MANUAL PARA A IMPLEMENTAÇÃO DE SEGURANÇA COM UM SERVIDOR FREERADIUS EM UMA REDE WI-FI COM AP'S UNIFI GERENCIADOS PELO SISTEMA OPERACIONAL ROUTER’OS

G U I L H E R M E L E V Y

GUARAPUAVA / PARANÁ

OUTUBRO / 2017

SUMÁRIO

ÍNDICE DE ILUSTRAÇÕES

LISTA DE ABREVIATURAS E SIGLAS

AP	Access Point
ADD	Addiction
ARP	Address Resolution Protocol
DB	Data Base
DHCP	Dynamic Host Configuration Protocol
DNS	Domain Name System
DST	Destination
EAP	Extensible Authentication Protocol
HTTP	Hypertext Transfer Protocol
IP	Internet Protocol
LAN	Local Architecture Network
MAC	Media Access Control
NAS	Network Access Server
NAT	Network Address Translation
OS	Operating System
PEAP	Protected Extensible Authentication Protocol
POE	Power Over Ethernet
SQL	Structured Query Language
SRC	Source
SSID	Service Set IDentifier
TCP	Transmission Control Protocol
VDSL	Very high bit rate Digital Subscriber Line
VPN	Virtual Private Network
WI-FI	Wireless Fidelity
WPA	Wi-fi Protected Access

1. OBJETIVO DO MANUAL

O principal objetivo deste manual é orientar o administrador da rede na configuração, criação de regras de autenticação em um servidor Hotspot e implementação de segurança no nível de autenticação da rede wi-fi através de um servidor Freeradius.

Devido ao crescente número de usuários e tentativas de conexão em uma rede wireless que faz a autenticação dos usuários após a conexão na rede wi-fi em um servidor Hotspot em uma Routerboard foi necessário implementar regras que exijam credenciais de autenticação do usuário já ao se conectar na rede wi-fi, pois isso irá diminuir o número de usuários conectados na rede que não possuem credenciais para autenticação no Hotspot e consequentemente diminuir o fluxo de dados nos access points, melhorando assim seus desempenhos.

2. CONFIGURAÇÃO DO SISTEMA OPERACIONAL ROUTER'OS

2.1. INTRODUÇÃO

Para o gerenciamento principal da rede, gerenciamento dos endereços de IP dos AP's Ubiquiti Unifi e gerenciamento dos usuários que se autenticarão no servidor Hotspot utilizaremos uma Routerboard RB750 conforme a imagem abaixo, com o sistema operacional RouterOS da empresa Mikrotik.

Imagem 1: Routerboard RB750

Esse capítulo traz o roteiro detalhado para a configuração das interfaces, criação das redes, configuração de Web Proxy, configuração de Firewall, criação e configuração do servidor Hotspot e usuários, podendo ser utilizado também em outros modelos de Routerboards Mikrotik ou no sistema operacional RouterOS instalado em um microcomputador.

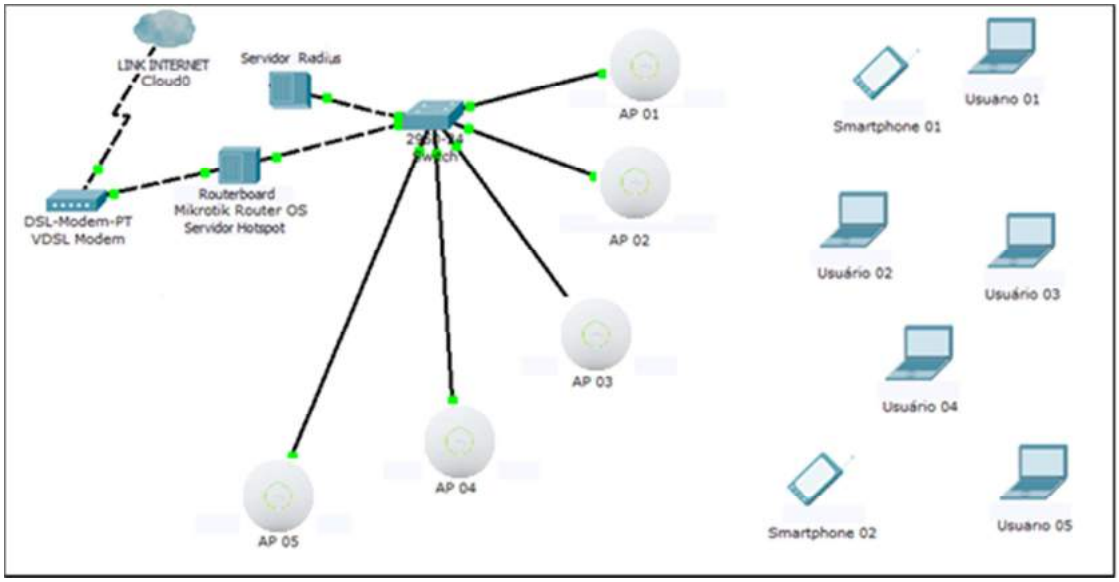

Imagem 2: Rede após a instalação do servidor Hotspot

Conforme a representação da Imagem02 a Routerboard deve ser instalada entre o uplink de internet e os dispositivos de distribuição da internet para a rede local.

2.2. PRIMEIRO ACESSO E CONFIGURAÇÃO INICIAL

Para a criação das regras e acesso aos menus de configuração utilizaremos o programa Winbox na sua versão 3.0, que pode ser baixado gratuitamente na internet conforme o link http://download2.mikrotik.com/routeros/winbox/3.0rc12/winbox.exe.

Iremos conectar nosso computador à porta número 5 da Routerboard.

Na imagem abaixo podemos visualizar a tela de login do programa Winbox para nos conectar ao sistema operacional RouterOS da Routerboard. Como a Routerboard ainda não possui configuração de rede devemos nos conectar pelo seu respectivo endereço MAC, esse endereço encontra-se em um adesivo colado embaixo da Routerboard. O usuário padrão é admin e o campo senha não deverá ser preenchido conforme especificação padrão do equipamento.

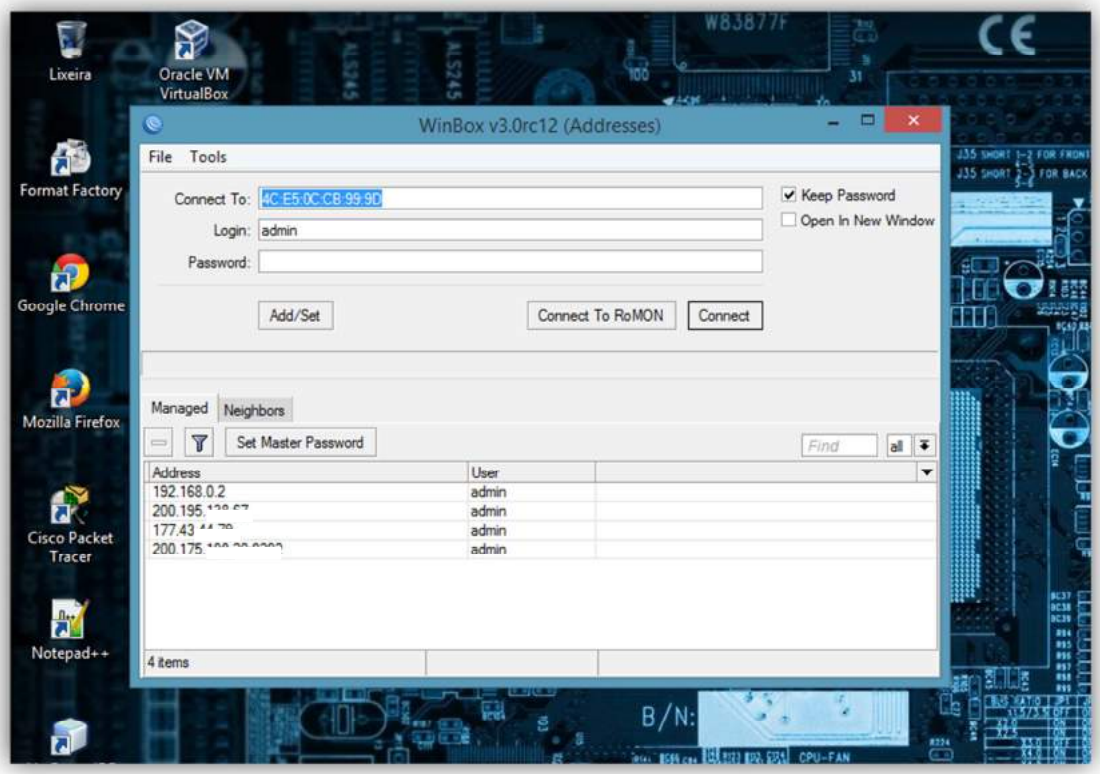

Imagem 3: Tela de login do aplicativo Winbox

Na imagem abaixo podemos visualizar a tela inicial após o acesso com o login e senha realizado pelo administrador no RouterOS com o programa Winbox. Nos próximos itens as imagens serão redimensionadas e focadas nos menus e submenus para uma melhor visualização e entendimento do conteúdo.

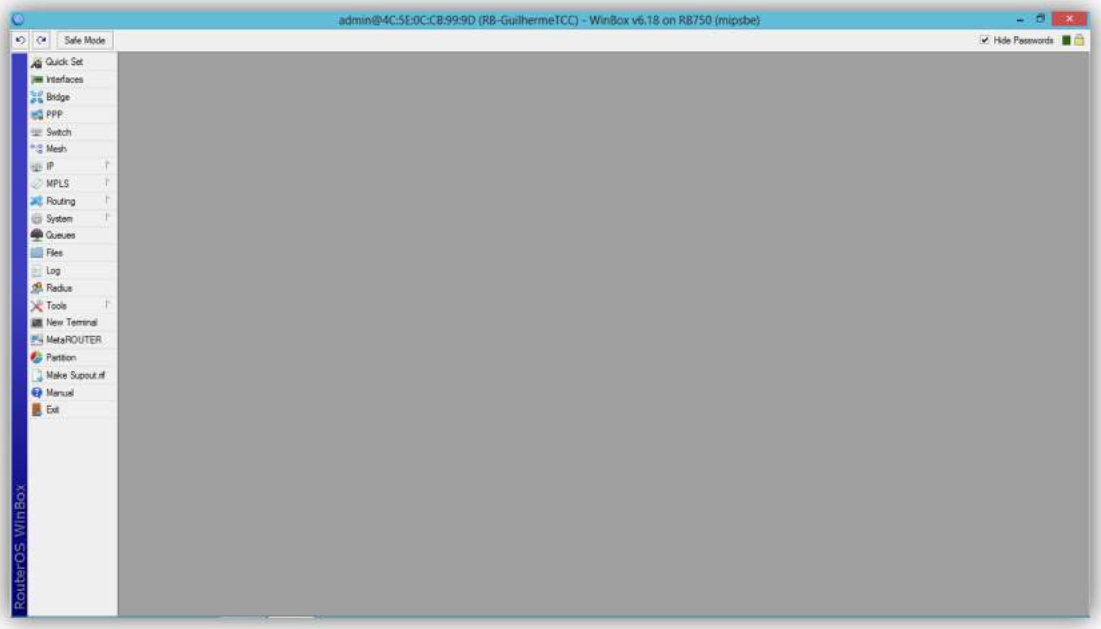

Imagem 4: Tela inicial do Winbox

Para iniciar os procedimentos de configuração devemos identificar nossa Routerboard a fim de personalizá-la em utilizações futuras, tal como identificação de arquivo de backup.

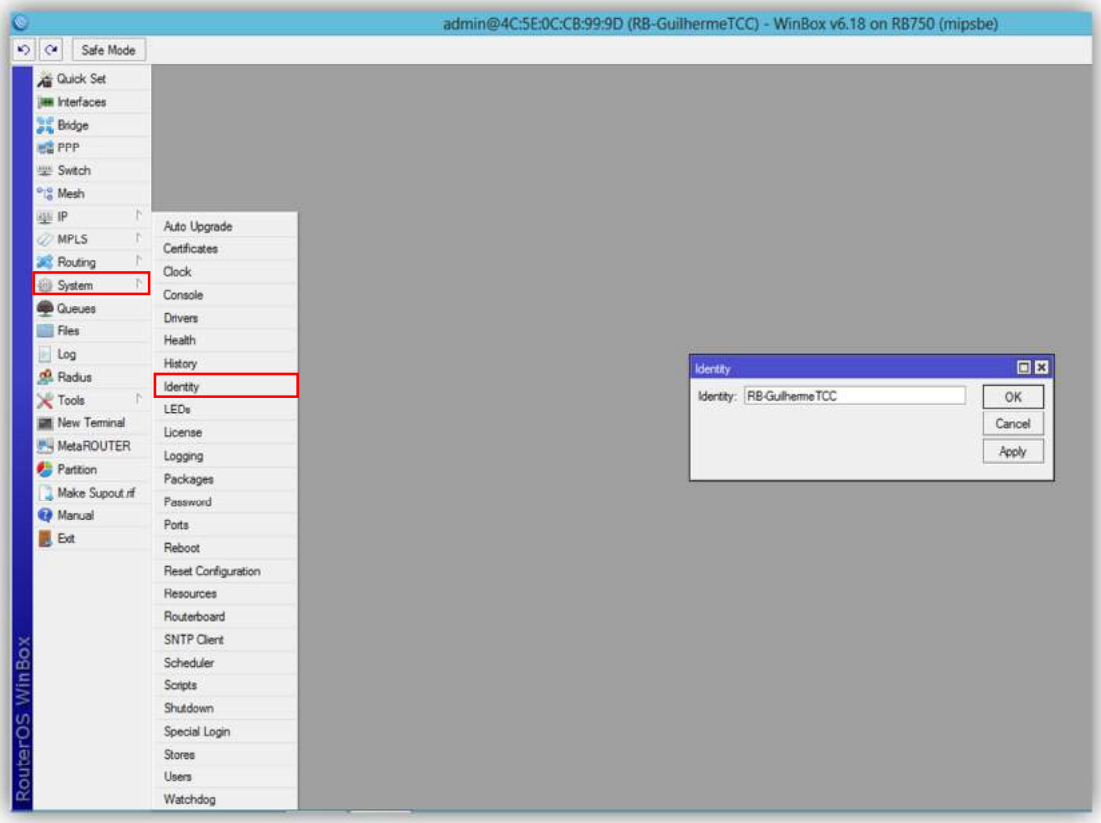

Imagem 5: Identificação da Routerboard

Seguindo a ideia de personalizar a Routerboard para uma correta geração dos relatórios e arquivos de backup quando necessário e para garantir um funcionamento sem erros de interpretação das regras devemos fazer as configurações de hora, data e fuso horário.

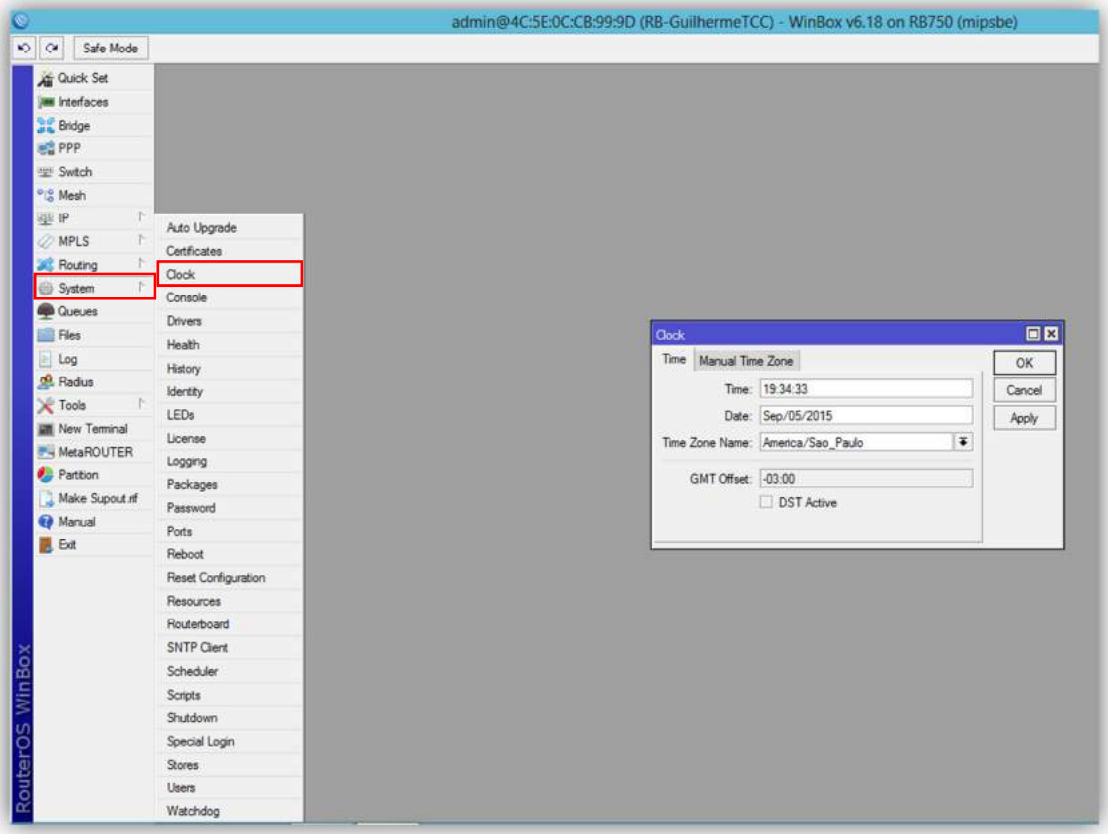

Imagem 6: Correção de hora/data

2.3. IDENTIFICAÇÃO E PERSONALIZAÇÃO DAS INTERFACES

Na imagem abaixo podemos visualizar a tela das interfaces disponíveis para a utilização no RouterOS. Entraremos no Menu: **Interfaces**

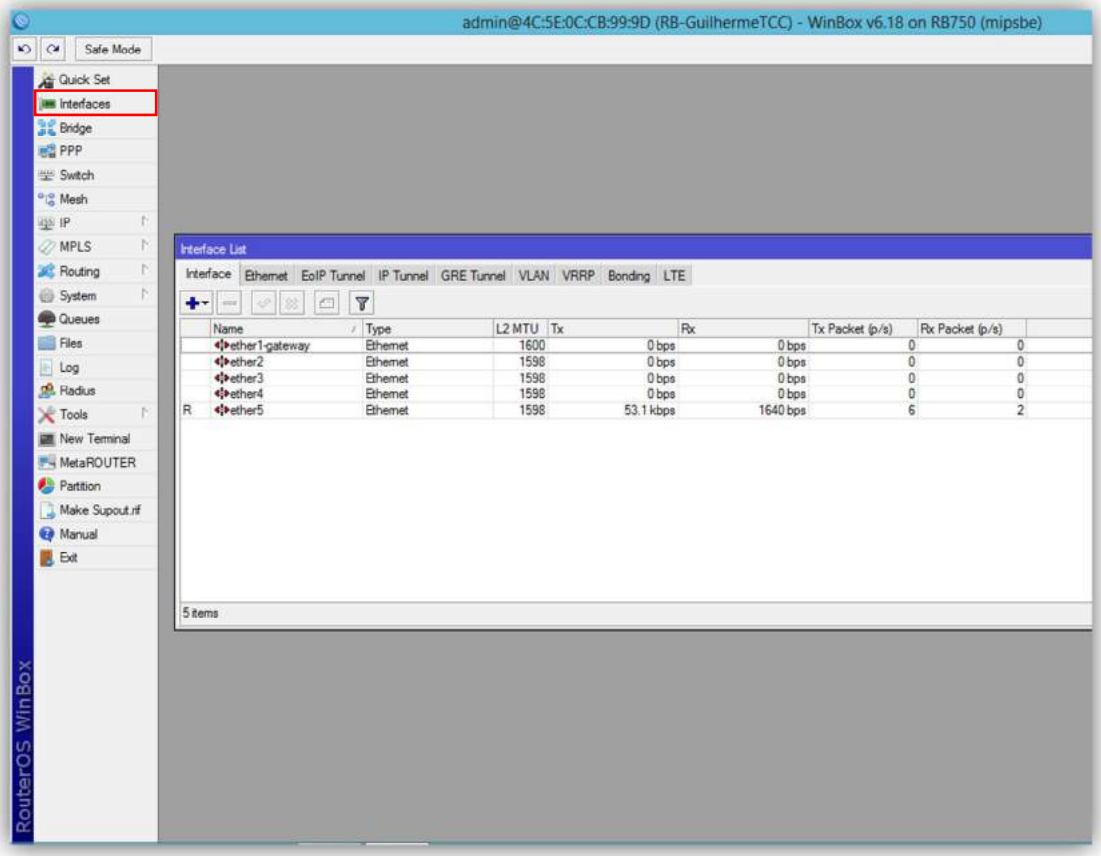

Imagem 7: Interfaces da Routerboard

2.3.1. RENOMEANDO A ETHER1 (UPLINK)

Escolheremos primeiramente a interface ether1-gateway (porta1) dando dois cliques para que nos seja mostrada a janela com as configurações padrão da porta. Na opção **Name** colocaremos o nome Uplink para identificá-la como a porta em que conectaremos o link de entrada da internet, na configuração utilizada nesse manual será disponibilizada somente uma porta para o uplink de internet.

Deixaremos a opção **ARP** como enable para que os pacotes de reconhecimento da rede que seja conectada na porta possam ser utilizados por essa interface, na opção de **Bandwidth** que limita o fluxo de dados na interface deixaremos unlimited, ou seja, sem limite de banda de tráfego de dados nessa interface. Os outros campos deixaremos com os valores padrão do RouterOS e clicaremos em OK.

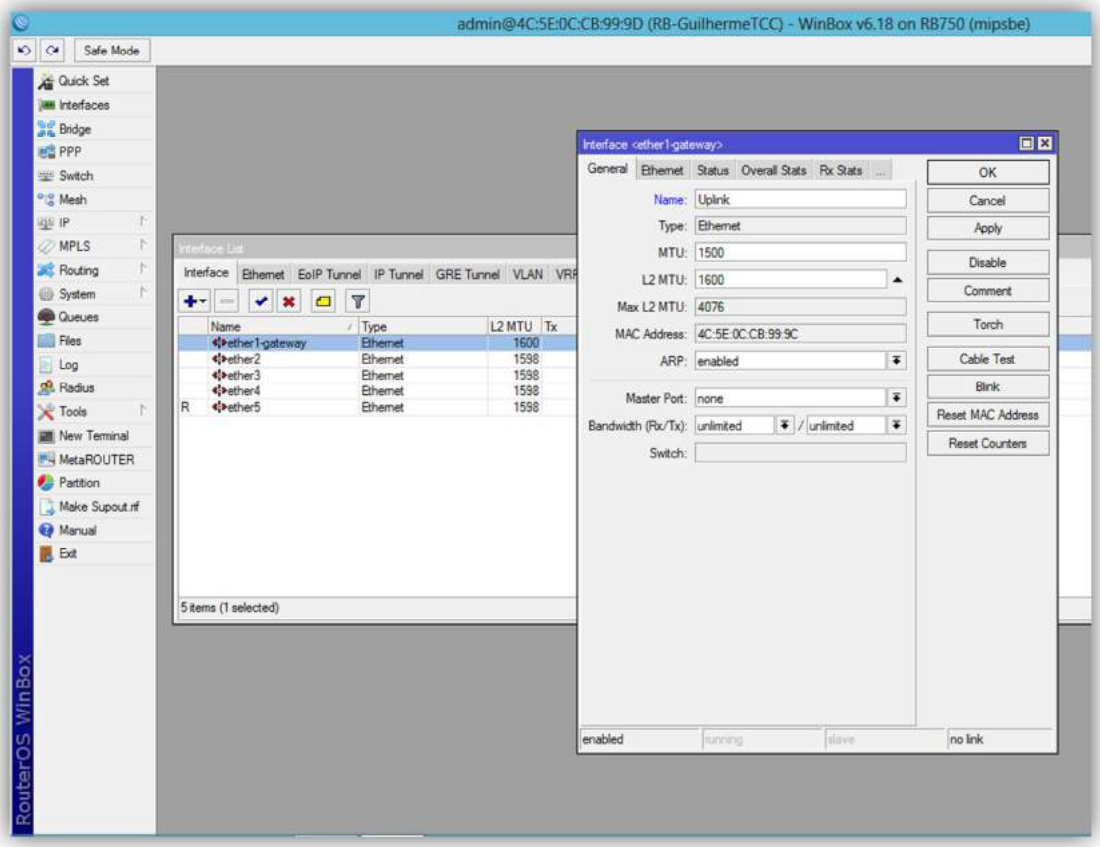

Imagem 8: Nomeação da interface ether1

2.3.2. RENOMEANDO A ETHER5 (OUTSWITCH)

Assim como na ether1 alteraremos somente o nome da ether5 (porta5) para OutSwitch, essa interface será responsável por transmitir os dados já tratados pela Routerboard para um microcomputador ou para os dispositivos de rede responsáveis pela distribuição da rede, em nosso caso, um Acess Point Wireless e um Swtich ethernet.

Na imagem abaixo podemos visualizar como ficará a tela de configuração da ether5 após as alterações.

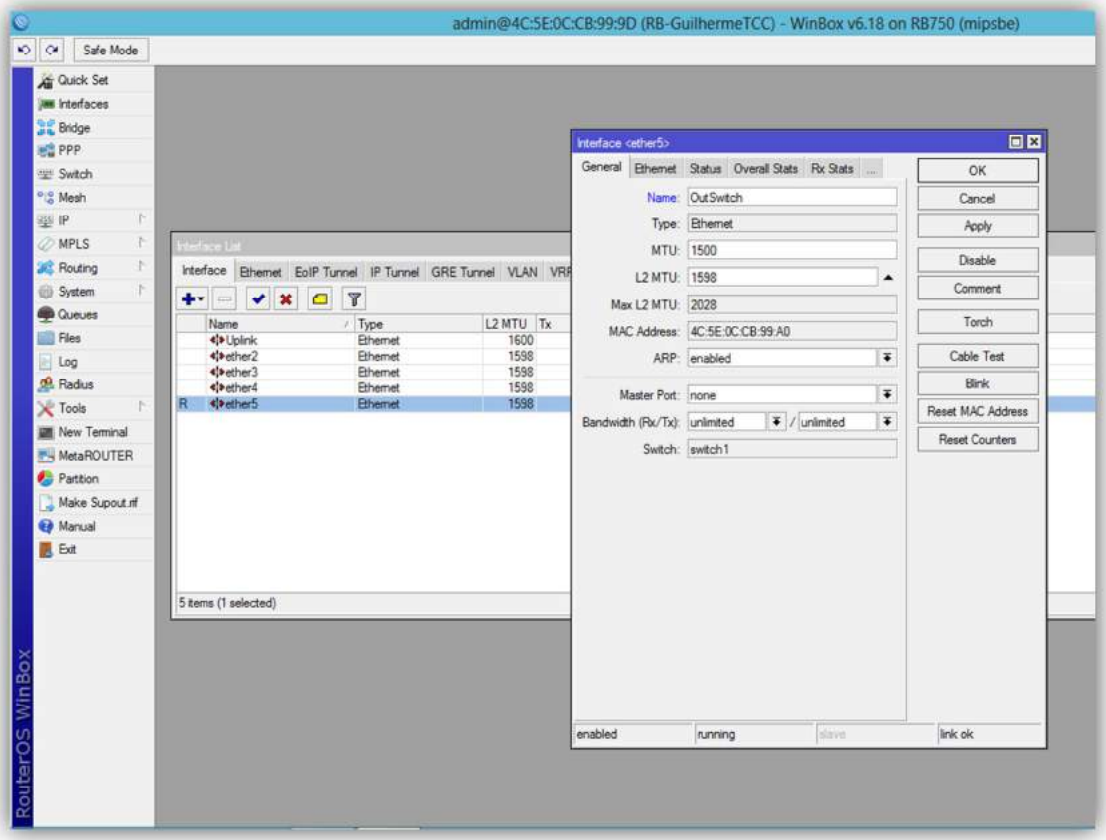

Imagem 9: Nomeação da interface ether5

2.3.3. FINALIZANDO A PERSONALIZAÇÃO DAS INTERFACES

Na imagem a seguir podemos visualizar a listagem de interfaces após à sua personalização e identificação. Podemos reparar ainda na letra **R** ao lado da interface OutSwitch que significa “Running”, ou seja, a interface já reconheceu o cabo conectado em sua porta e já está em funcionamento.

Obs: Lembrando que o cabo do Uplink de internet ainda não deve estar conectado na porta 5 da routerboard, conectaremos o cabo somente após a criação do DHCP Client, tópico abordado nos capítulos a seguir.

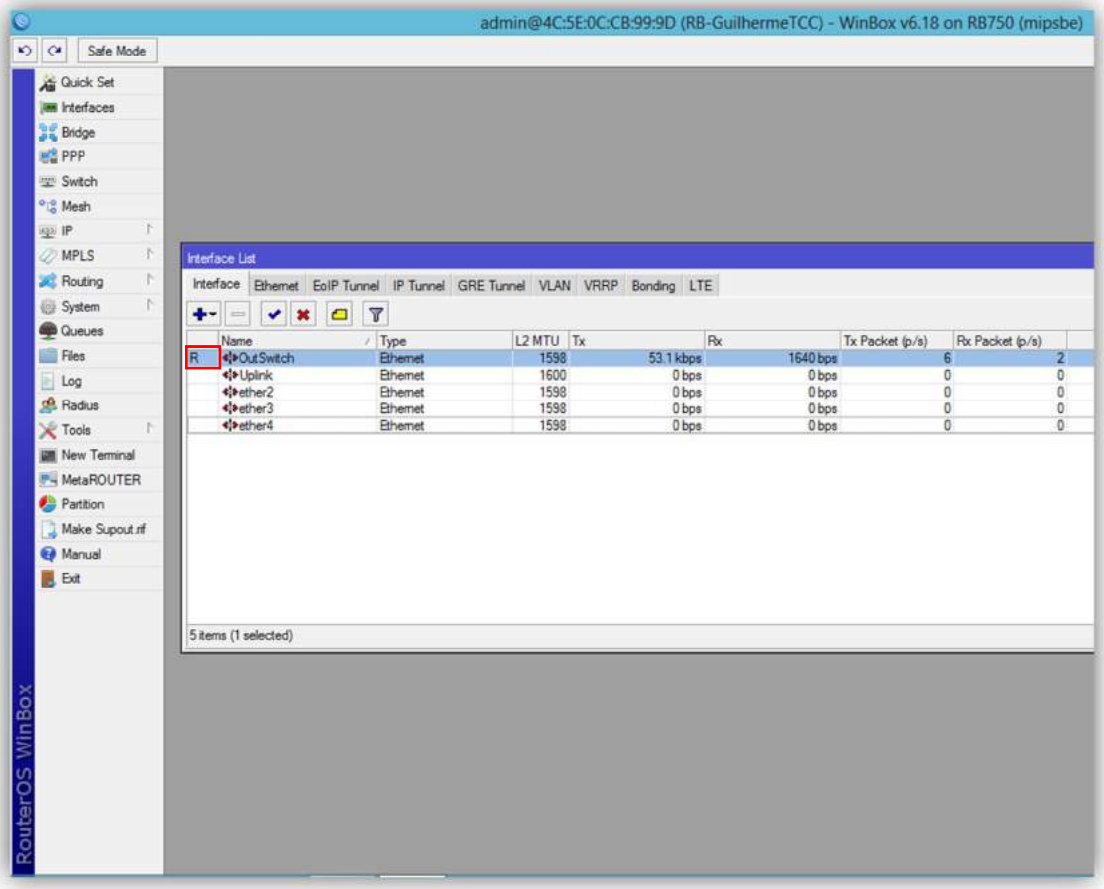

Imagem 10: Tela das interfaces após as alterações

2.4. ADDRESS LIST

Agora iniciaremos a configuração dos endereços de rede estáticos que poderão trafegar dados dentro de nossa Routerboard. Entraremos no Menu: **IP=>Addresses** e selecionaremos a opção ADD, simbolizada no Winbox pelo ícone ✚ .

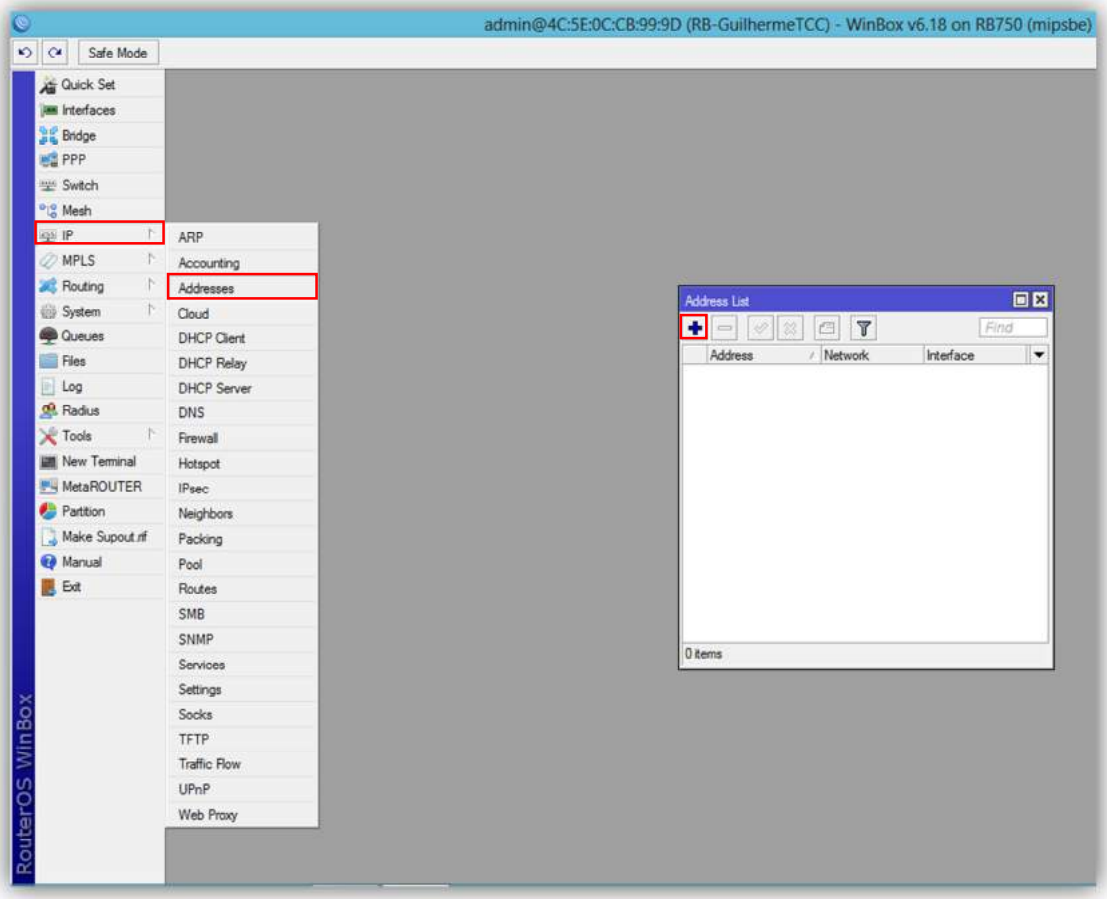

Imagem 11: Tela de configuração da Address List

2.4.1. ADICIONANDO UM NOVO ADDRESS ESTÁTICO

Antes de iniciar as configurações específicas de cada função no RouterOS precisamos definir quais são os endereços estáticos que poderão trafegar dados dentro de nossa Routerboard. Escolheremos a classe 192.168.10.0 para a criação de nosso servidor Hotspot, portanto na opção **Address**, que será o enderenço IP que nossa Routerboard poderá ser acessada através do Winbox colocaremos 192.168.10.1/24, na opção **Network** colocaremos o endereço da rede escolhida 192.168.10.0 e no campo **Interface** escolheremos por qual delas essa rede estará acessível, em nosso caso a interface **OutSwitch** e depois clicaremos em **OK**. Nesse ponto já começamos a entender a importância da correta personalização prévia das interfaces, para que na hora das configurações dos vínculos das interfaces com os addresses não ocorra nenhuma troca e dificulte a finalização da implantação do servidor Hotspot.

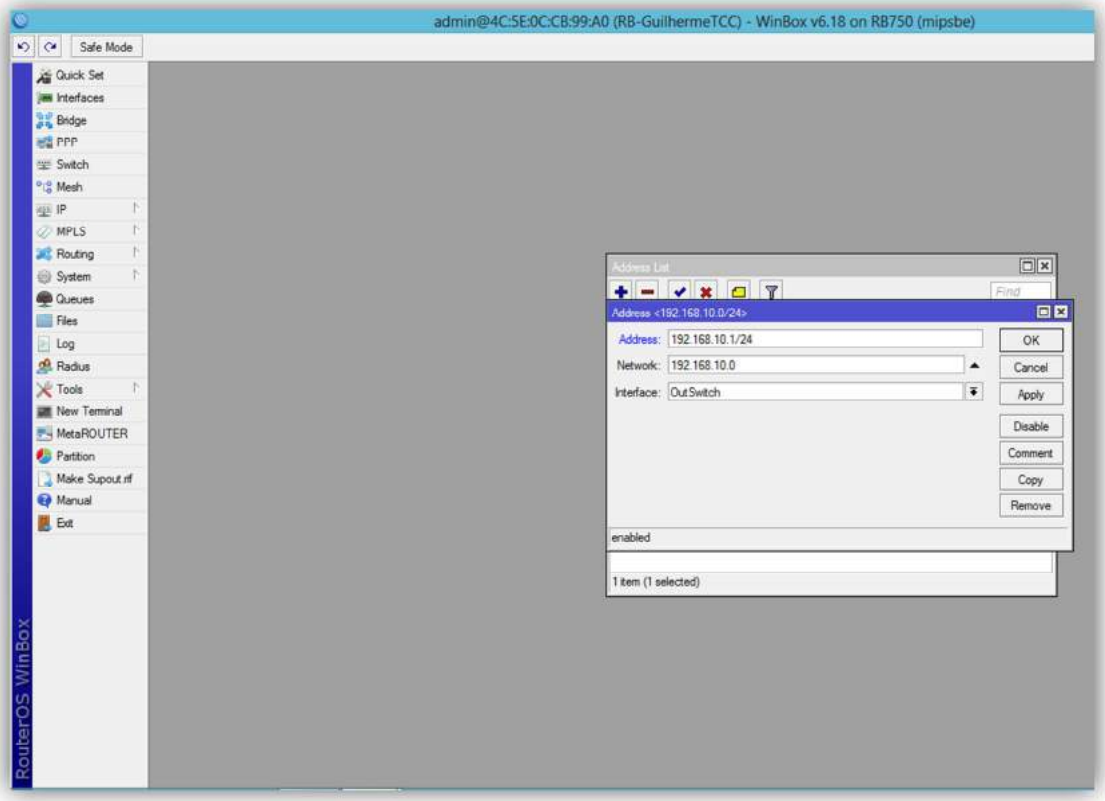

Imagem 12: Tela de inclusão de um Address estático

Na imagem abaixo podemos visualizar como ficará a Address List após a inclusão da nossa rede principal.

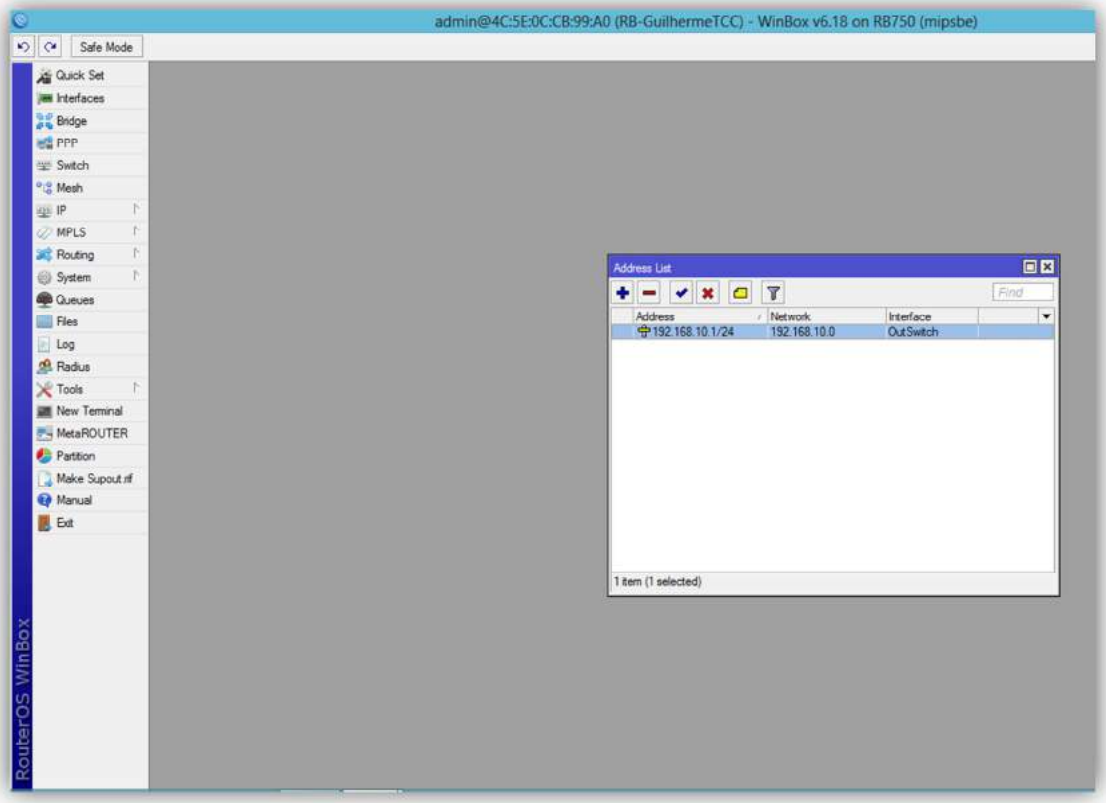

Imagem 13: Finalizando a inclusão de um Address estático

2.5. IP POOL

Agora iremos configurar um POOL de endereços de ip para nossa rede, o IP POOL é o escopo do DHCP Server, ou seja, é uma faixa de endereços de ip que o DHCP Server poderá conceder dinamicamente aos clientes.

Agora iniciaremos a inclusão de um POOL de endereços de ip em nossa Routerboard. Entraremos no Menu: **IP=>IP POOL** e selecionaremos a opção ADD, simbolizada no Winbox pelo ícone ✚ .

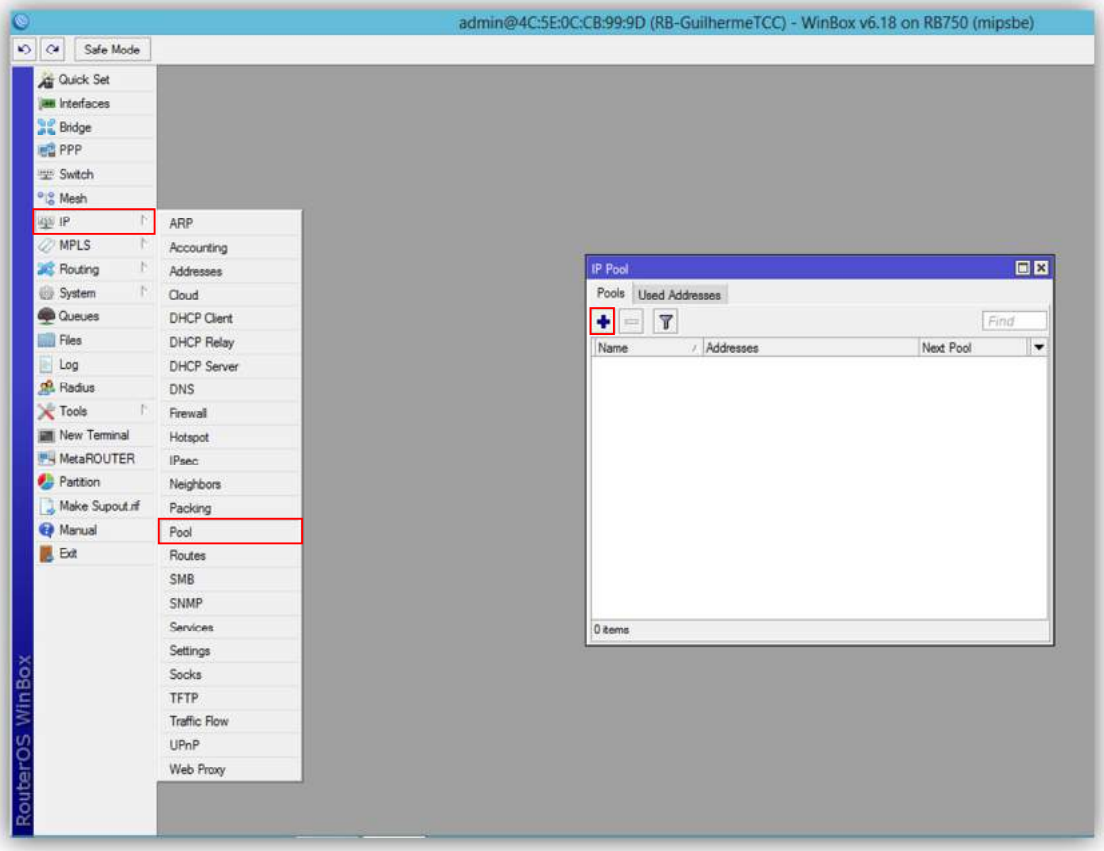

Imagem 14: Tela inicial de configuração do IP Pool

2.5.1. ADICIONANDO UM NOVO IP POOL

Na janela “**New IP POOL**” colocaremos no campo **Name** o nome de “**PoolHSP**” para o novo Pool de endereços de ip, no campo **Addresses** colocaremos a faixa de ip que será disponibilizada pelo DHCP Server, nesse caso utilizaremos a faixa de 192.168.10.5-192.168.10.254, portanto serão 250 endereços de ip utilizáveis pelo no DHCP Server para os microcomputadores ou dispositivos conectados a ele.

