ACADEMIA MILITAR DAS AGULHAS NEGRAS ACADEMIA REAL MILITAR
(1811)

Ciro José de Padua Souza

Aplicação de Sistemas Operacionais e Seus Serviços na Montagem de Infraestrutura Básica de Rede de Computadores para uma Companhia de Comunicações em Operações de GLO

Resende

2018

CIRO JOSÉ DE PADUA SOUZA

Aplicação de Sistemas Operacionais e Seus Serviços na Montagem de Infraestrutura Básica de Rede de Computadores para uma Companhia de Comunicações em Operações de GLO

Trabalho de conclusão de curso apresentado à Academia Militar das Agulhas Negras como parte integrante do Trabalho de Conclusão do Curso de Bacharel em Ciências Militares, sob a orientação do Tenente-Coronel Nivio Paula de Souza.

Resende

2018

CIRO JOSÉ DE PADUA SOUZA

APLICAÇÃO DE SISTEMAS OPERACIONAIS E SEUS SERVIÇOS NA MONTAGEM DE INFRAESTRUTURA BÁSICA DE REDE DE UMA COMPANHIA DE COMUNICAÇÕES EM OPERAÇÕES DE GLO

Trabalho de comclusão de curso apresentado à Academia Militar das Agulhas Negras como parte integrante do Trabalho de Conclusão do Curso de Bacharel em Ciências Militares, sob a orientação do Tenente-Coronel Nivio Paula de Souza.

COMISSÃO AVALIADORA

_____

Nivio Paula de Souza, TC Inf – Orientador

_____

Avaliador

_____

Avaliador

Resende

2018

Em memória do meu querido avô, que foi a pessoa mais entusiasmada com a escolha da minha carreira.

AGRADECIMENTOS

Ao TC Nivio, meu orientador, pela disponibilidade de seu tempo livre para orientação e correção do trabalho e por compartilhar experiências de vida e da carreira militar.

A todos os mestres da minha vida estudantil, que foram as pessoas mais importantes para meu aprendizado e responsáveis por fornecerem todas as ferramentas necessárias para a conclusão do curso da AMAN.

A minha família, pelo incessante apoio e suporte para conclusão deste curso.

Aos companheiros da turma Mestre de Campo Francisco Barreto de Menezes e ao Curso de Comunicações da AMAN, os quais compartilhei os momentos mais intensos e difíceis da minha vida durante a formação acadêmica.

RESUMO

SOUZA, Ciro José de Padua. **Aplicação de Sistemas Operacionais e Seus Serviços na Montagem de Infraestrutura Básica de Rede de Computadores de uma Companhia de Comunicações em Operações de GLO**. Resende: AMAN, 2018. Monografia.

Este trabalho se trata de um estudo sobre o uso de diferentes Sistemas Operacionais para a implementação de uma rede de computadores em uma Operação de Garantia da Lei e da Ordem. Foram estudados os sistemas operacionais *Windows Server 2012 R2* e o *Debian* e os serviços que possibilitam uma infraestrutura básica de uma rede. Alguns parâmetros desses sistemas operacionais como custo de licença, *hardware* necessário para implementação e capacitação de usuários, facilidade de implementação e flexibilidade nas operações serviram como referências para a conclusão. O tipo de pesquisa realizada foi exploratória através de uma revisão bibliográfica. Durante o desenvolvimento da pesquisa são apresentadas as características das Operações de Garantia da Lei e da Ordem que devem ser atendidas pelos sistemas operacionais, bem como os parâmetros dos sistemas operacionais que servem como referência para a escolha e os serviços básicos de uma rede. Este trabalho não serve como manual de instrução para o uso dos sistemas operacionais e serviços aqui apresentados.

Palavras-chave: Operações GLO. Sistemas Operacionais. Linux. Windows. Rede.

ABSTRACT

SOUZA, Ciro José de Padua. **Application of Operating Systems and Their Services in the Assembly of Basic Network Infrastructure of a Signals Company in LOG Operations** Resende: AMAN, 2018. Monograph.

This work is about a study on the use of different Operating Systems for the implementation of network in a Operation of Guarantee of Law and Order. We studied the Windows Server 2012 R2 operating systems and Debian, and the services that enable a basic infrastructure of a network. Some parameters of these operating systems such as license cost, hardware required for implementation and user empowerment, ease of implementation and flexibility in operations served as references for completion. The type of research carried out was exploratory through a bibliographic review. During the development of the research are presented the characteristics of the Law and Order Guarantee Operations that must be fulfilled by the operating systems, as well as the parameters of the operating systems that serve as reference for the choice and the basic services of a network. This work does not serve as an instruction manual for the use of the operating systems and services presented here.

Key words: LOG Operations. Operating Systems. Linux. Windows. Network.

SUMÁRIO

LISTA DE FIGURAS

1. INTRODUÇÃO

Este trabalho foi realizado dentro do escopo de Rede de Computadores e tem como tema central rede de computadores. O tema está delimitado na aplicação de sistemas operacionais e seus serviços na montagem de infraestrutura básica de rede de computadores para uma Companhia de Comunicações em Operações de Garantia da Lei e da Ordem.

A pesquisa tem relevância nos dias atuais tendo em vista os avanços tecnológicos dos meios de informação que presenciamos nos últimos anos ao passo que essas transformações no cotidiano das pessoas causam impactos diretos ao meio militar. Cada vez mais observamos uma migração das doutrinas antigas de comunicações para meios modernos da tecnologia da informação. Os métodos de transmissão de mensagens são tomados por computadores que, além de proverem os serviços mais facilmente, apresentam versatilidade e grau de segurança elevado. Contudo, essa migração demanda uma especialização de seus usuários, bem como modernização da infraestrutura.

Em face a esse cenário, o estudo de redes de computadores para compreensão do seu funcionamento se tornam fundamentais para integração de todos os meios cibernéticos que se apresentam como possibilidades para as comunicações, para atender da melhor forma possível as operações.

O objetivo central do trabalho foi analisar de maneira sistêmica as vantagens e as desvantagens dos sistemas operacionais *Windows* e a distribuição *Debian* do *Linux* com objetivo de definir qual é o melhor para implementação de uma rede de computadores em uma Operação de Garantia da Lei e da Ordem. Para isso, estudamos as características dessas operações, que são apresentadas no capítulo 3, e levantamos os aspectos a serem atingidos pelos sistemas operacionais pautados para suprir essas características.

O trabalho está estruturado em uma revisão bibliográfica a cerca dos assuntos rede de computadores e operações de GLO. Durante o desenvolvimento dos capítulos procuraremos descrever as principais características dos sistemas operacionais estudados com intuito de definir qual sistema operacional apresenta o melhor relação custo-benefício, e dos principais serviços que permitem o estabelecimento e funcionamento de uma infraestrutura de rede. O trabalho estudou os sistemas operacionais *Windows Server 2012 R2* e a distribuição *Debian* do *Linux.*

No capítulo 4, são apresentadas as principais características e os quesitos do *Windows Server 2012 R2* que atendam às necessidades das operações GLO, levantados no capítulo 3. No capítulo 5 estudaremos as características do *Linux* e a distribuição *Debian*, que foi o alvo

da pesquisa para comparação do o *Windows Server 2012 R2*. Os capítulos 6, 7 e 8 abordam os temas relacionados aos serviços necessários para estabelecimento de uma infraestrutura básica de rede, que foram o *DHCP*, *DNS* e serviço de autenticação, respectivamente. Nesses capítulos são explicados o funcionamento dos serviços e como eles podem influências as operações. São apresentados os requisitos para instalação em cada um dos Sistemas Operacionais estudados.

Por fim, uma análise de dados e a conclusão, com um compilado das informações colhidas durante a pesquisa. Durante análise de dados, faremos uma comparação das vantagens e desvantagens de cada sistema operacional de acordo com as características de seus serviços, dentro dos parâmetros de comparação estabelecidos, que serão levados em conta durante a conclusão do trabalho.

2. REFERENCIAL TEÓRICO-METODOLÓGICO

Este trabalho utiliza a abordagem qualitativa e desenvolve-se basicamente na revisão bibliográfica, ou seja, em um processo investigativo a partir do levantamento de referências, a fim de atender os objetivos pautados, que são a resolução do problema: qual Sistema Operacional de Rede atende melhor a uma Operação GLO para o estabelecimento de uma infraestrutura básica de rede de computadores? Segundo Gerhardt e Silveira, na pesquisa qualitativa "O desenvolvimento da pesquisa é imprevisível. (2009, p. 32). O conhecimento do pesquisador é parcial e limitado". Ainda segundo Gerhardt e Silveira, as características da pesquisa qualitativa são:

> Objetivação do fenômeno; hierarquização das ações de descrever, compreender, explicar, […]; busca de resultados os mais fidedignos possíveis; oposição ao pressuposto que defende um modelo único de pesquisa para todas as ciências. (SILVEIRA, GERHARDT, 2009, p. 32).

Para a coleta de dados a cerca do assunto de rede de computadores e sistemas operacionais, foram utilizados livros sobre os assuntos, além de consultas a fóruns e portais de *internet*, sempre embasando as informações colhidas nessas fontes em conhecimentos científicos já publicados.

Partimos da premissa da seguinte hipótese: Dadas a situação orçamentária e as necessidades do Exército Brasileiro atualmente e, levando em consideração as diferenças de aplicação, *hardware* necessário e custo da implementação dos sistemas operacionais *Windows Server* e *Linux*, qual desses sistemas operacionais é o mais adequado para o estabelecimento de infraestrutura básica de rede de computadores em operações GLO? Qual apresenta condições mais favoráveis ao uso?

O processo de pesquisa é do tipo exploratório. Segundo Köche, "o objetivo fundamental de uma pesquisa exploratória é o de descrever ou caracterizar a natureza das variáveis que se quer conhecer". (2000, p. 126). O objetivo da pesquisa exploratória é tornar o objetivo estudado mais explícito, através de levantamento bibliográfico, como é o caso deste trabalho.

Neste trabalho, vamos estudar basicamente os sistemas *Windows Server* R2 2012 e o *Debian*, distribuição do *Linux* que é sugerida pelo Plano de Migração para *Software* Livre do Exército Brasileiro. O motivo da escolha desses dois sistemas será explanado mais à frente. Para fins de análise e conclusão, foram observados alguns aspectos de relevância para o Exército Brasileiro na escolha do Sistema Operacional. Os pontos a serem abordados são: o custo do Sistema Operacional, custo de licença, de *hardware* necessário para instalação, con-

figuração e operação; custo de capacitação de usuários, facilidade de implementação, a flexibilidade em caso de desdobramento do PC nas operações e requisitos doutrinários das operações GLO que precisam ser atendidos por essa infraestrutura básica.

Sabemos que o Exército sofre, atualmente, com restrições orçamentárias, e dentro do processo administrativo, o valor dos produtos a serem adquiridos são fatores preponderantes na sua escolha durante uma licitação. Por isso o valor do *software* é relevante para análise deste trabalho.

Através da pesquisa qualitativa poderemos chegar a essas respostas. Utilizando o método exploratório procuraremos entender basicamente como funciona uma rede e as possibilidades de implementação dos Sistemas Operacionais propostos para o estabelecimento dessa rede em uma Operação GLO. Através da revisão bibliográfica acerca do assunto Redes de Computadores, teremos o embasamento teórico necessário relativo à parte técnica do tema proposto neste trabalho.

O presente trabalho trata de um tipo de operação, as operações GLO. O emprego desse tipo de operações é descrito no manual MD33-M-10: Garantia da Lei e da Ordem. Do ponto de vista legal, essas operações são reguladas pela Constituição Federal de 1988, a Lei Complementar no 97/99 e as suas modificações (Lei Complementar no 117, de 02 de setembro de 2004 e Lei Complementar no 136, de 25 de agosto de 2010) e as diretrizes específicas de emprego das Forças Armadas, em Operações GLO, o Decreto n° 3.897, de 24 de agosto de 2001.

2.1 Revisão Bibliográfica

No contexto dos conflitos do século XXI e dos conflitos no amplo espectro, cresceu de importância a utilização dos meios de Tecnologia de Informação e Comunicações (TIC), de modo que elas se tornaram vitais para o sucesso das operações em geral. As informações passaram a circular nos meios informatizados e a *internet* tomou espaço no campo de batalha. Para isso, passamos a utilizar diversas tecnologias disponíveis no mercado, entretanto, cabe uma análise de qual a melhor opção, tanto em questões de eficiência do serviço, quanto em questões de segurança, de confiabilidade dos sistemas e de custo de implementação, haja vista a quantidade de ofertas no mercado cibernético. O objeto de estudo deste trabalho será a implementação de Sistemas Operacionais para estabelecimento de infraestrutura básica de rede em Operações de Garantia da Lei e da Ordem (Op GLO), no qual tentaremos definir qual sistema operacional é o mais adequado para esse tipo de operação. Estudaremos os sistemas *Linux* e o *Microsoft Windows Server* 2012 R2.

A *Microsoft* teve um papel fundamental para a popularização dos computadores pessoais com seu sistema operacional *Windows.* Por muito tempo, ele foi protagonista como o sistema operacional mais popular do mundo e, por isso, ele se encontra no escopo da pesquisa. Atualmente, em nível de servidores, esse posto é ocupado pelo *Linux*, através de suas diversas distribuições, sendo o sistema operacional mais utilizado para fornecimento de serviços de rede. Em nível de sistemas operacionais para *desktop* (computadores pessoais), a solução da *Microsoft* ainda é homogênea, mas para outros dispositivos, como *smartphones*, a situação se inverte e o Android, que é uma distribuição *Linux*, é dominante. O motivo da escolha da versão *Windows Server 2012 R2* se dá pelo fato de que essa versão ainda é estável e possui suporte. Além disso, as literaturas são mais abundantes que as da versão 2016, visto que, até o momento deste trabalho de pesquisa, a versão 2016 não possuía dois anos de lançamento.

