Parte 1: Procedimento de configuração para acessar remotamente as ONTs 142N W, 121 W em OLT sem CPE-manager

1) Descrição

Mesmo que a OLT não forneça uma função para gerenciar remotamente as CPEs tal como a função CPE-manager, continua sendo possível acessar as ONTs via telnet ou web remotamente ao configurar uma VLAN específica na interface WAN da ONT. Também é possível acessar as ONTs a partir da internet desde que seja criado regras de redirecionamento de portas no roteador. As ONTs 142N W e 121 W, saem de fábrica pré-configuradas para o prover acesso remoto através VLAN 7. Este tutorial tem o objetivo descrever como ativar estes recursos em uma rede com o roteador Routerboard Mikrotik e OLT FiberHome.
Para prover gerenciamento remoto das ONTs intelbras em qualquer outra OLT, siga as dicas do item 3.
A topologia da rede de acesso via rede local é ilustrado na figura 1 e via rede externa (internet) na figura 19. Os passos descritos na parte 1 referem-se as configurações essenciais no roteador mikrotik, ONT e OLT para acessar as ONTs via a rede local e externa. Na parte 2 é referente a criação das regras NAT e liberação de portas para prover o acesso externo às ONTs.

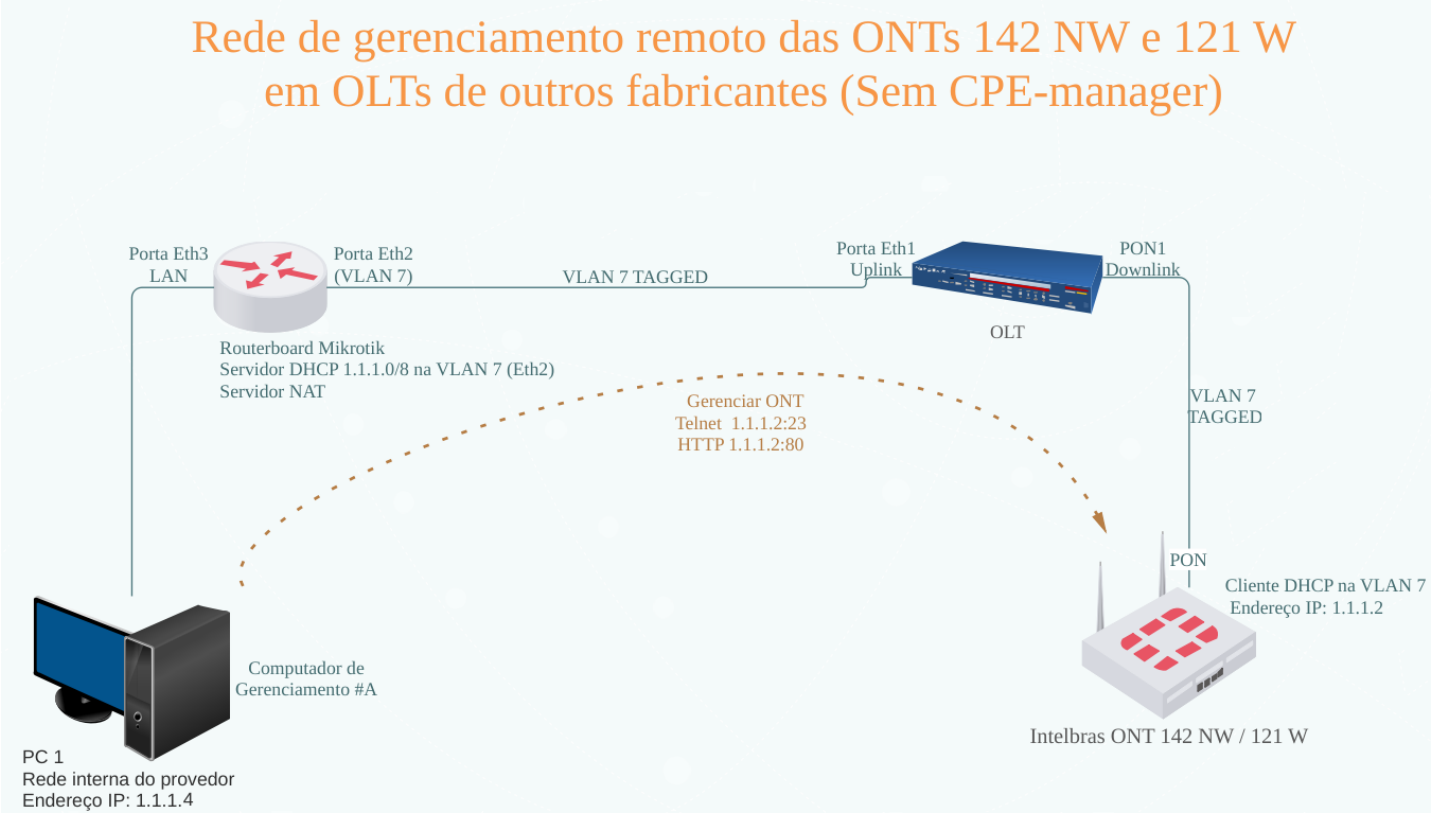


Figura 1 - Topologia da rede de acesso remoto a partir da rede local do provedor

2) Objetivo

Prover acesso remoto para gerenciamento das ONTs Intelbras a partir da rede local em OLTs que não possuem a função CPE-manager.

3) Resumo do procedimento

Configuração a ser realizada na OLT:

Passo 1: Criar uma VLAN 7 tagged do tipo Downlink e atribuí-la na porta PON da OLT conectado a ONT Intelbras que queira acessar remotamente;
Passo 2: Definir uma porta uplink na OLT para ser destinada a bridge de gerenciamento;
Passo 3: Criar uma VLAN 7 tagged do tipo uplink e atribuí-la à porta de gerenciamento definida no **passo 2** e conecte ao roteador Mikrotik;

Configuração no roteador Mikrotik:

Passo 4: Criar uma VLAN 7 tagged e atribuí-la à interface de rede conectada à porta de gerenciamento da OLT;
Passo 5: Criar uma bridge de gerenciamento e inclua na aba *ports* a VLAN 7 criada e a porta do mikrotik que será destinada ao computador que gerenciará as ONTs;
Passo 6: Adicionar em *AddressList* o endereço de rede 1.1.1.254/8 e na aba interface atribua a bridge de gerenciamento criada no passo anterior;
Passo 7: Criar uma *pool* de endereço IPv4 na rede 1.1.1.0/8;
Passo 8: Criar um servidor DHCP e selecionar a bridge de gerenciamento criada. Se estiver configurando o roteador mikrotik via winbox, assim que concluir estas configurações, poderá listar as ONT na rede gerenciamento através do menu ***IP>DHCP Server>Leases*** e acessar via telnet pelo menu ***Tools->Telnet*** para acessar a ONT ou através de um computador conectado na porta do mikrotik que incluído na bridge de gerenciamento das ONTs.

4) Detalhamento da configuração de acesso remoto na ONTs 142N W e 121 W em Routerboard Mikrotik e OLT FiberHome

Nesta seção será demonstrado o passo-a-passo para criar o acesso remoto nas ONTs Intelbras em OLT FiberHome e routerboard Mikrotik.

Acesse a ONT 142N W ou 121 W e realize as configurações abaixo:

Passo 1: Acessar a porta LAN da ONT pelo endereço IP 192.168.1.1;
Passo 2: Acessar o menu configuração de gerenciamento. Clique no menu “Segurança” e em seguida “Gerenciar acesso”;
Passo 3: Selecionar “Ativar” em “Gerenciar”;
Passo 4: Selecionar a Interface “wan.v7” e “ativar”;
Passo 5: Selecione os serviços que ficarão acessíveis através da rede de gerenciamento remoto. Veja o resumo da configuração na figura 2:

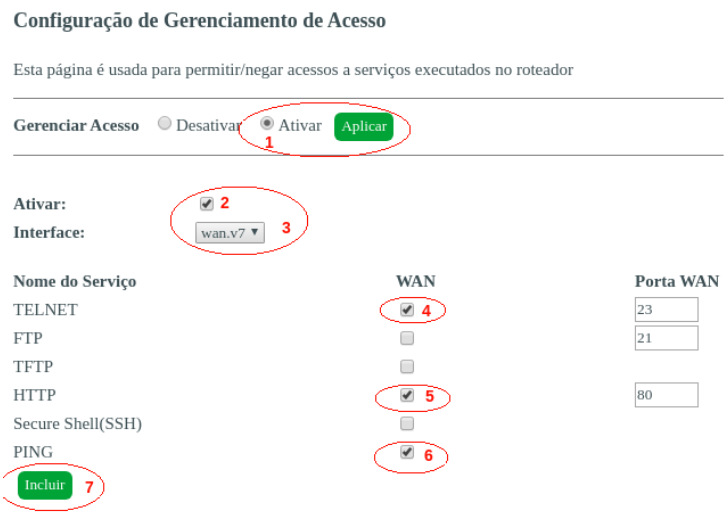


Figura 2 - Interface de configuração da ONT para definir os serviços de acesso remoto.

