

**INSTITUTO POLITÉCNICO DE BEJA**  
**Escola Superior de Tecnologia e Gestão**  
**CTeSP em Redes e Sistemas Informáticos**

**Gestão de Equipamento Ativo de Rede**  
**Projeto**

**Guilherme Rodrigues Vieira**

**Beja**

**15/06/2021**

## Índice Geral

Introdução .....	6
Tabela de VLSM .....	7
Topologia da Rede .....	8
Configurações dos Routers .....	9
Servidor TFTP.....	12
Monitorização .....	18
Instalação e Configuração do Zabbix.....	21
Configuração dos Hosts Administrador e Utilizador .....	32
Ativar a UFW (Uncomplicated Firewall).....	37
Guardar todas as configurações aplicadas aos Routers e Importar e Exportar essas mesmas configurações .....	38
Instalação / Upgrade IOS .....	39
Recuperação de passwords em Routers e Switches Cisco .....	40
Routers – Passo a Passo .....	40
Switches – Passo a Passo .....	41
Conclusão.....	43

## Lista de Tabelas

Tabela 1 – VLSM.....	7
Tabela 2 - Endereços de Todas as Interfaces.....	7

## Lista de Figuras

Figura 1 - Topologia da Rede.....	8
Figura 2 - Atribuição de DHCP ao Router 1.....	9
Figura 3 - Atribuição de IP às interfaces Serial do R1, ping 8.8.8.8 e config guardada.....	9
Figura 4 - Criação da Rota no CMD para que todos os Routers tenham internet.....	10
Figura 5 - Atribuição de IPs às interfaces do R2, adição do encaminhamento para o Router 1 e config guardada.....	10
Figura 6 - Atribuição de IPs às interfaces do R3, adição do encaminhamento para o Router 1, ping 8.8.8.8 e config guardada.....	11
Figura 7 - Adicionar memória a um disco.....	12
Figura 8 - Remover eventuais ficheiros da flash preparando o Router para possíveis reposições de memória através do Servidor TFTP.....	12
Figura 9 – Verificar se o Servidor tem acesso á internet e fazer update ao mesmo.....	13
Figura 10 – Configuração do netplan.....	13
Figura 11 – Instalação do TFTP e TFTPd.....	14
Figura 12 – Depois de todas as configurações podemos ver que o Router consegue pingar o google.com.....	14
Figura 13 – Aceder por SSH ao Servidor com o software PUTTY (SSH já estava instalado por padrão).....	14
Figura 14 – Aplicação de configurações na diretória tftpd-hpa.....	15
Figura 15 – Aplicação de várias configurações ao Servidor TFTP.....	15
Figura 16 – Upload da running-config do Router 3 para o Servidor TFTP.....	16
Figura 17 – Upload da running-config de todos os Routers.....	16
Figura 18 – Conjunto de códigos que permite acesso ao Router 1 por SSH.....	16
Figura 19 – Aceder ao Router 2 por SSH com o software PUTTY.....	17
Figura 20 – Alteração das configurações da diretória netplan do PC de Monitorização.....	18
Figura 21 – IP Add.....	19
Figura 22 – Pings PC Monitorização.....	19
Figura 23 – Apt update Monitorização.....	20
Figura 24 – Aceder por SSH ao PC de Monitorização.....	21
Figura 25 – Comandos para fazer a instalação do Zabbix através do PUTTY.....	21
Figura 26 – Comando SNMP.....	22
Figura 27 – Instalação do SNMP e SNMPD no PC de Monitorização. ....	22

Figura 28 – Alteração das credenciais para entrar no Zabbix na diretoria zabbix_server.conf...	23
Figura 29 – Instalação e Configuração do Zabbix – Parte 1.....	23
Figura 30 – Instalação e Configuração do Zabbix – Parte 2.....	24
Figura 31 – Finalização da Instalação do Zabbix. ....	24
Figura 32 – Dashboard inicial do Zabbix.....	25
Figura 33 – Alteração da config dentro da diretoria SNMPD.conf.....	25
Figura 34 – Criação de hosts no Zabbix.....	26
Figura 35 – Escolha de Template.....	26
Figura 36 – Criação do host Zabbix.....	27
Figura 37 – Escolha do Template para o PC de Monitorização.....	27
Figura 38 – Criação de todos os Routers e Servidores.....	28
Figura 39 – Criação do mapa da rede.....	28
Figura 40 – Router 3 inserido no Mapa.....	29
Figura 41 – Routers e Servidor Zabbix inseridos no mapa.....	29
Figura 42 – Instalação do snmp e snmpd no servidor tftp.....	30
Figura 43 – Criação do Host Server TFTP.....	30
Figura 44 – Dashboard do Zabbix.....	31
Figura 45 – Todos os equipamentos de rede inseridos no mapa do Zabbix.....	31
Figura 46 – Configurar o DHCP no Router 2 permitindo aos PCs dos utilizadores ter ip atribuído por DHCP.....	32
Figura 47 – Configuração do netplan do PC Administrador.....	33
Figura 48 – Configuração do netplan do PC Utilizador.....	33
Figura 49 – Ping ao google.com através do Servidor TFTP.....	34
Figura 50 – Exclusão dos IPs dos PCs Administrador e Utilizador da pool DHCP.....	34
Figura 51 – Criação da ACL UTILIZADORES no Router 2.....	35
Figura 52 – Ping 172.16.1.129 (PC Administrador e Utilizador).....	36
Figura 53 – UFW.....	37
Figura 54 – Guardar todas as configs na memória do Router 2 (fez-se o mesmo para todos os Routers).....	38
Figura 55 – Códigos que temos de executar para exportar a config do Router 3 para o Server TFTP.....	38
Figura 56 – Config de todos os Routers guarda no Servidor TFTP.....	39
Figura 57 – Exemplificação da Instalação/Upgrade IOS.....	40

Figura 58 - Switch Boot.....42

## **Introdução**

Com este trabalho pretendeu-se realizar uma rede com equipamentos Cisco, mostrando a sua instalação, configuração, atualização e monitorização. Os softwares utilizados foram o GNS3 e o VirtualBox.

No decorrer do projeto houve várias etapas, sendo a primeira a utilização do TFTP para assim gerir a configuração dos routers Cisco, com este foi possível guardar as configurações dos routers, na etapa seguinte foi inserido um PC com um software de monitorização (Zabbix), este software permitiu a gestão de todos os equipamentos através do protocolo SNMP.

Depois da execução das etapas acima descritas aplicou-se ao projeto a criação das ACLs na Rede 2, possibilitando o uso mais pormenorizado/específico com o intuito de mostrar o quão vantajoso e a quantidade de possibilidades que esta implementação permite à rede e à gestão da mesma, no dispositivo que contém o TFTP também foi implementada a UFW (Uncomplicated Firewall), de forma a garantir uma maior proteção.

Por fim mostrou-se apenas no relatório como fazer a instalação e atualização do sistema operativo IOS em routers Cisco e o Procedimento de recuperação de password em equipamentos Cisco.

## Tabela de VLSM

Antes de começar o projeto propriamente dito tivemos de primeiro definir os endereços necessários para a rede, depois de definidos foi possível começar a atribuí-los á rede.

Na primeira tabela temos os endereços que cada segmento da rede detém, temos as redes internas onde se encontram os dispositivos (Rede 2 e Rede 3), na Rede 1 encontra-se apenas a interface loopback, depois temos as R1-R2 e R1-R3 que são as sub-redes que interligam os Routers.

Na segunda tabela temos os endereços de cada interface, tal como o endereço de cada dispositivo dentro das redes internas.

Tabela 1 - VLSM

TABELA DE VLSM								
Subnet Name	Needed Size	Allocated Size	Address	Mask	Dec Mask	Assignable Range	Broadcast	WildCard
R1 - Rede Interna	1	254	192.168.137.0	255.255.255.0	/24	192.168.137.1 - 192.168.137.254	192.168.137.255	0.0.0.255
R2 - Rede Interna	3	126	172.16.1.0	255.255.255.128	/25	172.16.1.1-172.16.1.126	172.16.1.127	0.0.0.127
R3 - Rede Interna	3	6	172.16.1.128	255.255.255.248	/29	172.16.1.129-172.16.1.134	172.16.1.135	0.0.0.7
R1-R2	2	2	172.16.1.136	255.255.255.252	/30	172.16.1.137-172.16.0.138	172.16.1.139	0.0.0.3
R1-R3	2	2	172.16.1.140	255.255.255.252	/30	172.16.1.141-172.16.0.142	172.16.1.143	0.0.0.3

Tabela 2 - Endereços de Todas as Interfaces

Endereços de Todas as Interfaces			
Equipamento	Interface	Endereço	Mascara
R1	F0/0	192.168.137.18	255.255.255.0
	S0/0	172.16.1.137	255.255.255.252
	S0/1	172.16.1.141	255.255.255.252
R2	F0/0	172.16.1.1	255.255.255.128
	S0/0	172.16.1.138	255.255.255.252
R3	F0/0	172.16.1.129	255.255.255.248
	S0/0	172.16.1.142	255.255.255.252
R2 - PC Administrador		172.16.1.2	255.255.255.128
R2 - PC Utilizador		172.16.1.3	255.255.255.128
R3 - TFTP		172.16.1.130	255.255.255.248
R3 - Monitorização		172.16.1.131	255.255.255.248

## Topologia da Rede

Como podemos ver esta topologia está um pouco alterada em relação á topologia base dada no enunciado, mas isto deve-se ao facto de ter 2 PCs (Rede 2 - interna) para representar algumas alterações que se pode fazer na rede utilizando ACLs, o que nos permite ter um melhor controlo da rede pois podemos permitir ou restringir acesso de acordo com o que se pretende fazer.

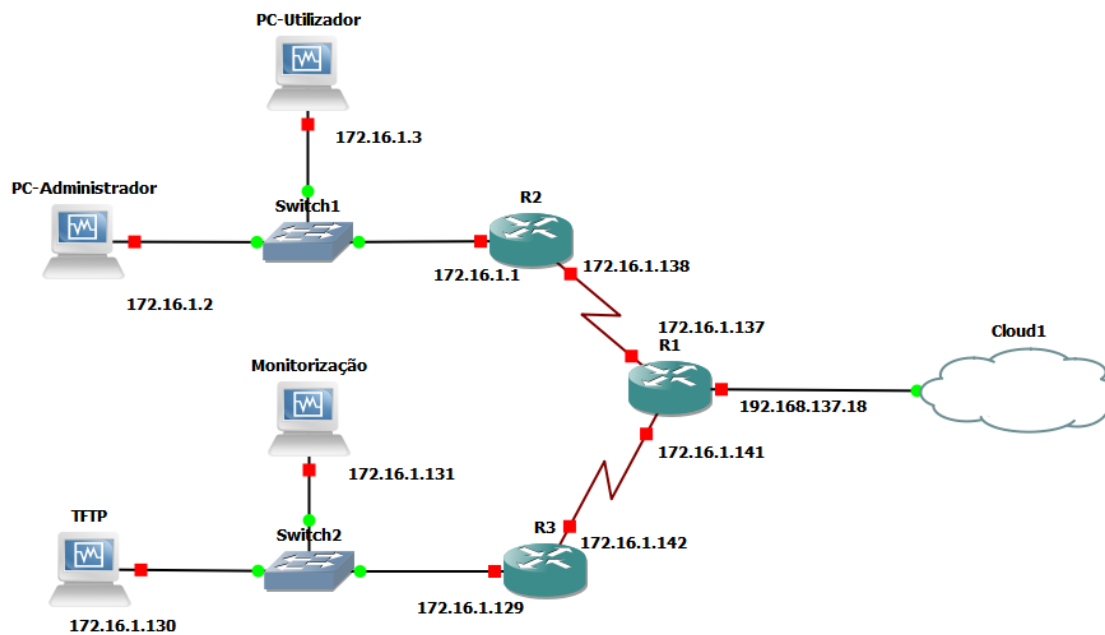


Figura 1 - Topologia da Rede



## Configurações dos Routers

Nesta etapa teve-se de inserir os respectivos endereços a cada interface (Tabela 2), fazer o DHCP no Router 1 interface F0/0, fazer o encaminhamento estático, adicionar uma rota na linha de comandos, para assim permitir que a rede toda tenha acesso á internet.

```
R1#sh
R1#show ip interface br
Interface
FastEthernet0/0      unassigned      YES unset administratively down down
Serial0/0            unassigned      YES unset administratively down down
FastEthernet0/1      unassigned      YES unset administratively down down
Serial0/1            unassigned      YES unset administratively down down
R1#cofn
Translating "cofn"

Translating "cofn"
% Unknown command or computer name, or unable to find computer address
R1#
R1#conf
Configuring from terminal, memory, or network [terminal]?
Enter configuration commands, one per line.  End with CNTL/Z.
R1(config)#int f0/0
R1(config-if)#ip ad
R1(config-if)#ip address dh
R1(config-if)#ip address dhcp
R1(config-if)#no sh
R1(config-if)#no shutdown
R1(config-if)#exit
R1(config)#exit
R1#
*Mar 1 00:00:55.319: %LINK-3-UPDOWN: Interface FastEthernet0/0, changed state to up
R1#
*Mar 1 00:00:55.443: %SYS-5-CONFIG_I: Configured from console by console
*Mar 1 00:00:56.319: %LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet0/0, changed state to up
R1ping 8.8.8.8
% Unrecognized host or address, or protocol not running.

R1#s
*Mar 1 00:01:05.783: %DHCP-6-ADDRESS_ASSIGN: Interface FastEthernet0/0 assigned DHCP address 192.168.137.94, mask 255.255.255.0, hostname R1
R1#show ip inter
R1#show ip interface br
Interface
FastEthernet0/0      192.168.137.18  YES DHCP    up          up
Serial0/0            unassigned      YES unset    administratively down down
FastEthernet0/1      unassigned      YES unset    administratively down down
Serial0/1            unassigned      YES unset    administratively down down
R1ping 8.8.8.8

Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 8.8.8.8, timeout is 2 seconds:
!!!!
Success rate is 80 percent (4/5), round-trip min/avg/max = 44/47/48 ms
R1ping 8.8.8.8

Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 8.8.8.8, timeout is 2 seconds:
!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 40/68/160 ms
```

Figura 2 - Atribuição de DHCP ao Router 1

```
R1(config)#int s0/0
R1(config-if)#ip address 172.16.1.137 255.255.255.252
R1(config-if)#no sh
R1(config-if)#no shutdown
R1(config-if)#exit
R1(config)#int
*Mar 1 00:02:40.095: %LINK-3-UPDOWN: Interface Serial0/0, changed state to up
R1(config)#int s0/
R1(config-if)#ip address 172.16.1.141 255.255.255.252
R1(config-if)#no shutdown
R1(config-if)#ex
*Mar 1 00:03:09.431: %LINK-3-UPDOWN: Interface Serial0/1, changed state to up
*Mar 1 00:03:10.431: %LINEPROTO-5-UPDOWN: Line protocol on Interface Serial0/1, changed state to up
R1(config-if)#exit
R1(config)#
*Mar 1 00:03:11.851: %LINEPROTO-5-UPDOWN: Line protocol on Interface Serial0/0, changed state to down
R1(config)#ip
*Mar 1 00:03:31.863: %LINEPROTO-5-UPDOWN: Line protocol on Interface Serial0/1, changed state to down
R1(config)#ip route 172.16.1.0 255.255.255.128 172.16.1.138
R1(config)#ip route 172.16.1.128 255.255.255.248 172.16.1.142
R1(config)#exit
R1#ping
*Mar 1 00:04:34.447: %SYS-5-CONFIG_I: Configured from console by console
R1#ping 8.8.8.8

Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 8.8.8.8, timeout is 2 seconds:
!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 40/46/48 ms
R1#
*Mar 1 00:07:41.851: %LINEPROTO-5-UPDOWN: Line protocol on Interface Serial0/0, changed state to up
R1#sh
R1#show ip in
R1#show ip interface br
Interface
FastEthernet0/0      192.168.137.18  YES DHCP    up          up
Serial0/0            172.16.1.137    YES manual  up          up
FastEthernet0/1      unassigned      YES unset    administratively down down
Serial0/1            172.16.1.141    YES manual  up          down
R1#
R1#
*Mar 1 00:09:51.859: %LINEPROTO-5-UPDOWN: Line protocol on Interface Serial0/1, changed state to up
R1#copy r
R1#copy ru
R1#copy running-config st
R1#copy running-config startup-config
Destination filename [startup-config]?
Building configuration...
[OK]
R1#
```

