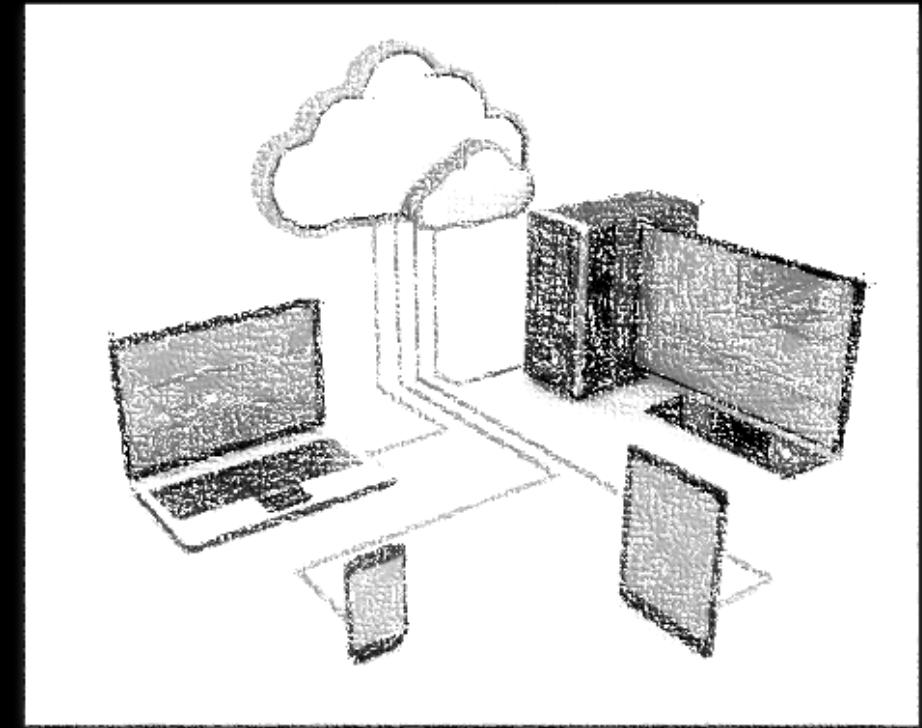


Serviços de Rede I

Licenciatura em Engenharia Informática
Ramo de Redes e Administração de Sistemas



Aula 1

Apresentação

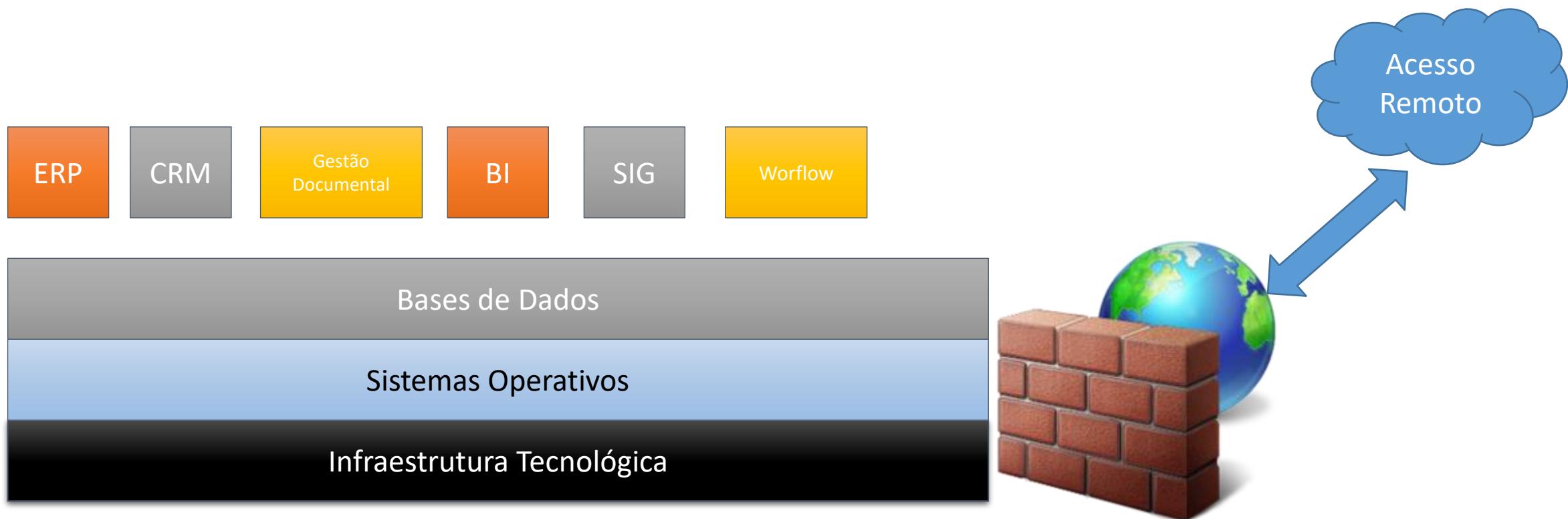
Agenda

- 1** Âmbito
- 2** Objetivos
- 3** Programa e Cronograma
- 4** Carga Horária e Funcionamento
- 5** Avaliação
- 6** Elementos de Estudo
- 7** Contactos

Âmbito

- As organizações modernas estão perante novos desafios que lhe são impostos pela globalização e pela digitalização (industria 4.0 e sociedade 5.0), pela nova forma de acesso à informação e por novas formas de gestão organizacional e dos recursos humanos.
- A infraestrutura tecnológica tem de dar resposta a esta nova forma de atuar criando condições para:
 - **flexibilizar as redes tornando-as simples de usar;**
 - **garantir que a rede é fiável e tem a largura de banda adequada às necessidades;**
 - **possuir configurados os serviços de rede necessários à organização;**
 - **garantir que a rede é segura;**
 - **promover a partilha e o acesso remoto à informação;**
 - **garantir mecanismos de interconetividade e de interoperabilidade.**

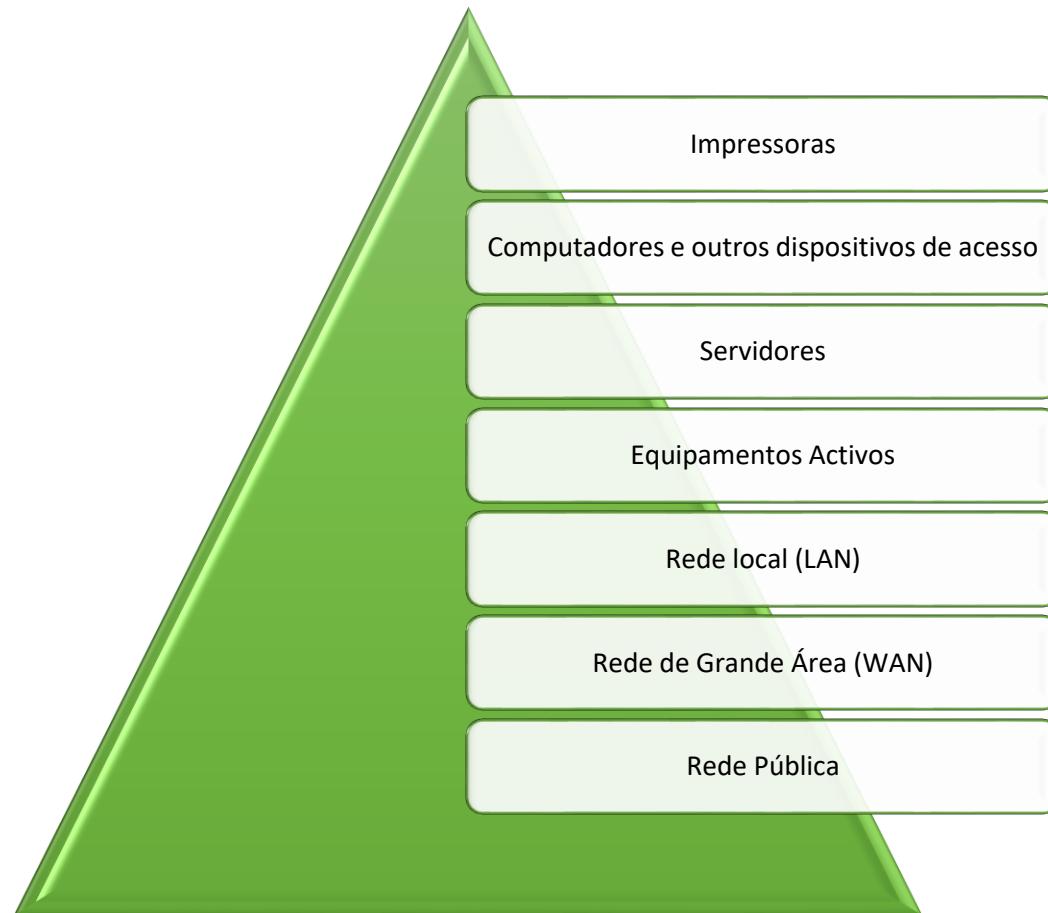
Âmbito



Âmbito

- Por **infraestrutura tecnológica** entende-se o equipamento informático e de comunicações que serve de suporte às aplicações informáticas utilizadas por uma organização.
- Os requisitos técnicos dessa infra-estrutura dependem do tipo de sistema de informação que a organização pretende desenvolver em função dos seus objectivos estratégicos, processos de negócio, dimensão e estrutura funcional.

Âmbito

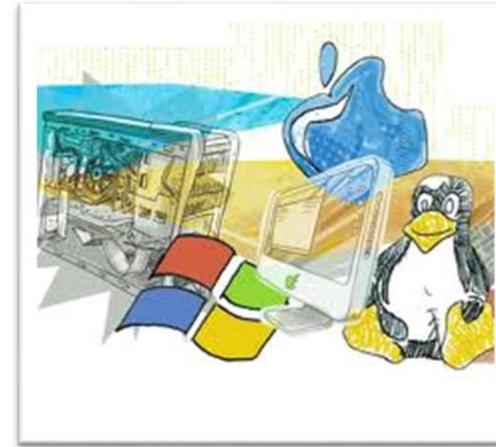


Objectivos

- Pretende-se que os alunos adquiram competências no planeamento, configuração e manutenção dos serviços de rede de suporte a:
 - endereçamento IP e serviços de endereçamento;
 - serviços de resolução de nomes;
 - serviços de acesso remoto;
 - outros serviços relacionados com a infraestrutura de rede.

Programa

- Tópicos:
 - Endereçamento IP.
 - Endereçamento dinâmico (DHCP).
 - Translação de endereços (NAT).
 - Resolução de nomes (DNS).
 - Acesso remoto (VPNs).
 - Serviços de *Proxy*.
 - Serviços de sincronização de relógio (NTP).



Calendarização

2º Semestre	Inicio	Fim
Período Letivo		
Semana de apoio a exames (não há avaliações, há defesas de trabalhos)	20 de fevereiro	16 de junho
Época de Exames - Normal	19 de junho	22 de junho
Época de Exames - Recurso	23 de junho	11 de julho
Férias da Páscoa	12 de julho	25 de julho
Queima das Fitas	03 de abril	10 de abril
	22 de maio	26 de maio

Tópico	Nº de aulas (Módulo de 2 horas)
Apresentação	1
IP e DHCP	3
NAT	1
DNS	3
Configurar uma rede empresarial – Parte I	1
NTP	1
Proxy	1
VPN	1
Configurar uma rede empresarial – Parte II	1
Revisões e conclusões	1

Carga horária

- 5 ECTS ⇔ 133,5 horas
- Horas de contacto – 56 horas
 - Componente teórica: 28 horas
 - Componente prática-laboratorial: 28 horas
- Horas de estudo não acompanhado – 73 horas
 - Estudo : 28 horas
 - Estudo prático: 45 horas
- Avaliação – 4,5 horas



Avaliação

- **Avaliação teórica (11 valores)**

- Exame escrito **SEM CONSULTA**.
- A nota da componente prática será nas três épocas a que foi obtida na avaliação contínua pelo que os exames serão corrigidos para 11 valores.



- **Avaliação prática (9 valores)**

- Três mini testes **individuais** no final de cada um dos tópicos e a realizar nas aulas práticas (3 valores cada). Estes testes serão sobre os seguintes temas:

- Teste 1 – **Endereçamento IP, DHCP e NAT – 29 ou 30 de Março**
- Teste 2 – **DNS - 26 ou 27 de abril**
- Teste 3 – **NTP, VPN e PROXY - 7 ou 8 de junho**

- **Não há mínimos em nenhuma das componentes.**

Elementos de Estudo

• Principal

- Mackin, J. C., & McLean, I. (2006). MCSA/MCSE Self-Paced Training Kit (Exam 70-291): Implementing, Managing, and Maintaining a Microsoft® Windows Server(TM) 2003 Network Infrastructure, (Microsoft Press Training Kit) (2nd ed.). Microsoft Press. COTA: 1A-3-197/201
- Mackin, J. C., & McLean, I. (2006). MCSA/MCSE Self-Paced Training Kit (Exam 70-291): Implementing, Managing, and Maintaining a Microsoft® Windows Server(TM) 2003 Network Infrastructure, (Microsoft Press Training Kit) (2nd ed.). Microsoft Press. COTA: 1A-3-192
- Aidan Finn Windows Server 2012 Hyper-V Installation and Configuration Guide (1st Edition). (2013). Sybex. COTA 1A-3-244
- Granjal, J. (2021). Gestão de Sistemas e Redes em Linux (Portuguese Edition). FCA. COTA: 1A-6-201

• Secundária

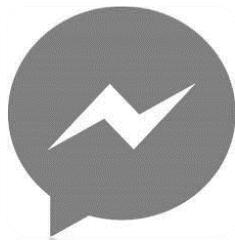
- CCNA Exploration Course Booklet: Routing Protocols and Concepts, Version 4.0 1st Edition by Academy, Cisco Networking published by Cisco Press. (2009). Cisco Press.
- Rushton, N. (2016). Windows Server 2016 Essentials Installation Guide for Small Businesses. CreateSpace Independent Publishing Platform.
- Rosa, A. (2021). Windows Server 2012 - Curso Completo (Informática ed.). FCA

Elementos de Estudo

- *Os slides são um auxiliar...*
 - *do professor para apresentação dos conteúdos;*
 - *do aluno para organização do estudo, não devendo ser o elemento principal de estudo;*
 - *nos fim de cada temática será apresentada uma lista de referências na Internet complementar à bibliografia já apresentada.*

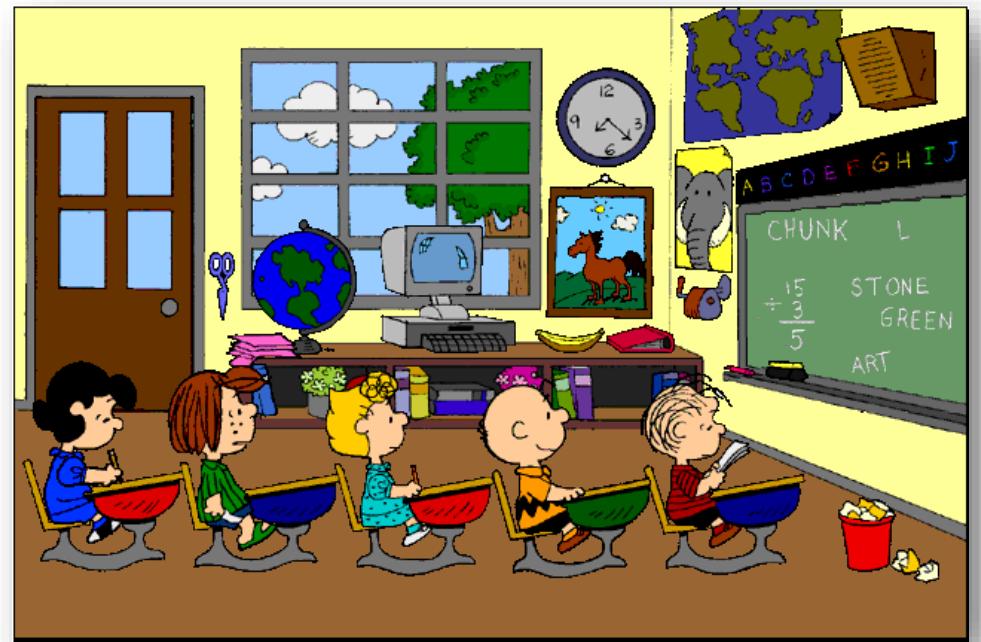
Contacto Do Docente

- **Teóricas**
 - Pedro Miguel Geirinhas (pedro.geirinhas@ccdr.pt ou pgeirinh@isec.pt)
- **Práticas**
 - Pedro Miguel Geirinhas (pedro.geirinhas@ccdr.pt ou pgeirinh@isec.pt)
- E ainda ...



Apresentação dos alunos

- O que sabe de serviços de rede?
- Qual a sua experiência nesta área?
- O que acha que vai aprender?
- Ou o que gostava de aprender?



Serviços de Rede 1

2022-2023

Pedro Miguel Geirinhas

Aula 2

Endereçamento IP

Agenda

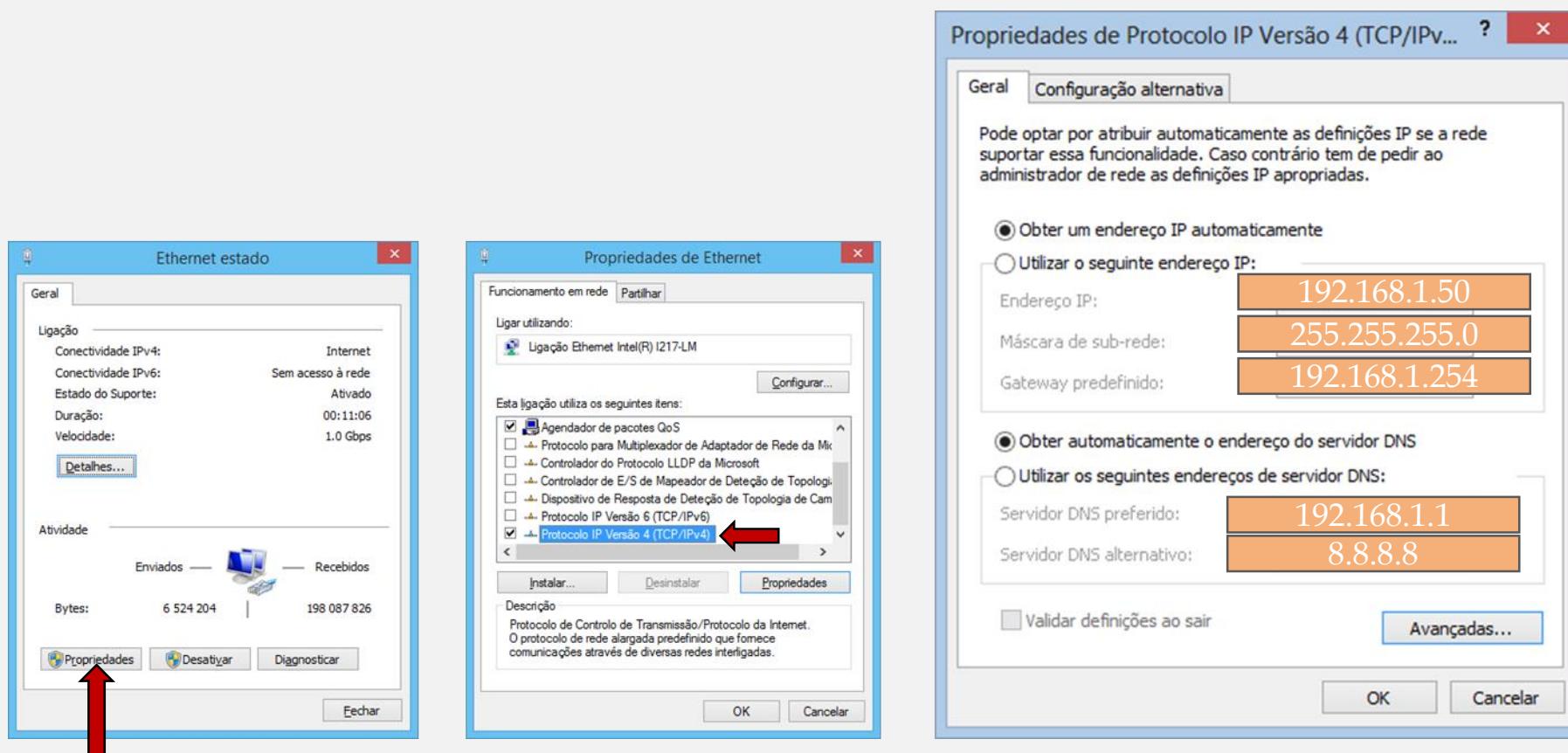
- 1** Introdução
- 2** Endereçamento IPv4 e IPv6
- 3** Classes de endereçamento
- 4** Máscara de rede
- 5** Endereçamento privado
- 6** Sub-endereçamento

Endereçamento IP

- Os principais parâmetros que devem ser configurados em qualquer equipamento que se liga a uma rede, para que o protocolo TCP/IP funcione corretamente, são os seguintes:
 - **Endereço IP** - informação que identifica conjuntamente com a máscara uma máquina na rede.
 - **Máscara de sub-rede** - informação que identifica conjuntamente com o endereço IP uma máquina na rede.
 - ***Default Gateway* ou *Gateway Predefinido*** - endereço da máquina que é responsável pelo encaminhamento dos dados para fora da rede.
 - **Endereço IP de um ou mais servidores DNS** - máquina responsável por fazer a conversão de nomes em endereços IP.

Endereçamento IP

- A configuração de um PC a correr Windows pode ser a seguinte:



Endereçamento IP

- Cada máquina é identificado por um endereço IP.
- Numa mesma rede, esse endereço **é exclusivo** de cada máquina não podendo assim existir duplicação desta identificação.
- Como um endereço postal residencial que tem um formato padrão composto por duas partes (nome da rua e número da casa), cada endereço IP é separado internamente em duas partes:
 - **identificação da rede**
 - **identificação da máquina**

Endereçamento IP v4

- Os endereços IP v4 têm tamanho fixo de 32 bits disponibilizando assim **4.294.967.296** (2^{32}) endereços diferentes.
- Exemplo de um endereço IPv4:

192.168.1.1

Nome:	Ethernet
Descrição:	Intel(R) Ethernet Connection (6) I219-V
Endereço físico (MAC):	f8:75:a4:de:fa:1c
Estado:	Não operacional
Unidade de transmissão máxima:	1500
Endereço IPv4:	169.254.131.73/16
Endereço IPv6:	fe80::91d:e92c:2c78:8349%4/64
Servidores DNS:	10.47.0.17, 10.47.0.18
Sufixo de ligação DNS:	isec.pt
Conectividade (IPv4/IPv6):	Desligado



Endereçamento IP v6

- Os endereços IPv6 têm tamanho fixo de 128 bits disponibilizando assim **340.282.366.920.938.463.463.374.607.431.768.211.456** (2^{128}) endereços diferentes, sendo apresentados em 8 grupos de 4 dígitos hexadecimais separados por ':'.
- Exemplo de um endereço IPv6

1234:5678:90AB:CDEF:FEDC:BA09:8765:4321

Nome:	Ethernet
Descrição:	Intel(R) Ethernet Connection (6) I219-V
Endereço físico (MAC):	f8:75:a4:de:fa:1c
Estado:	Não operacional
Unidade de transmissão máxima:	1500
Endereço IPv4:	169.254.131.73/16
Endereço IPv6:	fe80::91d:e92c:2c78:8349%4/64
Servidores DNS:	10.47.0.17, 10.47.0.18
Sufixo de ligação DNS:	isec.pt
Conectividade (IPv4/IPv6):	Desligado

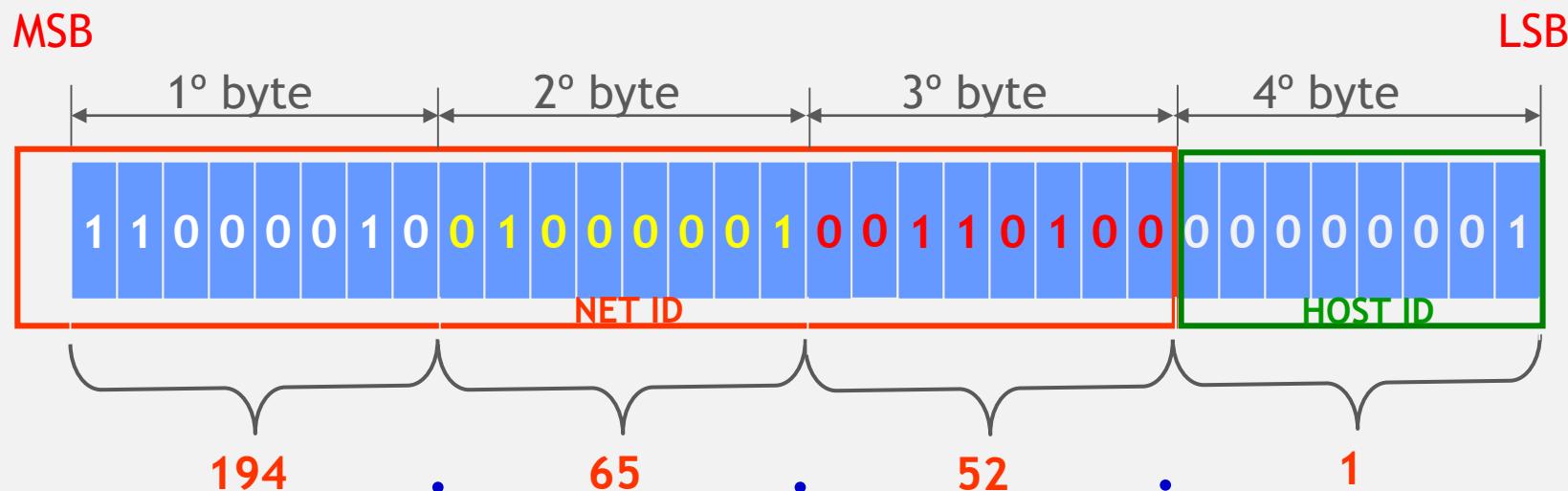
Endereçamento IP v4

- No caso do IP v4 existe uma divisão rígida da identificação da rede (**NET ID**) e das máquinas (**HOST ID**). Consideremos o exemplo:



Endereçamento IP

- Uma das formas de escrever os endereços IP é usar a notação “*dotted decimal*” do endereço IP baseada em quatro números decimais de 0 a 255, separados por pontos.
- Cada número corresponde à representação decimal de um dos 4 bytes do endereço IP.



$$1^{\text{o}} \text{ byte} = 2^7 * 1 + 2^6 * 1 + 2^5 * 0 + 2^4 * 0 + 2^3 * 0 + 2^2 * 0 + 2^1 * 1 + 2^0 * 0 = 128 + 64 + 2 = \mathbf{194}$$

$$2^{\text{o}} \text{ byte} = 2^7 * 0 + 2^6 * 1 + 2^5 * 0 + 2^4 * 0 + 2^3 * 0 + 2^2 * 0 + 2^1 * 0 + 2^0 * 1 = 64 + 1 = \mathbf{65}$$

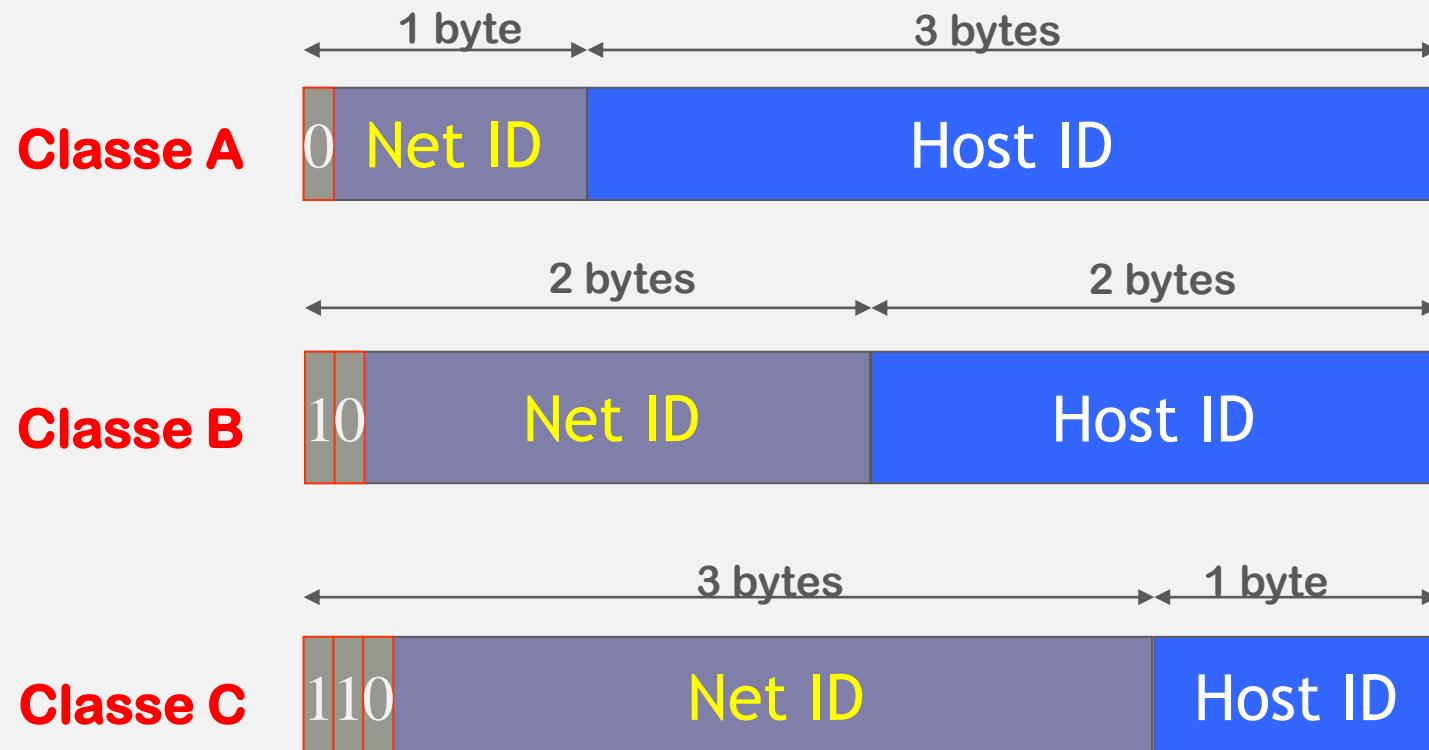
$$3^{\text{o}} \text{ byte} = 2^7 * 0 + 2^6 * 0 + 2^5 * 1 + 2^4 * 1 + 2^3 * 0 + 2^2 * 1 + 2^1 * 0 + 2^0 * 0 = 32 + 16 + 4 = \mathbf{52}$$

Endereçamento IP

- O crescimento viral da Internet implicou uma análise mais estruturada do endereçamento a utilizar e o primeiro passo foi a sua divisão em classes.
- Divisão do espaço de endereçamento em 3 classes:
 - Classe A
 - Classe B
 - Classe C
- Existem ainda as classes D e E mas que são de uso limitado ou reservado pelo que não são objeto de estudo nesta disciplina.
- Objetivo para esta divisão é a necessidade de **escalabilidade** e **flexibilidade** da estrutura de endereçamento a utilizar.

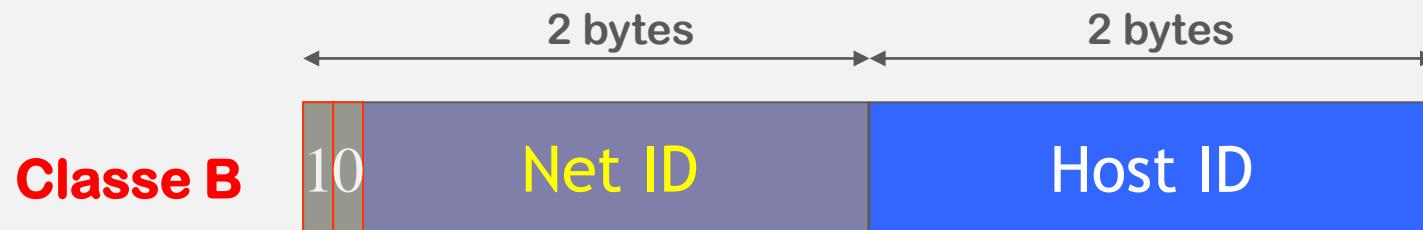
Endereçamento IP

- São estas as classes propostas:



Endereçamento IP

- Qual o número máximo de redes que podemos ter em cada um das classes?
- Em cada classe podemos ter **2^N º de bits do net ID** de redes.
- Por exemplo na classe B teremos 16.384 redes ou seja **2^{6+8}** :



- No caso da classe A teremos de retirar duas redes que estão reservadas:
 - endereço 0.0.0.0 (ou seja todos os bits a “0”) que é reservado para uso como a rota default.
 - endereço 127.0.0.0 é reservado para a função de *loopback* ou de *localhost* (pode por exemplo ser utilizado para as aplicações TCP se testarem)

Endereçamento IP

- Em todas as redes há endereços reservados para efeitos especiais e que não podem ser atribuídos a *hosts*:
 - **Todos os bits do host id a 0** - Endereço que identifica a rede
 - **Todos os bits do host id a 1** - Endereço de *broadcast* (quando um dispositivo envia uma mensagem a todos os dispositivos da rede)
 - **Por exemplo:**
 - na rede 192.168.1.0 (classe C) há 256 endereços disponíveis. Desde o 192.168.1.0 até ao 192.168.1.255. Como o primeiro é utilizado para designar a rede e o último é o endereço de *broadcast* só estão disponíveis para máquinas desde o 192.168.1.1 até 192.168.1.254 ou seja 254.
- Temos assim numa rede **$2^{N^{\circ} \text{ de bits do host ID } - 2}$** endereços disponíveis para as máquinas/equipamentos periféricos.

Endereçamento IP

- O espaço de endereçamento por classe é o seguinte:

Classe	1º byte	Nº de bits para o NET ID	Nº de Redes	Nº de bits para o HOST ID	Nº de Máquinas por rede
A	0 - 126	7 (8-1)	126 ($2^7 - 2$)	24	16.777.214 ($2^{24}-2$)
B	128 - 191	14 (8-2+8)	16.384 (2^{14})	16	65.534 ($2^{16}-2$)
C	192 - 223	21(8-3+8+8)	2.097.152 (2^{21})	8	254 (2^8-2)

Endereçamento IP

- E qual é a primeira e última rede de cada classe? Vamos considerar a classe C como exemplo:



- A primeira rede será **11000000.00000000.00000000.00000000**

192.0.0.0

- A última rede será **11011111.11111111.11111111.00000000**



223.255.255.0

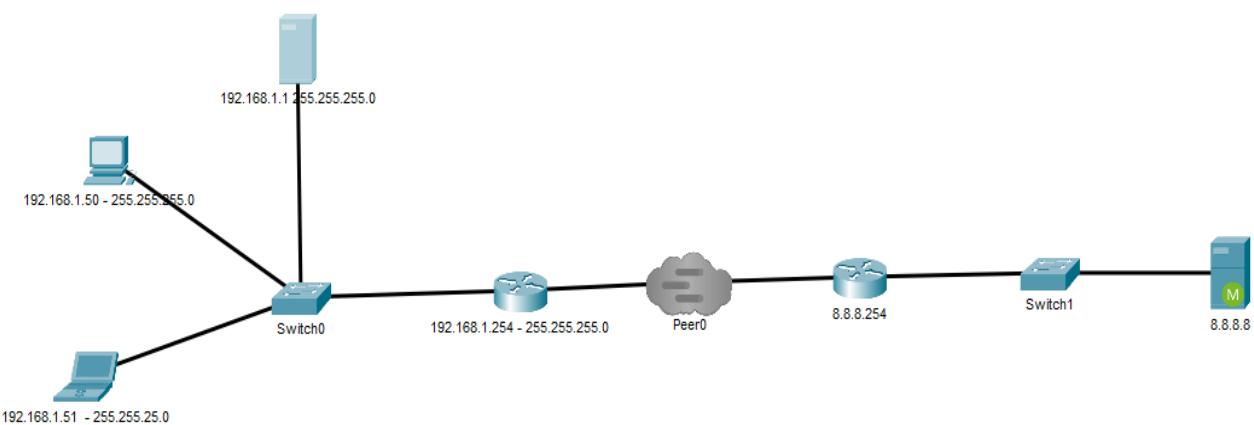
Endereçamento IP

- A que rede pertence o endereço 192.168.200.225? Podemos dizer que é uma classe C. Mas se tiver sub-redes? A resposta é assim tão fácil?
- Para que um endereço esteja corretamente definido, deve-se indicar quantos bits fazem parte da rede (net Id) e dos dispositivos (host id). Isso é feito pela **máscara de rede!**
- A máscara de rede:
 - Indica a fronteira entre a identificação da rede e do *host*.
 - Também é formada por 32 bits agrupados em conjunto de 1 byte cada.

Endereçamento IP

- O binário 1 na máscara de rede indica que esse bit pertence à identificação da rede (*net*) e o binário 0 indica que pertence ao dispositivo (*host*).
- Temos assim:
 - Classe A - 255.0.0.0
 - Classe B - 255.255.0.0
 - Classe C - 255.255.255.0
- A máscara pode ser representada num formato idêntico ao endereço IP com quatro bytes separados por pontos, ou no formato barra (/). Neste formato explicitamos o número de bits que se utiliza na identificação da rede.
- Temos assim:
 - Classe A - /8
 - Classe B - / 16
 - Classe C - /24

Endereçamento IP



- **Desafio:**

- Qual o endereço IP do PC?
- Qual a máscara da sub-rede do portátil?
- Qual o IP do *default gateway* que devemos colocar nos equipamentos da rede do lado esquerdo? e na máquina da rede do lado direito?
- E os servidores de DNS?
- O DNS pode estar numa rede fora da nossa rede?
- E o *default gateway* pode estar fora da nossa rede?

Endereços Púlicos *versus* Endereços Privados

- Problema "*Com o crescimento da Internet, não existem endereços suficientes para ligar todas as máquinas.*"
- Uma das forma de resolver este problema foi estabelecer um conjunto de endereços de uso privado para colocar nas máquinas sem acesso à Internet (**endereços privados**).
- Os endereços utilizados na Internet são **endereços públicos**.

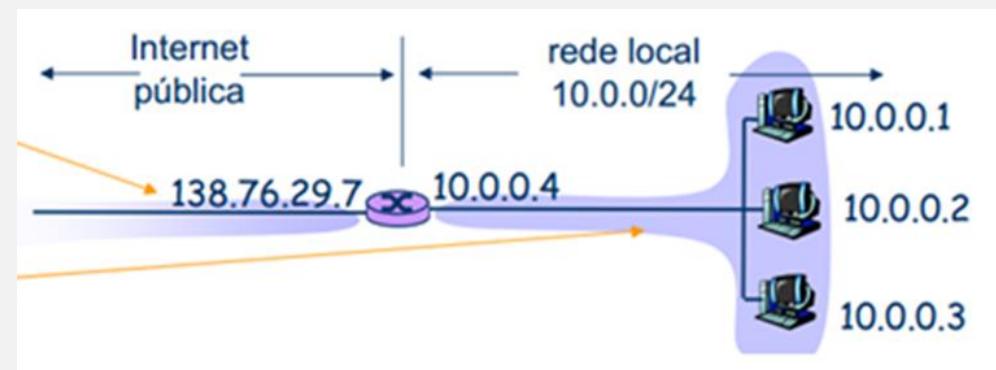
Redes Privadas

- As redes privadas utilizam um conjunto específico de endereços. Temos assim por classe:

Classe	De...	...A
A	10.0.0.0	10.255.255.255
B	172.16.0.0	172.31.255.255
C	192.168.0.0	192.168.255.255

Redes Privadas

- Estes conjuntos de endereços estão reservados para utilização em redes privadas.
- Podem ser usados por milhões de equipamentos em simultâneo.
- Os pacotes contendo esses endereços **não podem** ser encaminhados para o exterior/internet.



Redes Privadas

- As máquinas com endereços privados não podem aceder directamente à internet.
- Os endereços públicos são um recurso limitado e atualmente escasso.
 - Não existem endereços suficientes para fazer face à quantidade de equipamentos que se encontram interligados.
- Contudo as máquinas têm de aceder e ser acedidas através da internet.
- Soluções:
 - IP v6
 - Máquinas intermédias a prestar os serviços pretendidos de forma indirecta (ex. *Proxys*).
 - Tradução de endereços privados em endereços públicos (NAT).

Redes Privadas

- A sua utilização não é sujeita a licenciamento.
- Routers não podem propagar para a Internet informação sobre estas redes.
- Tráfego com origem e destino privados não devem utilizar a Internet.
- Referência a endereços privados não devem ser publicitadas (DNS).

Sub-Endereçamento

- Outra solução para “poupar” endereços, passa pelo sub-endereçamento que não é mais do que a subdivisão de uma classe de endereçamento IP em um conjunto de redes menores.
- Quantas sub-redes podemos ter ?
 - $N=2^X$ onde o X representa o nº de bits que foram “emprestados” pelo *host id*.
- Quantos hosts temos por cada sub-rede?
 - $N=2^X-2$ onde o X representa o nº de bits usados para o *host id* ou seja que estão a “0” da máscara rede.
 - **Não se esqueça** que em cada rede todos os bits do *host id* a 0 indica/identifica a rede e todos a 1 indica o *broadcast* dessa rede, daí a razão do -2.

Sub-endereçamento

- Consideremos que estamos a fazer sub-endereçamento de uma rede classe C (ou seja /24), podemos “partir” essa rede em outras sub-redes da seguinte forma:

Nº de sub-redes	Nº de bits rede	máscara	Nº de hosts
2 (2^1)	25 (24+1)	255.255.255.128	126 (2^7 -2)
4 (2^2)	26 (24+2)	255.255.255.192	62 (2^6 -2)
8 (2^3)	27 (24+3)	255.255.255.224	30
16 (2^4)	28 (24+4)	255.255.255.240	14
32 (2^5)	29 (24+5)	255.255.255.248	6
64 (2^6)	30 (24+6)	255.255.255.252	2
128 (2^7)	31 (24+7)	255.255.255.254	0

Sub-endereçamento

Classe A

Tabela de host/sub-rede classe A

Class A Number of Bits Borrowed from Host Portion	Subnet Mask	Effective Subnets	Number of Hosts/Subnet	Number of Subnet Mask Bits
1	255.128.0.0	2	8388606	/9
2	255.192.0.0	4	4194302	/10
3	255.224.0.0	8	2097150	/11
4	255.240.0.0	16	1048574	/12
5	255.248.0.0	32	524286	/13
6	255.252.0.0	64	262142	/14
7	255.254.0.0	128	131070	/15
8	255.255.0.0	256	65534	/16
9	255.255.128.0	512	32766	/17
10	255.255.192.0	1024	16382	/18
11	255.255.224.0	2048	8190	/19
12	255.255.240.0	4096	4094	/20
13	255.255.248.0	8192	2046	/21
14	255.255.252.0	16384	1022	/22
15	255.255.254.0	32768	510	/23
16	255.255.255.0	65536	254	/24
17	255.255.255.128	131072	126	/25
18	255.255.255.192	262144	62	/26
19	255.255.255.224	524288	30	/27
20	255.255.255.240	1048576	14	/28
21	255.255.255.248	2097152	6	/29
22	255.255.255.252	4194304	2	/30
23	255.255.255.254	8388608	2*	/31

Sub-endereçamento

Tabela de host/sub-rede classe B

Class B Bits	Subnet Mask	Effective Subnets	Effective Hosts	Number of Subnet Mask Bits
1	255.255.128.0	2	32766	/17
2	255.255.192.0	4	16382	/18
3	255.255.224.0	8	8190	/19
4	255.255.240.0	16	4094	/20
5	255.255.248.0	32	2046	/21
6	255.255.252.0	64	1022	/22
7	255.255.254.0	128	510	/23
8	255.255.255.0	256	254	/24
9	255.255.255.128	512	126	/25
10	255.255.255.192	1024	62	/26
11	255.255.255.224	2048	30	/27
12	255.255.255.240	4096	14	/28
13	255.255.255.248	8192	6	/29
14	255.255.255.252	16384	2	/30
15	255.255.255.254	32768	2*	/31

Classe B

Host classe C/Tabela de sub-rede

Class C Bits	Subnet Mask	Effective Subnets	Effective Hosts	Number of Subnet Mask Bits
1	255.255.255.128	2	126	/25
2	255.255.255.192	4	62	/26
3	255.255.255.224	8	30	/27
4	255.255.255.240	16	14	/28
5	255.255.255.248	32	6	/29
6	255.255.255.252	64	2	/30
7	255.255.255.254	128	2*	/31

Classe C

Sub-endereçamento

- Considere agora o exemplo:
 - Tem uma rede 193.137.78.0/24 e deseja “partir” esta rede em 8 sub-redes.
 - Para isso necessita de 3 ($8=2^3$) bits adicionais no último byte do endereço para o *net id*. Temos assim na máscara:

11111111. 11111111. 11111111. 11100000



Nº de bits para o <i>network id</i>	27 (24+3)
Nº de bits para os <i>host id</i>	5 (32-27 ou 8-3)
Nº de sub-redes	$2^3=\mathbf{8}$
Nº de <i>hosts</i> por rede	$2^5-2=\mathbf{30}$

Sub-endereçamento

- Mas como posso calcular as diferentes sub-redes?
 - **1º Processo:** Fazer as 8 combinações possíveis dos bits que está a utilizar do *host id* para o *network id*.

Bits	Resultado	Rede
000	$2^7*0+2^6*0+2^5*0=0$	193.137.78.0
001	$2^7*0+2^6*0+2^5*1=32$	193.137.78.32
010	$2^7*0+2^6*1+2^5*0=64$	193.137.78.64
011	$2^7*0+2^6*1+2^5*1=96$	193.137.78.96
100	$2^7*1+2^6*0+2^5*0=128$	193.137.78.128
101	$2^7*1+2^6*0+2^5*1=160$	193.137.78.160
110	$2^7*1+2^6*1+2^5*0=192$	193.137.78.192
111	$2^7*1+2^6*1+2^5*1=224$	193.137.78.224

Sub-endereçamento

- Mas como posso calcular as diferentes sub-redes?
 - **2º Processo:** Fazer “contas” utilizando a informação da tabela.

Primeira rede - 193.137.78.0

Segunda rede - Primeira rede + n^o de host + 2
193.137.78.(0+30+2=32)

Terceira rede - Segunda rede + n^o de hosts + 2
193.137.78.(32+30+2=64)

Nº de bits para o <i>network id</i>	27 (24+3)
Nº de bits para os <i>host id</i>	5 (32-27ou 8-3)
Nº de sub-redes	2³=8
Nº de <i>hosts</i> por rede	2⁵-2=30

Sub-endereçamento

- Podemos agora construir a tabela completa das sub-redes. Assim para cada uma das sub-rede temos:
 - O primeiro endereço identifica a rede.
 - O primeiro endereço disponível será o da rede mais 1.
 - O último endereço será o de *broadcast*.
 - O último endereço disponível será o endereço de *broadcast* menos 1.

Rede	Sub-rede	1º Host	Último host	Broadcast
1ª sub-rede	192.137.78.0	192.137.78.1	192.168.78.30	192.1637.78.31
2ª sub-rede	193.137.78.32	193.137.78.33	193.137.78.62	193.137.78.63
3ª sub-rede	193.137.78.64	193.137.78.65	193.137.78.94	193.137.78.95
4ª sub-rede	193.137.78.96	193.137.78.97	193.137.78.126	193.137.78.127
5ª sub-rede	192.137.78.128	193.137.78.129	193.137.78.158	193.137.78.159
6ª sub-rede	192.137.78.160	193.137.78.161	193.137.78.190	193.137.78.191
7ª sub-rede	192.137.78.192	193.137.78.193	193.137.78.222	193.137.78.223
8ª sub-rede	192.137.78.224	193.137.78.225	193.137.78.254	193.137.78.255

Sub-endereçamento

- E a máscara de sub-rede de cada uma destas sub-redes como é calculada?
- A rede “mãe” tem a máscara 255.255.255.0 como está a utilizar 3 bits do último byte para o *net id* na máscara estes bits têm de estar a “1”. Ou seja:

11111111.11111111.11111111.**111**00000

255 . 255 . 255 . $2^7+2^6+2^5= \mathbf{224}$

- Sendo esta máscara de sub-rede e igual para todas as oito sub-redes criadas.

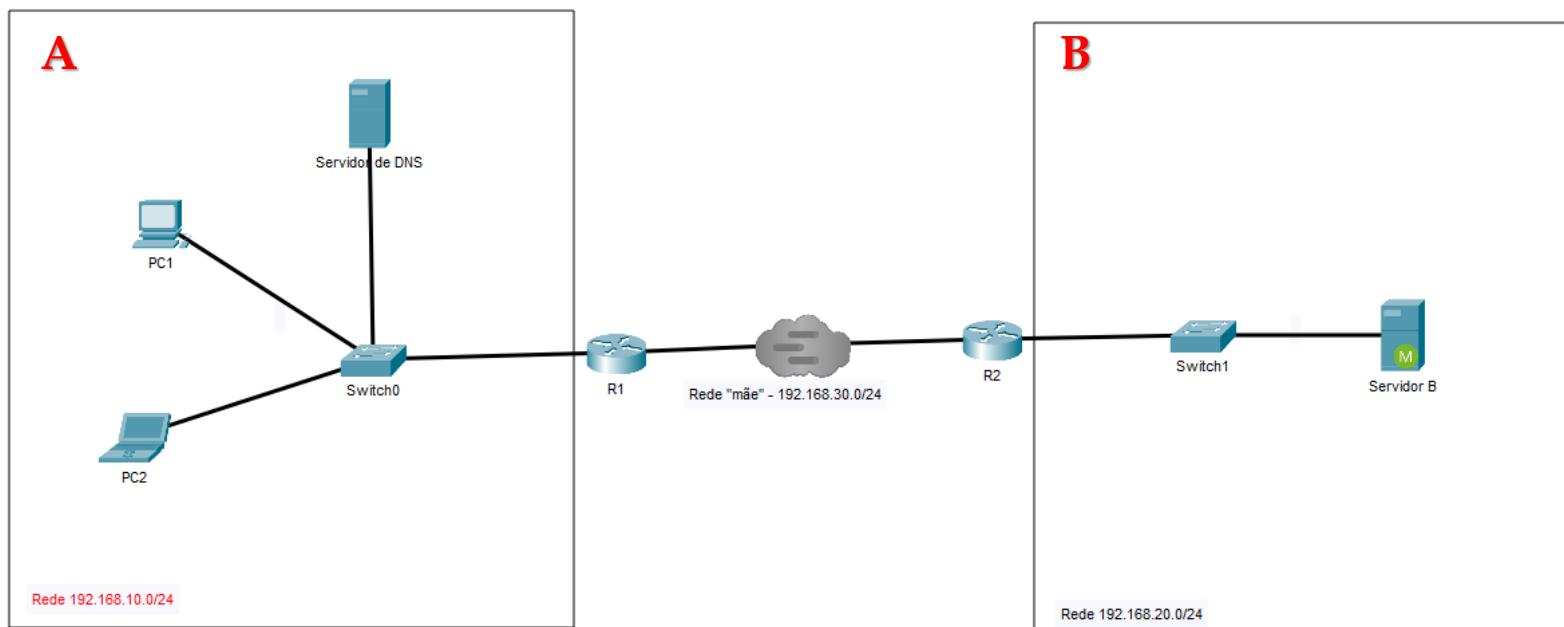
Sub-endereçamento

- Para determinar a rede de uma dada máquina só tem que fazer o AND do endereço com a máscara de rede.
- Considere a máquina com o endereço 10.20.237.15 e máscara 255.255.248.0 (ou seja 10.20.237.15/21), a sua rede é:

	10	20	237	15
AND	255	255	248	0
	10	20	232	0

	00001010	00010100	11101101	00001111	Mask
AND	11111111	11111111	11111000	00000000	
	00001010	00010100	11101000	00000000	

Desafio



• Rede A:

- O router deve estar no último endereço disponível. A interface que o liga à rede local é f0/0
- O servidor deve estar no primeiro endereço disponível.
- Os PC no endereço 50 e seguinte da rede.

• Rede B:

- O router deve estar no último endereço disponível. A interface que o liga à rede local é f0/0
- O servidor deve estar no primeiro endereço disponível.

• Rede de ligação entre os router:

- A sub-rede deve apenas ter dois host.
- Os router usam a interface s0/0 para ligação.

Desafio

- Qual o endereço IP do PC1? E a máscara de rede?
- Qual o *default gateway* que deve colocar em todas as máquinas da rede A?
- Qual o endereço que deve colocar na interface do router que liga à rede A?
- Qual é a identificação da rede B?
- Qual o endereço IP do servidor da rede B?
- Qual o endereço de *broadcast* da rede A? E o da rede B?
- Qual a rede que deve usar para as interfaces serial dos routers?
- Qual a máscara de rede dessa rede?
- Que endereços deve colocar nos interfaces serial dos router?
- Se desejar usar a próxima rede, qual a sua identificação? E qual o primeiro endereço disponível? E qual o endereço de *broadcast*?

Desafio - Respostas

- Qual o endereço IP do PC1? **192.168.10.50** E a máscara de rede? **255.255.255.255.0**
- Qual o *default gateway* que deve colocar em todas as máquinas da rede A? **192.168.10.254**
- Qual o endereço que deve colocar na interface do router que liga à rede A? **192.168.10.254**
- Qual é a identificação da rede B? **192.168.20.20/24**
- Qual o endereço IP do servidor da rede B? **192.168.20.1**
- Qual o endereço de *broadcast* da rede A? **192.168.10.255** E o da rede B? **192.168.20.255**
- Qual a rede que deve usar para as interfaces serial dos routers? **192.168.30.0/30**
- Qual a máscara de rede dessa rede? **255.255.255.252**
- Que endereços deve colocar nos interfaces serial dos router? **192.168.30.1 255.255.255.252 e 192.168.30.2 255.255.255.252**
- Se desejar usar a próxima rede, qual a sua identificação? **192.168.30.4/30** E qual o primeiro endereço disponível? **192.168.30.5 255.255.255.252** E qual o endereço de *broadcast*? **192.168.30.7 255.255.255.252**

Dúvidas



Serviços de Rede 1

2022-2023

Pedro Miguel Geirinhas

Aula 3

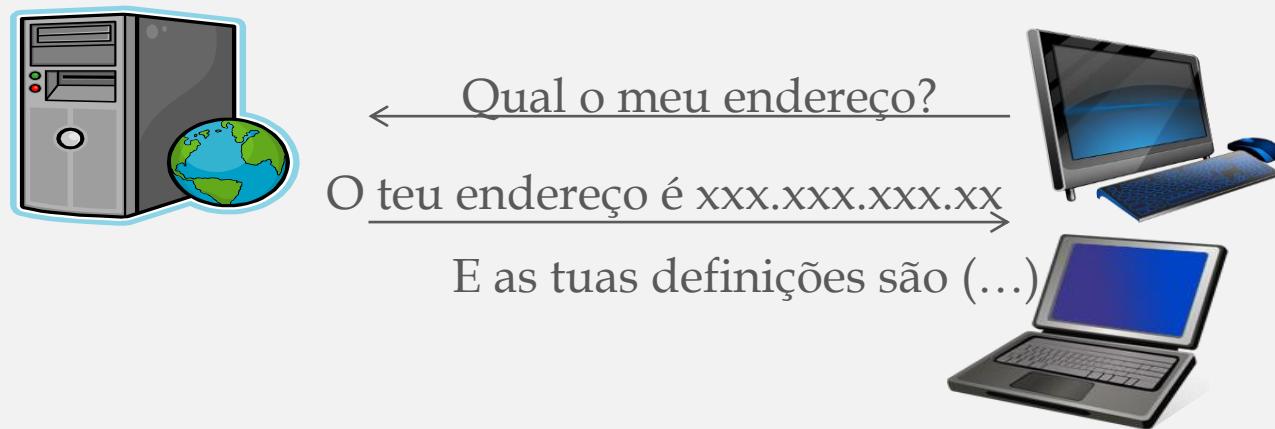
Dynamic Host Configuration Protocol (DHCP)

Agenda

- 1.** MAC (*Media Access Control*)
- 2.** ARP (*Address Resolution Protocol*)
- 3.** RARP (*Reverse Address Resolution Protocol*)
- 4.** BOOTP (*BOOTstrap Protocol*)
- 5.** DHCP (*Dynamic Host Configuration Protocol*)

Atribuição dinâmica de informação IP

- Se a sua rede tiver 5 computadores, o trabalho e os erros que pode cometer na atribuição e configuração manual dos endereços são poucos.
- Mas se a sua rede tiver 300 ou mais máquinas? Com máquinas portáteis sempre a entrar e a sair da rede? Não seria fácil configurar manualmente todos os endereços.
- Solução: arranjar um serviço centralizado que faça essa função de forma automática.

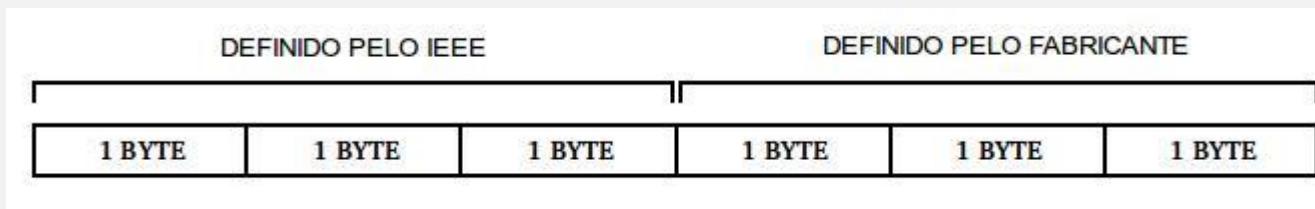


Endereço MAC (*Media Access Control*)

- Cada máquina com uma placa de rede possui uma identificação única e que não se repete.
- Esta identificação é uma sequência de bits, que se chama o endereço físico na rede (**MAC address**).
- O endereço MAC é formado por um conjunto de 6 bytes separados por dois pontos (“：“) ou hífen (“-”), sendo cada byte representado por dois algarismos na forma hexadecimal, como por exemplo: "00:19:B9:FB:E2:58". Cada algarismo em hexadecimal corresponde a uma palavra binária de quatro bits, desta forma, os 12 algarismos que formam o endereço totalizam 48 bits.

Endereço MAC (*Media Access Control*)

- Há um padrão para os endereços MAC que é administrada pela IEEE (*Institute of Electrical and Electronics Engineers*) que define:
 - Os três primeiros bytes - chamados OUI (*Organizationally Unique Identifier*), e que são destinados a identificação do fabricante são fornecidos pela própria IEEE.
 - Os três últimos bytes são definidos pelo fabricante, sendo este responsável pelo controle da numeração de cada placa que produz.



- O endereço MAC é único no mundo para cada placa de rede (apesar de existirem ferramentas que possibilitam a sua alteração), e é mantido na memória ROM , sendo posteriormente essa informação copiada para a memória RAM aquando da inicialização da placa.

Endereço MAC (*Media Access Control*)

```
Placa de rede local sem fios Ligação de rede sem fios:  
Estado do suporte : Suporte desligado  
Sufixo DNS específico da ligação :  
Descrição : Placa LAN Sem Fios 802.11n  
Endereço físico : 00-22-5F-55-91-D9  
DHCP activado : Sim  
Autoconfiguração activada : Sim  
  
Adaptador ethernet Ligação de Área Local:  
Sufixo DNS específico da ligação : ccdrc.global  
Descrição : Realtek PCIe GBE Family Controller  
Endereço físico : 00-23-54-A4-04-FD  
DHCP activado : Sim  
Autoconfiguração activada : Sim  
Endereço IPv6 de local de ligação : fe80::8091:72:f2ca:e150%11<Preferido>  
Endereço IPv4 : 10.9.35.199<Preferido>  
Máscara de sub-rede : 255.255.255.0  
Concessão obtida : quinta-feira, 5 de Março de 2015 08:56:39  
Concessão obtida válida até : quinta-feira, 5 de Março de 2015 17:26:23
```

Endereço MAC de duas placas de rede de uma máquina

ARP - *Address Resolution Protocol*

1) Quando pretendemos comunicar com outra máquina, o que precisamos de saber?

- Endereço IP (ou o nome que depois é traduzido num endereço IP).

2) Qual a informação que é inserida numa frame relativamente ao destinatário?

- O MAC Address do PC de destino (endereço físico) é incluído na frame.

3) Mas se eu só sei o IP, como descobrir o MAC do PC de destino?

- Recorrendo ao protocolo ARP, que permite obter o endereço MAC (do PC de destino) usando o endereço IP (do PC de destino).

4) No caso do envio de informação para fora do domínio da rede local, o endereço físico a ser registado na tabela ARP de um PC local será o endereço físico do *gateway*.

ARP - *Address Resolution Protocol*

- Sempre que uma máquina começa a comunicar com outra é consultada a sua tabela de ARP.
- Se o endereço pedido não se encontrar na tabela, o protocolo ARP emite um pedido para a rede (ARP Request).
- As máquinas ligadas na rede vão comparar o endereço IP (endereço lógico) do pedido ao seu.
- Se alguma das máquinas reconhecer o seu endereço IP no pedido vai responder enviando um (ARP Reply).
- Esta resposta vai conter o endereço físico (MAC) da máquina destino, que será guardado na tabela de ARP da máquina origem

ARP - Address Resolution Protocol

```
Linha de comandos
Microsoft Windows [Version 6.3.9600]
(c) 2013 Microsoft Corporation. Todos os direitos reservados.

C:\Users\pgeirinhas>arp -a

Interface: 10.9.35.199 --- 0x3
 Internet Address Physical Address      Type
 10.9.35.1          78-fe-3d-4f-2a-c1  dynamic
 10.9.35.255        ff-ff-ff-ff-ff-ff  static
 224.0.0.22         01-00-5e-00-00-16  static
 224.0.0.251        01-00-5e-00-00-fb  static
 224.0.0.252        01-00-5e-00-00-fc  static
 239.255.255.250   01-00-5e-7f-ff-fa  static

Interface: 192.168.206.1 --- 0xa
 Internet Address Physical Address      Type
 192.168.206.255   ff-ff-ff-ff-ff-ff  static
 224.0.0.22         01-00-5e-00-00-16  static
 224.0.0.251        01-00-5e-00-00-fb  static
 224.0.0.252        01-00-5e-00-00-fc  static
 239.255.255.250   01-00-5e-7f-ff-fa  static

Interface: 192.168.196.1 --- 0xc
 Internet Address Physical Address      Type
 192.168.196.255   ff-ff-ff-ff-ff-ff  static
 224.0.0.22         01-00-5e-00-00-16  static
 224.0.0.251        01-00-5e-00-00-fb  static
 224.0.0.252        01-00-5e-00-00-fc  static
 239.255.255.250   01-00-5e-7f-ff-fa  static

C:\Users\pgeirinhas>
```



<https://blog.pantuza.com/artigos/o-protocolo-arp-address-resolution-protocol>

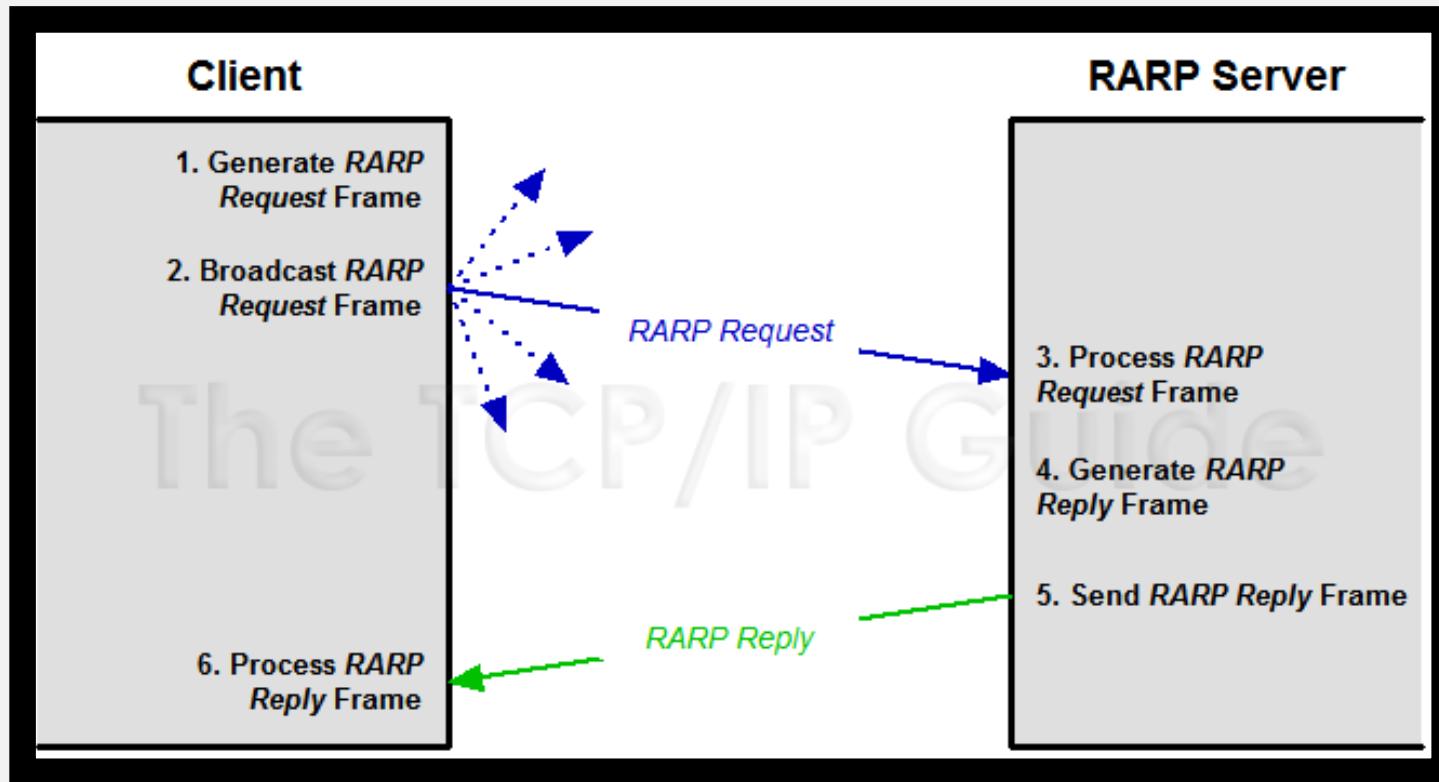
RARP (Reverse Address Resolution Protocol)

- O equipamento tem de utilizar um protocolo que permite a obtenção do endereço IP fazendo uso do endereço físico da placa (o MAC address).
- O primeiro protocolo para fazer esta tarefa foi o **RARP**.
- O RARP atribui assim a um endereço MAC um endereço IP.
- Um dispositivo de rede, como uma estação de trabalho sem disco, por exemplo, pode conhecer seu endereço MAC, mas não seu endereço IP. O RARP permite que o dispositivo faça uma solicitação para saber o seu endereço IP.
- Os dispositivos que usam este protocolo exigem que haja um servidor RARP presente na rede para responder as estas solicitações.

RARP

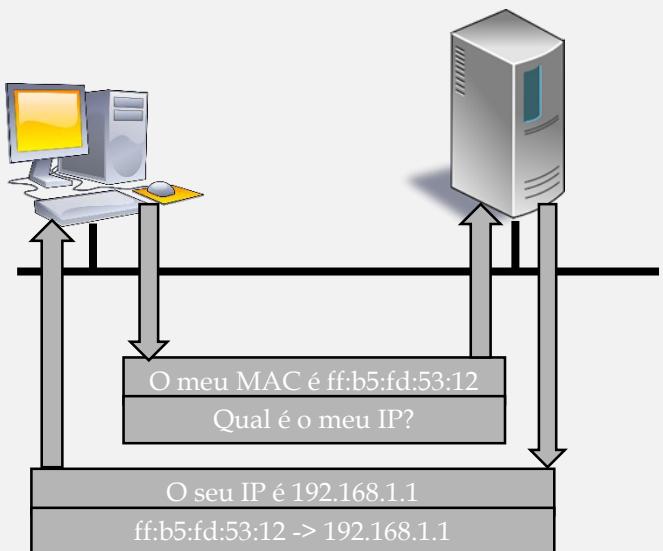
- A comunicação é feita a partir da difusão da solicitação de uma estação na rede local para aquisição de um endereço IP. A estação remete, na mensagem, o endereço MAC no campo **target HA**.
- Somente os servidores RARP irão processar a mensagem enviada.
- Os servidores respondem às solicitações preenchendo o campo **tipo de protocolo**, mudando o campo **operação de solicitação** para **resposta** e enviando a mensagem diretamente a máquina.
- Esta recebe as respostas de todos os servidores RARP, mesmo tendo aceito a primeira.
- A partir deste momento, a máquina só utilizará o RARP novamente se for feita uma reinicialização do sistema.

RARP



RARP X ARP

RARP



ARP

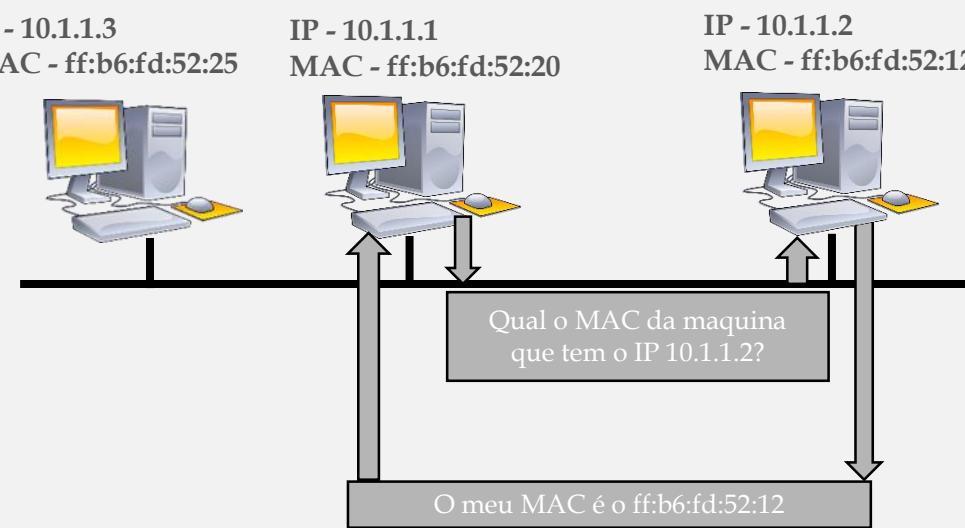


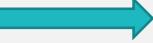
Tabela ARP
10.1.1.2 ->ff:b6:fd:52:12

Tabela ARP
10.1.1.1 ->ff:b6:fd:52:20

RARP - Limitações

- Os servidores RARP precisam de estar na mesma rede dos seus clientes.
- Por operarem tão próximo do hardware da máquina complicavam o desenvolvimento de aplicações cliente-servidor.
- Não conseguiam ter mecanismos automáticos de atribuição de endereços.
- A troca de informação entre os clientes e o servidor estava limitada apenas a um endereço IP.
- Foi assim substituído pelo **BOOTP** (*BOOtstrap Protocol*).

BOOTP (*BOOtstrap Protocol*)

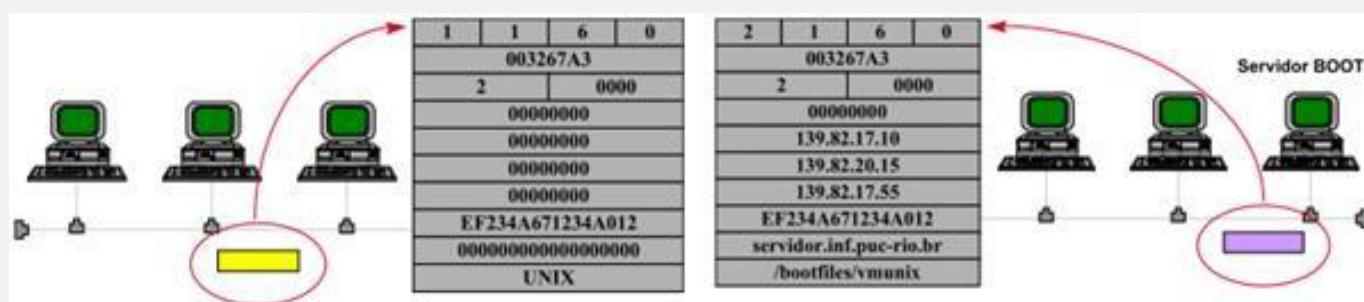
- O BOOTP é um protocolo de configuração de servidor desenvolvido antes do DHCP.
- O BOOTP é definido pelo RFC 951. 
- Baseia-se:
 - Numa única troca de mensagens.
 - Transfere muito mais informação do que o RARP.
 - Como utiliza o UDP é muito mais fácil de programar.
 - Prevê apenas um mapeamento estático entre um identificador da máquina e um conjunto de parâmetros para aquela máquina.

Nota:

Os protocolos e normas são definidos em documentos conhecidos como RFCs (Request for Comments)

<http://www.rfc-editor.org/>

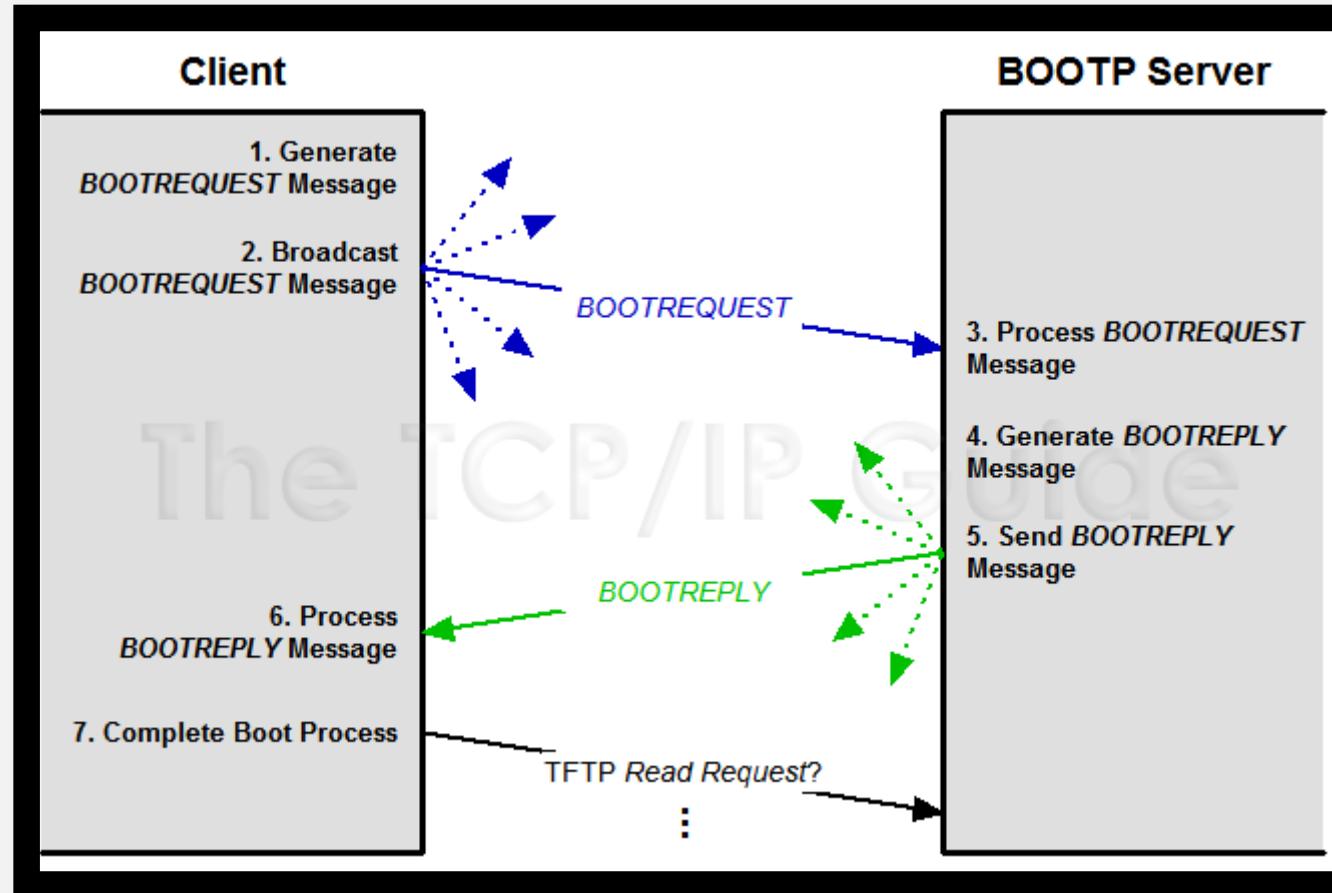
BOOTP (*Bootstrap Protocol*)



0	7	15	23	31
Octeto 1	Octeto 2	Octeto 3	Octeto 4	
OP (1=Req,2=Rep)				
HW TYPE				
HLENGTH				
HOPS				
TRANSACTION ID				
SECONDS (tempo desde o boot)				
UNUSED				
CLIENT IP ADDRESS (se cliente souber)				
YOUR IP ADDRESS				
SERVER IP ADDRESS				
GATEWAY IP ADDRESS				
CLIENT HARDWARE ADDRESS (16 OCTETS)				
SERVER HOST NAME (64 OCTETS)				
BOOT FILE NAME (128 OCTETS)				
VENDOR-SPECIFIC AREA (64 OCTETS)				

<https://notloaded.files.wordpress.com/2011/08/image002.jpg>

BOOTP (*BOOtstrap Protocol*)

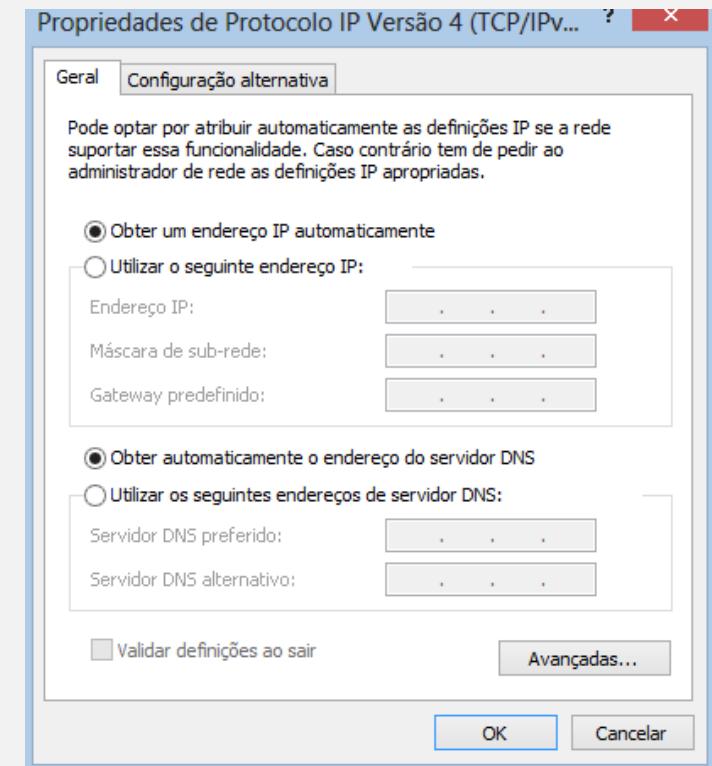


BOOTP - Limitações

- Limitações:
 - Não permite a configuração dinâmica das máquinas.
 - Não permite a reutilização de endereços IPs para diferentes máquinas.
 - Só permite 4 parâmetros de opções.
- Com os portáteis e as redes móveis era necessário encontrar outro protocolo de inicialização.
- Assim surge o ***Dynamic Host Configuration Protocol***

DHCP (*Dynamic Host Configuration Protocol*)

- DHCP é a sigla para Dynamic Host Configuration Protocol. Trata-se de um protocolo utilizado em redes de equipamentos terminais que lhes permite obter um endereço IP de forma automática.
- Oferece configuração dinâmica de terminais, com concessão de endereços IP de host e outros parâmetros de configuração para clientes de rede.



DHCP (*Dynamic Host Configuration Protocol*)

- Surgiu como padrão em Outubro de 1993.
- O RFC 2131 e RFC 2131 contêm as especificações mais atuais (Março de 1997).
- A última norma para a especificação do DHCP sobre IPv6 (DHCPv6) foi publicado a Julho de 2003 como RFC 3315.
- O DHCP é no essencial uma versão melhorada e estendida do BOOTP, funcionando, tal como este, em modo cliente-servidor e possibilitando a obtenção automática de endereços IP, nomes de servidores, máscara de sub-rede e gateway de defeito.

DHCP - Vantagens

- Automação do processo de configuração do protocolo TCP/IP nos dispositivos da rede.
- Facilidade de alteração de parâmetros tais como *Default Gateway*, Servidor DNS etc., em todos os dispositivos da rede, através de uma simples alteração no servidor DHCP.
- Eliminação de erros de configuração, tais como escrita incorreta de uma máscara de sub-rede ou utilização do mesmo número IP em dois equipamentos diferentes, gerando um conflito de endereço IP.
- Os endereços IP são renovados em intervalos de tempo pré-definidos no servidor. Pode ainda configurar que o IP ficará livre quando o host se desligar da rede.

DHCP

- Podemos ter vários mecanismos de alocação de endereços:
 - **Manual ou estática**
 - O administrador configura no servidor DHCP o IP a atribuir a cada máquina através da utilização do seu MAC. Ou seja é atribuído um determinado IP a uma máquina específica.
 - **Dinâmica**
 - O serviço DHCP atribui endereços IP a um equipamento, entre um conjunto de endereços disponíveis **por um intervalo de tempo pré-definido**.
 - Endereço é atribuído por um período de tempo limitado – aluguer (lease)
 - Quando for libertado (explicitamente ou por não renovação), fica disponível para atribuir a outras máquinas.
 - **Automática**
 - É uma mistura dos dois mecanismos anteriores. O serviço DHCP atribui automaticamente um IP estático a um equipamento, entre um conjunto de endereços disponíveis.
 - Servidor guarda associação do endereço atribuído ao Client Identifier (ou MAC Address) do cliente
 - Sempre que o cliente pedir um endereço, é-lhe atribuído o mesmo.

DHCP - Termos

- **Servidor:**

- Deve ser configurado pelo administrador da rede para disponibilizar aos clientes, endereços IP numa das três formas de fornecimento descritas.
- É importante deixar endereços fixos em algumas máquinas os seus endereços IP (por exemplo os routers e os servidores).
- Deve ainda ser estabelecido o prazo de locação de um endereço. Esse prazo pode variar de horas a dias ou simplesmente ser ilimitado.

- **Cliente:**

- Um cliente DHCP é um equipamento que está configurado para solicitar a um servidor um endereço IP.

DHCP- Termos

- **Scope:**

- Intervalo consecutivo completo dos endereços IP possíveis de atribuir numa rede de forma dinâmica. Por exemplo a gama de endereços de 10.10.10.100 a 10.10.10.150 na rede 10.10.10.0 máscara 255.255.255.0

- **Intervalo de exclusão**

- Sequência limitada de endereços IP excluidos para serem fornecidos pelo DHCP dentro de um determinado scope.
 - Ex.: dentro da faixa 10.10.10.100 a 10.10.10.150 (rede 10.10.10.0/máscara 255.255.255.0), é criada uma faixa de exclusão de 10.10.10.120 a 10.10.10.130

- **Pool de endereços**

- São os endereços remanescentes da scope após a definição do intervalo de exclusão.
 - No exemplo anterior o pool de endereços é formado pelos endereços de 10.10.10.100 a 10.10.10.119, mais os endereços de 10.10.10.131 a 10.10.10.150

DHCP- Termos

- **Concessão**

- Período de tempo especificado por um servidor DHCP durante o qual um computador cliente pode utilizar um endereço IP que ele recebeu do servidor DHCP.

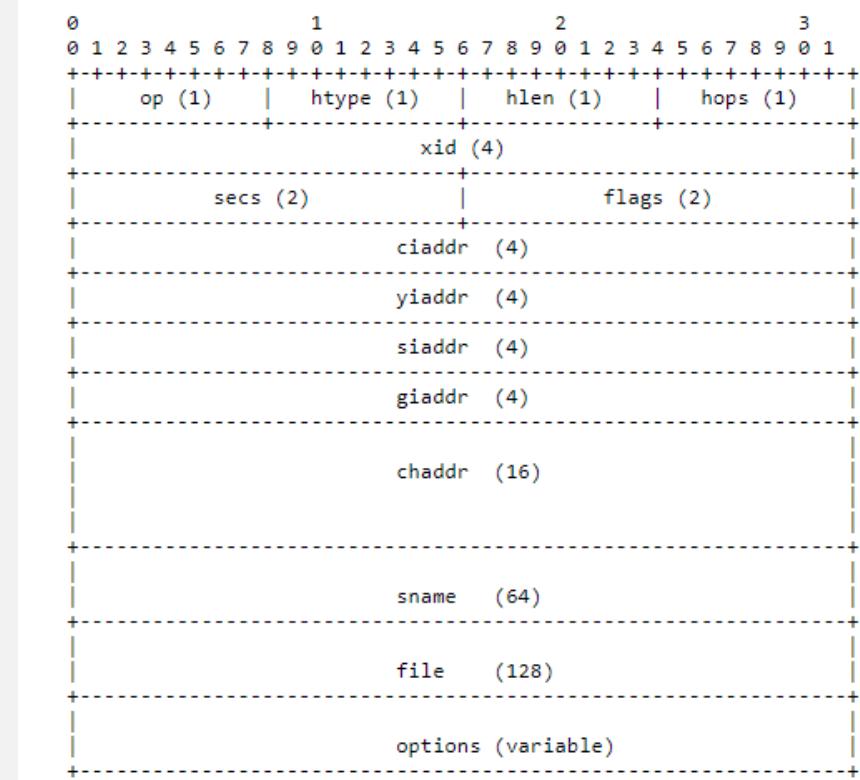
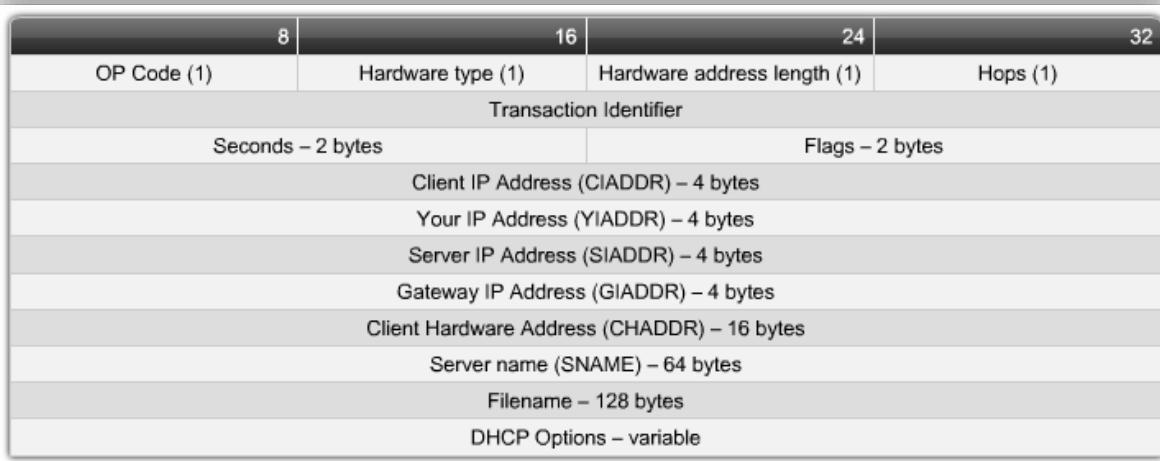
- **Reserva**

- Concessão de endereço permanente pelo servidor DHCP, assegurando que um dispositivo de hardware especificado na sub-rede possa utilizar sempre o mesmo endereço IP.

