UNIVERSIDADE TECNOLÓGICA FEDERAL DO PARANÁ
DEPARTAMENTO ACADÊMICO DE ELETRÔNICA
CURSO DE ESPECIALIZAÇÃO SEMIPRESENCIAL EM CONFIGURAÇÃO E GERENCIAMENTO DE SERVIDORES E EQUIPAMENTOS DE REDES

JULIANO PARREIRA DOS SANTOS

SERVIDOR RADIUS COM CONEXÃO LDAP

MONOGRAFIA

CURITIBA
2011

JULIANO PARREIRA DOS SANTOS

SERVIDOR RADIUS COM CONEXÃO LDAP

Monografia apresentada como requisito parcial para obtenção do grau de Especialista em Configuração e Gerenciamento de Servidores e Equipamentos de Redes, do Departamento Acadêmico de Eletrônica da Universidade Tecnológica Federal do Paraná.
Orientador: Prof. M.Sc. Fabiano Scriptore de Carvalho

CURITIBA
2011

RESUMO

Santos, Juliano P. **Servidor RADIUS com Conexão LDAP**. 2011. 57 f. Monografia (Especialização em Configuração e Gerenciamento de Servidores e Equipamentos de Redes) – Programa de Pós-Graduação em Tecnologia, Universidade Tecnológica Federal do Paraná, Curitiba, 2011.

Este projeto tem como objetivo central a segurança no acesso a redes de computadores e equipamentos. Será abordado o tema de segurança de redes com ênfase no acesso utilizando um servidor Remote Authentication Dial In User Service (RADIUS) com conexão a um banco de dados Lightweight Directory Access Protocol (LDAP). Todos os usuários que necessitarem de acesso à rede deverão primeiramente se autenticar neste servidor para poder ter acesso em equipamentos e softwares disponíveis.

Palavras-chave: Redes. Segurança. Acesso. Permissão

ABSTRACT

Santos, Juliano P. **Server RADIUS with LDAP Connection**. 2011. 57 f. Monograph (Specialization in Configuration and Management of Servers and Network Equipments) – Federal Technological University of Paraná. Curitiba, 2011.

This project has as main objective to secure access to computer networks and equipment. Will address the topic of network security with an emphasis on access by using a Remote Authentication Dial In User Service (RADIUS) with connection to a database, Lightweight Directory Access Protocol (LDAP). All users who need access to the network must first authenticate to this server to have access to equipment and software available.

Keywords: Networks, Security, Access, Permission

LISTA DE FIGURAS

LISTA DE SIGLAS

ADSL	Asymmetric Digital Subscriber Line
AOL	America Online
ARPA	Advanced Research Projects Agency
ARPANET	Advanced Research Projects Agency Network
BDB	Berkeley DataBase
CRC	Cyclic Redundancy Check
DAP	Directory Access Protocol
DARPA	Defense Advanced Research Projects Agency
DIT	Directory Information Tree
DN	Distinguished Name
DNS	Domain Name System
DOS	Denial of Service
FTP	File Transfer Protocol
HDB	Hierarchical DataBase
HTTP	HyperText Transfer Protocol
IEEE	Institute of Electrical and Electronics Engineers
IP	Internet Protocol
ITU-T	International Telecommunication Union Telecommunication
LDAP	Lightweight Directory Access Protocol
LLC	Logical Link Control
MAC	Media Access Control
OSI	Open Systems Interconnection
PC	Portatil Computers
PCI	Peripheral Component Interconnect
RADIUS	Remote Authentication Dial In User Service
RDN	Relative Distinguished Names
RFC	Request For Comments
RPC	Remote Procedure Call
RSA	Rivest, Shamir and Adleman
SMTP	Simple Mail Transfer Protocol
TCP	Transmission Control Protocol
UDP	User Datagram Protocol

SUMÁRIO

1 INTRODUÇÃO

Atualmente o acesso às redes está se tornando cada vez mais fácil, isso é uma vantagem para o crescimento da rede, porém isto traz um problema relacionado à segurança, com o acesso facilitado, os administradores de rede tem que trabalhar constantemente visando a segurança.

Este projeto pretende discutir uma forma de aumentar a segurança da rede e esta primeira parte esta dividida em tema, problema, objetivos geral e específicos e justificativa.

1.1 TEMA

Durante as primeiras décadas de sua existência, as redes de computadores foram usadas principalmente por pesquisadores universitários, com a finalidade de enviar mensagens de correio eletrônico, e também por funcionários de empresas, para compartilhar impressoras. Sob essas condições, a segurança nunca precisou de maiores cuidados (TANENBAUM, 2003). Com a evolução nas comunicações a comunicação de dados tem se tornado indispensável para qualquer tipo de mercado (COMUNICAÇÃO DE DADOS, 1997). Esta comunicação se faz necessária para transações bancárias, troca de dados entre empresas matriz e suas filiais, acessos remotos a uma rede de computadores ou equipamentos de rede, entre outros. Como essa transmissão de informação ocorre entre diversas redes que são controladas por operadoras distintas, a segurança da informação pode ser comprometida. Com isso brechas são abertas para diversos tipos de ataques e/ou obtenção de informações que podem ser utilizadas tanto para corromper um sistema como para obter algum benefício financeiro.

Quando os protocolos de internet foram criados não se pensava na situação da segurança (ASSUNÇÃO, 2008). Os criadores da internet não imaginavam que ela tomaria tamanha proporção. Atualmente as empresas têm investido altos valores na segurança de rede com instalação de equipamentos que fazem um controle do que

deve ser acessado pela empresa para a internet e vice-versa. Os equipamentos que realizam o *firewall*, em geral, são equipamentos mais caros do que os equipamentos que fazem a rede funcionar, pois eles bloqueiam os acessos não permitidos a rede empresarial por pessoas com a intenção de prejudicar ou obter informações.

Visando a segurança no acesso a informação este projeto tem por objetivo estudar e implantar um mecanismo de segurança baseado em um servidor. Este deverá possuir um cadastro dos usuários que têm permissão de acesso em uma determinada rede.

1.2 PROBLEMA

Os ataques direcionados as organizações estão cada dia mais freqüentes, pessoas tentam entrar no sistema de rede das organizações para poder obter alguma informação de valor que possa ser utilizada posteriormente ou, simplesmente como um *hobby*, para prejudicar a rede, alterando encaminhamentos, inundando a rede com informações desnecessárias para congestionar a rede e/ou tirando equipamentos de serviço.

Outro grande problema nas redes atualmente está no acesso não autorizado de pessoas, com más intenções, que entram fisicamente nas empresas com o intuito de prestar algum tipo de serviço. Geralmente estas pessoas entram nas empresas com um *notebook* ou *Ipad* e, com acesso a algum ponto de rede livre ou rede *wireless*, conseguem conectar-se a rede tendo acesso a todo o conteúdo de informação que é confidencial da empresa. Após a obtenção do acesso, da rede e das informações, por esta pessoa, as empresas ficam desprotegidas de ataques que poderão ocorrer dentro da própria empresa devido à falta de segurança interna. A partir do momento que a pessoa mal intencionada está dentro de uma rede, praticamente pouco pode ser feito visando evitar os danos que irão ser causados por ela.

1.3 OBJETIVOS

1.3.1 Objetivo Geral

Com base na brecha de segurança oferecida por diversas empresas na atualidade, este trabalho tem como objetivo a implantação de um sistema, com um servidor Remote Authentication Dial In User Service (RADIUS) que solicita autenticação para qualquer pessoa que necessite de acesso a rede, mesmo que esta pessoa esteja conectada fisicamente. Os usuários que necessitem de acesso a rede deverão estar cadastrados em um banco de dados Lightweight Directory Access Protocol (LDAP). O LDAP é um protocolo para acessar serviços de diretório distribuídos que atuam de acordo com modelos de dados e serviço X.500 (LIGHTWEIGHT DIRECTORY ACCESS PROTOCOL, 2006), em que os dados se encontram em forma de nós, onde cada nó consiste de um conjunto de atributos. Com seus respectivos valores (PEREIRA, 2009). Somente pessoas que realmente precisem acessar a rede e, conseqüentemente as informações, terão acesso a elas.

1.3.2 Objetivos Específicos

- Estudar os protocolos mais utilizados nas redes de computadores;
- Verificar requisitos básicos e avançados de segurança;
- Instalar um servidor RADIUS em um servidor Linux;
- Configurar o servidor RADIUS com usuários;
- Realizar testes de acessos com os usuários criados;
- Criar um banco de dados LDAP;
- Realizar a conexão do servidor RADIUS com o banco de dados LDAP e testar os acessos com esta configuração;
- Verificar resultados obtidos.

1.4 JUSTIFICATIVA

Atualmente a maioria dos dados de uma empresa estão em arquivos de mídia, ao contrário do que acontecia há alguns anos, onde as informações eram arquivadas em mídias impressas e, por conseqüência, eram colocadas em gavetas e/ou armários. Para obter estas informações era necessário entrar fisicamente na empresa e roubar os dados impressos para obter as informações. Nos dias atuais apenas utilizando a internet é possível se conectar ao banco de dados de qualquer instituição que não realizou medidas de segurança em sua rede.

Visando a segurança da informação é necessário que as empresas possuam um sistema de segurança bem definido para acesso aos dados, pois determinadas informações são confidenciais e pode custar um preço elevado se forem difundidas antes do tempo ou então obtidas por concorrentes. Para que estas informações estejam seguras é necessário um sistema de cadastro de usuários, onde cada um possui uma senha e só pode obter acesso aos dados após a inserção da mesma em uma interface especifica.

Este projeto tem por objetivo a implantação do sistema de autenticação RADIUS com acesso a uma plataforma LDAP visando proteger qualquer informação de uma pessoa que não tenha cadastro para acesso aos dados da empresa. Como conseqüência gerando mais segurança para a empresa.

1.5 PROCEDIMENTOS METODOLOGICOS

Para execução deste projeto, os processos serão utilizados utilizando-se a pesquisa exploratória, pois estas pesquisas têm como objetivo principal o aprimoramento de idéias (GIL, 2002, p. 41). Para GIL (2002) este tipo de pesquisa é flexível de modo que possibilite a consideração dos mais variados aspectos. Com base nesta afirmativa este trabalho tem sua fonte de pesquisa em Request For Comments (RFCs), em documentações técnicas relacionadas a segurança de rede

e em documentos que estejam relacionados com a implantação de um servidor RADIUS.

Com os dados necessários obtidos a parte pratica terá inicio. Serão utilizadas máquinas virtuais para a realização de simulações de redes reais. Processos de instalação do servidor RADIUS e a conexão utilizando o protocolo LDAP terão como base as RFCs para sua implantação.

1.6 EMBASAMENTO TEÓRICO

No inicio das redes de computadores não houve uma preocupação relevante com relação à segurança, pois foram utilizadas somente por universitários visando a troca de e-mails e por funcionários de empresas para compartilhamento de impressoras. Porém, na atualidade, milhares de pessoas estão utilizando a rede para realização de compras e transações bancárias, estas atividades exigem que a segurança seja aplicada a rede de forma a garantir integridade e confidencialidade dos dados.

Para Tanenbaum (2003) a maior parte dos problemas de segurança é causada principalmente por pessoas maliciosas que tentam obter algum beneficio, chamar a atenção ou prejudicar alguém. Uma política de segurança é um instrumento importante para proteger qualquer organização contra ameaças à segurança da informação que a ela pertence ou que está sob sua responsabilidade (PRÁTICAS DE SEGURANÇA PARA ADMINISTRADORES DE REDES INTERNET, 2003).

2 REFERENCIAL TEÓRICO

Este capitulo tem como objetivo explanar alguns tópicos que servem como referência para a realização deste trabalho.

2.1 REDES

2.1.1 História

Uma rede de computadores é a conexão de dois ou mais computadores para permitir o compartilhamento de recursos e a troca de informação entre as máquinas (CANTU, Evandro, 2003, p.3). A primeira rede de computadores foi criada na década de 60 e o objetivo era transmitir informações de um computador para outro. Entre o final da década de 60 e o inicio da década de 70 foi criada pela *Advanced Research Projects Agency* – ARPA – a *Advanced Research Projects Agency Network* – ARPANET. A ARPANET interligava quatro universidades dos Estados Unidos da América, eram elas a Universidade da Califórnia em Los Angeles, o *Stanford Research Institute*, a Universidade da Califórnia em Santa Bárbara e a Universidade de Utah. Além das universidades ela também atendia a comunidade militar americana (A ARPANET, 1997).

Antes da criação da ARPANET os sistemas de computadores consistiam de computadores muito grandes, em muitos casos um computador ocupava uma sala inteira (Como Funciona a ARPANET). A partir de 1970 a Intel Corporation começou a fabricar os microprocessadores e em 1975 o primeiro microcomputador foi criado, este foi chamado de ALTAIR 8800. Neste mesmo ano foi criado, por Paul Allan e Bill Gates, a Microsoft e o primeiro software para microcomputadores: uma adaptação *BASIC* para o ALTAIR (Um Pouco da História dos Computados, 2011).

Em 1982 surgiu o 286, este já usava memória de 30 pinos, slots de 16 bits e já vinha equipado com memória cache, para auxilio do processador. Em 1985 surgiu o 386 que era capaz de rodar softwares gráficos mais avançados. O 286 e o 386 foram evoluindo até que em 1993 foi criado o Pentium. Neste ocorreram grandes mudanças em relação aos seus antecessores, entre as principais estão o uso das memórias de 108 pinos, o aparecimento das placas de video e do aprimoramento do

slot *Peripheral Component Interconnect* (PCI). Em 1997 o Pentium II foi anunciado, após esta data as mudanças estão basicamente na velocidade dos processadores (UM POUCO DA HISTÓRIA DOS COMPUTADORES, 2011).

2.1.2 Modelo de Referência OSI

Como o volume de fabricantes de equipamentos de rede estava aumentando com o decorrer dos anos, as soluções para comunicação eram proprietárias, isso é, uma determinada tecnologia só era suportada por seu fabricante (O MODELO DE REFERÊNCIA OSI PARA PROTOCOLOS DE REDE, 09/10/11). Foi necessário criar um padrão para que equipamentos de diferentes fabricantes pudessem se comunicar. No inicio da década de 1980 o *International Standards Organization* (ISO) aprovou um modelo de arquitetura para sistemas abertos, visando a comunicação entre máquinas de diversos fabricantes e definiu diretivas genéricas para a construção de redes de computadores, independente da tecnologia aplicada. Esse modelo foi chamado de *Open Systems Interconnection* ou simplesmente OSI (O MODELO OSI, 09/10/11).

O modelo OSI foi dividido em sete camadas, conforme a figura 1. Segundo Tanenbaum (2003) houve cinco princípios aplicados para se chegar as sete camadas, são eles:

1) Uma camada deve ser criada onde houver necessidade de outro grau de abstração;
2) Cada camada deve executar uma função bem definida;
3) A função de camada deve ser escolhida tendo em vista a definição de protocolos padronizados internacionalmente;
4) Os limites de camada devem ser escolhidos para minimizar o fluxo de informações pelas interfaces;
5) O número de camadas deve ser grande o bastante para que funções distintas não precisem ser desnecessariamente colocadas na mesma camada e pequeno o suficiente para que a arquitetura não se torne difícil de controlar.

Figura 1 - Camadas Modelo OSI
Fonte: O MODELO OSI E SUAS 7 CAMADAS

Abaixo estão descritas cada camada e um breve resumo sobre cada uma delas visando facilitar a compreensão do Modelo OSI:

Camada Física: Os protocolos desta camada tratam da codificação e decodificação de símbolos e caracteres em sinais elétricos ou ópticos que serão lançados no meio físico (O MODELO OSI, 09/10/11).

