
- *SetRequest* – atribui um valor escalar a um objeto;
- *Trap* – utilizado pelo agente para encaminhar uma notificação para um gerente.

O PDU é construído usando a estrutura ANS.1 (*Abstract Syntax Notation*) definida no RFC 1157 (Request for Comments). Para iniciar uma transmissão, a entidade realiza as seguintes ações:

1. O PDU é passado para um serviço de autenticação, junto com o endereço de origem e destino e o nome da community. O serviço de autenticação realiza alguma transformação necessária para esta troca, como criptografia ou a inclusão de um código de autenticação e retorna o resultado.
2. A entidade do protocolo então constrói a mensagem, consistindo de um campo versão, nome da community, e o resultado do passo 1.
3. O novo objeto ANS.1 (Abstract Syntax Notation) é representado usando as regras básicas de codificação, e passado ao serviço de transporte.

2.1.9 Recebimento de uma mensagem SNMP

De acordo com Stallings (2006), uma entidade SNMP (*Simple Network Management Protocol*) realiza as seguintes ações assim que recebe uma mensagem SNMP:

1. Confere a sintaxe básica da mensagem e a descarta se ela falhar na comunicação;
2. Verifica o número da versão e descarta a mensagem se é incompatível;
3. A entidade do protocolo então passa o nome do usuário, a parcela PDU (Protocolo de Unidade de Dados) da mensagem e a origem e destino do endereço de transporte para um serviço de autenticação:
    a. Se a autenticação falha, o serviço de autenticação avisa a entidade do protocolo SNMP (*Simple Network Management Protocol*), que descarta a mensagem;
    b. Se a autenticação tem sucesso, o serviço de autenticação retorna na forma de um objeto ANS.1 (Abstract Syntax Notation One).
4. A entidade do protocolo faz uma supervisão na sintaxe básica do PDU. Por outro lado, usando o nome da comunidade, o plano de acesso SNMP apropriado é selecionado e o PDU é processado de acordo.

O SNMP (*Simple Network Management Protocol*) possui um controle de limite de tempo (time-out) para o recebimento de uma mensagem executado em

paralelo às demais funções de gerência, permitindo que a aplicação de gerência não fique dependendo de uma mensagem de um nodo falho e detectando a falha de comunicação entre nodos (STALLINGS, 2006).

2.2 VARIÁVEIS (*VARIABLE-BINDINGS*)

Blokdyk (2020) relata que toda operação envolve acesso a uma instância de objeto. Somente objetos folhas na árvore de instância de objetos podem ser acessados, isto é, somente objetos escalares. Entretanto, é possível em um grupo SNMP um número de operações do mesmo tipo (Get, Set, Trap) em uma mensagem simples. Assim, se uma estação de gerenciamento quer receber os valores de todos objetos escalares em um grupo particular para um agente particular, ele pode enviar uma mensagem simples requerendo todos os valores e recebendo uma resposta, listando os valores. Para implementar trocas de múltiplos objetos, todos os objetos da PDU SNMP incluem um campo de ligação de variáveis. Estes campos consistem de uma sequência de referências a instâncias de objetos, junto com o valor desses objetos.

2.2.1 Operações do protocolo SNMP

Blokdyk (2020) afirma que as operações de gerenciamento são componentes da aplicação gerente que controlam e monitoram os agentes pertencentes à comunidade de um determinado domínio de gerenciamento. As operações de gerenciamento podem ler e escrever em variáveis da MIB da cada aplicação agente para gerenciar o dispositivo de rede. As operações de gerenciamento podem também armazenar informações de gerenciamento recuperadas junto às aplicações agentes em uma MIB própria e/ou em um Banco de Dados. O gerente SNMP (*Simple Network Management Protocol*) realiza basicamente duas funções durante a gerência: get (leitura de valores), para monitoramento das características do nodo; e set (escrita de valores), para controle das características do nodo.

A troca de mensagens no SNMP (*Simple Network Management Protocol*) ocorre através das PDUs (*Protocol Data Units*) utilizadas pelo protocolo para a troca de informações entre os diversos elementos da gerência e a estrutura utilizada para o transporte de variáveis BLOKDYK (2020).

Perkins (1996) explica que a entidade SNMP (*Simple Network Management Protocol*) de recebimento responde a um PDU do tipo SetRequest com um PDU do tipo GetResponse contendo o mesmo request-id. Se a entidade de resposta for capaz de estabelecer valores para todas as variáveis listadas na entrada da lista de variáveis, então o PDU do tipo GetResponse inclui o campo variáveis de ligação com um valor fornecido para cada variável.

A PDU do tipo GetRequest (notificação) é emitida por uma entidade SNMP (*Simple Network Management Protocol*) como representante de uma aplicação do gerente. Ela é usada para prover a estação uma resposta na forma de um GetResponse, cujo contém os valores dos objetos solicitados, com isso o gerenciamento feito é uma notificação assíncrona de alguns eventos significantes (BLOKDYK, 2020).

2.2.2 Restrições das Operações

O SNMP apresenta diversas restrições nas operações que impactam sua flexibilidade e eficácia na gestão de dispositivos de rede. Uma das principais limitações refere-se ao tipo de operações que podem ser realizadas: o SNMP permite apenas a inspeção e/ou a alteração de variáveis específicas. Isso significa que, durante uma operação, um administrador pode consultar o estado atual de uma variável gerenciada ou, em alguns casos, modificar seu valor. No entanto, essa capacidade se limita a um conjunto restrito de dados, o que pode ser um obstáculo em ambientes de rede complexos onde múltiplas variáveis precisam ser gerenciadas de maneira simultânea.

Além disso, a estrutura da MIB (Management Information Base) é rígida e não pode ser alterada pelas operações realizadas através do SNMP. Essa rigidez significa que, ao desenvolver ou implementar novos dispositivos ou aplicações, os administradores não têm a flexibilidade de personalizar a estrutura de dados para atender a necessidades específicas. Como resultado, a MIB deve ser cuidadosamente planejada e estruturada desde o início, limitando as adaptações que podem ser feitas no futuro para acomodar novas funcionalidades ou requisitos de monitoramento.

