Managing Internet Access

Lucas Martins Dallabeneta
Dept. de Ciência da Computação
UDESC
Joinville, Santa Catarina
lucas@lmd.com.br

Victor Eduardo Requia
Dept. de Ciência da Computação
UDESC
Joinville, Santa Catarina
victorrequia@gmail.com

Dept. de Ciência da Computação
UDESC
Joinville, Brasil

***Abstract*—Este trabalho apresenta um estudo sobre gerenciamento de redes, com foco na administração de switches utilizando mensagens SNMP. Foi implementado um sistema de monitoramento e desligamento de portas de switch, oferecendo funcionalidades úteis para administradores de sistema e professores. O sistema inclui a modelagem de um banco de dados em SQLite, um backend desenvolvido em Python com Flask e um frontend em React. As principais funcionalidades incluem a obtenção do estado das portas do switch, indicando se estão abertas ou fechadas, e fornecendo informações sobre o endereço físico (MAC) das máquinas conectadas. Adicionalmente, foram implementadas funcionalidades para o gerenciamento de usuários, administradores, salas de aula e computadores, além do agendamento de desligamento de computadores. Este projeto proporcionou uma compreensão aprofundada do funcionamento do switch, do protocolo SNMP e dos conceitos de redes, especialmente as configurações de endereços IP.**

***Index Terms*—SNMP, Gerenciamento de Redes, Sistema de Gerenciamento, Monitoramento, MIB**

I. Introdução

O controle de acesso à Internet em ambientes educacionais é um desafio significativo para administradores de redes, especialmente em laboratórios de ensino. Nestes ambientes, a Internet é uma ferramenta essencial, mas precisa ser restrita durante avaliações ou atividades que não devem ser realizadas com consultas na *web*. Neste contexto, a necessidade de um sistema eficiente de gerenciamento de acesso à Internet é relevante e evidente.

Existem várias maneiras de impor restrições à Internet, como o uso de software através de firewalls ou bloqueios de endereços IP não permitidos, ou via hardware, desconectando manualmente o usuário da rede via cabo. Este trabalho propõe a implementação de um sistema de controle de acesso via software, controlando as portas de um switch real com acesso à Internet na rede da UDESC em Joinville, utilizando tecnologias como SNMP (Simple Network Management Protocol), MIB e uma interface *web* para gerenciamento.

A proposta visa criar um ambiente onde o professor, através de uma máquina autorizada, possa controlar o acesso à Internet de outras máquinas em uma sala de aula ou laboratório, abrindo ou fechando portas em um switch real. O sistema permite o bloqueio ou desbloqueio do acesso à Internet de forma agendada ou instantânea. A interface *web* deve ser acessível apenas a partir da máquina do professor, onde é feita uma verificação de endereço MAC para garantir que apenas o computador registrado possa gerenciar os agendamentos. Este controle é implementado através de um processo agendador no Linux (CronTab) e de um gerente SNMP, que envia comandos para o *switch* da rede, possibilitando o bloqueio ou desbloqueio das portas físicas de conexão.

Além disso, este sistema pode ser expandido para incluir monitoramento e relatórios de uso de rede, possibilitando aos administradores identificar padrões de uso inadequados ou suspeitos, melhorando a segurança e eficiência da rede educacional. A implementação de um sistema de controle de acesso tão robusto não apenas melhora a gestão de recursos educacionais, mas também prepara os alunos para uma utilização consciente e responsável da Internet

II. Trabalhos Relacionados

A presente seção discute pesquisas relacionadas ao uso do SNMP para o gerenciamento de redes, com foco na gestão de acesso à internet.

Segundo [1], o gerenciamento de redes de computadores é uma necessidade crescente devido à expansão dos dispositivos e tecnologias de rede nas empresas modernas. Os autores analisaram o uso do Zabbix em conjunto com o protocolo SNMP para centralizar a gestão de redes e reduzir custos. O gerenciador Zabbix, combinado com o SNMP, não apenas monitoriza e controla os dispositivos de rede, mas também antecipa e resolve problemas, melhorando a resiliência da rede. Os autores de [1] propõem uma metodologia onde o sistema detecta anomalias pré-determinadas e toma ações corretivas automaticamente, minimizando a indisponibilidade do sistema. Esta abordagem é relevante em ambientes com um grande número de dispositivos de rede, onde o gerenciamento centralizado é crucial para a eficiência operacional. A pesquisa de [1] é relevante pois demonstra uma aplicação prática e eficiente do protocolo em conjunto com ferramentas de monitoramento para melhorar a gestão e a resiliência das redes corporativas.

