INSTITUTO POLITÉCNICO DE BEJA

Escola Superior de Tecnologia e Gestão

Projeto redes de computadores 2

Trabalho individual de avaliação

Elaborado por:

Hugo Silva Nº 18544

Docente:

Armando Ventura

Beja, 17/06/2020

Índice

Lista de Figuras

1. Introdução

Neste trabalho pretende-se a elaboração de um projeto que visa a implementação de conhecimentos obtidos nas aulas de Redes de Computadores 2, com intuito de criar uma rede com dois routers mickotik, um router cisco, dois switch e duas maquinas clientes com sistema operativo.

O projeto consiste na realização e implementação de uma rede local, segura, com acesso restrito, juntamente com ligação por cabo UTP e GNS3.

A rede terá instalado um router mikrotik com firewall ativa para apenas permitir as comunicações da “máquina virtual cliente 2” só pode aceder ao exterior à Internet ao site do portal das finanças “https://www.portaldasfinancas.gov.pt/”, tudo o resto é negado.

Será necessário também que “máquina virtual cliente 2” acede por telnet ao router “R3” a. Introduza password “proj” ao acesso por telnet ao router e modo privilegiado.

Efetuar-se-á a configuração de um servidor DHCP para a rede local no router mikrotik com a gama de IPs:

RedeA -> Endereço de Rede: F.20.20.0/30

RedeB -> Endereço de Rede: F.21.20.0/30

RedeC -> Endereço de Rede: 172.F.1.0/30

RedeD -> Endereço de Rede: F.22.20.0/24.

O F citado acima será calculado da seguinte forma:

F = resto da divisão inteira do número de aluno a dividir por 100 + 10

F = (Nºaluno % 100) + 10

A saber 18544%100 = 44 + 10 = 54, (cinquenta e quatro o numero a ser utlizado).

Para testar tudo iremos precisar de duas máquina virtual cliente para aceder à internet através da rede local que criamos, o GNS3, WinBox, RoutresOS da microtik, router cisco.

Abaixo demonstro as máquinas virtuais criadas e a topologia proposta pelo professor no enunciado do trabalho.

