

UNIVERSIDADE TECNOLÓGICA FEDERAL DO PARANÁ  
DEPARTAMENTO ACADÊMICO DE INFORMÁTICA  
CURSO DE ESPECIALIZAÇÃO EM REDES DE COMPUTADORES

DOUGLAS LUIZ MONDSTOCK

**IMPLANTAÇÃO DE FERRAMENTA PARA GERENCIAMENTO E  
MONITORAMENTO NA REDE DA PREFEITURA MUNICIPAL DE PATO  
BRANCO**

MONOGRAFIA DE ESPECIALIZAÇÃO

PATO BRANCO  
2018

DOUGLAS LUIZ MONDSTOCK

**IMPLANTAÇÃO DE FERRAMENTA PARA GERENCIAMENTO E  
MONITORAMENTO NA REDE DA PREFEITURA MUNICIPAL DE PATO  
BRANCO**

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: Prof. MEng. Anderson Luiz Fernandes

PATO BRANCO  
2018

## TERMO DE APROVAÇÃO

### IMPLANTAÇÃO DE FERRAMENTA PARA GERENCIAMENTO E MONITORAMENTO NA REDE DA PREFEITURA MUNICIPAL DE PATO BRANCO

por

**Douglas Luiz Mondstock**

Esta monografia foi apresentada às 18h00min do dia 11 de dezembro 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

## RESUMO

MONDSTOCK, Douglas Luiz. Implantação de ferramenta para gerenciamento e monitoramento na rede da Prefeitura Municipal de Pato Branco. 2018. 40 f. Monografia (Especialização em Redes de Computadores) – Departamento Acadêmico de Informática, Universidade Tecnológica Federal do Paraná, Câmpus Pato Branco, 2018.

As redes de computadores estão presentes no cotidiano de toda empresa, entidade ou meio de comunicação na atualidade. O impacto diretamente aos negócios e ao desenvolvimento das sociedades certamente exige que essas redes desempenhem suas funções e possam atingir seus objetivos. A fim de garantir um serviço sempre ativo, confiável e disponível para o uso, foi necessária a implantação de uma ferramenta, para gerenciar e monitorar a rede. Este trabalho trata da implantação de uma ferramenta para gerenciamento e monitoramento na rede interna da Prefeitura Municipal de Pato Branco. Através do uso do protocolo SNMP é possível gerenciar vários tipos de dispositivos, essencial para órgãos públicos que possuem dispositivos de diversos fabricantes na maioria dos casos. Com o uso da ferramenta The Dude a equipe de gerência de redes pode agir verificando a existência de problemas e posteriormente resolvê-los, atenuando ou findando efeitos negativos na rede.

**Palavras-chave:** Redes de computadores. Gerenciamento. Monitoramento. SNMP.

## **ABSTRACT**

MONDSTOCK, Douglas Luiz. 2018. Implementation of a tool for management and monitoring in the network of the Pato Branco City Hall. 40 f. Monografia (Especialização em Redes de Computadores) – Departamento Acadêmico de Informática, Universidade Tecnológica Federal do Paraná, Câmpus Pato Branco. Pato Branco, 2018.

Computer networks are present in the daily life of every company, entity or medium of communication at the present time. The direct impact on business and the development of societies certainly requires that these networks perform their functions and achieve their goals. In order to ensure a service that is always active, reliable and available for use, it was necessary to deploy a tool to manage and monitor the network. This work deals with the implementation of a tool for management and monitoring in the internal network of the Pato Branco City Hall. Through the use of the SNMP protocol it is possible to manage several types of devices, essential for public agencies that have devices from several manufacturers in most cases. With the use of The Dude tool the network management team can act by checking for problems and then solving them, mitigating or ending negative effects on the network.

**Keywords:** Computer network. Management. Monitoring. SNMP.

## LISTA DE FIGURAS

Figura 1 - Modelo SNMP gerente/agente.....	16
Figura 2 – Cooperação de três protocolos .....	18
Figura 3 - Atributos dos objetos .....	20
Figura 4 - Nomes de identificador de objetos.....	20
Figura 5 - Novo Mapa de rede .....	29
Figura 6 - Painel de monitoramento rede Interligação The Dude .....	30
Figura 7 - Painel de monitoramento rede Gerência The Dude .....	30
Figura 8 - Descoberta de Dispositivo .....	31
Figura 9 - Adicionando dispositivo ao The Dude.....	32
Figura 10 - Descoberta de serviços.....	32
Figura 11 - Configurações do dispositivo.....	33
Figura 12 - Configurações do dispositivo aba Serviços .....	34
Figura 13 - Interfaces descobertas pelo SNMP .....	34
Figura 14 - Armazenamento do dispositivo .....	35
Figura 15 - Largura de banda entre enlaces.....	35
Figura 16 - Servidor de dados.....	36
Figura 17 - Alerta de serviço inativo .....	37
Figura 18 - Arquivo de log .....	37

## LISTA DE QUADROS

Quadro 1 - Descrição de grupos da MIB2 .....	19
Quadro 2 - Tipos de dados SMIV2.....	21
Quadro 3 - Comparativo entre ferramentas de gerenciamento e monitoramento de rede .....	26
Quadro 4 – Tecnologias e ferramentas utilizadas na modelagem e na implementação do aplicativo .....	27

## LISTA DE SIGLAS

ASN.1	<i>Abstract Syntax Notation 1</i>
CMEI	Centro Municipal de Educação Infantil
CPD	Central de Processamento de Dados
DNS	<i>Domain Name System</i>
GNU	<i>General Public License</i>
IETF	<i>Internet Engineering task Force</i>
IPMI	<i>Intelligent Platform Management Interface</i>
ICMP	<i>Internet Control Message Protocol</i>
ISO	<i>International Organization for Standardization</i>
LAN	<i>Local Area Network</i>
MIB	<i>Management Information Base</i>
MD5	<i>Message Digest 5</i>
MYSQL	<i>My Structured Query Language</i>
OID	<i>Object Identifier</i>
PHP	<i>Hypertext Preprocessor</i>
PING	<i>Packet Internet Network Grouper</i>
RFC	<i>Request for Coments</i>
RRDTool	<i>Round Robin Database Tool</i>
SLA	<i>Service Level Agreements</i>
SMI	<i>Structure of Management Information</i>
SNMP	<i>Simple Network Management Protocol</i>
TCP/IP	<i>Transmission Control Protocol/Internet Protocol</i>
UDP	<i>User Datagram Protocol</i>
WAN	<i>Wide Area Network</i>



## SUMÁRIO

Ministério da Educação.....	3
1 INTRODUÇÃO.....	10
1.1 OBJETIVOS.....	10
1.1.1 Objetivo Geral.....	10
1.1.2 Objetivos Específicos.....	10
1.2 JUSTIFICATIVA.....	11
1.3 ESTRUTURA DO TRABALHO.....	12
2 REFERENCIAL TEÓRICO.....	13
2.1 GERENCIAMENTO DE REDE.....	13
2.2 MODELO DE GERENCIAMENTO DE REDE.....	15
2.3 SNMP - PROTOCOLO SIMPLES DE GERENCIAMENTO DE REDES.....	15
2.3.1 Versões do SNMP.....	16
2.3.2 MIB ( <i>Management Information Base</i> ).....	18
2.3.3 SMI ( <i>Structue of Management Information</i> ).....	19
2.4 FERRAMENTAS DE GERENCIAMENTO E MONITORAMENTO DE REDE.....	22
2.4.1 Zabbix.....	22
2.4.2 Cacti.....	23
2.4.3 The Dude.....	24
2.4.4 Escolha da ferramenta.....	26
3 MATERIAIS E METODOLOGIA.....	26
3.1 Materiais.....	27
3.2 Metodologia.....	27
4 RESULTADOS.....	28
4.1 A prefeitura municipal de pato branco.....	28
4.2 monitoramento da rede.....	28
5 Conclusões.....	38
5.1 Trabalhos futuros.....	38
REFERÊNCIAS.....	41

# 1 INTRODUÇÃO

Devido ao crescimento acelerado de componentes que compõe redes de computadores, e em decorrência dos benefícios que elas oferecem aos seus usuários, é primordial que essas redes apresentem confiabilidade, acompanhada de disponibilidade para que os serviços sejam entregues da melhor maneira possível.

Com o objetivo de planejar o crescimento das redes estruturadas, efetuar o monitoramento em tempo real da infraestrutura e seus ativos (servidores, estações de trabalho e impressoras), surge a necessidade do gerenciamento de redes de computadores. O aumento significativo dessas redes torna cada vez mais trabalhoso o gerenciamento realizado apenas por esforços humanos, faz-se necessária então à adoção de ferramentas automatizadas, que disponibilizem informações necessárias sobre os equipamentos de forma rápida e precisa, auxiliando a gerência e a tomada de decisões do gestor. Para Albuquerque (2001) a gerência deve manter a rede operacional e aperfeiçoar o seu desempenho.

Para facilitar o gerenciamento da rede, foi utilizado o protocolo SNMP (*Simple Network Management Protocol*) em português Protocolo Simples de Gerência de Rede, o qual trabalha com diversos produtos e fabricantes, permitindo o monitoramento de dispositivos que estejam fora da rede de origem e proporcionando informações úteis à tomada de decisões por parte da equipe responsável pela gerência e infraestrutura da rede.

## 1.1 OBJETIVOS

### 1.1.1 Objetivo Geral

Implantar uma ferramenta para gerenciamento e monitoramento da rede da Prefeitura Municipal de Pato Branco.

### 1.1.2 Objetivos Específicos

- Realizar o mapeamento na rede do paço Municipal da Prefeitura de Pato Branco com gráficos da topologia da rede e relacionamentos lógicos entre os dispositivos;

- Gerar gráficos em tempo real de serviços mostrando utilização de banda e informações de enlaces;
- Gerar o armazenamento do histórico de eventos (*logs*) da rede, com momentos de queda e restabelecimentos.

## 1.2 JUSTIFICATIVA

A complexidade e o uso massivo das redes de computadores no dia a dia exigem um estudo na área de gerência e monitoramento, pois torna a tarefa do gestor cada vez mais difícil como quando novos dispositivos são conectados à rede e com o tráfego de dados que aumenta a cada dia. Conforme Comer (2006), o gerente que precisar controlar várias máquinas que não estejam conectadas à mesma rede física, pode-se deparar com a impossibilidade de comunicar-se com máquinas sendo controladas, a menos que o software de gerenciamento use protocolos que forneçam conectividade ponto a ponto através da Internet.

O referido trabalho possui grande relevância em sua relação com os conhecimentos adquiridos durante o curso. Segundo Specialski (1999), o monitoramento de rede é importante, para que, após o aparecimento de uma falha, seja possível: rapidamente determinar o componente em que a falha ocorreu, isolar a rede do nó com falha, reconfigurar ou modificar a rede para minimizar o impacto da operação sem o nó problemático e reparar ou trocar o componente com falha.

Pretende-se obter dados em relação à utilização de banda, informações físicas de *links*, entre outros dados que serão proporcionados pelo uso da ferramenta e, analisando esses dados, verificar a existência de problemas e posteriormente resolvê-los atenuando ou findando efeitos negativos na rede.

### **1.3 ESTRUTURA DO TRABALHO**

Este documento está organizado em cinco capítulos, dos quais este é o primeiro e apresenta a ideia e o contexto do trabalho, incluindo os objetivos e a justificativa.

O Capítulo 2 contém o referencial teórico. Neste é apresentado o embasamento para o tema proposto abordando gerenciamento de redes e alguns dos protocolos utilizados, assim como padrões de gerenciamento.

