

MANUAL B2B NOC



NOC CGR RYAN SILVA

NOC MASTER OUTUBRO 2024

Sumário

APRESENTAÇÃO DE PRODUTOS	3
CONFIGURAÇÕES NE	4
Configurações de rota estática com IP válido e IP de enlace no NE	8
CONFIGURAÇÕES GFW (FREE-BSD)	9
Configurações de rota estática com IP válido e IP de enlace no GFW	13
SWITCH	14
Configurações de Switch:.....	18
CONFIGURAÇÕES DE SWITCH DATACOM (EDD).....	19
Configurações de EDD 2104 (1GB).....	19
Configurações de EDD 4370 (10 GB)	21
LIMITAÇÃO DE TRÁFEGO	23
CONFIGURAÇÕES DE MIKROTIK.....	25
Configurações CRS.....	25
Configurações CCR:	27
Configuração de vlan nas CCRs.....	33
Bandwidth Teste	35
WIFI-SEGURO.....	37
Configurações WIFI-SEGURO sistema hotspot	41

APRESENTAÇÃO DE PRODUTOS

Os produtos que o atendimento é de responsabilidade do NOC são:

- **IP DEDICADO :**

Consiste em um bloco de IP válido que é entregue de forma livre para que o cliente utilize e aplique as regras que quiser neste bloco. Esse produto pode ser entregue de 2 formas. A primeira é a forma convencional no qual utilizamos 1 IP do bloco contratado pelo cliente para utilizar de gateway e firmar a comunicação cliente <> roteador. A segunda forma é o bloco de IP válido porém sem utilizar 1 IP do bloco para ser o gateway, sendo assim, é utilizado um segundo bloco de IP (Bloco de enlace) destinado apenas a comunicar cliente <> gateway, sendo que este bloco de enlace não comunica com a internet. Desta forma além do bloco de enlace também há uma configuração adicional no roteador no qual é feito uma rota estática (apontamento) do bloco de enlace para o bloco válido, se tornando um tipo de “extensão”.

Resumindo: Bloco de IP destinado ao cliente e configurado manualmente no roteador de borda.

- **IP FIXO:**

Consiste em um IP que nunca mudará, mesmo que o cliente reinicie os equipamentos, sendo entregue por PPOE (na rede FTTH) e DHCP (na rede wireless). Este produto pode ser impactado por regras de firewall dos autenticadores. É o mesmo que IP light, IP semi dedicado. Possui cadastro no I-NS no I-manager e utiliza os escopos reserva de cada regional.

- **LAN TO LAN:**

Consiste em uma comunicação simples de uma ponta “a” até uma ponta “b” em camada 2 (Camada de enlace, sem utilizar IP) por meio de vlans.

- **WIFI SEGURO:**

Consiste em uma configuração em que todos que conectarem em certa rede de wifi, terão de fazer cadastro e login em uma plataforma que armazena tudo que este login navegou. Evitando futuros problemas de acessos indevidos a sites proibidos da rede do cliente por outras pessoas que acessaram. Esse produto pode ser utilizado em conjunto com o IP Dedicado e IP Fixo.

Os produtos IP TRÂNSITO e TRANSPORTE PTT, são produtos gerenciados diretamente pela equipe de engenharia, pois na maioria das vezes são contratos com bastante capacidade de banda e configuração mais complexa, no caso do IP TRÂNSITO. O IPT consiste em uma sessão BGP diretamente ligada ao contratante, que quase sempre serão outros provedores. O TRANSPORTE PTT consiste em um LTL da ponta “a” que é o cliente até o ponto de troca de tráfego de São Paulo.

CONFIGURAÇÕES NE

- 1- Primeiramente identificar a interface que está comunicando com o próximo switch (geralmente o switch mpls).

```
<DVL-HED-NEV-01>dis int desc
PHY: Physical
  down: administratively down
  ^down: standby
  (l): loopback
  (s): spoofing
  (E): E-Trunk down
  (B): BFD down
  (B): Bit-error-detection down
  (e): ETHoAM down
  (d): Dampening suppressed
  (p): port alarm down
  (lh): link heartbeat down
  (ld): loop-detect trigger down
interface      PHY    Protocol Description
Eth-Trunk0     up     down   | NE20 x 6730(SWT 03) |
Eth-Trunk0.5   up     down   | GER | CDN-EDGIO |
Eth-Trunk0.8   up     down   | CDN_NFX | 20Gb - DVL
Eth-Trunk0.10  up     up     [CDN]NETFLIX[IT]
Eth-Trunk0.11  up     up     [CDN] FACEBOOK | 20G
Eth-Trunk0.15  up     up     CLIENTES FITTH
Eth-Trunk0.20  up     up     CLIENTES WIRELESS
Eth-Trunk0.30  up     up     CMTS
Eth-Trunk0.50  up     up     GER | OLT-ZTE | DVL
Eth-Trunk0.52  up     up     description GER | OLT-ZTE | HED | DVL
Eth-Trunk0.60  up     up     servidores 189.91.0.5
Eth-Trunk0.65  up     up     IPTV Master
Eth-Trunk0.70  up     up     Servidores 189.91.0.65
Eth-Trunk0.99  up     up     TESTE-CONEXAOP-BETO
Eth-Trunk0.120 up     up     CLI | IPD | SENETO | 59561 | 50MB
Eth-Trunk0.127 up     up     CLI | IPD | UNTMED | 533091 | 300MB
Eth-Trunk0.128 up     up     CLI | IPD | CONSORZIO SBE | 343081 | 10MB
Eth-Trunk0.132 up     up     CLI | IPD | CIAFAL | 619171 | 50MB
Eth-Trunk0.134 up     up     CLI | IPD | FERRAZ & MEIRA | 557691 | 20MB
```

Command:

dis int desc //verificar descrições, e ver qual Eth-trunk está sendo configurada as demais sub-interfaces

- 2- Configurar uma sub-interface para a vlan específica do cliente.

```
[~DVL-HED-NEV-01] interface Eth-Trunk 0.441
[*DVL-HED-NEV-01-Eth-Trunk0.441]vlan-type dot1q 441
[*DVL-HED-NEV-01-Eth-Trunk0.441]
```

Obs (sempre que houver o * dentro dos colchetes significa que há configurações não aplicadas, então é necessário dar o commit para aplicar)

```
[*DVL-HED-NEV-01-Eth-Trunk0.441]commit
[~DVL-HED-NEV-01-Eth-Trunk0.441]dis this
#
interface Eth-Trunk0.441
  vlan-type dot1q 441
#
```

Command:

```
sys
interface eth-trunk0.441
  vlan-type dot1q 441 //criar a sub-interface, no exemplo seria para a vlan 441
                      //definir a vlan 441 na sub-interface
```

3- Setar o IP (gateway) para fechar o enlace.

```
[~DVL-HED-NEV-01-Eth-Trunk0.441] ip address 191.240.92.173 30
[*DVL-HED-NEV-01-Eth-Trunk0.441] commit
[~DVL-HED-NEV-01-Eth-Trunk0.441] dis this
#
interface Eth-Trunk0.441
  vlan-type dot1q 441
  ip address 191.240.92.173 255.255.255.252
#
```

Command:

```
sys
interface eth-trunk0.441          //criar a sub-interface, no exemplo seria para a vlan 10
  vlan-type dot1q 441            //definir a vlan 10 na sub-interface
  ip address 191.240.92.173 30   //setando o ip de gateway do cliente /30, o bloco é 191.240.92.172/30
```

4- Habilitar coleta de estatísticas na sub-interface.

```
[~DVL-HED-NEV-01-Eth-Trunk0.441] statistic enable
[*DVL-HED-NEV-01-Eth-Trunk0.441] ip netstream inbound
[*DVL-HED-NEV-01-Eth-Trunk0.441] commit
[~DVL-HED-NEV-01-Eth-Trunk0.441] dis this
#
interface Eth-Trunk0.441
  vlan-type dot1q 441
  ip address 191.240.92.173 255.255.255.252
  statistic enable
  ip netstream inbound
#
```

Command:

```
sys
interface eth-trunk0.10           //criar a sub-interface, no exemplo seria para a vlan 10
  vlan-type dot1q 10              //definir a vlan 10 na sub-interface
  ip address 191.240.0.1 30       //setando o ip de gateway do cliente /30, o bloco é 191.240.0.0/30
  statistic enable                //habilita a coleta de estatísticas
  ip netstream inbound           //habilita a coleta de estatísticas de tráfego de entrada nesta interface
```

5- Divulgar o IP de network no protocolo BGP, utilizando o filtro padrão dos outros B2Bs do NE.

```
[~DVL-HED-NEV-01]bgp 28202
[~DVL-HED-NEV-01]ipv4-family unicast
[~DVL-HED-NEV-01]bgp-af-ipv4]dis this
#
network 177.44.47.0/23 route-policy ADD-COMM
network 177.44.47.128/25 route-policy ADD-COMM
network 177.44.66.0/25 route-policy ADD-COMM
network 177.44.66.0/25 route-policy ADD-COMM
network 177.44.66.0/25 route-policy ADD-COMM
network 177.44.66.128/25 route-policy ADD-COMM
network 177.44.67.0/25 route-policy ADD-COMM
network 177.44.67.0/25 route-policy ADD-COMM
network 177.44.67.128/25 route-policy ADD-COMM
network 177.44.68.0/25 route-policy ADD-COMM
network 177.44.104.0/25 route-policy ADD-COMM
network 177.44.104.0/25 route-policy ADD-COMM
network 177.44.104.0/25 route-policy ADD-COMM
network 177.44.104.128/25 route-policy ADD-COMM
network 177.44.105.0/25 route-policy ADD-COMM
network 177.44.105.0/25 route-policy ADD-COMM
network 177.44.105.128/25 route-policy ADD-COMM
network 177.44.111.128/25 route-policy ADD-COMM
network 177.130.132.0/25 route-policy ADD-COMM
network 177.130.132.0/25 route-policy ADD-COMM
network 177.130.132.128/25 route-policy ADD-COMM
network 177.130.133.0/25 route-policy ADD-COMM
network 177.130.133.0/25 route-policy ADD-COMM
network 177.130.133.128/25 route-policy ADD-COMM
[~DVL-HED-NEV-01]bgp-af-ipv4]network 191.240.92.172 30 route-policy ADD-COMM
network 191.240.92.172 255.255.255.252 route-policy ADD-COMM
```

Command:

```
sys
bgp 28202 //entra na configuração do BGP (28202 é o asn da Master)
ipv4-family unicast //entra na pasta de ipv4 do BGP
dis this //mostra as configurações do local onde está
network 191.240.0.0 30 route-policy ADD-COMM //divulga o bloco no protocolo BGP, com os filtros da policy
```

6- Permitir o IP no prefixo criado para BRE e BHE quando houver. (No exemplo estou usando o DVL-HED-NEV)

```
[~DVL-HED-NEV-01]dis cu | in ip-prefix
ip ip-prefix BHE-20Gb-DWDM-EXPORT index 2860 permit 191.240.81.60 30
ip ip-prefix BHE-20Gb-DWDM-EXPORT index 2870 permit 191.53.156.0 22 greater-equal 22 less-equal 30
ip ip-prefix BHE-20Gb-DWDM-EXPORT index 2880 permit 191.53.126.160 30
ip ip-prefix BRE-20Gb-DWDM-EXPORT index 10 permit 191.240.92.12 30 greater-equal 30 less-equal 32
ip ip-prefix BRE-DVL-ELT-EXPORT index 930 permit 186.216.124.0 22
ip ip-prefix BRE-DVL-ELT-EXPORT index 960 permit 186.216.80.80 30
ip ip-prefix BRE-DVL-ELT-EXPORT index 980 permit 177.44.72.0 22 greater-equal 22 less-equal 32
ip ip-prefix BRE-DVL-ELT-EXPORT index 1000 permit 189.91.20.0 22 greater-equal 22 less-equal 32
ip ip-prefix BRE-DVL-ELT-EXPORT index 1020 permit 189.91.28.0 22 greater-equal 22 less-equal 32
ip ip-prefix BRE-DVL-ELT-EXPORT index 1030 permit 191.53.180.0 22
ip ip-prefix BRE-DVL-ELT-EXPORT index 1040 permit 191.53.184.0 21
ip ip-prefix BRE-DVL-ELT-EXPORT index 1050 permit 191.53.196.0 22
ip ip-prefix BRE-DVL-ELT-EXPORT index 1070 permit 191.53.204.0 22
ip ip-prefix BRE-DVL-ELT-EXPORT index 1120 permit 191.53.188.0 22 greater-equal 22 less-equal 24
[~DVL-HED-NEV-01]ip ip-prefix BHE-20Gb-DWDM-EXPORT permit 191.240.92.172 30
[~DVL-HED-NEV-01]ip ip-prefix BRE-20Gb-DWDM-EXPORT permit 191.240.92.172 30
```

Command:

```
sys
dis cu | in ip-prefix
ip ip-prefix BHE-20Gb-DWDM-EXPORT permit 191.240.0.0 30 //permite o ip no prefix criado para BHE
ip ip-prefix BRE-DVL-ELT-EXPORT permit 191.240.0.0 30 //permite o ip no prefix criado para BRE
```

7- Commit para aplicar as configurações e run save para salvar na memória flash.

```
[~DVL-HED-NEV-01]commit  
[~DVL-HED-NEV-01]run save  
Warning: The current configuration will be written to the device.  
Are you sure to continue? [Y/N]:y  
Now saving the current configuration to the slot 3 ..  
Info: Save the configuration successfully.
```

Command:

```
commit  
run save  
yes
```

Finalizado você já irá conseguir ping para o IP setado na sub-interface (Quando esse IP for um ip válido do bloco divulgado) via internet, pois seu bloco de IP já estará divulgado nos Upstreams .

```
C:\Users\Master>ping 191.240.92.173  
  
Disparando 191.240.92.173 com 32 bytes de dados:  
Resposta de 191.240.92.173: bytes=32 tempo=4ms TTL=254  
Resposta de 191.240.92.173: bytes=32 tempo=2ms TTL=254  
Resposta de 191.240.92.173: bytes=32 tempo=1ms TTL=254  
Resposta de 191.240.92.173: bytes=32 tempo=2ms TTL=254
```

Configurações de rota estática com IP válido e IP de enlace no NE

Descrição: Utilizamos este tipo de configuração quando o cliente deseja utilizar o “Bloco de IP completo”, mas esse tipo de configuração apenas libera 1 IP válido a mais para o cliente, que no caso seria o IP válido que seria configurado na sub-interface como gateway.

Ex: Cliente possui o IP 191.240.92.172/30.

Então para configurarmos a rede do cliente da forma convencional, o IP 191.240.92.172 é o IP de networking que serve para divulgação do bloco na internet, o IP 191.240.92.173 seria usado na sub-interface como gateway para comunicar com o IP 191.240.92.174 que seria setado no equipamento do cliente na ponta final para fechar a comunicação cliente <> roteador, e, por fim, o IP 191.240.92.175 é o IP de broadcast.

Se o cliente solicitasse 2 Ips válidos para utilizar da maneira que desejar, faríamos o enlace cliente <> roteador com IPs falsos, por exemplo 172.16.25.0/30, onde seria setado o IP 172.16.25.1 na sub-interface do roteador e o IP 172.16.25.2 no lado do cliente, sendo que agora ele poderia utilizar como IP válido tanto o 191.240.92.173 quanto o 191.240.92.174 em seus equipamentos, sendo que o gateway seria o 172.16.25.1 (O IP setado na sub-interface).

- 1- A configuração de IP da sub-interface será o segundo IP do bloco de enlace. (Ex: Bloco de enlace: 172.25.16.0/30) a configuração na sub-interface seria:

Command:

```
sys  
interface eth-trunk0.10          //criar a sub-interface, no exemplo seria para a vlan 10  
vlan-type dot1q 10              //definir a vlan 10 na sub-interface  
ip address 172.25.16.1 30        //setando o ip de gateway do cliente /30  
statistic enable                //habilita a coleta de estatísticas  
ip netstream inbound            //habilita a coleta de estatísticas de tráfego de entrada nesta interface
```

- 2- As demais configurações se mantém, faltando apenas a configuração da rota estática onde apontamos o bloco válido para o bloco de enlace, funcionando como uma “extensão da sub-rede”

Command:

```
sys  
ip route-static 191.240.92.172 30 172.25.16.2      //apontando o bloco válido para o IP de enlace que será setado do lado do cliente.
```

CONFIGURAÇÕES GFW (FREE-BSD)

Descrição: A configuração do GFW segue a mesma lógica que o NE, afinal, ambos tem a mesma função, realizar a comunicação de sub-redes distintas. A diferença é que no GFW a configuração é parecida com a navegação em linux onde você precisa acessar diretórios e digitar o texto (comando) dentro de uma parte destes diretórios para que funcione as configurações.

- 1- O primeiro diretório que precisamos acessar pode ser diferente em cada GFW da rede. Primeiro devemos acessar a pasta “ee /etc/start_if.xxxxx” onde no lugar do x seria uma pasta específica no GFW. Para descobrir qual pasta correta devemos aplicar as primeiras configurações, basta digitarmos “ee /etc/start_if.” e apertar a tecla tab para identificar as opções de diretórios, e entrar em um por um até achar as configurações de outros clientes.

```
root@VGA-HED-GFW-01:~ # ee /etc/start_if.  
start_if.em0  start_if.em1  start_if.ix0  start_if.ix1
```

```
root@VGA-HED-GFW-01:~ # ee /etc/start_if.em0  
^[[ (escape) menu ^y search prompt ^k delete Line ^p prev li ^g prev page  
^o ascii code ^x search ^l undelete Line ^n next li ^v next page  
^u end of file ^a begin of Line ^w delete word ^b back 1 char  
^t top of text ^e end of Line ^r restore word ^f forward 1 char  
^c command ^d delete char ^j undelete char ^z next word  
====Line 1 col 0 lines from top 1 =====  
/sbin/ifconfig em0 up
```

```
root@VGA-HED-GFW-01:~ # ee /etc/start_if.em1  
^[[ (escape) menu ^y search prompt ^k delete Line ^p prev li ^g prev page  
^o ascii code ^x search ^l undelete Line ^n next li ^v next page  
^u end of file ^a begin of Line ^w delete word ^b back 1 char  
^t top of text ^e end of Line ^r restore word ^f forward 1 char  
^c command ^d delete char ^j undelete char ^z next word  
====Line 1 col 0 lines from top 1 =====  
/sbin/ifconfig em1 up
```

```
root@VGA-HED-GFW-01:~ # ee /etc/start_if.ix0  
^[[ (escape) menu ^y search prompt ^k delete Line ^p prev li ^g prev page  
^o ascii code ^x search ^l undelete Line ^n next li ^v next page  
^u end of file ^a begin of Line ^w delete word ^b back 1 char  
^t top of text ^e end of Line ^r restore word ^f forward 1 char  
^c command ^d delete char ^j undelete char ^z next word  
====Line 1 col 0 lines from top 1 =====  
/sbin/ifconfig ix0  
/sbin/ifconfig lag1 create  
/sbin/ifconfig lag1 lagproto lacp lagport ix0 lagport ix1  
/sbin/ifconfig lag1 up  
/sbin/ifconfig vlandev create  
/sbin/ifconfig vlandev285 191.240.1.129/27 vlandev 3285 vlandev tagg1  
/sbin/ifconfig vlandev389 191.240.3.147/29 vlandev 3789 vlandev tagg1  
/sbin/ifconfig vlandev60 create  
/sbin/ifconfig vlandev60 191.240.1.24 vlandev 60 vlandev tagg1  
/sbin/ifconfig vlandev30 create  
/sbin/ifconfig vlandev30 10.30.0.1/24 vlandev 30 vlandev tagg1  
/sbin/ifconfig vlandev51 create  
/sbin/ifconfig vlandev51 191.240.111.113/30 vlandev 151 vlandev tagg1  
#B28 | AMPLA | ID 110871-134741 | FTTH  
/sbin/ifconfig vlandev64 create  
/sbin/ifconfig vlandev64 191.240.111.165/30 vlandev 164 vlandev tagg1  
#B28 | TRES MARIAS | ID 135101-134801 | FTTH  
/sbin/ifconfig vlandev77 create  
/sbin/ifconfig vlandev77 191.240.111.205/30 vlandev 177 vlandev tagg1
```

Neste caso o ix0 é o correto.

