

Instituto Politécnico de Leiria

Escola Superior de Tecnologia e Gestão

Licenciatura em Engenharia Informática – Tecnologias de Informação (2º ano)

Unidade Curricular: Redes de Dados

Ano letivo 2019/2020

RELATÓRIO DO PROJETO

Grupo de trabalho:

- Gonçalo Vicente 2172131
- Paulo Custódio 2171151

Docentes:

- Joana Costa
- Carlos Rabadão

1. Introdução

O presente documento serve para dar a conhecer a implementação do nosso projeto, sendo este proposto pelos docentes da unidade curricular de Redes de Dados, e que consiste na implementação da rede de uma empresa com acesso à internet.

Iremos descrever toda a topologia e como ela está estruturada e endereçada. Para este projeto foi nos dado os seguintes pressupostos:

- Dispõe do endereço 192.100.1.0/24 para todas as necessidades de endereçamento.
- Deve utilizar o menor número de endereços possíveis.
- A empresa tem duas sucursais para além da sede, geograficamente distantes.
- Em cada uma das filiais, incluído a sede, há 3 redes locais: Vendas (20 PCs em cada filial), Recursos Humanos (10 PCs em cada filial) e Administração (5 PCs em cada filial), sendo que cada uma terá endereçamento próprio.
- Não haverá conectividade *layer 2* entre as 3 redes locais, sendo que podem partilhar o mesmo *switch*.
- Existirá um servidor de ficheiros, acessível a partir de qualquer um dos computadores da empresa. Existirá ainda um servidor público, para alojamento da página *web* da empresa.
- As configurações de toda a empresa devem ser obtidas por DHCP, com exceção do servidor.
- A ligação entre a empresa e o ISP será feita com recurso a PPPoE.
- Todos os endereços LAN da empresa devem ser traduzidos (NAT) para o endereço público, único, mas fixo, atribuído à interface WAN do router de ligação à Internet.
- Os administradores da empresa devem conseguir aceder remotamente de forma segura (através da sua ligação residencial) à sua rede local da empresa.

De forma a garantir estes pressupostos foi configurado o seguinte:

- Políticas de acesso
- *Vlans*
- Encaminhamento
- Servidor de *DHCP*
- Servidor *Web*
- Servidor *FTP*
- Translação de endereços
- Ligação *PPPoE*
- *VPN*

Para uma melhor integração do nosso projeto num ambiente real, definimos um nome fictício para a empresa e implementamos alguns extras.

2. Topologia e Endereçamento

Decidimos idealizar a empresa “PGNET”, este nome provém das iniciais dos seus fundadores (P=Paulo e G=Gonçalo) e “NET” de *network*, esta consiste na venda de equipamentos de rede, como por exemplo, *routers*, *switches*, *access-points*, *hub's*, cablagem, entre os demais produtos existentes nesta área.

A “PGNET” tem a sua sede em Leiria, e duas sucursais, uma em Santarém e outra em Portalegre.

A sede e cada uma das sucursais têm 3 redes locais distintas, cada uma com endereçamento próprio: Vendas (20 PC's em cada sucursal), RH (Recursos Humanos) (10 PC's em cada sucursal) e Administração (5 PC's em cada sucursal). De notar que apenas adicionamos 1 PC para cada uma destas redes locais, mas o endereçamento está feito de modo a ser possível ligar os restantes PC's.

Na sede, numa outra rede, é onde estão os servidores:

- *DHCP & DNS*
- *FTP*
- *HTTP*
- *MAIL*
- *SYSLOG & NTP.*

Na figura(fig.1), à esquerda representado com a cor laranja é a sede da nossa empresa, ao centro com a cor rosa é a sucursal Santarém e do lado direito com a cor azul a sucursal Portalegre. Representado pela cor verde, é a WAN da nossa empresa (ligações entre sede e sucursais). Em cima à esquerda está representado a casa de um administrador.