No Capítulo 3 estão os materiais e a metodologia empregados no desenvolvimento deste trabalho.

O Capítulo 4 contém os resultados obtidos no desenvolvimento deste trabalho.

No Capítulo 5 é apresentada a conclusão com as considerações finais.

## 2 REFERENCIAL TEÓRICO

Segundo Forouzan (2006), uma rede é um conjunto de dispositivos (normalmente conhecido como nós) conectados por enlaces de comunicação. Um nó pode ser um computador, uma impressora ou outro dispositivo de envio e/ou recepção de dados, que estejam conectados a outros nós da rede.

Uma rede local (*Local Areal Network - LAN*) é privada e interliga dispositivos em um escritório, prédio ou campus. Dependendo das necessidades de uma organização e do tipo de tecnologia usada, uma LAN pode ser muito simples, a ponto de conectar apenas dois PCs e uma impressora no escritório doméstico de uma pessoa ou se estender por toda a empresa e incluir periféricos de áudio e vídeo. Atualmente, o tamanho de uma LAN é limitado a alguns quilômetros (FOROUZAN, 2006).

Independentemente do tamanho de uma rede de computadores, é fundamental que ela seja gerenciada. Segundo Kurose e Ross (2014), quando centenas ou milhares de componentes são montados em conjunto por alguma organização para formar uma rede, não é nada surpreendente que por vezes eles apresentem defeitos, que elementos da rede sejam mal configurados, que recursos da rede sejam utilizados em excesso ou que componentes simplesmente “quebrem”. O administrador de rede, cuja tarefa é mantê-la “viva e atuante”, deve estar habilitado a reagir a esses contratemplos (e, melhor ainda, a evitá-los). Com potencialmente milhares de componentes espalhados por uma grande área, ele, evidentemente necessita de ferramentas que o auxiliem a monitorar, administrar e controlar a rede.

### 2.1 GERENCIAMENTO DE REDE

Para Forouzan e Mosharraf (2013) o gerenciamento de redes pode ser definido como “(...) a tarefa de testar, monitorar, configurar e resolver problemas dos componentes de rede com o objetivo de atender um conjunto de requisitos definidos por uma organização”.

Além dos protocolos que fornecem serviços em nível de rede e programas aplicativos que utilizam esses serviços, é necessário um subsistema que permita a um administrador configurar uma rede, controlar roteamento, depurar problemas e identificar situações em que computadores violam políticas. A essas atividades chamamos gerenciamento de rede (COMER, 2006).

Nos primórdios das redes de computadores, quando elas ainda eram artefatos de pesquisa, e não uma infraestrutura usada por milhões de pessoas por dia, “gerenciamento de rede” era algo de que nunca se tinha ouvido falar. Se alguém descobrisse um problema, poderia realizar alguns testes, em seguida, modificar os ajustes do sistema a fim de corrigi-lo. Como a Internet pública e as intranets privadas cresceram e se transformaram de pequenas redes em grandes infraestruturas globais, a necessidade de gerenciar mais sistematicamente a enorme quantidade de componentes de hardware e software nessas redes também se tornou mais importante (KUROSE; ROSS,2014).

Segundo Kurose e Ross (2014), mesmo para uma rede simples, há muitos cenários em que o administrador se beneficia por ter à mão ferramentas de gerenciamento adequadas:

- Detecção de falha em uma placa de interface em um hospedeiro ou roteador. Com ferramentas de gerenciamento apropriadas, uma entidade de rede pode indicar ao administrador que uma de suas interfaces não está funcionando. Isso poderá ser feito, por exemplo, se o administrador notar um aumento de erros de somas de verificação em quadros que estão sendo enviados por uma placa de interface que está prestes a falhar.

- Monitoração de hospedeiro. O administrador de rede pode verificar periodicamente se todos os hospedeiros da rede estão ativos e operacionais. Ele pode, de fato, impressionar um usuário da rede, reagindo proativamente a um problema (falha em um hospedeiro) antes de o defeito ser relatado pelo usuário.

- Monitoração de tráfego para auxiliar o oferecimento de recursos. Um administrador de rede pode monitorar padrões de tráfego entre origens e destinos e notar, por exemplo, que, trocando servidores entre segmentos de LAN, o total de tráfego que passa por várias LANs poderia ser reduzido de maneira significativa.

- Detecção de mudanças rápidas em tabelas de roteamento. A alternância de rotas — mudanças frequentes em tabelas de roteamento — pode indicar instabilidades no roteamento ou um roteador mal configurado. Evidentemente, um administrador de rede que configurou um roteador de modo inapropriado prefere ele mesmo descobrir o erro antes que a rede caia.

- Monitoração de SLAs. Acordos de Nível de Serviços (*Service Level Agreements*) são contratos que definem parâmetros específicos de medida e níveis aceitáveis de desempenho do provedor de rede em relação a essas medidas

## 2.2 MODELO DE GERENCIAMENTO DE REDE

Segundo Kurose e Ross (2014) A ISO (*International Organization for Standardization*) define o gerenciamento de redes em cinco as áreas principais:

- Gerenciamento de desempenho. Sua meta é quantificar, medir, informar, analisar e controlar o desempenho de diferentes componentes da rede. Entre esses componentes estão dispositivos individuais como um trajeto pela rede.

- Gerenciamento de falhas. Seu objetivo é registrar, detectar e reagir às condições de falha da rede. A linha divisória entre gerenciamento de falha e gerenciamento de desempenho é bastante indefinida. Pode-se entender o primeiro como o tratamento imediato de falhas transitórias da rede enquanto o segundo adota uma abordagem de longo prazo em relação ao desempenho da rede em face de demandas variáveis de tráfego e falhas ocasionais na rede.

- Gerenciamento de configuração. Permite que um administrador de rede saiba quais dispositivos fazem parte da rede administrada e quais são suas configurações de hardware e software.

- Gerenciamento de contabilização. Permite que o administrador da rede especifique, registre e controle o acesso de usuários e dispositivos aos recursos da rede. Quotas de utilização, cobrança por utilização e alocação de acesso privilegiado a recursos fazem parte do gerenciamento de contabilização.

- Gerenciamento de segurança. Sua meta é controlar o acesso aos recursos da rede de acordo com alguma política bem definida. O uso de firewalls para monitorar e controlar pontos externos de acesso à rede é outro componente crucial.

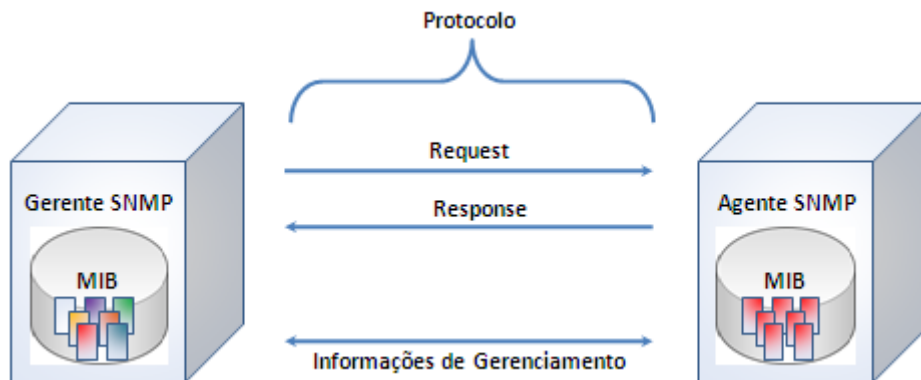
## 2.3 SNMP - PROTOCOLO SIMPLES DE GERENCIAMENTO DE REDES

O SNMP é um protocolo da camada de aplicação que pode usar qualquer mecanismo de transporte. Ele é mais usado com o UDP usando a porta 161, que é obrigatória para concordância com os padrões do SNMP. O SNMP é um protocolo de cliente-servidor, onde os agentes de gerenciamento se conectam com os dispositivos gerenciados e emitem requisições. Os dispositivos gerenciados retornam respostas (FARREL, 2005).

Segundo RFC 1157 (*Request for Comments*) (IETF, 2018) quatro operações foram definidas no SNMP que são:

- GET – esta operação possibilita ao software de gerenciamento recuperar uma instância de um objeto no agente.
- GETNEXT – esta operação permite ao software de gerenciamento recuperar a próxima instância de objetos de uma tabela ou lista. Inicia-se com uma operação “GET” e depois várias operações de “GETNEXT”.
- SET – possibilita ao software de gerenciamento alterar valores de uma instância de objetos no agente.
- TRAP – é utilizado pelo agente para informar ao software de gerenciamento algum evento ocorrido. Trap são alertas enviados do agente diretamente ao gerente, sem que este tenha solicitado previamente, para informações sobre mudanças de estado do agente.

No mundo do SNMP, existem dois tipos de entidades: gerenciadores e agentes. Um gerenciador é um servidor executando algum tipo de sistema de software que pode lidar com tarefas de gerenciamento de uma rede. Os gerenciadores costumam ser chamados NMS (*Network Management Stations* – estações de gerenciamento de rede). A Figura 1 apresenta o modelo SNMP com o gerente e o agente trocando informações.



**Figura 1 - Modelo SNMP gerente/agente**  
Fonte: DÉO(2018)

### 2.3.1 Versões do SNMP

A primeira publicação do SNMP foi no RFC 1067(IETF, 2018). Posteriormente, a RFC 1157(IETF, 2018) publicou a versão SNMPv1. A segunda versão do protocolo, o SNMPv2, foi publicado na RFC 1901(IETF, 2018), e incluiu melhorias, como a possibilidade de uma implementação de gerenciamento distribuído, novos objetos MIBs e alteração nos nomes e formatos de operações já existentes. A última versão do SNMP, o SNMPv3, foi



publicado na RFC 2571 (IETF, 2018), incluindo ao protocolo algumas questões de segurança e padronização da implementação dos agentes e gerentes, utilizando o SMI e a MIB do SNMPv2 (LOBÃO, 2011).

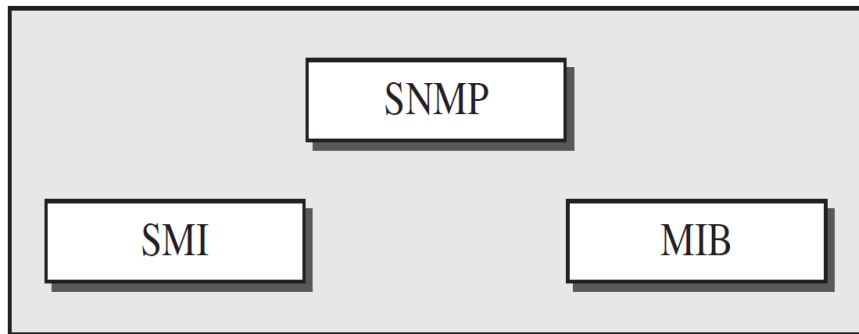
Douglas e Schmidt (2005) reiteram que o maior problema com o protocolo SNMP sempre foi a segurança, já que, nas duas primeiras versões, a autenticação entre a estação de gerência e os agentes era feita apenas por uma senha, chamada de *community*; essa senha é transferida entre o gerente e o agente de forma textual pura, sem nenhum tipo de criptografia. O principal objetivo de se criar uma nova versão do SNMP foi justamente melhorar a segurança, sendo que o SNMPv3 possui um método de autenticação que utiliza os algoritmos de criptografia MD5 (*Message Digest 5*) e SHA1 (*Secure Hash Algorithm 1*), substituindo o texto puro da *community* (DOUGLAS; SCHMIDT; 2005).

O SNMP evoluiu por meio de três gerações. Conseqüentemente, a versão atual é conhecida como SNMPv3. As mudanças entre as versões têm sido relativamente pequenas – todas as três versões usam a mesma estrutura geral e muitos recursos são compatíveis com as versões anteriores (COMER, 2006).

