

DNS

DOMAIN NAME SYSTEM

O DNS (Domain Name System) é um serviço de resolução de nomes. Embora cada programa pudesse referir os utilizadores por números é difícil para os humanos terem presente em memória todos os endereços que pretendem utilizar. No caso dos endereços IP o facto de estarem organizados em grupos de números xxx.yyy.zzz.hhh mesmo assim torna-se inconveniente utilizar um endereço de mail eu@85.123.34.42. Se por acaso o endereço do servidor de mail é alterado o mail também o é. Torna-se assim necessário a existência de uma tabela de conversão de nomes em endereços de modo a poder desarticular as duas referências.

No início da ARPANET havia um ficheiro hosts.txt com o nome de todos os utilizadores e seus endereços IP. Ao fim do dia todos os equipamentos utilizadores iriam buscar este ficheiro para actualizar os seus. Este método funciona relativamente bem para redes com o máximo de uma centena de máquinas.

Com o aumento do número de máquinas ligadas procurou-se adoptar outro método, não só devido à dimensão dos ficheiros mas também porque diversas subredes poderiam atribuir endereços cujos nomes entrariam em conflito, o que obrigaria a uma gestão centralizada de nomes. Surge assim o DNS.

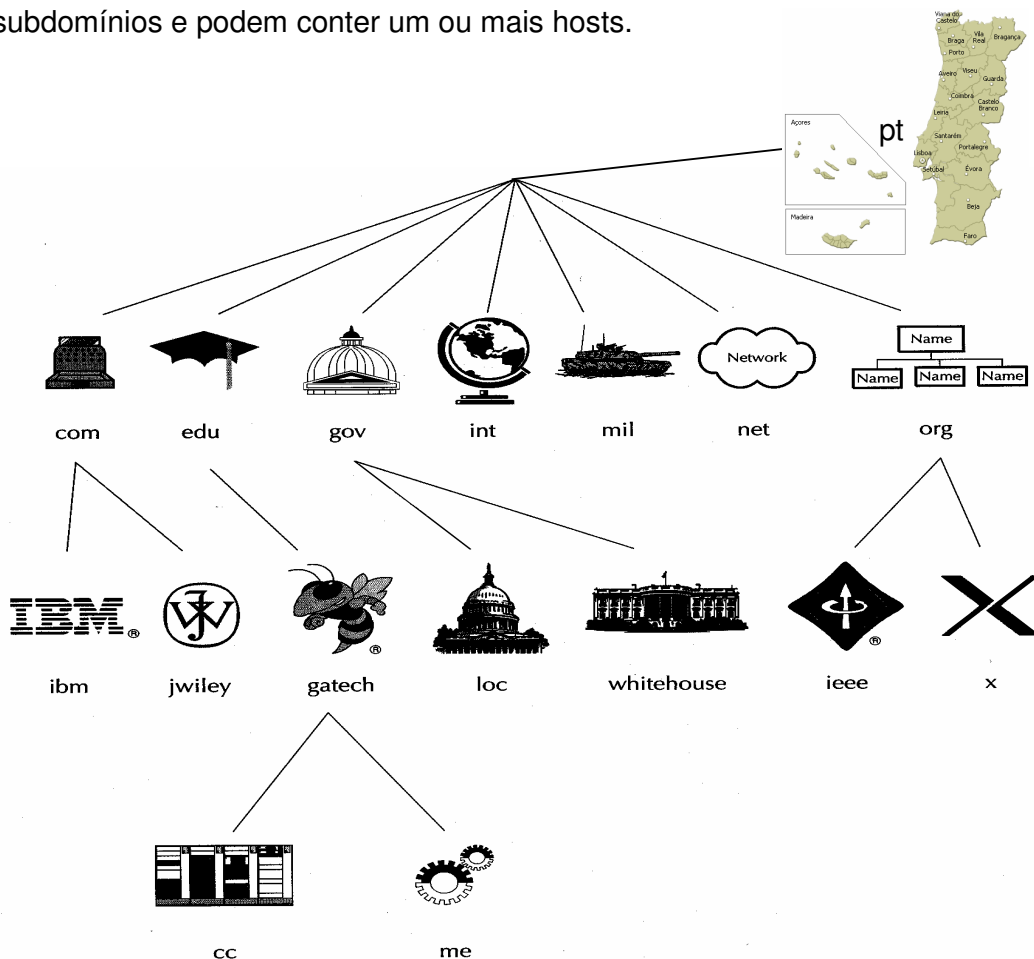
O DNS, Domain Name System, é um esquema hierárquico de mapeamento de nomes numa base de dados distribuída. Embora a utilidade principal do DNS seja a da atribuição de nomes das máquinas e dos endereços de e-mail também pode ser utilizado para outro tipo de informação. Está definido nos RFCs 1034 e 1035.

