CENTRO UNIVERSITÁRIO DE BRASÍLIA - UniCEUB

CURSO DE ENGENHARIA DE COMPUTAÇÃO

DANIEL PAULA PESSÔA CÉLESTIN

CUSTOMIZAÇÃO DO MONITORAMENTO DE LINKS E REDES

Orientador: Prof. MsC. Francisco Javier De Obaldía Díaz

Brasília

dezembro, 2013

DANIEL PAULA PESSÔA CÉLESTIN

CUSTOMIZAÇÃO DO MONITORAMENTO DE LINKS E REDES

Trabalho apresentado ao Centro Universitário de Brasília (UniCEUB) como pré-requisito para a obtenção de Certificado de Conclusão de Curso de Engenharia de Computação.

Orientador: **Prof. MsC. Francisco Javier De Obaldía Díaz**

Brasília

dezembro, 2013

DANIEL PAULA PESSÔA CÉLESTIN

CUSTOMIZAÇÃO DO MONITORAMENTO DE LINKS E REDES

Trabalho apresentado ao Centro Universitário de Brasília (UniCEUB) como pré-requisito para a obtenção de Certificado de Conclusão de Curso de Engenharia de Computação.

Orientador: **Prof. MsC. Francisco Javier De Obaldía Díaz**

Este Trabalho foi julgado adequado para a obtenção do Título de Engenheiro de Computação, e aprovado em sua forma final pela Faculdade de Tecnologia e Ciências Sociais Aplicadas FATECS.

_____
Prof. Abiezer Amarília Fernandes
Coordenador do Curso

Banca Examinadora:

_____
Prof. MsC. Francisco Javier De Obaldía Díaz, Mestre
Orientador

_____
Prof. nome, titulação.
Instituição

_____
Prof. nome, titulação.
Instituição

_____
Prof. nome, titulação.
Instituição

AGRADECIMENTOS

Agradeço primeiramente a Deus, por estar sempre me guiando, e agora estar dando condições de finalizar este curso.

Agradeço a meus pais, Gilberto e Ana, por sempre me apoiarem em todos os momentos da vida, que sempre estiveram ao meu lado com todo amor, carinho e apoio.

Agradeço à família maravilhosa que tenho, meu irmão, meus tios e meus avós, que juntos me apoiaram em momentos difíceis com muita dedicação, amor e carinho.

Agradeço a todos os meus amigos que me apoiaram e me ajudaram, não apenas nesse projeto, mais em todas as dificuldades já passadas. Em especial, agradeço ao Fernando Lopes, à Suzana Romão, ao Rodrigo Queiroz, e à Wanessa Bastos.

Agradeço à instituição UniCEUB, ao João Batista do setor administrativo, e a todos os professores do curso de Engenharia da Computação, que com muita dedicação me mostraram o melhor caminho a seguir. Em especial, agradeço aos professores Abiezer Fernandes, Eliomar Lima, Fabiano Oliveira, Francisco Diaz, Layany Damázio, Luciano Duque, Luiz Claudio, Marco Araújo, Maria Farias e Thiago Toribio, que ao longo do curso, além de professores, se tornaram amigos, e me ajudaram a chegar ao ponto em que estou, próximo a me tornar um de seus colegas de profissão.

A todos, muito obrigado.

SUMÁRIO

LISTA DE FIGURAS **8**

LISTA DE TABELAS **11**

LISTA DE SIGLAS E SÍMBOLOS **12**

CAPÍTULO Nº 1 – INTRODUÇÃO **16**

1.1 - Motivação **16**

1.2 - Objetivo do Trabalho **17**

1.3 - Justificativa e Importância do Trabalho **18**

1.4 - Escopo do Trabalho **18**

1.4.1 - Trabalho a ser desenvolvido e implementado **18**

1.4.2 - Processo a ser utilizado **19**

1.4.3 – Recursos que serão utilizados **19**

1.4.4 – Fronteiras do trabalho **22**

1.5 - Resultados Esperados **23**

CAPÍTULO Nº 2 – APRESENTAÇÃO DO PROBLEMA **25**

2.1 – A Evolução Tecnológica e o Monitoramento de Redes **25**

2.2 – A Complexidade das Redes de Computadores **26**

2.3 - Monitoramento de redes **28**

CAPÍTULO Nº 3 - REFERENCIAL TEÓRICO **29**

3.1 – GNU/Linux **29**

3.2 - CentOS **30**

3.3 – Componentes do Monitoramento de Rede de computadores **31**

3.3.1 - Monitoramento de dispositivos de rede **31**

3.3.2 - Monitoramento de rede, serviços e servidores **32**

3.3.3 – Tecnologias utilizadas em redes **32**

3.3.4 - Ativos e serviços de redes **33**

3.3.5 - Nagios **37**

3.3.6 – Centreon **38**

3.3.7 - Zabbix **39**

3.4 - Links de Dados e Comunicação 41

3.5 - Novas Tecnologias de Servidores 41

3.5.1 – Servidor de dados Dropbox 41

3.5.2 – Servidor de voz Vono (GVT) 41

3.5.3 – Servidores *WEB* 42

3.6 – SNMP (*Simple Network Management Protocol*) 42

3.7 – FAN (*Fully Automated Nagios*) 45

3.8 - NAT 46

3.9 – NO-IP 47

CAPÍTULO Nº 4 – DESENVOLVIMENTO DO PROJETO DE CUSTOMIZAÇÃO DE MONITORAMENTO DE LINKS E REDES 48

4.1 - Visão Geral do Projeto 48

4.2 - Etapas do Projeto 52

4.3 - Implementação do Projeto 53

4.3.1 - Instalação e configuração dos principais recursos deste trabalho 53

4.3.1.1 – Configuração do modem GVT, e habilitação da DMZ 54

4.3.1.2 – Configuração do roteador RB750GL e das NATs 56

4.3.1.3 - Instalação do sistema operacional CentOS e da ferramenta Centreon 63

4.3.1.4 - Instalação da ferramenta Zabbix no servidor. 77

4.3.1.5 - Configurando o SNMP no Windows 2008 server 87

4.4 - Considerações Finais. 88

CAPÍTULO Nº 5 – TESTES E RESULTADOS 89

5.1 - Telas que Sintetizam o Universo Monitorado 89

5.1.1 – Tela síntese do Zabbix 90

5.1.2 – Tela síntese do Centreon 90

5.2 – Gráficos de Rede 91

5.2.1 – Gráficos de rede do equipamento AM-Filial01. 92

5.2.2 – Gráficos de rede do equipamento AM-Filial02. 93

5.2.3– Gráficos de rede do equipamento AM-Filial03. 94

5.2.4– Gráficos de rede do equipamento AM-Filial04. 95

5.2.5– Gráficos de rede do equipamento Multi. 96

5.2.6– Gráficos de rede do equipamento RB750GL. 97

5.2.7– Gráficos de rede do equipamento Celestin. 98

5.2.8– Gráficos de rede do equipamento Ultrabook. 100

5.3 – Testes Realizados 101

5.3.1 – Transferência de arquivo do servidor Celestin para AM-Filial04. 101

5.3.2 – Transferência de arquivo de AM-Filial04 para AM-Filial02 102

5.3.3 – Download e upload do servidor Celestin para o servidor Dropbox. 103

5.3.4 – Download de vídeo do Youtube para o servidor Celestin. 105

5.3.5 – Download e upload da estação Ultrabook para o servidor Vono - Zabbix 106

5.3.6 – Transferência de Arquivos entre máquinas da LAN passando pelo RB750GL. 107

5.3.7 – Transferência de Arquivos para AM-Filial01 no limite de seu link. 108

5.4 – Alertas do monitoramento 109

5.4.1 – Alerta sobre links interrompidos através da tela. 109

5.4.2 – Alerta sobre links interrompidos através de email. 111

5.5 – Dificuldades Encontradas 112

5.6 - Custo da Solução de Monitoramento 113

5.7 - Características das Ferramentas 114

5.7.1 – Características do Zabbix 114

5.7.2 – Características do Centreon 115

5.7.3 – Comparativos entre as duas ferramentas. 115

5.8 – Análise dos Resultados 116

5.9 - Considerações finais 117

CAPÍTULO Nº 6 – CONCLUSÕES E TRABALHOS FUTUROS 118

6.1 - Conclusões 118

6.2 - Sugestões de Trabalhos Futuros 119

REFERÊNCIAS 120

ANEXO A – INSTRUÇÕES E COMANDOS PARA INSTALAÇÃO DO ZABBIX 121

ANEXO B – INSTRUÇÕES E COMANDOS PARA INSTALAÇÃO DO NO-IP 128

LISTA DE FIGURAS

Figura 1.1 - Recursos e interligações a serem implementados. 20
Figura 2.1 – Uma rede elementar onde pontos são interligados por linhas 26
Figura 2.2 – Representação simplificada da rede Internet 26
Figura 2.3 - Por meio de uma conexão, um ponto isolado pode se conectar à rede 27
Figura 3.1 – Representação de um servidor FTP 33
Figura 3.2 – Representação de conexões Cliente-Servidor 34
Figura 3.3 – Representação de um servidor de DNS 34
Figura 3.4 – Representação de um servidor de arquivos 35
Figura 3.5 – Representação de um servidor proxy. 35
Figura 3.6 – Roteador RB750GL 36
Figura 3.7 – Switch CISCO 2950-24 37
Figura 3.8 - Arquitetura de uma rede gerenciada por meio de SNMP 43
Figura 4.1 – Cenário elaborado para o projeto 49
Figura 4.2 – Resultado do comando ipconfig mostrando o IP do modem GVT 54
Figura 4.3 – Tela de login do endereço 192.168.25.1 54
Figura 4.4 – Tela de configuração do modem GVT 55
Figura 4.5 - Tela de configuração e habilitação da DMZ do modem GVT 55
Figura 4.6 – Área de trabalho com o ícone do winbox 56
Figura 4.7 – Tela de login no winbox 57
Figura 4.8 – Tela de configuração de NAT entrada – aba general 57
Figura 4.9 - Tela de configuração de NAT – aba Action. 58
Figura 4.10 - Tela de configuração de NAT saída – aba general 59
Figura 4.11 - Tela de configuração de NAT saída – aba Action. 59
Figura 4.12 – Resultado do comando ipconfig em um servidor monitorado. 60
Figura 4.13 – Tela de login para configuração de modem de um servidor monitorado 61
Figura 4.14 – Tela inicial de configuração do modem D-Link 61
Figura 4.15 – Tela de configuração do modem D-Link 62
Figura 4.16 - Tela para definição do modo de instalação do FAN. 63
Figura 4.17 – Escolha da linguagem a ser FAN 64
Figura 4.18 – Solicitação do tipo de teclado a ser utilizado pelo FAN 64
Figura 4.19 – Solicitação de dados para a partição pelo FAN 65

Figura 4.20 – Solicitação de região e fuso horário pelo FAN 65
Figura 4.21 – Fornecimento de senha de administrador para o FAN 66
Figura 4.22 – Informação de instalação bem sucedida do FAN 67
Figura 4.23 – Tela de seleção Setup Agent do FAN 67
Figura 4.24 – Tela Select Action do FAN 68
Figura 4.25 – Tela Select A Device do FAN 68
Figura 4.26 – Tela Devernet Configuration do FAN 69
Figura 4.27 – DNS configuration do FAN 69
Figura 4.28 – Tela de console do FAN 70
Figura 4.29 – Informações apresentadas pelo comando ifconfig 70
Figura 4.30 – Console do FAN 71
Figura 4.31 – Tela inicial do Centreon para configuração de hosts e serviços 71
Figura 4.32 – Página resumo de hosts do Centreon 72
Figura 4.33 – Tela de configuração de host da AM-Filial01 72
Figura 4.34 – Tela de configuração de serviços – Cheks 74
Figura 4.35 – Tela de configuração de serviços – Modificação de comando 74
Figura 4.36 – Tela de exportação de configuração do Centreon 75
Figura 4.37 – Informações da comunidade monitorada para o SNMP - Centreon. 76
Figura 4.39 - Configuração dos hosts do Zabbix 77
Figura 4.40 – Pup-up para escolha de template no Zabbix 78
Figura 4.41 – Tela inicial de mapas do Zabbix 79
Figura 4.42 – Configuração de formato da tela no Zabbix 80
Figura 4.43 – Tela de configuração dos hosts no mapa de rede do Zabbix 81
Figura 4.44 – Mapa da rede a ser monitorado pelo Zabbix 82
Figura 4.45 – Tela inicial de configuração de telas do Zabbix 82
Figura 4.46 – Tela de configuração de telas do Zabbix. 83
Figura 4.47 – Tela de um gráfico criado no Zabbix 84
Figura 4.48 – Informações da comunidade monitorada para o SNMP - Zabbix. 85
Figura 4.49 – Visão geral dos gráficos e hosts monitorados no Zabbix. 85
Figura 4.50 – Console de monitoramento do Zabbix 86
Figura 4.51 – Propriedades de Serviço SNMP (Computador local) – Agente 87
Figura 4.52 - Propriedades de Serviço SNMP (Computador local) – Segurança 88
Figura 5.1 – Tela síntese do Zabbix 90
Figura 5.2 – Tela síntese do Centreon 91

Figura 5.3 - Gráfico de rede do AM-Filial01 mostrado pelo Zabbix 92
Figura 5.4 - Gráfico de rede do AM-Filial01 mostrado pelo Centreon.....93
Figura 5.5 - Gráfico de rede do AM-Filial02 mostrado pelo Zabbix 93
Figura 5.6 - Gráfico de rede do AM-Filial02 mostrado pelo Centreon.....94
Figura 5.7 - Gráfico de rede do AM-Filial03 mostrado pelo Zabbix 94
Figura 5.8 - Gráfico de rede do AM-Filial03 mostrado pelo Centreon.....95
Figura 5.9 - Gráfico de rede do AM-Filial04 mostrado pelo Zabbix 96
Figura 5.10 - Gráfico de rede do AM-Filial04 mostrado pelo Centreon 96
Figura 5.11 - Gráfico de rede do Multi mostrado pelo Zabbix 97
Figura 5.12 - Gráfico de rede do Multi mostrado pelo Centreon 97
Figura 5.13 - Gráfico de rede do RB750GL mostrado pelo Zabbix 98
Figura 5.14 -Gráfico de rede do RB750GL - Centreon 98
Figura 5.15 - Gráfico de rede do Celestin - Zabbix 99
Figura 5.16 - Gráfico de rede do Celestin mostrado pelo Centreon 99
Figura 5.17 - Gráfico de rede do Ultrabook mostrado pelo Zabbix 100
Figura 5.18 - Gráfico de rede do Ultrabook mostrado pelo Centreon 100
Figura 5.19 - Gráfico do tráfego entre Celestin e AM-Filial04 – Zabbix 102
Figura 5.20 - Gráfico do tráfego entre Celestin e AM-Filial04 – Centreon 102
Figura 5.21 - Gráfico do tráfego da AM-Filial04 p/ AM-Filial02 – Zabbix 103
Figura 5.22 - Gráfico do tráfego da AM-Filial04 para AM-Filial02 – Centreon 103
Figura 5.23 - Gráfico do down/upload de Celestin para Dropbox – Zabbix 104
Figura 5.24 - Gráfico do down/upload de Celestin para Dropbox – Centreon 104
Figura 5.25 - Gráfico do download de vídeo do Youtube – Zabbix 105
Figura 5.26 - Gráfico do download de vídeo do Youtube – Centreon 105
Figura 5.27 - Gráfico de download/upload do Ultrabook para Vono – Zabbix.....106
Figura 5.28 - Gráfico do down/upload de Ultrabook para Vono – Centreon 107
Figura 5.29 - Gráfico de transferência de arquivos pela RB750GL – Zabbix 107
Figura 5.30 - Gráfico de transferência de arquivos pela RB750GL - Centreon 108
Figura 5.31 - Gráfico do limite de tráfego no link da AM-Filial01 – Zabbix 108
Figura 5.32 - Gráfico do limite de tráfego no link da AM-Filial01 – Centreon.....109
Figura 5.33 - Tela do Zabbix com o status do host Ultrabook (15/11/2013).....110
Figura 5.34 - Tela do Centreon com o status do host AM-Filial03 (15/11/2013).....110
Figura 5.35 - Email enviado pelo Zabbix com o status do host Ultrabook (15/11/2013). 111
Figura 5.36 - Email enviado pelo Centreon com o status do host Ultrabook (15/11/2013)...112

LISTA DE TABELAS

Tabela 1 – Especificação do servidor AM–FILIAL01 20
Tabela 2 – Especificação do servidor AM–FILIAL02, AM–FILIAL03 e AM–FILIAL04 20
Tabela 3 – Especificação do servidor de monitoramento 21
Tabela 4 – Especificação do equipamento Celestin 21
Tabela 5 – Especificação do roteador do servidor de monitoramento 21
Tabela 6 – Especificação dos roteadores dos servidores monitorados 21
Tabela 7 – Especificação do roteador do equipamento Multi 21
Tabela 8 – Especificação do equipamento Multi 22
Tabela 9 – Especificação do equipamento Ultrabook 22
Tabela 10 – Endereços das NATs do servidor de monitoramento 58
Tabela 11 – Endereço da NAT para servidor Celestin 58
Tabela 12 – Endereços das NATs dos servidores monitorados 62
Tabela 13 - Endereços dos hosts no Centreon 73
Tabela 14 – Informações para configuração dos hosts no Zabbix. 79
Tabela 15 – Resumo de recursos das ferramentas de monitoramento 115

LISTA DE SIGLAS E SÍMBOLOS

ADSL - Asymmetric Digital Subscriber Line

API - *Application Programming Interface* (interface de programação de aplicativos)

ASP - *Active Server Page*

ATA - Adaptador para Telefone Analógico

CGI - *Common Gateway Interface*

CPU - *Central Processor Uni*t (unidade central de processamento)

DHCP - *Dynamic Host Configuration Protocol* (protocolo de configuração dinâmica de host)

DMZ - DeMilitarized Zone (zona desmilitarizada)

DNS - *Domain Name System* (Sistema de Nomes de Domínios)

DSO - *Dynamic Shared Objects*

DVD – *Digital Versatile Disc* 1 (disco digital versátil 1).

FAN - *Fully Automated Nagios*

FTP - *File Transfer Protocol* (protocolo de transferência de arquivos)

GPL - *General Public License* (licença pública geral)

HTTP - *Hypertext Transfer Protocol* (protocolo de transferência de hipertexto)

ICMP - *Internet Control Message Protocol*

IIS - *Internet Information Services*

IP - *Internet Protocol* (Protocolo de internet)

JDBC - *Java Database Connectivity*

JNDI - *Java Naming and Directory Interface*

JSP - Java *Server Page*

LAN - *Local Area Network*

MAC - *Media Access Control*

MAN - *Metropolitan Area Network* (rede metropolitana)

MD5 - *Message-Digest algorithm* 5

NaReTo - *Nagios Reporting Tool*

NAT - *Network Address Translation* (Tradução de Endereços IP)

NMS - *Network Management System*

PHP - *Personal Home Page*, atualmente conhecido como *Hypertext Preprocessor*

POP - *Post Office Protocol* (protocolo do correio)

QoS - *Quality of Service* (qualidade do serviço)

RDP - *Remote Desktop Protocol*

RDtool - *Round-Robin Database Tool*

SLA - *Service Level Agreement* (acordo de nível de serviço)

SMS - *Short Message Service* (serviço de mensagem curta)

SMTP - *Simple Mail Transfer Protocol* (protocolo de transferência de correio simples)

SNMP - *Simple Network Management Protocol* (protocolo simples de gerência de rede)

SQL - *Structured Query Language* (Linguagem de Consulta Estruturada)

SSH - *Secure SHell*

TCP - *Transmission Control Protocol* (protocolo de controle de transmissão)

TI - Tecnologia da Informação

TIC - Tecnologia da Informação e Comunicação

UDP - *User Datagram Protocol*

URL - *Uniform Resource Locator*

VLAN - *Virtual Local Area Network* ou Virtual LAN (rede local virtual)

VoIP - *Voice over Internet Protocol* (voz sobre IP)

XML - *eXtensible Markup Language*

WAN - *Wide Area Network* (rede de longa distância)

WEB - *World Wide* Web (teia mundial)

RESUMO

Este trabalho apresenta uma implementação de monitoramento de redes que utiliza soluções integradas do sistema operacional CentOS (distribuição Linux de classe Enterprise) com os softwares de monitoramento de rede Centreon e Zabbix, além do uso do protocolo SNMP (*Simple Network Management Protocol*). Será mostrado que o uso destas ferramentas de monitoramento é fundamental para orientar o administrador de uma rede, fornecendo informações gerenciais do tráfego nos links da rede, resultando em um melhor dimensionamento dos recursos, e consequentemente contribuindo para a estabilidade e confiabilidade da rede. Tudo isso, com as vantagens de que tanto este sistema operacional, quanto os softwares de monitoramento são de código aberto e licenças GPL (*General Public License*), que permitem soluções a custos mínimos para o usuário, além de estarem em constante desenvolvimento, e permitirem a adequação as particularidades de uma determinada rede. Para concretização do projeto, foram instalados e configurados o sistema operacional CentOS e as ferramentas de monitoramento Centreon e Zabbix, em um servidor doméstico, que através de um roteador foi conectado em rede com quatro servidores de filiais de uma empresa sediada no Distrito Federal, e um servidor de outra empresa, também localizada no DF. Durante os testes serão acessados também o servidor de dados Dropbox, o servidor de voz Vono, e o servidor de vídeo Youtube. Para avaliação das ferramentas de monitoramento foram provocadas diversas situações de tráfego e problemas na rede, e observadas, registradas, e documentadas as respostas de cada uma das ferramentas. Como resultado, é apresentado um resumo das características de cada software testado, e uma avaliação destas ferramentas.

Palavras Chave:

CentOS, Centreon, Zabbix, SNMP, links, licenças GPL, Dropbox, Vono, Youtube.

ABSTRACT

This paper presents an implementation of network monitoring using integrated solutions using the CentOS (enterprise-class Linux distribution) operating system with software network monitoring Centreon and Zabbix, and the use of SNMP (Simple Network Management Protocol). It will be shown that the use of these monitoring tools are essential to guide the administrator of a network, providing information management of traffic on the network links, resulting in a better dimensioning of resources, and thus contributing to the stability and reliability of the network. All this, with the advantages of both this operating system, as the monitoring software are open source and GPL (General Public License), which allow solutions at minimal cost to the user, are in constant development, and allow the adequacy of the particularities of a given network. To carry out the project, have been installed and configured the CentOS operating system and monitoring tools Centreon and Zabbix on a home server, that through a router was networked with four servers of subsidiaries of a company based in the Federal District, and a server from another company, also located in the DF. During the test will be also accessed the data server Dropbox, the voice server Vono, and video server Youtube. To evaluate the monitoring tools were caused several traffic situations and problems in the network, and observed, recorded, and documented the responses of each of the tools. As a result, a summary of the characteristics of each tested software, and an evaluation of these tools.

CAPÍTULO Nº 1 – INTRODUÇÃO

1.1 - Motivação

O crescimento cada vez maior da necessidade do uso das redes de computadores obriga as instituições a terem a sua própria rede, além de terem a necessidade de acessar outras redes externas, como é o caso da principal delas, que é a internet.

A dependência da estabilidade destas redes hoje é tão grande, que nos sentimos impotentes quando, por exemplo, há falhas em uma rede do sistema bancário, e não conseguimos realizar uma simples operação de pagamento de um boleto.

É cada vez mais urgente dotar as instituições de ferramentas que auxiliem no monitoramento destas redes, de forma a avisar sobre problemas surgidos ou na eminência de ocorrerem, informar permanentemente sobre o desempenho do tráfego na rede, e fatores que contribuam para a paralização do serviço, ou a baixo desempenho de todo o sistema.

Neste último cenário, procurou-se estudar um conjunto de softwares de código aberto, distribuídos gratuitamente através de licenças GPL, utilizando recursos de ativos configuráveis de baixo custo, de forma a demonstrar que é possível monitorar redes WAN (*Wide Area Network*), com soluções práticas e com custo mínimo.

A motivação deste trabalho é demostrar a possibilidade de realizar monitoramento em tempo real de *links* de comunicação, com o uso de ferramentas gratuitas, e de tecnologias modernas e baratas de ativos de rede. O desafio é demostrar dois *softwares* de monitoramento instalados em um único servidor, acionados independentemente, porém monitorando simultaneamente a rede, conseguindo assim ter como resultante as características de cada ferramenta, e as vantagens e desvantagem de cada uma.

Neste trabalho será utilizado o sistema operacional CentOS, que é uma das distribuições Linux que vem sendo bastante utilizada na atualidade, e estudadas as ferramentas de monitoramento Zabbix e Centreon, consideradas atualmente como as grandes aliadas das instituições no monitoramento de redes.

Para este estudo, além dos softwares citados, foi criado um ambiente de rede WAN, utilizando o roteador configurável RB750GL, e outros recursos necessários para os testes.

Pretende-se que este trabalho, assim como as soluções de monitoramento estudadas, sejam divulgados, e sirvam de base para que instituições que ainda não dispõem destas ferramentas, implementem uma dessas soluções, que auxiliarão no diagnósticos de erros, resolução de problemas e detecção de gargalos, contribuindo para a excelência de uma rede.

1.2 - Objetivo do Trabalho

Este trabalho tem como objetivo principal o estudo de soluções de monitoramento de uma rede WAN, que permitam visualizar e analisar de forma integrada o tráfego de dados, voz e vídeo, utilizando o sistema operacional CentOS, e as ferramentas de monitoramento Centreon e Zabbix.

Como objetivos específicos relacionam-se:

. Estudar, instalar e configurar o sistema operacional CentOS, as ferramentas de monitoramento Centreon, e Zabbix, e demais recursos necessários;

. Documentar passo a passo como proceder a instalação e as configurações necessárias, para a implementação dos softwares;

. Estudar e analisar o comportamento das ferramentas de monitoramento utilizadas como apoio à solução apresentada neste trabalho, acompanhando o funcionamento de uma rede WAN;

. Estudar, instalar e configurar os equipamentos e os demais ativos utilizados na rede WAN montada para este projeto;

. Monitorar o estado dos recursos e ativos de rede, e o comportamento do tráfego nesta rede.

. Apresentar os resultados do estudo e as principais características das ferramentas Centreon e Zabbix, como soluções de monitoramento de links de uma rede WAN.

1.3 - Justificativa e Importância do Trabalho

Atualmente, as empresas necessitam aplicar técnicas de monitoramento em suas redes. O presente trabalho poderá ser usado como base para a mudança da mentalidade dos administradores de instituições, que ainda não perceberam que estas soluções de monitoramento devem ser adotadas de forma imediata.

Na solução elaborada, serão apresentados gráficos de medição de desempenho dos links da rede gerados pelas ferramentas. Serão apresentados os sistemas de monitoramento Centreon e Zabbix, que ainda não são aplicados e difundidos na maioria das empresas. São poucas as que se preocupam com a necessidade do monitoramento dos links de comunicação.

O conhecimento destas ferramentas de monitoramento é de suma importância não só para os profissionais de redes e de infraestrutura, como também para estudantes e pesquisadores. O domínio destas tecnologias servirá de alicerce para a implementação de soluções ajustadas a cada problema apresentado.

1.4 - Escopo do Trabalho

1.4.1 - Trabalho a ser desenvolvido e implementado

O foco é demostrar que, utilizando um conjunto de técnicas adequadas de monitoramento, é possível haver o funcionamento eficiente e sem interrupção da rede. O modelo a ser apresentado demonstrará que é possível adotar soluções baratas utilizando softwares de distribuição gratuita, de código aberto.

Serão implementadas e apresentadas soluções de monitoramento de redes utilizando o sistema operacional CentOS, as ferramentas de Monitoramento Zabbix e Centreon, o protocolo SNMP e o redirecionamento de portas, com o uso do roteador RB750GL.

1.4.2 - Processo a ser utilizado

Será especificada solução envolvendo as ferramentas de monitoramento e o sistema operacional CentOS e como estarão integradas. Será exposto como podem ser usadas essas ferramentas, individualmente e de forma integrada. Para tanto, serão realizadas simulações do funcionamento de um link de comunicação, passando pelo servidor de monitoramento, feito individualmente pelo Zabbix e pelo Centreon através de técnicas de redirecionamento de portas, IP fixo, NO-IP e roteadores, montando assim uma rede WAN. Nesta rede serão trafegados em tempo real, dados, voz e vídeo, através do roteador RB750GL, e monitorados também os servidores localizados externamente.

1.4.3 – Recursos que serão utilizados

A figura 1.1 dá uma visão geral da rede a ser implantada e o ambiente do projeto, que é composto por uma WAN Fast Ethernet que possui:

. Uma central de monitoramento (residência), com uma LAN que tem 1 Servidor de Monitoramento - celestin.no-ip.info, 1 servidor - Celestin (agente monitorado), 1 Ultrabook (agente monitorado), 1 Roteador RB750GL, 1 Link ADSL.

. AM-Filial (01/02/03/04) (localizados em vários pontos do DF)
4 Servidores (agentes monitorados) e 4 modens.

. Servidor Multi (localizado no DF).
1 Servidor (agente monitorado) e 1 modem

Foi implementado um servidor de monitoramento de rede com as seguintes ferramentas: um gerente Zabbix, e um gerente Centreon. Foram também instalados sete agentes Zabbix para Windows, nos equipamentos a serem monitorados e configurados sete SNMP no Windows para uso do Centreon . Além de equipamentos de rede como o roteador RB750GL, cinco roteadores de várias operadoras e redirecionamento de portas usando NAT.

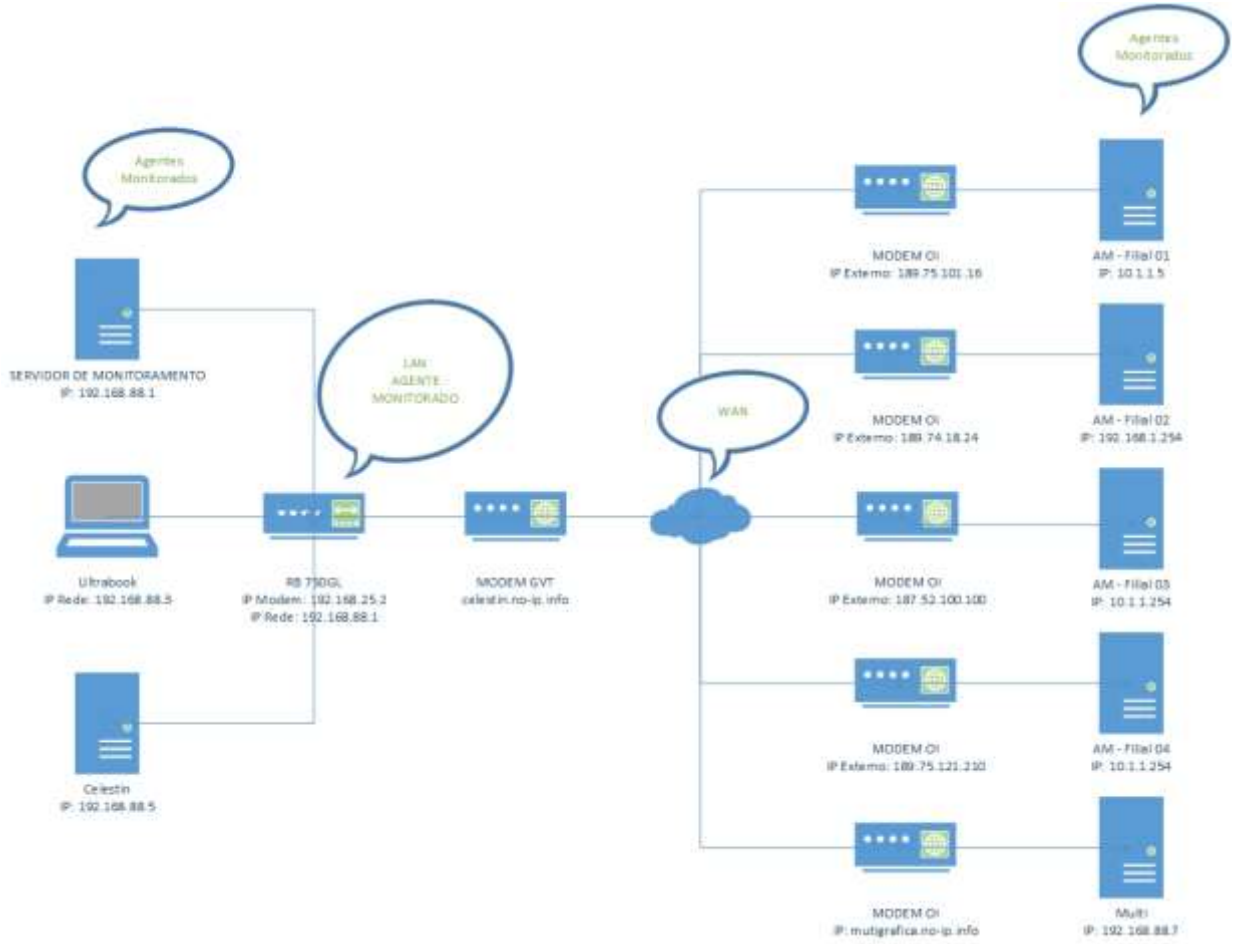

Figura 1.1 - Recursos e interligações a serem implementados. (Autor do Projeto, 2013)

As especificações de cada equipamento da rede são apresentadas nas tabelas a seguir:

Tabela 1 – Especificação do servidor AM–FILIAL01

Equipamento	Servidor
Nome/Modelo	HP Proliant Gen 8 ML350
Processador	Intel® Xeon® CPU E5-2420 0 @ 1.90 GHZ
HD	500 GB
Memória RAM	4 GB
Wi-Fi	Não
Placa de Rede	10/100/1000 Mbps

Tabela 2 – Especificação do servidor AM–FILIAL02, AM–FILIAL03 e AM–FILIAL04

Equipamento	Servidor
Nome/Modelo	IBM X3100 M4
Processador	Xeon E3 1220v2 3.1 GHZ

HD	500 GB
Memória RAM	4 GB
Wi-Fi	Não
Placa de Rede	10/100/1000 Mbps

Tabela 3 – Especificação do servidor de monitoramento

Equipamento	Servidor
Nome/Modelo	Servidor Montado – Soyo
Processador	Processador AMD 2500+
HD	80 GB
Memória RAM	3 GB
Wi-Fi	Não
Placa de Rede	10/100 Mbps

Tabela 4 – Especificação do equipamento Celestin

Equipamento	Servidor
Nome/Modelo	Servidor Montado - Asus
Processador	Processador Core 2 duo 3 Ghz
HD	1000 GB
Memória RAM	8 GB
Wi-Fi	Sim
Placa de Rede	10/100/1000 Mbps

Tabela 5 – Especificação do roteador do servidor de monitoramento

Equipamento	Roteador
Nome/Modelo	RB 750 GL
Velocidade da porta	1000 Mbps
Quantidade de Portas	5

Tabela 6 – Especificação dos roteadores dos servidores monitorados

Equipamento	Roteador
Nome/Modelo	DSL-2500E
Velocidade da porta	10/100 Mbps
Quantidade de Portas	1

Tabela 7 – Especificação do roteador do equipamento Multi

Equipamento	Roteador
Nome/Modelo	DSL-2730B
Velocidade da porta	10/100 Mbps
Quantidade de Portas	1

Tabela 8 – Especificação do equipamento Multi

Nome/Modelo	DELL
Processador	Intel® Pentium® Dual CPU E2220 2.4 GHZ 2.4GHZ
HD	1000 GB
Memória RAM	2 GB
Wi-Fi	Não
Placa de Rede	10/100 Mbps

Tabela 9 – Especificação do equipamento Ultrabook

Nome/Modelo	Sansung/NP530U3C
Processador	Intel® Core™ i5-2537M CPU @ 1.4GHZ 1.4 GHZ
HD	500 GB
Memória RAM	4 GB
Wi-Fi	Sim
Placa de Rede	10/100/1000 Mbps

A rede prove serviços de internet, FTP (fi*le Transfer Protocol*) e HTTP (*Hypertext Transfer Protocol*), entre outros. Todos rodam sobre a pilha de protocolos do TCP (*Transmission Control Protocol*) / IP (*Internet Protocol*).