[2] discutem a importância crescente do SNMP na gestão de redes industriais, ressaltando sua aplicação na monitorização e controle de dispositivos de automação, como Controladores Lógicos Programáveis (CLPs) e outros ativos de rede. Com a integração cada vez maior entre as tecnologias de automação e tecnologia da informação, o uso do SNMP torna-se crucial para garantir o desempenho e a confiabilidade das redes industriais. O artigo enfatiza que, em ambientes industriais, o SNMP facilita a coleta de dados em tempo real, diagnóstico de problemas e gerenciamento de mudanças, promovendo uma

abordagem proativa para a manutenção da rede. A capacidade do SNMP de fornecer informações detalhadas sobre o status dos dispositivos e a performance da rede permite antecipar falhas e implementar ações corretivas rapidamente, minimizando o impacto na operação. A aplicação do SNMP para monitorar e gerenciar o desempenho da rede e a disponibilidade dos serviços é crucial para a manutenção da qualidade do acesso à Internet.

Outro estudo relevante é o do Eagle Network, que apresenta uma solução para o gerenciamento de redes utilizando SNMP, ITIL e CobIT, além de técnicas de Business Intelligence e Inteligência Artificial para apoiar as decisões do administrador da rede. O sistema proposto é dividido em dois módulos, onde o primeiro realiza operações de coleta de dados e o segundo trata esses dados, transformando-os em informações úteis para apoio às decisões. Este estudo demonstra a eficácia do uso de SNMP em conjunto com metodologias de gerenciamento de TI para criar um sistema robusto e adaptável a diversas plataformas

Esses trabalhos mostram que o uso do SNMP é amplamente aceito e aplicado em diversos contextos de gerenciamento de redes, desde ambientes corporativos até industriais, destacando sua flexibilidade e eficiência na coleta e monitoramento de dados em tempo real. Além disso, o protocolo SNMP pode ser integrado com outras tecnologias emergentes, como a inteligência artificial e a análise de big data, para criar soluções ainda mais sofisticadas e proativas na gestão de redes.

III. Desenvolvimento

O desenvolvimento da solução de controle de acesso à Internet iniciou-se com a utilização de Node.js no backend e React no frontend. No entanto, devido a problemas com bibliotecas desatualizadas e a ausência de tipagem adequada, foi decidido migrar para Python com Flask no backend. O Flask foi escolhido por permitir a criação de rotas de forma simples e eficiente. Para o banco de dados, optou-se pelo SQLite, uma solução leve e fácil de configurar. Inicialmente, foi considerado o uso do Firebase Realtime Database, mas essa opção foi descartada devido a limitações técnicas encontradas durante a implementação. Toda a implementação ocorreu em um computador com Linux e SNMP instalado conforme tutorial na página do Moodle, dispensando o uso da máquina virtual disponibilizada pelo professor da disciplina por ter problemas de desempenho e desatualizações do sistema operacional. A seguir, são apresentadas as principais tecnologias e ferramentas utilizadas no desenvolvimento do sistema:

A. Backend

O backend, responsável pela comunicação de obtenção e armazenamento dos dados da aplicação, foi desenvolvido utilizando o Flask, um microframework em Python conhecido por sua simplicidade e eficiência na criação de rotas e manipulação de requisições HTTP. A utilização do Flask permitiu a criação rápida de várias rotas, como as rotas *POST* para a criação de usuários, salas, computadores e administradores, e as rotas *GET* para a recuperação de informações sobre esses componentes.

Na proposta inicial do trabalho, previa-se o uso do CronTab (Linux) para tarefas agendadas. No entanto, foi decidido implementar uma *thread* no servidor do backend para verificar se há mudanças no banco de dados. Esse tipo de abordagem permitiu verificar continuamente se era necessário desbloquear a porta de um computador em horários específicos, melhorando a resposta do uso de datas no agendamento dos desligamentos das portas do switch.

B. Frontend

O frontend, responsável por exibir de maneira amigável e elegante as informações para o usuário e enviar dados do usuário para o backend, inicialmente considerou o uso da tecnologia React. Devido aos problemas encontrados durante o desenvolvimento, decidiu-se simplificar utilizando tecnologias básicas como HTML, CSS e JavaScript. Essa abordagem permitiu focar na funcionalidade principal sem preocupações com compatibilidade de bibliotecas desatualizadas. Toda a comunicação do frontend com o backend é realizada utilizando requisições HTTP.