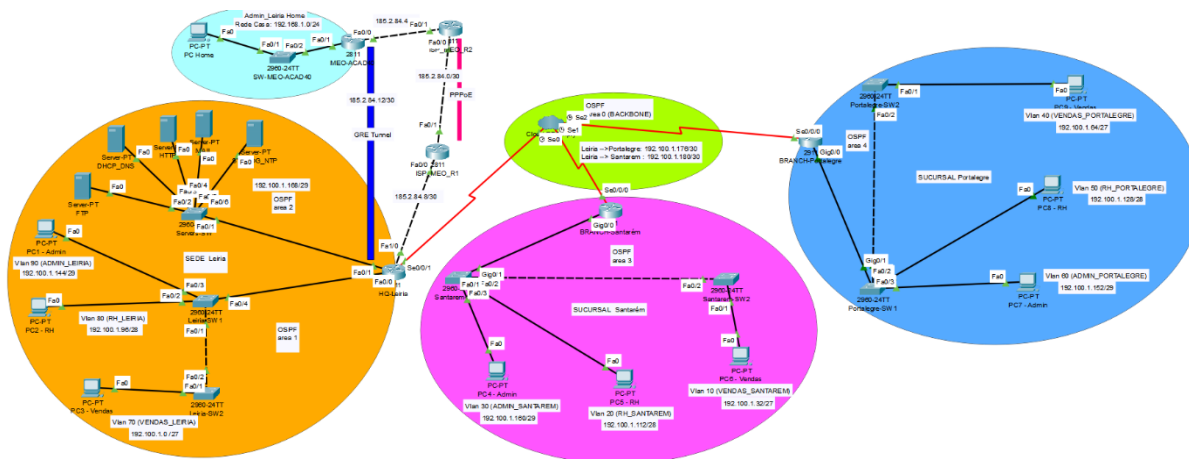


Figura 1 - Topologia da Rede

Podemos ver também representado, dois traços, azul e rosa, sendo respetivamente, *VPN* e *PPPoE*.

A topologia adotada para implementação do cenário da empresa “PGNET” no que toca às redes locais da sede (apenas PC's) e das sucursais é denominada como *Router-on-a-Stick*, onde temos uma interface de um router que serve várias sub-redes através de *sub-interfaces* (ex: fastEthernet 0/0.70).

Para a ligação entre a sede e as sucursais utilizou-se a tecnologia *WAN frame relay*, sendo o router “*HQ-Leiria*” situado na sede, que garante a comunicação entre sede e sucursais.

Para simular o acesso à internet, estão presentes dois routers no cenário que simulam o ISP, “*MEO-ISP-R1*” e “*MEO-ISP-R2*”, e o acesso à internet é garantido pelo router “*HQ-Leiria*”.

Em relação ao endereçamento, foi-nos dado o endereço de rede 192.100.1.0/24 para todo o endereçamento da empresa, com este, sub endereçamos em várias sub-redes utilizando o menor número de endereços possíveis.

Quanto à rede publica (*Internet*), não faria sentido também usarmos esta gama de endereços, sendo que é uma gama de endereços privados, definimos que a nossa empresa é cliente da MEO, e, portanto, fomos ao site <https://ipinfo.io/AS3243> onde podemos ver as gamas de IP's públicos da *MEO*, e escolhemos a rede 185.2.84.0/22 que é referente a *MEO- Soluções Empresariais* (fig. 2), com esta gama de IP's, sub endereçamos em 4 redes com a mascara 255.255.255.252, sendo que serão para 4 ligações ponto-a-ponto, sendo uma delas referente à *VPN*.

Netblock	Description	Num IPs
144.64.0.0/16	MEO - SERVICOS DE COMUNICACOES E MULTIMEDIA S.A.	65,536
176.78.0.0/15	MEO - SERVICOS DE COMUNICACOES E MULTIMEDIA S.A.	131,072
185.2.84.0/22	MEO - Solucoes Empresariais	1,024
188.250.0.0/15	MEO - SERVICOS DE COMUNICACOES E MULTIMEDIA S.A.	131,072

Figura 2 - Endereços Públicos da MEO

Existe ainda a gama IP 192.168.1.0/24, que é referente à rede da casa de um dos administrados da nossa empresa.

A tabela seguinte, mostra-nos o endereçamento efetuado.

