UNIVERSIDADE TECNOLÓGICA FEDERAL DO PARANÁ
DEPARTAMENTO ACADÊMICO DE ELETRÔNICA
CURSO DE ESPECIALIZACÃO EM CONFIGURAÇÃO E GERENCIAMENTO DE SERVIDORES E EQUIPAMENTOS DE REDE

ADRIANO ROBERTO VIDAL JUNIOR

# MONITORAMENTO DE EQUIPAMENTOS UTILIZANDO O PROTOCOLO SNMP

MONOGRAFIA

CURITIBA
2012

ADRIANO ROBERTO VIDAL JUNIOR

# MONITORAMENTO DE EQUIPAMENTOS UTILIZANDO O PROTOCOLO SNMP

Monografia apresentada como requisito parcial para obtenção do grau de especialista em Configuração e Gerenciamento de Servidores e Equipamentos de Redes, do Departamento Acadêmico de Eletrônica da Universidade Tecnológica Federal do Paraná.

Orientador: Prof. Dr. Kleber Kendy Horikawa Nabas

CURITIBA
2012

# RESUMO

VIDAL JUNIOR, Adriano Roberto. **Monitoramento de equipamentos utilizando protocolo SNMP**. 2012. 30 f. Monografia (Especialização em Gerenciamento de Redes) – Programa de Pós-Graduação em Tecnologia, Universidade Tecnológica Federal do Paraná. Curitiba, 2012.

O propósito deste trabalho é estudar o protocolo SNMP, os sistemas de monitoramento em código aberto que realizam monitoramento SNMP e implementá-lo de forma didática, apenas para teste das suas funcionalidades. O ambiente de teste é uma central técnica de uma emissora de televisão. Foram selecionados alguns equipamentos compatíveis com o protocolo SNMP e os parâmetros principais para monitoramento. O sistema de monitoramento implementado foi o Zabbix, devido a sua compatibilidade com o procolo SNMP, além de possuir um próprio agente para monitoramento de servidores.

**Palavras-chave:** SNMP. Zabbix. TV. Radiodifusão. Redes.

# ABSTRACT

VIDAL JUNIOR, Adriano Roberto. **SNMP Monitoring.** 2012. 30 f. Essay (Graduate Certificate in Networking and Systems Administration) - Graduate Programs in Technology, Federal Technological University of Paraná. Curitiba, 2012.

The purpose of this essay is to study is the SNMP protocol, monitoring systems that perform open source SNMP monitoring and implement it in a didactic way, just to test its functionalities. The test environment is a central technique of a broadcast television station. Some equipment compatible with the SNMP protocol was selected and the key parameters for monitoring. The monitoring system was implemented Zabbix, due to its compatibility with the Procolo SNMP, besides having a proper agent for monitoring servers.

**Keywords:** SNMP. Zabbix. TV. Broadcast. Network.

# LISTA DE FIGURAS

# LISTA DE TABELAS

# SUMÁRIO

# 1 INTRODUÇÃO

As empresas de radiodifusão utilizam-se de uma grande variedade de equipamentos, diversas são as fontes de sinais e muitos os dispositivos aplicados na distribuição e processamento de sinais de áudio e vídeo. A necessidade de transmissão ininterrupta destes sinais exige alta disponibilidade dos equipamentos compõem a cadeia o sistema de radiodifusão. São grandes os investimentos em equipamentos de alta qualidade e confiabilidade e também ma sua manutenção, que em sua maioria possuem interfaces de rede destinadas à configuração e monitoração. Um sistema capaz de monitorar as diversas variáveis de cada equipamento e informar qualquer desvio dos parâmetros pré estabelecidos pode auxiliar muito na identificação de problemas, permitindo rápida atuação e, conseqüentemente, a diminuição no tempo de indisponibilidade do sistema. Sendo assim, objetivo deste trabalho é a implantação de um sistema de monitoramento de equipamentos utilizados em uma emissora de televisão.

## 1.1 JUSTIFICATIVA

Uma grande quantidade de equipamentos é utilizada na cadeia de um sistema de transmissão de televisão, cada um destes possui uma função específica no processamento ou distribuição dos sinais de áudio e vídeo que são transmitidos aos telespectadores. A maioria dos equipamentos profissionais possui pelo menos uma interface de rede para configuração e gerenciamento das principais suas principais funcionalidades.

Como o sistema de transmissão exige alta disponibilidade, é de fundamental importância, além da manutenção preventiva periódica, o monitoramento dos equipamentos que compõem esta cadeia, fazendo uma escolha adequada dos principais parâmetros a serem observados e, conseqüentemente implementando um sistema de fácil visualização e que emita alertas para cada parâmetro divergente.

Desta maneira pretende-se minimizar o tempo de descoberta do problema, a fim e evitar a indisponibilidade do sistema, ou ao menos agilizar a tomada de ações em caso de problema.

## 1.2 OBJETIVOS

O objetivo geral é implementar um sistema de monitoramento em código aberto em uma cadeia de equipamentos de sistema de televisão.

Os objetivos específicos são:

- Instalar o sistema de monitoramento de rede Zabbix;
- Criar uma rede com os equipamentos a serem monitorados;
- Configurar os principais parâmetros de cada equipamento monitorado;
- Configurar o envio de alertas e indicação visual e parâmetros fora da normalidade.

## 1.3 PROCEDIMENTOS METODOLÓGICOS

O desenvolvimento do projeto seguirá as seguintes etapas:

- Pesquisar;
- Especificar;
- Implementar;
- Testar.

1. Pesquisar:
    - O protocolo SNMP;
    - Os possíveis sistemas de monitoramento SNMP;
    - As características do sistema de monitoramento escolhido;
    - Os parâmetros de cada equipamento.
2. Especificar:
    - A rede de monitoramento;
    - Os equipamentos monitorados;
    - Os parâmetros de cada equipamento;
    - Os alarmes de cada equipamento.
3. Implementar:
    - A rede de monitoramento;
    - O sistema de monitoramento.
4. Testar

- Os equipamentos monitorados;

Os alertas gerados pelo sistema.

## 1.4 CRONOGRAMA

O trabalho será executado em etapas, seguindo o seguinte cronograma:

| TAREFA | Junho | Julho | Agosto | Setembro | Outubro |
|---|---|---|---|---|---|
| Estudar o protocolo SNMP e os sistemas de monitoramento | X | X | | | |
| Escolher os equipamentos e os parâmetros a serem monitorados | | | X | | |
| Configurar uma rede de monitoramento e implementar o sistema de monitoramento | | | | X | |
| Entrega da monografia e defesa | | | | | X |

**Tabela 1 - Cronograma**

# 2 PROTOCOLO SNMP

O protocolo SNMP (*Simple Network Managment Protocol*) foi lançado em 1988 como um padrão para gerenciamento de dispositivos IP (*Internet Protocol*). Seu núcleo é constituído de um conjunto simples de operações que permitem a leitura de informações ou a escrita de parâmetros em dispositivos baseados em SNMP, permitindo o gerenciamento remoto destes dispositivos. O SNMP pode ser utilizado para o gerenciamento de diversos tipos de dispositivos, incluindo dispositivos físicos, como equipamentos de rede (roteadores, switches), fontes de energia, e também softwares, como servidores de bancos de dados, por exemplo (MAURO; SCHIMIDT, 2001).

Os padrões SNMP são definidos em uma série de documentos, chamados *request for comments* ou RFCs, propostas pelo *Internet Engineering Task Force* (IETF). Existem três versões do SNMP disponíveis atualmente:

- SNMP versão 1 (SNMPv1) - definida na RFC 1157;
- SNMP versão 2 (SNMPv2) - definido na RFC 1901, RFC 1908, RFC 3416 e RFC 3417;
- SNMP versão 3 (SNMPv3) - definido na RFC 3410, RFC 3411, RFC 3412, RFC 3413, RFC 3414, RFC 3415, RFC 3416, RFC 3417, RFC 3584, RFC 3826 e RFC 5343.

O IETF alterou o status de recomendação do SNMPv1 e SNMPv2c para histórico, e recomenda o uso SNMPv3 para o gerenciamento da internet. O SNMPv3 oferece mais segurança em relação às versões anteriores.

São dois os componentes principais no sistema de gerenciamento SNMP, os gerenciadores e os agentes. O gerenciador constitui-se de um servidor executando algum tipo de sistema de *software* responsável pelas tarefas de gerenciamento de uma rede. Os gerenciadores são chamados NMSs (*Network Management Stations* - estações de gerenciamento de rede). Uma NMS solicita informações dos agentes através de *poolings*, pode alterar a configuração dos agentes, caso tenha permissão de gravação e também pode receber *traps* de agentes de rede (MAURO; SCHIMIDT, 2001).