Na opção **Next Pool** deixaremos none, essa opção é utilizada quando necessitamos de uma quantidade maior que 253 endereços de ip para o DHCP Server conceder aos microcomputadores ou dispositivos, então se temos dois IP POOL criados colocamos nessa opção esse segundo IP POOL criado e ao acabar os endereços do primeiro ele automaticamente começará a conceder os endereços de ip do segundo IP POOL existente.

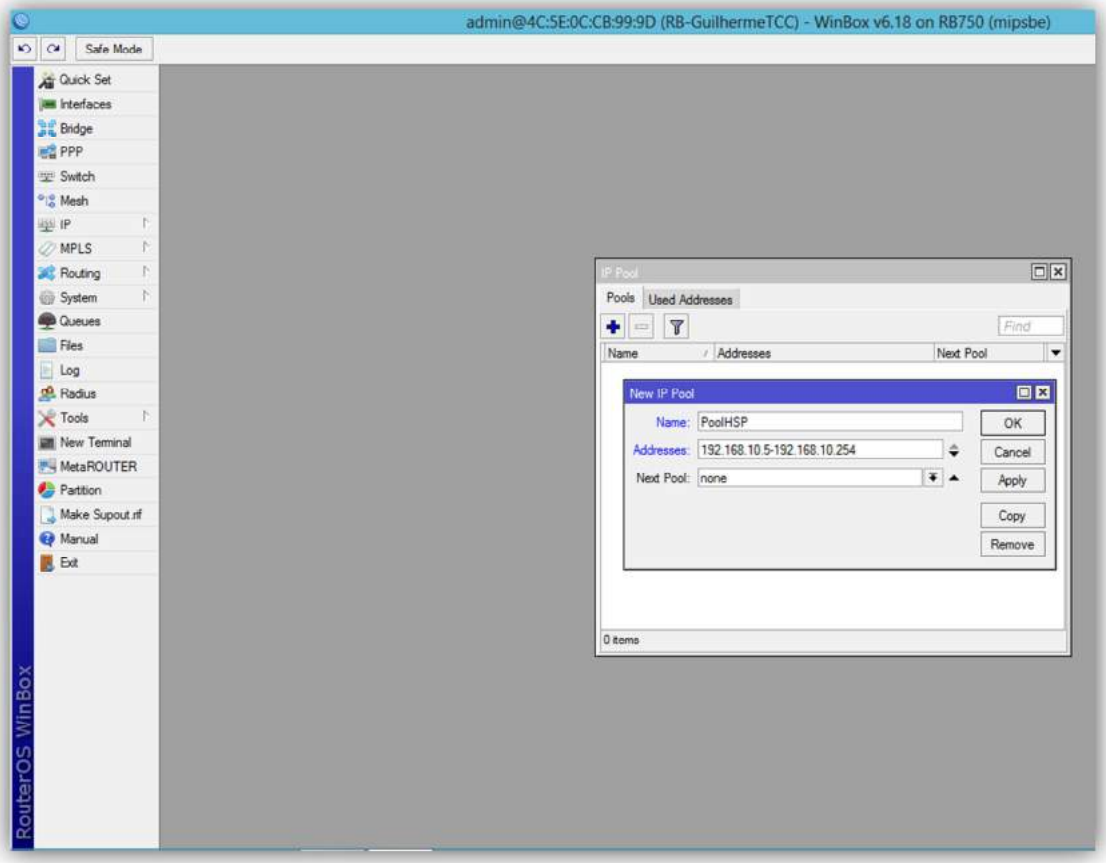

Imagem 15: Tela de inclusão de um novo IP Pool

Na imagem abaixo podemos visualizar como ficará a tela inicial do IP POOL após a inclusão do nosso novo IP POOL.

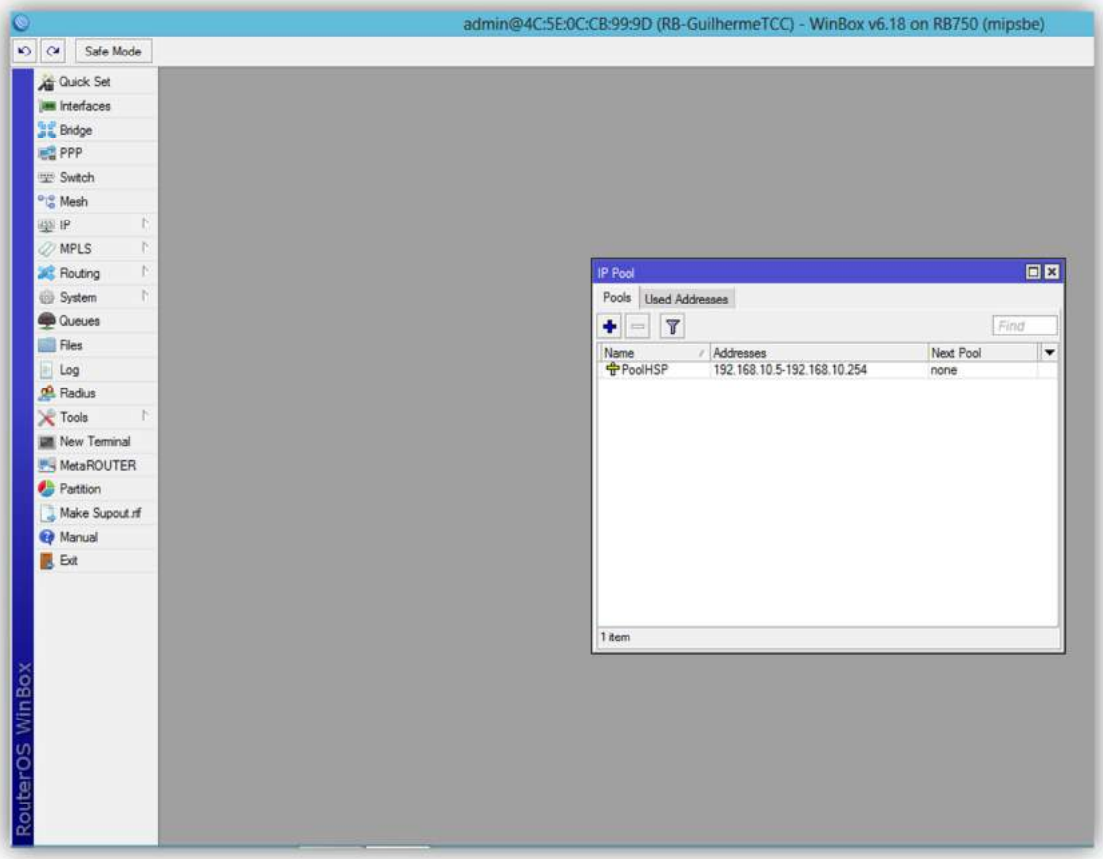

Imagem 16: Finalizando a inclusão de um IP POOL

2.6. DHCP SERVER

A imagem abaixo nos mostra os servidores DHCP existentes em nossa routerboard, o protocolo DHCP é o serviço responsável por uma configuração dinâmica dos microcomputadores ou dispositivos conectados a ele, incluindo atribuição de IP, máscaras de sub-rede, default gateway e servidores DNS.

Agora iniciaremos a inclusão de um servidor DHCP em nossa Routerboard. Entraremos no Menu: **IP=>DHCP Server** e selecionaremos a opção ADD, simbolizada no Winbox pelo ícone ✚ .

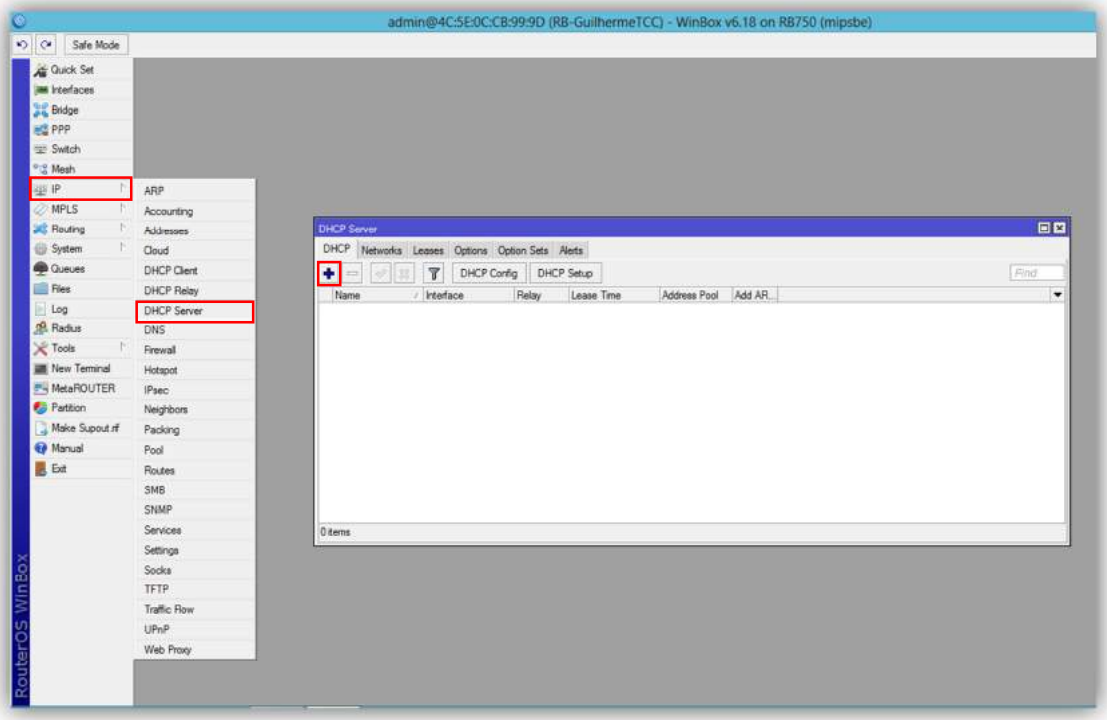

Imagem 17: Tela inicial de configuração do DHCP Server

2.6.1. ADICIONANDO UM NOVO DHCP SERVER

Na janela “**New DHCP Server**” iniciaremos a configuração dando um nome ao nosso servidor, sempre lembrando que é uma boa prática colocarmos nomes que facilitem a identificação do serviço nas próximas etapas, no caso de você possuir mais de um servidor DHCP configurado nesse mesmo RouterOS.

Nesse caso colocaremos no campo **Name** o nome de “**ServerHSP**” para o novo servidor, no campo **Interface** selecionaremos a interface que será responsável por fornecer as configurações do DHCP aos microcomputadores e dispositivos conectados a ele, nesse caso a interface OutSwitch. No campo **Lease Time** colocaremos o tempo de 02:00:00 horas, o Lease Time é o tempo que o endereço de ip estará disponível para um endereço MAC após a primeira utilização desse ip por esse determinado MAC. No campo Address Pool selecionaremos o “**PoolHSP**” criado anteriormente. Nos demais campos deixaremos o padrão do RouterOS, como mostrado na imagem abaixo.

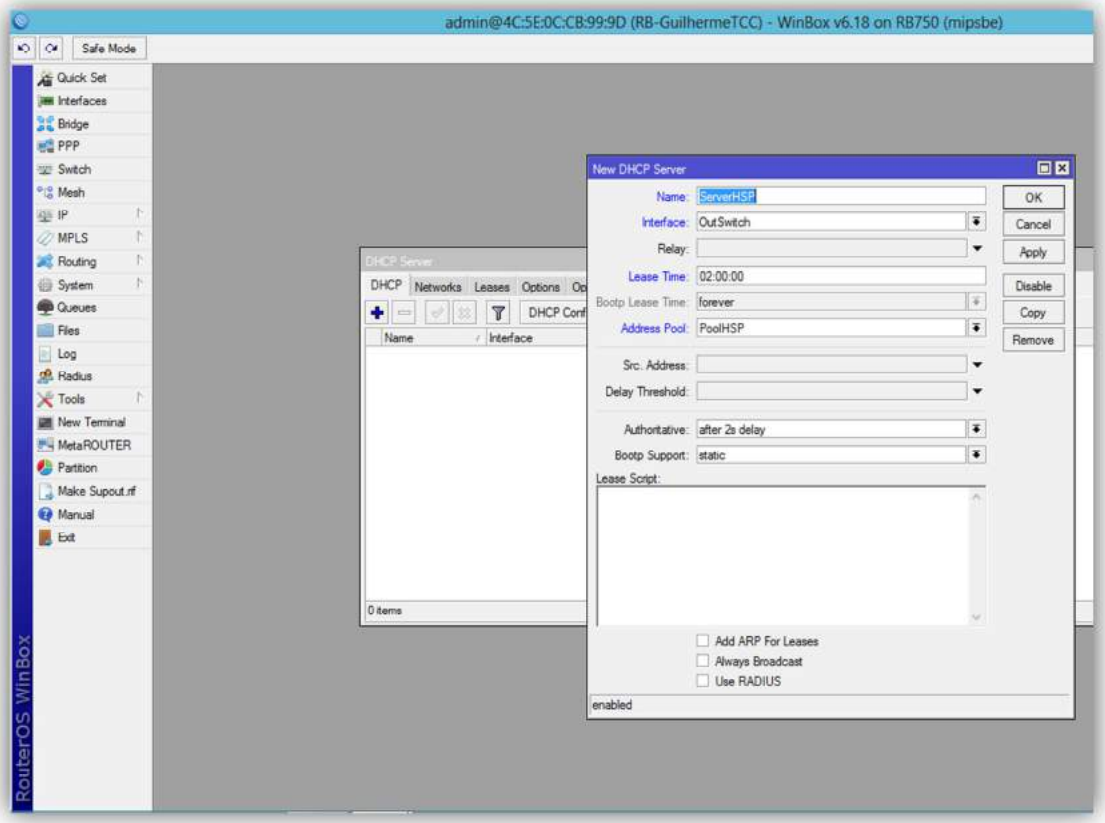

Imagem 18: Criando um novo DHCP Server

Na imagem abaixo podemos visualizar como ficará a tela inicial do DHCP Server após a inclusão do nosso novo servidor DHCP.

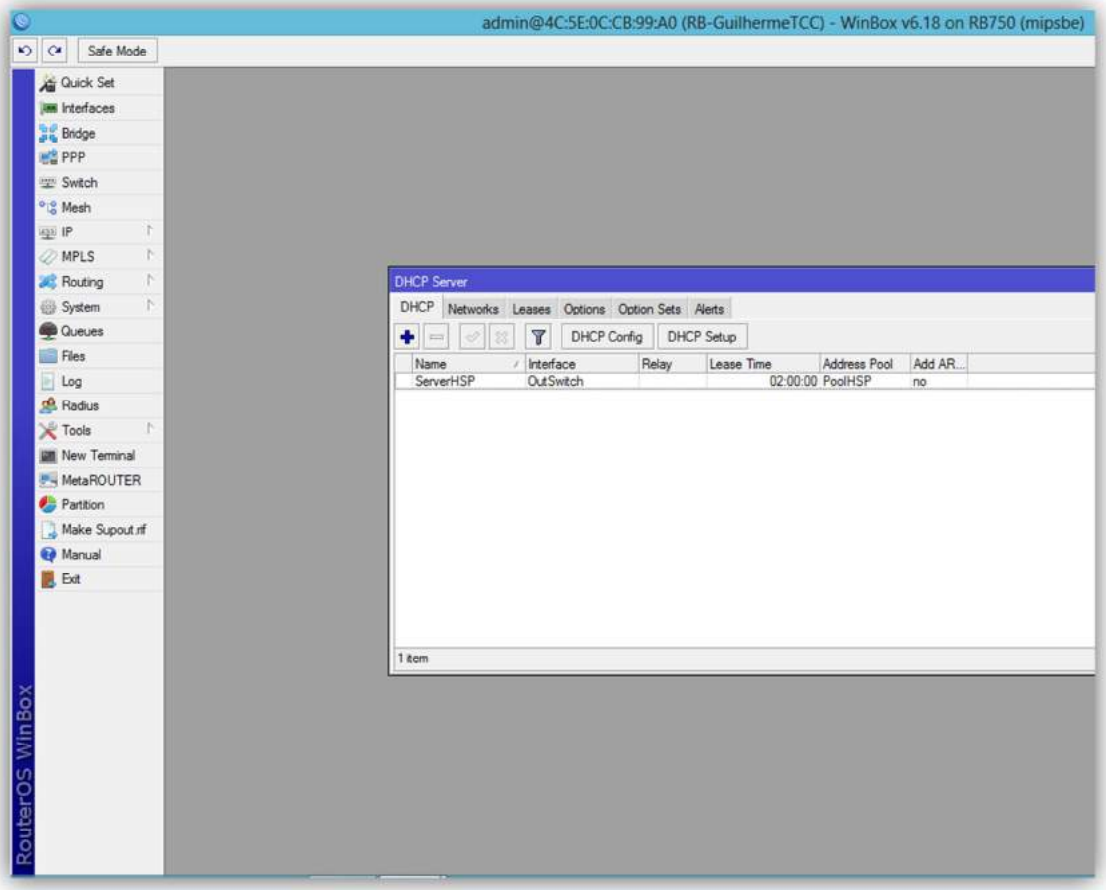

Imagem 19: Finalizando a inclusão de um DHCP server

2.6.2. DHCP Server =>NETWORKS

Na opção **Networks** do Router iremos configurar os Gateways de nossas redes, na opção Networks também é possivel configurar servidores DNS individuais para cada rede, nós não faremos isso e será explicado o motivo no tópico **DHCP Client**.

Agora iniciaremos a configuração de um Networks. Entraremos no Menu: **IP=>DHCP Server** e clicaremos na guia **Networks,** selecionaremos a opção ADD, simbolizada no Winbox pelo ícone ✚ .

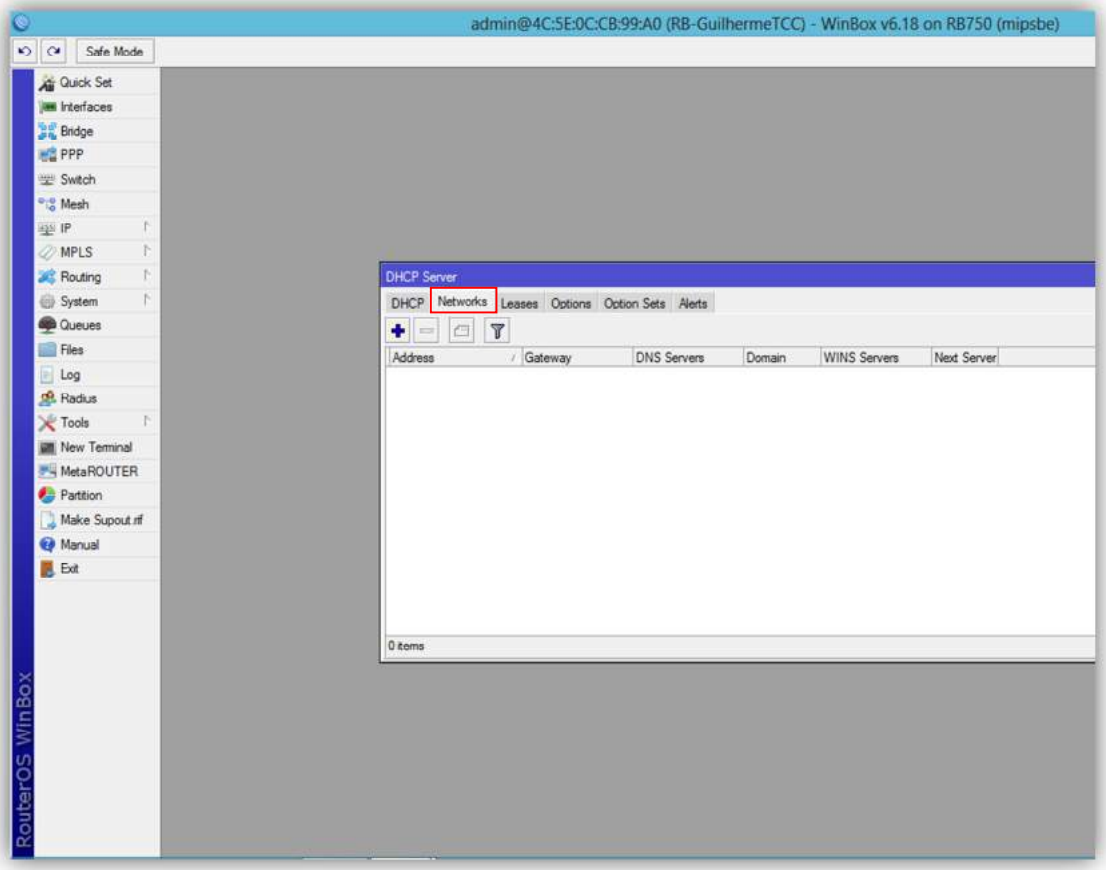

Imagem 20: Tela inicial de configuração Networks

2.6.2.1. ADICIONANDO UM NOVO NETWORKS

No campo **Address** colocaremos a classe de nossa rede que será utilizada seguida pela máscara de sub-rede, nesse caso 192.168.10.0/24 e no campo **Gateway** colocaremos o gateway de nossa classe, 192.168.10.1, os demais campos serão não serão alterados.

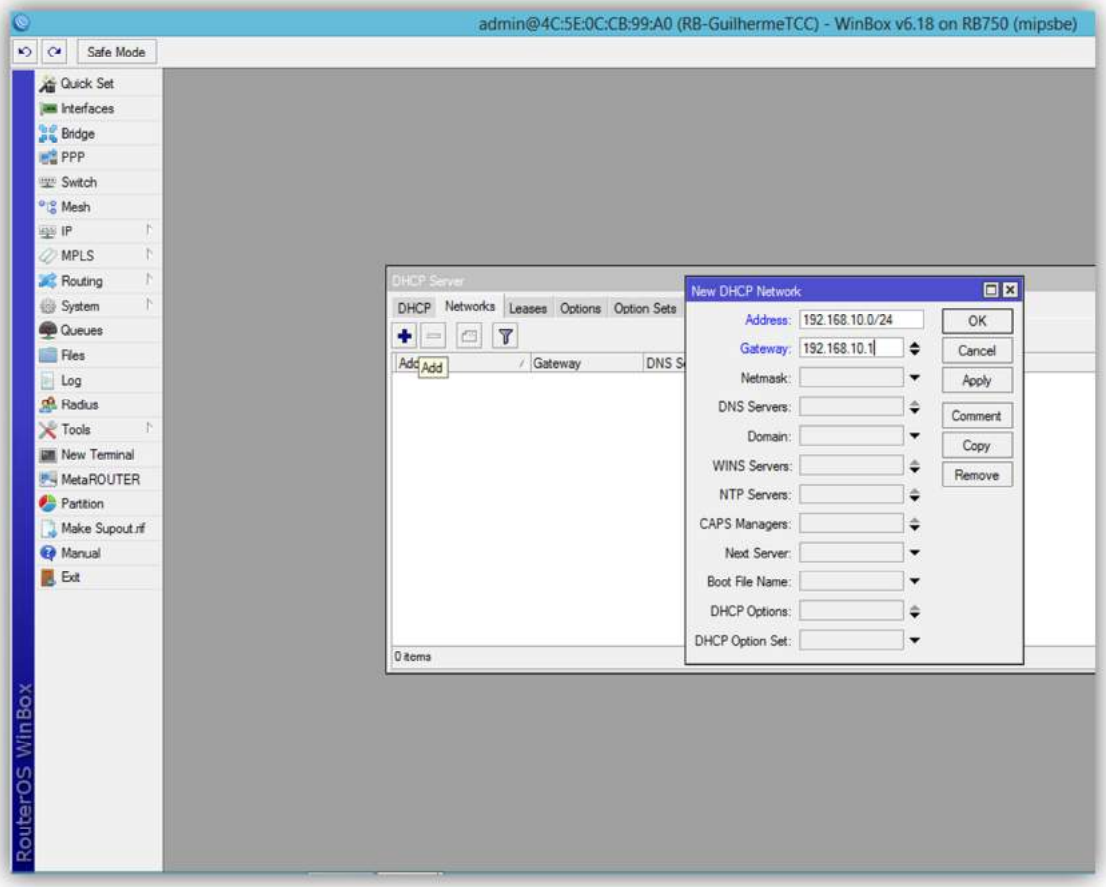

Imagem 21: Tela de inclusão de um novo Networks

Na imagem abaixo podemos visualizar como ficará a tela inicial do Networks após a inclusão do nosso novo Networks.

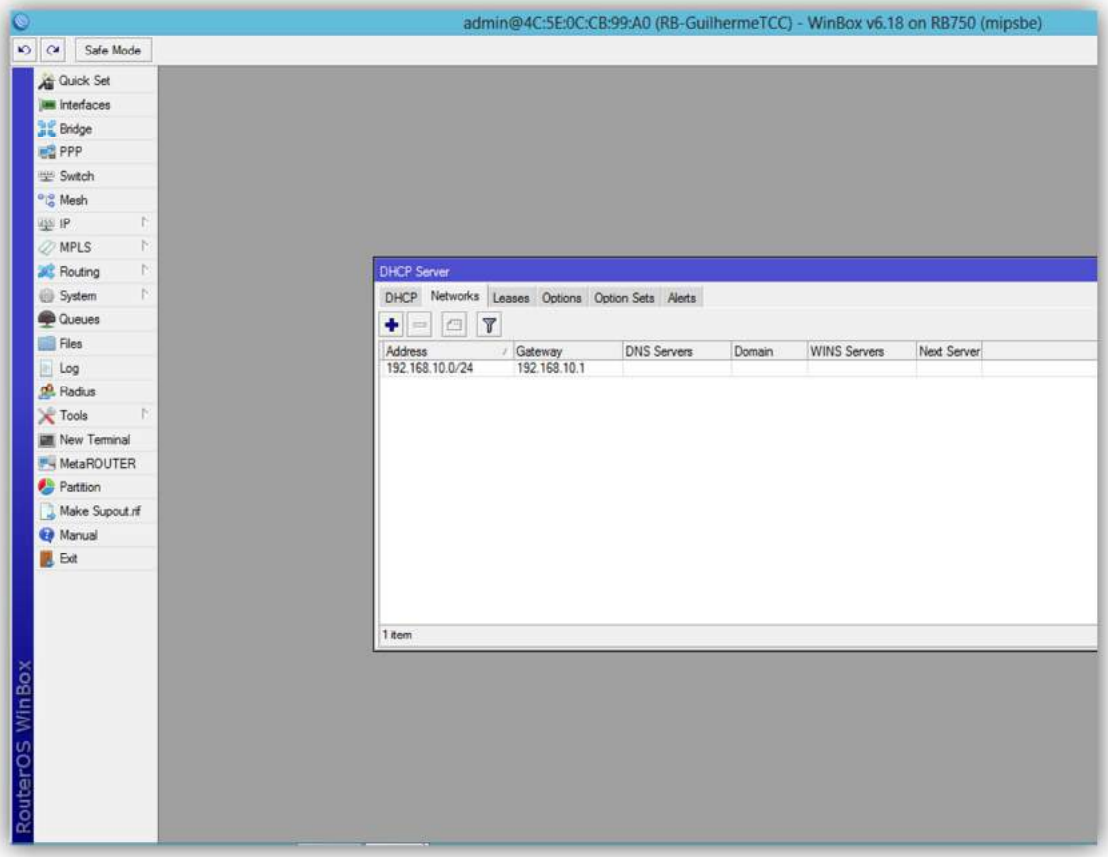

Imagem 22: Finalizando a inclusão de um Networks

Após essa etapa da configuração já é possível fazer o login no RouterOS pelo endereço de ip e não mais pelo endereço MAC, em nosso caso faremos o login pelo ip do gateway 192.168.10.1, como mostra a Imagem23.

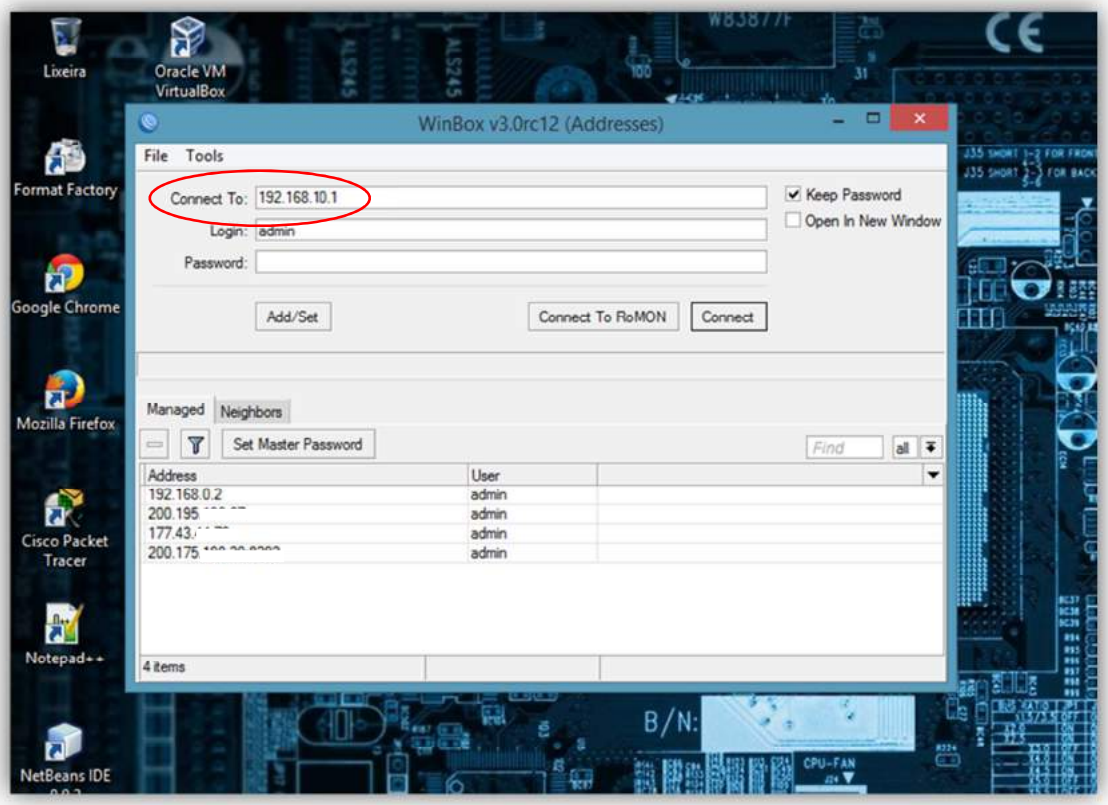

Imagem 23: Tela de login no RouterOS pelo endereço de ip

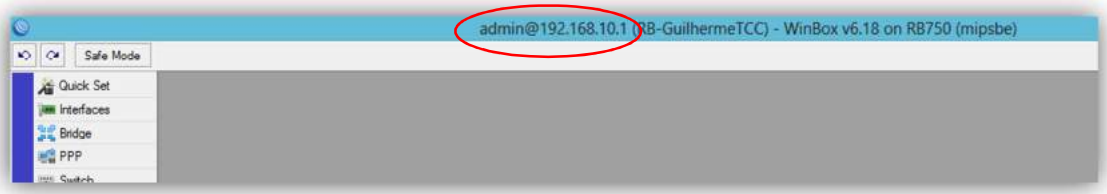

Imagem 24: Conectado no RouterOS pelo endereço de ip

2.7. DHCP CLIENT

A imagem abaixo nos mostra os clientes DHCP existentes em nossa Routerboard, o DHCP Client assim como o DHCP Server, possui uma configuração dinâmica dos dispositivos conectados a ele, mas por ser um cliente ele recebe dinamicamente as configurações de um servidor DHCP externo.

Agora iniciaremos a inclusão de um cliente DHCP em nossa Routerboard. Entraremos no Menu: **IP=>DHCP Client**e selecionaremos a opção ADD, simbolizada no Winbox pelo ícone ✚ .

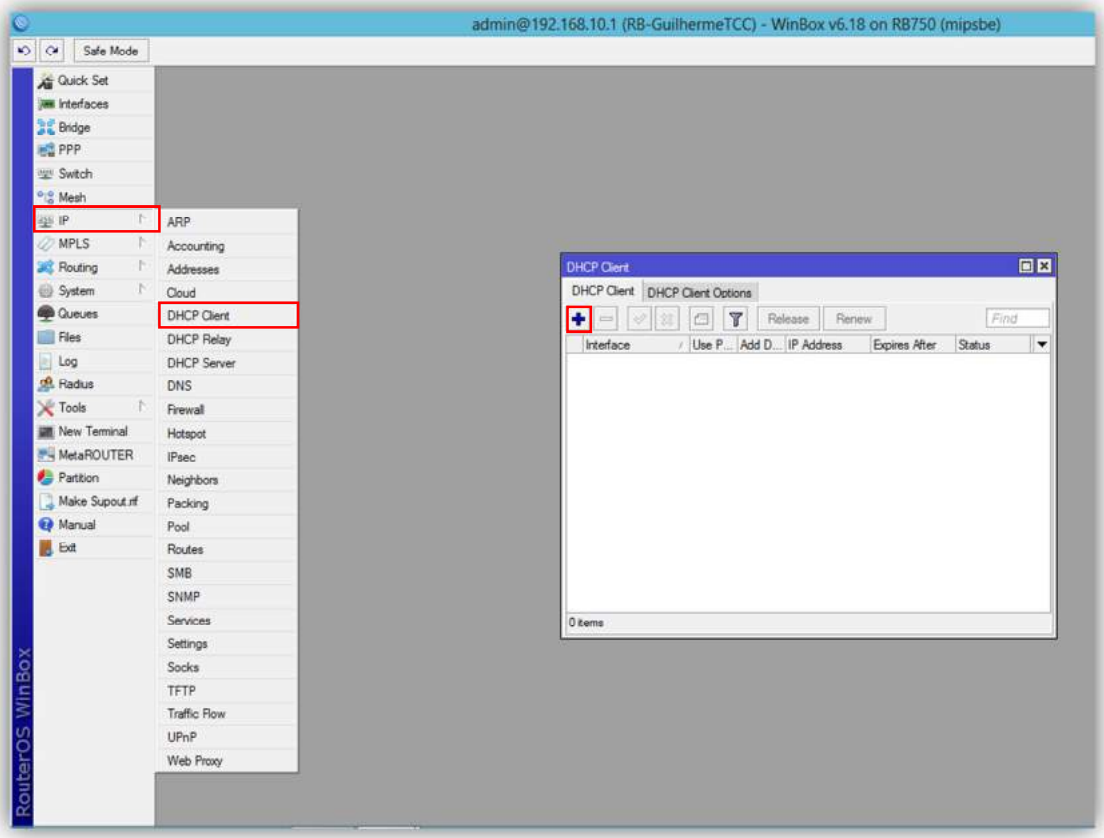

Imagem 25: Tela inicial de configuração do DHCP Client

2.7.1. ADICIONANDO UM NOVO DHCP CLIENT

Na inclusão de um DHCP Client faremos somente a escolha de qual interface será a responsável por receber as configurações dinâmicas, No campo **Interface** selecionaremos UpLink, portanto utilizaremos essa interface para receber o uplink de internet.

As opções **Use peer DNS** e **Use peer NTP** que fazem a sincronia com os servidores DNS e com os relógios dos dispositivos da rede do cliente respectivamente, deixaremos marcados.

Criando um DHCP Client desse modo faremos com que qualquer link de internet possa ser conectado a essa interface, desde que fornecido por um DHCP Server, os demais campos devem permanecer com a configuração padrão do RouterOS, como a figura abaixo.

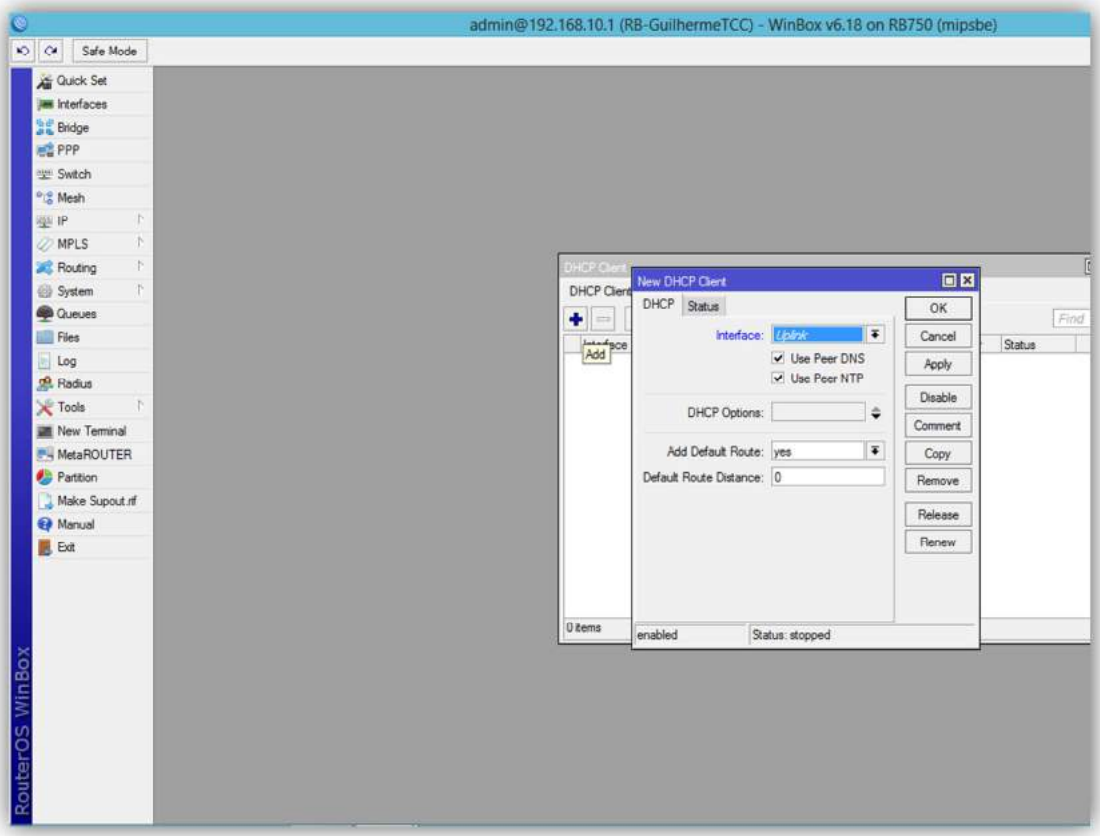

Imagem 26: Tela de inclusão de um DHCP Client

2.7.2. CONECTANDO UM UPLINK AO DHCP CLIENT

Como o protocolo DHCP trabalha dinamicamente, ao conectar o cabo na interface UpLink ele receberá as configurações de ip e DNS do DHCP Server que estiver fornecendo essas configurações e automaticamente configurará os servidores DNS de nossa rede, também criará na opção **Address List** os Address para que nossa rede reconheça e receba os dados da rede que o DHCP Client dinamicamente se configurou. Nas imagens abaixo mostramos como o DHCP se configura após a conexão do cabo do UpLink.

A Imagem28 mostrou que ele recebeu do servidor DHCP externo o endereço de ip 192.168.0.10/24.

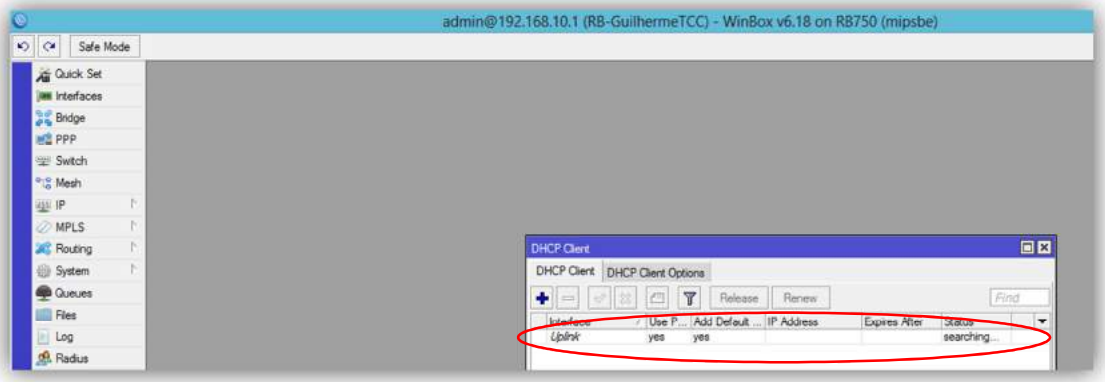

Imagem 27: DHCP Cliente antes da conexão do Uplink

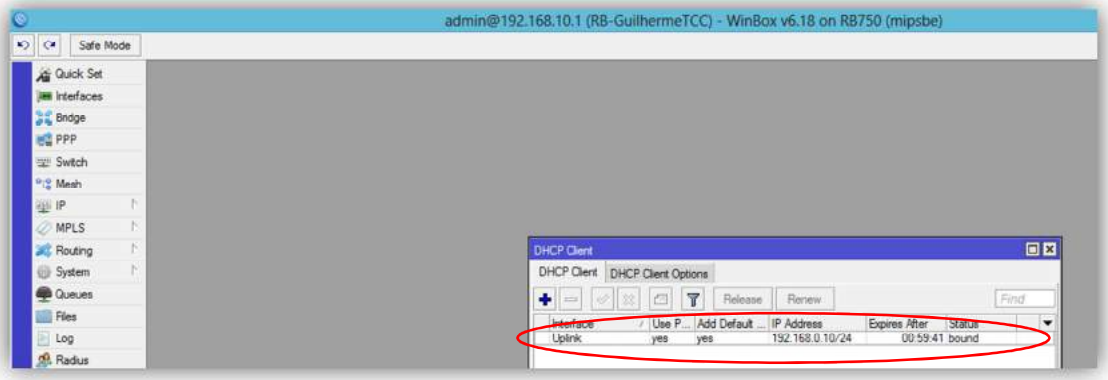

Imagem 28: DHCP Cliente após da conexão do Uplink

A Imagem29 mostrou que após ele receber o endereço de ip 192.168.0.10/24, ele dinamicamente cria o Address com sua Network e configura a interface responsável por ele, a letra **D** no inicio do Address significa **Dynamic**.

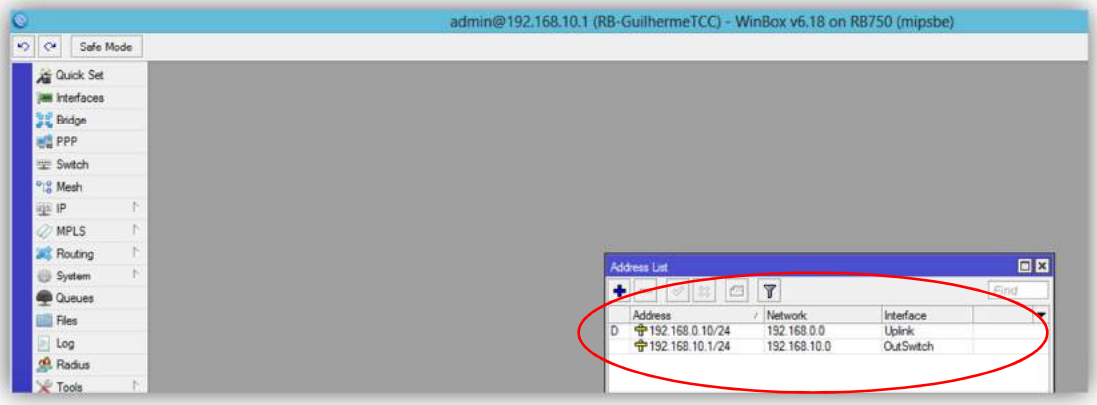

Imagem 29: Criação automática do Address

A Imagem30 mostrou que ele também configurou os servidores DNS automaticamente de acordo com as configurações do DHCP Server externo.

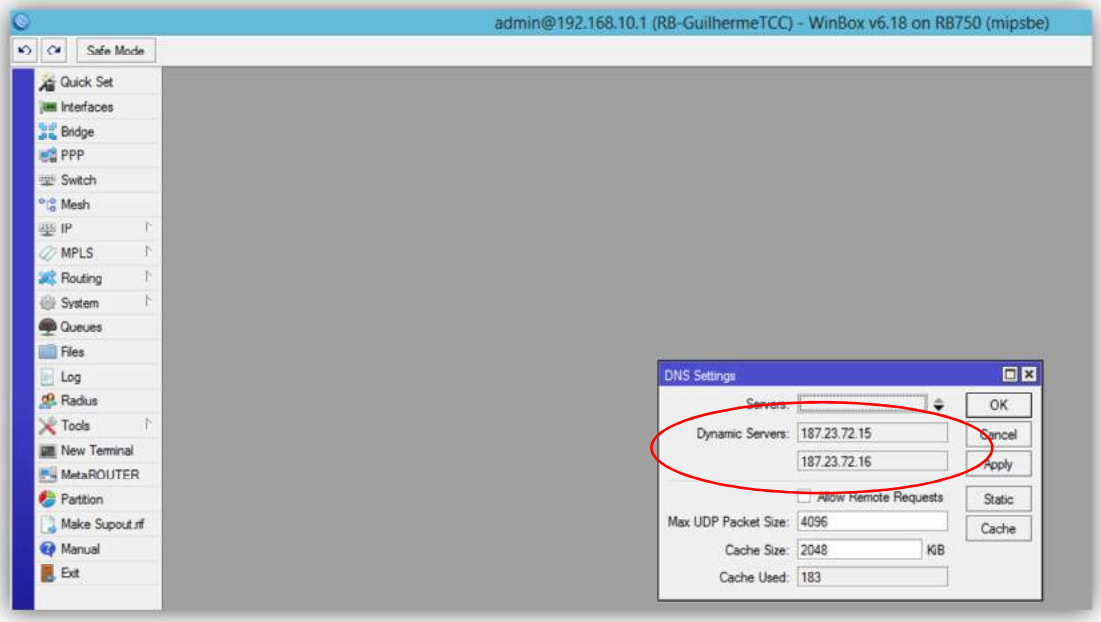

Imagem 30: Configuração automática dos servidores DNS

2.8. TESTANDO A CONEXÃO DA ROUTERBOARD

A conexão do uplink na Routerboard e o reconhecimento do uplink pelo DHCP Client faz com que a Routerboard esteja conectada na internet.