2- Após acessar a pasta correta, navegamos pelas setas do teclado até a última configuração de cliente, damos um enter e digitamos na linha abaixo.

Nesta pasta, como analogia ao NE, seria a sub-interface. Nela iremos criar a vlan e setar o IP de gateway em cima da mesma vlan.

As linhas que estão escritas iniciando com um # significa comentário e não aplica nenhuma alteração.

As linhas sem # são os comandos de fato.

Como os comandos são os mesmos para qualquer cliente, só irá alterar a vlan e IP, primeiramente faremos a descrição para o cliente que será configurado e na linha abaixo faremos as configurações da vlan e IP exatamente como os anteriores, mudando apenas vlan e IP.

```
#CLI | IPD | VENTURI | 1059605 | 1GB
/sbin/ifconfig wlan215 create
/sbin/ifconfig wlan215 172.25.17.85/30 wlan 215 vlandev lagg1

#|CLI | B2B | REX | IPD-VGA-000-1062537 | 100MB
/sbin/ifconfig wlan290 create
/sbin/ifconfig wlan290 191.53.126.97/29 wlan 290 vlandev lagg1

#CLI | IPD | STONEX | 1063633 | 50MB
/sbin/ifconfig wlan216 create
/sbin/ifconfig wlan216 191.53.126.193/30 wlan 216 vlandev lagg1
```

Command:

```
#CLI | IPD | STONEX | 1063633 | 50MB          //descrição do cliente que será configurado abaixo
/sbin/ifconfig wlan216 create                  //cria a vlan 216 no diretório
/sbin/ifconfig wlan216 191.53.126.193/30 wlan 216 vlandev lagg1 //setar o IP de gateway em cima da vlan
```

Obs: Para sair do diretório e salvar, apertar a tecla ESC e irá aparecer uma caixa de opções, a, a novamente. Ou se a tecla ESC não funcionar, CTRL C, digitar exit e clicar na tecla enter.

O teclado numérico pode bugar o Sistema enquanto estiver passando as configurações. Sempre preferir pelos números que ficam acima das letras no teclado.

3- Quando saímos da pasta, voltamos a raiz do GFW, onde nela iremos repetir os dois comandos de criação da vlan e do IP de gateway novamente.

Command:

```
/sbin/ifconfig wlan216 create          //cria a vlan 216 no diretório
/sbin/ifconfig wlan216 191.53.126.193/30 wlan 216 vlandev lagg1 //setar o IP de gateway em cima da vlan
```

4- Agora irá faltar apenas a configuração do BGP, da mesma forma que o NE. Teremos que divulgar o bloco do cliente, e permitir ele nos prefixos criados. Para isso devemos acessar a pasta “ee /usr/local/etc/bgpd.conf”.

```
root@VGA-HED-GFW-01:~# ee /usr/local/etc/bgpd.conf
[[ (escape) menu ^y search prompt ^k delete line ^p prev li ^g prev page
^o ascii code ^x search ^l undelete line ^n next li ^v next page
^u end of file ^a begin of line ^w delete word ^b back 1 char
^t top of text ^e end of line ^r restore word ^f forward 1 char
^c command ^d delete char ^j undelete char ^z next word
===== line 1 col 0 lines from top 1 =====
AS 28202
Holdtime 90
Listen on 191.240.3.145
router-id 191.240.1.140

#Tecnologia_Fibra
#Classes /22
#RB_FTTH 1
network 191.53.172.0/22

#Classes /23
#RB_FTTH 1
network 179.189.176.0/23
network 191.53.172.0/23
network 191.53.174.0/23
network 191.240.26.0/23
#RB_FTTH 2
network 179.189.176.0/23

#Classes /24
#RB_FTTH 1
network 177.44.19.0/24
network 179.189.176.0/24
network 179.189.177.0/24
network 191.53.172.0/24
network 191.53.173.0/24
network 191.53.174.0/24
network 191.53.175.0/24
network 191.240.26.0/24
network 191.240.27.0/24

#Classes /24
#RB_FTTH 2
```

Navegar pela seta do teclado até o comentário onde estão as configurações de B2B.

```
##### CLIENTES_B2B_FTTH #####
##CLIENTE_B2B_LIV
network 191.240.111.72/29
##CLIENTE_B2B_STCRED | 134321
network 191.240.111.112/30
#CLIENTE_B2B_AMPLA_ID 110871-134741 | FTTH
network 191.240.111.164/30
#CLIENTE_B2B_TRES_MARIAS | ID 135101-134801 | FTTH
network 191.240.111.204/30
#CLI_B2B_GLUCIO-RETIFICA-MOTORES | IPD-VGA-13606-135971
network 191.240.111.8/29

#CLI_B2B_AMG | IPD-VGA-000-149581 | 20M
network 186.216.80.124/30
#B2B_TELLEGROUP | IPD-VGA-000-155191 | 20M
network 186.216.96.12/30
#CLI_B2B_NKG | IPD-VGA-000-156091 | 500M
network 186.216.96.88/29
#CLI_B2B_CENTURYTELECOM | IPD-VGA-000-158301 | 50M
network 186.216.96.216/30
#CLI_B2B_SUCAFINA_BRASIL | IPD-VGA-000-159101 | 300M
network 186.216.97.8/29

#CLI_B2B_SICOOB_CREDIVAR | IPD-VGA-000-162401 | 150M
network 186.216.97.224/29
#CLI_B2B_CENTURYTELECOM | IPD-VGA-000-162491 | 30M
network 186.216.97.201/29
#CLI_B2B_NAVA_SERVICOS | IPD-VGA-000-162981 | 20M
network 186.216.97.232/30
#CLI_B2B_NOVA_SAFRA | IPD-VGA-000-163231 | 100M
network 186.216.97.248/30
#CLI_B2B_PAULO_EDIBERTO | IPD-VGA-000-163541 | 20M
network 186.216.110.148/30
```

Continuar descendo até o ultimo cliente configurado dentro deste comentário, apertar enter e dar a descrição e divulgar o bloco do cliente que estiver configurando.

```
===== line 265 col 0 lines from top 265 =====
#CLI_IPD_TOWER | 1051137 | 50MB
network 191.240.92.224/30

#CLI_IPD_TOWER | 1051143 | 50MB
network 191.240.92.228/30
#CLI_IPD_BRASIL_TECPAR | 1052546 | 20MB
network 191.240.93.12/30
#CLI_IPD_CREDIVAR | 168631 | 30MB
network 191.240.93.60/30

#CLI_IPD_PLASCAR | 1053962 | 200MB
network 191.240.93.56/30

#CLI_IPD_VENTURI | 1059605 | 1GB
network 191.240.93.152/29
#[CLI_B2B_REX | IPD-VGA-000-1062537 | 100MB]
network 191.53.126.96/30
#CLI_IPD_STONEX | 1063633 | 50MB
network 191.53.126.192/30
```

Command:

```
#CLI_IPD_STONEX | 1063633 | 50MB //descrição do cliente
network 191.53.126.92/30 //divulga o Bloco do cliente no BGP
```

- 5- Continuar descendo pela seta do teclado até chegar na configuração de prefixos (Cada GFW terá configurações de prefixos diferentes, basta se basear pelos clientes que já estão funcionando).**

```
##### CMG NE20 BHE #####
allow to 191.240.3.145 prefix 191.240.26.0/23 prefixlen 23 - 32 set { community 28202:310 community 28202:359 community 28202:3592 }
allow to 191.240.3.145 prefix 191.53.172.0/23 prefixlen 22 - 32 set { community 28202:310 community 28202:359 community 28202:3592 }
allow to 191.240.3.145 prefix 177.44.19.0/24 prefixlen 24 - 32 set { community 28202:310 community 28202:359 community 28202:3592 }
allow to 191.240.3.145 prefix 179.189.176.0/23 prefixlen 23 - 32 set { community 28202:310 community 28202:359 community 28202:3592 }

### RB_FTTB_2 ###
allow to 191.240.3.145 prefix 179.189.184.0/24 prefixlen 24 - 32 set { community 28202:310 community 28202:359 community 28202:3592 }
allow to 191.240.3.145 prefix 179.189.161.0/24 prefixlen 22 - 32 set { community 28202:310 community 28202:359 community 28202:3592 }
allow to 191.240.3.145 prefix 179.189.162.0/24 prefixlen 24 - 32 set { community 28202:310 community 28202:359 community 28202:3592 }
allow to 191.240.3.145 prefix 179.189.163.0/24 prefixlen 24 - 32 set { community 28202:310 community 28202:359 community 28202:3592 }
allow to 191.240.3.145 prefix 179.189.176.0/23 prefixlen 23 - 32 set { community 28202:310 community 28202:359 community 28202:3592 }

### RB_WIRELESSES ###
allow to 191.240.3.145 prefix 177.44.24.0/22 prefixlen 22 - 32 set { community 28202:310 community 28202:359 community 28202:3592 }
allow to 191.240.3.145 prefix 177.130.160.0/22 prefixlen 22 - 32 set { community 28202:310 community 28202:359 community 28202:3592 }
allow to 191.240.3.145 prefix 187.120.96.0/23 prefixlen 23 - 32 set { community 28202:310 community 28202:359 community 28202:3592 }
allow to 191.240.3.145 prefix 191.53.16.0/21 prefixlen 21 - 32 set { community 28202:310 community 28202:359 community 28202:3592 }
allow to 191.240.3.145 prefix 191.53.116.0/22 prefixlen 22 - 32 set { community 28202:310 community 28202:359 community 28202:3592 }

### B2B_RB_FTTB_1 ###
#FIBRA | B2B-LIV
allow to 191.240.3.145 prefix 191.240.111.72/29 set { community 28202:310 community 28202:359 community 28202:3592 }
#PLASCAR | ID 1053962 | 200MB
allow to 191.240.3.145 prefix 191.240.111.112/30 set { community 28202:310 community 28202:359 community 28202:3592 }
#CLIENTE_B2B | AMPLA | ID 110871-134741 | FTTH
allow to 191.240.3.145 prefix 191.240.111.164/30 set { community 28202:310 community 28202:359 community 28202:3592 }
#CLIENTE_B2B | TRES_MARIAS | ID 135101-134801 | FTTH
allow to 191.240.3.145 prefix 191.240.111.204/30 set { community 28202:310 community 28202:359 community 28202:3592 }
```

No exemplo acima temos o prefixo CMG NE20 BHE, descemos até o comentário onde estão os B2Bs, vamos até o último configurado, teclar enter e configurar na linha abaixo.

```
allow to 191.240.3.145 prefix 191.240.93.60/30 set { community 28202:310 community 28202:359 community 28202:3592 }
#CLT | IPD | PLASCAR | 1053962 | 200MB
allow to 191.240.3.145 prefix 191.240.93.56/30 set { community 28202:310 community 28202:359 community 28202:3592 }
#CLT | IPD | VENTURI | 1059605 | 16GB
allow to 191.240.3.145 prefix 191.240.93.152/30 set { community 28202:310 community 28202:359 community 28202:3592 }
#|CLI | B2B | REX | IPD-VGA-000-1062537 | 100MB
#|CLI | IPD | STONEX | 1063633 | 50MB
allow to 191.240.3.145 prefix 191.53.126.192/30 set { community 28202:310 community 28202:359 community 28202:3592 }
```

Command:

```
#CLI | IPD | STONEX | 1063633 | 50MB // descrição do cliente
allow to 191.230.3.145 prefix 191.53.126.92/30 set { community 28202:310 community 28202:359 community 28202:3592 } // permite o bloco do cliente no prefixo 191.230.3.145 (cada GFW terá prefixos diferentes e Community diferentes, devemos nos basear pelos outros clientes que já estão configurados, e usar o mesmo, alterando apenas o IP do cliente.
```

- 6- Após configurar o diretório do BGP, devemos sair e salvar. E executar o comando “bgpctl reload”. Para rodar as configurações aplicadas. Neste momento se estiver tudo certo, teremos que ter ping para o IP de gateway setado na pasta start_if.**

Command:

```
bgpctl reload //aplica a configuração realizada
```

Obs: Se tiver algo errado, letra faltando, IP sem barramento ou algo do tipo, quando executar o comando acima ou ele dará erro, ou aplicará a configuração incorreta e poderá gerar loop e falhas na rede.

Configurações de rota estática com IP válido e IP de enlace no GFW

- 1- Na configuração da pasta start_if teremos que setar o IP do enlace.

Command:

```
#CLI | IPD | STONEX | 1063633 | 50MB          // descrição do cliente que será configurado abaixo  
/sbin/ifconfig wlan216 create                 // cria a vlan 216 no diretório  
/sbin/ifconfig wlan216 172.25.16.1/30 wlan 216 vlandev lagg1 // setar o IP de gateway em cima da vlan
```

- 2- Na raiz teremos que executar o seguinte comando para apontar o Bloco válido para o IP de enlace:

Command:

```
/sbin/route add -net 191.240.92.172/30 172.25.16.2 // aponta o IP válido 191.240.92.172/30 para o IP 172.25.16.2
```

- 3- Acessar a pasta ee /etc/rc.local, descer até a última linha, teclar enter e setar:

Command:

```
#CLI | IPD | STONEX | 1063633 | 50MB          // descrição do cliente que será configurado abaixo  
/sbin/route add -net 191.240.92.172/30 172.25.16.2 // aponta o IP válido 191.240.92.172/30 para o IP 172.25.16.2
```

SWITCH

As configurações realizadas nos switchs para os B2Bs são basicamente comunicação de camada 2, mais especificamente VLAN (Virtual Local Área Network), VPLS (Serviço de comunicação ponto-multi-ponto do protocolo MPLS, que utiliza a VSI), VPWS (Serviço de comunicação ponto-a-ponto do protocolo MPLS, que utiliza o L2VC para criar túneis diretos através da rede).

Conceito básico de VLAN:

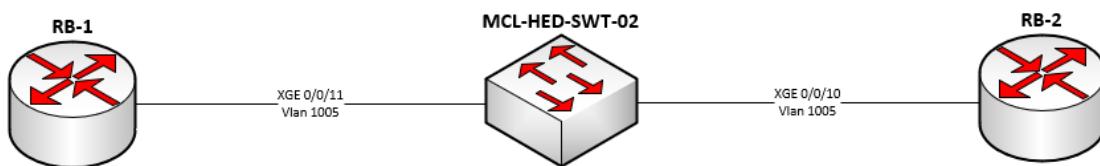
- VLAN é uma rede local virtual que permite a passagem do tráfego de forma segmentada utilizando um VID (Identificação única da vlan, o valor pode variar de 1 a 4094 isso significa que pode haver até 4094 vlans em uma rede).

Temos algumas formas de configurar uma Vlan, tagged, untagged (access), qinq (encapsulamento de vlans), transparent (Utilizado em OLTs).

As configurações que mais utilizamos nos switchs são:

Tagged: quando aplicamos uma vlan como tagged, a próxima interface também terá que ter essa vlan em tagged para dar continuidade na propagação do tráfego segmentado.

QinQ (que também se trata de uma vlan untagged ou access): Esta configuração é utilizada para encapsular vlans dentro de uma vlan de serviço específica. Exemplo: Temos a seguinte topologia



Onde na interface XGE 0/0/11 configuramos uma ponta do QinQ sendo a configuração:

```
interface xg 0/0/11  
port link-type dot1q-tunnel  
port default vlan 1005
```

E na porta xg 0/0/10 configuramos a outra ponta do QinQ da mesma maneira.

Dessa forma se o cliente quisesse configurar as vlans 10, 11, 12, 13, e 14 na RB-1 e também na RB-2, ele conseguiria passar cada tráfego segmentado de cada vlan encapsulado dentro da vlan 1005 na nossa rede. Em resumo, para Master existe apenas a vlan 1005, já para o cliente poderia existir todas as 4094 vlans, da maneira que ele quisesse.

Uma boa analogia para entender o QinQ seria um cano de água ou então um Túnel de uma rodovia. Se realizarmos a configuração em apenas uma das pontas, não teremos saída ou entrada do outro lado, então os carros apenas entrariam no tunel e não teriam saída do outro lado.

Obs: Essa configuração de QinQ passada acima serve para switchs huawei.

Em resumo, uma analogia fácil de ser usada para uma VLAN seria um cabo físico. Para que tenhamos uma conexão de uma ponta “a” até uma ponta “b”, precisamos de um cabo ligando-as. Porém como faríamos pra ter um cabo específico ligando essas pontas se temos muitos equipamentos entre elas? Então utilizamos a VLAN, que nada mais é que um cabo virtual.

- Conceitos básicos de VPLS (vsi):

Neste serviço, utilizamos um protocolo que já está em uso na rede, que é o MPLS. Este protocolo serve para comutação de pacotes baseado em Labels (Uma identificação dada pelo protocolo LDP para cada equipamento na rede). O protocolo MPLS por si só já utiliza um protocolo de roteamento anterior a ele que estiver ativo, como OSPF, BGP, IS-IS, mas para um conceito básico isso poderá confundir.

Basicamente o serviço VPLS utiliza a VSI para fechar comunicações que tomam decisão de melhor caminho para se encaminhar o tráfego na rede MPLS e fechar a comunicação de um ponto “a” com um ponto “b”, ou um ponto “a” com pontos “b”, “c” e “d”. Por isso o termo ponto-multi-ponto. Como a configuração da VSI deve ser feita uma interface vlanif (interface L3) para que a comunicação de uma VSI funcione, primeiramente a VLAN do cliente deve estar configurada em uma porta física que esteja UP, pois se a porta física estiver down, mesmo configurando a VSI, não irá comunicar.

Para que uma VSI encontre a outra na rede MPLS devemos configurar igualmente tanto em um ponto quanto no outro, isso quando utilizado o BGP interno que já está configurado em todos os switchs MPLS. Exemplo:

```
vsi BHE<>QUALQUER
bgp-ad                                //utilizar o bgp como parâmetro
vpls-id 65037:441
vpn-target 65037:441 import ext-community
vpn-target 65037:441 export ext-community
```

Se fosse usado a configuração acima, teríamos que replicar a mesma VSI com exatamente as mesmas configurações para fechar comunicações na rede MPLS.

Ou então poderíamos configurar a VSI utilizando o parâmetro pwsignal onde especificamos os peers que a VSI deverá fechar a comunicação.

Exemplo: Vamos simular uma VSI que comunicaria BHE com BRE e com DVL.

Em BHE seria configurado:

```
vsi BHE<>QUALQUER
pwsignal ldp
vsi-id 44124
peer 172.16.255.0                      //colocamos o IP do switch que queremos comunicar
peer 172.16.255.5                      //colocamos o IP do switch que queremos comunicar
```

Em DVL seria configurado:

```
vsi BHE<>QUALQUER
pwsignal ldp
vsi-id 44124
peer 172.16.255.4                      //colocamos o IP do switch que queremos comunicar
```

Em BRE seria configurado:

```
vsi BHE<>QUALQUER
pwsignal ldp
vsi-id 44124
peer 172.16.255.4                      //colocamos o IP do switch que queremos comunicar
```

Dessa forma fecharíamos uma comunicação BHE<>BRE e BHE<>DVL utilizando a mesma VSI. As vantagens da utilização da VSI é conseguir aprender MAC em cima da VSI, a comunicação multi ponto e comutação de rotas MPLS quando necessário de forma automática.

- Conceitos básicos de VPWS (L2VC):

O L2VC é utilizado para comunicação ponto a ponto, ou seja, ele é utilizado quando você deseja ligar uma ponta “a” até uma ponta “b”, sem a necessidade de mais pontos.

