Redes de Computadores

(RCOMP – 2015/2016)

IPv6 e ICMPv6

Resolução de nomes (DNS)

Internet Protocol v6

Nos anos 90 a expansão da INTERNET atingiu valores inicialmente impensáveis que conduziram a uma situação de esgotamento dos endereços IPv4 disponíveis. Foram tomadas várias medidas para permitir um melhor aproveitamento do espaço de endereçamento de 32 bits do IPv4:

>> definição de 3 classes de rede com 8, 16 ou 24 bits (na versão inicial as redes IPv4 usavam sempre 8 bits para identificar a rede).
>> definição livre de outras mascaras de rede mais ajustadas às realidades de cada situação concreta (por exemplo mascaras de 30 bits para ligações dedicadas).
>> utilização de redes privadas associado a dispositivos capazes de traduzir endereços (NAT – Network Address Translation). Cada conjunto de redes privadas necessita apenas de um endereço oficial.

Tendo como principal objetivo resolver as limitações do espaço de endereçamento de 32 bits foi desenvolvido um sucessor do IP versão 4, inicialmente conhecido por IP-NG (Next Generation) foi-lhe atribuído o número de versão 6, sendo atualmente conhecido por IPv6.

IPv6 – Endereços de 128 bits

Os endereços IPv6 são constituídos por 4 vezes mais bits do que os IPv4, como o número de endereços cresce exponencialmente com o número de bits, 2^{128} no IPv6 contra 2^{32} no IPv4. O espaço de endereçamento do IPv6 é "imenso", permitindo quase um espaço de endereçamento IPv4 para cada habitante da Terra.

Os melhoramentos da versão 6 do protocolo IP não se limitaram ao espaço de endereçamento:

>> Abandono da fragmentação, apenas "*Path MTU discovery*" (PMTUD)**.**
>> Integração do endereço físico (MAC) no endereço IPv6 (ARP desnecessário).
>> Suporte de MULTICAST (no IPv4 é uma opção).
>> Configuração automática de nós, evitando a necessidade do BOOTP/DHCP.
>> Suporte JUMBOGRAMS – pacotes IP até 4 Gb (o IPv4 apenas suporta 64Kb).
>> IPSEC – protocolo de autenticação e confidencialidade integrado.

Endereçamento IPv6 - representação

Os endereços IPv6 são representados sob a forma de texto através de uma sequência de 8 conjuntos de 16 bits em notação hexadecimal, separados por ":".

XXXX:XXXX:XXXX:XXXX:XXXX:XXXX:XXXX:XXXX

A grande extensão dos endereços tornam a sua representação pouco cómoda e pouco legível. No sentido de facilitar um pouco os zeros são comprimidos, assim em cada conjunto de 16 bits eliminam-se os zeros à esquerda, além disso os conjuntos de 16 bits com valor nulo são omitidos. Por exemplo:

"0000:3278:0A04:0005:0000:0000:0000:0034" = ":3278:A04:5::34"

Nunca pode existir mais do que uma sequência "::" pois representa um número indeterminado de conjuntos nulos.

Os endereços IPv4 podem ser representados na forma IPv6, isso é útil quando há necessidade de encaminhar pacotes IPv6 através de uma rede IPv4 ("IPv4 compatible"), ou quando pretendemos representar um nó que não possui IPv6 ("IPv4 mapped"), . Nestes casos o endereço IPv4 ocupa os dois últimos conjuntos e pode ser representado na notação IPv4, por exemplo (respetivamente):

::193.136.62.9 e ::FFFF:193.136.62.9

IPv6 – tipos de endereço

Tal como acontecia no IPv4 o espaço de endereçamento é estruturado em redes, sendo a parte inicial do endereço usada para identificar a rede (prefixo de rede) e a parte restante identifica um nó nessa rede. Por exemplo

2001:0db8:2b00::/40

Representa uma rede com mascara de 40 bits.

1º nó da rede: 2001:0db8:2b00::1 (2001:0db8:2b00:0000:0000:0000:0000:0001 **)**

Último nó da rede: 2001:0db8:2bff:ffff:ffff:ffff:ffff:ffff

(o IPv6 não usa endereços de BROADCAST, para o mesmo efeito existem endereços MULTICAST)

O protocolo IPv6 suporta 3 tipos de endereço

UNICAST – identifica um nó único numa dada rede.
MULTICAST – identificam conjuntos de nós, os dados têm de ser entregues em todos eles.
ANYCAST – identificam conjuntos de nós, os dados são entregues em apenas um deles.

IPv6 – endereços MULTICAST

Os endereços MULTICAST identificam-se por terem os primeiros 8 bits com o valor um.

O bit X tem o valor zero para endereços MULTICAST normalizados (*well-known*) e o valor um para outros grupos de nós. Os 4 bits seguintes (SSSS) definem a zona limite (SCOPE) até onde o MULTICAST pode ser aplicado:
1 – “Node-Local” – Apenas no nó emissor
2 – “Link-Local” – Na mesma rede física (nível 2)
5 – “Site-Local”
8 – “Organization-Local”
E – “Global” – Toda a INTERNET

Os endereços MULTICAST “well-known” servem por exemplo para identificar serviços, por exemplo:
“FF02:0:0:0:0:0:0:C” identifica todos os servidores DHCPv6 da rede local (SCOPE=2).
“FF02::1” identifica todos os nós da rede local (equivalente ao BROADCAST do IPv4).
“FF02::2” identifica todos os ROUTERS da rede local.
“FF01::43” identifica os servidores NTP existentes no mesmo nó (SCOPE=1).
“FF0E::43” identifica todos os servidores NTP da INTERNET (SCOPE=E).

IPv6 – endereços MULTICAST - Ethernet

Os pacotes IPv6 destinados a endereços *multicast* IPv6 são transportados por tramas *ethernet* com endereços de destino começados por “33:33”. Uma vez que o bit menos significativo do primeiro octeto tem o valor um são tratados pelos comutadores de nível 2 como endereços *multicast* e são retransmitidos em todas as portas.

Os 32 bits menos significativos do endereço IPv6 *multicast* são diretamente copiados para os 32 bits menos significativos do endereço Ethernet, deste modo a cada endereço *multicast* IPv6 corresponde um endereço *multicast ethernet*, por exemplo:

O endereço IPv6 *multicast*: **FF00::2AB1:20A3**
vai corresponder ao endereço *ethernet multicast*: **33:33:2A:B1:20:A3**

No IPv6 a gestão dos grupos *multicast* é assegurada pelo ICMPv6, ou seja as funcionalidades do IGMP para o IPv4 foram no IPv6 integradas no ICMPv6.

IPv6 – endereço UNICAST link-local

Os endereços *unicast* são endereços únicos que cada nó IPv6 possui. Para poder funcionar com IPv6 todos os nós necessitam antes de mais de possuir um endereço *unicast link-local*. O endereço *link-local* é gerado autonomamente pelo próprio nó usando o prefixo FE80::/10 e preenchendo os bits de nó com um valor gerado a partir do endereço MAC de nível 2.

Sendo o endereço MAC único existe alguma garantia de que o endereço *link-local* será único, mesmo assim o endereço gerado é testado através de mensagens *Neighbor Solicitation* e *Neighbor Advertisement* do ICMPv6.