Outro aspecto crítico das operações do SNMP é que, em cada operação, somente podem ser acessados valores escalares. Isso implica que os dados

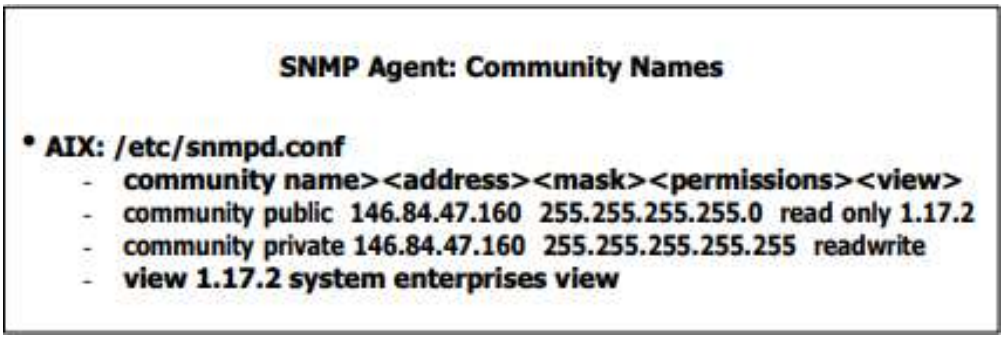
retornados ou alterados são restritos a valores únicos, ao invés de permitir a manipulação de conjuntos de dados mais complexos ou estruturados. Essa limitação na manipulação de dados escalares torna a análise e a visualização de informações mais desafiadoras, especialmente em cenários onde a inter-relação entre múltiplas variáveis é crucial para a tomada de decisões informadas.

Essas restrições das operações do SNMP têm implicações significativas para a gestão de redes, exigindo que administradores busquem alternativas ou soluções complementares para garantir uma supervisão abrangente e adaptável das infraestruturas de rede. A compreensão dessas limitações é fundamental para que os profissionais de TI possam planejar e implementar estratégias eficazes para gerenciar seus ambientes de forma proativa, levando em conta as necessidades específicas de suas organizações e a evolução contínua das tecnologias de rede.

2.2.3 Segurança no protocolo SNMP

Stallings (2006) explica que o protocolo SNMP (*Simple Network Management Protocol*) pode realizar operações de reconfiguração na rede alterando características de equipamentos ou até desligando máquinas, sendo que não existe qualquer mecanismo de segurança aplicado ao conteúdo das mensagens. O controle é feito através da verificação do conteúdo de um campo especial no pacote do SNMP denominada comunidade. A comunidade é definida como sendo o relacionamento entre duas entidades do SNMP (*Simple Network Management Protocol*). Ela é definida como um conjunto de bytes formando caracteres ASCII (American Standard Code for Information Interchange) que serão utilizados para efetuar este relacionamento. Dessa forma, quando é realizada a comunicação entre duas entidades do SNMP (*Simple Network Management Protocol*), a entidade destinatária da mensagem realiza a verificação do conteúdo da comunidade para averiguar se esta informação é proveniente do remetente indicado.

Figura 4 – Community Names.



Fonte: Cisco - Brasil (2024).

Através da comunidade é possível que o agente realize uma verificação da integridade do agente realizando autenticação e políticas de acesso (agente controla que diferentes gerentes podem obter diferentes variáveis da MIB) através deste campo. O mais importante no entendimento da comunidade, é que sem o conhecimento prévio da comunidade de um determinado equipamento gerenciável, será impossível a qualquer aplicação de gerência acessar as informações da MIB. Outra consideração importante é que um equipamento pode ter mais de uma comunidade configurada, como uma com direitos de leitura, escrita e trap. Portanto, um mesmo equipamento poderá contar com três strings de comunidade diferentes. Isto tem o objetivo de aumentar a segurança no acesso aos equipamentos (STALLINGS, 2006).

De acordo com Stallings (2006), no exemplo, o arquivo snmpd.conf é onde se pode configurar o acesso que se quer fornecer às estações gerente quando realizam a requisição SNMP (*Simple Network Management Protocol*). Pode-se limitar o acesso com *read-only* e *read-write*.

Com esse tipo de autenticação, o acesso à MIB se torna pouco seguro, devido principalmente a (i) identificação da origem: a comunidade é transmitida sem qualquer proteção; (ii) integridade da mensagem: ao ser interceptada a mensagem não garante qualquer proteção referente ao conteúdo; (iii) tempo-limite: período de tempo que a mensagem pode ficar presa por algum serviço; (iv) privacidade: qualquer serviço pode monitorar uma comunicação entre entidades SNMP, e; (v) autorização: não há controle de autorização de acesso aos dados da MIB.

2.2.4 Limitações do SNMP

As limitações do SNMP são diversas e impactam sua eficácia na gestão de redes. Primeiramente, destaca-se a falta de segurança, que se agrava devido a um esquema de autenticação trivial, tornando o protocolo vulnerável a acessos não autorizados. Além disso, existem limitações no uso do método SET, o que restringe as operações de configuração em dispositivos gerenciados.

Outra questão importante é a ineficiência do SNMP, caracterizada por um esquema de eventos limitado e fixo, que não se adapta facilmente a diferentes cenários de rede. A operação baseada em pooling também contribui para essa ineficiência, uma vez que requer verificações periódicas que podem sobrecarregar a rede. Os comandos, por sua vez, transportam apenas uma quantidade reduzida de dados, o que limita a quantidade de informações que podem ser transmitidas em uma única operação.

Adicionalmente, o SNMP carece de funções específicas que poderiam enriquecer a gestão de dispositivos, e a MIB (*Management Information Base*) possui uma estrutura fixa que não permite personalizações necessárias para diferentes ambientes. A falta de comandos de controle e a ausência de comunicação entre gerenciadores também são fatores que comprometem sua funcionalidade. Por fim, o protocolo é considerado não confiável, uma vez que é baseado em UDP/IP e as traps não possuem reconhecimento, o que dificulta a garantia de entrega de mensagens e a monitorização efetiva da rede.

2.2.5 SNMPv2 e SNMPv3

Visando obter melhorias com relação aos aspectos de segurança foram desenvolvidas novas versões do SNMP. A segunda versão, o SNMPv2 contém mecanismos adicionais para resolver os problemas relativos à segurança como: privacidade de dados, autenticação e controle de acesso STALLINGS (2006)..

A terceira versão, o SNMPv3 tem como objetivo principal alcançar a segurança, sem esquecer-se da simplicidade do protocolo, através de novas funcionalidades como: autenticação de privacidade, autorização e controle de

acesso, nomes de entidades, pessoas e políticas, usernames e gerência de chaves, destinos de notificações, relacionamentos proxy e configuração remota.

3 METODOLOGIA

Este trabalho foi desenvolvido utilizando a seguinte ordem metodológica: a) pesquisa bibliográfica; b) elaboração de questionários; c) aplicação dos questionários; d) análise dos dados observados; e) criação do protótipo.