Figura 3 - Atribuição de IP às interfaces Serial do R1, ping 8.8.8.8 e config guardada

```
C:\WINDOWS\system32>route add 172.16.1.0 mask 255.255.255.0 192.168.137.18
OK!

C:\WINDOWS\system32>
```

Interface	IP-Address	OK?	Method	Status	Protocol
FastEthernet0/0	192.168.137.18	YES	DHCP	up	up
Serial0/0	172.16.1.137	YES	manual	up	up
FastEthernet0/1	unassigned	YES	unset	administratively down	down
Serial0/1	172.16.1.141	YES	manual	up	down

```
R1#
R1#
```

Figura 4 - Criação da Rota no CMD para que todos os Routers tenham internet

```
R2(config)#int s0/0
R2(config-if)#ip ad
R2(config-if)#ip address 172.16.1.138 255.255.255.252
R2(config-if)#no sh
R2(config-if)#no shutdown
R2(config-if)#
*Mar 1 00:05:43.819: %LINK-3-UPDOWN: Interface Serial0/0, changed state to up
*Mar 1 00:05:44.819: %LINEPROTO-5-UPDOWN: Line protocol on Interface Serial0/0, changed state to up
R2(config-if)#exit
R2(config)#int f0/0
R2(config-if)#ip ad
R2(config-if)#ip address 172.16.1.1 255.255.255.128
R2(config-if)#no sh
R2(config-if)#no shutdown
R2(config-if)#exit
R2(config)#i
*Mar 1 00:06:45.399: %LINK-3-UPDOWN: Interface FastEthernet0/0, changed state to up
*Mar 1 00:06:46.399: %LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet0/0, changed state to up
R2(config)#ip route 0.0.0.0 0.0.0.0 172.16.1.137
R2(config)#exit
R2#co
*Mar 1 00:07:10.819: %SYS-5-CONFIG_I: Configured from console by console
R2#copy ru
R2#copy running-config st
R2#copy running-config startup-config
Destination filename [startup-config]?
Building configuration...
[OK]
R2#
```

Figura 5 - Atribuição de IPs às interfaces do R2, adição do encaminhamento para o Router 1 e config guardada

```

R3(config)#int s0/0
R3(config-if)#ip add
R3(config-if)#ip address 172.16.1.142 255.255.255.252
R3(config-if)#no shutdown
R3(config-if)#exit
R3(config)#i
*Mar 1 00:09:42.043: %LINK-3-UPDOWN: Interface Serial0/0, changed state to up
*Mar 1 00:09:43.043: %LINEPROTO-5-UPDOWN: Line protocol on Interface Serial0/0, changed state to up
R3(config)#ip route 0.0.0.0 0.0.0.0 172.16.1.141
R3(config)#exit
R3#ping 8.8.8.8

Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 8.8.8.8, timeout is 2 seconds:
!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 76/77/80 ms
R3#[~conf
% Unknown command or computer name, or unable to find computer address
R3#conf
Configuring from terminal, memory, or network [terminal]?
Enter configuration commands, one per line. End with CNTL/Z.
R3(config)#int f0/0
R3(config-if)#ip ad
R3(config-if)#ip address 172.16.1.129 255.255.255.248
R3(config-if)#no sh
R3(config-if)#no shutdown
R3(config-if)#
R3(config-if)#exit
R3(config)#exit
R3#copy
*Mar 1 00:31:35.999: %SYS-5-CONFIG_I: Configured from console by console
R3#copy ru
R3#copy running-config star
R3#copy running-config startup-config
Destination filename [startup-config]?
Building configuration...
[OK]
R3#

```

Figura 6 - Atribuição de IPs às interfaces do R3, adição do encaminhamento para o Router 1, ping 8.8.8.8 e config guardada

## Servidor TFTP

Na criação do Servidor TFTP foi usado um computador com o Sistema Operativo Ubuntu, este foi utilizado para guardar a configuração dos equipamentos de rede, neste caso as configurações dos Routers Cisco.

Nas imagens seguintes irá ser demonstrado como se cria o Servidor TFTP, como se prepara os Routers para guardarem as configurações, como importar as configurações do Router para o Servidor TFTP, como ir buscar a configuração ao Servidor e aplicar no Router e como aceder ao Servidor via SSH.

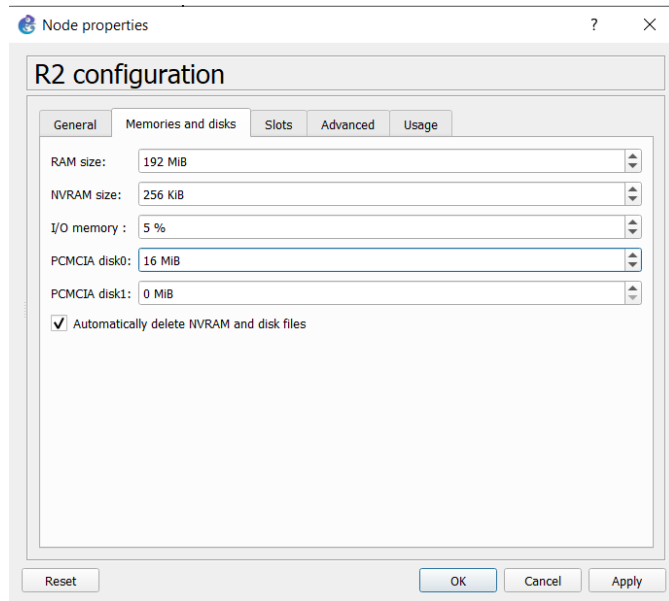


Figura 7 - Adicionar memória a um disco

```
R2#erase fl
R2#erase flash:
Erasing the flash filesystem will remove all files! Continue? [confirm]
Current DOS File System flash card in flash: will be Formatted into Low End File System flash card! Continue? [confirm]
Erasing device... ..erased
Erase of flash: complete
R2#copy ru
R2#copy running-config new
R2#copy running-config newconfig
Destination filename [newconfig]?
Erase flash: before copying? [confirm]
Erasing the flash filesystem will remove all files! Continue? [confirm]
Erasing device... ..erased
Erase of flash: complete
Verifying checksum... OK (0x7AE8)
920 bytes copied in 0.456 secs (2018 bytes/sec)
```

Figura 8 - Remover eventuais ficheiros da flash preparando o Router para possíveis reposições de memória através do Servidor TFTP

```

from 172.16.1.130 icmp_seq=4 Destination Host Unreachable
from 172.16.1.130 icmp_seq=5 Destination Host Unreachable
from 172.16.1.130 icmp_seq=6 Destination Host Unreachable
2
[1]+  Stopped                  ping 8.8.8.8
gear@gear:~$ ping 172.16.1.129
PING 172.16.1.129 (172.16.1.129) 56(84) bytes of data.
from 172.16.1.130 icmp_seq=1 Destination Host Unreachable
from 172.16.1.130 icmp_seq=2 Destination Host Unreachable
from 172.16.1.130 icmp_seq=3 Destination Host Unreachable
2
[2]+  Stopped                  ping 172.16.1.129
gear@gear:~$ ping 172.16.1.129
PING 172.16.1.129 (172.16.1.129) 56(84) bytes of data.
64 bytes from 172.16.1.129: icmp_seq=1 ttl=255 time=11.8 ms
64 bytes from 172.16.1.129: icmp_seq=2 ttl=255 time=4.36 ms
2
[3]+  Stopped                  ping 172.16.1.129
gear@gear:~$ ping 8.8.8.8
PING 8.8.8.8 (8.8.8.8) 56(84) bytes of data.
64 bytes from 8.8.8.8: icmp_seq=1 ttl=56 time=41.0 ms
2
[4]+  Stopped                  ping 8.8.8.8
gear@gear:~$ sudo apt update
Hit:1 http://pt.archive.ubuntu.com/ubuntu bionic InRelease
Hit:2 http://pt.archive.ubuntu.com/ubuntu bionic-updates InRelease
Hit:3 http://pt.archive.ubuntu.com/ubuntu bionic-backports InRelease
Get:4 http://security.ubuntu.com/ubuntu bionic-security InRelease [88.7 kB]
Fetched 88.7 kB in 1s (66.5 kB/s)
Reading package lists... Done
Building dependency tree
Reading state information... Done
All packages are up to date.
gear@gear:~$

```

Figura 9 – Verificar se o Servidor tem acesso á internet e fazer update ao mesmo

```

root@gear:~# nano /etc/netplan/01-netcfg.yaml

# This file describes the network interfaces available on your system
# For more information, see netplan(5).
network:
  version: 2
  renderer: networkd
  ethernets:
    enp0s3:
      addresses:
        - 172.16.1.130/29
      gateway4: 172.16.1.129
      nameservers:
        addresses: [8.8.8.8, 1.1.1.1]

```

Figura 10 – Configuração do netplan

```

gear@gear:~$ sudo apt install tftp-hpa tftpd-hpa
Reading package lists... Done
Building dependency tree
Reading state information... Done
Suggested packages:
  pxelinux
The following NEW packages will be installed:
  tftp-hpa tftpd-hpa
0 upgraded, 2 newly installed, 0 to remove and 0 not upgraded.
Need to get 57.5 kB of archives.
After this operation, 172 kB of additional disk space will be used.
Get:1 http://pt.archive.ubuntu.com/ubuntu bionic/main amd64 tftp-hpa amd64 5.2+20150808-1ubuntu3 [10.3 kB]
Get:2 http://pt.archive.ubuntu.com/ubuntu bionic/main amd64 tftpd-hpa amd64 5.2+20150808-1ubuntu3 [9.1 kB]
Fetched 57.5 kB in 1s (97.5 kB/s)
Preconfiguring packages ...
Selecting previously unselected package tftp-hpa.
(Reading database ... 59201 files and directories currently installed.)
Preparing to unpack .../tftp-hpa_5.2+20150808-1ubuntu3_amd64.deb ...
Unpacking tftp-hpa (5.2+20150808-1ubuntu3) ...
Selecting previously unselected package tftpd-hpa.
Preparing to unpack .../tftpd-hpa_5.2+20150808-1ubuntu3_amd64.deb ...
Unpacking tftpd-hpa (5.2+20150808-1ubuntu3) ...
Setting up tftpd-hpa (5.2+20150808-1ubuntu3) ...
Setting up tftp-hpa (5.2+20150808-1ubuntu3) ...
Processing triggers for systemd (237-3ubuntu10.47) ...
Processing triggers for man-db (2.8.3-2ubuntu0.1) ...
Processing triggers for ureadahead (0.100.0-21) ...
gear@gear:~$ _

```

Figura 11 – Instalação do TFTP e TFTPd

```

gear@gear:~$ ping google.com
PING google.com (172.217.168.174) 56(84) bytes of data:
64 bytes from mad07s10-in-f14.1e100.net (172.217.168.174): icmp_seq=1 ttl=56 time=30.7 ms
64 bytes from mad07s10-in-f14.1e100.net (172.217.168.174): icmp_seq=2 ttl=56 time=41.9 ms
64 bytes from mad07s10-in-f14.1e100.net (172.217.168.174): icmp_seq=3 ttl=56 time=42.9 ms
^C
[2]+  Stopped                  ping google.com
gear@gear:~$

```

Figura 12 – Depois de todas as configurações podemos ver que o Router consegue pingar o google.com

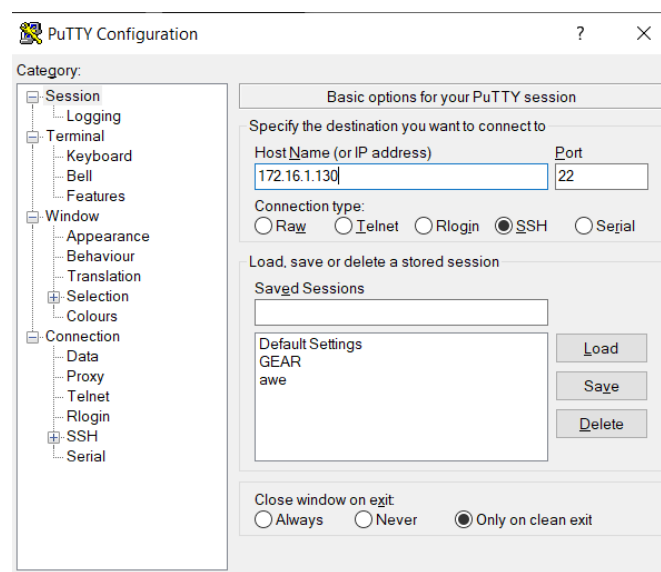


Figura 13 – Aceder por SSH ao Servidor com o software PUTTY (SSH já estava instalado por padrão)

```
GNU nano 2.9.3 /etc/default/tftpd-hpa Modified
# /etc/default/tftpd-hpa

TFTP_USERNAME="tftp"
TFTP_DIRECTORY="/var/lib/tftpboot"
TFTP_ADDRESS=":69"
TFTP_OPTIONS="--secure --create"

^G Get Help ^O Write Out ^W Where Is ^K Cut Text ^J Justify ^C Cur Pos
^X Exit ^R Read File ^\ Replace ^U Uncut Text ^T To Spell ^_ Go To Line
```

Figura 14 – Aplicação de configurações na diretória tftpd-hpa

Nesta imagem podemos ver que temos códigos de proteção diferentes (Jojlh/MZ72I), isto deve se ao facto de estar a guardar imagens durante a criação do projeto e em dada altura ter um problema que impossibilitava de continuar o projeto e depois tinha de refazer tudo novamente, fazendo com que na fez seguinte tivesse um código diferente.

```
login as: gear
gear@172.16.1.130's password:
Welcome to Ubuntu 18.04.5 LTS (GNU/Linux 4.15.0-144-generic x86_64)

* Documentation:  https://help.ubuntu.com
* Management:    https://landscape.canonical.com
* Support:        https://ubuntu.com/advantage
New release '20.04.2 LTS' available.
Run 'do-release-upgrade' to upgrade to it.

Last login: Sat Jun  5 19:15:51 2021
gear@gear:~$ cd /var/lib/tftpboot/
gear@gear:/var/lib/tftpboot$ ls
gear@gear:/var/lib/tftpboot$ sudo mktemp -d XXXXX --suffix=-outgoing
[sudo] password for gear:
Jojlh-outgoing
gear@gear:/var/lib/tftpboot$ sudo chmod 755
gear@gear:/var/lib/tftpboot$ sudo chmod 755 Jojlh-outgoing
gear@gear:/var/lib/tftpboot$ ls -la
total 12
drwxr-xr-x  3 root nogroup 4096 Jun  5 19:38 .
drwxr-xr-x 36 root root    4096 Jun  5 19:26 ..
drwxr-xr-x  2 root root    4096 Jun  5 19:38 Jojlh-outgoing
gear@gear:/var/lib/tftpboot$
gear@gear:/var/lib/tftpboot$ sudo mktemp -d XXXXX --suffix=-incomming
MZ72I-incomming
gear@gear:/var/lib/tftpboot$ sudo chown tftp:tftp MZ72I-incomming
gear@gear:/var/lib/tftpboot$ sudo nano /etc/default/tftpd-hpa
```