Camada de Enlace de dados: Esta camada é responsável por coletar os dados da camada de Rede e converter em quadros que serão transmitidos pelo meio físico. Nesta camada são inseridos endereço de placa de rede de origem e destino, dados de controle e uma soma de verificação para controle de erros (O MODELO DE REFERÊNCIA OSI PARA PROTOCOLOS DE REDE, 09/10/11).

Camada de Rede: A camada de rede determina como os pacotes são roteados da origem até o destino (TANENBAUM, 2003). As principais funções desta camada são o roteamento dos pacotes, o controle de congestionamento e a contabilização do número de *bytes* utilizados pelo usuário (O MODELO OSI, 09/10/11).

Camada de Transporte: Esta camada é responsável por receber os dados da camada superior e dividi-los em pacotes que serão transmitidos pela rede. No computador receptor, esta camada é responsável por remontar os pacotes recebidos da camada inferior (O MODELO DE REFERÊNCIA OSI PARA PROTOCOLOS DE REDE, 09/10/11).

Camada de Sessão: Esta camada administra e sincroniza diálogos entre dois processos de aplicação. Os dois tipos de diálogo oferecidos por esta camada são *Half Duplex* e *Full Duplex*. Uma sessão pode ser aberta entre duas estações a fim de permitir que um usuário se conecte a um sistema remoto (O MODELO OSI,

09/10/11).

Camada de Apresentação: Esta camada é responsável por traduzir formatos da/para a camada de aplicação. Também pode ser usada para e/ou criptografar dados (O MODELO DE REFERÊNCIA OSI PARA PROTOCOLOS DE REDE, 09/10/11).

Camada de Aplicação: A camada de aplicação contém uma série de protocolos utilizados pelos usuários (TANENBAUM, 2003). O mais utilizados é o *HyperText Transfer Protocol* (HTTP).

2.1.3 TCP/IP

O conjunto de protocolos denominado *Transmission Control Protocol/Internet Protocol* (TCP/IP) foi criado em meados da década de 70 pela *Defense Advanced Research Projects Agency* (DARPA). O principal interesse era que esta rede pudesse suportar um ataque nuclear (SEGURANÇA ..., 2000, p. 49). Este protocolo foi desenvolvido para fornecer comunicação através da própria DARPA. A idéia inicial era criar um protocolo que fosse capaz de fazer uma rede sobreviver a qualquer guerra ou conflito, independente do meio (cabos, microondas, satélites, fibras ópticas) o importante é que o pacote sempre chegue ao seu destino (ASSUNÇÃO, 2008).

O protocolo TCP/IP possuía duas vantagens sobre outros protocolos: ele era leve e seu custo era mais baixo do que as outras opções disponíveis na época. Devido a estes fatores o TCP/IP tornou-se muito popular. No ano de 1983, o protocolo TCP/IP foi adicionado em um software da Unix chamado *Berkeley Software Distribution*. Sua união com o Unix em formas comerciais logo se seguiu fazendo com que o TCP/IP fosse estabelecido como o padrão Internet (SEGURANÇA ..., 2000, p. 49).

Atualmente o TCP/IP é utilizado, além da Internet, em intranets. Nos ambientes internos o TCP/IP pode oferecer vantagens significativas sobre os outros protocolos de rede existentes. Por exemplo, ele funciona sobre uma variedade ampla de *hardwares* e sistemas operacionais, com isso pode uma rede heterogênea pode ser criada utilizando Macs, *Portatil Computers* (PCs) compatíveis com IBM, Sun SPARCstations e assim por diante. Por esta razão o TCP/IP permaneceu

extremamente popular.

2.1.3.1 Funcionamento do TCP/IP

O TCP/IP não é na verdade um protocolo único e sim uma pilha de protocolos, como é mais comumente conhecido. Como pode ser observado o seu nome faz referência a dois protocolos distintos o TCP e o IP.

A pilha de protocolos TCP/IP possui quatro camadas (figura 2). A comunicação dos programas é com a camada de aplicação. Alguns exemplos de protocolos de aplicação são *Simple Mail Transfer Protocol* (SMTP), o *File Transfer Protocol* (FTP) e o HTTP. Cada programa se comunica com um protocolo de aplicação diferente, o que define qual protocolo deve ser utilizado é a finalidade do programa.

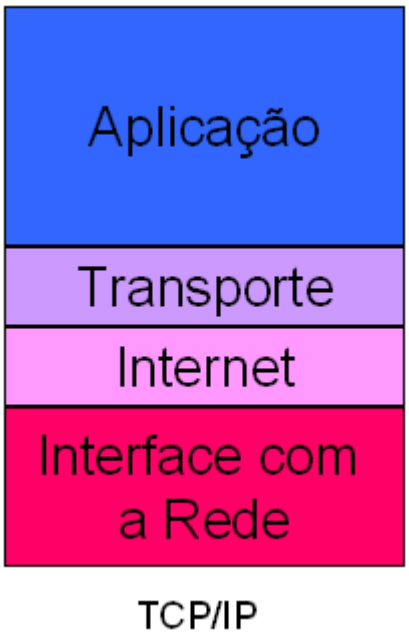

Figura 2 - Arquitetura TCP/IP
Fonte: Como o Protocolo TCP/IP Funciona

A camada de aplicação realiza a comunicação entre os programas e a camada inferior. Por exemplo, quando um programa cliente de e-mail quer baixar os e-mails que estão em um servidor de e-mail ele irá interagir com a camada de aplicação do TCP/IP. A camada de aplicação recebe esta solicitação do programa e se comunica com a camada de transporte através de uma porta (Figura 3). As portas são numeradas e as aplicações padrão sempre utilizam a mesma porta. No exemplo

citado anteriormente a camada de aplicação iria utilizar a porta 25 (SMTP). Com base no número de portas a camada de transporte identifica o conteúdo do pacote de dados e, quando o pacote chegar ao receptor, o mesmo sabe para qual protocolo de aplicação deverá entregar o pacote de dados (COMO O PROTOCOLO TCP/IP FUNCIONA, 09/10/11).

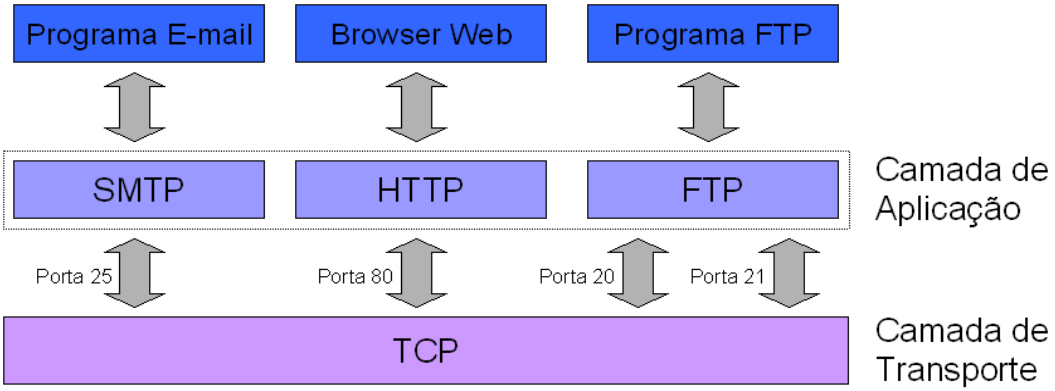

Figura 3 - Como a Camada de Aplicação Funciona
Fonte: Como o Protocolo TCP/IP Funciona

A camada de transporte é responsável pela confiabilidade, controle de fluxo e, se necessário, correção de erros da entrega dos dados. O TCP é o protocolo mais utilizado na camada de transporte. Quando os pacotes chegam ao destino o TCP é o responsável por colocar estes pacotes em ordem e verificar se o pacote não foi corrompido no trajeto, caso o pacote esteja íntegro o TCP envia um sinal chamado *acknowledge*, ou simplesmente *ack*, para informar ao transmissor que o pacote foi recebido corretamente. Se nenhum sinal de confirmação for recebido pelo transmissor ele enviará novamente o pacote que foi perdido ou que estava corrompido.

Existe outro protocolo que também opera na camada de transporte chamado *User Datagram Protocol* ou UDP. O UDP não reordena os pacotes recebidos no destino e não usa mecanismos de confirmação de recebimento, por este motivo é considerado um protocolo não confiável. Este protocolo é usado quando os dados que são transmitidos não são importantes como, por exemplo, requisições *Domain Name System* (DNS). Quando é solicitada a utilização do UDP a camada de aplicação é responsável por fazer todo o controle de fluxo e verificar a existência de erros nos pacotes e, caso necessário, será ela que deverá solicitar a retransmissão

do pacote.

Quando o TCP ou UDP recebem os dados da camada de aplicação é inserido um cabeçalho. Neste cabeçalho são inseridas informações de controle como número da porta de origem, número da porta de destino, um número de seqüência (utilizado pelo TCP para reordenar os pacotes) e uma soma de verificação chamada de *checksum* ou *Cyclic Redundancy Check* (CRC) que é utilizada para verificar se os dados chegaram íntegros ao destino. O cabeçalho UDP tem 8 bytes enquanto o cabeçalho TCP pode variar entre 20 e 24 bytes. Esta variação ocorre no TCP devido a utilização ou não do campo opções (COMO O PROTOCOLO TCP/IP FUNCIONA).

A camada de Internet tem como objetivo assegurar que os dados cheguem ao seu destino, independente das redes e do caminho que utilizem para isso (ASSUNÇÃO, 2008). Nesta camada é identificado o melhor caminho e como será realizada a comutação dos pacotes até o destino.

Nas redes TCP/IP cada computador é identificado com um endereço único, chamado de endereço IP. Na camada de Internet é inserido um cabeçalho contendo as informações do endereço IP de origem e o endereço IP de destino, dentre outras informações. Com base neste endereço IP de destino é que o pacote irá trafegar na rede até seu destino. O protocolo IP será abortado em mais detalhes no item 2.4 deste trabalho.

A camada de interface com a rede é a camada responsável por se relacionar a todos os requisitos que um pacote IP necessita para realmente estabelecer um link físico (ASSUNÇÃO, 2008). Os pacotes gerados na camada de Internet são passados para a camada de interface com a rede durante a transmissão dos dados que estão sendo enviados e quando ocorre o recebimento de informações pela rede esta camada é responsável em enviar estes dados para a camada de Internet. Nesta camada é definido o tipo de rede física que um computador, ou outro equipamento, está conectado a rede.

A camada de interface do modelo TCP/IP abrange duas camadas do modelo OSI, a camada física e a camada de enlace de dados. O protocolo comumente utilizado nesta camada é o *Ethernet* (COMO O PROTOCOLO TCP/IP FUNCIONA, 09/10/11).

O *Ethernet* possui três camadas: *Logical Link Control* (LLC), pelo endereço *Media Access Control* (MAC) e a camada física. O MAC e o LLC, juntos,

correspondem juntos a camada de enlace do modelo OSI (figura 4).

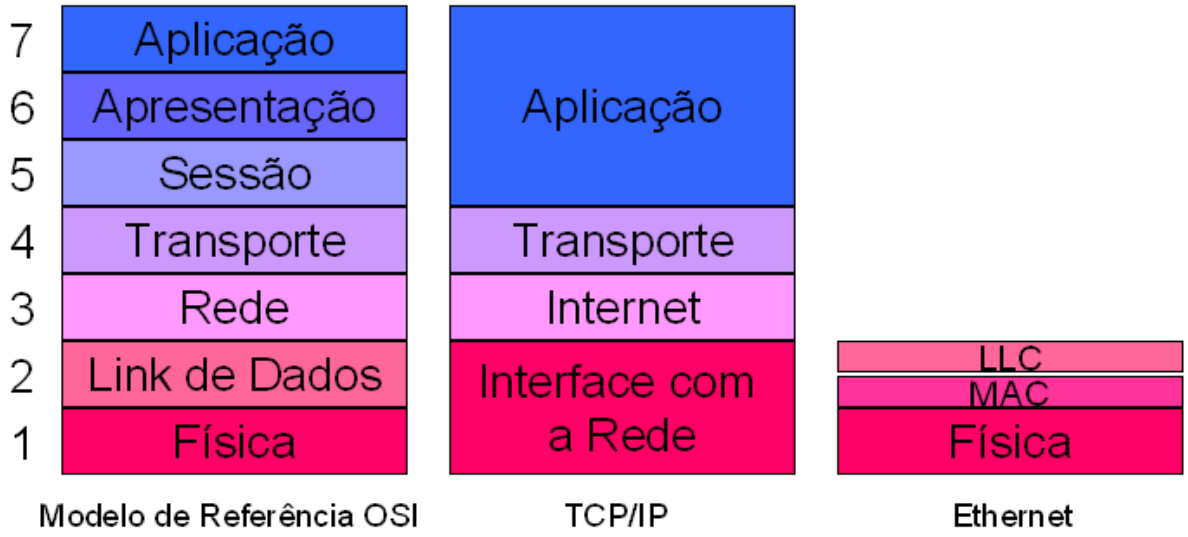

Figura 4 - Arquitetura de Protocolos
Fonte: Como o Protocolo TCP/IP Funciona

O LLC é responsável pela identificação, no quadro, o protocolo da camada de Internet que gerou os dados para que o LLC de destino identifique para qual protocolo de Internet estes dados devem ser entregues. Esta camada é definida pelo *Institute of Electrical and Electronics Engineers* (IEEE) 802.2.

A camada MAC realiza a montagem do quadro que será enviado para a rede. Nesta camada é inserido o endereço MAC de origem e o endereço MAC de destino. Este endereço é um endereço físico de uma placa de rede. Este endereço é reconhecido dentro de uma rede, porém quando o destino se encontra fora desta rede o endereço MAC que é inserido nesse quadro é o endereço do *gateway* ou roteador, que será responsável por enviar os dados até a rede de destino. O protocolo MAC é definido pelo protocolo IEEE 802.3 para redes que utilizam cabos ou pelo protocolo IEEE 802.11 para redes sem fio.

A camada física tem a responsabilidade de transformar o quadro gerado pela camada MAC em sinais elétricos, se a rede for cabeada, ou em sinais eletromagnéticos, se a rede for sem fio.

2.1.4 Internet Protocol – IP

O protocolo *Internet Protocol* ou protocolo IP, é utilizado para identificar os

hosts na rede. Com base nos endereços IP é possível que um e-mail seja enviado a um destinatário ou que um site possa ser acessado.

O endereço IP versão 4 é uma seqüência numérica composta por 32 bits e está dividido em 4 octetos. Cada octeto é separado por um ponto e, além de se chamar de octeto, pode receber o nome de byte. Esta divisão em 4 octetos é utilizada para facilitar a organização da rede.

O protocolo IP não é orientado a conexão, pois ele não fornece um serviço de confiabilidade, de controle de fluxo, de seqüenciamento ou outros serviços normalmente encontrados em outros protocolos ponto-a-ponto (INTRODUÇÃO AO PROTOCOLO INTERNET – IP, 09/10/11). De um modo simplificado o protocolo IP envia o pacote até o próximo roteador até que este pacote encontre o endereço de destino.

Dentro do protocolo IP foram criadas cinco classes que são representadas por letras maiúsculas. São elas classes A, B, C, D e E, porém somente as três primeiras são utilizadas para atribuir endereços a hosts na rede. As classes D e E são utilizadas para fins específicos, como por exemplo, *multicast* (INTRODUÇÃO AO PROTOCOLO INTERNET – IP, 09/10/11).

A classe A é utilizada quando se é necessário poucas redes e muitos *hosts*. Nesta classe o primeiro octeto é utilizado para endereço de rede e os outros três são utilizados para endereços de *hosts*. A faixa de endereços que corresponde a classe A vai de 0.0.0.0 à 127.255.255.255. Os endereços de classe B são utilizados quando o número de redes tem que ser semelhante ao número de hosts, para isso são usados dois octetos para o endereço de rede e dois octetos para destinar endereços IPs aos *hosts*. A faixa de endereços da classe B é compreendida entre 128.0.0.0 à 191.255.255.255. A classe C é necessária onde a quantidade de hosts for pequena, porém existem muitas redes. Nesta classe são usados três octetos para destinar as redes e apenas o último octeto é utilizado para endereços de *hosts* (Endereço IP). A faixa de endereços que corresponde a classe C vai de 192.0.0.0 à 255.255.255.255.

