UNIVERSIDADE TECNOLÓGICA FEDERAL DO PARANÁ
DIRETORIA DE PESQUISA E PÓS-GRADUAÇÃO
DEPARTAMENTO ACADÊMICO DE ELETRÔNICA
CURSO DE ESPECIALIZAÇÃO EM AUTOMAÇÃO INDUSTRIAL

ALEX SANDRO IVANKIO

MONITORAMENTO DE EQUIPAMENTOS DA REDE DE AUTOMAÇÃO EM SUBESTAÇÕES UTILIZANDO O PROTOCOLO SNMP

MONOGRAFIA DE ESPECIALIZAÇÃO

CURITIBA
2018

ALEX SANDRO IVANKIO

MONITORAMENTO DE EQUIPAMENTOS DA REDE DE AUTOMAÇÃO EM SUBESTAÇÕES UTILIZANDO O PROTOCOLO SNMP

Monografia de Especialização, apresentada ao Curso de Especialização em Automação Industrial, do Departamento Acadêmico de Eletrônica – DAELN, da Universidade Tecnológica Federal do Paraná – UTFPR, como requisito parcial para obtenção do título de Especialista.

Orientador: Prof. Dr. Valmir de Oliveira

CURITIBA
2018

Ministério da Educação
Universidade Tecnológica Federal do Paraná
Câmpus Curitiba

Diretoria de Pesquisa e Pós-Graduação
Departamento Acadêmico de Eletrônica
Curso de Especialização em Automação Industrial

TERMO DE APROVAÇÃO

MONITORAMENTO DE EQUIPAMENTOS DA REDE DE AUTOMAÇÃO EM SUBESTAÇÕES UTILIZANDO O PROTOCOLO SNMP

por

ALEX SANDRO IVANKIO

Esta monografia foi apresentada em 29 de Novembro de 2018 como requisito parcial para a obtenção do título de Especialista em Automação Industrial. O candidato foi arguido pela Banca Examinadora composta pelos professores abaixo assinados. Após deliberação, a Banca Examinadora considerou o trabalho aprovado.

_____
Prof. Dr. Valmir de Oliveira
Orientador

_____
Prof. Dr. Kleber Kendy Horikawa Nabas
Membro titular

_____
Prof. M. Sc. Omero Francisco Bertol
Membro titular

- O Termo de Aprovação assinado encontra-se na Coordenação do Curso -

Dedico esse trabalho primeiramente a Deus pelo dom da Vida. Também agradeço a minha família, minha esposa Franciane e minhas filhas Alice e Sofia, pela compreensão e pela paciência e pelo incentivo para que eu desenvolvesse essa monografia. Agradeço também aos meus pais Ana Maria e Osvaldo que sempre me incentivaram a estudar.

AGRADECIMENTOS

Agradeço a todos os professores da pós-graduação pelos ensinamentos ao longo do curso. Agradeço em especial ao professor Valmir pela sua dedicação e pela orientação deste trabalho.

Agradeço aos meus colegas de trabalho que contribuíram diretamente e indiretamente a elaboração deste trabalho.

Deixem que o futuro diga a verdade e avalie cada um de acordo com o seu trabalho e realizações. O presente pertence a eles, mas o futuro pelo qual eu sempre trabalhei pertence a mim (Nikola Tesla).

RESUMO

IVANKIO, Alex Sandro. **Monitoramento de equipamentos da rede de automação em subestações utilizando o protocolo SNMP**. 2018. 51 p. Monografia de Especialização em Automação Industrial, Departamento Acadêmico de Eletrônica, Universidade Tecnológica Federal do Paraná. Curitiba, 2018.

Nos últimos anos, a comunicação das UCC'S (Unidade Central e Controle) com os relés de proteção e com as UAC'S (Unidade de Aquisição e Controle) era exclusivamente via serial RS232 através do distribuidor ótico/elétrico. Este equipamento possui dez portas elétricas que distribuem os dados vindos da UCC'S para os relés, UAC'S e outros equipamentos instalados em campo. Com a atualização tecnológica e o avanço no sistema de proteção e comunicação na automação, ocorre a substituição gradativa dos distribuidores elétrico/óptico por switches gerenciáveis e servidores seriais. Estes equipamentos permitem uma comunicação mais rápida e mais eficiente entre as UCC'S e os relés de proteção, ocupam um menor espaço físico nos bastidores da automação e nos permitem realizar o monitoramento a distância. Uma das características disponíveis destes equipamentos é o protocolo SNMP (*Simple Network Management Protocol*), protocolo de gerenciamento de redes simples, desenvolvido na década de oitenta. Por padrão de fábrica este protocolo encontra-se inicialmente desabilitado. O SNMP é um protocolo que nos permite coletar informações dos equipamentos instalados em uma rede, tais como: temperatura, processamento da CPU, estados das portas ópticas, estados das portas elétricas entre outros itens. Para realizar o monitoramento destes equipamentos necessita-se de um software que possui uma comunicação com o protocolo SNMP. O software que está sendo estudado para realizar este monitoramento é o Zabbix. Este trabalho tem como objetivo mostrar: a configuração dos equipamentos, os dados coletados em campo e as dificuldades encontradas para a instalação. E, portanto, através destas informações coletadas será possível realizar uma manutenção preditiva destes equipamentos.

Palavras-chave: Protocolo SNMP. Switches. Servidor serial.

ABSTRACT

IVANKIO, Alex Sandro. **Monitoring of substation automation network equipment using the SNMP protocol**. 2018. 51 p. Monografia de Especialização em Automação Industrial, Departamento Acadêmico de Eletrônica, Universidade Tecnológica Federal do Paraná. Curitiba, 2018.

In recent years, communication of the UCC's (Control and Central Unit) with the protection relays and with the UAC's (Unit of Acquisition and Control) was exclusively RS232 through the optical/electrical distributor. This equipment has ten electric gates that distribute data coming from UCC'S to the relays, UAC's and other field installed equipment. With the technological upgrade and the advance in the protection and communication system in the automation, there is the gradual replacement of the electrical/optical distributors with manageable switches and serial servers. These devices allow faster and more efficient communication between the UCC's and the protection relays, occupy less physical space behind the panel of the automation and allow us to carry out remote monitoring. One of the available features of this equipment is the Simple Network Management Protocol (SNMP), a simple network management protocol, developed in the eighties. By default this protocol is initially disabled. SNMP is a protocol that allows us to collect information from equipment installed in a network, such as: temperature, CPU processing, optical port states, electric port states, among other things. To carry out the monitoring of these equipments, a software that has a communication with the SNMP protocol is required, the software that is being studied to perform this monitoring is Zabbix. This work aims to show: the configuration of the equipment, the data collected in the field and the difficulties encountered for the installation. And, through this information collected will be possible to carry out a predictive maintenance of these equipments.

Keywords: Protocol SNMP. Switch. Serial server.

LISTA DE FIGURAS

LISTA DE TABELAS

LISTA DE SIGLAS

COD	Centro de Operação da Distribuição
COG-T	Centro de Operação da Geração e Transmissão
GOOSE	*Generic Object Oriented Substation Event*
IED	*Intelligent Electronic Device* (Dispositivo Eletrônico Inteligente)
IP	*Internet Protocol* (Protocolo de Internet)
ISO	*International Organization for Standardization* (Organização Internacional para Padronização)
LAN	*Local Area Network* (Rede Local)
LTS	*Long Time Support*
MIB	*Management Information Base*
ONS	Operador Nacional do Sistema Elétrico
OSI	*Open System Interconnection* (Sistema Aberto de Interconexão)
PCI	*Peripheral Component Interconnect* (Interconector de Componentes Periféricos)
PCIe	*Peripheral Component Interconnect express* (Interconector de Componentes Periféricos express)
QoS	*Quality of Service* (Qualidade dos Serviços)
RFC	*Request for Comments*
SCADA	*Supervisory Control and Data Acquisition*
SMI	*Structure of Managemente Information*
SNMP	*Simple Network Management protocol* (Protocolo Simples de Gerenciamento de Redes)
TA	Tecnologia da automação
TCP/IP	*Transmission Control Protocol/ Internet Protocol* (Protocolo de Controle de Transmissão/ Protocolo de Internet)
TI	Tecnologia da informação

UDP	*User Datagram Protocol* (Protocolo de Datagrama de Usuário)
UTR	Unidade Terminal Remota
WAN	*Wide Area Network* (Rede de Longa Distância)

SUMÁRIO

1 INTRODUÇÃO

Neste capítulo serão apresentados o tema da monografia, as delimitações do estudo, os problemas e premissas, bem como os objetivos propostos, a justificativa e o procedimento metodológico utilizado neste trabalho.

1.1 TEMA

Segundo Branquinho et al. (2014) as redes de automação proporcionaram um aumento da produtividade dos processos, os equipamentos utilizados são na maioria das vezes robustos, porém sem nenhum tipo de sistema de segurança. Essa falta de segurança coloca em riscos a produção dos serviços como também pode ocasionar danos aos equipamentos.

Com a avanço das tecnologias de telecomunicações observou-se a convergência da TI (Tecnologia da Informação) com a TA (Tecnologia da Automação), esse alinhamento está expondo as fragilidades desses ambientes (BRANQUINHO et al., 2014).

Segundo Branquinho et al. (2014), a rede de automação é algo complexo e para garantir seu funcionamento não basta somente ter *software* e *hardware* específicos, mas tem que haver funcionários capacitados.

Ainda segundo Branquinho et al. (2014), uma rede de automação oferece uma gama de aplicações e dados em tempo real. Devido a esses fatores se tornam cada vez mais necessário o monitoramento contínuo da qualidade dos serviços (QoS). O parâmetro QoS procura atender prioridades de largura de banda e controle de latência de uma rede.

Um sistema SCADA (*Supervisory Control and Data Acquisition*) em perfeito funcionamento apresenta QoS único, o sistema raramente muda devido ao processo ser repetitivo. O monitoramento contínuo dos parâmetros de QoS de uma rede de automação pode antecipar alguns problemas com vírus e defeitos de equipamentos, como nos *switches* (BRANQUINHO et al., 2014).

Este trabalho tem como objetivo realizar o monitoramento a distância dos equipamentos da rede da automação como *switches*, servidores seriais instalados nas subestações. Os equipamentos utilizam o protocolo SNMP (*Simple Network*

Management Protocol). Para executar o monitoramento dos equipamentos será necessário a instalação de um servidor que execute o monitoramento e também armazenem os dados coletados. Para realizar esse monitoramento está sendo estudado o *software* Zabbix.

1.2 DELIMITAÇÃO DO ESTUDO

Durante alguns anos o sistema de comunicação serial utilizado pelos equipamentos, relés de proteção, UTR (Unidade Terminal Remota) foram sendo atualizados com os avanços tecnológicos, com isso a comunicação que era basicamente serial, tais como RS485, RS232, GP-IB, entre outros, passou-se ao protocolo Ethernet. Devido essas mudanças foi necessário a instalação de *switches* e servidores seriais. Esses equipamentos comunicam com os relés em campo, trafegando protocolos como DNP3.0, MODBUS, IEC61850, essas informações coletadas são repassadas para o sistema SCADA. O sistema SCADA coleta esses dados decodifica as informações e as repassam aos operadores.

Os *switches* e os servidores seriais estabelecem uma ponte de comunicação entre o sistema SCADA e os relés tornando-se aqueles equipamentos importantíssimos para os processos. Devido tal importância verifica-se que há necessidade de monitoramento daqueles equipamentos e conhecer exatamente os pontos críticos do sistema.

1.3 PROBLEMA

Os *switches* e os servidores seriais são equipamentos que cada vez mais estão sendo aplicados na automação. Porém não existe nenhum monitoramento contínuo nos equipamentos da rede da automação. Sem tal monitoramento não se pode verificar se os equipamentos estão comunicando corretamente ou se existe algum problema de *hardware*.

Em subestações controladas pelo sistema SCADA, caso exista a perda de *switches* e/ou servidores seriais, por defeitos ou desconfiguração, por exemplo, a subestação perde as referências dos equipamentos de campo e, em alguns casos,

pode se perder inclusive os intertravamentos de equipamentos que são realizados por mensagem *GOOSE* (*Generic Object Oriented Substation Event*).

1.4 OBJETIVOS

Nesta seção são apresentados os objetivos geral e específicos do trabalho, relativos ao problema anteriormente apresentado.

1.4.1 Objetivo Geral

Serão realizadas as configurações dos equipamentos instalados em campo para operarem via protocolo SNMP (*Simple Network Management Protocol*). Serão também realizadas a parametrização e a configuração do servidor de rede. O Servidor será responsável pela aquisição e pelo armazenamento da base de dados, aquisitadas pelos equipamentos de campo. Após a configuração dos equipamentos serão realizadas análises dos pontos a serem monitorados para determinar quais pontos são de maior relevância para o monitoramento.

1.4.2 Objetivos Específicos

- Parametrização dos equipamentos a serem monitorados: *switches* e servidores seriais;
- Coletar e processar os dados aquisitados;
- Realizar o monitoramento da temperatura, capacidade de processamento, estados da porta ótica, estado da porta elétrica dos equipamentos;
- Realizar a configuração e parametrização do servidor;
- Identificar as principais falhas e as prováveis causas.