O agente SNMP é executado nos dispositivos de rede monitorados, pode ser um aplicativo separado ou incorporado ao sistema operacional do dispositivo. O agente responde às solicitações de informações da NMS, rastreando os diversos aspectos operacionais dos

dispositivos monitorados. O agente também pode enviar *traps* ao NMS informando alguma transição de estado do dispositivo (MAURO; SCHIMIDT, 2001).

Os *polls* utilizam-se de consultas de informações dos agentes geradas pelo NMS e as *traps* tratam-se do método utilizado por um agente para informar o NMS a ocorrência de algum evento importante (MAURO; SCHIMIDT, 2001).

As informações acessadas pela NMS estão definidas em uma lista de objetos que o agente pode rastrear, a MIB (*Management Information Base* - base de informações de gerenciamento), que pode ser considerada um banco de dados de objetos gerenciados que o agente rastreia. Todo tipo de informações sobre status ou estatísticas acessado pela NMS é definida em uma MIB. Várias MIBs podem ser implementadas por um agente, mas uma MIB específica, denominada MIB-II (RFC 1213), é implementada por todos os agentes, e engloba informações gerais sobre gerenciamento de TCP/IP. Mas cada fornecedor pode definir variáveis de MIB para uso próprio, de acordo com as necessidades e características de seus equipamentos, ampliando o número de equipamentos que podem ser monitorados pelo NMS (MAURO; SCHIMIDT, 2001).

O protocolo de transporte utilizado pelo SNMP para a troca de informações entre gerenciadores e agentes é o *User Datagram Protocol* (UDP) que embora não seja orientado à conexão, e não se tenha garantia na entrega da informação, não sobrecarrega a rede com retransmissões. O SNMP, por padrão, utiliza a porta 161 do UDP para enviar e receber solicitações e a porta 162 para receber *traps* dos dispositivos gerenciados (MAURO; SCHIMIDT, 2001).

Para garantir a confiabilidade da troca de informações entre gerenciadores e agentes, o SNMPv1 e SNMPv2 utilizam o conceito de comunidades. Os nomes das comunidades configurados em um agente SNMP consistem basicamente em uma senha utilizada pelo gerenciador para acesso às informações. O agente pode ser configurado com três nomes de comunidade: *read-only*, *read-write* e *trap*. Cada uma define um nível de acesso. O SNMPv3 oferece mais segurança pois utiliza, entre outros aspectos, autenticação e comunicação segura entre os dispositivos SNMP (MAURO; SCHIMIDT, 2001).

A mensagem que os gerenciadores e agentes utilizam para a troca de informações é chamada de *Protocol Data Unit* (PDU), são possíveis os comandos: *get*, *get-next*, *get-bulk* (SNMPv2 e SNMPv3), *set*, *get-response*, *trap*, *notification* (SNMPv2 e SNMPv3), *inform* (SNMPv2 e SNMPv3) e *report* (SNMPv2 e SNMPv3); cada uma com seu formato padrão de PDU (MAURO; SCHIMIDT, 2001).

# 3 NMS ZABBIX

Existem diversos sistemas de gerenciamento no mercado, inclusive sistemas proprietários dos fabricantes dos equipamentos escolhidos para o desenvolvimento deste trabalho. O objetivo é implementar, em pequena escala, um sistema não proprietário para o monitoramento destes equipamentos e testar a sua eficácia, visto que os softwares proprietários tem um custo elevado.

Entre os diversos sistemas em código aberto disponíveis optou-se pelo Zabbix por possuir uma interface gráfica amigável, com possibilidade de montagem de relatórios, gráficos e mapas, compatibilidade com SNMP, agente SNMP próprio para monitoramento de servidores.

O Zabbix foi criado por Alexei Vladishev, e atualmente é desenvolvido ativamente e suportado pela Zabbix SIA. Zabbix é uma solução em código aberto de monitoração para empresas. Zabbix é um *software* que monitora vários parâmetros de rede de computadores e saúde e integridade de servidores. Zabbix usa um mecanismo de notificação flexível que permite aos usuários configurarem alerta de *e-mail* baseado em praticamente qualquer evento. Isto permite uma rápida reação para problemas em servidores. Zabbix oferece relatórios e visualização de dados com excelentes características baseados nos dados armazenados. Isso faz do Zabbix ideal para o planejamento de capacidade (Zabbix, 2012).

O Zabbix suporta polling e trapping. Todos os relatórios Zabbix e estatísticas, bem como os parâmetros de configuração, são acessados através de uma ferramenta *Web* que é o *front-end* do produto. Uma ferramenta *web* assegura que o *status* da rede e da saúde dos servidores pode ser avaliado a partir de qualquer localização. Devidamente configurado, Zabbix pode desempenhar um papel importante no controle da infra-estrutura de Tecnologia de Informação (TI). Isto é igualmente verdadeiro para as pequenas organizações com poucos servidores e para as grandes empresas com muitos servidores (Zabbix, 2012).

O Zabbix é um *software* é gratuito e é desenvolvido e distribuído de acordo com a GPL (*General Public License*) versão 2. Isso significa que seu código-fonte é distribuído gratuitamente e está disponível para o público em geral. O suporte comercial está disponível e é fornecido pela Zabbix Company (Zabbix, 2012).

## 3.1 INSTALAÇÃO DO SISTEMA

Como o objetivo do trabalho é testar as funcionalidades e o desempenho de um sistema de monitoramento em código aberto, o mesmo foi instalado em máquina virtual, por tratar-se de uma solução de baixo custo. Foi utilizado o sistema de virtualização VirtualBox da Oracle. Neste sistema, foi criada uma máquina virtual com o sistema operacional Linux Debian. Todos os sistemas escolhidos são código aberto e podem facilmente ser encontrados na internet. O computador escolhido para a instalação dos *softwares* atende os requisitos mínimos dos mesmos.

A instalação do sistema Zabbix e a sua configuração foi realizada de acordo com as instruções disponíveis no Manual do Zabbix. A versão instalada foi a 1.8. Os requisitos de *software* para o sistema são:

- Apache – servidor *web*;
- PHP – para interface *web*;
- MySQL – banco de dados.

Adicionalmente foram instalados:

- Fping – para suporte à ICMP;
- Net-SNMP – para suporte à SNMP.

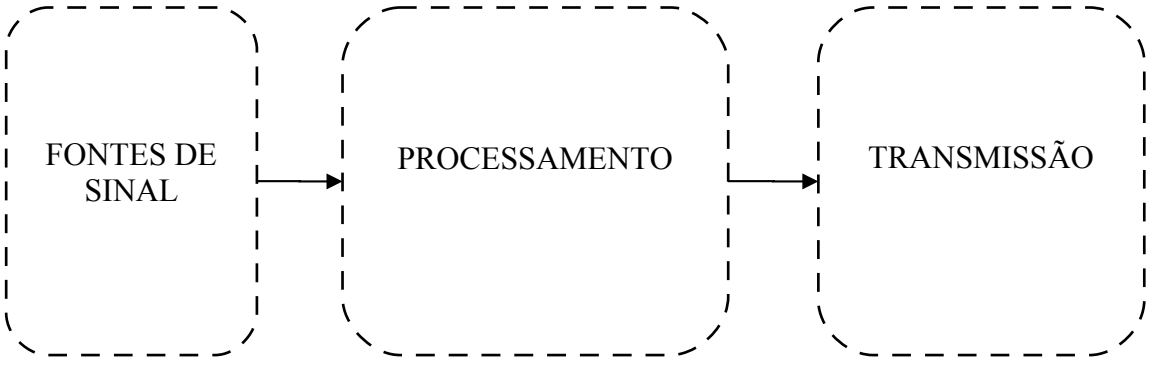
Foram necessárias algumas correções de bugs conhecidos da instalação do sistema, como a formatação do banco de dados MySQL, que torna possível a utilização de ícones personalizados para a montagem dos mapas. Também foi adicionado um *script* para a utilização do sistema para recepção de *traps* SNMP. O sistema Zabbix utiliza o *snmptrapd*, um *daemon* do Net-SNMP para receber as *traps*, e então um *script* se encarrega de enviá-las para o Zabbix.

# 4 IMPLEMENTAÇÃO

O sistema de monitoramento foi aplicado no ambiente de Central Técnica de uma emissora de televisão. Neste ambiente operacional ocorrem o recebimento, o processamento, a distribuição e a transmissão dos sinais de áudio e vídeo provenientes das geradoras, bem como a inserção dos sinais de áudio e vídeo provenientes da própria emissora.

