Faculdade de Tecnologia de Americana
Curso de Segurança da Informação

MARCOS TEODORO DA SILVA

GERÊNCIA DE REDES COM ZABBIX

Americana, SP
2013

Faculdade de Tecnologia de Americana
Curso de Segurança da Informação

MARCOS TEODORO DA SILVA

GERÊNCIA DE REDES COM ZABBIX

Trabalho de conclusão de curso apresentada a Faculdade de Tecnologia de Americana como partes das exigências do curso de Tecnologia em Segurança da Informação para obtenção de título de Tecnólogo em Segurança da Informação.

Orientador: Prof. Esp. Rogério Nunes de Freitas

Americana, SP
2013

MARCOS TEODORO DA SILVA

GERÊNCIA DE REDES COM ZABBIX

Trabalho de conclusão de curso aprovada como requisito para obtenção do título de Tecnólogo em Segurança da Informação no curso de Tecnologia em Segurança da Informação da Faculdade de Tecnologia de Americana.

Banca Examinadora

Orientador: _____
Prof. Esp. Rogério Nunes de Freitas – FATEC

Convidado: _____
Prof. Esp. Benedito Aparecido Cruz – FATEC

Presidente:_____
Prof. Ms. Carlos Henrique Rodrigues Sarro – FATEC

Americana, 12/05/2013

AGRADECIMENTOS

Agradeço a Deus por ter me dado força nos momentos difíceis e me proporcionar a oportunidade de fazer graduação em uma ótima faculdade pública.

Agradeço a minha esposa por ter sido muitas vezes pai e mãe do nosso filho nos momentos em que estive ausente e também por me dar muita força nesta etapa da minha vida.

Agradeço aos amigos que durante essa caminhada estiveram me ajudando nas dificuldades.

Agradeço a todos os professores que me deram um pouco do seu conhecimento e em especial aos professores orientadores Rogério e Carlos Sarro pela paciência na orientação deste trabalho.

Ao professor Benedito por ser meu convidado na banca desta monografia.

A todos o meu muito obrigado.

RESUMO

As organizações vêm investindo alto na automatização de seu parque tecnológico, com isso as redes de computadores têm ficado cada vez maiores e mais complexas. Para que a empresa tenha o controle sobre seus ativos, segurança e disponibilidade de suas informações se torna fundamental que a mesma seja gerenciada de forma segura e eficaz. Para isso é necessário ter um bom software de gerenciamento de redes que possibilite ter informações em tempo real para tomada de decisões precisas. O estudo de caso apresentado neste trabalho vem demonstrar que o Zabbix é uma ferramenta precisa, segura e robusta proporcionando ao administrador da rede todas as informações necessárias para que se tenha uma rede funcional e segura, permitindo que a alta administração se preocupe somente com o negócio principal da empresa.

Palavras Chave: Zabbix, Gerência de Rede, Segurança.

ABSTRACT

Organizations are heavily investing in automating their technological park, therefore computer networks have become increasingly larger and more complex. The company has to keep control over their assets, so security and availability of their information becomes critical, in order to be safely and effectively managed. It is really necessary to have a good network management software that allows to have real-time information for decision making to be more accurate. The case study presented in this paper demonstrates that Zabbix is an accurate tool, always providing safe and robust information to the network administrator, in order to have a functional and a safe network, allowing senior management to only worry about the main business activities.

Keywords: Zabbix, Network Management, Security.

LISTA DE FIGURAS

LISTA DE TABELAS

LISTA DE ABREVIATURAS E SIGLAS

Mbps – *Megabits*/s

Gbps – *Gigabits*/s

LAN – *Local Area Network*

MAN – *Metropolitan Area Network*

HTTP - *Hypertext Transfer Protocol*

SMTP – *Simple Mail Transfer Protocol*

ICMP – *Internet Control Message Protocol*

SMS – *Short Message Service*

TI – Tecnologia da Informação

IEEE – Instituto de Engenheiros Eletricistas e Eletrônicos

FTP – *File Transfer Protocol*

IP – *Internet Protocol*

TCP - *Transmission Control Protocol*

MAC – *Media Access Control*

RFC – *Request for Comments*

SUMÁRIO

1. INTRODUÇÃO

Com o avanço da tecnologia e a redução dos custos com computadores, as empresas tem agregado cada vez mais equipamentos em sua rede, com isso as redes de computadores vêm se tornando cada vez maiores e mais complexas. As organizações estão se expandindo para lugares distantes em busca de novos mercados, isso faz com que os dados necessitem trafegar por longas distâncias entre filiais. Com o crescimento das empresas, aumenta também o número de funcionários e por consequência a quantidade de informações que trafegam pela rede. A competitividade faz com que exista um desenvolvimento constante de novos produtos, com isso é preciso manter a segurança da rede, para que as informações não se tornem acessíveis para os concorrentes.

Algumas empresas disponibilizam uma parte de sua base de dados aos fornecedores, como por exemplo, o estoque, assim o fornecedor pode repor na hora certa permitindo que a empresa trabalhe com o mínimo de estoque possível. Para isso é muito importante o monitoramento de quem está utilizando o sistema, quantas vezes e qual o tempo que a pessoa utilizou o sistema da empresa. A terceirização também deve ser levada em conta, já que é muito comum serviços que não são o foco dos negócios sejam terceirizados, assim, um guarda, um supervisor de restaurante, entre outros possam utilizar o sistema da organização sem maiores problemas.

Diante desse cenário se torna indispensável o gerenciamento dos ativos de TI de forma correta e segura para manter a disponibilidade e segurança do negócio. O gerenciamento consiste na coleta de informações sobre os dados que estão trafegando pela rede, espaço disponível em disco, quais usuários estão autenticados na rede, monitoramento de *logs,* existência de servidor parado, tudo em tempo real. Com isso o administrador tem condições de tomar a decisão certa em tempo hábil para que o negócio não seja prejudicado ou em caso de falhas a mesma possa ser minimizada de forma a afetar a operação da menor maneira possível.

Esse trabalho pretende demonstrar os benefícios de se ter uma rede com monitoramento, iremos simular dois ambientes, onde um não possui nenhum tipo de monitoramento e na outra o administrador conta com sistema de NMS (*Network*

Management System) que coleta as informações via agentes e os envia para uma estação de gerenciamento.

Para isso iremos utilizar uma solução de código aberto que utiliza interface *web*, armazena as informações em bancos de dados. Essa ferramenta se propõe monitorar vários parâmetros de rede de computadores, assim como a saúde e integridade de servidores, utiliza um mecanismo de notificação flexível que permite aos usuários configurarem alerta de *e-mail* baseado em praticamente qualquer evento. Isto permite que os administradores possam tomar as decisões acertadas e de forma rápida (SIA, 2010).

2. REDE DE COMPUTADORES

Conforme Kurose (2010), podemos dizer que rede de computadores é um termo que está desatualizado, já que uma rede pode ser formada por uma enorme quantidade de equipamentos, como: celulares, *tablets*, impressoras, *notebook* e uma infinidade de dispositivos que podem se comunicar uns com os outros através de meios físicos, que podem ser pares metálicos ou cabos coaxiais, o nome dado aos dispositivos finais de uma rede é *Host*.

Essa comunicação permite uma interação mais rápida e dinâmica de forma que as pessoas podem utilizar um recurso de um determinado local mesmo estando a quilômetros de distância.

2.1. Classificação de Redes

As redes podem ser classificadas por 3 tipos:

LAN – *Local Area Network* (Rede local);

MAN – *Metropolitan Area Network* (Rede de área metropolitana);

WAN – *Wide Area Network* (Rede Geograficamente Distribuída).

2.1.1. LAN – *Local Área Network*

Conforme Behrouz (2008), uma rede local pode ser privada ou pública, seus *links* estão delimitados por um muro ou pelas paredes de um prédio, podendo ser uma rede de um escritório com apenas dois computadores e uma impressora ligada entre si, ou a rede de uma grande empresa com centenas de computadores. Essa denominação é utilizada para uma rede que tenha no máximo alguns quilômetros entre seus *hosts*.

Tem como características o compartilhamento de equipamentos e *software*s formando grupos de trabalhos com um objetivo em comum, permitindo que se possa obter agilidade e o tráfego de muita informação de forma rápida. Outro ponto forte é a possibilidade de se ter servidores centralizados e permitir que os usuários da rede utilizem os *softwares* instalados nesse servidor de forma que toda a sua configuração

seja feita apenas em uma única máquina, reduzindo drasticamente a necessidade de um gerenciamento complexo e de alto custo.

Conforme Tanenbaum (2003), as LANs tem velocidades que vão de 10 Mbps a 100 Mbps e muitas já possuem a velocidade de 10 Gbps, têm baixas taxas de erro e alto tempo de resposta. Além disso, outra característica que pode diferenciar os tipos de redes é a topologia, que nada mais é que a forma com que os hosts de uma rede são ligados entre si.

2.1.2. MAN – *Metropolitan Area Network*

São redes que ligam podem ligar pontos que estão geograficamente distantes, mas dentro de uma cidade ou em cidades vizinhas, trafegam dados, voz e imagens em altas velocidades.

Conforme Tanenbaum (2003), uma MAN é uma versão ampliada de uma LAN isso pelo fato de usarem tecnologias muito semelhantes e todos os serviços de uma rede local deve estar disponível em qualquer ponto da mesma. Essas redes podem ser públicas ou privadas, nos dias de hoje é muito utilizada por operadoras de TV a cabo por permitirem altas velocidades em distâncias razoáveis.

2.1.3. WAN – *Wide Area Network*

Conforme Tanenbaum (2003), WAN é uma rede geograficamente distribuída que abrange uma grande área podendo ser um país ou até mesmo um continente, que tem como finalidade executar aplicações dos usuários.

2.2. Topologia de Redes

Conforme Soares (1995), a topologia de redes refere-se à maneira de como os enlaces físicos e os nós de comutação estão organizados determinando os caminhos físicos existentes e utilizáveis entre quaisquer pares de dispositivos finais. Outros fatores podem determinar a topologia são as restrições dos equipamentos e as características das tecnologias utilizadas.

2.2.1. Malha

Esta topologia apresenta baixa taxa de erros de transmissão e melhor velocidade reduzindo o tempo de espera, pois todos os nós estão ligados a vários outros nós, quando um *enlace* é rompido os pacotes são enviados por outros caminhos garantindo que os pacotes chegarão ao seu destino (SOARES, 1995).

Um ponto negativo desta topologia é a quantidade de placas de rede que cada máquina deve ter para que possa ser conectada a outras máquinas. A figura 1 mostra que uma máquina possui vários *enlaces* conectados (SOARES, 1995).

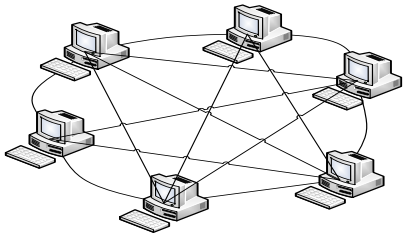


Figura 1 - Topologia em Malha (BMED, 2012).

2.2.2. Barramento

Apenas um *host* pode enviar os dados em um determinado momento, quando um dado está trafegando o *host* reconhece que aquele dado está destinado e ele e retira da rede de forma que fica liberado para o próximo equipamento disponibilizar seus pacotes na rede (SOARES, 1995).

Nesta topologia o fluxo de transmissão de dados é chamado serial, pois o *enlace* é compartilhado por tempo e frequência. A figura 2 mostra *hosts* ligados por barramento.

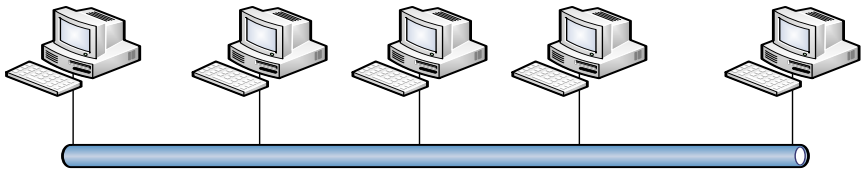


Figura 2 - Topologia Barramento (BMED, 2012).

2.2.3. Anel

Conforme Soares (1995), a figura 3 demonstra que nesta topologia os dispositivos são conectados de maneira a formar um circuito fechado, os dados são transmitidos em apenas uma direção passando por todos os nós da rede até chegar ao destinatário. Possui algumas limitações devido à sua distribuição, se a quantidade de máquinas for aumentada o tempo de transmissão aumenta muito, tornando a rede inviável.

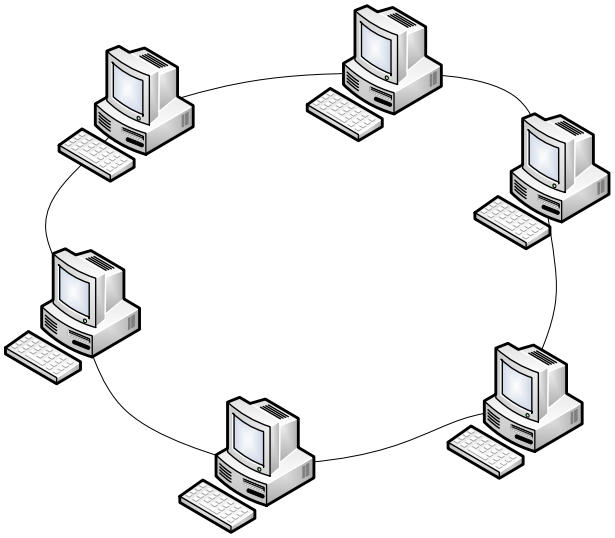


Figura 3 - Topologia Anel (BMED, 2012).

