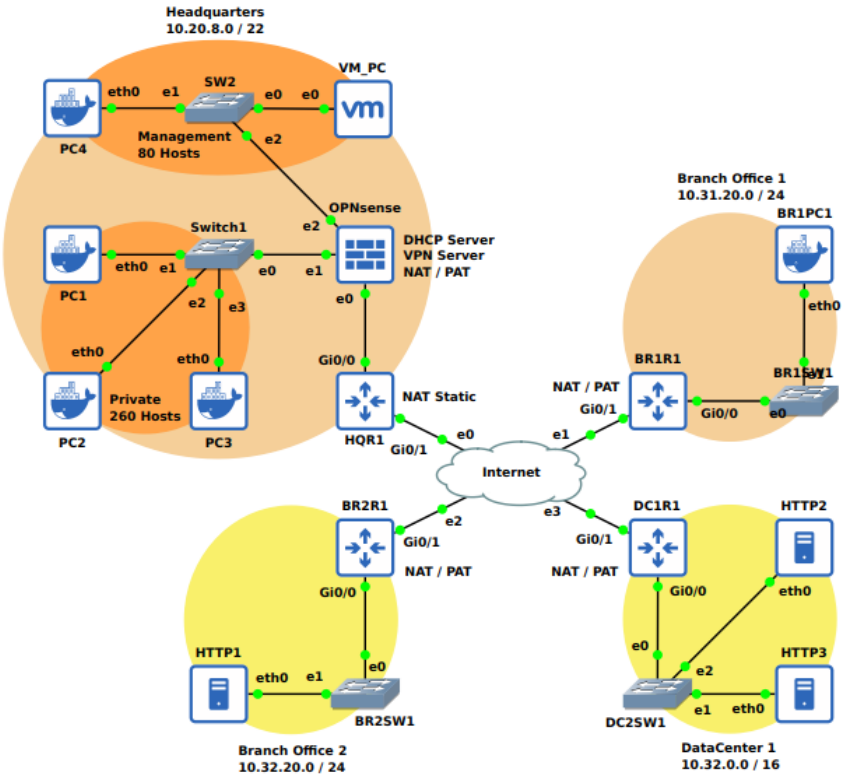
**Universidade Fernando Pessoa**

*Redes de Computadores 2*

*Trabalho Prático – Parte 1*




# Redes de Computadores 2

**Pedro Sobral**
pmsobral@ufp.edu.pt

**Bruno Gomes**
bagomes@ufp.edu.pt

## Março de 2023

## Universidade Fernando Pessoa

**Faculdade de Ciências e Tecnologias**

## Objectivo:

Fase 1 - Configuração de encaminhamento estático, DHCP, ACLs, NAT e serviços no contexto de uma empresa de e-commerce.

## 1. Definição do problema

No âmbito de uma empresa de e-commerce é proposta a topologia de rede representada na figura 1. Quatro *sites* distintos e interligados devem ser considerados: **H**ead**Q**uarters; **Br**anch Office **1 e 2** e **D**ata**C**enter. PC1 - 4, BR1PC1 e HTTP1 - 3 são contentores Docker (netutils), os router HQR1, BR1R1, BR2R1 e DC1R1 deverão ter a imagem IOSvL3. OPNsense [3] e VM_PC (uma qualquer VM com interface gráfica) são máquinas virtuais a importar para a GNS3.

