

Serviços de Rede 1 – **Aula 1 - Práticas**

2022-2023

Instituto Politécnico de Coimbra

Departamento de Engenharia Informática



Pre – Requisitos

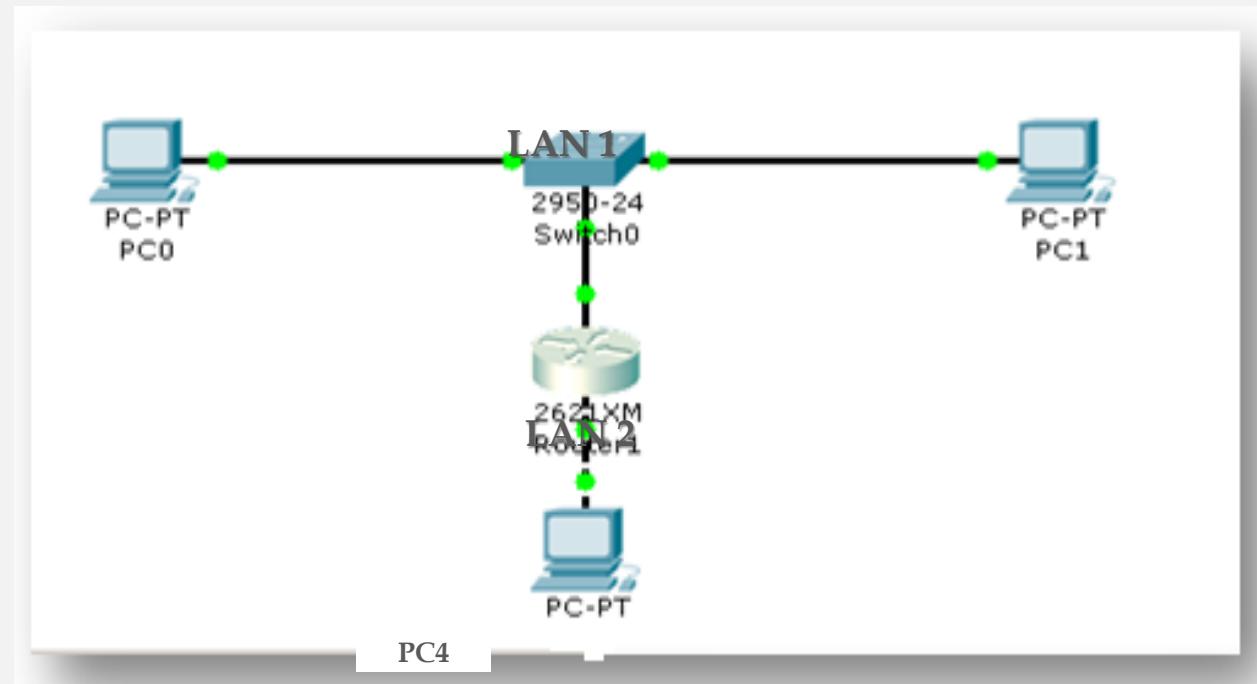
- Ter instalado o *Cisco Packet Tracer* versão 8.2.0



Exercício 1 – Configurar uma rede simples com o Cisco *Packet Trace*

Exercício 1

- Inicie o Cisco Packet Tracer.
- Crie a rede que está no desenho (**Não necessita de ser com os mesmos modelos de equipamentos ativos**).
- O router deve ter pelo menos uma porta serie e duas Fast Ethernet.
- Altere o nome do router para sr1-cbr-2022.
- Coloque a password de *enable* como *sr12022*.
- Coloque os seguintes endereços:
 - **Rede local 1 (LAN1) -192.168.1.xx ->255.255.255.0**
 - PC0 - 192.168.1.1 -> 255.255.255.0
 - PC1- 192.168.1.2 -> 255.255.255.0
 - Router - 192.168.1.254 -> 255.255.255.0
 - **Rede local 2 (LAN2) -192.168.2.xx ->255.255.255.0**
 - PC4 - 192.168.2.1 -> 255.255.255.0
 - Router - 192.168.2.254 -> 255.255.255.0
- Teste as ligações na rede local 1 (PC0<->PC1).
- Verifique o estado das interfaces.
- Teste a conectividade do router para o PC0 e do PC4 para o router.
- Teste a conectividade do PC1 para o PC4 e vice versa.



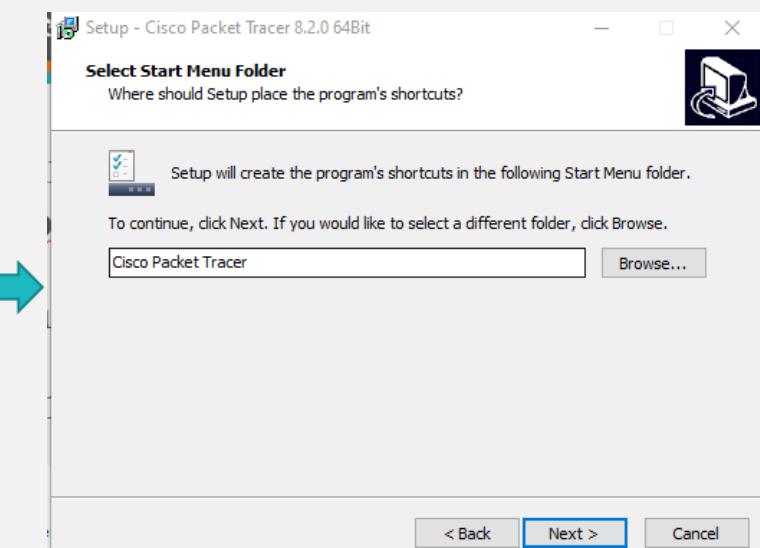
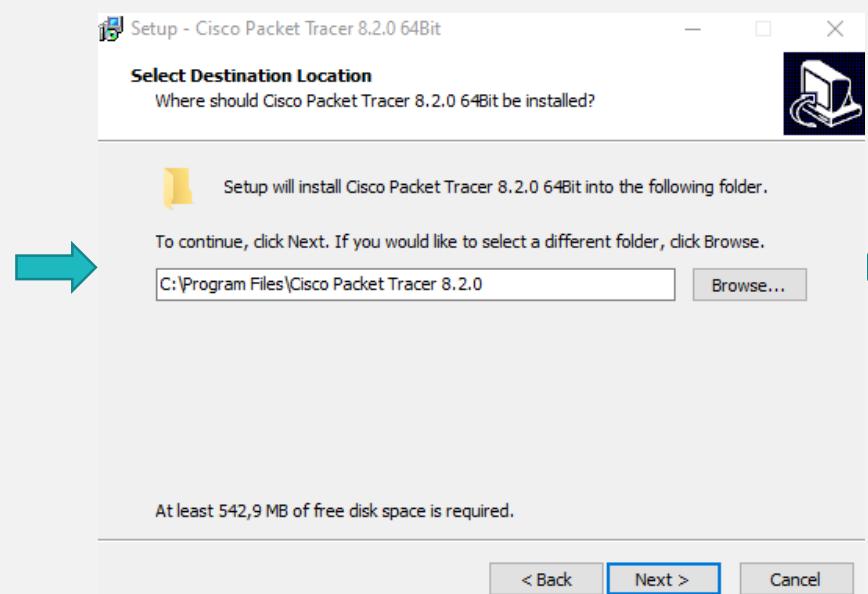
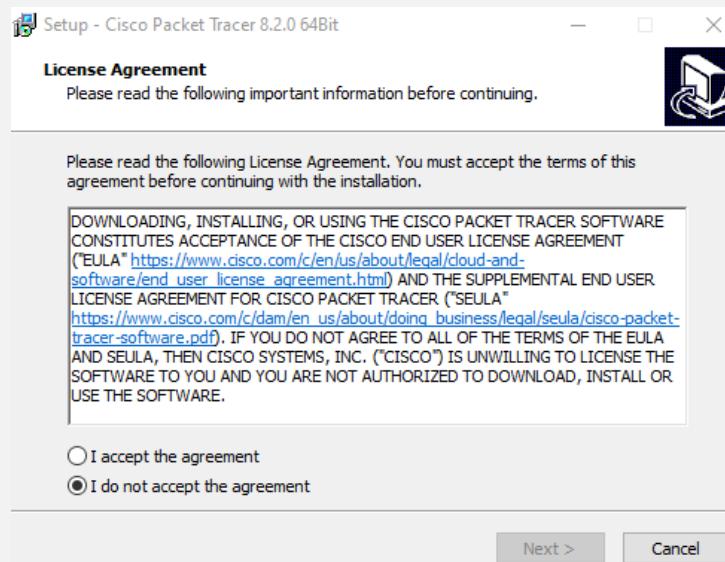
Exercício 1

- Coloque uma descrição em ambas as interfaces das redes locais.
- Tente aceder por telnet de um PC da rede local LAN 1 ao router. Consegue?
- Faça as alterações necessárias para que isso aconteça.
- Coloque um *banner* indicando que está a aceder a um sistema seguro.
- Escreva uma palavra sem significado na configuração. O que acontece? Anule a funcionalidade nativa dos routers para fazer a resolução de nomes. Repita a escrita da palavra. O que acontece?

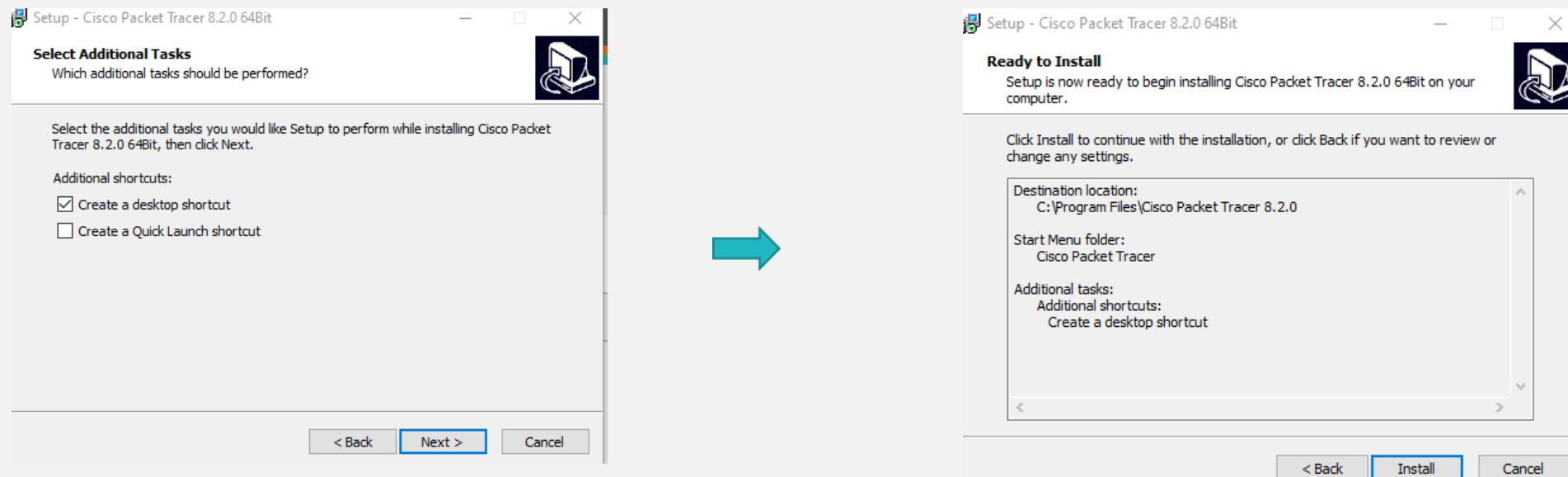
How To

Instalação

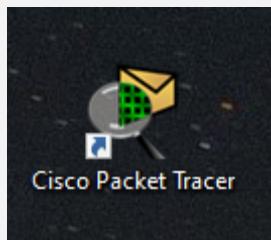
- Tem o instalador do Packet Tracer versão 8.2.0 para 64bits e 32 bits no Moodle.
- Escolha o que se adequa ao seu sistema operativo.
- Faça a instalação.



Instalação

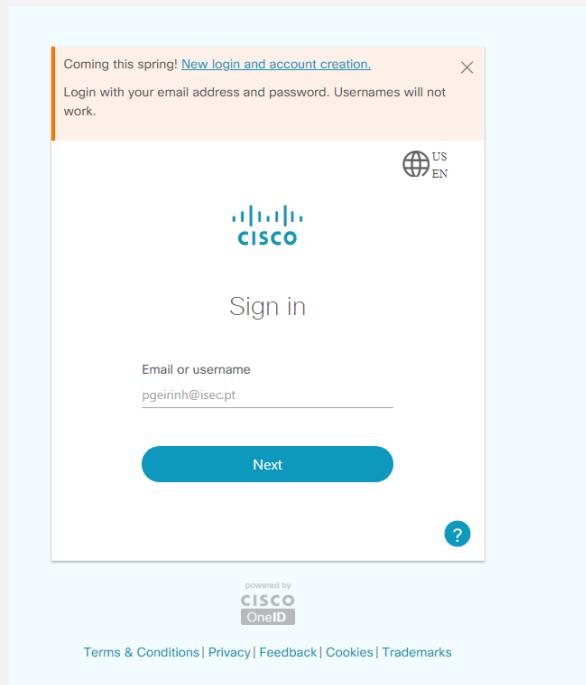


Instalação



Instalação

- Se já tiver um utilizador em utilizador e a password para aceder ao programa. Deve ter recebido no seu mail do ISEC uma mensagem sobre isto e que aqui se recorda:



coloque o nome de utilizador e a password para aceder ao programa. Deve ter recebido no seu mail do ISEC uma mensagem sobre isto e que aqui se recorda:

Log In na Academia Cisco

Todos os alunos do ramo RAS são automaticamente inscritos no início do semestre em que entram para o ramo RAS. Depois deste processo estar concluído (no presente ano letivo hoje, dia 2023/02/23) recebem um email da Cisco com indicação de como devem proceder para concluir o processo.

Instalação

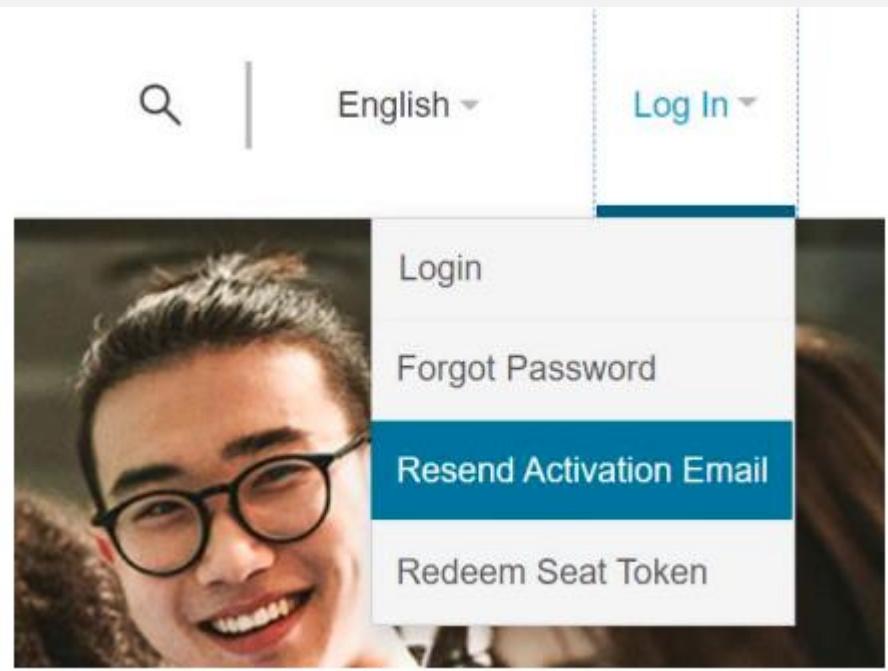
Log In na Academia Cisco

Alguns alunos não recebem os emails por terem a caixa de correio cheia, não sabendo por isso como ativar a respetiva conta. Outros recebem esse email classificado como SPAM, não se apercebendo dele.

Por estes motivos solicita-se aos alunos que:

- Libertem espaço suficiente na sua mailbox institucional e consultem o seu email pelo menos no início e final de cada dia durante o período escolar.
- Se não possuem esta mailbox cheia e ainda não se depararam com o email da Cisco procurem nos emails diários de resumo de SPAM (remetente sgit@isec.pt), de hoje e dos próximos dias, por emails com a palavra “Cisco”. Certamente estará por lá o email de ativação.

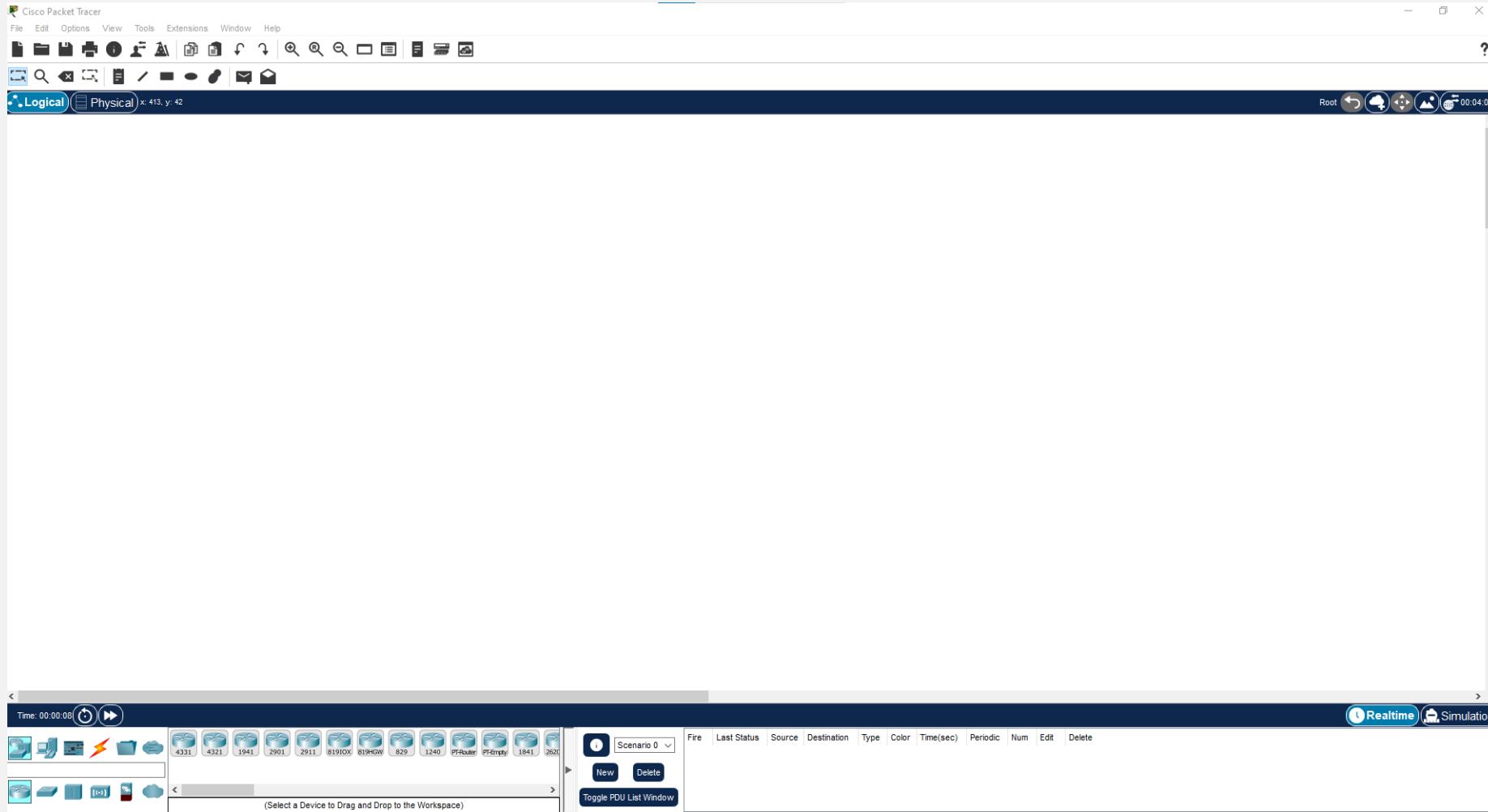
Instalação



Log In na Academia Cisco

Se não tiverem recebido o email (pode suceder para os alunos que têm a mailbox cheia) basta entrar em cisco.netacad.com, clicar em Log In e depois em Resend Activation Email (é quase certo que o email será classificado como SPAM e que por isso devem no dia seguinte analisar o sumário de SPAM proveniente de sgit@isec.pt).
Aos alunos que já foram inscritos em anos letivos anteriores e se tenham esquecido da senha de entrada (como login devem usar o email institucional) devem usar a opção Forgot Password.

Instalação



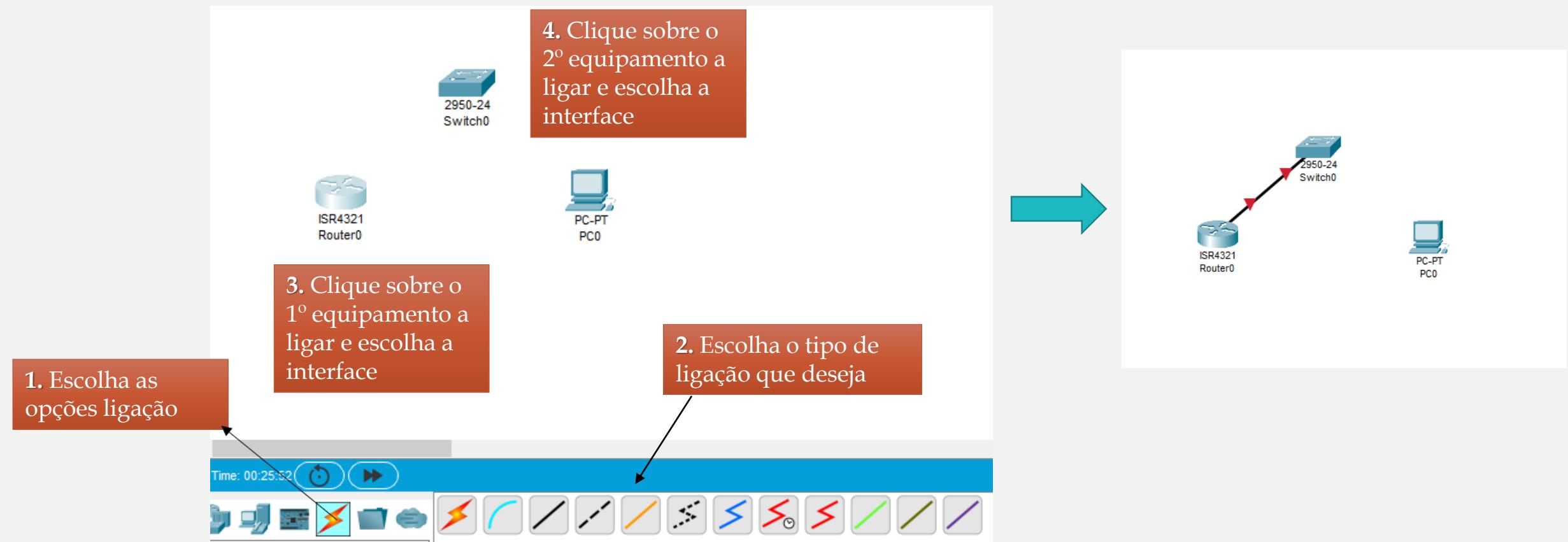
Trabalhar com...

- Para inserir um novo equipamento de rede



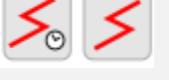
Trabalhar com...

- Para ligar os equipamentos:



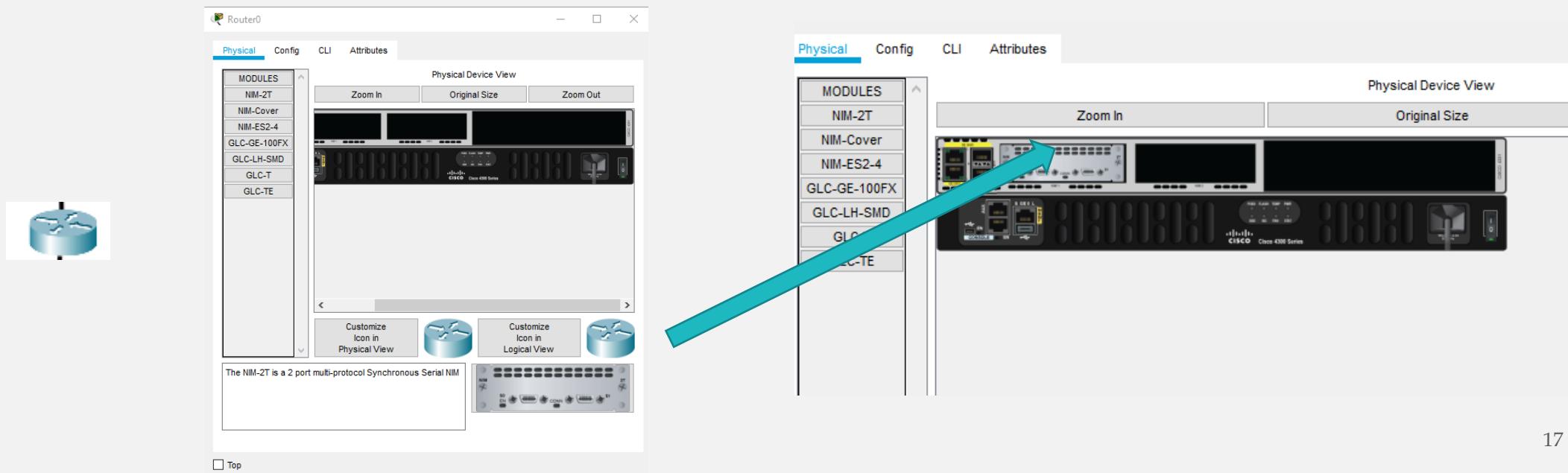
Trabalhar com ...

- As ligações mais utilizadas são as seguintes:

-  → **Automática** - Seleciona de forma automática o cabo mais adequado à ligação. Deve evitar usar esta função porque tal funcionalidade não existe na vida prática
-  → **Cabo de consola**. Adequado para ligar um PC à porta de consola do router. Essa porta serve para fazer a configuração e a manutenção quando nos ligamos diretamente no equipamento.
-  → **Chicote RJ45 direto**. Adequado para ligar um equipamento de rede a um switch ou HUB.
-  → **Chicote RJ45 cruzado**. Adequado para ligar dois equipamentos ativos diretamente entre si.
-  → **Chicote de FO**. Adequado para ligar um equipamento de rede a uma porta de fibra ótica de um switch
-  → **Cabos Serie**. Adequado para ligar às portas serie dos router.

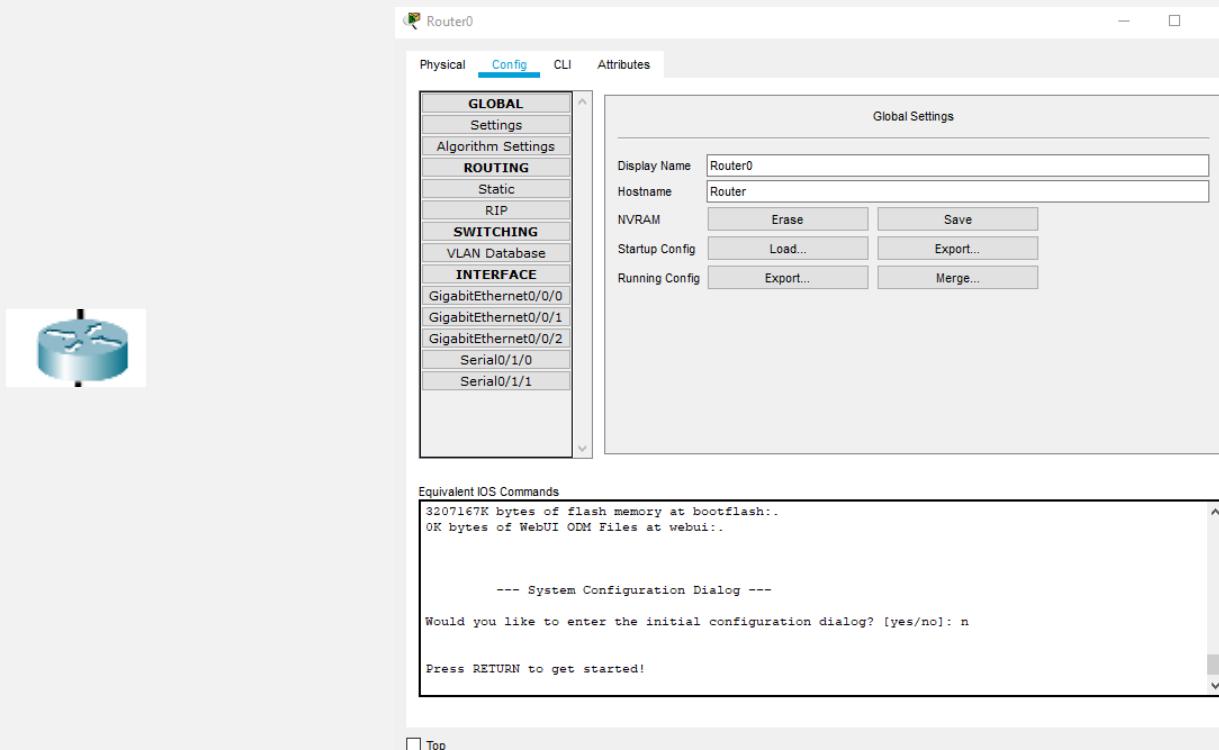
Trabalhar com...

- No separador da parte física (*Physical*) pode colocar e tirar interfaces aos routers.
- Para isso tem de “desligar” o router, escolher a placa desejada, arrasta-la até ao interface livre e “ligar” o router.



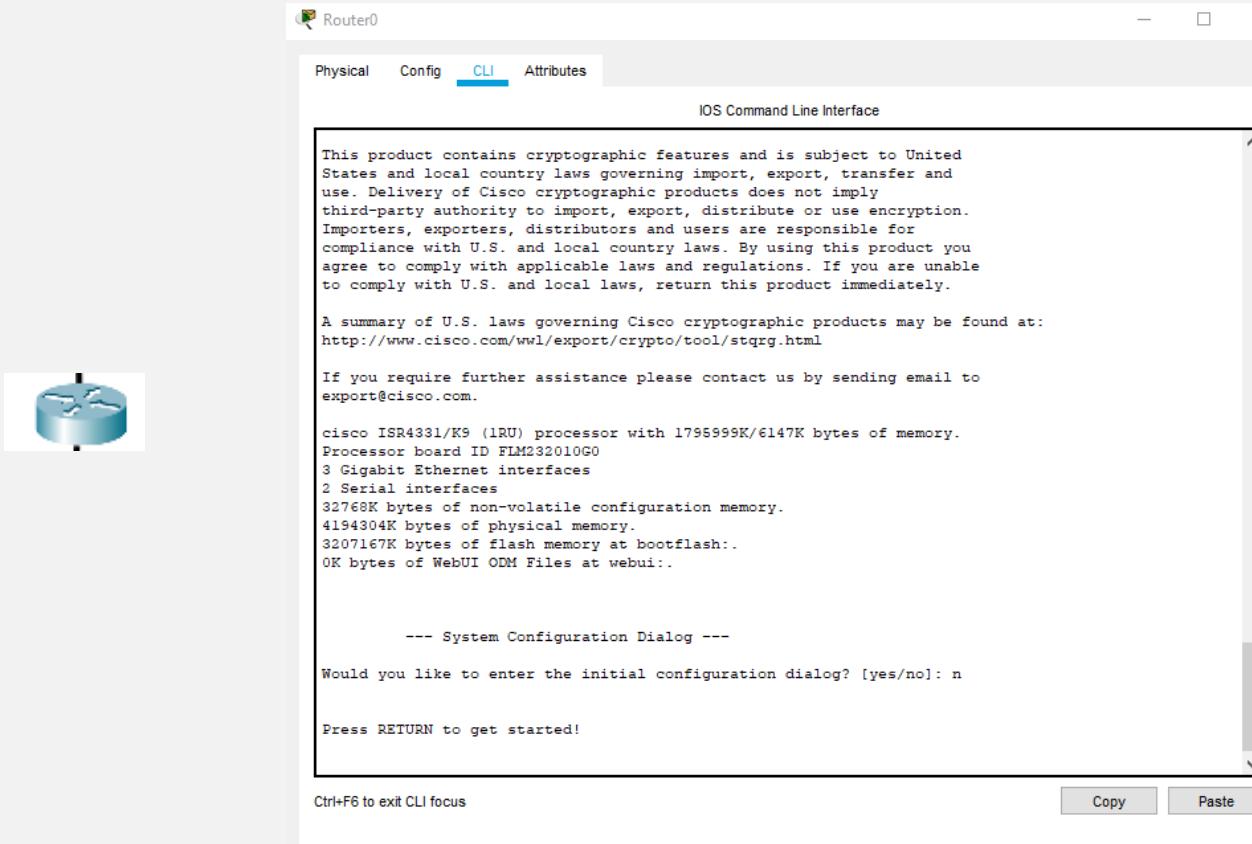
Trabalhar com...

- No separador da configuração pode ver e configurar os routers e as suas interface.
- Não deve usar este separador para configurar os equipamentos porque na vida prática esta funcionalidade não existe.



Trabalhar com ...

- O separador CLI (*Command line interface*) vai permitir configurar o router usando o Cisco IOS.

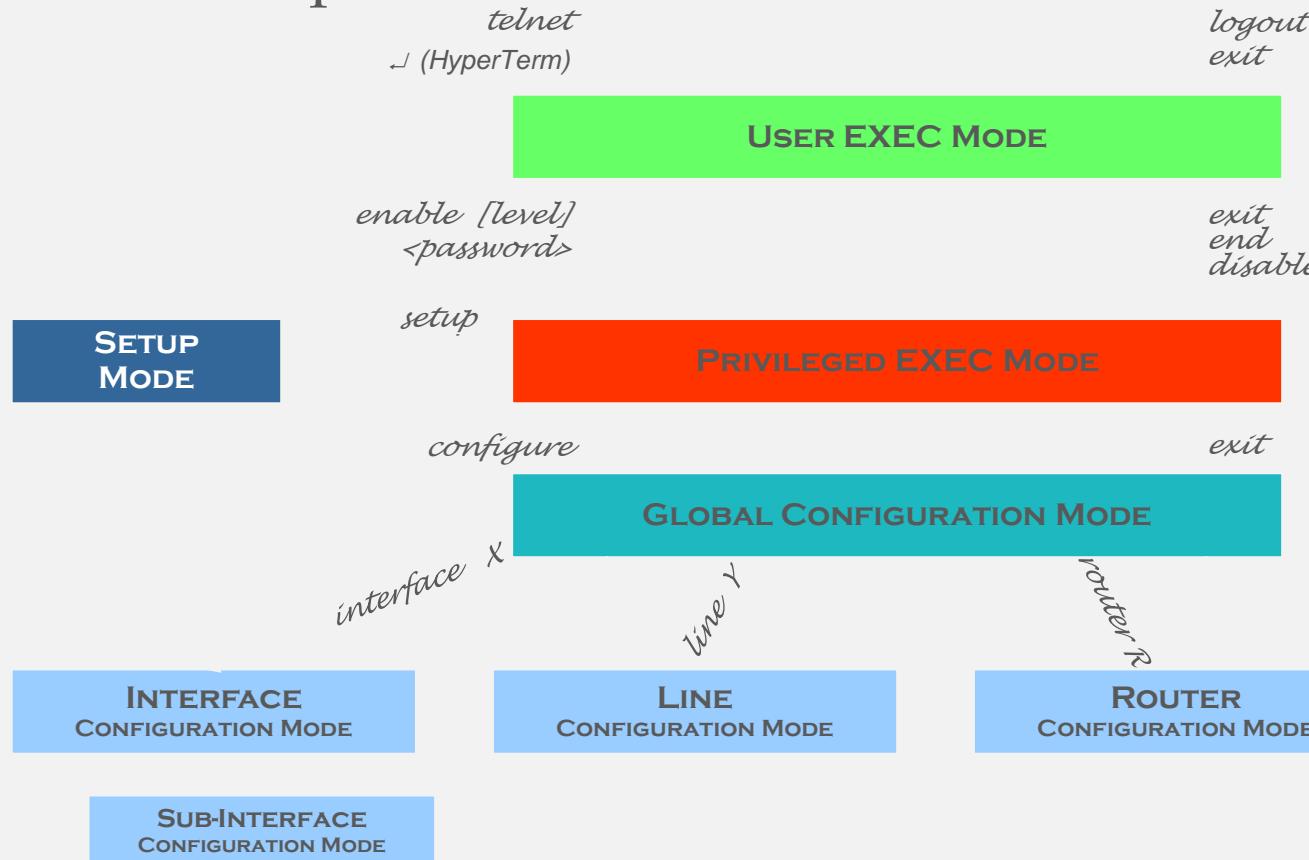


Command line interface (CLI)

- O modo mais completo e mais flexível de configuração de um *router* é através da interface de linha de comandos (*Command line interface* – CLI) do sistema operativo IOS.

CLI

- Hierarquia



Configuration Mode	Prompt
Interface	Router(config-if)#
Subinterface	Router(config-subif)#
Controller	Router(config-controller)#
Map-list	Router(config-map-list)#
Map-class	Router(config-map-class)#
Line	Router(config-line)#
Router	Router(config-router)#
IPX-router	Router(config-ipx-router)#
Route-map	Router(config-route-map)#

```

Router
Router con0 is now available.

Press RETURN to get started.

User Access Verification
Password:
Router> ┏━━━━━ User-Mode Prompt
Router>enable
Password:
Router# ┏━━━━━ Privileged-Mode Prompt
Router#disable
Router>
Router>exit
  
```

CLI

- Ajuda contextualizada

```
Cisco>?  
Exec commands:  
access-enable      Create a temporary Access-  
                      entry  
access-profile     Apply user-profile to inte  
access-template    Create a temporary Access-
```

```
Cisco#cl?  
clear clock  
Cisco#clock  
% Incomplete command.  
Cisco#clock ?  
    set Set the time and date  
Cisco#clock set  
% Incomplete command
```

- Sinalização de erros sintáticos

```
Router#configure terminal  
^  
% Invalid input detected at '^' marker.  
Router#configure terminal
```

- Abreviação de comandos

```
Router# conf term  
Router(config)#i  
% Ambiguous command: "i"
```

- Anulação de comandos

```
Router# conf term  
Router(config)# no cmd...
```

CLI

- **Hot keys**

TAB	Completa um comando abreviado
Ctrl+P (↑)	Comando anterior
Ctrl+N (↓)	Comando mais recente
Ctrl+L	Refresca o <i>Command Prompt</i>
Ctrl+Z	Regressa ao EXEC Mode
Ctrl+^	Interrompe a tarefa corrente
Ctrl+Shift+6, x	Interrompe resolução de nomes
Ctrl+U	Apaga do cursor ← início da linha

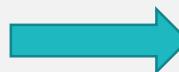
Ctrl+K	Apaga do cursor → fim da linha
Ctrl+A	Coloca o cursor no início da linha
Ctrl+E	Coloca o cursor no fim da linha
Ctrl+V	A keystroke seguinte é input
ESC+B (←)	Regressa à palavra anterior
Ctrl+B	Regressa ao caracter anterior
ESC+F	Avança para a próxima palavra
Ctrl+F (→)	Avança para o próximo caracter

Router> show history	Shows command buffer
Router> terminal history size number-of-lines	Sets the command history buffer size*
Router> terminal no editing	Disables advanced editing features
Router> terminal editing	Re-enables advanced editing
<Tab>	Completes the entry

Configuração inicial

- Alterar o nome do router

```
Router(config)# hostname Coimbra  
Tokyo (config)#{
```



```
Router>en  
Router#conf t  
Enter configuration commands, one per line. End with CNTL/Z.  
Router(config)#host  
Router(config)#hostname Coimbra  
Coimbra(config)#{  
  
Ctrl+F6 to exit CLI focus  
  
Top
```

- Evitar a resolução de nome (DNS)

```
Router(config)# no ip domain-lookup
```

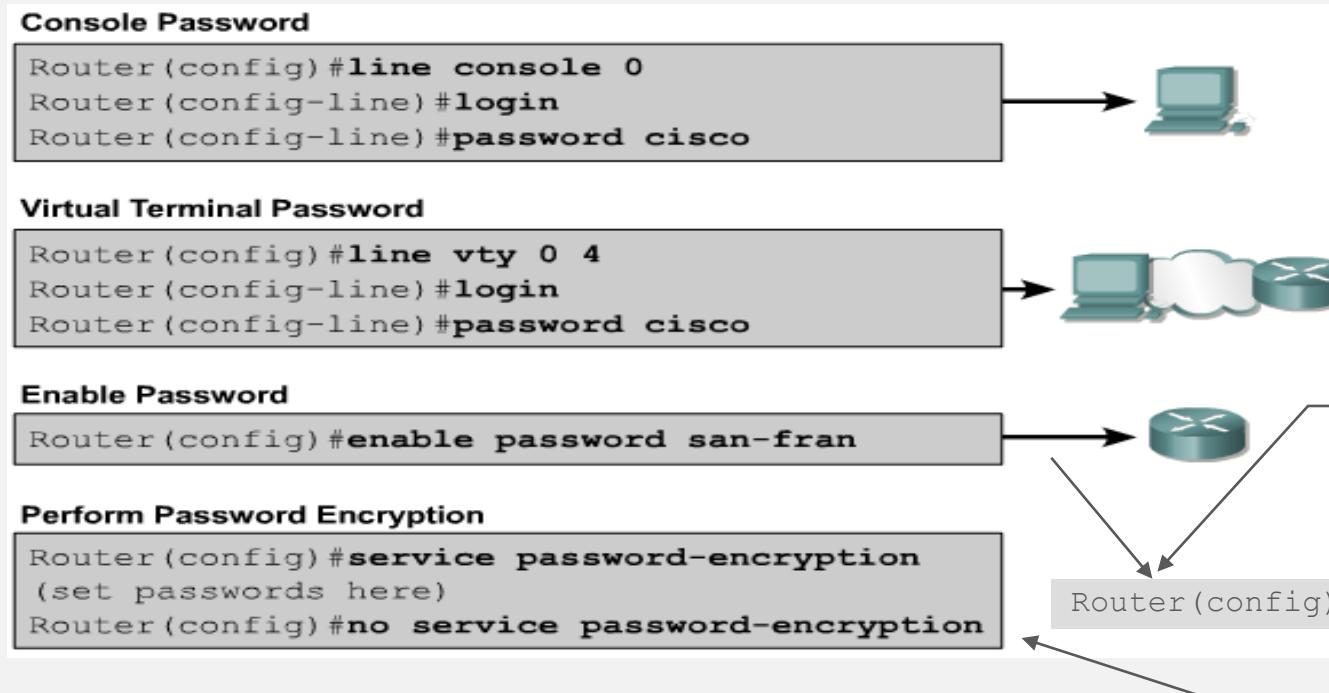
- Nome dos sistemas vizinhos (*host table*)

```
Router (config) #ip host Auckland 172.16.32.1  
Router (config) #ip host Beirut 192.168.53.1  
Router (config) #ip host Capetown 192.168.89.1  
Router (config) #ip host Denver 10.202.8.1
```

```
LAB_A#show hosts  
Default domain is not set  
Name/address lookup uses domain service  
Name servers are  
  
Host Flags Age Type Address(es)  
LAB_A (perm, OK) ** IP 192.5.5.1 205.7.5.1 201.100.11.1  
LAB_B (perm, OK) ** IP 219.17.100.2 199.6.13.1 201.100.11.2  
LAB_C (perm, OK) ** IP 223.8.151.1 204.204.7.1 199.6.13.2  
LAB_D (perm, OK) ** IP 210.93.105.1 204.204.7.2  
LAB_E (perm, OK) ** IP 210.93.105.2
```

Configuração inicial

- *Passwords* de acesso



Toma precedência sobre o “enable password”. Usa o algoritmo encriptação MD5.

Evita que as *passwords* não encriptadas sejam legíveis.

Configuração inicial

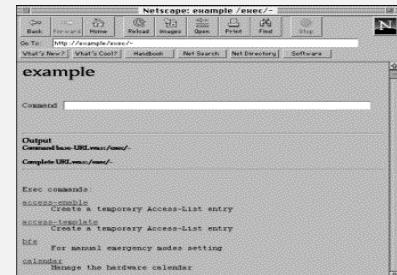
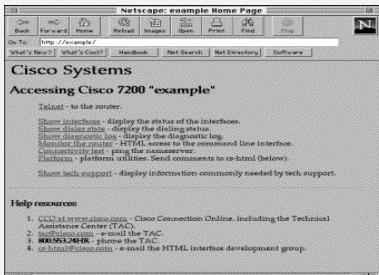
- Acesso por Web browser
 - Activar Http server

```
Router# configure terminal  
Router(config)# ip http server
```

- Alterar porto

```
Router(config)# ip http port number
```

- Acesso: http://IP/



- Banners

- MOTD - Message of the Day

```
LAB_A con0 is now available  
Press RETURN to get started.
```

```
This is a secure system. Authorized Access ONLY!!!
```

User Access Verification

Password:

```
LAB A>enable
```

```
LAB A(config)# banner motd # This is a secure system.  
Authorized access ONLY!!! #
```

Outros Comandos Básicos

- *Enable* – entra em modo de privilegiado
- *Conf t* – entra em modo de configuração
- *No comando* – nega o comando
- *Ctrl+z ou exit* – deixa o modo de configuração
- *Show running-config* – mostra a configuração do router que está guardada na RAM
- *Show startup-config* - mostra a configuração que é carregada na RAM quando o router arranca.
- *Write memory (wri mem)* – grava a configuração que está a correr.
- *Clock* – actualiza o relógio
 - Clock set 12:50:00 18 Dez 2007
 - Clock timezone GMT 0

Configurando uma *interface* Ethernet

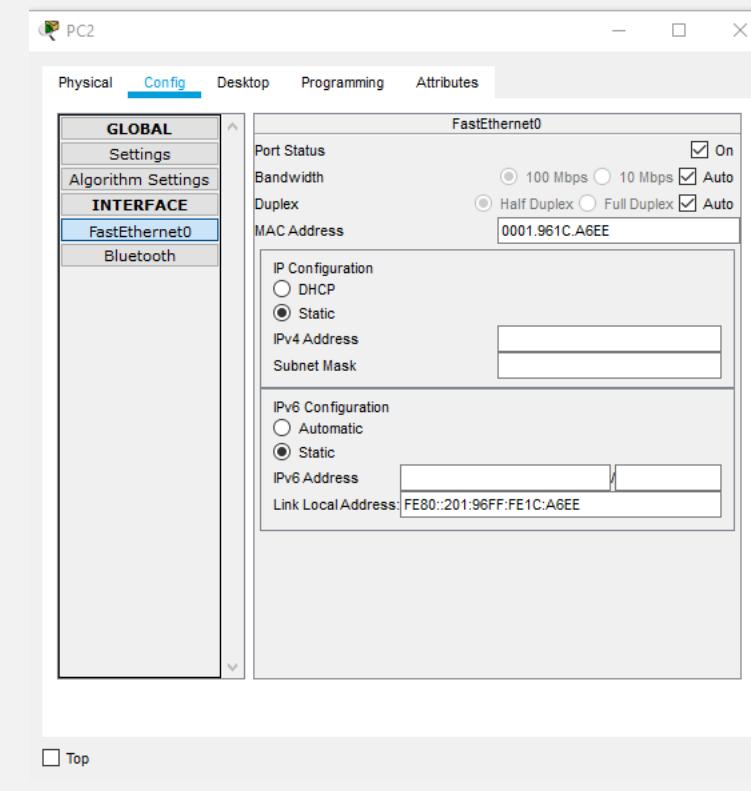
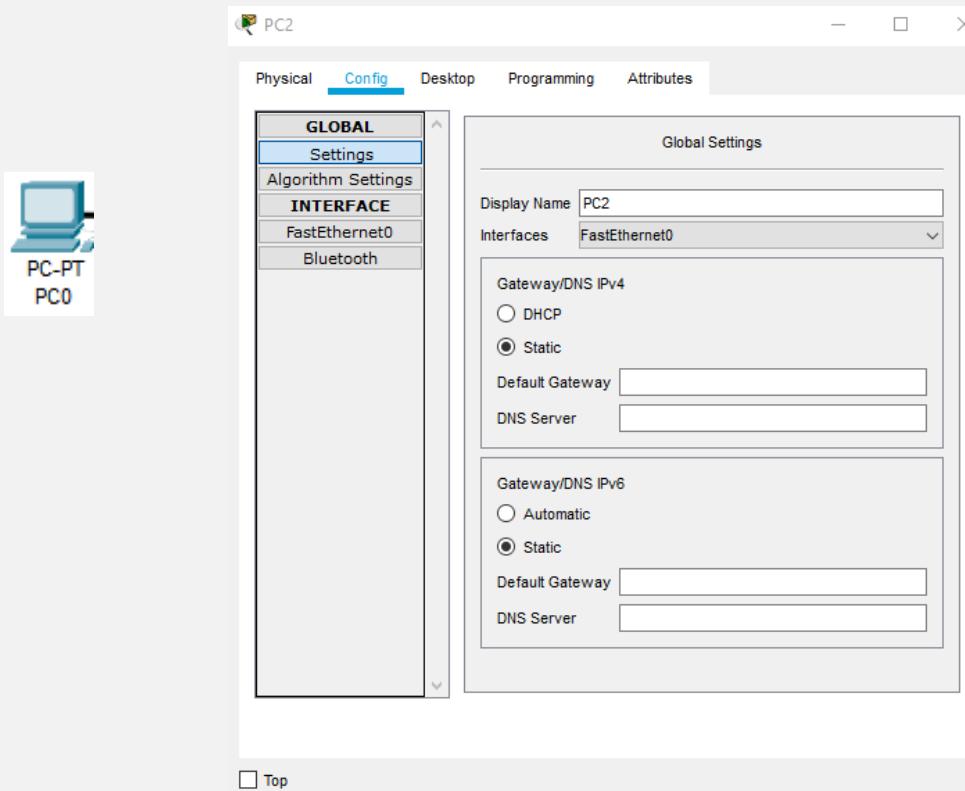
```
R1(config)#interface fastethernet 0/0
R1(config-if)#ip address 172.16.1.254 255.255.255.0
R1(config-if)#description LAN1
R1(config-if)#no shutdown
```

```
R1#show interfaces fastethernet 0/0
FastEthernet0/0 is up, line protocol is up
  Hardware is AmdFE, address is 000c.3010.9260 (bia 000c.3010.9260)
  Internet address is 172.16.3.1/24

R1#
```

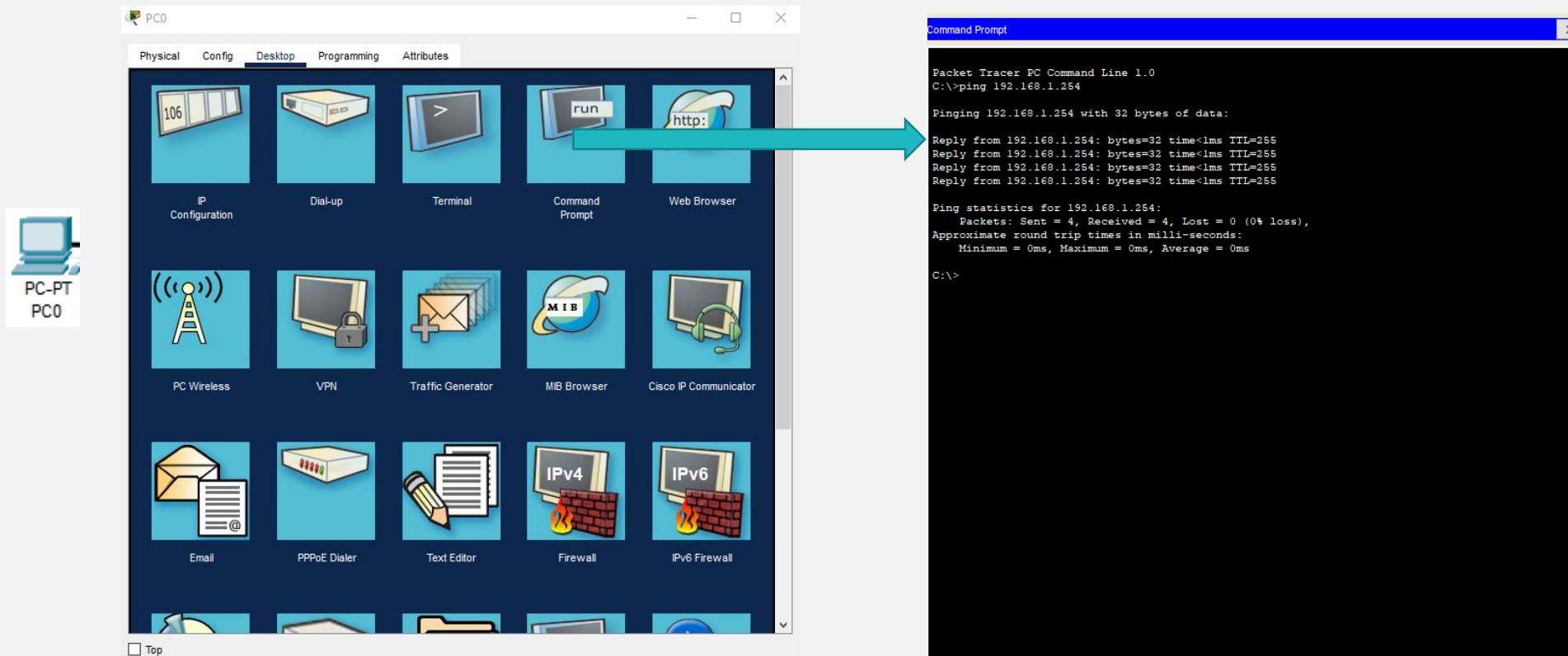
Trabalhar com...

- No separador “Config” pode configurar os valores globais ou das diferentes placas dos equipamentos.



Trabalhar com...

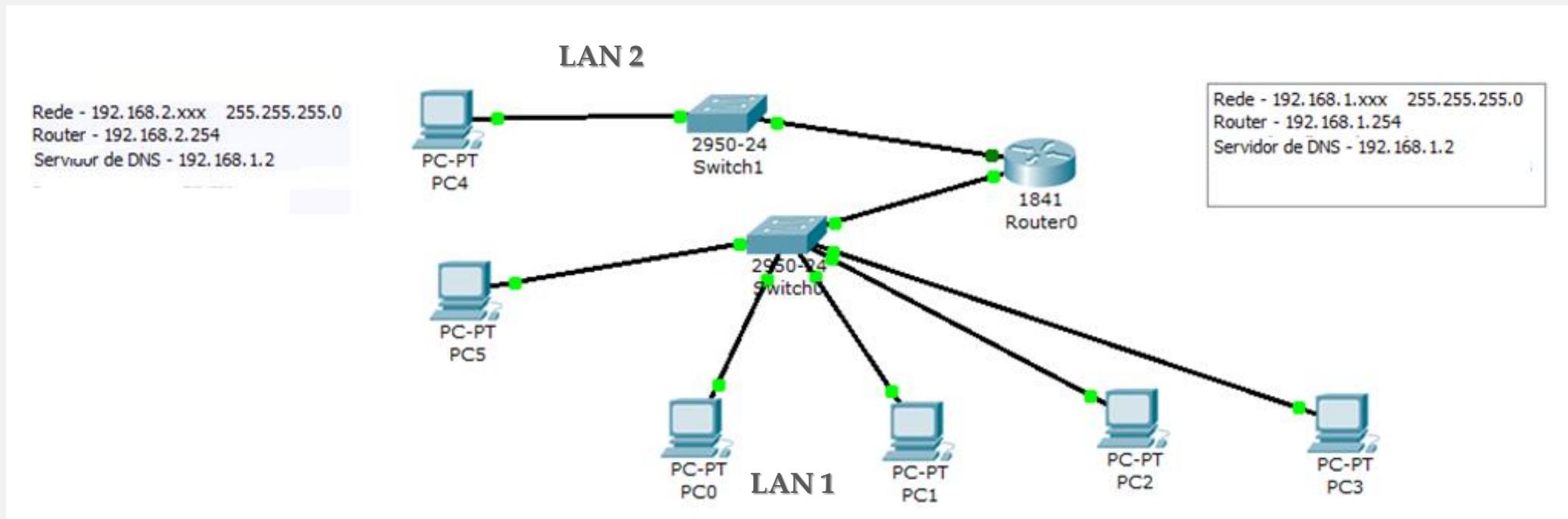
- No separador “Desktop” permite o acesso a aplicativos que permitem configurar ou testar o seu equipamento e a rede.



Exercício 2 - Alargando a rede

Exercício 2

- Faça as alterações necessárias ao exercício anterior para obter a seguinte topologia:



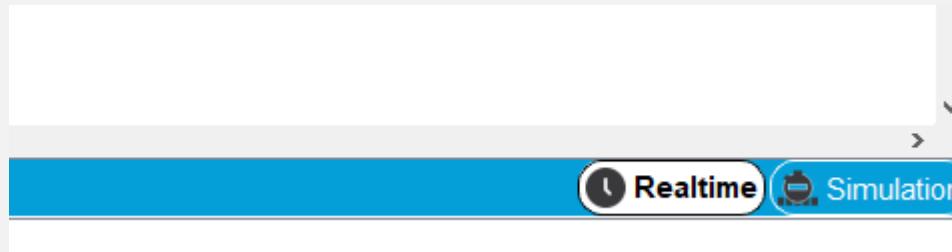
Exercício 2

- Teste se a sua rede está a funcionar.
- Simule um *ping* do PC4 até ao PC5 e acompanhe o trajeto do pacote de informação. Analise os diferentes pacotes que são gerados.

How To

Simulação

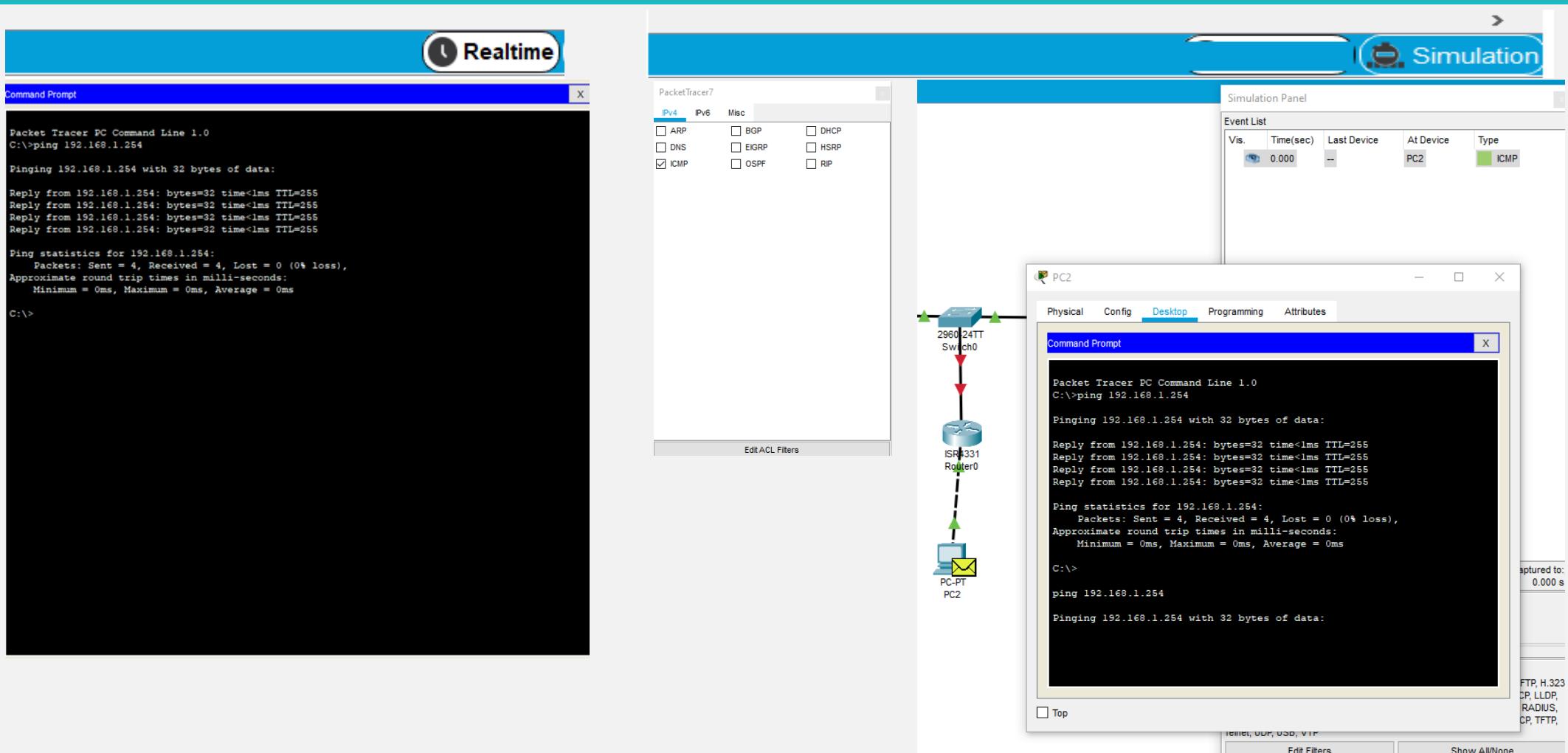
- O Packet Tracer permite dois tipos de simulação:



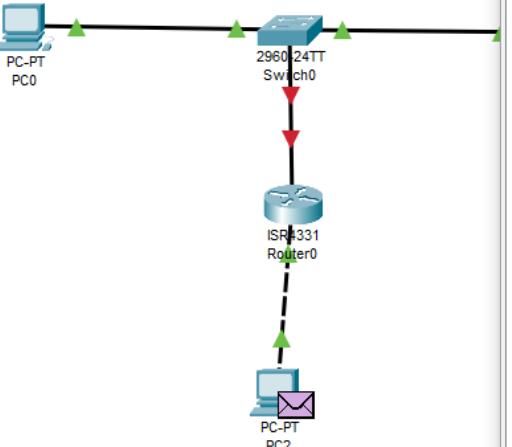
RealTime - onde a simulação utilizada é feita de forma seguida com na “vida real”

Simulation - onde pode escolher o tipo de protocolo que deseja observar e pode ir acompanhando o que vai acontecendo de equipamento para equipamento.

Simulação



Simulação



The diagram illustrates a network topology. A computer icon labeled "PC-PT PC0" is connected to a switch labeled "2960 24TT Switch0". This switch is connected to a router labeled "ISR 331 Router0", which in turn connects to another computer icon labeled "PC-PT PC2".

Event List

Vis.	Time(sec)	Last Device	At Device	Type
0.000			PC2	ICMP
0.001		PC2	Router0	ICMP
0.002		Router0	PC2	ICMP
1.005		--	PC2	ICMP
1.006		PC2	Router0	ICMP
1.007		Router0	PC2	ICMP
2.007		--	PC2	ICMP
2.008		PC2	Router0	ICMP
2.009		Router0	PC2	ICMP
3.012		--	PC2	ICMP
3.013		PC2	Router0	ICMP
3.014		Router0	PC2	ICMP

Reset Simulation Constant Delay Captured to: 450.825 s

Play Controls

Event List Filters - Visible Events
ICMP
[Edit Filters](#) [Show All/None](#)

Detalhe de um pacote de informação

PDU Information at Device: PC2

OSI Model **Outbound PDU Details**

At Device: PC2
Source: PC2
Destination: 192.168.1.254

In Layers

- Layer7
- Layer6
- Layer5
- Layer4
- Layer3
- Layer2
- Layer1

Out Layers

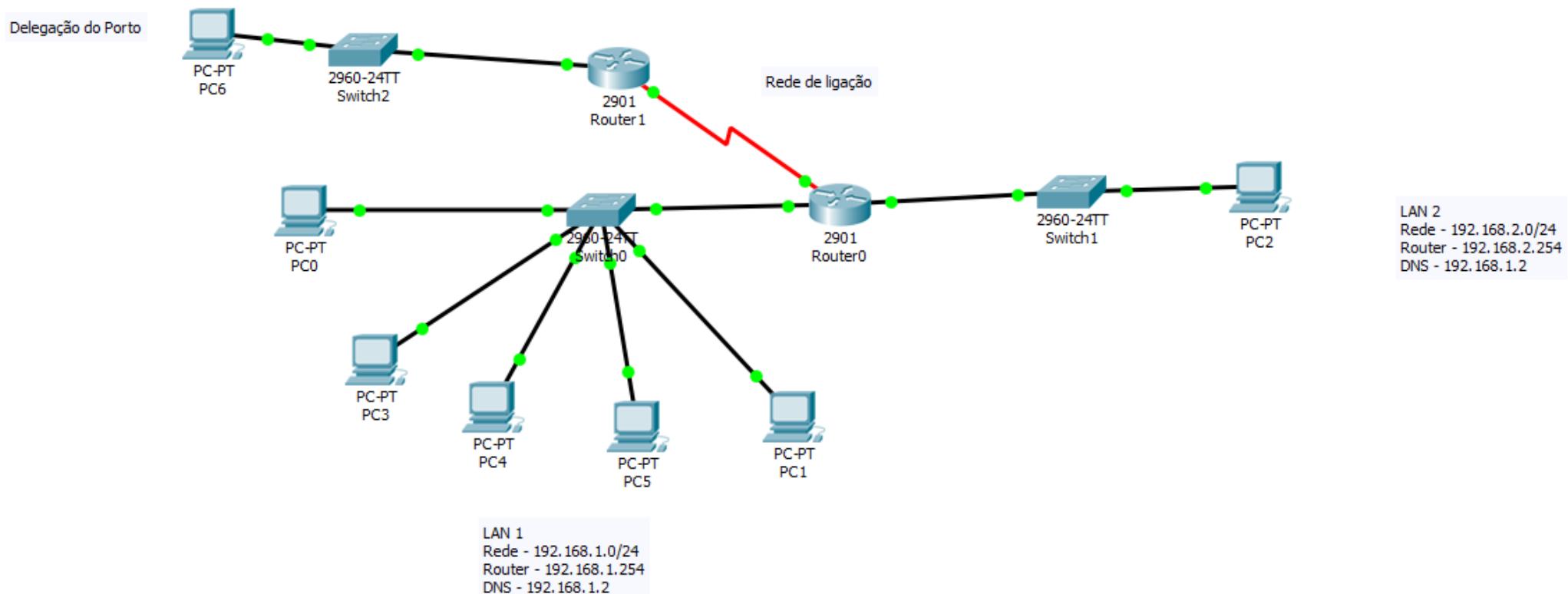
- Layer7
- Layer6
- Layer5
- Layer4
- Layer 3: IP Header Src. IP: 192.168.1.1, Dest. IP: 192.168.1.254 ICMP Message Type: 8
- Layer 2: Ethernet II Header 000A.411E.9818 >> 00D0.FF8C.2101
- Layer 1: Port(s): FastEthernet0

1. The Ping process starts the next ping request.
2. The Ping process creates an ICMP Echo Request message and sends it to the lower process.
3. The source IP address is not specified. The device sets it to the port's IP address.
4. The destination IP address is in the same subnet. The device sets the next-hop to destination.

[Challenge Me](#) [<< Previous Layer](#) [Next Layer >>](#)

Exercício 3 – Configurar uma ligação serial

Exercício 3



Exercício 3

- A empresa abriu uma delegação no Porto sendo a topologia de rede a apresentada no slide anterior.
- Estabeleça para esse delegação duas redes IP sabendo que:
 - Deve considerar que na LAN terá até 254 equipamentos
 - Na WAN (rede de ligação dos router) só terá dois equipamentos para ligar.
- Faça a ligação da delegação à sede com uma ligação serie ponto-a-ponto.
- Teste a conectividade.

NOTA:

- Ao falar de conectividade de rede, deve garantir que as máquinas têm acesso na sua rede local e na WAN da empresa (por exemplo, que um PC de rede LAN1 pode alcançar as máquinas que estão em LAN1, LAN2 e Porto).

Exercício 3

- Qual é o conteúdo da tabela de *routing* do Router0
- Para a rede que liga os router, indique:
 - Endereço da rede;
 - Máscara de rede;
 - Endereço de *broadcast*;
 - Gama de endereços disponíveis para endereçar máquinas.

How To

Configuração de uma *Interface Serial*

- Configuração base

Identificação do endereço IP e máscara

Identificação da interface a configurar

```
Router> enable
Router# configure terminal
Router(config)# interface serial0
Router(config-if)# description Delegação - Porto
Router(config-if)# ip address <ip address> <netmask>
Router(config-if)# clock rate 56000
Router(config-if)# no shutdown
```

Activação administrativa da interface

Nas interfaces série quando o router actua como DCE (i.e. assume o papel de CSU/DSU) é necessário gerar relógio. Ritmos (bps) válidos: 1200, 2400, 9600, 19200, 38400, 56000, 64000, 72000, 125000, 148000, 500000, 800000, 1000000, 1300000, 2000000, 4000000.

Rotas Estáticas

- **Comando *ip route***

- Para configurar uma rota estática utiliza-se o seguinte comando:

```
Router(config)# ip route network-address subnet-mask  
{ip-address | exit-interface }
```

Parâmetro	Descrição
network-address	Endereço da rede de destino da rede remota a ser adicionado à tabela de roteamento.
subnet-mask	Máscara de sub-rede da rede remota a ser adicionada à tabela de roteamento. A máscara de sub-rede pode ser modificada para sumarizar um grupo de redes.
ip-address	Normalmente conhecido como o endereço IP do roteador do próximo salto.
exit-interface	Interface de saída usada no encaminhamento de pacotes para a rede de destino.

Rotas Estáticas

- Rotas estáticas configuradas com uma interface de saída são mais eficientes.
- A tabela de *routing* pode identificar a interface de saída em uma única consulta, ao invés de duas quando utiliza o endereço IP.

```
R1(config)#no ip route 192.168.2.0 255.255.255.0 172.16.2.2
R1(config)#ip route 192.168.2.0 255.255.255.0 serial 0/0/0
R1(config)#end
R1#show ip route
Codes: C - connected, S - static, I - IGRP, R - RIP, M - mobile, B - BGP
      D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
      N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
      E1 - OSPF external type 1, E2 - OSPF external type 2, E - EGP
      i - IS-IS, L1 - IS-IS level-1, L2 - IS-IS level-2, ia - IS-IS inter area
      * - candidate default, U - per-user static route, o - ODR
      P - periodic downloaded static route

Gateway of last resort is not set

      172.16.0.0/24 is subnetted, 3 subnets
S        172.16.1.0 [1/0] via 172.16.2.2
C        172.16.2.0 is directly connected, Serial0/0/0
C        172.16.3.0 is directly connected, FastEthernet0/0
S        192.168.1.0/24 [1/0] via 172.16.2.2
S        192.168.2.0/24 is directly connected, Serial0/0/0
```

Agora a interface de saída está especificada na rota estática. Não há necessidade de uma pesquisa recursiva.

Modificando Rotas Estáticas

- As rotas estáticas existentes não podem ser modificadas. Uma rota antiga deve ser removida colocando um **no** antes do comando **ip route**.
no ip route 192.168.2.0 255.255.255.0 serial 0/0/1
- A nova rota estática deve ser reescrita na configuração do router:

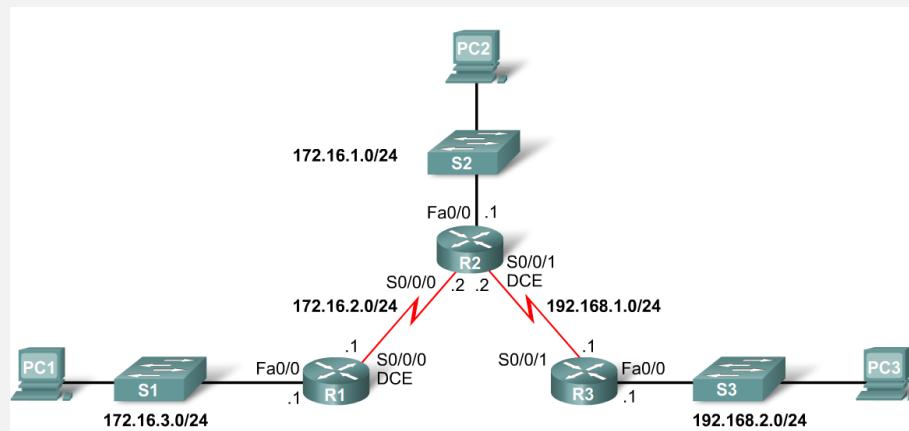
```
R1(config)#no ip route 172.16.1.0 255.255.255.0 172.16.2.2
R1(config)#ip route 172.16.1.0 255.255.255.0 serial 0/0/0
R1(config)#no ip route 192.168.1.0 255.255.255.0 172.16.2.2
R1(config)#ip route 192.168.1.0 255.255.255.0 serial 0/0/0
```

```
R2(config)#no ip route 172.16.3.0 255.255.255.0 172.16.2.1
R2(config)#ip route 172.16.3.0 255.255.255.0 serial 0/0/0
R2(config)#no ip route 192.168.2.0 255.255.255.0 192.168.1.1
R2(config)#ip route 192.168.2.0 255.255.255.0 serial 0/0/1
```

```
R3(config)#no ip route 172.16.1.0 255.255.255.0 192.168.1.2
R3(config)#ip route 172.16.1.0 255.255.255.0 serial 0/0/1
R3(config)#no ip route 172.16.2.0 255.255.255.0 192.168.1.2
R3(config)#ip route 172.16.2.0 255.255.255.0 serial 0/0/1
R3(config)#no ip route 172.16.3.0 255.255.255.0 192.168.1.2
R3(config)#ip route 172.16.3.0 255.255.255.0 serial 0/0/1
```

Verificar as Rotas Estáticas

- Para verificar a configuração da rota estática:
 - **Passo 1** - *show running-config*
 - **Passo 2** - verificar se a rota estática foi inserida corretamente
 - **Passo 3** - *show ip route*
 - **Passo 4** - verificar se a rota foi adicionada na tabela de roteamento
 - **Passo 5** - utilizar o comando *ping* para verificar se os pacotes conseguem alcançar o destino e que o caminho de regresso está funcionado.



Dúvidas



- <https://www.youtube.com/watch?v=AEvZ9A-dJP8> – acedido em fevereiro de 2023

Serviços de Rede 1 – **Aula 2 - Práticas**

2022-2023

Instituto Politécnico de Coimbra

Departamento de Engenharia Informática



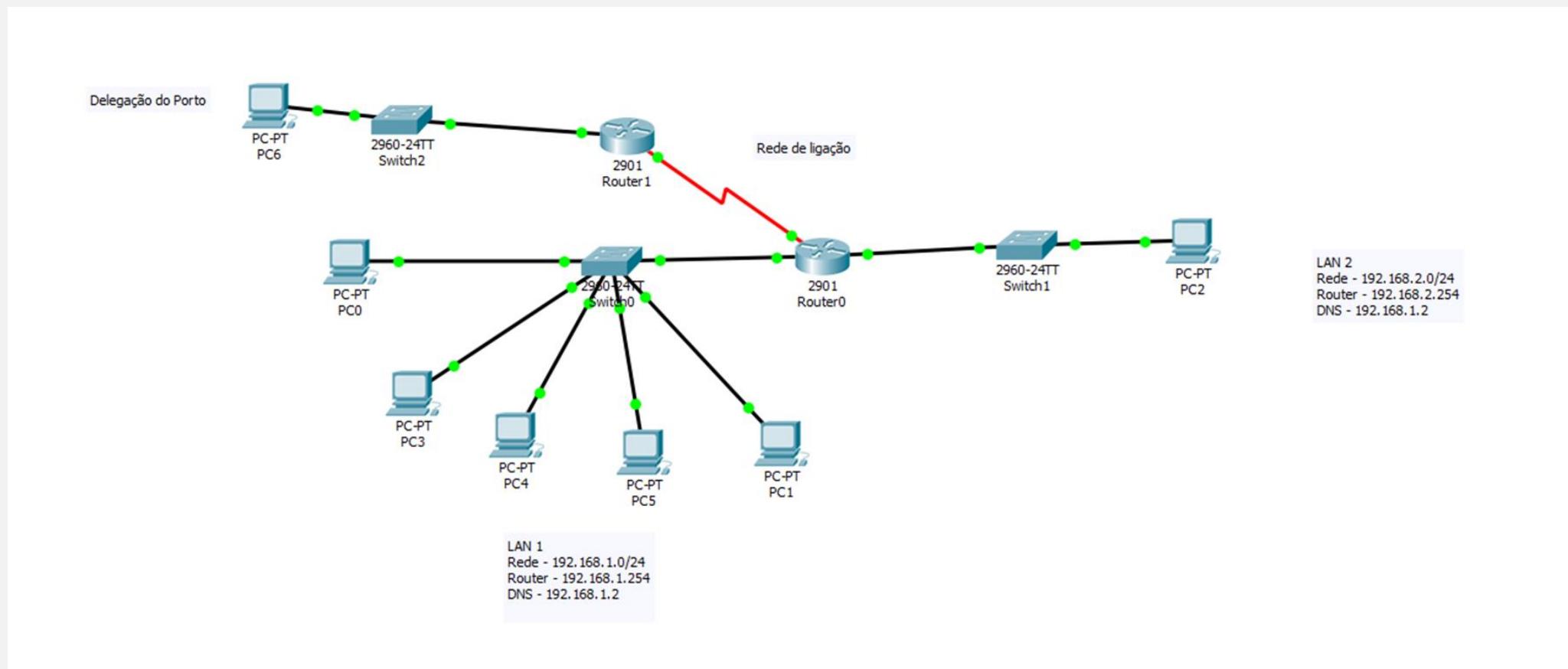
Pre – Requisitos

- Ter instalado o *Cisco Packet Tracer* versão 8.2.0



Pre-Requisito

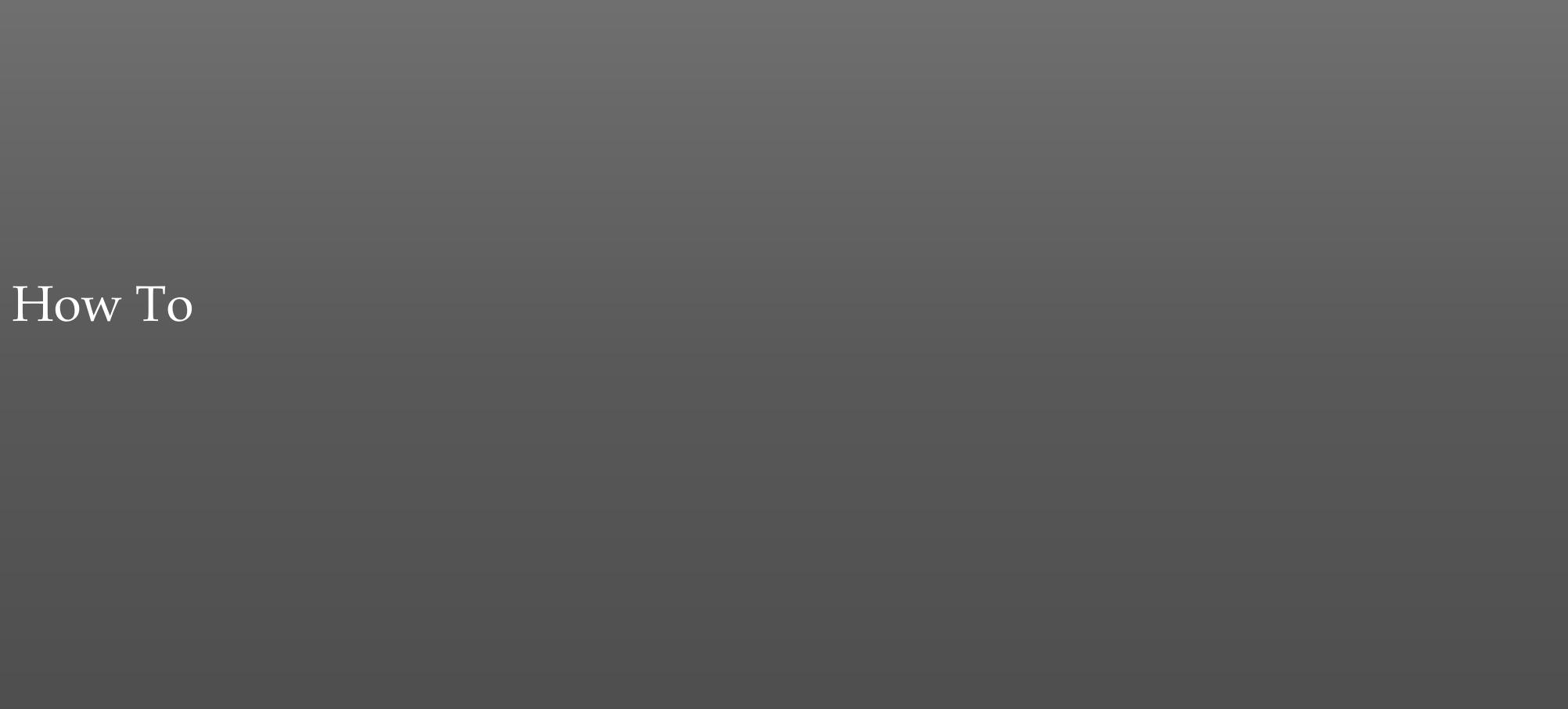
- Garanta que a topologia do exercício 3 da aula passada está a funcionar:



Exercício 1 – Configurar o serviço DHCP num router

Exercício 1

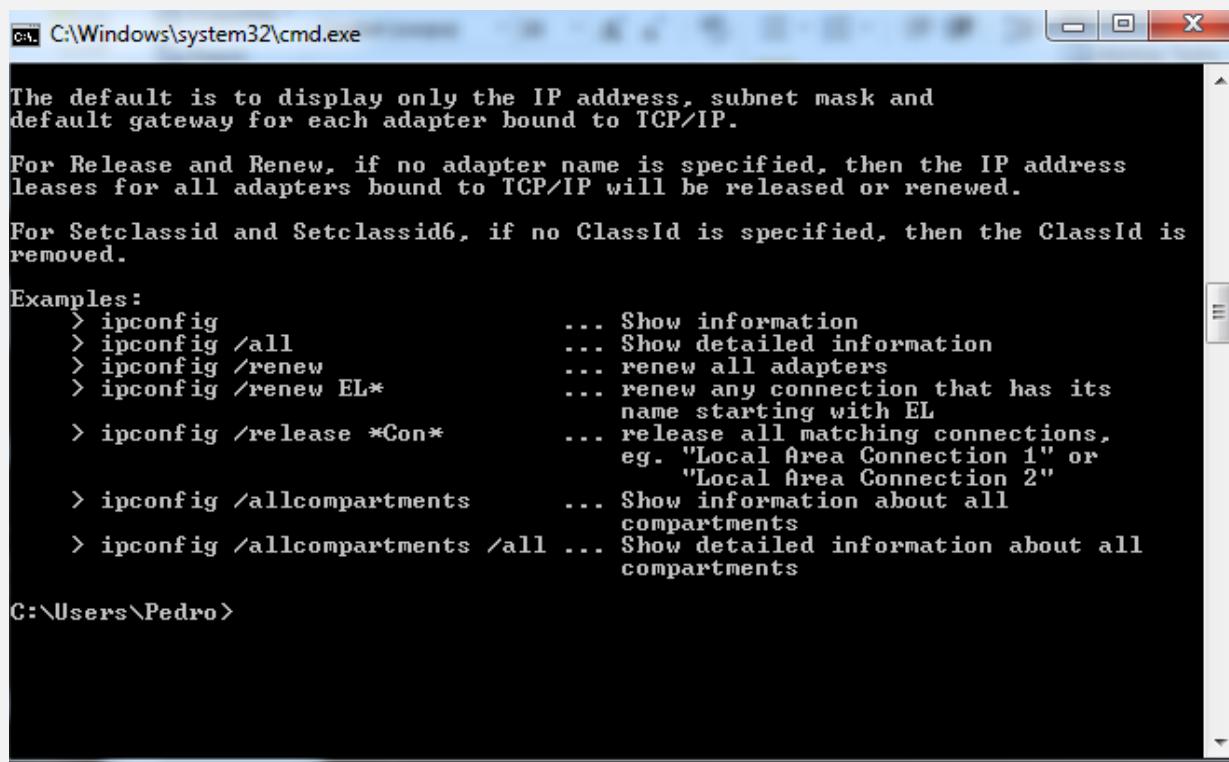
- Configure no router 0 o serviço DHCP para a LAN1 (todos os PC devem ter endereço automático e configurações básicas de rede). Deve ter as seguintes definições:
 - Nome da pool - LAN1.
 - Os endereços disponíveis para os PC devem ser do 10 ao 253.
 - O *default-gateway* é o último endereço disponível da rede.
- Verifique que todos os equipamentos estão corretamente configurados e que tem acesso aos recursos de rede.
- Configure no router 0 o serviço DHCP para a LAN2 (todos os PC devem ter endereço automático e configurações básicas de rede). Deve ter as seguintes definições:
 - Nome da pool - LAN2
 - Os endereços disponíveis para os PC devem ser do 1 ao 253.
 - O *default-gateway* é o último endereço disponível da rede
- Verifique se a sua rede continua funcional.
- Configure no router 0 o DHCP para a rede local da delegação do Porto:
 - Nome da pool - Porto
 - Os endereços disponíveis para os PC devem ser do 50 ao 100.
 - O *default-gateway* é o último endereço disponível da rede
- Verifique se a sua rede continua funcional.



How To

DHCP (Cliente)

- Num cliente para saber/alterar a configuração IP pode/deve utilizar estes comandos:
 - *Ipconfig /all*
 - *Ipconfig /renew*
 - *Ipconfig /release*



The default is to display only the IP address, subnet mask and default gateway for each adapter bound to TCP/IP.