De um modo simples pode-se dizer que o DNS funciona da seguinte forma: Para mapear um nome ao seu endereço IP correspondente a aplicação evoca um procedimento da biblioteca (library) chamado *resolver* tendo o dito

nome como parâmetro. O resolver (`gethostbyname()`) envia um pacote UDP para o servidor DNS local que procura na tabela e devolve um endereço IP ao resolver, e este por sua vez entrega-o ao processo cliente que estabelece contacto com o destinatário usando pacotes TCP ou UDP.

Domain Name Space

Encontramos como um bom exemplo de atribuição de nomes a experiência que os correios têm na entrega de cartas. Pessoas distintas com o mesmo nome, em ruas com o mesmo nome, em localidades diferentes têm a sua correspondência bem encaminhada. Este método de endereçamento hierárquico funciona muito bem e em poucas linhas nome, rua, localidade, país determina qualquer pessoa que vive numa habitação numa zona urbanizada. O equivalente ao país é na Internet o top-level domain com mais de 200. Cada domínio destes está subdividido em vários subdomínios e estes noutros e assim sucessivamente. Podemos representar esta distribuição, como também a dos correios, numa árvore. As folhas das árvores representam domínios sem subdomínios e podem conter um ou mais hosts.



O top-level domain pode conter dois tipos de domínios, os genéricos e os de países. Os genéricos (gTLD - generic Top Level Domain) são os seguintes:

- arpa — (advance research projects agency) – Address and Routing Parameter Area
- com — comercial
- edu — estabelecimentos comerciais (primarily US)
- gov — governo dos EUA
- net — infraestrutura de rede
- org — outras organizações que não se enquadram nas restantes gTLDs
- mil — serviços militares dos EUA

Para os países existe uma notação de duas letras (ex: Portugal Pt, Brasil Br) e estão definidos no ISSO 3166.

Foram introduzidos depois do ano 2000 mais outros domínios na raiz

- aero — industria aeronáutica
- biz — businesses, negócios
- coop — cooperativas
- info — informação sem restrições (unrestricted use)
- museum — museus
- name — individuais
- pro — profissionais

Há uma série de LLDs reservados pela RFC 2606 para que não seja possível encontrar esses domínios a partir da raiz.

reserves the following four top-level domain names for various purposes, with the intention that these should never become actual TLDs in the global DNS:

- example — reservado para uso em exemplos
- invalid — reservado para uso em domínios não válidos
- localhost — reservado para evitar confusão com o termo localhost

- test — reservado para uso em testes

Os nomes de domínio podem ser relativos ou absolutos. Os nomes absolutos terminam sempre com um ponto (. dot), (ex: sapo.pt.). Os nomes relativos têm de ser vistos dentro de um determinado contexto (ex: meu.blog = meu.blog.sapo.pt.)

É indiferente a utilização de letras maiúsculas ou minúsculas na atribuição dos nomes.