Acesse a Routerboard Mikrotik e realize as configurações abaixo:

Passo 6: Criar um pool de endereço para o serviço DHCP server na routerboard Mikrotik. Defina a faixa de endereço IP a ser usada pelo servidor DHCP respeitando o endereço de rede 1.1.1.0/8. Exemplo 1.1.1.0-1.1.1.100

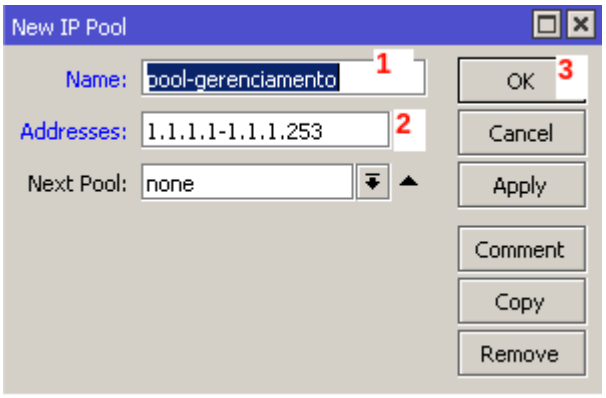


Figura 3 - Menu de criação do Pool de endereços.

Passo 7: Crie a VLAN 7 e atribua a interface do mikrotik conectada na interface na OLT configurada para gerenciamento das ONTs.

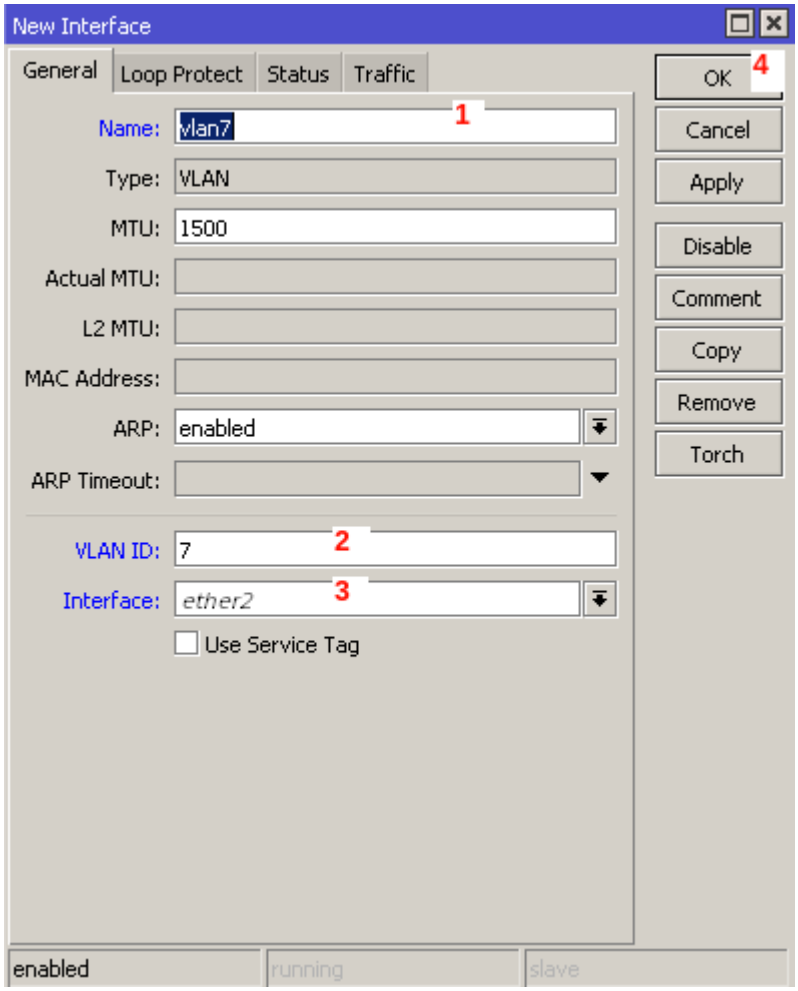


Figura 4 - Menu de configuração de nova VLAN.

Passo 8: Criar uma bridge de gerenciamento:

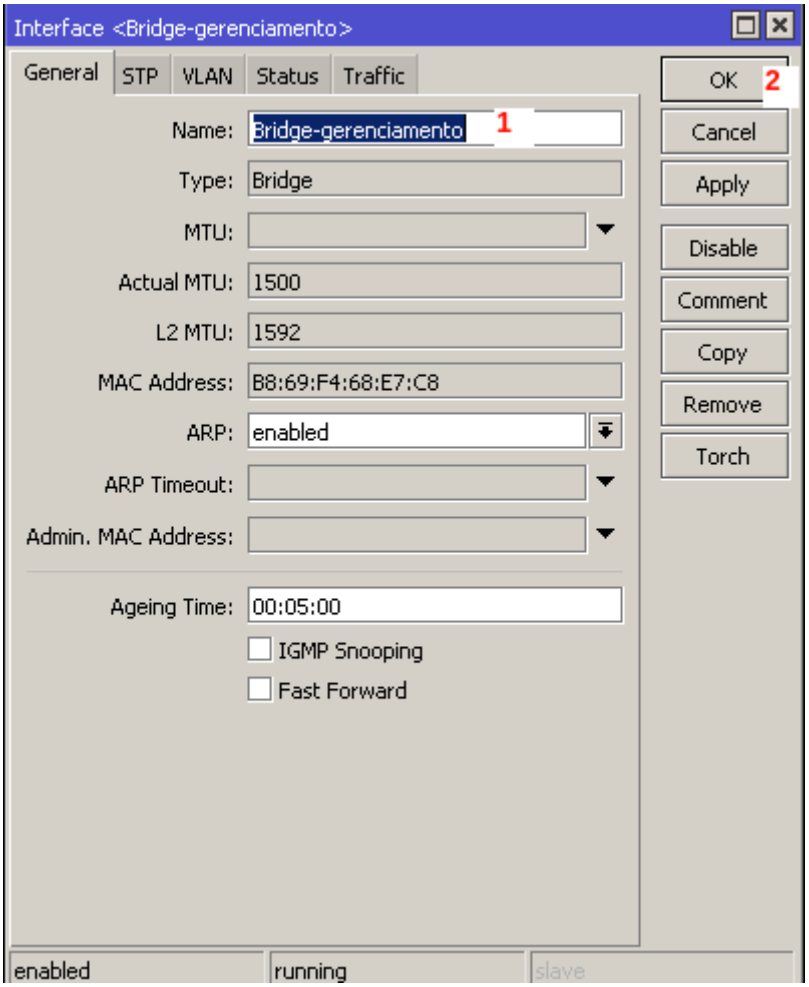


Figura 5 - Menu de criação de nova bridge.

Passo 9: Na aba *ports* incluir a bridge de gerenciamento e a porta do Mikrotik destinada para o computador que acessa a rede de gerenciamento.

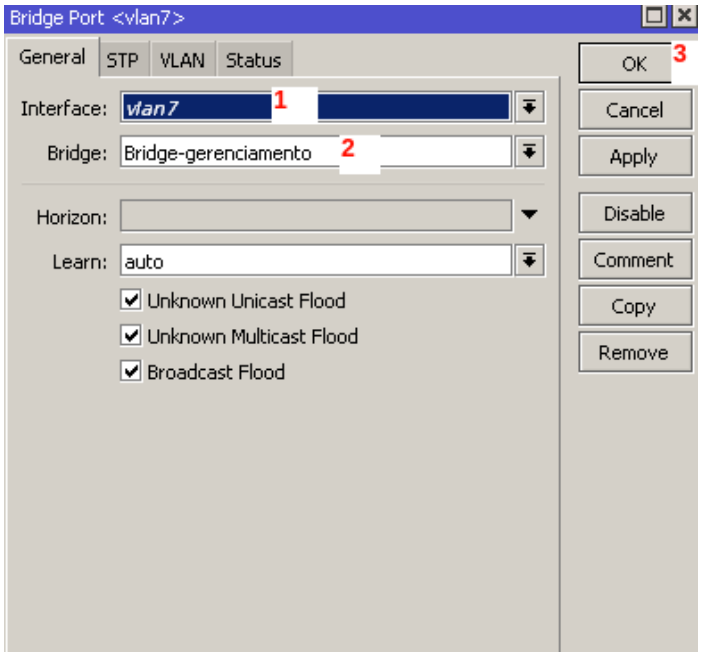


Figura 6 – Inclusão da VLAN 7 na bridge de gerenciamento.

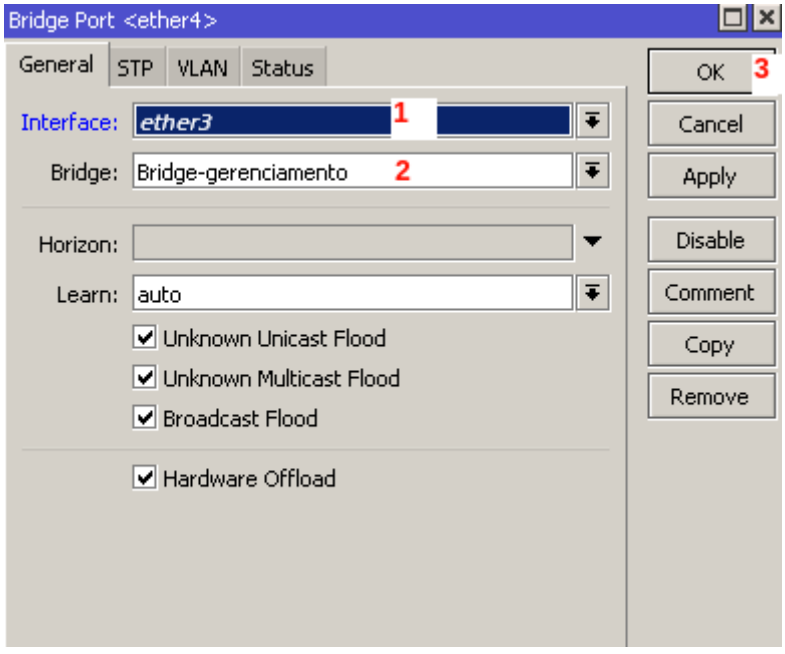


Figura 7 – Inclusão da interface de rede 3 (ethr3) do mikrotik na bridge de gerenciamento.

