

# PROJETO TEMÁTICO EM REDES DE COMPUTADORES

## Relatório Final

Escola Superior de Tecnologia e Gestão de Águeda

Universidade de Aveiro

2º semestre

2016-2017

### **Grupo 4:**

Ana Lopes	nº 84049
Eduardo Silva	nº 83971
João Teixeira	nº 84205
Luís Pinho	nº 83926
Raquel Monteiro	nº 83589
Rui Duarte	nº 29979





# Escola Superior de Tecnologia e Gestão de Águeda



# PROJETO TEMÁTICO EM REDES DE COMPUTADORES

## Relatório Final

Escola Superior de Tecnologia e Gestão de Águeda

Universidade de Aveiro

2º semestre

2016-2017

### **Grupo 4:**

Ana Lopes	nº 84049
Eduardo Silva	nº 83971
João Teixeira	nº 84205
Luís Pinho	nº 83926
Raquel Monteiro	nº 83589
Rui Duarte	nº 29979

***Orientadores: Luís Silva, Joaquim  
Ferreira***





## **Escola Superior de Tecnologia e Gestão de Águeda**



# Escola Superior de Tecnologia e Gestão de Águeda

## Índice

### Índice

<b>1.</b>	<b>INTRODUÇÃO.....</b>	<b>8</b>
<b>2.</b>	<b>PLANEAMENTO.....</b>	<b>12</b>
2.1.	TAREFAS.....	12
2.2.	ESCALONAMENTO DE TAREFAS.....	14
<b>3.</b>	<b>REDE BÁSICA.....</b>	<b>16</b>
3.1.	SOLUÇÃO PROPOSTA .....	16
3.2.	RECURSOS HUMANOS E EQUIPAMENTOS.....	17
3.3.	CONFIGURAÇÕES BÁSICAS DA REDE.....	18
3.4.	CONFIGURAÇÕES/EXPLICAÇÃO DOS DIFERENTES SERVIÇOS/SOFTWARES .....	18
	<i>Active Directory (AD).....</i>	<i>19</i>
	<i>DNS.....</i>	<i>21</i>
	<i>DHCP.....</i>	<i>22</i>
	<i>NAT.....</i>	<i>22</i>
	<i>VPN.....</i>	<i>23</i>
	<i>Firewall.....</i>	<i>25</i>
	<i>Proxy.....</i>	<i>25</i>
	<i>FileServer.....</i>	<i>27</i>
	<i>WebServer.....</i>	<i>29</i>
3.5.	ERROS / PROBLEMAS / OBSERVAÇÕES.....	30
<b>4.</b>	<b>CONCLUSÃO.....</b>	<b>32</b>
<b>5.</b>	<b>FONTES E MATERIAL DE REFERÊNCIA .....</b>	<b>34</b>
<b>6.</b>	<b>ANEXOS .....</b>	<b>36</b>

## Índice de Figuras

FIGURA 1 - CALENDARIZAÇÃO .....	12
FIGURA 2 - TAREFAS POR ETAPAS .....	12
FIGURA 3 - MAPA DE GANTT PREVISTO PARA CADA ETAPA .....	13
FIGURA 4 - LOGOTIPO DO WINDOWS SERVER 2012 R2 .....	14
FIGURA 5 - PAINEL INICIAL CCPROXY .....	15
FIGURA 6 - CONFIGURAÇÃO DA REDE PROPOSTA.....	16
FIGURA 7 - TESTE DA ROTA CONFIGURADA PARA A REDE COMWIFI.....	19
FIGURA 8 - CLIENTE LOGADO COM O DOMÍNIO CRIADO .....	21
FIGURA 9 - TESTE DE DHCP .....	22
FIGURA 10 - CONFIGURAÇÃO DE ENDEREÇOS ESTÁTICOS PARA A VPN .....	24
FIGURA 11 - TESTE VPN NO CLIENTE .....	24
FIGURA 12 - TESTE DA PROXY.....	26
FIGURA 13 - CCPROXY WEBFILTER.....	27
FIGURA 14 - CONFIGURAÇÕES DAS PARTILHAS DOS UTILIZADORES .....	28
FIGURA 15 - DRIVES PARTILHADAS COM CADA UTILIZADOR .....	29

## Escola Superior de Tecnologia e Gestão de Águeda

### Índice de Tabelas

TABELA 1 - REQUISITOS DE HOSTS POR DEPARTAMENTO .....	10
TABELA 2 - REQUISITOS DE HOSTS POR DEPARTAMENTO .....	18
TABELA 3 - QUANTIDADES E CUSTOS DE CADA RECURSO.....	18
TABELA 4 – CONFIGURAÇÕES.....	18



## **Escola Superior de Tecnologia e Gestão de Águeda**



## Escola Superior de Tecnologia e Gestão de Águeda

### 1. INTRODUÇÃO

Este trabalho foi proposto no âmbito do Módulo Temático de Redes de Computadores, mais concretamente na componente do Projeto Temático em Redes de Computadores.

Este projeto tem como objetivo o desenvolvimento de uma nova rede, que nela deverão ser incluídas as seguintes componentes:

- Estrutura da intranet;
- Conectividade;
- Endereçamento;
- Serviços de rede;
- Serviços de virtualização;
- Opcionais (bloqueio de sites/serviços, redundância lógica/física da intranet).

Além disso outra componente de uso obrigatório neste projeto seria o uso da aplicação Web `code.ua.pt` onde o projeto deveria conter um repositório de informação colocando as tarefas a serem executadas permitindo ao professor acompanhar o desenvolvimento do mesmo.

De forma a que todos os elementos do grupo pudessem trabalhar no projeto sem ser necessário movê-lo para diferentes computadores, criámos o projeto num computador e mantivemos este computador ligado e conectado à internet com uma sessão de TeamViewer pronta ser usada. Cada membro registou os dados de ligação ao PC e Ligava-se ao mesmo sempre que queria efetuar uma alteração.

Os grupos foram contactados de forma a fornecer uma proposta de solução para a criação da nova rede para a empresa ANOVTEC, acompanhada de um orçamento e de uma planificação dos trabalhos.

Em seguida estão descritas as componentes deste documento e as suas metodologias:

- Planificação do trabalho (contém tudo o que está associado à fase de planeamento de um projeto: as tarefas desenvolvidas ao longo do

## Escola Superior de Tecnologia e Gestão de Águeda

mesmo, esquematização das tarefas, atividades do projeto em cronogramas e tipos de requisitos associados ao desenvolvimento da rede);

- Descrição das atividades inerentes ao desenvolvimento da rede (tipos de softwares usados;
- Fontes e material de referência.

O cliente deste projeto é uma empresa com diversos departamentos que pretende ter uma rede estruturada na qual possa distribuir internet, partilhar ficheiros, e aumentar a eficiência da empresa por todos os departamentos e edifícios da mesma.

- Necessidades da empresa:
- Rede completamente funcional e dinâmica (DHCP,DNS);
- Wifi num dos departamentos;
- Servidor de ficheiros;
- Proteção (Firewall, Proxy).
- Acesso a partir do exterior (VPN)

A empresa está distribuída por 3 edifícios e está dividida por 3 departamentos (“Gestão, “Engenharia” e “Comercial”) e por um “Datacenter” (onde está situado o servidor da empresa e o router). O primeiro edifício é onde será alojado o datacenter. O departamento de “Gestão” está sediado no edifício 2 e os restantes departamentos (“Engenharia” e “Comercial”) estão no edifício 3. Cada departamento tem de suportar um número mínimo de hosts ligados ao mesmo tempo. Estes requisitos podem ser consultados na tabela seguinte.