Há domínios que podem estar duplicados por exemplo cc.yale.edu é idêntico a cc.yale.ct.us, o que acontece frequentemente por estarem nos EUA. Há também organizações multinacionais que têm diversos domínios registados, como é o caso da sony.com, sony.nl.

Cada país faz a sua organização, por exemplo a Holanda coloca tudo sob o nl, como o caso de Portugal pt, porém o Brasil utiliza uma distribuição que imita o top-level domain (sombrasil.ig.com.br).

Para se registar um nome tal tem de ser pedido ao registar do domínio, por exemplo (edu, com, pt, br, com.br). Depois os subdomínios são atribuídos responsabilmente pelo detentor do domínio sem ter de ir ao registar da raiz. Deste modo os ISP portugueses como o caso do clix, sapo, netcabo, e outros podem aceitar os nomes que bem entenderem escolhidos pelos seus clientes sem que seja necessária qualquer aprovação por uma instância superior. Pode também haver repetições de nomes sem qualquer confusão, por exemplo zecabra.no.sapo.pt e zecabra.netcabo.pt.

A organização em domínios nada tem a ver com a distribuição espacial física, podendo assim coexistirem no mesmo local máquinas com domínios diferentes e pertencendo ao mesmo domínio de outras noutros lugares do mundo.

Resource Records

Todos os domínios, quer sejam de uma única máquina ou um dos da raiz podem ter um conjunto de resource records associado. Para o caso de uma única máquina, o registo *resource records* apenas tem o endereço IP da

máquina. Quando um *resolver* dá um nome a um servidor DNS obtém os *resource records* associados com esse nome. Assim, a função primária do DNS é a de mapear nomes de domínio a um registo de recursos.

Um registo de recursos é uma tabela com 5 colunas. Estão codificadas em binário por uma questão de eficiência, e são representadas em ASCII para se poder compreender.

Domain_Name Time_to_Live Class Type Value

Domain_Name – indica o domínio a que se refere o registo. Podem haver diversas entradas com o mesmo nome de domínio. A ordem pela qual está escrita a tabela não tem qualquer importância. É este o nome que o DNS vem procurar.

Time_to_Live – Dá uma indicação da estabilidade do valor da entrada correspondente. No caso do domínio correspondente ser muito estável, o valor pode ser grande, 86400 (o número de segundos num dia). Informação volátil pode ter valores como 60 segundos. Este campo é utilizado pela cach que será explicada mais à frente.

Class – No caso da Internet este valor é sempre IN, e toma outros valores para informação que não pertence à Internet.

Type – Indica o tipo de registo. Ao tipo está associado o campo seguinte de Value que contém valores necessários para o tipo de registo assinalado. Existem os seguintes tipos:

TYPE	Significado	VALUE
SOA	Start of Authority	Parâmetros
A	IP address of a host	Inteiro a 32 bits
MX	Mail Exchange	Prioridade, domínio_e_mail
NS	Name Server	Nome do servidor para este domínio
CNAME	Canonical name	Nome do Domínio
PTR	Pointer	Alias para um endereço IP
HINFO	Host description	CPU e Sistema Operativo, em ASCII
TXT	Text	Comentário

SOA – Contém o nome da fonte primária de informação do servidor de zona (explicado mais à frente), o endereço de mail do administrador, um número de série único, algumas flags e timeouts.

A – Este é o valor pretendido quando se quer saber o endereço IP de uma determinada máquina neste domínio. Uma máquina pode ter mais do que um endereço IP o que se reflecte aqui com tantas entradas quantos os endereços IP que tiver. Nesta situação, oDNS pode ser configurado para responder com um endereço diferente de cada vez que se recebe um pedido do *resolver* com o mesmo nome. Este é o tipo de registo mais importante da tabela.

MX – É o segundo tipo de registo mais importante. Especifica o nome do host preparado para receber mail para o domínio especificado. Isto é necessário porque nem todas as máquinas estão preparadas para receber e-mail.