Dentro do endereço IP é possível separar qual é a parte destinada a endereços de rede e qual é a parte destinada aos endereços de *hosts*, para isso é utilizada a máscara de sub-rede. Para as classes A, B e C temos as seguintes máscaras: 255.0.0.0, 255.255.0.0 e 255.255.255.0, respectivamente. Para se saber

exatamente qual é a parte de rede e host é necessário converter os endereços IP e suas respectivas máscaras em binários, realizar uma operação *AND* de cada *bit*. A parte que representa a rede é onde o resultado obtido for 1 e a parte que representa os *hosts* é indicada pelos zeros. Quando este resultado obtido é convertido para decimal é possível identificar qual é o endereço da rede em que este equipamento está inserido.

A principal função do protocolo IP é o roteamento. O roteamento é processo de encaminhar pacotes entre redes interconectadas. A troca dos datagramas ou pacotes IP ocorre na camada de Internet da pilha de protocolos TCP/IP em cada host por onde estes pacotes passam.

Como citado anteriormente, o pacote IP contém um endereço de origem e um endereço de destino. O endereço de destino de cada pacote IP é analisado pelos serviços da camada de Internet em cada *host*, este por sua vez compara este endereço de destino a uma tabela de roteamento mantida localmente e decide para onde e por qual interface este pacote deve ser enviado. Este processo ocorre em todos os *hosts* por onde o pacote passa até que o destino seja encontrado e o pacote seja entregue (ROTEAMENTO IP, 2011).

2.1.5 Transmission Control Protocol – TCP

O protocolo *Transmission Control Protocol* (TCP) foi criado devido à necessidade de oferecer um fluxo de byte fim a fim confiável em uma inter-rede não confiável (TANENBAUM,2003).

O TCP se adapta dinamicamente as diferentes características das redes por onde o pacote irá passar, como por exemplo, largura de banda, latência, tamanho de pacote e alguns outros parâmetros diferentes. Essa característica do TCP garante uma entrega confiável independente da rede por onde o pacote esta trafegando.

Na transmissão o TCP receberá os dados da camada de aplicação e irá inserir um cabeçalho, conforme figura 5. No cabeçalho estão inseridas algumas informações de controle, como exemplo as portas de origem e destino, número de seqüência e uma soma de verificação, também conhecida como *checksum*. O *checksum* é um cálculo utilizado para verificar a integridade dos dados, verificar se os dados não estão corrompidos (COMO O PROTOCOLO TCP/IP FUNCIONA,

09/10/11).

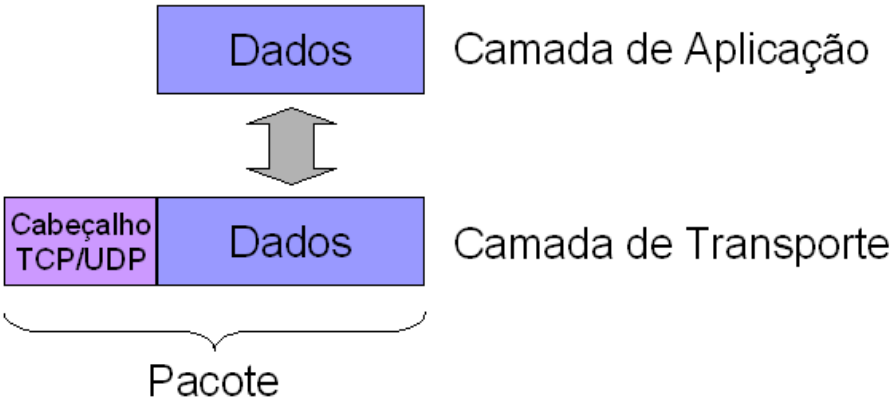

Figura 5 - Inserção Cabeçalho TCP
Fonte: Como o Protocolo TCP/IP Funciona

Este protocolo trabalha na camada quatro do modelo de referência OSI ou na camada de transporte do modelo TCP/IP. O TCP recebe os dados da camada de rede e reordena-os, pois os pacotes podem chegar ao destino fora de ordem, confirma se os dados estão íntegros e envia um *acknowlodge* ao transmissor, informando que os dados estão todos corretos (COMO O PROTOCOLO TCP/IP FUNCIONA, 09/10/11).

2.2 SEGURANÇA

No inicio da comunicação entre computadores a segurança de rede não foi algo estudado, pois a idéia era que as redes fossem utilizadas por pesquisadores universitários e também por funcionários de empresas para o envio de mensagens eletrônicas e compartilhamento de impressoras. Atualmente milhões de cidadãos comuns estão utilizando a rede para realizar compras, transações bancárias, entre outras atividades *online*, a segurança de rede está se tornando um problema potencial quando não planejada (TANENBAUM, 2003).

A segurança nas redes tem se tornado algo muito necessário tanto para um usuário comum que utiliza seu computador para tarefas simples, como por exemplo, ler e-mails, navegar na internet e utilizar um aplicativo de mensagens instantâneas como para uma empresa que possui servidores dos mais variados tipos contendo, na maioria dos casos, todas as informações pertinentes a ela.

O mundo da segurança evolui de uma forma continua. Quando uma brecha de segurança é encontrada e solucionada outra nova já está sendo estudada e utilizada pelos *hackers*, isto faz com que um ciclo seja formado. Por isso a segurança deve ser realizada de forma continua e evolutiva, isso porque as ferramentas atuais podem ser extremamente eficientes para as técnicas de ataques já conhecidas, porém ineficientes para as novas técnicas que estão sendo desenvolvidas.

Algumas características da rede incentivam pessoas com conhecimento avançado a tentar burlar os sistemas existentes, dentre elas estão à disponibilização ampla de informação, a interoperabilidade e intercambio de informação e gerenciamento remoto, ou seja, a informação está disponível, basta encontrar um meio de acessá-la e, em muitos casos, este meio é ultrapassando as ferramentas que são utilizadas para gerar a segurança da informação.

A segurança de rede é importante para garantir a proteção do patrimônio de uma empresa, credibilidade, vantagem competitiva, cumprimento das responsabilidades, continuidade da operação e atividade, pois se uma informação confidencial for obtida por uma pessoa que esteja ligada a concorrência, dependendo o negócio da empresa, esta pode deixar de exercer suas atividades,

pois o seu concorrente, por exemplo, lançou um produto que seria chave para a empresa antes.

O custo da segurança pode ser medido pelo valor do patrimônio e pela necessidade do negócio. A segurança esta diretamente relacionada com os itens mencionados anteriormente e deve ser balanceada. Uma instituição que pretende criar medidas de segurança deve verificar as vulnerabilidades, ameaças, tipos de ataques e quais são as probabilidades delas serem executadas, após isso deve ser criada uma política e procedimentos de segurança.

Alguns elementos essenciais para segurança são identificação e autenticação, controle de acesso, confidencialidade, integridade e disponibilidade.

2.2.1 Vulnerabilidades e Ameaças

Uma vulnerabilidade ou brecha de segurança ocorre quando existe uma deficiência de hardware, software ou uma diretiva que permite a um atacante ganhar acesso não autorizado ao sistema (SEGURANÇA ..., 2000, p. 308). Esta brecha pode ocorrer por uma falha na instalação, ou configuração, incorreta por falta de experiência, falta de treinamento ou por um simples descuido do administrador da rede. Após a rede estar funcionado pode ocorrer uma deficiência no gerenciamento devido a procedimentos inadequados, monitoramento e verificações insuficientes.

Uma má proteção física dos equipamentos e mídia, situações não previstas, *bugs* no projeto, limites, roubo e danificação de mídias, interceptações de sinais, grampos e desleixos na configuração são exemplos de ações que podem gerar vulnerabilidade em qualquer sistema de rede. Uma brecha pode afetar uma ampla variedade de elementos em uma rede, como por exemplo, roteadores, software de cliente e servidores, sistemas operacionais e *firewalls*.

Uma vulnerabilidade pode ser divulgada de diferentes maneiras. Se ela for distribuída por *crackers* (programadores que invadem sistemas com a intenção de destruir), ela vem acompanhada de vários servidores que foram invadidos por ele. Se a vulnerabilidade for divulgada por um *hacker* (são programadores que descobrem brechas, porém não destroem os dados), ela surge como recomendação e boletim de segurança (SEGURANÇA ..., 2000, p. 309).

As ameaças de rede são reais e estão cada vez mais presente na vida dos

usuários de computadores. Muitas destas ameaças vêm em forma de e-mail ou *pop-ups*. Os atacantes de uma rede conseguem invadir uma rede quando há brechas na segurança ou quando um usuário libera este acesso não autorizado a eles.

A principal ameaça a uma rede de computadores é o vírus (D'AVILA, 2011). Os vírus são pequenos programas, com fins maliciosos, que são inseridos em equipamentos de redes e podem apagar dados, capturar informações, alterar ou impedir o funcionamento do sistema e são capazes de causar grandes transtornos a empresas, indivíduos e outras instituições.

Os vírus receberam esta denominação por serem semelhantes aos vírus biológicos. Eles invadem um computador, tentam executar as ações para as quais estão programados e depois tentam se espalhar para outros equipamentos da rede com a mesma intenção de danificá-los ou obter informações.

Existem alguns vírus que são colocados, de maneira não autorizada, dentro de programas legítimos e que realizam funções desconhecidas. Esse tipo de vírus recebe o nome de cavalo de tróia ou *trojan*. O programa que abriga um cavalo de tróia eficientemente foi infectado (SEGURANÇA..., 2000, p. 235).

Um cavalo de tróia sempre realiza uma atividade a mais que o usuário espera e essa atividade extra é prejudicial. Um cavalo de tróia pode criptografar ou reformatar um disco rígido e sabotar um sistema. Um cavalo de tróia conhecido foi o AOLGOLD que foi distribuído por correio eletrônico e era destinado a ser um pacote aprimorado para acessar o *América Online* (AOL).

Os cavalos de tróia podem ser encontrados em quase todo lugar, em qualquer programa ou em qualquer sistema operacional. Devido a este motivo a cautela deve ser maior com o *download* de softwares da internet. Os cavalos de tróia são difíceis de serem detectados e, geralmente, permanecem em arquivos binários, uma forma não legível para humanos. Por estes motivos os cavalos de tróia representam um alto risco na segurança (SEGURANÇA..., 2000, p. 241).

Existem, também, os *worms* ou vermes que são interpretados com vírus mais inteligentes. A diferença de um *worm* para outros vírus está na propagação. Um vírus comum necessita do auxilio do usuário para se propagar pela rede, um *worm* não, ele pode agir de uma maneira discreta. A partir do momento que um computador for infectado por um *worm*, ele se espalha pela rede sem o auxilio do usuário.

Existem também os *spywares* que são programas que espionam todas as atividades executadas pelos usuários ou capturam informações sobre eles. Os *spywares* são embutidos em programas de procedência duvidosa, na maioria das vezes, oferecidos como softwares *freeware* ou *shareware*.

Semelhante aos *spywares* também foram criados os *keyloggers*. Este tipo de vírus tem o objetivo de capturar tudo o que foi digitado em um teclado. Este tipo de programa pode ser utilizado para fins legais como, por exemplo, em uma empresa e para fins ilícitos para obter informações de forma que o usuário não saiba que estas estão sendo coletadas.

Os vírus citados ilustram apenas alguns exemplos de uma infinidade de outros existentes e novos que ainda serão criados, pois como foi mencionado anteriormente a segurança está sendo atualizada constantemente devido a criação, também constante, de novas ameaças.

2.2.2 Ataques

Os ataques podem ocorrer somente a um equipamento de rede, por exemplo, utilizando um vírus ou pode afetar um serviço prestado em uma rede. A função da maioria dos ataques são para degradar ou, em muitos casos, parar o serviço prestado. Esta ação de parar o serviço recebe o nome de *Denial of Service* (DoS) ou Negação de Serviço.

Segundo Assunção (2008) os ataques de DoS tem como objetivo principal derrubar todo um sistema de rede e para isso ele consome todos os seus recursos. Os ataques visam, através do envio de requisições diversas a um computador alvo, causar a indisponibilidade de algum, ou todos, os serviços oferecidos por ele. Existem alguns tipos de ataques de Negação de Serviço, os que exploram as falhas que um sistema possui, os que simplesmente consomem os recursos da rede e os que utilizam softwares zumbis.

Um exemplo de ataque que explorou uma falha no sistema foi o vírus Blaster (ASSUNÇÃO, 2008) que explorava um *bug* no servidor *Remote Procedure Call (*RPC) do Windows 2000 e XP, que fazia com que o computador reiniciasse em poucos segundos.

Entre os ataques mais conhecidos que consomem recursos da rede estão o

Ping da morte e o *Syn Flood*. O *Ping* da morte é uma técnica antiga e, atualmente ineficaz (ASSUNÇÃO, 2008). Esta técnica era realizada enviando um ping com um pacote muito grande fazendo com que o sistema travasse. O ataque de *Syn Flood* envia pacotes *Syn* para um sistema, mas não completa a transação de três vias que utilizada pelo TCP para que a comunicação seja iniciada. O alvo recebe inúmeros pacotes de *Syn* fazendo com que todos os recursos sejam consumidos.

O ataque com software zumbis consiste em instalar um software em diversas máquinas com a intenção de que todas ataquem um alvo em comum, um servidor na internet, por exemplo, fazendo com que o serviço deste servidor seja afetado e, na maioria das vezes, o serviço pare completamente.

2.2.3 Criptografia

Segundo Tanenbaum (2003) a palavra criptografia vem do grego e significa escrita secreta. Durante a história quatro grupos de pessoas utilizaram e contribuíram para a criação da criptografia: os militares, os diplomatas, os amantes e as pessoas que gostavam de guardar memórias. Dos quatro grupos citados o que teve mais importância para as bases da tecnologia foi o militar porque as mensagens que deveriam ser enviadas eram entregues a auxiliares com uma remuneração muito baixa, estes se encarregavam de criptografá-las e transmiti-las. Como o volume de mensagens era elevado, isso impedia que o trabalho de criptografia e transmissão fosse realizado por alguns poucos especialistas. Como o risco de um auxiliar de criptografia ser captura existia, isso fez com que os códigos criptográficos tivessem que ser alterados com maior freqüência (TANENBAUM, 2003).

A criptografia visa à confidencialidade das informações que estão saindo de uma origem até o seu destino. Também garante a integridade, autenticação e controle de acesso.

As chaves utilizadas na criptografia devem ser de conhecimento tanto da origem quanto do destino. Isso deve acontecer porque ao enviar uma mensagem a origem utiliza um chave para criptografar a mensagem, se o destino não possuir a mesma chave ele não conseguirá desencriptografar a mensagem, fazendo com que esta comunicação não tenha sentido.

A forma mais antiga de realizar a criptografia, que também é conhecida como criptografia de chave compartilhada ou criptografia de chave secreta, possui dois elementos básicos: Um algoritmo e uma chave que deve ser compartilhada entre a origem e o destino, por este motivo este método recebe o nome e criptografia de chave compartilhada ou criptografia simétrica.

Quando ocorre a necessidade de comunicação entre duas partes a primeira tarefa a ser realizada é realizar um acordo de qual algoritmo irão utilizar nesta comunicação. A troca de informações para decidir qual chave utilizar pode ocorrer em uma rede não segura, pois a informação de qual chave utilizar não interfere na segurança do sistema, uma vez que a responsabilidade da segurança é da chave que será utilizada.