For Release and Renew, if no adapter name is specified, then the IP address leases for all adapters bound to TCP/IP will be released or renewed.

For Setclassid and Setclassid6, if no ClassId is specified, then the ClassId is removed.

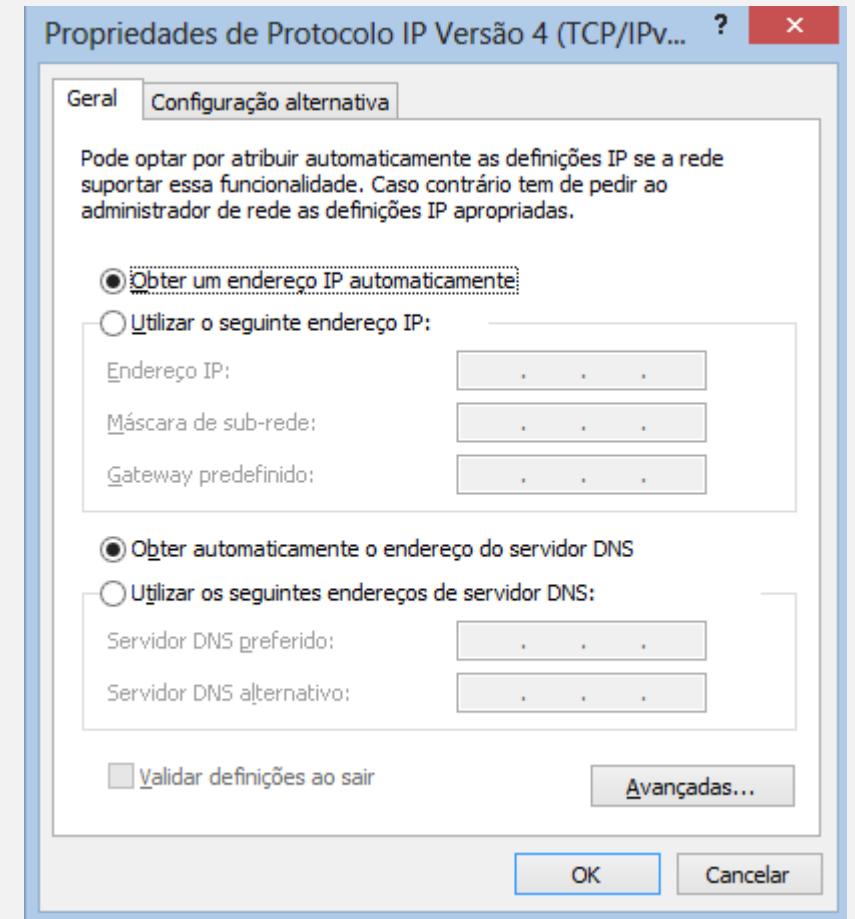
Examples:

> ipconfig	... Show information
> ipconfig /all	... Show detailed information
> ipconfig /renew	... renew all adapters
> ipconfig /renew EL*	... renew any connection that has its name starting with EL
> ipconfig /release *Con*	... release all matching connections, eg. "Local Area Connection 1" or "Local Area Connection 2"
> ipconfig /allcompartments	... Show information about all compartments
> ipconfig /allcompartments /all	... Show detailed information about all compartments

C:\Users\Pedro>

DHCP (Cliente)

- Na configuração do cliente pode definir quais os parâmetros que são obtidos de forma automática (DHCP) ou manual.



Configuração DHCP (Cisco)

- Passos de configuração
 - Activar o serviço: **service dhcp**
 - Por omissão, está activo
 - Definir um intervalo de endereços para ser usado na atribuição dinâmica
 - Poderão ser indicadas excepções – endereços ou conjunto de endereços pertencentes ao intervalo mas que não devem ser atribuídos
 - Criar uma *pool*
 - Usar o comando **ip dhcp pool**
 - Configurar parâmetros específicos da *pool* (default Gateway, servidores de DNS, etc)

Configuração DHCP (Cisco)

Configuring DHCP Step 1: Excluding IP Addresses

```
R1(config)#ip dhcp excluded-address low-address [high-address]
```

```
R1(config)#ip dhcp excluded-address 192.168.10.1 192.168.10.9  
R1(config)#ip dhcp excluded-address 192.168.10.254
```

Configuring DHCP Step 2: Configuring a DHCP Pool

```
R1(config)#ip dhcp pool pool-name
```

```
R1(config)#ip dhcp pool LAN-POOL-1  
R1(dhcp-config)#

```

Configuração DHCP (Cisco)

Configuring DHCP Step 3: Specific Tasks

Required Tasks	Command
Define the address pool	<code>network network-number [mask /prefix-length]</code>
Define the default router or gateway	<code>default-router address [address2...address8]</code>

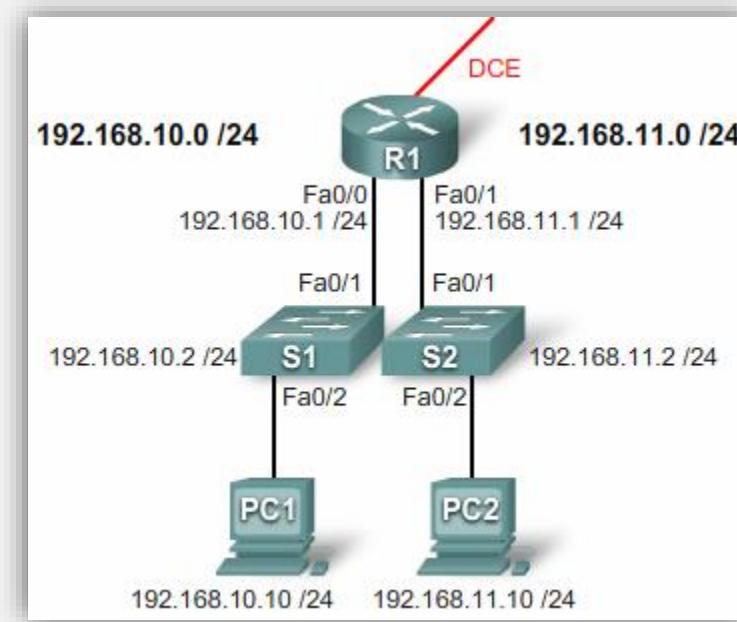
Optional Tasks	Command
Define a DNS server.	<code>dns-server address [address2...address8]</code>
Define the domain name	<code>domain-name domain</code>
Define the duration of the DHCP lease	<code>lease { days [hours] [minutes] infinite}</code>
Define the NetBIOS WINS server	<code>netbios-name-server address [address2...address8]</code>

DHCP Configuration Example

```
R1(config)# ip dhcp excluded-address 192.168.10.1 192.168.10.9
R1(config)# ip dhcp excluded-address 192.168.10.254
R1(config)# ip dhcp pool LAN-POOL-1
R1(dhcp-config)# network 192.168.10.0 255.255.255.0
R1(dhcp-config)# default-router 192.168.10.1
R1(dhcp-config)# domain-name span.com
R1(dhcp-config)# end
```

Configuração DHCP (Cisco)

- Um router pode possuir várias ‘pools’ configuradas,
- A escolha da ‘pool’ a usar para a atribuição dinâmica de informação IP é efectuada tendo por base o interface que recebe o pedido de DHCP (mensagem DHCPDISCOVER).



Verificação de configuração DHCP (Cisco)

- Alguns comandos usados para verificar a configuração (alguns podem não estar disponíveis no Packet Tracer):

- show ip dhcp binding** – informação sobre os clientes que estão a utilizar o serviço de DHCP.
- show ip dhcp server statistics** – mostra estatísticas do serviço, por exemplo quantos pacotes de DHCP foram transmitidos/recebidos (não disponível no simulador).
- show ip dhcp pool** – mostra informações sobre a pool que foi criada.
- clear ip dhcp binding {address | *}** – limpa uma entrada do DHCP.
- clear ip dhcp server statistics** – limpa as estatísticas

```
R1#sho ip dhcp binding
Bindings from all pools not associated with VRF:
  IP address          Client-ID/          Lease expiration      Type
                                         Hardware address/
                                         User name
 192.168.10.10        0100.e018.5bdd.35   Oct 03 2007 06:14 PM  Automatic
 192.168.11.10        0100.b0d0.d817.e6   Oct 03 2007 06:18 PM  Automatic

R1#sho ip dhcp server statistics
Memory usage           25307
Address pools          2
Database agents         0
Automatic bindings      2
Manual bindings         0
Expired bindings        0
Malformed messages      0
Secure arp entries      0

Message                Received
BOOTREQUEST             0
DHCPDISCOVER              8
DHCPREQUEST                  3
DHCPDECLINE                  0
DHCPRELEASE                   0
DHCPINFORM                     0

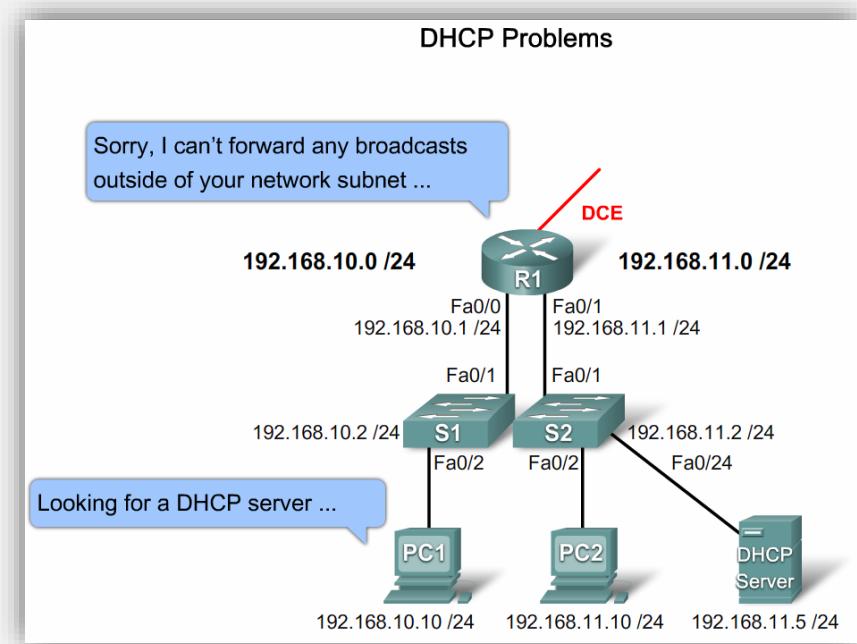
Message                Sent
BOOTREPLY                 0
DHCPOFFER                  3
DHCPACK                      3
DHCPNAK                      0
R1#

R1#show ip dhcp pool
Pool LAN-POOL-1 :
  Utilization mark (high/low) : 100 / 0
  Subnet size (first/next)    : 0 / 0
  Total addresses            : 254
  Leased addresses           : 1
  Pending event               : none
  1 subnet is currently in the pool :
    Current index      IP address range          Leased addresses
    192.168.10.11       192.168.10.1 - 192.168.10.254      1

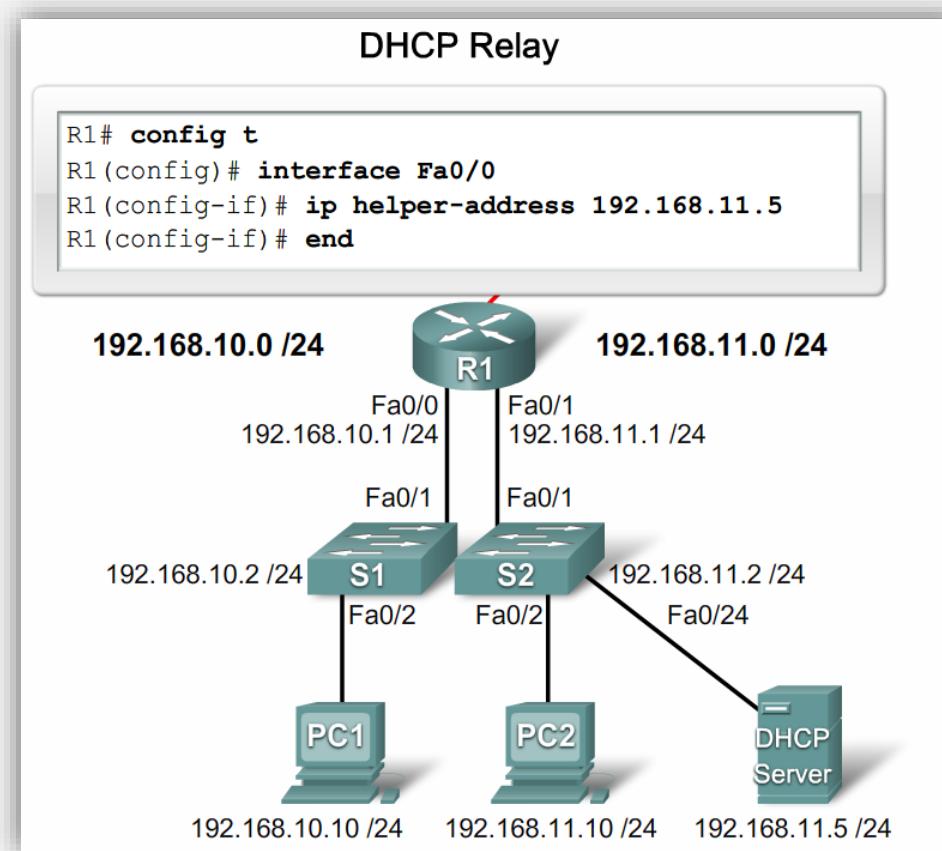
Pool LAN-POOL-2 :
  Utilization mark (high/low) : 100 / 0
  Subnet size (first/next)    : 0 / 0
  Total addresses            : 254
  Leased addresses           : 1
  Pending event               : none
  1 subnet is currently in the pool :
    Current index      IP address range          Leased addresses
    192.168.11.11       192.168.11.1 - 192.168.11.254      1
R1#
```

DHCP Relay

- Um cliente DHCP utiliza mecanismos de broadcast para localizar o DHCP e solicitar as configurações TCP/IP.
- Os routers por defeito não encaminham este tipo tráfego. Ou seja, os clientes só poderão obter as configurações do TCP/IP caso o servidor DHCP esteja localizado na mesma rede local.
- Pode haver situações na qual o servidor DHCP está localizado em uma outra sub-rede, ou seja, localizado em uma outra rede local. Nesse caso, deveremos configurar um DHCP Relay Agent na rede onde não existe o servidor DHCP.
- O DHCP Relay Agent pega nos pacotes enviados pelos clientes DHCP, transforma esses pacotes num formato que o router os possa encaminhar para o servidor DHCP, ou seja, é um intermediário entre os clientes DHCP e o servidor DHCP.



DHCP Relay - Cisco



Configurando uma *interface* Ethernet

```
R1(config)#interface fastethernet 0/0  
R1(config-if)#ip address 172.16.1.254 255.255.255.0  
R1(config-if)#no shutdown
```

```
*Mar 1 01:16:08.212: %LINK-3-UPDOWN: Interface FastEthernet0/0, changed state to up  
*Mar 1 01:16:09.214: %LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet0/0, changed  
state to up
```

```
R1#show interfaces fastethernet 0/0  
FastEthernet0/0 is up, line protocol is up  
    Hardware is AmdFE, address is 000c.3010.9260 (bia 000c.3010.9260)  
    Internet address is 172.16.3.1/24
```

```
R1#
```

Configuração de uma *Interface Serial*

- Configuração base

Identificação do endereço IP e máscara

Identificação da interface a configurar

```
Router> enable
Router# configure terminal
Router(config)# interface serial0
Router(config-if)# description Delegação - Porto
Router(config-if)# ip address <ip address> <netmask>
Router(config-if)# clock rate 56000
Router(config-if)# no shutdown
```

Activação administrativa da interface

Nas interfaces série quando o router actua como DCE (i.e. assume o papel de CSU/DSU) é necessário gerar relógio. Ritmos (bps) válidos: 1200, 2400, 9600, 19200, 38400, 56000, 64000, 72000, 125000, 148000, 500000, 800000, 1000000, 1300000, 2000000, 4000000.

Rotas Estáticas

- **Comando *ip route***

- Para configurar uma rota estática utiliza-se o seguinte comando:

```
Router(config)# ip route network-address subnet-mask  
{ip-address | exit-interface }
```

Parâmetro	Descrição
network-address	Endereço da rede de destino da rede remota a ser adicionado à tabela de roteamento.
subnet-mask	Máscara de sub-rede da rede remota a ser adicionada à tabela de roteamento. A máscara de sub-rede pode ser modificada para sumarizar um grupo de redes.
ip-address	Normalmente conhecido como o endereço IP do roteador do próximo salto.
exit-interface	Interface de saída usada no encaminhamento de pacotes para a rede de destino.

Rotas Estáticas

- Rotas estáticas configuradas com uma interface de saída são mais eficientes.
- A tabela de *routing* pode identificar a interface de saída em uma única consulta, ao invés de duas quando utiliza o endereço IP.

```
R1(config)#no ip route 192.168.2.0 255.255.255.0 172.16.2.2
R1(config)#ip route 192.168.2.0 255.255.255.0 serial 0/0/0
R1(config)#end
R1#show ip route
Codes: C - connected, S - static, I - IGRP, R - RIP, M - mobile, B - BGP
      D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
      N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
      E1 - OSPF external type 1, E2 - OSPF external type 2, E - EGP
      i - IS-IS, L1 - IS-IS level-1, L2 - IS-IS level-2, ia - IS-IS inter area
      * - candidate default, U - per-user static route, o - ODR
      P - periodic downloaded static route

Gateway of last resort is not set

      172.16.0.0/24 is subnetted, 3 subnets
S        172.16.1.0 [1/0] via 172.16.2.2
C        172.16.2.0 is directly connected, Serial0/0/0
C        172.16.3.0 is directly connected, FastEthernet0/0
S        192.168.1.0/24 [1/0] via 172.16.2.2
S        192.168.2.0/24 is directly connected, Serial0/0/0
```

Agora a interface de saída está especificada na rota estática. Não há necessidade de uma pesquisa recursiva.

Não se esqueça de utilizar a rota por defeito...

Modificando Rotas Estáticas

- As rotas estáticas existentes não podem ser modificadas. Uma rota antiga deve ser removida colocando um **no** antes do comando **ip route**.

no ip route 192.168.2.0 255.255.255.0 serial 0/0/1

A nova rota estática deve ser reescrita na configuração do router:

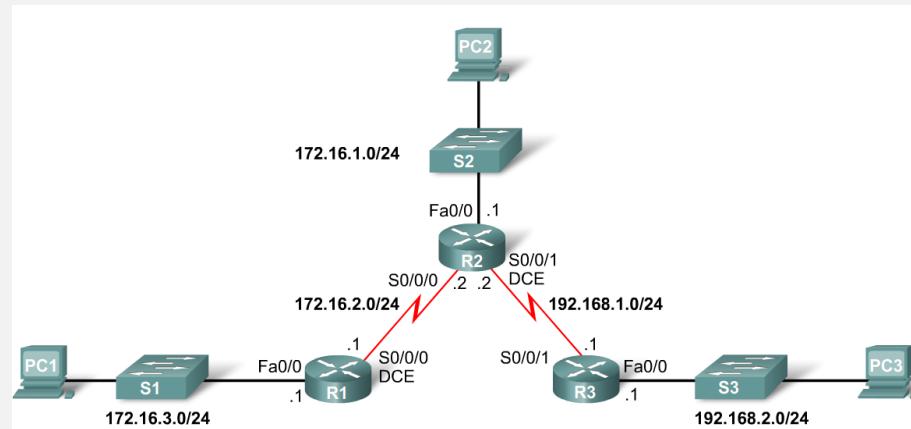
```
R1(config)#no ip route 172.16.1.0 255.255.255.0 172.16.2.2
R1(config)#ip route 172.16.1.0 255.255.255.0 serial 0/0/0
R1(config)#no ip route 192.168.1.0 255.255.255.0 172.16.2.2
R1(config)#ip route 192.168.1.0 255.255.255.0 serial 0/0/0
```

```
R2(config)#no ip route 172.16.3.0 255.255.255.0 172.16.2.1
R2(config)#ip route 172.16.3.0 255.255.255.0 serial 0/0/0
R2(config)#no ip route 192.168.2.0 255.255.255.0 192.168.1.1
R2(config)#ip route 192.168.2.0 255.255.255.0 serial 0/0/1
```

```
R3(config)#no ip route 172.16.1.0 255.255.255.0 192.168.1.2
R3(config)#ip route 172.16.1.0 255.255.255.0 serial 0/0/1
R3(config)#no ip route 172.16.2.0 255.255.255.0 192.168.1.2
R3(config)#ip route 172.16.2.0 255.255.255.0 serial 0/0/1
R3(config)#no ip route 172.16.3.0 255.255.255.0 192.168.1.2
R3(config)#ip route 172.16.3.0 255.255.255.0 serial 0/0/1
```

Verificar as Rotas Estáticas

- Para verificar a configuração da rota estática:
 - Utilize os seguintes comandos:
 - **Passo 1** - *show running-config*
 - **Passo 2** - verificar se a rota estática foi inserida corretamente
 - **Passo 3** - *show ip route*
 - **Passo 4** - verificar se a rota foi adicionada na tabela de roteamento
 - **Passo 5** - utilizar o comando *ping* para verificar se os pacotes conseguem alcançar o destino e que o caminho de regresso está funcionado.

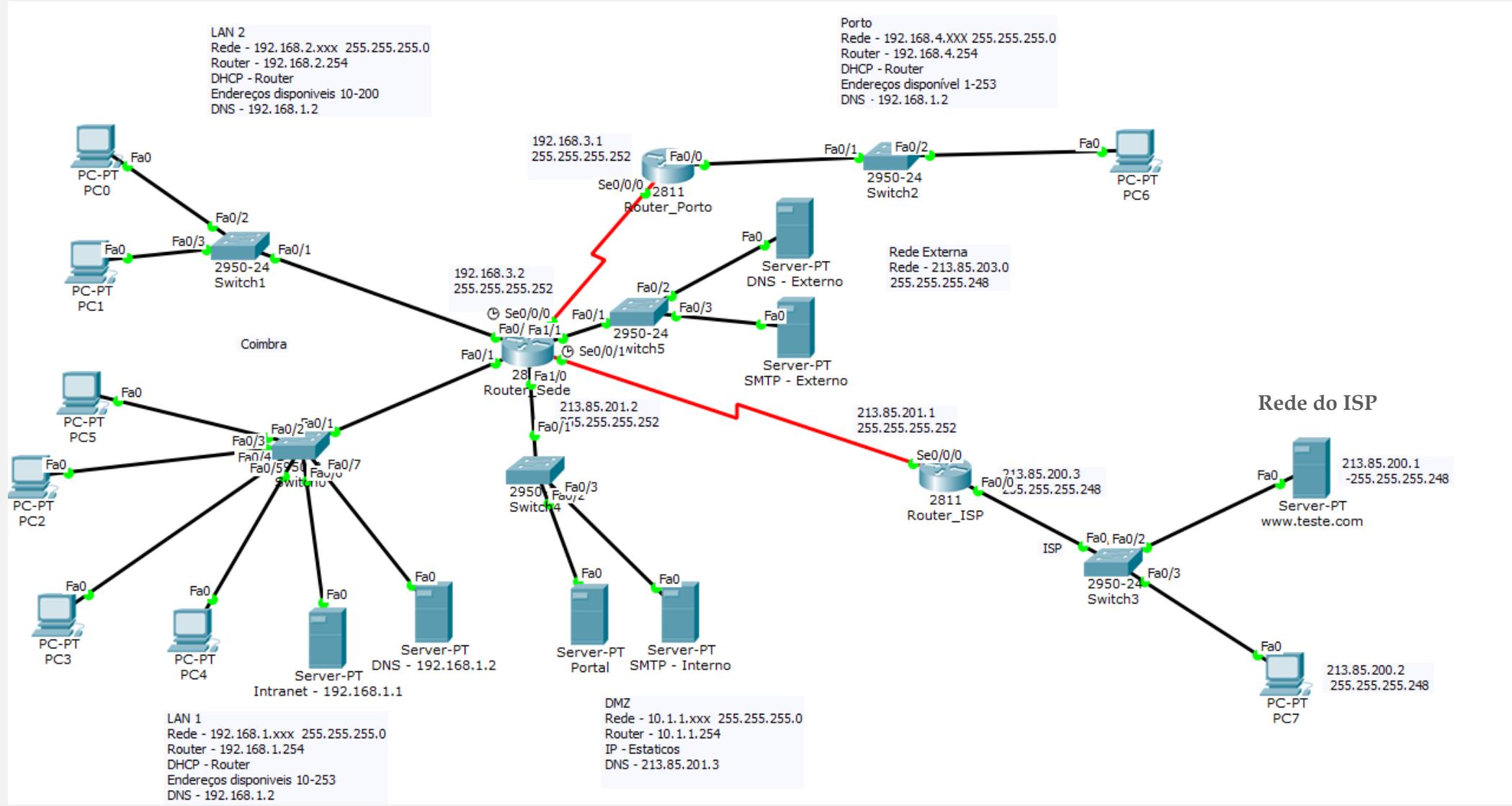


Exercício 2 – Configurar uma rede alargada

Exercício 2

- A empresa SR1 SA tem uma rede com a topologia indicada na figura na página seguinte (a topologia de rede tem como base o exercício anterior).
 - Na sede tem duas LAN (LAN1 e LAN2), uma DMZ e uma zona exterior.
 - Os endereços das redes são os seguintes:
 - LAN 1 - 192.168.1.0 - 255.255.255.0
 - LAN 2 - 192.168.2.0 - 255.255.255.0
 - DMZ - 10.1.1.0 - 255.255.255.0
 - Zona externa - 213.85.203.0 - 255.255.255.248
 - A rede LAN 1 e 2 têm os IP fornecidos por DHCP no router.
 - Na DMZ e zona externa os IP são fixos.
 - Tem uma delegação no Porto com a rede 192.168.4.0 - 255.255.255.0. Os IP são dados por DHCP configurado no router da sede.
 - A rede do ISP é 213.85.200.0 - 255.255.255.248 e os IP são fixos.
 - As redes de ligação são as seguintes:
 - Sede - Porto -> 192.168.3.1 - 255.255.255.252
 - Porto - Sede -> 192.168.3.2 - 255.255.255.252
 - Sede - Internet -> 213.85.201.1 - 255.255.255.252
 - Internet - Sede -> 213.85.201.2 - 255.255.255.252
- Garanta que a sua rede está funcional e que todos os PC (sede e Porto) acedem à rede interna e DMZ configurando a sua simulação igual à da imagem anterior seguindo todos as condições lá indicadas.

Exercício 2

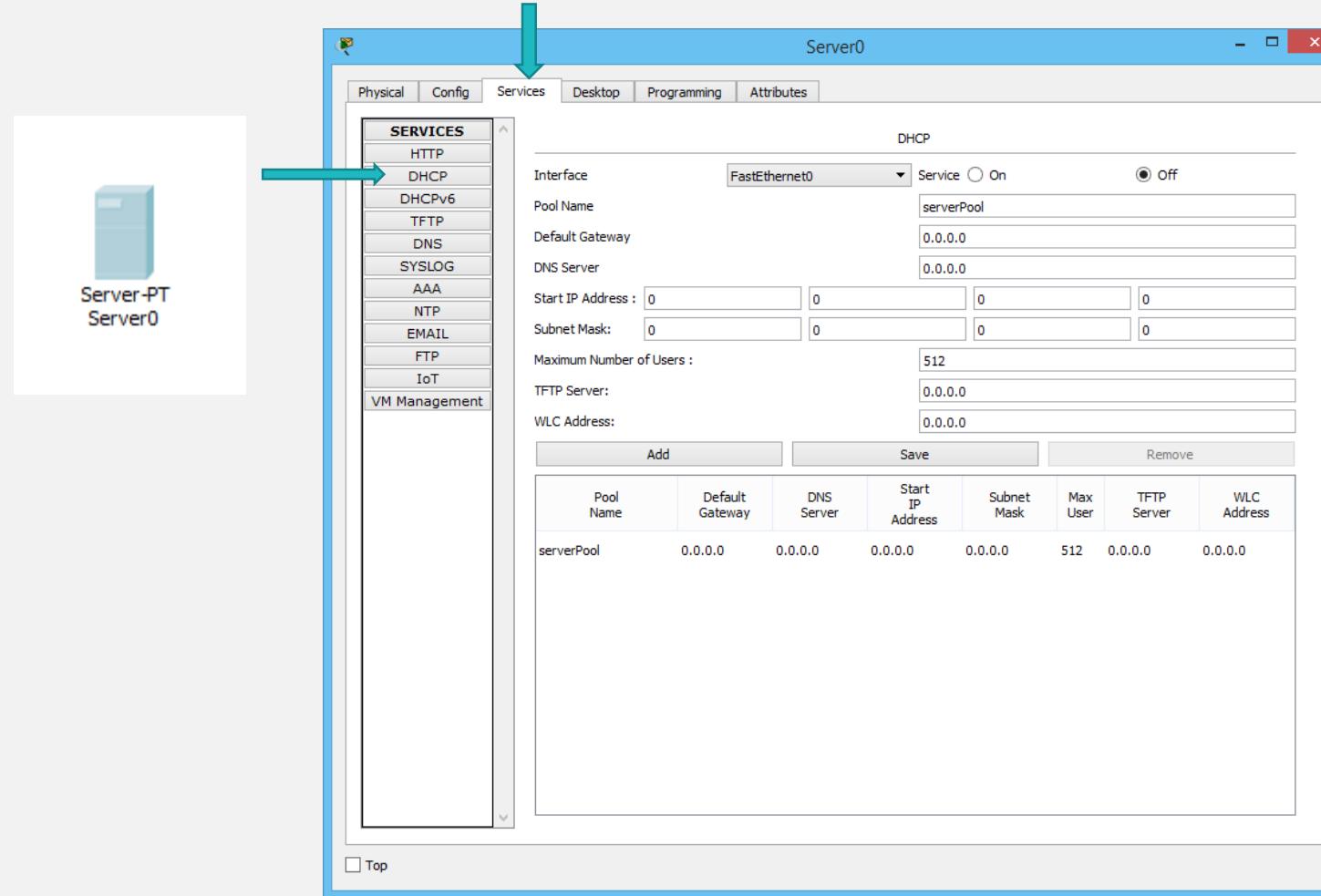


Exercício 2

- A empresa abriu uma nova delegação em Lisboa. Todos os serviços vão ficar centrados em Coimbra, ou seja só vão existir postos de trabalho na nova delegação.
 - IP da LAN – 192.168.5.0
 - IP do Router – 192.168.5.254
 - DNS – 192.168.1.2
- Deve:
 - Ligar esta nova delegação a Coimbra utilizando uma ligação Serie.
 - Configurar um par de endereços IP para esta ligação. Utilizar a rede seguinte à que foi utilizada para a ligação ao Porto.
 - Colocar 4 PCs. Dar um IP estático a um deles, fazer as alterações necessárias na rede e testar se tudo funciona.
 - Colocar um servidor de DHCP na sede em Coimbra com o endereço 192.168.1.3. Este servidor deverá ter as seguintes características
 - Pool de Lisboa – Inicio 192.168.5.10 – Máximo 250 utilizadores.
 - Pool do Porto – Inicio 192.168.4.10 – Máximo de utilizadores 50.
 - Não esquecer a informação do gateway e DNS (192.168.1.2).
 - Anular no router da sede o DHCP para Lisboa e Porto.
 - Garantir que tanto os PCs de Lisboa e do Porto tem endereços “dados” pelo servidor DHCP que está na rede. Os IP das redes da sede (LAN1 e LAN2) continuam a ser dados pelo router central.
- Teste toda a rede e verifique que tudo está a funcionar corretamente.
- Entre em modo de simulação e “siga” o processo de atribuição de um IP por DHCP. Veja o formato dos pacotes que são trocados entre os terminais e o servidor.

How To

Packet Tracer - Servidor DHCP



Dúvidas



Serviços de Rede 1 – **Aula 3 - Práticas**

2022-2023

Instituto Politécnico de Coimbra

Departamento de Engenharia Informática



Exercício 1

- Se estiver a trabalhar remotamente, estabeleça a ligação por VPN para aceder aos recursos do ISEC.
- Se estiver no ISEC ligado à rede local será apenas necessário aceder ao share de rede.
- Copie as imagens das máquinas virtuais e o instalador do VirtualBox.
- Instale o VirtualBox.
- Arranque com o VirtualBox.
- Importe as imagens do Windows 2012 Server e do Windows 10.
- Altere o nome das máquinas no VirtualBox para:
 - Windows2012r2 para “Servidor2023”.
 - Windows 10 para “Cliente2023”.
- Ajuste alguns parâmetros (RAM, Disco, etc) para aumentar o desempenho das maquias virtuais. Este “ajuste” está dependente das características da maquina hospedeira (ou seja do seu PC).

How To

Configurar o ambiente de simulação

- Para aceder às imagens das máquinas **e se estiver em regime remoto**, tem de aceder à VPN do ISEC. Em my.isec.pt tem uma explicação de como o fazer.
- O conceito de VPN surgiu a partir da necessidade de utilizar redes de comunicação não confiáveis (logo não seguras: como a Internet) para a transmissão de dados privados de uma forma segura.
- A ligação é efetuada através da criação de um túnel encriptado sobre a rede pública de comunicações para garantir mecanismos de segurança e confidencialidade da informação.
- O ISEC usa a solução openVPN que terá assim de instalar o cliente no seu computador.

Configurar o ambiente de simulação

1 Aceder a my.isec.pt



2

Acesso VPN



Open VPN UDP (standard)

Open VPN TCP 443

Para utilizar a VPN do ISEC deve:

1. Fazer o download do cliente OpenVPN e instalar, <https://openvpn.net>
2. Fazer o download do ficheiro de configuração e copiá-lo para a directória "config".
Exemplo: C:\Program Files\OpenVPN\config
3. Executar o Cliente OpenVPN, escolher a opção Ligar/Connect e introduzir as suas credenciais de acesso ao domínio ISEC.

Caso tenha dúvidas sobre a instalação / configuração do OpenVPN, por favor consulte o seguinte manual: [OpenVPN-2015.pdf](#).

Qualquer questão/dúvida deve ser enviada através de um [Pedido de Manutenção](#) ou por email para sgit@isec.pt.

[Download do ficheiro de configuração](#)

3

Configurar o ambiente de simulação

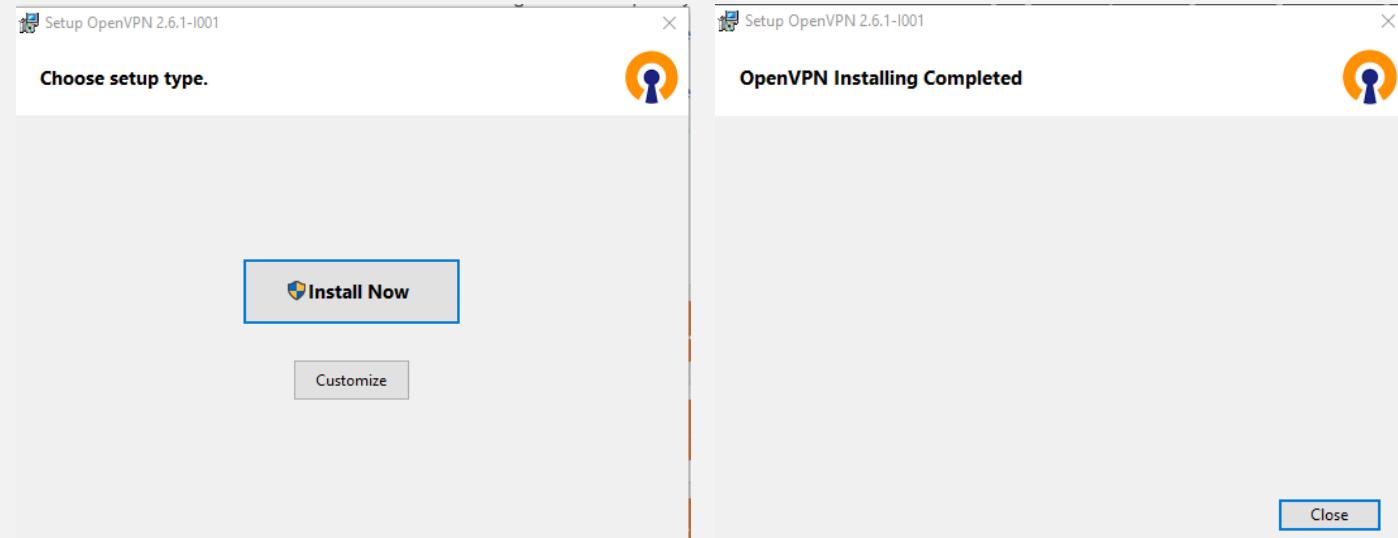
4 Aceder ao site para fazer o download do cliente da openVPN

The screenshot shows the OpenVPN website's "Community Downloads" section. At the top, there is a navigation bar with links for Solutions, Products, Pricing, Resources, Community, Get Started, and Request Demo. Below the navigation bar, a large blue header box contains the text "Community Downloads". Underneath this, there is a white box containing the text "OpenVPN 2.6.1 -- Release 8 March 2023" and a small "+" icon. Further down, there is a section titled "Windows MSI changes since 2.6.1:" with a bullet point: "Update included ovpn-dco-win driver to 0.9.2". Below this, there are four download options: "Windows 64-bit MSI installer" (GnuPG Signature, [OpenVPN-2.6.1-I001-amd64.msi](#)), "Windows ARM64 MSI installer" (GnuPG Signature, [OpenVPN-2.6.1-I001-arm64.msi](#)), "Windows 32-bit MSI installer" (GnuPG Signature, [OpenVPN-2.6.1-I001-x86.msi](#)), and "Source archive file" (GnuPG Signature, [openvpn-2.6.1.tar.gz](#)).

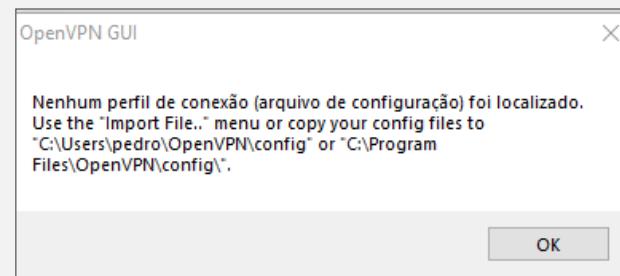
5 Escolher o instalador correto para o seu sistema operativo

Configurar o ambiente de simulação

6 Fazer a instalação do cliente



7 Ao arrancar deve dar um erro porque ainda não tem o ficheiro de configuração



Configurar o ambiente de simulação

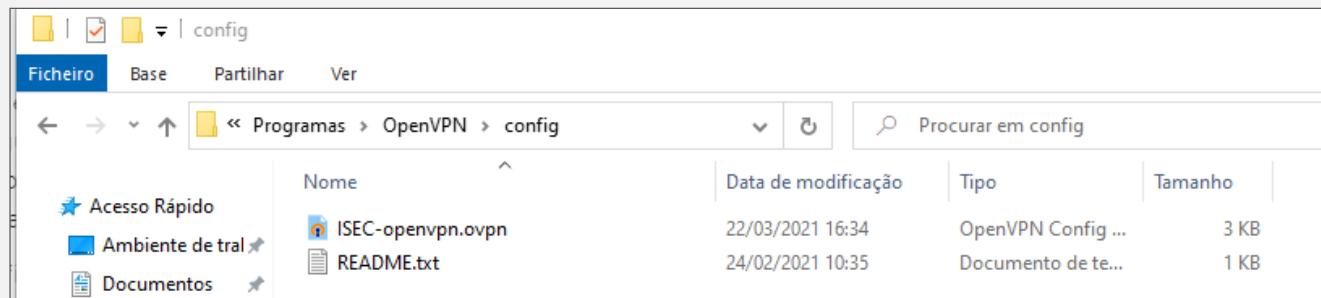
8

Em MyIsec faça o download do ficheiro de configuração.



9

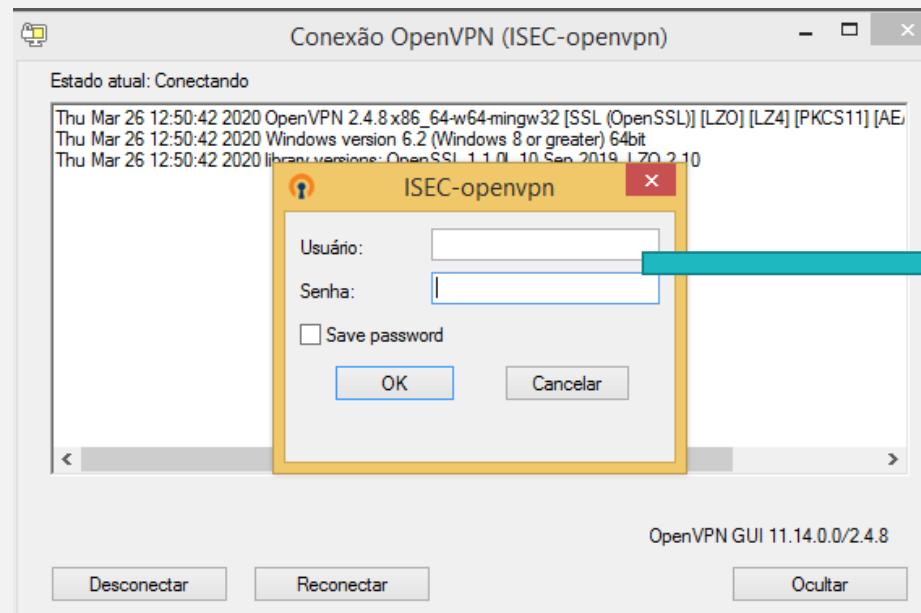
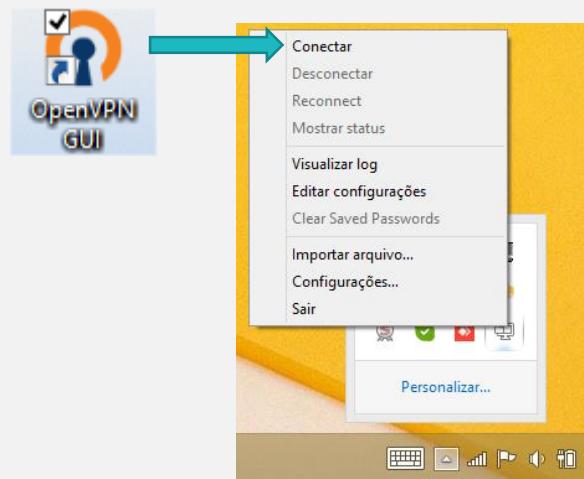
Copie o ficheiro para a pasta de configuração do OpenVPN.



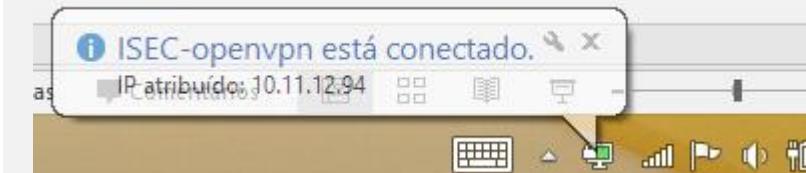
Configurar o ambiente de simulação

10

Arranque com o OpenVPN.



Nome e palavra chave que
usa no acesso ao ISEC



Copiar as imagens

Configurar o ambiente de simulação

Se estiver em modo remoto tem de ter a VPN ligada se tiver na rede do ISEC pode copiar os recursos para a sua máquina sem ter que fazer mais nada:

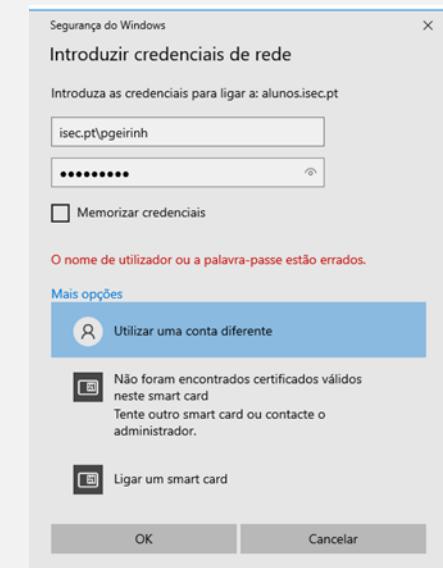
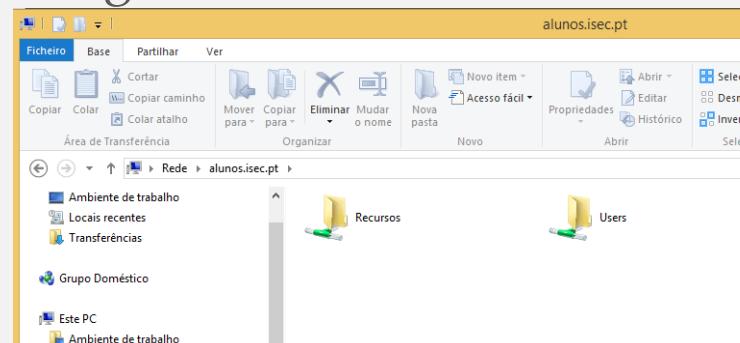
- Abra por exemplo o programa Explorador do Windows e escreva:

\alunos.isec.pt

- Se lhe pedir para se autenticar, não se esqueça de colocar a informação do domínio antes do seu nome de utilizador:

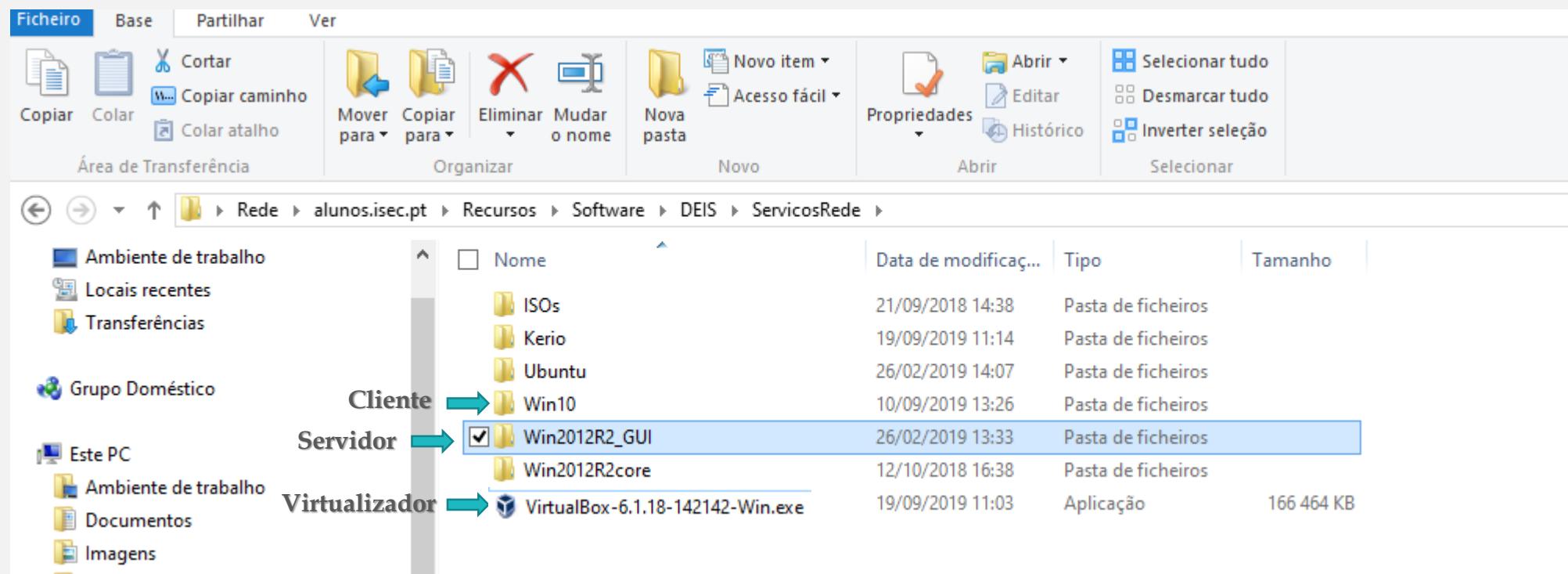
isec.pt*nome de utilizador*

- Ao aceder deve ter uma janela igual a esta:



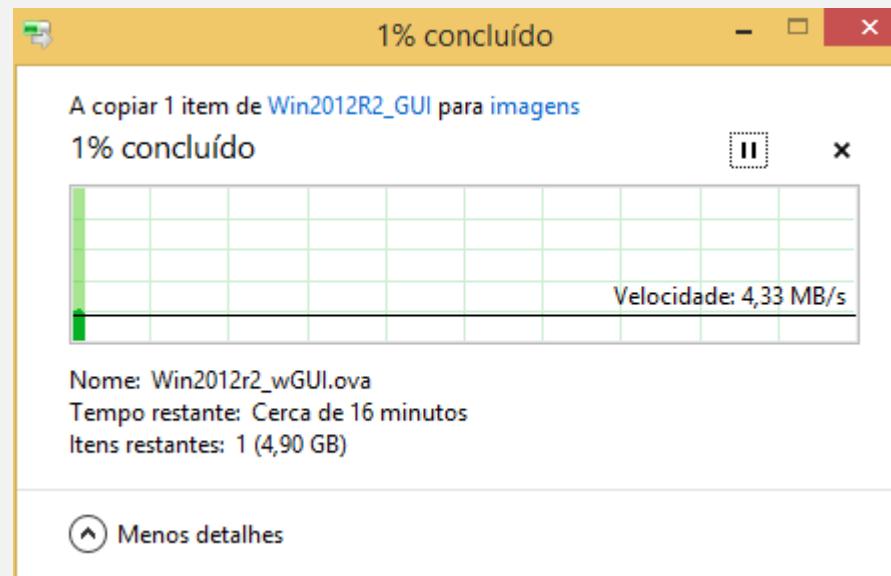
Configurar o ambiente de simulação

- As máquinas virtuais e o VirtualBox estão em:
alunos.isec.pt\Recursos\Software\DEIS\ServicosRede



Configurar o ambiente de simulação

- Copie para a sua máquina física os ficheiros indicados no slide anterior.
- Devido ao volume de informação, deverá fazê-lo de forma individual e não todos de uma vez.



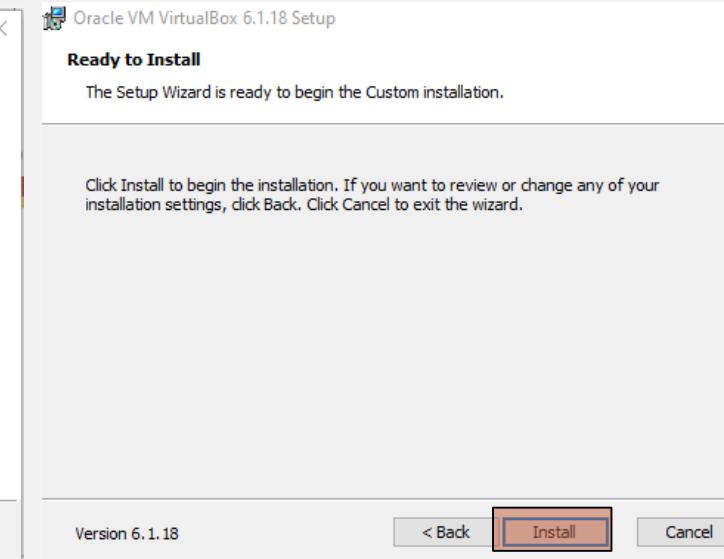
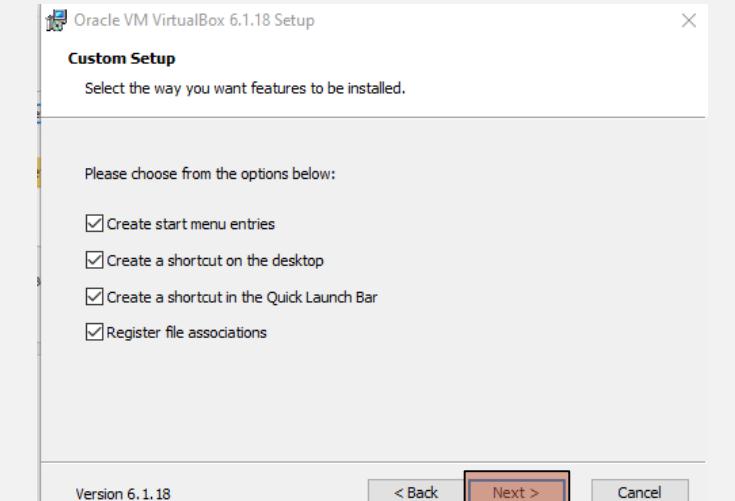
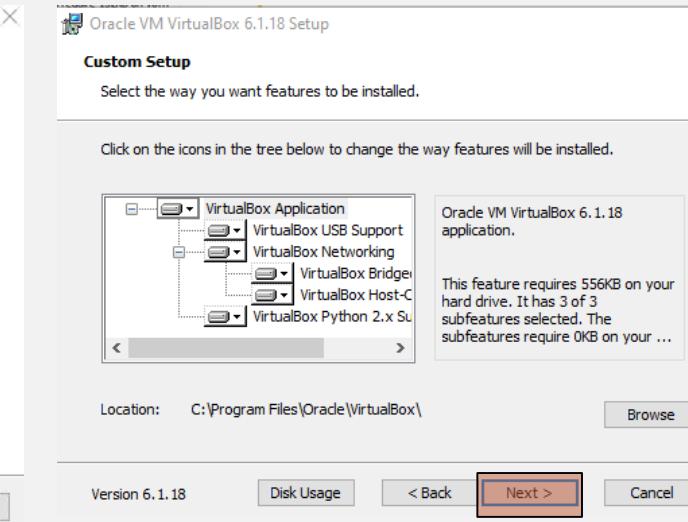
Configurar o ambiente de simulação

- Deve guardar os ficheiros OVA para sempre que necessite de uma “máquina limpa” a possa voltar a criar ou a importar.
- As imagens foram feitas para a versão 6.1.18 do VirtualBox pelo que deve ser esta a versão que deve utilizar.

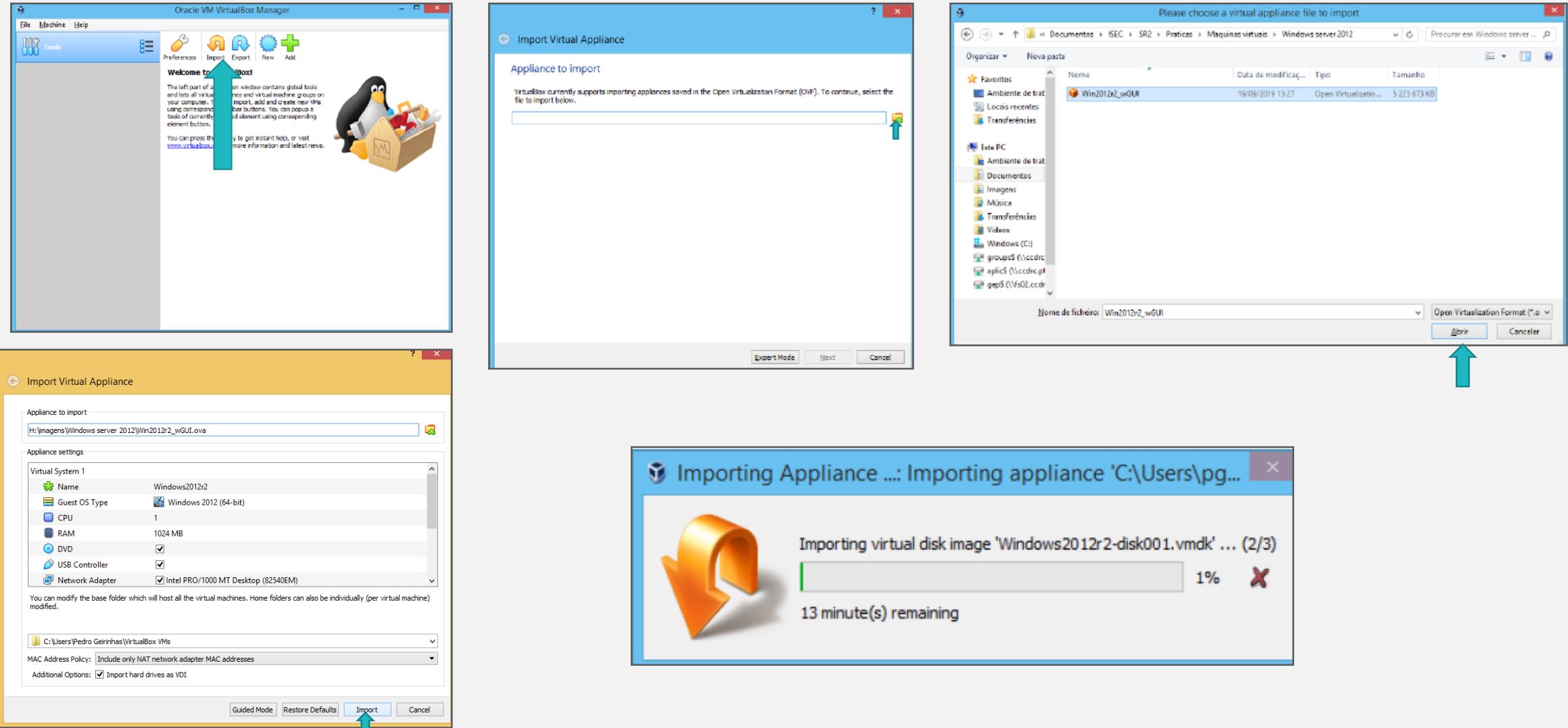
Nota: Nas imagens e exercícios das aulas práticas será utilizado o Virtual Box pelo que se aconselha a utilização desta ferramenta e não de outro virtualizador.

Instalação do VirtualBox

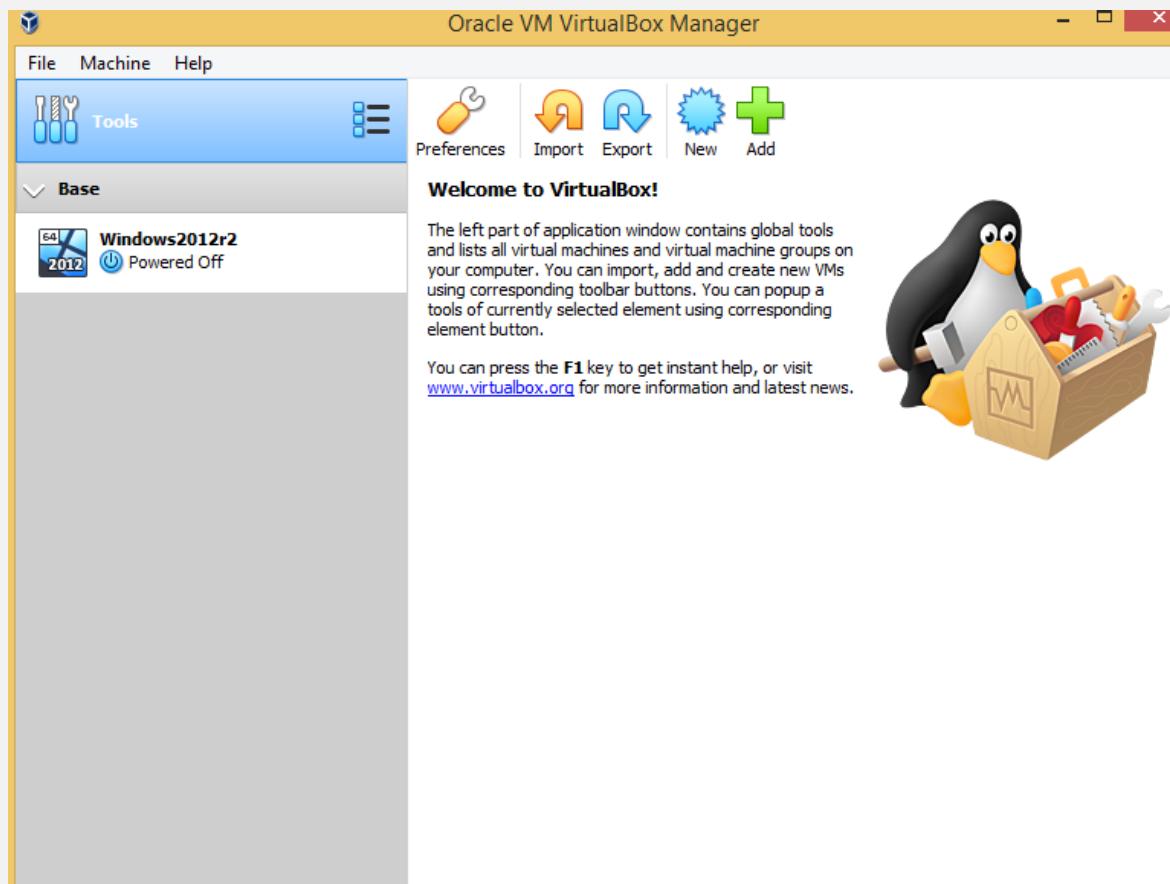
Instalação do VirtualBox



Importação de Máquinas Virtuais

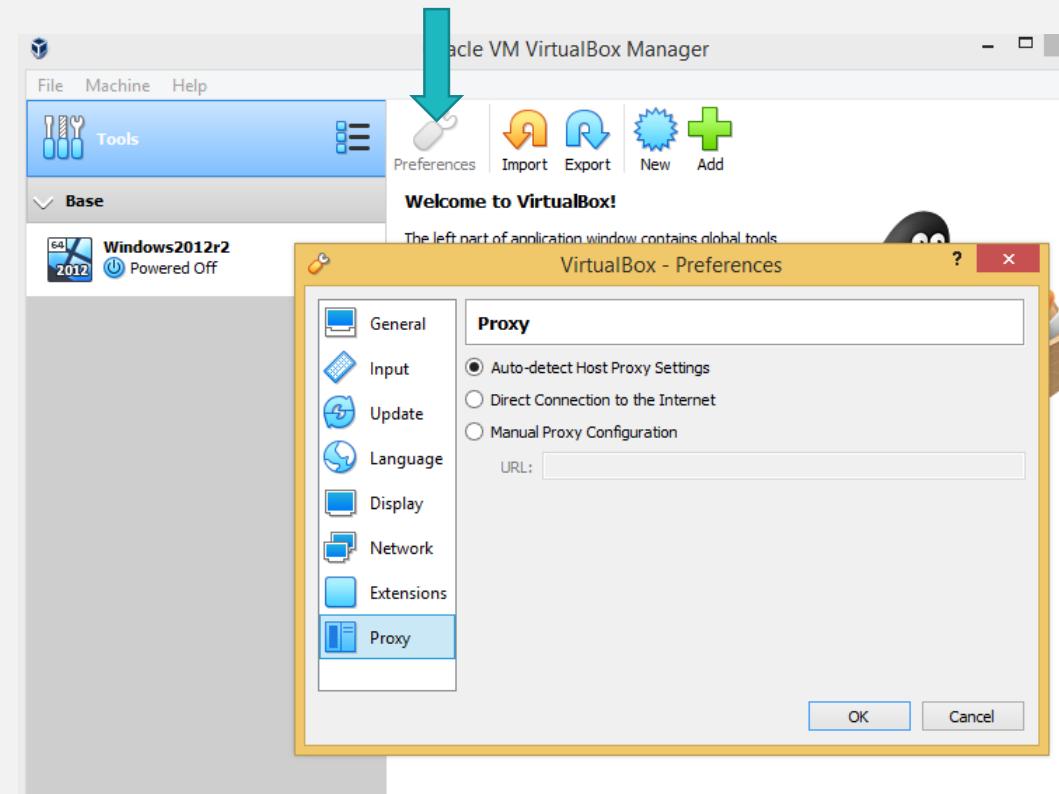
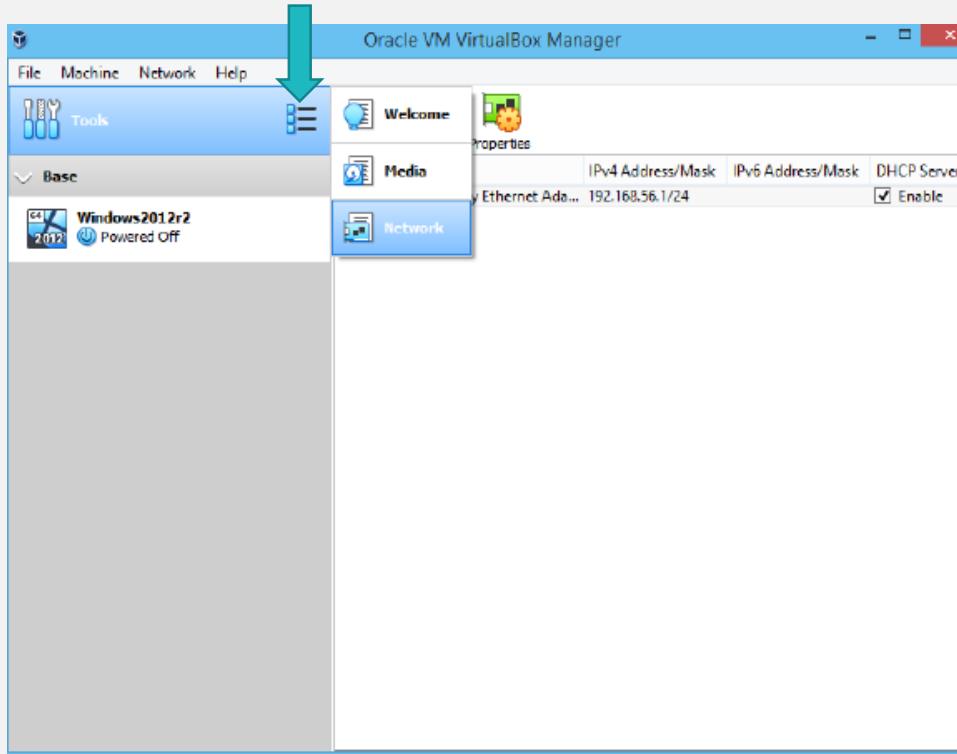


Virtual Box



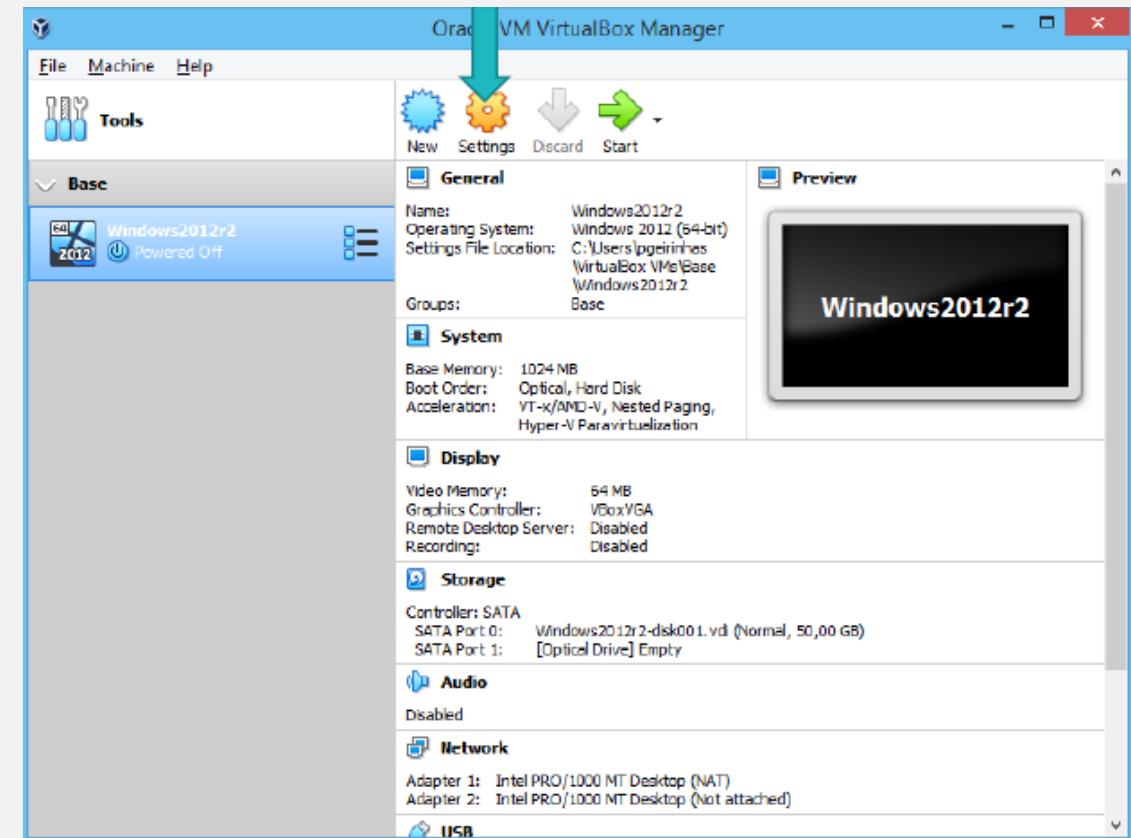
Virtual Box

- Pode gerir as opções do VirtualBox em:



Virtual Box

- Pode gerir as definições da sua máquina virtual. Por exemplo:
 - **General**: o nome da máquina.
 - **System** : RAM e CPU.
 - **Storage**: HardDisk (virtual) e CD/DVD
 - **Network**: Interfaces de rede.
 - **Shared Folder** : permite configurar uma pasta para partilhar informação entre a máquina física e a virtual. É importante para que possa copiar ficheiros entre a máquina física e a virtual.



Virtual Box

The image displays three side-by-side screenshots of the VirtualBox software interface, showing configuration options for virtual machines.

- General:** Shows basic information like Name (Server), Type (Microsoft Windows), and Version (Windows 2012 (64-bit)).
- System:** Shows system-level configurations including Base Memory (4 MB to 1024 MB), Boot Order (Floppy, Optical, Hard Disk, Network), Chipset (PIIX3), Pointing Device (USB Tablet), and Extended Features (Enable I/O APIC, Enable EFI, Hardware Clock in UTC Time).
- Network:** Shows network adapter settings for Adapter 1 (Attached to Internal Network, Adapter Type Intel PRO/1000 MT Desktop (82540EM), MAC Address 080027451E39, Promiscuous Mode Deny, Cable Connected, Port Forwarding).

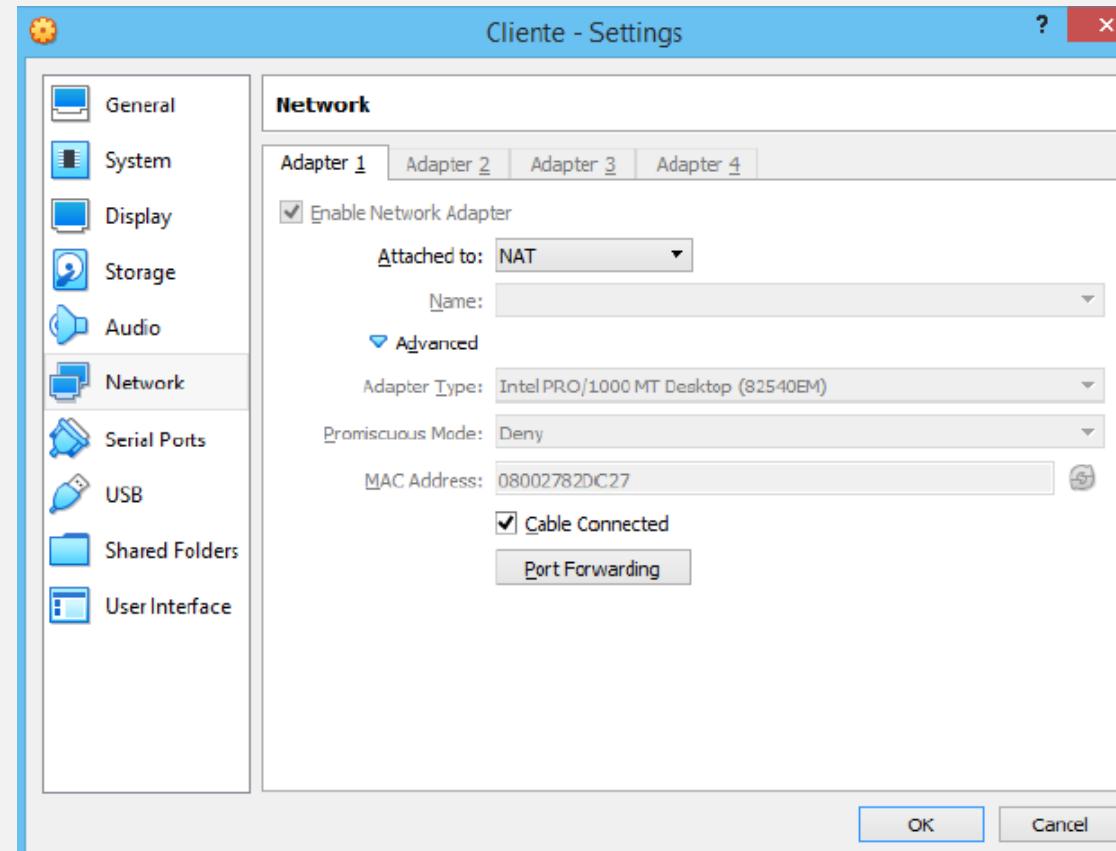
Alterar o nome

Alterar as definições

Alterar as definições de rede

Configuração da rede da maquina virtual

- Pode alterar o tipo de rede ou acrescentar outros adaptadores à sua máquina virtual:



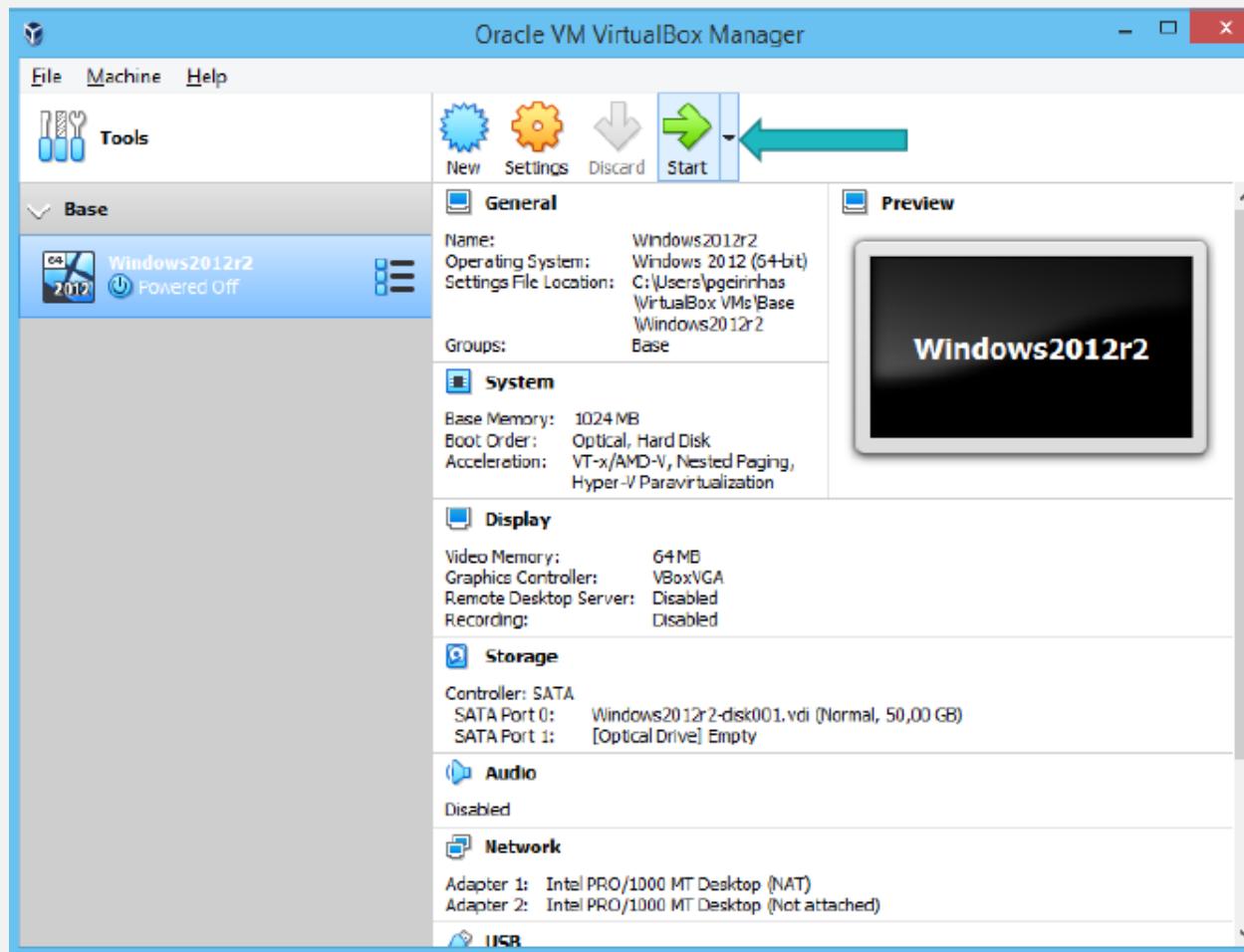
Exercício 2 – Alterar alguns parâmetros de um servidor, serviços e eventos

Exercício 2

- Arranque com o Windows Server 2012. Faça a sua configuração inicial.
- A palavra chave do utilizador administrator é 1qazZAQ!
- Altere o nome da máquina Windows Server 2012 para ServSR1.
- Altere o workgroup para SR1
- Veja os serviços que estão a correr no seu servidor.
- Qual o estado do serviço *Workstaion*? Faça um *restart* a esse serviço.
- Veja os eventos de sistema *windows*. Analise os mais recentes.
- Apague os eventos “Application”, “Security” e “System”.
- Veja como está a performance do seu servidor.
- Veja como estão a ser utilizadores os recursos de hardware do seu servidor.

How To

Arrancar com uma máquina



Servidor - Configuração inicial

Settings

Country or region

Portugal

App language

Portuguese (Portugal)

Keyboard layout

Portuguese

Next

POR

 **Settings**

Please read the license terms.

MICROSOFT SOFTWARE LICENSE TERMS

MICROSOFT WINDOWS SERVER 2012 R2 STANDARD

These license terms are an agreement between Microsoft Corporation (or based on where you live, one of its affiliates) and you. Please read them. They apply to the software named above, which includes the media on which you received it, if any. The terms also apply to any Microsoft:

- updates,
- supplements,
- Internet-based services, and
- support services

for this software, unless other terms accompany those items. If so, those terms apply.

By using the software, you accept these terms. If you do not accept them, do not use the software. Instead, return it to the retailer for a refund or credit. If you cannot obtain a refund there, contact Microsoft or the Microsoft affiliate serving your country for information about Microsoft's refund policies. See www.microsoft.com/worldwide. In the United States and Canada, call (800) MICROSOFT or see www.microsoft.com/info/nareturns.htm.

As described below, using some features also operates as your consent to the transmission of certain standard computer information for Internet-based services.

EVALUATION USE RIGHTS: If you purchased this software for evaluation purposes, you may use it only for evaluation purposes. You may not copy, modify, rent, lease, loan, sell, distribute, or otherwise transfer the software, except as provided in the license terms.

I accept

POR

Servidor - Configuração inicial

④ Settings

Type a password for the built-in administrator account that you can use to sign in to this computer.

User name

Password

Reenter password

A password no nosso caso é :
1qazZAQ!