C. Banco de Dados

O banco de dados do sistema foi projetado utilizando SQLite, um sistema de gerenciamento de banco de dados relacional leve e amplamente utilizado para protótipos rápidos e funcionais. O SQLite foi escolhido devido à sua simplicidade de configuração, baixo consumo de recursos e facilidade de uso, tornando-o ideal para este projeto. Abaixo estão as definições das tabelas principais utilizadas, com uma breve descrição de seus campos e finalidades:

A tabela `users` armazena informações sobre os usuários do sistema. Cada usuário possui um identificador único, um nome de usuário e uma senha.

1) Tabela `users`:

```
CREATE TABLE IF NOT EXISTS users (
    id INTEGER PRIMARY KEY AUTOINCREMENT,
    username TEXT NOT NULL UNIQUE,
    password TEXT NOT NULL
);
```

A tabela `port_blocks` gerencia os agendamentos de bloqueio de portas do switch, armazenando as informações sobre quais portas serão bloqueadas e em que intervalos de tempo.

2) Tabela `port_blocks`:

```
CREATE TABLE IF NOT EXISTS port_blocks (
    id INTEGER PRIMARY KEY AUTOINCREMENT,
    port INTEGER NOT NULL,
    startDate TEXT NOT NULL,
    endDate TEXT NOT NULL
);
```

A tabela `administradores` armazena informações sobre os administradores do sistema. Cada administrador possui um identificador único e um nome de usuário.

3) Tabela `administradores`:

```
CREATE TABLE IF NOT EXISTS administradores(
    id INTEGER PRIMARY KEY AUTOINCREMENT,
    username TEXT NOT NULL UNIQUE
);
```

A tabela `salas` gerencia as informações sobre as salas de aula. Cada sala possui um identificador único, um nome e está associada a um administrador.

4) Tabela `salas`:

```
CREATE TABLE IF NOT EXISTS salas (
    id INTEGER PRIMARY KEY AUTOINCREMENT,
    nome TEXT NOT NULL UNIQUE,
    admin_id INTEGER,
    FOREIGN KEY (admin_id)
    REFERENCES administradores (id)
);
```

A tabela `computadores` armazena informações sobre os computadores em cada sala de aula. Cada computador possui um identificador único, endereço MAC, número da porta do switch, status, uma descrição opcional e está associado a uma sala.

5) Tabela `computadores`:

```
CREATE TABLE IF NOT EXISTS computadores (
    id INTEGER PRIMARY KEY AUTOINCREMENT,
    mac_address TEXT NOT NULL UNIQUE,
    port INTEGER NOT NULL,
    status TEXT NOT NULL,
    description TEXT,
    sala_id INTEGER,
    FOREIGN KEY (sala_id)
    REFERENCES salas (id)
);
```

Essas tabelas foram projetadas para assegurar a integridade dos dados e a eficiência nas operações de consulta e atualização, facilitando o gerenciamento do sistema de controle de acesso à Internet em um ambiente educacional.

IV. Conclusões e Resultados

Neste trabalho, o sistema de monitoramento e desligamento de portas do switch foi implementado com sucesso, proporcionando várias funcionalidades úteis tanto para administradores de sistema quanto para professores.

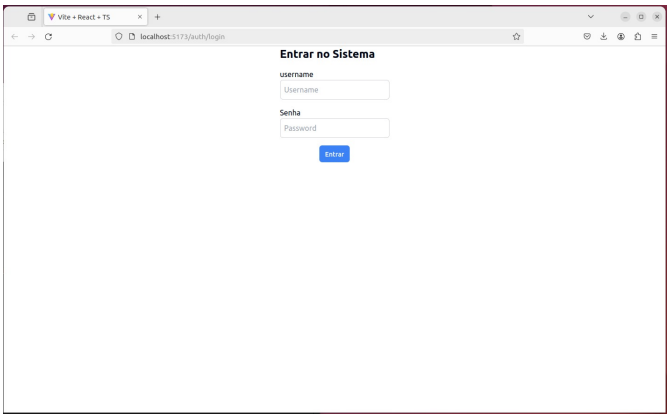
Além da modelagem de um banco de dados em SQLite, desenvolvimento de um backend em Python e do frontend em React, desenvolvemos funções que permitem a obtenção do estado de todas as portas do switch estudado, indicando se estão abertas (representadas em verde na interface gráfica) ou fechadas (representadas em vermelho na interface gráfica). Além disso, o sistema fornece informações detalhadas sobre o endereço físico (MAC) das máquinas conectadas às portas ativas do switch.