NS – Especifica o name server que está acima hierarquicamente caso este não tenha a informação pretendida.

CNAME – É um modo de criar aliases. Por exemplo para enviar mail para o marius no ISR pode enviar-se assim marius@isr.ist.pt, contudo o endereço correcto é marius@dsor.isr.ist.utl.pt. Facilita assim o envio de mail sem que o remetente saiba exactamente o endereço correcto do destinatário e apenas a empresa em que trabalha.

PTR – É idêntico ao CNAME mas neste caso associado a um endereço IP físico. Pode ser utilizado de um modo indirecto para obter o endereço IP de uma máquina e depois devolver o nome correcto dessa máquina que entretanto está com uma entrada A. Esta procura inversa tem o nome de *reverse lookups*.

HINFO – Permite saber informação acerca da máquina a que corresponde o domínio.

TXT – É utilizado como uma identificação própria, serve de comentário e este valor não é essencial, tal como o HINFO, nem todos os programas os

procuram nem tem de haver uma resposta a um pedido para este tipo de informação.

Apresenta-se um exemplo hipotético para o domínio cs.vu.nl

```
; Authoritative data for cs.vu.nl
cs.vu.nl.      86400  IN  SOA   star boss (9527,7200,7200,241920,86400)
cs.vu.nl.      86400  IN  TXT   "Divisie Wiskunde en Informatica."
cs.vu.nl.      86400  IN  TXT   "Vrije Universiteit Amsterdam."
cs.vu.nl.      86400  IN  MX    1 zephyr.cs.vu.nl.
cs.vu.nl.      86400  IN  MX    2 top.cs.vu.nl.

flits.cs.vu.nl. 86400  IN  HINFO Sun Unix
flits.cs.vu.nl. 86400  IN  A     130.37.16.112
flits.cs.vu.nl. 86400  IN  A     192.31.231.165
flits.cs.vu.nl. 86400  IN  MX    1 flits.cs.vu.nl.
flits.cs.vu.nl. 86400  IN  MX    2 zephyr.cs.vu.nl.
flits.cs.vu.nl. 86400  IN  MX    3 top.cs.vu.nl.
www.cs.vu.nl.   86400  IN  CNAME star.cs.vu.nl
ftp.cs.vu.nl.   86400  IN  CNAME zephyr.cs.vu.nl

rowboat        IN  A     130.37.56.201
               IN  MX    1 rowboat
               IN  MX    2 zephyr
               IN  HINFO Sun Unix

little-sister  IN  A     130.37.62.23
               IN  HINFO Mac MacOS

laserjet       IN  A     192.31.231.216
               IN  HINFO "HP Laserjet III Si" Proprietary
```

As primeiras entradas nesta tabela são a identificação do domínio e seu administrador. Seguem-se duas entradas que indicam os servidores de mail que devem ser tentados pela prioridade apresentada. Se for recebido um mail para `pessoa@cs.vu.nl`, o mail será encaminhado para a máquina `zephyr.cs.vu.nl` e caso esta não esteja disponível encaminha-se para a `top.cs.vu.nl`

Segue-se a máquina `flits` com dois endereços IP e três possíveis servidores de mail.

A linha seguinte é um alias para a página `www.cs.vu.nl` de modo que o servidor pode alterar sem que essa mudança se reflita em todos os que já

conhecem o endereço. Tanto o servidor de web como o de ftp estão nas máquinas indicadas pelo alias.