17:40
segunda-feira, 22 de março

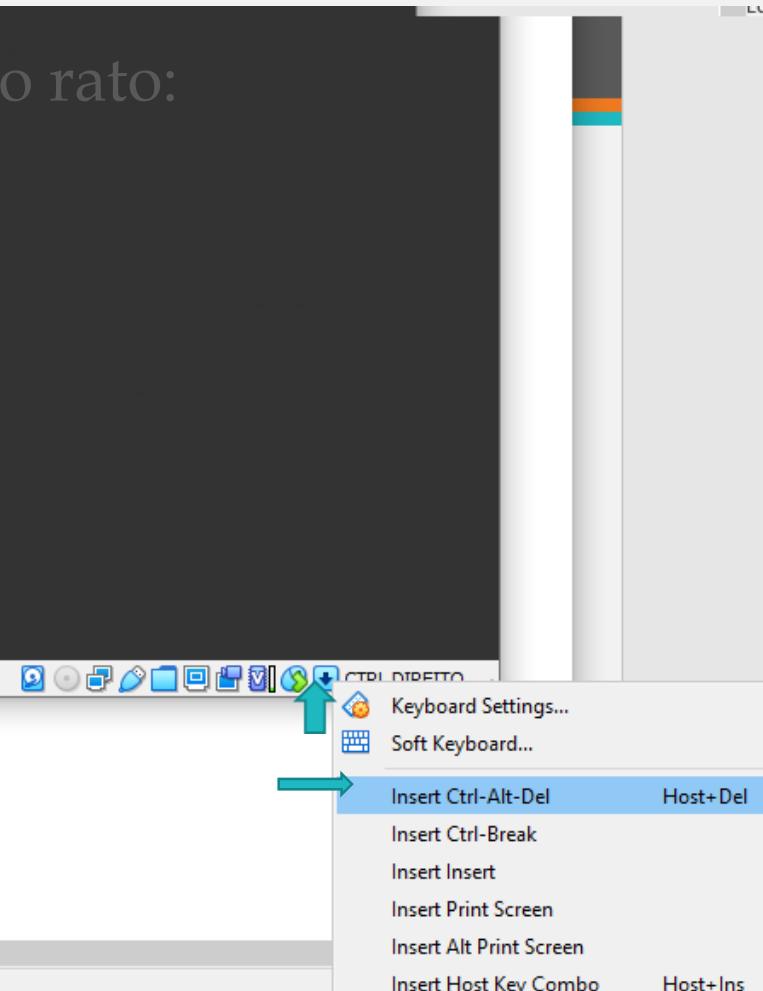


Servidor - Entrar

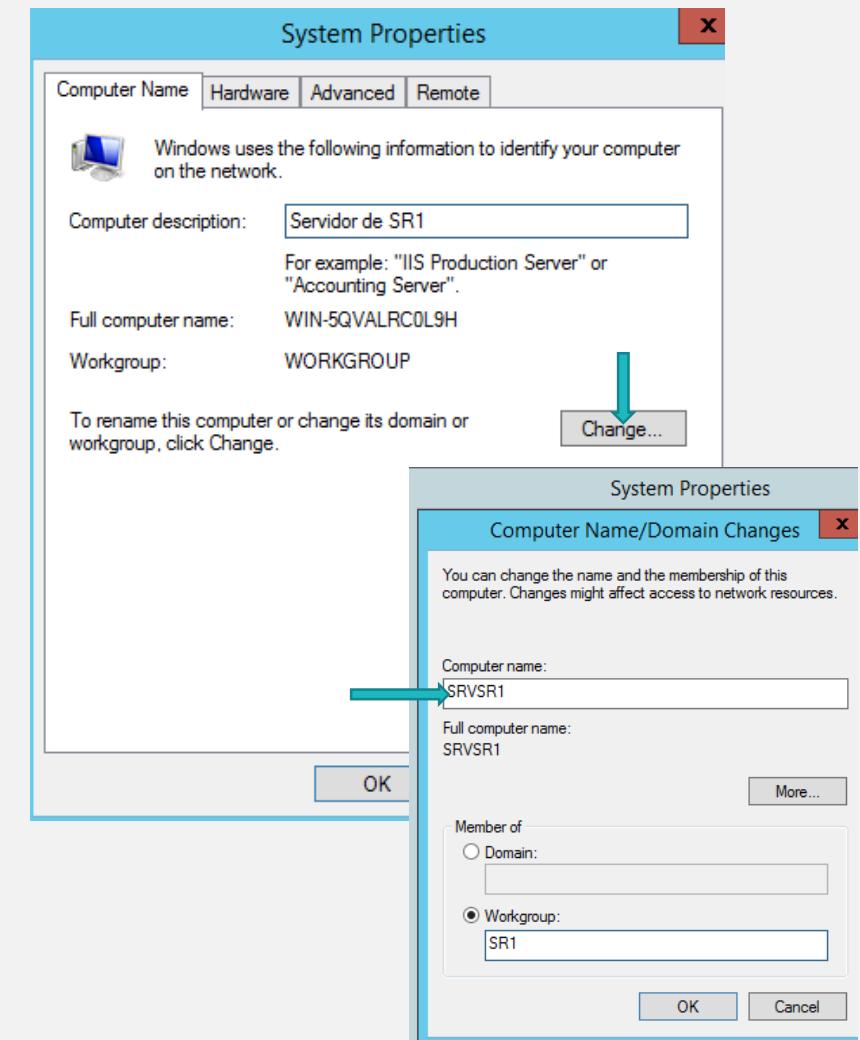
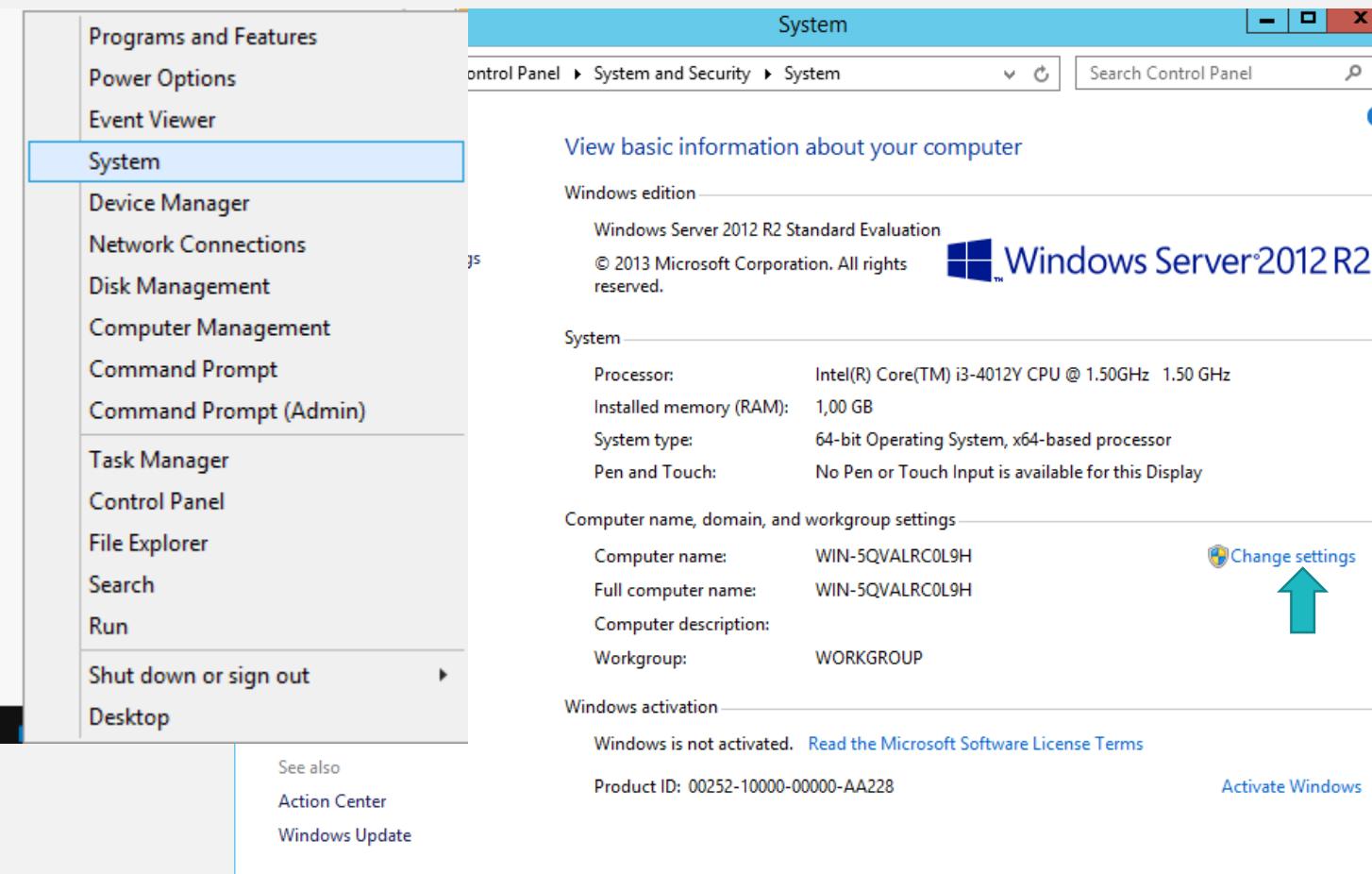
- Clique com o botão do lado esquerdo do rato:

17:41

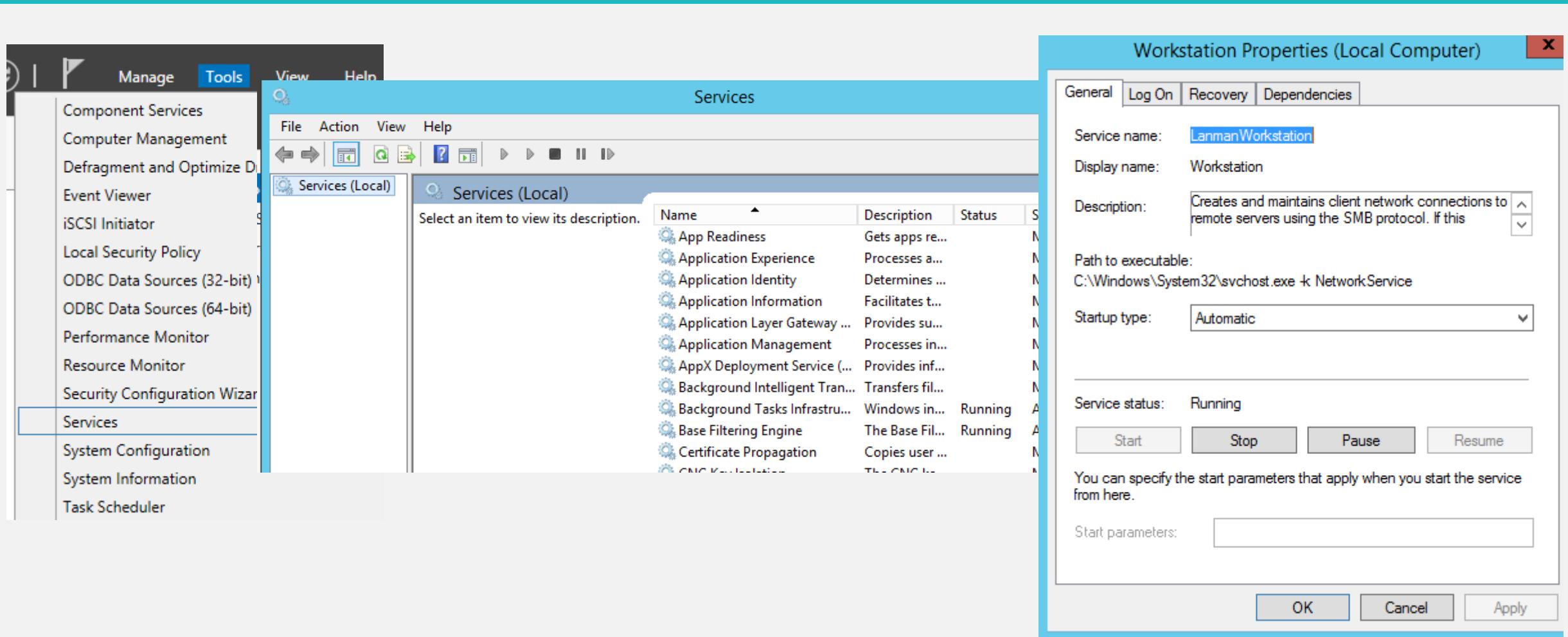
segunda-feira, 22 de março



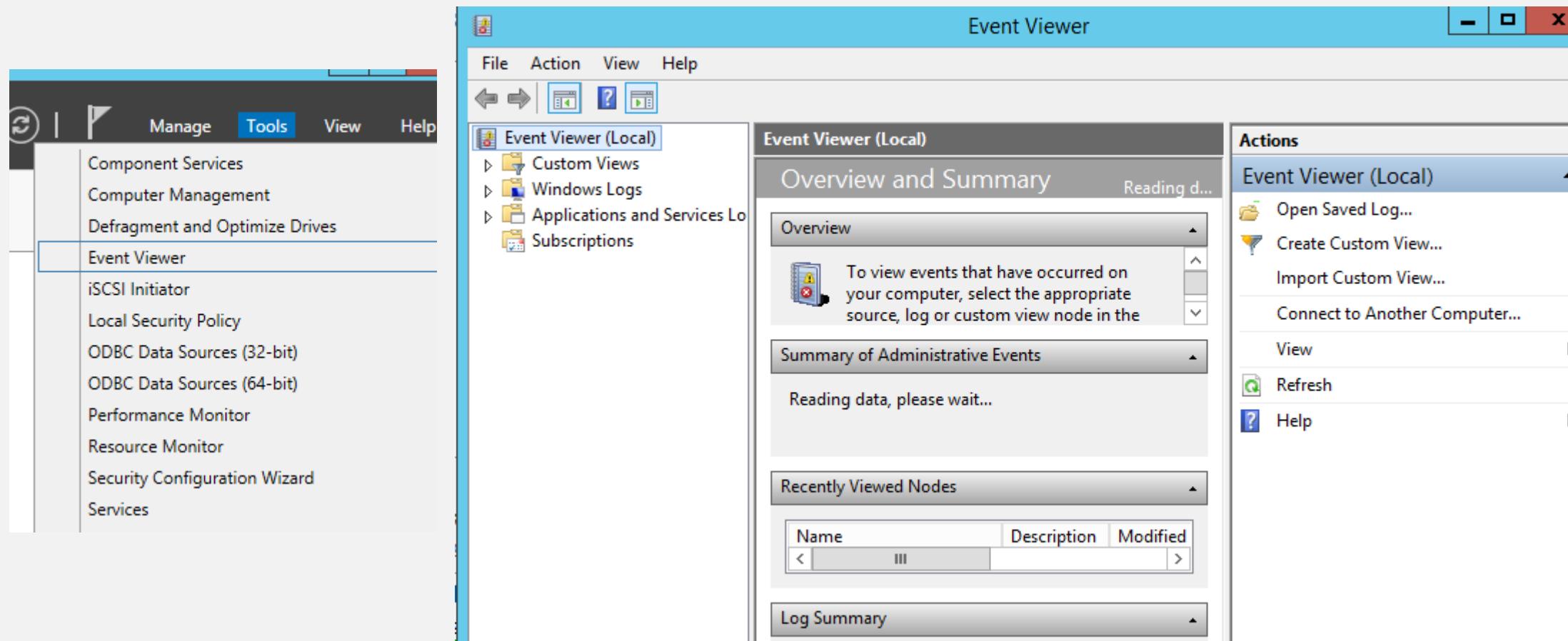
Alterar o nome e o domínio/workgroup de um servidor



Serviços do Servidor



Eventos (*Event Viewer*)



Performance

Server Manager • Local Server

Dashboard Local Server All Servers DHCP File and Storage Services ▾

PERFORMANCE

All results | 1 total | Last 24 hours

CPU Usage

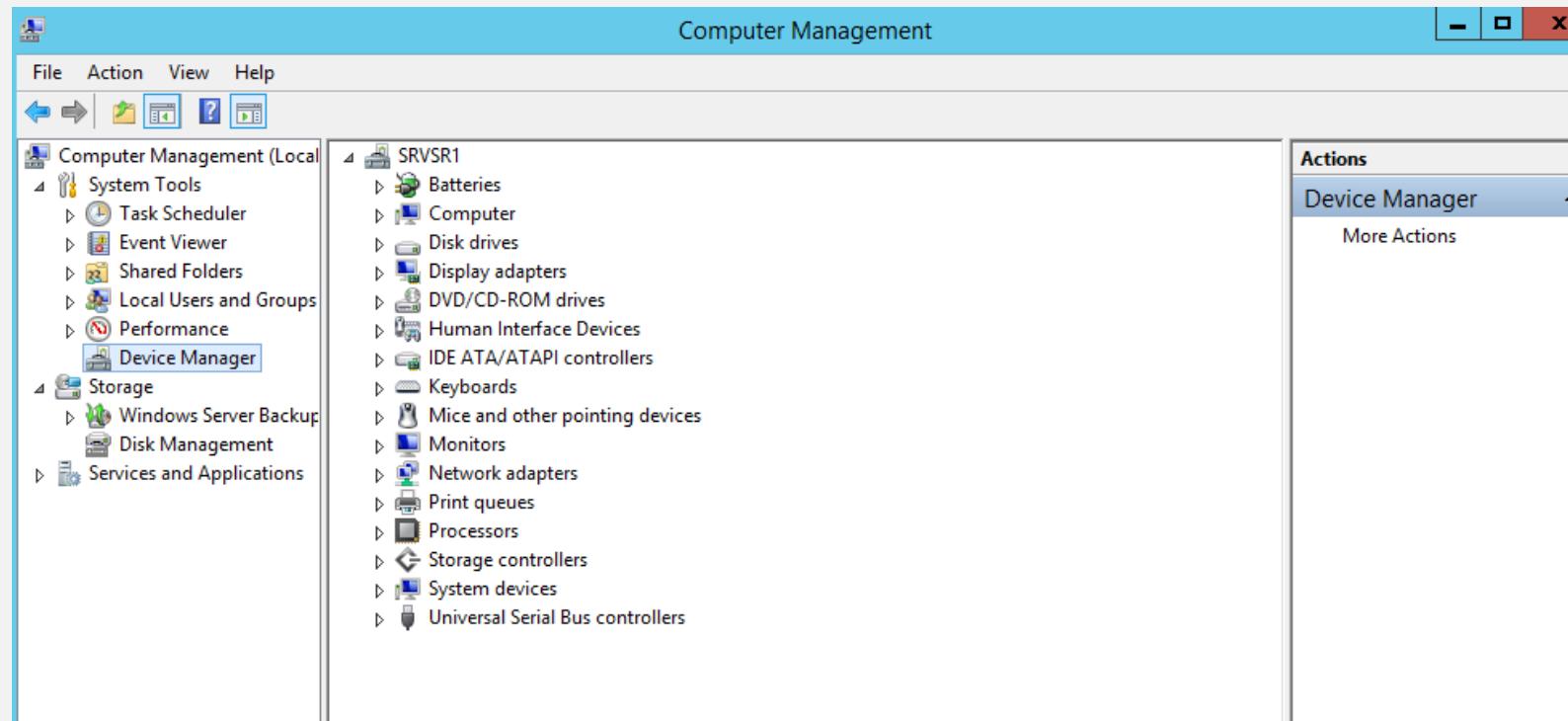
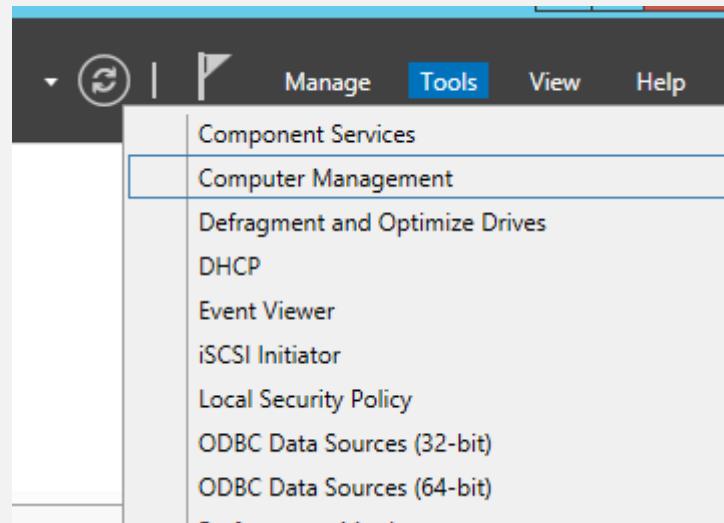
Available Memory

Filter

Server Name	Counter Status	CPU Alert Count	Memory Alert Count	First Occurrence	Last Occurrence
SRVSR1	Off	-	-	-	-

The screenshot shows the Windows Server Manager interface for a local server. The left navigation pane includes links for Dashboard, Local Server (which is selected), All Servers, DHCP, and File and Storage Services. The main content area is titled 'PERFORMANCE' and displays two charts: 'CPU Usage' and 'Available Memory'. Below the charts is a 'Filter' bar and a table with columns for Server Name, Counter Status, CPU Alert Count, Memory Alert Count, First Occurrence, and Last Occurrence. The table contains one row for 'SRVSR1' with the 'Counter Status' set to 'Off'.

Device Manager



Exercício 3 – Criação de uma rede entre servidor e o cliente

Exercício 3

- O servidor (Windows server 2012) é o elemento central da empresa SR1 SA. Terá as seguintes definições:
 - Nome - ServSR1
 - Workgroup - SR1
 - Endereço IP - 192.168.20.1 255.255.255.0
 - Default GW - 192.168.20.254
 - Servidor DNS primário - 192.168.20.1
- O posto de trabalho (Windows 10) deverá ter as seguintes definições:
 - Nome - PT01
 - Workgroup - SR1
 - Endereço IP - 192.168.20.50 255.255.255.0
 - Default GW - 192.168.20.254
 - Servidor DNS primário - 192.168.20.1
 - O utilizador por defeito é wk1 com a palavra chave 1qazZAQ!
 - Garanta que esse utilizador tem privilégios de administração.
- Depois de feitas estas alterações, garanta que as máquinas têm conetividade entre si.
- **A rede deverá ser interna ao ambiente de virtualização, NÃO devendo existir qualquer comunicação com a rede física .**
- **Não se esqueça de verificar o estado das duas firewall (servidor e cliente)....**

How To

Cliente (Windows 10) - Configuração inicial

The image consists of four screenshots from the Windows 10 initial setup process:

- Screenshot 1: Who's going to use this PC?**

Account

Who's going to use this PC?
What name do you want to use?

A placeholder text "sr2" is shown in the input field.
- Screenshot 2: Create a super memorable password**

Account

Create a super memorable password
Make sure to pick something you'll absolutely remember.

A placeholder text "....." is shown in the input field.
- Screenshot 3: Find my device**

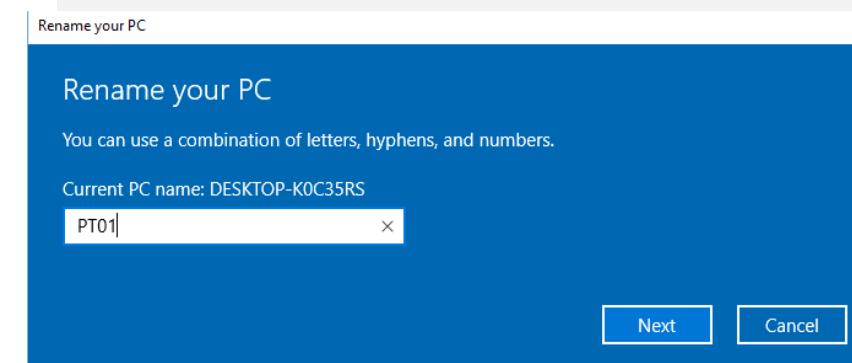
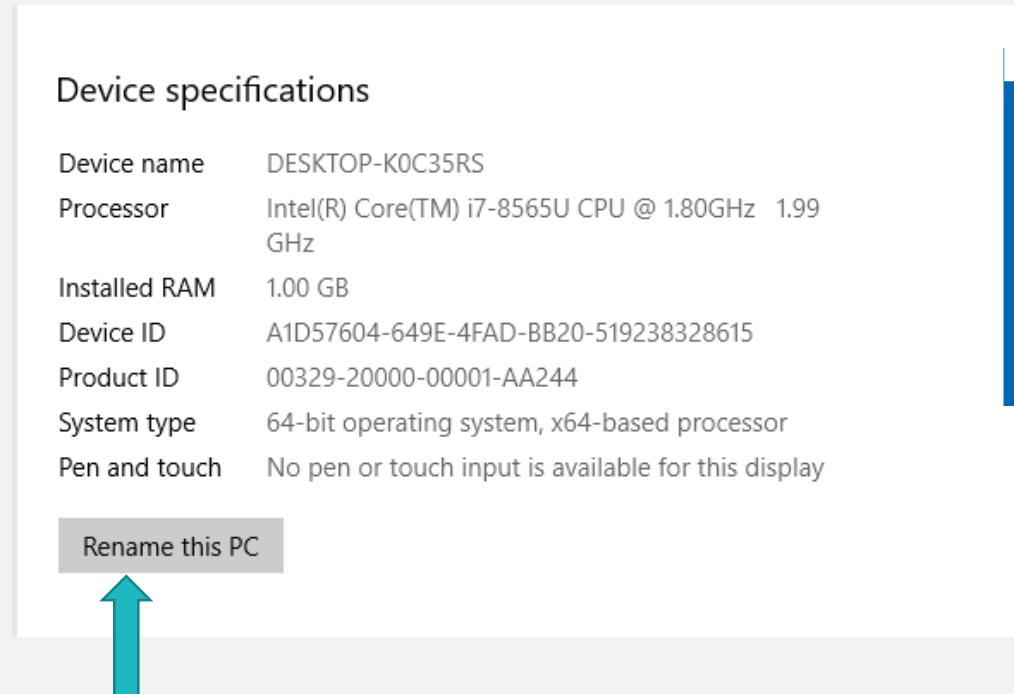
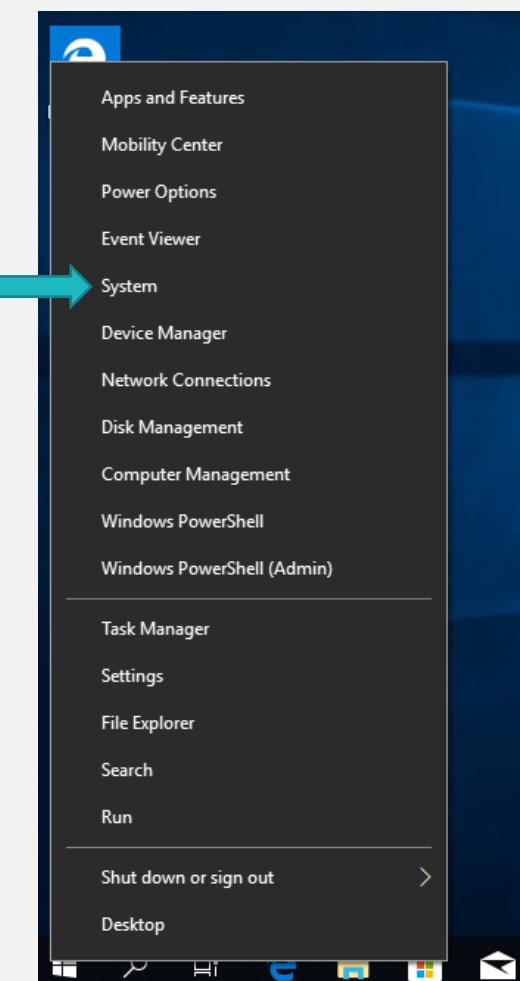
Choose your settings, then select 'Accept' to save them. Check the 'Learn more' link for info on these settings, how to change them, how Windows Defender SmartScreen works, and the related data transfers and uses.

Yes: Turn on Find my device (requires Microsoft account) and use your device's location data to help you find your device if you lose it.

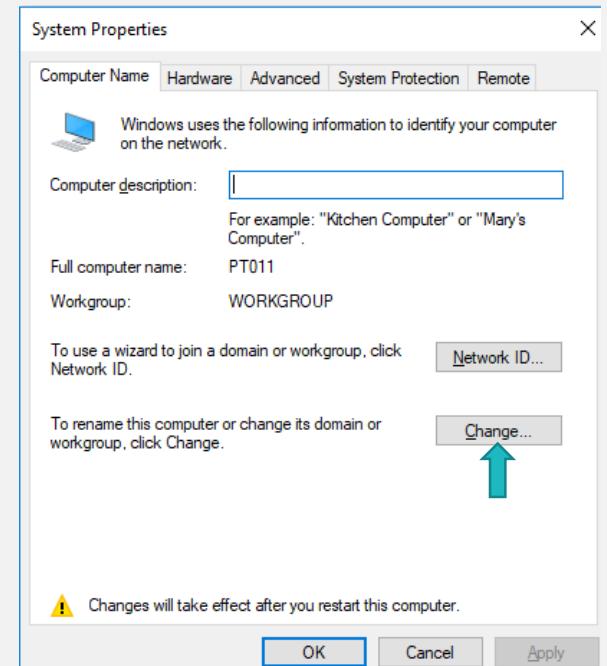
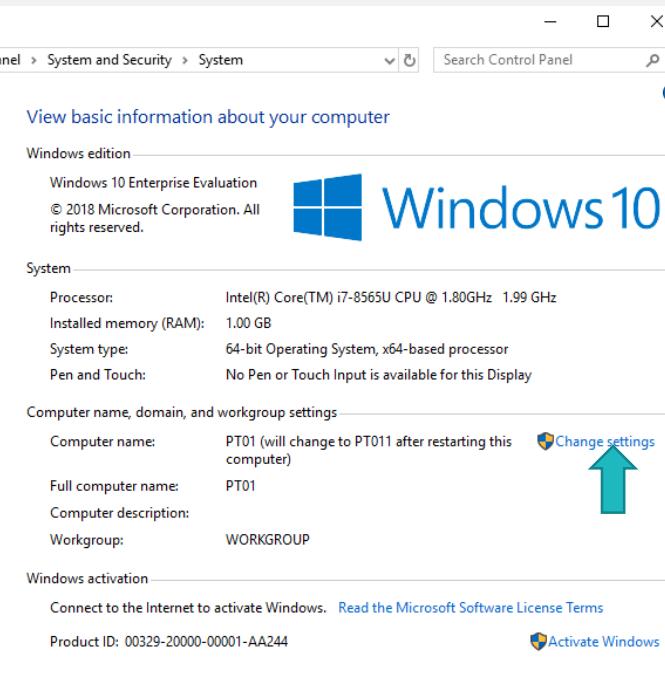
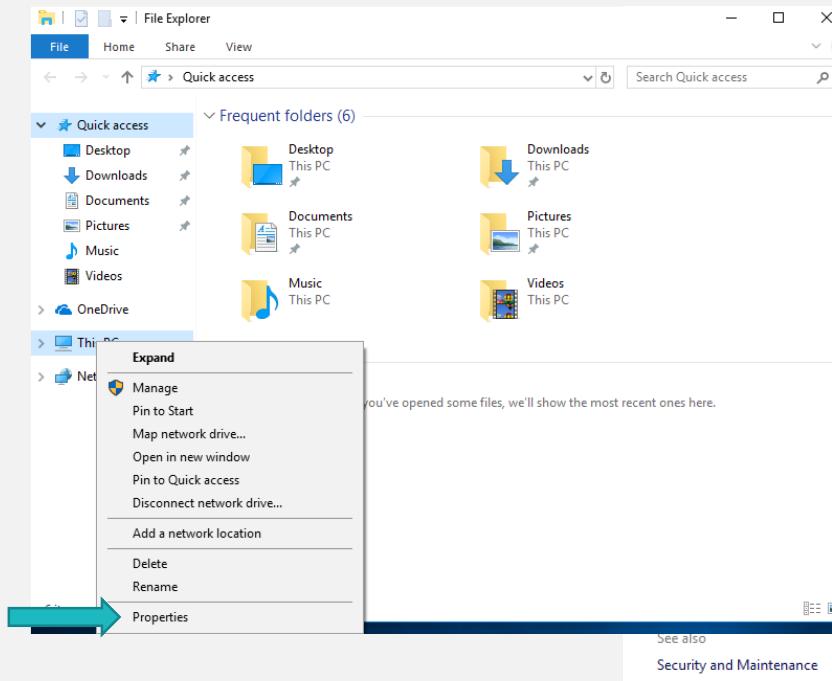
No: Windows won't be able to help you keep track of your device if you lose it.
- Screenshot 4: This might take several minutes**

Don't turn off your PC

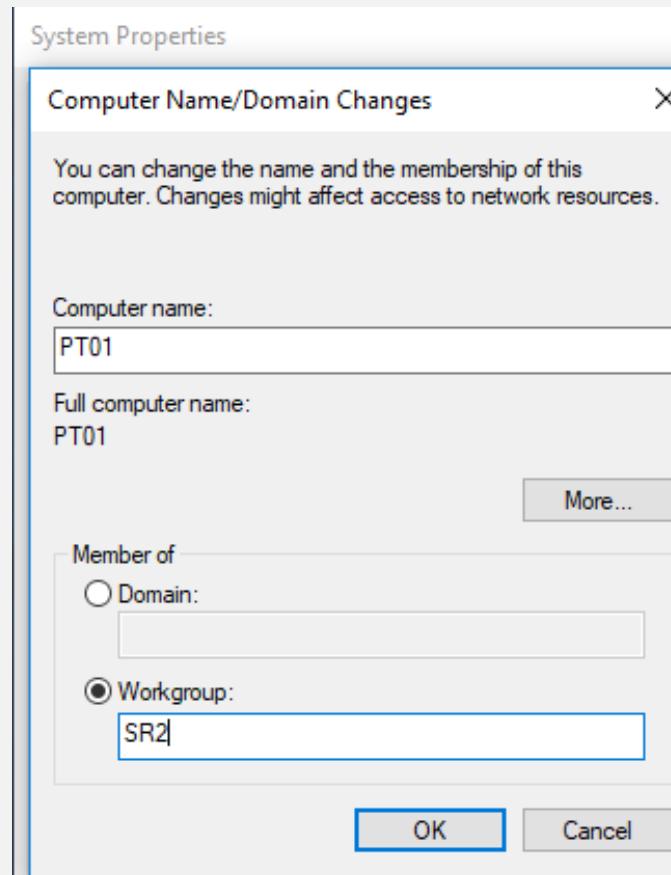
Alterar o nome de uma maquina Windows 10



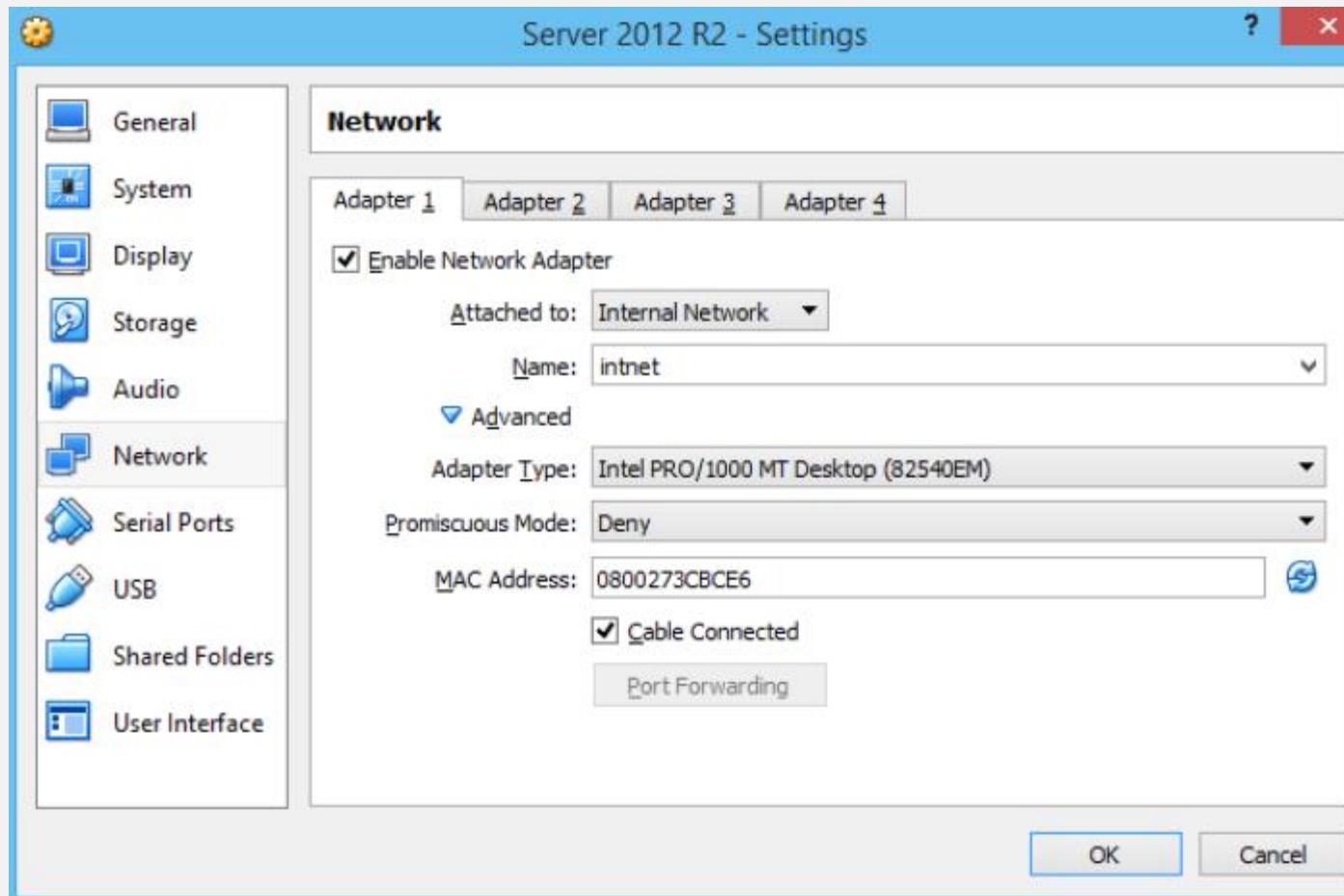
Alterar o workgroup de uma maquina Windows 10



Alterar o *workgroup* de uma maquina Windows 10



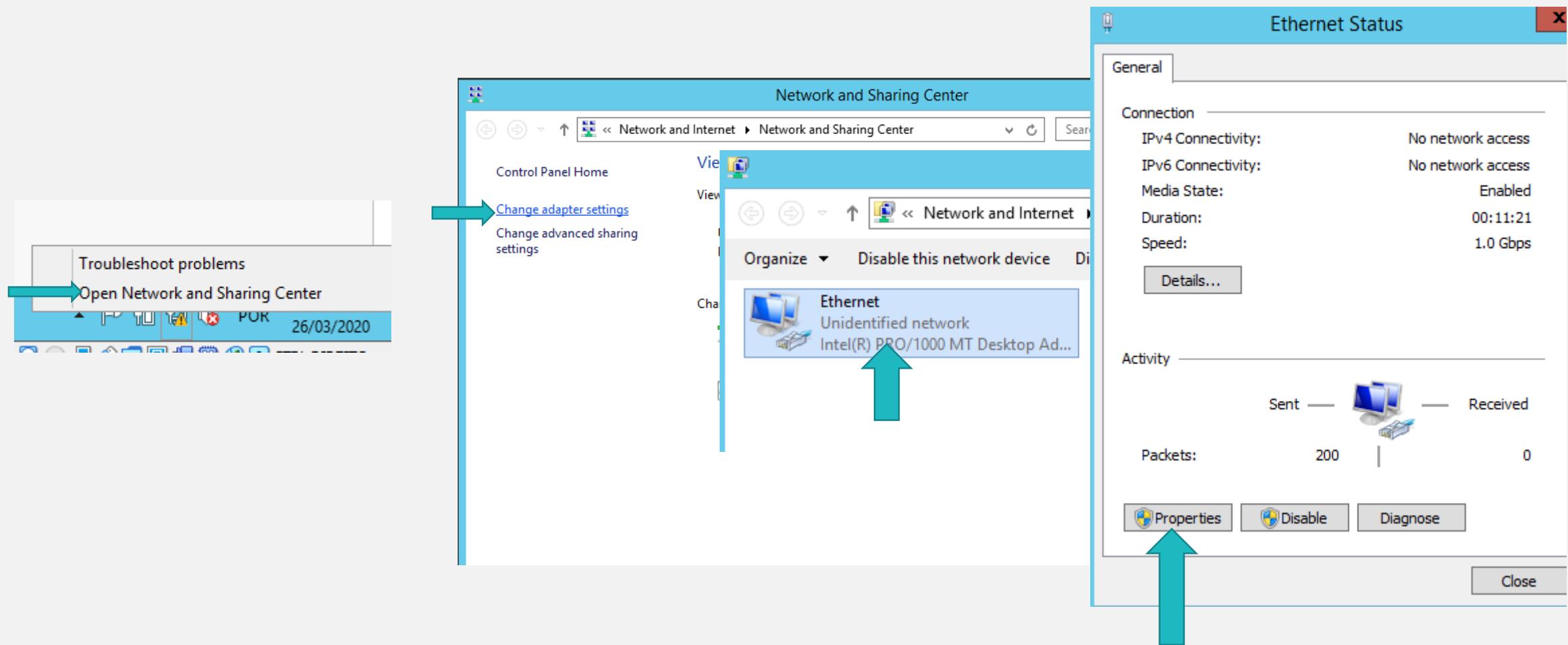
Modos de ligação à rede



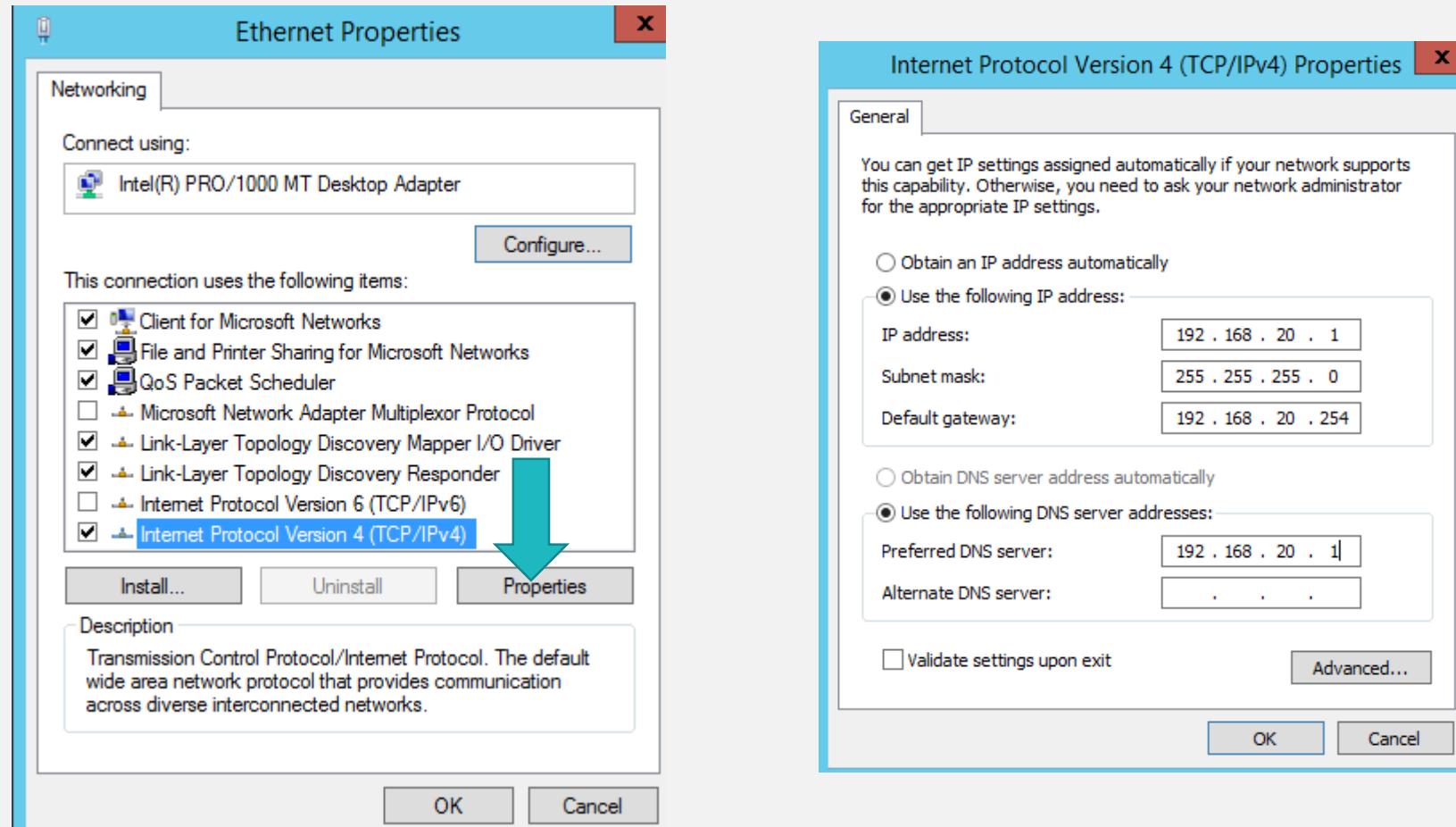
Modos de ligação à rede

- O Virtual Box permite configurar a máquina virtual com quatro modos principais de ligação à rede:
 - **modo nat**: a placa de rede acede à rede física com o mesmo endereço IP da máquina hospedeira, como se estivesse numa rede com NAT. Usada em ambientes onde as máquinas virtuais não fornecem serviços, mas podem aceder à rede.
 - **modo bridge**: a placa de rede acede à rede física, como se fosse uma máquina real. A VM pode inclusive ser acedida por outras máquinas da rede. Usada em ambientes onde as máquinas virtuais fornecem serviços ou participam de uma rede real. Tem de indicar qual a placa física que vai utilizar.
 - **modo internal network**: a placa de rede não tem acesso à rede física, sendo visível apenas para a máquina hospedeira. Usada em ambientes de teste isolados onde as máquinas virtuais não precisam se comunicar com outros ambientes externos.
 - **modo host-only**: é uma mistura dos dois primeiros modos. As máquinas virtuais comunicam entre si e com a máquina hospedeira mas não com outras máquinas da rede local desta.

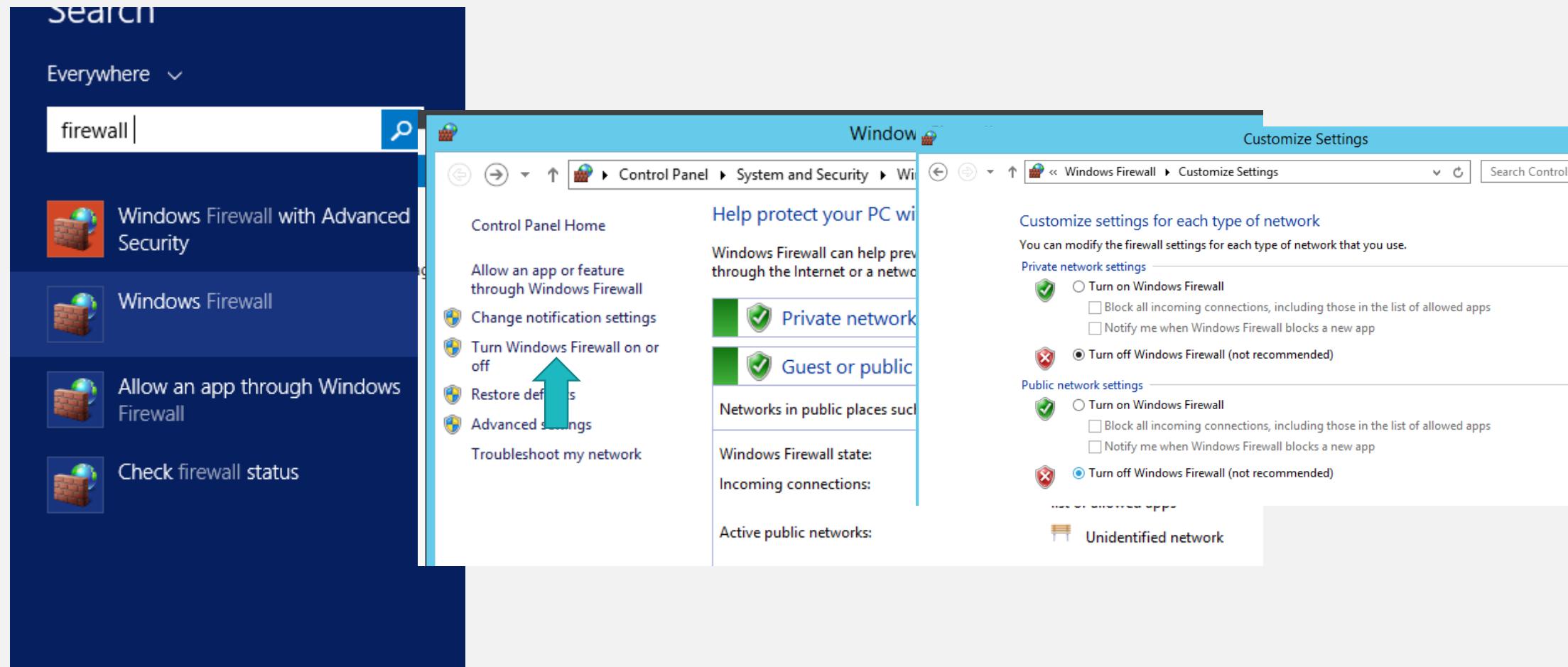
Alterar o IP de um servidor Windows Server 2012



Alterar o IP de um servidor Windows Server 2012



Firewall - Servidor

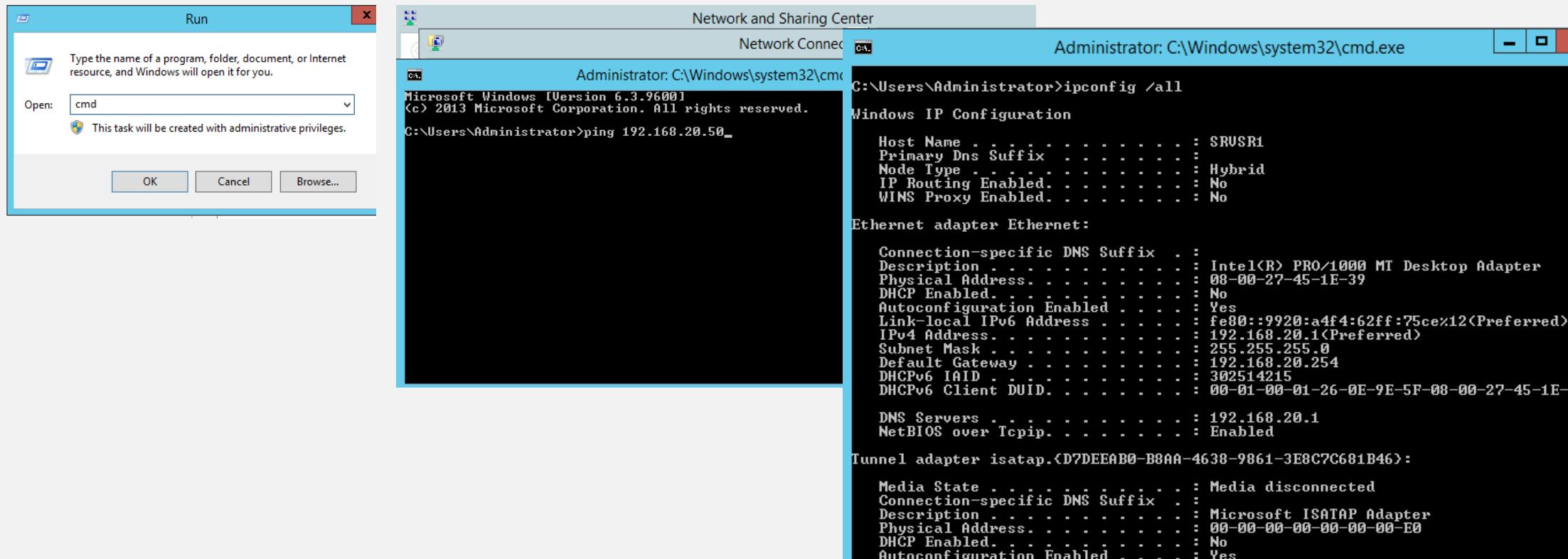


Firewall - Cliente

The image shows a Windows 10 desktop environment with two windows open. On the left is a VirtualBox window titled "Cliente [Running] - Oracle VM VirtualBox". The main content of this window is the Windows Settings interface, specifically the "About" section. It displays a summary of system protection features: Virus & Threat Protection (highlighted with a red dot), Firewall & Network Protection, Device performance & Health, App & browser control, Account protection, and Device security. Below this, it says "Your PC is monitored and protected." and provides a link to "See details in Windows Defender". The left sidebar of the Settings app lists various system categories like Home, Find a setting, System, Display, Sound, Notifications & actions, Focus assist, Power & sleep, Storage, Tablet mode, Multitasking, Projecting to this PC, Shared experiences, Remote Desktop, and About. The "About" item is currently selected. At the bottom of the Settings window, there's a "Rename this PC" button and some small text about the Windows license. The taskbar at the bottom of the screen shows icons for File Explorer, Edge, and other system tools.

The right window is titled "Customize Settings" and is part of the Windows Control Panel under "Windows Defender Firewall". It is titled "Customize settings for each type of network". It contains two sections: "Private network settings" and "Public network settings". Under "Private network settings", there are two radio buttons: "Turn on Windows Defender Firewall" (selected) and "Turn off Windows Defender Firewall (not recommended)". Under "Public network settings", there are also two radio buttons: "Turn on Windows Defender Firewall" (selected) and "Turn off Windows Defender Firewall (not recommended)". Both sections include checkboxes for "Block all incoming connections, including those in the list of allowed apps" and "Notify me when Windows Defender Firewall blocks a new app". At the bottom right of this window are "OK" and "Cancel" buttons.

Diagnóstico



Exercício 4 – Configurar o servidor DHCP

Exercício

- Instale o serviço DHCP no servidor.
- Deve ter as seguintes configurações:
 - Rede - 192.168.20.0/24
 - Router – 192.168.20.254
 - Domínio – sr1.pt
 - DNS:
 - Primário – 192.168.20.1
 - Secundário – 8.8.8.8
 - Gama de IP dinâmicos – 20 ao 200.
 - Nome da scope – Rede Local
 - Servidor NTP – 192.168.20.10
- Verifique o funcionamento do serviço DHCP.

Exercício

- Coloque o PC (cliente) a obter o endereço IP por DHCP.
- Teste que o serviço DHCP está a atribuir o IP correto ao cliente.
 - Usando o comando ipconfig.
 - Usando a aplicação de gestão do serviço DHCP.
- Garanta que entre o Servidor e o cliente existe conectividade IP.

How To

DHCP - Instalação do serviço



Copyright © 2013 Microsoft Corporation. All rights reserved.

A screenshot of the Windows Server Manager dashboard. The title bar says "Server Manager". The left navigation pane shows "Dashboard" (which is selected), "Local Server", and "All Servers". The main area has a "WELCOME TO SERVER MANAGER" section with a large orange "QUICK START" button and a "WHAT'S NEW" button below it. To the right of the "QUICK START" button is a numbered list: 1. Configure this local server (with a red circle and a teal arrow pointing to it), 2. Add roles and features, 3. Add other servers to manage, and 4. Create a server group. Below this is a "ROLES AND SERVER GROUPS" section showing "Roles: 0 | Server groups: 1 | Servers total: 1". It lists "Local Server" (1) under "Manageability" and "Events", and "All Servers" (1) under "Manageability" and "Events".

Server Manager

Server Manager • Dashboard

Dashboard Local Server All Servers

WELCOME TO SERVER MANAGER

1 Configure this local server

2 Add roles and features

3 Add other servers to manage

4 Create a server group

QUICK START

WHAT'S NEW

LEARN MORE

ROLES AND SERVER GROUPS

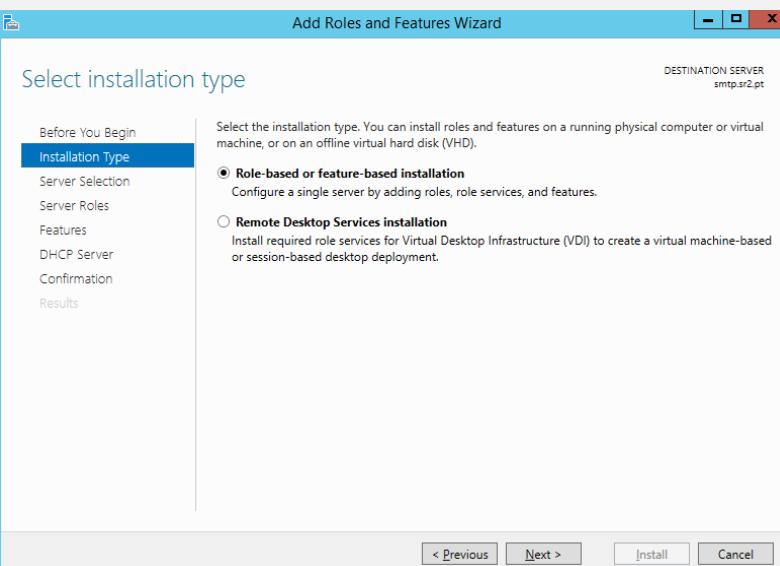
Roles: 0 | Server groups: 1 | Servers total: 1

Local Server	1
Manageability	
Events	

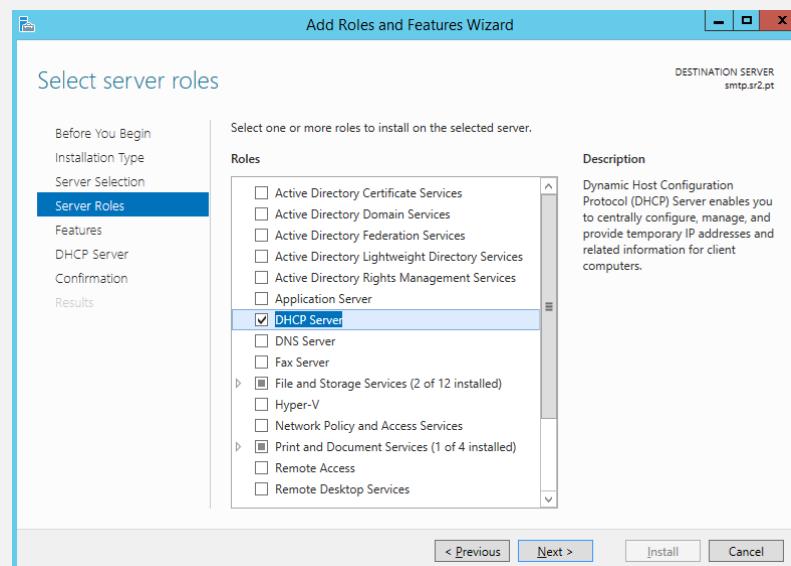
All Servers	1
Manageability	
Events	

DHCP - Instalação do serviço

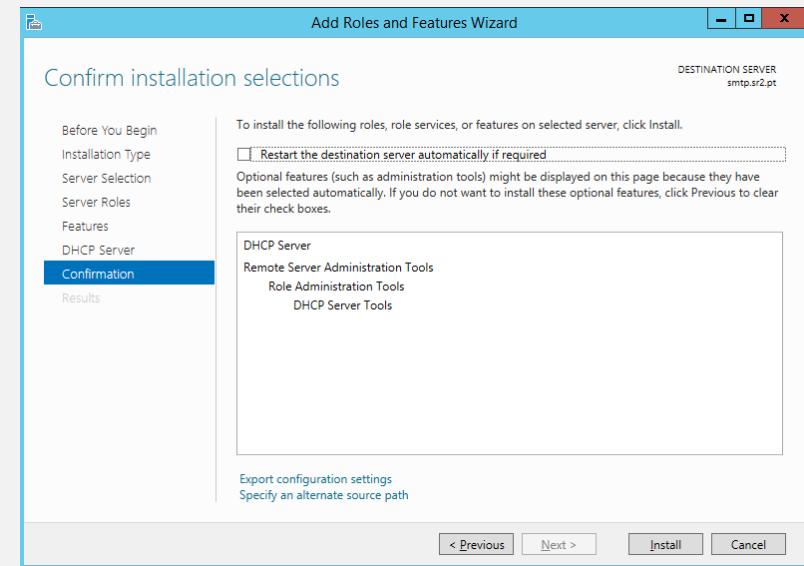
1



2

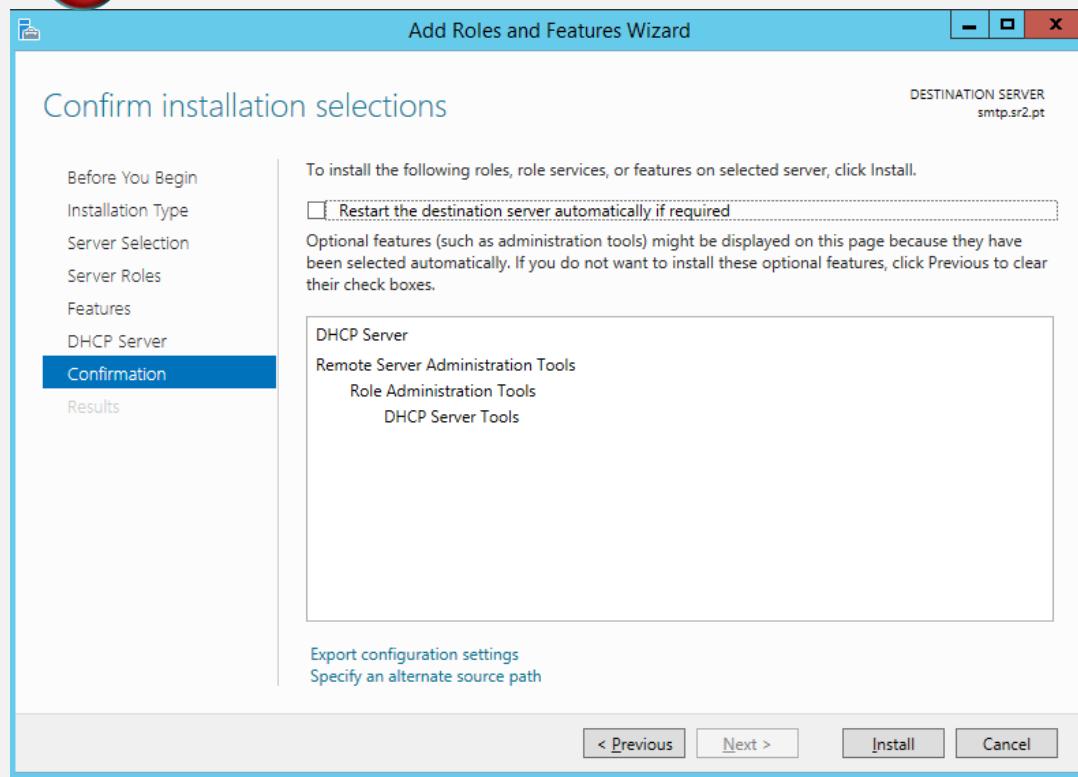


3

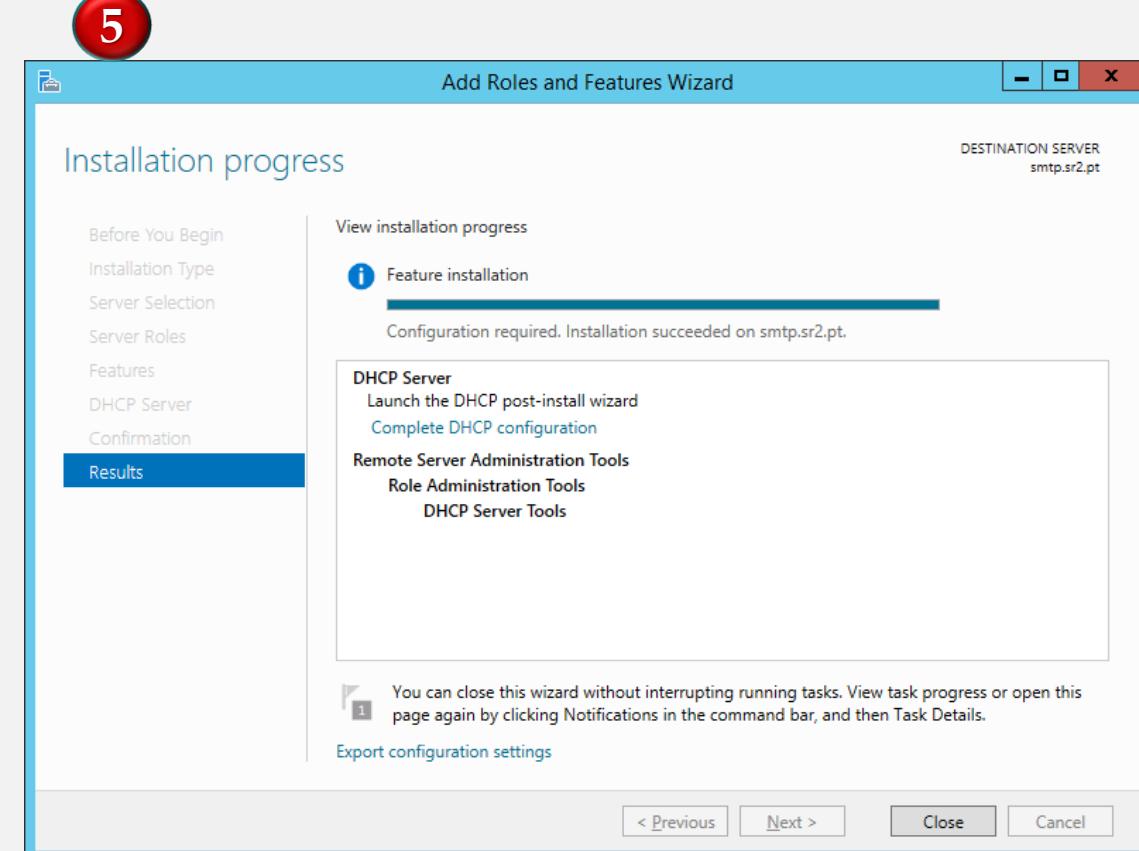


DHCP - Instalação do serviço

4

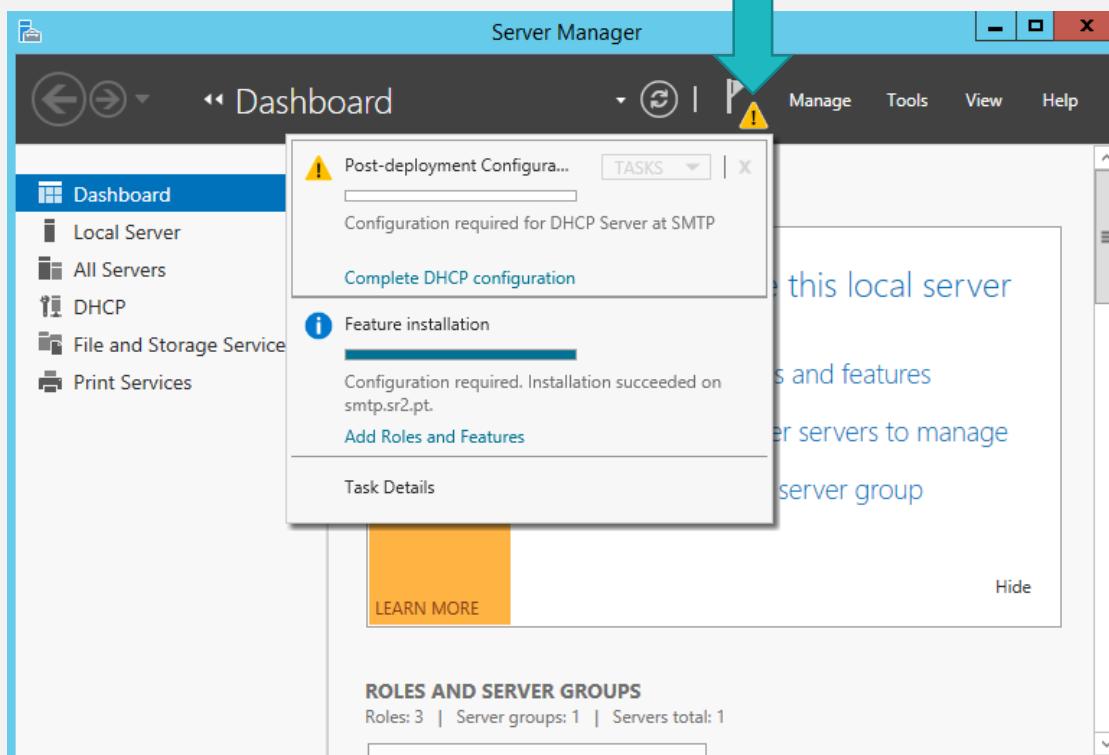


5



DHCP - Instalação do serviço

6



7



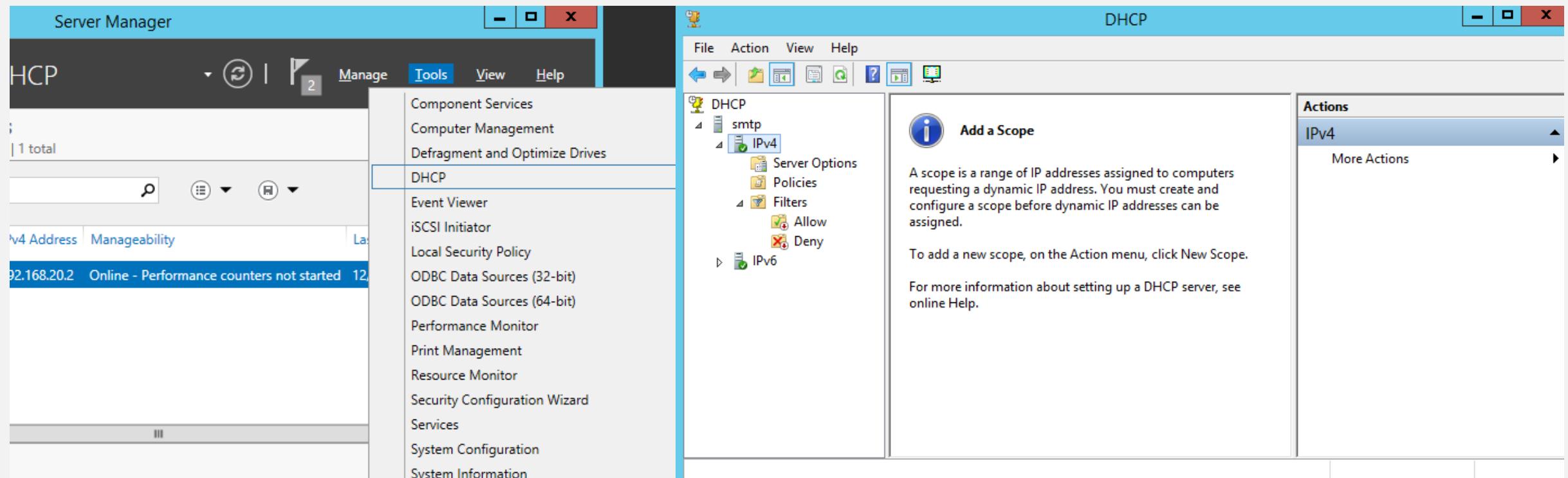
DHCP - Instalação do serviço

The status of the post install configuration steps are indicated below:

Description	
Summary	<p>Creating security groups Done Please restart the DHCP server service on the target computer for the security groups to be effective.</p>

< Previous Next > Close Cancel

DHCP - Instalação do serviço



DHCP - Configuração de *scopes*

- *Scope*
 - Conjunto de endereços IP pertencentes a uma sub-rede lógica
 - Exemplo: 192.168.1.1-192.168.1.254
- *Lease*
 - Acto de atribuir um endereço IP a um cliente
 - Quando é feita a atribuição diz-se que o *lease* está activo
 - Quando o *lease* é efectuado é indicada a duração máxima
 - Duas configurações base (posteriormente pode ser alterado)
 - Redes com fios (6 dias)
 - Redes sem fios (8 horas)
 - O cliente deve efectuar a renovação e pode ser:
 - **Automaticamente** (operação realizada pelo SO)
 - Nos sistemas *Windows* o pedido de renovação é realizado quando for atingido metade do tempo de empréstimo (informação proveniente do servidor)
 - **Manualmente**
 - `ipconfig /release` (para libertar - opcional)
 - `ipconfig /renew`

DHCP - Configuração de scopes

- Indicar:
 - **Scope Name** : Nome
 - **Starting IP Address e Ending IP Address**: Endereço inicial e final. Deve sempre colocar a rede toda e depois excluir o que não deseja atribuir.
 - **Subnet Mask** : Mascara de subrede utilizada
 - **Default Gateway**: endereço do router por defeito
 - **Subnet Type**: Escolha entre Wired (6 dias) ou Wireless (8 dias) para definir o tempo de duração da concessão de endereçamento IP.
 - Marque a opção Activate this scope para ativar o scope ao terminar a configuração.

The screenshot shows the 'New Scope Wizard' interface, divided into two main sections:

- Scope Name**: A step where users provide an identifying scope name and optional description. It includes fields for 'Name' and 'Description'.
- IP Address Range**: A step where users define the scope address range by identifying a set of consecutive IP addresses. It includes fields for 'Start IP address' (192.168.20.1) and 'End IP address' (192.168.20.254).

At the bottom, there are navigation buttons: '< Back', 'Next >', and 'Cancel'.

DHCP

New Scope Wizard

Router (Default Gateway)
You can specify the routers, or default gateways, to be distributed by this scope.

To add an IP address for a router used by clients, enter the address below.

IP address:

192.168.20.254	Add
	Remove
	Up
	Down

New Scope Wizard

Domain Name and DNS Servers
The Domain Name System (DNS) maps and translates domain names used by clients on your network.

You can specify the parent domain you want the client computers on your network to use for DNS name resolution.

Parent domain:

To configure scope clients to use DNS servers on your network, enter the IP addresses for those servers.

Server name:
IP address:
Add
Resolve
Up
Down

< Back Next > Cancel

DHCP

File Action View Help

DHCP

srvsr1

IPv4

Scope [192.168.20.0] Reservations

Address Pool

Address Leases

Reservations

Scope Options

Policies

Server Options

Policies

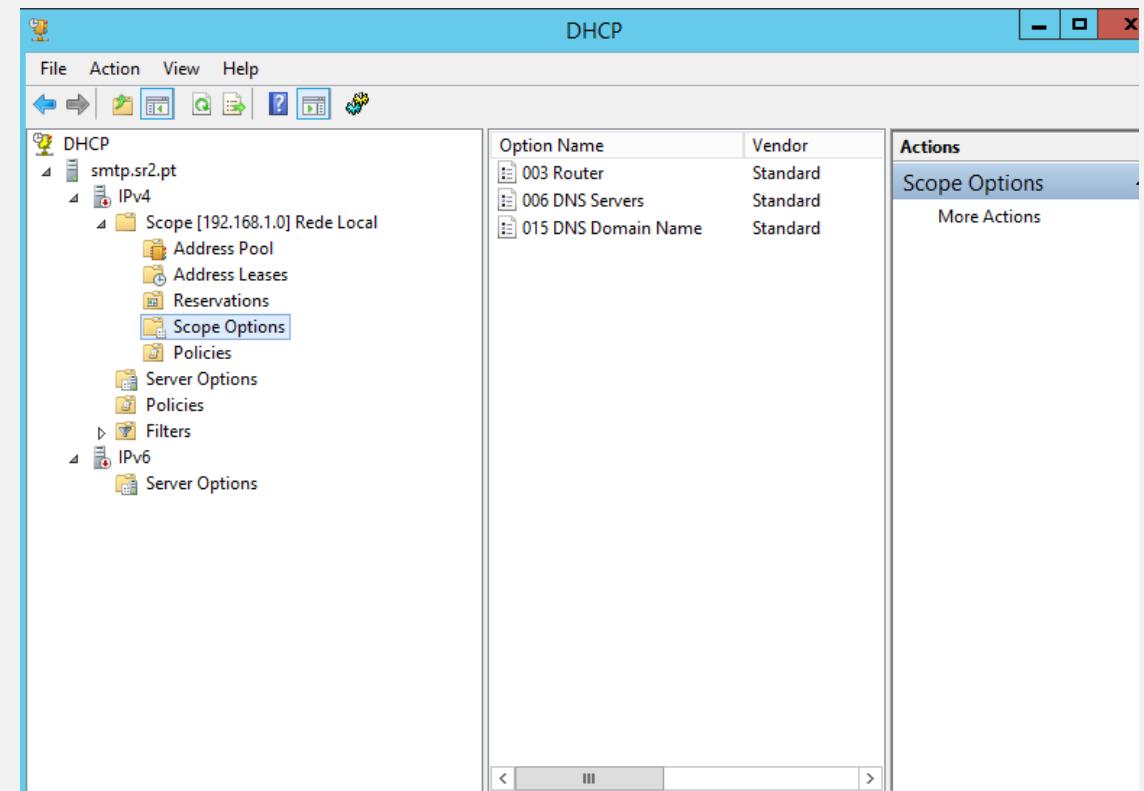
Filters

IPv6

Start IP Address	End IP Address	Actions
192.168.20.1	192.168.20.254	Address Pool
192.168.20.1	192.168.20.19	
192.168.20.201	192.168.20.254	

DHCP – Verificação e configuração do serviço

- Indo ao **Server Manager**, DHCP Server pode verificar como o seu servidor está a funcionar.
- **Address Pool** – indica qual a gama de endereços.
- **Address leases** – quais as maquinas que tem os IP “alugados”
- **Reservations** – Quais os IPs que estão reservados
- **Scope Options** – definições de TCP específicas para a lease (DNS, Router, etc)



DHCP - Adicionar reservas

- Uma gama de IPs
- Um IP específico

Add Exclusion ? X

Type the IP address range that you want to exclude. If you want to exclude a single address, type an address in Start IP address only.

Start IP address:

End IP address:

Add Close

New Reservation ? X

Provide information for a reserved client.

Reservation name:

IP address:

MAC address:

Description:

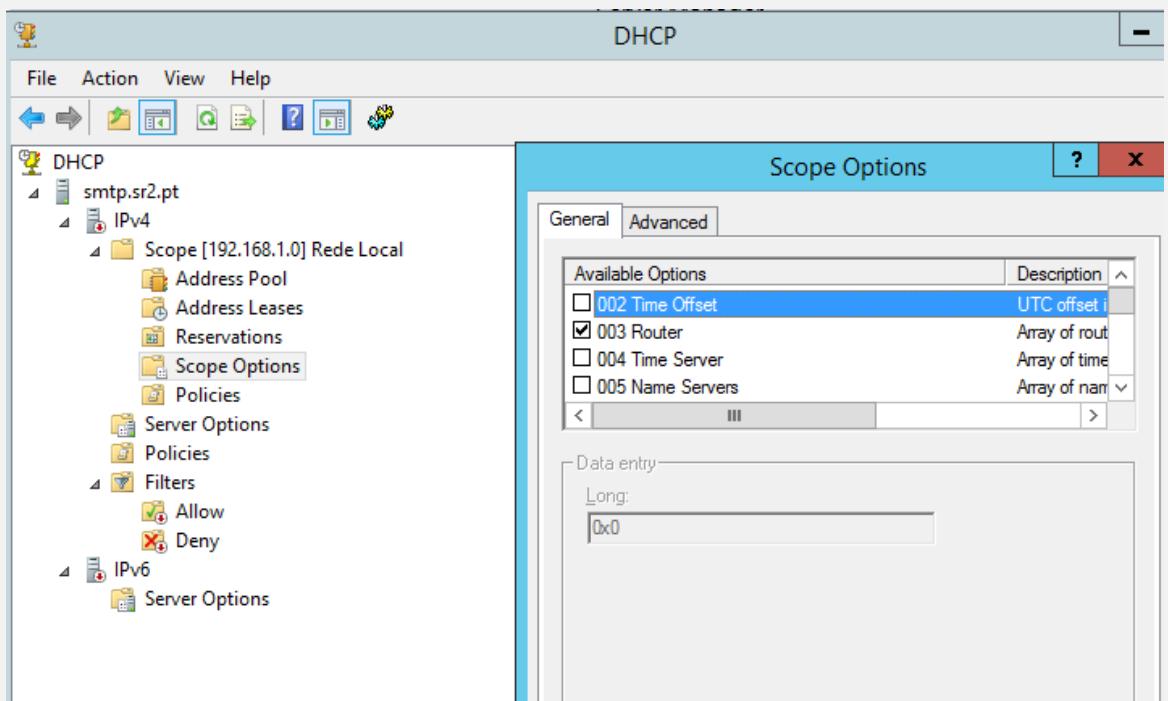
Supported types

Both
 DHCP
 BOOTP

Add Close

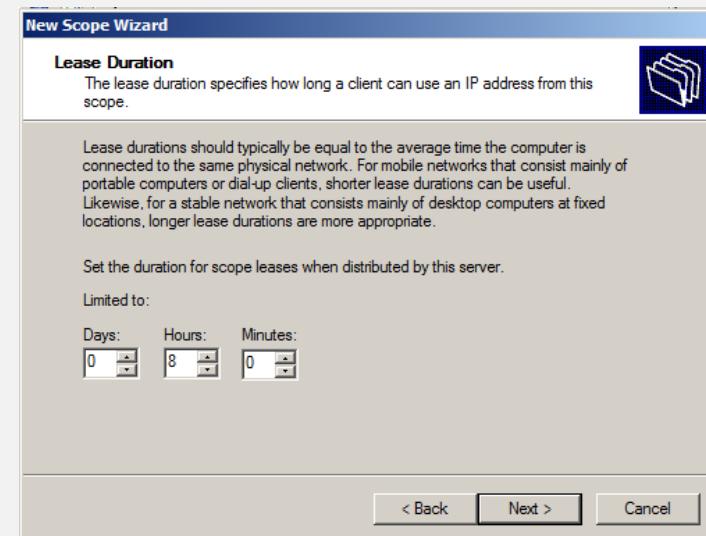
DHCP - *Server Options*

- Aqui pode configurar as opções e as configurações de TCP comuns a todas as scopes.
- Clicar com o botão do lado direito do rato e escolher *Configure options* → *Separador General* e escolher a opção pretendida.
- Posteriormente as configurações realizadas neste espaço vão aparecer no “*Server Options*”, conforme imagem seguinte.



DHCP - Opções

- *Lease Duration* este deve ser ajustado de acordo com o tipo de rede existente de forma a não existirem salvaguardas de endereços que possam prejudicar a atribuição de novos IP's.
- Caso a rede seja mais estática deve ser atribuído um valor maior, se a rede for mais dinâmica(por exemplo utilização de muitos clientes externos(portáteis)) deve ter um valor mais pequeno.



Dúvidas



Serviços de Rede 1 – **Aula 4 - Práticas**

2022-2023

Instituto Politécnico de Coimbra

Departamento de Engenharia Informática



Lembrete...

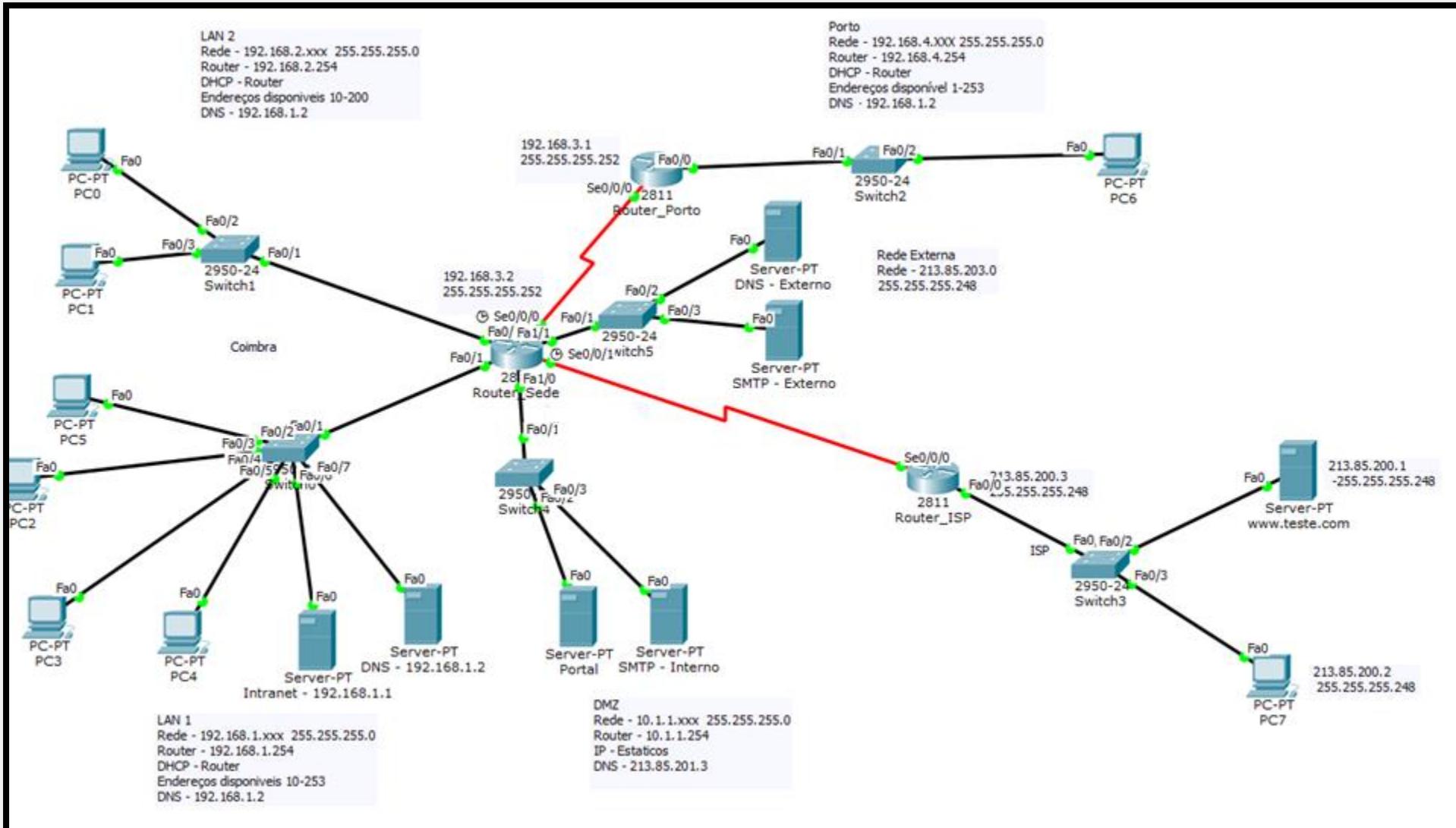
- Nas próximas 4^a e 5^a feira (**29 e 30 de março**) irá decorrer o 1º teste prático.
- Será feito durante as aulas práticas mediante **inscrição previa** no Moodle.
- A matéria que sai é:
 - Aulas Teóricas - Endereçamento IP, DHCP e NAT.
 - Aulas Práticas - Da aula 1 à aula 4.
- Devem ter instalado no computador onde vai realizar o teste o seguinte:
 - *Cisco Packet Tracer*.
 - Um virtualizador sendo que o desejável será o VirtualBox 6.1.
 - Importadas as máquinas “limpas” do Windows 2012 Server e do Windows 10.

Pre – Requisitos

- Ter instalado o *Cisco Packet Tracer* versão 8.2.0



Pre - Requisitos - Topologia do final da aula 2



Pre - Requisitos - Topologia do final da aula 2

- A empresa SR1 SA tem uma rede com a seguinte topologia:
 - Na sede (Coimbra) tem duas LAN (LAN1 e LAN2), uma DMZ e uma zona exterior.
 - Os endereços das redes são os seguintes:
 - LAN 1 - 192.168.1.0 - 255.255.255.0
 - LAN 2 - 192.168.2.0 - 255.255.255.0
 - DMZ - 10.1.1.0 - 255.255.255.0
 - Zona externa - 213.85.203.0 - 255.255.255.248 - ou seja 6 endereços disponíveis.
 - A rede LAN 1 e 2 têm os IP fornecidos por DHCP configurado no router da sede (Router_Sede).
 - Na DMZ e zona externa os IP atribuídos aos terminais são fixos.
 - Tem uma delegação no Porto com a rede 192.168.4.0 - 255.255.255.0. Os IP são dados por DHCP configurado no servidor da sede.
 - Tem uma delegação em Lisboa com a rede 192.168.5.0 /24. Os IP são dados por DHCP configurado no servidor da sede (não está na imagem mas é para colocar entre o Porto e a LAN 2).
 - O servidor de DHCP na sede em Coimbra tem o endereço 192.168.1.3. Este servidor tem as seguintes características:
 - Pool de Lisboa - Inicio 192.168.5.10 - Máximo 230 utilizadores.
 - Pool do Porto - Inicio 192.168.4.10 - Máximo de utilizadores 50.
 - Não esquecer a informação do(s) gateway e DNS (192.168.1.2).

Pre - Requisitos - Topologia do final da aula 2

- A rede do ISP é 213.85.200.0 – 255.255.255.248 e os IP são fixos.
- As redes de ligação são as seguintes:
 - Sede <-> Porto -> 192.168.3.0/30
 - Sede <-> Lisboa -> 192.168.3.4 /30
 - Sede – Internet -> 213.85.201.0 /29 – **Rede pública**
- **Garanta que a sua rede está funcional e que todos os PC (sede, Lisboa, Porto) acedem às diferentes redes internas, externa, DMZ e ISP. Teste toda a rede e verifique que tudo está a funcionar corretamente.**

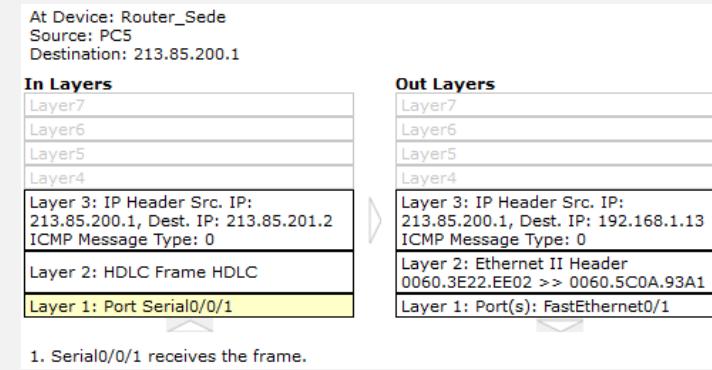
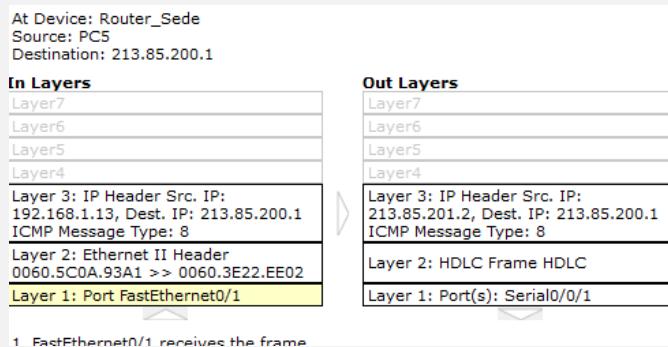
Exercício - Configurar o NAT com o Cisco Packet Trace

Exercício

- Implemente o NAT estático para o Portal da organização (10.1.1.XX) que está instalado numa máquina que está na rede DMZ da sede. Este servidor deverá sair com um IP da rede pública (213.85.203.4)
- Garanta que esta máquina continua a aceder a todas as redes da empresa e à rede do ISP.
- Faça uma análise dos pacotes de dados antes e depois do router e verifique que alterações aconteceram para as seguintes situações:
 - Quando o servidor acede a uma máquina da rede do ISP.
 - Quando a máquina acede a uma máquina de uma rede local da empresa.