O SNMPv1 e o SNMPv2 não têm preocupação com a segurança, mesmo que em redes a troca de dados é segura, por exemplo usando os recursos do IPsec, que não há controle dentro dessas versões do SNMP quanto a quem na rede segura tem permissão de realizar operações SNMP e acessar os objetos nesse módulo MIB. Ou seja, qualquer usuário na rede que pode trocar pacotes UDP com dispositivo gerenciado será capaz de examinar e modificar os objetos MIB (FARREL, 2005).

Além da criptografia, o SNMPv3 implementa algumas outras regras de segurança, porém, não implementa nenhuma nova operação ao protocolo, suportando apenas as operações já conhecidas do SNMPv1 e do SNMPv2. O SNMPv3 ainda modificou alguns conceitos e terminologias, a principal delas foi o abandono da ideia de agente e gerente, passando a chamá-los de entidades SNMP. (DOUGLAS, SCHMIDT; 2005).

Para realizar suas tarefas de gerenciamento, o SNMP usa dois outros auxiliares: SMI (*Structure of Management Information* — estrutura de informações de gerenciamento) e MIB (*Management Information Base* — base de informações de gerenciamento). Em outras palavras, o gerenciamento na Internet é realizado por meio da cooperação de três protocolos: SNMP, SMI e MIB, conforme ilustrado na Figura 2 (FOROUZAN, 2006).



**Figura 2 – Cooperação de três protocolos**  
 Fonte: FOROUZAN(2006)

### 2.3.2 MIB (*Management Information Base*)

A arquitetura de gerenciamento SNMP, segundo Case (1990), consiste em: MIB (*Management Information Base*), que tem a função de descrever quais são os objetos contidos na mesma; SMI (*Structure and Identification of Management Information for TCP/IP-based Internets*), que descreve como os objetos gerenciados contidos na MIB são definidos; e o próprio SNMP, que é o protocolo a ser utilizado para gerenciar estes objetos.

Conhecido como Base de Informações de Gerenciamento (*Management Information Base - MIB*), o padrão especifica os itens de dados que cada dispositivo gerenciado precisa manter, as operações permitidas em cada um e o seu significado. Por exemplo, o MIB para IP especifica que o software precisa manter uma contagem de todos os octetos que chegam através de cada interface de rede e que o software de gerenciamento só pode ler a contagem. (COMER, 2006).

A MIB pode ser imaginada como um banco virtual de informações que guarda objetos gerenciados cujos valores, coletivamente, refletem o “estado” atual da rede. Esses valores podem ser consultados e/ou definidos por uma entidade gerenciadora por meio do envio de mensagens SNMP ao agente que está rodando em um dispositivo gerenciado em nome da entidade gerenciadora (KUROSE; ROSS, 2014).

Atualmente está em sua segunda versão (MIB2), definida na RFC (Request for Comments) 1213(IETF, 2018). Segundo Forouzan (2006), a MIB nada mais é do que uma coleção de todos os objetos que o gerente pode manipular no agente. A MIB2 é uma versão atualizada da MIB versão 1 e fornece informações gerais sobre o equipamento gerenciado. Os objetos contidos na MIB2 são categorizados em dez diferentes grupos. O Quadro 1 apresenta esses grupos e suas descrições.

**Quadro 1 - Descrição de grupos da MIB2**

<b>Objeto</b>	<b>OID</b>	<b>Descrição</b>
System	1.3.6.1.2.1.1	Define uma lista de objetos pertencentes á operação do sistema, como o tempo de funcionamento, contato e nome.
Interfaces	1.3.6.1.2.1.2	Mantém o status de cada interface da entidade que está sendo gerenciada ( <i>up</i> ou <i>down</i> , octetos enviados e recebidos, etc).
AT	1.3.6.1.2.1.3	Informações a respeito da tabela ARP ( <i>Address Resolution Protocol</i> ).
IP (Internet Protocol)	1.3.6.1.2.1.4	Informações a respeito de IP, incluindo roteamento.
ICMP ( <i>Internet Control Message Protocol</i> )	1.3.6.1.2.1.5	Informações a respeito do protocolo ICMP (erros, pacotes enviados e recebidos, etc).
TCP ( <i>Transmission Control Protocol</i> )	1.3.6.1.2.1.6	Informações sobre o protocolo TCP ( <i>closed, listen, synSen</i> , etc).
UDP ( <i>User Datagram Protocol</i> )	1.3.6.1.2.1.7	Informações sobre o protocolo UDP (datagramas internos e externos, etc).
EGP ( <i>Exterior Gateway Protocol</i> )	1.3.6.1.2.1.8	Informações gerais sobre o protocolo EGP.
Transmission	1.3.6.1.2.1.10	Reservado para MIBs específicas.
SNMP	1.3.6.1.2.1.11	Informações gerais sobre o protocolo SNMP.

**Fonte: Douglas e Schmidt(2005)**

Todos esses grupos pertencem a MIB2 e são utilizados pelo protocolo SNMP, porém, ainda há outros dois tipos de MIB: a MIB experimental, utilizada para objetos que estão em fase de desenvolvimento e testes; e a MIB privada, que contém objetos específicos do elemento gerenciado.

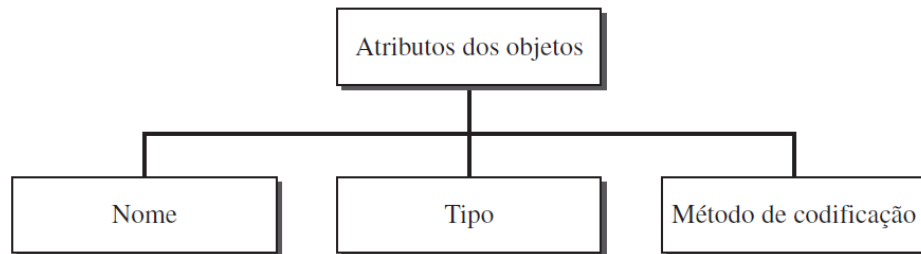
### **2.3.3 SMI (*Structue of Management Information*)**

A Estrutura de Gestão de Informação (Structure of Management Information - SMI) é a linguagem que define os objetos gerenciados, seu comportamento e garantem que a sintaxe e semântica dos dados sejam bem definidas e não tenham ambiguidade. (KUROSE e ROSS, 2009).

O SMI possui duas versões, sendo que a primeira foi apresentada na RFC1155(IETF, 2018) e é denominada SMIV1. Já a segunda, apresentada na RFC2578 (IETF, 2018), é denominada SMIV2 e apresenta melhorias para a segunda versão do protocolo SNMP, além de possuir novos tipos de dados, como o *Counter64*.

Segundo Forouzan (2006), o SMI tem três funções: nomear os objetos, definir o tipo de dados que são armazenados em determinado objeto e exibir o método de codificação para os dados a serem transmitidos. O SMI é uma diretriz para o SNMP. Ele enfatiza três atributos

que identificam um objeto: nome, tipo de dados e método de codificação conforme mostra a Figura 3.

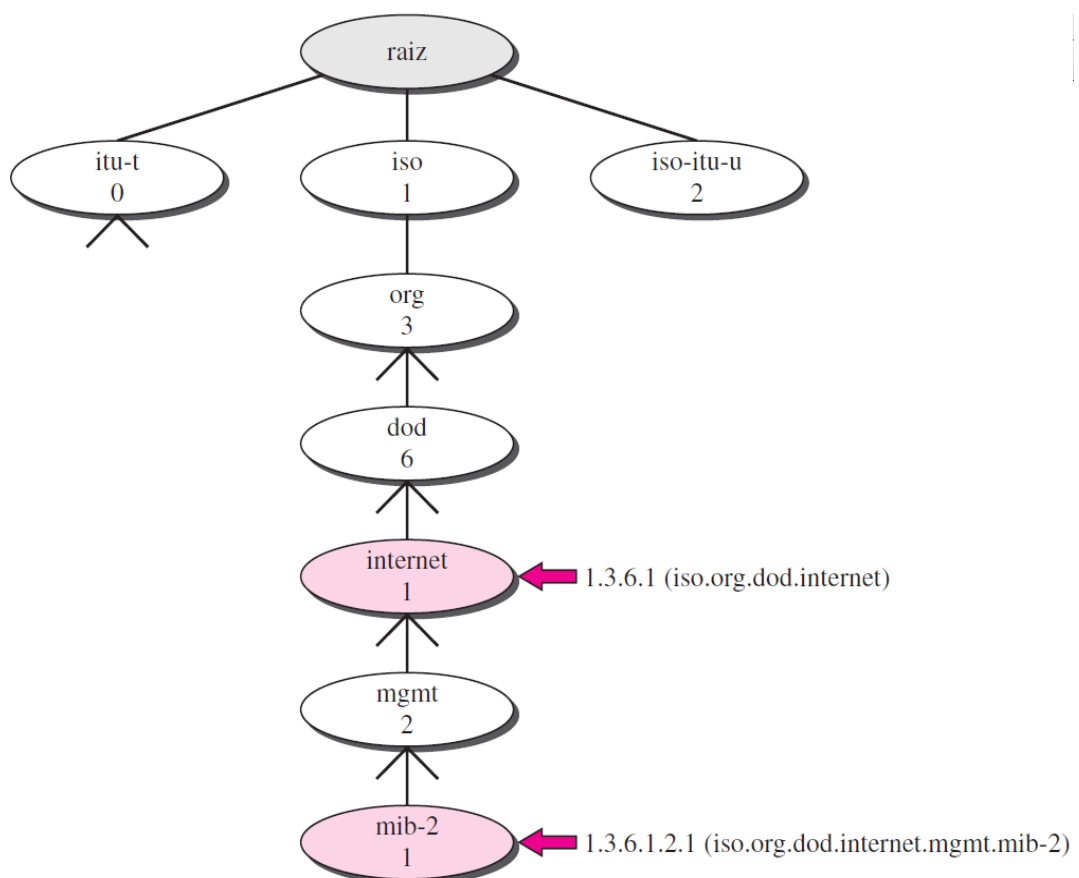


**Figura 3 - Atributos dos objetos**

Fonte: FOROUZAN (2006)

### 2.3.3.1 Nome ou OID

O SMI requer que cada objeto gerenciado (por exemplo, um roteador, uma variável em um roteador, um valor) tenha um nome exclusivo. Para atribuir nomes a objetos de forma global, o SMI usa um identificador de objetos, que é um identificador hierárquico com base em uma estrutura na forma de árvore conforme mostra a Figura 4 (FOROUZAN, 2006).



**Figura 4 - Nomes de identificador de objetos**

Fonte: FOROUZAN (2006)

### 2.3.3.2 Tipo

É responsável pelo tipo de dados dos objetos. O SMI possui dois tipos de dados: simples (dados atômicos que não possuem nenhuma relação entre si, como inteiros, caracteres, *strings*) e estruturados (dados constituídos por uma estrutura de dados simples que possuem relação entre seus valores, como os *structs* e *arrays*).

Segundo Comer (2006). O padrão SMI especifica que todas as variáveis MIB precisam ser definidas e referenciadas usando a ASN. 1 (*Abstract Syntax Notation 1*) da ISO. A ASN.1 é uma linguagem formal que possui dois recursos principais: uma notação usada em documentos lidos por humanos e uma representação codificada compacta das mesmas informações usadas nos protocolos de comunicação.

Além de especificar o nome e o conteúdo de cada item, a ASN.1 define um conjunto de regras de codificação básicas (*Basic Encoding Rules – BER*) que especifica precisamente como codificar nomes e itens de dados em uma mensagem (Comer, 2006).