Implementamos também uma tela de login para o usuário administrador e uma série de funcionalidades adicionais, tais como: adicionar novos usuários e administradores, criar novas salas de aula, adicionar computadores às salas de aula, desligar todos os computadores de uma sala específica, desligar computadores individuais, agendar o desligamento de computadores, cancelar agendamentos, e ligar imediatamente uma porta do switch que tenha sido bloqueada.

As telas implementadas no frontend que fazem comunicação com o backend são mostradas a seguir:

Na Figura 1, é possível ver a tela de login desenvolvida. Ela permite que os administradores entrem no sistema de maneira segura através de um usuário criado via método POST para adicionar o usuário como administrador no banco de dados.

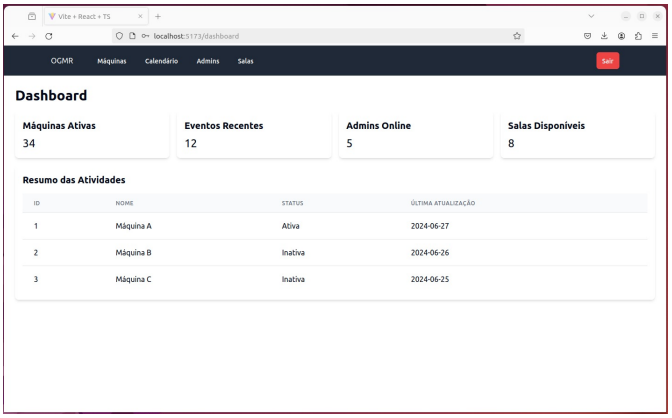
Fig. 1. Tela de Login.



Fonte: Próprios autores.

Na Figura 2, é mostrado um exemplo de tela desenvolvida como dashboard para visualização de todos os dados de maneira geral. Essa tela pode ser utilizada para implementação prática em trabalhos futuros, sendo nesse trabalho, implementada apenas a interface sem a comunicação ou obtenção de dados reais.

Fig. 2. Tela Principal (Dashboard)

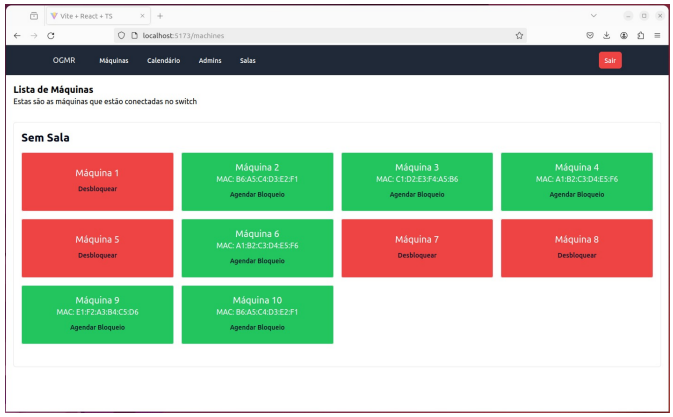


Fonte: Próprios autores.

Na Figura 3, é apresentado a tela onde é possível visualizar

uma matriz de cartões, representando todas as portas do switch, incluindo as portas abertas (cartão de visualização verde) e portas fechadas (cartão de visualização vermelho). Nessa tela, também é possível observar que o sistema desenvolvido também mostra o endereço MAC das máquinas conectadas nas portas ligadas do switch, a opção de agendamento, detalhado na Figura 5, a opção de desbloquear as portas bloqueadas do switch imediatamente e a opção de bloquear todas as portas de uma sala em um único botão.

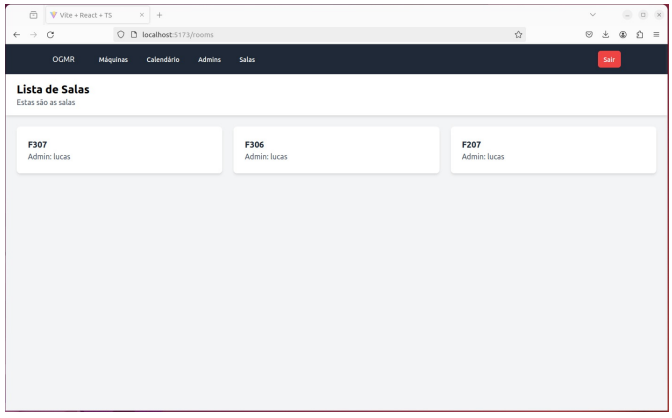
Fig. 3. Tela das Máquinas



Fonte: Próprios autores.