1.5 JUSTIFICATIVA

A rede de automação de uma subestação nos permite aquisitar vários dados analógicos e digitais dos equipamentos instalados em campo. Como estado do disjuntor, medição da corrente do transformador, tensão dos barramentos V_{CA} e V_{CC} dos retificadores, entre outros parâmetros presentes em uma subestação. Aqueles

dados são coletados em tempo real, e são repassados ao ONS (Operador Nacional do Sistema Elétrico), COG-T (Centro de Operação da Geração e Transmissão) e COD (Centro de Operação da Distribuição). Caso algum equipamento venha a falhar, o ONS pode ficar sem supervisão de uma subestação inteira. Assim torna-se necessário cada vez mais o monitoramento contínuo dos equipamentos instalados na rede.

1.6 PROCEDIMENTOS METODOLÓGICOS

O presente trabalho tem como objetivo resolver os problemas descrito no item 1.3, ou seja, monitorar em tempo real o estado dos *switches* e dos servidores seriais. Também foi realizada pesquisa bibliográfica do assunto para melhor entendimento. Neste levantamento foi visto a complexidade do protocolo utilizado. Em seguida foram feitas as configurações, dos equipamentos em campo, configuração e parametrização do servidor SNMP. Aquisição dos dados e avaliação dos resultados obtidos.

1.7 EMBASAMENTO TEÓRICO

Em relação ao tema: necessidade do monitoramento dos equipamentos na rede da automação utilizou-se Branquinho et al. (2014). Porém no gerenciamento de redes e do funcionamento do protocolo SNMP foi consultado Forouzan (2008). Para instalação e configuração dos equipamentos, bem como no monitoramento de rede, utilizou-se com Zabbix (LIMA, 2014).

O Zabbix é uma ferramenta de *software* de monitoramento de código aberto para diversos componentes de TI, incluindo redes, servidores, máquinas virtuais e serviços em nuvem.

1.8 ESTRUTURA DO TRABALHO

- Capítulo 1 - Introdução: serão apresentados o tema, o problema, os objetivos da pesquisa, a justificativa e a estrutura geral do trabalho.

- Capítulo 2 - Sistema de Comunicação: será abordado as camadas de comunicação de um sistema OSI.
- Capítulo 3 - Gerenciamento de Redes: será abordado a necessidade de realizar o monitoramento da rede de uma subestação.
- Capítulo 5 - Equipamentos da Rede de Automação: será descrito neste trabalho o funcionamento dos equipamentos utilizados neste trabalho
- Capítulo 6 - Configuração dos equipamentos: Será abordado as metodologias utilizada para configurar os equipamentos que estão instalados nas Subestações, como também será abordado a configuração do servidor serial.
- Capítulo 7 - Apresentação e Análise dos Resultados: neste capítulo será descrito os resultados obtidos com as devidas análises relacionadas ao monitoramento dos equipamentos utilizado nas subestações.
- Capítulo 8 - Considerações Finais: Demostrar se os objetivos propostos foram alcançados, se o monitoramento dos equipamentos trouxe um ganho para a manutenção. Sugerir novos trabalhos nessa área de pesquisa.

2 SISTEMA DE COMUNICAÇÃO

2.1 MODELO DE REFERÊNCIA OSI

O modelo OSI (*Open System Interconection*) foi criado em 1984 pela ISO (*International Organization Standardization*), organização Internacional para Padronização. O objetivo do modelo OSI é servir como mecanismo de padronização de protocolos dos diferentes fabricantes. De tal forma é um código aberto e permite que futuramente outros protocolos utilizassem o mesmo princípio. O modelo OSI é dividido em sete camadas que juntas formam uma pilha, como mostra a Figura 1, cada camada pode fornecer ou receber as informações das camadas adjacentes (SCHMITT; PERES; LOUREIRO, 2013).

Figura 1 - Camadas do modelo de referência OSI

Fonte: Schmitt, Peres e Loureiro (2013).

As camadas do modelo OSI são: 1: Física, 2: Enlace, 3: Rede, 4: Transporte, 5: Sessão, 6: Apresentação, 7: Aplicação (SCHMITT; PERES; LOUREIRO, 2013).

A camada “1: Física”: é responsável pelo meio de comunicação, podendo especificar meios de transmissão para sinais elétricos ou óticos. O sistema RS232 é um exemplo padrão de camada física (ARNETT, 1997).

A camada de “2: Enlace”: é o primeiro nível que reúne os bits e trata os dados de um pacote. Esse nível executa o agrupamento final de uma mensagem como também faz a primeira inspeção no recebimento de um pacote. Essa camada pode também adicionar uma verificação dos erros nos pacotes que estão chegando, através da análise dos pacotes que estão saindo e chegando. Os pacotes que apresentam erros são descartados (ARNETT, 1997).

Na camada de 3: Rede” há dispositivos como roteadores, pontes e *gateways* que dividem a rede local e criam subredes. Esta camada garante que os pacotes de origem cheguem aos seus destinos (ARNETT, 1997).

A camada de “4: Transporte” é responsável por gerenciar os pacotes de endereço de origem para o endereço final (SCHMITT; PERES; LOUREIRO, 2013).

A camada de “5: Sessão” estabelece uma conexão e uma sincronização entre os sistemas. Esta camada possibilita que a comunicação com dois processos ocorra. Essa camada verifica a sincronização de uma mensagem adicionando pontos de verificação em trechos da mensagem enviadas para o destinatário (FOROUZAN, 2008).

A camada de “6: Apresentação”, realiza a criptografia e as traduções das mensagens (SCHMITT; PERES; LOUREIRO, 2013).

A camada de “7: Aplicação”, disponibiliza os serviços de transferências de arquivos, acesso via web e gerência bancos de dados compartilhados.

2.2 COMUNICAÇÃO TCP/IP

Na comunicação TCP/IP (*Transmission Control Protocol/ Internet Protocol*) as camadas dos protocolos não são exatamente iguais as camadas de modelo OSI. O protocolo TCP/IP possui quatro camadas sendo: 1-2: Interface, 3: Rede, 4: Transporte, e 7: Aplicação (ARNETT, 1997).

A camada de “1-2: Interface” é uma combinação das camadas física e enlace. A camada de rede no TCP/IP equivale a mesma camada de rede OSI. A Camada de “2: Transporte no modelo TCP/IP equivale as camadas de aplicação, apresentação e sessão no modelo OSI (ARNETT, 1997).

O funcionamento da camada de “7: Aplicação” do modelo OSI é igual ao funcionamento do TCP/IP.

A camada de “4: Transporte” possui dois tipos de protocolos sendo TCP, que é orientando a conexão e o UDP (Protocolo de Datagrama de Usuário - *User Datagram Protocol*), que não é orientando a conexão. De maneira geral os dados do serviço orientado a conexão garantem que os dados sejam entregues aos destinatários em ordem e completos. O serviço não orientado a conexão não

garante essa entrega. No entanto o seu objetivo é transmitir seus pacotes de dados de um meio físico para outro (FOROUZAN, 2008).

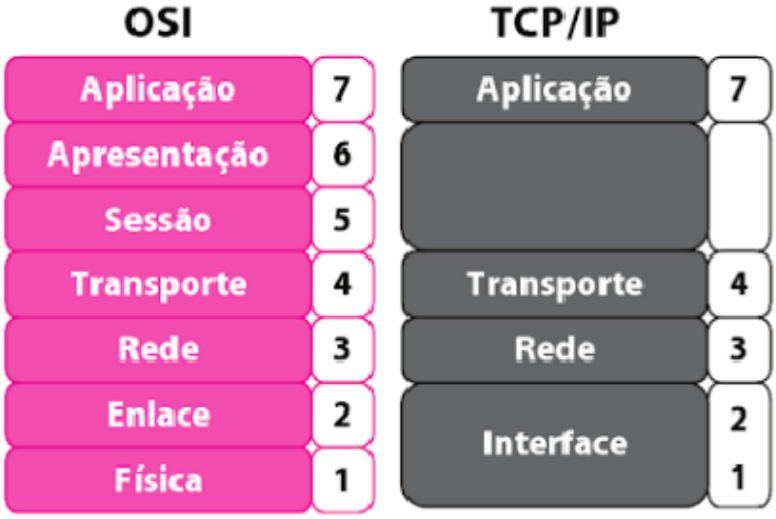
Na comunicação UDP as informações são somente enviadas ao destino sem confirmação que os dados foram recebidos pelo cliente (ARNETT, 1997).

Na camada de “3: Rede” o principal protocolo é o IP (*Internet Protocol*), esse protocolo utiliza endereço formado por quatro conjuntos de oito octetos separados por pontos para identificar outros computadores conectados em uma rede (ARNETT, 1997).

Camada de “1-2: Interface” é de responsabilidade da placa de rede. Nessa camada os pacotes são decodificados em bits chamado de quadro (*frame*) enviados através de meio físico a outros computadores ou roteadores (ARNETT, 1997).

A Figura 2, mostra uma comparação do modelo OSI com o TCP/IP.

Figura 2 - Modelo OSI versus modelo TCP/IP



Fonte: Schmitt, Peres e Loureiro (2013).

3 GERENCIAMENTO DE REDES

Através do gerenciamento de rede pode-se realizar o monitoramento, teste, configuração e diagnósticos de componentes para atender aos requisitos de supervisão de uma rede numa organização. Para realizar esta função de gerenciamento de rede é utilizado *hardware*, *software* e pessoas. O protocolo que realiza o gerenciamento de rede é o SNMP (*Simple Network Management Protocol*, ou Protocolo Simples de Gerenciamento de Redes) (FOROUZAN, 2008).

Segundo Forouzan (2008), o sistema de gerenciamento de redes é dividido em cinco categorias:

- Gerenciamento de configuração (*Configuration Management*);
- Gerenciamento de Falhas (*Fault Management*);
- Gerenciamento de desempenho (*Performance Management*);
- Gerenciamento de Segurança (*Security Management*);
- Gerenciamento de Contabilização (*Accounting Management*).

3.1 GERENCIAMENTO DE CONFIGURAÇÃO

Uma grande rede é constituída por centenas de equipamentos conectados de uma forma física e lógica. Quando a rede é ativada pela primeira vez essa rede possui uma característica, porém pode-se reconfigurar com o tempo. Portanto o gerenciamento de configuração precisa saber o tempo inteiro o estado de cada entidade como também a relação com outras entidades. Esse sistema de gerenciamento é dividido em dois subsistemas, reconfiguração e documentação (FOROUZAN, 2008).

A reconfiguração pode ser de *hardware* e/ou *software*. A reconfiguração de *hardware* abrange todas as mudanças no *hardware*, como transferência de um *switch* para outro lugar da rede. Este tipo de configuração não pode ser automatizada, deve-se ser realizada manualmente (FOROUZAN, 2008). A reconfiguração de *software* está associada as mudanças no *software*, pode-se ser necessário haver a atualização do sistema operacional. A reconfiguração das contas de usuários permite retirar ou adicionar privilégios de leituras e escritas em uma conta (FOROUZAN, 2008).

Com relação a documentação, o *hardware*, o *software* e contas de usuários devem possuir a sua documentação apropriada. A documentação de *hardware* pode ser os diagramas das conexões dos equipamentos de cada rede como também um diagrama lógico de cada sub-rede. Também deve-se existir uma especificação de cada equipamento ligado na rede, nessa especificação deve-se constar o tipo de *hardware* e o número de série (FOROUZAN, 2008).

3.2 GERENCIAMENTO DE FALHAS

Um gerenciamento de falhas eficaz apresenta dois subsistemas, sendo o gerenciamento de falhas reativo e o proativo. O Gerenciamento de falhas reativo é responsável pela detecção, isolamento, correção e registro de falhas. Este tipos de soluções é para os problemas de curtos prazos (FOROUZAN, 2008).

Um exemplo de falha reativo é quando um meio de transmissão é danificado interrompendo a comunicação entre equipamentos gerando assim um número excessivos de erros. Outra função de gerenciamento reativo de falha é isolar a falha e notificar os usuários afetados. A última função deste gerenciamento de falha é corrigir a falha detectada, isto pode ser executado através da substituição ou reparo dos equipamentos. Após a falha ser sanada deve-se ser documentada. Neste documento deve-se ser constado a localização das faltas e as possíveis causas as ações que foram tomadas (FOROUZAN, 2008).

3.3 GERENCIAMENTO DE DESEMPENHO

Segundo Forouzan (2008), o monitoramento e o controle de uma rede é necessário para garantir o seu bom funcionamento. No gerenciamento de uma rede pode-se quantificar o desempenho de uma rede usando quantidades mensuráveis como capacidade, tráfego e o tempo de respostas desta rede. Toda rede tem uma capacidade de taxa de dados limitada, o gerenciamento deve garantir que esta capacidade não seja ultrapassada. Porém o tráfego pode ser medido internamente e externamente. O tráfego interno é medido pelo número de pacotes ou *bytes* que trafegam por uma rede, já o tráfego externo é medido pelas trocas dos pacotes fora

da rede. O uso excessivo dos pacotes, *bytes* dentro ou fora da rede ocasiona a interrupção da rede.