Abaixo, na figura 1, um esquema simplificado do fluxo de sinais da emissora de televisão onde foi testado o sistema de monitoramento.

**Figura 1 - Esquema simplificado**




São diversas as fontes de sinais, fontes externas como receptores de satélite, decodificadores de fibra óptica e receptores de rádio e fontes de sinais internas como

exibidores de comerciais e exibidores de jornalismo. Todos estes sinais, antes da sua transmissão, são processados. O processamento inclui a distribuição dos sinais, comutação, controle de nível de áudio e vídeo, inserção de caracteres e logos, inserção de atraso na programação, etc. É grande a quantidade de equipamentos utilizados neste sistema, e a grande maioria deles possuem pelo menos uma interface de rede.

A figura 2 abaixo representa uma rede real com os equipamentos utilizados no processamento, distribuição e comutação de uma pequena emissora. Esta cadeia é utilizada tanto no fluxo de sinal SD, para a transmissão do canal analógico, quanto no fluxo de sinal HD, para a TV Digital. Como a emissora está em processo de implantação da TV Digital, optou-se por uma solução completa, renovando o parque de equipamentos da TV Analógica, ao mesmo tempo apto para a TV Digital. Durante o processo de aquisição dos equipamentos, optou-se pelo mesmo fornecedor, Harris Corporation®, obtendo vantagens de compatibilidade de protocolos e facilidade de manutenção, além dos ganhos de negociação para a compra em massa.

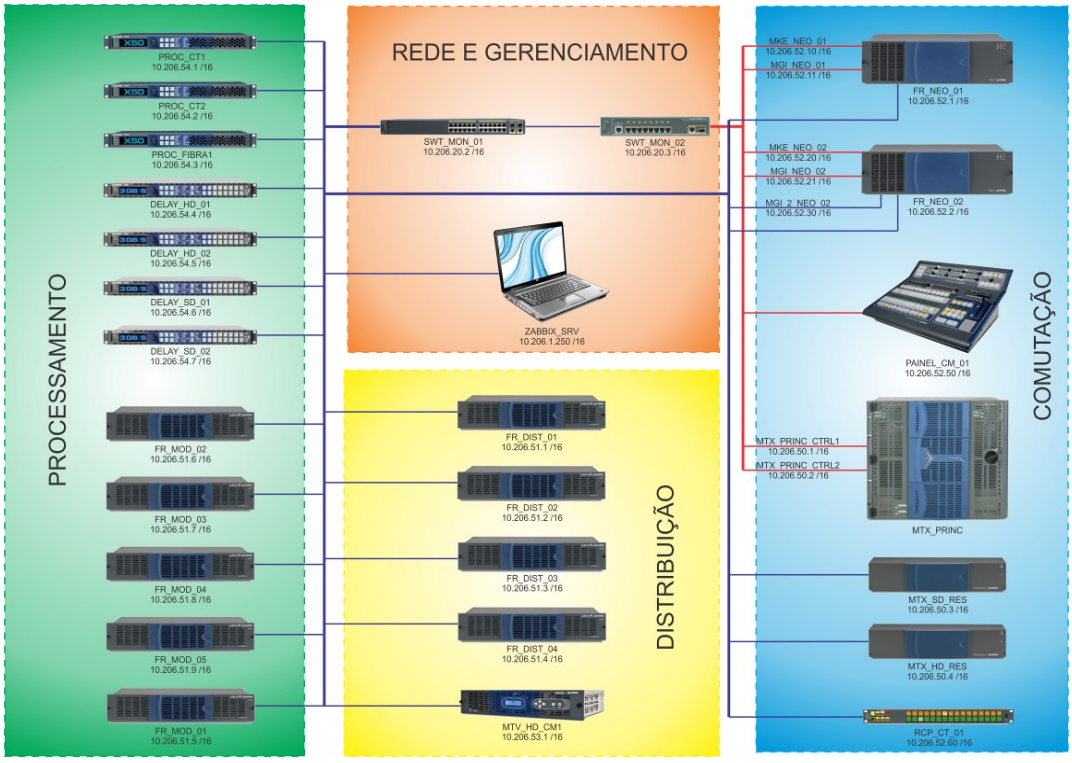



**Figura 2 - Diagrama da rede completa**

Para o desenvolvimento do trabalho, uma rede menor foi montada, com o objetivo de facilitar a implementação, devido ao curto espaço de tempo para tal e também com o

intuito de criar um modelo de cada equipamento dentro da ferramenta Zabbix, facilitando uma posterior expansão do sistema.

Os equipamentos escolhidos para a monitoração foram:

*Frame* NEO® da marca Harris®, modelo FR-3923-E, com placas que compõem o sistema IconMaster™;

Processador da marca Harris®, modelo X50™, para múltiplas aplicações da plataforma de áudio e vídeo;

*Switch* da marca Cisco®, modelo Catalyst 2960.

Na figura 3, a rede montada para teste do sistema:

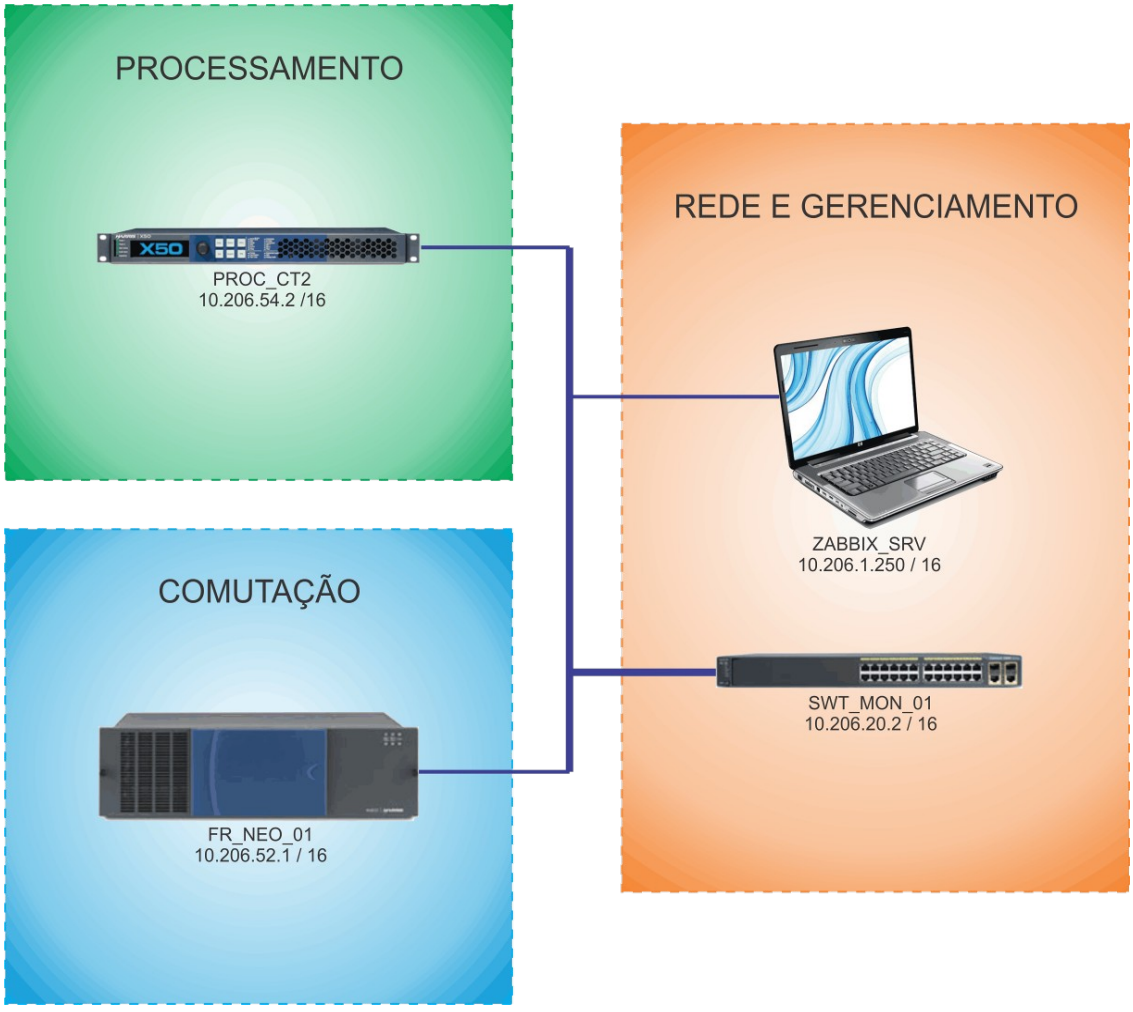



**Figura 3 - Diagrama da rede de testes**

Os equipamentos escolhidos têm compatibilidade com SNMP versão 1 e 2 e suas MIBs podem ser encontradas no site do próprio fabricante, necessitando apenas a criação de *login* para o acesso.

