

Instituto Superior de Engenharia De Lisboa

Licenciatura em Engenharia Informática e Multimédia

Redes de Computadores – 2024/2025 SV

4ª Fase – Deploy Services

Docente: Nuno Garcia

Realizado pelo grupo NG-16:

Carolina Raposo n.º 51568

Carlos Simões n.º 51696

Lara Camões n.º 51742

Lisboa, 06 de junho de 2025

Índice

1. Introdução	2
2. Phase 4 – Deploy Services	3
2.1 DHCP, DNS e HTTP	3
2.2 Configuração do servidor DHCP	4
2.3 Configuração do servidor DNS.....	5
2.4 Configuração do DHCP <i>Relay Agent</i>	5
2.5 Configuração dos dispositivos em cada LAN	6
2.6 Testes finais	6
2.6.1 Teste da configuração do DNS.....	6
2.6.2 Teste da configuração do DHCP	7
2.6.3 Teste do servidor web	7
2.6.4 Teste final utilizando ARP e traceroute	8
3. Conclusão	9
4. Referências	9

Índice de Figuras

Figura 1 - Esquema da ligação entre redes.....	3
Figura 2 - Output do ping do PC0 para o servidor DNS	6
Figura 3 - Output do ipconfig do PC0 após fazer ipconfig /release	7
Figura 4 - Output do ipconfig do PC0 após fazer ipconfig /renew	7
Figura 5 - Output da Web Browser App	7
Figura 6 - Output da tabela ARP do ponto 3	8
Figura 7 - Output da tabela ARP do ponto 5.....	8
Figura 8 - Traceroute do PC1 para o servidor DHCP	8

Índice de tabelas

Tabela 1 - Valores atribuídos a cada pool.....	4
--	---

1. Introdução

O presente relatório descreve as atividades realizadas no Fase 4 do projeto da unidade curricular de Redes de Computadores. Este projeto, estruturado em quatro fases de complexidade crescente, tem como objetivo principal a construção de uma rede corporativa funcional, desde a implementação de servidor *web* até à configuração de uma infraestrutura de rede típica.

Na Fase 4, concentramo-nos na implementação e configuração de serviços de redes essenciais, nomeadamente DHCP, DNS e um servidor *web*, utilizando o simulador Cisco Packet Tracer. O objetivo principal foi garantir que os utilizadores das LANs A e B recebam configurações de rede automáticas via DHCP, acedam ao servidor *web* através do nome do domínio www.company.com com suporte DNS, e que todos os serviços estejam plenamente operacionais. Para tal, foram realizadas configurações adicionais nos servidores da LAN Server e nos dispositivos de rede, incluindo ajustes em *routers* para suportar a funcionalidade dos serviços.

A metodologia adotada incluiu a configuração detalhada de pools DHCP específicas para cada LAN, a criação de registos DNS no servidor dedicado, e a implementação de um DHCP Relay Agent no router R1 para garantir a comunicação entre sub-redes. Para validação, foram executados testes rigorosos, como a verificação da atribuição automática de IPs, a resolução de nomes através de *ping* ao domínio www.company.com, e o acesso ao conteúdo alojado no servidor web. Os resultados obtidos confirmaram não apenas a funcionalidade individual de cada serviço, mas também a sua integração harmoniosa na rede global, cumprindo integralmente os requisitos definidos no enunciado.

2. Phase 4 – Deploy Services

Como referido anteriormente, esta fase do projeto consiste em configurar os serviços de DHCP, DNS e Web Server na rede construída, de forma a torná-la mais realista. O objetivo é que os dispositivos das LANs A e B obtenham automaticamente as suas configurações de rede e consigam aceder ao servidor web através do nome www.company.com. Para isso, é necessário ajustar as configurações dos servidores e dos restantes dispositivos de rede, garantindo o correto funcionamento dos serviços e a conectividade entre todos os elementos.