Os endereços *link-local* permitem a comunicação com todos os outros nós da mesma rede IPv6, mas não com nós de outras redes.

Adicionalmente um nó pode registar-se em endereços *multicast* locais (ff02::).

Após a definição do endereço *unicast link-local* o nó pode então comunicar em IPv6 começando por solicitar um *router* enviando uma mensagem ICMPv6 tipo 133 (*Router Solicitation*) para o endereço *multicast* ff02::2 (local routers). Os routers presentes respondem com a mensagem tipo 134 (*Router Advertisement*) contendo uma lista de prefixos em uso na rede e a forma como o nó se deve configurar, uma de:

- Stateless via SLAAC (Stateless Address Autoconfiguration)
- Stateful via DHCPv6

IPv6 – SLAAC (*Stateless Address Autoconfiguration*)

De acordo com a informação fornecida na mensagem *Router Advertisement* poderá ser indicado ao nó que deve usar SLAAC, nesse caso o nó usa o prefixo que foi fornecido na mensagem a gera automaticamente a parte relativa ao endereço de nó de forma semelhante ao que fez para definição do endereço *link-local*. De igual modo é verificada a existência de endereços duplicados.

O endereço *unicast* gerado via SLAAC é um endereço global e permite a comunicação com qualquer outro nó IPv6 na mesma ou em qualquer outra rede IPv6.

O SLAAC permite também informar o nó sobre os servidores DNS que deve usar e o nome do domínio DNS (RFC 6106, "*IPv6 Router Advertisement Options for DNS Configuration*"), no entanto nem todos os nós suportam esta funcionalidade.
Na mensagem *Router Advertisement* o nó pode ser informado que para obter estes parâmetros deve recorrer ao serviço DHCPv6.

Uma outra alternativa é usar endereços atribuídos por DHCPv6, se a resposta *Router Advertisement* indicar configuração *stateful* o nó não vai gerar o seu endereço, em vez disso vai recorrer ao serviço DHCPv6 obtendo assim o seu endereço de nó IPv6 e parâmetros DNS. Neste caso o servidor DHCPv6 tem de ser configurado para gerir uma *pool* de endereços.

IPv6 – endereços ANYCAST

Os endereços ANYCAST são endereços UNICAST normais, a única diferença é que são atribuídos a vários nós da rede. Pode ser útil de diversas formas, quando um encaminhador recebe um pacote destinado a um endereço ANYCAST determina qual é o nó que está mais próximo dentro do conjunto de nós que possui esse endereço ANYCAST.
O endereço "subnet-router *anycast* address" é um exemplo deste tipo de endereço, é constituído pelo prefixo de uma dada rede IPv6, seguido de zeros, serve para identificar um dos encaminhadores dessa rede.

Os endereços UNICAST estão divididos em várias gamas de acordo com os valores dos primeiros bits:

010… – Endereços associados a fornecedores de serviço.
100… - Endereços associados a zonas geográficas
11111110 … (FD …) - Endereços privados IPv6.
.

Alguns endereços especiais são:

:: (0:0:0:0:0:0:0:0), tal como no IPv4, zero representa um endereço desconhecido.
::1 (0:0:0:0:0:0:0:1) endereço de LOOPBACK (equivalente ao 127.0.0.1 do IPv4).

Pacotes IPv6

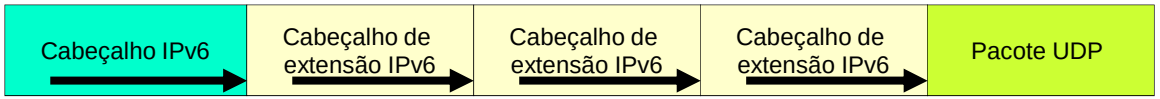
O cabeçalho IPv6 denota várias simplificações, incluindo a eliminação do CHECKSUM, ficando com um comprimento fixo de 40 bytes, dos quais 32 são ocupados com os endereços de origem e destino. Alguns campos mudam de nome, mas mantêm em grande medida a funcionalidade anterior, por exemplo o identificador de protocolo tem agora a designação *Próximo Cabeçalho*.

O 2º campo ("Classe de Tráfego") serve para definir a prioridade e tipo de tratamento que o pacote de ter por parte da rede (ROUTERS), por exemplo se se trata de uma aplicação interativa ou se a recuperação de dados é irrelevante. Está associado ao 3º campo de 24 bits que é usado como identificador de um dado fluxo de dados com determinadas características QoS negociadas.

Pacotes IPv6 – cabeçalhos de extensão

Apesar de um tamanho de cabeçalho fixo (40 bytes) o IPv6 também suporta opções que envolvem a existência de mais informação de controlo. O campo *NEXT HEADER* do cabeçalho IPv6 é usado para identificar o protocolo a que pertencem os dados transportados (multiplexagem, com os mesmos identificadores que eram usados no campo PROTOCOL do IPv4). O IPv6 permite contudo que o *NEXT HEADER* seja um bloco de opções IPv6 designado de *Cabeçalho de extensão*.

Os cabeçalhos de extensão começam pelos campos *NEXT HEADER* e *LENGTH*, tornando-se possível a existência de uma sucessão de cabeçalhos.



Além dos valores normalizados para os protocolos de transporte, tais como 6 para TCP e 17 para UDP, o campo *NEXT HEADER* suporta valores especiais que identificam cabeçalhos de extensão:

0	HOP-BY-HOP OPTIONS – opções que necessitam de ser processadas nos nós intermédios, EX.: JUMBOPAYLOAD
43	ROUTING – opções de encaminhamento (Ex.: SOURCE-ROUTING)
44	FRAGMENTAÇÃO – no IPv6 a fragmentação em nós intermédios não é suportada, apenas entre nós finais
50	ENCAPSULAMENTO – TUNNELING – CONFIDENCIALIDADE - INTEGRIDADE
51	AUTENTICAÇÃO - CONFIDENCIALIDADE- INTEGRIDADE
60	DESTINATION OPTIONS – opções que apenas necessitam de ser verificadas no nó final de destino.

ICMPv6 (ICMP para IPv6)

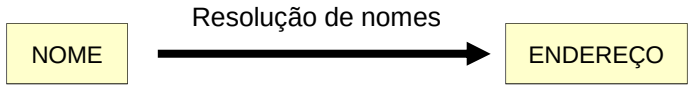
Embora muito semelhante ao protocolo ICMP usado com o IPv4 (ICMPv4) foi necessário realizar algumas adaptações e surgiu assim o ICMPv6 com identificador de protocolo 58. O formato das mensagens ICMPv6 é igual ao das mensagens ICMPv4, ou seja:

TIPO (8 bits) + CÓDIGO (8 bits) + CHECKSUM (16 bits) + DADOS (comprimento variável)

As diferenças estão nos tipos de mensagens:

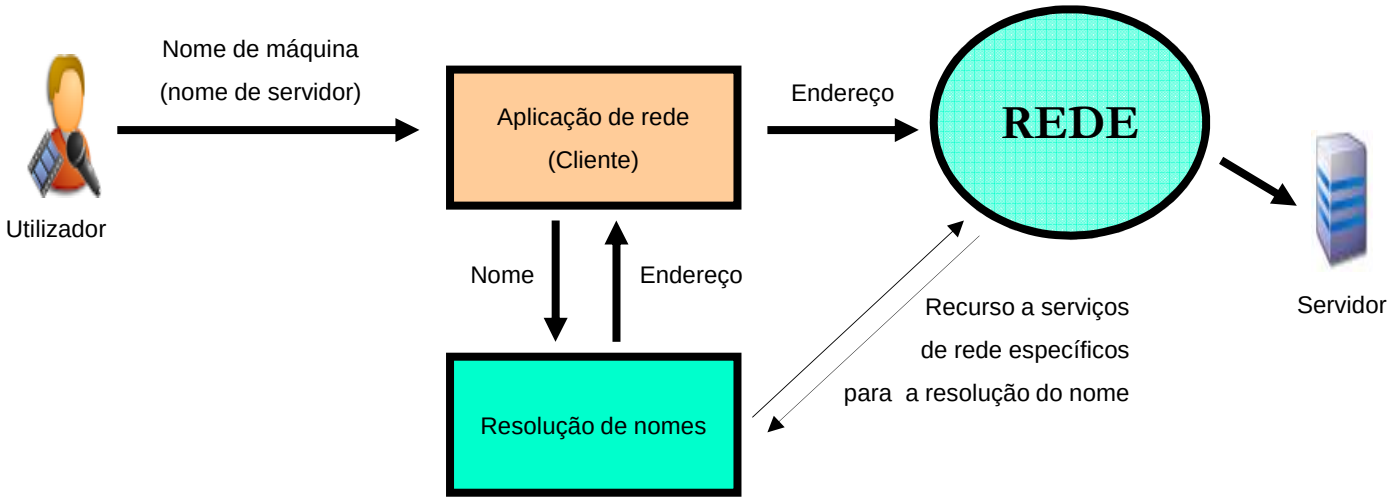
TIPO ICMPv6	
1	Destino inatingível – o pacote não chegou ao destino, o código indica a razão (existem códigos diferentes do ICMPv4).
2	Pacote demasiado grande – pacote não cabe no MTU seguinte, usado para PATH MTU DISCOVERY
3	Tempo excedido (TTL) – idêntico ao IPv4 (Código 0 = TTL esgotado; Código 1 = Reagrupamento falhou)
4	Erro no cabeçalho IP, é indicada a posição do erro no cabeçalho do pacote IP original.
128/129	Respetivamente pedido e ECHO e resposta de ECHO. Implementação igual à do ICMPv4.
130	"GROUP MEMBERSHIP QUERY" – enviada aos ROUTERS para obter informação sobre grupos locais MULTICAST.
131	"GROUP MEMBERSHIP REPORT" – enviada pelos ROUTERS em resposta aos "GROUP MEMBERSHIP QUERY".
132	"GROUP MEMBERSHIP REDUCTION" – enviada aos ROUTERS quando um nó pretende sair de um grupo MULTICAST.
133	Pedido de ROUTER (RS) - enviada para o endereço MULTICAST ALL-ROUTERS para obter uma lista de ROUTERS.
134	Anúncio de ROUTER (RA) - enviada pelos ROUTERS em resposta ao pedido anterior.
135	Pedido de vizinho (NS) – usado para obter um endereço físico de um nó vizinho (equivalente a um pedido ARP).
136	Anúncio de vizinho (NA) – resposta ao pedido anterior (equivalente a uma resposta ARP).
137	REDIRECT – enviada pelo 1º ROUTER quando existe um caminho mais direto ou o nó de destino é vizinho.

Resolução de nomes



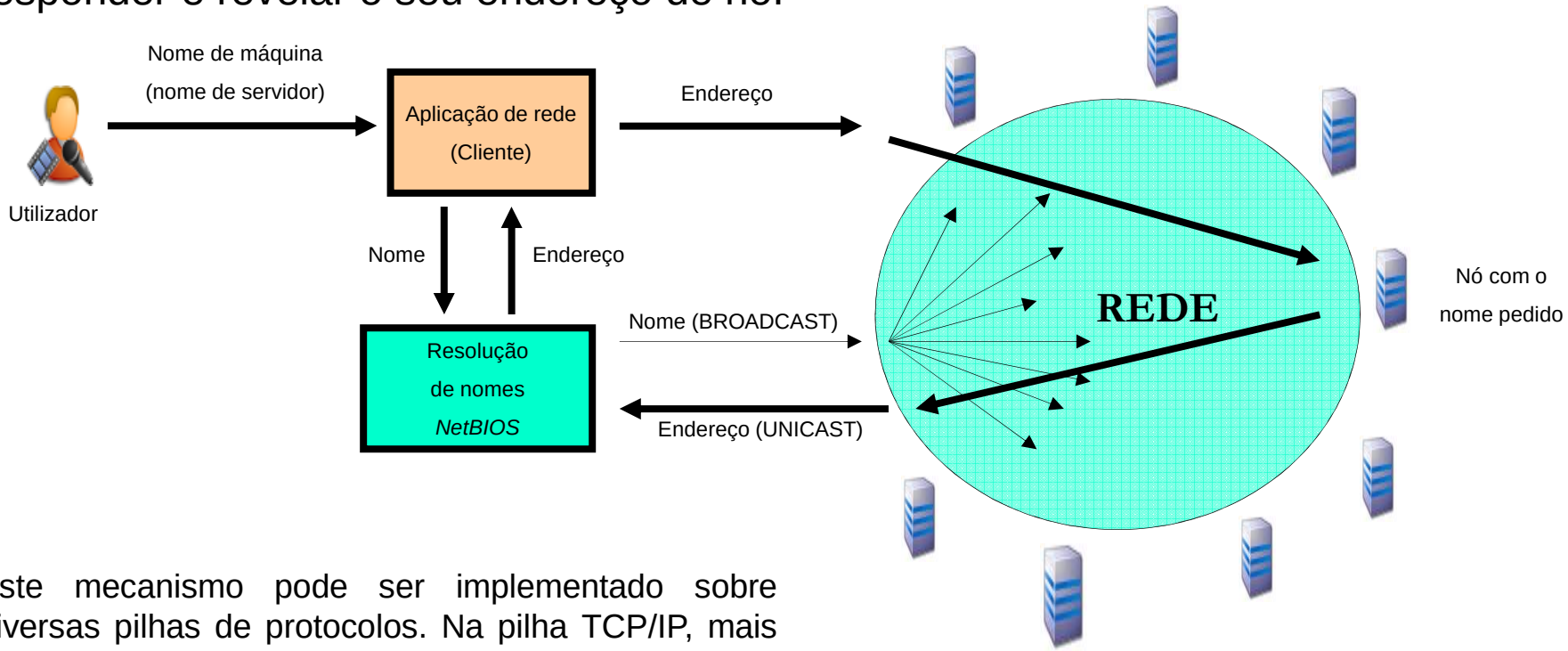
A manipulação de endereços de nó pelos utilizadores e administradores não é cómoda, mas em sob o ponto de vista da rede é o único elemento aceitável para identificar um nó sem ambiguidades.

A resolução de nomes tem como objetivo estabelecer uma ligação entre os utilizadores e os endereços de rede de tal forma que os primeiros não tenham de interagir diretamente com os segundos. Apoiados neste serviço os utilizadores podem usar nomes de máquinas bastante mais representativos para o ser humano.