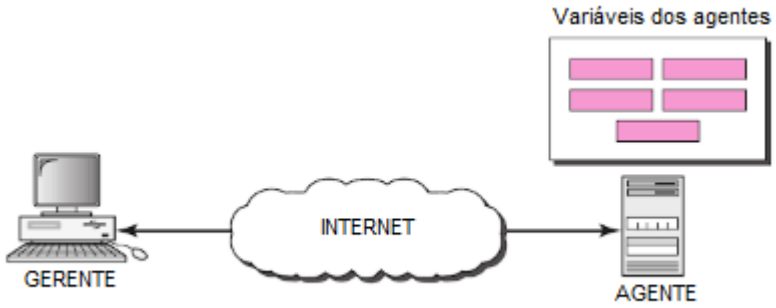
O tempo de resposta em uma rede é medido a partir do instante em que o usuário solicita um serviço até o momento que este serviço é atendido. Um tempo de resposta grande em uma rede é uma condição muito grave, este indicador pode referir-se que a rede está operando acima de sua capacidade (FOROUZAN, 2008).

4 PROTOCOLO SNMP

O SNMP (*Simple Network Management Protocol),* possui diversas funções para realizar o monitoramento de uma rede, esse protocolo utiliza os conjuntos de protocolo TCP/IP, ele opera sobre o *User Datagram Protocolo* (UDP), o SNMP roda na camada de aplicação, e utiliza o conceito de agente e gerente, onde o gerente controla e monitora, através das portas UDP 161, os agentes e os agentes enviam *traps* através da porta UDP 162 (FOROUZAN, 2008).

O SNMP é capaz de monitorar vários equipamentos em uma LAN ou WAN de fabricantes diferentes instalados em redes físicas diferentes. A Figura 3, mostra uma configuração de agente e gerente em uma rede.

Figura 3 - Comunicação gerente e agente



Fonte: Forouzan (2008).

Gerente é a denominação dada a *host* que roda o programa-cliente SNMP, o gerenciado é o agente que é um roteador, *switch* que executa o programa-servidor SNMP. A troca de informações é realizada através da interação do gerente com o agente (FOROUZAN, 2008).

O agente mantém as informações de desempenho em uma base de dados e o gerente acessa essa base de dados e coleta os valores. O gerente, além de acessar a base de dados, também pode enviar comando para o agente, como um *reset* no equipamento. Já o agente pode ser programado para transmitir uma mensagem de algo anormal no processo, essa mensagem transmitida é denominada *TRAP* (FOROUZAN, 2008).

Para realizar o monitoramento o SNMP utiliza-se dois protocolos auxiliares, o SMI (*Structure of Managemente Information)* estrutura de informações de

gerenciamento e MIB (*Management Information Base)* base de informações de gerenciamento (FOROUZAN, 2008).

Para utilizarmos o SNMP necessitamos de regras, e o SMI é responsável pela realização dessas regras. O SMI determina os nomes, comprimento e como realizar a codificação dos objetos, conforme Tabela 1, porém o SMI não determina o número de objetos que uma entidade pode gerenciar (FOROUZAN, 2008).

Tabela 1 - Tipos de dados SNMP

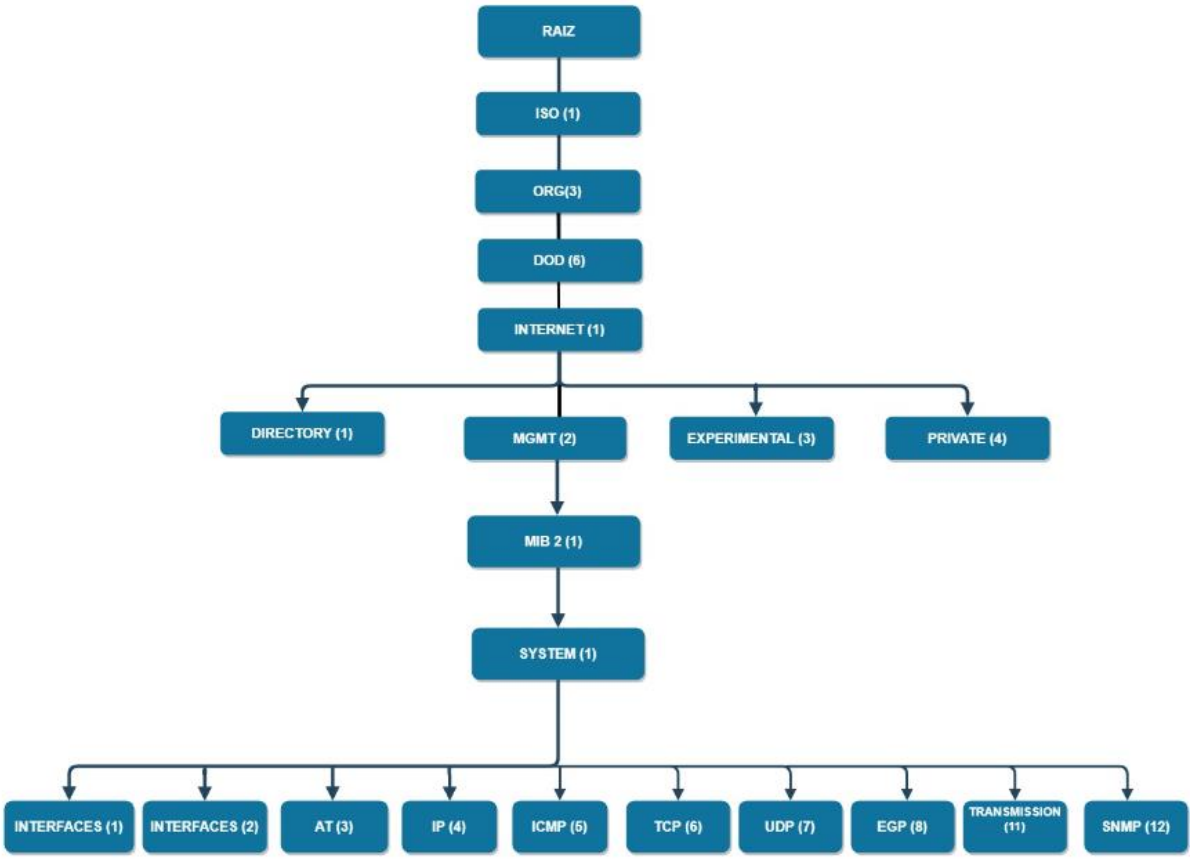
Tipos de dados	Descrição
INTEGER	Inteiros na faixa de -2^{31} a 2^{31} -1
UInteger32	Inteiros na faixa de 0 a 2^{32} -1
Counter32	Um inteiro não negativo que pode ser incrementado em módulo 2^{32}
Counter64	Um inteiro não negativo que pode ser incrementado em módulo 2^{64}
Gauge32	Um interio não negativo que pode aumentar ou diminuir, mas não deve exceder um valor máximo. O valor máximo não pode ser mairo que 2^{32} -1.
TimeTicks	Um inteiro não negativo que representa o tempo, módulo 2^{32}, em centésimos de segundo.
OCTET STRING	Strings de octeto para dados binários ou textuais arbitrários; pode-se limitar a 255 octetos.
IpAddress	Um endereço de inter-redes de 32 bits.
Opaque	String não interpretada
BIT STRING	Uma enumeração de bits nomeados.
OBJECT IDENTIFIER	Nome atribuido a um objetor ou outro elemento padronizado.

Fonte: Stallings (2005).

O SNMP também utiliza MIB, que é um banco de dados que contém um conjunto de objetos com nomes, tipos e relações entre si que estão em uma entidade a ser gerenciada. Então o SNMP armazena, altera e interpreta os valores dos objetos já declarados na MIB de acordo com as regras definidas pelo SMI (FOROUZAN, 2008).

De acordo com a RFC (*Request for Comments*) 1155 o SMI determina que cada objeto gerenciado tenha o seu próprio nome e que utilize um sistema hierárquico com base em uma estrutura na forma de árvore, conforme Figura 4 (FOROUZAN, 2008).

Figura 4 - Identificador de objetos SMI



Fonte: Forouzan (2008).

Cada objeto é separado por uma sequência de números inteiros separados por pontos e também pode ser representados pelos nomes separados por pontos como por exemplo (FOROUZAN, 2008): *iso.org.dod.internet.mgmt.mib-2 = 1.3.6.1.2.1*

Então para acessar uma variável da MIB que contenha as informações do objeto do sistema devemos seguir este caminho (FOROUZAN, 2008): *iso.org.dod.internet.mgmt.mib-2. sys = 1.3.6.1.2.1.1*

Para realizar o acesso de todas as MIBS deve-se seguir a estrutura SMI. O SNMP possui três versões: 1) SNMPv1, 2) SNMPv2, e 3) SNMPV3.

4.1 VERSÃO SNMPV1

Na sua primeira versão do SNMP, definida pela RFC1157, não possuía mecanismo de segurança e nem autenticação e comprovação da origem da informação enviada. A segurança baseava-se em *strings*, como *public* e *private* .

Nesta versão o protocolo SNMP permite somente leitura (*Get*), escrita (*Set*) e Notificações (*Notify*) dos agentes monitorados (STALLINGS, 2005).

4.2 VERSÃO SNMPV2

Tanto o SNMPv1 como o SNMPv2 utiliza um banco de dados local de informações, MIB e a mesma estrutura das informações de gerenciamento SMI. O SNMPv2 através da RFC 1442 e RFC 1448 busca além de gerenciar recursos da rede gerencia as aplicações e os sistemas de comunicação. Nesta versão é permitido as seguintes operações como GetRequest, GetNextRequest, SetRequest, Response, GetBulkReques, Trap e InformRequest, muito além da versão um deste protocolo. Tanto a versão um como a versão dois do protocolo possui pouca segurança nas mensagens trafegadas (BRANCO, 2015).

Segundo Stallings (2005), o gerenciador pode solicitar através de comando como:

GetRequest é uma mensagem solicitada que inclui uma lista de um ou mais objetos, no GetNextRequest é solicitado uma visão geral da MIB dinamicamente no SetRequest é uma mensagem não confirmada enviada para alterar um objeto, no SNMPV2 o agente responde com uma Response que contém uma mesma identificação da requisição.

GetBulkRequest permite que o gerenciador solicite que a resposta inclua quantas variáveis forem possíveis. Trap é gerada para transmitir a um gerente um evento incomum. InformeRequest é mensagem entre gerenciadores que verifica informações de gerenciamento de uma aplicação (STALLINGS, 2005).

4.3 VERSÃO SNMPV3

Segundo Stallings (2005), algumas deficiências funcionais foram consertadas no versão dois do SNMP. Porém com relação a segurança nos dados tráfegados, tanto a versão um como a versão dois deixou a desejar. O SNMPv3 foi lançado para resolver o problema de segurança, este protocolo utiliza as *RFCs* 3410 a 3415.

Esta versão fornece três serviços importante de segurança, autenticação, privacidade e controle de acesso. Os serviços de segurança são controlados pela

identidade do usuário, essa identidade pode ser um indivíduo, um grupo ou uma aplicação (STALLINGS, 2005).

Conforme *RFC* 2274, o mecanismo de autenticação garante que a mensagem transmitida foi recebida corretamente, esta identificação é feita através da análise do cabeçalho da mensagem. Esse tipo de verificação pode determinar que a mensagem não foi alterada no percurso realizado. O código de autenticação real pode ser conhecida como HMAC - MD5 - 96, que é o mecanismo de identificação padrão da Internet (STALLINGS, 2005).

De acordo com a RFC 2274 temos as informações criptografadas como CBC - DES. Para realizar a comunicação o emissor deve criptografar e enviar a mensagem utilizando o algoritmo DES-CBC como sendo sua chave secreta e o receptor deve descriptografar utilizando o mesmo algoritmo do emissor (STALLINGS, 2005).

4.4 ARQUITETURA DE REDE DA SUBESTAÇÃO DE ENERGIA ELÉTRICA

A Subestação Curitiba Norte fica no município de Almirante Tamandaré e nela estão conectadas as linhas de transmissão das subestações Pilarzinho e Bateias 230 kV, além de atender a empresa Companhia de Cimento Portland Rio Branco (Votorantim). A Subestação injeta energia proveniente da Rede Básica no sistema de distribuição, usando dois transformadores com potência total de 300 MVA. A subestação Curitiba Norte opera em 230 kV e recebeu R$ 69 milhões em investimentos.

A supervisão remota desta subestação é realizada através do COG-T (Centro de Operação da Geração e Transmissão).