Equipamento	Interface	IP	Máscara de rede	Default Gateway	Descrição
HQ-Leiria	Fa1/0	185.2.84.9	255.255.255.252		Leiria-ISP
	Se0/0/0.1	192.100.1.182	255.255.255.252		Leiria-Santarém
	Se0/0/0.2	192.100.1.178	255.255.255.252		Leiria-Portalegre
	Fa0/0.70	192.100.1.30	255.255.255.224		Vlan70-Vendas
	Fa0/0.80	192.100.1.110	255.255.255.240		Vlan80-RH
	Fa0/0.90	192.100.1.150	255.255.255.248		Vlan90-Admin
	Fa0/1	192.100.1.174	255.255.255.248		Servidores
	Tunnel0	185.2.84.13	255.255.255.252		VPN(<i>GreTunnel</i>)
BRANCH-Santarém	Se0/0/0.1	192.100.1.181	255.255.255.252		Santarém-Leiria
	Gig0/0.10	192.100.1.62	255.255.255.224		Vlan10-Vendas
	Gig0/0.20	192.100.1.126	255.255.255.240		Vlan20-RH
	Gig0/0.30	192.100.1.166	255.255.255.248		Vlan30-Admin
BRANCH-Portalegre	Se0/0/0.1	192.100.1.177	255.255.255.252		Portalegre-Leiria
	Gig0/0.40	192.100.1.94	255.255.255.224		Vlan40-Vendas
	Gig0/0.50	192.100.1.142	255.255.255.240		Vlan50-RH
	Gig0/0.60	192.100.1.158	255.255.255.248		Vlan60-Admin
ISP_MEO_R1	Fa0/0	185.2.84.10	255.255.255.252		Internet

	Dialer1(Fa0/1)	IPCP (185.2.84.1)	255.255.255.252		PPPoE(Internet)
ISP_MEO_R2	Fa0/0	185.2.84.2	255.255.255.252		PPPoE(Internet)
	Fa0/1	185.2.84.5	255.255.255.252		Internet
MEO- ACAD40	Fa0/0	185.2.84.6	255.255.255.252		Internet
	Fa0/1	192.168.1.254	255.255.255.0		Rede de Casa
	Tunnel 0	185.2.84.14	255.255.255.252		VPN(GreTunnel)
FTP	Fa0	192.100.1.169	255.255.255.248	192.100.1.174	Servidores
DHCP_DNS	Fa0	192.100.1.170	255.255.255.248	192.100.1.174	
HTTP	Fa0	192.100.1.171	255.255.255.248	192.100.1.174	
MAIL	Fa0	192.100.1.172	255.255.255.248	192.100.1.174	
SYSLOG_NTP	Fa0	192.100.1.173	255.255.255.248	192.100.1.174	
PC1 - Admin	Fa0	DHCP	255.255.255.248	192.100.1.150	Leiria
PC2 - RH	Fa0	DHCP	255.255.255.240	192.100.1.110	Leiria
PC3 - Vendas	Fa0	DHCP	255.255.255.224	192.100.1.30	Leiria
PC4 - Admin	Fa0	DHCP	255.255.255.248	192.100.1.166	Santarém
PC5 - RH	Fa0	DHCP	255.255.255.240	192.100.1.126	Santarém
PC6 - Vendas	Fa0	DHCP	255.255.255.224	192.100.1.62	Santarém
PC7 - Admin	Fa0	DHCP	255.255.255.248	192.100.1.94	Portalegre
PC8 - RH	Fa0	DHCP	255.255.255.240	192.100.1.142	Portalegre
PC9 - Vendas	Fa0	DHCP	255.255.255.224	192.100.1.158	Portalegre

Tabela 1 - Endereçamento de Rede

3. Configurações Básicas

Efectuamos algumas configurações básicas em todos os equipamentos de rede presentes no cenário, de forma a garantir de certo modo alguma segurança, tais foram:

- Definir o hostname -> *hostname <nome>*
- Password (*cisco*) para o acesso à consola (*CLI*)
- Password (*cisco*) para os terminais virtuais (acesso remoto)
- Password (*class*) de acesso ao modo privilegiado
- Mensagem de *banner motd*

4. Vlans

Para cumprir com o pressuposto “Não haverá conectividade layer 2 entre as 3 redes locais, sendo que podem partilhar o mesmo switch.”, houve a necessidade de implementação de *VLAN's*, criando assim vários domínios de Broadcast.