O *Linux* é o sistema operacional que concorre com as versões do *Windows* e tem uma grande importância e influência na comunidade mundial das TIC. Usaremos como objeto da pesquisa a distribuição *Debian*, pois é a estabelecida pelo Plano de Migração para *Software* Livre do Exército Brasileiro. Uma distribuição *Linux* é composta pelo *kernel Linux* e um conjunto de *softwares* determinados pelos seus desenvolvedores. Segundo Morimoto, o *kernel* é como o coração do sistema operacional, aquilo que provê a infraestrutura básica para os programas funcionarem, e é comum a todas as distribuições *Linux*, sendo que o que muda nas diferentes distribuições existentes são as aplicações e os pacotes de funcionalidade que cada uma pode oferecer ao usuário.

2.2 Operações de Garantia da Lei e da Ordem

Nos últimos anos, vemos uma crescente demanda do emprego do Exército Brasileiro em Op GLO. “Somente entre 2010 e 2017, GLO foi decretada 29 vezes” no Brasil. (PORTAL PLANALTO, 2017). Diversos são os exemplos que podemos citar, como as operações de ocupação em várias comunidades do Rio de Janeiro; a segurança pública nos estados do Espírito Santo e Bahia, devido às greves das polícias militares; os vasculhamentos dos presídios durante as rebeliões que ocorreram no primeiro semestre de 2017 e, a mais recente, a intervenção federal no estado do Rio de Janeiro, a qual teve o decreto assinado pelo Presidente da República e aprovado pelo Senado no dia 20 de fevereiro de 2018.

As Op GLO são operações realizadas pelo Exército que atua em localidades urbanas ou rurais, com características bem distintas daquelas da guerra convencional. Segundo o

manual MD33-M-10, Garantia da Lei e da Ordem:

> As Operações de Garantia da Lei e da Ordem (Op GLO) caracterizam-se como operações de “não guerra”, pois, embora empregando o Poder Militar, no âmbito interno, não envolve o combate propriamente dito, mas podem, em circunstâncias especiais, envolver o uso de força de forma limitada, podendo ocorrer tanto em ambiente urbano quanto rural. (BRASIL, 2013, p. 17).

A Constituição Federal de 1988 cita, no texto do seu art. 142, as Op GLO como um das funções das Forças Armadas. Essas operações são reguladas pela Lei Complementar n° 97/99, nos art. 15, art. 16 e art. 17, que versam sobre o emprego e preparo das Forças Armadas, e pelo decreto n° 3.897, de 24 de agosto de 2001, que tem como objetivo “orientar o planejamento, a coordenação e a execução das ações das Forças Armadas, e de órgãos governamentais federais, na garantia da lei e da ordem.” (BRASIL, 2001).

2.3 Rede de Computadores

Uma Companhia de Comunicações (Cia Com) tem por missão instalar, explorar e manter os meios de comunicações de uma Brigada de Infantaria ou Cavalaria.

Dentre todos os meios de comunicações possíveis podemos citar o estabelecimento de rede de computadores para levantamento de diversos serviços necessários para uma missão. (BRASIL, 1997).

Redes de computadores são conexões de vários dispositivos computacionais com a finalidade de compartilhar informações entre si. Uma rede de computadores pode se resumir em uma simples conexão de dois computadores ou centenas de dispositivos diferentes conectados e compartilhando recursos. (DA SILVA, 2010, p. 41).

2.3.1 Generalidades a respeito de Redes de Computadores

Neste tópico, vamos explicar sucintamente algumas generalidades a respeito do funcionamento de uma rede de computadores, para o melhor entendimento dos conceitos abordados nos próximos capítulos.

2.3.1.1 Protocolo de Rede

Uma rede é a conexão de dois ou mais dispositivos que compartilham informações.

Para que haja essa interação, é necessária a utilização de protocolos, que são conjuntos de regras que permitem a comunicação entre os dispositivos conectados à rede. Analogamente podemos comparar como se essas regras fossem a linguagem falada entre duas pessoas. Para que ocorra a comunicação, ambas as partes precisam falar o mesmo idioma, e isso também se aplica ao meio cibernético.

> O protocolo de rede é a linguagem usada para a comunicação entre um computador e outro. Existem vários tipos de protocolos usados para a comunicação de dados, alguns são projetados para pequenas redes (como é o caso do NetBios) outros para redes mundiais (TCP/IP que possui características de roteamento).
> Dentre os protocolos, o que mais se destaca atualmente é o TCP/IP devido ao seu projeto, velocidade e capacidade de roteamento. (DA SILVA, 2010, p. 42).

Todos os dispositivos, que estão conectados, são reconhecidos e localizados dentro da rede por uma sequência de números denominada endereço *Internet Protocol* (IP). De acordo com Gleydson Mazioli da Silva (2010, p. 42), os endereços IP podem ser comparados aos números de telefone de cada usuário. Quando alguém na rede deseja se comunicar com outra máquina, são utilizados os IPs, para identificar qual dispositivo está falando com quem, assim há uma organização no fluxo de informações dentro da rede. Existem duas versões de endereços IP: a versão 4 e a versão 6. Utilizamos a versão 4 por ser a mais difundida no mundo e também por que a versão 6 ainda está em fase de implementação.

Os endereços IP versão 4 são constituídos por quatro octetos contendo 8 bits em cada, e são separados por pontos, por exemplo “192.168.0.1”. Os bits por sua vez, são potências de 2, ou seja, 8 bits é equivalente a 2^8 que é igual a 256.

2.3.1.2 Serviços de rede, servidores e usuários

Serviços de rede são as aplicações que serão utilizadas na rede, “é o que está disponível para ser acessado pelo usuário” (MAZIOLI, 2010, p. 52). Uma das vantagens da rede, que serão abordadas mais à frente, é justamente o compartilhamento de serviços. Alguns desses serviços são essenciais para o funcionamento da rede, como, por exemplo, o *DNS*. Outros serviços, no entanto, são ferramentas de trabalho que visam facilitar as tarefas executadas em um ambiente operacional, ou agregam valor às atividades com serviços específicos, de uma empresa ou de qualquer outro ambiente em que se trabalhe com sistemas computadorizados. Podemos citar como exemplos os serviços de videoconferências, correio eletrônico, mensagens instantâneas, etc., em uma operação GLO.

Esses serviços estão instalados em servidores, que são “Computadores que fornecem

recursos compartilhados para os usuários da rede.” (LANZA, 2007, p. 10) Nada mais são do que computadores com alguma aplicação instalada e conectados à rede, capazes de fornecer um ou mais serviços aos usuários.

Os clientes, também chamados de *hosts*, por sua vez são quaisquer computadores conectados à rede que fazem acesso aos serviços dela. Geralmente cada usuário da rede possui uma credencial de acesso com nome de usuário e senha e não se restringem apenas em utilizadores da rede. Programadores e gerentes também são denominados usuários. Basicamente usuários são aqueles que utilizam os serviços.

2.3.2 Por que utilizar uma rede de computadores?

Nas décadas de 60 e 70 do século passado, durante o período da Guerra Fria, iniciaram os primeiros estudos a respeito da troca de informações entre computadores que, no futuro, viriam se tornar a *Internet*. A tecnologia avançou e os computadores passaram a ter processadores mais rápidos até que, em agosto de 1995, a empresa americana *Microsoft* lançou o *Windows* 95 que possuía uma interface diferente dos sistemas operacionais anteriores muito mais intuitiva e fácil de ser usada. Nos anos 2000, os computadores invadiram os lares e a *internet* cresceu a nível global tanto que, anos depois, em 2010, já havia quase 1,4 bilhão de pessoas conectadas à *internet*. (SERAGGI, 2015, p. 9).

A evolução dos meios de informação, o surgimento dos computadores e posteriormente a *internet* motivaram as pessoas a se adequarem a esse novo meio de comunicação. Um computador isolado não é capaz de transmitir uma informação para outro, sem que haja um canal específico para essa tarefa. Para existir uma comunicação entre os dispositivos são necessários uma rede que ligue os computadores e protocolos que realizem essa interação. Existem várias vantagens de se utilizar uma rede de computadores em um ambiente operacional: o alargamento da comunicação entre escalões, a facilidade de compartilhamento de serviços e a facilidade de definir os clientes que possuem acesso à rede, tudo isso com uma única estrutura física, diferentemente do passado em que cada meio de comunicação exigia uma estrutura própria.

O Comandante da Brigada consegue realizar contato informatizado através de textos, videoconferências e telefonia com os comandantes dos batalhões destacados mais facilmente, utilizando uma única infraestrutura. Caso não houvesse o emprego TIC nas operações, a alternativa para a comunicação seria via rádio ou mensageiro, meios utilizados durante a Segunda Guerra Mundial, há 70 anos, obsoletos nos dias atuais, se considerarmos as opções dispo-

níveis que as redes de computadores nos oferecem, a velocidade na transmissão dos dados, o alcance e a quantidade de dados transmitido em relação ao tempo.

Além da facilidade da tramitação das informações, diversos serviços podem ser compartilhados, como serviços de correio eletrônico, telefonia IP (VoIP), mensagens instantâneas, etc. Devido ao tamanho pequeno de uma rede de computadores de uma Brigada, não é necessário ter diversos servidores do mesmo serviço nos postos de comando (PC) de cada unidade. Basta apenas que um desses servidores esteja configurado e que todos os computadores da brigada tenham acesso à rede, para que os serviços sejam comuns a todos e isso implica em redução de custo. Em vez de comprar vários servidores ou várias impressoras para cada terminal, basta apenas um de cada conectado à rede.

Uma rede precisa ser controlada um sistema de autenticação o qual permite o acesso somente a usuários cadastrados. Entretanto esses sistemas podem apresentar vulnerabilidades, como, por exemplo, roubo de senhas, mas, mesmo assim, o emprego de redes é mais seguro que meios alternativos como rádio ou mensageiro.

2.3.3 Infraestrutura Básica de Rede

Uma série de configurações preliminares são necessárias para o estabelecimento de uma rede de computadores. Este trabalho estudou três serviços básicos para se ter uma infraestrutura básica de rede. São eles o *DHCP* (*Dynamic Host Configuration Protocol)*, o *DNS* (*Domain Name System*) e o sistema de autenticação, pois estes são os serviços básicos para o funcionamento automático de uma rede com um mínimo de segurança.

2.3.3.1 DHCP

Imagine a seguinte situação: uma Cia Com está apoiando a Brigada em uma operação, e para isso foi necessária a configuração de uma rede interna para o Comando e Controle dessa Brigada. Os PCs de cada escalão deverão possuir os terminais para suas sessões de acordo com a necessidade, além dos elementos destacados que utilizam sistemas de comando e controle como, por exemplo, o Pacificador, *software* utilizado para o apoio à decisão. Como vimos anteriormente, cada dispositivo da rede é identificado pelo seu endereço IP. Porém, esses números não são distribuídos aleatoriamente. Existem regras a serem respeitadas para o correto funcionamento da rede. Para entendermos melhor vamos utilizar o mesmo exemplo da comunicação entre duas pessoas: mesmo que elas falem o mesmo idioma (protocolo), as pa-

lavras devem ser colocadas na ordem correta (regras), para a conversa ser efetiva. Por isso é necessária a configuração das informações da rede nos computadores. Se esse serviço fosse executado manualmente, demandaria tempo e uma equipe grande, inviabilizando o processo e para isso foi criado o *DHCP*.

DHCP é a abreviatura de *Dynamic Host Configuration Protocol* que significa Protocolo de Configuração Dinâmica de Endereços de Rede. Ou seja, através desse protocolo, o cliente que se conectar à rede receberá as informações da rede e um endereço IP válido. Com o *DHCP* o usuário não precisa configurar manualmente o endereço IP, máscara de sub-rede, *gateway* padrão, *DNS*, etc. (COMER, 2006, p. 271).

2.3.3.2 DNS

O acrônimo *DNS* significa *Domain Name System* ou Sistema de Nomes de Domínios. Segundo Renan Osório Rios, é um dos serviços mais importantes da *internet*, responsável pela conversão do nome das páginas web para endereços IP. (2011, p. 37). Como disse Gleydson Mazioli da Silva:

> O *DNS* foi criado com o objetivo de tornar as coisas mais fáceis para o usuário, permitindo assim, a identificação de computadores na *Internet* ou redes locais através de nomes […]. A parte responsável por traduzir os nomes como www.nome.com.br em um endereço IP é chamada de resolvedor de nomes.
> O resolvedor de nomes pode ser um banco de dados local (controlador por um arquivo ou programa) que converte automaticamente os nomes em endereços IP ou através de servidores *DNS* que fazem a busca em um banco de dados na *Internet* e retornam o endereço IP do computador desejado.Através do *DNS* é necessário apenas decorar o endereço sem precisar se preocupar com o endereço IP […]. (DA SILVA, 2010, p. 48).

Uma analogia muito utilizada para explicar esse serviço é o sistema de telefonia no qual os IPs são comparados aos números dos telefones dos serviços da rede. Você pode decorar o telefone de todos os serviços da rede ou utilizar um endereço mais intuitivo, fácil de decorar, por exemplo: suponhamos que vamos acessar o Zimbra, um serviço de correio eletrônico amplamente utilizado em operações, e o seu endereço IP seja “192.168.10.132”. Esse endereço pode se confundir com IPs de outros serviços que estarão na mesma faixa de IP, porém seria muito mais fácil acessá-lo se o endereço fosse um nome simples como zimbra.opglo. É isso que o *DNS* faz: traduz os endereços IP em nomes e vice-versa, que facilita o cliente encontrá-los na rede e gerencia esses endereços hierarquicamente.

2.3.3.3 Autenticação

O serviço de autenticação auxilia a segurança da rede contra intrusos, impedindo que usuários não autorizados acessem a rede. Como o próprio nome diz, ele possibilita que a rede esteja protegida de usuários não autorizados, exigindo um *login* e uma senha.