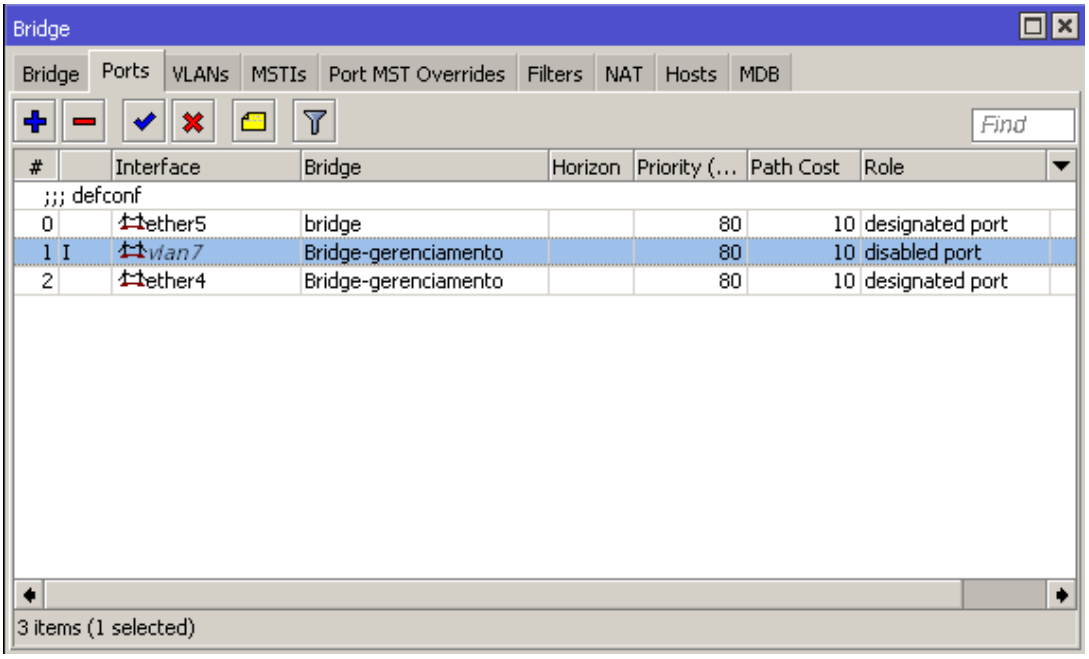


Figura 8 – Resultado da inclusão da VLAN e interface ethernet 3 na bridge de gerenciamento.

Passo 10: Criar um nome para o servidor DHCP em “interface” e selecionar a bridge de gerenciamento criada no passo 2 e a pool de endereços IPv4 criada no passo 1.

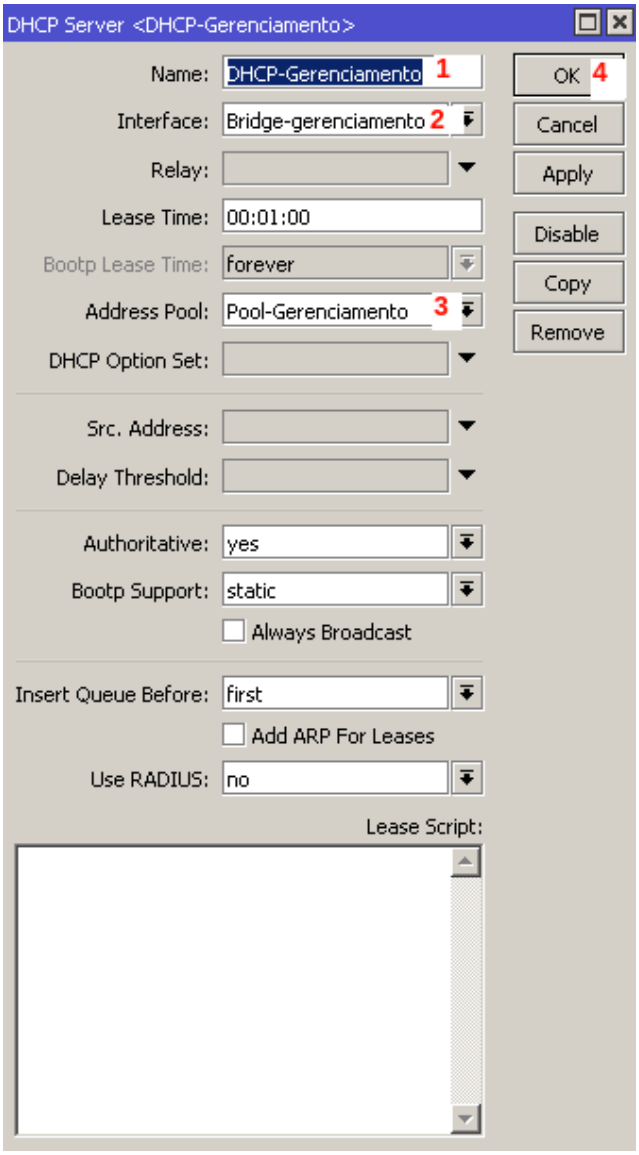


Figura 9 - Menu de criação de novo servidor DHCP

Passo 11: Clicar “**IP->AdressList**” e criar o endereço IP para interface conectada à OLT com máscara /8, definir no campo network o endereço de rede 1.0.0.0 e selecionar a bridge de gerenciamento:

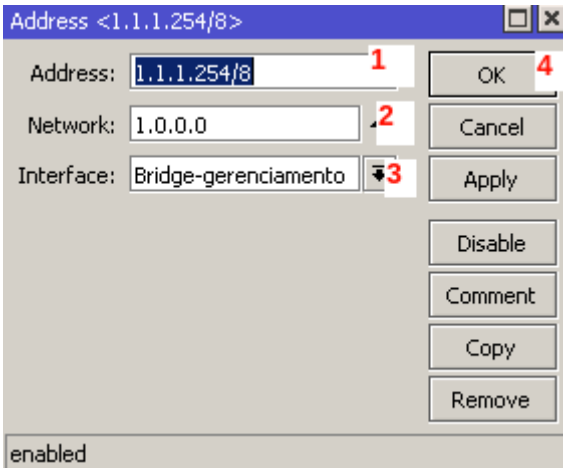
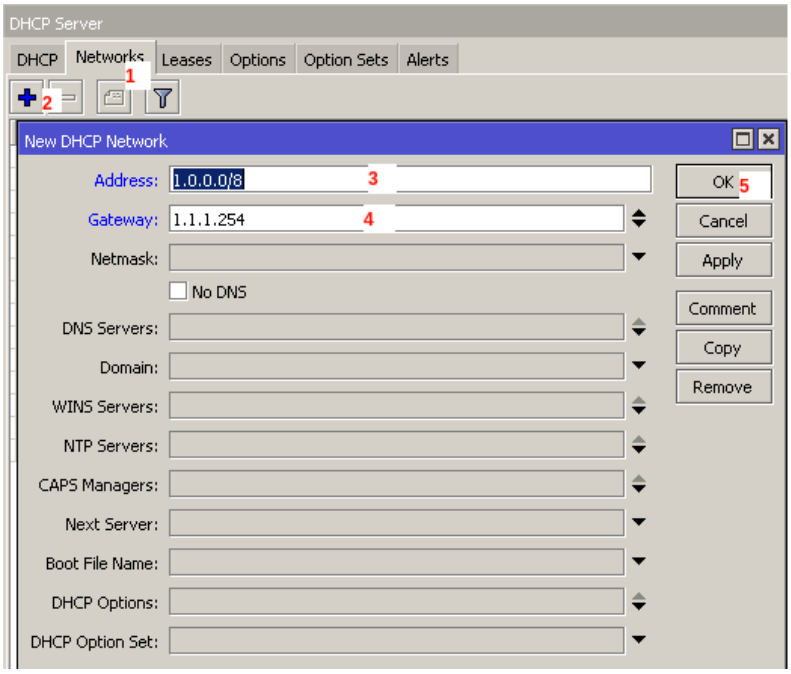


Figura 10 - Menu de criação de endereços de rede

Passo 12: Clique Networks e adicione nova configuração de rede que será informada via protocolo DHCP para a ONT. No campo **Address** digite 1.0.0.0/8 e **gateway** 1.1.1.254.



Acesse a OLT FiberHome através do software AMN 2000 e realize as configurações abaixo:

Pré-requisito:

- ONT devidamente ativada.

Passo 13: Acessar *"Service Config Management"* para criar a VLAN 7 clicando com o direito na interface HSUB.