Foi então necessário criar nove *VLAN's*, seguindo uma numeração de 10 em 10, começando na *VLAN 10* e acabando na *VLAN 90*. Seguiu-se sempre a ordem de Vendas, RH (Recursos Humanos) e Administração.

Na sede da empresa, em Leiria, o encaminhamento entre as 3 *Vlan's* existentes é garantido através do router HQ-Leiria, usando as suas sub-interfaces (*Router on a stick*). Na ligação entre os diversos computadores ao router existem dois *switch's* de 24 portas. No *switch* Leiria-SW1, estão ligados os cinco computadores pertencentes ao departamento dos Administradores e os 10 computadores pertencentes ao departamento

dos Recursos Humanos, configurados em modo *access*. Neste *switch* existe uma interface configurada em modo *trunk*, que se vai ligar a um novo *switch*, Leiria-SW2, que se encontra ligado aos 20 computadores do departamento de Vendas, em modo *access*. Estas configurações são necessárias para garantir o encaminhamento entre *Vlan's*.

Nas sucursais Santarém e Portalegre, o funcionamento é semelhante, sendo o encaminhamento entre as *Vlan's* garantido através dos routers *BRANCH-Santarem* e *BRANCH-Portalegre*, respetivamente.

5. Encaminhamento

O encaminhamento da empresa é assegurado pelo protocolo *RIP*, configurado nos routers da sede e das sucursais.

No router *HQ-Leiria* está configurada uma rota estática por omissão para o router *ISP_MEO_R1* para simular o acesso à internet, e dentro do protocolo *RIP* neste router é feito o comando *default-information originate* que redistribui a rota por omissão. Nos routers da sede e das sucursais é feito o comando *passive-interface <nome interface>* para que o router não partilhe informações de encaminhamento com as suas redes locais.

O *ISP* está configurado com rotas estáticas.

O router *MEO-ACAD40* da casa do Administrador tem uma rota por omissão para o router *ISP_MEO_R2*, para o administrador ter acesso à *Internet*.

Ao analisarmos, escolhemos o *RIP* essencialmente por ser um protocolo que consome poucos recursos (Memoria e *CPU*), por ser um protocolo simples, e um protocolo que funciona para redes pequenas a medias, sendo baseado no número de saltos (**Max. 15**).

6. Tecnologia WAN

Devido a ser uma empresa que tem a sede e as sucursais geograficamente distantes, optou-se por utilizar uma tecnologia WAN, neste caso utilizamos o *Frame Relay*. É um protocolo WAN de alto desempenho que opera na camada física e na camada de ligação de dados do modelo de referência OSI, e é usado para transmitir de maneira rápida e barata a informação, essa informação é dividida em *frames*.

Através de uma *Cloud* configurou-se as *DLCI* necessárias, e nos routers da sede e sucursais efetuou-se configurações relativas ao *frame relay* (fig.3).

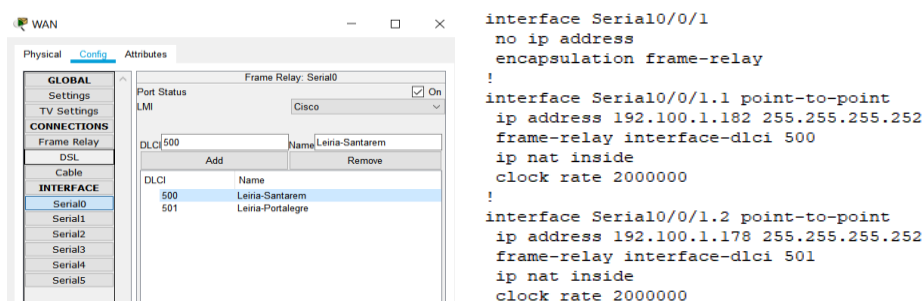


Figura 3 - Exemplo de parte da configuração *Frame Relay* realizada

7. Políticas de Acesso (*ACL's*)

De modo a controlar onde é que os funcionários da empresa podem aceder, configurou-se 2 *ACL's* em cada router (Sede e Sucursais), uma referente à rede local das vendas e outra à rede local de recursos humanos.