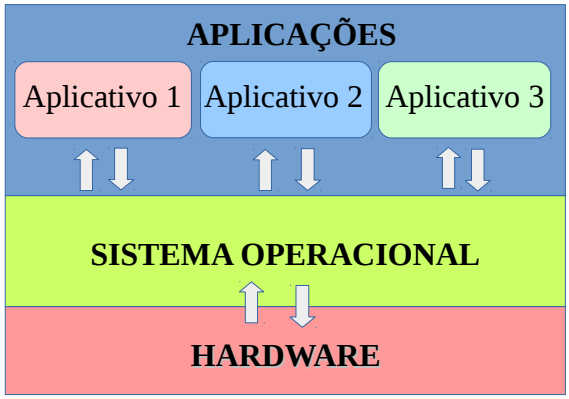
Para se conectar em uma rede cabeada é necessário um meio físico, como os cabos *Unshielded Twisted Pair (UTP)*. Isso oferece uma relativa proteção contra intrusos, pois é necessário que ele possua uma conexão física, ou seja, um cabo ligado à rede. No exemplo de Operações GLO, os escalões estão separados por distâncias que inviabilizam o uso de cabos, pois eles sofrem atenuações do sinal e porque esses escalões necessitam de mobilidade constante. Para fazer frente a essas dificuldades, antenas são utilizadas para realizar os *links*, e nesse caso bastaria uma outra antena para um intruso estar apto a tentar invadir a rede. Por isso que o serviço de autenticação é de suma importância para uma rede, principalmente em uma operação militar, onde o tráfego de informações sigilosas é constante. (RIOS, 2010, p. 70).

2.4 Sistemas Operacionais

Um computador é formado por sistemas complexos de dispositivos e circuitos eletrônicos, que utilizam uma linguagem muito distante daquela usada na programação dos *softwares* das aplicações (chamada de linguagem de baixo nível). Se cada programador tivesse de entender como esses circuitos funcionam, pouquíssimos códigos seriam escritos. “Por isso, os computadores têm um dispositivo de *software* denominado Sistema Operacional, cujo trabalho é fornecer aos programas do usuário um modelo de computador melhor, mais simples e limpo”, algo praticável e fácil de entender, “e lidar com o gerenciamento de todos os recursos mencionados”. (TANENBAUM, 2009, p. 1).

“O sistema operacional é uma camada de *software* que opera entre o *hardware* e os programas aplicativos voltados ao usuário final”. (MAZIERO, 2017, p. 1). Ou seja, entre a parte física do computador (as placas e circuitos eletrônicos) e os aplicativos utilizados pelo usuário está o sistema operacional, o “cérebro” encarregado de realizar a interação da máquina com os aplicativos, como ilustra figura 1.

Figura 1 – Diagrama de um sistema operacional



Fonte: o autor.

Existem alguns tipos de sistemas operacionais específicos para uma tarefa que queria realizar. Geralmente todo dispositivo eletrônico possui um sistema operacional encarregado de fazer com que o *hardware* execute os aplicativos. Por exemplo, um caixa eletrônico de um banco possui o seu sistema operacional específico programado e configurado para realizar aquelas operações do caixa, assim como um *smartphone* possui um sistema operacional capaz de traduzir a linguagem do celular para os seus aplicativos, e os computadores pessoais também possuem os sistemas operacionais próprios para determinada situação.

O trabalho foi desenvolvido em cima de rede de computadores, portanto o tipo de sistema operacional estudado foi o Sistema Operacional de Rede (SOR). Os SOR são especializados para realizar as tarefas inerentes a uma rede de computadores. Alguns recursos comuns a sistemas operacionais para computadores domésticos são suprimidos e outros são potencializados para o melhor desempenho na hospedagem de serviços de rede. O Professor Carlos A. Maziero define:

> Um sistema operacional de rede deve possuir suporte à operação em rede, ou seja, a capacidade de oferecer às aplicações locais recursos que estejam localizado sem outros computadores da rede, como arquivos e impressoras. Ele também deve disponibilizar seus recursos locais aos demais computadores, de forma controlada. A maioria dos sistemas operacionais atuais oferece esse tipo de funcionalidade. (MAZIERO, 2017, p. 4).

3. OPERAÇÕES GLO

No Brasil, operações GLO são aquelas operações realizadas pelas Forças Armadas em apoio a órgãos governamentais, com o objetivo de manter a ordem pública. Possuem o caráter de “não guerra”, pois, mesmo empregando o poder militar, não envolvem o combate propriamente dito, mas não excluem a possibilidade do uso da força em determinadas situações. Ocorrem quando todos os instrumentos destinados à preservação da ordem pública se esgotam após instaurada uma crise na segurança pública, sendo o emprego delas decidido somente pelo Presidente da República. O manual de MD33-M-10 define que “o emprego das FA em Op GLO deverá ser episódico, em área previamente definida e ter a menor duração possível”, ou seja, não são operações duradouras que se desenvolvem rotineiramente. (BRASIL, 2013, p. 18).

O emprego do Exército em operações GLO caracteriza-se pelo caráter preventivo, através das estratégias da presença e da dissuasão, ou seja, “operações presença” com intenção de mitigar a atividade e a capacidade de atuação das forças adversas, aplicando operações tipo polícia e adotando os dispositivos legais atribuídos a elas. (BRASIL, 2013, p. 38) As operações tipo polícia tem a finalidade de controlar a população, diminuir a capacidade de atuação das forças oponentes, apreender material e suprimentos, etc.

Uma Brigada de Infantaria padrão do Exército Brasileiro, possui em seu organograma unidades de manobra, que são os batalhões de infantaria e esquadrão ou regimento de cavalaria, dependendo da brigada; e as unidades de comando e apoio, que são as unidades de artilharia, engenharia, comunicações e logísticas. Geralmente uma brigada de infantaria é composta por 4 unidades de manobra, sendo três Batalhões de Infantaria e um Esquadrão de Cavalaria, além das unidades de apoio: um Grupo de Artilharia (GAC), uma Companhia de Engenharia (Cia Eng), uma Companhia de Comunicações (Cia Com), uma Companhia de Comando (Cia Cmdo), um Pelotão da Polícia do Exército (Pel PE) e um Batalhão Logístico (B Log). (BRASIL, 1984, p. 1-13)

3.1 Rede de computadores nas Operações GLO

A rede de computadores implementada em uma operação deve atender algumas características dessas operações. Vamos analisar as necessidades que os sistemas operacionais e os servidores devem atender para o bom prosseguimento das operações GLO.

A coordenação dessas operações é realizada pelo Ministério da Defesa, que mantém li-

gação direta com as forças empregadas (Forças Armadas, polícias militares e civis, bombeiros, órgãos não governamentais, etc.). O Centro de Coordenação de Operações (CCOp) é a estrutura responsável por concentrar todo o sistema de comando e controle, onde funcionam os órgãos responsáveis pela organização, planejamento e condução das Operações GLO. É no CCOp que se encontram as estruturas responsáveis por assessorar o comando na consciência situacional e na tomada de decisão, onde abriga, entre outros, os sistemas de comunicações da operação.

A quantidade de estações utilizadas durante a operação influencia no servidor em questão. Quanto mais máquinas conectadas na rede, mais capacidade de processamento será exigido. Isso quer dizer que uma operação de grande vulto necessitará de um ou mais servidor mais potentes. Primeiramente, devemos ter ciência da demanda no próprio CCOp. Uma brigada padrão possui cinco elementos em seu Estado-Maior (EM) Geral (formados pelos chefes da 1ª, 2ª, 3ª, 4ª e 5ª seções), e outros elementos de apoio que constituem o EM Especial, formado pelos chefes de diferentes serviços, além dos comandantes das unidades de apoio (GAC, Cia Eng, Pel PE, Cia Cmd, Cia Com e B Log) e do ajudante geral. Pelo menos, duas estações para cada elemento do EM da brigada devem ser disponibilizadas. Para atendê-los vamos utilizar como parâmetro mínimo 22 estações e mais 2 estações para o comandante, totalizando 24 estações e serem atendidas, somente no CCOp da Brigada. (BRASIL, 1984, p. 1-13).

As unidades destacadas também possuem o seu EM que necessitam de suas estações próprias, além dos elementos de menor escalão. Cada unidade nível batalhão possui 5 elementos em seu EM. Utilizando o mesmo raciocínio do EM de uma Brigada, com 2 estações para cada elemento, teremos 10 estações mais 2 estações para o comando, e nos menores escalões destacados, pelo menos um operador de sistema de comando e controle (Pacificador ou C2 em Combate). (BRASIL, 2003 p. 2-3)

O B Log, por sua vez, é a unidade responsável por prover todo o apoio logístico da Brigada, tanto em suprimentos quanto em manutenção, e a sua capacidade de apoio “depende, entre outras coisas, da eficiência do sistema de comunicações, o qual deve proporcionar segurança e flexibilidade, permitindo ao comando um efetivo controle administrativo da unidade” (BRASIL, 1984b, p. 10-1). É constituído por uma Companhia de Saúde, uma Companhia de Intendência, uma Companhia de Material Bélico e uma Companhia de Comando e Serviços. (BRASIL, 1984b, p. 2-1). A principal necessidade de comunicação são as realizadas com os elementos apoiados, ou seja, com o escalão superior e todas as suas unidades orgânicas, com a finalidade de receber dados e informações necessárias ao cumprimento da missão. A consti-

tuição do EM de um batalhão não se distingue de outro batalhão comum. São necessárias 10 estações para o EM, e mais 2 para o comandante. Para a ligação entre os seus elementos internos são necessários duas estações para cada subunidade, ou seja, um total de 10 estações para cada elemento do batalhão.

As operações GLO são operações que geralmente possuem uma duração curta. Contudo, essas operações não podem sofrer interrupções, justamente por serem operações com objetivo a ser atingido rapidamente. Ou seja, qualquer interrupção nos meios de comunicações significaria um grande prejuízo para o sucesso da operação. Visando esse requisito, é valido utilizar redundância de servidores.

Geralmente, essas operações são realizadas por uma Brigada, com adaptações necessárias dependendo da necessidade de cada operação. O CCOp de uma operação geralmente é instalado no próprio quartel-general do escalão empregado, isso quer dizer que todas as centrais dos sistemas ficarão estacionadas em um mesmo lugar. Essa característica é importante, pois é um dos fatores proposto neste trabalho a ser analisado para a escolha do sistema operacional de rede. Como o CCOp é estacionado, o fator mobilidade pode ser suprimido durante a análise dos resultados. Por outro lado, alguns escalões poderão se destacar no terreno durante algumas ações GLO, porém isso não interfere nos servidores dos serviços empregados durante a operação.

As operações GLO são muitas vezes aplicadas em ambiente urbano, como tem demonstrado as últimas atividades do Exército Brasileiro. Há um grande uso de *softwares* de comando e controle como Pacificador e o C2 em Combate (*softwares* utilizados durante operações que promovem a consciência situacional e apoio à decisão), que são executados no navegador de *internet*. Ambos os serviços já possuem seus servidores fixos e necessitam apenas da *EBNet* (rede privada do Exército) para sua utilização.

4. *WINDOWS* SERVER 2012 R2

O *Windows Server* 2012 R2 é um sistema operacional da *Microsoft*, lançado em 2013. É um *software* proprietário, de código fechado, ou seja, existem custos sobre sua licença e não é permitido o acesso ao código fonte. A Microsoft oferece 4 versões diferentes do *Windows Server* 2012 R2 para cada situação. São elas: *Foundation, Essential, Standart e Datacenter*. (SERAGGI, 2015, p. 51).

Segundo Márcio R. Seraggi, em um ambiente com mais de 25 computadores e com a necessidade de instalação de algumas máquinas virtuais, ambiente semelhante ao de uma Op GLO, o mais recomendado é a versão *Standard Edition.* (2015, p. 51). No site da *Microsoft* é possível constatar que o preço dessa versão é de 882 dólares atualmente.

Ainda existe o licenciamento por núcleo de processador. Alguns serviços do *Windows Server 2012 R2* necessitam de licenças para rodar. Esse tipo de licença está relacionada com a quantidade de processadores que existe no servidor. Ou seja, dependendo do servidor, o valor da licença será multiplicado pelo número de núcleos do processador, tornando o preço do licenciamento mais alto.

Além da licença do servidor, existem as licenças de acesso, chamadas de *Client Access License* (CAL), que também necessitam ser adquiridas. Existem dois tipos de CAL: a de dispositivo e a de cliente. A licença CAL de dispositivo permite que uma estação de trabalho acesse a rede independendo do usuário. Esse tipo de licença é a mais ideal no contexto das Operações GLO, pois existe uma rotatividade de pessoal dentro do Exército, logo é mais interessante que a estação esteja habilitada, e não o usuário. Já a licença CAL de usuário permite o acesso de um usuário em uma estação qualquer. Um pacote de 5 CAL, tanto usuário quanto dispositivo, para o *Windows Server 2012 R2*, gira em torno de 490 reais, ou seja, aproximadamente 100 reais por licença.

É importante observar o preço do *hardware* necessário para instalação dos servidores. As recomendações de *hardware* para configuração de um servidor *Windows*, que atenda às necessidades de uma Operação GLO (*Standard Edition)* são:

- Processador: Intel Xeon E5-2690 2,9 GHz;
- Memória *RAM:* entre 32 GB e 64 GB;
- Disco Rígido: 2 *HDs* com pelo menos 1 TB;

Outro fator que implica aumento no custo é a capacitação de usuários. Um exemplo prático observado foi o preço das fontes bibliográficas utilizadas nesse trabalho. Os livros referentes ao *Windows Server 2012 R2* eram mais caros e a versão mais recente, o *Windows*

Server 2016, não possuía fontes traduzidas para o português.

Em questão de cursos para qualificação e certificação dos usuários, vamos tomar como base o *Microsoft Certified Solutions Expert* (*MCSE*) e o *Microsoft Certified Solutions Associate* (*MCSA*). Ambas as certificações são fornecidas pela *Microsoft* e qualificam o usuário a ser um especialista e administrador de rede, sendo que o *MCSE* exige como pré-requisito o *MCSA*. Para obter o certificado *MCSA* do *Windows Server 2012 R2 é* necessária a realização de três exames específicos, cada exame desses com um valor de US$ 100,00, resultando em um custo total de U$ 300,00, ou um total de R$ 1102,00 em valores de maio de 2018. Para o *MCSE*, é necessária a realização de 10 exames, com valor de US$ 100,00 cada, que resulta num total de U$ 1000,00, ou R$ 3674,50 em valores de maio de 2018. (*MICROSOFT*, 2018).