Exemplo de configuração: BHE <> BRE

Em BHE

```
interface vlanif 441
desc BHE<>BRE-RYAN
mpls l2vc 172.16.255.5 44124 //seta o IP do proximo dispositivo e um identificador
mpls l2vpn flow-label both //permite a passagem de entrada e saída de tráfego
```

Em BRE

```
interface vlanif 441
desc BHE<>BRE-RYAN
mpls l2vc 172.16.255.4 44124 //seta o IP do proximo dispositivo e o identificador
mpls l2vpn flow-label both //permite a passagem de entrada e saída de tráfego
```

A vantagem do VPWS é a facilidade de manipulação de tráfego devido a ser uma comunicação que liga apenas 2 pontos.

Levando em conta que as configurações nos switchs se tratam de propagar vlans, temos algumas formas de configurações de portas para que isso seja possível. São elas:

- Port link-type trunk :

É a configuração mais comum que veremos nos switchs da rede Master. O tipo trunk permite que a interface transporte várias tags de vlans. Dessa forma ela é utilizada para transportar muitas vlans em tag em uma única interface. Mas também conseguimos utilizar uma vlan em untagged, sendo que, todo tráfego com alguma tag vlan consiga passar com suas respectivas tags porém o tráfego sem uma tag vlan seria destinado a vlan configurada para isso.

Exemplo de configuração:

```
interface xgigabitethernet 0/0/1
port link-type trunk
port trunk allow pass vlan 15 16 17
port trunk pvid vlan 10
```

Nessa configuração, os equipamentos que tiverem as vlans 15, 16 e 17 seriam encaminhadas com suas tags normalmente, porém o tráfego sem uma vlan específica seria direcionado a vlan 10, e a partir desta interface este tráfego estaria na vlan 10 para o restante da rede.

- **Port link-type access:**

Comum em interfaces de torres ou rede wireless. Este tipo de configuração define que a interface está em modo acesso, ou seja, os clientes conectados neste tipo de interface não precisam configurar vlans em seus equipamentos, pois todo o tráfego que chega na interface é destinado a vlan configurada como default. Exemplo de configuração:

```
interface xgigabitethernet 0/0/1
port link-type access
port default vlan 15
quit
```

Nessa configuração o tráfego sem tag vlan seria destinado a vlan 15.

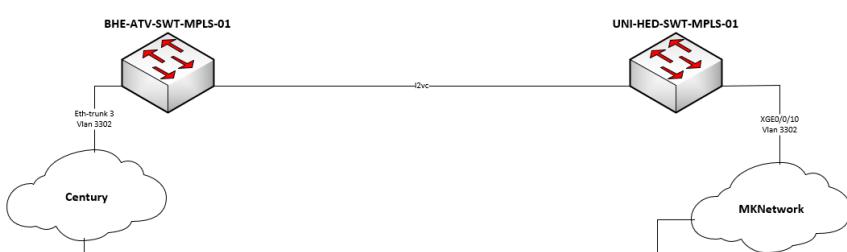
- **Port link-type hybrid:**

Neste modo a interface poderá funcionar tanto como trunk quanto access, sendo que será possível configurar várias vlans em untagged e várias vlans em tagged.

Configurações de Switch:

A configuração que realizamos nos switchs é fechar a comunicação de camada 2 do roteador até o cliente (quando é o produto IP Dedicado), ou de uma ponta “a” até uma ponta “b” (quando o produto é um LTL), utilizando as ferramentas apresentadas acima.

Vamos utilizar a seguinte topologia de exemplo:



BHE-ATV-SWT-MPLS-01:

```

vlan batch 3302 //criar vlan no switch
vlan 3302 //entrar na vlan
desc EXEMPLO-B2B //adicionar uma descrição para vlan
q //sair da configuração da vlan

interface eth-trunk 3 //entrar na interface
desc NNI-CENTURY //adicionar uma descrição para interface
port link-type trunk //definir um tipo para porta (trunk permite passagem de várias vlans)
port trunk allow-pass vlan 3302 //passar vlan 3302 na porta em tagged
q //sair da configuração da porta

interface vlanif 3302 //criar uma interface vlanif (uma interface virtual para a vlan especificada)
mpls l2vc 172.16.255.30 330224 //adicionar o serviço VPWS na interface.
mpls l2vpn flow-label both //permitir a passagem de entrada e saída de tráfego nesta instância do VPWS.
q
  
```

UNI-HED-SWT-MPLS-01

```

vlan batch 3302 //criar vlan no switch
vlan 3302 //entrar na vlan
desc EXEMPLO-B2B //adicionar uma descrição para vlan
q //sair da configuração da vlan

traffic classifier EXEMPLO-B2B //criar uma classificação de tráfego (Um nome para um tráfego específico)
if-match vlan 3302 //definir qual tráfego terá a classificação criada
q //sair do classifier criado

traffic behavior EXEMPLO-B2B //criar um comportamento no switch (porém ainda não atrelou a nada)
car cir 102400 pir 102400 green pass yellow pass red discard //definir um limite de tráfego de 100MB (o valor deve ser colocado em KBPS)
statistic enable //habilitar coleta de estatísticas no comportamento
q //sair do comportamento criado

traffic policy EXEMPLO-B2B //criar uma regra
classifier EXEMPLO-B2B behavior EXEMPLO-B2B //definir que a classificação criada terá o comportamento criado
q //sair da regra

interface xg 0/0/10 //entrar na interface
port link-type trunk //definir um tipo para porta (trunk permite passagem de várias vlans)
port trunk allow-pass vlan 3302 //passar vlan 3302 na porta em tagged
traffic-policy EXEMPLO-B2B inbound //atrelar a regra criada para entrada de tráfego
traffic-policy EXEMPLO-B2B outbound //atrelar a regra criada para saída de tráfego
q //sair da interface

interface vlanif 3302 //criar uma interface vlanif (uma interface virtual para a vlan especificada)
mpls l2vc 172.16.255.4 330224 //adicionar o serviço VPWS na interface (o IP deve ser do outro switch)
mpls l2vpn flow-label both //permitir a passagem de entrada e saída de tráfego nesta instância do VPWS.
q

run save //salvar a configuração aplicada na memória pra quando reiniciar manter
yes //confirmar o save
  
```

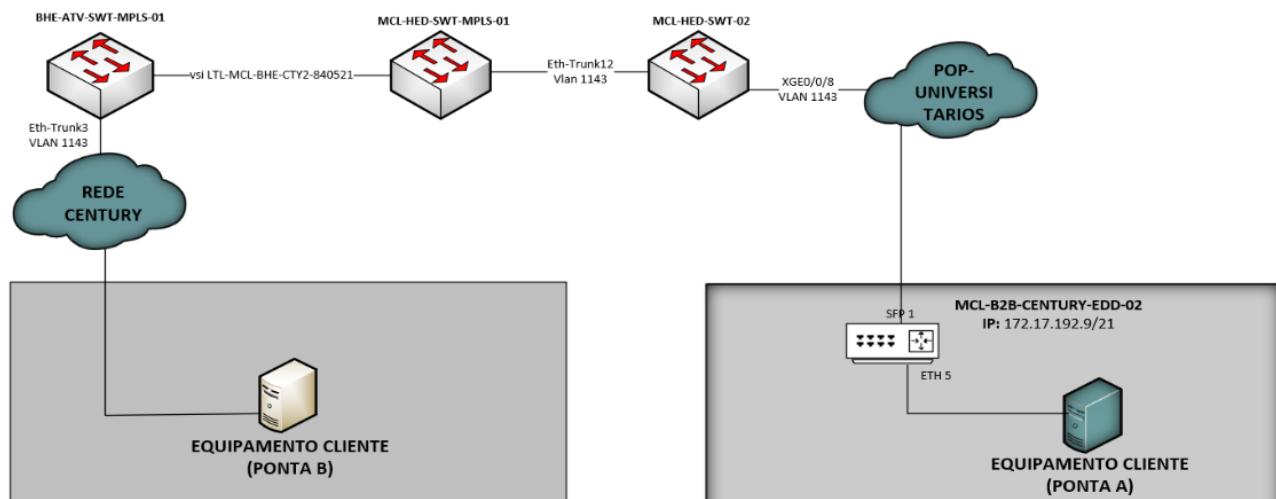
CONFIGURAÇÕES DE SWITCH DATACOM (EDD)

O EDD pode ser utilizado de várias formas. O principal motivo do uso é a coleta de snmp, para monitoramento do “ativo” final na ponta do cliente e também permite a utilização de algumas configurações de portas, formas de configurar vlans, etc.

Como o nome já diz, o EDD é um switch, sendo assim, utilizado para comunicação de camada 2 para o cliente. Vamos para as configurações:

O exemplo de configuração será baseado na seguinte topologia:

REDE NACIONAL DE ENSINO E PESQUISA – MONTES CLAROS – LTL-MCL-BHE-840521 1GB



Será abordado apenas a configuração do EDD, visto que as configurações dos demais switchs já foi explicada. A configuração básica feita para os clientes se resume em configurar gerência, vlans, interfaces e snmp.

Configurações de EDD 2104 (1GB)

Conectar via cabo console.

User: admin
Password: admin

Configurações de nome e horário

```
configure //entrar no modo de configuração
hostname MCL-B2B-1061251-EDD-01 //dar nome ao dispositivo
clock timezone BRA -3 //definir fuso horário
exit //sair do modo de configuração
clock set 10:00:00 07 10 2024 //definir horário
```

Configurações de usuário

```
configure //entrar no modo de configuração
username nocuser access-level 15 //criar usuário “nocuser” com acesso full
username nocuser password 0 %%NoC.2018 //definir senha para o user “nocuser” sem criptografia “password 0”
```

Configurações de acesso remoto

```
no ip telnet server //desabilitar o acesso telnet (telnet é um acesso não seguro)
no ip http secure-server //desabilitar o acesso web
ip ssh host-key generate dsa //gerar chave para acesso seguro (ssh)
ip ssh server //habilitar acesso seguro (ssh)
```

Configurações de SNMP (coleta de dados)

```
ip snmp-server //habilitar o snmp do EDD
ip snmp-server location Montes Claros //definir a localização do SNMP como "Montes Claros"
ip snmp-server community McxMCL@RNP //criar community para puxar dados SNMP
```

Configuração de Vlan

```
interface vlan 1143 //criar e entrar na vlan
name LTL-MCL-BHE-840521 //definir descrição para vlan
set-member tagged ethernet 1/1 //setar a vlan como tagged na interface
set-member untagged ethernet 1/5 //setar a vlan como untagged (access) na interface
exit //sair da configuração da vlan
```

Configuração de Gerência

```
interface vlan 2635 //criar e entrar na vlan
name GER-CLIENTES-B2B-MCL //definir descrição para vlan
ip address 172.17.192.9/21 //definir ip de gerência
set-member tagged ethernet 1/1 //setar a vlan como tagged na interface que chega o link
exit //sair da configuração da vlan
ip default-gateway 172.17.192.1 //definir o gateway da gerência (Esse IP fica na sub-interface do NE20
de DVL, que permite que tenhamos a gerência da rede do NOC)
```

Configuração de interfaces

```
interface ethernet 1/1 //entrar na interface
no shutdown //habilitar a interface (retirar o shutdown)
description LINK-B2B-RNP-EDD //definir descrição para a interface
exit //sair da interface

interface ethernet 1/5 //entrar na interface
no shutdown //habilitar interface (retirar o shutdown)
switchport native vlan 1143 //definir a vlan de acesso (com a vlan em untagged e o switchport
native, todo o tráfego que vier na interface ethernet 1/5 é adicionado automaticamente na vlan definida, ou seja, não é
necessário que o próximo dispositivo configure a na sua interface.
exit //sair da interface
```

Configuração de banner para ficar bonito e no padrão.

```
banner login //acessa as configurações de banner (na linha abaixo colocar as
informações de banner iniciando com um ~ e quando finalizar o banner colocar um ~ novamente para finalizar
```

```
=====
_____
| \_ \ / \ / \ \ \ / \ \ \ / \ \ \
| | | | | | | | | | | | |
| | | | | | | | | | | | |
=====MASTER=====~
```

Obs: ~ inicia o banner e ~ finaliza o banner

Salvar configurações e rebootar para logar com o usuário criado

```
copy run st //salva as configurações que estão rodando (este comando deve ser aplicado fora do modo config)
reboot //reiniciar o EDD
```

Logar com nocuser e excluir o usuário admin e salvar novamente

```
config
no username guest //exclui o user guest
no username admin //exclui o user admin
```

Configurações de EDD 4370 (10 GB)

Configurações de nome e horário

```
config //entrar no modo de configuração
hostname MCL-B2B-840521-EDD-01 //definir nome do EDD
clock timezone BRA -3 //definir fuso horário
```

Configurações de usuário

```
aaa user nocuser //criar e entrar na configuração do usuário
password %$NoC.2018 //definir senha do usuário
group admin //definir permissão de administrador para o usuário
exit //sair da configuração do usuário "nocuser"
commit //aplicar config
```

Configurações de SNMP (coleta de dados)

```
snmp system location Montes Claros //definir a localização do equipamento
snmp traps config-commit //habilitar notificação do snmp quando aplicar configurações
snmp traps cpu-load //habilitar notificação do snmp sobre o processamento
snmp traps link-status //habilitar notificação do snmp sobre o status das interfaces
snmp traps login-success //habilitar notificação do snmp quando algum usuário logar
snmp agent enabled //habilitar o snmp
snmp agent ip 172.17.192.9 //definir o ip de origem do snmp como o IP da gerencia do EDD
snmp agent version v2c //habilitar a versão 2 do snmp
snmp community McxMCL@RNP //criar e entrar na community SNMP (aqui o nome poderia ser outro)
sec-name McxMCL@RNP //definir a community (aqui é de fato a community que será usada)
exit //sair da configuração da community
snmp vacm group McxMCL@RNP //criar e entrar no grupo para conseguir ler as informações do snmp
member McxMCL@RNP //criar e entrar no membro dentro do grupo
sec-model v2c //habilitar a leitura do snmp v2 no membro
exit //sair da configuração do membro
access " v2c no-auth-no-priv //criar e entrar no acesso para habilitar as permissões
read-view root //habilitar a permissão leitura
write-view root //habilitar a permissão de escrita
notify-view root //habilitar a permissão de notificações
exit //sair do acesso criado
exit //sair do grupo criado
snmp vacm view root //criar e entrar no grupo de visualização "root"
subtree 1.3 //entrar na árvore 1.3 onde fica a maior parte dos objetos no protocolo
included //habilitar a coleta de dados dessa árvore pelo grupo root
exit //sair da árvore 1.3
exit //sair do grupo root
commit //aplicar config
```

Configurações de Vlans

```
dot1q //entrar no modo de configuração das vlans
vlan 2635 //criar e entrar na vlan
name GER-CLI-B2B-MCL //definir descrição para a vlan
interface ten-gigabit-ethernet 1/1/1 //acessar a interface dentro da vlan
tagged //definir a configuração da vlan como tag na interface
exit //sair da configuração da interface dentro da vlan
exit //sair da configuração da vlan
vlan 1143 //criar e entrar na vlan
name LTL-MCL-BHE-840521 //definir descrição para a vlan
interface ten-gigabit-ethernet 1/1/1 //acessar a interface dentro da vlan
tagged //definir a configuração da vlan como tag na interface
exit //sair da configuração da interface na vlan
interface gigabit-ethernet 1/1/5 //entrar na configuração da interface na vlan
untagged //definir a vlan como access na interface
exit //sair da configuração da interface na vlan
exit //sair da configuração da vlan
exit //sair da configuração de dot1q
```

```

switchport                                //acessar as configurações de switchport
interface gigabit-ethernet 1/1/5          //acessar as configurações de switchport da interface
native vlan                               //acessar as configurações de native vlan da interface
vlan-id 1143                               //definir a vlan 1143 em access na interface
exit                                      //sair do native vlan
exit                                      //sair da interface
exit                                      //sair do switchport
commit                                     //aplicar configuração

```

Configurações de gerência e acesso

```

interface l3 GER-CLI-B2B-MCL               //criar interface de camada 3 (que fala ipv4)
lower-layer-if vlan 2635                   //definir que o l3 irá conversar com o l2 na vlan 2635 (passar a vlan)
ipv4 address 172.17.192.9/21              //definir ip de gerência
exit                                       //sair da interface l3
ssh-server port 2021                      //definir o acesso via ssh pela porta 2021
ssh-server max-connections 16             //definir o máximo de conexões simultâneas via ssh
telnet-server disable                     //desabilitar o acesso via telnet (não seguro)
router static                            //acessar a configuração de rota estática
address family ipv4                      //entrar na configuração de ipv4
0.0.0.0/0 next-hop 172.17.192.1        //definir o gateway da gerência
exit                                       //sair da configuração de rota estática.
commit                                     //aplicar config

```

Configurações da interface

```

interface ten-gigabit-ethernet 1/1/1        //acessar a interface
no shutdown                             //habilitar a interface (tirar o shutdown)
exit                                     //sair da interface
interface gigabit-ethernet 1/1/5          //acessar interface
no shutdown                             //habilitar interface (tirar shutdown)
exit                                     //sair da interface
commit                                    //aplicar config

```

Obs: As demais configurações da interface são configurações de negociação que é utilizado para firmar o link entre a interface x com a interface y. Essas configurações já são aplicadas por padrão na interface e com a auto negociação ativada. Em alguns casos, a auto negociação ativa pode acarretar a problemas para linkar as interfaces conectadas devido a não conseguirem negociar os valores de speed, banda e duplex, nesses casos onde as interfaces não linkam, devemos desabilitar a auto negociação com o comando “no negotiation” dentro da interface.

Logar com nocuser e excluir o usuário admin e salvar novamente

```

config                                         //entrar no modo de configuração
no aaa user admin                          //excluir usuário admin
commit                                        //aplicar configuração

```

LIMITAÇÃO DE TRÁFEGO

A limitação de banda pode ser feita de diversas formas e difere de produto para produto. Nos clientes que funcionam através de cadastro no I-manager a limitação é feita pelo plano selecionado. Já em clientes LTL, IPD, IPT, TRANSPORTE PTT e qualquer outro tipo de produto que seja inventado que deve ser feito configurações nos switchs e roteadores, a limitação é setada de forma manual.

- Limitação em switchs:

Limitação através de traffic classifier, behavior e policy:

A maioria dos clientes são limitados dessa forma. Consiste em configurar uma classificação (nome) para o tráfego da vlan, um comportamento (behavior) e atribuir esta classificação a esse comportamento através de uma policy.

Exemplo: Cliente possui 100MB, vlan 1515, e passa pela interface XGE 0/0/14 que vai pra OLT-2 de Divinópolis.

A configuração seria:

```
sys                                         //entrar no modo de configuração
traffic classifier B2B-NOC-100MB          //criar e entrar na classificação
if-match vlan 1515                         //atrelar a vlan na classificação criada
quit                                         //sair da classificação

traffic behavior B2B-NOC-100MB           //criar e entrar no comportamento
car cir 102400 pir 102400 green pass yellow pass red discard //definir o limite em 100MB, o valor deve ser setado
em KBPS
quit                                         //sair do comportamento

traffic policy B2B-OLT-2                  //criar e entrar na policy
classifier B2B-NOC-100MB behavior B2B-NOC-100MB //definir que a classificação criada terá o comportamento
criado
quit                                         //sair da policy

interface xg 0/0/14                         //entrar na interface onde vamos passar a policy
traffic-policy B2B-OLT-2 inbound            //passar a política de entrada
traffic-policy B2B-OLT-2 outbound           //passar a política de saída.
```

- Limitação em NEs:

Acessar a sub-interface do cliente e configurar. Como exemplo vamos utilizar a vlan 441 com o tráfego de 100MB.

```
sys                                         //entrar no modo de configuração
interface eth-trunk 0.441                  //entrar na sub-interface
qos car cir 102400 pir 102400 green pass yellow pass red discard inbound //limitar em 100MB entrada
qos car cir 102400 pir 102400 green pass yellow pass red discard outbound //limitar em 100MB saída
```

- Limitação diretamente em interfaces:

Também conseguimos fazer limitações diretamente em interfaces de switchs huawei e também em switch datacom. Geralmente esses equipamentos possuem a configuração de qos ou rate-limit para tal finalidade porém não é muito usual, mas sempre devemos validar em caso de reclamação de clientes se não há este tipo de configuração nos equipamentos.