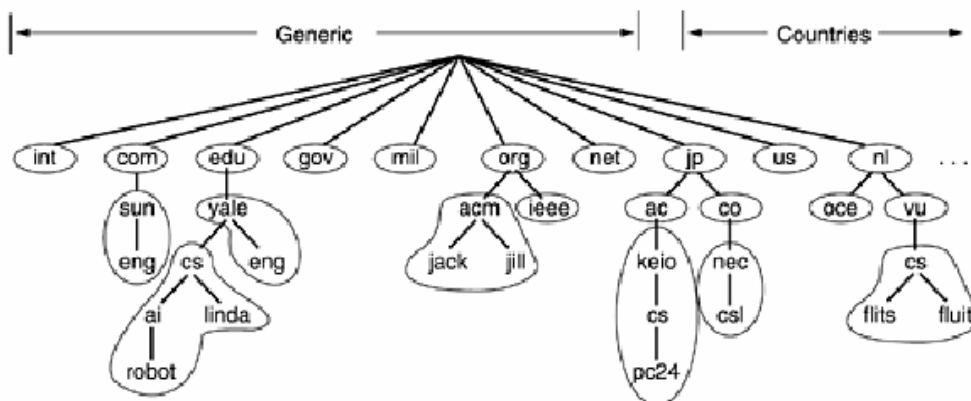
Segue-se a entrada para uma workstation rowboat, e a de uma máquina que não pode receber e-mail directamente, a little-sister, e por fim uma impressora de rede.

A informação que não está neste ficheiro e que se encontra noutra é a dos endereços IP dos servidores de nomes para este domínio, hierarquicamente acima, e como não pertencem ao domínio cs.vu.nl, não se encontram aí.

Essa informação está nos root servers cujos endereços IP estão presentes num ficheiro de configuração e que é introduzido na cache do DNS quando o servidor é iniciado a partir do boot. Há cerca de 13 root-servers e basta saber o endereço de um que esse sabe o endereço dos outros e a partir daí qualquer endereço IP na Internet pode ser conhecido.

Name Servers

Teoricamente bastaria um único root-server para dar os endereços IP, mas como há a possibilidade das máquinas e ligações falharem bem como todo o peso do tráfego dirigido a uma única máquina o espaço de nomes é dividido em zonas que não se intersectam. As zonas podem ser divididas de modo a conter parte da árvore e alguns name-servers que contêm informação dessa zona. Um exemplo encontra-se na figura seguinte.



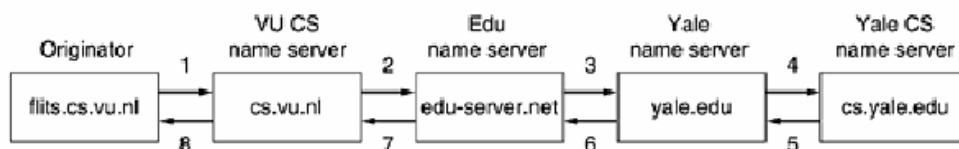
Cada zona contém normalmente um primary name server que tem a informação em disco, e um secondary name server que obtém a informação do primary name-server. O name-server secundário ou outros podem situar-se fora da zona por uma questão de fiabilidade.

Os limites de zona ficam sob a responsabilidade do administrador. Na figura apresentada, na universidade de Yale o name-server yale.edu serve yale.edu e eng.yale.edu e o departamento de ciências da computação cs.yale.edu tem o seu próprio servidor de nomes e enquadra-se assim numa outra zona.

Quando um resolver interroga acerca de um nome de domínio um dos servidores locais responde. Se o domínio procurado enquadra-se dentro do domínio do name-server, é devolvido o *authoritative resource record*. Por exemplo a procura do domínio de ai.cs.yale.edu pertence a cs.yale.edu e é devolvido o registo correspondente.

O registo *authoritative* é aquele que é gerido directamente pela administração e por isso está sempre correcto. Os outros que não são *authoritative* pertencem à cache e podem por isso estar desactualizados.