Resolução de nomes - *NetBIOS*

De entre vários, um dos sistemas de resolução de nomes que teve bastante sucesso foi o do sistema *NetBIOS*. Integrado em redes PEER-TO-PEER, em que não existem servidores, o *NetBIOS* envolve o envio em BROADCAST do nome a resolver (*NAME QUERY*), desta forma o detentor desse nome vai ter oportunidade de responder e revelar o seu endereço de nó.



Este mecanismo pode ser implementado sobre diversas pilhas de protocolos. Na pilha TCP/IP, mais comum atualmente, é usado o protocolo UDP e o serviço é acessível no porto 137.

NetBIOS – Registo de nomes

O sistema de nomes *NetBIOS* foi concebido para redes sem servidores, cada nó tem a missão de responder aos pedidos de rede relativos ao seu nome.

Mesmo sem servidores há necessidade de ter algumas garantias de que os nomes são únicos, para esse efeito quando os nós arrancam enviam para a rede em BRODCAST vários pedidos de registo com o nome pretendido, durante este processo, qualquer nó que já esteja a usar o mesmo nome deve responder com uma mensagem de erro.

A ausência de qualquer resposta aos sucessivos pedidos de registo (*NAME REGISTRATION*), significa que o registo foi bem sucedido.

Um nó *NetBIOS*, antes de ser desligado anuncia à rede a libertação do nome que estava a usar (*NAME RELEASE*).

Tipos de Nomes *NetBIOS* (Windows)

Os nomes *NetBIOS* podem ser únicos ou de grupo, os nomes de grupo são registados pela mesma forma que os nomes únicos, mas podem estar registados por vários nós em simultâneo. Trata-se de um mecanismo simples de MULTICAST que pode ser usado para definir estruturas lógicas de grupos de nós na rede, por exemplo as redes Microsoft usam nomes de grupo para implementar os conceitos de WORKGROUP e DOMAIN.

Na norma original um nome *NetBIOS* pode ter até 16 caracteres, na implementação mais divulgada (Redes Windows) o 16º serve para identificar o tipo de nome. Habitualmente o tipo de nome é representado em notação hexadecimal separado por um "#" do nome. Por exemplo "SERVIDOR1#20" representa o nome "SERVIDOR1" do tipo 20 (hexadecimal). Alguns dos tipos de nomes importantes para as redes Windows são:

00	Nome único de uso geral
01	Associado ao nome especial "__MSBROWSE__" que identifica o coletor local de listas de nomes.
03	Nome de utilizador (clientes Windows antigos) e nome de nó/servidor.
1B	Associado ao nome do domínio identifica o PDC.
1C	Associado ao nome do domínio identifica um servidor de LOGIN no domínio.
1D	Associado ao nome do domínio identifica o representante local do domínio.
1E	Nome de domínio ou grupo de trabalho (WORKGROUP), todos os membros possuem este nome.
20	Nome de servidor (File Server)

Cada nó de rede *NetBIOS* contém vários nomes, por exemplo:

MYSERVER#00
MYSERVER#03
MYSERVER#20
__MSBROWSE__#01
MYDOMAIN#1B
MYDOMAIN#1C
MYDOMAIN#1D
MYDOMAIN#1E
HST222#00
HST222#03
HST222#20

WINS – Servidor de nomes *NetBIOS*

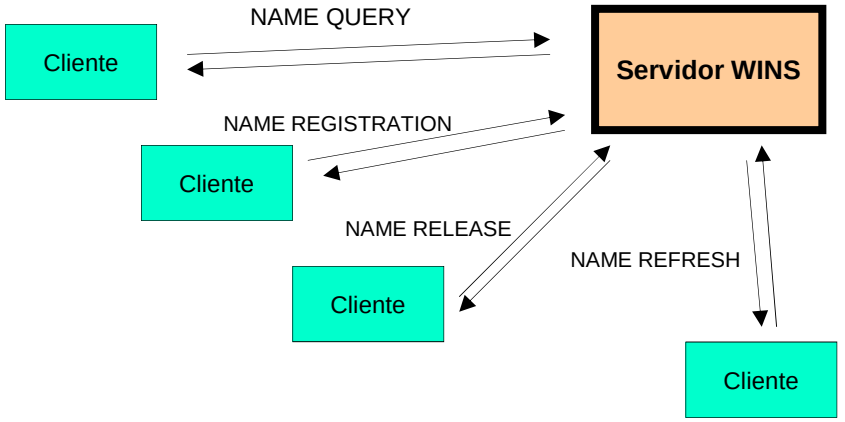
O protocolo de resolução de nomes *NetBIOS* baseado em *BROADCAST* apresenta vários problemas:
- Insegurança e falta de fiabilidade (registo por omissão; ambiente de confiança geral entre nós)
- Limitação de propagação do *BROADCAST* (sistema limitado a uma única rede)
- O tráfego em *BROADCAST* é penalizador para o desempenho das redes pois anula a segmentação de nível 2.

Para resolver estes problemas a Microsoft desenvolveu o serviço WINS (*Windows Internet Name Service*), contendo muito poucas alterações ao protocolo original de resolução de nomes, a principal diferença é que deixa de ser usado o *BROADCAST*.

Todos os pedidos são enviados em *UNICAST* para o servidor WINS, isso significa o servidor WINS pode encontrar-se numa rede remota e servir clientes de várias redes.

Além desta vantagem a transição para um modelo cliente/servidor leva a um aumento geral da segurança e fiabilidade. Agora todos os pedidos têm resposta.

Os registos de nomes estão associados a um tempo de vida, esgotado esse tempo são eliminados.



Futuro da resolução de nomes *NetBIOS*

O responsável por trazer até aos dias de hoje o *NetBIOS* é a Microsoft e os seus sistemas operativos. A utilização de servidores WINS em substituição do *BROADCAST* veio resolver quase todos os problemas e limitações que o sistema tinha anteriormente.

Os servidores WINS podem ser interligados de várias formas (usando protocolos proprietários), por exemplo numa perspetiva de replicação ou de consulta/registo remoto.
Apesar de eficiente num ambiente limitado, a sua aplicação em larga escala é problemática por se tratar de uma estrutura de nome totalmente rasa, para suportar um milhão de máquinas será necessário gerir uma base de dados com um milhão de registos distribuída por uma grande área (sem nunca haver registos repetidos).