As restrições aplicadas foram as seguintes:

- Tanto Administradores, funcionários do departamento de vendas e do departamento de RH só podem comunicar entre si via email (em toda a empresa)
- Funcionários do departamento de vendas e de RH, apenas acedem aos servidores somente no porto do respetivo serviço
 - Servidor mail – porto 25 e 110
 - Servidor web – porto 80 e 443
 - Servidor DNS – porto 53
 - Servidor DHCP – porto 67
 - Servidor FTP – porto 21
- É permitido também aos funcionários o acesso à internet;

Os administradores conseguem comunicar entre si de todas as formas, e podem aceder aos servidores através de qualquer porto, visto serem administradores.

Foi criada uma *ACL* que diz respeito à translação de endereços, que iremos abordar noutro capítulo deste documento.

A Figura(fig. 4) mostra o exemplo de configuração, neste caso no router *HQ-Leiria*, de notar que na parte que diz respeito ao servidor *FTP*, colocou-se o porto na *ACL*, e os computadores conseguiam aceder ao servidor fazendo login, mas ao irem buscar um ficheiro ou colocar no servidor surgia um erro, daí termos retirado o porto do *FTP* da *ACL*.

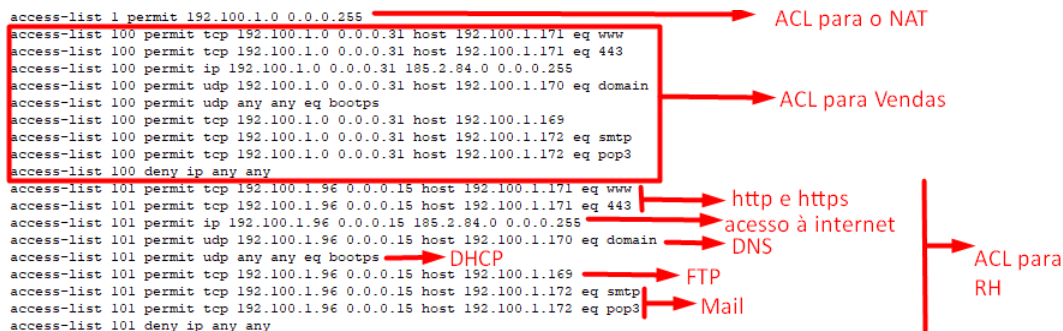


Figura 4 - Access list's do router *HQ-Leiria*

8. Serviço DHCP

Foi configurado um servidor de *DHCP* ("*DHCP_DNS*"), para que fosse atribuído de forma dinâmica a todos os computadores da empresa a sua configuração de rede, ou seja, o *IP*, máscara de rede, *default-gateway*, bem como o endereço *IP* do servidor de *DNS*. Os *IP's* dos servidores estão configurados estaticamente.

Desta forma, ativou-se o serviço e criamos 9 *Pool's*, onde foi necessário configurar o *default-gateway*, o *IP* do servidor de *DNS*, o primeiro *IP* disponível, a máscara de sub-rede e o número máximo de utilizadores (fig 5).

Foi necessário nas interfaces do router correspondentes a cada rede local, utilizar o comando *ip helper-address 192.100.1.170* (IP do servidor *DHCP_DNS*), devido ao servidor estar num domínio de *broadcast* diferente das redes locais.

Este serviço encontra-se 100% funcional, sendo que todos os computadores da empresa obtêm a sua configuração de rede por *DHCP*.

Pool Name	Default Gateway	DNS Server	Start IP Address	Subnet Mask	Max User	TFTP Server	WLC Address
Vendas_Leiria	192.100.1.30	192.100.1.170	192.100.1.1	255.255.255.224	20	0.0.0.0	0.0.0.0
RH_Leiria	192.100.1.110	192.100.1.170	192.100.1.97	255.255.255.240	10	0.0.0.0	0.0.0.0
Admin_Leiria	192.100.1.150	192.100.1.170	192.100.1.145	255.255.255.248	5	0.0.0.0	0.0.0.0
Admin_Santarem	192.100.1.168	192.100.1.170	192.100.1.161	255.255.255.248	5	0.0.0.0	0.0.0.0

Figura 5 - Exemplo de configuração de uma pool

9. Servidor de Transferência de Ficheiros (FTP)

Na sede em Leiria, foi criado um servidor de FTP que se encontra disponível em toda a rede da empresa. Neste servidor, foram criados um conjunto de *usernames* e *passwords* para todos os funcionários da empresa.