Para elicitar os requisitos do sistema em questão, foram aplicados dois questionários com perguntas de múltipla escolha e subjetivas por meio da ferramenta digital *Google Forms.* O público-alvo foi composto por clientes e profissionais que atuam em provedores de internet em Angicos/RN.

As questões se referiram a questões de qualidade de serviço, problemas e reclamações no dia-a-dia de técnicos e clientes dos provedores. O questionário foi aplicado com o intuito de coletar informações possíveis para elicitar requisitos para um sistema de monitoramento de rede, cujo principal objetivo será reduzir o tempo da solução de incidentes, diminuindo assim reclamações e problemas de rede.

As questões buscaram compreender as reclamações tanto dos usuários quanto dos trabalhadores dos provedores locais de Internet. A temática das questões incluíram, mas não se limitaram a:

- Expor necessidades dos clientes referente aos serviços ofertados;
- Expor problemas sofridos pelos técnicos;
- Analisar situações vividas pelos clientes e técnicos;
- Observar vantagens e desvantagens relatadas pelos clientes a respeito dos serviços dos provedores de internet;
- Verificar o tempo de resposta a respeito de problemas sofridos pelos técnicos;
- Investigar o desempenho dos provedores de internet;
- Observar como os técnicos trabalham.

Com base nas informações coletadas, será feita uma análise para validar as informações necessárias que estejam alinhadas com o objetivo do projeto. Com isso será possível elaborar um plano de projeto, estimar recursos, determinar cronograma, identificar riscos, planejar as atividades necessárias para o desenvolvimento do protótipo. Após todo o planejamento, dar-se-á início ao desenvolvimento do protótipo da ferramenta, envolvendo principais componentes e interface.

3.1 REQUISITOS

Esta seção descreve todos os requisitos definidos para o desenvolvimento do protótipo.

3.1.1 Requisitos Funcionais (RF)

A Tabela 2 mostra os requisitos funcionais considerados durante o desenvolvimento do sistema.

Tabela 2 – Requisitos Funcionais (RF).

RF	**Monitoramento:** O sistema permitirá monitorar através de gráficos, a frequência e o desempenho da rede.
RF	**Alertas e Notificações:** O sistema gerará notificações e alertas por meio de e-mail ou SMS.
RF	**Status de dados de desempenho:** Será possível expor os dados de desempenho através de coleta rápida.
RF	**Status da Rede:** Uma representação visual do funcionamento da rede em si.
RF	**Relatórios Atualizados:** Os administradores receberão relatórios atualizados ao fim do dia.
RF	**Segurança de Acesso:** O sistema incluirá autenticação de usuários, para proteger dados sensíveis.

Fonte: Autoria própria (2024).

3.1.2 Requisitos Não-Funcionais (RNF)

A Tabela 3 mostra os requisitos não-funcionais considerados durante o desenvolvimento do sistema.

Tabela 3 – Requisitos Não-Funcionais (RNF).

RNF	**Desempenho:** O sistema deve ser responsivo e capaz de lidar com grandes volumes de dados de monitoramento sem atrasos significativos.
RNF	**Disponibilidade:** Deve estar disponível 24 horas por dia, 7 dias por semana, com tempo de inatividade mínimo planejado para manutenção.
RNF	**Segurança:** Deve ser altamente seguro, protegendo dados confidenciais e oferecendo mecanismos de detecção de intrusões.
RNF	**Escalabilidade:** Deve ser escalável para lidar com o crescimento da rede sem comprometer o desempenho.
RNF	**Usabilidade:** A interface de usuário deve ser intuitiva e de fácil utilização para administradores de rede de diferentes níveis de experiência.
RNF	**Backup e Recuperação:** Deve oferecer recursos de backup e recuperação de dados para evitar a perda de informações críticas.
RNF	**Documentação:** Deve fornecer documentação completa e atualizada para orientar os usuários na configuração e uso do sistema.

Fonte: Autoria própria (2024).

3.2 ESCOPO DO PROJETO

Esta seção tem como objetivo mostrar todas as funcionalidades que serão implementadas no protótipo do site de monitoramento de rede.

O objetivo deste site é desenvolver um protótipo de uma ferramenta de monitoramento de rede, projetada para auxiliar administradores de redes e equipes de TI na manutenção da eficiência, segurança e disponibilidade dos recursos de uma rede de computadores. A página inicial oferecerá uma visão atrativa, com um layout simples e fácil de navegar, incluindo um cabeçalho com menu e informações de usuários ativos. A página de login contará com formulários para autenticação segura, recuperação de senha e cadastro de novos usuários.

O monitoramento da rede será realizado através de um dashboard que exibirá informações como dispositivos conectados, uso de largura de banda e gráficos de latência. Relatórios detalhados sobre dispositivos conectados, tráfego de rede e desempenho poderão ser visualizados e impressos para análises mais aprofundadas. O sistema também terá uma seção de alertas e notificações que informará sobre problemas nos dispositivos e notificará quando esses forem resolvidos. Um formulário de suporte estará disponível para que os usuários possam relatar possíveis problemas.

Em termos de design, o foco será em um layout limpo e funcional, com ênfase na usabilidade e na visualização clara dos dados, garantindo uma interface de navegação simples e acessível. O desenvolvimento do projeto será realizado na plataforma VSCode, utilizando HTML e CSS para o frontend. O cronograma do projeto se dividirá em três fases: planejamento (março a abril de 2024), desenvolvimento (maio a julho de 2024) e entrega (agosto a setembro de 2024).

3.2.1 Tecnologias Utilizadas

A plataforma de desenvolvimento escolhida é o Visual Studio Code (VSCode), um editor de código-fonte desenvolvido pela Microsoft, compatível com Windows, Linux e macOS. O VSCode oferece uma variedade de recursos, incluindo suporte para depuração, controle de versionamento integrado com Git, realce de sintaxe, complementação inteligente de código, snippets e refatoração de código, tornando-o uma ferramenta robusta e eficiente para o desenvolvimento de software.

3.2.2 Linguagens de Programação

De acordo com Alves (2013), existem diversos tipos de linguagens de programação que funcionam de maneiras diferentes. No início da era da

computação, os programadores eram obrigados a utilizar a linguagem de máquina, composta por combinações de 0s e 1s. Isso gerou a necessidade de criar uma linguagem que fosse compreensível para os humanos, substituindo sequências numéricas por palavras. As linguagens de programação foram desenvolvidas para transmitir ao computador quais instruções devem ser executadas.