2.2.4. Estrela

Conforme Soares (1995), é a topologia mais comum, utiliza como *enlace* o cabo par trançado e um concentrador que fica encarregado de fazer o roteamento para que os pacotes sejam entregues somente ao destinatário, tornando a transferência muito

mais eficaz já que não passa por todos os nós da rede. Caso um *host* apresente problemas, apenas ele ficará fora da rede, todos os outros continuarão a receber seus pacotes normalmente.

Conforme Soares (1995), esta topologia apresenta várias as vantagens: não requer muito trabalho para a instalação de novos *hosts*, fica mais simples identificar problemas, em caso de mudanças e expansões fica mais fácil dispor os equipamentos, caso um componente precise ser retirado o restante continua trabalhando normalmente. A figura 4 mostra uma rede que possui um servidor centralizado.

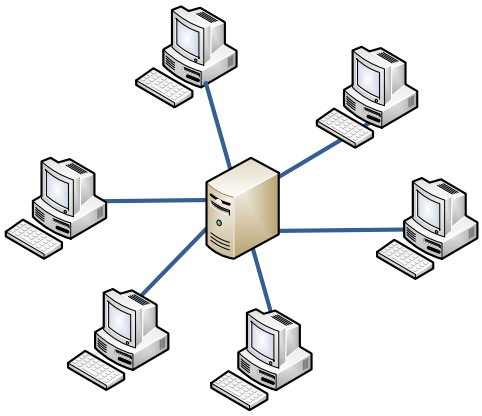


Figura 4 - Topologia Estrela (BMED, 2012).

2.3. Protocolo TCP/IP

Quando falamos de redes de computadores, estamos falando diretamente de dispositivos finais ligados entre si, como já foi dito podemos ter os mais diversos tipos de equipamentos em uma rede, basta que esse dispositivo possa enviar e receber informações.

Conforme Behrouz (2008), para que esses diferentes dispositivos possam se comunicar é preciso de um protocolo, que é um conjunto de regras que os equipamentos dever seguir para que suas informações sejam compreendidas pelo dispositivo na outra extremidade da rede, ou seja, um protocolo nada mais é que um conjunto de regras que determinam como será realizada a comunicação entre os equipamentos da rede.

Para diminuir a complexidade da implementação de um serviço ou facilitar a manutenção de um dispositivo ou uma aplicação, foi definido pelo IEEE[1] a arquitetura em camadas, onde cada camada tem seu próprio protocolo e fornece um serviço à camada de nível superior e assim por diante, até que se tenha um serviço prestado ao usuário.

Devido à necessidade de comunicação entre sistemas de computadores e diversas organizações militares o Departamento de Defesa Americano criou em 1969 o ARPANET[2] um projeto experimental para fornecer técnicas robustas e confiáveis de comunicação para *links* de alta velocidade utilizando redes de comutação de pacotes (HUNT, 1993).

Em 1983 os militares adotaram o protocolo TCP/IP[3] como padrão e definiram que todos os computadores que fizessem parte da ARPANET passariam a utilizar esse protocolo, com isso a rede foi se expandindo para universidades, organizações até que usuários domésticos passassem a fazer parte dela e hoje conhecemos por Internet. O nome TCP/IP vem dos protocolos (*Trasmission Control Protocol*) e (*Internet Protocol)* que são mais utilizados, porém, existem muitos outros.

Conforme Hunt (1993), o protocolo TCP/IP se tornou o mais utilizado por possuir grandes vantagens:

- ✓ Padrão aberto, disponível livremente e independente do *hardware* ou sistema operacional, permitindo que tanto novas quanto as mais antigas tecnologias possam se comunicar;
- ✓ Protocolo altamente escalável, multiplataforma, permite a tecnologia cliente-servidor;
- ✓ Possibilita que todo dispositivo possa se comunicar com outro na rede, seja qual for o tamanho da rede;
- ✓ Permite conectar sistemas mesmo não sendo similares, para transferência de dados entre si.

[1] Instituto de Engenheiros Eletricistas e Eletrônicos
[2] *Advanced Research and Projects Agency Network* – Rede que deu origem à Internet
[3] Conjunto de protocolos de rede

Conforme Tanenbaum (2003), os protocolos foram organizados em camadas que são dispostas umas sobre as outras de forma a reduzir a complexidade, onde as funções são as mesmas, independente da rede em que esteja.

Outro modelo de camadas é o OSI - *Open Systems Interconnection* (Sistema Aberto de Interconexão), modelo criado pela ISO - *International Organization for Standardization* (Organização Internacional de Padronização), porém o modelo TCP é mais prático e utiliza-se de quatro camadas como mostra a figura 5.

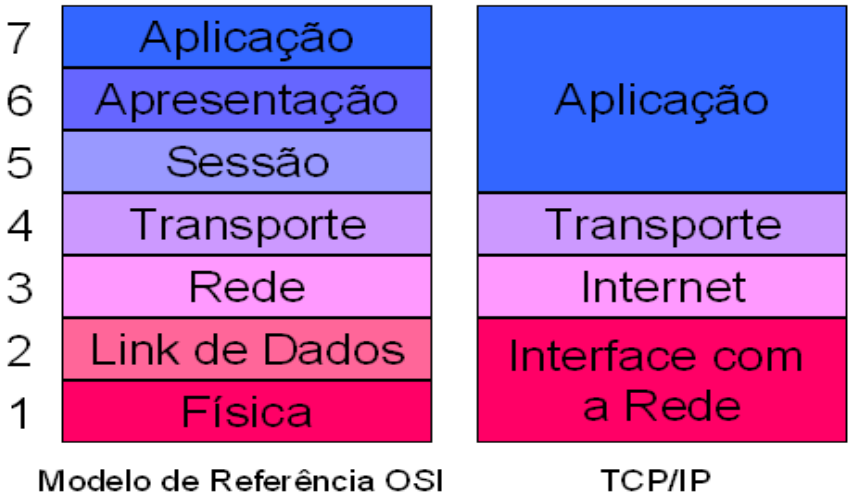


Figura 5 - Arquitetura em Camadas (TORRES, 2007).

A figura 6 demonstra alguns protocolos e suas respectivas camadas:

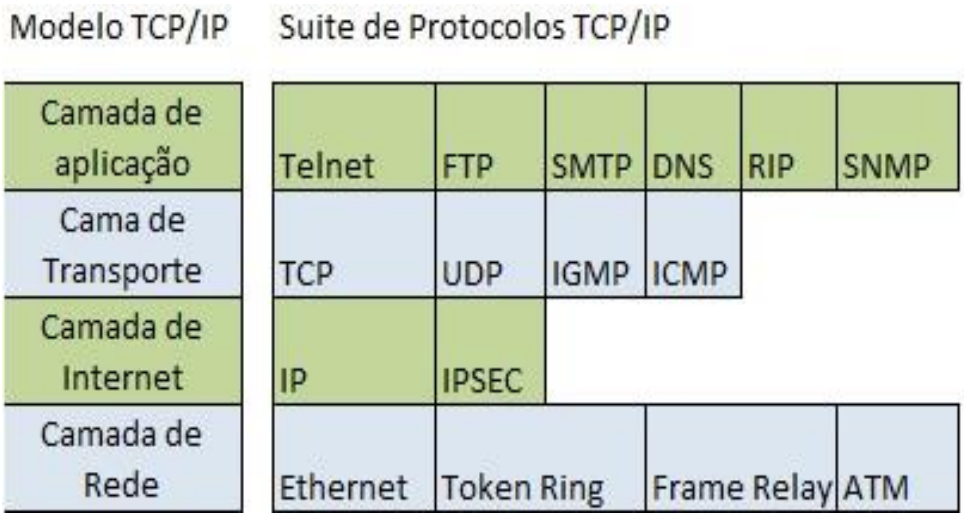


Figura 6 - Protocolos TCP/IP (MICROSOFT, 2013).

2.3.1. Camada de Aplicação

Conforme Tanenbaum (2003), a camada de aplicação é responsável por suportar as aplicações de rede e que tratam diretamente com o usuário. Existem diversos protocolos operando nesta camada, onde os mais conhecidos são: HTTP *(Hypertext Transfer Protocol), SMTP (Simple Mail Transfer Protocol), FTP (File Transfer Protocol), DNS (Domain Name Service)* entre outros.

Essa camada comunica-se com a inferior através de portas representadas por números, onde é possível identificar o tipo de conteúdo que trafega por determinada porta podemos citar como exemplo o HTTP que utiliza a porta 80, o SMTP a porta 25, o FTP a porta 21.

Essa camada se preocupa com a aplicação que está sendo utilizada pelo usuário e não como dos dados trafegam por entre a rede, esse tráfego diz respeito às outras três camadas.

2.3.2. Camada de Transporte

Conforme Tanenbaum (2003), a função da camada de transporte é permitir que pares de *hosts* (origem e destino) mantenham uma conversação. O protocolo TCP é confiável e orientado a conexão, permitindo que seja entregue sem erros um fluxo de *bytes* de uma máquina origem para qualquer outra da rede.

Esse protocolo fragmenta o fluxo de *bytes* e passa para a camada imediatamente inferior onde envia para o destino que recebe repassa novamente para a camada de transporte que irá juntar os fragmentos e montar as mensagens novamente, também é responsável pelo controle de fluxo para que o destino não seja sobrecarregado com uma grande quantidade de mensagens.

Conforme Tanenbaum (2003), outro pacote que opera nesta camada é o UDP[4] *(User Datagram Protoco*l) que não é um pacote orientado a conexão e por isso não

[4] User Datagram Protocol - Protocolo de rede da camada de transporte

verificar se o pacote chegou ao seu destino, com essa característica ele não pode ser utilizado para a entrega de mensagens importantes como *e-mail* e etc.

2.3.3. Camada de Rede

Conforme Kurose (2010), a função desta camada é permitir que dispositivos finais enviem pacotes a outros dispositivos independente do destino, mesmo estando localizada geograficamente distante, esses pacotes podem chegar até mesmo em uma orde diferente da que foi enviado, cabe as camadas superiores a juntas e ordenar esses pacotes.

Nessa camada é utilizado o protocolo de IP que oferece o serviço de datagramas que é tratado de forma independente, não recebendo nenhum tipo de tratamento. Ao receber um segmento da camada acima (transporte) ela o encapsula escreve o endereço IP e envia ao primeiro roteador com destino ao *host* indicado, e essa camada envolve todos os roteadores até o seu destino final.

A figura 7 mostra a estrutura de um datagrama IP.

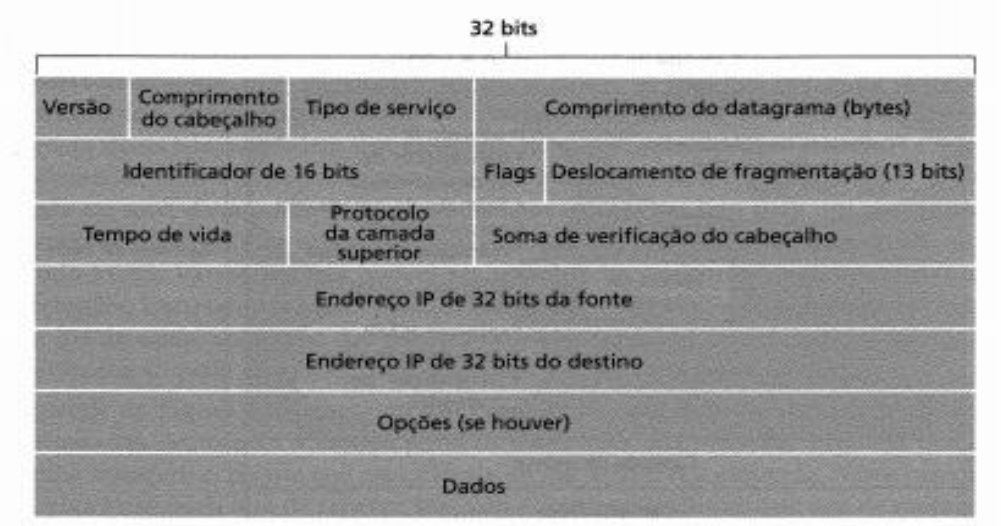


Figura 7 - Datagrama do Protocolo IP (KUROSE, 2010).

2.3.4. Camada de *Enlace*

Conforme Kurose (2010), enlace é o canal de comunicação entre dois *hosts* ao longo de uma rota, a função desta camada é fazer a interface entre o modelo TCP/IP e os diferentes tipos de redes, onde inclui o driver e a interface de rede que juntos

tratam do *hardware* e da mídia por onde os *frames* (datagramas em formato que possa trafegar pelo meio físico) possam trafegar.

2.4. Equipamentos de Rede

Para que haja comunicação entre os equipamentos de uma rede, é necessário que além do cabeamento a rede tenha equipamentos que possam fazer a transferência dos dados entre rede e subredes de forma que uma rede por menor que seja possa se comunicar com outra geologicamente distante (PINHEIRO, 2004).