Após a escolha da chave ser definida e aceitação ocorrer por ambos os lados da comunicação, o sistema pode proceder com a codificação das mensagens a serem enviadas. O processo de criptografia ocorre com a inserção da mensagem original e a chave compartilhada em uma função criptográfica. Após a execução desta função o resultado obtido é um texto cifrado que pode ser transmitido por uma rede não segura. O destino realiza o processo inverso para que a mensagem original possa ser processada.

Também existem as chaves assimétricas que trabalham com duas chaves distintas, uma denominada chave privada e outra denominada chave publica. Neste método a origem deve criar uma chave de codificação e enviar ao seu destino. Essa é a chave publica. Outra chave deve ser criada para a decodificação. Esta recebe o nome de chave privada. Neste tipo de comunicação a chave publica criada por um sistema é utilizada para que outros sistemas enviem mensagens a ele, pois somente ele tem a chave privada e somente ele conseguir realizar a decriptografia destas mensagens.

Entre os métodos mais conhecidos de chaves assimétricas está o *Rivest, Shamir and Adleman* ou RSA. Neste algoritmo são utilizados números primos da seguinte forma: é realizada uma multiplicação de dois números primos para que seja obtido um terceiro valor. Para se obter quais são os dois números primos utilizados na multiplicação é necessário realizar uma fatoração e, neste caso, é considerado uma tarefa muito difícil. Se forem utilizados dois números primos grandes é necessário utilizar muito processamento para descobri-los, tornando esta tarefa

praticamente inviável. Resumindo a chave privada no RSA são os dois números e a chave pública é o resultado obtido nesta multiplicação.

Além do RSA existem outros métodos utilizados na geração das chaves públicas como, por exemplo, o *Diffie-Hellman, o* ElGamal, o *Schnorr* e o *Digital Signature Algorithm* (DSA), os três últimos são utilizados em assinaturas digitais que será abordado no item 3.4 sobre autenticação.

2.2.4 Autenticação

O significado de autenticação é o ato de confirmar que alguém ou algo é verdadeiro, autêntico. No contexto de redes de computados o conceito de autenticação é amplamente utilizado para atestar que um programa ou página da internet é confiável.

A maneira como os computadores validam sua identidade varia. Entre os mais utilizados estão o uso de senhas, certificados digitais, números especiais, entre outros tipos de dados.

A maneira de autenticação mais conhecida, e utilizada, é o uso de senhas para a realização de *logins*. O conhecimento de uma senha é suficiente para atestar que o usuário é legítimo. Porém o uso de senhas não garante que outros usuários consigam obtê-las ou adivinhá-las. Por este motivo outros métodos de autenticação, via transações de internet, são utilizam processos mais rigorosos para autenticar os usuários, um exemplo deles e a certificação digital.

2.2.4.1 Certificados Digitais

A certificação digital é um arquivo eletrônico que contêm, dentre outras informações, o nome do usuário, uma chave pública. Estas informações são referentes à entidade pela qual este certificado foi emitido. Um certificado é uma credencial, fazendo uma analogia a documentos impressos pode-se citar a licença de motorista, cartão de seguro social, certidão de nascimento, dentre outros. Cada um destes tem um pouco de informação que podem identificar uma pessoa.

A certificação digital é utilizada para associar uma empresa a uma chave pública. Este certificado é por uma autoridade certificadora que é a própria entidade

que emitiu este certificado. Existe também uma assinatura associada a cada certificado assinado por outros, estes assinam um certificado por confiar na emissora do mesmo.

O objetivo das assinaturas digitais são declarar que a informação do certificado foi atestada por outra entidade. Com esta assinatura o certificado não recebe uma autenticidade total, apenas garante que a informação de identidade assinada esta ligada a uma chave pública.

O formato de certificado mais utilizado é o X.509 que obedece o patrão *International Telecommunication Union Telecommunication* (ITU-T) X.509. Este padrão contém campos contendo informações sobre um usuário ou dispositivo e sua correspondente chave pública. Este padrão define qual informação está contida neste certificado e descreve a forma de codificação.

Os certificados X.509 possuem os seguintes campos:

Número de Versão: contém a versão do certificado X.509;

A chave pública: especifica qual sistema de criptografia pertence a chave e quais são os parâmetros associados.

O número de série: é utilizado para distinguir este de outros certificados.

Identificação única do possuidor: Esta identificação tem que ser única na internet. Identifica o nome, organização, unidade, país, dentre outros.

Validade do certificado: indica até quando o certificado é valido.

Identificação do emissor: o nome da entidade que assinou o certificado.

Assinatura digital do emissor: assinatura da entidade que emitiu o certificado.

Algoritmo de assinatura: Identifica o algoritmo utilizado para assinar o certificado.

2.3 RADIUS

O Remote Authentication Dial In User Service (RADIUS) é um protocolo que é utilizado para gerenciar o acesso a diversos serviços de rede. O protocolo RADIUS define um padrão para ser utilizado na troca de informações entre um *Network Access Server* (NAS) e um servidor de autenticação, autorização e informações de gerenciamento de contas (auditoria), ou também conhecido como servidor de

Authentication, *Authorization* e *Accounting* (AAA).

A autenticação é o processo de reconhecer usuários que são verdadeiros dentro de uma rede, normalmente ocorre entre um cliente e um servidor. A autenticação ocorre através da apresentação de uma identidade e as credenciais correspondentes.

A autorização é a associação de alguns privilégios para um usuário, baseados nas informações utilizadas para autenticar. Dentre as políticas utilizadas no processo de autorização estão a restrição de utilização em determinados horários, restrições relacionadas ao grupo que o usuário pertence e proteção, que evita diversas conexões simultâneas realizadas pelo mesmo usuário.

A auditoria está relacionada a utilização e o comportamento dos usuários e de que forma estes consomem os recursos da rede. Estas informações são utilizadas para gerenciar os recursos da rede, para o planejamento dos setores da rede que precisam ser melhorados e para a cobrança de serviços utilizados pelos usuários.

O servidor RADIUS gerencia de forma eficiente diversos perfis de usuários para realizar a autenticação dos mesmos. Também fornece informações de configuração que especificam quais os tipos de serviços que serão entregues e quais as políticas de cada um destes tipos. Estes parâmetros são utilizados para garantir o uso apropriado dos recursos disponíveis na rede.

Alguns exemplos de serviços que utilizam o RADIUS são as redes sem-fio, conexões DSL e VPNs. Existem soluções pagas utilizadas para implementar o RADIUS, mas neste trabalho será utilizada uma solução de código aberto de qualidade, que é o FreeRadius.

As principais vantagens na utilização do protocolo RADIUS, dentre uma série de funcionalidades que tornam este tipo de protocolo eficiente, são as seguintes:

Modelo Cliente/Servidor: O NAS (roteador *wireless*, por exemplo) é considerado um cliente para o servidor RADIUS. O cliente é responsável por enviar todas as informações dos usuários que querem utilizar o seu serviço ao servidor RADIUS, que irá verificar a autenticidade dos usuários finais e informar a sua validade para o NAS, que por sua vez envia uma resposta aos usuários finais. O NAS apenas recebe alguns parâmetros do servidor RADIUS para controlar o uso dos recursos disponíveis, como por exemplo, qual é o tempo máximo que o usuário deverá ficar conectado e quais são os limites de acesso para este usuário.

Segurança: As transferências de informações entre o cliente (NAS) e o servidor RADIUS são autenticadas através de um segredo compartilhado (*shared secret*). Este segredo é conhecido previamente, tanto pelo NAS quanto pelo servidor RADIUS e garante a autenticidade do usuário em uma determinada requisição.

Flexibilidade e Adaptabilidade: Diversos dispositivos de rede não conseguem armazenar uma grande quantidade de usuários em sua base de dados. Utilizando o RADIUS estes dispositivos podem permitir a autenticação de diversos usuários, atuando como *proxy* para o servidor RADIUS, que por sua vez possui uma maior capacidade de processamento.

Protocolo extensível: O protocolo RADIUS possui um campo de atributos de tamanho variável em seus pacotes que permite que novos atributos sejam adicionados sem que a estrutura padrão do protocolo seja alterada.

Compatibilidade: O servidor RADIUS pode utilizar um banco de dados de usuários de fontes externas para realizar a autenticação dos usuários, como por exemplo, banco de dados *Structured Query Language* (SQL), *Kerberos* ou LDAP. Este último será utilizado no decorrer deste trabalho.

Atualmente o protocolo RADIUS é utilizado em uma ampla gama de serviços, dentre os mais comuns está o protocolo de autenticação IEEE 802.1X, freqüentemente é utilizado em redes sem fio com a finalidade de melhorar a criptografia padrão do *Wired Equivalency Privacy* (WEP) e também utiliza outros métodos de autenticação como o EAP e algumas de suas variantes. Como os servidores RADIUS atuam como *proxys* em dispositivos de rede, por exemplo, roteadores sem-fio, ele permite que estes equipamentos autentiquem e mantenham um gerenciamento de acesso a um grande número de usuários, fazendo com que a memória utilizada nestes sistemas embarcados não seja desperdiçada com estas tarefas.

2.3.1 Funcionamento do Protocolo RADIUS

Quando um usuário necessita utilizar um determinado serviço de rede ele envia as suas informações para o NAS, que por sua vez solicita a autenticação deste usuário ao servidor RADIUS, em forma de uma mensagem de requisição, ou uma *Access-Request message*. Após o recebimento da solicitação do cliente (NAS),

o servidor RADIUS realiza a autenticação do usuário e informa ao NAS as configurações e políticas a serem liberadas para o usuário final. Se a resposta do servidor RADIUS for de que o usuário foi autenticado, o NAS fornece os serviços solicitados pelo usuário de acordo com as políticas de autorização informadas.

Como o protocolo RADIUS é extremamente flexível e possui diversas tecnologias que são agregadas, o servidor RADIUS pode ser utilizado também como um cliente *proxy* que, ao invés de autenticar os usuários ele envia os pedidos de acesso à outro servidor remoto. Nesta configuração o servidor RADIUS é o responsável por intermediar as mensagens trocadas entre o cliente e o servidor remoto. Um servidor pode ser configurado para realizar a autenticação em determinadas situações localmente e servir como um *proxy* de servidores remotos em outras.

O pacote de dados do protocolo RADIUS possui os campos de código, identificador, comprimento, autenticador e atributos (vide figura 6).

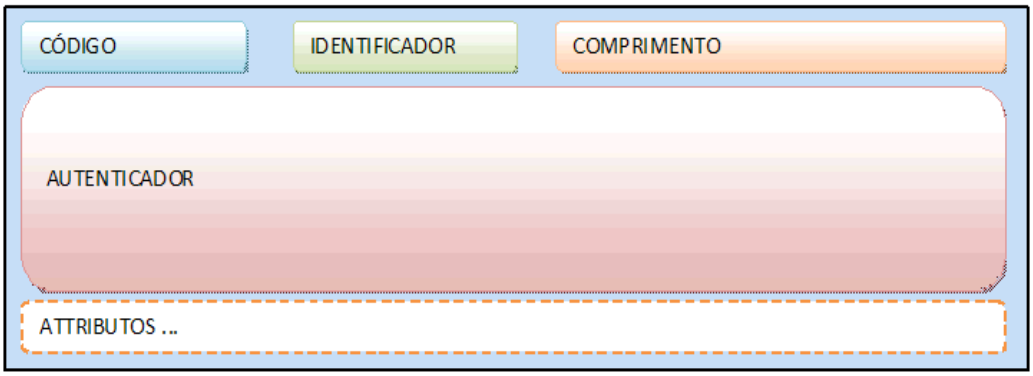

Figura 6 – Pacote RADIUS
Fonte: PACOTE DE DADOS RADIUS

O campo de código possui o tamanho fixo de um octeto e é utilizado para realizar a identificação do tipo de pacote RADIUS que está sendo enviado/recebido. Se o valor que estiver dentro do código for um valor desconhecido, o pacote é descartado sem que nenhuma informação seja enviada a origem. Na tabela 1 estão descritos os códigos que são mencionados na RFC 2138 referente à implementação do RADIUS.

CÓDIGO	DESCRIÇÃO
1	*Access-Request*
2	*Access-Accept*
3	*Access-Reject*
4	*Accounting-Request*
5	*Accounting-Response*
11	*Access-Challenge*
12	*Status-Server (experimental)*
13	*Status-Client (experimental)*
255	*Reserved*

Tabela 1 - Códigos RADIUS
Fonte: RFC 2138

O campo identificador possui um tamanho fixo de um octeto e sua principal função é identificar as requisições e respostas.

O comprimento tem tamanho fixo de dois bytes e informa o tamanho do pacote RADIUS. Neste campo estão contempladas todas as informações que estão neste pacote, incluindo o código, identificador, o próprio comprimento, autenticador e os atributos. Se o tamanho marcado neste campo for menor que o tamanho real do pacote, os bits posteriores ao tamanho citado serão ignorados e se o tamanho do pacote for menor do que o especificado neste campo, ele será descartado. Os limites de tamanho dos pacotes RADIUS variam entre 20 e 4096 octetos.

O campo de autenticação possui o tamanho de 16 bytes. Neste campo estão incluídos os valores utilizados para autenticar as respostas do servidor e também é utilizado algum algoritmo de ocultação de senha.

O campo de atributos carrega informações referentes à autenticação ou autorização. Neste campo estão detalhes mais específicos de uma requisição ou de uma determinada resposta.

2.4 LDAP

O *Lightweight Directory Access Protocol* ou LDAP é um protocolo que atua sobre uma camada TCP/IP e permite organizar os recursos de uma rede de forma hierárquica, semelhante a uma árvore de diretórios, onde o principal é o diretório raiz, sendo seguido pela rede de uma entidade, pelos seus departamentos e por fim pelos computadores de funcionários e pelos recursos de rede (LDAP, 2005).

Um diretório dentro do LDAP, ao contrário do que o nome sugere, não são pastas de um disco rígido ou outro armazenador de arquivos, por exemplo um *pendrive*. Esta designação de diretório é utilizada somente por ser similar com a estrutura de armazenamento de informações. O diretório no protocolo LDAP é uma base especializada e otimizada para leitura. Esta estrutura foi criada para ser mais lida do que atualizada, pois as informações que são guardadas em diretórios tendêm a ser mais estáticas do que as que são armazenadas em um banco de dados relacional, em que o número de consultas pode ser igual ao de atualizações.

O protocolo LDAP foi desenvolvido em 1993 pela Universidade do Michigan (O PROTOCOLO LDAP, 2009) e tinha como objetivo substituir o *Directory Access Protocol* (DAP), que era utilizado no modelo OSI. O LDAP é uma versão mais rápida do DAP, por isso o nome *Lightweight* (leve).

O LDAP é utilizado para armazenar informações estáticas. Ele é estruturado como diretório otimizado para buscas. Esta forma de estrutura em árvore é útil para estruturas organizacionais de conceituação. Uma de suas principais vantagens é a facilidade na busca de informações. Com o sobrenome de um funcionário é possível localizar dados sobre ele, como departamento, projetos em que esta atuando, telefone e demais informações incluídas no sistema, além de arquivos que foram criados por ele ou que lhe façam alguma referência.

O protocolo LDAP possui escalabilidade. É possível que servidores sejam replicados para *backup* ou balanceamento de carga e incluir novos servidores de forma hierárquica. Neste caso a organização dos servidores é similar ao DNS, um servidor principal, ou raiz, é definido e a partir dele é possível se ter vários níveis de sub-servidores, além de *mirrors* do servidor principal.

O protocolo LDAP é um padrão aberto e pode ser utilizado sobre qualquer rede TCP/IP, isto permite que existam produtos para diversas plataformas. Um dos mais utilizados é o OpenLDAP, que é *opensource* e será utilizado na continuidade deste trabalho. Maiores detalhes da instalação e configuração serão abordados no item de instalação do OpenLDAP.