A rede foi configurada conforme a tabela 2 a seguir:

| EQUIPAMENTO | *HOSTNAME* | ENDEREÇO IP | MÁSCARA DE SUBREDE |
|---|---|---|---|
| FR-3923-E | FR_NEO_01 | 10.206.52.1 | 255.255.0.0 |
| X50™ | PROC-2 | 10.206.54.2 | |
| *SWITCH* | SWT_MON_01 | 10.206.20.2 | |
| SERVIDOR ZABBIX | ZABBIX_SRV | 10.206.1.250 | |

**Tabela 2 - Configurações de rede**

Cada equipamento tem uma grande quantidade de itens SNMP que podem ser monitorados, e a escolha de cada item ocorreu de acordo com as necessidades.

Da MIB do *frame* FR-3923-E foram selecionados os parâmetros, mostrados na tabela 4:

| NOME | OID | DESCRIÇÃO | LISTA DE VALORES |
|---|---|---|---|
| mke3901CommunicationErrorValue | 1.3.6.1.4.1.3142.2.3.160.1.52.1.81 | *Communication Error* | *no (0)*<br>*yes (1)* |
| mgi3902dReferenceIPValue | 1.3.6.1.4.1.3142.2.3.180.1.7.1.81 | *Reference I/P Present* | *OCTET STRING* |
| mgi3902dProgrammeIPAlarmValue | 1.3.6.1.4.1.3142.2.3.180.1.31.1.81 | *Programme Input Alarm* | *no (0)*<br>*yes (1)* |

**Tabela 3 - Parâmetros do FR-3923-E**

Da MIB do processador X50™ foram selecionados os parâmetros, mostrados na tabela 5:

| NOME | OID | DESCRIÇÃO | LISTA DE VALORES |
|---|---|---|---|
| x50FanStatusValue | 1.3.6.1.4.1.3142.2.4.10.1.516.1.81 | *Display the status of the cooling fans* | *OCTET STRING* |
| x50SDI1VideoStatusValue | 1.3.6.1.4.1.3142.2.4.10.1.20.1.81 | *Display the SDI 1 input video status* | *ENUM* |
| x50ReferenceStatusValue | 1.3.6.1.4.1.3142.2.4.10.1.454.1.81 | *Displays the reference video status* | *ENUM* |

**Tabela 4 - Parâmetros do X50™**

Os itens ENUM dispõem de uma lista de possíveis valores que representam o formato do sinal de entrada.

Além da monitoração utilizando SNMP, foi criado um item de monitoração simples, que nada mais é que o resultado do *ping* executado pelo próprio Zabbix para verificação da disponibilidade do equipamento na rede.

Para cada parâmetro selecionado foi criada uma *trigger*, que gera um alerta em caso de valores fora do padrão. Também foram criadas telas com mapas e gráficos de alguns dados do sistema.

## 4.1 CONFIGURANDO O ZABBIX

Para que o sistema Zabbix monitore itens SNMP, é necessário o funcionamento correto do NET-Snmp. Foram necessárias algumas alterações nos arquivos de configuração deste utilitário para que ele pudesse encontrar as MIBS dos equipamentos selecionados.

Foram criados dois grupos de hosts para os equipamentos a serem monitorados, além dos grupos existentes. Os grupos criados foram:

- REDE;
- Eqptos_Harris.

Dentro do grupo REDE foi criado um host que representa o *switch* utilizado na rede de monitoramento, denominado SW_MON_01. Este host foi associado ao *template*

Template_Cisco_2960, que contém diversos itens pré configurados para monitoramento do switch, como a taxa de transferência de entrada e saída de dados de cada porta do *switch*.

Na figura 4, estão os grupos criados no Zabbix:

| Nome | # | Membros |
|---|---|---|
| Discovered Hosts | Templates (0)<br>Hosts (0) | - |
| Eqptos Harris | Templates (0)<br>Hosts (2) | FR_NEO_01, PROC-2 |
| Linux servers | Templates (0)<br>Hosts (0) | - |
| REDE | Templates (0)<br>Hosts (1) | SW_MON_01 |
| SNMP Devices | Templates (0)<br>Hosts (1) | snmptraps |
| Templates | Templates (42)<br>Hosts (0) | Template_3COM_3824, Template_3COM_4400, Template_AIX, Template_APC_Automatic_Transfer_Switch, Template_APC_Battery, Template_App_MySQL, Template_C3750-48TS, Template_Cisco_837, Template_Cisco_877, Template_Cisco_2960, Template_Cisco_PIX, Template_Cisco_PIX515E, Template_Cisco_PIX_525, Template_Dell_OpenManage, Template_Dell_PowerConnect_5224, Template_Dell_PowerConnect_5324, Template_Dell_PowerConnect_6248, Template_Dell_PowerEdge, Template_FreeBSD, Template_Hibernate, Template_HPUX, Template_HP_ColorLaserJet, Template_HP_InsightManager, Template_HP_Procurve, Template_IPMI_Sun_Fire_X4100_M2, Template_Java, Template_Linux, Template_MacOS_X, Template_Microsoft_Exchange_2003, Template_Microsoft_Exchange_2007, Template_Microsoft_SQLServer_2005, Template_NetScreen_25, Template_Netware, Template_OpenBSD, Template_pfSense, Template_SNMPv1_Device, Template_SNMPv2_Device, Template_Solaris, Template_Standalone, Template_Tomcat, Template_Tru64, Template_Windows |
| Windows servers | Templates (0)<br>Hosts (0) | - |
| Zabbix Servers | Templates (0)<br>Hosts (1) | Zabbix Server |

**Figura 4 - Grupos criados no Zabbix**

Para habilitar o agente SNMP do *switch*, foram utilizados os comandos *snmp-server community itws ro*, onde *itws* é o nome da comunidade e *ro* define o acesso somente-leitura para esta comunidade.

O *template* do *host* SW_MON_01 contém o tráfego de dados de entrada e saída de cada porta do *switch*, conforme a figura 5:

Lista de hosts | Aplicações (0) | Triggers (0) | Gráficos (26) | **Host:** SW_MON_01 | **DNS:** - | **IP:** 10.206.20.2 | **Porta:** 10050 | **Status:** Monitorado | **Disponibilidade:** Desconhecido