Para que isso seja possível é preciso que alguns equipamentos faça a interconexão das redes, a figura 8 demonstra os principais equipamentos:

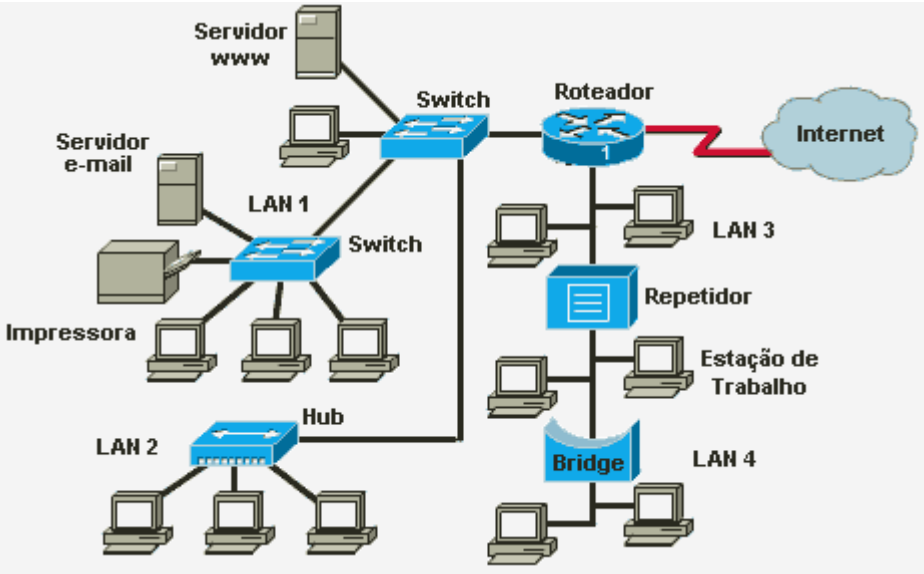


Figura 8 - Equipamentos Interconectados (PINHEIRO, 2004).

2.4.1. Rack de rede

Armário ou gabinete onde são instalados os *switches*[5], roteadores, *patch-panel* e outros equipamentos conforme as normas técnicas vigentes para que possam ser feitas as ligações dos cabos nos aparelhos dando condições para a comunicação da rede (RUSSO, 2012).

[5] Equipamento de rede responsável por encaminhar os pacotes aos devidos nós.

2.4.2. Patch-Panel

Painel de distribuição de cabos que serve de intermediário entre pontos de conexão de *switches* e roteadores (PINHEIRO, 2004).

Quando uma rede é planejada, todos os locais que podem ter um equipamento tem seu cabeamento passado e se encontra com a identificação no *patch-panel*, dessa forma basta colocar o equipamento em uma ponta e fazer a ligação da outra ponta com o *switch* ou *hub* facilitando o trabalho no momento da instalação.

2.4.3. Repetidor

Responsável por amplificar o restaurar o sinal, fazendo a interpretação e amplificação do sinal recebido para que possa chegar de forma que o receptor possa trabalhar, o número de repetidores deve ser limitado e não podem estar a mais de 2,5 Km de distância. É o mais básico dos equipamentos de interconexão de redes, atua na camada física (PINHEIRO, 2004).

2.4.4. Hub

Conforme (Cisco Systens, 2003), *hub* é o ponto central de conexão entre segmentos de rede, o que o diferencia de um repetidor é o número de portas, um repetidor possui normalmente duas portas, já u Hub possui de 4 a 24 portas. O *hub* recebe os sinais e retransmite a outros nós da rede, atualmente é encontrado três tipos de *Hubs* no mercado:

- ✓ Passivos: Atua por *broadcast*, ou seja, transmite o sinal a todos os outros nós da rede, e com isso a distância dos equipamentos é limitada pelo tipo de mídia por onde os dados são trafegados;

- ✓ Ativos: Atua da mesma forma que os passivos, porém, limpa e amplifica os sinais, mas ainda assim transmite para todos os outros nós.

- ✓ Inteligentes: Por possuir uma tabela onde armazena os endereços de mac address[6] dos nós, tem a capacidade de fazer a comutação dos dados de forma que seja transmitido apenas ao interessado.

2.4.5. Pontes (*Bridges*)

É o equipamento responsável pela interconexão de redes, ou seja, permite segmentar uma rede em várias subredes, trabalham na camada de interconexão e operam apenas com o endereço físico (*mac address*) (PINHEIRO, 2004).

Quando configurado de forma correta tem a função de filtragem de sinais, permitindo descartar sinais endereçados a outros nós evitando o *broadcast* desnecessário. Outro aspecto que deve ser ressaltado é a diferença de velocidade entre as redes, apesar de não alterar a velocidade ele pode amortecer a diferença armazenando quadros de forma temporária.

2.4.6. Switches

Semelhante ao *Hub*, mas com funções de pontes e roteadores oferece alta eficiência a um preço acessível. Possuem barramentos que são comutáveis permitindo chavear conexões, o que torna dedicado a dois nós fornecendo toda a capacidade do meio físico existente. Com a o aumento da demanda por maiores velocidades de transmissão tornou-se muito necessário nas redes locais (PINHEIRO, 2004).

Tem como função filtrar as mensagens de forma que só sejam transmitidas a que de fato está endereçada, ler o pacote e restransmiti-lo, armazenar pacotes quando o tráfego for muito grande e também funciona como uma estação repetidora (PINHEIRO, 2004).

2.4.7. Placa de rede

Todos os nós de uma rede devem possuir uma placa de rede que funciona como uma interface entre o computador e o cabeamento. Tem um *software* (*driver*)

[6] Media Access Control Endereço associado à placa de rede

que faz a comunicação entre a placa e o sistema operacional, permitindo receber e transmitir dados a partir da rede onde se encontra (PINHEIRO, 2004).

Para que os dados possam ter uma velocidade compatível com a rede, a placa de rede possui uma área de armazenamento denominada *Buffer*, pois existe uma diferença na forma que o computador processa dos dados e como são lançados na rede.

3. GERÊNCIA DE REDES

Uma rede de computadores é formada por uma enorme variedade de equipamentos (computadores, impressoras, roteadores, entre outros dispositivos), *softwares* e protocolos, que precisam interagir entre si para que seu objetivo que é a troca de informações e compartilhamento de dispositivos seja alcançado de forma plena.

Conforme Kurose (2010), quando esses dispositivos estão em funcionamento, não é de surpreender que eles apresentem defeitos, estejam mal configurados, sobrecarregados ou até mesmo quebrem. É nesta hora que o administrador de redes deve estar preparado para atuar de forma proativa para que não haja interrupção dos serviços prestados.

Conforme (SAYDAM, 1996), expressa de forma mais formal o que é a gerência de redes:

> ***"Gerenciamento de rede inclui o oferecimento, a integração e a coordenação de elementos de hardware, software e humanos, para monitorar, testar, consultar, configurar, analisar, avaliar e controlar os recursos da rede, e de elementos, para satisfazer às exigências operacionais, de desempenho e de qualidade de serviço em tempo real a um custo razoável"***

Conforme Kurose (2010), para que a rede seja administrada de forma adequada é necessário que se tenha monitoramento constante. Com uma ferramenta adequada e que o administrador tenho o domínio sobre ela.

3.1. Tipos de Monitoramentos

Através da detecção de falhas em placas de hospedeiros ou roteadores, é possível ver que o tráfego na placa está alterado o que pode indicar que a mesma está necessitando ser trocada, podendo evitar que pare de funcionar repentinamente e deixar o usuário insatisfeito, para que possam ser visualizados esses eventos nos equipamentos existem tipos de monitoramentos (KUROSE, 2010).

3.1.1. Monitoramento de Hospedeiros

O sistema de monitoramento pode ser configurado para que em caso de queda, seja enviada uma notificação ao responsável pelo suporte, com isso muitas vezes o usuário nem tomará conhecimento de que o equipamento esteve parado por alguns instantes (KUROSE, 2010).

3.1.2. Monitoramento do tráfego

Com o monitoramento de tráfego é possível melhorar o roteamento para que o desempenho da LAN tenha melhora significativa. Da mesma forma quando se monitora um enlace seja interno ou de ligação ao mundo externo, é possível identificar a sobrecarga e então solicitar um *link* de maior capacidade (KUROSE, 2010).

3.1.3. Detecção de mudanças rápidas nas tabelas de roteamento

Essas mudanças podem indicar roteador mal configurado ou instabilidades no roteamento, o administrador tem plenas condições de alterar as configurações antes que o serviço seja interrompido (KUROSE, 2010).

3.1.4. Detecção de intrusos

Para garantir a segurança o administrador terá que saber quais os pacotes que chegam a sua rede, a fim de detectar a existência de certos tipos de tráfegos podendo prevenir ataques e invasões (KUROSE, 2010).

3.2. Tipos de gerência

Para que a rede seja gerenciada de forma eficiente e segura, se faz necessário a utilização de um sistema de gerenciamento de rede segundo o modelo FCAPS (*Fault, Configuration, Accounting, Performance and Security Management*), estabelecida pela ISO (*International Organization for Standardization*) (BRISA, 1993).

3.2.1. Gerenciamento de desempenho

A meta do gerenciamento de desempenho é quantificar, medir, informar, analisar e controlar o desempenho (por exemplo, utilização e vazão) de diferentes componentes da rede. Entre esses componentes estão dispositivos individuais (por exemplo, *enlaces*, roteadores, e hospedeiros), bem como abstrações fim a fim, como um trajeto pela rede (KUROSE, 2010).

3.2.2. Gerenciamento de Falhas

É necessário para registrar, detectar e reagir às condições de falhas da rede. Podemos fazer uma diferença entre gerência de falha e gerência de desempenho, onde a de falha requer uma intervenção imediata, já a de desempenho pode adotar uma abordagem em longo prazo (DUARTE, 2011).

3.2.3. Gerenciamento de configuração

Permite ao administrador saber quais dispositivos fazem parte da rede assim como suas configurações de *hardware* e *software*, permitindo que qualquer elemento que faça parte da rede seja rastreável e gerenciável (DUARTE, 2011).

3.2.4. Gerenciamento de contabilização

Permite que o administrador especificar registrar e controlar os acessos de usuários aos recursos e dispositivos da rede. Também fazem parte deste tipo de configuração as quotas e privilégios de acesso permitindo melhor utilização dos recursos diante da distribuição conforme sua capacidade (DUARTE, 2011).

3.2.5. Gerenciamento de segurança

É possível controlar os acessos aos recursos da rede de acordo com as políticas de segurança definidas pela organização realizando a prevenção de ataques e outros acontecimentos indesejados que possam interferir no pleno funcionamento da rede (DUARTE, 2011).

3.3. Agentes e Gerentes

Conforme Kurose (2010), para uma arquitetura de gerenciamento de redes é necessário que se tenha três componentes, entidade gerenciadora, dispositivo gerenciado e o protocolo de gerenciamento; Desta forma será possível que uma máquina central receba e trate todas as informações de todos os dispositivos que compõem a rede.

Entidade gerenciadora é uma estação central que tem uma pessoa controlando um *software* que se comunica com os demais componentes, é responsável por coletar, analisar e apresentar as informações de modo que possam ser interpretadas pelo administrador (KUROSE, 2010).

Dispositivo gerenciado é um componente que faz parte da rede, podendo ser um *hub*, roteador, computador, impressora ou qualquer outro componente que esteja na rede, e este dispositivo pode conter diversos componentes gerenciados (placas de rede, disco rígido, etc.), também é possível monitorar *softwares* e protocolos. Em cada dispositivo contém um agente de gerenciamento de rede que se comunica com a entidade de gerenciamento e através de seus controles e comandos executa as ações locais (KUROSE, 2010).

Protocolo de gerenciamento é executado entre a entidade gerenciadora e o agente de gerenciamento dos dispositivos gerenciados, com ele é possível que a unidade gerenciadora investigue o estado dos dispositivos gerenciados e tome as ações cabíveis. O protocolo de gerenciamento em si não gerencia a rede, ele fornece uma ferramenta para que o administrador possa administrar a rede.

A figura 9 demonstra o fluxo de informações entre os agentes gerenciados e o gerenciador.