2.4.1 Funcionamento do Protocolo LDAP

Dentro de um diretório LDAP a parte mais importante é o espaço de nomes. O

espaço de nomes referencia cada entrada num diretório e é hierárquico. As entradas são organizadas numa estrutura chamada *Directory Information Tree* (DIT). Dentro da estrutura da DIT cada entrada recebe um nome distinto, ou *Distinguished Name* (DN), que é um nome único utilizado para identificar cada entrada. Os DNs são constituídos por uma seqüência de nomes distintos relativos (*Relative Distinguished Names* – RDN). Um RDN representa um ramo da árvore e um DN é a concatenação de vários RDNs. Realizando uma analogia com uma lista telefônica a cidade e o nome de uma pessoa seriam, cada um, um RDN e a associação dos dois é o DN.

Cada entrada em uma DIT pode pertencer a uma ou mais classes de objetos. Uma classe de objeto é utilizada para descrever o conteúdo e a finalidade de um objeto. Na classe estão contidos atributos obrigatórios e opcionais que cada objeto deve possuir. Com isso o protocolo LDAP se assemelha a programação orientada a objetos e suporta herança simples e múltipla e classes abstratas.

2.4.2 Fluxo de Chamadas LDAP

Abaixo estão às ações que devem ser realizadas pelo cliente e servidor LDAP para que uma consulta seja realizada com sucesso:

1º) O cliente deve estabelecer uma conexão com o servidor LDAP. Este processo é conhecido como *binding*;

2º) O cliente tem a opção de fornecer um usuário e uma senha para se autenticar no servidor através de SSL/TLS ou estabelecer uma sessão anônima com permissões padrão;

3º) O cliente realiza operações sobre os dados. O servidor LDAP libera as operações de leitura e atualização, conforme permissões do cliente e permite que pesquisas utilizando alguns critérios (filtros) sejam realizadas. O cliente pode especificar que parte do DIT que pesquisar e se deseja receber alguma informação no retorno de sua consulta;

4º) O cliente finaliza a sessão (*unbindig*).

3 DESENVOLVIMENTO

Este capítulo tem como objetivo identificar todos os passos da instalação e configuração dos servidores RADIUS e LDAP para que ambos possam trabalhar em conjunto. Não será abordada neste capítulo a instalação do sistema operacional Linux Debian.

3.1 INSTALAÇÃO SERVIDOR RADIUS

O software que será utilizado para instalar o servidor RADIUS será o Freeradius, que é um software *opensource* e não há necessidade de que uma licença seja adquirida para que este possa ser utilizado.

O pacote Freeradius deve ser instalado através do comando *apt-get install freeradius*. Como o servidor Radius irá se conectar com o servidor LDAP também é necessário baixar o módulo do Freeradius que será utilizado na conexão com o LDAP, o módulo freeradius-ldap. Para otimizar a instalação ambos os softwares podem ser instalados juntos através do comando *apt-get install freeradius freeradius-ldap*, após a execução do comando é necessário confirmar a continuação da instalação, conforme pode ser observado na figura 7, depois que a confirmação é realizada a instalação é concluída e o servidor RADIUS é iniciado.

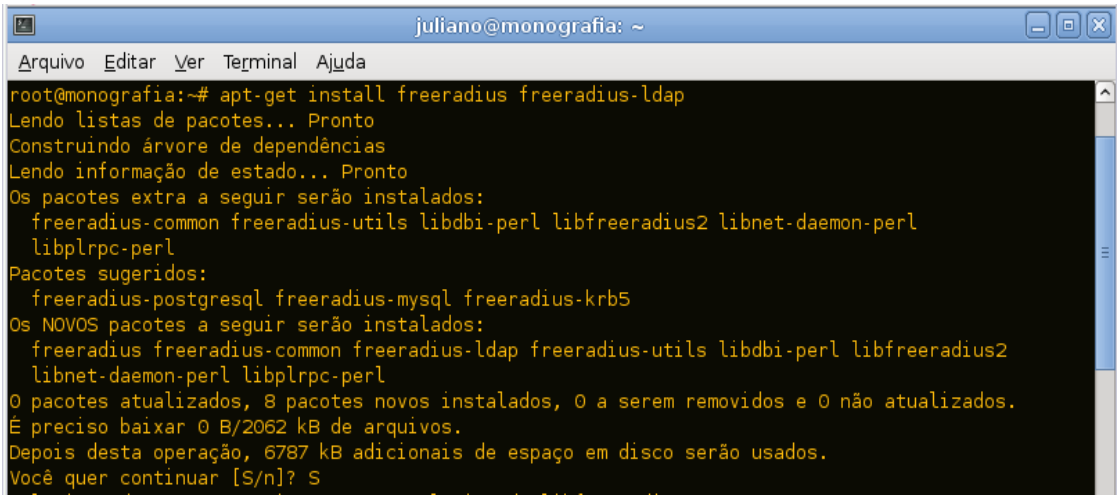

Figura 7 - Instalação Freeradius e Módulo Freeradius-Ldap
Fonte: Autoria própria

3.1.2 Testando o Freeradius

Após a instalação do Freeradius pode-se realizar um teste para verificar se o servidor RADIUS está funcionando normalmente. Para isso é necessário permitir o acesso de um IP, ou uma rede inteira, no servidor. Para realizar a permissão de um IP o arquivo */etc/freeradius/clients.conf* deve ser editado conforme a figura 8.

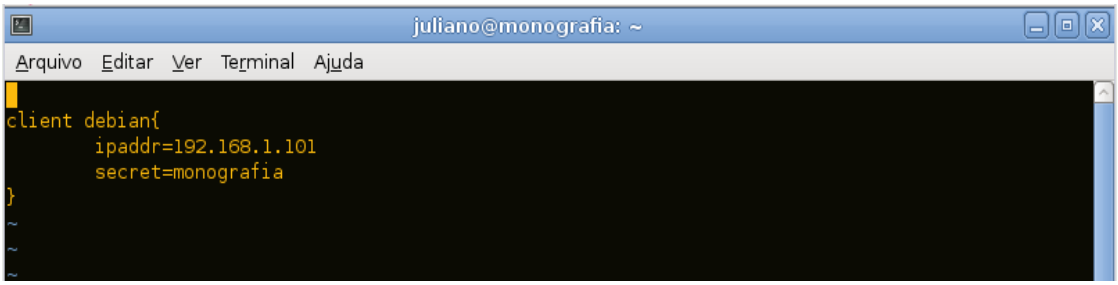

Figura 8 - Configuração de acesso ao RADIUS
Fonte: Autoria Própria

A configuração mostrada na figura 8 libera o acesso ao NAS com endereço 192.168.1.101 através da senha “monografia”. O nome debian apenas foi dado para identificar o NAS que esta realizando a solicitação.

Com o acesso liberado pelo servidor RADIUS ao NAS, o próximo passo é criar um usuário para teste. O arquivo que possui os usuários é o */etc/freeradius/users*. A criação do usuário é simples, basta inserir no inicio do arquivo o comando *usuário Cleartext-Password := “password”*. Para a realização do teste foi criado o usuário radius com a senha freeradius (vide figura 9). A informação *Cleartext-Password* é utilizado para enviar a senha sem criptografia, ou seja, em texto transparente.

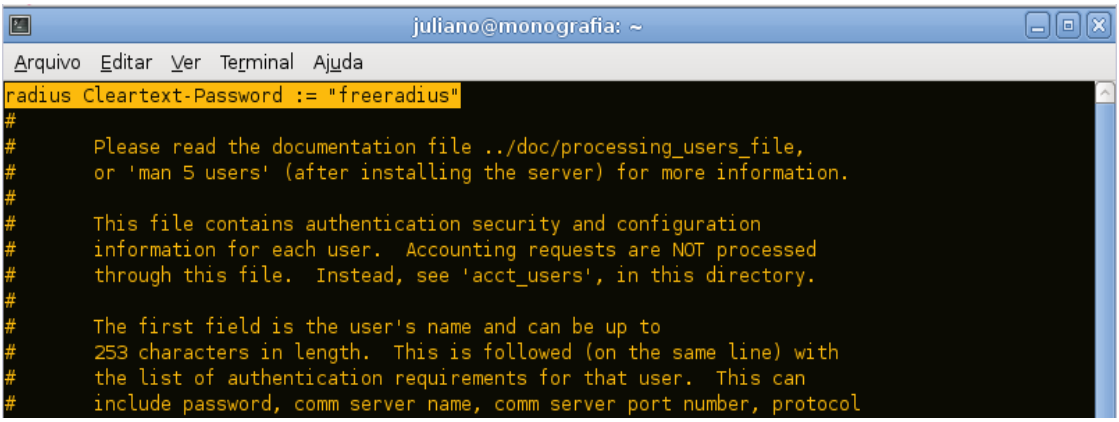

Figura 9 - Criação de usuário no RADIUS
Fonte: Autoria Própria

Após as alterações citadas serem realizadas, é necessário iniciar o servidor

Freeradius. O processo de inicio pode ser realizado de três formas diferentes, através do comando */etc/init.d/freeradius start*, utilizado com mais freqüência, também pelo comando *service freeradius start* ou pelo comando *freeradius –X*. O último comando é utilizado quando é necessária a visualização dos *logs* de *debug* do servidor RADIUS.

Com o servidor RADIUS iniciado o teste pode ser realizado apenas pela máquina 192.168.1.101 solicitando acesso ao servidor, pois este foi o único host que recebeu permissão no arquivo */etc/freeradius/clients.conf* para realizar uma consulta.

Para verificar a conectividade e a resposta do servidor RADIUS é necessário executar o comando *radtest usuário senha ip_solicitante porta chave_secreta*. Com a configuração que foi realizada o comando para realização do teste é o *radtest radius freeradius 192.168.1.101 1812 monografia* e o resultado obtido é mostrado na figura 10.

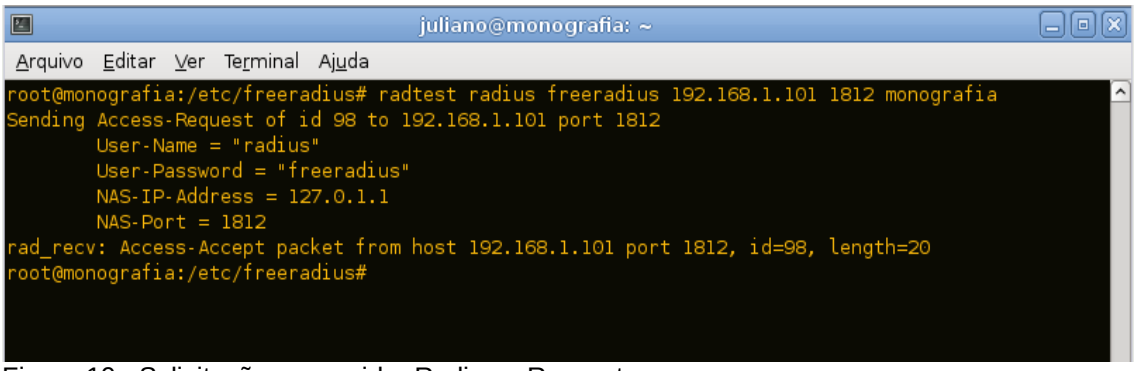

Figura 10 - Solicitação ao servidor Radius e Resposta
Fonte: Autoria Própria

Como foi observado o acesso solicitado pela mensagem *Access-Request* foi aceito pelo servidor RADIUS através da resposta *Access-Accept*. Na figura 11 temos a saída do debug.

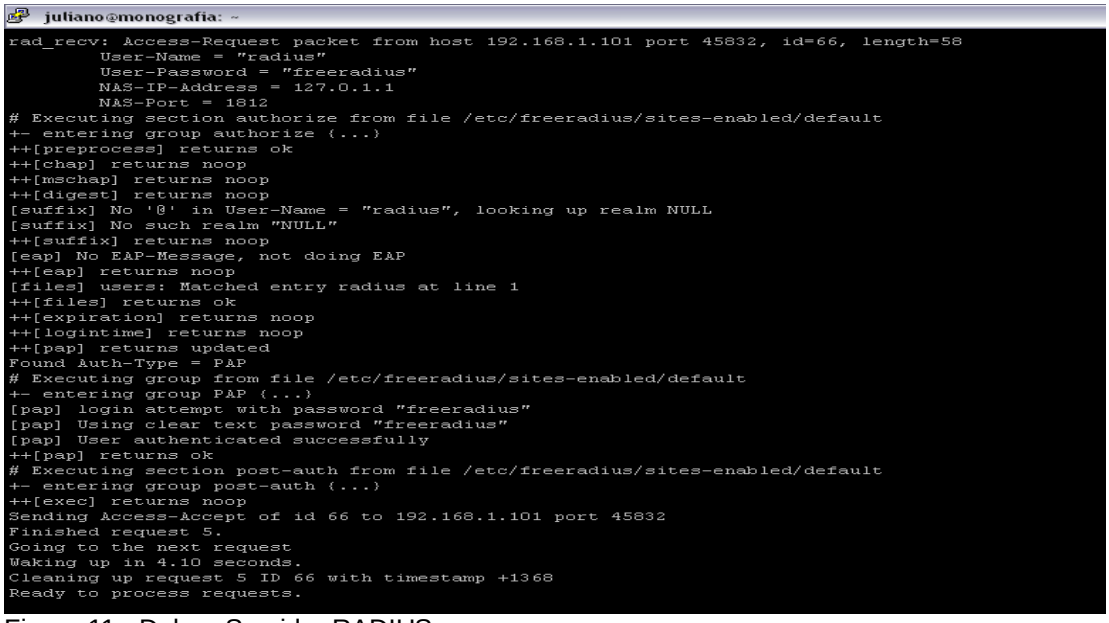

Figura 11 - Debug Servidor RADIUS
Fonte: Autoria Própria

Pode ser analisada também a resposta a um usuário inexistente ou uma senha incorreta na figura 12 e o seu respectivo *Debug* na figura 13. Como pode ser observado o usuário que solicitou acesso (teste) não existe nos cadastros do servidor RADIUS, portanto a resposta enviada a solicitação *Access-Request* é um *Access-Reject*. Na figura 13 pode se observar que o servidor RADIUS procura por todos os tipos de protocolos de autorização e por fim imprime a mensagem "*Failed to authenticate the user*", ou seja, o usuário não pode obter acesso do NAS ao serviço solicitado.