O Quadro 2 apresenta os tipos de dados do SMIV2.

**Quadro 2 - Tipos de dados SMIV2**

<b>Tipo</b>	<b>Tamanho</b>	<b>Descrição</b>
INTEGER	4 bytes	Um inteiro com o valor entre $-2^{31}$ e $2^{31}-1$
Integer32	4 bytes	O mesmo que o INTEGER
Unsigned32	4 bytes	Valor entre 0 e $2^{32}-1$
OCTET STRING	Variável	Sequência de até 65,535 <i>bytes</i>
OBJECT IDENTIFIER	Variável	Um identificador de objeto
IPAddress	4 bytes	Um endereço IP composto de quatro inteiros
Counter32	4 bytes	Inteiro que pode ser incrementado de 0 até $2^{32}$ e quando atingir o máximo, volta ao valor de 0
Counter64	8 bytes	Contador de 64 <i>bits</i>
Gauge32	4 bytes	Inteiro que pode ser incrementado de 0 até $2^{32}$ e quando atingir o máximo não volta ao valor de 0, ao menos que seja zerado
TimeTicks	4 bytes	Contador que registra tempo em centésimo de segundos
BITS		Sequência de <i>bits</i>
Opaque	Variável	Sequência não interpretada

Fonte: Forouzan(2006)

### 2.3.3.3 Método de codificação

O SMI utiliza o BER (*Basic Encoding Rules*) para codificar os dados a serem transmitidos na rede. O BER é um conjunto de regras de codificação ASN.1 “que define a forma através da qual um programa escrito nessa linguagem é compilado para ser traduzido para a linguagem de máquina do dispositivo da rede” (BERNAL, 2014).

Além de especificar o nome e o conteúdo de cada item, a ASN.1 define um conjunto de regras de codificação básicas (*Basic Encoding Rules – BER*) que especifica precisamente como codificar nomes e itens de dados em uma mensagem. Portanto, uma vez que a documentação de um MIB tenha sido expressa usando ASN.1, as variáveis podem ser traduzidas direta e mecanicamente para a forma codificada usada nas mensagens (Comer, 2006).

## **2.4 FERRAMENTAS DE GERENCIAMENTO E MONITORAMENTO DE REDE**

Uma ferramenta de gerência de rede permite ao administrador monitorar e controlar dispositivos remotos na rede para garantir o bom funcionamento dos ativos e serviços, para que no caso de falhas providências possam ser tomadas, a fim de evitar indisponibilidade para os usuários. Várias ferramentas estão disponíveis no mercado e para definir qual ferramenta é a mais adequada ao cenário, foram analisadas as características e requisitos das ferramentas Zabbix, Cacti e The Dude.

### **2.4.1 Zabbix**

O Zabbix é um software livre (e de código fonte aberto – *Open Source*) com sistema de monitoramento distribuído capaz de monitorar a disponibilidade e diferentes aspectos da infraestrutura de rede, além das aplicações e serviços de rede. É sistema que consegue coletar informações de todos dispositivos que estão interligados na rede, absorvendo as informações por meio de scripts, via agente nativo do Zabbix, agente SNMP ou agente IPMI (*Intelligent Platform Management Interface*).

Existe uma dependência em relação à estrutura do Zabbix, visto que o mesmo foi projetado com o intuito de ser uma ferramenta de código aberto (*Open Source*), seu servidor necessariamente deve ser hospedado em uma máquina com o Linux ou Mac OS, visto que não existe um pacote do servidor disponível para as versões do Windows (ZABBIX, 2018).

#### **2.4.1.1 Características:**

- Monitora serviços simples (http, pop3, imap, ssh) sem o uso de agentes;

- Suporte nativo ao protocolo SNMP;
- Possui Interface de gerenciamento Web, de fácil utilização;
- Possui suporte a maioria dos sistemas operacionais: Linux, Solaris, Mac OS X, Windows;
- Possui Geração de gráficos em tempo real;
- Possui Integração com os Contadores de Desempenho do Windows;
- Software *Open Source* distribuído pela Licença GPL v2;
- Envia alertas para: e-mail;

#### 2.4.1.2 Requisitos:

Atualmente o Zabbix está na versão 3.2, sendo que a versão analisada foi a 3.0.5. Segundo a documentação oficial da ferramenta, para um monitoramento com menos de 100 hosts são necessários 128Mb de memória RAM e 256Mb livre em disco, mas esse valor pode variar dependendo da quantidade de hosts monitorados pela ferramenta.

## 2.4.2 Cacti

É um software livre, com *FrontEnd* em PHP (*Hypertext Preprocessor*) que utiliza a plataforma RRDTool (*Round Robin Database Tool*) para criar gráficos e armazenar informações dos estados da rede em banco de dados MySQL (*My Structured Query Language*). As informações são repassadas para a ferramenta através de scripts ou outros programas escolhidos pelo usuário os quais devem se encarregar de obter os dados. O Cacti é distribuído sob a licença GNU (*General Public License*). (CACTI, 2018).

#### 2.4.2.1 Características:

- Coleta de dados: o Cacti permite que o usuário faça a coleta de dados através de scripts externos, além do suporte ao protocolo SNMP.
- Gerenciamento de usuários: permite que o administrador crie usuários e aplique regras de permissões aos mesmos.

- Gráficos: o Cacti possui um número ilimitado de gráficos, podendo ser configurados como gráficos de área, linha, barra, entre outros, além de possibilitar ao administrador configurar cores, legendas e outros detalhes para facilitar a visualização do gráfico;

#### 2.4.2.2 Requisitos:

O Cacti pode ser instalado tanto em sistemas Windows quanto em sistemas Linux, e, para as duas plataformas, exige alguns pré-requisitos, que são: RRDTool 1.0.49 ou superior, MySQL 4.1.x ou superior, PHP 4.3.6 ou superior e um *web server* como o Apache, por exemplo.

### 2.4.3 The Dude

O software é desenvolvido pela empresa Mikrotik (MIKROTIK, 2018) para monitoramento e configuração dos seus equipamentos, mas também suporta ativos de rede de outros fabricantes utilizando o SNMP para realizar esta comunicação.

Roda em Windows, Linux via Wine e MacOS via Darwine, já na versão RouterOS a integração é nativa via Winbox, suporta Server Dude e cliente local, descobre qualquer marca ou tipo de dispositivo, até a versão 4.0 ele é *free* para rodar no windows, a partir dessa versão é necessário ter um aparelho mikrotik e a versão 6 da licença. Será adotado o uso da versão 4.0 rodando em Windows (MIKROTIK, 2018).

#### 2.4.3.1 Estrutura

O servidor The Dude é o programa em si, que é executado em segundo plano. Não tem nenhuma interface gráfica, e só pode ser controlado por um aplicativo cliente Dude localizado na máquina local ou em qualquer lugar na rede. Existe a possibilidade de conectar-se ao servidor The Dude através de uma interface web se não possuir um computador. O acesso web foi principalmente concebida como uma ferramenta de revisão rápida e acessível, não uma ferramenta completa.

O cliente The Dude pode se conectar ao servidor local ou remoto do Servidor e é usado como uma interface gráfica para isso. Isso significa que toda ação é realmente executada na máquina do servidor e o cliente está apenas mostrando fotos. Assim, os layouts



de janela do usuário são armazenados no servidor e não são perdidos na desconexão. (MIKROTIK, 2018)

#### 2.4.3.2 Características

- É gratuito;
- Faz a autodescoberta de dispositivos de rede;
- Descobre qualquer tipo ou marca de aparelho;
- Possui fácil monitoramento de links e faz notificações;
- Possui fácil instalação e utilização;
- Permite que se desenhe os próprios mapas personalizados e adicione dispositivos;
- Suporta SNMP, ICMP, DNS e TCP;
- Faz o monitoramento de uso de links com gráficos;
- Suporta servidor remoto e cliente local;

#### 2.4.3.3 Requisitos

O The Dude é executado na maioria das versões do Microsoft Windows. Recomenda-se usar o Windows 2000 ou mais recente. A aplicação é utilizada com sucesso mesmo em máquinas de muito baixa potência, de modo geral, qualquer sistema que possa executar o Windows 2000 ou o Windows XP poderá executar o The Dude. O programa também pode ser usado em Linux e MacOS se estiver usando Wine ou Darwine respectivamente (MIKROTIK, 2018).

#### 2.4.4 Escolha da ferramenta

O quadro a seguir, demonstra algumas comparações em pontos importantes que as ferramentas oferecem em relação ao gerenciamento.

**Quadro 3 - Comparativo entre ferramentas de gerenciamento e monitoramento de rede**

	ZABBIX	CACTI	THE DUDE
Notificações	Sim	Sim	Sim
Criação de mapas	Sim	Não	Sim
Interface Web	Controle Total	Controle Total	Controle Parcial
SNMP	Sim	Sim	Sim
Syslog	Sim	Não	Sim
Auto Descoberta	Sim		
Facilidade de Instalação / Configuração	Não	Sim	Sim
Apresentação Gráfica Intuitiva	Sim	Não	Sim

A escolha de uma ferramenta de monitoramento está diretamente ligada aos problemas e necessidades que surgem na empresa ou instituição. A definição ficou entre as ferramentas Zabbix e The Dude, devido ao fato de a ferramenta The Dude já estar implantada no servidor da prefeitura municipal de Pato Branco apenas com serviço de ping ativo em alguns setores, assim como a familiarização da equipe com parte de suas funcionalidades e das outras ferramentas analisadas. The Dude foi escolhido por ser a melhor alternativa para as necessidades do Município no momento.

### 3 MATERIAIS E METODOLOGIA

Este capítulo tem o propósito de descrever os materiais e método utilizado para a realização da segmentação e da implantação da ferramenta de gerenciamento de rede.

### 3.1 MATERIAIS

Para o desenvolvimento deste trabalho foram utilizados comutadores de pacotes (*switchs*) gerenciáveis com 24 portas Gigabit da marca Tp-link modelo TL-SG2424 para a camada de núcleo e Opticom modelo OPT-G524C4 para camadas de distribuição e acesso. Como mostra o Quadro 4, seguindo modelo hierárquico definido por (CISCO,2018).

**Quadro 4 – Tecnologias e ferramentas utilizadas na modelagem e na implementação do aplicativo**

<b>Ferramenta / Tecnologia</b>	<b>Versão</b>	<b>Aplicação</b>
SNMP	SNMPv2c	Protocolo simples de gerenciamento de redes
The Dude	3.6	Entidade gerenciadora
Comutador TP-LINK TL-SG2424 24 portas	2.0.0 Build 20160922 Rel.68676(s)	Camada de núcleo
Comutador Opticom OPT-G524C4 24 portas	1.1.0 Build 20140617 Rel.63710(n)	Camadas de distribuição e acesso
Snmwalk	Toolset-v11.0.6	Consulta bando MIB dos dispositivos
Windows Server	2008	Demais Servidores
Windows Server	2012	Servidor de dados
Windows Server	2003	Servidor da entidade gerenciadora

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 específico, pode ser usado para executar uma linha de comando e trazer a informação já filtrada para aquele OID.

### 3.2 METODOLOGIA

Para o desenvolvimento desse trabalho um levantamento na infraestrutura de rede da Prefeitura Municipal de Pato Branco fez-se necessário, para dimensionar os ativos de rede e dispositivos de cada setor, foi reunida a equipe da TI e levando em conta o conhecimento já adquirido sobre as peculiaridades da rede, passando em cada setor, e fisicamente analisando a quantidade de usuários e dispositivos conectados.