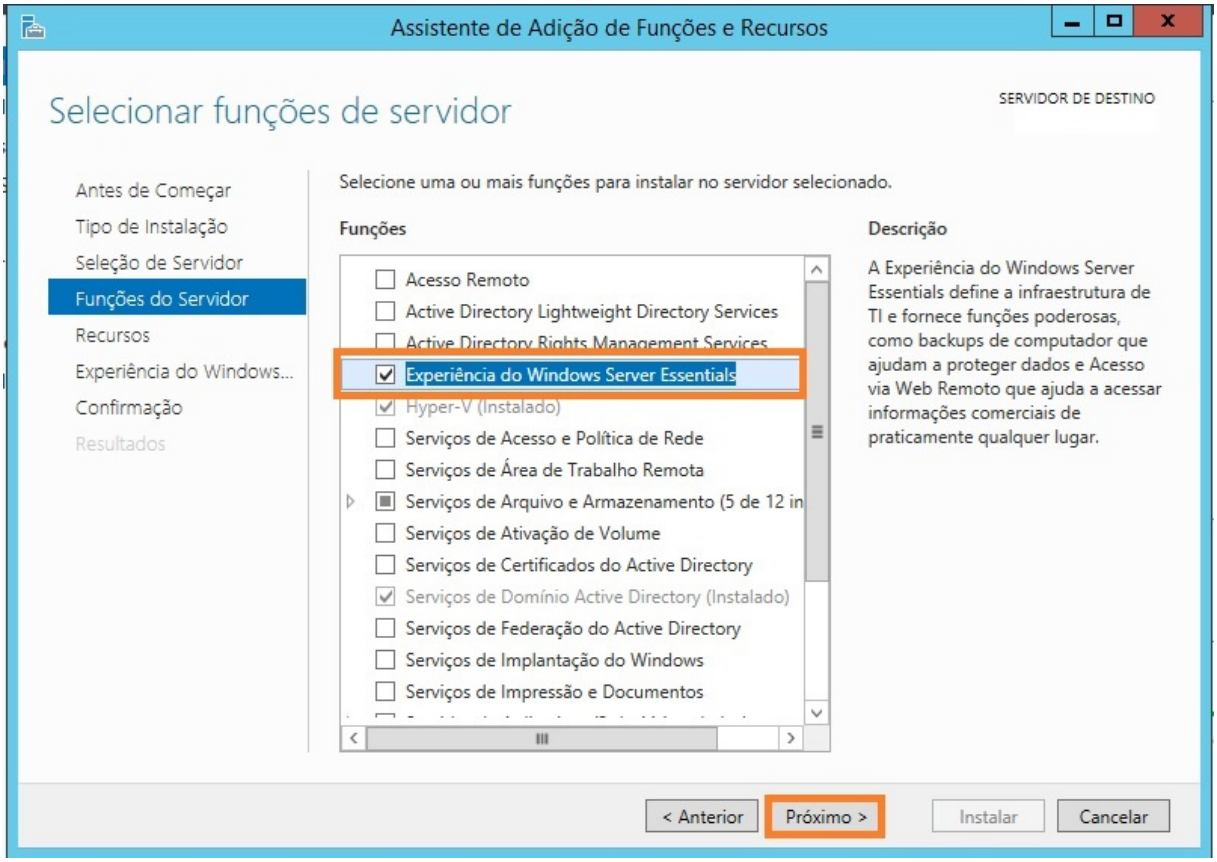
Os cursos destinados ao treinamento e preparação para a realização dos cursos são fornecidos por algumas empresas chamadas de *Microsoft Partner.* Essas empresas são credenciadas pela *Microsoft* a fornecer cursos aos alunos. O SENAC fornece cursos para o *MCSA* com valor de R$ 1726,00 a R$ 2158,00, dependendo do local dos cursos. (SENAC, 2018a). A *Impacta*, empresa consagrada em treinamentos de serviços de TIC, fornece curso preparatório para os exames *MCSA* com preço a partir de R$ 3207,00. Os cursos de certificação para o *MCSE* giram em torno de R$ 3500,00. (IMPACTA, 2018). A empresa *Trainning Education Service* oferece cursos com o preço de R$ 3561,00 para os exames dessa certificação. (TRAINNING, 2018). Como meios de consulta, foram encontrados livros específicos para cada exame do *MCSA*, com valor médio de R$ 60,00, na *Amazon.com*, e para o *MCSE*, livros na faixa de R$ 90,00.

Uma característica vantajosa notável do *Windows* é a interação do *software* com o usuário através da sua interface gráfica amigável, bastante intuitiva que facilita a operação até para usuários inexperientes. A configuração de diversos serviços no *Windows*, bem como instalação de aplicativos, são feitas graficamente, através do Gerenciador do Servidor, ferramenta utilizada para realizar as instalações dos serviços de rede do *Windows Server*, como mostra figura 2. São necessários poucos passos, entre a instalação e a conclusão, que se resumem basicamente em selecionar as opções desejadas na qual são apresentadas todas as possibilidades, e prosseguir clicando em “próximo” e “finalizar”. De fato esse processo facilita a configuração e não obriga o usuário a pensar demasiadamente, parar em algum ponto do processo, ou até cometer equívocos durante a configuração. (SEGGARI, 2015, p. 159).

Por ser tratar de um *software* proprietário, a compra de sua licença implica um contrato entre a empresa fornecedora do produto e o cliente. Isso quer dizer que a *Microsoft* tem a obrigação de fornecer suporte técnico para o cliente enquanto durar a garantia a qual foi con-

tratada. Esse suporte técnico se resume apenas em atualizações de *software* e correções de *bugs* (problemas de funcionamento que algum dispositivo ou *software* possa apresentar, seja por defeito ou programação), que é diferente de suporte de consultoria, o qual se resume em orientações sobre a configuração e manipulação do *software*. A *Microsoft* é uma empresa que possui enorme reputação no mercado de *Softwares*, principalmente pelo sucesso das versões *Windows* para computadores pessoais. Por isso o suporte fornecido conta como aspecto positivo para o *Windows Server 2012 R2*.

Figura 2 – Gerenciador do Servidor.



Fonte: *Microsoft*

5. LINUX

O *Linux* é um sistema operacional que começou a ser desenvolvido a partir de 1991 por Linus Torvalds, de código aberto distribuído gratuitamente pela *Internet*. “Seu código fonte é liberado como *Free Software* (*software* livre), sob licença *GPL* […] Isto quer dizer que você não precisa pagar nada para usar o *Linux*, e não é crime fazer cópias para instalar em outros computadores.” (DA SILVA, 2010, p. 4). Todas as ferramentas para o estabelecimento de uma rede podem ser adquiridos com pacotes disponibilizados gratuitamente. O software livre também acrescenta outra característica que é o seu código fonte aberto.

> O código fonte aberto permite que qualquer pessoa veja como o sistema funciona (útil para aprendizado), corrigir algum problema ou fazer alguma sugestão sobre sua melhoria, esse é um dos motivos de seu rápido crescimento, do aumento da compatibilidade de periféricos (como novas placas sendo suportadas logo após seu lançamento) e de sua estabilidade. (DA SILVA, 2010, p. 4).

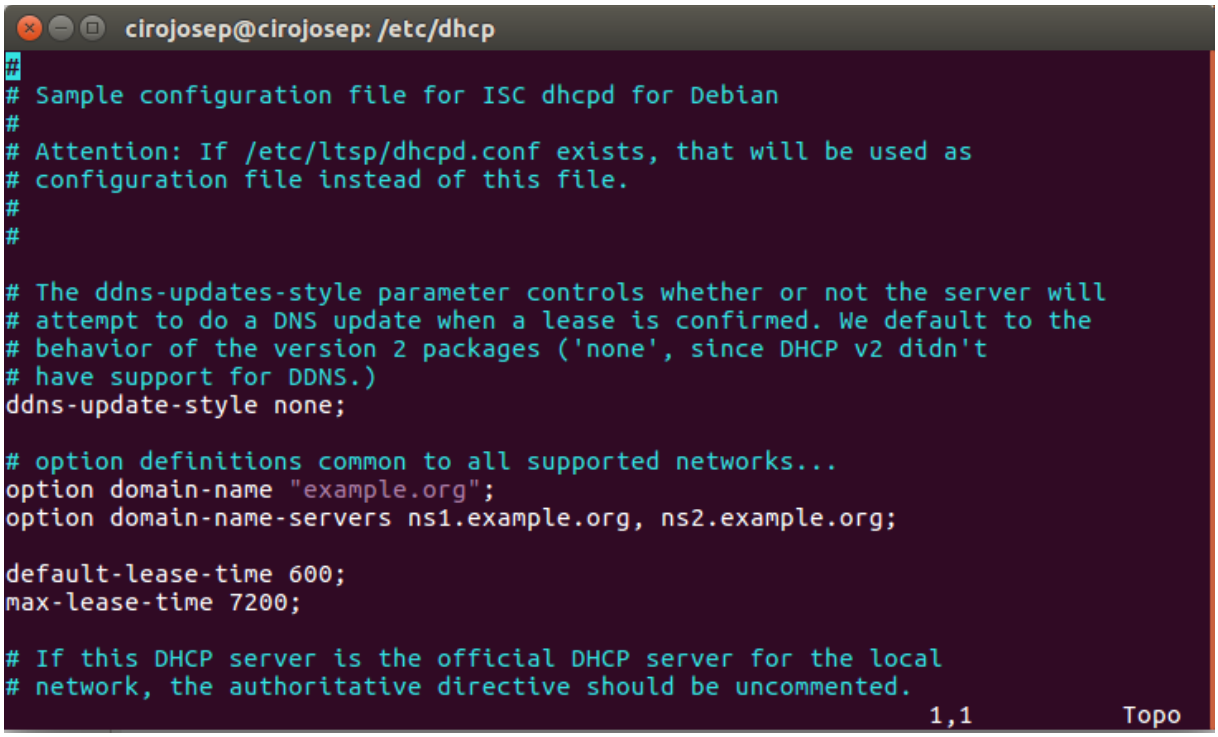
Isso é interessante de se observar visto que a grande maioria das informações que circulam em uma rede de uma Brigada em Operações GLO são sigilosas. Não sabemos ao certo em qual medida o proprietário do *software* tem acesso a essas informações. A possibilidade de ter acesso ao código fonte permite ao usuário entender como estão sendo executados os processos internos, para onde são destinadas as informações que tramitam dentro do computador. É um fator de segurança relevante.

Em relação à capacitação do administrador *Linux,* as principais bibliografias utilizadas neste trabalho, o *Debian Handbook* e o Guia Foca *Linux*, são disponibilizados gratuitamente na *internet*. Além disso, a comunidade entusiasta de usuários *Linux* é muito mais ativa nos fórums online. Isso facilita a busca de informações a respeito do sistema.

Em relação às características de interface do *Linux*, o administrador precisa ter uma certa intimidade com linhas de códigos e a “tela preta” (terminal), no qual são emitidos os códigos para realizar as tarefas. Essa característica assusta usuários menos acostumados com um ambiente abstrato, sem uma janela para selecionar a opção com o *mouse*. Apesar de ser um dificultador no entendimento do usuário sobre o programa, as linhas de código muitas vezes fornecem maiores possibilidades para ele. Vale ressaltar também que as distribuições que fornecem interface gráfica não são muito parecidas com o *Windows.* Existe uma certa resistência por parte da maioria das pessoas em transitar de um determinado sistema para o outro. De fato essa resistência se dá pela popularidade dos computadores domésticos possuírem o sistema da *Microsoft,* o qual crescemos e fomos acostumados a usar desde nosso pri-

meiro contato com o computador. A figura 3 traz um exemplo de um terminal, utilizando a distribuição *Ubuntu 16.04*, ao executar comando para edição de um arquivo de configuração do servidor *DHCP*.

Figura 3 – Terminal Linux



Fonte: o autor.

Na maioria das vezes é necessário realizar o *download* dos pacotes e arquivos de configuração através do terminal, e não apenas abrir uma janela onde são mostradas as aplicações e configurações desejadas. Entretanto, existem aplicativos que realizam *downloads* através de interface gráfica, como é o caso do *Synaptic*. Toda configuração, que não é intuitiva, é feita manualmente, porém uma vez os serviços configurados, o administrador precisa apenas salvar os arquivos de configuração em um *back-up* e, quando for necessário, reutilizá-las, estarão prontas para implementação. (HERTZORG, MAS, 2015).

Tomaremos como base para capacitação dos usuários os certificados da *Linux Professional Institute* (*LPI*), o Instituto Profissional *Linux*. O *LPI* é uma instituição sem fins lucrativos destinada a fornecer um padrão de certificação universal para administradores *Linux*. O *LPI* oferece certificações em três níveis: o *LPIC 1, LPIC 2 e LPIC 3*, porém nos interessa apenas os níveis 1 e 2, pois são os mínimos necessários para formar um administrador de redes. Cada certificação possui dois exames, sendo que cada exame custa US$ 200,00, resul-

tando em um custo total de US$ 800,00. Em valores de maio de 2018, seria equivalente a R$ 2939,60. (PRITCHARD et al., 2007, p. IX). Além do custo dos exames, poderíamos incluir o preço dos materiais necessários e cursos preparatórios para a certificação. Os livros consultados na *Amazon.com* variam entre R$ 68,00 e R$ 75,00, tanto para *LPIC* 1 quanto *LPIC* 2. Os cursos preparatórios para os exames de certificação possuem variações dependendo da empresa. O SENAC oferece curso preparatório presencial para o *LPIC 1*, que variam de R$ 744,10 a R$ 1519,00, e para o *LPIC 2*, que variam de R$ 1063,00 a R$ 1519,00, dependendo do local onde se deseja realizar o curso. (SENAC, 2018b). Já a empresa *Impacta* oferece cursos para *LPIC 1* com valor de R$ 1890,00, para os dois exames desse nível, e para *LPIC 2* com valor de R$ 1300,00 para o exame 201 e R$ 1219,00 para o exame 202. (IMPACTA, 2018).