No desenvolvimento deste projeto, foram utilizadas duas linguagens principais: HTML (*HyperText Markup Language*) e CSS (*Cascading Style Sheets*). O HTML é uma linguagem de marcação usada para construir páginas web, sendo interpretado pelos navegadores e baseado nos padrões HyTime e SGML (Standard Generalized Markup Language), permitindo a representação estruturada de hipermídia e conteúdo temporal. Já o CSS é um mecanismo para adicionar estilos às páginas web, aplicável diretamente nas tags HTML, dentro da tag <style>, ou por meio de um arquivo CSS vinculado.

3.2.3 Processo de desenvolvimento

Nesta seção, será apresentada a metodologia utilizada durante o desenvolvimento deste trabalho, detalhando os métodos e procedimentos adotados. A primeira etapa consistiu na observação e estudo de outros sites de monitoramento de rede, com o objetivo de identificar elementos essenciais que deveriam estar presentes em um sistema de monitoramento eficiente.

Na segunda etapa, foram escolhidas as ferramentas necessárias para o desenvolvimento do protótipo. O editor de código Visual Studio Code foi a primeira ferramenta selecionada, seguido da definição das linguagens de programação HTML e CSS para a construção da interface.

A terceira etapa focou no desenvolvimento do front-end, começando pela criação da tela de login, que permite o acesso ao sistema. Em seguida, foi desenvolvida a página de monitoramento, composta por um dashboard informativo. A próxima tela implementada foi a de relatórios, com o objetivo de exibir dados detalhados sobre a rede. Posteriormente, foi criada a página de alertas e notificações, destinada a informar sobre problemas e a resolução dos mesmos. Por fim, a última tela desenvolvida foi a de suporte, permitindo que os usuários relatem problemas não resolvidos ou detectados.

3.2.4 Apresentação do protótipo

Nesta seção é apresentado o protótipo do projeto, com telas e descrições do funcionamento do sistema. A página inicial, ilustrada na Figura 5, tem como objetivo exibir usuários fictícios ativos, apresentando uma gama de informações detalhadas.

Figura 5 – Página inicial.

Fonte: Autoria própria (2024).

A página de login, mostrada na Figura 6, foi desenvolvida para oferecer um acesso seguro ao site, garantindo uma melhor experiência para os usuários. Após efetuar o login, o usuário estará habilitado a navegar por todas as funcionalidades do sistema. A Figura 7 exibe a página de cadastro, criada para novos usuários que ainda não possuem registro no sistema. Nessa página, o usuário deverá preencher um formulário com os dados solicitados para completar o processo de cadastro.

Figura 6 – Página de login.

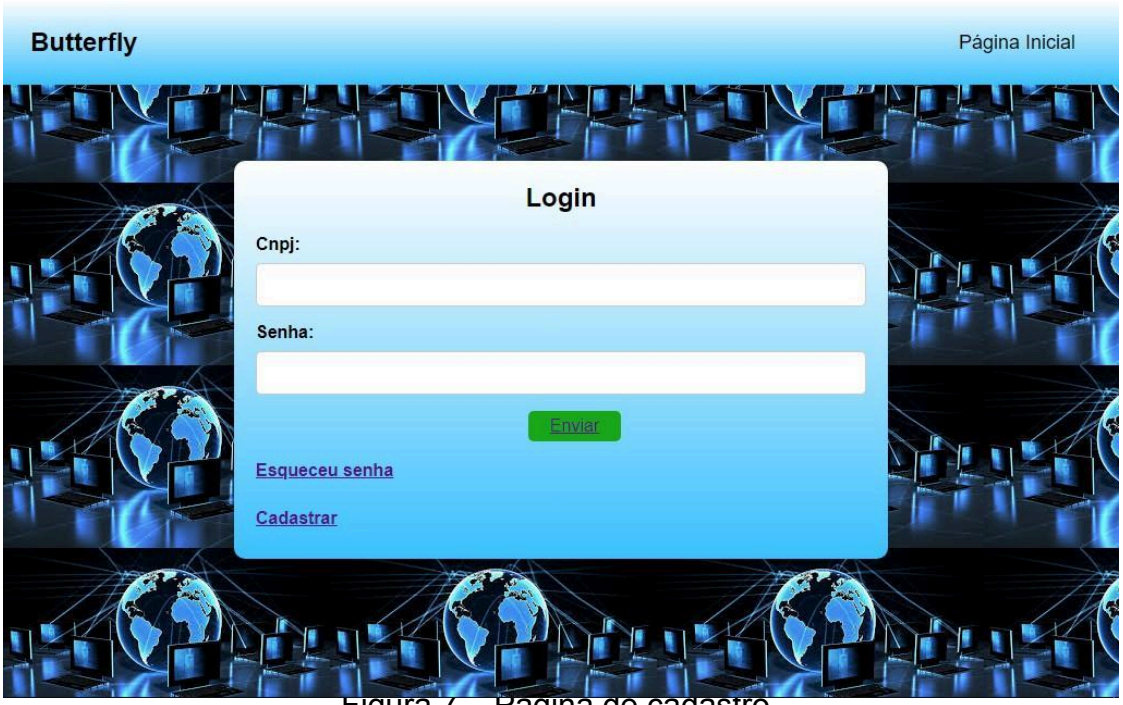
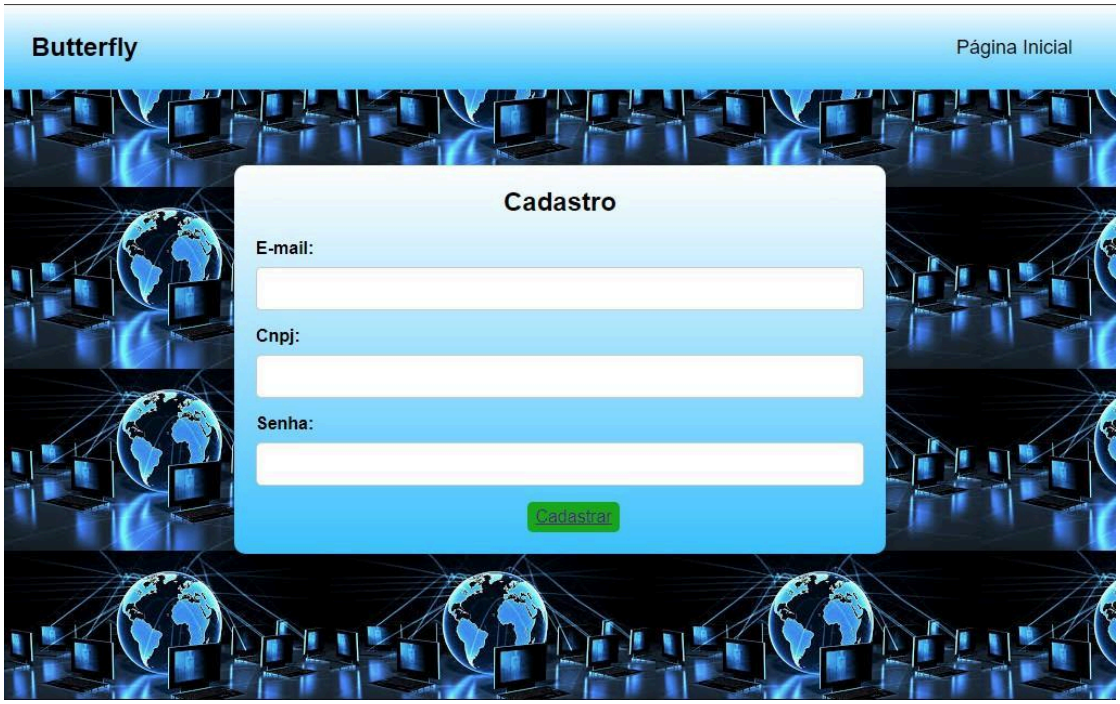


