

Camada de Rede (Protocolos de Suporte)

Redes e Serviços

**Licenciatura em Engenharia Informática
DETI-UA**



universidade de aveiro

deti.ua.pt

DHCP

Dynamic Host Configuration Protocol (DHCP)

↳ Configura tudo automaticamente ... e.g.: internet da UA

- Serviço de atribuição dinâmica de endereços IP a terminais
- Segue uma filosofia cliente-servidor
- Aluguer de endereços
- Configuração dos terminais com informação de máscara da rede, default gateway, servidores de DNS, servidores de WINS e domínio DNS

↳ Não é só o ip!



Configuração de um servidor DHCP

- Gama de endereços
 - ◆ Conjunto de endereços IP definido por um endereço inicial e um endereço final
- Gama(s) de exclusão
 - ◆ Conjuntos de endereços IP que se querem excluir
- Endereços reservados
 - ◆ Endereços IP atribuídos de uma forma permanente a endereços MAC
- Duração dos alugueres



Protocolo DHCP (IETF RFC 2131)

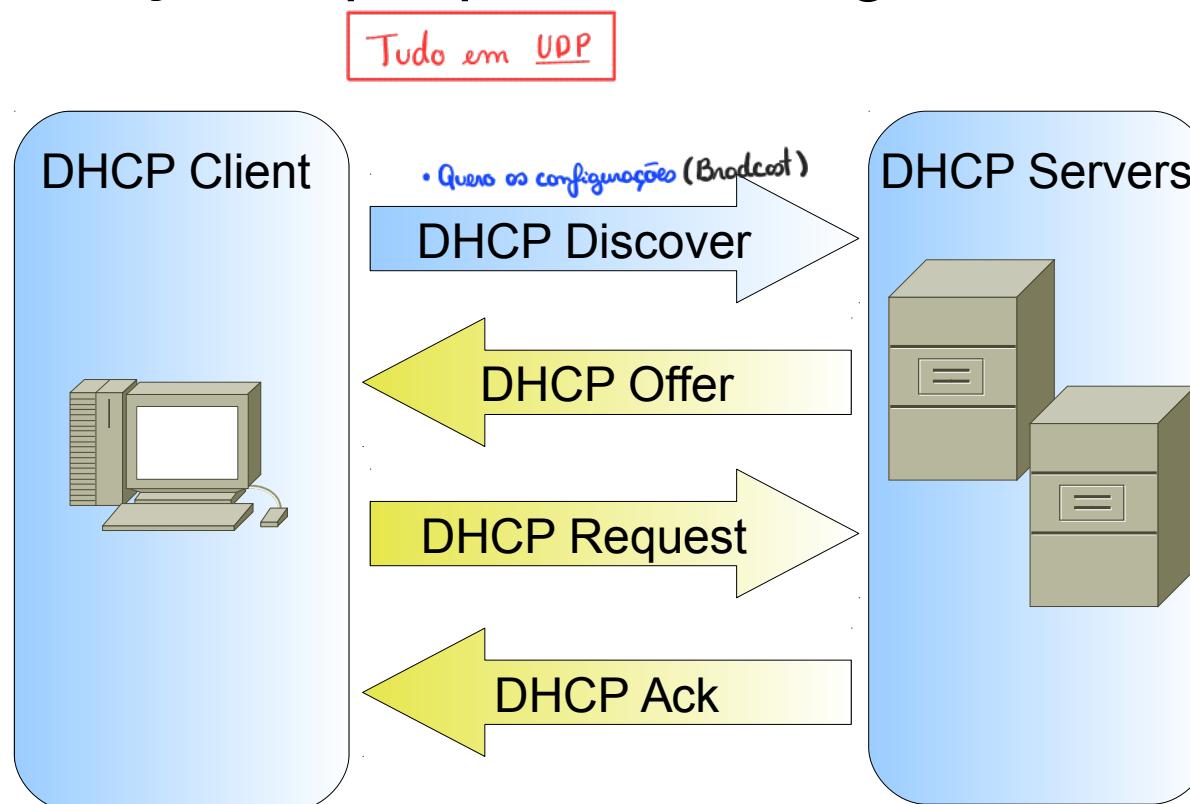
Configuração vinda de um servidor! //

- Extensão *Bootstrap Protocol*, BOOTP, (RFC 1542)
 - ◆ Corre sobre o UDP
• Não é TCP! Número de porto do Servidor: 67
Número de porto do Cliente: 68
 - ◆ O BOOTP permite que um terminal sem disco descubra o seu endereço IP, um endereço de um servidor e o nome de um ficheiro a pedir ao servidor para ser copiado para memória e executado localmente.
- Protocolo de aluguer em quatro fases:
 - ◆ *Discover*
 - ◆ *Offer*
 - ◆ *Request*
 - ◆ *Acknowledge*



1^a Fase: *Discover*

A mensagem *DHCP Discover* é encapsulada num pacote *BootP Request*. Serve para descobrir os servidores de DHCP existentes na rede. O cliente pode também indicar qual o endereço IP que pretende alugar.



DHCP Discover

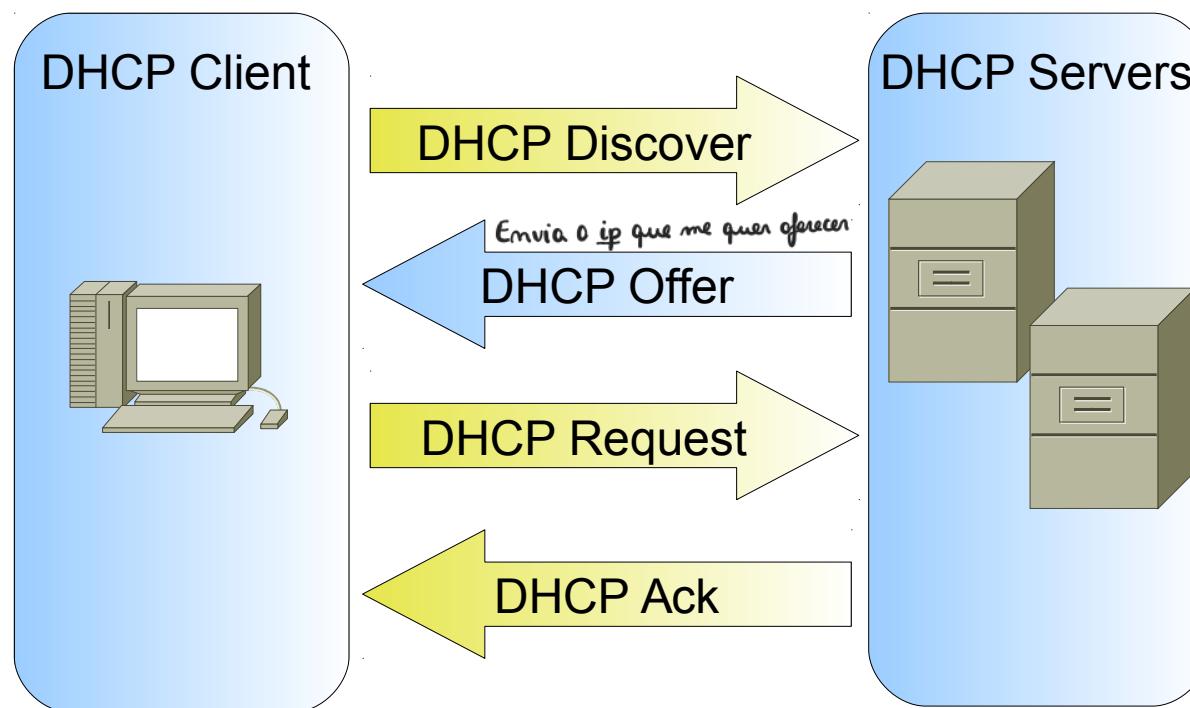
No.	Time	Source	Destination	Protocol	Info
1326	20.269579	0.0.0.0	255.255.255.255	DHCP	DHCP Discover
1337	20.561380	193.136.92.65	193.136.93.228	DHCP	DHCP Offer
1338	20.561592	0.0.0.0	255.255.255.255	DHCP	DHCP Request
1340	20.569560	193.136.92.65	193.136.93.228	DHCP	DHCP ACK

```
▶ Frame 1326 (342 bytes on wire, 342 bytes captured)
▶ Ethernet II, Src: 00:1d:ba:c0:a2:8e (00:1d:ba:c0:a2:8e), Dst: ff:ff:ff:ff:ff:ff (ff
▶ Internet Protocol, Src: 0.0.0.0 (0.0.0.0), Dst: 255.255.255.255 (255.255.255.255)
▶ User Datagram Protocol, Src Port: bootpc (68), Dst Port: bootps (67)
▽ Bootstrap Protocol
    Message type: Boot Request (1)
    Hardware type: Ethernet
    Hardware address length: 6
    Hops: 0
    Transaction ID: 0x42f5a54a
    Seconds elapsed: 0
    ▶ Bootp flags: 0x0000 (Unicast)
        Client IP address: 0.0.0.0 (0.0.0.0)
        Your (client) IP address: 0.0.0.0 (0.0.0.0)
        Next server IP address: 0.0.0.0 (0.0.0.0)
        Relay agent IP address: 0.0.0.0 (0.0.0.0)
        Client MAC address: 00:1d:ba:c0:a2:8e (00:1d:ba:c0:a2:8e)
        Client hardware address padding: 000000000000000000000000
        Server host name not given
        Boot file name not given
        Magic cookie: (OK)
        ▶ Option: (t=53,l=1) DHCP Message Type = DHCP Discover
        ▶ Option: (t=50,l=4) Requested IP Address = 192.168.1.71 → Ele pede sempre o ip, que
        ▶ Option: (t=12,l=15) Host Name = "salvador-laptop"
        ▶ Option: (t=55,l=13) Parameter Request List
        End Option
        Padding
```

→ Ele pede sempre o ip, que tinha anteriormente, para ver se coda

2^a Fase: *Offer*

A mensagem *DHCP Offer* é encapsulada num pacote *BootP Reply*. Cada servidor indica um endereço IP para ser alugado (se possível, os servidores respeitam a preferência do cliente).



DHCP Offer

No.	Time	Source	Destination	Protocol	Info
1326	20.269579	0.0.0.0	255.255.255.255	DHCP	DHCP Discover
1337	20.561380	193.136.92.65	193.136.93.228	DHCP	DHCP Offer
1338	20.561592	0.0.0.0	255.255.255.255	DHCP	DHCP Request
1340	20.569560	193.136.92.65	193.136.93.228	DHCP	DHCP ACK

- ▷ Frame 1337 (342 bytes on wire, 342 bytes captured)
- ▷ Ethernet II, Src: 00:d0:b7:17:5b:6d (00:d0:b7:17:5b:6d), Dst: 00:1d:ba:c0:a2:8e (00:1d:ba:c0:a2:8e)
- ▷ Internet Protocol, Src: 193.136.92.65 (193.136.92.65), Dst: 193.136.93.228 (193.136.93.228)
- ▷ User Datagram Protocol, Src Port: bootps (67), Dst Port: bootpc (68)
- ▽ Bootstrap Protocol

Message type: Boot Reply (2)

Hardware type: Ethernet

Hardware address length: 6

Hops: 0

Transaction ID: 0x42f5a54a

Seconds elapsed: 0

▷ Bootp flags: 0x0000 (Unicast)

Client IP address: 0.0.0.0 (0.0.0.0)

Your (client) IP address: 193.136.93.228 (193.136.93.228)

O seu ip vai ser...

Next server IP address: 193.136.92.65 (193.136.92.65)

Relay agent IP address: 0.0.0.0 (0.0.0.0)

Client MAC address: 00:1d:ba:c0:a2:8e (00:1d:ba:c0:a2:8e)

Client hardware address padding: 00000000000000000000

Server host name not given

Boot file name not given

Magic cookie: (OK)

▷ Option: (t=53,l=1) DHCP Message Type = DHCP Offer

▷ Option: (t=54,l=4) DHCP Server Identifier = 193.136.92.65

▷ Option: (t=51,l=4) IP Address Lease Time = 10 minutes

Esta configuração olhará 10 minutos ...