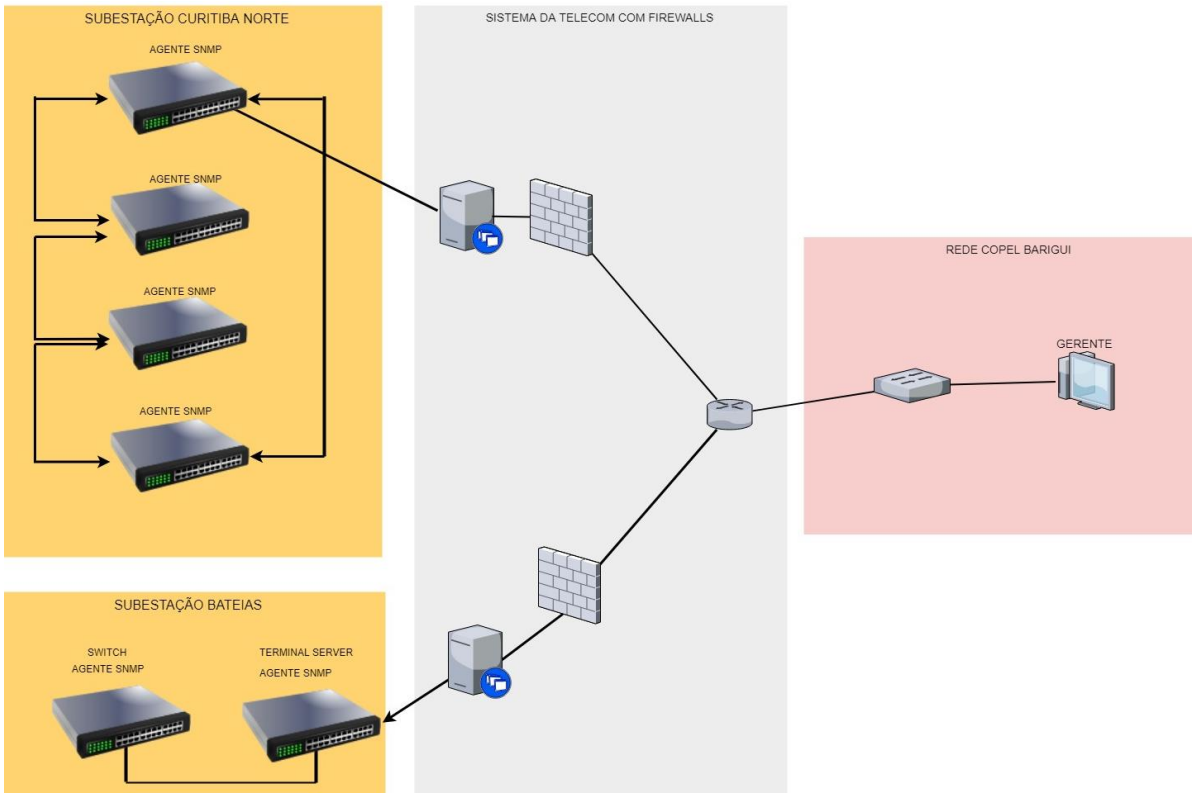
A função de proteção da subestação é realizada por vinte e dois relés digitais IED (*Intelligent Electronic Device*, ou Dispositivo Eletrônico Inteligente), que possuem duas portas de comunicação Ethernet ótica com conector LC, podendo ser configuradas de acordo com o sistema de rede utilizado. A comunicação dos relés de proteção com o sistema SCADA são através dos *switches* gerenciáveis e servidores seriais. Esses equipamentos são responsáveis pelo tráfego de protocolos, como mensagens GOOSE, DNP3.0 e Modbus da subestação, entre os relés e o sistema SCADA.

O *switch* utilizado é do fabricante SEL modelo 2730, este equipamento possui 16 portas ópticas multimodos e quatro portas de rede Ethernet RJ45, possui uma fonte de alimentação de 125 Vcc. O SEL-2730M suporta SNMPv1/v2c/v3 e sua faixa de temperatura de operação está entre -40 a 85 °C, o acesso as configurações do *switch* é realizado através do browser do computador.

Na subestação Bateias está disponível um servidor serial da Ruggedcom RS416NC responsável pela conversão das *interfaces* RS232, RS485 para uma *interface* Ethernet padrão com velocidade de comunicação de 10/100Base-TX, com encapsulamento dos dados TCP/IP e UDP/IP. Esse modelo possui dezesseis portas óticas para fibra multimodo operando em 1300 nm, com conectorização LC, este equipamento é alimentado por duas fontes distintas, a temperatura de operação está entre -40 a 85 °C. Para acessar este equipamento há duas maneiras, uma é utilizando o *browser* com IP configurado e a outra é utilizando o *software* PuTTy. PuTTy é um *software* de emulação de terminal grátis e de código livre.

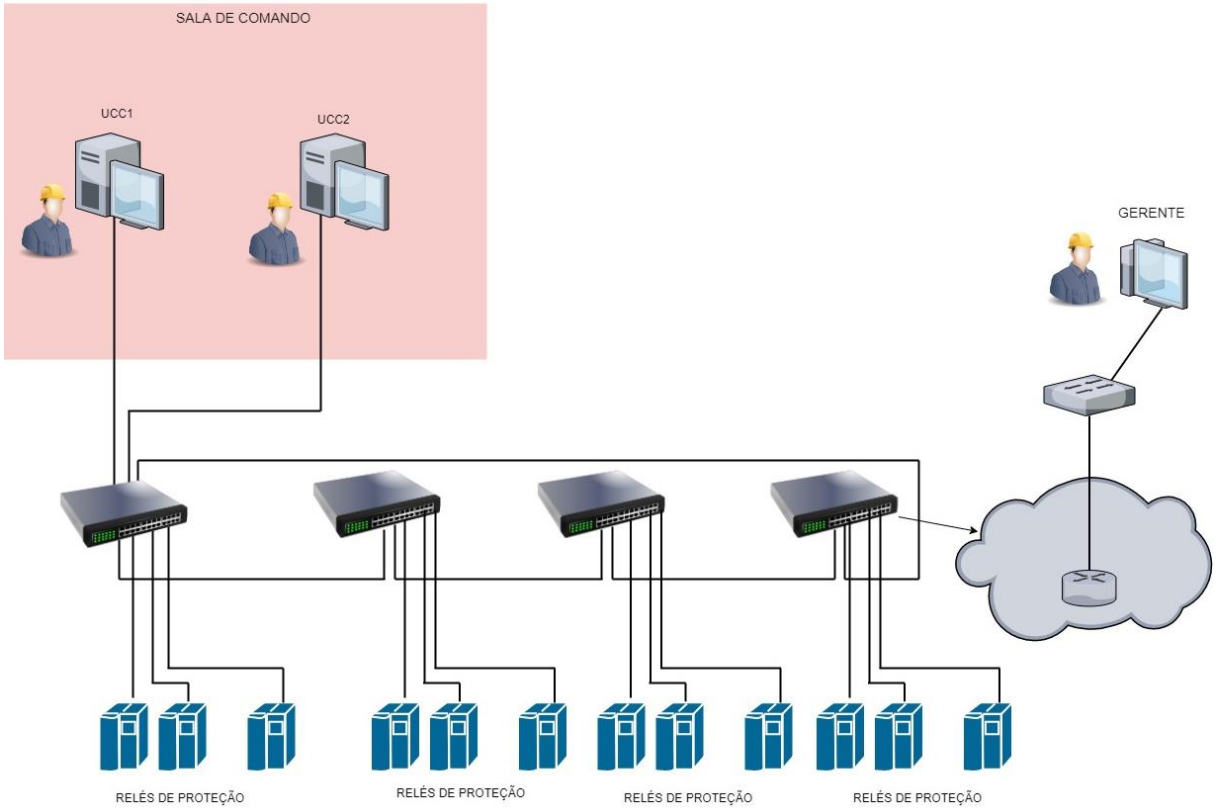
A Figura 5, detalha uma estrutura geral da rede e a Figura 6, uma estrutura da rede da subestação, na qual é possível observar os equipamentos na rede da automação ligados em anel.

Figura 5 - Arquitetura de rede



Fonte: Autoria própria.

Figura 6 - Arquitetura de rede da subestação



Fonte: Autoria própria.

5 CONFIGURAÇÃO DO SWITCH SEL 2730M

Devido a necessidade do monitoramento da infraestrutura da rede e dos novos equipamentos instalados na rede de automação e com a política de segurança implantada pela empresa, viu-se a necessidade da realização do monitoramento destes equipamentos. No primeiro momento este trabalho tem como objetivo mostrar somente uma parte dos equipamentos a serem monitorados, posteriormente será feito o monitoramento de todos os *switch* e servidores seriais instalados nas subestações da Concessionária de Energia Elétrica.

O primeiro passo para a realização do monitoramento dos equipamentos é a realização da configuração dos *switches* e servidores serial em campo.

Os *switches* e o servidor serial possuem o protocolo SNMP, porém estes equipamentos veem de fábrica com protocolo SNMP desabilitado. O primeiro passo para habilitar esse protocolo é realização da configuração dos parâmetros nos equipamentos.

Para acessar as configurações internas do *switch* deve-se configurar e conectar o computador na mesma sub-rede do *switch*, o endereço utilizado foi 192.168.1.5/24. A porta F do *switch* é a porta de configuração do equipamento, o endereço *default* cadastrado é: 192.168.1.2/24. Após inserir o computador na mesma sub-rede do *switch* deve-se digitar em qualquer *browser* o endereço da porta F, então abrirá uma tela de *login* e senha. A senha e o *login* são definidas no primeiro acesso do equipamento.

Para realizar a configuração dos equipamentos foi verificado os endereços disponíveis na rede de operação da subestação. A rede de operação é a rede que permite o acesso remoto dos equipamentos. Verificado os endereços disponíveis e definido cinco endereços IP para os equipamentos, como na Tabela 2.

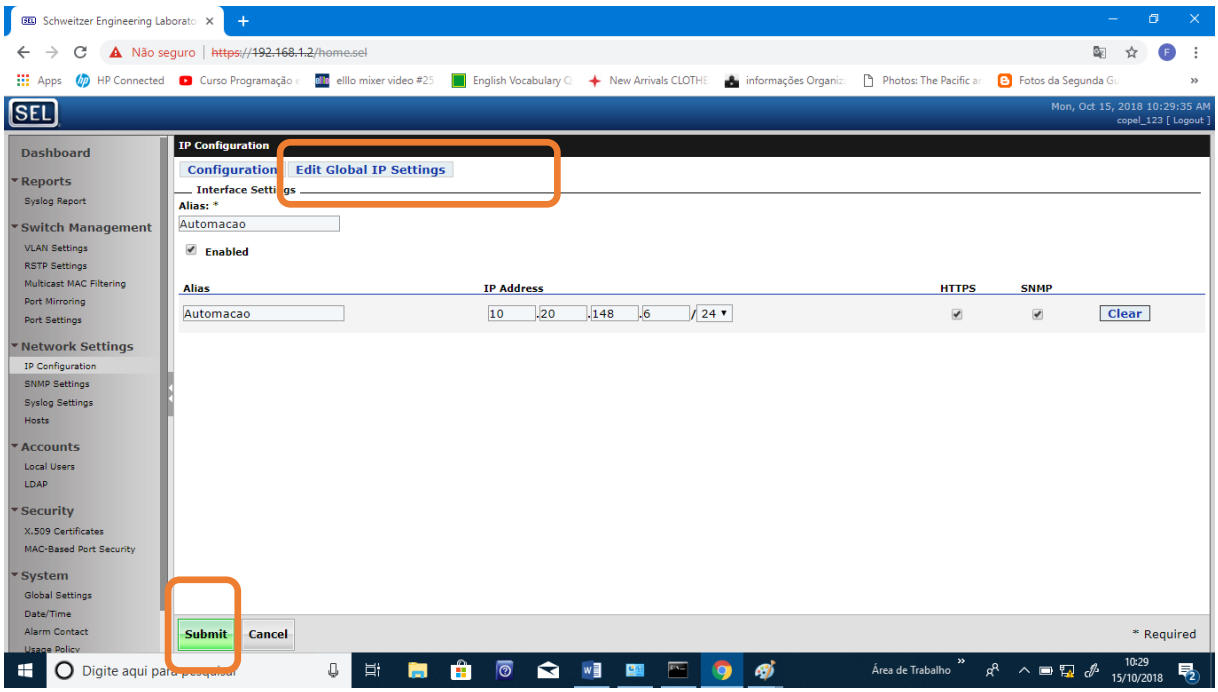
Tabela 2 - Endereços dos equipamentos na rede da subestação

Subestação Curitiba			
	Endereço	**Máscara**	**Gateway**
Switch 01	10.20.148.6	255.255.255.0	10.20.148.1
Switch 02	10.20.148.7	255.255.255.0	10.20.148.1
Switch 03	10.20.148.8	255.255.255.0	10.20.148.1
Switch 04	10.20.148.9	255.255.255.0	10.20.148.1

Fonte: Autoria própria.

Em *Network Settings/ IP Configuration* deve-se clicar em *Edit*, após isso irá abrir uma tela solicitando que seja preenchido o nome e o endereço IP, neste lugar que o SNMP é habilitado, após inserir os dados deve-se clicar em *submit*, para salvar os dados modificados, conforme Figura 7. Este equipamento disponibiliza as três versões do SNMP.