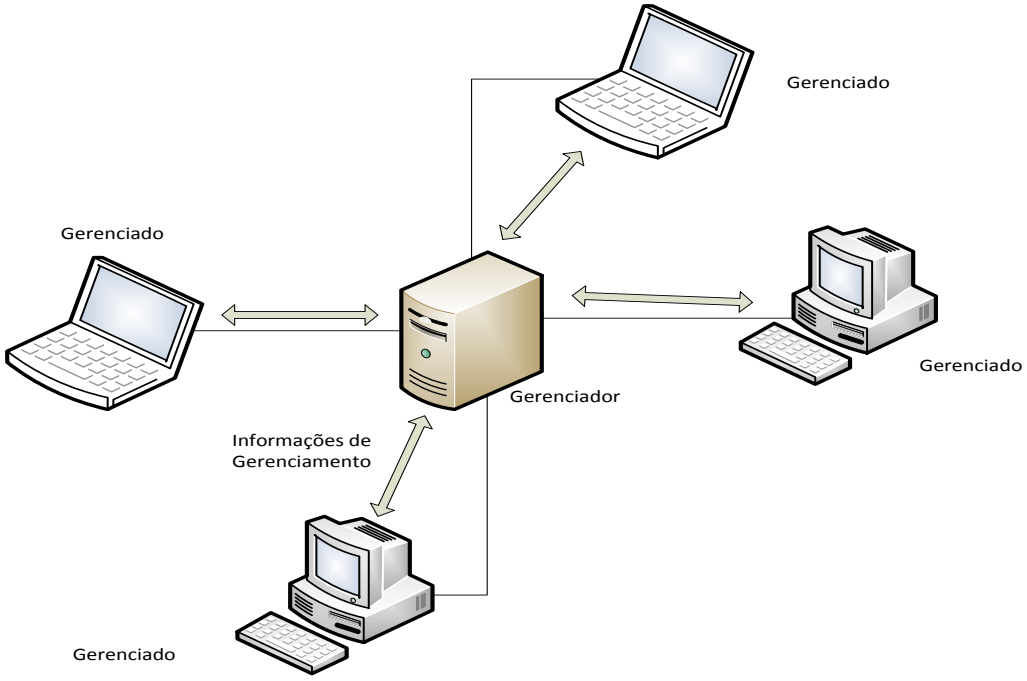


Figura 9 - Entidades de Gerenciamento (KUROSE, 2010).

3.4. Protocolo SNMP

O protocolo SNMP é o padrão de gerência de redes para o sistema TCP/IP, está definido nos documentos RFC-1155, RFC-1156 e RFC-1157. Descreve um conjunto de regras que definem informações de gerência e um conjunto oficial de informações, se encontra na camada de aplicação e permite que o administrador colete informações e faça diagnósticos dos nós por toda a extensão da rede (COSTA, 2008).

No SNMP existem os gerenciadores e agentes:

- ✓ O gerenciador costuma ser chamado de NMS *(Network Management System),* que é responsável por receber *traps*, que é um método utilizado pelo agente para informar à NMS que algo não planejado aconteceu nos agentes, elas são enviadas de modo assíncrono e não em respostas. A NMS também é responsável por executar ações baseadas em informações que foram enviadas pelos agentes (SCHMIDT, 2001).

- ✓ O agente é um *software* residente em um nó da rede, pode ser um *software* incorporado pelo sistema operacional ou um sistema operacional de baixo nível (*software* que controla um *nobreak*). Esse *software* faz o rastreamento das informações referentes ao estado e as alterações do *host* e envia ao gerente que reage às informações de forma adequada (SCHMIDT, 2001).

4. ZABBIX - A FERRAMENTA DE MONITORAMENTO

Zabbix é uma ferramenta *Open Source*[7] que monitora os mais diversos parâmetros de rede de computadores assim como a saúde e integridade dos servidores, ele utiliza mecanismos que permite que seja enviado alerta por sms, celular e *e-mail* com base em qualquer evento. Oferece ótima visualização de relatórios e gráficos gerados por dados armazenados em banco de dados, tornado a ferramenta ideal para o planejamento de capacidade (ZABBIX SIA, 2010).

A ferramenta suporta monitoramento ativo e passivo, além de *trapping* (notificação por alarmes), todas as informações são acessadas pelo *frontend* que é uma *interface web* que permite ser configurada conforme a necessidade do administrador. Os gráficos gerados pela ferramenta têm suas informações atualizadas em tempo real, possui modo *slide show* onde é possível agrupar as informações mais relevantes assim como o tempo que a mesma será mostrada, permitindo que as informações se alternem sem a intervenção do administrador (ZABBIX SIA, 2010).

Quando configurado de forma correta permite que um ativo seja monitorado pela entidade gerenciadora esteja ele em qualquer ponto, seja local ou remoto, tornando mais fácil o monitoramento da rede, da mesma forma para redes de grandes organizações ou pequenas redes particulares. É um *software* distribuído nos termos da licença GPL Versão 2[8] (*General Public License* 2), não possui versão paga e as mesmas atualizações recebidas pelas grandes corporações também estão acessíveis para as pequenas empresas familiares (ZABBIX SIA, 2010).

4.1. Componentes da Aplicação

O Zabbix é uma ferramenta composta basicamente por cinco componentes que juntos proporciona ao administrador uma ferramenta robusta e que oferece recursos para monitorar equipamentos mesmo estando localizados em outra unidade da organização.

[7] Código Aberto que permite o acesso do usuário ao código fonte do software.
[8] Licença baseada em quatro liberdades: Executar, Estudar o funcionamento, Redistribuir e Aperfeiçoar.

4.1.1. Servidor

Conforme ZABBIX SIA (2012), o servidor é a unidade centralizadora onde os agentes enviar as informações dos *hosts* que estão sendo monitorados e essas são tratadas e retornadas em forma que o administrador possa entendê-las. Também é no servidor que toda a informação tanto de configuração como de estatística é armazenada.

4.1.2. Proxy

Conforme ZABBIX SIA (2012), esta aplicação realiza a coleta de dados sobre desempenho e disponibilidade para o servidor, todos os dados coletados localmente são transferidos para o servidor. Com essa característica se torna altamente recomendado para ambientes que não tenha administradores de rede.

4.1.3. Agente

Aplicação localizada no equipamento monitorado responsável pela coleta de informações do dispositivo e realizar o repasse dessa informação ao servidor.

4.1.4. Banco de Dados

Todas as informações são armazenadas em banco de dados, de forma que tanto o servidor quanto a interface *web* possam interagir. Por exemplo, ao criar um item na interface *web*, os dados são armazenados em banco de dados e o servidor busca uma vez por minuto essas informações de forma que pode demorar até dois minutos para que uma informação possa estar visível na interface (ZABBIX SIA, 2012).

4.1.5. Frontend

Nada mais é que uma interface *web* que facilita a entrada de dados e a visualização de informações dos itens monitorados (ZABBIX SIA, 2012).

4.2. Requerimentos para a instalação

Como a tabela 1 demonstra, é possível a instalação em uma máquina com *hardware* de baixo desempenho, em uma máquina Pentium II já é possível monitorar 20 hosts (ZABBIX SIA, 2010).

Tabela 1 - Requisitos de *Hardware* (SIA, 2010).

Nome	Plataforma	CPU/Memoria	Banco de Dados	Máquinas Monitoradas
Fraco	*Ubuntu Linux*	PII 350MHz 256MB	SQLite	20
Médio	*Ubuntu Linux 64 bit*	AMD Athlon 3200+ 2GB	MySQL InnoDB	500
Potente	*Ubuntu Linux 64 bit*	Intel Dual Core 6400 4GB	RAID10 MySQL InnoDB ou PostgreSQL	>1000
Muito potente	*RedHat Enterprise*	Intel Xeon 2xCPU 8GB	Fast RAID10 MySQL InnoDB ou PostgreSQL	>10000

A tabela 2 mostra os vários bancos de dados que podem ser utilizados para o armazenamento de informações tanto da ferramenta como do próprio monitoramento.

Tabela 2 - Requisitos de Banco de Dados (SIA, 2010).

Software	Versão
MySQL	5.0 *or later*
Oracle	10g *or later*
PostgreSQL	8.1 *or later*
SQLite	3.3.5 *or later*
IBM DB2	9.7 *or later*

A tabela 3 mostra os requisitos necessários para a instalação do *frontend* da ferramenta que facilita a interação com usuário.

Tabela 3 - Requisitos para Frontend (SIA, 2010).

Software	Versão
Apache	1.3.12 *or later*
PHP	5.1.6 *or later*

4.3. Telas

Logo abaixo serão apresentados os principais recursos que o administrador necessita para o monitoramento básico de uma rede.

A ferramenta permite configurar *hosts*, criar itens que serão monitorados, configurar *triggers* para que sejam disparados conforme os acontecimentos, gerar gráficos a partir de itens configurados e até criar um *slide show* com os gráficos, mapas e outras informações que o administrador julgar necessário.

4.4. Dashboard

Ao abrir o Zabbix é apresentada a tela inicial (*Dashboard*), onde é possível configurar itens que o administrador julgar mais importantes.

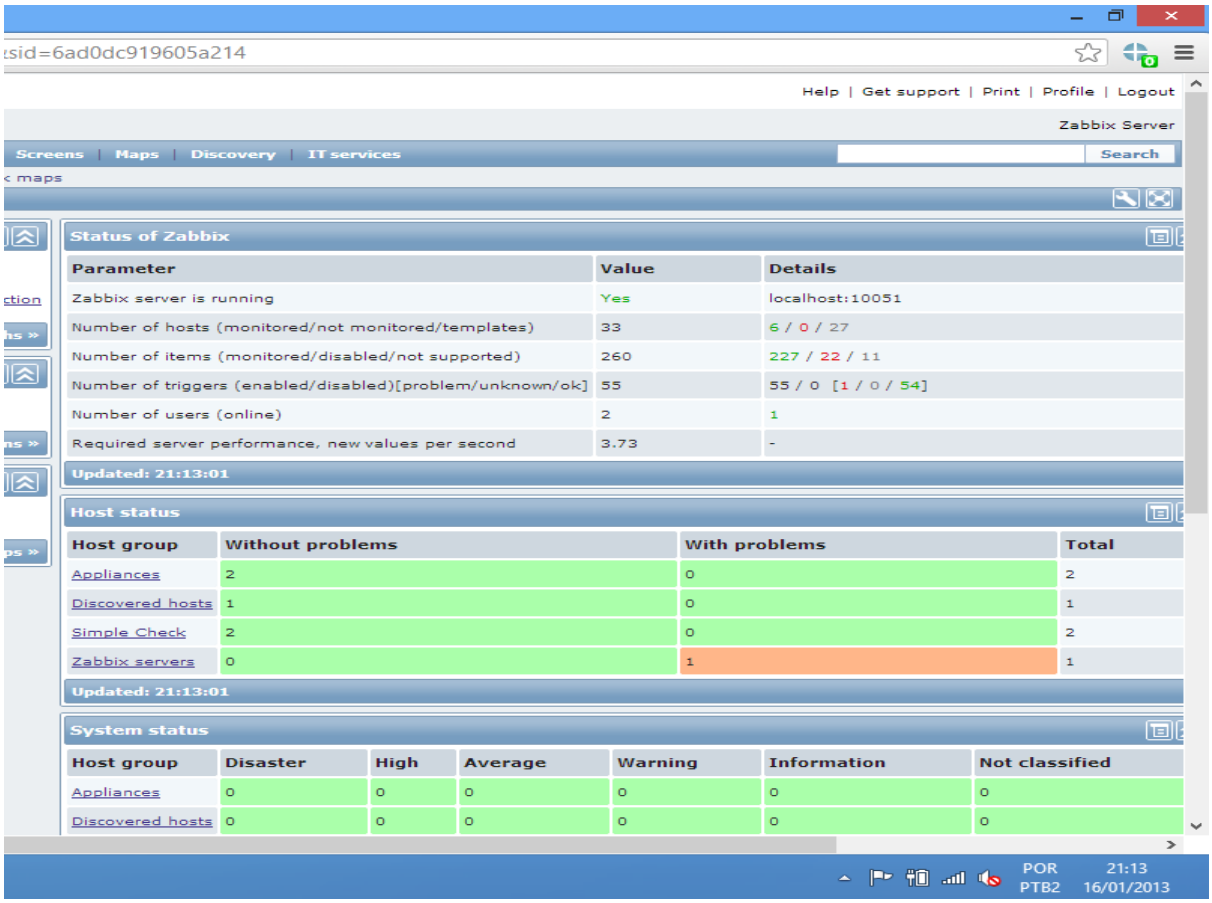


Figura 10- *Dashboard* (SIA, 2010).

4.5. Hosts

Antes de monitorar uma máquina é necessário cadastrá-la para que seja possível criar itens de monitoramento, para máquinas é necessário instalar o agente e depois criar o *host*. Para equipamentos que não permitem a instalação do agente, é possível realizar o monitoramento de checagem simples através do protocolo ICMP[9].

Também é possível criar outros tipos de *hosts* que não sejam máquinas, como *sites* ou até monitorar o *status* de um *e-mail*.

