UNIVERSIDADE TECNOLÓGICA FEDERAL DO PARANÁ

DEPARTAMENTO ACADÊMICO DE INFORMÁTICA

CURSO DE ESPECIALIZAÇÃO EM REDES DE COMPUTADORES

GIOVANI FABRIS MARCARINI

IMPLANTAÇÃO DE FERRAMENTA PARA GERÊNCIA DA REDE LÓGICA DO COLÉGIO MATER DEI

MONOGRAFIA DE ESPECIALIZAÇÃO

PATO BRANCO

2018

GIOVANI FABRIS MARCARINI

IMPLANTAÇÃO DE FERRAMENTA PARA GERÊNCIA DA REDE LÓGICA DO COLÉGIO MATER DEI

Monografia de especialização apresentada ao III Curso de Especialização em Redes de Computadores – Configuração e Gerenciamento de Servidores e Equipamentos de Rede, do Departamento Acadêmico de Informática, da Universidade Tecnológica Federal do Paraná, Câmpus Pato Branco, como requisito parcial para obtenção do título de Especialista.

Orientador: MEng. Anderson Luiz Fernandes

PATO BRANCO

2018

Ministério da Educação
Universidade Tecnológica Federal do Paraná
Câmpus Pato Branco
Departamento Acadêmico de Informática
III Curso de Especialização em Redes de Computadores

TERMO DE APROVAÇÃO

IMPLANTAÇÃO DE FERRAMENTA PARA GERÊNCIA DA REDE LÓGICA DO COLÉGIO MATER DEI

por

Giovani Fabris Marcarini

Esta monografia foi apresentada às 09h30min do dia 24 de novembro de 2018, como requisito parcial para obtenção do título de ESPECIALISTA, no III Curso de Especialização em Redes de Computadores – Configuração e Gerenciamento de Servidores e Equipamentos de Redes, da Universidade Tecnológica Federal do Paraná, Câmpus Pato Branco. O acadêmico foi arguido pela Banca Examinadora composta pelos professores abaixo assinados. Após deliberação, a Banca Examinadora considerou o trabalho **aprovado**.

Prof. M. Eng. Anderson Luiz Fernandes
Orientador / Faculdade Mater Dei

Prof. Dr. Fábio Favarim
UTFPR-PB

Prof. Dr. Eden Ricardo Dosciatti
UTFPR-PB

Prof. Dr. Fábio Favarim
Coordenador do III Curso de Especialização
em Redes de Computadores

A Folha de Aprovação assinada encontra-se na Coordenação do Curso.

RESUMO

MARCARINI, F G. Implantação de ferramenta para gerência da rede lógica do Colégio Mater Dei. 2018. 46 f. Monografia (Especialização em redes de Computadores) – Departamento Acadêmico de informática, Universidade Tecnológica Federal do Paraná, Câmpus Pato Branco, 2018.

Este trabalho trata da implantação de uma ferramenta para a gerência e monitoramento da rede lógica do Colégio Mater Dei. O uso do protocolo SNMP permite que equipamentos de diversos fabricantes possam ser gerenciados através de um único sistema, o que é uma facilidade para trabalhar com a vasta heterogeneidade de equipamentos atualmente encontrados. A utilização de uma ferramenta para a gerência e monitoramento, fornece dados para a equipe responsável com eventuais problemas, minimizando assim o impacto do usuário final com a rapidez na solução do problema, uma vez que o estado atual da rede pode ser facilmente verificado e também alertas podem ser configurados para serem emitidos de forma automática caso ocorra alguma anomalia na rede. Com a ferramenta de gerenciamento de redes, os esforços exigidos pelos responsáveis, para o perfeito funcionamento da rede, serão minimizados e os eventuais problemas, solucionados de maneira mais eficiente, garantindo assim maior satisfação do usuário final.

Palavras-chaves: SNMP, Gerenciamento de rede, satisfação do usuário, diagnóstico preciso.

ABSTRACT

MARCARINI, F G. Implementation of tool for management of the logical network of Mater Dei College. 2018. 46 f. Monograph (Specialization in Computer Networks) - Academic Department of Informatics, Federal Technological University of Paraná, Campus Pato Branco, 2018.

This paper deals with the implementation of a tool for the management and monitoring of the logical network of the Mater Dei College. The use of the SNMP protocol allows equipment from several manufacturers to be managed through a single system, which is a facility to work with the vast heterogeneity of equipment currently encountered. The use of a tool for management and monitoring provides data to the responsible team with possible problems, thus minimizing the impact of the end user with the speed in solving the problem, since the current state of the network can be easily verified, and alerts can also be configured to be issued automatically if any anomalies occur. With the network management tool the efforts required by those responsible for the perfect functioning will be minimized and any problems solved more efficiently, ensuring greater end-user satisfaction.

Keywords: SNMP, Network management, user satisfaction, accurate diagnosis.

LISTA DE ABREVIATURAS, SIGLAS E ACRÔNIMOS

ASN.1	*Abstract Syntax Notation One*
DHCP	*Dynamic Host Configuration Protocol*
IETF	*Internet Engineering task Force*
LAN	*Local Area Network*
MAC	*Media Access Control*
MIB	*Management Information Base*
OID	*Object Identifier*
OSI	*Open System Interconnection*
PDU	*Protocol Data Units*
PING	*Packet Internet Network Grouper*
POE	*Power over Ethernet*
QoS	*quality of service*
SMI	*Structure of Management*
SNMP	*Simple Network Management Protocol*
UDP	*User Datagram Protocol*
VLAN	*virtual local área network*
VOIP	*voice over internet protocol*

LISTA DE FIGURAS

LISTA DE QUADROS

SUMÁRIO

1. INTRODUÇÃO

Neste capítulo são apresentadas as considerações iniciais sobre redes de computadores, objetivos e motivos que justificam a construção deste trabalho.

1.1 CONSIDERAÇÕES INICIAIS

Nos primórdios das redes de computadores, quando elas eram usadas para finalidades restritas e não para uma infraestrutura com milhões de usuários, o gerenciamento de redes era algo que nunca se tinha ouvido falar. Se alguém por ventura descobrisse um problema, o famoso PING (*Packet Internet Network Grouper*) poderia ser utilizado para localizar a fonte deste problema e em seguida modificar os ajustes para sanar o ocorrido (KUROSE, 2013).

Com a grande evolução das redes e consequentemente da tecnologia, a busca por confiabilidade, disponibilidade e principalmente à segurança dos dados trafegados nas redes de computadores se torna uma busca incessante, e como consequência obriga empresas a adequarem suas redes de maneira eficiente visando aumentar a disponibilidade e produtividade.

Contudo, a complexidade para a administração das redes aumenta a cada novo serviço que é ligada a ela, e para isso é de fundamental a utilização de sistemas para gerenciamento e monitoração da rede.

O gerenciamento de redes envolve cinco áreas funcionais (ISO/IEC 7498):

- Gerência de configuração: é fundamental para a configuração inicial da rede descobrindo a topologia e monitorando a alternância de topologias físicas e lógicas da rede.
- Gerência de falhas: tem por objetivo o diagnóstico e a detecção de falhas no ambiente de rede.
- Gerência de desempenho: permite ao administrador analisar o desempenho da rede e permite o planejamento de capacidade da rede.
- Gerência de segurança: objetiva a proteção dos ativos da rede, monitorando violações nas políticas de segurança implementadas.

- Gerência de contabilidade: se responsabiliza por verificar a utilização dos recursos da rede por seus usuários.

Todas as cinco áreas elencadas desempenham funções cruciais que o ambiente de rede desempenhe sua total capacidade de comutação.

O grande e constante crescimento das redes de computadores, fez com que novas técnicas para o gerenciamento e detecção de falhas fossem implementadas visando a complexidade encontrado nos cenários atuais, que quando se compara aos cenários dos primórdios das redes de computadores percebe-se que um simples “ping” já não é mais viável para detectar falhas com rapidez dentro de uma rede (KUROSE, 2013).

O gerenciamento de redes envolve diversas atividades para o bom funcionamento de uma rede de computadores, em outras palavras, encarrega-se de monitorar e afirmar que todos os elementos tanto físicos como lógicos estejam operando adequadamente a fim de na medida do possível, se ter um nível considerável de qualidade de serviço (ROSE, 1996).

Ao longo dos últimos anos os equipamentos passaram a oferecer cada vez mais possibilidades para gerenciar, com o intuito de facilitar as detecções de falhas e a visualização de eventos dentre outras. Com a crescente evolução no setor, empresas que fabricam esses equipamentos já possuem seus próprios protocolos e ferramentas para a monitoração, contudo é difícil a implementação de uma linha de equipamentos específica em redes de pequenas e médias empresas principalmente pelo custo que acaba sendo mais elevado do que manter uma heterogeneidade de equipamentos dentro da rede.

Para este projeto destaca-se o protocolo SNMP (*Simple Network Management Protocol*), protocolo este escolhido para ser usado na implementação por ser um protocolo de comunicação padrão, utilizado por praticamente todos os fabricantes além de seus protocolos proprietários oferecem suporte a ele.

O protocolo SNMP é um protocolo Padrão da IETF (*Internet Engineering task Force*), e pertencente a camada de aplicação do modelo OSI (*Open System Interconnection*), (TANENBAUM, 2011) e utiliza na camada de transporte o UDP (*User Datagram Protocol*), para enviar as suas requisições através da rede IP, assim cada dispositivo a ser gerenciado é chamado de nodo gerenciado.

Uma rede de computadores após ser concebida, naturalmente com o decorrer do tempo terá uma quantidade de equipamentos ligados a ela cada vez maior, é necessário simplificar o

processo de gerência. Dessa forma o protocolo SNMP pode ser usado para a gerência dos equipamentos ligados a rede de uma forma mais ágil.

1.2 OBJETIVOS

1.2.1 Objetivo Geral

Implantar um sistema de monitoramento e gerenciamento na rede lógica do Colégio Mater Dei, para monitorar o fluxo e o tráfego de dados, bem como a atividade dos equipamentos conectados.

1.2.2 Objetivos Específicos

- Avaliar qual o melhor sistema de gerenciamento baseado em software livre para a rede de uma escola;
- Identificar, em tempo real, o fluxo de dados da rede;
- Centralizar o gerenciamento, de forma a identificar anomalias na rede;
- Manter a lista de equipamentos em constante atualização;
- Disponibilizar informações para melhorar a expansão da rede lógica.

1.3 JUSTIFICATIVA

A utilização de um sistema de gerenciamento de equipamentos e aviso de falhas dos ativos da rede, permitirá explorar e aplicar protocolos estudados e explanados, em sala, durante o andamento da especialização em redes de computadores, no câmpus da UTFPR em Pato Branco.

O Colégio Mater Dei é uma empresa que vem crescendo e se destacando na sociedade pela imersão da tecnologia em sala de aula, contudo, preza pela qualidade dos serviços ofertados aos seus alunos e funcionários. O gerenciamento da rede lógica, no entanto, será mais um ponto positivo para a equipe de informática sustentar a qualidade dos serviços por ela ofertada.

O gerenciamento de redes permite avaliar diversos fatores, um deles e talvez o principal é a largura de banda contratada junto ao provedor, é possível gerar gráficos de consumo por determinados períodos/dispositivos, sendo muito comum encontrar dispositivos com grandes

consumos desnecessários. Nesses casos os gráficos auxiliam na tomada de decisão para corte parcial, otimizando recursos e diminuindo a banda para dentro da faixa adequada.

Muitos outros pontos positivos no gerenciamento se dão através dos avisos de falhas dos ativos de rede, sendo possível receber e-mails quando um determinado dispositivo parar de funcionar corretamente ou até mesmo quando o sistema identificar anomalias nos enlaces entre os ativos. Também permite gerar arquivos de *log* contendo detalhes dos serviços que estão aparentando problemas para análise posterior.

Com este trabalho, pretende-se documentar todo processo de escolha da ferramenta de gerenciamento e a trajetória de implantação da mesma. Ao final, este trabalho poderá servir como material de referência para pesquisa e apoio para outros trabalhos que pretendam implementá-la em projetos similares.