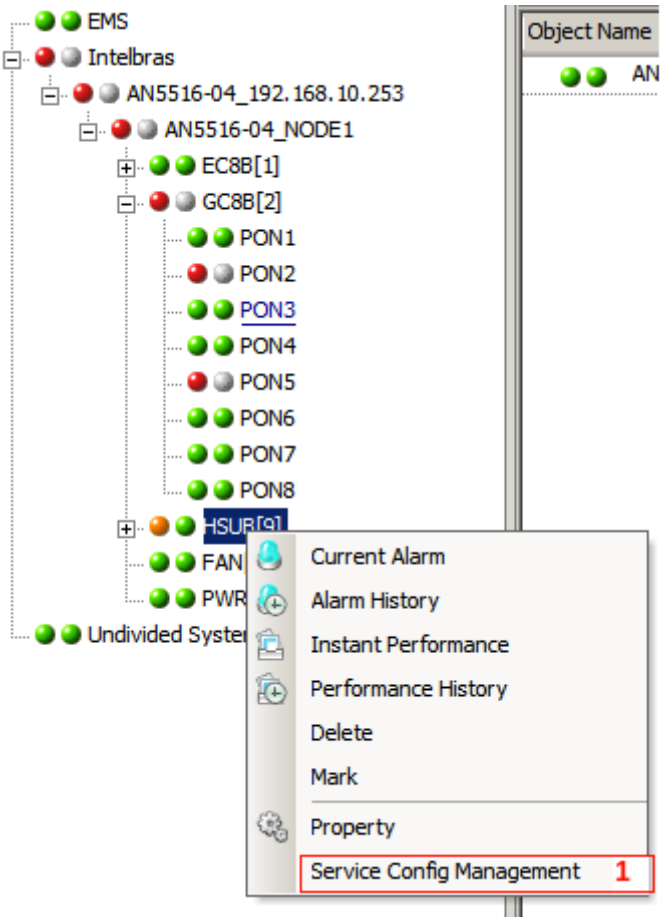


Figura 11 - Menu de opções para a interface HSUB

Passo 14: Crie a VLAN 7 Tagged de gerenciamento clicando em *append* para adicionar nova linha conforme ilustração abaixo (*Starting VLAN ID*: 7, *VLAN ID End:*7, interface: uplink, *Service Type: data, Slot Bind mode*: *Auto Bind):*

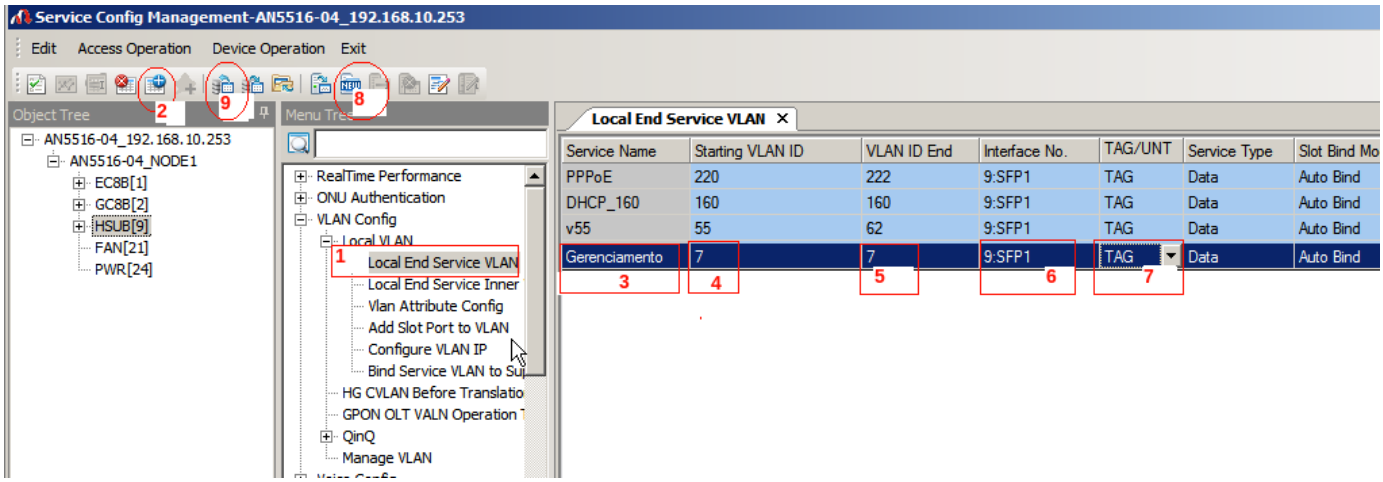


Figura 12 – Menu de inclusão de nova VLAN.

Passo 15: Crie o modelo de serviço da ONT, clique com o botão direito do mouse na OLT desejada e encontre o menu "*Service Config Management*"
Passo 4: Navegue entre as opções até a opção "*Service Model Profile*"

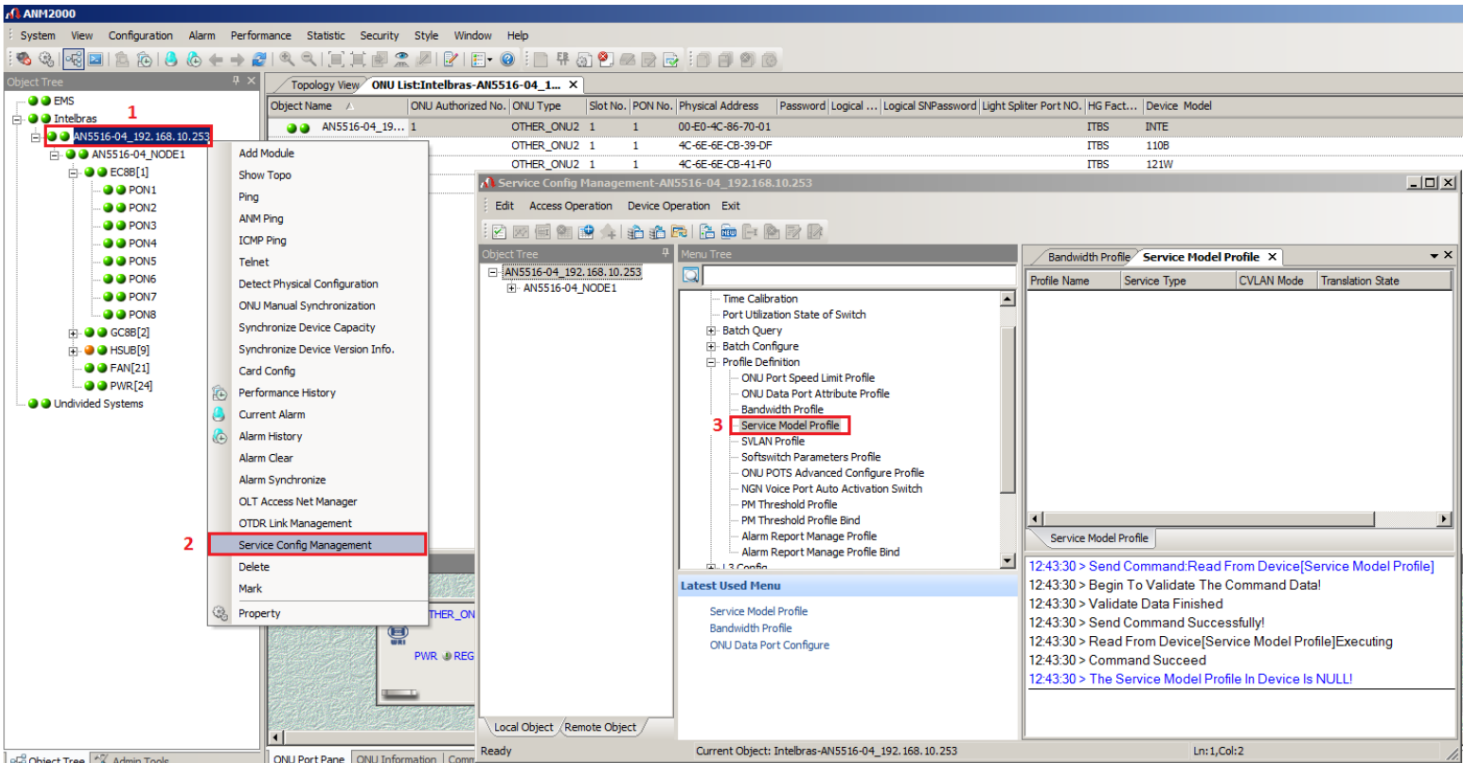


Figura 13 – menu de criação de novo *Service Model Profile*

Passo 16: Clique no menu *"Append"* para inserir as informações. Neste momento, será aberto uma caixa de diálogo solicitando a confirmação, clique em OK
Passo 17: Dê um duplo clique na coluna "Profile Name" e insira o nome do profile, neste exemplo utilizamos GerenciaONT