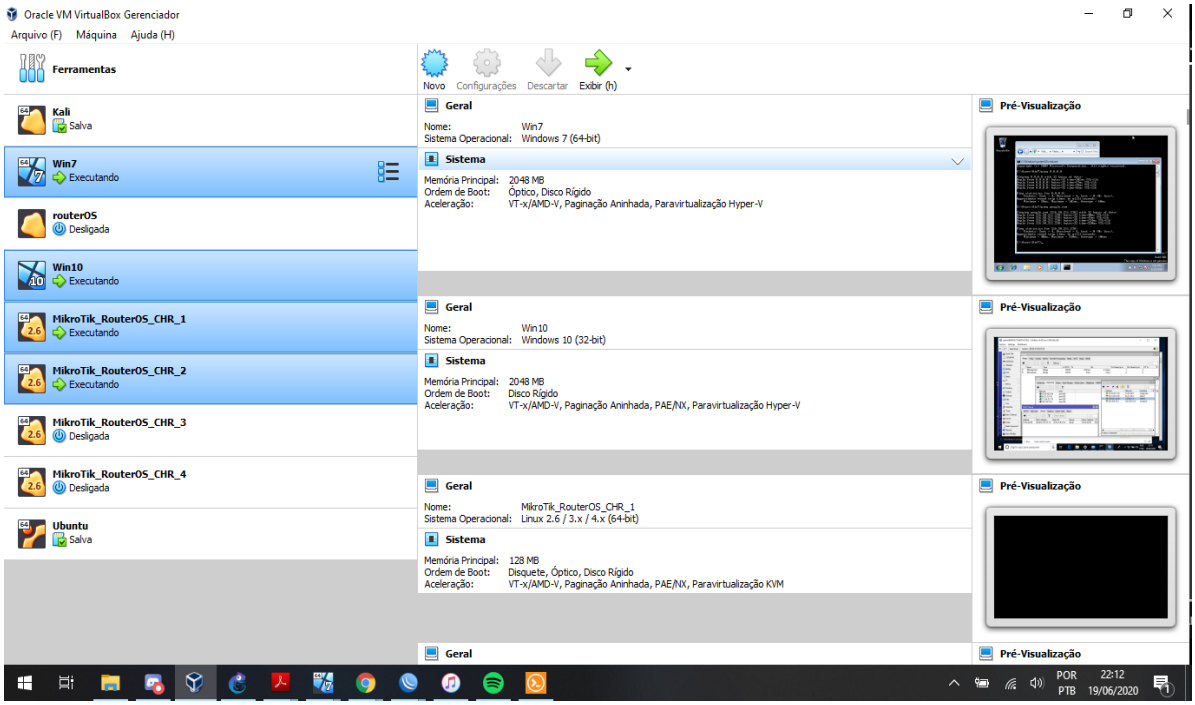

Figura 1 – Máquinas Virtuais

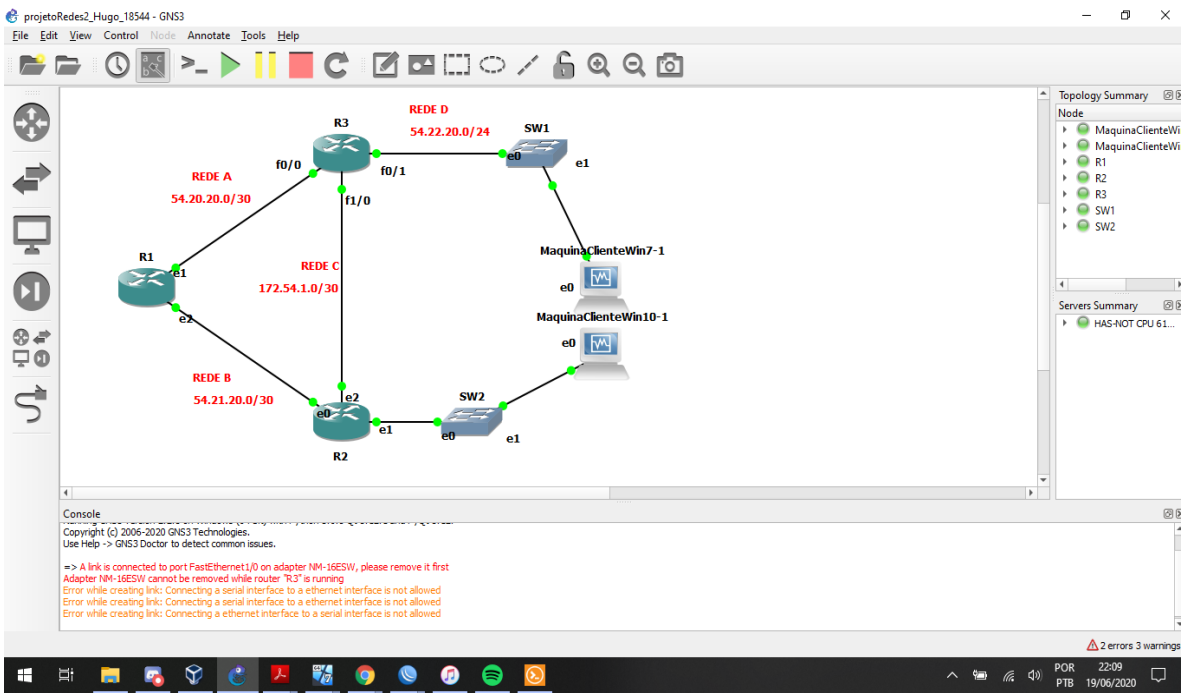

Figura 2 – Topologia da rede local no GNS3

2. Realização das Tarefas

2.1. Configuração de servidor DHCP

Depois de todas as máquinas virtuais terem sido corretamente instaladas e colocadas na topologia, começa-se por fazer download na máquina cliente do *software* “winbox” para se poder configurar o router *mikrotik* e assim criar o servidor DHCP e o resto das opções para que a máquina cliente possa ter acesso à internet e ao mesmo tempo.

A saber as configurações das maquinas:

Observações sobre Router “R1”

O router “R1” a interface WAN(ether1) deverá estar em modo bridge ou NAT (residência em NAT) no virtualbox, ether2 e ether3 em modo “generic driver” no virtualbox.

• A interface WAN(ether1) deverá estar em dhcp–cliente

Observações sobre Router “R2”

O router “R2” deverá ter todas as suas interfaces (ether1,ether2 e ether3) em modo “generic driver” no virtualbox.

• A interface ether3 deverá estar com o dhcp server configurado (range 10.54.40.10 <-> 10.54.40.50)

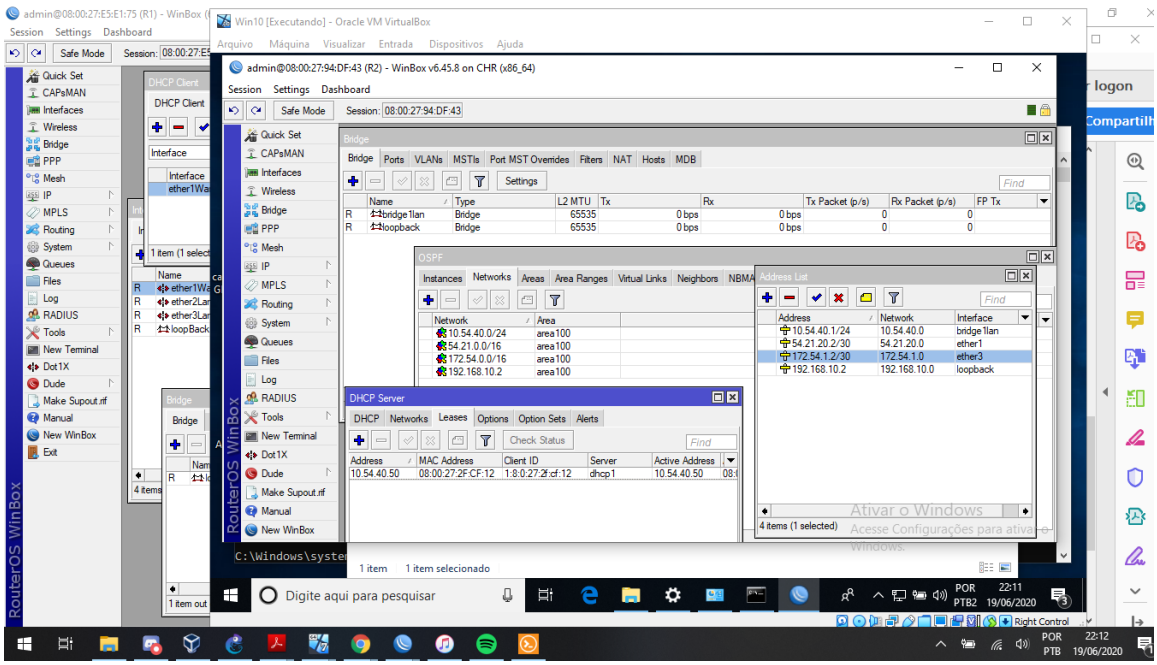

Figura 3 – Configuração R2 - Microtik

Com o *software winbox* iremos fazer uma ligação ao router *mikrotik* a partir da máquina cliente com o sistema operacional, Windows 10, para que consigamos configurar o servidor DHCP e as restantes opções necessárias para ter acesso à rede.