## Escola Superior de Tecnologia e Gestão de Águeda

Departamento	Número de hosts
Edifício 1 – Datacenter	15
Edifício 2 – Dep. Gestão	10
Edifício 3 – Dep. Comercial (Cablada)	20
Edifício 3 – Dep. Comercial (Wireless)	20
Edifício 3 – Dep. Engenharia	100

*Tabela 1 - Requisitos de hosts por departamento*

Cada departamento deverá ter uma rede IP única atribuída. Um dos requisitos da rede é que deverá ter os seguintes serviços implementados: DHCP, DNS, NAT e AD (Active Directory).



## **Escola Superior de Tecnologia e Gestão de Águeda**

# Escola Superior de Tecnologia e Gestão de Águeda

## 2. PLANEAMENTO

### 2.1. Tarefas

#### *Tarefas por etapa do projeto*

No âmbito da fase de planeamento, a elaboração de um cronograma é uma forma de organizar e gerir as tarefas durante a execução de um projeto. Consiste na determinação da melhor forma de posicionar as tarefas ao longo do tempo de acordo com a duração das mesmas, das relações de precedência entre elas e dos prazos a cumprir. Com base nisto, foi elaborado uma calendarização do projeto (Fig. 1) e um cronograma (Fig. 3) no qual estão presentes as atividades previstas para cada etapa bem como o tempo previsto de execução de cada uma delas (Fig. 2).

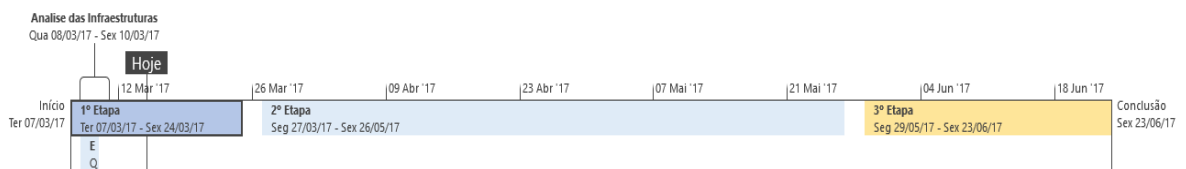


Figura 1 - Calendarização

1		Projeto	79 dias	Ter 07/03/17	Sex 23/06/17
2		1ª Etapa	14 dias?	Ter 07/03/17	Sex 24/03/17
3					
4		Desenho da Rede	1 dia	Ter 07/03/17	Ter 07/03/17
5		Análise das Infraestrut	3 dias	Qua 08/03/17	Sex 10/03/17
6		Levantamentos de Rec	2 dias	Seg 13/03/17	Ter 14/03/17
7		Esboço do relatório.	2 dias	Qua 08/03/17	Qui 09/03/17
8		Configuração básica da	4 dias	Qua 15/03/17	Seg 20/03/17
9		Configuração DHCP e D	3 dias	Ter 21/03/17	Qui 23/03/17
10		Entrega do Primeiro R	1 dia	Sex 24/03/17	Sex 24/03/17
11		2ª Etapa	45 dias	Seg 27/03/17	Sex 26/05/17
12		Configuração da Firew	3 dias	Seg 27/03/17	Qua 29/03/17
13		Configuração do servic	4 dias	Qui 30/03/17	Ter 04/04/17
14		Entrega do Relatório Ir	1 dia	Sex 26/05/17	Sex 26/05/17
15		3ª Etapa	20 dias	Seg 29/05/17	Sex 23/06/17
16		Configuração da gestã	3 dias	Seg 29/05/17	Qua 31/05/17
17		Configuração do Servic	2 dias	Seg 29/05/17	Ter 30/05/17
18		Configuração do Servic	1 dia	Seg 29/05/17	Seg 29/05/17
19		Configuração do Servic	1 dia	Seg 29/05/17	Seg 29/05/17
20		Entrega do Pré-Relatór	1 dia	Sex 16/06/17	Sex 16/06/17
21		Entrega do Relatório Fi	1 dia	Sex 23/06/17	Sex 23/06/17

Figura 2 - Tarefas por etapas



## Escola Superior de Tecnologia e Gestão de Águeda

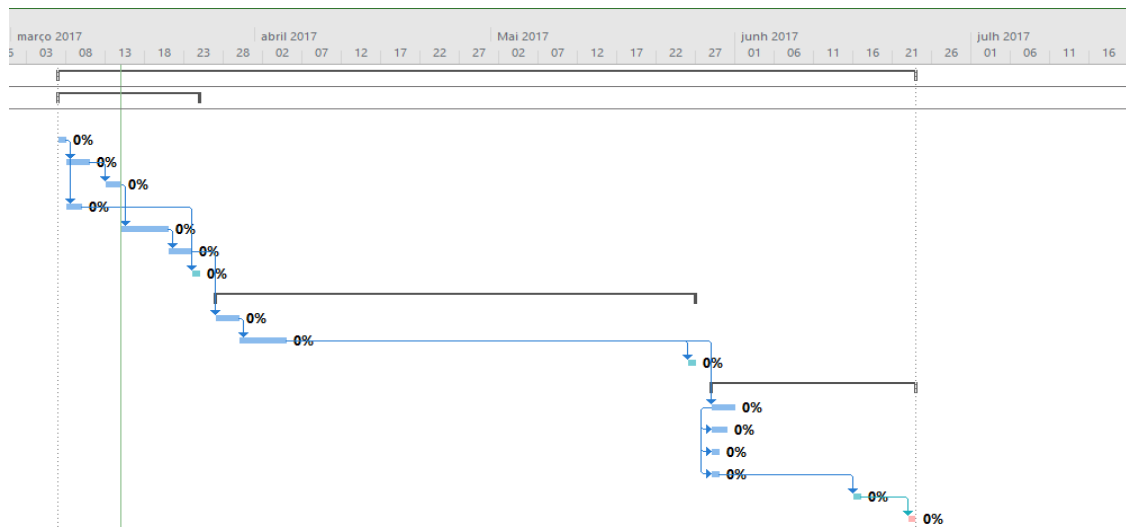


Figura 3 - Mapa de Gantt previsto para cada etapa

### 2.2. Escalonamento de tarefas

#### *Primeira Etapa*

Na primeira fase do Projeto, tivemos que desenhar a estrutura da rede, analisar as infraestruturas e realizar uma configuração básica da rede, **DHCP**, **DNS** e **NAT**. Para tal, recorreremos à instalação do Windows Server 2012 R2.

**DHCP** - na configuração do DHCP, usamos o router principal, para fazer a configuração das diferentes DHCP Pools e para fazer a distribuição do DHCP para os diferentes departamentos.

**DNS** - na configuração do DNS, utilizamos o DNS do Windows Server. A configuração do DNS é passada automaticamente pelo DHCP, que redireciona para o servidor.

**NAT** - na configuração da NAT, ligamos o router principal há cloud no GNS3 e na configuração do router atribuímos a essa ligação o IP do exterior atribuído ao nosso grupo, "192.168.229.204".

O Windows Server 2012 R2 é um sistema computacional, desenvolvido pela Microsoft, lançado a 17 de outubro de 2013.