A imagem abaixo nos mostra uma janela do New Terminal com o teste de ping ao host 8.8.8.8 feito com sucesso.

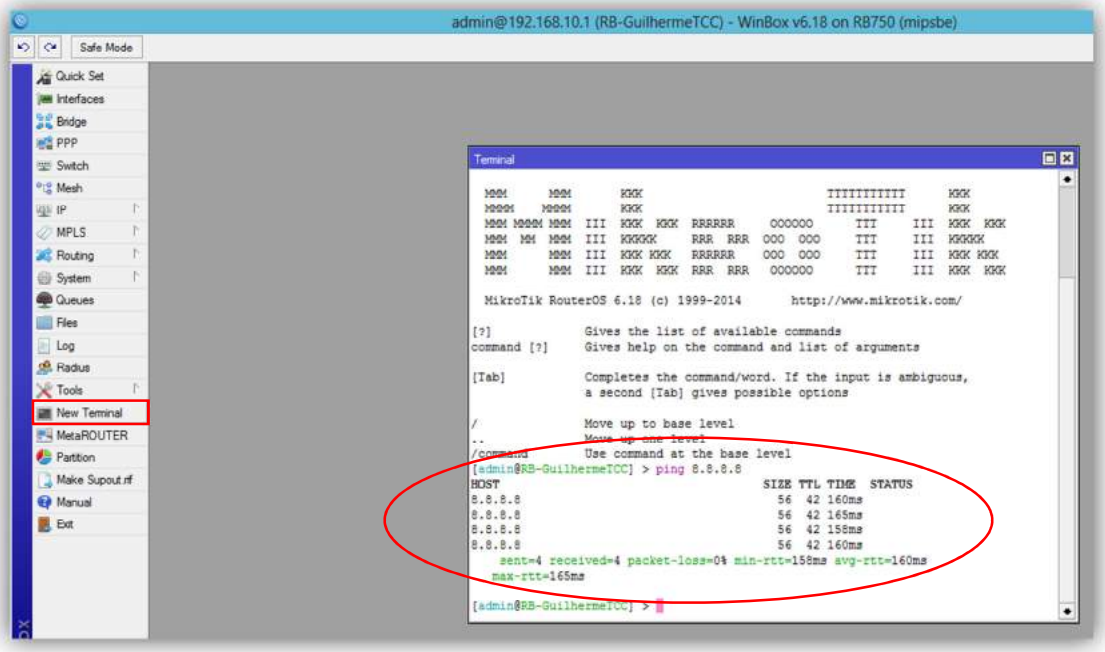

Imagem 31: Tela de teste de ping da Routerboard

2.9. FIREWALL

Após as configurações iniciais para fazermos a Routerboard navegar precisamos configurar o firewall para que a nossa rede tenha permissão do Firewall para trafegar dados.

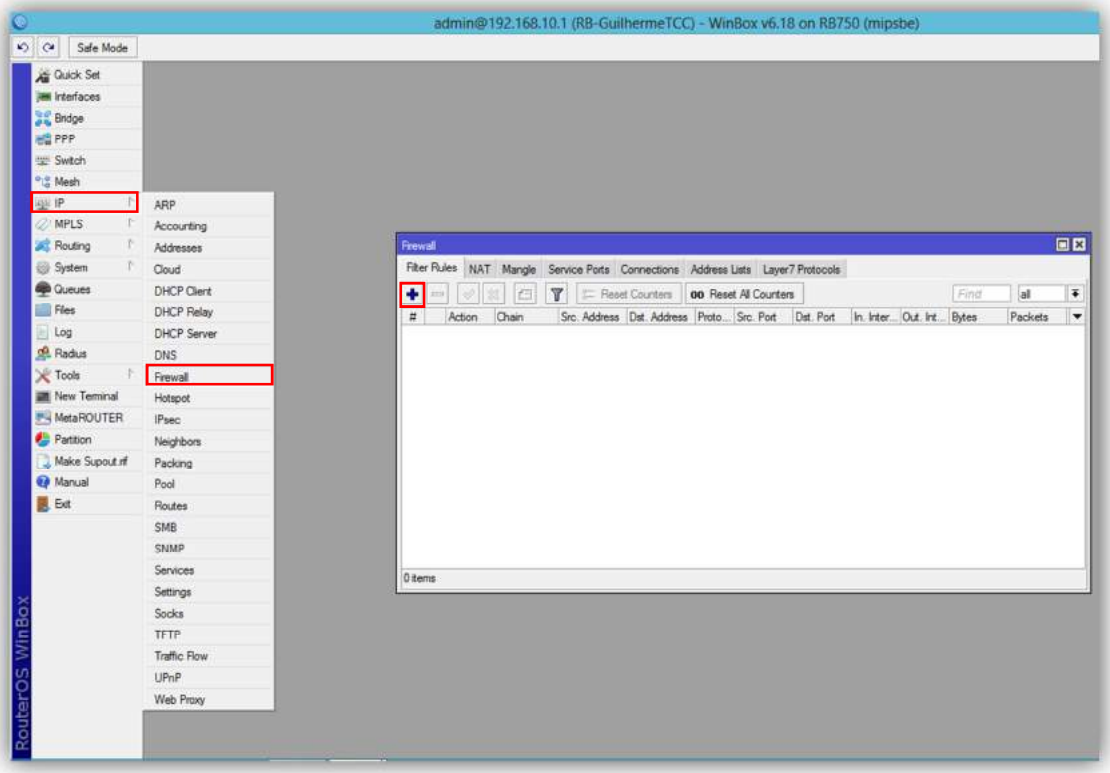

Imagem 32: Tela do Firewall

2.9.1. ADICIONANDO REGRAS DE FIREWALL

Agora iniciaremos a inclusão de uma regra no **Firewall**do RouterOS em nossa Routerboard. Entraremos no Menu: **IP=>Firewall** e selecionaremos a opção ADD, simbolizada no Winbox pelo ícone ✚ , após isso será exibida uma tela de **New Firewall Rule** como pode ser visualizado na imagem abaixo.

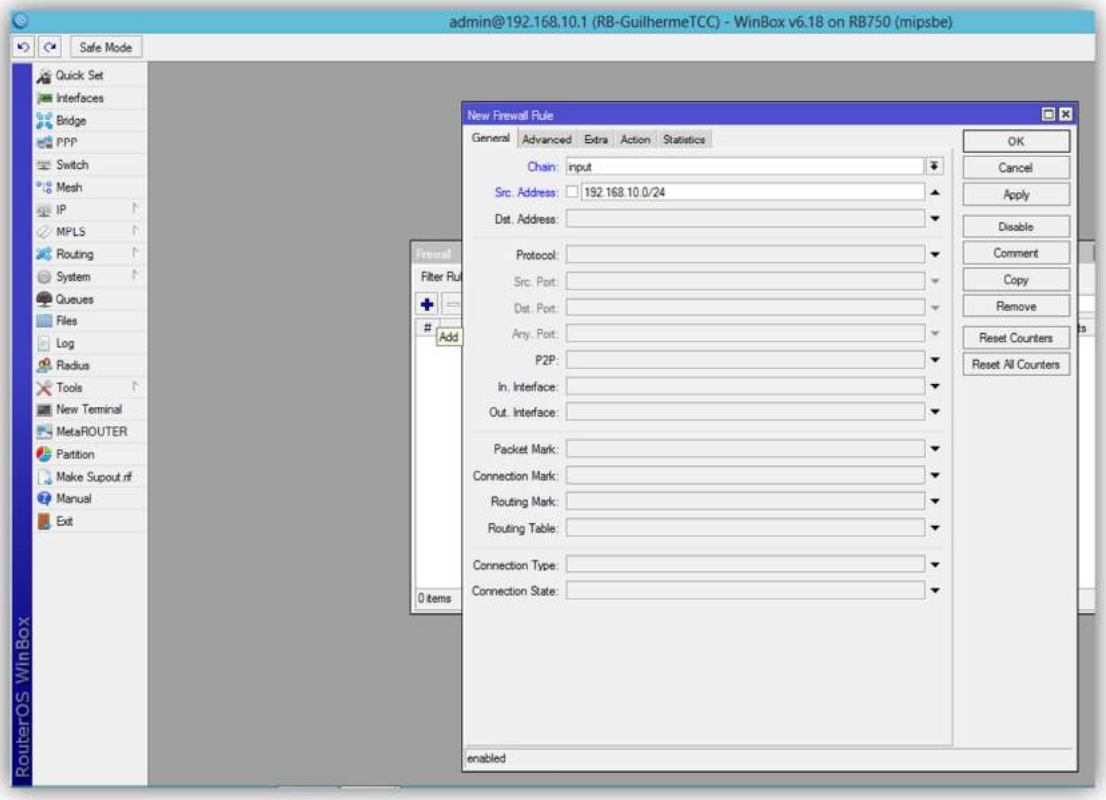

Imagem 33: Tela de criação de regras do Firewall

No campo **Chain** selecionaremos a opção input, ou seja, é todo o tráfego que vai para a Routerboard, no campo **Src.Address** colocaremos a classe e a máscara de sub-rede de nossa rede 192.168.10.0/24, devemos clicar na guia Action e no campo **Action** selecionar a opção accept e em seguida OK, como nos mostra a Imagem34.

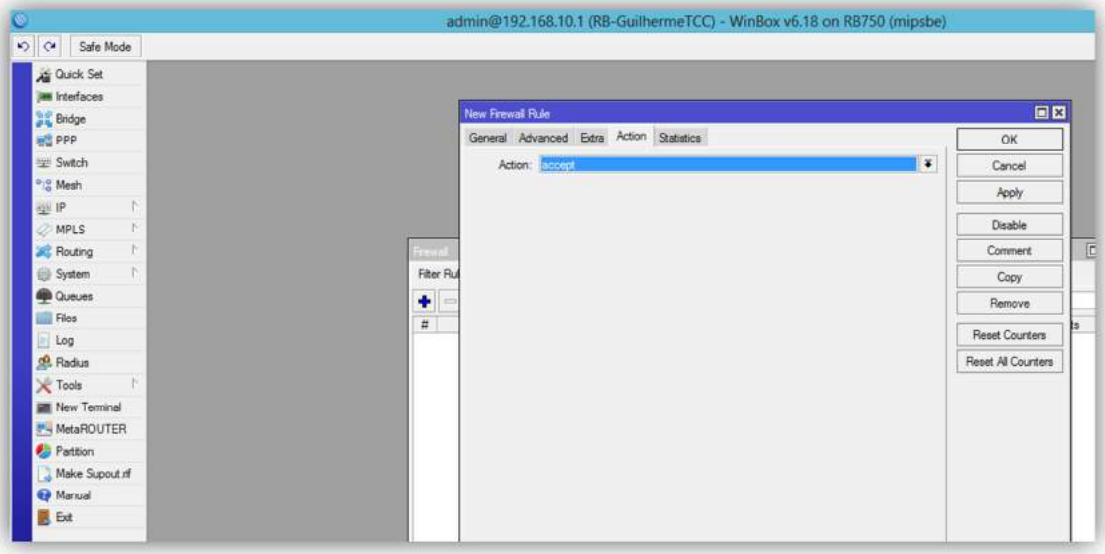

Imagem 34: Tela de criação de regras do Firewall

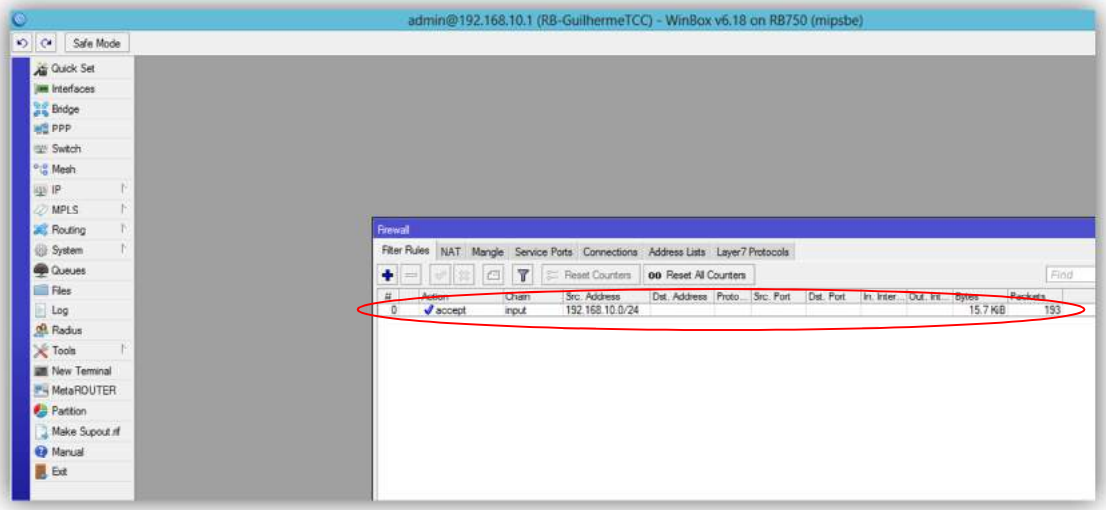

Imagem 35: Após a inclusão de uma regra no Firewall

Essa regra fará com que todo o tráfego que entre na Routerboard**(input)** e que tenha origem da classe 192.168.10.0/24**(Src.Address)** seja aceito e liberado**(accept)**.

2.9.2. ADICIONANDO REGRAS DE NAT

2.9.2.1 ADICIONANDO REGRAS DE MASCARAMENTO DE IP

Agora iniciaremos a inclusão de uma regra de NAT em nossa Routerboard. Entraremos no Menu: **IP=>Firewall** e clicaremos na guia NAT, em seguida na opção ADD, simbolizada no Winbox pelo ícone ✚, após isso será exibida uma tela de **New NAT Rule** como mostra a imagem abaixo.

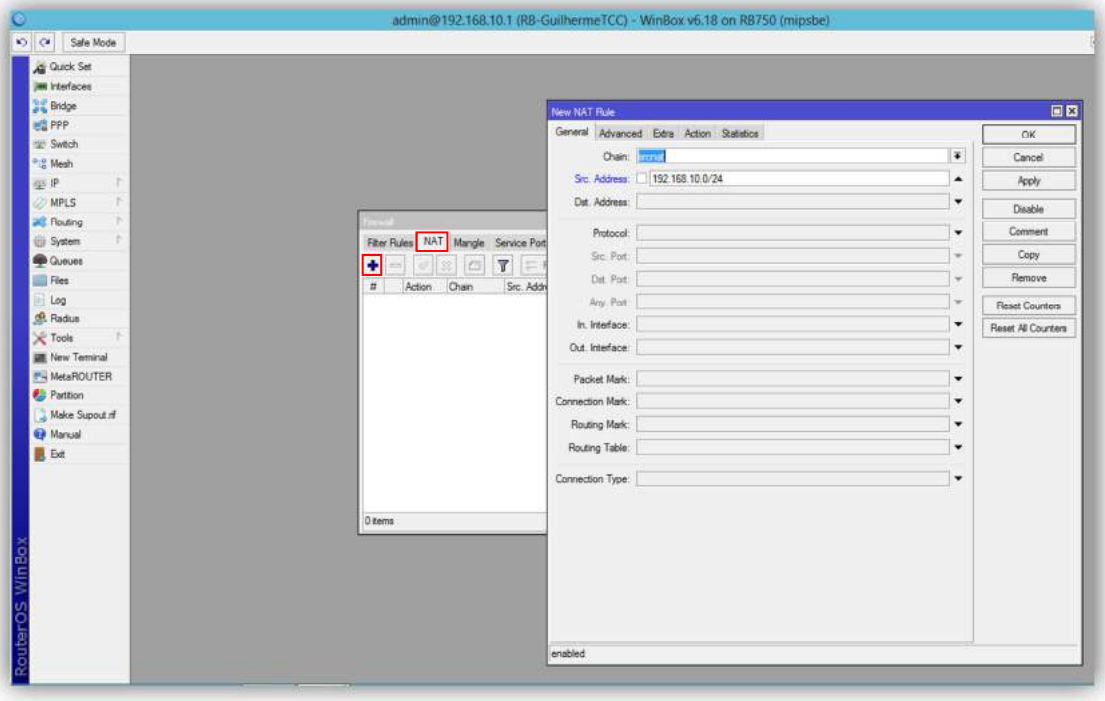

Imagem 36: Tela de inclusão de uma regra de NAT

No campo **Chain** selecionaremos a opção srcnat, e no campo **Src.Address** colocaremos a classe e a máscara de sub-rede de nossa rede 192.168.10.0/24, ou seja, são os pacotes que vierem da rede 192.168.10.0/24 sairão para a Internet com o endereço de ip público disponibilizado pela interface UpLink, devemos clicar na guia Action e no campo **Action** selecionar a opção masquerade e em seguida OK.

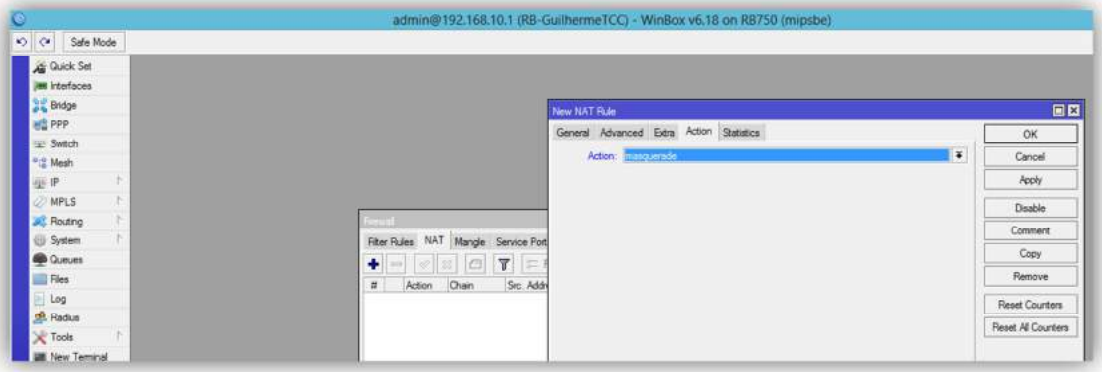

Imagem 37: Tela de inclusão de uma regra de NAT

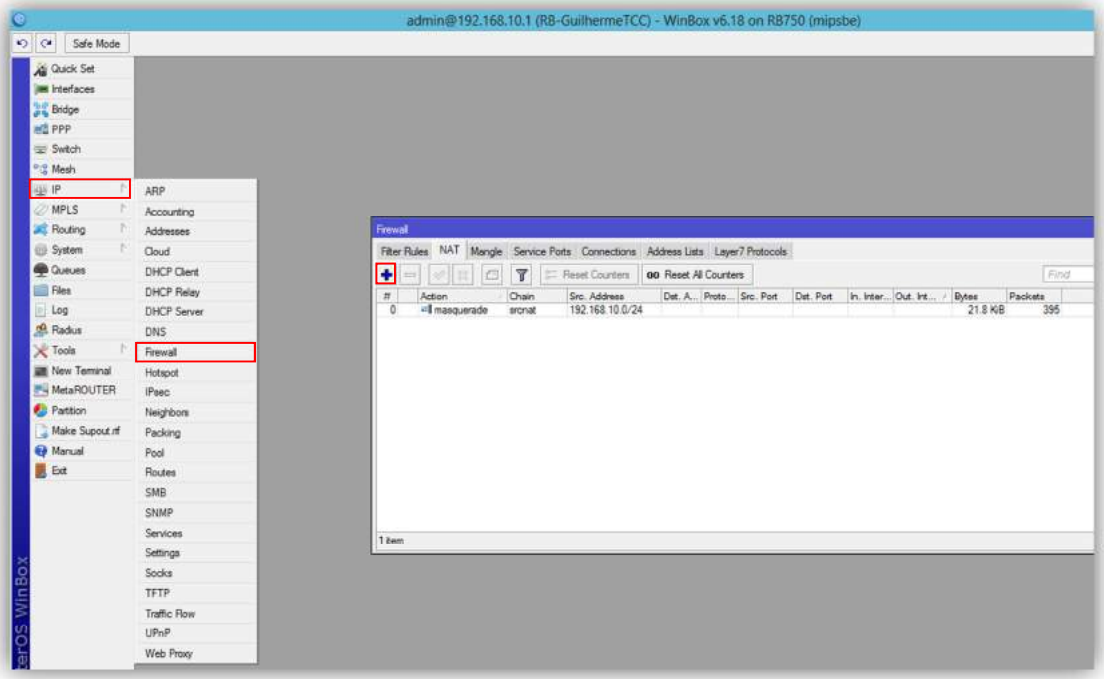

Imagem 38: Após a inclusão de uma regra de NAT

Essa regra fará que todo o tráfego de pacotes que vierem**(srcnat)** da classe 192.168.10.0/24**(Src.Address)** sejam traduzidos**(masquerade)** do endereço de rede local para o endereço de ip público disponibilizado pela interface UpLink ao sair para a internet.

2.9.2.2 ADICIONANDO REGRAS DE REDIRECIONAMENTO DE PORTA

Agora vamos criar uma regra de NAT para o redirecionamento da porta 80(HTTP) para a porta do nosso Web Proxy, que será configurado nos tópicos a seguir, usaremos a porta 3128 para o Web Proxy.

No campo **Chain** selecionaremos a opção dstnat, no campo **Src.Address** colocaremos a classe e a máscara de sub-rede de nossa rede 192.168.10.0/24, no campo **Protocol** selecionaremos a opção 6(tcp) e **Dst.Port**. colocaremos a porta 80, após isso devemos clicar na guia Action e no campo **Action** vamos selecionar a opção redirect e na opção **To Ports** colocaremos a porta 3128, em seguida clicaremos em OK.

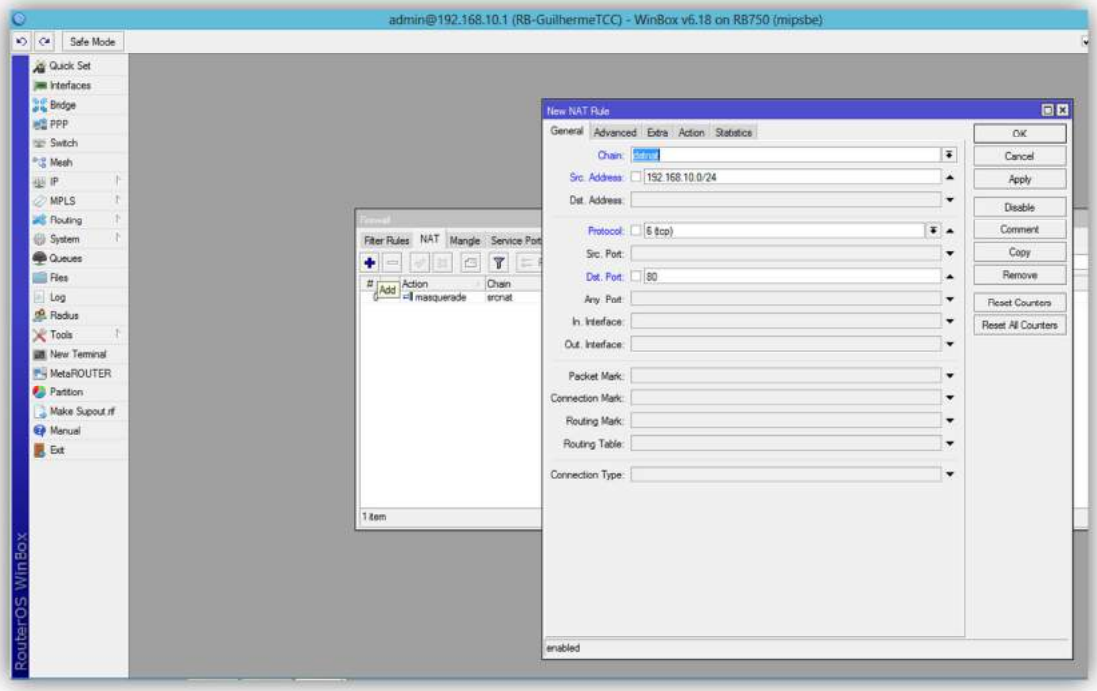

Imagem 39: Tela de inclusão de uma regra de NAT

Essa regra fará que todo o tráfego de pacotes que trafegarem com destino**(dstnat)** à classe 192.168.10.0/24**(Src.Address)** sejam redirecionados**(redirect)** da porta 80(**Dst.Port**) para a porta 3128(**To Ports**) antes que sejam liberados para o usuário.

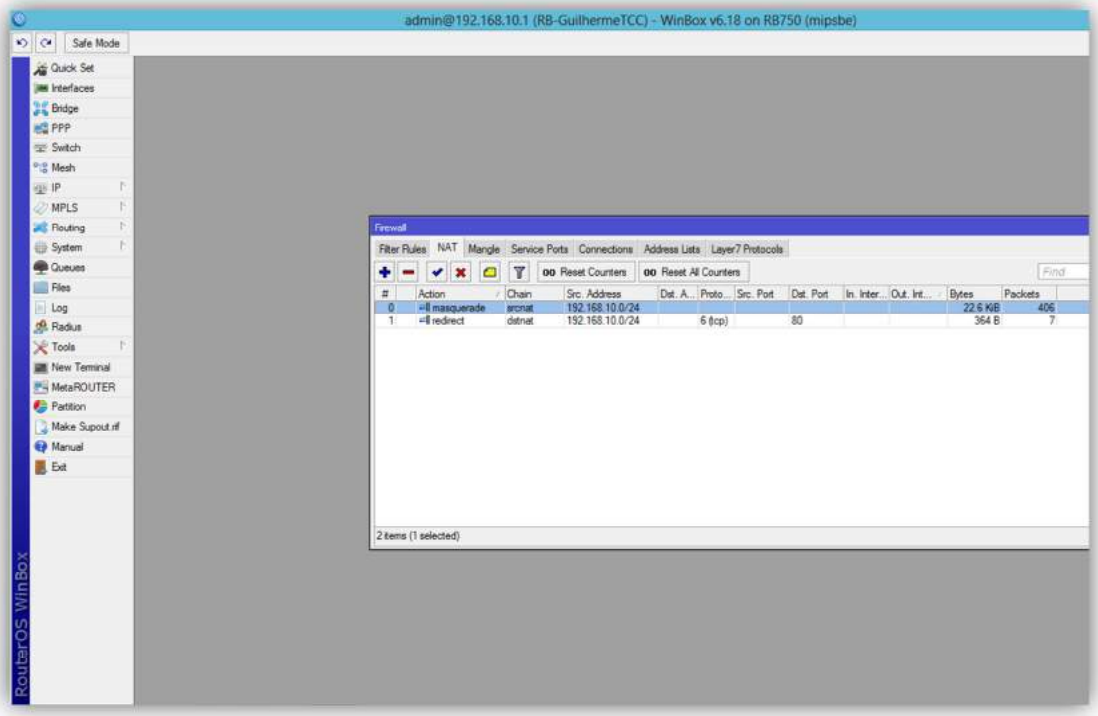

Imagem 40: Tela após a inclusão das regras de NAT

2.10. WEBPROXY

2.10.1. CONFIGURANDO O WEB PROXY

Agora iniciaremos a configuração de nosso Web Proxy. Entraremos no Menu: **IP=>Web Proxy** e clicaremos na opção Enable, habilitando assim o nosso Web Proxy. Colocaremos a porta 3128 como a porta do Web Proxy, que será a porta que o NAT fará o redirecionamento da porta 80 para a 3128, como configuramos anteriormente no **Firewall=>NAT.**

No campo **Cache Administrator** colocaremos um nome ou email de referência para que o usuário que sofre algum bloqueio e necessite de suporte consiga contactar o responsável pelas regras do Web Proxy, nesse caso colocaremos o email guilhermelevy.cpd@faculdadeguairaca.com.br

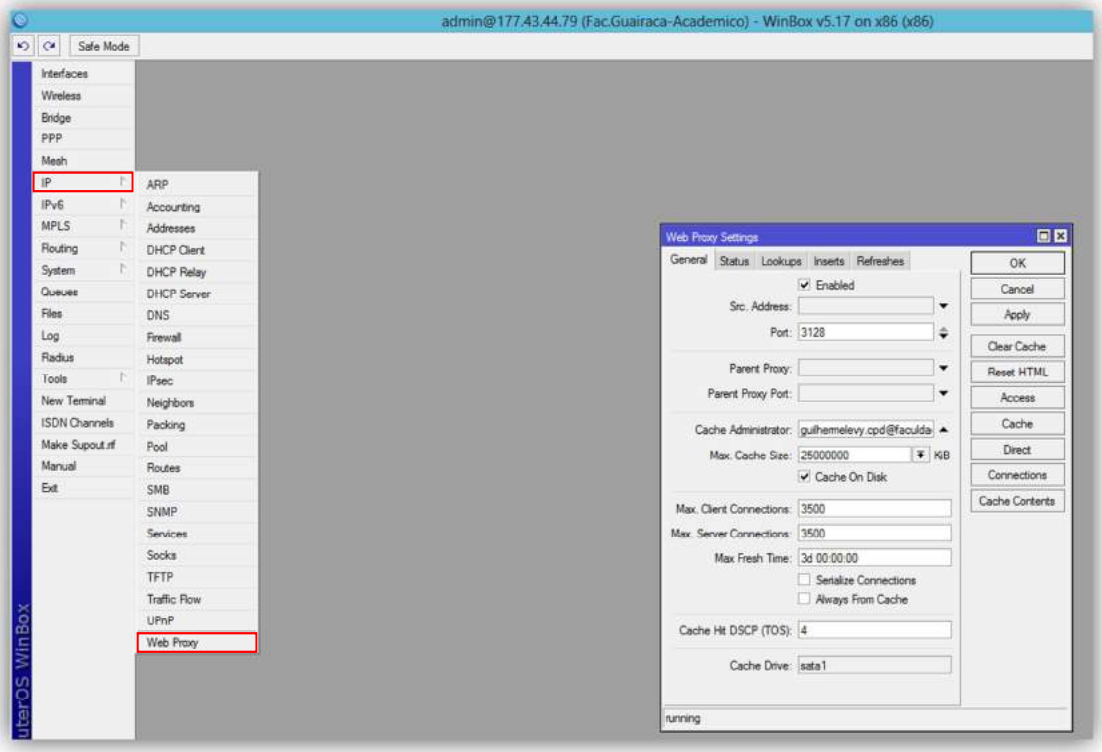

Imagem 41: Tela de configuração inicial do Web Proxy

A opção **Max.Cache Size** serve para quando o administrador deseja criar uma área no armazenamento do RouterOS para fazer um cache no Web Proxy, ele colocará uma quantidade, por exemplo 500000KiB (500MB) e marcará a opção **Cache On Disk**. No nosso caso, por utilizarmos uma Routerboard com pouco espaço de armazenamento não utilizaremos essa opção de Cache On Disk.

Na opção **Max.Client Connections**, que seria a quantidade máxima de conexões simultâneas no proxy deixaremos 1500. Na opção **Max.Server Connections**, que seria a quantidade máxima de conexões simultâneas no proxy para servidores externos deixaremos 1500.

Os demais campo deverão ficar no padrão do RouterOS como a Imagem41.

2.10.2. ADICIONANDO REGRAS NO WEB PROXY

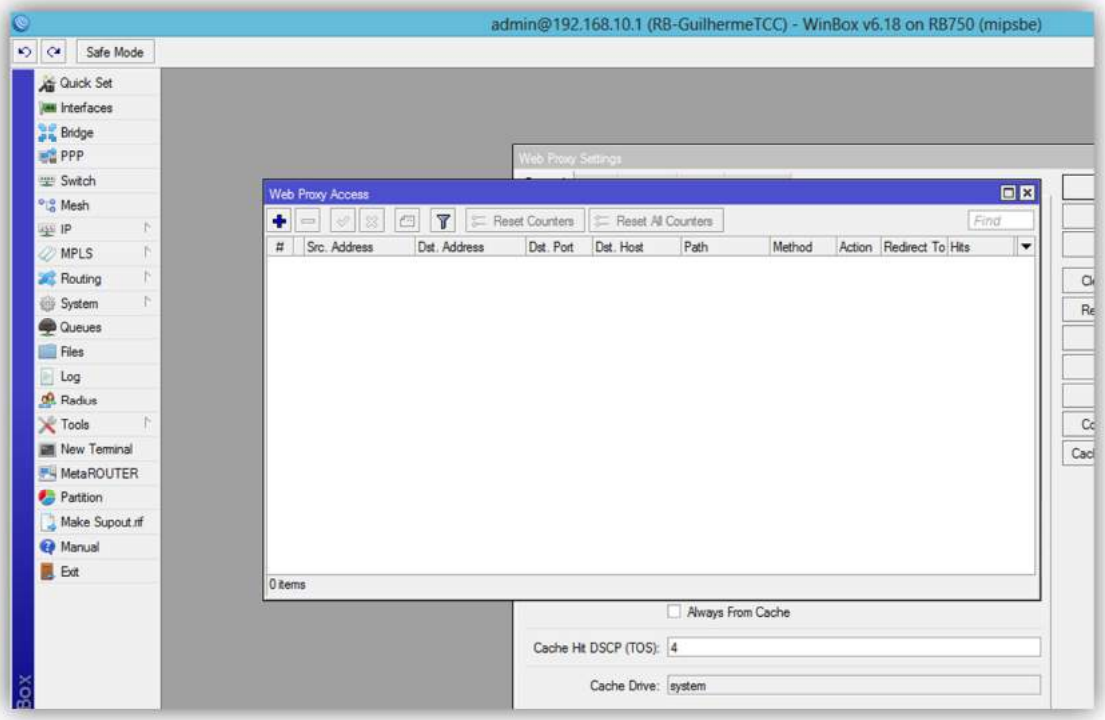

Imagem 42: Tela de configuração das regras do Web Proxy

Após a configuração inicial do Web Proxy podemos iniciar a criação das regras, clicaremos na opção ADD, simbolizada no Winbox pelo ícone ✚ .

Primeiramente criaremos a liberação da classe da nossa rede, no campo **Src.Address** colocaremos a classe da rede que queremos que essa regra se aplique, nesse caso 192.168.10.0/24 e no campo **Action** selecionaremos a opção allow que libera o trafego para essa rede.

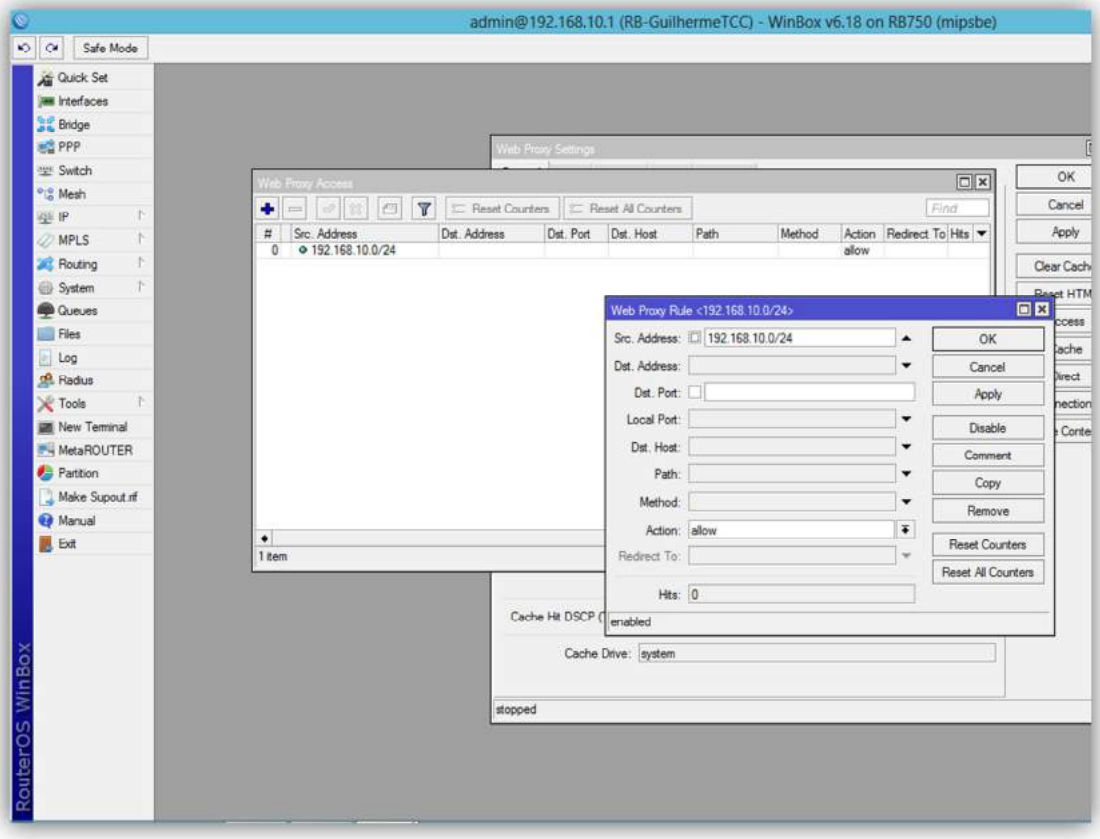

Imagem 43: Liberando o tráfego da classe principal

2.10.3. BLOQUEANDO TERMOS NO WEBPROXY

Agora criaremos duas regras de bloqueio para dois termos(palavras) dentro de nosso Web Proxy, no caso de regras de bloqueio por palavras preencheremos somente o campo **Dst.Host** com a palavra a ser bloqueada e no campo **Action** selecionaremos a opção deny que nega o tráfego dos dados que contenham essa palavra em seus endereços, ou seja, o Web Proxy bloqueará as páginas HTTP que contenham em seu endereço a palavra especificada.

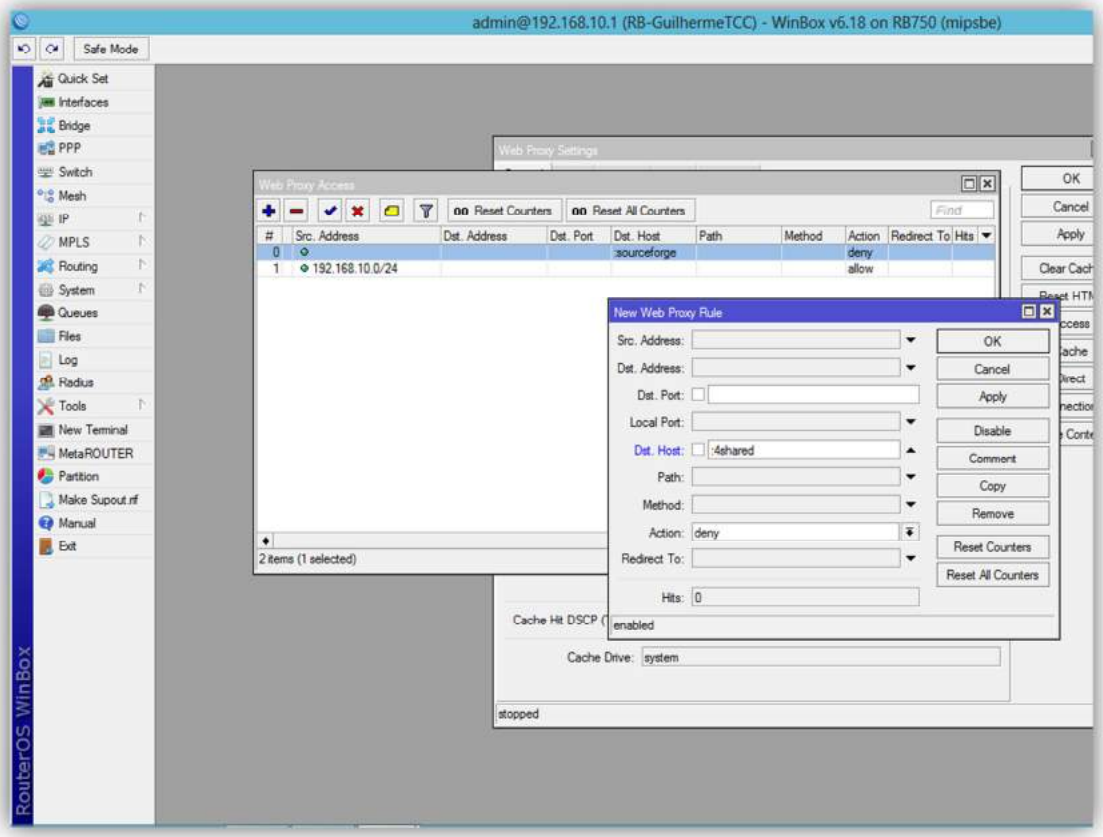

Imagem 44: Bloqueando o termo “4shared”

Nessas duas regras nós bloqueamos as palavras “4shared” e “sourceforge”.

2.10.4. O FUNCIONAMENTO DO WEBPROXY

Como em todas a regras do RouterOs, o Web Proxy trata suas regras através do princípio da gravidade, o sistema começa a leitura das regras por ordem, seguindo sua numeração(#), ou seja, de cima para baixo e para ao se adequar em uma das regras.

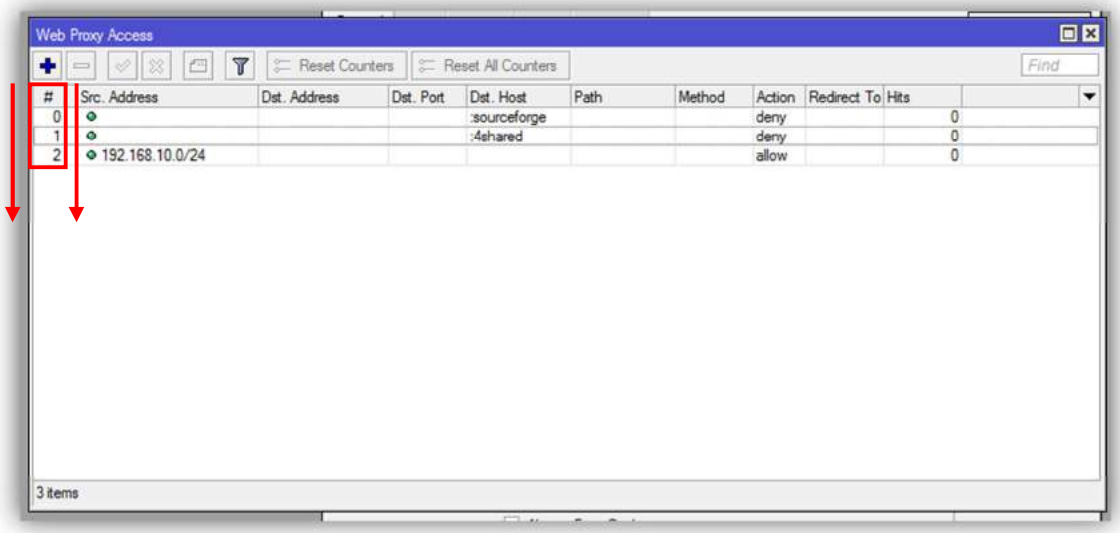

Imagem 45: Adequação da regra por gravidade

Como nos mostra a Imagem45, se o usuário com o endereço de ip 192.168.10.5 tentar acessar o site www.uol.com.br o pacote irá testar todas as regras e como não há nenhuma restrição nos itens 0 e 1 chegará ao item 3, se adequando a essa regra que libera o tráfego para a classe na qual ele se encontra. Se esse mesmo usuário tentar acessar o site www.4shared.com ele testaria a regra 0, passaria para a próxima regra mas se adequaria à regra 1 em que ele bloqueia os endereços com a palavra 4shared, descartando nessa hora o pacote sem passar para a próxima regra.

Nas duas imagens abaixo podemos visualizar como será a mensagem de negação no microcomputador do usuário quando ele tentar acessar um dos sites que estiverem com as regras de bloqueio.

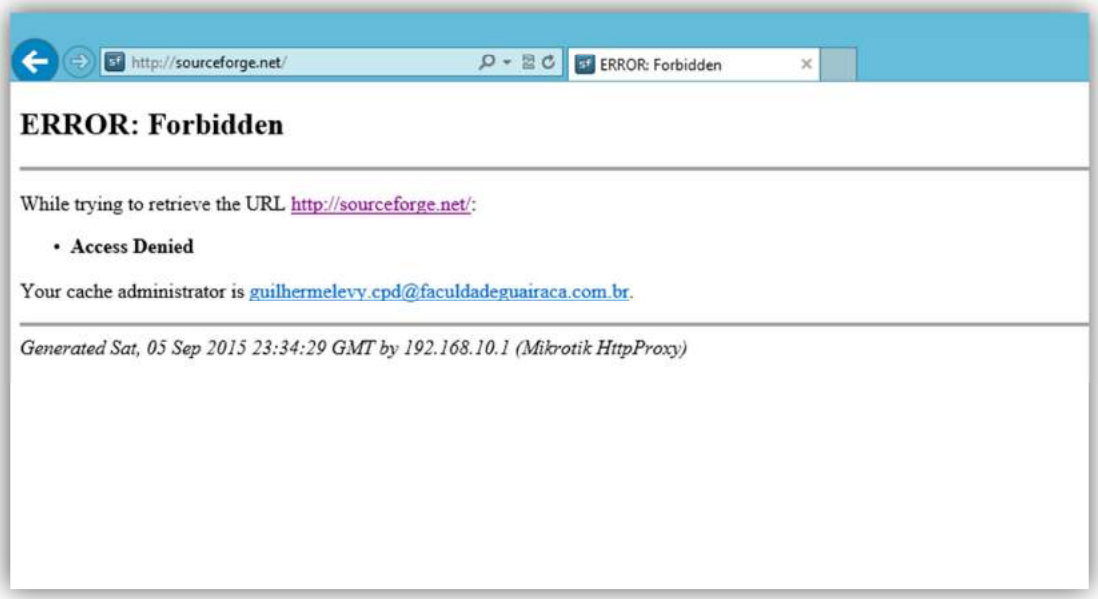

Imagem 46: Tela com a negação do site sourceforge.net

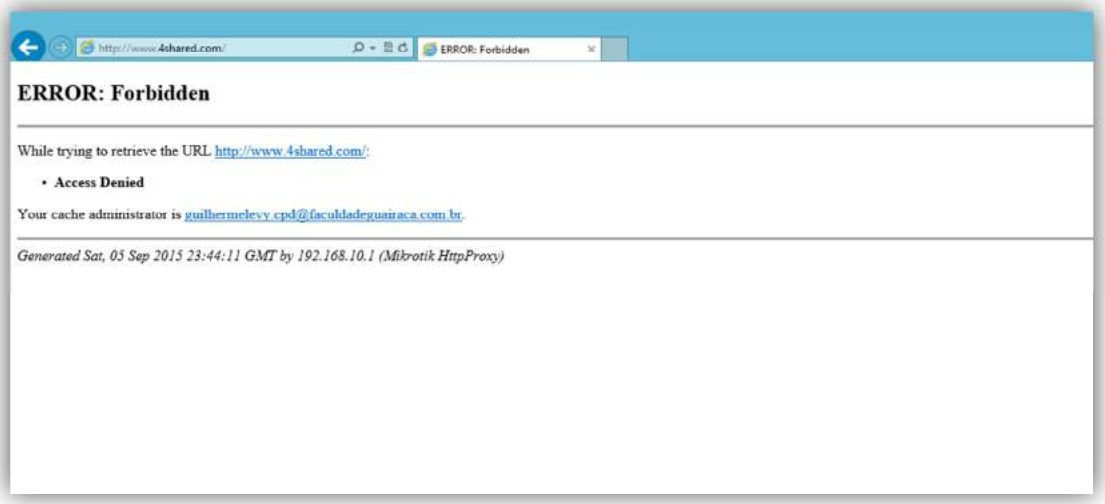

Imagem 47: Tela com a negação do site 4shared.com

2.11. HOTSPOT

Com a estrutura de nossa rede finalizada podemos agora iniciar a criação e configuração de nosso servidor Hotspot. Entraremos no Menu: **IP=>Hotspot,** na guia **Servers** e selecionaremos a opção ADD, simbolizada no Winbox pelo ícone ✚ .