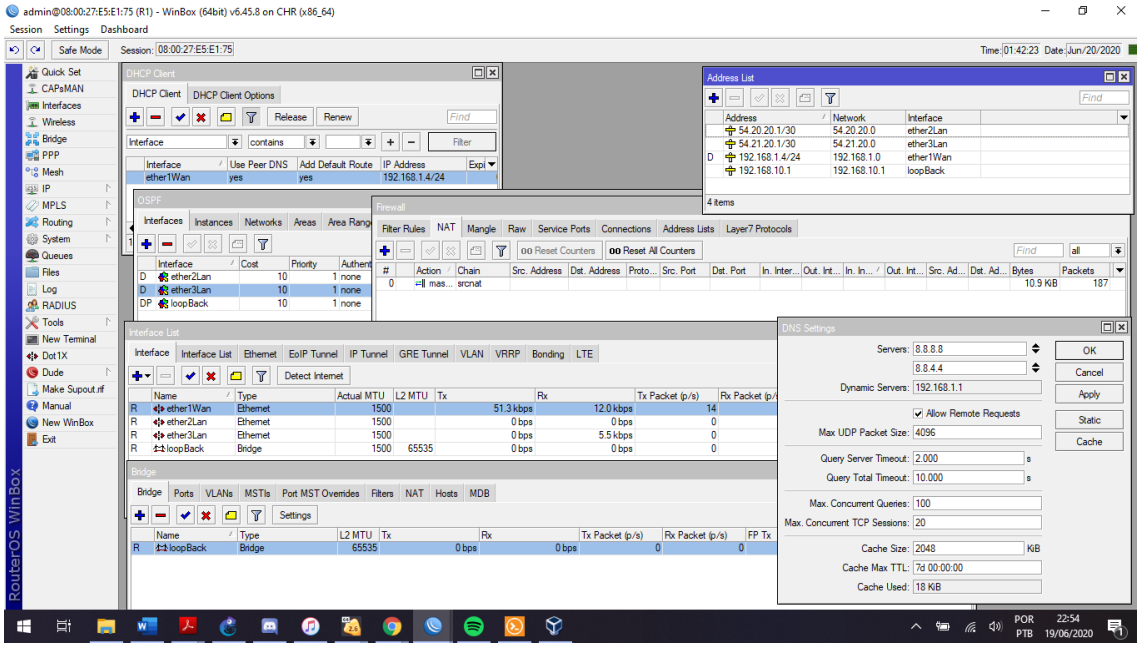

Figura 4 – Configuração R1 - Microtik

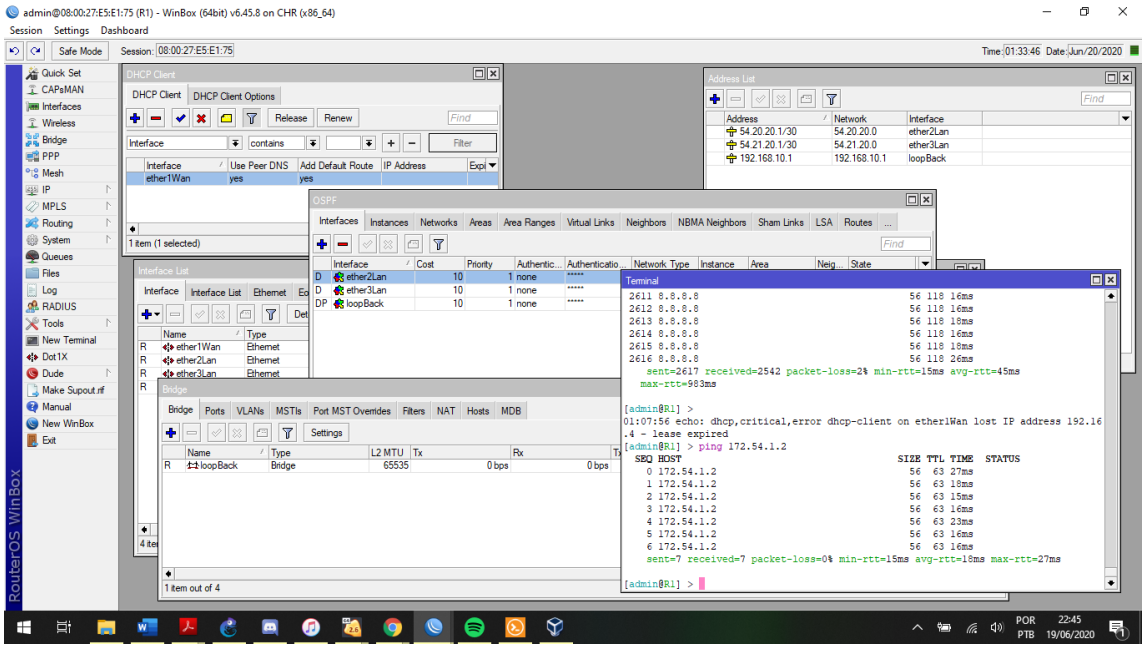

Figura 5 – pingando externo e interno – R1

Configurado o encaminhamento OSPF para toda a topologia, incluindo mikrotik e cisco. Como demonstrado nas imagens acima a configuração deve ser

realizada nos três routers para que pudessem operar com os protocolos IP, onde OSPF é um protocolo de roteamento para redes que operam com protocolo IP, sendo necessário para a comunicação e transferência.