A ferramenta The Dude foi instalada no servidor e implantada, contendo como principal ponto de monitoramento o Ping de cada equipamento da rede.

Após levantamento realizado na infraestrutura junto ao com o Gerente de TI, foi realizada a troca de *switchs* nos setores de RH, Almoxarifado e no próprio CPD, onde foram colocados *Switchs* com velocidade Gbps.

O próximo passo foi levantar se a ferramenta The Dude continuaria sendo utilizada, com possibilidade de implementar novas funções, ou se seria necessário a instalação de outra ferramenta.

Por ser a melhor alternativa para as necessidades no momento, foi escolhido The Dude e realizada a configuração da ferramenta e adicionado novo mapa de rede com seus dispositivos.

## **4 RESULTADOS**

### **4.1 A PREFEITURA MUNICIPAL DE PATO BRANCO**

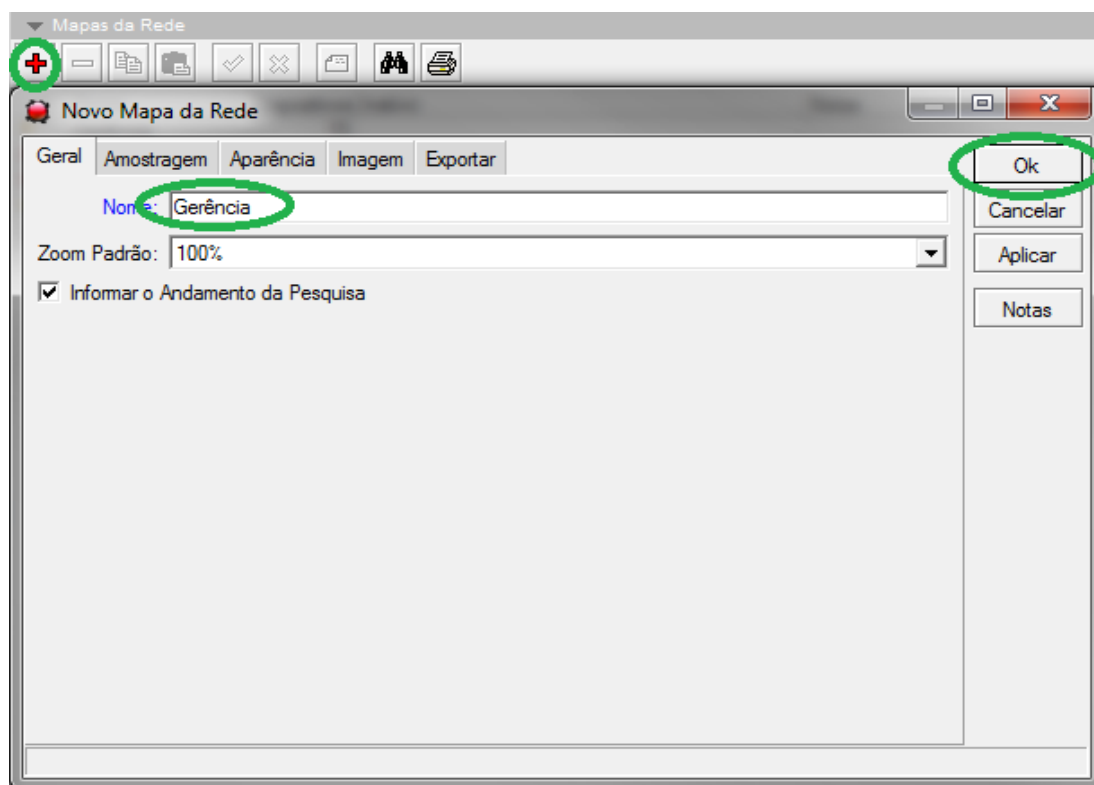
O Prédio da Prefeitura Municipal de Pato Branco foi inaugurado no ano de 1968. O CPD (Central de Processamento de Dados) que é onde ficam os servidores e serviços de tecnologia, entrou em funcionamento no ano de 2002, unificando as redes existentes até então no prédio. Desde então a equipe vem realizando o trabalho de assistência técnica dos equipamentos de informática de todas as secretarias municipais. Também realiza a manutenção da rede e dos servidores (*Data Center*) da prefeitura.

### **4.2 MONITORAMENTO DA REDE**

Para fornecer informações à equipe responsável pela manutenção da rede, da situação atualizada dos *switchs* e da utilização dos enlaces de dados foi utilizado o software The Dude.

The Dude possui uma funcionalidade onde é possível criar mais de um mapa de rede para gerenciamento. Há atualmente na prefeitura duas redes, sendo uma interna onde foi criado no The Dude o mapa de rede **Gerência**, e a rede WAN (*Wide Area Network*) denominada Interligação na qual já possuíamos um mapa criado no software somente com monitoramento de *ping*. A Prefeitura Municipal de Pato Branco depende de empresa terceirizada para realizar a ativação do protocolo nos aparelhos, considerando que o contrato com a operadora local está chegando ao seu prazo final e no mesmo não constar nenhuma cláusula obrigatória em relação à ativação do protocolo SNMP em seus roteadores, não foi

possível a implantação no cenário da Interligação, porém o mapa de rede foi criado e a rede mapeada ficando assim para trabalhos futuros a implementação do protocolo SNMP na rede da interligação. Sendo assim o protocolo SNMP foi ativado nos dispositivos da rede de Gerência que é composta por um Switch camada de núcleo, switches camada de distribuição e acesso, servidores e dispositivos finais. A Figura 5 a seguir mostra o processo de criação do mapa de rede.



**Figura 5 - Novo Mapa de rede**

Fonte: Autoria Própia

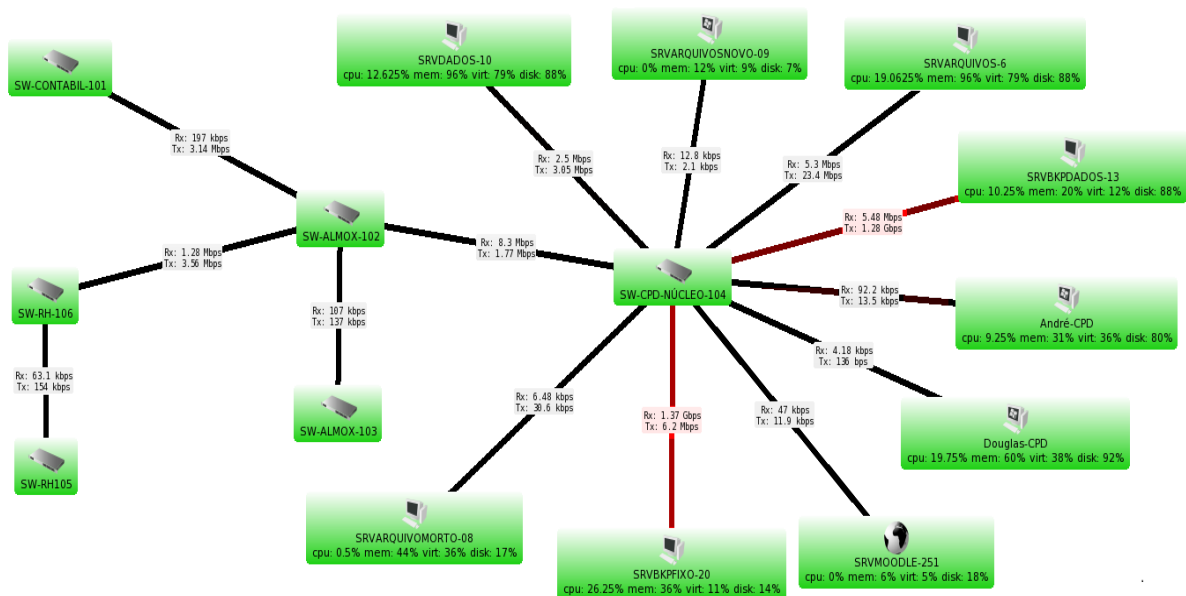
Para criar um mapa, como é possível observar na Figura 5, basta clicar no botão “+” e a janela de Novo mapa de Rede é aberta, onde basta colocar o nome e clicar em Ok, avançar e o mapa está criado.

A Figura 6 mostra o mapa de rede Interligação com os dispositivos espalhados pela cidade que abrangem escolas, Centros Municipais de Educação Infantil (CMEI), Unidades básicas de saúde entre outros departamentos.



**Figura 6 - Painel de monitoramento rede Interligação The Dude**  
Fonte: Autoria Própria

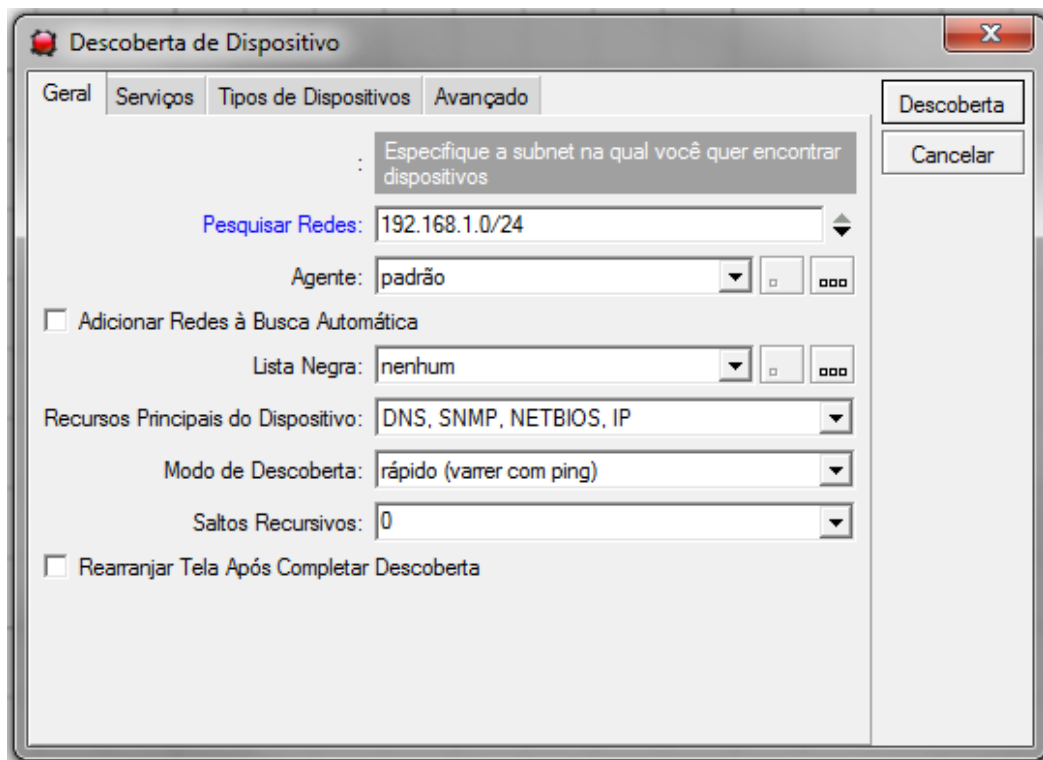
Após realizar a configuração do SNMP nos *switchs*, servidores e computadores de setores chave, cada dispositivo foi adicionado ao mapa de rede e realizado as configurações para a apresentação dos dados, como pode ser visto na Figura 7.



**Figura 7 - Painel de monitoramento rede Gerência The Dude**  
Fonte: Autoria Própria

O mapa de rede “Gerência” foi criado para monitorar a rede interna da prefeitura, com seus principais ativos de rede, onde é possível visualizar na Figura 7 o Switch SW-CPD-NÚCLEO, que se trata do *switch* de núcleo, o *switch* SW-ALMOX-102 foi utilizado para camada de distribuição, e os demais *switchs* para camada de acesso.