Na criação de utilizadores (fig.6), concedemos todas as permissões aos administradores da empresa (*Read*, *Write*, *Delete*, *Rename* e *List*). Enquanto aos funcionários do departamento de vendas, e de recursos humanos apenas têm a possibilidade de ler e listar os ficheiros existentes no servidor (*Read* e *List*).

O servidor *FTP* responde por <ftp.pgnet.pt> sendo este *URL* resolvido pelo servidor de DNS. Este serviço encontra-se 100% funcional, sendo que é possível aceder ao serviço *FTP*.

User Setup

Service: ☒ On ☐ Off

Username: adminSantarem Password: cisco

☒ Write ☒ Read ☒ Delete ☒ Rename ☒ List

	Username	Password	Permission
3	adminSantarem	cisco	RWDL
4	rhLeiria	cisco	RL
5	rhPortalegre	cisco	RL
6	rhSantarem	cisco	RL

PC1 - Admin

Physical Config Desktop Programming Attributes

Command Prompt

```

Packet Tracer PC Command Line 1.0
C:\>ftp ftp.pgnet.pt
Trying to connect...ftp.pgnet.pt
Connected to ftp.pgnet.pt
220- Welcome to FT Ftp server
Username:adminLeiria
331- Username ok, need password
Password:
230- Logged in
(passive mode On)
ftp>put pgnet.txt
Writing file pgnet.txt to ftp.pgnet.pt:
File transfer in progress...
[Transfer complete - 7 bytes]
7 bytes copied in 0.022 secs (318 bytes/sec)

```

Figura 6 – Exemplos: Configuração de utilizador e acesso ao servidor de FTP

10. Servidor Web (HTTP & HTTPS)

Como qualquer empresa, também a nossa, tem um servidor web situado na sede em Leiria onde está alojado a página web da empresa. Este servidor é acedido através da internet com recurso ao *NAT* (conceito a ser explicado no próximo tópico) e acedido internamente dentro da empresa. Outra forma era ter o servidor alojado num serviço de *Cloud* na internet.

Criamos o servidor web com acesso por HTTP no porto 80, e com acesso por HTTPS no porto 443 pois é a forma segura e aconselhável.

Para simular o site da empresa, existe uma página principal com uma mensagem de boas vindas, e depois dois links, que redirecionam para uma página com a história da empresa e outra com os contactos, respetivamente. O *URL* para acesso ao site é resolvido pelo servidor de *DNS* implementado.

Este serviço encontra-se 100% funcional, sendo que tanto os computadores da empresa, como alguém externo à empresa pode aceder ao *website*.



Figura 7 - Vista do website

11. Translação de Endereços (NAT)

Pelo pressuposto, todos os endereços da empresa devem ser traduzidos para um endereço único que está associado à interface WAN do router ligado ao *ISP*.

Para isto, no router que fornece o acesso à internet *HQ-Leiria*, foi criada uma *ACL* (com a rede da empresa) a ser usada no *NAT*, de seguida fez-se o *NAT overload*, onde se define qual a interface de saída e o que vai ser traduzido, neste caso associamos a *ACL* criada.

ip nat inside source list 1 interface FastEthernet1/0 overload

De seguida na interface de saída do router fez-se *ip nat outside*, nas restantes interfaces que pertencem a rede da empresa fez-se *ip nat inside*, e com isto ao efetuarmos um *ping* para um router do *ISP* o endereço de origem é traduzido no endereço publico da interface do router. Podemos confirmar o funcionamento com o comando *show ip nat translations* (fig. 9).