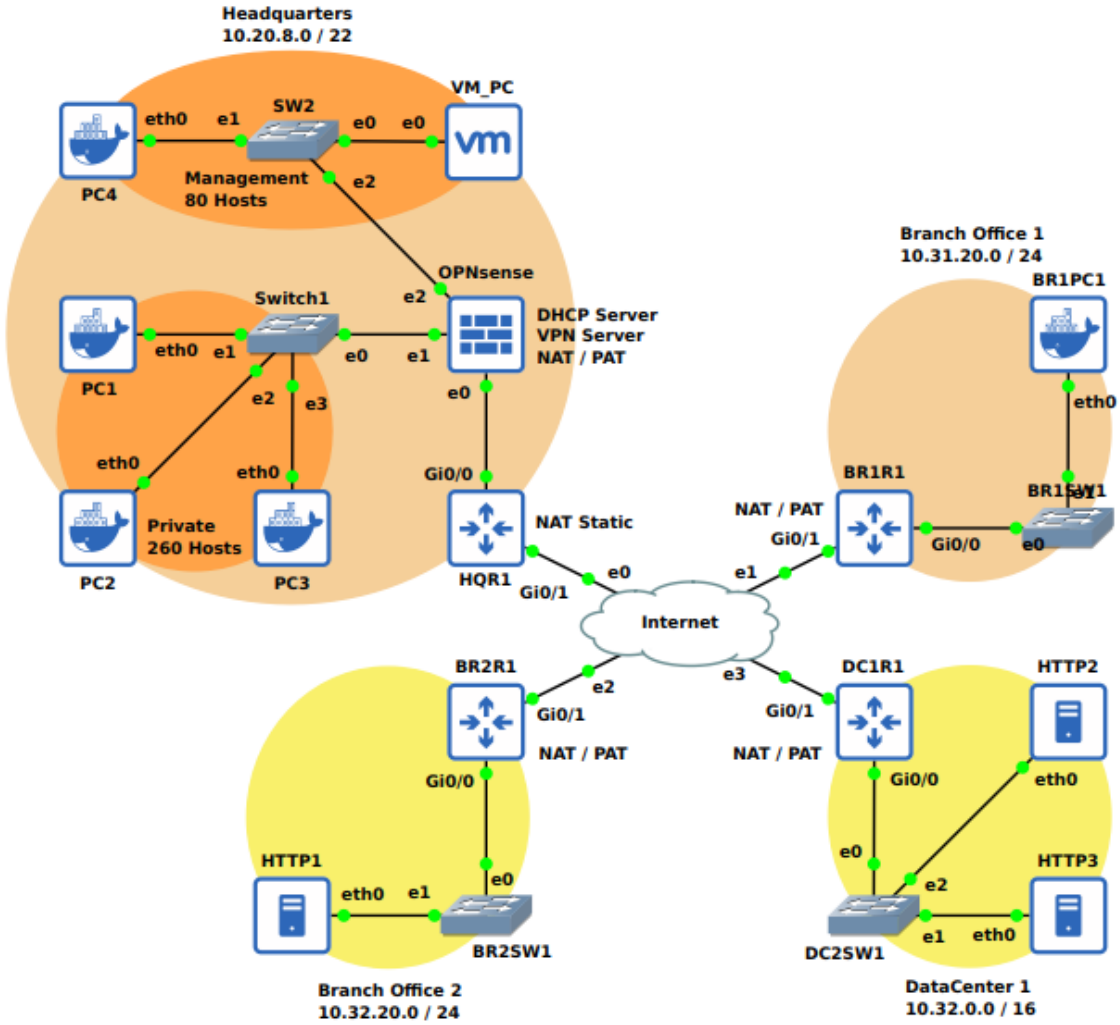



*Figura 1 - Topologia fase 1*

**HeadQuarters (HQ)**

Representando a rede interna da sede/centro administrativo da empresa, HQ deverá ser configurado tendo em vista a utilização de máscaras de rede de tamanho variável (VLSM), partindo do IP de rede 10.20.8.0 / 22. Um total de 2 subnets distintas devem ser consideradas:

- Management (80 hosts), destinada a equipamentos conectados para fins de gestão de rede e administração de dispositivos e recursos de rede;
- Main (260 hosts), correspondente à subnet principal da empresa, onde todos os dispositivos cliente (e. g. Desktops, Dispositivos Móveis, impressoras, etc) deverão ser mantidos (excluindo convidados ou máquinas da rede management);

Nota: deverão ser atribuídas aos router e servidores, respetivamente, os primeiros e últimos IP válidos da sub rede em que se encontram inseridos. A regra deverá ser aplicada a todos os *sites* considerados na topologia.

HQR1 deverá funcionar como porta de saída dos HQ para a internet. Este router terá de ser configurado com NAT estático na interface g0/1..