*Figura 4 - Logotipo do Windows Server 2012 R2*

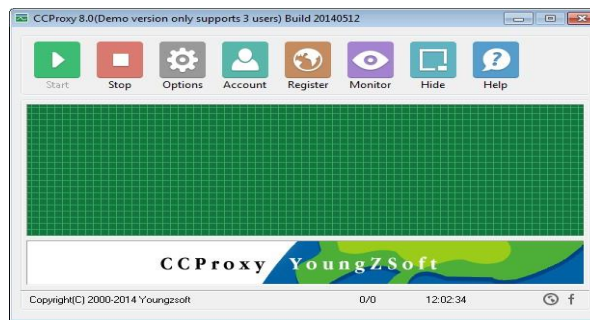
#### *Segunda Etapa*

Na segunda etapa, fizemos a configuração do **Proxy** e **firewall**.

No **Proxy**, usámos um software para servir de proxy: o CCProxy. A

## Escola Superior de Tecnologia e Gestão de Águeda

configuração do mesmo foi efetuada no programa.



*Figura 5 - Painel inicial CCProxy*

Na **firewall**, usámos a firewall do Windows Server.

### ***Terceira Etapa***

Na terceira etapa, configurámos os serviços de redes (**Gestão de utilizadores, Servidor de ficheiros, Servidor web**)

Na **Gestão de utilizadores**, utilizamos o **Active Directory (AD)**, tendo assim um serviço que faz tudo o que nos é pedido em relação á gestão de utilizadores.

No **Servidor de ficheiros**, utilizamos SMB share.

No **servidor web**, utilizamos o **IIS (Internet Information Services)**, serviço para criação de servidores web da Microsoft. Utilizamos o servidor web para hospedar o ficheiro de configuração automática do proxy e o website da empresa.



### 3. REDE BÁSICA

#### 3.1. Solução proposta

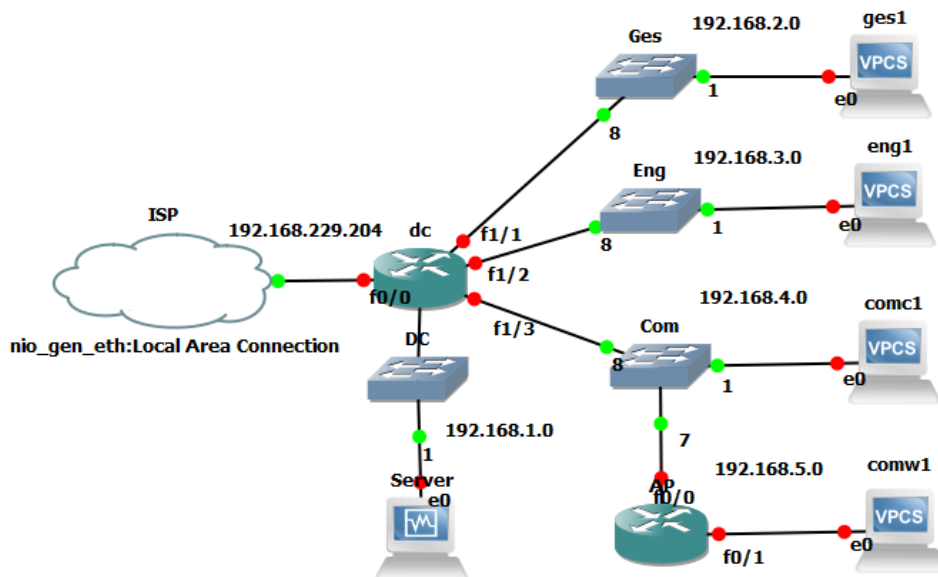


Figura 6 - Configuração da rede proposta

Para a configuração da rede, usámos um router para ligar ao exterior (onde está configurado o NAT). Este switch (ou router) liga o servidor principal (onde estão configurados serviços como DNS e Firewall) aos diferentes departamentos detalhados na imagem. Para o servidor principal, optámos por usar uma máquina virtual com o sistema Windows Server 2012 R2, sendo que oferece melhor desempenho que os PC's fornecidos para o mesmo, fortalecendo também a integração do mesmo com o GNS. Para o Datacenter, departamento de Engenharia e Gestão é colocado um switch para ligar as diferentes máquinas por cabo. No departamento comercial, é colocado um switch para as diferentes máquinas ligadas por cabo. Ainda ligados a este switch, temos 3 Access Points para a criação da rede wireless. De referir que, por uma questão de limitações do GNS3, os mesmos foram substituídos por um router.

## Escola Superior de Tecnologia e Gestão de Águeda

### 3.2. Recursos humanos e equipamentos

Durante o planeamento do projeto foi necessário pesquisar determinadas informações associadas ao mesmo. Estas estão relacionadas com todos os requisitos associados à criação de uma rede, desde os cabos aos routers e softwares necessários, bem como aos custos associados a estes. Na tabela abaixo (Tabela 1) está exemplificado o material necessário.

Levantamento de requisitos
Router Gigabit
Access Points Wireless
Switchs Gigabit (2x48p+4x24p)
Servidor
Fibra ótica
Cabo Ethernet (cat6)
Microsoft Windows Server 2012 R2
Mão de obra

### Orçamento

O orçamento previsto para a configuração da nova rede é de 53.350€. Para melhor compreender este valor, a tabela 3 indica o preço de cada recurso bem como o total.

Considerando os requisitos em causa (tabela 2), necessitamos de 1 switch L3 para gestão e monitorização do tráfego (GN3 usámos 1 router), 1 switch de 24 portas para o *Datacenter*, 1 switch de 24 portas para o departamento de *Gestão*, 2 switch de 48 portas e 1 switch de 24 portas para o departamento de *Engenharia*, 1 switch de 24 portas POE (para alimentar os APs) para o departamento *Comercial*. Relativamente às necessidades sem fios do departamento Comercial consideramos o uso de 3 access points ser suficiente para a cobertura de rede e para o número de utilizadores em causa.

## Escola Superior de Tecnologia e Gestão de Águeda

Departamento	Número de hosts
Edifício 1 – Datacenter	15
Edifício 2 – Dep. Gestão	10
Edifício 3 – Dep. Comercial (Cablada)	20
Edifício 3 – Dep. Comercial (Wireless)	20
Edifício 3 – Dep. Engenharia	100

Tabela 2 - Requisitos de hosts por departamento

Quantidade	Recurso	Custo
1	Cisco Catalyst 3850-24S-S	18.792,80€
3	Cisco Catalyst 2960X-24TS-L	2.250,44€
2	Cisco Catalyst 2960X-48TS	3.941,79€
1	Cisco Catalyst 2960X-24PS-L	3.002,15€
3	Cisco Aironet 18321	653,05€
1	Cisco UCS SmartPlay Select	10362,05€
1	Microsoft Windows Server 2012 R2 Datacenter Edition	4.600,00€
6	Técnicos	-----
<b>Total</b>		

Tabela 3 - Quantidades e Custos de cada recurso

### 3.3. Configurações Básicas da rede

O router foi configurado com as definições em anexo. Considerando as limitações mencionadas, o AP (um router neste caso) teve de ser configurado com um relay para o router principal, de forma a conseguir aos computadores da rede comercial wifi conseguirem obter IP.