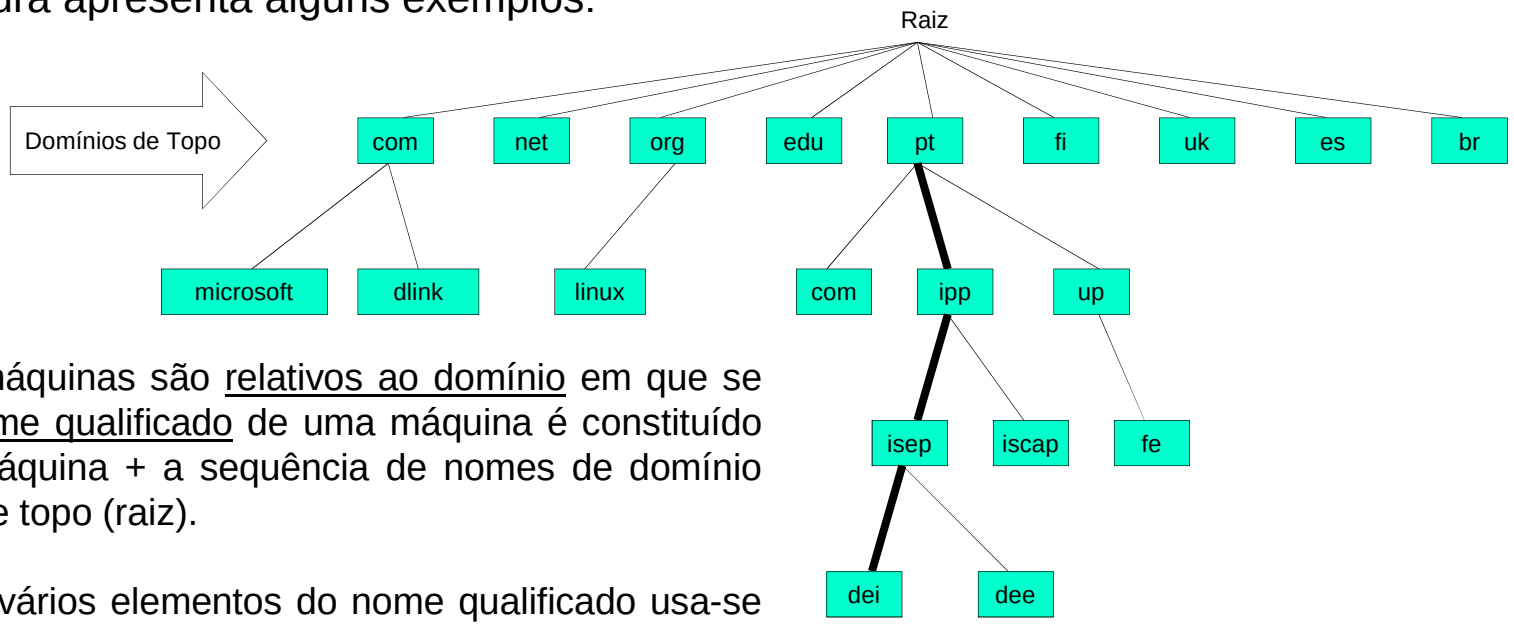
Outra lição que a história das redes e protocolos ensinou é que a coexistência de duas implementações paralelas que fazem o mesmo não dura muito tempo. Tal como a pilha de protocolos TCP/IP fez desaparecer outras implementações, também é previsível que o sistema DNS acabe por substituir totalmente o *NetBIOS*. Isso já é possível nos sistemas que usam *Active Directory*.

De momento verifica-se a coexistência WINS/DNS, alguns servidores WINS podem ser até configurados para recorrer a DNS quando não conseguem resolver um nome. Os clientes Windows também combinam o recurso a *NetBIOS* em *BROADCAST*, WINS e DNS, criando por vezes alguma confusão.

DNS – Domain Name System

O *Domain Name System* tem a grande vantagem de ser estruturado em árvore de tal forma que cada ramo é administrativamente independente dos outros ramos.

A independência entre ramos existe porque cada nome apenas tem significado no ramo em que é definido, para identificar globalmente um nome é necessário especificar não apenas o nome, mas também o ramo. Os ramos desta estrutura são conhecidos por nomes de domínios, a figura apresenta alguns exemplos:

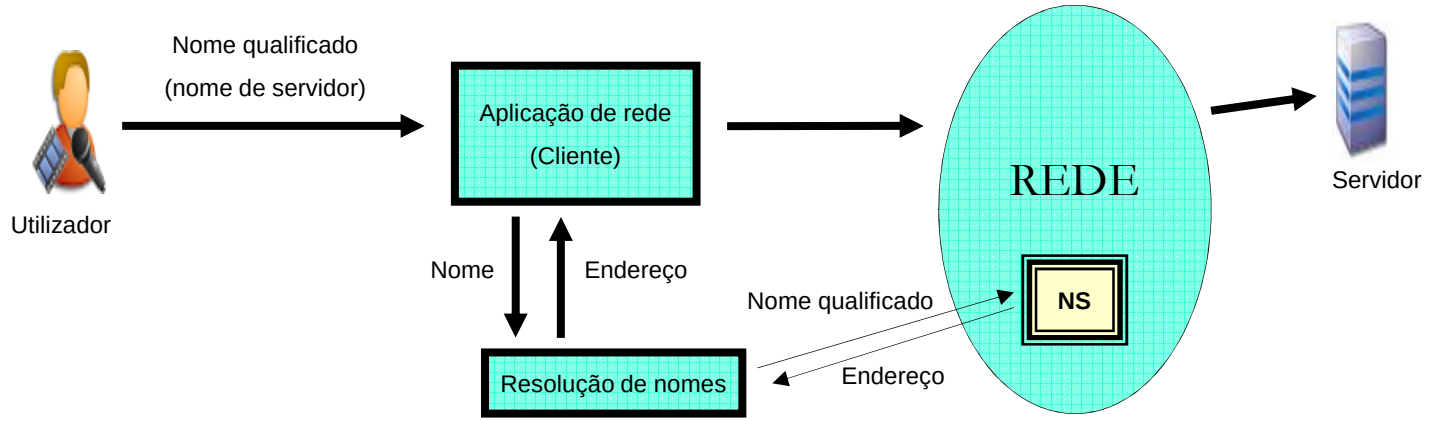


Os nomes das máquinas são relativos ao domínio em que se encontram, o nome qualificado de uma máquina é constituído pelo nome da máquina + a sequência de nomes de domínio até ao domínio de topo (raiz).

Para separar os vários elementos do nome qualificado usa-se um ponto. Por exemplo a máquina de nome “www” existente no DEI tem como nome qualificado “www.dei.isep.ipp.pt”

Servidores DNS

A estrutura lógica do DNS usa como plataforma uma rede de servidores de nomes. Os vários servidores de nomes (NS) comunicam entre si de tal forma que cada um deles é capaz de resolver qualquer nome qualificado de qualquer domínio. Para um cliente poder resolver qualquer nome da INTERNET basta-lhe conhecer o endereço de um servidor de nomes.



Cada servidor de nomes (NS) contém uma base de dados com todos os registos, mas apenas dos domínios que serve (normalmente apenas um domínio). Estes servidores têm autoridade sobre o domínio (*authoritative DNS servers*). Isso permite-lhe responder diretamente a pedidos referentes a esse domínio.
Para responder relativamente a toda a INTERNET o servidor de nomes tem de recorrer a outros servidores de nomes.