The Dude possui uma função de descoberta automática de dispositivos, com a possibilidade de selecionar algumas opções e realizar uma busca de dispositivos conectados na rede. Clicando no botão descoberta de dispositivo abre-se a janela para descoberta automática como mostra a Figura 8, nela é possível adicionar o endereço de rede com a máscara, marcar as opções necessárias desejadas e o software faz a descoberta de dispositivos.

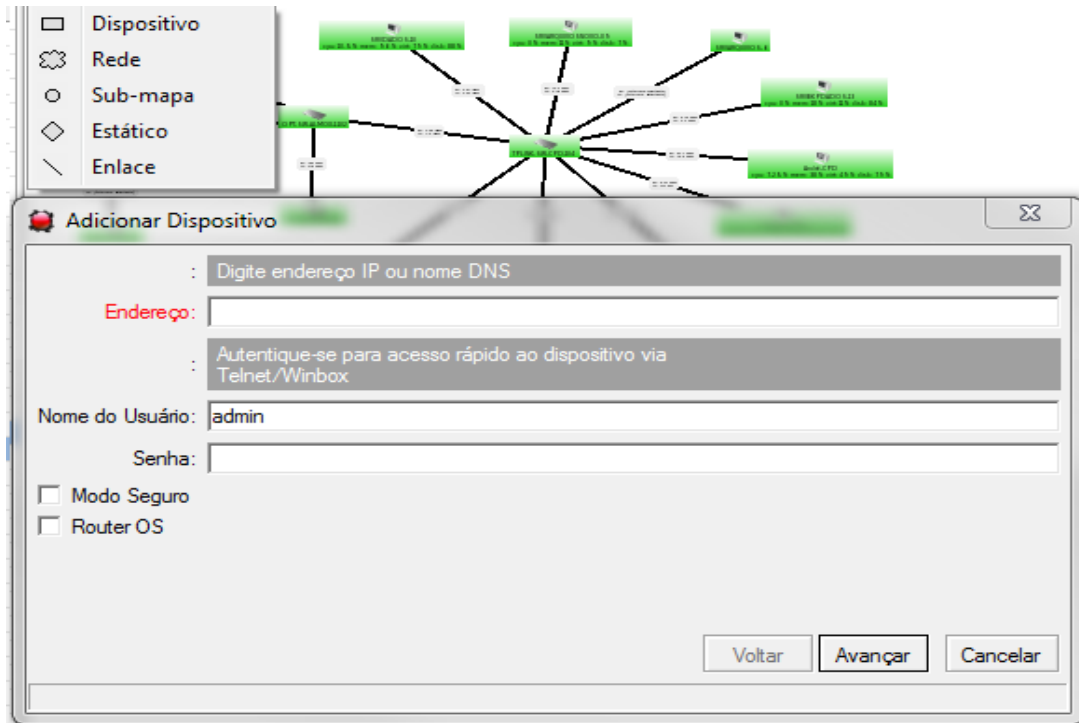


**Figura 8 - Descoberta de Dispositivo**

Fonte: Autoria Própria

É possível também adicionar novos dispositivos colocando seu nome ou endereço IP e avançar para configuração como mostra a

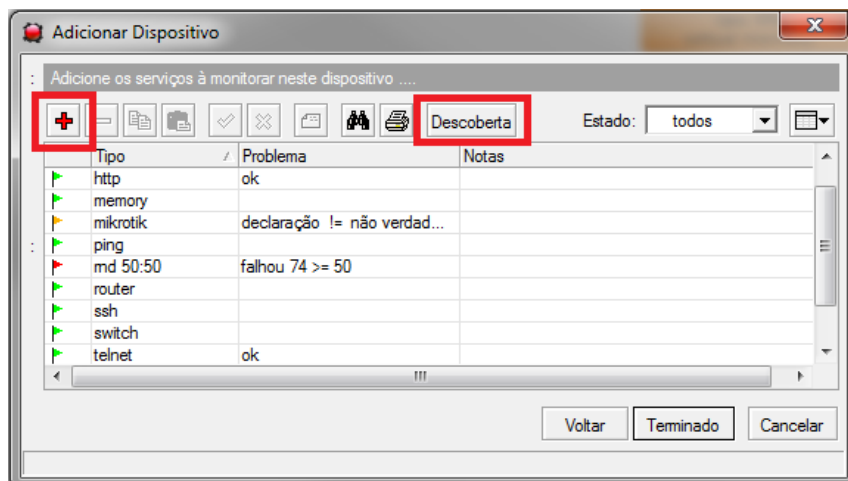
Figura 9.



**Figura 9 - Adicionando dispositivo ao The Dude**  
Fonte: Autoria Própria.

Clicando no botão “+” é possível inserir novos serviços, ou clicar no botão “descoberta” que o The Dude faz uma descoberta nos serviços disponíveis no dispositivo, como mostra a

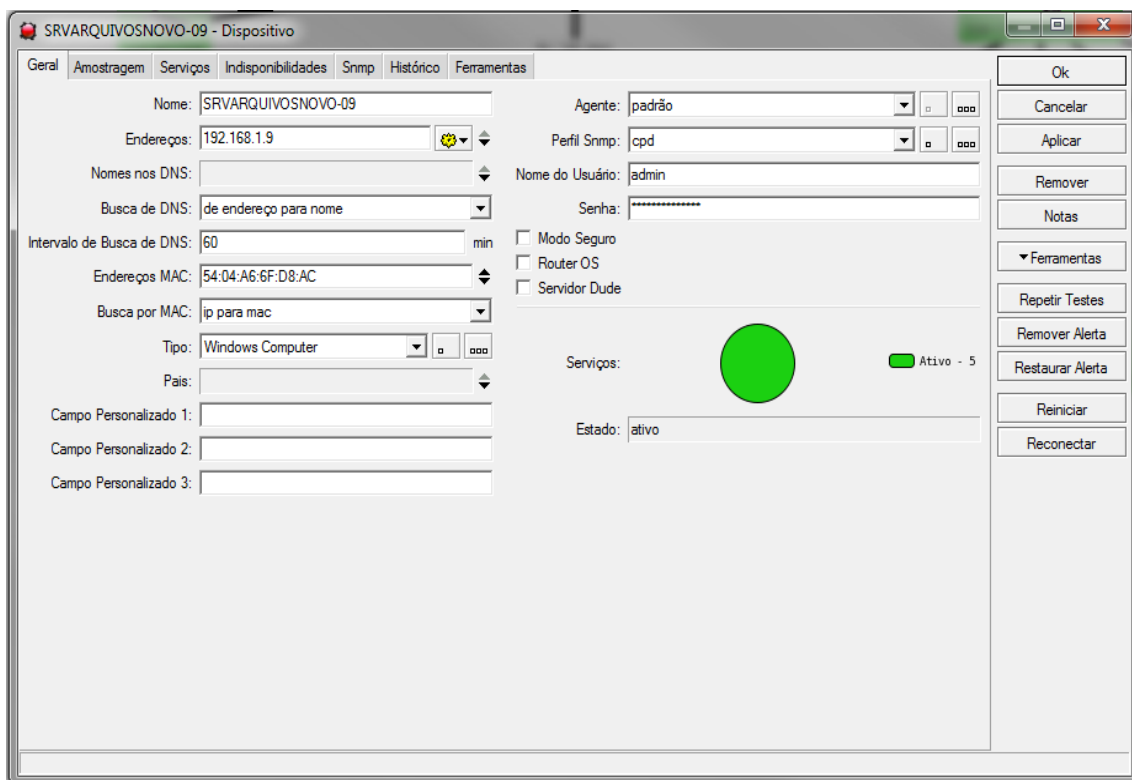
Figura 10.



**Figura 10 - Descoberta de serviços**  
Fonte: Autoria Própria



Depois de adicionado o dispositivo na próxima aba é possível alterar algumas configurações importantes que constam na aba geral como mostra a Figura 11.

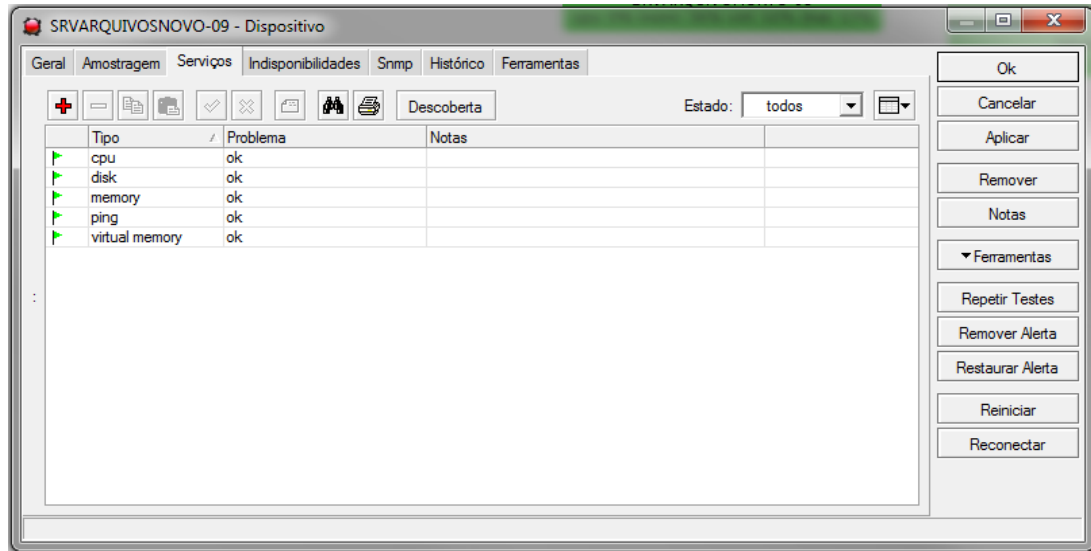


**Figura 11 - Configurações do dispositivo**

Fonte: Autoria Própria

- Nome - qualquer nome, por exemplo, nosso SRVARQUIVOSNOVO-09
- Endereços - os endereços IP do dispositivo.
- Nomes de DNS - Nomes de DNS do dispositivo se houver.
- MAC - endereços MAC do dispositivo.
- Tipo - Tipo de dispositivo para selecionar o ícone a ser usado no mapa. Um dispositivo (genérico) é usado por padrão.
- Campos Personalizados - Podem ser usados campos personalizados, como endereço, coordenadas ou informações de contato.
- Perfil SNMP - perfil de SNMP a ser utilizada para este dispositivo. Padrão de seleção entre SNMP1 e 2, pode-se adicionar SNMPv3 abrindo a janela de edição.
- Nome de Usuário e Senha - Como acessar o dispositivo a partir do menu Ferramentas, utilizado apenas para dispositivos Mikrotik
- Dude Server - Se for outro servidor Dude que poderia ser usado como um agente

Na aba de Serviços, mostrada na Figura 12 pode-se realizar a busca de serviços que o The Dude tem por padrão e que estão ativos no dispositivo pelo protocolo SNMP ou adicionar novos serviços.