Figura 15 – Aplicação de várias configurações ao Servidor TFTP

No lado direito podemos ver que estamos no Router 3 e fazemos uma cópia da running-config do mesmo para o Servidor TFTP (lado esquerdo) e podemos ver que esta foi concluída com sucesso pois essa mesma config encontra-se lá.

```
gear@gear:/var/lib/tftpboot$ sudo /etc/init.d/tftpd-hpa restart
[ ok ] Restarting tftpd-hpa (via systemctl): tftpd-hpa.service
.
gear@gear:/var/lib/tftpboot$
gear@gear:/var/lib/tftpboot$ sudo ufw status
Status: inactive
gear@gear:/var/lib/tftpboot$ sudo ls MZ72I-incomming/
R3-backup
```

```
R3#copy running-config tftp://172.16.1.130/MZ72I-incomming/R3-backup
Address or name of remote host [172.16.1.130]?
Destination filename [MZ72I-incomming/R3-backup]?
!!
922 bytes copied in 0.244 secs (3779 bytes/sec)
R3#
```

solarwinds | Solar-PuTTY free tool

Figura 16 – Upload da running-config do Router 3 para o Servidor TFTP

```
gear@gear:/var/lib/tftpboot$ sudo ls MZ72I-incomming/
[sudo] password for gear:
R1-backup R2-backup R3-backup
gear@gear:/var/lib/tftpboot$
```

Figura 17 – Upload da running-config de todos os Routers

Este conjunto de códigos foi executado em todos os Routers de forma a permitir o acesso a estes mesmos por SSH.

```
R1#conf
Configuring from terminal, memory, or network [terminal]?
Enter configuration commands, one per line. End with CNTL/Z.
R1(config)#aaa new-model
R1(config)#aaa aut
R1(config)#aaa authentication login default local
R1(config)#line vty 0 4
R1(config-line)#login authentication default
R1(config-line)#end
R1#
R1(config)#ip domain-name gear.pt
R1(config)#enable secret gear

R1(config)#crypto key generate rsa
The name for the keys will be: R1.gear.pt
Choose the size of the key modulus in the range of 360 to 2048 for your
General Purpose Keys. Choosing a key modulus greater than 512 may take
a few minutes.

How many bits in the modulus [512]: 2048
R1(config)#username gear password gear
R1(config)#line vty 0 15
R1(config-line)#transport input ssh
R1(config-line)#ip ssh version 2
R1(config)#end
```

Figura 18 – Conjunto de códigos que permite acesso ao Router 1 por SSH



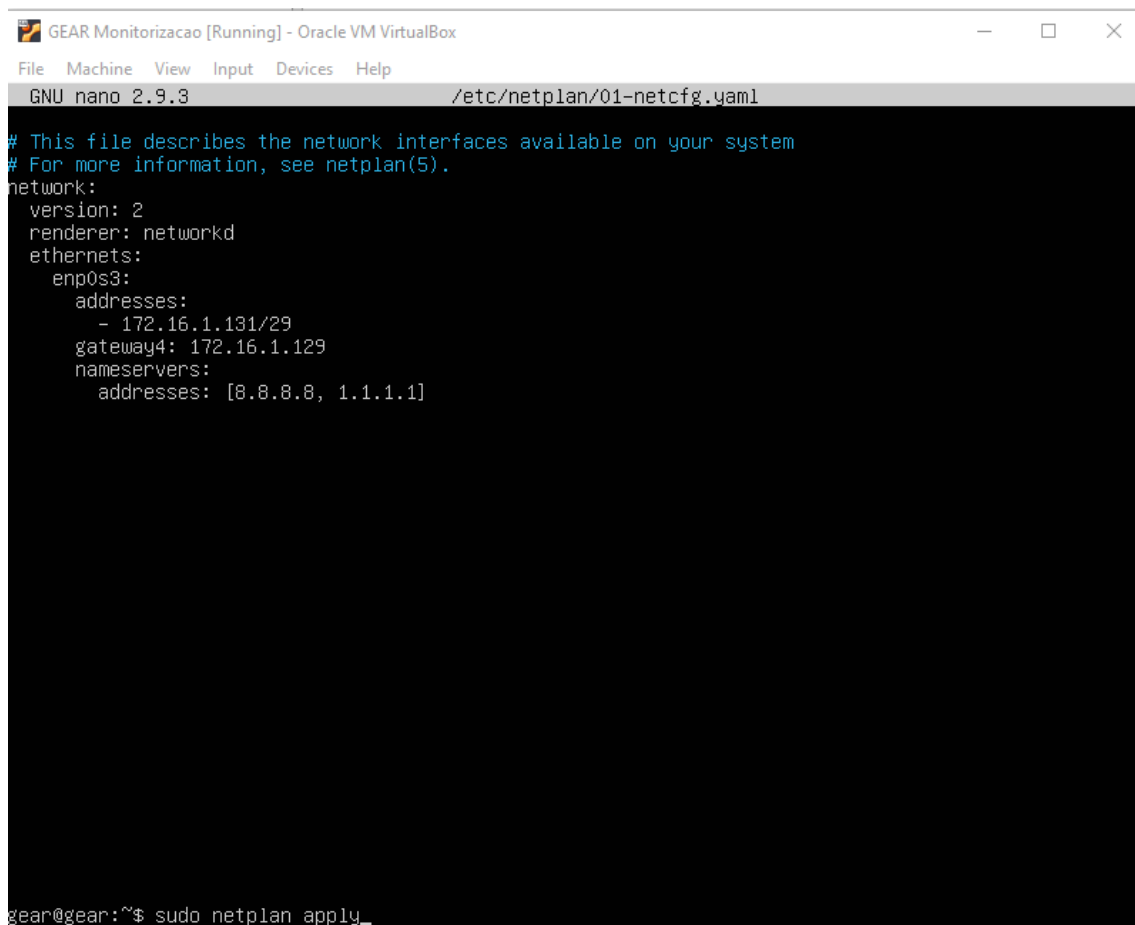
Nesta imagem podemos ver que é possível aceder por SSH ao Router 2, sendo que também é possível aceder aos demais Routers por SSH com os seus endereços das interfaces, s0 (R2 e R3), f0 (R1 - DHCP)



Figura 19 – Aceder ao Router 2 por SSH com o software PUTTY

## Monitorização

Esta virtual machine (Monitorização) permite-nos fazer a monitorização de todos os equipamentos de rede através do protocolo SNMP, a monitorização é uma ferramenta bastante importante pois permite visualizar vários parâmetros importantes de cada dispositivo, tais como a temperatura, velocidade de transferência de dados, uso de recursos entre outros. Num caso prático se uma empresa tiver este recurso implementado na rede pode ser possível detetar um futuro problema/vulnerabilidade, conseguindo minimizar os estragos.



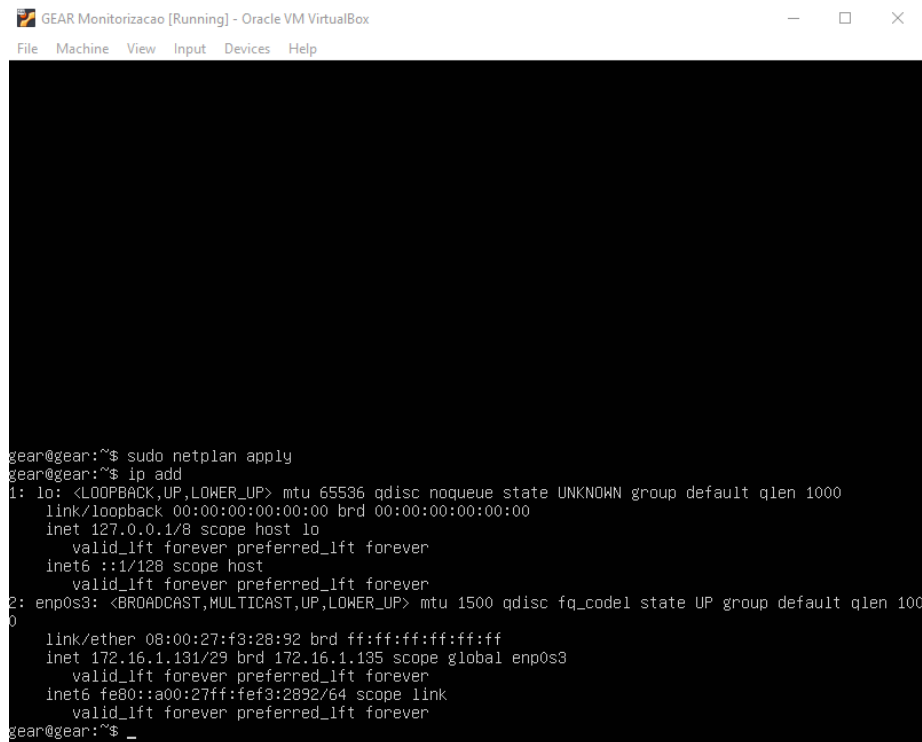
```
GEAR Monitorizacao [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
GNU nano 2.9.3 /etc/netplan/01-netcfg.yaml

# This file describes the network interfaces available on your system
# For more information, see netplan(5).
network:
  version: 2
  renderer: networkd
  ethernets:
    enp0s3:
      addresses:
        - 172.16.1.131/29
      gateway4: 172.16.1.129
      nameservers:
        addresses: [8.8.8.8, 1.1.1.1]

gear@gear:~$ sudo netplan apply_
```

Figura 20 – Alteração das configurações da diretória netplan do PC de Monitorização

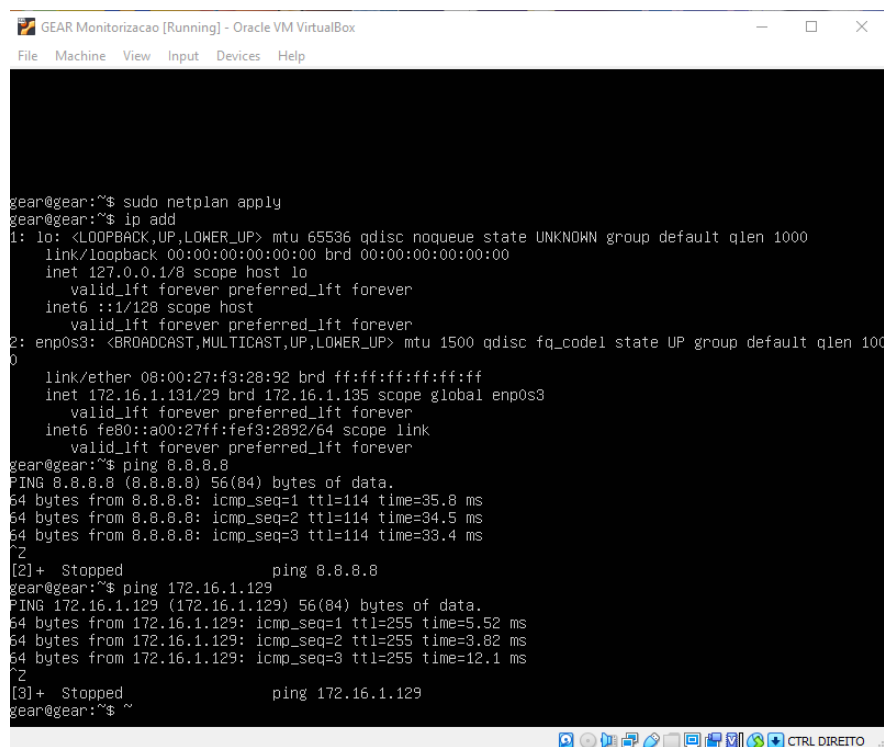
Com o uso do IP add podemos verificar se o endereço da máquina está corretamente atribuído



```
GEAR Monitorizacao [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help

gear@gear:~$ sudo netplan apply
gear@gear:~$ ip add
1: lo: <LOOPBACK,UP,LOWER_UP> mtu 65536 qdisc noqueue state UNKNOWN group default qlen 1000
    link/loopback 00:00:00:00:00:00 brd 00:00:00:00:00:00
    inet 127.0.0.1/8 scope host lo
        valid_lft forever preferred_lft forever
    inet6 ::1/128 scope host
        valid_lft forever preferred_lft forever
2: enp0s3: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc fq_codel state UP group default qlen 1000
    link/ether 08:00:27:f3:28:92 brd ff:ff:ff:ff:ff:ff
    inet 172.16.1.131/29 brd 172.16.1.135 scope global enp0s3
        valid_lft forever preferred_lft forever
    inet6 fe80::a00:27ff:fe3:2892/64 scope link
        valid_lft forever preferred_lft forever
gear@gear:~$ _
```

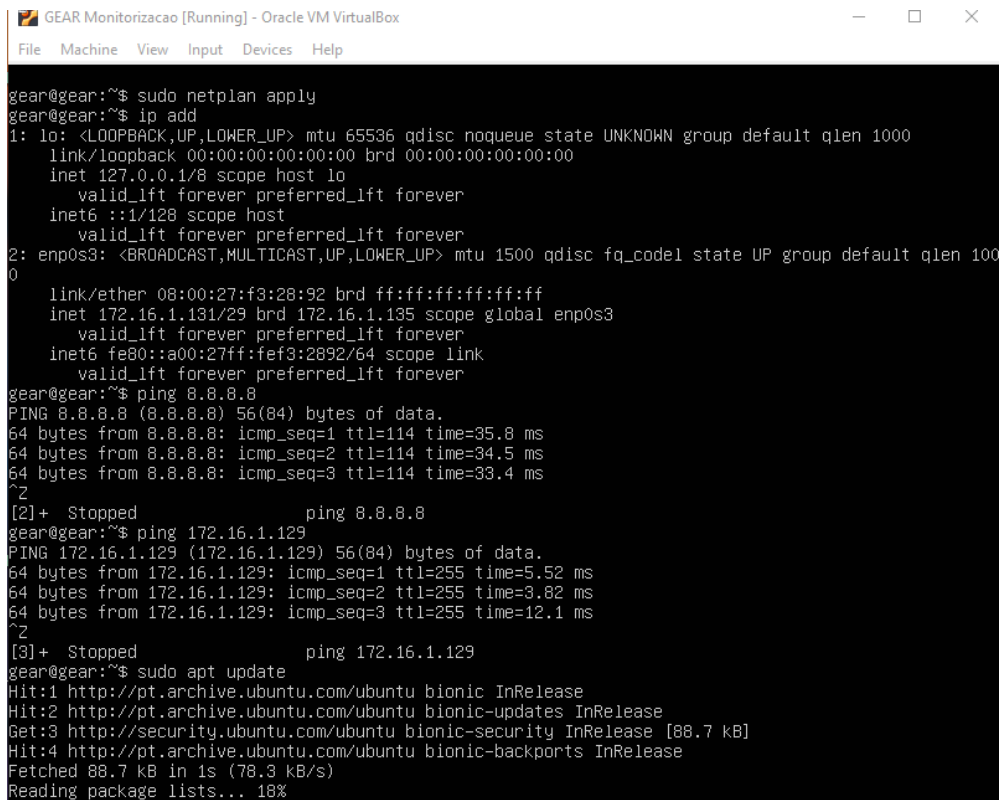
Figura 21 – IP Add



```
GEAR Monitorizacao [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help

gear@gear:~$ sudo netplan apply
gear@gear:~$ ip add
1: lo: <LOOPBACK,UP,LOWER_UP> mtu 65536 qdisc noqueue state UNKNOWN group default qlen 1000
    link/loopback 00:00:00:00:00:00 brd 00:00:00:00:00:00
    inet 127.0.0.1/8 scope host lo
        valid_lft forever preferred_lft forever
    inet6 ::1/128 scope host
        valid_lft forever preferred_lft forever
2: enp0s3: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc fq_codel state UP group default qlen 1000
    link/ether 08:00:27:f3:28:92 brd ff:ff:ff:ff:ff:ff
    inet 172.16.1.131/29 brd 172.16.1.135 scope global enp0s3
        valid_lft forever preferred_lft forever
    inet6 fe80::a00:27ff:fe3:2892/64 scope link
        valid_lft forever preferred_lft forever
gear@gear:~$ ping 8.8.8.8
PING 8.8.8.8 (8.8.8.8) 56(84) bytes of data.
64 bytes from 8.8.8.8: icmp_seq=1 ttl=114 time=35.8 ms
64 bytes from 8.8.8.8: icmp_seq=2 ttl=114 time=34.5 ms
64 bytes from 8.8.8.8: icmp_seq=3 ttl=114 time=33.4 ms
^C
[2]+  Stopped                  ping 8.8.8.8
gear@gear:~$ ping 172.16.1.129
PING 172.16.1.129 (172.16.1.129) 56(84) bytes of data.
64 bytes from 172.16.1.129: icmp_seq=1 ttl=255 time=5.52 ms
64 bytes from 172.16.1.129: icmp_seq=2 ttl=255 time=3.82 ms
64 bytes from 172.16.1.129: icmp_seq=3 ttl=255 time=12.1 ms
^C
[3]+  Stopped                  ping 172.16.1.129
gear@gear:~$ ~
```