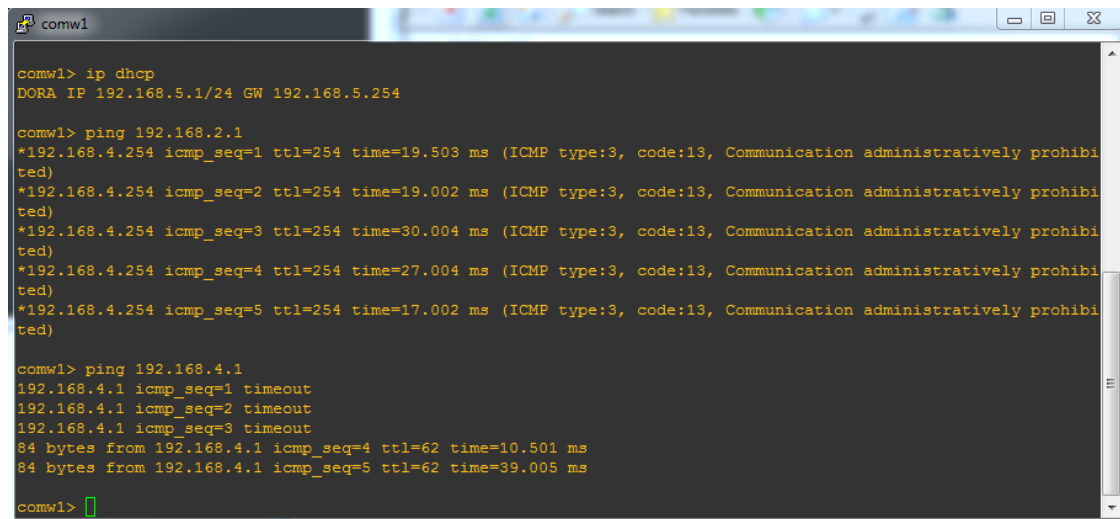
Edifício	Tipo de Ligação	Departamento	IP's	DHCP - Pool	Gateway	DNS	DNS - Exterior	Gateway - Exterior
1	Cabo	Server	192.168.1.0		192.168.1.254	192.168.1.1	192.168.229.1	192.168.229.254
2	Cabo	Gestão	192.168.2.0	1 - 253	192.168.2.254			
3	Cabo	Engenharia	192.168.3.0	1 - 253	192.168.3.254			
3	Cabo	Comercial	192.168.4.0	1 - 252	192.168.4.254			
3	Wifi	Comercial	192.168.5.0	1 - 253	192.168.5.254			

Tabela 4 – Configurações

### 3.4. Configurações/Explicação dos diferentes Serviços/Softwares

#### *Roteamento*

Para esta rede foram criadas apenas 2 rotas. Uma das rotas serve encaminhar todo o tráfego desconhecido (que não é destinado dentro da rede interna) para o exterior. De forma a bloquear o acesso entre máquinas do departamento comercial Wi-Fi e os restantes departamentos, foi criada uma segunda regra que bloqueia todo o tráfego vindo de dentro da rede COMWIFI para o exterior. Testámos esta regra realizando um ping de dentro da rede COMWIFI para outro dispositivo dentro da rede COM e para a rede GES, verificando que estava tudo isolado como configurado.



```
comw1> ip dhcp
DORA IP 192.168.5.1/24 GW 192.168.5.254

comw1> ping 192.168.2.1
*192.168.4.254 icmp_seq=1 ttl=254 time=19.503 ms (ICMP type:3, code:13, Communication administratively prohibited)
*192.168.4.254 icmp_seq=2 ttl=254 time=19.002 ms (ICMP type:3, code:13, Communication administratively prohibited)
*192.168.4.254 icmp_seq=3 ttl=254 time=30.004 ms (ICMP type:3, code:13, Communication administratively prohibited)
*192.168.4.254 icmp_seq=4 ttl=254 time=27.004 ms (ICMP type:3, code:13, Communication administratively prohibited)
*192.168.4.254 icmp_seq=5 ttl=254 time=17.002 ms (ICMP type:3, code:13, Communication administratively prohibited)

comw1> ping 192.168.4.1
192.168.4.1 icmp_seq=1 timeout
192.168.4.1 icmp_seq=2 timeout
192.168.4.1 icmp_seq=3 timeout
84 bytes from 192.168.4.1 icmp_seq=4 ttl=62 time=10.501 ms
84 bytes from 192.168.4.1 icmp_seq=5 ttl=62 time=39.005 ms

comw1>
```

*Figura 7 - Teste da rota configurada para a rede COMWIFI*

Não foi necessário criar encaminhamento dinâmico dentro da rede sendo que apenas temos um router dentro da rede.

Estas rotas podem ser consultadas no capítulo [#routes](#) do anexo.

#### **Active Directory (AD)**

O **Active Directory (AD)** é uma implementação de serviço de diretório no protocolo LDAP que armazena informações sobre objetos em rede de computadores

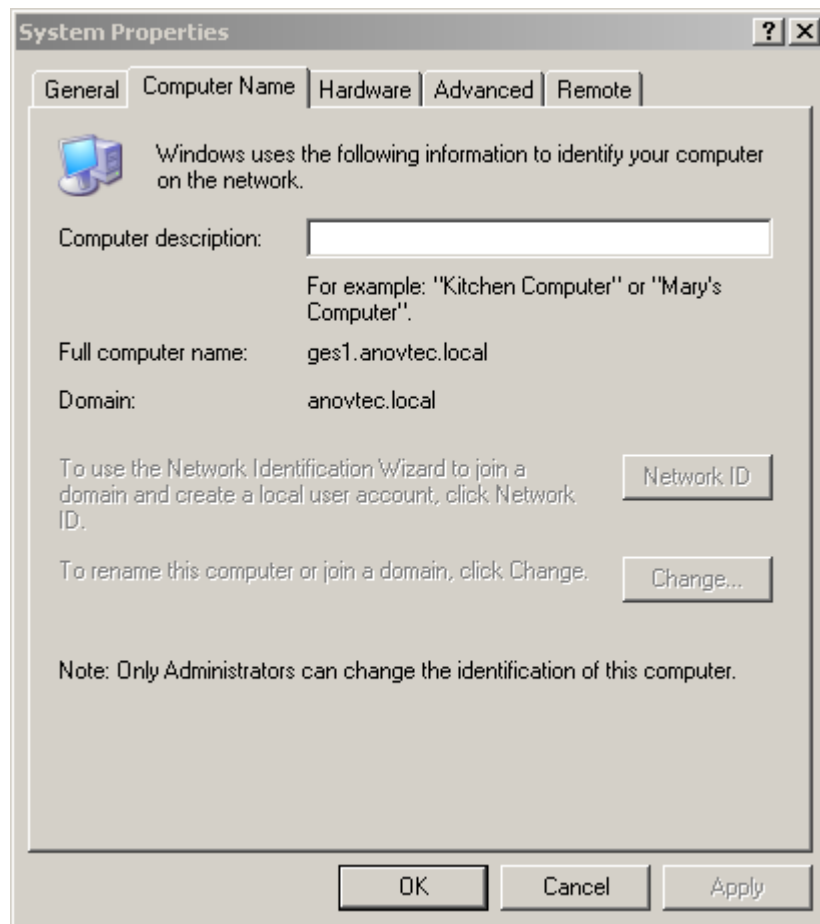
## Escola Superior de Tecnologia e Gestão de Águeda

e disponibiliza essas informações a usuários e administradores desta rede. É um software da Microsoft utilizado em ambientes Windows, presentes no active directory.

**Group Policy Object (GPO)** é um conjunto de regras que controlam o ambiente de trabalho de contas de utilizadores e contas de computador. Fornece a gestão e configuração centralizadas de sistemas operacionais, aplicativos e configurações dos utilizadores num ambiente Active Directory.