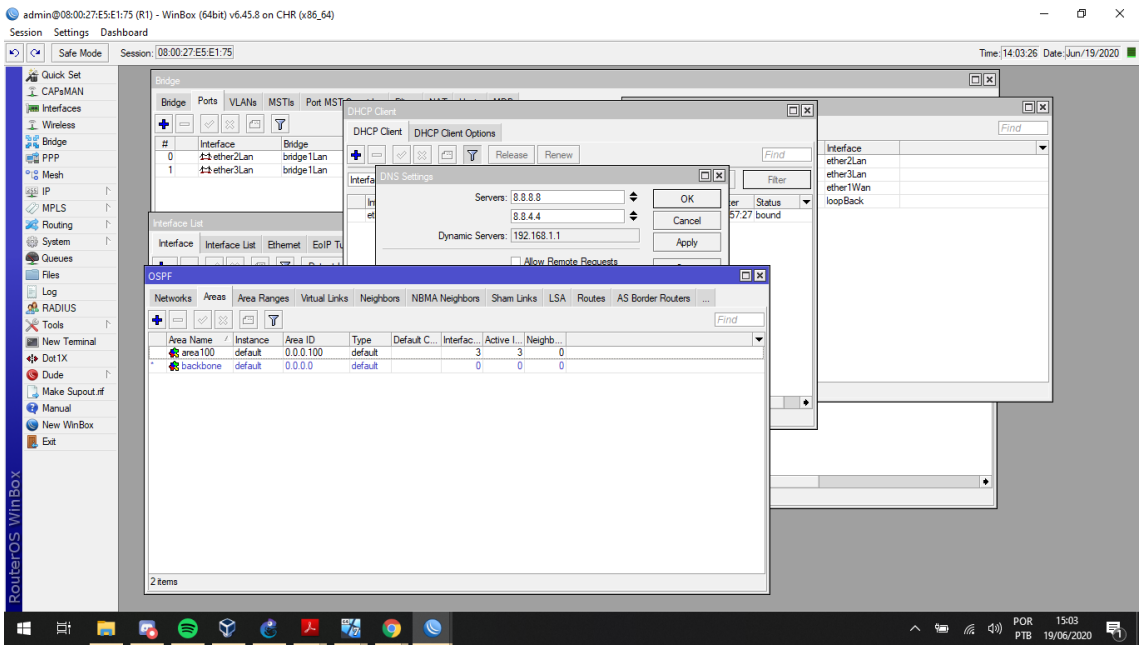

Figura 6 – configuração2 – R1

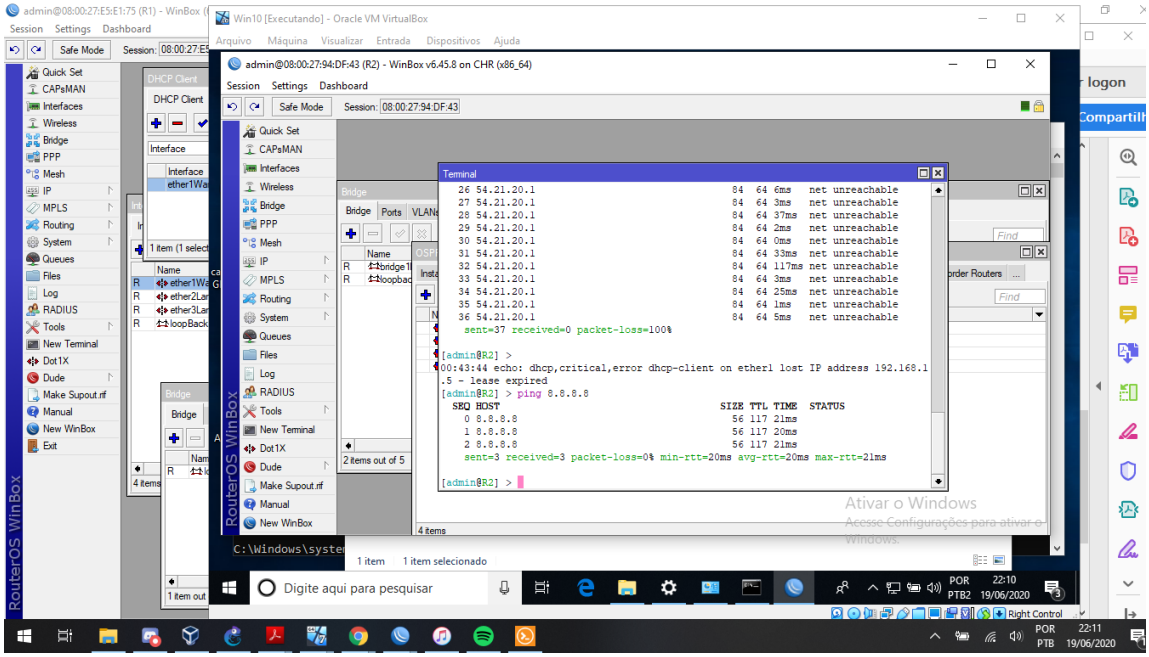

Figura 7 – pingando para externo – R2

Para configurar o servidor DHCP, é preciso usar o endereço MAC da interface ligada do router *mikrotik* à maquina cliente para ela conseguir conectar-se à configuração do router a partir do *winbox*, caso não ocorra a comunição podemos temporariamente, colocar a ether1 como “bridge” para configurar o R2

e assim posteriormente efetuar a configuração e ao concluir voltando a mesma para “genericDriver”. Na figura 3, já se encontra o endereço IP do *router*, a faixa do DHCP, password, loopback, que por defeito precisamos configurar para efetuar a coneção não apenas interna mas externa, configurado o servidor DHCP as maquina relacionadas a ele já receberam as devidas configurações e acesso a rede interna e externa.

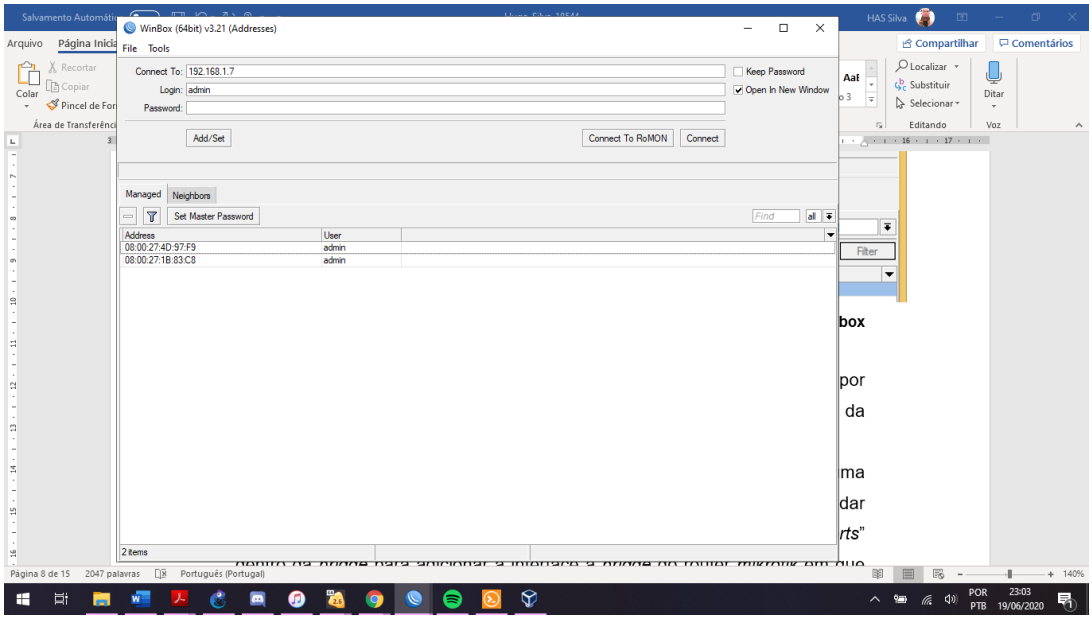

Figura 8 – Winbox

Antes de tudo, iremos mudar a password de acesso ao router *mikrotik* por indo à opção “*system*” e em seguida “Password” para se alterar a password da login ‘admin’ do router.

Depois na opção “*bridge*” que irá abrir uma janela, vai-se adicionar uma nova *loopback*, para tal não é preciso de muito apenas clicar no adicionar e de dar o seu nome. Se fosse uma “bridge” era necessário ir à página das “*ports*” dentro da *bridge* para adicionar a interface à *bridge* do router *mikrotik* em que está ligada à máquina cliente.

Em seguida será criada a gama de IPs para que se irá usar no servidor DHCP, no caso será efetuada apenas no R2 e para isso vamos à opção “IP” e depois “Addresses” onde se pode adicionar a gama de IPs pedida pelo profesor no enunciado, como se pode reparar na imagem 3.

Tendo já o cliente DHCP vindo do routers R2, não será necessário efetuar IP’s fixos as maquinas clientes e podemos fazer através do “DHCP *Server*” para termos acesso à internet na máquina cliente. Para tal é carregar na opção “DHCP *Setup*” da janela aberta para começar a criar, escolhe-se a interface *bridge*,

depois disso é só fazer *next* pois se estiver tudo corretamente feito, não haverá complicações na criação do DHCP.