Ainda em relação ao *NAT*, para que o servidor alojado na rede interna da empresa seja acedido através da internet, teve que se configurar o *NAT*, redirecionando para o *IP* e porto do servidor web, ou seja, todos os pedidos feitos à interface WAN (185.2.84.9) no porto 80 (*HTTP*) ou 443(*HTTPS*) serão redirecionados para o servidor web interno, pode-se testar no *PC Home*, colocando no browser <http://185.2.84.9> ou <https://185.2.84.9>.

```
ip nat inside source static tcp 192.100.1.171 80 185.2.84.9 80
ip nat inside source static tcp 192.100.1.171 443 185.2.84.9 443
```

Figura 8 - Configuração do NAT para acesso externo ao servidor Web

Por considerarmos revelante, configuramos também *NAT* no *router* da casa do administrador (*MEO-ACAD40*), porque é este processo que acontece em todas as casas.

```
HQ-Leiria#sh ip nat translations
Pro Inside global      Inside local      Outside local      Outside global
icmp 185.2.84.9:2      192.100.1.113:2  185.2.84.10:2      185.2.84.10:2
tcp 185.2.84.9:443     192.100.1.171:443 ---                ---
tcp 185.2.84.9:443     192.100.1.171:443 185.2.84.6:1028    185.2.84.6:1028
tcp 185.2.84.9:80      192.100.1.171:80  ---                ---
tcp 185.2.84.9:80      192.100.1.171:80  185.2.84.6:1025    185.2.84.6:1025
tcp 185.2.84.9:80      192.100.1.171:80  185.2.84.6:1026    185.2.84.6:1026
```

Figura 9 - Verificação das traduções no Router HQ-Leiria

12. PPPoE (Point-to-Point Protocol over Ethernet)

No nosso projeto o serviço PPPoE encontra-se 100% funcional e foi configurado entre os *routers* *ISP_MEO_R1* (cliente) e *ISP_MEO_R2* (servidor).

Num cenário real, o serviço PPPoE e o NAT poderiam ter sido configurados apenas num *router* (*HQ-Leiria*), mas visto que estamos a trabalhar num ambiente virtual e devido às limitações do *Cisco Packet Tracer*, de não possuir a imagem completa do *IOS*, foi necessário utilizar dois *routers* diferentes de forma a não causar problemas com o NAT.

```
ISP_MEO_R1#sh ip int br
Interface      IP-Address      OK? Method Status      Protocol
FastEthernet0/0 185.2.84.10    YES manual up          up
FastEthernet0/1 unassigned      YES unset up          up
Virtual-Access1 unassigned      YES unset up          up
Virtual-Access2 unassigned      YES manual up          up
Dialer1         185.2.84.1     YES IPCP up          up
Vlan1           unassigned      YES unset administratively down down
ISP_MEO_R1#
```

Figura 10 - Verificação do IP atribuído à interface Dialer1

```
interface FastEthernet0/1
no ip address
pppoe enable
pppoe-client dial-pool-number 1
duplex auto
speed auto
!
interface Dialer1
dialer pool 1
ip address negotiated
mtu 1492
encapsulation ppp
ppp chap hostname pgnet
ppp chap password cisco
!
username pgnet password 0 cisco
bba-group pppoe PGNET
virtual-template 1
interface Virtual-Template1
peer default ip address pool pgnet
ppp authentication chap
ip unnumbered FastEthernet0/0
encapsulation ppp
interface FastEthernet0/0
ip address 185.2.84.2 255.255.255.252
pppoe enable group PGNET
duplex auto
speed auto
ip local pool pgnet 185.2.84.1 185.2.84.1
```

Figura 11 - Configuração cliente e servidor (PPPoE)

13. VPN (Virtual Private Network)

De forma a que um administrador da empresa através da sua casa possa aceder de forma segura à sua rede local na empresa, tivemos que implementar uma *VPN*.

Para tal, utilizamos o protocolo *GRE*, onde foi criado um *tunnel* entre o *router* *MEO-ACAD40* (casa do administrador) e o *router* da *HQ-Leiria*, definimos no cenário que a casa é referente a um administrador da sede Leiria.

Assim, foi configurada uma *VPN*, 100% funcional, estabelecendo então uma ligação segura entre a casa do administrador e a sua rede local da empresa.