▷ Option: (t=1,l=4) Subnet Mask = 255.255.254.0

▷ Option: (t=3,l=4) Router = 193.136.92.1 → Default gateway

Para traduzir nomes
em IP,

▷ Option: (t=15,l=8) Domain Name = "av.it.pt"

▷ Option: (t=6,l=4) Domain Name Server = 193.136.92.65

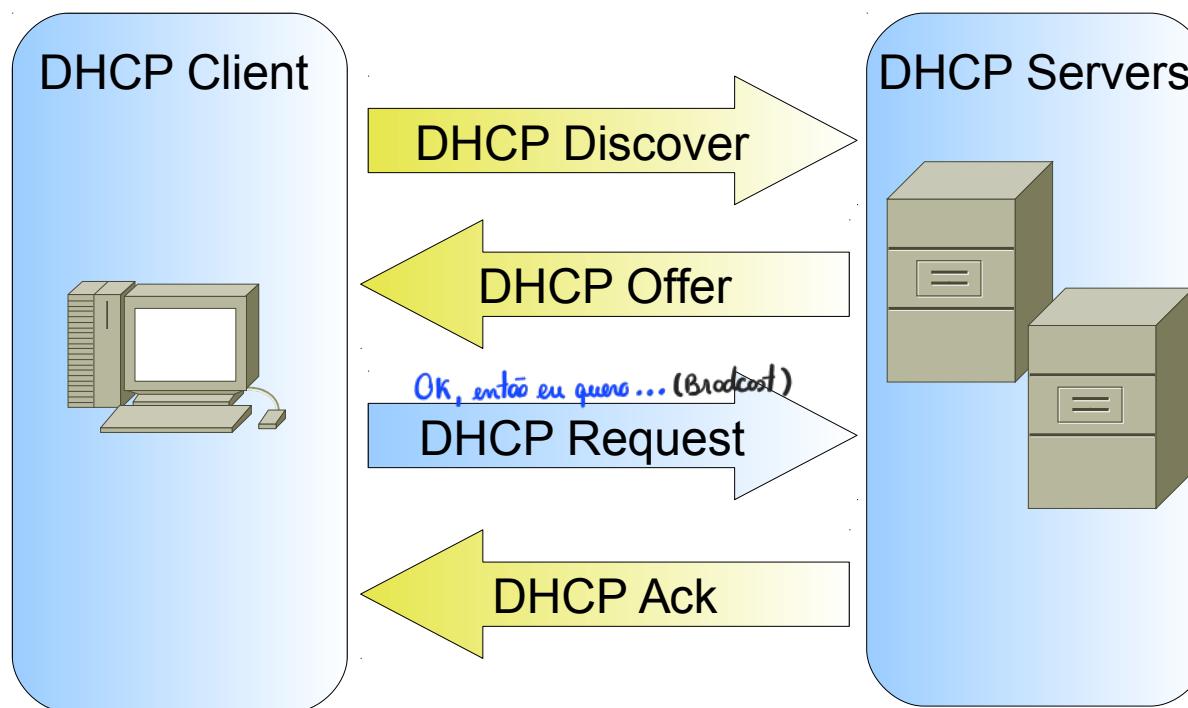
End Option

Padding



3^a Fase: *Request*

A mensagem *DHCP Request* é encapsulada num pacote *BootP Request*. Após escolha entre as possíveis diferentes ofertas recebidas, o cliente indica qual o endereço IP pretendido.



DHCP Request

→ Continua a ser broadcast! Pode haver mais do que um servidor...

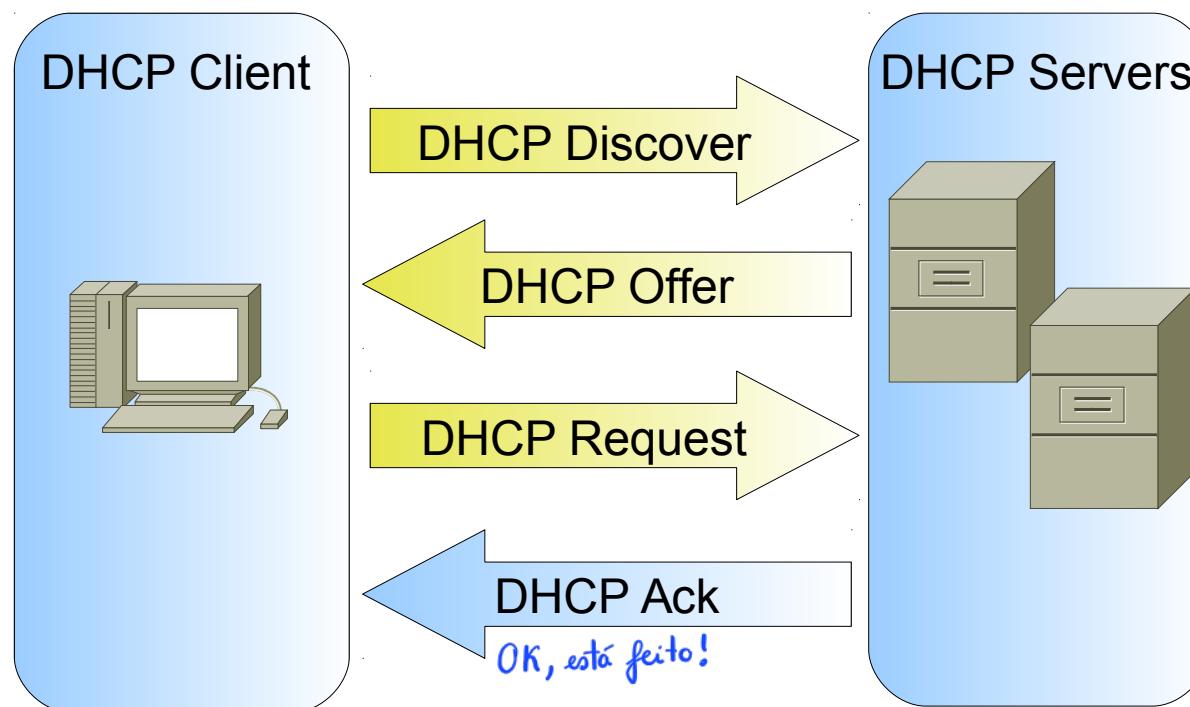
No.	Time	Source	Destination	Protocol	Info
1326	20.269579	0.0.0.0	255.255.255.255	DHCP	
1337	20.561380	193.136.92.65	193.136.93.228	DHCP	
1338	20.561592	0.0.0.0	255.255.255.255	DHCP	
1340	20.569560	193.136.92.65	193.136.93.228	DHCP	

- ▶ Frame 1338 (342 bytes on wire, 342 bytes captured)
- ▶ Ethernet II, Src: 00:1d:ba:c0:a2:8e (00:1d:ba:c0:a2:8e), Dst: ff:ff:ff:ff:ff:ff (ff:ff:ff:ff:ff:ff)
- ▶ Internet Protocol, Src: 0.0.0.0 (0.0.0.0), Dst: 255.255.255.255 (255.255.255.255)
- ▶ User Datagram Protocol, Src Port: bootpc (68), Dst Port: bootps (67)
- ▼ Bootstrap Protocol
 - Message type: Boot Request (1)
 - Hardware type: Ethernet
 - Hardware address length: 6
 - Hops: 0
 - Transaction ID: 0x42f5a54a
 - Seconds elapsed: 0
 - ▶ Bootp flags: 0x0000 (Unicast)
 - Client IP address: 0.0.0.0 (0.0.0.0)
 - Your (client) IP address: 0.0.0.0 (0.0.0.0)
 - Next server IP address: 0.0.0.0 (0.0.0.0)
 - Relay agent IP address: 0.0.0.0 (0.0.0.0)
 - Client MAC address: 00:1d:ba:c0:a2:8e (00:1d:ba:c0:a2:8e)
 - Client hardware address padding: 000000000000000000000000
 - Server host name not given
 - Boot file name not given
 - Magic cookie: (OK)
 - ▶ Option: (t=53,l=1) DHCP Message Type = DHCP Request
 - ▶ Option: (t=54,l=4) DHCP Server Identifier = 193.136.92.65
 - ▶ Option: (t=50,l=4) Requested IP Address = 193.136.93.228 → Endereço oferecido por ele
 - ▶ Option: (t=12,l=15) Host Name = "salvador-laptop"
 - ▶ Option: (t=55,l=13) Parameter Request List
 - End Option
 - Padding



4^a Fase: Acknowledge

A mensagem *DHCP Ack* é encapsulada num pacote *BootP Reply*. O servidor identifica positivamente o aluguer do endereço IP indicado fornecendo simultaneamente outras informações de interesse.



DHCP Ack

→ Confirmação

No.	Time	Source	Destination	Protocol	Info
1326	20.269579	0.0.0.0	255.255.255.255	DHCP	DHCP Discover
1337	20.561380	193.136.92.65	193.136.93.228	DHCP	DHCP Offer
1338	20.561592	0.0.0.0	255.255.255.255	DHCP	DHCP Request
1340	20.569560	193.136.92.65	193.136.93.228	DHCP	DHCP ACK

- ▷ Frame 1340 (342 bytes on wire, 342 bytes captured)
- ▷ Ethernet II, Src: 00:d0:b7:17:5b:6d (00:d0:b7:17:5b:6d), Dst: 00:1d:ba:c0:a2:8e (00:1d:ba:c0:a2:8e)
- ▷ Internet Protocol, Src: 193.136.92.65 (193.136.92.65), Dst: 193.136.93.228 (193.136.93.228)
- ▷ User Datagram Protocol, Src Port: bootps (67), Dst Port: bootpc (68)
- ▽ Bootstrap Protocol

Message type: Boot Reply (2)

Hardware type: Ethernet

Hardware address length: 6

Hops: 0

Transaction ID: 0x42f5a54a

Seconds elapsed: 0

- ▷ Bootp flags: 0x0000 (Unicast)

Client IP address: 0.0.0.0 (0.0.0.0)

Your (client) IP address: 193.136.93.228 (193.136.93.228)

Next server IP address: 193.136.92.65 (193.136.92.65)

Relay agent IP address: 0.0.0.0 (0.0.0.0)

Client MAC address: 00:1d:ba:c0:a2:8e (00:1d:ba:c0:a2:8e)

Client hardware address padding: 000000000000000000000000

Server host name not given

Boot file name not given

Magic cookie: (OK)

- ▷ Option: (t=53,l=1) DHCP Message Type = DHCP ACK
- ▷ Option: (t=54,l=4) DHCP Server Identifier = 193.136.92.65
- ▷ Option: (t=51,l=4) IP Address Lease Time = 10 minutes
- ▷ Option: (t=1,l=4) Subnet Mask = 255.255.254.0
- ▷ Option: (t=3,l=4) Router = 193.136.92.1
- ▷ Option: (t=15,l=8) Domain Name = "av.it.pt"
- ▷ Option: (t=6,l=4) Domain Name Server = 193.136.92.65

End Option

Padding

→ Confirma a atribuição



Protocolo DHCP

- Aluguer de endereços
 - ◆ *T1 Time* (50% do *Lease Time*) – tempo ao fim do qual o terminal deve tentar renovar o aluguer
 - ◆ *T2 Time* (85% do *Lease Time*) – tempo ao fim do qual o terminal deve tentar novamente renovar o aluguer se a primeira tentativa não for bem sucedida ↗ Vai tentar outra vez ...
 - ◆ *Lease Time* – tempo ao fim do qual o terminal deve deixar de usar o endereço IP se o aluguer não for renovado
- Existência de múltiplos servidores DHCP
 - ◆ Vantagem: redundância a falhas de funcionamento
 - ◆ Requisito: gamas disjuntas de endereços nos diferentes servidores
↗ Claro senão corria mal ...