Finalmente para concluir tudo isto e finalmente ter acesso à internet basta ir só mais uma vez à opção “IP”, mas neste caso depois à opção “Firewall” para adicionarmos uma nova regra na página “NAT” da janela aberta, a única opção que alteramos no *menu* aberto será na página “*Action*” mudamos a *action* para ‘*masquerade*’.

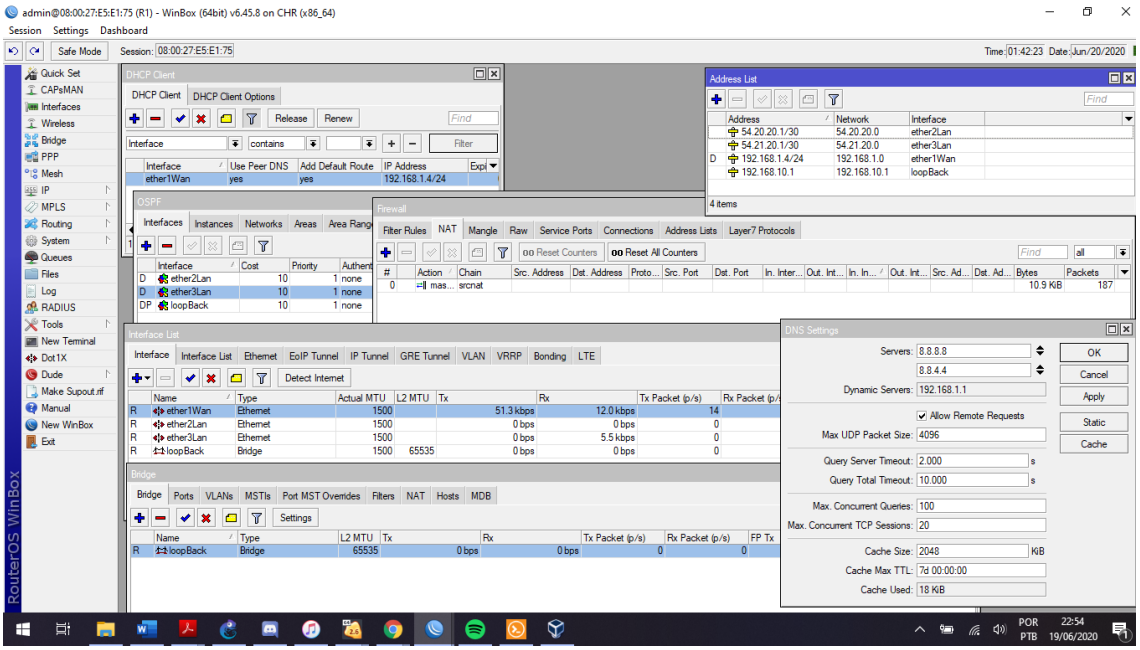

Figura 9 – Demosntrando Masquered, ospf e dns

Estando tudo concluído podemos ver o fruto do nosso trabalho nas imagens 5 e 7, que como se pode ver temos os routers com acesso à internet e com um endereço da gama de IPs pedida pelo professor no enuciado.

Após a etapa dos routres concluída, podemos efetuar o teste de ping pelas máquinas, a maquina cliente Win7 esta tendo acesso pelo router da cisco e a cliente Win10 esta tendo acesso pelo router R2e ambas obtem a resolução do DNS como podemos ver nas imagens 10 e 11, onde os pings ocorrem por IP como nome.