HQR2 / OPNsense será configurado como servidor DHCP. Paralelamente deverá implementar as seguintes regras nas suas listas de acesso:

- permitir tráfego entre Main e Management, apenas quando iniciado em Management
- Bloquear acesso aos servidores HTTP (porta 80) do data center 1 a partir da subnet Main
- Permitir a VM_PC e só a VM_PC aceder a HQR1 via telnet

Para além de controlar acessos e servir DHCP, o HQR2 / OPNsense, deverá estar configurado para fazer NAT / PAT na interface e0 e disponibilizar serviço de VPN “a pedido”

**Branch Office 1 (BR1)**

Representa um branch office da empresa. BR1R1 terá de ser configurado para fazer NAT / PAT na interface g0/1. Deverá ser instalado em BR1PC1 um cliente VPN para ligação ao servidor configurado nos HQ.

**Branch Office 2 (BR2)**

Representa um segundo branch office da empresa. Este branch office conta com um servidor HTTP que deverá estar acessível apenas localmente ou a pedidos originados em HQ. BR2R1 ficará responsável por fazer NAT / PAT na interface g0/1.

**Data Centers (DC1)**

Apresenta uma visão simplificada de um datacenter web. DC1R1 deverá ser configurado para fazer NAT / PAT na interface g0/1 garantindo que os servidores HTTP2 e HTTP3 se encontram disponíveis através da internet (*Port Forwarding*).

Não estando considerados, para esta primeira fase, protocolos de encaminhamento dinâmico, a componente de internet é apenas figurativa, mantendo os router ligações diretas entre si (i. e. a "internet" poderá ser representada por um ethernet switch). Os IP a atribuir serão os representados na tabela 1.

| Router | Interface | IP | Máscara |
|---|---|---|---|
| HQR1 | G0/1 | 209.162.12.1 | 255.255.255.248 |
| BR1R1 | G0/1 | 209.162.12.2 | 255.255.255.248 |
| BR2R1 | G0/1 | 209.162.12.3 | 255.255.255.248 |
| DC1R1 | G0/1 | 209.162.12.4 | 255.255.255.248 |

*Tabela 1 - Configuração IP HQR1, BR1R1, DC1R1 e DC2R1*

## 2. Requisitos

**Fase 1 (50%)**

A. (10 %) Configuração VLSM para os HQ e encaminhamento estático com sumarização de rotas, sempre que aplicável;
B. (25 %) Configuração DHCP para Head Quarters;
    a. Configurar HQR2 / OPNsense como servidor DHCP
    b. Um ataque de DHCP starvation [2] deverá ser implementado e iniciado por um dos PCs da rede main
    c. Configurar em HQR2 / OPNsense, técnicas para prevenir o referido ataque de negação de serviço

    **Nota**: A utilização de um Router HQR2 ao invés do OPNsense limita a cotação máxima do requisito a 60%

C. (20 %) Configuração de todas as ACL descritas, direta ou indiretamente, na definição do problema;
D. (20 %) Configurações NAT em todos os *sites;*
E. (25 %) Configuração de todos os serviços presentes na topologia (i. e. Servidor VPN, servidores HTTP) assim como os devidos clientes/ferramentas necessários à validação das configurações (e. g. openvpn client, wget, Curl, telnet, nping, ssh, etc). Com exceção de OPNsense [3] e HQ_VM (uma qualquer VM com interface gráfica), deverão ser utilizados containers Docker [1] para cada um destes serviços e clientes.

## 3. Notas

Este trabalho será realizado individualmente ou em grupos de dois alunos. O *portable* do projeto tem de ser submetido até à data indicada no sistema de elearning (trabalhos) e será apresentado e defendido de "viva voz" em data a designar pelo docente.

Mais do que a correta configuração dos protocolos/requisitos propostos, a avaliação refletirá o domínio apresentado pelo aluno em cada um dos pontos, assim como a correta demonstração (i. e. utilização de ferramentas de teste) da sua operação.

## 4. Bibliografia


[1] *GNS3 Documentation.* Create a docker container for GNS3 - https://docs.gns3.com/docs/emulators/create-a-docker-container-for-gns3/

[2] DHCP Starvation Attack using Python - https://kavigihan.medium.com/dhcp-starvation-attack-using-python-ab2f49c2d558

[3] OPNsense - https://opnsense.org/