No caso do domínio pretendido ser remoto e não haver informação acerca dele localmente, o o name server envia um pedido para o top-level name server do domínio pretendido. Por exemplo o flits.cs.vu.nl quer saber o endereço IP de linda.cs.yale.edu. Então o pedido segue o trajecto da figura até chegar a cs.yale.edu que responde com o authoritative resource record. À medida que a resposta segue o caminho de volta, ela é colocada em cache de tal modo que se houver mais algum pedido para o mesmo endereço IP, é devolvido o da cache. Contudo, esse valor pode mudar, por isso é que é atribuído a cada valor de cache um tempo de vida *time_to_live*, para assegurar que alterações efectuadas pelo administrador nas entradas authoritative, acabam por serem sentidas mais tarde por aqueles que pretendem aceder às máquinas desse domínio.



- o ver http://www.juliobattisti.com.br/artigos/windows/tcpip_p8.asp

13 root name servers, nomeados na forma X.ROOT-SERVERS.NET onde o X indica uma letra de A a M

	old name	operator	location
A	ns.internic.net	VeriSign	Dulles, VA
B	ns1.isi.edu	ISI	Marina Del Rey, CA
C	c.psi.net	Cogent	Herndon, VA
D	terp.umd.edu	University of Maryland	College Park, MD
E	ns.nasa.gov	NASA	Mountain View, CA
F	ns.isc.org	ISC	Palo Alto, CA
G	ns.nic.ddn.mil	U.S. DoD NIC	Vienna, VA
H	aos.arl.army.mil	U.S. Army Research Lab	Aberdeen, MD
I	nic.nordu.net	Autonomica	Stockholm
J		VeriSign	Dulles, VA
K		RIPE	London
L		ICANN	Los Angeles
M		WIDE Project	Tokyo

Sistema de nomes de domínios ()

1. Estrutura de nomes
2. Nomes no domínio Internet
3. Nomes de domínios versus endereços
4. Resolução de nomes de domínios
5. Translação eficiente
6. Caching: chave para a eficiência
7. Formato das mensagens do DNS
8. Formato dos nomes comprimidos

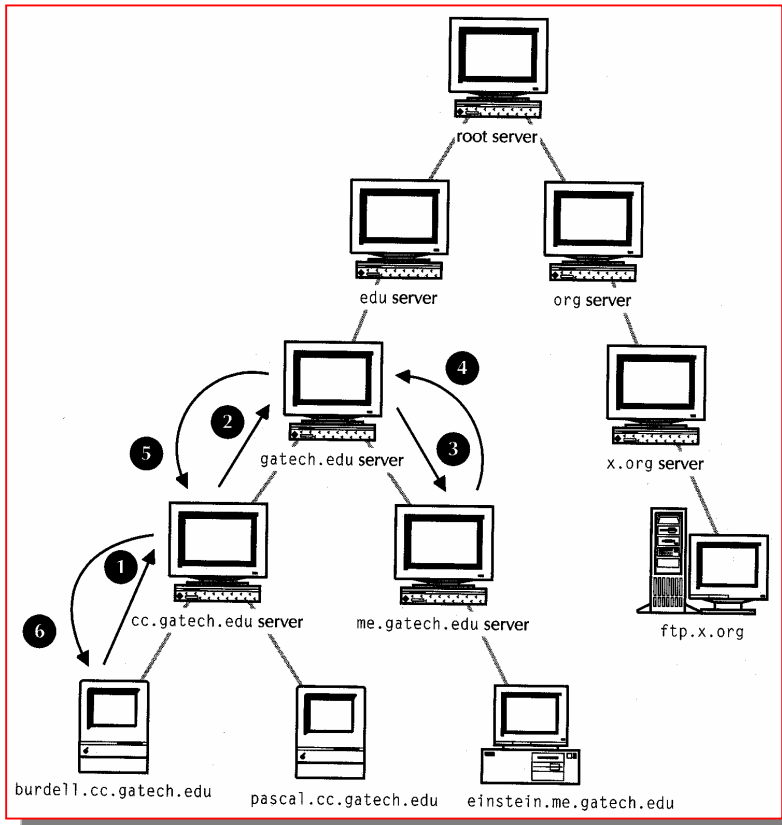
- 53/tcp [DNS](#) Domain Name Server e 53/udp