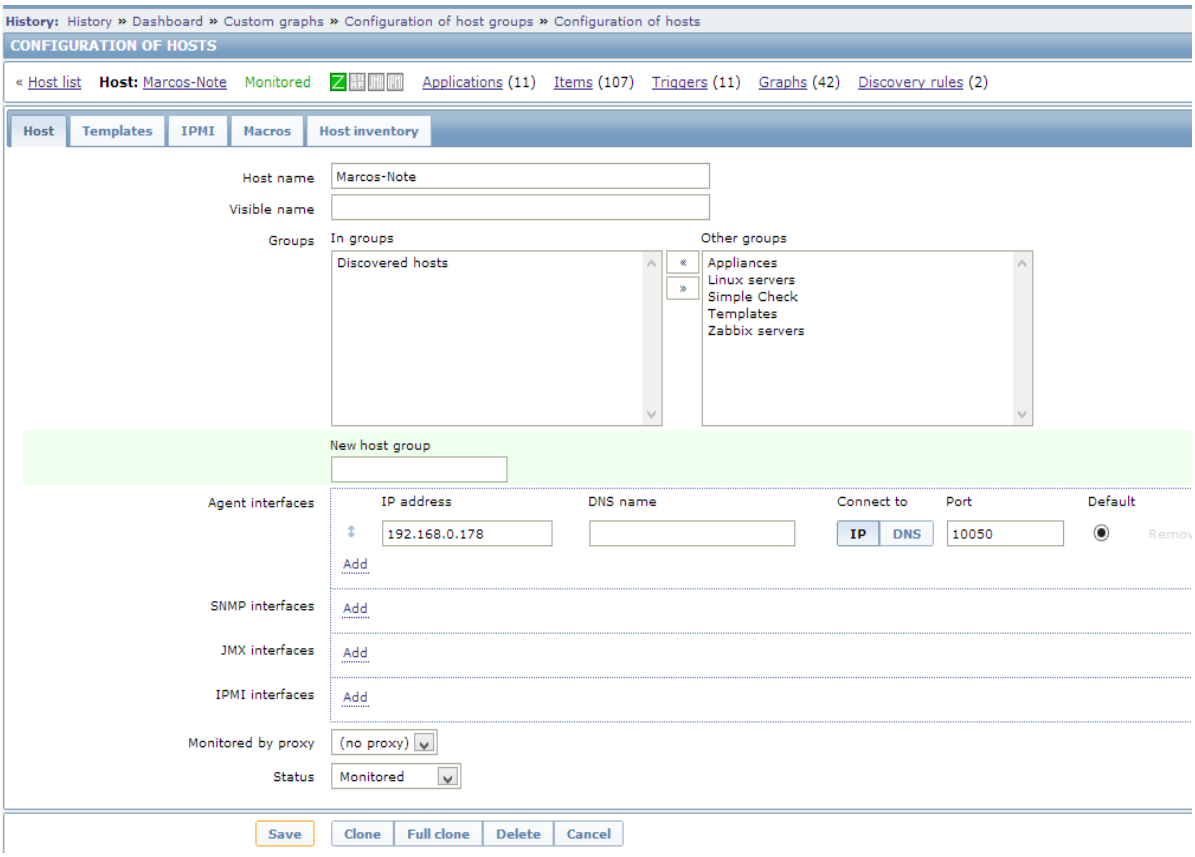


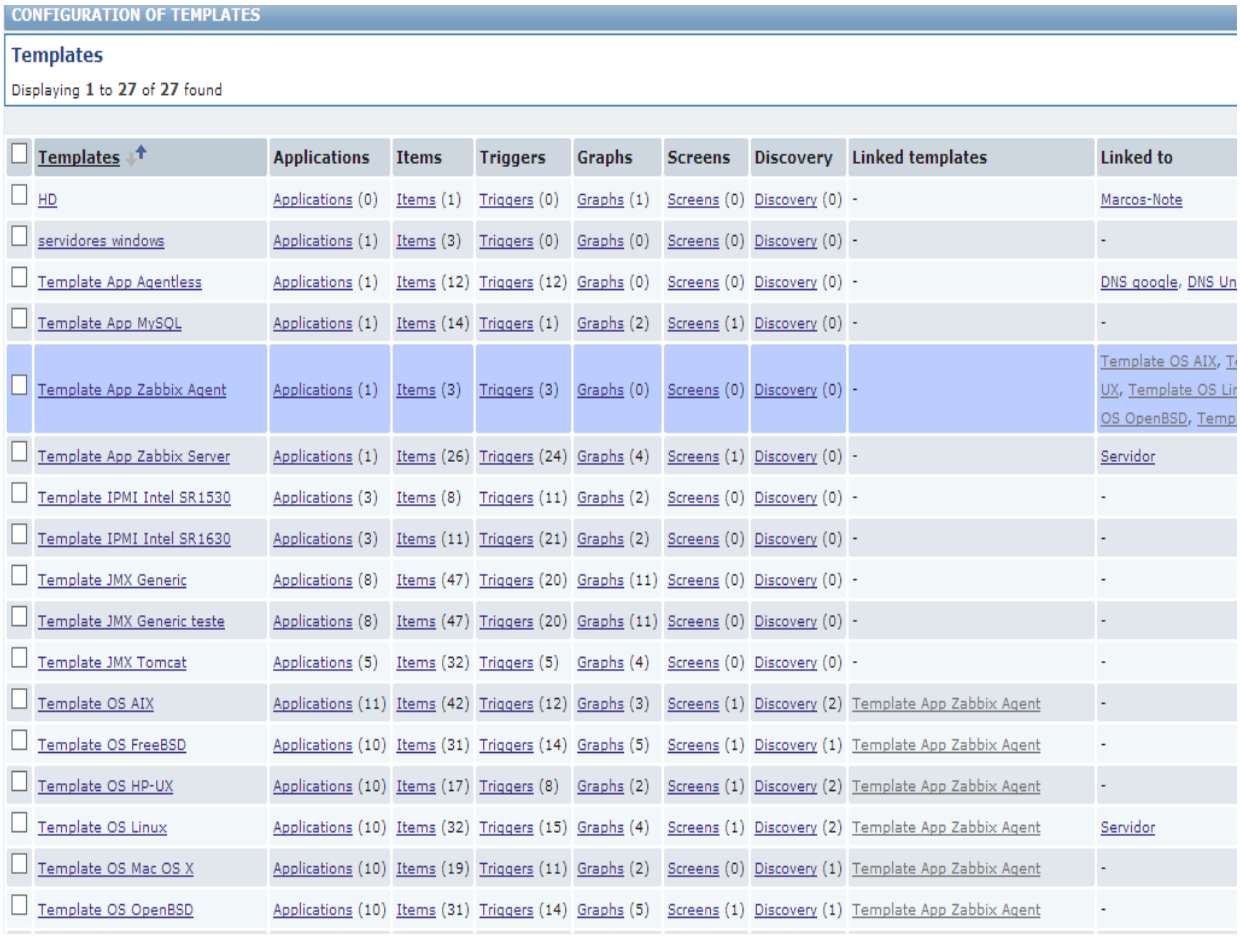
Figura 11 – *Hosts* (SIA, 2010).

4.6. Templates

[9] Protocolo que faz parte do protocolo IP

Um conjunto de entidades (gatilhos, itens, gráficos), prontas para serem aplicadas em um ou vários *hosts*. Seu trabalho é agilizar a implantação do monitoramento ou tornar mais fácil a atividade de monitoramento em massa (ZABBIX SIA, 2012).

Ao instalar a ferramenta já é possível utilizar os diversos *templates* existentes para iniciar o monitoramento,



CONFIGURATION OF TEMPLATES

Templates

Displaying 1 to 27 of 27 found

Templates	Applications	Items	Triggers	Graphs	Screens	Discovery	Linked templates	Linked to
HD	Applications (0)	Items (1)	Triggers (0)	Graphs (1)	Screens (0)	Discovery (0)	-	Marcos-Note
servidores windows	Applications (1)	Items (3)	Triggers (0)	Graphs (0)	Screens (0)	Discovery (0)	-	-
Template App Agentless	Applications (1)	Items (12)	Triggers (12)	Graphs (0)	Screens (0)	Discovery (0)	-	DNS google, DNS Un
Template App MySQL	Applications (1)	Items (14)	Triggers (1)	Graphs (2)	Screens (1)	Discovery (0)	-	-
Template App Zabbix Agent	Applications (1)	Items (3)	Triggers (3)	Graphs (0)	Screens (0)	Discovery (0)	-	Template OS AIX, T UX, Template OS Lir OS OpenBSD, Temp
Template App Zabbix Server	Applications (1)	Items (26)	Triggers (24)	Graphs (4)	Screens (1)	Discovery (0)	-	Servidor
Template IPMI Intel SR1530	Applications (3)	Items (8)	Triggers (11)	Graphs (2)	Screens (0)	Discovery (0)	-	-
Template IPMI Intel SR1630	Applications (3)	Items (11)	Triggers (21)	Graphs (2)	Screens (0)	Discovery (0)	-	-
Template JMX Generic	Applications (8)	Items (47)	Triggers (20)	Graphs (11)	Screens (0)	Discovery (0)	-	-
Template JMX Generic teste	Applications (8)	Items (47)	Triggers (20)	Graphs (11)	Screens (0)	Discovery (0)	-	-
Template JMX Tomcat	Applications (5)	Items (32)	Triggers (5)	Graphs (4)	Screens (0)	Discovery (0)	-	-
Template OS AIX	Applications (11)	Items (42)	Triggers (12)	Graphs (3)	Screens (1)	Discovery (2)	Template App Zabbix Agent	-
Template OS FreeBSD	Applications (10)	Items (31)	Triggers (14)	Graphs (5)	Screens (1)	Discovery (1)	Template App Zabbix Agent	-
Template OS HP-UX	Applications (10)	Items (17)	Triggers (8)	Graphs (2)	Screens (1)	Discovery (2)	Template App Zabbix Agent	-
Template OS Linux	Applications (10)	Items (32)	Triggers (15)	Graphs (4)	Screens (1)	Discovery (2)	Template App Zabbix Agent	Servidor
Template OS Mac OS X	Applications (10)	Items (19)	Triggers (11)	Graphs (2)	Screens (0)	Discovery (1)	Template App Zabbix Agent	-
Template OS OpenBSD	Applications (10)	Items (31)	Triggers (14)	Graphs (5)	Screens (1)	Discovery (1)	Template App Zabbix Agent	-

Figura 12 - *Template* (SIA, 2010).

4.7. Itens

É possível monitorar diversos itens em um *host:* placas de rede de servidores, quantidade de usuários conectados, uso de disco, memória disponível, entre outros. Para isso basta que seja configurado os itens pertencentes ao *host* desejado, com isso esses itens serão monitorados simultaneamente.

A configuração de um item é realizada escolhendo uma chave, o valor retornado pode ser do tipo numérico, *string*, ponto flutuante, *caracter*, *log* ou texto.

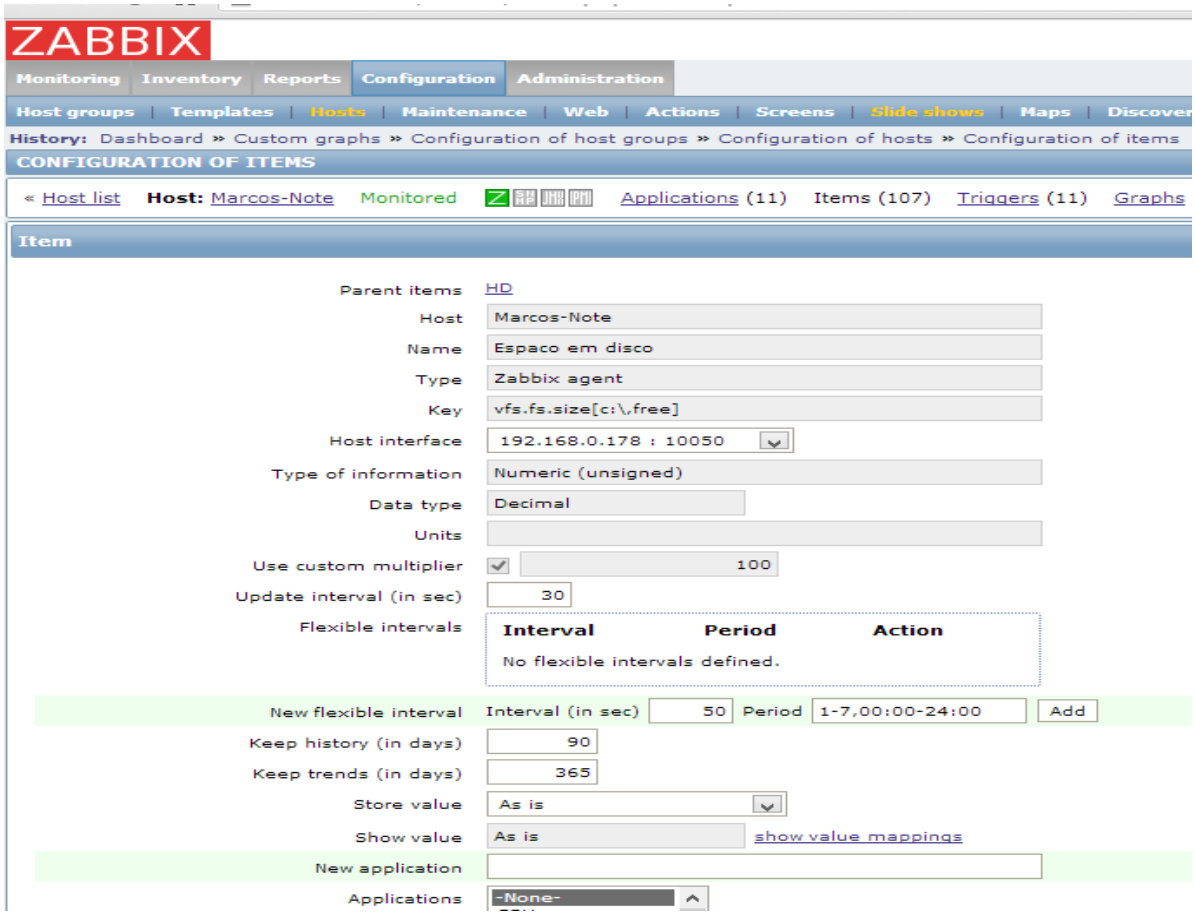


Figura 13 – Itens de configuração (SIA, 2010).