DNS – Rede de NS

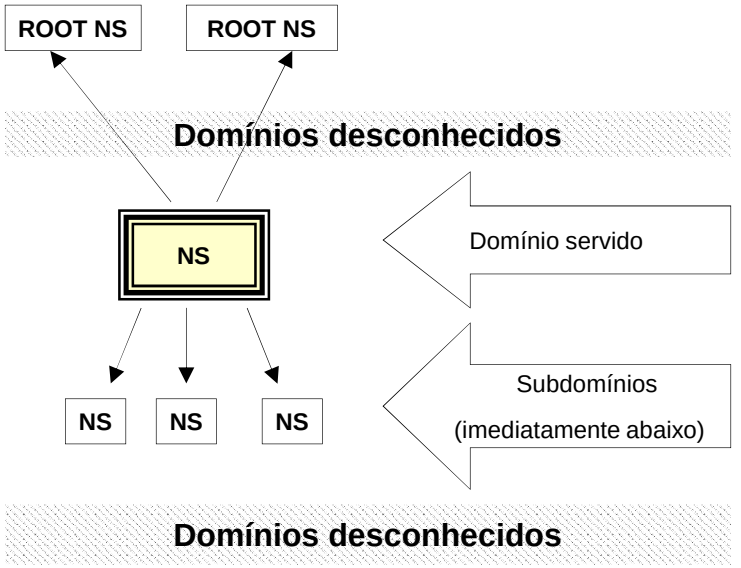
Para que o conjunto de servidores de nomes (NS) de todos os domínios permitam o funcionamento em conjunto é necessário que cada servidor de nomes contenha a seguinte informação:

- ✓ registos (nomes) do domínio que serve (ou cópia obtida do servidor principal).
- ✓ endereço dos servidores de nomes da raiz (acima dos domínios de topo).
- ✓ endereço dos servidores de nomes de cada subdomínio.

Todos os outros domínios e servidores de nomes são desconhecidos, mesmo assim é possível resolver qualquer nome.

A resolução é um processo descendente que começa num servidor de nomes da raiz.

Uma vez que cada servidor de nomes é obrigado a conhecer os servidores de nomes do domínio imediatamente abaixo, este processo conduz sempre ao servidor de nomes correto.



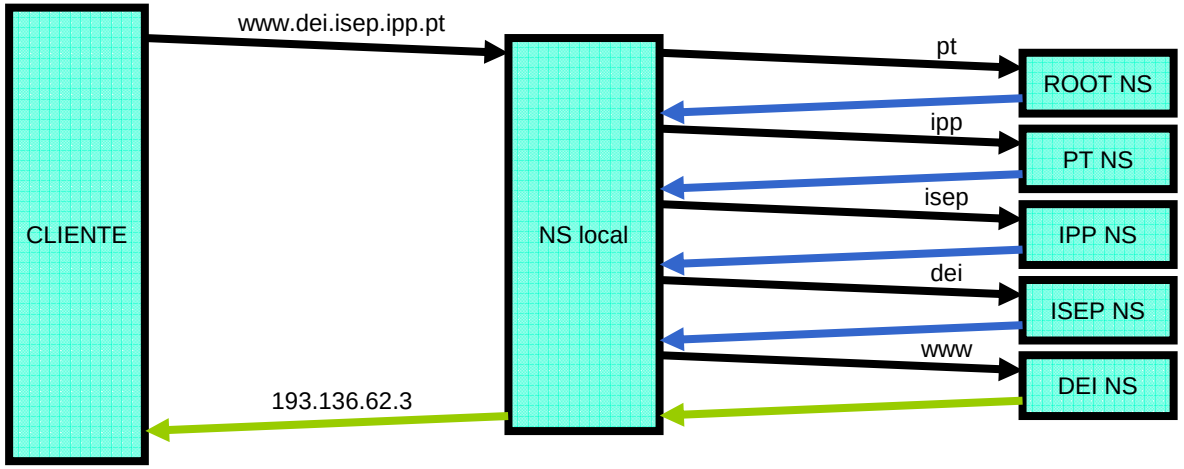
Resolução de nomes DNS

A resolução de nomes funciona em sentido descendente desde os domínios de topo. Se algures na INTERNET uma aplicação necessita do endereço de www.dei.isep.ipp.pt começa por contactar o servidor de nomes local cujo endereço conhece. O NS local contacta um NS de raiz e pede-lhe um servidor de nomes de "pt", o "ROOT NS" devolve-lhe o nome de um servidor de nomes do domínio "pt". O processo repete-se até chegar ao último elemento do nome.

Quando se pede um NS de um domínio é fornecido um nome e não um endereço.

Se o nome do NS pertence ao domínio, então ocorre um bloqueio do sistema devido a uma dependência circular.

Para resolver este problema adiciona-se ao domínio acima um registo com o endereço IP do NS. Este registo é conhecido por "glue record".



Os servidores de nomes têm de manter em cache as respostas que vão obtendo, para o efeito cada resposta tem associado um tempo de vida (TTL). O tempo de vida é definido pelo administrador de cada domínio e pode ter valores mais ou menos elevados. O *caching* das respostas reduz de forma muito significativa o recurso direto aos servidores de nomes de topo, nomeadamente os de raiz. Quanto maior for o TTL estipulado pelo administrador menor será a quantidade de pedidos que os respetivos servidores vão receber.

Registos DNS (*Resource Records*)

A base de dados de um servidor DNS é constituída por registos de diferentes tipos com diversas finalidades (*Resource Records*). Cada registo (RR) tem os seguintes elementos:

NOME (até 255 caracteres)	- Nome da entidade a quem se aplica o registo (proprietário do registo), terminado com ZERO.
TIPO	- Número de 16 bits que identifica o tipo de registo (RR TYPE)
CLASSE	- Número de 16 bits que identifica a classe (RR CLASS), para o IP apenas se usa o valor 1 (classe IN)
TTL	- Número de 32 bits que o tempo de vida em segundos do registo
RDLENGTH	- Número de 16 bits que define o tamanho do campo de dados em octetos
DADOS (comprimento variável)	- Dados que constituem o valor do registo (RDATA)

Os registos DNS (RR) são armazenados pelos servidores de nomes e são fornecidos aos clientes e outros servidores quando solicitados através de pedidos através da rede (DNS QUERY). Os servidores de nomes DNS atendem os pedidos devidamente formatados, no porto 53, normalmente as mensagens de pedido são encapsuladas em DATAGRAMAS UDP. Cada pedido contém uma ou mais perguntas segundo o formato:

NOME (até 255 caracteres)	TIPO	CLASSE

No campo “TIPO”, além dos valores de tipo de registo (RR TYPE), podem ser usados alguns valores especiais: o valor 255 (“*”) representa “qualquer tipo” e o valor 252 (“AXFR”) representa todos os RR do domínio, os pedidos AXFR são usados para sincronizar os vários servidores de nomes de um domínio, devido ao volume de registos envolvidos, neste caso recorre-se a uma ligação TCP para o mesmo número de porto usado em UDP.

Tipos de *Resource Record*

TIPO (RR TYPE)	Nome do Tipo - Objetivo	NOME (Proprietário)	DADOS
1	A - Endereço IPv4 correspondente um nome de nó	Nome de nó	Endereço IPv4
2	NS - Servidor de nomes	Nome de domínio (subdomínio)	Nome do NS (qualificado)
5	CNAME - Nome alternativo (alias)	Nome alternativo ou apelido (alias)	Nome oficial (Nome de nó)
6	SOA (Start Of Authority) define parâmetros do dom.	Nome do domínio	Diversos, incluindo nº de série da base de dados, …
12	PTR – nome correspondente a um endereço	Endereço (nome em IN-ADDR.ARPA.)	Nome de nó (qualificado)
15	MX – define um "mailhub" do domínio	Nome do domínio	Prioridade+Nome do servidor
16	TXT – define um comentário	Nome de domínio	Texto livre (comentário)
28	AAAA - Endereço IPv6 correspondente um nome de nó	Nome de nó	Endereço IPv6
29	LOC – define a localização geográfica do domínio	Nome de domínio	Coordenadas geográficas
33	SRV – define um serviço de rede	_serviço._protocolo.Nome de domínio	Prioridade+Peso+Porto+Nome do servidor
99	SPF – "Sender Policy Framework"	Nome de domínio	Restrições ao envio de mail em nome do domínio

Exemplo de registo SOA em ficheiro de configuração de zona do "BIND 9" em Linux

```
@ 99999999 SOA picasso.dei.isep.ipp.pt. root.picasso.dei.isep.ipp.pt. (
                                2008042402      ; serial
                                28800           ; refresh (8 hours)
                                7200            ; retry (2 hours)
                                604800          ; expire (7 days)
                                86400           ; minimum (1 day)
                                )
```

@ representa o nome do domínio da zona a que este registo se aplica, no caso "dei.isep.ipp.pt". (diretiva "$ORIGIN" no BIND)

TTL – é sempre um valor numérico em segundos, pode ser omitido.