Figura 7 - Configuração do endereço de rede do switch 2730M

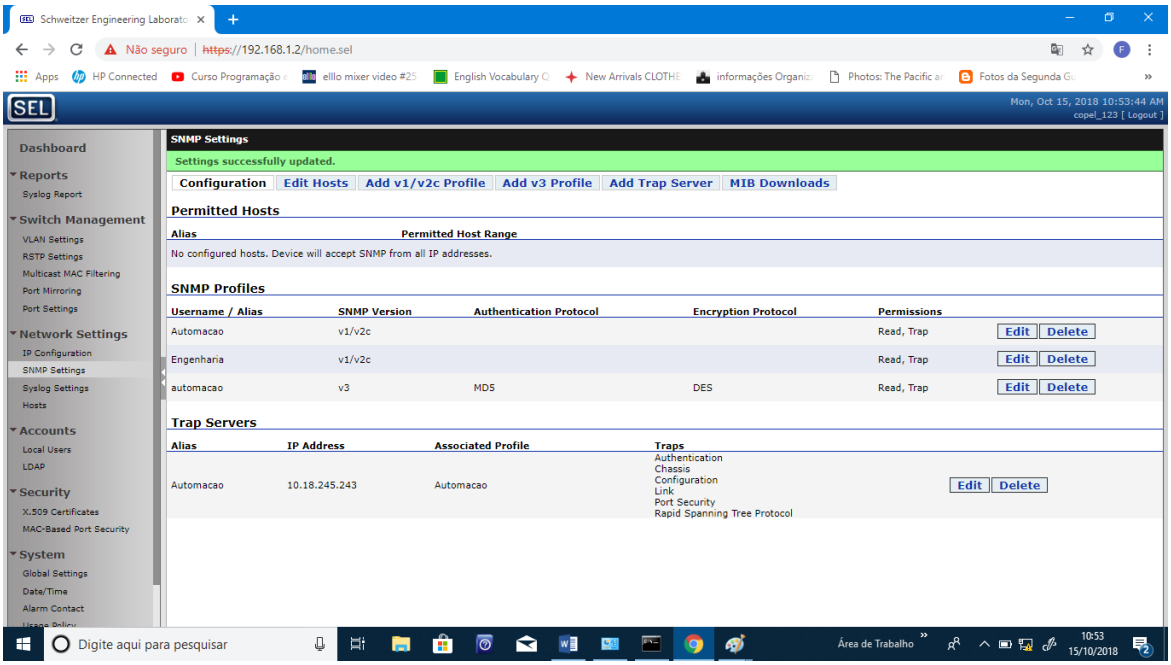


Fonte: Autoria própria.

Na aba “Edit Global IP Settings” deve-se habilitar o *Gateway* do *switch*, o endereço utilizado é 10.20.148.1.

A próxima etapa é a configuração do SNMP. Habilitar os alarmes (*traps*) que o equipamento pode enviar, habiltar a leitura (*read*). Conforme apresentado na Figura 8.

Figura 8 - Endereço do servidor Zabbix



Fonte: Autoria própria.

Neste equipamento foi configurado a Versão 1, 2 e 3 do SNMP, foi habilitado a leitura e os Trap, este equipamento não permite executar a escrita. O endereço 10.18.245.243 é o endereço do Servidor Zabbix, qualquer anomalia que o switch detectar, conforme configurado na tela acima, o switch enviará um sinal (TRAP) para o endereço do servidor Zabbix.

Após as configurações acima este equipamento, switch SEL 2730M, está habilitado a responder via protocolo SNMP.

5.1 CONFIGURAÇÃO DO SERVIDOR SERIAL E DO SWITCH DA RUGGEDCOM

Os equipamentos que serão monitorados são, o Servidor Serial do fabricante Ruggedcom modelo RS416 e o *Switch* da Ruggedcom modelo RSG2100.

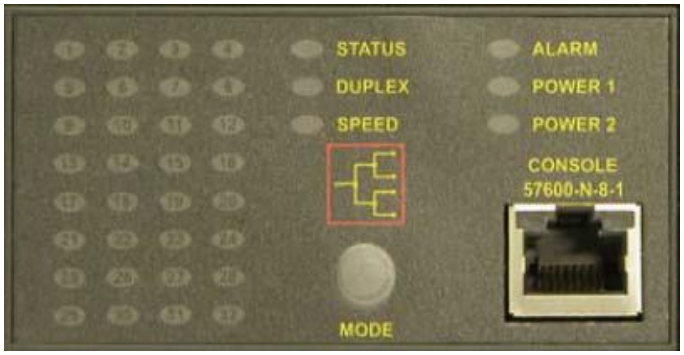
O acesso para configuração do *switch* e do servidor serial são iguais. Essa configuração e realizada pela porta serial. Estes equipamentos possuem uma porta frontal para alteração dos parâmetros. O *software* utilizado para alterações dos parâmetros foi o PuTTy. Esse *software* é de código aberto desenvolvido pela Microsoft que permite acesso remoto via SSH, telnet, Rlogin e Serial.

Atualmente os equipamentos *notebook* ou *desktop* não são fornecidos com serial RS232 (conector DB9), o que acarreta na necessidade de um adaptador para *interface* RS232 - DB9, geralmente obtido através da porta USB.

O primeiro passo é conectar o equipamento de acesso *notebook* ou *desktop* à porta serial RS232 (RJ45) do *switch* através do cabo que é fornecido com o *switch*. A Figura 9 mostra a foto do terminal server e sua entrada RJ45.

O cabo tem uma das suas extremidades com conexão RJ45, a qual deve ser conectada ao *switch* e outra extremidade apresenta conector DB9, que deve ser conectada no *notebook* ou *desktop*.

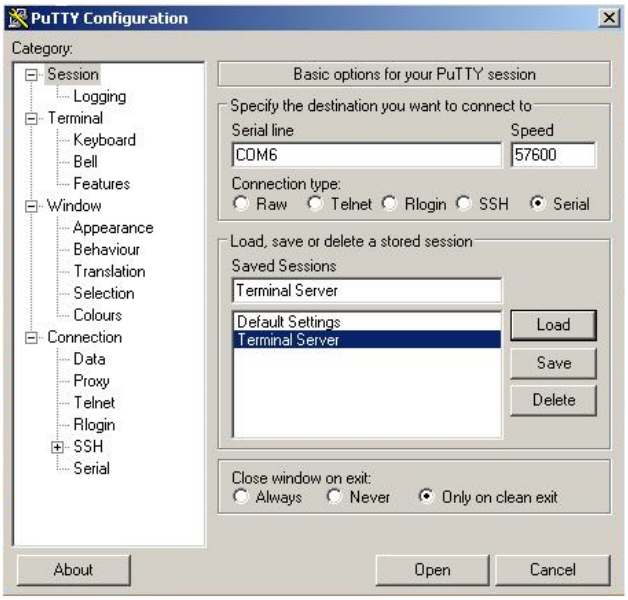
Figura 9 - Porta de configuração dos modelos da Ruggdcom



Fonte: Autoria própria.

As configurações necessárias para o acesso remoto, via PuTTy deve-se seguir conforme Figura 10.

Figura 10 - Configuração do PuTTy



Fonte: Autoria própria.

Para identificar qual a porta (*Serial Line*) o computador reservou deve-se ir em gerenciador de dispositivos do *Windows* no item portas.

As configurações para acesso ao servidor serial são, velocidade 57600 na porta COM6.

A senha para acesso do servidor serial é: Username: “admin”; Senha: “admin”. Esta senha é configuração de fábrica do equipamento e pode ser alterada.

Para configurar o SNMP neste equipamento deve-se clicar nos seguintes itens: 1) Administration, e 2) Configure SNMP.

A tela, Configure SNMP apresentará mais três tópicos como, Configure SNMP Users, Configure SNMP Security to Group Maps e Configure SNMP Access conforme Figura 11. Cada tópico desse deve ser preenchido.

O parâmetro, Configure SNMP User permite configurar usuários para o mecanismo SNMPv1, SNMPv2 e SNMPv3. Se o nível de segurança que for utilizado for SNMPv1 ou SNMPv2, o nome do usuário corresponde ao nome da comunidade. Até 32 usuários podem ser configurados.

Figura 11 - Configuração do servidor serial RS416

Fonte: Autoria própria.

No mapa de grupo de segurança e cadastrado uma tabela de configuração de modelo de segurança, nome e grupo, o qual é usado para definir a política de acesso.

O parâmetro Access SNMP, permite configurar o acesso dos grupos.A configuração do servidor e do *switch* da Ruggedcom são absolutamente iguais e ficaram conforme mostrado nas Tabelas de 3 a 6.

Tabela 3 - Configuração da interface de rede Ruggdcom

Configure Interfaces de rede		
	Servidor Serial	**Switch**
Type	VLAN	VLAN
ID	1	1
Mgmt	YES	YES
IP Address Type	Static	Static
IP Address Type	10.18.240.20	10.18.240.21
Subnet	255.255.255.0	255.255.255.0

Fonte: Autoria própria.

Tabela 4 - Configuração dos usuários SNMP

SNMP Users		
Name	**engenharia**	**public**
IP Address		
V1/V2c Community	PRAT	public
Auth Protocol	HMACMD5	HMACMD5
Priv Protocol	noPriv	noPriv
Auth Key	*******	*******
Confirm Auth Key	*******	*******
Priv Key		
Confirm Priv Key		

Fonte: Autoria própria.

Tabela 5 - Configuração do modelo de segurança

Security Model		
Security Model	snmpV3	snmpV2
Name	engenharia	public
Group	PRAT	public

Fonte: Autoria própria.

Tabela 6 - Configuração do acesso SNMP

SNMP Acess		
GROUP	PRAT	public
Security Model	snmpV3	snmpV2c
SecurityLevel	authNoPriv	noAuthNoPriv
ReadViewName	allofMib	allofMib
WriteViewName	allofMib	allofMib
NotifyViewName	allofMib	allofMib

Fonte: Autoria própria.

5.2 CONFIGURAÇÃO DO SERVIDOR ZABBIX

Somente a configuração dos equipamentos em campo não é necessário para realizar o monitoramento, e necessário também de um *software* (Zabbix), e um *hardware* (servidor) para realizar a aquisição dos dados configurados.

O modelo utilizado para o servidor é uma Matrix MXC-2000 da ADLINK, mostrado na Figura 12.

Figura 12 - Servidor Zabbix Mxc2000

Fonte: Autoria própria.

O servidor MXC-2000 é robusto e industrial, possui *slots* PCI e PCIe configurável. Essa máquina é projetada para fornecer uma plataforma confiável para uma ampla variedade de aplicações aceitando cartões PCI e PCIe padrão. O Matrix MXC-2000 pode operar em uma faixa de temperatura de -20 a 70 °C.

O processador utilizado é o Intel® Atom™ N270 com processamento de 1,6 GHz para fornecer desempenho adequado com baixa potência, possui também um HD SATA de 40 Gb e com 2 Gb de memória Ram. Esse PC industrial possui os seguintes recursos: a) Entrada de energia embutida alimentada por 9 a 32 V_{CC}; b)

Possui duas portas Ethernet 1000/100/10Mbs; e c) Duas portas RS-232 e duas portas RS-232/422/485.

Para rodar o *software* de monitoramento de rede é primeiro necessário realizar a instalação do sistema operacional. O sistema operacional escolhido é o Linux Ubuntu Server LTS (*Long Time Support*) versão 14.04.

O *software* utilizado para realizar a monitoramento da rede de automação é o Zabbix versão 3.0.

O *software* Zabbix foi criado por Alexei Vladishev, e atualmente o seu desenvolvimento é feito pela Zabbix SAI. Essa ferramenta é uma solução *Open Source* que permite monitorar vários parâmetros de uma rede e a integridade de servidores, *switches* e impressoras. O seu código-fonte e a sua documentação é distribuído gratuitamente e está publicada na *Internet* para o público em geral (ZABBIX, 2010).

Para realizar a instalação do Zabbix no servidor são necessários alguns requisitos mínimos, como 128 MB de memória e de armazenamento 256 MB, porém o armazenamento necessário pode aumentar, tanto a memória quanto o armazenamento vão depender da quantidade de monitorados e a quantidades de parâmetros configurados.

Para executar a instalação do Zabbix deve-se acessar o Linux como super usuário, através do comando *sudo su* e seguir os passos descritos no site do desenvolvedor do software (ZABBIX, 2018):

1° Passo

Através do comando wget foi executado o *download* dos arquivo na rede.

```
wget http://repo.zabbix.com/zabbix/3.0/ubuntu/pool/main/z/zabbix-release/zabbix-release_3.0-1+trusty_all.deb
dpkg -i zabbix-release_3.0-1+trusty_all.deb
apt-get update
```

2° Passo

Executado a instalação dos pacotes do banco de dados, da interface web e do MySQL (Gerenciador do banco de dados):

```
apt-get install zabbix-server-mysql zabbix-frontend-php
```

3° Passo

Instalação do Zabbix Agent:

```
apt-get install zabbix-agent
```

4° Passo
Criando o banco de dados MySQ:
cd /usr/share/doc/zabbix-server-mysql
zcat create.sql.gz | mysql -uroot zabbix

5° Passo
Configuração do Zabbix_server.conf
# vi /etc/zabbix/zabbix_server.conf
DBHost=localhost
DBName=zabbix
DBUser=zabbix
DBPassword=zabbix

6° Passo
Iniciar o processo Zabbix_Server
service zabbix-server start

7° Passo
Configurar o arquivo Apache, no diretório /etc/zabbix/apache.conf
php_value max_execution_time 300
php_value memory_limit 128M
php_value post_max_size 16M
php_value upload_max_filesize 2M
php_value max_input_time 300
php_value always_populate_raw_post_data -1
php_value date.timezone America/Sao_Paulo

8° Passo
Alterar e reiniciar o processo Apache
Acessar o arquivo no diretório /etc/php5/apache2/php.ini e alterar o seguinte parâmetro:
date.timezone = ‘America/São_Paulo’

Reiniciar o serviço apache2 utilizando o seguinte comando:
service apache2 restart

9 Passo
Realizar a instalação das Mibs padrão SNMP no Linux através do seguinte comando:
apt-get -y install snmp-mibs-dowloader

Editar o arquivo e comentar a palavra Mib no /etc/snmp/snmpd.conf
mibs:

10° Passo
Realização da configuração da interface web

Nessa etapa o software verifica os pré-requsitos mínimos do hardware para seguir com a instalação, todos os pré-requisitos foram preenchidos corretamente. Também deve-se realizar a configuração, da conexão da interface web com o banco de dados. A configuração ficou conforme descrito abaixo:
Database Type: MySQL
Database host: 127.0.0.1
Database port: 0
Database name: zabbixdb
User: zabbix
Password: zabbix

O próximo passo é a configuração do nome do servidor Zabbix e também o endereço do servidor, conforme descrição abaixo:
Host: 127.0.0.1
Port: 10051
Name: copel_zabbix

Após essas configurações o software Zabbix está pronto para realizar o monitoramento da rede.