Exercício

- Implemente o PAT (Network Address Port Translation) ou NAT Overload para todas as máquinas da empresa com exceção da rede externa utilizando o IP da interface da rede publica do router da sede (Router_sede).
- Garanta que a sua rede está funcional e que todos os PC e servidores (sede, Porto e Lisboa) acedem a todas as redes internas e à rede do ISP.
- Faça as alterações necessárias às rotas...
- Faça uma análise dos pacotes de dados antes e depois do router e verifique que as alterações aconteceram.



Exercício

- De uma máquina da rede externa da empresa chegue ao servidor de uma máquina do ISP. Veja o que acontece ao endereço IP durante esse caminho.

How To

NAT estático: configuração

Configuring Static NAT

Server
192.168.10.254

R2

S0/0/0
10.1.1.2

S0/1/0
209.165.200.225

Inside network

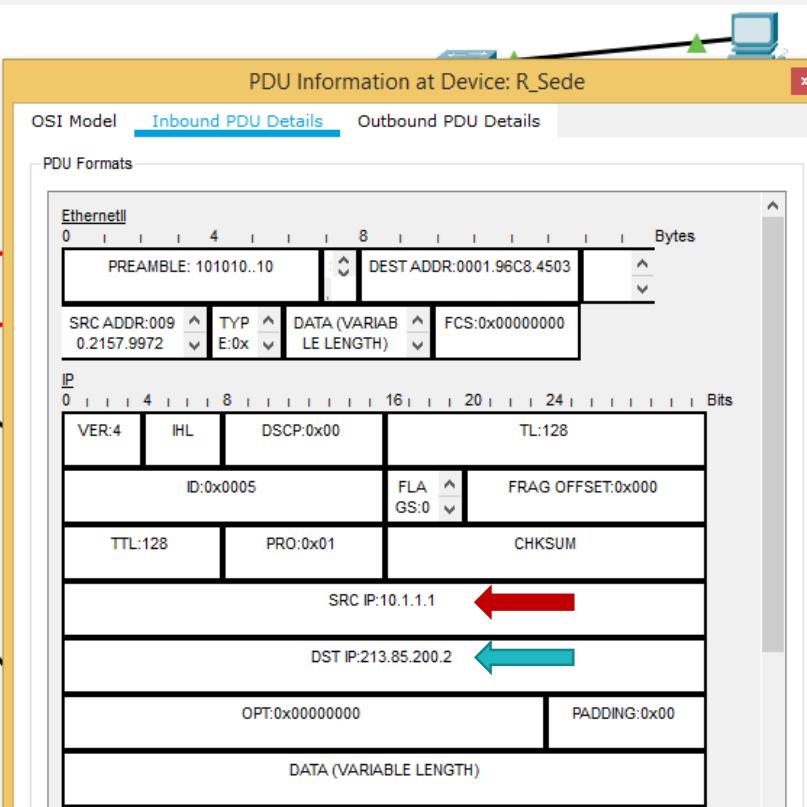
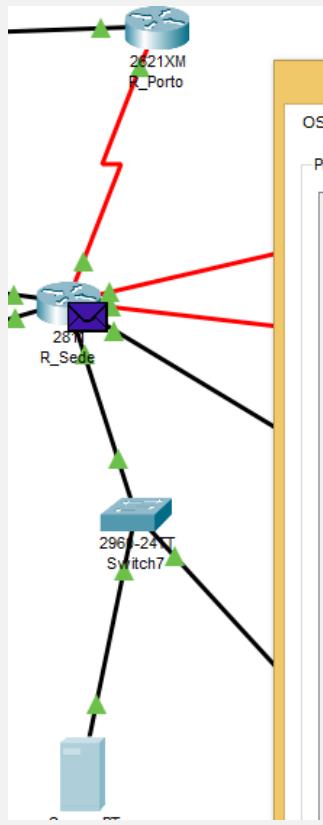
Internet

```
ip nat inside source static 192.168.10.254 209.165.200.254
!—Establishes static translation between an inside local address and an inside global address.
interface serial 0/0/0
ip nat inside
!—Identifies Serial 0/0/0 as an inside NAT interface.
interface serial 0/1/0
ip nat outside
!—Identifies Serial 0/1/0 as an outside NAT interface.
```

With this configuration, 192.168.10.254 will always translate to 209.165.200.254

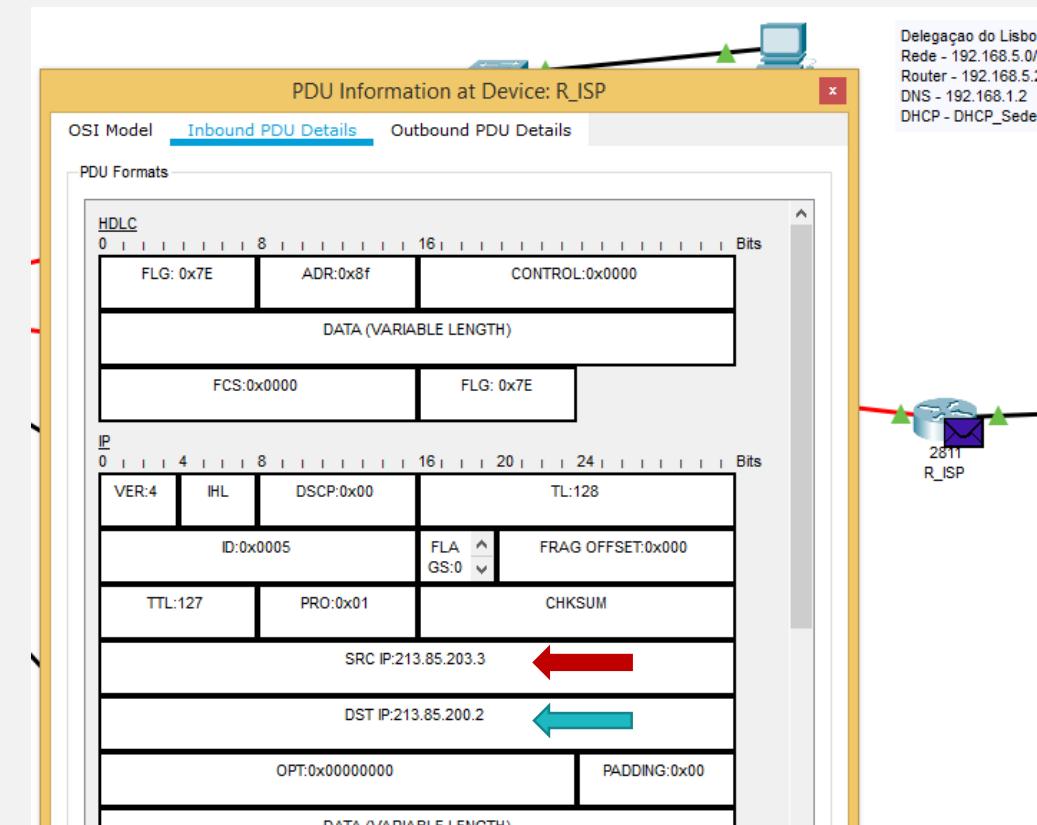
NAT Estático

Sentido Rede Interna -> Rede Externa



Antes do Router de Saída (R_Sede)

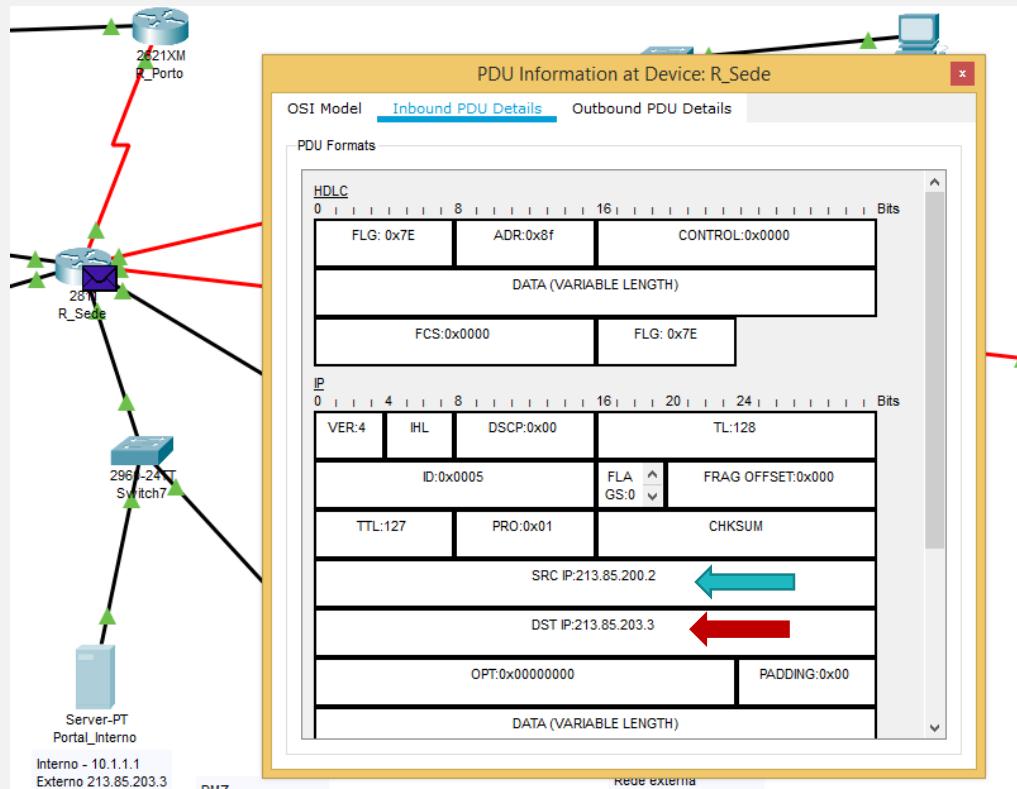
213.85.203.3 -> 10.1.1.1



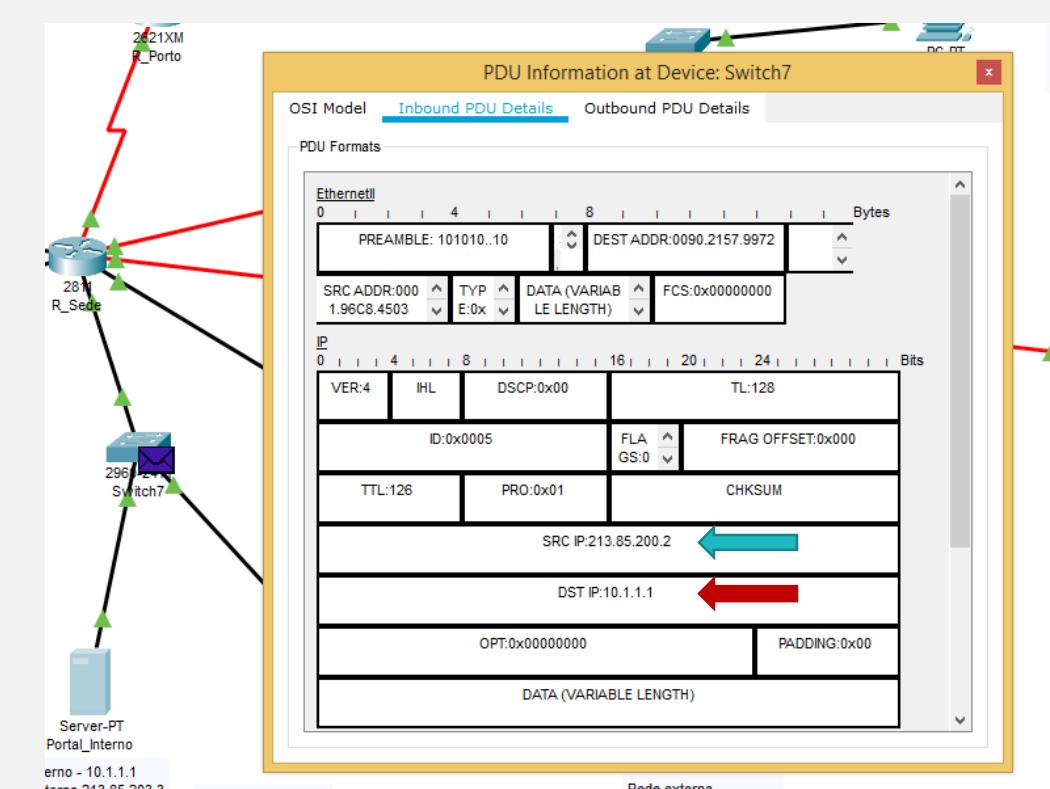
Depois do Router de Saída (R_Sede)

NAT Estático

Sentido Rede Externa -> Rede Interna

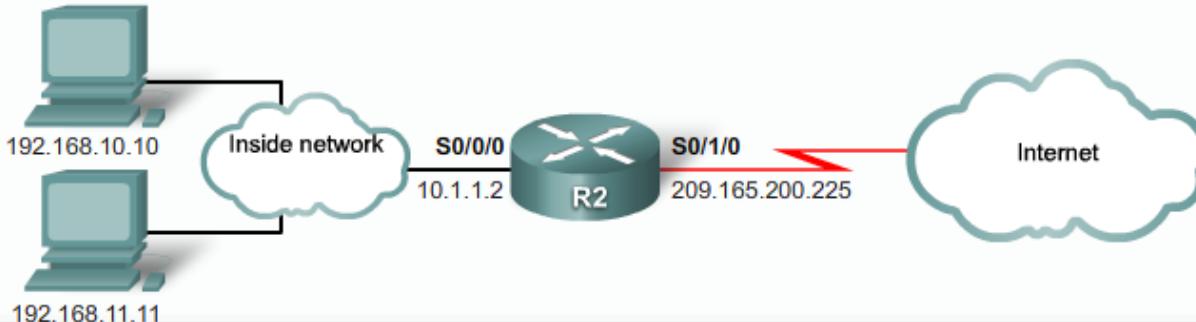


Antes do Router de Saída

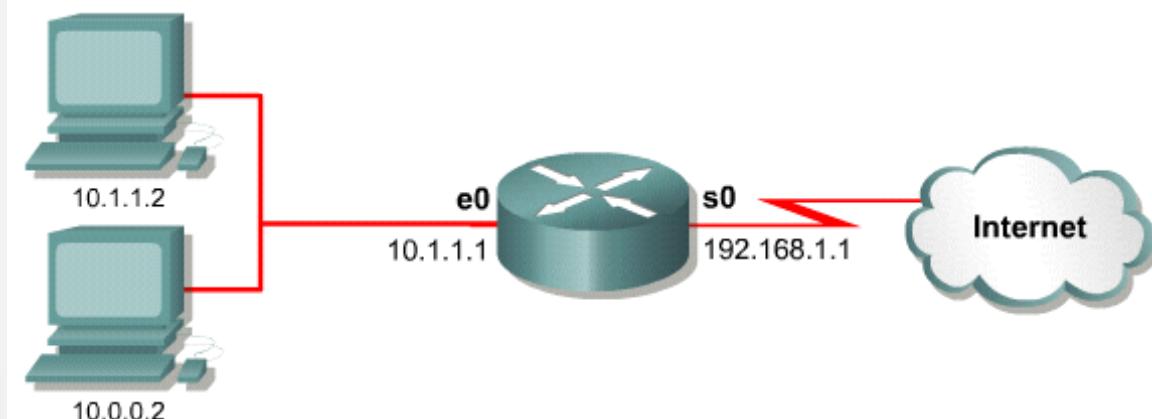


Depois do Router de Saída

NAT dinâmico



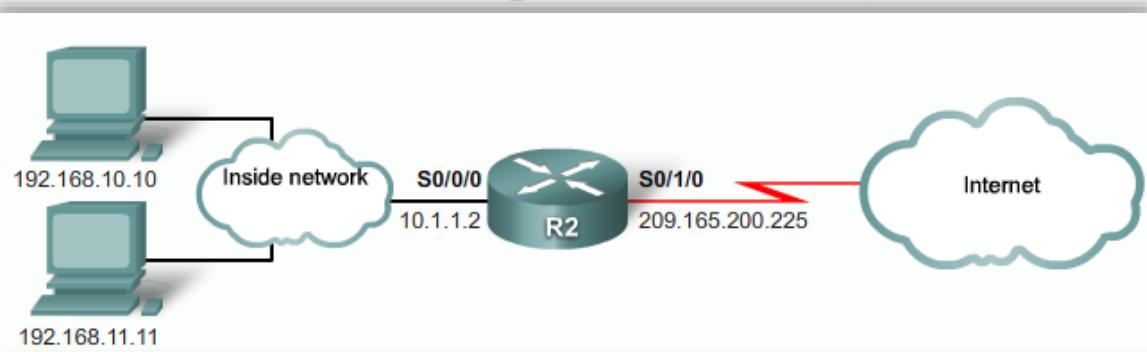
```
ip nat pool NAT-POOL1 209.165.200.226 209.165.200.240 netmask 255.255.255.224
!—Defines a pool of public IP addresses under the pool name NAT-POOL1
access-list 1 permit 192.168.0.0 0.0.255.255
!—Defines which addresses are eligible to be translated
ip nat inside source list 1 pool NAT-POOL1
!—Binds the NAT pool with ACL 1
interface serial 0/0/0
 ip nat inside
!—Identifies interface Serial 0/0/0 as an inside NAT interface
interface serial 0/1/0
 ip nat outside
!—Identifies interface Serial 0/1/0 as the outside NAT interface
```



```
ip nat pool nat-pool 1 179.9.8.80 179.9.8.95 netmask 255.255.255.0
ip nat inside source list 1 pool nat-pool
!
interface ethernet 0
 ip address 10.1.1.1 255.255.255.0
 ip nat inside
!
interface serial 0
 ip address 192.168.1.1 255.255.255.0
 ip nat outside
!
access-list 1 permit 10.0.0.0 0.0.0.255.255
```

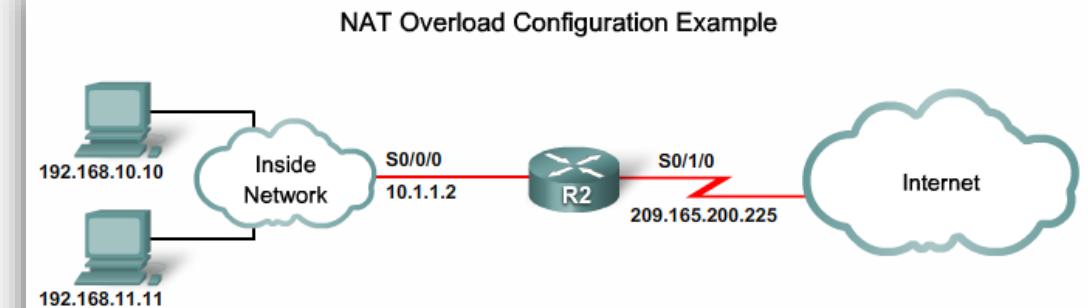
PAT (Network Address Port Translation) ou NAT Overload

Utilizando uma “pool” de endereços



```
access-list 1 permit 192.168.0.0 0.0.255.255
! - Defines which addresses are eligible to be translated
ip nat pool NAT-POOL2 209.165.200.226 209.165.200.240
! - Defines a pool of addresses named NAT-POOL2 to be used in NAT translation
ip nat inside source list 1 pool NAT-POOL2 overload
! - Binds the NAT pool with ACL 1
interface serial 0/0/0
ip nat inside
! - Identifies interface Serial 0/0/0 as an inside NAT interface
interface serial 0/1/0
ip nat outside
! - Identifies interface Serial 0/1/0 as an outside NAT interface
```

Utilizando um endereço

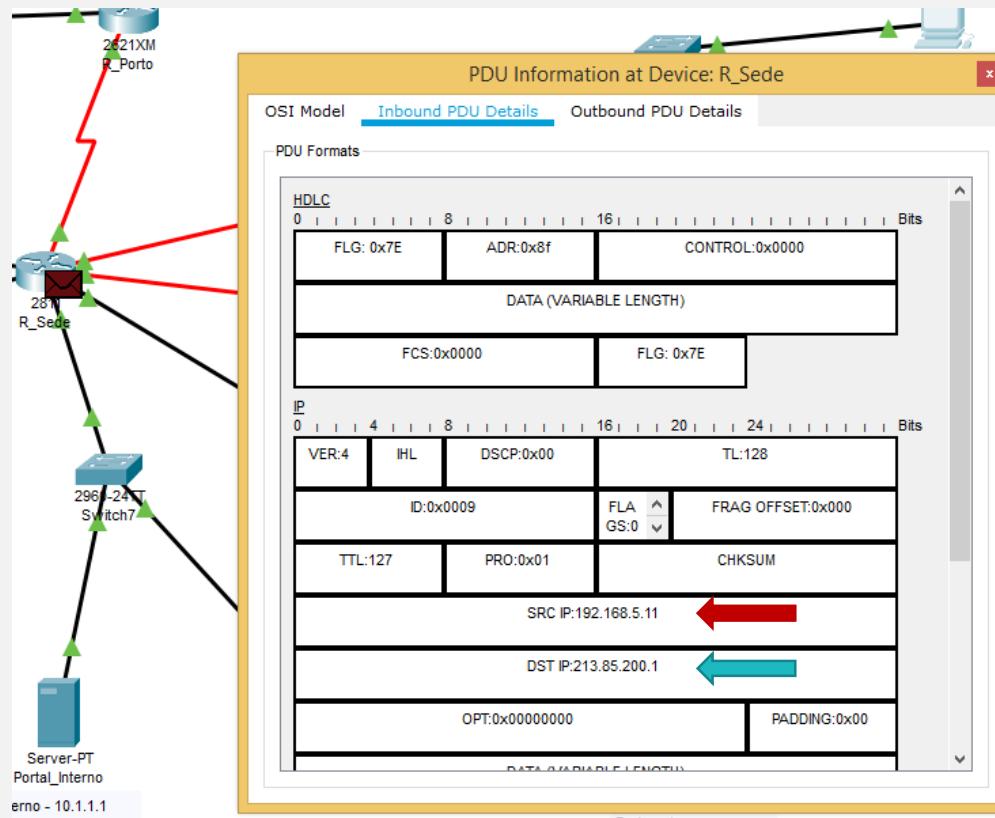


NAT Overload Configuration Example

```
access-list 1 permit 192.168.0.0 0.0.255.255
ip nat inside source list 1 interface serial 0/1/0 overload
interface serial 0/0/0
ip nat inside
interface serial 0/1/0
ip nat outside
```

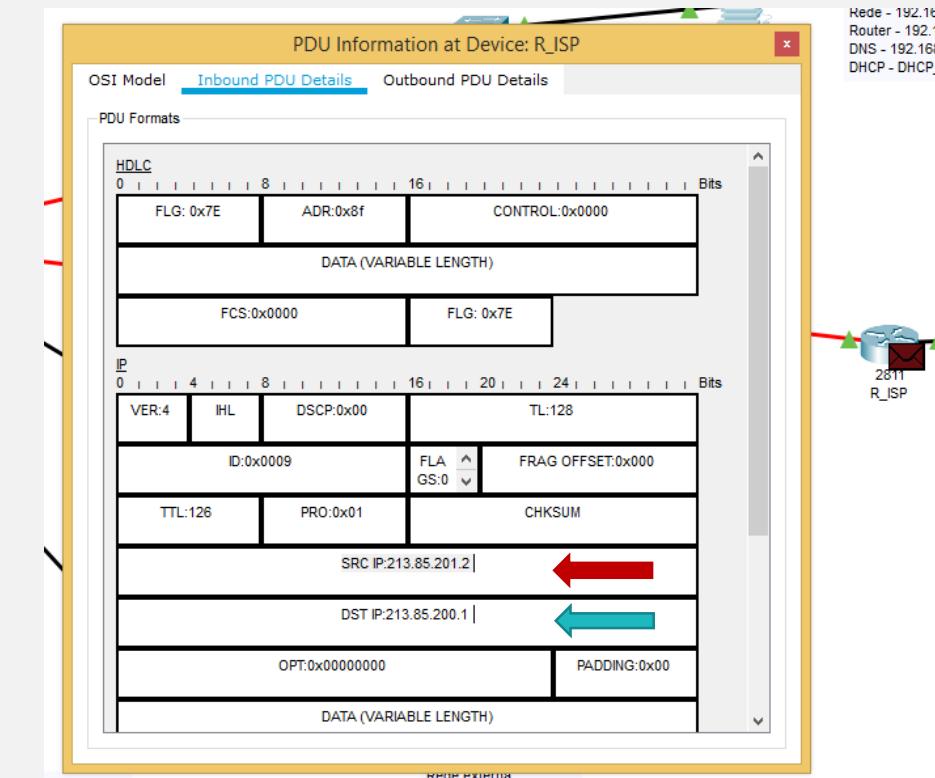
PAT (Network Address Port Translation) ou NAT Overload

Sentido Rede Interna -> Rede Externa



Antes do Router de Saída (R_sede)

192.168.5.11->213.85.201.2

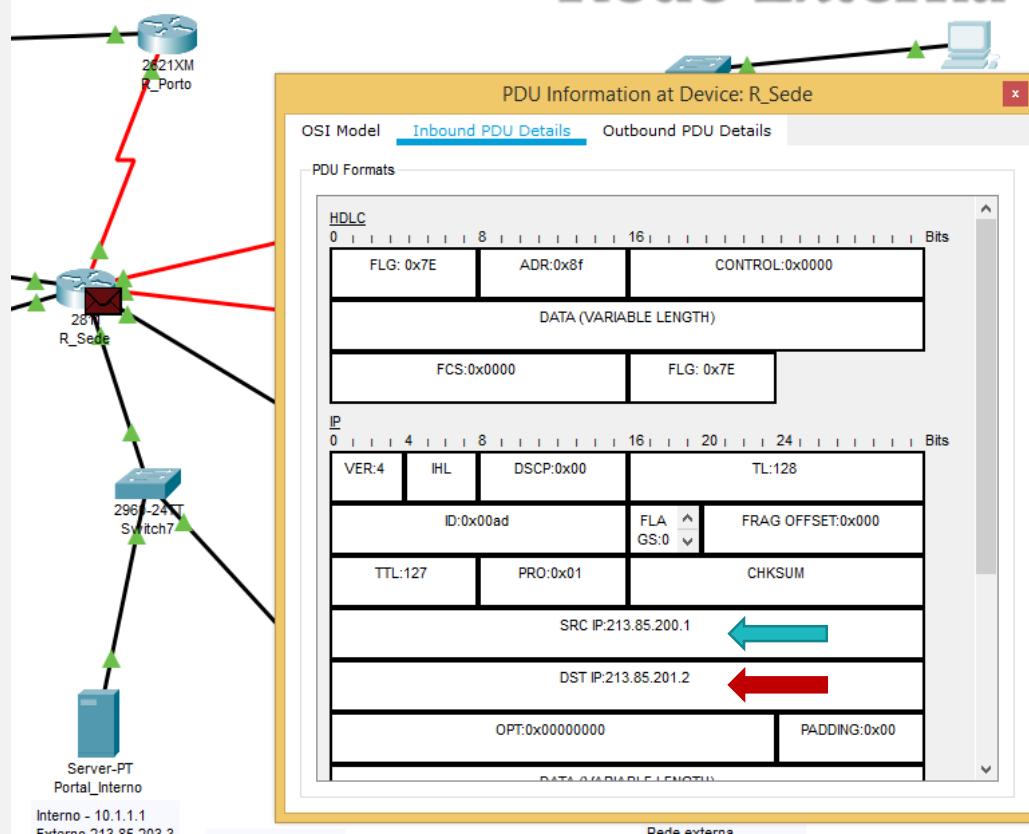


Depois do Router de Saída (R_Sede)

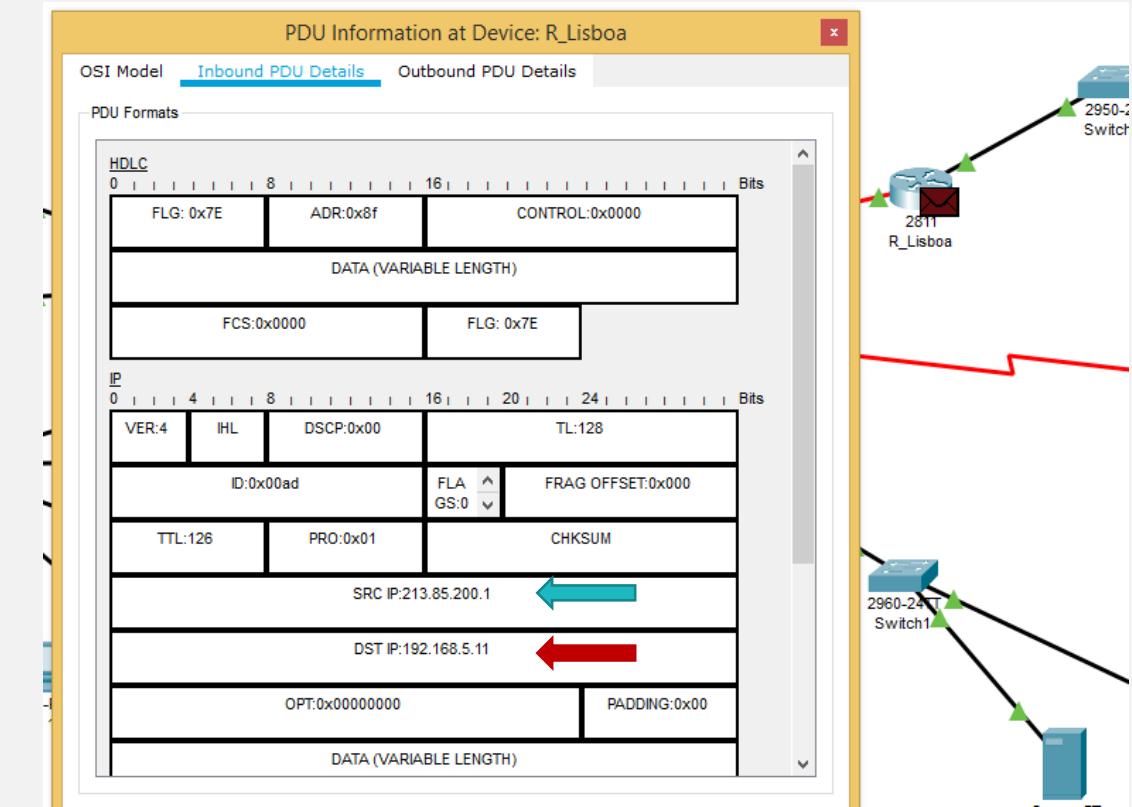
Rede - 192.168.
Router - 192.161.
DNS - 192.168.1
DHCP - DHCP_S

PAT (Network Address Port Translation) ou NAT Overload

Sentido Rede Externa -> Rede Interna



Antes do Router de Saída

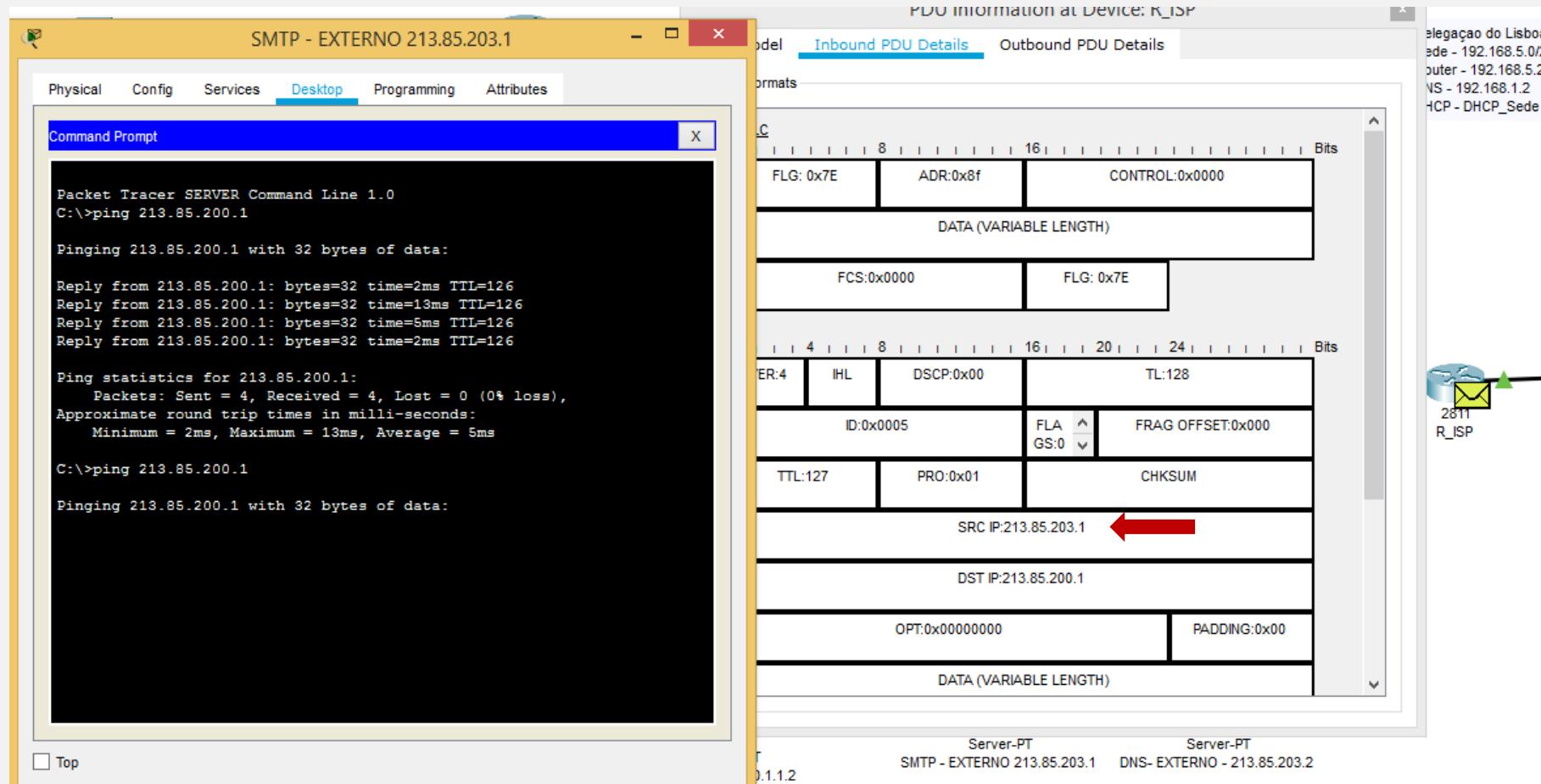


Depois do Router de Saída

213.85.201.2->192.168.5.11

Sem NAT

As máquinas da zona externa não devem ter NAT já que têm IP públicos



Verificação da configuração NAT

NAT Translations Example

```
R2#show ip nat translations
Pro Inside global      Inside local      Outside local      Outside global
tcp 209.165.200.225:16642 192.168.10.10:16642 209.165.200.254:80 209.165.200.254:80
tcp 209.165.200.225:62452 192.168.11.10:62452 209.165.200.254:80 209.165.200.254:80
```

```
R2#show ip nat translations verbose
Pro Inside global      Inside local      Outside local      Outside global
tcp 209.165.200.225:16642 192.168.10.10:16642 209.165.200.254:80 209.165.200.254:80
  create 00:01:45, use 00:01:43 timeout:86400000, left 23:58:16, Map-Id(In): 1,
  flags:
extended, use_count: 0, entry_id: 4, lc_entries: 0
tcp 209.165.200.225:62452 192.168.11.10:62452 209.165.200.254:80 209.165.200.254:80
  create 00:00:37, use 00:00:35 timeout:86400000, left 23:59:24, Map-Id(In): 1,
  flags:
extended, use_count: 0, entry_id: 5, lc_entries: 0
R2#
```

NAT Translations Example

```
R2#show ip nat translations
Pro Inside global      Inside local      Outside local      Outside global
icmp 209.165.200.225:3 192.168.10.10:3 209.165.200.254:3 209.165.200.254:3
tcp 209.165.200.225:11679 192.168.10.10:11679 209.165.200.254:80 209.165.200.254:80
icmp 209.165.200.225:0 192.168.11.10:0 209.165.200.254:0 209.165.200.254:0
tcp 209.165.200.225:14462 192.168.11.10:14462 209.165.200.254:80 209.165.200.254:80
```

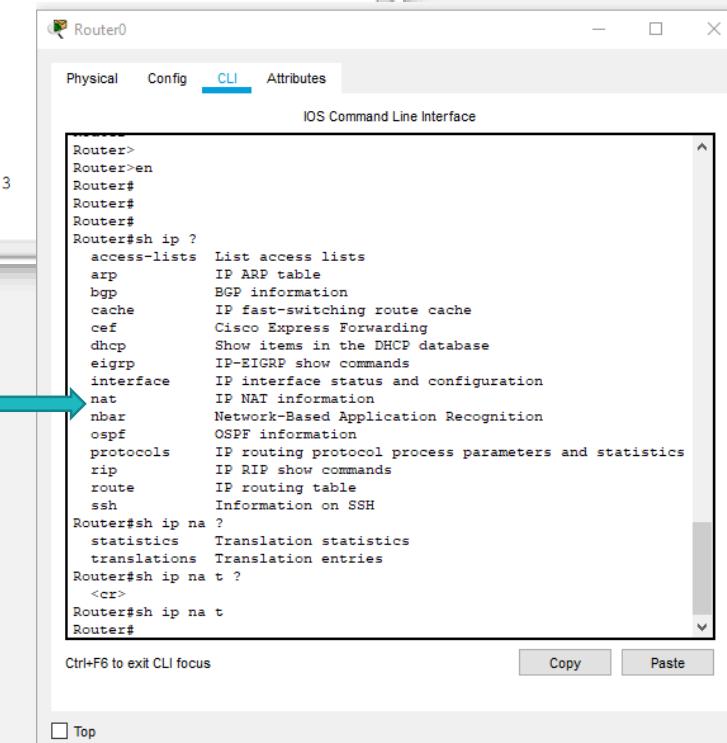
```
R2#show ip nat statistics
Total active translations: 3 (0 static, 3 dynamic; 3 extended)
Outside interfaces:
  Serial0/1/0
Inside interfaces:
  Serial0/0/0, Serial0/0/1
  Hits: 173  Misses: 9
CEF Translated packets: 182, CEF Punted packets: 0
Expired translations: 6
Dynamic mappings:
-- Inside Source
[Id: 1] access-list 1 interface Serial0/1/0 refcount 3
Queued Packets: 0
R2#
```

Clearing NAT Translations

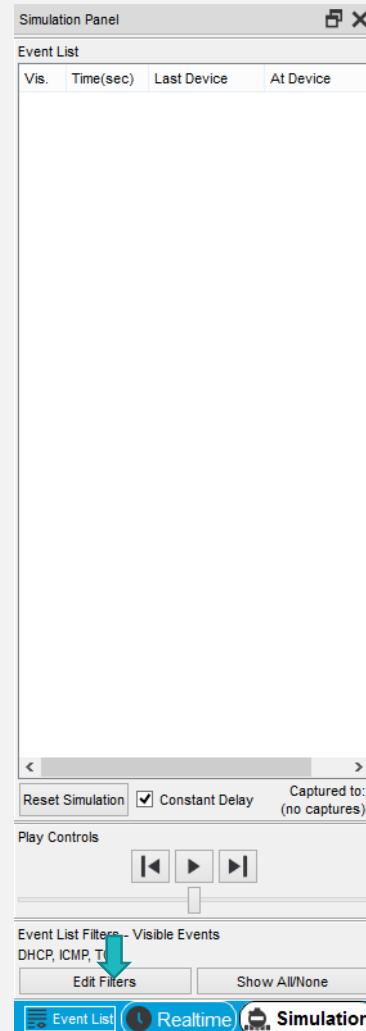
```
R2#clear ip nat translation *
R2#show ip nat translations
```

```
R2#
```

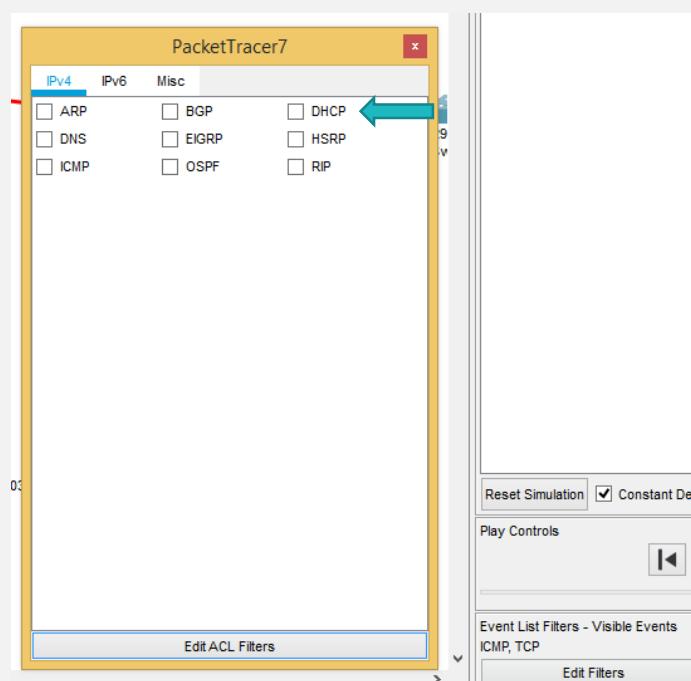
Command	Description
clear ip nat translation *	Clears all dynamic address translation entries from the NAT translation table
clear ip nat translation inside global-ip local-ip [outside local-ip global-ip]	Clears a simple dynamic translation entry containing an inside translation or both inside and outside translation
clear ip nat translation protocol inside global-ip global-port local-ip local-port [outside local-ip local-port global-ip global-port]	Clears an extended dynamic translation entry



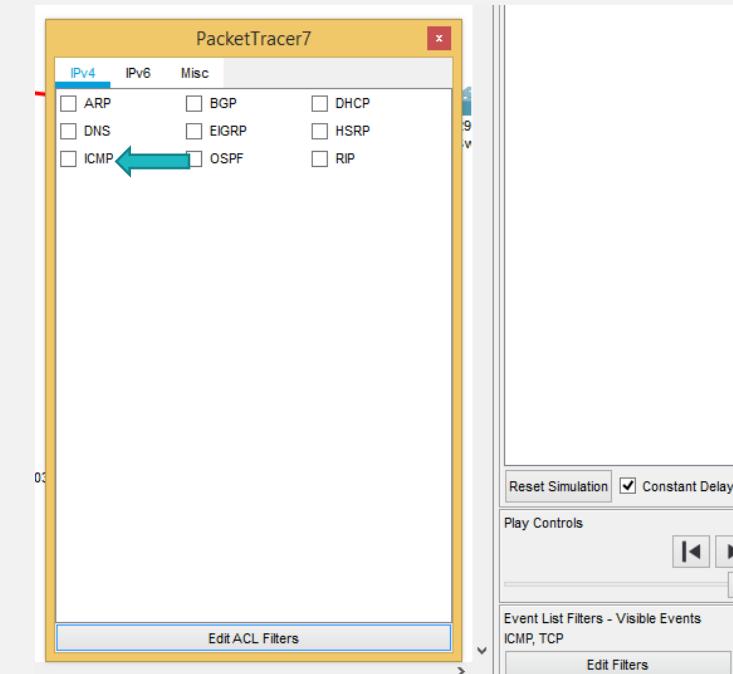
Modo de simulação no PT



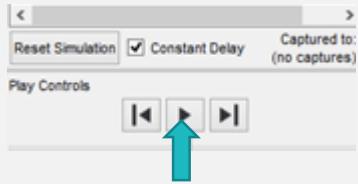
Escolhe o que deseja ver.
No caso de estar a
analisar o DHCP:



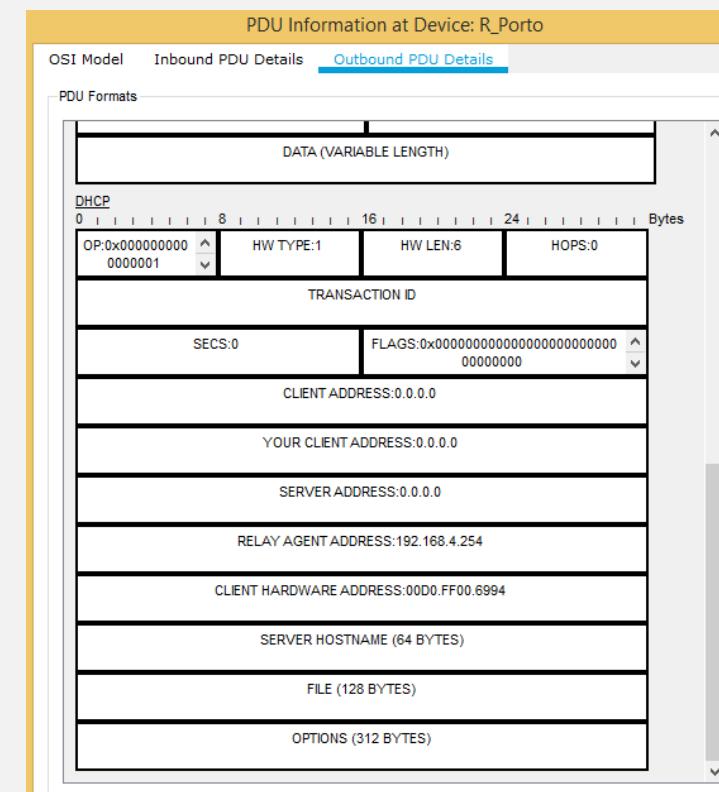
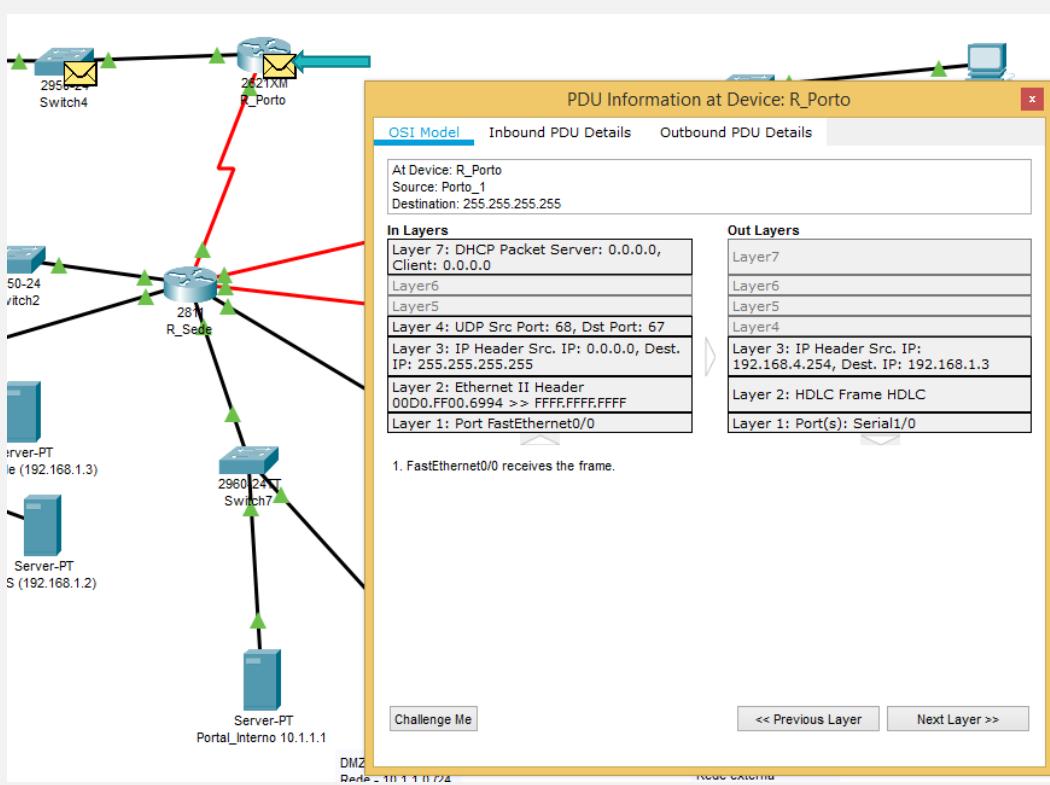
Escolhe o que deseja ver.
No caso de uma análise
genérica IP.



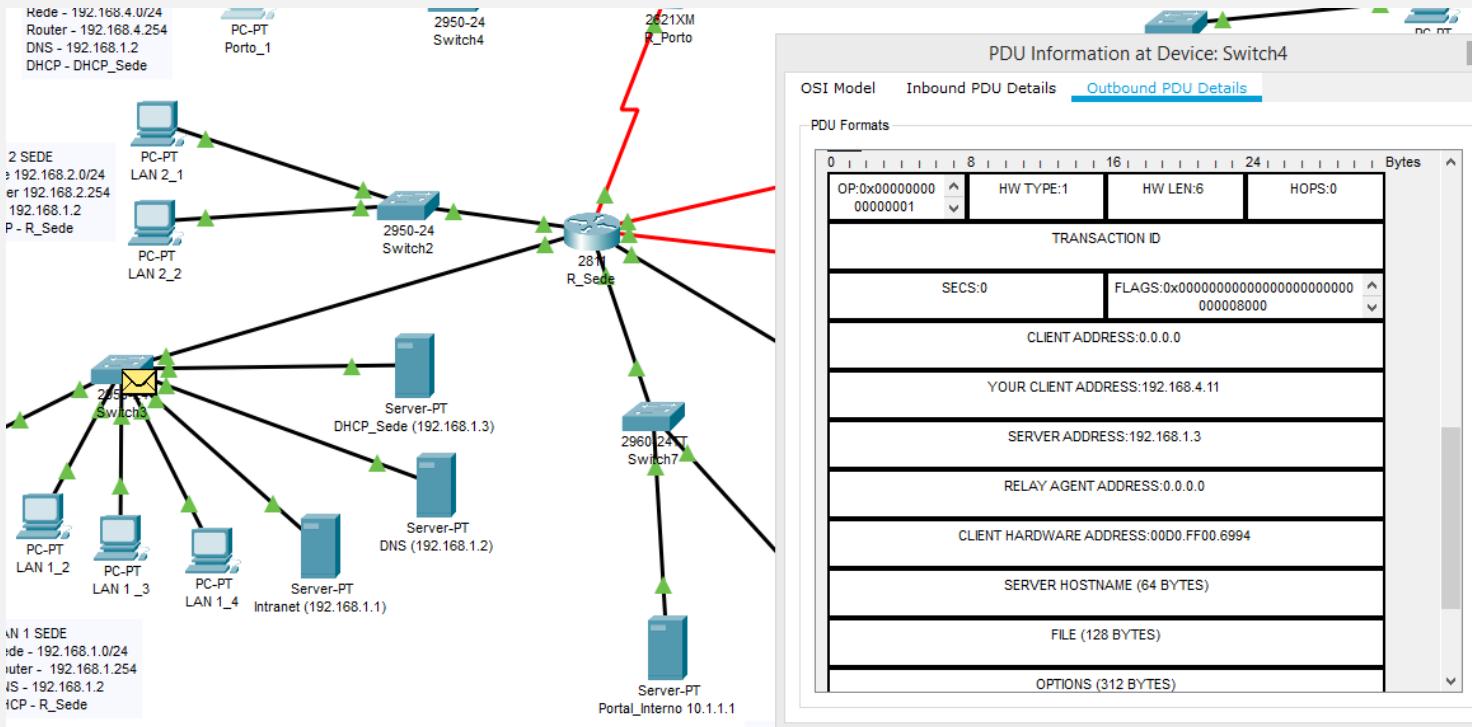
Modo de simulação no PT



Para analisar o pacote de informação, clicar em cima do envelope:



DHCP - Exemplo



Dúvidas



Serviços de Rede 1 – **Aula 6 - Práticas**

2022-2023

Instituto Politécnico de Coimbra

Departamento de Engenharia Informática



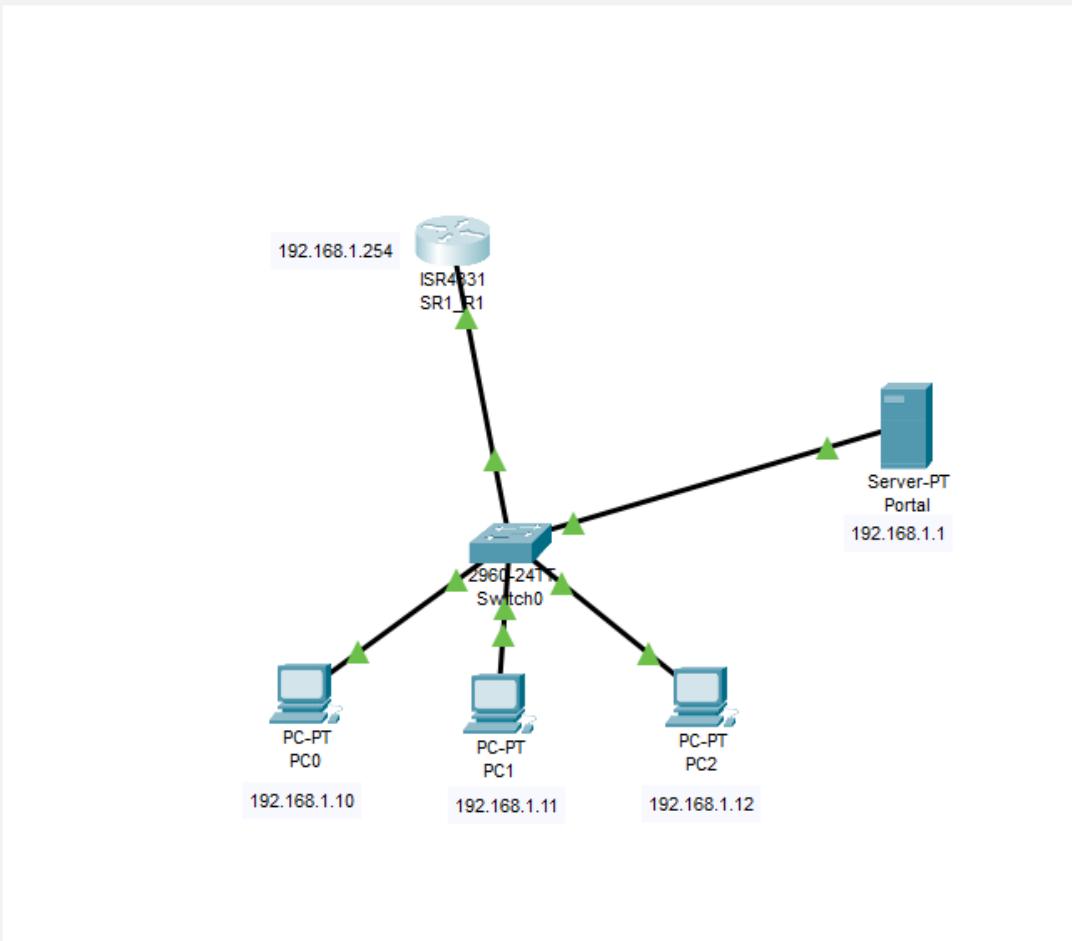
Pre – Requisitos

- Ter instalado o *Cisco Packet Tracer* versão 8.2.0



Exercício 1 - Configurar o “DNS” num router

Exercício 1



Exercício 1

- Faça a topologia do *slide* anterior no simulador Packet Tracer.
- O nome do router é SR1_R1 e a password de enable é “sr1”.
- Os endereços IP das maquinas (PC, Servidor e Router) estão definidos no desenho e são para colocar de forma manual. A rede é 192.168.1.0 /24.
- Coloque a descrição na interface que liga o router à rede como “Interface Rede Local”.
- Desabilite no router a possibilidade de ele fazer consultas DNS.
- Teste a conetividade do router para os PC e para o servidor.
- Define a possibilidade de chegar por nome às máquinas quando está no router. Teste essa ligação. **Nota:** Isto não é ter um serviço de DNS....

Exercício 1

- Coloque num PC o router como DNS server. Entre em modo de simulação ativando apenas o visionamento dos pacotes DNS. O que se passa?
- Infelizmente o *Packet Tracer* não tem o comando que permite ativar o router como um DNS Server (ip dns server). Temos assim de encontrar outra solução....
- Grave o ficheiro como *Primeiro nome_último nome_aula6_ex1*

How To

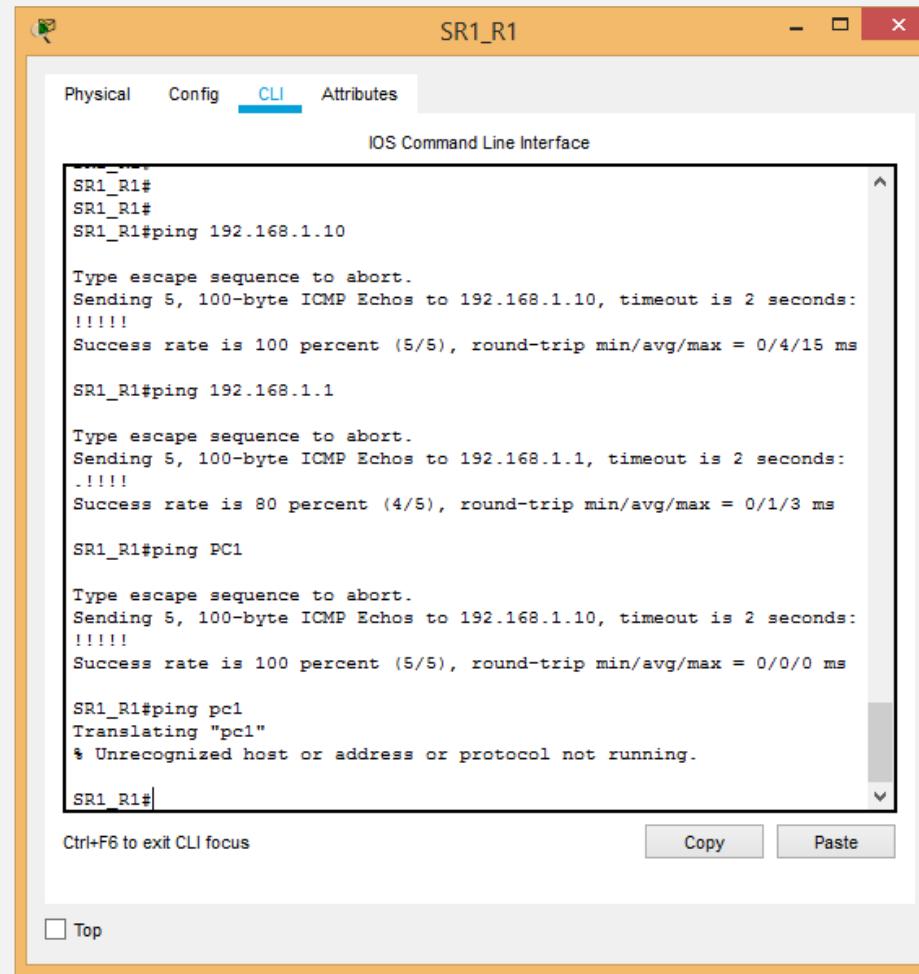
Colocar hosts num Router

The screenshot shows a Cisco IOS Command Line Interface (CLI) window titled "SR1_R1". The window has tabs for "Physical", "Config", "CLI" (which is selected), and "Attributes". The main area displays the following configuration commands:

```
SR1_R1(config-if)#  
SR1_R1(config-if)#exit  
SR1_R1(config)#ip ?  
access-list      Named access-list  
cef             Cisco Express Forwarding  
default-gateway Specify default gateway (if not routing IP)  
default-network Flags networks as candidates for default routes  
dhcp             Configure DHCP server and relay parameters  
domain           IP DNS Resolver  
domain-lookup   Enable IP Domain Name System hostname translation  
domain-name     Define the default domain name  
flow-export     Specify host/port to send flow statistics  
forward-protocol Controls forwarding of physical and directed IP  
broadcasts  
  ftp            FTP configuration commands  
  host           Add an entry to the ip hostname table  
  local          Specify local options  
  name-server    Specify address of name server to use  
  nat            NAT configuration commands  
  route          Establish static routes  
  routing        Enable IP routing  
  scp            Scp commands  
  ssh            Configure ssh options  
  tcp            Global TCP parameters  
SR1_R1(config)#ip host PC1 192.168.1.10  
SR1_R1(config)#ip host PC2 192.168.1.11  
SR1_R1(config)#ip host PC3 192.168.1.12  
SR1_R1(config)#
```

At the bottom of the window, there are buttons for "Copy" and "Paste". A checkbox labeled "Top" is located at the very bottom left.

Testar a conectividade



The screenshot shows a Windows application window titled "SR1_R1". The window has tabs at the top: "Physical", "Config", "CLI" (which is selected), and "Attributes". Below the tabs is a title bar "IOS Command Line Interface". The main area contains the following CLI session output:

```
SR1_R1#
SR1_R1#
SR1_R1#ping 192.168.1.10
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 192.168.1.10, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 0/4/15 ms

SR1_R1#ping 192.168.1.1
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 192.168.1.1, timeout is 2 seconds:
..!!!!
Success rate is 80 percent (4/5), round-trip min/avg/max = 0/1/3 ms

SR1_R1#ping PC1
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 192.168.1.10, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 0/0/0 ms

SR1_R1#ping pc1
Translating "pc1"
% Unrecognized host or address or protocol not running.

SR1_R1#
```

At the bottom of the window, there are buttons for "Copy" and "Paste". A status message "Ctrl+F6 to exit CLI focus" is also present. A checkbox labeled "Top" is located at the very bottom left.

Simulação

Realtime Simulation

PacketTracer7

IPv4 IPv6 Misc

ARP BGP DHCP
DNS EIGRP HSRP
ICMP OSPF RIP

PC0

Physical Config Desktop Programming Attributes

Command Prompt

Packet Tracer PC Command Line 1.0
C:\>ping pc1.sr1.pt

ISR431 SR1_R1
192.168.1.254

Switch0
192.0.241

PC-PT PC0
192.168.1.10

PC-PT PC1
192.168.1.11

PC-PT PC2
192.168.1.12

Server-PT Portal
192.168.1.1

PDU Information at Device: PC0

OSI Model Outbound PDU Details

PDU Formats

DATA (VARIABLE LENGTH)

DNS Message

QDCOUNT: 1	ANCOUNT: 0
NSCOUNT: 0	ARCOUNT: 0

DNS Query

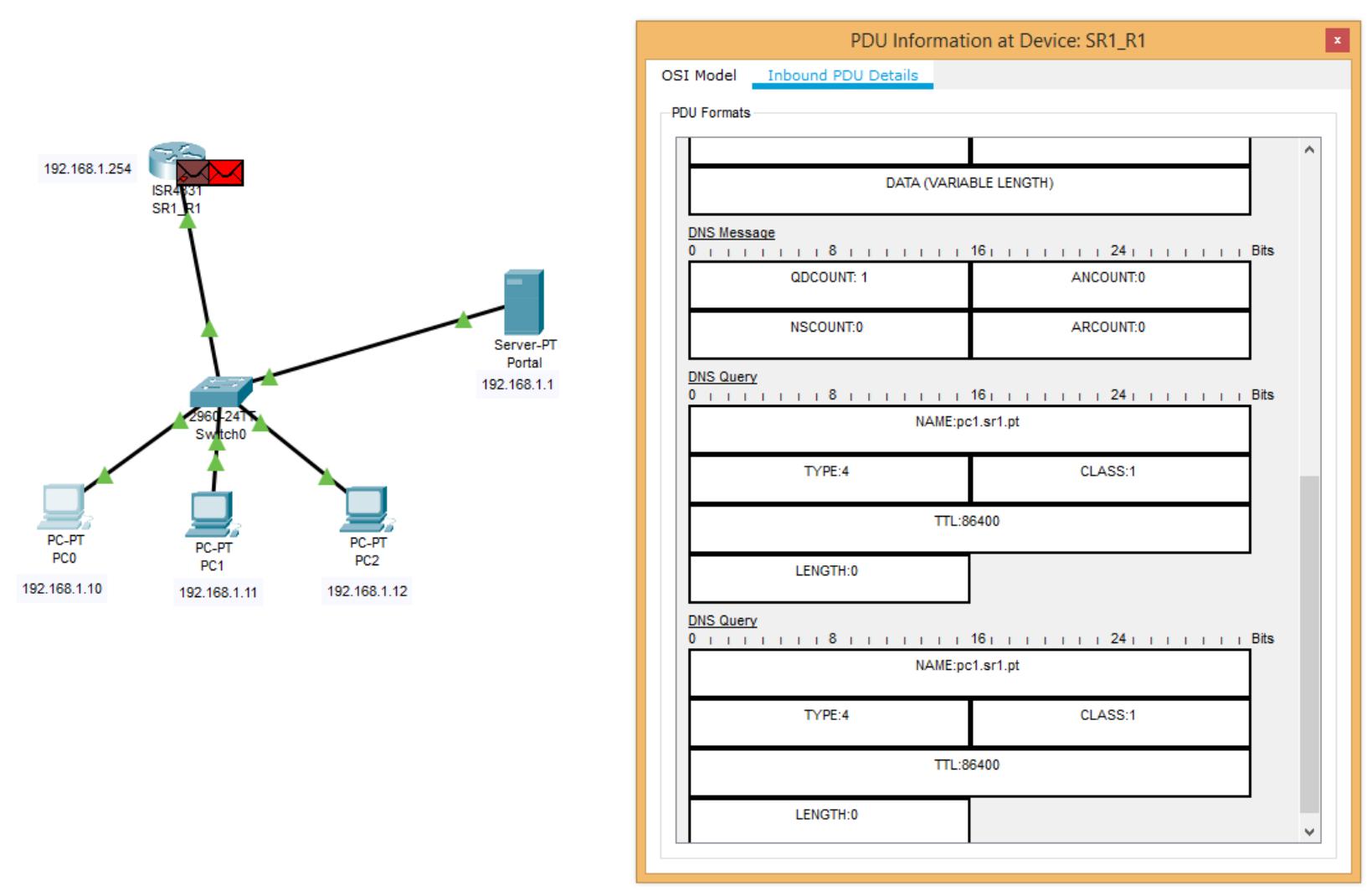
NAME:pc1.sr1.pt	
TYPE:4	CLASS:1
TTL:86400	
LENGTH:0	

DNS Query

NAME:pc1.sr1.pt	
TYPE:4	CLASS:1
TTL:86400	
LENGTH:0	

Edit ACL Filters

Simulação



Exercício 2 – Configurar o DNS no *Packet Tracer*

Exercício 2

- Desabilite todos os serviços do servidor Portal (192.168.1.1) com exceção do HTTP.
- Configure a página de entrada para que está fique com o seguinte aspeto e ainda a página objetivos da cadeira:

The screenshot shows a web browser window titled 'PC0'. The address bar displays 'http://192.168.1.1/index.html'. The main content area shows the text 'Bem vindo ao Portal da Disciplina de SR1' and a navigation menu with 'Opções' and 'Objetivos' underlined. To the right, a sidebar titled 'Objetivos da cadeira' lists the following items:

- Endereçamento dinâmico (DHCP).
- Translação de endereços (NAT).
- Resolução de nomes (DNS).
- Acesso remoto (VPNs).
- Serviços de Proxy.
- Serviços de sincronização de relógio (NTP).
- Aplicação dos conceitos na configuração de uma rede empresarial

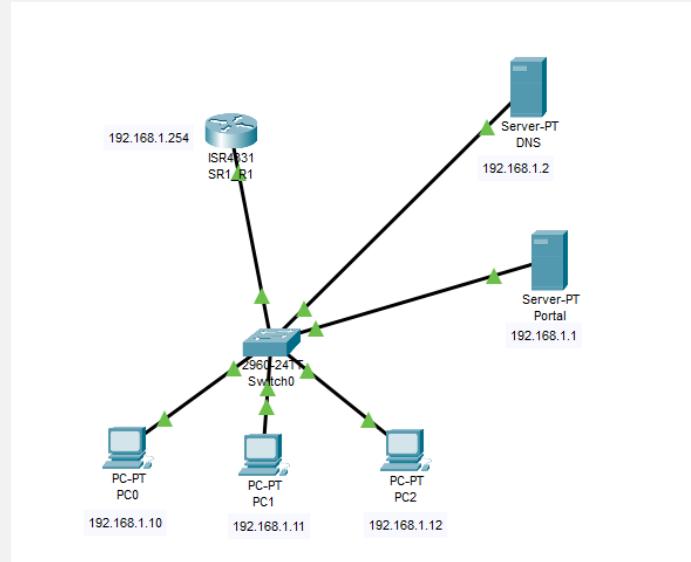
A blue arrow points from the 'Objetivos' menu item in the browser to the 'Objetivos da cadeira' sidebar.

- Teste o acesso de um PC a essas páginas.

The image contains two side-by-side screenshots of a web browser window titled 'PC0'. Both screenshots show the same interface: a top menu with tabs 'Physical', 'Config', 'Desktop' (which is selected), 'Programming', and 'Attributes'; a toolbar with 'Web Browser' buttons; and a main content area with the text 'Bem vindo ao Portal da Disciplina de SR1' and a navigation menu with 'Opções' and 'Objetivos'. The left screenshot shows the 'Objetivos' page, while the right screenshot shows a different page with the same layout and content, indicating a successful test of the configured pages.

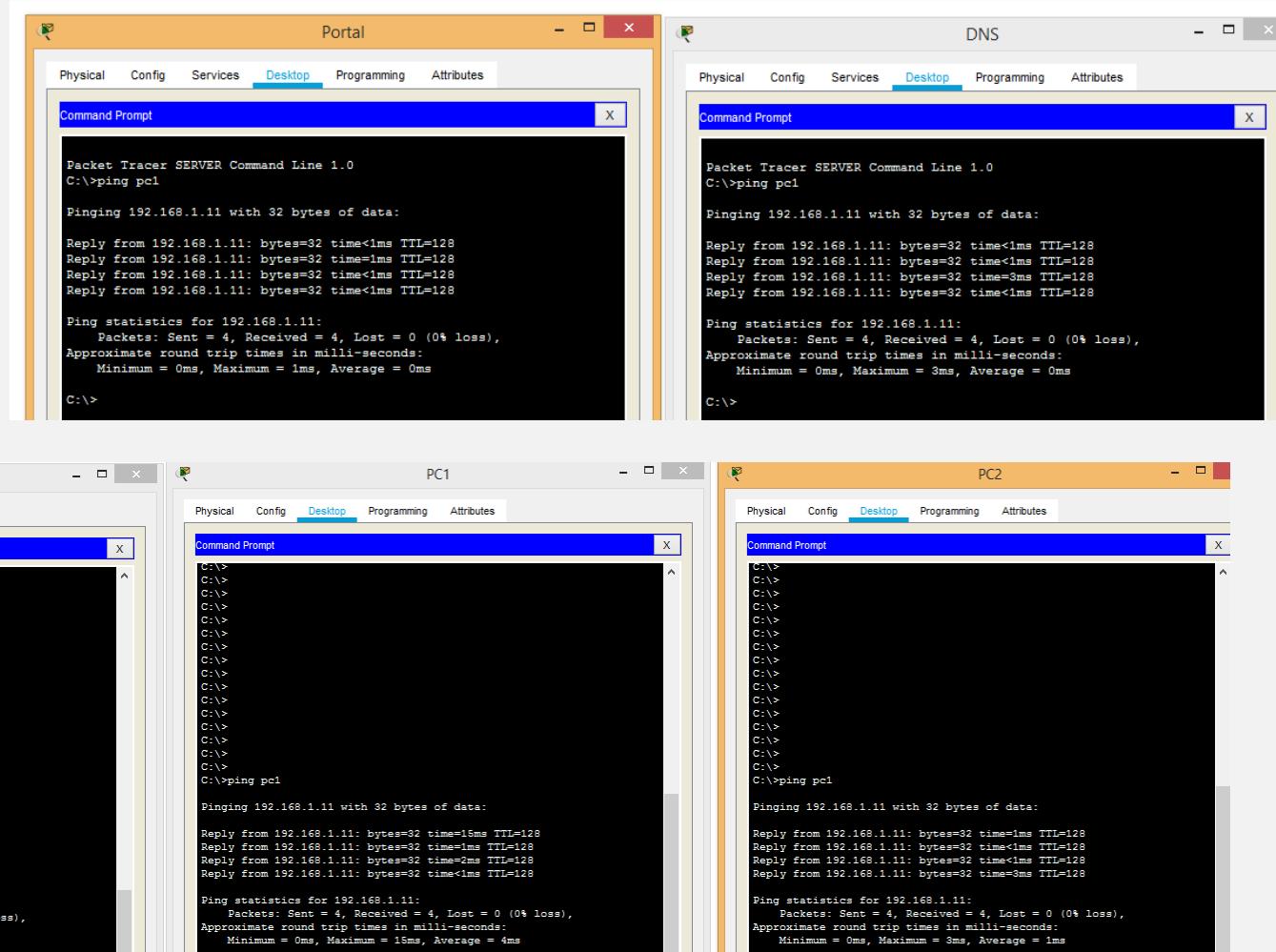
Exercício 2

- Coloque um novo servidor na topologia. Deve ficar no endereço 192.168.1.2 e com o nome de DNS
- Teste a sua ligação à rede.
- Desabilite todos os serviços deste novo servidor com exceção do DNS.
- Acrescente no servidor DNS um registo do tipo A para que seja possível atingir o PC1 por nome.



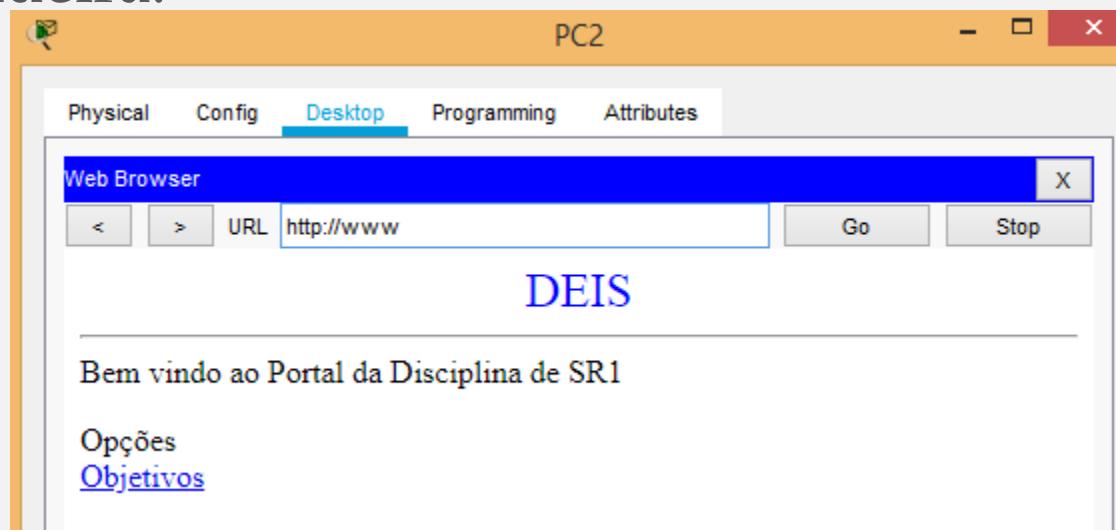
Exercício 2

- Faça as alterações necessárias em todas as máquinas da rede (PC e servidores) para que seja possível atingir o PC1 por nome. Teste em todos.



Exercício 2

- Configure o seu servidor de DNS para conseguir atingir **todos** os equipamentos da sua rede por nome.
- Teste se consegue chegar ao servidor www por nome acedendo à página da cadeira.



Exercício 2

- Apague as configurações os hosts que tinha configurado no seu router. Ative a possibilidade de ele fazer consultas DNS.
- Altere a configuração do router para ele “use” como servidor de DNS o 192.168.1.2 e consiga assim chegar às máquinas da sua rede por nome.

```
SR1_R1#
SR1_R1#
SR1_R1#ping pc1
Translating "pc1"...domain server (192.168.1.2)
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 192.168.1.11, timeout is 2 seconds:
!!!!!
Success rate is 80 percent (4/5), round-trip min/avg/max = 0/1/3 ms

SR1_R1#ping pc2
Translating "pc2"...domain server (192.168.1.2)
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 192.168.1.12, timeout is 2 seconds:
!!!!!
Success rate is 80 percent (4/5), round-trip min/avg/max = 3/3/3 ms

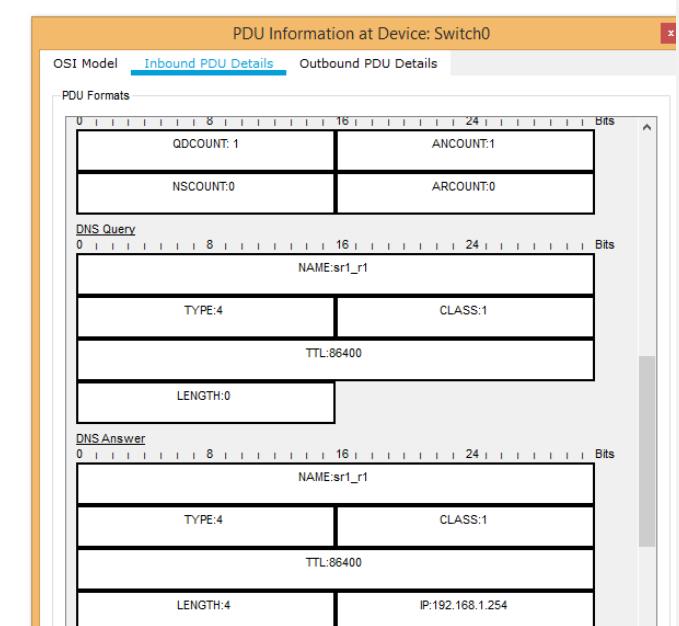
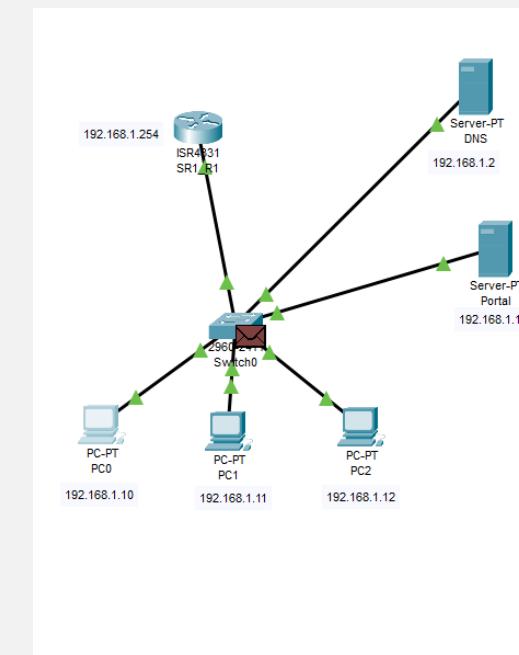
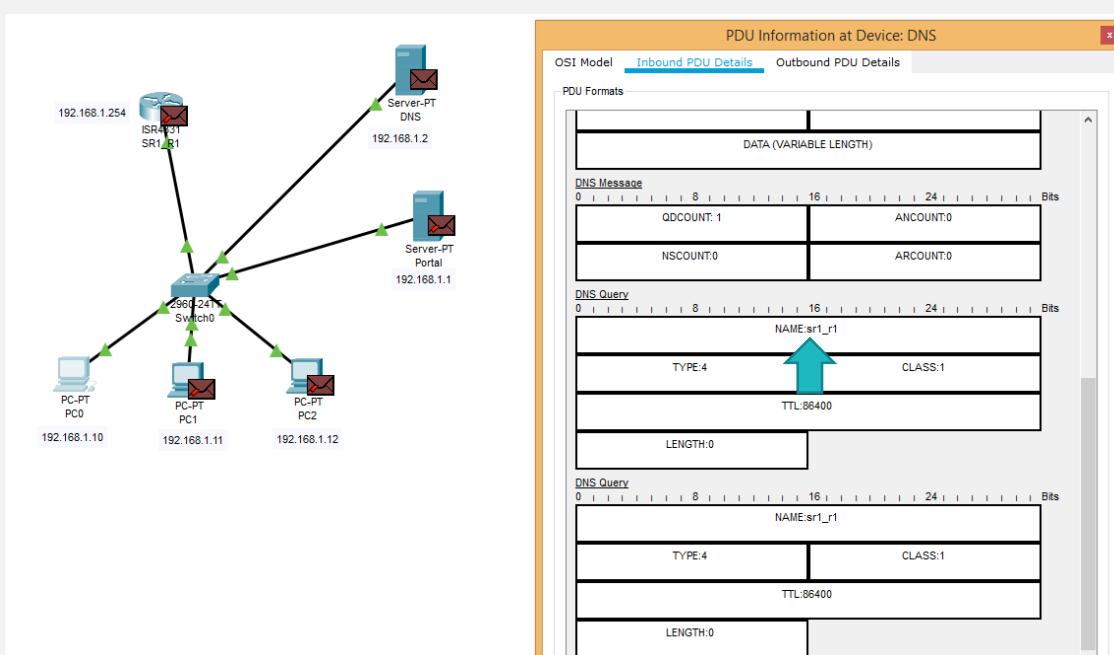
SR1_R1#ping pc4
Translating "pc4"...domain server (192.168.1.2)
* Unrecognized host or address or protocol not running.

SR1_R1#ping www
Translating "www"...domain server (192.168.1.2)
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 192.168.1.1, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 0/1/3 ms

SR1_R1#
```

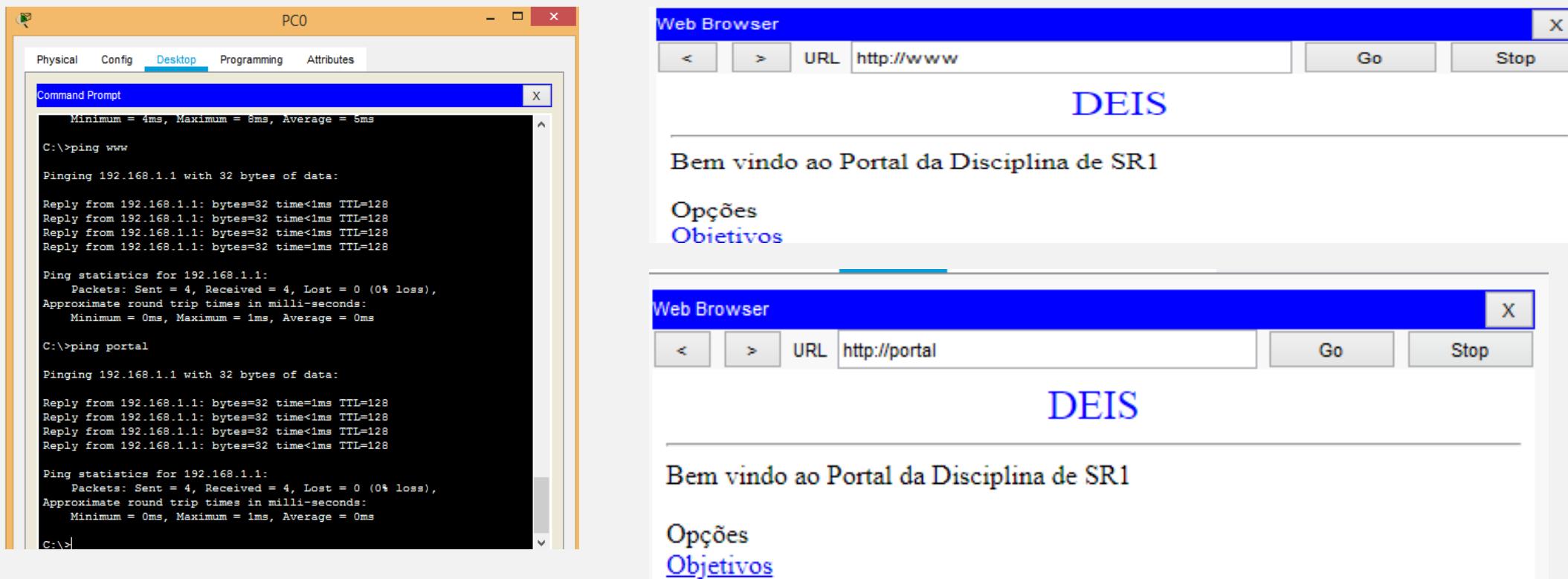
Exercício 2

- Coloque um novo registo no seu servidor de DNS para o router (nome SR1_R1).
- Entre em modo de simulação e analise os pacotes DNS resultantes quando faz um ping do PC0 para o Router por nome.



Exercido 2

- Faça a alteração necessária no seu servidor de DNS para que o servidor 192.168.1.1 seja possível atingir pelo nome de www e de portal.