1 | 2 | Próximo >

| Log | Descrição | Triggers | Chave | Intervalo | Histórico | Estatísticas | Tipo | Status | Aplicações | Erro |
|---|---|---|---|---|---|---|---|---|---|---|
| | Template_Cisco_2960:FastEthernet0/1-IN | Triggers (0) | ifInOctets.10001 | 15 | 7 | 365 | Agente SNMPv2 | Ativo | - | ✓ |
| | Template_Cisco_2960:FastEthernet0/1-OUT | Triggers (0) | ifOutOctets.10001 | 15 | 7 | 365 | Agente SNMPv2 | Ativo | - | ✓ |
| | Template_Cisco_2960:FastEthernet0/2-IN | Triggers (0) | ifInOctets.10002 | 15 | 7 | 365 | Agente SNMPv2 | Ativo | - | ✓ |
| | Template_Cisco_2960:FastEthernet0/2-OUT | Triggers (0) | ifOutOctets.10002 | 15 | 7 | 365 | Agente SNMPv2 | Ativo | - | ✓ |
| | Template_Cisco_2960:FastEthernet0/3-IN | Triggers (0) | ifInOctets.10003 | 15 | 7 | 365 | Agente SNMPv2 | Ativo | - | ✓ |
| | Template_Cisco_2960:FastEthernet0/3-OUT | Triggers (0) | ifOutOctets.10003 | 15 | 7 | 365 | Agente SNMPv2 | Ativo | - | ✓ |
| | Template_Cisco_2960:FastEthernet0/4-IN | Triggers (0) | ifInOctets.10004 | 15 | 7 | 365 | Agente SNMPv2 | Ativo | - | ✓ |
| | Template_Cisco_2960:FastEthernet0/4-OUT | Triggers (0) | ifOutOctets.10004 | 15 | 7 | 365 | Agente SNMPv2 | Ativo | - | ✓ |
| | Template_Cisco_2960:FastEthernet0/5-IN | Triggers (0) | ifInOctets.10005 | 15 | 7 | 365 | Agente SNMPv2 | Ativo | - | ✓ |
| | Template_Cisco_2960:FastEthernet0/5-OUT | Triggers (0) | ifOutOctets.10005 | 15 | 7 | 365 | Agente SNMPv2 | Ativo | - | ✓ |
| | Template_Cisco_2960:FastEthernet0/6-IN | Triggers (0) | ifInOctets.10006 | 15 | 7 | 365 | Agente SNMPv2 | Ativo | - | ✓ |
| | Template_Cisco_2960:FastEthernet0/6-OUT | Triggers (0) | ifOutOctets.10006 | 15 | 7 | 365 | Agente SNMPv2 | Ativo | - | ✓ |
| | Template_Cisco_2960:FastEthernet0/7-IN | Triggers (0) | ifInOctets.10007 | 15 | 7 | 365 | Agente SNMPv2 | Ativo | - | ✓ |
| | Template_Cisco_2960:FastEthernet0/7-OUT | Triggers (0) | ifOutOctets.10007 | 15 | 7 | 365 | Agente SNMPv2 | Ativo | - | ✓ |
| | Template_Cisco_2960:FastEthernet0/8-IN | Triggers (0) | ifInOctets.10008 | 15 | 7 | 365 | Agente SNMPv2 | Ativo | - | ✓ |
| | Template_Cisco_2960:FastEthernet0/8-OUT | Triggers (0) | ifOutOctets.10008 | 15 | 7 | 365 | Agente SNMPv2 | Ativo | - | ✓ |
| | Template_Cisco_2960:FastEthernet0/9-IN | Triggers (0) | ifInOctets.10009 | 15 | 7 | 365 | Agente SNMPv2 | Ativo | - | ✓ |
| | Template_Cisco_2960:FastEthernet0/9-OUT | Triggers (0) | ifOutOctets.10009 | 15 | 7 | 365 | Agente SNMPv2 | Ativo | - | ✓ |
| | Template_Cisco_2960:FastEthernet0/10-IN | Triggers (0) | ifInOctets.10010 | 15 | 7 | 365 | Agente SNMPv2 | Ativo | - | ✓ |
| | Template_Cisco_2960:FastEthernet0/10-OUT | Triggers (0) | ifOutOctets.10010 | 15 | 7 | 365 | Agente SNMPv2 | Ativo | - | ✓ |
| | Template_Cisco_2960:FastEthernet0/11-IN | Triggers (0) | ifInOctets.10011 | 15 | 7 | 365 | Agente SNMPv2 | Ativo | - | ✓ |
| | Template_Cisco_2960:FastEthernet0/11-OUT | Triggers (0) | ifOutOctets.10011 | 15 | 7 | 365 | Agente SNMPv2 | Ativo | - | ✓ |
| | Template_Cisco_2960:FastEthernet0/12-IN | Triggers (0) | ifInOctets.10012 | 15 | 7 | 365 | Agente SNMPv2 | Ativo | - | ✓ |
| | Template_Cisco_2960:FastEthernet0/12-OUT | Triggers (0) | ifOutOctets.10012 | 15 | 7 | 365 | Agente SNMPv2 | Ativo | - | ✓ |
| | Template_Cisco_2960:FastEthernet0/13-IN | Triggers (0) | ifInOctets.10013 | 15 | 7 | 365 | Agente SNMPv2 | Ativo | - | ✓ |

**Figura 5 - Parte dos itens do *host* SW_MON_01**

No grupo de *hosts* denominado Eqptos_Harris, foram criados os *hosts* FR_NEO_01 e PROC-2.

A figura 6, mostra detalhadamente como foi criado o *hosts* FR_NEO_01. Os demais *hosts* foram criados de maneira similar:

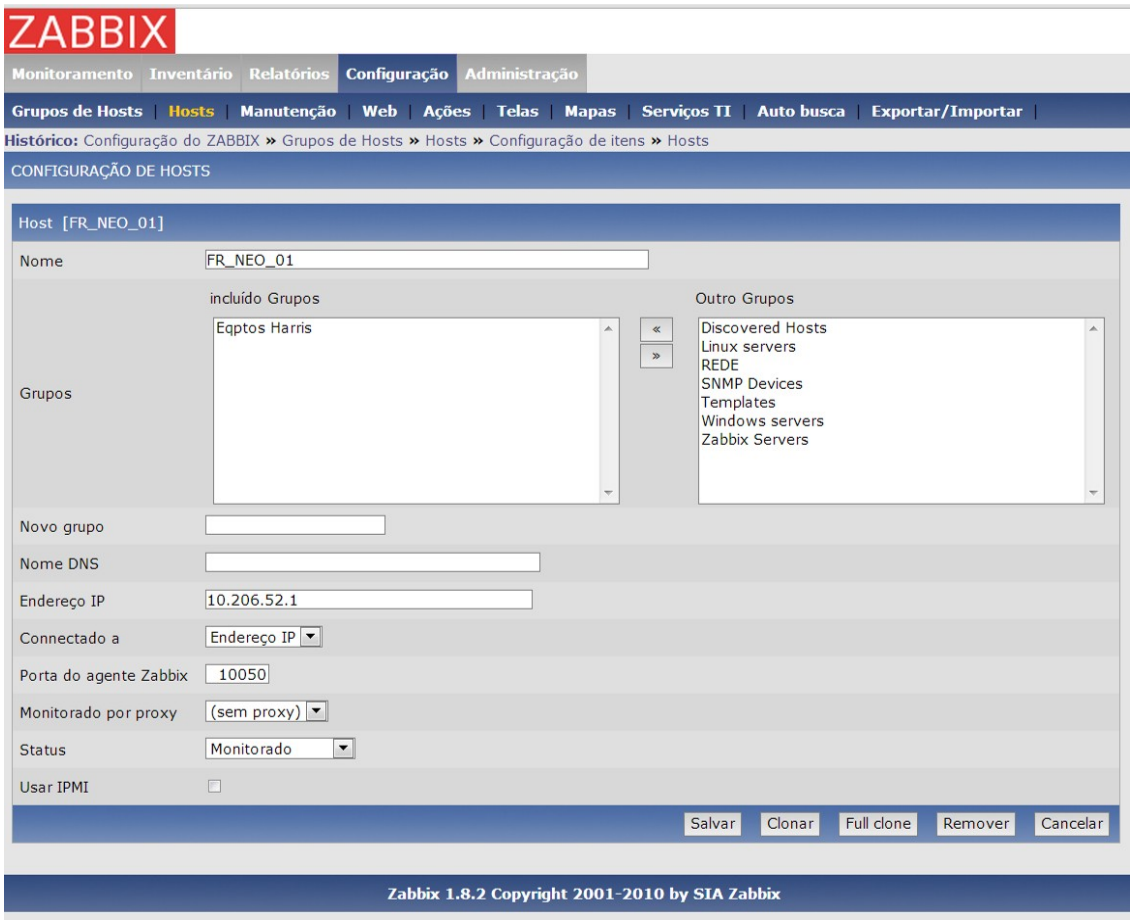



**Figura 6 - Detalhamento da criação do *host* FR_NEO_01**

Para o *host* FR_NEO_01 foram criados os seguintes itens:

- *MKE_Alarm*, do tipo agente SNMP, indica se existe algum alarme;
- *PGM_in_Present*, do tipo agente SNMP, indica a presença de sinal na entrada PGM do dispositivo;
- *REF_in_Present*, do tipo agente SNMP, indica a presença de sinal na entrada REF do dispositivo;
- *Ping Check*, do tipo monitoração simples, indica a presença do dispositivo na rede.

Para cada um destes itens foi criada uma *trigger*, que acusa caso o parâmetro monitorado esteja fora dos padrões pré-estabelecidos. No caso do item *MKE_Alarm*, se o

resultado da leitura SNMP for igual a um, indica que o *frame* está com algum alarme ativo. Para os demais itens (*PGM in present* e *REF in present*), se o resultado da leitura for igual a zero, indica que os sinais nas respectivas entradas não estão presentes. O resultado *Ping Check* igual a zero, indica que o *frame* não está respondendo às solicitações de *ping*.