. Sistemas Operacionais utilizados:

- Servidor de monitoramento: CentOS
- Servidores monitorados: Windows 2008 Server
- Estações de trabalho: Windows 7 Professional

. Ferramentas de monitoramento: Centreon e Zabbix

. Servidores Externos: Dropbox, Vono e Youtube

. Equipamentos de Rede: roteador RB750, Modem (GVT) e Modem (OI)

1.4.4 – Fronteiras do trabalho

Não serão testadas outras soluções de monitoramento existentes no mercado além das aqui citadas, ou seja, Zabbix e Centreon.

A implementação do monitoramento com as duas ferramentas citadas será realizada com a utilização do sistema operacional CentOS, com o uso do protocolo SNMP e o redirecionamento de portas.

Não será implantada uma solução de uso integrado e complementar das ferramentas de monitoramento Zabbix e Centreon.

Não será abordada a customização das ferramentas de monitoramento, como por exemplo a forma de tratar os dados capturados e o layout de apresentação dos gráficos, pois é muito abrangente e merece um trabalho a parte, tendo sido utilizada a customização padrão de cada ferramenta.

O trabalho também não contemplará outros recursos existentes em um ambiente de rede, tais como firewall, antivírus, equipamentos wireless, dentre outros.

1.5 - Resultados Esperados

Pretende-se demostrar em tempo real, o monitoramento do desempenho de uma rede WAN com links de diversas operadoras. Pretende-se efetuar um monitoramento para obter um resultado comparativo entre as soluções estudadas, utilizando o trafego de dados, voz e vídeo, e alertas sobre falhas ocorridas. Serão apresentas as formas com que as ferramentas são instaladas e configuradas, e através de gráficos e tabelas, as suas principais características e diferenças. O modelo que será implantado utilizará o sistema operacional CentOS, trabalhando de forma integrada com as ferramentas de monitoramento Zabbix e Centreon, acionadas para fazer o monitoramento simultâneo. A partir da análise das características e diferenças de cada ferramenta, e do comparativo de resultados obtidos, no que elas tiverem em comum, será possível apresentar um resumo das principais vantagens e desvantagens observadas em cada ferramenta.

A proposta apresentada visa auxiliar a equipe de TIC (Tecnologia da Informação e Comunicação) de uma empresa na solução de seus problemas relacionados ao gerenciamento da rede, e permitir uma rede mais saudável através do monitoramento.

1.6 - Estrutura do Trabalho

Este trabalho está estruturado em seis capítulos conforme disposto a seguir:

CAPÍTULO Nº 1 - INTRODUÇÃO: trata do tema abordado, bem como sua relevância. O texto ainda apresenta a justificativa para desenvolvimento do projeto;

CAPÍTULO Nº 2 - APRESENTAÇÃO DO PROBLEMA: apresenta a contextualização do problema dentro do cenário atual das tecnologia existentes e aponta desafios enfrentados no mercado;

CAPÍTULO Nº 3 – REFERENCIAL TEÓRICO: abrange todo o referencial teórico necessário para compreensão do que foi desenvolvido;

CAPÍTULO Nº 4 – DESENVOLVIMENTO DO PROJETO DE CUSTOMIZAÇÃO DE MONITORAMENTO DE LINKS E REDES: refere-se à solução projetada, juntamente com a sua explicação e funcionamento;

CAPÍTULO Nº 5 – TESTES E RESULTADOS: aborda a implementação juntamente com os testes realizados para o total funcionamento do projeto;

CAPÍTULO Nº 6 – CONCLUSÕES E TRABALHOS FUTUROS: conclui o trabalho, avaliando as soluções e propostas, e sugerindo novos estudos a serem realizados.

CAPÍTULO Nº 2 – APRESENTAÇÃO DO PROBLEMA

A complexidade que envolve as redes de servidores, estações de trabalho, ativos de redes, e outros recursos existentes atualmente, exigem sistemas operacionais ágeis e ferramentas de monitoramento do conjunto envolvido, de forma que estas redes funcionem de forma estável e segura, permitindo que problemas sejam detectados e alertados imediatamente, permitindo que o Administrador da rede corrija o defeito rapidamente.

2.1 – A Evolução Tecnológica e o Monitoramento de Redes.

O desenvolvimento da informática e das telecomunicações, associado à evolução da internet, fez com que surgissem as redes de computadores tão necessárias à vida contemporânea. Porém, é importante que seja garantida a disponibilização das informações ou serviços aos usuários, de forma permanente e com qualidade.

Hoje a necessidade de troca de informação é tão grande que um computador que não esteja ligado a uma rede tem pouca utilidade, e se a rede de uma organização ficar inoperante, todos os setores, de uma certa forma, serão afetados.

O monitoramento em tempo real e de forma ininterrupta tornou-se indispensável para o administrador de TI. Este monitoramento permite obter as informações necessárias sobre infraestrutura de redes e seus ativos de forma rápida, precisa e confiável, auxiliando o administrador na verificação do desempenho dos serviços, solução de problemas, e o planejamento, adaptação e expansão dos recursos da rede.

Contudo, com a rápida evolução da informática e das comunicações, e embora com muitas ferramentas de monitoramento disponíveis, muitos as utilizam sem o devido conhecimento, ou não tem conhecimento das armadilhas e perigos existentes.

2.2 – A Complexidade das Redes de Computadores

Atualmente as redes são utilizadas em todos os segmentos da sociedade, seja para o uso pessoal, para enviar ou receber um email, ou para se comunicar com as redes sociais, até a utilização em empresas, para servir informações e serviços para os funcionários ou diretamente aos clientes. Uma rede de computadores pode oferecer um meio de comunicação altamente eficaz para funcionários que trabalham em locais muito distantes um do outro (TANENBAUM, 2003).

Para melhor compreensão dos problemas enfrentados com a explosão no uso das redes, é necessário iniciar com a definição do que é uma rede. De uma maneira muito elementar, conforme apresentado na figura 2.1, rede é um agrupamento de pontos que se ligam a outros pontos por meio de linhas (MARTINHO; 2003).

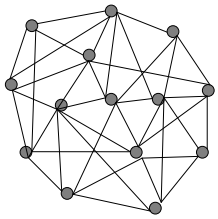

Figura 2.1 – Uma rede elementar onde pontos são interligados por linhas (TANENBAUM-Adaptação de figura, 2013)

Neste trabalho a rede a ser estudada é retratada na figura 2.2 (Computadores e ativos de rede são os pontos (nodos) e o meio são as linhas (conexões)) e trata-se da rede Internet, que liga computadores a outros computadores em todo o mundo.

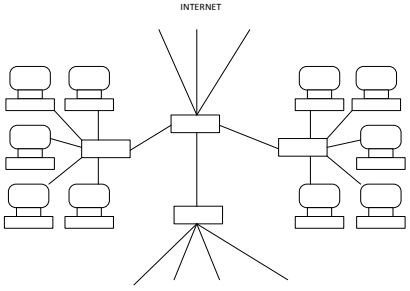

Figura 2.2 – Representação simplificada da rede Internet (TANENBAUM-Adaptação de figura, 2013)

Existem questões importantes que devem ser consideradas, como por exemplo: Como os pontos da rede estão conectados; A utilidade dessas ligações; Como aqueles pontos atuam quando interligados; Como estes pontos e linhas podem ser monitorados em conjunto. Precisa-se saber as propriedades dos recursos e as ferramentas existentes para monitorá-los, para que uma rede possa ser administrada de forma a garantir a disponibilidade das informações e serviços aos seus usuários.

Em uma rede, as linhas são mais importantes do que os pontos, porque são as conexões que fazem a rede. É o relacionamento entre os pontos que dá qualidade ao conjunto. Como se pode observar na figura 2.3, são as conexões (as linhas) que ligam os pontos, e são elas responsáveis pelo desempenho da rede. E é a conectividade que constitui a dinâmica da rede. Toda a rede existe em função da realização contínua de conexões entre os seus pontos, e ela só existe na medida em que houver ligações sendo estabelecidas.

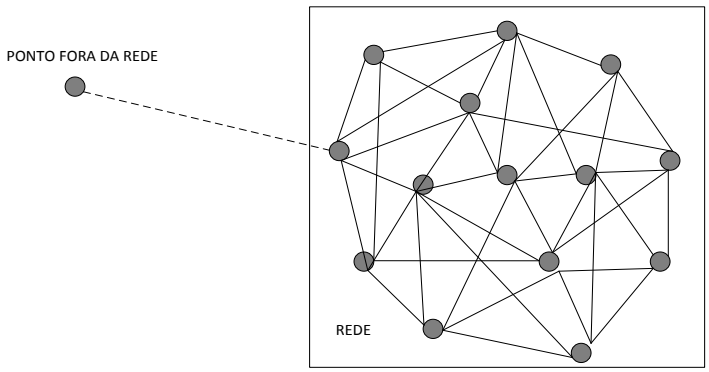

Figura 2.3 - Por meio de uma conexão, um ponto isolado pode se conectar à rede (TANENBAUM-Adaptação de figura, 2013)

Toda a conexão interliga um par de pontos. Desta forma, uma linha equivale a dois pontos. Em contrapartida, cada ponto pode manter uma infinidade de linhas que se interligam a outros, correspondendo à quantidade de pontos da rede ligados a ele.

Assim, a densidade da rede está relacionada à quantidade de conexões que esses pontos estabelecem entre si. Essa característica faz com que a capacidade da rede ultrapasse a soma dos elementos que a constituem, sendo o limite de conectividade do sistema alcançado, quando todos os pontos estabelecem ligações com os demais, sem ponto intermediário.

Portanto, é fundamental que exista o monitoramento dessas conexões e dos pontos que interligam, permitindo o gerenciamento da rede pertencente a uma instituição, de forma que problemas existentes ou em potencial, sejam detectados e alertados automaticamente, para que os administradores de rede possam atuar de forma preventiva, impedindo um transtorno que haveria no sistema, ou minimizar os efeitos provocados por uma falha surgida.

2.3 - Monitoramento de redes

Um monitoramento de uma rede compreende a coleta e o tratamento de dados do funcionamento dos componentes desta rede, para que os especialistas interpretem estes dados e tomem decisões. Assemelha-se aos exames médicos que realizamos em nosso organismo para que um médico, os analise, diagnostique um problema, e indique o tratamento para a cura. No caso das redes, estes exames necessitam de softwares desenvolvidos para esta finalidade, que façam a coleta automática e permanente de dados do funcionamento de todos os componentes de uma rede, compreendendo os links, os computadores, os ativos de rede e os serviços, que tratem estes dados, e apresentem o resultado em tempo real, através de telas, gráficos, relatórios, e avisos de alerta, para que os administradores de redes possam gerenciá-las de forma a garantir o seu funcionamento com um bom desempenho e sem interrupção, servindo também, como instrumento de planejamento para adequação, melhoria, ou crescimento das redes e dos serviços oferecidos por elas. Para aprofundamento do estudo sobre gerenciamento de redes com o uso de ferramentas de monitoramento, é indicado o livro Melhores Práticas para a Gerência de Redes de Computadores (SAUVÉ, LOPES, NICOLLETT, 2003).

Neste trabalho serão estudadas as ferramentas de monitoramento Nagios e Centreon, distribuídas gratuitamente através de licenças GPL. Serão realizados testes e verificados os resultados que cada uma apresentou. Serão também relacionadas as instruções (manuais) de instalação, e as técnicas utilizadas para a instalação, configuração e monitoramento. Finalmente será feita uma analise dos resultados, buscando assim, demonstrar como pode ser resolvido, pelo menos em parte, o grande problema do monitoramento de redes.

CAPÍTULO Nº 3 - REFERENCIAL TEÓRICO

Neste capítulo serão apresentados todos os conceitos e bases tecnológicas para o desenvolvimento do trabalho, descrevendo o sistema operacional utilizado, as ferramentas de monitoramento que serão testadas, os ativos de redes, os mais recentes servidores de dados, voz, imagem, e novas tecnologias existentes para o uso e o monitoramento de redes.

3.1 – GNU/Linux

O GNU/Linux é um sistema operacional muito utilizado no mundo. Por se tratar de um sistema que tem o seu código-fonte aberto, e é distribuído gratuitamente através de licenças GPL, existem variantes do código original, que são chamadas de distribuições. As distribuições têm características próprias implantadas pelos seus desenvolvedores, que criam comunidades voltadas para a constante correção de problemas detectados e permanente evolução do produto. Para conhecimento mais aprofundado pode-se consultar o livro de João Eriberto Mota Filho - Descobrindo o Linux (NOVATEC, 2012).

O Linux é um sistema operacional multitarefa e multiusuário, e que funciona nas mais diversas plataformas. Surgiu em 1991 como um sistema operacional *free*. Seu desenvolvimento foi iniciado por Linus Benedict Torvalds, que divulgou a sua ideia pela internet, tendo conseguido uma quantidade cada vez maior de adeptos, que passaram a contribuir com seu projeto de sistema operacional, transformando-o no fabuloso sistema operacional GNU/Linux (http://www.ici.curitiba.org.br/exibirArtigo.aspx?idf=2, 30/09/2013).

Embora os diversos pacotes deste sistema operacional sejam conhecidos apenas como Linux, a denominação correta é GNU/Linux, porque Linux é apenas o kernel do sistema operacional, e ele necessita de outros *softwares* para rodar, estando estes recursos contidos no projeto GNU. Consequentemente o sistema operacional CentOS utilizado neste trabalho contem um kernel Linux agregado à ferramentas GNU, e desta forma trata-se de um GNU/Linux (http://www.vivaolinux.com.br/linux/, 30/09/2013).

O GNU/Linux possui diversos pacotes diferentes que recebem o nome de distribuições. Cada uma tem um perfil próprio, e encontram-se formas diferentes de

instalação, interfaces mais ou menos amigáveis, recursos gráficos mais ou menos sofisticados, e variações nos aplicativos agregados.

No Brasil existem mais de vinte distribuições diferentes, sendo as principais:

Ubuntu GNU/Linux, openSUSE GNU/Linux, Debian GNU/Linux, Slackware GNU/Linux, Kurumin GNU/Linux, Fedora GNU/Linux, LinuxMint e CentOS GNU/Linux: que por ser o sistema operacional utilizado neste projeto, será apresentado a seguir.

Como o núcleo das distribuições citadas neste item é Linux/GNU, tanto o Centreon quanto o Zabbix, podem ser também instalados nas outras distribuições. O que muda é a forma de instalação e configuração, que depende dos pacotes inseridos em cada uma delas.

3.2 - CentOS

É uma distribuição de classe Enterprise oriunda de códigos fonte cedidos pela Red Hat Enterprise Linux. A partir desta cessão, o CentOS Project fica responsável pela sua manutenção. Até a numeração da versão do CentOS corresponde a do Red Hat Enterprise Linux. A diferença que existe entre os dois sistemas é que para o Red Hat Enterprise Linux o cliente paga pelo suporte.

O CentOS Linux tem compatibilidade com os programas e aplicativos desenvolvidos para a Red Hat Enterprise Linux, proporcionando a mesma segurança e suporte das outras soluções Linux Enterprise, sem custo. Pode ser um excelente servidor para aplicações críticas, ou pode operar como estação de trabalho, possuindo uma versão Live CD. O CentOS possui colaboradores que participam de forma ativa e crescente, permitindo uma evolução rápida e consistente, seus downloads são realizados com facilidade, os seus desenvolvedores são bastante acessíveis, e tem suporte em português, entre outras vantagens (http://pt.wikipedia.org/wiki/CentOS, 27/09/2013).

Por ser o CentOS um sistema seguro, utilizado por muitas empresas de grande porte, optou-se pelo seu uso junto com as ferramentas de monitoramento Centreon e Zabbix.

3.3 – Componentes do Monitoramento de Rede de computadores

3.3.1 - Monitoramento de dispositivos de rede

O monitoramento consiste na observação de informações relevantes ao gerenciamento podendo ser classificado em três categorias: (FILHO, 2012)

. Estático: caracteriza elementos na atual configuração, como o número de identificação das portas de um roteador;

. Dinâmico: relacionada a eventos na rede, como a transmissão de um pacote;

. Estatístico: pode ser derivada de informações dinâmicas como a média de pacotes transmitidos por unidade de tempo em um determinado sistema.

As informações são coletadas e armazenadas por agentes e repassada para um ou mais gerentes. Duas técnicas podem ser utilizadas na comunicação:

. *Polling*: interação do tipo request/response, onde o gerente solicita a um agente, o envio de diversos elementos de informação;

. *Event-reporting*: a iniciativa parte do agente. Onde o gerente fica apenas na escuta, esperando pela chegada de informações.

Tanto o *polling* como o *event-reporting* são usados nos sistemas de monitoramento. A escolha da técnica depende de muitos fatores:

. Quantidade de tráfego gerada por cada método e de processamento nos equipamentos gerenciados;

. Robustez em situações críticas;

. Tempo entre a ocorrência do evento e a notificação ao gerente;

. Transferência confiável versus não confiável;

. As aplicações de monitoração suportadas pela rede;

. As considerações caso um equipamento falhe antes do envio do relatório.

3.3.2 - Monitoramento de rede, serviços e servidores

A utilização das ferramentas de monitoramento permite analises de possíveis ameaças, penetradas na rede ou que podem por em riscos os servidores, e por meio de alertas configurados para serem apresentados em tela, por email, via celular, ou SMS (*Short Message Service*), avisar a equipe de tecnologia, para que esta possa agir imediatamente. Neste trabalho serão implementados os alertas apresentados em tela e via email. O alerta na rede pode ser em diversos serviços como DHCP (*Dynamic Host Configuration Protocol*), SMTP (*Simple Mail Transfer Protocol*), POP (*Post Office Protocol*), HTTP (*Hypertext Transfer Protocol*), FTP (*File Transfer Protocol*), SSH (Secure Shell) e outros, e em servidores com monitoramento de recursos tais como CPU (Central Processor Unit – unidade central de processamento), disco, memória, e demais recursos. Possui muitos benefícios como o monitoramento 24x7 (vinte e quatro horas, sete dias por semana), que melhora a disponibilidade do sistema e de relatórios e logs de acessos.

3.3.3 – Tecnologias utilizadas em redes

A tecnologia utilizada para a construção de uma rede pode ser:

. ponto a ponto, que consiste em conexão de pares individuais de máquinas que se comunicam direto sem passar por um intermediário onde tem um emissor e um receptor de dados;

. multiponto, que permite a conexão de várias máquinas compartilhando entre todos os dispositivos de rede um meio de transmissão único, através do qual toda a informação é transmitida.

Quanto ao escopo, a rede pode ser caracterizada como rede local, a chamada LAN (*Local Area Network*), que compartilha recursos e trata-se de rede privada. As LANs alcançam até 10 km e conectam servidores, estações de trabalho, periféricos e outros dispositivos de rede que possuem dispositivos de processamento em escritórios, residências, ou edifícios. Quando a rede tem maior alcance é denominada MAN (*Metropolitan Area Network*), que atende uma cidade. Já a rede WAN, conhecida como rede geograficamente

distribuída, pode abranger um país ou um continente, como é o caso da Internet (http://wirelesspt.net/wiki/Rede_de_computadores, 25/09/2013).

Outro tipo de rede que vem conquistando espaço é a rede *wireless* (sem fio), sendo cada vez mais utilizada em dispositivos móveis, *smartphones* e celulares. Trata-se de uma conexão de rede efetuada através de radiofrequência e utilizada tanto em ambiente doméstico ou escritório, quanto em um ambiente público, como bares, aeroportos, hotéis e parques. A grande vantagem desta tecnologia de rede é a mobilidade permitida ao usuário.

3.3.4 - Ativos e serviços de redes

Uma rede é formada por vários tipos de recursos, como computadores, roteadores, switches e serviços de rede. Os equipamentos e serviços devem ser monitorados, evitando falhas ou interrupção do funcionamento da rede.

Os servidores da rede podem possuir funcionalidades de diferentes naturezas. Alguns tipos de servidores/serviços de rede são:

O servidor FTP, representado na figura 3.1 por FTP Server, é o servidor onde os usuários têm acesso a arquivos em rede, que a partir da solicitação via FTP Commands, tem a função de ceder os dados ao FTP Client, que é o equipamento que requereu a informação, fornecendo a resposta via Data Connection;

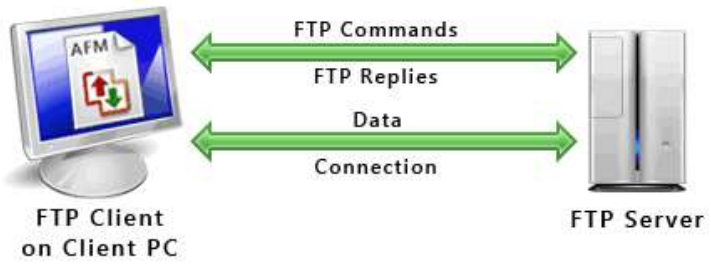

Figura 3.1 – Representação de um servidor FTP (http://www.deskshare.com/lang/po/resources/articles/ftp-how-to.aspx, 20/10/2013)

O servidor WEB, representado na figura 3.2 por Servidor, é responsável por aceitar pedidos HTTP de clientes, servindo com páginas web e arquivos de site;

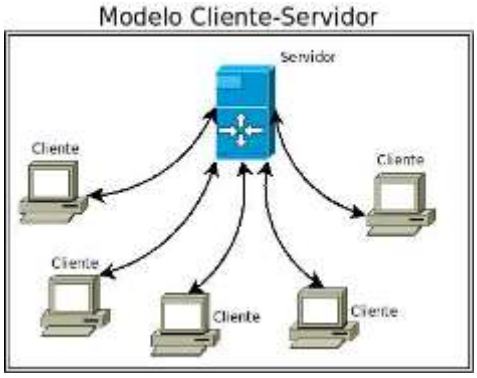

Figura 3.2 – Representação de conexões Cliente-Servidor (http://www.deskshare.com/lang/po/resources/articles/ftp-how-to.aspx, 20/10/2013)

O servidor DNS (*Domain Name System*) representado na figura 3.3 por Servidor DNS, é responsável por nomear computadores, representado por Navegador, e serviços em redes TCP/IP, e a partir de uma solicitação via consulta DNS, retorna por esta via o respectivo IP do equipamento ou serviço;

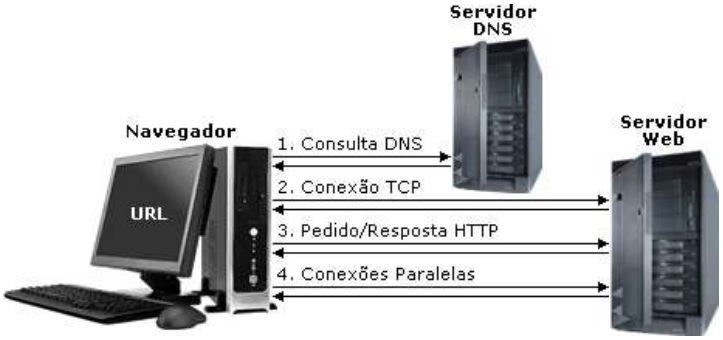

Figura 3.3 – Representação de um servidor de DNS (http://www.teleco.com.br/tutoriais/tutorialinter/pagina_3.asp, 20/10/2013)

O servidor de arquivos, representado pela figura 3.4 por Servidor de Arquivos, é o responsável por armazenar arquivos de clientes, neste caso, através de um Switch/Hub, com a proteção de um firewall, atendendo às estações de trabalho e a uma impressora;

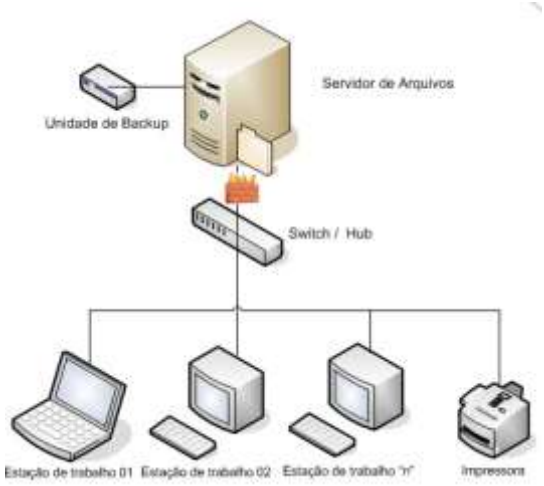

Figura 3.4 – Representação de um servidor de arquivos (http://gratishospedagem.com.br /servidor-de-arquivos/servidor-de-arquivos/, 20/10/2013)

O servidor Webmail, que é responsável pelo envio/recebimento de contas eletrônicas e armazenamento de e-mails;

O servidor de Proxy, representado na figura 3.5 por proxy P, é um servidor intermediário, que atende às requisições do cliente, representado por usuário U, repassa a solicitação a um outro servidor, representado pelo globo terrestre, recebe o resultado da solicitação, e devolve ao cliente solicitante, funcionando como um cache.

Figura 3.5 – Representação de um servidor proxy (http://canaltech.com.br/o-que-e/software/Conheca-todos-os-formatos-de-audio/, 20/10/2013).

Para a conexão de computadores e periféricos na rede é necessário a utilização de dispositivos tais como o *switches* e roteadores.

O roteador tem a atribuição de definir a melhor rota para transferir e receber protocolos na rede. Utiliza-se para interconectar diferentes redes de computadores provendo a

comunicação entre computadores distantes entre si. A figura 3.6 apresenta o roteador RB750GL, utilizado neste trabalho.

Figura 3.6 – Roteador RB750GL (http://www.mikrotik-shop.de/product_info.php?Language=en&products_id=544, 20/10/2013)

O roteador RB750GL, também conhecido como routerboard RB750GL, oferece 5 portas com padrão Gigabit, permitindo um grande trafego de informações, e em operações como load balance pode balancear de 2 a 4 links. Possui processador de 400 Mhz e memória de 64 MB. Esse equipamento utiliza o RouterOS com licença nível 4, que por suas características permite que possa gerenciar toda uma rede sem dificuldades. (http://www.fullwireless.com.br/produto/Mikrotik/Routerboard/Mikrotik/RB750GL, 20/10/2013).

O *switch* tem a função de criar um barramento de comunicação entre os dispositivos de rede pertencentes à estrutura. Este dispositivo reencaminha os dados entre os nós. Possuem diversas portas, e operam na camada acima dos hubs. É ele que segmenta a rede internamente através de portas, cada porta correspondendo a um segmento diferente, não permitindo que haja colisões entre os equipamentos de segmentos diferentes.

Existem *switches* podem ser gerenciados para administrar as portas individualmente. O *switch* gerenciável costuma possuir outras funcionalidades, como o recurso de criar VLANs (*Virtual Local Area Network* ou Virtual LAN), QoS (Quality of Service) e *firewall*. Tem a possibilidade de habilitar e desabilitar as portas, definir a velocidade da conexão, especificar VLANs, configurar o *spanning tree*, e permite a utilização de *software* de monitoramento que acessa o *switch* através de protocolos como o SNMP. Abaixo a figura 3.7 apresenta o CISCO 2950-24, um dos modelos de *switches* disponíveis no mercado.

Figura 3.7 – Switch CISCO 2950-24 (http://www.cisco.com/en/US/products /hw/switches/ ps628/products_data_sheet09186a00801cfb71.html, 20/10/2013)

3.3.5 - Nagios

Criado originalmente com o nome de Netsaint, foi escrito em 1996 por Ethan Galstad e é atualmente mantido por ele e uma equipe de desenvolvedores, que ativamente mantém *plugins* oficiais e não oficiais. A ideia inicial era que o Nagios, através de arquivos .bat (*Batch* ou arquivo de lote) no MS-DOS, executasse *pings* em dispositivos de rede. Mas como o sistema ficaria limitado, foi dado continuidade no Linux, tornando o sistema mais robusto e granular podendo desenvolver *plugins* integrados com os módulos de rede como SNMP, HTTP, e FTP entre outros. O Nagios pode rodar em outros Unixes também. (http://pt.wikipedia.org/wiki/Nagios, 18/09/2013)

Em 1999 foi fundada uma empresa para suporte ao Nagios e em 2003 foi desenvolvida sua primeira versão comercial.

O Nagios é um programa que roda em Linux como um *deamon* e depende de vários outros arquivos. Tudo começa quando o binário do Nagios é executado e então ele lê o arquivo principal onde possui as configurações pai do sistema.

O Nagios é um executor de tarefas através de comandos parametrizados em seus arquivos de configuração.

O arquivo principal, Nagios.cfg possui os *paths* dos seus principais arquivos de monitoramento.

O Nagios é uma ferramenta de código aberta distribuída sobre a licença GPL (*General Public License*). Ele pode monitorar tanto *hosts* quanto serviços, alertando-o quando ocorrem problemas e também quando os problemas foram resolvidos.

Principais características: (CELUPPI, 2009)

. Monitoramento de aplicação, serviços, sistemas operacionais e componentes de infraestrutura;

. API (*Application Programming Interface*) para desenvolvimento de sistemas customizados;

. Cliente / proprietário;

. Suporte ao protocolo SNMP;

. Visão centralizada de todos os sistemas monitorados;

. Informações detalhadas dos componentes monitorados na interface web;

. Rápida detecção de problemas na infraestrutura;

. Alertas via email e SMS;

. Alertas customizáveis, para envio diretamente para a pessoa responsável;

. Base de conhecimento para problemas e situações conhecidas;

. Configurações de eventos para ações pré-configuradas, como reiniciar o serviço ao surgir o problema;

. Planejamento de infraestrutura para o acompanhamento do envelhecimento tecnológico;

. Paradas programadas, para o sistema não enviar alertas nesses períodos;

. Relatórios para acompanhamento de SLAs (*Service Level Agreement*);

. Histórico de envio de alertas e notificações;

. Suporte a *plugins* de terceiros;

. Multiusuário *web* com níveis de acesso.

3.3.6 – Centreon

Inicialmente chamado de Oreon, o Centreon é um software de monitoramento de rede, com código livre, disponibilizado sob a licença GPL, que usa o Nagios como seu núcleo. O Centreon necessita do Nagios para funcionar. Na verdade o Centreon é um front-end para o Nagios. Nativamente o Nagios já possui sua interface Web, mas o Centreon implementa outros recursos interessantes.

Centreon tem uma interface simplificada e amiga e se utiliza muito de gráficos, fazendo com que a consulta ao resultado do monitoramento seja mais compreensível a maior parte dos usuários, inclusive pessoas não técnicas na área.