Outras mensagens DHCP

- DHCP Decline: → Não couve bem!
 - ◆ O cliente rejeita a oferta que lhe foi feita e reinicia o processo de aluguer de endereço
- DHCP Nack: → Não aceita o pedido!
 - ◆ O servidor informa que não pode satisfazer o pedido que este lhe fez, através da mensagem DHCP Request
- DHCP Release: → Quando acaba o aluguer!
 - ◆ O cliente informa que pretende terminar o aluguer
- DHCP Inform: → Solicitar um parâmetro específico
 - ◆ O cliente solicita apenas alguns parâmetros (neste caso, o cliente já tem um endereço IP, mas pretende solicitar, por exemplo, o endereço de um servidor DNS)



\$ sudo dhclient

DHCP Release

→ Quando libera

No.	Time	Source	Destination	Protocol	Info
1330	24.011686	193.136.93.228	193.136.92.65	DHCP	DHCP Release

► Frame 1330 (342 bytes on wire, 342 bytes captured)
► Ethernet II, Src: 00:1d:ba:c0:a2:8e (00:1d:ba:c0:a2:8e), Dst: 00:d0:b7:17:5b:6d (00:d0:b7:17:5b:6d)
► Internet Protocol, Src: 193.136.93.228 (193.136.93.228), Dst: 193.136.92.65 (193.136.92.65)
► User Datagram Protocol, Src Port: bootpc (68), Dst Port: bootps (67)
▽ Bootstrap Protocol
 Message type: Boot Request (1)
 Hardware type: Ethernet
 Hardware address length: 6
 Hops: 0
 Transaction ID: 0xc099a870
 Seconds elapsed: 0
 Bootp flags: 0x0000 (Unicast)
 Client IP address: 193.136.93.228 (193.136.93.228)
 Your (client) IP address: 0.0.0.0 (0.0.0.0)
 Next server IP address: 0.0.0.0 (0.0.0.0)
 Relay agent IP address: 0.0.0.0 (0.0.0.0)
 Client MAC address: 00:1d:ba:c0:a2:8e (00:1d:ba:c0:a2:8e)
 Client hardware address padding: 000000000000000000000000
 Server host name not given
 Boot file name not given
 Magic cookie: (OK)
 Option: (t=53,l=1) DHCP Message Type = DHCP Release
 Option: (t=54,l=4) DHCP Server Identifier = 193.136.92.65
 Option: (t=12,l=15) Host Name = "salvador-laptop"
 End Option
 Padding



DHCP Inform

No.	Time	Source	Destination	Protocol	Info
3117	18.9.105.1	193.136.93.122	255.255.255.255	DHCP	DHCP Inform
4107	65.374546	193.136.93.173	255.255.255.255	DHCP	DHCP Inform
5446	86.143470	193.136.93.102	255.255.255.255	DHCP	DHCP Inform

► Frame 4107 (342 bytes on wire, 342 bytes captured)
► Ethernet II, Src: d0:df:9a:cb:d1:3c (d0:df:9a:cb:d1:3c), Dst: ff:ff:ff:ff:ff:ff (ff:ff:ff:ff:ff:ff)
► Internet Protocol, Src: 193.136.93.173 (193.136.93.173), Dst: 255.255.255.255 (255.255.255.255)
► User Datagram Protocol, Src Port: bootpc (68), Dst Port: bootps (67)

▼ Bootstrap Protocol

Message type: Boot Request (1)
Hardware type: Ethernet
Hardware address length: 6
Hops: 0
Transaction ID: 0xfb8eebf9
Seconds elapsed: 0

► Bootp flags: 0x8000 (Broadcast)
Client IP address: 193.136.93.173 (193.136.93.173)
Your (client) IP address: 0.0.0.0 (0.0.0.0)
Next server IP address: 0.0.0.0 (0.0.0.0)
Relay agent IP address: 0.0.0.0 (0.0.0.0)
Client MAC address: d0:df:9a:cb:d1:3c (d0:df:9a:cb:d1:3c)
Client hardware address padding: 000000000000000000000000
Server host name not given
Boot file name not given
Magic cookie: (OK)

► Option: (t=53,l=1) DHCP Message Type = DHCP Inform
► Option: (t=61,l=7) Client identifier
► Option: (t=12,l=7) Host Name = "IT-TOSH"
► Option: (t=60,l=8) Vendor class identifier = "MSFT 5.0"
► Option: (t=55,l=13) Parameter Request List

End Option
Padding

► Option: (t=55,l=13) Parameter Request List
Option: (55) Parameter Request List
Length: 13
Value: 010F03062C2E2F1F2179F92BFC
1 = Subnet Mask
15 = Domain Name
3 = Router
6 = Domain Name Server
44 = NetBIOS over TCP/IP Name Server
46 = NetBIOS over TCP/IP Node Type
47 = NetBIOS over TCP/IP Scope
31 = Perform Router Discover
33 = Static Route
121 = Classless Static Route
249 = Private/Classless Static Route (Microsoft)
43 = Vendor-Specific Information
252 = Private/Proxy autodiscovery

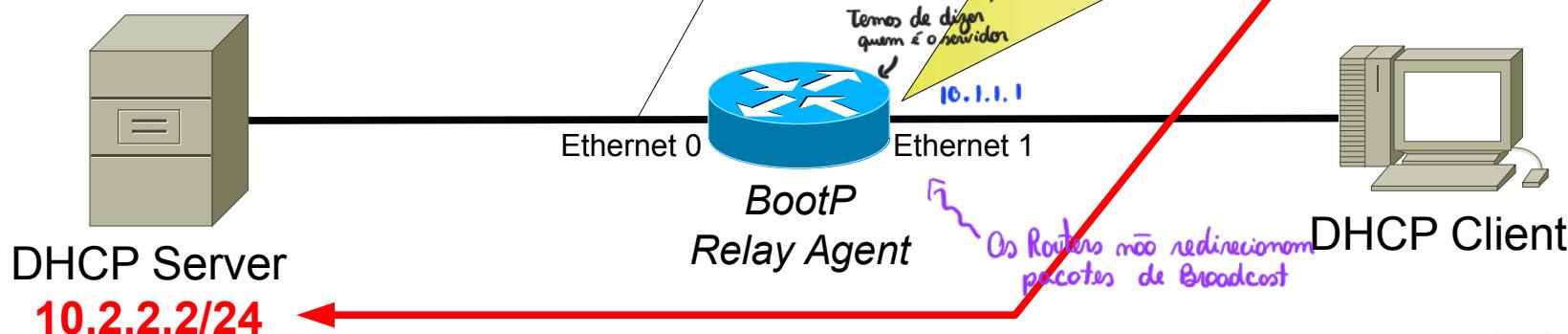
► Quando preciso de alguma coisa envio o DHCP Informe com um destes códigos



Uso de Servidores DHCP em Ambientes Complexos

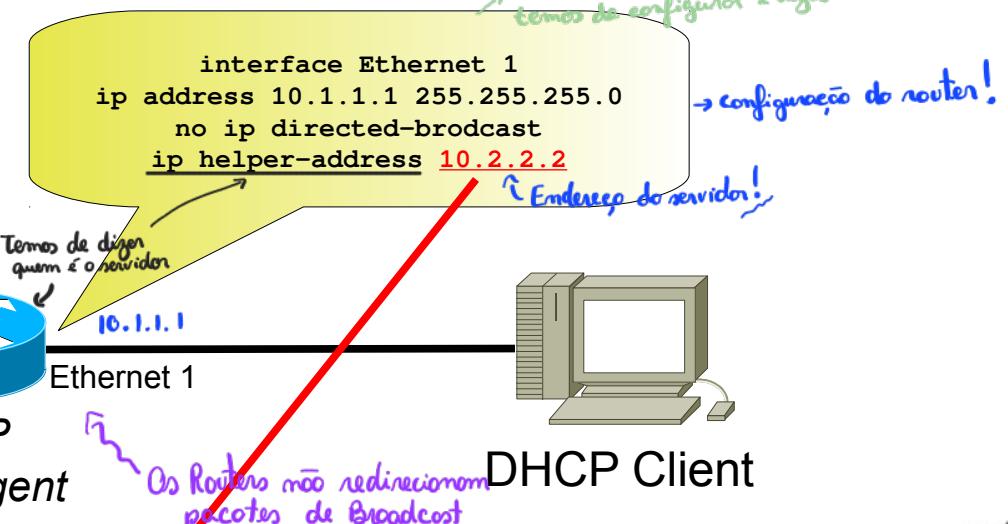
- Em ambientes de rede complexos onde um (ou mais) servidor DHCP fornece endereços a múltiplas redes locais (subredes IP).
- O *gateway* de cada rede local deverá ser configurado como “*BootP Relay Agent*”.
- O router irá redirecionar todos os pacotes DHCP (recebidos em *broadcast*) para o servidor DHCP usando *unicast*.

- Adiciona informação na mensagem com a indicação da rede/interface onde recebeu o pedido.
- As respostas do servidor são reenviadas para o cliente.
- Do ponto de vista do cliente, o *router* comporta-se como um servidor DHCP.



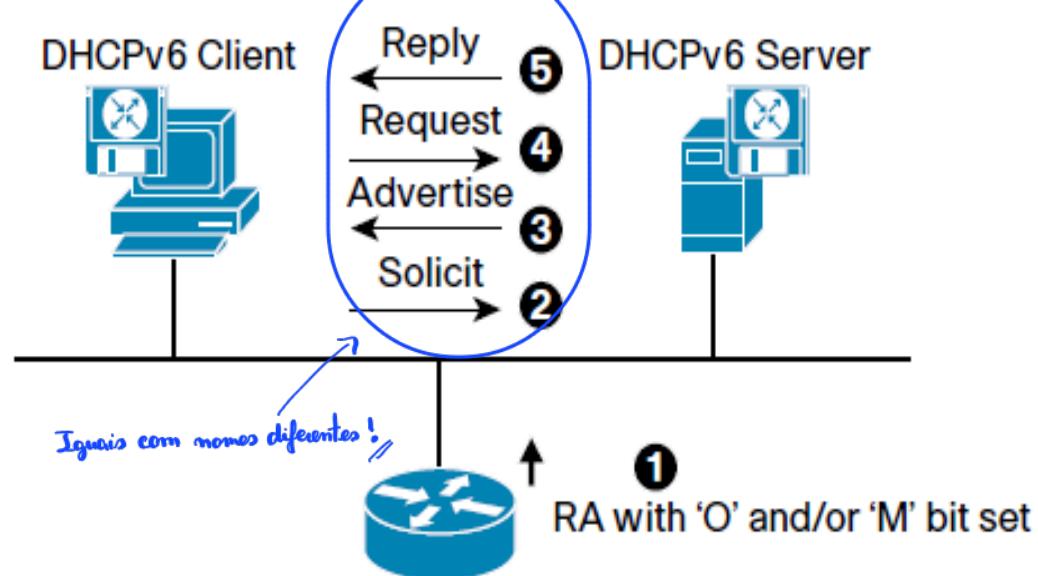
No.	Time	Source	Destination	Protocol	Info
3	2.933744	10.1.1.1	10.2.2.2	DHCP	DHCP Discover
4	5.935516	10.1.1.1	10.2.2.2	DHCP	DHCP Discover
5	8.939088	10.1.1.1	10.2.2.2	DHCP	DHCP Discover

► User Datagram Protocol, Src Port: bootps (67), Dst Port: bootps (67)
▼ Bootstrap Protocol
Message type: Boot Request (1)
Hardware type: Ethernet
Hardware address length: 6
Hops: 1
Transaction ID: 0xd668f173
Seconds elapsed: 0
► Bootp flags: 0x0000 (Unicast)
Client IP address: 0.0.0.0 (0.0.0.0)
Your (client) IP address: 0.0.0.0 (0.0.0.0)
Next server IP address: 0.0.0.0 (0.0.0.0)
Relay agent IP address: 10.1.1.1 (10.1.1.1)
Client MAC address: 00:aa:00:2a:15:00 (00:aa:00:2a:15:00)
Client hardware address padding: 00000000000000000000000000000000
Server host name not given
Boot file name not given
Magic cookie: (OK)
► Option: (t=53,l=1) DHCP Message Type = DHCP Discover
► Option: (t=61,l=7) Client identifier
► Option: (t=12,l=3) Host Name = "box"



DHCPv6

- Usado para obter endereços IPv6 e/ou parâmetros de rede IPv6.
- Conceito similar ao do DHCP para IPv4.
- Um terminal que queira receber quaisquer parâmetros de configuração irá enviar um pedido para detetar os servidores de DHCPv6 disponíveis.
 - ◆ Usando a mensagem “Solicit”.
 - ◆ O endereço de destino da mensagem “Solicit” é um endereço de multicast específico do DHCPv6.
 - ◆ As respostas virão em mensagens “Advertise”.
- De seguida, o cliente DHCPv6 irá enviar um pedido usando uma mensagem “Request”. O servidor de DHCPv6 irá responder com a informação pedida usando uma mensagem “Reply”.
- O relay em DHCPv6 funciona de forma distinta do que no DHCP para IPv4.
 - ◆ O Relay Agent encapsula completamente as mensagens DHCPv6 do cliente numa nova mensagem do tipo RELAY-FORW message. → *um pouco diferente*
 - ◆ Reencaminha esta nova mensagem para o servidor de DHCPv6.
 - ◆ A resposta é feita igualmente usando uma nova mensagem (RELAY-REPL message) que contém encapsulada a mensagem a enviar ao cliente DHCPv6 pelo Relay Agent.