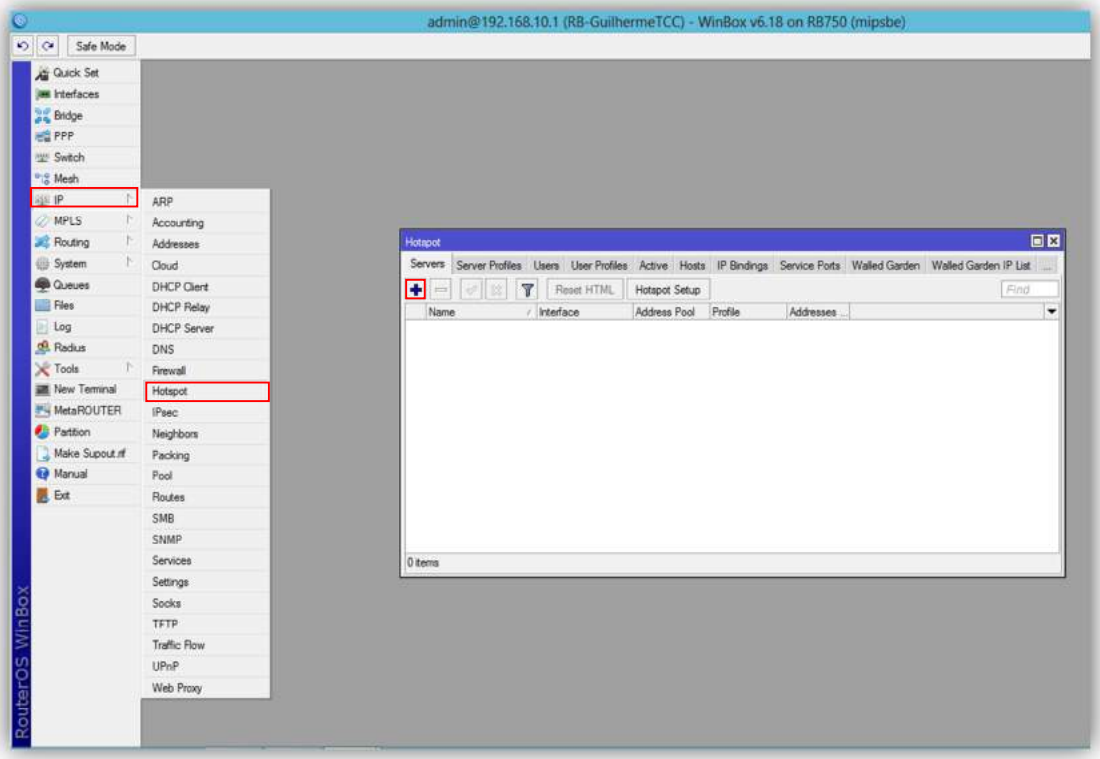

Imagem 48: Tela inicial de configuração de um Hotspot Server

2.11.1. ADICIONANDO UM HOTSPOT SERVER

No campo **Name** colocaremos o server1, que será o nome do nosso servidor Hotspot, no campo **Interface** selecionaremos a interface que será responsável por fornecer os dados já tratados pelo nosso Hotspot, no campo **Address Pool** escolheremos qual a faixa de endereços que queremos que o Hotspot forneça aos usuários que nele se conectarem, o campo **Idle TimeOut** será o período de ociosidade máximo permitido por nosso servidor para os clientes autenticados, se não houver trasmissão de dados para o servidor nesse período a sessão com esse usuário será finalizada, deixaremos 02:00:00 horas nesse campo e para finalizar o campo **Addresses per MAC** que é a quantidade de endereços de ip permitidos para cada endereço MAC dos clientes, deixaremos 2, pois se o cliente vier com seu microcomputador ou dispositivo já com um ip configurado manualmente e que não seja da classe de nossa rede o Hotspot automaticamente lhe fornecerá um endereço de ip da nossa rede para que ele possa trafegar nela, vinculando assim os dois endereços de ip a esse endereço MAC. Os demais campos permanecem no padrão do RouterOS.

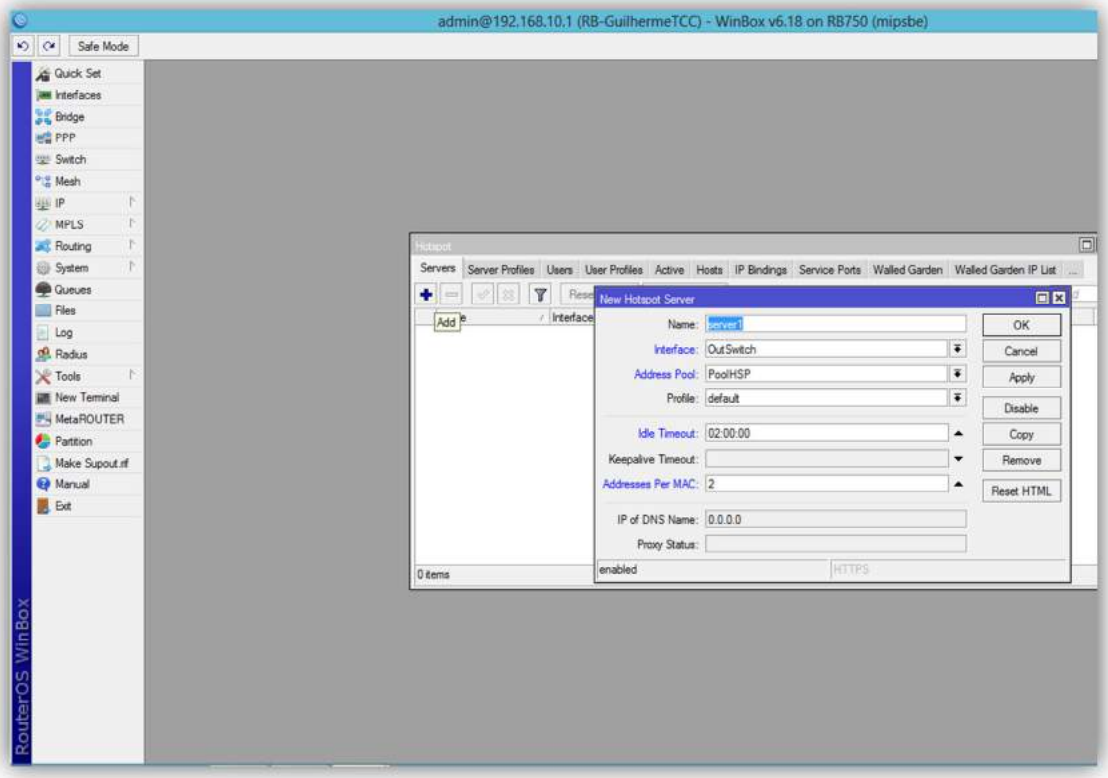

Imagem 49: Tela de inclusão de um Hotspot Server

Na imagem abaixo podemos visualizar como ficará a tela inicial do Hotspot após a inclusão de um servidor Hotspot.

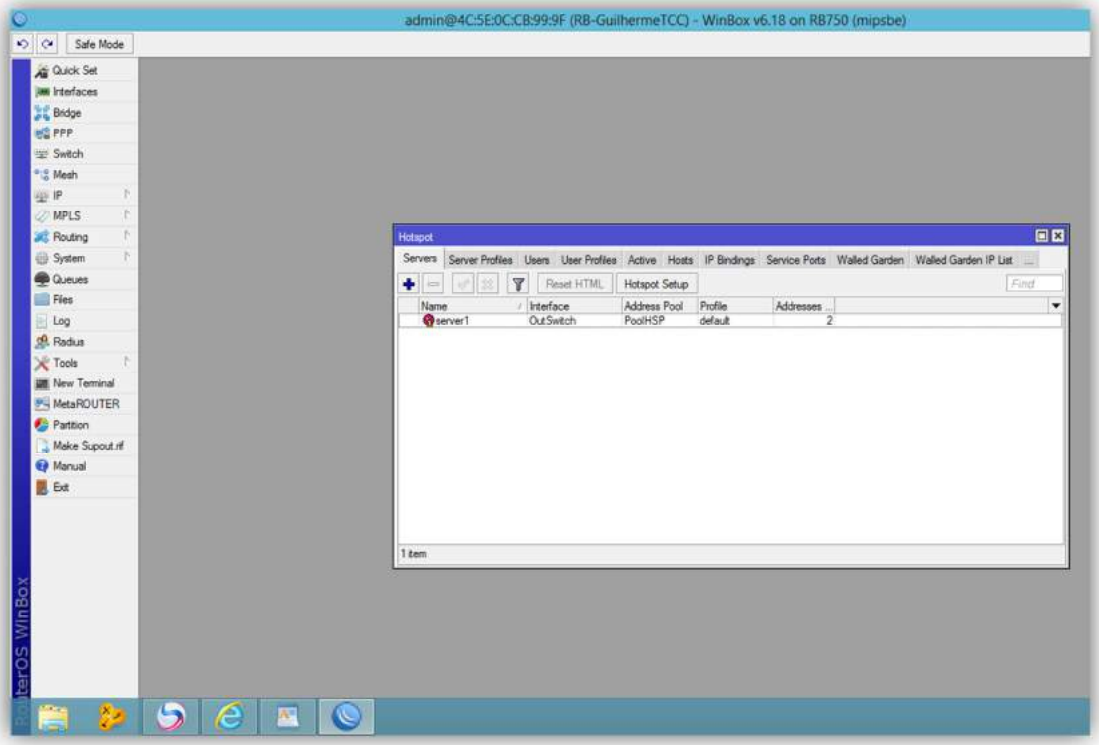

Imagem 50: Tela após a inclusão de um Hotspot Server

2.11.2. CONFIGURANDO UM HOTSPOT SERVER PROFILE

Agora iremos configurar o perfil default do servidor Hotspot. Entraremos no Menu: **IP=>Hotspot** e clicaremos na guia Server Profiles, em seguida daremos um duplo clique encima do perfil padrão existente em nosso Hotspot, o perfil default.

Nesse perfil existente somente iremos alterar o campo **DNS Name**, que é o nome pelo qual nosso Hotspot será identificado e acessado manualmente, colocaremos Hotspottcc.com.br nesse campo.O DNS Name aparecerá na tela de login do Hotspot e irá mascarar o endereço de ip do Hotspot. Agora clicaremos em OK finalizando a configuração.

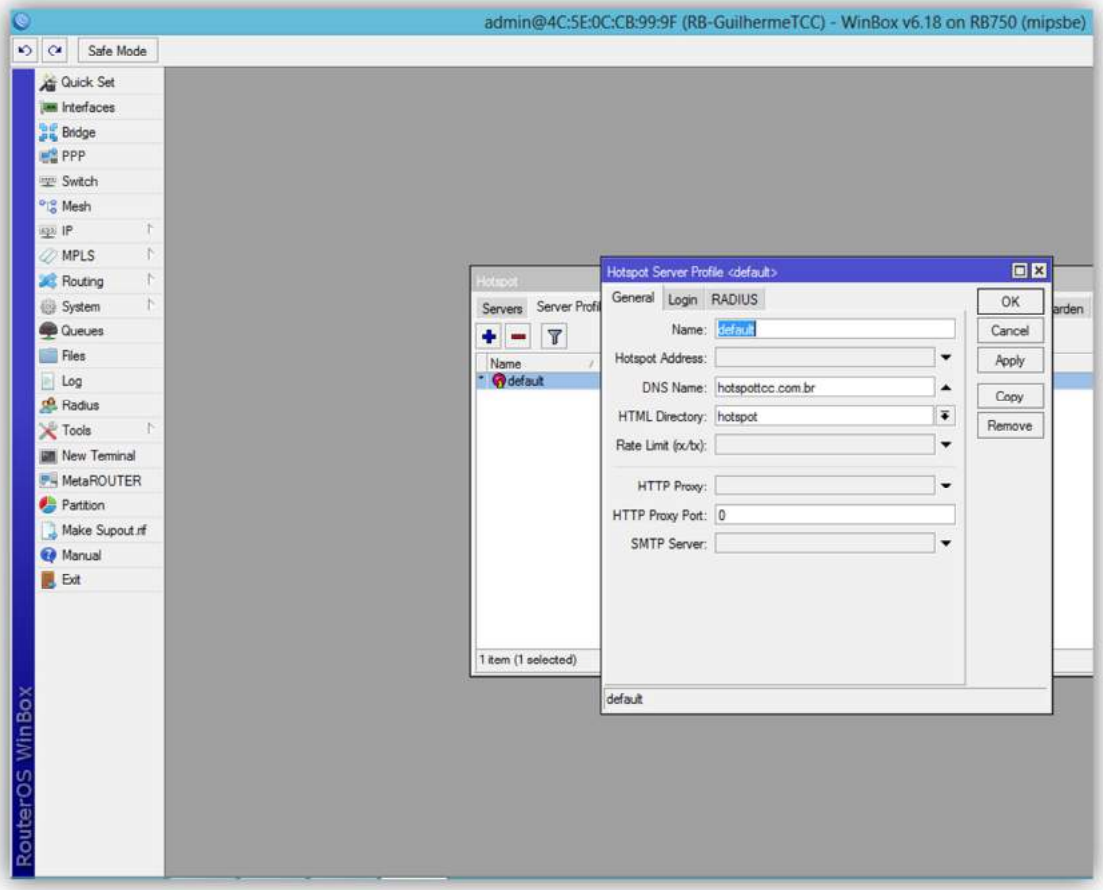

Imagem 51: Configuração do Hotspot Server Profile default

Os demais campos devem permanecer no padrão do RouterOS, conforme a Imagem51.

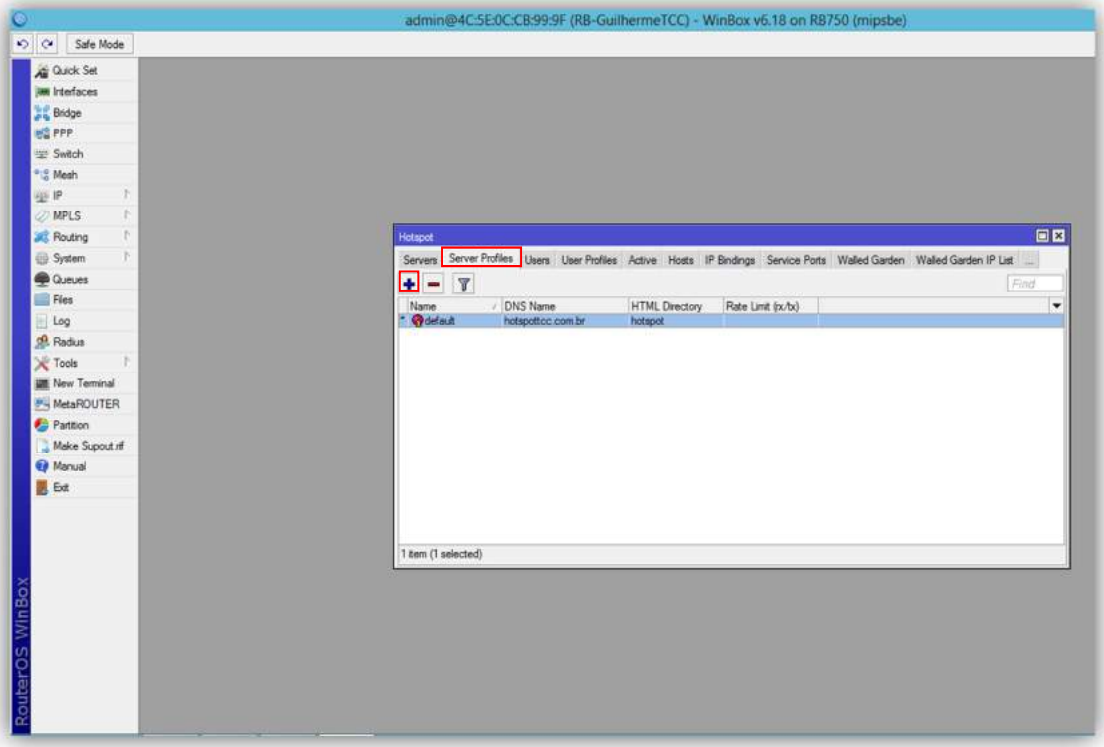

Imagem 52: Tela após a inclusão de um Hotspot Server Profile

2.11.3. CONFIGURANDO UM HOTSPOT USER PROFILE

Primeiramente iremos configurar o perfil default de usuário do Hotspot. Entraremos no Menu: **IP=>Hotspot** e clicaremos na guia User Profiles, em seguida daremos um duplo clique encima do perfil padrão existente em nosso Hotspot, o perfil default.

Deixaremos o **Name** como default, no campo **Address Pool** selecionaremos o Pool de endereços de ip que fornecerá o ip ao nosso cliente após a autenticação, no campo **Idle Timeout** selecionaremos a opção none, ou seja, não finalizará a sessão se o usuário ficar um período de tempo ocioso. O campo **Shared Users** nos diz quantos usuários simultâneos com a mesma credencial poderão estar autenticados, em nosso caso permitiremos um usuário autenticado com a mesma credencial. O campo **Rate Limit** é responsável pelo limite de banda de perfil de usuário, iremos colocar 5Mb de upload e 5Mb de download para cada um dos usuários autenticados com esse perfil, ou seja, 5M/5M. Os demais campos deverão ficar no padrão do RouterOS, como na imagem abaixo.

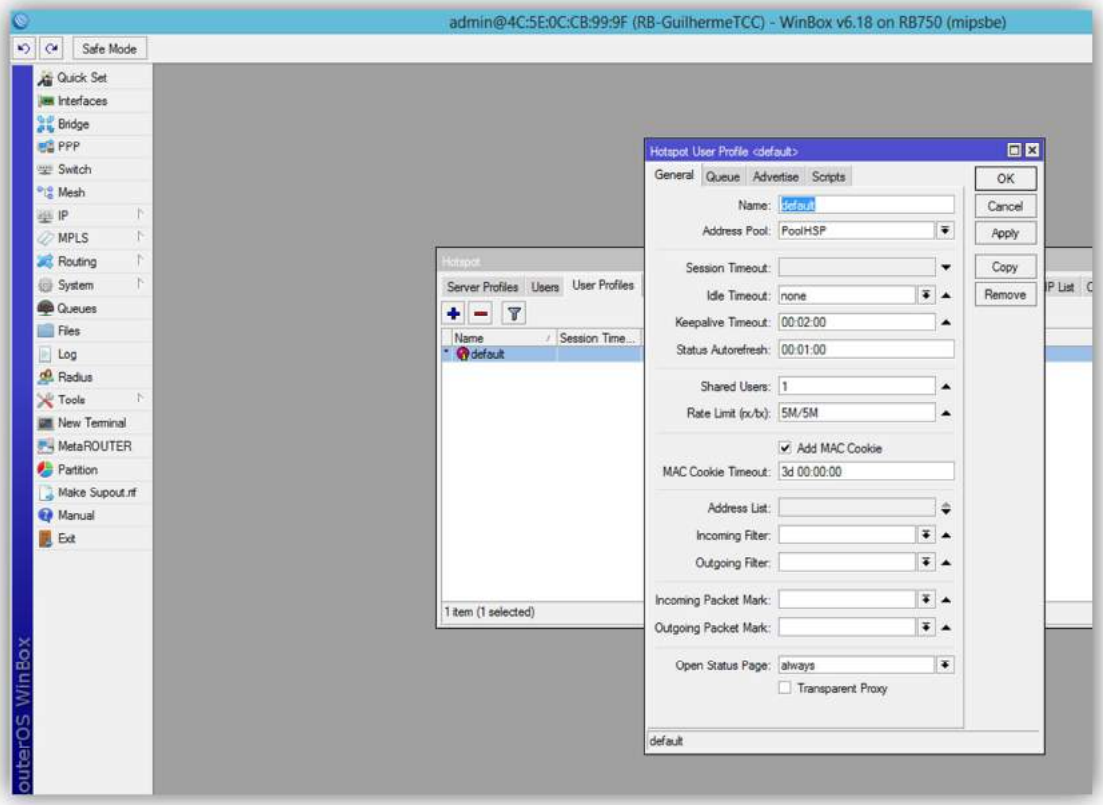

Imagem 53: Tela após a inclusão de um Hotspot User Profile

Seguindo os passos anteriores para a configuração de um User Profile, faremos também a inclusão de um User Profile Limitado em nosso Hotspot. Clicaremos na opção ADD, simbolizada no Winbox pelo ícone ✚ , após isso será exibida uma tela de **New User Profile**.

Daremos o nome de limitado a esse perfil e no campo **Rate Limit** daremos um limite de banda de 1Mb de upload e 1Mb de download para cada um dos usuários autenticados nesse perfil, ou seja, 1M/1M

Após a inclusão dos dois perfis de usuário a tela de User Profiles deverá estar como a imagem abaixo.

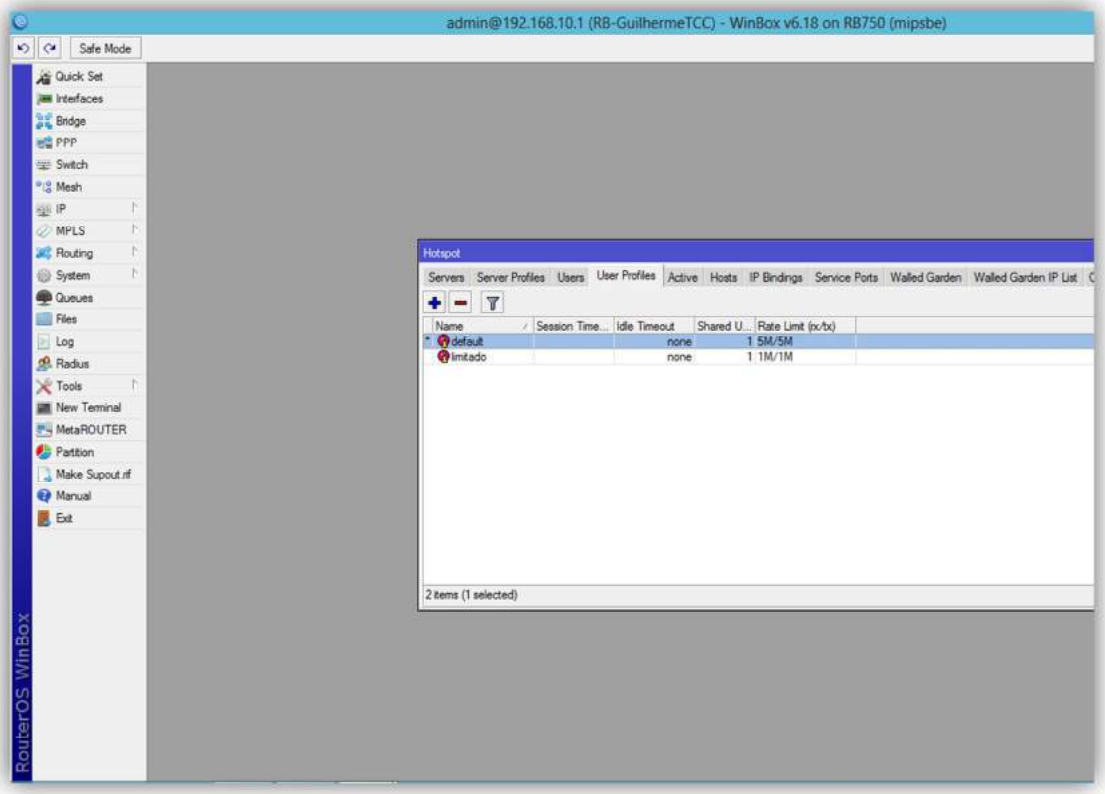

Imagem 54: Tela após a inclusão dos Hotspot User Profile

2.11.4. ADICIONANDO USUÁRIOS

Agora iremos criar os usuários que poderão autenticar em nosso Hotspot, clicaremos na guia User e na tela inicial de usuários clicaremos na opção ADD, simbolizada no Winbox pelo ícone ✚ , após isso será exibida a tela **Hotspot User**, que é a tela de inclusão de usuários, como na Imagem56.

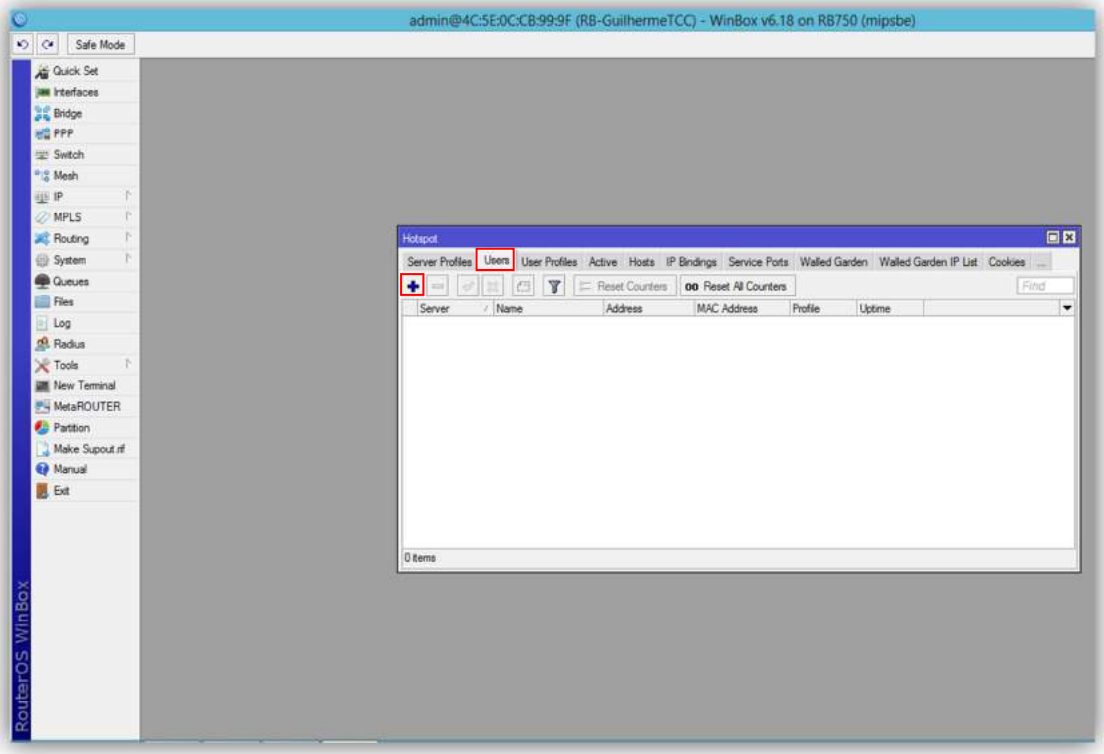

Imagem 55: Tela inicial dos usuários cadastrados no Hotspot

2.11.4.1. USUÁRIO AUTENTICANDO COM SENHA

No campo **Name** colocaremos o nome que nosso usuário efetuará a autenticação, no campo **Password** colocaremos a senha que o usuário utilizará, no nosso caso utilizaremos o usuário e senha admin.

O campo **Address** não será alterado, esse campo é utilizado quando desejamos dar um ip estático para um determinado usuário. No campo **Profile** selecionaremos o perfil que esse usuário estará vinculado quando se autenticar, nesse caso ele será vinculado ao perfil default, que possui um limite de banda maior, conforme especificamos no Hotspot Users Profile anteriormente. Os demais campos devem ficar no padrão do RouterOS, como mostra a imagem abaixo.

Esse modo de autenticação estará disponível ao cliente que possuir usuário e senha cadastrado, podendo ser utilizado esse usuario e senha em qualquer microcomputador ou dispositivo.

Criaremos também um segundo usuário com o nome de user e nele utilizaremos o perfil limitado, que disponibiliza menos limite de banda, conforme o User Profile.

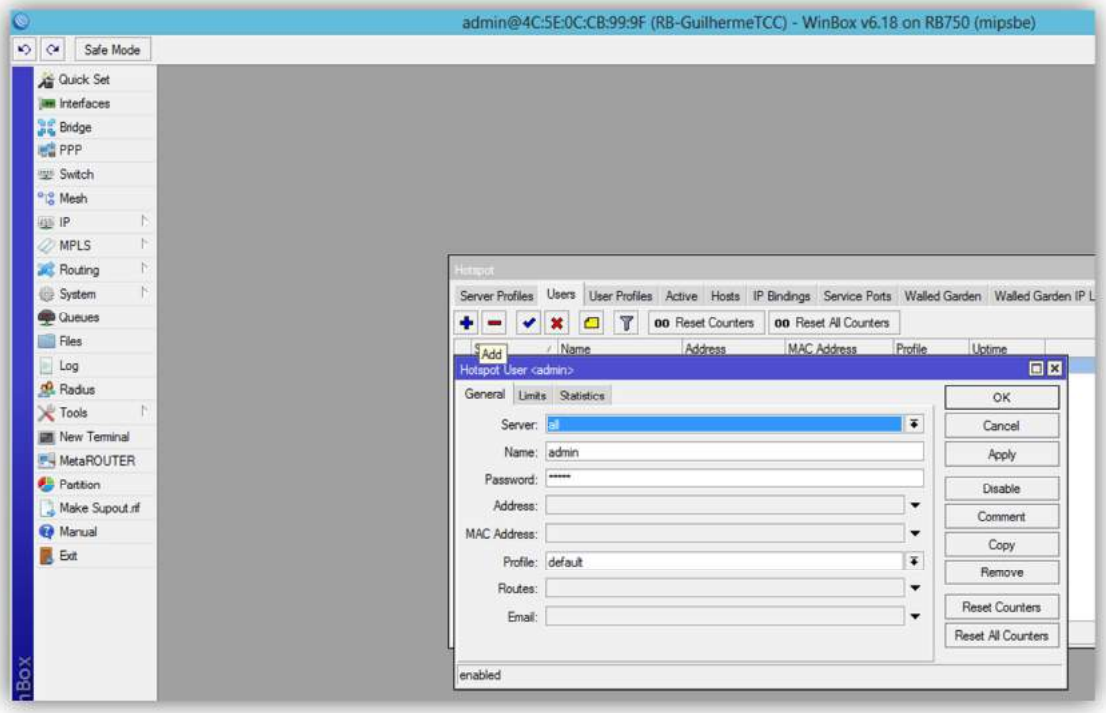

Imagem 56: Tela de inclusão de usuário/senha

2.11.4.2. USUÁRIO AUTENTICANDO COM MAC

No campo **Name** colocaremos o nome que nosso usuário efetuará a autenticação, no nosso caso utilizamos o usuário usermac. No campo **MAC** colocaremos o endereço MAC do microcomputador ou dispositivo do nosso cliente e no campo **Profile** selecionaremos o perfil Limitado.

Os demais campos devem ficar no padrão do RouterOS, como mostra a imagem abaixo.

Esse modo de autenticação não necessitará que o cliente possua uma senha para seu usuário, pois fará uma verificação do vínculo entre o nome de usuário e o endereço MAC do micromputador ou dispositivo em que se está sendo feito a autenticação, se for o endereço MAC correto o Hotspot irá autenticá-lo, neste tipo de autenticação usuário/MAC o cliente somente poderá utilizar suas credencias no micromputador ou dispositvo que tiver o MAC cadastrado em seu usuário.

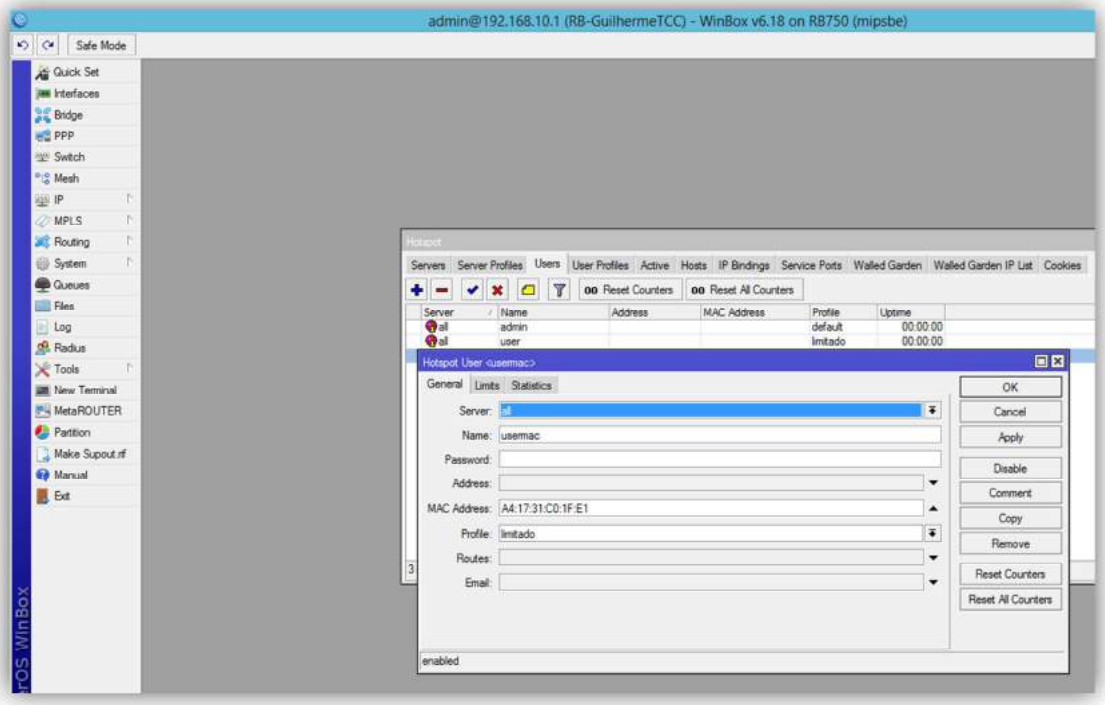

Imagem 57: Tela de inclusão de usuário/MAC

Na imagem abaixo podemos visualizar como ficará a tela inicial da lista de usuários cadastrados em nosso Hotspot após a inclusão dos usuários.

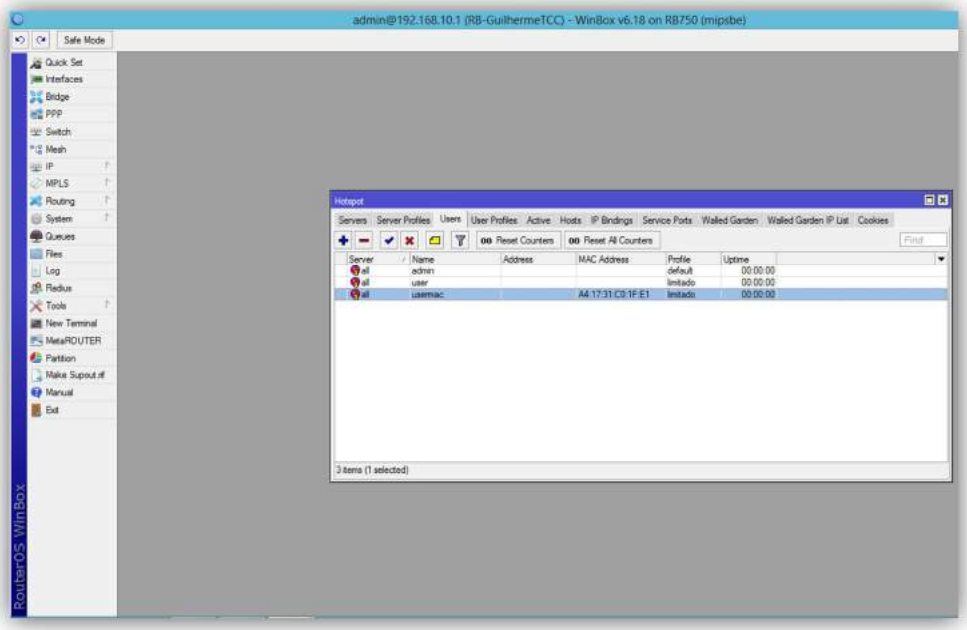

Imagem 58: Tela após a inclusão dos usuários

2.11.5. CONFIGURAÇÕES DO HOTSPOT NO FIREWALL E NAT

Ao ser criado o Hotspot cria automaticamente regras no Firewall, essas regras acabam bloqueando o acesso do Winbox à Routerboard, então após a criação do Hotspot devemos nos conectar ao RouterOS pelo endereço MAC da Routerboard como na Imagem abaixo, assim como fizemos no inicio deste manual na Imagem03.

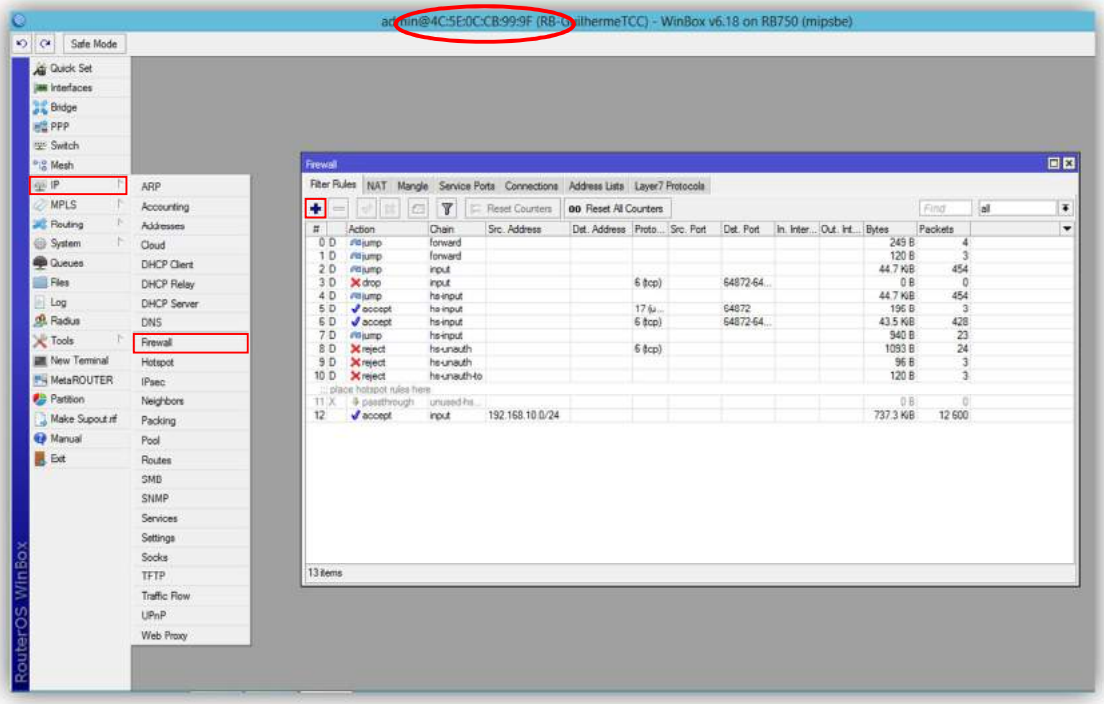

Imagem 59: Liberando acesso do Winbox no Firewall

Agora iniciaremos a inclusão da regra de liberação no **Firewall** em nosso RouterOS. Entraremos no Menu: **IP=>Firewall** e selecionaremos a opção ADD, simbolizada no Winbox pelo ícone ✚ , após isso será exibida uma tela de **Firewall Rule** como a Imagem60.

No campo **Chain** selecionaremos a opção forward, ou seja, é todo o tráfego que passa pela Routerboard, no campo **Protocol** selecionaremos a opção 6(tcp) e no campo **Dst.Port** colocaremos a porta 8291, que é a porta por onde o Winbox se comunica com o RouterOS, após isso devemos clicar na guia Action e no campo **Action** selecionar a opção accept e em seguida OK.

Os demais campo deverão permanecer no padrão do RouterOS, como na imagem abaixo.

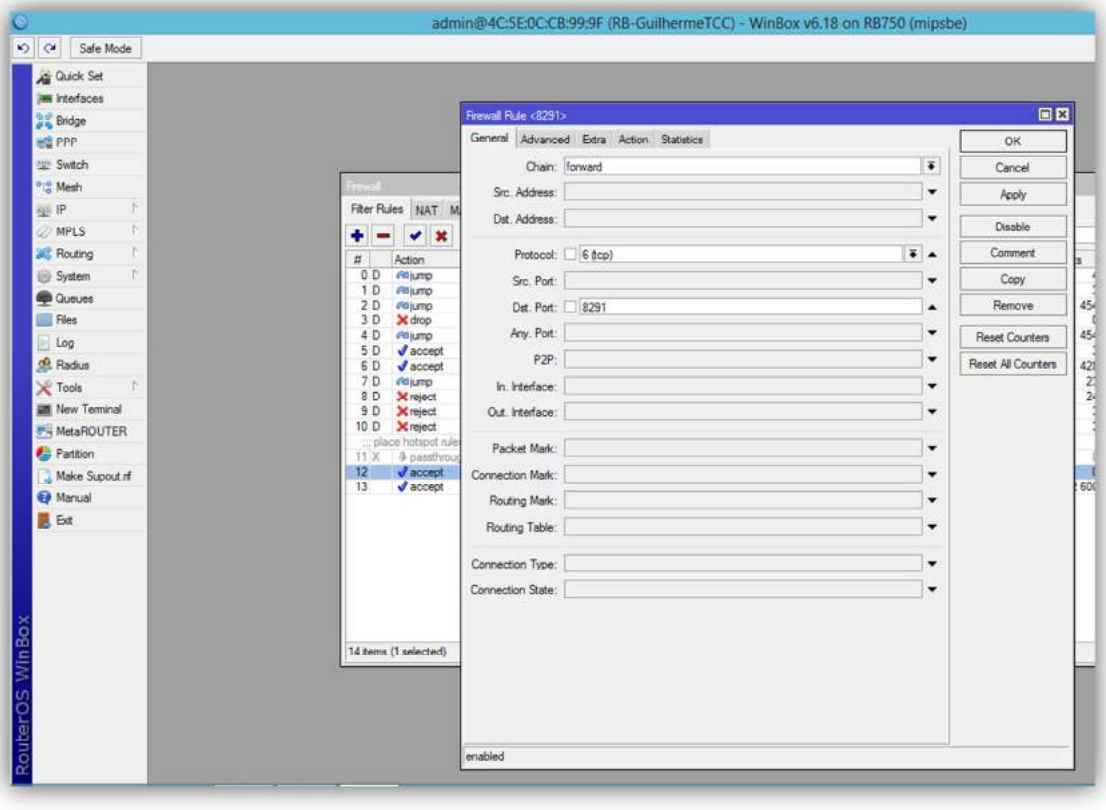

Imagem 60: Criando regra de acesso do Winbox

Na imagem abaixo podemos visualizar como ficará a tela inicial do Firewall após a inclusão da regra de liberação do acesso do Winbox ao RouterOS.

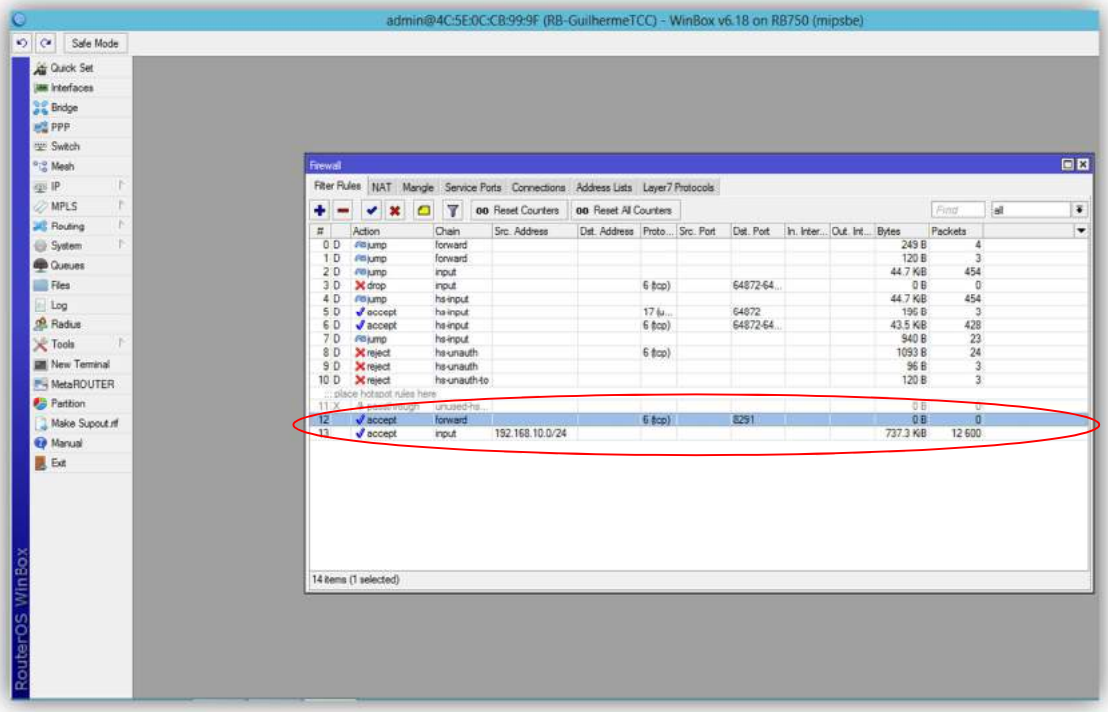

Imagem 61: Firewall após a inclusão da regra de acesso do Winbox

Após a criação dessa regra podemos novamente nos conectar ao RouterOS pelo endereço de ip como efetuado anteriormente e pode ser visualizado na Imagem23 deste manual, pois essa regra irá liberar o acesso do Winbox ao RouterOS.