Em 2005, a empresa MERETHIS foi a responsável por unir a comunidade em torno dessa solução de código aberto. Em julho de 2007, o nome desta ferramenta muda de Oreon para Centreon. Em 2009 a empresa MERETHIS se concentra em seu papel de editor do software e opta por um modelo de desenvolvimento de núcleo aberto, e o coração do Centreon passa a ser Open Source. A partir daí o desenvolvido desta ferramenta passa a ser feito pela comunidade, e empresa MERETHIS se responsabiliza pelo sdesenvolvimento e distribuição dos módulos de carga. Desde o início de 2012, este software vem se destacando como uma das melhores ferramentas de monitoramento. (http://fr.wikipedia.org/wiki /Centreon, 18/10/2013)

Com esta ferramenta é possível monitorar, gerenciar, gerar gráficos de disponibilidade e serviços, receber traps SNMP e avisar quando algum problema é detectado. Pode ser instalada de forma simplificada em conjunto com o sistema operacional CentOS, através do software FAN, que além de tornar estas instalações uma tarefa simples, também dispões de ferramentas que interagem com o Centreon, e complementam as suas funcionalidades. O Centreon é uma solução muito importante para gerenciar a rede e manter a disponibilidade do serviço, garantindo assim a qualidade do serviço prestado.

3.3.7 - Zabbix

O Zabbix teve seu início em 2001. Foi desenvolvido usando a linguagem PHP (*Personal Home Page*, atualmente conhecido como *Hypertext Preprocessor*), disponibilizando ao usuário uma linguagem *web* com suporte a banco de dados. Adota uma licença *Open Source*, sendo considerado como uma das melhoras ferramentas de monitoramento da atualidade. Muitas de suas funcionalidades que foram herdadas do Nagios e do Cacti a tornaram uma das ferramentas mais poderosas e completas disponíveis. O *software* tem suporte a praticamente todos os sistemas operacionais.

É uma ferramenta de monitoramento de rede que permite acompanhar o desempenho e a disponibilidade de todos os serviços e ativos de rede, desde aplicações envolvidas na rede, até inúmeros equipamentos que são ligados a ela, tais como servidores, *hosts*, *switches*, e roteadores. Coleta informações de todos os dispositivos que estão interligados na rede. Este poderoso sistema de gerenciamento e monitoramento absorve todas as informações requisitadas, e permite que as informações sejam coletadas em um banco de dados SQL

(*Structured Query Language*) ou até mesmo Oracle (ZABBIX – Monitorar é preciso. http://www.zabbix.com/, 10/10/2013).

O Zabbix é dividido em três partes distintas:

. Servidor Zabbix - responsável pela coleta e armazenamento dos dados;

. Agente Zabbix - responsável por repassar todas as informações que foram coletadas do sistema operacional no qual o servidor esta rodando;

. Interface Zabbix - é a estrutura que permite o administrador interagir e administrar o sistema.

Características: (CELUPPI, 2009)

. Gerenciamento centralizado;

. Acesso centralizado a informações;

. Número ilimitado de proxies;

. Monitoramento em tempo real;

. Monitoramento de alertas de disponibilidade e integridade, entre outros;

. Alertas via SMS, *email*, mensagem instantânea e via script configurado;

. Log de auditoria;

. Visualização, através de abas *web* e mapas;

. Execução e comandos remotos;

. Suporte a serviços de TI hierárquico;

. Relatório em tempo real de SLA´S;

. Facilidade de integração com sistemas de terceiros;

. Modelos pré-configurados de *hosts*;

. Facilidades de compartilhamento de modelos;

. Sistema de auto busca de dispositivos a serem monitorados;

. Monitoramento de páginas web.

3.4 - Links de Dados e Comunicação

A disponibilidade de *links* da internet se tornou crítica na maioria das empresas. A escolha de *links* profissionais com SLA envolve um custo alto e mesmo assim não garante estar 100% disponível. Muitas empresas utilizam dois *links* de internet em um mesmo servidor, pois caso um caia o outro pode assumir.

3.5 - Novas Tecnologias de Servidores

Nos dias atuais há muitas tecnologias surgindo, tais como os servidores de Dados e a Telefonia VOIP (*Voice over Internet Protocol*), também tem-se a necessidade de acesso externo aos servidores *WEB*. É necessário o conhecimento destas tecnologias, para que se usufrua destes recursos.

3.5.1 – Servidor de dados Dropbox

O Dropbox é um servidor de dados, que possibilita aos usuários o armazenamento de informações externamente ao seu ambiente, nos servidores do Dropbox. Suas principais características são: (https://www.dropbox.com/business/pricing, 2010)

. Sincroniza todo o trabalho em todos os dispositivos;
. Possibilita o gerenciamento dos acessos e o acompanhamento do uso da conta;
. Permite o compartilhamento de pastas com outros usuários externos;
. Integração com o AD;
. Acesso a versões antigas ou restauração de arquivos excluídos.

3.5.2 – Servidor de voz Vono (GVT)

O Vono (GVT) é um servidor de telefonia. Com esta ferramenta, é possível a comunicação de voz, via internet banda larga, com o uso da tecnologia VOIP. O serviço é oferecido com as possibilidades a seguir: Acesso pelo computador; Acesso pelo telefone

comum; Acesso pelo telefone IP (VOIP); Acesso pelo *smartphone*; Acesso pelo PABX; Acesso direto ao Vono (FALEVONO. Conheça o Vono. http://www.falevono.com.br/conheca/conheca.html. Última visita 20/09/2013).

3.5.3 – Servidores *WEB*

O servidor *WEB* é um recurso responsável por aceitar pedidos HTTP de clientes, que geralmente são os navegadores, e servi-los com respostas HTTP, incluindo opcionalmente dados, que geralmente são paginas *web*.

Os principais servidores *WEB* existentes atualmente são: (http://www.mutukagames.xpg.com.br/pg4.html. Última visita 27/09/2013)

Apache - É um *software* de elevado desempenho e excelente qualidade, a um custo mínimo; IIS (*Internet Information Services*) - é o *Webserver* da Microsoft; .*Websphere* - *Webserver* da IBM; BEA *WebLogic* - Concorrente da IBM; Tomcat - Servidor *Web* livre para aplicações J2EE; Jboss – Servidor WEB que possui liderança entre os servidores J2EE gratuitos; Thttpd - tiny/turbo/throttling HTTP server - é um servidor muito rápido para volume alto de páginas simples; Jrun - Servidor pago da Macromedia para aplicações J2EE; Zeus Web Server – É muito poderoso, porém o custo é muito alto (http://www.mutukagames.xpg.com.br/pg4.html, 27/09/2013).

3.6 – SNMP (*Simple Network Management Protocol*)

O SNMP é um protocolo de gerência típica de redes IP, que facilita o intercâmbio de informações entre os dispositivos de rede, como placas e comutadores (*switches*). O SNMP permite que o administrador gerencie o desempenho da rede, encontre e resolva possíveis e eventuais problemas, e forneça informações para o planejamento da expansão desta rede.

A primeira versão foi lançada em 1989. Após inúmeras revisões na primeira versão, a segunda versão, ou SNMPv2, foi lançada quatro anos após. A terceira versão, ou SNMPv3, foi desenvolvida para permitir o acesso às informações de gerenciamento de forma mais segura, utilizando recursos de autenticação e criptografia.

Conforme se observa na figura 3.8, a topologia lógica de redes (maneira como os dados são transmitidos através da rede de um dispositivo para o outro, sem ter em conta a interligação física dos dispositivos), gerenciadas utilizando o SNMP, é composta por três elementos: (SALVO, http://www.ti-redes.com/gerenciamento/snmp/intro/, 27/09/2013).

. Dispositivos gerenciados – São os recursos físicos pertencentes à rede, compreendendo os roteadores, *switches*, dispositivos *wireless*, e servidores e outros;

. Agentes – É o conjunto de *softwares* que armazena as informações sobre os dispositivos gerenciados em uma base que tem uma estrutura conhecida como MIBs.

. Sistema de Gestão de Rede NMS (*Network Management System*) – É o *software* que efetivamente realiza o monitoramento e controle de dispositivos gerenciados.

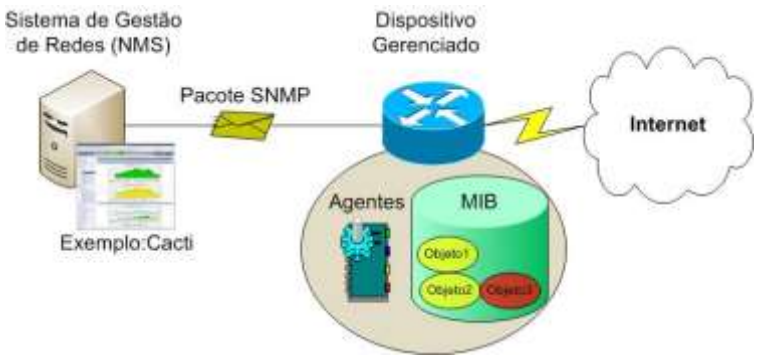

Figura 3.8 - Arquitetura de uma rede gerenciada por meio de SNMP (http://www.ti-redes.com/gerenciamento/snmp/intro/, 27/09/2013)

O SNMP usa as portas 161 e 162 na camada de transporte UDP (*User Datagram Protocol*) para a comunicação entre o sistema de gestão de rede (NMS) e os dispositivos gerenciados.

A figura 3.8 ilustra o pacote SNMP transportando dados entre o dispositivo gerenciado, que no caso deste projeto são os equipamentos monitorados, e o sistema de gestão de redes (NMS), que neste caso são as ferramentas Centreon e Zabbix.

O gerenciamento é realizado utilizando-se três categorias de mensagens:

. *Get* (obter) – possibilita a obtenção do valor dos objetos MIB do agente pela estação de gerenciamento;

. *Set* (definir) – possibilita a definição do valor do objeto MIB do agente pela estação de gerenciamento;

. *Trap* (armadilha) – possibilita que a estação de gerenciamento seja notificada pelo agente sobre eventos significativos.

A versão utilizada neste projeto é a do protocolo SNMPv2. Optou-se por este protocolo ao invés do mais recente, que é o SNMPv3, pelo fato deste possuir os recursos de autenticação e criptografia, que podem ser incompatíveis com ativos mais antigos, e neste caso específico, poderiam conflitar com a configuração dos hosts monitorados, que pertencem a redes de empresas do DF. O protocolo SNMPv2 possui as seguintes características (https://www.rnp.br/newsgen/9712/gerencia.html, 12/10/2013):

Esta versão trouxe grandes avanços que foram incorporados ao protocolo original. Tais avanços podem ser classificados de acordo com as seguintes categorias: Estrutura de informação; Primitivas de comunicação (PDUs); Comunicação gerente-gerente e gerenciamento hierárquico; Segurança.

A estrutura de informação de gerenciamento (SMIv2) para o SNMPv2 é mais elaborada, e eliminou ambiguidades nas definições dos objetos encontrados nas especificações anteriores.

Em relação às primitivas foram acrescentados dois novos PDUs:

. *Get-bulk-request-PDU*: que permite que uma grande quantidade de informações possa ser transferida do agente para o gerente eficientemente;

. *inform-request-PDU:* que permite a um gerente enviar ou eventualmente solicitar informações a outro gerente.

A comunicação gerente-gerente, como também o gerenciamento hierárquico, foram incorporados ao protocolo com a introdução do novo tipo de mensagem, *inform-request;* e com a SNMPv2-M2M MIB, que é constituída por dois grupos: um grupo de alerta e um grupo de eventos.

No tocante a segurança, o SNMPv2 acrescentou ao protocolo novos conceitos e serviços que trouxeram mais segurança ao protocolo. Os conceitos incluídos foram: o conceito de visão de MIB definido em termos de sub-árvores, restringindo o acesso a porções predefinidas da MIB; e o conceito de contexto, que é uma coleção de objetos e seus respectivos agentes, e a especificação dos privilégios envolvidos.

3.7 – FAN (*Fully Automated Nagios*)

A instalação e configuração de sistemas operacionais de distribuições Linux e das ferramentas desenvolvidas para estes sistemas, são normalmente complexas e exigem conhecimento e paciência. As distribuições do Nagios não fogem desta regra, e a configuração do software para uma pessoa com pouca experiência pode ser uma experiência muito frustrante. Como Centreon é uma ferramenta cujo núcleo é o Nagios, tem-se a mesma dificuldade. Mas existe um aliado para solucionar este problema, que é o software FAN.

Com esta ferramenta, a complexidade de instalação e configuração do CentOS e do Centreon deixa de existir. É possível ter o sistema completo de monitoramento instalado em menos de uma hora. É preciso apenas que se tenha uma imagem do sistema em um CD, e que se faça o boot pelo CD-ROM. Atualmente encontra-se na versão 2.4 e é disponível para sistemas x86 ou 64 bits. É uma ferramenta gratuita e o download pode ser feito no site do projeto http://www.fullyautomatednagios.org/wordpress/download/ (15/10/2013).

O FAN disponibiliza os aplicativos a seguir, prontos para utilização:

. Nagios: O Nagios Core, ou núcleo do Nagios.

. Nagios Plugins: Diversos Plugins de checagem, notificação e outros.

. NagVis: Ferramenta de visualização gráfica de dados do Nagios.

. NDOUtils: Ferramenta que armazena os dados de monitoramento em um banco de dados, permitindo a recuperação para futuras análises.

. NaReTo (*Nagios Reporting Tool*): Ferramenta para geração de relatórios a partir dos dados armazenados do Nagios. Permite análise dos serviços, identificando pontos de falha e de melhorias.

. Centreon: Ferramenta de monitoramento utilizada neste projeto. Responsável pela configuração gráfica do Nagios, pode ser utilizado para configurar os serviços, hosts e notificações, evitando o uso e edição de arquivos de configuração.

. Wiki: Ferramenta de documentação do FAN.

3.8 - NAT

O NAT (*Network Address Translation*) surgiu como uma alternativa real para o problema de falta de endereços IP v4 na Internet. Cada computador que acessa a Internet deve ter o protocolo TCP/IP corretamente instalado e configurado. Para isso, cada computador da rede interna, precisaria de um endereço IP válido na Internet. Não haveria endereços IP v4 suficientes. A criação do NAT veio para solucionar este problema, até que os endereços IP v6 estejam disseminados na rede. O princípio de funcionamento será explicado nos parágrafos a seguir: (http://www.juliobattisti.com.br/artigos/windows/tcpip_p20.asp, 10/10/2013)

Com o uso do NAT, os computadores da rede Interna, utilizam os endereços privados. Os endereços privados não são válidos na rede internet, ou seja, pacotes que tenham como origem ou como destino, um endereço na faixa dos endereços privados, não serão encaminhados e serão descartados pelos roteadores. O software dos roteadores é configurado para descartar pacotes com origem ou destino dentro das faixas de endereços IP privados. As faixas de endereços privados são definidas na RFC 1597 e são: de 10.0.0.0 a 10.255.255.255, de 172.16.0.0 a 172.31.255.255, e de 192.168.0.0 a 192.168.255.255.

Como os endereços privados só podem ser utilizados na rede interna de uma empresa, isso permite que várias empresas utilizem a mesma faixa de endereços privados, ou seja, qualquer empresa pode utilizar endereços nas faixas descritas.

Para que um pacote possa ser enviado para a Internet, o NAT substitui o endereço IP de origem por um dos endereços IP da interface externa do NAT (endereço fornecido pelo provedor de Internet).

O NAT ao executar a função de tradução de endereços, associa um número de porta, que é único, com cada um dos computadores da rede interna. Todos os endereços da rede interna são traduzidos para o mesmo endereço externo, porém com um número diferente de porta para cada equipamento da rede interna.

Quando a resposta retorna, o NAT consulta a sua tabela interna e, pela identificação da porta, sabe para qual computador da rede interna deve ser enviado o pacote de informações, uma vez que a porta de identificação está associada com um endereço IP da rede interna

3.9 – NO-IP

Para que um equipamento possa ser acessado de qualquer ponto de uma rede, e em qualquer momento, é necessário que o seu endereço IP seja fixo, porém o que ocorre normalmente é que um endereço IP é dinâmico e este está em constante mudança. Sempre que o modem ou *router* faz *refresh*, recebe um IP dinâmico diferente, logo seria impossível acessar novamente aquele equipamento, sem saber o seu novo endereço IP.

Para contornar este problema existe um serviço de DNS chamado NO-IP que permite que um determinado equipamento seja sempre localizado, mesmo com seu endereço IP sendo dinâmico, e estar sendo alterado com frequência. É necessário criar uma conta no site www.no-ip.com, e atribuir um *hostname* para o equipamento, que substituirá o endereço IP dinâmico. A partir daí, o endereçamento do equipamento será feito pelo seu *hostname* e não mais pelo endereço IP. (http://www.canaldainfo.com.br/ index.php/no-ip-eu-quero-um-ip-fixo/, 11/10/2013)

De uma forma simplificada, depois de cadastrado, o equipamento passa a ser endereçado pela referência http://hostname.domain.com, sendo sempre acessado, independente do endereço IP dinâmico que esteja ostentando.

Os conceitos e tecnologias abordados neste capítulo formam o alicerce para o desenvolvimento deste projeto. Viu-se a complexidade de uma rede de computadores; As redes LAN, as MAN, e especialmente as WAN; A necessidade e a finalidade do monitoramento; O link de dados e comunicação; Os ativos de rede; O que é o sistema operacional Linux, suas distribuições, e a distribuição Centreon escolhida; As ferramentas de monitoramento Centreon e Zabbix; O protocolo SNMP; as NATs; A utilização de NO-IP; A importância de um roteador configurável; Enfim, é necessário todos estes conhecimentos para atingir o objetivo proposto. Poderá ser observado nos capítulos seguintes, a importância da teoria aqui descrita e referenciada, na instalação, na configuração, e no uso das soluções de monitoramento de links e redes aqui estudadas.

CAPÍTULO Nº 4 – DESENVOLVIMENTO DO PROJETO DE CUSTOMIZAÇÃO DE MONITORAMENTO DE LINKS E REDES

Este projeto iniciou-se com a pesquisa e seleção de duas soluções de monitoramento de links e redes que fossem de distribuição gratuita, e estivessem sendo consideradas como das melhores entre as existentes. Outra pesquisa e seleção foi feita para se definir o sistema operacional a ser utilizado, que também fosse distribuído através de licença GPL. Como resultado foram escolhidos o sistema operacional CentOS, e as ferramentas de monitoramento Centreon e Zabbix.

Após estudo destes *softwares*, iniciou-se a instalação, e após algumas dificuldades, optou-se por utilizar a ferramenta FAN para instalar de forma integrada o CentOS e o Centreon, e posteriormente instalou-se o Zabbix, seguindo instruções contidas no anexo A deste projeto.

Outra fase que exigiu bastante estudo e testes refere-se às configurações destas ferramentas, e dos demais recursos utilizados, e que resultaram na topologia da rede a ser monitorada.

Seguiu-se a fase de testes e ajustes na configuração, que resultou nos gráficos e alertas aqui apresentados.

Finalmente foram analisados e comparados os resultados obtidos, e elaborado um resumo das características, vantagens e desvantagens de cada ferramenta, e feito um comparativo entre elas, naquilo que tem em comum, indicando-se aquela considerada como a que apresentou melhores qualidades.

Os procedimentos para instalação e configuração das ferramentas e dos outros recursos, a topologia da rede implantada, os gráficos e alertas obtidos como resultado dos testes, e as conclusões deste trabalho, são apresentadas a seguir.

4.1 - Visão Geral do Projeto

O cenário idealizado para o projeto é constituído de uma central de monitoramento composta de um servidor de monitoramento, um ultrabook, uma estação de trabalho, um roteador, e um modem, situada em instalação residencial. Externamente, compõem-se de 4 servidores de rede de filiais de uma empresa e seus respectivos modems, cada filial localizada

em um ponto do DF, e mais um servidor de rede de outra empresa também instalado no DF, e o seu modem . Este cenário pode representar a realidade de várias redes de empresas na atualidade. A estrutura da rede é apresentada na figura 4.1, e os seus componentes são descritos logo a seguir. No caso o provedor de acesso internet do servidor de monitoramento é a empresa GVT, mas poderia ser qualquer outro que forneça este serviço.

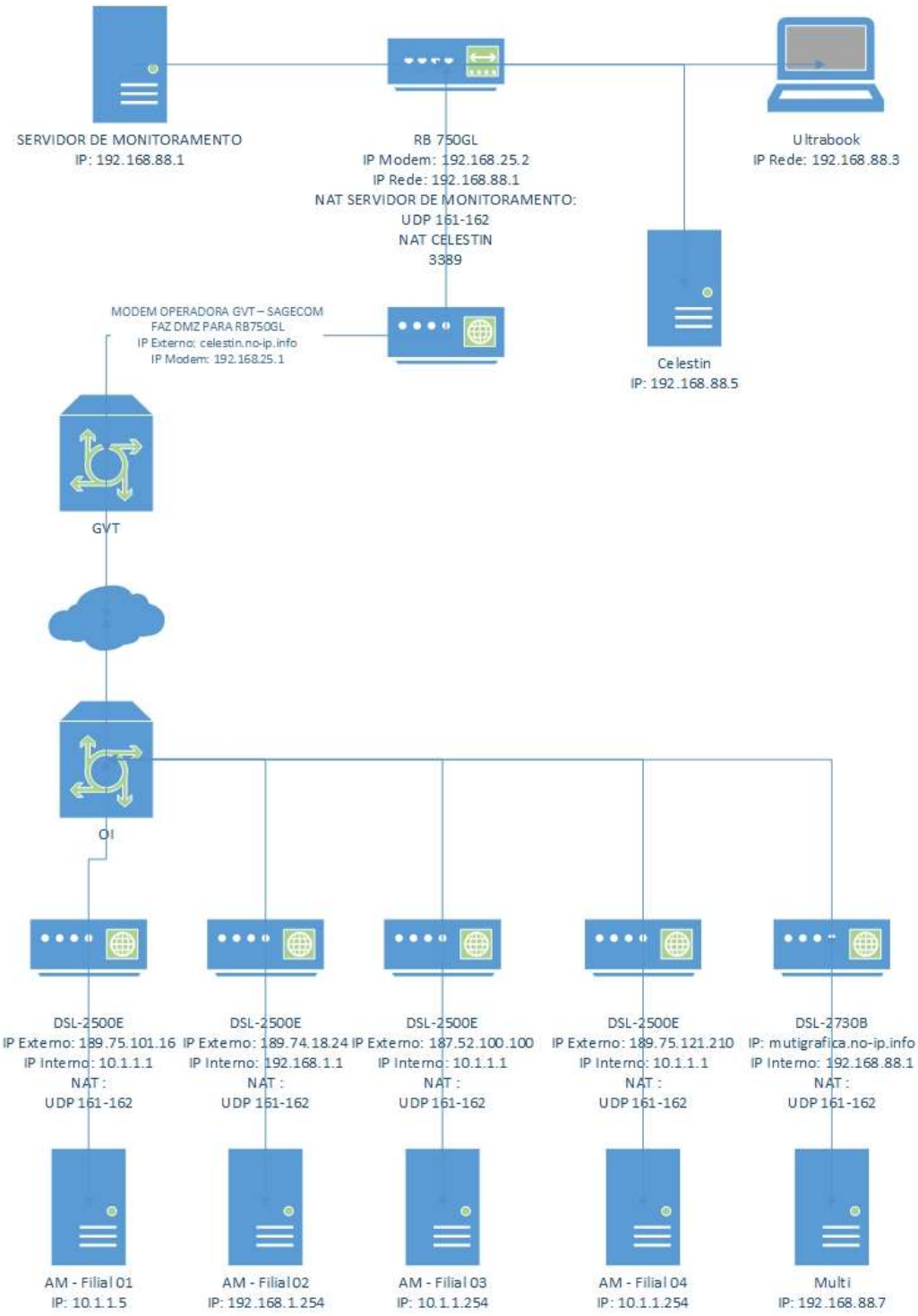

Figura 4.1 – Cenário elaborado para o projeto (Autor do Projeto, 2013)

Relação de equipamentos e função deles no cenário elaborado:

Central de Monitoramento (residência)

. 1 SERVIDOR DE MONITORAMENTO - Servidor Montado – Soyo (celestin.no-ip.info).

Servidor responsável pelo monitoramento de toda rede.

IP 192.168.88.1

. 1 Desktop Montado – Assus (Celestin)

Agente a ser monitorado onde será passará todo o trafego de voz, dados e vídeo.

IP 192.168.88.5

. 1 Ultrabook Sansung NP530U3C

Agente a ser monitorado, no qual serão provocadas situações críticas ou de falha.

IP 192.168.88.3

. 1 Roteador - RB750GL

Agente a ser monitorado e responsável pelo redirecionamento de portas.

IP Modem 192.168.25.2; IP Rede 192.168.88.1

NAT SERVIDOR DE MONITORAMENTO UDP 161-162

NAT CELESTIN 3389

. 1 Modem operadora GVT - SAGECOM

Responsável para interligar a rede externa com o roteador RB750GL.

Faz DMZ para o roteador RB750GL.

IP externo celestin.no-ip.info; IP modem 192.168.25.1

AM-Filial01

. 1 Servidor - HP Proliant Gen 8 ML350

Agente a ser monitorado externamente.

IP 10.1.1.5

. 1 Modem roteador DSL-2500E – Router Internet

Roteador responsável pela entrada, saída e o redirecionamento através de NAT.

IP Externo 189.75.101.16; IP Interno 10.1.1.1

NAT: UDP 161-162

AM-Filial02

. 1 Servidor - IBM X3100 M4

Agente a ser monitorado externamente.

IP 10.1.1.5

. Modem roteador DSL-2500E – Router Internet

Roteador responsável pela entrada, saída e o redirecionamento através de NAT.

IP Externo 189.74.18.24; IP Interno 192.168.1.1

NAT: UDP 161-162

AM-Filial03

. 1 Servidor - IBM X3100 M4

Agente a ser monitorado externamente.

IP 10.1.1.254

. Modem roteador DSL-2500E – Router Internet

Roteador responsável pela entrada, saída e o redirecionamento através de NAT.

IP Externo 187.52.100.100; IP Interno 10.1.1.1

NAT: UDP 161-162

AM-Filial04

. 1 Servidor - IBM X3100 M4

Agente a ser monitorado externamente.

IP 10.1.1.254

. Modem roteador DSL-2500E – Router Internet

Roteador responsável pela entrada, saída e o redirecionamento através de NAT.

IP Externo 189.75.121.210; IP Interno 10.1.1.1

NAT: UDP 161-162

Servidor Multi

. 1 Servidor DELL

Agente a ser monitorado externamente.

IP 192.168.88.7

. 1 Modem roteador DSL-2730B

Roteador responsável pela entrada, saída e o redirecionamento através de NAT.
IP Externo multigrafica.no-ip.info; IP Interno 192.168.88.1

NAT: UDP 161-162

Para o conjunto funcionar são utilizadas ferramentas como IP Fixo, NO-IP, NAT e SNMP. Estas técnicas permitem que o roteador se comunique com os equipamentos monitorados na residência e com os equipamentos monitorados externamente. O monitoramento é realizado com as ferramentas Zabbix e Centreon rodando no sistema operacional CentOS.

Este cenário visa o monitoramento dos links dos servidores instalados em diversos locais do Distrito Federal, utilizando o servidor de monitoramento da central, mesmo os equipamentos monitorados estando em redes segmentadas e distintas.

4.2 - Etapas do Projeto

Inicialmente foram realizadas pesquisas para definição do sistema operacional, das ferramentas de monitoramento, e de outros recursos necessários para a execução do projeto.

Em seguida, foram adquiridos componentes e realizada a montagem um computador para ser utilizado como servidor de monitoramento.

Com a necessidade de um roteador para viabilizar a comunicação do servidor de monitoramento com os links monitorados, foi adquirido o roteador RB750GL, que tem ótimo desempenho e é de baixo custo.

Estudou-se as portas necessárias e o redirecionamento adequado, para o monitoramento da WAN, e definiu-se os parâmetros para a configuração do serviço SNMP.

Para se mostrar o potencial de monitoramento das ferramentas Zabbix e Centreon foi necessário instalar e configurar os softwares, os ativos de rede e os serviços, de maneira a criar as condições adequadas para o monitoramento da rede. As principais instalações e configurações realizadas foram na sequencia:

. Modem GVT e habilitação da DMZ.

. Roteador RB750GL e NATs.

. Sistema operacional CentOS e o Centreon instalados em um mesmo processo.

. Ferramenta Zabbix.

. SNMP no Windows 2008 serve dos servidores monitorados.

. Configurações finais de ajuste das soluções.

Com as soluções de monitoramento configuradas e em funcionamento, foram registrados, analisados e documentados os gráficos produzidos como resultado deste monitoramento.

Também foram realizados testes de carga na rede, utilizando transporte de dados, voz, e vídeo, e analisados e apresentados os resultados.

Finalmente, foi efetuada simulação de interrupções nos links, e verificado os alertas apresentados em tela, e enviados por email, registrando os resultados obtidos.

4.3 - Implementação do Projeto

4.3.1 - Instalação e configuração dos principais recursos deste trabalho

A instalação e configuração de distribuições do Linux, e ferramentas desenvolvidas para este sistema operacional, não são efetuadas de maneira simples para o usuário, como é no caso do Windows. Pelo contrário, na maioria dos casos só é executada de maneira correta por um técnico com conhecimento destes softwares. Neste item serão apresentados os principais passos realizados neste trabalho para a instalação e configuração do sistema operacional CentOS, das ferramentas de monitoramento Centreon e Zabbix, de ativos da rede, e de outras ferramentas e recursos utilizados para execução do projeto.

4.3.1.1 – Configuração do modem GVT, e habilitação da DMZ

É necessário saber o IP do modem. Utiliza-se o comando cmd, para ter acesso ao prompt do DOS, quando digita-se o comando ipconfig /all, e será mostrada a tela apresentada na Figura 4.2 a seguir.

Figura 4.2 – Resultado do comando ipconfig mostrando o IP do modem GVT (C:\windows\system32\cmd.exe, 18/10/2013)

Após conhecer o endereço do modem ADSL, acessa-se o endereço da WEB 192.168.25.1, quando surge a tela mostrada na Figura 4.3 a seguir.

Figura 4.3 – Tela de login do endereço 192.168.25.1 (192.168.25.1, 18/10/2013)

Será solicitado o nome do usuário e a senha, normalmente informados pela operadora ou constante no manual do modem.

Liga-se um cabo de rede para conexão da LAN do modem com a WAN do roteador RB750GL.

Feito o login, seleciona-se Configurações\Rede Local

Neste passo será configurado o roteador, e associado o endereço MAC ao endereço IP, neste caso a *routerboard* RB750GL (Mikrokit), tendo sido definido o endereço IP 192.168.25.2 conforme apresentado na Figura 4.4 a seguir.

Figura 4.4 – Tela de configuração do modem GVT

Após esta configuração seleciona-se a opção DMZ na tela Power Box GVT apresentada na Figura 4.5 a seguir, escolhe-se a opção Habilitar, redireciona-se o endereço IP para o roteador RB750GL fornecendo o endereço 192.168.25.2 da *routerboard*. Ao clicar em Salvar, a DMZ está configurada.

Figura 4.5 - Tela de configuração e habilitação da DMZ do modem GVT (Power Box GVT, 18/10/2013)

Após estas configurações, todos os equipamentos que serão conectados ao roteador RB750GL, como é o caso ddo desktop e do ultrabook, tem que ser redirecionados para o endereço IP do roteador, e configuradas as entradas e saídas de portas, conforme a seguir:

IP 192.168.88.3, Máscara 255.255.255.0, Gateway 192.168.88.1, DNS 192.168.88.1.

4.3.1.2 – Configuração do roteador RB750GL e das NATs

O próximo passo é configurar o roteador RB750GL para fazer as NATs (*Network Address Translation*) para o servidor de Monitoramento.

Para o acesso ao roteador RB750GL é necessário fazer o download e instalação do winbox, que é baixado do site http://wirelessconnect.eu/articles/winbox_download, 18/10/2013. Após a instalação, na área de trabalho, clica-se no ícone do winbox, que aparece na figura 4.6 a seguir.

Figura 4.6 - Área de trabalho com o ícone do winbox

Surgirá a tela apresentada na Figura 4.7 a seguir, so licitando o login e a e a senha.

Figura 4.7 – Tela de login no winbox

Depois de acessado, seleciona-se IP/FIREWALL/NAT, para configurar os redirecionamentos de portas. Ao clicar no símbolo de +, surge a tela apresentada na Figura 4.8, que permite a configuração uma NAT.

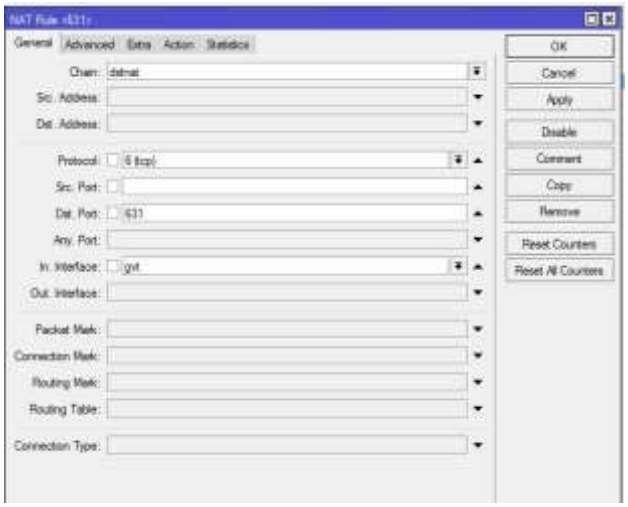

Figura 4.8 – Tela de configuração de NAT entrada – aba general

Primeiro configura-se NATs de entrada.

Em Chain sempre se digita dsnat.