DNS

Domain Name System (DNS)

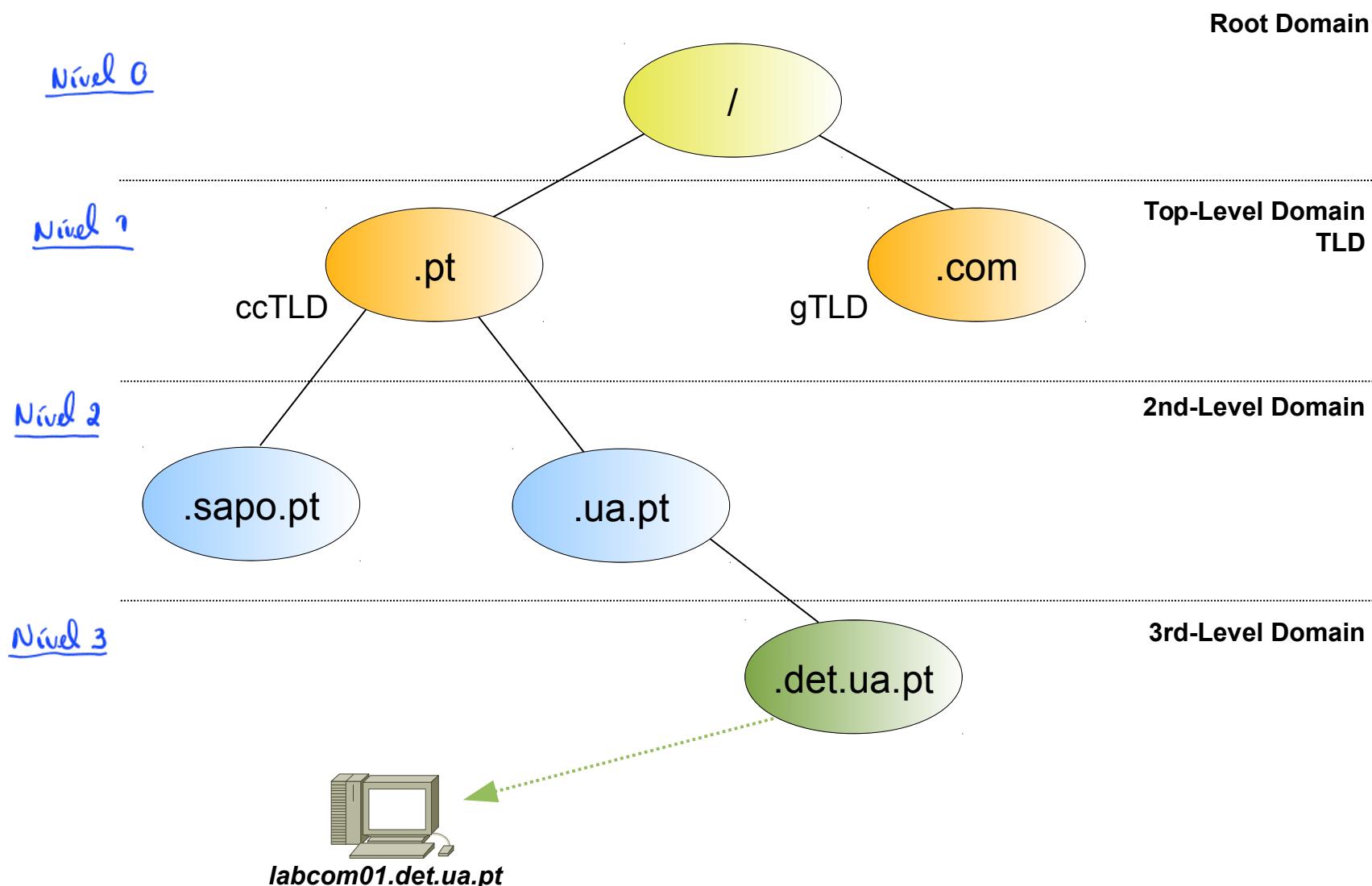
↳ Base de dados distribuída a nível mundial

Converter nomes em ip's

- Distributed database system that facilitates a translation service (resolution) between host names and IP addresses.
- Allows also the translation/resolution between IP addresses and host names
 - The name "DD.CC.BB-AA.in-addr.arpa" allows the resolution of the IPv4 address AA.BB.CC.DD
 - The name 0.0.0.8.b.d.0.1.0.0.2.ip6.arpa allows the resolution of the IPv6 address 2001:0db8:0000::/48
 - Resolution name-ip and ip-name is not symmetrical.
Não vai dar SEMPRE resultados simétricos!!
- Organizes the names in domains according to an hierarchical structure.
- Each DNS system defines one or more zones over which has the resolution authority. → Nós contactamos o servidor do nosso domínio!,,

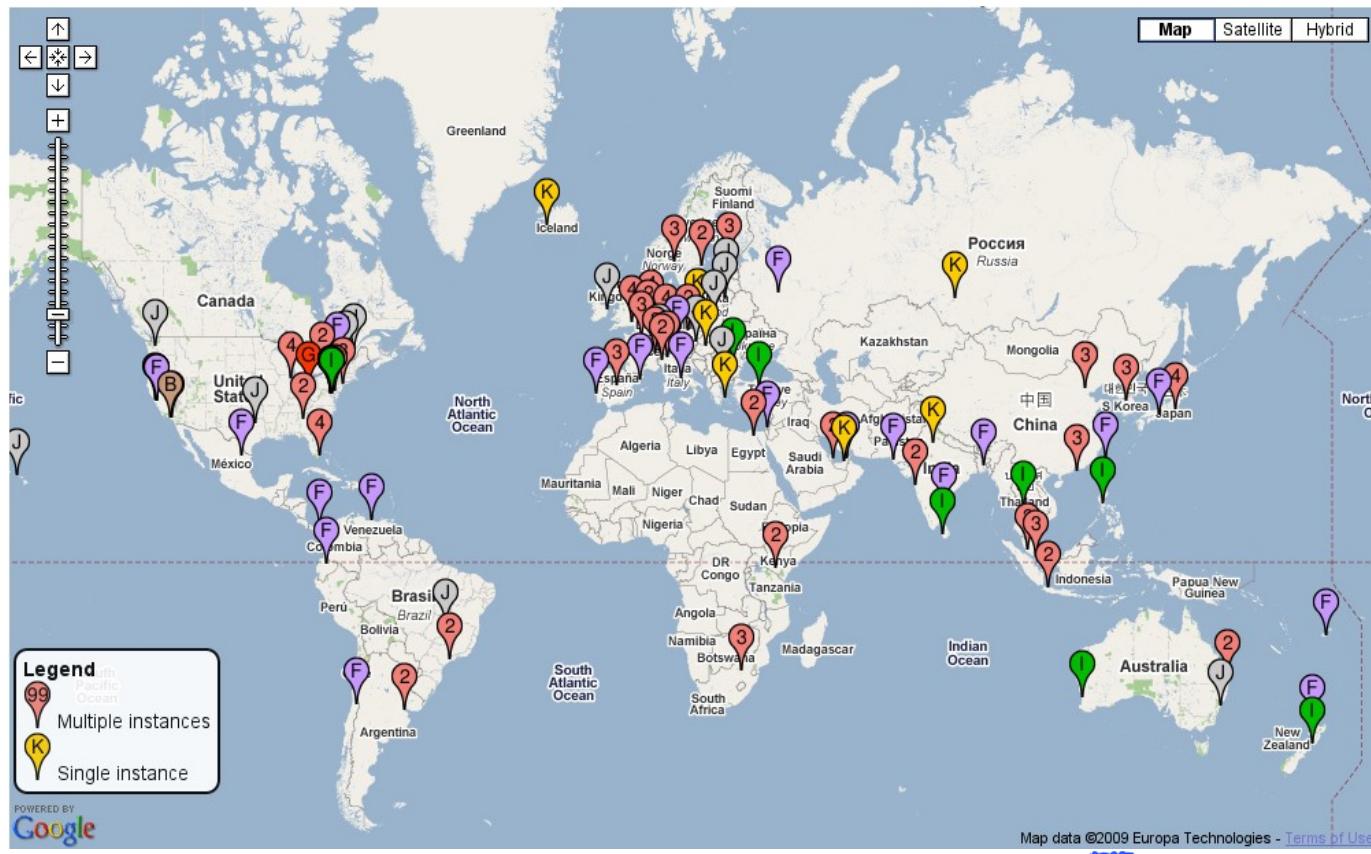


Hierarchical Structure of Domain Names



Root Servers & Root Zone File

- Root servers
- Root Zone File (sample)



.....
COM. NS A.GTLD-SERVERS.NET.
COM. NS G.GTLD-SERVERS.NET.
COM. NS H.GTLD-SERVERS.NET.
COM. NS C.GTLD-SERVERS.NET.

.....
PT. NS NS.DNS.BR.
PT. NS NS2.NIC.FR.
PT. NS NS.DNS.PT.
PT. NS SUNIC.SUNET.SE.
PT. NS NS2.DNS.PT.
PT. NS NS-EXT.ISC.ORG.

.....
NET. NS A.GTLD-SERVERS.NET.
NET. NS G.GTLD-SERVERS.NET.
NET. NS H.GTLD-SERVERS.NET.
NET. NS C.GTLD-SERVERS.NET.

.....
INFO. NS B0.INFO.AFILIAS-NST.ORG.
INFO. NS C0.INFO.AFILIAS-NST.INFO.
INFO. NS D0.INFO.AFILIAS-NST.ORG.