1.4 ESTRUTURA DO TRABALHO

O presente trabalho, está dividido em capítulos, de forma que apresente uma melhor abordagem sequencial para implantação de um sistema de gerenciamento em redes de computadores.

No Capítulo 2 é feito o levantamento e embasamento teórico sobre o gerenciamento de redes. A definição do sistema de gerenciamento e o protocolo a ser usado são os principais itens abordados. A finalização deste capítulo contempla os fatores principais na administração dos dispositivos em uma rede de computadores.

O Capítulo 3 contempla a descrição dos materiais e métodos utilizados para o desenvolvimento deste experimento.

O Capítulo 4 traz os resultados obtidos com a aplicação dos métodos adotados, aonde as atividades são reproduzidas e detalhadas de forma sequencial para reproduções futuras.

No Capítulo 5 são apresentadas as considerações finais do trabalho bem como os resultados colhidos com a implementação.

No Capítulo 6 apresenta-se uma estimativa para futuras implementações, visando sempre a melhor qualidade de serviço oferecido.

2. REFERENCIAL TEÓRICO

Para começar, uma pergunta muito frequente: “o que é gerenciamento de redes? ”. Para (SAYDAM, 1996) o gerenciamento de redes inclui a implementação, a integração e a coordenação de elementos de hardware, software e humano, tendo por objetivo testar, consultar, configurar, analisar, avaliar e controlar todos os recursos disponíveis em uma rede de computadores, satisfazendo as exigências operacionais, de desempenho e de qualidade de serviço com um custo razoável.

Para uma melhor definição de uma área a ser gerenciada, (CASTELI, 2004) diz que uma LAN (*Local Areal Network*) pode ser definida como um conjunto de computadores de uma empresa ou ambientes interconectados geograficamente, podendo ser definida atualmente uma LAN pertencente a um mesmo grupo de domínio *broadcast* e administrada por uma única organização.

Para o gerenciamento existe a exigência e a capacidade de monitorar, consultar, analisar, configurar e controlar os componentes da rede. Para (KUROSE, 2013) a forma como os dispositivos de redes é distribuída na topologia não tem relevância, exigirá que o administrador consiga no mínimo coletar dados de um elemento remoto e também efetuar mudanças, tendo como exemplo para a coleta de dados, o monitoramento, e para a efetivação de mudanças, o controle.

2.1 ARQUITETURA DE UM SISTEMA DE GERENCIAMENTO

A arquitetura de um sistema de gerência de redes é conceitualmente idêntica a uma organização humana. Há aqui três componentes principais na arquitetura: uma entidade gerenciadora (o chefe, na analogia apresentada) e os dispositivos gerenciados (as filiais) e por fim o terceiro item crucial a integração de um protocolo para a comunicação entre a entidade gerenciadora e os dispositivos gerenciados (KUROSE, 2013).

A entidade gerenciadora consiste em ser uma aplicação que no geral é executada em uma central de gerenciamento de rede “Servidor de gerenciamento”. Para (KUROSE, 2013) ela é o centro das atividades, é ela quem controla e coleta os dados das entidades gerenciáveis e

apresenta as informações para o administrador da rede, seja em forma de gráficos em monitores, alertas por e-mail, mensagens para o celular, enfim, é ela quem tem a responsabilidade de identificar as anomalias e apresentar ao administrador.

Kurose (2013) diz que é na central de gerenciamento que são iniciadas as ações de controle de comportamento dos ativos gerenciáveis e é nesse momento que o administrador humano interage com os dispositivos da rede.

Um dispositivo gerenciado é um dos vários equipamentos que reside em uma rede gerenciada, incluindo o seu software. Exemplos de hospedeiros gerenciados podem ser, impressoras, roteador, switch dentre outros diversos, podendo haver em seu interior vários objetos a serem gerenciados propriamente ditos como as peças do hardware (KUROSE, 2013).

Esses objetos gerenciados, tem informações ligadas a eles coletadas dentro de uma base de informação de gerenciamento, denominada de MIB (*Management Information Base*) especificada pela RFC 3418 (IETF, 2018) a qual trataremos posteriormente.

O terceiro item da arquitetura de gerenciamento é o protocolo de gerenciamento da rede, responsável em fazer a comunicação ente a entidade gerenciadora e os elementos gerenciados. Permite que entidade gerenciadora investigue o estado dos dispositivos gerenciados, indiretamente permite que em alguns casos a entidade gerenciadora execute ações sobre seus elementos gerenciados.

Os itens gerenciados podem usar este protocolo para informar a entidade gerenciadora sobre a ocorrência de eventos, como exemplo falhas de componentes, falhas de desempenho entre outras. É importante destacar que o protocolo de gerenciamento em si não gerencia a rede, faz assim o meio campo entre os dispositivos permitindo que o administrador possa gerenciar, monitorar e testar a rede (KUROSE, 2013).

A Figura 1 apresenta graficamente a estrutura da arquitetura do gerenciamento de redes.

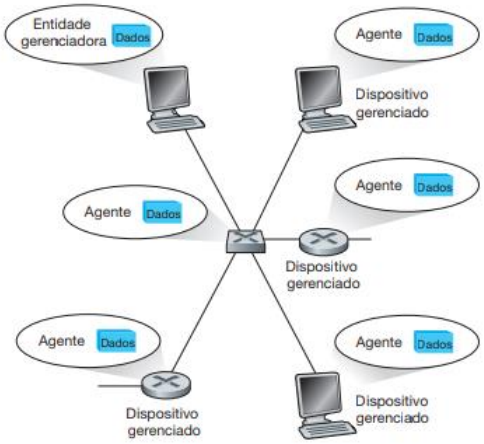

Figura 1. Principais componentes da arquitetura de gerenciamento de redes
Fonte: (KUROSE, 2013)

Pode-se ter noção dos três pilares da arquitetura de gerenciamento, citados por Kurose (2013), que são: a entidade gerenciadora; o agente "protocolo"; e os dispositivos gerenciados.

2.1.1 MIB

Ao contrário do que possa parecer, o gerenciamento de redes é muito mais do que apenas um protocolo para transportar os dados dos dispositivos gerenciados para a entidade gerenciadora, com a evolução constante isso começou a ficar complexo.

A MIB na estrutura de gerenciamento padrão da Internet, é representada por uma coletânea de objetos gerenciados, que juntos formam um banco de dados ou um banco de informações virtuais conhecidas como MIB especificadas na RFC 3418 (IETF, 2018), essas informações coletivamente refletem no estado atual da rede (KUROSE, 2013).

Um objeto MIB pode ser um contador, como um número de um datagramas IP descartados em um roteador por eventuais erros, um número de erros de detecção de porta em uma interface Ethernet entre outros. Além dos contadores pode conter informações descritivas exemplificadas como a versão do software, informações de estado ou informações específicas sobre protocolos e caminhos para roteamento.

A linguagem de definição de dados conhecida como SMI (*Structure of Management Information*) a qual será tratada posteriormente, é usada para definir um modelo de regras para

escrever e revisar as informações de gerenciamento. Objetos MIB são especificados nesta linguagem de definição de dados (KUROSE, 2013).

Basicamente são definidos três tipos de MIB (SILVA, 2018)

- MIB II: é considerara a evolução da MIB I, fornece informações gerais de gerenciamento de um determinado equipamento, através desta MIB II podemos obter informações como número de pacotes transmitidos, status do equipamento, estado da interface entre outros.
- MIB Experimental: é aquela que seus componentes (objetos) ainda então em faze de desenvolvimento e testes, em geral elas oferecem informações mais especificas sobre a tecnologia dos meios de transmissão e equipamentos empregados, é utilizada somente para estudos em laboratório.
- MIB privada: fornecem informações especificas dos equipamentos gerenciados, como configurações, colisão e também é possível reinicializar, desabilitar portas dentre outras configurações nos equipamentos gerenciados. Essa MIB é utilizada por fabricantes que desenvolveram suas próprias ferramenta de gerenciamento de seus dispositivos de rede.

Dentre as três MIBs descritas acima a que mais é utilizada é a MIB II, por ser uma estrutura aberta e facilmente consumida com a utilização do protocolo SNMP, o qual será descrita no decorrer do trabalho.

Para (SILVA, 2018) os objetos são organizados de forma hierárquica em uma espécie de árvore, e são reconhecidos por um OID (*Object Identifier*), sendo a base do esquema de atribuições de nomes do protocolo SNMP.

Um OID é formado por uma sequência de inteiros baseados nos nós da arvore citada, sendo separados por um ponto (.), a Figura 2 apresenta um exemplo da árvore MIB.

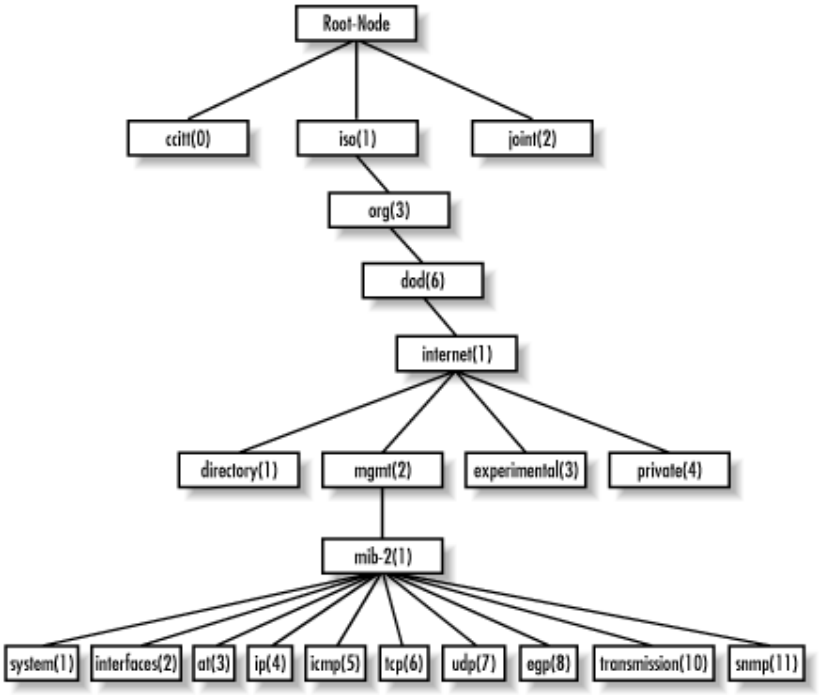

Figura 2. Estrutura da árvore MIB.
Fonte: (SILVA, 2018)

Seguindo a árvore representada na Figura 2, por exemplo, pode-se referenciar uma chamada com o protocolo SNMP ao módulo de interfaces de duas formas. A primeira seria utilizando a referência como “iso.org.dod.internet.mgmt.mib.interfaces”, a segunda forma de fazer a referência seria “1.3.6.1.2.1.2” utilizando assim o número do referencial da árvore.

A MIB, como observada na árvore na Figura 2 é dividida em vários grupos, cada uma responsável por uma parte dos dados que serão armazenados e posteriormente consultados por uma entidade de gerenciamento, os grupos são (SILVA, 2018):

- System: define uma lista de objetos pertencentes as operações do sistema, bem como tempo de funcionamento, contato, nome do sistema etc;
- Interfaces: responsável por rastrear dados de cada interface a ser gerenciada, monitora as interfaces em funcionamento ou mesmo as inativas rastreando aspectos, como exemplo octetos enviados, recebidos, erros entre outros;
- AT: Grupo *Address Translation*, existe para manter a compatibilidade com versões anteriores;
- IP: Rastreia informações relacionadas com diversos aspectos IP, incluído listas de roteamento IP;

- ICMP: responsável por aspectos de erros ICMP;
- TCP: responsável por aspectos como o estado de conexões TCP, exemplos (*Closed, listen*) entre outras;
- UDP: responsável por aspectos estatísticos relacionados ao protocolo UDP;
- EGP: responsável por dados estatísticos sobre o EGP;
- TRANSMISSION: item reservado para MIBs específicas de mídia;
- SNMP: responsável pela avaliação do tráfego SNMP;

Descreve (KUROSE, 2013), como citado anteriormente que o grupo *system* contém as informações gerais do dispositivo gerenciado, e para melhor entendimento o Quadro 1 abaixo define os objetos gerenciados no grupo *system* de acordo com a RFC 1213 (IETF, 2018).