Assimilação de Conceitos

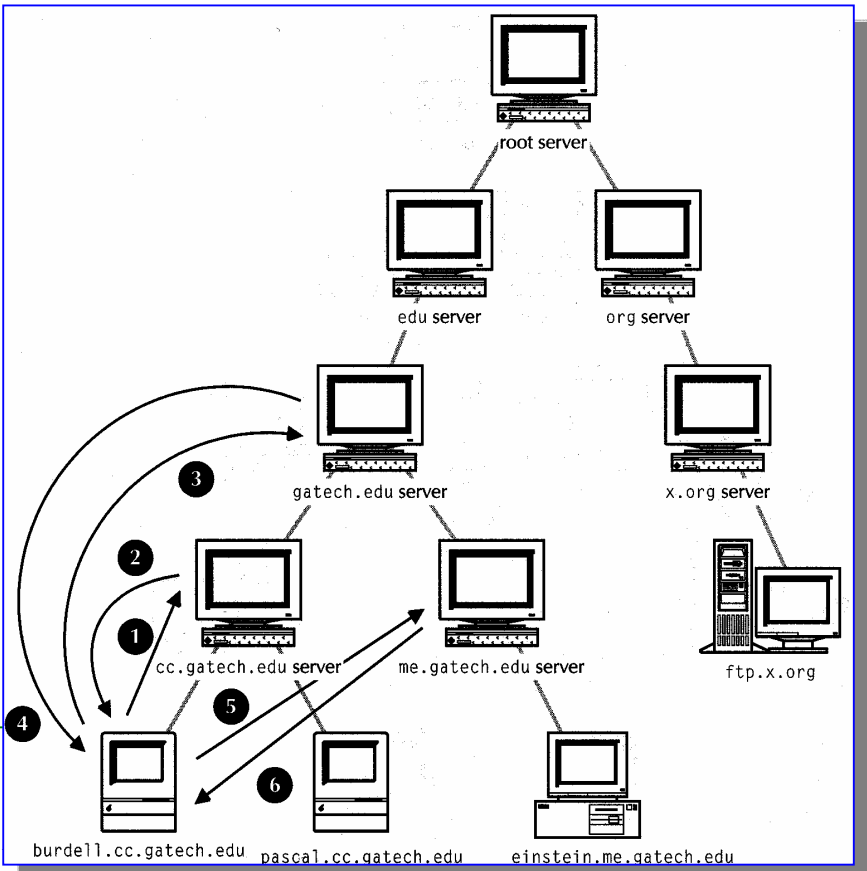
- DNS
- ISP
- Domain Name Space
- http://www.juliobattisti.com.br/artigos/windows/tcpip_p8.asp
-

Para Aprofundar

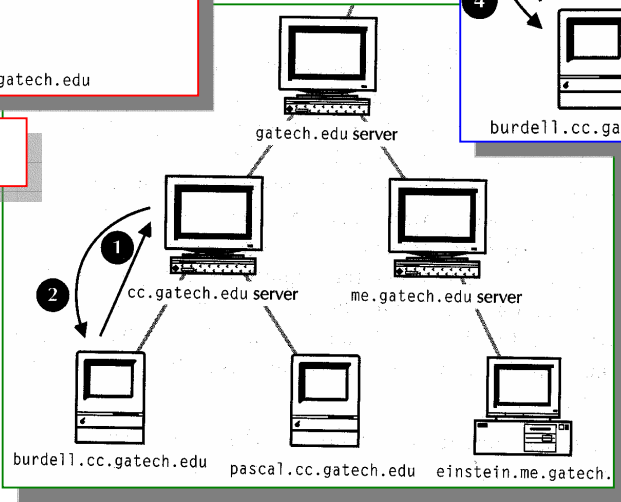
- RFC 1034
- RFC 1035



Two-Level Domain Name Query



Non-Recursive Domain Name



Single-Level Domain Name Query