Na figura 7, estão os itens criados para o *host* FR_NEO_01:

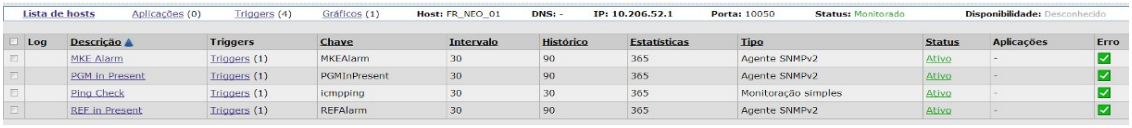



**Figura 7 - Itens do *host* FR_NEO_01**

Na figura 8, estão as *triggers* criadas para o *host* FR_NEO_01:

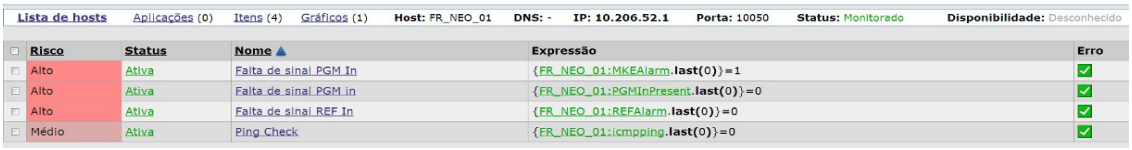



**Figura 8 - *Triggers* do *host* FR_NEO_01**

Para o *host* PROC-2, foram criados os seguintes itens:

- *FanStatus*, do tipo agente SNMP, indica o status da ventilação do sistema;
- *InputStatus*, do tipo agente SNMP, indica a presença de sinal na entrada SDI1 do dispositivo;
- *RefStatus*, do tipo agente SNMP, indica a presença de sinal na entrada REF do dispositivo;
- *Ping Check*, do tipo monitoração simples, indica a presença do dispositivo na rede.

A figura 9, apresenta os itens criados para o *host* PROC-2:


**Figura 9 - Itens do host PROC-2**

A figura 10, apresenta as *triggers* criadas para o *host* PROC-2:

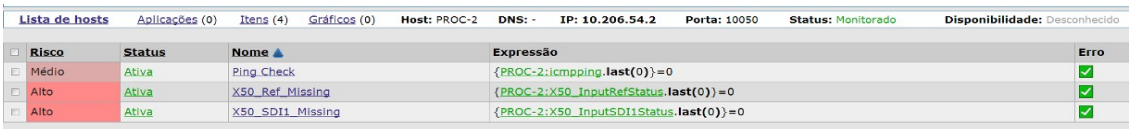
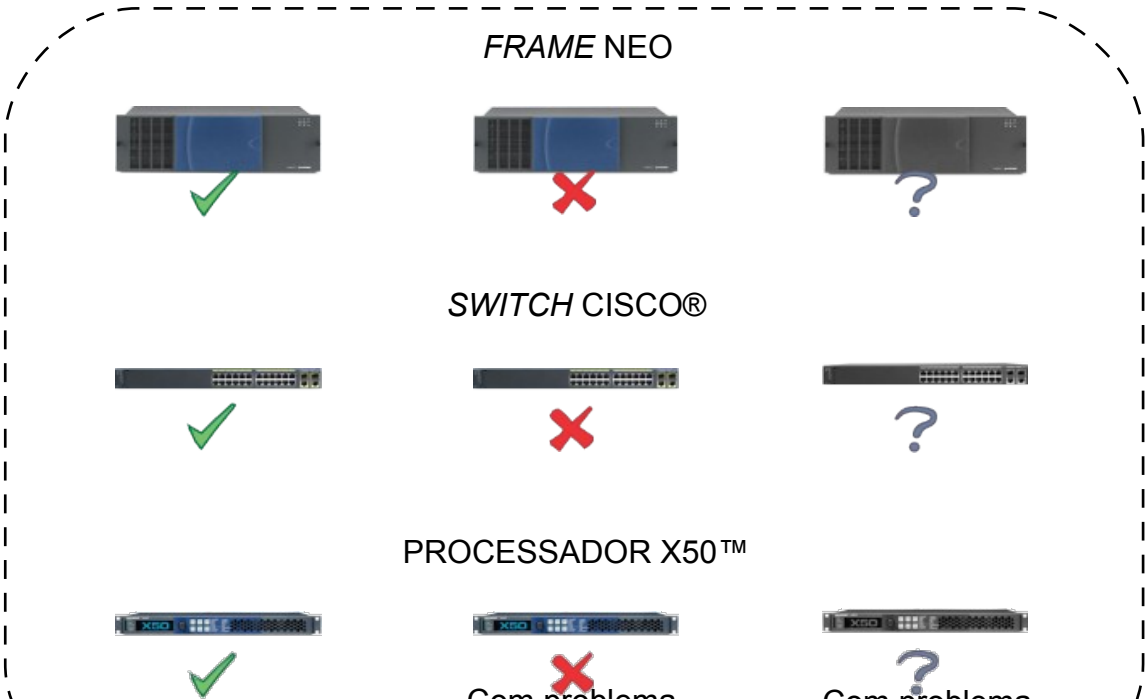



**Figura 10 - *Triggers* do *host* PROC-2**

Para cada *host* implementado no sistema, foram criados três ícones, um indicando que o *host* está normal, outro indicando que o *host* está com problemas e o último indicando que o *host* está com um erro desconhecido, conforme a figura 11:

**Figura 11 - Ícones que representam os *hosts***



Foi elaborado na guia “Mapas” do Zabbix, um mapa com todos os *hosts* escolhidos para o sistema, conforme a figura 12:

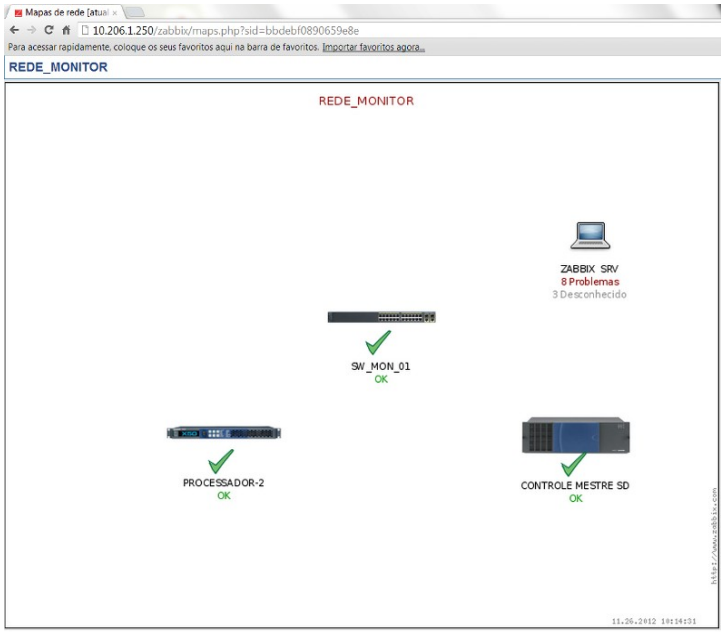



**Figura 12 - Mapa da rede monitorada**

Um teste foi realizado no sistema, retirando um cabo de vídeo da entrada do equipamento PROC-2, gerou um alerta indicado no mapa, conforme a figura 13:

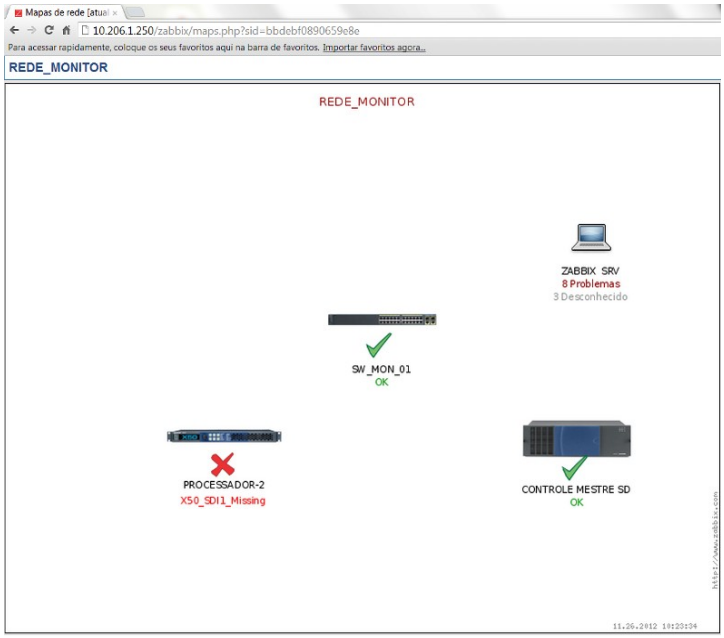



**Figura 13 - Teste retirando cabo SDI do *host* PROC-2**

Outro teste, retirando o cabo de rede do mesmo equipamento resultou na alteração do mapa, mostrada na figura 14:

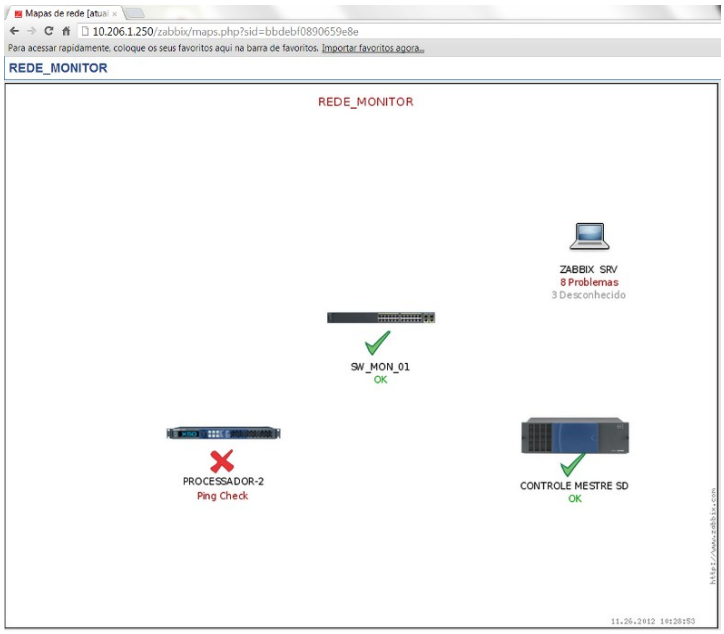



**Figura 14 - Teste retirando cabo de rede do *host* PROC-2**

Na guia "Telas" do Zabbix, foi criada a tela SW_MON_01 com os dados de tráfego de entrada e saída das portas *Gigabit Ethernet 0/1* e *Gigabit Ethernet 0/2* do *switch* de monitoramento, conforme a figura 15:

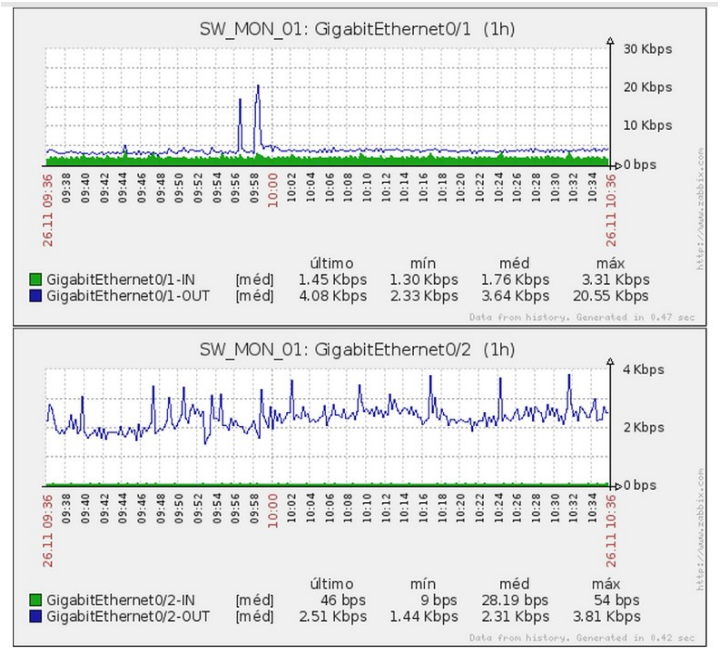



**Figura 15 - Tráfego monitorado das portas Gi0/1 e Gi0/2**

Para todos os itens monitorados, todos os dados requisitados são registrados no banco de dados MySql configurado e podem ser acessado a partir da guia "Dados recentes", mostrada na figura 16:

| | | | | | |
|---|---|---|---|---|---|
| FR_NEO_01 | - **outro** - (4 Itens) | | | | |
| | MKE Alarm | 26 Nov 10:52:04 | 0 | - | Gráfico |
| | PGM in Present | 26 Nov 10:52:31 | 1 | - | Gráfico |
| | Ping Check | 26 Nov 10:52:17 | 1 | - | Gráfico |
| | REF in Present | 26 Nov 10:52:32 | 1 | - | Gráfico |
| PROC-2 | - **outro** - (4 Itens) | | | | |
| | FanStatus | 26 Nov 10:52:08 | No failures | - | Histórico |
| | InputStatus | 26 Nov 10:52:10 | 14 | - | Gráfico |
| | Ping Check | 26 Nov 10:52:09 | 1 | - | Gráfico |
| | RefStatus | 26 Nov 10:52:11 | 16 | - | Gráfico |
| SW_MON_01 | - **outro** - (54 Itens) | | | | |
| | FastEthernet0/1-IN | 26 Nov 10:52:24 | 121 bps | +4 bps | Gráfico |
| | FastEthernet0/1-OUT | 26 Nov 10:52:20 | 2.04 Kbps | -346 bps | Gráfico |
| | FastEthernet0/10-IN | 26 Nov 10:52:18 | 4 bps | - | Gráfico |
| | FastEthernet0/10-OUT | 26 Nov 10:52:29 | 2 Kbps | +90 bps | Gráfico |
| | FastEthernet0/11-IN | 26 Nov 10:52:19 | 0 bps | - | Gráfico |
| | FastEthernet0/11-OUT | 26 Nov 10:52:30 | 1.94 Kbps | +68 bps | Gráfico |
| | FastEthernet0/12-IN | 26 Nov 10:52:20 | 10 bps | +10 bps | Gráfico |
| | FastEthernet0/12-OUT | 26 Nov 10:52:31 | 2.08 Kbps | +106 bps | Gráfico |
| | FastEthernet0/13-IN | 26 Nov 10:52:21 | 10 bps | -23 bps | Gráfico |
| | FastEthernet0/13-OUT | 26 Nov 10:52:32 | 2.04 Kbps | +74 bps | Gráfico |
| | FastEthernet0/14-IN | 26 Nov 10:52:22 | 0 bps | - | Gráfico |
| | FastEthernet0/14-OUT | 26 Nov 10:52:18 | 0 bps | - | Gráfico |
| | FastEthernet0/15-IN | 26 Nov 10:52:23 | 497 bps | -28 bps | Gráfico |

**Figura 16 - Informações da guia "Dados recentes"**

A partir desta mesma guia, podem ser gerados gráficos escolhendo-se o item desejado. A figura 17 mostra um gráfico gerado com os dados registrados no período de uma hora para o item *InputStatus*, do *host* PROC-2. É possível observar a interrupção provocada intencionalmente para teste do sistema:

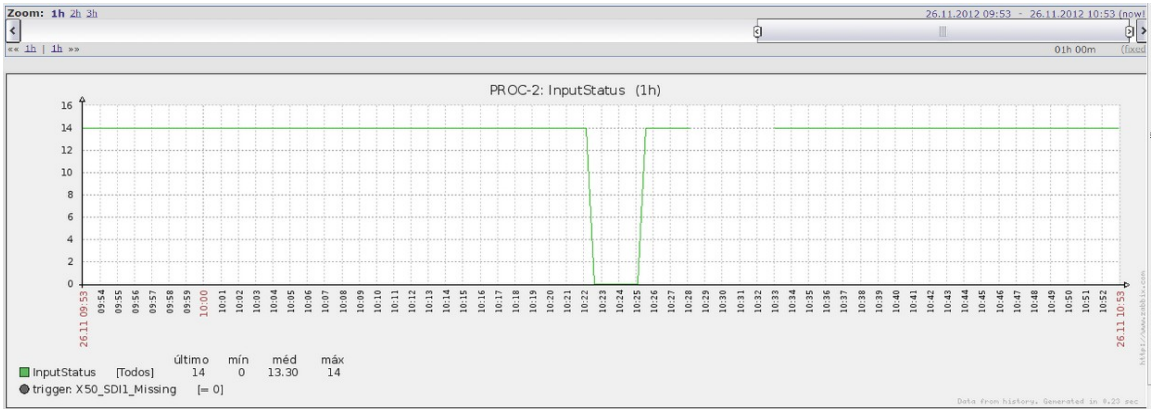



**Figura 17 - Gráfico do item *InputStatus* do *host* PROC-2**

A partir desta mesma guia, podem ser gerados gráficos escolhendo-se o item desejado. A figura 17 mostra um gráfico gerado com os dados registrados no período de uma hora para o item *InputStatus*, do *host* PROC-2. É possível observar a interrupção provocada intencionalmente para teste do sistema:

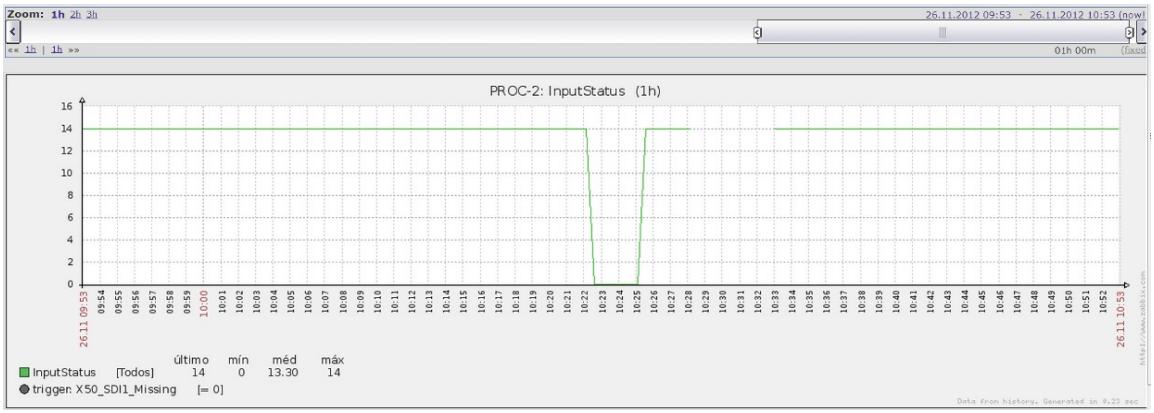



**Figura 17 - Gráfico do item *InputStatus* do *host* PROC-2**

No caso dos itens criados no formato texto, como é o caso do item *FanStatus* do *host* PROC-2, é possível visualizar um histórico dos registros das leituras realizadas, como é possível observar na figura 18:

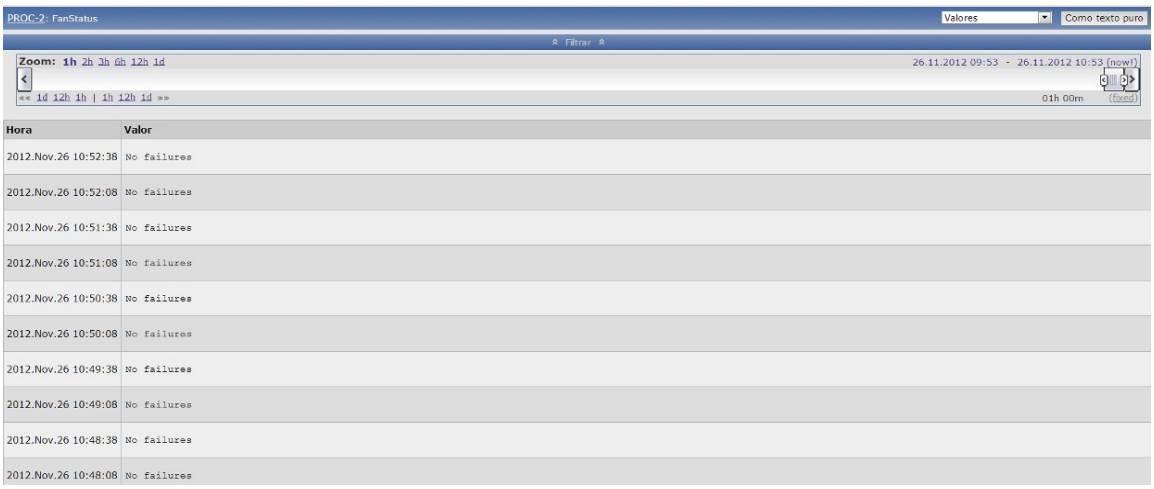



**Figura 18 - Histórico do item *FanStatus* do *host* PROC-2**

As alterações de itens que causaram ativações das *triggers*, podem ser visualizadas na guia "*Triggers*", onde é possível observar também a data da última alteração, a idade e nível de risco da *trigger* ativada. É possível "Vistar" a *trigger*, preenchendo com informações relevantes à solução do problema. A figura 19 mostra os dados da guia "*Triggers*":

| Risco | Status | Última alteração | Idade | Visto | Host | Nome | Comentários |
|---|---|---|---|---|---|---|---|
| Alto | OK | 03 Dec 11:44:10 | 6m 38s | Vistar (1) | PROC-2 | X50_SDI1_Missing | Mostrar |
| Informação | OK | 03 Dec 11:38:01 | 12m 47s | Vistar (10) | Zabbix Server | Zabbix Server has just been restarted | Adicionar |
| Informação | OK | 03 Dec 11:38:00 | 12m 48s | Visto | Zabbix Server | Host information was changed on Zabbix Server | Adicionar |
| Informação | OK | 03 Dec 11:37:55 | 12m 53s | Visto | Zabbix Server | Hostname was changed on Zabbix Server | Adicionar |
| Informação | OK | 03 Dec 11:37:19 | 13m 29s | Visto | Zabbix Server | Configured max number of processes is too low on Zabbix Server | Adicionar |
| Informação | OK | 03 Dec 11:37:18 | 13m 30s | Visto | Zabbix Server | Configured max number of opened files is too low on Zabbix Server | Adicionar |
| Médio | OK | 03 Dec 11:37:16 | 13m 32s | Visto | Zabbix Server | Version of zabbix_agent(d) was changed on Zabbix Server | Adicionar |
| Alto | OK | 03 Dec 11:30:41 | 20m 7s | Visto | PROC-2 | X50_Ref_Missing | Mostrar |
| Alto | OK | 03 Dec 11:30:32 | 20m 16s | Visto | FR_NEO_01 | Falta de sinal REF In | Adicionar |
| Alto | OK | 03 Dec 11:30:31 | 20m 17s | Visto | FR_NEO_01 | Falta de sinal PGM in | Adicionar |
| Advertência | OK | 03 Dec 11:28:08 | 22m 40s | Visto | Zabbix Server | /vmlinuz has been changed on server Zabbix Server | Adicionar |
| Médio | OK | 03 Dec 11:28:06 | 22m 42s | Visto | Zabbix Server | /usr/bin/ssh has been changed on server Zabbix Server | Adicionar |
| Médio | OK | 03 Dec 11:28:05 | 22m 43s | Visto | Zabbix Server | /etc/services has been changed on server Zabbix Server | Adicionar |
| Médio | OK | 03 Dec 11:28:04 | 22m 44s | Visto | Zabbix Server | /etc/passwd has been changed on server Zabbix Server | Adicionar |
| Médio | OK | 03 Dec 11:27:02 | 23m 46s | Visto | Zabbix Server | Too many users connected on server Zabbix Server | Adicionar |
| Alto | OK | 03 Dec 11:26:49 | 23m 59s | Visto | Zabbix Server | Low free disk space on Zabbix Server volume /var | Adicionar |

**Figura 19 - Informações da guia "*Triggers*"**

# 5 CONCLUSÃO

O Zabbix demonstra-se uma ferramenta bastante versátil para monitoramento de equipamentos devido à possibilidade de utilizar seu próprio agente (no caso de monitoramento de servidores) e o agente do próprio equipamento (no caso de monitoramento SNMP).

Na rede estudada foram utilizados apenas alguns equipamentos que compõem a cadeia de transmissão de televisão. Ainda existem diversos equipamentos que possuem suporte ao SNMP e podem ser monitorados através do mesmo sistema, como por exemplo, os transmissores da TV Digital e os servidores integrantes do sistema de edição.

O próximo passo é a implementação do sistema em toda a Central Técnica, com a finalidade de garantir um ambiente totalmente monitorado e agilidade em detectar e resolver os diversos problemas possíveis. Para isso faz-se necessário o investimento em um servidor que atenda os requisitos mínimos de *hardware* para a quantidade de equipamentos a serem monitorados.

# REFERÊNCIAS

MAURO, D. R.; SCHIMIDT, K. J. **SNMP Essencial**. Rio de Janeiro: Campus, 2001.

OLUPS, RIHARDS. Zabbix **1.8 Network Monitoring**. Birmingham: Packt Publishing, 2010.

SNMP Research International, Inc. Disponível em: <**http://www.snmp.com**>. Acesso em: 1 jun. 2012.

VLADISHEV, A. Manual online do Zabbix. Disponível em: <**http://www.zabbix.com/documentation/start**>. Acesso em: 1 jun. 2012.