**Figura 12 - Configurações do dispositivo aba Serviços**

Fonte: Autoria Própria

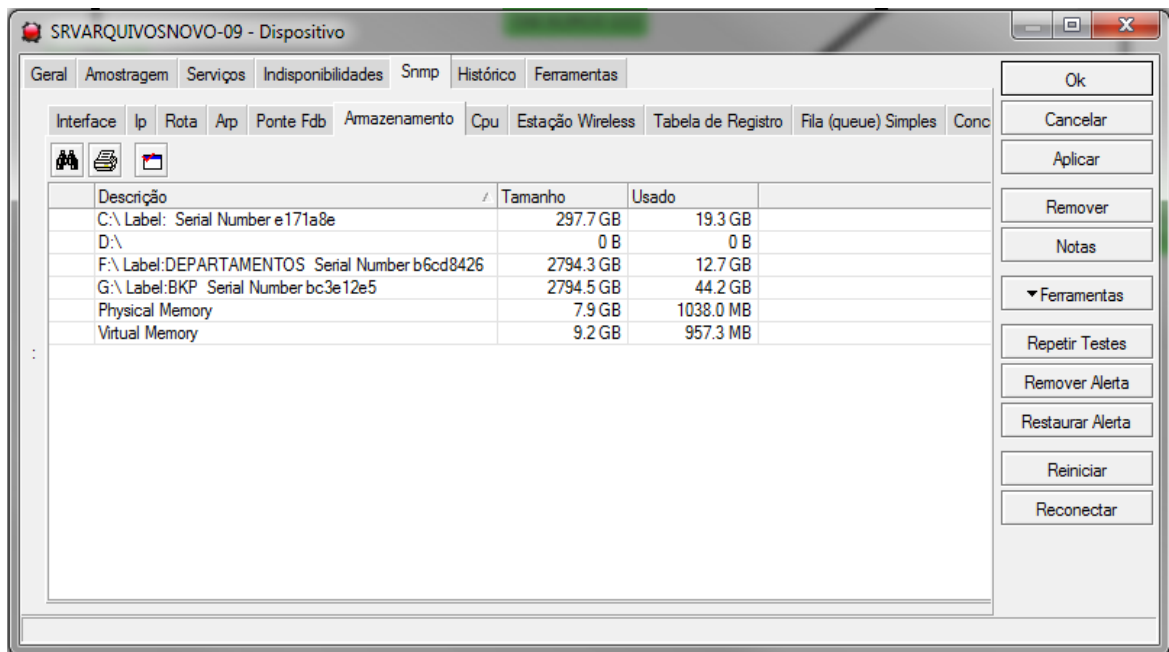
Na Aba SNMP tem-se outras abas com várias informações que são fornecidas pelo dispositivo através do protocolo SNMP, dentre as quais com mais relevância para esse trabalho as abas de: Interface, IP, Rota, ARP, Armazenamento e CPU, que são mostrados na Figura 13.

Nome	Tipo	MTU	Taxa de TX	Taxa de Re...
Adaptador do Mi...	tunnel	1280	0 bps	0 bps
Adaptador do Mi...	tunnel	1280	0 bps	0 bps
Adaptador do Mi...	tunnel	1280	0 bps	0 bps
Adaptador do Mi...	tunnel	1280	0 bps	0 bps
X Microsoft Keme...	ethernet-csma...	0	0 bps	0 bps
Miniporta WAN (...)	tunnel	1480	0 bps	0 bps
Miniporta WAN (...)	ppp	1494	0 bps	0 bps
Miniporta WAN (...)	tunnel	4091	0 bps	0 bps
Miniporta de Re...	ethernet-csma...	1500	0 bps	0 bps
Miniporta de Re...	ethernet-csma...	1500	0 bps	0 bps
Miniporta de Re...	ethernet-csma...	1500	0 bps	0 bps
Miniporta de red...	ethernet-csma...	1500	0 bps	0 bps
Miniporta de red...	ethernet-csma...	1500	0 bps	0 bps
Miniporta de red...	ethernet-csma...	1500	0 bps	0 bps
Miniporta de red...	ethernet-csma...	1500	0 bps	0 bps
Miniporta de red...	ethernet-csma...	1500	0 bps	0 bps
Miniporta de red...	tunnel	1460	0 bps	0 bps
Miniporta de red...	ethernet-csma...	1500	0 bps	0 bps
Miniporta de red...	ethernet-csma...	1500	0 bps	0 bps
Miniporta de red...	ethernet-csma...	1500	0 bps	0 bps
Miniporta de red...	ethernet-csma...	1500	0 bps	0 bps
Miniporta de red...	ethernet-csma...	1500	0 bps	0 bps
Miniporta de red...	ethernet-csma...	1500	0 bps	0 bps
Miniporta de red...	tunnel	1464	0 bps	0 bps
X RAS Async Ada...	ppp	0	0 bps	0 bps
Realtek PCIe G...	ethernet-csma...	1500	2.42 kbps	10.1 kbps
Realtek PCIe G...	ethernet-csma...	1500	8 bps	4.46 kbps
Realtek PCIe G...	ethernet-csma...	1500	8 bps	4.46 kbps
Realtek PCIe G...	ethernet-csma...	1500	8 bps	4.46 kbps
Realtek PCIe G...	ethernet-csma...	1500	8 bps	4.46 kbps
Realtek PCIe G...	ethernet-csma...	1500	8 bps	4.46 kbps
Realtek PCIe G...	ethernet-csma...	1500	7.2 kbps	15.1 kbps
Realtek PCIe G...	ethernet-csma...	1500	7.2 kbps	15.1 kbps

**Figura 13 - Interfaces descobertas pelo SNMP**

Fonte: Autoria Própria

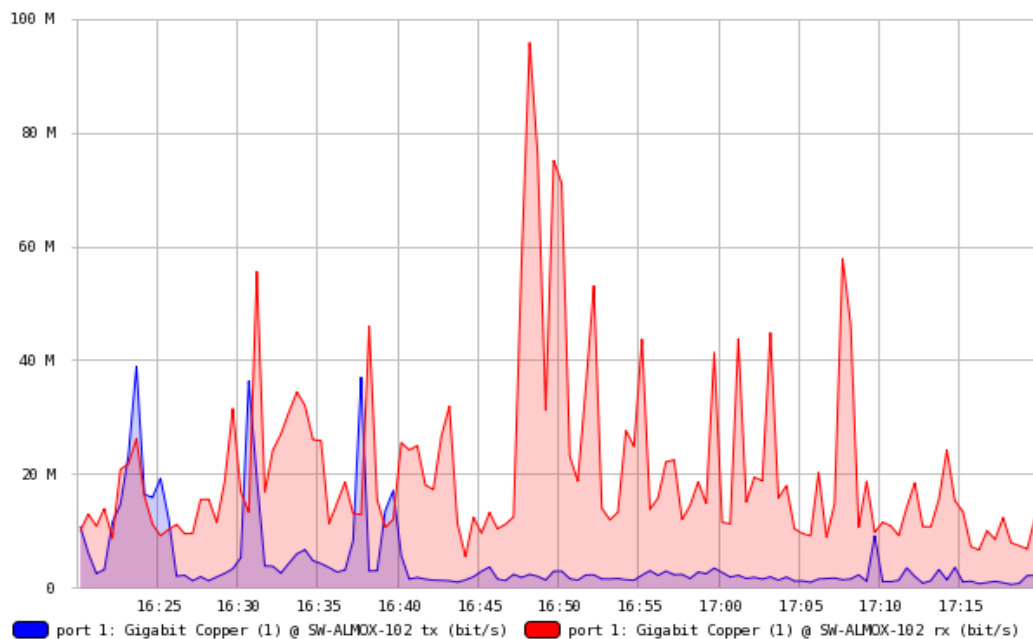
Na Figura 14 é possível observar o armazenamento do dispositivo, Descrição, tamanho e quando está sendo usado.



**Figura 14 - Armazenamento do dispositivo**

Fonte: Autoria Própria

Através da ferramenta The Dude a equipe de tecnologia da informação consegue monitorar os ativos de rede a fim de diagnosticar com mais facilidade caso um enlace de dados ou dispositivos apresente algum problema. Também é possível diagnosticar a largura de banda utilizada em cada enlace de dados como é apresentado na Figura 15.

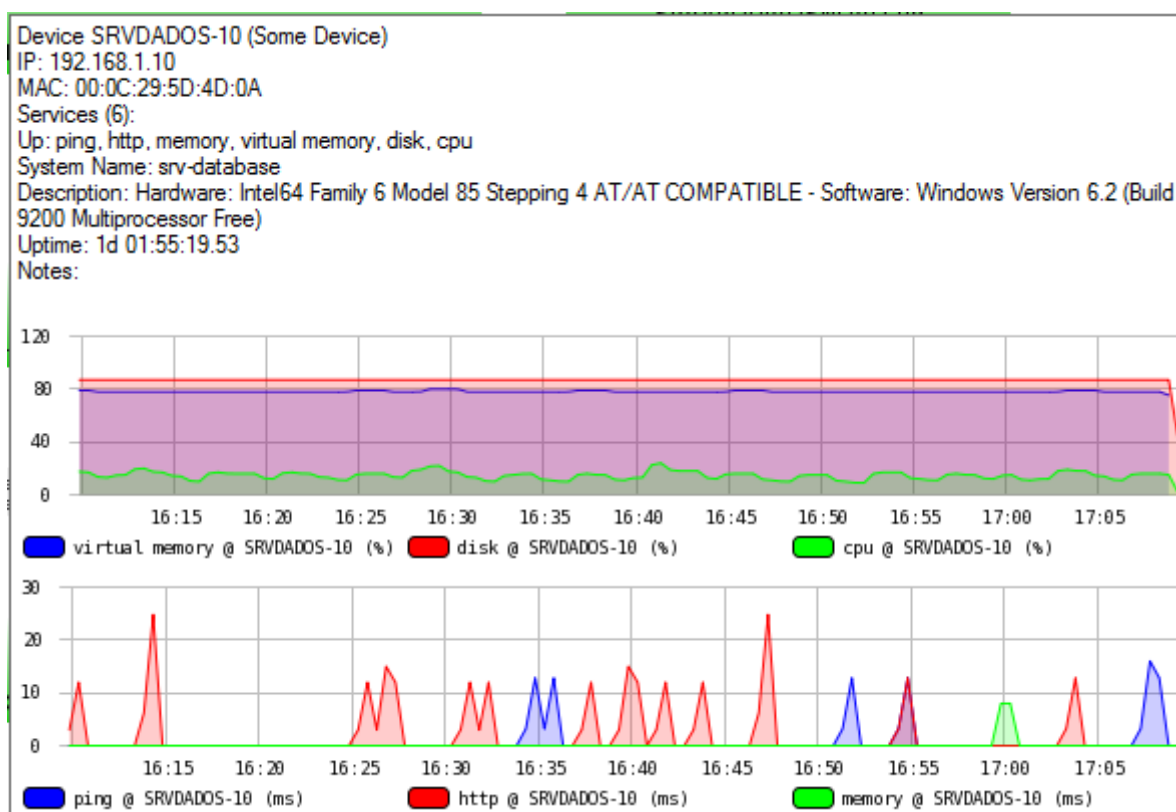


**Figura 15 - Largura de banda entre enlaces.**

Fonte: Autoria Própria.

É possível visualizar na Figura 15 um pico de transferência de aproximadamente 100Mbps às 16:47h em um enlace da rede, esse gráfico torna possível uma análise mais detalhada por parte da equipe de tecnologia para determinar quais são os momentos de mais utilização de tráfego nos enlaces, determinando com o monitoramento do gráfico se a ocorrência é normal ou algo está errado na rede.

Alguns MIBs foram adicionados ao The Dude devido à heterogeneidade encontrada na rede, permitindo assim a possibilidade de adição de novos serviços para monitoramento por parte da equipe de TI. A Figura 16 mostra os serviços de ping, http, memória, memória virtual utilização de disco de um dos servidores da Prefeitura.