5.1 Distribuição Debian

Utilizamos a distribuição *Debian*, pois ela é a distribuição definida pelo Plano de Migração para *Software* Livre do Exército Brasileiro.

O *Debian* vem sendo desenvolvido desde 1993, quando seu criador Ian Murdock lançou o manifesto *Debian*. Apresenta as principais ferramentas GNU para desenvolvimento de *software*, gerenciamento de arquivos, gerenciamento de redes, servidores de rede, etc. Dentre as principais vantagens do sistema *Debian*, podemos citar que é mantido pelos seus usuários, possui fácil instalação, possui pacotes bem integrados, código fonte aberto, gerenciamento de pacotes e atualizações de fácil utilização, rapidez e leveza do sistema (em comparação com outros disponíveis) e, uma das mais importantes características, não apresenta nenhum custo sob sua licença. (SPI, 2017).

Os requisitos de *hardware* para instalação do *Debian* são mais modestos que *Windows*, e variam de acordo com a aplicação do sistema. Em geral, uma máquina destinada a hospedar um servidor vai exigir um *hardware* mais potente, principalmente em memória RAM e processador. Mesmo um servidor de grande porte como de uma brigada em operação GLO, o servidor utilizando *Linux* exige muito menos que o *Windows*. Uma máquina contendo as seguintes configurações é possível suportar um servidor do porte necessário para uma Operação GLO a nível Brigada:

- Processador: Intel Xeon Quad-Core 2.5 GHz;
- Memória: de 16G a 32G;
- Disco rígido: 1 TB;

O *Debian* é destinado para usuários mais experientes, devido a sua principal desvantagem que é a pouca praticidade. “Muitos *hardwares* […] poderiam ser mais fáceis de configurar. Alguns *softwares* também poderiam utilizar um *script* que guiasse o usuário através da configuração (pelo menos para as configurações mais comuns)”. (SPI, 2017). Alguns *softwares* não possuem uma interface interativa com o usuário, e isso inclui configuração de serviços de rede, tornando o *Debian*, e demais distribuições *Linux* em geral, um sistema que apresenta uma resistência ao seu uso, por parte dos usuários iniciantes.

A falta de *softwares* comerciais espanta alguns usuários. De fato muitos *software* proprietários não estão disponíveis para a plataforma *Debian*, “Há, no entanto, programas que substituem a maioria deles, criados para imitar as melhores características dos programas proprietários, com o valor agregado de serem *softwares* livres.” (SPI, 2017). Apesar desse percalço, as ferramentas necessárias para o estabelecimento de infraestrutura básica de rede estão inclusas nos pacotes do *Debian.*

6. SERVIÇO *DHCP*

Já temos uma noção básica de *DHCP*, que fora abordada no item 2.3.3.1. Ao configurar um serviço *DHCP,* podemos fazer a interação dos equipamentos conectados à rede, ou seja, colocar todos eles para “falarem o mesmo idioma”, além disso definir os escopos que cada um terá, explica Seraggi. O *Dynamic Host Configuration Protocol* é um protocolo que fornece endereços IP e outras informações da rede para os computadores que se conectam a ela. Como o próprio nome diz, ele realiza configuração dinâmica, ou seja, uma configuração automática das informações necessárias para o computador se conectar à rede.

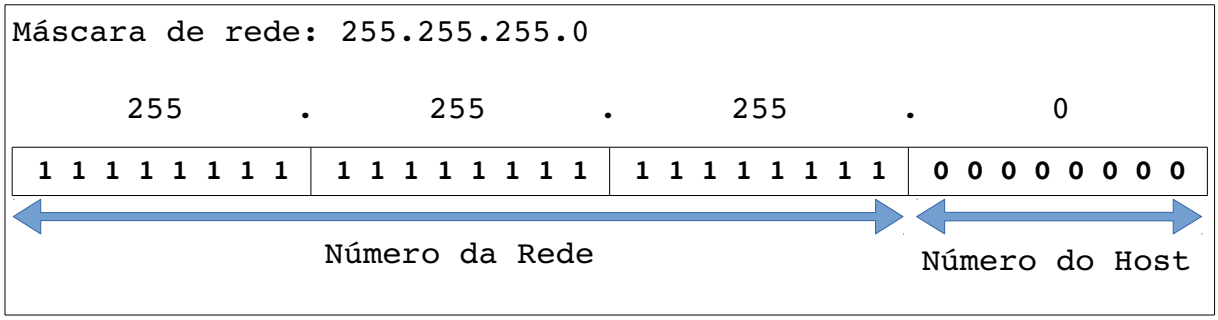
As principais informações fornecidas pelo *DHCP* são o endereço IP, aquele que vai identificar o computador na rede e através dele realizar o fluxo de informações dentro dela, já especificado no tópico *2.3.1.1*, o *gateway* padrão, máscara de sub-rede e o endereço do serviço *DNS*.

O *gateway* padrão é uma porta de entrada e saída da rede, a qual realiza a ligação de redes distintas, por exemplo a *internet*. Vamos entender melhor: Temos uma rede com os seus dispositivos conectados entre si e trocando informações. Todos esses dispositivos possuem um endereço IP que os identificam dentro daquela rede, porém são desconhecidos em uma rede externa. O *gateway*, que geralmente é um roteador, por sua vez realiza uma ligação entre essas duas redes e possui um endereço IP dentro da rede e outro fora dela, na *internet*. O endereço da rede interna é o chamado *gateway* padrão, pois é a porta de saída da rede. Os outros dispositivos que estão conectados à rede local tomam o IP do roteador para transmitirem e receberem informações de uma rede externa. Um exemplo prático é o seguinte: suponhamos que temos uma rede com quatro dispositivos conectados com os seguintes endereços IP: “192.168.0.1” para o dispositivo 1, “192.168.0.2” para o dispositivo 2, “192.168.0.3” para o dispositivo 3 e “192.168.0.4” para o dispositivo 4, sendo que o dispositivo 1 compartilha o acesso à *internet*. Os outros 3 dispositivos deverão ser configurados para que o IP “192.168.0.1” seja o *gateway* padrão da rede. (MORIMOTO, 2006, p. 57). Nesse contexto o *DHCP* é o responsável por fornecer essa configuração para os outros dispositivos.

Outra informação fornecida pelo *DHCP* é a máscara de sub-rede, requisito importante para separar a parte do endereço IP que define a rede e a parte que define o *host.* O octeto (números formados por 8 bits, separados por pontos que constituem o endereço IP) de uma máscara de sub-rede é formado por valores de 0 a 255, similar ao endereço IP. A diferença é que a parte do endereço da máscara constituída pelos *bits* “1” vai indicar o endereço da rede, e o restante ao endereço do *host*. A figura 4 ilustra como é feita essa divisão.

Esses endereços servem para “mascarar” o endereço IP, ou seja, através deles podemos saber qual octeto do endereço IP define a rede e qual octeto define o *host*. Exemplo prático: temos um endereço IP “192.168.1.100” e uma máscara “255.255.255.0”. A parte dos octetos representados pelo bit “1” da máscara referem-se aos octetos do IP do cliente que representam o endereço da rede, e o octeto representado pelo número “0” refere-se ao endereço do *host*, ou seja, os três primeiros octetos “192.168.100” do IP é o endereço da rede e o último octeto “100” é o *host.* Se tivéssemos uma máscara diferente, por exemplo “255.255.0.0”, esse IP pertenceria a uma rede diferente, e não “conversariam” entre si. Por isso é de suma importância que todos os dispositivos conectados à rede tenham a máscara de sub-rede configurada corretamente, para o seu bom funcionamento. (MORIMOTO, 2006, p. 56).

Figura 4 – Máscara de Sub-rede



Fonte: o autor.

Se a máscara fosse 255.255.224.0, o terceiro octeto dessa máscara seria formado pelos *bits* “1110000”. Os dois primeiros octetos mais os três primeiros *bits* do terceiro octeto seriam referentes ao endereço da rede, e os *bits* “0” seriam referentes ao endereço do *host.*

O *DHCP* também é responsável por fornecer o endereço dos servidores *DNS*, que já foi abordado no item 2.3.3.2 e será explanado mais detalhadamente à frente.

6.1 Como funciona o protocolo *DHCP*

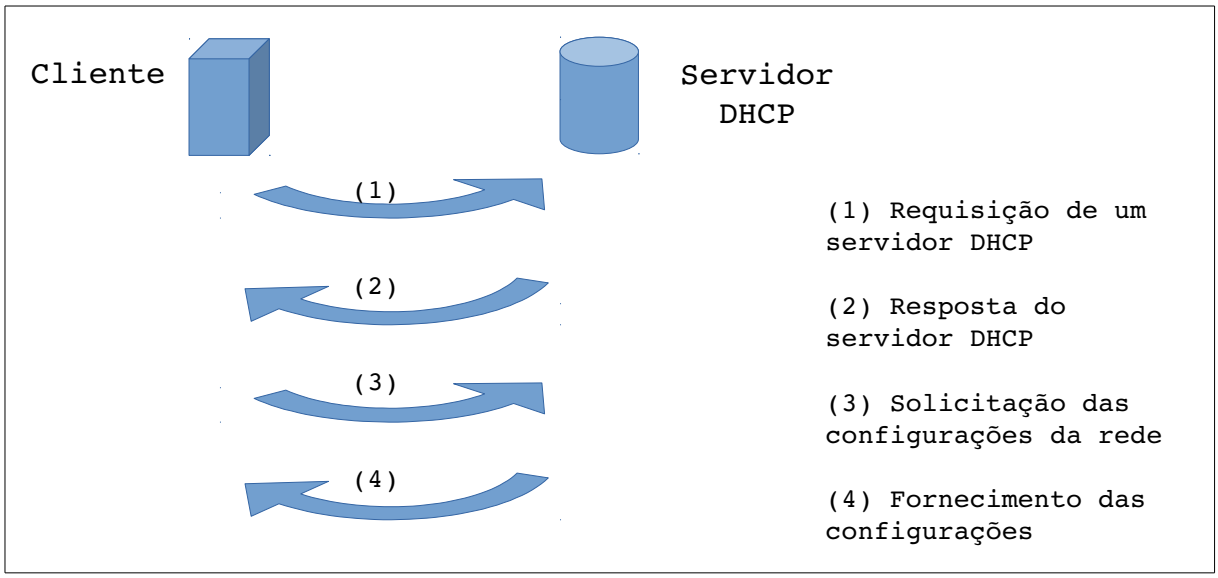
Sabemos quais são as principais funcionalidades do protocolo *DHCP*, mas como ele funciona dentro de uma rede? Nesse tópico, abordaremos sucintamente quais são os trâmites para que as informações da rede sejam fornecidas para os clientes conectados. O processo é dividido em 4 etapas: o momento em que o cliente faz a requisição de um servidor *DHCP*, a resposta do *DHCP*, a solicitação de um endereço IP válido e o fornecimento do IP ao cliente.

Um cliente conectado à rede é reconhecido através do seu endereço IP, porém, inicial-

mente, um dispositivo que se conecta a uma rede não possui esse endereço IP configurado, a menos que tenha sido configurado manualmente. Vamos levar em conta que não, pois é o cenário mais comum. Nesse momento, o servidor *DHCP* reconhece o dispositivo através do endereço *MAC*, que é particular de cada placa de rede, ou seja, um número específico e único daquele dispositivo.

Para obter as configurações da rede, o cliente envia um pacote destinado a todos os dispositivos de uma mesma rede, chamado de *broadcast*, a procura de um servidor *DHCP*. O servidor *DHCP*, ao receber esse pacote, responde ao cliente, através do endereço *MAC*, dizendo que está disponível e, após a resposta do *DHCP*, esse dispositivo solicitará as informações necessárias. O servidor consultará o seu banco de dados à procura de um IP válido que esteja disponível, e fornecê-lo ao cliente, além das demais configurações daquela rede.

Figura 5 – Requisição de um servidor DHCP



Fonte: O autor.

Os endereços IP fornecidos pelo *DHCP* ficam reservados por um determinado período de tempo para todos os clientes que requisitarem. De tempo em tempo, antes do esgotamento do tempo reservado, o cliente faz uma solicitação de renovação daquele endereço IP. Assim, aquele IP fica marcado no banco de dados do *DHCP* que permanecerá locado por mais um ciclo de tempo. Caso o tempo de reserva do IP se esgote, o servidor *DHCP* entenderá que aquele IP está disponível e poderá fornecê-lo a outro cliente que se conecte a rede posteriormente. Esse processo de renovação evita todo o processo anterior de requisição de IP e melhora o gerenciamento dos IPs disponíveis no banco de dados do servidor.

6.2 Servidor *DHCP* no *Windows Server 2012 R2*

Para instalar e configurar o *DHCP* no *Windows Server* 2012 R2, é necessária uma série de passos através da própria interface gráfica do *Windows*. Em seu livro, Seraggi divide a instalação em 16 passos simples. Inicialmente o usuário precisa acessar o Gerenciador do Servidor o qual o direcionará para o Assistente de Adição de Funções e Recursos. O assistente é um recurso que norteia o usuário durante a instalação das diversas aplicações. O usuário deve seguir os passos, os quais explicam basicamente o que o assistente faz, clicando em "próximo" até a janela perguntar qual serviço deseja instalar. Nessa janela, são listadas todas as funções possíveis de instalação utilizando esse assistente. Nesse ponto, o usuário deve selecionar o Servidor *DHCP* e prosseguir. A próxima janela explica sucintamente o que é o *DHCP* e o que será feito durante a instalação. Após confirmar a instalação, a janela a seguir mostrará o progresso da instalação das ferramentas do *DHCP* através de uma barra. Após a conclusão da instalação, um *link* de configuração será apresentado ao usuário onde ele deve clicar, para definir os números de IP que o servidor deverá fornecer para os dispositivos que se conectarem a rede, o tempo de concessão dos endereços e, por fim, ativar o servidor.

O serviço *DHCP* já é um serviço incluso no pacote de aplicativos do *Windows Server 2012 R2*, por isso não existe custo específico para sua aquisição, se não a própria licença do *Windows Server 2012 R2*.