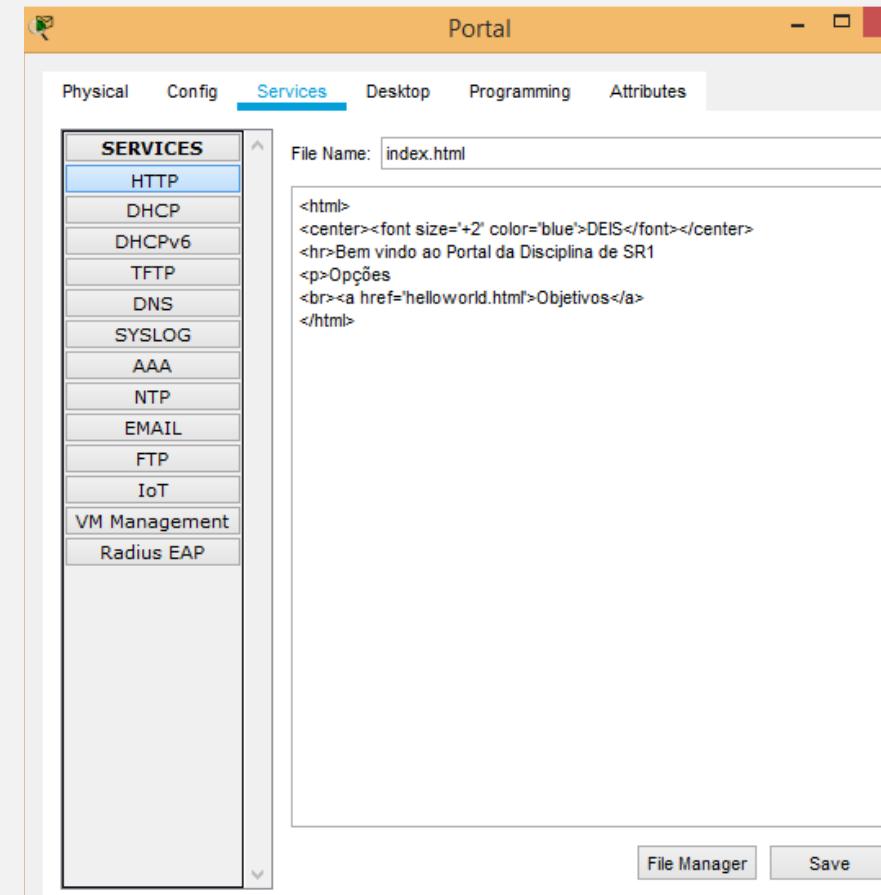
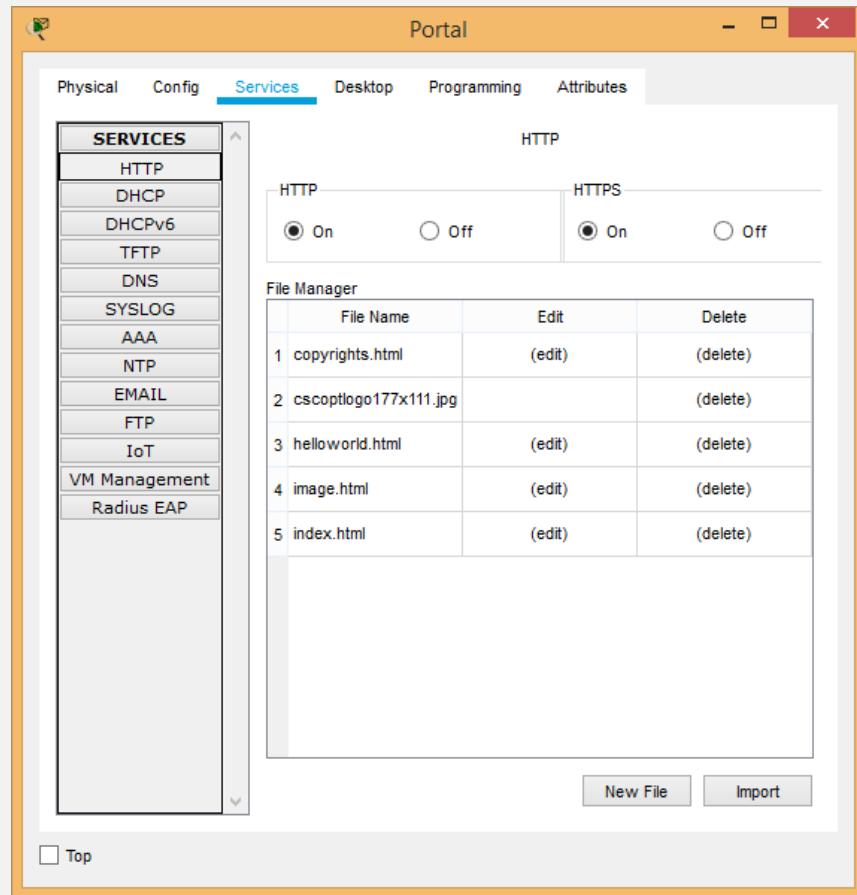


Exercício 2

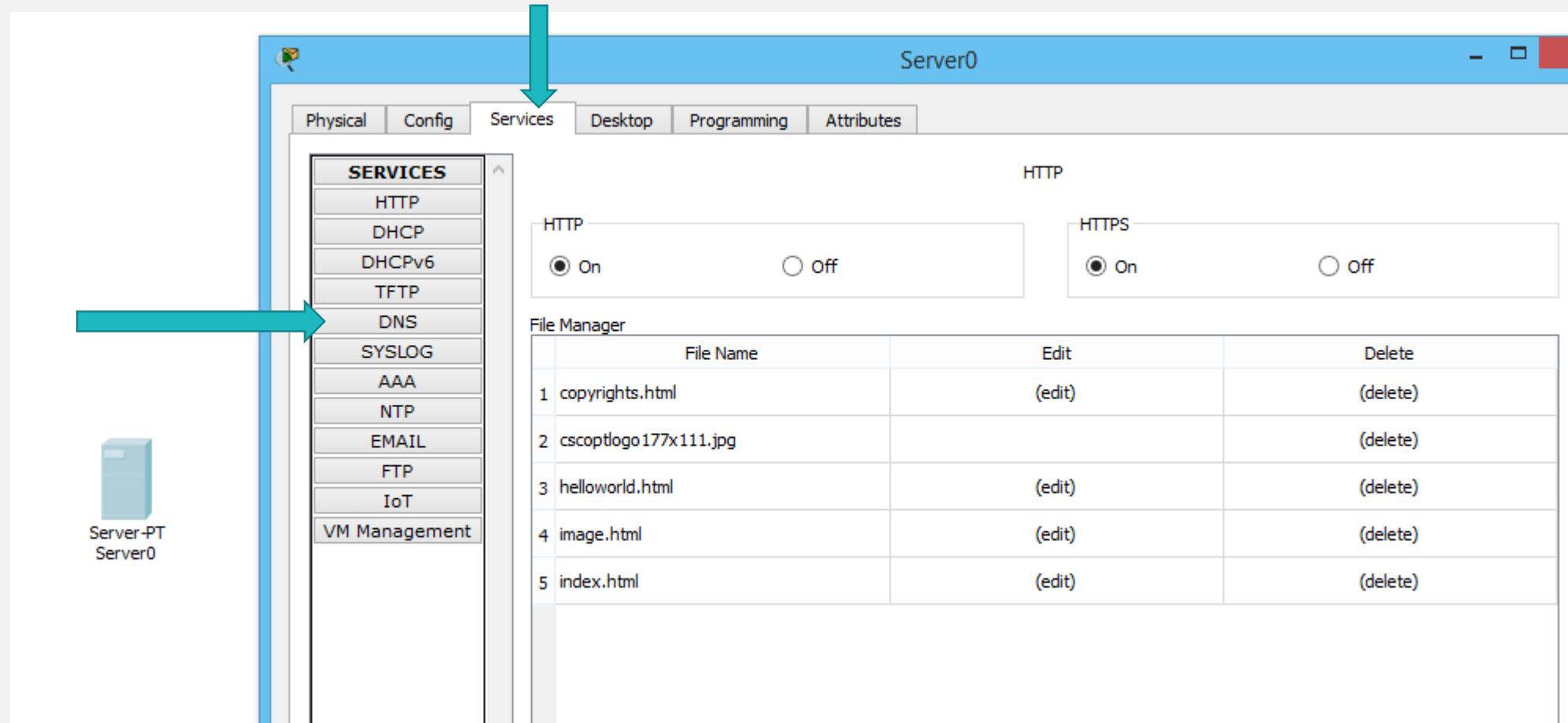
- Crie o registo SOA e preencha com os valores típicos.
- Utilize o comando **nslookup** no PC1 para ver se o seu servidor está a responder corretamente:
 - Faça uma consulta do tipo A e veja qual o IP que ele indica para o PC0
 - Faça uma consulta do tipo A e veja qual o IP que ele indica para o Portal
 - Faça uma consulta do tipo A e veja qual o IP que ele indica para o www
- Grave o ficheiro com o nome de *Primeiro nome_último nome_aula6_ex2*.
- **Nota:** O comando nslookup está **muito** limitado no Packet Tracer mas na próxima aula em ambiente Windows vamos poder explorar melhor o comando.

How To

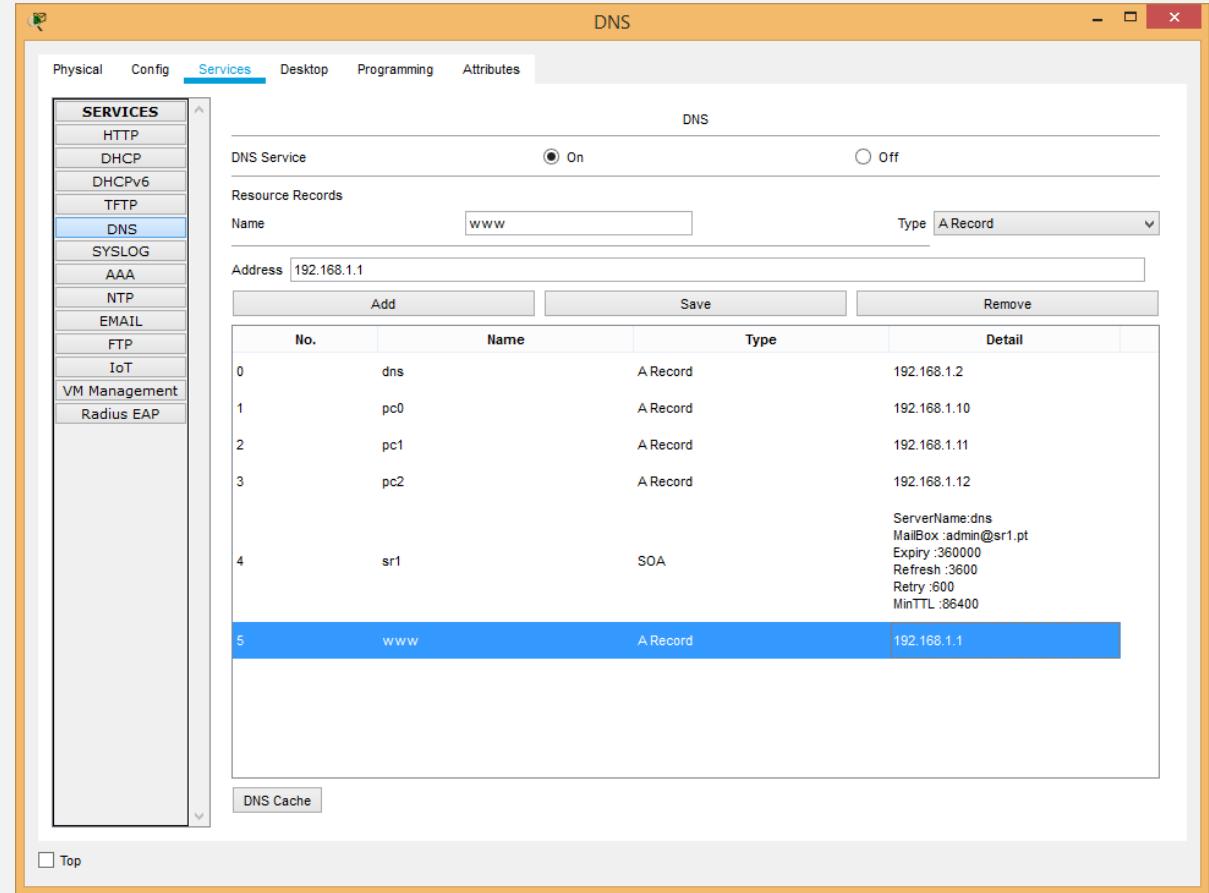
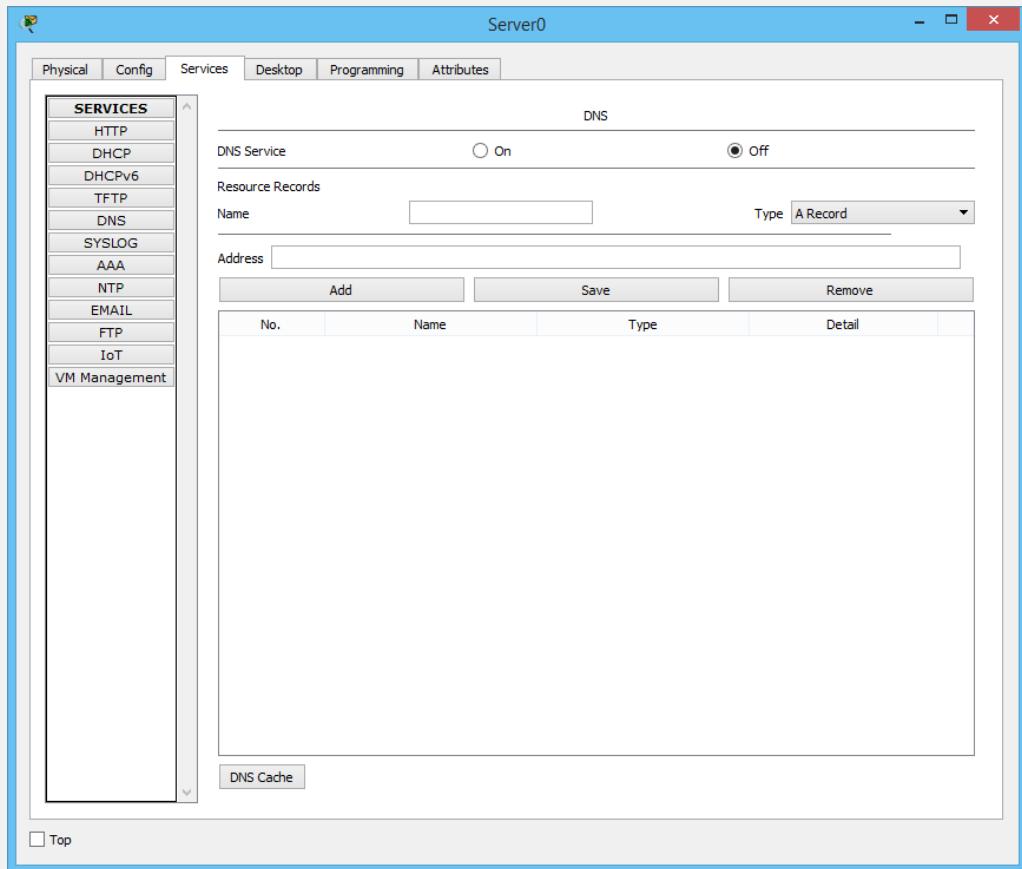
Configurar o Servidor Web



Configurar o Serviço DNS



Configurar o Serviço DNS



Registros DNS

- **SOA** - *Start of Authority* - define as características gerais da zona
 - **NAMESERVER:** indica o servidor DNS autoritário daquela zona;
 - **MNAME** - nome de domínio do nameserver (ex. isec.pt);
 - **RNAME** - endereço de email do administrador da zona (domínio);
 - **SERIAL** - versão do ficheiro de zona. Este valor deve ser incrementado sempre que alguma parte da informação do ficheiro de zona é alterada. A tácita vulgarmente usada é escrever um número com o formato de data (ano/mês/dia/versão - 0..99): 2001053000.
 - **REFRESH** - periodicidade (em segundos) com que os servidores secundários consultam o primário para averiguar a versão atual da zona. Valor típico: 3600 = 1h
 - **RETRY** - Periodicidade (em segundos) com que os servidores secundários repetem a tentativa de averiguar o número de série do master file após falharem um contacto. Valor típico: 600 = 10m
 - **EXPIRE** - Limite máximo (em segundos) de retenção de réplica da zona sem conseguir averiguar o número de série. Após este valor expirar os secundários deixam de poder responder pela zona. Valor típico: 3600000 -> 42d;
 - **MINIMUM TTL** - define quanto tempo o registro dessa zona deverá permanecer no cache de um servidor DNS antes que seja feito uma atualização. Valor típico: 864000 -> 10d

Registros DNS

- **A** - trata-se do tipo básico que estabelece a correspondência entre um nome canónico e um endereço IP (IP V4)
- **AAAA** - igual ao anterior mas para IP V6.
- **CNAME** - mapeia um alias para um nome de domínio verdadeiro ou canônico. Ou seja, indica que um nome é um nome alternativo para um outro nome. É particularmente útil para fornecer nomes alternativos que correspondem aos diferentes serviços de uma mesma máquina
- **MX** - *Mail Exchanger* - Informa os IPs dos servidores SMTP de um domínio. Esse tipo de registro tem como particularidade um campo a mais, que informa a prioridade do servidor SMTP. Quanto mais baixo o valor, maior a prioridade. Cada registo MX deve corresponder a um registo A.
- **SRV** - *Service Location* - permitem definir quais os servidores que suportam um determinado serviço para um domínio.
- **NS** - *nome do domínio* - é o que faz com que a hierarquia de nomes funcione. Indica o nome (canónico) de uma máquina que aloja um servidor DNS para o domínio referido.
- **TXT** - servem para associar informação ao domínio. Estas informações são com que pequenos ficheiros de texto, que podem conter qualquer informação pública que se pretenda associar ao domínio.
- **PTR** - *Pointer* (IP => nome) - Associa um endereço IP a um hostname para a resolução de DNS reverso.

nslookup

- É uma ferramenta, que existe no Windows e no Linux, e que é utilizada para obter informações sobre registros de DNS de um determinado domínio, máquina ou IP.
- Numa consulta padrão, o servidor DNS definido na placa de rede da máquina é o consultado, e responde com as informações sobre o domínio ou máquina pesquisado.
- A informação "*Non-authoritative answer*" significa que o servidor DNS utilizado não responde por este domínio, em outras palavras, isto significa que foi feita uma consulta externa aos servidores DNS. Imagine que está em sua casa que faz uma consulta sobre uma máquina do ISEC, se for o seu servidor a responder a essa questão a resposta será *Non-authoritative answer* se for o servidor do ISEC será *Authoritative answer*.

nslookup - Consultas

- O tipo de consulta pretendida é definido pelo comando set q=
 - **A**
 - Uma simples consulta solicitando o endereço IP correspondente a um computador.
 - **CNAME**
 - Um dado computador pode possuir diversos nomes DNS. Um destes é o nome canónico (canonical name) ou de referência.
 - **MX**
 - Uma consulta para saber quem é o servidor de correio eletrónico de um determinado domínio.
 - **SOA**
 - Uma consulta ao Start of Authority de um determinado domínio .
 - **PTR**
 - Uma consulta PTR, que demonstra a resolução inversa (inverse ou reverse). Repare na forma algo esquisita da consulta, o que acontece parcialmente devido ao facto dos endereços IP possuírem a parte mais significativa no lado esquerdo enquanto os endereços DNS possuem-na no lado direito do endereço.

nslookup - Exemplos

```
C:\Users\Pedro Geirinhas>nslookup
Default Server: vodafonegw
Address: 192.168.1.1

> sapo.pt
Server: vodafonegw
Address: 192.168.1.1

Non-authoritative answer:
Name: sapo.pt
Addresses: 2001:8a0:2102:c:213:13:146:142
          213.13.146.142

> www.isec.pt
Server: vodafonegw
Address: 192.168.1.1

Non-authoritative answer:
Name: www.isec.pt
Address: 193.137.78.72

> set q=Mx
> isec.pt
Server: vodafonegw
Address: 192.168.1.1

Non-authoritative answer:
isec.pt MX preference = 20, mail exchanger = prxmx1.isec.pt
isec.pt MX preference = 30, mail exchanger = prxmx1.isec.pt
isec.pt MX preference = 10, mail exchanger = prxmx1.isec.pt
isec.pt MX preference = 40, mail exchanger = prxmx2.isec.pt

isec.pt nameserver = ns2.isec.pt
isec.pt nameserver = ns.isec.pt
prxmx1.isec.pt internet address = 193.137.78.24
prxmx2.isec.pt internet address = 193.137.78.26
ns2.isec.pt internet address = 193.137.78.3
ns.isec.pt internet address = 193.137.78.1

> set q=Mx
> sapo.pt
Server: vodafonegw
Address: 192.168.1.1

Non-authoritative answer:
sapo.pt MX preference = 5, mail exchanger = mx.ptmail.sapo.pt

sapo.pt nameserver = ns.sapo.pt
sapo.pt nameserver = dns01.sapo.pt
sapo.pt nameserver = ns2.sapo.pt
sapo.pt nameserver = dns02.sapo.pt
mx.ptmail.sapo.pt internet address = 212.55.154.36
ns.sapo.pt internet address = 212.55.154.202
ns2.sapo.pt internet address = 212.55.154.194
dns01.sapo.pt internet address = 213.13.28.116
dns02.sapo.pt internet address = 213.13.30.116
dns01.sapo.pt AAAA IPv6 address = 2001:8a0:2106:4:213:13:28:116
dns02.sapo.pt AAAA IPv6 address = 2001:8a0:2206:4:213:13:30:116
>
```

```
C:\Users\Pedro Geirinhas>nslookup
Default Server: vodafonegw
Address: 192.168.1.1

> set q=SOA
> isec.pt
Server: vodafonegw
Address: 192.168.1.1

Non-authoritative answer:
isec.pt
    primary name server = ns.isec.pt
    responsible mail addr = sysadmin.isec.pt
    serial = 2020041501
    refresh = 28800 <8 hours>
    retry = 3600 <1 hour>
    expire = 604800 <7 days>
    default TTL = 86400 <1 day>

isec.pt nameserver = ns2.isec.pt
isec.pt nameserver = ns.isec.pt
ns.isec.pt internet address = 193.137.78.1
ns2.isec.pt internet address = 193.137.78.3
>
```

```
C:\Users\Pedro Geirinhas>nslookup
Default Server: vodafonegw
Address: 192.168.1.1

>
> set q=A
> www.isec.pt
Server: vodafonegw
Address: 192.168.1.1

Non-authoritative answer:
Name: www.isec.pt
Address: 193.137.78.72
```

```
C:\Users\Pedro Geirinhas>nslookup
Default Server: vodafonegw
Address: 192.168.1.1

> server ns2.isec.pt
Default Server: ns2.isec.pt
Address: 193.137.78.3

> www.isec.pt
Server: ns2.isec.pt
Address: 193.137.78.3

Name: www.isec.pt
Address: 193.137.78.72
```

Dúvidas



Serviços de Rede 1 – **Aula 7 - Práticas**

2022-2023

Instituto Politécnico de Coimbra

Departamento de Engenharia Informática



Nota Importante

- Na próxima aula (26 e 27 de abril) será realizado o 2º teste prático.
- A matéria é:
 - DNS no *Packet Tracer*.
 - DNS em Windows.
- Devem ter instalado o Virtual Box 6.1.
- Devem antecipadamente importar para o VirtualBox as imagens do Windows Server 2012 e do Windows 8/10 “limpas”.
- Devem ter o *Cisco Packet Tracer* versão 8.2.0 ou versão mais atual.
- Será **obrigatória a inscrição no Moodle**.

Aula 7 - Pre - Requisitos

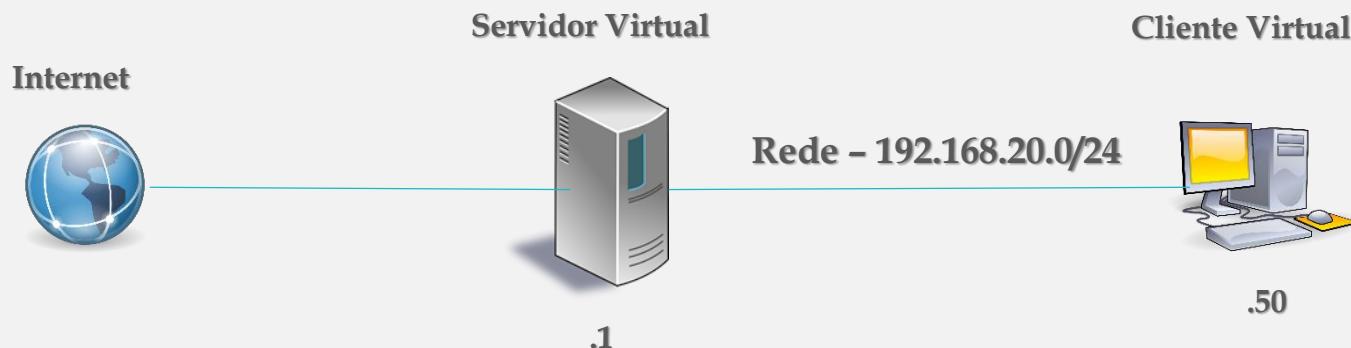
- Ter instalado o VirtualBox.
- Uma imagem de um servidor Windows Server 2012 “limpa”.
- Uma imagem de um cliente Windows 10 “limpa”.



Exercício 1 – Configurar o servidor Windows como um “router”

Exercício 1

Considere a seguinte topologia



Exercício 1

- Implemente a topologia anterior no Virtual Box, tendo como base as seguintes definições:
 - **Windows Server 2012**
 - Dois interfaces de rede:
 - **Interface 1** - do tipo NAT para ligação à rede pública. Deve obter um endereço de forma dinâmica (DHCP).
 - **Interface 2** - do tipo *Internal Network* para ligação à rede privada. Deve configurar um endereço fixo da sua rede (192.168.20.1).
 - **Windows 8/10**
 - Interface de rede do tipo *Internal Network* para ligação à rede privada. Deve configurar a placa de rede com um endereço fixo da sua rede (192.168.20.50).

Exercício 1

- Veja os endereços IP das placas de rede do seu Servidor. As suas placas de rede devem ter um IP idênticos aos da figura.



```
Administrator: C:\Windows\system32\cmd.exe
C:\Users\Administrator>ipconfig
Windows IP Configuration

Ethernet adapter Ethernet 2:
  Connection-specific DNS Suffix  . : lan
  Link-local IPv6 Address . . . . . : fe80::a18d:db6c:9eb2:c26f%23
  IPv4 Address. . . . . : 10.0.3.15
  Subnet Mask . . . . . : 255.255.255.0
  Default Gateway . . . . . : 10.0.3.2

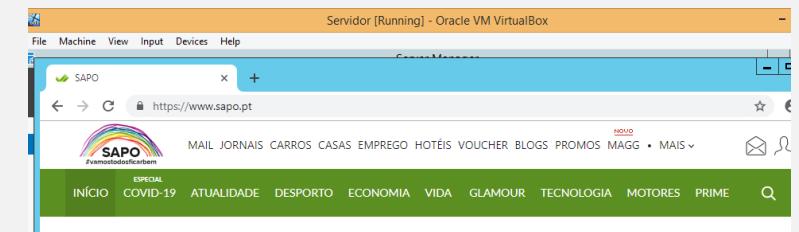
Ethernet adapter Ethernet:
  Connection-specific DNS Suffix  . :
  Link-local IPv6 Address . . . . . : fe80::9920:a4f4:62ff%12
  IPv4 Address. . . . . : 192.168.20.1
  Subnet Mask . . . . . : 255.255.255.0
  Default Gateway . . . . . : 192.168.20.254

Tunnel adapter isatap.(D7DEEAB0-B8AA-4638-9861-3E8C7C681B46):
  Media State . . . . . : Media disconnected
  Connection-specific DNS Suffix  . : lan

Tunnel adapter isatap.lan:
  Media State . . . . . : Media disconnected
  Connection-specific DNS Suffix  . : lan

C:\Users\Administrator>
```

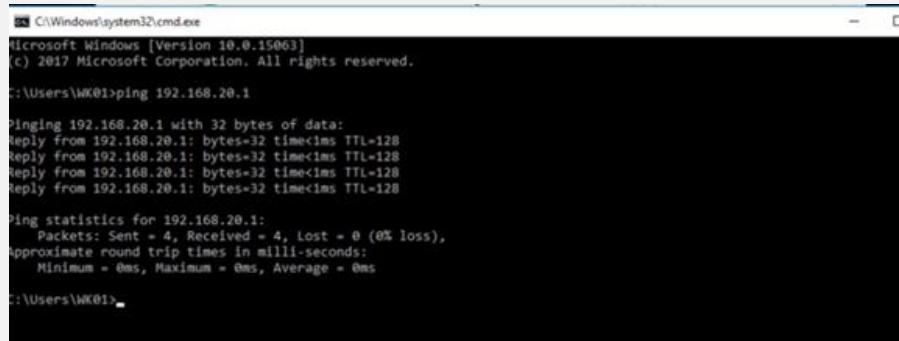
Este IP pode ser diferente
depende da sua máquina física
e da rede onde está ligado.



- Comprove que o seu servidor consegue aceder à Internet.

Exercício 1

- Instale no servidor o serviço *Remote Access* de forma que esta máquina seja o router da sua rede e permita ao PC aceder à Internet.
- Garanta que o seu cliente pinga o servidor.
- Configure o seu cliente para que ele tenha acesso à Internet utilizando como router o servidor Windows mantendo o modo de rede em *Internal Network*. Não se esqueça de configurar de forma correta todos os parâmetros das placas de rede do servidor e PC (*default gateway* e servidores de DNS).



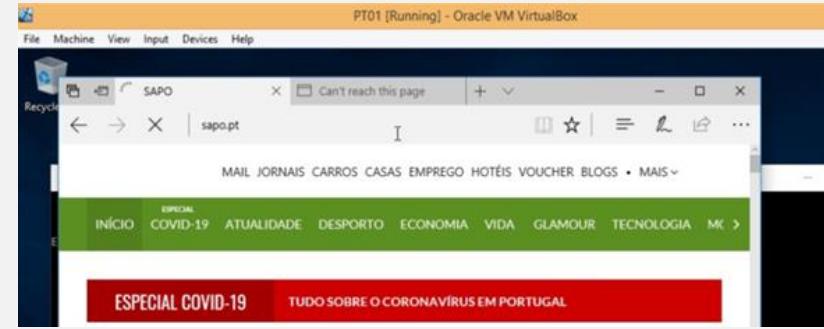
```
C:\Windows\system32\cmd.exe
Microsoft Windows [Version 10.0.15063]
(c) 2017 Microsoft Corporation. All rights reserved.

C:\Users\WK01>ping 192.168.20.1

Pinging 192.168.20.1 with 32 bytes of data:
Reply from 192.168.20.1: bytes=32 time<1ms TTL=128

Ping statistics for 192.168.20.1:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 0ms, Maximum = 0ms, Average = 0ms

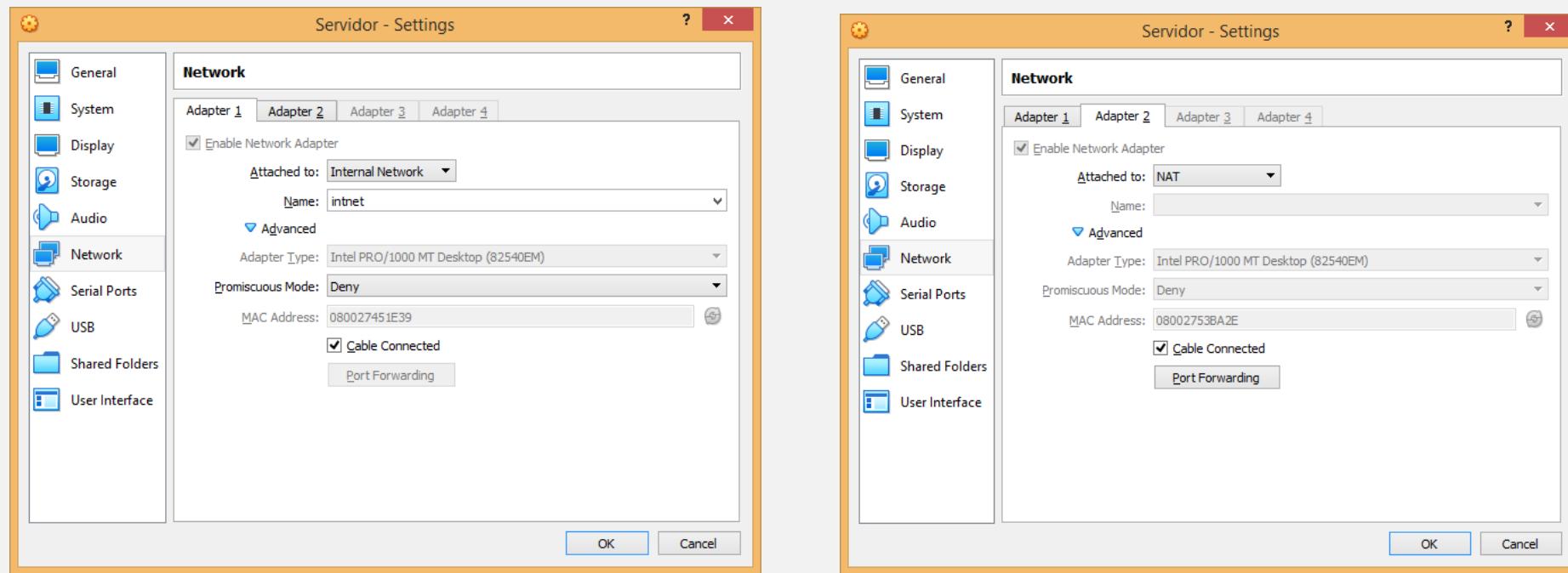
C:\Users\WK01>
```



How To

Máquina Virtual - Rede

- Uma máquina virtual pode ter mais do que uma placa de rede. Podem ainda estar a “correr” diferentes modos (veja a aula prática 4).



Instalar o Remote Access

Select server roles

Before You Begin

Installation Type

Server Selection

Server Roles

Features

Remote Access

Role Services

Confirmation

Results

Select one or more roles to install on

Roles

- Application Server
- DHCP Server (Installed)
- DNS Server
- Fax Server
- File and Storage Services (2)
- Hyper-V
- Network Policy and Access
- Print and Document Services
- Remote Access**
- Remote Desktop Services
- Volume Activation Services
- Web Server (IIS)

Select role services

Before You Begin

Installation Type

Server Selection

Server Roles

Features

Remote Access

Role Services

Web Server Role (IIS)

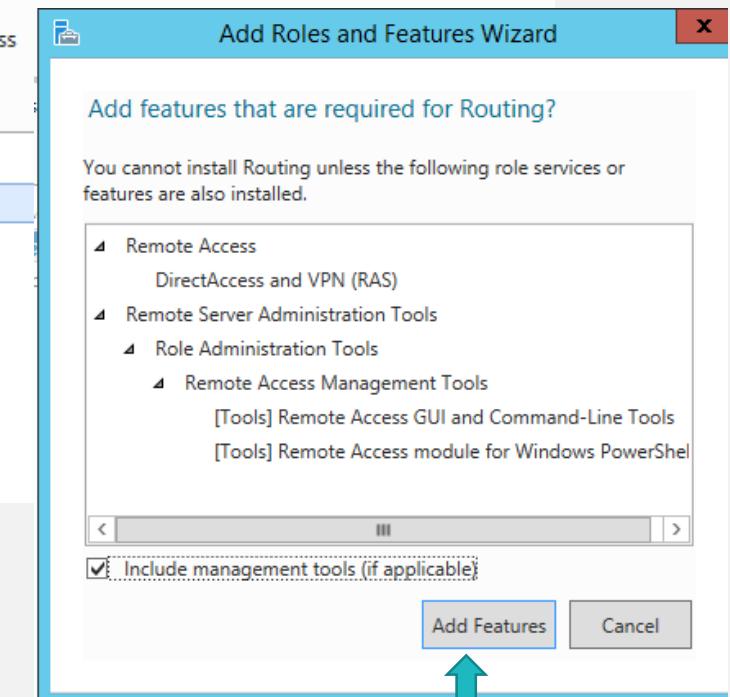
Role Services

Confirmation

Select the role services to install for Remote Access

Role services

- DirectAccess and VPN (RAS)
- Routing**
- Web Application Proxy



Instalar o Remote Access

The image displays three windows of the 'Add Roles and Features Wizard' for Windows Server 2012 R2. The first window shows the 'Web Server Role (IIS)' step, detailing the role's purpose and noting that it includes IIS 8.5, ASP.NET, and the Communication Foundation. It lists 'Things to note' about WSRM and the default IIS 8.5 installation. The second window shows the 'Select role services' step, where 'Web Server' is selected under 'Role services'. Under 'Web Server', 'Common HTTP Features' and 'Health and Diagnostics' are checked. The third window shows the 'Confirm installation selections' step, listing optional features like Group Policy Management, RAS Connection Manager Administration Kit (CMAK), and Remote Access (DirectAccess and VPN). The destination server is SRVSR1.

Add Roles and Features Wizard

Web Server Role (IIS)

Before You Begin
Installation Type
Server Selection
Server Roles
Features
Remote Access
Role Services
Web Server Role (IIS)
Role Services
Confirmation
Results

Web servers are computers that let you share information over the Internet, or through intranets. The Web Server role includes Internet Information Services (IIS) 8.5 with enhanced diagnostic and administration, a unified Web platform that integrates IIS 8.5, ASP.NET, and the Communication Foundation.

Things to note:

- Using Windows System Resource Manager (WSRM) can help ensure equitable servicing of server traffic, especially when there are multiple roles on this computer.
- The default installation for the Web Server (IIS) role includes the installation of role services that enable you to serve static content, make minor customizations (such as default document errors), monitor and log server activity, and configure static content compression.

More information about Web Server IIS

< Previous Next > Install

Select role services

Before You Begin
Installation Type
Server Selection
Server Roles
Features
Remote Access
Role Services
Web Server Role (IIS)
Role Services
Confirmation
Results

Select the role services to install for Web Server (IIS)

Role services

Web Server

- Common HTTP Features
 - Default Document
 - Directory Browsing
 - HTTP Errors
 - Static Content
 - HTTP Redirection
 - WebDAV Publishing
- Health and Diagnostics
 - HTTP Logging
 - Custom Logging
 - Logging Tools
 - ODBC Logging
 - Request Monitor

< Previous Next >

CONFIRMATION

Before You Begin
Installation Type
Server Selection
Server Roles
Features
Remote Access
Role Services
Web Server Role (IIS)
Role Services
Confirmation
Results

To install the following roles, role services, or features on selected server, click **Install**.

Restart the destination server automatically if required

Optional features (such as administration tools) might be displayed on this page because they have been selected automatically. If you do not want to install these optional features, click **Previous** to clear their check boxes.

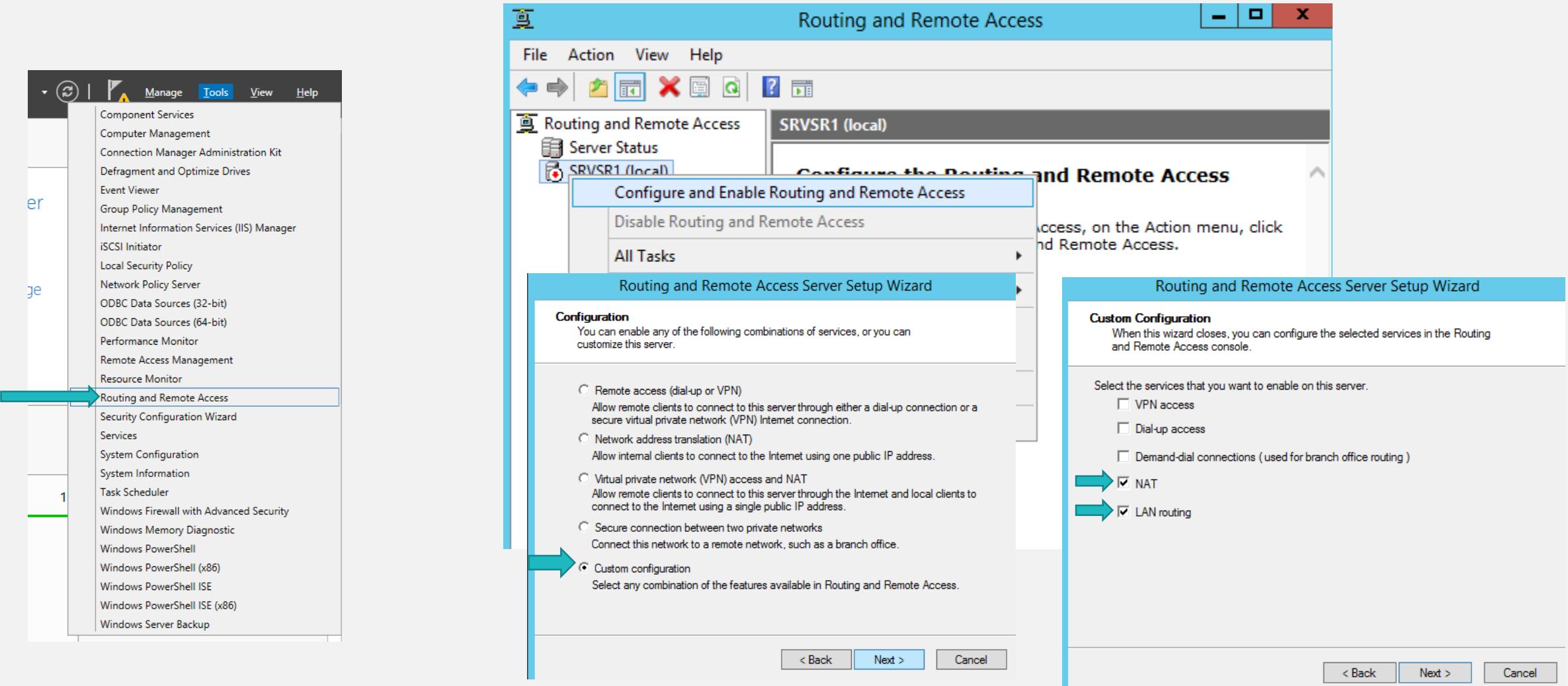
Group Policy Management
RAS Connection Manager Administration Kit (CMAK)
Remote Access

- DirectAccess and VPN (RAS)**
- Routing**

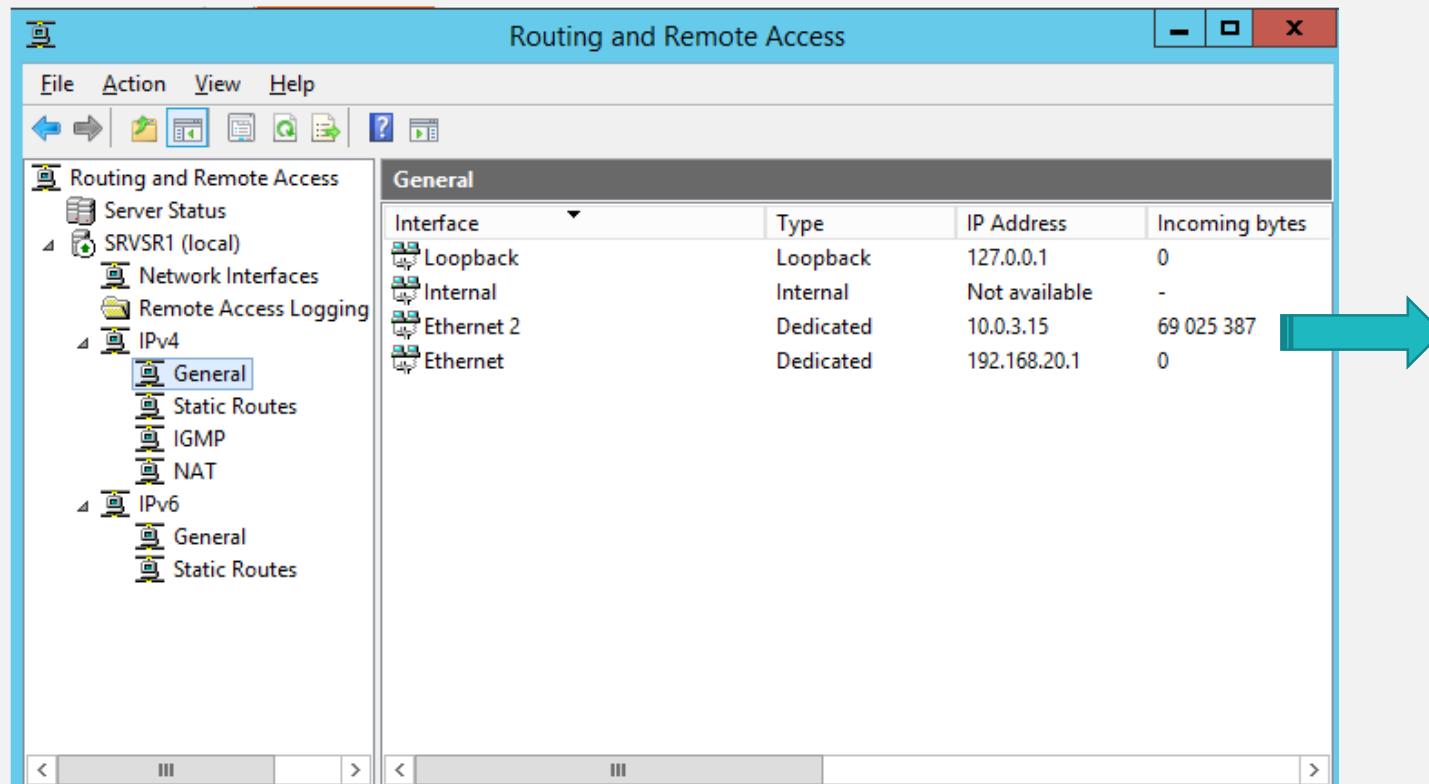
Remote Server Administration Tools

- Role Administration Tools**
 - Remote Access Management Tools**
 - Remote Access GUI and Command-Line Tools
 - Remote Access module for Windows PowerShell

Configurar o Routing and Remote Access



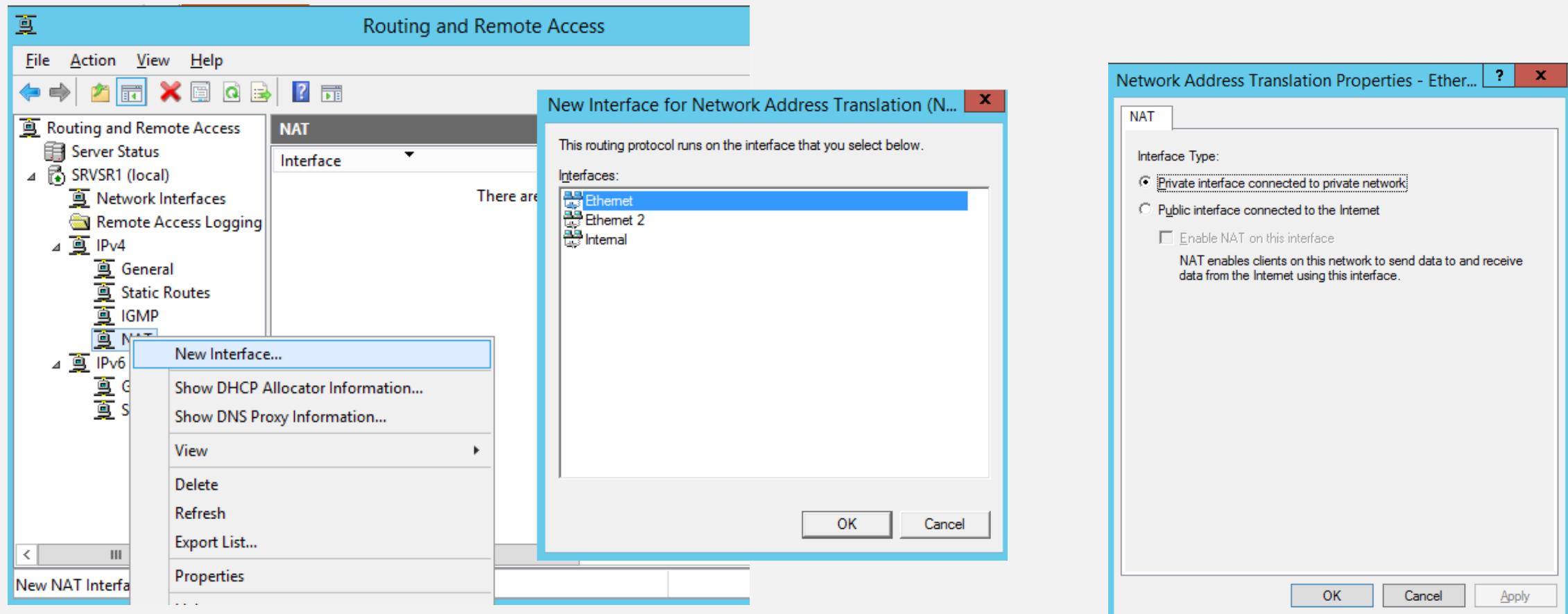
A consola do *Routing and Remote Access*



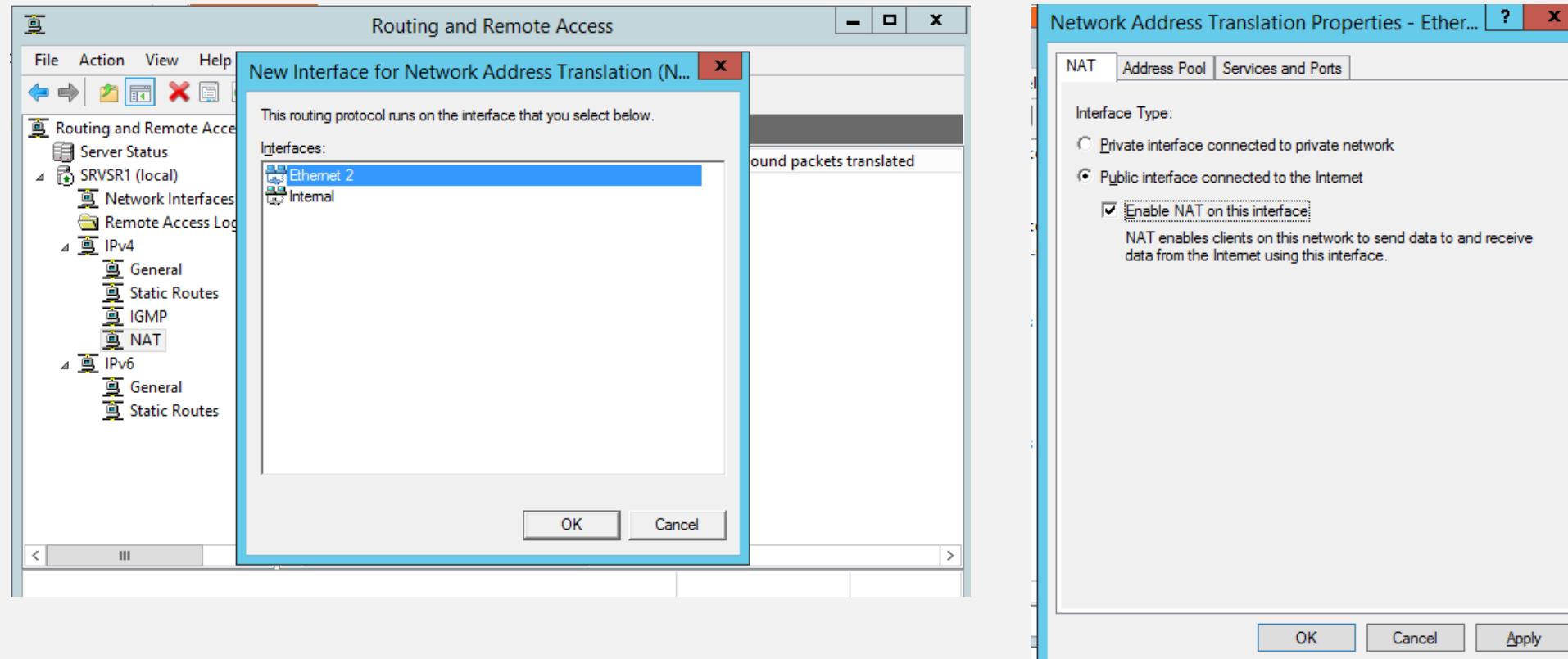
Têm de ter em atenção o nome das placas e a sua função. Neste exemplo temos:

- Ethernet é a placa que está em Internal network
 - Ethernet 2 é a placa que está em NAT.
- Como sabe esta informação? Analisando os IPs!!

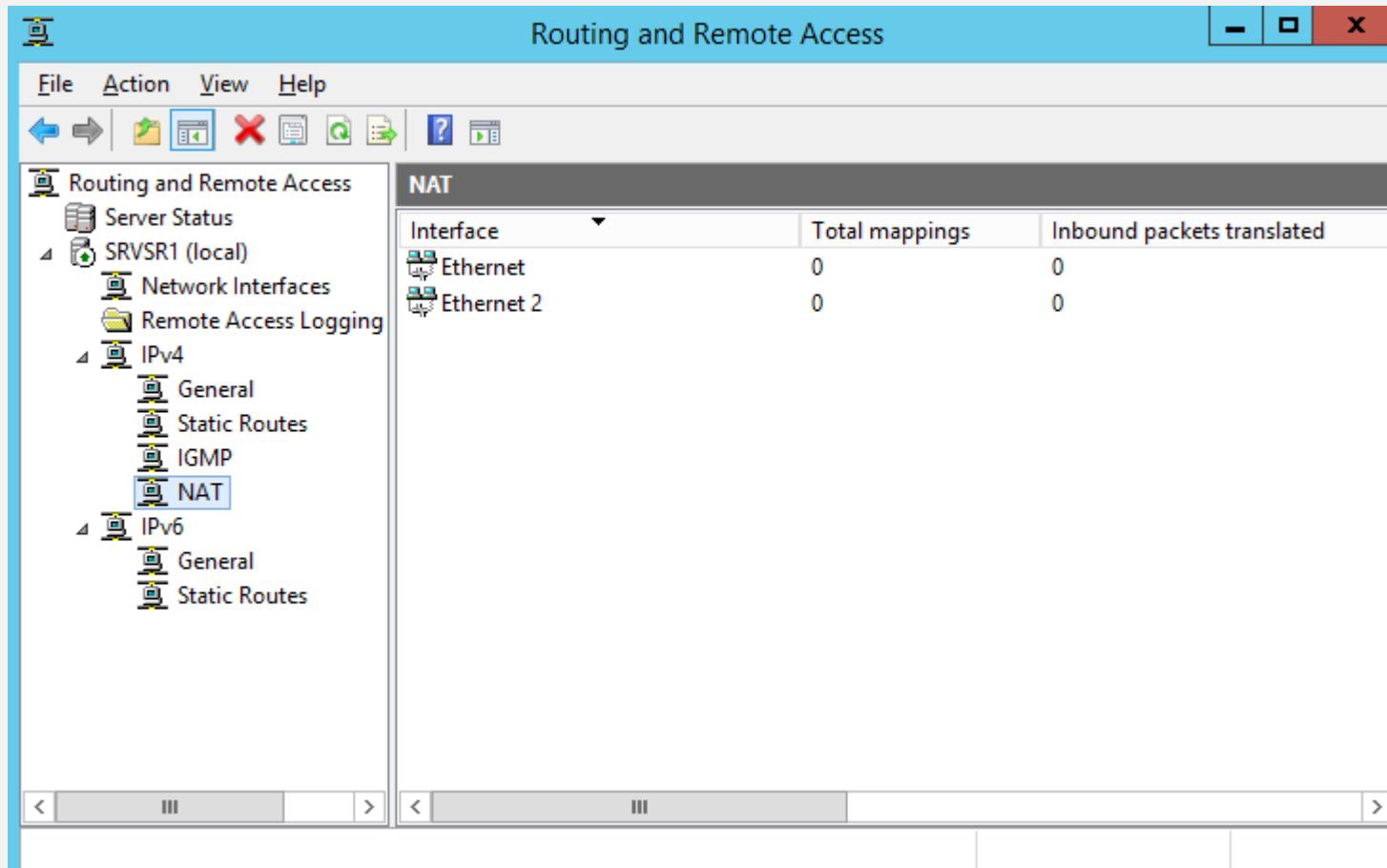
Configurar o NAT - Interface interna



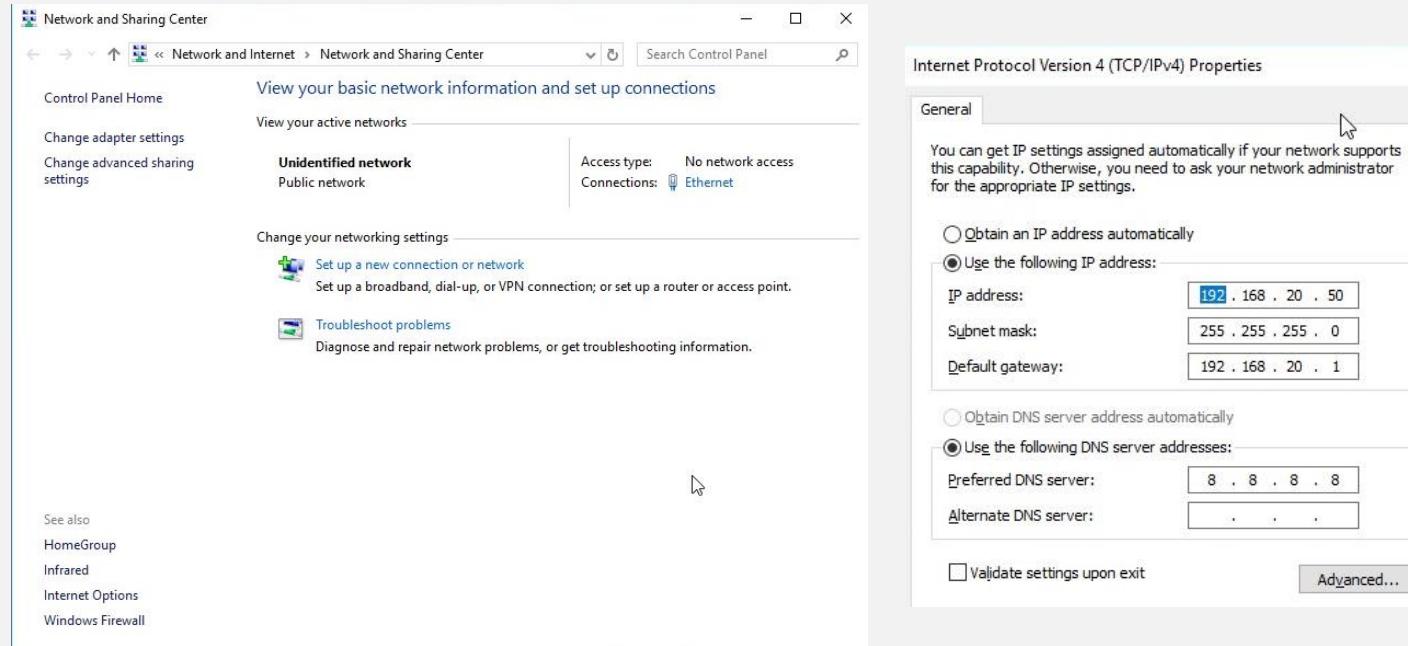
Configurar o NAT - Interface externa



Configuração Final - NAT



Configuração do cliente



Exercício 2

Exercício 2 – Configurar o DNS no Windows Server

Exercício 2

- Instale e configure o serviço DNS no seu servidor com as seguintes definições:
 - Domínio “sr1.pt”
 - Responsável pelo domínio: administrador@sr1.pt
 - Registe o servidor no DNS server com o nome de dns e com o ip 192.168.20.1.
 - Edite o registo SOA para colocar o servidor dns.sr1.pt como o seu *primary server*. Coloque ainda no SOA os valores típicos nos restantes tempos. Use como base os valores do DNS do ISEC.
 - Registe o host www com o endereço IP 192.168.20.2.
 - Neste servidor (www) estão alojados, também, os sites “webmail.sr1.pt” e “moodle.sr1.pt”. Registe os fqdn de forma adequada.
 - O servidor de mail é o mail.sr1.pt e responde no endereço 192.168.20.3.
 - Verifique no servidor a resolução do nome: www.sapo.pt.
 - Verifique no cliente a resolução de nomes das maquinas registadas no seu DNS.
 - Verifique no cliente a resolução do nome: www.cisco.com.
 - Coloque o 8.8.8.8 como o *Forwarder* do seu serviço de DNS.

Exercício 2

Servidor

```
C:\Users\Administrator>ping www.sapo.pt

Pinging www.sapo.pt [213.13.146.142] with 32 bytes of data:
Reply from 213.13.146.142: bytes=32 time=14ms TTL=247
Reply from 213.13.146.142: bytes=32 time=15ms TTL=247
Reply from 213.13.146.142: bytes=32 time=15ms TTL=247
Reply from 213.13.146.142: bytes=32 time=15ms TTL=247

Ping statistics for 213.13.146.142:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 14ms, Maximum = 15ms, Average = 14ms
```

Cliente

```
Administrator: C:\Windows\system32\cmd.exe - ping www.sr1.pt

Microsoft Windows [Version 6.3.9600]
(c) 2013 Microsoft Corporation. All rights reserved.

C:\Users\Administrator>ping www.sr1.pt

Pinging www.sr1.pt [192.168.20.2] with 32 bytes of data:
Reply from 192.168.20.1: Destination host unreachable.
Request timed out.
```

```
C:\Users\Administrator>ping webmail.sr1.pt

Pinging www.sr1.pt [192.168.20.2] with 32 bytes of data:
Request timed out.
```

```
C:\Users\Administrator>ping mail.sr1.pt

Pinging mail.sr1.pt [192.168.20.3] with 32 bytes of data:
Reply from 192.168.20.1: Destination host unreachable.
```

```
C:\Users\sr2>ping www.cisco.com

Pinging e2867.dsca.akamaiedge.net [104.89.180.30] with 32 bytes of data:
Reply from 104.89.180.30: bytes=32 time=6ms TTL=56
Reply from 104.89.180.30: bytes=32 time=6ms TTL=56
Reply from 104.89.180.30: bytes=32 time=7ms TTL=56
Reply from 104.89.180.30: bytes=32 time=13ms TTL=56

Ping statistics for 104.89.180.30:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 6ms, Maximum = 13ms, Average = 8ms
```

How To

DNS - Instalação

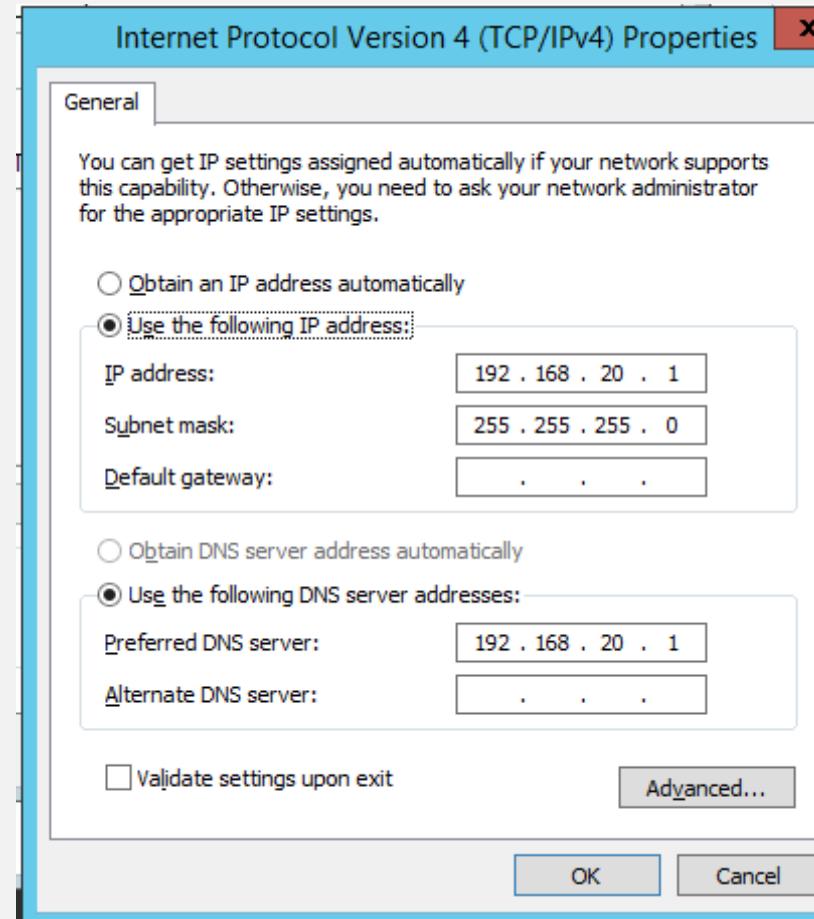
- Existem algumas propriedades genéricas que podem ser configuradas
 - *Interfaces*
 - Endereços dos interfaces de rede nos quais são aceites pedidos.
 - *Forwarders*
 - São servidores aos quais são reenviados pedidos de resolução que não conseguem ser resolvidos localmente.
 - Podem ser definidos *forwarders* genéricos ou específicos por domínio.
 - *Root hints*
 - Lista de servidores de topo.
 - Podem ser actualizados a partir de outro servidor.
 - *Advanced features*
 - Várias opções, por exemplo: *round robin*, recursividade,...

DNS - Instalação

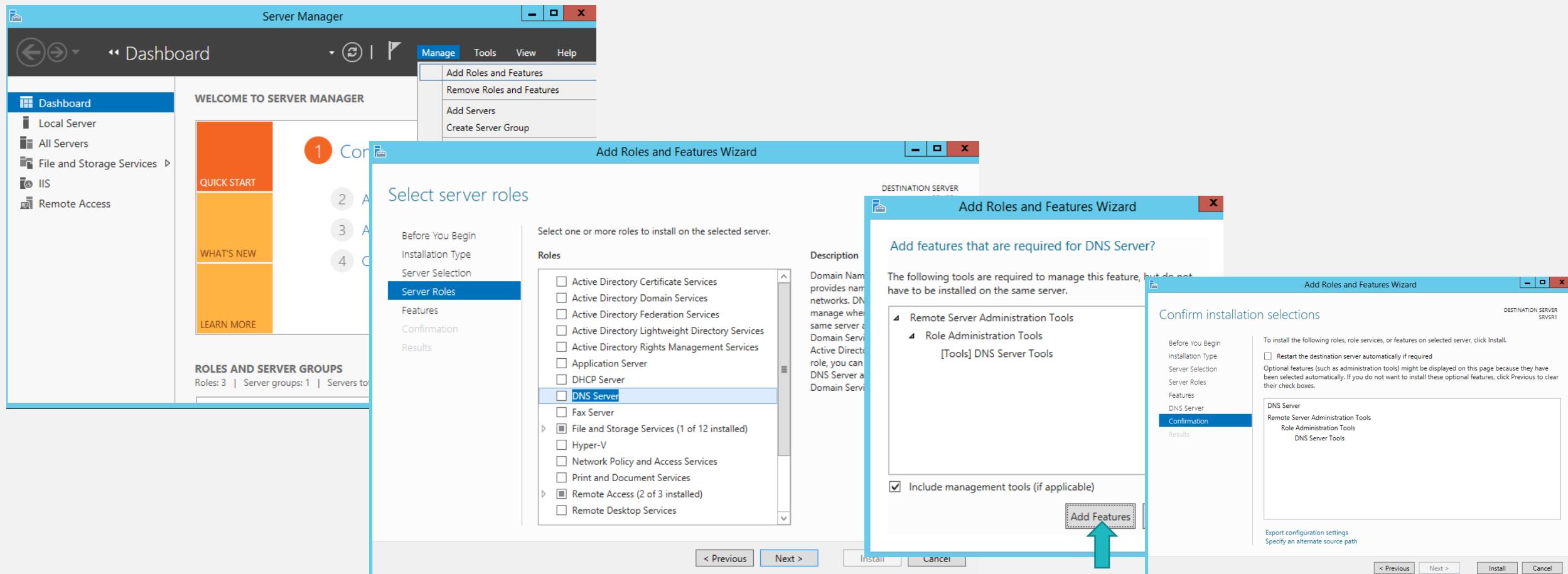
- Antes de iniciarmos a instalação do DNS é necessário configurar um IP estático para o servidor, assegurar que todas as atualizações do servidor estão em dia e uma boa prática é ativar/monitorizar o *Event Viewer*.
- **Nota 1:** A configuração do IP estático é necessária para que não tenha problemas futuros com conectividade, performance da rede e resolução de nomes.
- **Nota 2:** No *event viewer* são gravados logs de aviso e erros que podem ajudar a resolver diversos problemas antes e depois da instalação do DNS. O *event viewer* é sempre um excelente elemento de diagnóstico...
- **Nota 3:** Na nossa simulação o IP da ligação à rede exterior terá de continuar a ser dinâmico. Só o interno deve estar com um IP estático.

DNS - Instalação

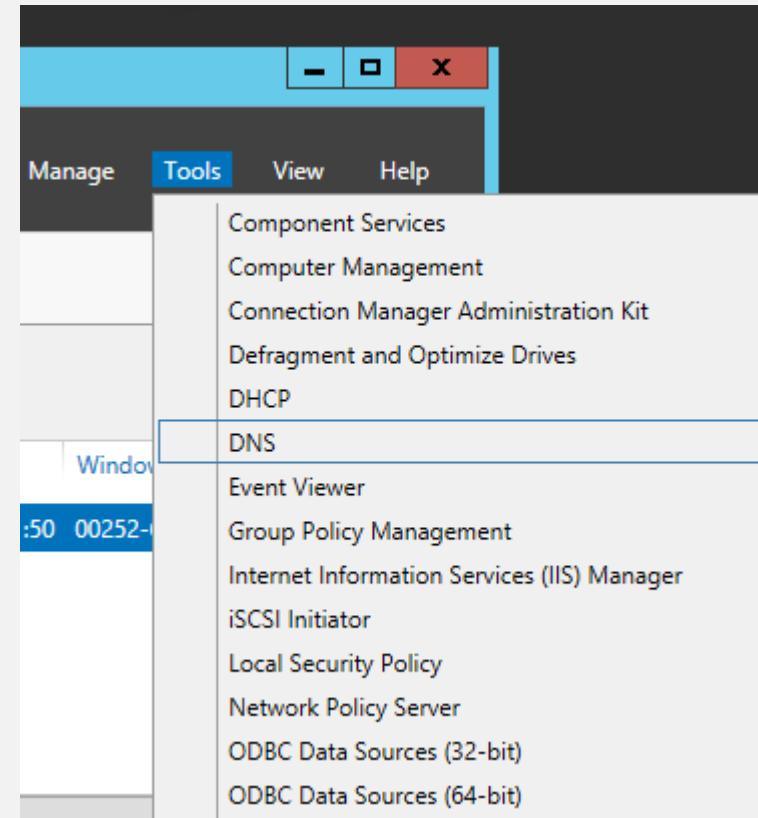
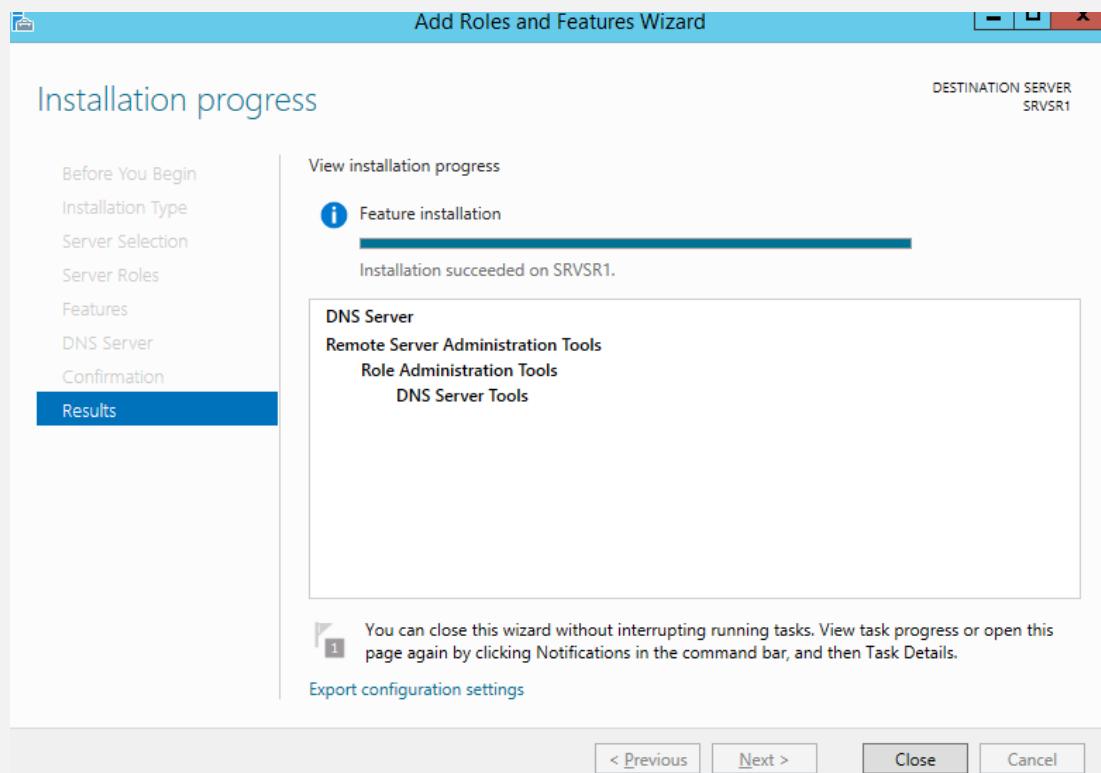
- Nas propriedades da placa do servidor, em **Preferred DNS server** deve ser configurado o mesmo endereço IP do servidor onde está a instalar o DNS. Em **Alternate DNS server** devemos configurar o DNS secundário, se existir.



DNS - Instalação do serviço

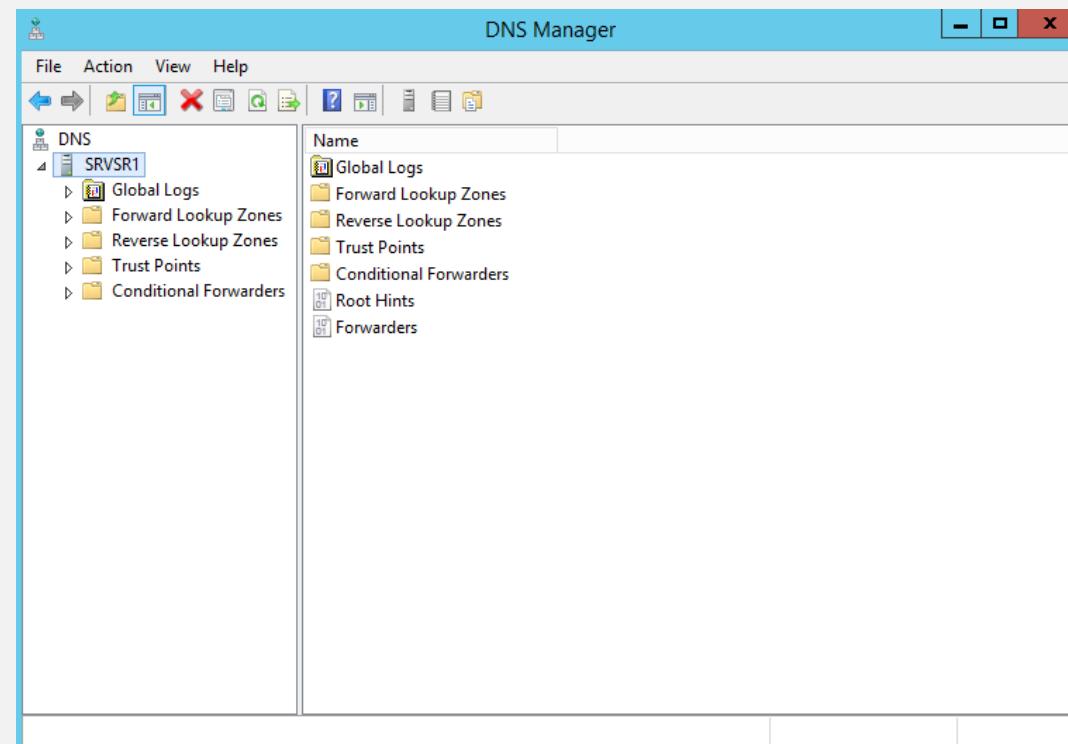


DNS - Instalação do serviço

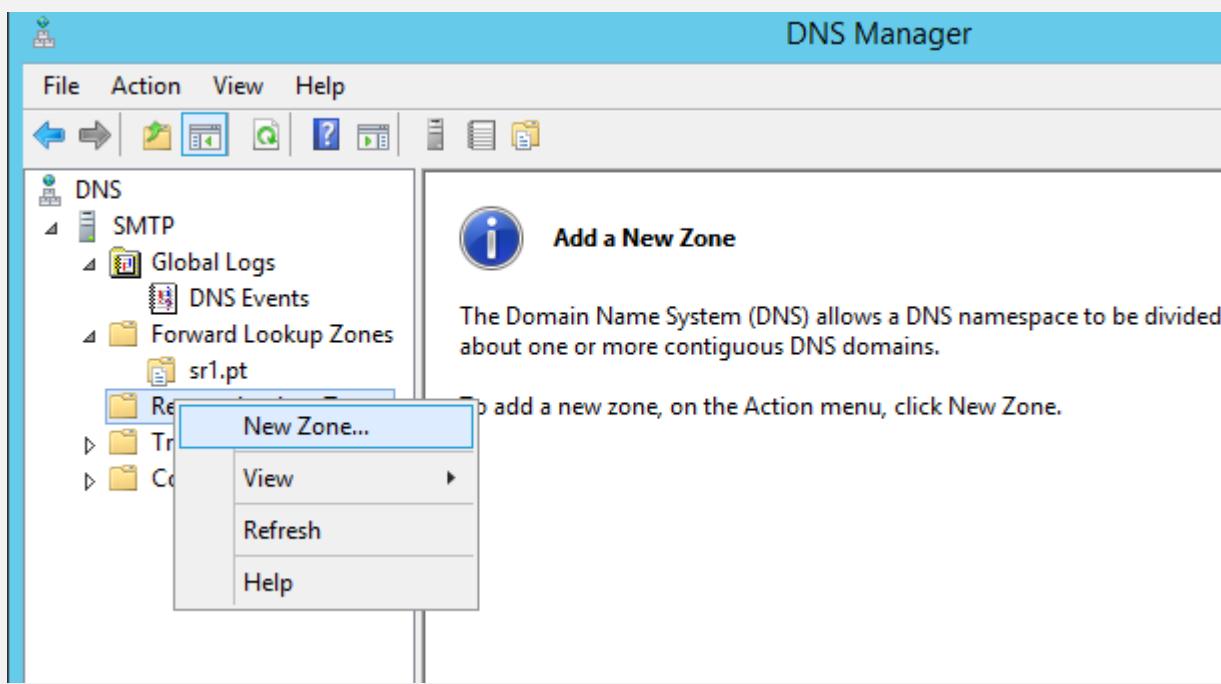


DNS - Configuração do serviço

- Para configurar o serviço é necessário definir:
 - Forward Lookup Zones;
 - Reverse Lookup Zones;
 - Conditional Forwarders.

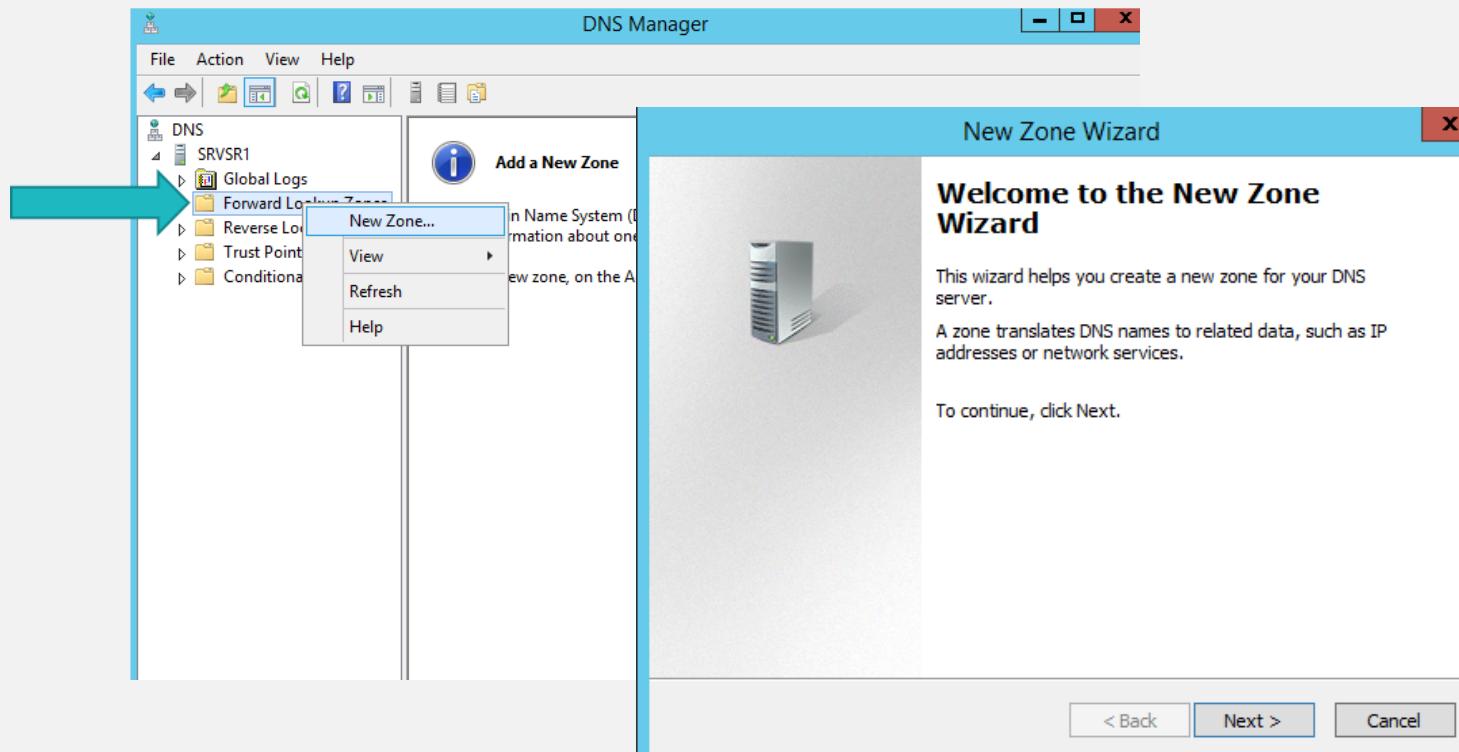


Criar uma nova Zona Primária



- **Zona Primaria** - o nome já diz tudo. Deve ser a primeira zona a ser criada e sem ela o domínio não existe.
- **Zona Secundaria** - Só pode existir se já existir uma primaria. Esta será uma cópia somente de leitura da zona primaria.
- **Zona tipo Stub** - Um tipo de zona que armazena apenas registros NS (Name Server), SOA (start of authority) e alguns registros do tipo A. Esta zona não é autoritária.
- **Zona Integrada ao Active Directory** - Quando existe um controlador de domínio, podemos integrar a zona, assim os dados serão armazenados no próprio Active Directory e replicados pelo domínio se configurado.

Criar uma nova Zona Primária



Criar uma nova Zona Primária

New Zone Wizard

Zone Type
The DNS server supports various types of zones:
Select the type of zone you want to create:

Primary zone
Creates a copy of a zone that can be used by multiple servers.

Secondary zone
Creates a copy of a zone that exists on another server to reduce the processing load of primary servers.

Stub zone
Creates a copy of a zone containing only the Start of Authority (SOA), and possibly glue Host (A) records, to make that zone authoritative for that zone.

Store the zone in Active Directory (available on domain controllers)

Zone Name
What is the name of the new zone?
The zone name specifies the portion of the DNS namespace for which your server will be authoritative. It might be your organization's domain name (for example, contoso.com) or a portion of the domain name (for example, newzone.microsoft.com). This is not the name of the DNS server.

Zone name:

Zone File
You can create a new zone file or use a file copied from another DNS server.
Do you want to create a new zone file or use an existing file that you have copied from another DNS server?

Create a new file with this file name:

Use this existing file:

To use this existing file, ensure that it has been copied to the folder %SystemRoot%\system32\DNS on this server, and then click Next.

< Back Next >

New Zone Wizard X

Zone File
You can create a new zone file or use a file copied from another DNS server.


Do you want to create a new zone file or use an existing file that you have copied from another DNS server?

Create a new file with this file name:

Use this existing file:

To use this existing file, ensure that it has been copied to the folder %SystemRoot%\system32\DNS on this server, and then click Next.

< Back Next > Cancel

Criar uma nova Zona Primária - Tipo de atualização

New Zone Wizard

Dynamic Update

You can specify that this DNS zone accepts secure, nonsecure, or no dynamic updates.

Dynamic updates enable DNS client computers to register and dynamically update their resource records with a DNS server whenever changes occur.

Select the type of dynamic updates you want to allow:

- Allow only secure dynamic updates (recommended for Active Directory)
This option is available only for Active Directory-integrated zones.
- Allow both nonsecure and secure dynamic updates
Dynamic updates of resource records are accepted from any client.
⚠️ This option is a significant security vulnerability because updates can be accepted from untrusted sources.
- Do not allow dynamic updates
Dynamic updates of resource records are not accepted by this zone. You must update these records manually.

< Back Next > Cancel

New Zone Wizard

Completing the New Zone Wizard

You have successfully completed the New Zone Wizard. You specified the following settings:

Name:	sr1.pt
Type:	Standard Primary
Lookup type:	Forward
File name:	sr1.pt.dns

Note: You should now add records to the zone or ensure that records are updated dynamically. You can then verify name resolution using nslookup.

To close this wizard and create the new zone, click Finish.