Top-Level Domains (TLD)

- gTLDs (generic TLDs)
 - ◆ .com, .edu, .gov, .mil, .net, .org, .int, .aero, .biz, .coop, .info, .museum, .name, .pro, .cat, .jobs, .mobi, .travel, .tel, .asia
- ccTLDs (country code TLDs)
 - ◆ 2 letter domains that identify a specific country (ISO 3166)
 - ◆ Management is delegated (by ICANN) to a governmental institution from each country.
 - ◆ Those can (re)-delegate to private companies.
 - ◆ Ex: .pt, .es, .us, .fr, etc...
- New gTLDs (under approval)
 - ◆ **.amazon, .app, .apple, .bank, .bet, .blog, .book, .cars, .goog, .goggle, .hotel, ...**



TLD Zone Files (sample)

- .ORG (Public Interest Registry)

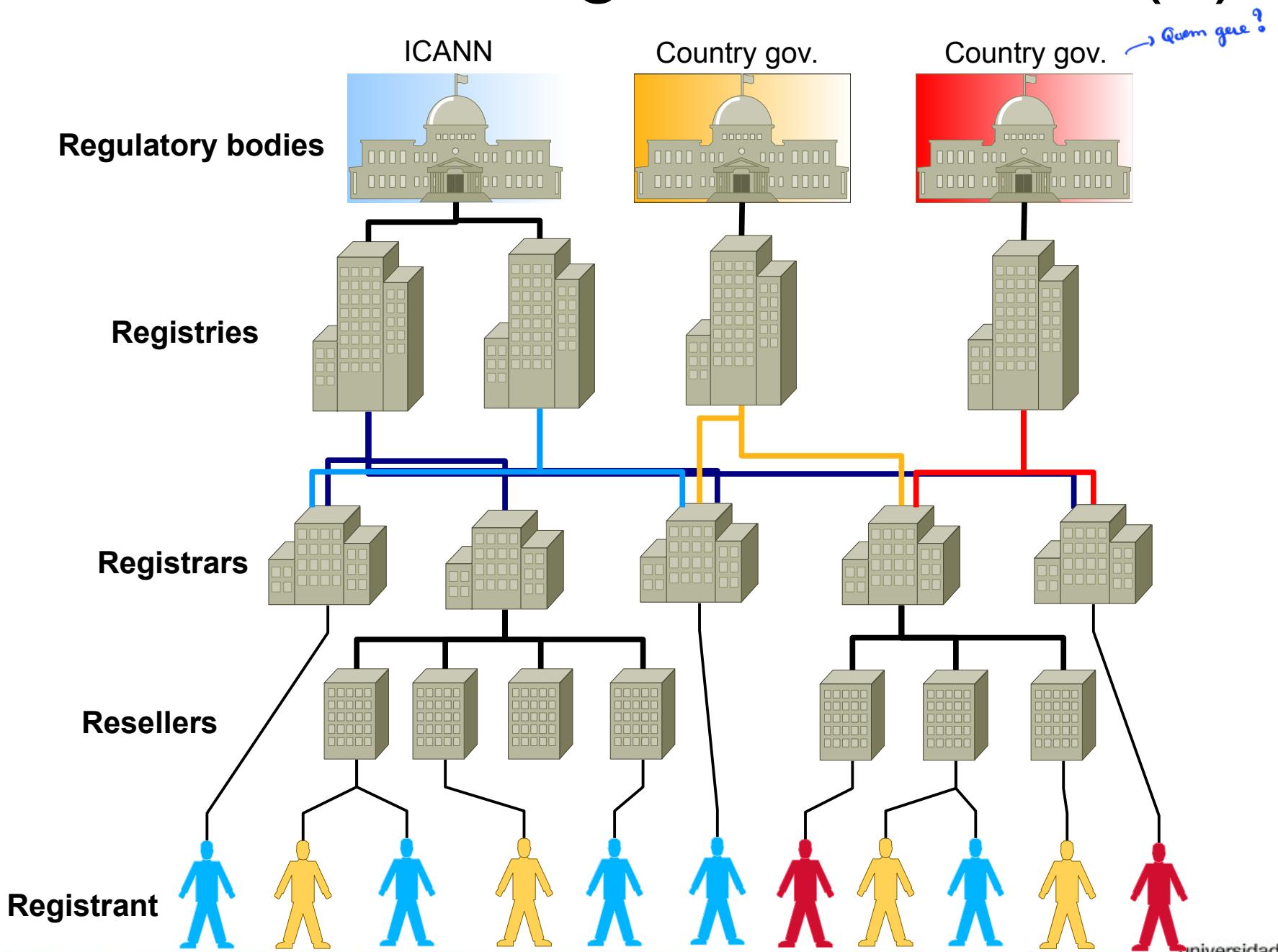
```
.....  
AASELFSTORAGE.ORG. NS DNS02.GPN.REGISTER.COM.  
AASELFSTORAGE.ORG. NS DNS03.GPN.REGISTER.COM.  
AASELFSTORAGE.ORG. NS DNS04.GPN.REGISTER.COM.  
AASELFSTORAGE.ORG. NS DNS05.GPN.REGISTER.COM.  
AASEMI.ORG. NS DPNS1.DNSNAME SERVER.ORG.  
AASEMI.ORG. NS DPNS2.DNSNAME SERVER.ORG.  
AASEMI.ORG. NS DPNS3.DNSNAME SERVER.ORG.  
AASEMI.ORG. NS DPNS4.DNSNAME SERVER.ORG.  
AASEN.ORG. NS NS1.MAILBANK.COM.  
AASEN.ORG. NS NS2.MAILBANK.COM.  
AASENIORMORTGAGE.ORG. NS NS13.DOMAINCONTROL.COM.  
AASENIORMORTGAGE.ORG. NS NS14.DOMAINCONTROL.COM.  
AASENT.ORG. NS NS51.1AND1.COM.  
AASENT.ORG. NS NS52.1AND1.COM.  
AASENTMORTGAGE.ORG. NS NS51.1AND1.COM.  
AASENTMORTGAGE.ORG. NS NS52.1AND1.COM.  
AASENY.ORG. NS NS27.1AND1.COM.  
AASENY.ORG. NS NS28.1AND1.COM.  
AASEP.ORG. NS NS1.CASTIRONCODING.COM.  
AASEP.ORG. NS NS2.CASTIRONCODING.COM.  
AASERV.ORG. NS NS1.RENEWYOURNAME.NET.  
.....
```

- .COM (Verisign)

```
.....  
AMERICANHUNTING NS NS1.HITFARM  
AMERICANHUNTING NS NS2.HITFARM  
ATSCAF NS CBRU.BR.NS.ELS-GMS.ATT.NET.  
ATSCAF NS CMTU.MT.NS.ELS-GMS.ATT.NET.  
ACTIONNETS NS NS.TULSAWEB  
ACTIONNETS NS NS.TIBP  
ACI-APPLICAD NS NS2.WEBNJ.NET.  
ACI-APPLICAD NS NS1.WEBNJ.NET.  
ANZAPACK NS DNS3.TERRA.ES.  
ANZAPACK NS DNS4.TERRA.ES.  
ALPHASOFTDE NS DNS1.EPAG.NET.  
ALPHASOFTDE NS DNS2.EPAG.NET.  
ALPHASOFTDE NS DNS01.KUTTIG.NET.  
AAI-TENN NS AUTH00.DNS.BELLSOUTH.NET.  
AAI-TENN NS AUTH01.DNS.BELLSOUTH.NET.  
AAI-TENN NS AUTH02.DNS.BELLSOUTH.NET.  
ALLIEDMAXCUT NS NS3.DHCNET.NET.  
ALLIEDMAXCUT NS NS0.DHCNET.NET.  
ATLANTAEXOTICS NS NS1.APHOST  
ATLANTAEXOTICS NS NS2.APHOST  
ATLANTA-EXOTICS NS NS3.LNHI.NET.  
ATLANTA-EXOTICS NS NS2.LNHI.NET.  
ATLANTA-EXOTICS NS NS1.LNHI.NET.  
.....
```



Domain Management Model (1)



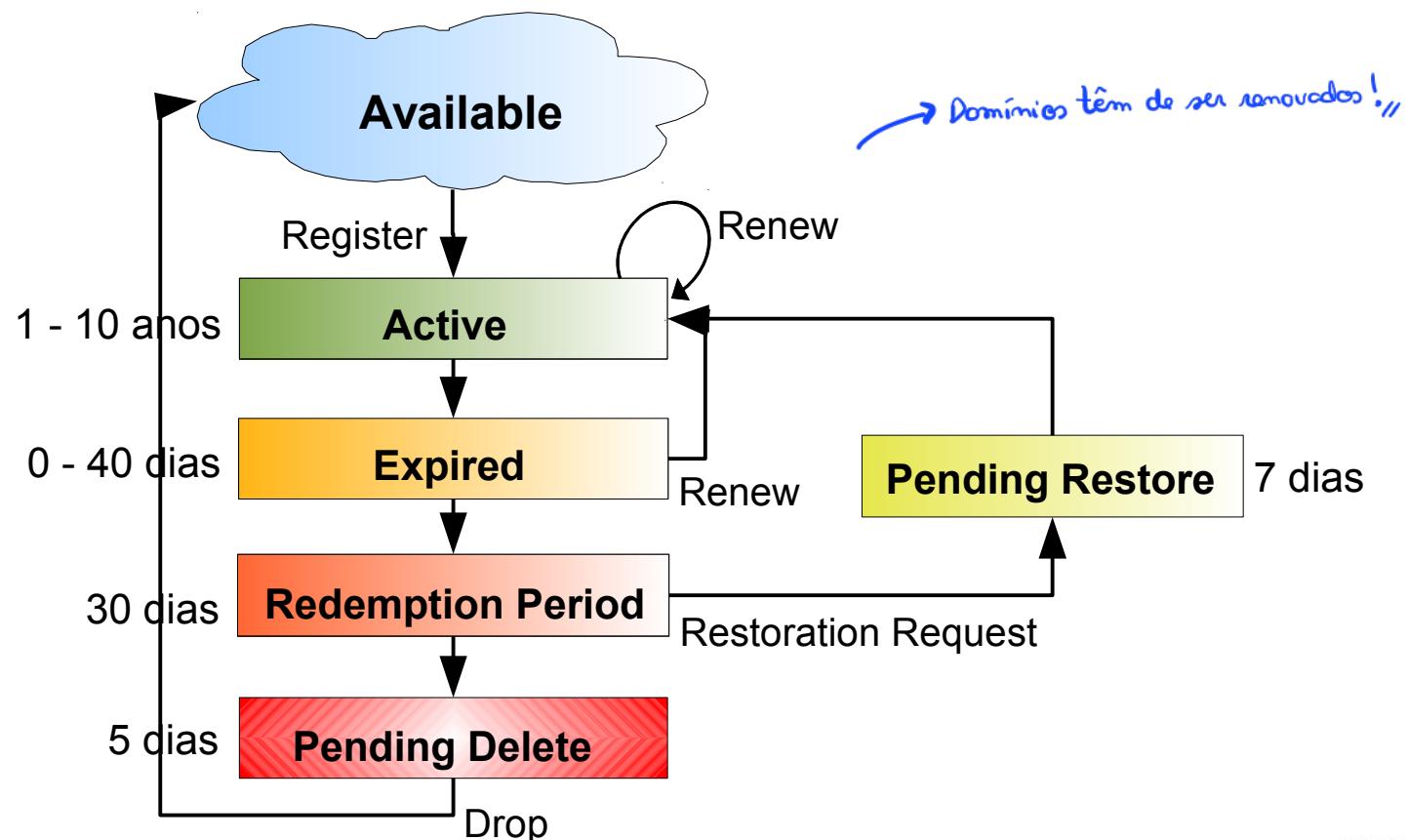
Domain Management Model (2)

- Delegation and Authority lie at the core of the domain name system hierarchy.
- The Authority for the root domain lies with Internet Corporation for Assigned Numbers and Names (ICANN).
 - ◆ gTLDs are authoritatively administered by ICANN and delegated to a series of accredited entities.
 - ◆ ccTLDs are delegated to the individual countries for administration purposes.
- The entity responsible by a specific domain is called **Registry**.
 - ◆ In charge of maintaining the Zone File of the TLD.
↳ Entidade governamental ...
- **Registries** (usually) delegate to **Registrar** the operational management and marketing of a domain.
 - ◆ One **Registry** can delegate to multiple **Registrars**
 - ◆ The **Registrar** stores and manages the information and status of a domain.
- One **Registrar** may still accept **Resellers**
 - ◆ A **Reseller** sells domains from a **Registrar** (for a commission)
 - ◆ The management of the domains is not responsibility of a **Reseller**.
- A **Registrant** is any entity that wants to register a domain name.