Feitas a instalação e a configuração, basta apenas configurar as máquinas clientes para obter as informações automaticamente através do servidor *DHCP.*

6.3 Servidor *DHCP* no *Debian*

O servidor *DHCP* do *Debian* difere-se na sua instalação e configuração. Como visto no capítulo 5, referente ao *Linux* e à distribuição *Debian*, as configurações dos aplicativos nesse sistema são realizadas através de comandos via terminal. A fim de economia de recursos da máquina (processador, memória e espaço de disco), é desejável que não se utilize a interface gráfica, sendo necessário ao operador ser um bom entendedor do sistema para realizar a configuração de maneira correta.

Inicialmente o pacote *DHCP* deve ser instalado utilizando um comando de gerenciamento de pacotes. O gerenciador de pacotes é uma ferramenta do sistema *Linux* para aquisição e manipulação, seja para instalar ou apagar pacotes de aplicativos, realizando o *download* e a instalação automaticamente. Depois de instalada a aplicação, fica a cargo do

operador apenas a configuração dos parâmetros necessários para o funcionamento do servidor na rede. A configuração desses parâmetros é feita em um arquivo de texto o qual é possível alterar as variáveis do servidor *DHCP* da maneira como a situação exigir. O Anexo 1 – dhcpd.conf mostra um arquivo de configuração do servidor *DHCP.*

Nesse arquivo de texto são inseridos os parâmetros da rede que serão fornecidos pelo *DHCP* aos clientes que se conectarem à rede. São eles o endereço da rede, os endereços dos servidores *DNS*, a máscara de rede, o intervalo de endereços IP que serão disponibilizados, o endereço do *gateway* e o endereço *Broadcast*, tudo feito em linhas de códigos, pouco intuitivas. Por isso é exigido de seu operador um nível elevado de conhecimento a cerca do sistema e do protocolo em questão.

No *Linux*, ainda é necessário realizar a instalação do *DHCP Client*. O download e a instalação é realizada através do gerenciador de pacotes e a sua configuração padrão gerada durante a instalação já é suficiente para o funcionamento do cliente na rede.

7. SERVIÇO *DNS*

O serviço *DNS*, como já sabemos é aquele responsável por traduzir os nomes em endereços IP e vice-versa e é uma das ferramentas mais importantes para o funcionamento de uma rede. Aqui vamos entender melhor o seu funcionamento e sua aplicação nos dois sistemas operacionais estudados.

Nos primórdios da *internet*, quando não existiam muitos servidores, cada estação de trabalho possuía dentro de seus arquivos de configuração uma lista de *host names*, basicamente um banco de dados com todos os nomes e os IPs correspondentes aos nomes dos servidores. Sempre que houvesse uma atualização de um servidor ou a implementação de um novo, esse arquivo tinha que ser distribuído para os demais servidores. Com o crescimento da *internet*, isso deixou de ser viável e necessitou de uma criação de um serviço que centralizasse esses "nomes" e realizasse esse serviço de maneira distribuída. Sabemos que a *internet* é baseada em endereços IP e quando acessamos um *site* através da sua *URL*, por exemplo "http://www.aman.eb.mil.br/", não estamos acessando o endereço, mas sim o IP que representa esse endereço. O serviço responsável por essa tradução é o *DNS*.

O professor Paulo Kretcheu, em seu vídeo blog no *youtube*, utiliza uma analogia com uma lista telefônica. Por exemplo: suponhamos que você queria ligar para uma pessoa que mora em uma cidade de um determinado estado em um determinado país. Ao discar para a telefonista, você solicitará o telefone dessa pessoa. A telefonista, por sua vez, solicitará o telefone para a central do país, que solicitará para central do estado que solicitará para a central da cidade e assim terá o telefone da pessoa. (KRETCHEU, 2012).

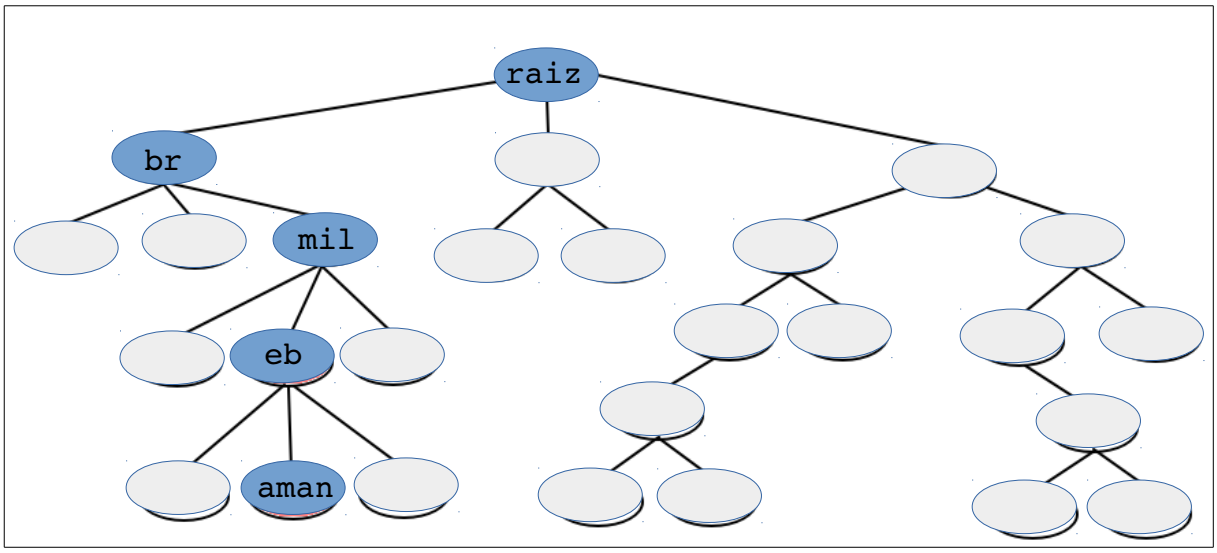
Essa distribuição é feita de maneira hierárquica. Seria inviável concentrar todos os endereços em um único servidor, devido ao tamanho da *internet*, por isso há uma distribuição em níveis hierárquicos de servidores *DNS*. É possível reparar na estrutura de um endereço de um *site*. Ele é formado por nomes separados por pontos (“.”). Esses pontos são os que separam os domínios dos servidores.

Existe um servidor chamado de servidor raiz, que está no topo da cadeia hierárquica dos servidores *DNS*. Esse servidor conhece todos os outros servidores abaixo dele, que são os *Top-Level Domain (TLD)*, ou Domínio de Alto Nível. Como exemplo de domínio de alto nível estão os pontos “.”. Através desses domínios é que serão indicados os outros domínios, como “.br”, “.com”, “.org”, etc. A partir desses domínios de alto nível é possível acessar todos os outros domínios, que possuem os seus servidores *DNS*, e hospedam os diversos serviços da *internet*. O endereço final de um domínio na árvore hierárquica do *DNS* é chamado de *Full*

Qualified Domain Name (*FQDN*).

Utilizando o exemplo do endereço da AMAN: ao acessar “http://www.aman.eb.mil.br/”, o domínio “br” solicita o endereço *IP* para o domínio “mil” que por sua vez solicita para o domínio “eb” e assim obtém o endereço do domínio “aman”, que por último informa o IP relativo ao *FQDN* do *site* da AMAN. Por isso, esse serviço tem essa característica de ser distribuído. Um ponto interessante de se analisar é caso o domínio da AMAN tenha um *FQDN* modificado, apontando para outro IP, ou um novo *FQDN*, não será necessário o domínio “br” saber disso, pois ele apenas redireciona a solicitação para “mil” que redireciona para “eb” que redireciona para “aman”.

Figura 6 – Árvore hierárquica de domínios



Fonte: O autor.

Os servidores que respondem por determinados domínios são chamados de *DNS* autoritativos, pois eles possuem autoridade sobre aqueles domínios.

7.1 Servidor *DNS* no *Windows Server 2012 R2*

A configuração do *DNS* no *Windows Server 2012 R2* segue a mesma lógica do *DHCP*. São realizados passos simples autoexplicativos pela interface gráfica do Gerenciador do Servidor do *Windows Server 2012 R2*.

Basicamente o usuário deve acessar o Assistente de Adição de Funções e Recursos similiar ao explicado durante a instalação do *DHCP*, no tópico 6.2, porém selecionar o serviço *DNS*. A partir daí, basta apenas seguir as instruções do instalador.

Não há nenhum complicador na instalação e configuração. O serviço *DNS* do *Windows Server 2012 R2* já é incluso no pacote de sua licença e não necessita de gastos adicionais para incrementar esse recurso na rede.

7.2 Servidor *DNS* no *Debian*

O servidor *DNS* no *Linux* é baixado e instalado utilizando o gerenciador de pacotes, similar ao processo executado para instalação do servidor *DHCP*, alterando apenas o nome do pacote instalado.

O serviço *DNS* no *Debian* é fornecido pelo pacote *Bind9*. Os arquivos de configuração do *Bind*, assim como o *DHCP*, e a maioria de outros aplicativos, são feitos em arquivos de texto com instruções e parâmeros nas linhas de código do arquivo-texto. Novamente, a grande diferença entre os serviços fornecidos pelo *Windows* e *Linux* está na interface gráfica. Durante as configurações do servidor, é muito importante observar as pontuações e regras de programação utilizada nos arquivos-texto de configuração. Qualquer pontuação ao espaço errado compromete todo o serviço.

8. SERVIÇO DE AUTENTICAÇÃO

O sistema de autenticação está diretamente ligado com o conceito de segurança na rede. Autenticação significa confirmar a veracidade, ou tornar algo autêntico. Esse tipo de sistema possui alguns tipos de funcionamento, e podem estar presentes juntos ou isolados. Alguns exemplos são: *Login* e senha, esse são os mais comuns, o qual o usuário define um nome e uma senha que serão necessários para utilização de algum serviço; *CAPTCHA (Completely Automated Public Turing test to tell Computers and Humans Apart),* que é uma confirmação de usuário humano, algo que uma máquina não conseguiria definir, geralmente uma imagem ou uma sequência de algarismos levemente distorcidos; impressão digital, muito comum em bancos; entre outros. Através de um servidor de autenticação é possível definir os usuários que terão acesso à rede e ainda definir os níveis e permissões de cada usuário, qual a amplitude de acesso que um usuário pode ter, quais domínios são bloqueados.

Para entendermos a importância desse serviço é preciso entender os conceitos mais básicos de uma rede, como a sua constituição física. Uma rede cabeada é mais simples de gerenciar. Nela, os acessos por outros dispositivos são limitados pela necessidade do cabo e pelo alcance que eles possuem. A partir do momento que substituímos os cabos pelas redes *wireless* (do inglês literal “sem fio”), alguns aspectos começam a ser suprimidos, como o custo, e outros tomam um grau maior de relevância, como é o caso da segurança.

Em uma rede sem fio, o sinal é espalhado no espectro eletromagnético e a rede fica visível para todos que estiverem dentro de seu alcance. Alguém que possua um receptor *wireless* consegue se conectar à rede. Portanto, o controle de permissões de usuários na rede se torna importante para a sua segurança e esse controle é feito através de senha. Depois o acesso aos serviços da rede podem ser controlados pelo serviço de autenticação.

Visando diminuir todas as possibilidades de invasão, os serviços de autenticação são implementados nas redes, para garantir o mínimo de segurança possível.

8.1 *Active Directory – Windows Server 2012 R2*

No *Windows*, o aplicativo encarregado de realizar esse serviço é o *Active Directory* (*AD*). O *AD* foi desenvolvido na versão *Windows Server* 2000 e é uma ferramenta utilizada para armazenamento de informações dos usuários e elementos da rede em um único lugar, funcionando como um controlador de domínios. Em vez de cada usuário ter uma senha diferente para acessar cada serviço da rede, ele concentra em apenas uma senha para o usuário ter

acesso a todos os recursos da rede, sendo que essas informações ficam retidas em um banco de dados. (SERAGGI, 2015, p. 195).

Sua instalação é semelhante a qualquer outra instalação dos serviços já apresentados, através do Gerenciador do Servidor do *Windows Server 2012 R2*. Feita a instalação, basta configurar. O AD apresenta ao usuário a *Active Directory Administrative Center*, que significa Central Administradora do AD. “Por meio dela conseguimos criar usuários, inserir computadores, acessar servidores de outras redes e fazer várias tarefas administrativas.” (SERAGGI, 2015, p. 210). O AD utiliza o protocolo *LDAP* para realizar o gerenciamento das informações.

> *LDAP* é um protocolo que ajuda o administrador a fazer uma pesquisa com critérios definidos por ele, utilizando mecanismos e métodos para armazenamento dessas pesquisas.
> *LDAP* significa *Lightweight Directory Access Protocol* (em português, protocolo leve de acesso a diretórios), que em resumo é um protocolo que consegue acessar informações centralizadas em uma rede. (SERAGGI, 2015, p. 212)

O AD permite criar usuários, grupos de usuários e fornecer permissões para os grupos. É possível implementar uma ferramenta chamada GPO, que significa Group Policy Object, ou Objeto de Políticas de Grupo, que é uma infraestrutura hierárquica responsável por estabelecer regras para a permissão de alterações nos objetos da rede (usuários, grupos, diretórios, computadores, etc.), que inibe significativamente riscos à segurança da rede. (SERAGGI, 2015, p. 251)

8.2 Autenticação de usuários no *Debian*

Uma das opções para o serviço de autenticação de usuários nos servidores *Linux* é o *Samba*. O servidor *Samba* inicialmente foi desenvolvido para que servidores *Unix* e *Windows* se comunicassem, e teve o seu início em 1992. Devido o sucesso de projeto, hoje o *SAMBA* possui diversos recursos para gerenciamento de rede, garantindo um controle mais rigoroso de acesso de usuários e serviços de diretórios. Dentre as características do *SAMBA*, o que importa para o nosso trabalho são as possibilidades de controle de acesso. (DA SILVA, 2010, p. 301)

> Com o SAMBA, é possível construir domínios completos, fazer controle de acesso a nível de usuário, compartilhamento, montar um servidor WINS, servidor de domínio, impressão, etc. Na maioria dos casos o controle de acesso e exibição de diretórios no samba é mais minucioso e personalizável que no próprio Windows. (DA SILVA, 2010, p. 299)

Hoje, o *SAMBA* é um AD completo, podendo ser realizadas todas as atividades que o

AD proporciona. Com ele é possível controlar o acesso para usuários autenticados, com uso de um banco de dados de senha do sistema e autenticação dos usuários através do protocolo *LDAP.* Para instalação dos pacotes, basta executar os comandos necessários no terminal para *download* e logo depois a configuração.