4.8. Triggers (Gatilhos)

Caso um agente leia uma informação que não é a esperada, o Zabbix permite disparar um evento que pode ser uma ação no próprio *host*, até mesmo um SMS para um celular. Esse item é muito importante em um sistema onde é necessária uma resposta rápida a um acontecimento inesperado.

Um *switch* apresenta portas com mau funcionamento, é possível que seja disparado um aviso para que o administrador possa trocar o equipamento ou trocar a porta caso tenha outras disponíveis.

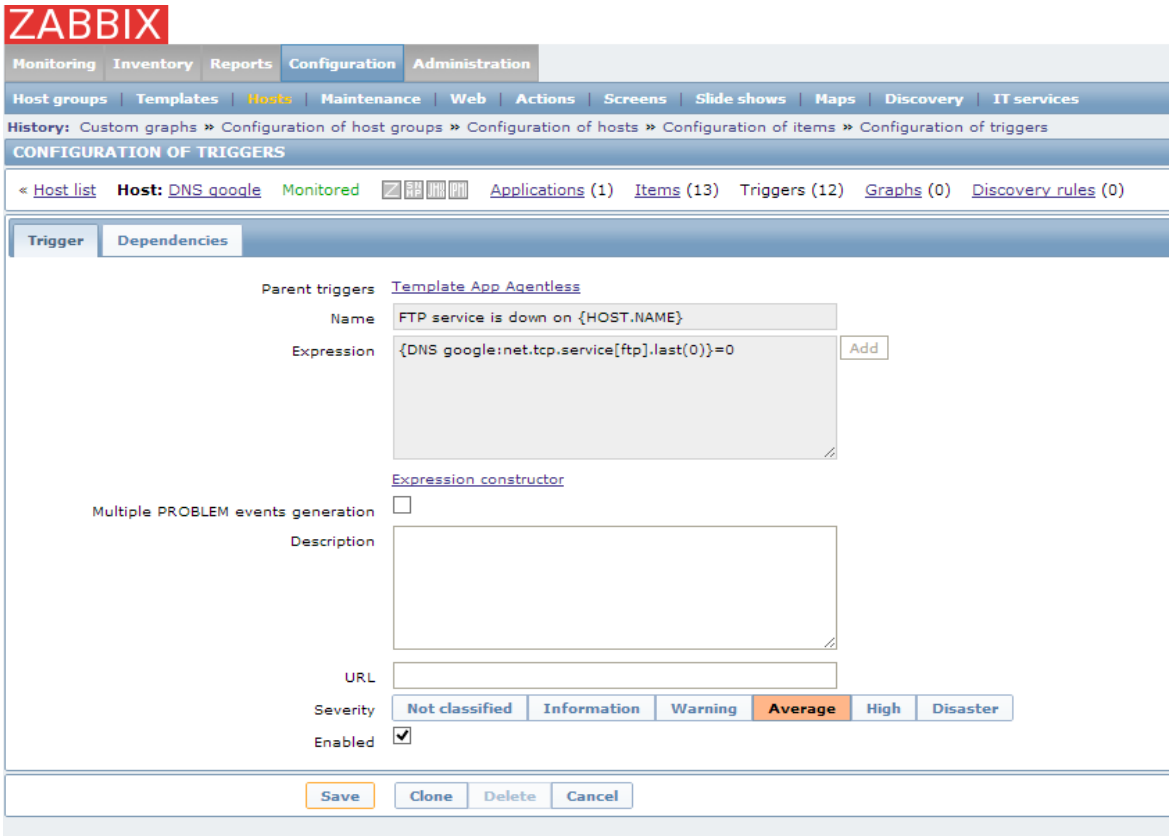


Figura 14 - *Triggers* (SIA, 2010).

4.9. Gráficos

Uma das partes mais importantes da ferramenta é o gráfico, pois torna a visualização mais fácil de ser interpretada e consequentemente a resposta ao acontecimento mais rápida, permitindo que a rede tenha sempre um bom desempenho.

Os gráficos podem ser configurados como pizza, barra, linha, com diversas cores de forma a facilitar a sua visualização. A figura 15 mostra um exemplo de gráfico.

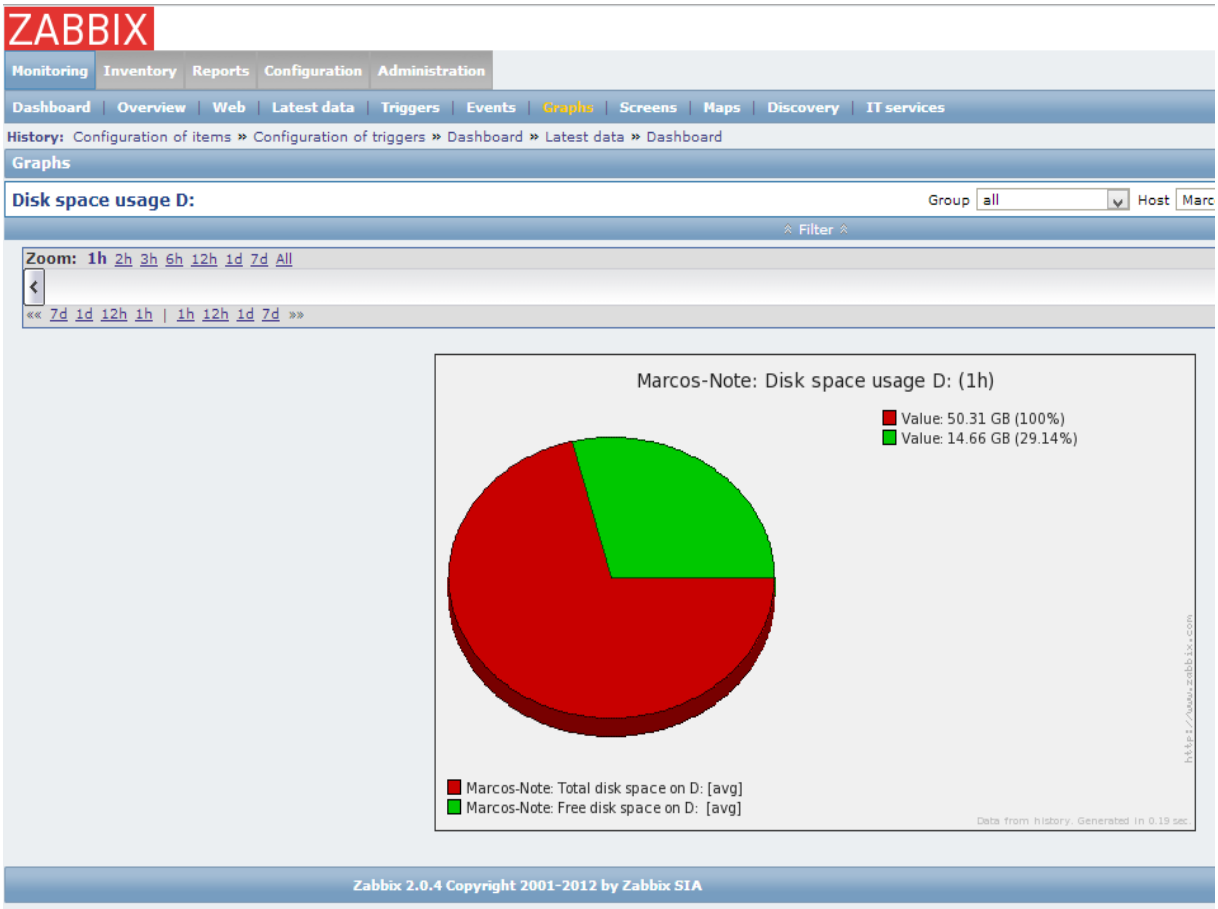


Figura 15 - Gráficos (SIA, 2010).

5. ESTUDO DE CASO

Neste trabalho foi implementada uma ferramenta para que uma pequena rede seja monitorada, com isso iremos demonstrar como uma ferramenta de NMS pode dar informações que auxiliam o monitoramento do ambiente demonstrado na figura 16.

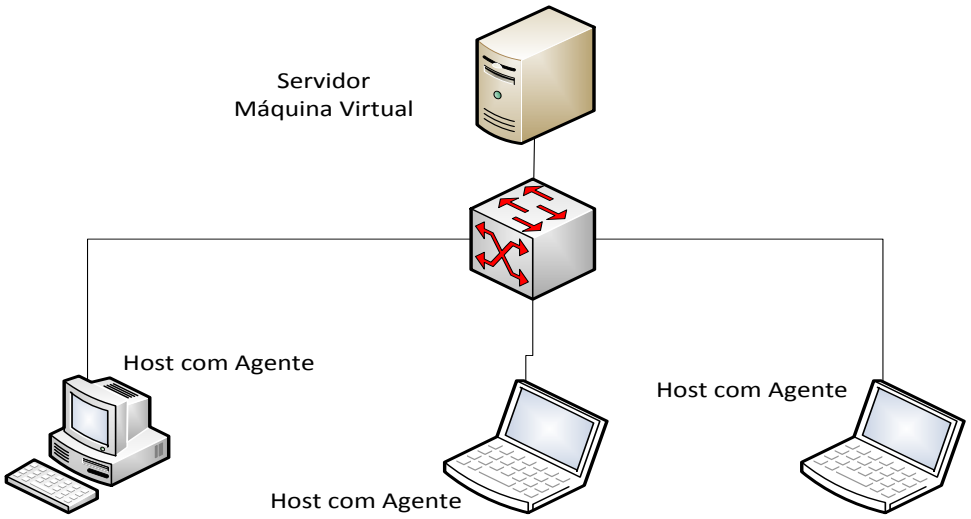


Figura 16 - Mapa da Rede Local (BEHROUZ, 2008).

A tabela 4 mostra a configuração dos equipamentos utilizados neste estudo de caso.

Tabela 4 - Máquinas utilizadas (AUTORIA PRÓPRIA, 2013).

Equipamento	**Servidor**	**Notebook Agente**	**Notebook Agente**	**Desktop Agente**
Marca/Modelo	Virtual Box	Dell Inspiron	STI	Positivo
Processador	Core 2 Duo	Core 2 Duo	Dual Core	Dual Core
HD	20 GB	250 GB	250 GB	160
Memória RAM	1 GB	4 GB	2 GB	2 GB
WI-FI	54 Mbps	54 Mbps	54 Mbps	
Placa de rede	10/100	10/100	10/100	10/100
Sistema Operacional	CentOS	Window 8	Windows 7	Windows 7

Serão apresentadas algumas telas que foram utilizadas no monitoramento da rede e que demonstraram ser muito uteis para o administrador, oferecendo informações em tempo real e de fácil entendimento.

5.1. Monitoramento de *Host*

Antes do sistema de monitoramento, uma das formas para que o administrador saiba se uma máquina da rede ou um servidor está ligado, é executar o comando *ping*[10] a partir de uma máquina ou servidor, mediante a resposta o administrador saberá se o *host* está ou não ligado, desta forma ele teria que repetir esse procedimento de máquina em máquina até que fosse feito para todas as máquinas, além de ter que saber o nome ou IP de todas elas, ou então ir até a máquina e verificar pessoalmente a situação que se encontrava.

Como mostra a figura17 com a ferramenta implementada, foi possível saber o estado do equipamento logo na *dashboard*, assim como a quantidade de máquinas da rede que estão *online*. Qualquer equipamento que tenha uma placa de rede (*smartphone*, computador, roteador, catraca, etc.), é possível que seja monitorado o seu estado de forma a facilitar a visualização.

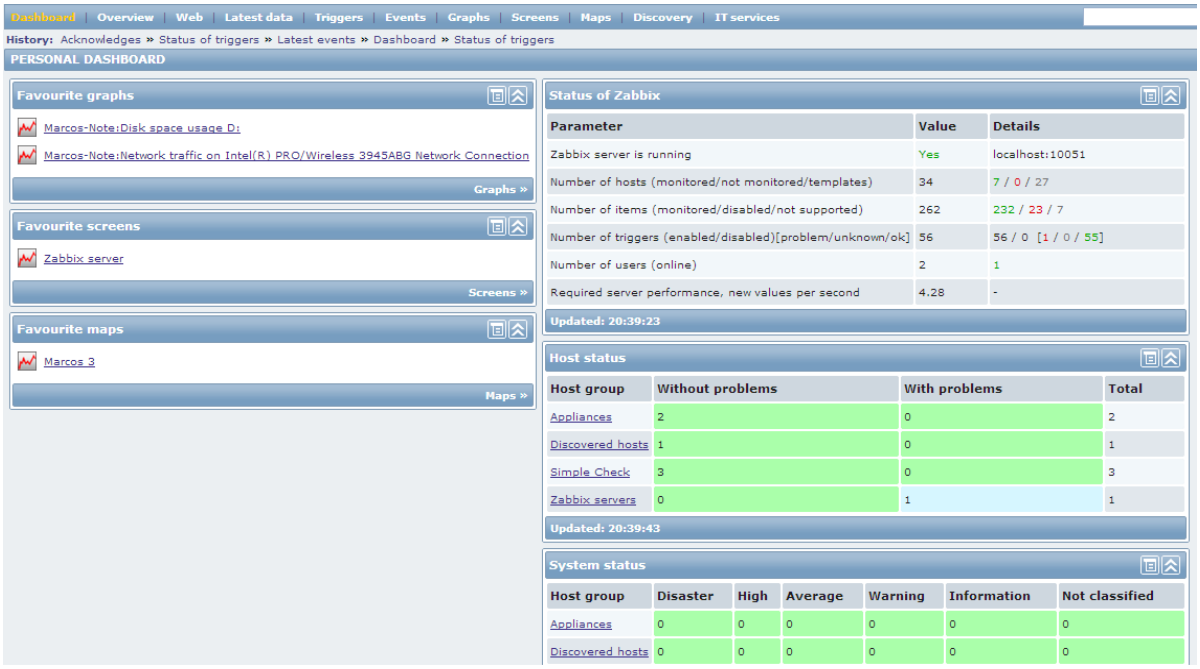


Figura 17 - Informações na tela inicial (SIA, 2010).