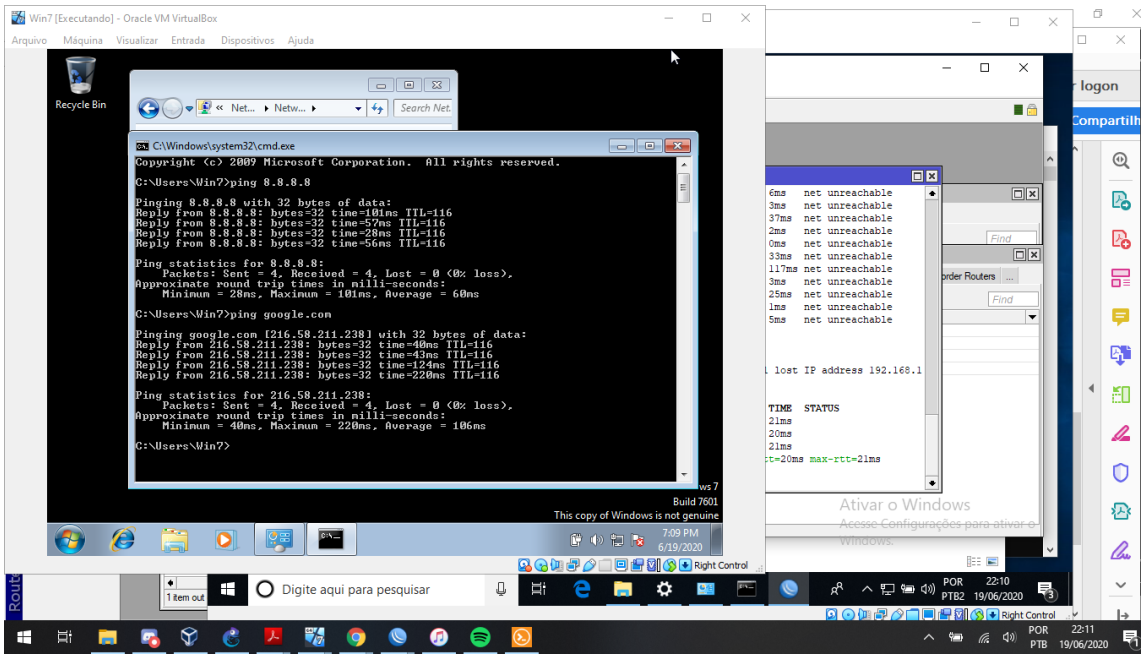

Figura 10 - Máquina cliente com acesso à internet pelo R3

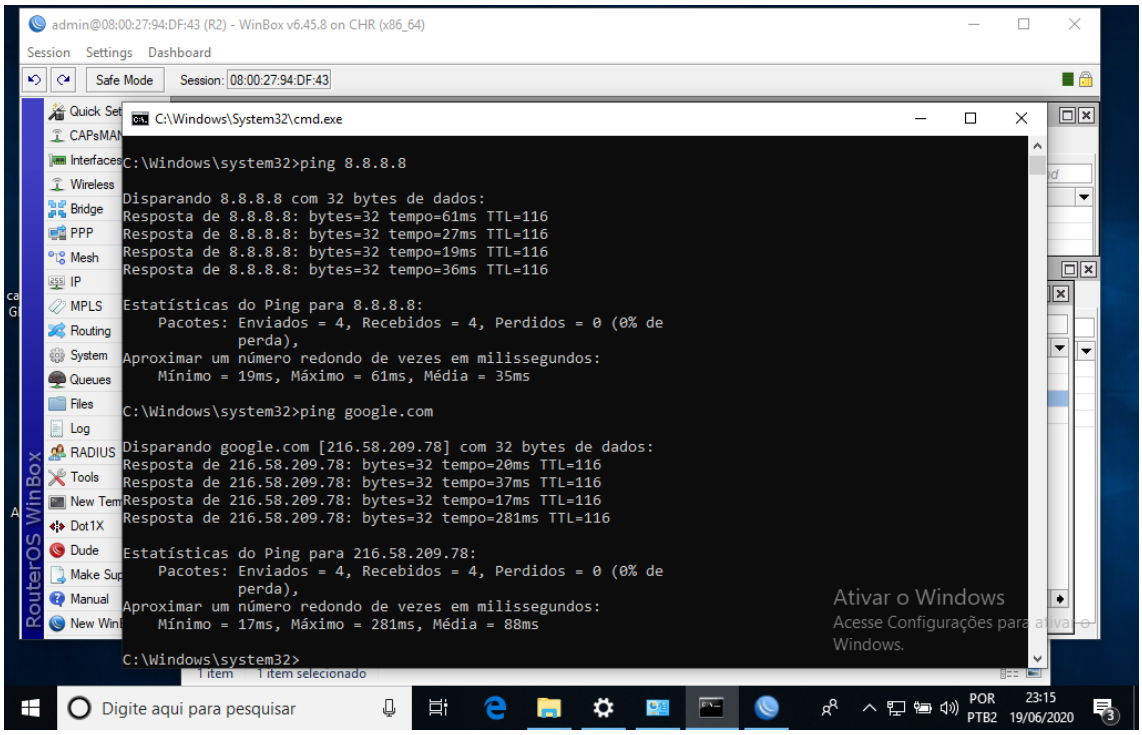

Figura 11 - Máquina cliente com acesso à internet pelo R2

A configuração através do terminal para o router da cisco, ocorre no proprio GNS3, podendo apenas clicar com o botão direito do mouse e ir em “console”, neste caso através de linhas de comando, como exemplo: “ip address ...”, “router ospf ...”, “interface fastethernet ...”, podemos configurar o router com as

informações para cada interface com os seus devidos IP's, a gama do OSPF e network, podemos ver que ambas as máquinas clientes obtem a resolução do DNS através das imagens 10 e 11, onde os pings ocorrem por IP como nome e as linhas de comando para configuração do R3 cisco nas imagens 12 e 13.