Identificador de objeto	Nome	Tipo	Descrição (segundo rfc 1213)
1.3.6.1.2.1.1.1	Sysdescr	Octet string	"nome completo e identificação da versão do tipo de hardware do sistema, do sistema operacional do software e do software de rede."
1.3.6.1.2.1.1.2	Sysobjectid	Object identifier	Id atribuído pelo fabricante do objeto fornece um meio fácil e não ambíguo para determinar que tipo de objeto está sendo gerenciado.
1.3.6.1.2.1.1.3	Sysuptime	Timeticks	"O tempo (em centésimos de segundo) desde que a parte de gerenciamento de rede do sistema foi reinicializada pela última vez. "
1.3.6.1.2.1.1.4	Syscontact	Octet string	"A pessoa de contato para esse nó gerenciado, junto a informação sobre como contatá-la. "
1.3.6.1.2.1.1.5	Sysname	Octet string	"Um nome atribuído administrativamente para esse nó gerenciado. Por convenção, esse é o nome de domínio qualificado do nó. "
1.3.6.1.2.1.1.6	Syslocation	Octet string	"A localização física do nó. "
1.3.6.1.2.1.1.7	Sysservices	Integer32	Um valor codificado que indica o conjunto de serviços disponível no nó: aplicações físicas (por exemplo, um repetidor), de enlace/sub-rede (por exemplo, ponte), de internet (por exemplo, *gateway* ip), fim a fim (por exemplo, hospedeiro).

Quadro 1. Objetos gerenciados no grupo *system* da MIB II.
Fonte: (KUROSE, 2013)

2.1.2 SMI

A estrutura de informações de gerenciamento “SMI” é a linguem utilizada para definir as informações de gerenciamentos que residem na entidade gerenciada na rede. Essa linguagem é essencial para assegurar que a sintaxe e a semântica dos dados de gerenciamento de rede estejam bem definidas e não aparentem nenhuma ambiguidade (KUROSE, 2013).

O SMI define as instâncias específicas para os dados das entidades gerenciadas de redes, seguindo a RFC 2578 (IETF, 2018), embora a SMI seja baseada em uma linguagem de definição de objetos ASN.1 (*Abstract Syntax Notation One*). O Quadro abaixo representa os onze tipos de dados básicos definidos na RFC 2578 (IETF, 2018).

Tipo de dado	Descrição
Integer	Número inteiro de 32 bits, como definido em asn.1, com valor entre – 231 e 231 – 1, inclusive, ou um valor de uma lista de valores constantes possíveis, nomeados.
Integer32	Número inteiro de 32 bits, com valor entre – 231 e 231 – 1, inclusive.
Unsigned32	Número inteiro de 32 bits sem sinal na faixa de 0 a 232 – 1, inclusive.
Octet string	Cadeia de bytes de formato asn.1 que representa dados binários arbitrários ou de texto de até 65.535 bytes de comprimento.
Object identifier	Formato asn.1 atribuído administrativamente (nome estruturado); veja a seção 9.3.2
Ipaddress	Endereço internet de 32 bits, na ordem de bytes da rede
Counter32	Contador de 32 bits que cresce de 0 a 232 – 1 e volta a 0.
Counter64	Contador de 64 bits
Gauge32	Número inteiro de 32 bits que não faz contagens além de 232 – 1 nem diminui para menos do que 0
Timeticks	Tempo, medido em centésimos de segundo, transcorrido a partir de algum evento.
Opaque	Cadeia asn.1 não interpretada, necessária por compatibilidade com versões anteriores

Quadro 2. Tipos de dados Básicos da SMI
Fonte: (KUROSE, 2013)

A linguagem SMI, além dos tipos de dados Básico, também permite a construção de linguagem de nível mais alta, para isso precisamos definir parâmetros para a comunicação semântica com os nódulos gerenciados.

O primeiro parâmetro é construção do OBJECT-TYPE é usada para especificar os tipos de dados, status e semântica de um objeto gerenciado. A construção objeto OBJECT-TYPE exige a definição de quatro parâmetros (KUROSE, 2013).

- SINTAX: define o tipo de dado básico associado ao objeto.
- MAX-ACCESS: especifica se o objeto gerenciado pode ser lido, escrito, criado ou ter o valor incluído em uma notificação.
- STATUS: demonstra se a definição do objeto atual é válida, obsoleta (quando citada essa definição ela apenas armazena histórico e não é executada), ou desaprovada (armazena histórico como a obsoleta, mas é implementável).
- DESCRIPTION: esse parâmetro contém uma definição textual e é legível ao objeto, ela armazena e deve fornecer todas as informações semânticas necessárias para executá-lo.

A Figura 3 mostra um exemplo de uma construção OBJECT-TYPE.

```
ipSystemStatsInDelivers OBJECT-TYPE
       SYNTAX Counter32
       MAX-ACCESS read-only
       STATUS current
       DESCRIPTION
              "The total number of datagrams successfully
              delivered to IPuser-protocols (including ICMP).

              When tracking interface statistics, the counter
              of the interface to which these datagrams were
              addressed is incremented. This interface might
              not be the same as the input interface for
              some of the datagrams.

              Discontinuities in the value of this counter can
              occur at re-initialization of the management
              system, and at other times as indicated by the
              value of ipSystemStatsDiscontinuityTime."
       ::= { ipSystemStatsEntry 18 }
```

Figura 3. Exemplo de OBJECT-TYPE
Fonte: (KUROSE, 2013)

Esse objeto define um controlador de 32 bits que monitora o número de datagramas IP recebidos no dispositivo gerenciado e entregues com sucesso a um protocolo da camada superior.

O segundo parâmetro é construção do MODULE-IDENTIFY permite que os objetos relacionados entre si sejam agrupados, como um conjunto dentro de um módulo. Seguindo a RFC 4293 (IETF, 2018) que especifica os módulos MIB que define objetos gerenciados para gerenciar implementações IP e seu protocolo ICMP, a RFC 4133 (IETF, 2018) que especifica o módulo MIB para o protocolo UDP.

Comenta (KUROSE, 2013) que além do MODULE-IDENTIFY conter as definições do OBECT-TYPE dos objetos gerenciados dentro do módulo a construção dele ainda contém

informações para documentar informações do contato do autor, data da última atualização, um histórico de revisões e uma descrição em forma de texto do modulo.

A Figura 4 exemplifica a construção do MODULE-IDENTIFY:

```
ipMIB MODULE-IDENTITY
      LAST-UPDATED "200602020000Z"
      ORGANIZATION "IETF IPv6 MIB Revision Team"
      CONTACT-INFO
            "Editor:
            Shawn A. Routhier
            Interworking Labs
            108 Whispering Pines Dr. Suite 235
            Scotts Valley, CA 95066
            USA
            EMail: <sar@iwl.com>"
      DESCRIPTION
            "The MIB module for managing IP and ICMP
            implementations, but excluding their
            management of IP routes.

            Copyright (C) The Internet Society (2006).
            This version of this MIB module is part of
            RFC 4293; see the RFC itself for full legal
            notices."

      REVISION "200602020000Z"
      DESCRIPTION
            "The IP version neutral revision with added
            IPv6 objects for ND, default routers, and
            router advertisements. As well as being the
            successor to RFC 2011, this MIB is also the
            successor to RFCs 2465 and 2466. Published
            as RFC 4293."

      REVISION "199411010000Z"
      DESCRIPTION
            "A separate MIB module (IP-MIB) for IP and
            ICMP management objects. Published as RFC
            2011."

      REVISION "199103310000Z"
      DESCRIPTION
            "The initial revision of this MIB module was
            part of MIB-II, which was published as RFC
            1213."
      ::= { mib-2 48}
```

Figura 4. Exemplo do MODULE-IDENTIFY
Fonte: (KUROSE, 2013).

O terceiro parâmetro é a construção do NOTIFICATION-TYPE, responsáveis por especificar as mensagens de TRAP (ação onde o agente envia uma mensagem para a entidade gerenciadora sem mesmo existir uma requisição) e *InformationRequest* geradas por um nódulo gerenciado na rede para a entidade gerenciadora. Essas informações fazem referência ao item DESCRIPTION citado no primeiro item da construção.

Especifica quando as tais mensagens devem ser enviadas bem como a lista de valores que deve ser incluída na mensagem gerada sendo especificada pela RFC 2578 (IETF, 2018).

2.2 PROTOCOLO SIMPLES DE GERENCIAMENTO DE REDE - SNMP

O protocolo SNMP foi desenvolvido para que dispositivos que utilizam o protocolo IP possam ser gerenciados através de um conjunto de operações simples, utilizando para isso o modelo de gerente/agente (SILVA, 2018).

Comenta (DÉO, 2008) que o SNMP é um protocolo da camada de aplicação, tendo como objetivo principal coletar informações dos dispositivos gerenciáveis na rede sendo responsável por veicular as informações de gerencias (os valores contidos nas MIBs).

Para Kurose (2013) o SNMP é usado para transportar as informações contidas nas MIBs entre as entidades gerenciadoras. A utilização deste protocolo é em um modo de comando e resposta, na qual a entidade gerenciadora envia as informações a um agente, que a recebe e realiza a ação, respondendo assim com uma resposta a requisição, a Figura 5 apresenta o modelo SNMP como gerente e agente trocando informações.

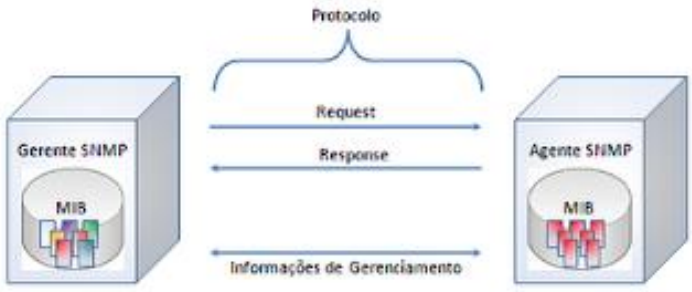

Figura 5. Modelo SNMP gerente/agente
Fonte: DÉO, 2018

A requisição a um agente pode ser usada para recuperar uma informação ou até mesmo modificar um valor contido no banco de dados lógico “MIB” no dispositivo gerenciado. (KUROSE, 2013).

As mensagens do tipo TAP são usadas para comunicar a entidade gerenciadora de alguma situação excepcional que resultou na mudança de valores na MIB, essas mudanças não estão atreladas a situações da rotina do gerenciamento, e sim o gerente do gerenciamento pode definir

querer receber uma mensagem TRAP quando uma interface do dispositivo ficar off-line, por exemplo (KUROSE, 2013).

As aplicações gerentes recebem as informações via protocolo SNMP e são as responsáveis por processar e assim gerar relatórios e também alarmes/alertas quando os valores limites definidos são atingidos (SILVA, 2018), permitindo para o administrador de redes rapidez na identificação e solução do problema.

O protocolo SNMP opera utilizando o UDP pela porta 161 e 162. A 161 é utilizada para a troca de informações entre gerente e agente, já a 162 é utilizada paras as mensagens de alerta enviadas pelos agentes ao gerente, como comentas anteriormente de denominadas de TRAP. A Figura 6 ilustra a troca de informações e suas portas.

Figura 6. Operações SNMP.
Fonte: DÉO 2018

Segundo a RFC 1157 (IETF, 2018), quatro operações foram definidas no SNMP que são:

- GET: esta operação possibilita ao software de gerenciamento recuperar uma instancia de um objeto no agente;
- GETNEXT: esta operação permite recuperar a próxima instância de objetos de uma tabela ou de uma lista, sendo iniciada com a operação “GET” e depois vários “GETNEXT”;
- SET: possibilita alterar valores de uma instância de objeto no agente;
- TRAP: é utilizado pelo agente para informar ao agente sobre um ocorrido, são alertas enviados do agente ao gerente mesmo sem a solicitação.