Em protocol coloca-se a porta de destino, neste caso 6 (tcp).

Em In. Interface fornece-se a porta de destino, neste caso gvt.

Após fornecer estes parâmetros, seleciona-se a aba Action, sendo apresentada a tela apresentada na Figura 4.9 a seguir.

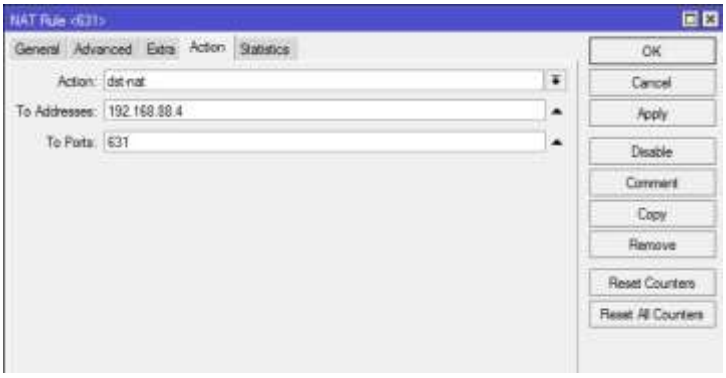

Figura 4.9 - Tela de configuração de NAT – aba Action.

Em Action digita-se dst-nat,.em To adresses digita-se o endereço IP 192.168.88.4, e em To Ports o endereço 631. Para terminar a configuração clica-se em OK.

Estes passos são repetidos para todas as portas, que são a 161(udp), a 162(udp), a 631(tcp), e a 80(tcp) redirecionando-as para o servidor de monitoramento 192.168.88.4.

Os endereços para configuração das NATs do servidor de monitoramento, entrada e saída encontram-se na Tabela 10.

Tabela 10 – Endereços das NATs do servidor de monitoramento

Descrição	NAT
Zabbix	161 UDP
UDP	161/162 UDP
Acesso Via Putty	2221 TCP
Acesso Via Navegador	80 TCP

O endereço para configuração da NAT para o servidor Celestin (Interno), usado para auxiliar a demonstração encontra-se na Tabela 11.

Tabela 11 – Endereço da NAT para servidor Celestin

Descrição	Nat
RDP	3389

Repetir para toda a porta 3389(tcp), redirecionando para o servidor de monitoramento 192.168.88.5, para acesso remoto.

Para configuração de uma NAT de saída, utiliza-se a tela do winbox, aba General para fornecer os parâmetros apresentados na Figura 4.10 a seguir.

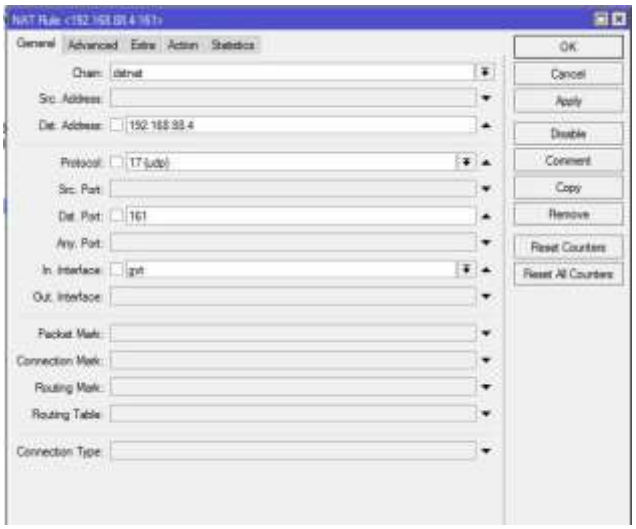

Figura 4.10 - Tela de configuração de NAT saída – aba general

Digita-se dstnat em Chain, 192.168.88.4 em Dst. Address, 17(udp) em protocol, e gvt em In. Interface.

Após fornecer estes parâmetros, seleciona-se a aba Action, sendo apresentada a tela apresentada na Figura 4.11 a seguir.

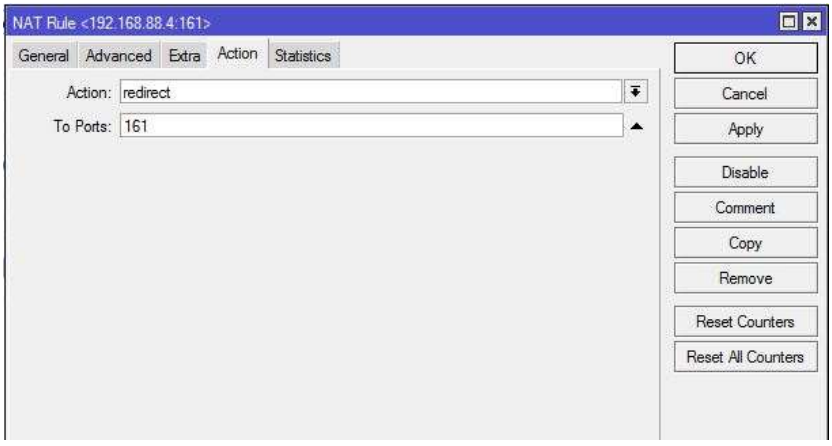

Figura 4.11 - Tela de configuração de NAT saída – aba Action.

Em Action digita-se redirect, e em To Ports: 161.

Para terminar a configuração clica-se em OK.

Após configurar a porta 161, repete-se os dois passos anteriores para a porta 199.

Como os modens ADSL conectados aos servidores monitorados são do mesmo modelo e ligados à operadora OI, será mostrado como exemplo, a configuração de um deles.

Para saber o endereço IP do modem executa-se o comando cmd, e no prompt digita-se ipconfig /all, surgindo a tela apresentada na Figura 4.12 a seguir

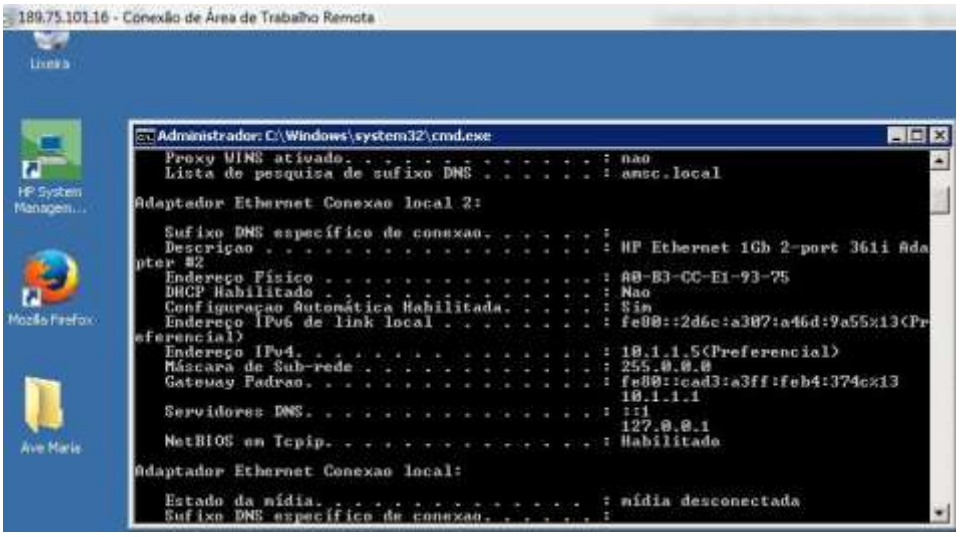

Figura 4.12 – Resultado do comando ipconfig em um servidor monitorado.

Após obter esta informação, acessa-se através de um navegador WEB o endereço 10.1.1.1, e é mostrada a tela de login apresentada na Figura 4.13 a seguir.

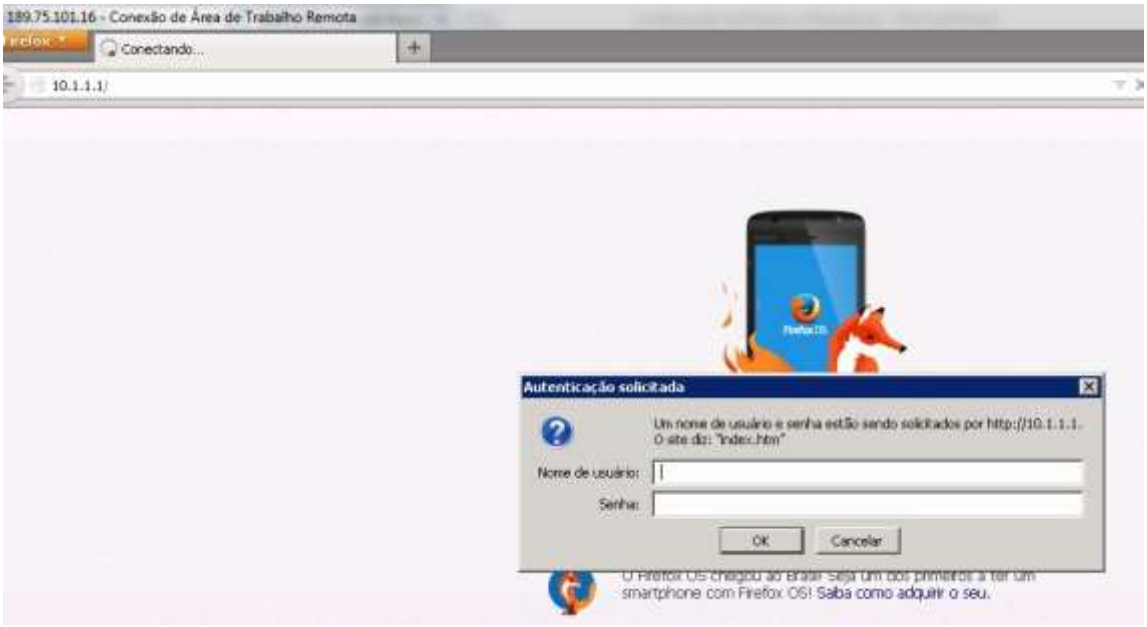

Figura 4.13 – Tela de login para configuração de modem de um servidor monitorado

Será solicitado login e senha. Normalmente são oferecidos pela operadora ou vem no manual do modem.

Surge a tela apresentada na Figura 4.14 a seguir.

Figura 4.14 – Tela inicial de configuração do modem D-Link

Clica-se na caixa ADVANCED e surge a tela apresentada pela figura 4.15 a seguir.

Figura 4.15 – Tela de configuração do modem D-Link

Em PORT FORWARDING SETUP são fornecidos os dados de configuração dos encaminhamentos de porta,

Na tabela 12 a seguir são apresentados os endereços para configuração de cada modem conectado aos servidores monitorados.

Tabela 12 – Endereços das NATs dos servidores monitorados

Host Name / Alias	Endereço de IP	Endereço de destino
AM-Filial01	189.75.101.16	10.1.1.5
AM-Filial02	189.74.18.24	192.168.1.254
AM-Filial03	189.75.121.210	10.1.1.254
AM-Filial04	187.52.100.100	10.1.1.254
Multi	multigrafica.no-ip.info	192.168.88.7

4.3.1.3 - Instalação do sistema operacional CentOS e da ferramenta Centreon

Para esta instalação utiliza-se a ferramenta denominada FAN, que, a partir de alguns parâmetros, realiza toda a instalação e a configuração do conjunto de forma automática.

Acessa-se o site http://www.fullyautomatednagios.org/wordpress/download/ (16/10/2013).

Seleciona-se para download a opção FAN 2.4-i386, MIRROR1, para baixar o arquivo FAN-2.4-i386.iso.

Grava-se o arquivo em CD ou DVD.

Efetua-se o boot pelo CDROM com a ISSO do FAN.

Este aplicativo instala automaticamente o CentOS, Centreon, MYSQLl server, Nagios, e os plugins necessários.

Ao iniciar, o programa apresenta a tela mostrada na Figura 4.16.

Figura 4.16 - Tela para definição do modo de instalação do FAN. (http://www.fullyautomatednagios.org/wordpress/documentation/how-to-install-fan/, 16/10/2013)

Tecla-se ENTER para prosseguir com a instalação padrão que é em modo gráfico.

A próxima tela, apresentada na Figura 4.17, solicita a linguagem a ser utilizada

Figura 4.17 – Escolha da linguagem a ser utilizada pelo FAN (http://www.fullyautomatednagios.org/wordpress/documentation/how-to-install-fan/, 16/10/2013)

Seleciona-se Português Brasil, e tecla-se na caixa OK.

A seguir é solicitado o tipo de teclado através da tela apresentada na Figura 4.18.

Figura 4.18 – Solicitação do tipo de teclado a ser utilizado pelo FAN (http://www.fullyautomatednagios.org/wordpress/documentation/how-to-install-fan/, 16/10/2013)

Seleciona-se ABNT2, e tecla-se na caixa OK.

Na próxima tela, apresentada na Figura 4.19 a seguir, solicita-se os dados para definição da partição do disco.

Figura 4.19 – Solicitação de dados para a partição pelo FAN (http://www.fullyautomatednagios.org/wordpress/documentation/how-to-install-fan/, 16/10/2013)

Deve-se pressionar a caixa NEXT para prosseguir com a instalação padrão que é utilizar o espaço disponível e o layout padrão.

O último parâmetro solicitado é a definição da região e do fuso horário, que é feito através da tela apresentada na Figura 4.20 apresentada a seguir.

Figura 4.20 – Solicitação de região e fuso horário pelo FAN (http://www.fullyautomatednagios.org/wordpress/documentation/how-to-install-fan/, 16/10/2013)

Seleciona-se a opção América/São Paulo e tecla-se na caixa NEXT

Finalmente é solicitada a senha a ser utilizada pelo administrador através da tela apresentada pela Figura 4.21 a seguir.

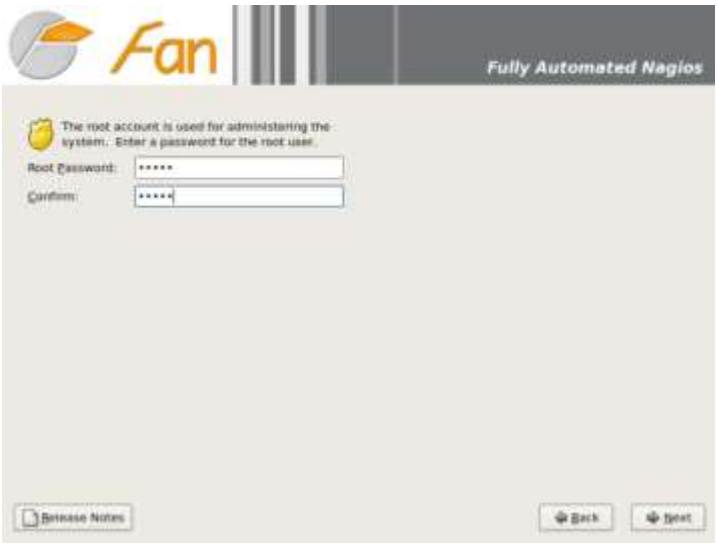

Figura 4.21 – Fornecimento de senha de administrador para o FAN (http://www.fullyautomatednagios.org/wordpress/documentation/how-to-install-fan/, 16/10/2013)

O padrão é nagiosadmin, porém pode-se definir outra senha, que deverá ser anotada.

A partir daí, a instalação do sistema operacional CentOS, da ferramenta de monitoramento Centreon, e demais componentes do pacote, será toda feita automaticamente.

Ao final da instalação, será apresentada a tela informando sobre o término da instalação, apresentada na figura 4.22 a seguir.

Figura 4.22 – Informação de instalação bem sucedida do FAN (http://www.fullyautomatednagios.org/wordpress/documentation/how-to-install-fan/, 16/10/2013)

Tecla-se na caixa Reboot para reinicializar o sistema.

Caso não seja exibida esta tela, pode ter-se fornecido parâmetros de partição errados quando do início da instalação. Esta instalação é totalmente automática e bastante utilizada pelos usuários dessa ferramenta, portanto, se não conseguir terminar a instalação com sucesso, deve haver problemas no hardware onde os softwares estão sendo instalados.

Quando do primeiro acesso à nova plataforma, será necessário fornecer algumas outras informações de configuração, que são os parâmetros de rede, tais como endereço de IP, DNS, e outros, como nome da máquina, e outros dados. Portanto, quando do reboot, aparecerá a tela apresentada pela Figura 4.23 a seguir.

Figura 4.23 – Tela de seleção Setup Agent do FAN (http://www.fullyautomatednagios.org/wordpress/documentation/how-to-install-fan/, 16/10/2013)

Seleciona-se a opção Network configuration e tecla-se a caixa Run Tool. Surgirá a tela apresentada pela Figura 4.24 a seguir.

Figura 4.24 – Tela Select Action do FAN (http://www. fullyautomatednagios.org/wordpress/ documentation/how-to-install-fan/, 16/10/2013)

Primeiramente clica-se a opção Edit Devices e aparecerá a tela Select A Device apresentada na figura 4.25 a seguir.

Figura 4.25 – Tela Select A Device do FAN (http://www. fullyautomatednagios.org/wordpress/documentation/how-to-install-fan/, 16/10/2013)

Ao selecionar New Device aparecerá a tela Devernet Configuration mostrada na figura 4.26 a seguir.

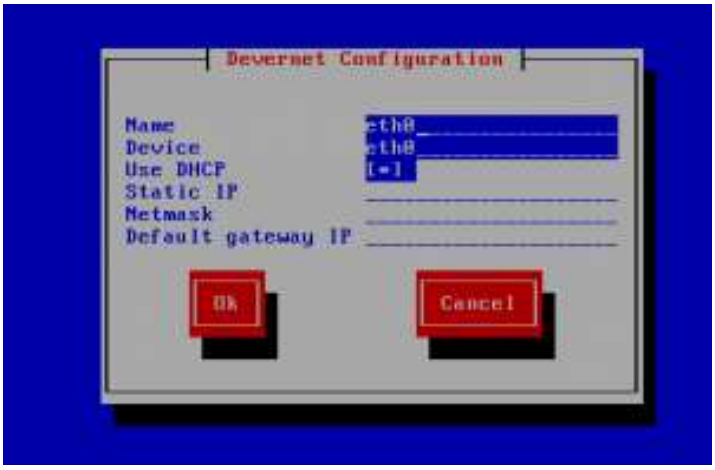

Figura 4.26 – Tela Devernet Configuration do FAN (http://www.fullyautomatednagios.org/wordpress/documentation/how-to-install-fan/, 16/10/2013)

Deve-se fornecer os dados solicitados e teca-se a caixa Ok. Esta operação deve se repetir para cada dispositivo que tiver que ser configurado.

Ao terminar, retorna-se à tela Select Action (Figura 4.14) e seleciona-se a opção Edit DNS configuration. Surge a tela DNS configuration apresentada na Figura 4.27 a seguir.

Figura 4.27 – DNS configuration do FAN (http://www.fullyautomatednagios.org/wordpress/documentation/how-to-install-fan/, 16/10/2013)

Fornece-se os dados solicitados e tecla-se a caixa Ok.

Ao término destas configurações todos os softwares deverão estar instalados e os dados configurados. Efetuar novo reboot.

Surge a tela de console do FAN apresentada pela figura 4.28, solicitando a senha de login, que foi fornecida ao FAN durante a instalação:

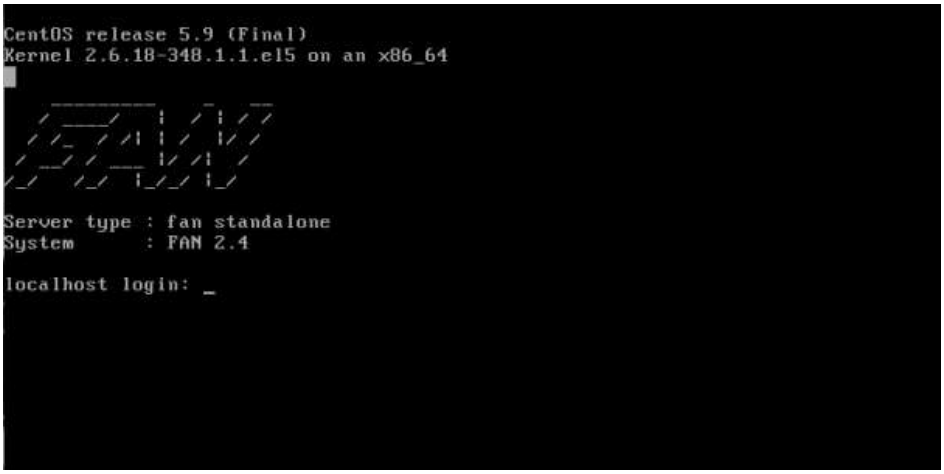

Figura 4.28 – Tela de console do FAN (http://aldoalves.wordpress.com/2013/05/19/instalando-o-fan-fully-automated-nagios-passo-a-passo/, 16/10/2013)

Agora pode-se usar o comando ifconfig para verificar o IP da interface de rede. Ao executa-lo aparece a tela a seguir, mostrada pela Figura 4.29.

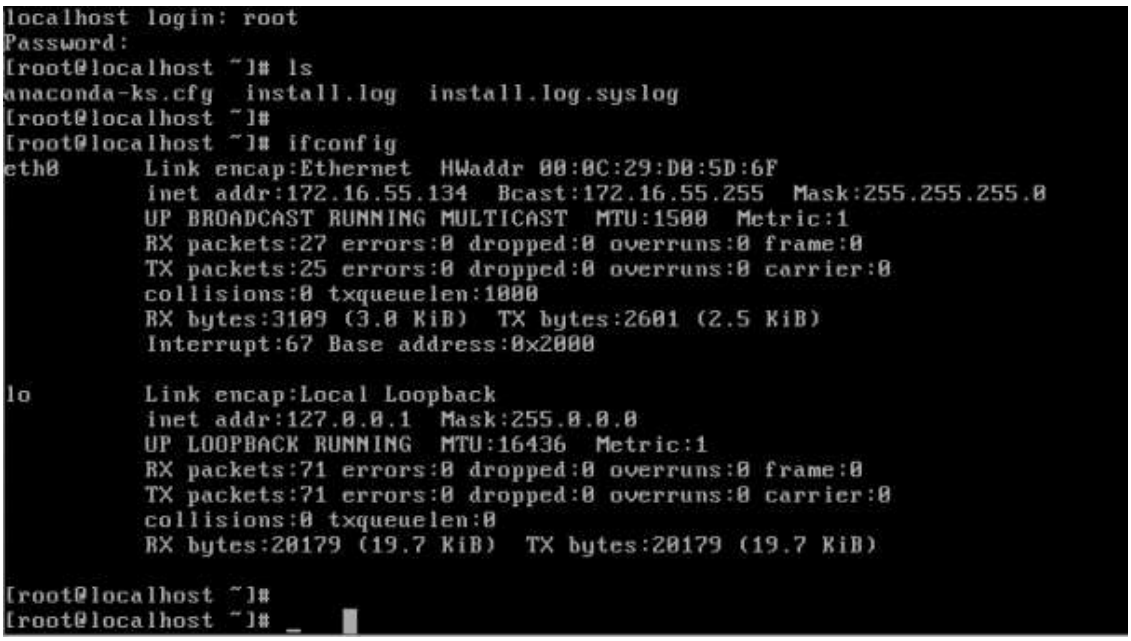

Figura 4.29 – Informações apresentadas pelo comando ifconfig (http://aldoalves.wordpress.com/2013/05/19/instalando-o-fan-fully-automated-nagios-passo-a-passo/, 16/10/2013)

Após a confirmação de que a interface subiu e que está ok, pode-se acessar a console do FAN pelo navegador Web conforme mostrado na figura 4.30 a seguir.

Figura 4.30 – Console do FAN (http://aldoalves.wordpress.com/ 2013/05/19/instalando-o-fan-fully-automated-nagios-passo-a-passo/, 16/10/2013)

Para configurar os hosts no Centreon acessa-se primeiramente o endereço na web da distribuição, 192.168.88.4/centreon/main.php?p=601. Surge a tela apresentada na Figura 4.31 a seguir.

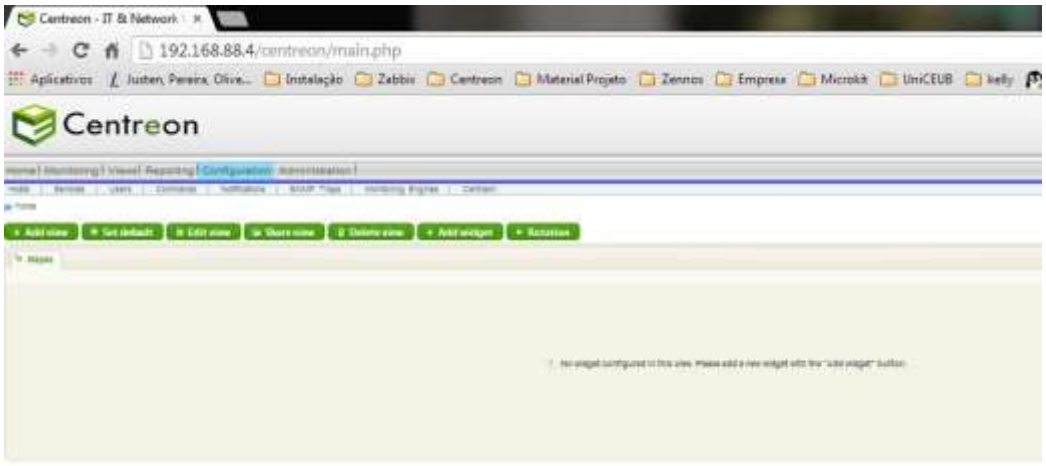

Figura 4.31 – Tela inicial do Centreon para configuração de hosts e serviços (192.168.88.4/centreon/main.php, 18/10/2013)

Seleciona-se a opção Configuration e após a opção Hosts. A página que aparece é apresentada na figura 4.32 a seguir.

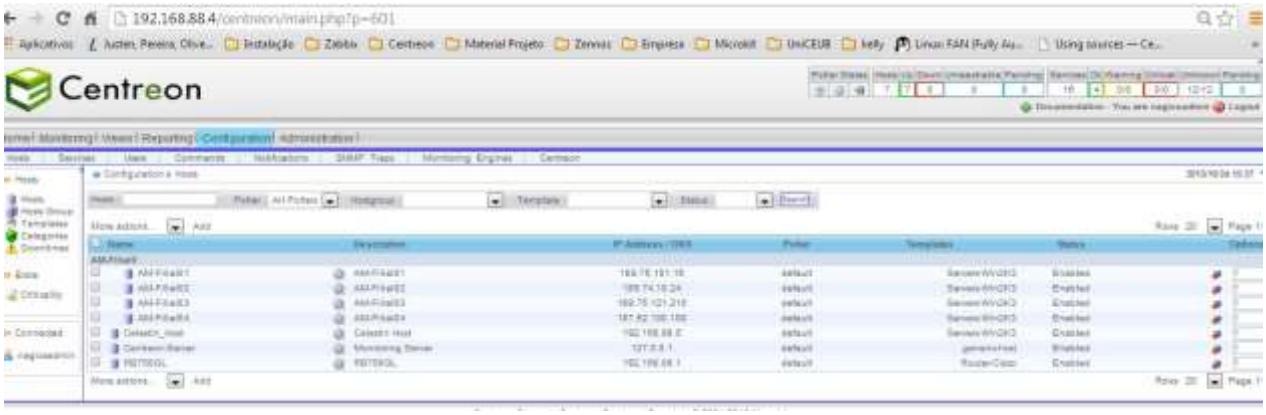

Figura 4.32 – Página resumo de hosts do Centreon (192.168.88.4/centreon/main.php?p=601, 18/10/2013)

É necessário acrescentar um Hostname/Alias, o IP do equipamento associado, e outros parâmetros, para cada equipamento a ser monitorado. Para cada inclusão clicar na opção Add e surgirá a tela apresentada na Figura 4.33 a seguir.

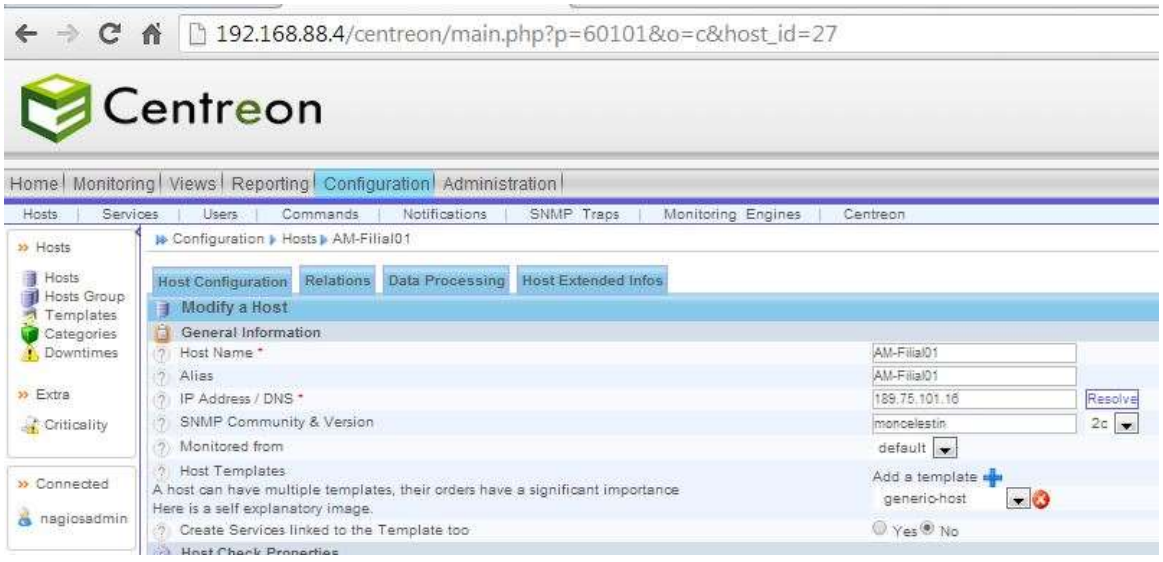

Figura 4.33 – Tela de configuração de host da AM-Filial01 (http://192.168.88.4/centreon/main.php?p=60101&o=c&host_id=27, 18/10/2013)

Em Host Name e Alias digita-se AM-Filial01; Em IP Address / DNS o endereço do IP, neste caso 189.75.101.16.

Todos os hosts incluídos farão parte de uma comunidade denominada moncelestin, que deverá ser configurada em SNMP Community & Version. A comunidade moncelestin constitui o ambiente de rede que será enxergado pelas ferramentas de monitoramento.

Em Monitored from seleciona-se default e em Add a template seleciona-se generic-host.

Configurar os endereços dos hosts no Centreon conforme a Tabela 13.

Tabela 13 - Endereços dos hosts no Centreon

Host Name / Alias	Endereço de IP
RB750GL	192.168.88.1
Ultrabook	192.168.88.3
Celestin	192.168.88.5
AM-Filial01	189.75.101.16
AM-Filial02	189.74.18.24
AM-Filial03	189.75.121.210
AM-Filial04	187.52.100.100
Multi	multigrafica.no-ip.info

Para efetuar a configuração dos serviços seleciona-se a aba Configuration, nela a sub-aba Commands, e clica-se em Checks. Surge a tela apresentada na Figura 4.34 a seguir.

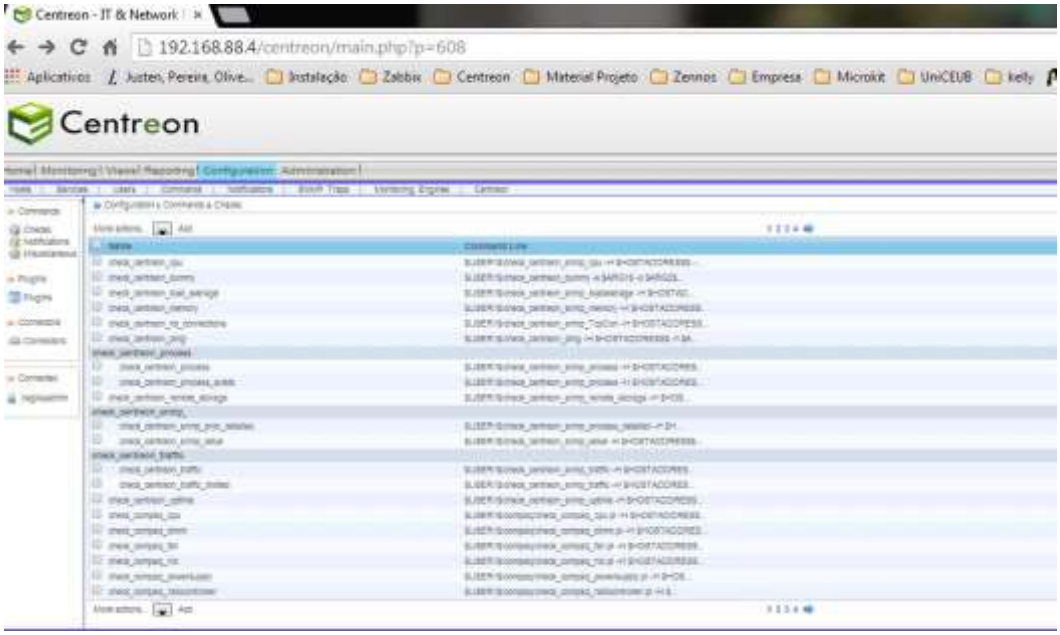

Figura 4.34 – Tela de configuração de serviços – Cheks (192.168.88.4/centreon/main.php?p=608, 18/10/2013)

Surge a lista de Checks que podem ser selecionados clicando-se a caixinha existente à frente de cada um. Porém, é preciso alterar o Check denominado check_centreon_traffic. Ao clicar na linha correspondente surge a tela apresentada pela Figura 4.35 a seguir.