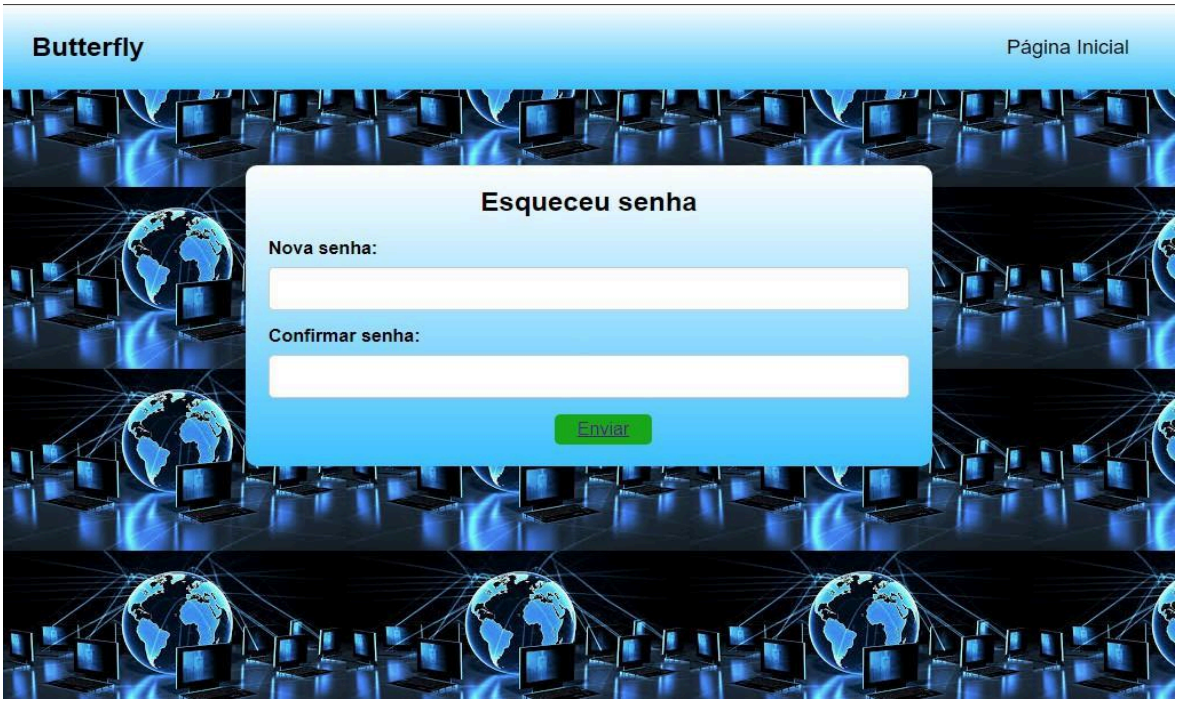
Figura 7 – Página de cadastro.



Fonte: Autoria própria (2024).

A página "Esqueceu a senha", ilustrada na Figura 8, foi criada para auxiliar o usuário caso ele não se lembre ou erre sua senha. Ela oferece a opção de recuperação por meio do preenchimento de um formulário, onde o usuário insere e confirma uma nova senha, garantindo assim o acesso ao sistema. A página de monitoramento, mostrada na Figura 9, apresenta de forma simples informações detalhadas sobre os dispositivos conectados, utilizando um gráfico de tráfego, além de dois gráficos adicionais que exibem o uso de largura de banda e a latência média da rede. Na página de relatórios, representada na Figura 10, as informações obtidas do monitoramento são exibidas de maneira clara e acessível, facilitando a compreensão dos usuários, com a opção de imprimir os relatórios para análises posteriores.

Figura 8 – Página de recuperação de senha.



Fonte: Autoria própria (2024).