O Hotspot também cria automaticamente regras no NAT ao ser configurado, nesse caso não é necessário fazer nenhuma configuração nas regras criadas dinamicamente por ele.

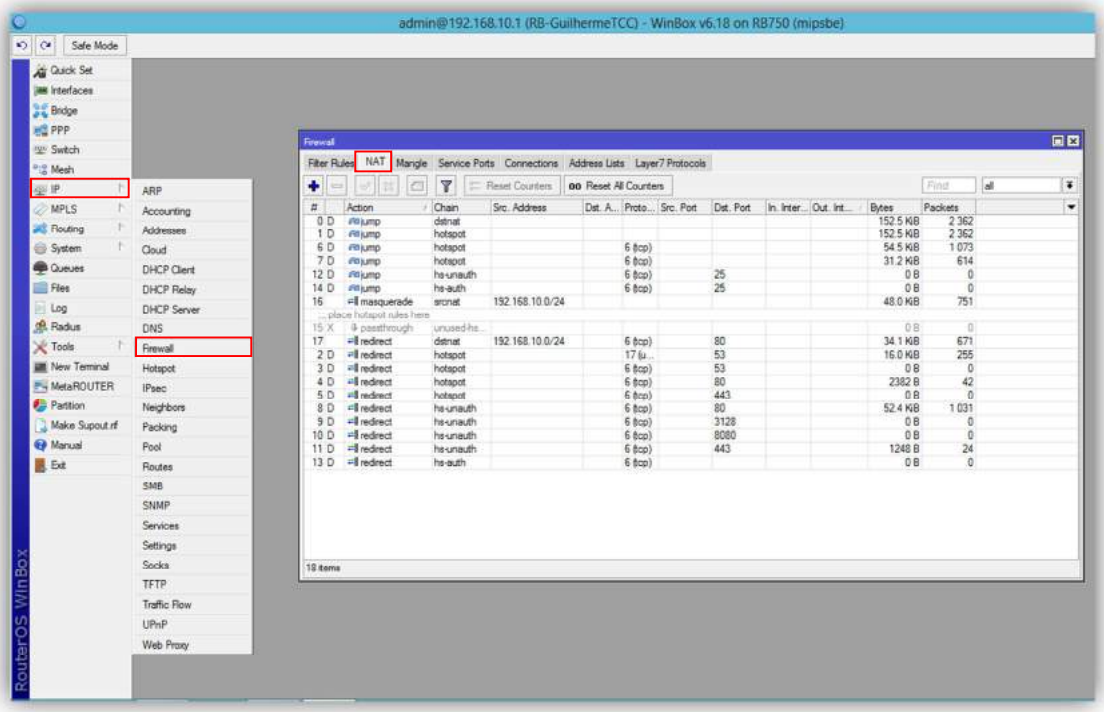

Imagem 62: NAT após a inclusão das regras pelo Hotspot

2.11.6. TELA DE AUTENTICAÇÃO DO HOTSPOT

A partir de agora se tentarmos navegar na internet seremos redirecionados à tela padrão de autenticação do Hotspot como na imagem abaixo. Essa tela solicitará as credenciais do cliente para que o Hotspot efetue ou não a autenticação dele no servidor.

Nesse momento o nosso servidor Hotspot já está em funcionamento.

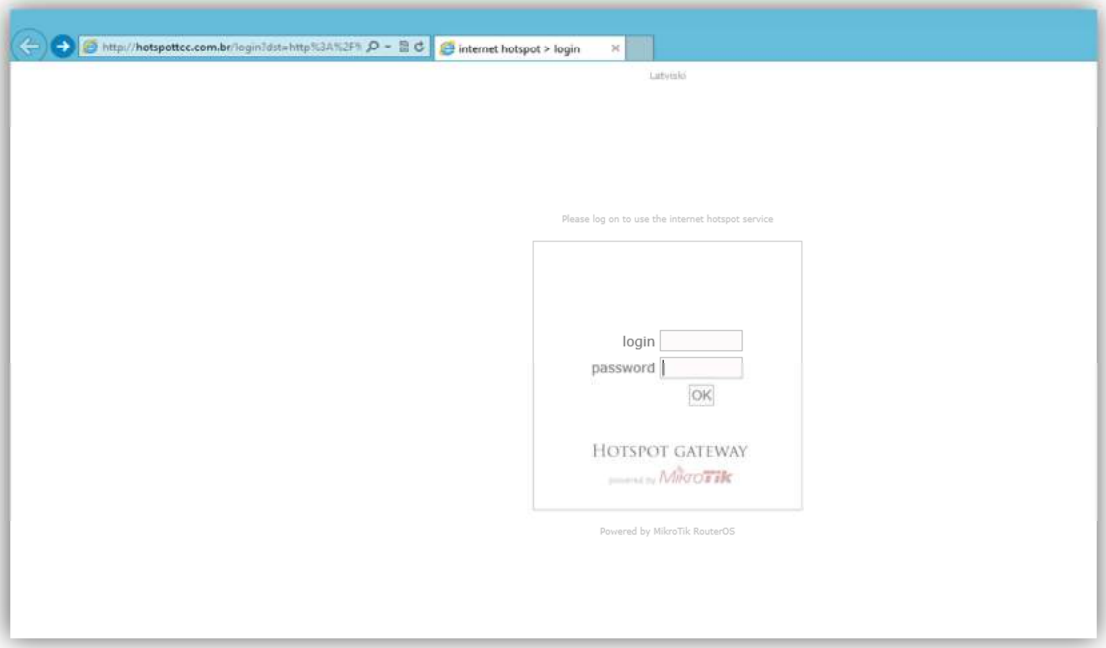

Imagem 63: Tela de solicitação de credenciais

Após preenchermos as credenciais na página de autenticação do Hotspot com o usuário e senha admin criados anteriormente, somos autenticados no Hotspot.

Como mostra a imagem abaixo entraremos no Menu: **IP=>Hotspot** e clicaremos na guia Active, essa tela nos mostra os usuários que estão autenticados no servidor Hotspot no momento, qual o ip dado a ele**(address)**, quanto tempo ele está conectado**(Uptime)**, quanto tempo a conexão está ociosa(**Idle Time)** e quais são as taxas de upload**(RX Rate)** e download**(Tx Rate)** utilizadas no momento por cada usuário.

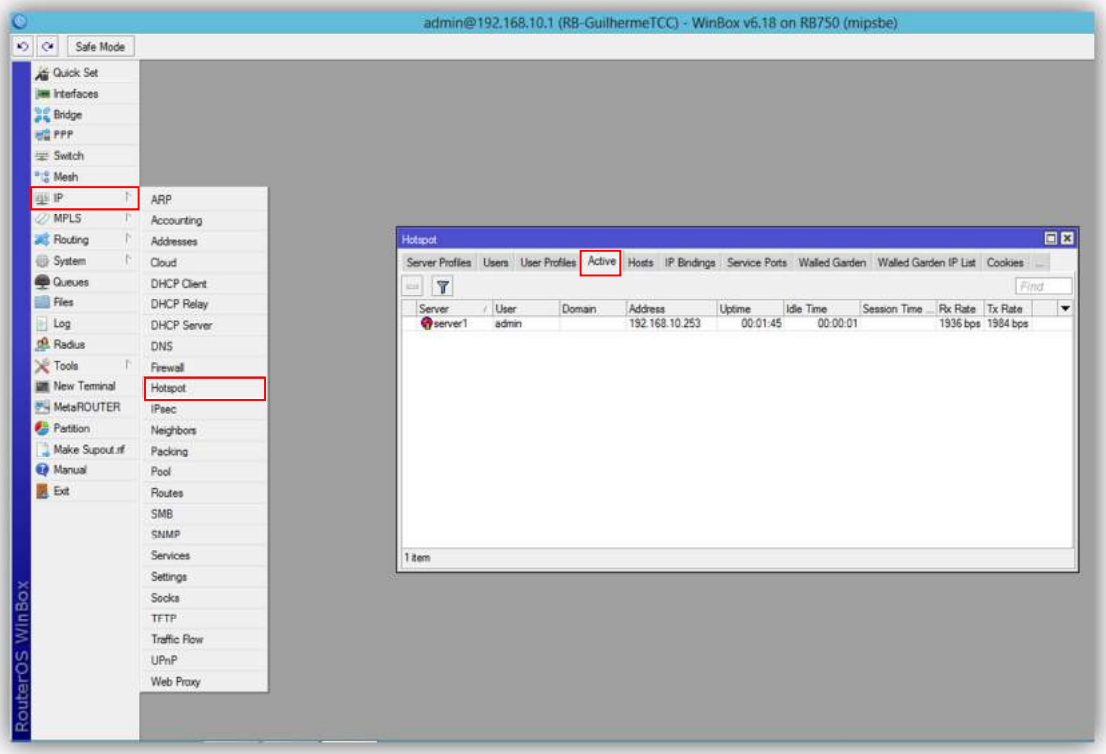

Imagem 64: Tela de usuários autenticados

2.11.7. IP BINDINGS, WALLED GARDEN E SIMPLE QUEUES

Depois de finalizada a configuração de nosso servidor Hotspot vamos detalhar o funcionamento de três recursos do Hotspot, o IP Binding, o Walled Garden e o Simple Queues.

2.11.7.1. ADICIONANDO UMA REGRA DE IP BINDINGS

Uma das funcionalidades do IP Bindings é a liberação de um usuário específico da autenticação via usuário/senha ou usuário/MAC do servidor Hotspot, sendo automaticamente autenticado ao se conectar na rede.

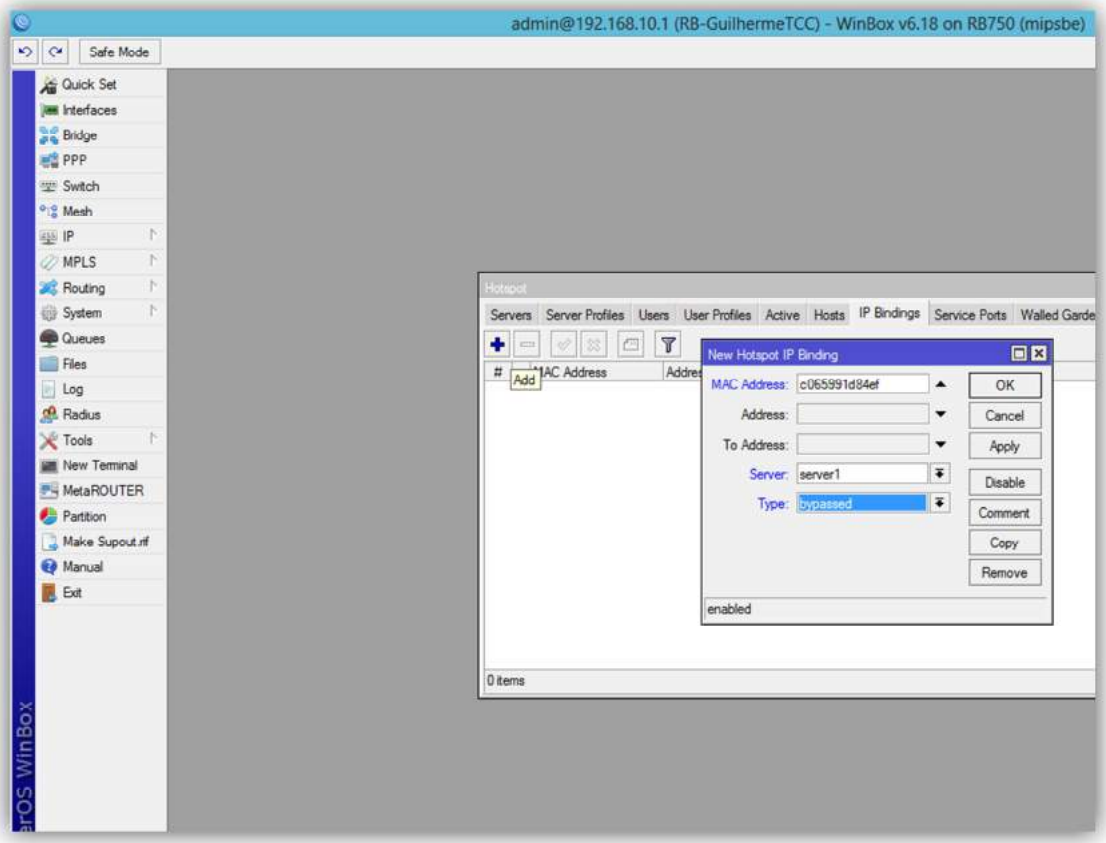

Imagem 65: Criação de regra IP Bindings

Agora iremos criar uma regra em que um usuário irá autenticar automaticamente sem precisar digitar as credencias na página de autenticação do Hotspot, clicaremos na guia IP Bindigs e na tela inicial clicaremos na opção ADD, simbolizada no Winbox pelo ícone ✚, após isso será exibida a tela **New Hotspot IP Binding**, que é a tela de inclusão das regras, como mostra a Imagem65.

No campo **MAC Address** colocaremos o endereço MAC do microcomputador ou dispositivo do cliente que queremos que autentique automaticamente e no campo **Type** selecionaremos a opção bypassed, que permitirá o endereço contornar a autenticação do Hotspot.

É possível também bloquear endereços para que não consigam autenticação somente alterando o campo **Type** para blocked em vez de bypassed, isso fará com que o endereço especificado não consiga autenticação no Hotspot.

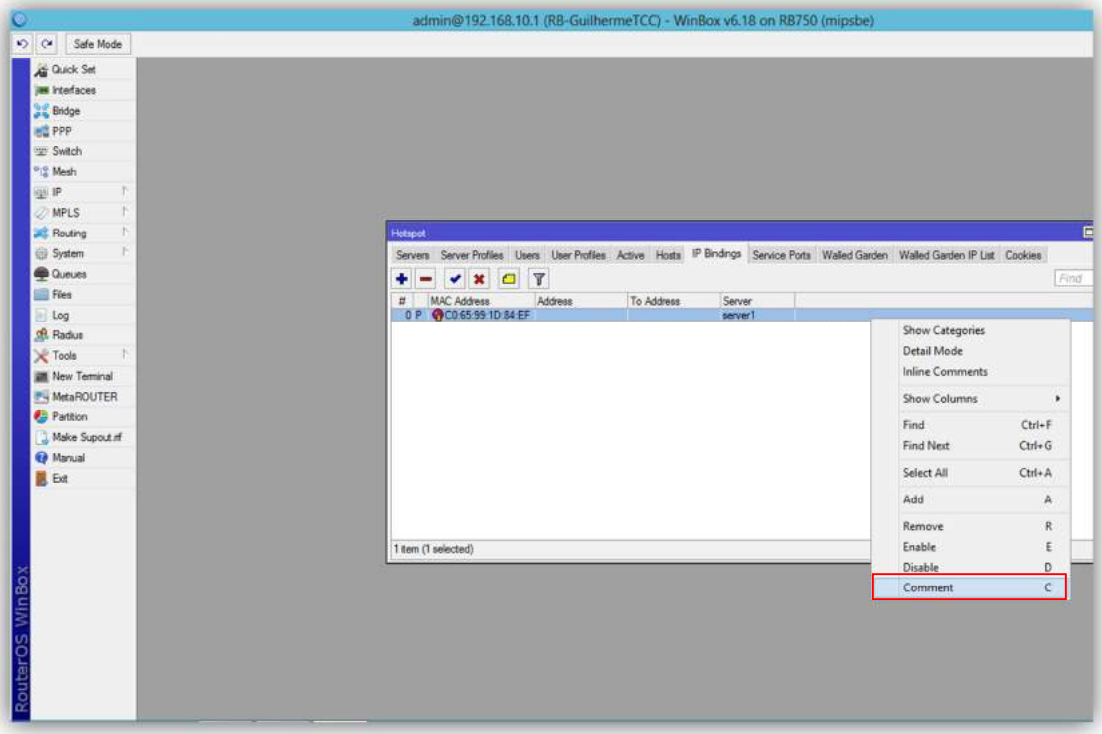

Imagem 66: Comentando uma regra no RouterOS

Uma dica importante para uma boa organização em nosso RouterOS é a identificação de nossas regras.

Clicaremos com o botão direito do mouse encima de uma regra escolheremos a opção **Comment** no menu, como na Imagem66.

Identificaremos a regra como Celular Guilherme, para que quando formos fazer alguma alteração nas regras nós saibamos o que significa essa regra e nesse caso específico do IP Bindings, a quem esse endereço MAC pertence.

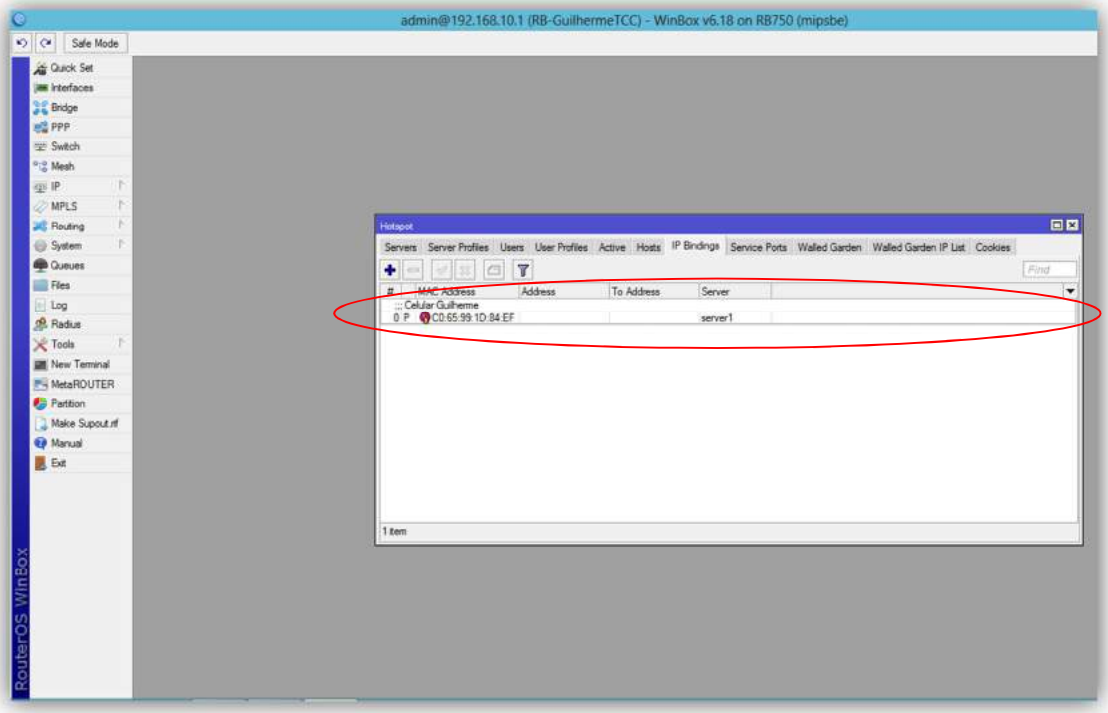

Imagem 67: Regra de IP Binding comentada

2.11.7.2. ADICIONANDO UMA REGRA DE WALLED GARDEN

Uma das funcionalidades do Walled Garden é a liberação da navegação de algum host específico mesmo sem a autenticação do usuário no Hotspot.

Agora iremos criar uma regra que liberará a navegação de um site mesmo que os clientes não estejam autenticados, clicaremos na guia Walled Garden e na tela inicial clicaremos na opção ADD, simbolizada no Winbox pelo ícone ✚ , após isso será exibida a tela **New Walled Garden Entry**, que é a tela de inclusão das regras, como mostra a Imagem68.

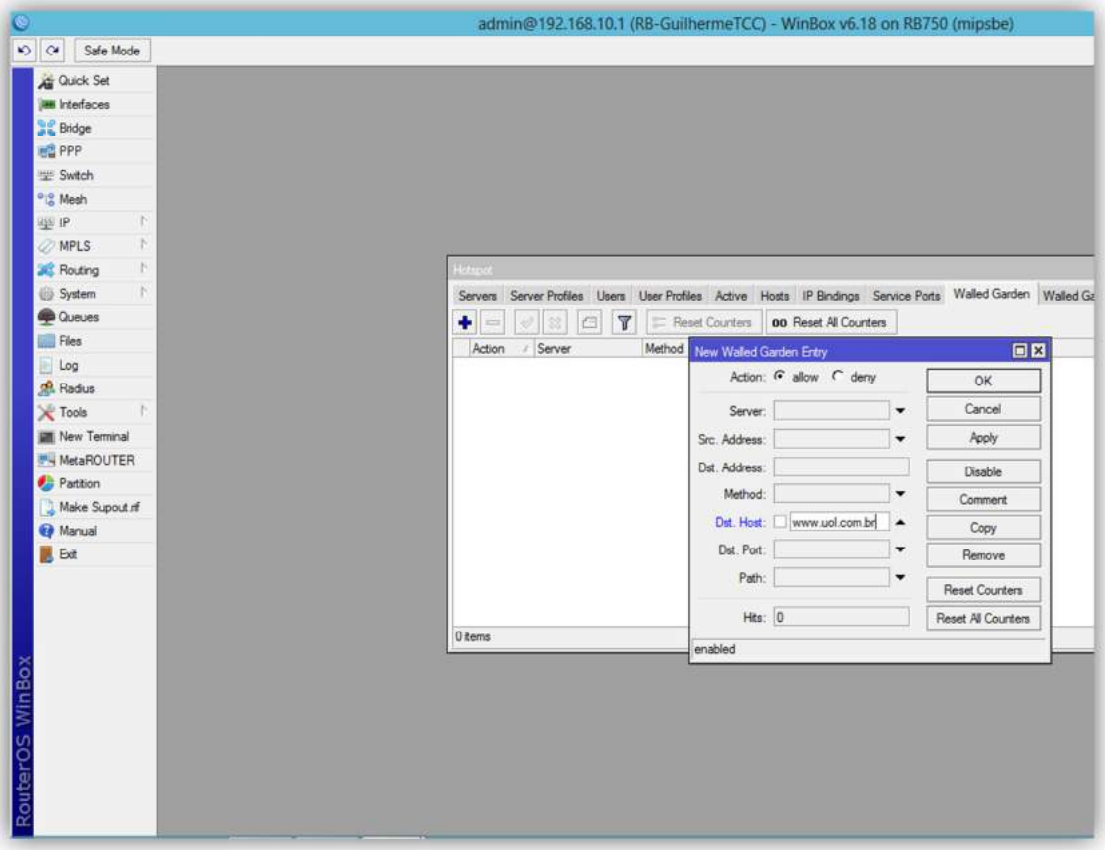

Imagem 68: Criação de regra Walled Garden

No campo **Action** selecionaremos a opção Allow, que irá liberar o acesso, no campo **Dst.Host** colocaremos o site que se deseja liberar a navegação mesmo o cliente não estando autenticado, nesse caso o site www.uol.com.br.

Os demais campos devem ficar no padrão do RouterOS, como na Imagem68.

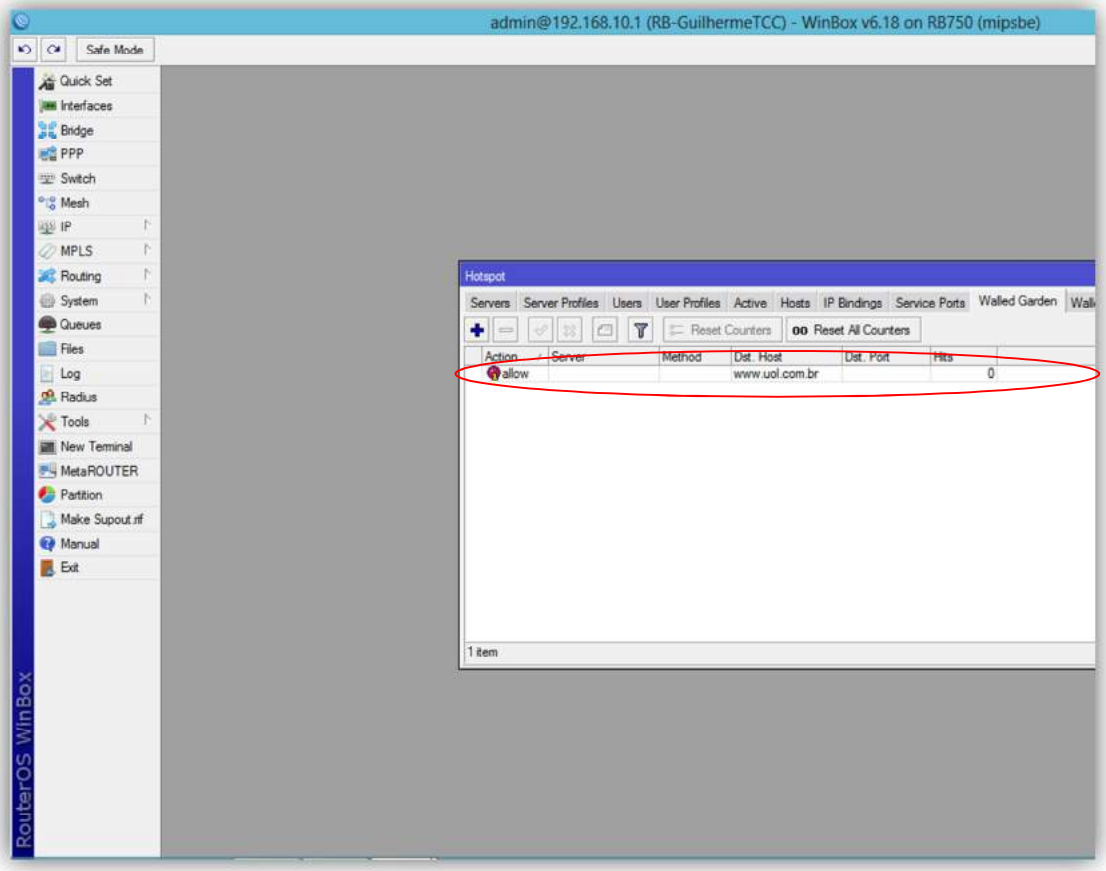

Imagem 69: Após a criação de regra Walled Garden

Essa regra fará que todo o tráfego de pacotes que o domínio de destino**(Dst.Host)** seja uol.com.br seja permitido(**Allow**) mesmo que o cliente não esteja autenticado no servidor.

2.11.7.3. SIMPLE QUEUES

No caso específico do Hotspot, o Simple Queues cria automaticamente uma regra de queue quando o usuário se autentica no servidor, baseado na regra de User Profile criada anteriormente, como mostra a imagem abaixo o Hotspot criou uma regra de queue para o usuário admin dando 5M de upload e 5M de download para sua navegação.

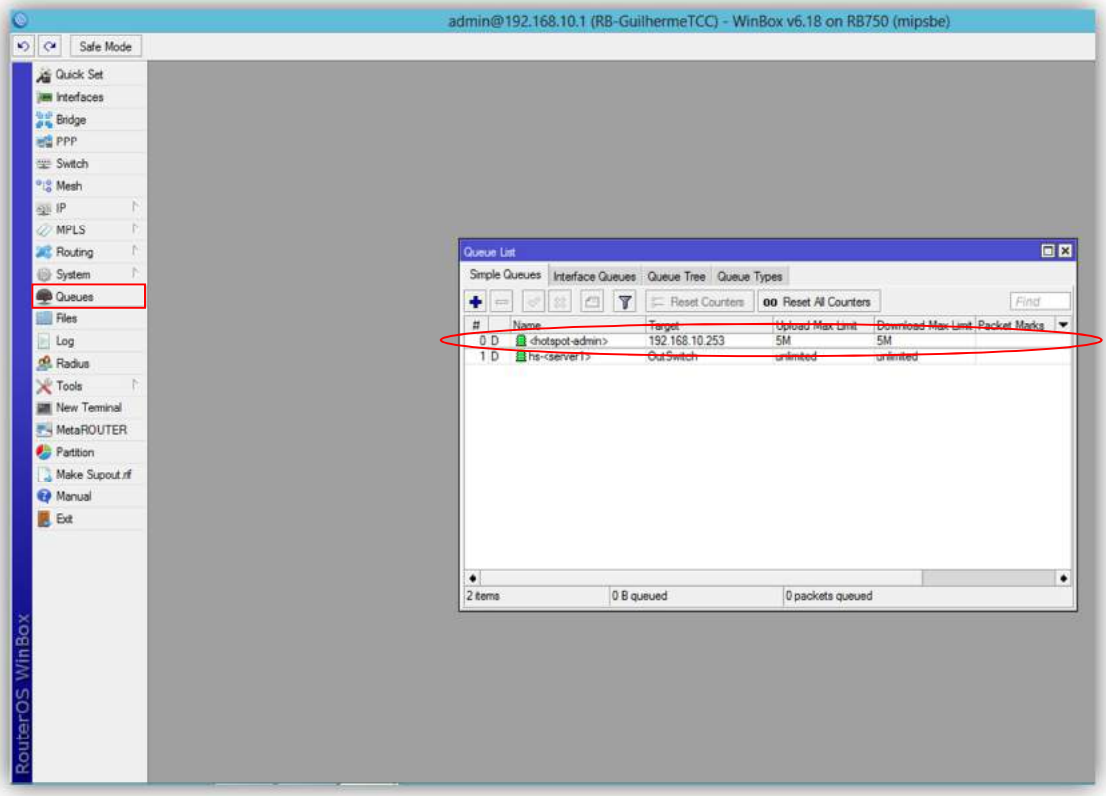

Imagem 70: Regras de Simple Queues

2.11.8. PERSONALIZANDO A TELA DE AUTENTICAÇÃO DO HOTSPOT

A tela de autenticação pode ser personalizada de acordo com a vontade do administrador do RouterOS ou da empresa responsável pelo servidor Hotspot.

Como pode ser visualizado na Imagem abaixo, quando clicamos em Files o Winbox nos mostra uma árvore de diretórios dos arquivos existentes em nossa Routerboard. Nessa árvore de diretórios podemos ver uma pasta com o nome de Hotspot, nessa pasta estão os arquivos da página de autenticação, que podem ser personalizados.

Entre os vários arquivos, cada um com a sua finalidade destacamos o arquivo login.html que é o arquivo da página inicial de autenticação e por onde começa a personalização da área de autenticação.

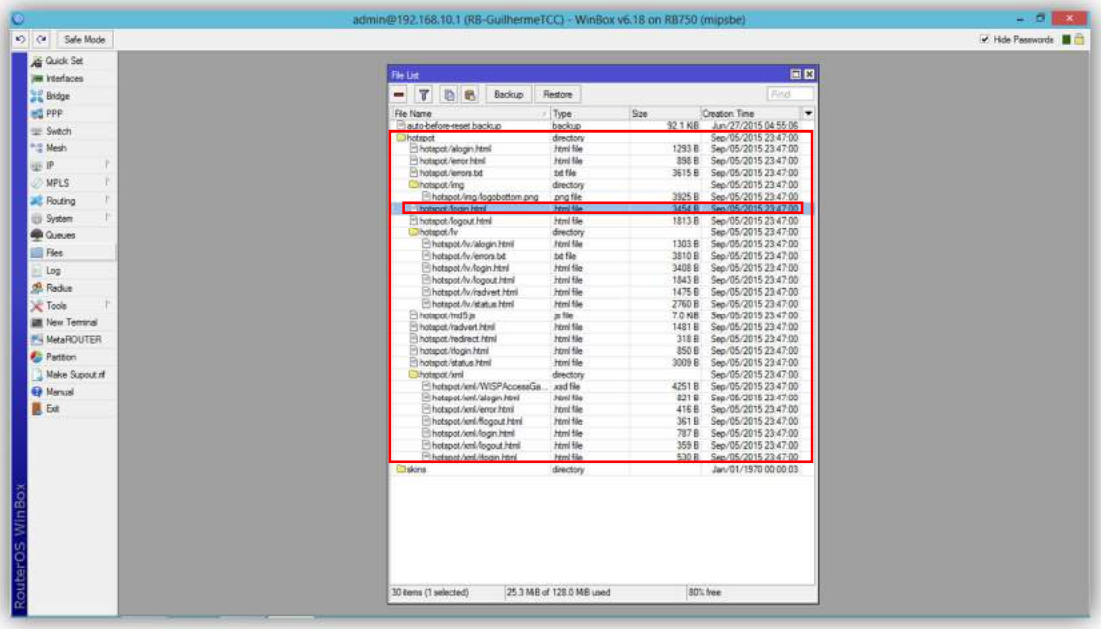

Imagem 71: Diretório de arquivos do RouterOS

Na imagem abaixo podemos visualizar uma página de autenticação do Hotspot já personalizada.

Imagem 72: Exemplo de tela de autenticação personalizada

2.12. ALTERANDO A SENHA DO ROUTEROS

Para finalizar esse manual não podemos nos esquecer de fazer a alteração da senha de acesso padrão do administrador do RouterOS.

Para iniciar a troca da senha do administrador do RouterOS entraremos no Menu: **System=>Users**, e em seguida daremos um duplo clique encima do usuário padrão existente em nosso RouterOS, o usuário admin.

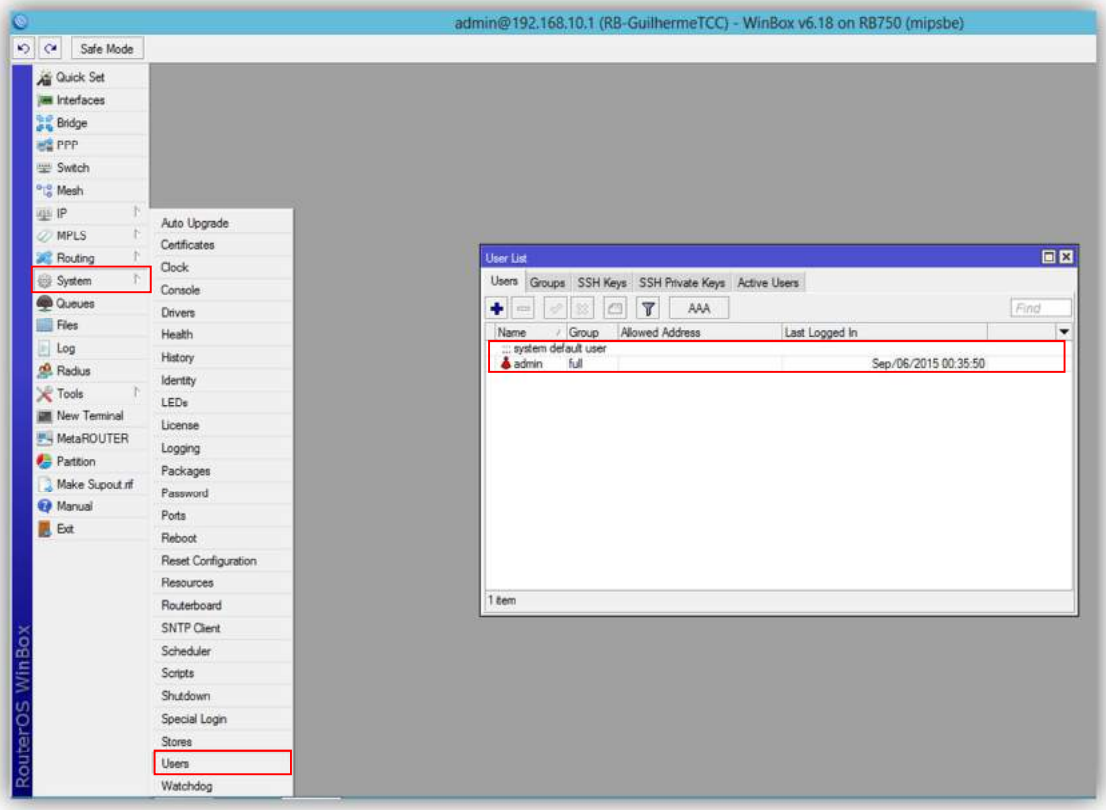

Imagem 73: User list do RouterOS

Será mostrada a tela de configuração do usuário admin, clicaremos então no botão Password .

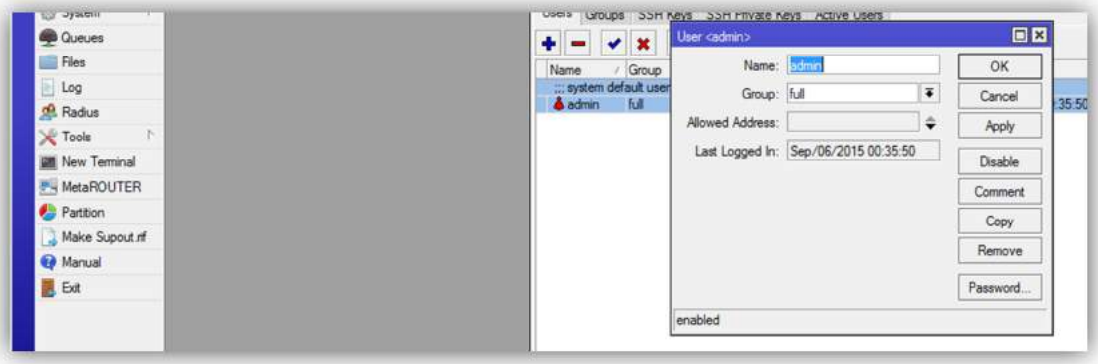

Imagem 74: Configuração do usuário admin

No campo **New Password** colocaremos a nova senha e confirmaremos a mesma senha no campo **Confirm Password**. Finalizaremos clicando em OK e seguida em OK novamente. A senha do administrador já está alterada.

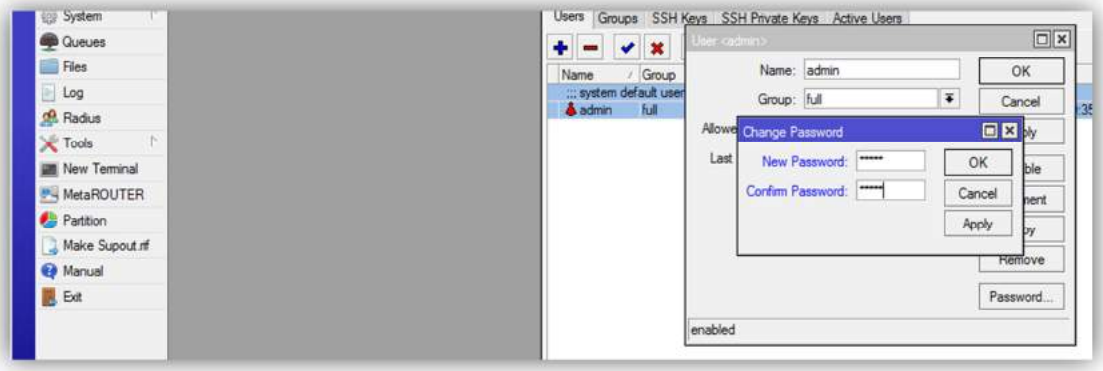

Imagem 75: Troca da senha do usuário admin

3. CONFIGURAÇÃO DOS ACCESS POINTS UBIQUITI UNIFI

3.1. INTRODUÇÃO

Nesse cenário estaremos configurando os access points da Ubiquiti Unifi conforme a imagem abaixo, para que eles recebam endereços de IP da Routerboard e configurando os parâmetros de rede para que os access points autentiquem os usuários da rede no servidor Freeradius antes de liberar o acesso à rede.

Imagem 76: Ubiquiti Unifi AP

3.2. CONFIGURANDO O DHPC SERVER NA ROUTERBOARD

Primeiramente temos que configurar o DHCP Server da Routerboard para que ele forneça um ip fixo ao access point quando solicitado pelo mesmo. Entraremos no Menu: **IP=>DHCP Server,** na guia **Leases** e selecionaremos a opção ADD, simbolizada no Winbox pelo ícone ✚ .

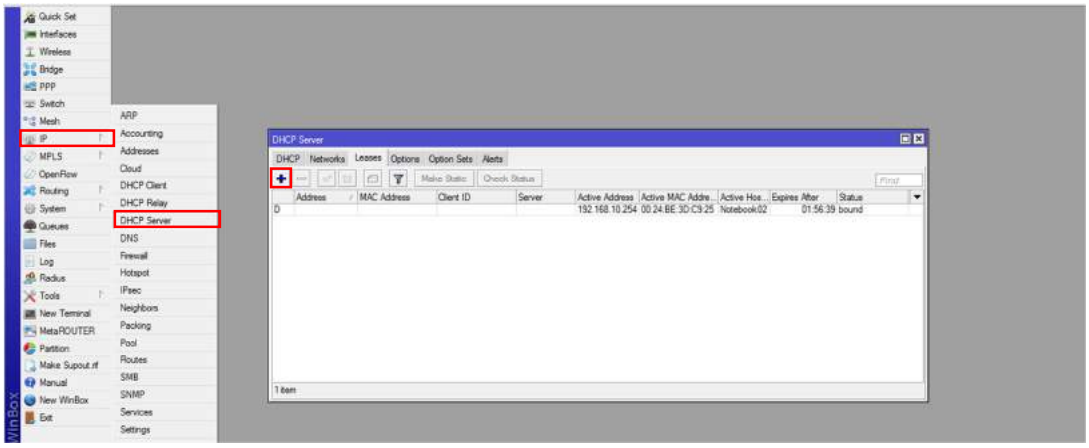

Imagem 77: Tela de Leases do DHCP Server

Iremos procurar na parte traseira do AP o endereço MAC do dispositivo para vinculá-lo à um endereço de IP fixo no DHCP Server da Routerboard.

Imagem 78: Parte traseira do Unifi AP

Agora iremos preencher o campo **Address** com o endereço de IP escolhido, nesse caso 192.168.10.2, lembrando que para efeito de controle e reduzir a chance de conflito de endereço de IP é melhor utilizar um endereço de IP que esteja fora do **POLL** criado na Routerboard, coforme explicado no capítulo 2.5. desse manual. No campo **MAC Address** iremos colocar o endereço MAC do access point, conforme a imagem abaixo.

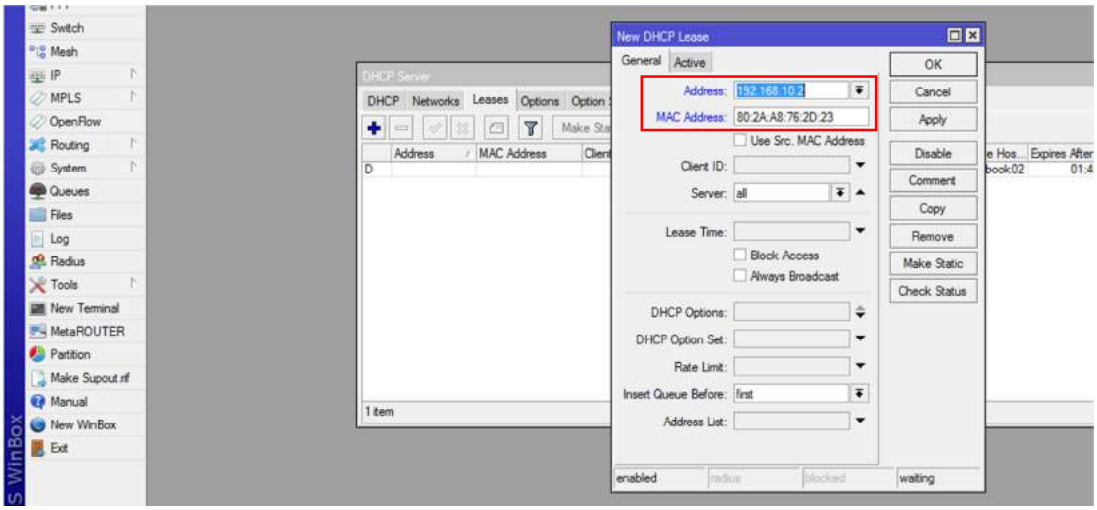

Imagem 79: Adicionando um DHCP Server Lease para o AP

Para uma boa documentação e organização da Routerboard iremos comentar o novo **DHCP Server Lease** com a identificação *UAP 01*, conforme as imagens abaixo.