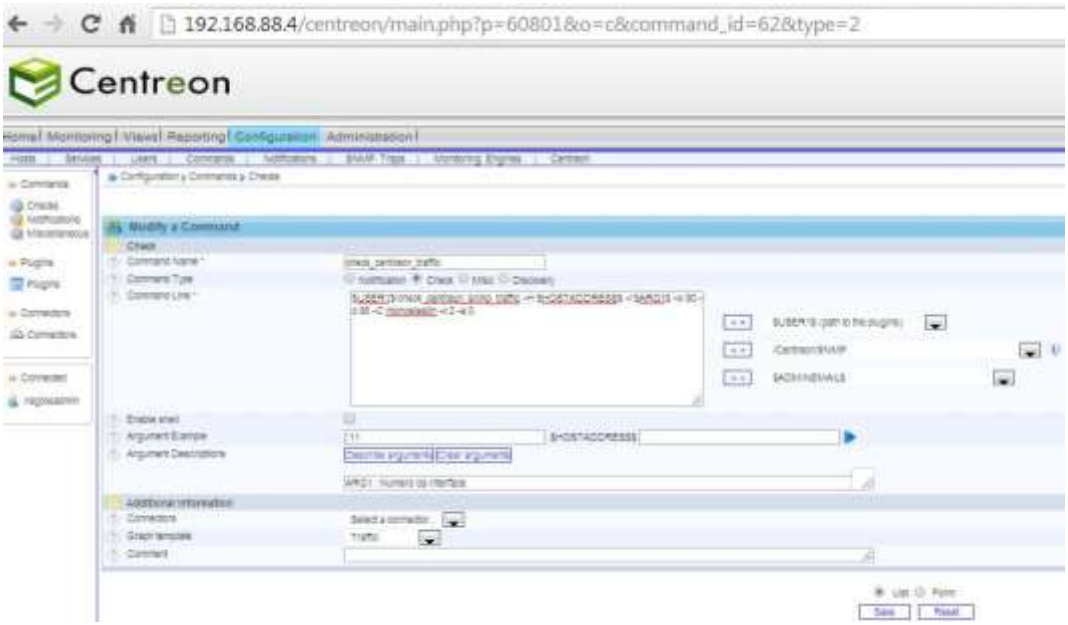

Figura 4.35 – Tela de configuração de serviços – Modificação de comando (192.168.88.4/centreon/main.php?p=60801&o=c&command_id=62&type=2, 18/10/2013)

Em Command Name digita-se o comando check_centreon_traffic, em Command Type a opção Check, e em command Line digita-se $USER1$/check_centreon_snmp_traffic -H $HOSTADDRESS$ -i $ARG1$ -w 80 -c 95 -C moncelestin -v 2 -a 0. Em Argument Example digita-se !11, em Argument Descriptions digita-se ARG1 : Numero da Interface, e finalmente clica-se em Save.

Retorna-se a tela anterior, seleciona-se outro serviço desejado e repete-se a operação.

Ainda é necessário salvar os arquivos configurados. Seleciona-se a aba Configuration, sub-aba Monitoring engines, opção Generate, e surge a tela apresentada na Figura 4.36.

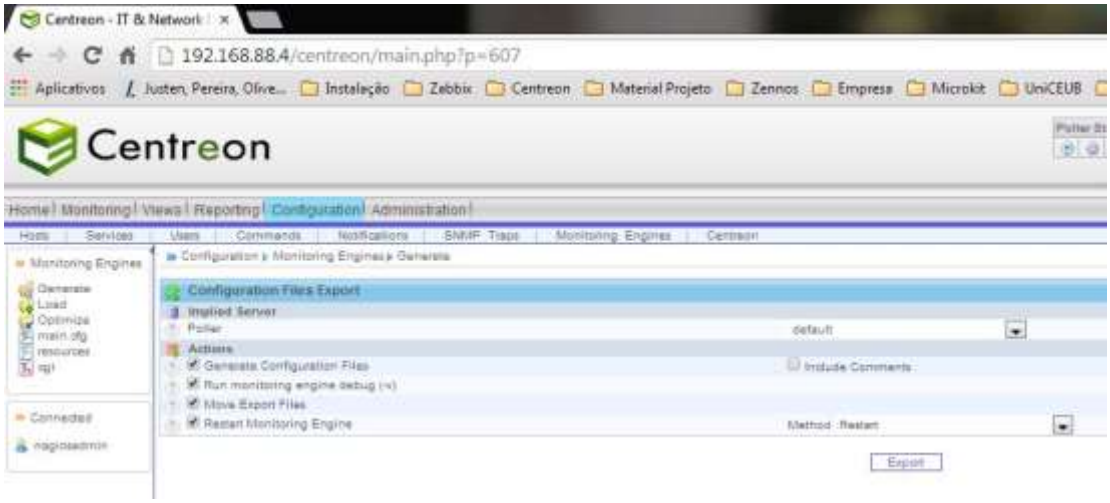

Figura 4.36 – Tela de exportação de configuração do Centreon (192.168.88.4/centreon/main.php?p=607, 18/10/2013)

Habilita-se todas as opções e clica-se em Export.

Por último é necessário informar ao SNMP qual a comunidade que será monitorada pelo Centreon. Seleciona-se a aba Administration, sub-aba Options, opção SNMP, e surgirá a tela apresentada na Figura 4.37 a seguir.

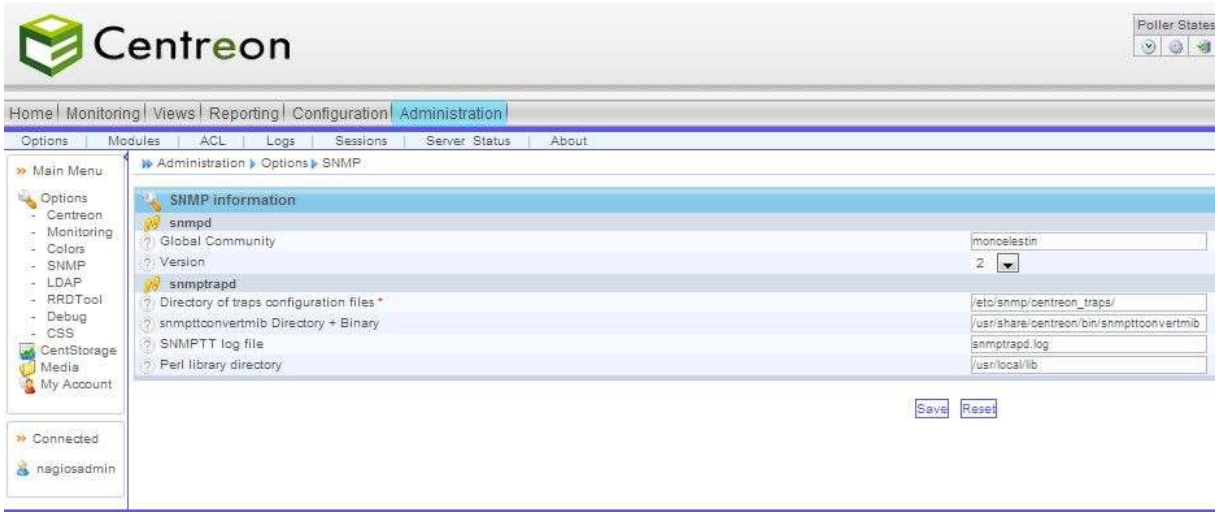

Figura 4.37 – Informações da comunidade monitorada para o SNMP - Centreon.

Fornece-se as informações a seguir: Em Global Community, moncelestin; Em Version, 2; Em Directory of traps Configuration files, /etc/snmp/centreon_trap; Em snmpttconvertmib Directory + Binary, /usr/share/centreon/bin/snmpttconvertmib; Em SNMPTT log file, snmptrapd.log; Em Perl library directory, usr/local/lib.

Clica-se na caixa SAVE, para armazenar estas informações.

Agora tem-se o Centreon configurado.

Seleciona-se a aba Monitoring, sub-aba Services, opção All Services, e é apresentada a tela apresentada na Figura 4.38 com a relação de hosts e serviços sendo monitorados.

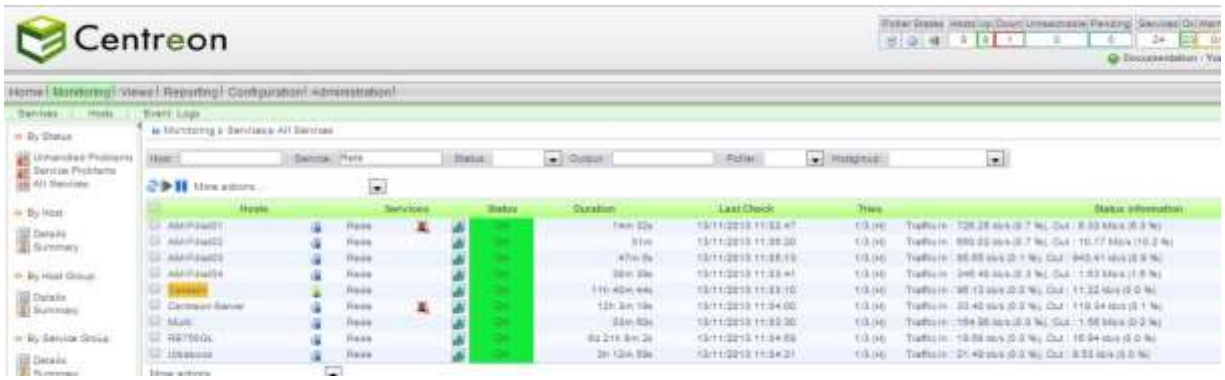

Figura 4.38 - Tela com a relação de hosts e serviços cadastrados no Centreon (192.168.88.4/centreon/main.php?p=20201&o=svc, 13/11/2013)

4.3.1.4 - Instalação da ferramenta Zabbix no servidor.

A instalação e configuração inicial da ferramenta de monitoramento Zabbix, é realizada conforme as instruções de instalação existentes no site http://www.vivaolinux.com.br/artigo/Zabbix-2-no-CentOS-6-Instalacao-e-configuracao, 16/10/2013. No ANEXO B – INSTRUÇÕES E COMANDOS PARA INSTALAÇÃO DO ZABBIX, são apresentados todos os passos e comandos necessários para realização da instalação e configuração inicial desta ferramenta.

Executados os passos constantes do ANEXO B, é necessária a configuração dos hosts e dos serviços no Zabbix.

Para configurar os hosts do Zabbix, entra-se no navegador através do endereço do IP: http://192.168.88.4/zabbix, seleciona-se a aba Configuração e a sub-aba Hosts (em amarelo), e é mostrada a tela apresentada na figura 4.39 a seguir.

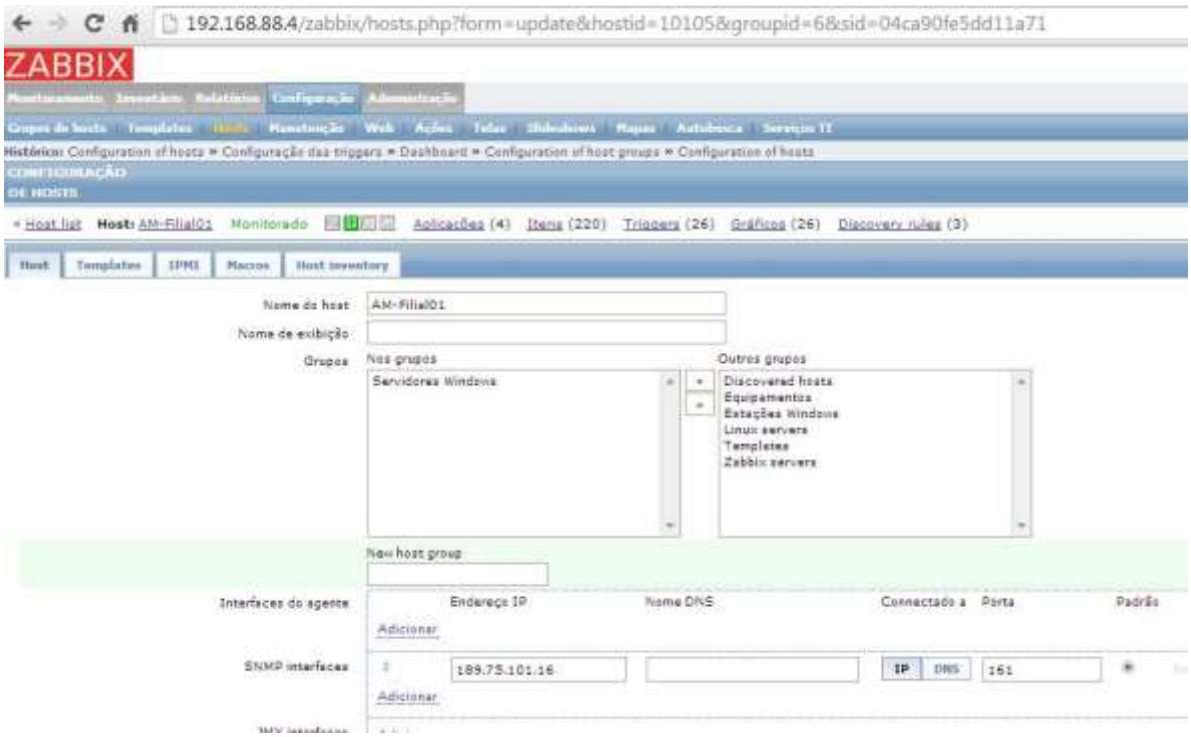

Figura 4.39 - Configuração dos hosts do Zabbix (192.168.88.4/Zabbix/hosts.php?form=update&hostid=10085&groupid=0&sid=4b0f23eff9040123, 16/10/2013)

Na caixa Nome do host digita-se o nome do host a ser configurado, neste caso AM-Filial01; Na caixa Grupos seleciona-se um grupo de hosts listados na caixa à esquerda e transfere-o para a caixa da esquerda, no caso Servidores Windows; Na caixa Endereço IP digita-se o IP associado ao host, no caso 189.75.101.16; Na caixa Conectado aparece IP e DNS; Na caixa porta colocar a porta a ser utilizada, no caso 161; Na caixa Monitorado por proxy seleciona-se (sem proxy); E em Status seleciona-se Monitorado.

Seleciona-se a sub-aba Templates, localizada à esquerda da sub-aba Host, e surge a pup-up apresentada na Figura 4.40 a seguir.

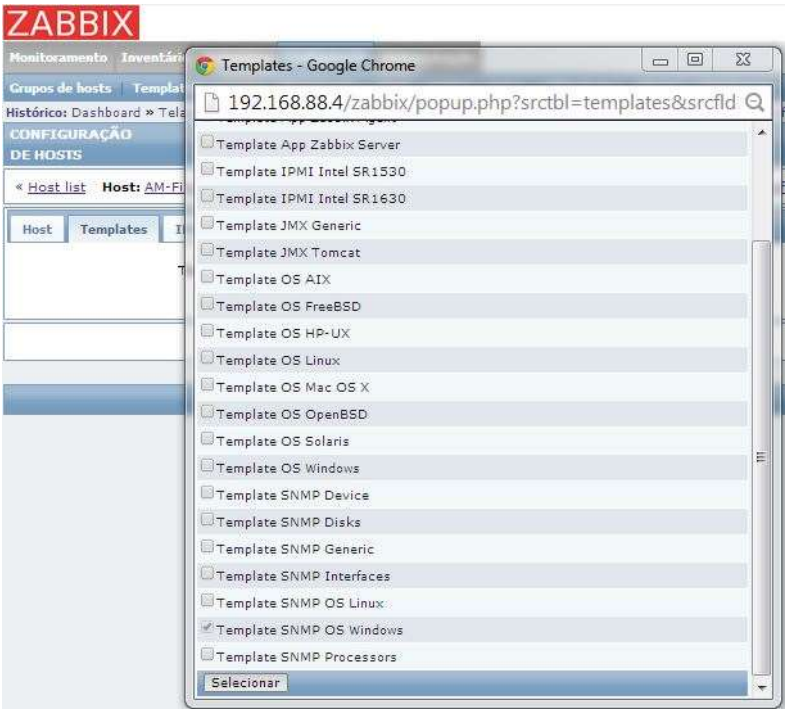

Figura 4.40 – Pup-up para escolha de template no Zabbix (192.168.88.4/Zabbix/popup.php?srctbl=templates&srcfld, 16/10/2013).

Seleciona-se o template desejado, no caso Template SNMP OS Windows.

Retorna-se a tela anterior e clica-se na caixa Salvar.

Os passos de configuração dos hosts no Zabbix mostrados até aqui, são repetidos para todos os outros, alterando-se os dados constantes da Tabela 14 a seguir, mantendo-se os demais conforme o primeiro host configurado.

Tabela 14 – Informações para configuração dos hosts no Zabbix.

Nome do Host / Nome de Exibição	Grupo	Endereço de IP
RB750GL	Equipamentos	192.168.88.1
Ultrabook	Estações Windows	192.168.88.3
Celestin	Servidores Windows	192.168.88.5
AM-Filial01	Servidores Windows	189.75.101.16
AM-Filial02	Servidores Windows	189.74.18.24
AM-Filial03	Servidores Windows	189.75.121.210
AM-Filial04	Servidores Windows	187.52.100.100
Multi	Servidores Windows	multigrafica.no-ip.info

Agora é necessário criar um mapa da rede a ser monitorada, conforme diagrama de projeto apresentado na figura 4.1. Para isto Seleciona-se a aba Configuração, e a sub-aba Mapas, mostrando a tela apresentada na Figura 4.41 a seguir.

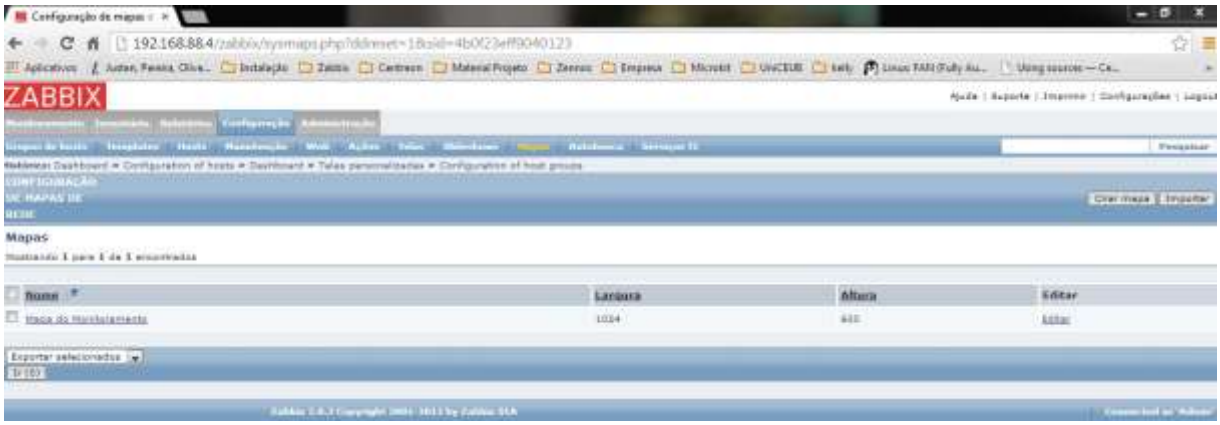

Figura 4.41 – Tela inicial de mapas do Zabbix (192.168.88.4/Zabbix/sysmaps.php?ddreset=1&sid=4b0f23eff9040123, 16/10/2013)

Clica-se na caixa Criar mapa, e surge a tela apresentada na Figura 4.42 a seguir.

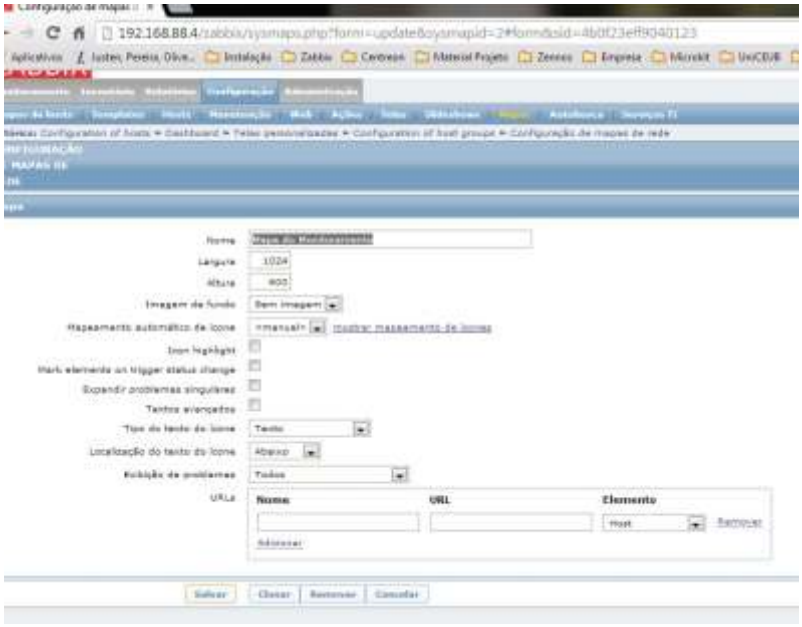

Figura 4.42 – Configuração de formato da tela no Zabbix (192.168.88.4/ Zabbix/sysmaps.php?form=update&sysmapid=2#form&sid=4b0f23eff904012, 16/10/2013)

Deve-se fornecer o nome do mapa, neste caso Mapa de Monitoramento; Os campos Largura e Altura são preenchidos de acordo com a especificação do monitor utilizado, neste caso 1024 x 600; Os demais campos foram preenchidos conforme apresentado na tela. Clica-se na caixa Salvar e o mapa está criado.

Retorna-se a aba Configuração, sub-aba Mapas (Figura 4.41) e clica-se em editar, na linha correspondente ao mapa criado, no caso Mapa de Monitoramento. Surge uma tela como a apresentada na Figura 4.43 a seguir.

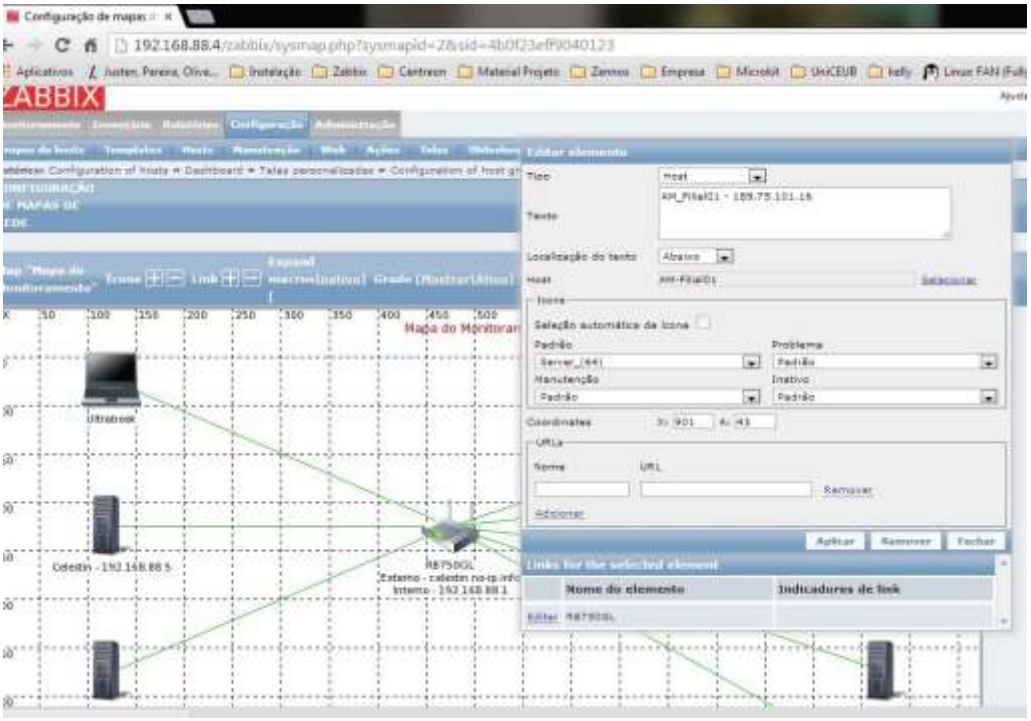

Figura 4.43 – Tela de configuração dos hosts no mapa de rede do Zabbix (192.168.88.4/Zabbix/sysmaps.php?sysmapid=2&sid=4b0f23eff9040123, 16/10/2013)

Na caixa Tipo seleciona-se Host; na caixa Texto o nome do host, neste caso AM_Filial01 – 189.75.101.16; Na caixa Localização do texto seleciona-se abaixo; Na caixa Host seleciona-se o host associado, neste caso AM-Filial01; Não se marca a Seleção automática de ícone; Na caixa Padrão seleciona-se o ícone do host a ser visualizado, neste caso o Server_(64); Nas caixas Problema, Manutenção e Inativo, seleciona-se Padrão. As coordenadas neste caso são X:901 e A:43; Em URLs, deixa-se em branco. Para todos os hosts incluídos, em Links for the selected elemento, campo Nome do elemento, é apontado o roteador RB750GL, para que todos eles estejam em rede com através deste roteador. Clica-se na caixa Aplicar para a inclusão deste elemento e do seu link.

Depois de incluídos todos os elementos do mapa, retornando a aba Configuração, sub-aba Mapas (Figura 4.41), e clicando no nome do mapa criado surge o mapa completo da rede, conforme apresentado na Figura 4.44 a seguir.

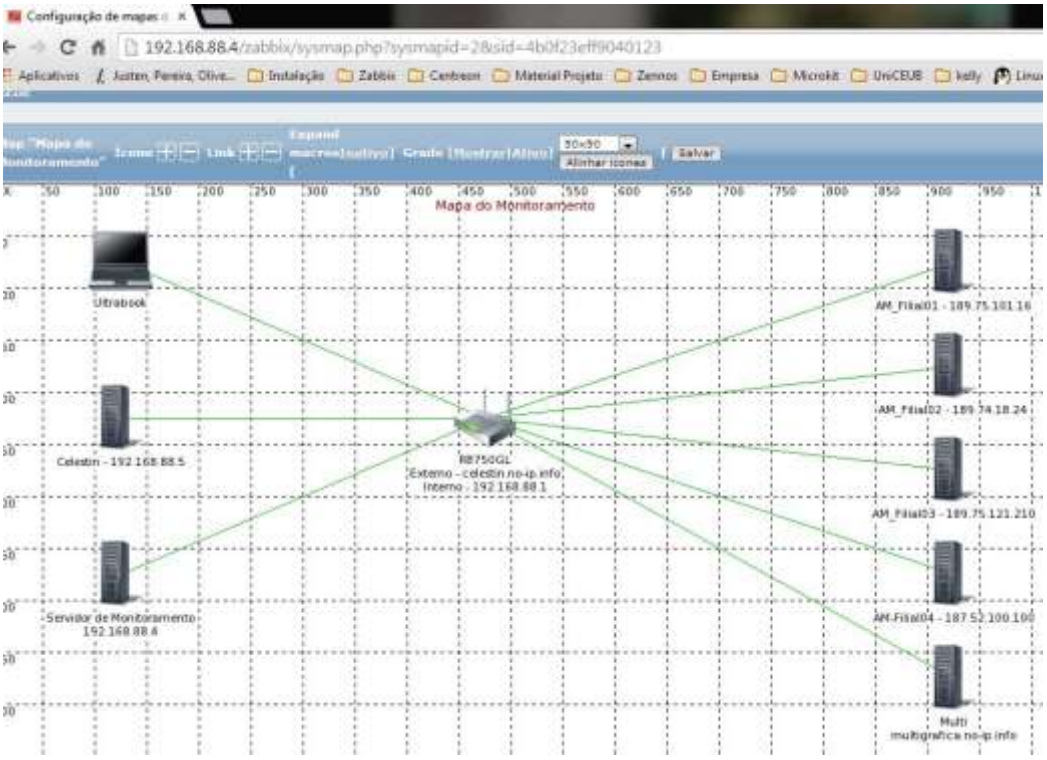

Figura 4.44 – Mapa da rede a ser monitorado pelo Zabbix (192.168.88.4/Zabbix/sysmaps.php?sysmapid=2&sid=4b0f23eff9040123, 16/10/2013)

É necessário também configurar as telas. Seleciona-se a aba Configuração e a sub-aba Telas. Surge a tela retratada na figura 4.45 a seguir.

Figura 4.45 – Tela inicial de configuração de telas do Zabbix (192.168.88.4/Zabbix/screenconf.php?ddreset=1&sid=4b0f23eff9040123, 16/10/2013).

Para especificar uma nova tela, clica-se na caixa Criar tela, e surge a tela apresentada na Figura 4.46 a seguir.

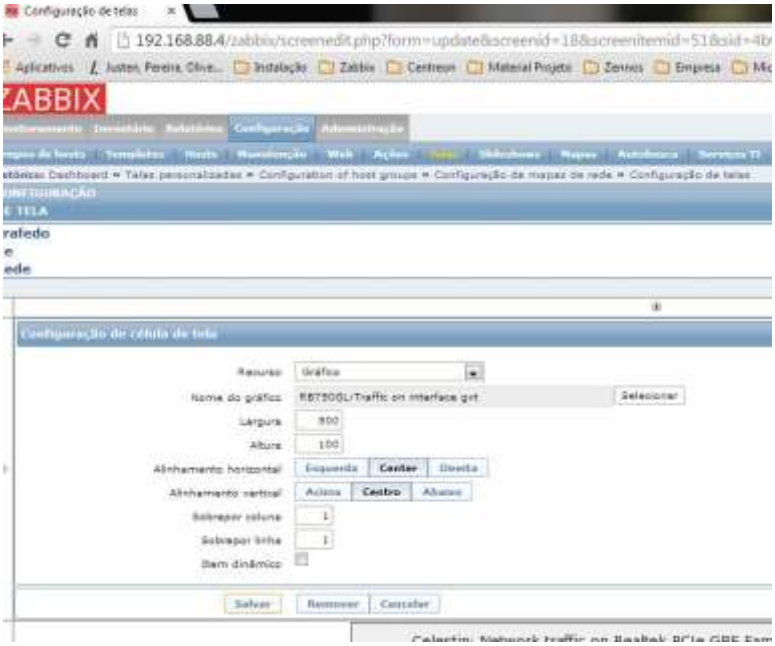

Figura 4.46 – Tela de configuração de telas do Zabbix (192.168.88.4/Zabbix/screenedit.php?form=update&screenid=18&screenitmid=51&sid=4b0f23eff9040123, 16/10/2013).

Para especificar um gráfico, na caixa Recurso selecionar Gráfico; Na caixa Nome do gráfico seleciona-se RB750GL:Traffic on interface gvt; Em Largura digita-se 500; Em Altura digita-se 100; Em Alinhamento horizontal Center; Em Alinhamento vertical Centro; Em Sobrepor coluna e Sobrepor linha 1; Não marcar Item dinâmico. Clica-se na caixa Salvar e a tela é criada. O resultado é apresentado na Figura 4.47 a seguir.

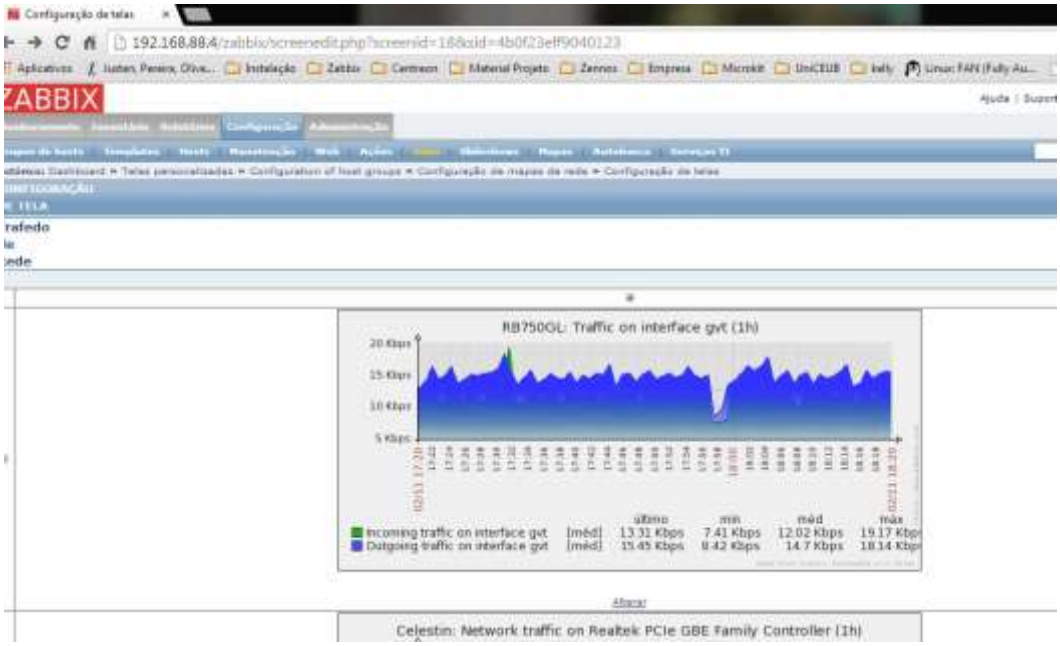

Figura 4.47 – Tela de um gráfico criado no Zabbix (192.168.88.4/Zabbix/screenedit.php?screenitmid=18&sid=4b0f23eff9040123, 16/10/2013).