**Domain Controller (DC)**, é um servidor que responde a pedidos seguros de autenticação (login, verificação de permissões etc.) dentro de um domínio Windows. Um domínio é um conceito introduzido no Windows NT que permite que um utilizador possa ter acesso a uma série de recursos através de uma única combinação de nome de utilizador e senha.

Para a configuração do AD foi criado um domínio local com o nome “ANOVTEC.LOCAL”. Foram depois criados e adicionados ao domínio alguns utilizadores para testar as configurações.



*Figura 8 - Cliente logado com o domínio criado*

## DNS

O Domain Name System (DNS) é um sistema de gerenciamento de nomes hierárquico e distribuído para computadores, serviços ou qualquer recurso conectado à Internet ou numa rede privada. Permite associar um IP a um nome específico de forma a, por exemplo, facilitar o acesso a websites. Este tipo de servidor usa como porta padrão a 53.

Configurámos a resolução direta de endereços para o servidor de DNS da Google e a resolução inversa para o nosso servidor.

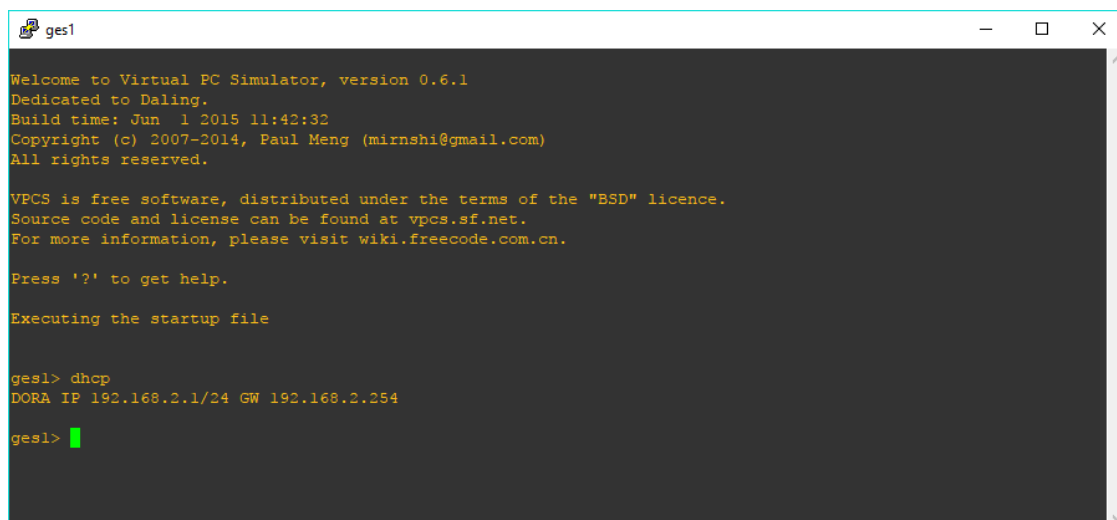
Testámos esta funcionalidade tentando aceder ao website [www.google.pt](http://www.google.pt) (com sucesso).

## Escola Superior de Tecnologia e Gestão de Águeda

### DHCP

O DHCP, Dynamic Host Configuration Protocol, é um protocolo de serviço TCP/IP que distribui automaticamente configurações de rede aos terminais que se liguem na rede. Este serviço oferece um endereço IP ao dispositivo, assim como máscara de rede, Default Gateway, servidor(es) de DNS, domínio de rede, entre outros serviços.

O DHCP foi configurado no router “Datacenter” na secção `#dhcp pools`. Foram criadas 3 pools (uma para cada departamento) cada uma delas foi atribuída à rede de cada departamento com a indicação do IP do servidor DNS, do gateway e de uma configuração deixar passar a configuração automática das proxy desde o servidor até aos clientes. Nesta **figura 9** podemos ver o pedido de DHCP feito a partir da máquina “ges1” ao router:



```
ges1
Welcome to Virtual PC Simulator, version 0.6.1
Dedicated to Daling.
Build time: Jun  1 2015 11:42:32
Copyright (c) 2007-2014, Paul Meng (mirnshi@gmail.com)
All rights reserved.

VPCS is free software, distributed under the terms of the "BSD" licence.
Source code and license can be found at vpcs.sf.net.
For more information, please visit wiki.freecode.com.cn.

Press '?' to get help.

Executing the startup file

ges1> dhcp
DORA IP 192.168.2.1/24 GW 192.168.2.254

ges1>
```

Figura 9 - Teste de DHCP

### NAT

NAT, Network Address Translation, também conhecido como *masquerading* é uma técnica que consiste em reescrever, utilizando-se de uma tabela hash, os endereços IP de origem de um pacote que passam por um router ou firewall de maneira que um computador de uma rede interna tenha acesso ao exterior ou Rede Mundial de Computadores (rede pública). Para isso no router utilizamos os comandos “ip nat outside” e “ip nat inside” na interface ligada à rede publica e às

## Escola Superior de Tecnologia e Gestão de Águeda

interfaces da rede interna, respetivamente. Ativou-se a NAT em modo overload recorrendo ao comando “ip nat inside source list 1 int f0/0 overload”.

### VPN

Uma VPN é uma conexão estabelecida sobre uma infraestrutura pública ou compartilhada, usando tecnologias de tunelamento e criptografia para manter seguros os dados trafegados. VPNs seguras usam protocolos de criptografia por tunelamento que fornecem a confidencialidade, autenticação e integridade necessárias para garantir a privacidade das comunicações requeridas. Alguns desses protocolos que são normalmente aplicados em uma VPN estão: L2TP, L2F, PPTP e o IPSec. Quando adequadamente implementados, estes protocolos podem assegurar comunicações seguras através de redes inseguras.

Foi necessária a criação e configuração de uma VPN para poder fornecer o acesso dos utilizadores ao interior da empresa a partir do exterior. Após alguns testes verificámos que a máquina que era ligada pela VPN não conseguia obter IP e por consequência aceder à rede da empresa. Resolvemos esta situação desativando o IP Forwarding do modo DHCP para uma pool específica (figura 10). Foi necessário efetuar um *port forwarding* na NAT do router da porta 1723 para permitir ligações VPN do exterior.



# Escola Superior de Tecnologia e Gestão de Águeda

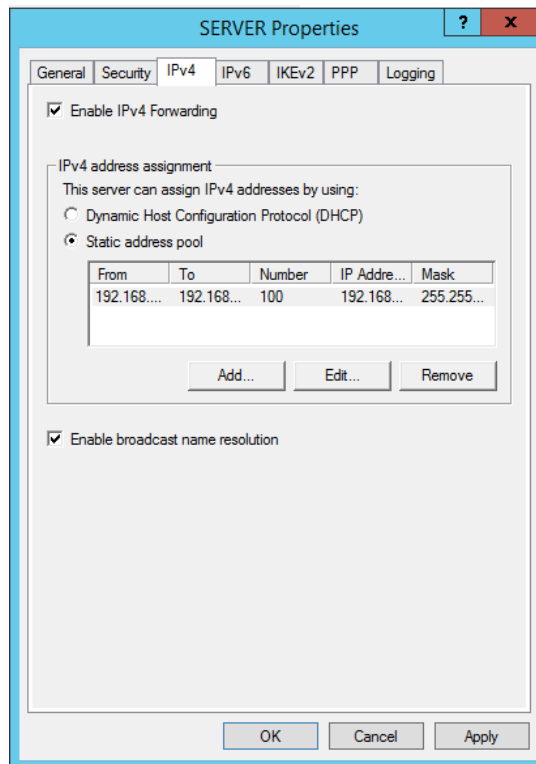


Figura 10 - Configuração de endereços estáticos para a VPN

Para testar a VPN, ligamos um PC a uma rede externa e configuramos uma nova ligação VPN, introduzindo os dados necessários (ip,username e password). Fizemos o respetivo login e verificámos a rede interna da empresa bem como os shares estavam acessíveis (figura 11).