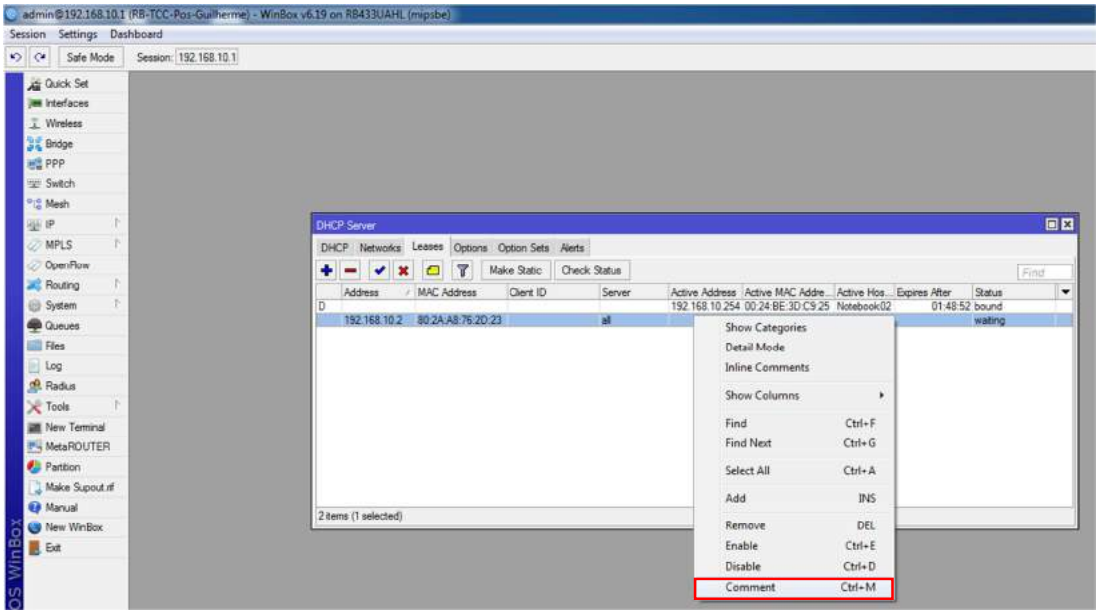

Imagem 80: Comentando o DHCP Server Lease

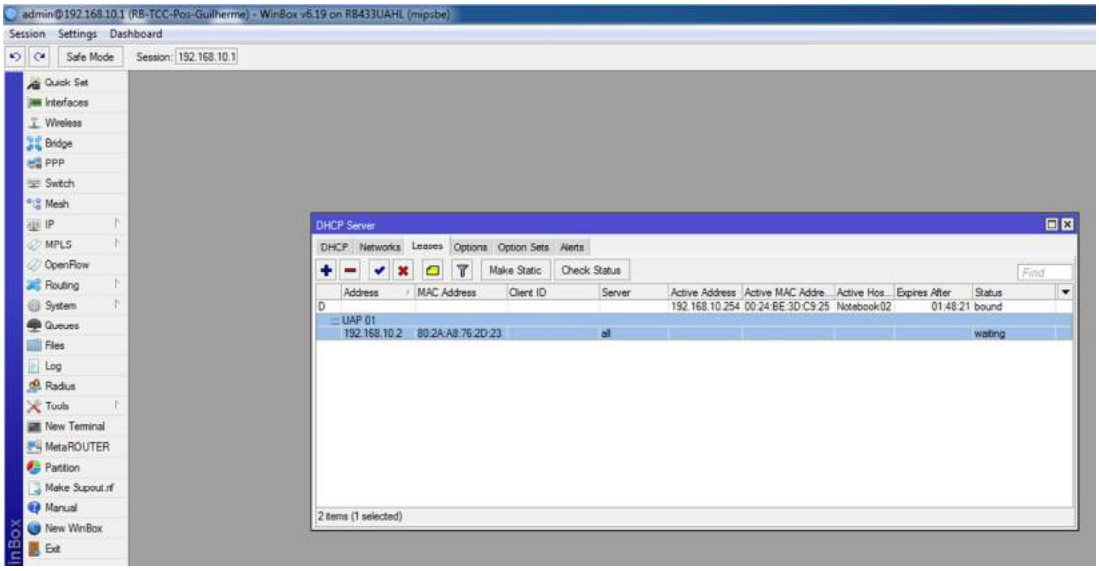

Imagem 81: Após a identificação do DHCP Server Lease com o comentário

Agora a Routerboard já está configurada para oferecer um endereço de IP ao access point quando este for ligado e conectado no switch da rede.

3.3. LIGANDO OS ACCESS POINTS

Conforme mostra a imagem abaixo, devemos conectar o adaptador POE na tomada, na porta LAN conectar o cabo que vem do switch, e na porta POE o cabo que está conectado no access point.

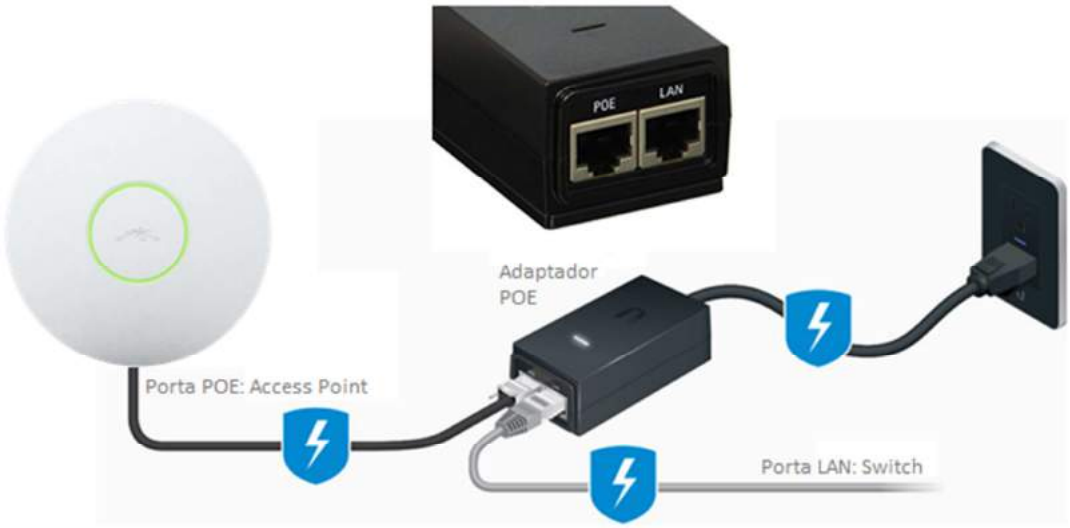

Imagem 82: Como ligar o Access Point

Após todos os cabos ligados o AP irá começar seu processo de inicialização, isso demorará cerca de 1 minuto, após esse tempo, para confirmar se o access point recebeu o endereço IP do **DHCP Server** iremos consultar nossa Routerboard, que deverá estar como a imagem abaixo.

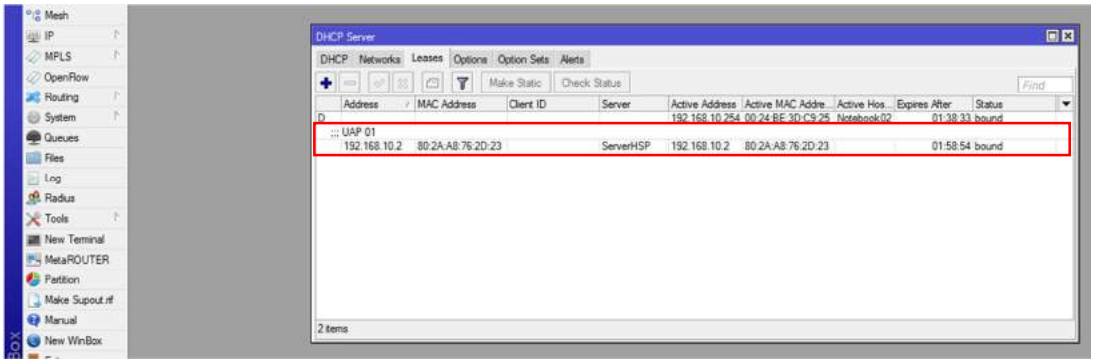

Imagem 83: Lease confirmando a entrega do endereço de IP

3.4. INSTALANDO A CONTROLADORA DOS ACCESS POINTS

Agora iremos instalar a Unifi Controller, que é o software de configuração dos access points, essa controladora pode ser utilizada também como sistema de controle de autenticações de usuários, limitador de banda, etc, mas em nosso caso só utilizaremos ela para configurar os AP's, pois a Routerboard será responsável pelo controle da nossa rede e do nosso sistema. Estaremos utilizando a versão 5.0.7 da Unifi Controller, que pode ser baixada diretamente no site na Ubiquiti, no endereço https://www.ubnt.com/download/unifi/unifi-ap.

Imagem 84: Tela inicial e final de instalação da Unifi Controller

Conforme vemos na imagem acima, executaremos o arquivo baixado do site, que nos apresentará esta tela inicial e final de instalação, deixaremos a opção "*Start UniFi Controller after installation*" marcada, para que o programa inicie automaticamente após a finalização da instalação da controladora.

Imagem 85: Tela de inicialização da Unifi Controller

Assim que a aplicação Unifi Controller abrir devemos esperar que ela encontre-se em seu estado "*Started*", que significa que ela esta pronta para utilização, conforme a Imagem85.

Assim que ela estiver iniciada iremos clicar na opção "*Launch a browser to manage the network".* Conforme mostra a imagem abaixo, é comum o navegador mostrar esse aviso de segurança devido ao erro de certificado, basta clicar na opção "*AVANÇADO*".

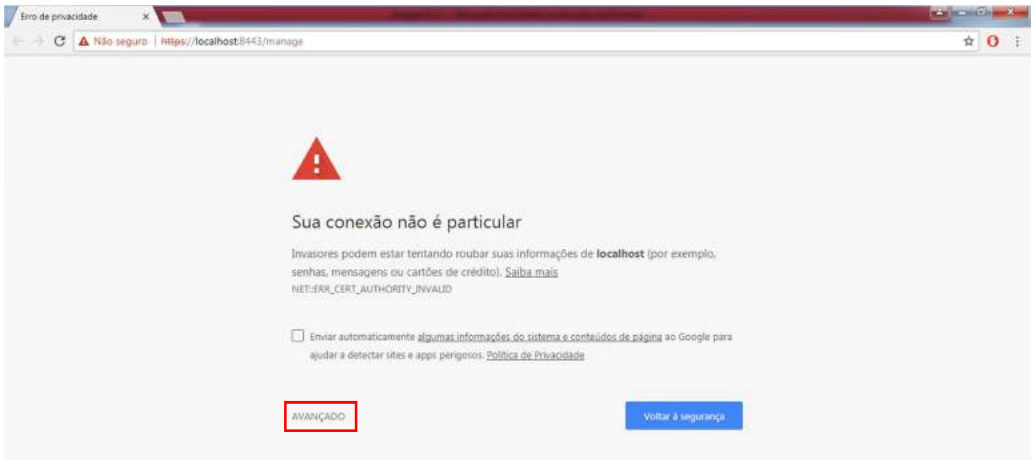

Imagem 86: Tela de aviso de segurança do navegador 01

Depois basta clicar na opção "*Ir para localhost (não seguro)*", lembrando que é um aviso padrão do navegador.

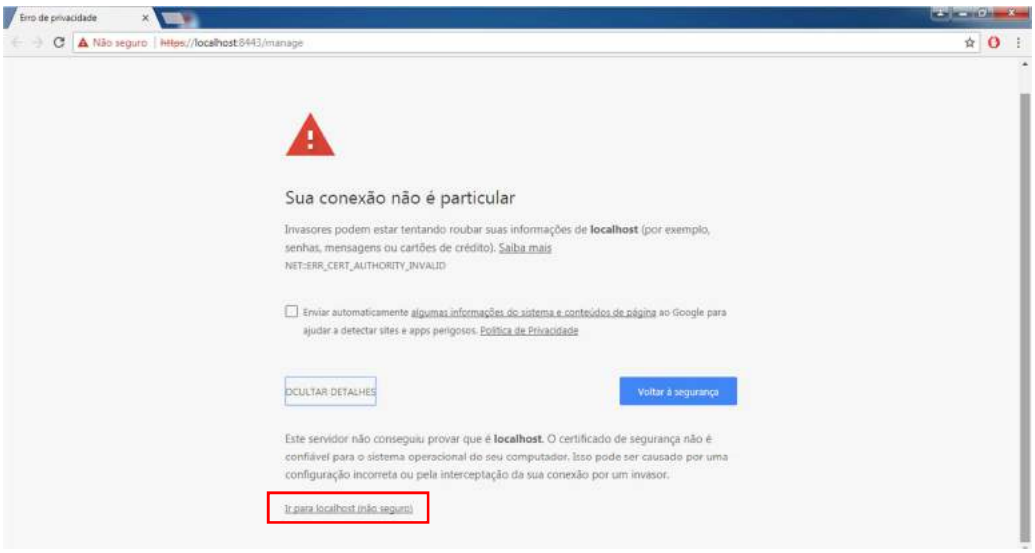

Imagem 87: Tela de aviso de segurança do navegador 02

Escolheremos o país "*Brazil*" e o fuso horário correspondente à região de onde estivermos, conforme a imagem abaixo.

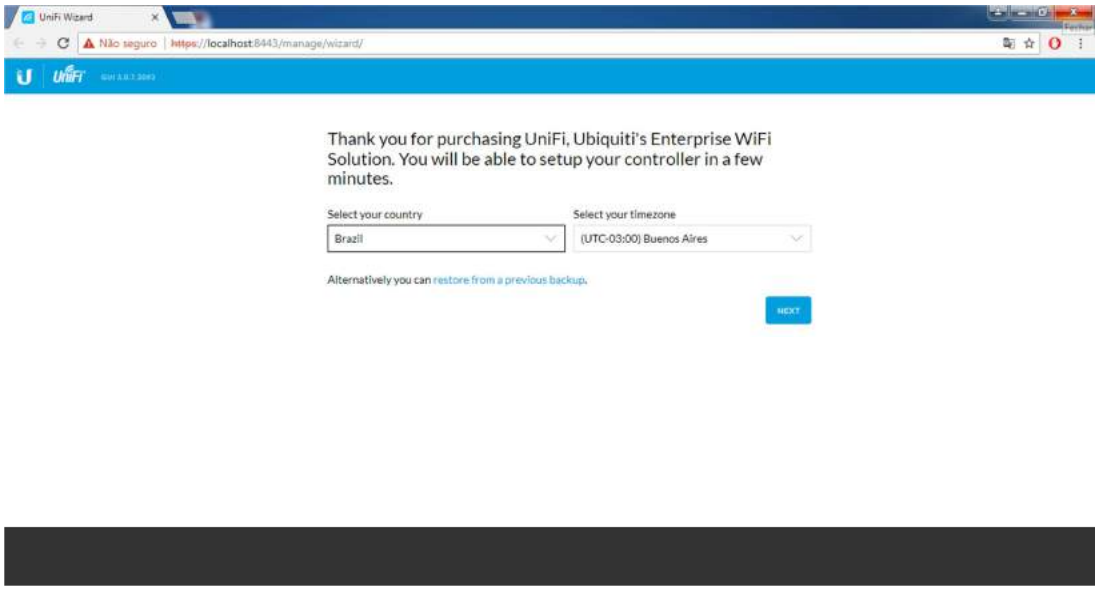

Imagem 88: Tela de pré-configuração da Unifi Controller 01

Nesta etapa a Unifi Controller fará uma busca na rede a procura de dispositivos para configurar, em nosso caso deverá aparecer o access point previamente preparado para configuração e adoção na rede, conforme a imagem abaixo.

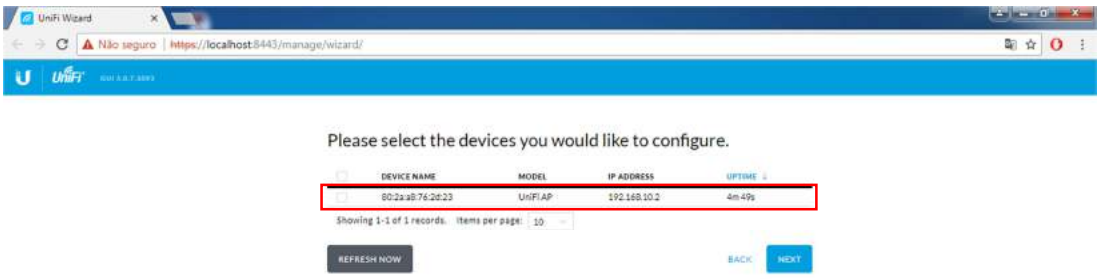

Imagem 89: Tela de pré-configuração da Unifi Controller 02

Agora clicaremos na opção “*Skip*” para pular esse passo, pois criaremos a rede com as configurações específicas de segurança WPA-Enterprise e faremos a configuração do AP após a finalização da pré-configuração inicial da Unifi Controller.

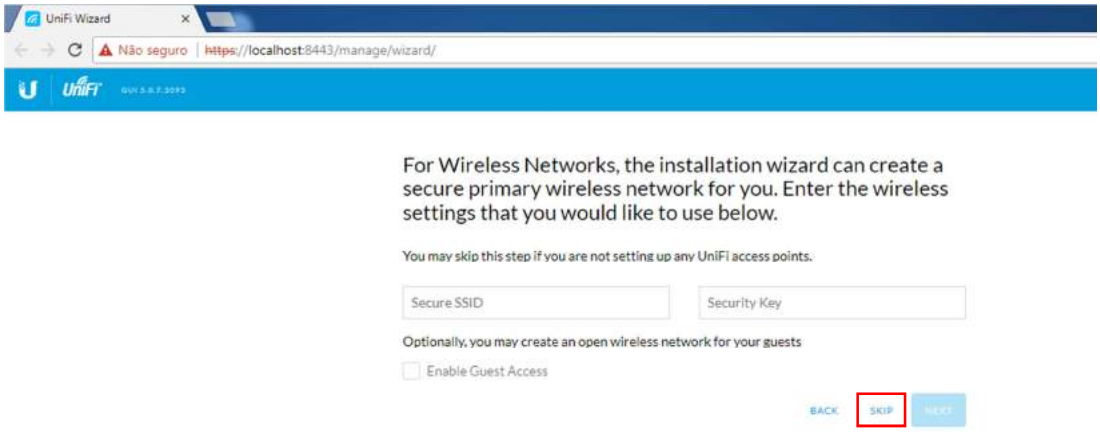

Imagem 90: Tela de pré-configuração da Unifi Controller 03

Nesta etapa criaremos o usuário administrador “**admin**”, especificaremos um e-mail para essa conta e uma senha para esse usuário conforme a imagem abaixo.

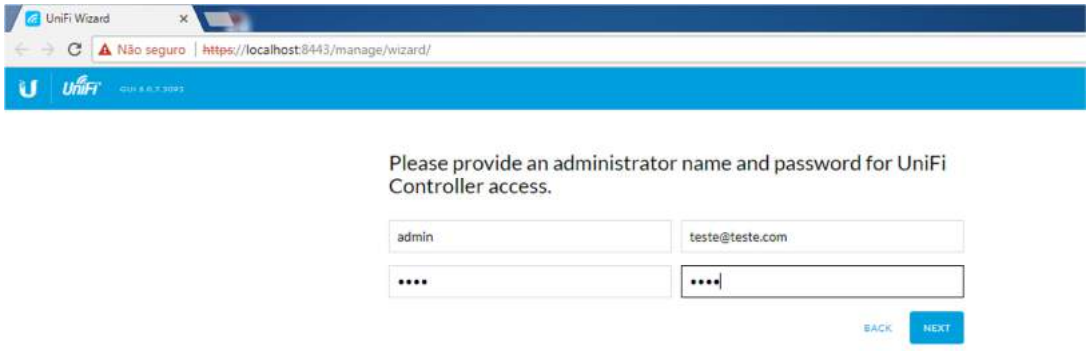

Imagem 91: Tela de pré-configuração da Unifi Controller 04

Desse modo chegaremos na fase final de pré-configuração da Unifi Controller, conforme a imagem abaixo.

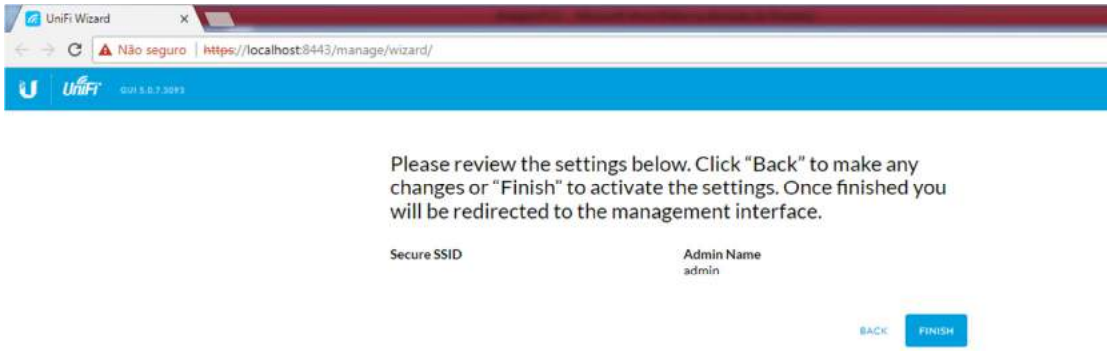

Imagem 92: Tela final de pré-configuração da Unifi Controller

Ao clicar no botão "*Finish*" para finalizar a pré-configuração seremos direcionados para a tela de login da Unifi Controller, onde utilizaremos as credenciais de login e senha previamente criadas.

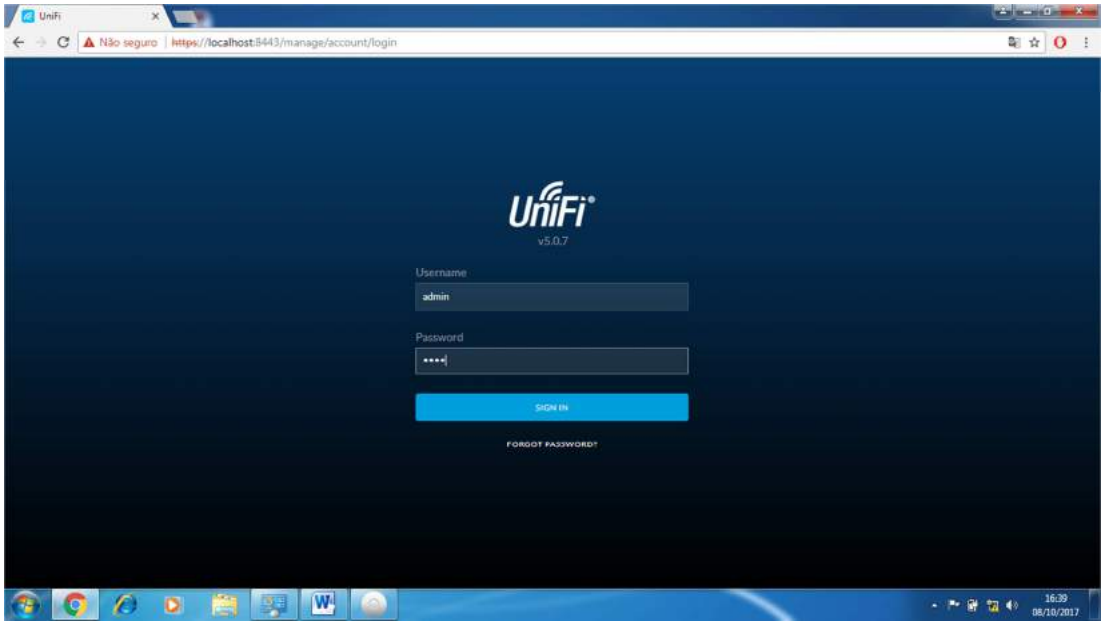

Imagem 93: Tela de login da Unifi Controller

3.5. CRIANDO A REDE WI-FI

Agora criaremos a rede wi-fi com as configurações específicas de segurança WPA-Enterprise, primeiramente clicaremos no ícone , depois na opção **Wireless Networks** e por último no botão **+ CREATE NEW WIRELESS NETWORK**.

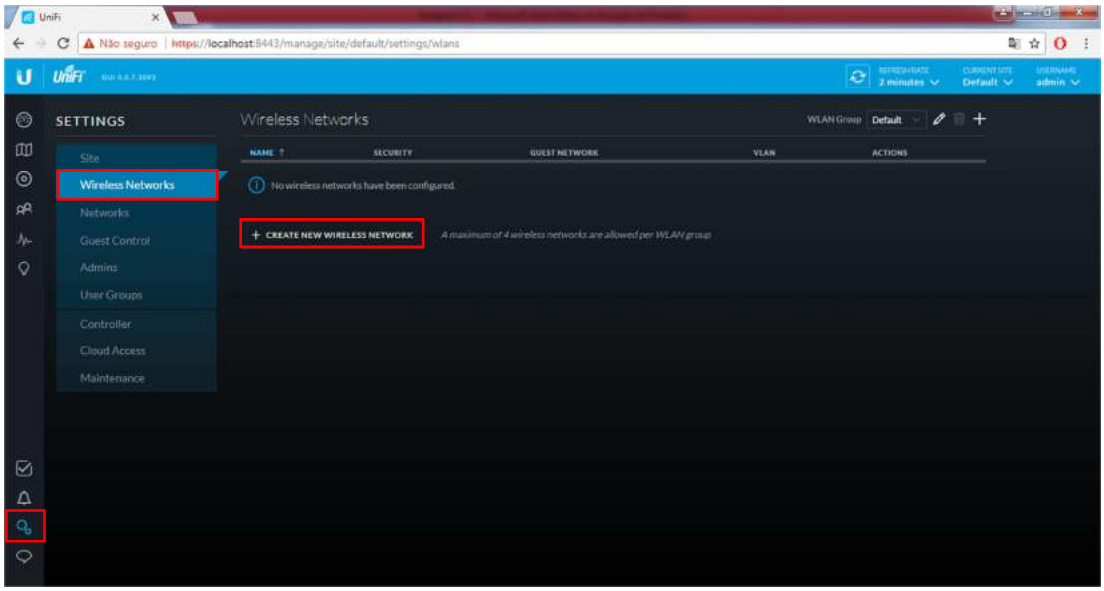

Imagem 94: Tela de configuração das redes wi-fi

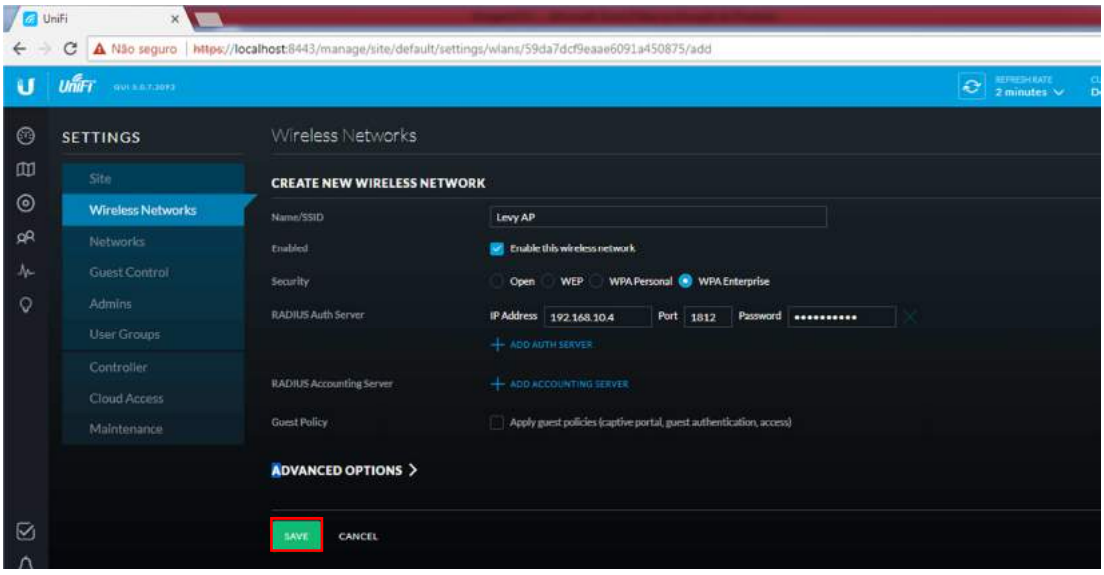

Imagem 95: Tela de criação de uma nova rede wi-fi

Conforme a Imagem95 escolhemos "**Levy AP**" como o SSID da rede, este será o nome visível de nossa rede wi-fi que pode ser personalizada de acordo com vontade do administrador da rede, deixamos marcado a opção "**Enable this wireless network**" que ativa a rede, no tipo de segurança iremos escolher **WPA-Enterprise**, que nos permitirá a autenticação em um servidor Freeradius.

Na opção "**IP Address**" do "*RADIUS Auth Server"* iremos colocar o endereço IP do nosso servidor Freeradius que será configurado futuramente no capítulo 4, em nosso caso escolhemos o endereço IP 192.168.10.4, pois esse endereço também está fora do **POOL** de endereços criados em nossa Routerboard, no campo "**Port**" iremos colocar a porta de conexão ao servidor, nesse caso a porta 1812, no campo "**Password**" escolheremos uma senha para a conexão ao servidor, em nosso caso colocamos a senha "*levyap2017*".

Nos outros campos não faremos modificações, somente clicaremos no botão "*SAVE*" para salvar as alterações e será mostrada uma tela como a imagem abaixo com a nossa rede já criada.

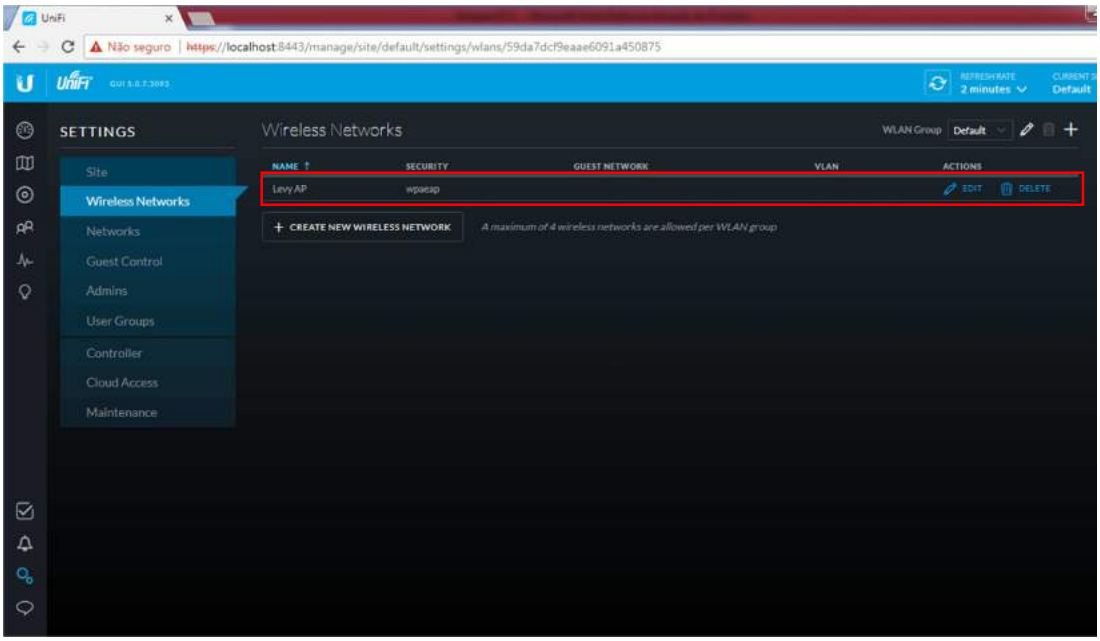

Imagem 96: Tela com a nova rede wi-fi criada

3.6. ADOTANDO O ACCESS POINT

A Unifi Controller utiliza o sistema de criação e configuração da rede e depois ela faz a "**Adoção**" dos access points que ainda não estão configurados para essa rede provisionando as configurações para os AP's, que após a finalização da adoção estarão sob a gestão dessa Unifi Controller.

Primeiramente clicaremos no ícone , essa opção nos levará à tela de configuração dos dispositivos disponíveis para adoção e configuração. Em nosso caso apareceu o access point que já foi pré-configurado em nossa Routerboard. Seu status está como "Pending Approval", ou seja, ele está aguardando a sua adoção por alguma rede configurada na controladora, para isso clicaremos no ícone com a descrição "**ADOPT**" como mostrado na imagem abaixo. A adoção desse access point pela rede *Levy AP* irá demorar aproximadamente 2 minutos, pois a controladora enviará todas as configurações de SSID, segurança, credenciais de autenticação WPA-Enterprise, etc ao access point.

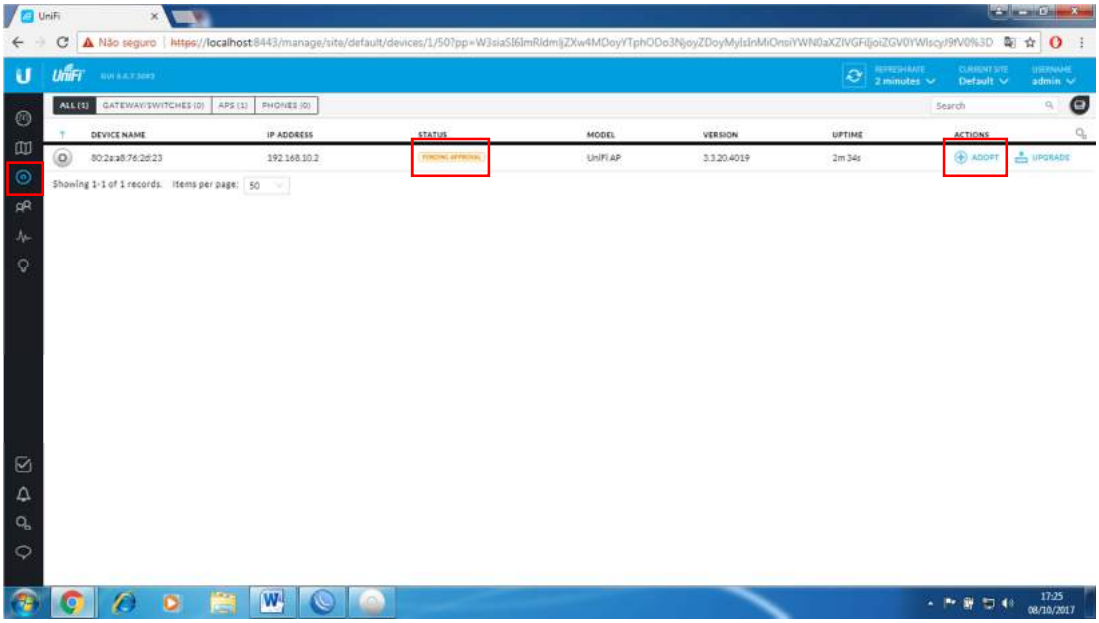

Imagem 97: Tela dos dispositivos (AP's)

ATENÇÃO: No caso do firmware do access point estar muito desatualizado a Unifi Controller não conseguirá finalizar o processo de provisionamento das configurações, ele mostrará a opção de status "**CONNECTED (NEEDS UPGRADE)**", assim como a imagem abaixo. Para atualizar o firmware do access point sugiro utilizar a versão 4.8.15 da Unifi Controller, pois se a versão do firmware for muito antiga a Unifi Controller 5.0.7 não conseguirá atualizá-lo.

Imagem 98: Tela de solicitação de upgrade

Na imagem abaixo podemos ver o access point já adotado pela rede **Levy AP** e com o status "**CONNECTED**".

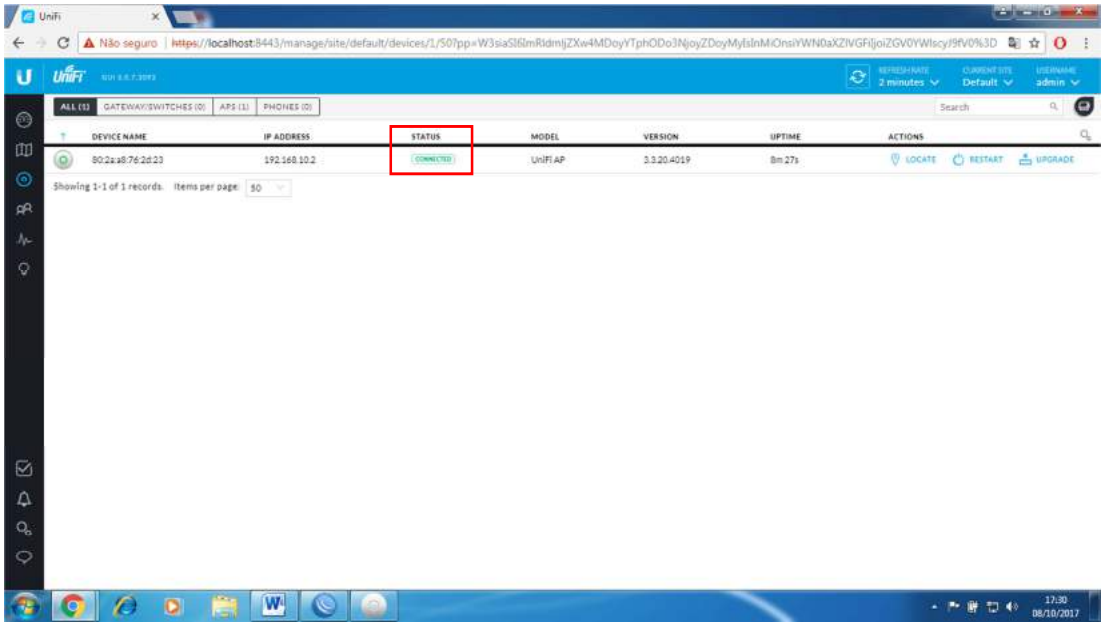

Imagem 99: Tela do dispositivo adotado

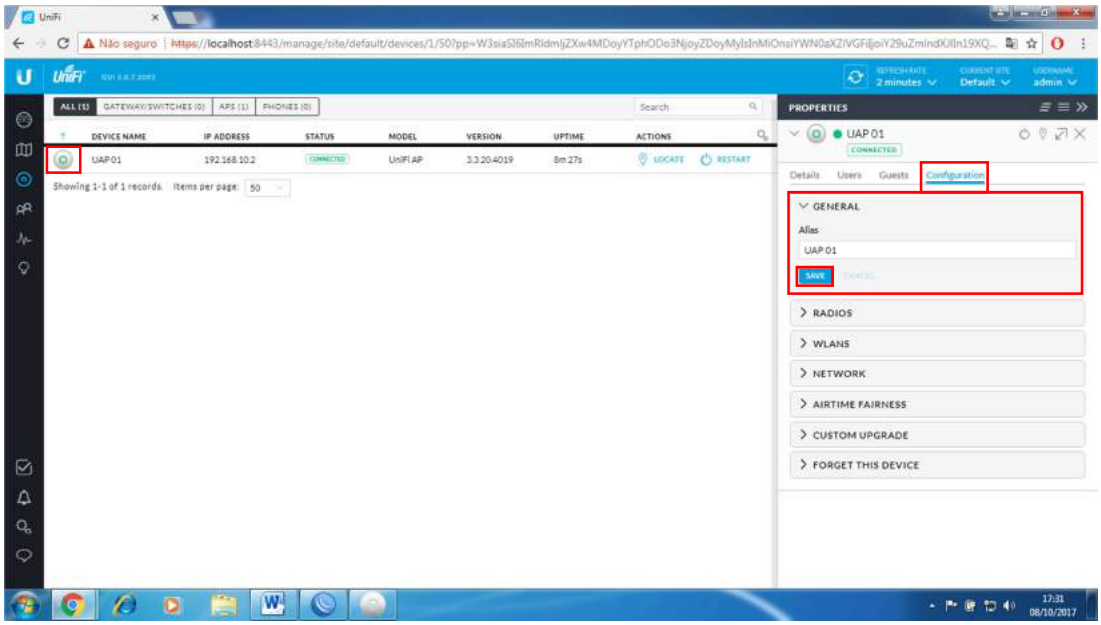

Imagem 100: Configuração do dispositivo adotado 01

Visando sempre uma boa documentação e organização do nosso sistema iremos clicar no ícone ⚪ referente ao access point que iremos configurar, depois clicaremos na aba "*Configuration*" e na opção "*Alias*" personalizaremos o nome de nosso access point para "**UAP 01**", clicando em seguida no botão "**SAVE**", assim como mostrado na Imagem100.

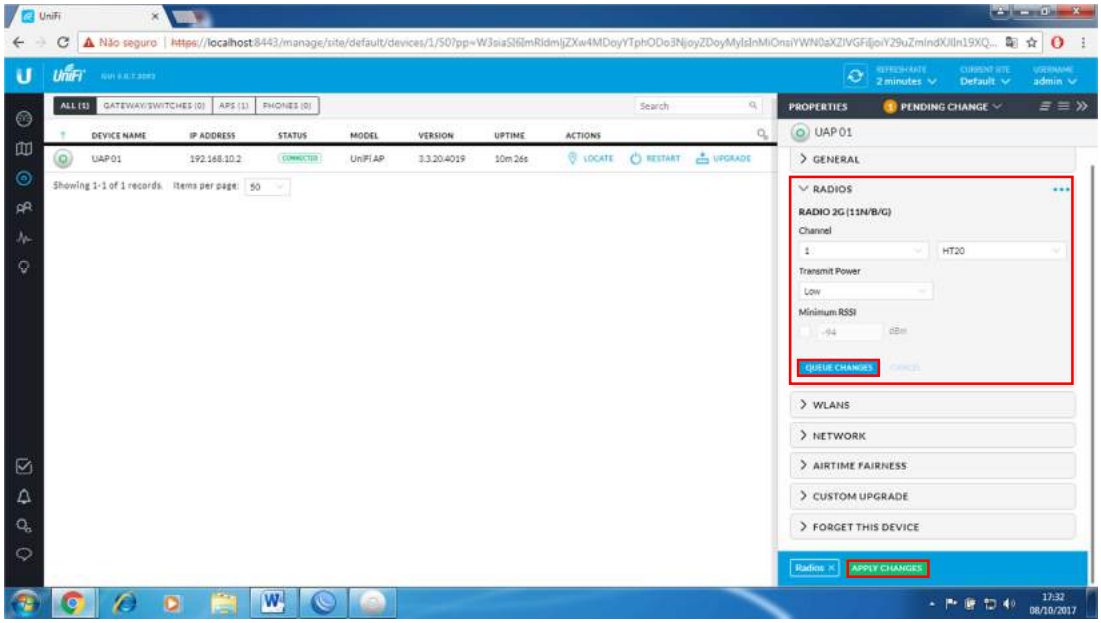

Imagem 101: Configuração do dispositivo adotado 02

Na imagem acima, na opção "**Channel**" iremos configurar o canal do access point para o canal 1, na opção "**Transmit Power**" que regula a força do sinal wi-fi iremos deixar como "*Low*" (baixo), mas essa opção é uma questão de escolha individual, pois se deve levar em consideração a utilização dessa rede e a necessidade do local atendido.

Após realizar as mudanças clicaremos no botão "**QUEUE CHANGES**", e logo em seguida no botão "**APPLY CHANGES**", que irá salvar as alterações e provisionar novamente os dados para o access point, já com as alterações feitas, isso irá demorar aproximadamente 2 minutos novamente. Neste ponto as configurações do access point estão prontas, conforme a imagem abaixo.

Imagem 102: Access Point com configuração finalizada

4. CONFIGURAÇÃO DO SERVIDOR FREERADIUS

4.1. INTRODUÇÃO

Para finalizar esse manual iremos efetuar a instalação e configuração de nosso servidor Freeradius rodando sobre o sistema operacional Debian 7.4 (Wheezy), desse modo nossos access points irão fazer a solicitação ao servidor para verificar a permissão do usuário antes de liberar ou não a conexão à rede **Levy AP**.

4.2. CONFIGURANDO O DHCP SERVER DA ROUTERBOARD

Inicialmente temos que configurar o DHCP Server da Routerboard para que ele forneça um ip fixo ao nosso servidor quando solicitado pelo mesmo. Entraremos no Menu: **IP=>DHCP Server,** na guia **Leases** e selecionaremos a opção ADD, simbolizada no Winbox pelo ícone ✚ .

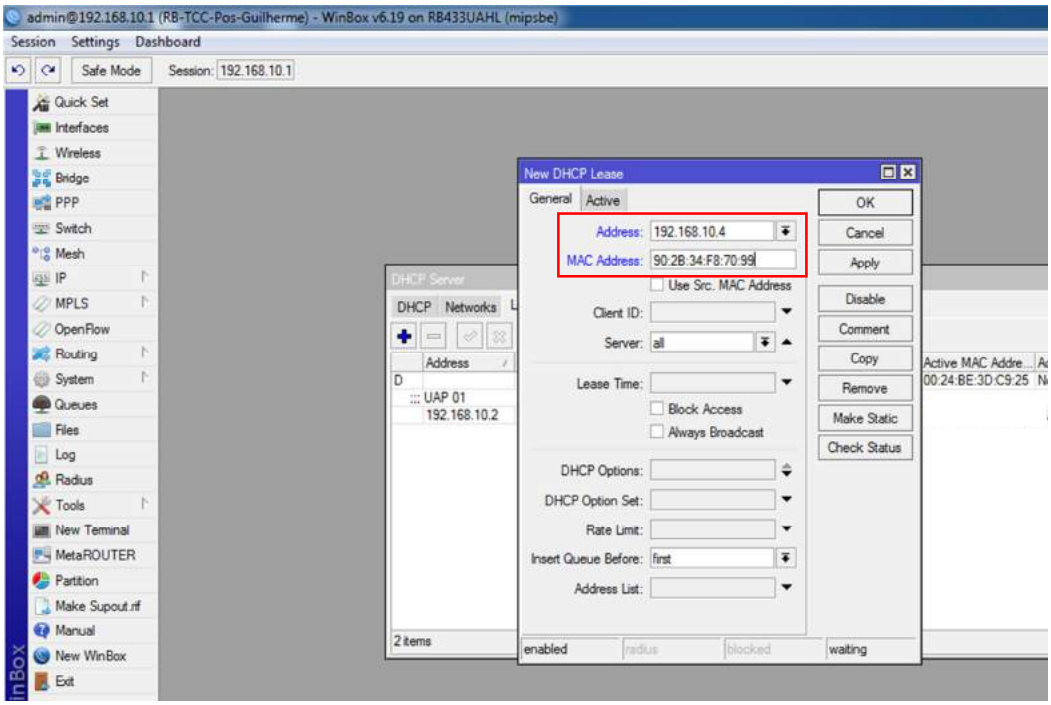

Imagem 103: Adicionando um DHCP Server Lease para o servidor

Agora iremos preencher o campo **Address** com o IP escolhido, nesse caso 192.168.10.4, lembrando o que falamos no capítulo 3.2., que para efeito de controle e para reduzir a chance de conflito de endereço de IP é melhor utilizar um endereço de IP que esteja fora do **POLL** criado na Routerboard. No campo **MAC Address** iremos colocar o endereço MAC da placa de rede ethernet do servidor, conforme a imagem acima.