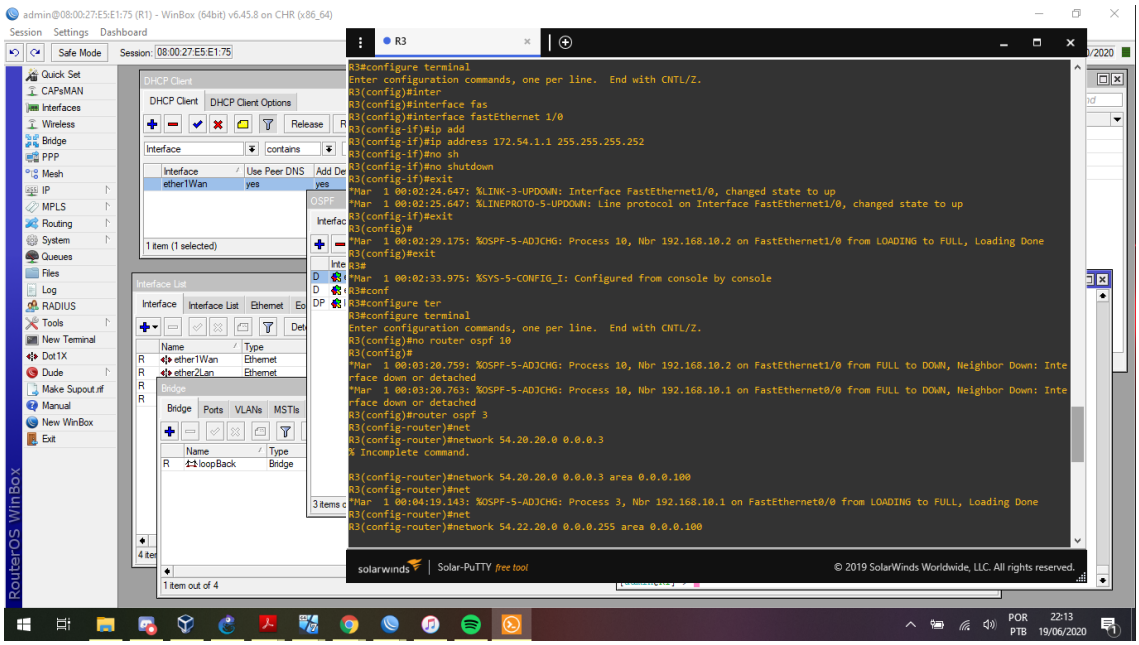

Figura 12 - configuração R3 - Cisco

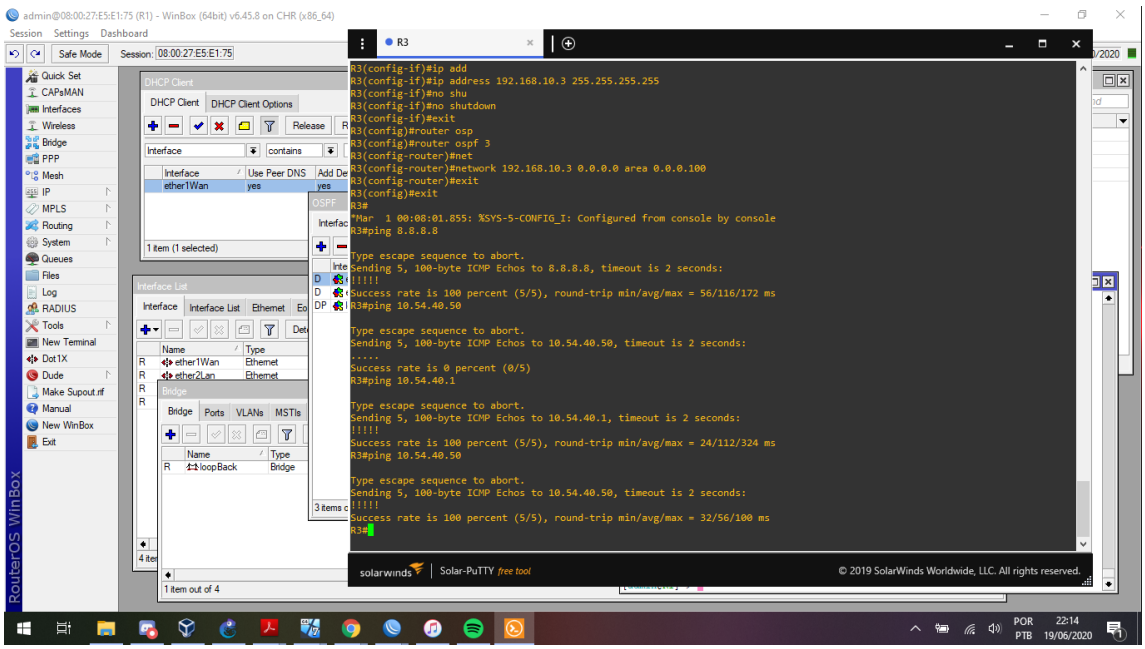

Figura 13 – Configuração R3 parte 2 - Cisco

2.2. Gestão de conteúdos

Ao ter acesso à internet com a máquina instalada, podemos começar a gerir o conteúdo que pode passar por ela e chegar à nossa máquina cliente, como por exemplo bloquear certos websites, IP's e até criar divisão com Vlan's para obter mais segurança quanto a informação trafegada. Como por exemplo
A "máquina virtual cliente 2" só pode aceder ao exterior à Internet ao site do portal das finanças "https://www.portaldasfinancas.gov.pt/", tudo o resto é negado.

Primeiramente Firewall é o nome dado ao dispositivo de uma rede de computadores que tem por objetivo aplicar uma política de segurança a um determinado ponto de controle da rede.

1. As regras de Firewall são sempre processadas por cadeia, na ordem que são listadas, ou seja, de cima para baixo.

2. As regras de fi rewall funcionam como em programação (expressões condicionais, "se <condição> então <ação>").

3. Se um pacote não atende TODAS as condições de uma regra, ele passa para a regra seguinte.

4. Quando o pacote atende a TODAS as condições da regra é formada uma ação com ele, não importando as regras que estejam abaixo dessa cadeia, pois NÃO serão processadas.

5. Existem algumas exceções ao crédito acima, que são as ações de "passthrougth" (passar adiante), log e add to address list.

6. Um pacote que não se enquadre em qualquer regra da cadeia, será por default aceito.

Tendo entrado na opção de criar um novo *service group*, vamos de chamar este novo grupo de 'DNS' e iremos adicionar ambas portas 53 (DNS) dos protocolos TCP e UDP no *service group*. Em seguida iremos à opção "Firewall *Rules*" que se consegue ver na figura 5, e vamos adicionar uma regra nova.

Nesta regra escolhemos como ponto de origem comunicações vindas da nossa rede local e como destino para fora da rede e para a *cloud* (internet), iremos usar o *service group* criado que contém as portas 53 dos protocolos TCP e UDP. No final obrigamos a rejeitar qualquer pacote que esteja a usar essas

portas de ambos os protocolos, isto será necessário para o funcionamento do próximo passo.

Para realizar-se a gestão de conteúdos será usada uma proxy, por isso era necessário bloquear todos os outros DNSs para não entrar em conflito com que iremos fazer agora a seguir. Começa-se por ir desta vez à sub-opção “Web Proxy” da opção “*Network*”, depois um bocado mais abaixo vai-se à opção “URL filter” para editar-se dos quais links serão bloqueados da máquina cliente e ativa-se também essa lista agora criada.

Exemplo:

Para serviços autorizados.

add chain=input protocol=icmp action=accept \ comment=”Permite ICMP”

add chain=input src-address=192.168.0.0/24 action=accept \ in-nterface=!ether1

add chain=input action=drop comment=”Ignora todo o restante”

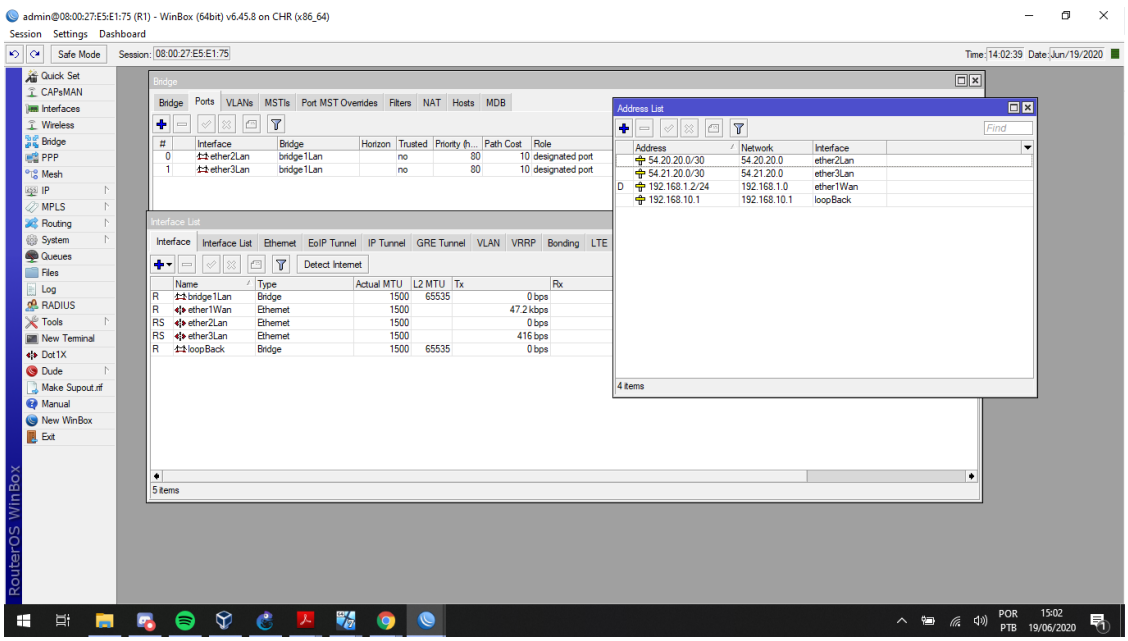

Figura 14 – Configuração R2 e R1

2.3. Ativação da firewall no *mikrotik*

Para fazer como é pedido no enunciado, e bloquear todas as comunicações exceto as que são feitas a partir das portas 80 e 443, e ao mesmo tempo permitir as comunicações do protocolo ICMP para testes de acesso à internet, apenas é necessário de voltar ao *software winbox* e na opção “Firewall” dentro da opção “IP” tem que se ir à página “*Filter Rules”* e adicionar as regras que possibilitam a