DHCP - Funcionamento

- Utiliza o protocolo UDP nas seguintes portas:
 - Servidor: porto 67
 - Cliente: porto 68
- As mensagens usadas no protocolo para negociação da informação são as seguintes:
 - ***Discover***
 - Enviada pelo cliente para verificar a existência de servidores DHCP na rede.
 - ***Offer***
 - Mensagem enviada pelos servidores com a proposta de informação.
 - ***Request***
 - Mensagem enviada pelo cliente em que escolhe a oferta (normalmente a primeira que lhe é enviada).
 - ***Ack***
 - Mensagem de confirmação enviada pelo servidor que “ganhou a negociação”.
 - Outras mensagens: ***Inform, Decline, Nack, Release***

Formato das mensagens

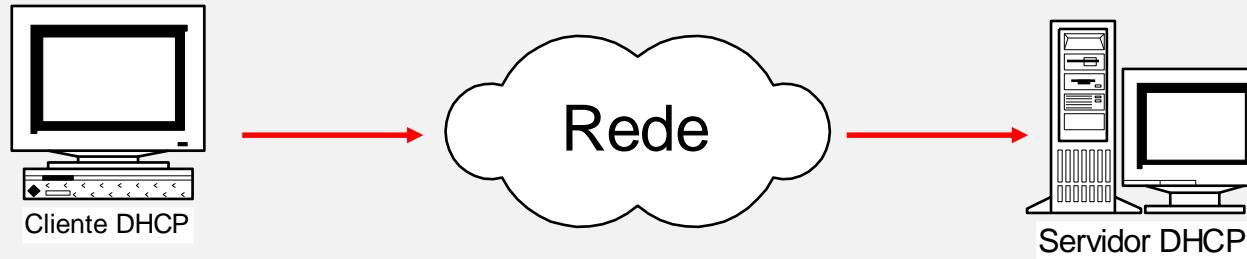


<https://tools.ietf.org/html/rfc2131>

Formato das mensagens

Opcode (op)	Tipo da mensagem (Opcode). 1-Pedido 2- Resposta. O tipo específico é indicado numa opção (DHCP Message Type)
Hardware type (htype)	Tipo do endereço do hardware. Informa o padrão de rede utilizado pelo adaptador de rede. Geralmente é Ethernet (1)
Hardware address length (hlen)	Tamanho do endereço do hardware. Se for Ethernet será o tamanho do MAC address (6)
Hops (hops)	Cliente coloca a zero o campo sendo apenas utilizado pelos routers indicando os saltos que necessita de fazer. Usado nos servidores de relay
Transation Identifier (xid)	Número identificador da transação servindo para associar pedidos e respostas da mesma transação
Seconds (secs)	Tempo em segundos desde que o cliente começou o processo de atribuição ou de renovação da concessão.
Flags	Para indicar opções especiais de resposta às solicitações. No caso do cliente não ter ainda endereço IP preenche este campo a 1 e o servidor saberá que tem de enviar em modo <i>broadcast</i> .
Client IP address (ciaddr)	Cliente informa, se possuir, o seu endereço IP. Caso não tenha ainda endereço preenche este campo com 0.0.0.0
Your IP address (yiaddr)	Usado pelo servidor para enviar um endereço IP para o cliente.
Server IP address (siaddr)	Preenchido pelo cliente com o endereço IP do servidor.
Gateway IP address (giaddr)	Endereço IP do relay agent, usado na inicialização pelo router
Client Hardware address (chaddr)	Endereço MAC do cliente.
Server Name (sname)	Nome do servidor. O cliente pode preencher este campo se ele sabe o nome do seu servidor (opcional).
File Name (file)	Nome do arquivo de imagem de boot.
Options (optins)	Campo opcional para parâmetros. Informar que tipo de resposta ou solicitação DHCP (DHCPDISCOVER, DHCPOFFER etc.) está sendo enviada para o cliente ou para o servidor. É ainda usado para enviar as outras informações da configuração da rede (por exemplo a máscara de rede, o default gateway e o DNS Server).

DHCP - Processo de concessão inicial

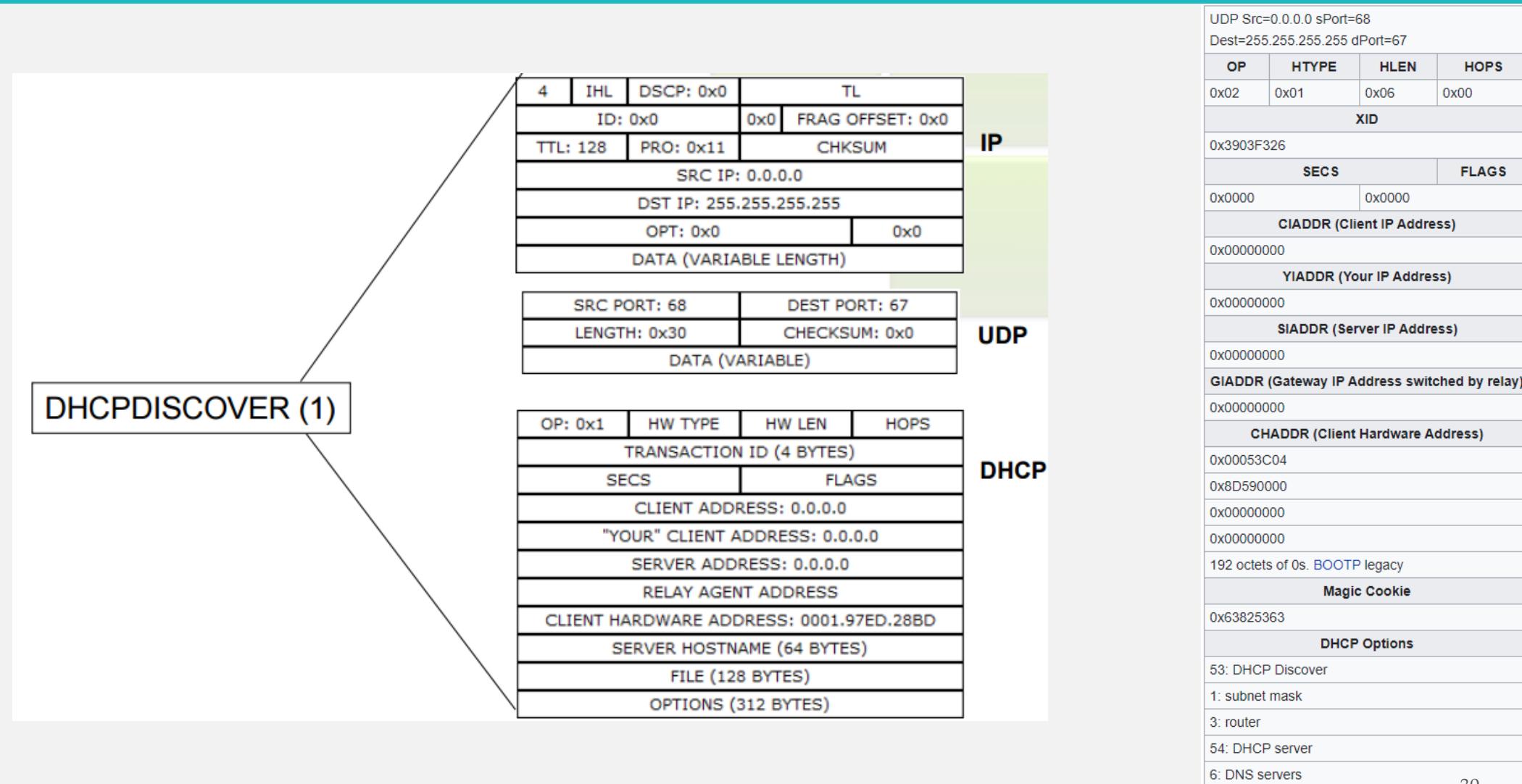


Cliente envia uma
mensagem “*DHCPOffer*”
para toda a rede (*broadcast*)

Descoberta de um
servidor DHCP
(*DHCPOffer*)

O formato desta mensagem é específico, sendo reconhecido apenas pelo(s)
servidor(es) DHCP que estejam presentes na rede local .

Processo de concessão

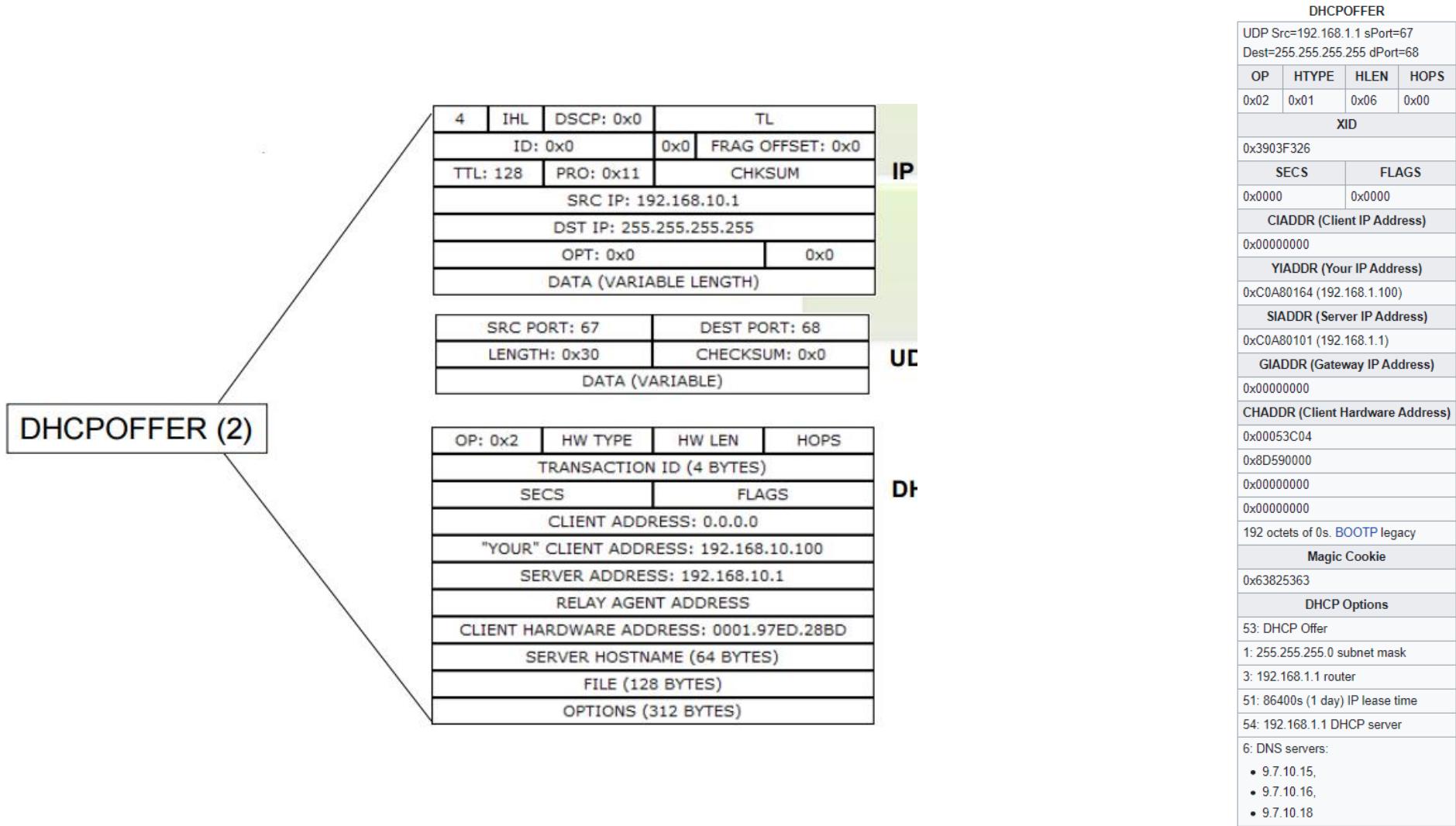


Processo de concessão inicial



O servidor DHCP “ouve” a mensagem enviada pelo cliente e responde com a oferta de um endereço IP e restantes configurações (máscara de sub-rede, gateway e DNS)

Processo de concessão



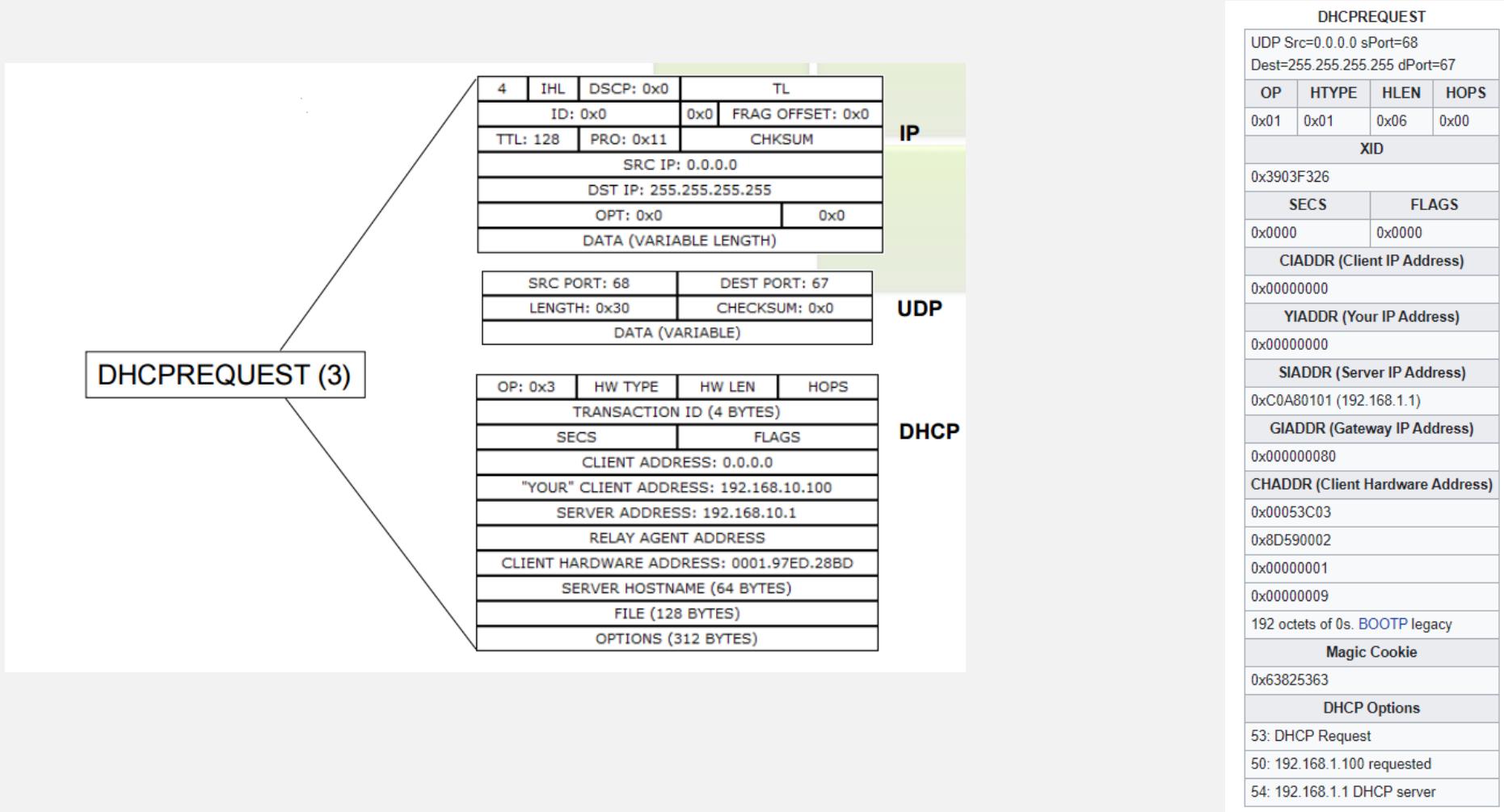
Processo de concessão inicial



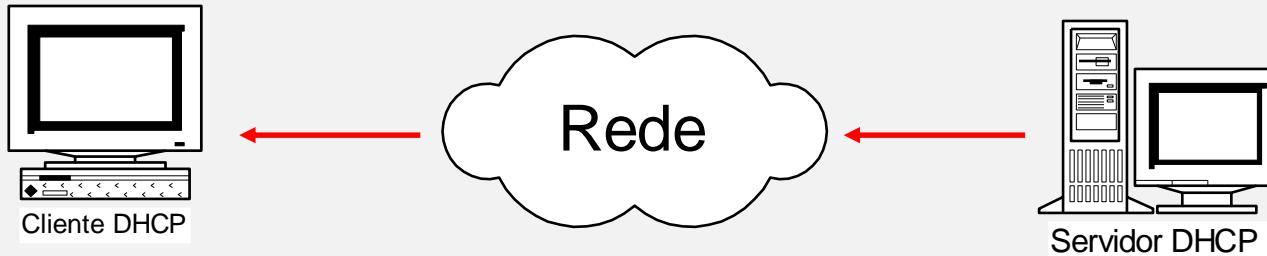
Assim que a mensagem DHCPOffer é recebida, o cliente seleciona o endereço oferecido respondendo ao servidor com uma solicitação de DHCP “DHCPRequest”, informando que a oferta foi aceita

Esta mensagem é enviada em broadcast, pois o cliente ainda não possui as configurações do protocolo TCP/IP

Processo de concessão



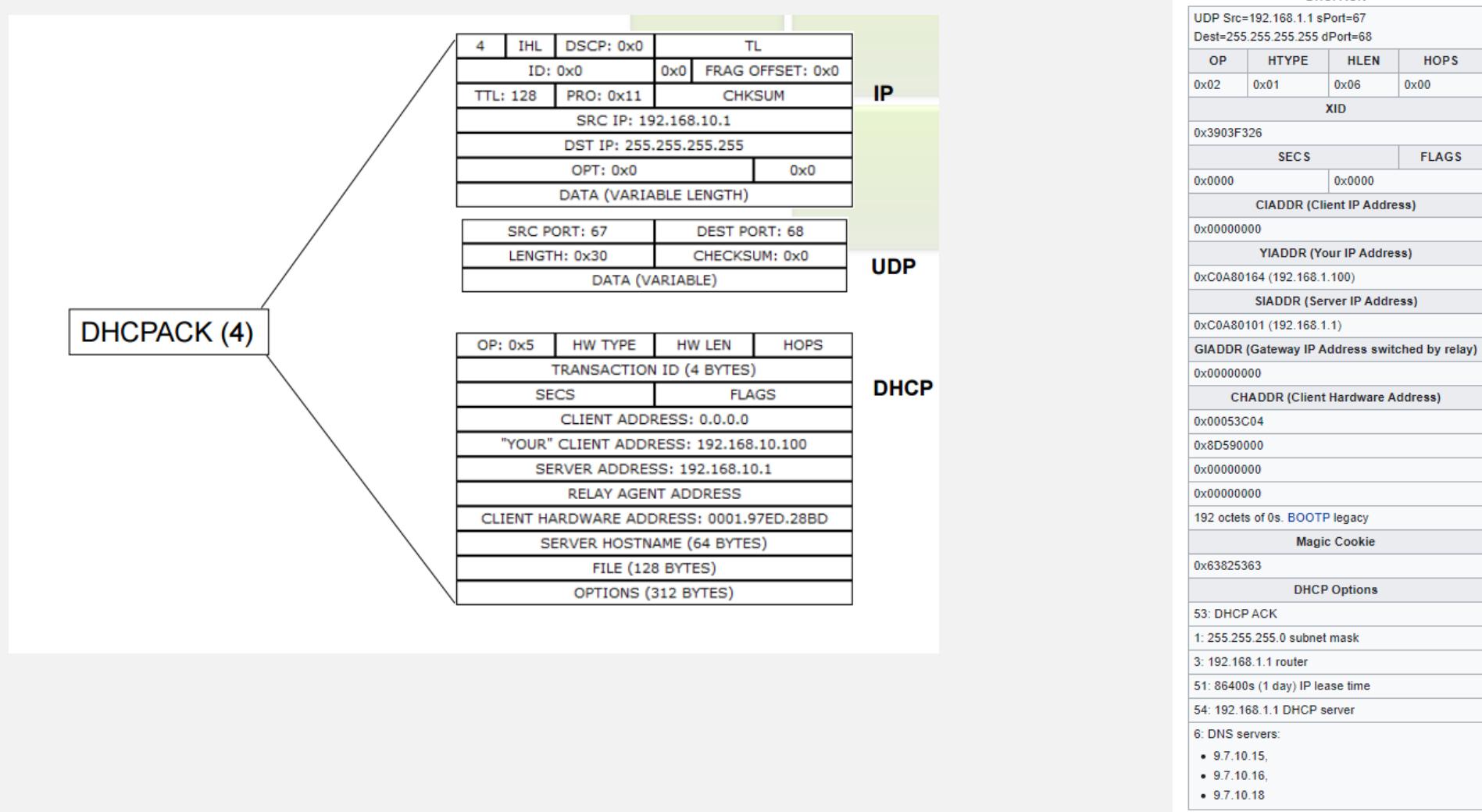
Processo de concessão inicial



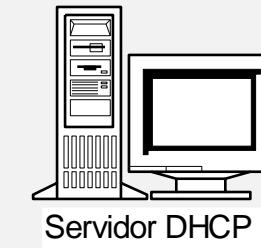
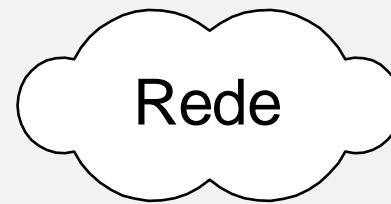
Reconhecimento de
DHCP (*DHCPAck*)

Após receber a mensagem *DHCPRequest*
do cliente, o servidor DHCP envia uma
mensagem de reconhecimento
("DHCPAck"), aprovando a concessão.

Processo de concessão



Processo de concessão inicial



Depois de receber o DHCPAck do servidor DHCP, o cliente configura as propriedades do TCP/IP utilizando as informações enviadas pelo servidor DHCP, na mensagem DHCPOffer e fica pronto a comunicar!

Processo de renovação de concessão

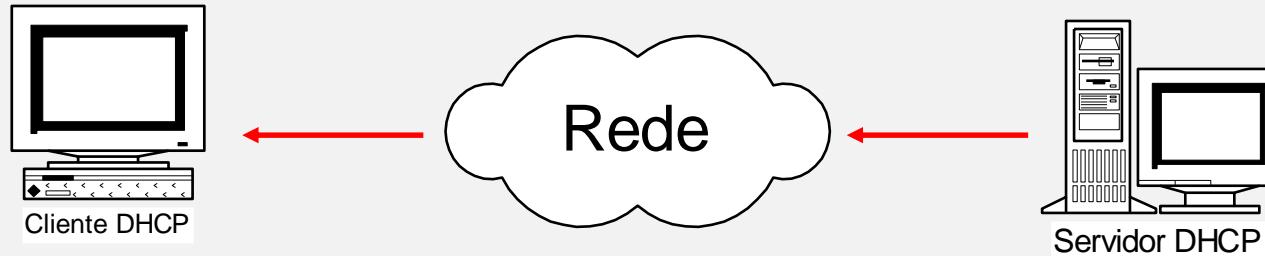
- Quando um cliente DHCP é desligado e reinicializado (na mesma sub-rede), geralmente obtém uma concessão para o mesmo endereço IP que tinha antes de ser desligado.
- Depois da metade do tempo de concessão do cliente ter decorrido, o cliente tenta **renovar** a concessão com o servidor DHCP.

Processo de renovação de concessão



O cliente envia uma mensagem **DHCPRequest** diretamente para o servidor que anteriormente havia efetuado a concessão (pois agora o cliente tem um endereço IP e sabe o endereço IP do servidor DHCP), para renovar e estender a concessão de endereço atual

Processo de renovação de concessão

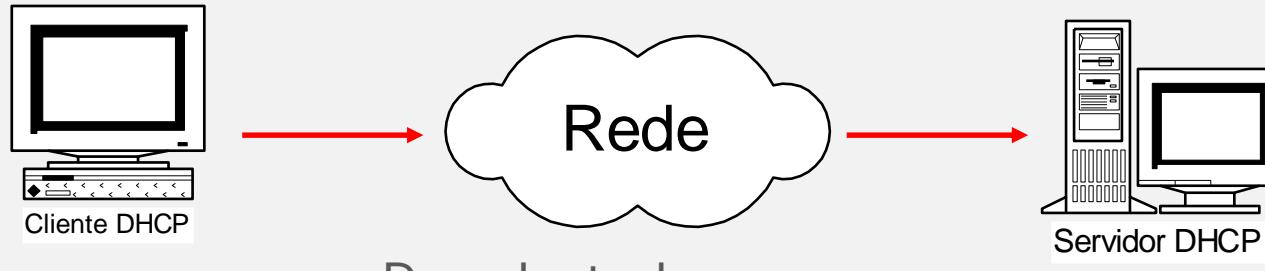


Reconhecimento de
DHCP (**DHCPAck**)

Se o servidor DHCP original estiver ativo, envia
uma mensagem DHCPAck, o que significa que a
concessão atual foi renovada

Se algumas das informações TCP-IP utilizadas
foram alteradas o servidor envia os novos valores
para que o cliente as possa atualizar.

Processo de renovação de concessão



Descoberta de um
servidor DHCP
(*DHCPDiscover*)

Se o cliente não conseguir comunicar com o servidor DHCP original, tenta renovar a concessão atual com outro qualquer servidor DHCP disponível, enviando um *DHCPDiscover* em broadcast

Processo de renovação de concessão



Se algum servidor responder com um DHCPOffer para atualizar a concessão atual, o cliente poderá renovar a concessão baseada na oferta do servidor DHCP, e continuando a trabalhar normalmente na rede

Processo de renovação de concessão

- Se chegar a 75% do tempo da concessão expirar e não tenha conseguido estabelecer nenhuma ligação com o servidor DHCP, o cliente repete todo o processo de obtenção de uma nova concessão.
- O cliente DHCP usa o campo “Checksum” do UDP para garantir a integridade do pacote recebido.
- No caso de a mensagem UDP ser perdida, o protocolo utiliza a técnica convencional de *timeout* com retransmissão.

Outros Comandos

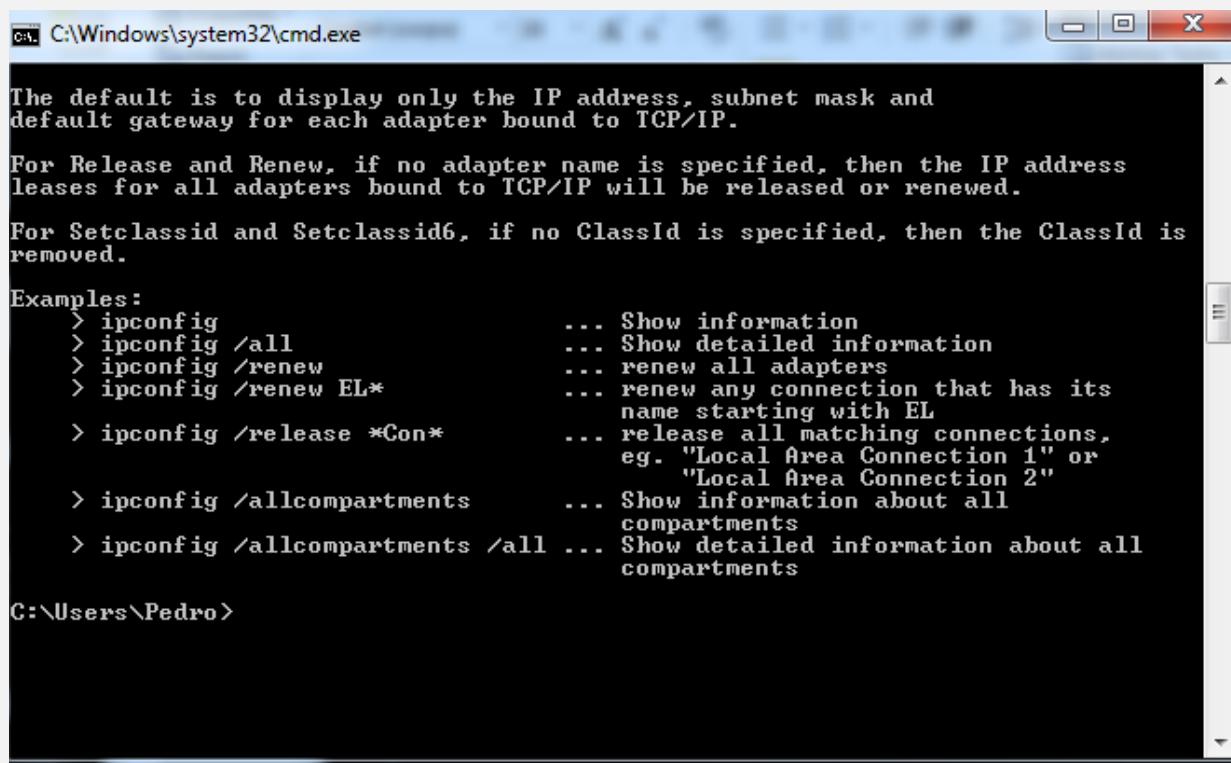
- **DHCPNack**
 - Enviado por um servidor DHCP a um cliente negando a mensagem do DHCPRequest. Isso pode ocorrer se o endereço solicitado está incorreto porque o cliente foi movido para uma nova sub-rede ou concessão e não pode ser renovado.
- **DHCPDecline**
 - Enviado por um cliente DHCP para um servidor, informando que o servidor que o endereço IP oferecido foi recusado porque ele parece estar em uso por outro computador.
- **DHCPInform**
 - Enviado de um cliente DHCP para um servidor DHCP, solicitando apenas parâmetros de configuração local adicional;
 - o cliente já tem um endereço IP configurado. Esse tipo de mensagem também é usado por servidores DHCP que executam o Windows Server 2008 para detetar servidores DHCP não autorizados.
- **DHCPRelease**
 - Enviada por um cliente DHCP para um servidor que lhe forneceu a concessão libertando assim o IP que lhe tinha sido atribuído.

Segurança

- O DHCP não inclui qualquer mecanismo de autenticação. Por isso é vulnerável a uma variedade de ataques.
- Estes podem ser divididos em três grupos fundamentais:
 - Fornecimento de informações erradas a clientes por servidores DHCP não autorizados
 - Clientes não autorizados com acesso a recursos.
 - Esgotamento dos recursos dos clientes.

DHCP (Cliente)

- Num cliente e para saber/alterar a sua configuração IP pode 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.

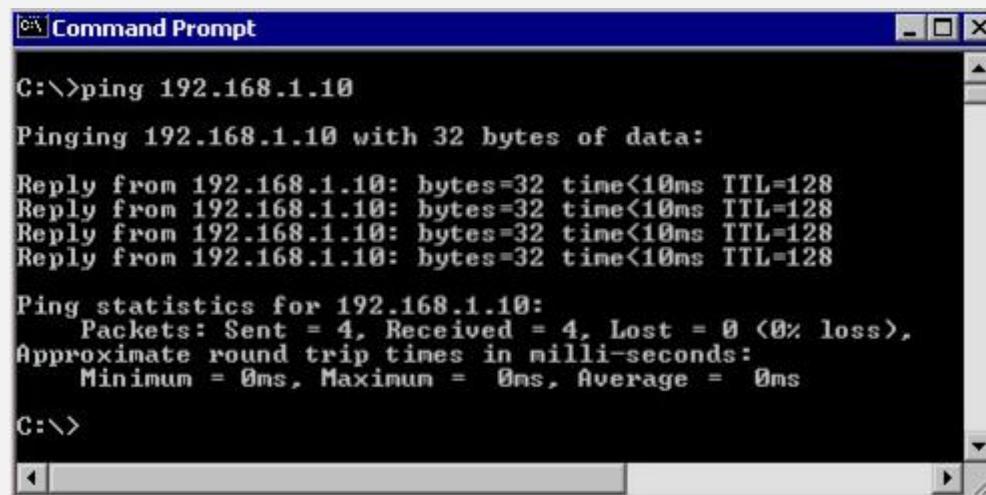
Examples:

> 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)

- O comando **ping** testa a conectividade física entre dois extremos, fornecendo uma indicação da fiabilidade da ligação uma vez que apresenta o resultado de quatro tentativas de comunicação.



```
C:\>ping 192.168.1.10

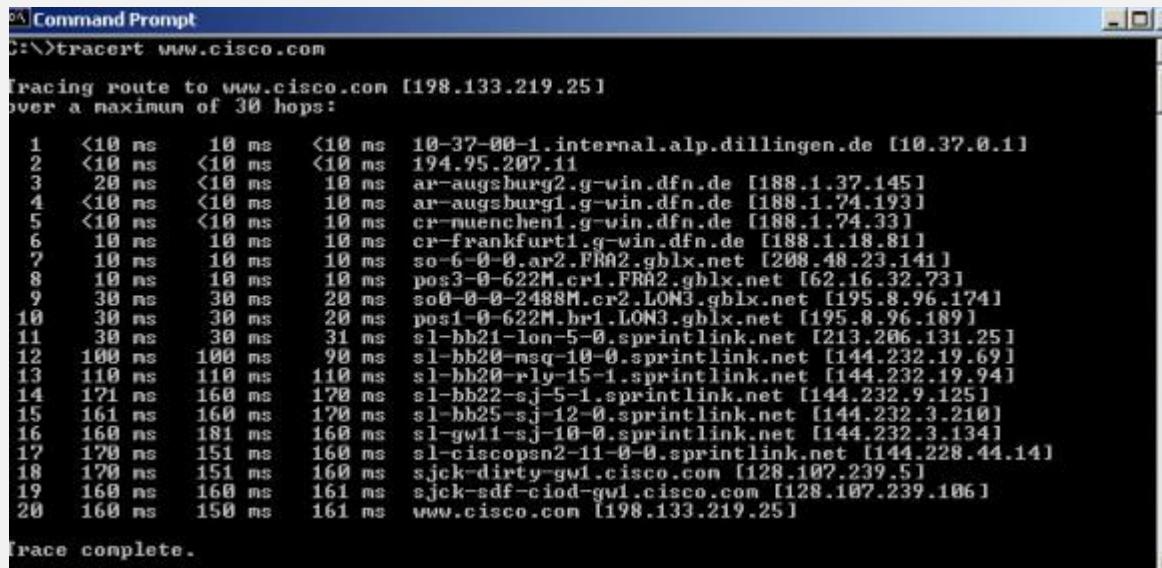
Pinging 192.168.1.10 with 32 bytes of data:
Reply from 192.168.1.10: bytes=32 time<10ms TTL=128

Ping statistics for 192.168.1.10:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 0ms, Maximum = 0ms, Average = 0ms

C:\>
```

DHCP (Cliente)

- O comando **tracert** é a abreviatura TCP/IP para trace route. O comando usa datagramas IP para apresentar os routers que são encontrados no caminho até ao destino.



The screenshot shows a Windows Command Prompt window titled "Command Prompt". The command entered is "tracert www.cisco.com". The output displays the tracing route to www.cisco.com over a maximum of 30 hops. The results are as follows:

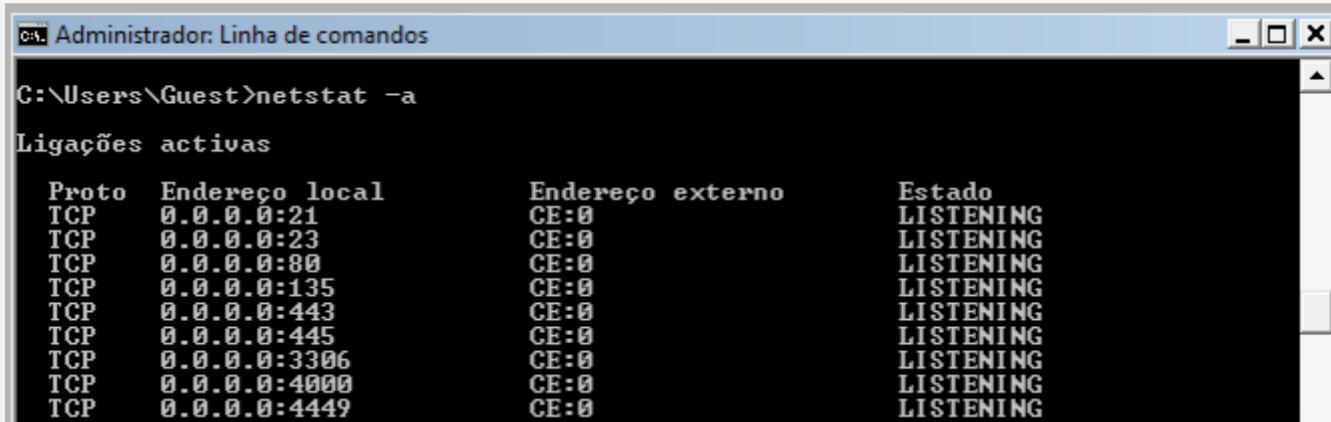
```
C:\>tracert www.cisco.com
Tracing route to www.cisco.com [198.133.219.25]
over a maximum of 30 hops:
 1  <10 ms   10 ms   <10 ms  10-37-00-1.internal.alp.dillingen.de [10.37.0.1]
 2  <10 ms   <10 ms   <10 ms  194.95.207.11
 3  20 ms    <10 ms   10 ms  ar-augsburg2.g-win.dfn.de [188.1.37.145]
 4  <10 ms   <10 ms   10 ms  ar-augsburg1.g-win.dfn.de [188.1.74.193]
 5  <10 ms   <10 ms   10 ms  cr-muenchen1.g-win.dfn.de [188.1.74.33]
 6  10 ms    10 ms   10 ms  cr-frankfurt1.g-win.dfn.de [188.1.18.81]
 7  10 ms    10 ms   10 ms  so-6-0-0.ar2.FRA2.gblx.net [208.48.23.141]
 8  10 ms    10 ms   10 ms  pos3-0-622M.cri.FRA2.gblx.net [62.16.32.73]
 9  30 ms    30 ms   20 ms  so0-0-0-2488M.cr2.LON3.gblx.net [195.8.96.174]
10  30 ms    30 ms   20 ms  pos1-0-622M.bri.LON3.gblx.net [195.8.96.189]
11  30 ms    30 ms   31 ms  sl-bb21-lon-5-0.sprintlink.net [213.206.131.25]
12  100 ms   100 ms   90 ms  sl-bb20-msq-10-0.sprintlink.net [144.232.19.69]
13  110 ms   110 ms   110 ms  sl-bb20-rly-15-1.sprintlink.net [144.232.19.94]
14  171 ms   160 ms   170 ms  sl-bb22-sj-5-1.sprintlink.net [144.232.9.125]
15  161 ms   160 ms   170 ms  sl-bb25-sj-12-0.sprintlink.net [144.232.3.210]
16  160 ms   181 ms   160 ms  sl-gw11-sj-10-0.sprintlink.net [144.232.3.134]
17  170 ms   151 ms   160 ms  sl-ciscopsn2-11-0-0.sprintlink.net [144.228.44.14]
18  170 ms   151 ms   160 ms  sjck-dirty-gwi.cisco.com [128.107.239.5]
19  160 ms   160 ms   161 ms  sjck-sdf-ciod-gwi.cisco.com [128.107.239.106]
20  160 ms   150 ms   161 ms  www.cisco.com [198.133.219.25]

Trace complete.
```

- A primeira linha de saída mostra o nome de destino seguido do seu endereço IP. Em seguida são apresentadas as listagens de todos os routers através dos quais o tracert teve que passar para chegar ao destino

DHCP (Cliente)

- O comando **netstat** permite ver informação acerca das ligações de rede TCP/IP na máquina local e estatísticas acerca dos protocolos utilizados.



The screenshot shows a Windows Command Prompt window titled "Administrador: Linha de comandos". The command entered is "C:\Users\Guest>netstat -a". The output displays "Ligações activas" (Active Connections) in a table format:

Proto	Endereço local	Endereço externo	Estado
TCP	0.0.0.0:21	CE:0	LISTENING
TCP	0.0.0.0:23	CE:0	LISTENING
TCP	0.0.0.0:80	CE:0	LISTENING
TCP	0.0.0.0:135	CE:0	LISTENING
TCP	0.0.0.0:443	CE:0	LISTENING
TCP	0.0.0.0:445	CE:0	LISTENING
TCP	0.0.0.0:3306	CE:0	LISTENING
TCP	0.0.0.0:4000	CE:0	LISTENING
TCP	0.0.0.0:4449	CE:0	LISTENING

DHCP (Cliente)

- Cada máquina é responsável por manter dinamicamente uma tabela de correspondência entre endereços físicos e endereços IP recentemente usados (tabela ARP), este procedimento reduz a frequência do recurso ao protocolo ARP. Para ver esta tabela faça **arp -a**):



```
-d Deletes the host specified by inet_addr. inet_addr may be
      wildcarded with * to delete all hosts.
-s Adds the host and associates the Internet address inet_addr
      with the Physical address eth_addr. The Physical address is
      given as 6 hexadecimal bytes separated by hyphens. The entry
      is permanent.
eth_addr Specifies a physical address.
if_addr If present, this specifies the Internet address of the
        interface whose address translation table should be modified.
        If not present, the first applicable interface will be used.
Example:
> arp -s 157.55.85.212 00-aa-00-62-c6-09 .... Adds a static entry.
> arp -a ..... Displays the arp table.

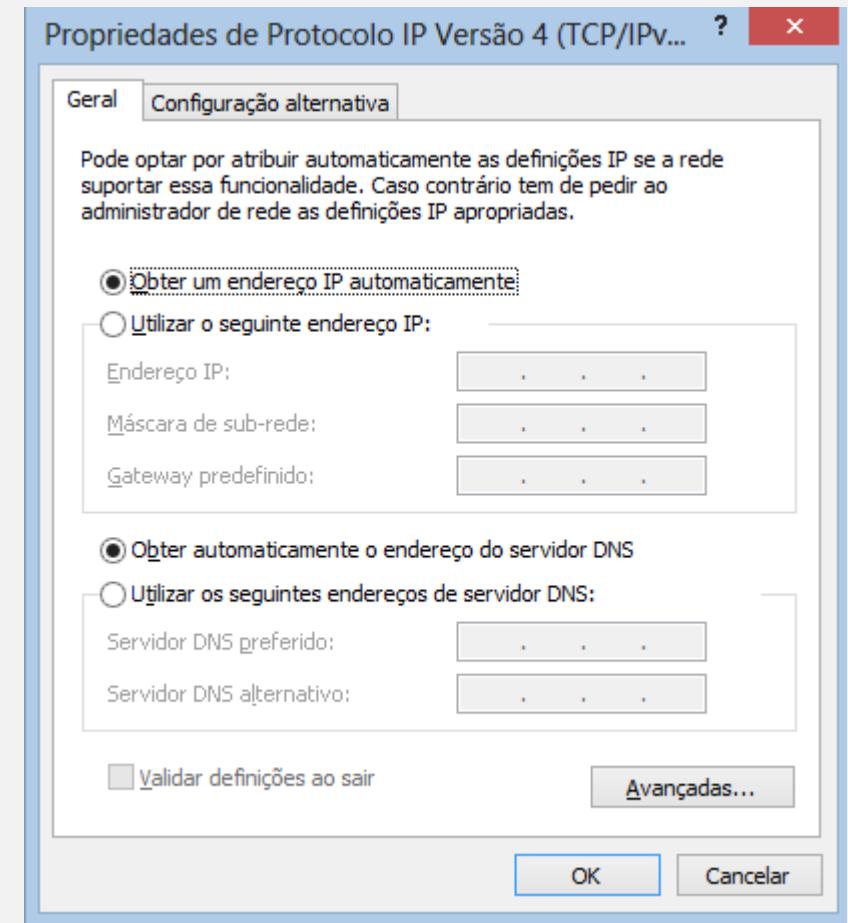
C:\Users\pgeirinhas>arp -a

Interface: 10.9.35.199 --- 0x3
Internet Address      Physical Address      Type
10.9.35.1              78-fe-3d-4f-2a-c1    dynamic
10.9.35.255             ff-ff-ff-ff-ff-ff    static
224.0.0.22               01-00-5e-00-00-16    static
224.0.0.252              01-00-5e-00-00-fc    static
239.255.255.250          01-00-5e-7f-ff-fa    static

C:\Users\pgeirinhas>
```

DHCP (Cliente)

- Na configuração do cliente pode definir quais os parâmetros que são obtidos de forma automática (DHCP) ou manual.
- Pode ainda no caso do W8 definir uma configuração alternativa para utilização da placa em multi-ambientes.



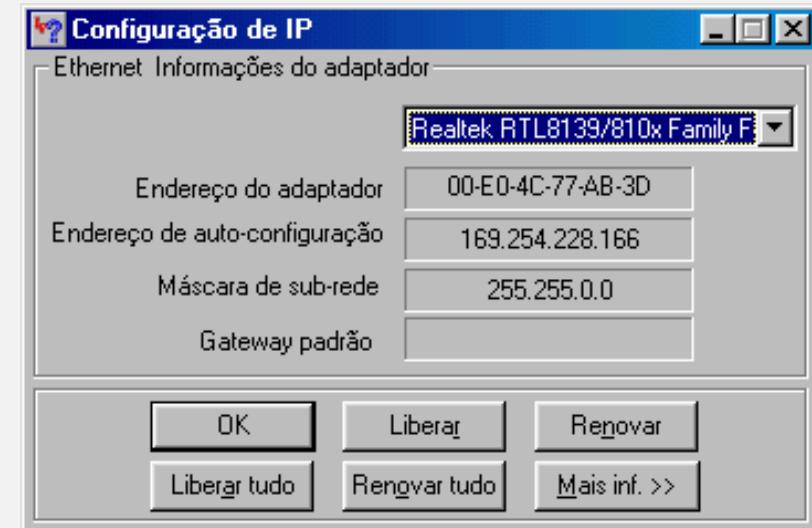
APIPA

- A Microsoft registou no iana.org, uma entidade encarregada da distribuição de IPs por todo o mundo, uma gama de endereços para uso em redes que não possuem DHCP. Esta gama é:

169.254.0.0 a 169.254.255.255

- Quando um computador com Windows conclui que não existe DHCP na rede, usará automaticamente um IP começando com 169.254 terminando com dois números que são gerados em função da configuração de hardware do computador. Isso garante que os computadores terão IPs “compatíveis”.

APIPA significa *Automatic Private IP Addressing*.



Dúvidas



Referências

- Windows Server 2012, António Rosa, FCA.
- www.cisco.com – acedido em março de 2023.
- https://pt.wikipedia.org/wiki/Dynamic_Host_Configuration_Protocol - acedido em março de 2023.
- <https://www.youtube.com/watch?v=YYEG4ZCUIjs> – acedido em março de 2023
- <https://www.dcc.fc.up.pt/~rprior/1819/AR/slides/05%20-%20DHCP.pdf> - acedido em março de 2023
- <http://pt.scribd.com/doc/22021856/Apresentacao-DHCP-Rosario> – acedido em março de 2021
- <http://pt.scribd.com/doc/22021986/DHCP-Apresentacao-no-power-point> – acedido em março de 2021
- <http://www.ccc.ipt.pt/~ricardo/ficheiros/RedesComputadores.pdf> – acedido em março de 2021

Serviços de Rede 1

2022-2023

Pedro Miguel Geirinhas

Aula 4

Dynamic Host Configuration Protocol (DHCP)

Agenda

- 1.** Analise dos pacotes DHCP
- 2.** DHCP em ambiente Windows
- 3.** DHCP em ambiente Linux



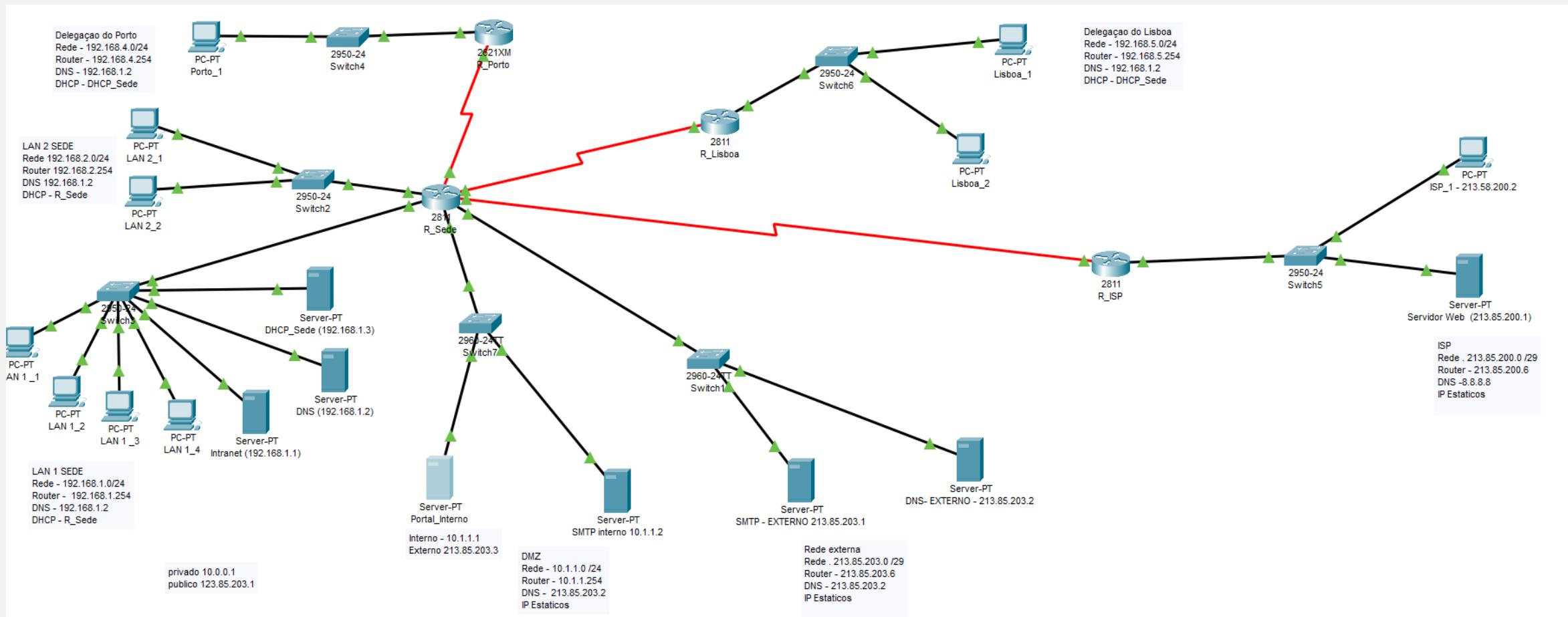
Licenciatura em Engenharia Informática
Ramo de Redes e Administração de Sistemas

Analise do processo e dos pacotes DHCP

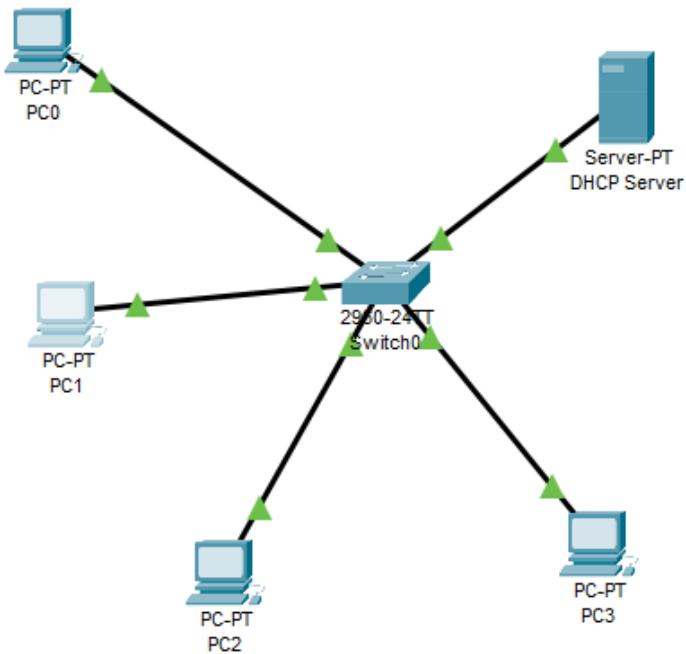
Ano Letivo 2021-2022

© - Pedro Geirinhas

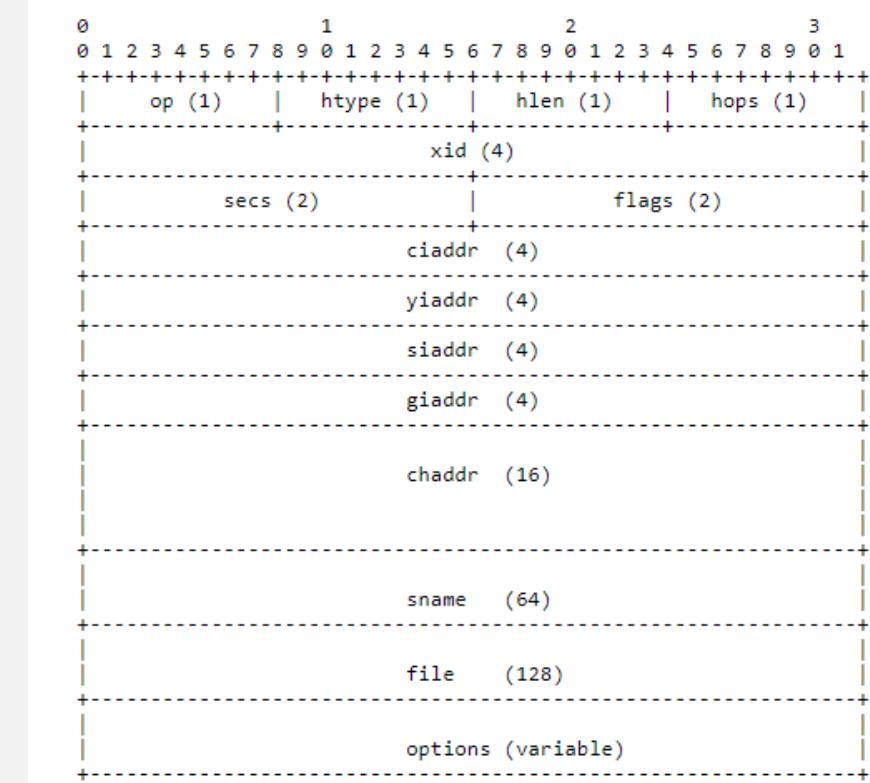
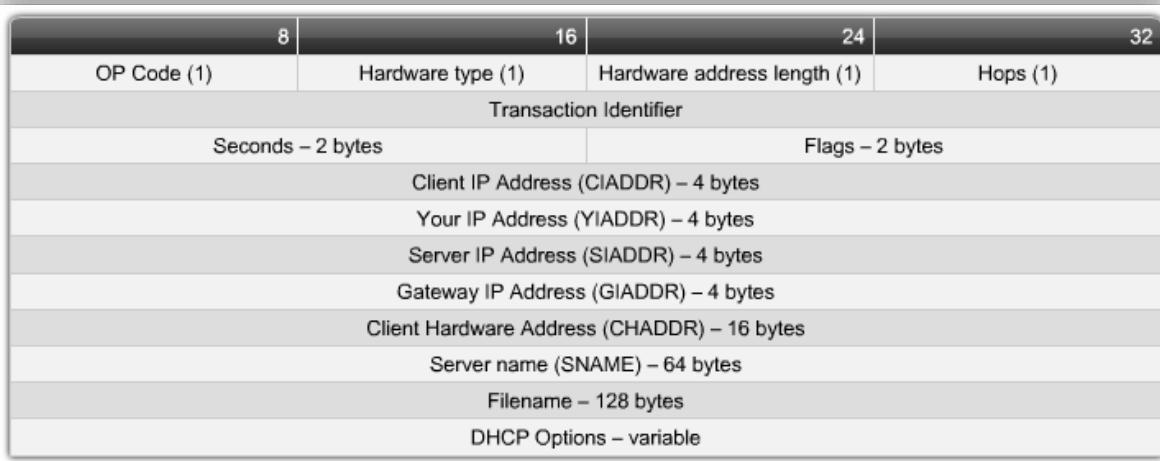
Já agora...



Processo de concessão



Formato das mensagens



<https://tools.ietf.org/html/rfc2131>

Formato das mensagens

Opcode (op)	Tipo da mensagem (Opcode). 1-Pedido 2- Resposta. O tipo específico é indicado numa opção (DHCP Message Type. Código 53)
Hardware type (htype)	Tipo do endereço do hardware. Informa o padrão de rede utilizado pelo adaptador de rede. Geralmente é Ethernet (1)
Hardware address length (hlen)	Tamanho do endereço do hardware. Se for Ethernet será o tamanho do MAC address (6)
Hops (hops)	Cliente coloca a zero o campo sendo apenas utilizado pelos routers indicando os saltos que necessita de fazer. Usado nos servidores de relay
Transation Identifier (xid)	Número identificador da transação servindo para associar pedidos e respostas da mesma transação
Seconds (secs)	Tempo em segundos desde que o cliente começou o processo de atribuição ou de renovação da concessão.
Flags	Para indicar opções especiais de resposta às solicitações. No caso do cliente não ter ainda endereço IP preenche este campo a 1 e o servidor saberá que tem de enviar em modo <i>broadcast</i> .
Client IP address (ciaddr)	Cliente informa, se possuir, o seu endereço IP. Caso não tenha ainda endereço preenche este campo com 0.0.0.0
Your IP address (yiaddr)	Usado pelo servidor para enviar um endereço IP para o cliente.
Server IP address (siaddr)	Preenchido pelo cliente com o endereço IP do servidor.
Gateway IP address (giaddr)	Endereço IP do relay agent, usado na inicialização pelo router
Client Hardware address (chaddr)	Endereço MAC do cliente.
Server Name (sname)	Nome do servidor. O cliente pode preencher este campo se ele sabe o nome do seu servidor (opcional).
File Name (file)	Nome do arquivo de imagem de boot.
Options (optins)	Campo opcional para parâmetros. Informar que tipo de resposta ou solicitação DHCP (DHCPDISCOVER, DHCPOFFER etc.) está sendo enviada para o cliente ou para o servidor. É ainda usado para enviar as outras informações da configuração da rede (por exemplo a máscara de rede, o default gateway e o DNS Server).

Processo de concessão

UDP Src=0.0.0.0 sPort=68			
Dest=255.255.255.255 dPort=67			
OP HTYPE HLEN HOPS			
0x02 0x01 0x06 0x00			
XID			
0x3903F326			
SEC S	FLAGS		
0x0000	0x0000		
CIADDR (Client IP Address)			
0x00000000			
YIADDR (Your IP Address)			
0x00000000			
SIADDR (Server IP Address)			
0x00000000			
GIADDR (Gateway IP Address switched by relay)			
0x00000000			
CHADDR (Client Hardware Address)			
0x00053C04			
0x8D590000			
0x00000000			
192 octets of 0s. BOOTP legacy			
Magic Cookie			
0x63825363			
DHCP Options			
53: DHCP Discover			
1: subnet mask			
3: router			
51: 86400s (1 day) IP lease time			
54: 192.168.1.1 DHCP server			
6: DNS servers			
• 9.7.10.15,			
• 9.7.10.16,			
• 9.7.10.18			

DHCP OFFER			
UDP Src=192.168.1.1 sPort=67			
OP	HTYPE	HLEN	HOPS
0x02	0x01	0x06	0x00
XID			
0x3903F326			
SEC S	FLAGS		
0x0000	0x0000		
CIADDR (Client IP Address)			
0x00000000			
YIADDR (Your IP Address)			
0xC0A80164 (192.168.1.100)			
SIADDR (Server IP Address)			
0xC0A80101 (192.168.1.1)			
GIADDR (Gateway IP Address)			
0x00000000			
CHADDR (Client Hardware Address)			
0x00053C04			
0x8D590000			
0x00000000			
192 octets of 0s. BOOTP legacy			
Magic Cookie			
0x63825363			
DHCP Options			
53: DHCP Offer			
1: 255.255.255.0 subnet mask			
3: 192.168.1.1 router			
51: 86400s (1 day) IP lease time			
54: 192.168.1.1 DHCP server			
6: DNS servers:			
• 9.7.10.15,			
• 9.7.10.16,			
• 9.7.10.18			

DHCP REQUEST			
UDP Src=0.0.0.0 sPort=68			
OP	HTYPE	HLEN	HOPS
0x01	0x01	0x06	0x00
XID			
0x3903F326			
SEC S	FLAGS		
0x0000	0x0000		
CIADDR (Client IP Address)			
0x00000000			
YIADDR (Your IP Address)			
0xC0A80164 (192.168.1.100)			
SIADDR (Server IP Address)			
0xC0A80101 (192.168.1.1)			
GIADDR (Gateway IP Address)			
0x00000000			
CHADDR (Client Hardware Address)			
0x00053C03			
0x8D590002			
0x00000001			
0x00000009			
192 octets of 0s. BOOTP legacy			
Magic Cookie			
0x63825363			
DHCP Options			
53: DHCP Request			
50: 192.168.1.100 requested			
54: 192.168.1.1 DHCP server			

DHCPACK			
UDP Src=192.168.1.1 sPort=67			
OP	HTYPE	HLEN	HOPS
0x02	0x01	0x06	0x00
XID			
0x3903F326			
SEC S	FLAGS		
0x0000	0x0000		
CIADDR (Client IP Address)			
0x00000000			
YIADDR (Your IP Address)			
0xC0A80164 (192.168.1.100)			
SIADDR (Server IP Address)			
0xC0A80101 (192.168.1.1)			
GIADDR (Gateway IP Address switched by relay)			
0x00000000			
CHADDR (Client Hardware Address)			
0x00053C04			
0x8D590000			
0x00000000			
192 octets of 0s. BOOTP legacy			
Magic Cookie			
0x63825363			
DHCP Options			
53: DHCP ACK			
1: 255.255.255.0 subnet mask			
3: 192.168.1.1 router			
51: 86400s (1 day) IP lease time			
54: 192.168.1.1 DHCP server			
6: DNS servers:			
• 9.7.10.15,			
• 9.7.10.16,			
• 9.7.10.18			



Licenciatura em Engenharia Informática
Ramo de Redes e Administração de Sistemas

Dynamic Host Configuration Protocol (DHCP)
- Windows

Ano Letivo 2022-2023

© - Pedro Geirinhas

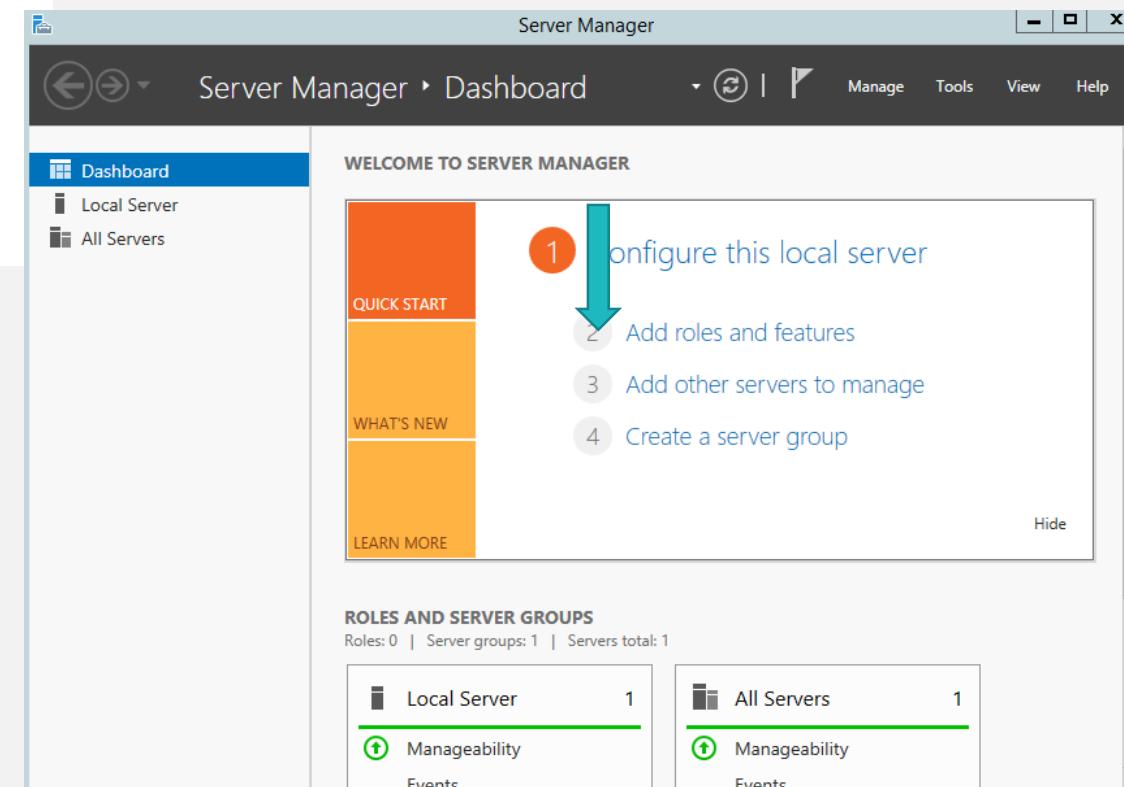
DHCP - Instalação do serviço

- A instalação do serviço de DHCP no *Windows Server 2012* é realizada através da aplicação Server Manager, escolhendo a opção “*Add roles*”.
- No final da instalação é adicionado uma nova entrada, DHCP, no menu “*Administrative Tools*”.
- Não deve utilizar um servidor/máquina com um endereço dinâmico para este tipo de serviço. É importante que o seu servidor DHCP tenha um endereço IP fixo.

DHCP - Instalação do serviço

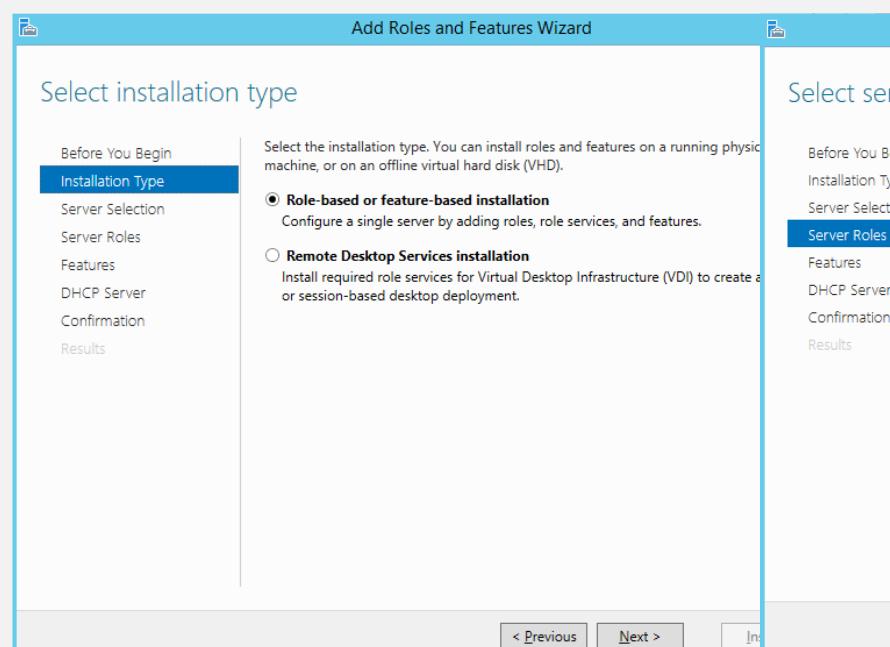


Copyright © 2013 Microsoft Corporation. All rights reserved.

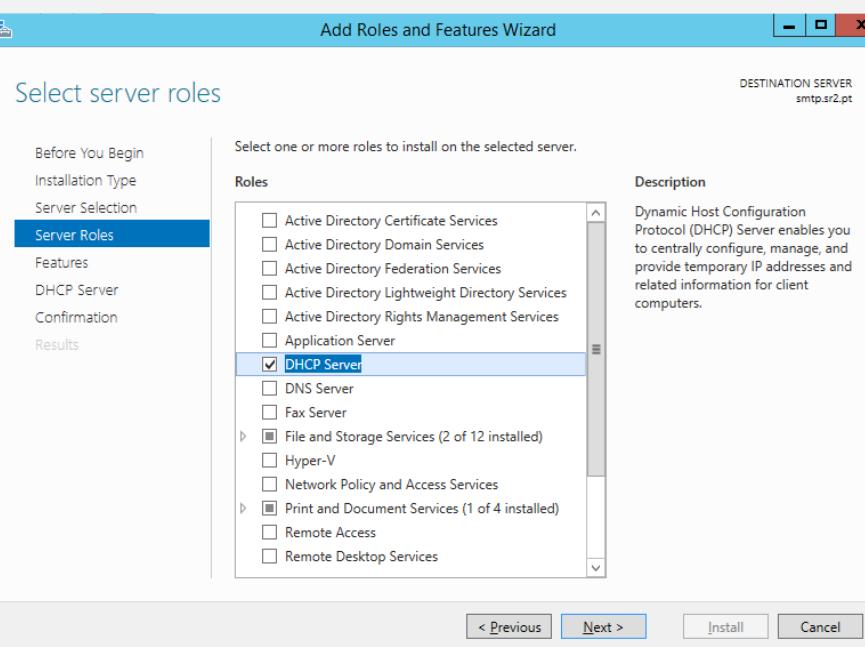


DHCP - Instalação do serviço

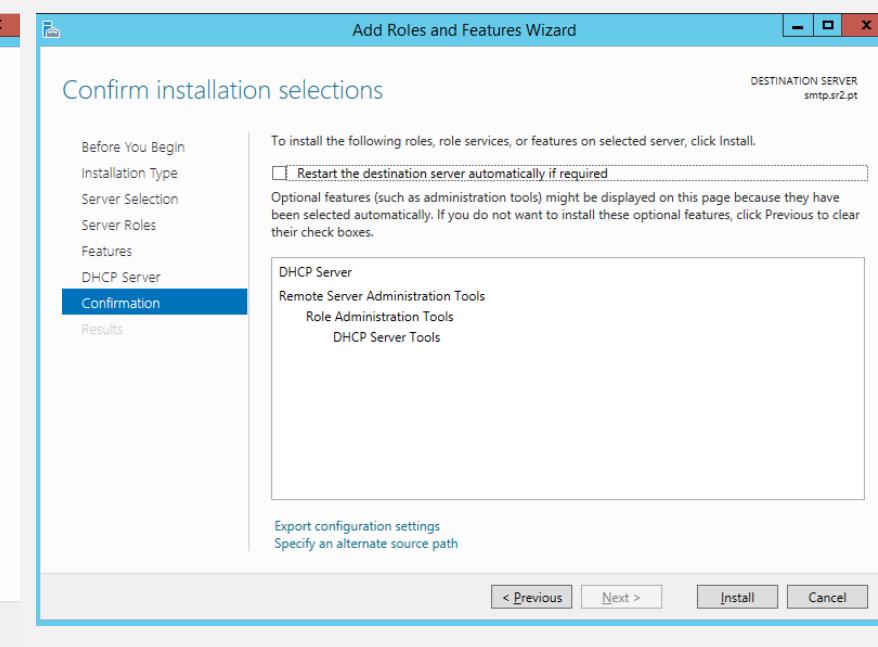
1



2

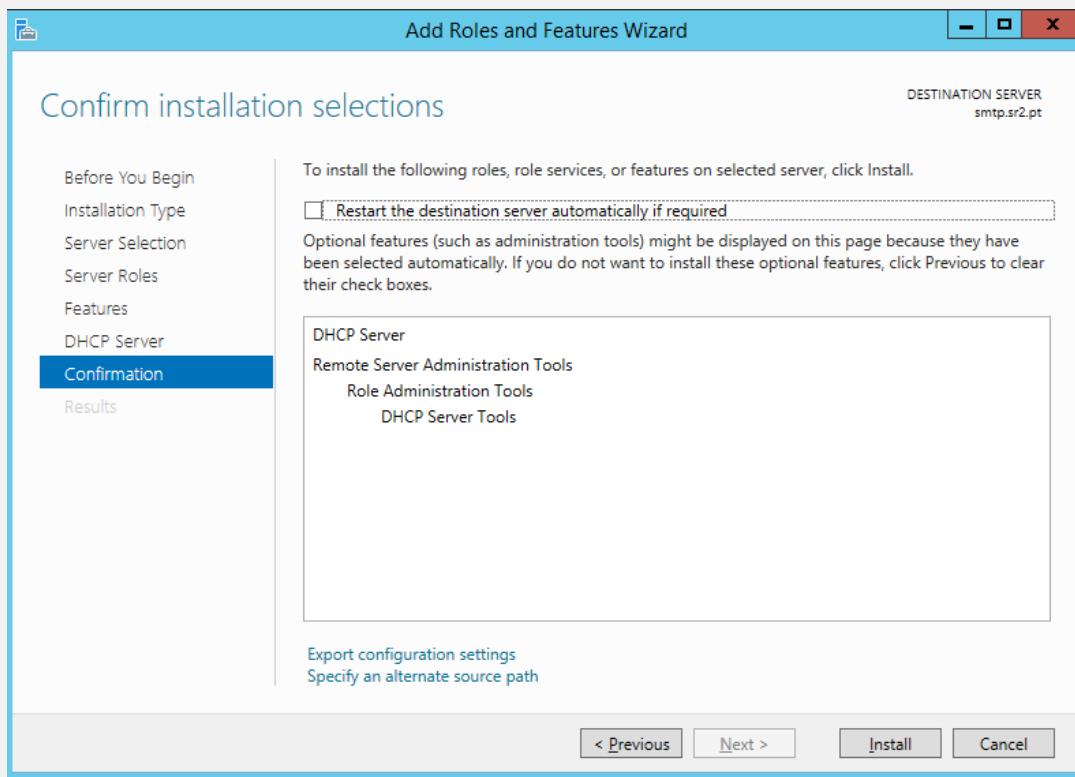


3

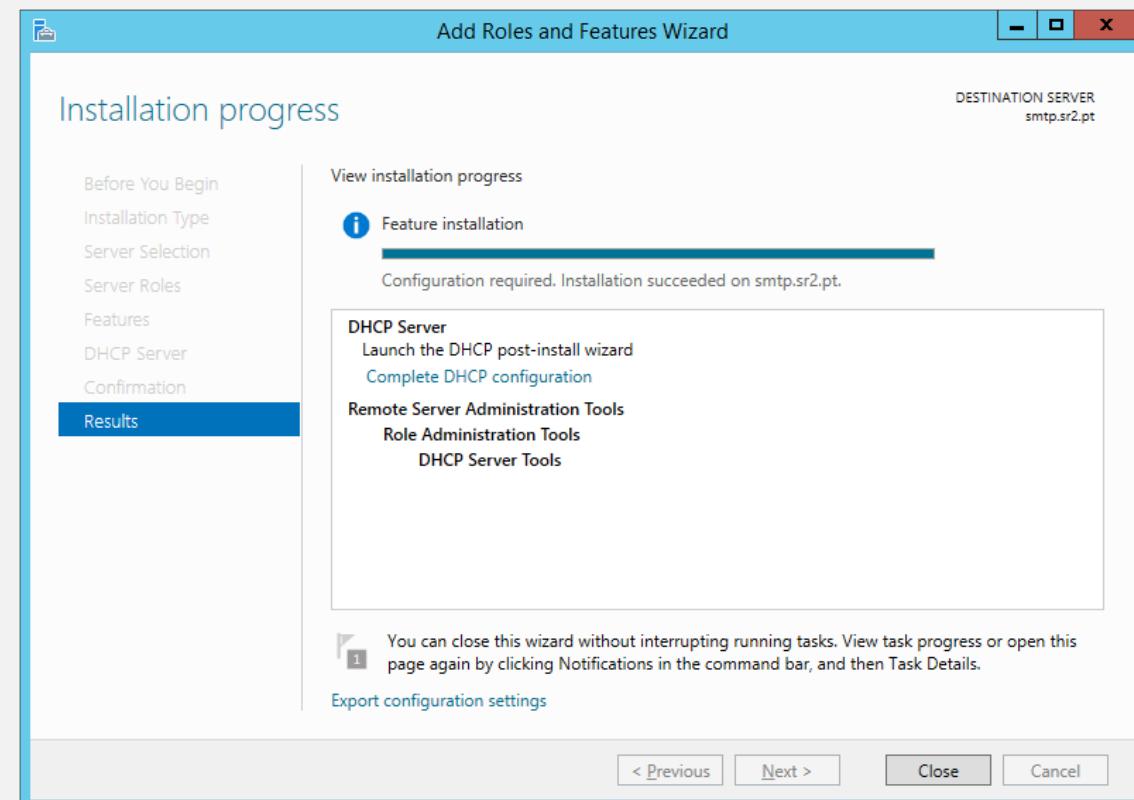


DHCP - Instalação do serviço

4

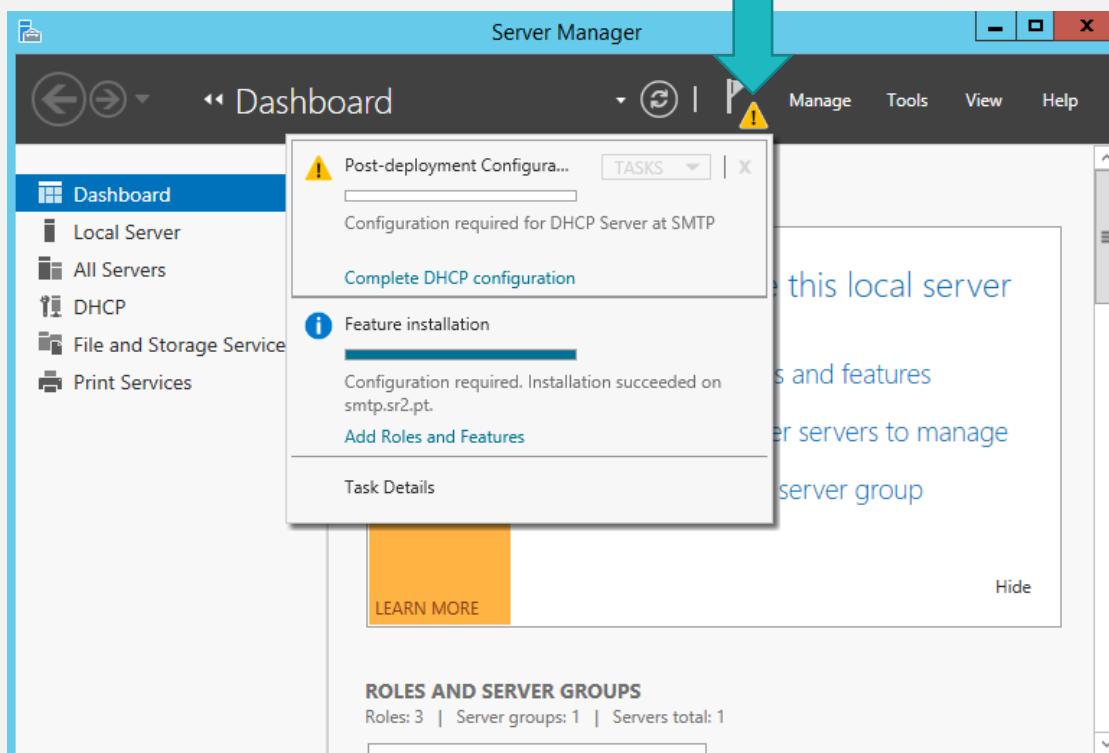


5



DHCP - Instalação do serviço

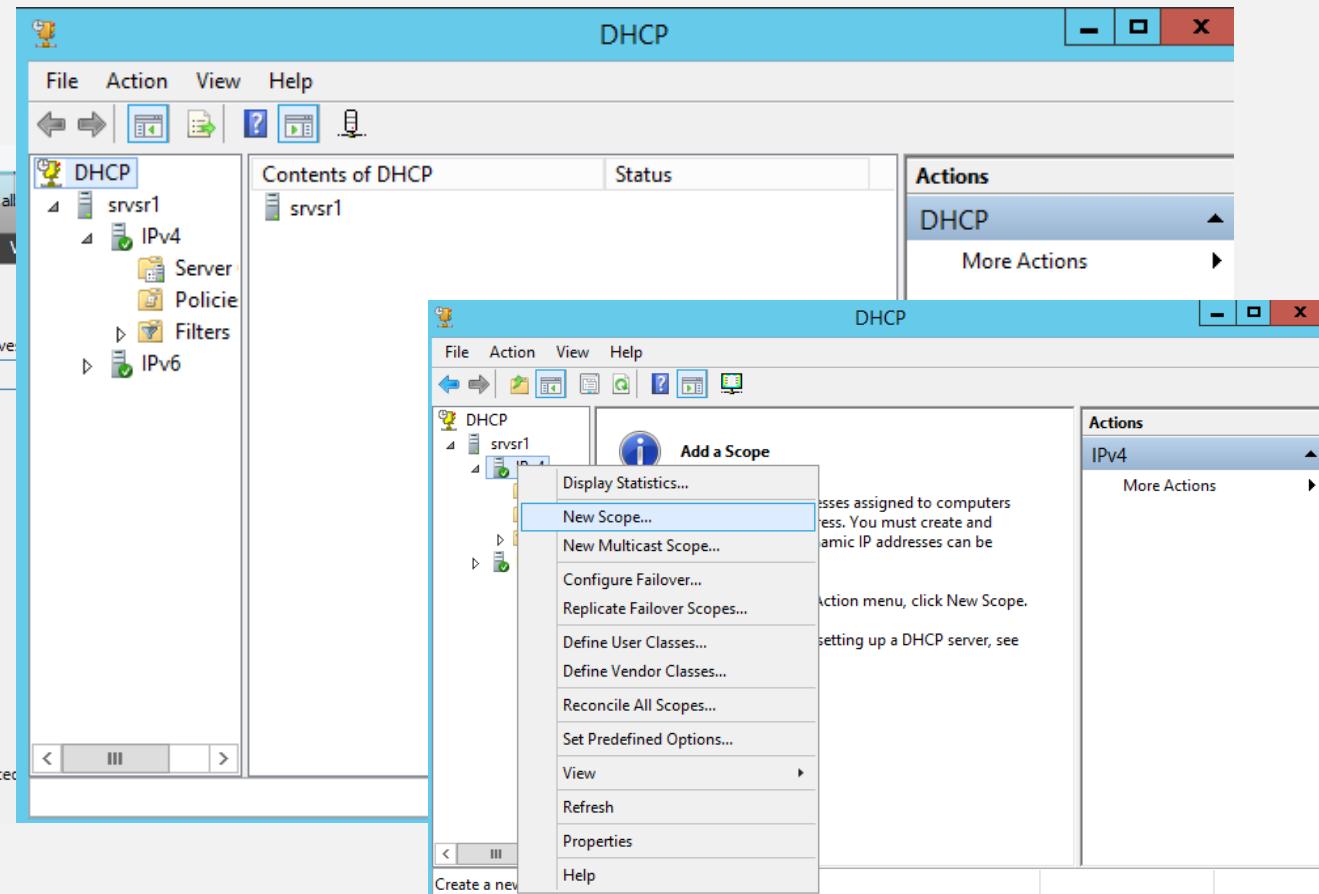
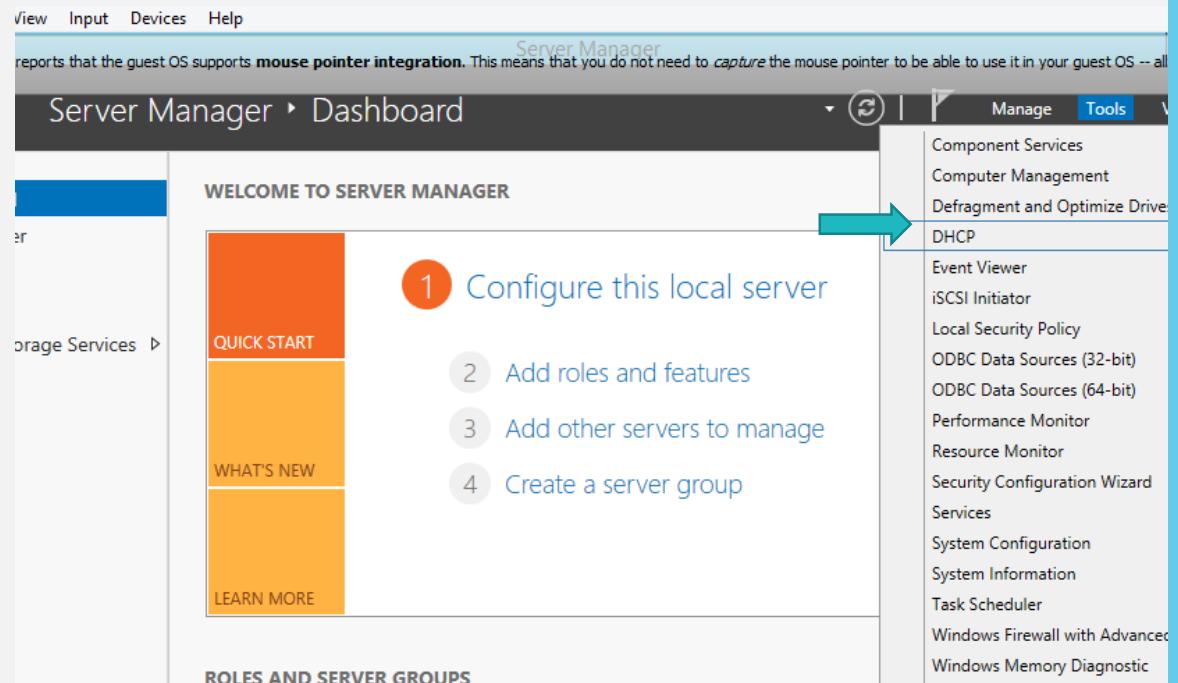
6



7



DHCP - Configuração do serviço



DHCP - Configuração de scopes

- Indicar:
 - **Scope Name**: Nome do scope que vai criar.
 - **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.