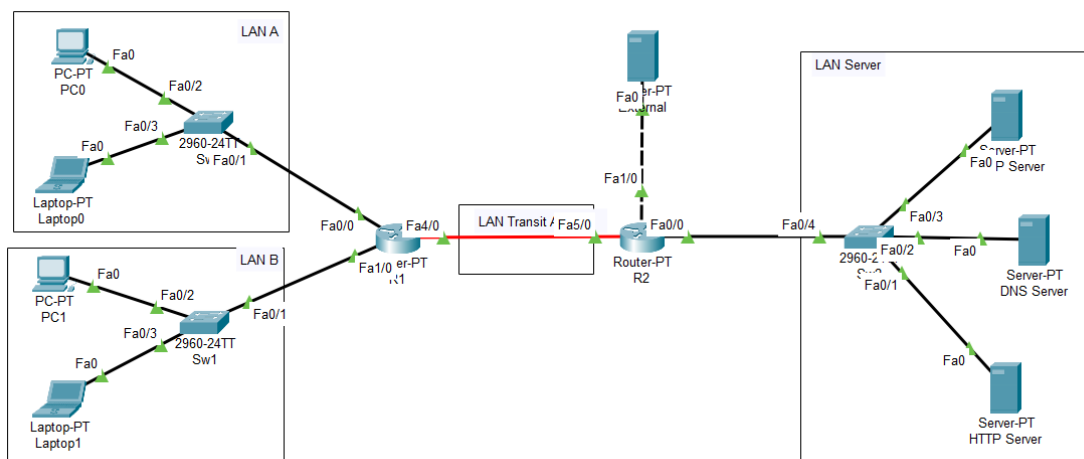


Figura 1 – Esquema da ligação entre redes

2.1 DHCP, DNS e HTTP

O DHCP é um protocolo da camada de aplicação do modelo TCP/IP utilizado para atribuir endereços IP dinamicamente a dispositivos numa rede. Este permite que um dispositivo obtenha automaticamente, para além do IP:

- *Subnet Mask*;
- *Default gateway*;
- Servidor DNS.

O DHCP funciona da seguinte maneira:

1. DHCP DISCOVER: o cliente envia uma mensagem *broadcast* à rede à procura de um servidor DHCP disponível;
2. DHCP OFFER: um servidor DHCP responde com uma oferta, isto é, uma mensagem que contém um endereço IP disponível e outros parâmetros de configuração de rede, mencionados em cima;
3. DHCP REQUEST: o cliente envia uma mensagem de solicitação, indicando que aceita a oferta daquele servidor DHCP específico;
4. DHCP ACKNOWLEDGEMENT: o servidor confirma a atribuição com uma mensagem de ACK, finalizando o processo.

Para além de se ter de saber o que é o DHCP e como funciona, foi necessário também ter noção do que é o DNS e HTTP.

O DNS – *Domain Name System* – é um protocolo utilizado para traduzir nomes de domínio legíveis por humanos em endereços IP que os dispositivos utilizam para comunicar entre si. Sem o DNS, os utilizadores teriam de memorizar os endereços IP de todos os servidores que desejam aceder, o que seria impraticável.

O funcionamento do DNS é baseado numa hierarquia de servidores que cooperam entre si para resolver nomes. Quando um cliente necessita de aceder a um determinado domínio, envia um pedido de resolução ao servidor DNS configurado. Esse servidor pode já ter a resposta na sua *cache*, ou reenviar o pedido a outros servidores DNS até encontrar o IP correspondente.

Por fim e para recordar, o HTTP, que já foi necessário para a primeira parte do projeto, é o protocolo responsável pela comunicação entre clientes e servidores web, permitindo a transferência de páginas e conteúdos. Cada pedido HTTP é independente (sem estado) e inclui informação como o método (ex: *GET*), o caminho do recurso, e os cabeçalhos associados. A resposta inclui o conteúdo solicitado e um código de estado que indica o resultado da operação (ex: *200 OK, 404 Not Found*).

2.2 Configuração do servidor DHCP

Como já foi referido, um servidor DHCP distribui automaticamente endereços IP a dispositivos numa rede. No contexto do projeto, o servidor vai distribuir os IPs pela LAN A e LAN B, e para isso, foi necessário definir uma *pool* de endereços no mesmo para cada LAN.

Uma *pool* de endereços é um intervalo de endereços IP definido no servidor DHCP, a partir do qual este pode atribuir dinamicamente configurações de rede aos dispositivos clientes. Definir uma pool específica para cada LAN é essencial porque permite ao servidor distribuir endereços válidos e compatíveis com a sub-rede correspondente, evitando conflitos e garantindo que cada dispositivo recebe parâmetros corretos, como o IP, *subnet mask*, *gateway* e DNS. Esta separação por LAN assegura que os dispositivos conseguem comunicar eficazmente dentro da rede e com outras redes externas.