Após as configurações dos equipamentos é necessário colocar o sistema operacional Linux em uma rede onde se consiga visualizar os *switches* e servidores seriais configurados. Para isso, foi necessário conversar com a equipe de informática para cadastrar um novo endereço do computador na rede e habilitar o tráfego do protocolo SNMP.

O endereço de rede do Servidor Zabbix ficou definido como na Tabela 7.

Tabela 7- Configuração de endereço de rede Zabbix

	Endereço	**Mascará**	**Gateway**
Servidor Zabbix	10.18.245.243	255.255.255.0	10.18.245.241

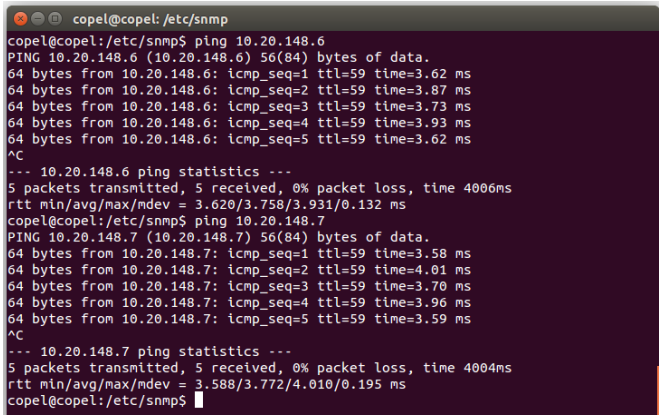
Fonte: Autoria própria.

Após inserir o servidor Zabbix na rede é necessário verificar se o servidor está conectado com os *switches* e o terminal serial na rede. Para isso foi executado o comando ping conforme descrição abaixo:

ping 10.18.240.20 Terminal Server 01 Subestação Bateias em Campo Largo.
ping 10.18.240.21 Switch 01 Subestação Bateias em Campo Largo
ping 10.20.148.6 Switch 01 Subestação Curitiba Norte Almirante Tamandaré
ping 10.20.148.7 Switch 02 Subestação Curitiba Norte Almirante Tamandaré
ping 10.20.148.8 Switch 03 Subestação Curitiba Norte Almirante Tamandaré.
ping 10.20.148.9 Switch 04 Subestação Curitiba Norte Almirante Tamandaré.

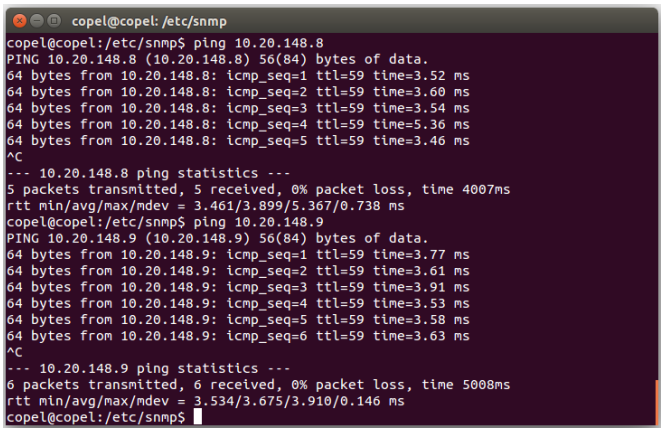
O comando ping conforme Figura 13,14 e 15 verifica se há uma conectividade em nível IP do computador de origem para o computador de destino.

Figura 13 - Conectividade entre o gerente e o agente



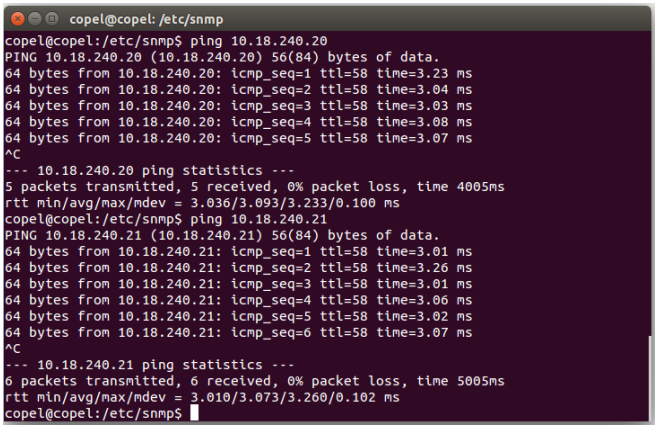
Fonte: Autoria própria.

Figura 14 - Conectividade entre o gerente e o agente



Fonte: Autoria própria.

Figura 15 - Conectividade entre o gerente e o agente



Fonte: Autoria própria.

Os equipamentos podem estar respondendo através do comando ping porém não é o suficiente para verificar se os equipamentos irão responder as solicitações do gerente para o agente utilizando o protocolo SNMP. Contudo podemos verificar se as informações de endereços e senhas estão cadastradas corretamente tanto no terminal server quanto no *switch* através do seguinte comando: *snmpwalk -v 2c -c senha configurada <host IP configurados>*

Este comando da plataforma Linux permite visualizar a estrutura completa de todas as das Mibs dos equipamentos e também os valores dos objetos solicitados.

Para saber o valor de um OID específico deve-se executar o comando: *Snmpget -v2c -c senhacadastrada <host IP configurados> número da OID*

Foi utilizado o programa SNMPB para verificar a estrutura completa de uma MIB.

5.3 PARAMETRIZAÇÃO DO ZABBIX

O Zabbix, neste trabalho está sendo utilizado para monitorar os equipamentos de rede utilizando o protocolo SNMP. Após a configuração dos parâmetros de rede devemos realizar a criação de Templates.

Segundo Horst, Déo e Pires (2016), *template* são regras para realizar coleta, alertas e representações gráficas de vários objetos dos elementos que estão sendo monitorados. Um template uma vez configurado pode ser utilizado várias vezes.

Para realizar a criação do template devemos realizar os seguintes passos: Configuração>Templates>Criar template.

A Tabela 8 mostra parâmetros de configuração de *template* na Zabbix.

Tabela 8 - Configuração de template no Zabbix

Propriedade	**Valor**
Nome	Ruggdcom
Nome visível	Monitoramento TS e Sw
Novo Grupo	*Discovered hosts*

Fonte: Autoria própria.

Na aba Associado aos Templates foi adicionado alguns templates existentes do protocolo SNMP, nestes templates estão configuradas alguns objetos do SNMP.

Depois de ter criado um template devemos criar um item. Segundo Horst, Déo e Pires (2016), qualquer dado que desejamos coletar é chamado de item, um template sem item é inútil.

Segue a Tabela 9 com os itens que queremos coletar dos *switches* e servidores seriais.

Tabela 9 - Identificação dos objetos mapeados no SNMP

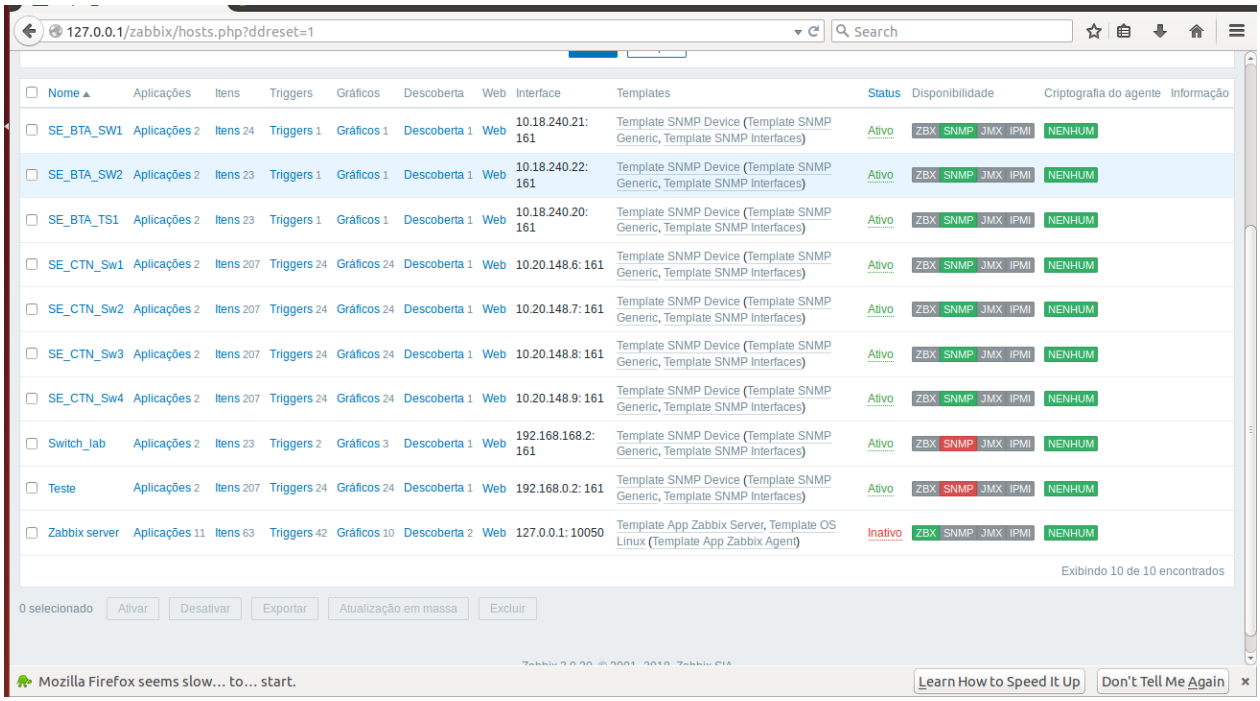
	OBJETO	**NOME**	**INFORMAÇÃO**
1	Grupo System 1.3.6.1.2.1.1	sysDesc.(1)	Descrição do sistema, nome completo e versão do tipo de hardware.
2		sysUpTime(3)	Tempo de atividade do sistema
3		sysContact (4)	Pessoa ou grupo responsável pelo equipamento na rede
4		sysName(5)	Nome do equipamento na rede
5		sysLocation (6)	Localização física do nó
6	1.3.6.1.2.1.2	ifNumber(1)	Número de interfaces de rede (independentemente do seu estado atual) presentes no sistema
7		ifSpeed(5)	Uma estimativa da largura de banda atual da interface em bits por segundo
8		ifAdminStatus(7)	Indica o estado desejado da interface
9		ifOperStatus(8)	Indica o estado atual de funcionamento do interface
10	1.3.6.1.4.1.15004.4.2.3.1.0	rcDeviceInfoSerialNumber	Indica o número serial do equipamento
11	1.3.6.1.4.1.15004.4.2.2.9.0	rcDeviceStsNoActiveAlarms	Indica o número de alarmes que há no equipamento
12	1.3.6.1.4.1.15004.4.2.2.6.0	rcDeviceStsCpuUsagePercent	Porcentagem da CPU utilizada
13	1.3.6.1.4.1.15004.4.2.2.6.0	rcDeviceStsPowerSupply1	Indica o estado de funcionamento da fonte1
14	1.3.6.1.4.1.15004.4.2.2.5.0	rcDeviceStsPowerSupply2	Indica o estado de funcionamento da fonte 2
15	1.3.6.1.4.1.15004.4.2.3.5.0	rcDeviceInfoTotalRam	Indica o tamanho total da memória Ram.
16	1.3.6.1.4.1.15004.4.2.2.2.0	rcDeviceStsAvailableRam	Indica o quanto o equipamento está consumindo de memória Ram
17	1.3.6.1.4.1.15004.4.2.3.3.0	rcDeviceInfoMainSwVersion	Indica a versão do Sistema Operacional

Fonte: Autoria própria.

Depois de cadastrados os itens mostrados na Tabela 9, deveremos criar *host* para cada equipamento a ser monitorado. É no *host* que adicionamos o nome do equipamento, endereço de rede, interface do tipo SNMP dos equipamentos a serem monitorados. Também é no *host* que foi vinculado ao template criado anteriormente.

Os *host* criados dos equipamentos a serem monitorados são apresentados na Figura 16.