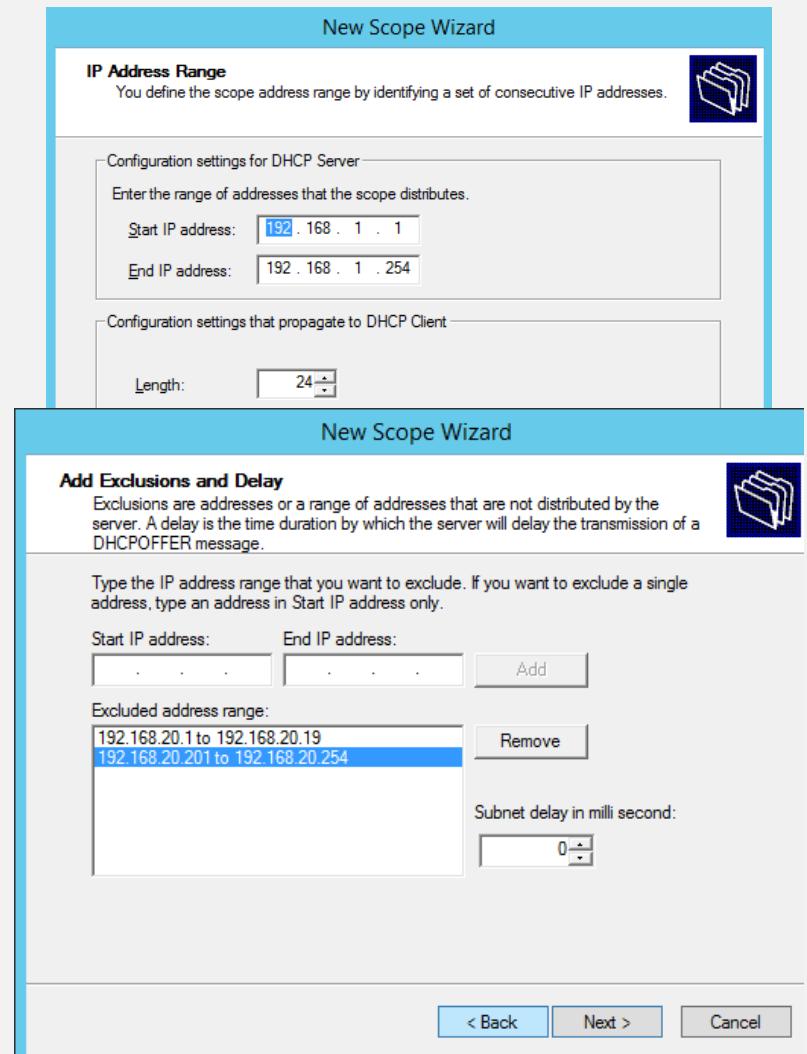
The screenshot shows the 'New Scope Wizard' interface, divided into two main sections:

- Scope Name**: A step where users enter a name and description for the scope. It includes fields for 'Name' and 'Description', and a note: "Type a name and description for this scope. This information helps you quickly identify how the scope is to be used on your network."
- IP Address Range**: A step where users define the range of addresses for the scope. It includes fields for 'Start IP address' (192.168.20.1) and 'End IP address' (192.168.20.254), and a note: "Enter the range of addresses that the scope distributes."

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

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

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

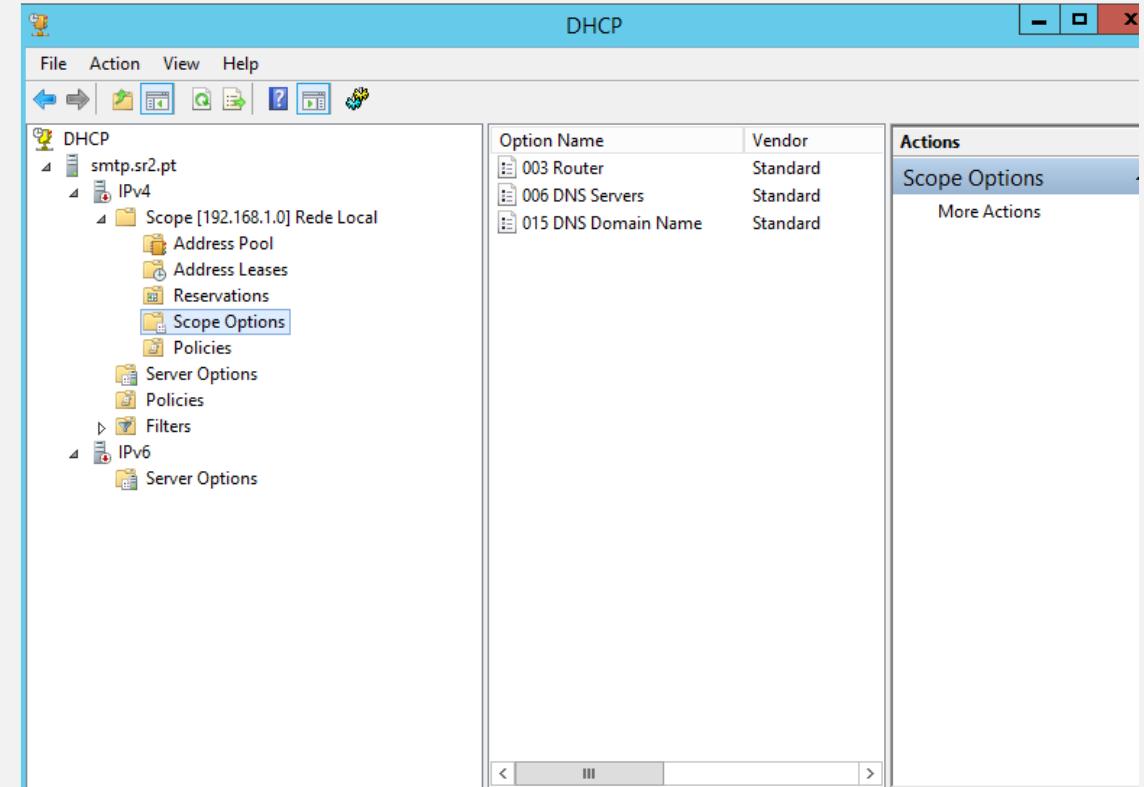
Filters

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 máquinas 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:

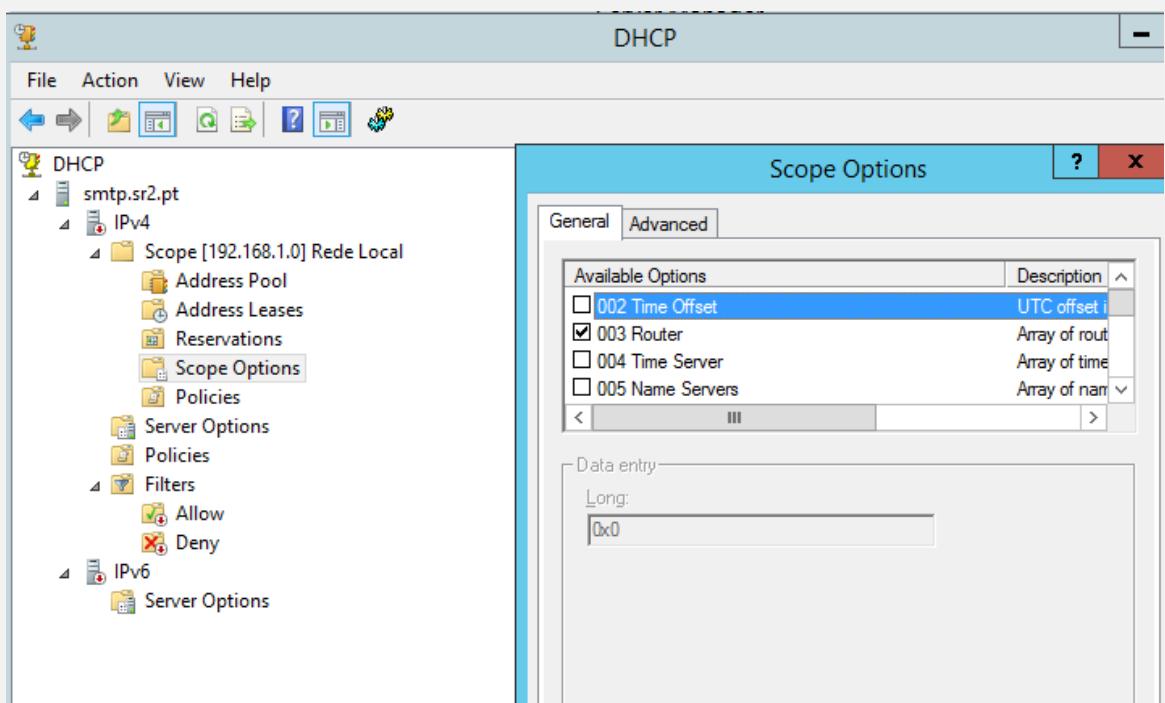
Supported types

Both
 DHCP
 BOOTP

Add Close

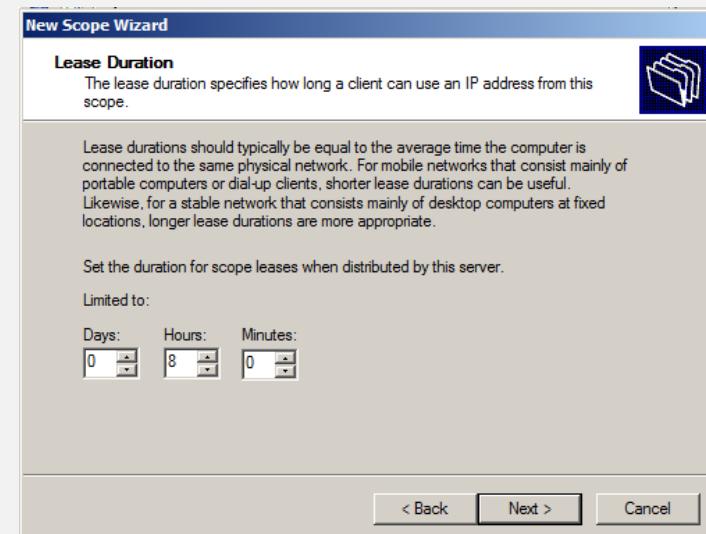
DHCP - *Server Options*

- 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.

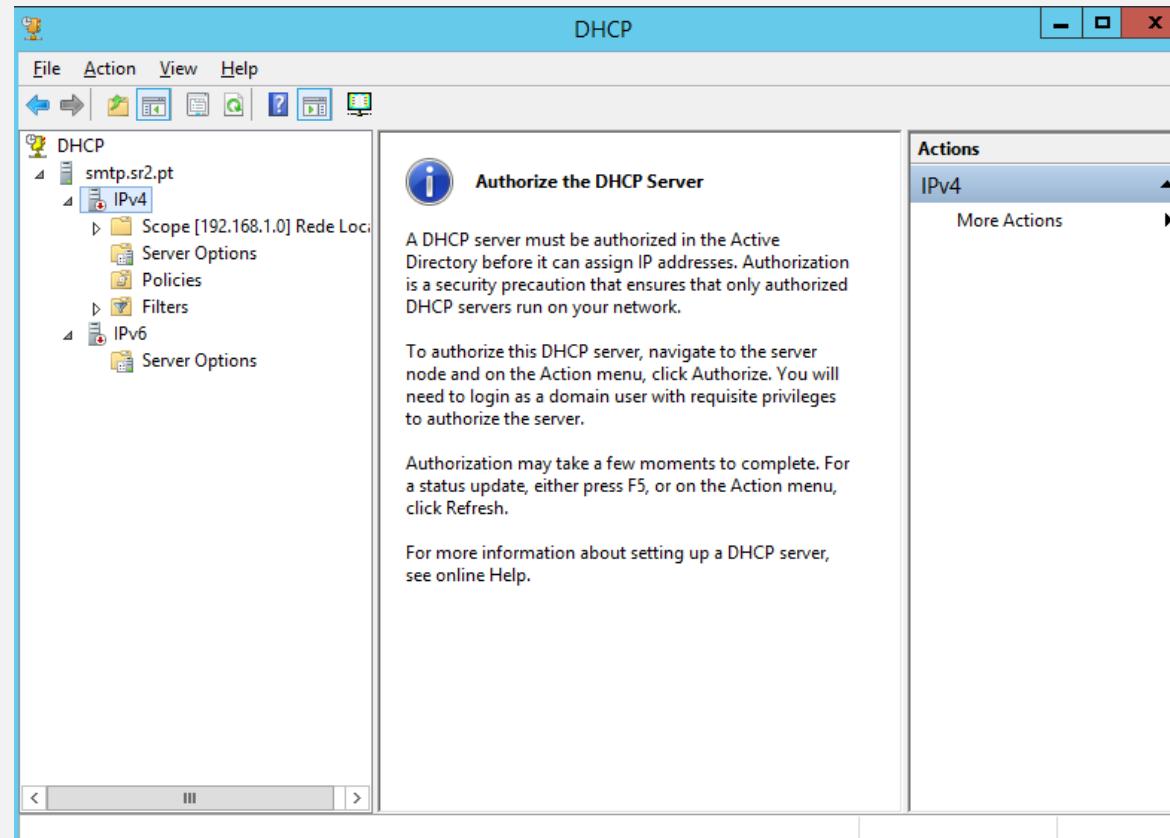


DHCP - Opções

- *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.



Ligaçāo DHCP - AD

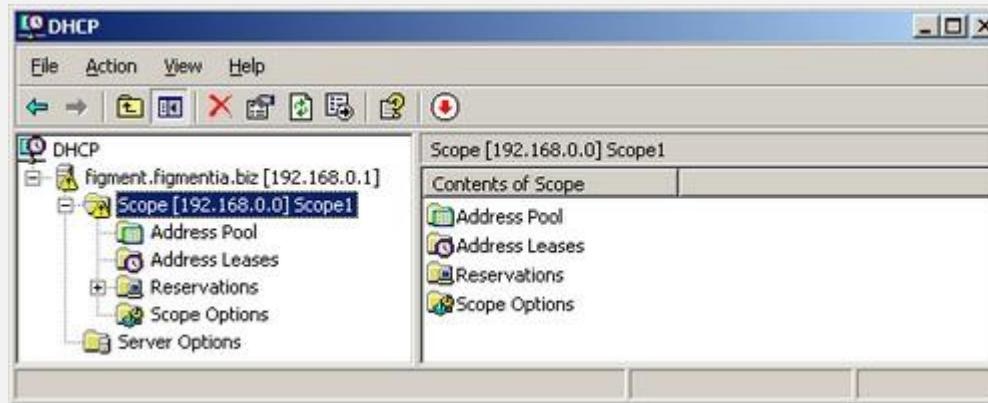


DHCP - Notas Finais

- *Superscopes*
 - Os *scopes* podem ser organizados/agrupados em *superscopes*
- *Dynamic Updates*
 - Os servidores podem ser configurados de modo a efectuar o registo dinâmico dos pares nome/IP em servidores DNS
- Redundância
 - Por questões de tolerância a falhas e balanceamento de carga é aconselhado a existência de dois servidores DHCP com a mesma gama configurada
- Atribuição baseada em politicas
- *DHCP Relay*

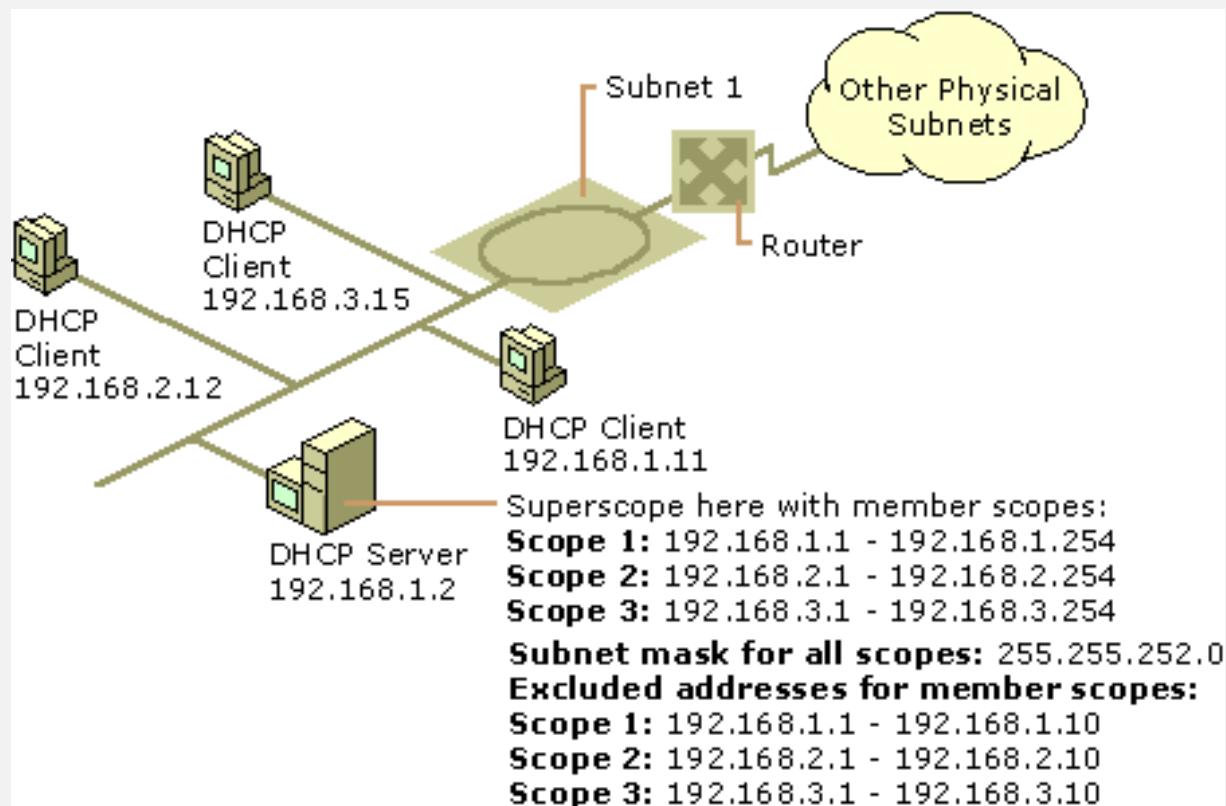
DHCP - *Superscopes*

- Os endereços IP de um servidor DHCP com o crescimento da rede podem ficar esgotados. Sobre a scope surge um sinal de exclamação...



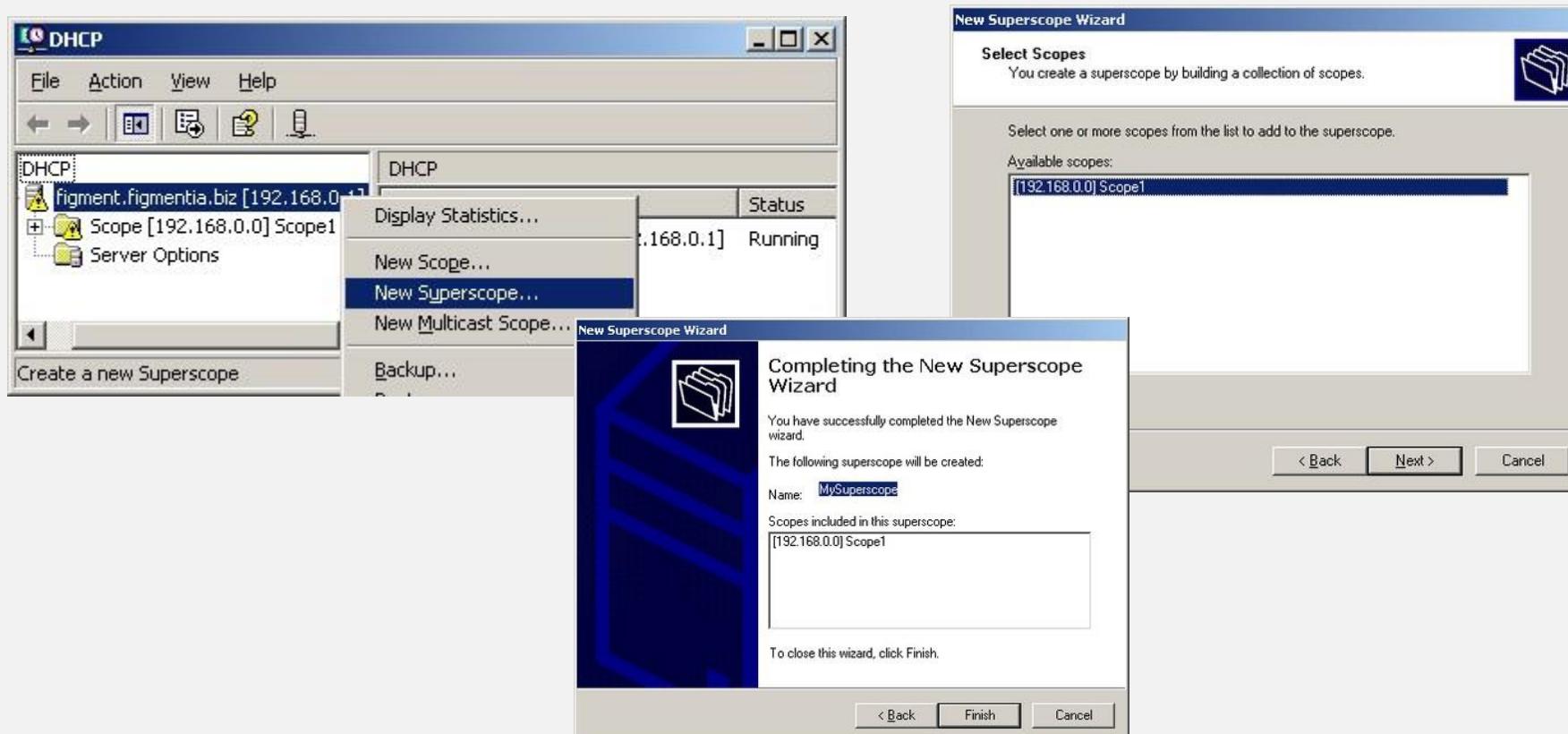
- Resoluções:
 - Comprar um router e um novo servidor DHCP em outra gama de endereços
 - Migrar toda a rede para uma classe superior
 - Ou ...

DHCP - *Superscopes*



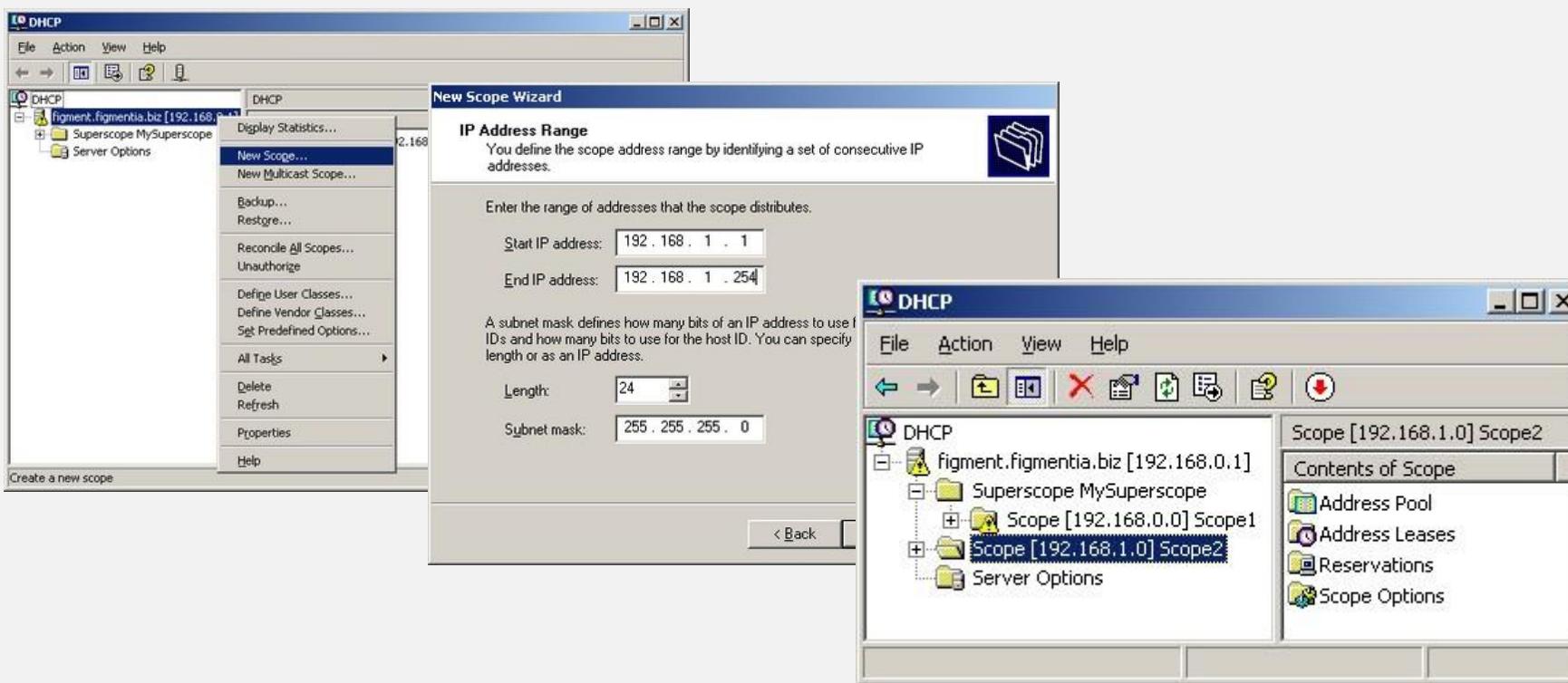
DHCP - *Superscopes*

- Pode criar um *superscope* que funciona como o pai de todas os outros que necessitamos de dar aos clientes



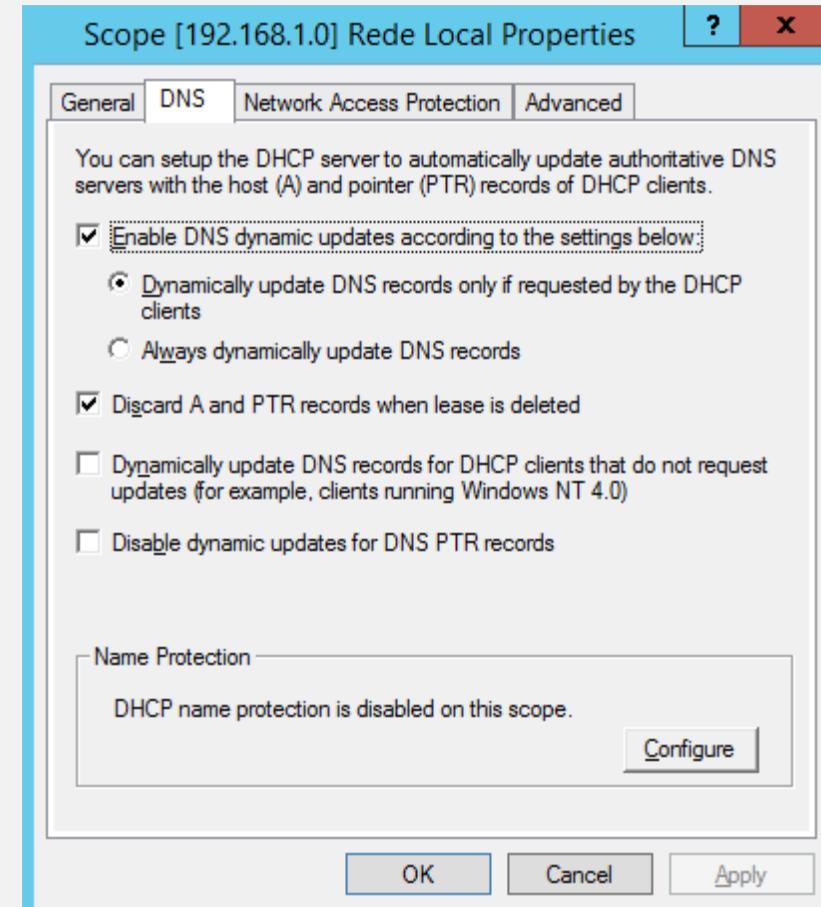
DHCP - *Superscopes*

- Tem agora de criar os scopes filhos



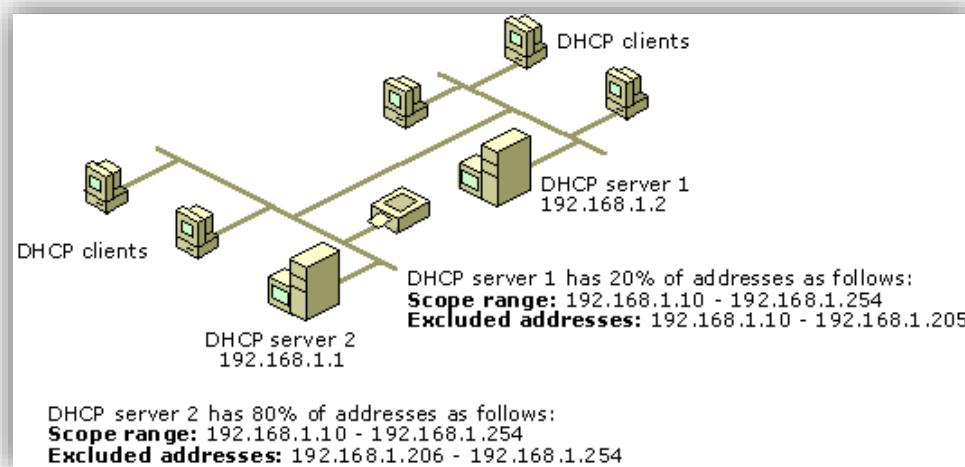
DHCP - DNS

- No windows server é possível colocar o DHCP a atualizar automaticamente o DNS.
 1. Ir Start | Administrative Tools e escolher DHCP
 2. Clicar com o botão do lado esquerdo no scope DHCP scope que se deseja configurar e escolher Properties.
 3. Clicar no Tab DNS e ativar essa possibilidade.
 4. Depois tem de ir ao servidor de DNS e aceitar esta possibilidade



DHCP - Redundância

- Ter mais de um servidor DHCP na mesma sub-rede fornece maior tolerância a falhas para atender a pedido dos clientes.
- Uma prática comum para equilibrar numa única rede os dois servidores DHCP é fazer com que X% dos endereços sejam distribuídos por um servidor DHCP e os Y% restantes sejam fornecidos por um segundo servidor (veja os gama de endereços excluídos em cada um dos servidores da imagem).
- Exemplo da regra dos 80-20:



Atribuição baseada em políticas

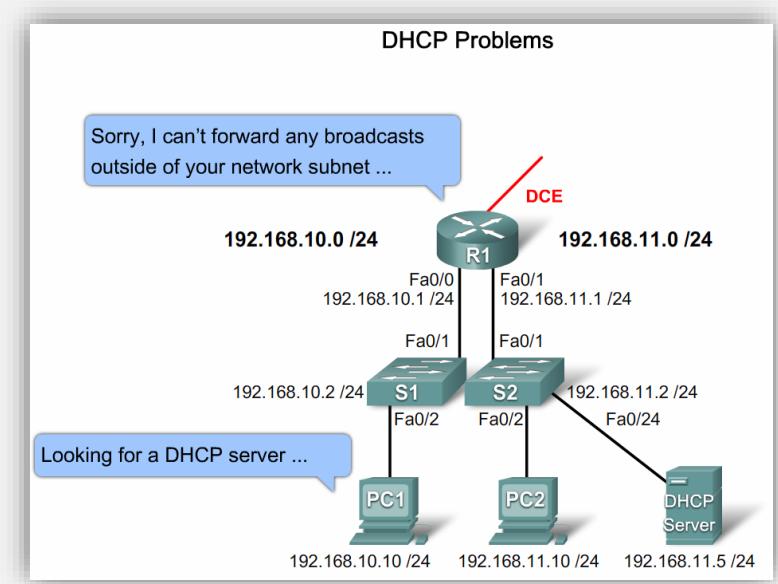
- **Múltiplos tipos de dispositivos:** Uma rede inclui muitos clientes diferentes como impressoras, telefones IP e desktops. Os administradores podem classificar esses dispositivos usando diferentes intervalos de endereço IP. Isto permite que as políticas de routing e qualidade de serviço (QoS) baseadas no intervalo do endereço IP controlem o acesso ou o tráfego na rede.
- **Múltiplas funções:** Uma rede inclui diferentes tipos de computadores, e servidores na mesma sub-rede. Dependendo do tipo de cliente, o administrador pode desejar fornecer diferentes configurações de duração da concessão. Todos os clientes wireless que se ligam através de um agente específico podem receber uma duração de concessão de quatro horas. As atualizações de DNS Dinâmico podem ser desativadas para clientes que corresponderem a esta política.

Atribuição baseada em políticas

- **Virtualização:** As máquinas virtuais são adicionadas e removidas dinamicamente dependendo dos requisitos de carga num determinado momento. O administrador pode fazer o routing do tráfego na rede de forma diferente para as máquinas virtuais podendo criar uma política baseada no prefixo do endereço MAC para atribuir uma duração curta de concessão, um intervalo específico de endereço IP e um gateway padrão diferente.

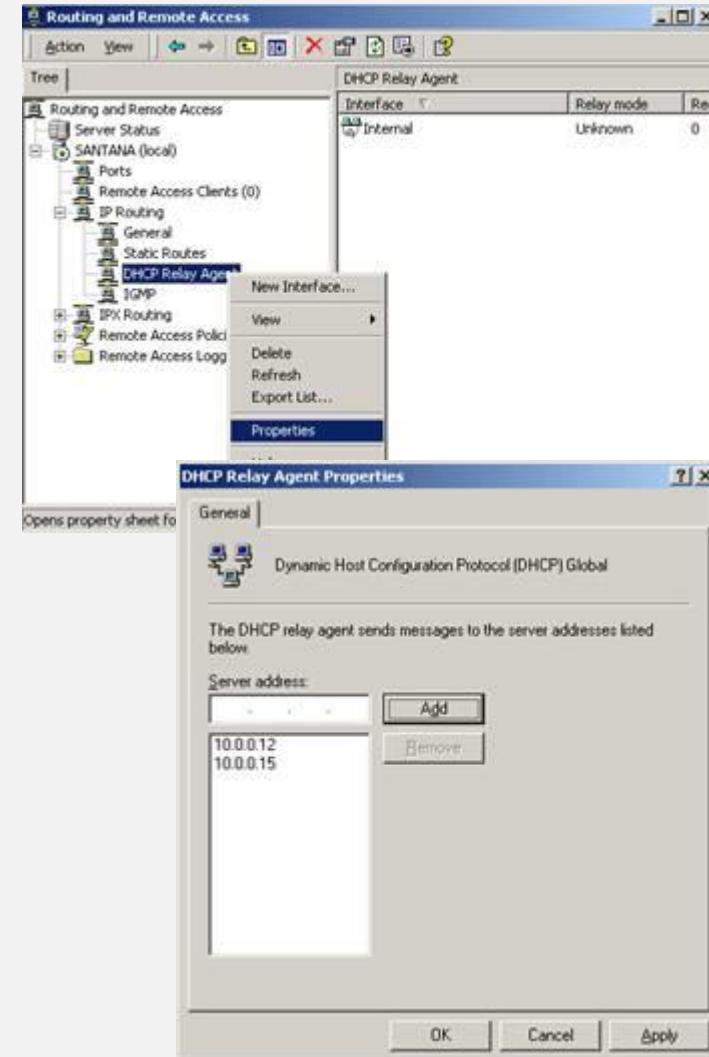
DHCP Relay

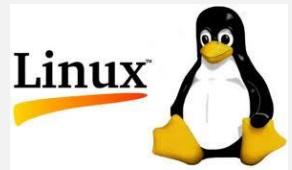
- Um cliente DHCP utiliza mecanismos de broadcast para localizar o DHCP e solicitar as configurações TCP/IP.
- Os routers por defeito não encaminham este tipo tráfego. Ou seja, os clientes só poderão obter as configurações do TCP/IP caso o servidor DHCP esteja localizado na mesma rede local.
- Pode haver 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 em um formato que o router os possa encaminhá-los para o servidor DHCP, ou seja, é um intermediário entre os clientes DHCP e o servidor DHCP.



DHCP Relay - windows

- O DHCP Relay Agent faz parte do serviço RRAS. Portanto, para que possamos configurar um DHCP Relay Agent deveremos habilitar o serviço RRAS
- Efetue logon com uma conta administrador;
- Abra o console Routing and Remote Access
 - Start, -> Administrative Tools, -> Server Manager;
 - Abra Roles, e Network Policy and Access Services, e clique em Routing and Remote Access RRAS;
- Clique no sinal de + ao lado da opção IP Routing (Roteamento IP);
- Clique com o botão direito sobre a opção DHCP Relay Agent (Agente de retransmissão DHCP) e clique em Properties (Propriedades);
- Escreva o endereço do servidor DHCP





Licenciatura em Engenharia Informática
Ramo de Redes e Administração de Sistemas

Dynamic Host Configuration Protocol (DHCP)
- Linux

Instalação do Serviço

- Das diferentes distribuições de Linux nesta aulas vamos considerar o Ubuntu 9.10.
- Ubuntu não tem incluído por omissão um serviço DHCP, portanto será necessário descarregar e instalar o serviço `dhcp3-server`
 - **`sudo apt-get install dhcp3-server`**
- Para que o servidor DHCP distribua IP's pelos clientes, é necessário alterar o seguinte ficheiro:
 - **`pico /etc/dhcp3/dhcpd.conf`**

Instalação do Serviço

- Neste ficheiro tem de configurar os seguintes aspetos:
 - **Opções Globais do Sevidor**
- ***option domain-name*** - Nome do domínio
- ***option domain-name-servers*** - IP do servidor de DNS
- ***Default-lease-time*** – define o tempo de duração em segundos do lease atribuído pelo servidor.
- ***Max-lease-time*** – tempo máximo em segundos que será atribuído a um lease
- ***[not] Authoritative*** – indica se o servidor é ou não autoritário para a rede em que está a servir endereços

Instalação do Serviço

- Depois tem de definir os parâmetros para a(s) scope(s) ou a(s) sub-net(s)
- **subnet** XXX.XXX.XXX.XX **netmask** YYY.YYY.YYY.YYY - identifica a rede
- **range** - define qual os endereços que vão ser disponibilizados (inicial e final)
- **option routers** - endereço IP do router
- **option broadcast** - endereço de broadcast
- **Default-lease-time** - define o tempo de duração em segundos desta lease. Se nada for dito será igual à definida para o servidor.
- **Host reserva** - indica os IP que pretende reservar

```
subnet 10.5.5.0 netmask 255.255.255.0 {  
    range 10.5.5.6 10.5.5.56;  
    option domain-name-servers dns.xpto.eu, 10.5.5.1;  
    option domain-name "xpto.eu";  
    option routers 10.5.5.254;  
    option broadcast-address 10.5.5.255;  
    default-lease-time 1200;  
    host reserva{  
        fixed-address 10.5.5.100;  
        hardware ethernet 00:80:ab:cd:ef:12;  
    }  
}
```

Instalação do Serviço

- Exemplo de um ficheiro já todo configurado para duas redes

```
option domain-name "grsi.eu"
option domain-name-servers 192.168.1.1;

default-lease-time 600;
max-lease-time 7200;

subnet 192.168.10.0 netmask 255.255.255.0 {
    range 192.168.10.10 192.168.10.128;
    option routers 192.168.10.254;
    option broadcast-address 192.168.10.255;
    default-lease-time 600;
    max-lease-time 7200;
}

subnet 192.168.20.0 netmask 255.255.255.0 {
    range 192.168.20.10 192.168.20.128;
    option routers 192.168.20.254;
    option broadcast-address 192.168.20.255;
    default-lease-time 600;
    max-lease-time 7200;
}
```

Teste do serviço

- Para testar o ficheiro de configuração deve digitar o comando

Dhcpd3 -t

- Para iniciar o serviço DHCP utilize o comando

Service dhcp3-serve start

- As leases atribuídas pelo serviço ficam registradas no ficheiro /va/lib/dhcp3/dhcp.leases

```
root@SrvRE:/var/lib/dhcp3# cat dhcpd.leases
# The format of this file is documented in the dhcpd.leases(5) manual page.
# This lease file was written by isc-dhcp-v3.1.2

lease 10.5.5.6 {
    starts 5 2011/06/03 14:40:11;
    ends 5 2011/06/03 15:00:11;
    cltt 5 2011/06/03 14:40:11;
    binding state active;
    next binding state free;
    hardware ethernet 00:03:ff:6f:d7:cf ;
    client-hostname "SrvRE";
}

lease 10.5.5.6 {
    starts 5 2011/06/03 14:49:09;
    ends 5 2011/06/03 15:09:09;
    cltt 5 2011/06/03 14:49:09;
    binding state active;
    next binding state free;
    hardware ethernet 00:03:ff:6f:d7:cf ;
    client-hostname "SrvRE";
}

root@SrvRE:/var/lib/dhcp3#
```

DHCP Relay

- 1. Instalar o serviço
 - sudo apt-get install dhcp3-relay
- 2. Editar o ficheiro
 - sudo pico /etc/default/dhcp3-relay
 - SERVERS="xxx.xxx.xxx.AAA xxx.xxxx.xxxx.BBB"
 - INTERFACES="eth1 eth2"
 - SERVERS corresponde aos IP's dos servidores DHCP e INTERFACES às interfaces onde o Relay Agent disponibiliza os IP's do DHCP.
- 3. Para finalizar a configuração do DHCP Relay, vamos reiniciar o serviço:
 - /etc/init.d/dhcp3-relay restart

Dúvidas



Referências

- Windows Server 2012, António Rosa, FCA.
- www.cisco.com – acedido em março de 2022.
- https://pt.wikipedia.org/wiki/Dynamic_Host_Configuration_Protocol - acedido em março de 2022.
- <https://www.youtube.com/watch?v=YYEG4ZCUIjs> – acedido em março de 2022
- <https://www.dcc.fc.up.pt/~rprior/1819/AR/slides/05%20-%20DHCP.pdf> – acedido em março de 2022.
- <http://www.ccc.ipt.pt/~ricardo/ficheiros/RedesComputadores.pdf> – acedido em março de 2022.

Serviços de Rede 1

2022-2023

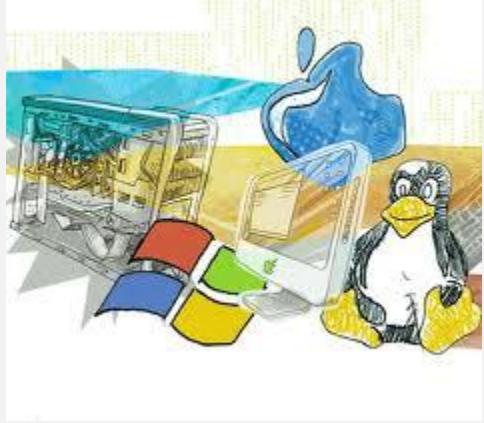
Pedro Miguel Geirinhas

Aula 5

NAT- Network Address Translation

Agenda

- 1.** Endereços Púlicos e Privados
- 2.** Os Diferentes tipos de NAT
- 3.** NAT - Cisco
- 4.** NAT - Windows



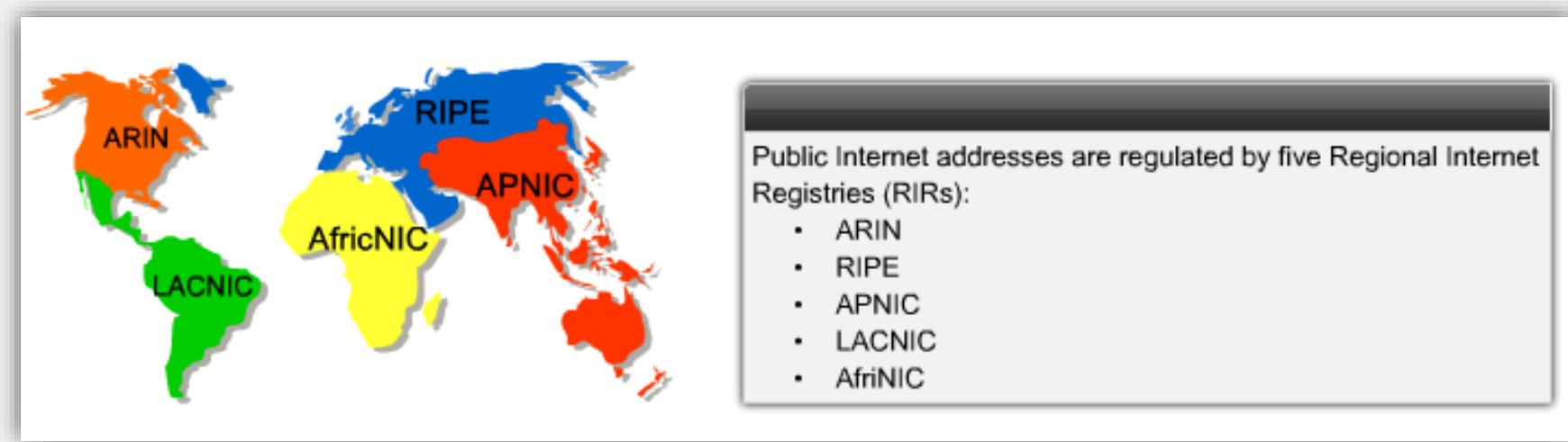
Serviços de Rede 1

NAT- Network Address Translation

© - Pedro Geirinhas

Endereços públicos

- Qualquer instituição ou empresa pode comprar ou alugar endereços IP ou gamas de IPs para atribuição a equipamentos que tenham a necessidade de acesso público.
 - O aluguer dos endereços pode ser solicitado ao ISP.
 - Os endereços IPs são disponibilizados aos ISP por entidades regionais a quem foi delegada essa competência.



Endereços privados

- Existem 3 conjuntos de endereços que não podem ser atribuídos especificamente a um cliente, estando reservados para utilização em redes privadas:
 - São designados por “endereços privados”.
 - Podem ser usados por milhões de equipamentos em simultâneo.
 - Os pacotes contendo esses endereços **não podem** ser encaminhados para o exterior.

Class	Private IP Address Range	Public IP Address Range
Class A	10.0.0.0 – 10.255.255.255	1.0.0.0 – 9.255.255.255 11.0.0.0 – 126.255.255.255
Class B	172.16.0.0 – 172.31.255.255	128.0.0.0 – 172.15.255.255 172.32.0.0 – 191.255.255.255
Class C	192.168.0.0 – 192.168.255.255	192.0.0.0 – 192.167.255.255 192.169.0.0 – 223.255.255.255

Private Internet addresses are defined in RFC 1918:		
Class	RFC 1918 Internal Address Range	CIDR Prefix
A	10.0.0.0 - 10.255.255.255	10.0.0.0/8
B	172.16.0.0 - 172.31.255.255	172.16.0.0/12
C	192.168.0.0 - 192.168.255.255	192.168.0.0/16

Endereços públicos e privados

- As máquinas com endereços privados não podem aceder directamente à internet.
- Os endereços públicos são um recurso limitado e atualmente escasso.
 - Não existem endereços suficientes para fazer face à quantidade de equipamentos que se encontram interligados.
- Contudo as máquinas têm de aceder e ser acedidas através da internet.
- Soluções:
 - IP V6
 - Máquinas intermédias a prestar os serviços pretendidos de forma indirecta (ex. *Proxys*).
 - **Tradução de endereços privados em endereços públicos (NAT)**.

Endereços públicos e privados

```
Linha de comandos
Microsoft Windows [Version 10.0.19042.867]
(c) 2020 Microsoft Corporation. Todos os direitos reservados.

C:\Users\pedro>ipconfig

Windows IP Configuration

Ethernet adapter Ethernet:
    Media State . . . . . : Media disconnected
    Connection-specific DNS Suffix . . .

Ethernet adapter Ethernet 3:
    Media State . . . . . : Media disconnected
    Connection-specific DNS Suffix . . .

Unknown adapter OpenVPN Wintun:
    Media State . . . . . : Media disconnected
    Connection-specific DNS Suffix . . .

Ethernet adapter Ethernet 4:
    Connection-specific DNS Suffix . . .
    Link-local IPv6 Address . . . . . fe80::3529:bd4d:23c5:aefd%40
    IPv4 Address. . . . . : 192.168.56.1
    Subnet Mask . . . . . : 255.255.255.0
    Default Gateway . . . . . :

Unknown adapter OpenVPN TAP-Windows6:
```



what is my ip address

Cerca de 1 830 000 000 resultados (0,57 segundos)

What's my IP

94.61.232.45

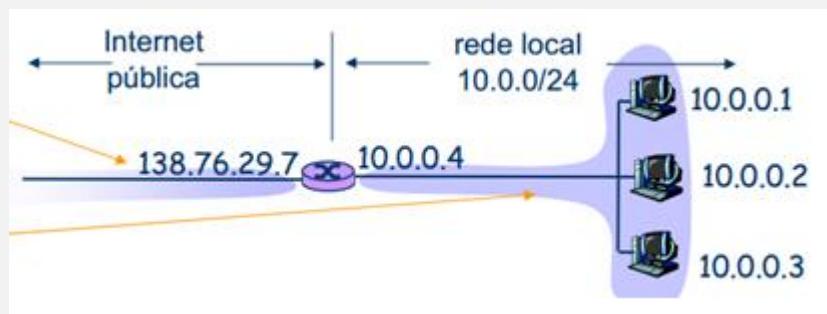
Your public IP address

→ Learn more about IP addresses

NAT

Network Address Translation (NAT)

- Com o NAT pode-se expandir o espaço de endereçamento IP através da utilização de endereços privados.



- Está regulamentado e definido nos seguintes RFCs:
 - 3022 – Traditional IP Network Address Translator (NAT)
 - 1918 – Address Allocation for Private Internets

Vantagens

- Permitem criar redes sem adquirir endereços válidos.
- Garante que os endereços privados não são passados para o domínio público.
- Garantem maior capacidade de gestão do espaço de endereçamento.
- Aumenta a flexibilidade do acesso a redes públicas.
- Garante uma gestão mais racional e eficiente do endereçamento público.
- Facilidade de mudança de ISP.
- Permite a criação de redes mais seguros e com maior garantia de privacidade de dados.

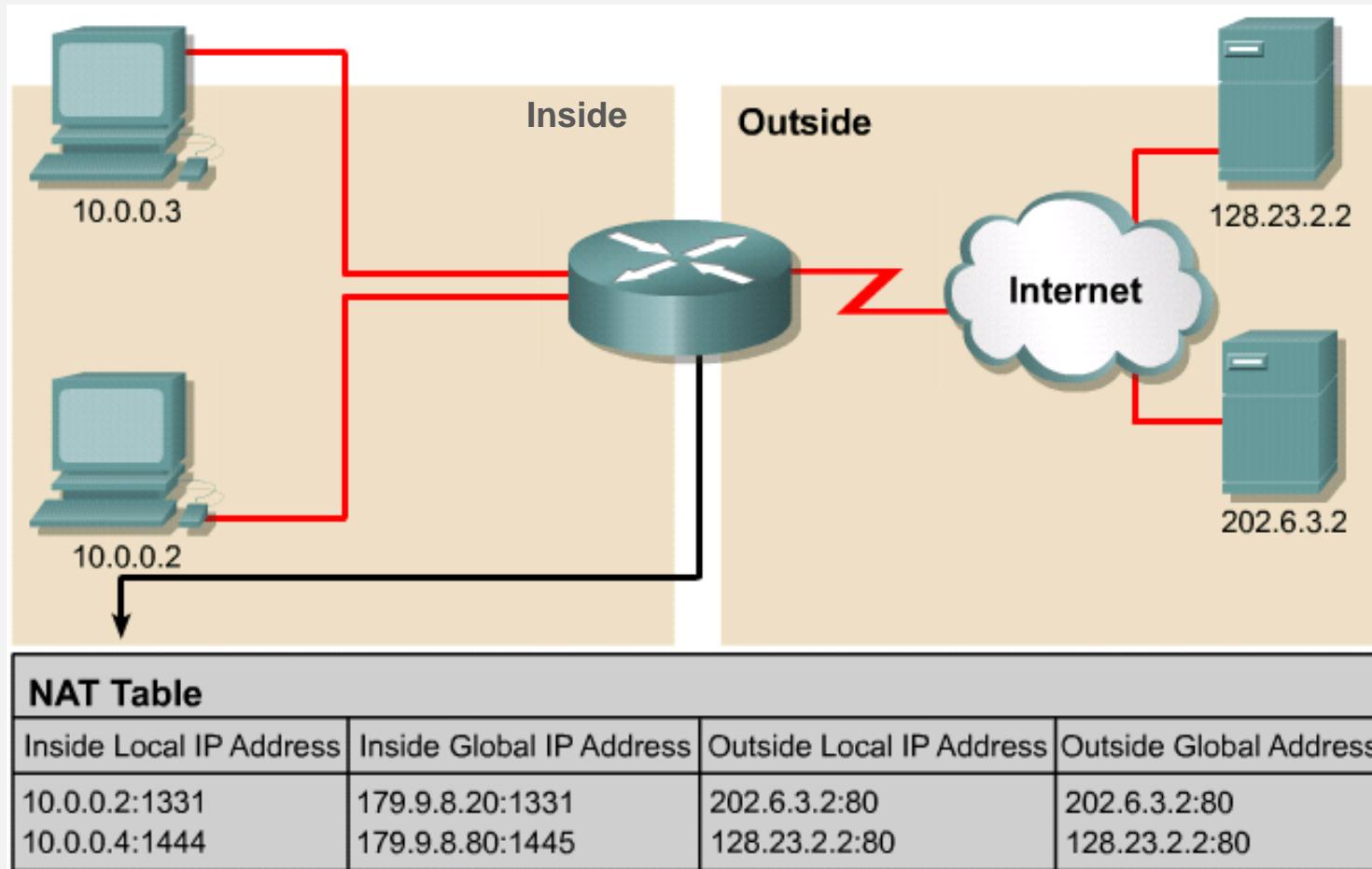
Desvantagens

- Nem todos os protocolos/aplicações suportam e/ou trabalham bem com o NAT.
- Pode aumentar a probabilidade de endereçamento incorreto.
- Diminui a performance do sistema de comunicação:
 - Aumenta o atraso do processo;
 - O primeiro pacote é traduzido sempre de forma mais lenta;
 - Como a CPU tem de analisar cada pacote para perceber se deve traduzi-lo ou não vai provocar atraso e maior necessidade de processamento;
 - É preciso alterar o endereço IP sempre que vai traduzir.
 - A tabela NAT consome memória.
- Deixamos de conseguir “reconstruir” toda a rota dos pacotes de dados.
- Dificulta a criação de tuneis.

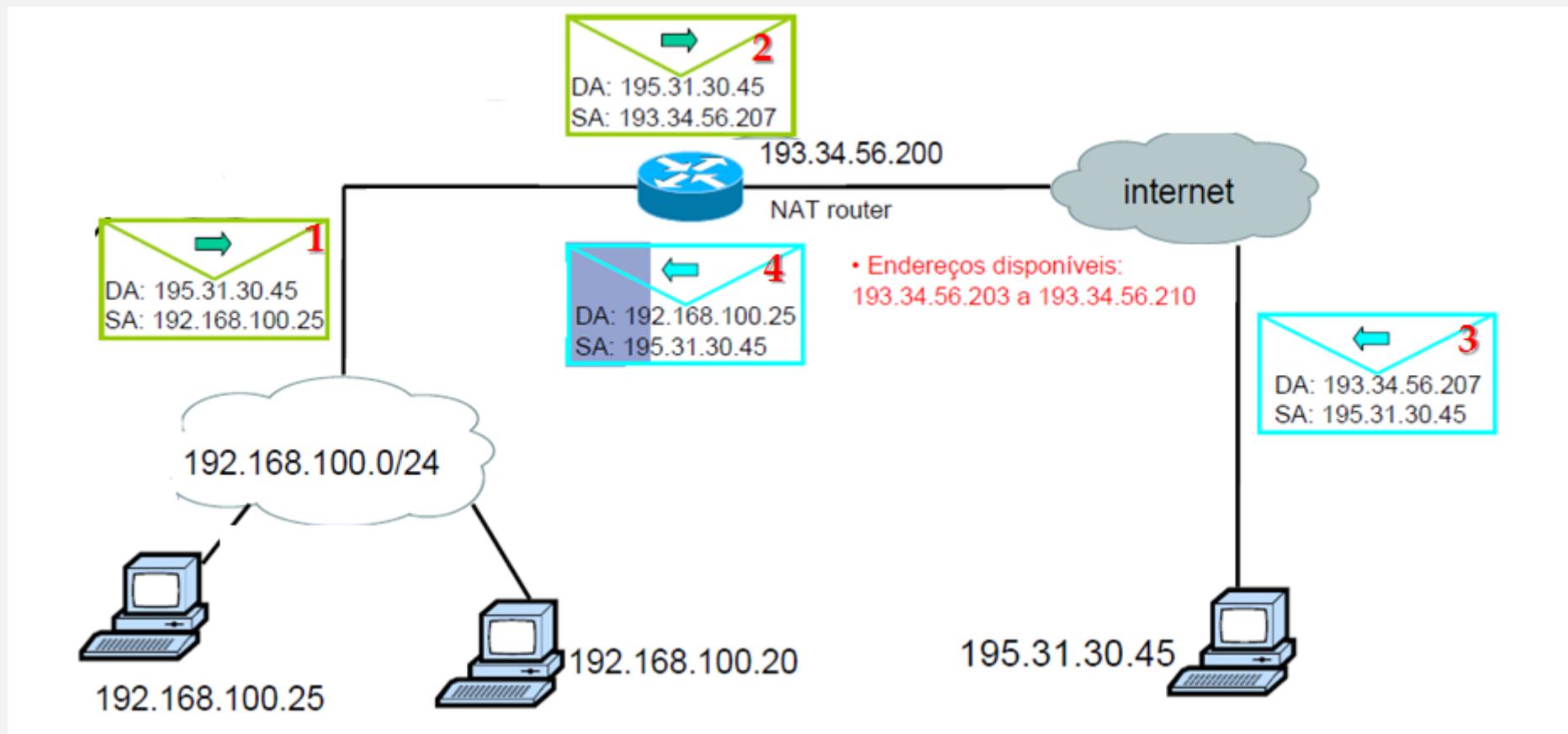
Termos

- **Endereço local interno** (*Inside local address*) – Endereço IP atribuído a um *host* da rede interna. Provavelmente, esse endereço é privado.
- **Endereço global interno** (*Inside global address*) – Um endereço IP legítimo atribuído pelo ISP e que representa um ou mais endereços IP públicos.
- **Endereço local externo** (*Outside local address*) – Endereço IP de um *host* externo, tal como é conhecido pelos *hosts* da rede interna.
- **Endereço global externo** (*Outside global address*) – Endereço IP atribuído a um *host* da rede externa. O proprietário do *host* atribui esse endereço. Na maioria das vezes estes dois endereços são iguais.

Termos



Funcionamento

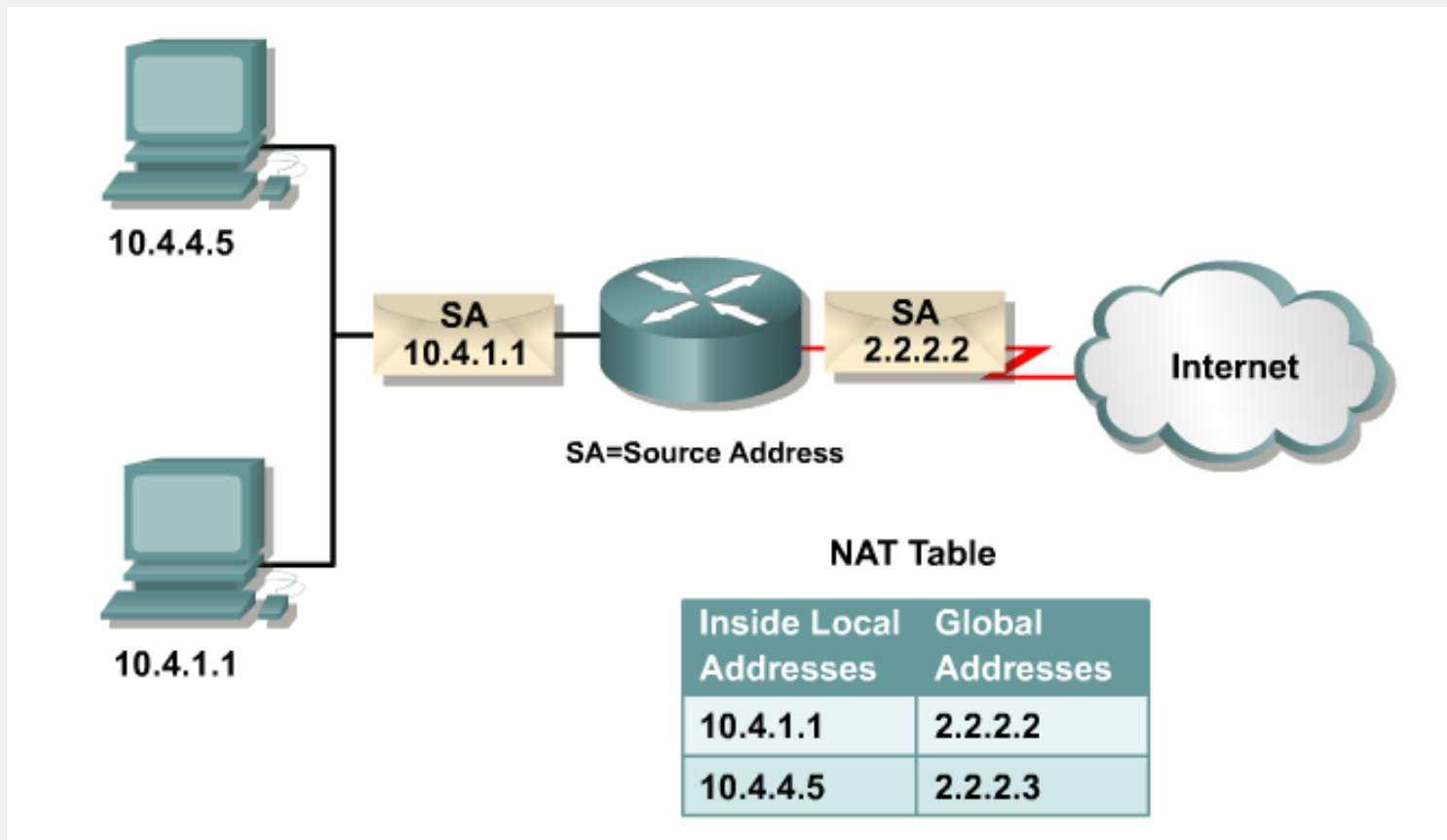


NAT - Fases

- **datagrama de saída:** substituir (*endereço IP privado de origem, porto*) de cada *datagrama de saída* por (*endereço IP público, novo porto*)
 - Os clientes/servidores remotos respondem usando como endereço de destino (*endereço IP público, novo porto*).
- **guardar** na tabela de tradução NAT todos os pares (*endereço IP privado de origem, porto*), (*endereço IP público, novo porto*).
- **datagrama de entrada:** substituir (*endereço IP público, novo porto*) no campo de endereço de destino de cada *datagrama de entrada* o valor correspondente na tabela de tradução NAT (*endereço IP privado de origem, porto*).

Tabela

- O equipamento que está a ter a função de NAT, regista numa a associação entre os endereços internos e externos.



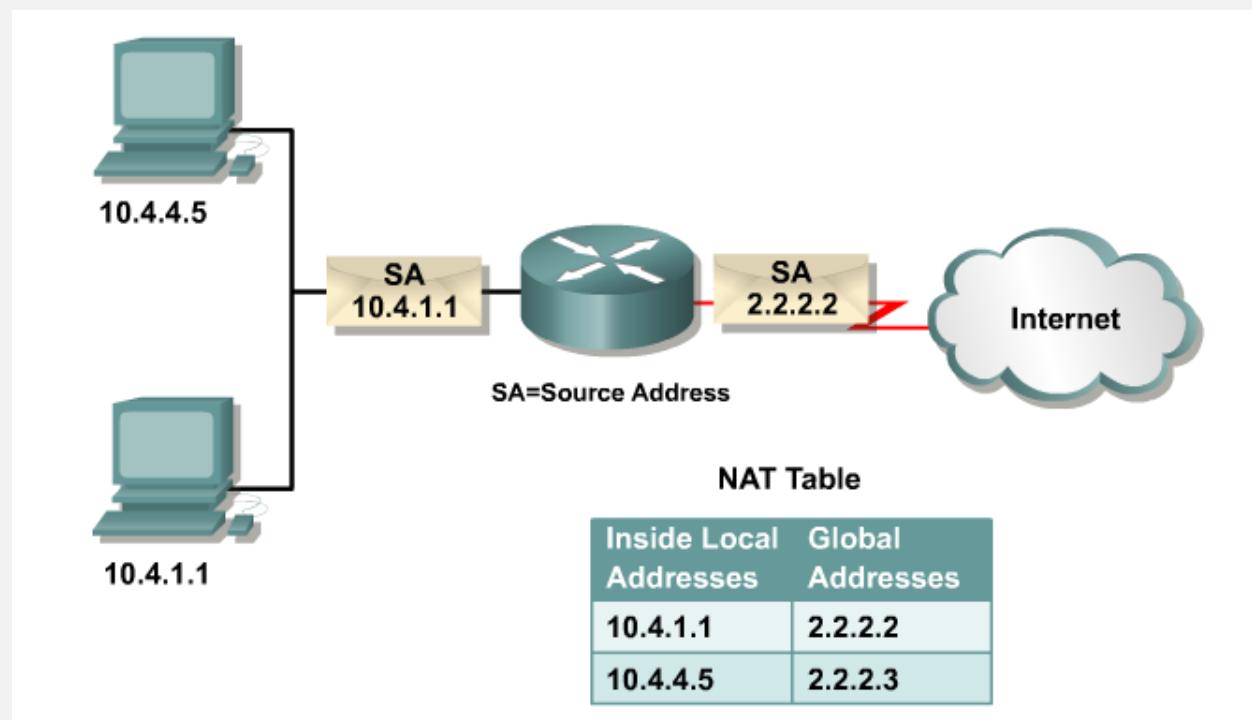
Tipos

- Existem os seguintes tipos de NAT:
 - **NAT Estático** - um endereço IP público para um endereço IP privado.
 - **NAT Dinâmico** - existe um conjunto de endereços públicos (*pool*), que as máquinas que usam endereços privados podem usar.
 - **PAT (Network Address Port Translation) ou NAT Overload** - Um endereço IP público para “n” endereços IP privados. Esta é certamente a técnica mais usada.
 - **Twice NAT** – o endereço publico é fornecido mediante condição ou condições internas ou externas.
 - **Destination NAT**– dar um endereço privado a uma maquina com o endereço público (“reverse NAT”).

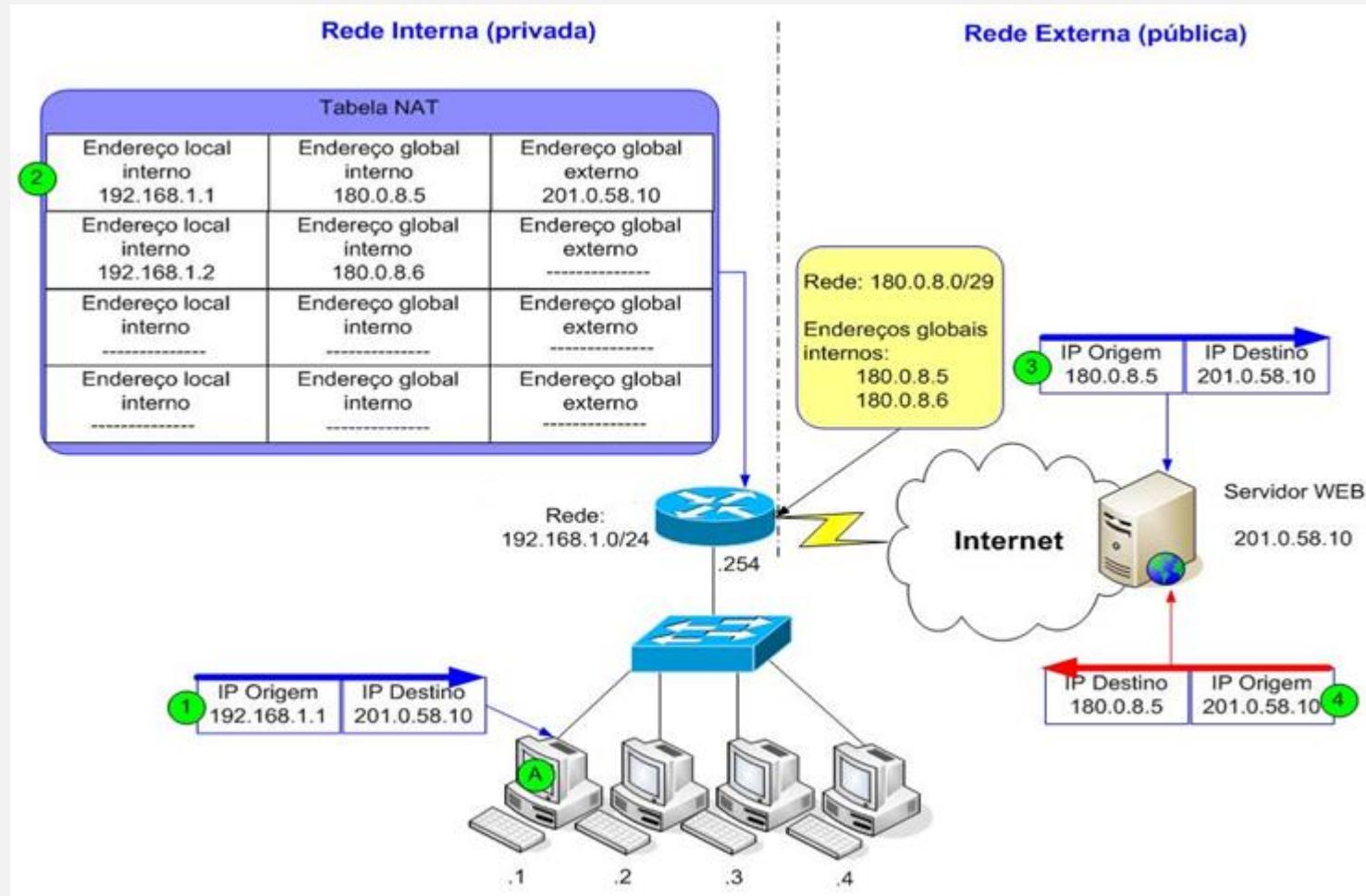
NAT Estático

- O NAT Estático faz o mapeamento direto de **endereços privados** para **endereços públicos**. Um IP privado será sempre associado ao mesmo IP público (regra de ‘um para um’).
- Este tipo de NAT é útil quando se quer fazer a referência de determinado dispositivo com um endereço IP consistente e constante.
- Não permite contudo fazer gestão e “poupança” dos endereços públicos disponíveis.

NAT Estático



NAT Estático

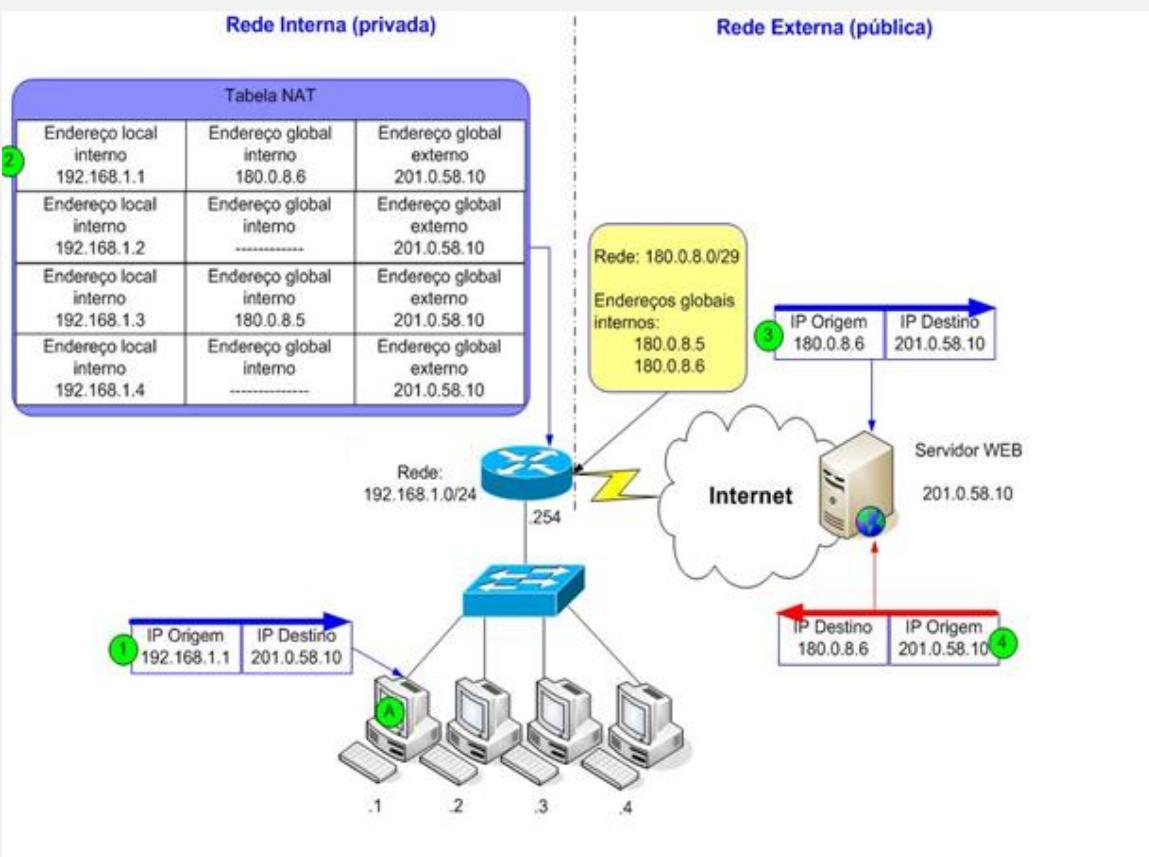


NAT Dinâmico

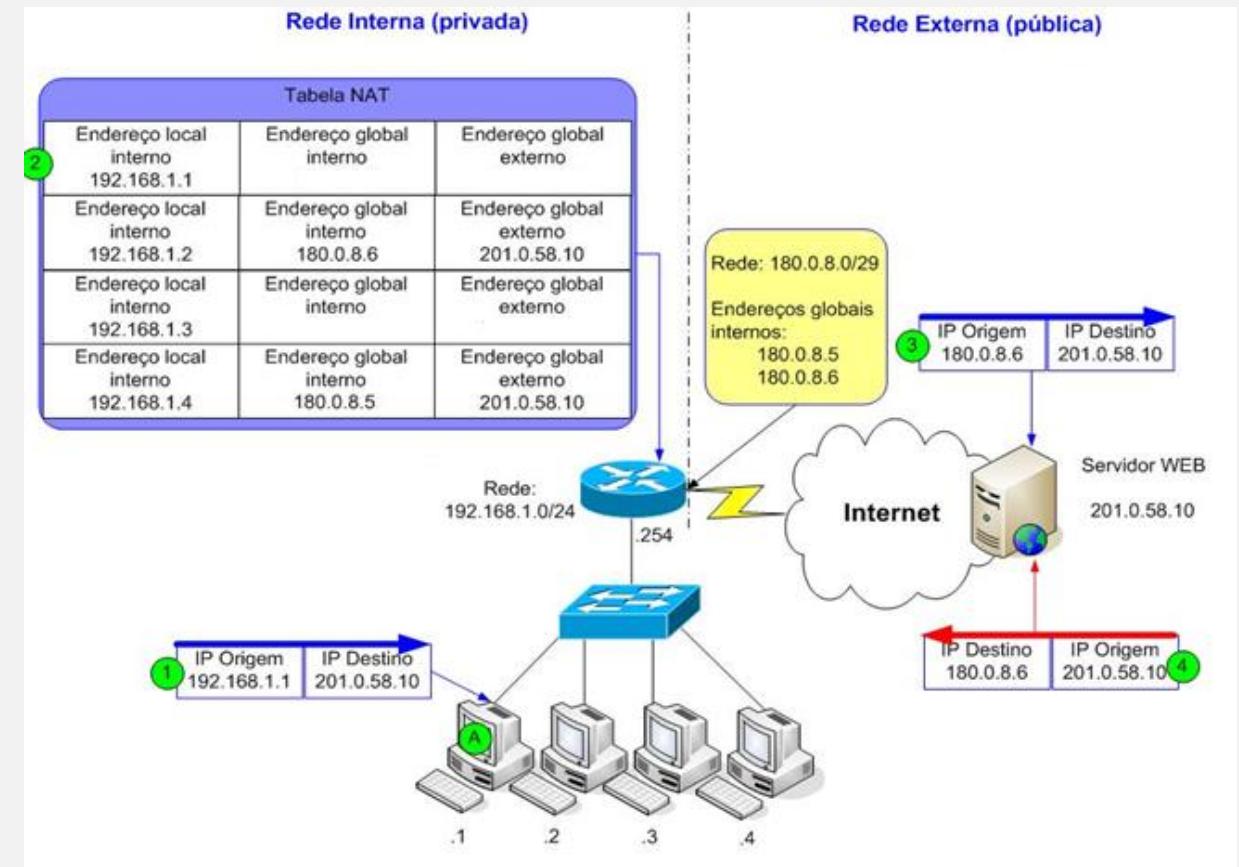
- O NAT Dinâmico faz o mapeamento de endereços privados para endereços públicos de forma dinâmica.
- Assim, qualquer endereço privado pode ser traduzido para uma gama de endereços públicos de forma dinâmica.
- Contrariamente ao NAT Estático, os endereços internos nem sempre vão ser traduzidos para o mesmo endereço público.
- Permite fazer uma gestão mais eficiente dos endereços públicos disponíveis.

NAT Dinâmico

1º Instante



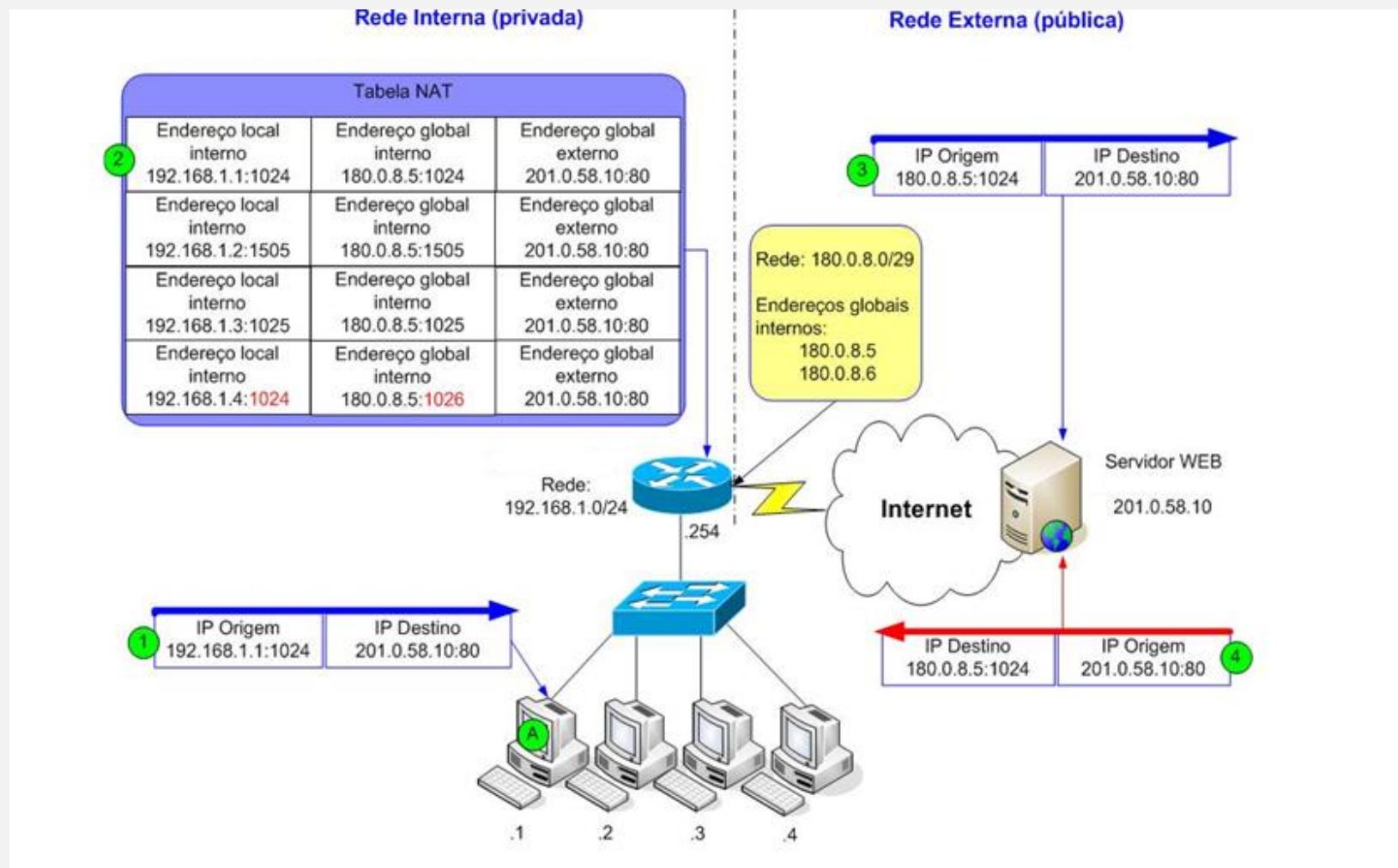
2º Instante



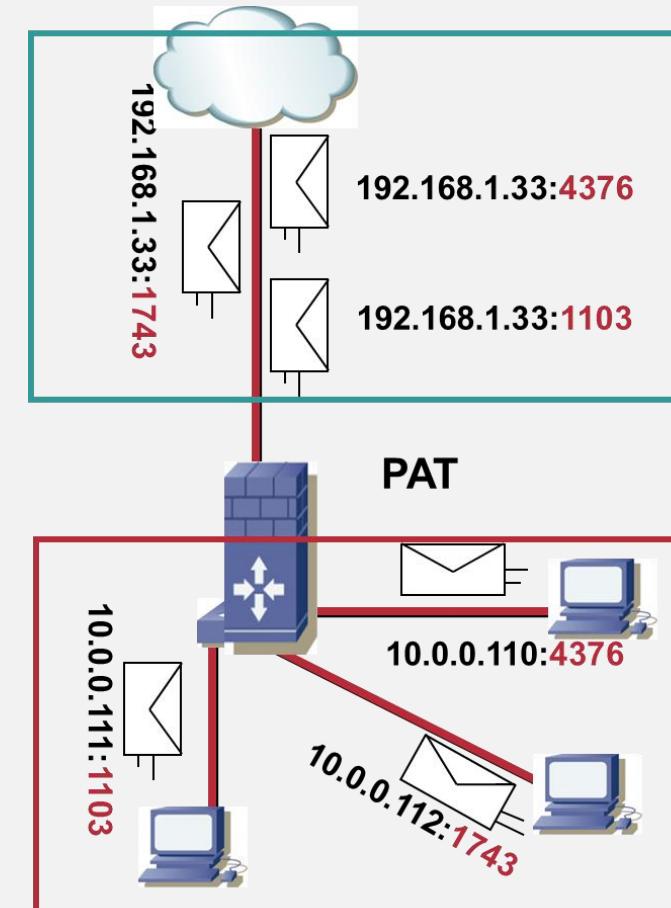
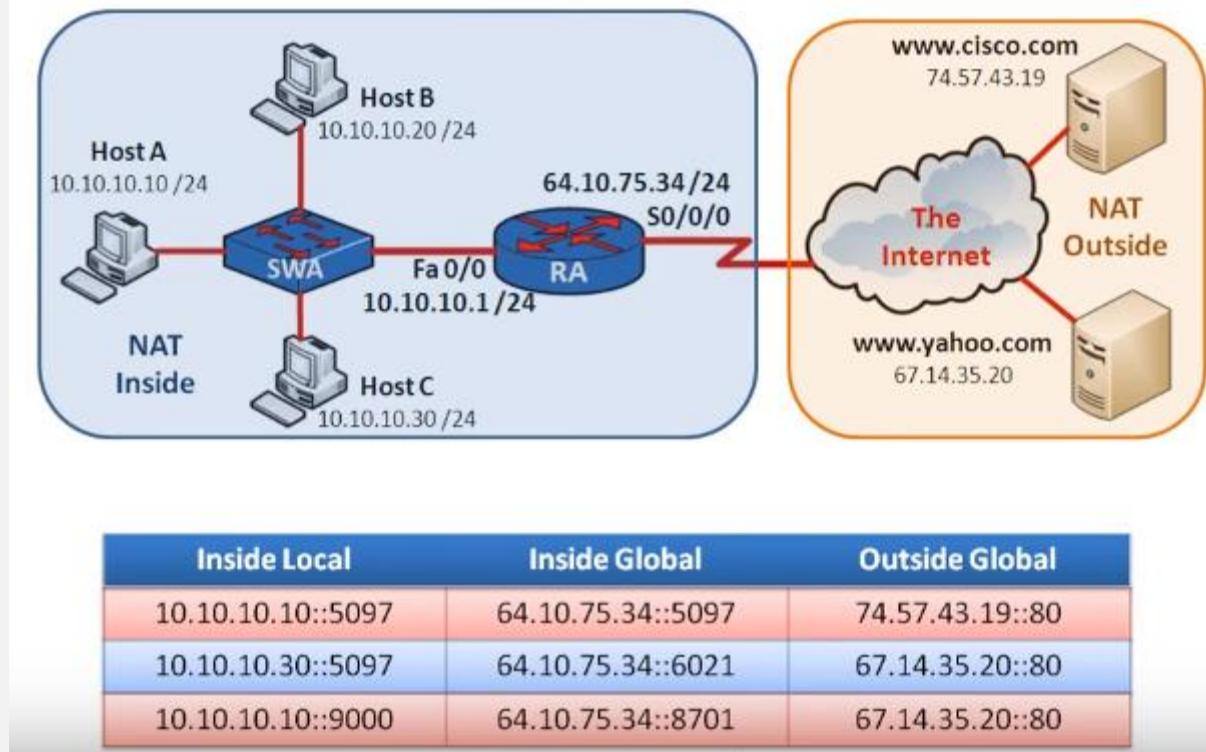
PAT - Network Address Port Translation ou NAT Overload

- O PAT ou *NAT Overload* surge como solução mais utilizada já que assim não são necessários tantos endereços públicos quantos os equipamentos que pretendem comunicar com o exterior.
- O número de portas disponíveis é de 65536 (16 bits), alocadas nos grupos de 0-511, 512-1023 ou 1024-65535. Desta forma, inúmeros dispositivos podem usar o mesmo endereço público, pois serão diferenciados pelo número da porta que estão a utilizar para comunicar.
- A distinção entre as comunicações é realizada com base no porto origem:
 - Quando dois equipamentos pretendem comunicar usando o mesmo valor para o porto origem, o serviço de NAT utiliza o porto seguinte que esteja livre.
 - Caso não existam portos livres mas tenha sido configurada uma *pool* com vários endereços IP, é usado o próximo endereço IP, tentando respeitar o porto originalmente escolhido.