Figura 22 – Pings PC Monitorização



```
gear@gear:~$ sudo netplan apply
gear@gear:~$ ip add
1: lo: <LOOPBACK,UP,LOWER_UP> mtu 65536 qdisc noqueue state UNKNOWN group default qlen 1000
    link/loopback 00:00:00:00:00:00 brd 00:00:00:00:00:00
    inet 127.0.0.1/8 scope host lo
        valid_lft forever preferred_lft forever
    inet6 ::1/128 scope host
        valid_lft forever preferred_lft forever
2: enp0s3: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc fq_codel state UP group default qlen 1000
    link/ether 08:00:27:f3:28:92 brd ff:ff:ff:ff:ff:ff
    inet 172.16.1.131/29 brd 172.16.1.135 scope global enp0s3
        valid_lft forever preferred_lft forever
    inet6 fe80::a00:27ff:fef3:2892/64 scope link
        valid_lft forever preferred_lft forever
gear@gear:~$ ping 8.8.8.8
PING 8.8.8.8 (8.8.8.8) 56(84) bytes of data.
64 bytes from 8.8.8.8: icmp_seq=1 ttl=114 time=35.8 ms
64 bytes from 8.8.8.8: icmp_seq=2 ttl=114 time=34.5 ms
64 bytes from 8.8.8.8: icmp_seq=3 ttl=114 time=33.4 ms
^C
[2]+  Stopped                  ping 8.8.8.8
gear@gear:~$ ping 172.16.1.129
PING 172.16.1.129 (172.16.1.129) 56(84) bytes of data.
64 bytes from 172.16.1.129: icmp_seq=1 ttl=255 time=5.52 ms
64 bytes from 172.16.1.129: icmp_seq=2 ttl=255 time=3.82 ms
64 bytes from 172.16.1.129: icmp_seq=3 ttl=255 time=12.1 ms
^C
[3]+  Stopped                  ping 172.16.1.129
gear@gear:~$ sudo apt update
Hit:1 http://pt.archive.ubuntu.com/ubuntu bionic InRelease
Hit:2 http://pt.archive.ubuntu.com/ubuntu bionic-updates InRelease
Get:3 http://security.ubuntu.com/ubuntu bionic-security InRelease [88.7 kB]
Hit:4 http://pt.archive.ubuntu.com/ubuntu bionic-backports InRelease
Fetched 88.7 kB in 1s (78.3 kB/s)
Reading package lists... 18%
```

Figura 23 – Apt update Monitorização

## Instalação e Configuração do Zabbix

Nesta etapa do projeto iremos instalar o Zabbix no computador de monitorização com a ajuda do Software PUTTY através do SSH, iremos instalar o SNMP para permitir monitorizar o PC de Monitorização assim como a todos os outros equipamentos da nossa rede, iremos mostrar o passo a passo de como criar hosts no Zabbix, criar mapas e definir a monitorização de certos parâmetros.

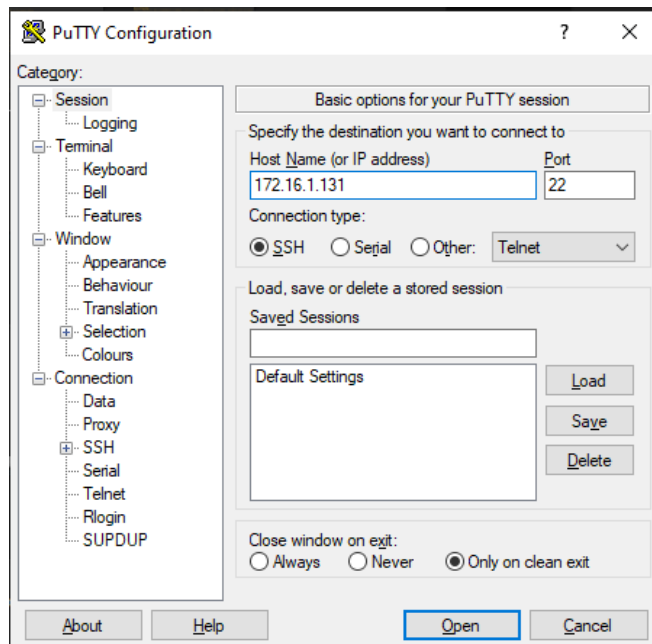


Figura 24 – Aceder por SSH ao PC de Monitorização

```
gear@gear:~$ wget https://repo.zabbix.com/zabbix/5.4/ubuntu/pool/main/z/zabbix-release/zabbix-release_5.4-1+ubuntu18.04_all.deb
gear@gear:~$ sudo dpkg -i zabbix-release_5.4-1+ubuntu18.04_all.deb
[sudo] password for gear:
gear@gear:~$ sudo apt update
gear@gear:~$ sudo apt install zabbix-server-mysql zabbix-frontend-php zabbix-apache-conf zabbix-sql-scripts zabbix-agent
gear@gear:~$ sudo su
root@gear:/home/gear# mysql -uroot -p
Enter password:
mysql> create database zabbix character set utf8 collate utf8_bin;
Query OK, 1 row affected (0.00 sec)

mysql> create user zabbix@localhost identified by 'gear';
Query OK, 0 rows affected (0.00 sec)

mysql> grant all privileges on zabbix.* to zabbix@localhost;
Query OK, 0 rows affected (0.00 sec)

mysql> quit;
Bye
gear@gear:~$ zcat /usr/share/doc/zabbix-sql-scripts/mysql/create.sql.gz | mysql -uzabbix -p zabbix
Enter password:
gear@gear:~$ sudo nano /etc/zabbix/zabbix_server.conf
gear@gear:~$ sudo systemctl restart zabbix-server zabbix-agent apache2
gear@gear:~$ sudo systemctl enable zabbix-server zabbix-agent apache2
Synchronizing state of zabbix-server.service with SysV service script with /lib/systemd/systemd-sysv-install.
Executing: /lib/systemd/systemd-sysv-install enable zabbix-server
Synchronizing state of zabbix-agent.service with SysV service script with /lib/systemd/systemd-sysv-install.
Executing: /lib/systemd/systemd-sysv-install enable zabbix-agent
Synchronizing state of apache2.service with SysV service script with /lib/systemd/systemd-sysv-install.
Executing: /lib/systemd/systemd-sysv-install enable apache2
```

Figura 25 – Comandos para fazer a instalação do Zabbix através do PUTTY

Este comando SNMP foi executado em todos os Routers de forma a permitir a sua monitorização.

```
R3(config)#snmp-server community public ro
```

Figura 26 – Comando SNMP

```
gear@gear:~$ sudo apt install snmp snmpd
gear@gear:~$ sudo snmpwalk -v2c -c public 172.16.1.129
iso.3.6.1.2.1.47.1.3.3.1.1.11 = INTEGER: 11
iso.3.6.1.2.1.47.1.3.3.1.1.2.3 = INTEGER: 3
iso.3.6.1.2.1.47.1.3.3.1.1.3.4 = INTEGER: 4
iso.3.6.1.2.1.47.1.3.3.1.1.3.7 = INTEGER: 7
iso.3.6.1.2.1.47.1.3.3.1.1.3.8 = INTEGER: 8
iso.3.6.1.2.1.47.1.3.3.1.1.3.9 = INTEGER: 9
iso.3.6.1.2.1.47.1.3.3.1.1.3.10 = INTEGER: 10
iso.3.6.1.2.1.47.1.3.3.1.1.3.12 = INTEGER: 12
iso.3.6.1.2.1.47.1.3.3.1.1.3.13 = INTEGER: 13
iso.3.6.1.2.1.47.1.3.3.1.1.4.5 = INTEGER: 5
iso.3.6.1.2.1.47.1.3.3.1.1.5.6 = INTEGER: 6
iso.3.6.1.2.1.47.1.4.1.0 = Timeticks: (254) 0:00:02.54
iso.3.6.1.2.1.51.2.1.0 = Gauge32: 0
iso.3.6.1.2.1.51.2.2.0 = INTEGER: 0
iso.3.6.1.2.1.51.2.3.0 = INTEGER: 0
iso.3.6.1.2.1.51.2.4.0 = INTEGER: 0
iso.3.6.1.2.1.51.2.5.0 = INTEGER: 0
iso.3.6.1.2.1.52.2.1.0 = INTEGER: 0
iso.3.6.1.2.1.68.1.1.0 = INTEGER: 1
iso.3.6.1.2.1.68.1.2.0 = INTEGER: 2
iso.3.6.1.2.1.68.2.1.0 = Counter32: 0
iso.3.6.1.2.1.68.2.2.0 = Counter32: 0
iso.3.6.1.2.1.68.2.3.0 = Counter32: 0
iso.3.6.1.2.1.83.1.1.1.0 = INTEGER: 2
iso.3.6.1.2.1.83.1.1.7.0 = Gauge32: 0
iso.3.6.1.2.1.88.1.1.1.0 = INTEGER: 60
iso.3.6.1.2.1.88.1.1.2.0 = Gauge32: 0
iso.3.6.1.2.1.88.1.1.3.0 = Gauge32: 0
iso.3.6.1.2.1.88.1.1.4.0 = Gauge32: 0
iso.3.6.1.2.1.88.1.1.5.0 = Counter32: 0
iso.3.6.1.2.1.88.1.2.1.0 = Counter32: 0
iso.3.6.1.2.1.88.1.4.1.0 = Counter32: 0
iso.3.6.1.2.1.92.1.1.1.0 = Gauge32: 500
iso.3.6.1.2.1.92.1.1.2.0 = Gauge32: 15
iso.3.6.1.2.1.92.1.2.1.0 = Counter32: 0
iso.3.6.1.2.1.92.1.2.2.0 = Counter32: 0
gear@gear:~$
```

Figura 27 – Instalação do SNMP e SNMPD no PC de Monitorização

```
gear@gear: ~
GNU nano 2.9.3 /etc/zabbix/zabbix_server.conf Modified
# Schema name. Used for PostgreSQL.
#
# Mandatory: no
# Default:
# DBSchema=

### Option: DBUser
# Database user.
#
# Mandatory: no
# Default:
# DBUser=

DBUser=zabbix

### Option: DBPassword
DBPassword=gear
# Database password.
# Comment this line if no password is used.
#
# Mandatory: no
# Default:
# DBPassword=

### Option: DBSocket
# Path to MySQL socket.
#
# Mandatory: no

^G Get Help ^O Write Out ^W Where Is ^K Cut Text ^J Justify ^C Cur Pos ^M-U Undo
^X Exit ^R Read File ^N Replace ^U Uncut Text ^T To Spell ^A Go To Line ^M-E Redo
```

Figura 28 – Alteração das credenciais para entrar no Zabbix na diretoria zabbix\_server.conf