Figura 16 - Estado de funcionamento dos hosts



Fonte: Autoria própria.

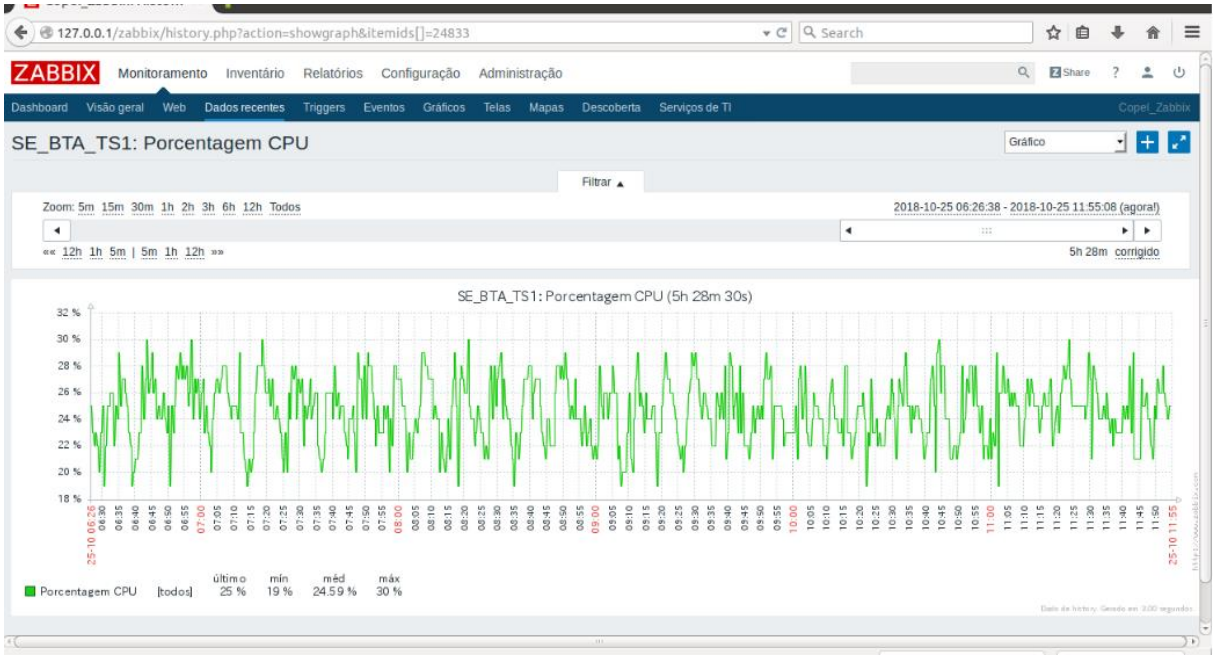
Os equipamentos que estão com cor verde na coluna disponibilidade, estão comunicando com os agentes corretamente.

6 APRESENTAÇÃO E ANÁLISE DOS RESULTADOS

Através das configurações em campo foi realizado a supervisão das portas elétricas e óticas como também da CPU, processamento, quantidade de memória Ram, número serial de equipamentos. Cada equipamento sob monitoração possui em torno de 2000 objetos a serem monitorados. Foram monitorados três diferentes equipamentos: um Switch 2730M do fabricante SEL, um Switch RSG2100, terminal Server RS416 do fabricante Ruggdcom. No equipamento do fabricante Ruggdcom foram realizados o monitoramento de todos os itens citados anteriormente, porém do fabricante da SEL não se conseguiu realizar o monitoramento da CPU, processamento, temperatura. Só foi possível realizar o monitoramento das *interfaces* elétrica e óticas. Através dos dados obtidos pode-se tomar uma decisão para executar uma manutenção mais adequada.

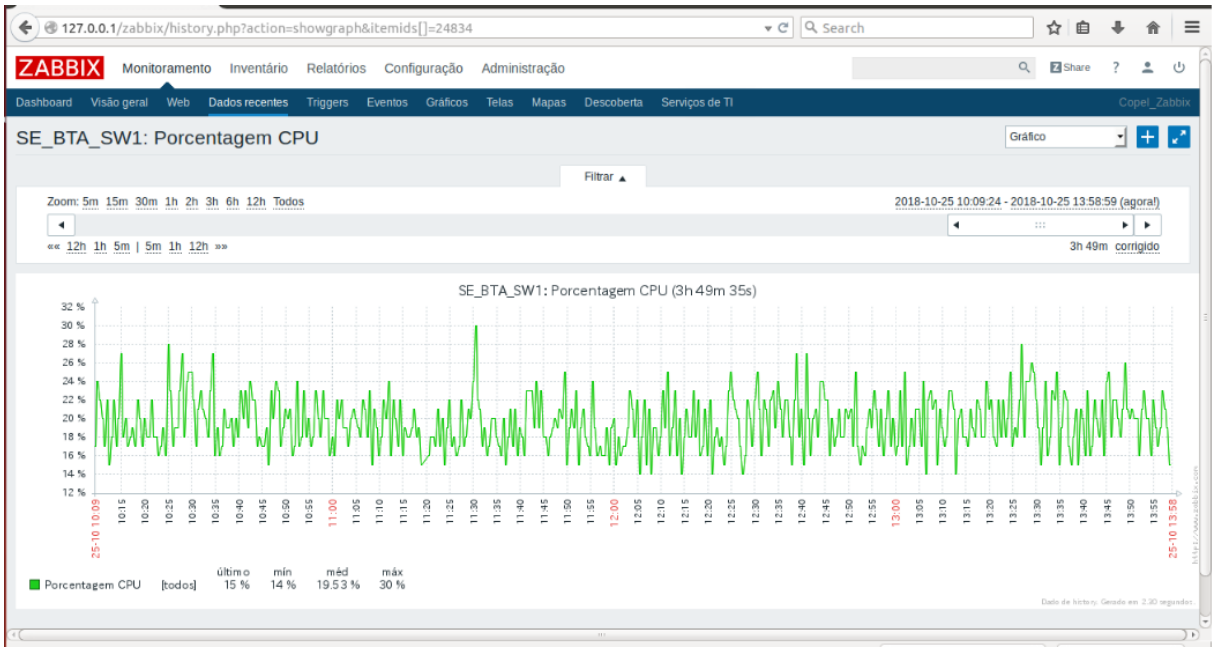
O primeiro ponto a ser monitorado foi a utilização da CPU do terminal server conforme Figura 17 e a Figura 18 nos mostra a utilização da CPU de um *switch*. Podemos observar que há uma grande variação da utilização da CPU, porém ainda é baixa, verificamos que este equipamento está trabalhando com folga.

Figura 17 - Monitoramento da CPU do terminal server



Fonte: Autoria própria.

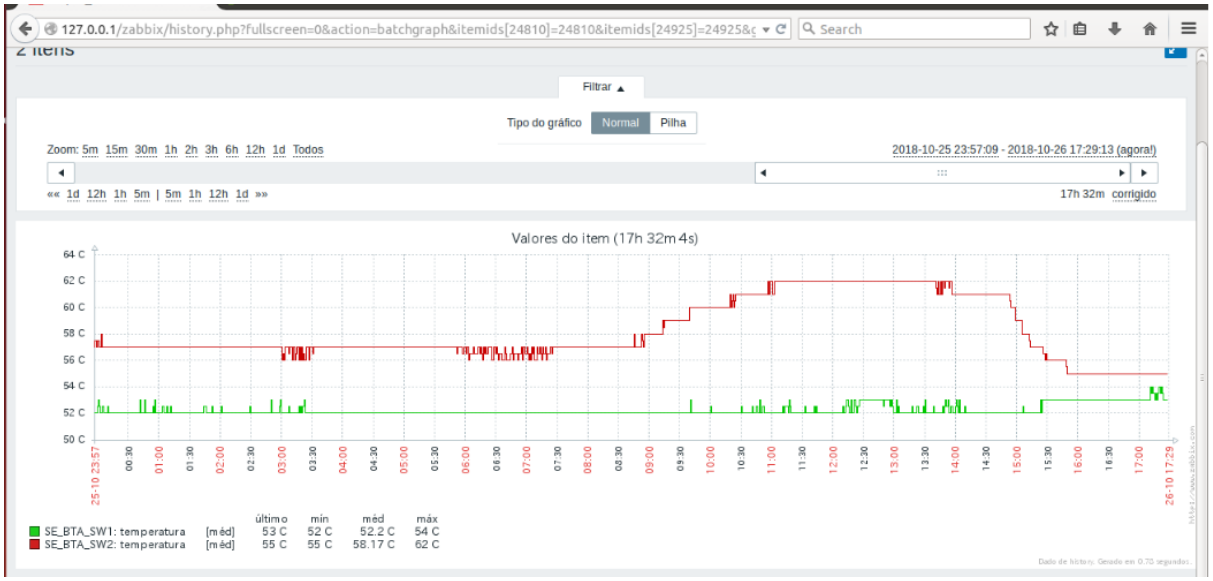
Figura 18 - Monitoramento da CPU do switch



Fonte: Autoria própria.

O segundo ponto a ser monitorado é a temperatura, observamos uma temperatura de trabalho com pouca variação conforme Figura 19. De acordo com o fabricante a temperatura de trabalho do *switch* da Ruggedcom está entre -40 à 85 °C. Tanto o terminal Server quanto o *Switch* apresentaram os valores próximos. O gráfico, ainda na Figura 19 nos mostra um equipamento com temperatura em condição ideal de trabalho, variando aproximadamente entre 52 e 62 ºC.

Figura 19 - Temperatura do switch



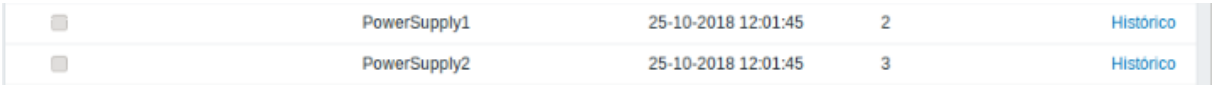
Fonte: Autoria própria.

O terceiro ponto a ser monitorado é a situação das fontes, esses equipamentos possuem duas fontes trabalhando de forma independente, o resultado do ponto coletado é um número inteiro onde:

O número 2 significa que a fonte está sendo alimentada com uma tensão de corrente contínua.

Entretanto o número 3 significa que a segunda fonte está sem alimentação e a se o dado coletado for 1 significa que a fonte de alimentação não está presente. A Figura 20 mostra o resultado da coleta dessa informação.

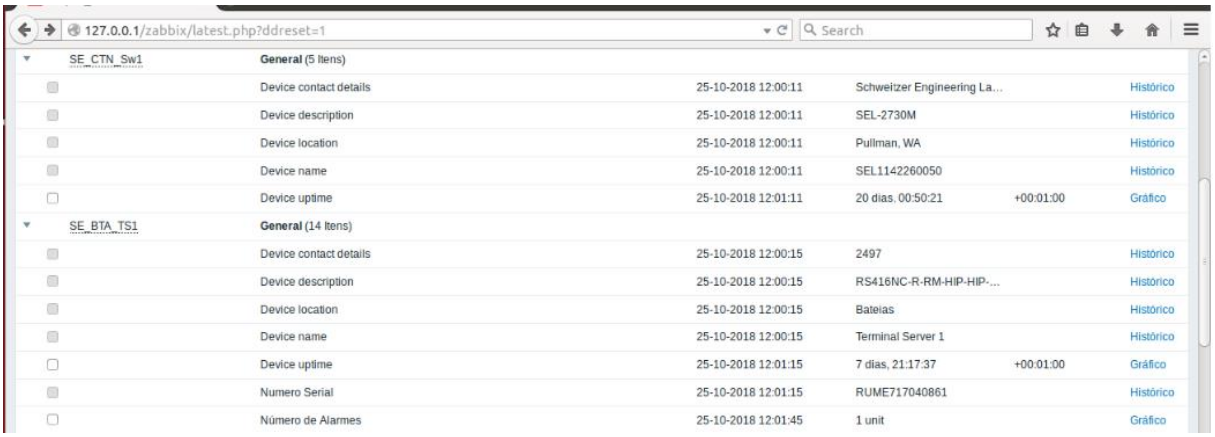
Figura 20 - Estado das fontes de alimentação



Fonte: Autoria própria.

Com relação a Figura 21, pode-se extrair vários dados do *switch* da subestação Curitiba Norte e da Subestação de Bateias.

Figura 21 - Estados coletados do dispositivo



Fonte: Autoria própria.

O primeiro ponto é o *Device Contact* esse ponto nos permite incluir o ramal da subestação que o equipamento foi colocado. No *switch* da Subestação Curitiba Norte ficou cadastrados os dados do fabricante, já no *switch* da Subestação Bateias cadastramos o ramal da Subestação.

O segundo ponto é o *Device Description* descreve o modelo do fabricante.

O terceiro ponto é o *Device Location,* é o lugar que o equipamento está instalado.

O quarto ponto é o *Device Name,* é o nome atribuído ao equipamento

O quinto ponto é o *Device uptime,* esse ponto mostra quanto tempo o equipamento está ligado, caso aconteça um *reset* no equipamento ele zera sua contagem.