Network Address Port Translation



Network Address Port Translation



Twice NAT

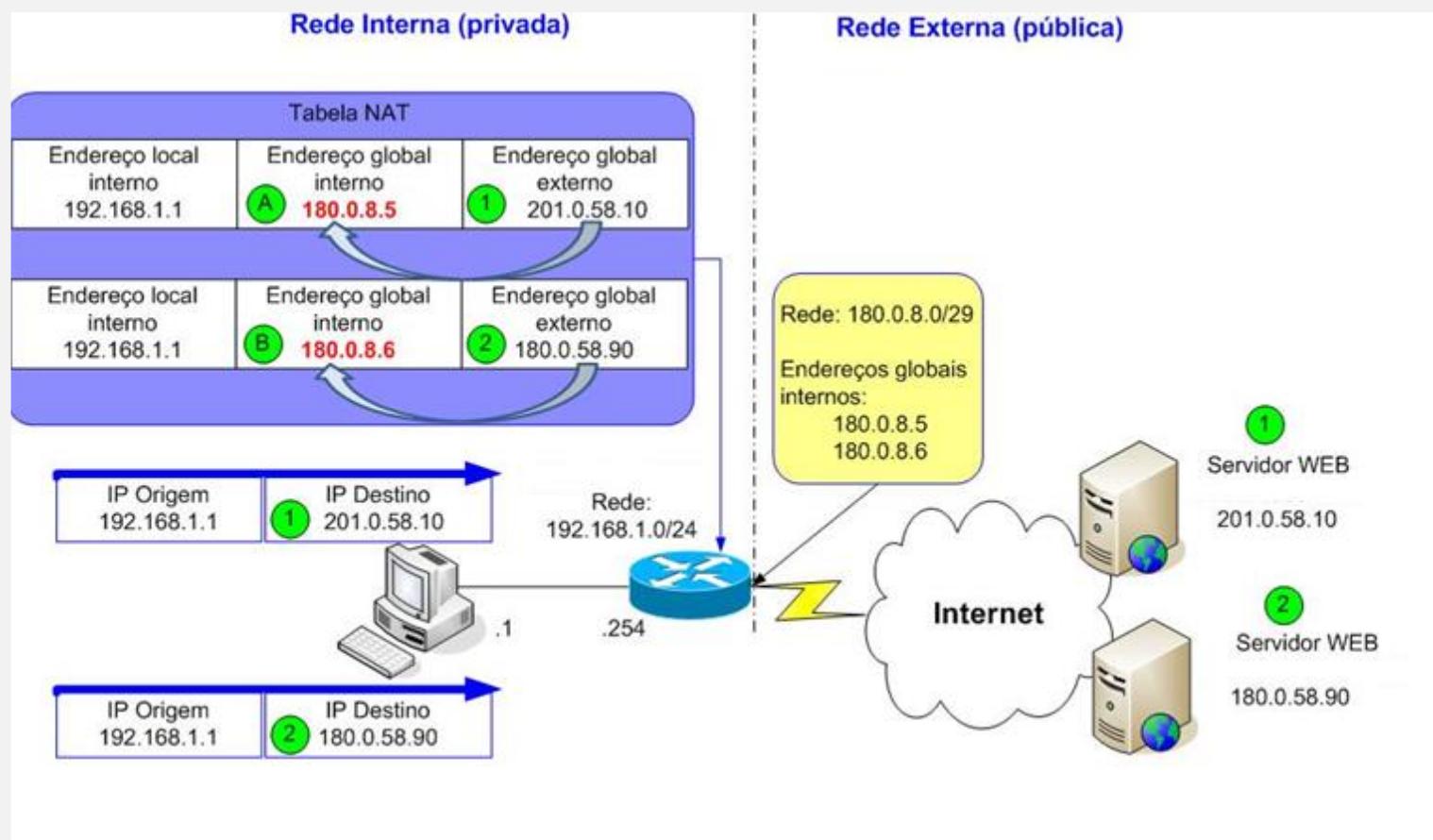
O Twice NAT permite que se decida qual o endereço público que será utilizado no processo de mapeamento, baseado no IP de destino ou pelo número da porta de destino.

Pode-se criar regras para determinar que um endereço interno seja traduzido para determinado endereço público, tomando como determinante o seu destino.

Ou no caso de portas, o determinante será o número da porta de destino.

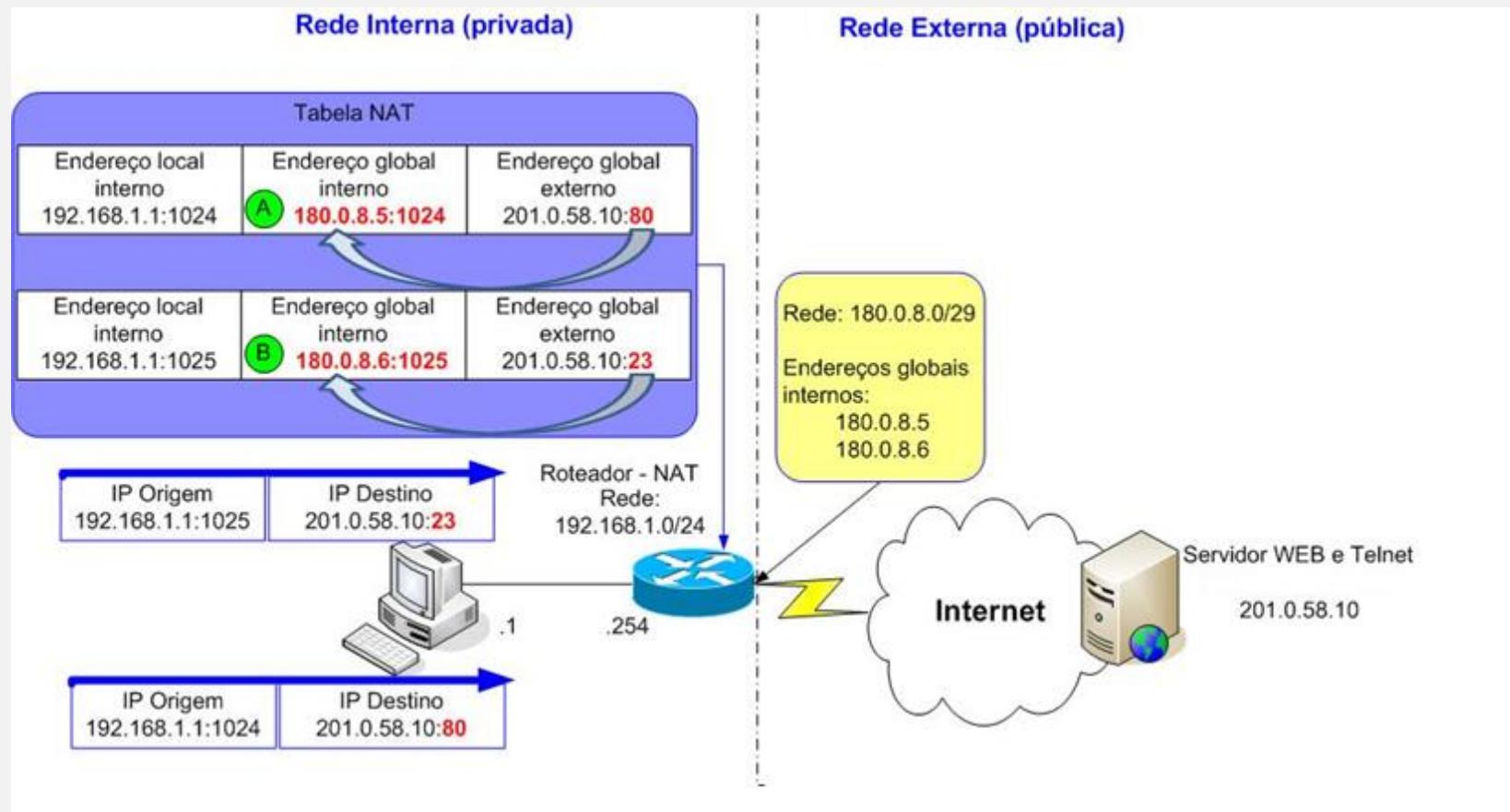
Twice NAT

- Determinante: Endereço IP do destino.



Twice NAT

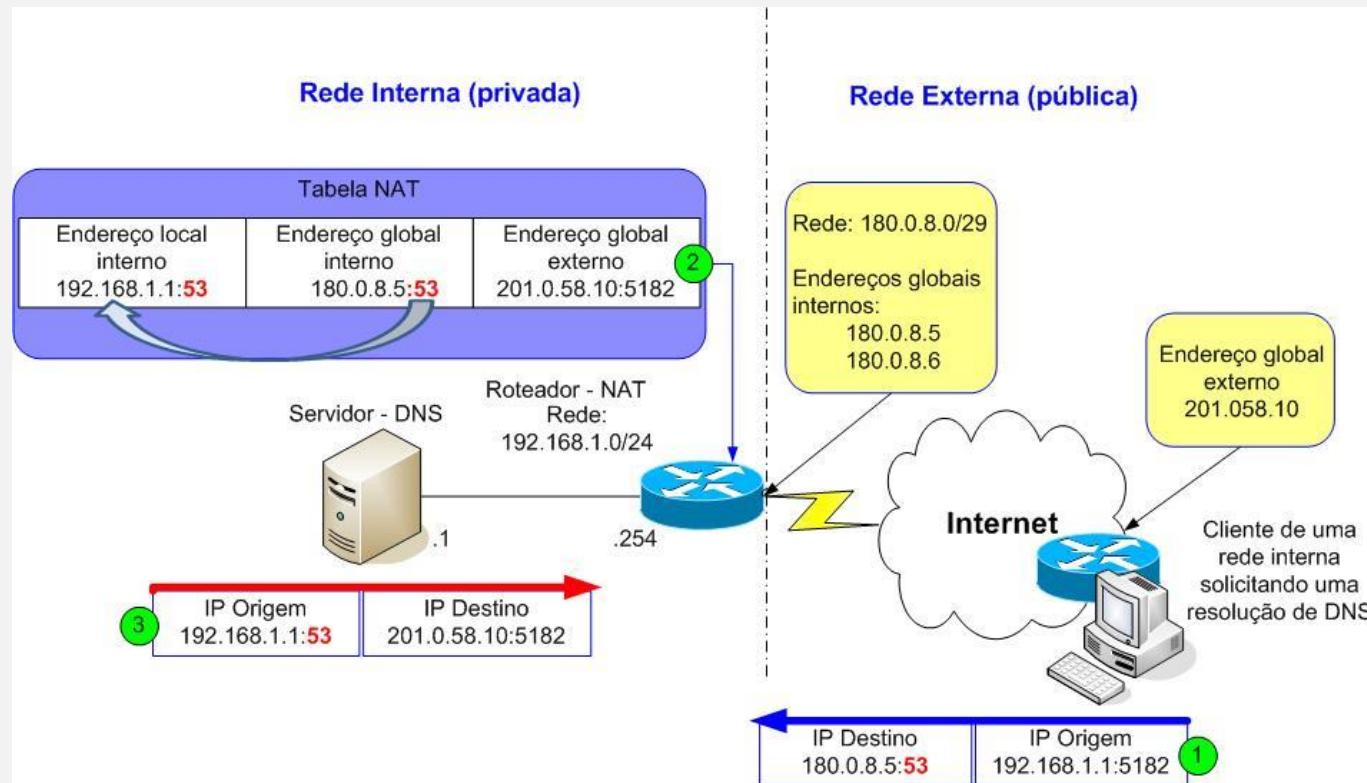
- Determinante: Número da porta do destino.



Destination ou Reverse NAT

- Com o Destination NAT as ligações são iniciadas a partir de hosts da rede pública (Internet).
- Esta característica foi incorporada no NAT para possibilitar capacidades/funcionalidades mais avançadas.
- Como, os *hosts* das redes externas não sabem o endereço IP de *hosts* da rede interna, então não podiam aceder a um recurso que estivesse localizado internamente. Para que isso aconteça temos de fazer um “Reverse NAT”.

Destination NAT





Network Address Translation (NAT) - Cisco

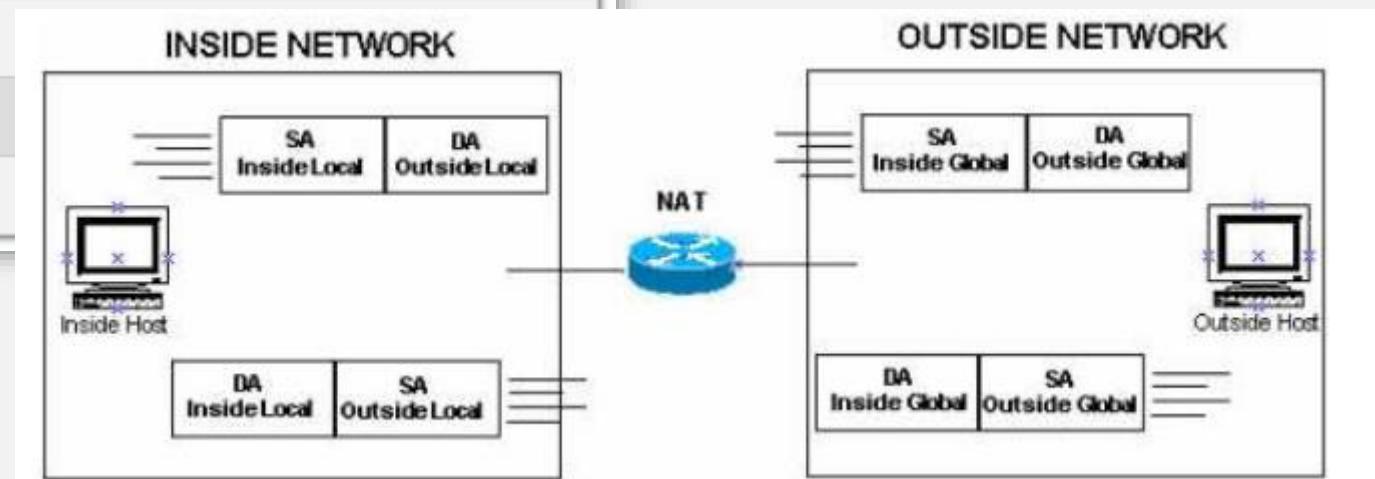
Serviços de Rede 1

Ano Letivo 2022-2023

NAT estático: configuração

Configuring Static NAT

Step	Action	Notes
1	Establish static translation between an inside local address and an inside global address. <code>Router(config)#ip nat inside source static local-ip global-ip</code>	Enter the global command <code>no ip nat inside source static</code> to remove the static source translation.
2	Specify the inside interface. <code>Router(config)#interface type number</code>	Enter the <code>interface</code> command. The CLI prompt will change from <code>(config) #</code> to <code>(config-if) #</code> .
3	Mark the interface as connected to the inside. <code>Router(config-if)#ip nat inside</code>	
4	Exit interface configuration mode. <code>Router(config-if)# exit</code>	
5	Specify the outside interface. <code>Router(config)#interface type number</code>	
6	Mark the interface as connected to the outside. <code>Router(config-if)#ip nat outside</code>	



NAT estático: configuração

Configuring Static NAT

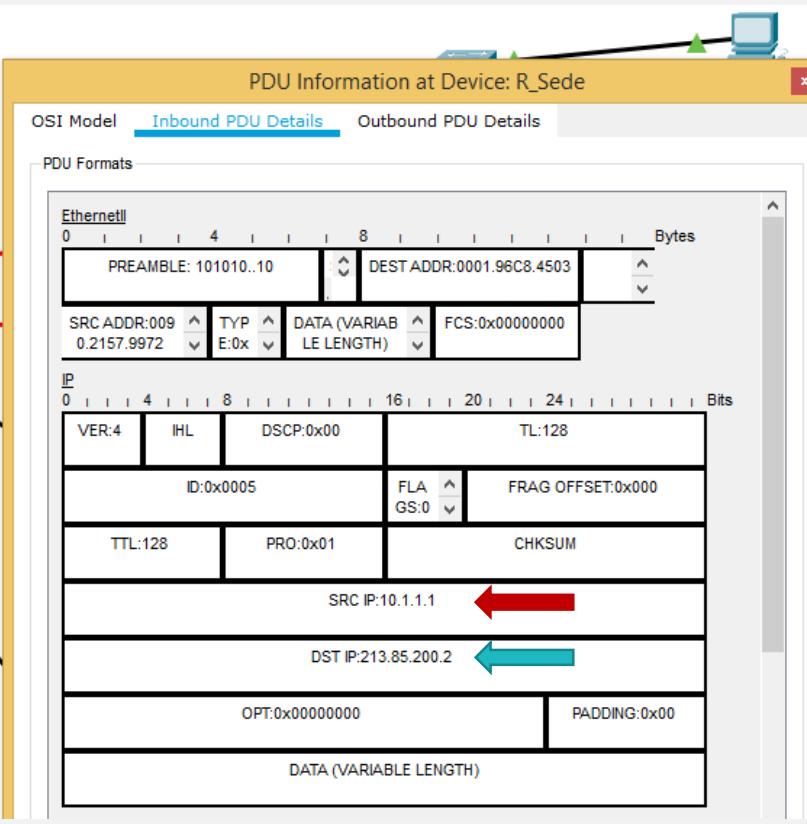
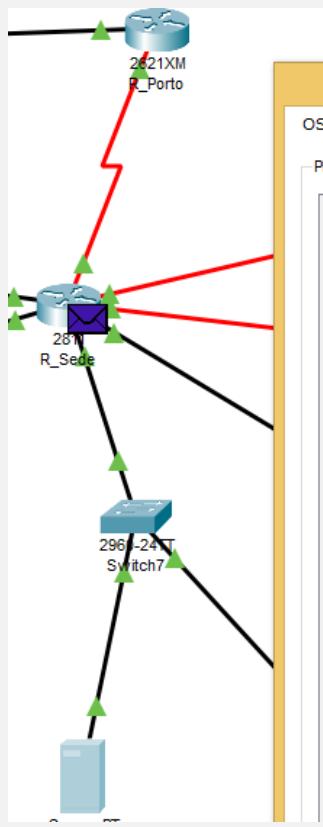
Server
192.168.10.254

```
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

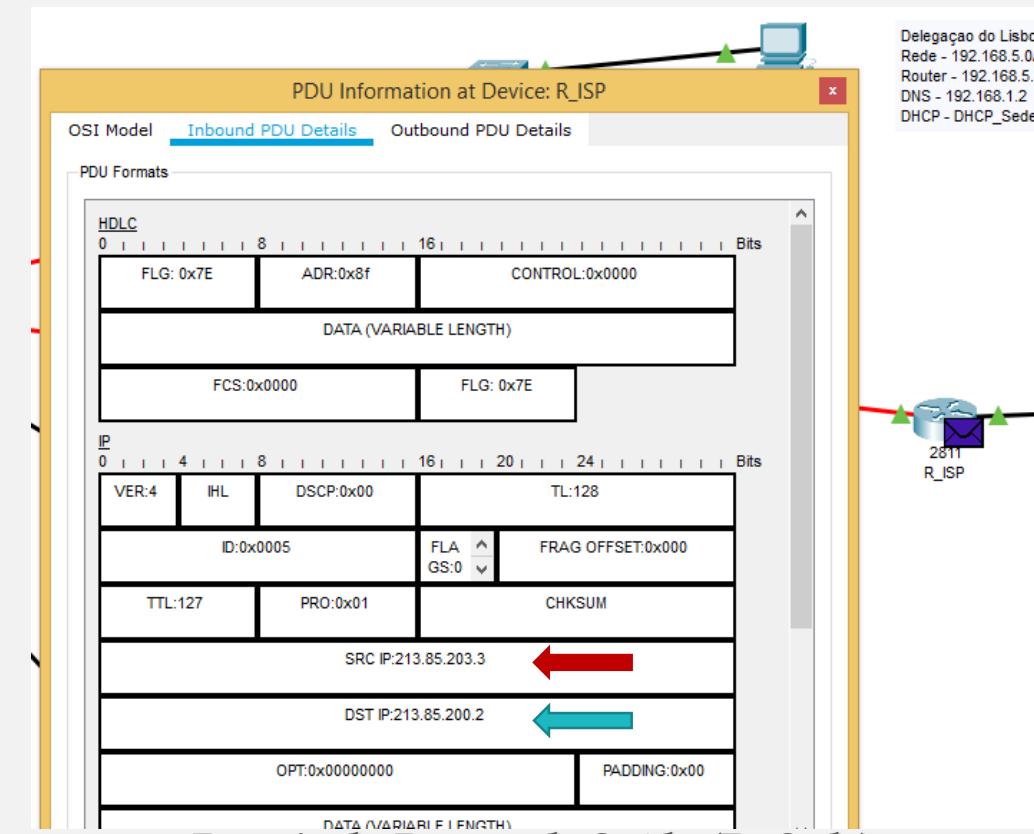
NAT Estático

Sentido Rede Interna -> Rede Externa



Antes do Router de Saída (R_Sede)

213.85.203.3 -> 10.1.1.1

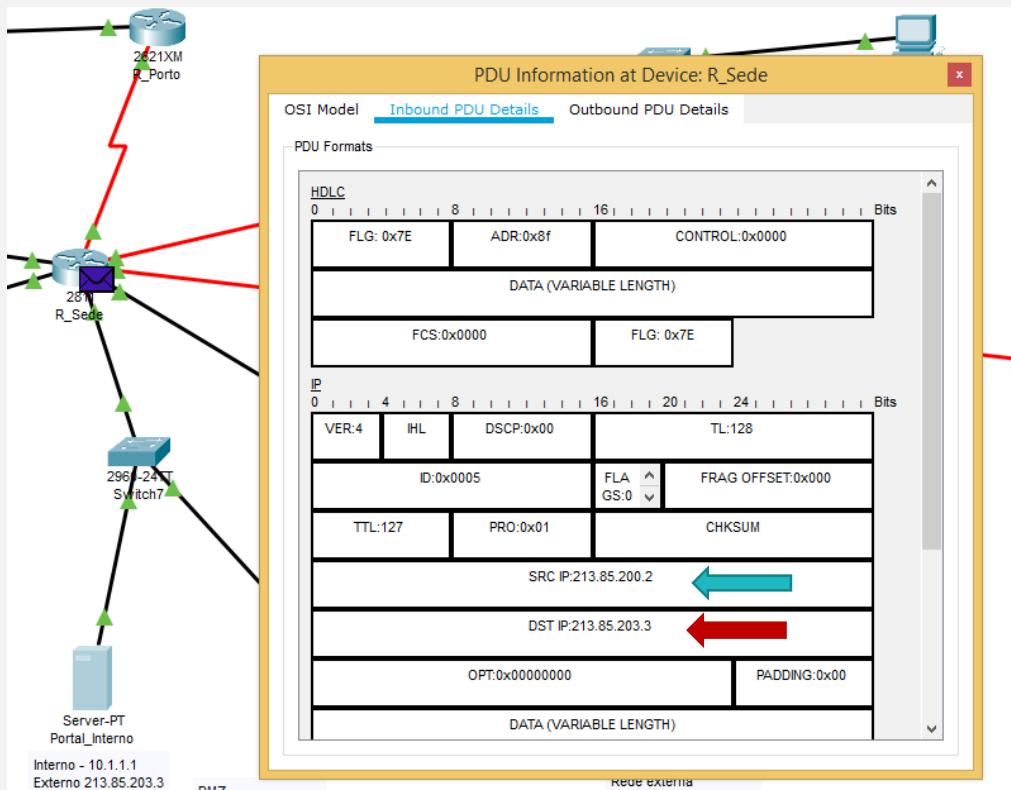


Depois do Router de Saída (R_Sede)

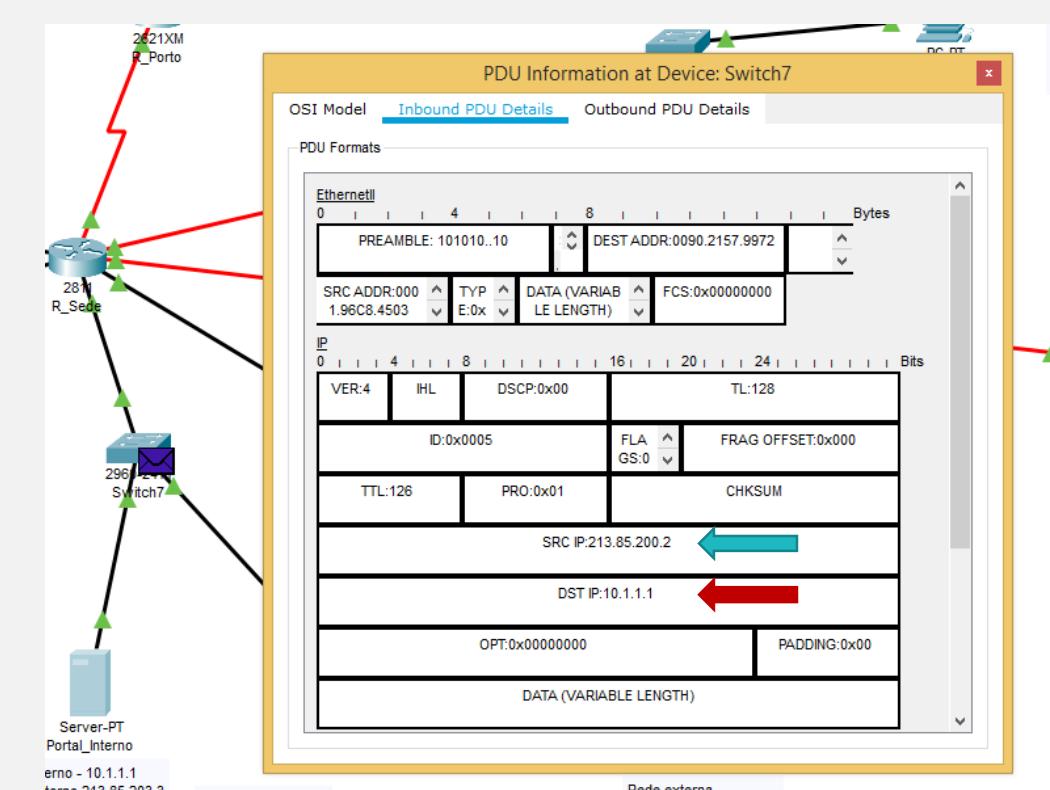
Delegação do Lisbo
Rede - 192.168.5.0/
Router - 192.168.5.1
DNS - 192.168.1.2
DHCP - DHCP_Sede

NAT Estático

Sentido Rede Externa -> Rede Interna



Antes do Router de Saída

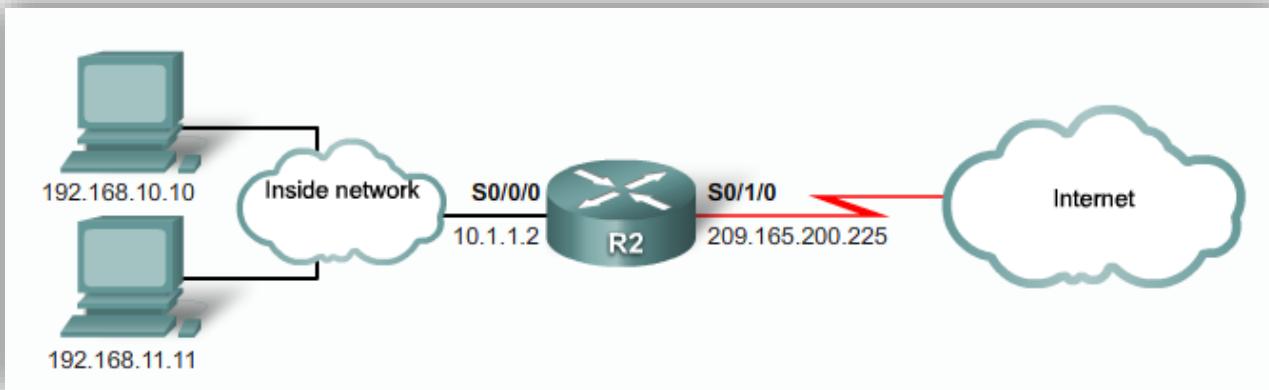


Depois do Router de Saída

NAT dinâmico: configuração

Configuring Dynamic NAT		
Step	Action	Notes
1	Define a pool of global addresses to be allocated as needed. Router(config)#ip nat pool name start-ip end-ip (netmask netmask prefix-length prefix-length)	Enter the global command no ip nat pool name to remove the pool of global addresses.
2	Define a standard access list permitting those addresses that are to be translated. Router(config)#access-list access-list-number permit source [source-wildcard]	Enter the global command no access-list access-list-number to remove the access list.
3	Establish dynamic source translation, specifying the access list defined in the prior step. Router(config)#ip nat inside source list access-list-number pool name	Enter the global command no ip nat inside source to remove the dynamic source translation.
4	Specify the inside interface. Router(config)#interface type number	Enter the interface command. The CLI prompt will change from (config) # to (config-if) #.
5	Mark the interface as connected to the inside. Router(config-if)#ip nat inside	
6	Specify the outside interface. Router(config)#interface type number	
7	Mark the interface as connected to the outside. Router(config-if)#ip nat outside	
8	Exit interface configuration mode. Router(config-if)# exit	

NAT dinâmico: configuração



```
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
```

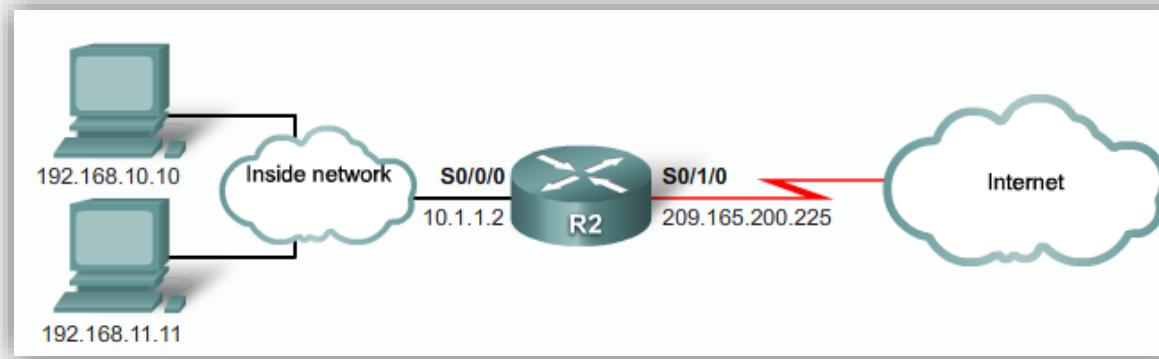
PAT/ NAT overload - configuração

Podemos configurar utilizando uma gama de endereço IP:

Step	Action	Notes
1	Define a standard access list permitting those addresses that are to be translated. <pre>Router(config)#access-list acl-number permit source [source-wildcard]</pre>	Enter the global command <code>no access-list access-list-number</code> to remove the access list.
2	Specify the global address, as a pool, to be used for overloading. <pre>Router(config)#ip nat pool name start-ip end-ip {netmask netmask prefix-length prefix-length}.</pre>	
3	Establish overload translation. <pre>Router {config}#ip nat inside source list acl-number pool name overload.</pre>	
4	Specify the inside interface. <pre>Router(config)#interface type number Router(config-if)#ip nat inside</pre>	Enter the <code>interface</code> command. The CLI prompt will change from <code>(config) #</code> to <code>(config-if) #</code> .
5	Specify the outside interface. <pre>Router(config-if)#interface type number Router(config-if)#ip nat outside</pre>	

PAT/ NAT overload - configuração

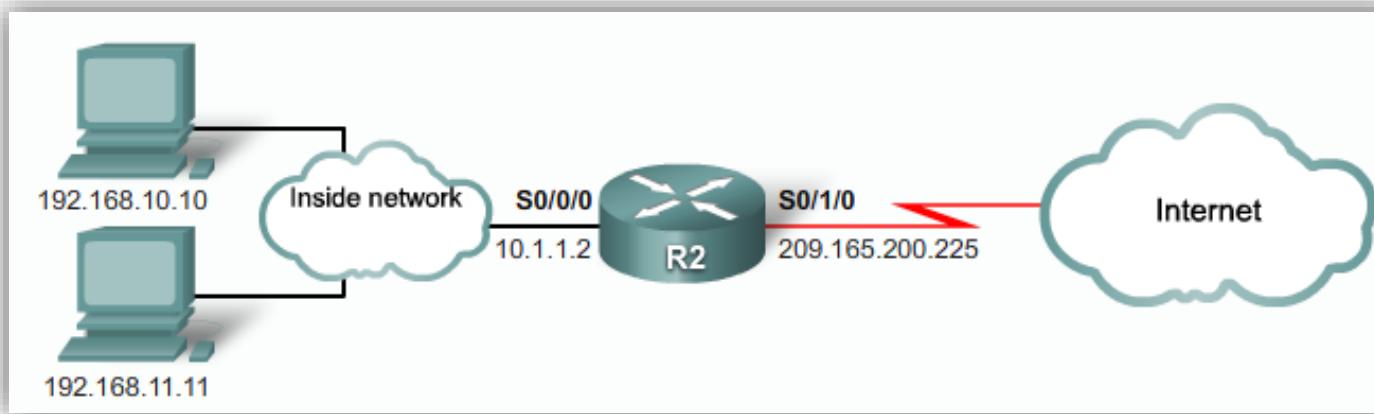
Utilizando uma “pool” de endereços



```
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
```

PAT/ NAT overload - configuração

Utilizando um endereço/interface



```
access-list 1 permit 192.168.0.0 0.0.255.255
```

I—Defines which addresses are eligible to be translated

```
ip nat inside source list 1 interface serial 0/1/0 overload
```

I—Identifies the outside interface Serial 0/1/0 as the inside global address to be overloaded
interface serial 0/0/0

```
    ip nat inside
```

I—Identifies interface Serial 0/0/0 as an inside NAT interface

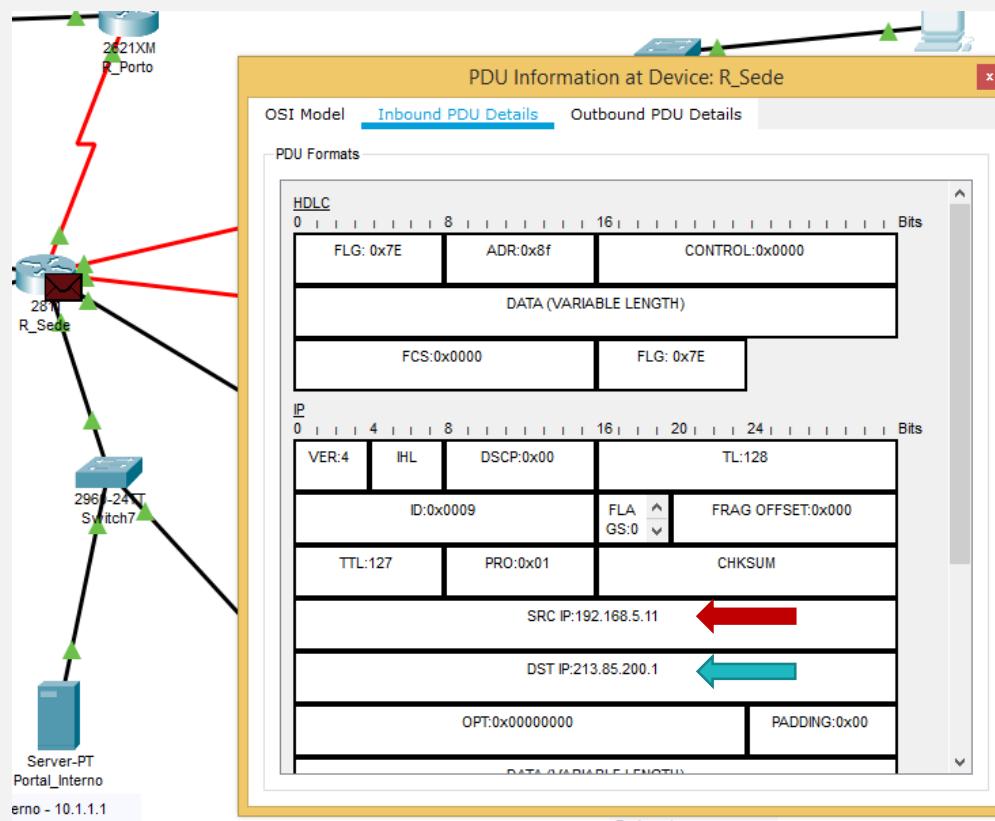
```
interface serial 0/1/0
```

```
    ip nat outside
```

I—Identifies interface Serial 0/1/0 as the outside NAT interface

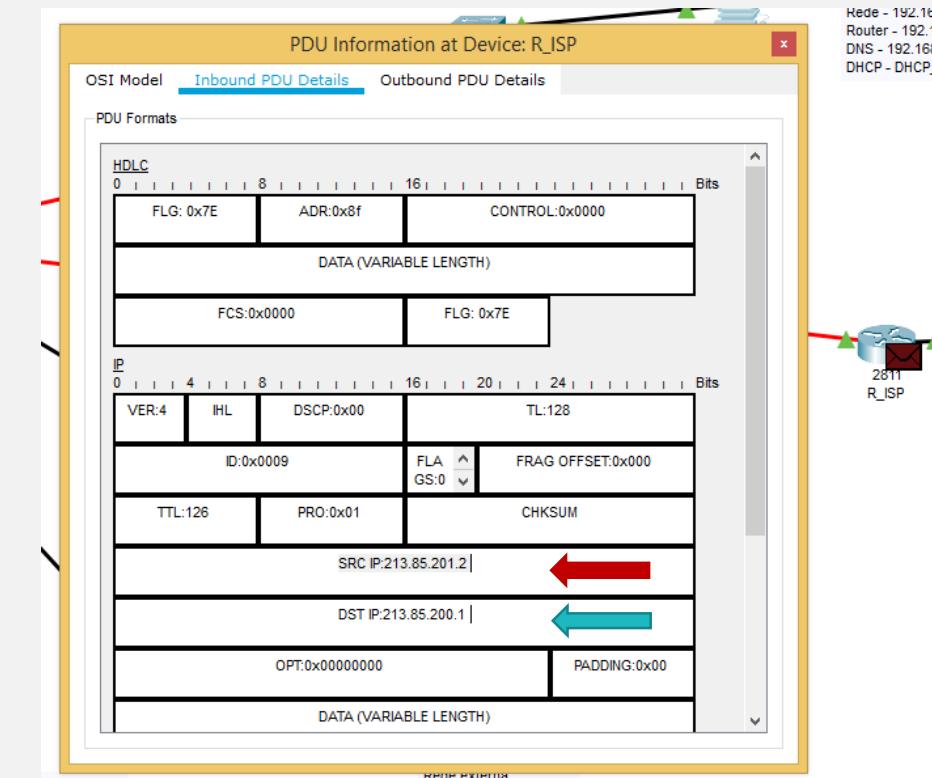
PAT/ NAT overload - configuração

Sentido Rede Interna -> Rede Externa



Antes do Router de Saída (R_sede)

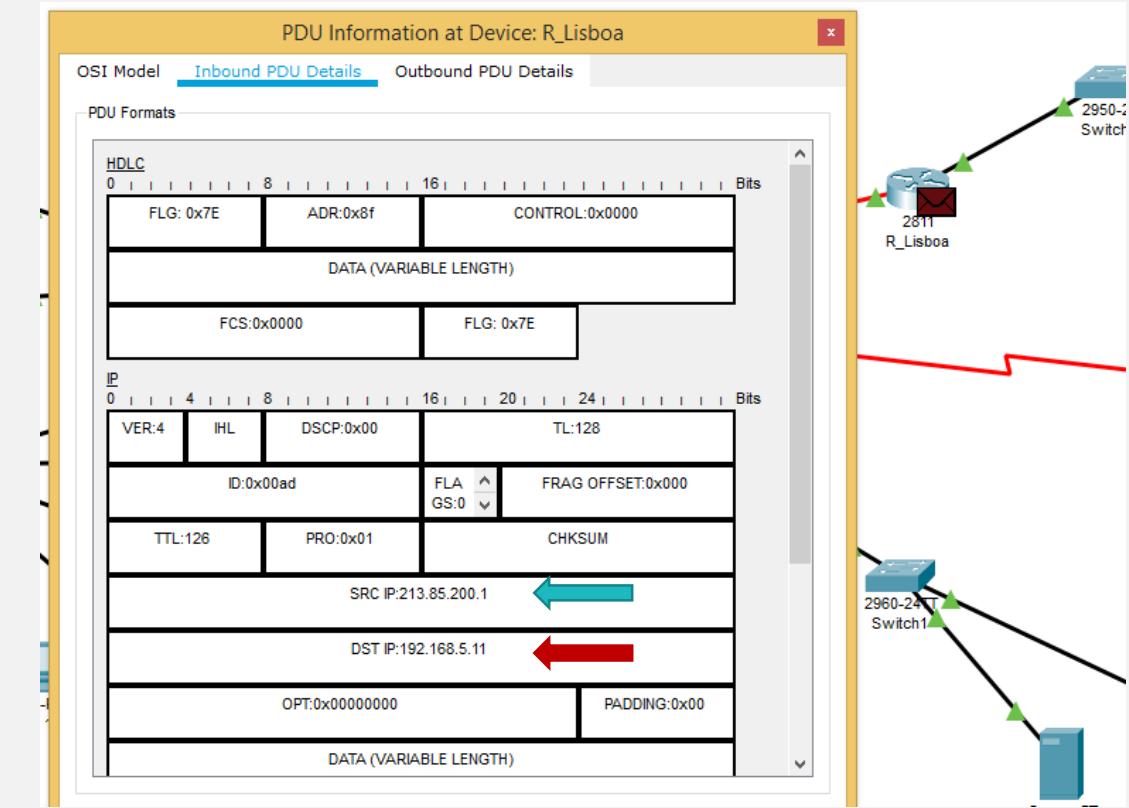
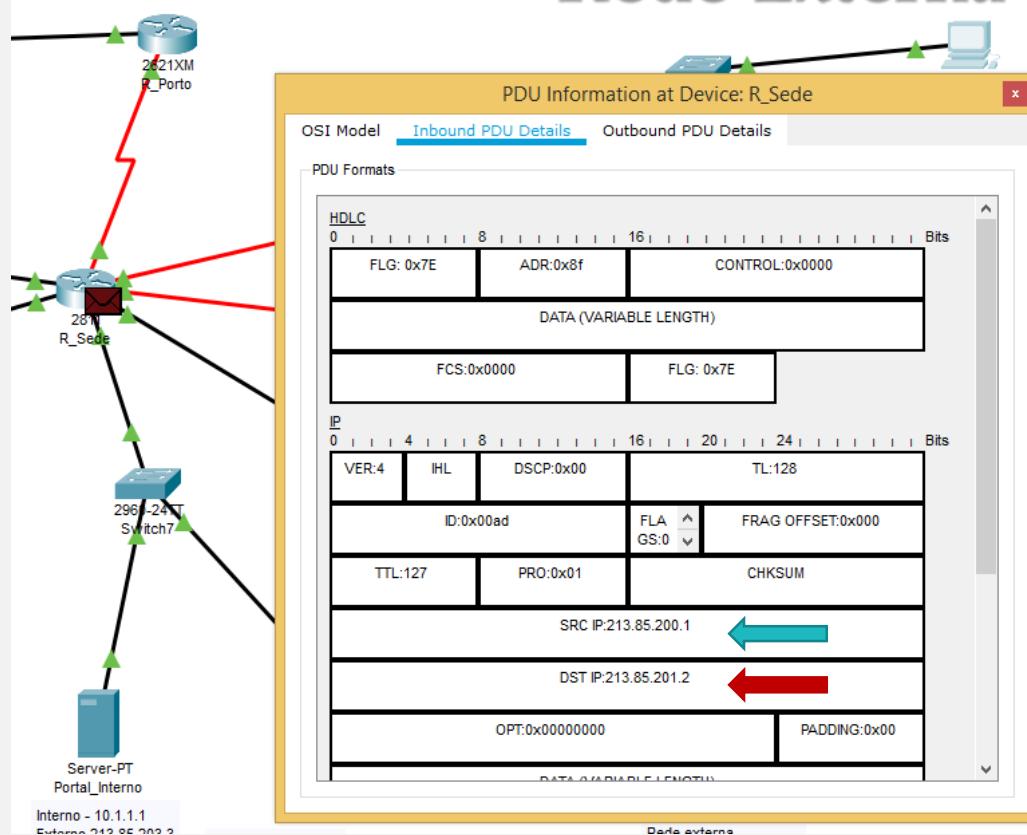
192.168.5.11->213.85.201.2



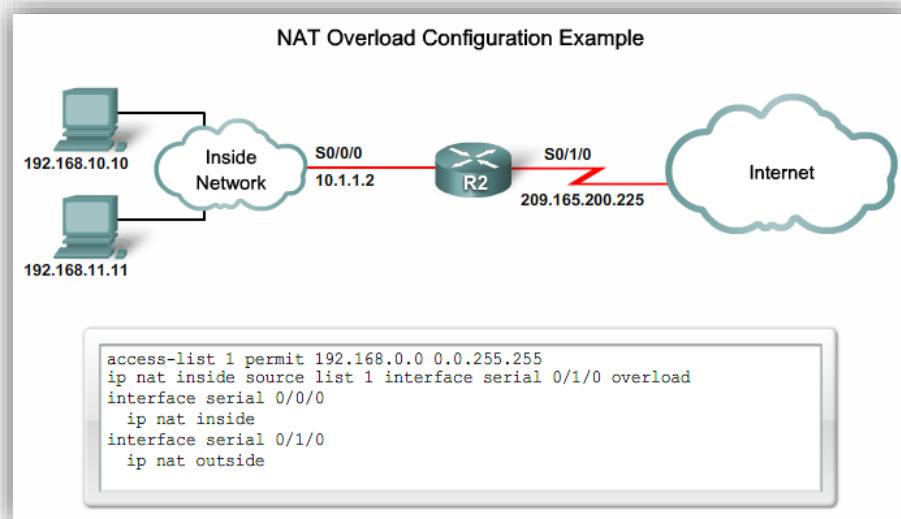
Depois do Router de Saída (R_Sede)

PAT/ NAT overload - configuração

Sentido Rede Externa -> Rede Interna



Verificação da configuração NAT



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

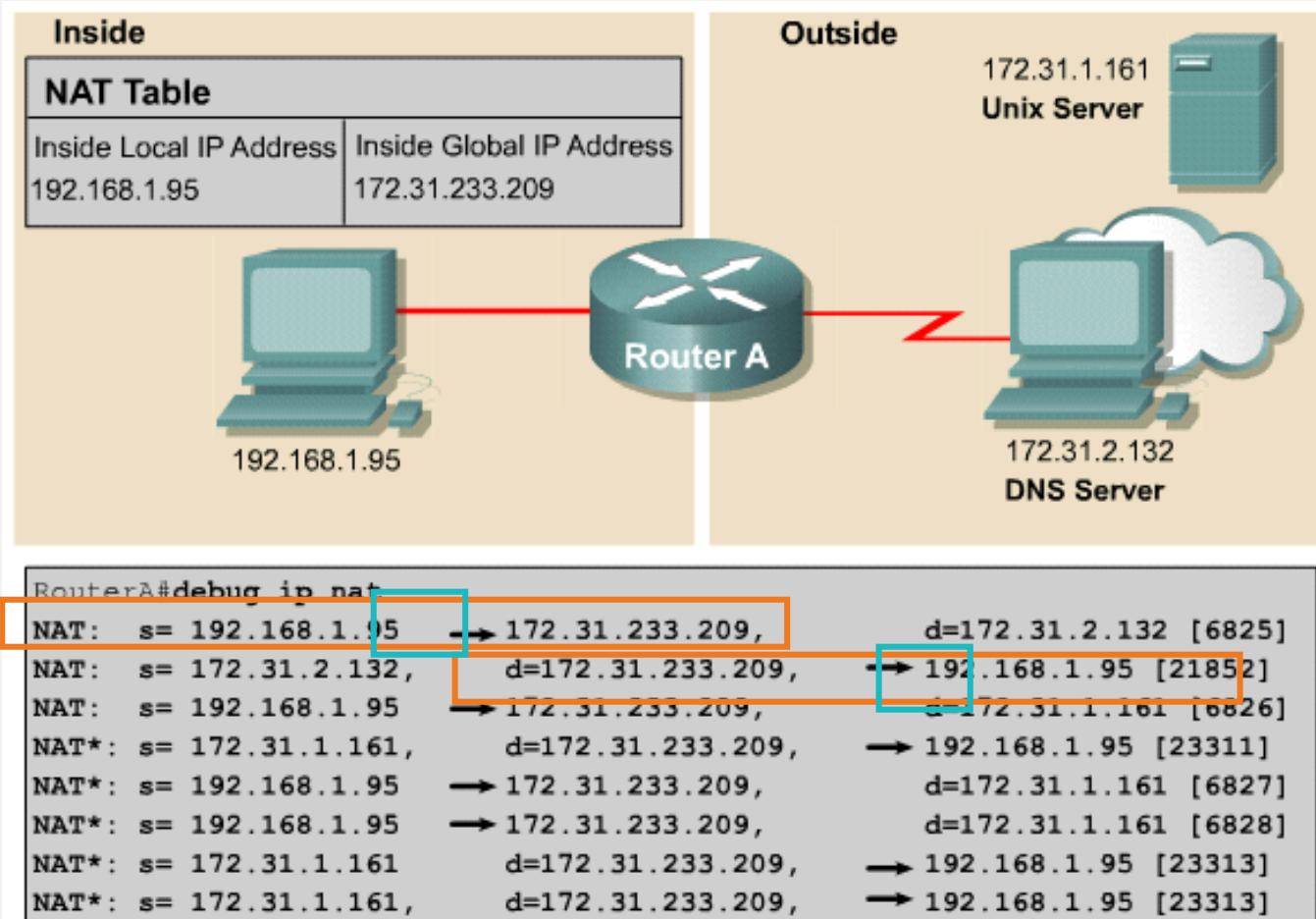
R2#show ip nat statistics
Total active translations: 3 (0 static, 3 dynamic; 3 extended)
Outside interfaces:
  Serial0/1/0
Inside interfaces:
  Serial0/0/0, Serial0/0/1
Hits: 173  Misses: 9
CEF Translated packets: 182, CEF Punted packets: 0
Expired translations: 6
Dynamic mappings:
-- Inside Source
[Id: 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
<code>clear ip nat translation *</code>	Clears all dynamic address translation entries from the NAT translation table
<code>clear ip nat translation inside global-ip local-ip [outside local-ip global-ip]</code>	Clears a simple dynamic translation entry containing an inside translation or both inside and outside translation
<code>clear ip nat translation protocol inside-global-ip global-port local-ip local-port [outside local-ip local-port global-ip global-port]</code>	Clears an extended dynamic translation entry

Verificação da configuração NAT





Network Address Translation
(NAT) - Windows

Serviços de Rede 1

Ano Letivo 2022-2023

Instalação do serviço

The image shows two windows side-by-side. On the left is the 'Server Manager' dashboard. It features a 'QUICK START' section with four steps: 1. Configure this local server (highlighted with a red circle), 2. Add roles and features, 3. Add other servers to manage, and 4. Create a server group. A large blue arrow points from the 'Configure this local server' step down to the 'Add roles and features' link. Below this is a 'ROLES AND SERVER GROUPS' section showing 0 Local Server and 1 All Servers, both with green 'Manageability' status. On the right is the 'Add Roles and Features Wizard' titled 'Select server roles'. The 'Server Roles' tab is selected. Under 'Roles', several checkboxes are available, with 'Remote Access' being checked. A detailed description of the 'Remote Access' role is provided, stating it provides seamless connectivity through DirectAccess, VPN, and Web Application Proxy. It also mentions RAS provides traditional VPN services, including site-to-site (branch-office or cloud-based) connectivity. Web Application Proxy enables the publishing of selected HTTP- and HTTPS-based applications from your corporate network to client devices outside of the corporate network. Routing provides traditional routing capabilities, including NAT and other connectivity options. RAS and Routing can be deployed in single-tenant or multi-tenant mode.

Server Manager

Server Manager > Dashboard

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	0
Manageability	

All Servers	1
Manageability	

Add Roles and Features Wizard

DESTINATION SERVER
smtp.sr2.pt

Select server roles

Before You Begin

Installation Type

Server Selection

Server Roles

Features

Remote Access

Role Services

Confirmation

Results

Active Directory Federation Services

Active Directory Lightweight Directory Services

Active Directory Rights Management Services

Application Server

DHCP Server (Installed)

DNS Server

Fax Server

File and Storage Services (2 of 12 installed)

Hyper-V

Network Policy and Access Services

Print and Document Services (1 of 4 installed)

Remote Access

Remote Desktop Services

Volume Activation Services

Web Server (IIS)

Description

Remote Access provides seamless connectivity through DirectAccess, VPN, and Web Application Proxy. DirectAccess provides an Always On and Always Managed experience. RAS provides traditional VPN services, including site-to-site (branch-office or cloud-based) connectivity. Web Application Proxy enables the publishing of selected HTTP- and HTTPS-based applications from your corporate network to client devices outside of the corporate network. Routing provides traditional routing capabilities, including NAT and other connectivity options. RAS and Routing can be deployed in single-tenant or multi-tenant mode.

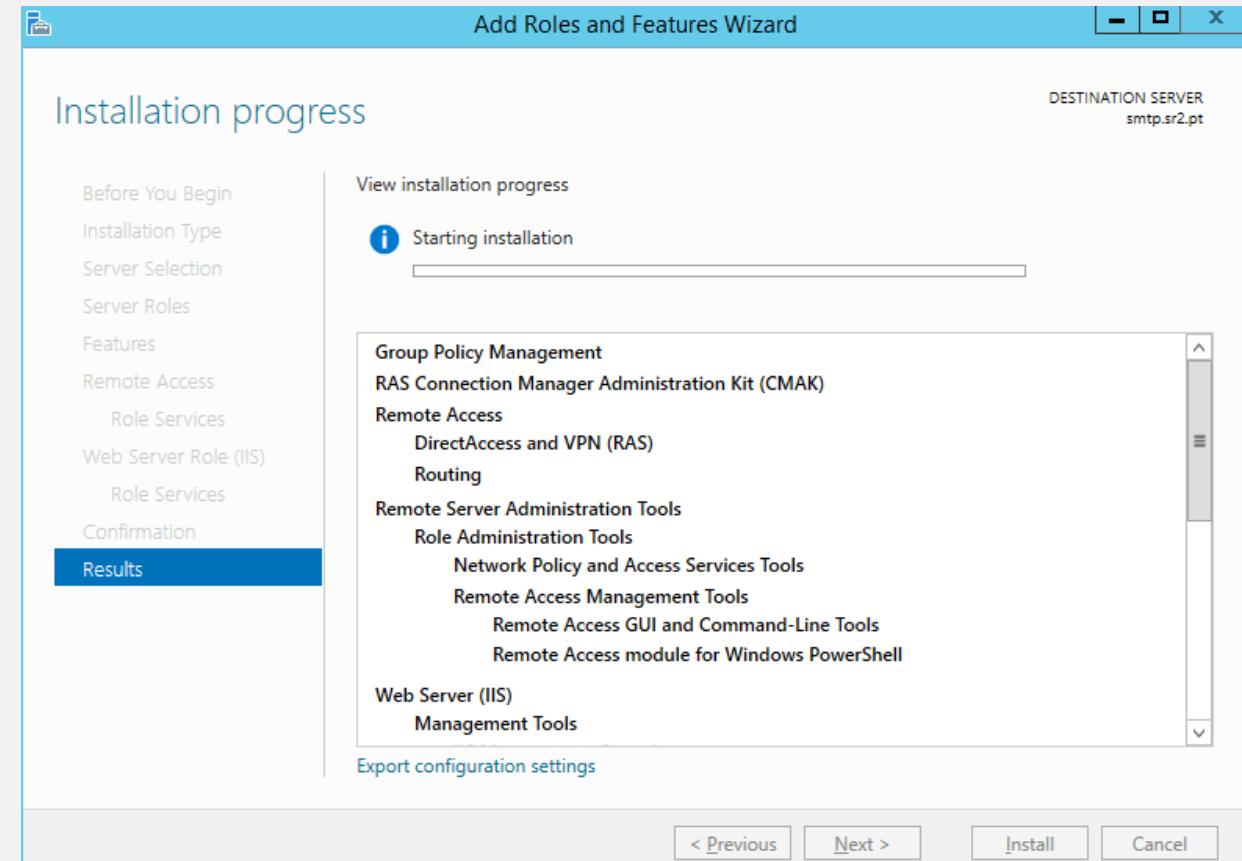
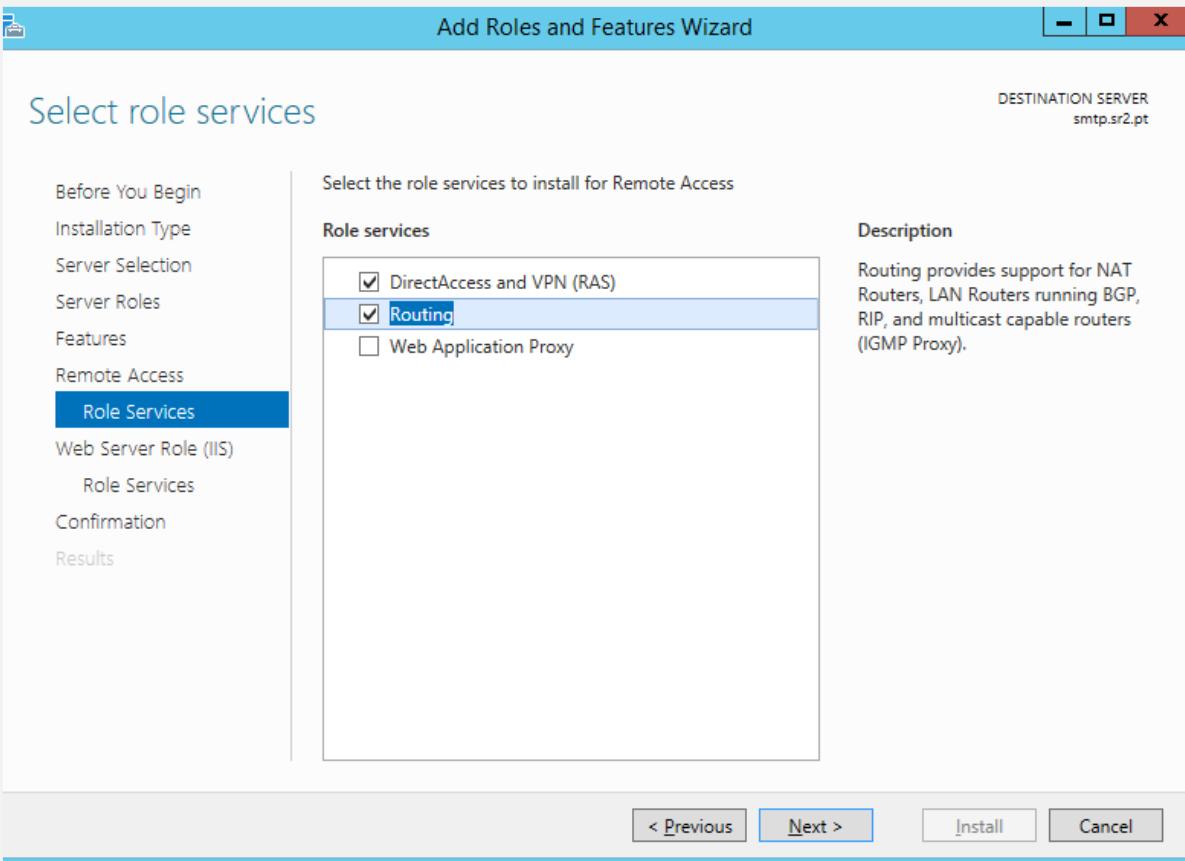
< Previous

Next >

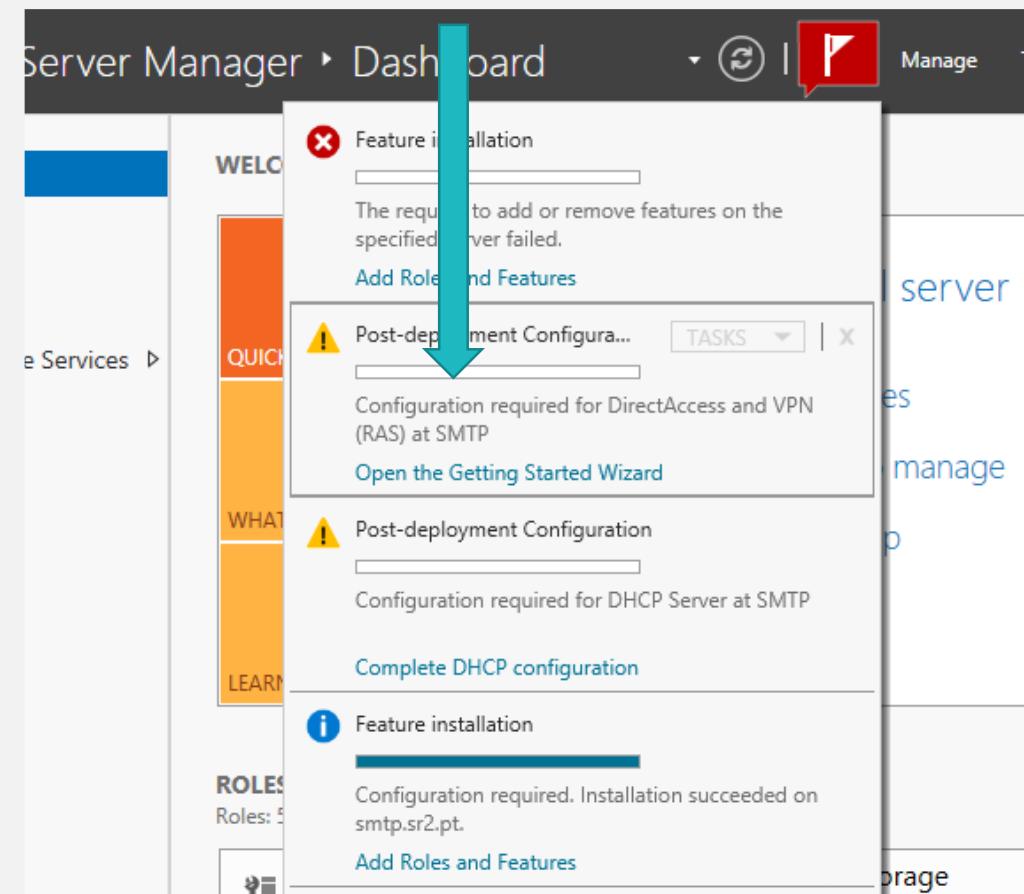
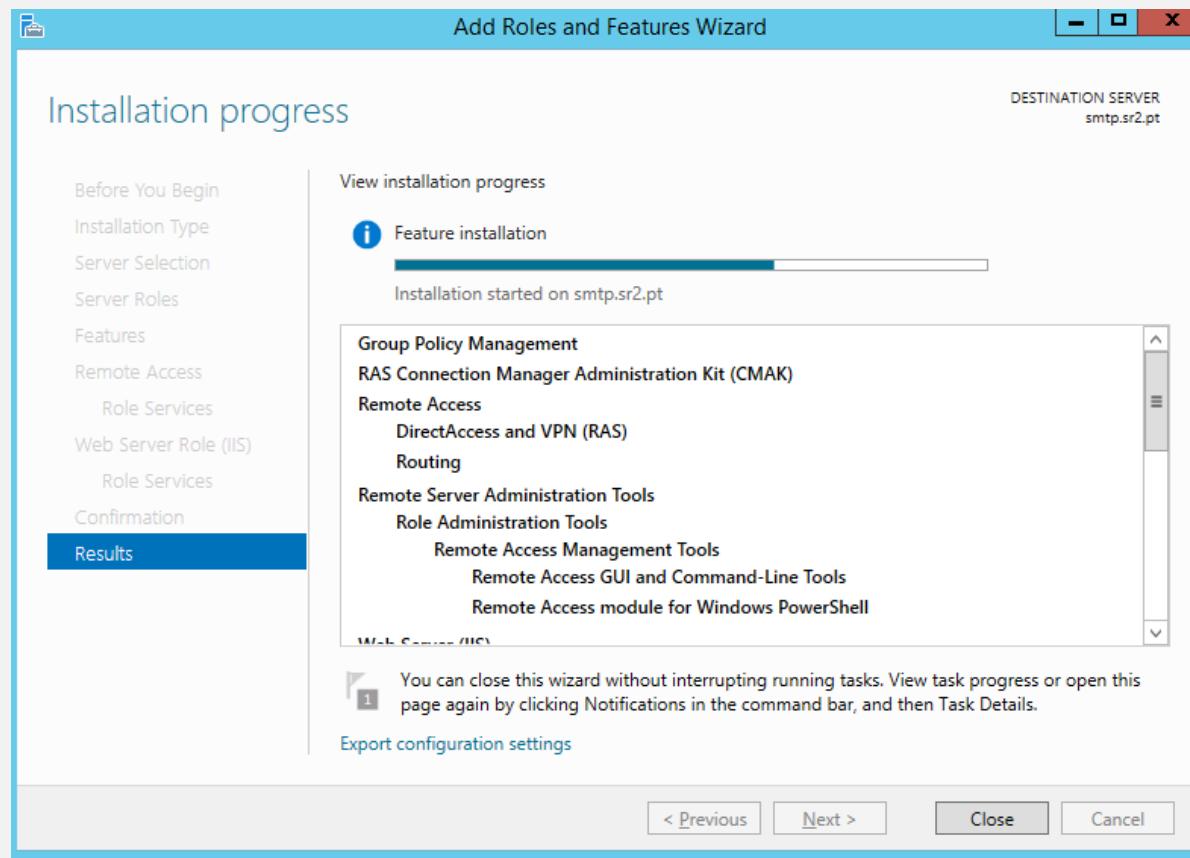
Install

Cancel

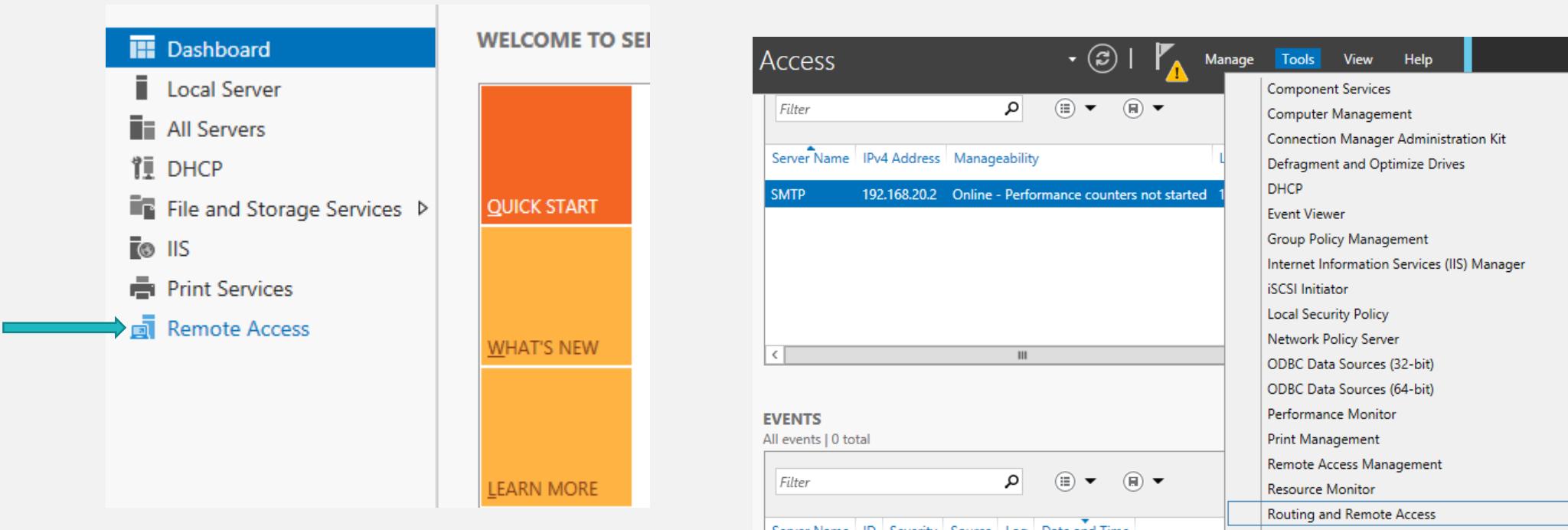
Instalação do serviço



Instalação do serviço



Instalação do serviço



The screenshot shows the Microsoft Server Explorer interface. On the left, a navigation pane lists various services: Dashboard, Local Server, All Servers, DHCP, File and Storage Services, IIS, Print Services, and Remote Access. A teal arrow points to the 'Remote Access' node. The main area displays a 'WELCOME TO SEI' panel with three buttons: 'QUICK START', 'WHAT'S NEW', and 'LEARN MORE'. Below this, two tables are shown: 'Access' and 'Events'. The 'Access' table has columns for Server Name, IPv4 Address, and Manageability, with one row for 'SMTP' (192.168.20.2). The 'Events' table shows 'All events | 0 total'. On the right, a sidebar lists management tools, with 'Routing and Remote Access' highlighted in blue.

Dashboard

Local Server

All Servers

DHCP

File and Storage Services

IIS

Print Services

Remote Access

WELCOME TO SEI

QUICK START

WHAT'S NEW

LEARN MORE

Access

Server Name	IPv4 Address	Manageability
SMTP	192.168.20.2	Online - Performance counters not started

Events

All events | 0 total

Source Name	ID	Severity	Source	Log	Date and Time
-------------	----	----------	--------	-----	---------------

Component Services

Computer Management

Connection Manager Administration Kit

Defragment and Optimize Drives

DHCP

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)

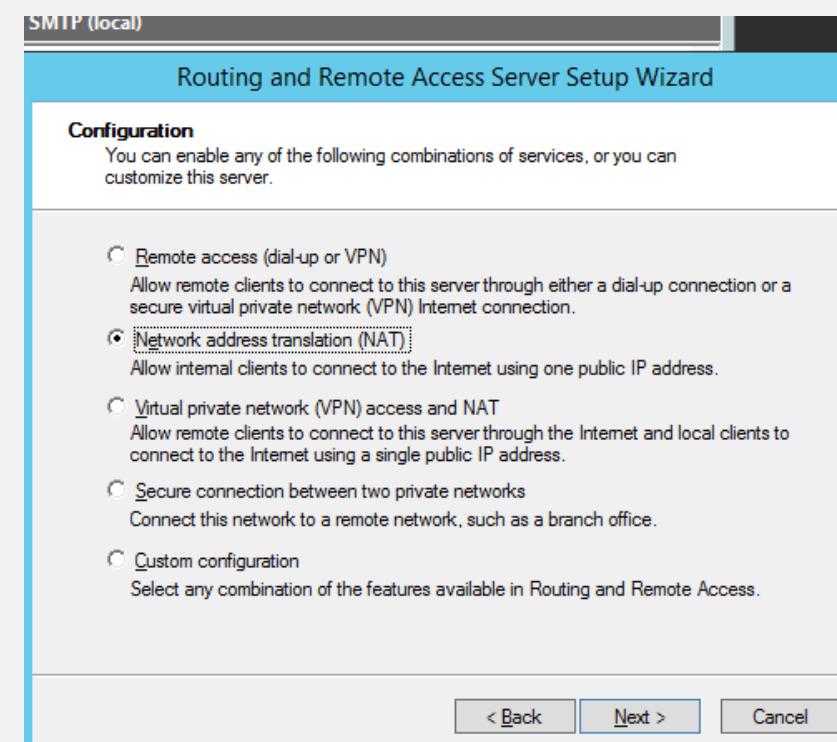
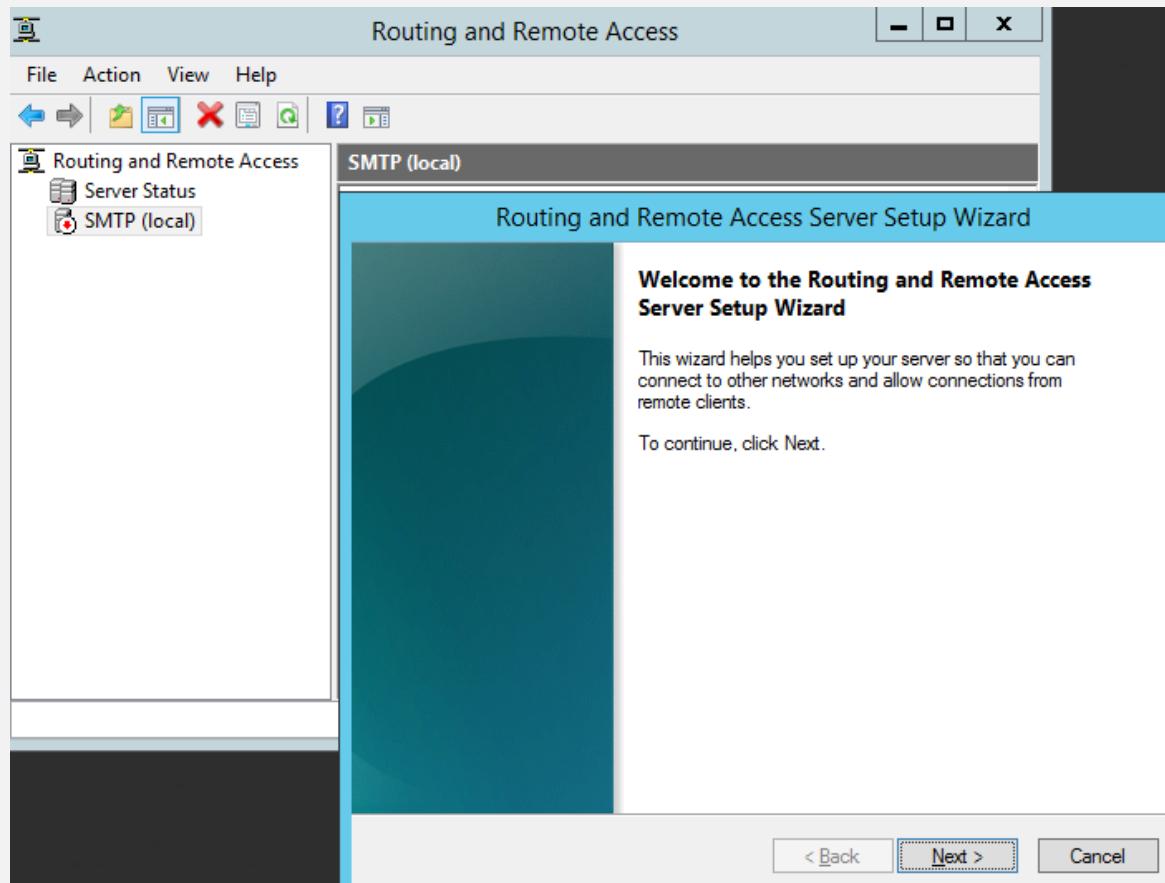
Performance Monitor

Print Management

Remote Access Management

Resource Monitor

Routing and Remote Access



Dúvidas



Referencias

- <https://tools.ietf.org/pdf/rfc1631.pdf> - acedido em março de 2023
- <https://tools.ietf.org/pdf/rfc3022.pdf> - acedido em março de 2023
- <https://www.youtube.com/watch?v=QBqPzHEDzvo> - acedido em março de 2023
- <https://www.youtube.com/watch?v=qij5qpHcbBk> - acedido em março de 2023
- <https://www.youtube.com/watch?v=l5wuJFoeVDQ> - acedido em março de 2023

Serviços de Rede 1

2022-2023

Pedro Miguel Geirinhas

Aula 6

DNS- Domain Name System

Agenda

- 1.** Introdução
- 2.** História
- 3.** Organizações
- 4.** Domínios
- 6.** Servidores
- 7.** Registros

Introdução

Já estudamos que o endereçamento/identificação dos computadores numa rede é feito com endereços IP e físicos MAC que eles têm de ser únicos. Então, porque quando navegamos na Internet utilizamos nomes e não estes identificadores?

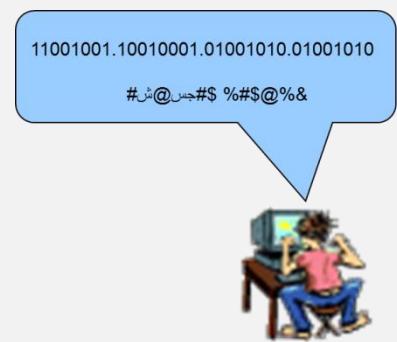
Introdução

- O ser humano memoriza mais facilmente nomes do que números. Habitualmente, mais facilmente decoramos o nome de um conhecido que o seu número do cartão do cidadão.
- Uma solução passa assim, por associar aos IPs nomes facilmente memorizáveis:
 - 193.137.78.20 => webmail.isec.pt
 - 213.13.146.140 => www.sapo.pt
- Esta solução implica a existência de um sistema que efetue a tradução/mapeamento entre os nomes e os respetivos endereços IP:
 - Sistema para a resolução de nomes em IPs (Domain Name System – DNS)
 - Sistemas para traduzir IPs em nomes (reverse DNS)



Introdução

- O DNS permite:
 - A possibilidade ao ser humano de se abstrair de endereços de rede (endereços IP) cuja memorização é complexa.
 - Permite que as alterações aos endereços se possam fazer sem que o utilizador tenha que conhecer essa alteração para continuar a usar um serviço. Ou seja pode mudar o IP de um determinado serviço e isso ser completamente transparente para o utilizador.
 - A garantia que as máquinas e os seus nomes são geridos de forma hierárquica e distribuída permitindo assim uma maior disponibilidade da informação.



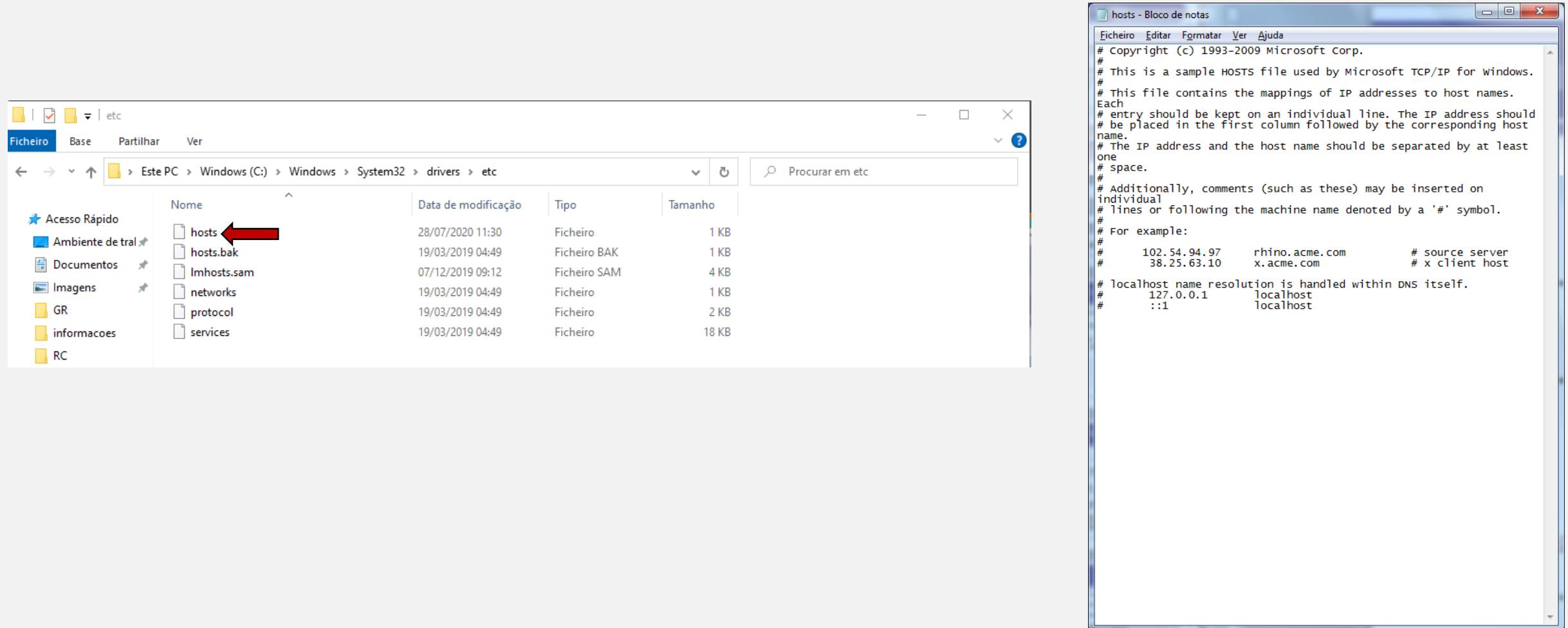
História

- Início dos anos 70
 - Usavam-se apenas IPs para identificar os sistemas da rede ARPANET (a rede “mãe” da Internet).
 - À medida que o número de sistemas ligado à rede crescia tornava-se impraticável aceder às máquinas pelos seus endereços IP já que estes começavam a ser em grande número.
 - Em busca de um processo de memorização simplificada surgiu a ideia de “batizar” as máquinas com nomes.
 - Assim, em cada sistema estava presente um ficheiro (hosts.txt) global com os mapeamentos usados.

História

- Esta foi a primeira solução e encontra-se ainda ativa nos sistemas atuais.
 - Ainda existe atualmente nas maquinas em **Windows\System32\drivers\etc**.
 - Assim, se desejar fazer um mapeamento IP-Nome não dependente do servidor DNS que utiliza, pode fazer essa alteração neste ficheiro já que este é o local onde primeiro a sua máquina vai procurar.
- A solução passava por ter um ficheiro (hosts.txt) por máquina:
 - Implicava uma gestão individual do ficheiro em cada sistema.
 - Os nomes guardados eram nomes simples (só o nome da máquina).
- A “evolução” foi ter um ficheiro que era atualizado centralmente e distribuído depois por todas as máquinas ligadas na rede.

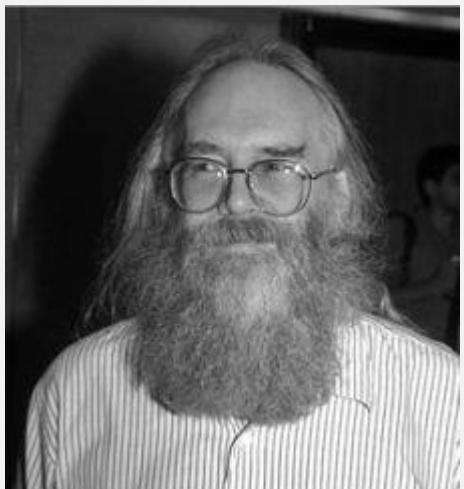
História



Nota: Existe sempre o endereço 127.0.0.1 que identifica o localhost...

História

- O ficheiro hosts.txt era mantido centralmente (inicialmente na University of California, Los Angeles, UCLA) e distribuído por FTP para todos os sistemas que pretendiam ter presente a resolução de nomes.
- A gestão central desse ficheiro ficou inicialmente a cargo de Jon(athan) B. Postel, na altura um estudante graduado da UCLA ao abrigo de um acordo mantido com Department of Defense (DoD). Postel é considerado um dos pioneiros da Internet e um dos seus maiores pensadores.



https://www.internethalloffame.org//inductees/jon-postel?gclid=Cj0KCQjwm9D0BRCMARIsAlfvfIaVlkisWaj7DBVVbGfvWHjOgoUFqe18bm_L7YBGNF3YUN8RXqR05b4aAp5WEALw_wcB

História

- Então porque não colocar no ficheiro todos os IPs existentes na Internet?
 - Passaríamos uma boa parte da nossa vida a escrever IPs e nunca teríamos a tabela atualizada!
 - Qualquer alteração num nome ou IP, ou qualquer adição ou remoção da tabela, exigiria que todos os utilizadores fizessem um novo download do ficheiro;
 - E quem se responsabilizava por esta atualização e gestão dos nomes e IPs?

História

- Em paralelo, Jon Postel iniciou a organização do arquivo de documentos técnicos escritos pelos investigadores da ARPANET, denominados **Request For Comments (RFC)** mantendo-se até falecer como seu editor.
- Em 1971 (27 de Setembro) J. Postel publica o RFC 229 propondo uma lista de nomes (host mnemonics) e alcunhas normalizadas de 8 caracteres identificando assim todos sistemas da ARPANet de forma diferenciada.
- Durante 1972, J. Postel publica dois RFC (em maio o RFC 229 e em Dezembro o RFC 433) onde é proposta uma lista dos números normalizados das portas a serem utilizados por cada um dos serviços de rede.

História

- Devido à expansão na interligação de sistemas através de redes de dados, surgiu a necessidade de organizar os nomes atribuídos às máquinas.
- Um nome simples (“alpha”, “omega”, ...) não respondia às necessidades e originava, por vezes, conflitos entre sistemas porque existiam máquinas diferentes com o mesmo nome.
- Em agosto de 1982 é publicado o RFC 819 Z. Su, J. Postel, "*Domain naming convention for Internet user applications*" onde é definido a estrutura “**“nome da maquina. domínio”**”:

Antes	Depois
alpha	apha.xxx.yyy
omega	omega.aaa.bbb

História

- Contudo, existia ainda a dificuldade introduzida pela variedade/multiplicidade de ficheiros de resolução de nomes.
- Cada sistema tinha de ter o seu ficheiro e isso era um problema já que:
 - As tarefas de atualização/gestão do ficheiro não eram efetuadas de igual forma em todos os sistemas.
 - Existia a necessidade de liberalizar a atribuição de nomes aos sistemas de uma organização sem que isso implicasse aumento da complexidade da manutenção nos sistemas de outra organização.
 - Existia uma maior probabilidade de erros.

História

- Em 1983 surgiram as primeiras experiências e implementações de um sistema distribuído para efetuar a resolução de nomes o **Domain Name System** (DNS).
- Arquitetura foi desenvolvida por Paul Mockapetris.
- Em Novembro são publicados vários RFC fundamentais para o DNS:
 - RFC 881 J. Postel, "*Domain names plan and schedule*" onde apresentado o calendário de introdução do DNS.
 - RFC 882 P. Mockapetris, "*Domain names – concepts and facilities*" onde são especificados os conceitos chave do DNS.
 - RFC 883 P. Mockapetris, "*Domain names – implementation and specification*" onde é detalhada a implementação do DNS.



História

- Em 1984 é colocado em funcionamento o DNS, substituindo o ficheiro hosts.txt por servidores a correr este serviço.
- Em março de 1985 é registado o primeiro domínio DNS (symbolics.com)
- Em 1986 é atribuída à *National Science Foundation* (NSF) o desenvolvimento da NSFNET que constitui hoje o principal *backbone* da Internet.
- O crescimento exponencial da Internet iniciou-se...
- Em novembro 1987 Paul Mockapetris publica dois RFC que se tratam de uma revisão da especificação inicial e na qual assenta ainda hoje o DNS:
 - RFC 1034 P.V. Mockapetris, "*Domain names - concepts and facilities*"
 - RFC 1035 P.V. Mockapetris, "*Domain names - implementation and specification*"

História

- Os RFCs mais importantes para o DNS são:
 - RFCs 882 e 883 – Funcionamento básico
 - RFCs 1034, 1035 – Modelo Vigente
 - RFCs 1535, 1536, 1537 – Segurança, Implementação, Administração.

1034	Domain Names -- Concepts and Facilities
1035	Domain Names -- Implementation and Specification
1123	Requirements for Internet Hosts -- Application and Support
1886	DNS Extensions to Support IP Version 6
1995	Incremental Zone Transfer in DNS
1996	A Mechanism for Prompt Notification of Zone Changes (DNS NOTIFY)
2136	Dynamic Updates in the Domain Name System (DNS UPDATE)
2181	Clarifications to the DNS Specification
2308	Negative Caching of DNS Queries (DNS NCACHE)
2535	Domain Name System Security Extensions (DNSSEC)
2671	Extension Mechanisms for DNS (EDNSo)
2782	A DNS RR for specifying the location of services (DNS SRV)
2930	Secret Key Establishment for DNS (TKEY RR)
3645	Generic Security Service Algorithm for Secret Key Transaction Authentication for DNS (GSS-TSIG)
3646	DNS Configuration options for Dynamic Host Configuration Protocol for IPv6 (DHCPv6)

História

- Uma das grandes vantagens deste novo sistema é que nenhuma entidade é a única responsável por toda a atualização do sistema.
- Baseia-se no conceito de base de dados distribuída, existindo em muitos servidores de nomes diferentes em todo o mundo, mas nenhum desses servidores possui toda a informação. Isto permite assim um crescimento praticamente ilimitado do DNS.
- Nos sistemas da Microsoft o DNS passou a ser o serviço de resolução de nomes padrão a partir do Windows 2000 Server substituindo o *Windows Internet Name Service (WINS)*.

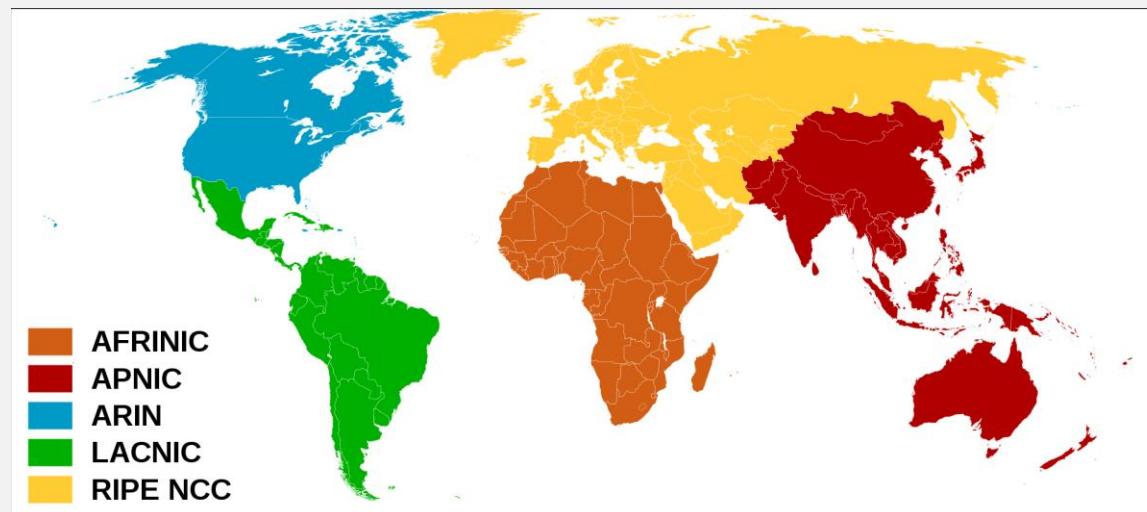
Organizações

- O serviço de DNS está diretamente dependente da atribuição de IPs e nomes de domínios às organizações.
- Esta função é da competência da IANA (Internet Assigned Numbers Authority) ou a quem ela delegar essa função.
- Em Portugal a competência foi delegada em 30 de Junho de 1988 à Fundação para a Computação Científica Nacional (FCCN), cabendo a esta a responsabilidade de gerir o domínio '.pt'.
- A Associação DNS.PT, foi formalmente criada no dia 9 de maio de 2013 e sucedeu à, FCCN nos direitos e obrigações na responsabilidade pela gestão, registo e manutenção de domínios sob o TLD (Top Level Domain) '.pt'.
- Tem como associados a Fundação para a Ciência e a Tecnologia, FCT - IP, Associação da Economia Digital (ACEPI) e a Associação Portuguesa para a Defesa do Consumidor (DECO).



Organizações

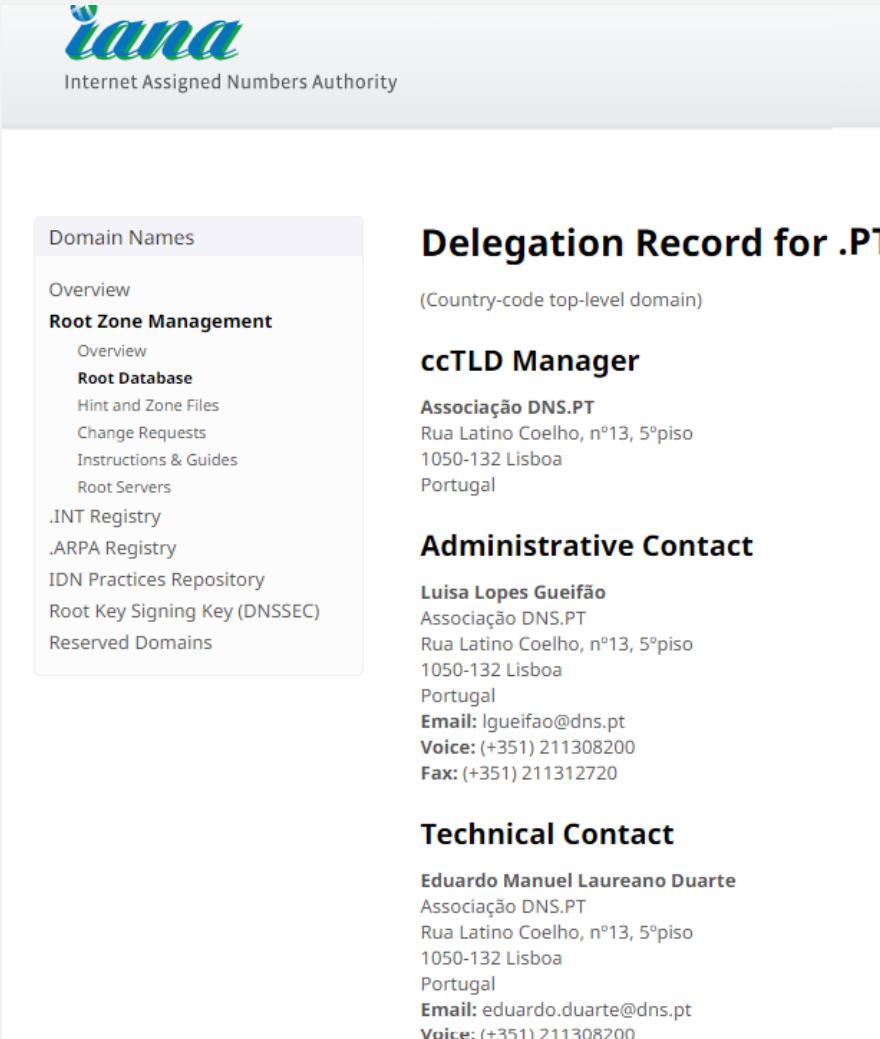
- No topo da hierarquia está a IANA (Internet Assigned Numbers Authority), vinculada à ICANN (Internet Corporation for Assigned Names and Numbers), que coordena as atividades globalmente.
- A IANA delega parte dessas atividades para autoridades com abrangência menor, normalmente da área de continentes que são denominadas RIR (Regional Internet Registry).
- Atualmente existem 5 entidades regionais (RIR) que são: ARIN, RIPE NCC, APNIC, LACNIC e AfriNIC



Fonte:

https://pt.wikipedia.org/wiki/Registro_Regional_da_Internet#/media/Ficheiro:Regional_Internet_Registries_world_map.svg

Organizações



The screenshot shows a web page from IANA (Internet Assigned Numbers Authority) regarding the delegation record for the .PT domain. The page has a sidebar on the left with links for Domain Names, Overview, Root Zone Management, Root Database, Hint and Zone Files, Change Requests, Instructions & Guides, Root Servers, .INT Registry, .ARPA Registry, IDN Practices Repository, Root Key Signing Key (DNSSEC), and Reserved Domains. The main content area displays the delegation record for .PT, which is a country-code top-level domain managed by the ccTLD Manager, Associação DNS.PT, located at Rua Latino Coelho, n°13, 5ºpiso, 1050-132 Lisboa, Portugal. It also lists the Administrative Contact (Luisa Lopes Gueifão) and Technical Contact (Eduardo Manuel Laureano Duarte) with their respective addresses, email, voice, and fax numbers.

Delegation Record for .PT
(Country-code top-level domain)

ccTLD Manager

Associação DNS.PT
Rua Latino Coelho, n°13, 5ºpiso
1050-132 Lisboa
Portugal

Administrative Contact

Luisa Lopes Gueifão
Associação DNS.PT
Rua Latino Coelho, n°13, 5ºpiso
1050-132 Lisboa
Portugal
Email: lgueifao@dns.pt
Voice: (+351) 211308200
Fax: (+351) 211312720

Technical Contact

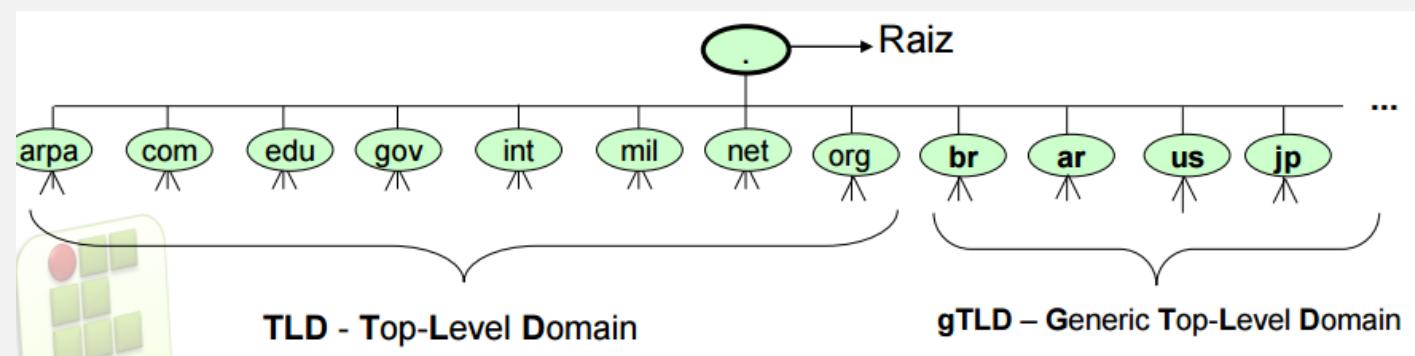
Eduardo Manuel Laureano Duarte
Associação DNS.PT
Rua Latino Coelho, n°13, 5ºpiso
1050-132 Lisboa
Portugal
Email: eduardo.duarte@dns.pt
Voice: (+351) 211308200

Domínios

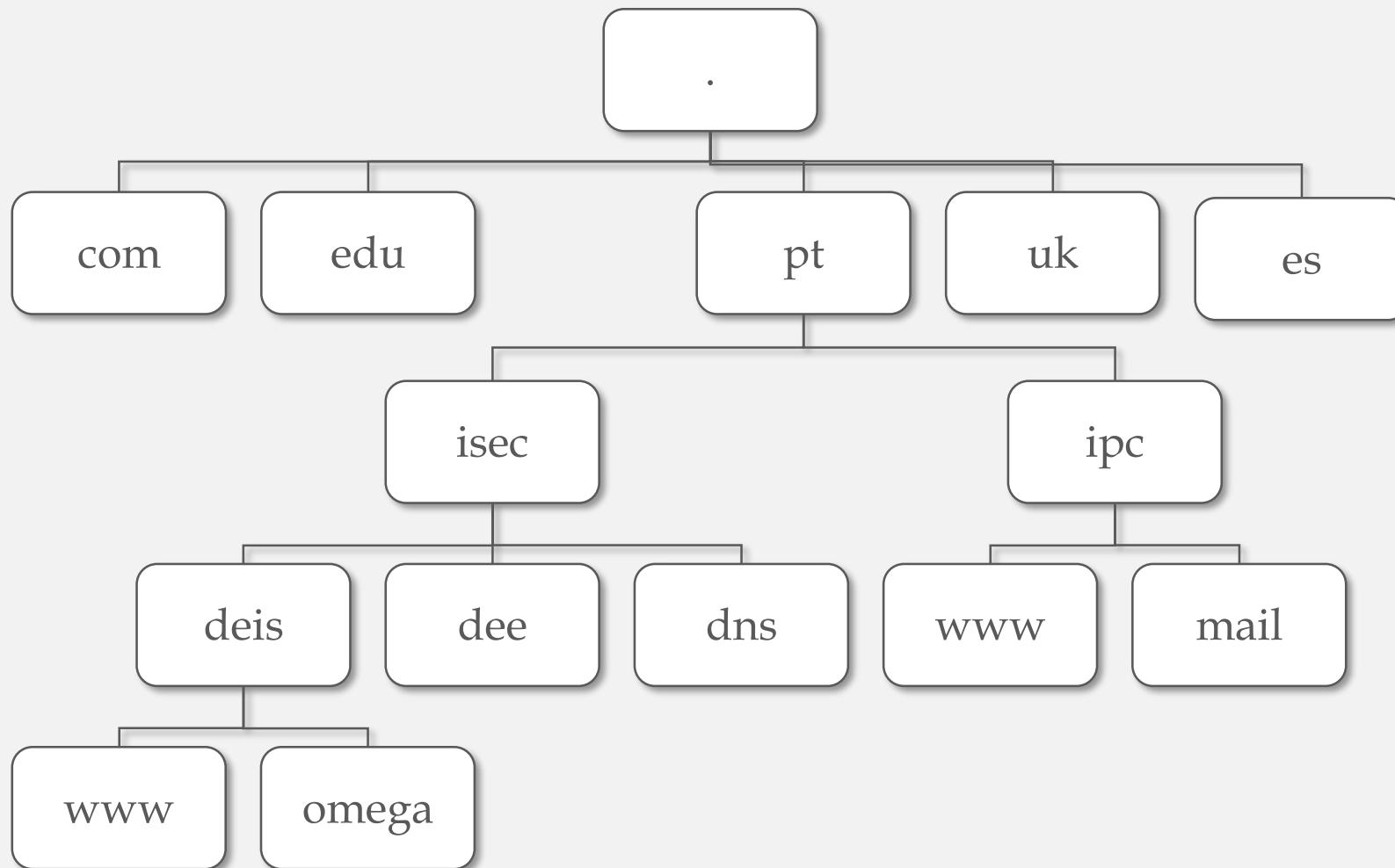
- Os nomes de domínios são construídos hierarquicamente, sendo o nível mais alto da hierarquia o último identificador.
- Como o DNS foi introduzido originalmente nos Estados Unidos, a parte final de um endereço destinava-se a indicar o tipo de organização onde estava localizado o computador. Dessa forma, alguns dos domínios de topo (.edu, .gov e .mil) ainda só são utilizados por organizações localizadas nos Estados Unidos.
- Os códigos de duas letras que indicam o país de origem estão definidos no **ISO 3166** com a exceção do uk utilizado pelo Reino Unido (United Kingdom) em vez de gb (Great Britain).
- Pode ver a lista em <https://www.iso.org/obp/ui/#iso:pub:PUB500001:en>.

Domínios

- Atualmente podem registar-se nomes sob vários domínios de topo:
 - com, aero, biz, cat, coop, edu, gov, info, int, jobs, mil, mobi, museum, name, net, org, pro, travel, tv ...
 - Domínios para os países ou regiões: pt, eu, es, fr, uk, ...
 - Veja a lista em <https://www.iana.org/domains/root/db>
- O nome de cada nó/identificador (exceto o do nó *root*) tem de ter, no máximo, **63 caracteres**, e é indiferente a utilização de maiúsculas ou minúsculas. Os identificadores têm de começar por uma letra e podem consistir apenas de letras, algarismos e traços (-).
- No conjunto, um nome de domínio completo **não pode exceder os 255 caracteres**.

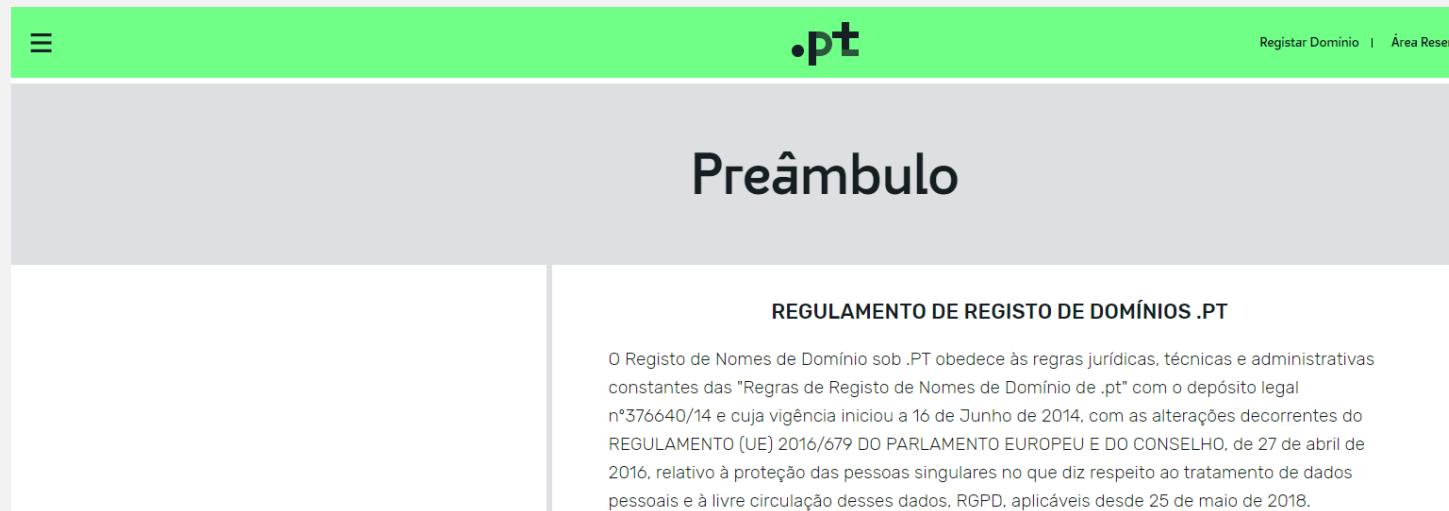


Domínios



Domínios

- Em Portugal, a FCCN disponibiliza também domínios de segundo nível para o domínios 'pt': com, edu, gov, int, net, nome, org, publ.
- As regras para o registo de um domínio em Portugal está definida em:
 - <https://www.pt.pt/pt/dominio/regras-de-registo-de-pt-2/>



Domínios

- As entidades que aceitam registo de nomes designam-se por Registrars.
- São entidades especializadas no registo e gestão de nomes de domínios.
- Em Portugal são credenciados pela FCCN através de protocolo que reconhece direitos e obrigações recíprocos, permitindo uma maior flexibilidade e agilidade na gestão de nomes de domínio por estas entidades.
- Para se candidatar a Agente de Registo (Registrar) credenciado pela DNS.PT deverá garantir um conjunto de requisitos que pode consultar em:
<https://www.dns.pt/pt/registrar/ser-registrar-pt/>
- Pode consultar a lista em (atualmente estão registadas 106 empresas) :
<http://www.dns.pt/pt/registrars/>

Números Globais

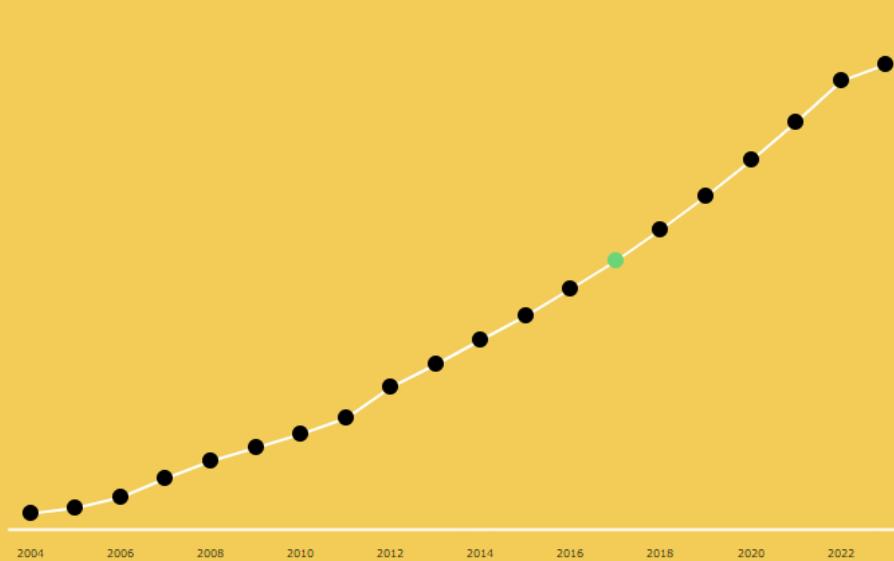
Estatísticas

Domínios Registados:

hoje **565**

última semana **3.750**

Evolução do Registo de Domínios



Fonte: <https://www.dns.pt>

Números Globais

Domínios Registrados por RIR

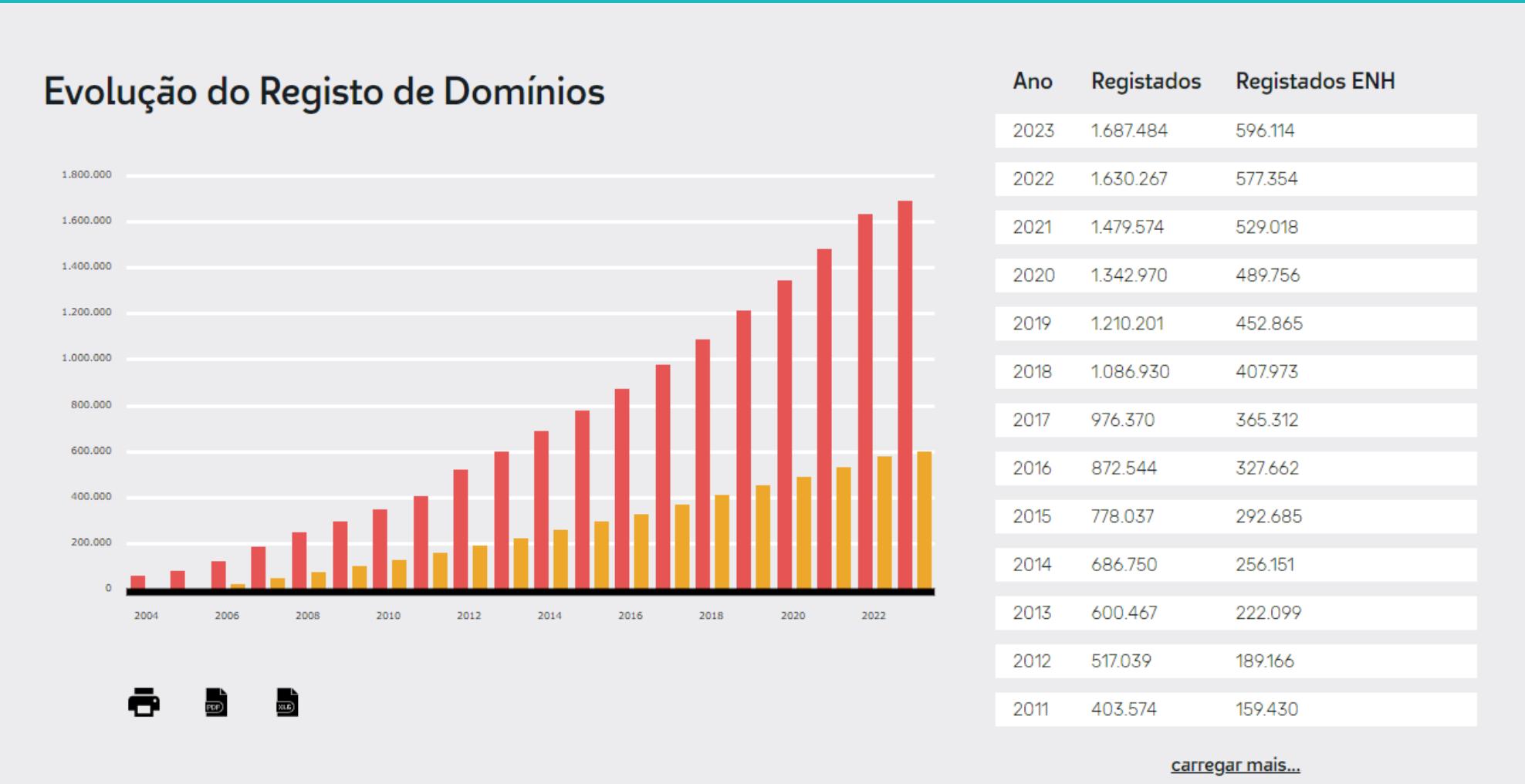


RIR Domínios (2023)

RIR	Domínios (2023)
AfriNIC	1680
APNIC	18334
ARIN	19063
LACNIC	15785
RIPE NCC	1590537

Fonte: <https://www.dns.pt>

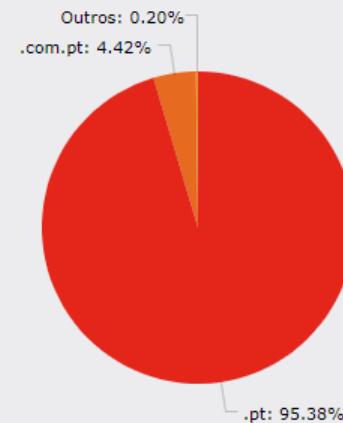
Números em Portugal



Fonte: <https://www.dns.pt>

Números em Portugal

Domínios registados por Hierarquia



Hierarquia Domínios

Hierarquia	Domínios
.pt	1.429.157
.com.pt	66.236
Outros	2.996

Fonte: <https://www.dns.pt>

Números em Portugal



Fonte: <https://www.dns.pt>

Custos

- O registo de domínios é habitualmente pago.
- Os preços podem variar consoante o tipo de domínio
 - Entre 10 € e 60 € por ano (por vezes, existe uma taxa inicial de submissão)
 - Para Portugal são estes os custos:

.pt e restantes hierarquias	S/IVA	IVA 23%	C/IVA	
	1 ano	23,00 €	5,29 €	28,29 €
	3 anos	50,00 €	11,50 €	61,50 €
	5 anos	70,00 €	16,10 €	86,10 €

Fonte: <https://www.dns.pt/pt/dominio/precos/>

- Quem registar um nome pode disponibilizá-lo a outra entidade (leia-se... vendê-lo ;-))

Domínios e Zonas

- **Domínio/Subdomínio**
 - Subárvore do espaço de nomes definido pelo DNS.
 - Exemplos:
 - isec.pt.
 - deis.isec.pt.
 - O domínio deis.isec.pt. é um subdomínio de isec.pt.
- **Zona**
 - Conteúdo de uma secção contígua do espaço de nomes normalmente delimitada por fronteiras administrativas que pode ser ou não coincidente com um domínio ou subdomínio.

Zonas

- Os computadores e organizações que estejam pendurados no mesmo nó da árvore do DNS partilham uma parte do nome dos respetivos domínios.
- Por exemplo, todos os computadores e departamentos existentes no ISEC utilizam o domínio `isec.pt`. Pode-se então definir uma zona para essa subárvore do DNS que pode ser um domínio nacional de topo (TLND - Top Level National Domain) ou ao nível do departamento/organização.
- Dentro de uma zona o serviço DNS para zonas subsidiárias pode ser delegado conjuntamente com um domínio subsidiário.
- Desta forma, embora exista uma entidade responsável pela administração do domínio `pt`, que é a FCCN, a responsabilidade da administração do domínio `isec.pt` foi delegada ao ISEC.

Nomes de Domínios

- **Nome absoluto (FQDN – Fully Qualified Domain Name)**
 - É estruturado da seguinte forma: "*host.3rd-level-domain.2nd-level-domain.top-leveldomain*"
 - O número de níveis não é fixo.
 - Caso nenhum domínio seja definido, o domínio default localdomain será usado.
 - Exemplo: www.isec.pt
- **Nome relativo**
 - Sequência não terminada por “.”
 - Exemplo: www

Servidores de ROOT

- São servidores autoritários com papéis especiais, sem eles a Internet não funciona.
- Existem 13 servidores (10 nos Estados Unidos, 2 na Europa e 1 na Ásia). O conteúdo de cada um é replicado 2 vezes por dia de forma automática.
- Existem replicas destes servidores espalhadas por todo o mundo.
- Possuem uma tabela que indica qual o servidor DNS responsável pela resolução de cada um dos *Top Level Domains*.

Servidor*	Localização	Responsável	Site
A	Virginia (EUA)	VeriSign	www.verisign.com
B	Califórnia (EUA)	ISI	www.isi.edu
C	EUA	Conget	www.congentco.com
D	Maryland (EUA)	Universidade de Maryland	www.umd.edu
E	Califórnia (EUA)	NASA	www.nasa.gov
F	Vários países	ISC	www.isc.org
G	Ohio (EUA)	US DoD	www.defenselink.mil
H	Maryland (EUA)	US Army Research Lab	www.defenselink.mil
I	Vários países	Autonomica	www.autonomica.se
J	Vários países	VeriSign	www.verisign.com
K	Vários países	RIPE	www.ripe.net
L	Califórnia (EUA)	ICANN	www.icann.org
M	Tóquio (Japão)	Wide Project	www.wide.ad.jp



Servidores *Top Level Domains*

- Existem de dois tipos:
 - **Generic Top level domains** - relacionados com as funções das organizações
 - **Generic** - usados para organizações genéricas (.com, .info, .net, .org)
 - **Generic restricted** - usados para determinadas funções (.biz, .name, .pro)
 - **Infrastructure** - utilizado apenas na infraestrutura do DNS (.arpa)
 - **Sponsored domains** - só podem ser utilizados por empresas ou entidades vinculadas a esses setores (.edu, .gov, .mil, .Travel etc)
 - **Country Code Top Level Domain** - relacionados com a localização das organizações(.pt, .br, .fr, etc)

Servidores Top Level Domains .pt

Name Servers

HOST NAME	IP ADDRESS(ES)
ns.dns.br	200.160.0.5 2001:12ff:0:a20:0:0:5
ns2.nic.fr	192.93.0.4 2001:660:3005:1:0:0:1:2
b.dns.pt	194.0.25.23 2001:678:20:0:0:0:23
c.dns.pt	204.61.216.105 2001:500:14:6105:ad:0:0:1
e.dns.pt	193.136.192.64 2001:690:a00:4001:0:0:0:64
a.dns.pt	185.39.208.1 2a04:6d80:0:0:0:0:1
d.dns.pt	185.39.210.1 2a04:6d82:0:0:0:0:1
g.dns.pt	193.136.2.226 2001:690:a80:4001:0:0:0:100
f.dns.pt	162.88.45.1 2600:2000:3009:0:0:0:1
h.dns.pt	194.146.106.138 2001:67c:1010:35:0:0:0:53

Servidores Locais

- A entidade responsável pela zona deve possuir um único servidor primário e, preferencialmente, um ou mais servidores secundários.
- A grande diferença entre estes dois tipos de servidores é que um servidor primário carrega toda a informação da zona em causa a partir de ficheiros (base de dados) existentes em disco, enquanto os servidores secundários obtêm toda a informação a partir do servidor primário.
- Quando um servidor secundário obtém a informação do primário respetivo, essa operação tem o nome de *zone transfer*.
- Quando um novo computador é adicionado à zona, o administrador adiciona a informação apropriada (nome e endereço IP) a um ficheiro em disco existente no servidor primário (que constitui a base de dados DNS local). O servidor de nomes primário é então notificado que tem de reler os ficheiros de configuração.
- Os servidores secundários contactam o primário de uma forma regular (normalmente cada 3 horas), e se o primário possuir novos dados, os secundários obtêm esses dados através do mecanismo de *zone transfer* (porta 53 TCP).
- Um determinado servidor pode ser primários ou secundário de diversas zonas.

Servidores Primários

- Trata-se de um servidor DNS responsável pelo menos por uma zona, obtendo os dados dessa Zona a partir de ficheiros locais (Zone files).
- Diz-se que é Autoritário para essa Zona, sendo que a alteração da informação relativa à mesma (adição de domínios ou máquinas) apenas pode ser feita localmente.
- Em geral o Master Name Server é o servidor primário da zona.
- Não precisa de correr na rede (física e lógica) da autoridade responsável pela Zona:
 - pode estar a correr numa rede distinta.
 - os Zone files podem ser importados por FTP ou email quando houver necessidade de atualizar a informação da zona.

Servidores Secundários

- Servidor que obtém os dados da zona a partir de outro servidor de DNS (*Master Zone Server* – servidor primário ou secundário)
- Periodicamente ou sempre que o servidor arranca é verificada a necessidade de efetuar uma atualização dos dados da zona (*Zone Transfer*)
- Cada ISP, instituição, etc. tem vários servidores locais que são usados diretamente pelos utilizadores as *queries* DNS dos utilizadores são dirigidas a estes servidores
- Vantagens de possuir servidores secundários:
 - **Redundância** - Se um dos servidores falhar os restantes poderão ser contactados em alternativa (mecanismo de *timeout*).
 - **Localização remota** - Para evitar a latência das ligações WAN é boa política os subdomínios possuírem um servidor secundário do seu domínio pai.
 - **Distribuição da carga de processamento** - Para evitar a congestão de um único servidor deve-se distribuir as consultas a um domínio por diversos servidores.

Outros Servidores

- ***Forward***
 - Trata-se do servidor de uma organização eleito para interagir com os servidores exteriores à mesma quando há necessidade de resolver nomes não locais.
 - É uma configuração feita por servidor e não por Zona.
 - Se os servidores internos ao contactar o forwarder não virem os seus pedidos resolvidos tentam pelos seus próprios meios efetuar a resolução contactando o exterior.
- ***Stub Server***
 - Mantém apenas uma cópia abreviada da zona (*stub zone*), contendo a lista dos servidores '*authoritative*' para essa zona.
- ***Caching-only server***
 - Apesar de todos os servidores fazerem caching de todas as consultas recebidas e resoluções corretamente realizadas existem servidores que são exclusivamente ativados para essa tarefa não efetuando a manutenção de nenhuma Zona.

Resolvers

- São servidores utilizados pelas aplicações cliente para consultar o DNS.
- Necessitam de conhecer pelo menos a localização de um servidor de nomes.
- Usam a informação fornecida pelo servidor de nomes conhecido para responder às consultas dos clientes.
- A resposta pode ser diretamente fornecida pelo servidor de nomes conhecido ou por contacto sucessivo de outros servidores referidos.
- São tanto mais eficientes quanto maior for a abrangência da sua cache.

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.

Exemplo