Para testar, pudemos fazer um *ping* do *PC Home* para o *PC1 – Admin*, e obtemos sucesso, podemos verificar também por onde passou o pedido e verificar que passou pelo *tunnel* criado.

```
interface Tunnel0
ip address 185.2.84.14 255.255.255.252
mtu 1476
tunnel source FastEthernet0/0
tunnel destination 185.2.84.9
!
ip route 192.100.1.144 255.255.255.248 185.2.84.13
```

```
C:\>tracert 192.100.1.145
Tracing route to 192.100.1.145 over a maximum of 30 hops:
  0  0 ms  0 ms  3 ms  192.168.1.254
  1  13 ms  3 ms  0 ms  185.2.84.13
  2  12 ms  0 ms  1 ms  192.100.1.145
Trace complete.
```

Figura 12 - Configuração do tunnel (MEO-ACAD40) e tracert

14. Funcionalidades Extra

Servidor DNS

Na sede em Leiria, foi criado um servidor de *DNS*, a ser atribuído a todos os computadores fazendo assim a resolução de endereços *IP* em nomes. Adicionou-se as entradas *pgnet.pt*, **www.pgnet.pt** referentes ao servidor *web*, **ftp.pgnet.pt** referente ao servidor *FTP* e **mx.pgnet.pt** referente ao servidor de email.

Servidor de Email

Na sede em Leiria, foi criado um servidor de Email, para que todas as redes da empresa tenham um email para comunicações institucionais. No servidor de Email, foram criadas nove contas de utilizador. O serviço de Email utiliza o protocolo SMTP para envio de email e o protocolo POP3 para receber os emails. Finda a configuração do servidor de email, foi necessário configurar o cliente, onde inserimos a conta e definimos como o servidor de email.

Acesso SSH aos routers

Foi configurado o acesso *SSH* em todos os routers da empresa, para que os administradores possam aceder remotamente e de forma segura. Tivemos que em todos os routers gerar uma chave com o comando ***crypto key generate rsa***, onde definimos o tamanho de 1024 bits, de seguida colocamos o comando ***transport input ssh*** dentro do terminal virtual 0 4. Criamos um utilizador e uma password, e de seguida é possível a partir de um computador de um administrador aceder por *SSH* aos routers através do comando ***ssh -l <username> <ip>***.

Servidor NTP e Syslog

De forma a que todos os *logs* dos routers da empresa fiquem centralizados num único servidor, foi implementado um servidor de *Syslog* na empresa. Para tal, foi apenas necessário ativar o serviço de *Syslog* no servidor, e, nos routers inserir o comando ***logging 192.100.1.173*** (*ip do servidor*).

Para que todos os *routers*, estejam sincronizados com a mesma hora, foi configurado um servidor *NTP*. Para tal foi necessário escolher a data e hora no servidor e ativar o serviço. Nos routers foi necessário efetuar o comando ***ntp server 192.100.1.173*** (*ip do servidor*).

Para que os logs sejam enviados com a data e hora do router, foi necessário efetuar o comando ***service timestamps log datetime msec***, em todos os routers.

15. Conclusão

Com a realização deste trabalho, podemos concluir que os requisitos propostos foram cumpridos, tendo-se conseguido gerir as necessidades de endereçamento de acordo com as necessidades pretendidas. Também como elementos extras, pudemos implementar servidores de *DNS* e de *MAIL*, que são indispensáveis a qualquer instituição/empresa. Optamos por centralizar os *logs* dos routers num único servidor, tornando-se mais fácil para os administradores analisarem causa ocorra algum problema.

De forma a garantirmos que a rede seja segura, utilizamos versões de protocolos seguros, como por exemplo, o protocolo, HTTPS e o SSH. Também os *routers* e *switches* estão protegidos com autenticação, de forma a proteger estes equipamentos de acessos de utilizadores não qualificados para o efeito.

Como melhoria deste projeto, poderíamos ter implementado uma firewall de forma a proteger melhor a rede da empresa.

Contudo, foi um trabalho que gostamos de elaborar, onde pudemos adquirir conhecimentos muito importantes, que ocorrem no dia-a-dia de todos nós em nossas casas, por exemplo o *NAT*, entre os demais. Achamos que com os pressupostos definidos pelos docentes, conseguimos realizar um bom trabalho aproveitando para aprofundar um pouco mais certos pontos.