Domain Name Life Cycle

- A domain can be registered for a period of 1 to 10 years.
 - ◆ After that period the domain must be renewed.
- In case of no renewal, it's initiated the process of deletion of the domain name from the DNS database.
 - ◆ Nowadays, the Registrars do not release the domain immediately after the redemption period, they initiate a reselling mechanism (usually some kind of auction) of the domain on the secondary market.



WHOIS Service and Information

- Contains information about the registrant of a domain
 - ◆ Name servers
 - ◆ Status of the domain
 - Registry-Registrar Protocol (RPP)
 - Extensible Provisioning Protocol(EPP)
 - ◆ Creation, expiration and last update dates.
 - ◆ Registrant contacts
 - General
 - Administrative
 - Technical
 - Billing
- This information can be retrieved using the WHOIS service
 - ◆ Executes recursive queries of Registry and Registrant databases.

Domain Name: NAME.COM
Registrar: NAME.COM LLC
Whois Server: whois.name.com
Referral URL: http://www.name.com
Name Server: NS1.NAME.COM
Name Server: NS2.NAME.COM
Name Server: NS3.NAME.COM
Name Server: NS4.NAME.COM
Status: ok
Updated Date: 30-jan-2009
Creation Date: 03-jan-1995
Expiration Date: 04-nov-2015

REGISTRANT CONTACT INFO

Name.com LLC
DNS Admin, 125 Rampart Way, Suite 300, Denver, CO 80230, US
Phone: +1.7202492374
Email Address: dns@name.com

ADMINISTRATIVE CONTACT INFO

Name.com LLC
DNS Admin, 125 Rampart Way, Suite 300, Denver, CO 80230, US
Phone: +1.7202492374
Email Address: dns@name.com

TECHNICAL CONTACT INFO

Name.com LLC
DNS Admin, 125 Rampart Way, Suite 300, Denver, CO 80230, US
Phone: +1.7202492374
Email Address: dns@name.com

BILLING CONTACT INFO

Name.com LLC
DNS Admin, 125 Rampart Way, Suite 300, Denver, CO 80230, US
Phone: +1.7202492374
Email Address: dns@name.com

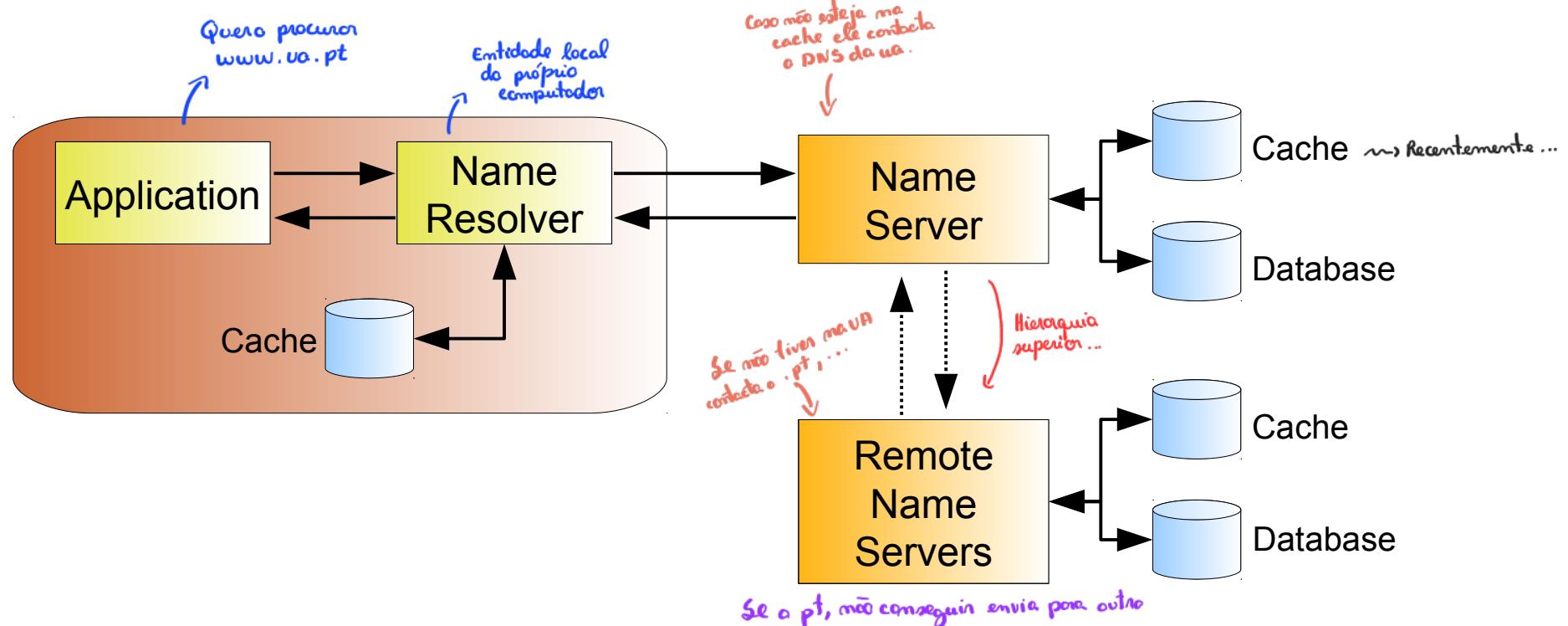


Name Servers Registration

- In order to set up a DNS server outside of your registrar, you need to:
 - ◆ Explicitly register your name server names and IPs.
 - i.e. Associate name with IP (ex: ns1.domain.com – 10.1.1.1).
 - ◆ Define server names (minimum 2) to your domain registration at your registrar.



Name Resolution



- Received answers are (may be) temporarily stored in cache (have an associated TTL)
 - Can be reused in future queries to speed up answers.
- Cache use improves the systems efficiency by eliminating unnecessary external queries.

DNS Query & DNS Response

Qual o ip?

Frame 1928 (69 bytes on wire, 69 bytes captured)

Ethernet II, Src: 00:15:f2:9f:38:9d, Dst:
00:60:08:1f:b8:26

Internet Protocol, Src: 193.136.92.160, Dst:
193.136.92.65

User Datagram Protocol, Src Port: 54277, Dst Port: 53

Source port: 54277 (54277)

Destination port: 53 (53)

Length: 35

Checksum: 0x3c27 [incorrect, should be 0xabba
(maybe caused by "UDP checksum offload"?)]

Domain Name System (query)

[Response In: 1929]

Transaction ID: 0xf1e4

Flags: 0x0100 (Standard query)

Questions: 1

Answer RRs: 0

Authority RRs: 0

Additional RRs: 0

Queries

www.ua.pt: type A, class I

ipv4

Internet
(publico)

Frame 1929 (152 bytes on wire, 152 bytes captured)

Ethernet II, Src: 00:60:08:1f:b8:26, Dst:
00:15:f2:9f:38:9d

Internet Protocol, Src: 193.136.92.65, Dst:
193.136.92.160

User Datagram Protocol, Src Port: 53, Dst Port: 54277

Source port: 53 (53)

Destination port: 54277 (54277)

Length: 118

Checksum: 0x1167 [correct]

Domain Name System (response)

[Request In: 1928]

[Time: 0.00510000 seconds]

Transaction ID: 0xf1e4

Flags: 0x8180 (Standard query response, No error)

Questions: 1

Answer RRs: 1

Authority RRs: 2

Additional RRs: 2

Queries

www.ua.pt: type A, class IN

O ip é este!



Answers

www.ua.pt: type A, class IN, addr 193.136.173.25

Eu sou este dns

Quem deu
a resposta?

Sou eu que estou a dar
a resposta, não pedi
a ninguém

Authoritative nameservers

ua.pt: type NS, class IN, ns ns2.ua.pt

ua.pt: type NS, class IN, ns ns.ua.pt

Additional records

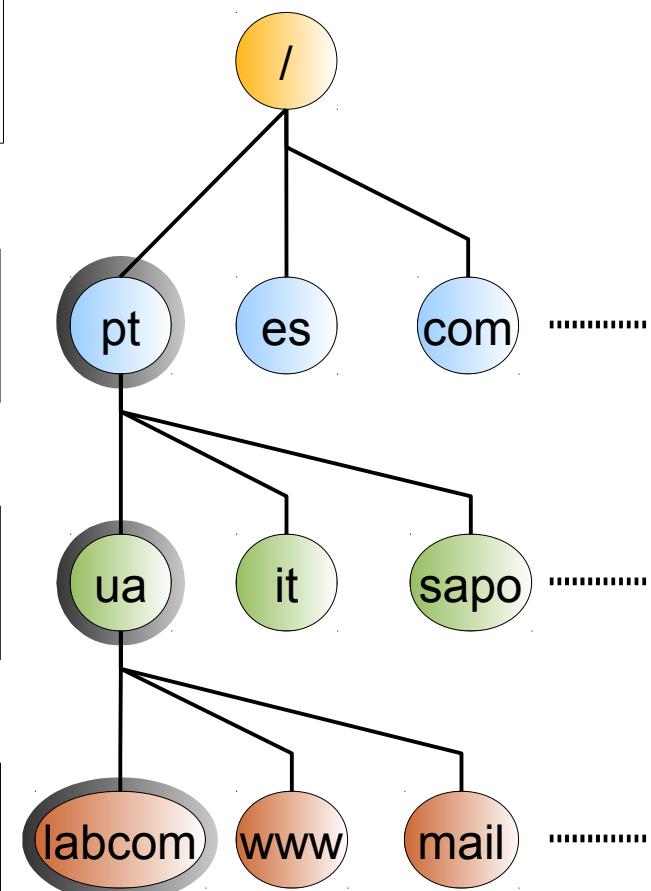
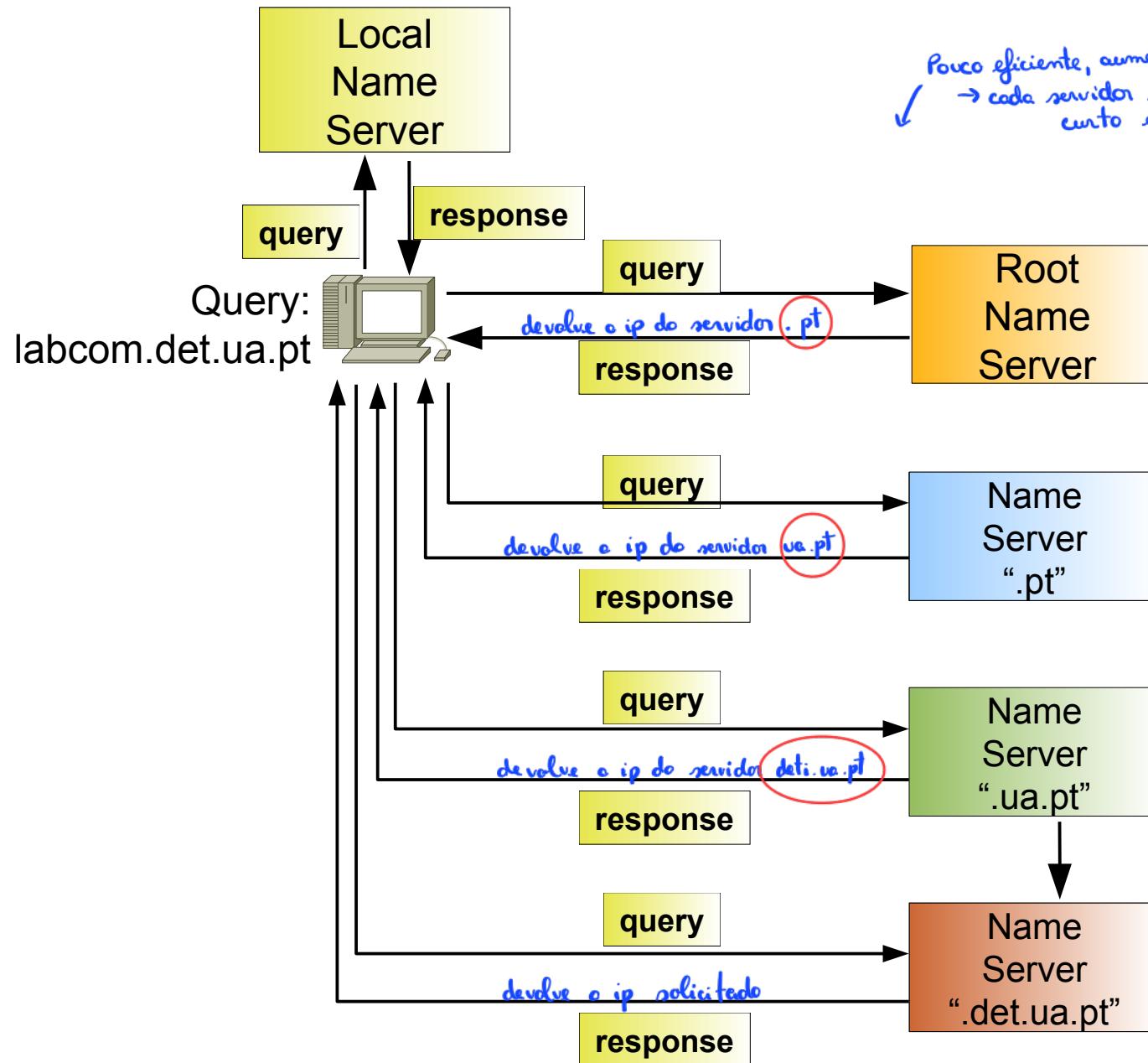
ns.ua.pt: type A, class IN, addr 193.136.172.18