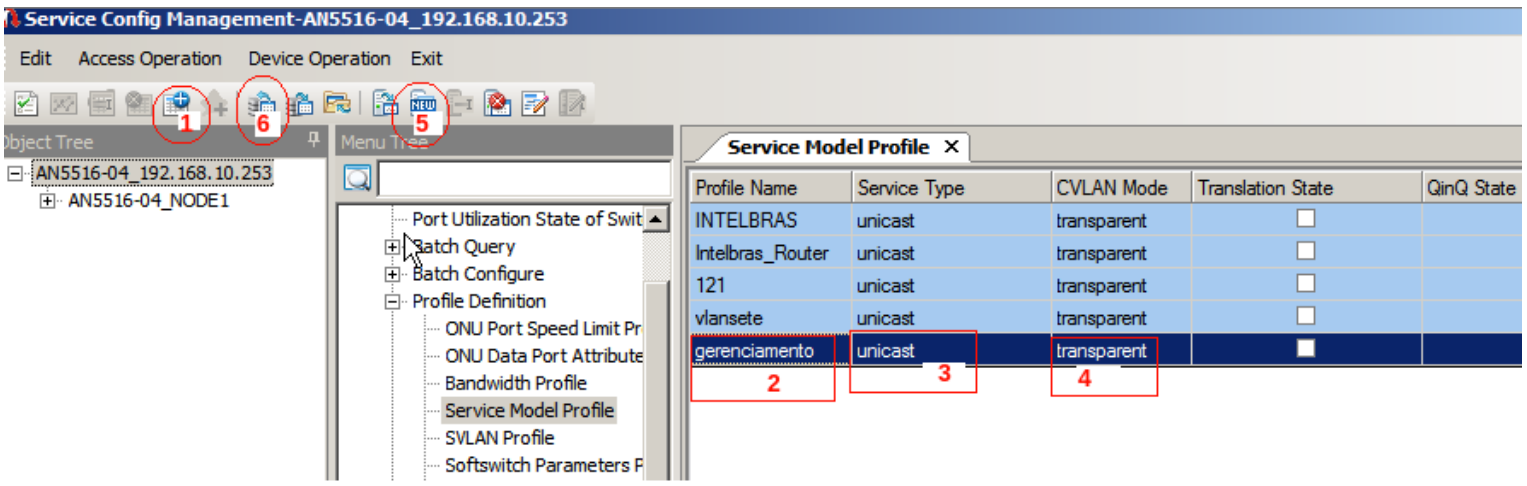


Figura 14 – Processo de inclusão de novo Service *Model Profile*

Passo 18: Salve a configuração Clicando no botão *"Create On Device"* em seguida *"Write To Database"*
Passo 19: Atribua a nova VLAN 7 na ONT desejada. Para tal, acessar a porta GPON na qual a ONT está ativada.
Passo 20: Clicar com o botão direito do mouse na ONT desejada.
Passo 21: Acessar o menu *"Service Config Management"*. Neste momento será aberto uma nova janela.
Passo 22: Clicar na opção *"VEIP data service config"* localizado dentro do menu *"Config"*.
Passo 23: Clicar no menu *"Append"* para inserir as informações. Neste momento, será aberto uma caixa de diálogo solicitando a confirmação, clique em OK

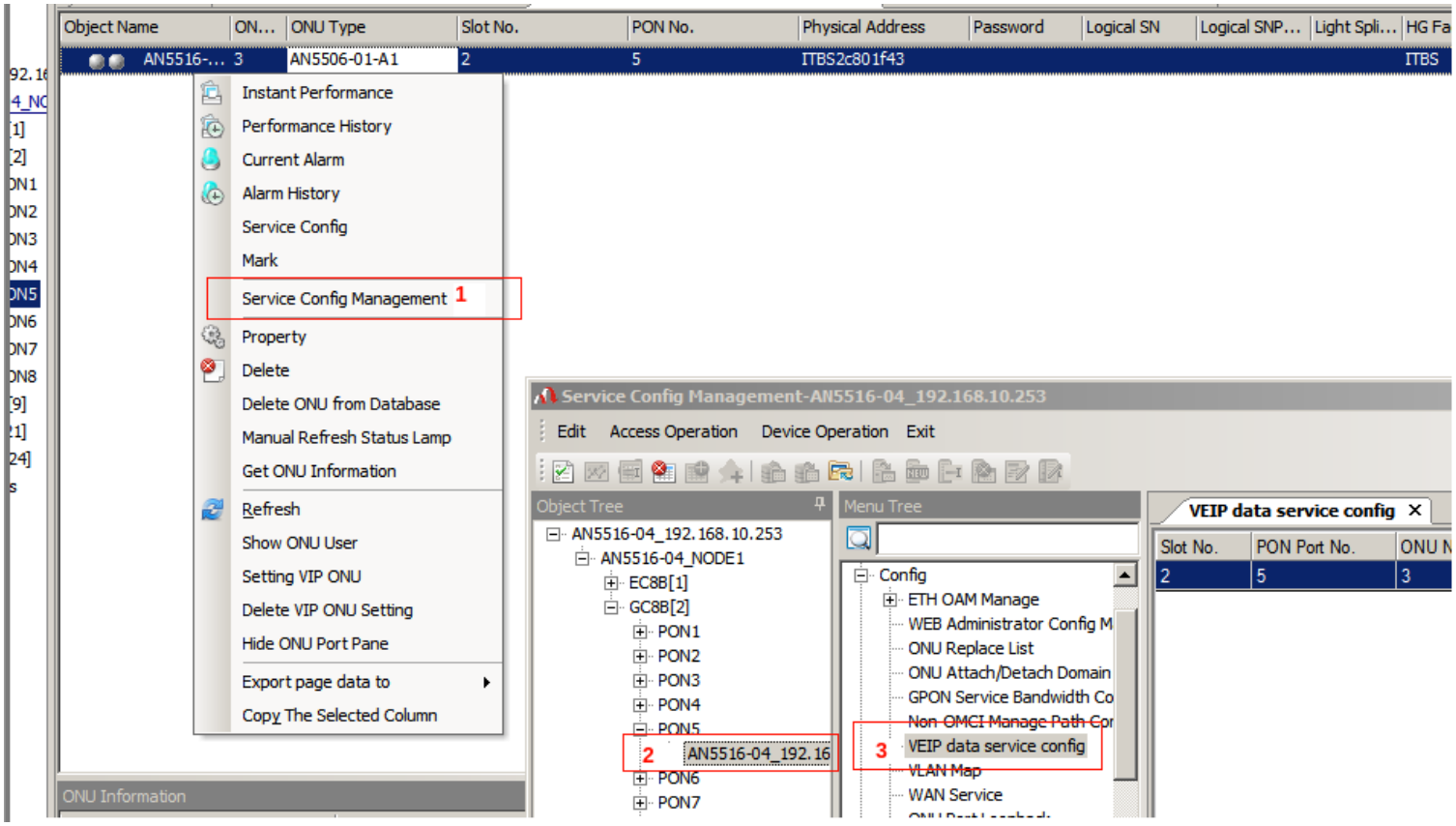


Figura 15 – Acesso ao menu de configuração de nova VEIP

Passo 24: Alterar o campo *CVLAN ID* para 7 (VLAN de gerenciamento)
Passo 25: Alterar o campo *Service Model* para o perfil *"Gerenciamento"*

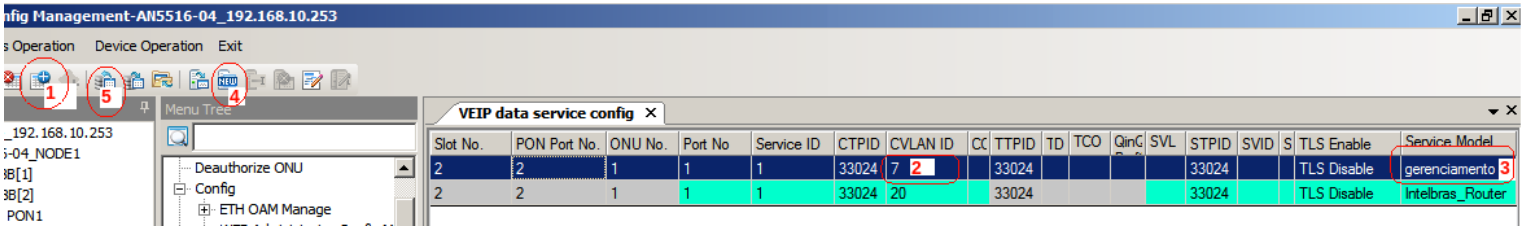


Figura 16 - Ilustração do menu após a inclusão da VLAN 7 na respectiva ONT.

Passo 26: Clicar no botão *"Create On Device"*
Passo 27: Clicar no botão *"Write To Database"*

Passo 28: A configuração foi concluída. Via software Winbox do mikrotik verifique o endereço IP que a ONT através no menu ***DHCP-Server->Leases***

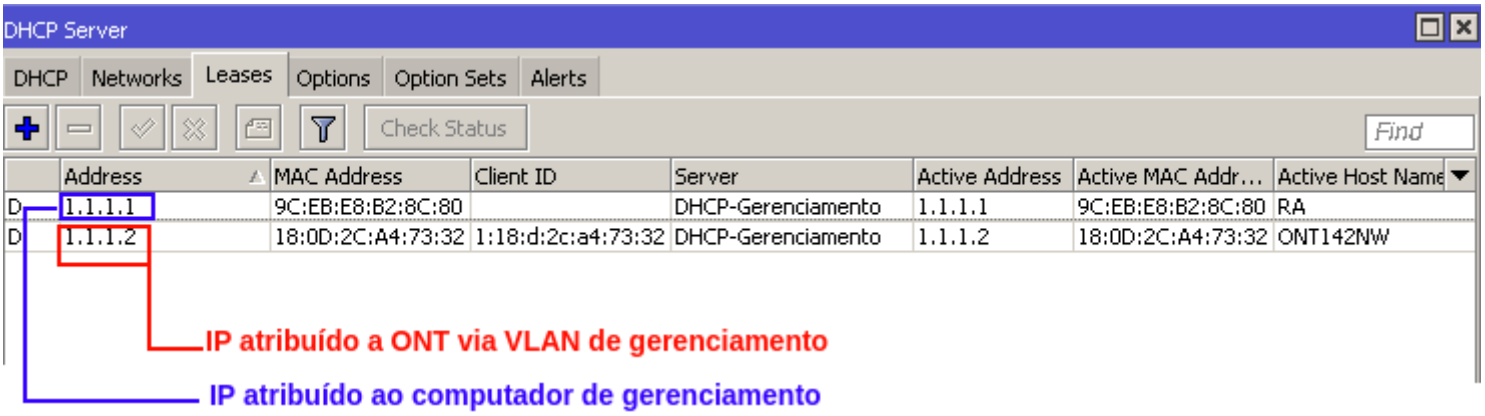


Figura 17 – Endereços IPs atribuídos a ONT e ao computador de gerenciamento via rede de gerenciamento.