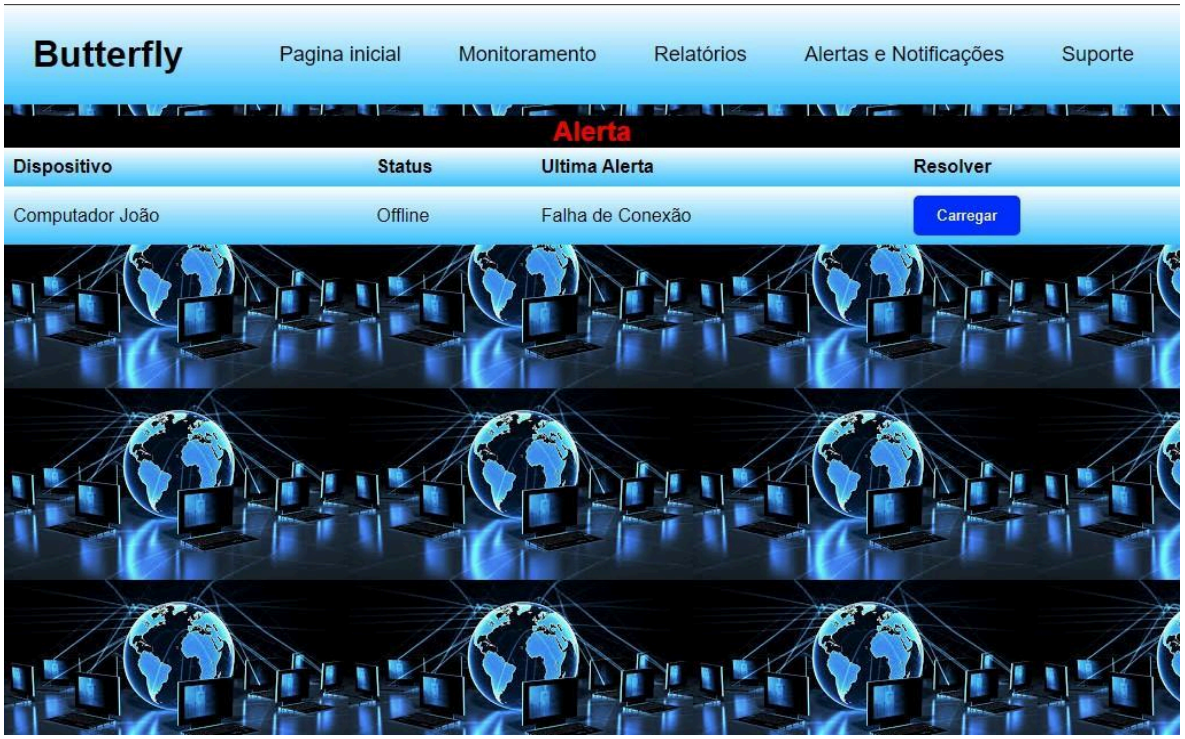
Figura 9 – Página de monitoramento.

Figura 10 – Página de relatórios.

Fonte: Autoria própria (2024).

A página de alertas e notificações, ilustrada na Figura 11, tem como principal função manter os técnicos (usuários) informados sobre possíveis problemas, oferecendo a opção de carregar mais informações para visualizar os detalhes.

Figura 11 – Página de alertas e notificações.



Fonte: Autoria própria (2024).

Em caso de demora na resolução, uma notificação será exibida no canto inferior direito da tela com a mensagem "Aguarde, será resolvido em breve", conforme mostrado na Figura 12. A página de suporte, representada na Figura 13, permite que o usuário relate problemas não registrados no sistema, preenchendo um formulário com o CNPJ (Cadastro Nacional de Pessoas Jurídicas) e uma descrição detalhada do problema, que será enviada diretamente para a central de suporte. A Figura 14 mostra o aviso que confirma ao usuário que o problema foi reportado com sucesso.

Figura 12 – Página alertas e notificações.

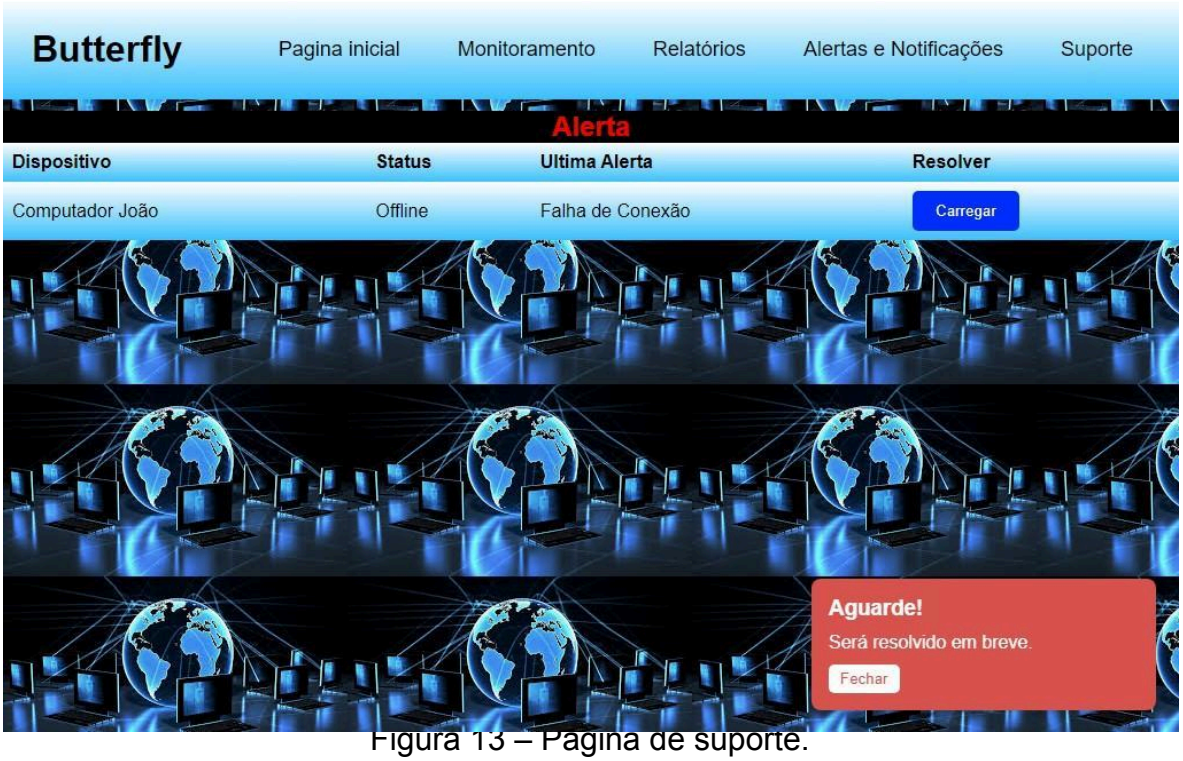


Figura 13 – Página de suporte.

Fonte: Autoria própria.

Figura 14 – Página de mensagem de sucesso.

Fonte: Autoria própria.

4 RESULTADOS

O objetivo desta etapa é descrever os resultados obtidos a partir da coleta e análise dos dados por meio da aplicação dos questionários.

O Questionário 1 foi elaborado com o propósito de avaliar e coletar informações sobre os administradores de redes dos provedores de internet da cidade de Angicos/RN. A intenção é realizar uma análise detalhada que possa contribuir para melhorias nos serviços prestados por esses profissionais.

Tabela 4 – Questionário para os administradores de redes.

	Pergunta	%	Resposta
1	Qual o problema mais comum relatado pelos clientes onde possivelmente se torna uma dor de cabeça para os agentes?	100	Rompimento de fibra
2	Quando um problema é relatado, os agentes dão um prazo para uma possível solução?	100	Sim
3	Em relação a rompimento de fibras, os agentes sabem o local exato do problema?	50	Não
		50	Sim
4	A empresa tem um dashboard para o monitoramento de frequência?	100	Sim
5	O que acham de uma ferramenta onde mostra o diagnóstico do problema ocorrido através de um dashboard de monitoramento de frequência?	100	Seria ótima

Fonte: Autoria própria (2024).