As *pools* foram definidas a partir das informações obtidas da fase anterior:

Sub-rede	LAN A	LAN B
Nome da <i>pool</i>	LAN_A_Pool	LAN_B_Pool
<i>Default Gateway</i>	10.0.16.30	10.0.16.46
Servidor DNS	10.0.16.130	10.0.16.130
Endereço IP inicial	10.0.16.1	10.0.16.33
<i>Subnet Mask</i>	255.255.255.224 (/27)	255.255.255.240 (/28)
Número máximo de utilizadores	20	10

Tabela 1 - Valores atribuídos a cada *pool*

O que significa cada informação de cada *pool*?

- *Default gateway* – interface do router R1 onde cada LAN está ligada;
- Servidor DNS – endereço IP do servidor DNS existente na rede;
- Endereço IP inicial – primeiro endereço IP endereçável (utilizável) numa LAN;
- *Subnet Mask* – define os limites da sub-rede e permite identificar os endereços IP válidos dentro dessa rede.

2.3 Configuração do servidor DNS

Para o correto funcionamento do servidor DNS, foi definido no mesmo:

- Nome: www.company.com;
- Endereço: 10.0.16.131 -> endereço IP do servidor HTTP;
- *Type*: A.

O servidor foi assim configurado de forma a permitir que os dispositivos na rede possam aceder ao servidor *web* usando um nome de domínio em vez de um endereço IP. O tipo A (***Address Record***) indica que se trata de um registo que associa um nome de domínio a um endereço IPv4. Esta configuração facilita a navegação na rede, tornando o acesso ao site mais intuitivo para os utilizadores.

Não foi necessário configurar o servidor HTTP pois o mesmo já se encontrava implementado.

2.4 Configuração do DHCP *Relay Agent*

Só com estas configurações, a atribuição de IPs por parte do servidor DHCP ainda não estava completamente funcional. Então, foi necessário recorrer à configuração de um ***DHCP Relay Agent***.

O DHCP ***Relay Agent*** é uma componente de rede responsável por encaminhar mensagens do protocolo DHCP entre clientes e servidores que se encontram em sub-redes diferentes. Como o protocolo DHCP utiliza mensagens *broadcast* para a descoberta e atribuição de endereços IP, estas mensagens não atravessam normalmente os routers entre sub-redes distintas. O DHCP ***Relay Agent*** atua, portanto, recebendo estas mensagens *broadcast* dos clientes numa sub-rede e encaminhando-as, sob a forma de ***unicast*** (comunicação direta entre um emissor e um destinatário específico numa rede, onde a mensagem é enviada apenas para esse único dispositivo), para um servidor DHCP localizado noutra sub-rede. Desta forma, permite centralizar a gestão dos endereços IP e outras configurações de rede, evitando a necessidade de instalar um servidor DHCP em cada sub-rede.

Como o router R1 é o dispositivo onde as LANs A e B estão conectadas, foi necessário configurar, via CLI, cada interface associada a essas redes, utilizando o seguinte comando:

- `ip helper-address 10.0.16.129` - este comando transforma uma mensagem DHCP *broadcast* recebida numa interface em ***unicast*** para o endereço especificado, neste caso, 10.0.16.129, que é o IP do servidor DHCP, funcionando assim como um DHCP Relay Agent.

2.5 Configuração dos dispositivos em cada LAN

Com as configurações feitas anteriormente, foi, por fim, necessário definir cada dispositivo para obter um endereço IP como DHCP, deixando de ser *static*. Após fazer essa configuração, no CMD de cada dispositivo, foram feitos os seguintes comandos:

- `ipconfig /release` – este comando liberta o endereço IP atual atribuído à interface de rede. Ao executá-lo, o dispositivo deixa de ter um IP concedido, ficando temporariamente sem conectividade na rede até receber um novo;
- `ipconfig /renew` – este comando solicita um novo endereço IP ao servidor DHCP. Pode ser usado a seguir ao */release* para obter uma nova configuração de rede ou para forçar a renovação do IP atual.

Após fazer estas configurações, percebeu-se que de facto, cada dispositivo em cada LAN, obteve o seu próprio endereço IP a partir do servidor DHCP.