Passo 29: Para acessar telnet via winbox, acesse o menu ***Tools->Telnet*** e digite o endereço IP atribuído à ONT via rede de gerenciamento. Conforme ilustrado na figura do passo 17.

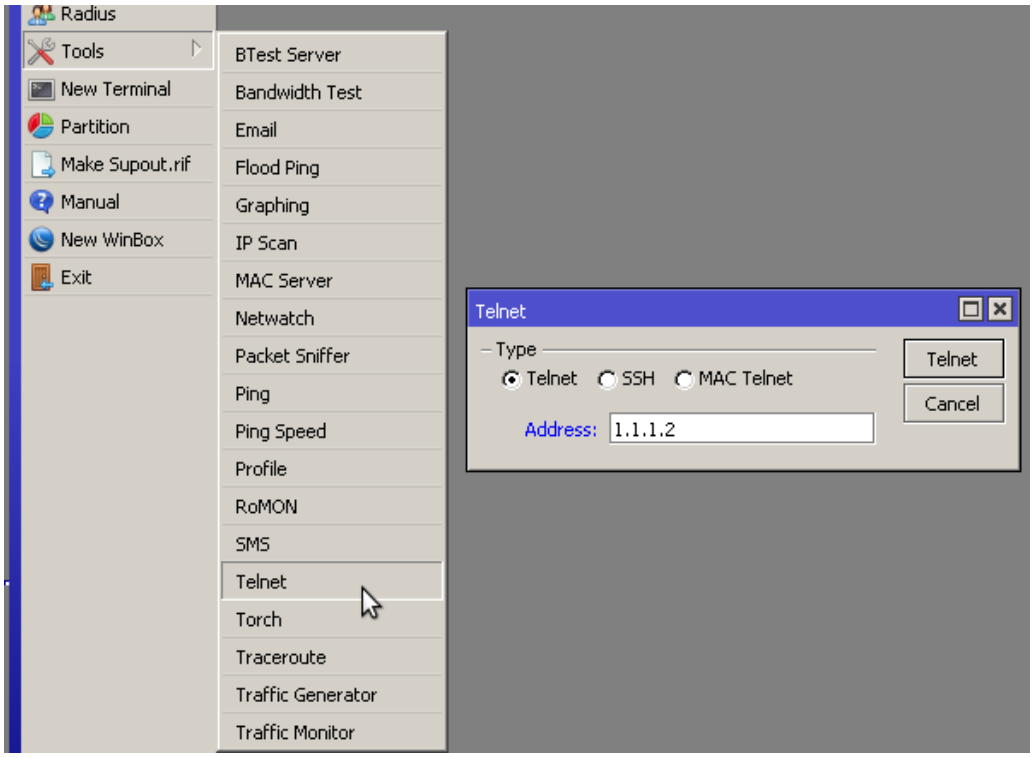


Figura 18: Menu de conexão Telnet

Passo 30: Para acessar a ONT a partir do computador de gerenciamento, conecte-o na porta do mikrotik que foi configurada no passo 4 e execute o comando: telnet + IP para a acessar a ONT via rede de gerenciamento remoto.

Parte 2: Acesso a rede de gerenciamento a partir da rede externa (Internet)

1) Descrição

Este procedimento é um complemento da parte 1. Visa descrever como acessar aos serviços telnet e web para administração das ONTs 121 W e 142N W a partir da rede externa (internet). A topologia completa da rede representando os acessos local e externo é ilustrado na figura 19.

Atenção: A configuração a seguir depende da abertura de portas no roteador. O principal risco é a possibilidade de que qualquer dispositivo conectado à rede internet tente se conectar aos equipamentos da rede interna mapeados no redirecionamento de portas. Para se prevenir destes tipos de ataque é importante configurar o Firewall restringindo o acesso aos endereços IP's públicos de sua preferência. Independente de qual solução adotar, é imprescindível alterar a senha das ONTs mapeados, tendo em vista que todas as ONTs possuem usuário e senha padrão de fábrica.

2) Objetivo:

Este documento detalha duas maneiras de criar as regras de redirecionamento de portas. A primeira é manualmente, no qual a cada nova ONTs deverá ser refeito os passos 30 e 31. A outra maneira é automaticamente via script criado pelo P&D. A vantagem do script é que a cada nova ONTs ativada, as regras serão criadas automaticamente e a ONT estará configurada para ser acessado remotamente.

3) Topologia da rede

As ONTs na rede GPON podem ser acessadas a partir de dois pontos na rede: Primeira via rede local representado pelo PC1, com o procedimento de configuração descrito na parte 1 deste documento e segundo via rede internet representado pelo PC2. Salientamos que a configuração por este documento descrito pode ser replicada para qualquer modelo de OLT ou roteador, tendo em vista que a essência do funcionamento do acesso remeto nas ONTs é a disponibilidade de endereços da 1.0.0.0/8 providos na porta PON das ONTs via VLAN 7 tagged.

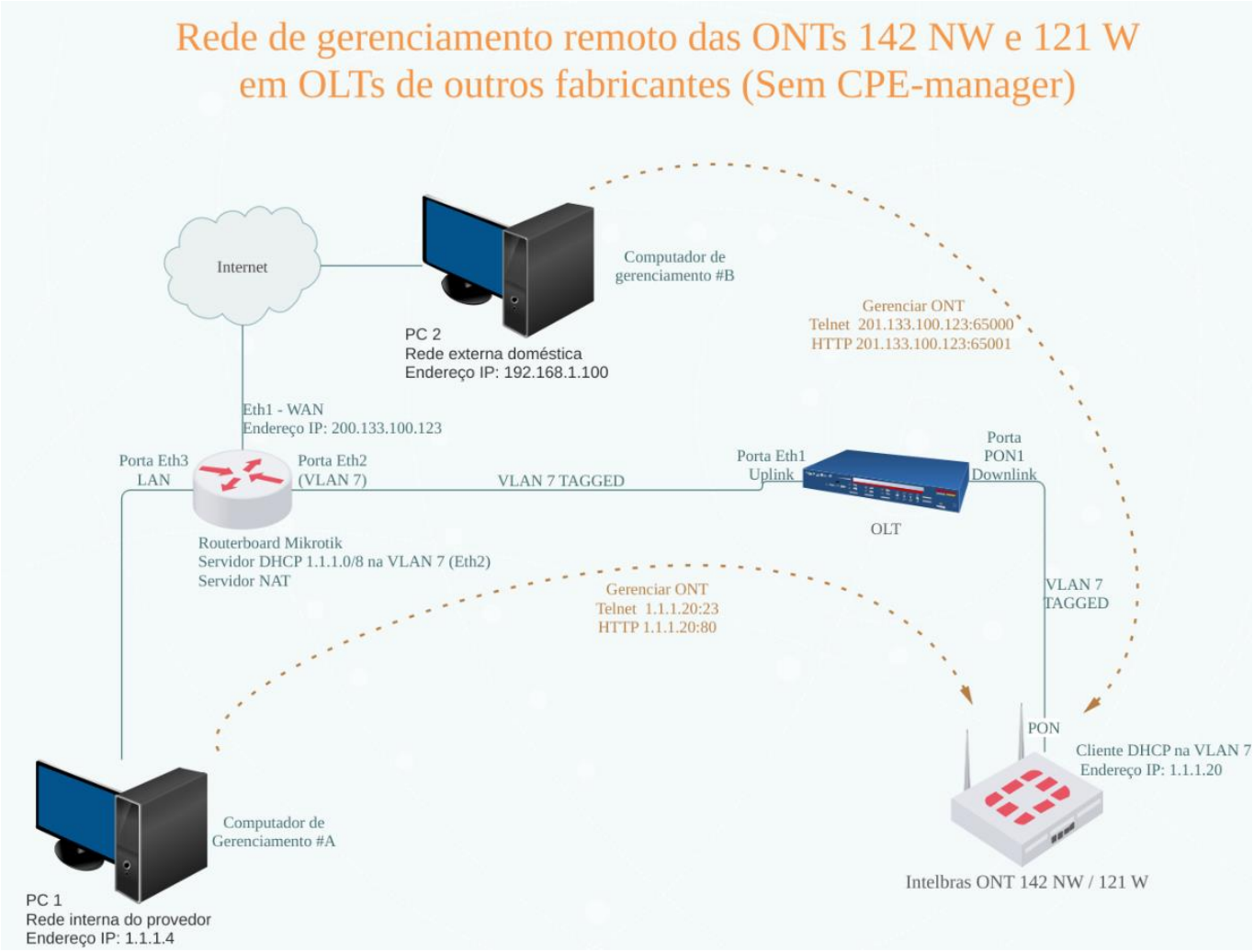


Figura 19: Topologia completa para acesso remoto via rede local e externa.