A Figura 4 mostra a tela para visualizar todas as salas cadastradas no sistema. Nela é possível ver todas as salas que estão salvas no banco de dados através de requisições pelo método POST para cadastrar as salas. Cada sala tem um usuário que deve ter permisão de administrador para cadastrar uma sala. Na interface gráfica, além do nome da sala, o nome do usuário administrador que criou a sala também aparece.

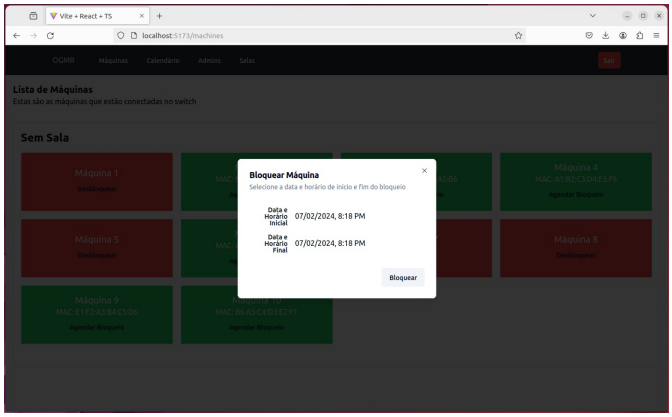
Fig. 4. Tela da Lista de Salas



Fonte: Próprios autores.

Na Figura 5, é possível ver a tela de agendamentos. Nessa tela, o administrador escolhe o início e o fim do dia e horário do bloqueio de uma porta específica. Após apertar no botão para confirmar o bloqueio por agendamento, será enviada a requisição para o backend pelo método POST para a rota reposnável por bloquear a porta durante o tempo definido. A data e horário de ínicio e fim do bloqueio são armazenadas no banco de dados também.

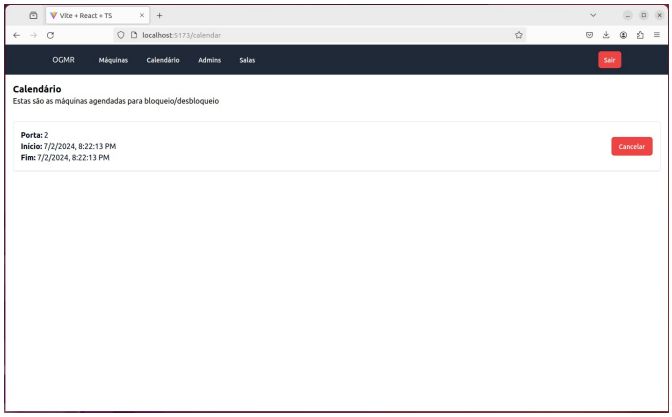
Fig. 5. Tela de Agendamento



Fonte: Próprios autores.

Na Figura 6, é possível observar a tela que mostra todos os agendamentos feitos para desligamento de portas. Nessa tela, também é possível realizar o cancelamento do agendamento caso necessário.

Fig. 6. Tela de Agendamento



Fonte: Próprios autores.

Como conclusão, este trabalho permitiu uma compreensão aprofundada do funcionamento do switch estudado e dos detalhes operacionais da MIB, bem como do fluxo de mensagens SNMP e das chamadas Get e Set no switch via SNMP. Também aplicamos os conhecimentos de gerenciamento adquiridos em sala para desenvolver e modelar o sistema. Além disso, absorvemos conceitos importantes de redes durante o estudo das configurações de rede do switch, especialmente no que diz respeito à configuração de endereços IP.

REFERENCES

[1] SILVA, W.M.C.; MEDEIROS, R.M.; MARTINS, R.S. Análise e gerenciamento de redes usando uma metodologia proativa com Zabbix. HOLOS, v. 8, 2015, pp. 277-289. Instituto Federal de Educação, Ciência e Tecnologia do Rio Grande do Norte

[2] FONSECA, Marcos de Oliveira et al. Monitoração do desempenho de redes de automação usando SNMP. Tecnologia em Metalurgia, Materiais e Mineração, v. 3, n. 1, p. 1-6, 2013.

[3] DOMINGOS, T., PEREIRA, S., REIS, D., SILVA, C., BARRÉRE, E. Gerenciamento de uma rede através do Protocolo SNMP. II Simpósio de Excelência em Gestão e Tecnologia – SEGeT, 2005, pp. 964-973. Disponível em: https://www.aedb.br/seget/arquivos/artigos05/335_EAGLE_SEGET.pdf