< Back Finish Cancel

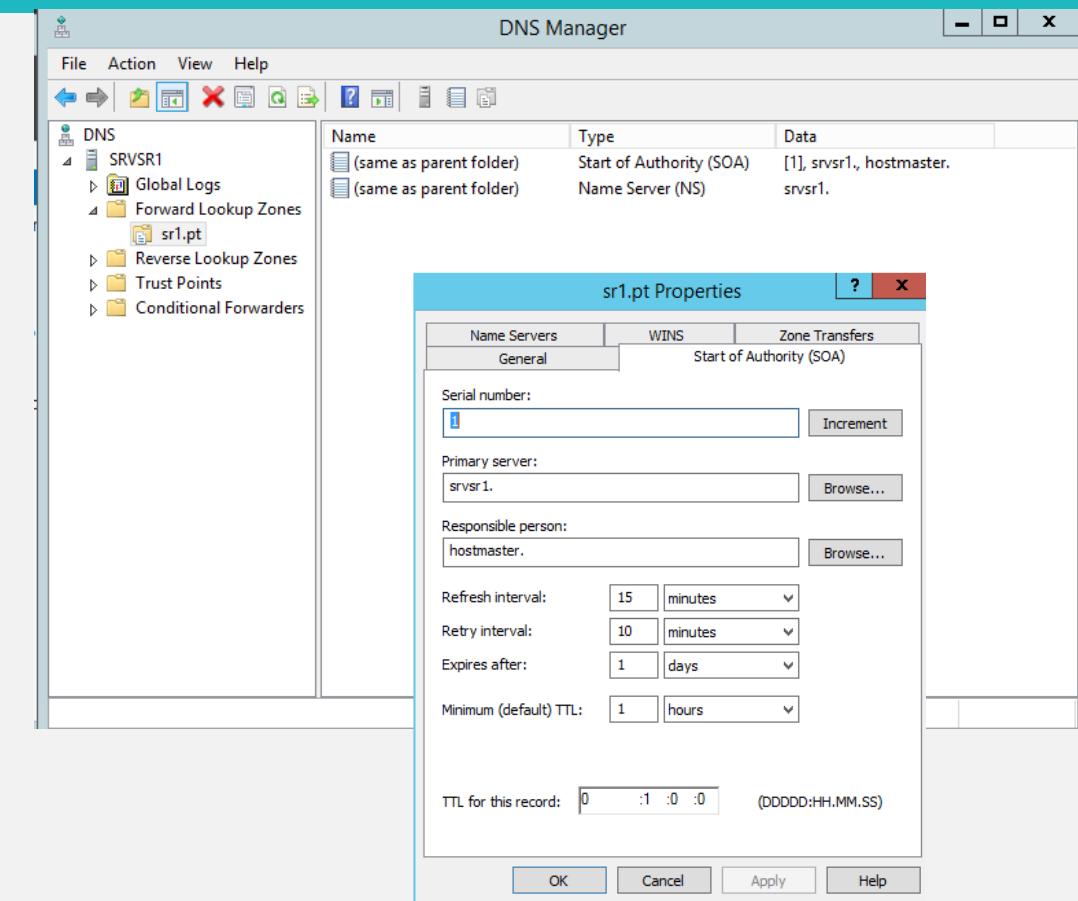
No nosso caso, já que não temos Active Directory nem o serviço DHCP.

Nota:

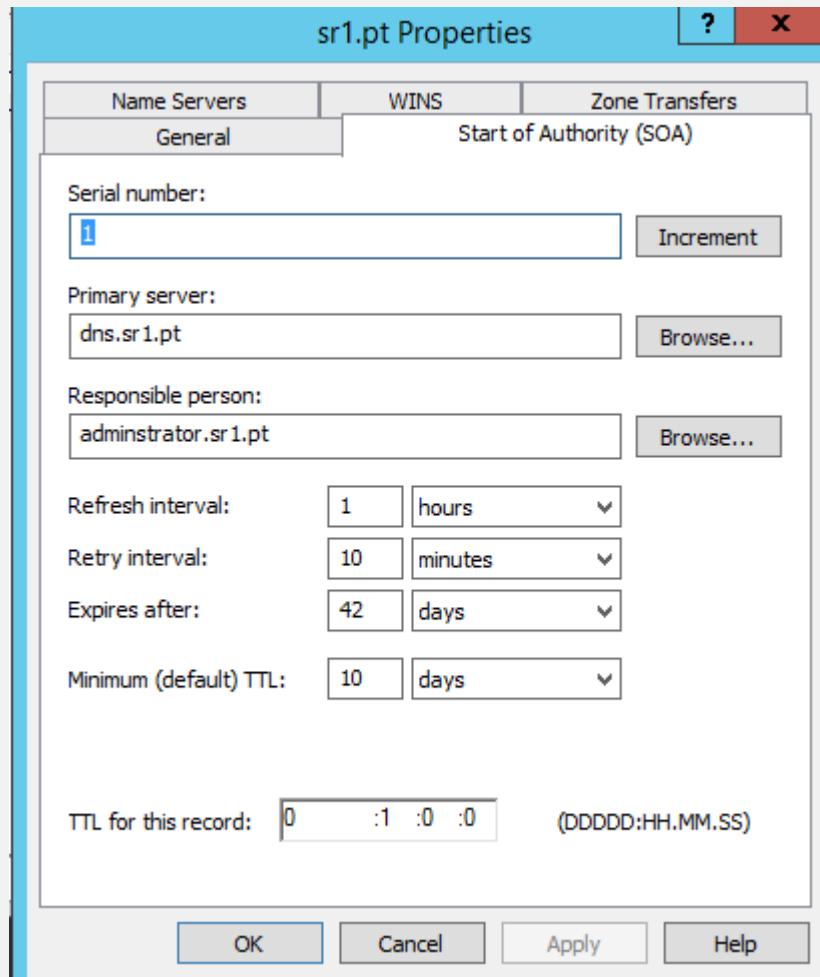
O arquivo com os dados do dns está localizado na pasta %SystemRoot%\System32\dns

Criar uma nova Zona Primária

- Depois de criar a Zona Direta surgiram automaticamente registos do tipo SOA e NS.
 - SOA: Start of Authority (SOA)** Primeiro registro de uma zona primaria, indica que este servidor é a melhor fonte de informações para os dados neste domínio DNS (servidor primário).
 - NS:** Especificam quais são os servidores DNS para o domínio.



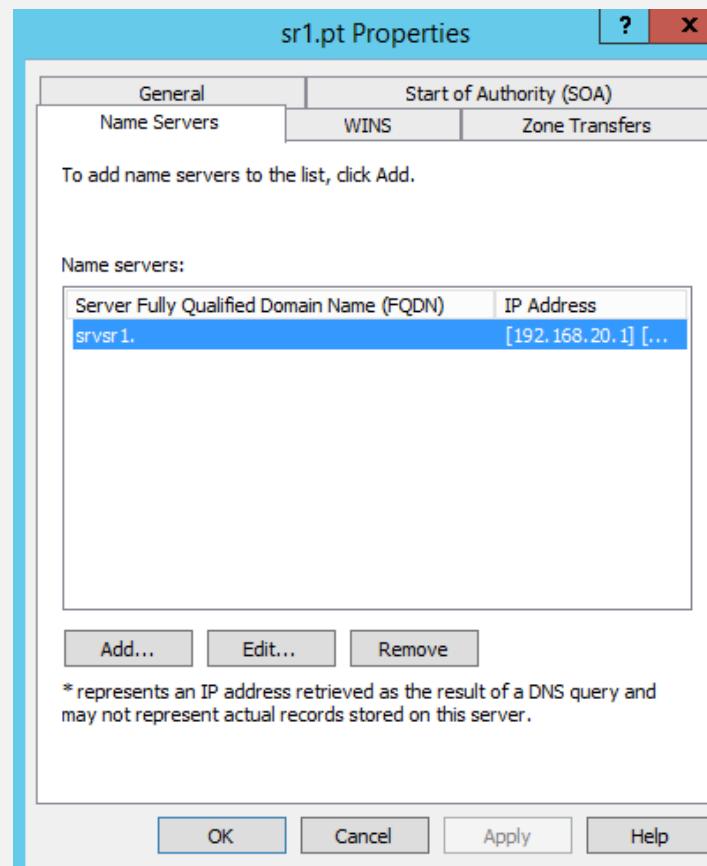
Configurar o SOA



- **SERIAL NUMBER**- versão do ficheiro de zona. Sempre que faz uma atualização ou deseja que o DNS seja propagado terá de incrementar este valor. A tática vulgarmente usada é escrever um número com o formato de data (ano/mês/dia/versão - 0..99). Exemplo: 2022042601.
- **PRIMARY SERVER**: Indica o servidor DNS autoritário daquela zona;
- **RESPONSIBLE PERSON** - endereço de email do administrador da zona (domínio);
- **REFRESH** - periodicidade (em segundos) com que os servidores secundários consultam o primário para averiguar a versão atual da zona. Valor típico: 3600 = 1h
- **RETRY** - Periodicidade (em segundos) com que os servidores secundários repetem a tentativa de averiguar o número de série do master file após falharem um contacto. Valor típico: 600 = 10m
- **EXPIRE** - Limite máximo (em segundos) de retenção de réplica da zona sem conseguir averiguar o número de série. Após este valor expirar os secundários deixam de poder responder pela zona. Valor típico: 3600000 -> 42d;
- **MINIMUM TTL** - define quanto tempo o registro dessa zona deverá permanecer no cache de um servidor DNS antes que seja feita uma atualização. Valor típico: 864000 -> 10d

Name Server

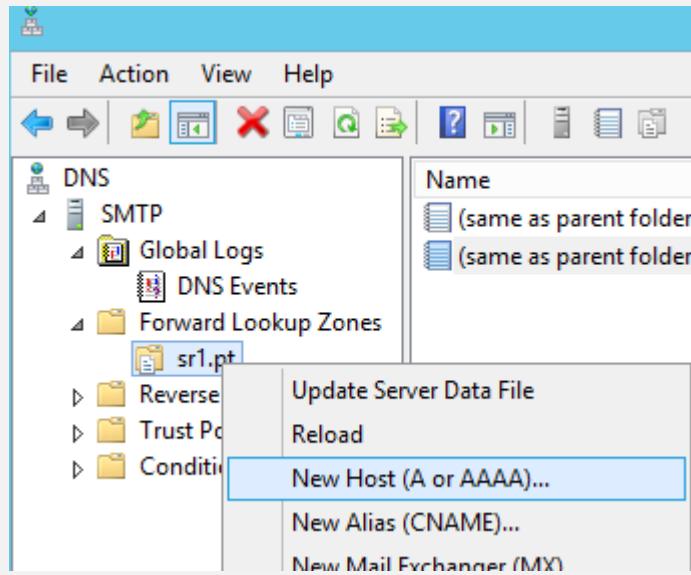
- Indica o servidor DNS autoritário daquela zona



Registros DNS

- São os registos da base de dados gerida pelos servidores de *DNS*.
- Existem registos de vários tipos. Alguns exemplos:
 - **A** - trata-se do tipo básico que estabelece a correspondência entre um nome canónico e um endereço IP (IP V4)
 - **AAAA** - igual ao anterior mas para IP V6.
 - **CNAME** - mapeia um alias para um nome de domínio verdadeiro ou canônico. Ou seja, indica que um nome é um nome alternativo para um outro nome. É particularmente útil para fornecer nomes alternativos que correspondem aos diferentes serviços de uma mesma máquina
 - **MX** - *Mail Exchanger* - Informa os IPs dos servidores SMTP de um domínio. Esse tipo de registro tem como particularidade um campo a mais, que informa a prioridade do servidor SMTP. Quanto mais baixo o valor, maior a prioridade. Cada registo MX deve corresponder a um registo A.
 - **SRV** - *Service Location* - permitem definir quais os servidores que suportam um determinado serviço para um domínio.
 - **NS** - *nome do domínio* - é o que faz com que a hierarquia de nomes funcione. Indica o nome (canónico) de uma máquina que aloja um servidor DNS para o domínio referido.
 - **TXT** - servem para associar informação ao domínio. Estas informações são com que pequenos ficheiros de texto, que podem conter qualquer informação pública que se pretenda associar ao domínio.
 - **PTR** - *Pointer* (IP => nome) - Associa um endereço IP a um hostname para a resolução de DNS reverso.

Registro do Tipo A



New Host

Name (uses parent domain name if blank):
dns

Fully qualified domain name (FQDN):
dns.sr1.pt.

IP address:
192.168.20.1

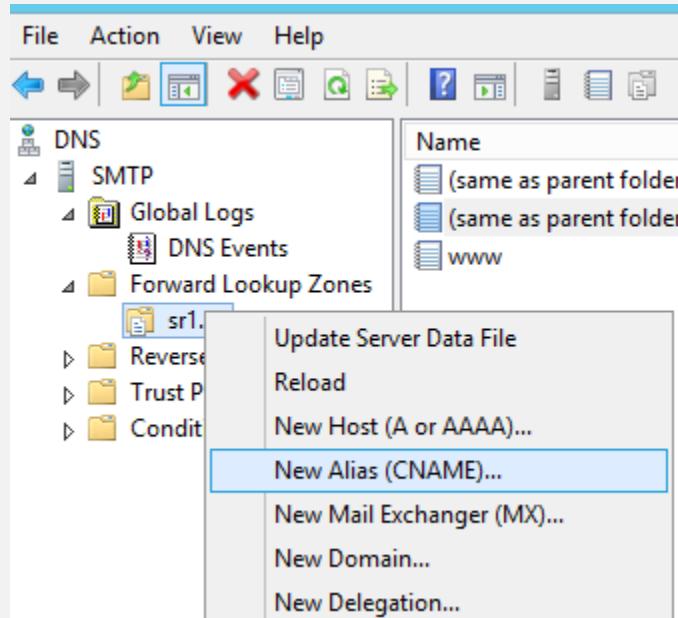
Create associated pointer (PTR) record

Add Host Cancel

Nome da máquina

IP da máquina

Registro CNAME

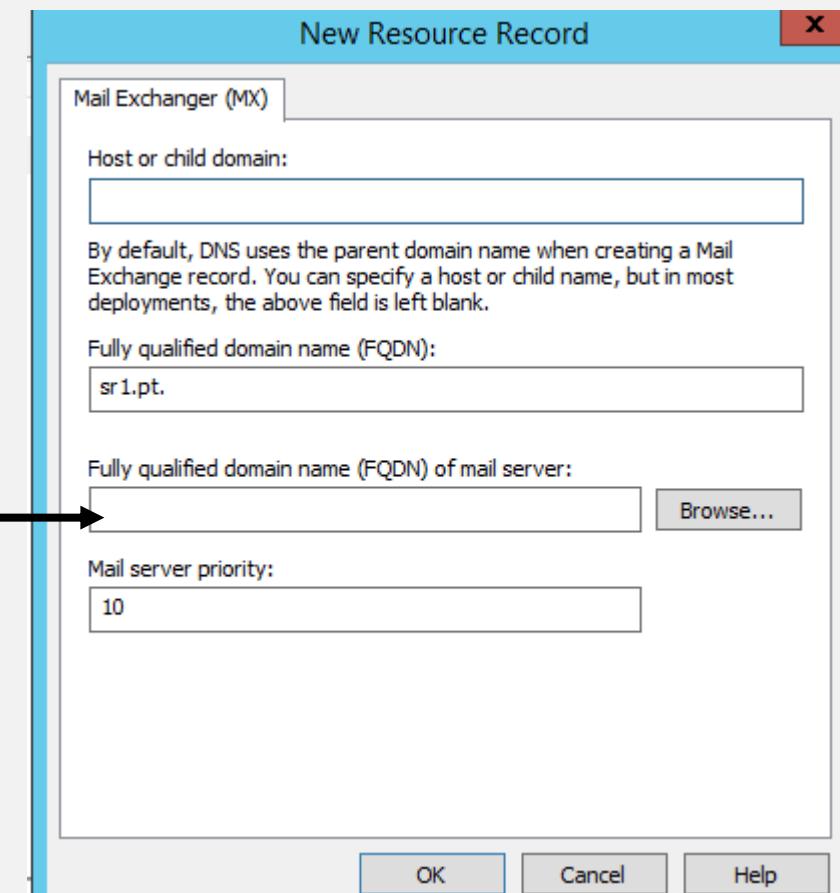


New Resource Record

This is a configuration dialog for creating a new CNAME record. It has tabs for 'Alias (CNAME)' (selected) and 'MX'. The 'Alias (CNAME)' tab contains fields for 'Alias name (uses parent domain if left blank)' (set to 'webmail') and 'Fully qualified domain name (FQDN)' (set to 'webmail.sr1.pt'). The 'MX' tab contains a field for 'Fully qualified domain name (FQDN) for target host' (set to 'www.sr1.pt') with a 'Browse...' button next to it.

Criar um Registo do tipo Mail Exchanger (MX)

- Controla para onde o correio electrónico será encaminhado no domínio.
- Clique com o botão do lado direito do rato sobre a zona primária, selecione a opção *New Mail Exchanger (MX)*
- Este campo indique o nome do servidor de mail.
- Na prioridade de servidor de correio coloque um número entre 0 e 65535 que indica a prioridade do servidor de correio relativamente aos outros servidores de correio. Os números menores têm preferência face aos servidores que são referenciados nos registos de recursos de intercâmbio de correio (MX) com números de prioridade mais elevados. A prioridade ou preferência mais elevada para um servidor de correio é atribuída quando é utilizado o valor zero (0).



Forwarders

The screenshot displays three windows related to DNS and SMTP configuration:

- Left Window (DNS Manager):** Shows the main navigation pane with options like "Configure a DNS Server...", "New Zone...", and "Forwarders". The "Forwarders" option is highlighted with a blue border.
- Middle Window (SMTP Properties):** A dialog box titled "SMTP Properties" with tabs for "Debug Logging", "Event Logging", and "Monitoring". The "Forwarders" tab is selected. It contains fields for "IP Address" (8.8.8.8) and "Server FQDN" (google-public-dns-a.go). A checkbox "Use root hints if no forwarders are available" is checked. A note at the bottom states: "Note: If conditional forwarders are defined for a given domain, they will be used instead of server-level forwarders. To create or view conditional forwarders, click the Conditional Forwarders link in the left pane." A red arrow points from the "Forwarders" link in the note to the "Forwarders" folder in the right window.
- Right Window (DNS Manager):** Shows the "Forwarders" folder under the "SMTP" node in the navigation pane. The folder contains sub-items: Global Logs, DNS Events, Forward Lookup Zones, Reverse Lookup Zones, Trust Points, and Conditional Forwarders. A red arrow points to the "Forwarders" folder.

Exercício 3

Exercício 3 – Configurar o DNS no Windows Server – Reverse Zone

Exercício 3

- Crie uma reverse zone no seu servidor de DNS.
- Registe os seus servidores. Como não tinha a zona criada aquando do registo na zona direta terá de o fazer na zona inversa.
- Registe em ambas as zonas o servidor crm.sr1.pt a responder no endereço 192.168.20.4
- Teste no cliente que a consulta inversa está a funcionar.

```
C:\Users\Administrator>ping -a 192.168.20.1

Pinging smtp [192.168.20.1] with 32 bytes of data:
Reply from 192.168.20.1: bytes=32 time<1ms TTL=128
```

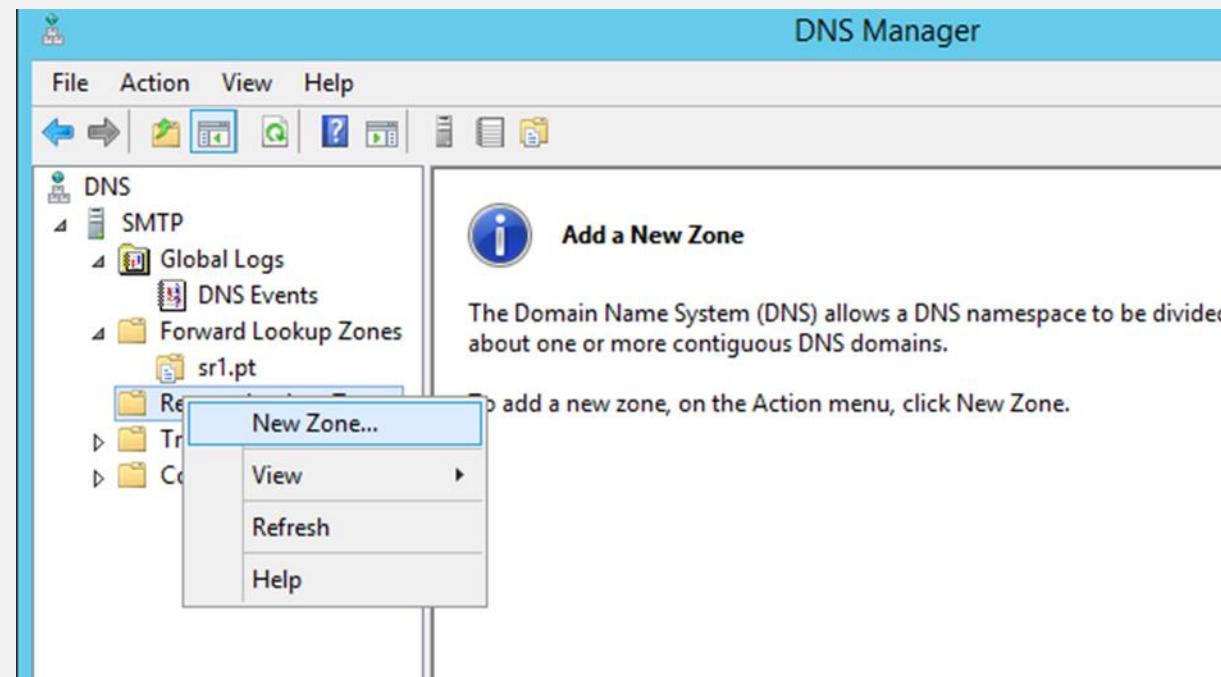
```
C:\Users\Administrator>ping -a 192.168.20.3

Pinging mail.sr1.pt [192.168.20.3] with 32 bytes of data:
Request timed out.
```

How To

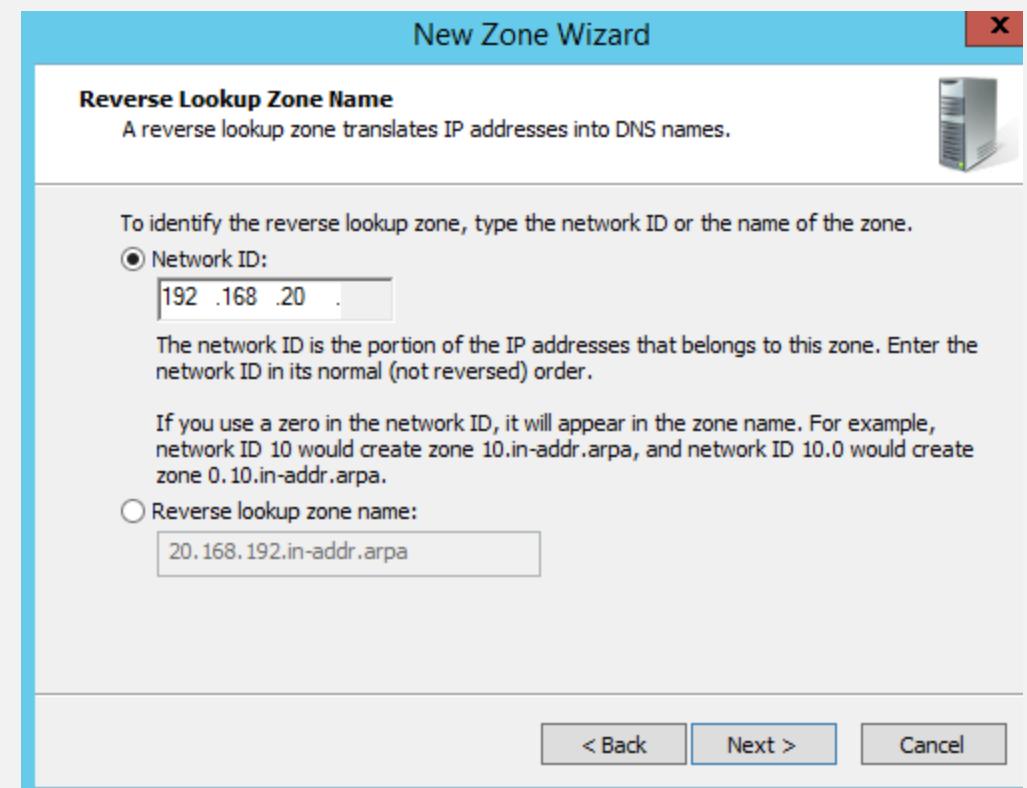
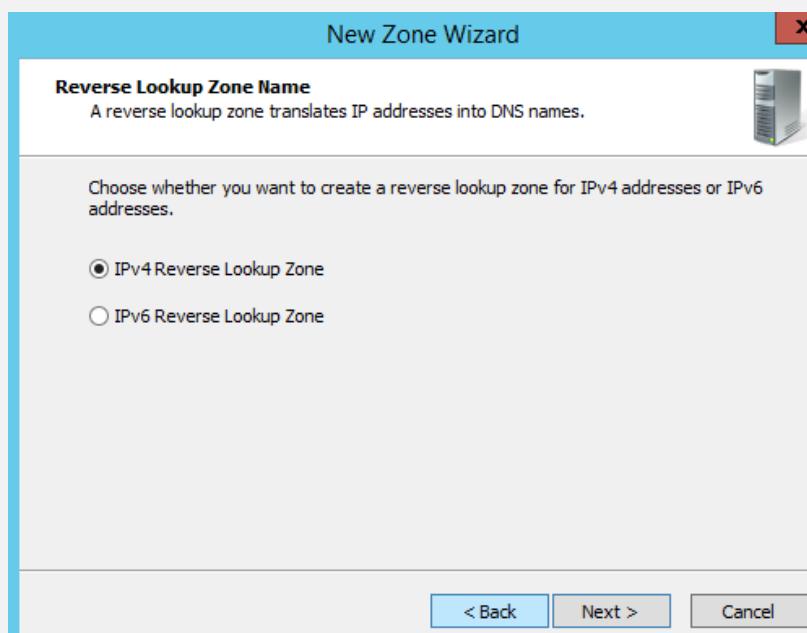
Criar Reverse Lookup Zone

- Clique com o botão do lado direito sobre *Reverse Lookup Zone* e escolha *New Zone*



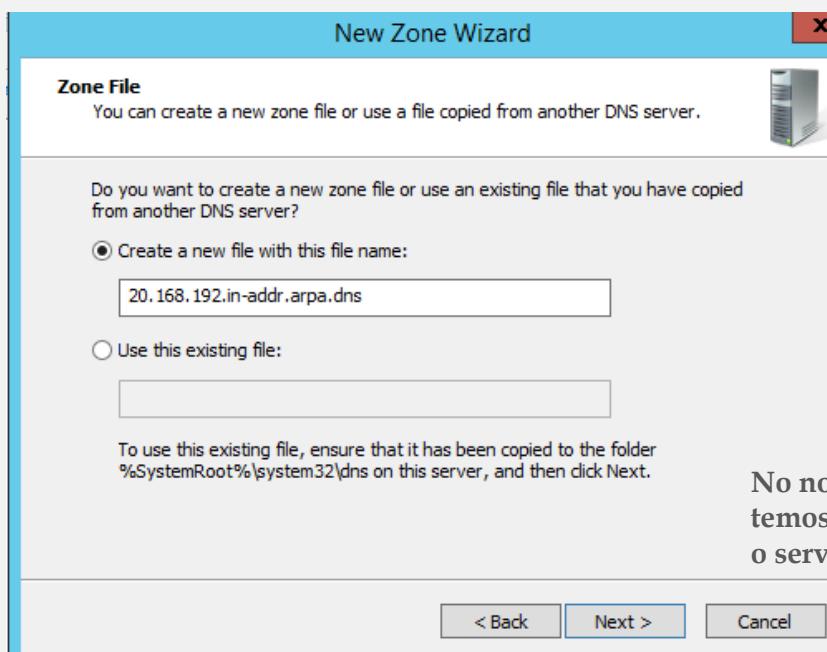
Criar Reverse Lookup Zone

- Escolher o tipo de versão de IP.
Selecione a opção IPv4 Reverse Lookup Zone
- No campo Network ID indique qual o endereço para o qual pretende fazer resolução inversa.

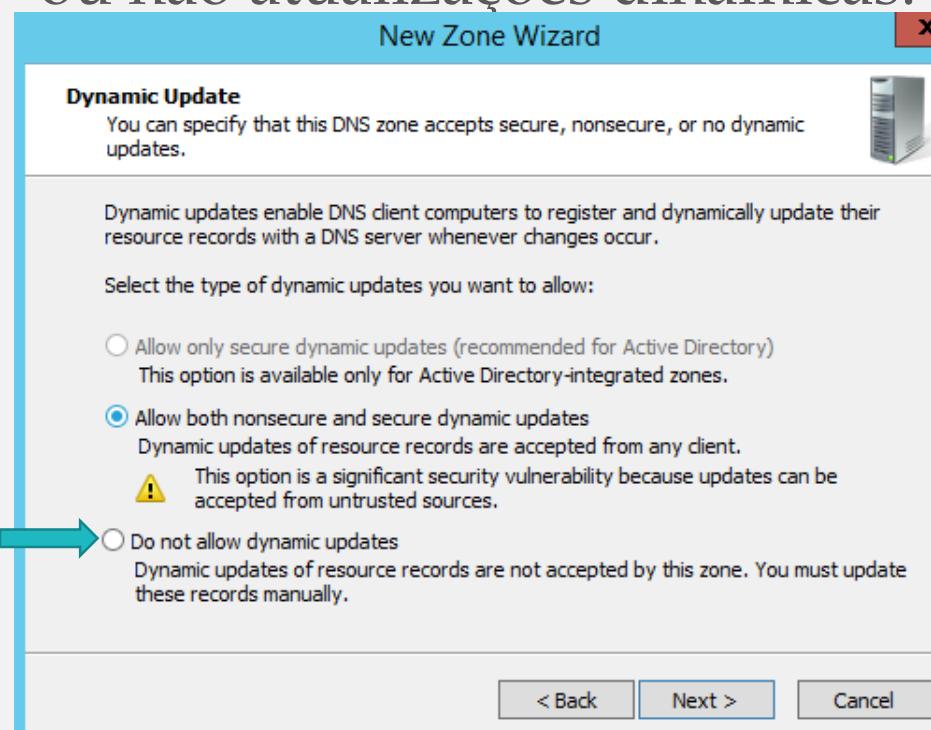


Criar Reverse Lookup Zone

- Indique se vai criar ou não um novo ficheiro. Pode usar um já existente.
- Selecionar o tipo de atualizações pretendida. As opções são permitir ou não atualizações dinâmicas.

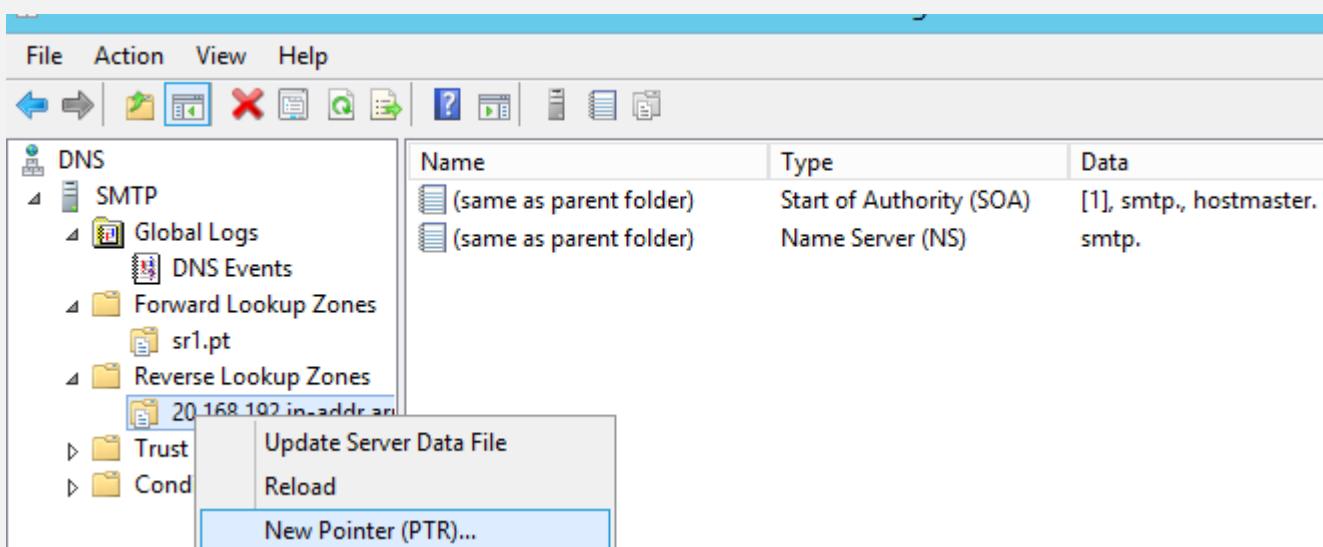


No nosso caso, já que não temos Active Directory nem o serviço DHCP.

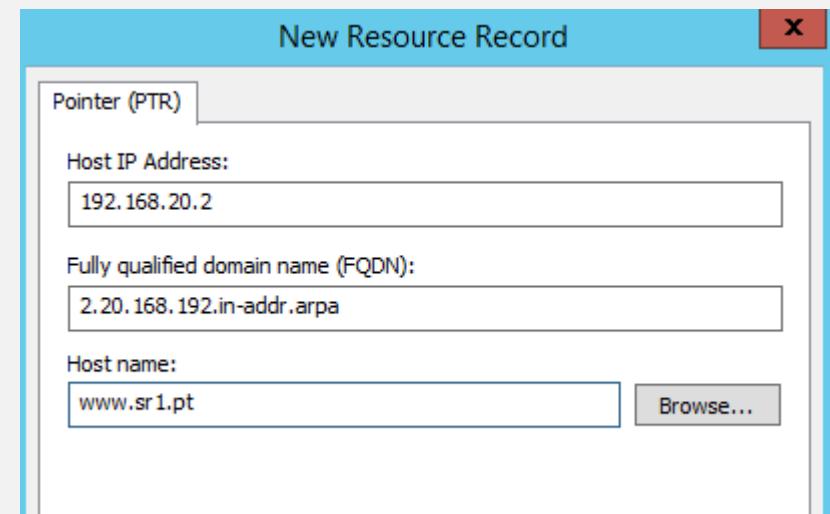


Criar novo Pointer (PTR)

- Clique com o botão do lado direito do rato na Reverse Lookup Zone e seleccione a opção New Pointer (PTR).



- Preencha o Host IP Address e Host name.
- Clique em Ok.



Exercício 4

Exercício 4 – Testar o DNS

Exercício 4

- Usando o comando *nslookup*:
 1. Verifique quais os servidores de DNS dos seguintes domínios:
 - sapo.pt
 - ipc.pt
 - isec.pt
 2. Qual o contacto do responsável pelo domínio “isec.pt”?
 3. Em caso de falha do serviço DNS do domínio isec.pt, por quanto tempo são válidas as informações (ou registos) existentes na cache do servidor 8.8.8.8 ?
 4. Qual o servidor responsável pela receção de correio eletrónico para o domínio isec.pt? E do ipc.pt?
 5. Qual o endereço IP do servidor Webmail.isec.pt?
 6. Qual o nome associado ao servidor 192.168.20.2?

How To

nslookup

- É uma ferramenta, que existe no Windows e no Linux, e que é utilizada para obter informações sobre registros de DNS de um determinado domínio, máquina ou IP.
- Numa consulta padrão, o servidor DNS definido na placa de rede da máquina é o consultado, e responde com as informações sobre o domínio ou máquina pesquisado.
- A informação "*Non-authoritative answer*" significa que o servidor DNS utilizado não responde por este domínio, em outras palavras, isto significa que foi feita uma consulta externa aos servidores DNS. Imagine que está em sua casa que faz uma consulta sobre uma máquina do ISEC, se for o seu servidor a responder a essa questão a resposta será *Non-authoritative answer* se for o servidor do ISEC será *Authoritative answer*.

nslookup - Consultas

- O tipo de consulta pretendida é definido pelo comando set q=
 - **A**
 - Uma simples consulta solicitando o endereço IP correspondente a um computador.
 - **CNAME**
 - Um dado computador pode possuir diversos nomes DNS. Um destes é o nome canónico (canonical name) ou de referência.
 - **MX**
 - Uma consulta para saber quem é o servidor de correio eletrónico de um determinado domínio.
 - **SOA**
 - Uma consulta ao Start of Authority de um determinado domínio .
 - **PTR**
 - Uma consulta PTR, que demonstra a resolução inversa (inverse ou reverse). Repare na forma algo esquisita da consulta, o que acontece parcialmente devido ao facto dos endereços IP possuírem a parte mais significativa no lado esquerdo enquanto os endereços DNS possuem-na no lado direito do endereço.

nslookup - Exemplos

```
C:\Users\Pedro Geirinhas>nslookup
Default Server: vodafonegw
Address: 192.168.1.1

> sapo.pt
Server: vodafonegw
Address: 192.168.1.1

Non-authoritative answer:
Name: sapo.pt
Addresses: 2001:8a0:2102:c:213:13:146:142
          213.13.146.142

> www.isec.pt
Server: vodafonegw
Address: 192.168.1.1

Non-authoritative answer:
Name: www.isec.pt
Address: 193.137.78.72

> set q=Mx
> isec.pt
Server: vodafonegw
Address: 192.168.1.1

Non-authoritative answer:
isec.pt MX preference = 20, mail exchanger = prxmx1.isec.pt
isec.pt MX preference = 30, mail exchanger = prxmx1.isec.pt
isec.pt MX preference = 10, mail exchanger = prxmx1.isec.pt
isec.pt MX preference = 40, mail exchanger = prxmx2.isec.pt

isec.pt nameserver = ns2.isec.pt
isec.pt nameserver = ns.isec.pt
prxmx1.isec.pt internet address = 193.137.78.24
prxmx2.isec.pt internet address = 193.137.78.26
ns2.isec.pt internet address = 193.137.78.3
ns.isec.pt internet address = 193.137.78.1

> set q=Mx
> sapo.pt
Server: vodafonegw
Address: 192.168.1.1

Non-authoritative answer:
sapo.pt MX preference = 5, mail exchanger = mx.ptmail.sapo.pt

sapo.pt nameserver = ns.sapo.pt
sapo.pt nameserver = dns01.sapo.pt
sapo.pt nameserver = ns2.sapo.pt
sapo.pt nameserver = dns02.sapo.pt
mx.ptmail.sapo.pt internet address = 212.55.154.36
ns.sapo.pt internet address = 212.55.154.202
ns2.sapo.pt internet address = 212.55.154.194
dns01.sapo.pt internet address = 213.13.28.116
dns02.sapo.pt internet address = 213.13.30.116
dns01.sapo.pt AAAA IPv6 address = 2001:8a0:2106:4:213:13:28:116
dns02.sapo.pt AAAA IPv6 address = 2001:8a0:2206:4:213:13:30:116
>
```

```
C:\Users\Pedro Geirinhas>nslookup
Default Server: vodafonegw
Address: 192.168.1.1

> set q=SOA
> isec.pt
Server: vodafonegw
Address: 192.168.1.1

Non-authoritative answer:
isec.pt
    primary name server = ns.isec.pt
    responsible mail addr = sysadmin.isec.pt
    serial = 2020041501
    refresh = 28800 <8 hours>
    retry = 3600 <1 hour>
    expire = 604800 <7 days>
    default TTL = 86400 <1 day>

isec.pt nameserver = ns2.isec.pt
isec.pt nameserver = ns.isec.pt
ns.isec.pt internet address = 193.137.78.1
ns2.isec.pt internet address = 193.137.78.3
>
```

```
C:\Users\Pedro Geirinhas>nslookup
Default Server: vodafonegw
Address: 192.168.1.1

>
> set q=A
> www.isec.pt
Server: vodafonegw
Address: 192.168.1.1

Non-authoritative answer:
Name: www.isec.pt
Address: 193.137.78.72
```

```
C:\Users\Pedro Geirinhas>nslookup
Default Server: vodafonegw
Address: 192.168.1.1

> server ns2.isec.pt
Default Server: ns2.isec.pt
Address: 193.137.78.3

> www.isec.pt
Server: ns2.isec.pt
Address: 193.137.78.3

Name: www.isec.pt
Address: 193.137.78.72
```

ipconfig

- Para visualizar a *cache* de resolução de nomes num cliente pode fazer:
 - ipconfig /displaydns

```
C:\Windows\system32\cmd.exe
Microsoft Windows 楔 Versão 6.1.7601
Copyright (c) 2009 Microsoft Corporation. Todos os direitos reservados.

C:\Users\peirinhas>ipconfig /displaydns

Configuração IP do Windows

www.youtube.com
Nome do registo : www.youtube.com
Tipo de registo : 5
TTL : 47
Comprimento de dados : 4
Sectião : Resposta
Registo CNAME : youtube-ui.l.google.com

pubads.g.doubleclick.net
Nome do registo : pubads.g.doubleclick.net
Tipo de registo : 5
TTL : 34
Comprimento de dados : 4
Sectião : Resposta
Registo CNAME : partnerad.l.doubleclick.net

fixe.ccdrc.global
Nome do registo : fixe.ccdrc.global
Tipo de registo : 1
TTL : 3584
Comprimento de dados : 4
Sectião : Resposta
Registo A <anfitrião> : 10.9.16.12
```

- Para esvaziar e repor uma cache de resolução de clientes:
 - ipconfig / flushdns

Dúvidas



Serviços de Rede 1 – **Aula 9 - Práticas**

2022-2023

Instituto Politécnico de Coimbra

Departamento de Engenharia Informática



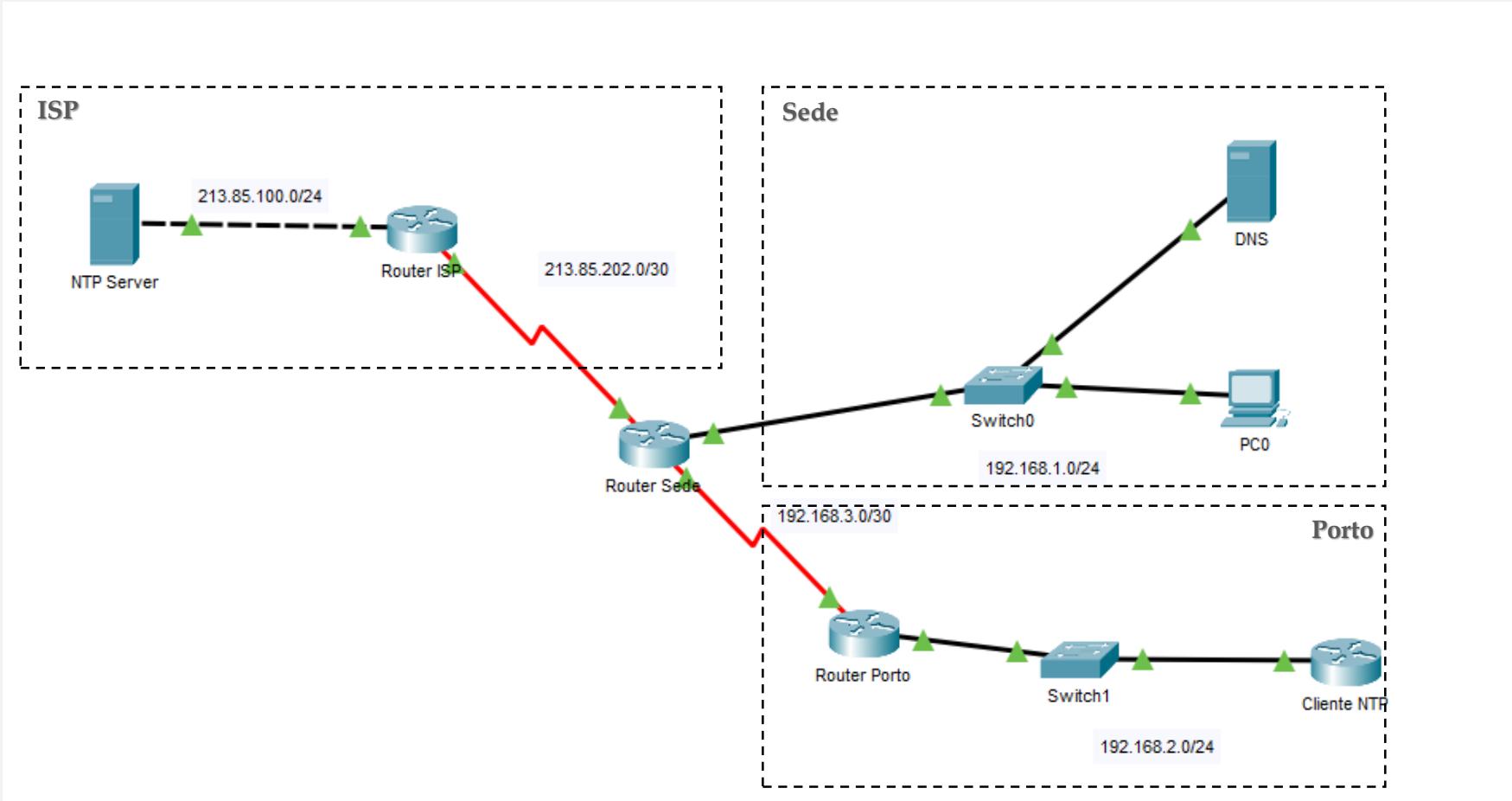
Pre – Requisitos

- Ter instalado o *Cisco Packet Tracer* na versão minima 7.3.1



Exercício 1 - NTP em ambiente Cisco

Exercício



Exercício

- Faça a topologia indicada na imagem anterior.
- Coloque o IP dos diferentes equipamentos de forma fixa mas de acordo com as redes indicadas na imagem.
- Garanta que todos os equipamentos têm conectividade com o servidor NTP (NTP Server) que está na rede do ISP.

Exercício

- Veja o tempo e a data no router da sede. Deve estar pouco certo...
- No servidor NTP Server desligue todos os serviços com exceção do NTP. Configure o serviço de NTP neste servidor.
- Configure o router da sede para se sincronizar com o servidor NTP.
- Force a atualização do calendário.
- Faça uma simulação (*Simulation*) para fazer uma análise dos pacotes de informação que são trocados entre o router e o servidor.

Exercício

PDU Information at Device: Router_Sede

OSI Model Inbound PDU Details

At Device: Router_Sede
Source: Router_Sede
Destination: 213.85.200.4

In Layers

- Layer 7: NTP
- Layer6
- Layer5
- Layer 4: UDP Src Port: 123, Dst Port: 123
- Layer 3: IP Header Src. IP: 213.85.200.4, Dest. IP: 213.85.201.2
- Layer 2: HDLC Frame HDLC
- Layer 1: Port Serial0/0/1

Out Layers

- Layer7
- Layer6
- Layer5
- Layer4
- Layer3
- Layer2
- Layer1

1. Serial0/0/1 receives the frame.

Challenge Me << Previous Layer Next Layer >>

PDU Information at Device: Router Sede

OSI Model Inbound PDU Details

PDU Formats

DATA (VARIABLE LENGTH)

NTP

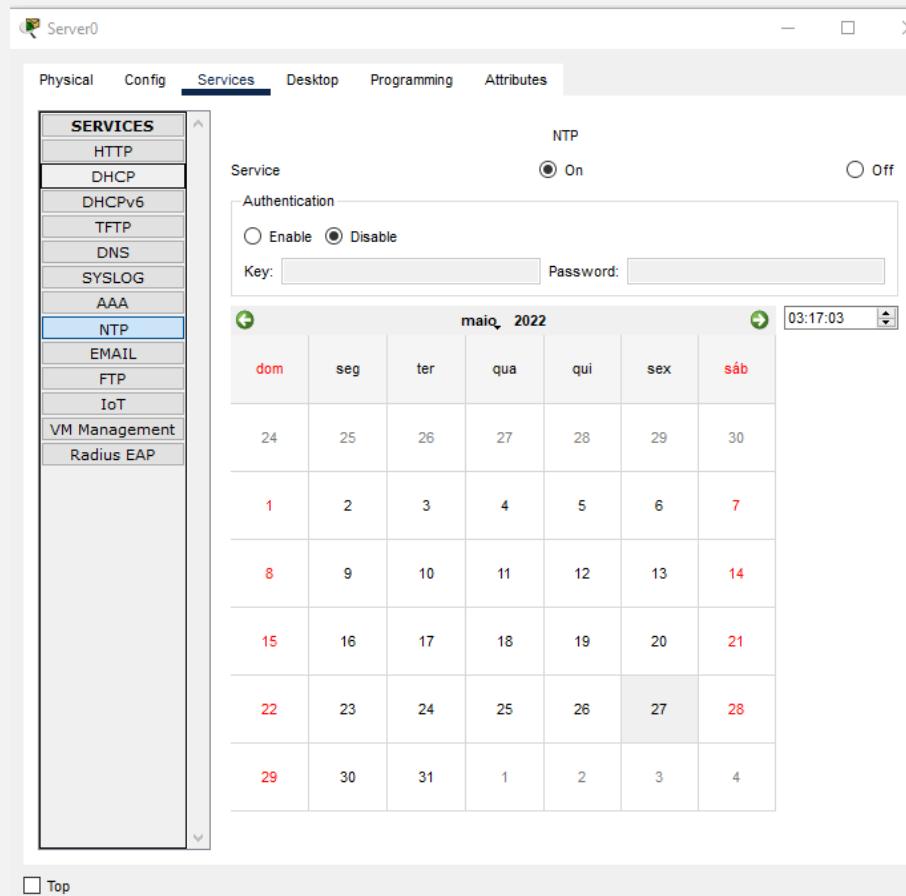
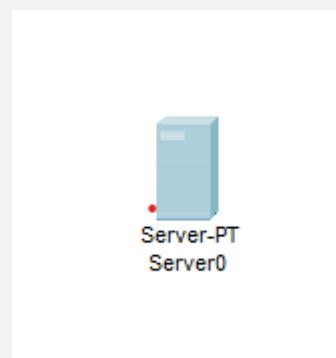
0	L	VN:4	MD:4	STRATUM:1	POLL:5	PREC:6e-08	Bits
ROOT DELAY:0							
ROOT DISPERSION:0.01006005983799696							
REFERENCE CLOCK IDENTIFIER:127.127.1.1							
REFERENCE TIMESTAMP:2020-05-12T01:03:58.302							
ORIGINATE TIMESTAMP:2020-05-12T00:55:45.996							
RECEIVE TIMESTAMP:2020-05-12T01:04:02.323							
TRANSMIT TIMESTAMP:2020-05-12T01:04:02.324							
KEY IDENTIFIER:0							
MESSAGE HASH: ***							

Exercício

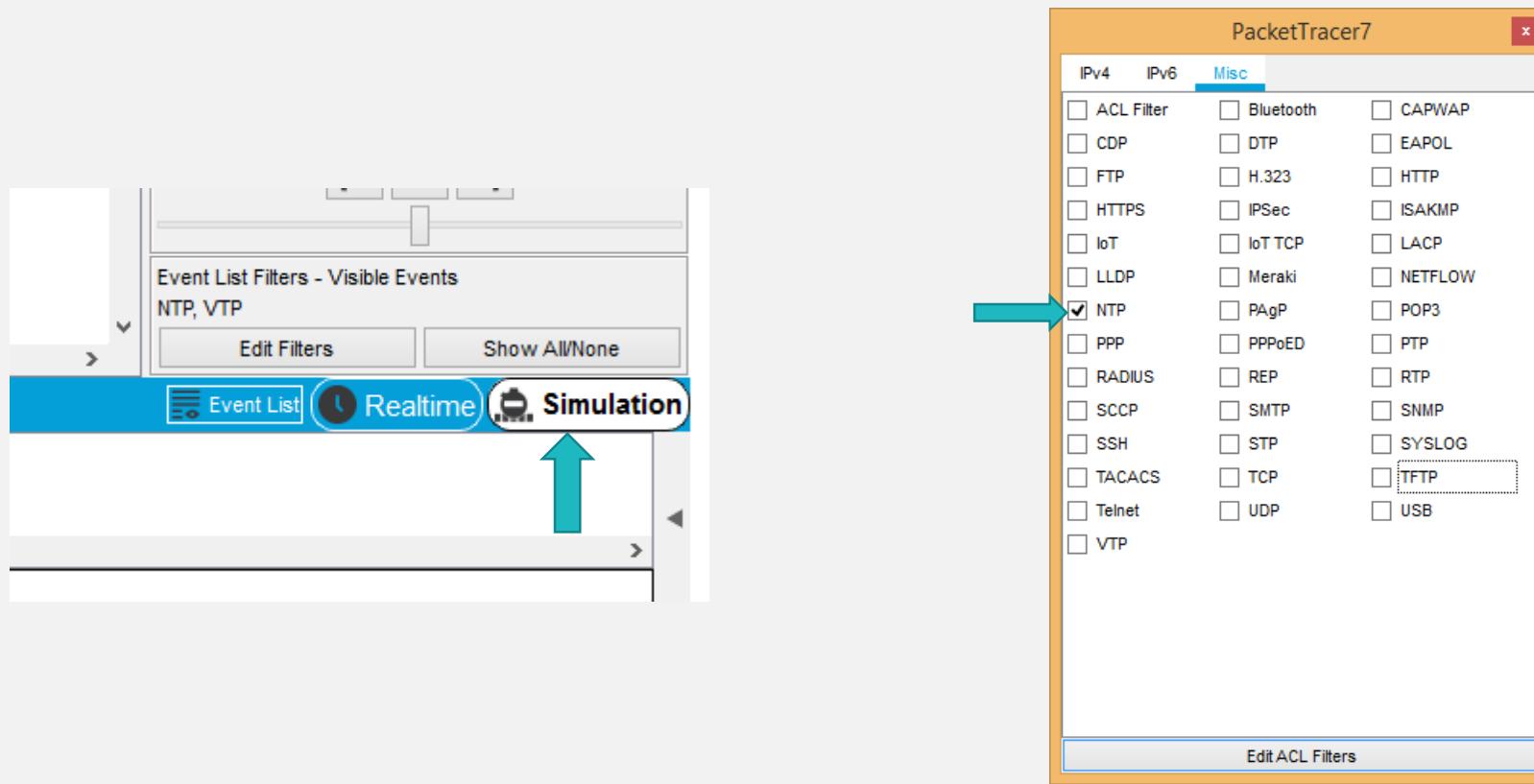
- Passe para modo *real time* e veja o tempo no router. Já está certo?
- Coloque o router do ISP a atualizar a hora no servidor NTP Server .
- Configure o router da sede como o *Stratum* da camada imediatamente seguinte ao do Servidor.
- Configure o router do Porto para se atualizarem no router da sede.

How To

Configurar o serviço NTP num servidor no PT



Simulação no PT



Configuração Cisco

- Para ver o tempo de um router deve correr o comando “*show clock*”:

```
R_Sede$sh clock  
*0:30:59.27 UTC Mon Mar 1 1993  
R_Sede#
```

- O NTP está activo em todos os interfaces por omissão

[no] **ntp enable**

Example:

```
switch(config)# ntp enable
```

Enables or disables the NTP protocol on the entire device. NTP is enabled by default.

- Definição do servidor de NTP

ntp server {ip-address | ipv6-address | dns-name} [**prefer**] [**use-vrf** vrf-name]

Example:

```
switch(config)# ntp server 192.0.2.10
```

Forms an association with a server. Optionally configures the NTP server to communicate over the specified VRF. The *vrf-name* can be any case-sensitive alphanumeric string up to 64 characters. Optionally use the **prefer** keyword to make this the preferred NTP server for the device.

Configuração Cisco

- Atualização do calendário

Command	Purpose
<code>ntp update-calendar</code>	Configures NTP to update the calendar.

- Estabelecer que o sistema é um servidor autoritário (master)

<code>[no] ntp master [stratum]</code> Example: switch(config)# ntp master	Configures the device as an authoritative NTP server. You can specify a different stratum level from which NTP clients get their time synchronized. The range is from 1 to 15.
---	---

- Podemos impor restrições usando *access-lists*

Command	Purpose
<code>ntp access-group {query-only serve-only serve peer} access-list-number</code>	Creates an access group and applies a basic IP access list to it.

Configuração Cisco

- Definir associações

```
ntp peer {ip-address | ipv6-address |  
dns-name} [prefer] [use-vrf vrf-name]  
  
switch(config)# ntp peer 2001:0db8::4101
```

Forms an association with a peer. You can specify multiple peer associations. Optionally configures the NTP peer to communicate over the specified VRF. Optionally use the **prefer** keyword to make this the preferred NTP peer for the device. The *vrf-name* can be any case-sensitive alphanumeric string up to 64 characters.

- Anúncios por *broadcast*

Command	Purpose
ntp broadcast [version number]	Sends NTP broadcast packets.
ntp broadcast client	Receives NTP broadcast packets.
ntp broadcastdelay microseconds	Adjusts estimated delay.

Configuração Cisco

- Monitorização

Command	Purpose
<code>show calendar</code>	Displays the current system calendar time.
<code>show clock [detail]</code>	Displays the current system clock time.
<code>show ntp associations [detail]</code>	Shows the status of NTP associations.
<code>show ntp status</code>	Shows the status of NTP.
<code>show sntp</code>	Displays information about SNTP (Cisco 1003, Cisco 1004, Cisco 1005, Cisco 1600, Cisco 1720, or Cisco 1750 only).

Exercício 2 – NTP em ambiente Windows

Exercício

- Faça o *download* e a instalação do programa The Meinberg NTP no servidor Windows 2012.
- O seu servidor deve ter as duas placas de rede ativadas: uma em NAT e outra para a rede interna.
- Na instalação deve:
 - Escolher os servidores NTP predefinidos para Portugal.
- Garanta que está instalado e a correr o The Meinberg NTP e que o serviço W32 time está desabilitado.
- Veja as propriedades do serviço NTP que acabou de instalar.

Exercício

- Identifique quem é o *system peer* do seu servidor NTP e quais são os outros servidores que participam no calculo da hora. Identifique o *stratum* desses servidores. Analise os outros parâmetros.
- Identifique qual a versão do NTP que está a correr e qual o *stratum* do seu servidor e a hora atual que ele tem.

How To

Ver e gerir os serviços num servidor

The screenshot shows the Windows Server Management console interface. On the left, the navigation pane includes links for Component Services, Computer Management, Connection Manager Administration Kit, Defragment and Optimize Drives, DNS, Event Viewer, Group Policy Management, Internet Information Services (IIS) Manager, iSCSI Initiator, Local Security Policy, Network Policy Server, ODBC Data Sources (32-bit), ODBC Data Sources (64-bit), Performance Monitor, Remote Access Management, Resource Monitor, Routing and Remote Access, Security Configuration Wizard, Services (selected), System Configuration, System Information, Task Scheduler, Windows Firewall with Advanced Security, Windows Memory Diagnostic, and Windows PowerShell.

The main area displays a table of services:

Name	Description	Status	Startup Type	Log On As
World Wide Web Publishing...	Provides W...	Running	Automatic	Local Syste...
Workstation	Creates and...	Running	Automatic	Network S...
WMI Performance Adapter	Provides pe...		Manual	Local Syste...
Wired AutoConfig	The Wired ...		Manual	Local Syste...
WinHTTP Web Proxy Auto...	WinHTTP i...		Manual	Local Service
Windows Update	Enables the ...		Manual (Trig...	Local Syste...
Windows Time	Maintains d...		Disabled	Local Service
Windows Store Service (WS...	Provides inf...		Manual (Trig...	Local Syste...
Windows Remote Manag...	Windows R...	Running	Automatic	Network S...
Windows Process Activatio...	The Windo...	Running	Manual	Local Syste...
Windows Modules Installer	Enables inst...		Manual	Local Syste...
Windows Management Inst...	Provides a c...	Running	Automatic	Local Syste...
Windows Licensing Monito...	This service ...	Running	Automatic	Local Syste...
Windows Internal Database ...	Provides th...	Running	Manual	Local Service
Windows Internal Database	Provides int...	Running	Manual	NT SERVIC...
Windows Installer	Adds, modifi...		Manual	Local Syste...
Windows Font Cache Service	Optimizes p...	Running	Automatic	Local Service
Windows Firewall	Windows Fi...	Running	Automatic	Local Service
Windows Event Log	This service ...	Running	Automatic	Local Service
Windows Event Collector	This service ...		Manual	Network S...
Windows Error Reporting Se...	Allows error...		Manual (Trig...	Local Syste...
Windows Encryption Provid...	Windows E...		Manual (Trig...	Local Service

Two windows are open in the foreground:

- Network Time Protocol Daemon Properties (Local Co...)**: Shows the service name as NTP, display name as Network Time Protocol Daemon, and startup type as Automatic. The description states: "Synchronizes the local system clock to a reference time source and (eventually) provide this time to NTP".
- Windows Time Properties (Local Computer)**: Shows the service name as W32Time, display name as Windows Time, and startup type as Disabled. The description states: "Maintains date and time synchronization on all clients and servers in the network. If this service is".

The Meinberg NTP

- O Windows possui, por padrão, uma implementação simplificada do NTP (w32time) que tem bastantes limitações. Recomenda-se então utilizar um programa especializado para gerir este serviço de rede.
- O “The Meinberg NTP” que é utilizado na maioria dos servidores NTP foi desenvolvido por David Mills o criador do primeiro RFC deste protocolo.
- Pode fazer o seu download em:
<https://www.meinbergglobal.com/english/sw/ntp.htm>

NTP for current Windows versions (Windows XP and later), with IPv6 support

The current stable NTP version can be used with current 32 and 64 bit Windows versions (Windows XP and newer). Beside the standard IPv4 network protocol it also supports **IPv6**. Alternatively, there's an [older version](#) available which can also be used on Windows 2000 or even Windows NT.

Note: Der current setup program **ntp-4.2.8p15a** supersedes **ntp-4.2.8p15** and **ntp-4.2.8p15-v2**. It includes preliminary patches for some minor vulnerabilities, see [this KB page](#).

This package also includes the current **openSSL libcrypto DLL v1.1.1t**.

It is explicitly recommended to upgrade earlier installations to this version.



[ntp-4.2.8p15a-win32-setup.exe](#) (4.25 MB)

19. April 2023

NTP package with IPv6 support for Windows XP and newer

SHA256 Checksum:

[ntp-4.2.8p15a-win32-setup.exe.sha256sum](#)

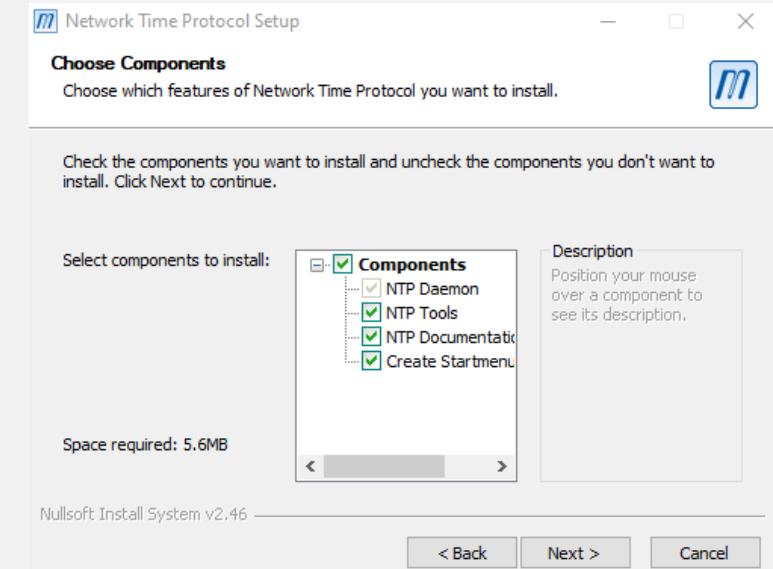
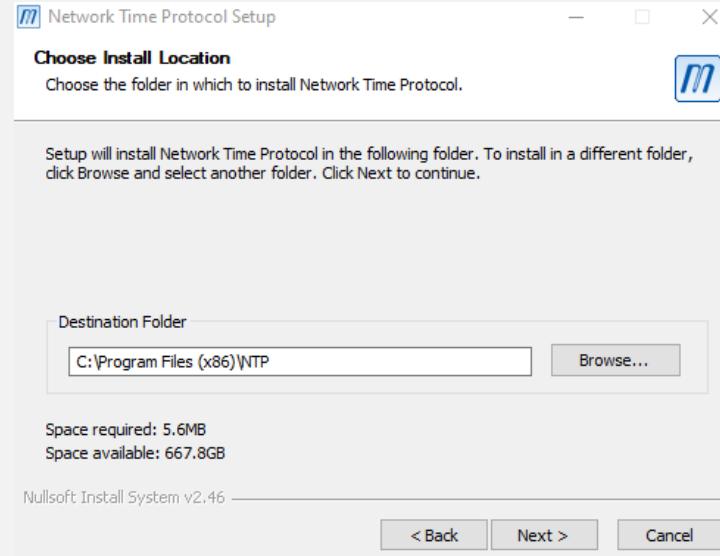
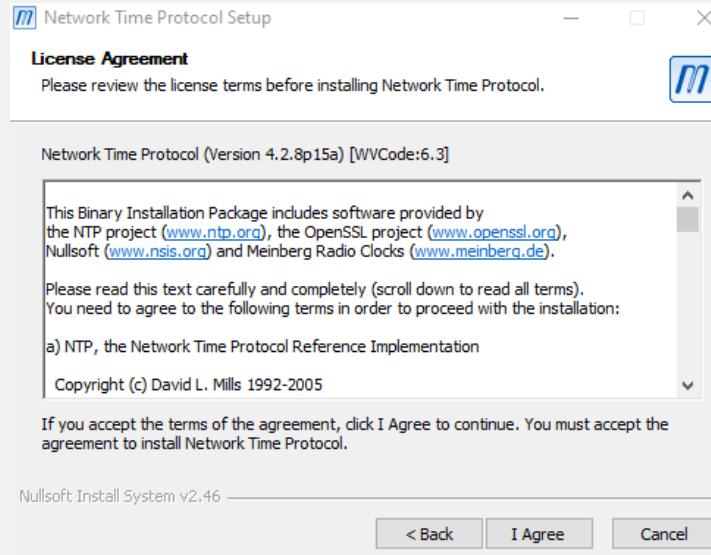
[How to verify integrity of the downloaded file](#)

Note: If the NTP service fails to start after installation on Windows XP or Windows 7, the **Visual Studio Redistributable** package may be missing, although it should be available by default on all current Windows installations. The 32 bit (x86) version of the redistributable is required even on 64 bit Windows systems. The package is available from the Microsoft download page:

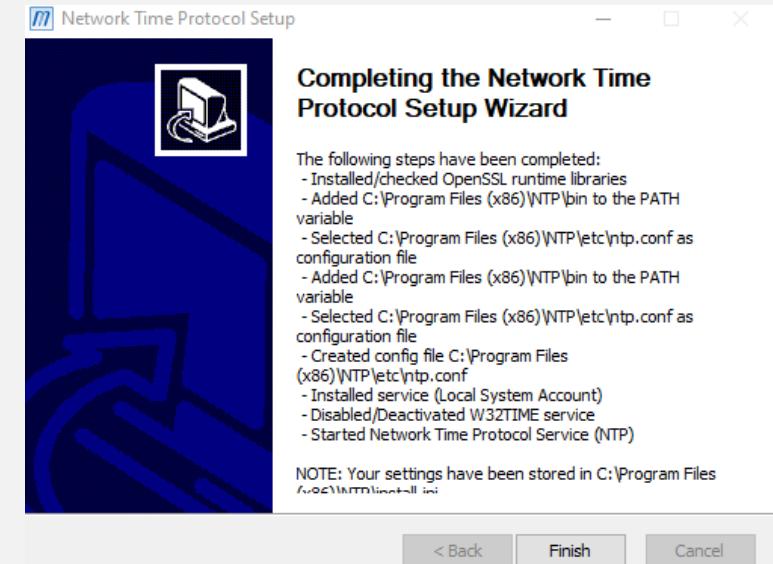
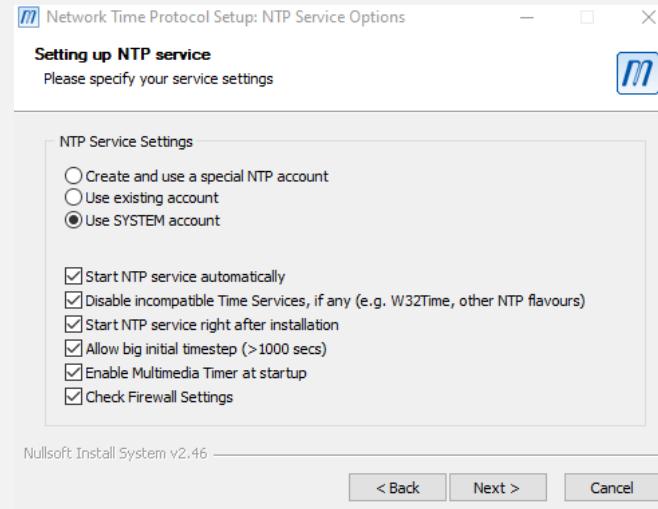
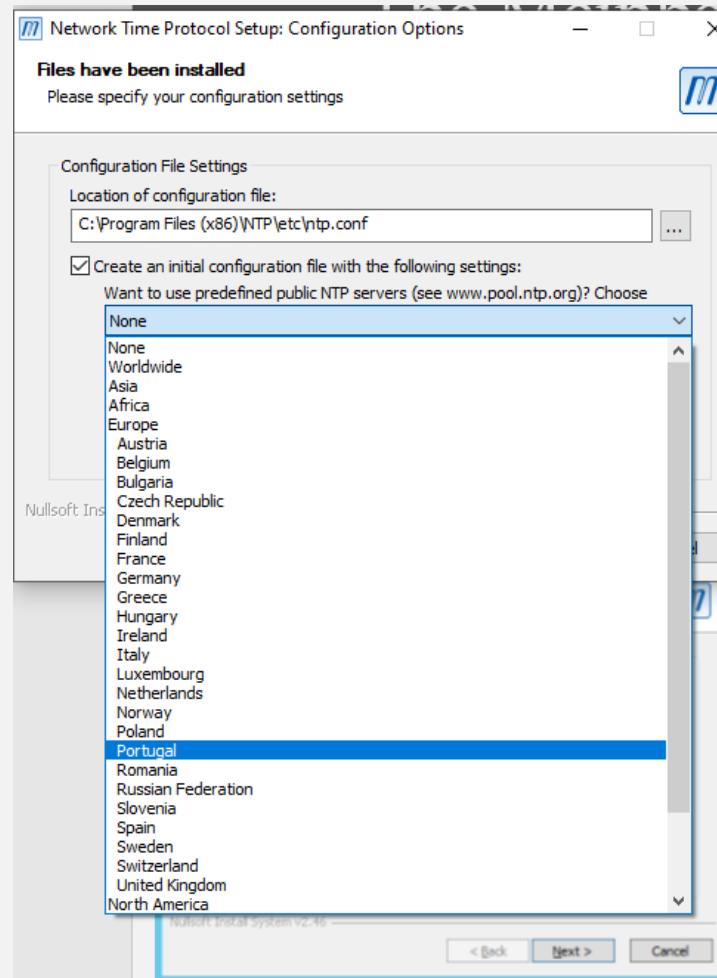
[Go to Windows Download Center](#)

[Installation of the Redistributable Package \(Screenshots\)](#)

The Meinberg NTP - Instalação



The Meinberg NTP - Instalação



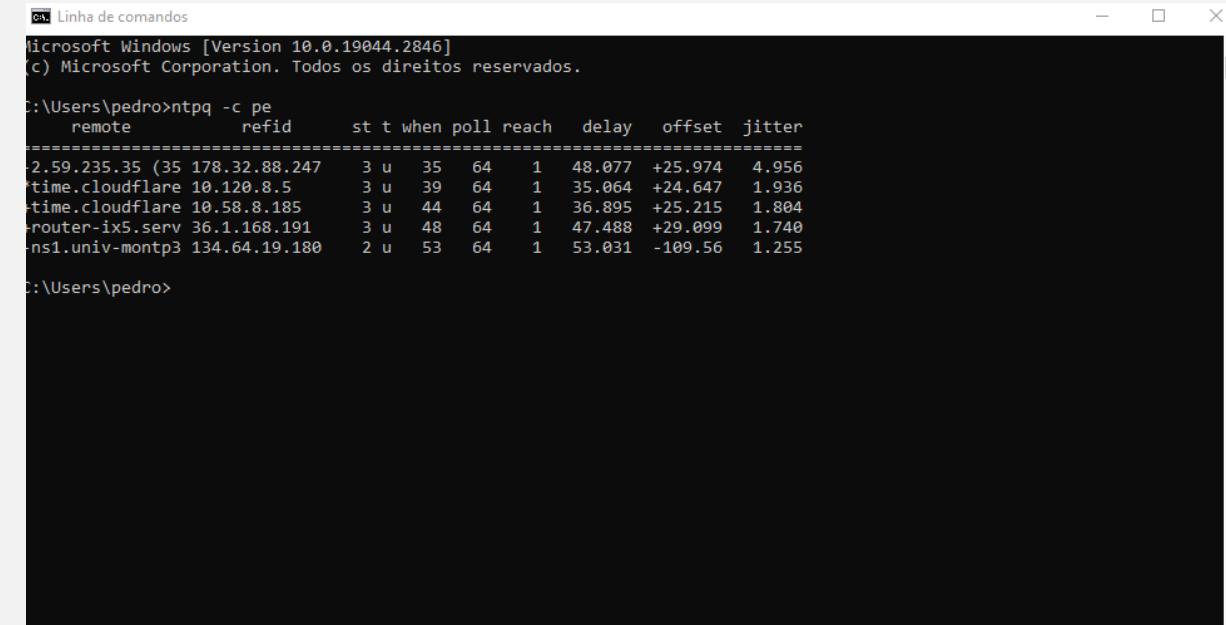
The Meinberg NTP - Monitorização do Servidor

- O NTP tem algumas ferramentas que permitem monitorar seu funcionamento. A mais importante é o "ntpq".

ntpq -c pe

- O * significa que este servidor foi escolhido como *system peer*, ou seja, a principal referência na sincronização do sistema. O + significa que o(s) servidor(es) também são usado(s), mas com um menor peso, para obter a hora certa.

- Pode ainda observar o offset, o deslocamento, delay, ou atraso, e o jitter, ou variação, todos em milissegundos.



Linha de comandos
Microsoft Windows [Version 10.0.19044.2846]
(c) Microsoft Corporation. Todos os direitos reservados.
C:\Users\pedro>ntpq -c pe
remote refid st t when poll reach delay offset jitter
*2.59.235.35 (35 178.32.88.247 3 u 35 64 1 48.077 +25.974 4.956
+time.cloudflare 10.120.8.5 3 u 39 64 1 35.064 +24.647 1.936
+time.cloudflare 10.58.8.185 3 u 44 64 1 36.895 +25.215 1.804
+router-ix5.serv 36.1.168.191 3 u 48 64 1 47.488 +29.099 1.740
+ns1.univ-montp3 134.64.19.180 2 u 53 64 1 53.031 -109.56 1.255
C:\Users\pedro>

- Se a resposta for "*ntpq: read: Connection refused*" é sinal que o seu servidor NTP **não** está a funcionar.

The Meinberg NTP- Monitorização do Servidor

Coluna	Significado
remote	Nome ou IP da fonte de tempo
refid	System pair ao qual o servidor de tempo remoto está sincronizado
st	O Stratum da fonte de tempo
t	Tipo de ligação- u para unicast, b para broadcast e l para local.
when	Quanto segundos passaram-se desde a última consulta à essa fonte de tempo
poll	De quantos em quantos segundos essa fonte é consultada
reach	Um registo de 8 bits representado na forma octal que vai rodando para a esquerda, que mostra o resultado das últimas 8 consultas à fonte de tempo: 377 = 11.111.111 significa que todas as consultas foram bem sucedidas; outros número indicam falhas, por exemplo 375 = 11.111.101, indica que a penúltima consulta falhou
delay	Atrasou, ou tempo de ida e volta, em milisegundos, dos pacotes até essa fonte de tempo
offset	Deslocamento, ou quanto o relógio local tem de ser adiantado ou atrasado, em milisegundos, para ficar igual ao da fonte de tempo
jitter	A variação, em milisegundos, entre as diferentes medidas de deslocamento para essa fonte de tempo

The Meinberg NTP Monitorização do Servidor

- Enquanto o comando anterior apresenta as variáveis relacionadas a cada associação, ou seja, a cada fonte de tempo, este comando apresenta as variáveis (globais) do seu servidor.
- Assim este comando permite ver informação adicional sobre o seu servidor:

ntpq -c rl

```
C:\Users\pedro>ntpq -c rl
associd=0 status=0618 leap_none, sync_ntp, 1 event, no_sys_peer,
version="ntpd 4.2.8p15a-o Apr 19 11:24:08 (UTC+02:00) 2023 (1)",
processor="x86", system="Windows", leap=00, stratum=4, precision=-22,
rootdelay=42.654, rootdisp=9.301, refid=162.159.200.1,
reftime=e804a979.966dae8d Tue, May  9 2023 12:14:01.587,
clock=e804aa8b.0a3cd205 Tue, May  9 2023 12:18:35.039, peer=61618, tc=7,
mintc=3, offset=-0.270937, frequency=+4.372, sys_jitter=1.520032,
clk_jitter=11.920, clk_wander=0.007

C:\Users\pedro>
```

The Meinberg NTP - Monitorização do Servidor

Variável	Significado
version	Versão do ntp
stratum	Stratum do servidor local
precision	Precisão indicada com o expoente de um número base 2
rootdelay	Atraso ou tempo de ida e volta dos pacotes até o Stratum 0, em milisegundos
rootdisp	Erro máximo da medida de offset em relação ao estrato 0, em milisegundos
refid	O par do sistema, ou principal referência
offset	Deslocamento, quanto o relógio local tem de ser adiantado ou atrasado para chegar à hora certa (hora igual à do estrato 0)
frequency	Erro na frequência do relógio local, em relação à frequência do estrato 0, em partes por milhão (PPM)

Exercício 3 – NTP em ambiente Windows – Consola de Gestão

Exercício

- Faça o *download* e a instalação do programa NTP Time Server Monitor no servidor Windows 2012.
- Faça na consola de gestão um Restart ao seu serviço NTP.
- Identifique quem é o *system peer* do seu servidor NTP e quais são os outros servidores que participam no calculo da hora. Identifique o *stratum* desses servidores. Analise os outros parâmetros.
- Gere estatísticas do seu servidor.
- Coloque os servidores **ntp02.oal.ul.pt** e **ntp04.oal.ul.pt** como os únicos servidores NTP ao qual o seu servidor vai usar para definir a hora. Veja qual é agora o *system peer* e quais são os outros servidores que participam no calculo da hora.
- Adicione agora o servidor **0.es.pool.ntp.org**. Veja o é agora o *system peer* e quais são os outros servidores que participam no calculo da hora.
- No cliente Windows 10 coloque o servidor NTP como o seu servidor.
- No cliente force a atualização. Veja o que acontece.

How To

NTP Time Server Monitor

- Existe uma ferramenta gráfica que facilita a gestão do servidor NTP.
- Como já pode ver, não necessita de ter essa ferramenta instalada para ter o serviço a correr e fazer as suas funções mas facilita a sua gestão.
- Essa ferramenta é o NTP Time Server Monitor e pode fazer o seu download em:

<https://www.meinbergglobal.com/english/sw/ntp-server-monitor.htm>

NTP Time Server Monitor

f share

tweet

in share

The NTP Time Server Monitor, available for the operating systems **Windows NT/2000 and later versions**, allows the user to configure and control the local NTP service with a userfriendly graphical user interface. Secondary the current status of the local NTP service, as well as external NTP services, can be displayed.

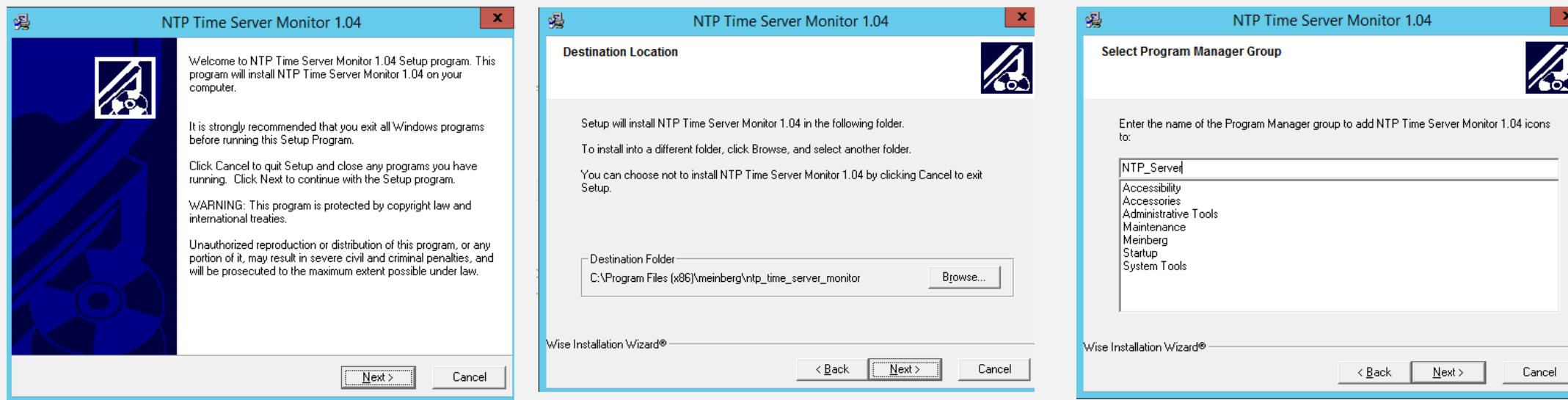
- [Download NTP Time Server Monitor for Windows operating systems](#)
- [Description of the Features](#)
- [Screenshots](#)
- [Changelog](#)
- [License Text](#)

NTP Time Server Monitor for Windows NT/2000 and later, Windows Server 2003 and later

 [ntp-time-server-monitor_1.04.exe](#) The 1.0 package is the first **stable release**, It is a self-extracting exe file for Windows operating systems, including a GUI setup program,
1,15 MB

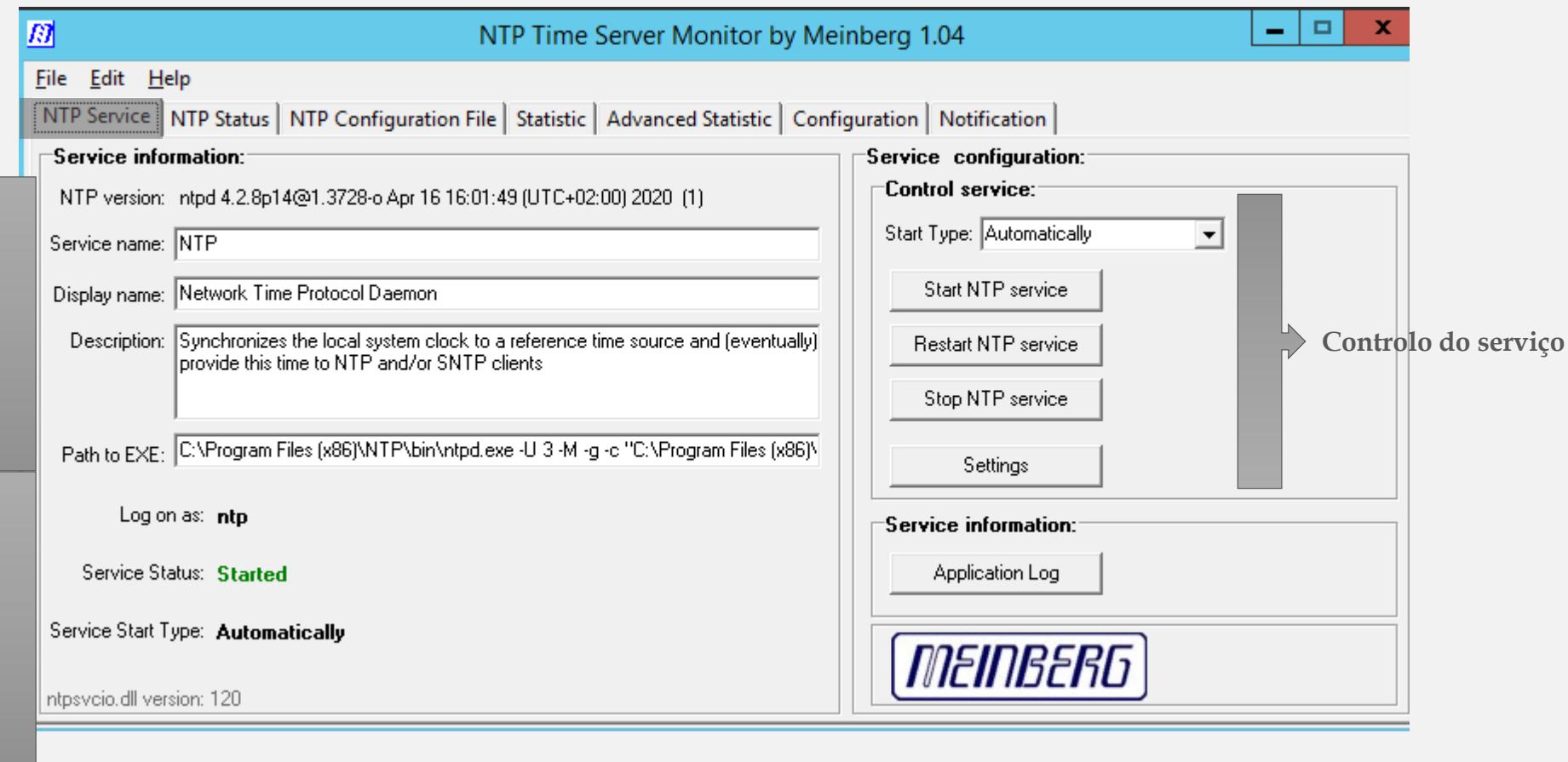
Please note: This version should not be used in production without intensive testing

NTP Time Server Monitor - Instalação



NTP Time Server Monitor - Operação

- Permite gerir o serviço de NTP



NTP Time Server Monitor - Operação

- Permite ver o estado dos servidores que está a utilizar para definir a hora:

The screenshot shows the 'NTP Time Server Monitor by Meinberg 1.04' application window. The title bar reads 'NTP Time Server Monitor by Meinberg 1.04'. The menu bar includes 'File', 'Edit', and 'Help'. The top navigation bar has tabs: 'NTP Service' (selected), 'NTP Status', 'NTP Configuration File', 'Statistic', 'Advanced Statistic', 'Configuration', 'NTP Event Log', and 'Notification'. Below the tabs, there's a 'localhost' dropdown. A status bar at the bottom displays 'Polling Status:' and 'Running NTP Version: ntpd 4.2.8p14@1.3728-o Apr 16 16:01:49 (UTC+02:00) 2020 (1)'.