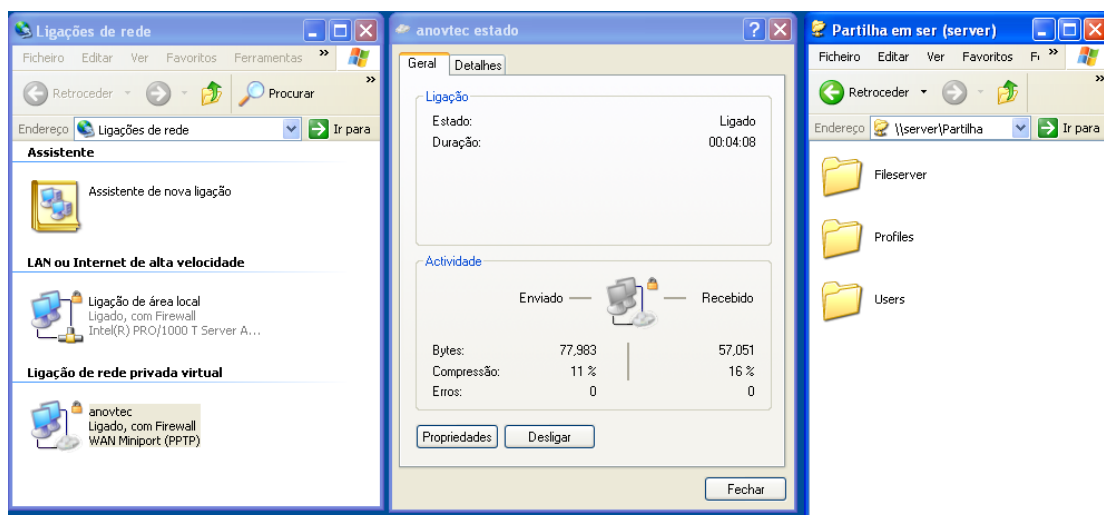


Figura 11 - Teste VPN no cliente

## Escola Superior de Tecnologia e Gestão de Águeda

### **Firewall**

Uma Firewall é um sistema de segurança implementado numa rede baseado em hardware ou software. Tem como objetivo monitorizar e controlar todo o tráfego de rede que entra e sai da rede. Ao configurarmos os diferentes serviços, as portas de Outbound e inbound, tanto TCP e UDP, necessárias para esses mesmo serviços eram configuradas automaticamente pelo Windows server.

Para testar esta configuração, realizámos o envio de tráfego de cada tipo de serviço pelas diferentes portas a partir de um pc de testes dentro de um dos departamentos para o exterior, para o protocolo WEB, e verificámos que a comunicação era executada com sucesso. Para testar a VPN, removemos a cloud ligado ao router e ligámos lá uma VM com um IP de gama pública e entrámos na rede pela VPN.

### **Proxy**

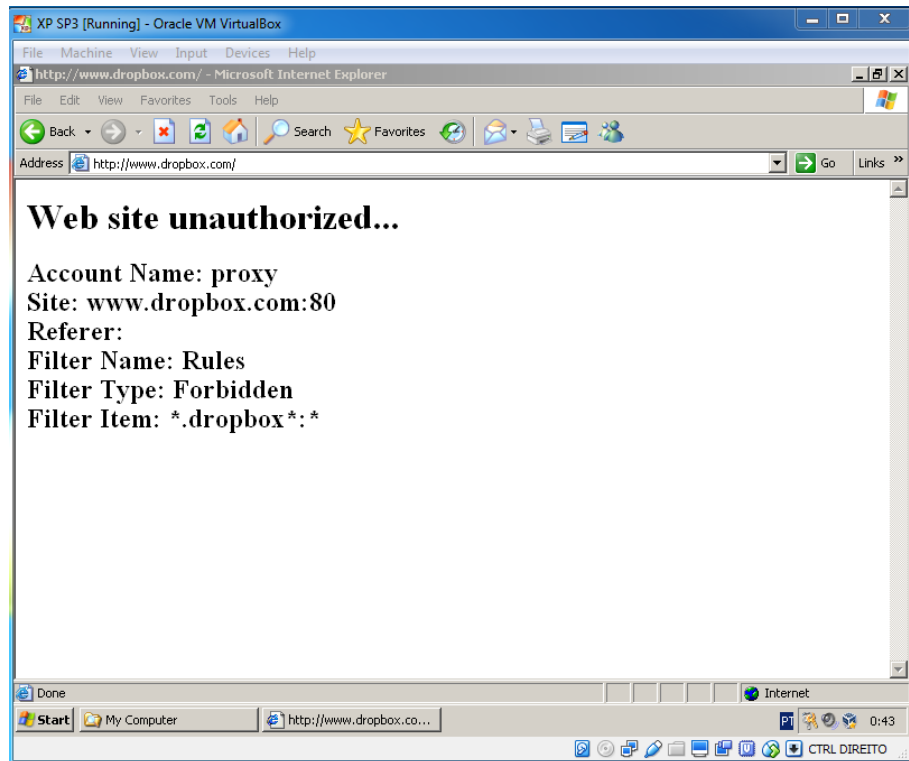
**Proxy** é um servidor que desempenha a função base de servir como intermediário dos pedidos dos clientes, para outros servidores. Para o projeto, utilizamos a proxy, para gestão dos acessos a certos sites, num determinado horário. Para a realização destas operações recorremos a um software para uma melhor gestão do mesmo (CCProxy).

Para a implementação da proxy, tivemos de configurar um ficheiro “wpad.dat” no servidor web (IIS), no servidor web, também tivemos de configurar um MIME TYPE, para ser possível aceder aquele tipo de ficheiro por “http”, para os clientes fazer o download do ficheiro de configuração do proxy, para com isto ser configurado automaticamente nas máquinas. Para além do servidor de web, tivemos de configurar o DHCP para a opção 252 (a opção 252 do DHCP server para mandar as configurações automáticas do proxy).

Na configuração de DNS, também se teve de configurar um “new host (A)”, com um nome wpad, também se teve de configurar o AD (Active Directory ), para atribuir automaticamente as configurações da proxy ao Internet Explorer.

## Escola Superior de Tecnologia e Gestão de Águeda

Nesta **figura 12**, podemos ver que o servidor não consegue aceder ao website “[www.dropbox.com](http://www.dropbox.com)” devido às configurações da proxy. No entanto, consegue aceder a outros sites como por exemplo “[www.apple.com](http://www.apple.com)”:



*Figura 12 - Teste da proxy*

Na **figura 13**, podemos ver os diferentes sites ( facebook, dropbox, gmail, youtube, doodle ) que foram bloqueados e como se procede para fazer essa configuração.