Comandos para troubleshooting

dis ip interface brief	//exibir todas interfaces e os IPs configurados nelas
dis cu in xxxx	//exibir todas configurações que tiverem o que estiver escrito no lugar do xxxx
dis mac-address vlan 10	//exibir MAC que estão sendo aprendidos na vlan
dis mac-address vsi NOME DA VSI	//exibir MAC que estão sendo aprendidos na VSI
dis vlan 10 //exibir informações da vlan (se existe, interfaces que está configurada, se está tagged ou untagged)	
dis lldp neighbor brief	//exibir os equipamentos vizinhos, a interface local e a interface que recebe no outro
ping vpls vsi NOME DA VSI peer IP DO PROXIMO SWITCH	//testar comunicação de uma VSI
tracert vpls vsi NOME DA VSI peer IP DO PROXIMO SWITCH	//traçar rota que a VSI está fazendo na rede MPLS
ping vc vlan NÚMERO ID label-alert no-control-word	//testar comunicação L2VC
tracert vc vlan NÚMERO ID label-alert no-control-word	//traçar rota que o L2VC está fazendo na rede MPLS
dis cu int INTERFACE	//mostrar configurações da interface
dis interface INTERFACE	//mostrar informações da interface, erros, descarte, etc
dis cu int vlanif VLAN	//mostrar configurações da interface vlanif quando existir
ping -c 1000 -s 9000 IP	//pingar MTU de 9000
interface vlanif VLAN ip address IP MASCARA	//configurar IP na vlan
dis access-user username PPOE	//verificar autenticação de cliente no NE
dis access-user qos-profile RADIUS-NO-QOS-PROFILE	//verificar clientes que estão sem banda cadastrada
show network-access requests pending detail	//verificar clientes batendo no log de autenticação no Juniper
display aaa online fail-record username	//verificar clientes batendo no log de autenticação do NE

CONFIGURAÇÕES DE MIKROTIK

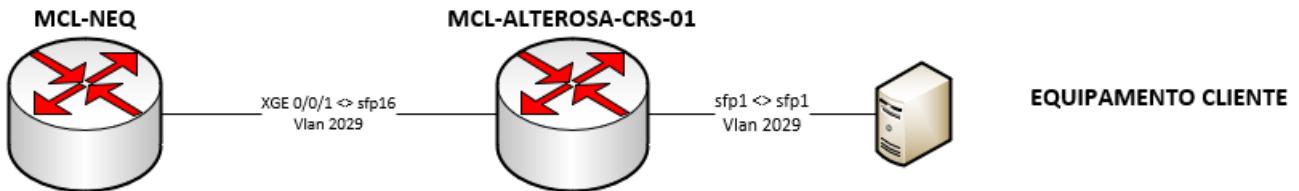
Em relação a clientes B2B, temos as possíveis configurações para utilizar este equipamento na ponta do cliente, como um equipamento gerenciável, também temos configurações nas mikrotiks existentes na rede Master para possibilitar a entrega de links, ou até mesmo como um equipamento para testes isolados, como por exemplo, teste de banda acima de 1GB que não é possível ser realizado em servidores de speedtest, é possível testar através de 2 mikrotiks pelo bandwidth teste.

Na rede backbone da master temos mikrotiks CCR e CRS. As CCRs são routers, utilizados como concentradores de clientes ou no caso da maioria dos B2Bs, como mais um equipamento onde deve ser propagado a vlan. Já as CRSs são utilizadas como verdadeiros switchs, onde configuramos apenas comunicação de camada 2 (vlan), e nada mais.

Configurações CRS

Para configurar vlans na Mikrotik CRS (São utilizadas em MCL) pode ser feito tanto pela interface do winbox quanto pelo terminal de configurações via linha de comando.

Como exemplo vamos utilizar a seguinte topologia:

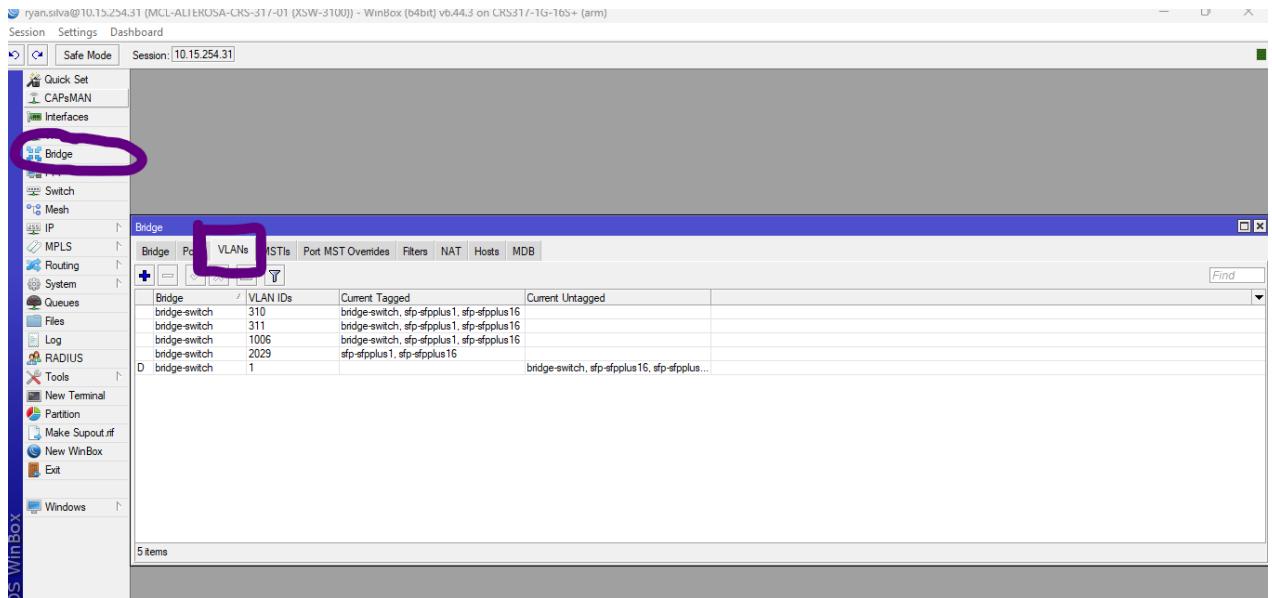


A configuração que deveria ser feita na CRS nesse caso seria apenas transportar a vlan 2029 na interface que comunica com o cliente e na interface que comunica com o NEQ.

Pela interface gráfica, devemos acessar o winbox:



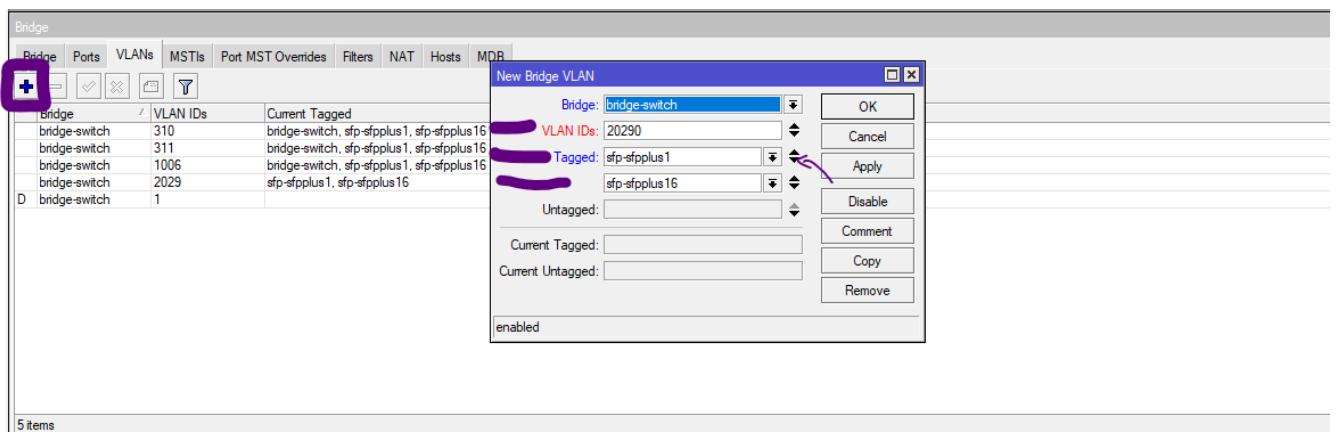
1. Clicar em Bridge e clicar na subconfig VLANs:



2. Clicar em + e alterar o VLAN Ids para o número da Vlan que você deseja passar nas interfaces.

Clicar em Tagged e selecionar a interface que deverá passar a vlan.

Clicar na seta pra baixo e colocar a segunda interface na qual queremos passar a vlan

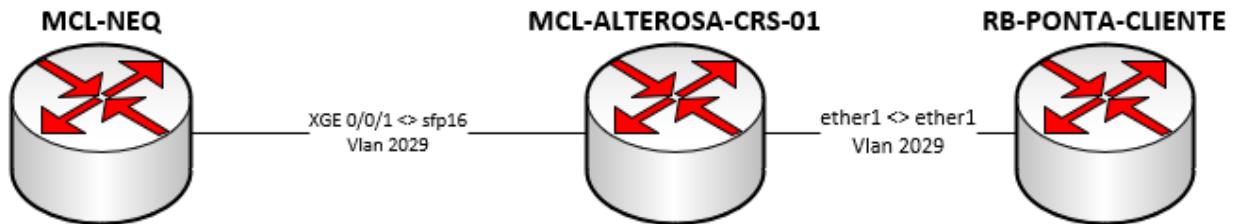


Clicar em apply e está pronto.

Configurações CCR:

- Para configurar uma mikrotik para ser um equipamento gerenciável devemos fazer a seguinte configuração:

Vamos usar como exemplo a seguinte topologia:



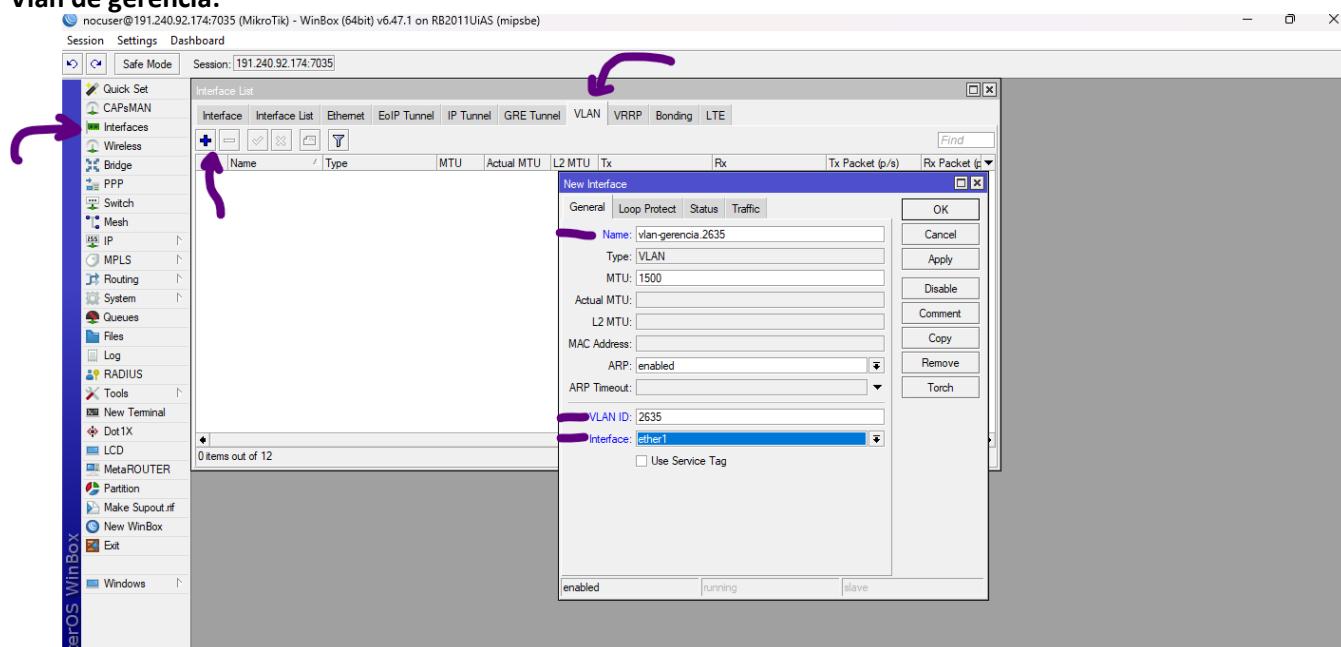
IP de gerência: 172.17.25.18/30

Vlan de gerência 2635

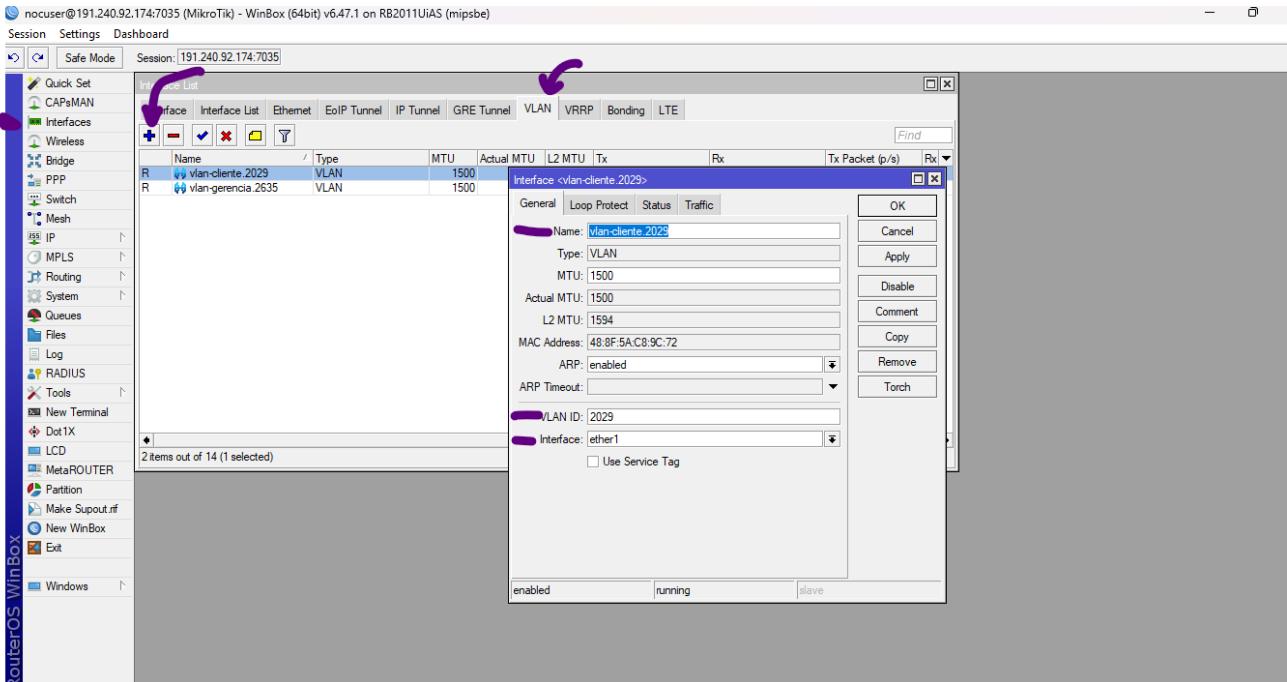
Com a mikortik resetada, conectar um cabo de rede em qualquer interface e conectar no notebook. Acessar o winbox no notebook e o mac da interface deverá aparecer no neighbors. Clicar nele e acessar com admin sem senha.

Primeiramente precisamos configurar a comunicação na camada 2, devemos configurar as vlans. Clicar em interface > VLAN > + > alterar o nome > alterar o VLAN ID > escolher a interface que está passando a vlan.

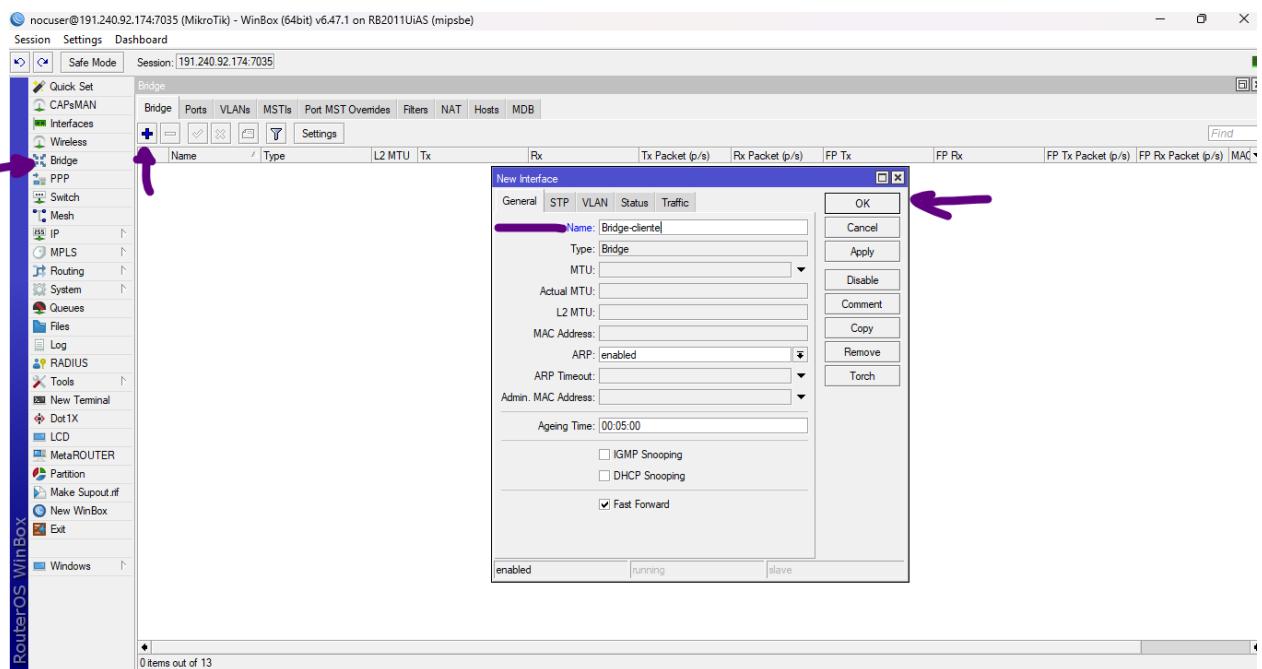
Vlan de gerência:



Vlan do cliente:

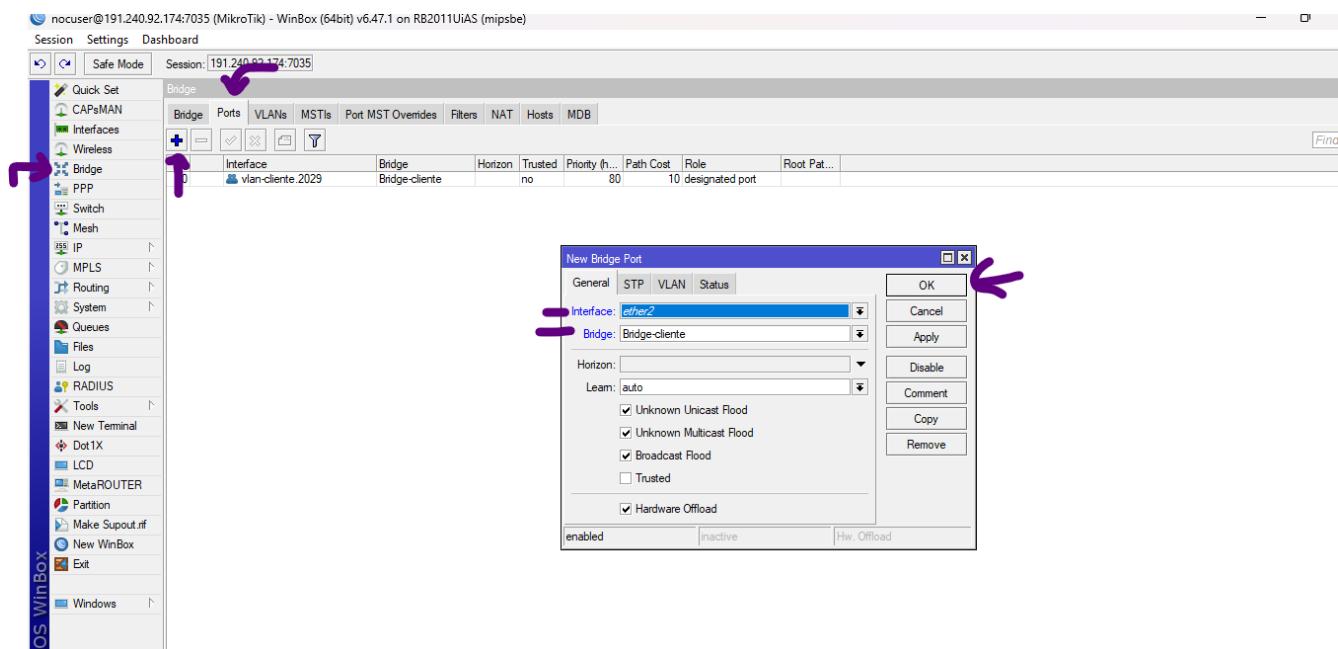
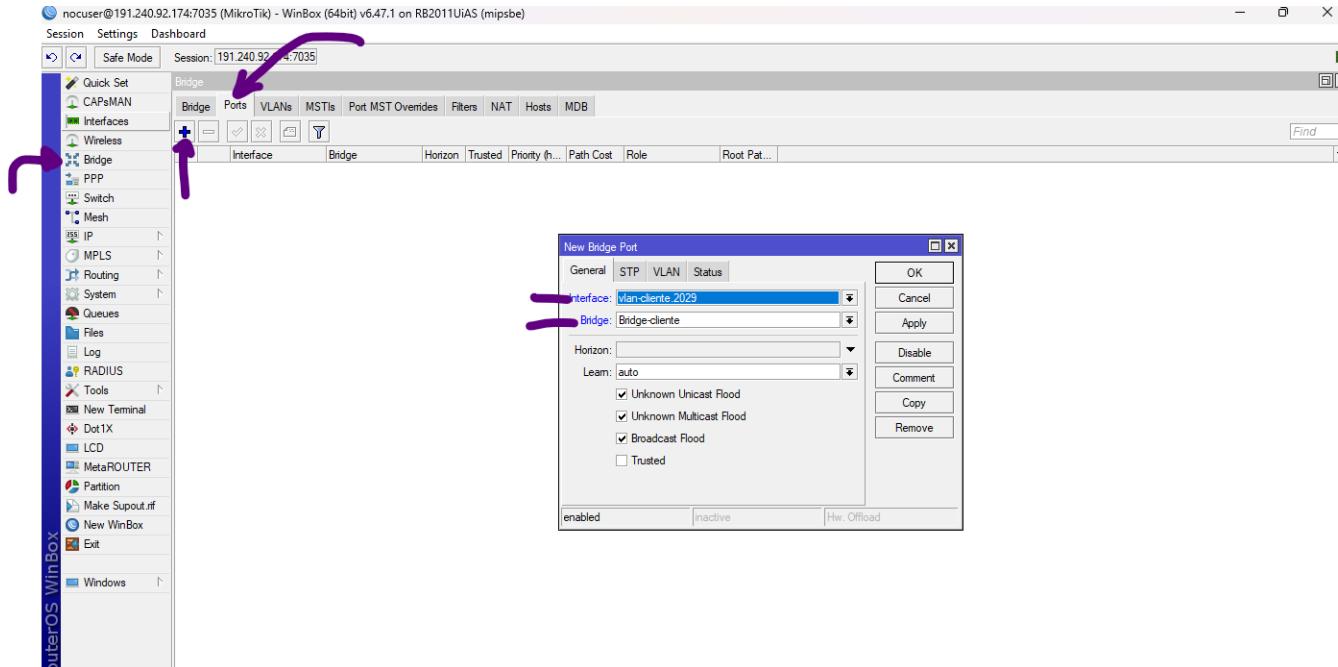


Após criar as vlans, precisamos fazer com que a interface que o cliente irá conectar o seu equipamento converse com a vlan 2029 que está na porta de link ether1. Para isso, é necessário criar uma bridge, onde será feito uma amarração entre a interface vlan e a interface que vai pro cliente.



Criado a Bridge deveremos fazer a amarração das interfaces que queremos que conversem.

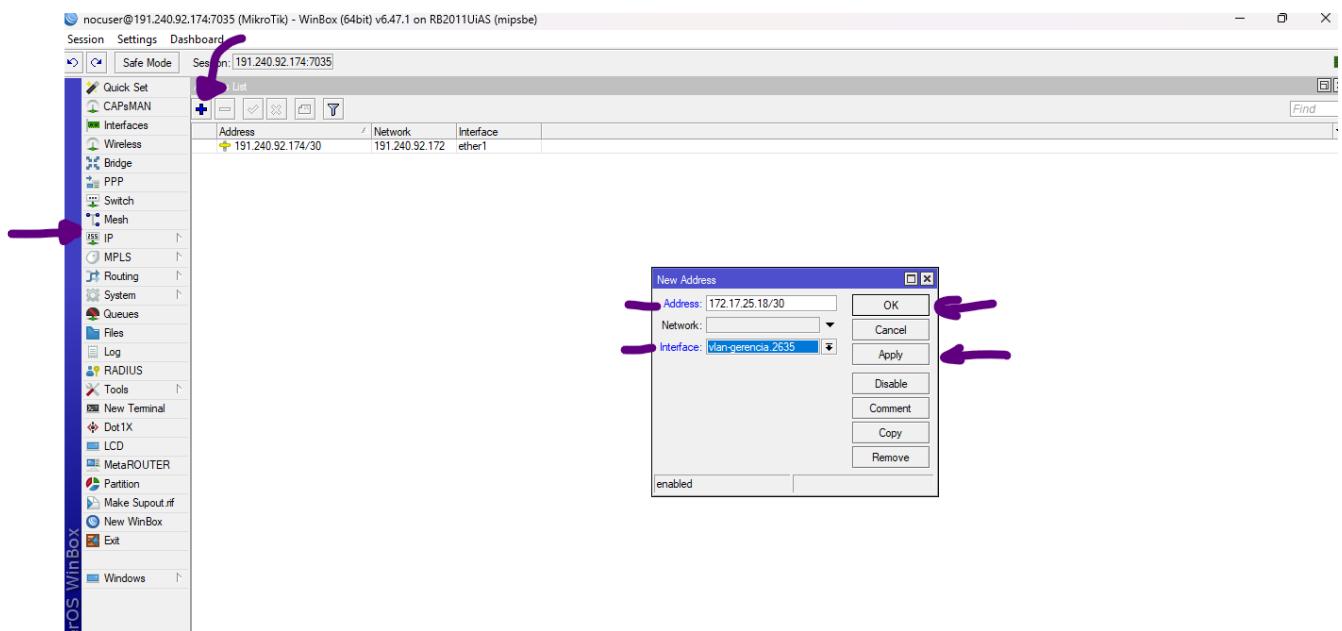
BRIDGE > PORTS > + > Escolher interface e escolher a bridge que criamos, fazer isso tanto pra interface vlan quanto pra interface que o cliente iria conectar, como exemplo vamos utilizar a ether2



Dessa forma o tráfego que entra na interface ether2 conversa diretamente com a vlan 2029 do cliente.

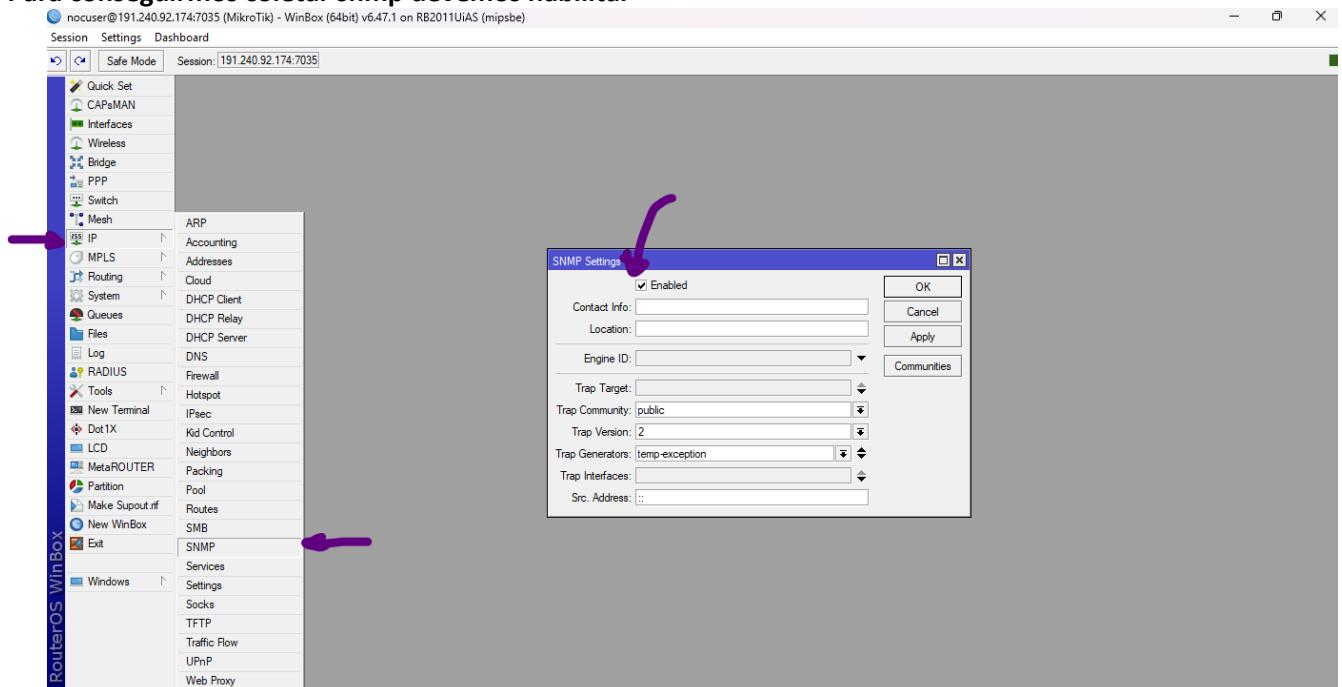
Feito isso a configuração de camada 2 está feita. Então podemos dar o próximo passo para a camada 3, camada de rede, então agora vamos configurar o IP de gerência.

IP > ADDRESS > + > Setar address/mascara > escolher a interface vlan da gerência.

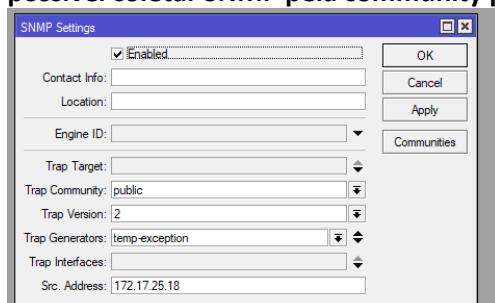


Feito isso já estamos com nossa gerência configurada.

Para conseguirmos coletar snmp devemos habilitar

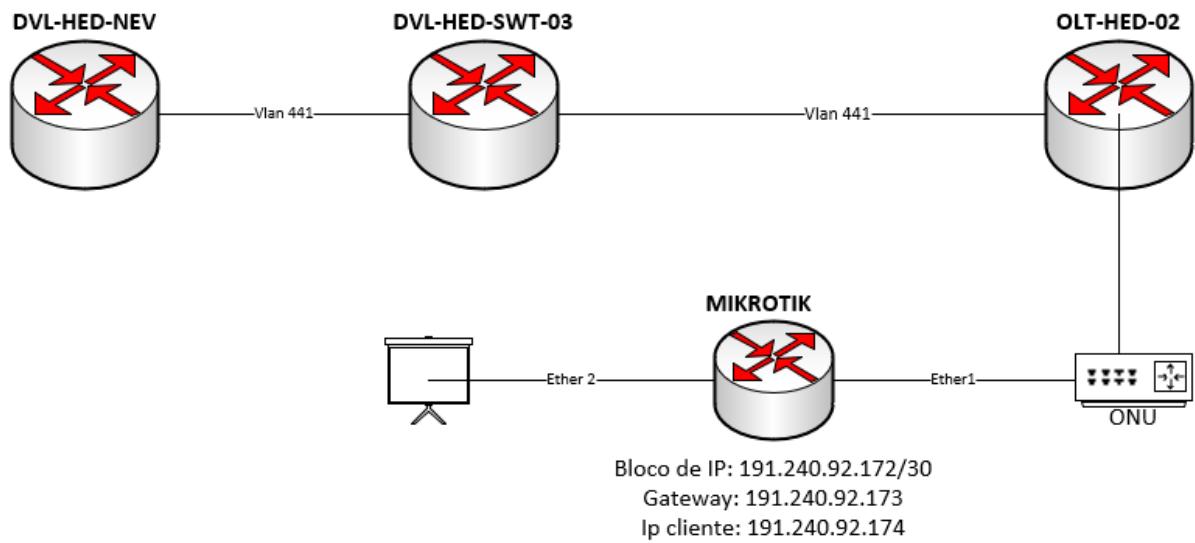


Definir o Src Address com o IP de gerência. (Src Address significa Endereço de origem). Com isso já será possível coletar SNMP pela community public e porta padrão 161.



- Para configurar uma mikrotik para teste isolado na nossa rede, e bandwidth teste:

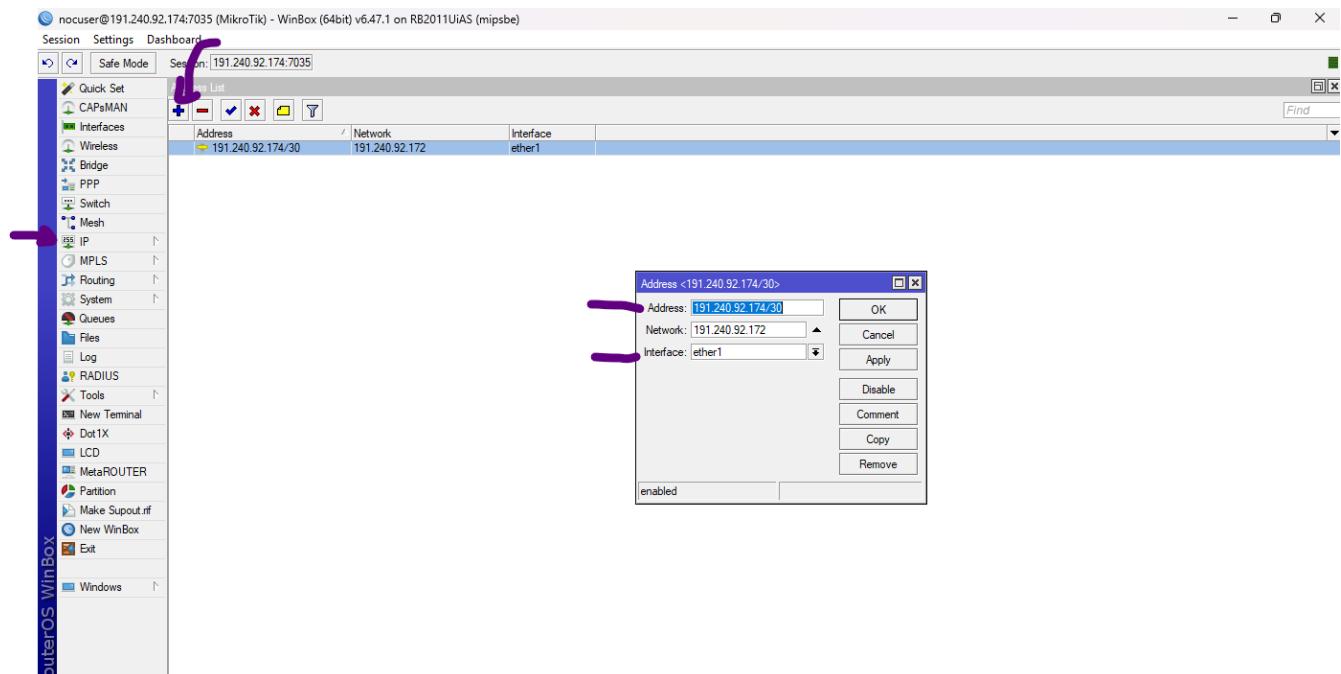
Vamos usar de exemplo a seguinte topologia:



Neste caso como se trata de uma ONU, temos uma particularidade. Quando configuramos a ONU em tag, ela funciona como uma porta access do switch huawei. Quando configuramos em transparent ele funciona como uma porta em trunk.

Suponhamos que esteja configurado em tag, ou seja, não preciso configurar a vlan na minha mikortik.

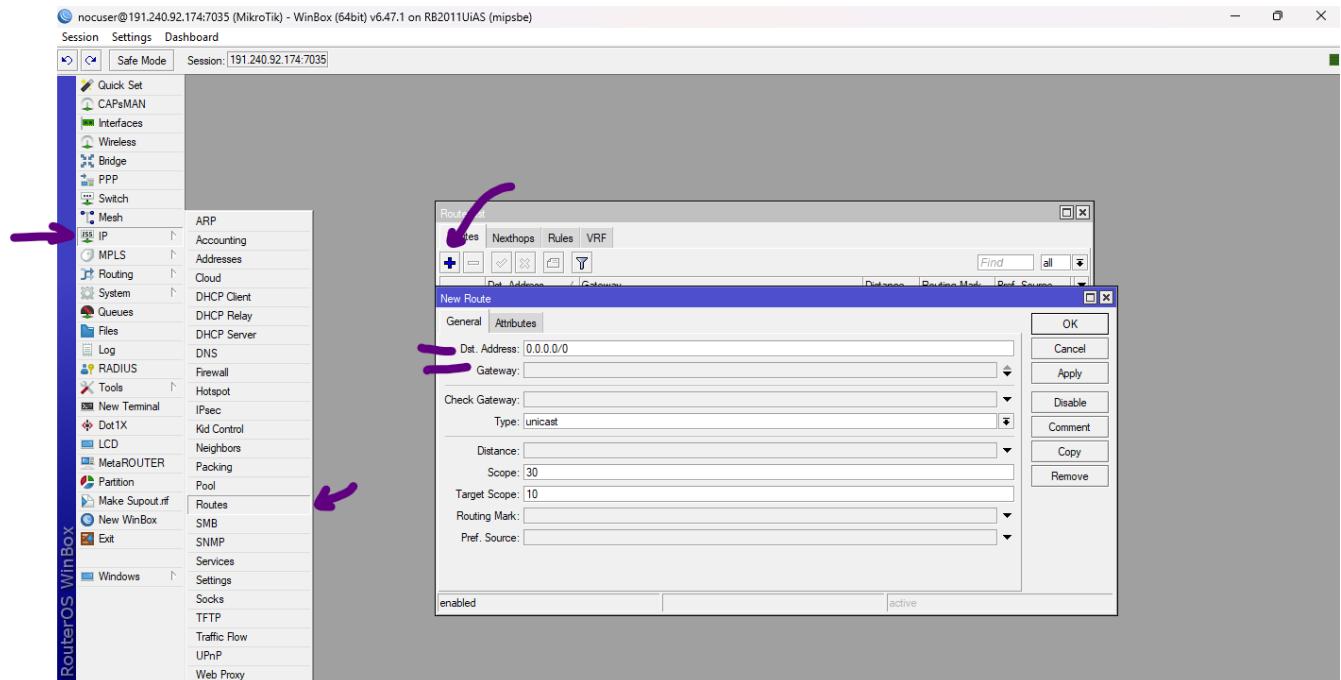
Acessar a mikortik, e já partir para a configuração de camada 3, setando o IP do cliente na interface em que recebemos o link, que no caso é a ether1.