```
#####
@ IN SOA dominio.com.br. root.dominio.com.br. (
    1996042901 ;versão
    10800 ;refresh (3 horas)
    1800 ;retry (30 minutos)
    3600000 ;expire (41 dias e 16 horas)
    86400) ;ttl default (1 dia)
;
;           IN NS      ns.dominio.com.br.
;           IN NS      ns.roadhash.com.br.
;
;           IN MX    5   ns.dominio.com.br.
;           IN MX   10  ns.roadhash.com.br.
gw          IN A      192.0.1.2
ns          IN A      192.0.1.1
www         IN CNAME  ns
ftp          IN CNAME  ns
gopher       IN CNAME  ns
async1       IN A      192.0.1.3
async2       IN A      192.0.1.4
async3       IN A      192.0.1.5
async4       IN A      192.0.1.6
async5       IN A      192.0.1.7
async6       IN A      192.0.1.8
async7       IN A      192.0.1.9
async8       IN A      192.0.1.10
#####
#
```

DNS Servers

ns.isec.pt	193.137.78.1
ns2.isec.pt	193.137.78.3

Lookup MX Records

Answer records

isec.pt.	IN	SOA	ns.isec.pt.
	(
		Email	psfaria@isec.pt
		Serial	2012022104
		Refresh	3600
		Retry	1800
		Min. TTL	43200
)		
isec.pt.	IN	MX	20 prxmx2.isec.pt.
isec.pt.	IN	MX	30 prxmx2.isec.pt.
isec.pt.	IN	MX	40 prxmx1.isec.pt.
isec.pt.	IN	MX	10 prxmx2.isec.pt.
isec.pt.	IN	NS	ns.isec.pt.
isec.pt.	IN	NS	ns2.isec.pt.
isec.pt.	IN	TXT	"v=spf1 ip4:193.137.78.24 ip4:193.137.78.26 ip4:193.137.78.20 ip4:193.137.78.21 -all"

Additional

prxmx2.isec.pt.	IN	A	193.137.78.26
prxmx1.isec.pt.	IN	A	193.137.78.24
ns.isec.pt.	IN	A	193.137.78.1
ns2.isec.pt.	IN	A	193.137.78.3

Serviços de Rede 1

2022-2023

Pedro Miguel Geirinhas

Aula 7

DNS- Domain Name System

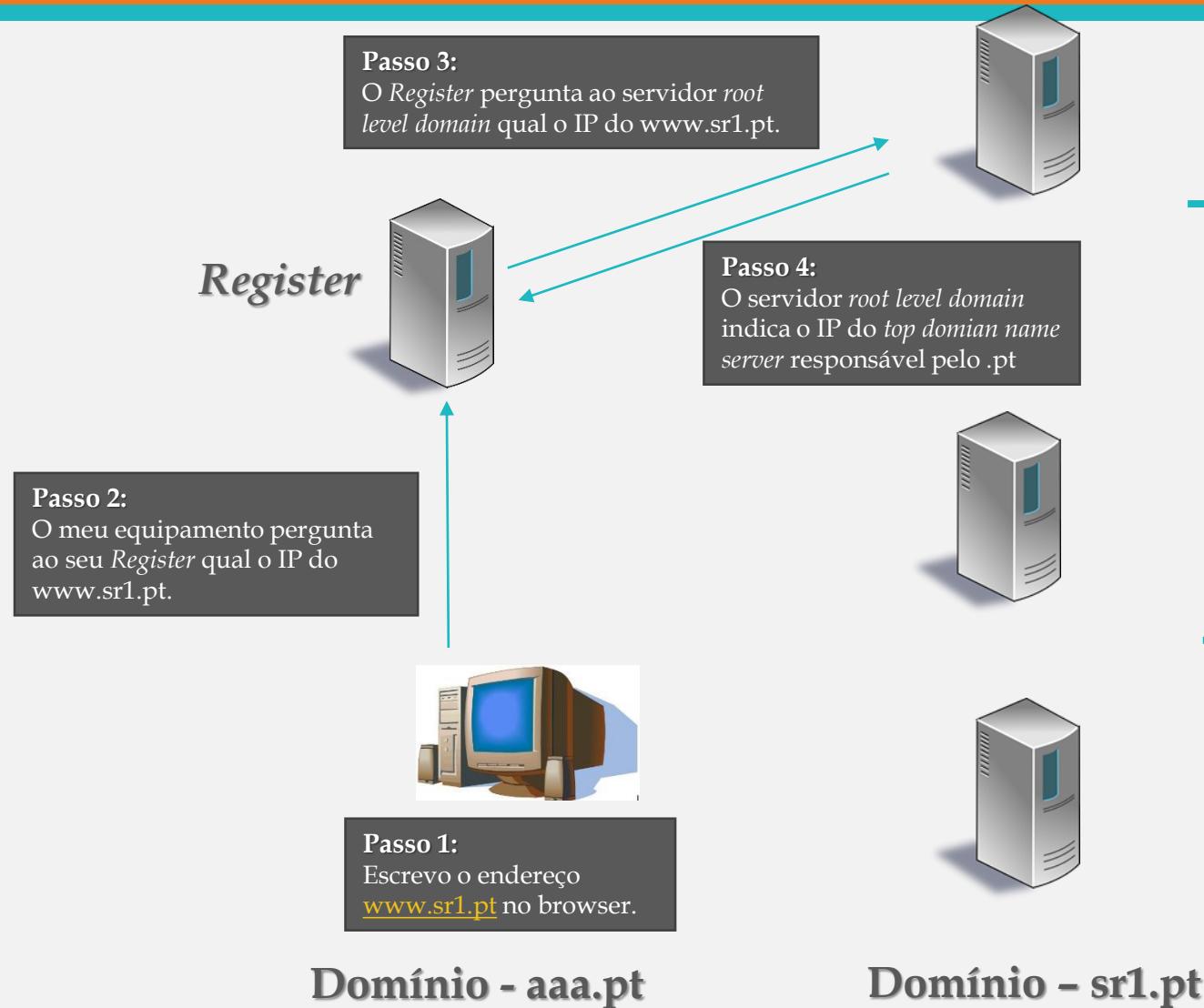
Agenda

- 1.** Funcionamento
- 2.** Tipo de consultas
- 3.** Ferramentas

Funcionamento

- Já vimos em outras aulas, que a ligação entre duas máquinas só é possível com o conhecimento de duas informações fundamentais:
 - Endereço IP.
 - Endereço físico (MAC).
- Então para que a máquina A se ligue à máquina B é necessário saber o endereço IP e depois o MAC dessa máquina.
- Mas se no browser eu escrevo o nome da máquina destino, como é que a minha máquina sabe o IP da máquina destino?
- Sim, eu sei que esse é o papel do DNS, mas como funciona?

Funcionamento



Root-Level Domain Server

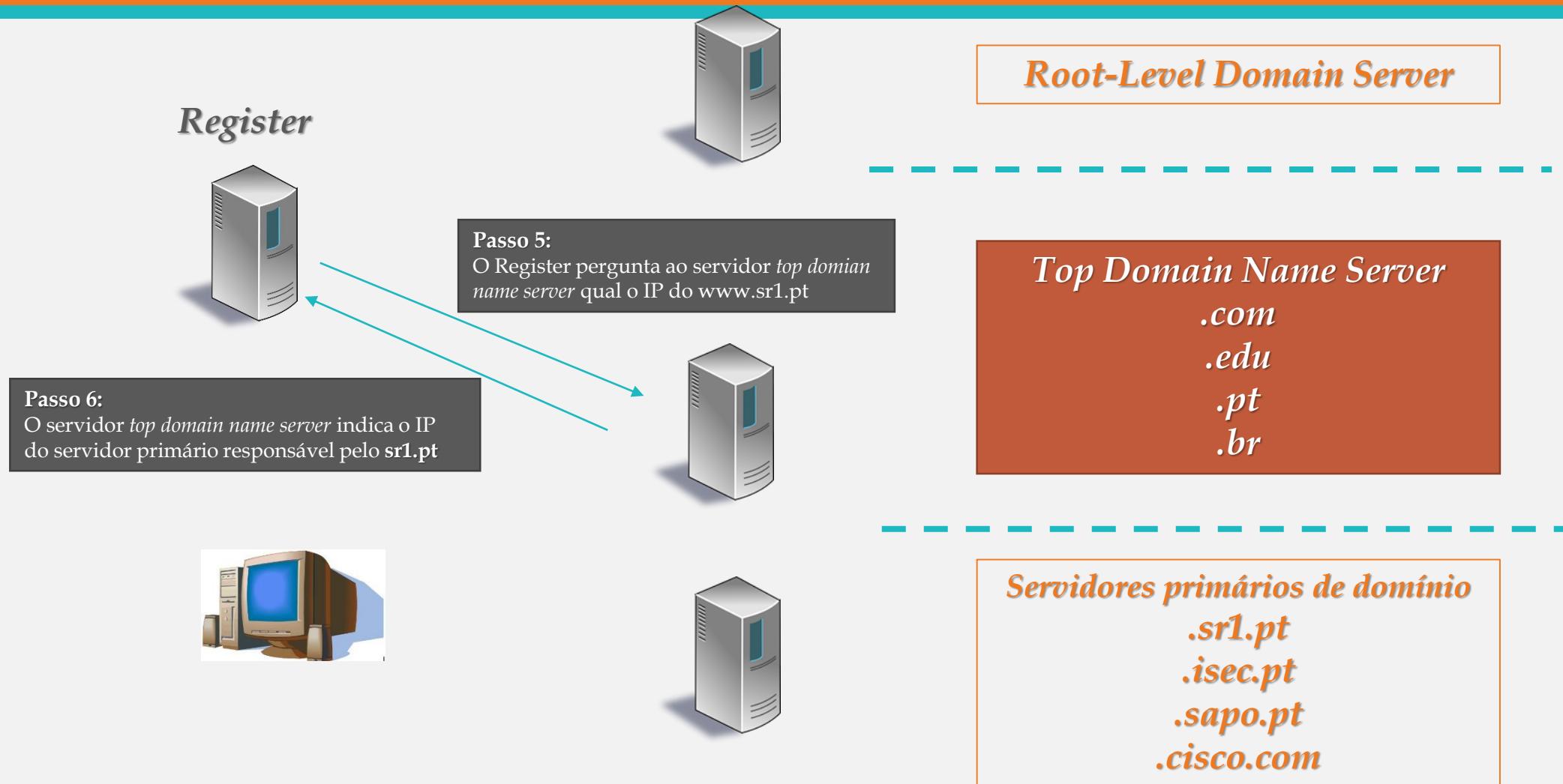
Top Domain Name Server

.com
.edu
.pt
.br

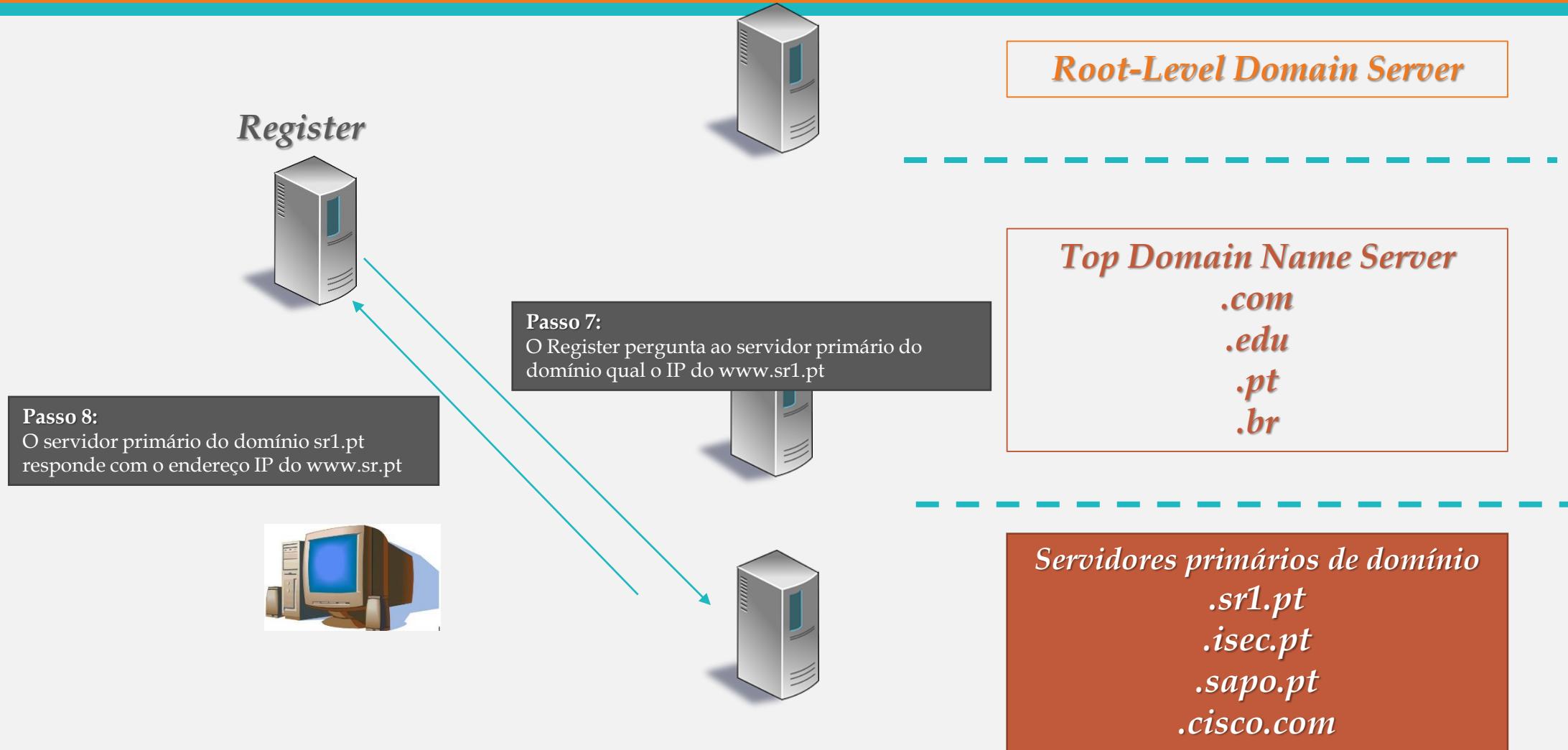
Servidores primários de domínio

.sr1.pt
.isec.pt
.sapo.pt
.cisco.com

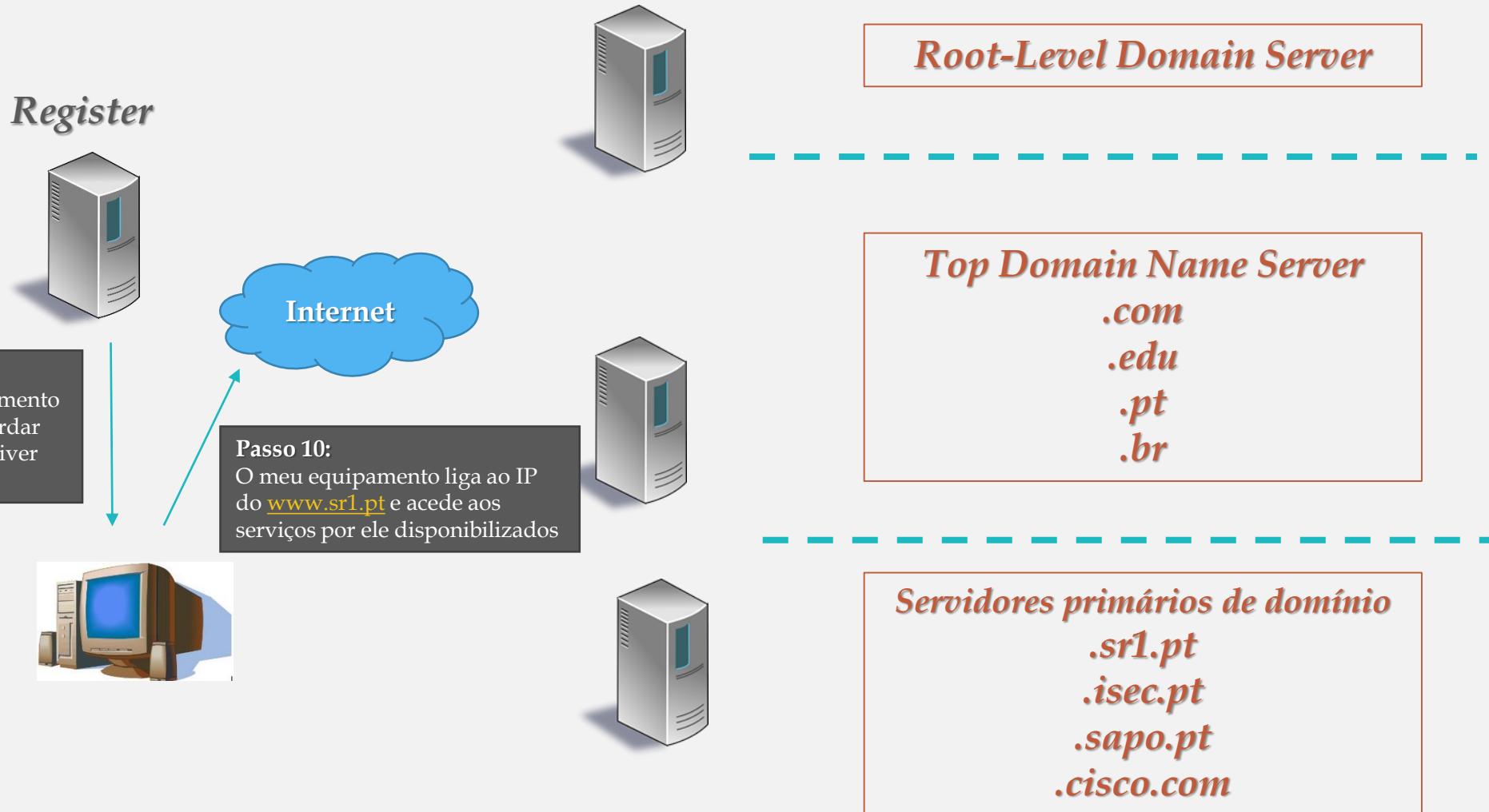
Funcionamento



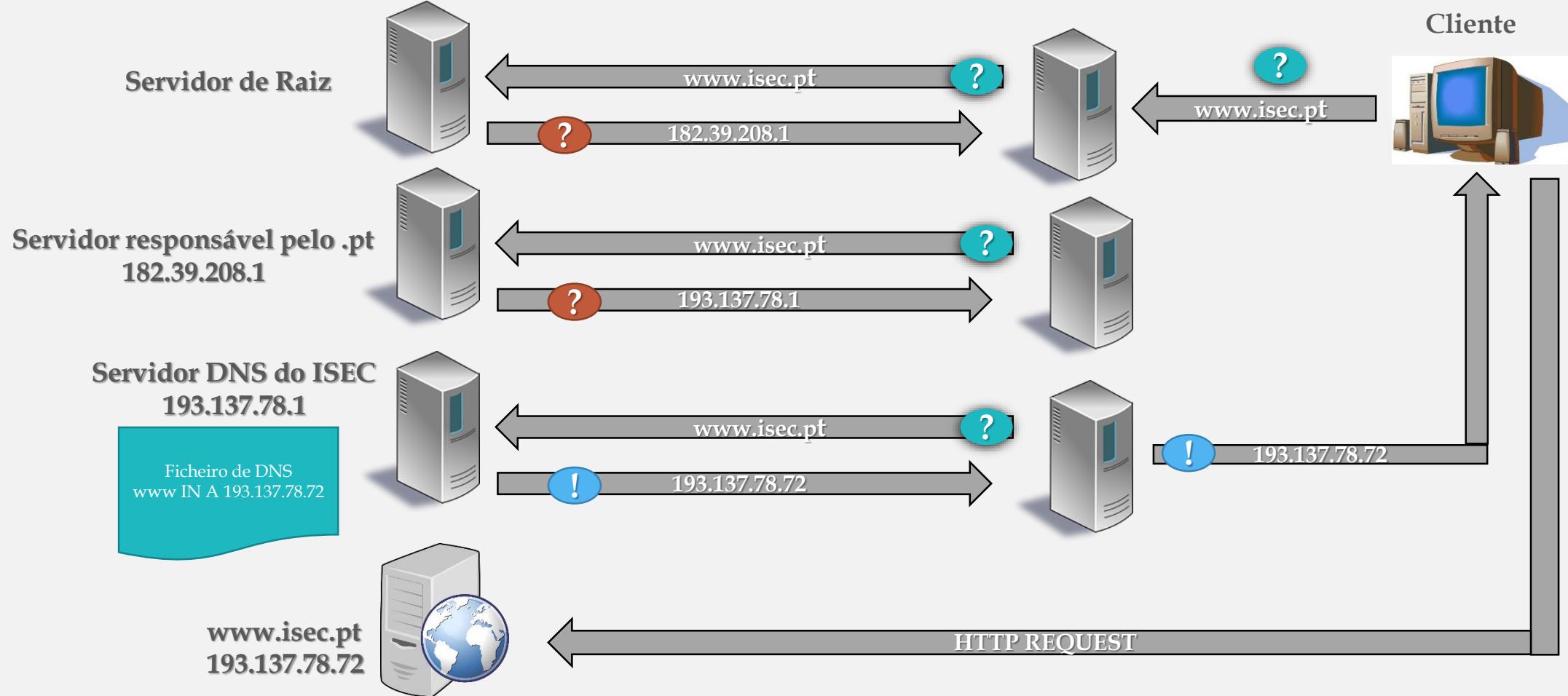
Funcionamento



Funcionamento

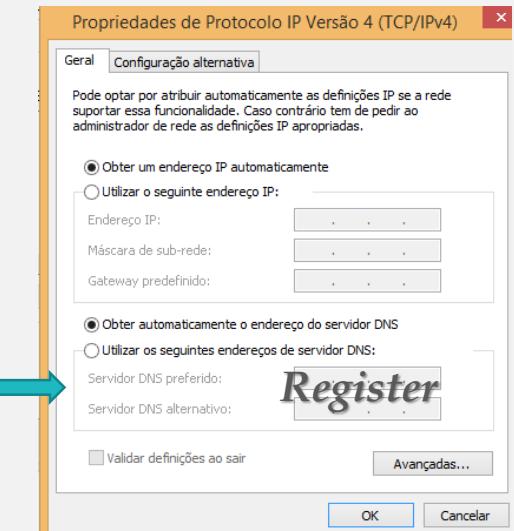


Funcionamento



Funcionamento

- **O Register é o primeiro local que a minha máquina usa para tentar obter o IP?**
 - Não. A sua máquina a primeira ação que faz é consultar o ficheiro hosts e só no caso de neste ficheiro não estar esta correspondência é que pergunta ao seu register.
- **Qual o endereço IP do Register que a máquina local utiliza?**
 - O IP que coloca na placa de rede do seu equipamento no campo DNS ou que está definido no seu serviço DHCP como o seu servidor DNS.
- **Qual o endereço IP que o servidor primário de um domínio devolve quando é questionada?**
 - O que estiver configurado na sua tabela. Assim, no exemplo anterior, se na tabela do servidor responsável pelo domínio sr1.pt estivesse criado um registo do tipo A com o IP 203.100.2001.1 para a máquina www seria esse o valor que ele respondia.
- **O Register que tenho definido no meu PC tem de ser uma máquina da minha rede local?**
 - Não, pode ser uma máquina fora da minha rede.
- **O Register pode ser o servidor primário do meu domínio DNS?**
 - Pode. O servidor de um dado domínio pode ser também o Register das máquinas desse domínio.



Caching

- Uma característica fundamental do DNS é o *caching*. Isto é, quando um servidor de nomes recebe informação sobre um mapeamento de um computador, faz o *caching* dessa informação para futuras utilização em perguntas iguais.
- Então, uma consulta posterior relativo a esse mapeamento pode utilizar o resultado *cached*, evitando assim inquéritos adicionais a outros servidores.
- O DNS utiliza o *caching* para otimizar o custo da pesquisa.
- Desta forma, os endereços dos servidores TLD (Top Level Domin) estão sempre em cache.
- Uma entrada é mantida na cache até um limite de tempo controlado pelo administrador do servidor responsável pelo nome *cached* através do atributo TTL (Time To Live).
- Entrada é automaticamente removida da cache quando seu TTL expira.

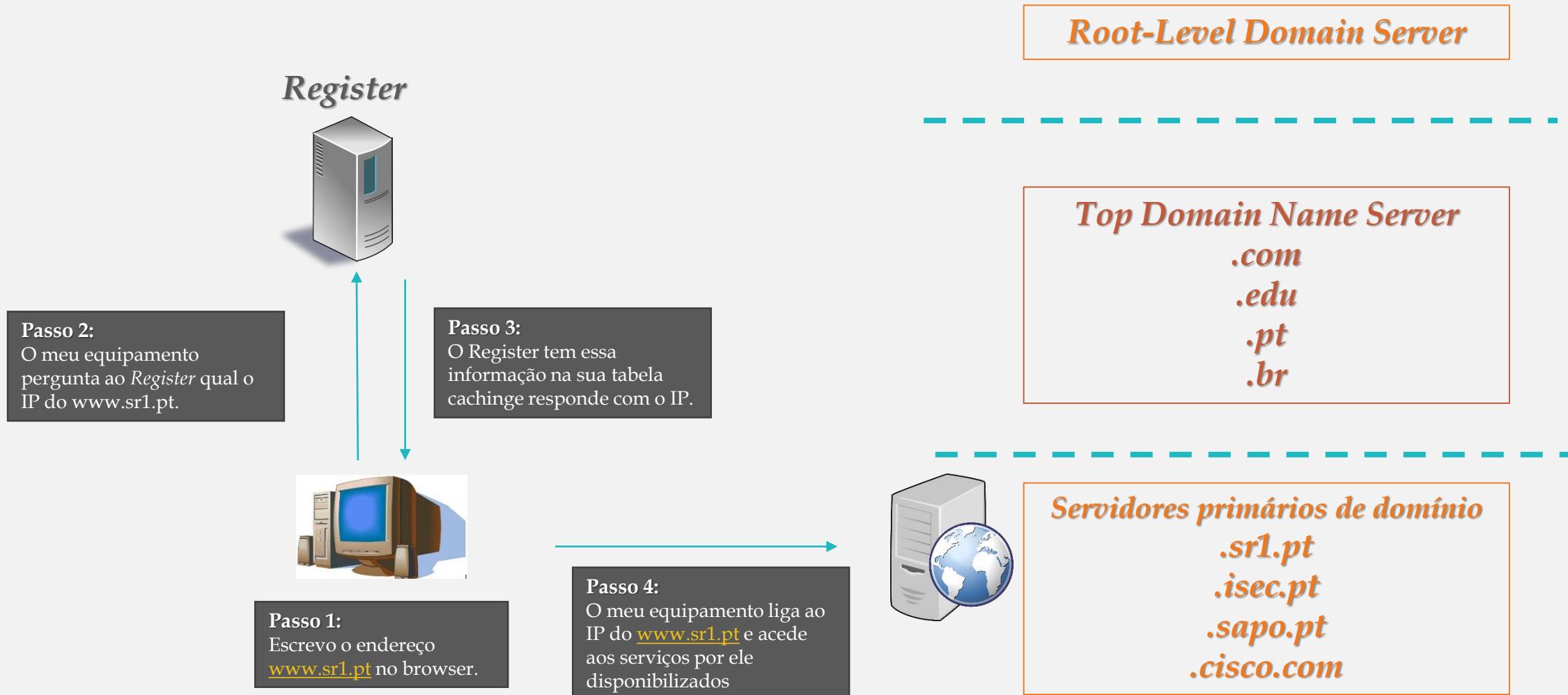
Caching

- Dado que a informação sobre um determinado nome pode ser alterada, um servidor pode possuir informação incorreta na sua tabela de *caching*.
- Utiliza-se então o valor TTL para decidir quando é que a informação não pode ser mais considerada como válida.
- Se um servidor responder a alguma consulta com informação em cache deve:
 - atualizar o TTL da RR fornecida na resposta
 - indicar que se trata de informação não autoritária bit AA (*authoritative answer*) colocado a 0 (false).

Caching

- O DNS suporta, opcionalmente, *caching* de respostas negativas.
 - Exemplo: um servidor pode distribuir um TTL com uma indicação de “name error”.
- O cliente que receber esta informação pode assumir que o nome em causa não existe durante TTL sem consultar dados autoritários.
- Da mesma forma pode ser realizada uma consulta com um QTYPE que represente múltiplos tipos e armazenar em cache uma resposta com a indicação de que parte dos tipos não estão presentes.
- Os servidores que fornecem serviço recursivo devem estar bem apetrechados de memória!

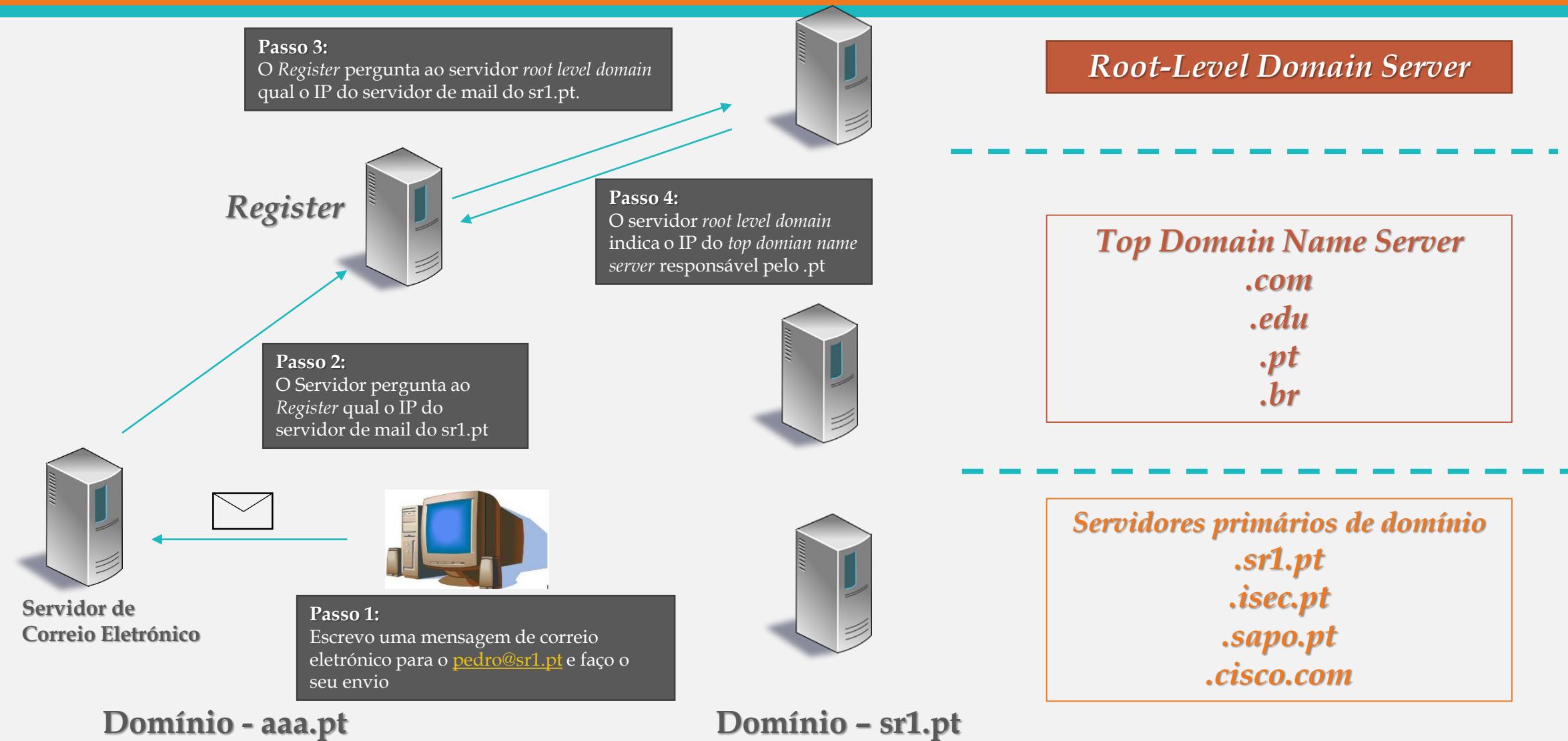
Funcionamento - *Caching* e no caso de o *Register* já tenha informação do IP do www.sr1.pt



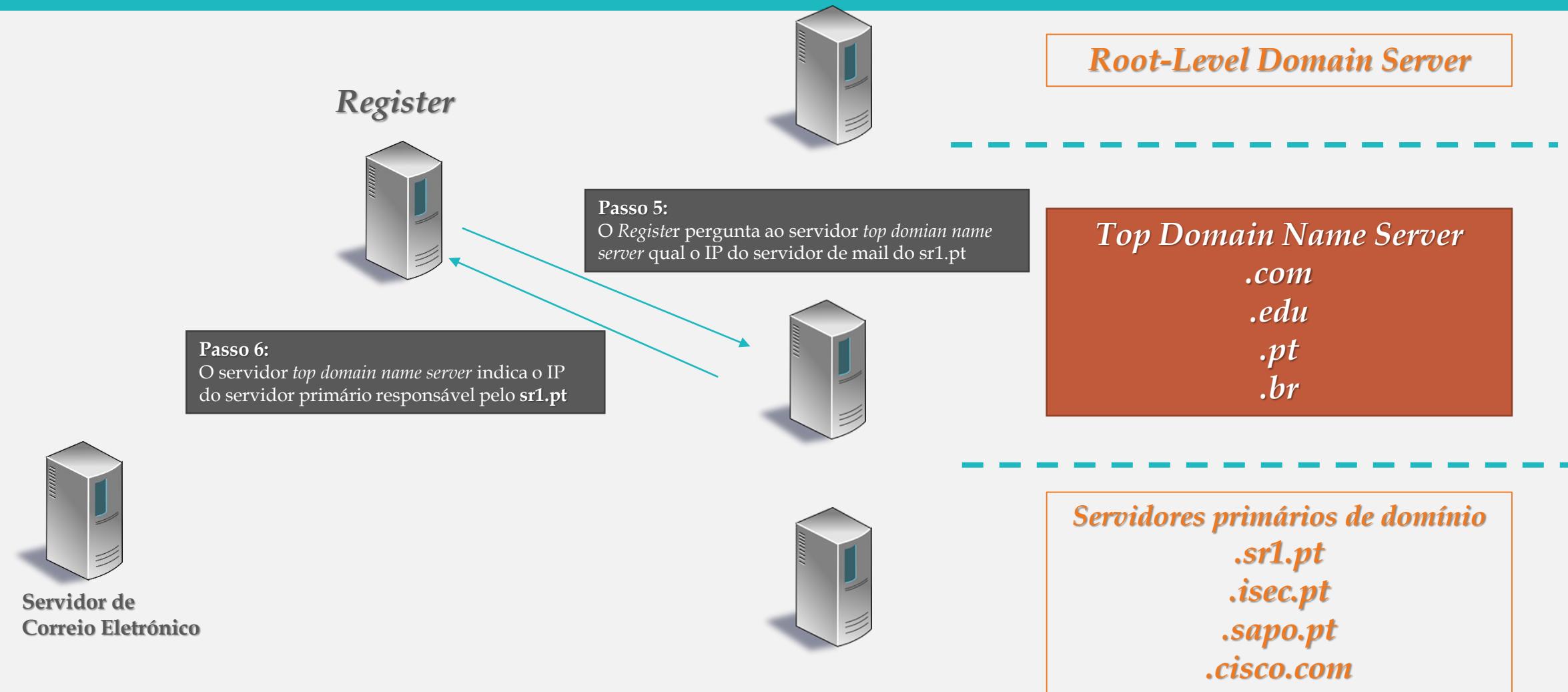
Funcionamento - Correio Eletrónico (MX)

- No caso de pretender enviar uma mensagem de correio eletrónico, o seu servidor não sabe o nome da máquina onde tem de entregar a mensagem. Conhece apenas o endereço de correio eletrónico do destinatário e consequentemente o domínio.
- O funcionamento será idêntico ao descrito para saber o IP do nome de uma máquina, mas agora a pergunta não terá como resposta o IP de um nome mas sim do registo MX do domínio destino.

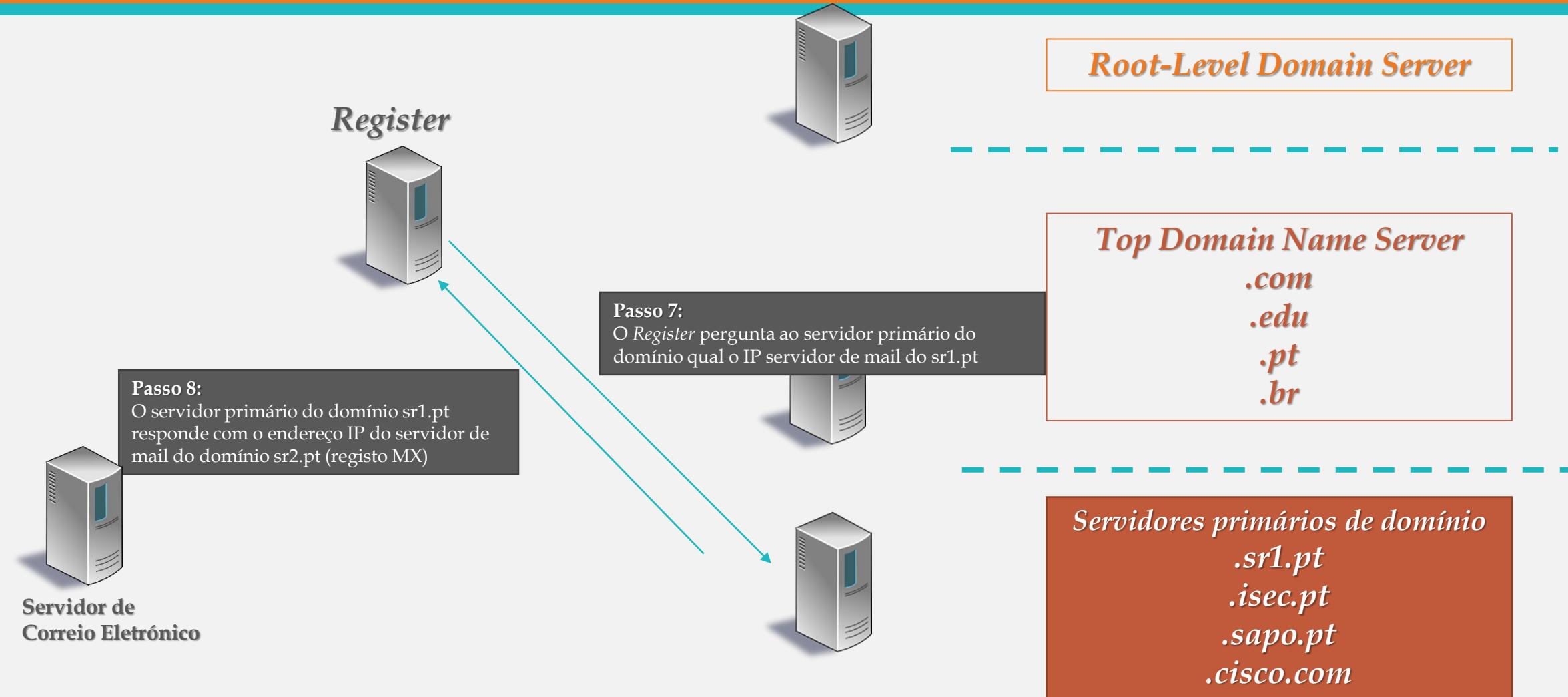
Funcionamento - Correio Eletrónico (MX)



Funcionamento - Correio Eletrónico (MX)



Funcionamento - Correio Eletrónico (MX)



Funcionamento - Correio Eletrónico (MX)

Register



Passo 9:

O Register informa servidor de mail do IP do servidor de mail de sr2.pt podendo guardar na sua tabela essa informação se tiver *caching* ativo.



**Servidor de
Correio Eletrónico
do domínio aaa.pt**

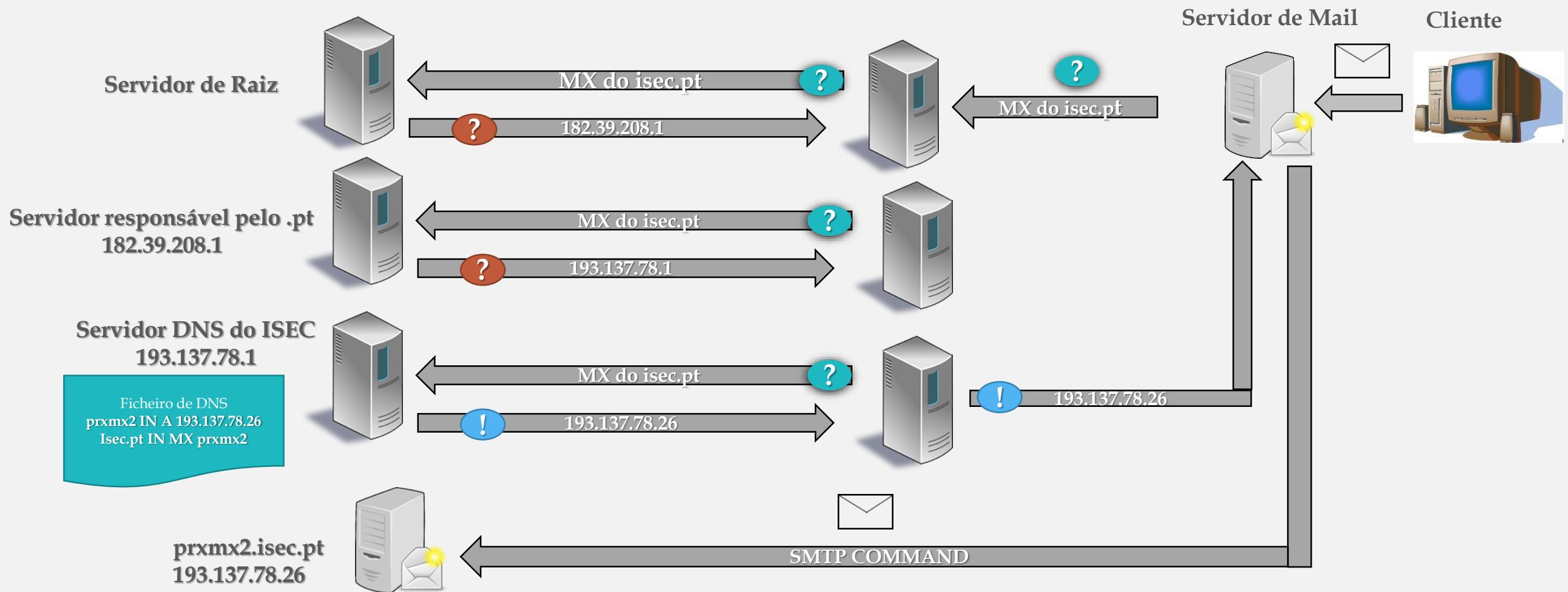


**Servidor de
Correio Eletrónico
do domínio sr1.pt**

Passo 10:

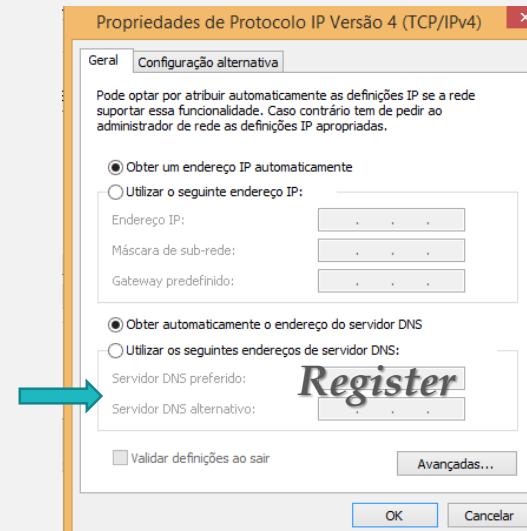
O servidor de mail de aa.pt estabelece a ligação com o servidor de mail sr1.pt e entrega a mensagem de mail para o pedro@sr1.pt

Funcionamento - Correio Eletrónico (MX)



Funcionamento

- **Qual o endereço IP do Register do servidor de mail do domínio aa.pt?**
 - O IP que coloca na placa de rede do seu servidor no campo DNS. Nos servidores não devemos utilizar endereços atribuídos por DHCP
- **Qual o endereço IP que o servidor primário de um domínio devolve quando é questionado, se não sabe o nome da máquina?**
 - Quando o servidor de mail inicia o processo não sabe nome da máquina destino, mas só o nome do endereço do destinatário da mensagem (a mensagem é para ser entregue em *utilizador@dominio*). Então a resposta do servidor DNS do domínio destino não será de uma máquina (registo do tipo A) mas sim da máquina que tem o registo MX.



Tipo de consultas

- **Interativa**
 - Trata-se de uma consulta à qual o servidor contactado responde com informação disponível localmente.
 - A resposta pode consistir:
 - No endereço IP- se for informação autoritária ou estiver em cache.
 - Numa referência a um servidor mais “próximo” da resposta.
 - Num erro - em caso de consultas mal formuladas.
 - Quem realiza estas consultas?
 - os servidores DNS que tentam responder a uma consulta recursiva.
 - os resolvers (raramente).
 - Os servidores são obrigados a aceitar este modo.

Tipo de consultas

- **Recursiva**
 - Trata-se de uma consulta à qual o servidor contactado responde sempre com a resolução pedida ou com uma indicação de erro (i.e. fornece a resposta final!)
 - Quem realiza estas consultas?
 - os *resolvers* (tipicamente).
 - os servidores DNS configurados para usar um *forward*.
 - Nenhum servidor DNS é obrigado a aceitar este tipo consulta (e.g.: os root servers não aceitam!)
 - Deve existir um servidor DNS, por rede local, capaz de aceitar consultas recursivas.
 - Centralizar a interação com o exterior melhora o efeito de *caching*!

Respostas

- **Com autoridade** (*authoritative*) - Gerada por servidores que possuem autoridade no domínio do nome resolvido. Resposta bastante confiável, mas pode estar incorreta (se fornecida por um servidor secundário e não pelo primário)
- **Sem autoridade** (*non-authoritative*) - Gerada por servidores que não possuem autoridade no domínio do nome resolvido. A resposta não é tão confiável, pois as informações podem ter sido modificadas.

Ferramentas

- Existem sites na Internet que permitem validar a correcta configuração do seu servidor de DNS .
- Um que pode utilizar é fornecido pela DNS.PT:

<http://www.dns.pt/pt/ferramentas/avaliador-tecnico/>

The screenshot shows the 'Avaliador Técnico' section of the DNS.PT website. The top navigation bar has a green header with the '.pt' logo. Below it, there's a menu with 'Ferramentas', 'WHOIS', and 'Avaliador Técnico' items, where 'Avaliador Técnico' is highlighted in yellow. A sub-menu for 'Avaliador Técnico' is open, showing options like 'DNS', 'MX', 'CNAME', and 'A'. The main content area has a green header with the text 'Ao registrar um novo domínio, ou sempre que realizar alterações técnicas deverá recorrer ao avaliador técnico'. It contains two main sections: 'Esta ferramenta permite confirmar a boa configuração dos servidores de DNS indicados para o seu domínio.' and 'Avaliar Domínio'. The 'Avaliar Domínio' section includes input fields for 'Domínio a verificar:' (with 'ex: nic.pt') and 'IP ou nome do servidor primário:' (with 'ex: 193.136.0.1 ou ns.dns.pt'), and a large black 'Avaliar' button at the bottom.

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 - Modos

- **Modo não-interativo**

- Este modo é utilizado para apresentar o nome e informação associada relativa a um computador (*host*) ou domínio.
- O nome ou endereço Internet é fornecido como primeiro parâmetro. O segundo parâmetro é opcional e corresponde ao nome ou endereço de um servidor de nomes de domínios (*name server*).

- **Modo interativo**

- Com o modo interativo, o utilizador pode questionar servidores de nomes de domínios de modo a obter informação sobre vários computadores e domínios ou para imprimir a lista de computadores existentes num domínio.
- Este modo é invocado quando especifica o comando nslookup sem parâmetros, sendo então utilizado o servidor de nomes de domínios pré-definido.
- Pode ainda invocar este modo interativo se o primeiro parâmetro utilizado for um - e o segundo parâmetro for o nome de um computador ou endereço Internet de um servidor de nomes de domínios.

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

```
C:\Users\Pedro Geirinhas>ipconfig /displaydns
Windows IP Configuration
win8.ipv6.microsoft.com
-----
Name does not exist.

youtube.com
-----
Record Name . . . . . : youtube.com
Record Type . . . . . : 1
Time To Live . . . . . : 83
Data Length . . . . . : 4
Section . . . . . : Answer
A <Host> Record . . . . . : 216.58.211.238

Record Name . . . . . : ns2.google.com
Record Type . . . . . : 1
Time To Live . . . . . : 83
Data Length . . . . . : 4
Section . . . . . : Additional
A <Host> Record . . . . . : 216.239.34.10

Record Name . . . . . : ns1.google.com
Record Type . . . . . : 1
Time To Live . . . . . : 83
Data Length . . . . . : 4
Section . . . . . : Additional
A <Host> Record . . . . . : 216.239.32.10

Record Name . . . . . : ns3.google.com
Record Type . . . . . : 1
Time To Live . . . . . : 83
Data Length . . . . . : 4
Section . . . . . : Additional
A <Host> Record . . . . . : 216.239.36.10

Record Name . . . . . : ns4.google.com
Record Type . . . . . : 1
Time To Live . . . . . : 83
Data Length . . . . . : 4
Section . . . . . : Additional
A <Host> Record . . . . . : 216.239.38.10

Record Name . . . . . : ns2.google.com
Record Type . . . . . : 28
Time To Live . . . . . : 83
Data Length . . . . . : 16
Section . . . . . : Additional
AAAA Record . . . . . : 2001:4860:4802:34::a
```

Serviços de Rede 1

2022-2023

Pedro Miguel Geirinhas

Aula 8

DNS- Domain Name System

Agenda

- 1.** Propagação
- 2.** Protocolo
- 3.** Segurança
- 4.** DNS reverse
- 5.** Atualizações dinâmicas

Propagação DNS

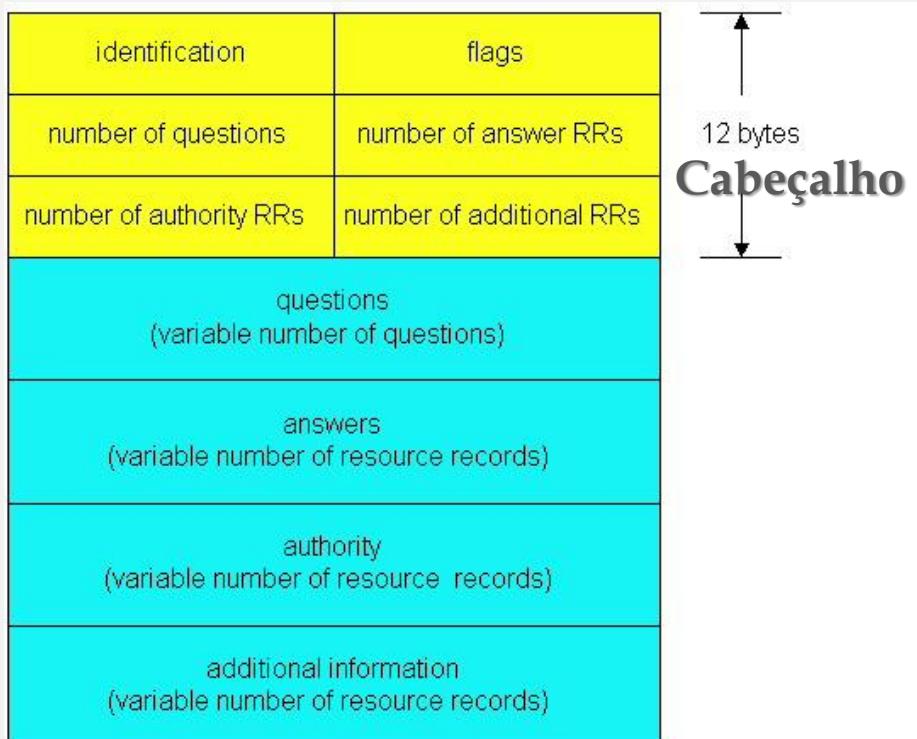
- É o tempo necessário para que um domínio seja publicado e divulgado em todos os servidores DNS existentes. Assim, entre a ativação do domínio e os servidores DNS receberem o novo domínio criado, demora um intervalo temporal, que é então o tempo de propagação de DNS.
- Este tempo também acontece quando altera a configuração do seu DNS por exemplo com a adição ou a alteração de um novo registo.
- A propagação leva de 8 a 48 horas. Durante este tempo o serviço fica instável, podendo funcionar em determinados momentos e dependente do *Register* que os clientes usem.
- Há várias razões, mas o que torna a operação lenta é justamente a necessidade de se informar outros servidores DNS do novo domínio ou da alteração efetuada como são alguns milhões de servidores demora o seu tempo...
- O processo de publicação é feito pelos órgãos responsáveis pelo registro de domínios. Estas entidades atualizam nos seus servidores e publicam uma "lista" de novos registros de domínios e alterações de servidores DNS, para domínios já registrados.
- Seguidamente ocorre a propagação, durante a qual as bases de dados dos servidores DNS dos ISP (Fornecedores de serviço de Internet) são atualizadas. Após esse processo, os domínios passam a apontar para o endereço IP do servidor onde estão as informações do site.
- Normalmente, a publicação não ultrapassa 48 horas, mas podem ocorrer situações, principalmente no caso de domínios internacionais, no qual este prazo pode ser maior. Isso depende exclusivamente da política da entidade que realiza os registros. Para além disso, a propagação dessas informações para os servidores DNS dos ISP pode também levar algum tempo e atrasar todo o processo.

Protocolos de Transporte

- **UDP**
 - Normalmente os pedidos e respostas DNS são transportados num *datagrama* UDP (< 512 bytes)
 - No caso de a informação a transportar ser superior ao tamanho desse *datagrama*, a resposta é enviada incompleta e a flag *Truncated* é ativada.
- **TCP**
 - Quando o volume de informação a transferir não cabe num *datagrama* UDP (>512 bytes), o cliente DNS estabelece uma ligação TCP com o servidor para realizar a transferência. Ou seja:
 - quando é recebida uma resposta com a flag *Truncated* ativada.
 - para transferência de informação de zonas do servidor primário para os secundários.
 - Em ambos o porto utilizado é o 53.

O Protocolo do DNS

- As mensagens de pergunta e de resposta têm ambas o mesmo formato:



- Cabeçalho** - identifica o tipo de operação DNS.
- Perguntas (Questions)** - pergunta a fazer ou feita.
- Respostas (Answers)** - o que o servidor consegue saber em resposta a essa pergunta (pode ser informação *cached*).
- Autoridade (Authority)** - dados sobre os *name servers* com autoridade sobre os dados listados na resposta.
- Informação Adicional (Additional information)** - dados que podem vir a ser úteis (informações suplementares que podem evitar mais perguntas).

Cabeçalho

- **Campo Identification**

Trata-se de um valor estabelecido pelo cliente e devolvido pelo servidor para que quem consulte saiba que a mensagem é a resposta a determinada questão.

- **Campo Flags**

QR	opcode	AA	TC	RD	RA	Z,AD,CD	rcode
1	4	1	1	1	1	3	4

identification	flags
number of questions	number of answer RRs
number of authority RRs	number of additional RRs

- QR = Tipo de Operação { 0 - Pergunta | 1- Resposta}
- opcode = Tipo de Pergunta { 0 - standard query | 1- inverse query | 2 - server status | ... }
- AA = Resposta autoritária? { 1 - authoritative answer | 0 }
- TC = Mensagem Truncada?{ 1- truncated (UDP máx = 512 bytes) | 0 }
- RD = Recursividade desejada?{ 1- recursion desired | 0 }
- RA =Recursividade disponível? { 1- recursion available | 0 }
- rcode = Tipo de resposta{ 0 - no error | 3 - name error (domínio inexistente) | ...}

Perguntas

- *query name* (32 bits): o domínio que está a ser consultado
- *query type* (16 bits): tipo de informação solicitada

Código	Nome	Descrição
1	A	IP address
2	NS	name server
5	CNAME	canonical name
252	AXFR	req. zone transfer

Código	Nome	Descrição
12	PTR	pointer records
13	HINFO	host info
15	MX	mail exchange
255	*ANY	req. all records

- *query class* (16 bits): possui somente um valor possível (internet).

Código	Descrição
1	Internet
2	CSNET
3	CHAOS
4	HESIOD

Respostas

- **Campo Answers**

- Domain Name
 - Chave de procura (Ex.: Nome de máquina)
- Type
 - Tipo de resposta
- Class
 - Tip. 1 - Internet
- Time To Live
 - Validade da informação (*cache*)
- Resource Data Domain Name
 - Informação adicional

domain name	
type	class
time to live (TTL)	
resource lenght	
resource data	

Resolução inversa - Reverse DNS resolution

- Recurso utilizado para resolver um nome através de um endereço IP ou seja a operação inversa a DNS
- Utilizado para garantir a confiabilidade do nome a ser apresentado, conferindo o nome com o endereço IP.
- Vantagens
 - Segurança (por exemplo: filtragem por nome ou zona geográfica).
 - Leitura facilitada de ficheiros de log.
 - Redução do SPAM (servidor destino pode questionar se o MX do domínio que lhe está a tentar entregar a mensagem tem o IP da máquina que lhe está a ligar).

Resolução inversa

Resolução Direta



Servidor DNS

Qual é o IP da máquina www.sr1.pt?

O registo A diz que é o 192.168.1.1



Cliente

Resolução Inversa



Servidor DNS

Qual é o nome da máquina que tem o IP 192.168.1.2?

O registo PTR diz que é o webmail.sr1.pt



Cliente

Resolução inversa

- A configuração da resolução inversa é efectuada através de domínios definidos para o efeito, pertencentes ao domínio ‘in-addr.arpa.’
 - Os subdomínios são definidos através da introdução dos octetos do endereço de rede, por ordem inversa
 - Exemplo (ISEC): 78.137.193.in-addr.arpa
- A gestão de um domínio ‘in-addr.arpa.’ só pode ser delegada se os endereços da classe (classe C, classe B,...) tiverem sido todos atribuídos a uma única entidade:
 - Exemplo (ISEC): o ISEC pode gerir o domínio 78.137.193.in-addr.arpa porque lhe foi delegada essa gestão por quem tem delegada a gestão da classe B 193.137.0.0 (FCCN).
 - A gestão de classes não completas é possível mas possui um nível de complexidade mais elevado, principalmente ao nível da sua manutenção.
- No caso do IPv6 a resolução inversa é efectuada através do domínio IP6.ARPA
 - o domínio inicial existente para este efeito, IP6.INT, está a ser abandonado.

Resolução inversa

```
root@gandalf:/home/pi# cat /etc/bind/zones/gondor.pt.db
$TTL 86400
@ IN SOA ns.gondor.pt. root.gondor.pt. (
    2014071101 ; Serial
    604800 ; Refresh
    86400 ; Retry
    2419200 ; Expire
    86400 ) ; Negative Cache TTL
;
@ IN NS ns.gondor.pt.
@ IN NS ns2.gondor.pt.