## Escola Superior de Tecnologia e Gestão de Águeda

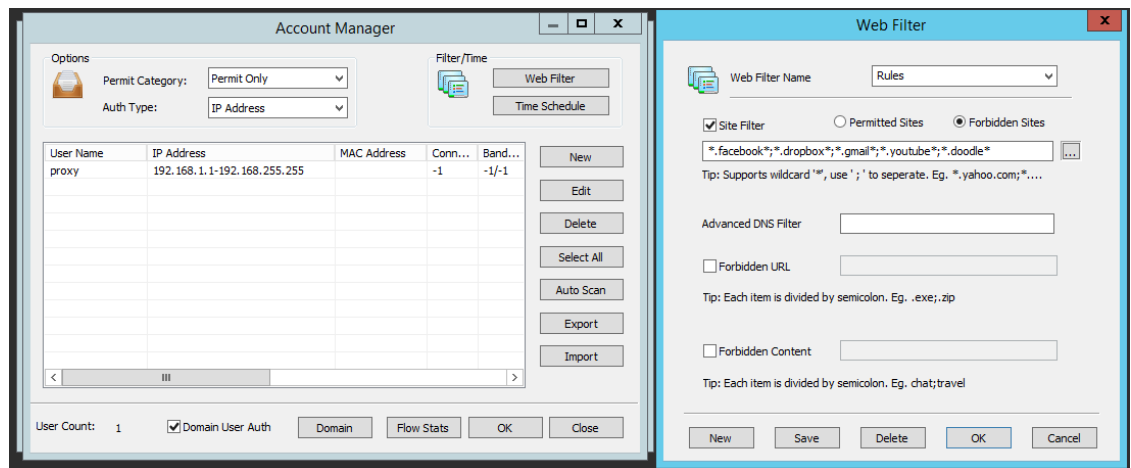


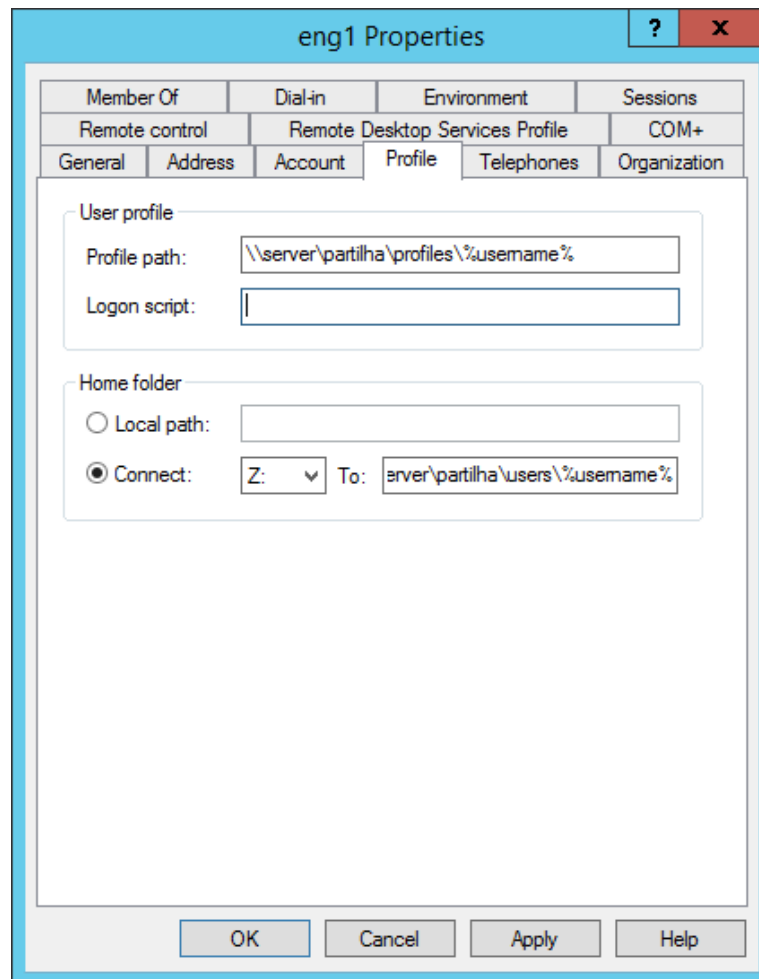
Figura 13 - CCProxy WebFilter

### FileServer

Um fileserver é um servidor de ficheiros localizado normalmente numa NAS (Network Attached Storage) que serve para fornecer o acesso partilhado de ficheiros e dados entre os diferentes computadores ligados à rede interna.

Para este projeto, foi necessário criar um fileserver local (a simular um NAS) para poder armazenar os perfis de cada um dos utilizadores, que inclui todos os documentos, imagens, ficheiros, configurações, ambiente de trabalho, entre outros, de cada utilizador.

Para isso criámos uma pasta chamada “Partilha” que foi partilhada e atribuídas permissões aos utilizadores do domínio. A partir daí foram criadas 3 subpastas: Fileserver como o share público, “Profiles” para armazenar os perfis dos utilizadores e “Users” como uma pasta pessoal. A partir daí fomos à parte das configurações dos utilizadores no AD e definimos o “profile path” e o “home folder” como está apresentado na figura 14

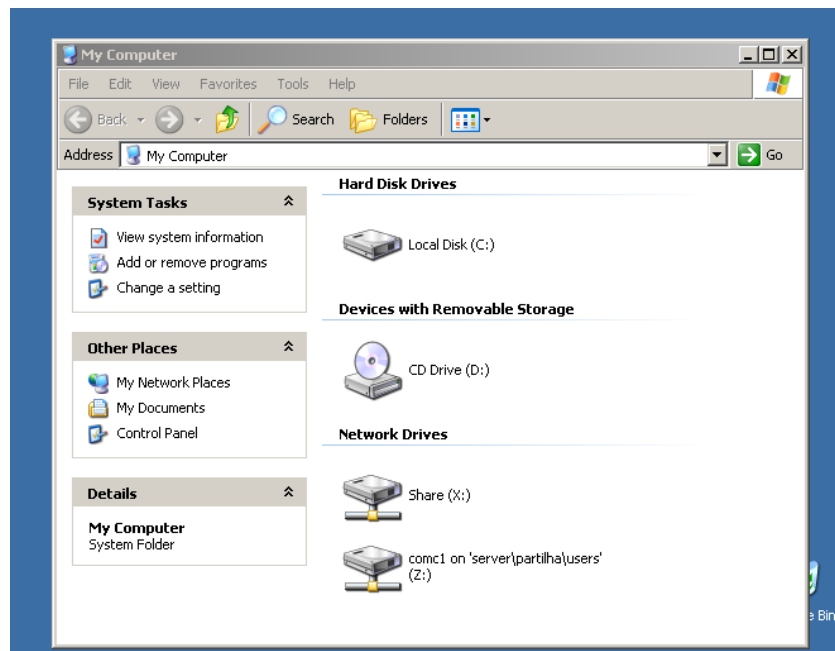


*Figura 14 - Configurações das partilhas dos utilizadores*

Para testar, adicionamos um PC ao GNS3 com Windows XP e entramos com um utilizador registado no domínio, verificando que todos os dados foram restabelecidos com sucesso.

Para testar o Servidor de ficheiros acedemos de um PC dentro da rede interna à pasta pessoal (drive Z:) e à pasta de acesso geral (drive X: denominada “share”) do utilizador que efetuou o login nesse PC. Esta operação foi também efetuada com sucesso.

## Escola Superior de Tecnologia e Gestão de Águeda



*Figura 15 - Drives partilhadas com cada utilizador*

### **WebServer**

Um WebServer é um servidor que tem como objetivo hospedar um ou mais websites.