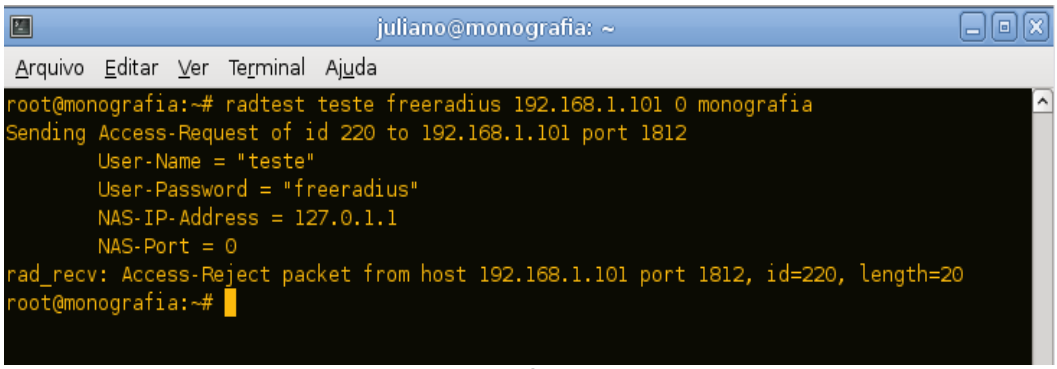

Figura 12 – Solicitação de Acesso Para Usuário Inexistente
Fonte: Autoria Própria

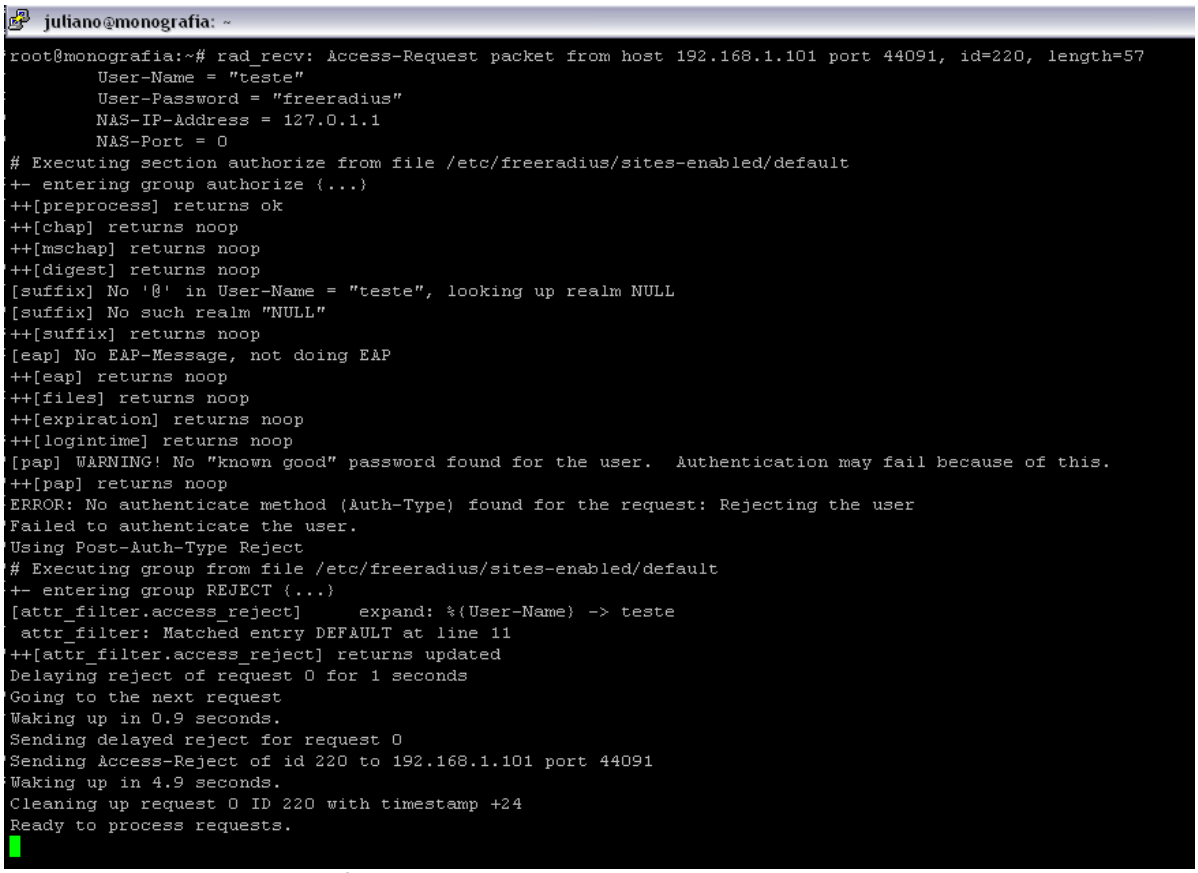

Figura 13 - Debug Para Usuário Inexistente
Fonte: Autoria Própria

3.2 INSTALAÇÃO DO SERVIDOR LDAP

Na instalação do servidor LDAP será utilizado o software OpenLdap, este também é um software *opensource* e não necessita o pagamento de licenças para o seu uso por se tratar de um software livre.

Para iniciar a instalação é necessário executar, como root, o comando *apt-get install slapd ldap-utils*. O pacote *Ldap-utils* contém os utilitários utilizados pelo servidor LDAP. Como acontece com o servidor RADIUS o OpenLdap também solicita uma confirmação antes do download dos pacotes necessários para a instalação.

Após a execução do comando será solicitada a senha do administrador do servidor LDAP (figura 14). Após isso o sistema é instalado e iniciado.

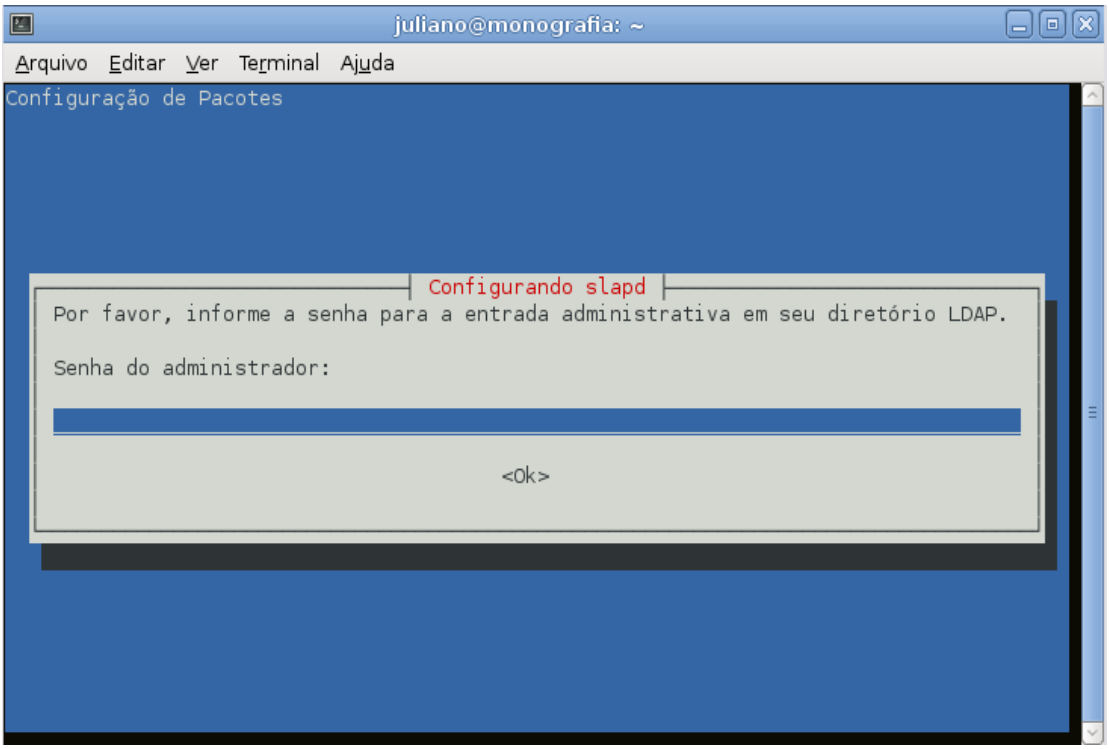

Figura 14 - Solicitação de Senha do Servidor LDAP
Fonte: Autoria Própria

Para saber se o servidor LDAP irá aceitar conexões na porta 389 é necessário verificar se o sistema está ouvindo nesta porta através do comando "*netstat –ant | grep 389*", conforme a figura 15.

Figura 15 - Resposta do comando Netstat
Fonte: Autoria Própria

Quando o openldap é instalado no Debian há um wizard que auxilia na configuração do servidor LDAP. Para iniciar este wizard é necessário executar o comando *dpkg-reconfigure slapd*. Após a execução do comando a tela da figura 16 é apresentada solicitando o cancelamento do wizard, a opção "Não" deve ser selecionada.

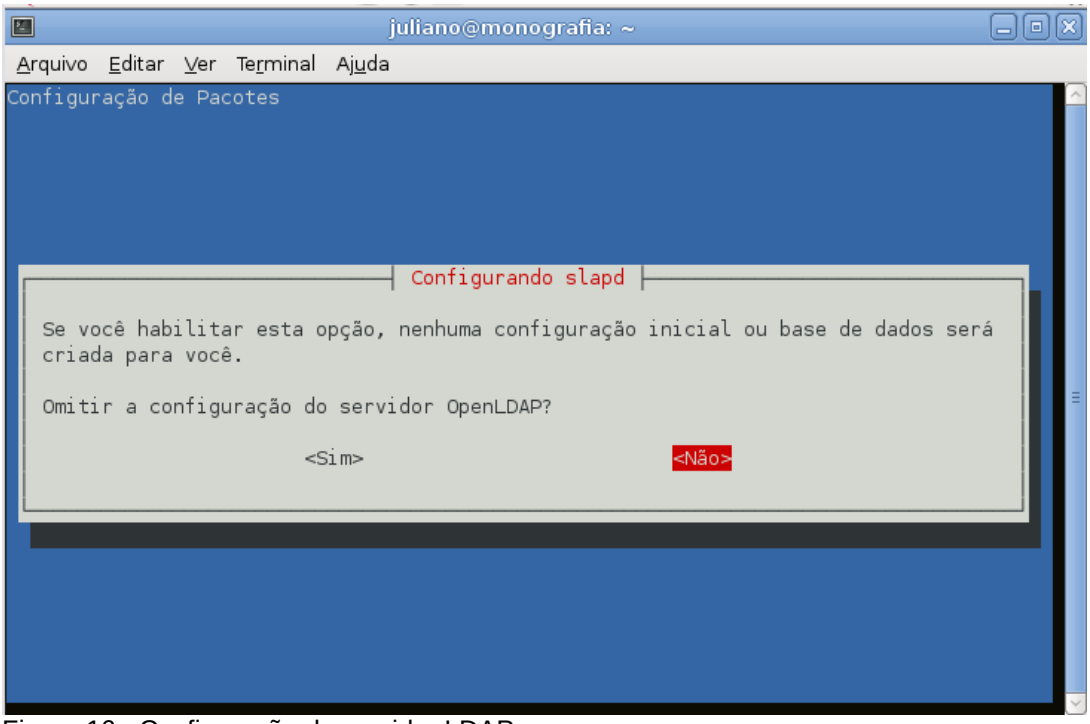

Figura 16 - Configuração do servidor LDAP
Fonte: Autoria Própria

A próxima etapa é definir um nome de domínio para construir a base de dados DN do diretório LDAP. Neste exemplo será utilizado o domínio dominiolocal.loc (figura 17).

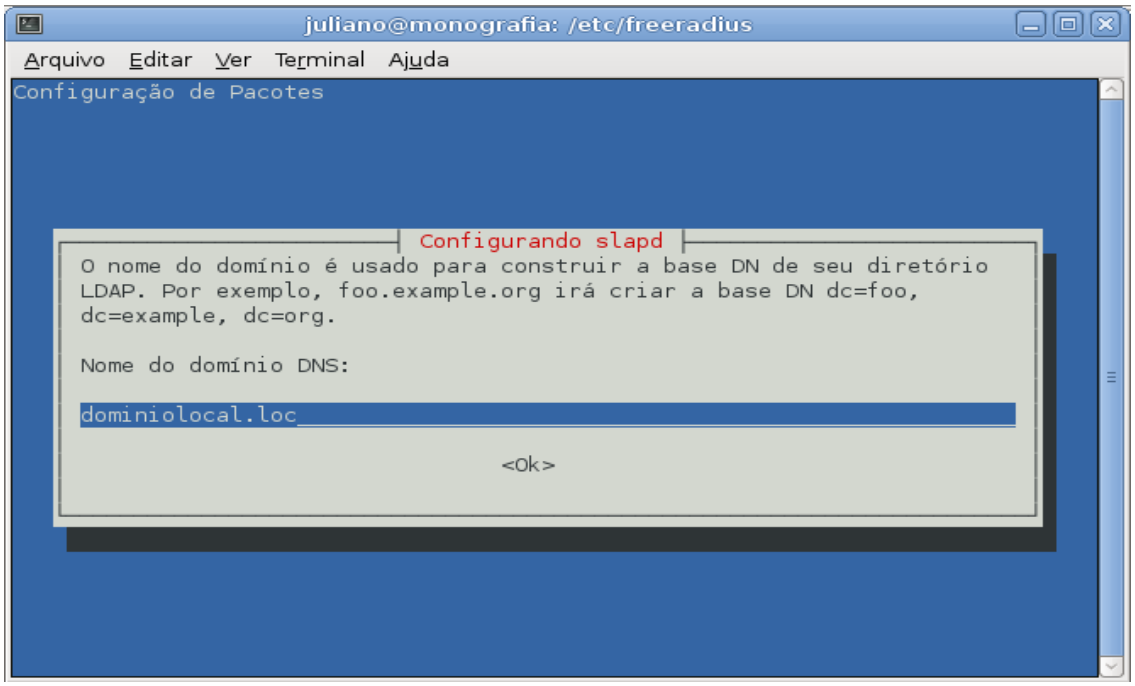

Figura 17 - Base DN para o Diretório LDAP
Fonte: Autoria Própria

Neste ponto deve ser definido um nome para a empresa ou organização. O

nome utilizado será “*People*”, conforme a figura 18.

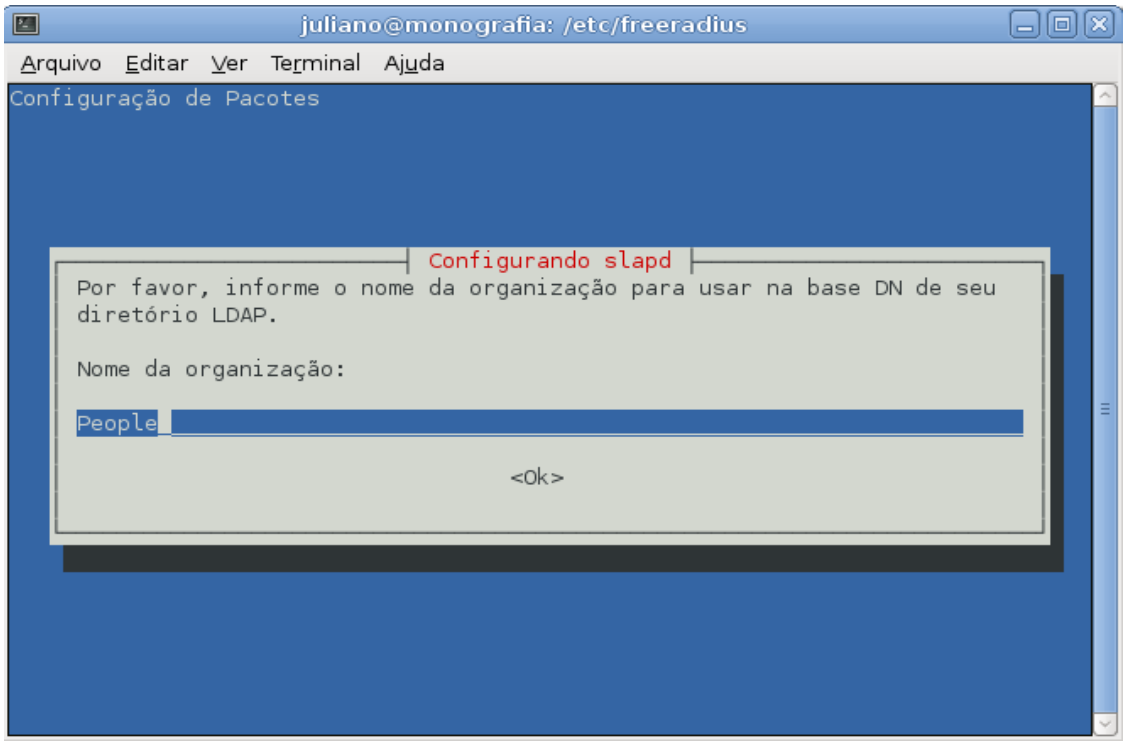

Figura 18 - Nome da organização
Fonte: Autoria Própria

A próxima etapa é a escolha de uma senha para o administrador do diretório que foi criado anteriormente (figura 19). É necessário realizar a confirmação da senha.