2.2.1 Evolução do protocolo SNMP

Segundo (ABREU e PIRES, 2004) existem três versões do protocolo SNMP, a versão um foi definida em três RFC's, a RFC 1155 (IETF, 2018) e a RFC 1212 (IETF, 2018) que definem os mecanismos usados para nomear os objetos gerenciados, a RFC 1157 (IETF, 2018) define o Protocolo Simples de Gerenciamento de redes, o SNMP.

A segurança nesta versão não era o item mais importante, sendo baseada somente em nomes de comunidades que são simplesmente senhas em texto aberto, pois nesta versão não existe um mecanismo de autenticação de usuário sendo necessário somente o gerente conhecer o nome da comunidade do item a ser gerenciado para obter os dados deste agente.

A versão dois, denominada de SNMPv2 ou SNMPv2c veio para corrigir alguns problemas de segurança já apresentadas na versão um do protocolo, adicionando nesta versão mais segurança, configuração remota via protocolo SNMP, novas operações e comunicação entre servidores com a função de gerentes.

O SNMPv2 segundo Kurose (2013) define sete tipos de mensagens, conhecidas genericamente como PDUs (*Protocol data Units*), conforme apresentados no Quadro 3.

Tipo de SNMPv2-PDU	Remetente-receptor	Descrição
GetRequest	Gerente a agente	Pega valor de uma ou mais instâncias de objetos MIB
GetNextRequest	Gerente a agente	Pega valor da próxima instância de objeto MIB na lista ou tabela
GetBulkRequest	Gerente a agente	Pega valores em grandes blocos de dados, por exemplo, valores em uma grande tabela
InformRequest	Gerente a agente	Informa à entidade gerenciadora remota valores da MIB que são remotos para seu acesso
SetRequest	Gerente a agente	Define valores de uma ou mais instâncias de objetos MIB
Response	Agente a gerente ou gerente a gerente	Gerado em resposta a GetRequest, GetNextRequest, GetBulkRequest, SetRequest PDU, ou InformRequest
SNMPv2-Trap	Agente a gerente	Informa ao gerente um evento excepcional

Quadro 3. Tipos de PDU SNMPv2
Fonte: (KUROSE, 2013)

A Figura 7 mostra o formato da PDU SNMPv2, na parte superior, demonstra-se o formato do cabeçalho da PDU e os campos que sempre são enviados do gerente ao agente, buscando consultar alguma informação ou alterar algum dado no agente.

Na parte inferior demonstra-se o cabeçalho da requisição TRAP enviada do agente para o gerente somente quando ocorre algo fora do programado com o agente.

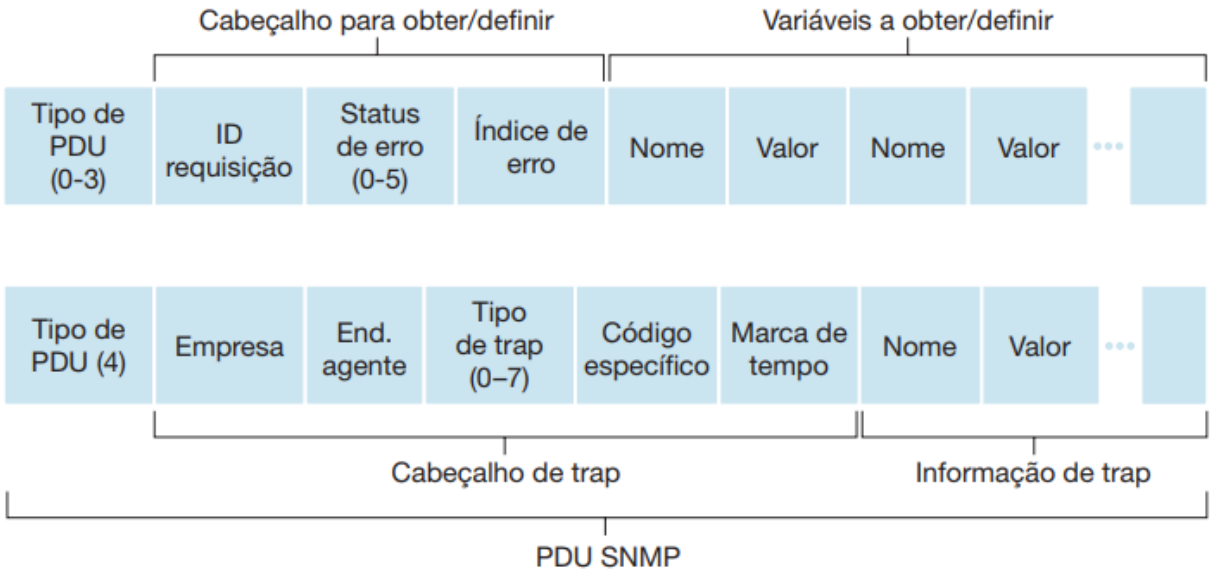

Figura 7. Formato da PDU SNMPv2
Fonte: (KUROSE, 2013)

A versão três é denominada de SNMPv3 tem como seu objetivo principal resolver problemas de segurança apresentados nas suas duas versões anteriores. Para isso foram adicionadas novas ferramentas de autenticação e privacidade, autorização e controle de acesso além de ferramentas administrativas como a nomeação de entidades, gerencia de chave, notificação dos destinos e configuração remota melhorada a partir da versão anterior.

Segundo (KUROSE, 2013), a segurança SNMPv3 é conhecida como segurança baseada em usuário, pois utiliza o conceito tradicional de usuário, identificado por um nome de usuário quais informações de segurança, definidas por uma senha, dão acesso aos privilégios a ele elencados.

2.3 SISTEMAS DE GERENCIAMENTO DE REDES

Atualmente existem várias ferramentas disponíveis no mercado para o gerenciamento de redes, ferramentas gratuitas e mantidas por organizações ou até mesmo ferramentas pagas. Para a escolha de um sistema de gerenciamento de redes deve-se levar em consideração alguns critérios,

como por exemplo, se o sistema vai apenas monitorar se o dispositivo está ativo na rede, se vai monitorar o consumo de recursos do equipamento, o trafego de dados em determinados setores ou link, dentre outros.

Todos esses fatores interferem na tomada de decisão para a escolha do sistema, e para isso destaca-se os sistemas mais conceituados no mercado (ALVES, 2018).

- NAGIOS: tem um grande potencial de utilização no mercado, atendendo perfeitamente grandes redes, por outro lado a configuração é feita totalmente por arquivos tornando o gerenciamento mais especialista (NAGIOS, 2018).
- CACTI: é um sistema ótimo para geração de gráficos em tempo real, possui suporte a todas as versões do protocolo SNMP, mas perde bastante conceito por ser fraco na geração de relatórios (CACTI, 2018)
- THE DUDE: Um sistema criado pela empresa MICROTICK para o monitoramento de seus roteadores, mas por possuir suporte também ao protocolo SNMP pode ser utilizado para gerenciar equipamentos de outros fabricantes. Possui grande facilidade na configuração e também é bastante configurável, possui sistema de alerta por e-mail quando configurado, roda em sistemas operacionais Windows ou no próprio SO (sistema operacional) dos roteadores da MICROTICK. Perde alguns pontos no sistema de log e de relatórios, por não serem muito atraentes (MICROTICK, 2018).
- ZABBIX: é um dos sistemas gratuitos mais completos disponível no mercado atualmente, monitora diversos serviços de forma completa, a captação dos dados dos agentes pode ser feita utilizando o protocolo SNMP ou instalando o agente da ZABBIX, o Zabbix-agent. Por ser um sistema mais completo exige um conhecimento avançado para a implantação e configuração, não sendo recomendado para redes de pequeno porte devido a sua dificuldade de configuração. Possui relatórios muito atrativos de mapas, alertas, gráficos entre outros (ZABBIX, 2018).

Levando em consideração o levantamento dos sistemas acima, o Quadro 4 faz um comparativo de alguns pontos cruciais no gerenciamento entre os sistemas.

	Suporte ao SNMP	Gerência de logs	Facilidade de implantação/configuração	Alertas por e-mail	Apresentação gráfica amigável
NAGIOS	Sim	Não	Não	Sim	Não
CACTI	Sim	Não	Sim	Não	Não
THE DUDE	Sim	Sim	Sim	Sim	Sim
ZABBIX	Sim	Sim	Não	Sim	Sim

Quadro 4. Comparativo entre sistemas de gerência de redes.
Autor: Autoria Própria

A definição do sistema para o gerenciamento dos ativos de rede ficou entre o THE DUDE (MIKROTICK, 2018) e o ZABBIX (ZABBIX, 2018) devido as qualidades que ambos apresentaram no levantamento dos sistemas mais conceituados descrito na Seção 2.3 do trabalho.

O sistema decidido a implantar foi o THE DUDE da empresa MIKROTIK, essa tomada de decisão se teve ao comparar alguns critérios:

- Facilidade de Implantação: o sistema da MIKROTICK possui um grande potencial de gerenciamento com pouca dificuldade para a implantação, quando comparamos com o sistema ZABBIX.
- Dimensão da rede: o tamanho da rede a ser gerenciada pode ser considerado de médio porte, tendo em média em horários de picos 500 conexões simultâneas. Com o grande crescimento das redes é possível que sofra uma expansão com o passar dos anos, mas ainda é atendida com precisão pela ferramenta THE DUDE. O ZABBIX é recomendado para redes de grande porte, mas atende, com precisão, redes menores, mas com maior custo de mão de obra.
- O que gerenciar na rede: outro fator importante a ser levado em consideração, na rede a ser implantado o objetivo é gerenciar o consumo de banda em todos os links, o consumo de recurso e atividade dos principais componentes e envio de notificações de anomalias para o e-mail do responsável. Nesse quesito o THE DUDE se destaca por apresentar todas essas informações em apenas uma interface nativa, sem a necessidade de adicionar componentes ou configurar um outro tipo de relatório diferente.

- Configuração dos agentes: ambos os sistemas possuem o suporte ao protocolo SNMP, mas THE DUDE possui uma forma mais amigável de adicionar os componentes em relação ao ZABBIX.

3. MATERIAIS E MÉTODO

Este capítulo tem por objetivo descrever os materiais e o método utilizados para a implantação do gerenciamento de redes na rede lógica do Colégio Mater Dei.

3.1 MATERIAIS

Para o desenvolvimento deste trabalho, os principais itens utilizados foram comutadores de pacotes (*switch*) da marca Ubiquiti, modelos Unifi switch 8 POE-150W e Unifi switch 16 POE-150W para camada de acesso, e para a camada de núcleo foi utilizado um comutador de pacotes da marca HP modelo HP 1910-24G como mostra o Quadro 5.

Quadro 5. Tecnologias e ferramentas utilizadas na implantação do gerenciamento.

Ferramenta/Tecnologia	**Versão Firmware**	**Aplicação**
Comutador HP 1910-24G	5.20 Release 1513P62	Camada de núcleo
Comutador Ubiquiti 8 portas POE-150W	3.9.54.9373	Camada de acesso
Comutador Ubiquiti 16 portas POE-150W	3.9.54.9373	Camada de acesso
Snmpwalk	4.0 Beta3	Consulta banco MIB dos dispositivos
The Dude	4.0 Beta3	Entidade gerenciadora
Windows Server	2008 R2 Enterprise	Servidor da entidade gerenciadora

Autor: Autoria Própria

A Figura 8 mostra o diagrama de distribuição da rede, que facilita o entendimento da topologia. Para este caso foi utilizando apenas camada de núcleo e acesso para a implementação, seguindo o modelo hierárquico definido por (CISCO, 2018).