Para a criação deste servidor, utilizámos o serviço IIS integrado no Windows Server e abrimos a porta 80 e 443 realizado o *port forwarding* na NAT do router para permitir o acesso ao site a partir do exterior. No servidor hospedámos o website geral do IIS (que poderá ser depois substituído pelo website da empresa ANOVTEC) e o ficheiro wpad, na tentativa de conseguirmos fazer a configuração automática do proxy.

## Escola Superior de Tecnologia e Gestão de Águeda

### 3.5. Erros / Problemas / Observações

Devido a não ser possível a virtualização/implementação de um AP (Access Point), por não ser suportada pelo GNS3, não conseguimos arranjar uma solução para este problema, mas como alternativa utilizamos um router para “fingir” de AP.

A configuração do proxy nos clientes de forma automática foi uma tarefa bastante penosa. Desde usarmos uma técnica chamada autoproxy do CCProxy, ao envio das configurações por DHCP usando o código 252 ou até mesmo pelo DNS com um ficheiro alojado no Webserver, os clientes nunca assumiram as definições de forma automática. A forma de contornar esta situação foi configurar as definições do browser dos clientes (Internet Explorer) na AD, fazendo com que essa configuração passasse a ser transparente para os clientes.

De salientar ainda a VPN no qual tivemos algumas dificuldades com a obtenção de IP, descritas anteriormente e resolvidas aquando da abordagem desse tema.

De referir que inicialmente, os utilizadores do departamento cablado comercial serem denominados com1, com2, com3, etc geraram problemas na criação dos perfis pelo facto de serem nomes reservados pelo sistema Windows. Os mesmos foram renomeados para comc1, comc2, comc3, etc.

Inicialmente, tivemos algum problema em trabalhar com o GNS3 (acesso à internet a partir de uma cloud, acesso entre dispositivos, entre outros) mas com a realização do trabalho prático da disciplina de redes, estas dificuldades foram bastante amenizadas.

A máquina virtual com Windows XP, usada para testes teve de sofrer algumas alterações para ser compatível com o ambiente GNS3. O network adapter foi alterado para Generic Driver (UDP tunnel) e o tipo foi alterado para Intel PRO/1000 T Server. Dessa forma o Windows conseguiu detetar e instalar os drivers necessários e a máquina em causa conseguiu comunicar com o server e com a respetiva rede interna.

Por fim, para realizar testes dentro da rede doméstica onde estava localizado o projeto, alterámos a rede para as mesmas definições da UA (Gateway 192.168.229.254 e IP de clientes dentro dessa rede).



## **Escola Superior de Tecnologia e Gestão de Águeda**



## Escola Superior de Tecnologia e Gestão de Águeda

### 4. CONCLUSÃO

Com este trabalho, tivemos a oportunidade de criar uma rede adequada a uma empresa com certas necessidades, o qual nos fez ver a importância de uma rede bem estruturada numa empresa. Contudo, ao fazermos o primeiro esboço da rede, encontramos alguns problemas evidentes. Um desses problemas foi a performance dos computadores que nos foram disponibilizados para o desenvolvimento deste projeto, sendo que não conseguimos instalar diversos softwares essenciais para a criação do mesmo. Esta situação provocou um atraso considerável no desenvolvimento do trabalho, obrigando-nos a repensar certas decisões feitas anteriormente quanto à configuração da rede. Face a este problema, optámos por usar o GNS3 e emular o servidor principal num computador pessoal.

Após a resolução deste problema, configuramos a nossa rede no software GNS3, configuramos os routers usados e emulamos o servidor e os clientes, com o sistema operativo Windows Server 2012 e o Windows XP, respetivamente, usando o software VirtualBox.

Por fim, ativamos os serviços necessários no servidor e efetuamos as respetivas configurações.



## **Escola Superior de Tecnologia e Gestão de Águeda**



## 5. FONTES E MATERIAL DE REFERÊNCIA

- (1) <https://pplware.sapo.pt/microsoft/windows/redes-vamos-conhecer-melhor-o-servico-dhcp/>
- (2) [https://pt.wikipedia.org/wiki/Domain\\_Name\\_System](https://pt.wikipedia.org/wiki/Domain_Name_System)
- (3) [https://pt.wikipedia.org/wiki/Network\\_address\\_translation](https://pt.wikipedia.org/wiki/Network_address_translation)
- (4) <https://findproxyforurl.com/deploying-wpad>
- (5) Enunciado Trabalho de PTRC 2017



## **Escola Superior de Tecnologia e Gestão de Águeda**

## 6. ANEXOS

### Configurações dos Router usados:

#DATACENTER

conf t

#routes

ip route 0.0.0.0 0.0.0.0 192.168.229.254

ip route 192.168.5.0 255.255.255.0 f1/3

#NAT ACLs

access-list 1 deny 192.168.5.0 0.0.0.255

access-list 1 permit any

ip nat inside source list 1 int f0/0 overload

#Port FW

ip nat inside source static tcp 192.168.1.1 80 192.168.229.204 80 extendable

ip nat inside source static tcp 192.168.1.1 443 192.168.229.204 443 extendable

ip nat inside source static tcp 192.168.1.1 1723 192.168.229.204 1723 extendable

ip nat inside source static tcp 192.168.1.1 3389 192.168.229.204 3389 extendable

#Interfaces

int f0/0

no sh

ip add 192.168.229.204 255.255.255.0

ip nat out



## Escola Superior de Tecnologia e Gestão de Águeda

exit

int f0/1

no sh

ip add 192.168.1.254 255.255.255.0

ip nat in

ip access-group 1 out

exit

int f1/1

no sh

no switchport

ip add 192.168.2.254 255.255.255.0

ip nat in

ip access-group 1 out

exit

int f1/2

no sh

no switchport

ip add 192.168.3.254 255.255.255.0

ip nat in

ip access-group 1 out

exit



## Escola Superior de Tecnologia e Gestão de Águeda

```
int f1/3
```

```
no sh
```

```
no switchport
```

```
ip add 192.168.4.254 255.255.255.0
```

```
ip nat in
```

```
end
```

```
# dhcp pools
```

```
conf t
```

```
ip dhcp pool ges
```

```
network 192.168.2.0 255.255.255.0
```

```
default-router 192.168.2.254
```

```
dns-server 192.168.1.1
```

```
option 252 ascii "http://192.168.1.1:808/wpad.dat "
```

```
exit
```

```
ip dhcp pool eng
```

```
network 192.168.3.0 255.255.255.0
```

```
default-router 192.168.3.254
```

```
dns-server 192.168.1.1
```

```
option 252 ascii "http://192.168.1.1:808/wpad.dat "
```

```
exit
```



## Escola Superior de Tecnologia e Gestão de Águeda

ip dhcp pool com

network 192.168.4.0 255.255.255.0

default-router 192.168.4.254

dns-server 192.168.1.1

option 252 ascii "http://192.168.1.1:808/wpad.dat "

exit

ip dhcp pool comwifi

network 192.168.5.0 255.255.255.0

default-router 192.168.5.254

dns-server 192.168.1.1

option 252 ascii "http://192.168.1.1:808/wpad.dat "

exit

end

wr

#####

#AP

conf t

ip route 0.0.0.0 0.0.0.0 192.168.4.254

int f0/0

no sh

ip add 192.168.4.253 255.255.255.0

exit





## Escola Superior de Tecnologia e Gestão de Águeda

```
int f0/1
```

```
no sh
```

```
ip add 192.168.5.254 255.255.255.0
```

```
ip helper-address 192.168.4.254
```

```
end
```

```
wr
```