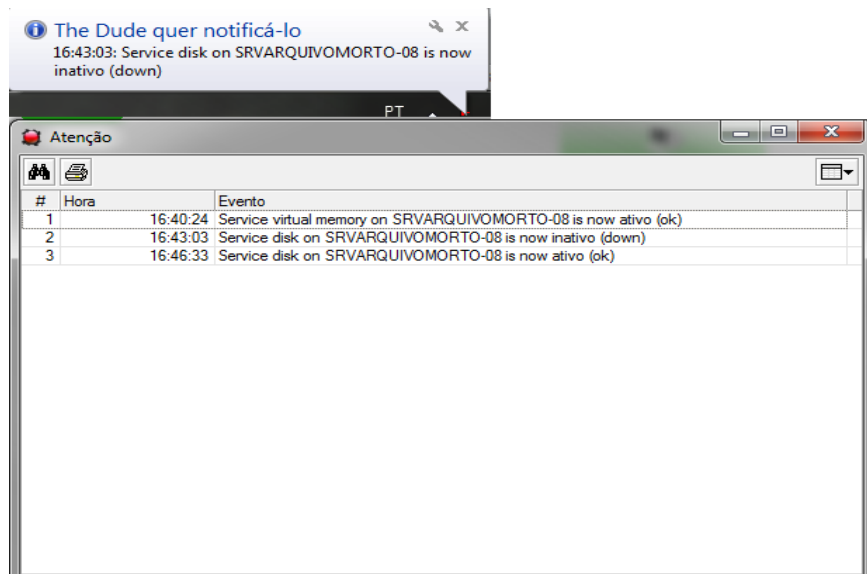


**Figura 16 - Servidor de dados.**

Fonte: Autoria Própria

A ferramenta possibilita que a equipe de Tecnologia da informação com base na análise das diversas informações que o software é capaz de produzir, como quando um link está *down*(inativo), gerar um alerta, assim a equipe pode saber exatamente onde está o problema, ou seja o tempo que era perdido atendendo usuário e deslocando equipe para procurar onde estava o problema é otimizado na resolução do mesmo.

A Figura 17, apresenta um exemplo de alerta em *pop-up* e logo abaixo a janela de alerta.



**Figura 17 - Alerta de serviço inativo**  
Fonte: Autoria Própria

Outra função importante é o arquivo de *log* que o The Dude gera, bastando selecionar no dispositivo a opção de salvar no *log*. Acessando o arquivo é possível verificar quando um dispositivo ficou inativo, e, se reestabeleceu a conexão também será registrado, como mostra a Figura 18.

Hora	Endereço	Evento
Feb/16 08:27:50	192.168.10.53	Service ping on CMEI Merino Deus wan 10.53 lan 44.1 Ramal 6064 is now ativo (ok)
Feb/16 08:27:50	192.168.10.56	Service ping on CMEI Cnanga Feliz wan 10.56 lan 47.1 Ramal 6028 is now ativo (ok)
Feb/16 08:31:48	192.168.0.234	Service ping on Aficio MP 301 - AdmEducação is now ativo (ok)
Feb/16 08:32:18	192.168.0.234	Service printer on Aficio MP 301 - AdmEducação is now ativo (ok)
Feb/16 08:34:17	192.168.5.187	Service ping on EMERSON-PC is now ativo (ok)
Feb/16 08:36:40	192.168.0.89	Service ping on MAURO089 is now ativo (ok)
Feb/16 08:40:03	192.168.0.115	Service ping on INDI115 is now inativo (tempo esgotado)
Feb/16 08:40:58	192.168.5.118	Service netbios on ENGENHARIA-PC is now ativo (ok)
Feb/16 08:43:41	192.168.0.231	Service ping on Aficio MP 301- Compras is now ativo (ok)
Feb/16 08:43:41	192.168.10.38	Service ping on Esc União wan10.38 lan 29.1 Ramal 6044 is now ativo (ok)
Feb/16 08:44:12	192.168.0.231	Service printer on Aficio MP 301- Compras is now ativo (ok)
Feb/16 08:44:17	192.168.5.225	Service netbios on IPPUPB-PC is now ativo (ok)
Feb/16 08:44:19	192.168.5.118	Service netbios on ENGENHARIA-PC is now inativo (tempo esgotado)
Feb/16 08:47:57	192.168.0.180	Service ping on MEIOAMB0180 is now inativo (tempo esgotado)
Feb/16 08:54:04	192.168.0.115	Service ping on INDI115 is now ativo (ok)
Feb/16 09:02:30	192.168.0.85	Service ping on ComMazin085 - Mazinho is now ativo (ok)
Feb/16 09:17:30	192.168.0.206	Service ping on JURID0206 - Estagiário is now inativo (tempo esgotado)
Feb/16 09:18:20	192.168.0.206	Service ping on JURID0206 - Estagiário is now ativo (ok)
Feb/16 09:24:35	192.168.0.105	Service ping on Comunic0105 - Mariza is now inativo (tempo esgotado)
Feb/16 09:33:07	192.168.10.38	Service ping on Esc União wan10.38 lan 29.1 Ramal 6044 is now inativo (tempo esgotado)
Feb/16 09:35:57	192.168.10.38	Service ping on Esc União wan10.38 lan 29.1 Ramal 6044 is now ativo (ok)
Feb/16 09:41:37	192.168.10.38	Service ping on Esc União wan10.38 lan 29.1 Ramal 6044 is now inativo (tempo esgotado)
Feb/16 09:56:23	192.168.10.38	Service ping on Esc União wan10.38 lan 29.1 Ramal 6044 is now ativo (ok)
Feb/16 10:03:05	192.168.10.121	Service ping on Esc Veneza wan 10.121 lan 104.1 Ramal 6078 is now inativo (tempo esgotado)
Feb/16 10:04:11	192.168.10.121	Service ping on Esc Veneza wan 10.121 lan 104.1 Ramal 6078 is now ativo (ok)
Feb/16 10:30:45	192.168.5.118	Service netbios on ENGENHARIA-PC is now ativo (ok)

**Figura 18 - Arquivo de log**  
Fonte: Autoria Própria

## 5 CONCLUSÕES

A importância das redes de computadores na vida das pessoas está implícita diariamente, mesmo para aqueles cuja vida não está diretamente ligada às tecnologias de comunicação. O gerenciamento e o monitoramento da rede garantem um serviço estável e confiável, aumentando significativamente a estabilidade da mesma.

A interface do The Dude é amigável e de fácil manipulação, além de possuir apresentação visual das informações, isso torna a ferramenta de gerenciamento o ponto central de consulta caso exista alguma suspeita ou uma eventual falha venha a ocorrer facilitando o diagnóstico e conseqüentemente diminuído o tempo necessário para que se restabeleça o serviço. Assim a equipe de TI pode economizar o tempo que era desperdiçado na identificação do problema, para resolução ou até prevenção do mesmo.

The Dude foi determinado como a solução mais adequada ao cenário apresentado, neste caso, a rede da Prefeitura de Pato Branco. Cabe ressaltar que as três ferramentas analisadas possuem o mesmo objetivo, todavia cada uma com as suas características. Destaca-se também que este estudo não teve a pretensão de definir qual era a melhor ferramenta, mas sim, qual se comportou de forma mais adequada durante o período de análise no referido cenário.

Este estudo também contribuiu para o desenvolvimento pessoal do autor, visto que ampliou seus conhecimentos através do trabalho multidisciplinar implementado, possibilitando a aplicação de diversos conteúdos apreendidos ao longo do curso.

### 5.1 TRABALHOS FUTUROS

Como sugestão para trabalhos futuros sugere-se a implantação do protocolo SNMP na rede de interligação, como mencionado nas Seções 3.2 e 4.2.

## REFERÊNCIAS

- ALBUQUERQUE, Fernando. **TCP/IP Internet Protocolos & Tecnologias**. 3ª edição. 2001.
- BERNAL, Huber F. **Simple Network Management Protocol (SNMP)**. Janeiro de 2014. Disponível em: [http://www.teleco.com.br/tutoriais/tutorialsnmp/pagina\\_1.asp](http://www.teleco.com.br/tutoriais/tutorialsnmp/pagina_1.asp). Acesso em: 15 de outubro de 2018.
- CACTI. **Documentation and Howtos**. Disponível em: <https://docs.cacti.net/>. Acesso dia 15 de agosto de 2018.
- CASE, J et al. **A Simple Network Management Protocol (SNMP)**, RFC1157, Maio 1990. Disponível em: <https://www.ietf.org/rfc/rfc1157>. Acesso em: 10 de setembro de 2018.
- CISCO. **CCNA EXPLORATION 6.0**. 2018, disponível em <http://pb.utfpr.edu.br/redes/cisco>. Acesso em 10 de novembro de 2018.
- COMER, Douglas E. **Interligação de redes com TCP/IP**. 5ª edição. 2006.
- DÉO, André. **Gerenciamento de Redes – O Protocolo SNMP**. 2011. Disponível em [http://andredeo.blogspot.com.br/2011\\_09\\_01\\_archive.html](http://andredeo.blogspot.com.br/2011_09_01_archive.html). Acesso em 25 de setembro de 2018.
- DOUGLAS, Mauro R.; SCHMIDT, Kevin J. **Essential SNMP**, 2nd ed, Sebastopol, O'Reilly Media, 2005.
- FARREL, Adrian. **A internet e seus protocolos**. 2005.
- FOROUZAN, Behrouz A. **Comunicação de Dados e Redes de Computadores**, 3.ed, Tradução de Glayson Eduardo de Figueiredo, Porto Alegre, Bookman, 2006.
- FOROUZAN, Behrouz A., MOSHARRAF, Firouz. **Redes de Computadores: Uma Abordagem Top-Down**. 1ª. Edição, 2013.
- IETF. **RFC 1067**. Disponível em: <https://tools.ietf.org/html/rfc1067>. Acesso em 10 de outubro de 2018.
- IETF. **RFC 1155**. Disponível em: <https://tools.ietf.org/html/rfc1155>. Acesso em 10 de outubro de 2018.
- IETF. **RFC 1157**. Disponível em: <https://www.ietf.org/rfc/rfc1157>. Acesso em 10 de outubro de 2018.
- IETF. **RFC 1213**. Disponível em: <https://tools.ietf.org/html/rfc1213>. Acesso em 15 de outubro de 2018.
- IETF. **RFC 2571**. Disponível em: <https://tools.ietf.org/html/rfc2571>. Acesso em 15 de outubro de 2018.

IETF. **RFC 2578**. Disponível em: <https://tools.ietf.org/html/rfc2578>. Acesso em 15 de outubro de 2018.

KUROSE, J. F., ROSS, K. W., **Redes de computadores e a internet – uma abordagem top-down**, 6ª Edição, 2014.

LOBÃO, Henrique F. **Comparativo entre as versões do SNMP**. Setembro de 2011. Disponível em <http://www.fassi.eti.br/artigos/gerencia-de-redes/comparativo-entre-as-versoes-do-snmp>. Acesso em: 20 de outubro de 2018.

MAURA, D. R., SCHMIDT, K. J., **SSNP Essencial**. Campus, 2001.

MIKROTIK. **Mikrotik Routers and Wireless**. 2018. Disponível em <http://www.mikrotik.com/thedude.php>. Acesso em 15 de agosto de 2018.

SNMPWALK. **Manpage of SNMPWALK**. 2012. Disponível em <http://www.netsnmp.org/docs/man/snmpwalk.html>. Acesso em 10 de novembro de 2018.

SPECIALSKI, Elizabeth. S. **Gerência de Redes de Computadores e de Telecomunicações**, Universidade Federal de Santa Catarina, Florianópolis, 1999.

ZABBIX. **Documentation**. 2018. Disponível em <https://www.zabbix.com/manuals>. Acesso em 15 de agosto de 2018.