Clicando-se em Alterar é possível alterar os parâmetros do gráfico, como quantidade de linhas e colunas, e outras informações de customização da tela.

Esta tela, usada como exemplo do gráfico criado na configuração apresentada na Figura 4.46, refere-se ao resultado do monitoramento do tráfego no roteador RB750GL, conectado no link da GVT, obtido com o uso do SNMP. A entrada de dados é apresentada em verde, e a saída de dados é apresentada em verde. No eixo horizontal é apresentado o tempo de dois em dois minutos, e no eixo vertical é apresentado o volume de tráfego com escala de 5 Kbps em 5 Kbps. É Mostrado também, os últimos, mínimos, médios, e máximos valores do trafego na entrada e na saída do link, no período entre 17h20min e 18h20min do dia 02/11.

Existem muitas opções de configuração de telas no Zabbix, sendo relatada a sequência mais simples de configuração delas.

Por último é necessário informar ao SNMP qual a comunidade que será monitorada pelo Zabbix. Seleciona-se a aba Hosts, seleciona-se o host desejado, e ao surgir a tela apresentada pela figura 4.48 a seguir, seleciona-se a sub-aba Macros.

Figura 4.48 – Informações da comunidade monitorada para o SNMP - Zabbix.

Fornece-se as informações a seguir: Em Macro, {$SNMP_COMMUNITY}; Em Valor, moncelestin.

Clica-se na caixa Salvar, para armazenar estas informações.

Repete-se esta operação para todos os hosts.

Após estas etapas tem-se o Zabbix configurado. Pode-se ter uma visão dos gráficos existentes e dos hosts monitorados selecionando a aba Monitoramento, sub-aba Visão geral, quando é mostrada a tela apresentada na figura 4.49 a seguir.

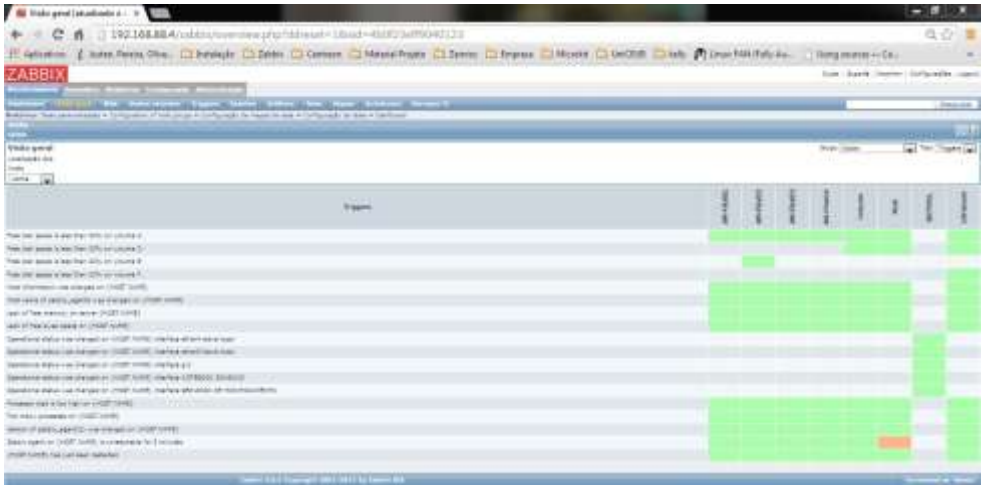

Figura 4.49 – Visão geral dos gráficos e hosts monitorados no Zabbix.

Nesta tela o Zabbix lista os eventos possíveis de monitoramento, que são apresentados como *triggers*, e em coluna mostra os hosts que estão sendo monitorados. Cada célula resultante desta matriz indica o status daquele monitoramento. Se estiver verde, significa que

aquele evento, naquele host está sendo monitorado e está ok; Se estiver vermelho, significa que aquele evento, naquele host está sendo monitorado e está com problema; Se estiver com a cor do fundo da tela, significa que não há monitoramento para aquele evento, naquele host.

Outra tela gerencial do Zabbix é apresentada na figura 4.50 a seguir:

Figura 4.50 – Console de monitoramento do Zabbix (192.168.88.4/zabbix/dashboard.php, 13/11/2013)

Esta tela informa sobre o status do Zabbix, que inclui o número de hosts monitorados, e não monitorados, itens monitorados e desativados, entre outros; Status do sistema, que informa por grupos de hosts, como equipamentos e estações windows entre outros, os problemas existentes por grau de importância; E dos hosts, informando por grupo de hosts quantos estão com ou sem problema.

Após o sistema CentOS, e as ferramentas Centreon e Zabbix estarem instalados, é necessário instalar o *software* NO-IP, para que o endereço IP do servidor seja identificado por qualquer equipamento ligado à rede, que tenha uma ADSL com uma DMZ apontada para ele.

1º Passo – Entrar no site http://www.noip.com/ e criar uma conta válida.

2º Passo – Instalar o NO-IP no centOS, seguindo as orientações contidas no site http://my.opera.com/sir-guil/blog/2013/02/01/instalando-no-ip-no-centos-6-dynamic-dns, 16/10/2013.

Agora verifica-se a necessidade de que os sistemas Windows instalados nas unidades externas se comuniquem com os roteadores e servidores locais. Para possibilitar esta comunicação é necessário configurar os parâmetros a seguir:

SMNP: 161-162

ICMP (*Internet Control Message Protocol*): 0-8

4.3.1.5 - Configurando o SNMP no Windows 2008 server

Aqui serão apresentados os procedimentos para a configuração do SNMP apenas no Windows do servidor da AM-Filial01. Para os outros equipamentos seguem-se os mesmos procedimentos, alterando-se apenas os parâmetros.

Acessar a pagina http://aaronwalrath.wordpress.com/2010/06/02/monitoring-windows-server-2008-r2-with-snmp-and-cacti/, 16/10/2013.

Surge a tela Propriedades de Serviço SNMP (Computador local). Selecionada a aba Agente, preenche-se os parâmetros conforme mostrado na Figura 4.51 a seguir.

Figura 4.51 – Propriedades de Serviço SNMP (Computador local) – Agente (http://aaronwalrath.wordpress.com/2010/06/02/monitoring-windows-server-2008-r2-with-snmp-and-cacti/, 16/10/2013)

A seguir, selecionada a aba Segurança, fornece-se os dados conforme mostrado na Figura 4.52 a seguir.

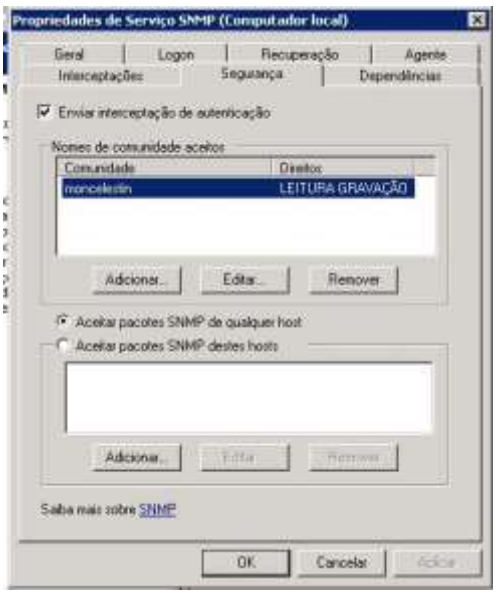

Figura 4.52 - Propriedades de Serviço SNMP (Computador local) – Segurança (http://aaronwalrath.wordpress.com/2010/06/02/monitoring-windows-server-2008-r2-with-snmp-and-cacti/, 16/10/2013)

Fornecidos os dados apresentados na figura 4.52, tecla-se em OK para salva-los.

4.4 - Considerações Finais.

Efetuadas todas estas instalações e configurações, consideram-se implementadas as condições para o monitoramento da rede. Talvez alguns pequenos ajustes possam ser necessários durante os testes, como a liberação das portas 161 e 162 do firewall do windows dos hosts monitorados, para que o serviço SNMP tenha acesso, e cada versão do windows tem uma forma diferente de configuração. A partir deste ponto será possível montar cenários, realizar testes e mostrar o resultado do monitoramento, e em consequência será possível fazer análises e chegar a conclusões, conforme será visto no capítulo a seguir.

CAPÍTULO Nº 5 – TESTES E RESULTADOS

No capítulo anterior foi mostrado como configurar as ferramentas Centreon e Zabbix para o monitoramento dos hosts, e dito que estas configurações tem que ser repetidas para todos os hosts da rede. Isto foi feito para todos os hosts deste projeto. Com a rede toda configurada, será mostrado neste capítulo, os gráficos de rede apresentados pelo Centreon e pelo Zabbix, referentes a todos os hosts monitorados.

Estando tudo configurado, conforme descrito no capítulo nº 4, o monitoramento dos links da rede passou a ser realizado no conceito 24/7, ou seja, de forma permanente, 24 horas por dia, 7 dias por semana, sendo os dados coletados de minuto em minuto.

Para mostrar o resultado do monitoramento, os gráficos das duas ferramentas foram capturados para o mesmo período de tempo. Poderá ser observado que os horários da coleta de informações do funcionamento normal da rede, referem-se ao horário comercial, onde os servidores monitorados operavam com as suas redes locais em expediente normal. Já os testes de tráfego elevado de dados, voz e vídeo, foram realizados em horário não comercial, para não afetar o funcionamento normal da rede.

Para facilitar a análise comparativa das ferramentas solicitou-se o resultado do monitoramento para o mesmo período de 3 horas, de forma a se verificar os resultados dos dados coletados simultaneamente. Também foram provocadas situações na rede, para que as ferramentas acionassem os alertas, em tela e por email. Como resultado, foi possível identificar as características, vantagens e desvantagens de cada software testado.

O ambiente implementado para a realização dos testes, é o apresentado na figura 1.1, constante do item 1.4 deste trabalho.

5.1 - Telas que Sintetizam o Universo Monitorado

Observa-se de forma imediata, que o layout da tela síntese do monitoramento das duas ferramentas difere bastante uma da outra.

5.1.1 – Tela síntese do Zabbix

A Figura 5.1 a seguir apresenta a tela síntese do Zabbix.

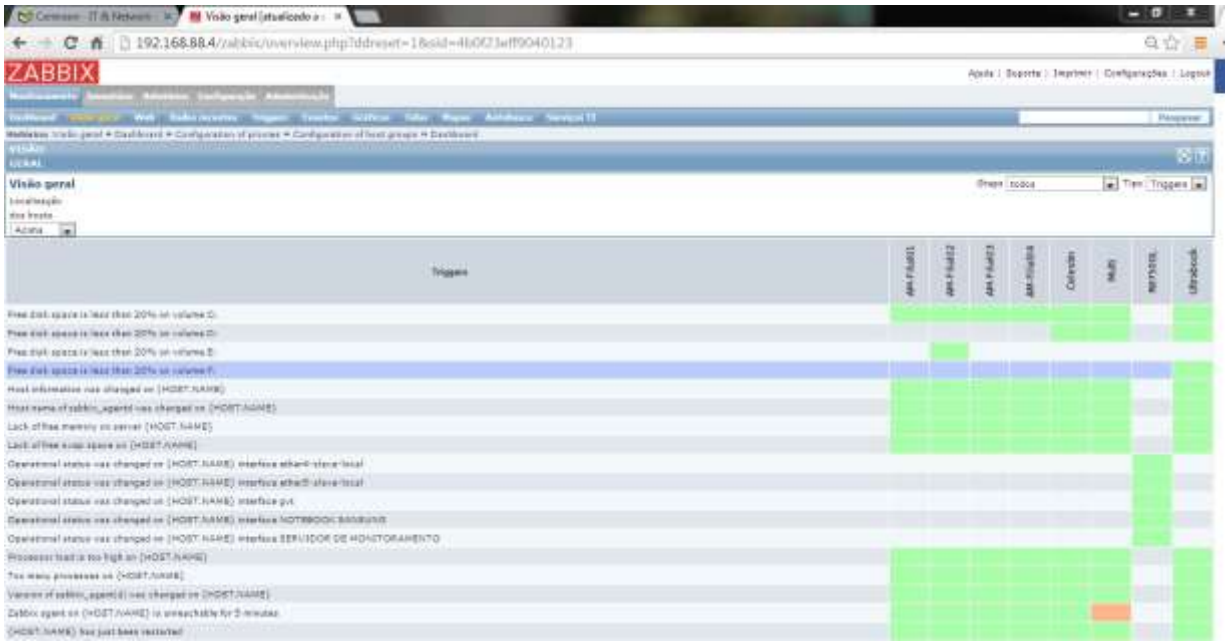

Figura 5.1 – Tela síntese do Zabbix (192.168.88.4/Zabbix/overview.php?ddreset=1&sid=4b0f23eff9040123, 21/10/2013)

Esta tela síntese do Zabbix, apresentada como exemplo, mostra os hosts e os itens monitorados de forma matricial, tendo um visual agradável. Nas linhas são listados os itens configurados para serem objeto de monitoramento, tais como links, disco, cpu, serviços, etc. Nas colunas, à direita, são relacionados os hosts monitorados. Para cada célula desta matriz, são apresentados retângulos que, se estiverem na cor do fundo, significa que não há monitoramento para aquela combinação item/host. Se o retângulo estiver na cor verde, significa que aquele item/host está sendo monitorado e está funcionando normal. Se o retângulo estiver vermelho, significa item/host monitorado e com problema.

5.1.2 – Tela síntese do Centreon

A Figura 5.2 a seguir, apresenta a tela síntese do Centreon

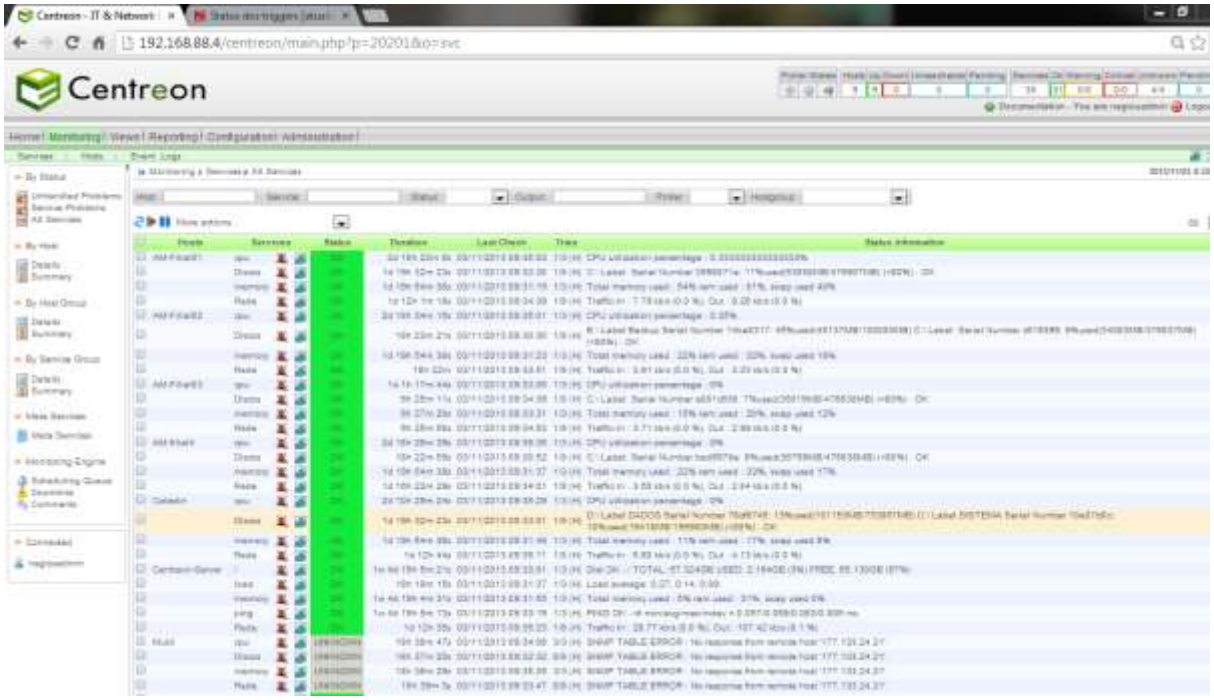

Figura 5.2 – Tela síntese do Centreon (192.168.88.4/centreon/main.php?p=20201&o=svc, 21/10/2013)

Esta tela síntese do Centreon, apresentada como exemplo, aparece em forma de lista, informando para cada host, a relação dos itens monitorados, e para cada item disponibiliza: Um ícone, que ao se clicar nele apresenta o gráfico correspondente àquele host/item monitorado; O status, que na cor verde com a inscrição OK, significa monitorado e funcionando corretamente, e na cor cinza com a inscrição UNKNOWN, significa que o item está com problema; Tempo total que o item se encontra com aquele status; Data/hora da última checagem; Dados sobre o item monitorado, que no caso de um link, informa o tráfego de entrada e saída na última checagem.

5.2 – Gráficos de Rede

As ferramentas de monitoramento, para o caso específico deste trabalho, fornecem a princípio, as informações sobre o volume do tráfego de entrada e de saída nos links da rede, apresentando estas informações através de gráficos. Quando detectada queda ou falta de informação em um link, é sinalizado este evento na tela, e é enviada mensagem via email comunicando o fato.

Os gráficos apresentados neste item referem-se às informações coletadas no horário comercial, onde os servidores monitorados operam com as suas redes locais em expediente normal. As amostragens foram colhidas para as duas ferramentas no mesmo período de 3 horas, de forma a se verificar os resultados dos dados coletados simultaneamente.

No Zabbix, o volume de saída (*upload*) é representado por pela cor azul, e o de entrada (*download*) é representado pela cor verde, apresentando as duas curvas sobrepostas. Já no Centreon a cor verde representa o volume de saída e a cor vermelha representa o volume de entrada, e apresenta o upload acima do eixo horizontal, e o download abaixo deste eixo.

Outra diferença que se nota entre os gráficos das duas ferramentas, é que o Zabbix plota as curvas de seus gráficos de acordo com todos os valores coletados e as suas tendências, enquanto o Centreon apresenta o gráfico com intervalo de cinco em cinco minutos, com as curvas cortadas bruscamente.

5.2.1 – Gráficos de rede do equipamento AM-Filial01.

A Figura 5.3 a seguir apresenta o gráfico de rede do AM-Filial01 mostrado pelo Zabbix.

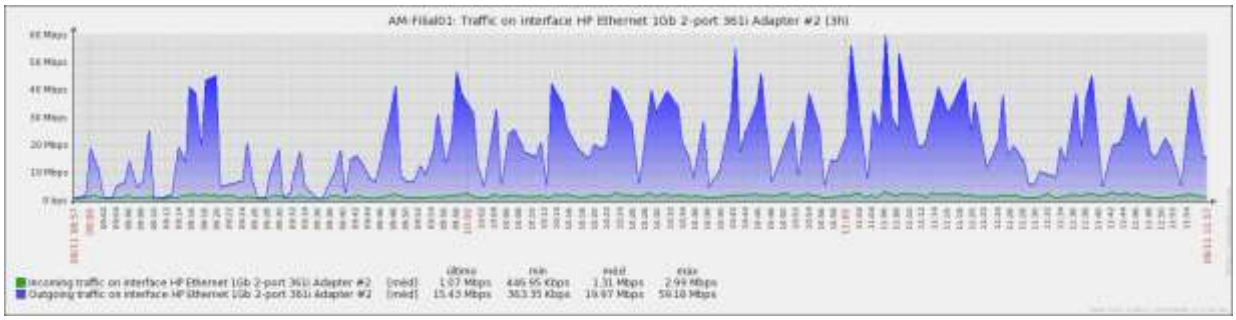

Figura 5.3 - Gráfico de rede do AM-Filial01 mostrado pelo Zabbix (09/11/2013)

Observa-se na figura que o servidor tem sido requisitado constantemente para busca de informações, chegando a um pico de upload (azul) de 59,18 Mbps, possui a média de upload de 19,97 Mbps (azul), e uma pequena taxa de download (verde) com uma média de 1,31 Mbps.

A Figura 5.4 a seguir apresenta o gráfico de rede do AM-Filial01 mostrado pelo Centreon.

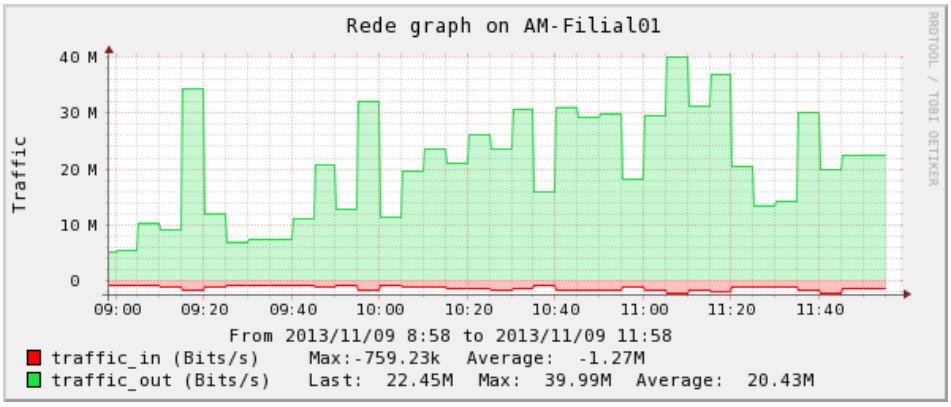

Figura 5.4 - Gráfico de rede do AM-Filial01 mostrado pelo Centreon (09/11/2013)

Observa-se na figura que o sistema tem sido requisitado constantemente para busca de informações, chegando a um pico de upload (verde) de 39,99 Mbps, possui a média de upload de 20,43 Mbps e uma pequena taxa de download (vermelho) com uma média de 1,27 Mbps.

5.2.2 – Gráficos de rede do equipamento AM-Filial02.

A Figura 5.5 a seguir apresenta o gráfico de rede do AM-Filial02 mostrado pelo Zabbix.

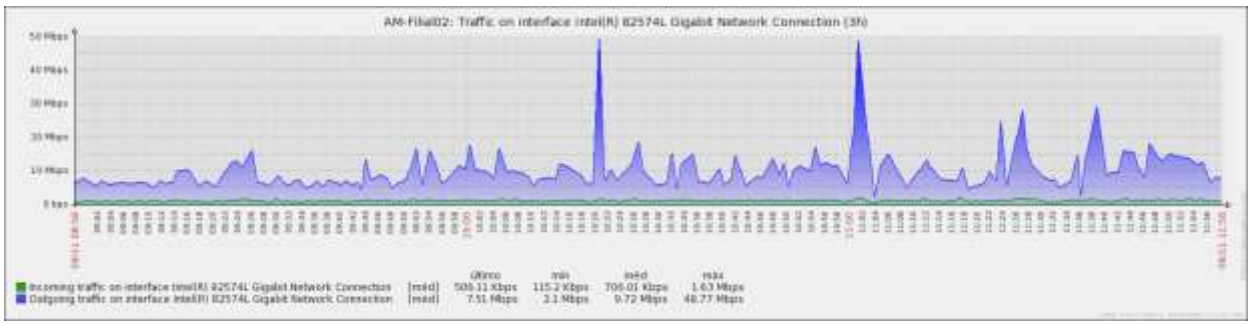

Figura 5.5 - Gráfico de rede do AM-Filial02 mostrado pelo Zabbix (09/11/2013)

Observa-se na figura que o sistema tem sido requisitado constantemente para busca de informações, chegando a um pico de upload (azul) de 48,77 Mbps, possui a média de upload de 9,72 Mbps e uma pequena taxa de download (verde) com uma média de 706,01 kbps.

A Figura 5.6 a seguir apresenta o gráfico de rede do AM-Filial02 mostrado pelo Centreon.

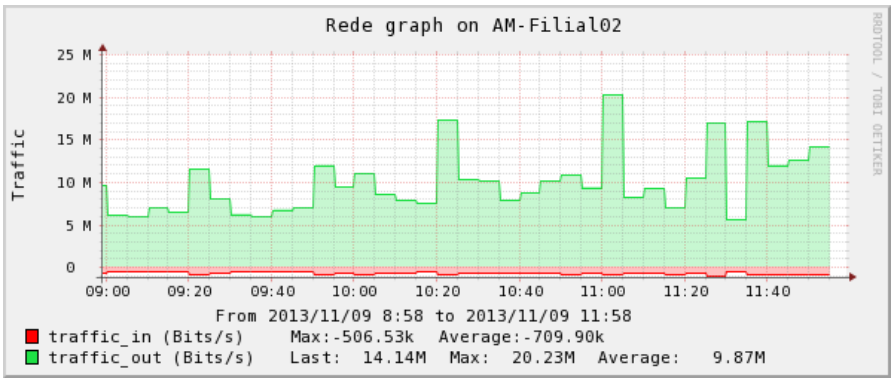

Figura 5.6 - Gráfico de rede do AM-Filial02 mostrado pelo Centreon (09/11/2013)

Observa-se na figura que o sistema tem sido requisitado constantemente para busca de informações, chegando a um pico de upload de 20,23 Mbps (verde), possui a média de upload de 9,87 Mbps e uma pequena taxa de download (vermelho), com uma média de 709,90 kbps.

5.2.3– Gráficos de rede do equipamento AM-Filial03.

A Figura 5.7 a seguir apresenta o gráfico de rede do AM-Filial03 mostrado pelo Zabbix.

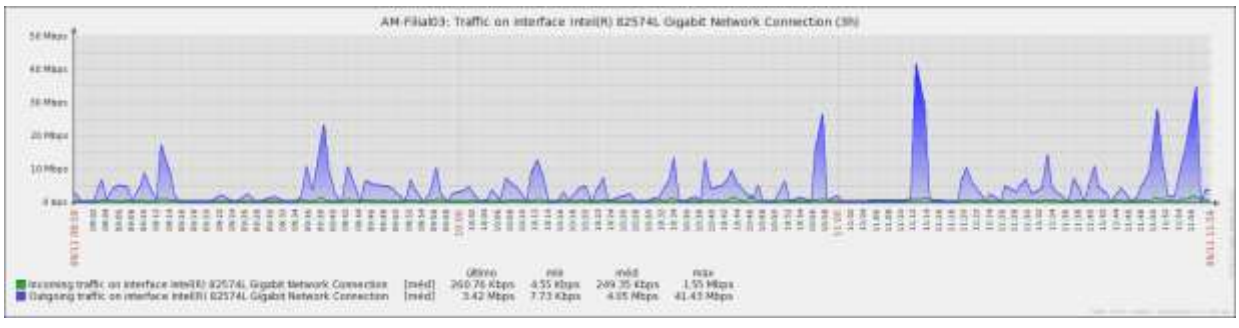

Figura 5.7 - Gráfico de rede do AM-Filial03 mostrado pelo Zabbix (09/11/2013)

Observa-se na figura que o sistema tem sido requisitado constantemente para busca de informações, chegando a um pico de upload (azul) de 41,43 Mbps, possui sua média de upload de 4,05 Mbps e uma pequena taxa de download c(verde) om a média de 249,35 Kbps.

A Figura 5.8 a seguir apresenta o gráfico de rede do AM-Filial03 mostrado pelo Centreon.

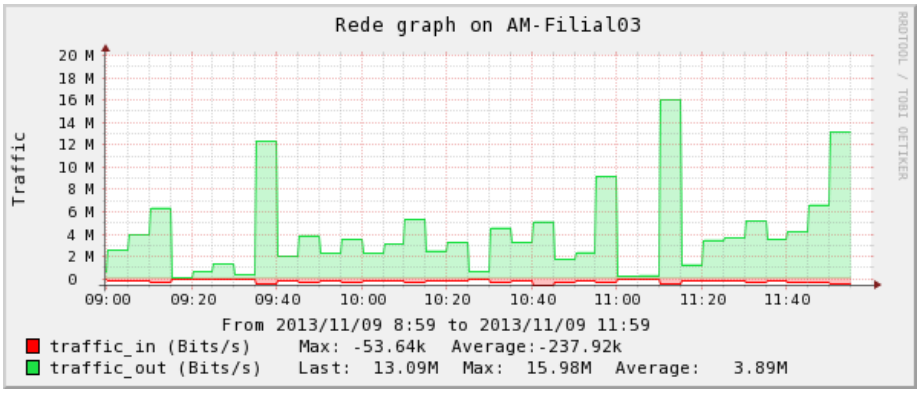

Figura 5.8 - Gráfico de rede do AM-Filial03 mostrado pelo Centreon (09/11/2013)

Observa-se na figura que o sistema tem sido requisitado constantemente para busca de informações, chegando a um pico de upload (verde) de 15,98 Mbps, possui a média de upload de 3,89 Mbps e uma pequena taxa de download (vermelho) com a média de 237,92 Kbps.

5.2.4– Gráficos de rede do equipamento AM-Filial04.

A Figura 5.9 a seguir apresenta o gráfico de rede do AM-Filial04 mostrado pelo Zabbix.

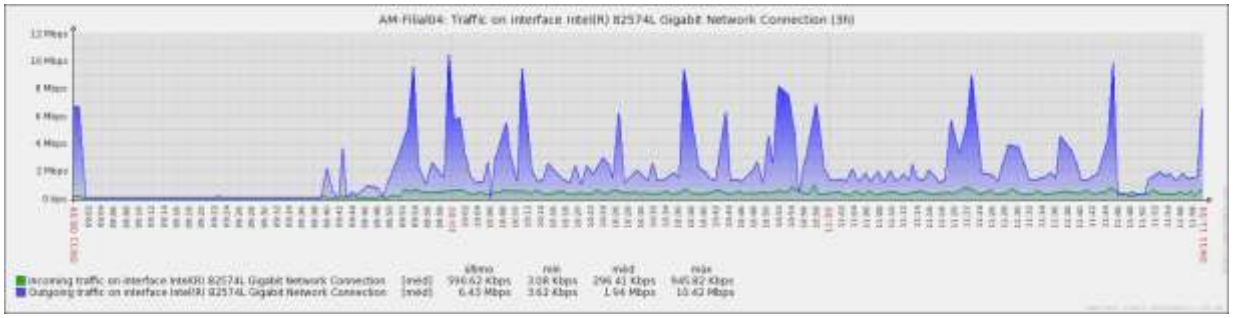

Figura 5.9 - Gráfico de rede do AM-Filial04 mostrado pelo Zabbix (09/11/2013)

Podemos ver na figura que o sistema tem sido requisitado constantemente para busca de informações, chegando a um pico de upload (azul) de 10,42 Mbps, possui a média de upload de 1,94 Mbps e uma pequena taxa de download (verde) com a média de 296,41 Kbps.

A Figura 5.10 a seguir apresenta o gráfico de rede do AM-Filial04 mostrado pelo Centreon.

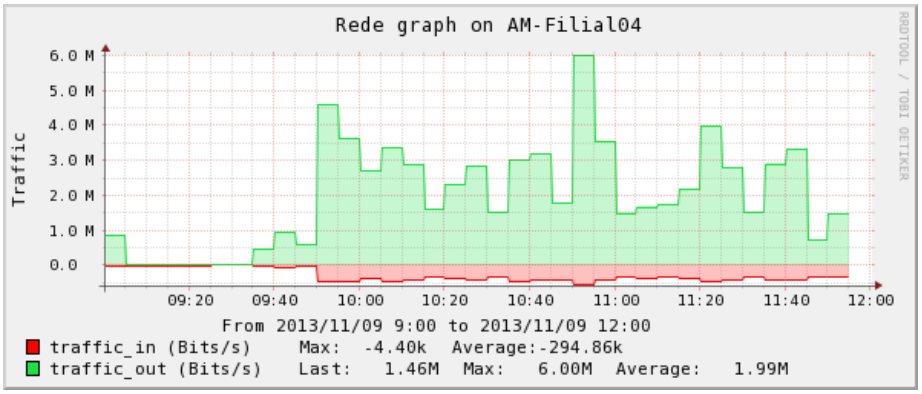

Figura 5.10 - Gráfico de rede do AM-Filial04 mostrado pelo Centreon (09/11/2013)

Observa-se na figura que o sistema tem sido requisitado constantemente para busca de informações, chegando a um pico de upload (verde) de 6 Mbps, possui a média de upload de 1,99 Mbps e uma pequena taxa de download (vermelho) com a média de 294,86 Kbps.

5.2.5– Gráficos de rede do equipamento Multi.

A Figura 5.11 a seguir apresenta o gráfico de rede do Multi mostrado pelo Zabbix.

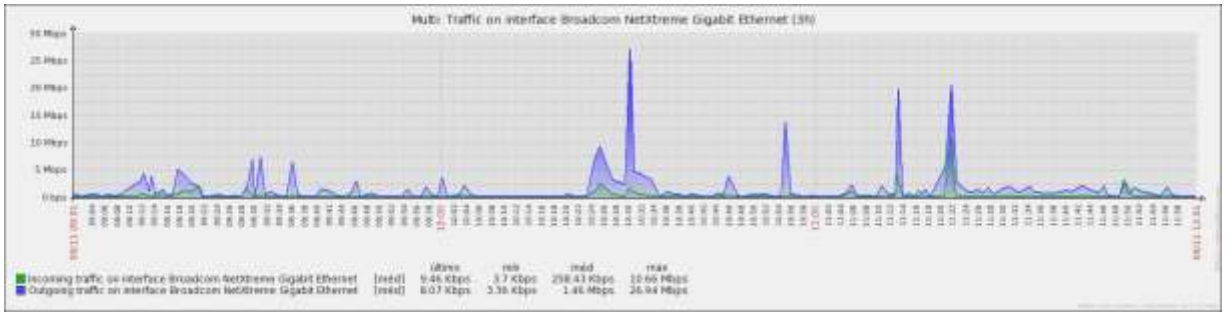

Figura 5.11 - Gráfico de rede do Multi mostrado pelo Zabbix (09/11/2013)

Observa-se na figura que o sistema tem sido requisitado constantemente para busca de informações, chegando a um pico de upload (azul) de 26,94 Mbps, possui a média de upload de 1,46 Mbps e uma pequena taxa de download (verde) com a média de 258,43 Kbps.