Pré-requisito:

- Concluir parte 1 deste documento.
- A interface WAN do roteador com acesso à internet.

Conceito de redirecionamento de portas:

É um serviço que o roteador oferece ao direcionar o acesso de uma rede externa para rede privada por meio da liberação de portas. As regras de redirecionamento de portas são definidas na tabela NAT do roteador. Se a requisição de conexão atende alguma regra definida na tabela NAT, efetua-se o redirecionamento de porta para o IP privado e a porta especificada na regra. Portanto, para cada ONT a ser acessada remotamente deverá ser aberto no mínimo uma porta no roteador e a regra deverá indicar qual o IP e a porta (telnet ou HTTP) da ONT.

Seguindo o exemplo da figura 19, deverá ser criado uma regra na tabela NAT para redirecionar a conexão em uma porta de entrada (ex:65000) para o IP 1.1.1.2 na porta 23. Acesse a Routerboard Mikrotik e realize as configurações descritas acima.

Procedimento manual para criação das regras de NAT para acessar remotamente via TELNET as ONTs 121 W e 142N W:

Os passos 30 e 31 deverão ser realizados para cada nova ONTs habilitada, porém pode ser substituído pelo procedimento automático para criação das regras de NAT.

Passo 31: Caso a regra masquerade não esteja criada na srcnat, clicar em **IP->Firewall**, aba NAT, adicionar *NAT Rule,* selecionar *chain srcnat, em Out Interface List* selecione WAN, clicar em *Action* e selecione *masquerade* e confirme em OK.

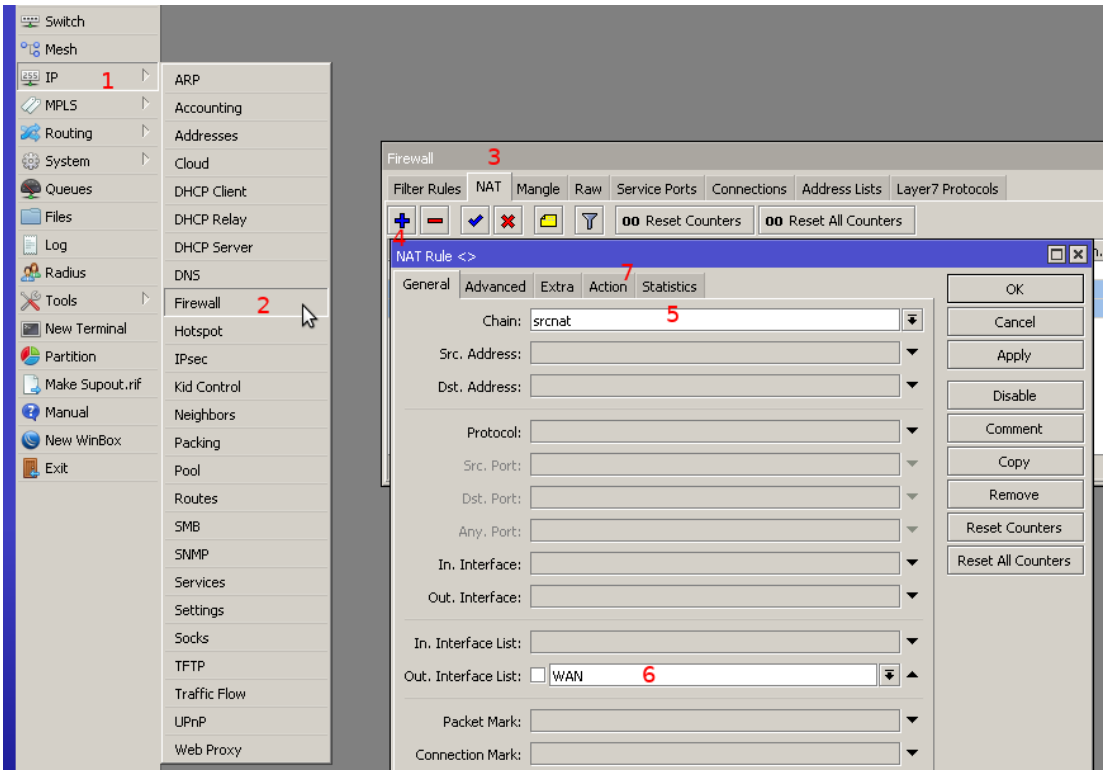


Figura 20: Inclusão de nova regra NAT.

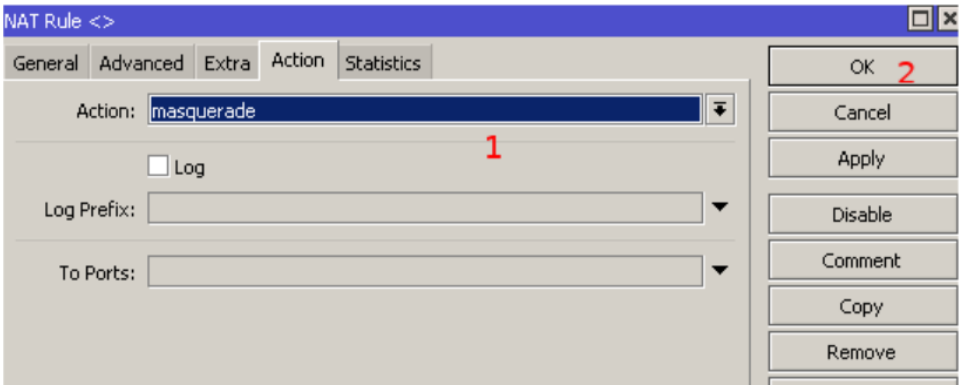


Figura 21: Definição do tipo de ação da nova regra NAT.

Passo 32: Redirecionar as conexões entrantes na porta 65000 para o IP 1.1.1.2 porta 23. Clicar em adicionar Nat Rule, em *Chain* selecione dstnat, definir o IP valido que terá acesso a rede interna em Src. Address, selecionar protocol TCP, Dst. Port 65000, clicar na aba Action, em Action selecione dst-nat e em To-Add Addresses digite 1.1.1.2 e em *To ports* 23 e finalize em OK.

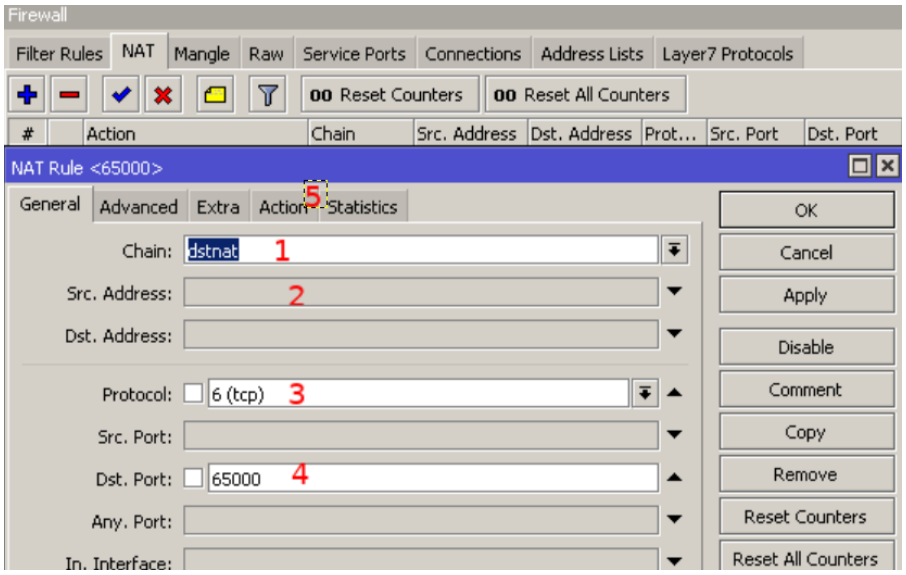


Figura 22: de nova regra NAT.