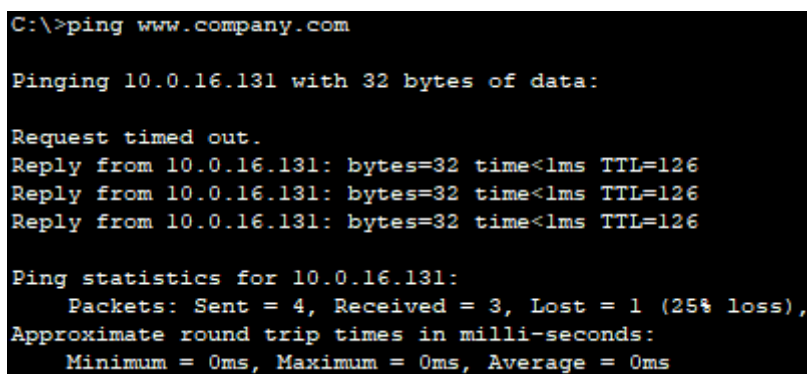
2.6 Testes finais

Com tudo já configurado, fizeram-se testes para verificar se a rede está corretamente implementada.

2.6.1 Teste da configuração do DNS

Foi feito a partir do PC0 (poderia ser de qualquer *host* de cada LAN) um *ping* para o nome do servidor web www.company.com, ou seja:

- `ping www.company.com`



```
C:\>ping www.company.com

Pinging 10.0.16.131 with 32 bytes of data:

Request timed out.
Reply from 10.0.16.131: bytes=32 time<1ms TTL=126
Reply from 10.0.16.131: bytes=32 time<1ms TTL=126
Reply from 10.0.16.131: bytes=32 time<1ms TTL=126

Ping statistics for 10.0.16.131:
    Packets: Sent = 4, Received = 3, Lost = 1 (25% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 0ms, Maximum = 0ms, Average = 0ms
```

Figura 2 - Output do *ping* do PC0 para o servidor DNS

Verificou-se que, como aconteceu na fase anterior, o primeiro pacote foi perdido porque o PC0 ainda não tinha na sua tabela ARP o endereço MAC do servidor DNS, e que, como é de esperar, os pacotes seguintes foram bem-sucedidos, pois o PC0 já contém na sua tabela ARP o endereço MAC do servidor DNS.

2.6.2 Teste da configuração do DHCP

Este teste também foi feito a partir do PC0. Primeiramente, na CMD, fez-se *ipconfig /release* e depois fez-se *ipconfig* e obteve-se o seguinte:

```
FastEthernet0 Connection:(default port)

Connection-specific DNS Suffix...:
Link-local IPv6 Address.....: FE80::201:42FF:FE9B:91A6
IPv6 Address.....: ::
IPv4 Address.....: 0.0.0.0
Subnet Mask.....: 0.0.0.0
Default Gateway.....: ::
                        0.0.0.0
```

Figura 3 - Output do *ipconfig* do PC0 após fazer *ipconfig /release*

Como era de esperar, este dispositivo ficou sem um IP atribuído. Então, de seguida, fez-se *ipconfig /renew*, e obteve-se o seguinte:

```
FastEthernet0 Connection:(default port)

Connection-specific DNS Suffix...:
Link-local IPv6 Address.....: FE80::201:42FF:FE9B:91A6
IPv6 Address.....: ::
IPv4 Address.....: 10.0.16.2
Subnet Mask.....: 255.255.255.224
Default Gateway.....: ::
                        10.0.16.30
```

Figura 4 - Output do *ipconfig* do PC0 após fazer *ipconfig /renew*

Este teste confirma o correto funcionamento da atribuição automática de IPs via DHCP.

2.6.3 Teste do servidor web

Para testar a conectividade dos *hosts* da LAN A ao servidor web, utilizou-se, novamente, o PC0 para aceder ao URL <http://www.company.com>. Abriu-se o Web Browser web nas configurações do PC0 (Desktop -> Web Browser), colocou-se o URL, e uma página *web* apareceu, que é a *index.html* que está disponível no servidor web. Este teste confirma que a ligação até ao servidor web está correta.

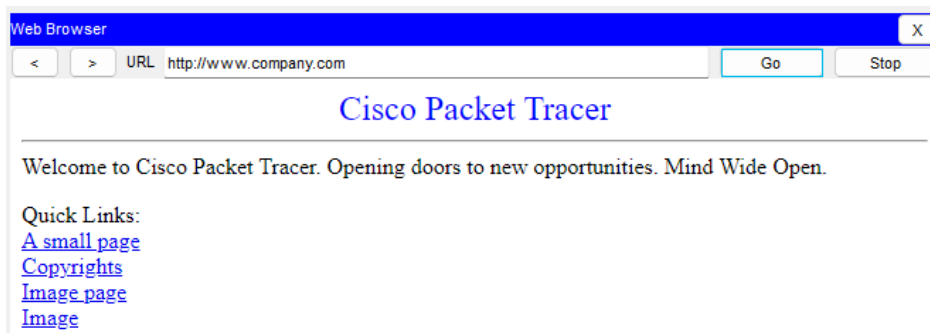


Figura 5 - Output da *Web Browser App*

2.6.4 Teste final utilizando ARP e *tracert*

Este teste foi feito seguindo os passos do enunciado, que são:

1. Desligar a interface de rede do servidor DHCP;
2. Ligá-la novamente;
3. Abrir o CMD no servidor DHCP e verificar a tabela ARP (comando arp -a);
4. Fazer um *ping* do PC1 para o servidor DHCP;
5. Verificar novamente a tabela ARP no servidor DHCP (novamente, comando arp -a).

O output do ponto 3 foi o seguinte:

```
C:\>arp -a
No ARP Entries Found
```

Figura 6 - Output da tabela ARP do ponto 3

Este *output* está correto e é esperado, pois, como a interface de rede foi desligada e depois ligada, é normal que a tabela não tenha entradas, pois não houve ainda nenhum pedido ARP a ser feito.

O output do ponto 5 foi:

```
C:\>arp -a
Internet Address      Physical Address      Type
10.0.16.254           0003.e425.d44a       dynamic
```

Figura 7 - Output da tabela ARP do ponto 5

Após fazer o *ping* do PC1 para o servidor DHCP, observou-se que a tabela ARP do servidor tem uma entrada, cujo endereço é a *default gateway* da LAN dos servidores, ou seja, é o endereço da interface FastEthernet0/0 do router R2, que é a interface que está a conectar o router R2 à LAN dos servidores. Também contém o seu endereço MAC (*physical address*).

Por fim, para verificar o caminho do tráfego do PC1 até ao servidor DHCP, fez-se, a partir do PC1, um *tracert* para o servidor, cujo output foi:

```
C:\>tracert 10.0.16.129

Tracing route to 10.0.16.129 over a maximum of 30 hops:

  1  0 ms      4 ms      0 ms      10.0.16.46
  2  0 ms      0 ms      0 ms      10.0.16.50
  3  0 ms      0 ms      0 ms      10.0.16.129

Trace complete.
```

Figura 8 - Traceroute do PC1 para o servidor DHCP

Este *output* indica que o tráfego é encaminhado até ao router 1, que por sua vez envia para o router 2, que finalmente conduz o tráfego até ao servidor DHCP, confirmando o correto funcionamento da comunicação.

3. Conclusão

A Fase 4 do projeto permitiu a implementação bem-sucedida dos serviços essenciais de rede — DHCP, DNS e HTTP — no ambiente simulado do Cisco Packet Tracer. Através da configuração de *pools* DHCP específicas para as LANs A e B, da definição de registos DNS no servidor dedicado e da ativação do *Relay Agent* no *router* R1, foi possível garantir que os utilizadores das redes locais recebessem automaticamente as suas configurações de IP e acessem ao servidor web através do domínio www.company.com.

Os testes realizados confirmaram o pleno funcionamento da infraestrutura:

- O DHCP foi validado através dos comandos *ipconfig /release* e *ipconfig /renew*, comprovando a atribuição dinâmica de endereços IP dentro dos intervalos definidos;
- O DNS foi testado com o comando *ping* www.company.com, verificando-se a correta resolução do nome para o endereço IP do servidor web;
- O servidor HTTP foi aceso com sucesso a partir de um browser nos *hosts* das LANs, utilizando o URL do domínio configurado;
- O encaminhamento entre redes foi analisado com *traceroute* e a tabela ARP, demonstrando a eficácia do *Relay Agent* e a conectividade entre todos os dispositivos.

Adicionalmente, o teste com a tabela ARP no servidor DHCP — onde se observou a entrada do *default gateway* (R2) após um *ping* — ilustrou o processo de descoberta de endereços MAC em redes locais, reforçando a compreensão prática do protocolo ARP.

Em suma, todos os objetivos desta fase foram alcançados: a rede corporativa está operacional, com serviços automatizados e acessíveis, cumprindo os requisitos do enunciado. Esta implementação não só solidificou os conceitos teóricos abordados na unidade curricular, como também reforçou a importância de uma configuração precisa e de testes rigorosos na implementação de infraestruturas de rede.

4. Referências

- https://www.ripe.net/media/documents/IPv4_CIDR_Chart_2015.pdf - “IPv4 CIDR Chart 2015”