ns2.ua.pt: type A, class IN, addr 213.228.152.1

Ip's DNS



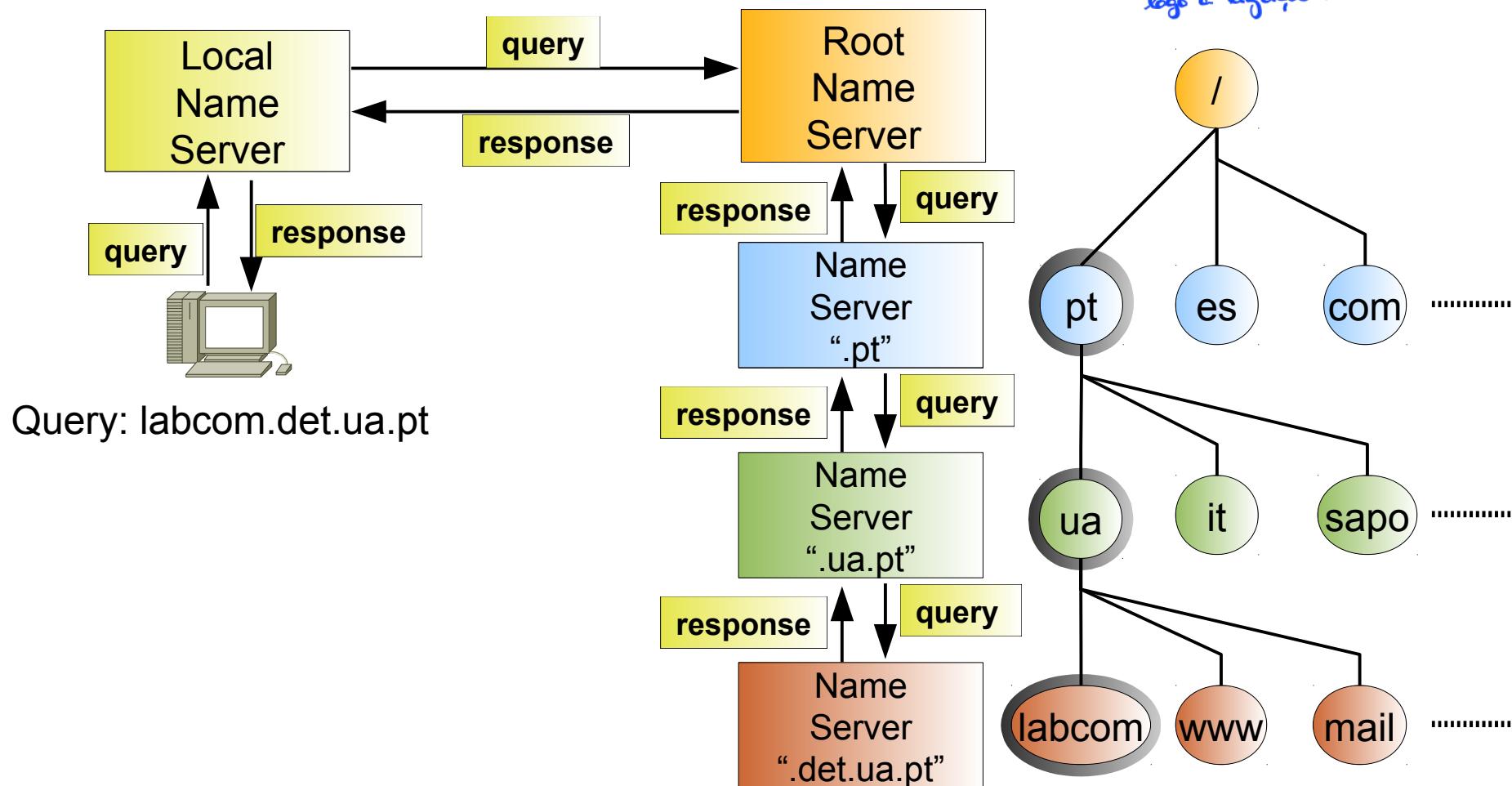
Iterative (Non-Recursive) Resolution



Atualidade: utilizamos este pois o tempo-resposta é mínimo! //

Recursive Resolution

2



→ Mais rápido: pedido - resposta
• Mas os servidores têm de ficar à espera da resposta,
logo a ligação não acaba



Iterative vs. Recursive Resolution

- Iterative resolution:

- Less efficient: increases the average time between a DNS query and its response.
Servidores não têm muito trabalho!
- Server loads are lower: each server responds immediately to a query,
 - Do not have to store any temporary information,
 - Do nor perform any interaction with other DNS servers.

- Recursive resolution:

- More efficient: minimizes the average time between a DNS query and its response.
Servidores têm de fazer tudo!
- Higher server loads: each server must simultaneously manage the state of multiple DNS queries.
 - More memory, more CPU.
→ tem de esperar pela resposta
 - Not a problem with current servers.



Zone Configuration

ficheiro que guarda as características da minha rede / PC do chefe: boss.salsichos.pt

- A zone is defined by
 - ◆ A zone declaration, which holds the type of the zone, a pointer to the zone file and type specific configuration statements (optional).
 - ◆ A zone file, which holds the DNS resource records for all of the domain names associated with the zone.
- Zone files store all of the data served by a DNS server.
- The basic format of the zone file is a time to live (TTL) field followed by the Start Of Authority (SOA) records.
 - ◆ The overall TTL instructs non-authoritative DNS servers how long to cache records retrieved from the zone file.
 - ◆ With large values it will take more time to propagate changes.
 - ◆ With smaller value, the DNS server load will increase (non-authoritative servers will have to send the same requests more frequently).
 - ◆ Typical values: 1 hour to a 1 day.
 - ◆ The SOA record defines the zone name, an e-mail contact and various time and refresh values applicable to the zone.

Associação entre nome ↪ endereço!

*→ Nome da zona
→ Pessoa responsável
→ ...*



Zone Types

- **Master:** The server reads the zone data direct from local storage (a zone file) and provides authoritative answers for the zone.
Authoridade de resolução local! //
- **Slave:** A slave zone is a replica of the master zone and obtains its zone data by zone transfer operations.
 - ◆ The slave will respond authoritatively for the zone as long as it has valid (not timed out) zone data.*Réplica do mestre* *Backup...*
- Forward: A zone of type forward is simply a way to configure forwarding on a per-domain or per zone basis.
 - ◆ To be effective both a forward and forwarders statement should be included.
- **Stub:** A stub zone is similar to a slave zone except that it replicates only the NS records of a master zone instead of the entire zone.
Slave mais fraco...
- Delegation-only: Indicates only referrals (or delegations) will be issued for the zone and should be used for TLDs only not leaf (non TLD) zones.



BIND – Zone Declaration Examples

Serviço possível para configurar DNS

salsichos.pt

```
zone "domain.com" {  
    type master; → para ter um slave, preciso de um master  
    file "zones/domain.com";  
};
```

Ao contrário

Dou um ip e ele dá-me o nome

inverse addresses

```
zone "200.136.193.in-addr.arpa" {  
    type master;  
    file "zones/193.136.200";  
};
```

Resolução inversa!

```
zone "example.com" in {  
    type slave;  
    file "slave.example.com";  
    masters {192.168.2.7; 10.2.3.15 port 1127; 2001:db8:0:1::15;};  
};
```

Quem são os masters?



Mais importante! →

Zone Files

→ O ficheiro que tem todos os registos!

- Zone files contain Resource Records that describe a domain or sub-domain.
 - ◆ Format of zone files is an IETF standard defined by RFC 1035.
- Contents
 - ◆ Data that indicates the top of the zone and some of its general properties,
 - ◆ A SOA Record.
 - ◆ Authoritative data for all nodes or hosts within the zone,
 - ◆ A (IPv4) or AAAA (IPv6) Records.
 - ◆ Data that describes global information for the zone
 - ◆ Mail MX Records and Name Server NS Records.
 - ◆ In the case of sub-domain delegation the name servers responsible for this sub-domain
 - ◆ One or more NS Records.
 - ◆ One or more A or AAAA Records



Name Server Records

- **SOA** (RFC 1035): Start of Authority. Defines the zone name, an e-mail contact and various time and refresh values applicable to the zone.
- **A** (RFC 1035): IPv4 Address record. An IPv4 address for a host.
- **AAAA** (RFC 3596): IPv6 Address record. An IPv6 address for a host.
- **NS** (RFC 1035): Name Server. Defines the authoritative name server(s) for the domain (defined by the SOA record).
- **MX** (RFC 1035) Mail Exchanger. A preference value and the host name for a mail server/exchanger.
- **CNAME** (RFC 1035): Canonical Name. An alias name for a host.
→ ter mais do que um nome!,,
- **PTR** (RFC 1035): IP address (IPv4 or IPv6) to host. Used in reverse maps.
- **TXT** (RFC 1035): Text information associated with a name.



SOA Record (1)

- @ - represents the base domain
- IN - class of the zone (INternet)
- SOA - record identifier
- The master DNS server for the zone
 - ◆ The host where the file was created (nameserver.domain.com)
- Contact e-mail - The e-mail address of the person responsible for administering the domain's zone file.
 - ◆ "." is used instead of an "@" in the e-mail name
 - ◆ adm.domain.com <=> adm@domain.com email

<i>Servidor</i>	<i>Domínio</i>	<i>Email: adm@domain.com</i>
@ IN SOA	nameserver.domain.com.	adm.domain.com. (
<i>Ip da Internet</i>		1 ; serial number
		3600 ; refresh [1h]
		600 ; retry [10m]
		86400 ; expire [1d]
		3600) ; min TTL [1h]



SOA Record (2)

→ Mais detalhada!