A análise dos resultados obtidos por meio de um questionário qualitativo revelou que, nas questões 1, 2, 4 e 5, alcançamos a taxa de 100% esperada, o que indica uma compreensão abrangente das atividades dos administradores em seus respectivos campos de atuação. No entanto, observamos um pico de indecisão na questão 3, onde 50% dos profissionais relataram dificuldades em identificar o local exato dos problemas de rompimento de fibra. Essa constatação sugere que nosso sistema pode atender a essa demanda, especialmente por meio de sua funcionalidade de relatórios, que fornece informações detalhadas sobre o cliente, incluindo seu endereço de IP (*Internet Protocol*).

O Questionário 2 foi desenvolvido para coletar dados dos clientes dos provedores da cidade (Angicos/RN), com intuito de adquirir informações sobre serviços prestados pelos provedores.

Tabela 5 – Questionário dos Clientes dos provedores de Angicos/RN.

Pergunta		%	Resposta
1	Sua internet é boa ou costuma ter bastante problemas, o senhor(a) poderia me dizer quais problemas ela apresenta?	50	Não,Lenta
		50	Boa
2	Quando o senhor(a) reclama de problemas é rápido?	50	Sim
		50	Não
3	Em relação a necessidades, sua internet consegue atendê-las?	100	Não
4	Falando sobre o valor do plano, o senhor(a) acha justo com o que a sua internet entrega?	50	Sim
		50	Não
5	Quando ocorre um problema, os técnicos informam ao senhor(a) sobre o mesmo?	100	Não

Fonte: Autoria própria (2024).

Os resultados obtidos por meio de um questionário qualitativo mostraram que, nas questões 3 e 5, atingimos a taxa de 100% esperada, permitindo uma boa compreensão do pensamento e das insatisfações dos clientes. Essa informação nos possibilita desenvolver uma solução a longo prazo que atenda às necessidades relatadas, através da implementação de normas e procedimentos que garantam a satisfação do cliente em relação a problemas enfrentados. No entanto, observamos um pico de indecisão nas questões 2 e 4, indicando que 50% dos clientes não estão tendo uma boa experiência com sua conexão à internet.

4.1 PROBLEMÁTICA

Nesta etapa, podemos identificar as problemáticas que o sistema precisará solucionar:

1. **Pouca informação de monitoramento:** Atualmente, a quantidade de dados disponíveis para monitoramento é insuficiente, dificultando uma análise mais abrangente e a formulação de soluções efetivas.
2. **Relatórios não detalhados:** Os relatórios gerados são muito superficiais, o que limita a realização de uma avaliação crítica das informações.
3. **Falta de alertas de problemas:** O sistema atual não oferece nenhum tipo de feedback, o que impede os administradores de monitorarem e acompanharem possíveis problemas de forma eficaz.

Essas questões indicam a necessidade de melhorias significativas em nosso sistema para atender às demandas dos administradores de redes.

4.2 SOLUÇÃO

O protocolo SNMP (Simple Network Management Protocol) foi amplamente utilizado no desenvolvimento da solução devido às suas funcionalidades robustas, como monitoramento de desempenho, detecção e resolução de falhas, além de notificação de eventos. Suas capacidades permitiram uma abordagem eficaz para a gestão e supervisão de redes, proporcionando uma compreensão detalhada de seu funcionamento interno. Dentre os diversos componentes que integram o protocolo, destaca-se o NMS (*Network Management Systems*), que desempenha um papel central ao monitorar e controlar elementos de rede, como switches e roteadores. Essas "estações de gerenciamento de rede" são essenciais para assegurar o correto funcionamento dos dispositivos conectados, permitindo um gerenciamento eficiente e proativo.

As aplicações do SNMP são observadas em ambientes críticos, como Datacenters, Provedores de Serviços de Internet (ISPs) e no setor de Telecomunicações. No entanto, para o escopo deste trabalho, o foco será direcionado aos ISPs, onde o SNMP é empregado para monitorar o tráfego de rede, a largura de banda disponível, bem como o desempenho geral da infraestrutura de comunicação. Através desta aplicação, torna-se possível garantir maior estabilidade e eficiência nas operações, ao mesmo tempo em que se antecipa a identificação de problemas e a tomada de decisões corretivas, com base em dados precisos e em tempo real.

Por meio do protocolo SNMP, foi possível desenvolver todo o dashboard do sistema, aproveitando suas funções de monitoramento de desempenho, detecção e resolução de falhas, configuração de dispositivos e notificações de eventos, que desempenharam um papel essencial na compreensão e eficácia da solução implementada. A partir de um estudo aprofundado sobre o protocolo, suas funcionalidades foram integradas ao desenvolvimento das principais funções do sistema, conforme ilustrado na Figura 15, com o objetivo de atender à demanda por dados abrangentes e precisos. Esse recurso permitirá uma análise detalhada de todas as informações disponíveis, capacitando os administradores de rede a identificar padrões e tendências que poderiam passar despercebidos em análises convencionais. Com o acesso facilitado a dados relevantes, será possível resolver problemas de monitoramento de maneira rápida e eficiente, otimizando a gestão da rede.

Figura 15 – Página de monitoramento.

Fonte: Autoria própria (2024).

O dashboard não apenas centraliza informações críticas, mas também proporciona uma visualização intuitiva que facilita a interpretação dos dados. Isso

significa que os usuários poderão rapidamente detectar anomalias, avaliar o desempenho da rede e tomar decisões informadas com base em dados concretos. A capacidade de analisar informações em tempo real permitirá uma resposta ágil a eventuais falhas ou interrupções, minimizando o tempo de inatividade e garantindo uma operação mais estável e confiável.

Além disso, a apresentação visual dos dados em gráficos e tabelas interativas enriquecerá a experiência do usuário, facilitando a comunicação de percepções importantes para a equipe. A implementação desse dashboard representa um avanço significativo na capacidade de monitoramento, contribuindo para a melhoria contínua dos serviços prestados e para a satisfação dos clientes. Assim, a ferramenta se torna um elemento indispensável para otimizar a gestão da rede, promovendo um ambiente mais seguro e eficiente.

Figura 16 – Página de relatórios.

Fonte: Autoria própria (2024).