A classe foi omitida, o valor por omissão é "IN".

Servidor de nomes primário.

O número de série é usado para sincronismo, contém a identificação do dia, e um número de série dentro desse dia.

DNS RR – Nomes e *aliases* (apelidos - pseudónimos)

Exemplo com endereços IPv4 (A), comentários (TXT) e apelidos (CNAME) - configuração de zona no BIND

```
mafalda2    99999999    A           193.136.62.4
frodo       99999999    A           193.136.62.2

frodo       99999999    TXT         "Servidor de mail e web"
mafalda2    99999999    TXT         "Servidor de contas de utilizador"

mafalda     99999999    CNAME       mafalda2
www         99999999    CNAME       frodo
pop         99999999    CNAME       frodo
mail        99999999    CNAME       frodo
pdc         99999999    CNAME       mafalda2
smb         99999999    CNAME       mafalda2
samba       99999999    CNAME       mafalda2
```

Apelidos (Alias)

Nomes canónicos
(nomes reais / próprios)

Uma vez que este exemplo se encontra associado à definição da zona "dei.isep.ipp.pt", entre outros, o nome "www.dei.isep.ipp.pt" vai ser resolvido para o endereço "193.136.62.2".

DNS RR – NS e “glue records”

Os registos NS são fundamentais no sistema DNS, são eles que garantem a ligação descendente entre os domínios. Para manter a ligação, cada domínio tem de conhecer os servidores de nomes dos seus subdomínios.

Exemplo com subdomínio (dei.isep.ipp.pt) - configuração de zona (isep.ipp.pt) no BIND

```
$ORIGIN isep.ipp.pt
@    IN SOA nsrv1.isep.ipp.pt admin.isep.ipp.pt 2007120500 2h 15M 3W12h 2h20M

@           IN          NS          nsrv1.isep.ipp.pt
@           IN          NS          nsrv2.isep.ipp.pt

nsrv1       IN          A           193.136.6.40
nsrv2       IN          A           193.136.6.47


dei.isep.ipp.pt         IN          NS          picasso.dei.isep.ipp.pt
dei.isep.ipp.pt         IN          NS          slave.dei.isep.ipp.pt

picasso.dei.isep.ipp.pt IN          A           193.136.62.3
slave.dei.isep.ipp.pt   IN          A           193.136.62.110
```

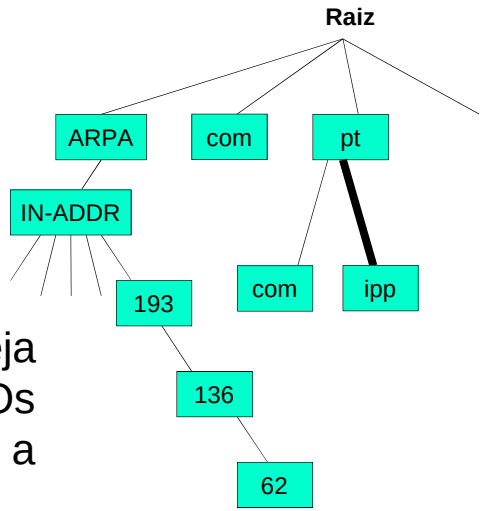
Os registos NS definem os nomes qualificados dos servidores de nomes

Os “glue records” (destacados a verde) são registos de endereço (A) que não pertencem ao domínio, mas são necessários para obter os endereços dos servidores de nomes.

Sem o “glue record” a última resolução não seria possível, pois quem a deveria realizar seriam os servidores de nomes do domínio “dei.isep.ipp.pt”.

DNS RR – PTR e domínio IN-ADDR.ARPA.

O domínio especial “IN-ADDR.ARPA” contém um registo da estrutura de endereços IPv4. Cada nível de subdomínio corresponde a um octeto do endereço IPv4, o octeto da esquerda corresponde ao subdomínio superior.



Os nomes “IN-ADDR.ARPA” servem para resolução inversa, ou seja obter o nome DNS usando o endereço como ponto de partida. Os registos PTR permitem definir estes nomes correspondentes a endereços.

Exemplo “in-addr.arpa.” - configuração de zona no BIND

```
2.62.136.193.in-addr.arpa          IN          PTR         frodo.dei.isep.ipp.pt
3.62.136.193.in-addr.arpa          IN          PTR         picasso.dei.isep.ipp.pt
4.62.136.193.in-addr.arpa          IN          PTR         mafalda2.dei.isep.ipp.pt
```

Exemplo “in-addr.arpa.” com directiva “$ORIGIN” - configuração de zona no BIND

```
$ORIGIN 62.136.193.in-addr.arpa

2    IN      PTR         frodo.dei.isep.ipp.pt
3    IN      PTR         picasso.dei.isep.ipp.pt
4    IN      PTR         mafalda2.dei.isep.ipp.pt
5    IN      PTR         srv1.dei.isep.ipp.pt
6    IN      PTR         srv2.dei.isep.ipp.pt
```

Os registos PTR têm de ser consistentes com os registos A.

Correio eletrónico

Os domínios DNS são usados pelo correio eletrónico da internet para identificar destinatários no domínio (DESTINATÁRIO@NOME-DO-DOMÍNIO).

Para entregar as mensagens de correio ao domínio é necessário identificar e contactar um dos seus servidores de correio SMTP (*Simple Mail Transfer Protocol*).

Uma solução possível é recorrer ao domínio superior e criar um registo “A” associado ao nome do domínio que representa o endereço IP do servidor de correio:

Exemplo com RR A para os subdomínios - configuração de zona (isep.ipp.pt) no BIND

```
$ORIGIN isep.ipp.pt
@    IN SOA nsrv1.isep.ipp.pt admin.isep.ipp.pt 2007120500 2h 15M 3W12h 2h20M

dei.isep.ipp.pt         IN          A          193.136.62.2
dee.isep.ipp.pt         IN          A          193.136.63.3
```

Servidor de mail de cada subdomínio

(MTA – Mail Transfer Agent ; Mail server; Mail Exchanger)

Por exemplo, o envio de uma mensagem para “username@dei.isep.ipp.pt”, começa pela resolução de “dei.isep.ipp.pt”, obtendo-se “193.136.62.2”. De seguida é usado o protocolo SMTP para enviar a mensagem ao nó 193.136.62.2, esse é o servidor de correio.