; Definicao de informacao textual do domnio
IN TXT "Dominio Rede Gondor"

; Definicao de servidores email do domnio
IN MX 10 mail

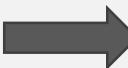
; Ativos de rede Gondor

gandalf IN A 192.168.100.253
ns IN A 192.168.100.253
www IN CNAME gandalf
mail IN A 192.168.100.253
ns2 IN A 192.168.100.246
ap1 IN A 192.168.100.151
ap2 IN A 192.168.100.152
ap4 IN A 192.168.100.153
chromecast IN A 192.168.100.154
ap3 IN A 192.168.100.245
gollum IN A 192.168.100.254
gw IN CNAME gollum
frodo IN A 192.168.100.251
aragorn IN A 192.168.100.250
nazgul IN A 192.168.100.252
saruman IN A 192.168.100.246
ippin IN A 192.168.100.247
meo1 IN A 192.168.100.248
meo2 IN A 192.168.100.249

; Clientes DHCP da rede Gondor

sauron-f IN A 192.168.100.1
sauron-w IN A 192.168.100.2
galadriel-f IN A 192.168.100.3
galadriel-w IN A 192.168.100.4
nexus4 IN A 192.168.100.5
motog IN A 192.168.100.6
sameiro-w IN A 192.168.100.7
sameiro-f IN A 192.168.100.8
hugom-p IN A 192.168.100.9
printer IN A 192.168.100.10
hugom-surface IN A 192.168.100.11
```

Direta



```
GNU nano 2.2.6          File: /etc/bind/zones/rev.100.168.192.in-addr.arpa

$TTL 86400
@ IN SOA ns.gondor.pt. root.gondor.pt. (
    2014070701 ; Serial
    604800 ; Refresh
    86400 ; Retry
    2419200 ; Expire
    86400 ) ; Negative Cache TTL

; Servidores com autoridade para a zona
IN NS ns.gondor.pt.
IN NS ns2.gondor.pt.

; Definicao de informacao textual do domnio
IN TXT "Dominio Rede Gondor"

; Ativos de rede Gondor

253 IN PTR gandalf.gondor.pt.
253 IN PTR ns.gondor.pt.
253 IN PTR mail.gondor.pt.
246 IN PTR ns2.gondor.pt.
246 IN PTR saruman.gondor.pt.
151 IN PTR ap1.gondor.pt.
152 IN PTR ap2.gondor.pt.
153 IN PTR ap4.gondor.pt.
154 IN PTR chromecast.gondor.pt.
245 IN PTR ap3.gondor.pt.
254 IN PTR gollum.gondor.pt.
251 IN PTR frodo.gondor.pt.
250 IN PTR aragorn.gondor.pt.
252 IN PTR nazgul.gondor.pt.
247 IN PTR ippin.gondor.pt.
248 IN PTR meo1.gondor.pt.
249 IN PTR meo2.gondor.pt.

; Clientes DHCP da rede Gondor

1 IN PTR sauron-f.gondor.pt.
2 IN PTR sauron-w.gondor.pt.
3 IN PTR galadriel-f.gondor.pt.
4 IN PTR galadriel-w.gondor.pt.
5 IN PTR nexus4.gondor.pt.
6 IN PTR motog.gondor.pt.
```

Inversa

Resolução inversa

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

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

Non-authoritative answer:
Name:   webmail.isec.pt
Address: 193.137.78.90

> set q=ptr
> 193.137.78.90
Server: vodafonegw
Address: 192.168.1.1

Non-authoritative answer:
90.78.137.193.in-addr.arpa      name = webmail.isec.pt
90.78.137.193.in-addr.arpa      name = smtp.isec.pt

78.137.193.in-addr.arpa nameserver = ns.isec.pt
78.137.193.in-addr.arpa nameserver = ns2.isec.pt
ns.isec.pt          internet address = 193.137.78.1
ns2.isec.pt         internet address = 193.137.78.3
```

Direta

Inversa

Load Balancing

- Balanceamento de carga nesta perspetiva consiste em distribuir os clientes de um recurso (servidor ftp, www, mail, ...) pelos diversos fornecedores do recurso.
- Assume-se portanto uma replicação do mesmo recurso por vários sistemas da rede.
- Uma técnica comum (RFC 1794) de, com base no DNS, efetuar balanceamento de carga consiste em ordenar de maneira diferente (e.g. por **round-robin**) os registo do mesmo domínio, classe e tipo em cada resposta a um pedido de resolução.
- Para tornar efetiva esta técnica a tais registos associam-se em geral valores TTL reduzidos.

Load Balancing

- Pode fazer um balanceamento de cargas dos seus servidores utilizando o DNS para tal. Tem apenas que ter múltiplos registos A, para um nome.
- Por exemplo, se existirem três servidores WWW com os endereços 10.0.0.1, 10.0.0.2 e 10.0.0.3, um conjunto de registos tal como os que se seguem implica que os clientes se irão ligar um terço do tempo a cada máquina:

Name	TTL	CLASS	TYPE	Resource Record (RR) Data
www	600	IN	A	10.0.0.1
	600	IN	A	10.0.0.2
	600	IN	A	10.0.0.3

- Quando um *resolver* perguntar por estes registos, o DNS irá rodá-los e responder à pergunta com os registos em ordem diferente. No exemplo acima os clientes irão receber aleatoriamente os registos pela ordem 1, 2, 3; 2, 3, 1; e 3, 1, 2. Muitos clientes irão usar o primeiro registo e ignorar os restantes.

Segurança

- O DNS sempre foi, e pretende continuar a ser, um repositório de informação pública e portanto não é fornecido nenhum mecanismo de suporte à confidencialidade da informação que manipula e troca.
- Contudo, com o evoluir e massificação da sua utilização começou a ser vulnerável a ataques. Por isso foi pensado forma de lhe introduzir alguma segurança.
- Os primeiros passos foram dados com o Secure DNS:
 - RFC 2065 - January 1997 "*Domain Name System Security Extensions*"
- Mais tarde, na sequência da proposta de atualização dinâmica do DNS (RFC 2136), e com base no DNSSEC, foi apresentado o
 - RFC 2137 - April 1997 "*Secure Domain Name System Dynamic Update*"
- Em 1999 são redefinidas as extensões de segurança do DNS de forma mais abrangente em quatro documentos:
 - RFC 2535 - March 1999 "*Domain Name System Security Extensions*"
 - RFC 2536 - March 1999 "*DSA KEYS and SIGs in the DNS*"
 - RFC 2538 - March 1999 "*Storing Certificates in the DNS*"
 - RFC 2541 - March 1999 "*DNS Operational Security Considerations*"

Segurança

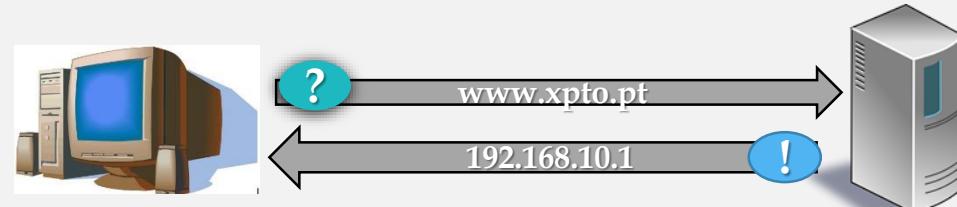
- O DNSSEC (*Domain Name System Security Extensions*) é o nome dado às extensões de segurança ao protocolo DNS concebidas para proteger e autenticar o seu tráfego.
- Os mecanismos de segurança previstos no DNSSEC são complementares e transparentes para o utilizador, não interferindo, desta forma, com o normal funcionamento do protocolo DNS.
- As extensões visam melhorar a confiabilidade dos utilizadores nos serviços prestados, nomeadamente:
 - Suprimir fragilidades;
 - Prevenir ataques;
 - Reduzir o risco de manipulação;
 - Prestar um serviço seguro;
 - Reforçar a segurança.
- Para que se obtenha total proveito deste serviço é necessário haver uma implementação do lado dos ISPs para que este serviço chegue ao cliente final.

Segurança

- As extensões de segurança assentam essencialmente nas tecnologias de criptografia de chave pública e em assinaturas digitais baseadas em chave pública.
- As extensões de segurança propostas no RFC 2535 consideram três serviços:
 - Distribuição de Chaves.
 - Autenticação da Origem dos Dados e Integridade.
 - Autenticação de Transações e Pedidos DNS.

Segurança - Ataque *man-in-the middle*

Situação Normal



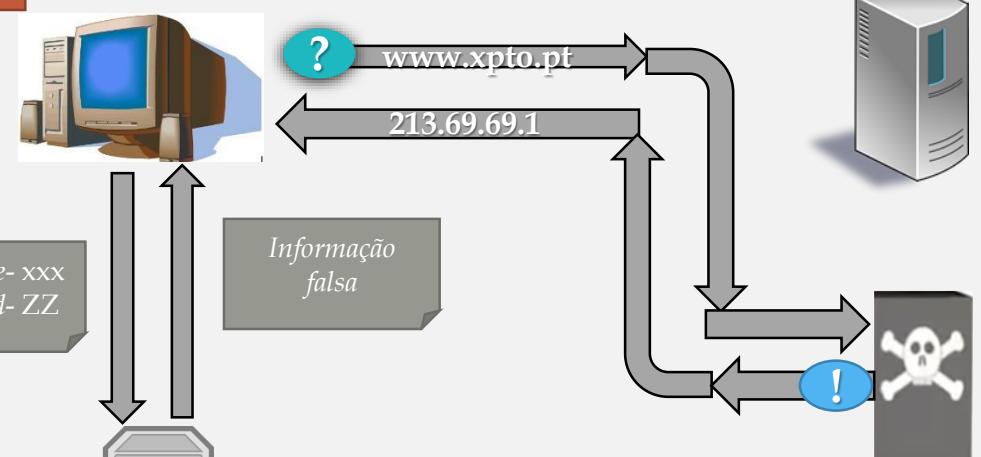
Username- xxx
Password- ZZ

Informação
bancária



Servidor Web do
banco XPTO
192.168.10.1

Ataque



Username- xxx
Password- ZZ

Informação
falsa



Servidor Web
Falso do banco
XPTO
213.69.69.1



Servidor Web do
banco XPTO

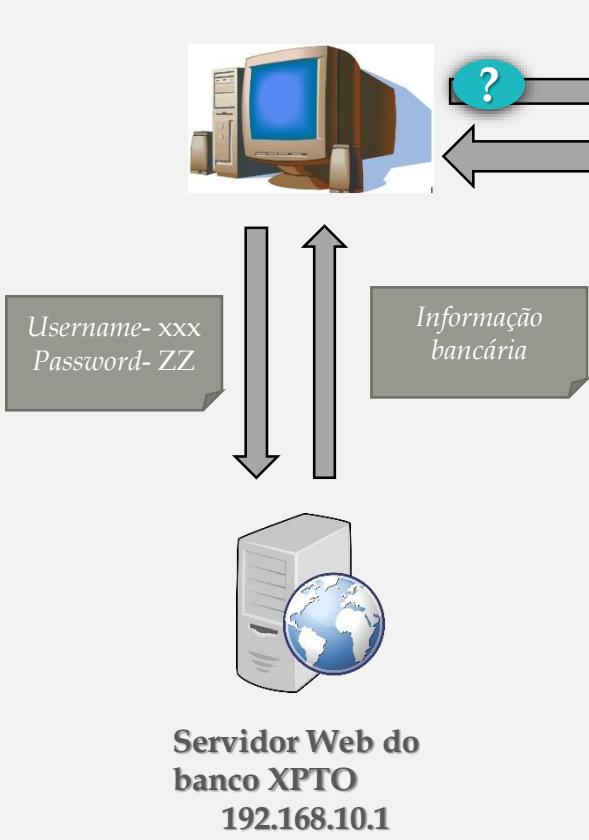
Username- xxx
Password- ZZ

Informação
bancária

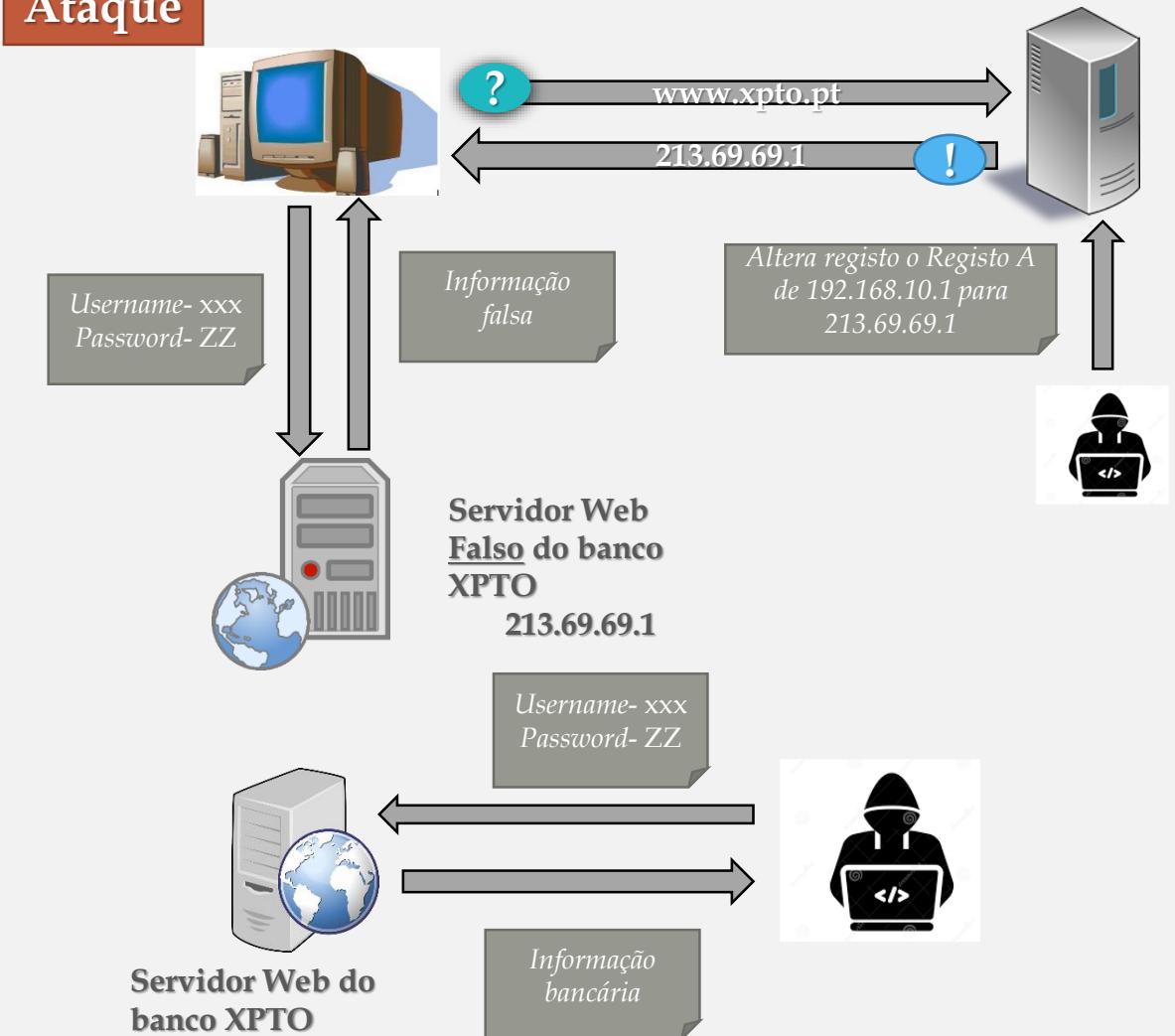


Segurança - Ataque *cache poisoning*

Situação Normal



Ataque



Segurança - A solução DNSSEC

Situação Normal



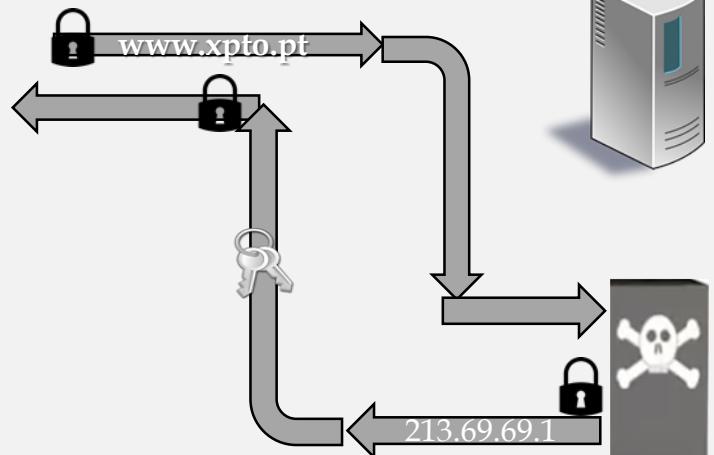
Username- xxx
Password- ZZ

Informação bancária



Servidor Web do
banco XPTO
192.168.10.1

Ataque



Username AAA
Password TT

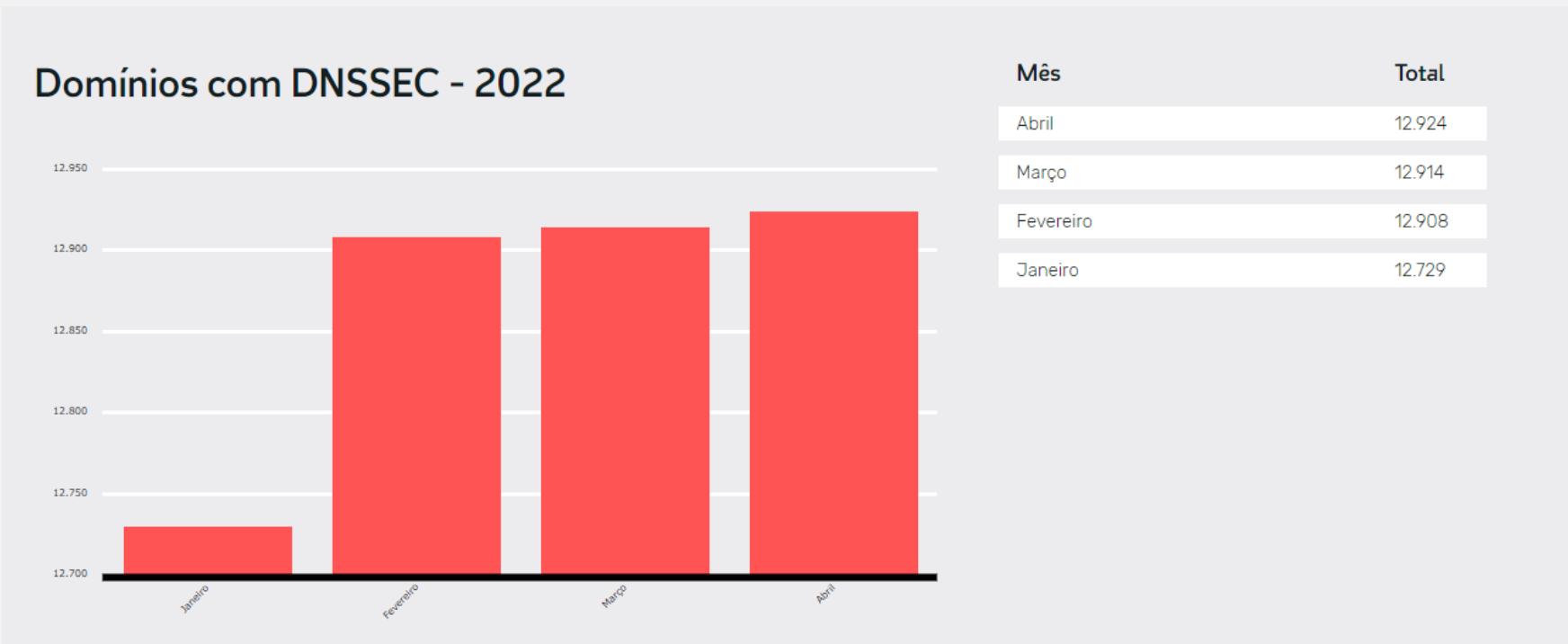


Servidor Web do
banco XPTO

Segurança

- O que garante?
 - Origem (Autenticidade).
 - Integridade.
- O que não garante?
 - Confidencialidade.
 - Proteção contra ataques de negação de serviço.

Segurança - Números em Portugal



Fonte: <https://www.dns.pt>

Segurança

- O DNSSEC introduz registos adicionais que se dividem em quatro tipos diferentes:
 - DNSKEY - Chave pública;
 - RRSIG - Assinatura Digital do RRset;
 - NSEC/NSEC3 - Resposta autenticada da não existência de um domínio ou conjunto de Resource Records associado a um domínio;
 - DS - Síntese da chave pública que faz a ligação entre um domínio e subdomínio de modo a construir uma cadeia de confiança;

Public DNS

- Quando a Google lançou no final do ano de 2009 o seu serviço público de DNS, este prometia ser o mais rápido, simples e robusto de utilizar.
- A ideia da empresa tornar a Internet ainda mais rápida, recorrendo a servidores distribuídos de DNS, mas que todos respondiam pelos mesmos endereços IP.
- Este projeto cresceu e atualmente é já um serviço maduro. É também já o serviço de DNS mais usado na Internet, processando por dia mais de 70 mil milhões de pedidos.



Public DNS

- Que vantagens:
 - Performance
 - Segurança
 - Taxa de acertos
- Pode ver mais detalhes deste serviço em
 - <https://developers.google.com/speed/public-dns/docs/intro>

Public DNS

GTEI DNS (agora Verizon)

4.2.2.1

4.2.2.2

4.2.2.3

4.2.2.4

4.2.2.5

4.2.2.6

Opennicproject

151.236.6.156

118.88.20.195

SafeDNS

195.46.39.39

195.46.39.40

OpenDNS

208.67.222.222

208.67.220.220

DynDNS

216.146.35.35

216.146.36.36

Comodo Secure DNS

8.26.56.26

8.20.247.20

Dnsadvantage

156.154.70.1

156.154.71.1

Atualizações dinâmicas

- O DNS é um serviço de diretoria que assume que a informação nas Zonas muda muito raramente.
- É, portanto, aceitável que o mecanismo de atualização dos ficheiros de Zona seja exterior ao próprio protocolo (geralmente por edição manual dos próprios ficheiros).
- Contudo, em ambientes com endereços dinâmicos (por exemplo: DHCP) torna-se útil um sistema de resolução de nomes que se atualize também dinamicamente.
- Estas atualizações podem ser requeridas pelos clientes ou por servidores de DHCP.
- Os serviços de DNS presentes nos sistemas operativos mais recentes permitem atualizações dinâmicas.

Atualizações dinâmicas

- O RFC 2136 define uma nova operação (opcode = UPDATE) que vai permitir:
 - adicionar ou eliminar RRs ou RRSets a uma zona específica
 - especificar pré-requisitos a verificar para efetivar tais operações de atualização:
 - a existência prévia (ou não) de um RRSet
 - a existência prévia (ou não) de uma RR específica
- A operação UPDATE apenas se verifica se todos os pré-requisitos forem verificados e nunca em paralelo com outra operação de UPDATE.

Atualizações dinâmicas

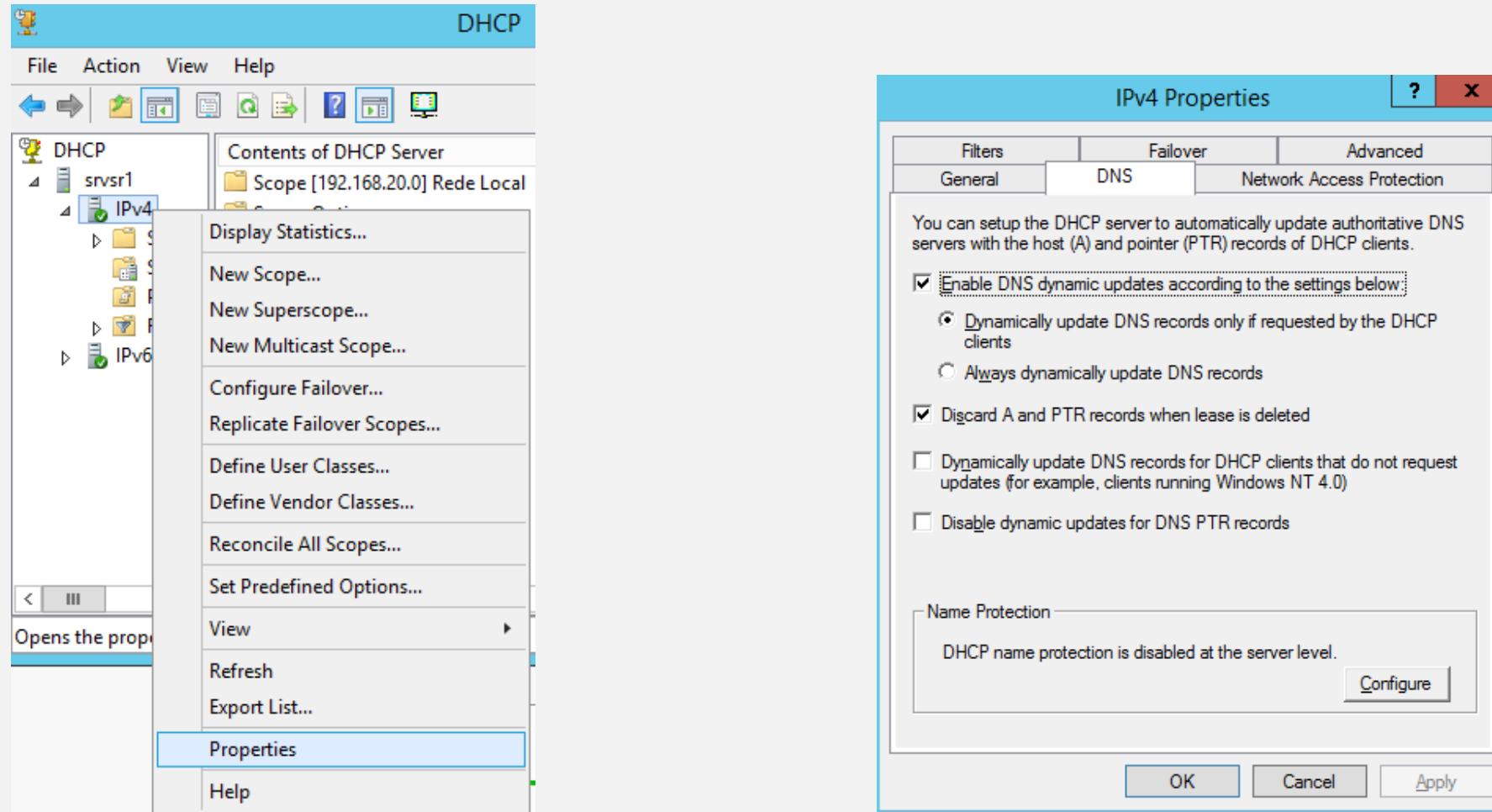
- Formato do pacote do UPDATE



Atualizações dinâmicas

- O requisitante de uma operação de UPDATE (e.g. servidor DHCP) deve tentar dirigir o pedido diretamente para o servidor primário da zona.
- Se por algum motivo tal for impossível deve contactar um dos restantes servidores autoritários da zona.
- Um servidor autoritário não primário ao receber um pedido de atualização deve reencaminhá-lo para o servidor primário assumindo o papel de requisitante da operação. Assim que receba a resposta deve retorná-la para o requisitante original.

Atualizações dinâmicas - DHCP - DNS



Dúvidas



Referências - Vídeos

- **Governação da Internet e domínios**
 - <https://youtu.be/GGhAXVKlUfo> - acedido em abril de 2022
- **Como funciona o DNS?**
 - <https://www.youtube.com/watch?v=ACGuo26MswI> - acedido em abril de 2022
- **A importância do DNS na sua rede?**
 - <https://www.youtube.com/watch?v=epWv0-eqRMw> - acedido em abril de 2022

Referências

- <https://www.iana.org/reports/2013/pt-report-20130808.html> - acedido em abril de 2020
- <https://www.profissionaisti.com.br/2018/04/cloudflare-dns-1-1-1-1-velocidade-e-privacidade-parte-16-o-que-e-dns/> - acedido em abril de 2020
- <https://www.hostnet.com.br/info/dns/> - acedido em abril de 2020.
- <http://paginas.fe.up.pt/~mgi97018/dns.html> - acedido em abril de 2020
- <http://www.dns.pt> - acedido em abril de 2021
- <http://docente.ifrn.edu.br/diegopereira/disciplinas/2012/redes-de-computadores-e-aplicacoes/aula-47-protocolo-dns/view> - acedido em abril de 2020
- “DNS” - Luís Santos - ISEC
- Material de suporte às aulas de Redes de Computadores de J. Legattheaux Martins DI - FCT/ UNL

Serviços de Rede 1

2022-2023

Pedro Miguel Geirinhas

Aula 9

NTP – Network Time Protocol

Agenda

- 1.** O Tempo
- 2.** Modos de operação
- 3.** Organização em camadas
- 4.** Protocolo – Relações
- 5.** Protocolo - Modos de Sincronismo
- 6.** O *datagrama*
- 7.** Funcionamento

O Tempo

- O tempo é o intervalo entre dois eventos, ou o momento indicado por um relógio.
- A unidade do Sistema Internacional de Unidades que mede o tempo é o **segundo**.
- Historicamente, o segundo era medido com base no dia solar médio ($1/86400$ do dia), mas a rotação da Terra é bastante imprecisa implicando assim um erro na medida da unidade.
- Em 1954, definiu-se o segundo com base na rotação da Terra em torno do Sol ($1/31.556.925,9747$ do tempo que levou a Terra a girar em torno do Sol à partir das 12h de 04/01/1900). Contudo, a rotação da Terra em torno do Sol também é imprecisa.
- Assim desde 1967, o segundo é definido com base na medição de relógios atómicos, como:
"O segundo é a duração de 9.192.631.770 períodos da radiação correspondente à transição entre dois níveis hiperfinos do estado fundamental do átomo de césio 133."

Tempo

- Uma característica básica e ao mesmo tempo importante do tempo é que ele avança sempre.
- O tempo não para e não volta para trás.
- Como vários programas de computador fazem uso dessa característica, o seu funcionamento pode estar comprometido se o relógio da máquina inesperadamente passar a indicar uma hora errada.
- Ainda pode ser mais complicado na Internet, com vários computadores a trocar informação. Imagine a confusão que se gerava se cada uma das maquina tivesse horas diferentes, não provocadas por estarem em diferentes fusos horários, mas sim por atrasos dos seus relógios.

Necessidade

- Porque temos necessidade de as máquinas terem o mesmo tempo?
 - Marcas temporais de segurança a associar em documentos e sua assinatura digital.
 - Comprovativo de entrega de documentação (*time stamp*).
 - Protocolos de segurança.
 - Analise de segurança (logs).
 - Autenticação.
 - Sistemas de marcação de eventos.
 - Controlo aéreo.
 - Detecções de intrusão.
 - Teleconferência e Videoconferência.
 - Jogos online.
 - Criptografia.
 - ...

Necessidade

- Outra boa definição para a necessidade é dada por Thomas Akin, no capítulo 10 do seu livro “*Hardening Cisco Routers*”:

Time is inherently important to the function of routers and networks. It provides the only frame of reference between all devices on the network. This makes synchronized time extremely important. Without synchronized time, accurately correlating information between devices becomes difficult, if not impossible. When it comes to security, if you cannot successfully compare logs between each of your routers and all your network servers, you will find it very hard to develop a reliable picture of an incident. Finally, even if you are able to put the pieces together, unsynchronized times, especially between log files, may give an attacker with a good attorney enough wiggle room to escape prosecution.



Network Time Protocol (NTP)

- O NTP é um protocolo para sincronização do relógio de um conjunto de computadores em redes de dados com latência variável baseado no protocolo UDP para sincronização do relógio.
- O NTP permite manter o relógio de um computador com a hora sempre certa e com grande exatidão.
- Originalmente idealizado por David L. Mills da Universidade do Delaware é ainda hoje mantido por si e por uma equipa de voluntários.
- Foi utilizado pela primeira vez em 1979, sendo ainda hoje muito popular.
- Usa o protocolo UTP e o porto 123.



Fonte:
https://en.wikipedia.org/wiki/File:DL_Mills-2.jpg

Network Time Protocol (NTP)

- Os servidores NTP permitem aos seus clientes a sincronização dos relógios dos equipamentos de rede a partir de uma referência padrão de tempo aceita mundialmente, conhecida como UTC (**Universal Time Coordinated**).
- Foi tendo varias atualizações e alterações ao longo do tempo:
 - 1979 - NTP V0 - RFC-958
 - 1998 - NTP v3 - RFC-1305

Network Time Protocol (NTP)

A versão actual, NTPv4, consiste na implementação dos seguintes RFCs:

- **RFC 5905**: Network Time Protocol Version 4: Protocol and Algorithms Specification
- **RFC 5906**: Network Time Protocol Version 4: Autokey Specification
- **RFC 5907**: Definitions of Managed Objects for Network Time Protocol Version 4 (NTPv4)
- **RFC 5908**: Network Time Protocol (NTP) Server Option for DHCPv6
- A tarefa é suportada por uma hierarquia de servidores de forma idêntica a outros serviços na Internet (recordar por exemplo o serviço DNS).
- São usados algoritmos para minimizar os problemas gerados com quebras de ligação, falha de servidores ou ataques ao serviço.

Network Time Protocol (NTP)

- Existem implementações mais simples do NTP mas que implicam uma menor precisão.
 - **Simple Network Time Protocol (SNTP)** - RFC 4330 - é uma implementação menos complexa do NTP que não exige o armazenamento do estado durante longos períodos de tempo. É usado em alguns sistemas embutidos e em aplicações onde a total funcionalidade do NTP não é necessária.
 - **Hora do Windows** - desde a versão do Windows 2000 que os sistemas operativos da Microsoft incluem o serviço de tempo (W32Time), que tem a capacidade de sincronizar o relógio do computador com um servidor NTP.
 - **Ntimed** - começou por ser implantado por Poul-Henning Kamp em 2014. É patrocinado pela Fundação Linux para substituir a versão original do NTP e pretende ser mais simples e mais segura que a original.
 - **Openntpd** - Em 2004, Henning Brauer apresentou o OpenNTPD, uma implementação com um maior foco nas necessidades genéricas do OpenBSD. Inclui ainda algumas melhorias na segurança do protocolo e continuam a ser compatível com servidores NTP existentes. A versão está disponível em vários repositórios de pacotes do Linux.

Network Time Protocol (NTP)

- O NTP não se baseia no princípio de sincronização das máquinas entre si, mas sim com base nos princípios de ter todas as máquinas chegar tão perto quanto possível para a hora correta: o **UTC**.
- A gestão dos fusos horários é da responsabilidade do sistema operativo e não do protocolo.
- Os clientes individuais correm um pequeno programa que consulta o servidor periodicamente para obter o tempo de referência (UTC).
- Estes procedimentos são realizados em intervalos de tempo definidos de modo a manter a precisão da sincronização requerida para a rede.
- As consultas aos servidores são realizadas:
 - Inicialmente a cada 64 s.
 - Em produção a cada 15-17 min.

Modos de operação

- A implementação do NTP baseada nos seguintes tipos de atores:
 - **Relógios de referência UTC**
 - Fonte de referência UTC, rigorosa, baseada em relógios atómicos, GPS, etc
 - **Servidor primário**
 - Servidor directamente sincronizado com uma fonte de relógio de referência UTC
 - **Servidor secundário**
 - Servidor intermediário que sincroniza o seu relógio a partir de um ou mais servidores.
 - Possui um ou mais clientes: servidores ou clientes finais.
 - **Cliente**
 - Efectua a sincronização do seu relógio a partir de um ou mais servidores.
 - Não fornece o serviço a outros equipamentos cliente.
 - Os servidores a utilizar pelo cliente podem ser configurados de forma explícita ou descobertos dinamicamente através da pacotes em *broadcast*.

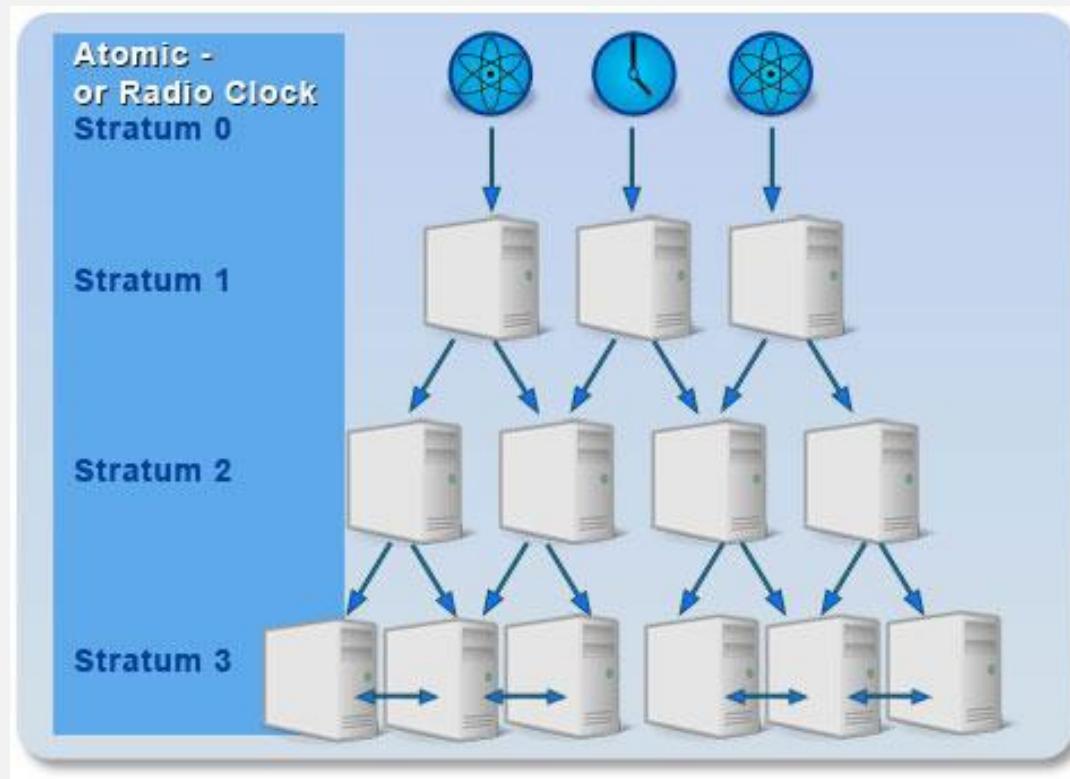
Organização em camadas

- Os servidores NTP formam uma topologia hierárquica, dividida em camadas ou *stratum* numerados de 0 (zero) a 16 (dezasseis).
- A camada 0 (*stratum 0*) na verdade não faz parte da rede de servidores NTP, mas representa a referência primária de tempo, que é geralmente um receptor do Sistema de Posicionamento Global (GPS) ou um relógio atómico. A camada 16 indica que um determinado servidor está inoperante.
 - *Stratum 0*
 - Relógios de referência (relógios atómicos, GPS, Galileo, ...)
 - *Stratum 1*
 - Servidores primários
 - *Stratum 2 .. N*
 - Servidores secundários
- O valor do *stratum* é calculado tendo por base o número de saltos (*hops*) desde a raiz até ao servidor que estamos a identificar.

Organização em camadas

- Qualquer servidor NTP que tenha como referência de tempo um servidor *stratum 1* passa a ser um *stratum 2*, qualquer servidor NTP que tenha como referência de tempo um servidor *stratum 2* passa a ser um *stratum 3*, e assim por diante.
- Quanto mais elevado for o *stratum* maior será a probabilidade de erro do relógio.
- Contudo, o aumento do erro entre *stratum* não é muito significativa.
 - É melhor estar ligado de forma correta ao *stratum 2* do que mal a um *stratum 1*.
- Do ponto de vista da administração de redes, a utilização do NTP é muito vantajosa, pois possibilita a sincronização automática de todos os equipamentos ligados à rede. Ou seja, o administrador não precisa ir de máquina em máquina para acertar o relógio local.

Organização em camadas



Fonte - <https://www.meinberg.co.uk/support/information/ntp-the-network-time-protocol.htm> - acedido em maio de 2021

Organização em camadas

Lista de servidores de *Stratum 1*

<http://support.ntp.org/bin/view/Servers/StratumOneTimeServers>

Lista de servidores de *Stratum 2*

<http://support.ntp.org/bin/view/Servers/StratumTwoTimeServers>



PL 05-850 Ożarów Mazowiecki, Polska (OVH Datacenter Warsaw)	Poland/Europe	OpenAccess	No	30 Sep 2022 - 16:35
PL 04-870 Warszawa, Polska (JAK Sp. z o.o. HQ, Vectra/VirtuaOperator fiber network).	Poland/Europe	OpenAccess	No	24 Mar 2019 - 19:05
PL 04-957 Warszawa, Polska (Orange network, UMTS & VDSL connection)	Poland/Europe	OpenAccess	No	20 Dec 2019 - 22:24
PL Warsaw, Poland	Poland, Europe	OpenAccess	Yes	26 Oct 2019 - 12:49
PL Europe	Poland	OpenAccess	Yes	03 Mar 2020 - 07:36
PT Lisboa, Portugal	Portugal/Europe	OpenAccess	No	30 Sep 2022 - 16:36
PT Lisboa, Portugal	Portugal/Europe	OpenAccess	Yes	04 Jul 2020 - 18:03
PY Asunción	Paraguay	OpenAccess	No	30 Sep 2022 - 16:37

ServerForm edit	
ServerStratum	StratumTwo
CountryCode	PT
Hostname	ntp2.insilicols.pt
IP Address	164.90.186.211
IPv6 Address	2a03:b0c0:3:f0::5d:6000
UseDNS	Yes
PoolMember	No
ServerLocation	Lisboa, Portugal
HostOrganization	INSILICO LABS (www.insilicols.pt)
GeographicCoordinates	
ServerSynchronization	Private StratumOne servers sync by PPS from atomic clocks
ServiceArea	Portugal/Europe
AccessPolicy	OpenAccess
AccessDetails	
NotificationMessage	Yes
AutoKeyURL	
SymmetricKeyType	
SymmetricKeyURL	
ServerContact	Eduardo Miranda (timekeeper@insilicols.pt)

Em Portugal

- O Observatório Astronómico de Lisboa (<http://www.oal.ul.pt/>) foi fundado no dia 11 de Março de 1861.
- Desenvolveu competências em trabalhos de Astrometria no séc. XIX e parte do séc. XX, que lhe granjearam fama internacional.
- O OAL é a instituição que tem a incumbência legal de manter e distribuir a Hora Legal em Portugal.
- OAL está equipado com diversos relógios atómicos que se mantêm sincronizados com o padrão mundial da hora UTC e possui diversos servidores que a disponibilizam segundo o protocolo NTP
- Atualmente, o OAL dirige a Comissão Permanente da Hora, desenvolve e apoia atividades de investigação científica em Astrofísica, de divulgação e formação, no estudo e preservação do excelente acervo patrimonial, além de manter um serviço público nas suas áreas de intervenção.



Em Portugal

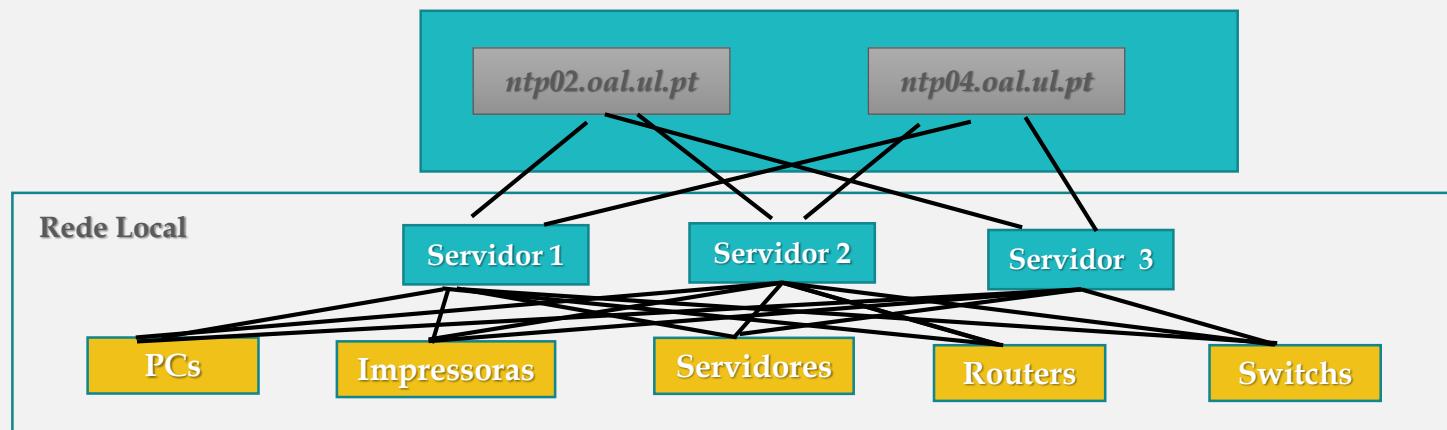
- Os endereços dos servidores NTP do Observatório Astronómico de Lisboa que mantêm o UTC são:
 - *ntp02.oal.ul.pt* e *ntp04.oal.ul.pt*.



- Pode em <http://oal.ul.pt/hora-legal/hora-legal-oal/> ver como ativar o surgimento da hora oficial num site e num cliente.

A minha topologia

- Se a sua rede for pequena pode configurar os seus equipamentos para se atualizarem diretamente num dos servidores NTP do Observatório Astronómico de Lisboa.
- Se a sua rede tiver alguma dimensão, deve ter 2 ou 3 servidores internos a proceder a sua atualização nos servidores externos e os seus clientes de rede a utilizá-los como os seus servidores NTP.



Protocolo - Relações

- As relações entre os diferentes dispositivos NTP são normalmente chamadas de associações. Estas podem ser:
 - **Permanentes:** são criadas por uma configuração ou comando e mantidas de forma permanente.
 - **Priorizáveis :** são específicas da versão 4 do NTP e são criadas por uma configuração ou comando, podendo ser desfeitas no caso de haver um servidor melhor, ou depois de um certo tempo.
 - **Efêmeras ou transitórias:** são criadas por solicitação de outro dispositivo NTP e podem ser desfeitas em caso de erro ou depois de um certo tempo.

Protocolo - Modos de Sincronismo

- Modo “*client/server*”
 - É uma associação permanente e a forma mais comum de configuração.
 - Um dispositivo faz o papel de cliente, solicitando informações sobre o tempo a um servidor. O cliente tem conhecimento das associações com os servidores e do estado da troca de pacotes.
 - Outro dispositivo faz o papel de servidor, respondendo à solicitação do cliente com informações sobre o tempo. O servidor não armazena informações sobre o diálogo com o cliente ou sobre sua associação com o mesmo.
 - No processo o cliente envia um pacote ao servidor e aguarda a resposta. Isso pode ser descrito também como uma operação do tipo pull, dizendo que o cliente busca os dados necessários sobre o tempo no servidor.
 - Um cliente pode criar associações com vários servidores simultaneamente (na verdade é recomendável que seja assim), e um servidor pode fornecer tempo simultaneamente a diversos clientes.
 - Um dispositivo (host) NTP pode ser cliente e servidor ao mesmo tempo.

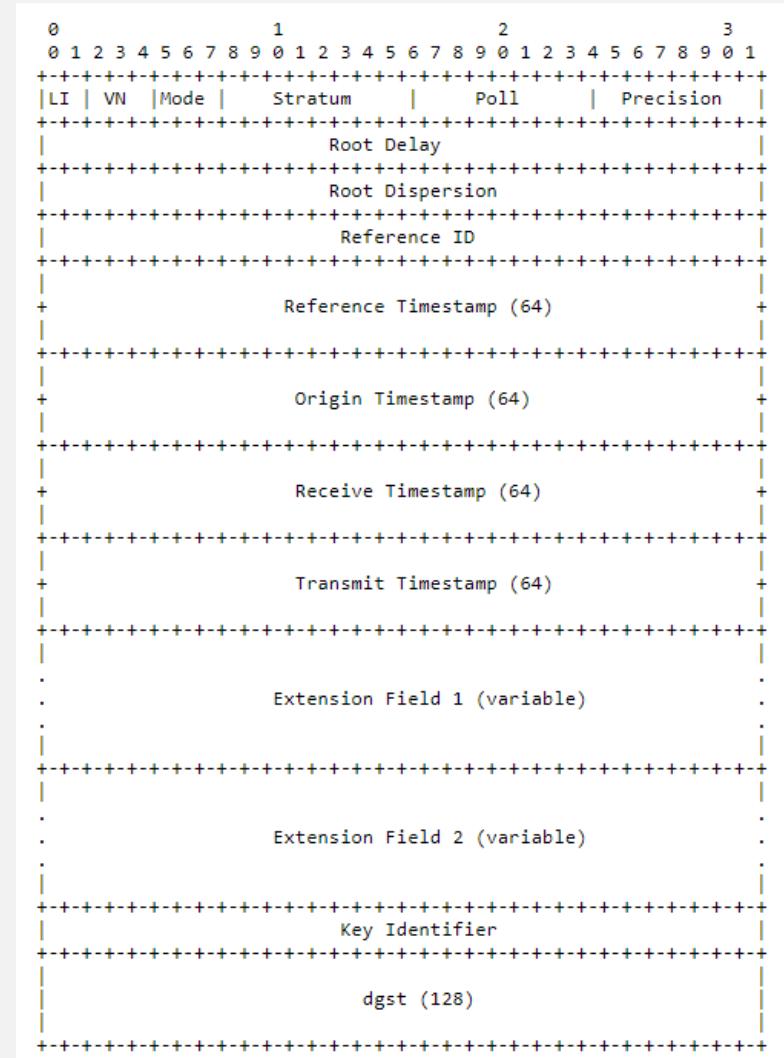
Protocolo - Modos de Sincronismo

- Modo “***symmetric***”
 - Dois ou mais dispositivos NTP podem ser configurados como pares (peers), de forma que possam tanto procurar o tempo, quanto fornecê-lo, garantindo redundância mútua.
 - Essa configuração faz sentido para dispositivos no mesmo *stratum*, configurados também como clientes de um ou mais servidores. Caso um dos pares perca a referência de seus servidores, os demais pares podem funcionar como referência de tempo.
 - O modo simétrico pode ser:
 - **Ativo:** O dispositivo A configura o dispositivo B como seu par (criando dessa forma uma associação permanente). Por sua vez, o dispositivo B também configura o dispositivo A como seu par (também cria uma associação permanente).
 - **Passivo:** O dispositivo A configura o dispositivo B como seu par (modo simétrico ativo). Mas o dispositivo B não tem o dispositivo A na sua lista de servidores ou pares. Ainda assim, ao receber um pacote de A, o dispositivo B cria uma associação transitória, de forma a poder fornecer ou receber o tempo de A. Esse modo é particularmente suscetível a ataques, onde um dispositivo intruso pode estar configurado no modo simétrico ativo e fornecer informações de tempo falsas para outro. Por isso deve sempre ser usado com criptografia.

Protocolo - Modos de Sincronismo

- Modo “**broadcast**”
 - NTP pode fazer uso de pacotes do tipo *broadcast* ou *multicast* para enviar ou receber informações de tempo.
 - Esse tipo de configuração pode ser vantajosa no caso de redes locais com poucos servidores alimentando assim uma grande quantidade de clientes.
 - O cliente NTP ao receber o primeiro pacote de um servidor, procura os dados por um curto período de tempo, como se estivesse no modo cliente - servidor, a fim de conhecer o atraso envolvido. Ou seja, durante alguns instantes há troca de pacotes entre cliente e servidor, depois disso o cliente passa apenas a receber os pacotes *broadcast* ou *multicast* enviados para a rede pelo servidor.
 - Tal como no caso do modo simétrico passivo, também se coloca aqui uma questão de segurança, porque um intruso pode facilmente enviar pacotes NTP falsos em modo broadcast. Assim a autenticação deve sempre estar habilitada.

Cabeçalho



Cabeçalho

- **LI (Leap Indicator)** - 2 bits - Indicador de salto

Value	Meaning
0	no warning
1	last minute of the day has 61 seconds
2	last minute of the day has 59 seconds
3	unknown (clock unsynchronized)

- **VN (Version Number)** - 3 bits - Número da versão
 - Atualmente versão 4

- **Mode** - 3 bits - Modo
 - Modos de associação entre os sistemas

Value	Meaning
0	reserved
1	symmetric active
2	symmetric passive
3	client
4	server
5	broadcast
6	NTP control message
7	reserved for private use

Cabeçalho

- **Stratum** – 8 bits - Nº do Stratum

Value	Meaning
0	unspecified or invalid
1	primary server (e.g., equipped with a GPS receiver)
2-15	secondary server (via NTP)
16	unsynchronized
17-255	reserved

- **Poll** – 8 bits- Máximo intervalo entre mensagens em Log2 (segundos)
- **Precision** – 8 bits - Precisão do relógio em Log2 (segundos)

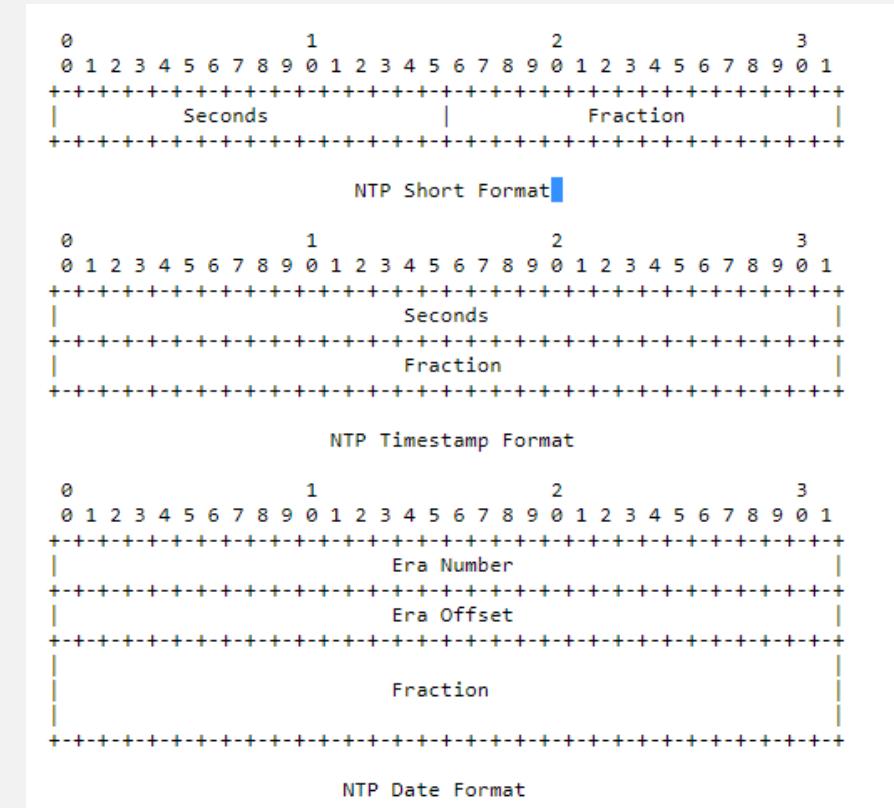
Cabeçalho

- **Root Delay** – 32 bits
 - Atraso do *round-trip* para o relógio de referência.
 - São actualizados/acumulados à medida que aumenta o *stratum*
- **Root Dispersion** – 32 bits
 - “dispersão” (erro) para o relógio de referência
 - São actualizados/acumulados à medida que aumenta o *stratum*
- **Reference ID** – 32 bits
 - Identificador do servidor ou relógio de referência para o *stratum 0*.

ID	Clock Source
GOES	Geosynchronous Orbit Environment Satellite
GPS	Global Positioning System
GAL	Galileo Positioning System
PPS	Generic pulse-per-second
IRIG	Inter-Range Instrumentation Group
WWVB	LF Radio WWVB Ft. Collins, CO 60 kHz
DCF	LF Radio DCF77 Mainflingen, DE 77.5 kHz
HBG	LF Radio HBG Prangins, HB 75 kHz
MSF	LF Radio MSF Anthorn, UK 60 kHz
JY	LF Radio JY Fukushima, JP 40 kHz, Saga, JP 60 kHz
LORC	MF Radio LORAN C station, 100 kHz
TDF	MF Radio Allouis, FR 162 kHz
CHU	HF Radio CHU Ottawa, Ontario
WWV	HF Radio WWV Ft. Collins, CO
WWVH	HF Radio WWVH Kauai, HI
NIST	NIST telephone modem
ACTS	NIST telephone modem
USNO	USNO telephone modem
PTB	European telephone modem

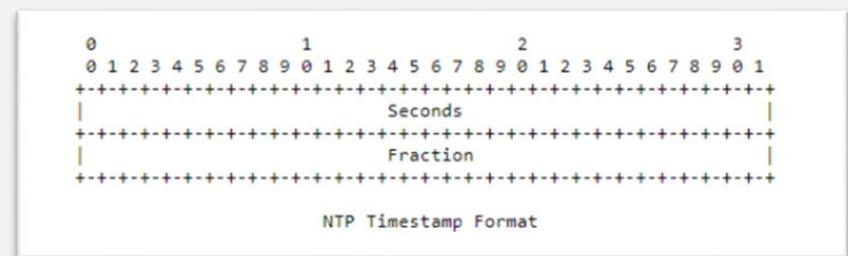
Tipo de Dados

- O formato da data de 128 bits é usado onde o armazenamento e tamanho de palavra são suficientes e estão disponíveis.
- Inclui um campo de segundos assinados de 64 bits, abrangendo 584 bilhões de anos e um campo de fração de 64 bits, resolvendo 0,05 attosegundos (isto é, $0,5e^{-18}$).



Timestamps

- São usados 64 bits para representar uma marca temporal (data/hora)
 - 32 bits representam os segundos
 - Suporta intervalos de 136 anos
 - Para suportar a representação de mais anos recorre-se ao conceito de Era
 - 32 bits representam frações de segundo com uma resolução de 232 picosegundos



Timestamps

- Para converter a hora do sistema em qualquer formato NTP tem de ser calculado o número de segundos (s) desde a época zero (00:00 01-01-1900) até à hora atual do sistema.

- Para determinar a era e o *timestamp* dado o s, deve fazer:

$$\text{era} = s / 2^{32} \text{ e } \text{timestamp} = s - \text{era} * 2^{32}$$

- Para determinar o s sabendo a era e o *timestamp* deve fazer:

$$s = \text{era} * 2^{32} + \text{timestamp}$$

Date	MJD	NTP Era	NTP Timestamp Era Offset	Epoch
1 Jan -4712	-2,400,001	-49	1,795,583,104	1st day Julian
1 Jan -1	-679,306	-14	139,775,744	2 BCE
1 Jan 0	-678,491	-14	171,311,744	1 BCE
1 Jan 1	-678,575	-14	202,939,144	1 CE
4 Oct 1582	-100,851	-3	2,873,647,488	Last day Julian
15 Oct 1582	-100,840	-3	2,874,597,888	First day Gregorian
31 Dec 1899	15019	-1	4,294,880,896	Last day NTP Era -1
1 Jan 1900	15020	0	0	First day NTP Era 0
1 Jan 1970	40,587	0	2,208,988,800	First day UNIX
1 Jan 1972	41,317	0	2,272,060,800	First day UTC
31 Dec 1999	51,543	0	3,155,587,200	Last day 20th Century
8 Feb 2036	64,731	1	63,104	First day NTP Era 1

Cabeçalho

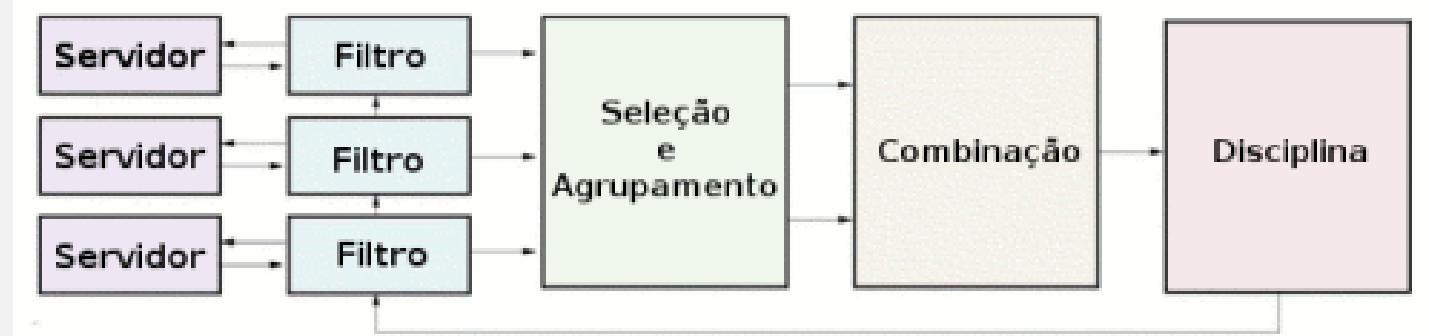
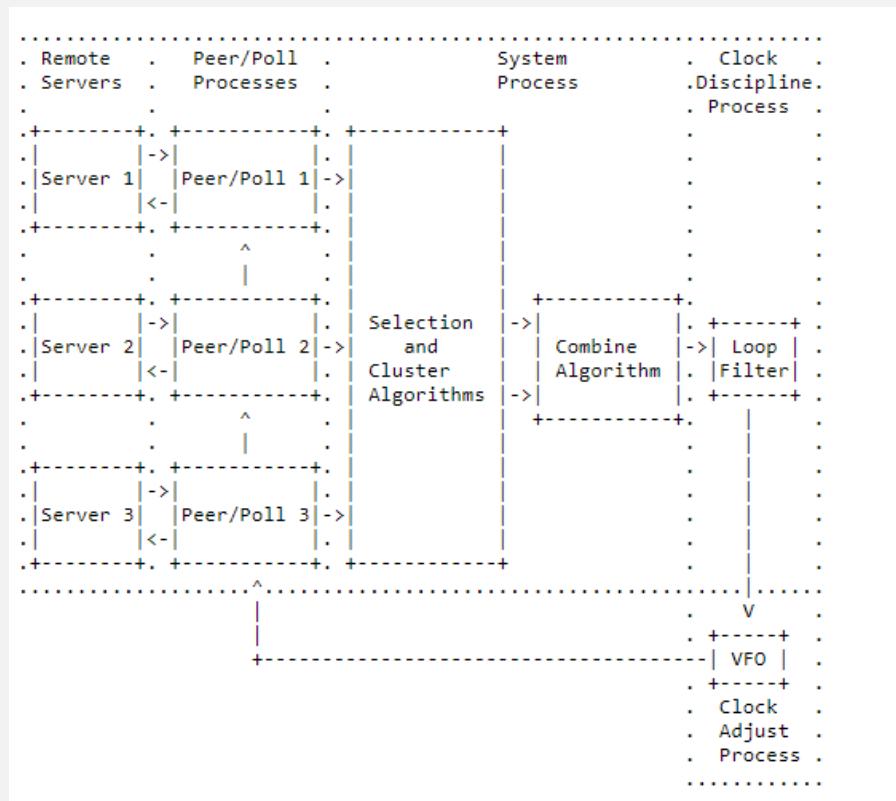
- **Reference Timestamp** – 64 bits
 - Hora em que o relógio do sistema foi ajustado pela última vez ou corrigido, no formato de carimbo de data / hora NTP.
- **Origin Timestamp** – 64 bits
 - Hora no cliente em que a solicitação partiu para o servidor, no formato de carimbo de data / hora NTP.
- **Receive Timestamp** – 64 bits
 - Hora no servidor em que a solicitação chegou do cliente, no formato de carimbo de data / hora NTP.
- **Transmit Timestamp** – 64 bits
 - Hora no servidor em que a resposta foi enviada para o cliente, no formato de carimbo de data / hora NTP.
- **Destination Timestamp** – 64 bits
 - Hora no cliente em que a resposta chegou do servidor, no formato de carimbo de data / hora NTP.

Parâmetros Globais

- O RFC 5905 define para o NTP versão 4 os seguintes parâmetros globais:

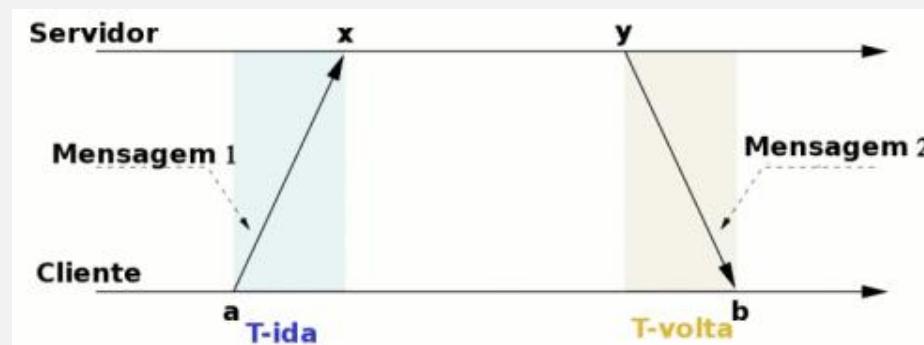
Name	Value	Description
PORT	123	NTP port number
VERSION	4	NTP version number
TOLERANCE	15e-6	frequency tolerance PHI (s/s)
MINPOLL	4	minimum poll exponent (16 s)
MAXPOLL	17	maximum poll exponent (36 h)
MAXDISP	16	maximum dispersion (16 s)
MINDISP	.005	minimum dispersion increment (s)
MAXDIST	1	distance threshold (1 s)
MAXSTRAT	16	maximum stratum number

Funcionamento



Funcionamento - *Remote Server*

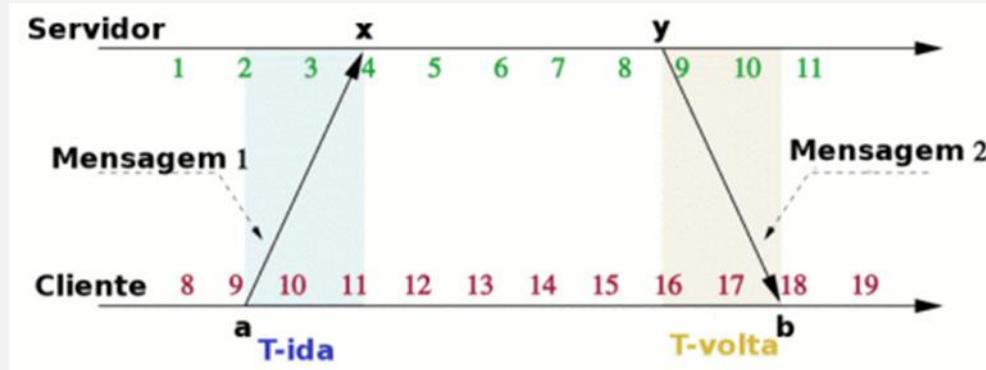
- Consideremos servidor e cliente com relógios não sincronizados. A troca de mensagens é a seguinte:
 - O **Cliente** lê seu relógio, que fornece o tempo **a**.
 - O **Cliente** envia a **Mensagem 1** com a informação de tempo **a** para o servidor.
 - O **Servidor** recebe a **Mensagem 1** e nesse instante lê seu relógio, que fornece o instante **x**.
 - O **Servidor** após algum tempo lê novamente seu relógio, que fornece o instante **y**.
 - O **Servidor** envia a **Mensagem 2** com **a**, **x** e **y** para o cliente.
 - O **Cliente** recebe a **Mensagem 2** e nesse instante lê seu relógio, que fornece o instante **b**.



Funcionamento - *Remote Server*

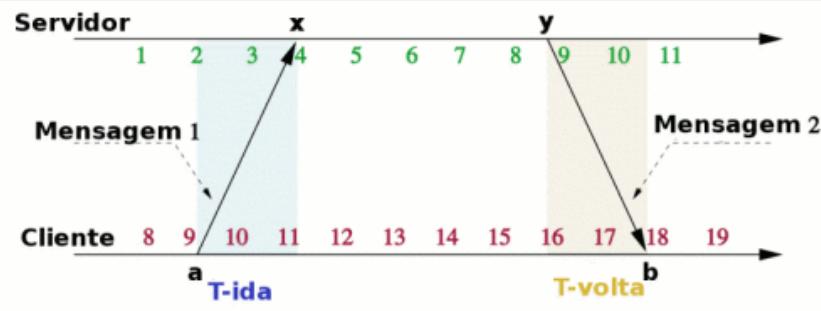
- Ao receber a **Mensagem 2**, o **Cliente** passa a conhecer os instantes **a**, **x**, **y** e **b**. Mas **a** e **b** estão numa escala de tempo, enquanto **x** e **y** em outra. O valor do incremento dessas escalas é o mesmo, mas os relógios não estão sincronizados.
- Não é possível, calcular o tempo que a **Mensagem 1** levou para ser transmitida (T_{ida}), nem o tempo que a **Mensagem 2** gastou na rede (T_{volta}). Contudo, o **tempo total** de ida e volta, ou **atraso** (também conhecido por *Round Trip Time* ou *RTT*) que é a soma $T_{ida} + T_{volta}$ pode ser calculado como:
- **atraso (RTT)** = $(b-a)-(y-x)$.
- Considerando-se que o **tempo de ida é igual ao tempo de volta**, pode-se calcular o deslocamento entre o servidor e o relógio local como:
- **deslocamento (offset)** = $x - (a + \text{atraso}/2) =$
deslocamento (offset) = $1/2 * [(x-a)+(y-b)]$.

Funcionamento - *Remote Server* - Exemplo



- O Cliente lê o relógio: $a=9$.
- O Cliente envia a Mensagem 1 ($a=9$).
- O Servidor recebe a Mensagem 1 ($a=9$) e lê seu relógio: $x=4$.
- O Servidor algum tempo depois lê seu relógio novamente: $y=9$.
- O Servidor envia a Mensagem 2 ($a=9, x=4, y=9$).
- O Cliente recebe a Mensagem 2 ($a=9, x=4, y=9$) e lê seu relógio: $b=18$.

Funcionamento - *Remote Server* - Exemplo

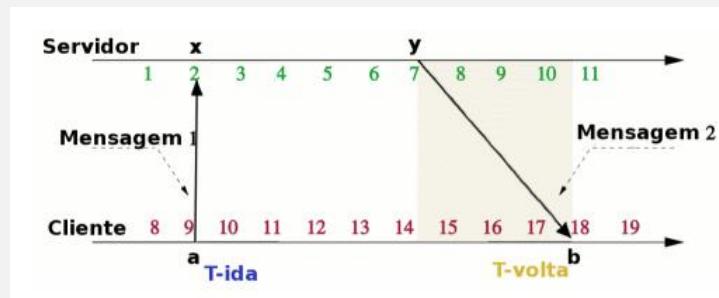


- É fácil observar que $T_{ida}=2$ e $T_{volta}=2$. Contudo, nem o **Cliente** nem o **Servidor** têm essa visão.
- O **Servidor** ao final da troca de mensagens descarta todas as informações sobre a mesma.
- O **Cliente** conhece as variáveis $a=9$, $x=4$, $y=9$ e $b=18$, mas com delas é impossível calcular T_{ida} ou T_{volta} .
- Contudo, é possível calcular o deslocamento:
$$\text{deslocamento} = \frac{1}{2} * [(x-a)+(y-b)] = \frac{1}{2} * [(4-9)+(9-18)] = -14/2 = -7.$$
- Um deslocamento de -7 significa que o relógio local do **Cliente** deve ser **atrasado 7 unidades de tempo** para se igualar ao do **Servidor**.

Funcionamento - *Remote Server* - Exemplo

- No exemplo anterior, consideramos que T_{ida} é igual ao T_{volta}
- Mas isso nem sempre é verdade! Há atrasos aleatórios nas redes devido às filas de espera dos routers e switchs. Numa WAN ou na Internet as ligações a diferentes velocidades e rotas assimétricas, tráfego além de outros fatores, também causam diferenças entre estes dois tempos.
- No entanto, o NTP funciona exatamente dessa forma, considerando sempre que T_{ida} é igual ao T_{volta} .
- E isso implica em erro...

Funcionamento - *Remote Server* - Exemplo



$$\text{atraso} = (b-a)-(y-x) = (18-9)-(7-2) = 9 - 5 = 4.$$

$$\text{deslocamento} = (x-a+y-b)/2 = (2-9+7-18)/2 = -18/2 = -9.$$

- O deslocamento está errado! Sabe-se que o valor correto é -7., contudo o valor calculado é -9. Isso deve-se a ao erro introduzido pela rede e que implica que o $T_{\text{id}}a$ e T_{volta} não sejam iguais.

- No entanto, à partir do cálculo do deslocamento e do atraso, e levando em conta a limitação do método, que considera $T_{\text{id}}a = T_{\text{volta}}$, sabe-se que o deslocamento verdadeiro está entre:

$$\text{deslocamento} - \text{atraso}/2 \leq \text{deslocamento verdadeiro} \leq \text{deslocamento} + \text{atraso}/2$$

$$-9 - 2 \leq \text{deslocamento verdadeiro} \leq -9 + 2$$

$$-11 \leq \text{deslocamento verdadeiro} \leq -7$$

- Ou seja, dado um deslocamento de -9 e um atraso de 4, sabe-se que o valor verdadeiro do deslocamento é algo entre -11 e -7, mas não há como ter certeza de qual o valor..

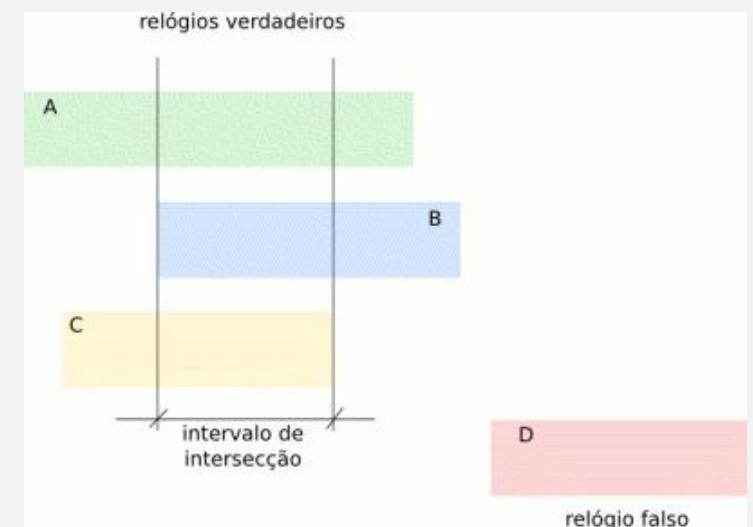
Funcionamento - Peer/Poll

- Através da troca de mensagens, o NTP consegue as informações de atraso e deslocamento de um servidor. Essa troca de mensagens não é realizada uma única vez, sendo que se repete periodicamente, num intervalo de tempo controlado pelo protocolo.
- No início da sincronização o cliente NTP faz uma consulta a cada servidor a cada 64s. Esse período varia ao longo do tempo, geralmente aumenta, até chegar a 1024s.
- Na realidade cada amostra é composta de 4 valores: atraso, deslocamento, dispersão e *timestamp*. O *timestamp* indica quando a amostra chegou e a dispersão é o erro estimado do relógio de servidor remoto, informada pelo servidor na mensagem NTP.
- A lista com os valores é ordenada em função do atraso. Considerando-se que as amostras com menor atraso são melhores porque provavelmente não se sujeitaram a filas de espera nos equipamentos de telecomunicações e assim estão mais próximas de garantir que o T_{ida} é igual ao T_{volta}
- Os valores mais antigos são descartados, porque o valor de deslocamento pode já não corresponder à realidade, já que a exatidão do relógio local varia ao longo do tempo e das condições da rede.
- Após descartar as amostras antigas, resta uma lista com as amostras mais recentes e ordenadas em função do atraso. Da primeira entrada dessa lista são retiradas o atraso e deslocamento para o par cliente-servidor (note-se que para cada par cliente - servidor há uma variável de cada tipo).