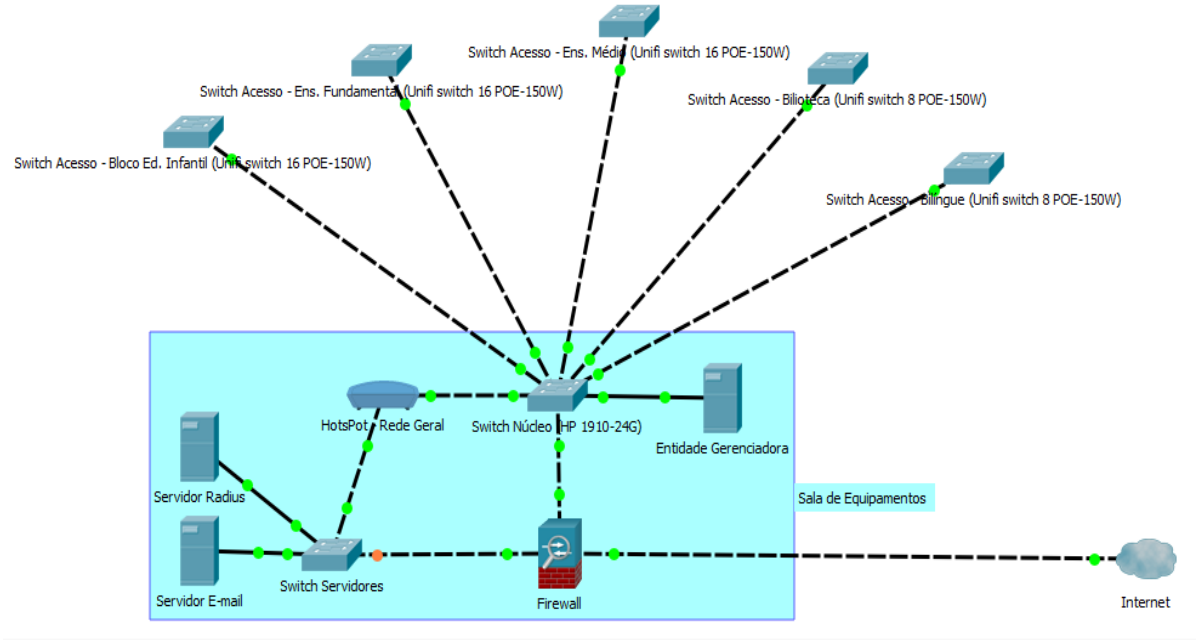

Figura 8. Diagrama de distribuição da rede.
Fonte: Autoria Própria.

Um fato curioso na topologia da rede é a existência de 2 *gateways* na rede interna, sendo um criado diretamente em uma interface do *firewall* e ligado ao *switch* de núcleo que atende configurações específicas das máquinas da rede cabeada (rede administrativa), tendo sua classe de IPs definida estaticamente, e o trafego só é permitido para máquinas que possuem o endereço MAC (*Media Access Control*) e respectivamente o IP fixo liberados no *firewall*.

O segundo *gateway* existente na rede é criado pelo *hotspot*, tendo configuração de DHCP (*Dynamic Host Configuration Protocol*) dinâmico e página para autenticação de usuário e senha. Essa rede é utilizada pelos alunos e demais pessoas da instituição.

Os comutadores, modelos Unifi switch 8 POE-150W e 16 POE-150W, possuem capacidade de comutação de 20Gbps e 36Gbps respectivamente, ambos como compatibilidade ao protocolo SNMP, suporte a VLAN e autenticação 802.1x para futuras implementações.

A escolha destes dispositivos para a camada de acesso, está ligada à sua capacidade de fornecerem alimentação aos pontos de acessos Unifi UAP-LR que criam a rede sem fio, já existente na instituição, nesse caso, eliminando a necessidade de utilização de fontes para a alimentação de energia para esses pontos de acesso separadas, de certa forma organizando melhor os *hacks* de distribuição dos blocos e passando a função de alimentação para esses comutadores.

Essa forma de alimentação POE (*Power over Ethernet*) feita diretamente pelo comutador traz alguns benefícios, como, por exemplo, o melhor controle dos pontos de acesso, podendo

reiniciar ou até mesmo desligar qualquer ponto de acesso, remotamente, sem a necessidade de se deslocar até a área física onde o ponto de acesso está instalado.

O comutador modelo HP 1910-24G possui 24 portas RJ 45 mais quatro portas SFP, tendo capacidade de comutação de até 56 Gbps, conta com suporte ao protocolo SNMP, VLAN estática ou VLAN dinâmica baseada na autenticação 802.1x, pensando já em futuras implementações de autenticação dinâmica.

O comutador HP 1910-24G possui capacidade para operar na camada três do modelo OSI, sendo assim sua utilização recomendada na camada de núcleo do projeto de redes (CISCO, 2018).

Para a instalação da entidade gerenciadora foi utilizado um servidor que a instituição já possuía, rodando o sistema operacional Windows, sendo que esta é uma das exigências específicas do sistema a ser utilizado.

Para consultar as MIBs nos agentes a serem gerenciados foi utilizado o *Snmpwalk* (SNMPWALK, 2018), que consiste em fazer solicitações GETNEXT para buscar informações, onde um identificador OID especifico pode ser usado para executar uma linha de comando e trazer a informação já filtrada para aquele OID.

As especificações dos equipamentos foram definidas considerando o levantamento de valores para a substituição dos equipamentos que haviam no local, sendo esses sem suporte ao protocolo de gerenciamento. Dentro do orçamento proposto foram escolhidas as melhores opções para a implementação do gerenciamento pensando em fatores de expansão futuras e implementação de outros controles de segurança e qualidade de serviço, como VLAN, autenticação 802.1x, e serviço de QoS.

3.2 MÉTODO

A primeira etapa para a realização do desenvolvimento deste trabalho foi o levantamento bibliográfico sobre LAN e gerenciamento de redes, utilizando assim obras dos principais autores conhecidos no assunto.

A segunda etapa foi o levantamento da estrutura da rede do Colégio Mater Dei, quantificando os ativos que precisariam ser substituídos, analisando a quantidade e o potencial

dos usuários que utilizavam em determinadas áreas, levando em consideração previsão de expansões futuras.

A terceira etapa foi a apresentação do projeto para a direção-geral da escola, estimando, nesta etapa, valores de investimento e benefícios que o gerenciamento traria para a qualidade do serviço ofertados pela rede, aos alunos e funcionários da instituição, também, foram especificados modelos de equipamentos a serem adquiridos.

A quarta etapa foi a instalação da entidade gerenciadora THE DUDE e o início da configuração dos equipamentos, sendo realizada de forma gradativa e controlada.

4. RESULTADO E DISCUSSÃO

Neste capítulo são apresentados os procedimentos para a instalação do sistema de gerenciamento de redes The Dude, bem como comentadas suas principais funcionalidades utilizadas no projeto.

4.1 O COLÉGIO MATER DEI

O Colégio Mater Dei, foi fundado em 1968 e a partir do ano de 1975 deu-se a implantação gradativa das séries iniciais, e de lá para cá a escola só cresceu. O Mater Dei sempre se caracterizou pela presença em buscar o melhor complemento educativo para os seus alunos (MATERDEI, 2018).

Com uma equipe especializada de professores e funcionários preparados para a dinâmica escolar, o Colégio Mater Dei busca utilizar os melhores recursos para o aprendizado de seus alunos, aliando técnicas pedagógicas com recursos tecnológicos (MATERDEI, 2018).

Salientando as principais práticas envolvendo tecnologia empregas pela escola, destaca-se as oficinas de programação Lego, uso de tablets para realização de atividades em sala de aula, utilização de tecnologia VR (*virtual reality*) visando a imersão do aluno em conceitos problemáticos sem a necessidade de sair da sala de aula. Além destas ferramentas, ainda possui suas salas equipadas com projetor multimídia, sistema de som e um computador.

4.2 PREPARAÇÃO DA REDE

Atualmente, a quantidade de dispositivos conectados à rede lógica do Colégio Mater Dei vem sofrendo constante crescimento, demandando dia após dia de maior qualidade de serviços e maior tráafego de banda entre os enlaces.

O cenário atual encontrado na instituição já permite algumas manobras sendo que o cabeamento já se encontra todo na categoria GIGALAN CAT.6, porém, os dispositivos, em sua maioria, ainda não suportavam o tráfego em Gbps por porta ou, se suportavam, não tinham o suporte ao protocolo SNMP.

Na apresentação da proposta de implantação de gerenciamento, instituiu-se um levantamento dos equipamentos, já pensando em valores monetários e também em implementações de melhorias futuras, como foram descritas na Seção 3.1.

A troca dos comutadores de pacotes, se deu de forma gradativa no decorrer da implantação do projeto, visando, desta forma, minimizar os impactos pela interrupção do tráfego de dados para os funcionários e utilizadores da rede.

Ao finalizar toda a migração para os novos dispositivos e, os mesmos, devidamente configurados, deu-se início a implantação do sistema de monitoramento da Mikrotik, o The Dude, descrito na Seção 4.3.

4.3 MONITORAMENTO DA REDE

Para fornecer informações e melhorar a agilidade na solução de problemas relacionados a rede lógica, pelo setor responsável da instituição, como citado no Seção 2.3 deste documento, optou-se pela implantação do sistema de gerenciamento The Dude (MIKROTIK, 2018), tendo por objetivo saber a situação atualizada dos ativos da rede e também a situação de consumo em cada enlace de dados da instituição.

O software é desenvolvido pela empresa Mikrotik, para o monitoramento e configuração de seus equipamentos, mas por ter suporte ao protocolo SNMP, suporta equipamentos de outros fabricantes, com suporte ao mesmo protocolo.

Após a realização da configuração do SNMP em todos os ativos, cada dispositivo foi adicionado ao painel de monitoramento e realizada a configuração para a exibição dos dados pela entidade gerenciadora, como mostrado na Figura 9, sendo que cada esfera representa um bloco da instituição.

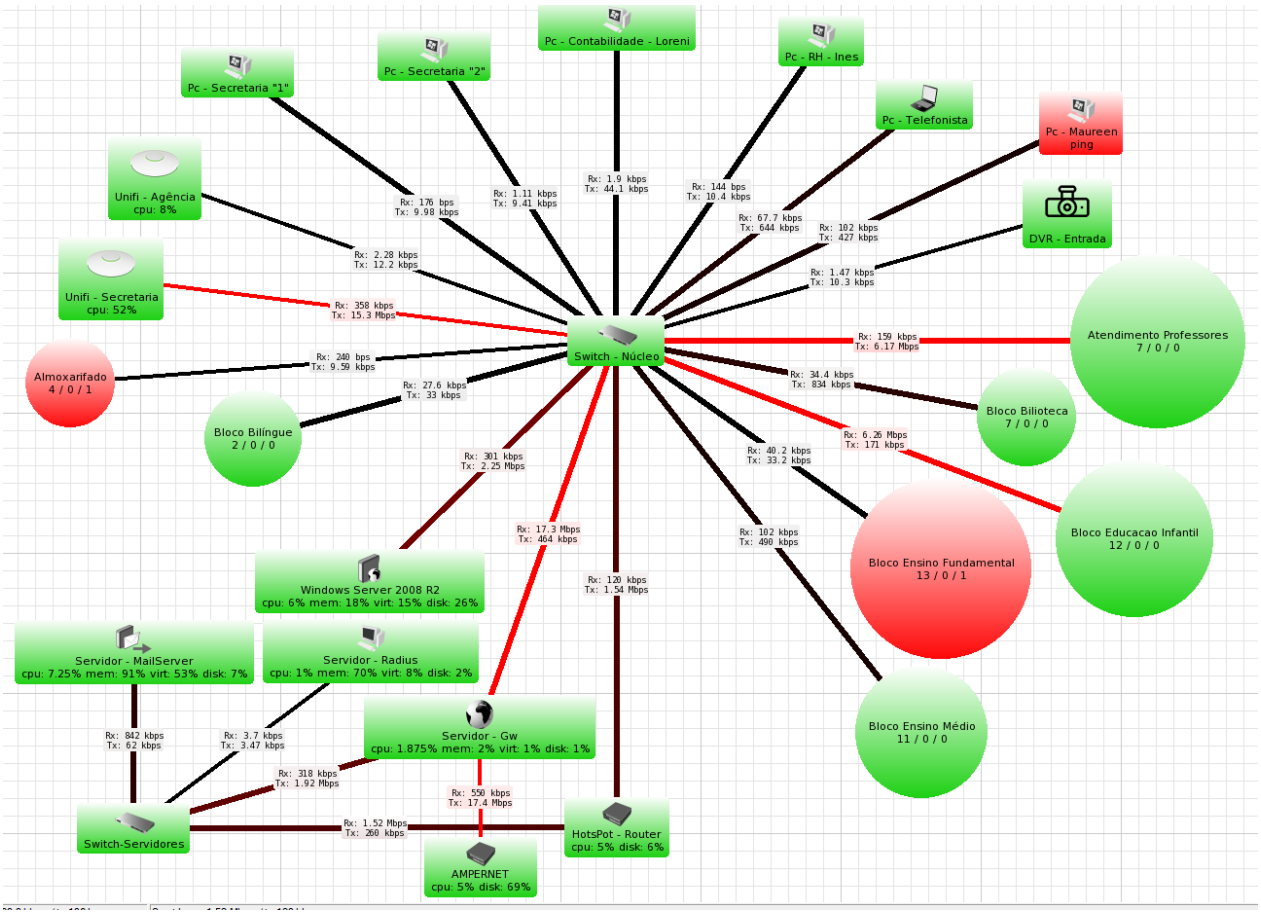

Figura 9. Painel de monitoramento do The Dude.
Fonte: Autoria Própria.