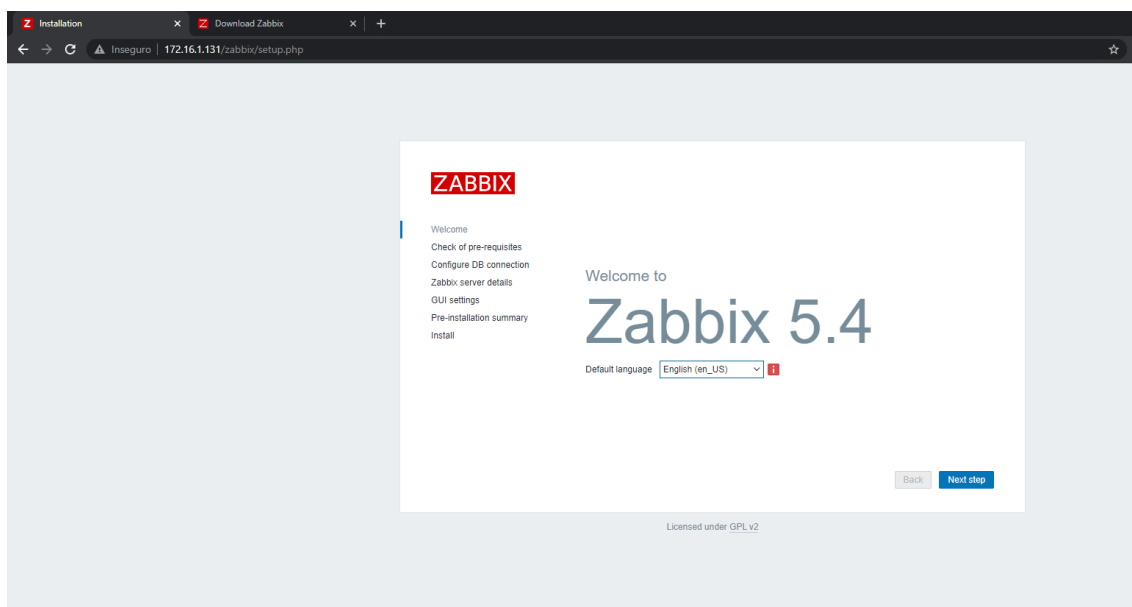


Figura 29 – Instalação e Configuração do Zabbix – Parte 1

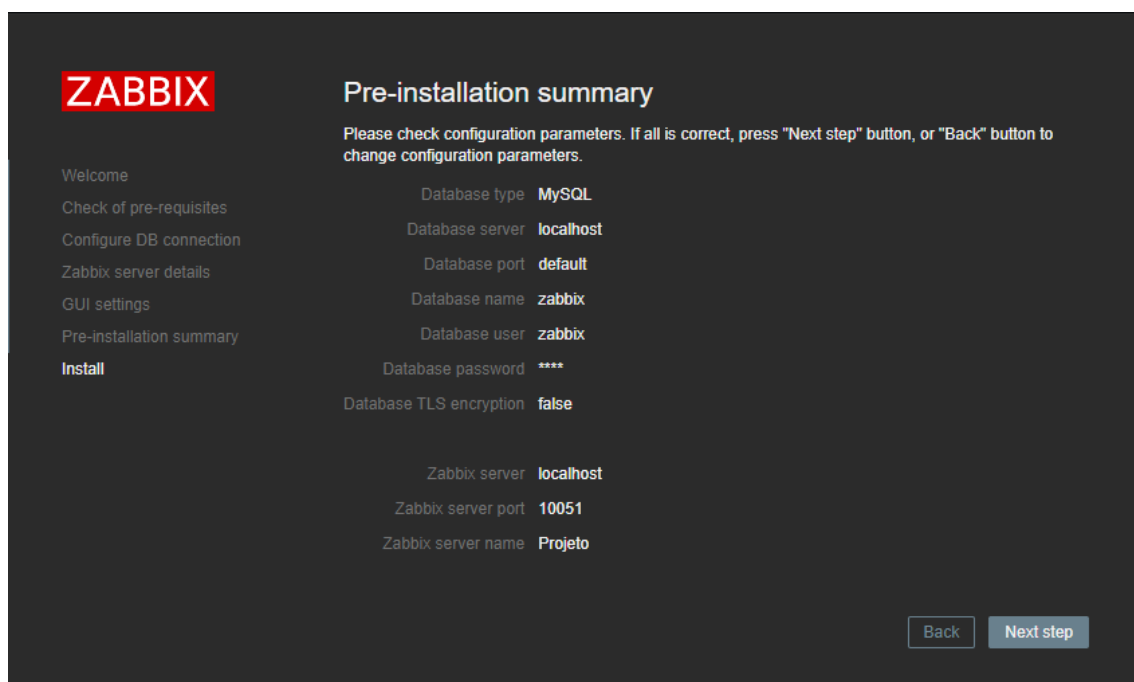


Figura 30 – Instalação e Configuração do Zabbix – Parte 2

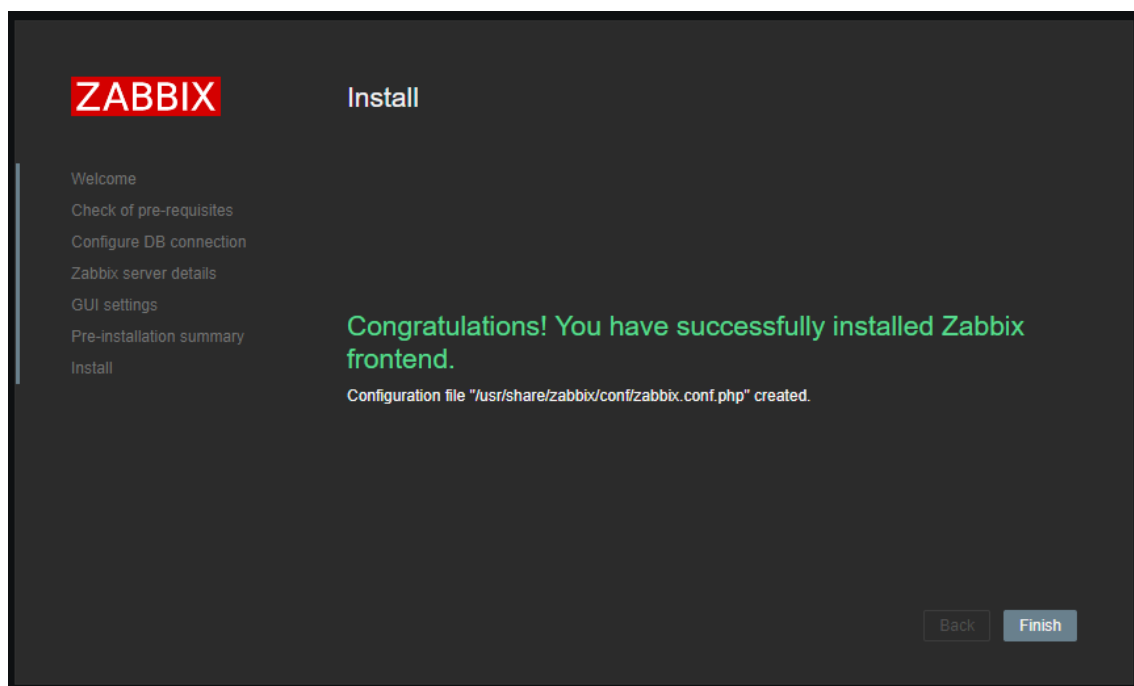


Figura 31 – Finalização da Instalação do Zabbix



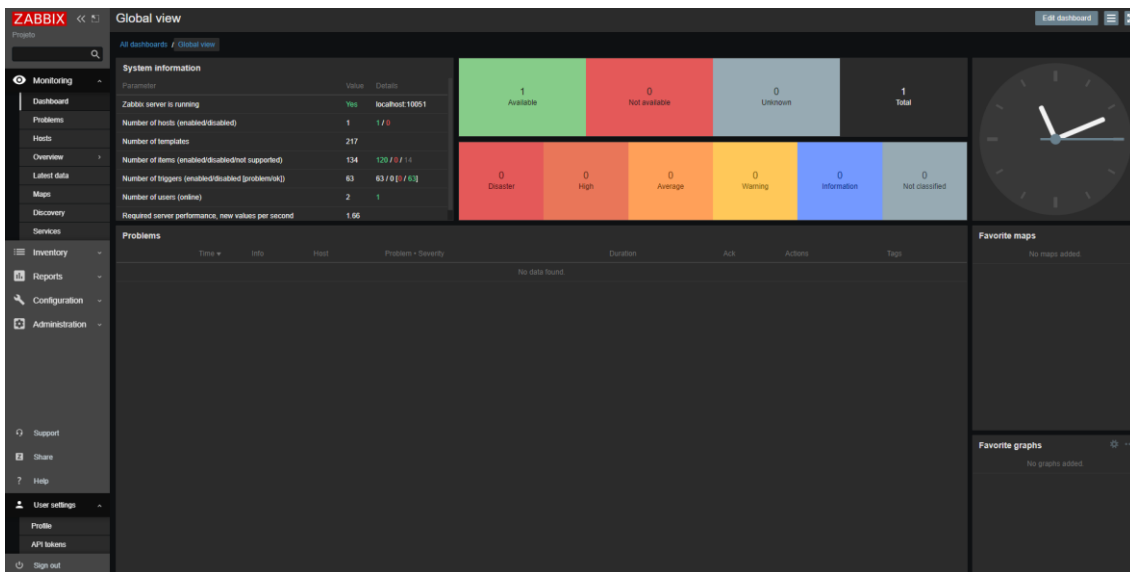


Figura 32 – Dashboard inicial do Zabbix

```
GNU nano 2.9.3 /etc/snmp/snmpd.conf Modified
#rocommunity public localhost
# Default access to basic system info
rocommunity public default -V gear
# rocommunity6 is for IPv6
rocommunity6 public default -V systemonly

# Full access from an example network
# Adjust this network address to match your local
# settings, change the community string,
# and check the 'agentAddress' setting above
#rocommunity secret 10.0.0.0/16

# Full read-only access for SNMPv3
rouser authOnlyUser

# Full write access for encrypted requests
# Remember to activate the 'createUser' lines $
#rwuser authPrivUser priv

# It's no longer typically necessary to use the full 'com2sec/group/access' configuration
# r[ow]user and r[ow]community, together with suitable views, should cover most requirements

#####
#
# SYSTEM INFORMATION
#

# Note that setting these values here, results in the corresponding MIB objects being 'read-only'
# See snmpd.conf(5) for more details
sysLocation Sitting on the Dock of the Bay
sysContact gear <gear@ipbeja.pt>
```

Figura 33 – Alteração da config dentro da diretoria SNMPD.conf

Na aba da configuração na parte dos hosts podemos criar hosts e configurar os mesmos, meter o Hostname, escolher o IP que queremos entre outras configurações.

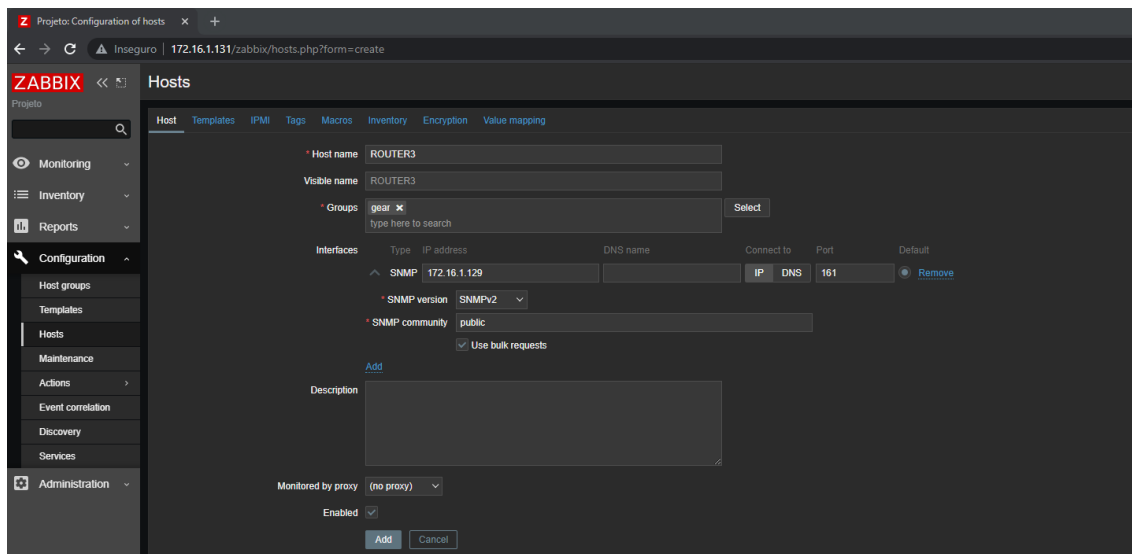


Figura 34 – Criação de hosts no Zabbix

Na parte do Template quando estamos a criar um host temos de ter em atenção qual a categoria em que o dispositivo criado se insere, neste caso como é um Router temos de escolher a opção mostrada na imagem, que é ideal para dispositivos de rede.

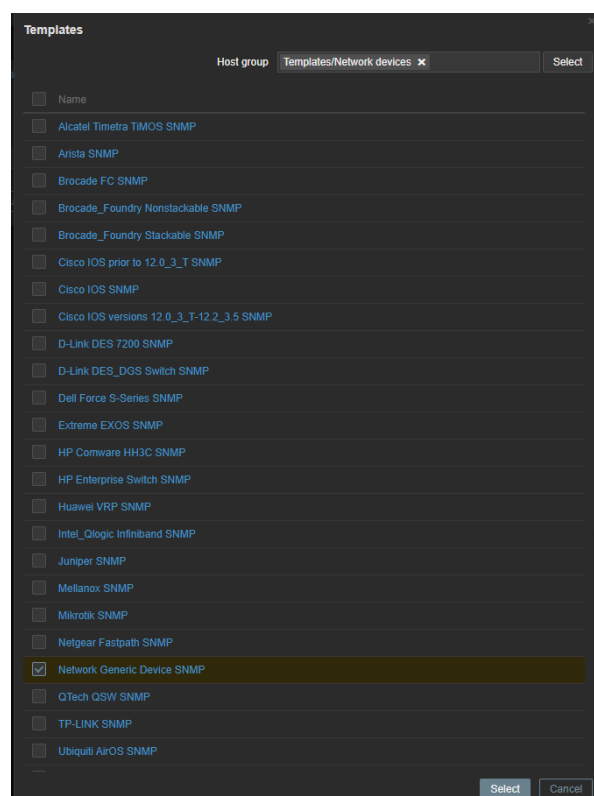


Figura 35 – Escolha de Template

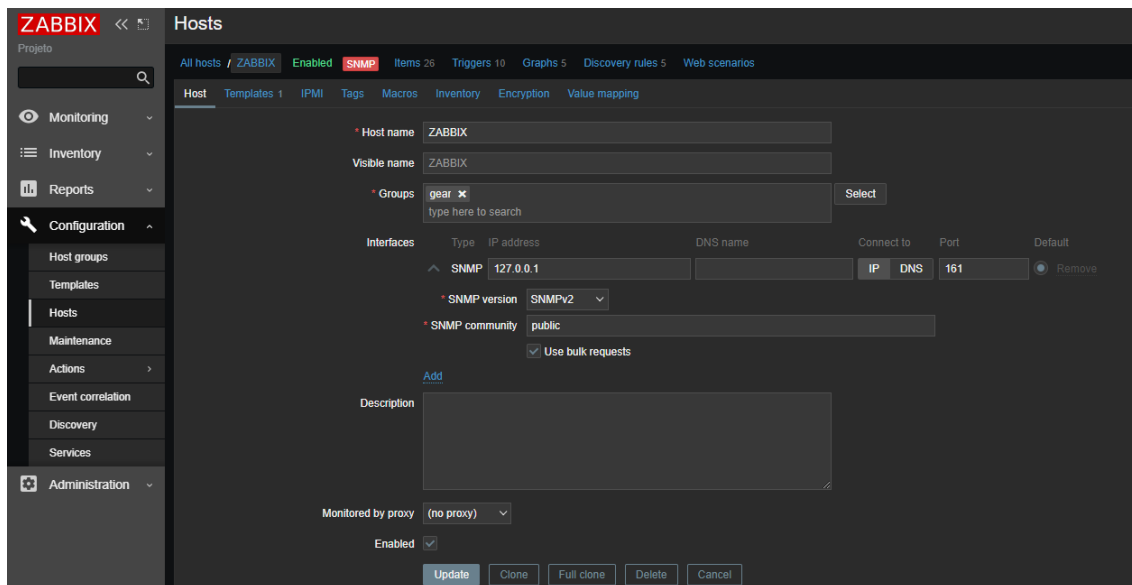


Figura 36 – Criação do host Zabbix

Neste host temos de escolher a opção Linux SNMP pois estamos a usar um PC com o Sistema Operativo Linux (Ubuntu)