ligação das portas 80 e 443, mais o protocolo ICMP e ao mesmo tempo bloquear todas as outras comunicações. Estas regras podem ser adicionadas pelo *winbox* mas também podem ser adicionadas diretamente pela máquina virtual do router *mikrotik* como foi feito neste caso e pode-se ver os comandos utilizados para as criar na figura 9, todos os comandos tem descrição exceto o último que simplesmente bloqueia todas as comunicações.

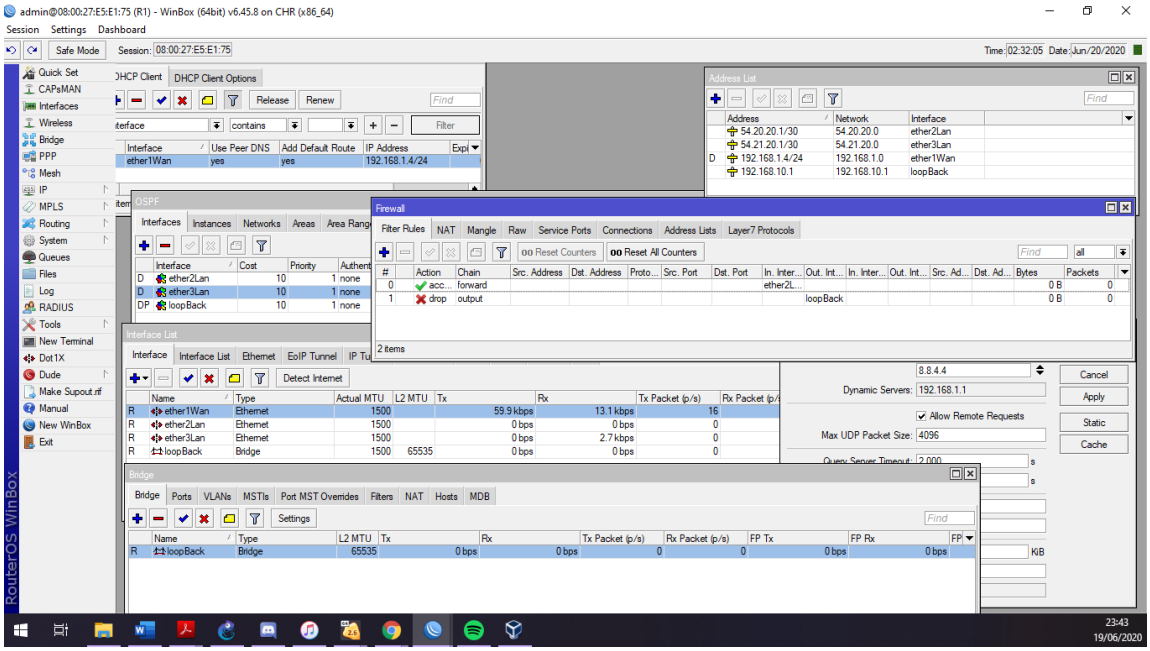

Figura 15 – Configuração R1 firewall

Como já está tudo pronto ser utilizada, basta ir ao painel de controlo e escrever na barra de pesquisa para encontrar as opções da internet, onde se pode configurar indo dentro das definições da proxy, na “Definições de LAN” e ativar a caixa em que ativa o servidor proxy para a rede local. Na figura 8 pode-se ver os sites bloqueados.

Foi necessário criar regras em que permitiam as portas 444 e 800, pois em elas não conseguiríamos aceder à configuração do IPFire e nem poderíamos usar a proxy que se encontra na porta 800.

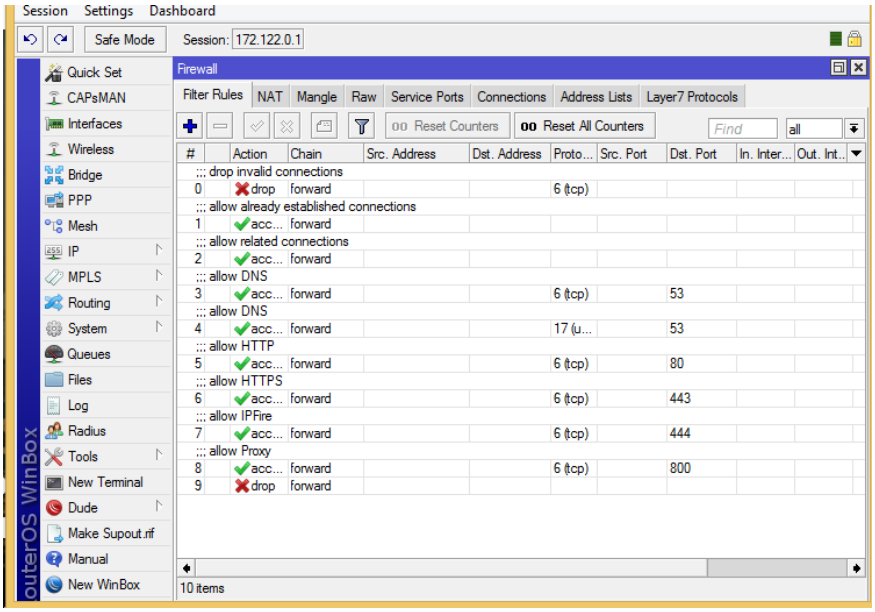

Figura 16 - Teste de acesso à internet com regras de acesso

3. Conclusão

Com a realização deste projeto e o seu relatório, foi adquerido o conhecimento de como instalar e usar routers da cisco e mickotik, além de regras de firewall e gestão de informações em rede de dados.

Foi também aprendido de como configurar um router *mikrotik* a partir do *software winbox* e criar um servidor DHCP para fornecer endereços IP ás máquinas ligadas ao routere ao mesmo tempo fornecer internet a tais máquinas. Por fim foi ainda adquirido o conhecimento de criação de regras de firewall no router *mikrotik,* em que podemos permitir e bloquear pacotes específicos de passarem pela rede.