Funcionamento - *Selection and Cluster*

- Após na fase anterior se ter calculado os principais parâmetros referentes a cada um dos servidores é agora importante descobrir quais deles são confiáveis e quais não são.
- Os servidores que têm algum erro no tempo fornecido são chamados de **relógios falsos**.
- Os servidores que fornecem a hora corretamente são chamados de **relógios verdadeiros**.
- Para a seleção dos relógios, o NTP considera como verdadeiro o deslocamento que se encontra dentro de um determinado intervalo de confiança, calculado como:

intervalo de confiança = (deslocamento/2) + dispersão.

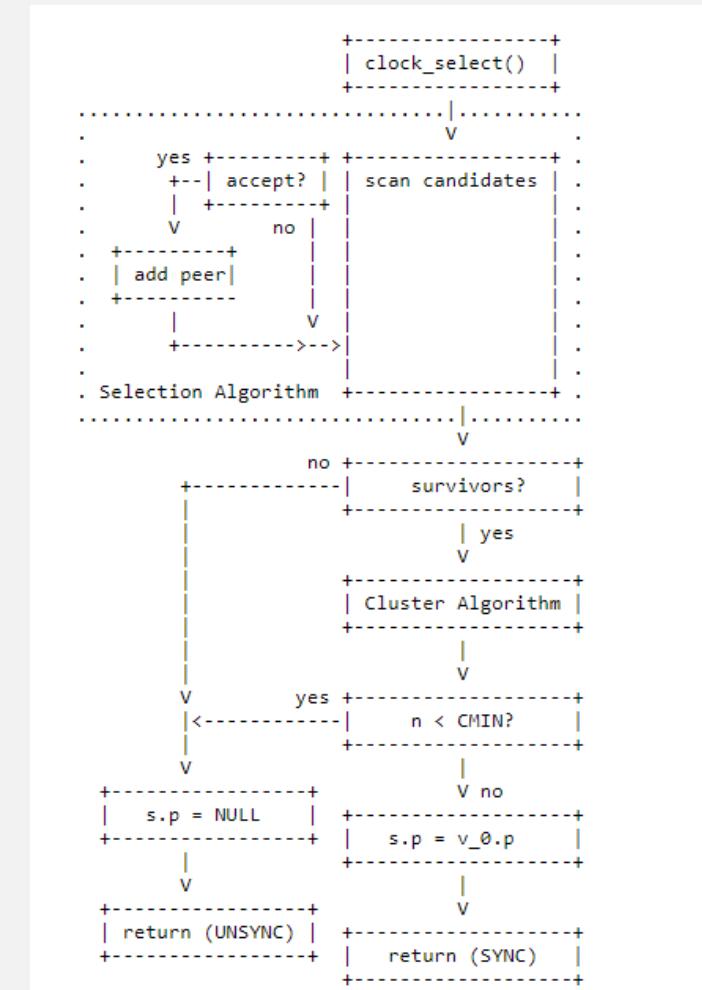


Funcionamento - *Selection and Cluster*

- Após terem sido escolhidos os relógios verdadeiros são utilizadas técnicas estatísticas, com o objetivo de selecionar os melhores.
- Os critérios de seleção utilizados são:
 - *Stratum*.
 - distância para a raiz.
 - variação (jitter).
- No processo alguns servidores são descartados, sendo chamados de relógios afastados.
- Os que permanecem são chamados de relógios sobreviventes.
- O melhor dos relógios sobreviventes é considerado como par do sistema (*system peer*).

Funcionamento - *Combine*

- Se o *system peer* for determinado pelo algoritmo da fase anterior já não entra nesta etapa.
- Para os outros casos em que há mais do que um sobrevivente e nenhum deles foi configurado como *system peer* é calcula uma média ponderada dos deslocamentos dos relógios, com o objetivo de aumentar a exatidão.



Funcionamento - *Discipline*

- O processo controla a fase e a frequência do relógio do sistema.
- O controle baseado na fase é melhor para as ocasiões onde há uma grande variação (*jitter*). Essa abordagem procura minimizar o erro no tempo, controlando indiretamente a frequência.
- O controle baseado na frequência é melhor para quando há instabilidades na frequência. A abordagem controla diretamente a frequência, e indiretamente o erro no tempo.
- O NTP disciplina o relógio local de forma contínua, mesmo em períodos onde não é possível consultar servidores de tempo.
- Assim:
 - São sempre que possível evitados saltos no tempo. O tempo é ajustado de uma forma gradual com a variação da frequência local do relógio.
 - Se a diferença for maior do que 128ms o NTP só proceder ao acerto do relógio se a mesma persistir por um período maior que 900s (15min).
 - Se a diferença for maior que 1000s (~16,7min) o algoritmo aborta a sua execução, considerando que algo muito errado aconteceu. As diferenças dessa ordem ou maiores devem ser corrigidas manualmente antes de se executar novamente a consulta NTP.

Segurança

- Em qualquer serviço de telecomunicações devemos garantir o seguintes aspetos no que diz respeito à informação:
 - integridade,
 - disponibilidade,
 - autenticidade;
 - confidencialidade.
- Os algoritmos vistos anteriormente, aliados à correta configuração do sistema, com um número suficiente de fontes de tempo com referências primárias independentes, garantem de forma satisfatória a integridade e disponibilidade do serviço.
- Os algoritmos de criptografia visam garantir a autenticidade da informação. Ou seja, têm o objetivo de assegurar ao cliente de que o servidor é quem ele diz ser.
- A confidencialidade não é considerada um problema no contexto do NTP. Ou seja, a informação de tempo irá “andar” na rede de forma aberta.
- As razões principais para o NTP funcionar dessa forma são:
 - o tempo é uma informação pública, não há razão para o esconder;
 - encriptar a informação iria introduzir complexidade e tempo de processamento tanto no servidor como no cliente o que iria degradar o desempenho do sistema, fazendo-o menos exato.

Segurança

- Existem basicamente dois métodos no NTP para realizar a autenticação:
 - chave simétrica (*symmetric key*)
 - chave pública (*autokey*).
- A autenticação por chave simétrica é o esquema utilizado originalmente na versão 3 do NTP, mas mantido da versão 4.
- Um conjunto de chaves deve ser gerado e partilhado pelo servidor e pelo cliente. O NTP não fornece meios para a transmissão ou armazenamento seguro das chaves sendo que isso deve ser feito com outros recursos.
- Chaves simétricas podem ser usadas para:
 - autenticar servidores ou pares no modo simétrico ativo;
 - autenticar pares no modo simétrico passivo ou servidores *broadcast* ou *multicast*;
 - autenticar requisições dos programas de monitoração e controlo.

Segurança

- **Autenticação por Chave Pública (*Autokey*)**
 - Na versão 4 do NTP é suportada uma nova forma de autenticação, baseada em chaves públicas e num protocolo que foi chamado de *autokey*.
 - A integridade dos pacotes é verificada através de chaves MD5 e a autenticidade das fontes de tempo é averiguada por meio de assinaturas digitais e vários esquemas de autenticação.
 - Esquemas de identificação (*identity schemes*) baseados em trocas do tipo desafio/resposta são usados para evitar vários tipos de ataques aos quais o método de chaves simétricas é potencialmente vulnerável.
 - A autenticação é baseada em **grupos de segurança** (*security groups*). Pode-se entender um **grupo de segurança** como um conjunto de servidores e clientes NTP que compartilha os mesmos métodos de autenticação, tendo na sua raiz um ou mais servidores considerados confiáveis, e administrados por uma mesma entidade.
 - Um grupo de segurança não tem de ter obrigatoriamente na sua raiz servidores stratum1, mas pode ser cliente de outros grupos de segurança onde exista esse servidor.

Dúvidas



Bibliografia

- <http://www.ntp.org/> - acedido em maio de 2023
- http://pt.wikipedia.org/wiki/Network_Time_Protocol - acedido em maio de 2022
- <http://oal.ul.pt/hora-legal/> - acedido em maio de 2022
- <https://ntp.br/ntp.php> - acedido em maio de 2022
- <https://tools.ietf.org/html/rfc5905> - acedido em maio de 2020
- <http://www.eecis.udel.edu/~mills/ntp/html/index.html> - acedido em maio de 2022
- <http://www.endruntechnologies.com/pdf/NTP-Intro.pdf> - acedido em maio de 2022
- <https://www.youtube.com/watch?v=qGJaJx7OfUo> - acedido em maio de 2022
- <https://www.youtube.com/watch?v=oCtkwEjhyD4> - acedido em maio de 2022
- <https://www.youtube.com/watch?v=WX5E8x3pYqg> - acedido em maio de 2022

Serviços de Rede 1

2022-2023

Pedro Miguel Geirinhas

Aula 10

Proxy

Agenda

- 1.** Objetivos
- 2.** Vantagens e desvantagens
- 3.** Modo de funcionamento
- 4.** Tipos

Proxy - significado

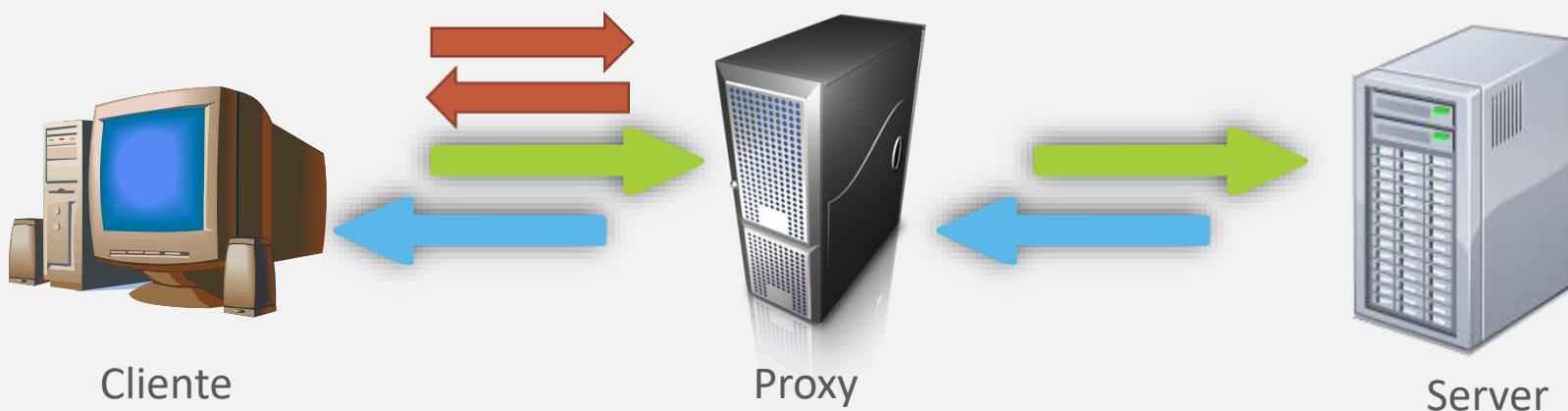
- Proxy é um termo em inglês que significa “*fazer algo em favor de alguém*” [LEXICO PUBLISHING GROUP, 1998].
- Em informática, o termo proxy é utilizado para definir um programa intermediário que atua entre o servidor que armazena um certo conteúdo e uma máquina cliente que faz requisições a este servidor [THE INTERNET SOCIETY – RFC 2616, 1999].
- Um servidor proxy é assim uma máquina intermediária entre um cliente que deseja um recurso e um servidor que o fornece.

Proxy

- Numa rede local devemos tentar impedir que um cliente possa aceder diretamente à Internet garantindo assim ter uma infraestrutura mais segura e eficiente.
- Todos os acessos internos tem/devem ser desencadeados por uma única ou por um conjunto maquinas que definimos como sendo **servidores proxy**.
- Com esta implementação, consegue-se um melhor nível de segurança, porque a rede interna não tem ligações diretas com a Internet, sendo assim mais difícil um invasor externo aceder e controlar uma máquina da rede local.

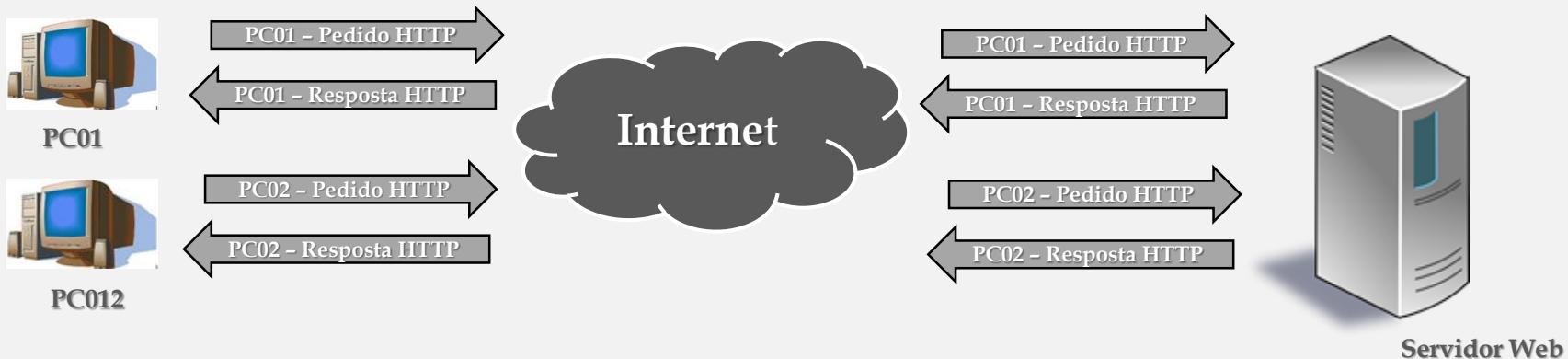
Proxy

- O pedido em vez de ser realizado pelo cliente directamente ao servidor destino é redireccionado através do servidor *proxy*.
- Essa máquina tem como responsabilidade efectuar o pedido em causa e devolver ao cliente a resposta obtida.
- Se tiver esse recurso em cache poderá até diretamente responder ao cliente.

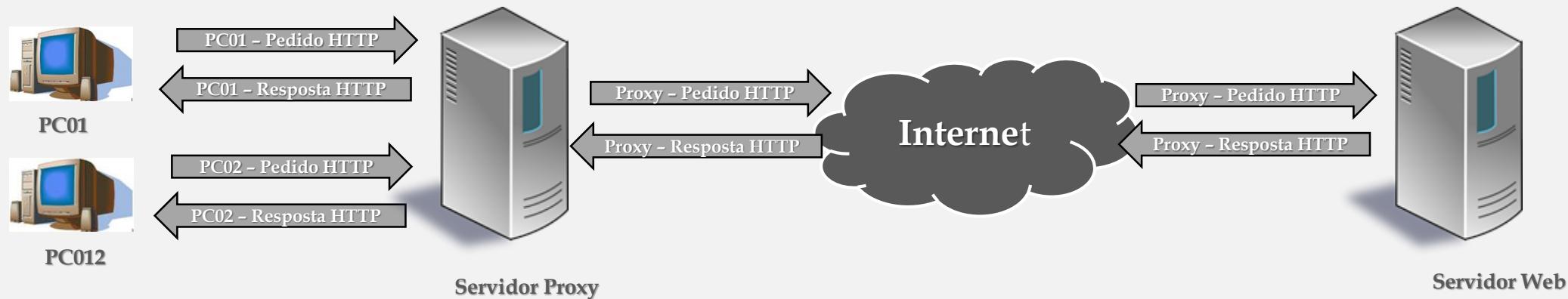


Proxy

Sem



Com



Objetivos

- O servidor Proxy tem os seguintes objetivos fundamentais:
 - Definir regras internas no acesso à Internet.
 - Manter os clientes anónimos.
 - Aumentar a velocidade de acesso à Internet.
 - Aumentar a segurança e controlo de utilização.
 - Fornecer um serviço de *caching* de recursos.
 - Diminuir custos de comunicação.
- **Um proxy não é nem substitui um firewall.**

Vantagens

- **Encaminhamento e gestão da largura de banda:**
 - Permite o acesso à internet a partir de máquinas com IPs privados.
 - Elimina a necessidade de activação de serviços encaminhamento e/ou tradução de endereços (NAT).
 - Permite contornar limitações geográficas.
 - Ponto único de acesso.
 - Facilita as acções de controlo e geração e análise de *logs*.
 - Minimiza o tráfego no caso em que se ativa a *cache* de conteúdos.
- **Relatórios de utilização:**
 - Com um *Proxy* pode definir um conjunto de relatórios que nos permitem analisar de forma detalhada o tipo de utilização que a nossa organização faz do acesso à internet (top de sites, distribuição por horário e por utilizador, etc.).
 - Estes relatórios servem para uma gestão mais racional dos recursos existentes.



Vantagens

- **Segurança:**
 - Os clientes podem ficar “escondidos” atrás do proxy.
 - Não revela a identificação do cliente.
 - Permite bloquear acessos a determinadas localizações (sites). Pode definir lista de servidores que não permite o acesso (*black-list*).
 - Permite filtrar conteúdos perigosos.
 - Controla quem pode aceder à Web, através de autenticação, ou ainda definir quem pode ter esse acesso e em que horário.



Desvantagens

- **Ponto único de falha:**
 - Se o proxy não funcionar todos os clientes da sua rede não acedem à Internet.

- **Cria um ponto possível de estrangulamento de serviço:**

- Todos os clientes acedem a este serviço/servidor para aceder o que pode colocar questões de desempenho.

- **Aumento de custos:**

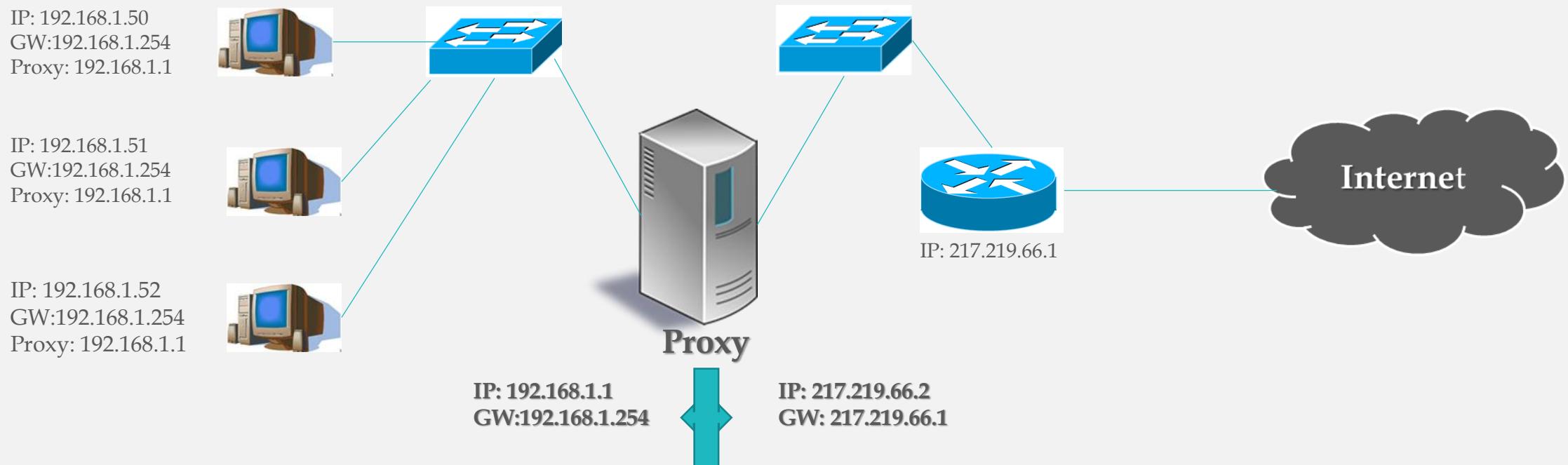
- Serviços de proxy podem exigir modificações nas aplicações e nos clientes.
- Necessidade de comprar, licenciar e manter mais um equipamento.



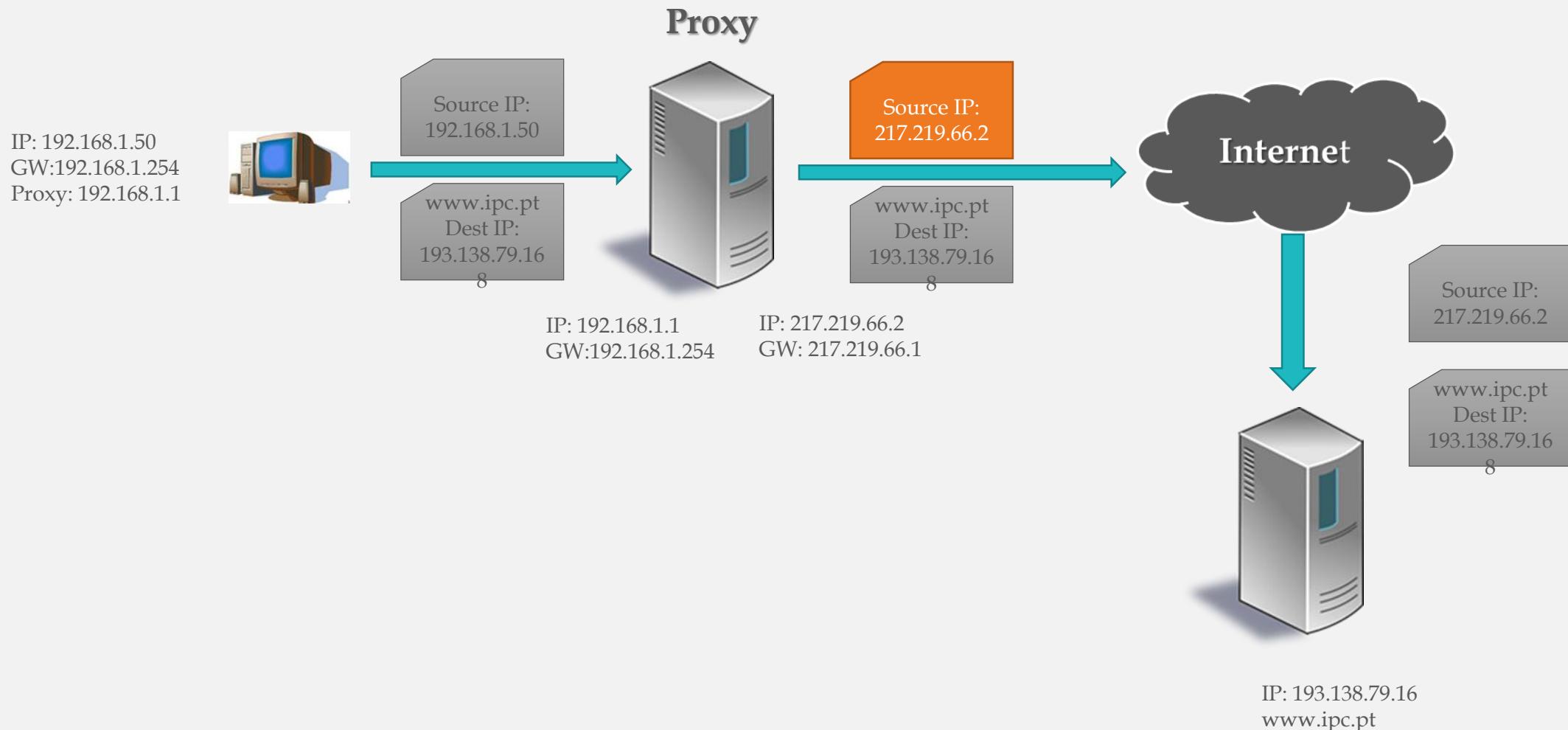
O que necessita?

- Uma “caixa” de hardware ou software específico e servidor com duas placas de rede.
- Um endereço interno e outro externo.
- Acesso à internet.

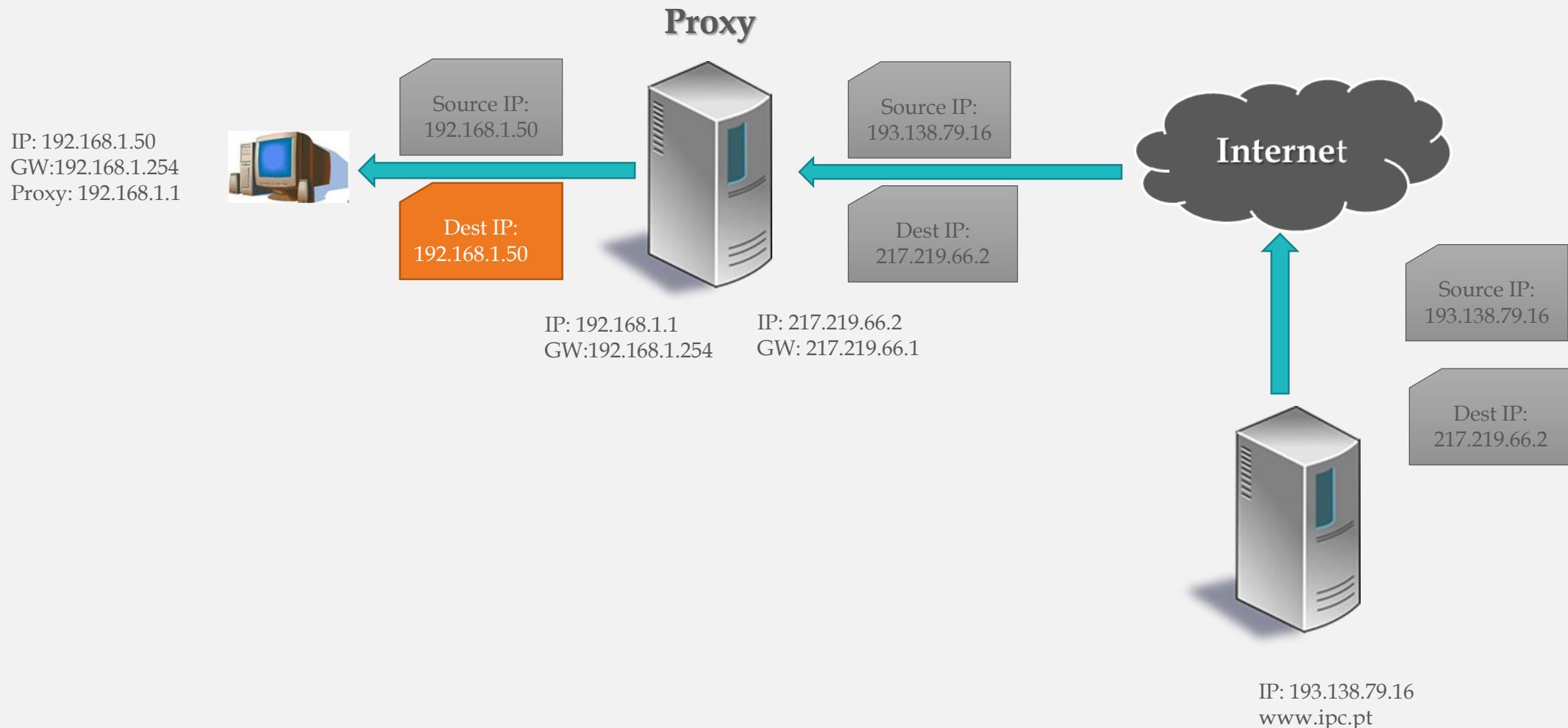
Como funciona



Como funciona



Como funciona



Propostas comerciais

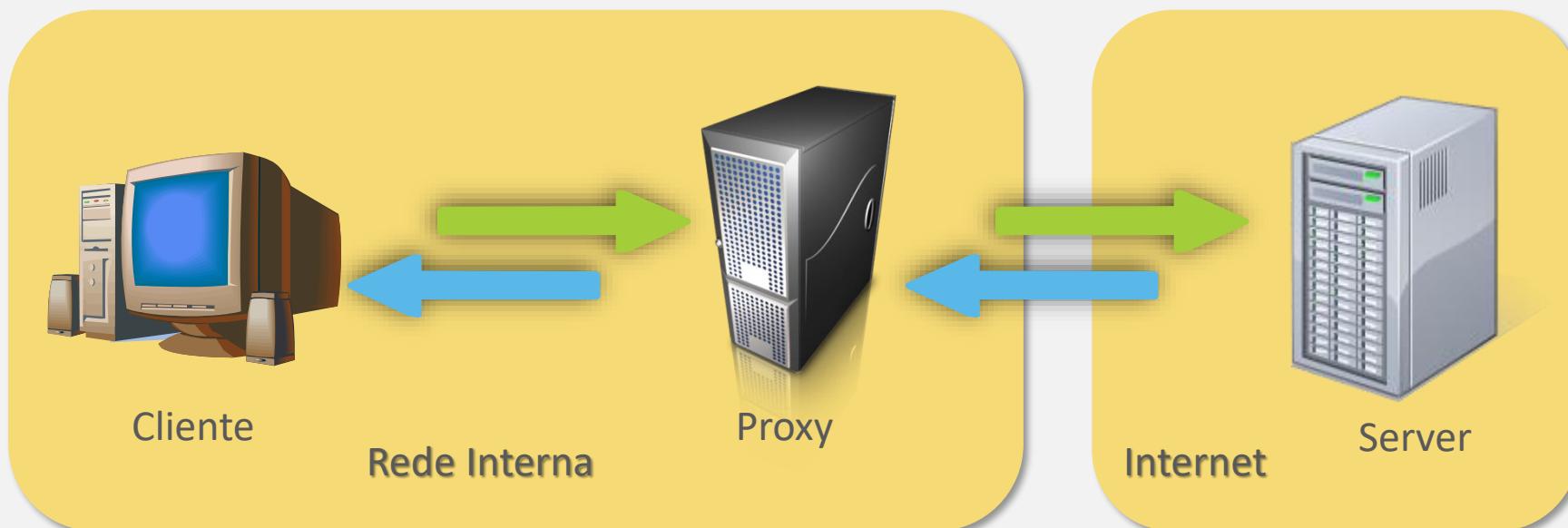
Software Proxy	Hardware Proxy
Squid	Cisco Pix
Kerio Winroute	Blue Coat
CCproxy	Cyberroam
CProxy	
Wingate	
Nginx	

Tipos de proxy

- Tipos de *proxy*:
 - *Forward proxy (Normal Regular/Caching)*
 - *Open proxy*
 - *Transparent proxy*
 - *Reverse proxy*

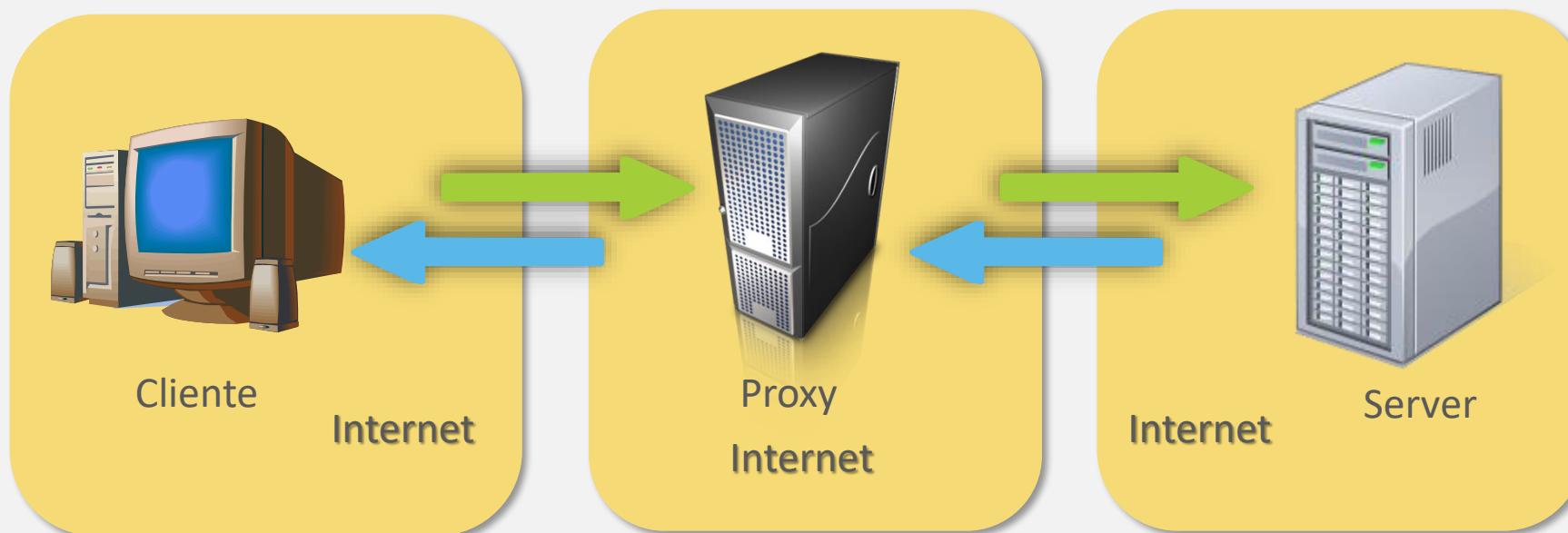
Forward proxy

- Tipo de *proxy* mais usual
- Permite o acesso à *internet* a máquinas com IPs privados ou cujo acesso ao exterior foi limitado
- Só permite o acesso a máquinas autorizadas



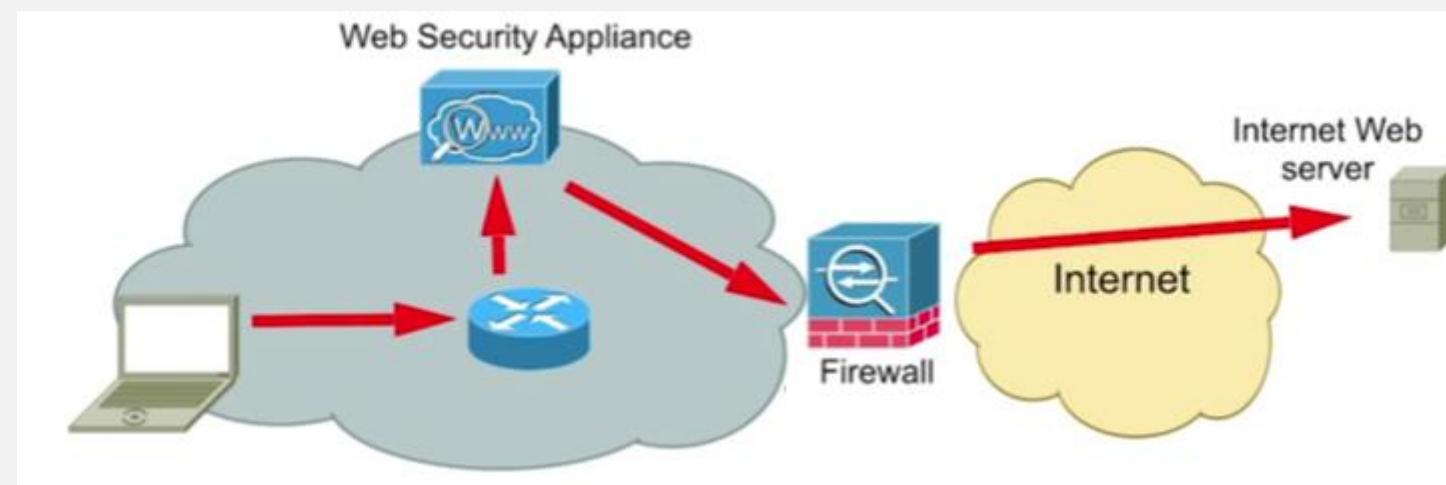
Open proxy

- Tipo especial de *forward proxy* que permite o acesso a qualquer cliente
- A utilização de um ou mais *open proxies* permite esconder a identidade dos clientes
- Existem na internet os chamados free Proxy que fazem esta função.



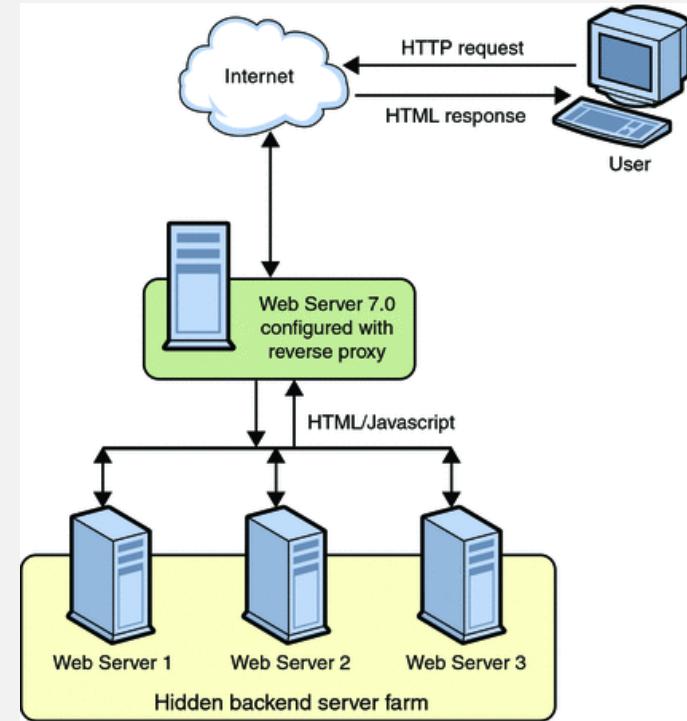
Proxy Transparente

- Idêntico ao *forward* mas não necessita de qualquer configuração no lado do cliente.
- É uma arquitetura que permite que o cliente não saiba da existência do proxy
- Utilizado em grandes empresas onde é critica a configuração dos clientes.



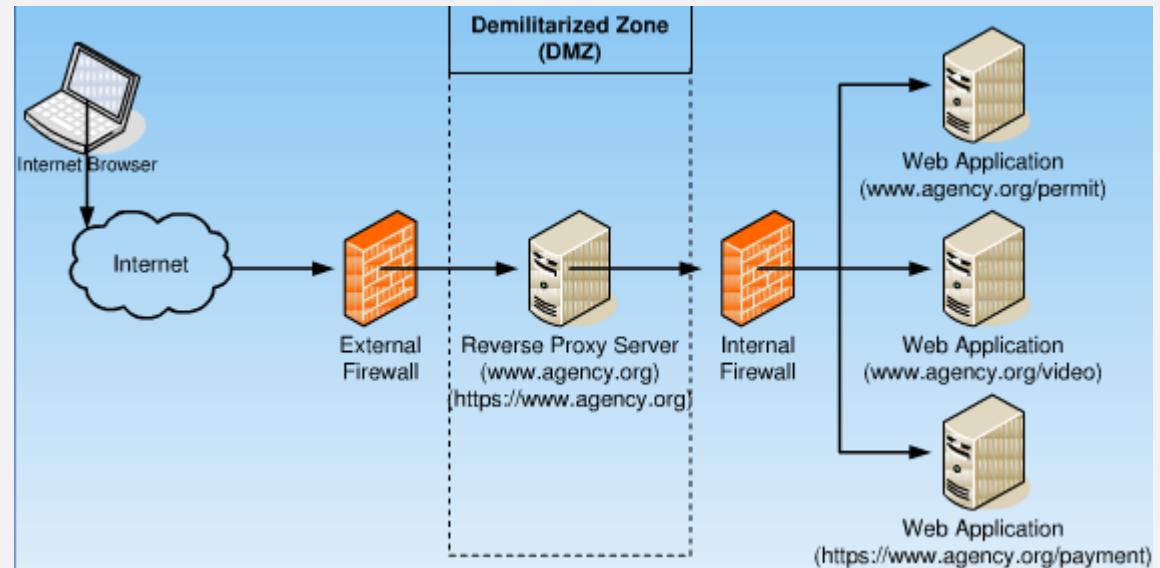
Reverse proxy

- Chama-se reverse-proxy a um servidor proxy-escondido “montado ao contrário”, quer dizer, um servidor proxy que permite não aos utilizadores aceder à rede Internet, mas aos utilizadores de Internet aceder indiretamente a certos servidores internos.
- Por exemplo, permite dar acesso a servidores internos ou distribuir os pedidos entre diversos servidores idênticos (*load balancing*)



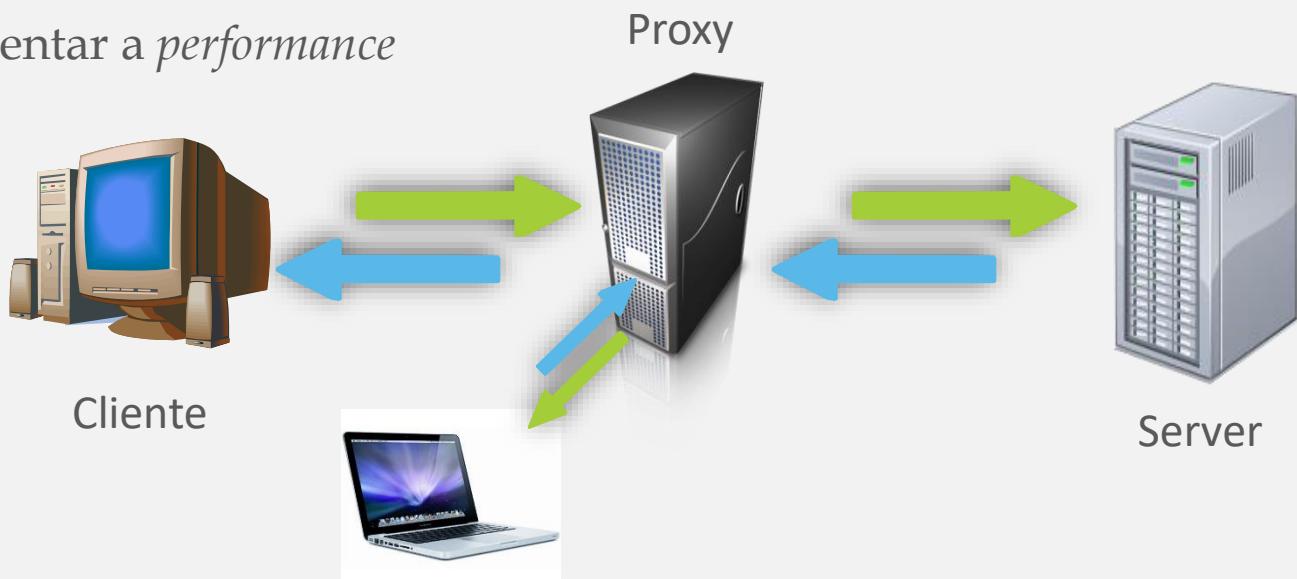
Reverse Proxy - Funções

- Criptografia / aceleração SSL
- Balanceamento de carga
- Compressão
- *Serve/cache static content*
- Segurança
- *Single Sign On*

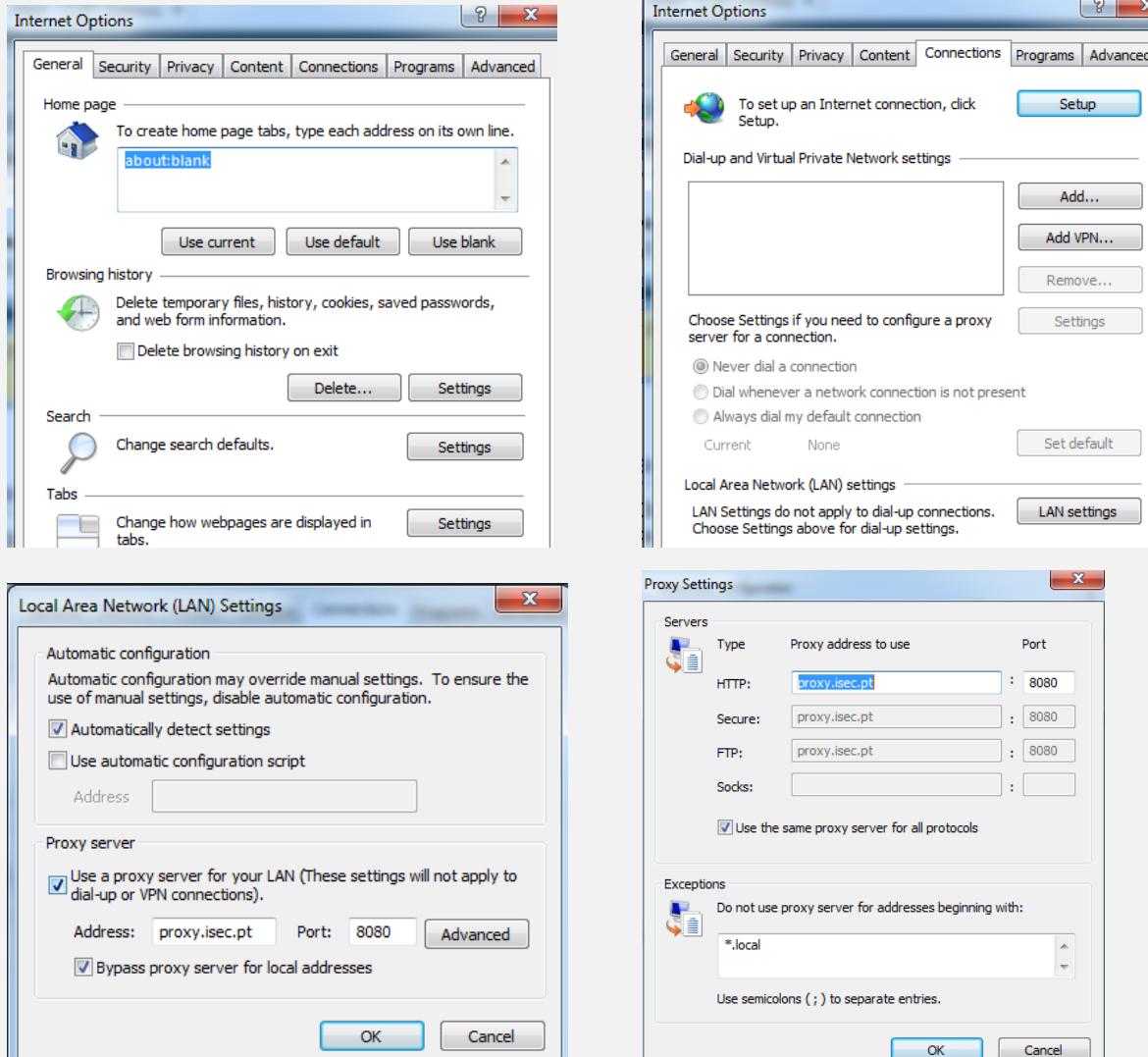


Caching

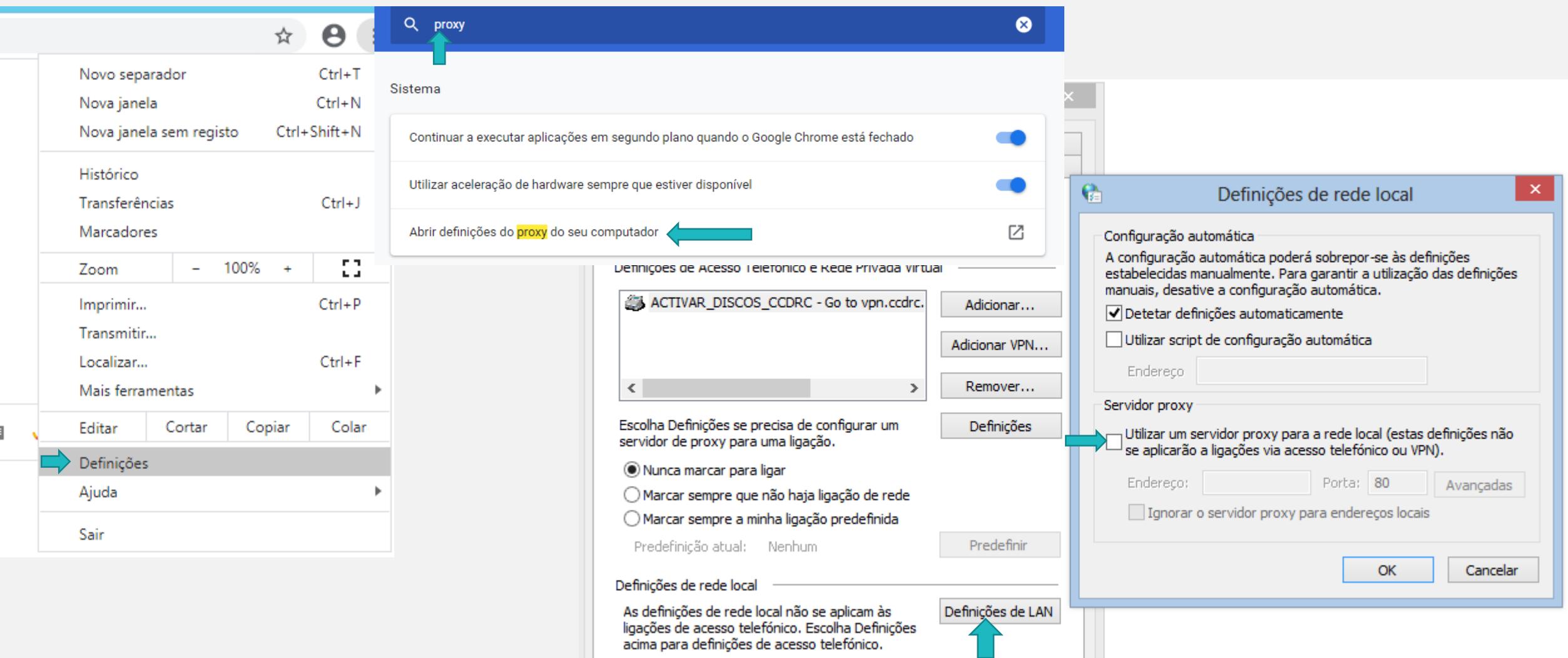
- Pode configurar nos servidores de proxy a funcionalidade de *caching*.
- Quando o mesmo conteúdo é pedido por dois clientes, ao segundo cliente é fornecida a cópia da informação armazenada em *cache*, aquando do primeiro pedido, tornando desnecessário um novo pedido ao servidor original
- Objectivos principais:
 - Minimizar o tráfego
 - Aumentar a *performance*



Configuração do cliente (internet explorer)



Configurar do cliente (chrome)



Software Proxy

- Squid
 - É um dos proxies mais utilizados.
 - Desenvolvido a partir do projeto Harvest da ARPA, mentor do seu projeto foi o Duane Wessels.
 - <http://www.squid-cache.org/>



Vantagens

- É suportado em vários sistemas operativos;
- Diminuição do uso de largura de banda;
- Rapidez de carregamento de páginas guardadas na cache;
- Filtragem de conteúdos usando o SquidGuard;
- Possibilidade de verificar a utilização da rede através dos geradores de relatórios;

Desvantagens

- Consome recursos;
- Demora no carregamento de páginas que não estejam guardadas na cache;
- Otimização difícil;

Dúvidas



Referencias

- <http://www.authorstream.com/Presentation/aSGuest31285-271167-web-proxy-server-entertainment-ppt-powerpoint/> - Acedido em maio de 2020
- <http://pt.kioskea.net/contents/lan/proxy.php3> - Acedido em maio de 2022
- www.slideshare.net/poustchi/proxy-servers-firewalls-178732?src=related_normal&rel=2467014 - Acedido em maio de 2022
- www.cisco.com
- www.microsoft.com
- <http://pt.wikipedia.org/wiki/Proxy> - Acedido em maio de 2022.

Serviços de Rede 1

2022-2023

Pedro Miguel Geirinhas

Aula 11

VPN

Agenda

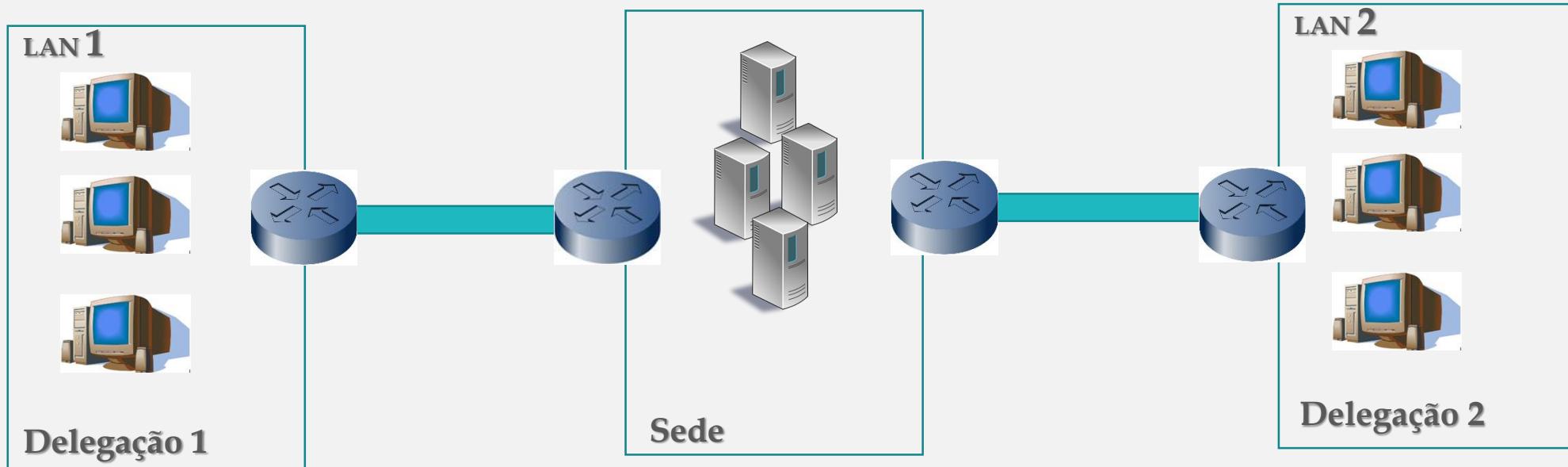
- 1.** Introdução
- 2.** Vantagens e desvantagens
- 3.** Túnel
- 4.** Encriptação
- 5.** Implementações
- 6.** VPN SSL
- 7.** Teletrabalho

Introdução

- Como nenhum homem é uma ilha e o mundo está a ficar mais pequeno, é previsível que necessite de se ligar a computadores remotos usando para isso a sua rede e mais qualquer coisa...
- A razão de ter acesso remoto:
 - Solução para ligar redes locais de outras empresas do mesmo grupo empresarial.
 - Solução para acesso remoto a utilizadores deslocalizados.
 - Solução para encriptação do tráfego numa ligação pública.
 - Solução global para acesso à Internet.

Introdução

- No passado a única possibilidade de dar acesso remoto ou interligar redes locais era muito caro porque obrigava a existência de ligações ponto-a-ponto privadas alugadas aos operadores de telecomunicações.



Introdução

- O conceito surgiu a partir da necessidade de utilizar redes de comunicação não confiáveis (logo não seguras) para a transmissão de dados privados de uma forma segura.
- ***Virtual Private Network - VPN***
 - *Network* - porque pelo menos temos uma ligação entre duas máquinas.
 - *Virtual* - porque a ligação é feita sem a utilização de um meio físico dedicado.
 - *Private* - porque estamos a ceder a recursos privados.
- Uma VPN é assim uma extensão virtual de uma rede privada (por exemplo a LAN).
- As VPNs permitem oferecer os mesmos recursos e vantagens comunicacionais das redes tradicionais mas sem a necessidade de instalação, configuração e manutenção de equipamentos de conexão.

Introdução

- Com a Internet foi possível implementar este tipo de ligações a baixo custo porque é oferecido aos seus utilizadores remotas as mesmas possibilidades/funcionalidades que as linhas dedicadas privadas, utilizando “como portadoras” as linhas públicas de telecomunicações que suportam a ligação à Internet.
- A ligação pode ser efetuada, de modo seguro, através de redes partilhadas ou públicas (utilizando por exemplo o acesso Internet da organização).

Introdução

- **Permite:**
 - o envio de dados entre um computador e a rede interna de modo similar a uma ligação privada ponto a ponto.
 - a ligação entre duas redes locais utilizando a rede publica de comunicações.
- 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.

Introdução

- **Benefícios:**
 - **Segurança** com o controlo dos acessos não autorizados a recursos e a dados.
 - **Redução de custos** já que permite eliminar a necessidade de aquisição/aluguer de linhas dedicadas, utilizando a(s) ligação (ões) à Internet.
 - **Escalabilidade** permitindo que a rede possa crescer sem a necessidade de instalação de nova infraestrutura.



Introdução

- Desvantagens
 - Na sua implementação e manutenção necessitam de uma compreensão dos problemas de segurança da rede pública e de precauções próprias com o processo de entrega de dados.
 - A disponibilidade e performance de uma VPN (particularmente sobre a Internet) de uma organização, depende de fatores que estão fora do seu controle.
 - As tecnologias VPN de vendedores diferentes podem não funcionar bem em conjunto devido a normas proprietárias.
 - Precisam de acomodar outros protocolos além do IP o que implica maior processamento e complexidade protocolar.



Introdução

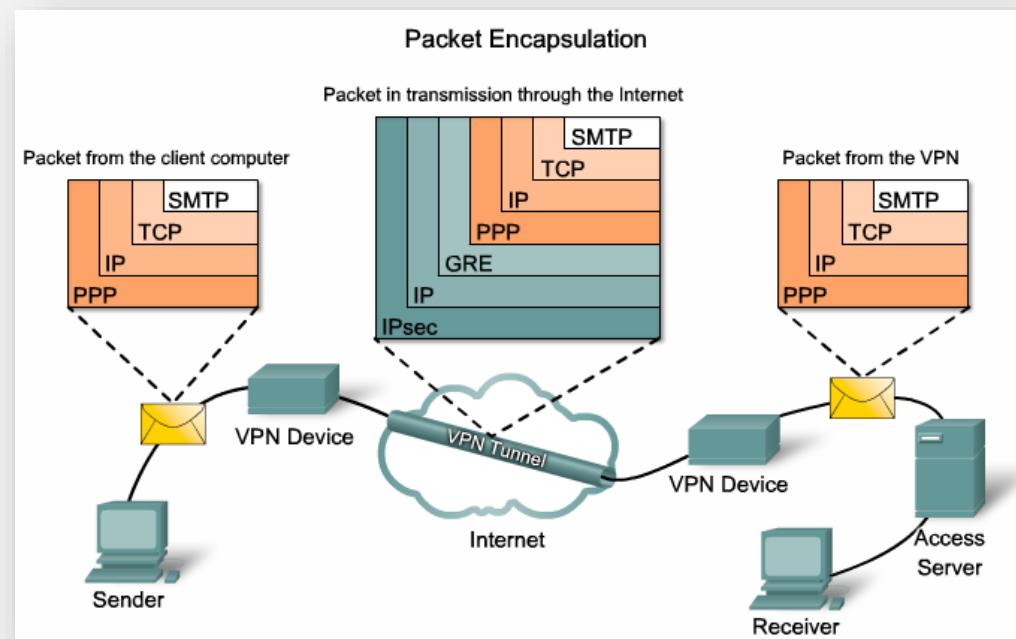
- As VPN devem garantir 4 pontos chave:
 - **Autenticação**
 - Garantir que a informação recebida foi enviada pelo verdadeiro emissor.
 - **Controlo de acesso**
 - Garantir que só os utilizadores autorizados acedem aos recursos.
 - **Confidencialidade**
 - Garantir que apenas o emissor e receptor têm acesso aos dados que são transmitidos.
 - **Integridade**
 - Garantir que os dados não são alterados/adulterados no processo de transporte.

Introdução

- Na implementação de uma VPN existem três conceitos fundamentais:
 - Encapsulamento
 - Túnel (*Tunneling*)
 - Encriptação
- Para que seja emulada uma ligação *ponto a ponto* os dados são encriptados e encapsulados num pacote com informação suficiente para que possa atingir o seu destino de forma **segura** e **confiável** navegando num túnel próprio.

Encapsulamento

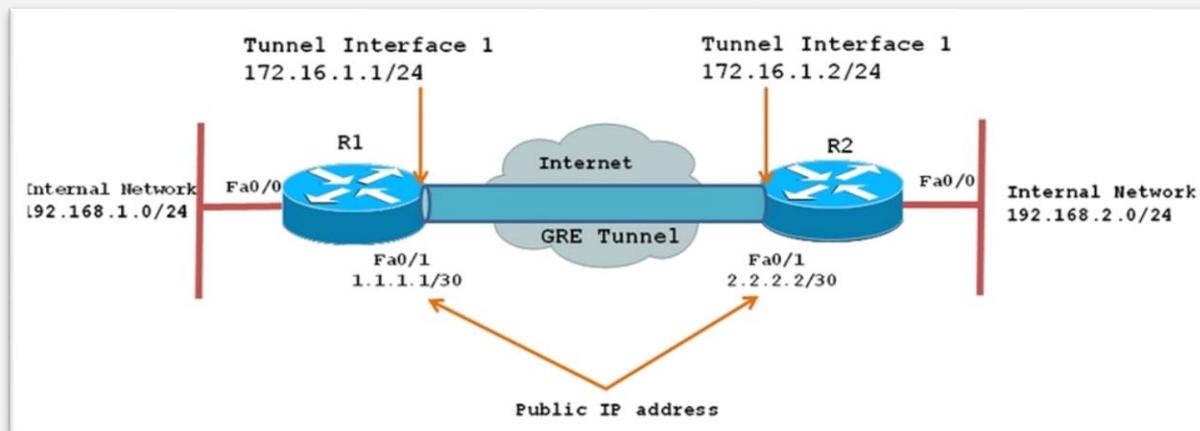
- Em redes de dados, o conceito de encapsulamento é a inclusão de dados de um protocolo de uma camada superior dentro de um protocolo de uma camada inferior.



Fonte: www.cisco.com

Túnel

- A parte da conexão em que os dados transitam encriptados chama-se **túnel**.
- Túnel é a denominação do caminho lógico percorrido pelos pacotes encapsulados.
- A rede VPN pode ser construída sobre uma rede pública (Internet) ou uma rede privada.



Encriptação

- Para ter uma VPN segura necessita de proceder à encriptação dos dados antes dos enviar pelo túnel.
- Encriptação é o processo de transformar informação (referida como texto original) usando um algoritmo (chamado cifra) de modo a impossibilitar a sua leitura a todos exceto aqueles que possuam uma informação particular, geralmente referida como chave.
- Mesmo que os pacotes sejam intercetados, torna-se praticamente impossível efetuar a sua desencriptação caso não se possuam as ‘chaves’ adequadas.

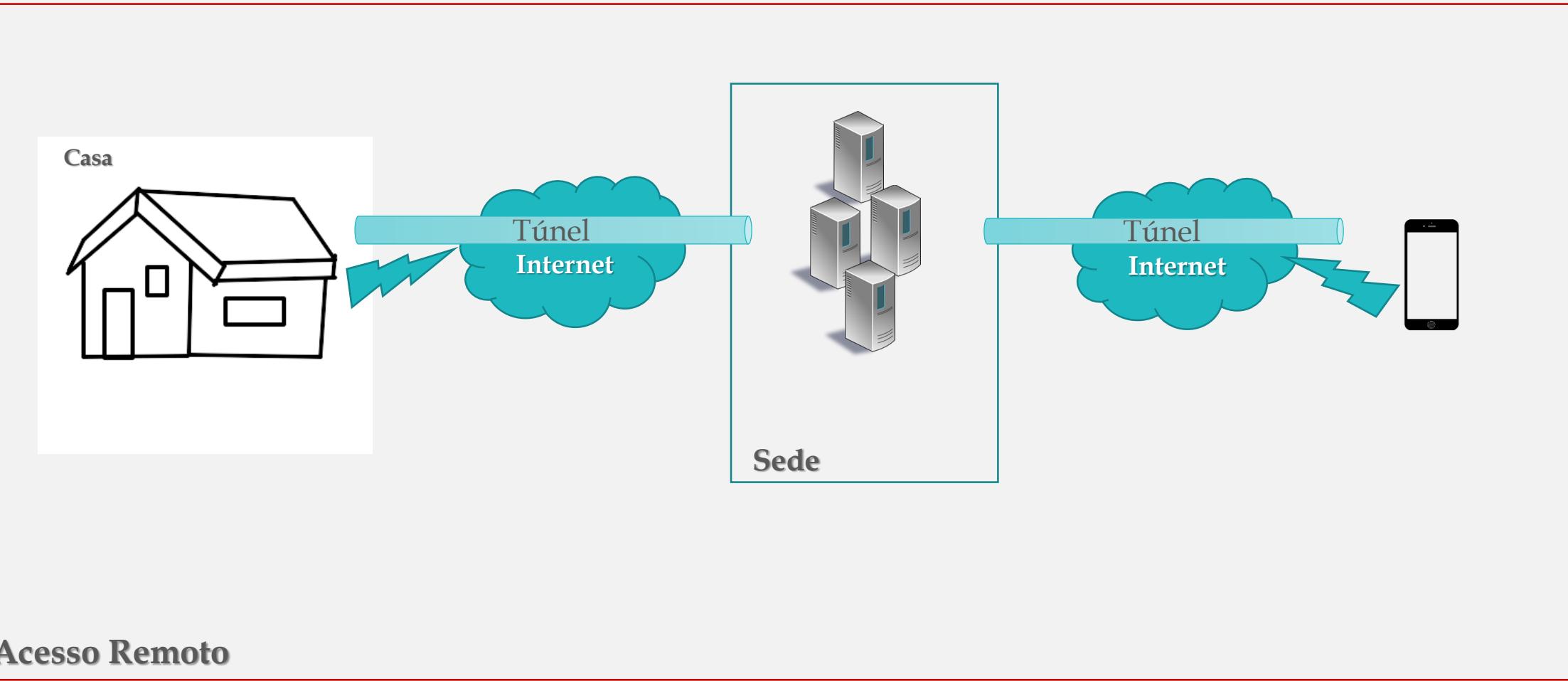
Implementações

- Podemos ter diferentes implementações da VPN, consoante o tipo de ligação, tecnologia, meios ligados e infraestrutura de telecomunicações utilizada.
 - *Demand-dial VPN Networking*
 - *Always-on VPN Networking*

Demand-dial VPN Networking

- A implementação deste acesso é semelhante a uma conexão *dial-up* entre dois equipamentos em localidades diferentes.
- A diferença é que os pacotes são transferidos por um túnel e não através da simples conexão convencional.
- Por exemplo, um utilizador liga-se a um fornecedor de serviços através da rede pública e através dessa ligação estabelece um túnel com a rede remota, podendo transferir dados com segurança.
- Pode utilizar a Internet ou outra ligação para proporcionar o acesso dos postos de trabalho à rede.
- Usado sobretudo para fornecer acesso remoto aos trabalhadores.

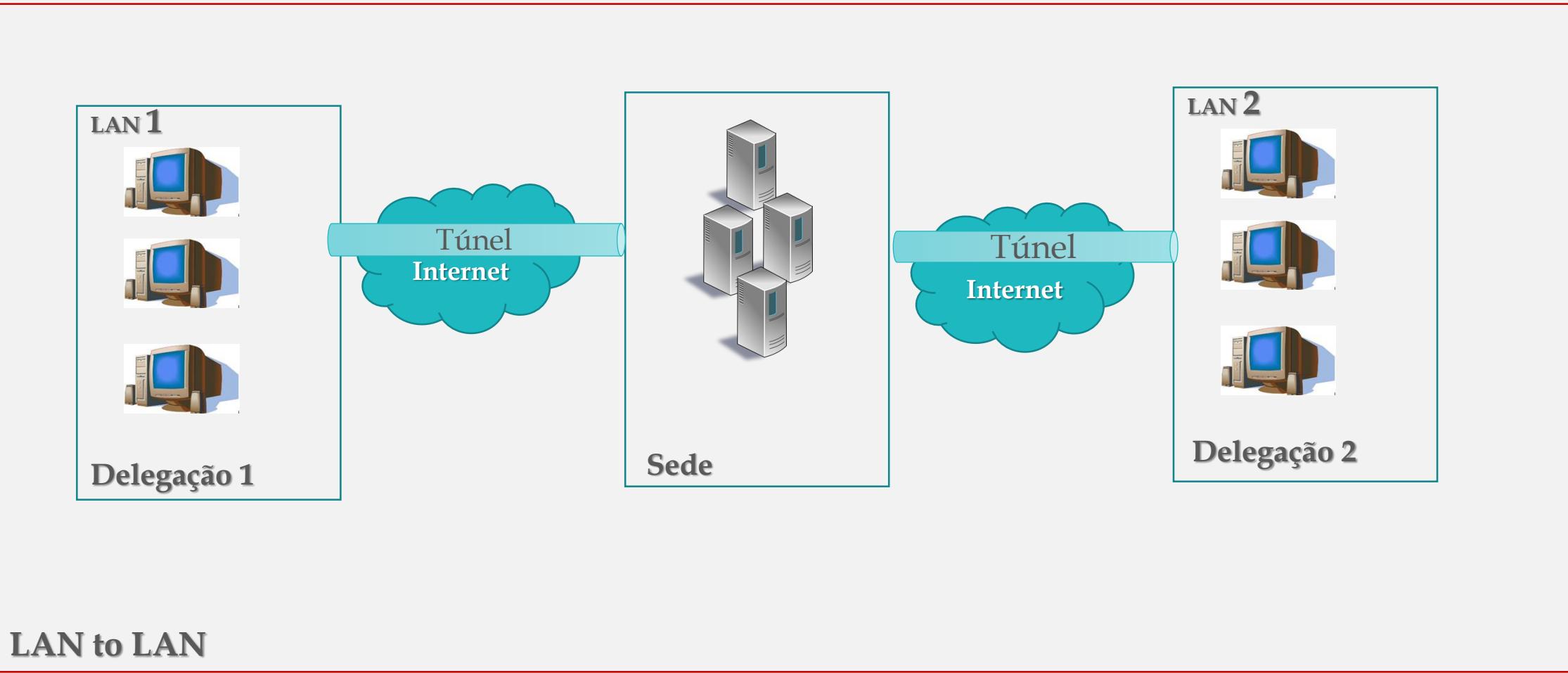
Introdução



Always-on VPN Networking

- O acesso por link dedicado, interligando dois pontos de uma rede, é conhecido como ligação LAN-to-LAN ou *Always-on VPN Networking*.
- O link dedicado as redes são interligadas por túneis que passam pelo *backbone* de rede pública.
- Habitualmente utilizado para ligação de delegações de empresas à sua sede.

Introdução

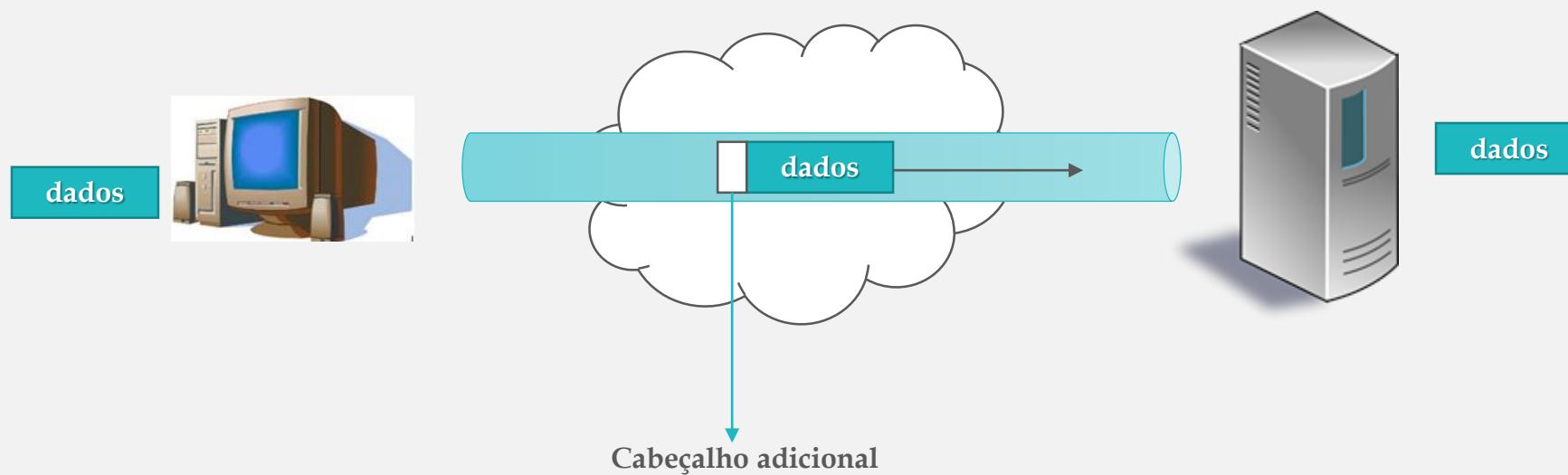


Componentes básicos

- **Autenticação de utilizadores**
 - Verificação da identidade dos utilizadores, autorização de acessos e sistema de logs
- **Gestão de endereços**
 - Atribuição de endereços da rede ao cliente remoto (IP, gateway, dns server,...)
- **Encriptação de dados**
 - Os dados que são enviados através da rede de suporte deverão ser encriptados de modo a garantir a sua confidencialidade
- **Gestão de chaves**
 - Para permitir a encriptação baseado em chaves é necessário fornecer um mecanismo de gestão das chaves – só com este mecanismo é possível efectivar a criação de um túnel

Tunneling

Tunneling



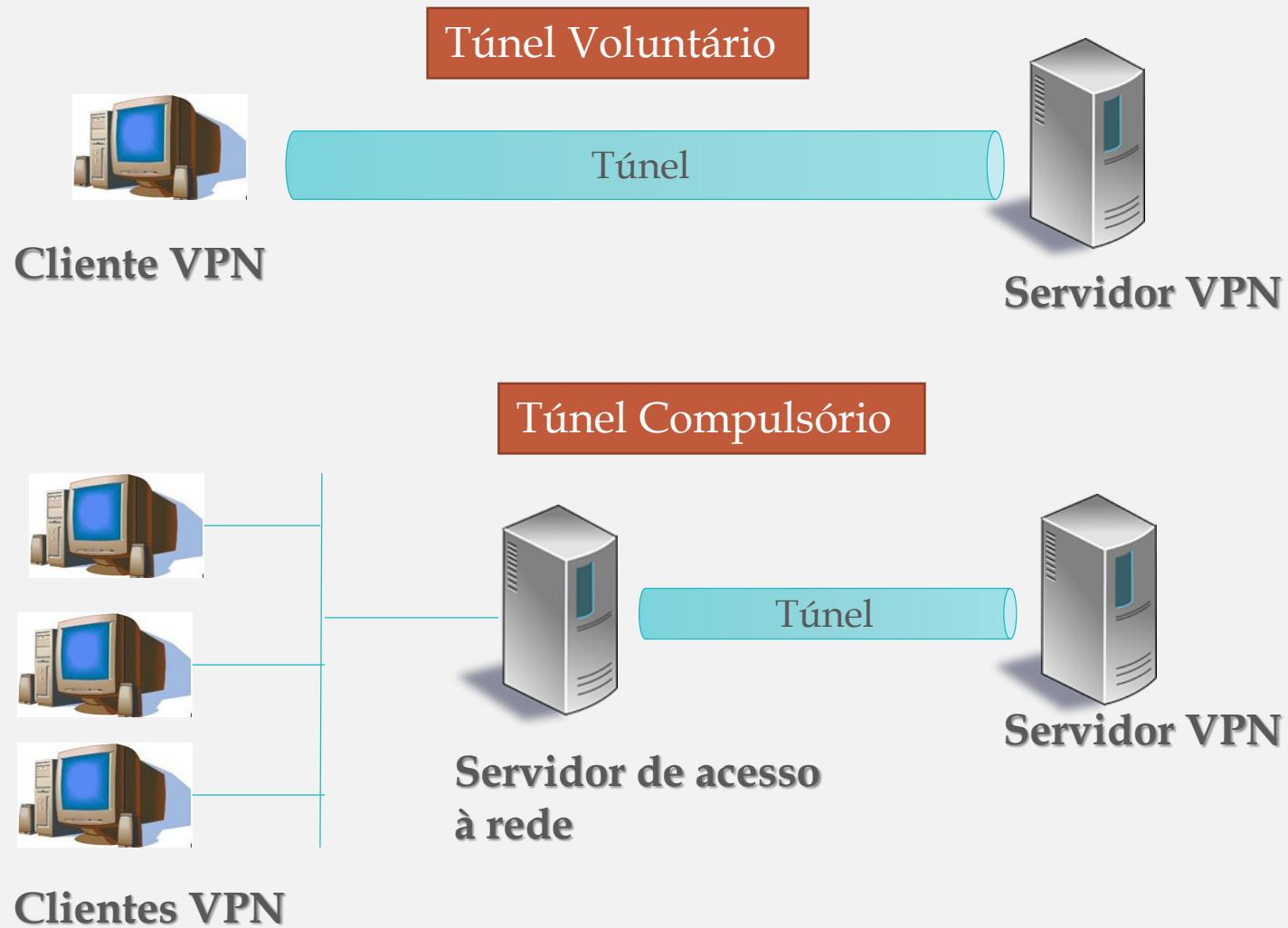
Tunneling

- Método em que se usa a infra-estrutura de rede intermediária, para efectuar a transferência de dados entre duas redes, mas garantindo a privacidade e controlo sobre os dados originais.
- Os dados transmitidos podem corresponder a pacotes ou *frames* de diferentes protocolos.
- Em vez de serem enviados os pacotes, estes são encriptados e encapsulados num pacote do protocolo de *tunneling* inserindo-lhe ainda um novo cabeçalho (*header*).
- O *header* adicional contém a informação de *routing* necessária para efectuar a entrega.

Tipos de Túneis

- **Túnel Voluntário** - um cliente emite um pedido VPN para configurar e criar um túnel. Neste caso, o computador do utilizador funciona como uma das extremidades do túnel e, também, como cliente do túnel.
- **Túnel Compulsório** - um servidor de acesso *dial* VPN configura e cria um túnel. Neste caso, o computador do cliente não funciona como extremidade do túnel. Outro dispositivo, o servidor de acesso remoto, localizado entre o computador do utilizador e o servidor do túnel, funciona como uma das extremidades e atua como o cliente do túnel.

Tunneling



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.

Tunneling

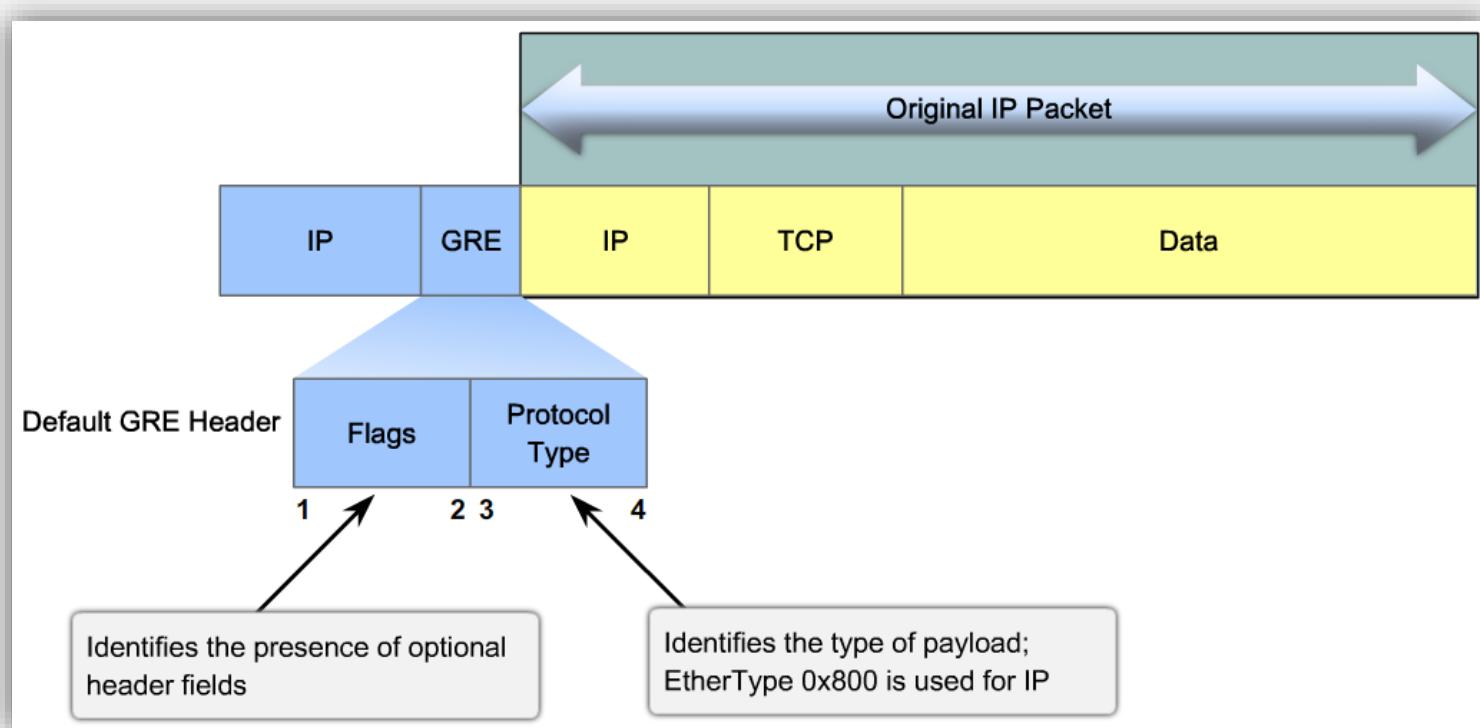
- Podem ser utilizados diferentes protocolos:
 - **GRE** - (*Generic Routing Encapsulation*) da Cisco.
 - **PPTP** - (*Point-to-Point Tunneling Protocol*) da Microsoft.
 - **L2F e L2TP** - (*Layer 2 Tunneling Protocol*) da IETF (*Internet Engineering Task Force*).
 - **IPSEC** - *Internet Protocol Security*
 - **Open VPN**
 - **SSL** - *Secure Sockets Layer*

GRE - *Generic Routing Encapsulation*

- Protocolo desenvolvido pela Cisco.
- Protocolo descrito pelos RFCs 1702 e 2784.
- O funcionamento deste tipo de túnel é muito simples, e consiste em pegar nos pacotes originais, adicionar o cabeçalho GRE, e enviar ao IP de destino (o endereço do destino é especificado no cabeçalho GRE), quando o pacote encapsulado chega na outra ponta do túnel (IP de destino) é retirado o cabeçalho GRE, sobrando apenas o pacote original, o qual é encaminhado normalmente ao destinatário.
- Suporta múltiplos protocolos.
- Através da introdução de uma cabeçalho adicional é possível a transmissão de múltiplos protocolos no mesmo túnel.
- Suporta *multicast*.