[10] Comando para utilizado para testar a conectividade entre equipamentos

5.2. Monitoramento de espaço em disco

Não havia monitoramento do espaço em disco, o administrador só tinha conhecimento de que não havia espaço livre quando a máquina apresentava a falha por falta de espaço.

Após a implantação do sistema tornou-se possível a visualização através de gráficos, permitindo visualizar com maior detalhe e melhor entendimento da situação.

A figura18 mostra o monitoramento de disco que é muito importante em servidores de arquivo, *e-mail*, imagens e qualquer outro dispositivo para armazenamento em massa de arquivos, pois permite que o administrador possa ter a dimensão exata da quantidade de espaço disponível, para que tome a decisão de adicionar novos discos para que o sistema não pare.

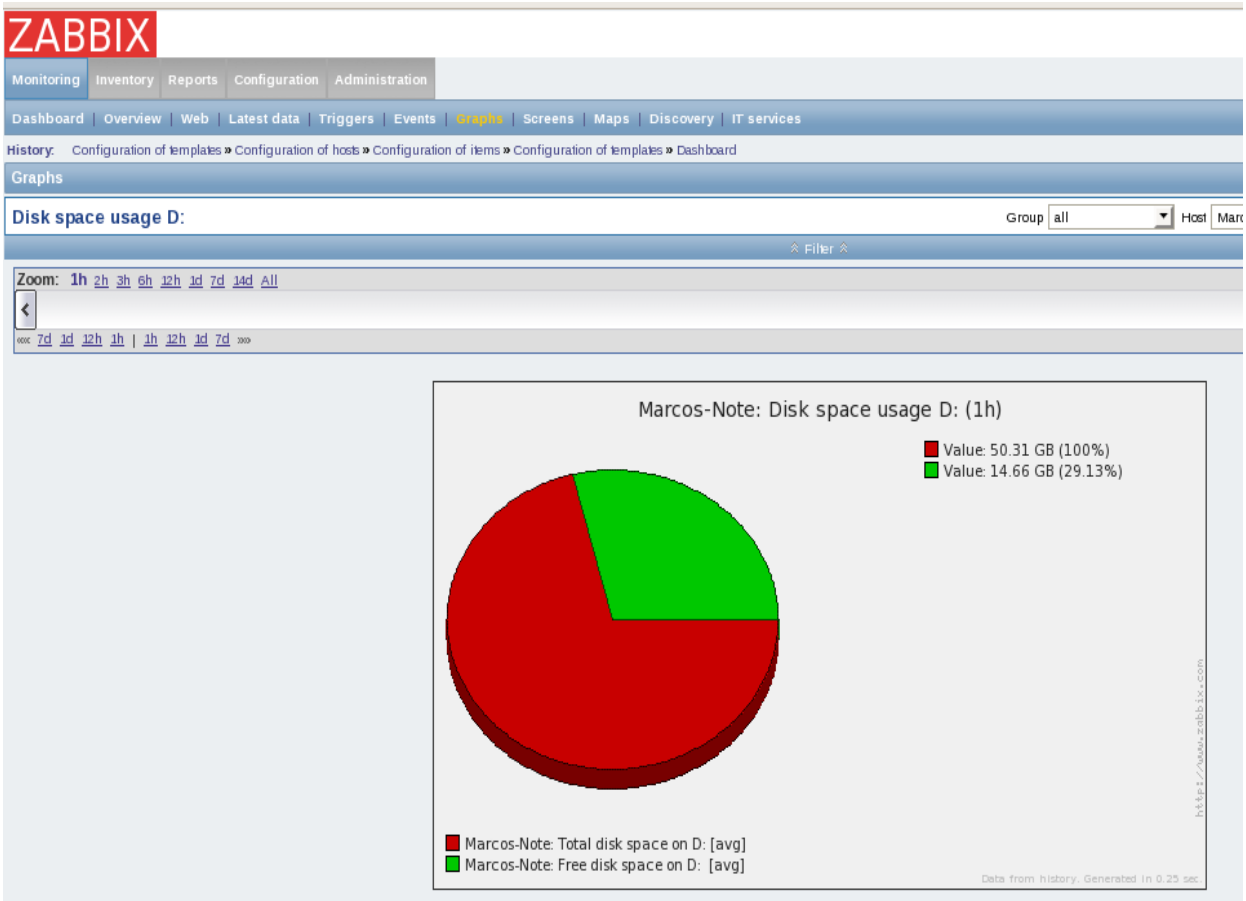


Figura 18 - Gráfico de espaço em disco (SIA, 2010).

5.3. Monitoramento de Interface de rede

Não havia monitoramento das interfaces de rede, só era possível saber que o *link* havia caído quando a Internet ou compartilhamentos estavam fora, então era feito a checagem para ver onde estava o problema.

Como não havia estatísticas, não era impossível saber qual o período de maior tráfego ou quando o consumo de banda era menor, de forma a direcionar as tarefas para determinados períodos do dia.

Com a implantação da ferramenta o monitoramento da interface permite ver em tempo real o tráfego, com isso o administrador tem a possibilidade de verificar se a banda está sendo fornecida conforme o contrato do fornecedor, ou até mesmo qual usuário consome mais banda e os motivos desse consumo.

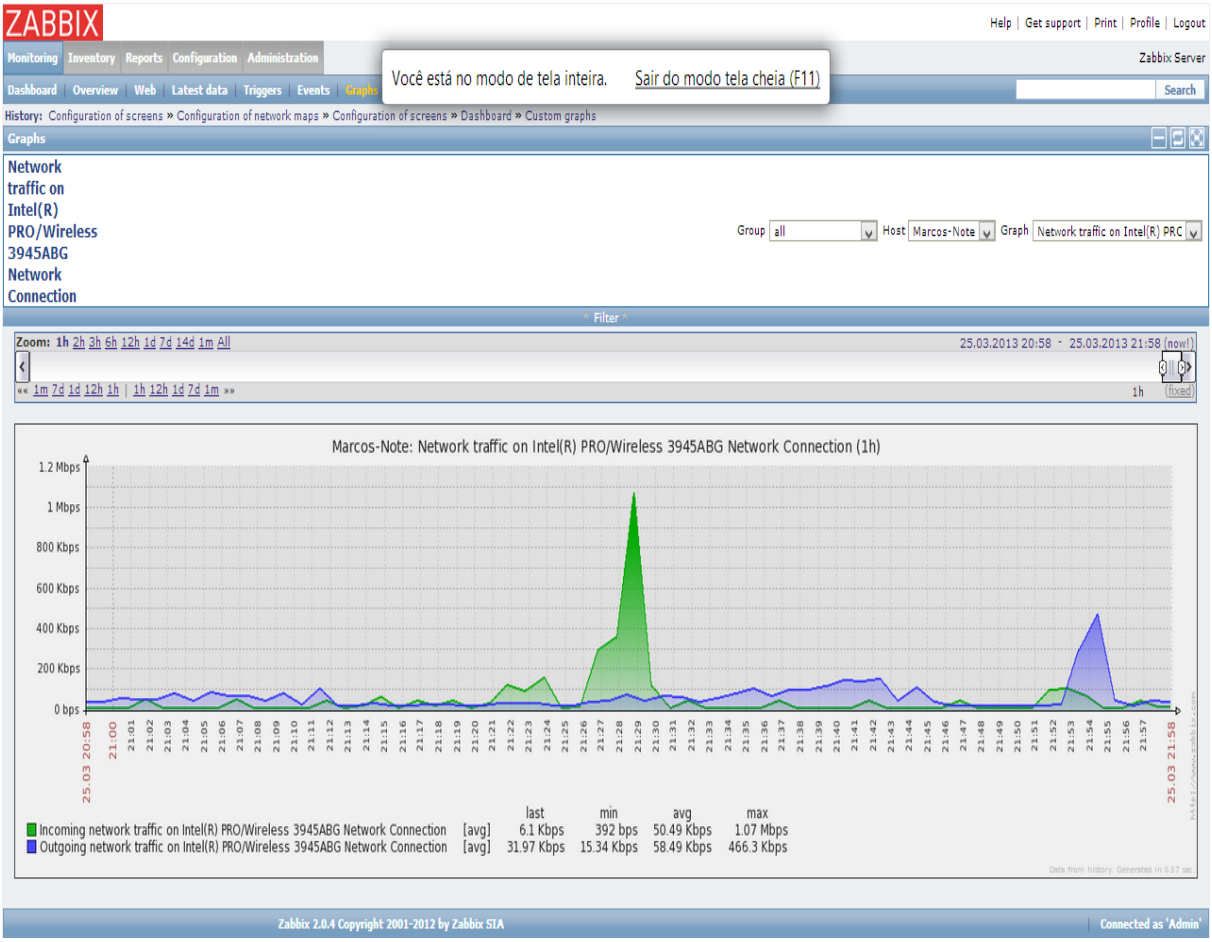


Figura 19 - Tráfego na interface de rede (SIA, 2010).

5.4. Monitoramento da CPU

Monitoramento da CPU consiste em dizer como está o processamento da máquina, ou seja, se está trabalhando com toda sua capacidade ou não. Capacidade de processamento de uma máquina impacta diretamente no custo, e com essas estatísticas em mãos o administrador pode direcionar os melhores equipamentos para quem realmente necessita e com isso pode investir melhor em outros pontos que possam melhorar a rede com um todo.

No ambiente em questão, não havia nenhum tipo de monitoramento de CPU, só era sabido que a máquina estava sobrecarregada quando apresentava travamentos ou até mesmo reiniciava. Enquanto outra máquina era utilizada de forma que o seu processamento não era totalmente aproveitado.

Após o monitoramento foi possível ver em quais momentos e aplicações o processador é mais exigido. Assim podemos direcionar as aplicações mais pesadas para as máquinas com maior poder de processamento, com isso diminuir e muitas vezes até impedir que a máquina apresente travamentos ou que as aplicações parem de responder durante algum tipo de trabalho. Com essa estatística é possível saber qual a máquina esta precisando ser substituída, por uma de maior capacidade.

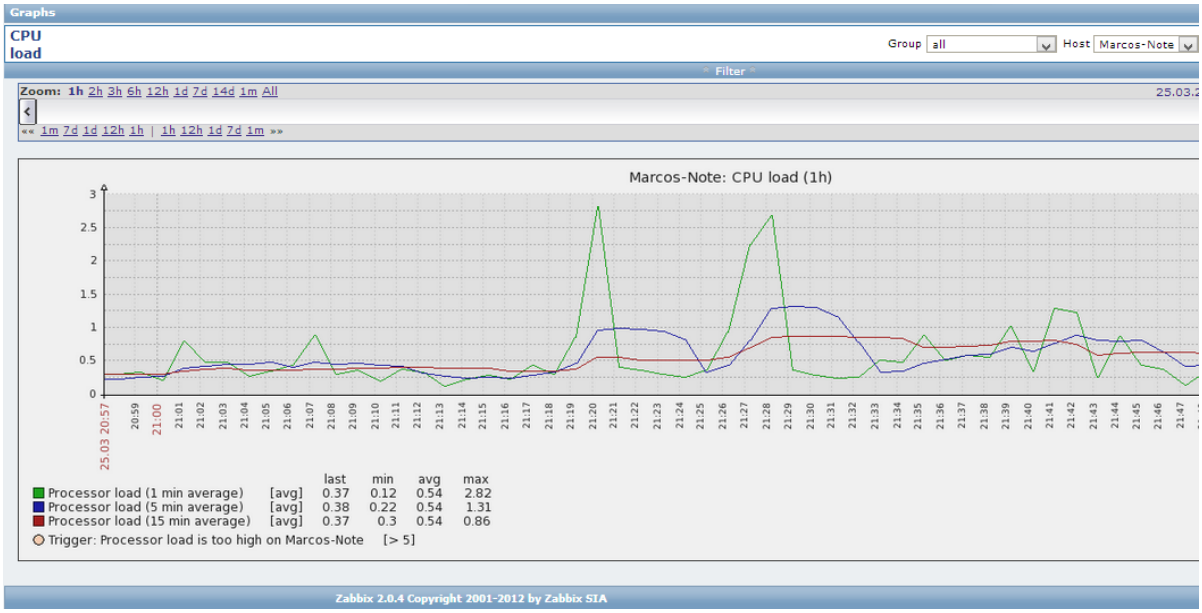


Figura 20 - Monitoramento de CPU (SIA, 2010).