DNS RR – MX

Os registos MX (Mail eXchanger) servem para identificar de forma mais eficiente os servidores de correio de um domínio, relativamente à alternativa anterior têm a vantagem de permitir definir vários servidores com diferentes níveis de preferência e além disso podem ser implementados sem recurso ao domínio superior.
Um domínio pode ter vários registos MX, cada um definindo o nome do servidor (tem de ser um nome canónico, não pode ser um apelido) e o nível de preferência de 16 bits (números inferiores significam preferência mais elevada).

Exemplo de registos MX - configuração de zona no BIND

```
dei.isep.ipp.pt          IN          MX          10          frodo.dei.isep.ipp.pt
dei.isep.ipp.pt          IN          MX          20          picasso.dei.isep.ipp.pt

picasso.dei.isep.ipp.pt IN          A           193.136.62.3
frodo.dei.isep.ipp.pt   IN          A           193.136.62.110
```

Utilizando a informação do exemplo, quem pretender enviar correio para o domínio "dei.isep.ipp.pt" vai obter uma lista de dois servidores, em primeiro lugar vai tentar usar o "frodo.dei.isep.ipp.pt".

É possível definir vários servidores de correio com a mesma preferência, nesse caso o BIND aplica o algoritmo "round-robin" à ordem dos registos devolvidos aos clientes, como nesta situação os clientes usam o primeiro registo consegue-se distribuir os pedidos pelos vários servidores.

DNS RR – SRV

Os registos SRV (RFC 7282) têm como objetivo permitir aos clientes identificar num domínio servidores de determinado tipo (serviços). Como consequência estes registos servem também para os servidores divulgarem os seus serviços (Ex.: Active Directory).

Os registos SRV são associados a nomes simbólicos que representam tipos de serviço no contexto de um domínio, na forma: **_{Serviço}._{Protocolo}.{Nome-do-domínio}**
O caractere sublinhado serve para evitar conflitos com nomes de domínio "normais".
{Serviço} é um identificador de serviço normalizado.
{Protocolo} identifica a plataforma de transporte a usar ("udp" ou "tcp").

O registo SRV propriamente dito contém um nível prioridade semelhante ao dos registos MX, e um nível de peso que se aplica entre registos com o mesmo nome e mesma prioridade. Segue-se o número de porto usado pelo serviço e o nome canónico do servidor.

Exemplo de registos SRV - configuração de zona no BIND

```
_ldap._tcp.dei.isep.ipp.pt          IN  SRV     5 4 389     mafalda2.dei.isep.ipp.pt
_ldap._tcp.dei.isep.ipp.pt          IN  SRV     5 6 389     frodo.dei.isep.ipp.pt
_ldap._tcp.dei.isep.ipp.pt          IN  SRV     20 20 389   picasso.dei.isep.ipp.pt
```

No exemplo, quando um cliente LDAP pretende encontrar um servidor no domínio "dei.isep.ipp.pt" pede ao servidor de nomes o registo SRV do nome "_ldap._tcp.dei.isep.ipp.pt", recebendo 3 respostas, destas seleciona desde logo as de mais elevada prioridade (no caso 5) de entre elas vai entrar em consideração com os pesos (4 e 6), por isso existe 40% de probabilidade de usar o 1º e 60% de probabilidade de usar o 2º.

DNS RR – SPF

O documento RFC 4408 (Sender Policy Framework (SPF) for Authorizing Use of Domains in E-Mail, Version 1) define formas de os domínios divulgarem as suas politicas relativamente a quem pode emitir mensagens de correio eletrónico em nome de utilizadores desse domínio.
Quando um servidor SMTP recebe uma mensagem, deve verificar no domínio do remetente (campo From) se quem está a tentar enviar tem autorização para tal.

O registo DNS SPF é um registo de texto associado ao nome do domínio, uma vez que este tipo de registo é bastante recente, inicialmente foi implementado através de um registo TXT.

Exemplo de registos SPF - configuração de zona no BIND

```
dei.isep.ipp.pt         IN  SPF     "v=spf1 +mx -all"
dei.isep.ipp.pt         IN  TXT     "v=spf1 +mx -all"
```

RFC 7208 acabou por descontinuar os registos do tipo SPF mantendo apenas a utilização de registos do tipo TXT para o efeito.

O texto associado define quem está autorizado a enviar em nome do domínio, começa por identificar a versão (v=spf1) e depois define quem está autorizado (+) e quem não está (-). No caso apenas os MX do domínio estão autorizadas a enviar.
O texto de autorização suporta um grande número de possibilidades (ver RFC 4408).

DNS RR – LOC

O registo LOC serve para definir a localização geográfica do domínio, como tal é normalmente associado ao nome de domínio.

O registo LOC contém:

- -Latitude em graus, minutos e segundos
- -Longitude em graus, minutos e segundos
- -Altitude em metros.
- -Tamanho em metros (diâmetro da esfera que contém o local)
- -Precisão horizontal e precisão vertical

Exemplo de registo LOC - configuração de zona no BIND

```
dei.isep.ipp.pt         IN  LOC  41 10 39.782 N 8 36 28.578 W 50.00m 100m 10m 10m
```

O registo define as características geográficas do domínio “dei.isep.ipp.pt” como sendo latitude = 41º 10’ 39,782” Norte ; longitude = 8º 36’ 28,578” Oeste ; altitude = 50 metros; dimensão = 100 metros; precisão horizontal = 10 metros e precisão vertical = 10 metros.

Exemplos de interrogação de registos LOC

```
-bash-3.00$ host -t LOC yahoo.com
yahoo.com location 37 23 30.900 N 121 59 19.000 W 7.00m 100m 100m 2m
-bash-3.00$ host -t LOC ckdhr.com
ckdhr.com location 42 21 43.528 N 71 5 6.284 W -25.00m 1m 3000m 10m
-bash-3.00$ host -t LOC dei.isep.ipp.pt
dei.isep.ipp.pt location 41 10 39.782 N 8 36 28.578 W 50.00m 100m 100m 10m
```

DDNS – DNS Dinâmico

As bases de dados DNS foram concebidas para serem raramente alteradas, as alterações são feitas manualmente, os valores TTL normalmente usados atestam isso mesmo.

Existem contudo situações em que o registo automático do nome pelo próprio cliente seria desejável, nomeadamente quando o cliente não possui um endereço fixo.
O carácter dinâmico dos registos torna a administração muito mais simples, por exemplo com os registos SRV, os atuais servidores Windows, nomeadamente os controladores de domínio anunciam-se no servidor DNS através de registos SRV.

O documento RFC 2136 adiciona ao sistema de mensagens DNS (RFC 1035) as funcionalidades necessárias para atualizações dinâmicas de registos DNS, é usado pelo comando “nsupdate”.
Os processo de alteração da base de dados estão protegidos por mecanismos de segurança dos quais se destaca o “Generic Security Service Algorithm for Secret Key Transaction Authentication for DNS (GSS-TSIG)” descrito no documento RFC 3645 e adotado pela Microsoft (*Microsoft DNS*).

Os servidores DNS também podem ser atualizados por outras vias paralelas, alteram os ficheiros de configuração DNS e obrigam o servidor DNS a reler os mesmos, por exemplo o comando “ddclient” funciona deste modo usando pedidos HTTP.