- Serial number - The revision number of this zone file.
 - ◆ Increment this number each time the zone file is changed.
 - ◆ It is important to increment this value each time a change is made, so that the changes will be distributed to any secondary DNS servers.
- Refresh Time - The time, in seconds, a secondary DNS server waits before querying the primary DNS server's SOA record to check for changes.
 - ◆ When the refresh time expires, the secondary DNS server requests a copy of the current SOA record from the primary.
 - ◆ The secondary DNS server compares the serial number of the primary DNS server's current SOA record and the serial number in its own SOA record. If they are different, the secondary DNS server will request a zone transfer from the primary DNS server.
 - ◆ The default value is 3,600.
- Retry time - The time, in seconds, a secondary server waits before retrying a failed zone transfer.
 - ◆ Usually, the retry time is less than the refresh time. The default value is 600.
- Expire time - The time, in seconds, that a secondary server will keep trying to complete a zone transfer.
 - ◆ If this time expires prior to a successful zone transfer, the secondary server will expire its zone file (stops answering queries).
 - ◆ The default value is 86,400.
- Negative caching TTL – the time, in seconds, a negative answers (such as when a requested record does not exist) can be cached on non-authoritative servers.
 - ◆ This field acts like the overall TTL but specifically for negative answers.
 - ◆ Small values are appropriate (15m to 2h).

@	IN	SOA	name	server.domain.com.	adm.domain.com.	(
				1	;	serial number
				3600	;	refresh [1h]
				600	;	retry [10m]
				86400	;	expire [1d]
				3600)	;	min TTL [1h]

Other Records (1)

- IPv4 Address Record (A)

- ◆ Syntax: “*name ttl class rr ipv4*”

```
; zone fragment for example.com
$TTL 2d ; zone default = 2 days or 172800 seconds
        name      IN      A      192.168.0.3 ; joe & www = same ip
        joe       IN      A      192.168.0.3
        www       IN      A      192.168.0.3
        www.example.com.   A      192.168.0.3
        fred      3600  IN      A      192.168.0.4 ; TTL overrides $TTL default
        ftp       IN      A      192.168.0.24 ; round robin with next
        ftp       IN      A      192.168.0.7
        mail      IN      A      192.168.0.15 ; mail = round robin
        mail      IN      A      192.168.0.32
        mail      IN      A      192.168.0.3
```

- IPv6 Address Record (AAAA)

- ◆ Syntax: “*name ttl class rr ipv6*”

```
; zone fragment for example.com
$TTL 2d ; zone default = 2 days or 172800 seconds
$ORIGIN example.com.
        joe      IN      AAAA    2001:db8::3 ; joe & www = same ip
        www      IN      AAAA    2001:db8::3
        ; functionally the same as the record above
        www.example.com. AAAA    2001:db8::3
        fred      3600  IN      AAAA    2001:db8::4 ; TTL overrides $TTL default
        ftp       IN      AAAA    2001:db8::5 ; round robin with next
        Name     IN      AAAA    2001:db8::6
        squat     IN      AAAA    2001:db8:0:0:1::13 ; address in another subnet
```



Other Records (2)

• Name Server Record (NS)

- ◆ Syntax: “name ttl class rr name”

✓
“
Não esquecer
de os definir
em cima

```
IN      NS      ns1 ; unqualified name
; the line above is functionally the same as the line below
; example.com. IN      NS      ns1.example.com.
; at least two name servers must be defined
IN      NS      ns2 → Vai ser um serviço DNS/
; the in-zone name server(s) have an A record
ns1      IN      A      192.168.0.3
ns2      IN      A      192.168.0.3
→ Pode ser AAAA se forse ipv6
```

• Mail Exchange Record (MX)

- ◆ Syntax: “name ttl class rr *pref* name”
- ◆ The pref (Preference) field is relative to any other MX record for the zone (value 0 to 65535). Low values are more preferred.

Preferência ...

```
IN      MX      10 mail ; short form
; the line above is functionally the same as the line below
; example.com. IN      MX      10 mail.example.com.
; any number of mail servers may be defined
IN      MX      20 mail2.example.com.
; use an external back-up
IN      MX      30 mail.example.net.
; the local mail server(s) need an A record
mail      IN      A      192.168.0.3
mail2     IN      A      192.168.0.3
→ A mesma máquina, mas
vai responder por mail e mail2
```



Other Records (3)

- Canonical Name Record (CNAME)
 - ◆ Syntax: “*name ttl class rr canonical_name*”

```
; zone fragment for example.com
$TTL 2d ; zone default = 2 days or 172800 seconds
$ORIGIN example.com.

.....
server1    IN      A        192.168.0.3
www        IN      CNAME    server1
ftp         IN      CNAME    server1
```

Vai ter 3 nomes!
→ server1
→ www
→ ftp

- ◆ Do not use CNAME records with NS and MX records,
 - ◆ Usually it works, but is theoretically not permitted!

Wrong!

			IN	MX	10 mail.example.com.
	mail		IN	CNAME	server1
	server1		IN	A	192.168.0.3

→ Registro mail
Tenho de definir primeiro o server!

Correct!

			IN	MX	10 mail.example.com.
	server1		IN	CNAME	mail
	mail		IN	A	192.168.0.3

mail já está definido



Example

```
$ORIGIN teste.com.

@ IN SOA teste.com. adm.teste.com. (
    199609206 ; serial, todays date + todays serial #
    8H         ; refresh, seconds
    2H         ; retry, seconds
    4W         ; expire, seconds
    1D )       ; minimum, seconds

    NS ns1.teste.com.
    NS ns2.teste.com.
    MX 10 teste.com. ; Primary Mail Exchanger
    TXT "TESTE Corp"
    → Podia haver A/AAA para ipv6 → Comentário, que é solicitado por vezes!//

localhost A 127.0.0.1
router A 206.6.177.1
teste.com. A 206.6.177.2
ns1 A 206.6.177.3
ns2 A 206.6.177.4
www A 207.159.141.192

ftp CNAME teste.com.
mail CNAME teste.com.
news CNAME teste.com.

funn A 206.6.177.2

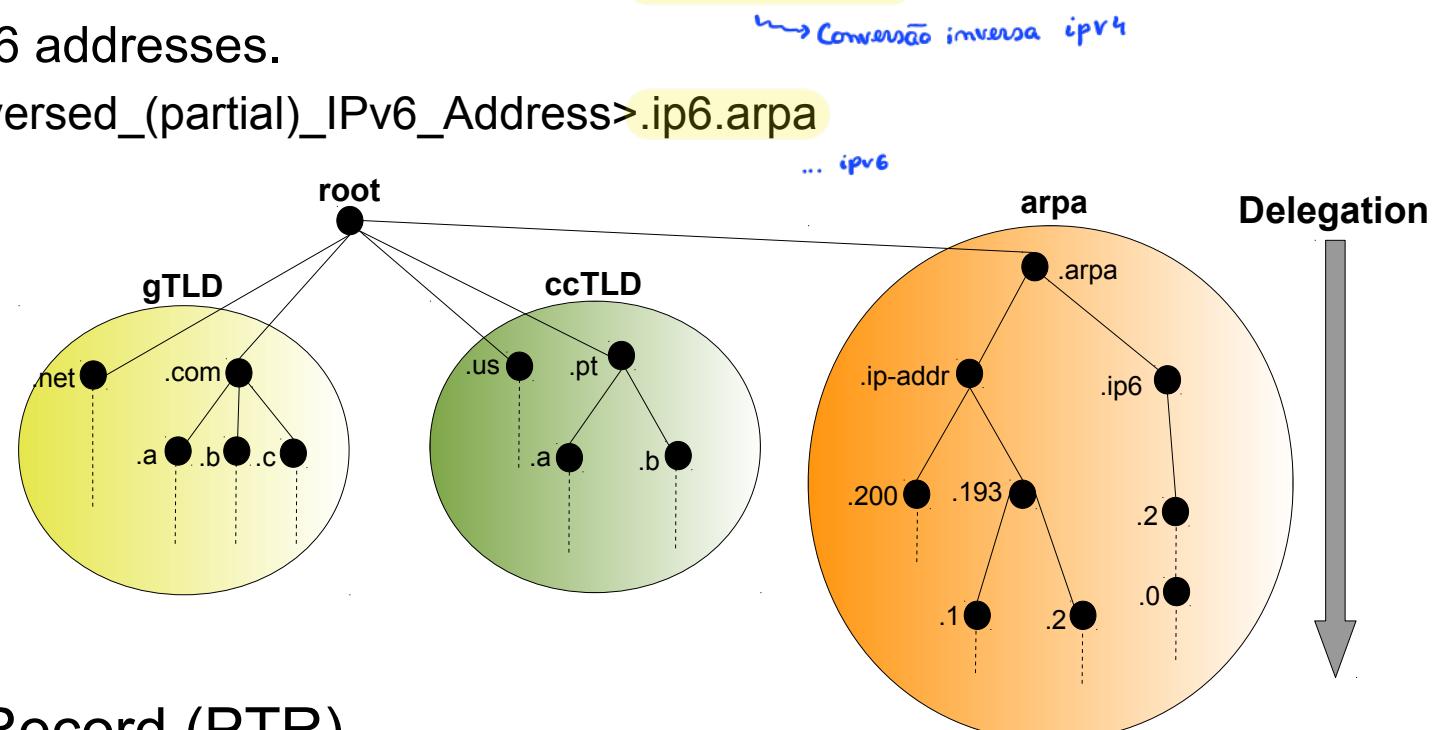
; Workstations
ws-177200 A 206.6.177.200
ws-177201 A 206.6.177.201
```



Reverse DNS

↳ Não muito utilizada! //

- In order to perform Reverse Resolution using normal recursive and Iterative queries the DNS designers defined a special (reserved) Domain Name called:
 - IN-ADDR.ARPA for IPv4 addresses,
 - Resolves <reversed_(partial)_IPv4_Address>.in-addr.arpa
 - IP6.ARPA for IPv6 addresses.
 - Resolves <reversed_(partial)_IPv6_Address>.ip6.arpa



- Uses the Pointer Record (PTR)
 - Pointer records are the opposite of A and AAAA.
 - Syntax: "name ttl class rr name"



IPv4 Reverse DNS - Example

escrita ao contrário!

```
zone "200.136.193.in-addr.arpa" {
    type master;
    file "zones/193.136.200";
};
```

onde estão as configurações?



```
$TTL 3D
@   IN      SOA    land-5.com. root.land-5.com. (
                      199609206      ; Serial
                      28800      ; Refresh
                      7200       ; Retry
                      604800     ; Expire
                      86400)    ; Minimum TTL
193.136.200.1,        NS      land-5.com.
                           NS      ns2.psi.net.

;

;          Servers
1 sufixo do Ip PTR      router.land-5.com.
2 PTR      land-5.com.
2 PTR      funn.land-5.com.
Qual o nome?           ↴ Mais simples!
                           → Todos são PTR

;

;          Workstations

200    PTR      ws-177200.land-5.com.
201    PTR      ws-177201.land-5.com.
202    PTR      ws-177202.land-5.com.
203    PTR      ws-177203.land-5.com.
```



IPv6 Reverse DNS – Example

```
$TTL 2d      ; default TTL for zone 172800 secs
$ORIGIN 0.0.0.0.8.b.d.0.1.0.0.2.IP6.ARPA.

@    IN      SOA   ns1.example.com. hostmaster.example.com. (
    exrito ao contrário
    (prefixo)          2003080800 ; sn = serial number
                      12h      ; refresh = refresh
                      15m      ; retry = update retry
                      3w      ; expiry = expiry
                      2h      ; min = minimum
)
; name servers Resource Records for the domain
        IN      NS     ns1.example.com.
; the second name servers is
; external to this zone (domain).
        IN      NS     ns2.example.net. } Exemplo de servidor com 2 nomes
; PTR RR maps a IPv6 address to a host name
; hosts in subnet ID 1
1.0.0.0.0.0.0.0.0.0.0.0.0.0.0.1.0.0.0    IN      PTR     ns1.example.com.
2.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.1.0.0.0    IN      PTR     mail.example.com.
; hosts in subnet ID 2
1.0.0.0.0.0.0.0.0.0.0.0.0.0.0.2.0.0.0    IN      PTR     joe.example.com.
2.0.0.0.0.0.0.0.0.0.0.0.0.0.0.2.0.0.0    IN      PTR     www.example.com.
```

prefixo →