5.5. Monitoramento de Memória

Não havia monitoramento de memória, com isso não era possível saber se o desempenho da máquina era afetado pela falta da mesma, podendo ocorrer travamentos, lentidão e sem uma causa definida.

Após a utilização deste monitoramento, tornou-se possível saber se a memória do equipamento estava atendendo de forma adequanda a ou se havia a necessidade de adição de novos pentes.

Essa informação é muito importante para que não se tenha gastos desnecessários ou até mesmo que sejam feitos nas máquinas com maiores necessidades, fazendo com que a vida do equipamento seja prolongada.

A figura 21 demonstra a quantidade de memória utilizada e disponível, com a somatória se obtem o total de memória disponível no equipamento.

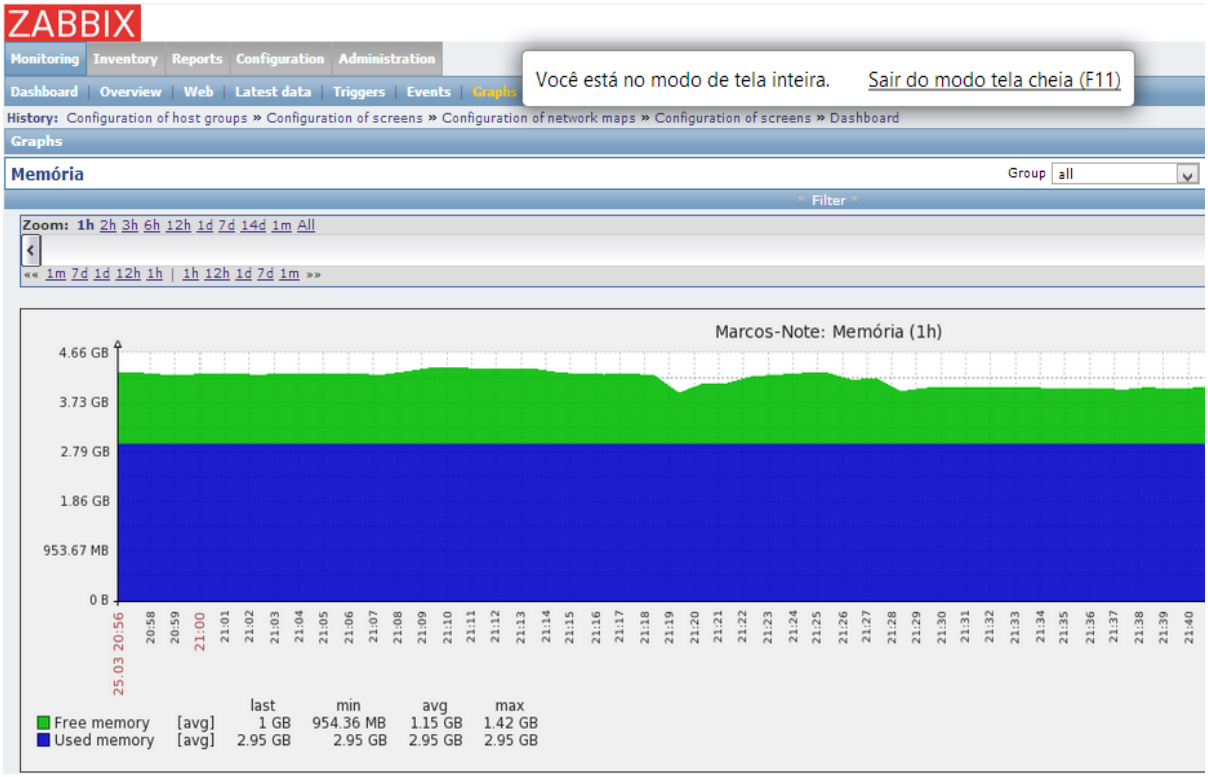


Figura 21 - Gráfico de memória disponível (SIA, 2010).

5.6. Screen (Tela)

Podemos utilizar o recurso de tela para monitorar vários itens simultaneamente, onde é possível configurar itens como: Mapas, gráficos, texto plano, entre outros.

Este recurso tornou possível visualizar graficamente qual *host* está *online* através do *status* que fica logo abaixo da figura que representa o *host*.

A figura abaixo mostra algumas informações referentes ao servidor como: O relógio com a hora do sistema do servidor, um mapa com algumas máquinas da rede que podem ser escolhidas conforme necessidade (servidor *web*, servidor de arquivos, etc), a performance da máquina algumas informações relevantes.

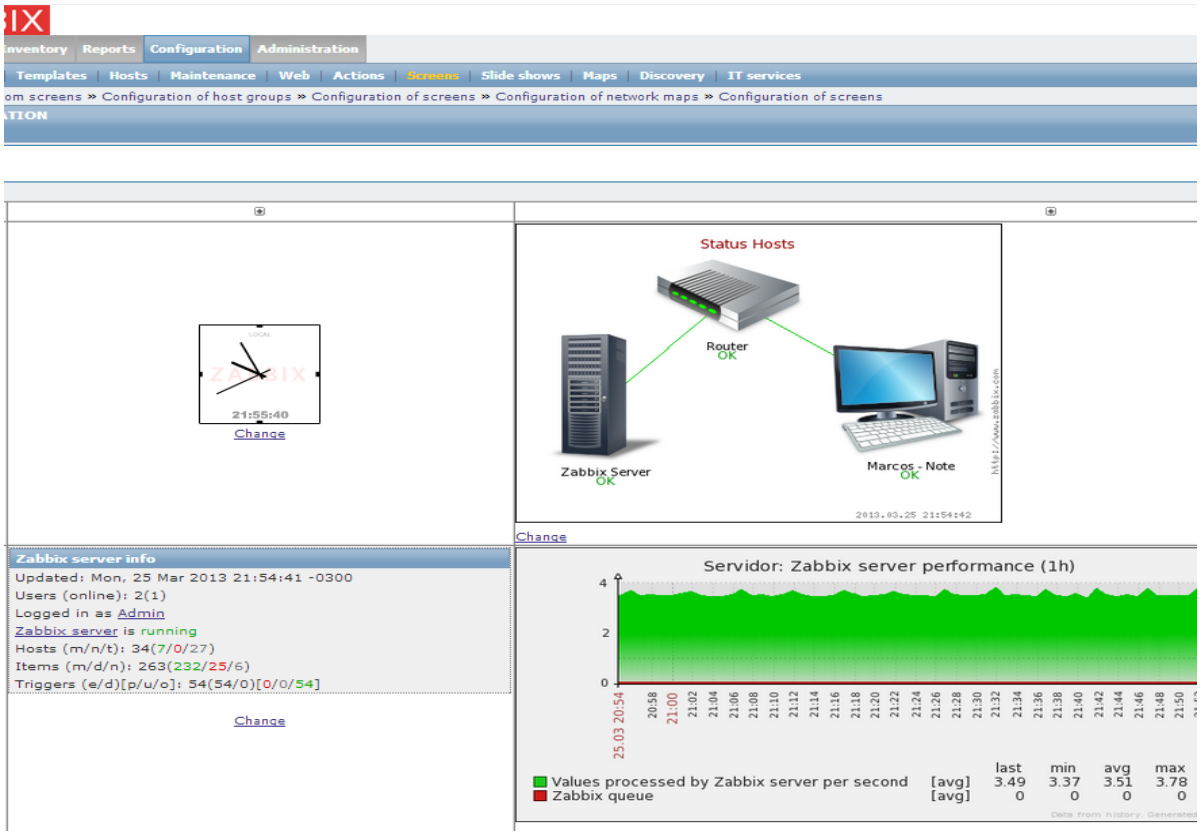


Figura 22 - Tela configurada conforme necessidade (SIA, 2010).

6. CONCLUSÃO

Quando não havia monitoramento na rede, era impossível saber em qual momento do dia o tráfego na rede era maior, ou se o *link* de internet fornecido era mesmo o contratado, ou até mesmo se alguma máquina estava sendo subaproveitada.

Dessa forma o administrador não tem condições de realizar investimento de forma correta, ou seja, comprar uma máquina nova ou melhorar o *link* de internet, pois sem as informações corretas ele não tem como saber se o gargalo é a máquina, a interface de rede ou até mesmo o *link* que não atende mais as necessidades. Isso causa transtorno aos usuários que não tem um bom serviço prestado, aos analistas de suporte que tem uma demanda excessiva de trabalho, mais gastos com pessoal para atender aos usuários, além de gerar altos custos, deixa tanto os colaboradores quanto os gestores da empresa descontentes.

Após o monitoramento ser implantado foi possível obter diversos tipos de estatísticas sobre qualquer equipamento existente da rede, a quantidade de dados que está trafegando, quais os usuários que mais utilizam a banda, quais e quantos usuários estão autenticados. Isso tornou possível ver quais máquinas estavam com carga excessiva e precisando de manutenção preventiva, para que fossem removidos arquivos inúteis, aumento de memória na máquina que estava com 2GB, foi possível verificar também que a velocidade da internet estava compatível com a contratada.

O mais importante é que esse resultado pode ser obtido apenas com a implantação de uma ferramenta *Open Source* que permite configurar qualquer equipamento da rede e até verificar o *status* de *sites* na internet, com uma comunidade brasileira que vem crescendo a cada dia, proporcionando a troca de informações em caso de dificuldades. Em uma empresa, essas informações relacionadas à rede permitem que os gastos possam ser direcionados para as áreas que estão com maior carência de investimentos, comprar equipamentos que atendam de forma adequada às necessidades da organização, redução na quantidade de pessoas necessárias para atendimento das ocorrências diárias referente aos equipamentos.

7. REFERÊNCIAS BIBLIOGRÁFICAS

BEHROUZ, A. F. ***Comunicação de Dados e Redes de Computadores,*** (3ª ed.), Bookman, 2008.

BMED, F. ***Tecnologias Negócios e outros assuntos***. Disponível em: Fabio Bmed: http://www.fabiobmed.com.br/tag/topologia-malha/. Acesso em 02 de Abril de 2013.

BRISA, S. B.. ***Gerenciamento de Redes: Uma Abordagem de Sistemas Abertos****,* Makron Books, São Paulo, 1993.

CASE, J. *RFC 1157* - ***Simple Network Management Protocol (SNMP)***. Disponível em: http://www.faqs.org/rfcs/rfc1157.html, acesso em 09 de Janeiro de 2012.

COSTA, F. ***Ambiente de Rede Monitorado com Nagios e Cacti****.*: Ciência Moderna, Rio de Janeiro, 2008.

Duarte, O. C.. ***SNMP.*** Disponível em GTA / UFRJ: http://www.gta.ufrj.br/grad/11_1/snmp/. Acesso em: 13 de Maio de 2013.

HUNT, C. ***TCP/IP Network Administration*** **(2ª ed.),** O'Reilly & Associates, 1993.

KUROSE, K. W. ***Redes de Computadores e a Internet - Uma Abordagem Top-down****,* Pearson Education do Brasil, São Paulo, 2010.

Microsoft. ***Technet.microsoft.com***. Disponível em: http://technet.microsoft.com/pt-br/library/cc786900%28v=WS.10%29.aspx, Acesso em 15 de Abril de 2013.

PINHEIRO, J. M. ***Equipamentos para rede***. Disponível em Projeto de Redes: http://www.projetoderedes.com.br/tutoriais/tutorial_equipamentos_de_redes_01.php#.UZGErkq5ddg. Acesso em 13 de Maio de 2013.

ROSE, M. ***Management Information Base for network management of***. Disponível em http://www.faqs.org/rfcs/rfc1155.html. Acesso em 09 de Janeiro de 2010

Russo, R. ***Escreve Assim***. Disponível em Redes - Sabe o que é um Rack de Rede.: http://escreveassim.com.br/2012/09/25/redes-rack-de-rede/. Acesso em 13 de Maio de 2013.

SAYDAM, T. ***From Networks and Network Management into Service and Service Managemen*** (Volume 4 ed.). Journal of Networks and System Management, 1996.

SCHMIDT, D. R. ***SNMP Essencial****.* Campus 2001.

SIA, Z. ***Zabbix Documentation****.* Disponível em https://www.zabbix.com/documentation/pt/1.8/manual. Acesso em 10 de Janeiro de 2013.

SOARES, L. F. ***Rede de Computadores*** **(2ª ed.)**. Campus. Rio de Janeiro, 1995.

SYSTENS, C. **Programa Cisco Network Academy**. *Conceito Básico de Redes V3.1* 2003.

TANENBAUM, A. S. ***Redes de Computadores*** **(4º ed.)**. Editora Campus, 2003.

TORRES, G. ***Modelo de Referência OSI para Protocoos de Rede***. Disponível em Clube do Hardware: http://www.clubedohardware.com.br/artigos/O-Modelo-de-Referencia-OSI-para-Protocolos-de-Rede/1349/4. Acesso em 15 de Abril de 2013.

ZABBIX, S. ***Zabbix documentation****.* Disponível em https://www.zabbix.com/documentation/2.2/manual/concepts. Acesso em 31 de Janeiro de 2013.