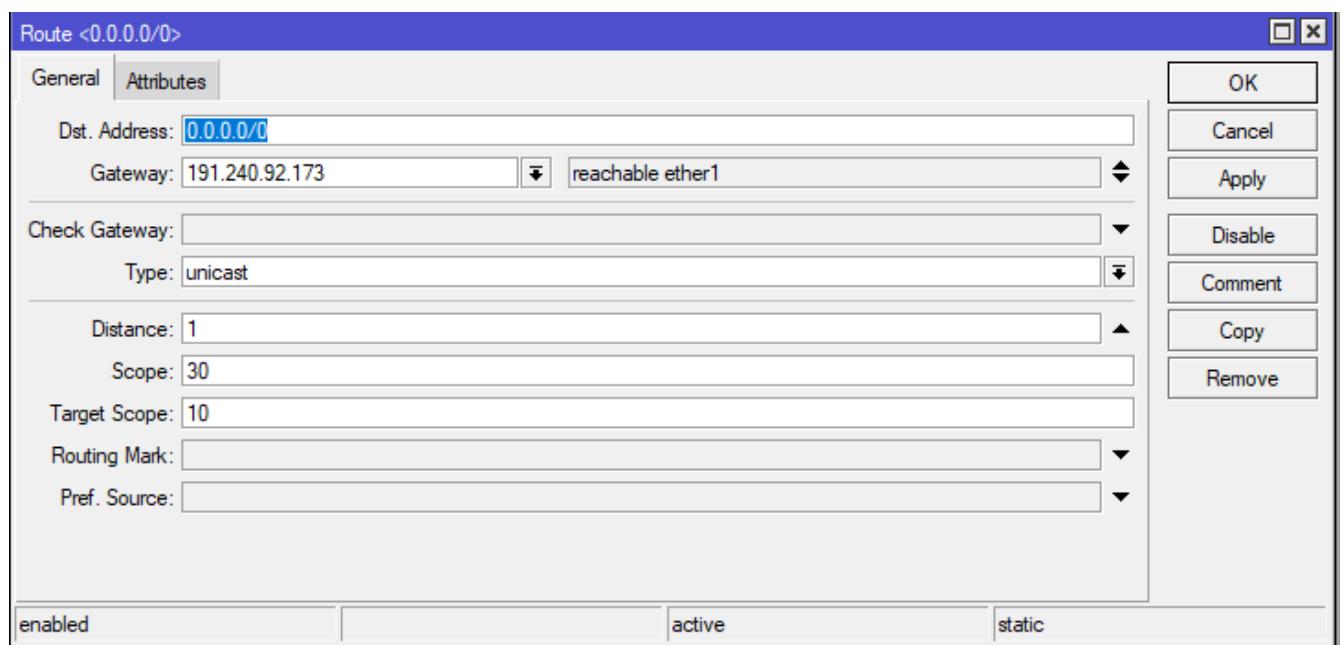
Obs: o network é calculado sozinho quando colocamos o IP address com o barramento.

Com o IP configurado, vamos configurar a rota default que é onde setamos o gateway do cliente.

IP > ROUTES > +



Então deixaremos o campo Dst Address como 0.0.0.0/0 que significa que qualquer IP será destinado para o gateway do cliente que configuraremos no campo gateway.



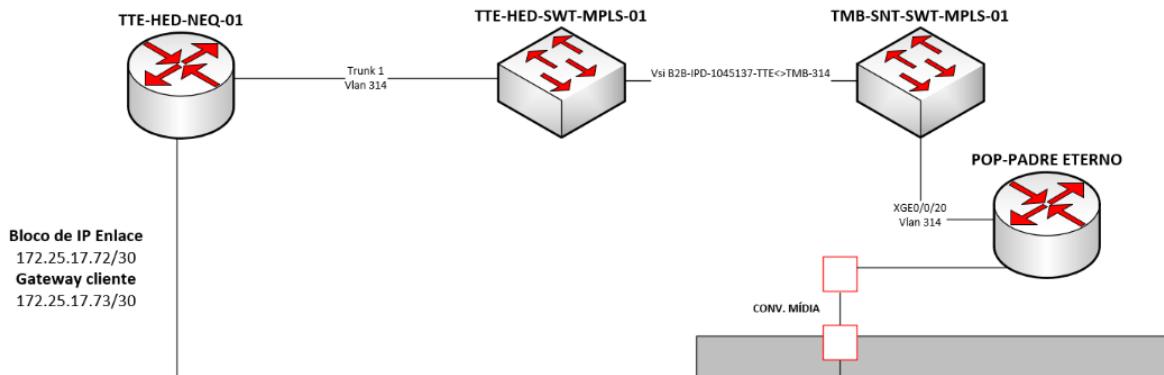
Com esta configuração aplicada já conseguiremos pingar algum IP da internet como por exemplo o 8.8.8.8.

```
..          Move up one level
/command     Use command at the base level
[nouser@MikroTik] > ping 8.8.8.8
SEQ HOST          SIZE TTL TIME STATUS
0 8.8.8.8          56 119 10ms
1 8.8.8.8          56 119 10ms
2 8.8.8.8          56 119 10ms
3 8.8.8.8          56 119 11ms
sent=4 received=4 packet-loss=0% min-rtt=10ms avg-rtt=10ms max-rtt=11ms
[nouser@MikroTik] >
```

Configuração de vlan nas CCRs

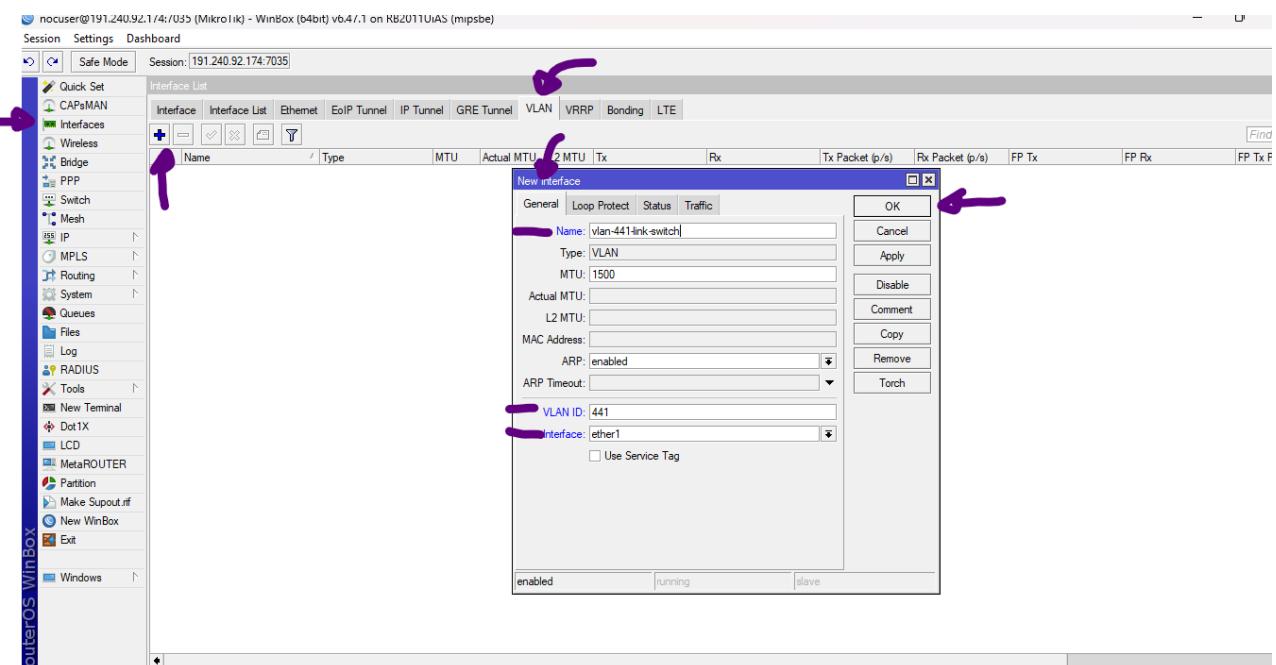
Em alguns casos de clientes B2B é necessário fechar a comunicação da VLAN do cliente passando por uma CCR, que por exemplo, faça uplink para uma OLT ou que seja uma interface direta da CCR com o cliente. Em ambos os casos, a configuração é a mesma e bem simples:

Vamos usar esta topologia de exemplo:

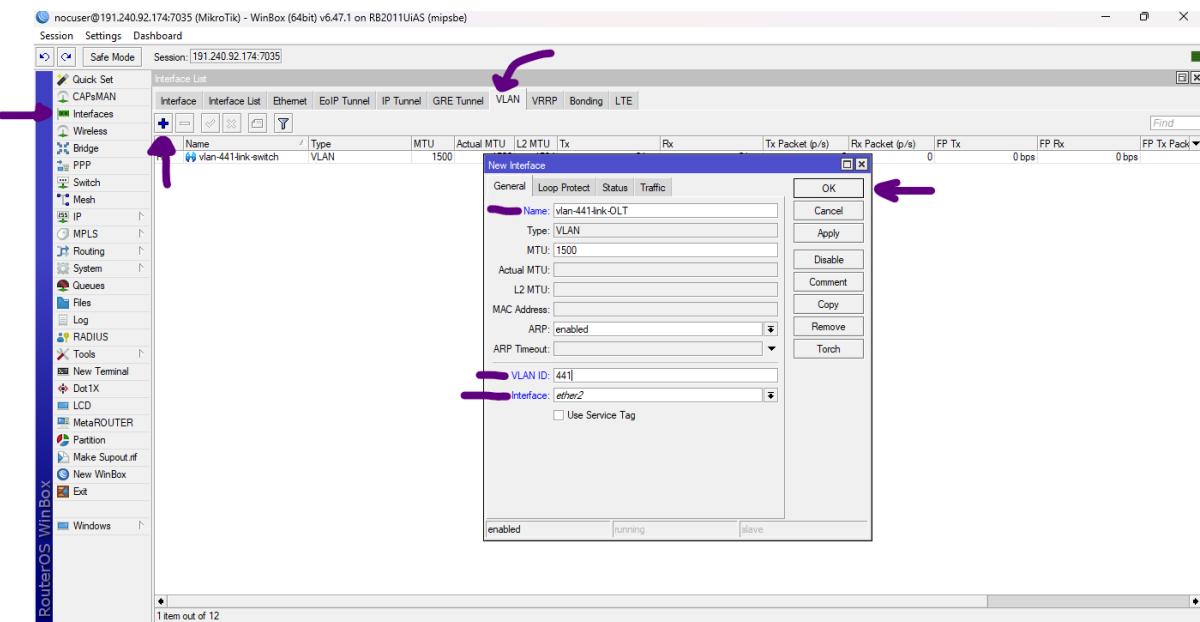


Suponhamos que a interface de link entre a RB e o switch seja pela ether 1 da RB, e a interface onde está o conversor de mídia ou a OLT ou o cliente seria a interface ether 2

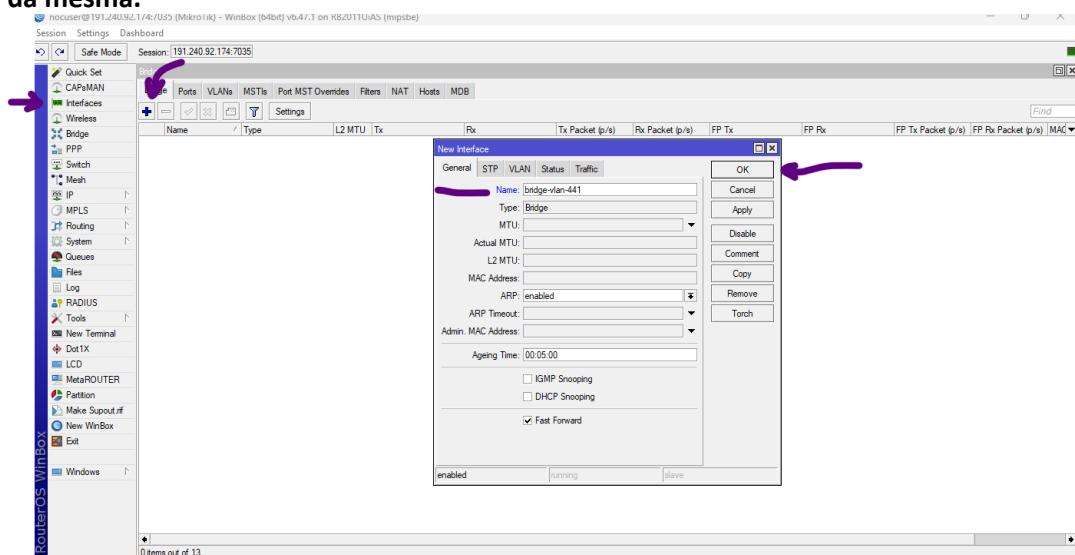
Primeiramente precisamos criar as vlans na Mikrotik. Tanto na interface que linka com o switch quanto na interface que linka com o processo equipamento que você deseja comunicar.



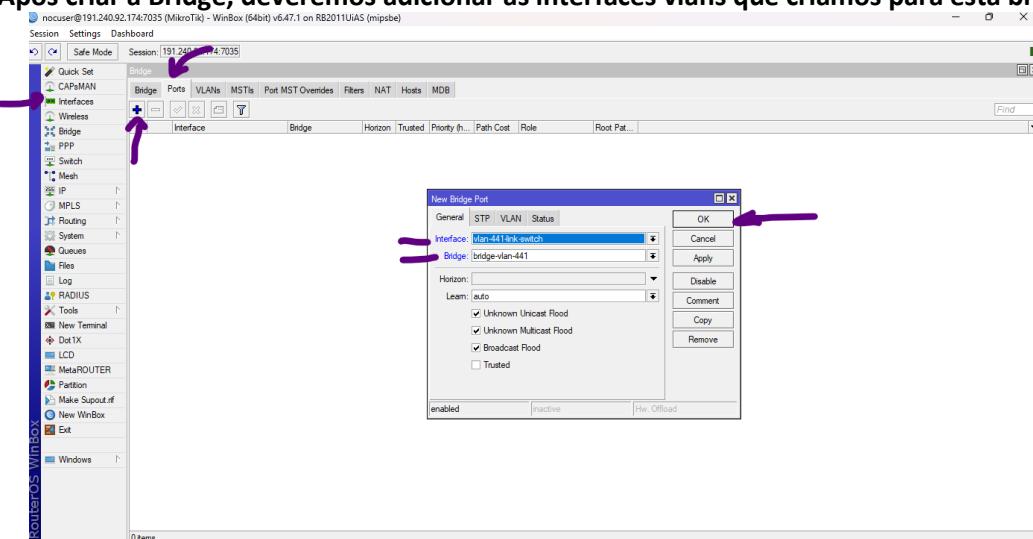
Repetir o mesmo processo só que apontando para a outra interface.



Após criar a vlan na interface de entrada e saída da Mikrotik só vamos precisar fazer com que a vlan que está em uma interface fale com a vlan que criamos na outra. Para isso criaremos uma bridge para comunicação da mesma.



Após criar a Bridge, deveremos adicionar as interfaces vlans que criamos para esta bridge.



Repetir o mesmo passo para a outra interface vlan que criamos e está finalizado. A vlan estará comunicando.

Bandwidth Teste

A partir do momento que temos uma conexão com a internet, conseguimos realizar um estress de banda para qualquer mikortik no mundo que tenha uma conexão com a internet e que tenhamos o usuário e o IP da mesma.

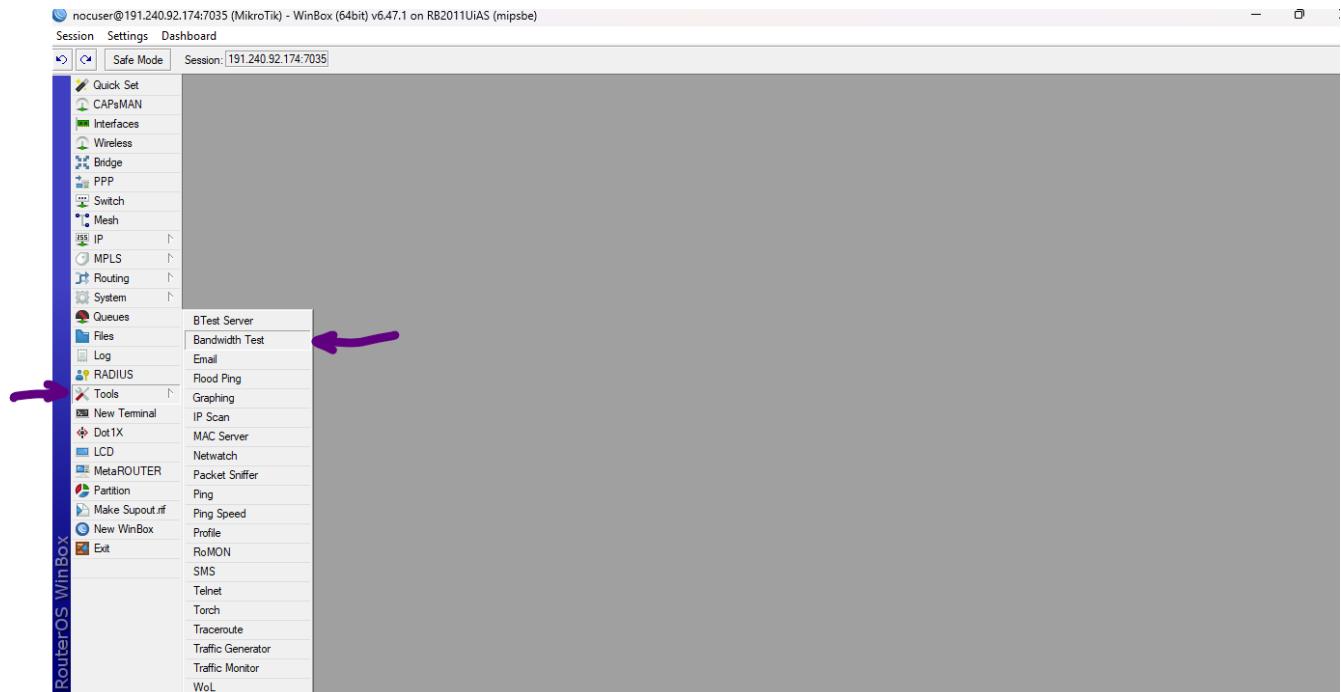
Para verificarmos qual o máximo de banda que este link do cliente consegue passar vou utilizar como outra ponta do bandwidth teste a mikrotik wireless de DVL que possui um uplink de 10GB e consegue testar até esse limite de banda.