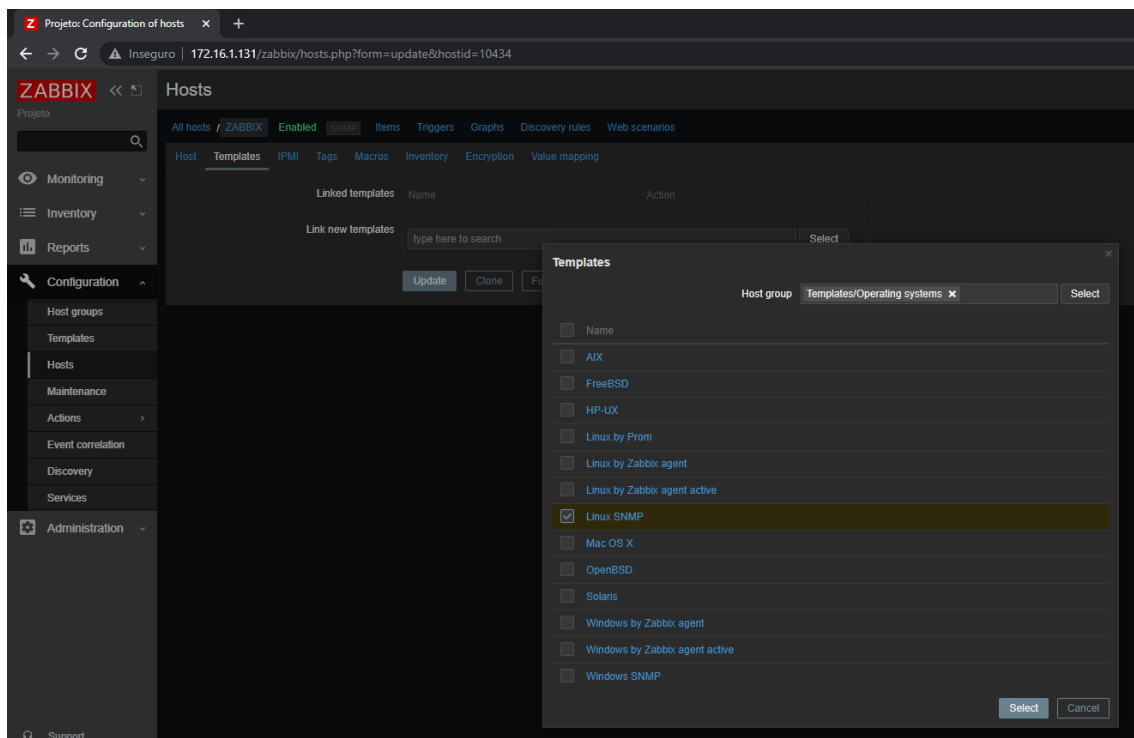


Figura 37 – Escolha do Template para o PC de Monitorização

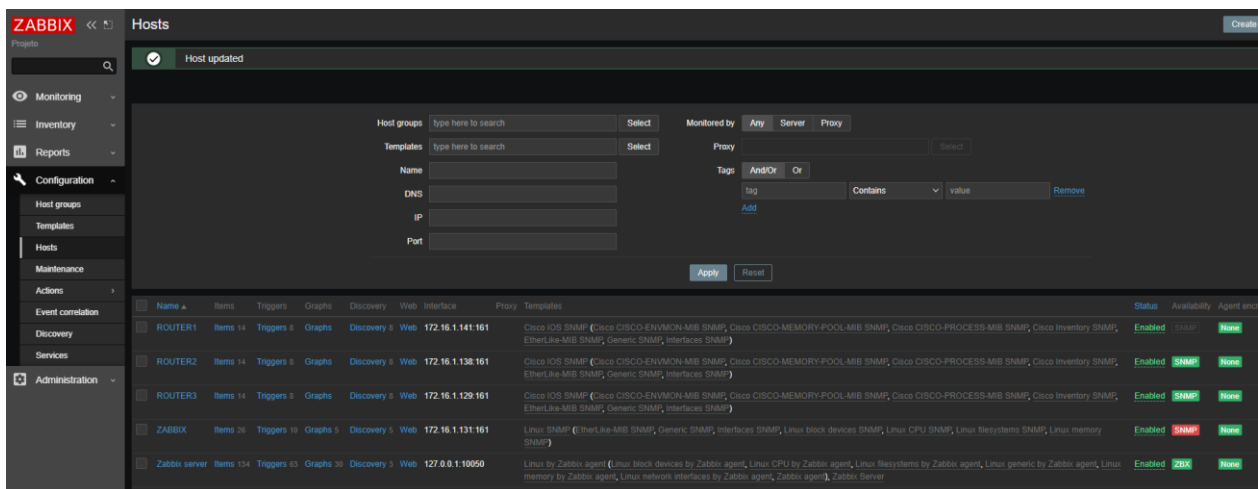


Figura 38 – Criação de todos os Routers e Servidores

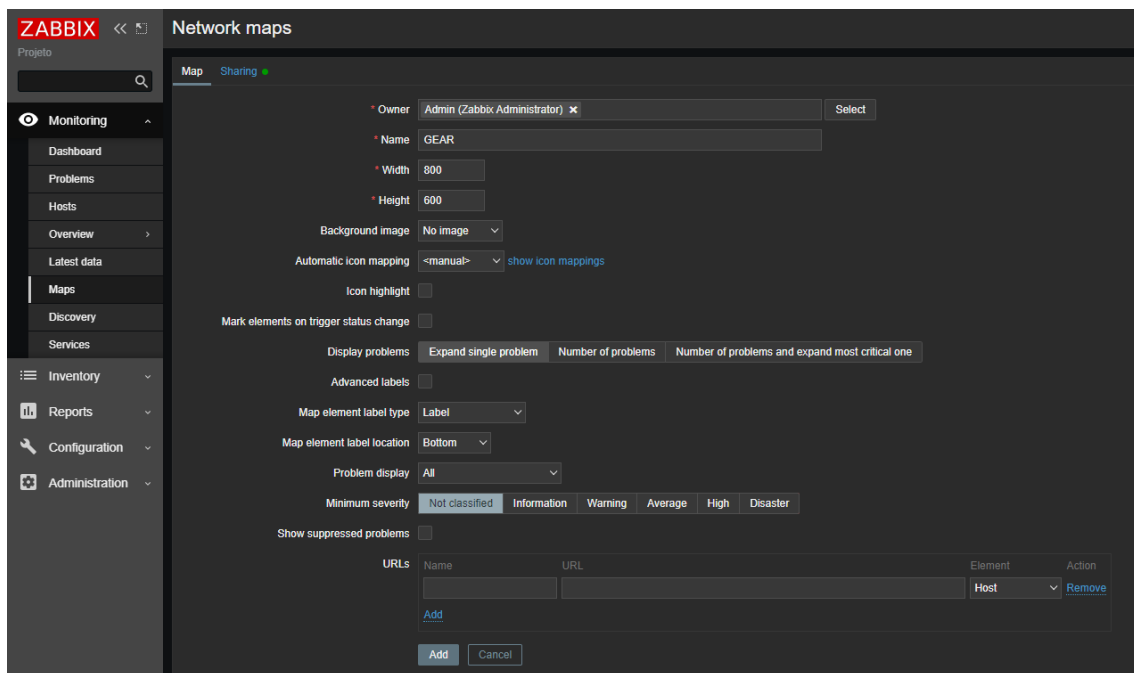


Figura 39 – Criação do mapa da rede

Nesta imagem podemos ver como é possível aplicar comandos que nos permitem ver vários parâmetros de cada dispositivo, neste caso o Router 3

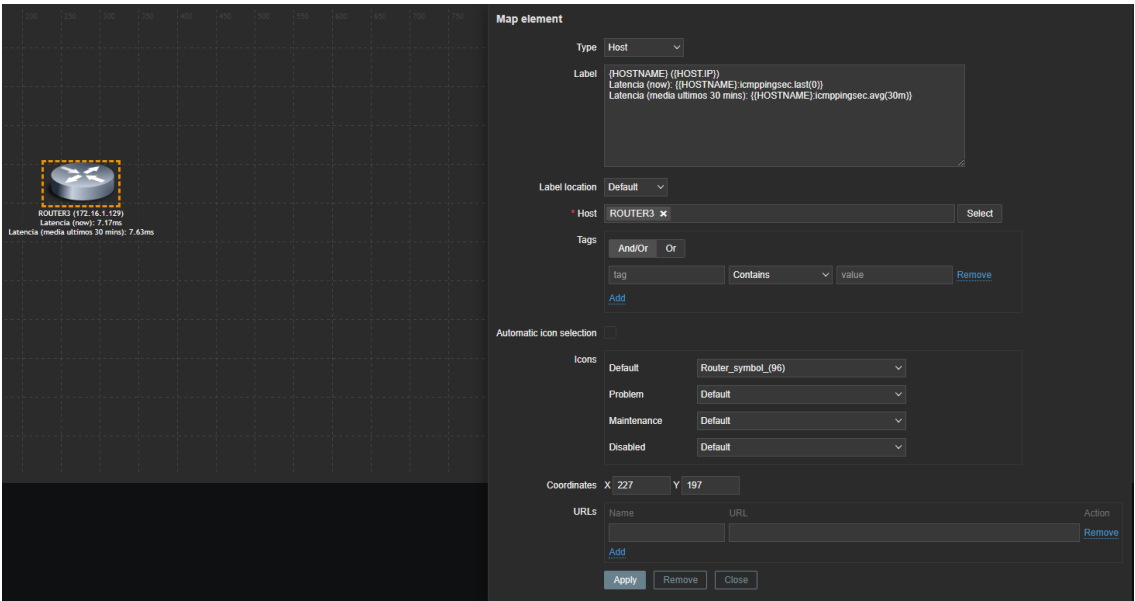


Figura 40 – Router 3 inserido no Mapa

Nesta imagem já temos mais equipamentos adicionados ao mapa e estamos a possibilitar ver a quantidade de dados que estão a entrar e a sair de cada dispositivo assim como a velocidade em Mbps da ligação entre esses mesmos dispositivos.

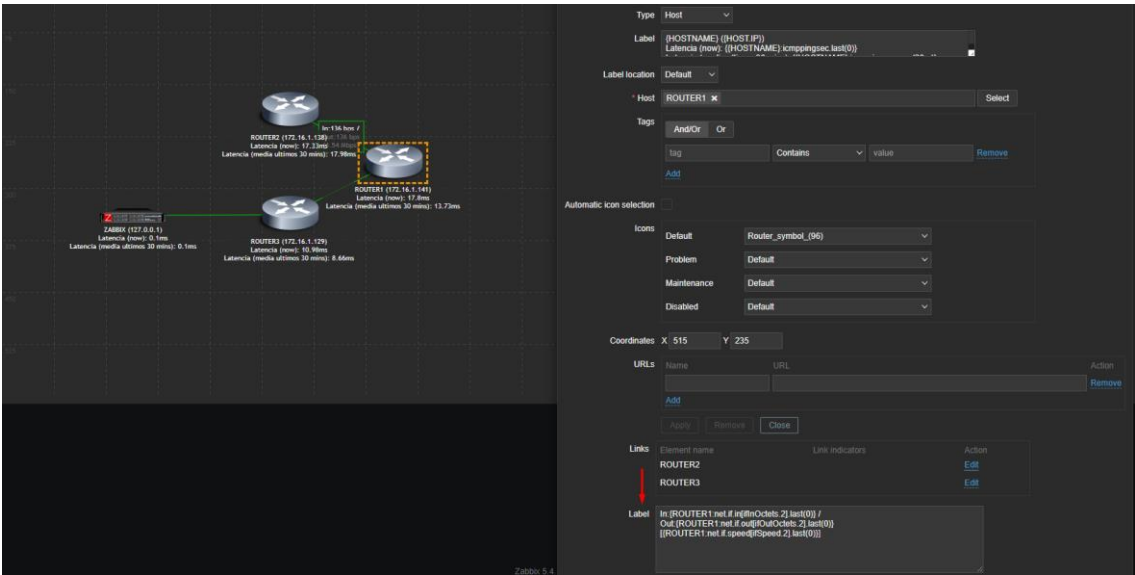


Figura 41 – Routers e Servidor Zabbix inseridos no mapa

```

gear@gear:~$ sudo apt install snmp snmpd
[sudo] password for gear:
Reading package lists... Done
Building dependency tree
Reading state information... Done
The following additional packages will be installed:
  libgdbm-compat4 libperl5.26 libsensors4 libsnmp-base libsnmp30 perl perl-modules-5.26
Suggested packages:
  lm-sensors snmp-mibs-downloader perl-doc libterm-readline-gnu-perl | libterm-readline-perl-perl
  make snmptrapd
The following NEW packages will be installed:
  libgdbm-compat4 libperl5.26 libsensors4 libsnmp-base libsnmp30 perl perl-modules-5.26 snmp snmpd
0 upgraded, 9 newly installed, 0 to remove and 0 not upgraded.
Need to get 7,897 kB of archives.
After this operation, 46.5 MB of additional disk space will be used.
Do you want to continue? [Y/h] y_
gear@gear:~$ sudo snmpwalk -v2c -c public 172.16.1.129_
iso.3.6.1.2.1.88.1.1.4.0 = Gauge32: 0
iso.3.6.1.2.1.88.1.1.5.0 = Counter32: 0
iso.3.6.1.2.1.88.1.2.1.0 = Counter32: 0
iso.3.6.1.2.1.88.1.4.1.0 = Counter32: 0
iso.3.6.1.2.1.92.1.1.1.0 = Gauge32: 500
iso.3.6.1.2.1.92.1.1.2.0 = Gauge32: 15
iso.3.6.1.2.1.92.1.2.1.0 = Counter32: 0
iso.3.6.1.2.1.92.1.2.2.0 = Counter32: 0
gear@gear:~$ _

```

Figura 42 – Instalação do snmp e snmpd no servidor tftp

**Hosts**

All hosts / Servidor TFTP Enabled Items Triggers Graphs Discovery rules Web scenarios

Host Templates IPMI Tags Macros Inventory Encryption Value mapping

\* Host name

Visible name

\* Groups    
type here to search

Interfaces	Type	IP address	DNS name	Connect to	Port	Default
SNMP		172.16.1.130		IP DNS	161	<input checked="" type="radio"/> Remove

\* SNMP version

\* SNMP community

☒ Use bulk requests

[Add](#)

Description

Monitored by proxy

Enabled ☒

Figura 43 – Criação do Host Server TFTP

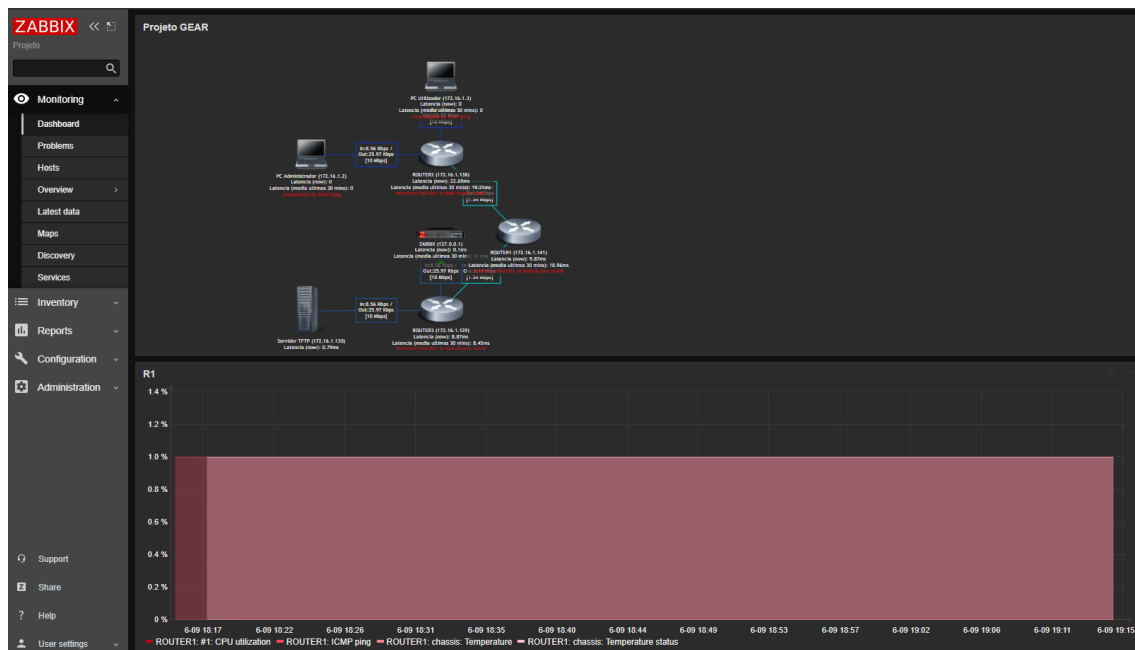


Figura 44 – Dashboard do Zabbix

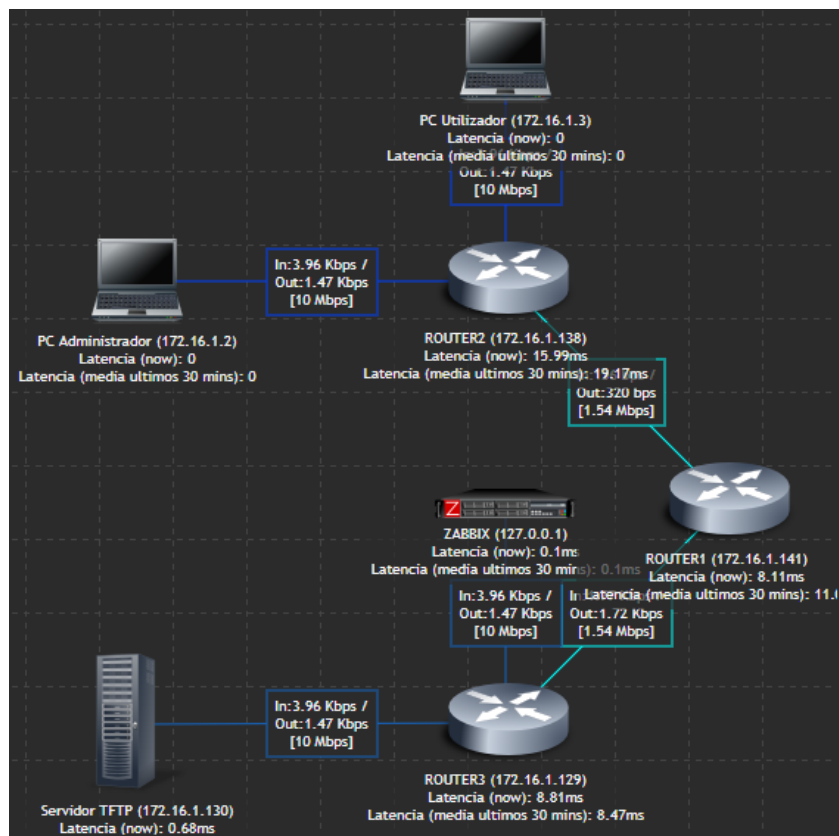


Figura 45 – Todos os equipamentos de rede inseridos no mapa do Zabbix

## Configuração dos Hosts Administrador e Utilizador

Nesta Etapa criámos 2 Virtual Machines sem configurações que serviram como PC Administrador e PC Utilizador a fim de mostrar algumas das restrições/permissões que é possível aplicar em cada um, estas regras vão ser aplicadas através da criação de ACLs no Router 2, estas ACLs vão permitir ao PC Administrador ter comunicação com qualquer equipamento da rede, visto que este é considerado o gestor da rede logo tem de ter acesso total a todos os equipamentos, e por fim temos o PC Utilizador que consegue comunicar com a rede toda menos com a sub-rede interna do Router 3.