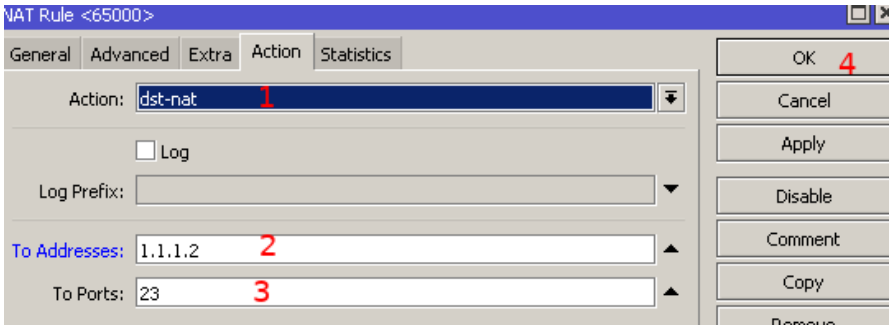
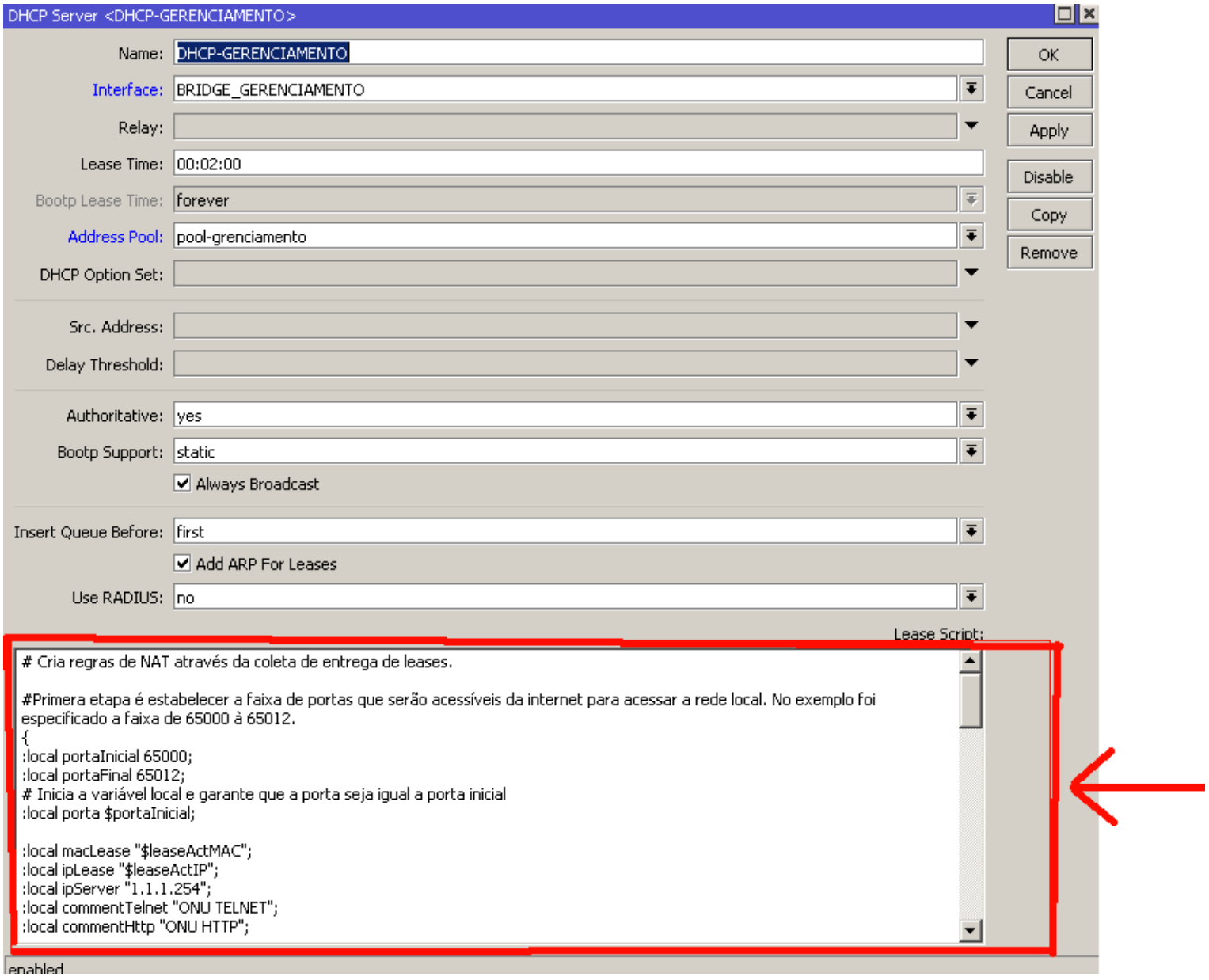


Figura 23: de nova regra NAT.

Após a conclusão destes passos a ONT estará acessível via telnet pelo endereço IP público na porta WAN do roteador porta 65000, que no roteador será redirecionada para o IP privado 1.1.1.2 na porta 23.

Script de criação das regras de NAT para acesso remoto TELNET e HTTP das ONTs 121 W e 142N W:

A cada nova ONT habilitada na OLT, a ONT receberá um endereço do servidor DHCP do mikrotik e automaticamente executará o script, no qual, criará duas regras de srcnat para acesso remoto dos serviços HTTP e TELNET das ONTs. Adicione o script abaixo no campo Lease script na tela de configuração do servidor DHCP criado no passo 10 (figura 9).


DHCP Server <DHCP-GERENCIAMENTO>
Name: DHCP-GERENCIAMENTO
Interface: BRIDGE_GERENCIAMENTO
Relay:
Lease Time: 00:02:00
Bootp Lease Time: forever
Address Pool: pool-grenciamento
DHCP Option Set:
Src. Address:
Delay Threshold:
Authoritative: yes
Bootp Support: static
Always Broadcast
Insert Queue Before: first
Add ARP For Leases
Use RADIUS: no
Lease Script:
Cria regras de NAT através da coleta de entrega de leases.
#Primera etapa é estabelecer a faixa de portas que serão acessíveis da internet para acessar a rede local. No exemplo foi especificado a faixa de 65000 à 65012.
{
:local portaInicial 65000;
:local portaFinal 65012;
Inicia a variável local e garante que a porta seja igual a porta inicial
:local porta $portaInicial;
:local macLease "$leaseActMAC";
:local ipLease "$leaseActIP";
:local ipServer "1.1.1.254";
:local commentTelnet "ONU TELNET";
:local commentHttp "ONU HTTP";
OK
Cancel
Apply
Disable
Copy
Remove
enabled

```
# Cria regras de NAT através da coleta de entrega de leases.

#Primeira etapa é estabelecer uma faixa de portas para o script criar as regras de
redirecionamento. Neste exemplo é definido a faixa de 65000 à 65012.
{
:local porta Inicial 65000;
:local porta Final 65012;
# Inicia a variável local e garante que a porta seja igual a porta inicial
:local porta $porta Inicial;

:local macLease "$leaseActMAC";          # MAC da ONT ativa no servidor DHCP via VLAN
7
:local ipLease "$leaseActIP";            # IP da ONT ativa no servidor DHCP via VLAN 7
:local ipServer "1.1.1.254";             # IP da porta da VLAN de gerenciamento
:local commentTelnet "ONU TELNET";       # Comentário a ser adicionado na regra NAT
:local commentHttp "ONU HTTP";           # Comentário a ser adicionado na regra NAT
:local ipServerWAN "10.207.1.32";   # Endereço IP de destino. Endereço IP da interface
WAN
:local interfaceWan "ether1";            #interface com acesso a internet

# Segunda etapa é definir qual ip externo poderá acessar a rede local. Este tipo de
configuração aumenta a segurança da rede pois restringir o acesso a determinado IP.
Exemplo 200.1.2.3/32 ou use o valor 0.0.0.0/0 para permitir qualquer um. Default está
0.0.0.0/0
:local ipInternetExterno "0.0.0.0/0";    # IP externo que terá acesso a rede de
gerenciamento


:if ($leaseBound = "1") do={
#caso tenha uma entrega de lease, faço esse bloco
#exemplos de variável
#/queue simple add name=$queueName target=($leaseActIP . "/32") limit-at=1024k/1024k
max-limit=1024k/1024k comment=[/ip dhcp-server lease get [find where active-mac-
address=$leaseActMAC && active-address=$leaseActIP] host-name];
:while ($portaInicial < $portaFinal) do={
# Garante que sempre a porta seja igual a porta inicial, que sofre incremento
:set porta $portaInicial;
# Verifica se a porta já esta em uso por outra regra, caso esteja, incrementa em 1 e
testa novamente
if ( [/ip firewall nat find where dst-port="$porta"] != "") do={
put "Porta $porta ocupada"
} else={
put "Porta $porta livre, regra add"
# Regra add DNAT telnet e http
/ip firewall nat add action=dst-nat chain=dstnat dst-address=$ipServerWAN  src-
address=$ipInternetExterno dst-port=$porta in-interface=$interfaceWan protocol=tcp to-
addresses=$ipLease to-ports=23 comment="$commentTelnet DNAT $macLease"
:set porta ($porta + 1);
put "Porta $porta livre, regra add"
/ip firewall nat add action=dst-nat chain=dstnat dst-address=$ipServerWAN  src-
address=$ipInternetExterno dst-port=$porta in-interface=$interfaceWan protocol=tcp to-
addresses=$ipLease to-ports=80 comment="$commentHttp DNAT $macLease"
```

```
# Seta a porta final para $portaFinal + 1 para garantir que saia do loop quando
adicionar as duas regras
:set portaInicial ($portaFinal + 1);
}
:set portaInicial ($portaInicial + 1);
}
# Regra add SNAT telnet e http
/ip firewall nat add action=src-nat to-addresses=$ipServer chain=srcnat dst-
address=$ipLease dst-port=23 protocol=tcp comment="$commentTelnet SNAT $macLease"
/ip firewall nat add action=src-nat to-addresses=$ipServer chain=srcnat dst-
address=$ipLease dst-port=80 protocol=tcp comment="$commentHttp SNAT $macLease"

} else={
#caso remova uma entrega de lease, faço esse bloco
# Regra delete telnet e http
# Deleta a regra baseada no comentário criado
/ip firewall nat remove  [find where comment="$commentTelnet DNAT $macLease"]
/ip firewall nat remove  [find where comment="$commentHttp DNAT $macLease"]
/ip firewall nat remove  [find where comment="$commentTelnet SNAT $macLease"]
/ip firewall nat remove  [find where comment="$commentHttp SNAT $macLease"]
}
}
```