9. ANÁLISE DOS RESULTADOS

Diante dos resultados encontrados, podemos fazer algumas observações. A resposta para o problema não parece ser tão evidente se analisarmos as variáveis como um todo, visto a aparente igualdade de vantagens e desvantagens entre os dois sistemas operacionais estudados, porém se observamos cada aspecto isolado vamos perceber que alguns possuem mais relevância e peso que outros.

Vamos destacar a seguir, isoladamente, cada um dos quesitos levantados durante o estudo. São eles o custo, a facilidade de implementação e flexibilidade. Em questão de funcionamento, em geral, ambos os sistemas demonstram certa igualdade. Tanto *Windows* quanto o *Linux* são os sistemas operacionais famosos e são amplamente utilizados em servidores e estão em desenvolvimento a bastante tempo.

9.1 Custos

Os custos em geral dos sistemas operacionais demonstraram ser uma das maiores diferenças entre eles. Eles não se resumem apenas em licença, mas outras condições afetam diretamente no preço entre eles. Podemos destacar os seguintes aspectos: O custo de licença, o custo do *hardware* necessário para instalação, configuração e operação e o custo da capacitação de usuários.

Para atender o princípio da continuidade das Operações GLO, devemos raciocinar sempre com elementos redundantes para a reserva. Isso quer dizer que o *hardware* do servidor, bem como os próprios usuários encarregados de sua gerência, devem ser multiplicados. Temos que ter em mente que um servidor pode apresentar defeitos, por qualquer tipo de pane, assim como os gerentes da rede podem sofrer baixas ou indisponibilidade por algum motivo adverso. Portanto, os gastos devem ser calculados visando atender essa necessidade.

O número de estações a ser atendido pela rede de computadores de uma brigada em Operação GLO foi calculado de acordo com o explicitado no capítulo 3. O EM de uma brigada demanda pelo menos 24 estações. O EM dos elementos de manobra, que geralmente são 4, demandam 12 estações cada, e cada pelotão demanda 1 estação. Portanto, cada unidade de manobra necessitará de pelo menos 15 estações. Para o B Log, foi calculado a quantidade de 22 estações para realizar sua tarefa de apoio. Logo, o total de estações de uma brigada são pelo menos 106 estações. O preço das estações não foi considerado, pois o objeto de estudo foi apenas os servidores e a rede de computadores, não levando em consideração os sistemas

operacionais dos terminais de trabalho. Ainda que fossem calculados, a diferença de preço seria pequena se comparada com a diferença existente entre os preços do servidor para o *Windows* e o *Linux.* Vale ressaltar que para utilização dos serviços da rede, não é necessário que os sistemas operacionais da rede e dos clientes sejam os mesmos. Uma rede implementada em *Linux*, pode fornecer os seus serviços para clientes *Windows* e vice-versa.

9.1.1 Custo de licença

O *Windows Server 2012 R2* é um *software* proprietário enquanto a distribuição *Debian* do *Linux* é livre. Todos os pacotes e utilitários necessários para a implementação de infraestrutura básica de rede, incluindo o *DHCP, DNS* e o serviço de autenticação, no *Debian* são fornecidos gratuitamente. Não é necessário nenhum gasto com qualquer tipo licença.

Em contrapartida, o *Windows Server 2012 R2* necessita de licença para utilização. A licença intermediária, da versão *Standard Edition*, custa 882 dólares. Em valores atuais, de maio de 2018, é equivalente à R$ 3000,45. Dependendo da quantidade de núcleos de processadores utilizados no servidor, esse preço pode se multiplicar, devido ao fato que cada núcleo necessita de uma licença. Se tratando de uma rede que atende uma Brigada em Operação GLO, o servidor utilizaria um *hardware* com mais núcleos no processador, para atender a demanda de recursos exigidos pelos elementos subordinados, fazendo assim a necessidade de mais licenças.

Além desse custo, são necessárias as licenças *CAL*, que custam em média 100 reais cada. Para atender a demanda da brigada, que foi calculada em 106 terminais, o dispêndio com o *Windows Server 2012 R2* seria de 10600 reais, enquanto no *Debian* esse custo seria zero.

É preciso ressaltar que, apesar dos custos referentes às estações de trabalho não serem levados em consideração, para as estações de trabalho *Windows* se conectarem em uma rede implementada com servidor *Windows Server*, há um custo de licença para conexão de rede, que não será tratado neste trabalho, mas que encareceriam ainda mais os custos de licença.

9.1.2 Custo hardware necessário para instalação, configuração e operação

No que diz respeito ao custo do *hardware* necessário para a utilização do sistema operacional, não observamos uma discrepância no valor como no preço da licença, embora tenha uma diferença relevante. O *hardware* necessário para instalação e utilização do *Windows*

Server 2012 R2 é mais potente que um *hardware* exigido pelo *Debian.* Apesar de o *Debian* funcionar com um servidor menos potente, vale ressaltar que quanto mais um servidor apresentar configurações elevadas melhor será o seu desempenho.

O servidor sugerido no capítulo 4, possuí valor aproximado de 14 mil reais, sem levar em conta os periféricos, como o *hack, mouse*, teclado, monitor, cabos e outros elementos de rede que são comuns a qualquer sistema. A configuração sugerida no capítulo 5.1, referente ao *Debian*, possuí valor aproximado de 8500 reais. O valor total, calculando a redundância dos meios, seria de 28 mil para *Windows* e 17 mil para *Debian.*

9.1.3 Custo de capacitação de usuários

O gerenciamento de uma rede não é tarefa fácil. Configurar e manter os sistemas funcionando demandam enorme conhecimento de rede, de serviços e do sistema. A capacitação de usuário para gerência de redes de computadores não difere muito quando comparamos diferentes sistemas operacionais a serem utilizados. Espera-se de um profissional da área um conhecimento amplo que inclui diversas possibilidades, inclusive o uso de diferentes sistemas. Não é desejável formar um profissional refém de uma única opção. Apesar de encontrarmos cursos específicos para cada sistema operacional, eles possuem relacionamento estreito.

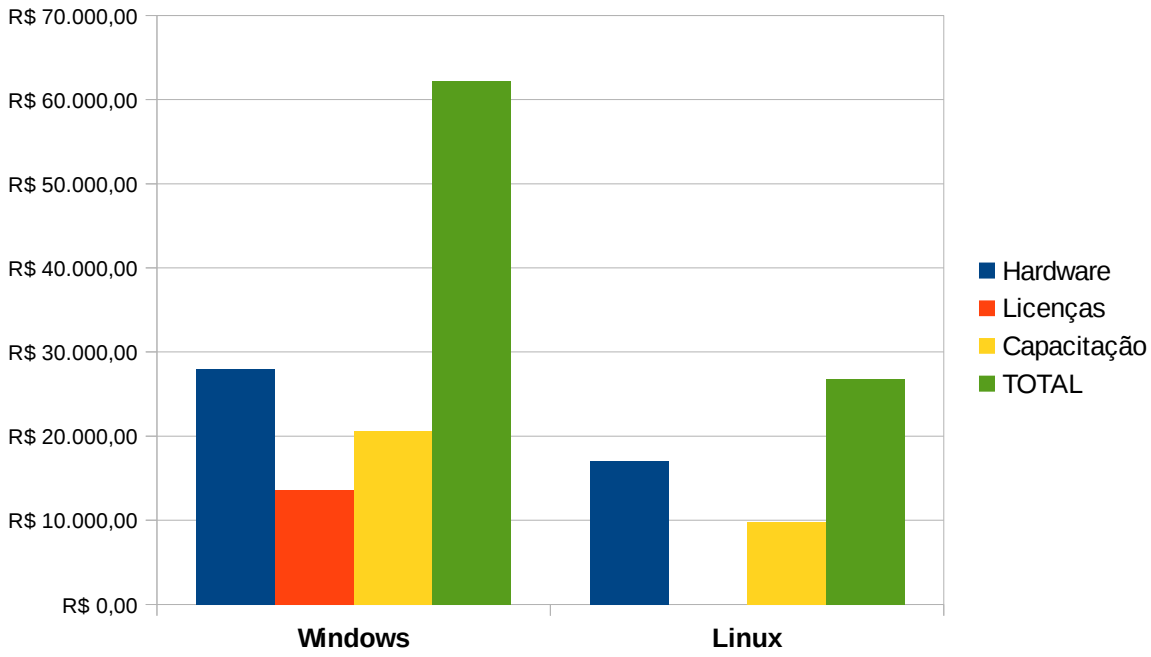
O que pode influenciar durante a capacitação do usuário é justamente a facilidade que o sistema apresenta. O *Linux* é um sistema bem mais complexo de se utilizar e a capacitação do usuário demanda um esforço por parte dele. Contudo, não devemos nos enganar que o sistema *Windows* é algo que se aprende rápido. Um gestor de rede requer conhecimentos muito mais profundos do que simplesmente o funcionamento do sistema operacional ou a utilização de aplicativos de um *desktop*. Questões como estudos avançados de rede e programação são elementos obrigatórios no currículo de um profissional da área.

Entre as opções para a capacitação em cada sistema, encontramos uma diferença nos preços. Os exames para certificação *LPIC* 1 e 2 são mais baratos que os exames da *Microsoft*, para *MCSA* e *MCSE.* A diferença se estende inclusive nos cursos preparatórios e apostilas sobre o assunto. Se optarmos pelas opções mais baratas, a formação de um especialista certificado pela *Microsoft,* com *MSCA* e *MCSE*, sairia na faixa de R$ 10300,00, incluindo os cursos preparatórios, material de consulta e as taxas dos exames. A certificação *LPIC* 1 e 2 sairia na faixa de R$ 4876,00, incluindo os cursos preparatórios, material e exames.

A Figura 7 nos traz uma compilação de todos os dados colhidos acerca dos custos dos sistemas operacionais. Ao todo, foi observado um gasto total de R$ 6200,00 para implemen-

tação da rede utilizando o sistema operacional da *Microsoft*, enquanto a distribuição *Debian* demanda um gasto de R$ 26752,00.

Figura 7 – Gráfico comparativo de preços



Fonte: o autor.

9.2 Facilidade de implementação

A facilidade de implementação foi a única grande vantagem apresentada pelo *Windows Server 2012 R2*, mas trata-se de um atributo subjetivo. Pela característica histórica da interface gráfica do *Windows*, que resultou na popularização do sistema operacional em questão, a sua configuração e manipulação fica facilitada. Porém, os recursos gráficos disponibilizados consomem muitos recursos da máquina, prejudicando o desempenho e exigindo mais poder de processamento o que onera os custos com o *hardware*.

A interface gráfica é apenas um facilitador. O usuário que opta por utilizá-la, além da desvantagem citada acima, se torna refém das limitações de processo que ela oferece. Isso quer dizer que, o terminal, onde executamos os comandos, oferece uma gama de possibilidades, pois elas não sofrem a limitação de serem acessadas somente quando estão visíveis. Esse é um dos motivos pela qual a *Microsoft* oferece a opção de configuração dos serviços pelo *Power Shell*.

Contudo, Gerenciador do Servidor do *Windows Server 2012 R2* mostrou uma ferra-

menta extremamente útil e fácil de usar durante as instalações dos serviços. Isso também é observado durante a configuração dos serviços para atender as requisições das operações GLO.

9.3 Flexibilidade

No quesito flexibilidade, pouca conclusão se pode tirar. Devido à característica do PC da Brigada em uma operação GLO, não é possível dizer realmente se um sistema apresenta vantagem sobre outro em questões de mobilidade do PC. Diante desse resultado, a comparação a respeito da flexibilidade do sistema pode ser suprimida. Vale ressaltar que esse quesito tem um relacionamento com a facilidade de implementação e manipulação do sistema. Com todos os sistemas instalados no servidor, a máquina, ao ser desligada, conserva todas as suas configurações no seu HD.

Nos sistemas *Linux*, as configurações das aplicações são salvas em arquivos de configurações, que são semelhantes a arquivos-texto, como mostro o Anexo 1. Caso seja necessário uma mobilização, bastaria apenas salvar os arquivos de configuração em *backup*, e reutilizá-los em outro servidor. No *Windows*, em caso de mudança do servidor físico, seria necessário novamente configurar todos os serviços. Apesar das características da Operação suprir esse aspecto, em uma outra situação a flexibilidade do sistema Linux apresentaria melhor desempenho.

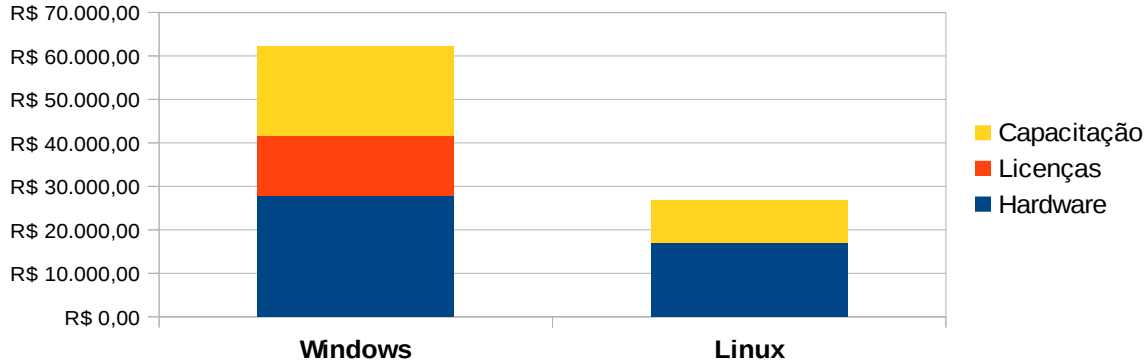
10. CONCLUSÃO

Nossa pesquisa teve como objetivo definir qual sistema operacional entre *Windows Server 2012 R2* e o *Debian* se ajusta melhor para o estabelecimento de uma rede básica no contexto de uma Operação GLO. Procuramos entender o funcionamento dos principais serviços de rede e as características de cada um nos dois sistemas operacionais para confirmar a nossa hipótese. Os principais fatores levados em consideração durante a análise dos resultados foram o custo de uma maneira geral dos sistemas, a facilidade de implementação e configuração, e flexibilidade durante as operações. Apesar de o sistema da *Microsoft* apresentar vantagem sobre o *Debian* quando tratamos da facilidade de implementação, vale ressaltar que o fator custo possui peso elevado por dois motivos:

O primeiro motivo é o fato de ser o parâmetro de comparação com maior disparidade entre os 2 sistemas. Tanto o sistema *Windows* quando o *Debian* possuem funcionamento satisfatório em qualquer ambiente, porém a diferença de preço total entre os dois possui uma amplitude muito grande.