A implementação de relatórios estruturados em formato de tabela, conforme ilustrado na Figura 16, foi desenvolvida com base em estudos sobre o protocolo SNMP, utilizando sua função de detecção de falhas como referência e suporte. O

principal objetivo dessa solução é permitir que os administradores de TI detectem e resolvam problemas de forma mais eficiente, facilitando a compreensão das informações apresentadas. Além de organizar os dados de maneira clara e acessível, essa abordagem contribui significativamente para a redução da perda de informações, um desafio comum enfrentado por muitos provedores de internet.

Com relatórios bem organizados, os administradores terão a capacidade de identificar rapidamente as métricas mais relevantes e, assim, realizar análises mais profundas e informadas. A possibilidade de imprimir esses relatórios para uma avaliação minuciosa é um recurso adicional que agrega valor à ferramenta, permitindo que os usuários conduzam uma revisão detalhada e compartilhem os resultados com suas equipes.

Essa funcionalidade não só promove uma maior transparência nas operações, mas também assegura que decisões baseadas em dados sejam tomadas com mais eficácia. Ao facilitar a análise, os relatórios em tabela desempenham um papel crucial na melhoria contínua dos serviços, permitindo que os provedores de internet respondam proativamente a desafios e otimizem suas operações. Assim, a utilização desses relatórios não só aprimora a qualidade do monitoramento, mas também contribui para uma gestão mais eficiente e estratégica da rede.

A implementação de alertas, conforme demonstrado na Figura 17, utiliza o protocolo SNMP para proporcionar uma compreensão aprofundada sobre a origem dos problemas que possam surgir na rede. Como uma ferramenta robusta de gerenciamento, o SNMP tem como objetivo auxiliar na administração geral e segura da rede. Um dos seus principais recursos é a funcionalidade de notificações de eventos, que permite aos dispositivos enviar alertas, conhecidos como traps SNMP, aos administradores quando surgem situações que requerem atenção. Esses alertas não apenas informam sobre a ocorrência de falhas, mas também fornecem informações contextuais detalhadas, facilitando a compreensão das circunstâncias em que os problemas se manifestaram e possibilitando uma resolução mais eficaz.

Com essa compreensão detalhada, os administradores são capacitados a identificar a raiz do problema com maior precisão, o que possibilita a formulação de soluções eficazes e a resolução de um ou mais problemas de maneira ágil e eficiente. A capacidade de agir rapidamente em resposta a alertas bem definidos

pode minimizar o impacto de falhas na rede, reduzindo o tempo de inatividade e melhorando a experiência do usuário final.

Figura 17 – Página de alertas e notificações.

Fonte: Autoria própria (2024).

Além disso, essa funcionalidade promove uma abordagem proativa na gestão da rede, permitindo que os administradores não apenas reajam a incidentes, mas também analisem tendências e padrões nos dados de alerta ao longo do tempo. Essa análise pode contribuir para a identificação de áreas que necessitam de melhorias, possibilitando um planejamento estratégico mais eficaz. Em última análise, a utilização de alertas não apenas fortalece a resposta a incidentes, mas também eleva a qualidade e a confiabilidade dos serviços prestados.

5 CONSIDERAÇÕES FINAIS

A análise dos resultados obtidos neste trabalho proporciona percepções valiosas, evidenciando que algumas questões atingiram um percentual de 100%. Isso não apenas demonstra que os objetivos inicialmente estabelecidos foram plenamente alcançados, mas também estabelece uma base sólida para futuras melhorias no sistema. O sucesso em atingir essa taxa máxima de concordância indica que as medidas e funcionalidades implementadas estão em alinhamento com as expectativas e necessidades dos usuários. Entretanto, é importante ressaltar que as questões que obtiveram apenas 50% de resposta positiva não serão descartadas ou negligenciadas. Pelo contrário, elas serão tratadas com especial atenção, pois suas respostas revelam áreas de insatisfação ou ineficiência que necessitam de um trabalho mais aprofundado. Essas questões nos oferecem uma oportunidade valiosa para identificar lacunas e entender melhor os desafios enfrentados pelos usuários, permitindo-nos desenvolver estratégias específicas para aprimorar esses aspectos.

Além disso, essas questões podem servir como referências significativas para estudos futuros, pois refletem preocupações e necessidades que, se bem abordadas, poderão resultar em inovações e melhorias substanciais. Assim, recomenda-se fortemente o desenvolvimento de novas pesquisas que complementem o tema abordado neste trabalho. Uma abordagem particularmente interessante seria a realização de estudos comparativos que investiguem a percepção dos administradores em relação às necessidades expressas pelos clientes. Essa linha de pesquisa pode não apenas elucidar as diferenças nas expectativas e experiências entre as duas partes, mas também ajudar a estabelecer um diálogo construtivo que contribua para a formulação de soluções mais eficazes e direcionadas. Ao promover essa interação, podemos garantir que as melhorias realizadas sejam realmente significativas e alinhadas às demandas do mercado, resultando em um avanço substancial na qualidade dos serviços oferecidos e, consequentemente, na satisfação dos usuários.

REFERÊNCIAS

ALVES, William P. **Linguagem e lógica de programação.** 1. ed. São Paulo: Editora Érica, 2013.

BLOKDYK, Gerardus. **Management information base.** 1. ed. [S.l.]: 5STARCooks, 2020.

CISCO - BRASIL. Cisco - Brasil. Disponível em: https://www.cisco.com/c/pt_br/index.html. Acesso em: 22 mar. 2024.

DOUGLAS, R. Mauro; SCHMIDT, Kevin J. **Essential SNMP.** 2. ed. [S.l.]: O′Reilly, 2005.

JIM, Kurose; ROSS, Keith. **Redes de computadores e a Internet: uma nova abordagem.** 6. ed. São Paulo: Pearson, 2013.

LARRY, Walsh. **SNMP MIB handbook.** [S.l.]: Wyndham Press, 2008.

PERKINS, David. **Understanding SNMP MIBs.** 1. ed. Upper Saddle River, NJ: Prentice Hall, 1996.

TELCOMANAGER. **TelcoManager.** Disponível em: https://www.telcomanager.com/. Acesso em: 13 mar. 2024.

MUNDO TI BRASIL. **Mundo TI Brasil.** Disponível em: https://www.mundotibrasil.com.br/. Acesso em: 13 mar. 2024.

STALLINGS, William. **SNMP, SNMPv2, SNMPv3, and RMON 1 and 2.** 3. ed. [S.l.]: Pearson Índia, 2006.