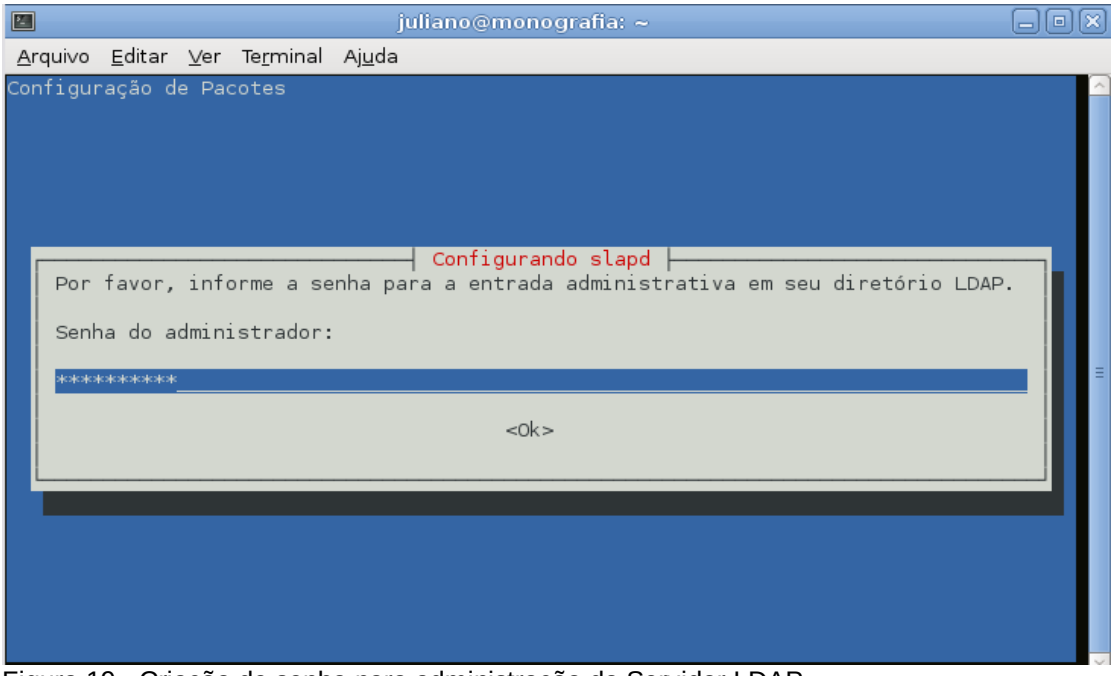

Figura 19 - Criação de senha para administração do Servidor LDAP
Fonte: Autoria Própria

Nesta etapa é necessário selecionar a forma como os dados serão armazenados (vide figura 20). É possível selecionar a opção *Berkeley DataBase* (BDB) ou a opção *Hierarchical DataBase* (HDB). Ambas são semelhantes, porém a segunda é mais indicada por possuir suporte para a renomeação de sub-diretórios.

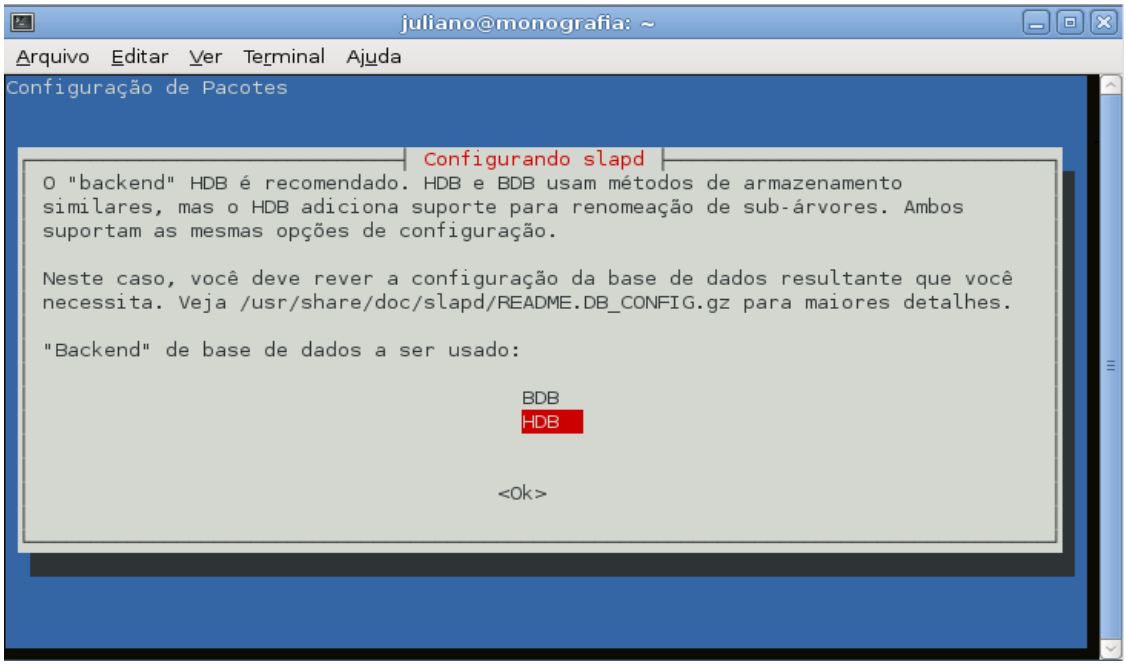

Figura 20 - Seleção de Método de Armazenamento LDAP
Fonte: Autoria Própria

A próxima opção apenas pergunta se quando o pacote *slapd* for removido a base de dados seja removida também. Neste caso a opção não foi escolhida, conforme a figura 21.

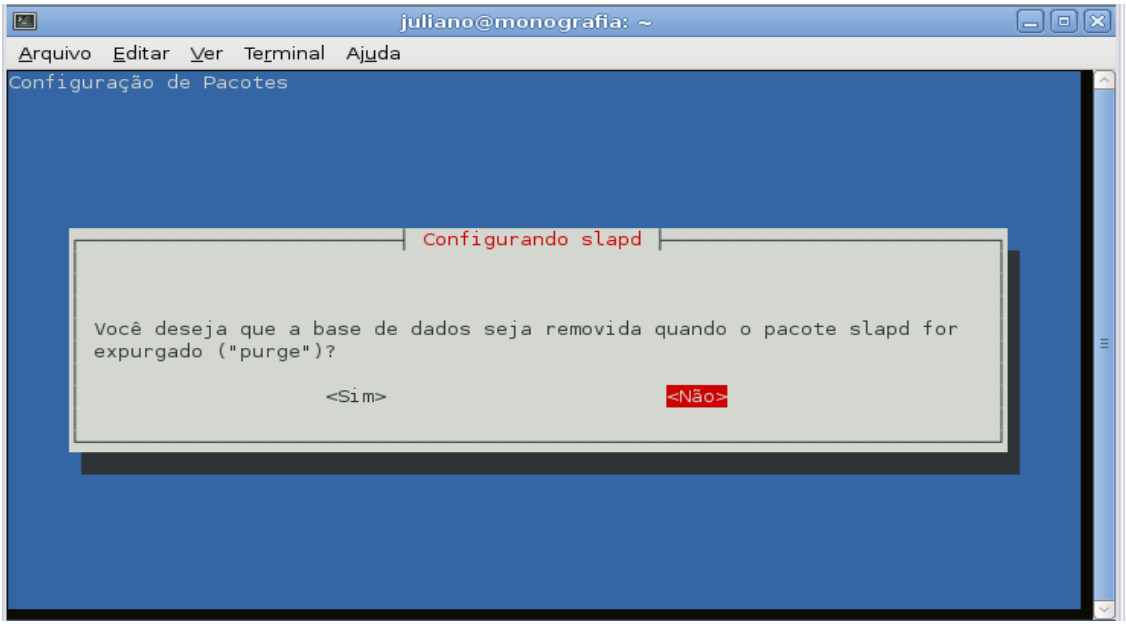

Figura 21 - Configuração Servidor LDAP
Fonte: Autoria Própria

Como o software OpenLdap foi instalado anteriormente o wizard identificou que há a arquivos que irão quebrar o processo de configuração e pergunta se é necessário remover estes arquivos. A resposta para este questionamento deve ser SIM (Figura 22).

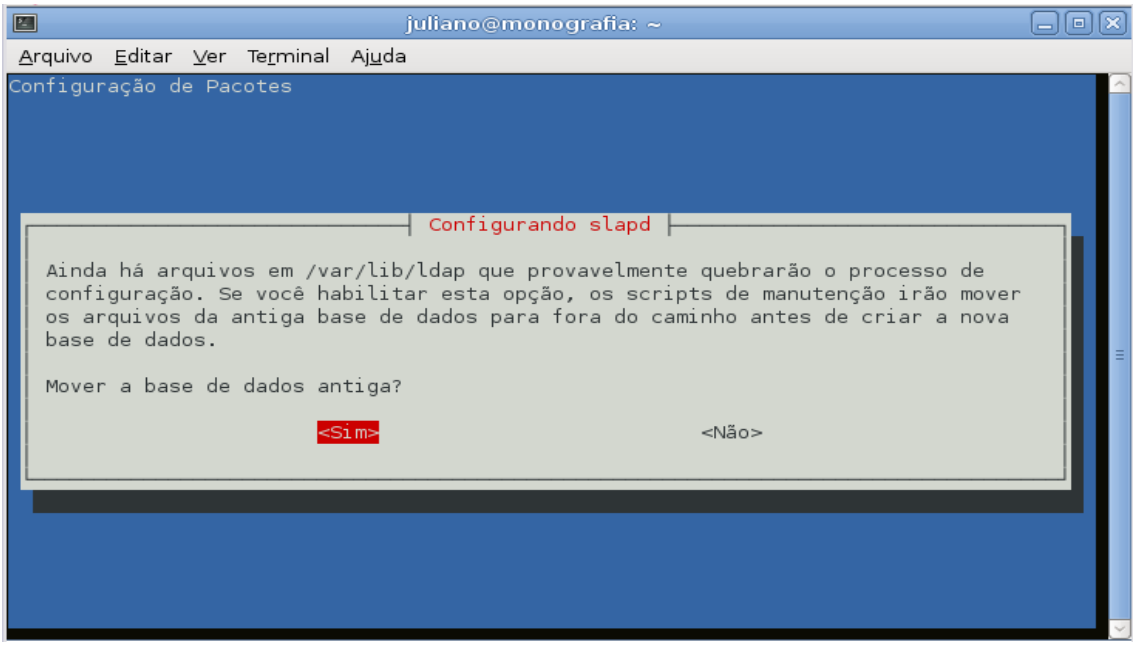

Figura 22 - Remoção de arquivos antigos LDAP
Fonte: Autoria Própria

A ultima pergunta do wizard verifica se a versão 2 do protocolo LDAP (LDAPv2) deve ser utilizada. Neste caso, tanto o FreeRadius quanto o OpenLdap estão em suas últimas versões e não há necessidade de se manter o suporte a esta versão (Figura 23). Esta versão só deverá ser utilizada quando programas antigos forem acessar o servidor LDAP.

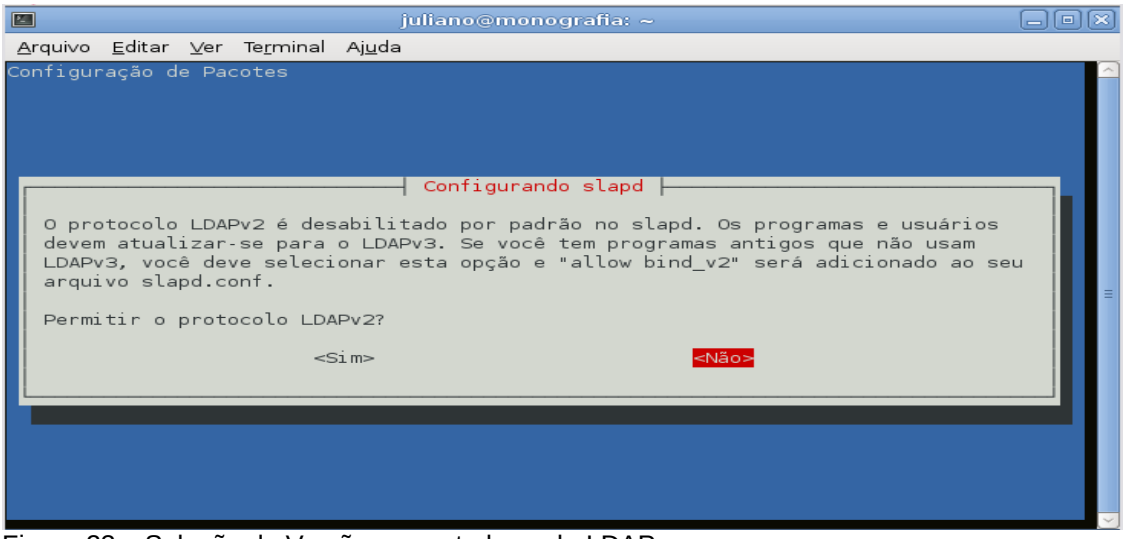

Figura 23 – Seleção de Versões suportadas pelo LDAP
Fonte: Autoria Própria

Após a instalação do servidor LDAP, é necessário que os usuários sejam criados. Para a criação de um usuário é necessário a criação de um arquivo com a extensão .ldif, parar o servidor ldap com o comando *service slapd stop* e executar o comando *slapadd –l arquivo.ldif*. Na figura 24 há um exemplo de um arquivo .ldif.

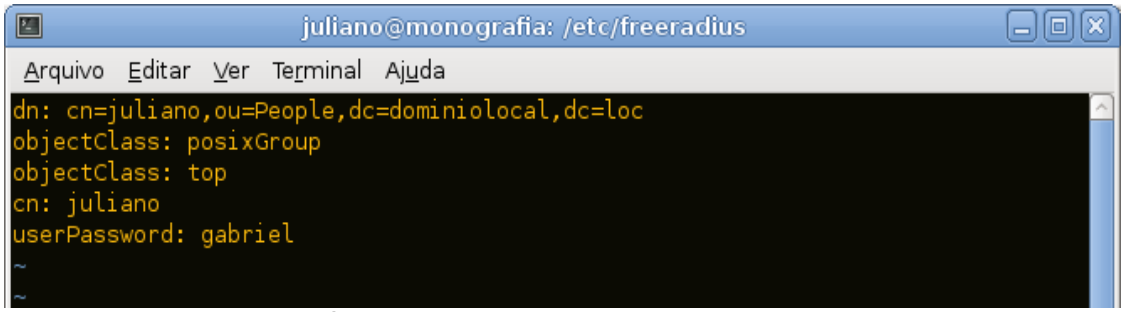

Figura 24 - Criação de Usuário no Servidor LDAP
Fonte: Autoria Própria

Após a inserção do usuário o servidor LDAP está configurado.

3.3 CONEXÃO SERVIDOR RADIUS COM SERVIDOR LDAP

Para realizar a conexão do servidor RADIUS com o servidor LDAP é necessário editar o arquivo de configuração *ldap*, que está localizado no diretório */etc/freeradius/modules/*, para adicionar as informações do servidor LDAP para que o RADIUS consiga acessá-lo. As informações que devem ser alteradas neste arquivo são as seguintes: *Server*, *basedn*, *filter*, e a *access_attr*. No exemplo configurado acima o Server deve ser igual a “dominiolocal.loc”, a *basedn* igual a “dc=dominiolocal,dc=loc”, o filter igual a “(uid=%u)” e o *access_attr* igual a “uid”. A informação uid significa *User Identify*.

Após estas alterações é necessário alterar o arquivo de autorização e autenticação do servidor RADIUS para que ele possa autenticar no servidor LDAP. O arquivo é o */etc/freeradius/sites-enable/default*. O arquivo deve estar configurado conforme a figura 25.

```
authorize {
    ldap
    expiration
    logintime
}

authenticate {
    Auth-Type LDAP {
        ldap
    }
}

preacct {
    preprocess
    acct_unique
    suffix
    files
}

accounting {
    detail
    unix
    radutmp
    attr_filter.accounting_response
}

session {
    radutmp
}

post-auth {
    Post-Auth-Type REJECT {
        attr_filter.access_reject
    }
}
```

Figura 25 - Arquivo de configuração servidor RADIUS
Fonte: Autoria Própria

3.4 TESTES DE CONEXÃO

Após a configuração de todos os arquivos a conexão deve estar estabelecida entre o servidor RADIUS e o servidor LDAP.