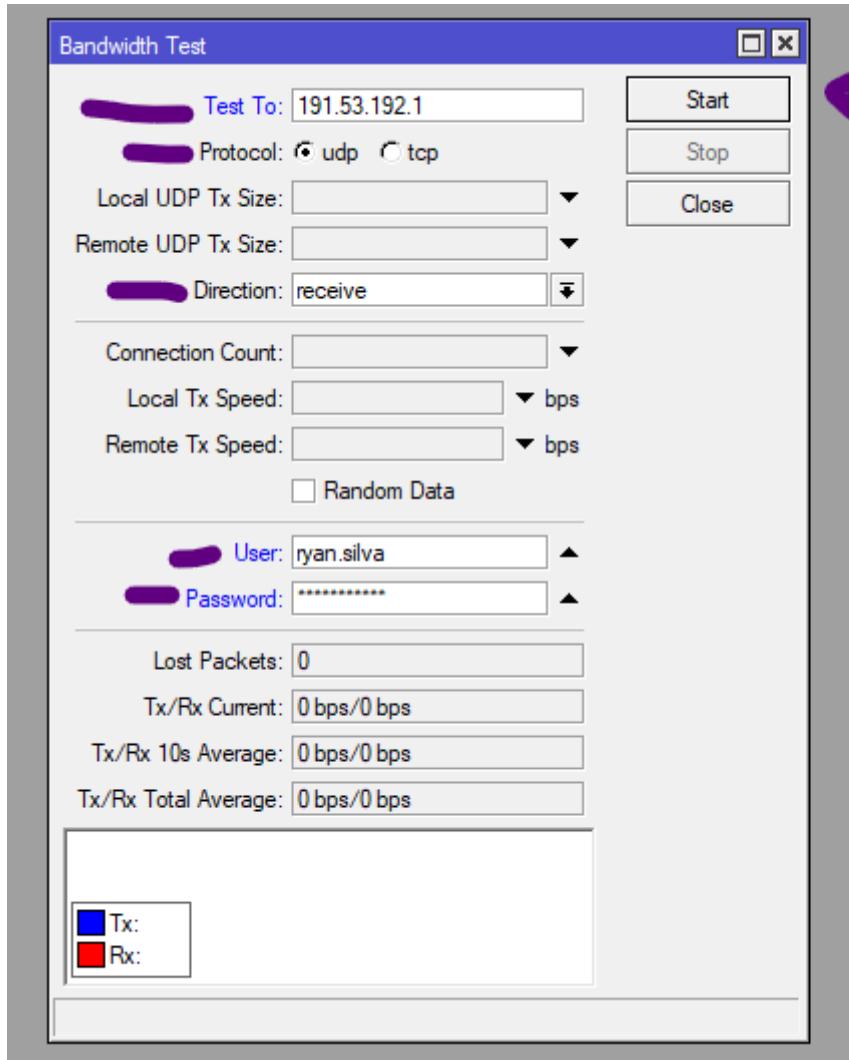
Primeiro passo: Possuir o IP e usuário de acesso da outra mikortik no qual será enviado o estress de banda.

IP DVL-RBW: 191.53.192.1

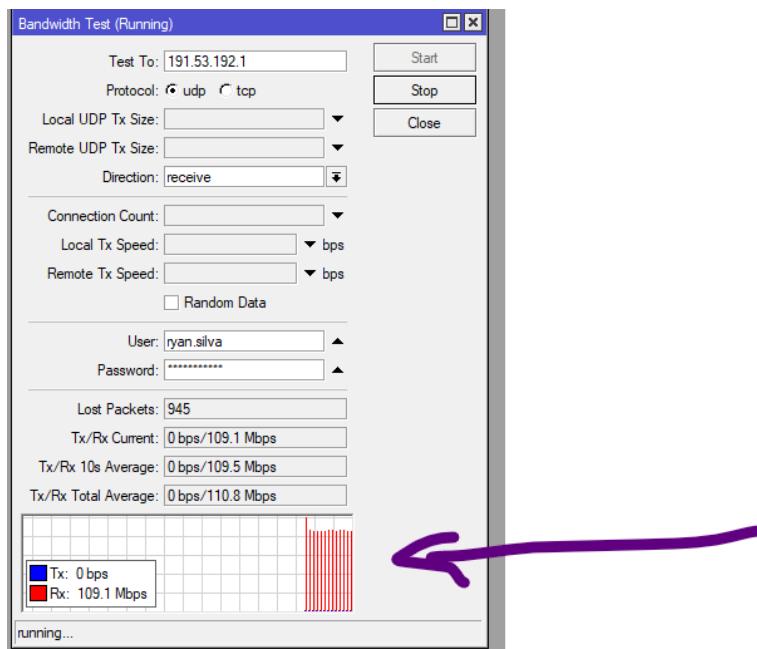
User: Qualquer usuário full

Segundo passo: Acessar a mikrotik do cliente que acabamos de configurar e clicar em tools > bandwidth teste > colocar as informações da Mikrotik do outro lado. Send para upload e receive para download. Utilizar o protocolo udp.





No caso do nosso cliente de exemplo o máximo de download que a mikortik conseguiu foi 109MB



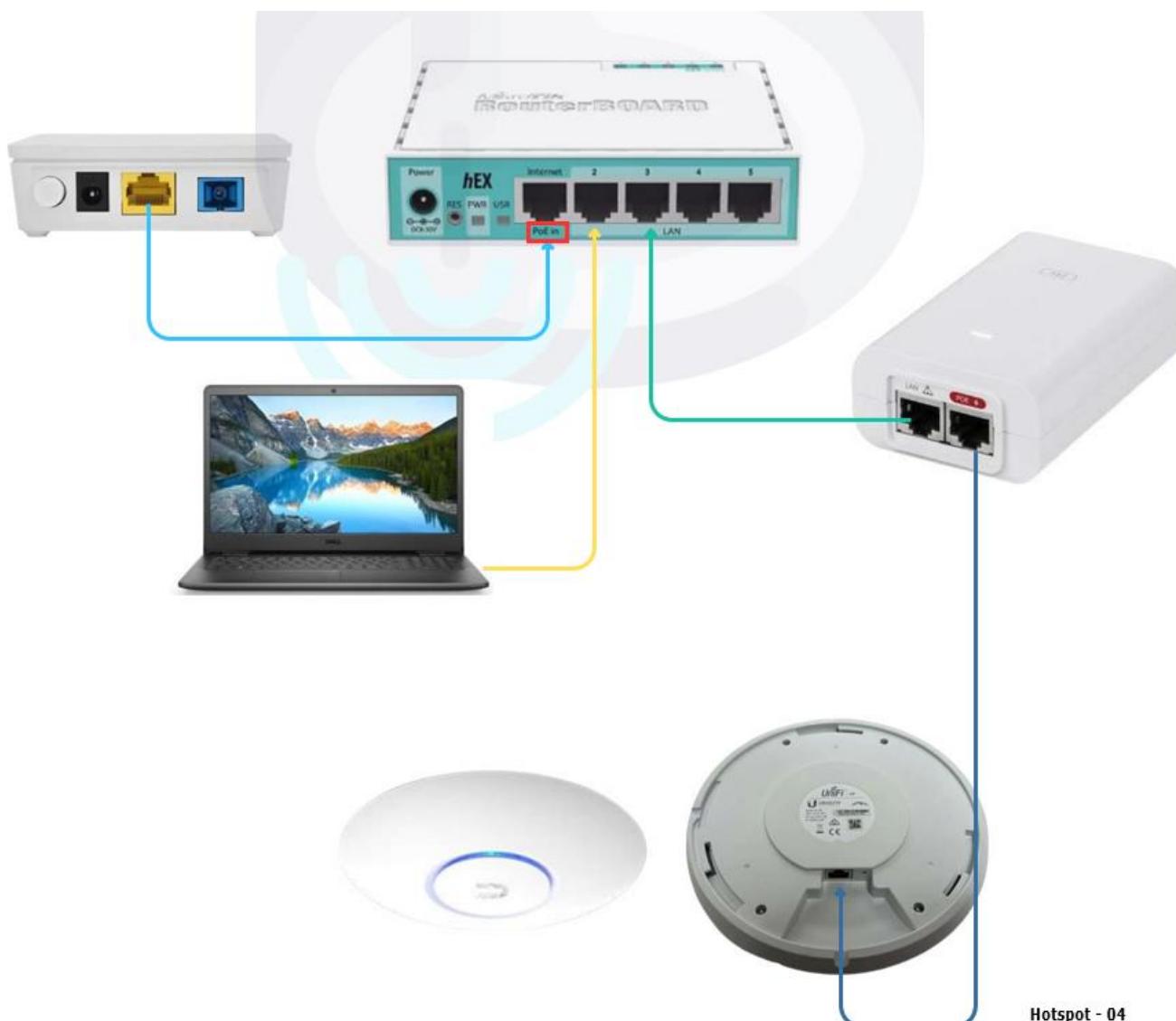
Isso depende de todos os fatores: cabos, limitações de banda, capacidade das portas dos dois lados e etc.

WIFI-SEGURO

Para instalarmos o produto WIFI-SEGURO precisamos de 2 equipamentos obrigatórios: Mikrotik e UniFi. O primeiro passo para a configuração do produto é garantir a conectividade da Mikrotik com a internet independente de qual modo seja (IP dedicado, PPOE, DHCP, etc.), sem conectividade na mikortik não adianta nem tentar. Como no tópico acima foi ensinado a configuração de um IP dedicado na Mikrotik, neste tópico vamos abordar a configuração da conectividade via PPPOE, que é o mais comum deste produto.

Checklist de configurações que precisam ser realizadas:

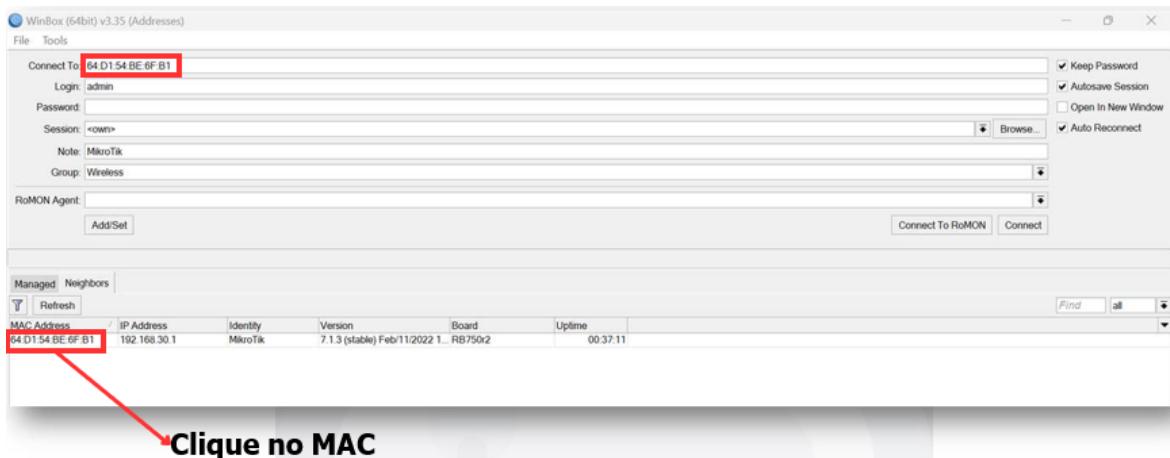
- Criar um usuário (System >> User)
- Desativar as portas de serviço e manter habilitada apenas a porta API 8728 e porta Winbox (IP >> Service)
- Fazer a conexão PPPOE (PPP >> Interface >> Adicionar)
- Testar a conexão pingando o google 8.8.8.8 (New terminal ou Tools >> Ping)
- Configurar o DNS: 191.240.0.70 e 191.240.2.71 (IP >> DNS)
- Pingar o google.com pelo Terminal ou pelo Tools >> Ping
- Criar uma Bridge e adicionar as interfaces que irão ser destinadas para o hotspot



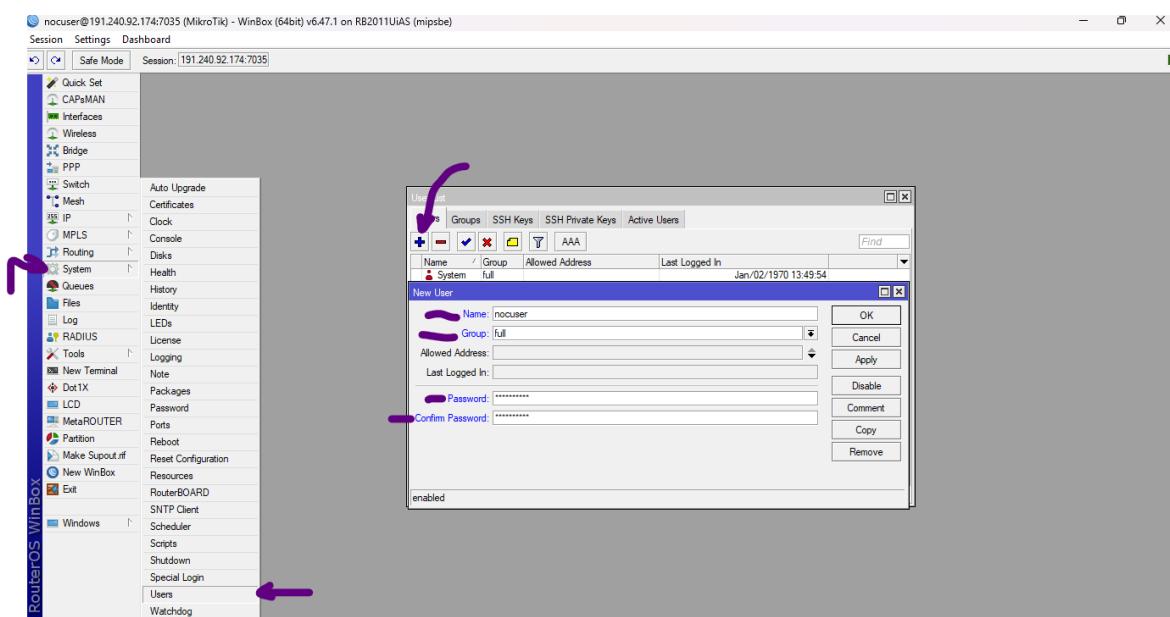
Hotspot - 04

Configurações Mikrotik para Wifi-Seguro

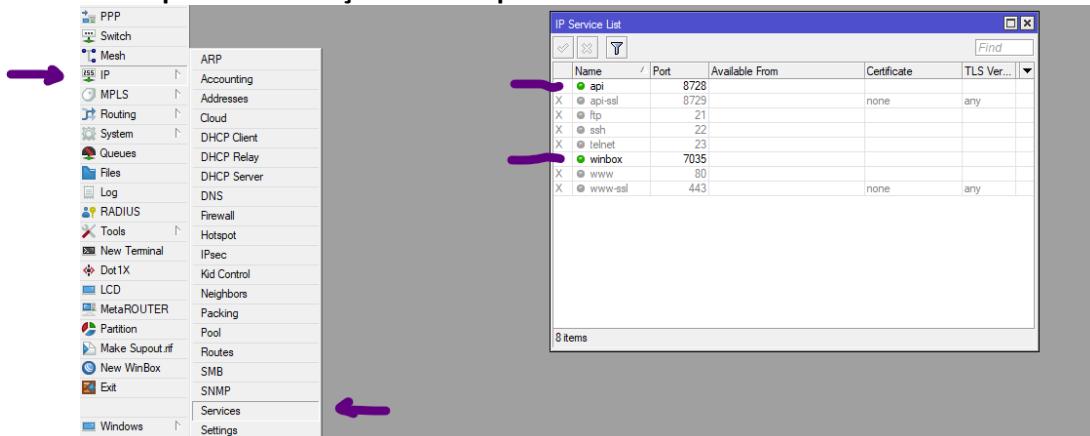
1. Abra o Winbox e acesse a Mikrotik. Com o cabo do notebook conectado na Mikrotik vá em "Neighbors" e clique no Mac que aparecer.
Usuário: admin
Senha: sem senha



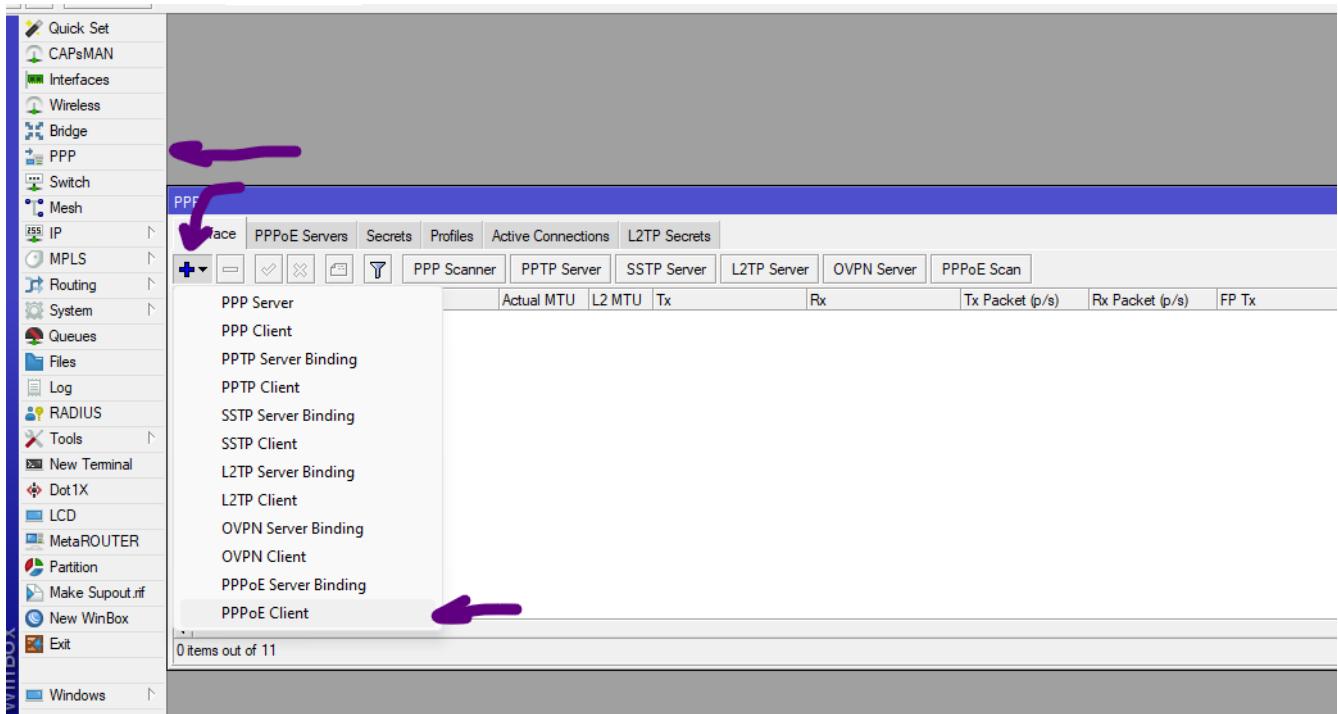
2. Após fazer o login, cadastre o novo usuário e exclua o usuário admin.