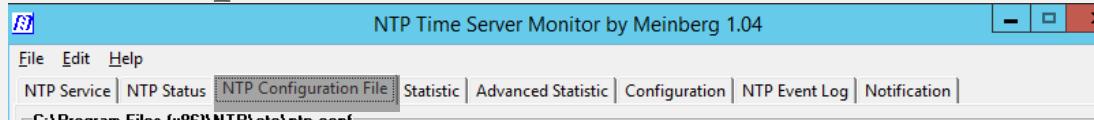
NTP Status:

Remote	Refid	Stratum	Type	When	Poll	Reach	Delay	Offset	Jitter
162.159.200.123	10.107.8.117	3	Unicast server	14	64	377	15.207	2620.925	25.754
+ 37.139.121.60	150.214.94.10	2	Unicast server	16	64	377	25.032	2618.480	47.269
5.56.160.3	212.183.233.76	2	Unicast server	19	64	377	57.405	2613.299	1.533
151.80.124.104	131.188.3.222	2	Unicast server	15	64	377	43.216	2617.214	16.809
* 82.64.165.222	GPS	1	Unicast server	19	64	301	54.512	2617.689	1.031

DNS lookup: Legend:

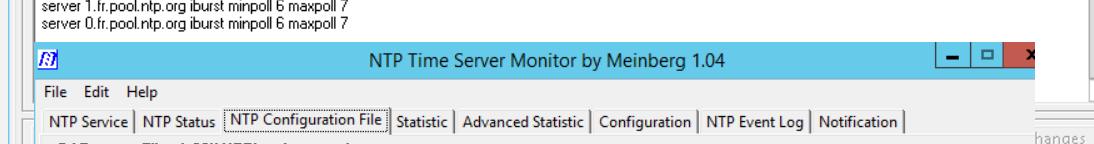
NTP Time Server Monitor - Operação

- Permite ver e editar o ficheiro de configuração do serviço.
- Para que as alterações tenham efeito, o serviço tem de ser reiniciado.



```
C:\Program Files (x86)\NTP\etc\ntp.conf
# your local system clock, could be used as a backup
# (this is only useful if you need to distribute time no matter how good or bad it is)
#server 127.127.1.0
# but it should operate at a high stratum level to let the clients know and force them to
# use any other timesource they may have.
#fudge 127.127.1.0 stratum 12

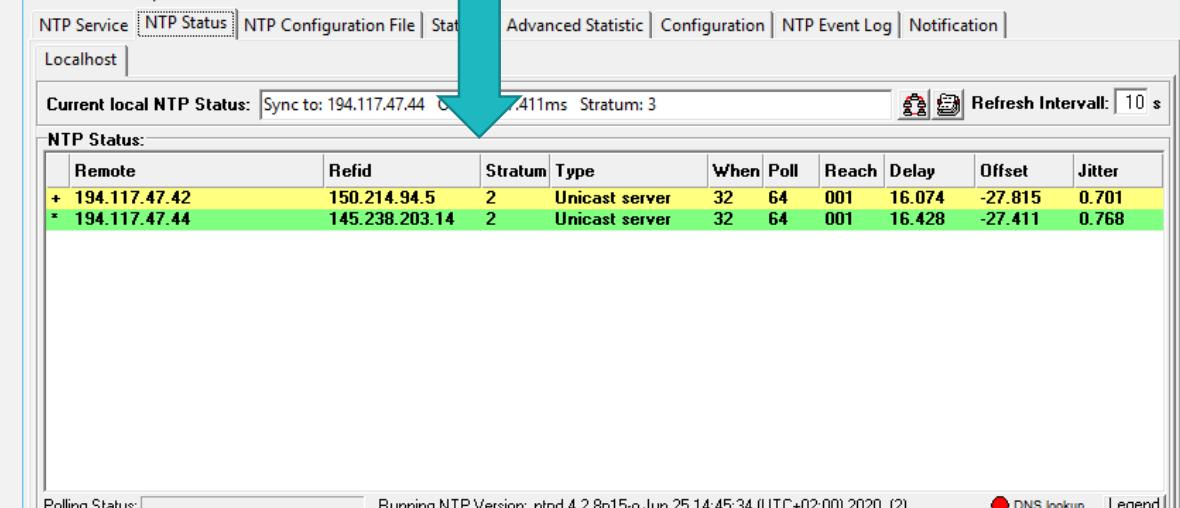
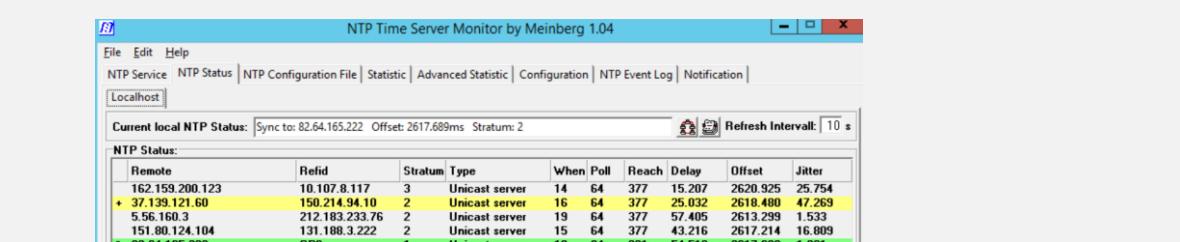
# Use a NTP server from the ntp pool project (see http://www.pool.ntp.org)
# Please note that you need at least four different servers to be at least protected against
# one falsicker. If you only rely on internet time, it is highly recommended to add
# additional servers here.
# The 'iburst' keyword speeds up initial synchronization, please check the documentation for more details!
server 0.es.pool.ntp.org iburst minpoll 6 maxpoll 7
server 1.es.pool.ntp.org iburst minpoll 6 maxpoll 7
server 2.es.pool.ntp.org iburst minpoll 6 maxpoll 7
server 1.fr.pool.ntp.org iburst minpoll 6 maxpoll 7
server 0.fr.pool.ntp.org iburst minpoll 6 maxpoll 7
```



```
C:\Program Files (x86)\NTP\etc\ntp.conf
# (this is only useful if you need to distribute time no matter how good or bad it is)
#server 127.127.1.0
# but it should operate at a high stratum level to let the clients know and force them to
# use any other timesource they may have.
#fudge 127.127.1.0 stratum 12

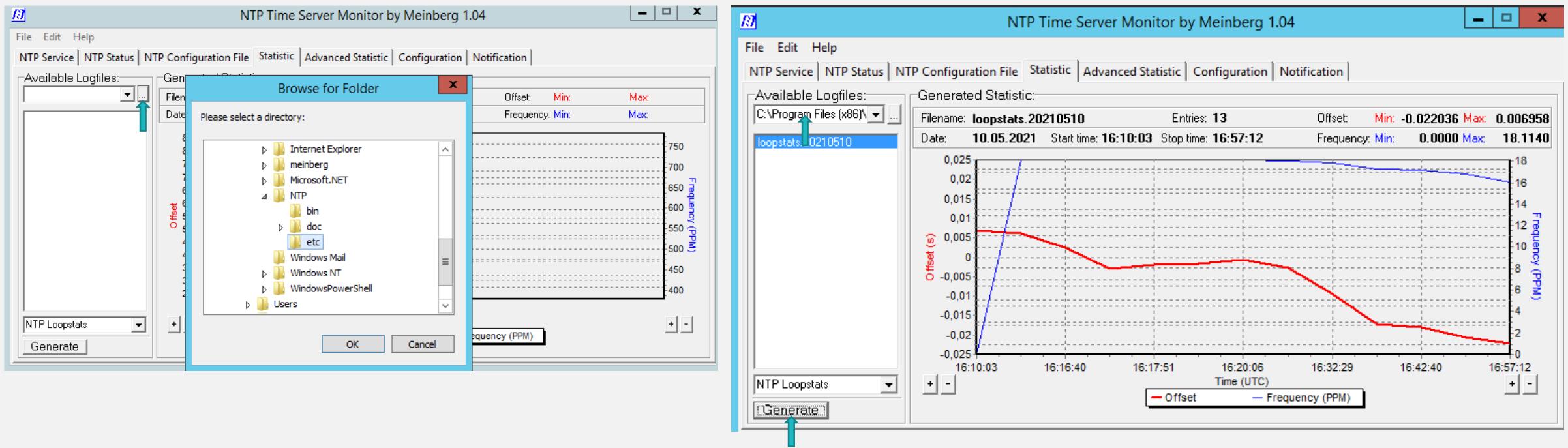
# Use a NTP server from the ntp pool project (see http://www.pool.ntp.org)
# Please note that you need at least four different servers to be at least protected against
# one falsicker. If you only rely on internet time, it is highly recommended to add
# additional servers here.
# The 'iburst' keyword speeds up initial synchronization, please check the documentation for more details!
server 0.es.pool.ntp.org iburst minpoll 6 maxpoll 7
server 1.es.pool.ntp.org iburst minpoll 6 maxpoll 7
server 2.es.pool.ntp.org iburst minpoll 6 maxpoll 7
server 1.fr.pool.ntp.org iburst minpoll 6 maxpoll 7
server 0.fr.pool.ntp.org iburst minpoll 6 maxpoll 7
server ntp02.oal.ul.pt iburst minpoll 6 maxpoll 7
server ntp04.oal.ul.pt iburst minpoll 6 maxpoll 7

# End of generated ntp.conf ... Please edit this to suite your needs
```



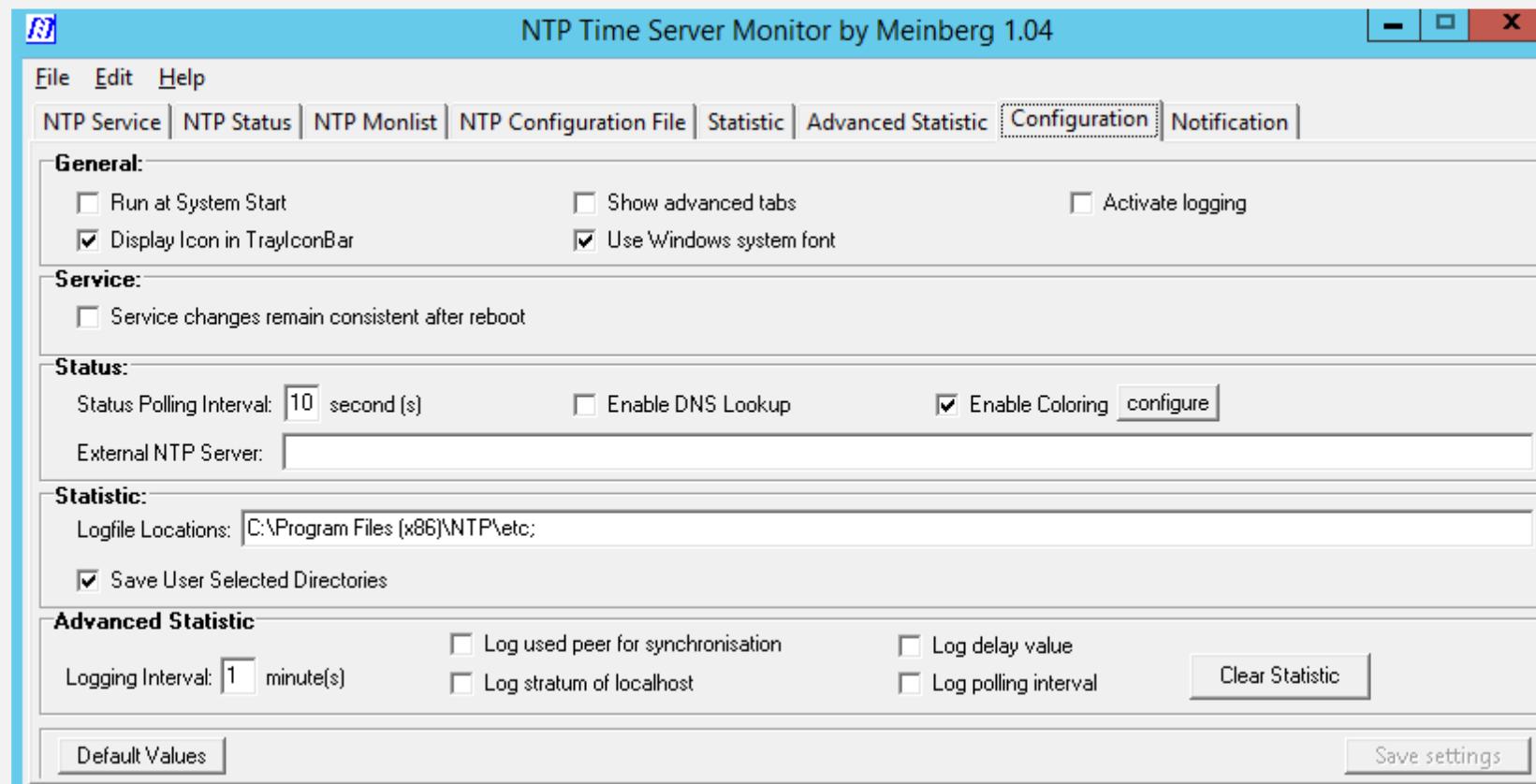
NTP Time Server Monitor - Operação

- Permite ver as estatísticas do seu servidor. Tem inicialmente de selecionar onde estão os LogFiles e qual o que vai usar para as estatísticas. Habitualmente os LogFiles estão em ...\\ntp\\etc



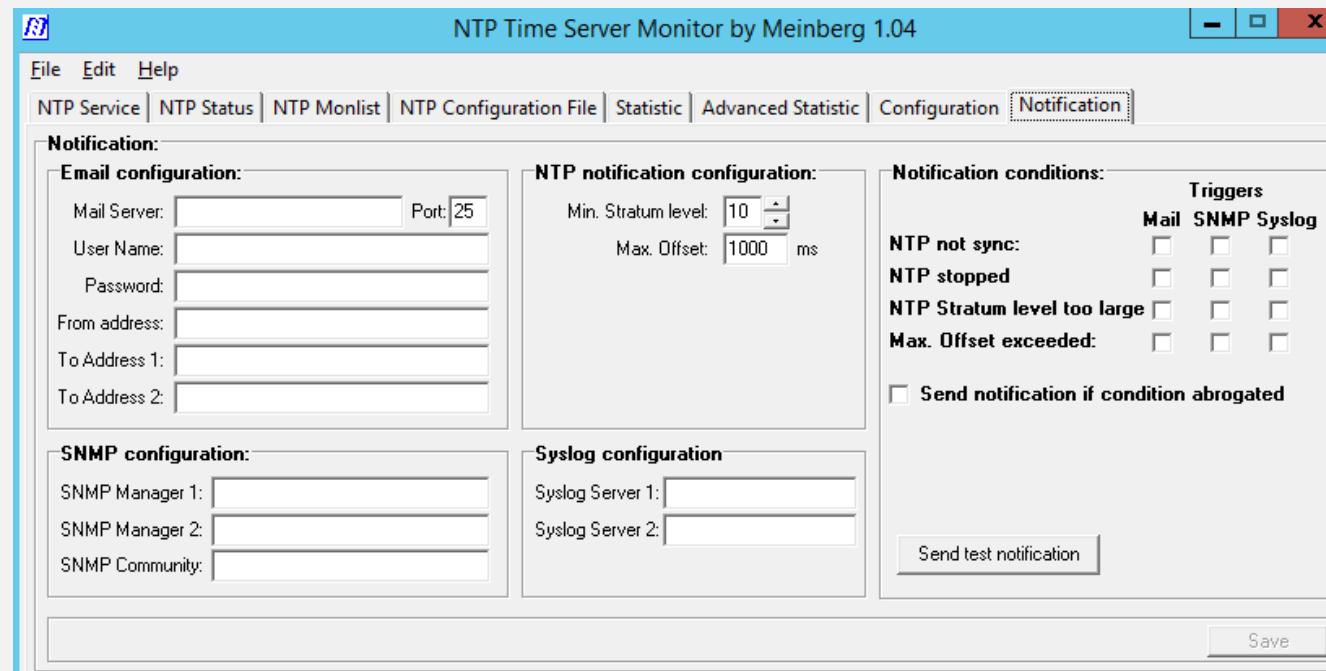
NTP Time Server Monitor - Operação

- Permite proceder à configuração do seu sistema

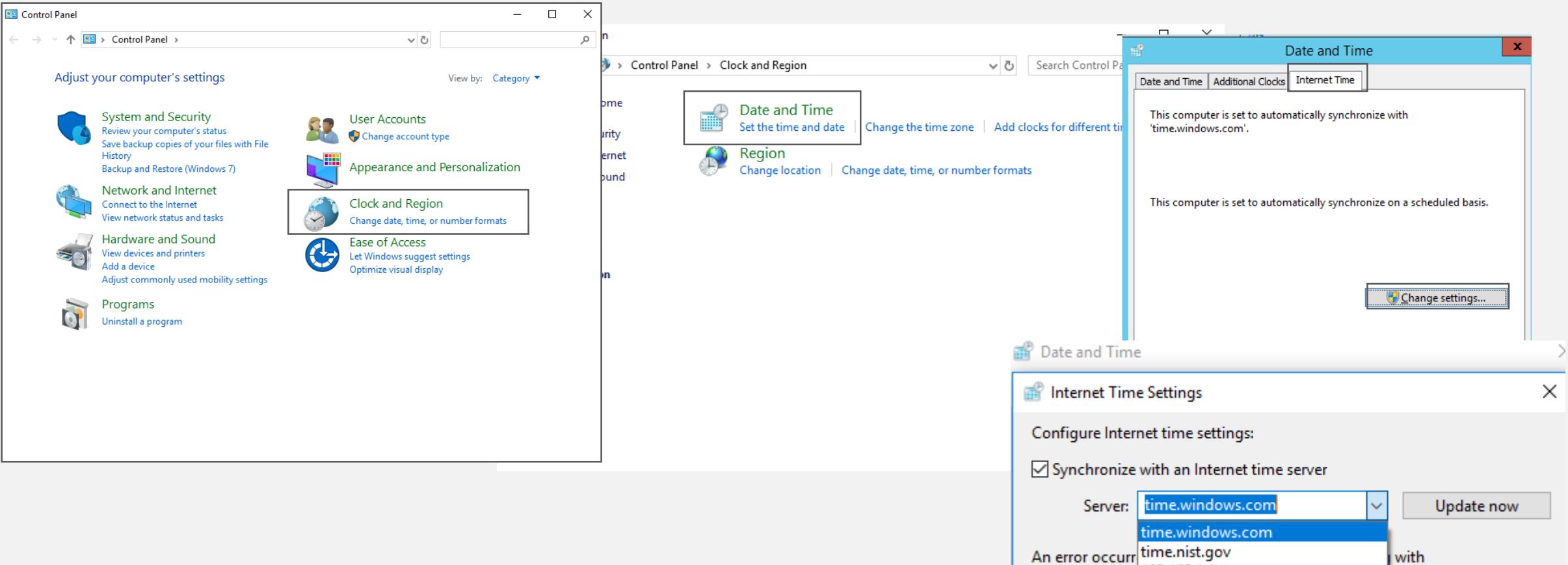


NTP Time Server Monitor - Operação

- Gerir as notificações, a configuração do SNMP e do syslog.

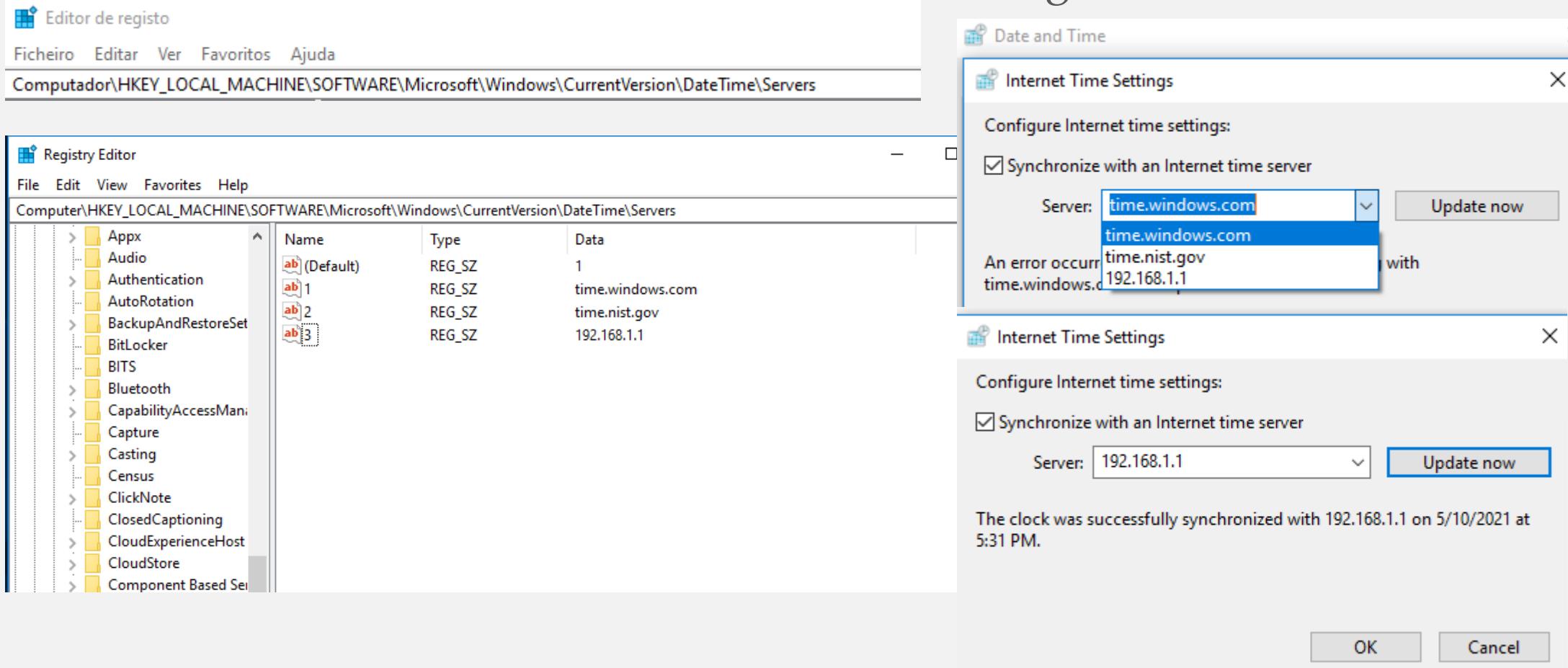


Alterar num cliente o servidor NTP



Adicionar um novo servidor NTP ao Cliente

- Corra o regedit no cliente e acrescente um novo registo



Dúvidas



Referências

- <https://www.cisco.com/c/en/us/td/docs/ios-xml/ios/bsm/configuration/15-2mt/bsm-time-calendar-set.html#GUID-A1071998-72BE-4F2E-8BC0-3A9FDC5D67EE> – acedido em Maio de 2022.
- https://www.cisco.com/c/en/us/td/docs/switches/datacenter/sw/4_2/nx-os/system_management/configuration/guide/sm_nx_os_cli/sm_3ntp.pdf – acedido em Maio de 2022.
- <https://www.youtube.com/watch?v=E7nglsM5n2Y> – acedido em Maio de 2022
- <https://ntp.br/guia-win-avancado.php> – acedido em Maio de 2022

Serviços de Rede 1 – **Aula 10 - Práticas**

2022-2023

Instituto Politécnico de Coimbra

Departamento de Engenharia Informática



Exercício 1 – Proxy em ambiente Windows

Exercício

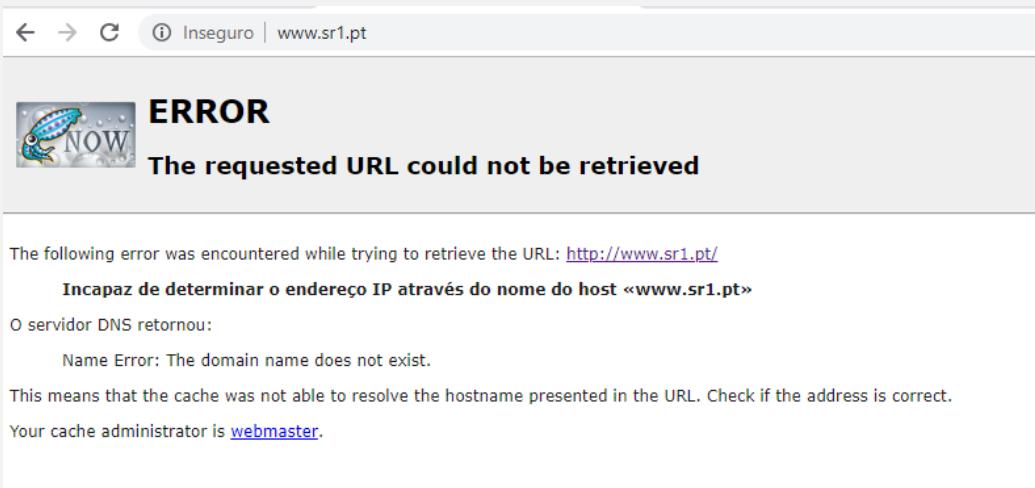
- A sua empresa deseja instalar um servidor Proxy garantindo que todos os clientes só acedem à Internet via este servidor.
- A topologia é a seguinte:



- Teste se o seu servidor Windows tem acesso à Internet.
- Teste se o seu cliente Windows tem acesso à Internet.

Exercício

- Faça o download do proxy Squid (<https://squid.diladele.com/>) Está igualmente disponível na página da cadeira no moodle.
- Faça a instalação do Squid no servidor.
- Configure no browser do cliente o proxy. Esta configuração terá de ser por IP e use o porto por defeito 3128 .
- Teste se tem acesso à Internet.
- Escreve na barra de endereços www.sr1.pt. Deve dar um erro... Quem informou desse erro?



Exercício

- Registe no DNS o servidor Proxy.
- Altere no cliente as definições do proxy para o controlo seja feito pelo nome do servidor e não por IP.
- Teste o acesso no cliente à Internet.
- Configure o Squid para que ele só aceite ligações da sua rede local.
- Teste o acesso no cliente à Internet.
- Altere na configuração do squid o porto de 3128 para 8080.
- Teste o acesso no cliente à Internet não alterando o porto no cliente. Não deve ter acesso...
- Coloque o porto 8080 do browser do cliente. Verifique como está a firewall do servidor. Já consegue aceder à Internet?

Exercício

- Teste se consegue aceder ao Facebook.
- Crie uma nova regra chamada **face** que bloquei o acesso ao Facebook. Grave o ficheiro de configuração do squid. Volte a arrancar com o serviço e teste se já está a funcionar a regra. Verifique que continua a conseguir aceder a outros sites.
- Teste que consegue aceder ao youtube.
- Crie uma nova regra chamada **externo** que vai ler a um ficheiro (bloq.txt) que está em *c:\squid\var\bloqueados*. Utilizando esse ficheiro, bloquei o acesso ao youtube. Teste o acesso a esse site e verifique que está a funcionar a regra. Teste se consegue aceder ao Facebook. Teste se consegue aceder a outros sites.
- Teste se acede ao wetransfer e dropbox.
- Utilizando o ficheiro anterior, bloquei o acesso a estes sites. Verifique que não acede a estes sites mas que consegue aceder a outros.
- Configure o bloqueio do facebook para ser feito pelo ficheiro e não por uma regra própria no ficheiro de configuração do squid. Teste e verifique que tudo está a funcionar corretamente.

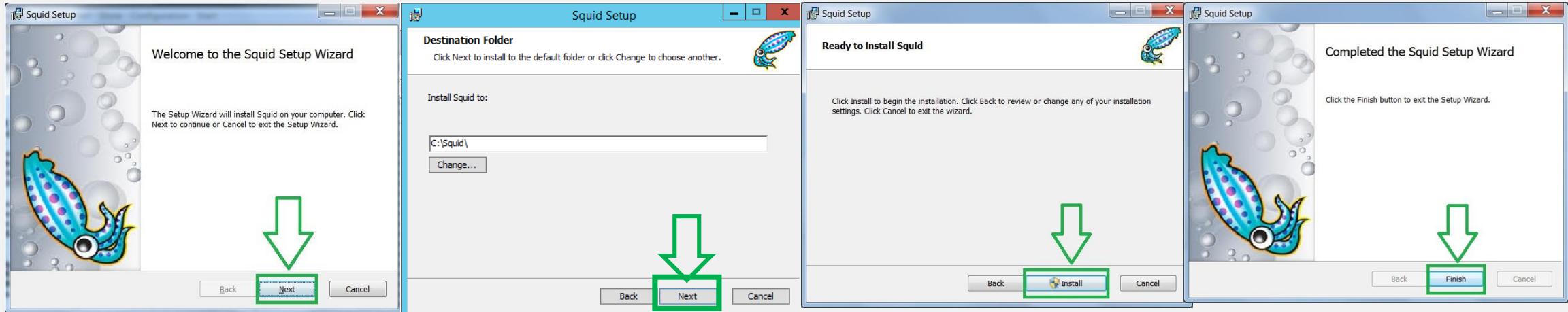
Exercício

- Teste que consegue aceder ao site do Soccer Manager
- Crie uma nova regra chamada *palavras* que vai ler a um ficheiro (bloq1.txt) que está em *c:\squid\var\bloqueados*. Utilizando esse ficheiro, bloquei o acesso a todos os sites que tenham a palavra soccer no seu URL.
- Teste o acesso no cliente a sites que contenham essa palavra e garanta que consegue aceder a outros sites.

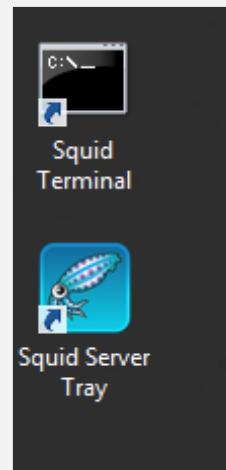
How To

Instalação

- A instalação é bastante fácil.

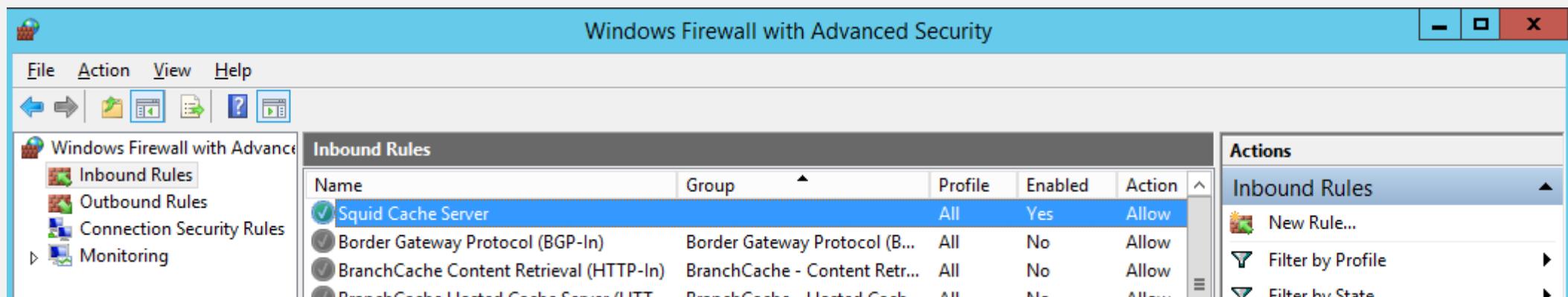


Devem surgir estes dois ícones depois da instalação

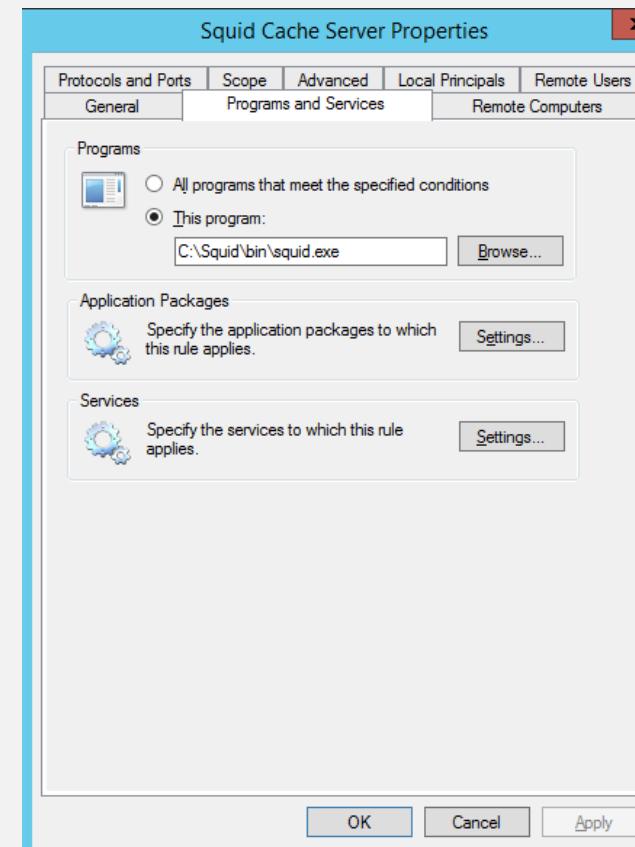
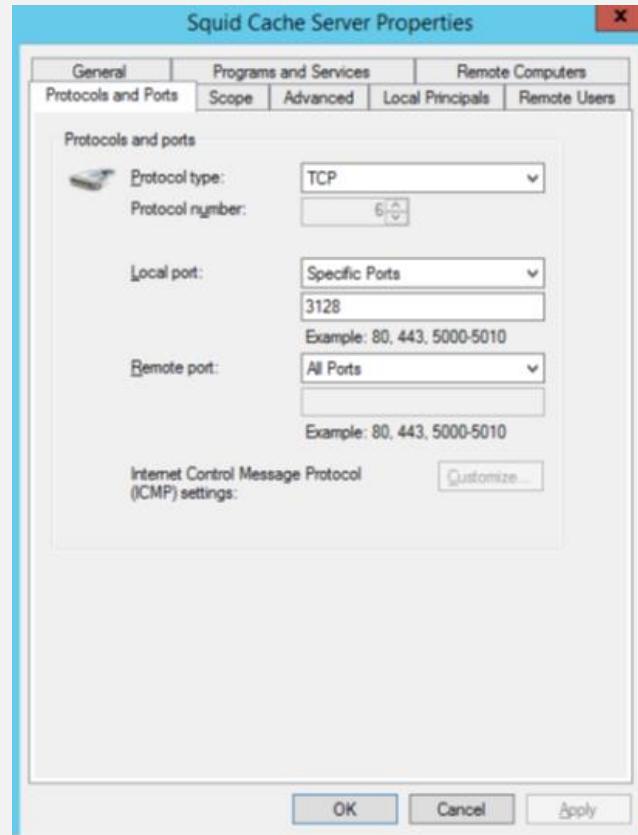
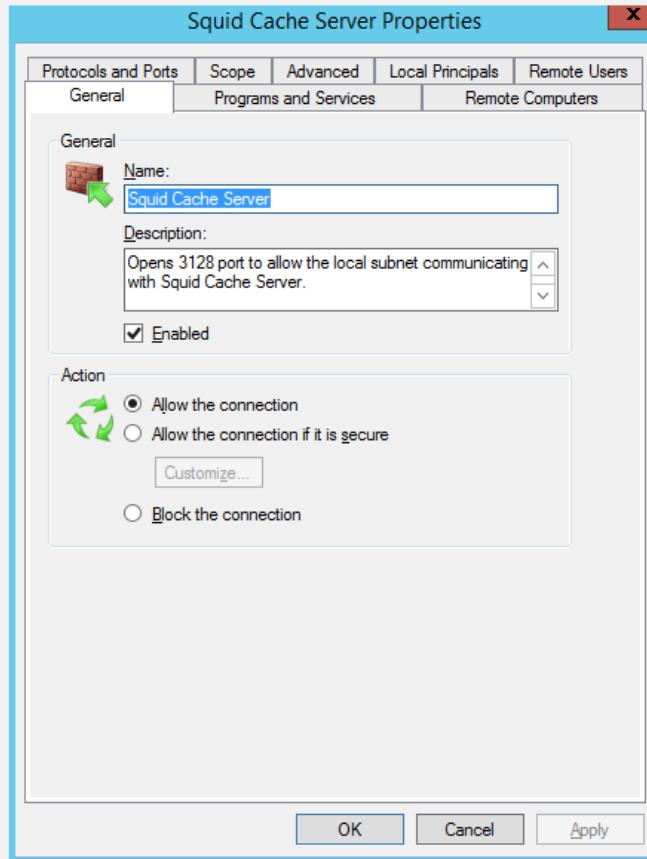


Firewall

- Depois de instalar o squid é aberto o porto 3128 que vai servir para que os clientes se liguem e utilizem este serviço.
- Se algo correr mal na instalação terá de criar esta rule de forma manual.

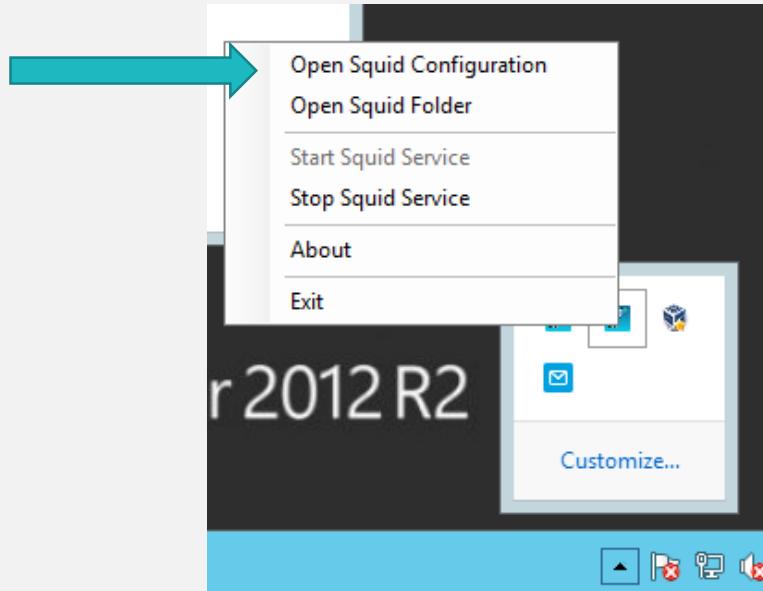


Firewall



Configuração

- Para configurar o squid deve ir a:



```
squid.conf - Notepad
File Edit Format View Help

#
# Recommended minimum configuration:
#
# Example rule allowing access from your local networks.
# Adapt to list your (internal) IP networks from where browsing
# should be allowed

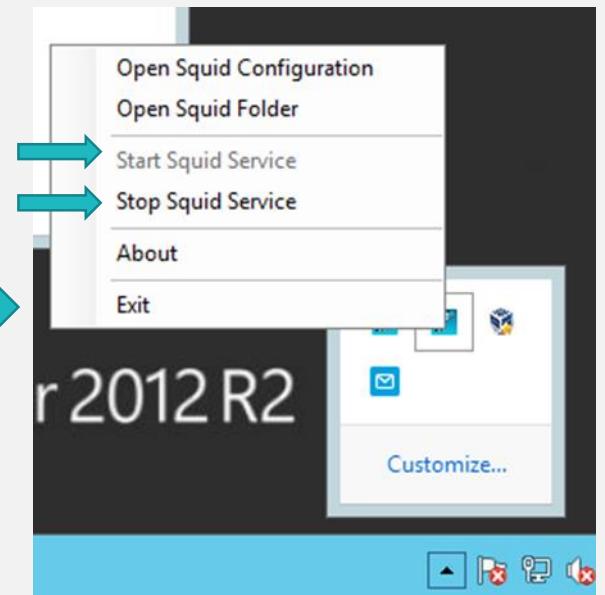
acl localnet src 10.0.0.0/8      # RFC1918 possible internal network
acl localnet src 172.16.0.0/12    # RFC1918 possible internal network
acl localnet src 192.168.0.0/16   # RFC1918 possible internal network
acl localnet src fc00::/7        # RFC 4193 local private network range
acl localnet src fe80::/10       # RFC 4291 link-local (directly plugged) machines

acl SSL_ports port 443
acl Safe_ports port 80          # http
acl Safe_ports port 21          # ftp
acl Safe_ports port 443         # https
acl Safe_ports port 70          # gopher
acl Safe_ports port 210         # wais
acl Safe_ports port 1025-65535  # unregistered ports
acl Safe_ports port 280         # http-mgmt
acl Safe_ports port 488         # gss-http
acl Safe_ports port 591         # filemaker
acl Safe_ports port 777         # multiling http
acl CONNECT method CONNECT

#
# Recommended minimum Access Permission configuration:
#
# Only allow cachemgr access from localhost
http_access allow localhost manager
```

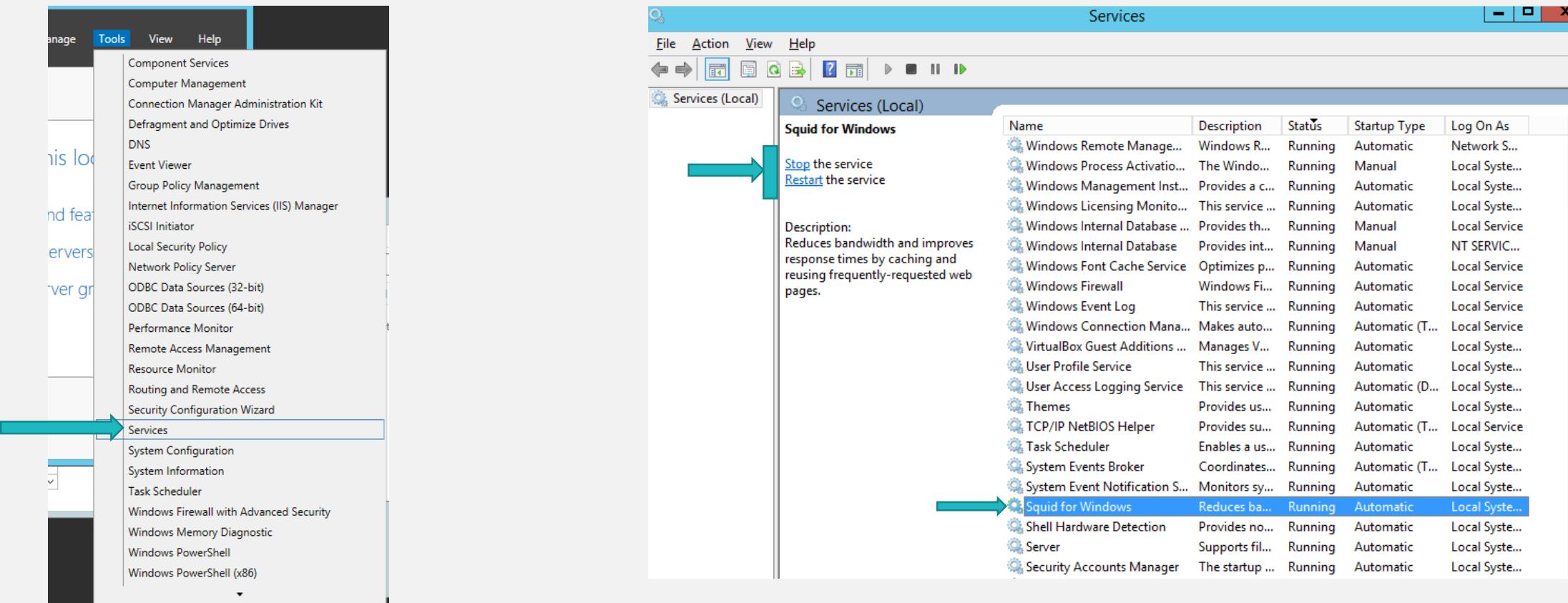
Configuração

- Para alterar as configurações do squid, tem de:
 1. Editar o ficheiro de configuração.
 2. Gravar o ficheiro de configuração.
 3. Fazer *Stop* ao serviço
 4. Fazer *Start* ao serviços
- Quando desejar colocar algum comentários deve começar a linha por #.



Configuração

- Pode também alterar o “estado” do serviço Squid em:



Configuração

- Um dos itens mais importantes do arquivo de configuração squid.conf são as listas de controle de acesso, ou ACLs.
- É possível criar ACLs com padrões diferentes de restrição e de acesso como, por exemplo, liberação e/ou bloqueio de acesso à internet para um determinado computador, rede de computadores ou sites indesejados. Temos assim:
 - **ACLs de origem:** são as regras que definem os IPs que poderão ter acesso ou restrição às regras definidas;
 - **ACLs de destino:** definem qual destino poderá ser ou não acessível. O controlo pode ser por site, para uma rede ou fazendo uso de expressões regulares;
 - **ACLs de horário:** permitem liberar ou bloquear o acesso de acordo com horários definidos nas regras;
 - **ACLs utilizando blacklist:** permite controlar de forma granular o bloqueio de acessos através de palavras específicas;
 - **ACLs utilizando whitelist:** permite controlar de forma granular a liberação de domínios que contenham palavras da blacklist.

Configuração

- O comando é:

acl [*nome*] [*tipo*] [*argumento*]

- Onde:
 - *nome* – é o nome da ACL
 - *tipo* – é o tipo de acl que via ser criada (ver os tipos possíveis no slide seguinte)
 - *argumento* – opções que podem ser adicionadas

Configuração

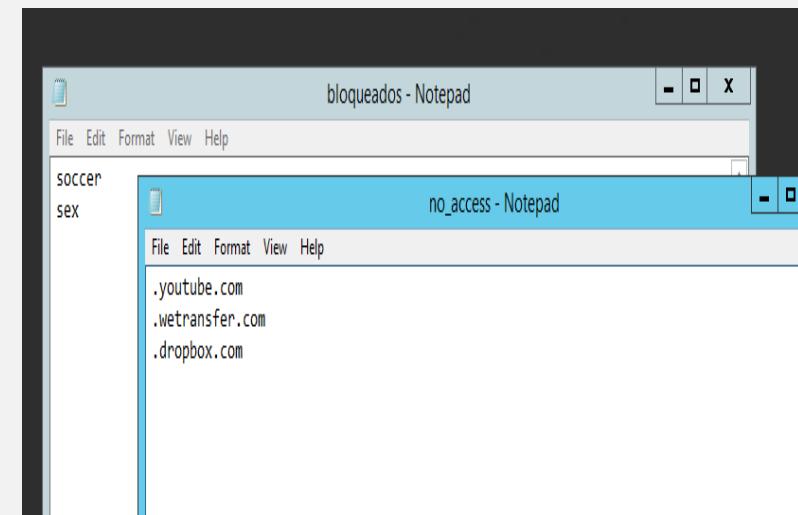
src	Filtro que define a origem dos hosts ou rede que será considerada na ACL
time	Filtro por hora e dia da semana
urlpath_regex	Filtro complementar de uma URL (\.gif, \.jpg).
url_regex	Filtro de uma string na URL
dstdomain	Filtro por domínio
proxy_auth	Filtro por utilizadores autenticados
arp	Filtro por MAC address
maxconn	Filtro por conexões
proto	Filtro por protocolos
port	Filtro por portas de serviço

- Através das ACLs são definidos os tipos controlo que desejamos fazer. Porém, ainda nessa etapa, os pedidos não são tratados, sendo necessário configurar o comando *http_access*.
- Uma vez que as ACLs de origem e destino foram criadas, é necessário definir o que será liberado (*allow*) e/ou o que será bloqueado (*deny*), com o comando:

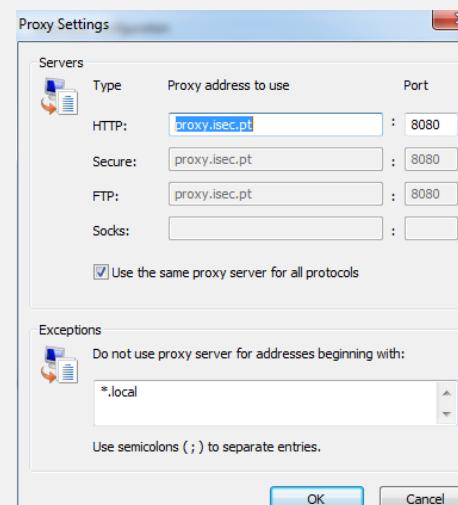
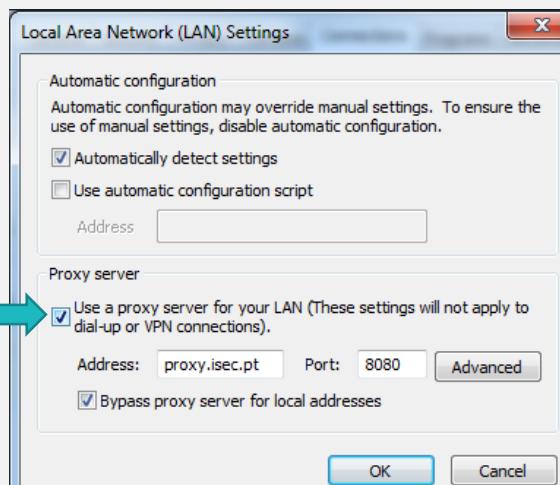
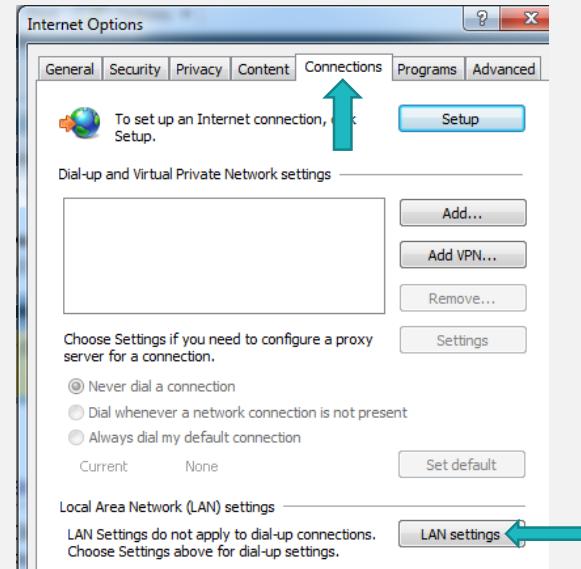
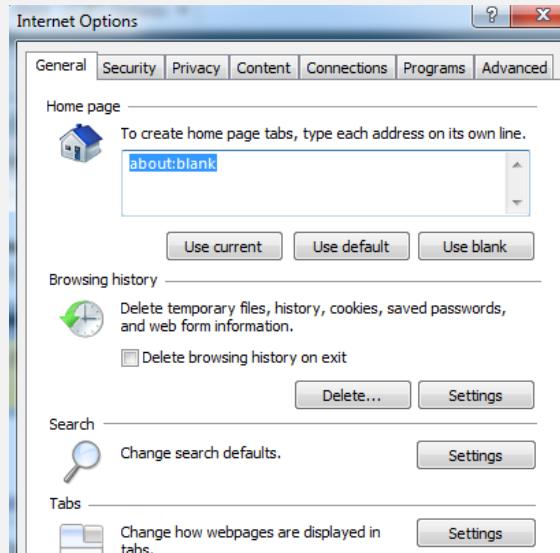
http_access [allow/denny] [nome da ACL]

Configuração

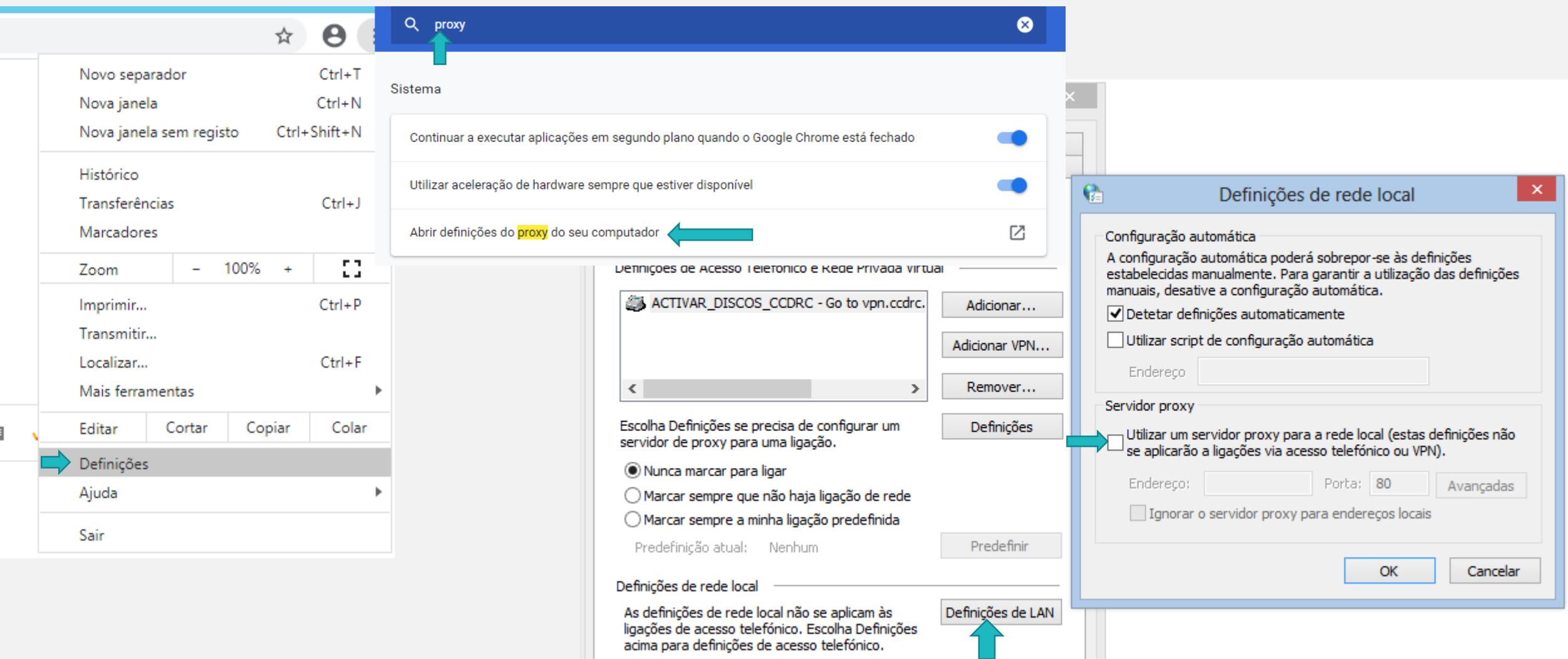
- Exemplos de ACL
 - Bloquear Sites/domínios
 - **acl nome_da_acl dstdomain "caminho/nome do ficheiro"**
 - **http_access deny nome_da_acl**
 - Bloquear palavras em URL
 - **acl nome_da_acl url_regex -i "caminho/nome do ficheiro"**
 - **http_access deny nome_da_acl**



Configuração do cliente (internet explorer)



Configurar do cliente (chrome)



Exercício 2 – Proxy em ambiente Windows – Funções Avançadas

Exercício

- Analise o ficheiro de Logs.
- Apague os logs existentes no ficheiro e acceda à Internet no cliente a:
 - www.isec.pt
 - Facebook.com
 - Youtube.com
 - www.cisco.com
- Veja o que acontece ao ficheiro de log e analise essa informação.
- Coloque no squid como servidor DNS secundário o 1.1.1.1.
Verifique que continua a aceder à Internet.

Exercício

- Converta as mensagens de erro produzidas pelo Squid de Inglês para Português. Teste o acesso a www.sr1.pt e veja o erro. Para além da configuração do squid tem de editar a página de erro para ficar totalmente configurado.



ERROR

O URL solicitado não pôde ser recuperado

O seguinte erro foi encontrado ao tentar recuperar o URL: <http://sr2.pt/>

Incapaz de determinar o endereço IP através do nome do host "sr2.pt"

O servidor DNS retornou:

Name Error: The domain name does not exist.

Isso significa que o cache não conseguiu resolver o nome do host apresentado na URL. Verifique se o endereço está correto.

Envie um mail para [webmaster](#).

Generated Tue, 19 May 2020 16:39:44 GMT by SRV_SR1 (squid/3.5.28)

Exercício

- Coloque o nome visível do servidor Squid como sendo SRV_SR1_2021. Gere um erro (por exemplo acesso a www.sr1.pt) e veja se surge esse nome.

 **ERRO**

O URL solicitado não pôde ser recuperado

O seguinte erro foi encontrado ao tentar recuperar o URL: <http://www.sr1.pt/>

Incapaz de determinar o endereço IP através do nome do host "www.sr1.pt"

O servidor DNS retornou:

 Erro de nome: O nome de domínio não existe.

Isso significa que o cache não foi capaz de resolver o nome do host apresentado na URL. Verifique se o endereço está correto.

Seu administrador de cache é [webmaster](#).

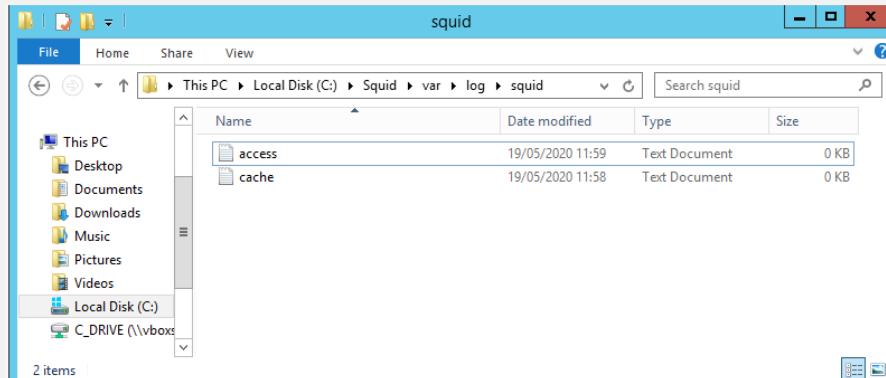
Gerado sex, 21 de maio de 2021 09:07:17 GMT por SRV_SR1_2021 (Iula / 4.14)



How To

Ficheiro de Log

- O Squid guarda por defeito o ficheiro de logs em:



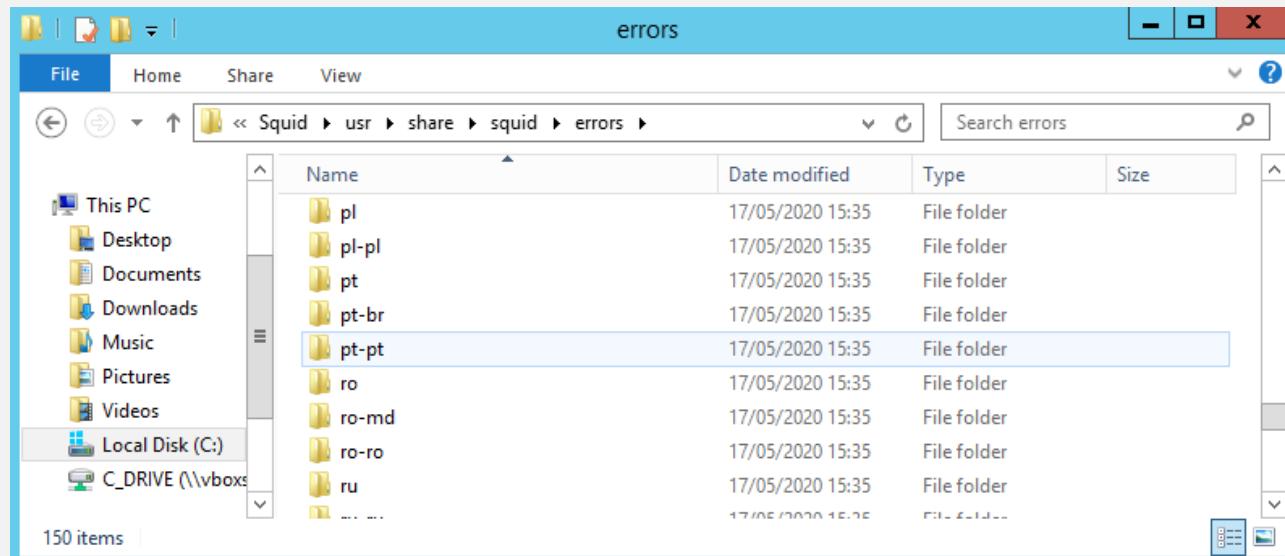
A screenshot of the Windows Notepad application titled 'access - Notepad'. The window contains a large amount of log data. The first few lines of the log are as follows:

```
1589886170.358 2851 192.168.20.1 TCP_MISS/200 45760 GET http://www.ccdrc.pt/ - HIER_DIRECT/83.240.153.217 text/html1589886170.617 3564 192.168.20.1 TCP_TUNNEL/200 3909 CONNECT www.google.com:443 - HIER_DIRECT/216.58.201.164 -1589886172.772 33 192.168.20.1 TCP_MISS/304 248 GET http://www.ccdrc.pt/images/Ano2020/banners/banner_15maio.jpg - HIER_DIRECT/83.240.153.217 -1589886175.544 2848 192.168.20.1 TCP_TUNNEL/200 4606 CONNECT www.google-analytics.com:443 - HIER_DIRECT/216.58.201.142 -1589886175.544 2135 192.168.20.1 TCP_TUNNEL/200 4516 CONNECT stats.doubleclick.net:443 - HIER_DIRECT/173.194.76.156 -1589886175.544 1878 192.168.20.1 TCP_TUNNEL/200 1564 CONNECT www.google.com:443 - HIER_DIRECT/216.58.201.164 -1589886175.544 1656 192.168.20.1 TCP_TUNNEL/200 3951 CONNECT www.google.pt:443 - HIER_DIRECT/216.58.211.35 -1589886198.559 3523 192.168.20.1 TCP_TUNNEL/200 3953 CONNECT clientservices.googleapis.com:443 - HIER_DIRECT/216.58.211.35 -1589886258.827 2915 192.168.20.1 TCP_TUNNEL/200 4691 CONNECT www.google.com:443 - HIER_DIRECT/216.58.201.164 -1589886260.032 34 192.168.20.1 TCP_DENIED/403 3887 CONNECT pt-pt.facebook.com:443 - HIER_NONE/- text/html1589886261.448 29 192.168.20.1 TCP_DENIED/403 3887 CONNECT pt-pt.facebook.com:443 - HIER_NONE/- text/html1589886261.792 0 192.168.20.1 TCP_DENIED/403 3887 CONNECT pt-pt.facebook.com:443 - HIER_NONE/- text/html1589886261.792 0 192.168.20.1 TCP_DENIED/403 3887 CONNECT pt-pt.facebook.com:443 - HIER_NONE/- text/html1589886261.849 3466 192.168.20.1 TCP_TUNNEL/200 8132 CONNECT www.google.com:443 - HIER_DIRECT/216.58.201.164 -1589886262.849 2817 192.168.20.1 TCP_TUNNEL/200 2580 CONNECT static.xx.fbcdn.net:443 - HIER_DIRECT/31.13.83.4 -1589886266.149 0 192.168.20.1 TCP_DENIED/403 3887 CONNECT pt-pt.facebook.com:443 - HIER_NONE/- text/html1589886271.545 5395 192.168.20.1 TCP_TUNNEL/200 482 CONNECT static.xx.fbcdn.net:443 - HIER_DIRECT/31.13.83.4 -1589886279.438 0 192.168.20.1 TCP_DENIED/403 3878 CONNECT www.youtube.com:443 - HIER_NONE/- text/html1589886279.472 17 192.168.20.1 TCP_DENIED/403 3878 CONNECT www.youtube.com:443 - HIER_NONE/- text/html1589886281.115 500 192.168.20.1 TCP_DENIED/403 3878 CONNECT www.youtube.com:443 - HIER_NONE/- text/html1589886281.115 4949 192.168.20.1 TCP_TUNNEL/200 4206 CONNECT www.google.com:443 - HIER_DIRECT/216.58.201.164 -1589886281.115 3338 192.168.20.1 TCP_TUNNEL/200 5284 CONNECT encrypted.tbn0.gstatic.com:443 - HIER_DIRECT/172.217.16.238 1678 192.168.20.1 TCP_TUNNEL/200 3522 CONNECT fonts.googleapis.com:443 - HIER_DIRECT/216.58.201.164 6894 192.168.20.1 TCP_TUNNEL/200 6076 CONNECT safefrowsing.googleapis.com:443 - HIER_DIRECT/172.217.171.234 -1589886291.641 386 192.168.20.1 TCP_TUNNEL/200 6368 CONNECT www.static-cisco.com:443 - HIER_DIRECT/104.126.97.17 -1589886291.641 386 192.168.20.1 TCP_TUNNEL/200 3099 CONNECT s.go-mpulse.net:443 - HIER_DIRECT/2.21.168.81 -1589886297.338 5265 192.168.20.1 TCP_TUNNEL/200 5273 CONNECT cdn.cookielaw.org:443 - HIER_DIRECT/152.21.175 -1589886297.338 5264 192.168.20.1 TCP_TUNNEL/200 6143 CONNECT tags.tiicdn.com:443 - HIER_DIRECT/152.199.23.241 -1589886297.338 2955 192.168.20.1 TCP_TUNNEL/200 5533 CONNECT cdn.cookielaw.org:443 - HIER_DIRECT/152.199.21.175 -1589886297.338 2192 192.168.20.1 TCP_TUNNEL/200 7313 CONNECT pps.cisco.com:443 - HIER_DIRECT/173.37.149.105 -1589886297.338 2157 192.168.20.1 TCP_TUNNEL/200 8857 CONNECT cdvcdps.cisco.com:443 - HIER_DIRECT/104.20.185.65 -1589886303.024 3905 192.168.20.1 TCP_TUNNEL/200 6755 CONNECT mcc-tags.cisco.com:443 - HIER_DIRECT/72.163.10.15 -1589886303.211 8862 192.168.20.1 TCP_TUNNEL/200 4462 CONNECT c.go-mpulse.net:443 - HIER_DIRECT/2.21.168.81 -1589886303.211 1131 192.168.20.1 TCP_TUNNEL/200 3470 CONNECT trial-eum-clientnts-s.akamaidh.net:443 - HIER_DIRECT/95.136.31.39 -1589886303.211 1129 192.168.20.1 TCP_TUNNEL/200 3473 CONNECT trial-eum-clientnts-s.akamaidh.net:443 - HIER_DIRECT/95.136.31.39 -1589886303.211 777 192.168.20.1 TCP_TUNNEL/200 3537 CONNECT 94-61-232-45_5-95-136-31-39_ts-1589886309-clientnts-s.akamaidh.net:443 - HIER_DIRECT/95.136.31.39 -1589886457.150 902 192.168.20.1 TCP_TUNNEL/200 3911 CONNECT www.google.com:443 - HIER_DIRECT/216.58.201.164 -1589886462.094 1341 192.168.20.1 TCP_TUNNEL/200 4741 CONNECT www.google.com:443 - HIER_DIRECT/216.58.201.164 -1589886465.128 1010 192.168.20.1 TCP_MISS/301 423 GET http://www.iiscpt.pt/ - HIER_DIRECT/199.78.72 text/html1589886466.682 4417 192.168.20.1 TCP_TUNNEL/200 5514 CONNECT www.google.com:443 - HIER_DIRECT/216.58.201.164 -1589886466.682 2629 192.168.20.1 TCP_TUNNEL/200 3484 CONNECT 6852bd07.aksstat.io:443 - HIER_DIRECT/2.21.168.81 -1589886475.247 5368 192.168.20.1 TCP_TUNNEL/200 2715 CONNECT fonts.gstatic.com:443 - HIER_DIRECT/216.58.211.227 -1589886475.247 9014
```

- Pode alterar esta localização no ficheiro de configuração.
- Para poder apagar o conteúdo do ficheiro terá de ter o serviço squid parado.

Páginas de erro

- As páginas de erro estão em:



Name	Date modified	Type	Size
ERR_ACCESS_DENIED	08/08/2018 08:01	File	2 KB
ERR_ACL_TIME_QUOTA_EXCEEDED	08/08/2018 08:01	File	2 KB
ERR_AGENT_CONFIGURE	08/08/2018 08:01	File	2 KB
ERR_AGENT_WPAP	08/08/2018 08:01	File	2 KB
ERR_CACHE_ACCESS_DENIED	08/08/2018 08:01	File	2 KB
ERR_CACHE_MGR_ACCESS_DENIED	08/08/2018 08:01	File	2 KB
ERR_CANNOT_FORWARD	08/08/2018 08:01	File	2 KB
ERR_CONFLICT_HOST	08/08/2018 08:01	File	2 KB
ERR_CONNECT_FAIL	19/05/2020 15:07	File	2 KB
ERR_DIR_LISTING	08/08/2018 08:01	File	1 KB
ERR_DNS_FAIL	19/05/2020 15:05	File	2 KB
ERR_ESI	08/08/2018 08:01	File	2 KB
ERR_FORWARDING_DENIED	08/08/2018 08:01	File	2 KB
ERR_FTP_DISABLED	08/08/2018 08:01	File	1 KB
ERR_FTP_FAILURE	08/08/2018 08:01	File	1 KB
ERR_FTP_FORBIDDEN	08/08/2018 08:01	File	2 KB
ERR_FTP_NOT_FOUND	08/08/2018 08:01	File	2 KB
ERR_FTP_PUT_CREATED	08/08/2018 08:01	File	1 KB
ERR_FTP_PUT_ERROR	08/08/2018 08:01	File	2 KB
ERR_FTP_PUT_MODIFIED	08/08/2018 08:01	File	1 KB
ERR_FTP_UNAVAILABLE	08/08/2018 08:01	File	1 KB
ERR_GATEWAY_FAILURE	08/08/2018 08:01	File	2 KB
ERR_ICAP_FAILURE	08/08/2018 08:01	File	2 KB
ERR_INVALID_REQ	08/08/2018 08:01	File	2 KB
ERR_INVALID_RESP	08/08/2018 08:01	File	2 KB
ERR_INVALID_URL	08/08/2018 08:01	File	2 KB

- Configurações adicionais:

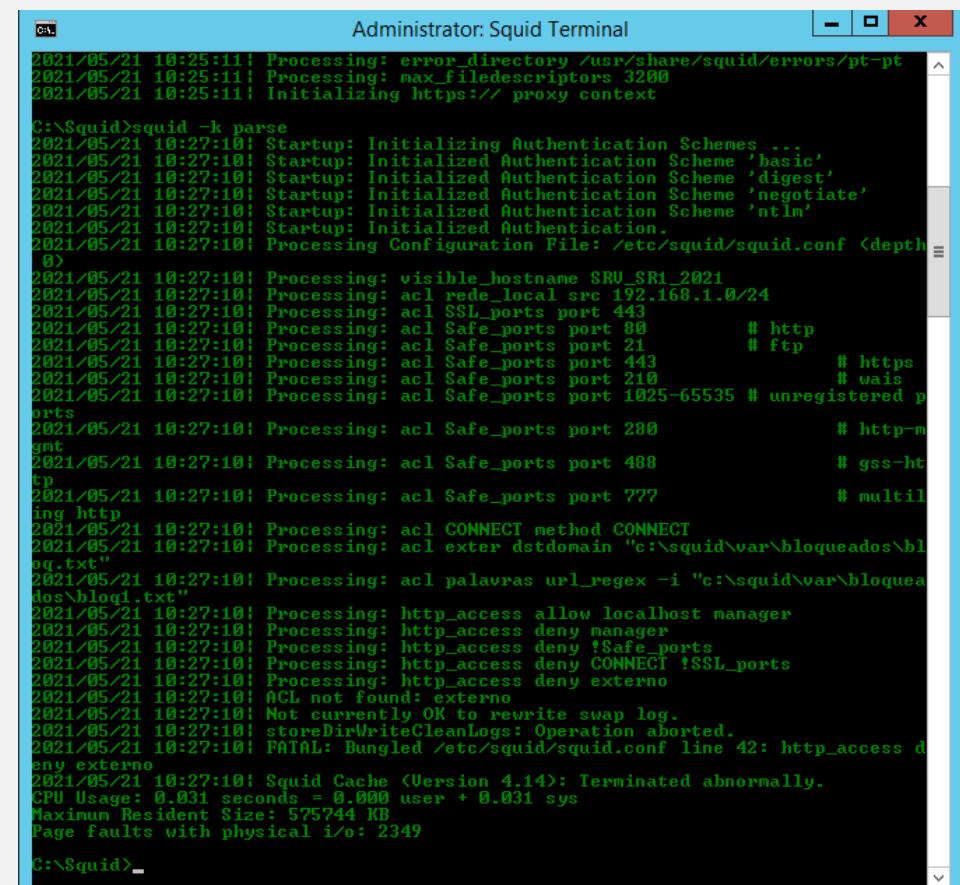
```
# Ficheiro de configuração aula 10  
  
#Mostra o nome do servidor  
  
visible_hostname SRV_SR1
```

```
#Servidores de DNS  
  
dns_nameservers 8.8.8.8 1.1.1.1  
  
#Converte as mensagens de erro para Português  
error_directory /usr/share/squid/errors/pt-pt
```

Exercício 3 – Squid configuração avançada

Exercício

- Na acl que criou no exercício anterior mude o seu nome para extern. Faça um restart aos serviços do squid e veja o que acontece. Deve estar sem acesso à rede.
- Pela janela do terminal identifique qual a linha em que está a ocorrer o erro.
- Faça a correção do erro e verifique que está tudo a correr como tinha configurado.
- Ainda na janela do terminal identifique qual é a versão do SQUID que está a utilizar.
- Veja os seus ficheiros de logs... Devem ter crescido de forma muito significativa. Apague os logs dos acessos.



```
Administrator: Squid Terminal
C:\>Administrator: Squid Terminal
2021/05/21 10:25:11: Processing: error_directory /usr/share/squid/errors/pt-pt
2021/05/21 10:25:11: Processing: max_filedescriptors 3200
2021/05/21 10:25:11: Initializing https:// proxy context

C:\>Squid>squid -k parse
2021/05/21 10:27:10: Startup: Initializing Authentication Schemes ...
2021/05/21 10:27:10: Startup: Initialized Authentication Scheme 'basic'
2021/05/21 10:27:10: Startup: Initialized Authentication Scheme 'digest'
2021/05/21 10:27:10: Startup: Initialized Authentication Scheme 'negotiate'
2021/05/21 10:27:10: Startup: Initialized Authentication Scheme 'ntlm'
2021/05/21 10:27:10: Startup: Initialized Authentication.
2021/05/21 10:27:10: Processing Configuration File: /etc/squid/squid.conf <depth 0>
2021/05/21 10:27:10: Processing: visible_hostname SRV_SR1_2021
2021/05/21 10:27:10: Processing: acl rede_local src 192.168.1.0/24
2021/05/21 10:27:10: Processing: acl SSL_ports port 443
2021/05/21 10:27:10: Processing: acl Safe_ports port 80 # http
2021/05/21 10:27:10: Processing: acl Safe_ports port 21 # ftp
2021/05/21 10:27:10: Processing: acl Safe_ports port 443 # https
2021/05/21 10:27:10: Processing: acl Safe_ports port 210 # wais
2021/05/21 10:27:10: Processing: acl Safe_ports port 1025-65535 # unregistered ports
2021/05/21 10:27:10: Processing: acl Safe_ports port 280 # http-mgmt
2021/05/21 10:27:10: Processing: acl Safe_ports port 488 # gss-ht
2021/05/21 10:27:10: Processing: acl Safe_ports port 777 # multiling http
2021/05/21 10:27:10: Processing: acl CONNECT method CONNECT
2021/05/21 10:27:10: Processing: acl exter dstdomain "c:\squid\var\bloqueados\bloq.txt"
2021/05/21 10:27:10: Processing: acl palavras url_regex -i "c:\squid\var\bloqueados\bloq1.txt"
2021/05/21 10:27:10: Processing: http_access allow localhost manager
2021/05/21 10:27:10: Processing: http_access deny !Safe_ports
2021/05/21 10:27:10: Processing: http_access deny CONNECT !SSL_ports
2021/05/21 10:27:10: Processing: http_access deny externo
2021/05/21 10:27:10: ACL not found: externo
2021/05/21 10:27:10: Not currently OK to rewrite swap log.
2021/05/21 10:27:10: storeDirWriteCleanLogs: Operation aborted.
2021/05/21 10:27:10: FATAL: Bungled /etc/squid/squid.conf line 42: http_access deny externo
2021/05/21 10:27:10: Squid Cache (Version 4.14): Terminated abnormally.
CPU Usage: 0.031 seconds = 0.000 user + 0.031 sys
Maximum Resident Size: 575744 KB
Page Faults with physical i/o: 2349
C:\>Squid>
```

Exercício

- Em squid/var/cache crie uma nova diretoria chamada SR1. Esta diretoria servirá para guardar os ficheiros da função de cache do seu servidor.
- Deve ativar a função cache com as seguintes caraterísticas:
 - Diretoria /var/cache/sr1
 - Tipo - UFS
 - 512MB de espaço, 128 diretórios e 256 subdiretórios
- Proceda à criação desta função.
- Valide na diretoria SR1 que foram criadas todas as pastas conforme estava definido no comando.

How To

- Como a configuração do SQUID é feita no ficheiro squid.conf por vezes não é fácil diagnosticar um erro. Uma hipótese é o comando **squid -k parse** na **janela de terminal** do squid e analisar os erros.



- Pode saber os comandos que tem disponíveis, deve utilizar o comando **squid - v**.

- **cache.log**
 - Este arquivo contém mensagens informativas, formatadas para o ser humano, sobre a operação do Squid. O nome do arquivo é definido pelo comando `cache_log`. Em condições normais, o ficheiro aumenta cerca de 10 a 100 KB por dia.
- **access.log**
 - Este arquivo contém uma entrada para todas as transações HTTP e (opcionalmente) ICP feitas pelos clientes do Squid. O nome do arquivo é definido pelo comando `cache_access_log`. Em condições normais o ficheiro cresce a uma taxa de 100-200 bytes por transação.

- Para ativar a função de cache deve utilizar o comando no ficheiro de configuração:
 - **cache_dir** [tipo] [caminho] [*tamanho em disco*] [*número de diretórios*] [*número de subdiretórios*]
- Deve depois correr o comando **squid -k parse** na **janela de terminal** do squid e analisar os possíveis erros.
- Depois deve correr o comando **squid -z** para que o programa crie na diretoria definida para a cache as diretórias de *swap*. Só necessita de o fazer na primeira vez que está a ativar a função de cache.

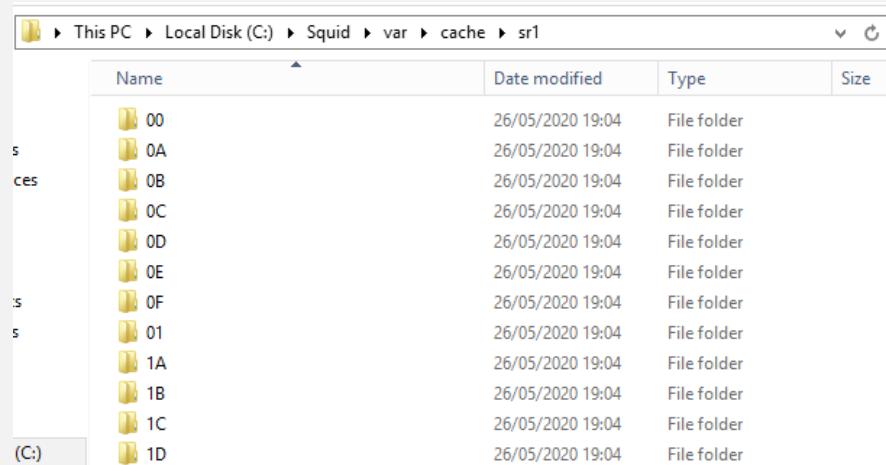
- Pode validar no ficheiro de logs a criação destas diretórias.

```

cache - Notepad
File Edit Format View Help
/var/cache/sr1/112020/05/26 19:04:43 kid1| Making directories in /var/cache/sr1/122020/05/26 19:04:43 kid1| Making directories in
/var/cache/sr1/132020/05/26 19:04:43 kid1| Making directories in /var/cache/sr1/142020/05/26 19:04:43 kid1| Making directories in
/var/cache/sr1/152020/05/26 19:04:44 kid1| Making directories in /var/cache/sr1/162020/05/26 19:04:44 kid1| Making directories in
/var/cache/sr1/172020/05/26 19:04:44 kid1| Making directories in /var/cache/sr1/182020/05/26 19:04:44 kid1| Making directories in
/var/cache/sr1/192020/05/26 19:04:44 kid1| Making directories in /var/cache/sr1/1A2020/05/26 19:04:44 kid1| Making directories in
/var/cache/sr1/1B2020/05/26 19:04:44 kid1| Making directories in /var/cache/sr1/1C2020/05/26 19:04:44 kid1| Making directories in
/var/cache/sr1/1D2020/05/26 19:04:44 kid1| Making directories in /var/cache/sr1/1E2020/05/26 19:04:44 kid1| Making directories in
/var/cache/sr1/1F2020/05/26 19:04:44 kid1| Making directories in /var/cache/sr1/202020/05/26 19:04:44 kid1| Making directories in
/var/cache/sr1/212020/05/26 19:04:45 kid1| Making directories in /var/cache/sr1/222020/05/26 19:04:45 kid1| Making directories in
/var/cache/sr1/232020/05/26 19:04:45 kid1| Making directories in /var/cache/sr1/242020/05/26 19:04:45 kid1| Making directories in
/var/cache/sr1/252020/05/26 19:04:45 kid1| Making directories in /var/cache/sr1/262020/05/26 19:04:45 kid1| Making directories in
/var/cache/sr1/272020/05/26 19:04:45 kid1| Making directories in /var/cache/sr1/282020/05/26 19:04:45 kid1| Making directories in
/var/cache/sr1/292020/05/26 19:04:45 kid1| Making directories in /var/cache/sr1/2A2020/05/26 19:04:45 kid1| Making directories in
/var/cache/sr1/2B2020/05/26 19:04:46 kid1| Making directories in /var/cache/sr1/2C2020/05/26 19:04:46 kid1| Making directories in
/var/cache/sr1/2D2020/05/26 19:04:46 kid1| Making directories in /var/cache/sr1/2E2020/05/26 19:04:46 kid1| Making directories in
/var/cache/sr1/2F2020/05/26 19:04:46 kid1| Making directories in /var/cache/sr1/302020/05/26 19:04:46 kid1| Making directories in
/var/cache/sr1/312020/05/26 19:04:46 kid1| Making directories in /var/cache/sr1/322020/05/26 19:04:46 kid1| Making directories in
/var/cache/sr1/332020/05/26 19:04:46 kid1| Making directories in /var/cache/sr1/342020/05/26 19:04:46 kid1| Making directories in
/var/cache/sr1/352020/05/26 19:04:46 kid1| Making directories in /var/cache/sr1/362020/05/26 19:04:47 kid1| Making directories in
/var/cache/sr1/372020/05/26 19:04:47 kid1| Making directories in /var/cache/sr1/382020/05/26 19:04:47 kid1| Making directories in
/var/cache/sr1/392020/05/26 19:04:47 kid1| Making directories in /var/cache/sr1/3A2020/05/26 19:04:47 kid1| Making directories in

```

- Ou validar a sua criação com o explorador do Windows.



Dúvidas



Referências

- <https://www.youtube.com/watch?v=32LcFAriMZ0&t=18s> – Acedido em maio de 2022
- <https://www.youtube.com/watch?v=HnFuxFP9wCo> – Acedido em Maio de 2022
- <https://www.thegeekstuff.com/2010/09/squid-control-internet-access/> – Acedido em maio de 2022
- <http://www.squid-cache.org/> - Acedido em maio de 2023

Serviços de Rede 1 – **Aula 11 - Práticas**

2022-2023

Instituto Politécnico de Coimbra

Departamento de Engenharia Informática



Nota Importante

- Dia 14 e 15 de junho será realizado o 3º teste prático.
 - Peso – 3 valores em 20.
 - Matéria:
 - NTP (aula 9)
 - Proxy (aula 10)
 - VPN (aula 11)
- Inscrição obrigatória no Moodle.
- Devem ter instalado o Virtual Box 6.0 e o Cisco Packet Tracer na versão mínima versão 8.2.0
- Devem antecipadamente importar para o VirtualBox as imagens do Windows Server 2012 e do Windows 8/10 “limpas”.
- Devem ter no servidor os ficheiros de instalação dos programas Squid, The Meinberg NTP e NTP Time Server Monitor nas versões dadas nas aulas práticas.
- Devem ter funcional as topologias indicadas na notificação desta semana.