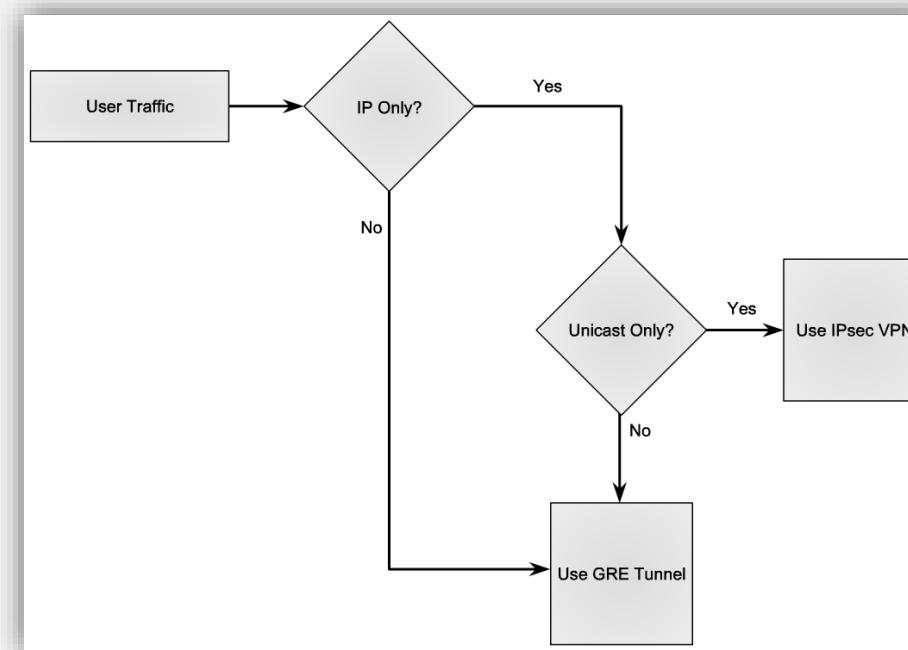
GRE - Generic Routing Encapsulation

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

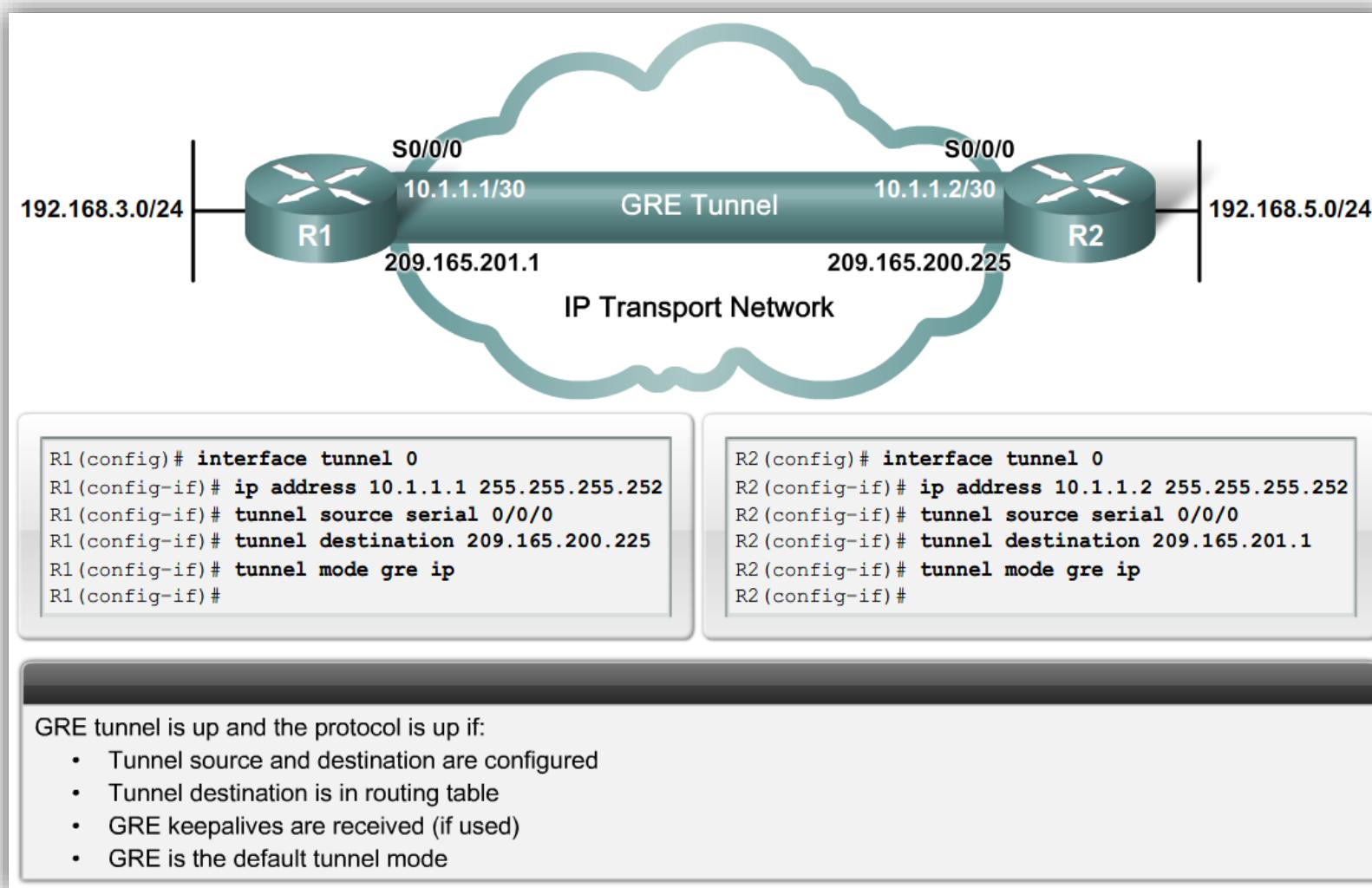


GRE - *Generic Routing Encapsulation*

- Contudo, os túneis GRE não fornecem mecanismos de encriptação de dados.
 - Solução:
 - Recorrer a protocolos específicos que funcionam sobre GRE
 - Recorrer a IPSec



GRE - Configuração

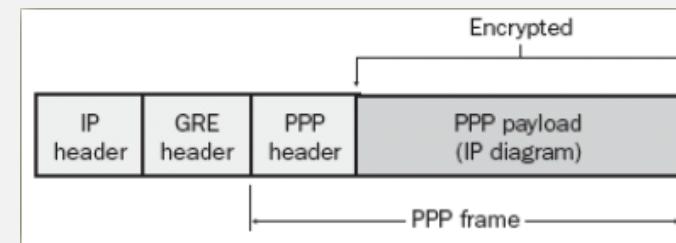


PPTP- Point-to-Point Tunneling Protocol

- Desenvolvido por um consórcio US-Robotics, Microsoft, 3Com, Ascend e ECI.
- Amplamente utilizado em sistemas operativos windows. Contudo, como apresenta alguns problemas de segurança pelo que começou a ser menos utilizado para soluções em que a segurança é um aspeto crítico.
- Utiliza-se quadros PPP (Point-to-Point Protocol), como unidades de troca de informação, encapsulando os pacotes IP.
- Autenticação feita através dos protocolos PAP,CHAP e MS-CHAP.
- Criptografia através do MPPE.

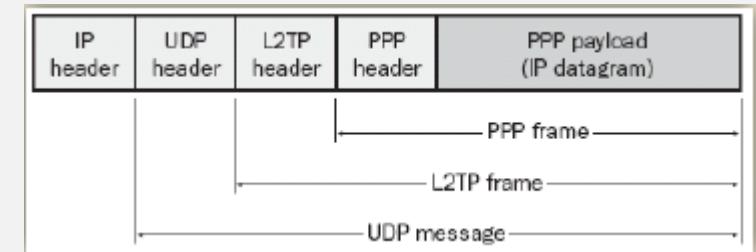
PPTP- Point-to-Point Tunneling Protocol

- Permite que o tráfego seja criptografado e encapsulado para serem enviados através de redes IP privadas ou públicas como a Internet.
- Principais características:
 - Todo o tráfego é enviado pela porta TCP 1723.
 - O túnel é iniciado pelo servidor de acesso.
 - Os túneis são estáticos.
 - Controle está nas mãos do provedor do serviço.
 - A encriptação começa depois da ligação.
 - Requer a autenticação dos utilizadores.
 - Não requer uma infraestrutura de certificados.
 - Suporta NAT.



L2TP- Layer 2 Tunneling Protocol

- L2TP (*Layer 2 Tunneling Protocol*) da IETF (*Internet Engineering Task Force*).
- As principais características são as seguintes:
 - Túneis iniciados pelo utilizador.
 - Túneis “on-demand”.
 - Controle nas mãos do utilizador.
 - A encriptação começa antes da ligação.
 - Requer autenticação de utilizadores e dos próprios computadores que tentam estabelecer a ligação.
 - Requer uma infraestrutura de certificados.
 - Não é compatível com sistema NAT.

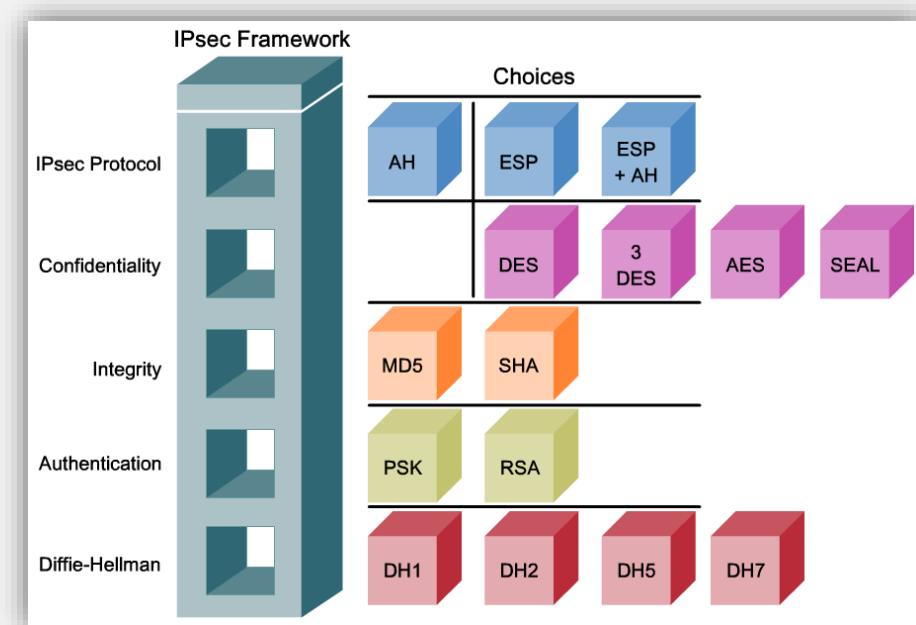


IPSec

- O RFC 1825, publicado em 1995, estabeleceu a arquitetura de segurança por meio da especificação dos protocolos AH e ESP cujos cabeçalhos seriam usados para fornecer serviços de segurança (autenticidade, integridade e confidencialidade) no IPv4 e IPv6.
- Detalhes da sua implementação foram inicialmente especificados nas RFC 1826 e RFC 1827.
- O RFC 1825 definiu a necessidade de existência de um protocolo de gestão de chaves como necessário ao uso de AH ou ESP, bem como especificou o conceito de Security Association (SA) como um conjunto de informações que definem uma ligação que suporta estes protocolos.
- Em novembro 1998 o IPsec teve novas definições que foram descritas nos RFC 2401 a 2412. Este conjunto de RFCs ficou conhecido como "antigo IPsec" ou "IPsec-v2".
- Em 2005 a arquitetura IPsec foi novamente renovada e expandida para uma terceira geração de RFCs (RFC 4301, 4302 e 4306, dentre outras), o que se convencionou chamar "IPsec-v3", ou "novo IPsec".
- Tem por objetivo proteger os dados “assinando” digitalmente e encriptando os mesmos antes de os transmitir.
- Consiste numa *framework* que suporta diferentes mecanismos para:
 - manter a confidencialidade e integridade dos dados.
 - autenticar a fonte de dados.
- Funciona ao nível da camada de rede (OSI Layer 3).

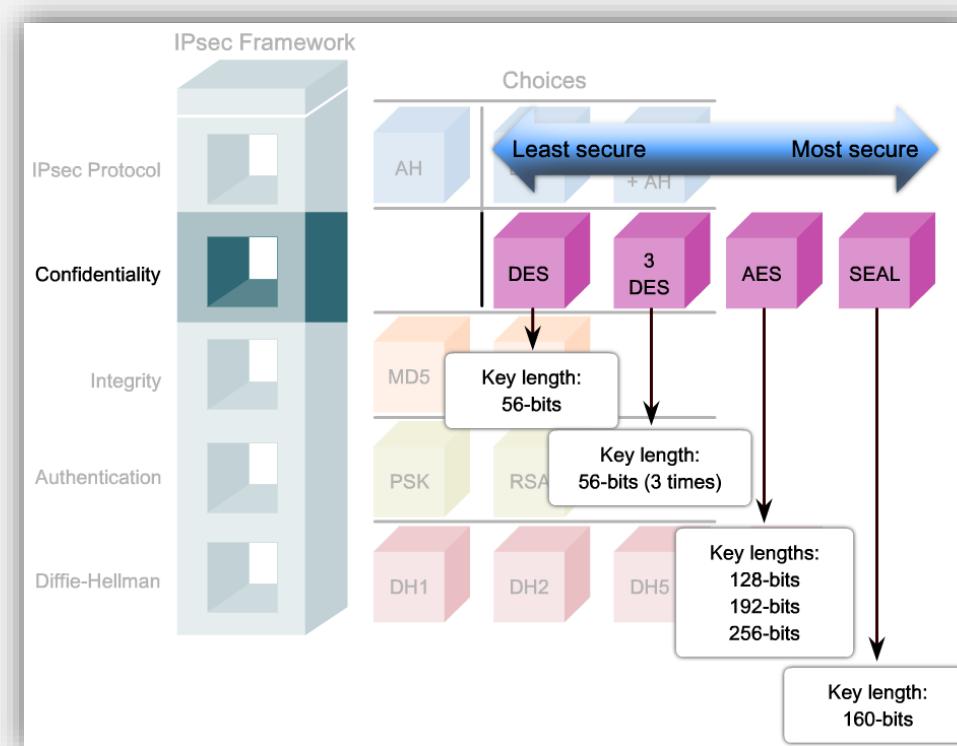
IPSec

- Constituído por 5 “blocos”:
 - Protocolos IPSec
 - Confidencialidade
 - Integridade
 - Autenticação
 - Gestão de troca de chaves de segurança



Confidencialidade

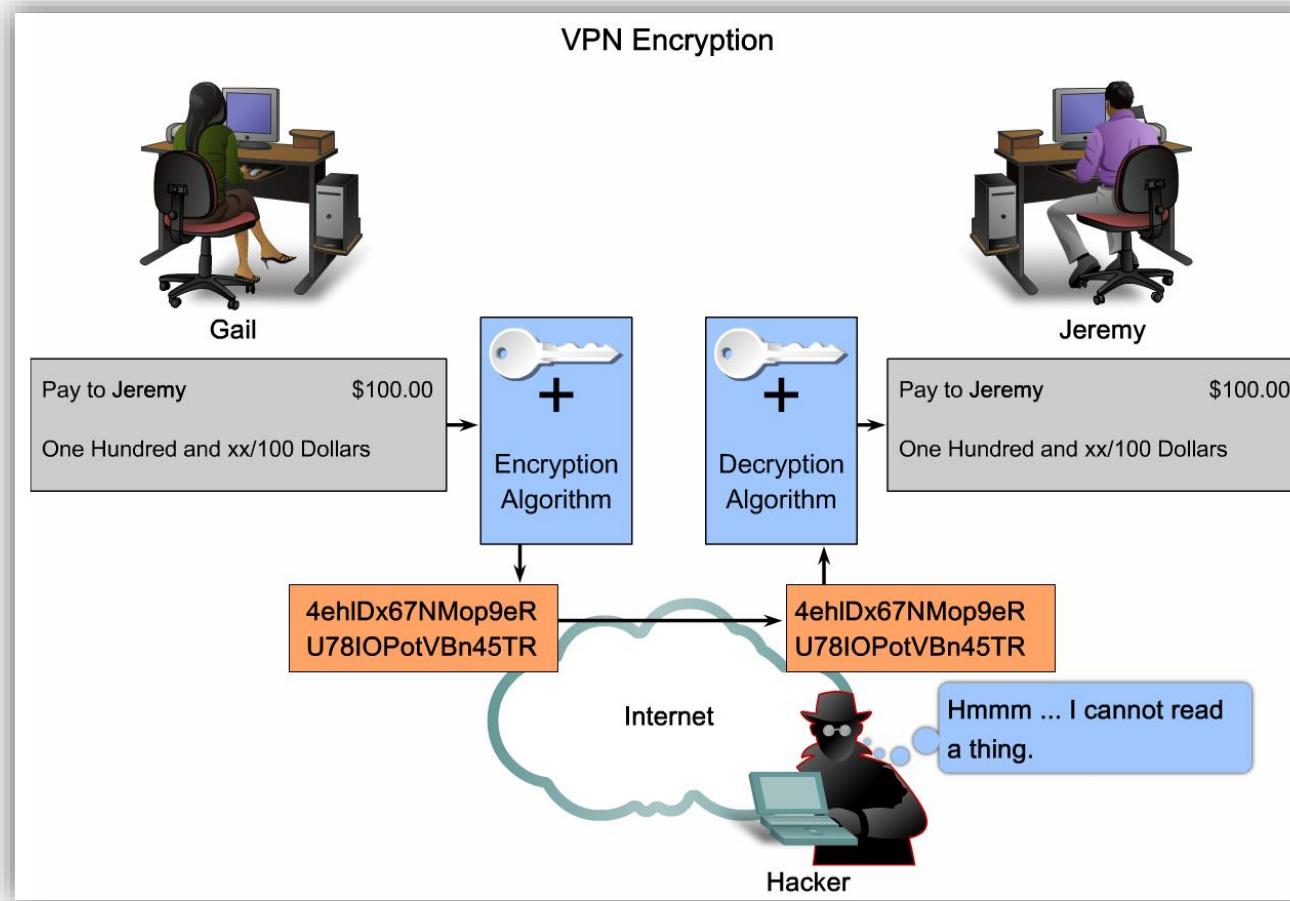
- Protege a privacidade na troca de informação através da encriptação dos dados.
- É a garantia que a informação se mantém protegida contra a sua revelação não autorizada.



Confidencialidade

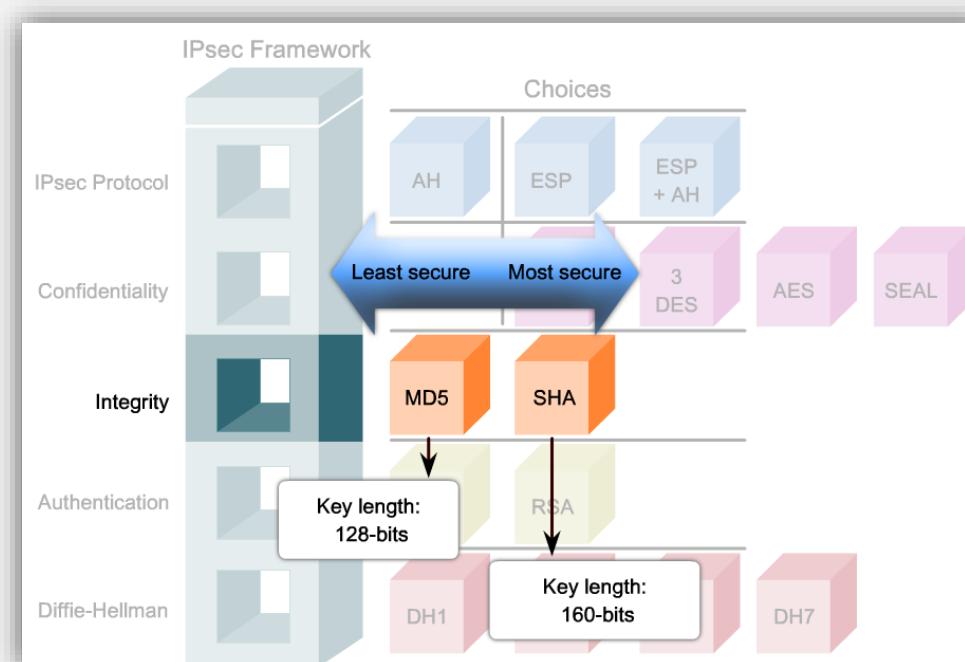
- Chaves secretas não devem ser trocadas pela rede por razões obvias.
- Chaves secretas e públicas são criadas aos pares e mantém uma relação matemática.
- Dados criptografados com a chave pública de alguém, só podem ser recompostos com a chave privada dessa mesma pessoa.
- Chaves públicas podem ser trocadas pela rede livremente.

Confidencialidade



Integridade

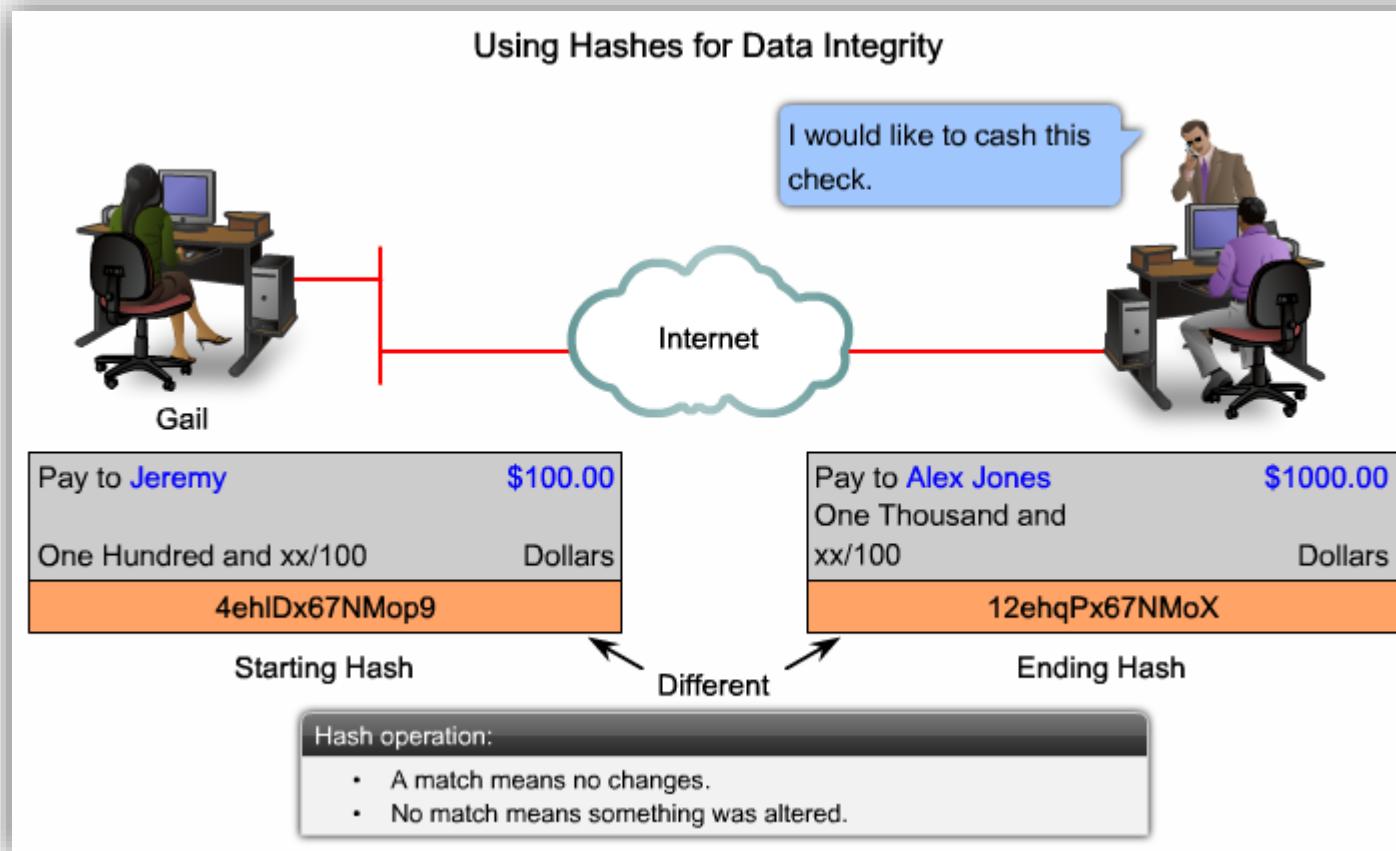
- Garantir que a informação transmitida não foi alterada de forma alguma.
- A integridade dos dados é garantida através de algoritmos *Hashed Message Authentication Codes* (HMAC)



Integridade

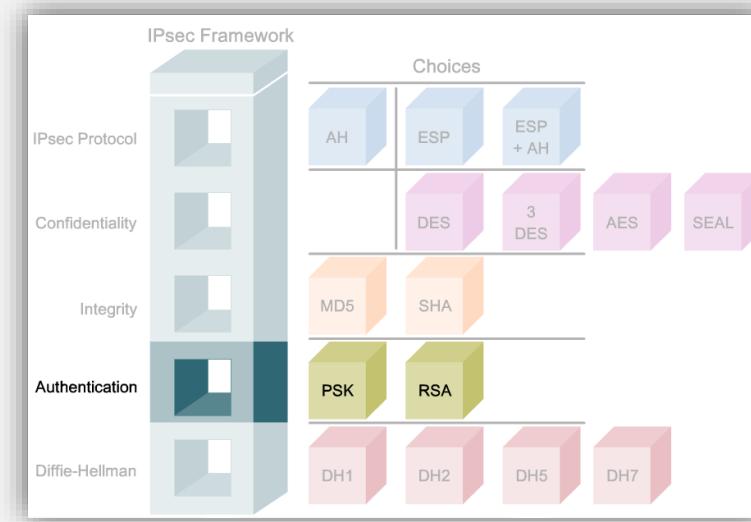
- *One way hash function*
 - espécie de um “checksum” [função $f(x) = y$] para um conjunto de dados segundo um padrão conhecido.
 - Gerado na saída e conferido na chegada.
- *Message-authentication codes (MACs)*
 - adicionar uma chave à função hash. O emissor cria o arquivo a ser enviado; calcula o MAC baseado na chave partilhada com o receptor e adiciona-a ao arquivo; receptor lê o arquivo, calcula o MAC e compara com o que veio anexado ao arquivo.

Integridade

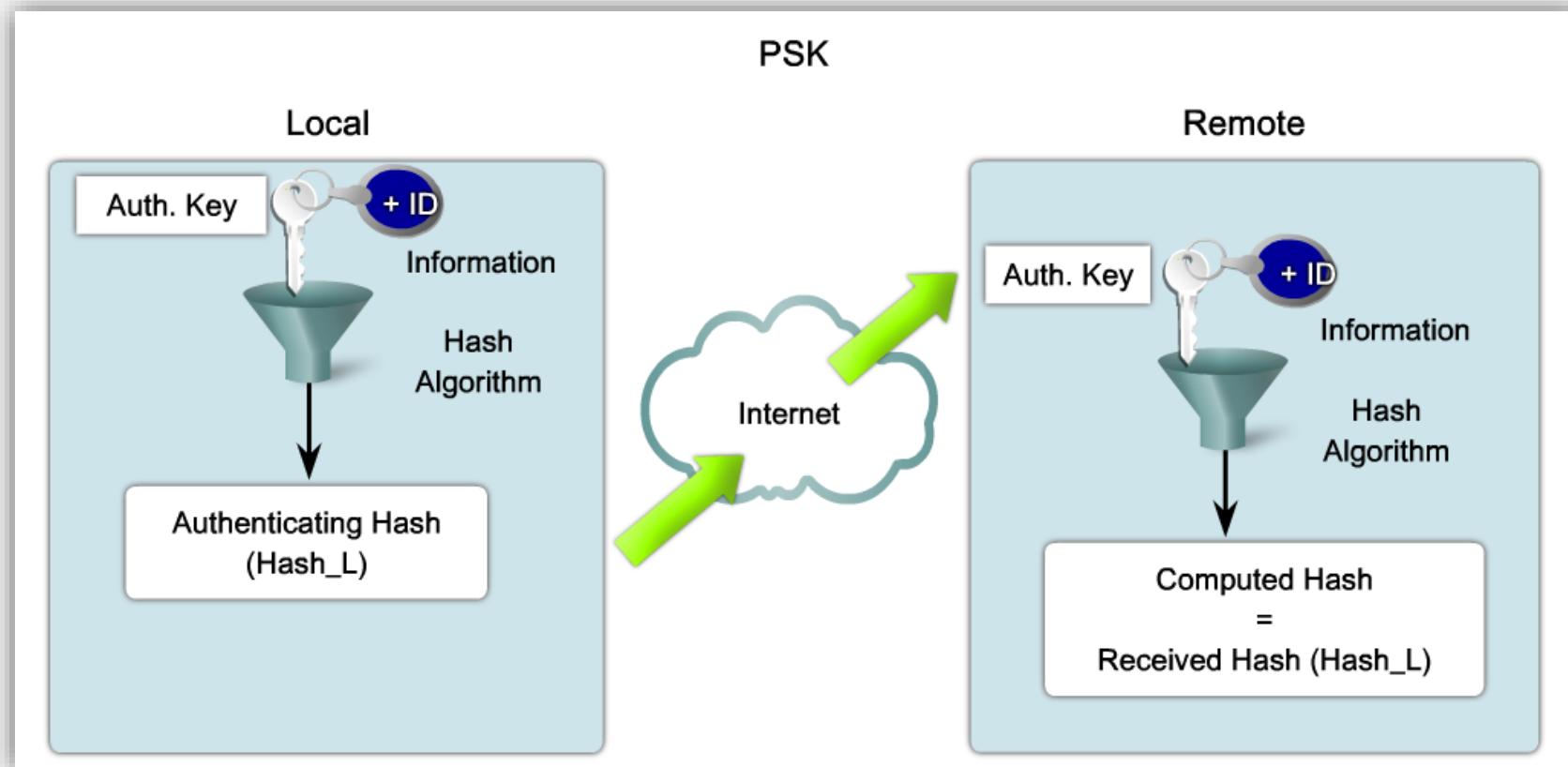


Autenticação

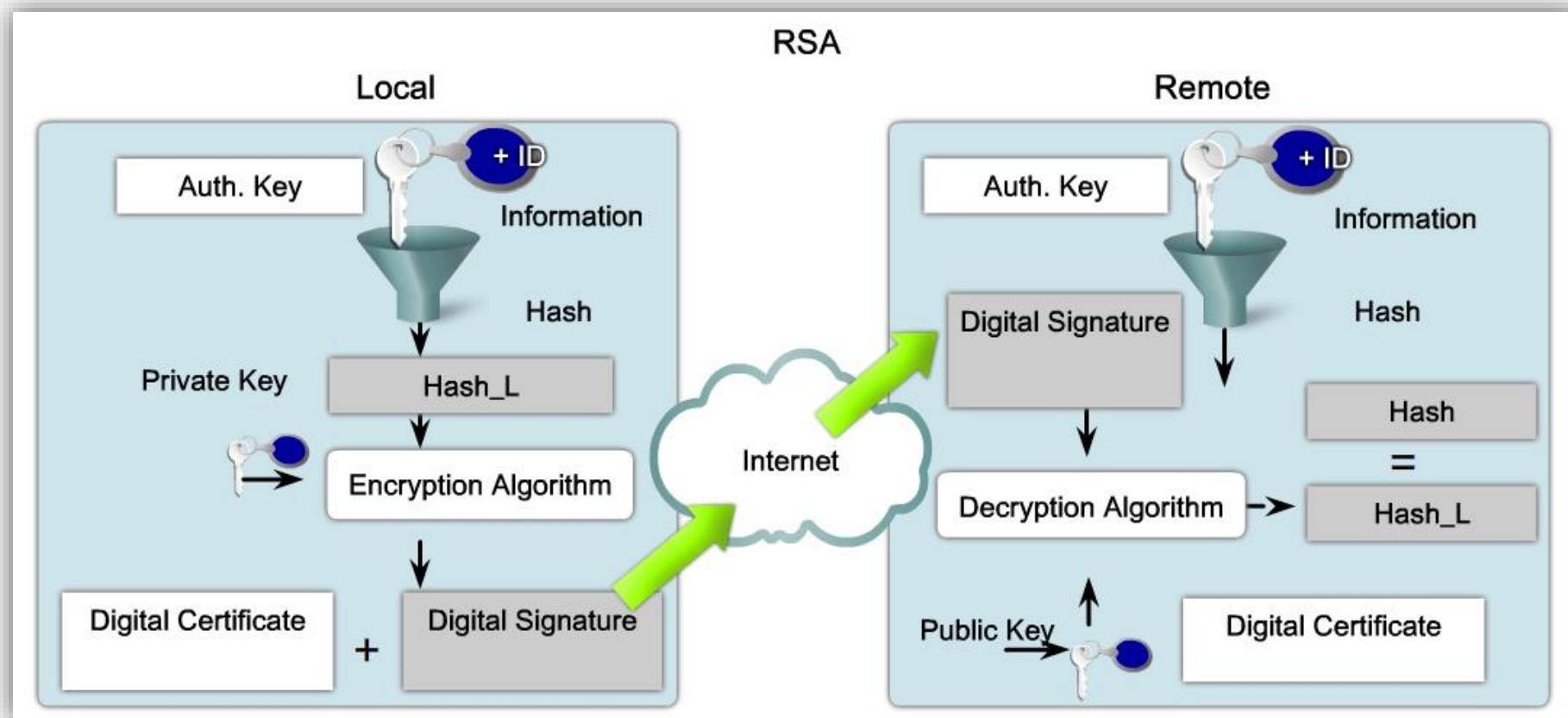
- A verificação da identidade do equipamento do lado oposto deve ser realizada antes de ser iniciada a comunicação de dados ou seja na fase de estabelecimento do túnel.
- Dois métodos base para realizar a autenticação
 - Pre-Shared Keys (PSK)
 - RSA Signatures



Pre-Shared Keys

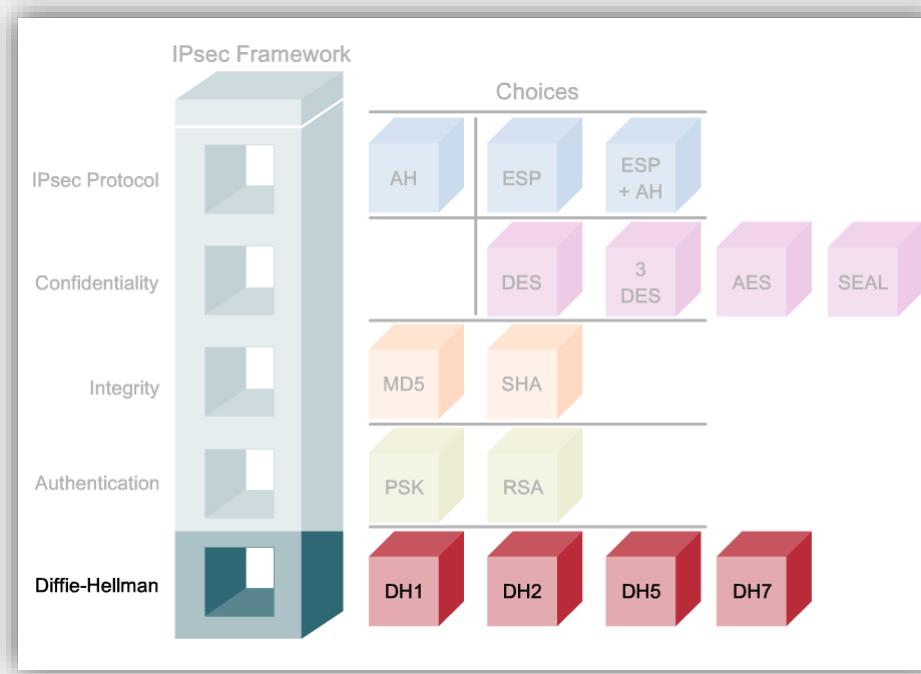


RSA Signatures



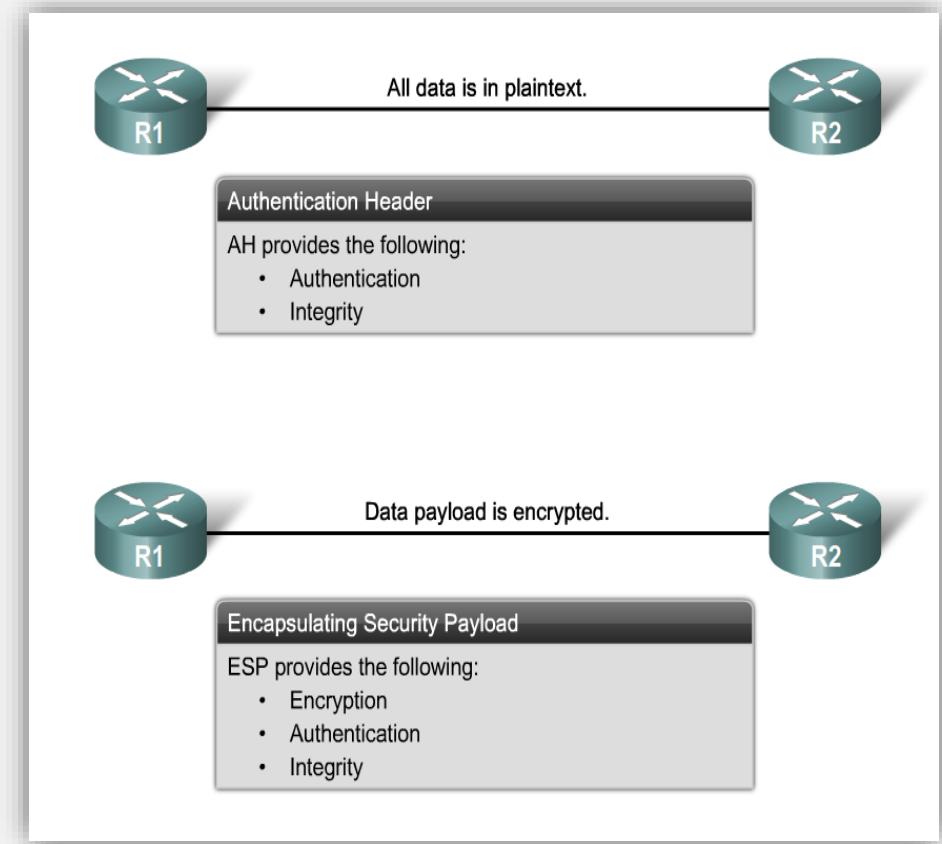
Gestão de chaves

- A gestão das chaves necessárias para o bom funcionamento dos diversos algoritmos é garantida através do método *Diffie-Hellman*. Com este protocolo são geradas em ambos os lados a mesma chave simétrica.



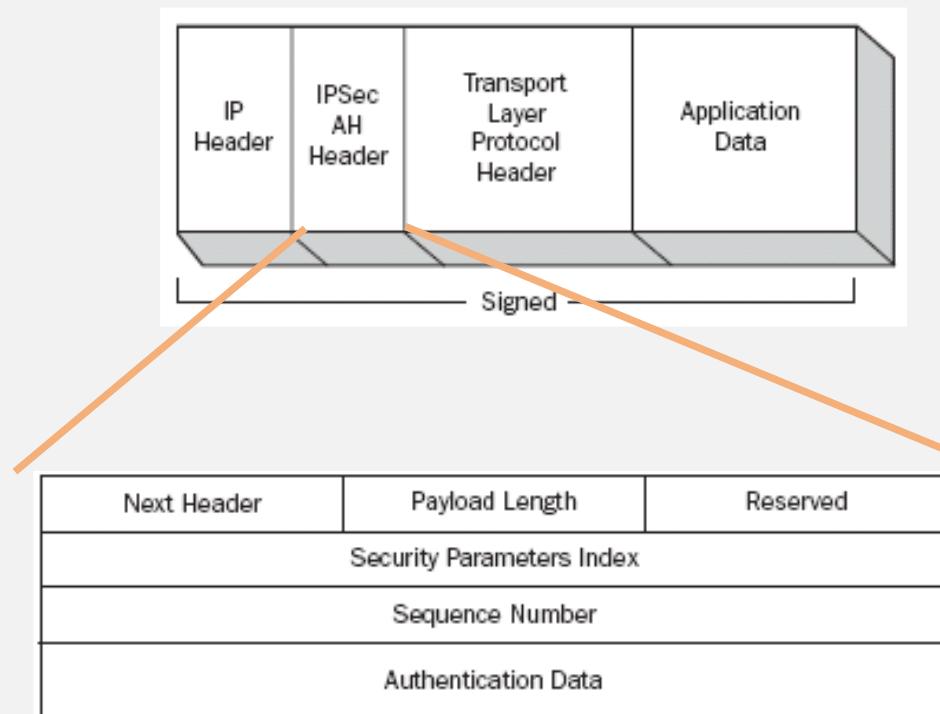
Protocolos IPSec

- Os principais protocolos usados no IPSec são:
 - *Authentication Header* (AH)
 - *Encapsulating Security Payload* (ESP)
 - *IKE*: (*Internet Key Exchange*)



Authentication Header (AH)

- Este protocolo não encripta os dados, mas permite a autenticação, proteção contra ataques de repetição e de manutenção de integridade dos dados.

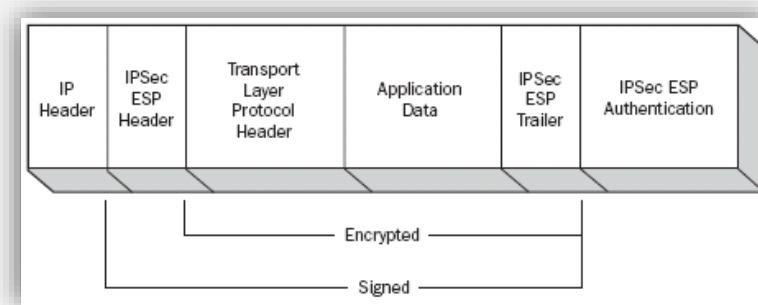


Authentication Header (AH)

- Campos do cabeçalho:
 - *Next header*
 - O código do protocolo que deu origem à existência do cabeçalho AH, normalmente TCP, UDP, ICMP
 - *Payload length*
 - Tamanho do cabeçalho AH
 - *Security Parameters Index*
 - Parâmetros de segurança, resultado da negociação
 - *Sequence Number*
 - Contém um valor que é iniciado em 1 e é incrementado por cada pacote que é enviado
 - *Authentication Data*
 - Contém um '*integrity check value*' (ICV) calculado pelo computador origem e recalculado, para comparação, no computador destino

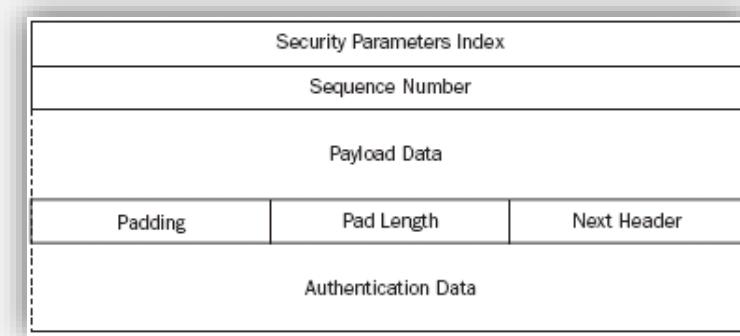
IP Encapsulating Security Payload (ESP)

- É o protocolo que permite a encriptação dos dados nos pacotes
- Também fornece mecanismos de autenticação, anti repetição e verificação de integridade
- Insere um cabeçalho e um campo de terminação específico



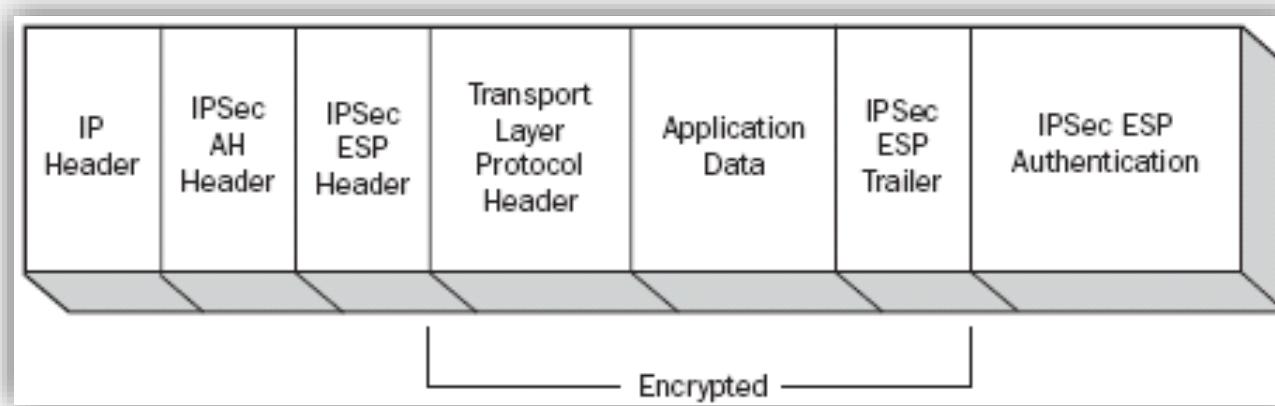
IP Encapsulating Security Payload (ESP)

- Campos da mensagem
 - *Security Parameters Index*
 - identifica os parâmetros de segurança em combinação com o endereço de IP;
 - *Sequence Number*
 - um número crescente, usado para impedir ataques repetitivos;
 - *Payload Data*
 - Contém a informação original existente no pacote IP original e, normalmente, corresponde a informação TCP, UDP ou ICMP
 - *Pad length*
 - Número de bytes acrescentados (campo *padding*) de modo a efectuar um alinhamento de 32 bits
 - *Next Header*
 - O código do protocolo que deu origem a esta mensagem e correspondente à informação existente em *Payload Data*
 - *Authentication Data*
 - contém os dados usados para autenticação do pacote.



AH e ESP

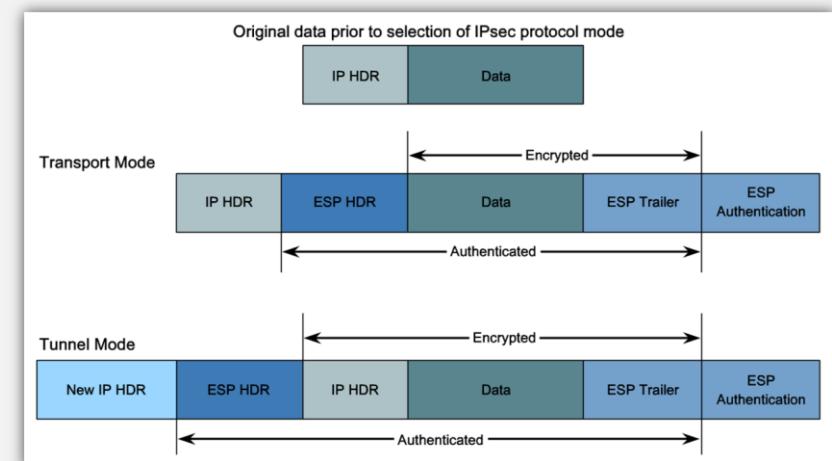
- O IPSec pode usar uma combinação do AH e do ESP



- O ESP não inclui no cálculo do ICV o cabeçalho IP (só inclui o que está entre o cabeçalho e a cauda ESP).
- O AH por seu turno inclui a maior parte da informação presente no cabeçalho IP para o cálculo do seu ICV.

IPSec - Modos de operação

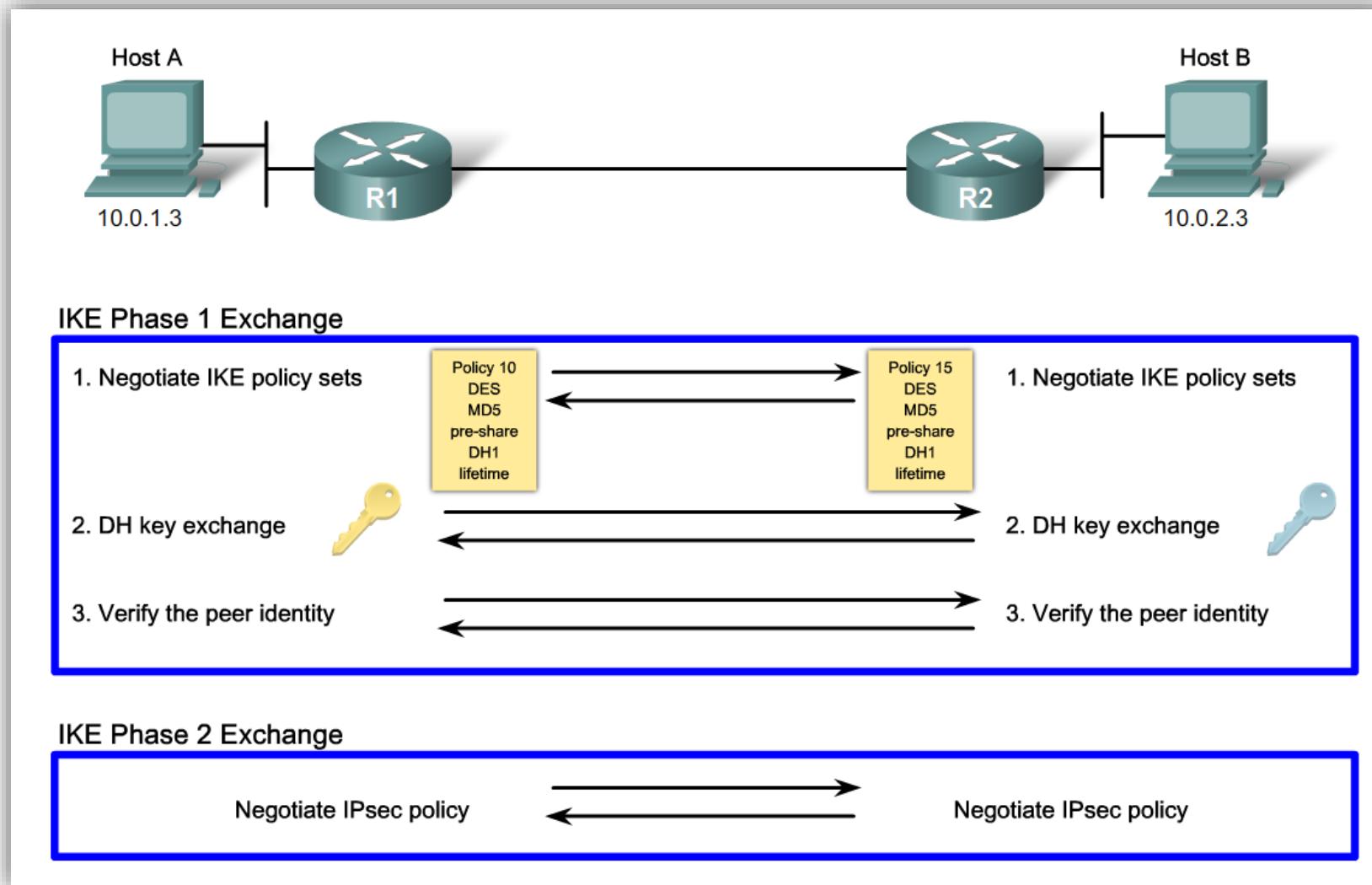
- O IPSec pode operar em dois modos
 - **Transport mode - Modo de transporte**
 - Usado para proteger a comunicação entre dois computadores de uma rede.
 - Os dois computadores têm que suportar IPSec, mas os equipamentos intermediários não necessitam de suportar.
 - Cabeçalho do datagrama IP é mantido.
 - Usados endereços originais (globais).
 - Alguns campos do cabeçalho não são protegidos.
 - **Tunnel mode - Modo de túnel**
 - Usado para proteger a comunicação de WANs e, particularmente, VPNs.
 - Os dois computadores não precisam de suportar IPSec.
 - Os routers dos dois lados da WAN necessitam de suportar IPSec.
 - Datagrama original encapsulado dentro do novo pacote.
 - Protege completamente o datagrama original.
 - Datagrama original pode ter endereços privados.



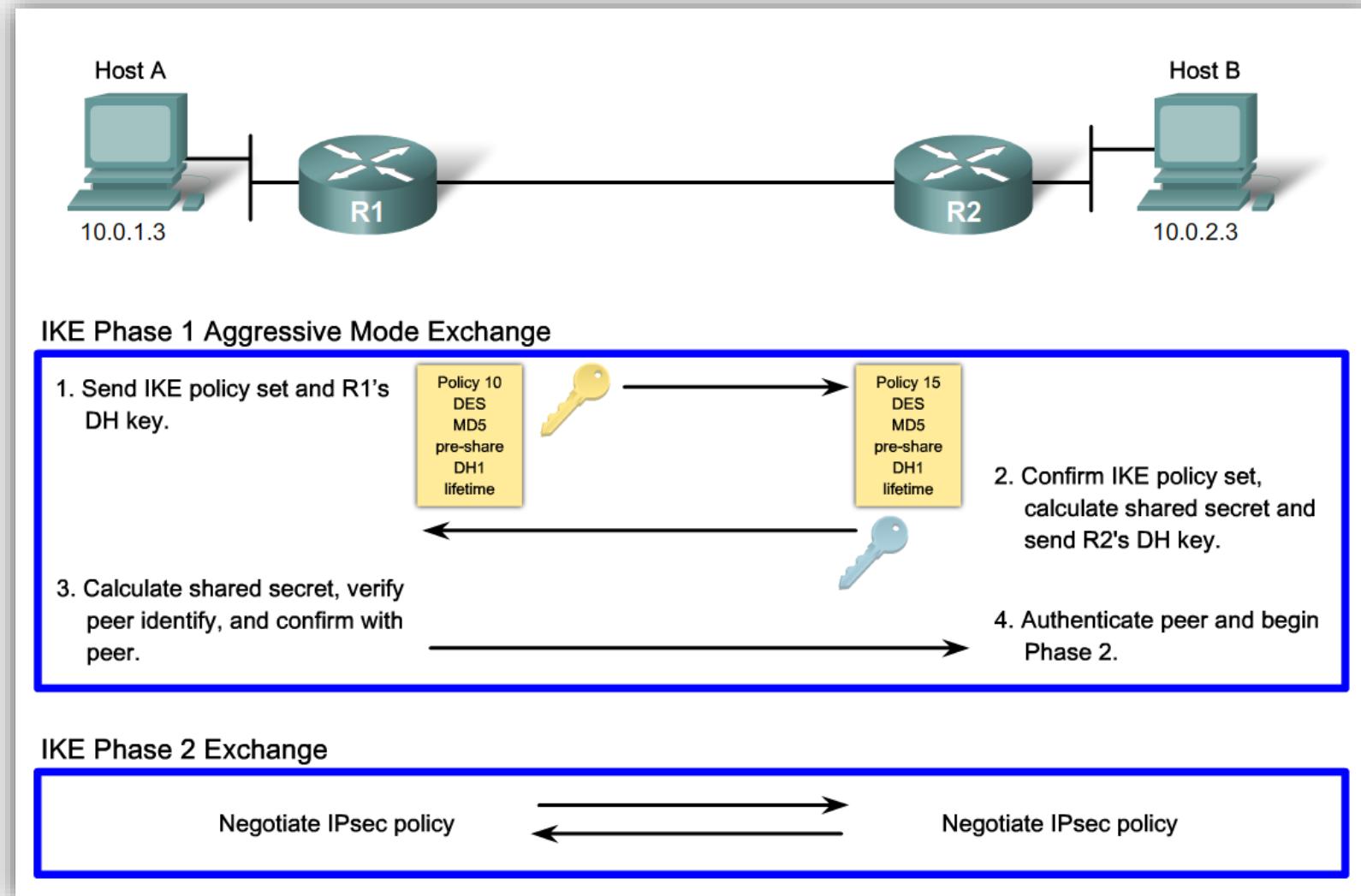
Internet Key Exchange (IKE)

- Usado para negociação dos parâmetros e chaves do IPSec.
- É um protocolo híbrido baseado em framework, definido pelo Internet Security Association and Key ManengementProtocol – ISAKMP.
- O conjunto de parâmetros negociados entre dois dispositivos é designado por Security Association (SA).
- Utiliza o porto UDP 500.

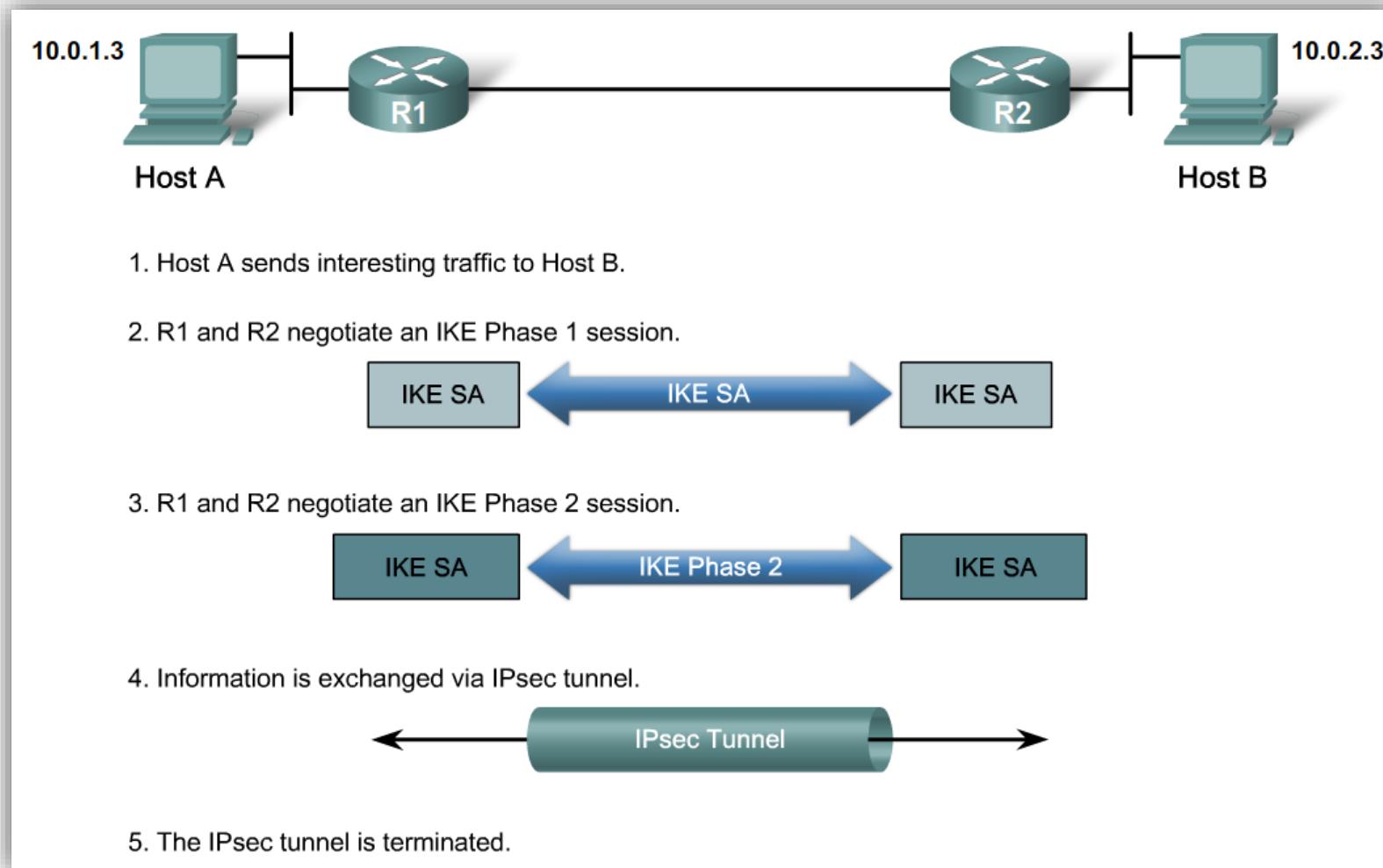
Funcionamento IKE



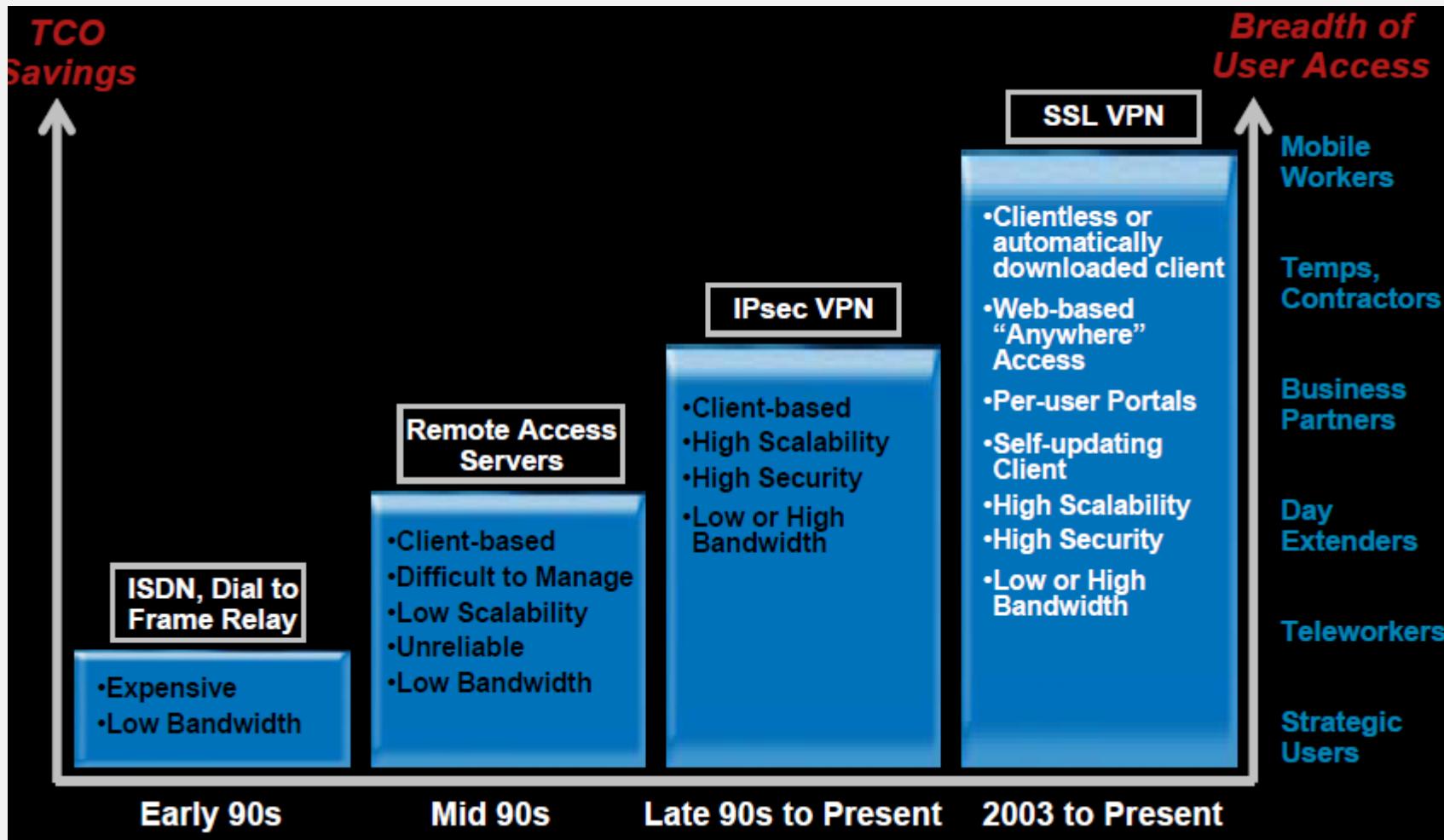
Funcionamento IKE (Aggressive mode)



Ciclo de vida de um túnel IPSec



Acesso remoto - evolução



VPN - SSL

- O protocolo Secure Sockets Layer (SSL) foi criado pela *Netscape Communications Corporation*, estando atualmente implementado em todos os browsers.
- Começou por ser um modo de assegurar a segurança das transações de comércio eletrónico, tornou-se uma alternativa de baixo custo ao protocolo IPSec utilizado nas redes privadas virtuais.
- O protocolo SSL baseia-se em certificados – cartões digitais de identificação que são passados entre o servidor e o cliente.
- A simplicidade do protocolo SSL traduz-se na facilidade de instalação e redução de custos no longo prazo devido a um suporte mais simples, por oposição ao protocolo IPSec VPN que requer um cliente dedicado em cada equipamento remoto.

VPN-SSL

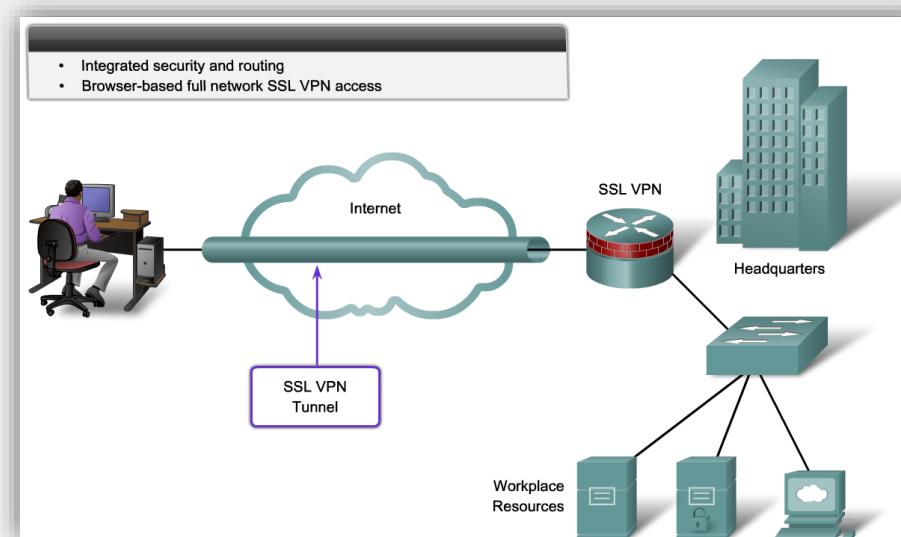
- “As empresas estão interessadas na tecnologia SSL VPN porque os browsers podem detetá-la. Isto torna esta tecnologia mais flexível do que o protocolo IPSec, que requer um cliente de software separado nos equipamentos remotos” sublinha o estudo do Gartner.

VPN - SSL

- A restrição da tecnologia SSL de apenas poder suportar aplicações Web foi um obstáculo inicial. Tal afastou alguns dos potenciais clientes cujos utilizadores necessitavam de aceder a aplicações cliente-servidor tradicionais (por exemplo acesso a aplicação VB).
- O crescimento das redes Wi-Fi no interior das organizações empresariais veio auxiliar a penetração da tecnologia SSL VPN. Com os problemas de segurança das redes Wi-Fi que possibilitaram a entrada ilegal nas redes corporativas, os especialistas em segurança pensaram um meio de reduzir o acesso através dos pontos de acesso wireless.
- Como as VPN preenchiam os requisitos porque podiam ser adicionadas às implementações *wireless* existentes para autenticar utilizadores na rede de comunicações e encriptar o tráfego à medida que viajava pelo ar as VPN-SSL eram atrativas e conheceram um grande desenvolvimento.

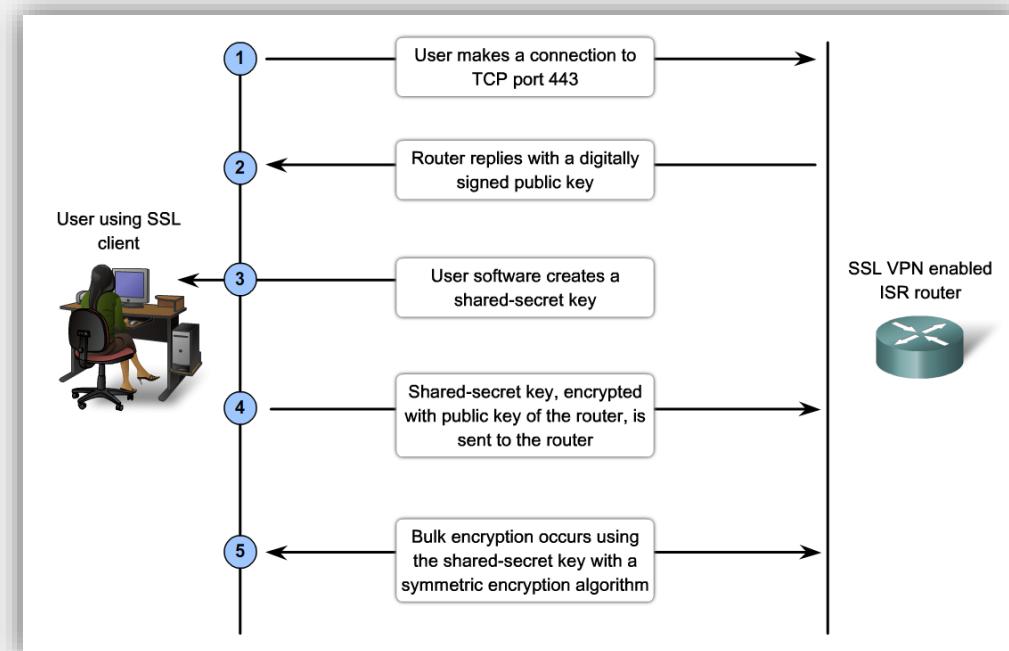
VPN - SSL

- Uma das principais vantagens é a utilização de protocolos de suporte que, normalmente, não estão bloqueados nas *firewall*:
 - Utiliza TCP, porto 443 (HTTPS)
- Suporta métodos “fortes” de autenticação como é o caso do EAP-TLS.
- Encriptação - 40-bit ou 128-bit RC4



VPN - SSL

1. O cliente liga-se ao site protegido por SSL e pede-lhe que se autentique. O cliente envia igualmente a lista dos sistemas criptográficos que suporta.
2. Quando o servidor recebe o pedido, envia um certificado, contendo a chave pública do servidor, assinado por uma autoridade de certificação (CA), bem como o nome do sistema criptográfico usado.
3. O cliente por sua vez verifica a validade e autenticidade do certificado, e cria uma chave secreta aleatória, em seguida encripta essa chave secreta com a chave pública do servidor, e envia o resultado para o servidor.
4. O servidor decifra a chave de sessão com a sua chave privada. Assim, as duas entidades estão na posse de uma chave comum da qual são os únicos conhecedores e a partir dessa chave são realizadas o resto das transações.

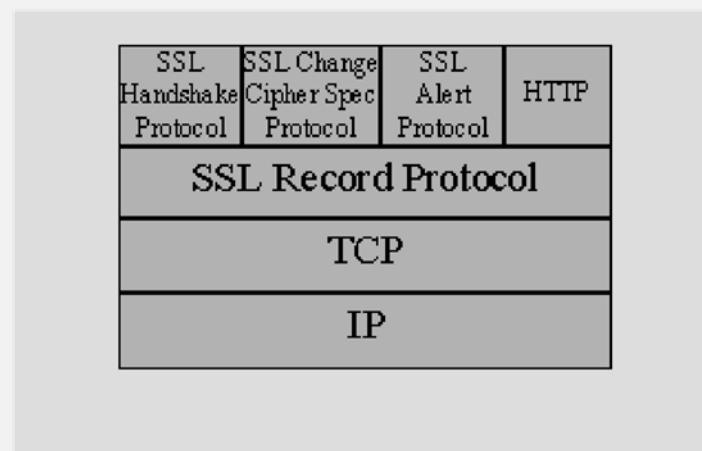


Tipos

- ***Clientless*** – fornece um acesso seguro a recursos privados e acesso a conteúdos. Este modo é utilizado quando o recurso desejado é acessível utilizando um browser tais como acesso à Internet, base de dados e aplicações on-line web.
- ***Thin Client (port-forwarding Java applet)*** – estende as capacidades de criptografia e permite o acesso remoto web a aplicações TCP como Post Office Protocol version 3 (POP3), Simple Mail Transfer Protocol (SMTP), Internet Message Access protocol (IMAP), Telnet, e Secure Shell (SSH).
- ***Tunnel Mode*** – é baseado na instalação de um cliente que permite o estabelecimento de um túnel entre o cliente e o servidor e assim o acesso a todas as aplicações.

VPN-SSL - Protocolos

- O protocolo SSL é dividido em duas Camadas, sendo uma de mais baixo nível que trabalha com o protocolo de transporte que é denominado protocolo *Record*.
- Este protocolo é responsável por encapsular os dados das camadas superiores em pacotes compactados e cifrados e encaminhá-los à camada de transporte.
- Na camada superior, encontra-se o protocolo de *Handshake*, o CCSP (*Change Cipher Spec Protocol*) e o *Alert Protocol*.



VPN-SSL - Protocolos

- O protocolo *Record SSL* fornece serviços de confiabilidade e integridade de mensagens nas ligações SSL.
- Define um conjunto de formatos e procedimentos pelos quais as mensagens da camada de aplicação são fragmentadas ou misturadas em blocos de um tamanho adequado para as próximas etapas.
- Fornece procedimentos de compactação, proteção, criptografia para as mensagens que são passadas para a camada inferior

VPN-SSL - Protocolos

- O **Protocolo Handshake** é responsável por manter a consistência dos estados de uma sessão tanto no cliente quanto no servidor.
- Os dados que formam uma sessão SSL são os seguintes:
 - **session ID** é um valor arbitrário escolhido pelo servidor para identificar a sessão;
 - **peer certificate** é usado para certificar uma organização. Está no formato X.509 e entre outras coisas contem a chave pública da entidade que está utilizando aquela aplicação;
 - **compression method** é o algoritmo usado na compressão dos dados;
 - **cipherspec** - especifica que conjunto de algoritmos de encriptação e de *hash* utilizados;
 - **mastersecret** - é um segredo de 48 bytes compartilhado pelo servidor e pelo cliente;
 - **isresumable** - é uma *flag* utilizada para indicar se a sessão pode ou não ser retomada ao iniciar uma nova conexão.

VPN-SSL - Protocolos

- O **protocolo *ChangeCipherSpec*** é responsável por sinalizar alguma modificação nas estratégias ou parâmetros de segurança utilizados
- Formado por uma única mensagem, a *change_cipher_spec*.
- Quando uma das partes do protocolo recebe uma mensagem *change_cipher_spec* durante o processo de *Handshake*, automaticamente troca as informações do estado atual de leitura pelos dados do estado pendente de leitura.

VPN-SSL - Protocolos

- O **Protocolo Alert** tem como responsabilidade o envio de alerta para o outro lado da ligação por cada erro gerado.
- Dependendo do nível do erro, a ligação pode ser abortada e as mensagens de alerta serão tratadas como mensagens normais sendo compactadas e encriptadas.
- Os níveis das mensagens de alerta são *warnings* e *fatal*s.
 - Os *warnings* são simples avisos que informam que alguma coisa não normal aconteceu ou foi detectada.
 - Quando são do tipo *fatal*s são apagados todos os dados daquela ligação.

IPSec versus SSL

- Nos quadros seguintes são apresentados as comparações/diferenças entre o IPSec e o SSL

	SSL VPN	IPSec VPN
Aplicação	Aplicações que suportem web browser, e-mail e compartilhamento de arquivos.	Serviços baseados em serviços IP.
Encriptação	Forte, porém variável - depende de como o web browser foi configurado.	Forte e consistente - a encriptação é amarrada a aplicação.
Autenticação	E variável - pode se usar uma ou duas formas de autenticação. Pode ser feita usando tokens e certificação digital.	E forte - pode se usar duas formas de autenticação, utilizando tokens e certificação digital.
Segurança	Moderada - pois com qualquer computador é possível estabelecer o túnel VPN.	Forte - devido ao fato da aplicação ser amarrada a um computador/usuário e uma aplicação específicos.
Facilidade de Utilização	Muito alta - o usuário precisa se familiarizar com o web browser.	Baixa - é preciso que usuários tenha conhecimento de instalação do software IPSec
Complexidade	Moderada	Alta
Custo	Baixo - pois não requer software em específico.	Alto - pois requer vários níveis de configuração.
Escalabilidade	Alta - facilidade em sua implementação.	Muito alta - funciona independente da aplicação.

IPSec versus SSL

	VPN - baseado em SSL/TLS	VPN - baseado em IPSec
Aplicações Cliente/Servidor	Sim	Sim
Aplicações Legadas	Sim	Sim
Aplicações HTTP	Sim	Sim
<i>File sharing</i>	Sim	Sim
Aplicações em Mainframe	Sim	Sim
<i>Terminal servers</i>	Sim	Sim
Dependência aplicação de <i>Server socket</i>	Sim	Sim
Aplicações <i>Web</i>	Sim	Sim
Conteúdo de <i>Intranet</i>	Sim	Sim
Voz sobre IP	Não	Sim
<i>File Servers</i>	Sim	Sim
Controle de acesso para Intranets e <i>Extranets</i>	Sim	Não
<i>Email</i>	Sim	Sim

Fonte: (ARRAY NETWORKS)

IPSec versus SSL

	VPN - baseado em IPSEC	VPN - baseado em SSL
Tipo de conexão	Fixa	Transitória
Tipo de dispositivo	Dispositivo Gerenciado	Vários dispositivos
Tipo de Acesso	site-to-site	Remoto
Controle de Acesso	Firewall	Através de políticas

Fonte:(WITNETWORKS)

IPSec versus SSL

	VPN - baseado em IPSEC	VPN - baseado em SSL
Proxy protection	Não	Sim
Strong user authentication	Proprietário	Sim
Strong central authorization	Limitado	Sim
Supporte à Single Sign-On (SSO)	Não	Sim
Dual/Stacked Authentication	Não	Sim
Proibe a visibilidade de nomes e IP	Não	Sim
Forms-based Authentication	Não	Sim
Controle ao nível de URL	Não	Sim

Fonte: (ISSA – INFORMATION SYSTEMS SECURITY ASSOCIATION)

“A tecnologia SSL VPN substituiu o protocolo IPSec como a escolha mais fácil para acesso casual e ad hoc dos empregados a VPN e para parceiros de negócios, fornecedores e manutenção exterior”, refere o estudo do Gartner

Teletrabalho

“Modalidade de prestação laboral que se processa em local diverso da sede do dador (empregador), recorrendo às tecnologias de informação e das comunicações.”

Teletrabalho

- Com a massificação de tecnologias de banda larga e redes *wireless* torna-se possível trabalhar fora das instalações das empresas.
- Os trabalhadores podem trabalhar em casa ou outros locais como se estivessem no escritório ou na sala ao lado.
- Permite a criação de SOHOs (*Small Offices and Home Offices*)
- Possibilidade de integrar trabalhadores que de outra forma não poderiam contribuir para o valor acrescentado da empresa
- Facilitar a implementação de soluções para satisfazer necessidades de trabalho contínuo

Teletrabalho

- Existem os seguintes tipos:
 - No Domicílio (“*Electronic Home Work*”): é a forma mais descentralizada de trabalho à distância, em que o trabalhador trabalha na sua própria casa utilizando tecnologias da informação de um modo direto (“online”) ou indireto (“offline”);
 - Em Centros (““*Small Offices* ”): traduz-se na atividade exercida em unidades organizacionais geograficamente separadas do estabelecimento principal, mas ligadas a este por meios telemáticos;
 - Móvel (“*Mobile Work*”): atividade exercida à distância por trabalhadores “itinerantes ou nómadas”, permanentemente conectados com a empresa por via telemática;
 - Em Tele Centros (“*Neighbourhood Work Center*”): espaços organizacionais implantados próximo do domicílio dos trabalhadores, equipados com material telemático partilhado por colaboradores de diversas empresas ou agentes autónomos.

Benefícios do teletrabalho

- Para o trabalhador
 - Maior disponibilidade para sua vida familiar.
 - Diminuição do stress e aumento do bem estar.
 - Elimina os problemas relacionados com deslocação com diminuição dos custos.
 - Redução dos custos de alimentação.
 - Controlar o seu próprio ritmo de trabalho/flexibilidade de horário.
 - Maior autonomia.

Benefícios do teletrabalho

- Para o Empregador
 - Maior flexibilidade na organização do trabalho.
 - Redução dos custos diretos (imobiliário, energia).
 - Combate ao absentismo.
 - Maior flexibilidade de horários.
 - Aumenta as possibilidades de recrutamento de mão de obra especializada.

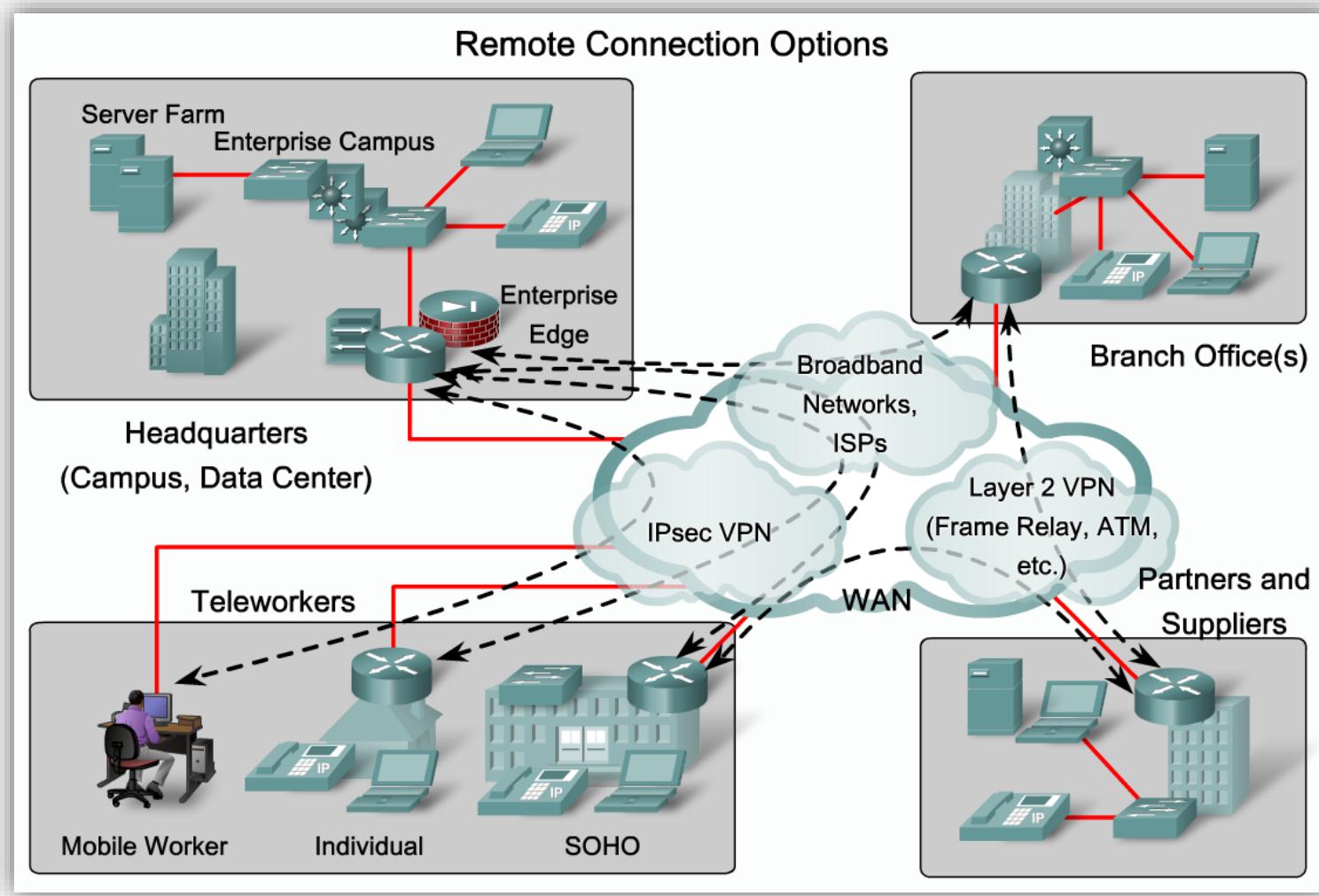
Desvantagens do teletrabalho

- Para o trabalhador
 - Falta de integração com o relacionamento entre colegas.
 - Isolamento social e profissional.
 - Dificuldade em separar a vida profissional e pessoal.
 - Problemas de metodologia/autodisciplina.
 - O espaço comum ao trabalho e à família pode gerar conflitos.

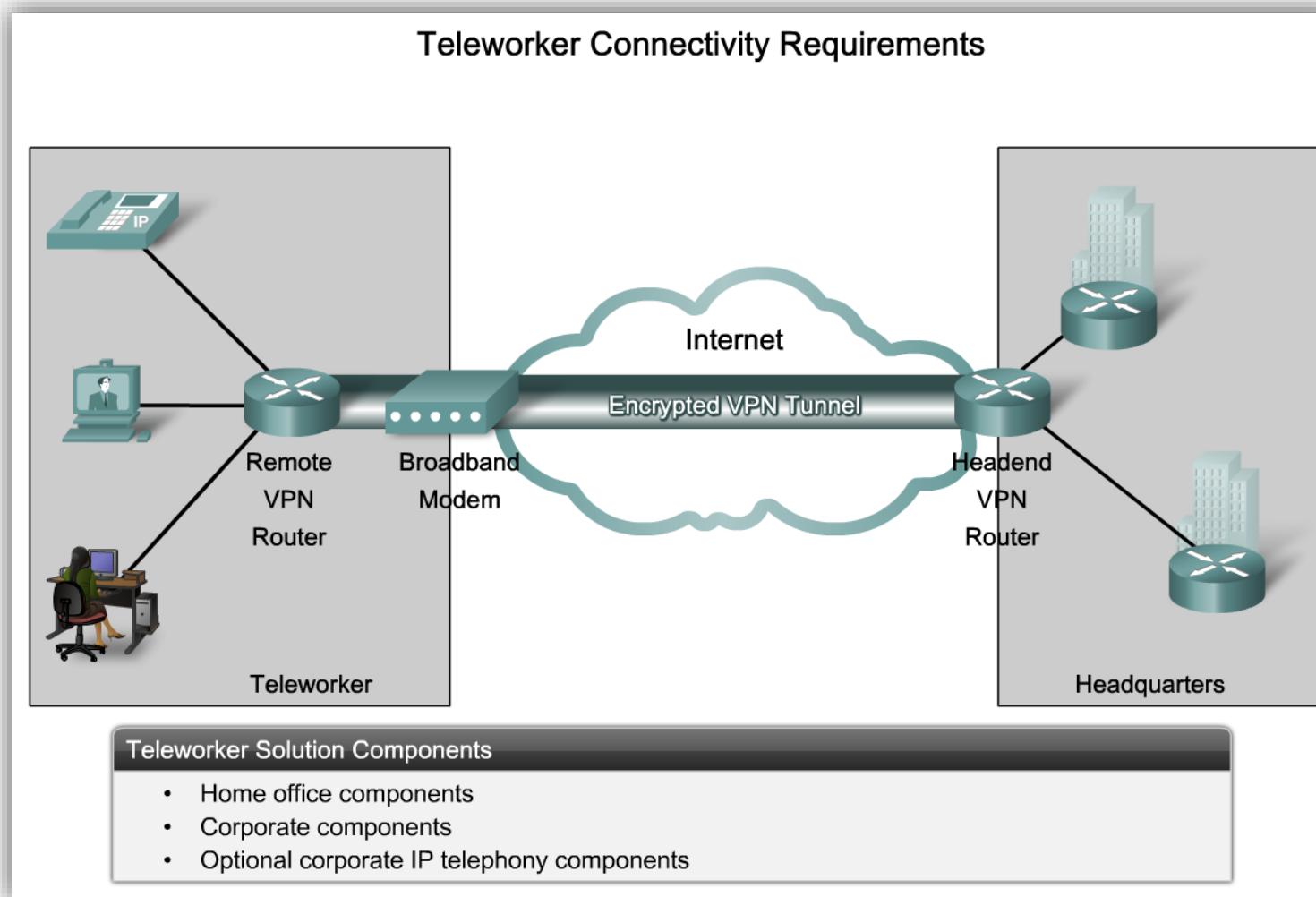
Desvantagens do teletrabalho

- Para o empregador
 - Resistência à mudança no momento da implementação.
 - Dificuldade em supervisionar o trabalho.
 - Problema de motivação dos trabalhadores.
 - Problemas na proteção de dados da empresa.
 - Diminuição da coesão n seio da empresa.
 - Problemas ao implementar o sistema de avaliação de desempenho.

Tecnologias de ligação



Componentes necessários



Dúvidas



Referencias

- www.cisco.com
- <http://pt.wikipedia.org/>
- Segurança em Redes IP, Faculdade de Engenharia da Universidade do Porto
- <http://www.computerworld.com.pt/2010/03/25/ssl-vpn-2/> - acedido em maio de 2021.
- <http://www.vivaolinux.com.br/artigo/VPN-IPSec-vs-SSL?pagina=5> - acedido em maio de 2021.
- <http://www.f5.com/> - acedido em maio de 2021.
- <http://www.cisco.com> – acedido em maio de 2021.
- <https://tools.ietf.org/html/rfc6071> -- acedido em maio de 2020.
- “Comparando o uso do IPSEC e do SSL/TLS em VPN”, Marcelo Fontes, 2010