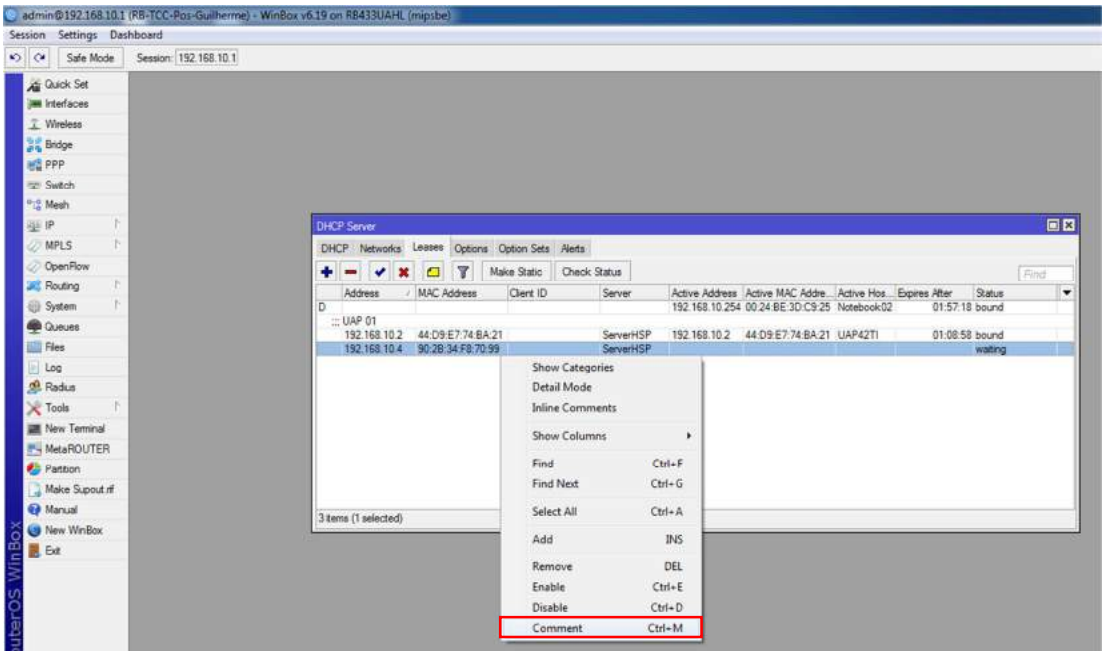

Imagem 104: Adicionando um comentário ao DHCP Server Lease do servidor 01

Para uma boa documentação e organização da Routerboard iremos comentar o novo **DHCP Server Lease** com a identificação *Servidor Radius*, conforme as imagens104 e 105.

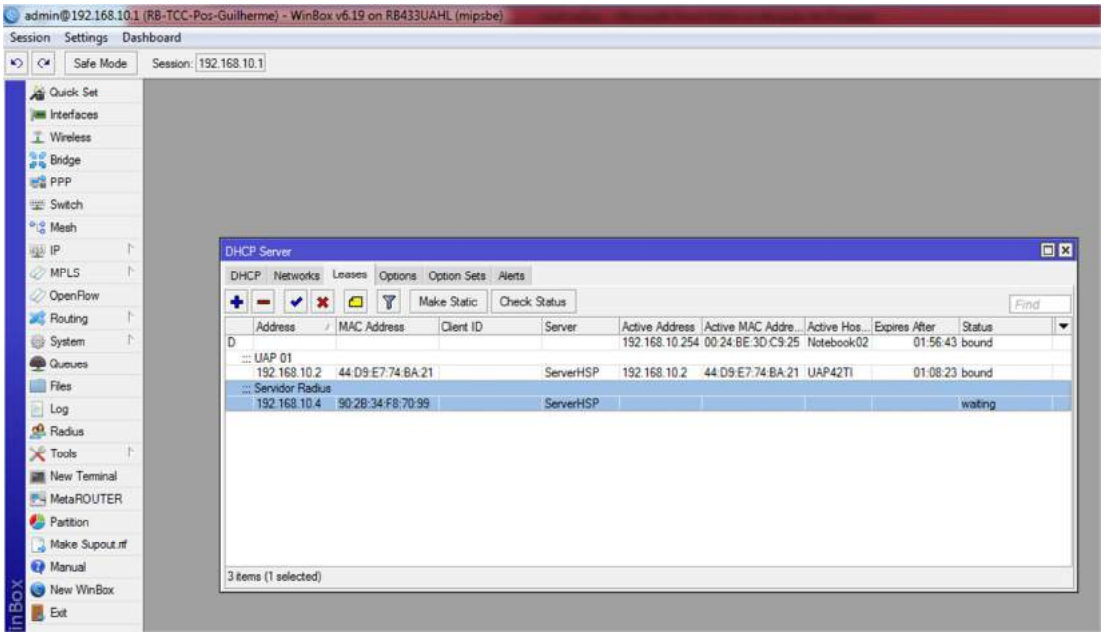

Imagem 105: Adicionando um comentário ao DHCP Server Lease do servidor 02

4.3. INSTALANDO O SISTEMA OPERACIONAL DEBIAN 7.4 (WHEEZY) NO SERVIDOR

Agora vamos instalar o sistema operacional em nosso servidor Freeradius, após testes com o CentOS6, CentOS7, Ubuntu14, Debian9 e Debian7, nós escolhemos o Debian 7.4 como sistema operacional, que se mostrou sem bugs, leve e extremamente estável ao instalar todos os programas e dependências necessárias para rodar o Freeradius com tranquilidade.

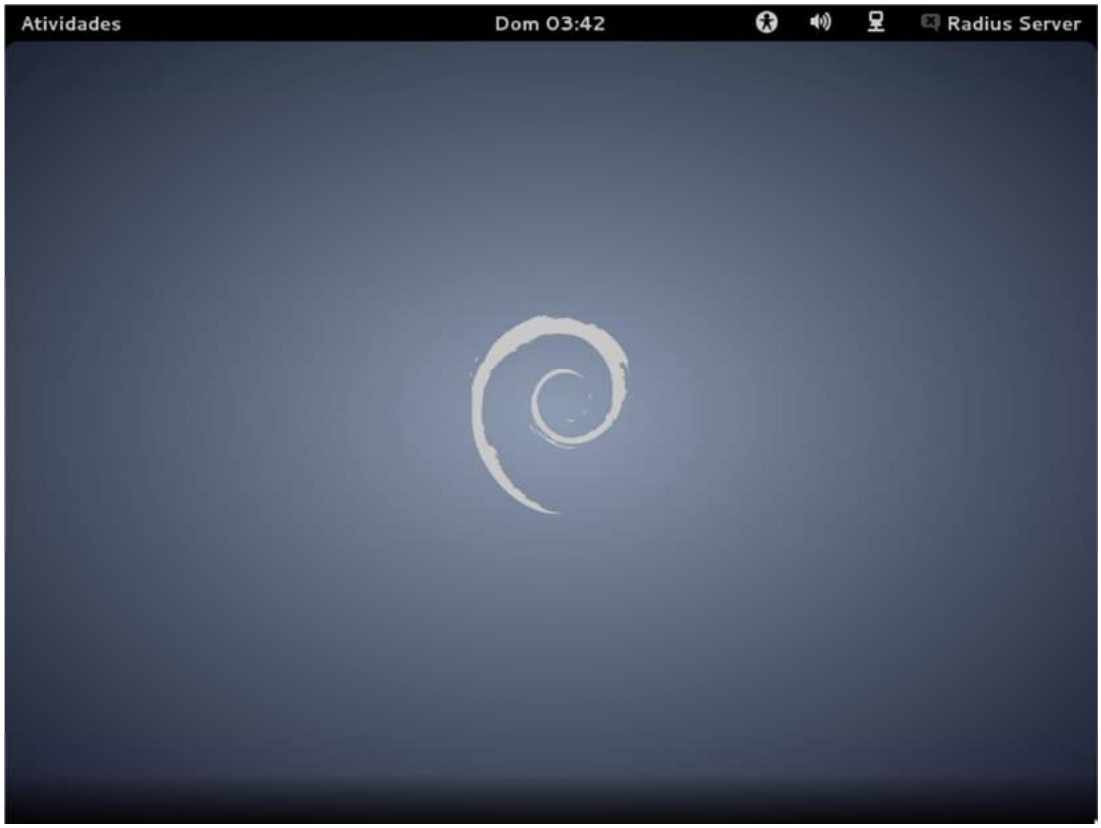

Imagem 106: Instalando o sistema operacional no servidor

Durante a instalação criamos um usuario **radius** e deixamos a rede com o DHCP ativado, pois irá receber o endereço de IP da Routerboard, conforme configurado anteriormente.

Para confirmar se a Routerboard ofertou o endereço de IP corretamente durante a instalação, possibilitando ao servidor que seu processo de instalação baixe os pacotes atualizados que forem necessários vamos entrar no menu: **IP=>DHCP Server,** na guia **Leases**, que deverá estar conforme a Imagem107.

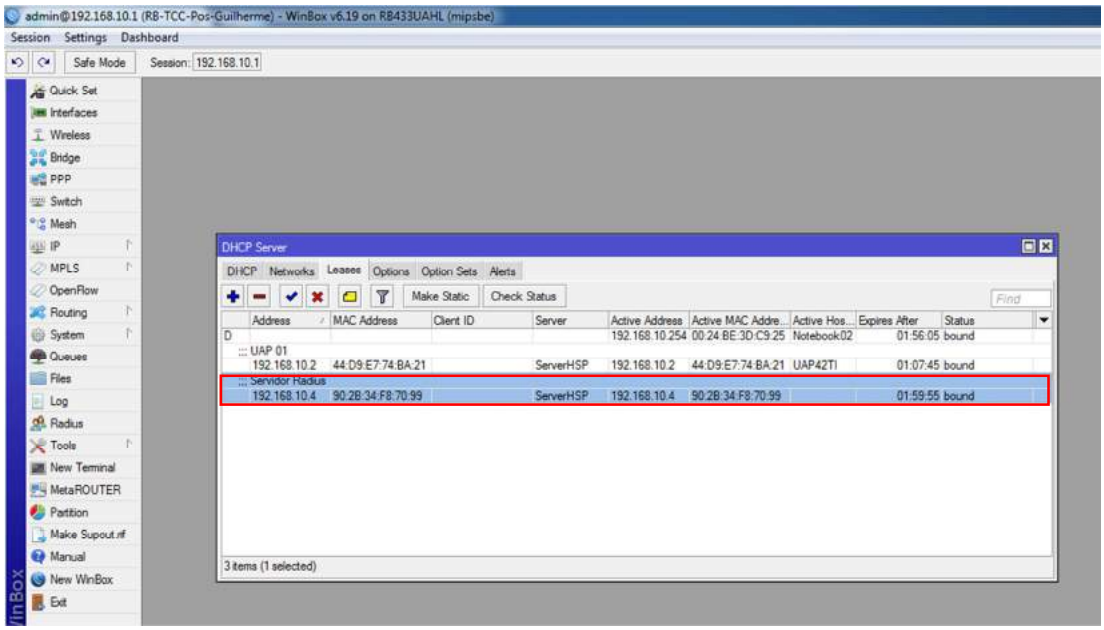

Imagem 107: Endereço de IP ofertado ao servidor Freeradius

Após finalizar a instação podemos verificar nas informações da conexão que o servidor recebeu e está utilizando corretamente o endereço de IP 192.168.10.4, como configurado em nossa Routerboard, assim como a imagem abaixo.

Imagem 108: Endereço de IP ofertado ao servidor Freeradius

4.4. INSTALANDO E CONFIGURANDO O FREERADIUS E O MYSQL-SERVER

Agora iniciaremos a instalação e configuração do programa Freeradius e do MySQL-Server, em todas as vezes que utilizarmos o Terminal do Debian para instalação e configuração dos programas devemos estar com previlégios de ROOT e com acesso à internet, sempre utilizaremos o parametro **"-y"** nas instalações dos pacotes, visando agilizar o processo de instalação, pois quando utizamos esse parametro o sistema entende que a resposta para todas as perguntas durante a instalação é **"yes"**.

Utilizaremos o comando a seguir, conforme a imagem abaixo:

apt-get install freeradius-mysql mysql-server –y

Isso levando em consideração que a máquina não possui o MySQL-Server instalado ainda, como é nosso caso, se o servidor já possuir o MySQL-Server instalado usaremos o seguinte comando:

apt-get install freeradius-mysql –y

Nos dois casos instalaremos o pacote **freeradius-mysql**, que já traz o Freeradius com a integração e a possibilidade da autenticação em uma base de dados MySQL.

Imagem 109: Instalando o Freeradius e o MySQL-Server

Na imagem abaixo podemos ver a configuração do MySQL-Server solicitando a criação de uma senha para o usuário ROOT e logo depois a confirmação da senha escolhida, escolhemos a senha **“2222gl”**.

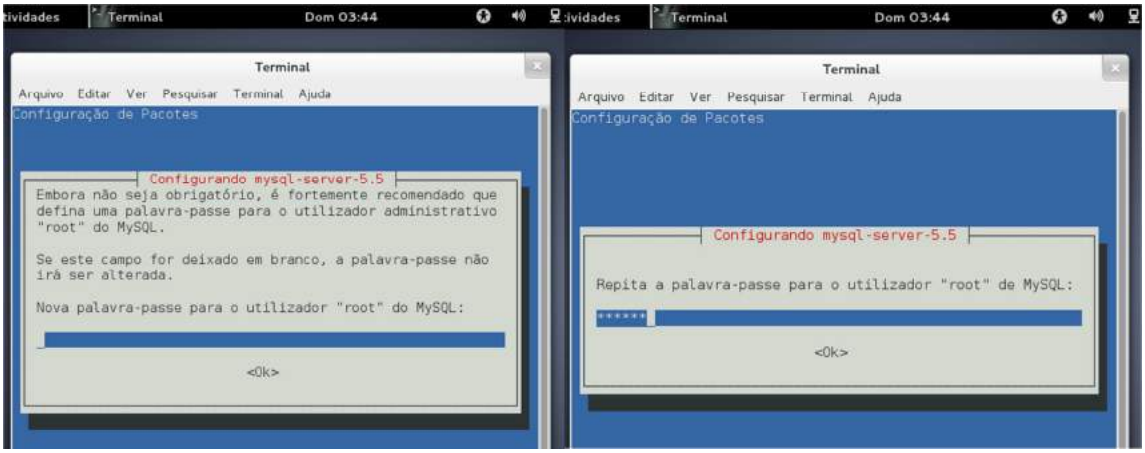

Imagem 110: Configurando uma senha no MySQL-Server

Após a criação da senha para o usuário ROOT o sistema irá continuar a instalação dos pacotes do Freeradius finalizando com uma tela como a imagem abaixo.

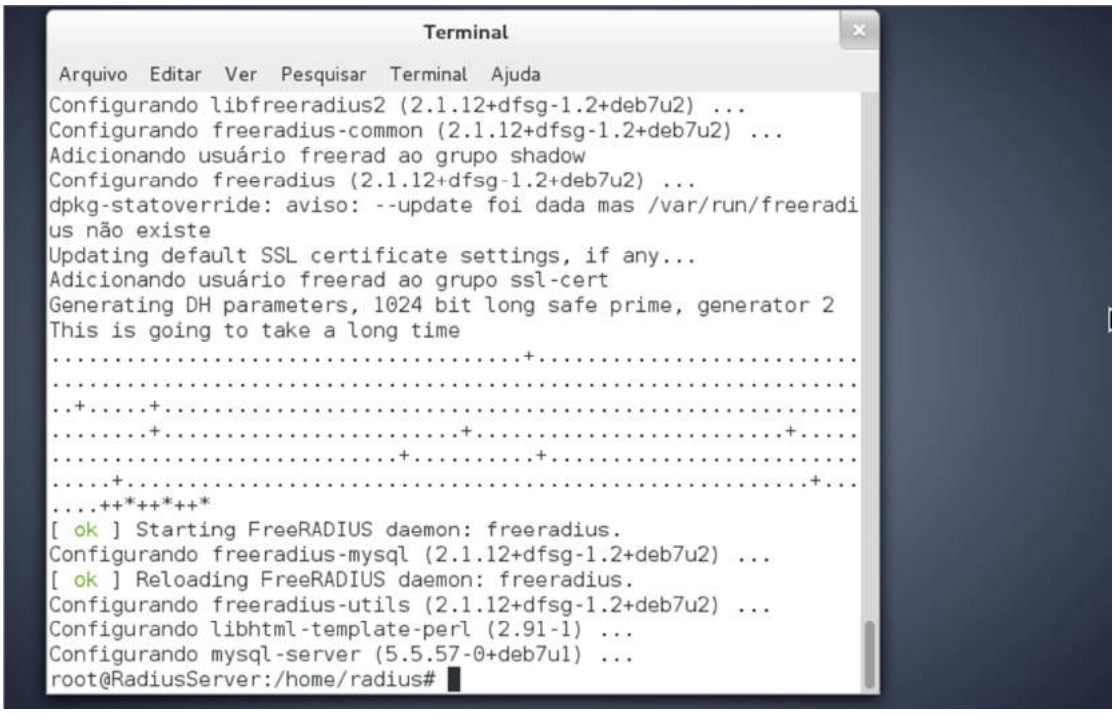

Imagem 111: Finalizando a instalação do Freeradius

Depois de finalizada a instalação precisamos efetuar as alterações nos arquivos de configuração do Freeradius, iniciaremos pelo arquivo **/etc/freeradius/radiusd.conf**. Conforme nos mostra a imagem abaixo, nossa instalação ficou no diretório **/etc/freeradius/**, sempre devemos verificar se a instalação também ficou nesse diretório, senão devemos alterar os caminhos nos comandos.

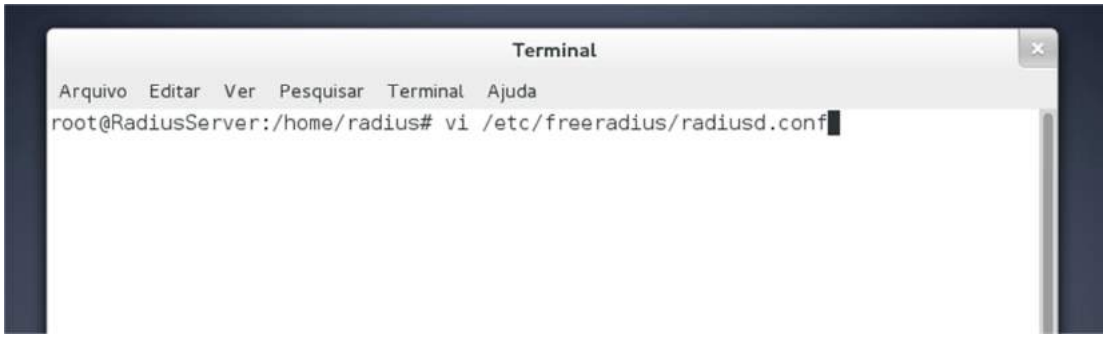

Imagem 112: Alterando o arquivo radiusd.conf 01

Conforme mostrado na imagem abaixo iremos descomentar, ou seja, ativar as duas regras que se referem à conexão do Freeradius com o banco de dados MySQL.

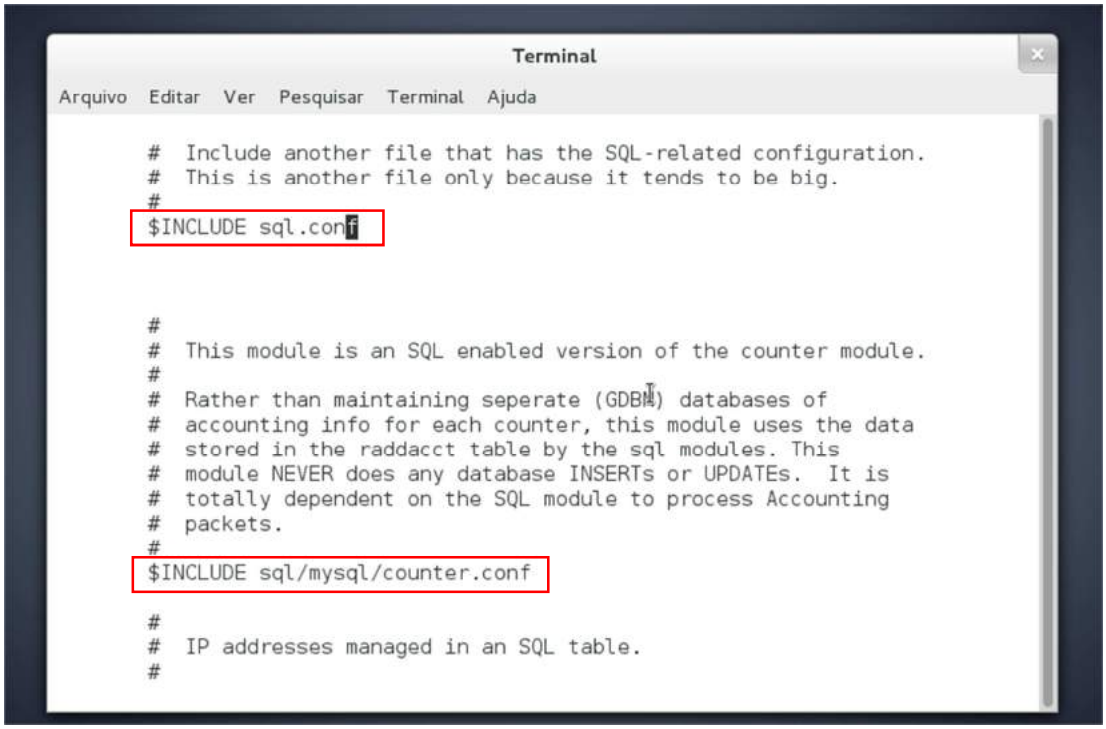

Imagem 113: Alterando o arquivo radiusd.conf 02

Agora iremos alterar o arquivo **/etc/freeradius/sql.conf**, que traz entre outras, as configurações de conexão do Freeradius com o banco de dados no MySQL-Server.

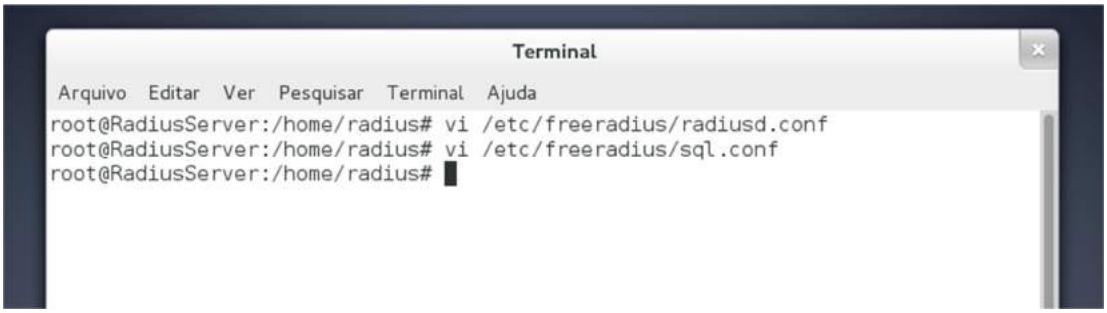

Imagem 114: Alterando o arquivo sql.conf 01

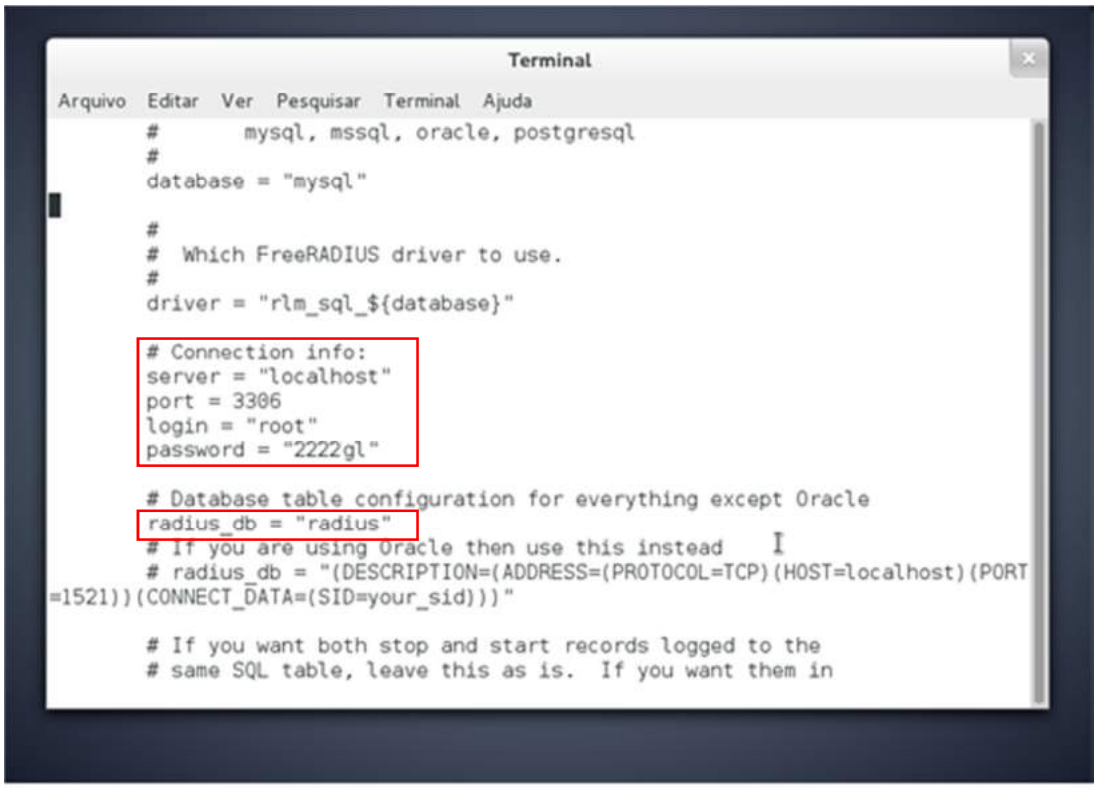

Imagem 115: Alterando o arquivo sql.conf 02

Conforme a imagem acima iremos alterar os parâmetros de conexão ao banco de dados, e o nome do banco de dados que será utilizado pelo Freeradius.

Em **“server”**, colocaremos *localhost*, pois em nosso caso o Freeradius acessará um banco de dados dentro do próprio servidor onde ele está instalado, em **“port”** iremos deixar a porta padrão do MySQL que é *3306*. Nos campos de login e password utilizaremos o usuário *root* e a senha que cadastramos durante a instalação do MySQL-Server.

Na opção **“radius_db”** colocaremos o nome do banco de dados que iremos criar no MySQL-Server futuramente e será o banco de dados do Freeradius, nesse caso nós optamos por escolher o nome *radius*. Assim acabamos a alteração do arquivo e salvamos o mesmo com as alterações feitas.

Imagem 116: Alterando o arquivo clients.conf 01

Conforme a imagem abaixo, no arquivo **/etc/freeradius/clientes.conf** iremos somente incluir a rede e mascara dos access points (*192.168.10.0/24*) que irão solicitar ao Freeradius a conexão e a senha (*levyap2017*) que foi cadastrada quando criamos a rede dos AP’s na Unifi Controller, conforme foi feita no capítulo 3.5.

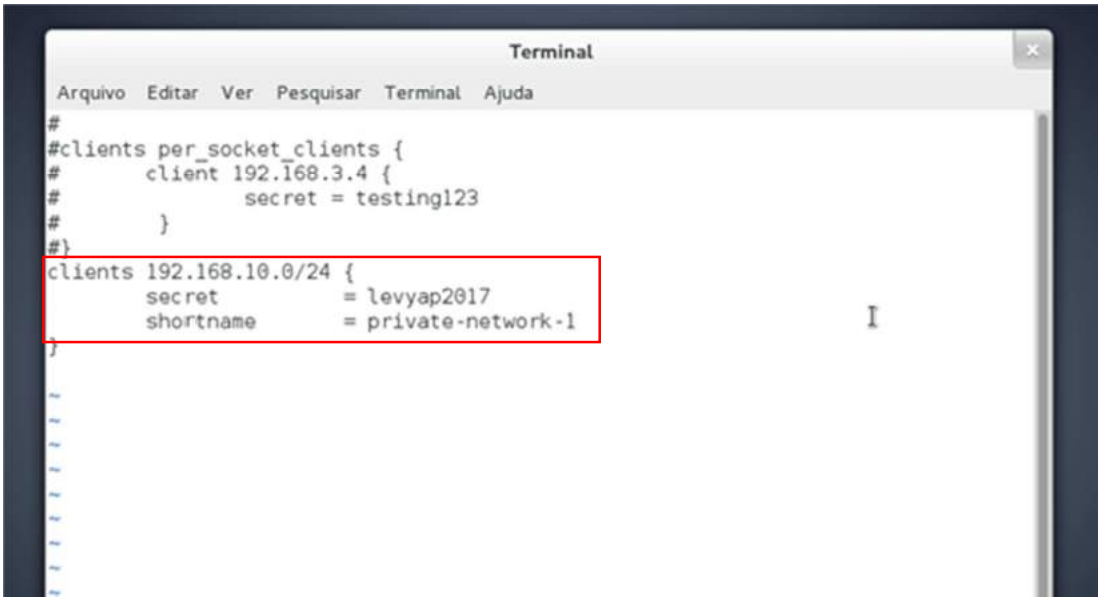

Imagem 117: Alterando o arquivo clients.conf 02

No arquivo **/etc/freeradius/eap.conf** vamos escolher o tipo de protocolo *eap* que iremos utilizar para a autenticação dos usuários no Freeradius.

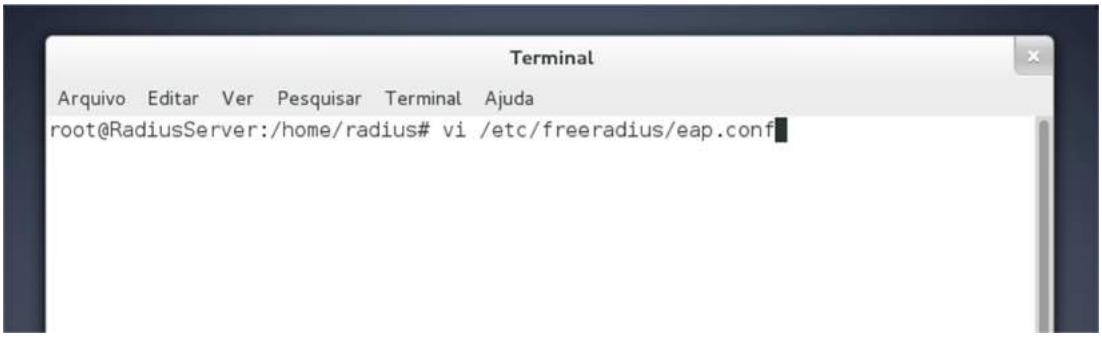

Imagem 118: Alterando o arquivo eap.conf 01

Em nosso caso escolhemos o protocolo *PEAP*, como mostra a imagem abaixo.

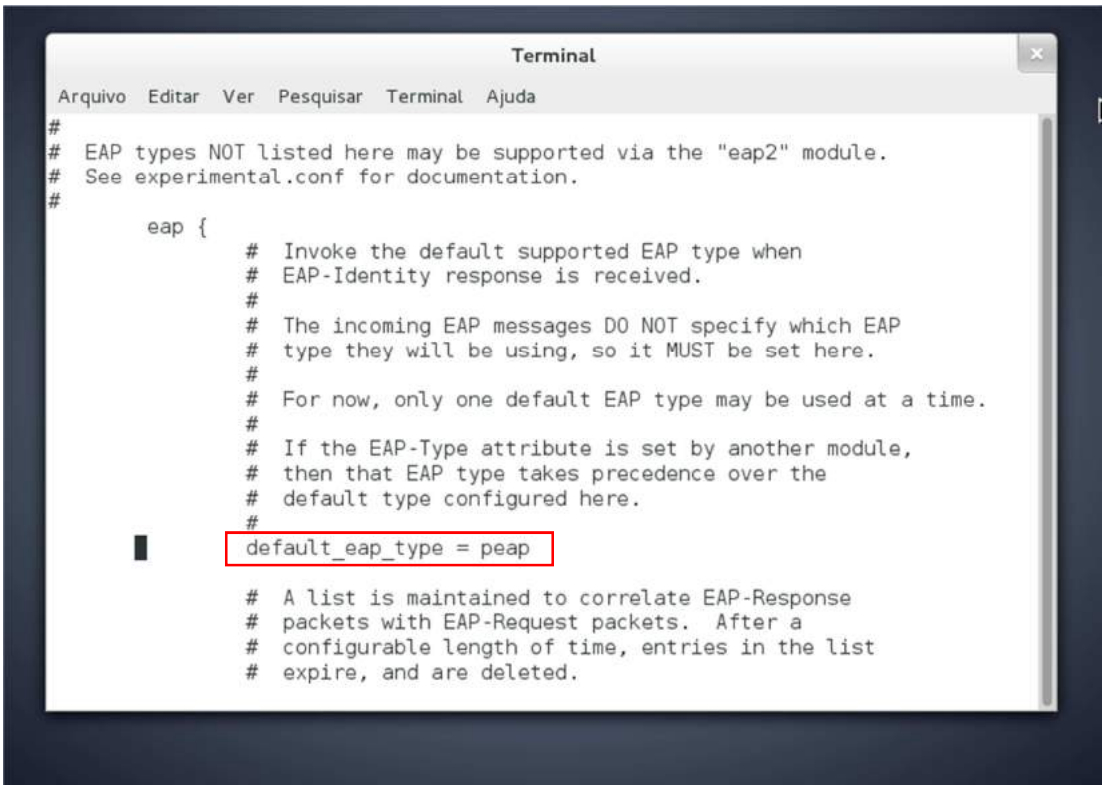

Imagem 119: Alterando o arquivo eap.conf 02

Nos arquivos **/etc/freeradius/sites-enabled/default** e **/etc/freeradius/sites-enabled/inner-tunnel** iremos descomentar todas as linhas que irão permitir a autenticação dos usuários em um banco de dados MySQL.

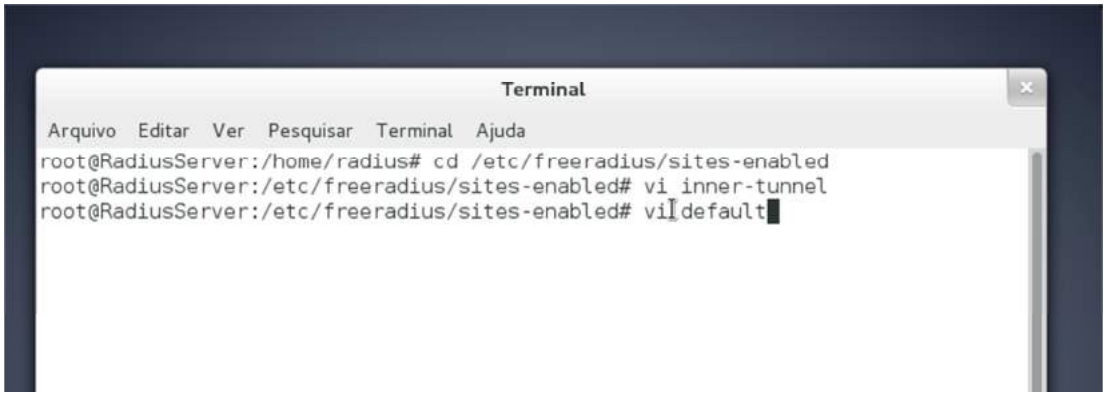

Imagem 120: Alterando os arquivos default e inner-tunnel 01

Conforme a imagem abaixo iremos descomentar todas as linhas *sql* do “Authorization Queries” dos dois arquivos.

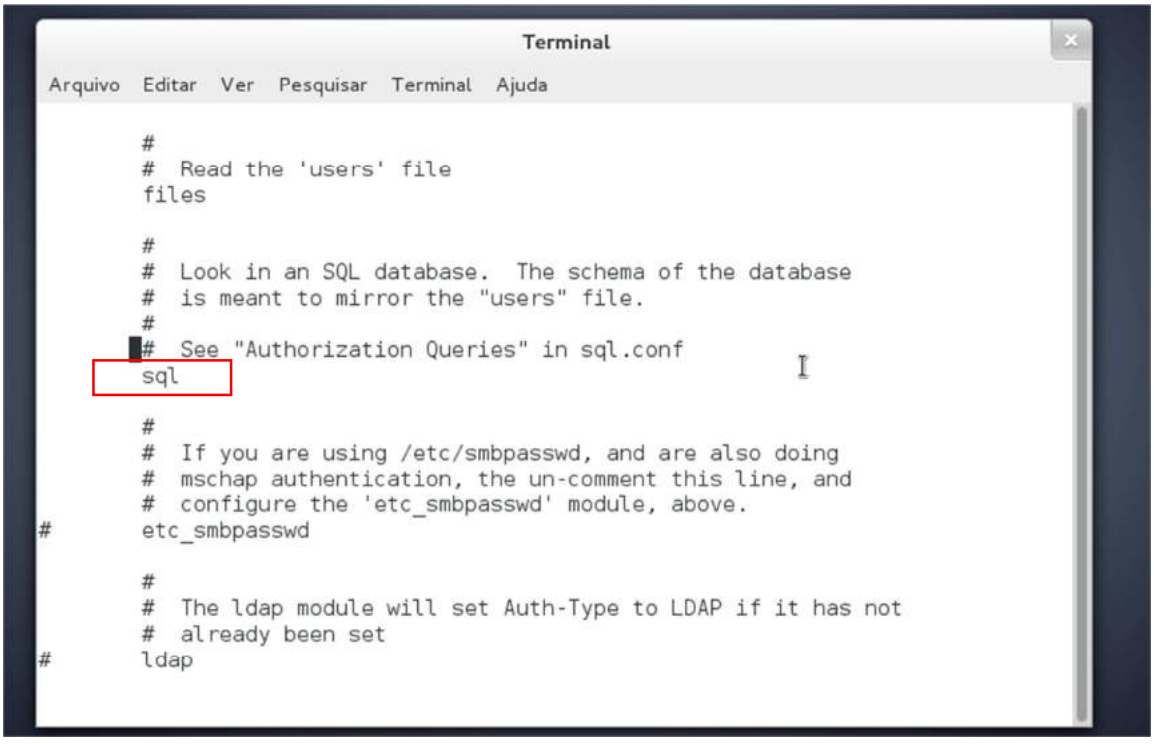

Imagem 121: Alterando os arquivos default e inner-tunnel 02

Conforme a imagem abaixo iremos descomentar todas as linhas *sql* do "Authentication Logging Queries" dos dois arquivos.

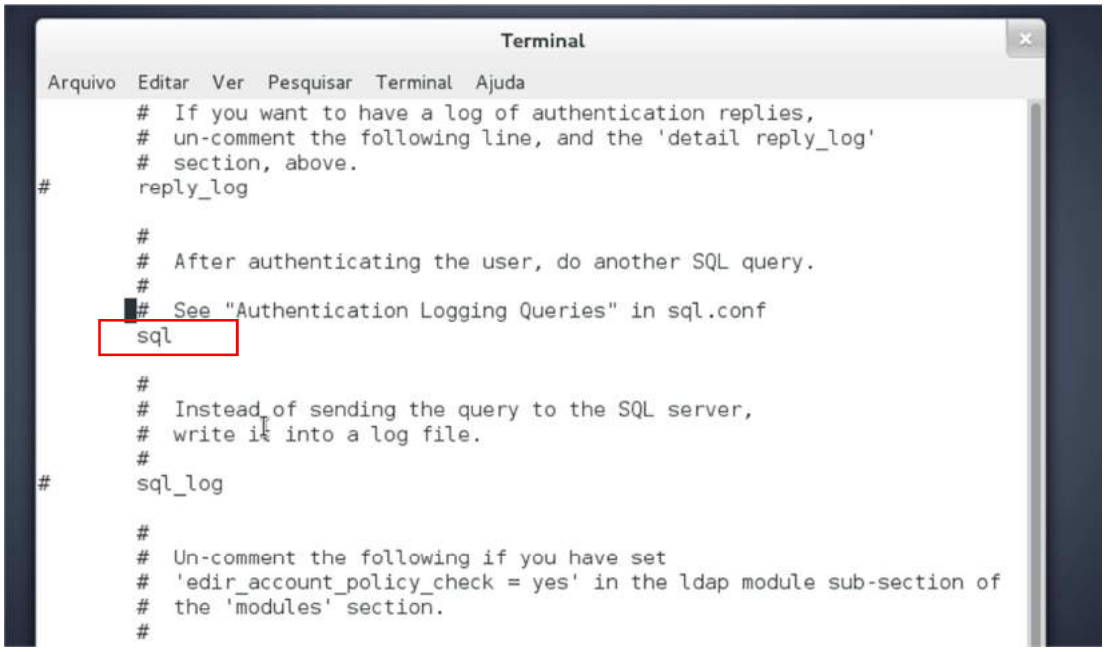

Imagem 122: Alterando os arquivos default e inner-tunnel 03

4.4.1. TESTANDO O FREERADIUS

Após finalizar as alterações dos arquivos de configuração do Freeradius já podemos fazer o teste e verificar se ele já encontra-se em funcionamento e já esta recebendo as solicitações dos access points.

Imagem 123: Testando o Freeradius 01

Conforme a imagem acima, utilizaremos o comando *service freeradius stop* para parar o serviço Freeradius e logo em seguida iniciaremos o serviço em seu modo de depuração utilizando o comando freeradius -X.

Após utilizarmos esse comando deverá ser apresentada uma tela como a imagem abaixo se a instalação estiver correta até esse momento, ou seja, o servidor está pronto e aguardando as requisições.

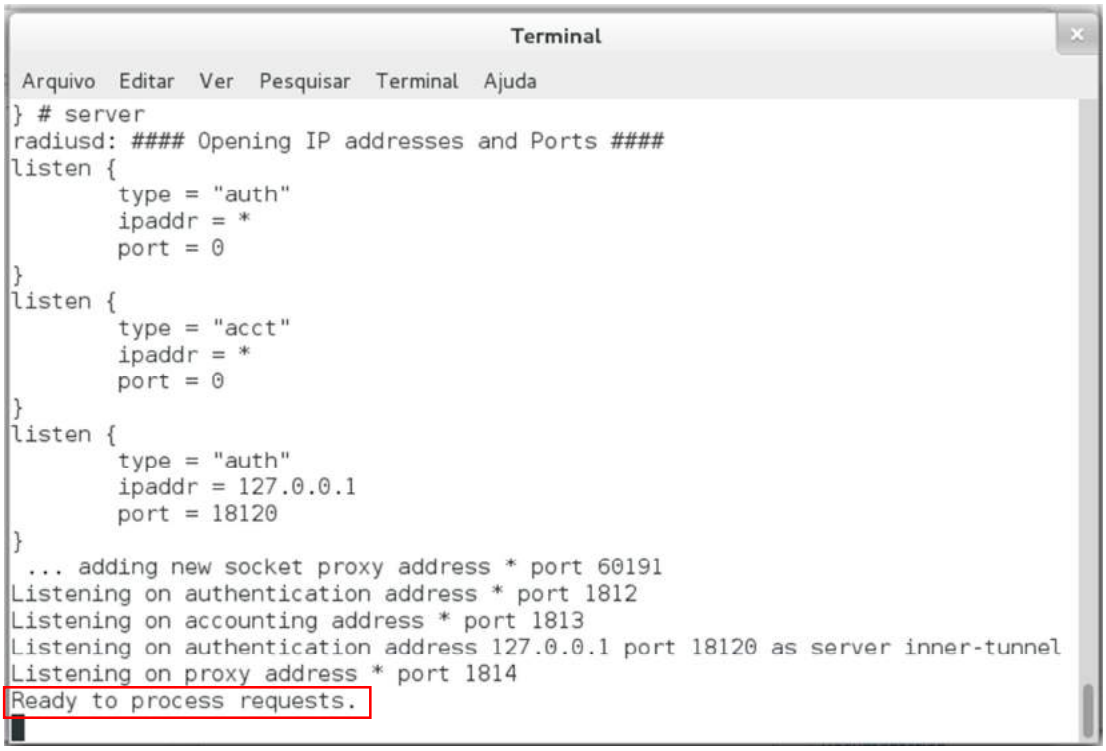

Imagem 124: Testando o Freeradius 02

Agora iremos fazer um teste e verificar se o access point já está se comunicando com o servidor e fazendo as requisições ao Freeradius.

Vamos tentar nos conectar a rede **"Levy AP"** que está configurada no UAP01 utilizando o protocolo PEAP, **usuário** "*guilherme*" e **senha** "*tcc*", mesmo sem criar o nosso banco de dados o Freeradius já deve nos mostrar uma tela como a Imagem125.

Ao tentarmos efetuar a autenticação na rede **"Levy AP"** o access point irá solicitar ao servidor Freeradius a liberação do usuário *guilherme*, o Freeradius então consultará o MySQL-Server para verificar se esse usuário existe no banco de dados radius e verificar as configurações referentes ao access point (nas), como esse banco de dados ainda não foi criado ele retornará a mensagem de erro, assim como aconteceu na Imagem125.