Pre – Requisitos

- Ter instalado o *Cisco Packet Tracer* versão 8.2.0



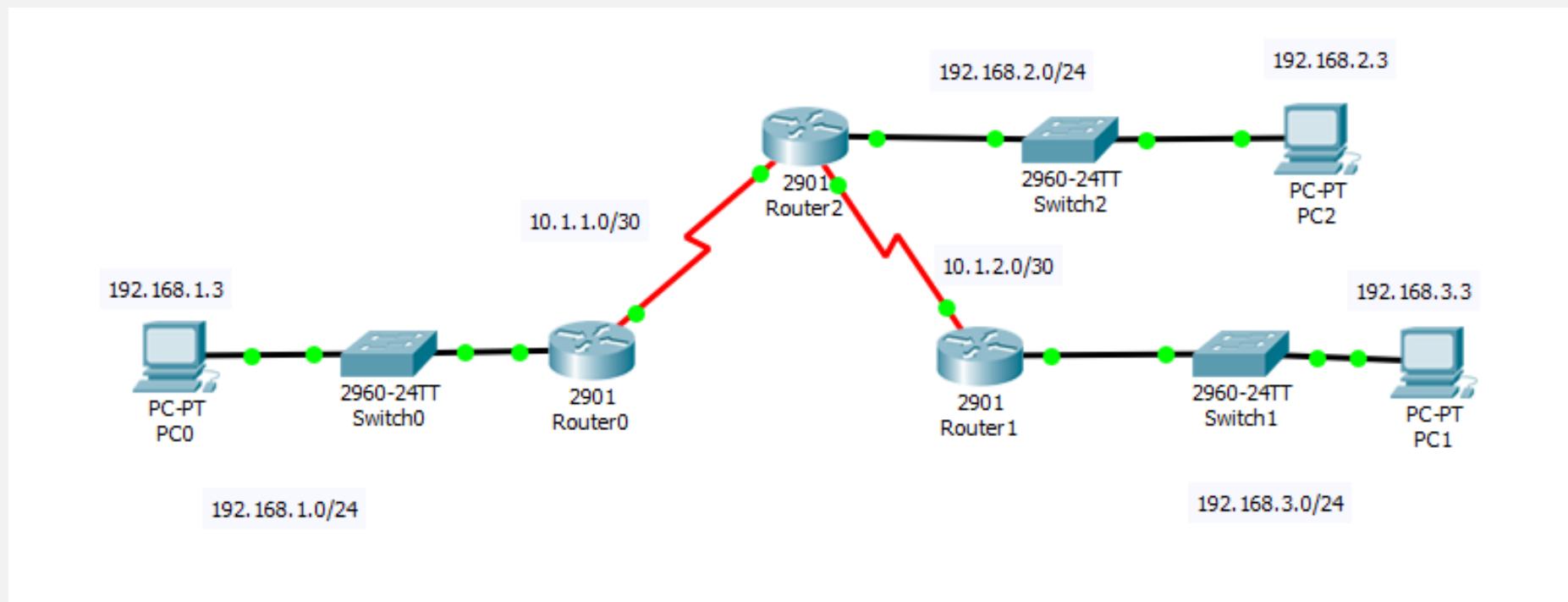
Exercício 1 - VPN com túnel GRE em ambiente Cisco

Exercício

A empresa SR1.SA necessita de ligar a rede da sede (192.168.1.0) à rede da delegação (192.168.3.0) utilizando a ligação de telecomunicações já instalada.

Numa primeira fase a empresa deseja que essa ligação seja feita sobre um túnel GRE.

Considere a seguinte topologia:



Exercício

- Faça a topologia indicada na imagem anterior. Grave a simulação como VPN_GRE.
- Coloque os endereços IP dos diferentes equipamentos de forma fixa e de acordo com as redes indicadas na imagem.
- Garanta que o PC0 e o PC1 conseguem ter conectividade para o PC2.
- Crie uma VPN entre os Routers 0 e 1 baseado num túnel GRE. O IP do túnel será a rede 50.50.50.0/24.
- Faça o ***tracert*** do PC0 para o PC1 e vice-versa.

```
C:\>tracert 192.168.3.3

Tracing route to 192.168.3.3 over a maximum of 30 hops:
  1  2 ms      0 ms      0 ms      192.168.1.254
  2  14 ms     12 ms     15 ms    50.50.50.2
  3  12 ms     13 ms     14 ms    192.168.3.3

Trace complete.
```

```
C:\>tracert 192.168.1.3

Tracing route to 192.168.1.3 over a maximum of 30 hops:
  1  1 ms      2 ms      0 ms      192.168.3.254
  2  14 ms     14 ms     14 ms    50.50.50.1
  3  16 ms     12 ms     11 ms    192.168.1.3

Trace complete.
```

How To

- É possível que tenha de ativar *Security Technology Package license* em alguns routers. Para isso:
 - Faça **show version** em modo *Enable*:

Technology	Technology-package		Technology-package Next reboot
	Current	Type	
ipbase	ipbasek9	Permanent	ipbasek9
security	None	None	None
uc	None	None	None
data	None	None	None

É necessário



Technology	Technology-package		Technology-package Next reboot
	Current	Type	
apxxk9	None	None	None
uck9	None	None	None
securityk9	securityk9	Permanent	securityk9
ipbase	ipbasek9	Permanent	ipbasek9
security	securityk9	Permanent	securityk9
ipbase	ipbasek9	Permanent	ipbasek9

cisco ISR4331/K9 (1RU) processor with 1795999K/6147K bytes of memory.
Processor board ID FLM232010G0

Não é necessário

- Pode não estar instalada a licença.
- Entre em modo de configuração e faça:
license boot module cXXXX technology-package securityk9

- Grave a configuração.
- Faça ***reload***.
- Faça ***show version*** e já deve ter ativada *Security Technology Package license*.

```
Technology Package License Information for Module:'c2900'
```

Technology	Technology-package	Technology-package	
Current	Type	Next reboot	
<hr/>			
ipbase	ipbasek9	Permanent	ipbasek9
security	securityk9	Evaluation	securityk9
uc	None	None	None
data	None	None	None

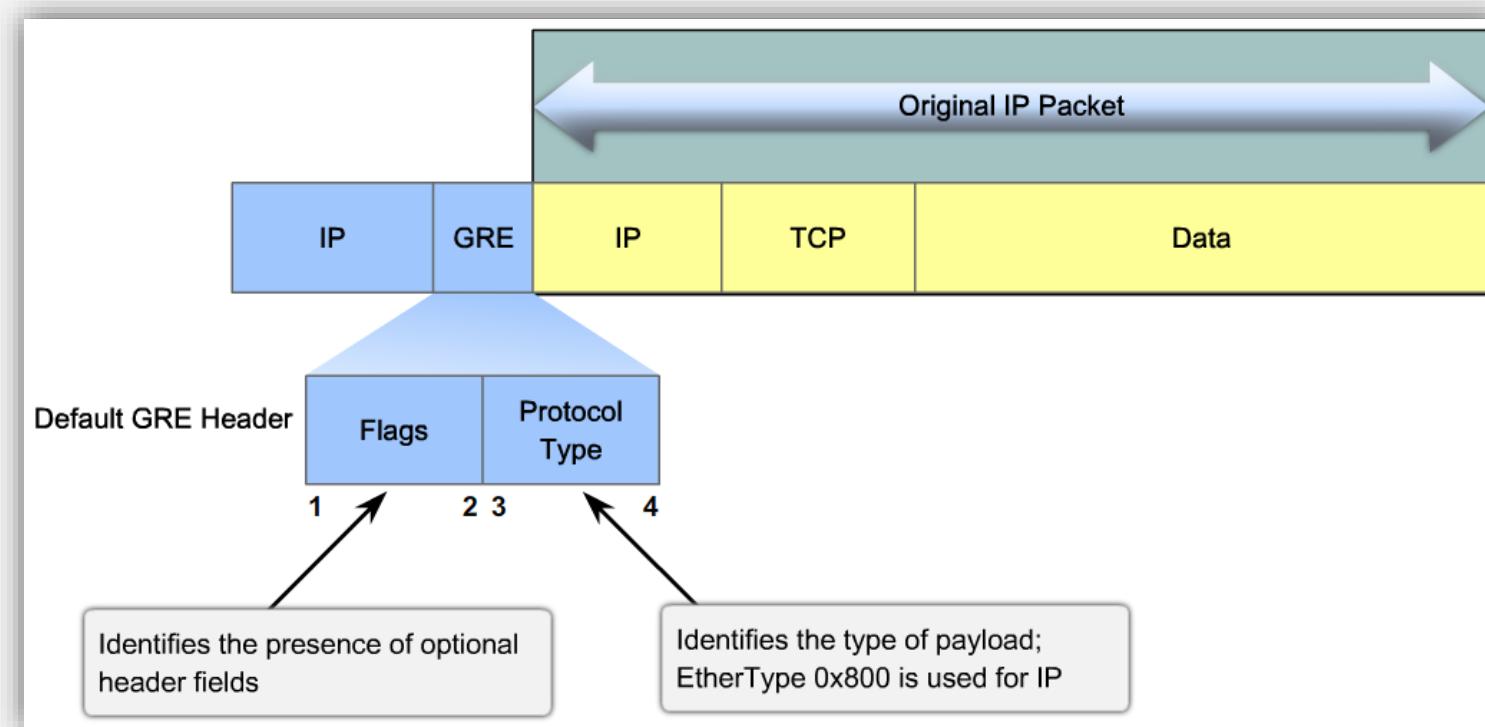


Tunneling

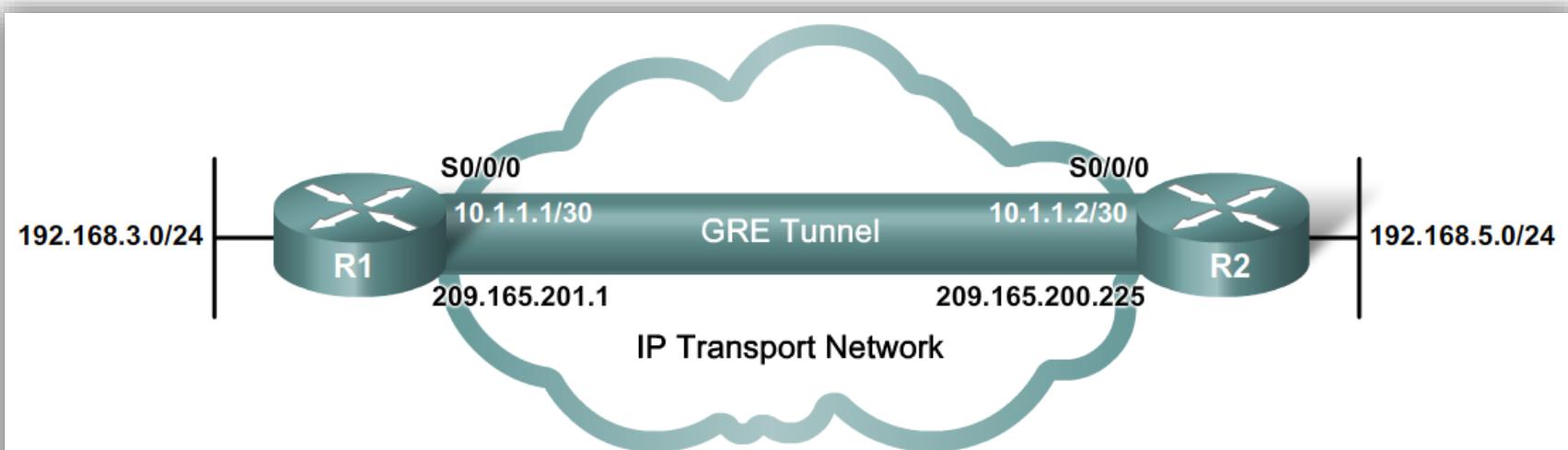
- Para que um túnel seja estabelecido é necessário que o servidor e o cliente utilizem o mesmo protocolo.
- Para o estabelecimento do túnel, são necessárias duas fases:
 - **Estabelecimento do túnel**
 - Negociação de variáveis, endereço, encriptação e compressão.
 - **Transmissão**
 - Encapsulamento e encriptação.
 - Envio.
 - Desencapsulamento e desencriptação.

GRE - Generic Routing Encapsulation

- Os pacotes IP são encapsulados num pacote GRE
 - *Implica um* payload adicional de, pelo menos, 24 bytes



GRE - Configuração



```
R1(config)# interface tunnel 0
R1(config-if)# ip address 10.1.1.1 255.255.255.252
R1(config-if)# tunnel source serial 0/0/0
R1(config-if)# tunnel destination 209.165.200.225
R1(config-if)# tunnel mode gre ip
R1(config-if)#

```

```
R2(config)# interface tunnel 0
R2(config-if)# ip address 10.1.1.2 255.255.255.252
R2(config-if)# tunnel source serial 0/0/0
R2(config-if)# tunnel destination 209.165.201.1
R2(config-if)# tunnel mode gre ip
R2(config-if)#

```

GRE tunnel is up and the protocol is up if:

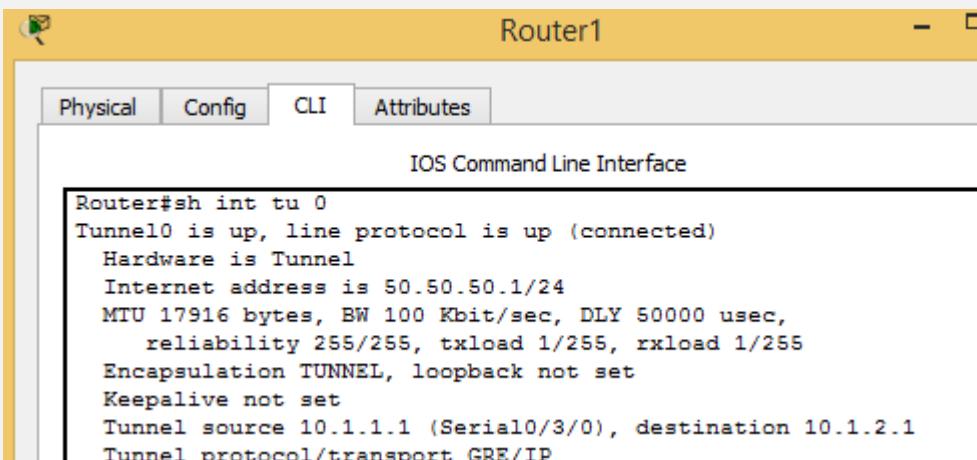
- Tunnel source and destination are configured
- Tunnel destination is in routing table
- GRE keepalives are received (if used)
- GRE is the default tunnel mode

GRE - Configuração

- Não se esqueça de fazer as rotas necessárias.

```
10.0.0.0/8 is variably subnetted, 3 subnets, 2 masks
C   10.1.1.0/30 is directly connected, Serial0/3/0
L   10.1.1.1/32 is directly connected, Serial0/3/0
S   10.1.2.0/30 is directly connected, Serial0/3/0
      50.0.0.0/8 is variably subnetted, 2 subnets, 2 masks
C   50.50.50.0/24 is directly connected, Tunnel0
L   50.50.50.1/32 is directly connected, Tunnel0
      192.168.1.0/24 is variably subnetted, 2 subnets, 2 masks
C   192.168.1.0/24 is directly connected, GigabitEthernet0/0
L   192.168.1.254/32 is directly connected,
      GigabitEthernet0/0
S   192.168.2.0/24 is directly connected, Serial0/3/0
S   192.168.3.0/24 [1/0] via 50.50.50.2
```

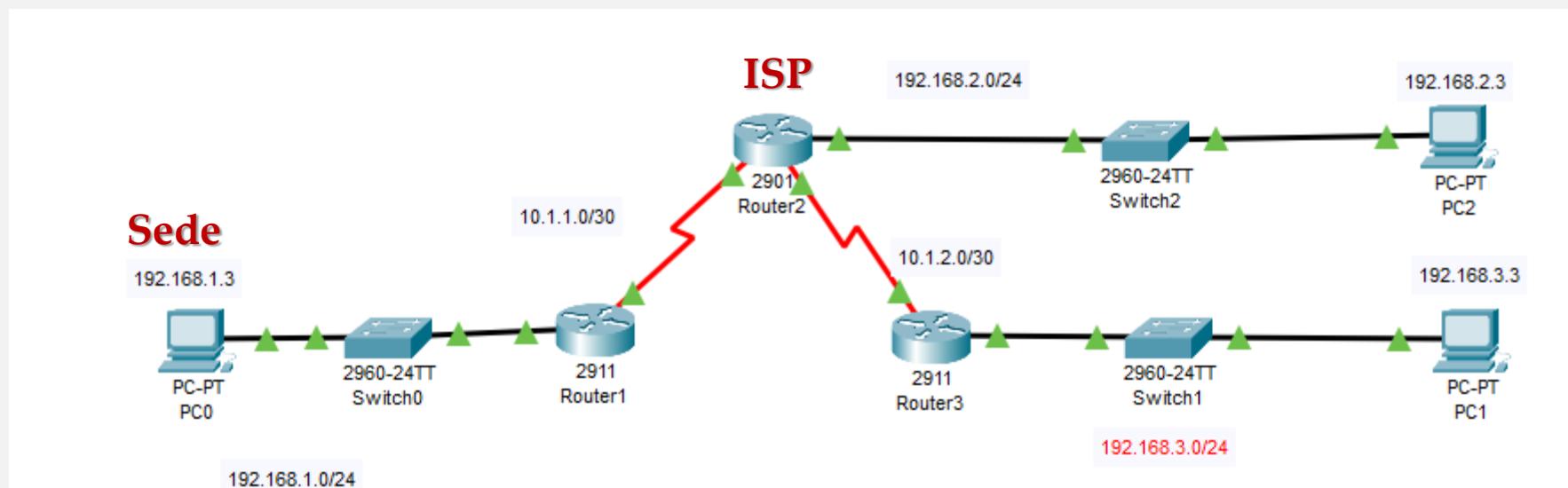
- Deve verificar se a sua interface está *up*



Exercício 2 - VPN IPSec em ambiente Cisco

Exercício

- A empresa SR1.SA, deseja ligar a sede (192.168.1.0/24) a uma delegação localizada em Londres (192.168.3.0/24). Para tal deseja utilizar um túnel seguro. Decidiu utilizar o IPSec para fazer essa ligação entre a sede e a delegação.
- A topologia é idêntica ao anterior exercício:



Exercício

- Grave a simulação como VPN_IPSEC.
- Retire a informação referente ao túnel GRE.
- Retire as rotas que tinha do exercício anterior no router 1 e router 3.
- Desabilite o “*IP Domain Name System hostname translation*”
- Coloque apenas uma rota por defeito no router 1 e router 3.
- Tente pingar do PC0 para o PC2.
- Tente pingar do PC0 para o PC1. Não deve conseguir...

Exercício

- Crie uma VPN entre o R1 e R3 com as seguintes definições:

Parâmetros da ISAKMP Phase 1

Parameters		R1	R3
Key distribution method	Manual or ISAKMP	ISAKMP	ISAKMP
Encryption algorithm	DES , 3DES, or AES	AES	AES
Hash algorithm	MD5 or SHA-1	SHA-1	SHA-1
Authentication method	Pre-shared keys or RSA	pre-share	pre-share
Key exchange	DH Group 1 , 2, or 5	DH 2	DH 2
IKE SA Lifetime	86400 seconds or less	86400	86400
ISAKMP Key		cisco	cisco

Parâmetros da ISAKMP Phase2

Parameters	R1	R3
Transform Set	VPN-SET	VPN-SET
Peer Hostname	R3	R1
Peer IP Address	10.2.2.2	10.1.1.2
Network to be encrypted	192.168.1.0/24	192.168.3.0/24
Crypto Map name	VPN-MAP	VPN-MAP
SA Establishment	ipsec-isakmp	ipsec-isakmp

Nota: Os parâmetros por *default* (estão a negrito) não necessitam de ser escritos na configuração do router

Exercício

- Etapas
 - Defina as access-list nos router 1 e router 3.
access-list 110 permit ip rede origem rede destino
 - Configure the ISAKMP Phase 1.
 - Configure the ISAKMP Phase 2.
 - Ligue o crypto map à interface de saída.
 - Verifique o estado do seu túnel.
 - Gere tráfego que vai ser encriptado (por exemplo do PC0 para o PC1).
 - Verifique o estado do seu túnel.

Exercício



```
R_Delega#sh crypto ipsec sa
```

```
interface: Serial0/3/0
    Crypto map tag: VPN-MAP, local addr 10.1.2.1

    protected vrf: (none)
    local ident (addr/mask/prot/port):
(192.168.3.0/255.255.255.0/0/0)
    remote ident (addr/mask/prot/port):
(192.168.1.0/255.255.255.0/0/0)
    current_peer 10.1.1.1 port 500
        PERMIT, flags={origin_is_acl,}
    #pkts encaps: 0, #pkts encrypt: 0, #pkts digest: 0
    #pkts decaps: 0, #pkts decrypt: 0, #pkts verify: 0
    #pkts compressed: 0, #pkts decompressed: 0
    #pkts not compressed: 0, #pkts compr. failed: 0
    #pkts not decompressed: 0, #pkts decompress failed: 0
    #send errors 0, #recv errors 0

    local crypto endpt.: 10.1.2.1, remote crypto endpt.:10.1.1.1
    path mtu 1500, ip mtu 1500, ip mtu idb Serial0/3/0
    current outbound spi: 0x0(0)
```

Antes de gerar tráfego encriptado

```
R_Delega#sh crypto ipsec sa
```

```
interface: Serial0/3/0
    Crypto map tag: VPN-MAP, local addr 10.1.2.1

    protected vrf: (none)
    local ident (addr/mask/prot/port):
(192.168.3.0/255.255.255.0/0/0)
    remote ident (addr/mask/prot/port):
(192.168.1.0/255.255.255.0/0/0)
    current_peer 10.1.1.1 port 500
        PERMIT, flags={origin_is_acl,}
    #pkts encaps: 3, #pkts encrypt: 3, #pkts digest: 0
    #pkts decaps: 2, #pkts decrypt: 2, #pkts verify: 0
    #pkts compressed: 0, #pkts decompressed: 0
    #pkts not compressed: 0, #pkts compr. failed: 0
    #pkts not decompressed: 0, #pkts decompress failed: 0
    #send errors 1, #recv errors 0

    local crypto endpt.: 10.1.2.1, remote crypto endpt.:10.1.1.1
    path mtu 1500, ip mtu 1500, ip mtu idb Serial0/3/0
    current outbound spi: 0x06264741(103171905)
```

Depois de gerar tráfego encriptado

Exercício

- Teste se o PC2 consegue chegar ao PC0.
- Veja o que aconteceu com o tráfego que não passa pelo túnel IPSec. Se tudo correr bem, deve conseguir “pingar” o PC e não “acrescentar” tráfego encriptado no túnel.
- Volte a pingar do PC0 para o PC1. O que aconteceu ao tráfego encriptado no túnel?

```
R_Sede#sh crypto ipsec sa

interface: Serial0/3/0
          Crypto map tag: VPN-MAP, local addr 10.1.1.1

          protected vrf: (none)
          local ident (addr/mask/prot/port):
(192.168.1.0/255.255.255.0/0/0)
          remote ident (addr/mask/prot/port):
(192.168.3.0/255.255.255.0/0/0)
          current_peer 10.1.2.1 port 500
            PERMIT, flags={origin_is_acl,}
          #pkts encaps: 6, #pkts encrypt: 6, #pkts digest: 0
          #pkts decaps: 7, #pkts decrypt: 7, #pkts verify: 0
          #pkts compressed: 0, #pkts decompressed: 0
          #pkts not compressed: 0, #pkts compr. failed: 0
          #pkts not decompressed: 0, #pkts decompress failed: 0
          #send errors 0, #recv errors 0
```

How To

Resumo

1. Configuração das políticas ISAKMP (Fase 1 do IKE – dados de gestão)

Comandos	Descrição
Router# configure terminal	Entrar no modo de configuração global
Router(config)# crypto isakmp policy [prioridade]	Definir a prioridade a atribuir a política. (Quanto menor o valor maior a prioridade)
Router (config-isakmp)# authentication pre-shared	Definir que a autenticação vai ser efectuada por uma chave partilhada pelos intervenientes.
Router (config-isakmp)# encryption [des 3des aes]	Definir o algoritmo de encriptação que vai ser utilizado. No caso de escolher aes pode-se ainda definir o numero de bits de encriptação. [128 192 256].
Router (config-isakmp)# group [1 2 5]	Definir o grupo utilizado para as chaves Diffie-Hellman. 1 – 768 bit 2 – 1024 bit 5 – 1536 bit
Router (config-isakmp)# hash [md5 sha]	Definir o algoritmo de hash que vai ser utilizado.
Router (config-isakmp)# lifetime [60 86400]	Definir o tempo que esta política de ser utilizada antes de ser renegociada. O tempo está expresso em segundos.
Router (config)# crypto isakmp key [0 6] segredo address endereço_publico_remoto no-xauth	Definir a chave partilhada utilizada na autenticação. O 0 ou 6 define se a palavra deve ou não ser encriptada. O endereço de ser o endereço público do local remoto. Por fim no-xauth previne confusões na autenticação em interface que possuem servidores de acesso remotos, em que os utilizadores têm que efectuar autenticação estendida. (username/password)

Resumo

2. Configuração do IPSec Transform Set (Fase 2 do IKE – dados de transmissão)

Comandos	Descrição
Router # configure terminal	Entrar no modo de configuração global
Router (config)# crypto ipsec transform-set <i>nome_atribuido</i> [opção de encriptação] [opção de hash]	Definição o nome que se vai atribuir a este transform-set. Opções de encriptação: esp-des esp-3des esp-aes [128 192 256] Opções de hash: esp-md5-hmac esp-sha-hmac

Resumo

3. Configuração do tráfego interessante

Criar uma access-list que defina o tráfico que será considerado interessante para activar a VPN assim como o tráfico que vai ser encriptado e que vai ser enviado pela VPN.

Comandos

```
Router# configure terminal  
Router(config)# ip access-list extended NOME_DA_LISTA  
Router(config)# permit ip ip_origem wild_card_origem ip_destino  
wild_card_destino
```

Resumo

4. Configurar crypto map

Comandos	Descrição
Router# configure terminal	Entrar no modo de configuração global
Router(config)# crypto map nome [numero de sequencia] ipsec-isakmp	Definir o nome que vai ser atribuído ao crypto map. Deve-se ter em conta que cada interface apenas pode ter um crypto map associado, deste forma o crypto map pode conter configurações de várias conexões VPN. O número de sequência indica qual o ordem em que vai ser colocada a conexão que estamos a criar.
Router (config-crypto-map)# set peer endereço_remote	Definir o ponto remoto de ligação da VPN.
Router (config-crypto-map)# match address acl-tráfego_interessante	Definir a access-list que define o tráfego interessante para a ligação VPN.
Router (config-crypto-map)# set transform-set nome_transform_set	Definir o nome do transform-set que vai ficar agregado a esta ligação VPN no crypto-map

Resumo

5. Atribuir o crypto map com um interface

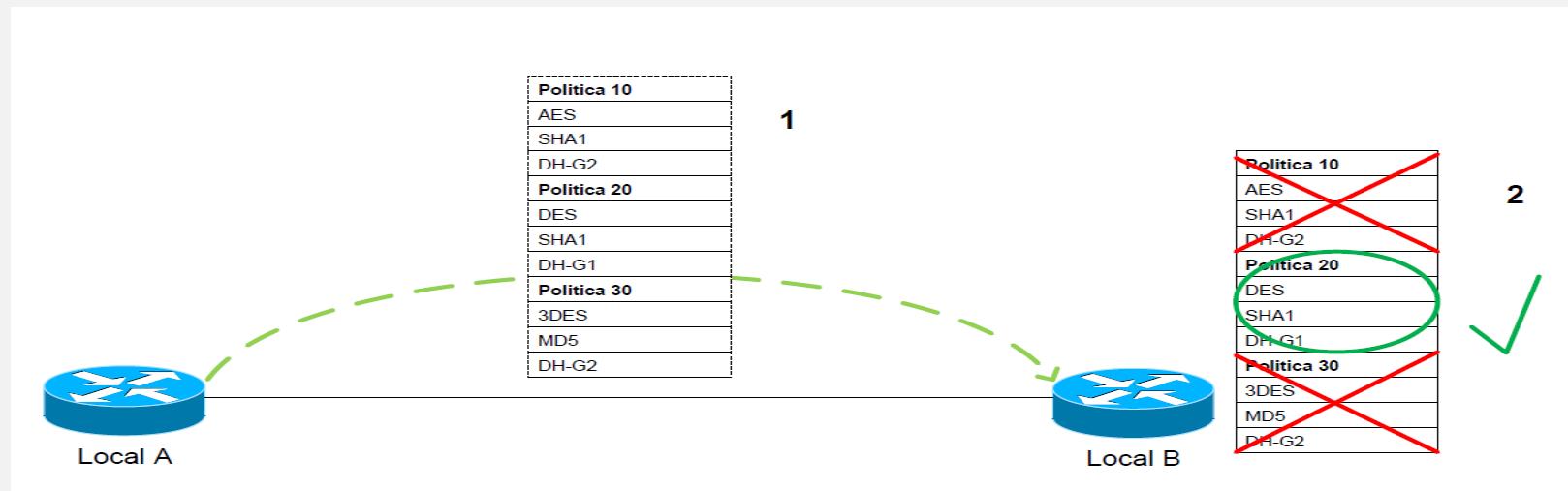
Comandos	Descrição
Router# configure terminal	Entrar no modo de configuração global
Router(config)# interface <i>interface</i>	Entrar no modo de configuração do interface de saída.
Router (config-if)# crypto map <i>nome</i>	Relacionar o crypto map definido anteriormente com o interface.

Configuração de túneis IPSec

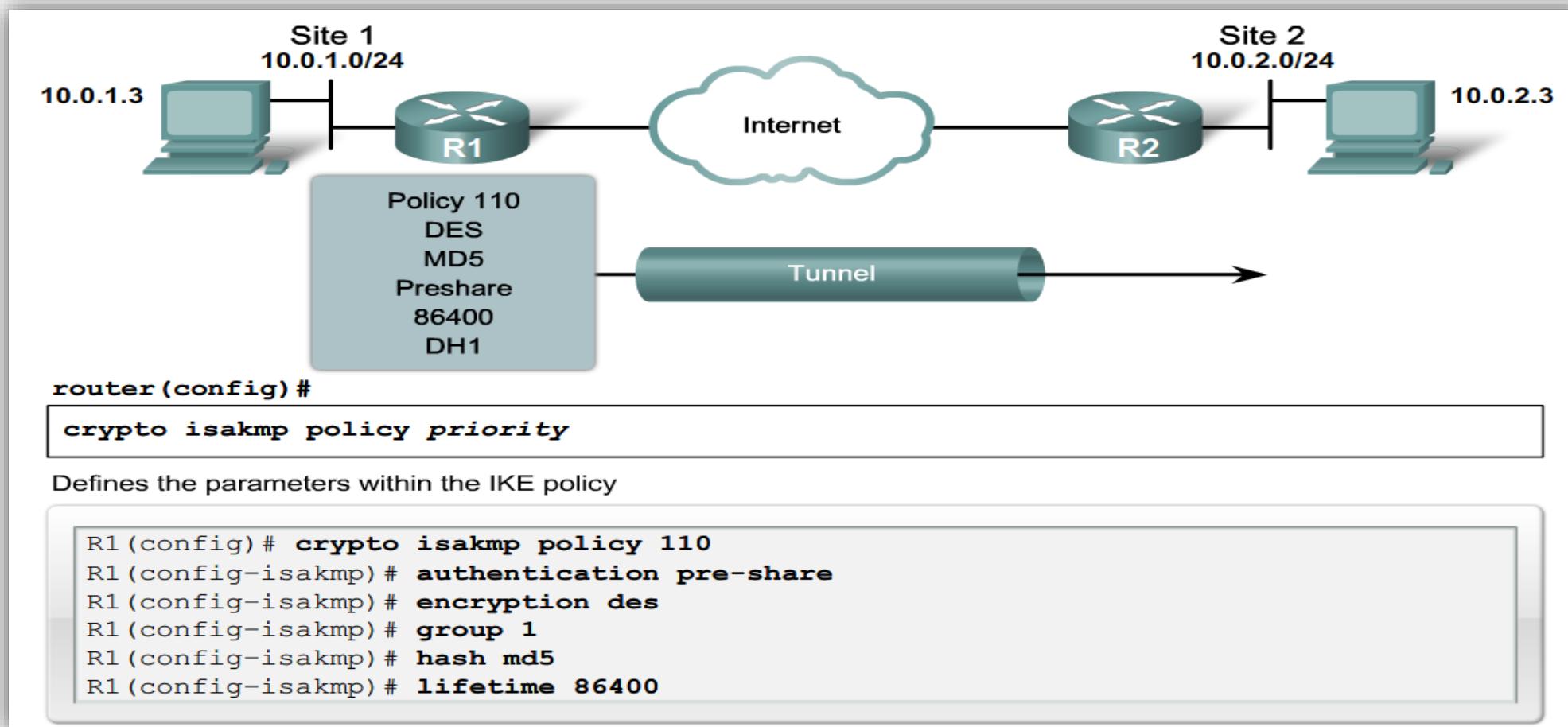
- Configurar as políticas a usar na fase de negociação.
- Isso é feito em duas fases:
 - **IKE fase 1:** Basicamente tem a função de negociar as políticas que serão utilizadas, autenticar os peers e fechar um túnel seguro, por onde serão configurados os demais parâmetros. Pode trabalhar em *Main Mode* ou *Agressive Mode*. Podemos dizer que é um “primeiro túnel”, para proteger as mensagens de negociação para o túnel principal.
 - **IKE fase 2:** É a negociação do “segundo túnel”. São definidos os parâmetros do IPSec e *transform sets*.

Configuração de túneis IPSec

- **Mensagem 1 (IKE 1- mainmode):** Troca e negociação de políticas de segurança O router que inicia a ligação VPN envia uma lista de políticas contendo vários grupos de possíveis alternativas. Dentro desta lista o receptor deve concordar com um conjunto para que seja possível criar a ligação.



Configuração de túneis IPSec



Configuração de túneis IPSec

- As diferentes opções que pode considerar para o definição dos parâmetros da ligação são:

ISAKMP Parameters				
Parameter	Keyword	Accepted Values	Default Value	Description
encryption	des 3des aes aes 192 aes 256	56-bit Data Encryption Standard Triple DES 128-bit AES 192-bit AES 256-bit AES	des	Message encryption algorithm
hash	sha md5	SHA-1 (HMAC variant) MD5 (HMAC variant)	sha	Message integrity (Hash) algorithm
authentication	pre-share rsa-encr rsa-sig	preshared keys RSA encrypted nonces RSA signatures	rsa-sig	Peer authentication method
group	1 2 5	768-bit Diffie-Hellman (DH) 1024-bit DH 1536-bit DH	1	Key exchange parameters (DH group identifier)
lifetime	<i>seconds</i>	Can specify any number of seconds	86,400 sec (one day)	ISAKMP-established SA lifetime

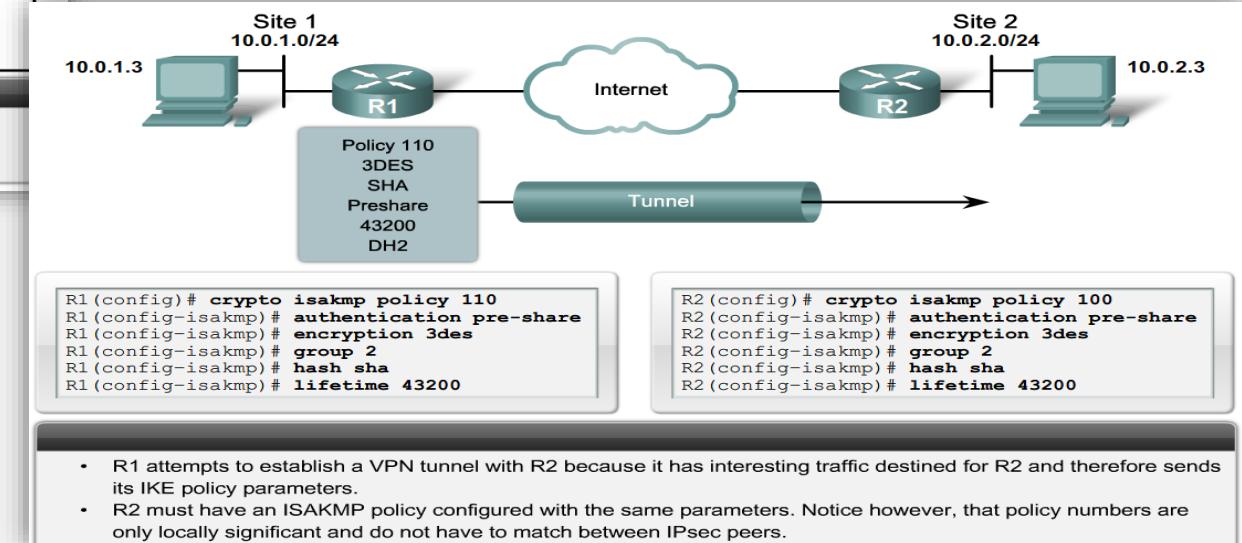
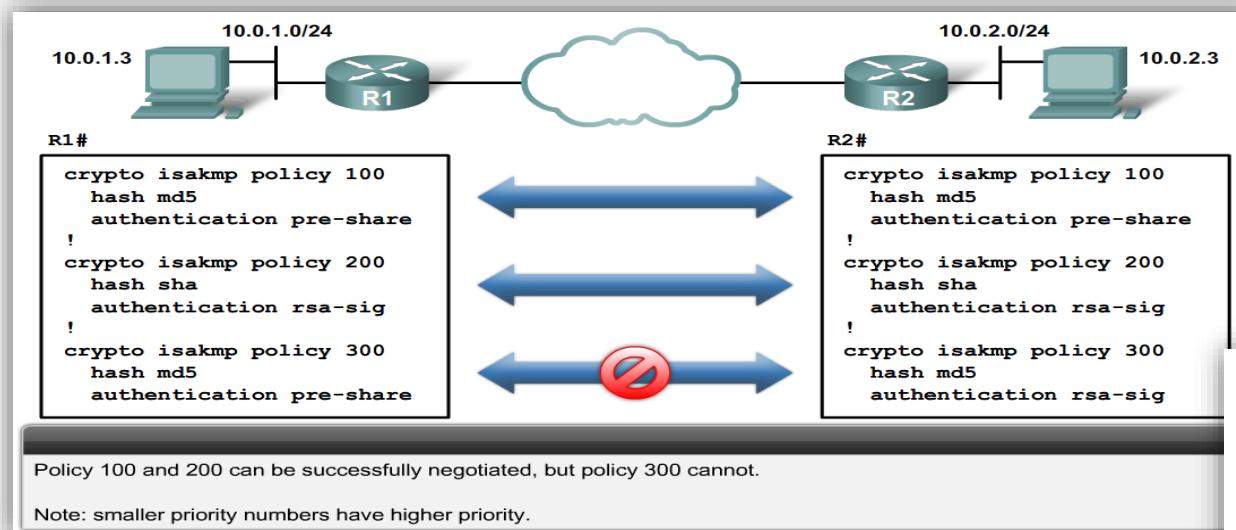
Note: Actual parameters vary based on IOS image.

Configuração de túneis IPSec

- **Mensagem 2 (IKE 1):** Troca de chaves públicas possibilitando uma ligação segura entre os pontos
- **Mensagem 2 (IKE 2):** Verificação de identidade. Uma vez garantida a segurança pode ser trocada a identificação dos intervenientes sem o risco de esta ser capturada por terceiros.

Configuração de túneis IPSec

- Temos de garantir que em ambos os extremos os parâmetros IKE são iguais.



Configuração de túneis IPSec

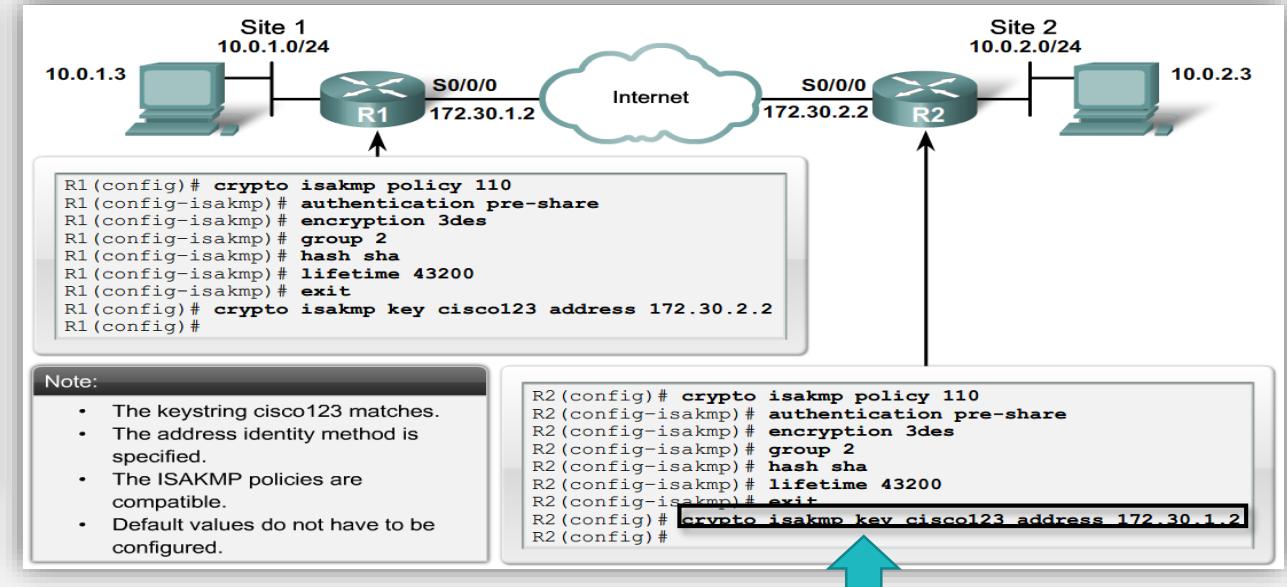
- A configuração da *Pre-SharedKey* (PSK) necessita ainda da definição em ambos os routers da palavra chave comum a utilizar na autenticação.

```
router(config)#  
crypto isakmp key keystring address peer-address  
  
router(config)#  
crypto isakmp key keystring hostname hostname
```

Parameter	Description
keystring	This parameter specifies the PSK. Use any combination of alphanumeric characters up to 128 bytes. This PSK must be identical on both peers.
peer-address	This parameter specifies the IP address of the remote peer.
hostname	This parameter specifies the hostname of the remote peer. This is the peer hostname concatenated with its domain name (for example, myhost.domain.com).

Note:

- The `peer-address` or `hostname` can be used, but must be used consistently between peers.
- If the `hostname` is used, then the `crypto isakmp identity hostname` command must also be configured.



Configuração de túneis IPSec

- Temos depois de definir os parâmetros da segunda fase de negociação:
 - Configurar os “*Transform Sets*”- Combinação de protocolos e modos de funcionamento do IPSec.

Configuração de túneis IPSec

```
router(config)#
```

```
crypto ipsec transform-set transform-set-name transform1 [transform2]
[transform3] [transform4]
```

crypto ipsec transform-set Parameters

Command	Description
<i>transform-set-name</i>	This parameter specifies the name of the transform set to create (or modify).
<i>transform1, transform2, transform3, transform4</i>	Type of transform set. Specify up to four "transforms": one Authentication Header (AH), one Encapsulating Security Payload (ESP) encryption, one ESP authentication. These transforms define the IP Security (IPsec) security protocols and algorithms.

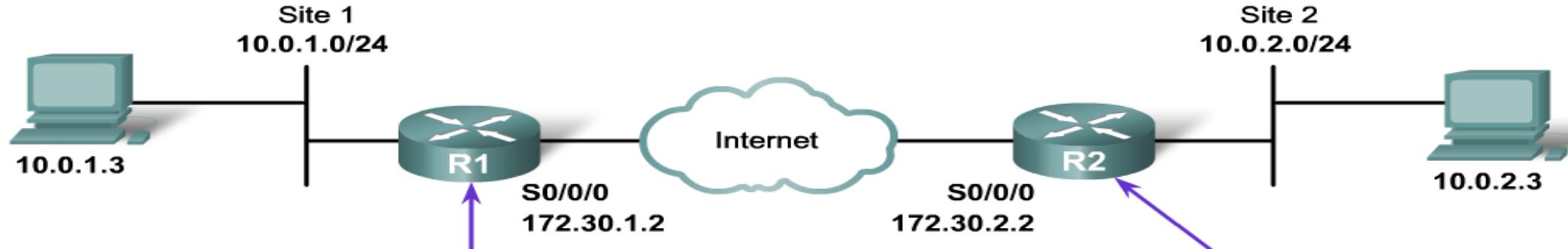
- A transform set is a combination of IPsec transforms that enact a security policy for traffic.
- A transform set can have one AH transform and up to two ESP transforms.

Configuração de túneis IPSec

- As combinações possíveis são as seguintes:

Allowed Transform Combinations		
Transform Type	Transform	Description
AH Transform (<i>Pick only one.</i>)	ah-md5-hmac ----- ah-sha-hmac	<ul style="list-style-type: none">AH with the MD5 (Message Digest 5) (a Hash-based Message Authentication Code [HMAC] variant) authentication algorithmAH with the SHA (Secure Hash Algorithm) (an HMAC variant) authentication algorithm
ESP Encryption Transform (<i>Pick only one.</i>)	esp-aes ----- esp-aes 192 ----- esp-aes 256 ----- esp-des ----- esp-3des ----- esp-null ----- esp-seal	<ul style="list-style-type: none">ESP with the 128-bit Advanced Encryption Standard (AES) encryption algorithmESP with the 192-bit AES encryption algorithmESP with the 256-bit AES encryption algorithmESP with the 56-bit Data Encryption Standard (DES) encryption algorithmESP with the 168-bit DES encryption algorithm (3DES or Triple DES)Null encryption algorithmESP with the 160-bit SEAL encryption algorithm.
ESP Authentication Transform (<i>Pick only one.</i>)	esp-md5-hmac ----- esp-sha-hmac	<ul style="list-style-type: none">ESP with the MD5 (HMACvariant) authentication algorithmESP with the SHA (HMACvariant) authentication algorithm
IP Compression Transform	comp-lzs	<ul style="list-style-type: none">IP compression with the Lempel-Ziv-Stac (LZS) algorithm

Configuração de túneis IPSec



```
R1 (config) # crypto isakmp key cisco123 address 172.30.2.2
R1 (config) # crypto ipsec transform-set MYSET esp-aes 128
R1 (cfg-crypto-trans) # exit
R1 (config) #
```

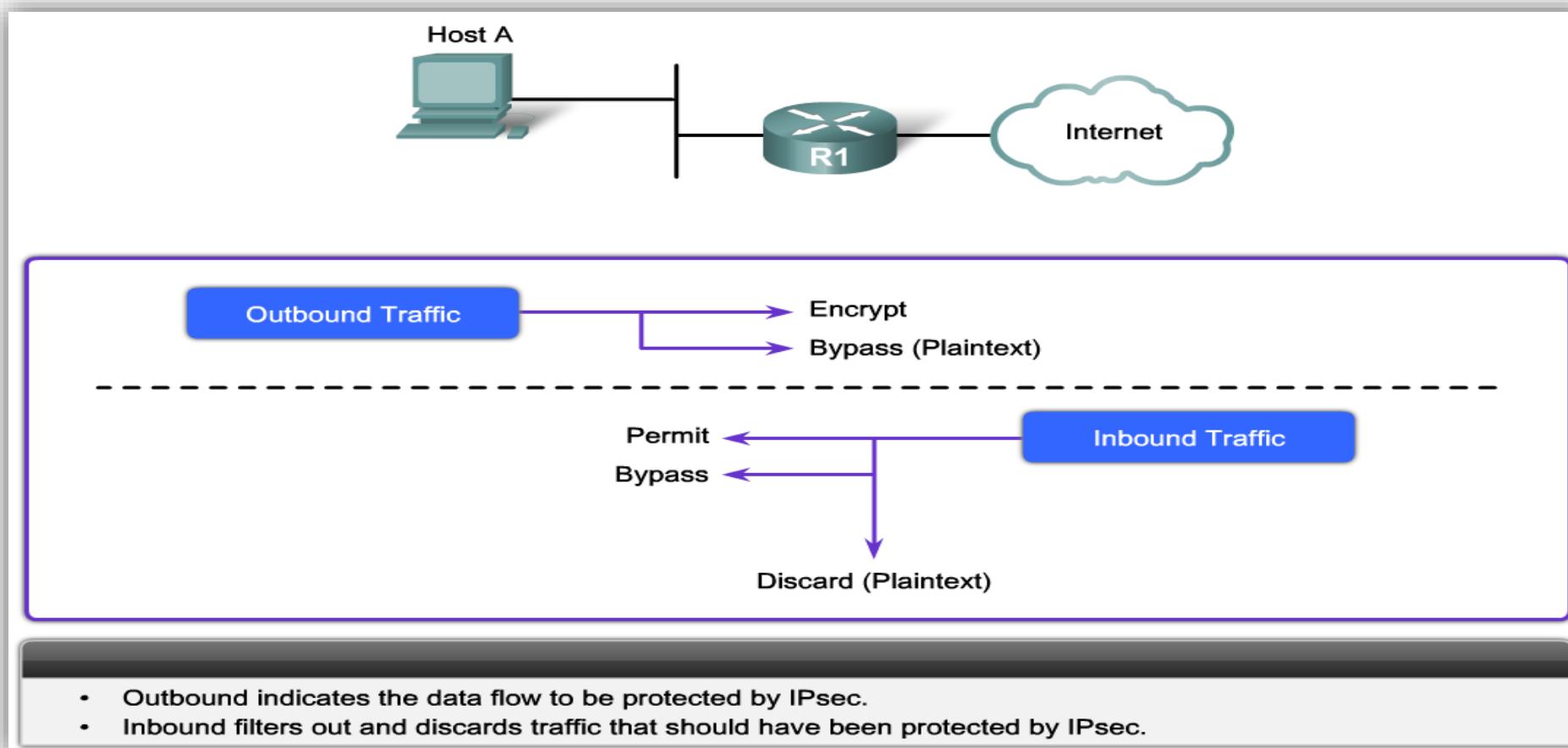
```
R2 (config) # crypto isakmp key cisco123 address 172.30.1.2
R2 (config) # crypto ipsec transform-set OTHERSET esp-aes 128
R2 (cfg-crypto-trans) # exit
```

Note:

- Peers must share the same transform set settings.
- Names are only locally significant.

Configuração de túneis IPSec

- Por fim, temos de proceder à configuração do “*Crypto ACLs*” que permita proteger o tráfego



Configuração de túneis IPSec

Site 1
10.0.1.0/24
10.0.1.3

R1
S0/0/0
172.30.1.2

Internet

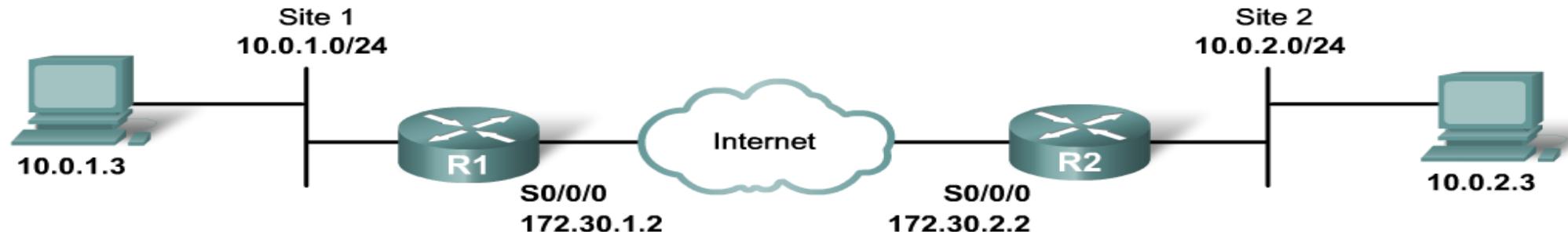
Site 2
10.0.2.0/24
10.0.2.3

R2
S0/0/0
172.30.2.2

```
router (config)#
access-list access-list-number {deny | permit} protocol source source-wildcard destination destination-wildcard
```

Command	Description
permit	This option causes all IP traffic that matches the specified conditions to be protected by cryptography, using the policy described by the corresponding crypto map entry.
deny	This option instructs the router to route traffic in plaintext.
protocol	This option specifies which traffic to protect by cryptography based on the protocol, such as TCP, UDP, or ICMP. If the protocol is IP, then all IP traffic matching that permit statement is encrypted.
source and destination	If the ACL statement is a permit statement, these are the networks, subnets, or hosts between which traffic should be protected. If the ACL statement is a deny statement, then the traffic between the specified source and destination is sent in plaintext.

Configuração de túneis IPSec



Applied to R1 S0/0/0 outbound traffic:

```
R1 (config) # access-list 110 permit tcp 10.0.1.0 0.0.0.255 10.0.2.0 0.0.0.255
```

Applied to R2 S0/0/0 outbound traffic:

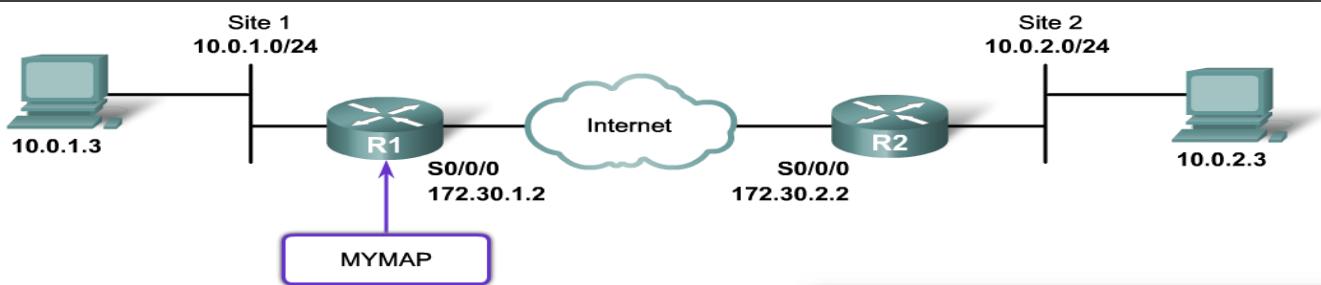
```
R2 (config) # access-list 101 permit tcp 10.0.2.0 0.0.0.255 10.0.1.0 0.0.0.255
```

Configuração de túneis IPSec

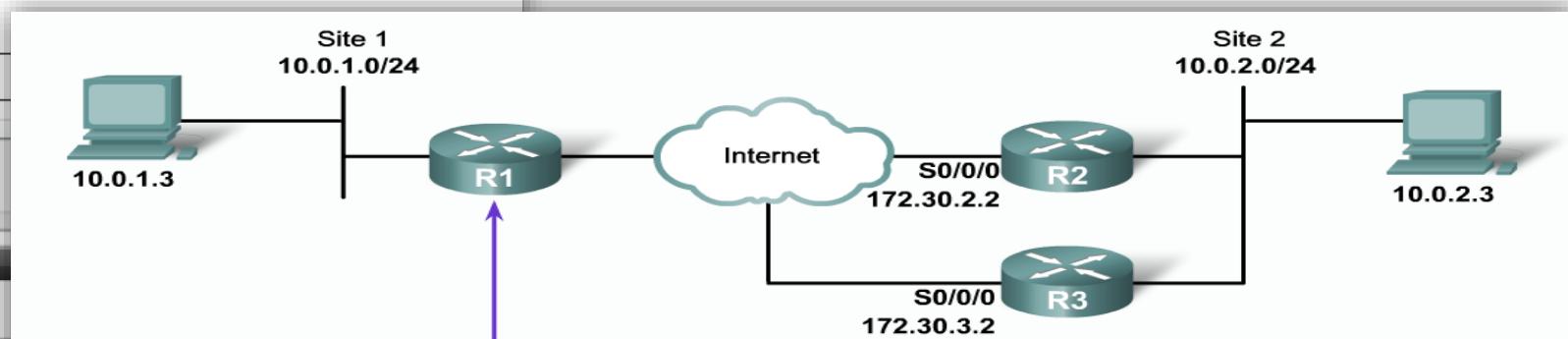
- Aplicação do “*Crypto Map*”
 - ACL a usar
 - Equipamentos remotos com os quais se vai estabelecer a VPN
 - Transform Set* a ser usada
 - Método de gestão de chaves
 - Tempo de vida das *Security Associations*
- Podem ser criados vários *Crypto Maps*

<pre>router(config)# crypto map map-name seq-num ipsec-manual crypto map map-name seq-num ipsec-isakmp [dynamic dynamic-map-name]</pre>	<p>crypto map Parameters</p> <table border="1"><thead><tr><th>Command Parameters</th><th>Description</th></tr></thead><tbody><tr><td><i>map-name</i></td><td>Defines the name assigned to the crypto map set or indicates the name of the crypto map to edit.</td></tr><tr><td><i>seq-num</i></td><td>The number assigned to the crypto map entry.</td></tr><tr><td><i>ipsec-manual</i></td><td>Indicates that ISAKMP will not be used to establish the IPsec SAs.</td></tr><tr><td><i>ipsec-isakmp</i></td><td>Indicates that ISAKMP will be used to establish the IPsec SAs.</td></tr><tr><td><i>cisco</i></td><td>(Default value) Indicates that CET will be used instead of IPsec for protecting the traffic.</td></tr><tr><td><i>dynamic</i></td><td>(Optional) Specifies that this crypto map entry references a preexisting static crypto map. If this keyword is used, none of the crypto map configuration commands are available.</td></tr><tr><td><i>dynamic-map-name</i></td><td>(Optional) Specifies the name of the dynamic crypto map set that should be used as the policy template.</td></tr></tbody></table> <p>crypto map Configuration Mode Commands</p> <table border="1"><thead><tr><th>Command</th><th>Description</th></tr></thead><tbody><tr><td>set</td><td>Used with the peer, pfs, transform-set, and security-association commands.</td></tr><tr><td>peer [<i>hostname</i> <i>ip-address</i>]</td><td>Specifies the allowed IPsec peer by IP address or hostname.</td></tr><tr><td>pfs [<i>group1</i> <i>group2</i>]</td><td>Specifies DH Group 1 or Group 2.</td></tr><tr><td>transform-set [<i>set_name(s)</i>]</td><td>Specify list of transform sets in priority order. When the ipsec-manual parameter is used with the crypto map command, then only one transform set can be defined. When the ipsec-isakmp parameter or the dynamic parameter is used with the crypto map command, up to six transform sets can be specified.</td></tr><tr><td>security-association lifetime</td><td>Sets SA lifetime parameters in seconds or kilobytes.</td></tr><tr><td>match address [<i>access-list-id</i> <i>name</i>]</td><td>Identifies the extended ACL by its name or number. The value should match the access-list-number or name argument of a previously defined IP-extended ACL being matched.</td></tr><tr><td>no</td><td>Used to delete commands entered with the set command.</td></tr><tr><td>exit</td><td>Exits crypto map configuration mode.</td></tr></tbody></table>	Command Parameters	Description	<i>map-name</i>	Defines the name assigned to the crypto map set or indicates the name of the crypto map to edit.	<i>seq-num</i>	The number assigned to the crypto map entry.	<i>ipsec-manual</i>	Indicates that ISAKMP will not be used to establish the IPsec SAs.	<i>ipsec-isakmp</i>	Indicates that ISAKMP will be used to establish the IPsec SAs.	<i>cisco</i>	(Default value) Indicates that CET will be used instead of IPsec for protecting the traffic.	<i>dynamic</i>	(Optional) Specifies that this crypto map entry references a preexisting static crypto map. If this keyword is used, none of the crypto map configuration commands are available.	<i>dynamic-map-name</i>	(Optional) Specifies the name of the dynamic crypto map set that should be used as the policy template.	Command	Description	set	Used with the peer , pfs , transform-set , and security-association commands.	peer [<i>hostname</i> <i>ip-address</i>]	Specifies the allowed IPsec peer by IP address or hostname.	pfs [<i>group1</i> <i>group2</i>]	Specifies DH Group 1 or Group 2.	transform-set [<i>set_name(s)</i>]	Specify list of transform sets in priority order. When the ipsec-manual parameter is used with the crypto map command, then only one transform set can be defined. When the ipsec-isakmp parameter or the dynamic parameter is used with the crypto map command, up to six transform sets can be specified.	security-association lifetime	Sets SA lifetime parameters in seconds or kilobytes.	match address [<i>access-list-id</i> <i>name</i>]	Identifies the extended ACL by its name or number. The value should match the access-list-number or name argument of a previously defined IP-extended ACL being matched.	no	Used to delete commands entered with the set command.	exit	Exits crypto map configuration mode.
Command Parameters	Description																																		
<i>map-name</i>	Defines the name assigned to the crypto map set or indicates the name of the crypto map to edit.																																		
<i>seq-num</i>	The number assigned to the crypto map entry.																																		
<i>ipsec-manual</i>	Indicates that ISAKMP will not be used to establish the IPsec SAs.																																		
<i>ipsec-isakmp</i>	Indicates that ISAKMP will be used to establish the IPsec SAs.																																		
<i>cisco</i>	(Default value) Indicates that CET will be used instead of IPsec for protecting the traffic.																																		
<i>dynamic</i>	(Optional) Specifies that this crypto map entry references a preexisting static crypto map. If this keyword is used, none of the crypto map configuration commands are available.																																		
<i>dynamic-map-name</i>	(Optional) Specifies the name of the dynamic crypto map set that should be used as the policy template.																																		
Command	Description																																		
set	Used with the peer , pfs , transform-set , and security-association commands.																																		
peer [<i>hostname</i> <i>ip-address</i>]	Specifies the allowed IPsec peer by IP address or hostname.																																		
pfs [<i>group1</i> <i>group2</i>]	Specifies DH Group 1 or Group 2.																																		
transform-set [<i>set_name(s)</i>]	Specify list of transform sets in priority order. When the ipsec-manual parameter is used with the crypto map command, then only one transform set can be defined. When the ipsec-isakmp parameter or the dynamic parameter is used with the crypto map command, up to six transform sets can be specified.																																		
security-association lifetime	Sets SA lifetime parameters in seconds or kilobytes.																																		
match address [<i>access-list-id</i> <i>name</i>]	Identifies the extended ACL by its name or number. The value should match the access-list-number or name argument of a previously defined IP-extended ACL being matched.																																		
no	Used to delete commands entered with the set command.																																		
exit	Exits crypto map configuration mode.																																		

Configuração de túneis IPSec



```
router(config-if)#  
crypto map map-name  
  
R1(config)# interface serial0/0/0  
R1(config-if)# crypto map MYMAP  
  
• Applies the crypto map to outgoing interface  
• Activates the IPsec policy
```

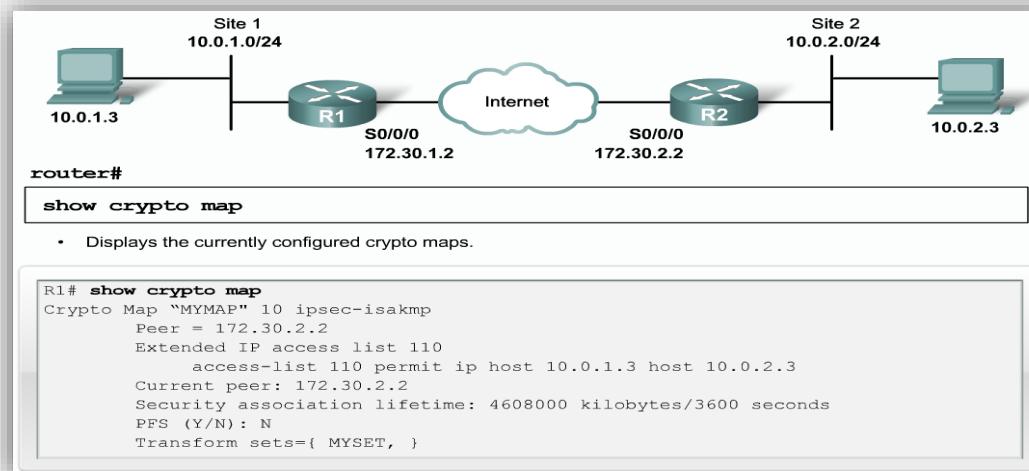


```
R1(config)# crypto map MYMAP 10 ipsec-isakmp  
R1(config-crypto-map)# match address 110  
R1(config-crypto-map)# set peer 172.30.2.2 default  
R1(config-crypto-map)# set peer 172.30.3.2  
R1(config-crypto-map)# set pfs group1  
R1(config-crypto-map)# set transform-set mine  
R1(config-crypto-map)# set security-association lifetime seconds 86400
```

- Multiple peers can be specified for redundancy.

Verificação da configuração

Show Command	Description
show crypto map	Displays configured crypto maps
show crypto isakmp policy	Displays configured IKE policies
show crypto ipsec sa	Displays established IPsec tunnels
show crypto ipsec transform-set	Displays configured IPsec transform sets
debug crypto isakmp	Debugs IKE events
debug crypto ipsec	Debugs IPsec events



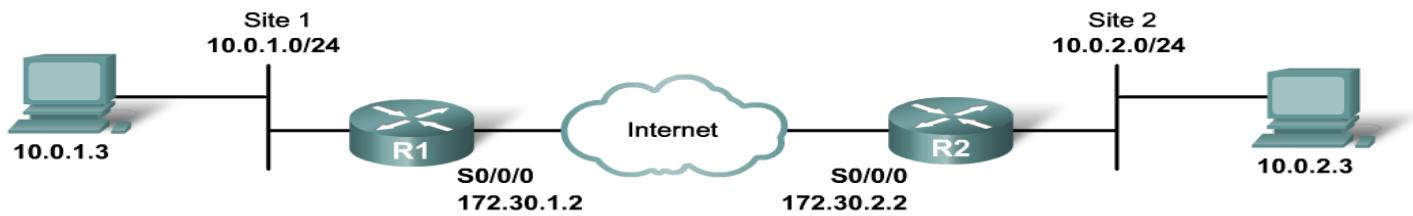
```

R1# show crypto isakmp policy
Protection suite of priority 110
  encryption algorithm: 3DES - Data Encryption Standard (168 bit keys).
  hash algorithm: Secure Hash Standard
  authentication method: preshared
  Diffie-Hellman group: #2 (1024 bit)
  lifetime: 86400 seconds, no volume limit

Default protection suite
  encryption algorithm: DES - Data Encryption Standard (56 bit keys).
  hash algorithm: Secure Hash Standard
  authentication method: Rivest-Shamir-Adleman Signature
  Diffie-Hellman group: #1 (768 bit)
  lifetime: 86400 seconds, no volume limit

R1# show crypto ipsec transform-set
Transform set AES_SHA: { esp-128-aes esp-sha-hmac }
will negotiate = { Tunnel, }, 
```

Verificação da configuração



```
R1# show crypto ipsec sa
Interface: Serial0/0/0
  Crypto map tag: MYMAP, local addr. 172.30.1.2
    local ident (addr/mask/prot/port): (172.30.1.2/255.255.255.255/0/0)
    remote ident (addr/mask/prot/port): (172.30.2.2/255.255.255.255/0/0)
    current_peer: 172.30.2.2
    PERMIT, flacs={origin_is_acl,}
      #pkts encaps: 21, #pkts encrypt: 21, #pkts digest 0
      #pkts decaps: 21, #pkts decrypt: 21, #pkts verify 0
      #send errors 0, #recv errors 0
  local crypto endpt.: 172.30.1.2, remote crypto endpt.: 172.30.2.2
  path mtu 1500, media mtu 1500
  current outbound spi: 8AE1C9C
```

```
router#  
debug crypto isakmp
```

```
1d00h: ISAKMP (0:1): atts are not acceptable. Next payload is 0 1d00h: ISAKMP  
(0:1); no offers accepted!  
1d00h: ISAKMP (0:1): SA not acceptable!  
1d00h: %CRYPTO-6-IKMP_MODE_FAILURE: Processing of Main Mode failed with peer  
at 172.30.2.2
```

- This is an example of the Main Mode error message.
- The failure of Main Mode suggests that the Phase 1 policy does not match on both sides.
- Verify that the Phase 1 policy is on both peers and ensure that all the attributes match.

Pre – Requisitos -Exercício 3

- Utilize o servidor e o cliente do segundo teste ou da aula prática nº. 10.
- No servidor Windows server 2012 desabilite o NAT.

Exercício 3 – VPN em ambiente *windows*

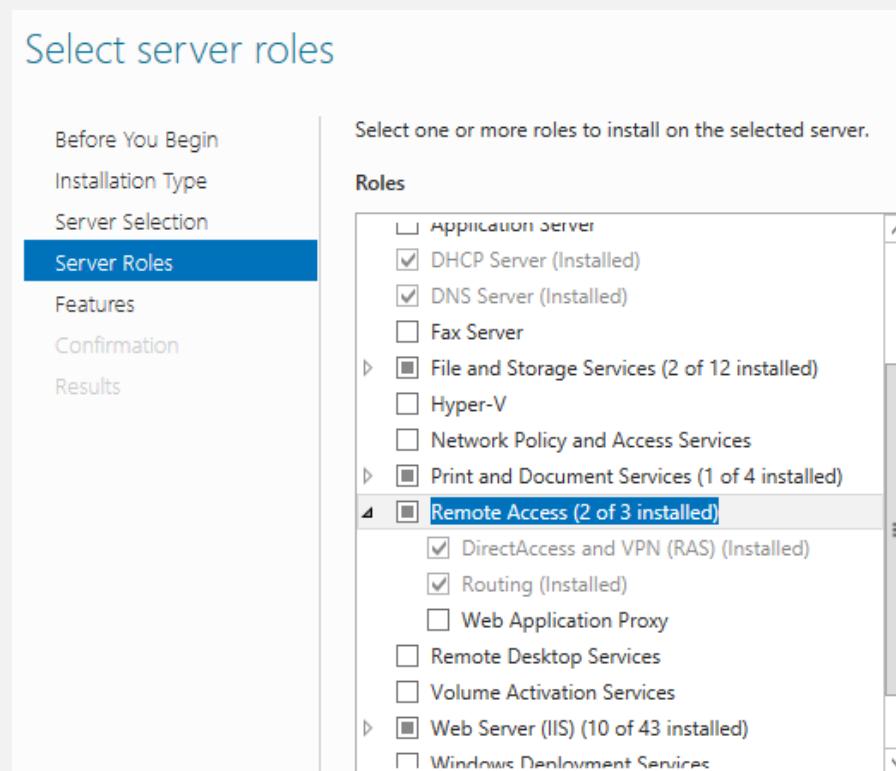
Exercício

- A empresa SR1.SA deseja implementar uma solução de acesso remoto por VPN para os seus vendedores.
- Como não tem um grande orçamento e deseja testar como funciona esta solução, foi decidido fazer esta VPN sobre Windows 2012 R2 utilizando o seu servidor de DNS.
- Instale o serviço
- Configure o serviço remoto no servidor:
 - Coloque 3 endereços da sua rede para serem disponibilizados para as ligações remotas.
 - Escolha o L2TP como protocolo VPN
- Configure a ligação no cliente.
- Tente aceder no cliente à VPN criada.

How To

Instalação do serviço

- O acesso remoto de computadores a um servidor Windows é feito através do serviço de acesso remoto (*Remote Access*)- **Veja a aula prática nº 7.**



Configuração do serviço

The image shows two windows side-by-side. On the left is the 'Server Manager' dashboard. It features a 'WELCOME TO SERVER MANAGER' section with a 'QUICK START' button containing four numbered steps: 1. Configure this local server, 2. Add roles and features, 3. Add other servers to manage, and 4. Create a server group. Below this is a 'WHAT'S NEW' section and a 'LEARN MORE' button. At the bottom, there's a 'ROLES AND SERVER GROUPS' section showing 'Roles: 6 | Server groups: 1 | Servers total: 1'. A large teal arrow points from the 'Configure this local server' step in the dashboard to the 'Routing and Remote Access' service configuration window on the right. The right window is titled 'Routing and Remote Access' and shows a list of tasks under 'ROUTING AND REMOTE ACCESS'. The 'Configure and Enable Routing and Remote Access' option is highlighted with a blue box.

Server Manager › Dashboard

Manage Tools View Help

Component Services
Computer Management
Connection Manager Administration Kit
Defragment and Optimize Drives
DHCP
DNS
Event Viewer
Group Policy Management
Internet Information Services (IIS) Manager
iSCSI Initiator
Local Security Policy
Network Policy Server
ODBC Data Sources (32-bit)
ODBC Data Sources (64-bit)
Performance Monitor
Print Management
Remote Access Management
Resource Monitor

Routing and Remote Access

File Action View Help

Routing and Remote Access

Server Status

SMTP (local)

Configure and Enable Routing and Remote Access

Disable Routing and Remote Access

All Tasks

View

Delete

Refresh

Properties

Help

Configure this local server

Add roles and features

Add other servers to manage

Create a server group

WHAT'S NEW

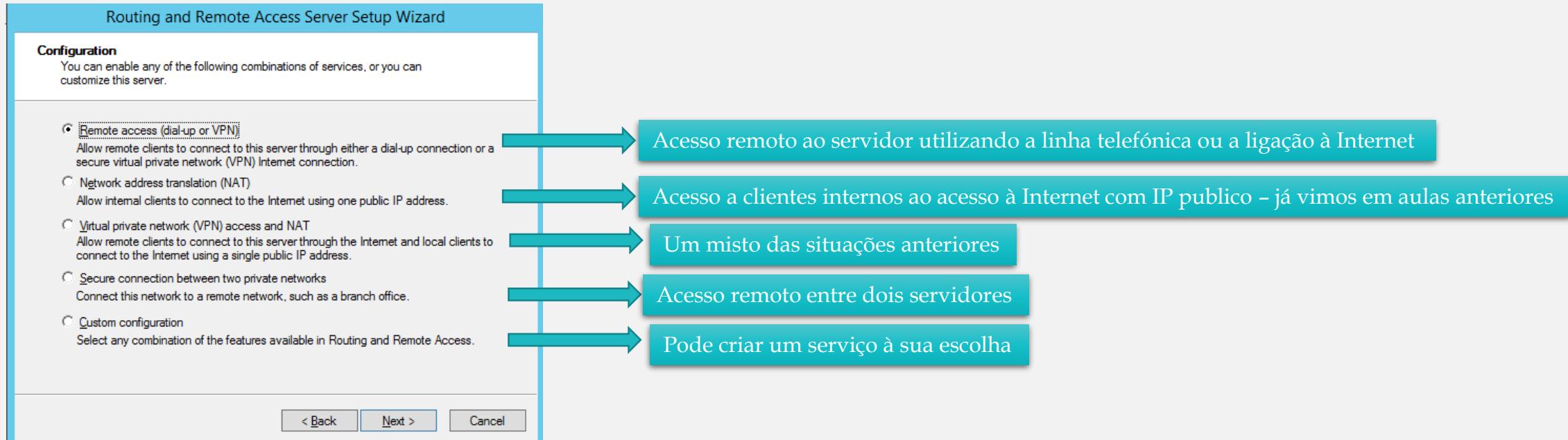
LEARN MORE

ROLES AND SERVER GROUPS

Roles: 6 | Server groups: 1 | Servers total: 1

DHCP DNS

Configuração do serviço



Configuração do serviço

Routing and Remote Access Server Setup Wizard

Remote Access
You can set up this server to receive both dial-up and VPN connections.

VPN
A VPN server (also called a VPN gateway) can receive connections from remote clients through the Internet.

Dial-up
A dial-up remote access server can receive connections directly from remote clients through dial-up media, such as a modem.

[< Back](#) [Next >](#) [Cancel](#)

Routing and Remote Access Server Setup Wizard

VPN Connection
To enable VPN clients to connect to this server, at least one network interface must be connected to the Internet.

Select the network interface that connects this server to the Internet.

Network interfaces:

Name	Description	IP Address
Ethernet	Intel(R) PRO/1000 MT ...	192.168.20.2
Ethernet 2	Intel(R) PRO/1000 MT ...	10.0.3.15 (DHCP)

Enable security on the selected interface by setting up static packet filters.
Static packet filters allow only VPN traffic to gain access to this server through the selected interface.

[< Back](#) [Next >](#) [Cancel](#)

Routing and Remote Access Server Setup Wizard

IP Address Assignment
You can select the method for assigning IP addresses to remote clients.

How do you want IP addresses to be assigned to remote clients?

Automatically
If you use a DHCP server to assign addresses, confirm that it is configured properly. If you do not use a DHCP server, this server will generate the addresses.

From a specified range of addresses

[< Back](#) [Next >](#) [Cancel](#)

Routing and Remote Access Server Setup Wizard

Address Range Assignment
You can specify the address ranges that this server will use to assign addresses to remote clients.

Enter the address ranges (static pools) that you want to use. You can add more ranges later. You can also edit existing ranges or delete them. To add a range, click New... and enter the address ranges. You can then click OK to save the changes and close the dialog box.

New IPv4 Address Range

Type a starting IP address and either an ending IP address or the number of addresses in the range.

Address ranges:

From	To

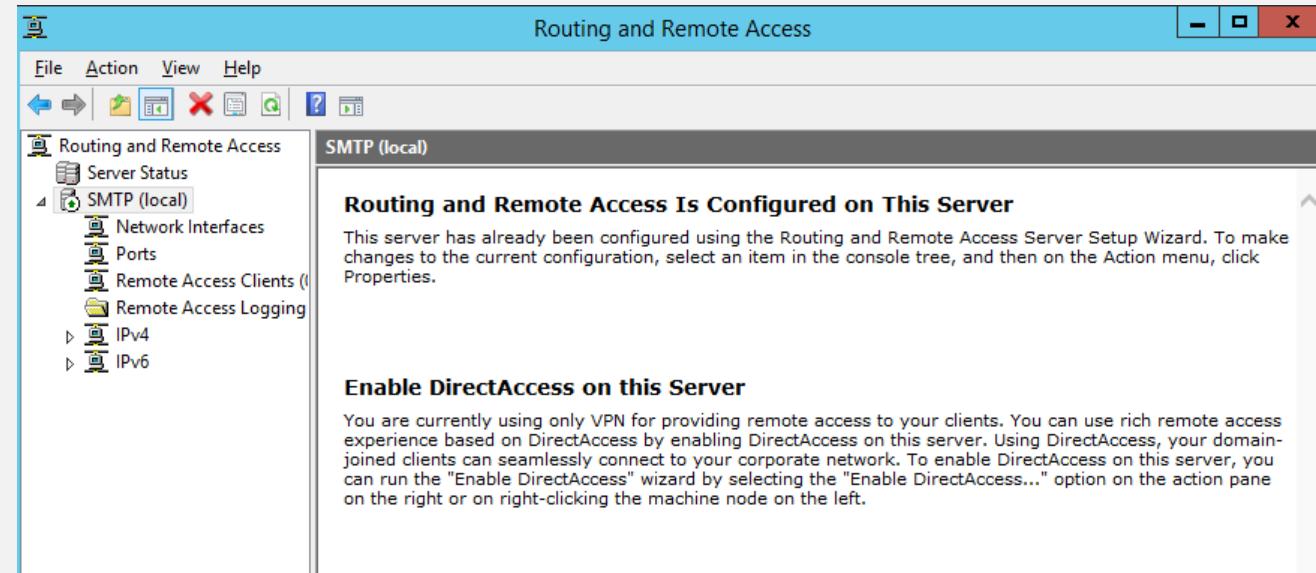
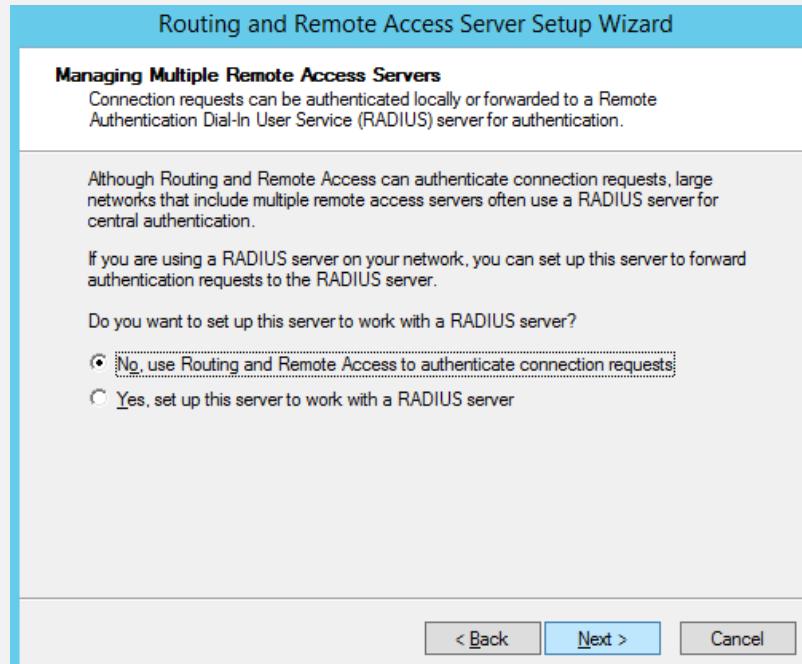
New...

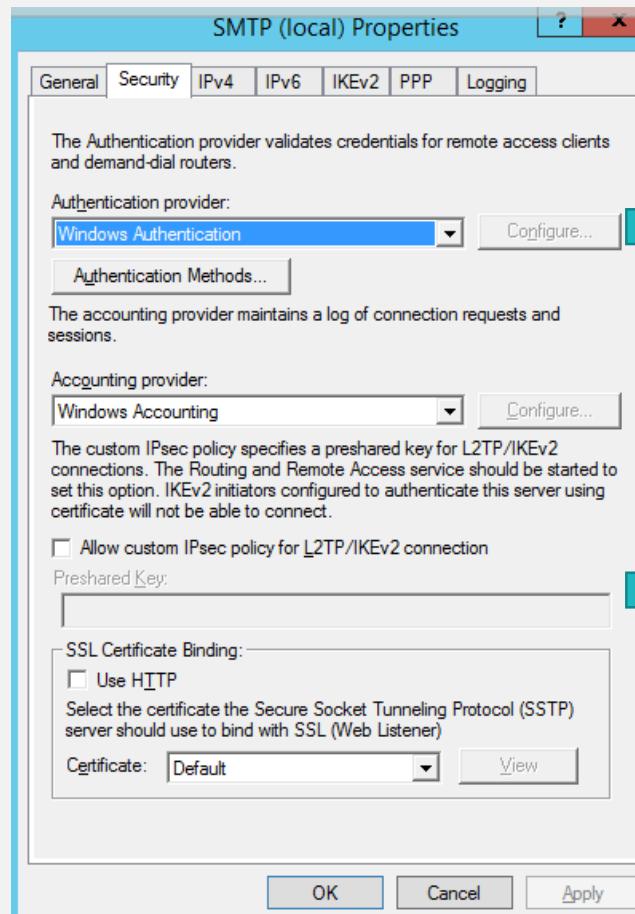
Start IP address: 192.168.20.10
End IP address: 192.168.20.12
Number of addresses: 3

[OK](#) [Cancel](#)

[< Back](#) [Next >](#) [Cancel](#)

Configuração do serviço





Tipo de autenticação do cliente

Tipo de gestão do túnel e encapsulamento dos dados

Configuração do Cliente

Network and Sharing Center

Control Panel Home

Change adapter settings

Change advanced sharing settings

Change your networking settings

- Set up a new connection or network
- Troubleshoot problems

See also

- HomeGroup
- Infrared
- Internet Options
- Windows Firewall

Network and Internet > Network and Sharing Center

Set Up a Connection or Network

Choose a connection option

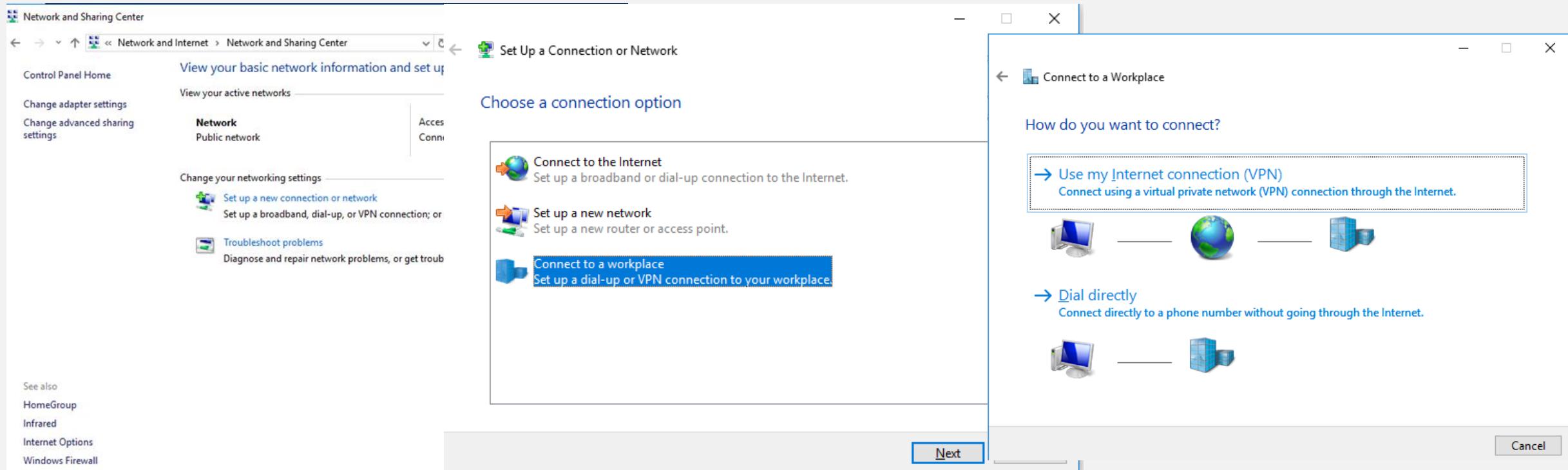
- Connect to the Internet
- Set up a new network
- Connect to a workplace

Connect to a Workplace

How do you want to connect?

- Use my Internet connection (VPN)
- Dial directly

Next Cancel



Configuração do Cliente

The screenshot shows the Windows Network Connections window with a context menu open over a 'VPN Connection' icon. The menu options include: Connect / Disconnect, Status, Set as Default Connection, Create Copy, Create Shortcut, Delete, Rename, and Properties.

Create a VPN connection

Type the Internet address to connect to
Your network administrator can give you this address.

Internet address: [Example:Contoso.com or 157.54.0.1 or 3ffe:1234::1111]
Destination name: VPN Connection 2

Use a smart card
 Remember my credentials
 Allow other people to use this connection
This option allows anyone with access to this computer to use this connection.

Create Cancel

Network Connections

Organize Start this connection Rename this connection Delete this connection

Ethernet Network Intel(R) PRO/1000 MT Desktop Ad...

VPN Connection Disconnected WAN M

Connect / Disconnect Status Set as Default Connection Create Copy Create Shortcut Delete Rename Properties

VPN

VPN

+ Add a VPN connection

VPN Connection

Connect Advanced options Remove

Advanced Options

Allow VPN over metered networks On

Allow VPN while roaming On

Related settings

Dúvidas



Referências

- Cisco Networking Academy – Packet Tracer – Configuring VPNs