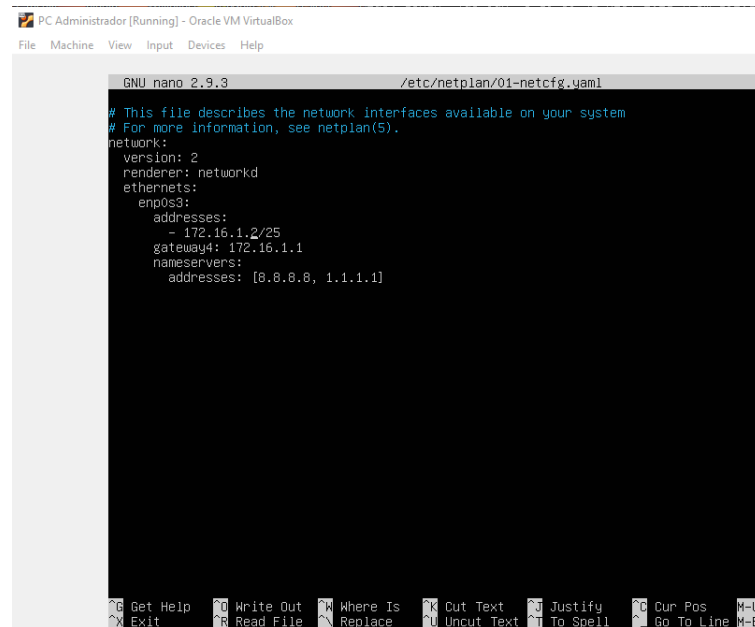
Na sub-rede interna do Router 2, faz-se a atribuição de endereços através do DHCP, pois é a parte da rede que se destina aos utilizadores “normais”.

```
R2#conf
Configuring from terminal, memory, or network [terminal]?
Enter configuration commands, one per line.  End with CNTL/Z.
R2(config)#ip dhcp pool rede2
R2(dhcp-config)#ne
R2(dhcp-config)#network 172.16.1.0 255.255.255.128
R2(dhcp-config)#default-router 172.16.1.1
R2(dhcp-config)#exit
R2(config)#ip dhc
R2(config)#ip dhcp excluded-address 172.16.1.1
R2(config)#
R2(config)#ip dhcp pool rede2
R2(dhcp-config)#dns-server 192.168.137.18
R2(dhcp-config)#exit
R2(config)#ip domain lookup
```

Figura 46 – Configurar o DHCP no Router 2 permitindo aos PCs dos utilizadores ter ip atribuído por DHCP



Nestas 2 imagens abaixo estamos a configurar o PC Administrador e o PC Utilizador com endereços estáticos, esta configuração é aplicada na diretoria /etc/netplan/01-netcfg.yaml



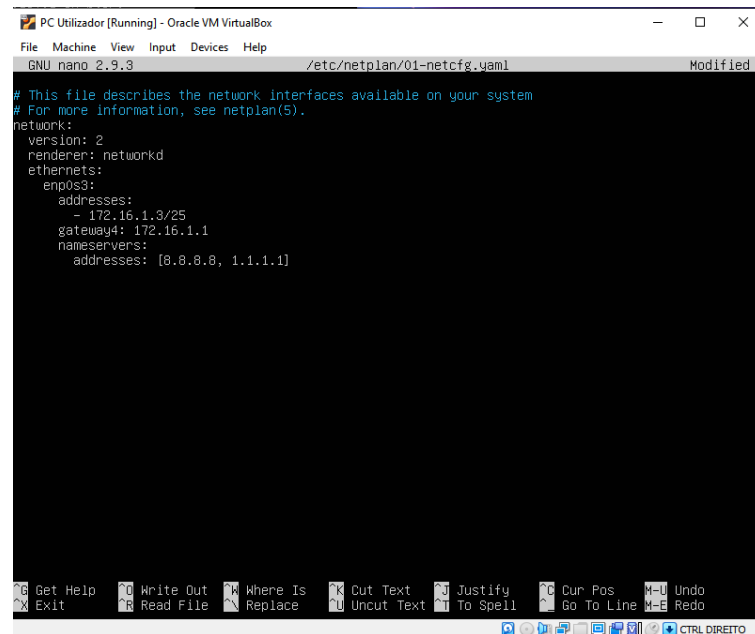
The screenshot shows a terminal window titled "PC Administrador [Running] - Oracle VM VirtualBox". The terminal is running the nano text editor, editing the file /etc/netplan/01-netcfg.yaml. The content of the file is as follows:

```
GNU nano 2.9.3 /etc/netplan/01-netcfg.yaml

# This file describes the network interfaces available on your system
# For more information, see netplan(5).
network:
  version: 2
  renderer: networkd
  ethernets:
    enp0s3:
      addresses:
        - 172.16.1.2/25
      gateway4: 172.16.1.1
      nameservers:
        addresses: [8.8.8.8, 1.1.1.1]
```

The terminal window has a menu bar with options: File, Machine, View, Input, Devices, Help. At the bottom, there is a toolbar with icons for various editing actions like Get Help, Write Out, Where Is, Cut Text, Justify, Cur Pos, Exit, Read File, Replace, Uncut Text, To Spell, Go To Line, and M-U.

Figura 47 – Configuração do netplan do PC Administrador



The screenshot shows a terminal window titled "PC Utilizador [Running] - Oracle VM VirtualBox". The terminal is running the nano text editor, editing the file /etc/netplan/01-netcfg.yaml. The content of the file is as follows:

```
GNU nano 2.9.3 /etc/netplan/01-netcfg.yaml Modified

# This file describes the network interfaces available on your system
# For more information, see netplan(5).
network:
  version: 2
  renderer: networkd
  ethernets:
    enp0s3:
      addresses:
        - 172.16.1.3/25
      gateway4: 172.16.1.1
      nameservers:
        addresses: [8.8.8.8, 1.1.1.1]
```

The terminal window has a menu bar with options: File, Machine, View, Input, Devices, Help. At the bottom, there is a toolbar with icons for various editing actions like Get Help, Write Out, Where Is, Cut Text, Justify, Cur Pos, Exit, Read File, Replace, Uncut Text, To Spell, Go To Line, M-U, Undo, M-E, and Redo. Additionally, there is a status bar at the very bottom showing "CTRL DIREITO".

Figura 48 – Configuração do netplan do PC Utilizador

```
GNU nano 2.9.3 /etc/netplan/01-netcfg.yaml

# This file describes the network interfaces available on your system
# For more information, see netplan(5).
network:
  version: 2
  renderer: networkd
  ethernets:
    enp0s3:
      dhcp4: yes
      nameservers:
        addresses: [8.8.8.8, 1.1.1.1]

gear@gear:~$ ping google.com
PING google.com (216.58.215.174) 56(84) bytes of data:
64 bytes from mad41s07-in-f14.1e100.net (216.58.215.174): icmp_seq=1 ttl=56 time=30.3 ms
64 bytes from mad41s07-in-f14.1e100.net (216.58.215.174): icmp_seq=2 ttl=56 time=38.9 ms
^Z
[5]+  Stopped                  ping google.com
gear@gear:~$ _
gear@gear:~$ sudo apt install snmp snmpd
gear@gear:~$ sudo snmpwalk -v2c -c public 172.16.1.1
```

Figura 49 – Ping ao google.com através do Servidor TFTP

Nesta imagem, estamos a excluir os endereços IP que atribuímos anteriormente aos PCs Administrador (172.16.1.2) e Utilizador (172.16.1.3), para que a DHCP pool não atribua esses endereços aos utilizadores comuns quando estes se conectaram á sub-rede interna do Router 2.

```
et0/1, changed state to down
*Mar  1 00:00:04.275: %LINEPROTO-5-UPDOWN: Line protocol on Interface Serial0/0,
changed state to up
R2#conf
Configuring from terminal, memory, or network [terminal]?
Enter configuration commands, one per line.  End with CNTL/Z.
R2(config)#ip dhcp pool rede2
R2(dhcp-config)#172.16.1.0 255.255.255.128
^
% Invalid input detected at '^' marker.

R2(dhcp-config)#no
R2(dhcp-config)#network 172.16.1.0 255.255.255.128
R2(dhcp-config)#default-router 172.16.1.1
R2(dhcp-config)#exit
R2(config)#ip dhcp
R2(config)#ip dhcp excluded-address 172.16.1.1
R2(config)#dh
R2(config)#dhcp pool rede2
^
% Invalid input detected at '^' marker.

R2(config)#ip dhcp pool rede2
R2(dhcp-config)#dns-server 192.168.137.18
R2(dhcp-config)#exit
R2(config)#ip domain lookup
R2(config)#[T
R2#E]M
R2#XTERM
*Mar  1 02:06:49.047: %SYS-5-CONFIG_I: Configured from console by console
R2#conf
Configuring from terminal, memory, or network [terminal]?
Enter configuration commands, one per line.  End with CNTL/Z.
R2(config)#ip dh
R2(config)#ip dhcp ex
R2(config)#ip dhcp excluded-address 172.16.1.2
R2(config)#ip dhcp excluded-address 172.16.1.3
R2(config)#
```

Figura 50 – Exclusão dos IPs dos PCs Administrador e Utilizador da pool DHCP

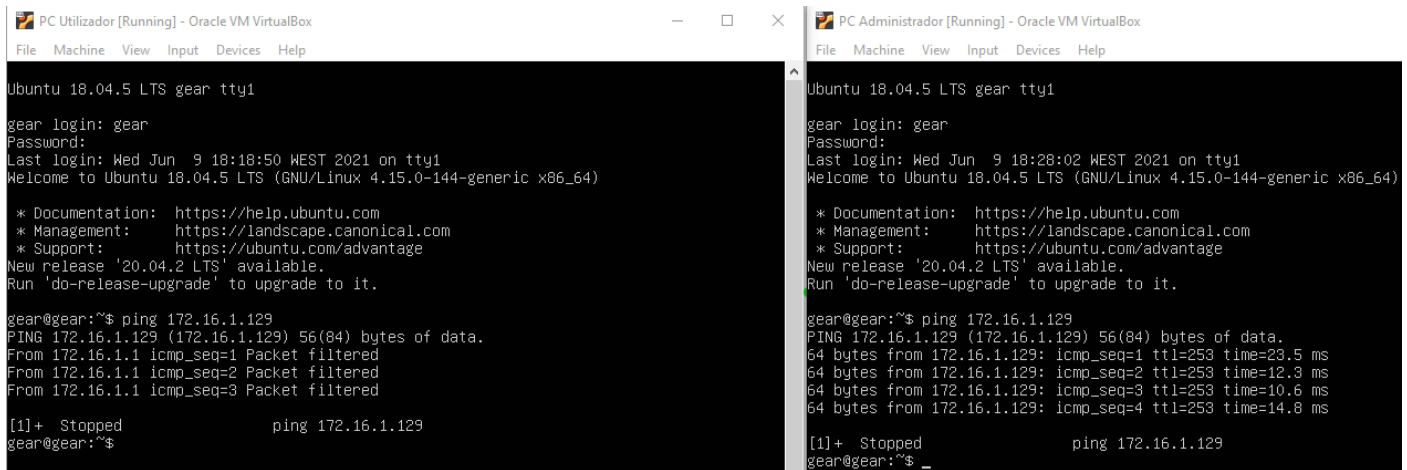
Nesta imagem abaixo podemos ver a criação das regras com ACLs estendidas, o uso das mesmas não foi deliberado, são usadas ACLs estendidas pois são mais flexíveis e permitem um vasto leque de configurações ao contrário das ACLs Padrão.

O nome dado á ACL foi UTILIZADORES, pois esta vai restringir a comunicação entre os utilizadores comuns e a rede interna do Router 3, no código abaixo permitimos que os 2 primeiros endereços possam comunicar com a sub-rede interna do Router 3, o endereço 172.16.1.1 representa a interface F0/0 do Router 2 e o 172.16.1.2 representa o PC Administrador, depois no código abaixo negámos a comunicação de todos os outros endereços, e mais abaixo permitimos todos os outros endereços de acederem a todos os endereços, por fim aplicamos a ACL á interface F0/0 do Router 2 no sentido in e mais abaixo com o show access-lists podemos visualizar as regras que acabámos de criar.

```
R2#conf
R2(config)#ip access-list extended UTILIZADORES
R2(config-ext-nacl)#permit ip 172.16.1.1 0.0.0.0 172.16.1.128 0.0.0.7
R2(config-ext-nacl)#permit ip 172.16.1.2 0.0.0.0 172.16.1.128 0.0.0.7
R2(config-ext-nacl)#deny ip 172.16.1.0 0.0.0.127 172.16.1.128 0.0.0.7
R2(config-ext-nacl)#permit ip any any
R2(config-ext-nacl)#exit
R2(config)#int f0/0
R2(config-if)#ip access-group UTILIZADORES in
R2(config-if)#exit
R2(config)#exit
R2#show
*Mar  1 03:38:45.055: %SYS-5-CONFIG_I: Configured from console by console
R2#show access-lists
Extended IP access list UTILIZADORES
 10 permit ip host 172.16.1.1 172.16.1.128 0.0.0.7
 20 permit ip host 172.16.1.2 172.16.1.128 0.0.0.7
 30 deny ip 172.16.1.0 0.0.0.127 172.16.1.128 0.0.0.7
 40 permit ip any any
R2#
```

Figura 51 – Criação da ACL UTILIZADORES no Router 2

Após aplicarmos a ACL verificou-se se a mesma estava a funcionar corretamente, para testar tivemos de ligar o PC Utilizador e PC Administrador e pingar a interface F0/0 do Router 3. Como se pode ver na imagem abaixo o PC Utilizador (parte esquerda da imagem) não consegue ter sucesso quando faz ping ao 172.16.1.129 (Router 2 – F0/0) pois a comunicação é filtrada, já no caso do PC Administrador (parte direita da imagem) essa filtragem não acontece, pois, o PC Administrador tem permissão total de comunicar com a toda a sub-rede interna pertencente ao Router 3.



```
PC Utilizador [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help

Ubuntu 18.04.5 LTS gear tty1
gear login: gear
Password:
Last login: Wed Jun  9 18:18:50 WEST 2021 on tty1
Welcome to Ubuntu 18.04.5 LTS (GNU/Linux 4.15.0-144-generic x86_64)

 * Documentation:  https://help.ubuntu.com
 * Management:    https://landscape.canonical.com
 * Support:       https://ubuntu.com/advantage
New release '20.04.2 LTS' available.
Run 'do-release-upgrade' to upgrade to it.

gear@gear:~$ ping 172.16.1.129
PING 172.16.1.129 (172.16.1.129) 56(84) bytes of data.
From 172.16.1.1 icmp_seq=1 Packet filtered
From 172.16.1.1 icmp_seq=2 Packet filtered
From 172.16.1.1 icmp_seq=3 Packet filtered

[1]+  Stopped                  ping 172.16.1.129
gear@gear:~$

PC Administrador [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help

Ubuntu 18.04.5 LTS gear tty1
gear login: gear
Password:
Last login: Wed Jun  9 18:28:02 WEST 2021 on tty1
Welcome to Ubuntu 18.04.5 LTS (GNU/Linux 4.15.0-144-generic x86_64)

 * Documentation:  https://help.ubuntu.com
 * Management:    https://landscape.canonical.com
 * Support:       https://ubuntu.com/advantage
New release '20.04.2 LTS' available.
Run 'do-release-upgrade' to upgrade to it.

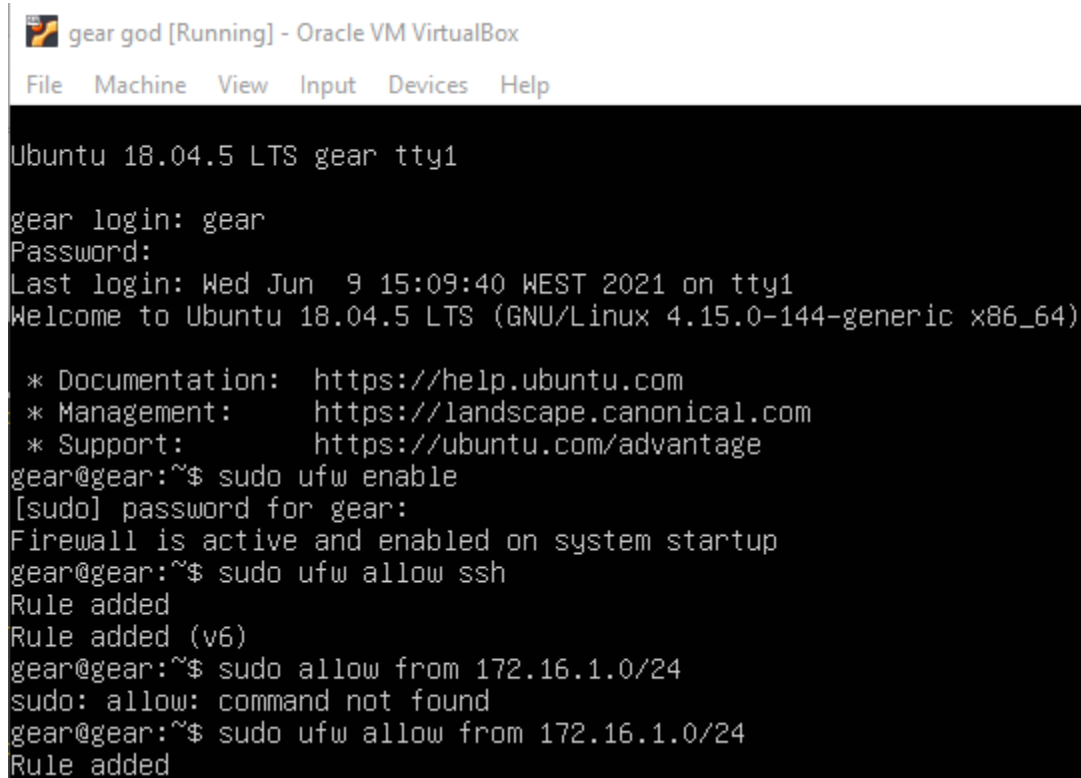
gear@gear:~$ ping 172.16.1.129
PING 172.16.1.129 (172.16.1.129) 56(84) bytes of data.
64 bytes from 172.16.1.129: icmp_seq=1 ttl=253 time=23.5 ms
64 bytes from 172.16.1.129: icmp_seq=2 ttl=253 time=12.3 ms
64 bytes from 172.16.1.129: icmp_seq=3 ttl=253 time=10.6 ms
64 bytes from 172.16.1.129: icmp_seq=4 ttl=253 time=14.8 ms

[1]+  Stopped                  ping 172.16.1.129
gear@gear:~$
```