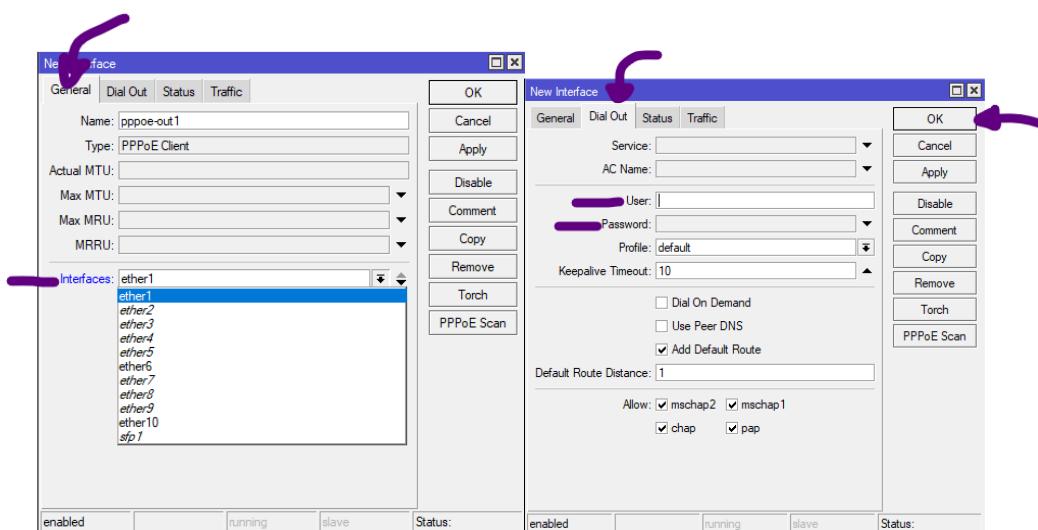
3. Desativar as portas de serviço e ativar a porta API 8728



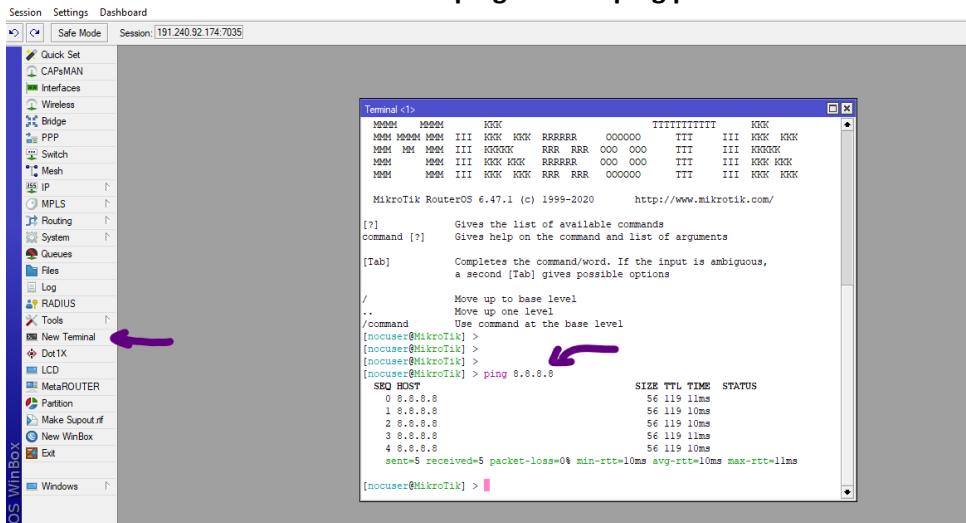
4. Configurar a conexão PPPoE (PPP >> + >> PPPoE CLIENT)



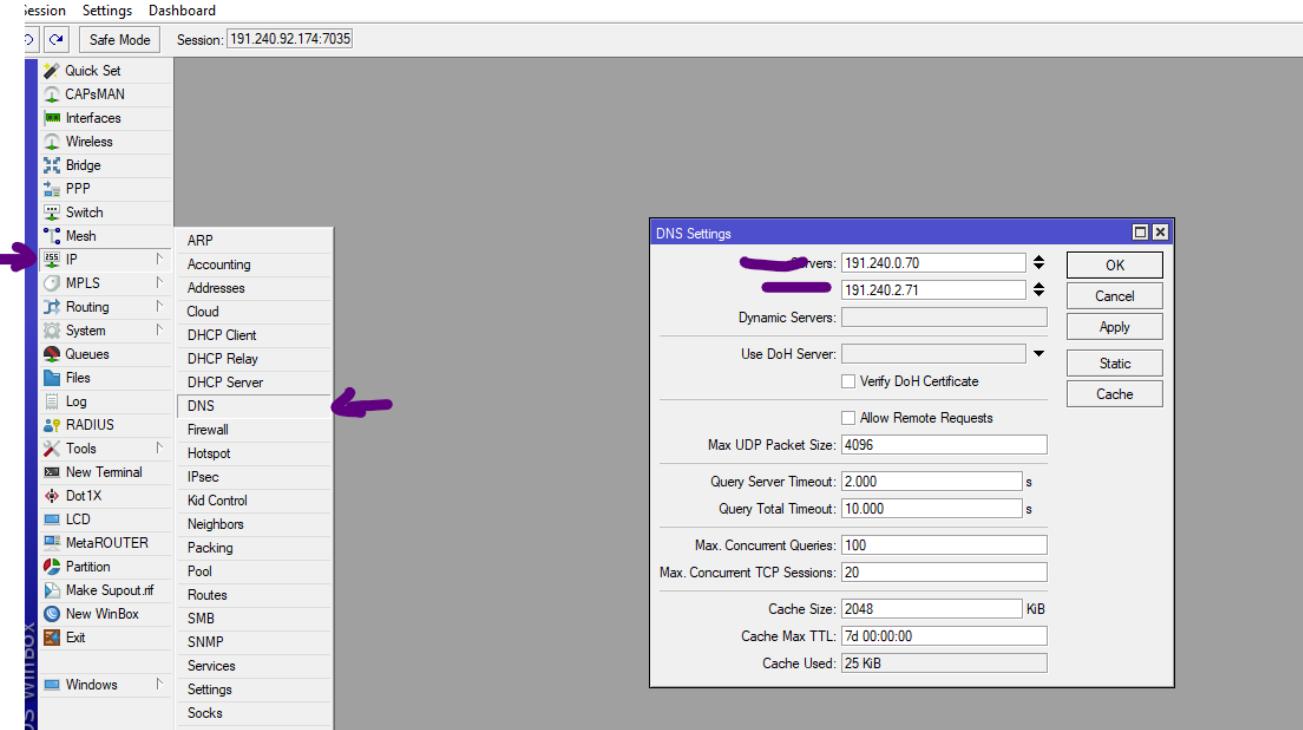
Aba General, selecionar a interface que está conectada na ONU, e discar usuário e senha do PPPoE na Aba Dial Out:



5. Acessar o terminal ou ir em Tools >> ping e testar ping para o 8.8.8.8.



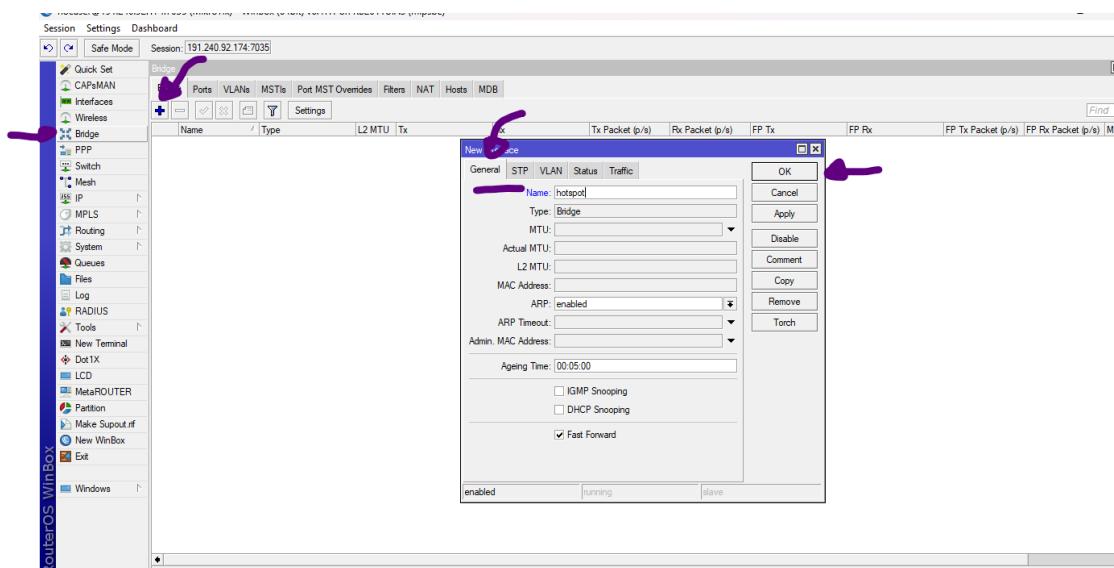
6. Configurar o DNS em IP >> DNS



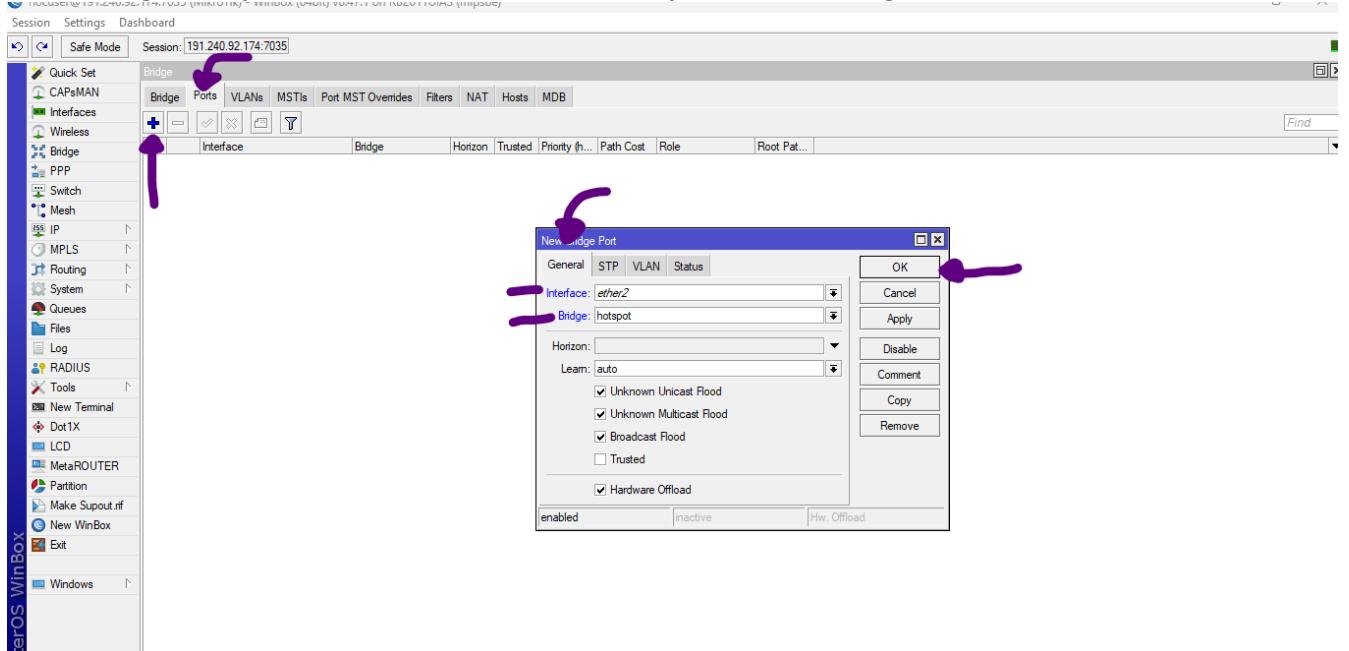
7. Voltar novamente no terminal e pingar o google.com para validar que o DNS está funcionando

```
MikroTik RouterOS 6.47.1 (c) 1999-2020      http://www.mikrotik.com/
[?]      Gives the list of available commands
command [?]      Gives help on the command and list of arguments
[Tab]      Completes the command/word. If the input is ambiguous,
           a second [Tab] gives possible options
/      Move up to base level
..      Move up one level
/command      Use command at the base level
[nouser@MikroTik] > ping google.com
SEQ HOST      SIZE TTL TIME STATUS
0 142.251.129.238      56 119 llms
1 142.251.129.238      56 119 llms
2 142.251.129.238      56 119 llms
3 142.251.129.238      56 119 llms
sent=4 received=4 packet-loss=0% min-rtt=llms avg-rtt=llms max-rtt=llms
[nouser@MikroTik] >
```

8. Criar e configurar a Bridge com as interfaces destinadas ao Hotspot. Exemplo: Vamos ter as interfaces 2, 3, 4 e 5 uma pra cada unifi e todos deverão ter o serviço de WIFI-SEGURO.



Com a bridge “hotspot” criada, basta adicionarmos as portas a essa bridge na aba Ports.



Repetir o mesmo para as demais interfaces.

Configurações WIFI-SEGURO sistema hotspot

Feito as configurações da Mikrotik falta apenas realizar o cadastro do cliente na plataforma online:

1. Acessar o servidor de hotspot: <https://masterhotspot.haysystems.com.br/>
Login e senha do colaborador.
2. Criar empresa:

Razão Social	Nome Fantasia	CNPJ ou CPF	Inscrição Municipal
CSM CLUBE DOS SERVIDORES	CSM CLUBE DOS SERVIDORES	20.913.653/0001-79	
NORTH HOTEL LTDA	NORTH HOTEL LTDA	51.880.153/0001-01	
KARLA JAQUELINE DE S. O. FREITAS	KARLA - WFS	46.338.753/0001-02	
VIVIANE VIRGINIA SANTANA 01292737670	VIVIANE (ARENA LILA)	20.173.861/0001-89	
PREFEITURA DVL	WI-FI Seguro Praças	18.291.351/0001-64	
Empresa B	Empresa B	92.541.441/0001-19	
Empresa A	Empresa A	42.044.490/0001-78	

Empresas

Organização

Relacionados

Ações

Auditor

Visualizar

Inserir

Editar

Excluir

Resultados por página: Auto Aiuste

Filtros Razão Social

contém

+

Razão Social	Nome Fantasia	CNPJ ou CPF	Inscrição Municipal	Edited Em	↑ Criado Em
PREFEITURA DVL	WI-FI Seguro Praças	18.291.351/0001-64		09/01/2024 às 14:35	09/01/2024 às 13:19
MOREIRA & QUEIROZ CLINICA ODONT. LTDA	MOREIRA & QUEIROZ CLINICA ODONT. LTDA	50.553.926/0001-82		02/01/2024 às 12:38	02/01/2024 às 12:38
Empresa B	Empresa B	92.541.441/0001-19		19/09/2023 às 11:29	19/09/2023 às 11:29
Empresa A	Empresa A	42.044.490/0001-78		19/09/2023 às 11:09	19/09/2023 às 11:09

Preencher com os dados da TAP

+ Inserir Empresa

Informações Básicas Endereço + Escrituração * Escrituração II

Razão Social	Data de Abertura	
Razão Social	Data de Abertura	
Nome Fantasia	Nome Abreviado	
Nome Fantasia	Nome Abreviado	
CNPJ ou CPF	Inscrição Municipal	Inscrição Estadual
CNPJ ou CPF	Inscrição Municipal	Inscrição Estadual
Classificação		
Organização		

Cancelar Salvar

+ Inserir Empresa

Informações Básicas Endereço + Escrituração * Escrituração II

Razão Social	Data de Abertura	
VIVIANE VIRGINIA SANTANA 01292737670	16/02/2024	
Nome Fantasia	Nome Abreviado	
VIVIANE (ARENA LILA)	WFS-DVL-000-1045861	
CNPJ ou CPF	Inscrição Municipal	Inscrição Estadual
20.173.861/0001-89	Inscrição Municipal	Inscrição Estadual
Classificação		
Organização		

Cancelar Salvar

+ Inserir Empresa

Informações Básicas Endereço + Escrituração * Escrituração II

Tipo de Endereço	Unidade Federativa	Cidade
Correspondência	Minas Gerais	Divinópolis
Bairro	Logradouro	Número
Centro	Rua Goiás, Centro, 2850	2850
Complemento		
Complemento		
Email Emitente	DDD	Numero Telefone
rocha.park@hotmail.com ,rocha.r	37	99968-7134

Cancelar Salvar

Não é necessário preencher os campos “Escrituração 1 e 2”

Após inserir a empresa ela aparecerá na lista de empresas.

Razão Social	Nome Fantasia	CNPJ ou CPF	Inscrição Municipal	Edited Em	↑ Criado Em
VIVIANE VIRGINIA SANTANA 01292737670	VIVIANE (ARENA LILA)	20.173.861/0001-89		16/02/2024 às 11:47	16/02/2024 às 11:47
PREFEITURA DVL	WI-FI Seguro Praças	18.291.351/0001-64		09/01/2024 às 14:35	09/01/2024 às 13:19
MOREIRA & QUEIROZ CLINICA ODONT. LTDA	MOREIRA & QUEIROZ CLINICA ODONT. LTDA	50.553.926/0001-82		02/01/2024 às 12:38	02/01/2024 às 12:38
Empresa B	Empresa B	92.541.441/0001-19		19/09/2023 às 11:29	19/09/2023 às 11:29
Empresa A	Empresa A	42.044.490/0001-78		19/09/2023 às 11:09	19/09/2023 às 11:09

3. Configurar grupo de usuário da empresa:

Clicar em + Inserir (Colocar o grupo a partir da ultimo cadastrado, exemplo, o ultimo é o grupo 2, então será adicionado o grupo 3)

4. Criar usuário para o cliente:

+INSERIR

Email: da empresa

Nome: Administrador – Nome da empresa

Login: a definir

Telefone: da empresa

Grupo de Usuário: foi configurado no passo anterior

Senha: master123

Obs: não é necessário preencher os campos de informações adicionais

+ Inserir Usuário

Informações Básicas

Nome: Administrador - ARENA LILA

Email: wagner.9@hotmail.com

Login: arena.lila

Telefone Pessoal: 3799968-7134

Grupo de Usuário: GRUPO 3 - VIVIA

Senha:
Confirme a Senha:

Classificação: Sistema

Cancelar | **Salvar**

5. Gerar script da RB no sistema:

HOTSPOT >> ROUTERBOARD

Routerboard

Resultados por página: Auto Ajuste

Filtros | Descrição | contém

Descrição	Endereço IP	Hostname	Porta	Ativo
MK CSM CLUBE	189.91.12.6	csm.clube	8.728	<input checked="" type="checkbox"/>
MK NORTH HOTEL	186.216.97.90	north.hotel	8.728	<input checked="" type="checkbox"/>
MK KARLA JAQUELINE	187.44.5.103	karla.jaquelle	8.728	<input checked="" type="checkbox"/>
MK VIVIANE VIRGINIA SANTANA	189.91.12.8	viviane.virginia	8.728	<input checked="" type="checkbox"/>
MK CLI KPARTY	191.240.102.0	evento.kparty	8.728	<input checked="" type="checkbox"/>
MK PRAÇA ELIZEU ZICA	189.91.12.5	praca.elizeu	8.728	<input checked="" type="checkbox"/>
MK PRAÇA CATEDRAL	189.91.12.4	praca.catedral	8.728	<input checked="" type="checkbox"/>
MK PRAÇA DA BIBLIA	189.91.12.3	praca.biblia	8.728	<input checked="" type="checkbox"/>
MK PRAÇA SANTUARIO	189.91.12.2	praca.santuario	8.728	<input checked="" type="checkbox"/>
MK TESTE NOC	189.91.12.7	noc.soumaster	8.728	<input checked="" type="checkbox"/>
RR RANCADA NOC	189.91.12.126	rrr.com.br	8.728	<input type="checkbox"/>

+Inserir

Editar Routerboard

Informações Básicas

Descrição: MK CSM CLUBE

Endereço IP: 189.91.12.6

Hostname: csm.clube

Porta: 8728

Usuário: operacao

Senha:

Solicita Voucher: Não

Ativo: Sim

Homologação: Não

Verificar Status: Verificar Status

Empresa Gestora: CSM CLUBE DOS SERVIDORES

Redirecionar: Redirecionar

Cancelar | **Salvar**

Descrição: Empresa

Endereço de IP: IP que foi configurado no I-manager

Hostname: sempre um “nome.algo” sempre deve ter o .

Porta: 8728 que foi configurada na mikrotik

Usuário e senha que foi configurada na Mikrotik.

Clicar em verificar status. Se estiver tudo ok deve ficar verde.

6. Ir na aba “Informações de Script”:

The screenshot shows a configuration interface for a Routerboard. At the top, there's a header with a plus sign and the text "Inserir Routerboard". To the right are icons for help and close. Below the header, there are two tabs: "Informações Básicas" (selected) and "Informações de Script" (with a checkmark). The "Informações Básicas" tab contains fields for "Bloco de Rede" (192.168.0.1/23) and "Interface WLAN" (bridge-hotspot). On the right, there are buttons for "Gerar Script" (with "Gerar" and "Aplicar" options), "Cancelar" (red button), and "Salvar" (blue button).

Bloco de Rede ②

192.168.0.1/23

Interface WLAN ②

bridge-hotspot

Gerar Script ②

Gerar Aplicar

Script de Configuração ②

```
:log info "Iniciando Execucao"  
# Remover quaisquer configuracoes existentes  
:do {  
    /ip pool remove hayhotspotpool;  
} on-error={
```

Cancelar **Salvar**

Bloco de rede: que será entregue para os clientes que conectarem no Wifi, pode ser qualquer bloco de rede interna.

Interface Wlan: colocar o nome da bridge que foi criada no mikrotik.

Clicar em “Gerar” e clicar em “Aplicar”.

Pronto. Agora o técnico que está realizando a instalação pode testar realizando o cadastro no Wifi.