Alguns fatores devem ser levados em consideração ao observar a Figura 9. É notável os enlaces onde se tem uma maior demanda de dados, que são representados na cor vermelha. Outro fator, são as esferas ou dispositivos apresentados na cor vermelha, pode-se deduzir que os mesmos estão com problemas por estarem *off-line*, mas, no caso deste projeto, a central controladora está configurada para gerenciar todos os dispositivos da rede, incluindo os microcomputadores e impressoras de todos os setores. Portanto, quando algum destes equipamentos se desconecta, a entidade alerta para o administrador e grava em seu arquivo de *logs*, o horário e a data do ocorrido.

Essa postura foi adotada a pedido da direção da instituição onde o projeto foi implantado, auxiliando assim, além da equipe de tecnologia a manter a rede em perfeitas condições, também a tomada de decisão por parte da equipe gestora sobre o rendimento dos seus funcionários.

Na Figura 10, apresenta-se a forma de como é feita a adição de dispositivos ao painel de monitoramento do The Dude (entidade gerenciadora), bastando, nesse passo, somente colocar o nome do dispositivo ou o seu endereço IP e avançar para a fase de configuração do protocolo SNMP.

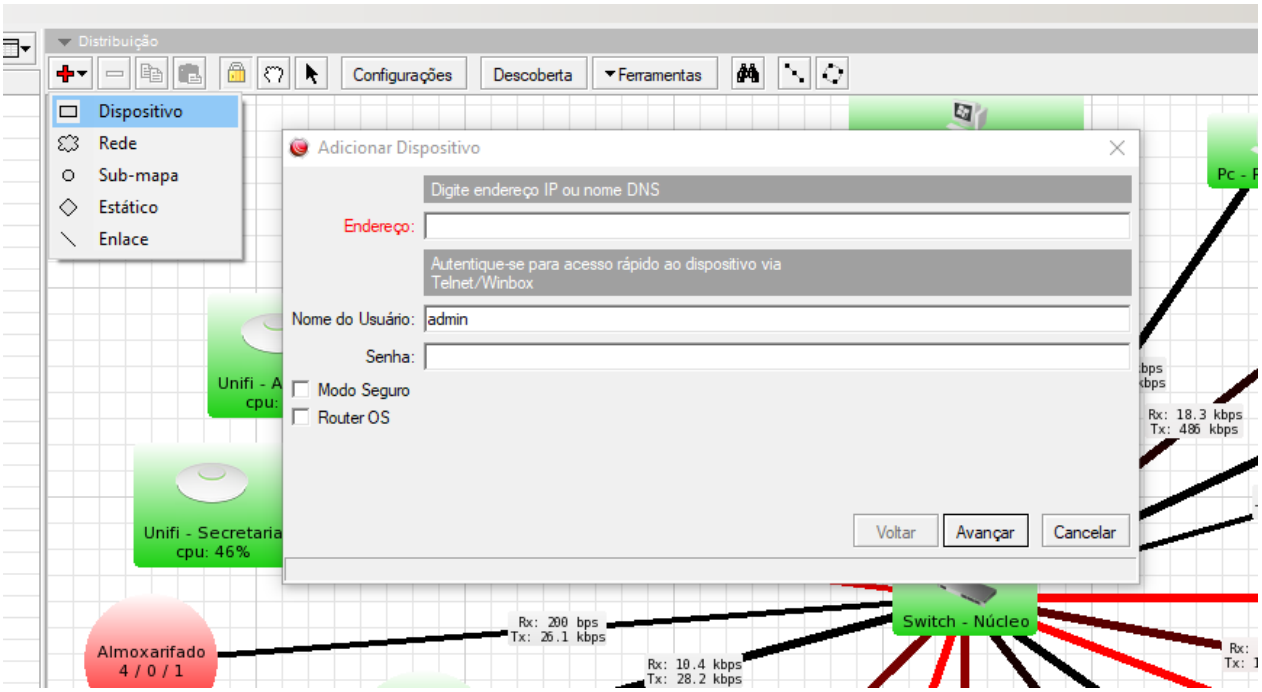

Figura 10. Adicionar novos dispositivos ao The Dude.
Fonte: Autoria Própria.

Ao avançar, a etapa de localização do equipamento, são apresentadas algumas outras configurações como mostrado na Figura 11. As configurações mais importantes para o funcionamento são:

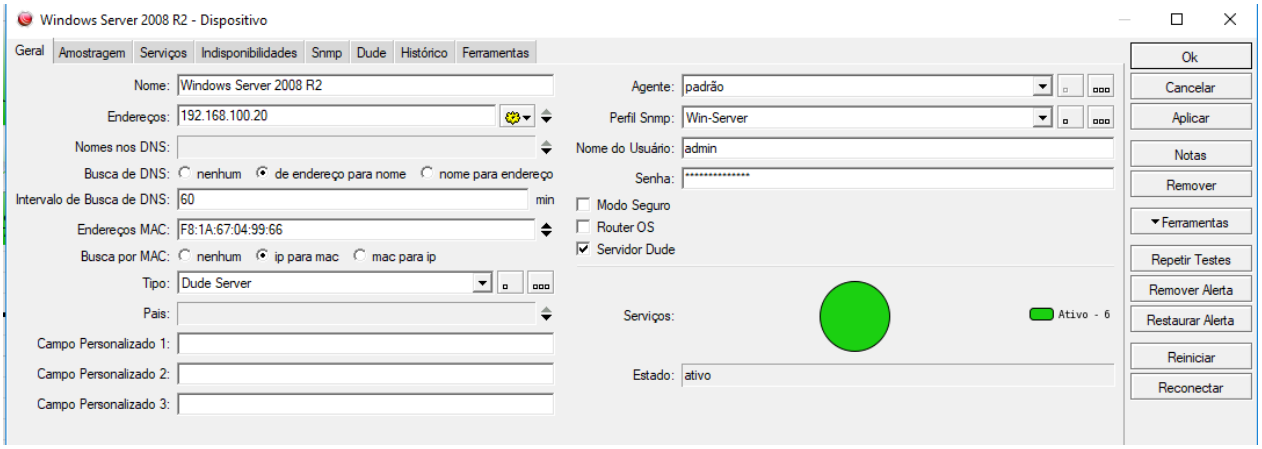

Figura 11. Configurações do dispositivo no The Dude.
Fonte: Autoria Própria

- Aba geral: deve ser defino um nome para o dispositivo. Não é de caráter obrigatório, mas essa definição implica na identificação rápida do dispositivo dentro da topologia. Ainda, na aba geral, deve ser definido um perfil SNMP. Para cada dispositivo a ser gerenciado é possível criar um grupo SNMP diferente. Nesta opção é necessário cadastrar o mesmo perfil ao qual o dispositivo a ser gerenciado foi configurado.
- Aba serviços: nesta aba encontram-se os serviços que a entidade gerenciadora vai monitorar no dispositivo que está sendo adicionado, podendo o administrador escolher os quais é de seu interesse. O The Dude por padrão traz vários serviços, mas é possível adicionar novos.

Quando finalizada a definição destas etapas básicas, o dispositivo já passa a ser gerenciado pela entidade gerenciadora, caso não possua equívocos nas configurações.

Dentre as etapas descritas anteriormente como básicas para o funcionamento, a plataforma mostra outras diversas configurações, também ilustradas na Figura 11, as principais são:

- Receber alertas via e-mail: essa funcionalidade pode ser ativada e configurada dentro da aba amostragem. É possível o administrador especificar para receber alertas para algumas funcionalidades de maior relevância e, para outras, não receber.
- Aba indisponibilidades: nesta aba da configuração, ficam registrados todas as indisponibilidades registradas pelo equipamento gerenciado, sejam elas indisponibilidades de serviços ou mesmo do equipamento.
- Aba SNMP: nesta aba encontrasse vários subitens, como dados das interfaces, processador, armazenamento, memória, dentre outros, conforme o modelo e o tipo do equipamento.
- Aba histórico: nesta aba concentra-se um histórico dos serviços que estão sendo monitorados no dispositivo. É possível o administrador consultar como um serviço, ou mesmo o equipamento, vem se comportando na rede, em um determinado período.

Através da ferramenta de monitoramento da Mikrotik, a equipe de tecnologia consegue monitorar os ativos da rede, identificando facilmente algum equipamento, ou até mesmo algum enlace de dados, que apresente alguma espécie de problema, facilitando também a identificação da largura de banda demandada entre os enlaces, como apresentado na Figura 12, antecipando-se assim de eventuais problemas de segurança, como, por exemplo, de um consumo exagerado de banda por algum serviço ou até mesmo pelo mau uso por parte dos usuários.

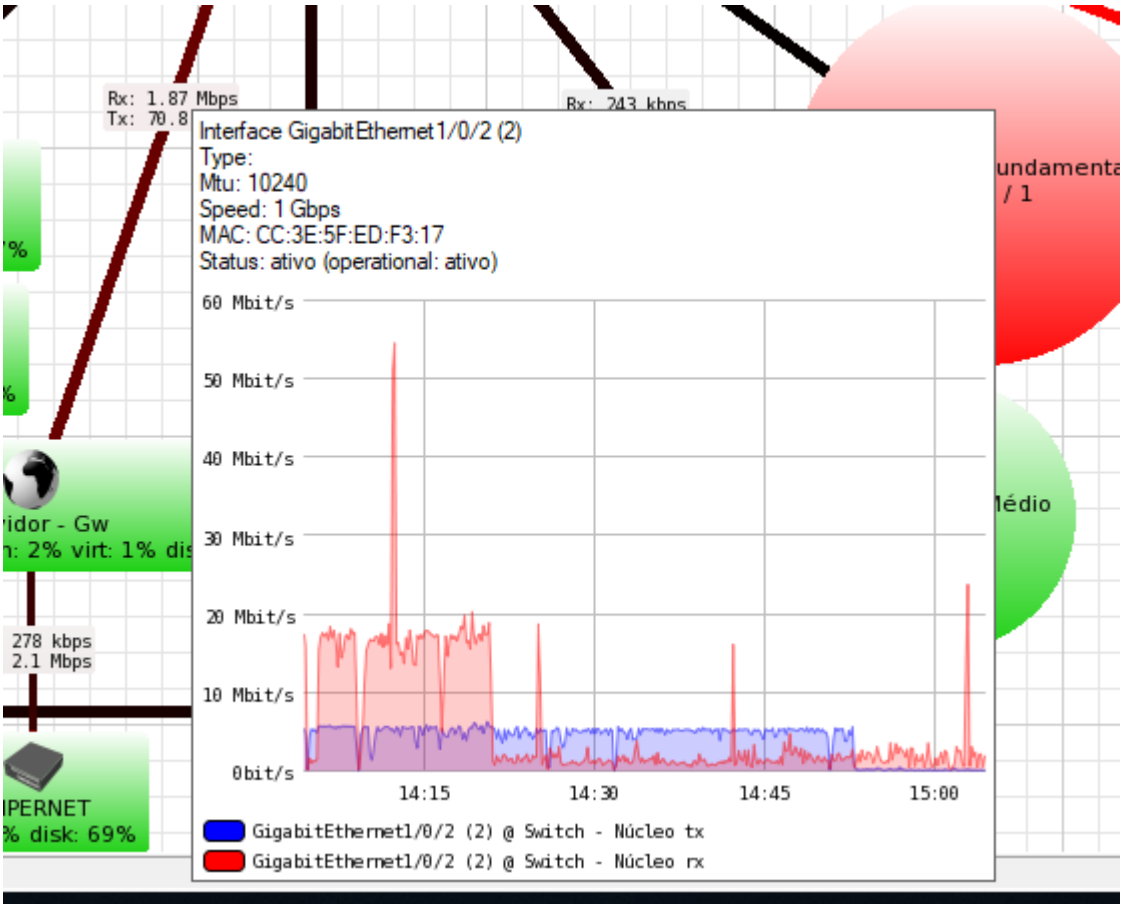

Figura 12. Largura de banda entre enlaces.
Fonte: Autoria Própria

No The Dude houve a necessidade da adição de algumas MIBs devido à heterogeneidade encontrada na rede e que estão atualmente sendo utilizadas, permitindo assim que através destes sensores ocorreu a possibilidade de adição de novas informações ao painel de informações utilizado pela equipe de tecnologia. A Figura 13 mostra a utilização do disco, da memória e do processador de um dos servidores da instituição. Este servidor também hospeda a entidade gerenciadora da rede.