A Figura 5.12 a seguir apresenta o gráfico de rede do Multi mostrado pelo Centreon.

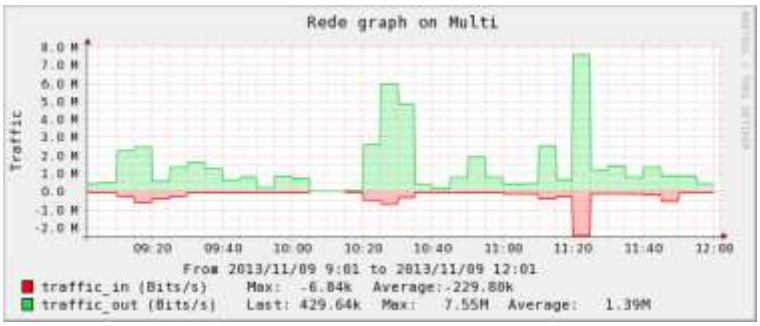

Figura 5.12 - Gráfico de rede do Multi mostrado pelo Centreon (09/11/2013)

Observa-se na figura que o sistema tem sido requisitado constantemente para busca de informações, chegando a um pico de upload (verde) de 7,55 Mbps, possui a média de upload de 1,39 Mbps e uma pequena taxa de download (vermelho) com uma média de 229,80 Kbps.

5.2.6– Gráficos de rede do equipamento RB750GL.

A Figura 5.13 a seguir apresenta o gráfico de rede do RB750GL mostrado pelo Zabbix.

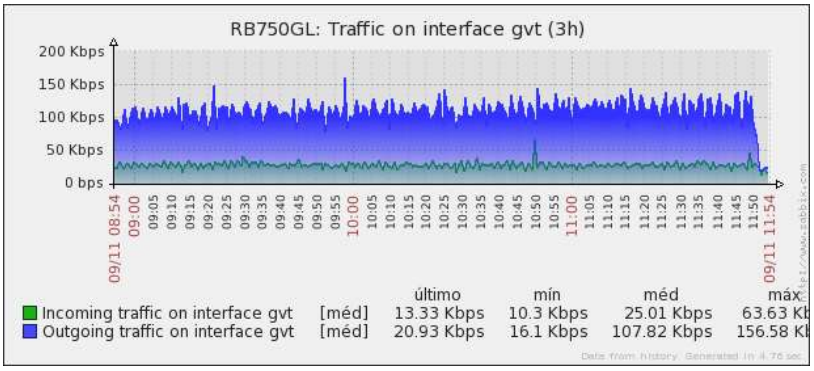

Figura 5.13 - Gráfico de rede do RB750GL mostrado pelo Zabbix (09/11/2013)

Observa-se na figura que o sistema tem sido requisitado constantemente para busca de informações, chegando a um pico de upload (azul) de 156,58 kbps, possui a média de upload de 107,82 kbps e uma pequena taxa de download (verde) com a média de 25,01 Kbps.

A Figura 5.14 a seguir apresenta o gráfico de rede do RB750GL mostrado pelo Centreon.

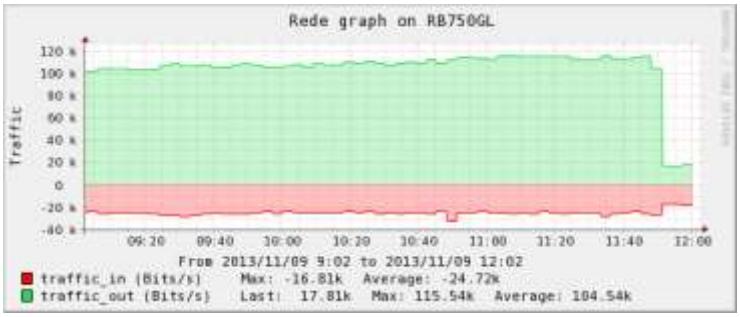

Figura 5.14 - Gráfico de rede do RB750GL - Centreon (09/11/2013).

Observa-se na figura que o sistema tem sido requisitado constantemente para busca de informações, chegando a um pico de upload (verde) de 115,54 kbps, possui a média de upload de 104,54 kbps e uma pequena taxa de download (vermelho) com a média de 24,72 Kbps.

5.2.7– Gráficos de rede do equipamento Celestin.

A Figura 5.15 a seguir apresenta o gráfico de rede do equipamento Celestin mostrado pelo Zabbix.

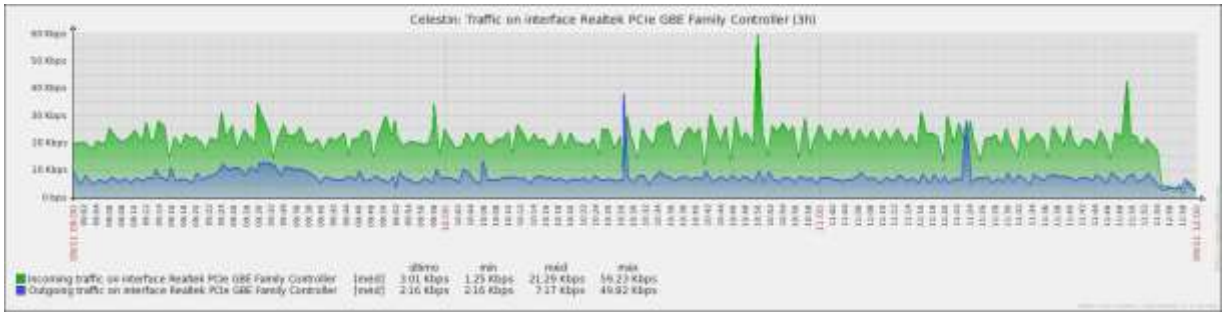

Figura 5.15 - Gráfico de rede do equipamento Celestin - Zabbix (09/11/2013)

Observa-se na figura que o sistema é pouco requisitado para busca de informações, chegando a um pico de upload (azul) de 49,82 kbps, possui a média de upload de 7,17 kbps e uma pequena taxa de download (verde) com a média de 21,29 Kbps.

A Figura 5.16 a seguir apresenta o gráfico de rede do equipamento Celestin mostrado pelo Centreon.

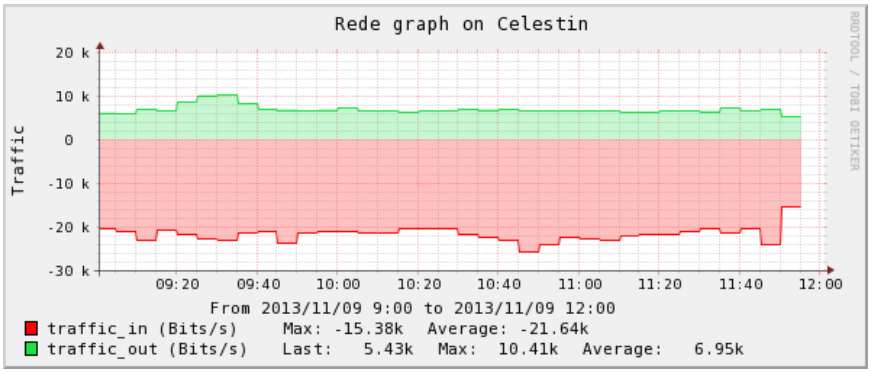

Figura 5.16 - Gráfico de rede do equipamento Celestin mostrado pelo Centreon (09/11/2013)

Observa-se na figura que o sistema tem sido pouco requisitado para busca de informações, chegando a um pico de upload (verde) de 10,41 kbps, possui a média de upload de 6,95 kbps e uma taxa de download (vermelho) com a média de 21,64 Kbps.

5.2.8– Gráficos de rede do equipamento Ultrabook.

A Figura 5.17 a seguir apresenta o gráfico de rede do Ultrabook mostrado pelo Zabbix.

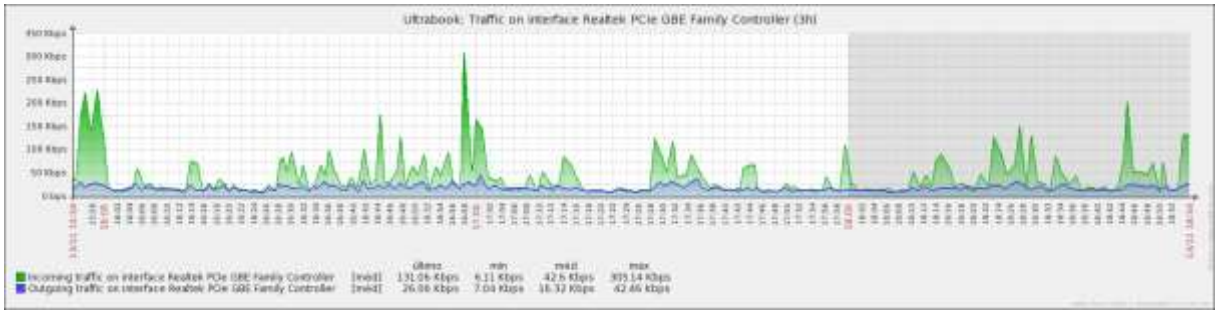

Figura 5.17 - Gráfico de rede do Ultrabook mostrado pelo Zabbix (13/11/2013)

Observa-se na figura que o sistema tem sido pouco requisitado para busca de informações, chegando a um pico de upload (azul) de 42,46 kbps, possui a média de upload de 16,32 kbps e uma taxa de download (verde) com a média de 42,06 Kbps.

A Figura 5.18 a seguir apresenta o gráfico de rede do Ultrabook mostrado pelo Centreon.

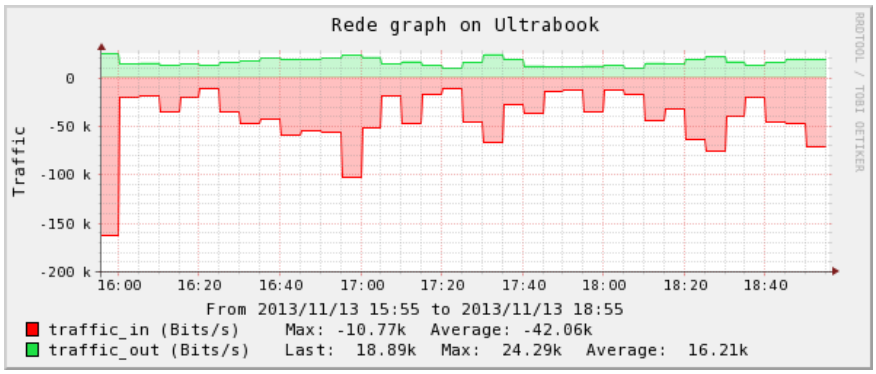

Figura 5.18 - Gráfico de rede do Ultrabook mostrado pelo Centreon (13/11/2013)

Observa-se na figura que o sistema tem sido pouco requisitado para busca de informações, chegando a um pico de upload (verde) de 24,29 Kbps, possui a média de upload de 16,21 Kbps e uma taxa de download (vermelho) com a média de 42,06 Kbps.

5.3 – Testes Realizados

Os gráficos apresentados neste item referem-se às informações coletadas fora do horário comercial, para não prejudicar o funcionamento das instituições monitoradas. As amostragens foram colhidas para as duas ferramentas no mesmo período de 3 horas, de forma a se verificar os resultados dos dados coletados simultaneamente.

Para estes testes foram simuladas situações de tráfego intenso entre equipamentos monitorados, e entre estes e os servidores Dropbox para dados, Vono para voz e Youtube para vídeos.

5.3.1 – Transferência de arquivo do servidor Celestin para AM-Filial04.

Foi simulado, através do RDP (*Remote Desktop Protocol*), a transferência de um arquivo do servidor Celestin passando pela RB750GL para a AM-Filial04 de 900 Mb, e constata-se que a capacidade de upload do Link GVT está trabalhando em seu limite. No caso a operadora fornece apenas 1 Mb de upload.

A Figura 5.19 a seguir apresenta o gráfico do tráfego entre o servidor Celestin e AM-Filial04 via RB750GL, monitorado pelo Zabbix. Constata-se que a capacidade de upload do Link GVT está trabalhando em seu limite. A operadora fornece apenas 1 Mb de upload.

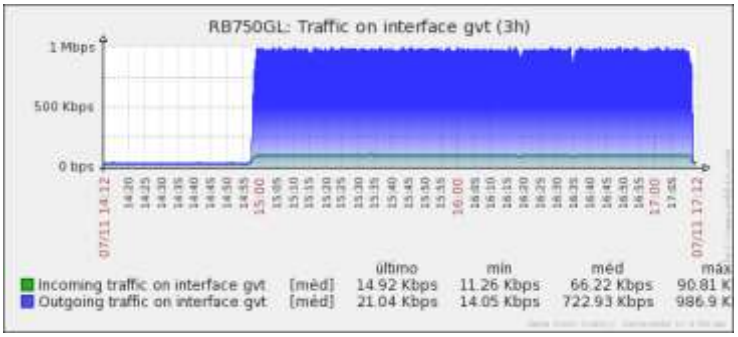

Figura 5.19 - Gráfico do tráfego entre Celestin e AM-Filial04 – Zabbix (07/11/2013)

Observa-se que o upload (azul) chegou a seu pico em 986,9 kbps.

A Figura 5.20 a seguir apresenta o gráfico do tráfego entre o servidor Celestin e AM-Filial04 via RB750GL, monitorado pelo Centreon.

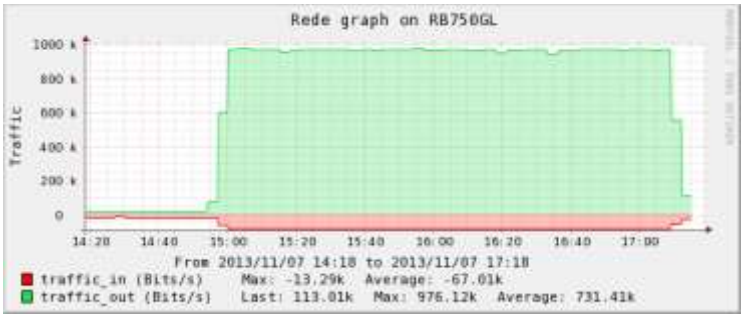

Figura 5.20 - Gráfico do tráfego entre Celestin e AM-Filial04 – Centreon (07/11/2013)

Observa-se que o upload (verde) chegou ao seu pico a 976,12 Kbps.

5.3.2 – Transferência de arquivo de AM-Filial04 para AM-Filial02

Foi simulado, através do RDP (*Remote Desktop Protocol*), a transferência de um arquivo da AM-Filial04 para a AM-Filial02 de 900 Mb, e constata-se que a capacidade de upload do Link GVT está trabalhando em seu limite. No caso a operadora fornece apenas 500 Kbps de upload.

A Figura 5.21 a seguir apresenta o gráfico do tráfego da AM-Filial04 para a AM-Filial02 monitorado pelo Zabbix.

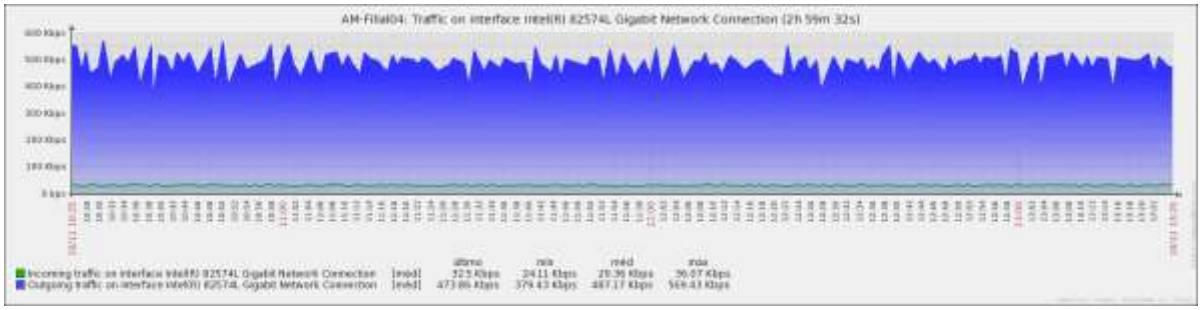

Figura 5.21 - Gráfico do tráfego da AM-Filial04 p/ AM-Filial02 – Zabbix (10/11/2013).

Observa-se que o upload (azul) chegou a seu pico em 569,43 kbps.

A Figura 5.22 a seguir apresenta o gráfico do tráfego da AM-Filial04 para a AM-Filial02 monitorado pelo Centreon.

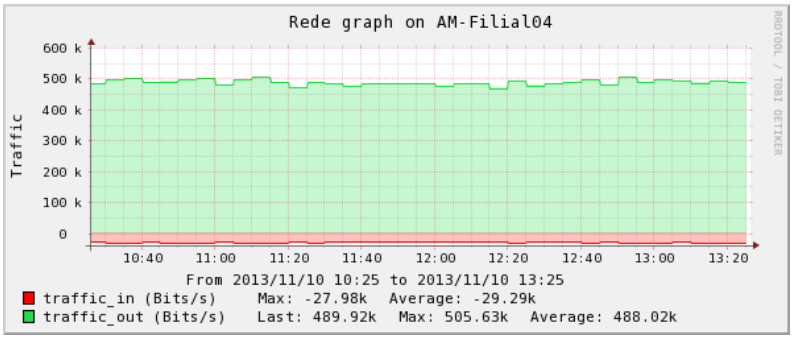

Figura 5.22 - Gráfico do tráfego da AM-Filial04 para AM-Filial02 – Centreon (10/11/2013).

Observa-se que o upload (verde) chegou ao seu pico a 505,63 Mbps.

5.3.3 – Download e upload do servidor Celestin para o servidor Dropbox.

A Figura 5.23 a seguir apresenta o gráfico do download e do upload do servidor Celestin para o servidor Dropbox monitorado pelo Zabbix.

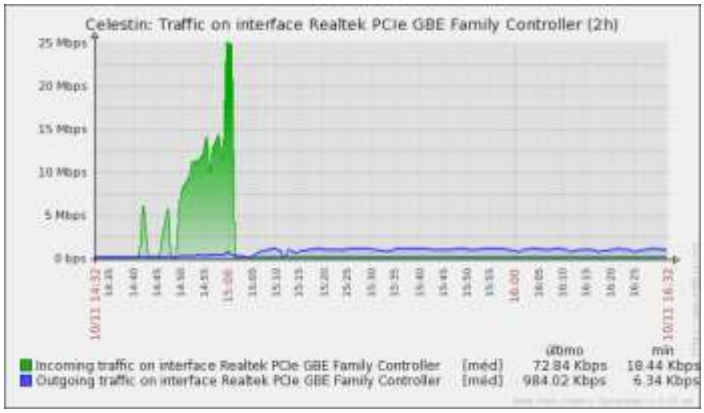

Figura 5.23 - Gráfico do down/upload de Celestin para Dropbox – Zabbix (10/11/2013).

Observa-se a uma variação no tráfego de download (verde) entre 11 Mbps a 15 Mbps no período de 14h50m às 15h e depois um upload (azul) no período de 15h10 às 16h25m, se mantendo na média de 984,02 Kbps.

A Figura 5.24 a seguir apresenta o gráfico do download e do upload do servidor Celestin para o servidor Dropbox monitorado pelo Centreon.

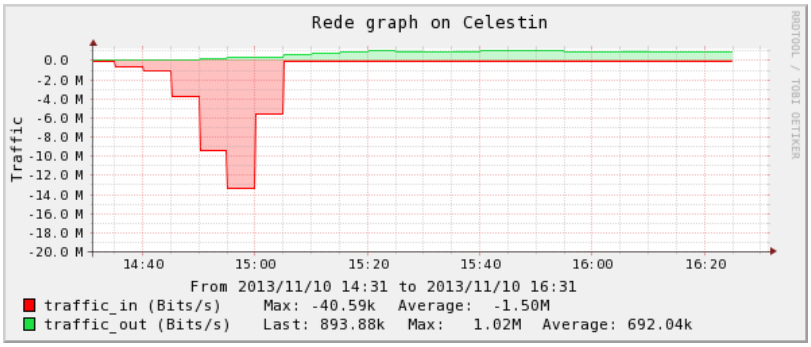

Figura 5.24 - Gráfico do down/upload de Celestin para Dropbox – Centreon (10/11/2013).

Observa-se uma variação no tráfego de download (vermelho) entre 09 Mbps a 13 Mbps no período de 14h50m às 15h e depois um upload (verde) no período de 15h10 às 16h25m, oscilando próximo a 1 Mbps.

5.3.4 – Download de vídeo do Youtube para o servidor Celestin.

A Figura 5.25 a seguir apresenta o gráfico do download durante exibição de vídeo do Youtube monitorado pelo Zabbix.

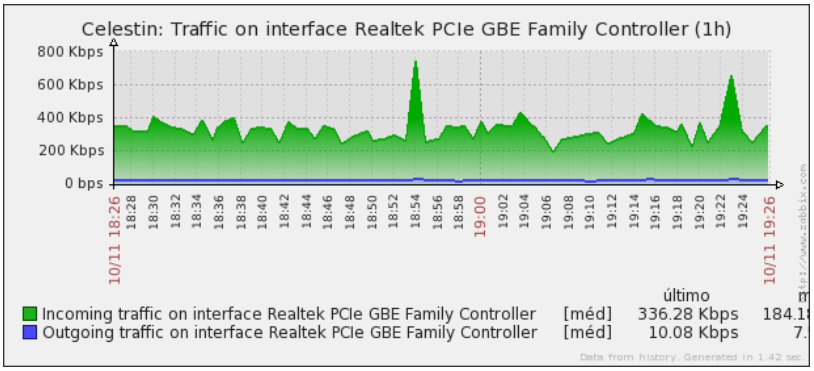

Figura 5.25 - Gráfico do download de vídeo do Youtube – Zabbix (10/11/2013)

Observa-se que durante a exibição do vídeo o download (verde) se manteve na média de 336,28 Kbps.

A Figura 5.26 a seguir apresenta o gráfico do download durante exibição de vídeo do Youtube monitorado pelo Centreon.

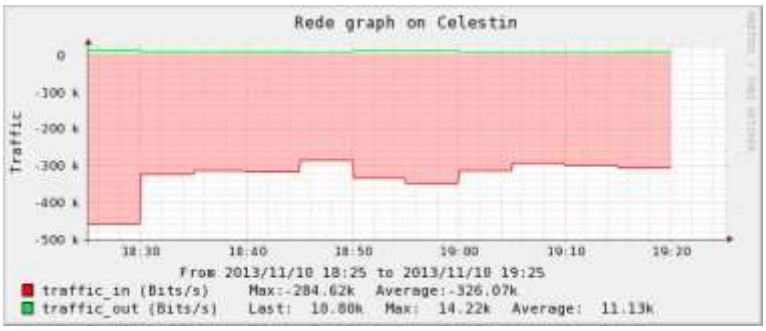

Figura 5.26 - Gráfico do download de vídeo do Youtube – Centreon (10/11/2013).

Observa-se que durante a exibição do vídeo o download (vermelho) se manteve na média de 326,07 Kbps.

5.3.5 – Download e upload da estação Ultrabook para o servidor Vono - Zabbix

A Figura 5.27 a seguir apresenta o gráfico de download e de upload da estação Ultrabook para o servidor Vono monitorado pelo Zabbix

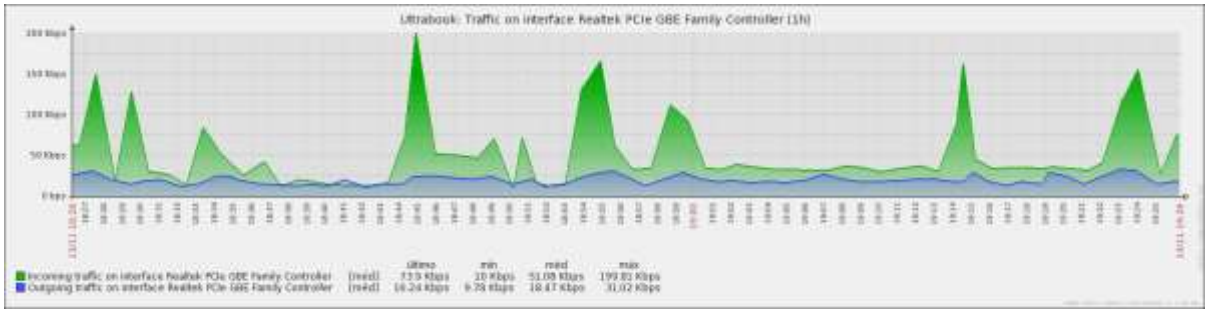

Figura 5.27 - Gráfico de download/upload do Ultrabook para Vono – Zabbix (13/11/2013).

Observa-se uma variação no tráfego de download (verde) entre 30 kbps e 50 kbps no período, e de upload (azul) entre 20 Kbps e 25 Kbps de 14h50m às 15h. Depois um upload no período de 19h01 às 19h20m. A operadora Falevono recomenda o mínimo de 42 Kbps por telefone.

A Figura 5.28 a seguir apresenta o gráfico do download e do upload da estação Ultrabook para o servidor Vono monitorado pelo Centreon.

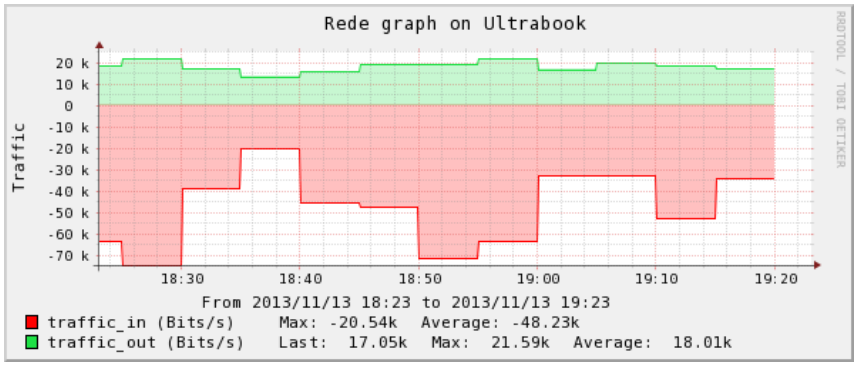

Figura 5.28 - Gráfico do down/upload de Ultrabook para Vono – Centreon (13/11//2013).

Observa-se uma variação no tráfego de download(vermelho) entre 30 kbps e 50 kbps no período e de upload (verde) entre 20 Kbps e 25 Kbps de 14h50m às 15h. Depois um upload no período de 19h01 às 19h20m. A operadora Falevono recomenda o mínimo de 42 Kbps por telefone.

5.3.6 – Transferência de Arquivos entre máquinas da LAN passando pelo RB750GL.

Foram transferidos arquivos entre estações da rede e o servidor de monitoramento, passando pelo roteador RB750GL, e constata-se que a capacidade de download do Link GVT está trabalhando em seu limite. No caso a operadora fornece 15 Mbps de download.

A Figura 5.29 a seguir apresenta o gráfico do tráfego na RB750GL monitorado pelo Zabbix.

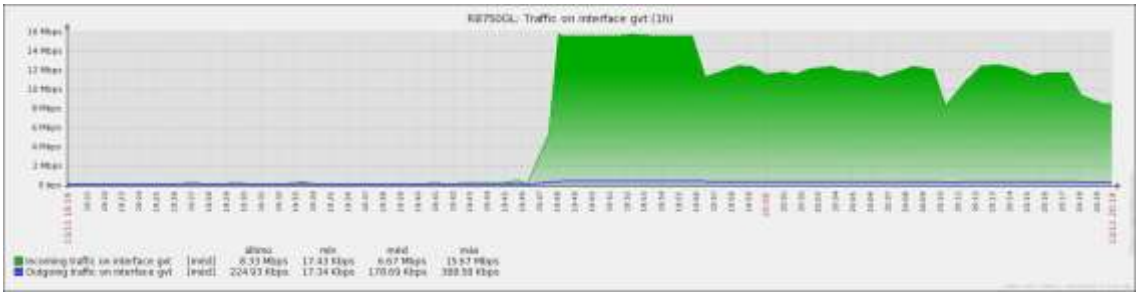

Figura 5.29 - Gráfico de transferência de arquivos pela RB750GL – Zabbix (13/11/2013).

Observa-se que o download (verde) chegou a seu pico em 15 Mbps.

A Figura 5.30 a seguir apresenta o gráfico do tráfego na RB750GL monitorado pelo Centreon.

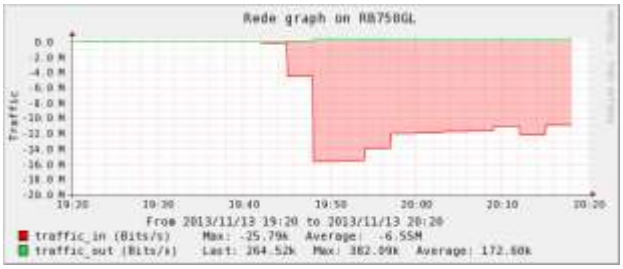

Figura 5.30 - Gráfico de transferência de arquivos pela RB750GL - Centreon (13/11/2013).

Observa-se que o download (vermelho) chegou a seu pico em 15 Mbps.

5.3.7 – Transferência de Arquivos para AM-Filial01 no limite de seu link.

Foram transferidos arquivos para o servidor AM-Filial01 durante o período da noite, e constata-se que a capacidade de download do Link OI está trabalhando em seu limite. No caso a operadora fornece apenas 10 Mb de download.

A Figura 5.31 a seguir apresenta o gráfico do tráfego limite no link do servidor AM-Filial01 monitorado pelo Zabbix.

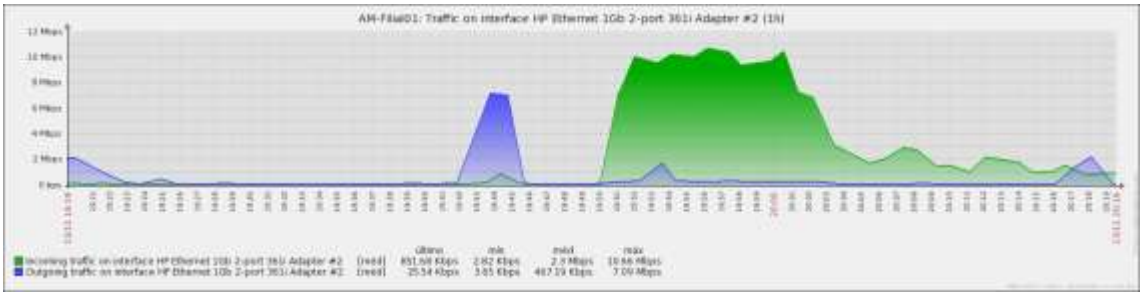

Figura 5.31 - Gráfico do limite de tráfego no link da AM-Filial01 – Zabbix (13/11/2013).

Observa-se que o download (verde) chegou a seu pico em 10 Mbps.

A Figura 5.32 a seguir apresenta o gráfico do tráfego limite no link do servidor AM-Filial01 monitorado pelo Centreon.

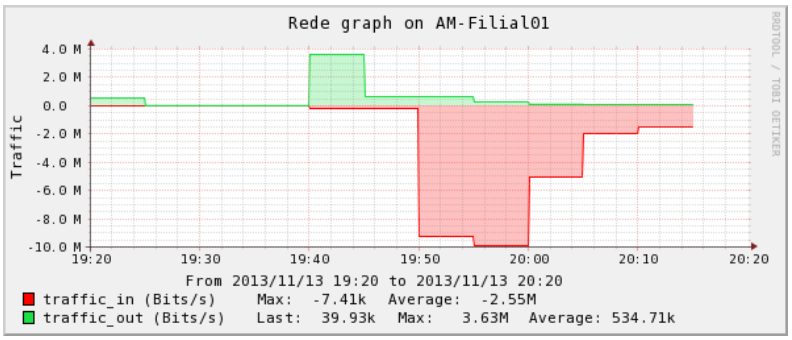

Figura 5.32 - Gráfico do limite de tráfego no link da AM-Filial01 – Centreon (13/11/2013).

Observa-se que o download (vermelho) chegou a seu pico em 10 Mbps.

5.4 – Alertas do monitoramento

Tanto o Centreon como o Zabbix podem ser configurados para detectar diversas situações ou problemas nos links ou na rede, e avisar em tempo real sobre o que foi detectado de diversas formas: Na tela, via email, ou SMS, por exemplo. Neste trabalho, é demonstrado apenas como as ferramentas comunicam por meio da tela e via email, se um link da rede está ativo ou interrompido.

5.4.1 – Alerta sobre links interrompidos através da tela.

Programadas para coletar as informações em períodos de um minuto, as ferramentas apresentam as telas conforme a seguir.

Na Figura 5.33 é apresentada a tela do Zabbix com o status do host Ultrabook.