O segundo motivo se dá pelo fato da conjuntura econômica atual do nosso país. O Brasil vem passando nos últimos anos por restrições orçamentárias que impactam as diversas instituições federais, inclusive o Exército Brasileiro. A situação econômica atual combinada com algumas medidas do governo como aprovação da Emenda Constitucional n.º 95, de 2016, que regula os gastos públicos, geram um cenário de limitações e tudo isso afeta o Exército. Economizar recursos e ainda assim utilizar meios que suprem as necessidades se torna imposição durante a tomada de decisão.

Figura 8 – Tabela resumo



	Hardware	Licenças	Capacitação	Total
Windows	R$ 28.000,00	R$ 13.600,00	R$ 20.600,00	R$ 62.200,00
Linux	R$ 17.000,00	R$ 0,00	R$ 9.752,00	R$ 26.752,00

Fonte: o autor.

Nesse aspecto, o *Linux* obteve vantagem absoluta sobre o sistema da *Microsoft*. Todos os quesitos apresentam resultados favoráveis para a sua escolha. No custo de licença, o *Linux* não apresenta nenhum gasto, o *hardware* necessário para suportar um servidor é mais simples e os gastos para capacitação de usuários também é inferior. É possível notar que a diferença de preço entre os dois sistemas é mais que o dobro, como mostra a figura 8. Somente o preço do *hardware* de um servidor *Windows* pagaria toda despesa necessária para implementar um servidor *Linux.*

Uma pesquisa realizada pela FGV, em 2016, chegou a conclusão que “apenas 22% dos *servers* nacionais são equipados com *Linux* […] enquanto o SO da *Microsoft* já ocupa uma fatia de 72%”. Porém esse cenário já foi diferente. Até 2010 os sistemas *Linux* ocupavam uma fatia de 40% dos servidores. (DE SOUZA, 2016). Esses números podem ser explicados pelas constantes atualizações que a *Microsoft* realiza com seus sistemas operacionais e, por se tratar de uma empresa privada de *softwares* proprietários com venda de licenças, ela possui obrigação de prestar suporte técnico. Para esse suporte ser efetivado, todos os servidores precisam estar cadastrados, o que facilita a contagem desses equipamentos. Já o *Linux* possui um suporte técnico mais “informal”, não é garantido pelos desenvolvedores e muitas vezes é preciso pagar avulso por esse suporte. Poucas distribuições, como é o caso da *Red Hat* e *Novell Suse*, possuem suporte pago. Demais distribuições não possuem registros, por isso ficam de fora das estatísticas, pois não podem ser computadas.

Por esse motivo, o sistema da *Microsoft* transmite uma confiança a mais para o cliente que deseja implementar uma rede em sua empresa. Contudo, diversos autores da área de TI colocam o sistema *Linux* à frente do *Windows* se tratando de servidores. Questões relevantes como estabilidade, segurança, *hardware* utilizado e a liberdade de operação, visto que o *Linux* possui código aberto, além do custo total de operação, alavancam o *Linux* a posição de destaque nessa comparação (NOYES, 2010).

Diante destes resultados e respondendo a hipótese desta pesquisa, podemos afirmar que o sistema *Linux* se mostra o mais adequado para a implementação de uma rede de computadores em Operações GLO. Se comparados com o que encontramos na teoria que sustentou a pesquisa, podemos concluir que as vantagens do *Linux* sobrepõe às do *Windows* e o colocam em primeiro lugar durante a escolha do sistema operacional ideal para uma rede de uma brigada em Operações GLO.

11. REFERÊNCIAS

BRASIL. Ministério da Defesa. **C 7-30**: Brigadas de Infantaria. 1. ed. Brasília: EGGCF, 1984a.

_____. Ministério da Defesa. **C 29-15**: Batalhão Logístico. 1. ed. Brasília: EGGCF, 1984b.

_____. Ministério da Defesa. **C 11-1**: Emprego das Comunicações. 2. ed. Brasília: EGGCF, 1997.

_____. Lei Complementar no 97, de 9 de junho de 1999. **Diário Oficial [da] República Federativa do Brasil**, Poder Executivo, Brasília, DF, 10 jun. 1999. Disponível em: <https://www.planalto.gov.br/ccivil_03/leis/lcp/lcp97.htm>. Acesso em: 30 set 2017.

_____. Decreto no 3.897, de 24 de agosto 2001. **Diário Oficial [da] República Federativa do Brasil**, Poder Executivo, Brasília, DF, 27 ago. 2001. Seção 1, p. 66 Disponível em: <http://www.planalto.gov.br/ccivil_03/decreto/2001/d3897.htm>. Acesso em: 25 fev 2018.

_____. Ministério da Defesa. **C 7-20**: Batalhões de Infantaria. 3. ed. Brasília: EGGCF, 2003.

_____. Constituição (1988). Constituição da República Federativa do Brasil. 17. ed. São Paulo: Rideel, 2013.

_____. Ministério da Defesa. **MD33-M-10**: Garantia da Lei e da Ordem. 1. ed. Brasília: EGGCF, 2013.

COMER, D. E. **Interligação de redes com TCP/IP**. Rio de Janeiro: Elsevier, 2006.

DA SILVA, Gleydson Mazioli. **Guia Foca GNU/Linux.** Disponível em: <http://www.guiafoca.org/?page_id=14>. Acesso em: 30 set 2017.

DE SOUZA, Ramon. **No Brasil, Linux perde para Windows até mesmo no uso em servidores**. 18 abr. 2016. Disponível em: <https://www.tecmundo.com.br/linux/103797-brasil-linux-perde-windows-mesmo-para-uso-servidores.htm> Acesso em: 21 maio 2018.

ENTENDA como funciona a operação de Garantia da Lei e da Ordem. **Portal do Planalto**, 24 maio 2017. Disponível em: <http://www2.planalto.gov.br/acompanhe-planalto/noticias/2017/05/entenda-como-funciona-a-operacao-de-garantia-da-lei-e-da-ordem/@@nitf_custom_galleria>. Acesso em: 25 fev. 2018.

GERHARDT, Tatiana Engel; SILVEIRA, Denise Tolfo. **Métodos de Pesquisa.** Porto Alegre: Editora da UFRGS, 2009.

IMPACTA. **Conheça os cursos de redes**. 2018. Disponível em: <https://www.impacta.com.br/escola/Redes>. Acesso em: 26 maio. 2018.

KRETCHEU, Paulo. **DNS - Domain Name System.** 2012 (20m10s). Disponível em: <https://www.youtube.com/watch?v=i4KMcl0tuEg>. Acesso em: 21 abr. 18.

KÖCHE, J. C. **Fundamentos de metodologia científica:** teoria e prática da pesquisa. Petrópolis: Vozes, 1997.

LANZA, Giuseppe Francisco. **Conceitos Básicos de Rede**. Apostilando.com, 2007. Apostila.

MAZIERO, Carlos A. **Sistemas Operacionais:** Conceitos e Mecanismos. Curitiba: DINF – UFPR, 2017.

MICROSOFT. **MCSA: Windows Server 2012**. 2018. Disponível em: <https://www.microsoft.com/pt-br/learning/mcsa-windows-server-certification.aspx>. Acesso em: 26 maio. 2018.

MORIMOTO, Carlos E. **Linux Entendendo o Sistema:** Guia prático. Sul Editores, 2006.

NOYES, Katherine. **Cinco motivos que colocam o Linux à frente do Windows em servidores**. 31 ago. 2010. Disponível em: <http://idgnow.com.br/ti-corporativa/2010/08/31/cinco-motivos-que-colocam-o-linux-a-frente-do-windows-em-servidores/> Acesso em: 21 maio 2018.
SERAGGI, Márcio Roberto. **Windows Server 2012 R2**. 1. ed. São Paulo: Senac. 2015

PRITCHARD, Steven et al. **Certificação Linux LPI – Nível 2: Exames 201 e 202**. 1. ed. Rio de Janeiro: Alta Books Ltda. 2007

RIOS, Renan Osório. **Protocolos e Serviços de Redes**. Colatina: CEAD/Ifes, 2011.

TANENBAUM, Andrew Stuart. **Sistemas operacionais modernos.** 3. ed. São Paulo: Pearson, 2009.

SENAC. **Cursos Livres Senac**: Certificação Linux LPI Nível 1 - LPIC1. 2018a. Disponível em: <http://www.sp.senac.br/portfolio/default.jsp?newsID=DYNAMIC,oracle.br.dataservers.-CourseDataServer,selectCourse&course=21068&template=395.dwt&unit=NONE&testeira=473>. Acesso em: 26 maio. 2018.

SENAC. **Cursos Livres Senac**: Formação MCSA - Windows Server 2012. 2018b. Disponível em: <http://www.sp.senac.br/jsp/default.jsp?newsID=DYNAMIC,oracle.br.dataservers.CourseDataServer,selectCourse&course=2686&template=395.dwt&unit=NONE&testeira=473>. Acesso em: 26 maio. 2018.

SPI. **Razões para Escolher o Debian**. 08 jun. 2017.Disponível em: <https://www.debian.org/intro/why_debian.pt.html>. Acesso em: 09 maio 2018.

TRAINNING. **Cursos Microsoft**. 2018. Disponível em: <https://www.trainning.com.br/cursos-mcsa-mcse-microsoft>. Acesso em: 26 maio. 2018.

12. ANEXOS

Anexo I – Dhcpd.conf

```
# Sample configuration file for ISC dhcpd for Debian
#
# Attention: If /etc/ltsp/dhcpd.conf exists, that will be used as
# configuration file instead of this file.
#
#

# The ddns-updates-style parameter controls whether or not the server will
# attempt to do a DNS update when a lease is confirmed. We default to the
# behavior of the version 2 packages ('none', since DHCP v2 didn't
# have support for DDNS.)
ddns-update-style none;

# option definitions common to all supported networks...
option domain-name "example.org";
option domain-name-servers ns1.example.org, ns2.example.org;

default-lease-time 600;
max-lease-time 7200;

# If this DHCP server is the official DHCP server for the local
# network, the authoritative directive should be uncommented.
#authoritative;

# Use this to send dhcp log messages to a different log file (you also
# have to hack syslog.conf to complete the redirection).
log-facility local7;

# No service will be given on this subnet, but declaring it helps the
# DHCP server to understand the network topology.

#subnet 10.152.187.0 netmask 255.255.255.0 {
#}

# This is a very basic subnet declaration.

#subnet 10.254.239.0 netmask 255.255.255.224 {
#  range 10.254.239.10 10.254.239.20;
#  option routers rtr-239-0-1.example.org, rtr-239-0-2.example.org;
#}

# This declaration allows BOOTP clients to get dynamic addresses,
# which we don't really recommend.

#subnet 10.254.239.32 netmask 255.255.255.224 {
#  range dynamic-bootp 10.254.239.40 10.254.239.60;
#  option broadcast-address 10.254.239.31;
#  option routers rtr-239-32-1.example.org;
#}

# A slightly different configuration for an internal subnet.
#subnet 10.5.5.0 netmask 255.255.255.224 {
#  range 10.5.5.26 10.5.5.30;
#  option domain-name-servers ns1.internal.example.org;
```

```
#  option domain-name "internal.example.org";
#  option subnet-mask 255.255.255.224;
#  option routers 10.5.5.1;
#  option broadcast-address 10.5.5.31;
#  default-lease-time 600;
#  max-lease-time 7200;
#}

# Hosts which require special configuration options can be listed in
# host statements.   If no address is specified, the address will be
# allocated dynamically (if possible), but the host-specific information
# will still come from the host declaration.

#host passacaglia {
#  hardware ethernet 0:0:c0:5d:bd:95;
#  filename "vmunix.passacaglia";
#  server-name "toccata.fugue.com";
#}

# Fixed IP addresses can also be specified for hosts.   These addresses
# should not also be listed as being available for dynamic assignment.
# Hosts for which fixed IP addresses have been specified can boot using
# BOOTP or DHCP.   Hosts for which no fixed address is specified can only
# be booted with DHCP, unless there is an address range on the subnet
# to which a BOOTP client is connected which has the dynamic-bootp flag
# set.
#host fantasia {
#  hardware ethernet 08:00:07:26:c0:a5;
#  fixed-address fantasia.fugue.com;
#}

# You can declare a class of clients and then do address allocation
# based on that.   The example below shows a case where all clients
# in a certain class get addresses on the 10.17.224/24 subnet, and all
# other clients get addresses on the 10.0.29/24 subnet.

#class "foo" {
#  match if substring (option vendor-class-identifier, 0, 4) = "SUNW";
#}

#shared-network 224-29 {
#  subnet 10.17.224.0 netmask 255.255.255.0 {
#    option routers rtr-224.example.org;
#  }
#  subnet 10.0.29.0 netmask 255.255.255.0 {
#    option routers rtr-29.example.org;
#  }
#  pool {
#    allow members of "foo";
#    range 10.17.224.10 10.17.224.250;
#  }
#  pool {
#    deny members of "foo";
#    range 10.0.29.10 10.0.29.230;
#  }
#}
```