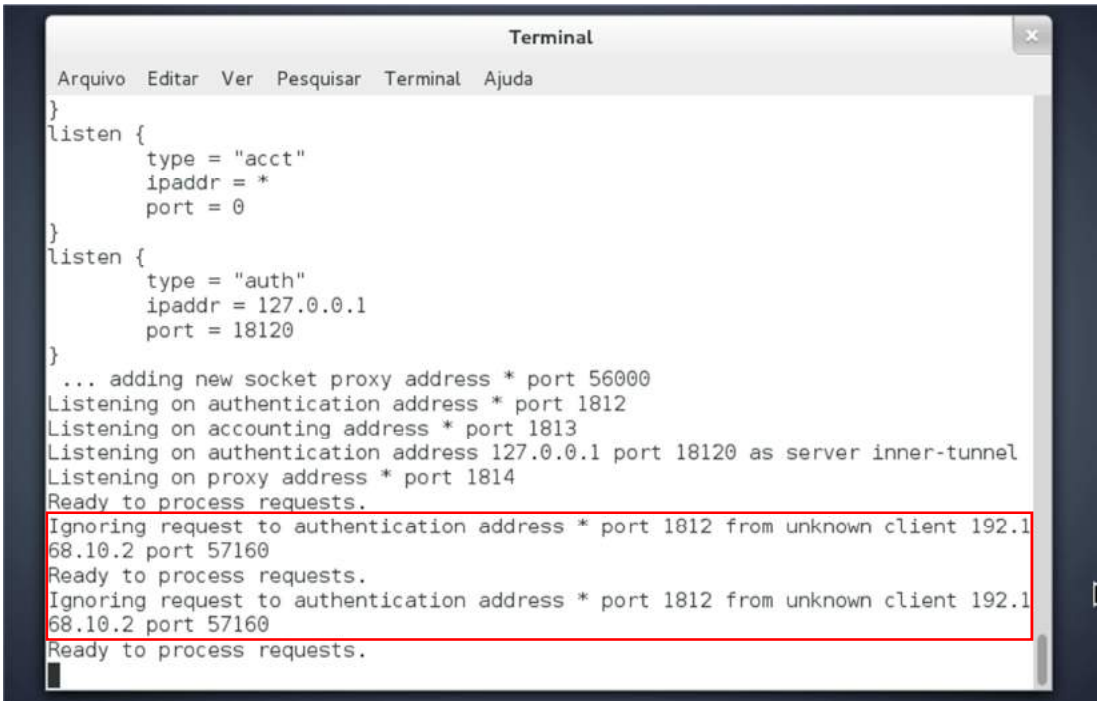

Imagem 125: Testando o Freeradius 03

4.5. CRIANDO O BANCO DE DADOS RADIUS

Primeiramente entraremos no MySQL-Server utilizando as credenciais de usuário e senha previamente criados no capítulo 4.4.

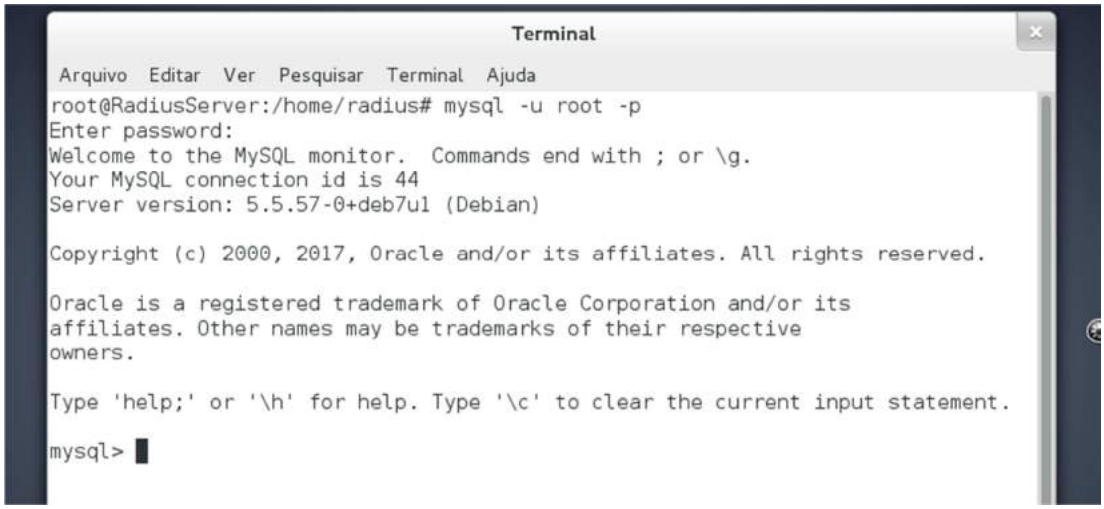

Imagem 126: Entrando do MySQL-Server

Após isso criaremos o banco de dados com o nome "*radius*" conforme especificamos previamente nos parâmetros do arquivo de configuração **/etc/freeradius/sql.conf**, mostrado no capítulo 4.4.

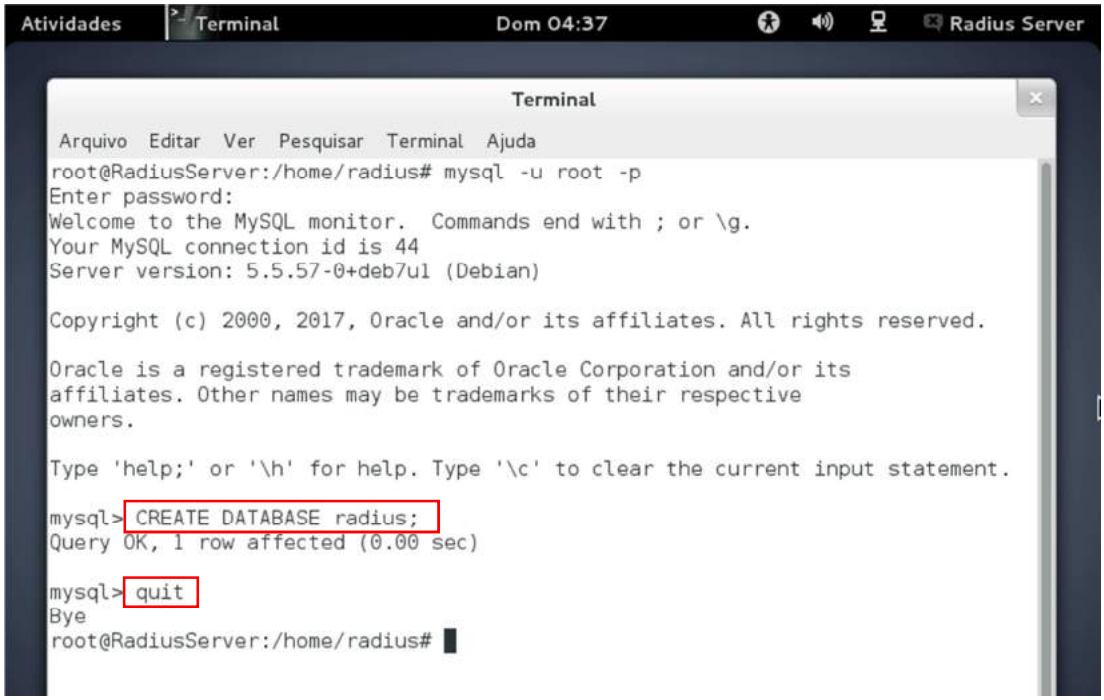

Imagem 127: Criando o BD radius

Agora iremos buscar dentro do diretório **/etc/freeradius/sql/mysql/** o arquivo *schema.sql* que traz o modelo de tabelas a serem criadas em nosso banco de dados.

Imagem 128: Criando as tabelas no BD radius

Assim como na Imagem128, após localizar o arquivo *schema.sql* devemos executar o comando a seguir:

```
mysql –u root –p radius </etc/freeradius/sql/mysql/schema.sql
```

Esse comando criará automaticamente as tabelas necessárias para a conexão do Freeradius ao MySQL-Server, para consultarmos se as tabelas foram criadas entraremos no banco radius e utilizaremos o comando SHOW tables;.

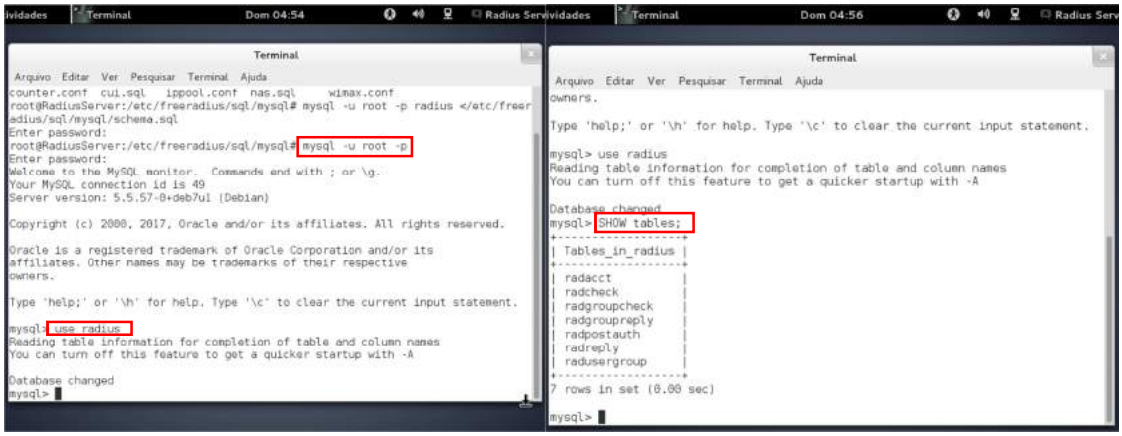

Imagem 129: Consultando as tabelas criadas no BD radius

Em alguns casos o arquivo *schema.sql* não cria a tabela "**nas**", que é responsável pelo cadastro dos endereços de IP dos access points que irão acessar nosso Freeradius, desse modo devemos criar a tabela manualmente, assim como a imagem abaixo.

```
mysql> use radius
Reading table information for completion of table and column names
You can turn off this feature to get a quicker startup with -A

Database changed
mysql> CREATE TABLE IF NOT EXISTS `nas` (
    ->   `id` int(10) NOT NULL AUTO_INCREMENT,
    ->   `nasname` varchar(128) NOT NULL,
    ->   `shortname` varchar(32) DEFAULT NULL,
    ->   `type` varchar(30) DEFAULT 'other',
    ->   `ports` int(5) DEFAULT NULL,
    ->   `secret` varchar(60) NOT NULL DEFAULT 'secret',
    ->   `server` varchar(64) DEFAULT NULL,
    ->   `community` varchar(50) DEFAULT NULL,
    ->   `description` varchar(200) DEFAULT 'RADIUS Client',
    ->   PRIMARY KEY (`id`),
    ->   KEY `nasname` (`nasname`)
    -> ) ENGINE=MyISAM  DEFAULT CHARSET=latin1 AUTO_INCREMENT=40 ;
Query OK, 0 rows affected (0.06 sec)
```

Imagem 130: Criando a tabela nas no BD radius

Após a criação da tabela *nas* no banco de dados *radius* podemos sair do MySQL-Server.

4.5.1. INSTALANDO O PHPMYADMIN

Para facilitar a visualização e inserção de dados em nosso banco de dados do Freeradius iremos instalar o phpMyAdmin através do comando:

apt-get install phpMyAdmin -y

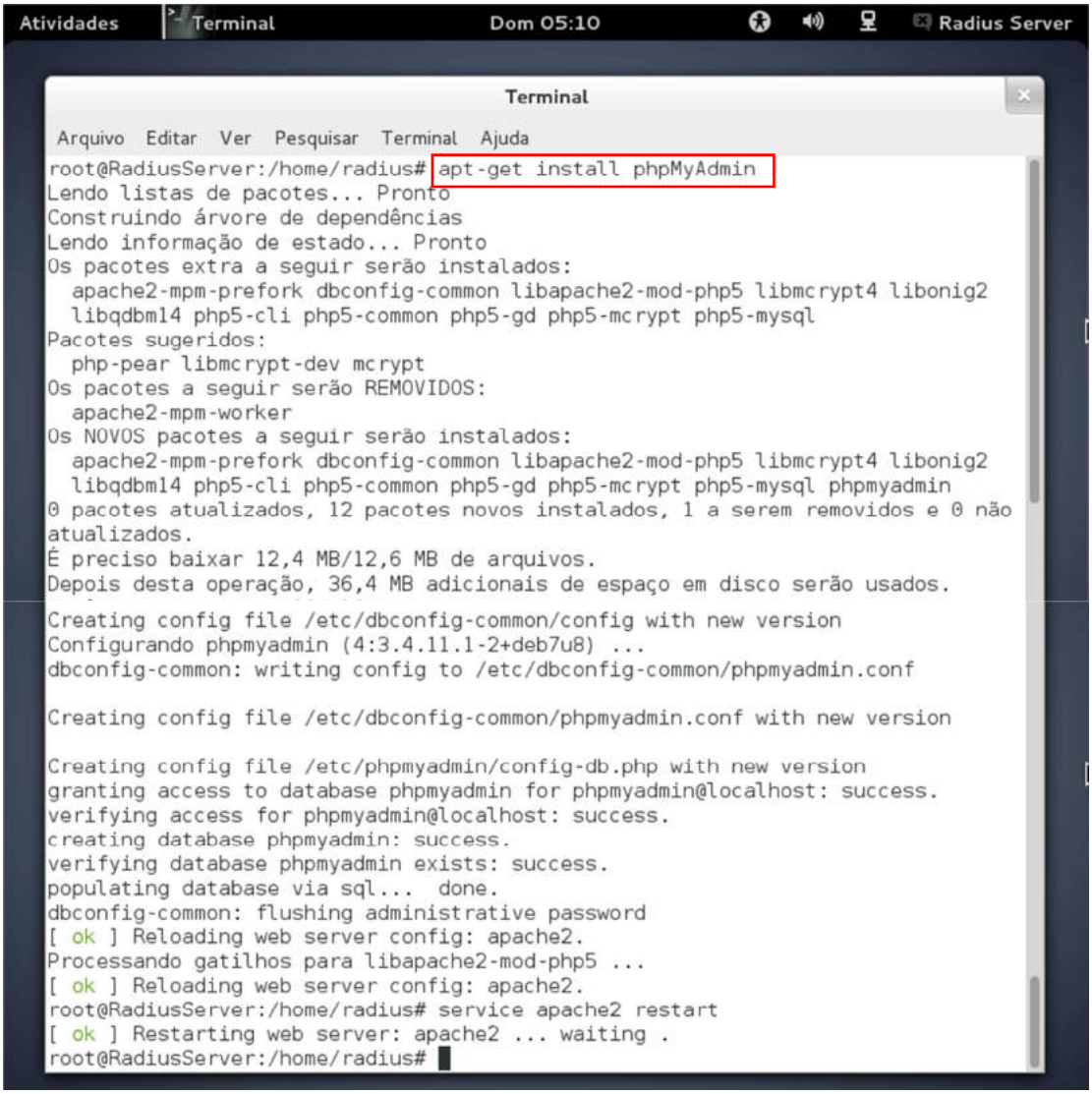

Imagem 131: Instalando o phpMyAdmin

Após o final da instalação já podemos acessar o phpMyAdmin através do endereço **127.0.0.1/phpmyadmin**, utilizando nossas credenciais do MySQL-Server criadas no capítulo 4.4., assim como a imagem abaixo.

Imagem 132: Acessando o phpMyAdmin

4.5.2. INSERINDO DADOS NO BANCO DE DADOS RADIUS

Primeiramente acessaremos a tabela *nas* no banco de dados *radius* e adicionaremos o registro do nosso access point, conforme a imagem abaixo.

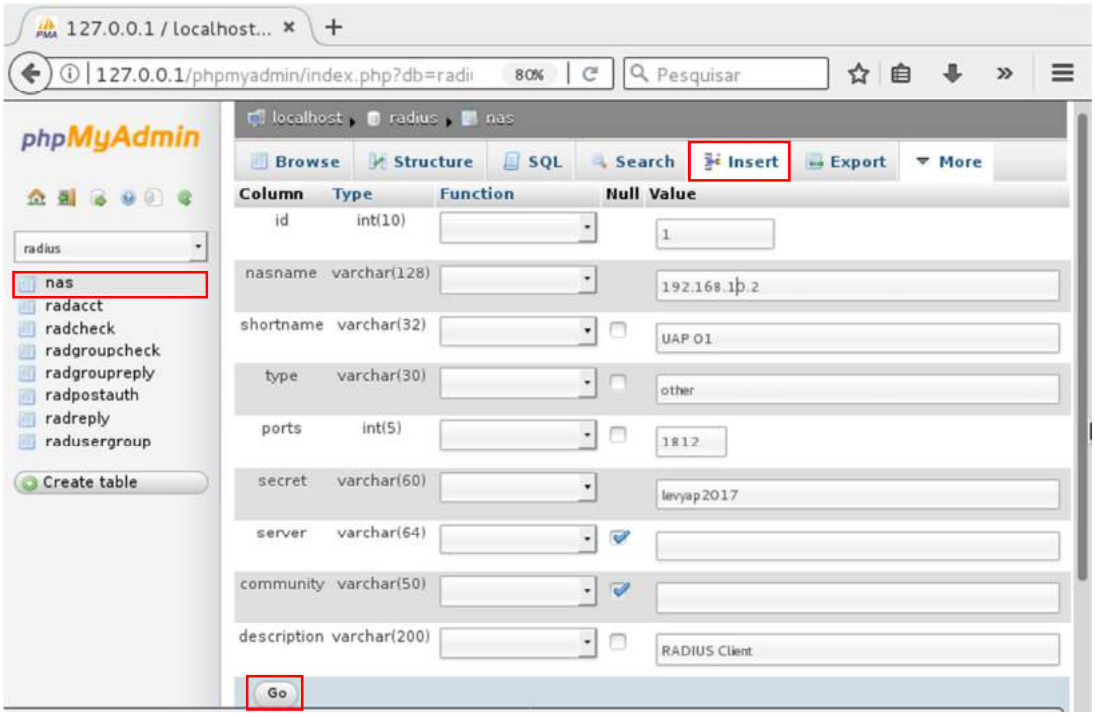

Imagem 133: Inserindo um Access Point (nas)

Como vemos na Imagem133, no campo **id** preencheremos um número que identificará nosso AP no banco de dados, nesse caso *1*, no campo **nasname** iremos preencher com o endereço de IP do AP, nesse caso *192.168.10.2*, no campo **shortname** vamos colocar um nome para fácil identificação do AP, vamos utilizar o mesmo nome que colocamos na Routerboard e na Unifi Controller, ou seja, *UAP01*, no campo **ports** utilizamos a porta *1812* e no campo **secret** vamos colocar a senha que escolhemos para nossos AP's se conectarem ao Freeradius, nesse caso *levyap2017*, após isso vamos salvar o registro clicando no botão **"GO"**.

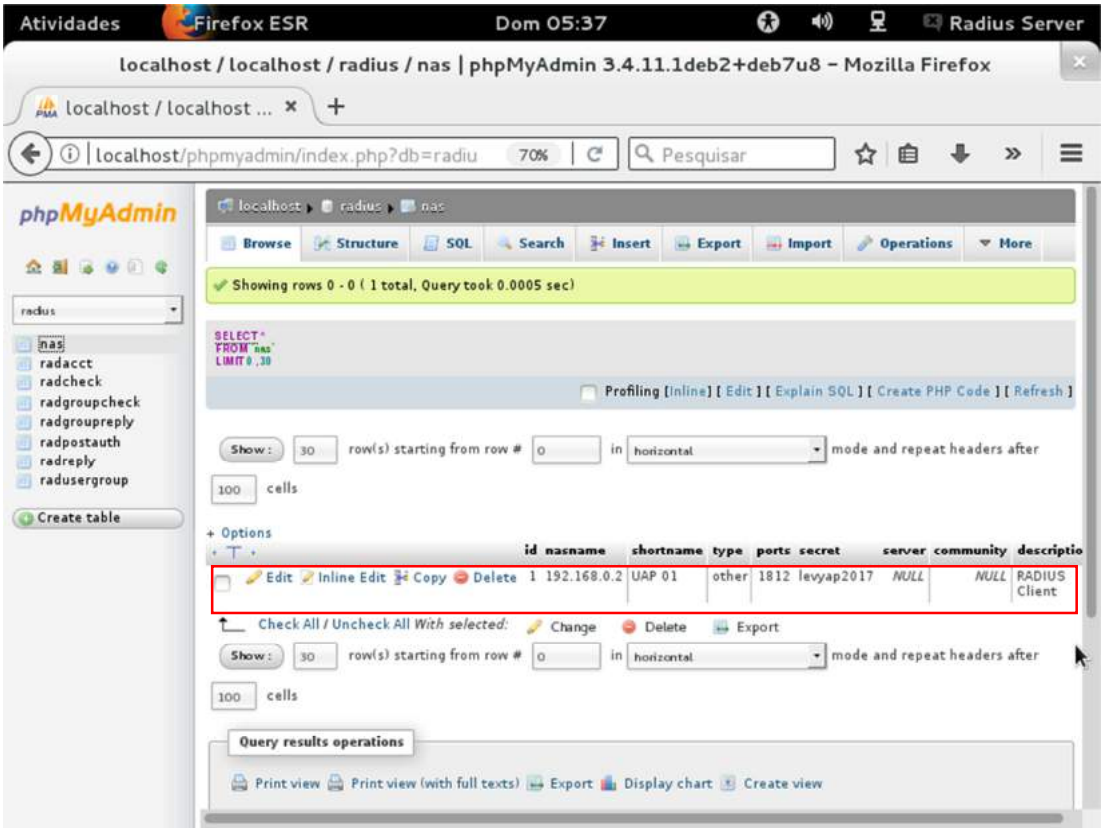

Imagem 134: Tabela depois de inserido o registro (nas)

Após a inclusão desse registro na tabela *nas* iremos incluir um usuário de teste na tabela *radcheck*, que é a tabela onde ficarão os cadastro dos usuários.

Criaremos um usuário e sua senha, mas o sistema também permite que crie usuários vinculados ao endereço MAC de seu equipamento, os parâmetros da autenticação dos usuários depende da necessidade do administrador da rede.

Como mostra a imagem abaixo, no campo **id** preencheremos um número que identificará nosso usuário no banco de dados, nesse caso *1*, no campo **username** iremos preencher com o login do usuário, nesse caso *guilherme*, no campo **attribute** vamos colocar password, pois vamos utilizar a autenticação via usuário/senha, no campo **op** vamos preencher *:=* e no campo **value** vamos colocar a senha que escolhemos para nosso usuário, nesse caso *tcc*, após isso vamos salvar o registro clicando no botão **"GO"**.

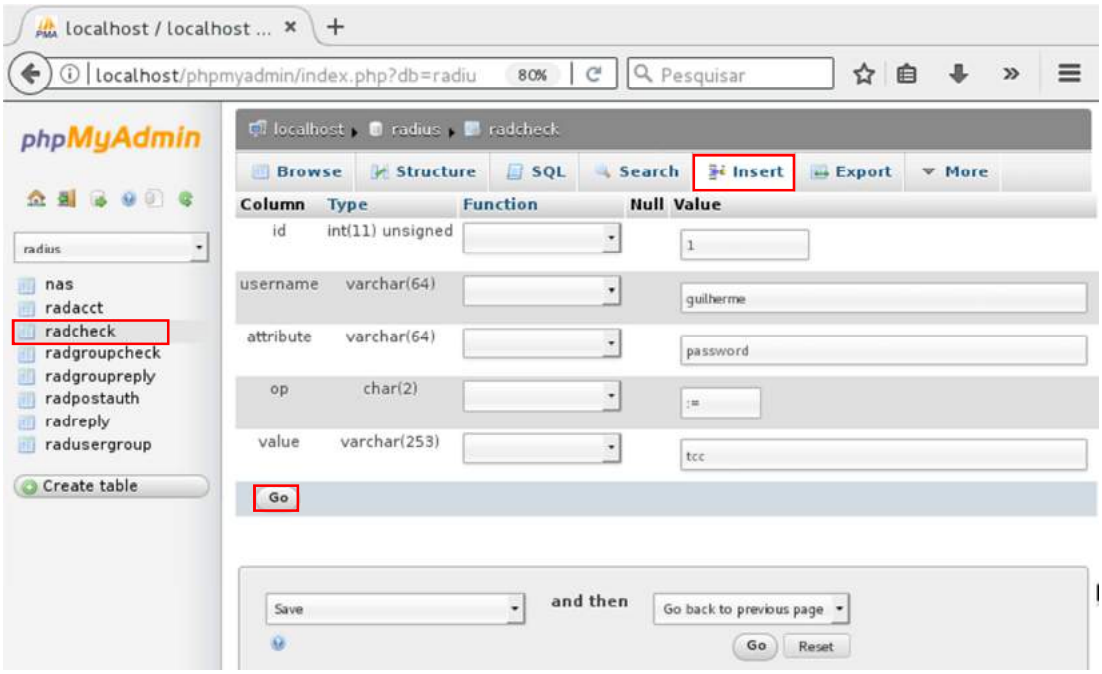

Imagem 135: Inserindo um usuário (radcheck)

4.6. CONFIGURANDO UM DISPOSITIVO PARA CONEXÃO

Como alterado no arquivo **/etc/freeradius/eap.conf** e explicado no capítulo 4.4. nós selecionamos *PEAP* como o tipo padrão de protocolo EAP para autenticação, portanto o dispositivo deve ter a opção de autenticação através desse protocolo ou através do protocolo *TTLS* que também foi configurado para conexão.

Em dispositivos com IOS, Android e Linux não é necessário nenhuma instalação adicional, basta selecionar o tipo de protocolo a ser utilizado e especificar um usuário e senha já cadastrados em nosso banco de dados, mas em dispositivos com o sistema operacional Microsoft Windows devemos utilizar o *PEAP*, portanto é necessário que o microcomputador tenha o protocolo *PEAP* instalado. Se o dispositivo não tiver, é necessário fazer a instalação, o software **EAP.msi** que instala esse protocolo pode ser baixado no site:

https://software.cisco.com/download/release.html?mdfid=286275122&softwareid=286275013

ATENÇÃO: Esse procedimento somente necessita ser feito devido à nossa configuração nos parâmetros de EAP no arquivo **/etc/freeradius/eap.conf** do Freeradius e pode ser adequada por necessidade do administrador da rede.

Imagem 136: Instalando o EAP.msi

Depois de instalado o protocolo *PEAP* devemos criar a rede manualmente, conforme imagem abaixo.

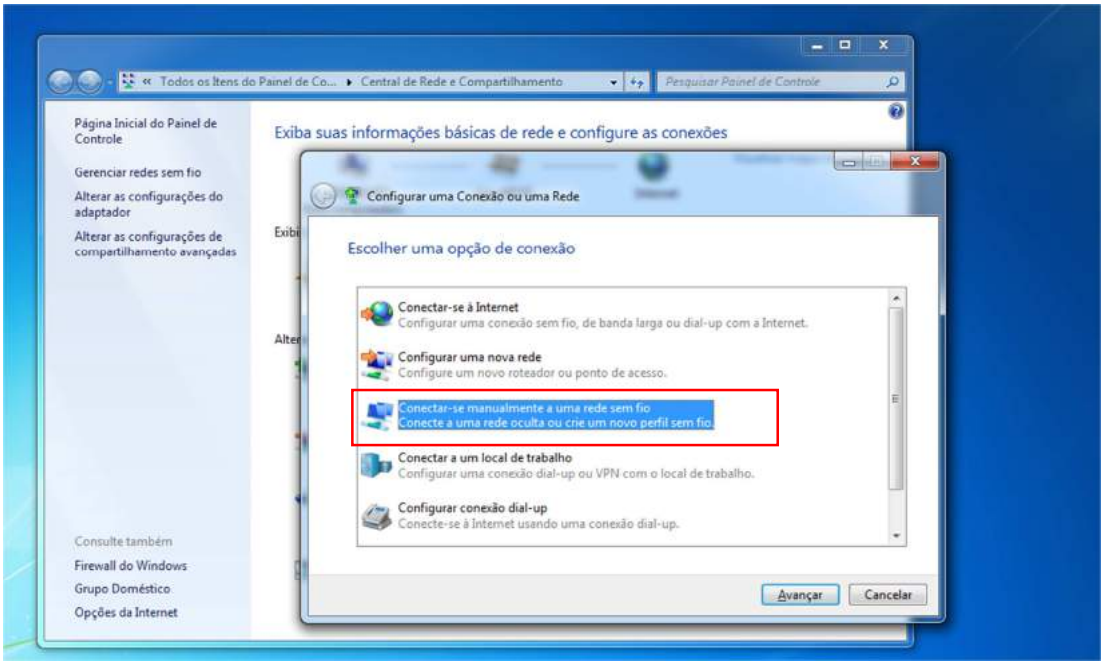

Imagem 137: Criando uma rede sem fio manualmente

Colocaremos o nome da nossa rede (*Levy AP*), o tipo de segurança *WPA2-Enterprise*, e criptografia *AES*.

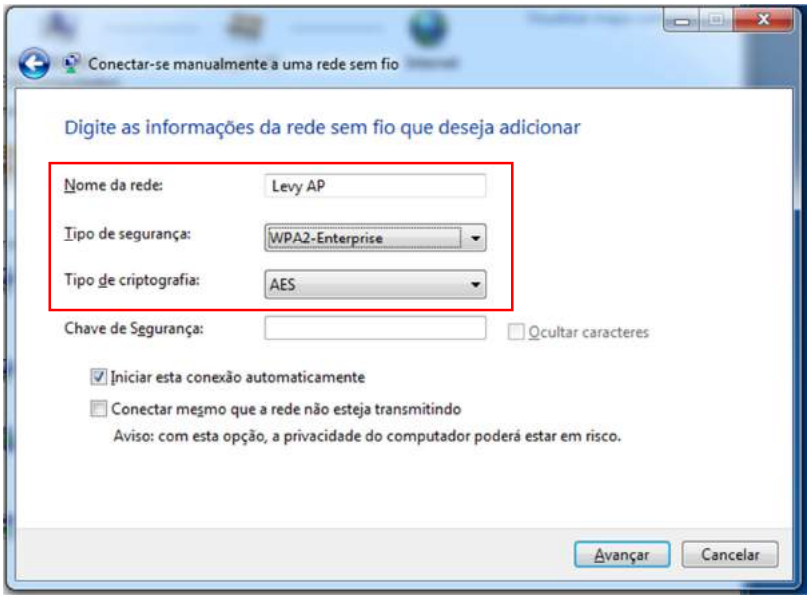

Imagem 138: Criando uma rede sem fio manualmente

Depois de criada a rede iremos alterar as configurações de conexão.

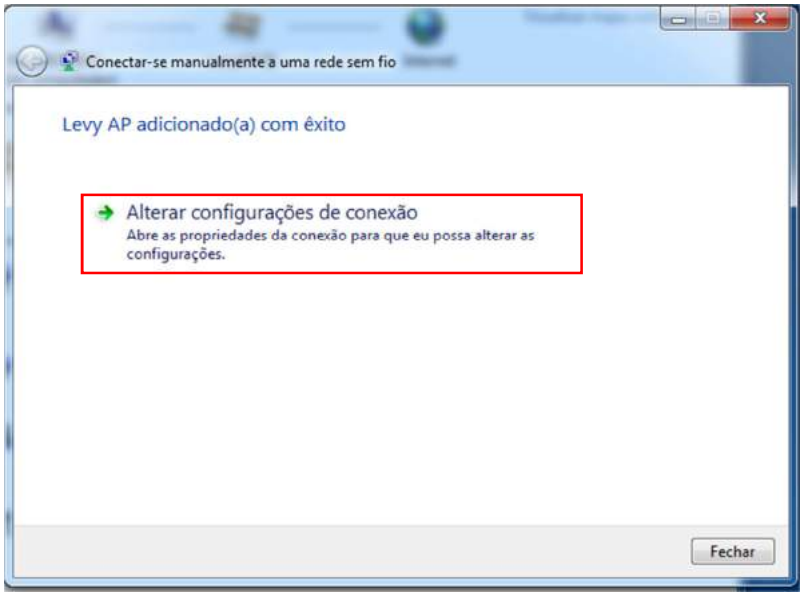

Imagem 139: Configurando uma rede sem fio criada manualmente

Agora clicaremos na aba **Segurança** e iremos alterar o método de autenticação de rede para *Cisco:PEAP*, e logo após clicaremos em *Configurações*.

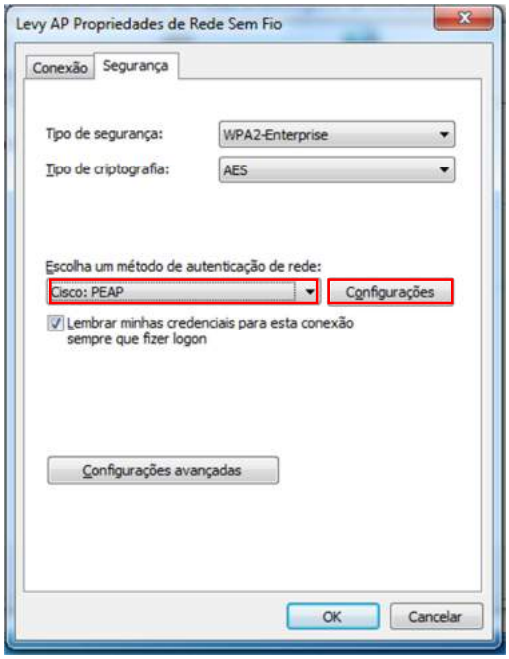

Imagem 140: Configurando a segurança uma rede sem fio criada manualmente

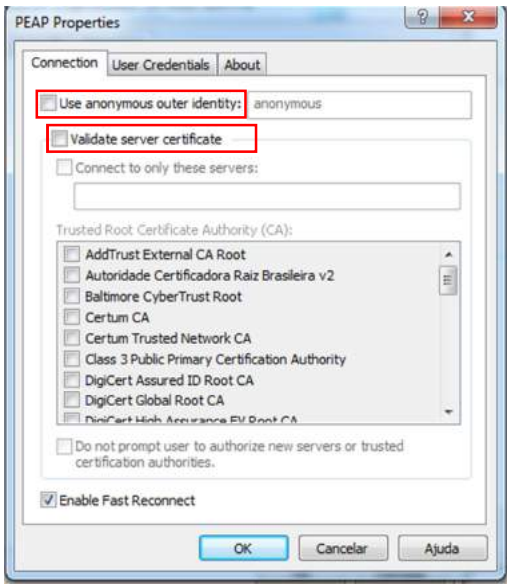

Imagem 141: Configurando a segurança do Protocolo PEAP

Conforme mostra a Imagem141 devemos desmarcar as opções "*Use anonymous outer identity*" e "*Validate Server Certificate"*.

Após isso devemos clicar na aba **User Credentials**, escolher a opção "*Use saved username and password*" e digitar as credenciais do usuário criado em nosso MySQL-Server no capítulo 4.4.2.

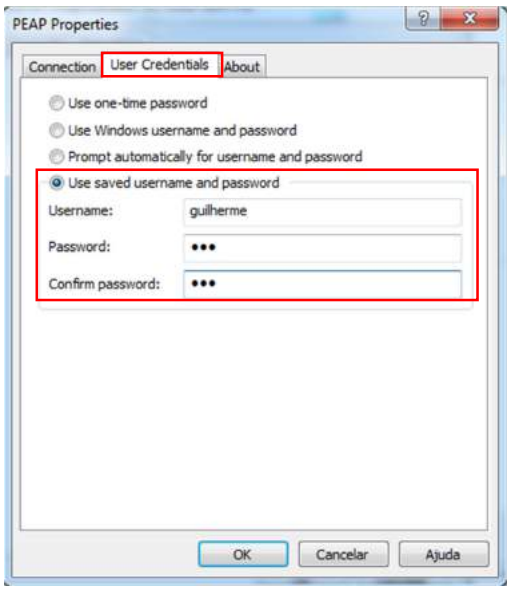

Imagem 142: Configurando as credenciais de usuário

Após essa configuração das credenciais basta confirmarmos. Nosso dispositivo está com a rede configurada.

4.7. FINALIZANDO E TESTANDO O FREERADIUS

ATENÇÃO: Antes de prosseguir com o teste final de funcionamento do Freeradius devemos reiniciar o nosso servidor Debian.

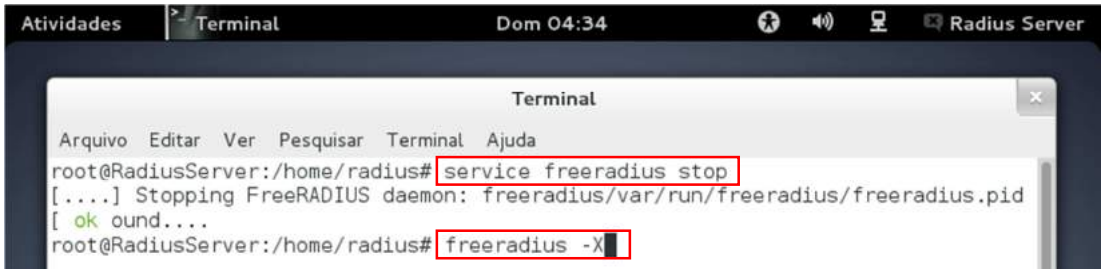

Imagem 143: Finalizando e testando o Freeradius

Após o microcomputador reiniciar já podemos fazer o teste final e verificar se ele já se encontra em funcionamento, recebendo as solicitações dos access points e liberando a conexão à rede **Levy AP** aos usuários cadastrados no banco de dados MySQL.

Conforme mostra a Imagem143 utilizaremos o comando *service freeradius stop* para parar o serviço Freeradius e logo em seguida iniciaremos o serviço Freeradius em seu modo de depuração utilizando o comando freeradius -X.

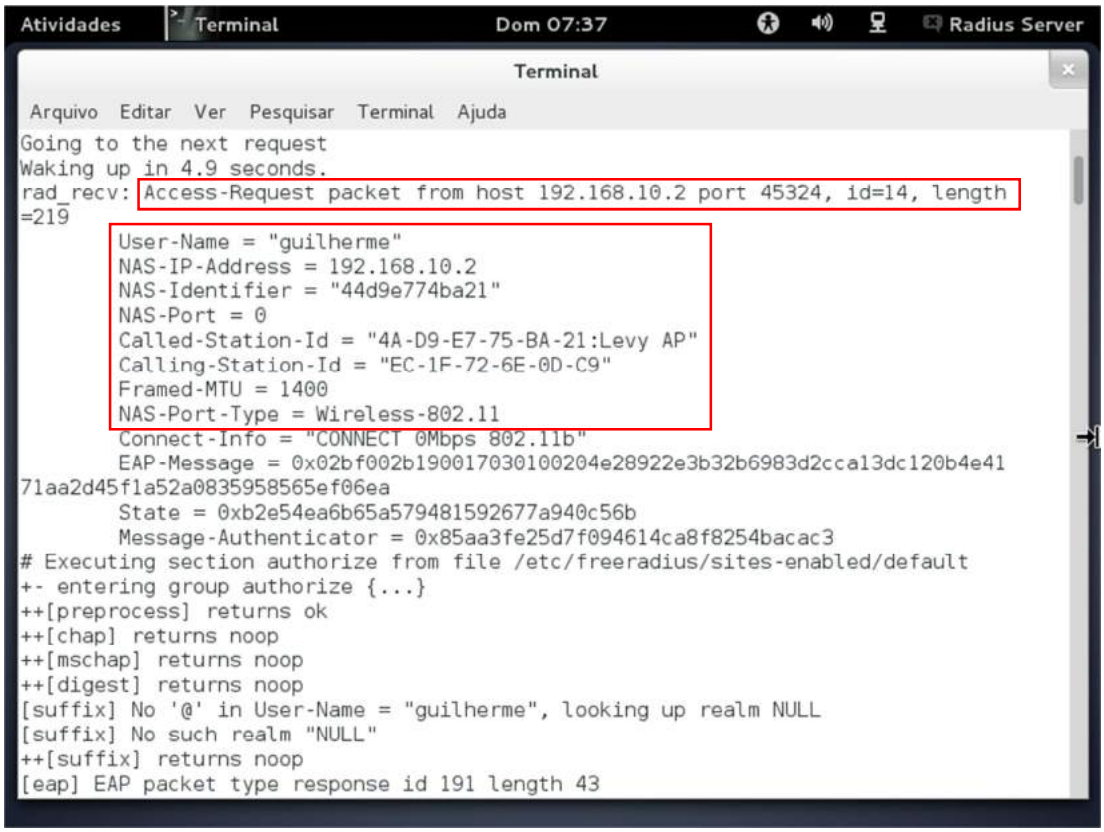

Imagem 144: Freeradius recebendo a requisição

Conforme podemos verificar na imagem acima o Freeradius recebeu um pacote de requisição do **host** *192.168.10.2* (endereço de IP do AP), essa requisição era do **User-Name** *guilherme* (inserido pelo usuário ao tentar conectar-se na rede), pelo campo **NAS-IP-Address** e **NAS-Identifier** podemos identificar que foi tentado a conexão através do access point *UAP01.*

Através do campo **Calling-Station-Id** (endereço MAC do dispositivo que tentou a conexão na rede) podemos criar usuários vinculando o usuário ao endereço MAC do seu dispositivo.

Como mostra a imagem abaixo, após a consulta dos dados contidos no pacote de requisição enviado pelo access point no banco de dados podemos ver que o Freeradius retorna com um **OK** ao AP, fazendo com que o access point UAP01 libere ao dispositivo o acesso à rede **Levy AP.**

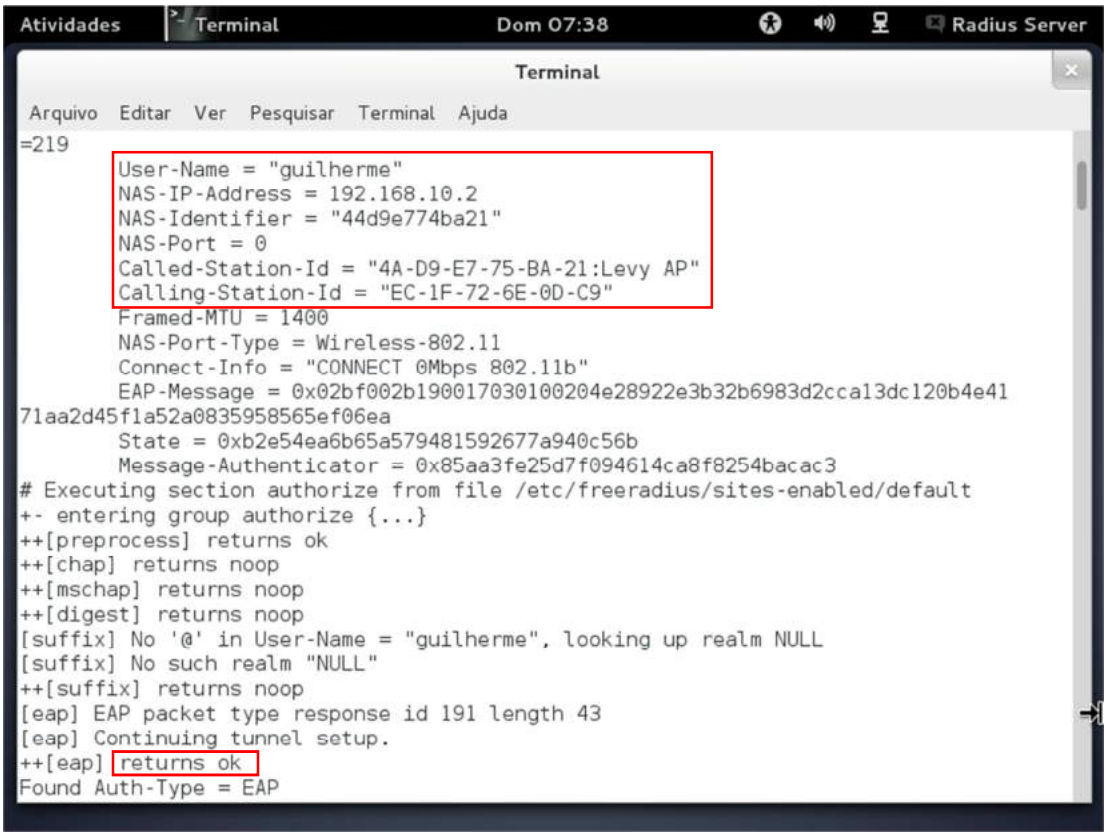

Imagem 145: Freeradius aceitando a requisição

O sistema esta funcionando...

5. CONSIDERAÇÕES FINAIS

Esse manual se propôs, como objetivo principal, elaborar um conjunto de regras e procedimentos para facilitar a criação e configuração de uma rede em uma Routerboard Mikrotik com RouterOs, configuração dos access points Ubiquiti Unifi, configuração de um servidor Debian 7.4, instalação e configuração de um servidor Freeradius autenticando em um banco de dados MySQL de um modo correto e otimizado, e assim, oferecer condições de utilização adequada dessa rede wi-fi, trazendo mais segurança e desempenho aos usuários e ao administrador.

Espero que esse manual ajude e potencialize o processo de criação e configuração do sistema.

GUILHERME LEVY

ti@guairaca.com.br

6. REFERÊNCIAS

LEVY, Guilherme. Manual para criação e configuração de um servidor Hotspot no sistema operacional RouterOS utilizando uma Routerboard Mikrotik. Trabalho de conclusão de curso de graduação em Tecnologia em Análise e Desenvolvimento de Sistemas, páginas 1 – 77, Faculdade Guairacá, Set 2015.

MIKROTIK.com. Site Oficial
Disponível em: http://www.mikrotik.com/pdf/what_is_routeros.pdf/> Acesso em 07 Out. 2017 às 14:34.

MIKROTIK Documentation.
Disponível em: http://wiki.mikrotik.com/wiki/Main_Page/> Acesso em 07 Out. 2017 às 18:48.

UBNT.com Site Oficial
Disponível em: https://www.ubnt.com/> Acesso em 08 Out. 2017 às 20:33.

Imagem cabeçalho 01

[1]

Imagem cabeçalho 02

[2]

[1]Disponível em: https://aacable.wordpress.com/tag/freeradius/;. Acesso em 08 Out. 2017.
[2]Disponível em: https://www.wifimedia.eu/en/ubiquiti-unifi-ap-ac-pro.html;. Acesso em 08 Out. 2017.

Imagem cabeçalho 03

[3]

Imagem cabeçalho 04

[4]

Imagem cabeçalho 05

[5]

Imagem 06

[6]

[3]Disponível em: http://www.academiamt.com.br/loja/licenca-mikrotik/licenca-mikrotik-routeros-level-4/;. Acesso em 08 Out. 2017.
[4]Disponível em: https://planet.phpmyadmin.net/;. Acesso em 15 Out. 2017.
[5]Disponível em: http://e-tinet.com/linux/debian-gnu-linux/;. Acesso em 16 Out. 2017.
[6]Disponível em: https://www.ubnt.com/;. Acesso em 08 Out. 2017.