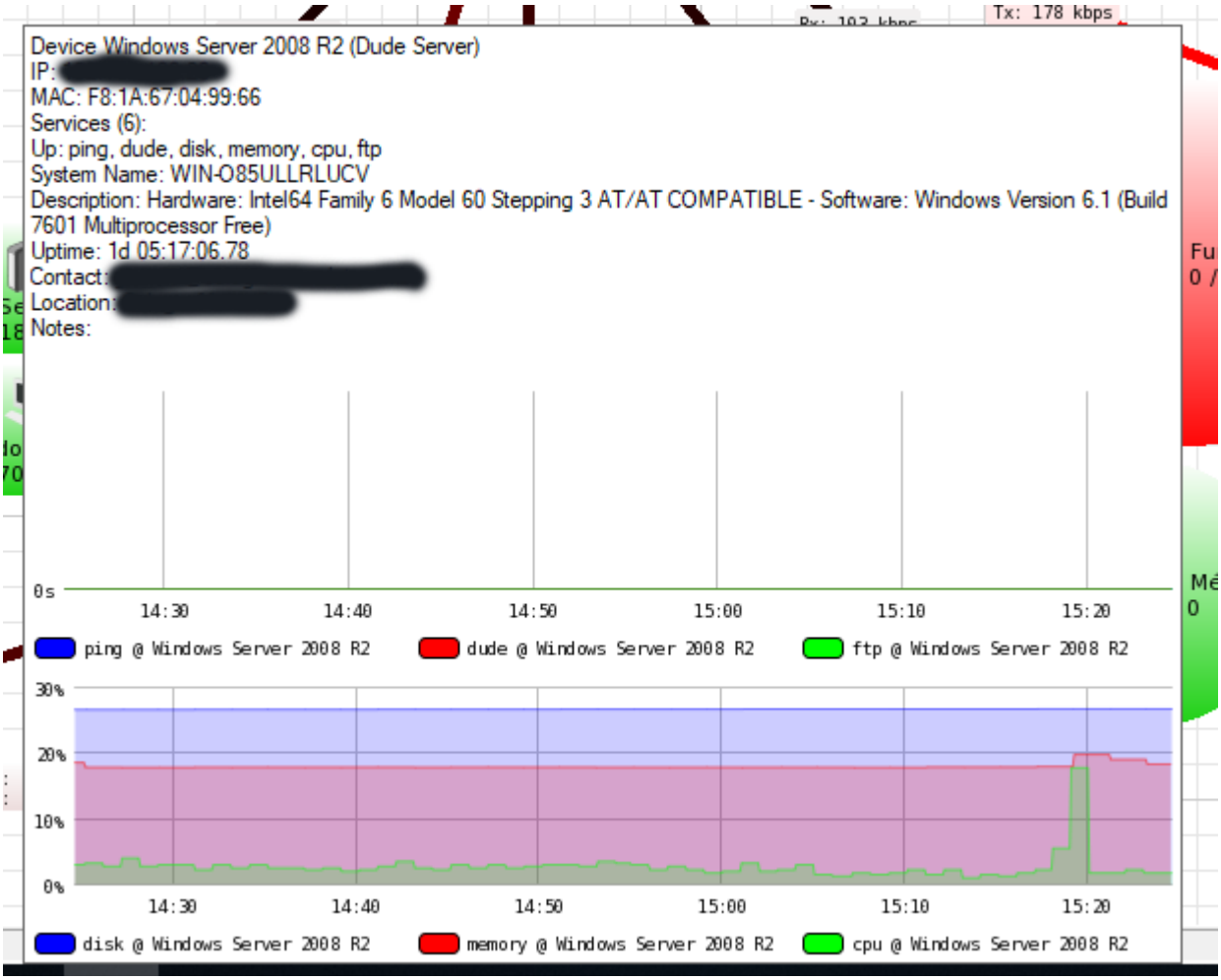

Figura 13. Informações gerenciadas no dispositivo.
Fonte: Autoria Própria

Apesar de muitas funções serem específicas para equipamentos da própria empresa Mikrotik, o The Dude se sai muito bem ao utilizar o protocolo SNMP, permitindo, dessa forma, gerar informações e alertas mesmo que os equipamentos sejam de outros fabricantes, tendo somente como quesito obrigatório que estes equipamentos também tenham suporte ao protocolo SNMP.

Na instituição foi instituída uma política de alertas para o administrador da rede, esses alertas foram definidos para serem disparados quando a entidade gerenciadora encontra alguma anomalia em algum equipamento crucial para o funcionamento da rede. Os alertas são disparados por dois meios, por e-mail e pelo aplicativo de mensagens instantâneas Telegram.

Tendo em vista que o e-mail hoje é uma ferramenta que se tem um acompanhamento menor do que as redes sociais e de mensagens instantâneas optou-se também pela integração com o aplicativo de mensagens Telegram.

Pelo The Dude já possuir suporte ao envio de notificações via e-mail, o único processo necessário foi a configuração das contas e a definição dos alertas a serem disparados. Na Figura 14 ilustra o alerta disparado quando a entidade gerenciadora encontra a anomalia e também quando este serviço volta a se comunicar com a entidade gerenciadora.

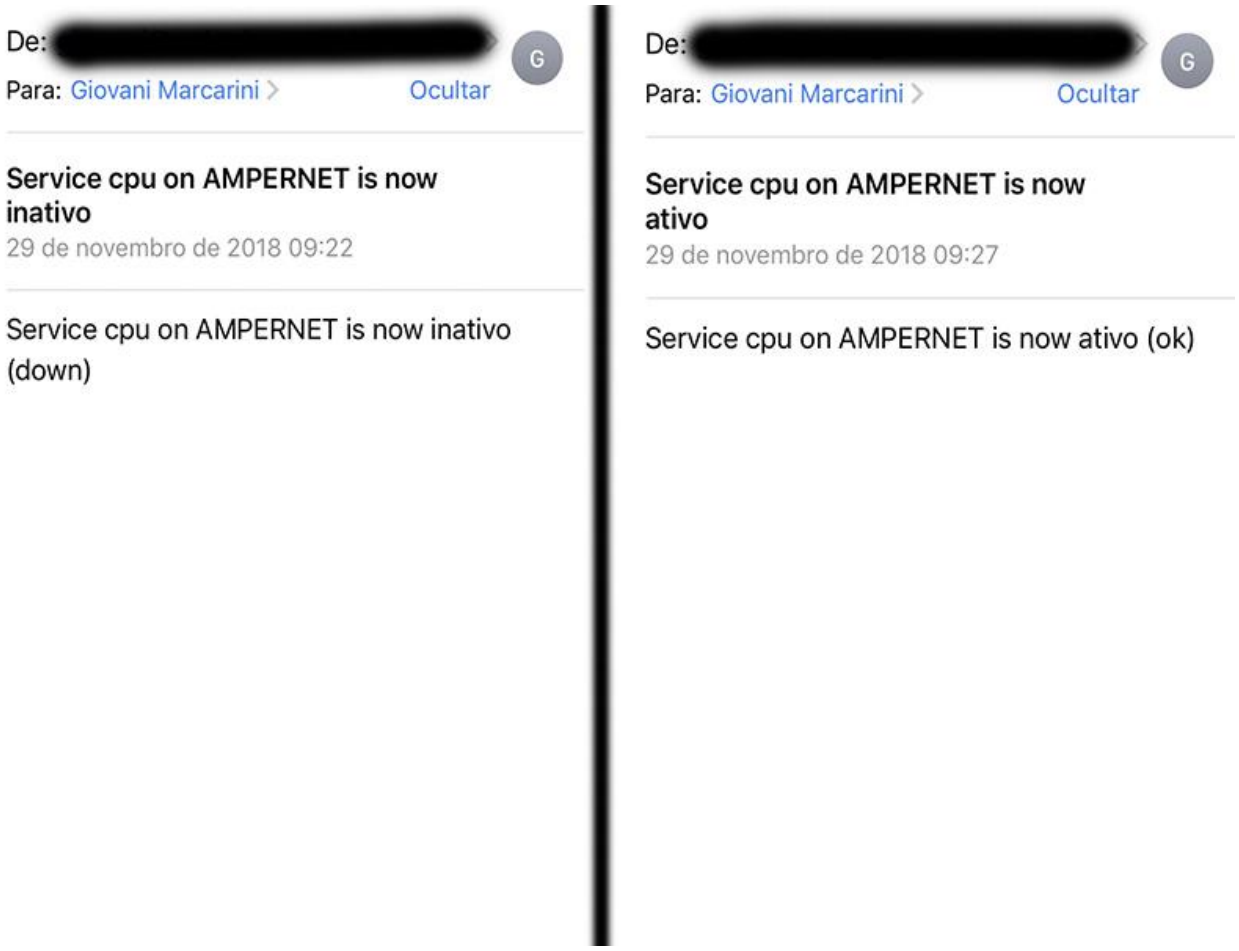

Figura 14. Alerta via e-mail.
Fonte: Autoria Própria

Para a integração com o aplicativo Telegram, houve a necessidade da criação de um *boot* para disparar as notificações. Essas configurações de integração são facilmente encontras na Internet atualmente, o que facilita a configuração e em contrapartida torna o processo de envio das notificações mais rápido em relação ao processo de envio por e-mail.

A Figura 15 ilustra as notificações recebidas pelo administrador da rede da instituição em seu aplicativo de mensagens instantâneas Telegram.

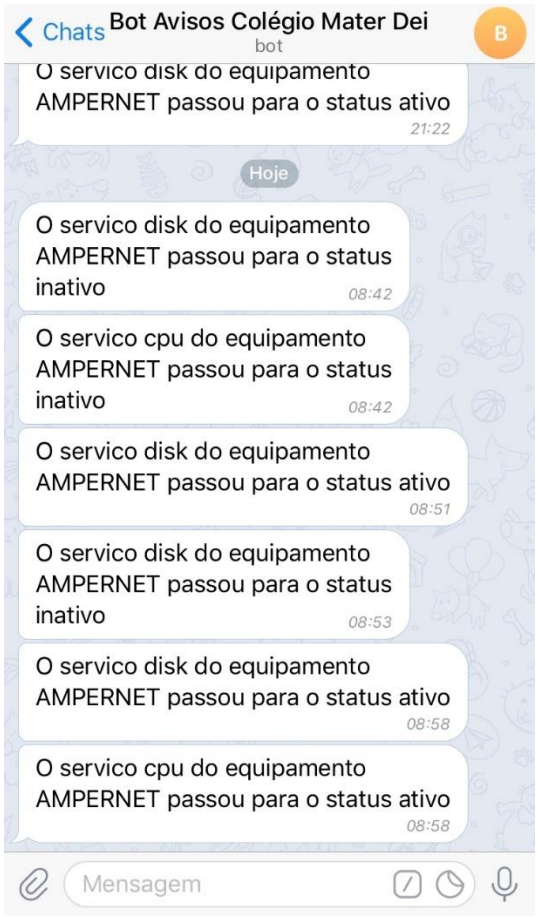

Figura 15. Notificações recebidas via Telegram.
Fonte: Autoria Própria

Esse processo de envio de notificações foi instituído somente para os equipamentos de crucial importância para inibir assim notificações que alguma estação de trabalho ou mesmo uma impressora é ligada ou desligada no início e término do expediente de trabalho notifique o administrador, diminuindo assim o fluxo de notificações enviadas e mantendo as que realmente são importantes.