Para realização dos testes o mesmo comando utilizando anteriormente, o *radtest*, será utilizado neste ponto. Com base no usuário configurado anteriormente o comando será o seguinte *radtest juliano gabriel 192.168.1.101:1812 0 monografia*. Abaixo temos a figura 26 que mostra o que a conexão foi bem sucedida no servidor RADIUS.

```
Sending Access-Request of id 103 to 192.168.1.101 port 1812
        User-Name = "juliano"
        User-Password = "gabriel"
        NAS-IP-Address = 127.0.1.1
        NAS-Port = 0
rad_recv: Access-Accept packet from host 192.168.1.101 port 1812, id=103, length=20
```

Figura 26 - Conexão RADIUS
Fonte: Autoria Própria

Observando somente a figura 26 não há como afirmar que o usuário foi autenticado no servidor LDAP. Para constatar que a autenticação foi realizada pelo protocolo LDAP é necessário realizar a coleta do debug no servidor RADIUS, conforme a figura 27.

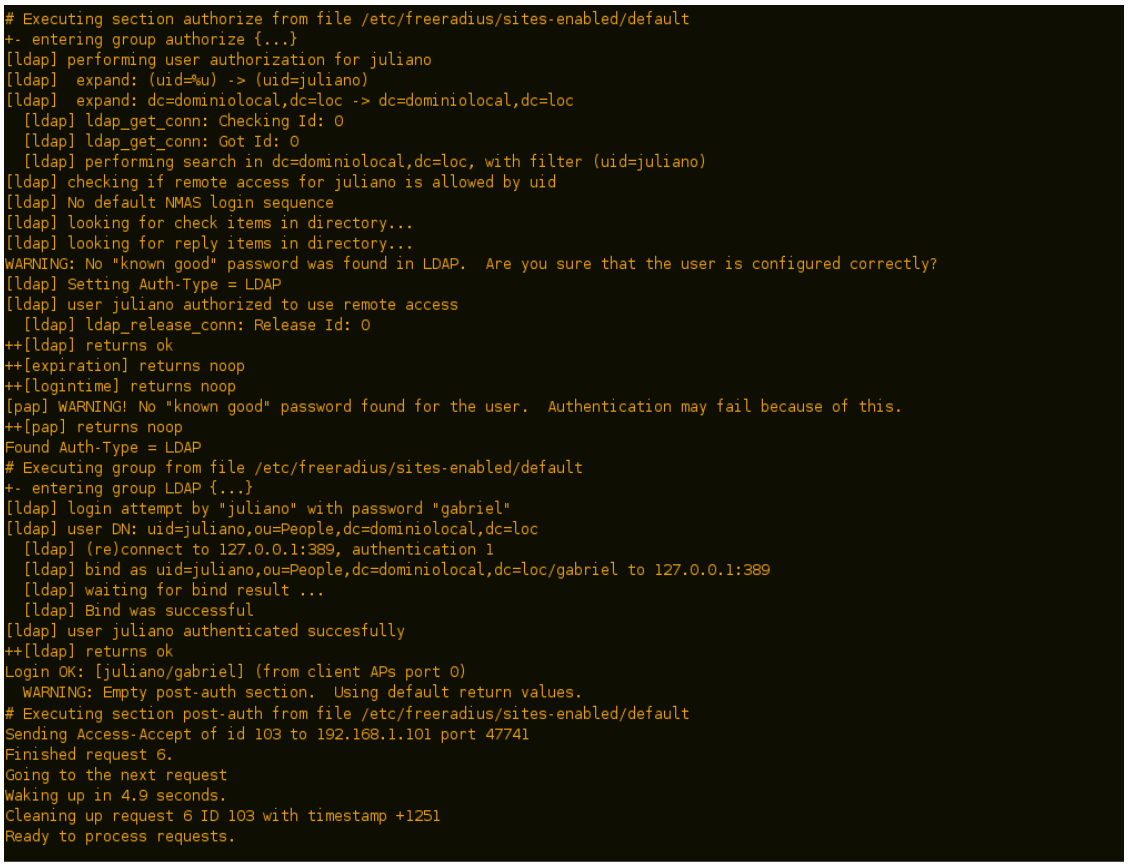

Figura 27 - Debug conexão RADIUS com LDAP
Fonte: Autoria Própria

No debug podemos visualizar que o servidor RADIUS está acessando a seção de autorização (*authorize*), dentro do diretório */etc/freeradius/sites-enabled/default*, e utilizando o protocolo LDAP para realizar a autenticação do usuário. A resposta que confirma a autenticação e a linha onde a mensagem *"[ldap] user Juliano authenticated succesfully*".

Como os testes foram realizados com sucesso, basta que qualquer NAS que tenha interesse em utilizar o servidor RADIUS seja cadastrado no arquivo */etc/freeradius/clients.conf*, para ter permissão de consultas no servidor LDAP através do servidor RADIUS. Dentre os NASs mais conhecidos e utilizados estão os roteadores CISCO, Servidores de empresas e clientes de autenticação *Asymmetric Digital Subscriber Line*（ADSL).

4 CONCLUSÃO

Com o crescimento da rede de computadores o presente trabalho trás como objetivo principal a segurança no acesso as informações. Atualmente o serviço oferecido pelo protocolo RADIUS é utilizado, na sua grande maioria, por grandes empresas de telecomunicações na autenticação de seus usuários ADSL, porém é um grande aliado à segurança que pode ser inserido nas empresas de médio e pequeno porte devido às falhas nas permissões ao acesso as redes.

Devido à simplicidade na instalação, o RADIUS é um poderoso aliado aos administradores de redes. Utilizando também o LDAP o nível de segurança é acrescido, pois os usuários podem ser separados por grupos e obter somente a liberação dos acessos necessários para sua rotina de trabalho.

Os objetivos do servidor RADIUS é a centralização de cadastros de usuários e a otimização de recurso dos equipamentos de rede, como por exemplo, de roteadores. No caso dos roteadores, há um limite para cadastro de usuários, variando de fabricante para fabricante, porém há necessidade de muitas pessoas acessarem o equipamento, isso gastaria muito recurso do mesmo que poderia ser dispensado para funções mais importante, como roteamento.

Com o exposto no decorrer deste trabalho conclui-se o objetivo do trabalho com êxito e apesar do protocolo RADIUS em conjunto com o LDAP ser pouco utilizado atualmente acredita-se que em pouco tempo ambos os protocolos serão mais difundidos e muito utilizados.

REFERÊNCIAS

A ARPANET. Disponivel em: <http://www.ime.usp.br/~is/abc/abc/node20.html>. Acesso em: 05/10/2011.

ASSUNÇÃO, Marcos F. Araujo. Segredos do Hacker Ético. 2ª Ed. Florianópolis: Visual Books, 2008.

CANTÚ, Evandro. Redes de Computadores e Internet. São José, SC:[s.n.], 2003.

Como Funciona a ARPANET. Disponível em: <http://informatica.hsw.uol.com.br/arpanet1.html> . Acesso em:05/10/2011.

Como o Protocolo TCP/IP Funciona. Disponível em: <http://www.clubedohardware.com.br/artigos/Como-o-Protocolo-TCP-IP-Funciona-Parte-1/1351/3>. Acesso em 09/10/2011

_____. Disponível em: <http://www.clubedohardware.com.br/artigos/Como-o-Protocolo-TCP-IP-Funciona-Parte-1/1351/1>. Acesso em:17/10/2011

Comunicação de dados. Disponível em: <http://www.ime.usp.br/~is/abc/abc/node5.html>. Acesso em: 18/10/2011

Endereço IP. Disponível em: <http://www.infowester.com/ip.php>. Acesso em: 09/10/2011

GIL, Antônio Carlos. Como elaborar projetos de pesquisa. 4ª. ed. São Paulo: Atlas, 2002.

Introdução ao Protocolo Internet – IP. Disponível em: <http://www.vivaolinux.com.br/artigo/Introducao-ao-Protocolo-Internet-IP>. Acesso em: 09/10/2011

Kurose, James F.; Ross, Keith W. **Redes de Computadores e a Internet: uma abordagem top-down**. São Paulo: Pearson Addison Wesley, 2006.

LDAP. Disponível em: <http://www.hardware.com.br/termos/ldap>. Acesso em: 13/11/2011

Lightweight Directory Access Protocol (LDAP): Technical Specification Road Map. Disponível em: <http://tools.ietf.org/html/rfc4510>. Acesso em: 04/07/2011.

O Modelo de Referência OSI para Protocolos de Rede. Disponível em: <http://www.clubedohardware.com.br/artigos/1349>. Acesso em 09/10/2011

O Modelo OSI. Disponível em: <http://www.projetoderedes.com.br/artigos/artigo_modelo_osi.php>. Acesso em 09/10/2011

O Modelo OSI e Suas 7 Camadas. Disponível em: <http://imasters.com.br/artigo/882/redes/o_modelo_osi_e_suas_7_camadas/>. Acesso em: 09/10/2011

O Protocolo LDAP. Disponível em:<http://pt.kioskea.net/contents/internet/ldap.php3>. Acesso em: 13/11/2011

Pacote de Dados RADIUS. Disponível em:< http://www.gta.ufrj.br/grad/08_1/radius/PacotededadosRADIUS.html>. Acesso em 07/11/2011

Práticas de Segurança para Administradores de Redes Internet. Disponível em: <http://www.cert.br/docs/seg-adm-redes/seg-adm-redes.html>. Acesso em: 02/08/2011.

PEREIRA, Marcos Heyse. Segurança de redes sem fio, uma proposta com serviços integrados de autenticação LDAP e RADIUS. 2009. 19 f. Monografia (Especialização em Rede e Segurança de Sistemas) – Pontifícia Universidade Católica do Paraná.

Roteamento IP. Disponível em:<http://technet.microsoft.com/pt-br/library/cc785246(WS.10).aspx>. Acesso em:18/10/2011

D’AVILA, Márcio C. H. **Segurança de Redes**. Disponível em: <http://www.mhavila.com.br/aulas/seguranca/material/segredes02.pdf>. Acesso em: 20/10/2011, 21:06

SEGURANÇA Máxima. Rio de Janeiro: Campus, 2000. 823 p.

TANENBAUM, Andrew S.. **Redes de computadores**. Rio de Janeiro: Elsevier, 2003 945 p.

Um pouco da história dos Computadores. Disponível em: <http://mansano.com/beaba/hist_comp.aspx>. Acesso em:05/10/2011

APÊNDICE A

Ministério da Educação
Universidade Tecnológica Federal do Paraná
Pró-Reitoria de Graduação e Educação Profissional
Pró-Reitoria de Pesquisa e Pós-Graduação
Sistema de Bibliotecas

DECLARAÇÃO DE AUTORIA

Autor[1]: Juliano Parreira dos Santos

CPF[1]: 042.113.229-90 Código de matrícula[1]: 753327

Telefone[1]: (41) 8823-9347 e-mail[1]: j_parreira_s@yahoo.com.br

Curso/Programa de Pós-graduação: Curso de Especialização Semi-Presencial em Configuração e Gerenciamento de Servidores e Equipamentos de Redes

Orientador: Fabiano Scriptore de Carvalho

Data da defesa: 26/11/2011

Título/subtítulo: Servidor RADIUS com Conexão LDAP

Tipo de produção intelectual: ( ) TCC[2] (X) TCCE[3] ( ) Dissertação ( ) Tese

Declaro, para os devidos fins, que o presente trabalho é de minha autoria e que estou ciente:

- dos Artigos 297 a 299 do Código Penal, Decreto-Lei nº 2.848 de 7 de dezembro de 1940;
- da Lei nº 9.610, de 19 de fevereiro de 1998, sobre os Direitos Autorais,
- do Regulamento Disciplinar do Corpo Discente da UTFPR; e
- que plágio consiste na reprodução de obra alheia e submissão da mesma como trabalho próprio ou na inclusão, em trabalho próprio, de idéias, textos, tabelas ou ilustrações (quadros, figuras, gráficos, fotografias, retratos, lâminas, desenhos, organogramas, fluxogramas, plantas, mapas e outros) transcritos de obras de terceiros sem a devida e correta citação da referência.

_____
Assinatura do Autor[1]

CURITIBA,26/11/2011
Local e Data

[1] Para os trabalhos realizados por mais de um aluno, devem ser apresentados os dados e as assinaturas de todos os alunos.
[2] TCC – monografia de Curso de Graduação.
[3] TCCE – monografia de Curso de Especialização.

APÊNDICE B

Ministério da Educação
Universidade Tecnológica Federal do Paraná
Pró-Reitoria de Graduação e Educação Profissional
Pró-Reitoria de Pesquisa e Pós-Graduação
Sistema de Bibliotecas

TERMO DE AUTORIZAÇÃO PARA PUBLICAÇÃO DE TRABALHOS DE CONCLUSÃO DE CURSO DE GRADUAÇÃO E ESPECIALIZAÇÃO, DISSERTAÇÕES E TESES NO PORTAL DE INFORMAÇÃO E NOS CATÁLOGOS ELETRÔNICOS DO SISTEMA DE BIBLIOTECAS DA UTFPR

Na qualidade de titular dos direitos de autor da publicação, autorizo a UTFPR a veicular, através do Portal de Informação (PIA) e dos Catálogos das Bibliotecas desta Instituição, sem ressarcimento dos direitos autorais, de acordo com a Lei nº 9.610/98, o texto da obra abaixo citada, observando as condições de disponibilização no item 4, para fins de leitura, impressão e/ou *download*, visando a divulgação da produção científica brasileira.

1. Tipo de produção intelectual: ( ) TCC[1] (X) TCCE[2] ( ) Dissertação ( ) Tese

2. Identificação da obra:

Autor[3]: JULIANO PARREIRA DOS SANTOS

RG[3]: 7.795.682-2 CPF[3]: 042.113.229-90 Telefone[3]: (41) 8823-9347

e-mail[3]: j_parreira_s@yahoo.com.br

Curso/Programa de Pós-graduação: Curso de Especialização Semi-Presencial em Configuração e Gerenciamento de Servidores e Equipamentos de Redes

Orientador: Fabiano Scriptore de Carvalho

Data da defesa: 26/11/2011

Título/subtítulo (português): Servidor RADIUS com Conexão LDAP

Título/subtítulo em outro idioma: RADIUS server with LDAP connection

Área de conhecimento do CNPq: Engenharia

Palavras-chave: Redes, Segurança, Acesso, Permissão

Palavras-chave em outro idioma: Network, Security, Access, Permission

3. Agência(s) de fomento (quando existir):

4. Informações de disponibilização do documento:

Restrição para publicação: ( ) Total[4] ( ) Parcial[4] (X) Não Restringir

Curitiba, 26 de Novembro de 2011
Local e Data

_____ _____
Assinatura do Autor[3] Assinatura do Orientador

[1] TCC – monografia de Curso de Graduação.
[2] TCCE – monografia de Curso de Especialização.
[3] Para os trabalhos realizados por mais de um aluno, devem ser apresentados os dados e as assinaturas de todos os alunos.
[4] A restrição parcial ou total para publicação com informações de empresas será mantida pelo período especificado no Termo de Autorização para Divulgação de Informações de Empresas. A restrição total para publicação de trabalhos que forem base para a geração de patente ou registro será mantida até que seja feito o protocolo do registro ou depósito de PI junto ao INPI pela Agência de Inovação da UTFPR. A íntegra do resumo e os metadados ficarão sempre disponibilizados.