Figura 52 – Ping 172.16.1.129 (PC Administrador e Utilizador)

## Ativar a UFW (Uncomplicated Firewall)

Com o objetivo de proteger o Servidor TFTP ativou-se a UFW (Uncomplicated Firewall), depois a mesma teve de ser configurada para permitir SSH e permitir apenas comunicação com a rede 172.16.1.0/24 (toda a rede do projeto).



```
gear god [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help

Ubuntu 18.04.5 LTS gear tty1

gear login: gear
Password:
Last login: Wed Jun  9 15:09:40 WEST 2021 on tty1
Welcome to Ubuntu 18.04.5 LTS (GNU/Linux 4.15.0-144-generic x86_64)

 * Documentation:  https://help.ubuntu.com
 * Management:    https://landscape.canonical.com
 * Support:       https://ubuntu.com/advantage
gear@gear:~$ sudo ufw enable
[sudo] password for gear:
Firewall is active and enabled on system startup
gear@gear:~$ sudo ufw allow ssh
Rule added
Rule added (v6)
gear@gear:~$ sudo allow from 172.16.1.0/24
sudo: allow: command not found
gear@gear:~$ sudo ufw allow from 172.16.1.0/24
Rule added
```

Figura 53 – UFW

## Guardar todas as configurações aplicadas aos Routers e Importar e Exportar essas mesmas configurações

```
R2#copy
R2#copy ru
R2#copy running-config st
R2#copy running-config startup-config
Destination filename [startup-config]?
Building configuration...
[OK]
R2#
```

Figura 54 – Guardar todas as configs na memória do Router 2 (fez-se o mesmo para todos os Routers)

Depois de guardarmos as configurações que aplicamos nos Routers tivemos de exportar as mesmas para o Servidor TFTP executando o código copy running-config tftp://172.16.1.130/MZ72I-incomming/R3-backup, este código foi aplicado em todos os Routers fazendo as devidas alterações.

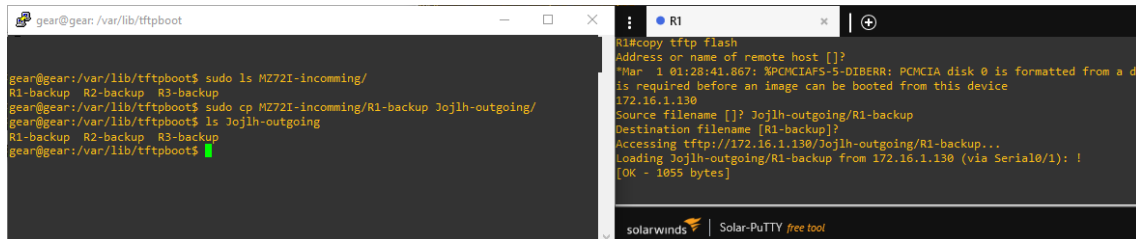
```
R3 R1 R2
% There may not be enough space available to collect the complete crashinfo
% It would be advisable to have 280755 bytes free space on flash:crashinfo

Press RETURN to get started!

*Mar 1 00:00:02.439: %LINEPROTO-5-UPDOWN: Line protocol on Interface VoIP-Null0
, changed state to up
*Mar 1 00:00:02.715: %SYS-5-CONFIG_I: Configured from memory by console
*Mar 1 00:00:02.823: %SYS-5-RESTART: System restarted --
Cisco IOS Software, 2600 Software (C2691-ENTSERVICESK9-M), Version 12.4(13b), RE
LEASE SOFTWARE (fc3)
Technical Support: http://www.cisco.com/techsupport
Copyright (c) 1986-2007 by Cisco Systems, Inc.
Compiled Tue 24-Apr-07 15:33 by prod_rel_team
*Mar 1 00:00:02.823: %SNMP-5-COLDSTART: SNMP agent on host R3 is undergoing a c
old start
*Mar 1 00:00:02.835: %PCMCIAFS-5-DIBERR: PCMCIA disk 0 is formatted from a diff
erent router or PC. A format in this router is required before an image can be b
ooted from this device
*Mar 1 00:00:03.295: %LINK-3-UPDOWN: Interface FastEthernet0/0, changed state t
o up
*Mar 1 00:00:03.347: %LINK-5-CHANGED: Interface FastEthernet0/1, changed state
to administratively down
*Mar 1 00:00:03.375: %LINK-3-UPDOWN: Interface Serial0/0, changed state to up
*Mar 1 00:00:04.295: %LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthern
et0/0, changed state to up
*Mar 1 00:00:04.347: %LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthern
et0/1, changed state to down
*Mar 1 00:00:04.375: %LINEPROTO-5-UPDOWN: Line protocol on Interface Serial0/0,
changed state to up
R3#copy running-config tftp://172.16.1.130/MZ72I-incomming/R3-backup
Address or name of remote host [172.16.1.130]?
Destination filename [MZ72I-incomming/R3-backup]?
!!
934 bytes copied in 0.980 secs (953 bytes/sec)
R3#
```

Figura 55 – Códigos que temos de executar para exportar a config do Router 3 para o Server TFTP

Nesta imagem (no lado esquerdo) podemos ver que as configurações de todos os Routers já se encontram guardadas dentro do Servidor TFTP e no lado direito da imagem podemos ver como fazemos para ir buscar a config do router que queremos, podemos ver que a única alteração é na palavra “outgoing” pois esta significa que estamos a ir buscar configurações que se encontram num local externo, no nosso caso o Servidor TFTP.



The image shows two terminal windows. The left window, titled 'gear@gear: /var/lib/tftpboot', shows the following commands and output:

```
gear@gear:/var/lib/tftpboot$ sudo ls MZ72I-incoming/
R1-backup R2-backup R3-backup
gear@gear:/var/lib/tftpboot$ sudo cp MZ72I-incoming/R1-backup Jojlh-outgoing/
gear@gear:/var/lib/tftpboot$ ls Jojlh-outgoing
R1-backup R2-backup R3-backup
gear@gear:/var/lib/tftpboot$
```

The right window, titled 'R1', shows the output of the 'copy tftp flash' command on a router:

```
R1#copy tftp flash
Address or name of remote host []?
*Mar  1 01:28:41.867: %PCMCIAFS-5-DIBERR: PCMCIA disk 0 is formatted from a di
is required before an image can be booted from this device
172.16.1.130
Source filename []? Jojlh-outgoing/R1-backup
Destination filename [R1-backup]?
Accessing tftp://172.16.1.130/Jojlh-outgoing/R1-backup...
Loading Jojlh-outgoing/R1-backup from 172.16.1.130 (via Serial0/1): !
[OK - 1055 bytes]
```

Figura 56 – Config de todos os Routers guarda no Servidor TFTP

## Instalação / Upgrade IOS

Esta etapa não foi feita durante o projeto pois não funciona no GNS3 mas é importante saber que a mesma existe e quais os comandos que devemos executar.

1. Temos de copiar a imagem do IOS para o servidor TFTP
2. executar no router:
  - I. copy tftp: flash:  
inserir dados do servidor tftp e nome do ficheiro
  - II. write memory
  - III. reload
  - IV. show version  
(depois de o router reiniciar  
para verificar se instalou a nova versão)

Esta configuração é bastante simples e apenas temos de seguir estes passos, na imagem abaixo está demonstrado os comandos acima dados, como já foi dito anteriormente esta função não é suportada pelo GNS3, mas se executada num Router que a suporte daria um resultado semelhante á imagem abaixo.

```
R1#copy IOS:tftp://172.16.1.130/MZ72I-incomming/IOS-backup
Address or name of remote host [172.16.1.130]?
Destination filename [MZ72I-incomming/IOS-backup]?
!!
934 bytes copied in 0.980 secs (953 bytes/sec)
R1#copy tftp: flash:
Address or name of remote host []?
*Mar 1 00:03:23.471: %PCMCIAFS-5-DIBERR: PCMCIA disk 0 is formatted from a different router or PC. A format in this router
is required before an image can be booted from this device
172.16.1.130
Source filename []? Jojlh-outgoing/IOS-backup...
Destination filename [R1-backup]?
Accessing tftp://172.16.1.130/Jojlh-outgoing/IOS-backup .
Loading Jojlh-outgoing,IOS-backup from 172.16.1.130 (via Serial0/1): !
[OK - 1055 bytes]
R1#write memory
R1#show version
```

Figura 57 – Exemplificação da Instalação/Upgrade IOS

## Recuperação de passwords em Routers e Switches Cisco

Esta etapa não foi feita no projeto, porém pode ser bastante útil numa situação real do dia a dia, como tal irá ser deixado o passo a passo abaixo, mostrando como se recupera as passwords em Routers e Switches Cisco.

### Routers – Passo a Passo

1. Reiniciar o router e interromper o procedimento de arranque premindo a tecla Break
2. Ativar o bit 6 do registo de configuração

Série 2600/2800:	Série 2500:
rommon 1> confreg 0x2142	>o/r 0x2142
3. Reiniciar o Router

Série 2600/2800:	Série 2500:
rommon 1> reset	>i
4. Entrar no modo privilegiado (que agora não necessita de password) e copiar o startup-config para o running-config



```
Router> enable
```

```
Router# copy startup-config running-config
```

5. Entrar no modo de configuração global e alterar (ou ver) a password

```
Router# configure terminal
```

```
Router(config)# enable secret "nova password"
```

6. Repor o registo de configuração no estado de leitura do startup-config

```
Router(config)# config.register 0x2102
```

7. Copiar o running-config para o startup-config

```
Router# copy running-config startup-config
```

8. Reiniciar o Router

```
Router# reload
```

## **Switches – Passo a Passo**

1. Ligue um computador à consola do switch e configure o hyper terminal no modo predefinido
2. Ligue o switch e simultaneamente pressione o botão Mode durante cerca de 5 segundos
3. O Switch deve apresentar a prompt "switch"
4. Seguidamente execute os seguintes comandos:

```
Switch: flash_init
```

```
Switch: load_helper
```

```
Switch: dir flash:
```

Agora deve-se renomear o ficheiro config.text para um nome que não exista na flash, por exemplo, "config13Jun21"

```
Switch: rename flash:config.text flash:config.13Jun21
```

Switch: boot

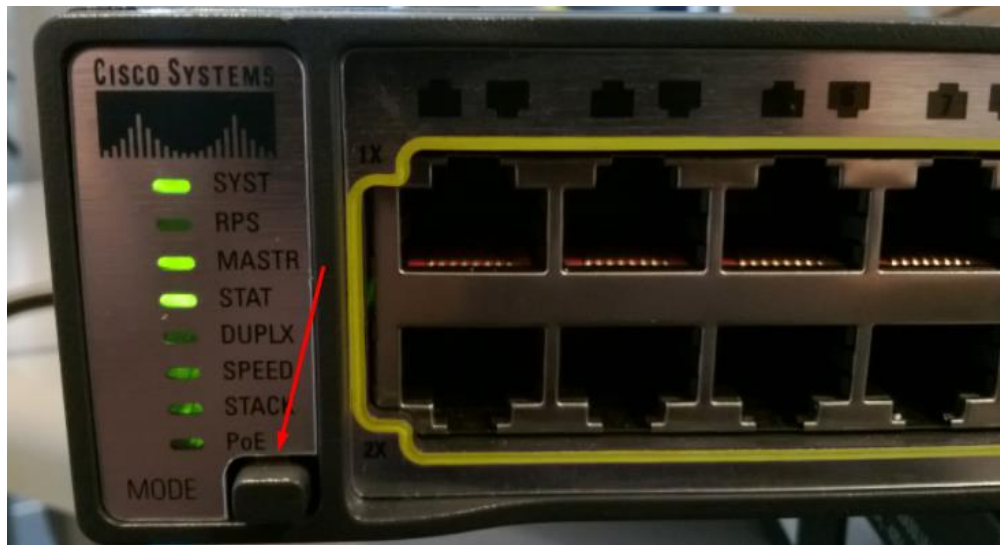


Figura 58 - Switch Boot

## **Conclusão**

Inicialmente tive alguma dificuldade em trabalhar com o GNS3, pois não conhecia o programa em si, os bugs/problemas que este apresentava e como tal não conseguia resolver os mesmos, foi algo que me deixou frustrado no início, mas depois com o uso/prática e com ajuda do Professor Pedro Moreira fui conseguindo perceber os erros que o mesmo apresentava e comecei a perceber como os resolver.

Com este projeto consegui aprender mais sobre como as redes funcionam, apesar de já ter alguma percepção devido às disciplinas onde utilizámos Packet Tracer. Como o projeto foi feito no Software GNS3 conseguiu se ter uma experiência de trabalho mais aproximada da vida real, pois ao contrário do Packet Tracer, o GNS3 tem mais funcionalidades e permite trabalhar de maneira mais aprofundada, ao contrário do Packet Tracer que não conseguimos exportar máquinas virtuais o GNS3 consegue o fazer, sendo possível que essas máquinas sejam usadas como um computador normal ou um Servidor, etc.

Neste projeto aprendi como criar servidores TFTP como configurar os mesmos, como guardar ficheiros de configuração de Routers dentro destes, aprendi como monitorizar e gerir a rede, aprendi a instalar e atualizar o Sistema Operativo IOS em Routers (apesar de não ser possível aplicar no GNS3), aprendi como recuperar uma password de um equipamento Cisco (apesar de não ser possível aplicar no GNS3).

Com todos estes pontos que acabei de referir quero deixar claro que este projeto foi bastante importante para desenvolver de maneira mais aprofundada o meu conhecimento, adquirir novas ferramentas de trabalho e desenvolver as minhas capacidades de resolução de problemas.