O painel de informações do The Dude está localizado na entrada da sala do setor responsável, tornando-se bem visível e com possibilidade do acompanhamento em tempo real de todos os fatores e acontecimentos, como mostra a Figura 16.

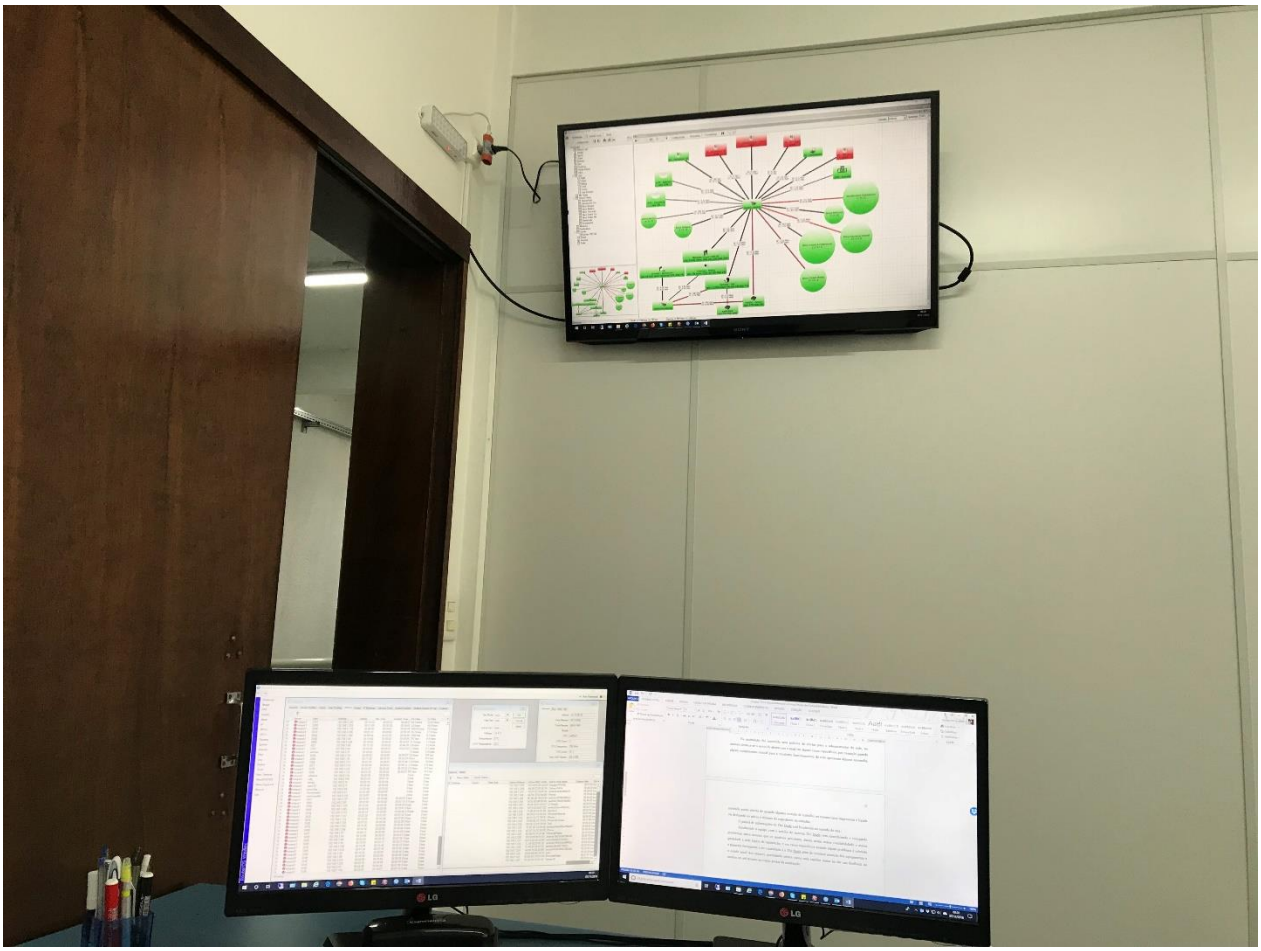

Figura 16. Sala de monitoramento e gerência da rede.
Fonte: Autoria Própria

Atualmente a equipe, com o auxílio do sistema The Dude, vem identificando e corrigindo problemas antes mesmo que os usuários percebam, dando assim maior confiabilidade e maior qualidade a rede lógica da instituição, e, em casos específicos, quando algum problema é relatado, a primeira ferramenta a ser consultada é o The Dude, a fim de verificar a situação dos equipamentos e o estado atual dos enlaces, permitindo, nestes casos, uma rapidez maior ao dar um *feedback* ao usuário ou até mesmo ao corpo gestor da instituição.

5. CONCLUSÃO

O gerenciamento da rede lógica do Colégio Mater Dei, trouxe maior confiabilidade e maior qualidade nos serviços disponibilizados aos seus colaboradores e alunos, aumentando significativamente a estabilidade da mesma.

Os novos *switchs* facilitaram ainda mais a gerência da rede e, consequentemente, aumentando a velocidade de transferência, uma vez que a taxa de transmissão, em cada uma de suas portas, é de 1 Gbps.

A interface amigável e intuitiva do The Dude, além da apresentação visual dos dados coletados nos dispositivos gerenciados, tornou-se o ponto central de consulta caso ocorra alguma anomalia ou, uma falha seja percebida, facilitando, de tal maneira, o diagnóstico e, consequentemente, diminuindo consideravelmente o tempo de estabilização da disponibilidade no acesso.

Hoje, o tempo em que era desperdiçado na procura e identificação de problemas que ocorriam na rede, são utilizados para estudos e implantação de novos serviços, visando facilitar as tarefas diárias dos usuários.

Se nota grande satisfação dos usuários em relação a implantação do gerenciamento de redes, pode-se observar isso nos relatos que chegaram após a ativação do serviço à equipe de tecnologia, por outro lado, pode-se observar também a diminuição na demanda de novos chamados para a equipe.

Conclui-se que o gerenciamento de redes, seja ela implantada em uma rede de pequeno porte ou grande porte, é essencial para que os administradores garantam o pleno funcionamento, a maior qualidade de serviço oferecido aos usuários com um esforço muito menor.

5.1 TRABALHOS FUTUROS

Os trabalhos futuros incluem em reestudar alguns quesitos específicos da rede, visando sempre a maior segurança da informação trafegada, além disso, implementar novos serviços para a melhoria da qualidade ofertada, como:

- Implantar segmentação VLAN (*virtual local área network*) dinâmica, onde cada usuário autenticado na rede trafegará em uma espécie de rua somente sua, inibindo que seja possível enxergar outros dispositivos conectados à mesma rede.
- Implementação de serviço QoS (*quality of servisse*), visando priorizar alguns tipos de informações trafegadas na rede e já pensando na implementação da tecnologia de telefonia IP, conhecida como VOIP (*voice over internet protocol*).
- Implantação de telefonia IP, tendo em vista a facilidade do colaborador se deslocar pela instituição e poder levar consigo o seu ramal.

6. REFERÊNCIAS BIBLIOGRÁFICAS

ABREU, Fabiano R.; PIRES, Herbert D. Gerência **de Redes.** 2004. Disponível em http://www.midiacom.uff.br/~debora/redes1/pdf/trab042/SNMP.pdf. Acesso em 09 de setembro de 2018.

ALVES, G. **Melhor sistema de monitoramento**, 2018. Disponivel em https://rafaelalvesti.wordpress.com/2012/11/28/melhor-sistema-de-monitoramento/. Acesso dia 13 de stembro de 2018.

CASTELI, M. J. **LAN switching first-step**. 1 ed. Indianapolis, IN, USA: Cisco Press, 2004.

CACTI. **Documenttation and Howtos**. Disponível em: https://docs.cacti.net/. Acesso dia 13 de setembro de 2018.

DÉO, André. Gerenciamento de Redes – O Protocolo SNMP. 2018. Disponível em http://andredeo.blogspot.com.br/2011_09_01_archive.html. Acesso em 06 de setembro de 2018.

CISCO. CCNA EXPLORATION 6.0. 2018, disponível em http://pb.utfpr.edu.br/redes/cisco. Acesso em 09 de setembro de 2018.

IETF. **Internet Engineering Task Force**. Disponível em: http://www.ietf.org/ Acesso em agosto de 2018.

IETF. **RFC 1155**. Disponível em: https://tools.ietf.org/html/rfc1155 Acesso em outubro de 2018.

IETF. **RFC 1157**. Disponível em: https://www.ietf.org/rfc/rfc1157.txt Acesso em outubro de 2018.

IETF. **RFC 1212**. Disponível em: https://www.ietf.org/rfc/rfc1212.txt Acesso em outubro de 2018.

IETF. **RFC 1213**. Disponível em: https://tools.ietf.org/html/rfc1213 Acesso em outubro de 2018.

IETF. **RFC 2578**. Disponível em: https://tools.ietf.org/html/rfc2578 Acesso em outubro de 2018.

IETF. **RFC 3418**. Disponível em: https://tools.ietf.org/html/rfc3418 Acesso em outubro de 2018.

IETF. **RFC 4133**. Disponível em: https://www.ietf.org/rfc/rfc4133.txt Acesso em outubro de 2018.

IETF. **RFC 4293**. Disponível em: https://tools.ietf.org/html/rfc4293 Acesso em outubro de 2018.

ISO/IEC. **Basic Reference Model**. International Organization for Standardization na International Electronical Committee, International Standard 7498, 1984.

KUROSE, James F.; ROSS, Keith W. **Redes de Computadores e a internet:** uma abordagem top-down. 6 ed. São Paulo, SP. Editora Pearson Addison-Wesley, 2013. Xxii, 634p.

MATER DEI. **Ambiente de Implantação.** Disponível em: http://www.colegiomaterdei.com.br/institucional/sintese-historica/ Acesso em 05 de novembro de 2018

MIKROTIK. **Mikrotik Routers and Wireless**. 2018. Disponível em http://www.mikrotik.com/thedude.php. Acesso em 09 de setembro de 2018.

NAGIOS. **Nagios Documentation**. 2018. Disponível em: https://www.nagios.org/documentation/. Acesso em 13 de setembro de 2018.

ROSE, T. M. **An Introduction to Network Management**. 2 ed. Editora Prentice Hall, Março, 1996.

SAYDAM, T.; MAGEDANZ, T. **From Networks and Network Management into Service and Service Management**. Journal of Networks and System Management. 1996.

SILVA, R. S. S. **Simple Network Managent Protocol (SNMP).** Disponível em https://www.gta.ufrj.br/grad/04_1/snmp/index.htm. Acesso em agosto de 2018.

SNMPWALK. **Manpage of SNMPWALK.** 2018. Disponível em http://www.netsnmp.org/docs/man/snmpwalk.html. Acesso em 09 de setembro de 2018.

TANENBAUM, A. **Computer Networks**. 3 ed, Prentice Hall, 2011

ZABBIX. **Documentation.** 2018. Disponível em https://www.zabbix.com/manuals. Acesso em 09 de setembro de 2018.