No sexto e sétimo pontos consegue-se monitorar respectivamente o número de série do equipamento e com quantos alarmes este equipamento está no momento.

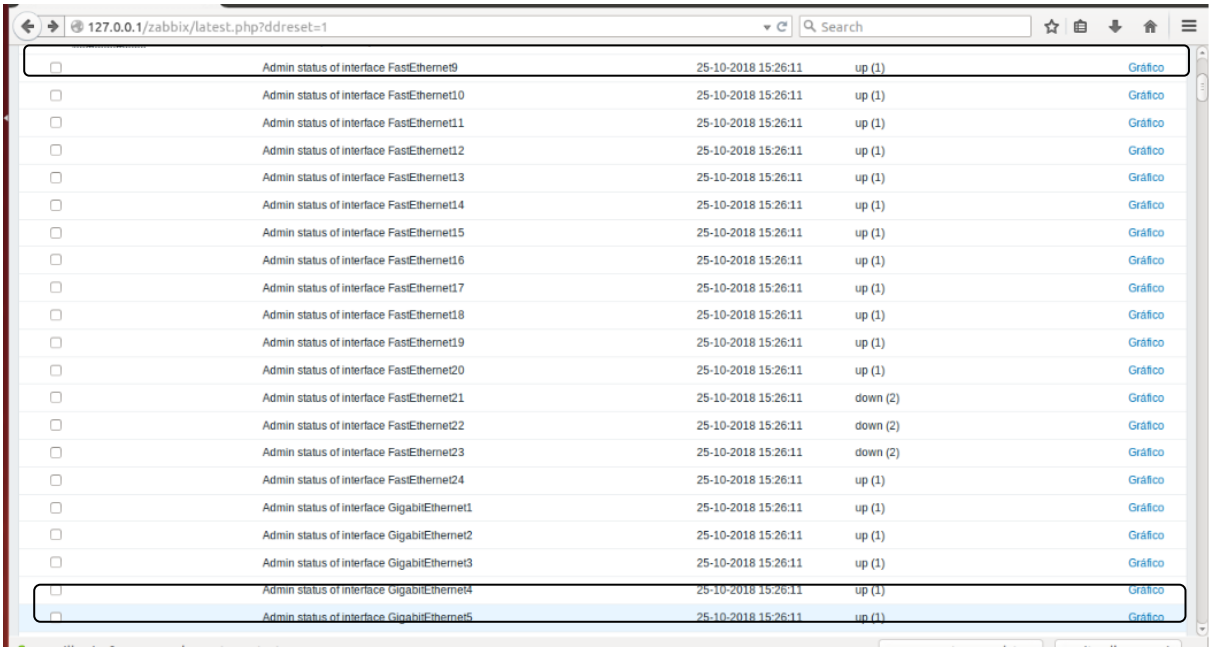
Outro ponto importante para o monitoramento é a versão do equipamento. Conforme Figura 22.

Figura 22 - Versão do sistema operacional

Fonte: Autoria própria.

Pode-se realizar o monitoramento tanto do estado das portas quanto o trafégo de dados das portas elétricas e óticas. Conforme Figura 23 verifica-se que a porta 5 e a porta 9 estão ativas, caso estivessem apresentando o número 2 a porta estaria inativa e se estivesse em 3 a porta estaria em teste.

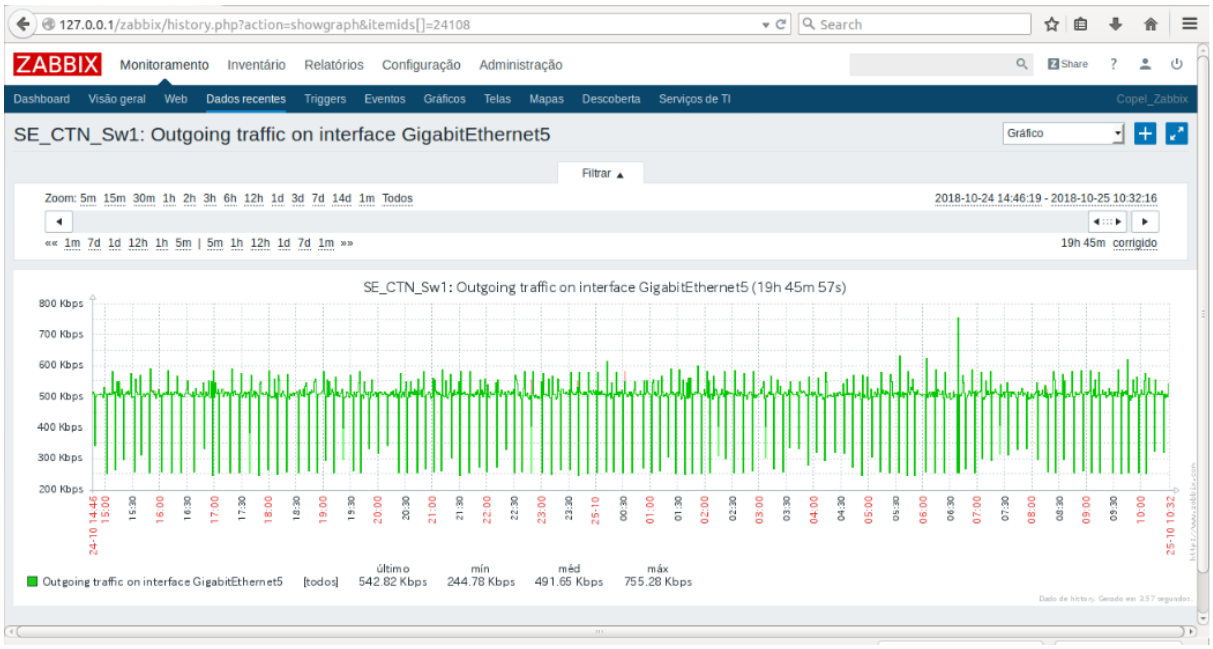
Figura 23 - Estado de funcionamento das portas elétricas e ópticas



Fonte: Autoria própria.

A porta 5, porta elétrica, verifica-se a taxa de transferência de entre os *switch*, conforme apresentado na Figura 24.

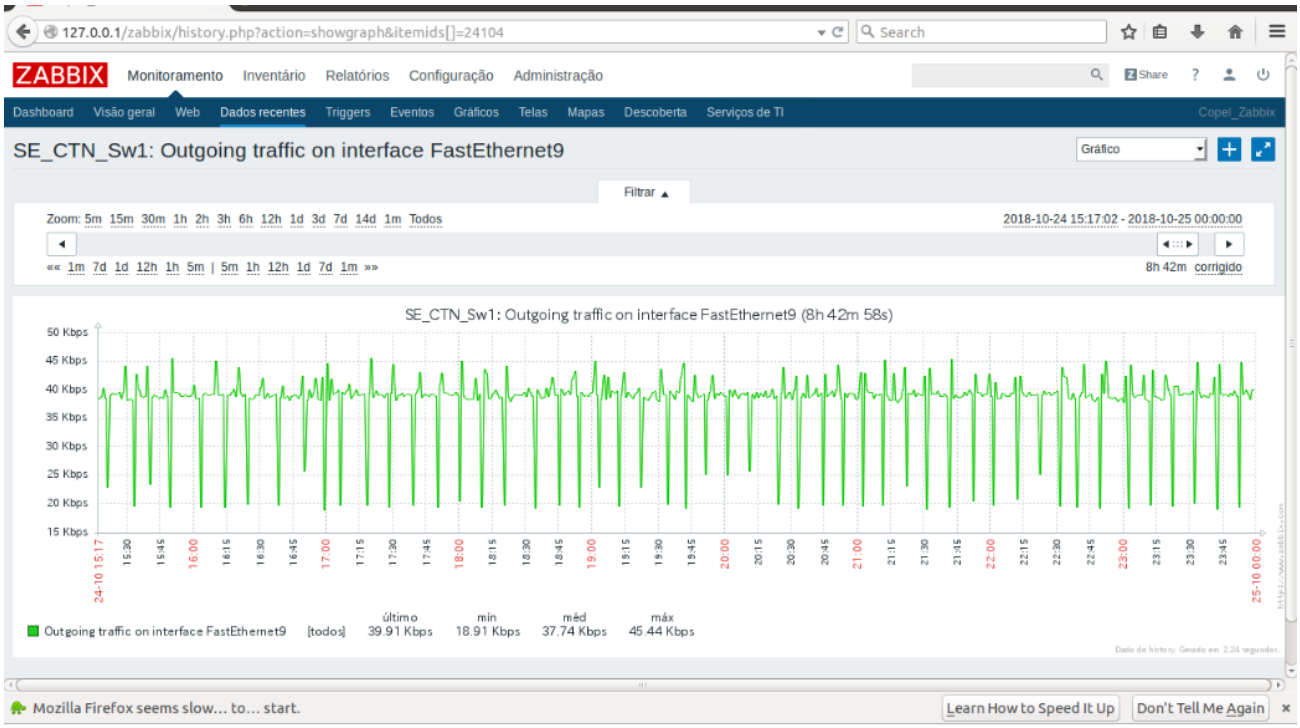
Figura 24 - Taxa de transferência da porta elétrica



Fonte: Autoria própria.

Na porta ótica 9 observa-se a taxa de transferência, essa porta é responsável pela aquisição de dados dos relés de proteção (Figura 25).

Figura 25 - Taxa de transferência da porta ótica



Fonte: Autoria própria.

7 CONSIDERAÇÕES FINAIS

Neste estudo prático pode-se observar o comportamento dos equipamentos em campo. O objetivo foi monitorar todos os parâmetros dos equipamentos principalmente temperatura, processamento, capacidade de armazenamento, porém verificou-se que em um equipamento de um fabricante específico não foi possível realizar o monitoramento, somente realizou-se o monitoramento do estado de funcionamento das portas. Tal dificuldade de monitoramento provavelmente esteja relacionada a erro configuração e será tratado futuramente.

Uma das maiores preocupações era em relação a temperatura de funcionamento dos *switch* e servidores seriais, alguns equipamentos estavam apresentando defeito, falha intermitente e queima de portas ópticas. As análises feitas anteriormente era por hipóteses, porém agora com o monitoramento contínuo desses equipamentos verificou-se através da Figura 19 que o *switch* está operando numa temperatura razoavelmente inferior à limitada pelo fabricante..

Também foi realizado as configurações das portas elétricas, para gerarem alarmes quando essas portas comutarem de estado ligado para desligado e vice-versa.

Com esses dados obtidos remotamente pode-se tomar decisões sem a necessidade de se deslocar até a subestação para retirar um relatório. Isso nos permite realizar uma tomada de decisão para manutenção mais rápida e com uma maior eficiência

O Software Zabbix também nos permite criar equações de monitoramento para o tráfego de dados de uma porta, isso nos ajuda a verificar uma anomalia no sistema, caso uma porta apresente uma taxa de comunicação maior ou menor que a banda de trabalho, pode-se gerar um alarme.

Como sugestão para trabalho futuro, pode-se incluir no Zabbix um sistema para envio dos alarmes via mensagem telefônica SMS para o supervisor ou gerente da área. Também observou-se que o gerente SNMP está apresentado uma leve demora ao coletar os dados, portanto para trabalhos futuros deverá ser instalado o Zabbix em um servidor com maior processamento e memória.

REFERÊNCIAS

ARNETT, Mattew Flint. **Desvendando o TCP/IP**. 1. ed. Rio de Janeiro: Campus, 1997.

BRANCO, Kalinka Castelo. **Redes de computadores**: da teoria à prática com Netkit. 1. Ed. Rio de Janeiro: Elsevier, 2015.

BRANQUINHO, Marcelo Ayres; et al. **Segurança da automação e SCADA**. 1. ed. Rio de Janeiro: Elsevier, 2014.

FOROUZAN, Behrouz A. **Comunicação de dados e redes de computadores**. 4. ed. São Paulo: McGraw-Hill, 2008.

HORST, Adail Spínola; DÉO, André Luis Boni; PIRES, Aécio dos Santos. **De A a ZABBIX**: Aprenda a monitorar e gerenciar aplicações e equipamentos de redes com o Zabbix. 3. ed. São Paulo: Novatec, 2016.

LIMA, Janssen dos Reis. **Monitoramento de redes com Zabbix**. 1. ed. Rio de Janeiro: Brasport, 2014.

SCHMITT, Marcelo Augusto Rauh; PERES, André; LOUREIRO, César Augusto Hass. **Rede de computadores**: Nível de aplicação e instalação de serviços. 1. ed. Porto Alegre: Bookman, 2013.

STALLINGS, William. **Redes e sistemas de comunicação de dados**: Teoria e aplicações corporativas. 5. ed. Rio de Janeiro: Elsevier, 2005.

ZABBIX. **Zabbix Documentação 1.8**. Copyright© 2001-2018 Zabbix SAI, publicado em: 19 mai. 2010. Disponível em: <https://www.zabbix.com/documentation/1.8/pt/manual/sobre>. Acesso em: 07 out. 2018.

ZABBIX. **Zabbix Documentation 3.0**: Instalação. Copyright© 2001-2018 Zabbix SAI. Disponível em: <https://www.zabbix.com/documentation/3.0/pt/manual/installation>. Acesso em: 07 out. 2018.