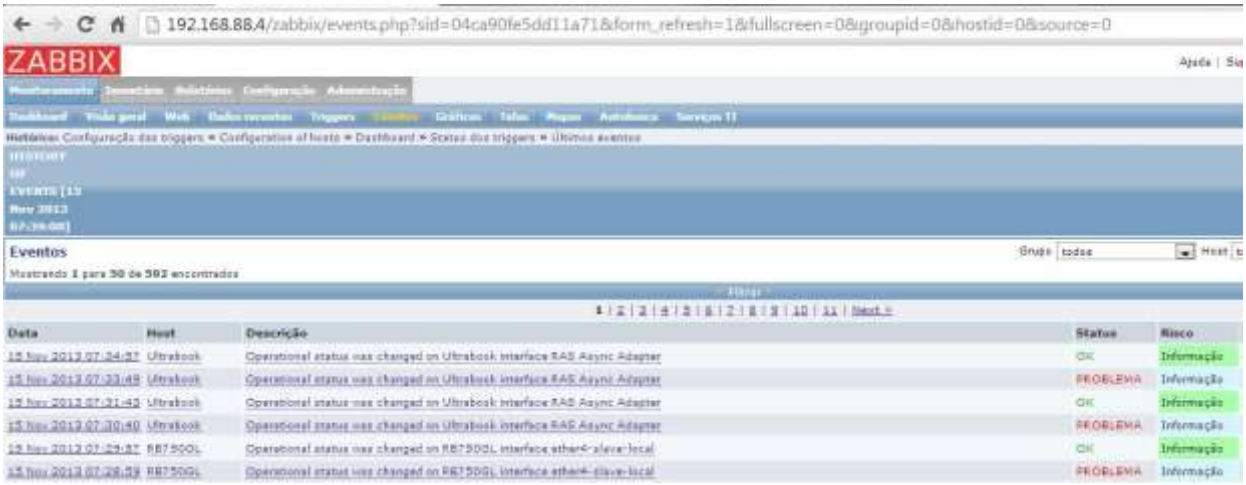

Figura 5.33 - Tela do Zabbix com o status do host Ultrabook (15/11/2013).

Para esta demonstração o cabo de rede do host Ultrabook foi conectado e desconectado várias vezes, e observa-se que nas medidas, o Zabbix informou alternativamente que o host monitorado apresentava o Status como OK, quando conectado, e PROBLEMA, quando desconectado.

Na Figura 5.34 é apresentada a tela do Centreon com o status do host AM-Filial03.

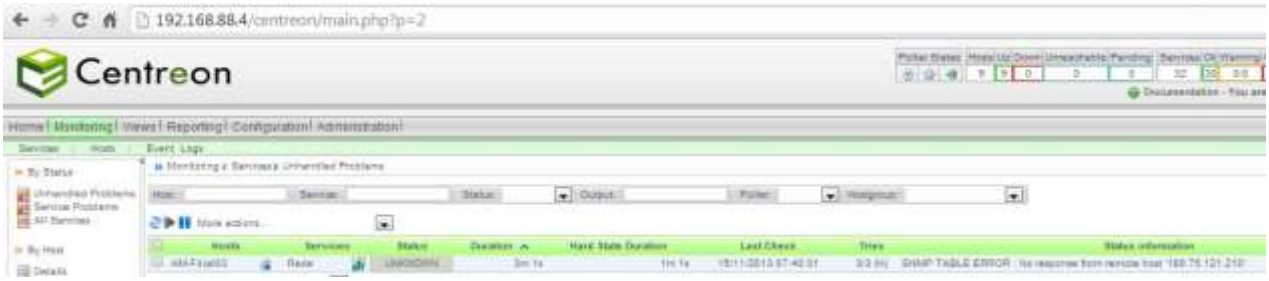

Figura 5.34 - Tela do Centreon com o status do host AM-Filial03 (15/11/2013).

Provocada a queda no link do host AM-Filial03, observa-se que o Centreon apresenta para este host, o Status como UNKNOWN, que significa desconhecido, indicando que perdeu-se a conexão..

5.4.2 – Alerta sobre links interrompidos através de email.

O alerta por email deve ser configurado de acordo com a necessidade do usuário, pois dependendo desta configuração, o serviço pode lotar a caixa do cliente e deixar de ser uma informação gerencial.

Na Figura 5.35 é apresentado o email enviado pelo Zabbix com o status do host Ultrabook.

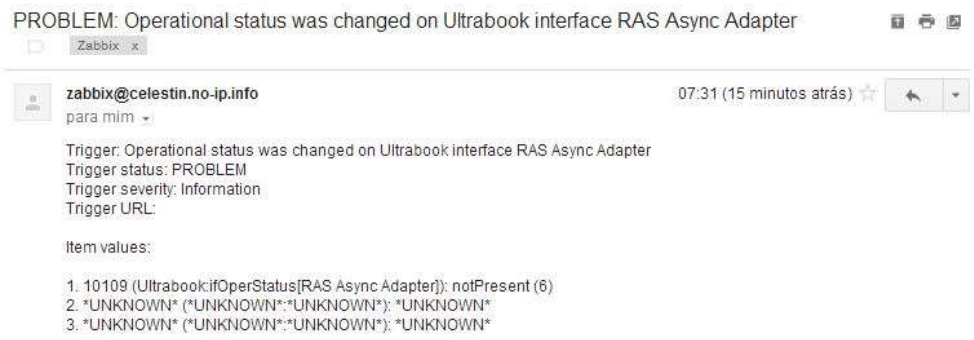

Figura 5.35 - Email enviado pelo Zabbix com o status do host Ultrabook (15/11/2013)

Observa-se que o Zabbix informa mudança no status de operação do Ultrabook, apresentando a mensagem Trigger status: PROBLEM.

Na Figura 5.36 é apresentado o email enviado pelo Centreon com o status do host AM-Filial01.

Figura 5.36 - Email enviado pelo Centreon com o status do host Ultrabook (15/11/2013)

Observa-se que o Centreon envia uma mensagem Type: PROBLEM, com State: UNKNWN, no Host: Ultrabook, Address: 192.168.88.3, indicando que existe um problema no link daquele host.

5.5 – Dificuldades Encontradas

Durante a implementação foram encontradas as seguintes dificuldades:

. Saber a melhor forma de instalar as ferramentas – Na instalação das duas ferramentas no mesmo servidor surgiram muitos conflitos, que inviabilizavam o funcionamento conjunto. A solução encontrada foi a utilização da ferramenta FAN, que além de outras funcionalidades, a partir de poucos parâmetros, instala o sistema operacional CentOS e a ferramenta de monitoramento Centreon. Depois de realizada a instalação desta forma, foi instalado e configurado o Zabbix, e as duas ferramentas funcionaram corretamente;

. Pouca literatura disponível em língua portuguesa, principalmente sobre a ferramenta Centreon;

. Dificuldade em definir o melhor caminho para a instalação do Zabbix, entre os diversos tutoriais disponíveis;

. Necessidade de liberar o firewall do Windows para as portas utilizadas;

. Saber quais as portas seriam necessárias para o acesso externo e quais redirecionamento fazer para que funcionasse externamente e internamente;

. Foi necessária a implementação do NO-IP, pois quando solicitado à operadora o IP Fixo não estava disponível, mas acabou sendo interessante para o projeto, pois mostrou que as ferramentas funcionam também em um IP dinâmico;

. Necessidade de substituição de alguns modens ADSL, que não estavam em perfeito funcionamento;

. Depois de tudo configurado, o HD apresentou problemas, sendo necessário uma imagem e uma restauração em um HD novo, que foi realizado com o uso da ferramenta Clonezilla, após isso passou-se a fazer o backup da imagem com frequência;

. Oscilação e queda de energia na central de monitoramento (residência), provocou a necessidade de instalação de dois nobreaks, um para o servidor de monitoramento e o outro para o desktop de auxílio aos testes, para garantir o monitoramento da central sem interrupções, e diminuir o risco de queima de aparelhos.

Embora estas dificuldades tenham surgido, a base de muito esforço e pesquisa, elas foram sendo sanadas, permitindo mostrar aqui como isso foi feito, para deixar a solução em pleno funcionamento.

5.6 - Custo da Solução de Monitoramento

Como os softwares utilizados são distribuídos sob Licença GPL, o custo destas soluções é bastante baixo, conforme apresentado a seguir:

Custo de implantação:

Sistema operacional CentOS:	R$ 0,00
Ferramenta de monitoramento Zabbix:	R$ 0,00
Ferramenta de monitoramento Centreon:	R$ 0,00
Servidor de Monitoramento:	R$ 1.300,00
Roteador RB750GL:	R$ 220,00
Custo Total:	R$ 1.520,00

Custo Mensal:

Para monitoramento de uma rede WAN é necessário ter IP Fixo ou conta no NO-IP.

O IP Fixo – O valor varia de acordo com a operadora utilizada, girando em torno de R$ 50,00 mensal, e é necessário um por unidade a ser monitorada

O NO-IP é comercializado por U$ 14,95, podendo endereçar até 50 hosts.

Observa-se que a escolha por qualquer das ferramentas de monitoramento não afeta o custo da solução, já que são de distribuição gratuita. O que afeta o custo é a escolha do método de endereçamento IP dos hosts, pois a aquisição de um IP fixo da operadora gera um custo mais elevado do que a ferramenta NO-IP, mas tem a vantagem de configurar-se a ferramenta apenas uma vez. Já com o serviço NO-IP, se for alterado o nome no serviço NO-IP, tem-se que alterar a configuração na ferramenta de monitoramento.

5.7 - Características das Ferramentas

As ferramentas estudadas apresentam características muito semelhantes, em geral, fornecem soluções para a maioria das necessidades que o gerenciamento de redes exige. Ainda assim, observam-se características únicas, que sobressaem na hora da comparação.

Para fins da análise e comparação das duas ferramentas, elas foram testadas em uma rede WAN com a seguinte configuração:

. Um servidor de monitoramento com o sistema operacional CentOS;

. Seis servidores monitorados com o Windows 2008 Server: servidor de domínio, DHCP, DNS, sistema e arquivos;

. Um roteador (*Routerboard*) RB750GL;

. Um ultrabook com Windows Seven Professional, apenas para trafego de rede;

. Seis modens: apenas fazendo direcionamento de portas.

5.7.1 – Características do Zabbix

O Zabbix se mostrou uma ferramenta completa, e possui uma interface robusta e amigável. Com o Zabbix instalado, gráficos, telas e mapas são facilmente gerados e acessados, proporcionando assim uma análise detalhada do ambiente da rede. Como ponto forte pode-se citar a documentação disponível que é em grande volume, e as comunidades de

usuários e desenvolvedores possuem bastante material sobre o software, sua instalação e a sua configuração. Como um ponto fraco pode-se comentar a sua instalação, que é complexa e não existe uma ferramenta de apoio, que torne este procedimento menos difícil, sendo necessário fazer os procedimentos passo a passo, com a utilização de arquivos texto. Já a sua configuração é simples. O Zabbix tem sido uma ferramenta muito utilizada por bancos, governos e empresas que necessitam do monitoramento.

5.7.2 – Características do Centreon

O Centreon se apresentou como uma ferramenta com uma interface agradável, e suas telas e gráficos tem um bonito visual. Seu núcleo é o Nagios, que é utilizado na captação e no armazenamento dos dados que são utilizados na geração dos seus mapas. Devido a sua origem ser francesa, não é tão difundido quanto o Zabbix, e a sua documentação no Brasil, em língua portuguesa, ainda é incipiente. Aos poucos começa a ser utilizada nas instituições que necessitam do monitoramento. Tem a seu favor o fato de existir uma ferramenta denominada FAN, que a partir de alguns parâmetros, instala de uma forma rápida e muito simples o sistema operacional CentOS e a solução de monitoramento Centreon, além de instalar algumas funcionalidades da própria ferramenta.

5.7.3 – Comparativos entre as duas ferramentas.

A tabela 15 a seguir fornece um resumo de recursos do Centreon e do Zabbix.

Tabela 15 – Resumo de recursos das ferramentas de monitoramento

	Zabbix	Centreon
Agente	Sim	Sim
Alertas	Sim	Sim
Auto Discovery	Sim	Não
Eventos	Sim	Sim
Front-end Web	Controle Completo	Controle Completo

Geração de Gráficos	Sim	Sim
Geração de Mapas	Sim	Pelo Nagios
Licenciamento	GPL	GPL
Linguagem que foi escrito	C e PHP	PERL
Método de Armazenamento de Dados	Oracle, MySQL, PostgreSQL e SQLite	Oracle, MySQL, MS SQL
Monitoramento Distribuído	Sim	Sim
Permite Scripts Externos	Sim	Sim
Plugins	Sim	Sim
SLA Reports	Sim	Sim
SNMP	Sim	Sim
Syslog	Sim	Sim

Uma característica comum às duas ferramentas é que não há limite máximo de hosts que estas soluções podem monitorar. A limitação fica condicionada ao hardware do servidor de monitoramento, quanto ao processador, memória, espaço em disco, placa de rede; Aos ativos, como *swithes* e roteadores; E velocidade e disponibilidade dos links.

5.8 – Análise dos Resultados

Em geral, as ferramentas apresentaram semelhanças, mudando a forma como são apresentados os gráficos de rede, como upload e download. A causa para as diferenças nos gráficos, além do aspecto de *design*, deve-se ao fato de que cada ferramenta utiliza algoritmos próprios para geração desses gráficos. Esses algoritmos tratam os valores coletados pela ferramenta e fazem a plotagem dos gráficos, e neste processo acontecem atenuações e adequações nas curvas, com isto provocando as diferenças de valores e das curvas entre os gráficos de uma ferramenta e da outra.

O Monitoramento passivo, feito sem o agente, obtém informações públicas do host, como portas abertas e protocolos como o icmp.

No comportamento de alerta em tela, as duas ferramentas também trabalham de forma semelhante, porém a forma com que o Zabbix configura o serviço é muito mais simples que no Centreon. O Zabbix possui um serviço de auto busca, em que a rede é identificada na busca padrão, enquanto que no Centreon é necessário criar o comando e identificar cada host.

No alerta por email, é recomendável configurar o alerta de acordo com a necessidade do administrador da rede, pois é possível alertar em tempo real apenas quando o evento ocorrer, ou ficar alertando sobre o problema até a sua solução.

As duas ferramentas fornecem um monitoramento de qualidade. Cabe ao administrador de rede selecionar a de sua preferência. A ferramenta FAN torna a instalação do Centreon muito mais simples do que a do Zabbix. Porém, para configuração e customização do ambiente, o Centreon leva desvantagem, pelo fato de sua documentação em português ser pobre em relação à do Zabbix. O Zabbix possui uma interface mais amigável e as curvas padrão de seus gráficos têm um visual mais agradável do que o Centreon. Quanto ao desempenho das duas ferramentas, elas se comportam com excelente qualidade, e fornecem resultados muito parecidos.

5.9 - Considerações finais

Como o objetivo deste trabalho é mostrar uma solução para o monitoramento de links e rede, as duas ferramentas foram estudadas focando apenas os links da rede. Porém as ferramentas Centreon e Zabbix monitoram todos os ativos e serviços de uma rede, além de monitorar os componentes dos equipamentos, tais como disco, processador por núcleo, e memória. Estes recursos já estão disponíveis nas ferramentas, bastando configurá-los e ativá-los. Com o uso completo dos recursos destas ferramentas é garantido um gerenciamento excelente de uma rede. Pode-se, a partir da análise destas informações, verificar quais elementos estão mais críticos em uma rede, criar uma relação de prioridades a serem atendidas, e em consequência, além do monitoramento para um bom funcionamento atual da rede, planejar esta rede para um funcionamento ainda melhor no futuro.

CAPÍTULO Nº 6 – CONCLUSÕES E TRABALHOS FUTUROS

6.1 - Conclusões

O desenvolvimento das tecnologias de comunicação acelerou os processos de informação. As redes de computadores tornaram-se complexas e na maioria dos casos instáveis. Hoje a sociedade é dependente dessas redes.

É importante que seja dada atenção ao monitoramento permanente destas redes, para que sejam detectados problemas potenciais antes que estes ocorram, e que a partir da análise das informações fornecidas por uma solução de monitoramento, sejam indicados ajustes em seus componentes, subsidiando por exemplo: a substituição de ativos de baixo rendimento por equipamentos modernos de alto desempenho, como é o caso do roteador RB750GL escolhido para este projeto; Acréscimo na capacidade de trafego em links congestionados, através de aumento da velocidade do link da operadora. É o caso do tráfego no roteador RB750GL, apresentado nas figuras 5.29 (Gráfico de transferência de arquivos pela RB750GL – Zabbix) e 5.30 (Gráfico de transferência de arquivos pela RB750GL – Centreon), quando ao ser provocada a transferência simultânea de vários arquivos entre os servidores monitorados e o servidor de monitoramento, as duas ferramentas acusaram naquele período a frequência de 15 Mbps, que é o limite do link da GVT utilizado. A observação desta situação em uma rede real, ocorrendo constantemente, indicaria ao administrador da rede a necessidade da substituição daquele link por outro de maior capacidade de tráfego.

Também, é através destas soluções de monitoramento, que pode-se alertar em tempo real o administrador da rede, sobre falhas em links, em equipamentos, ou em ativos da rede, para que seja providenciada solução no prazo o mais curto possível.

Estas ferramentas de monitoramento devem ser modernas e estar em constante desenvolvimento, como é o caso do Centreon e do Zabbix, escolhidos para este trabalho.

Finalmente, espera-se que este trabalho seja útil para conscientizar a comunidade sobre a importância do tema, e que este projeto seja uma importante contribuição para a implantação de uma das soluções estudadas em organizações que dependam de redes, e que terão com o seu uso, uma solução de seus problemas de estabilidade e confiabilidade da rede.

O bom conhecimento das ferramentas de monitoramento apresentadas, abre boas perspectivas para a comercialização de serviços, tais como: Consultoria em monitoramento de rede; Implantação e treinamento em instalações de clientes; Administração de redes, com monitoramento remoto em instalação própria do prestador do serviço.

Muito embora o trabalho apresente um conteúdo bastante extenso, acredita-se ter dado uma boa base teórica sobre os recursos utilizados neste projeto. Também foi necessário o detalhamento, passo a passo, da instalação e configuração das ferramentas necessárias para compor o cenário que foi monitorado. Por último, provocaram-se diversas situações na rede e nos links, para exemplificar as respostas dadas pelas soluções de monitoramento. Todo este conteúdo visa dar ao leitor, com maior riqueza de detalhes, material de consulta, que no caso de estar diante da necessidade da escolha e aplicação de uma solução de monitoramento, seja encorajado a iniciar o trabalho de uma forma organizada e com bases técnicas.

Os equipamentos utilizados, provedores, escolhas de links de monitoramento e cenários apresentados, são circunstanciais e podem ser alterados, bastando para isso seguir as recomendações em termos de especificações sobre os protocolos e as ferramentas que suportam, verificando se também na solução de gerenciamento se são suportados.

6.2 - Sugestões de Trabalhos Futuros

Pode-se eleger outras ferramentas de monitoramento, como o Zenoss, o icinga, o opennms, e o cacti, para realizar procedimentos semelhantes aos realizados neste trabalho, chegando-se a comparativos de maior abrangência em termos de gerenciamento de redes.

É interessante que se aprofunde no conhecimento das soluções de monitoramento aqui estudadas, para esmiuçar todas as possibilidades de configuração e customização que estas ferramentas permitem, que não era o objetivo deste trabalho.

É muito importante que sejam estudadas todas as possibilidades de elementos que podem ser monitorados na rede, que incluem disco, CPU, memória, ativos em geral, e serviços. Desta forma, monitorando todos os dispositivos e serviços de uma rede, tem-se como administrá-la com uma visão completa de seu funcionamento, e em consequência alcançar-se a excelência na eficiência e estabilidade da rede monitorada.

REFERÊNCIAS

CELUPPI, Raphael. **Implantação do Zabbix para monitoramento de infraestrutura**. 2009. http://www.ppgia.pucpr.br/~jamhour/RSS/TCCRSS08A/Raphael%20Celuppi%20-%20Artigo.pdf; Última visita 27/09/2013

Espaço Liberdade – Legacy. **Review do CentOS 6**; http://bespacoliberdade.wordpress.com/ 2011/07/26 /review-do-centos-6/; Última visita 27/09/2013.

FALEVONO. **Conheça o Vono**. http://www.falevono.com.br/conheca/conheca.html. Última visita 20/09/2013

FILHO, João Eriberto Mota. **Descobrindo o Linux** – Entenda o Sistema Operacional Gnu/Linux. 3ª ed. São Paulo: Novatec, 2012. 928 p.

MARTINHO, Cássio. Redes – **Uma Introdução às Dinâmicas da Conectividade e da Auto-organização**. Brasília: WWF Brasil, 2003.

NO-IP – Eu quero um IP fixo; http://www.canaldainfo.com.br/index.php/no-ip-eu-quero-um-ip-fixo/; Último aceso 11/10/2013.

Principais servidores web (softwares). Quais são os mais utilizados? Vantagens e desvantagens de cada um. http://www.mutukagames.xpg.com.br/pg4.html. Última visita 27/09/2013)

SALVO, Rodrigo. **SNMP – Introdução**. http://www.ti-redes.com/gerenciamento/snmp /intro/. Última visita 27/09/2013.

SAUVÉ, Jacques Philippe; LOPES, Raquel Vigolvino, NICOLLETT, Pedro Sérgio. **Melhores práticas para a gerência de redes de computadores**. 1ª. ed. Rio de Janeiro: Campus, 2003. 373.p.

TANENBAUM, Andrew S. **Formatado**: Português (Brasil). **Computer Networks**. 4ª ed. Rio de Janeiro: Campus, 2003. 632 p.

WikipédiA – A Enciclopédia Livre; http://pt.wikipedia.org/wiki/Nagios; Última visita 18.09.2013.

WikipédiA – A Enciclopédia Livre; http://pt.wikipedia.org/wiki/CentOS; Última visita 27.09.2013

ZABBIX – Monitorar é preciso; http://www.zabbix.com/ Última visita 10/10/2013.

ANEXO A – INSTRUÇÕES E COMANDOS PARA INSTALAÇÃO DO ZABBIX

Este conteúdo foi extraído em 16/10/2013 do site http://www.vivaolinux.com.br/artigo/Zabbix-2-no-CentOS-6-Instalacao-e-configuracao

Antes de mais nada, é necessário desabilitar o *SELinux*, para isso, é necessário entrar no arquivo */etc/selinux/config* e mudar a configuração de "enforcing" para "disabled".

 # vim /etc/selinux/config

```
# This file controls the state of SELinux on the system.
# SELINUX= can take one of these three values:
#     permissive - SELinux prints warnings instead of enforcing.
#     disabled - SELinux is fully disabled.

SELINUX=disabled
```

Depois, precisaremos parar o *IPtables* tanto agora, quanto no arranque do sistema:

 # /etc/init.d/iptables stop

 # ntsysv

Desmarcar: *iptables* e *ip6tables*

Começaremos agora a instalar os pacotes necessários para o funcionamento correto do *Zabbix*:

 # yum install gcc httpd php php-bcmath php-cli php-gd php-mbstring php-mcrypt php-mysql curl curl-devel net-snmp net-snmp-lib net-snmp-utils net-snmp-devel OpenIPMI OpenIPMI-devel mysql-server mysql-devel php-mysql php-xml gnutls-devel mod_ssl libssh2 libssh2-devel make

Baixar pacotes que não estão disponíveis nos repositórios:

 # wget http://pkgs.repoforge.org/fping/fping-2.4-1.b2.2.el5.rf.i386.rpm

 # wget http://pkgs.repoforge.org/iksemel/iksemel-1.4-1.el6.rf.i686.rpm

 # wget http://pkgs.repoforge.org/iksemel/iksemel-devel-1.4-1.el6.rf.i686.rpm

Instalar os pacotes:

 # rpm -ivh fping-2.4-1.b2.2.el5.rf.i386.rpm

 # rpm -ivh iksemel-1.4-1.el6.rf.i686.rpm

 # rpm -ivh iksemel-devel-1.4-1.el6.rf.i686.rpm

Ajustes no php.ini

De acordo com os requerimentos do *Zabbix*, abra o arquivo */etc/php.ini* e ajuste os itens:

 # vim /etc/php.ini

Alterar:

```
date.timezone=America/Sao_Paulo
max_execution_time = 600
post_max_size = 32M
upload_max_filesize = 16M
max_input_time = 600
```

Baixar o *Zabbix Server 2.0*:

#
wget http://sourceforge.net/projects/zabbix/files/ZABBIX%20Latest%20Stable/2.0.3/zabbix-2.0.3.tar.gz/download

Descompactar e instalar:

 # tar -zxvf zabbix-2.0.3.tar.gz

 # cd zabbix-2.0.3/

 # ./configure --with-mysql --enable-server --enable-agent --enable-proxy --with-jabber --with-net-snmp --with-libcurl --with-openipmi --with-ssh2

 # make install

 # mkdir /etc/Zabbix

 # cp /usr/local/etc/zabbix_server.conf /etc/zabbix/

 # cp /usr/local/etc/zabbix_agentd.conf /etc/zabbix/

 # useradd Zabbix

 # chown zabbix:zabbix /etc/zabbix/ -R

 # /etc/init.d/mysqld restart

 # mysql -u root -p

mysql> **create database zabbix character set utf8;**

mysql> **grant ALL on zabbix.* to zabbix@'localhost' identified by 'senha';**

 # cat database/mysql/schema.sql | mysql -u zabbix -p Zabbix

Enter password:

 # cat database/mysql/images.sql | mysql -u zabbix -p Zabbix

Enter password:

 # cat database/mysql/data.sql | mysql -u zabbix -p Zabbix

Enter password:

Configurando o zabbix_server e zabbix_agentd

Editar arquivo *zabbix_agentd.conf*:

 # vim /etc/zabbix/zabbix_agentd.conf

Como estamos criando o server na máquina em questão, basta manter o campo: *Server=127.0.0.1*

 # vim /etc/zabbix/zabbix_server.conf

```
DBHost=localhost
DBName=zabbix
DBUser=zabbix
DBPassword=senha
```

Ok, agora é a hora da verdade, vamos verificar se o agente e o servidor rodam corretamente:

 # zabbix_server

 # zabbix_agentd

Após executar estes dois comandos, digite:

 # ps aux | grep zabbix

Ele deve mostrar várias instâncias do *zabbix_agentd* e do *zabbix_server* rodando:

```
zabbix    2390  0.0  0.1  52908  1520 ?        S    15:32   0:00 zabbix_server
zabbix    2391  0.0  0.1  52912  1496 ?        S    15:32   0:00 zabbix_server
zabbix    2392  0.0  0.1  52908  1308 ?        S    15:32   0:00 zabbix_server
zabbix    2421  0.0  0.0  10164   912 ?        S    15:32   0:00 zabbix_agentd
zabbix    2422  0.0  0.0  10164   888 ?        S    15:32   0:00 zabbix_agentd
zabbix    2423  0.0  0.0  10164   728 ?        S    15:32   0:00 zabbix_agentd
```

(...)

Instalando o front-end do Zabbix Server:

 # mkdir /var/www/html/zabbix

 # cd frontends/php

 # cp * -R /var/www/html/zabbix/

 # chown apache:apache /var/www/html/zabbix/ -R

 # /etc/init.d/httpd start

Nos comandos acima, respectivamente:

- Criamos a pasta */var/www/html/zabbix*;
- Acessamos a pasta *frontends/php*;
- Copiamos todos os arquivos e diretórios da pasta *frontends/php* para a pasta */var/www/html/zabbix*;
- Demos permissão da pasta */var/www/html/zabbix* e todos os arquivos e diretórios para o usuário Apache;
- Iniciamos o serviço do Apache.

Para acessar o *front-end*, basta ir em seu navegador preferido (que não seja o IE, por favor!) e digitar:

- http://ip_do_servidor/zabbix

Clique em Next e deverá cair em uma tela mais ou menos assim, verifique se está tudo OK:

Nesta tela, coloque as configurações do nosso BD e teste a conexão se aparecer OK, estamos no caminho certo! Clique em Next.

Não é necessário colocar o nome, então basta clicar em Next.

Confira os dados e clique em Next.

Se a tela for semelhante a esta, parabéns! Você instalou o servidor Zabbix com sucesso, para prosseguir, basta clicar em Finish!

Entre com o nome de usuário *admin* e a senha *zabbix*

Esta é a interface gráfica administrativa do Zabbix.

Instalando e configurando clientes no GNU/Linux

Caso queira monitorar outro computador GNU/Linux, é necessário instalar o agente *Zabbix* no mesmo. No caso do *CentOS*, basta seguir os passos abaixo.

Baixar e instalar o *Atomic*:

 # wget -q -O - | sh

Atualizar o sistema:

 # yum update

Instalar o agente:

 # yum install zabbix-agent

Editar o arquivo:

 # vim /etc/zabbix/zabbix_agentd.conf

Server=<ip_do_servidor>
Hostname=<nome_do_computador>

Reiniciar o agente:

 # /etc/init.d/zabbix-agent restart

Para cadastrar o computador no Zabbix, acesse a interface Web e vá no menu:

Configuration → Hosts → Create Host

Em "Host name", colocar o nome da máquina exatamente do mesmo modo que você colocou na configuração do agente no arquivo "zabbix_agentd.conf", e em "IP Address" colocar o IP da máquina que deseja monitorar.

Feito isso, salve a configuração e vá em:

Monitoring → Latest Data

ANEXO B – INSTRUÇÕES E COMANDOS PARA INSTALAÇÃO DO NO-IP

Este conteúdo foi extraído em 16/10/2013 do site http://my.opera.com/sir-guil/blog/2013/02/01/instalando-no-ip-no-centos-6-dynamic-dns

Instalando no-ip no CentOS 6 "Dynamic DNS"

sexta-feira, 1 de fevereiro de 2013 12:00:00

centos, dynamic dns, no-ip, ddns, Linux

O grande obstáculo para rodar servidores ou programas de acesso remoto em uma conexão com IP dinâmico é justamente o fato de que o endereço muda constantemente. Você poderia muito bem instalar um servidor web, configurado para usar a porta 8080 e dizer para para um amigo acessá-lo através do http://seu-endereço-ip:8080, mas ele precisaria perguntar o endereço novamente cada vez que fosse acessar seu servidor, já que o endereço seria diferente. A situação seria ainda mais complicada se você precisasse acessar seu micro via SSH (ou qualquer programa de acesso remoto), já que se você não está em casa, não há como saber o endereço corrente.

A solução para o problema é utilizar um serviço de DNS Dinâmico (Dynamic DNS), onde você pode registrar um endereço de acesso como "meu-nome.no-ip.org", que passa a apontar para seu endereço IP corrente.

Então vamos lá!

A 1ª coisa a se fazer para usar este serviço é criar uma conta no no-ip, então se ainda não o fez http://www.noip.com/newUser.php

A 2ª é criar o hostname caso você não tenha feito durante o cadastro ou queira incluir mais, abra esta pagina https://www.noip.com/members/dns/host.php, faça o loguin e . . .

A etapa de criar acount e host esta muito bem documentada na web e também e muito simples por isso não abordei aqui mas se surgirem duvidas no final deste post deixo um link para ajudar, e mesmo assim estou aqui para ajudar.

A 3ª é instalar o aplicativo que atualiza o ip para que o serviço DDNS funcione, agora você pode optar por instalar em uma maquina windows dentro de sua rede para que ela atualize , mas se o windows parar ou travar (ta eu sei que isso não acontece estou apenas criando uma hipótese) o serviço ficará com o seu ip desatualizado e consequentemente você não terá mais o acesso desejado.

Vou apresentar duas maneiras de instalar o aplicativo no CentOS 6:

1ª maneira usando o yum

O no-ip não compõem o repositório oficial do centos, para suprir isto adicione o RPMForge, clique aqui caso ainda não tenha feito.

```
yum -y install noip
chkconfig noip on
noip2 -C
```

Passo a passo simples para configurar o no-ip

Selecione a interface de rede referente a internet pelos números ao lado esquerdo

Informe o usuário do no-ip

Senha do usuário

Caso tenha mais de um host cadastrado o sistema perguntará se deseja atualizar todos simultaneamente, digite “n”

Digite “y” para o host que deseja atualizar e “n” para os demais

Deixe o campo vazio “enter”

Informe um “n”

Reinicie o serviço

```
service noip restart
```

2ª maneira usando os dedos

```
yum -y install wget
yum -y install make
wget -v -c http://www.no-ip.com/client/linux/noip-duc-linux.tar.gz
tar -zxvf noip-duc-linux.tar.gz
cd noip-2.*
cp binaries/noip2-$(uname -m) noip2
make install
```

Mesmo passo a passo simples de cima

Selecione a interface de rede referente a internet pelos números ao lado esquerdo

Informe o usuário do no-ip

Senha do usuário

Caso tenha mais de um host cadastrado o sistema perguntará se deseja atualizar todos

simultaneamente, digite “n”

Digite “y” para o host que deseja atualizar e “n” para os demais

Deixe o campo vazio “enter”

Informe um “n”

Agora vamos colocar o no-ip para iniciar com o sistema

```
cp ./redhat.noip.sh /etc/init.d/noip2
cd ..
rm -f noip-2.* noip-duc-linux.tar.gz
chmod 755 /etc/init.d/noip2
chkconfig --add /etc/init.d/noip2
chkconfig noip2 on
service noip2 restart
```

Fei isso basta usar um "ping", "tracert", "nmap", "traceroute", "tracepath", "ssh", . . . de fora da sua rede para ter um retorno

Mais informações em http://www.noip.com/support/guides/update_clients /setting_up_linux_update_client.html

Principal fonte de pesquisa: http://www.hardware.com.br/dicas/servicos-dns-dinamico.html