

UNIVERSIDADE DO ESTADO DA BAHIA

DOMAIN NAME SYSTEM

SALVADOR 18 de junho de 2001

UNEB - UNIVERSIDADE DO ESTADO DA BAHIA
DEPARTAMENTO DE CIÊNCIA EXATAS E DA TERRA
CURSO: BACHARELADO EM ANÁLISE DE SISTEMAS
DISCIPLINA: REDES DE COMPUTADORES
PROFESSOR: MARCOS CÂMARA
ALUNO: FELIPE TITONEL ABREU

Esse trabalho foi apresentado ao professor Marcos Câmara, professor da disciplina Redes de computadores da Universidade do Estado da Bahia, como um trabalho voluntário, pelo aluno Felipe Titonel Abreu do curso de Análise de Sistemas, da mesma universidade.

INTRODUÇÃO

Você já parou para pensar como o seu computador é bem relacionado? No seu Web browser, basta digitar o nome de qualquer computador existente na Internet, que instantaneamente a conexão é efetuada. Seu computador conhece todos eles. Mas como isto é possível? Como um simples 486 com 16MB pode reconhecer e conversar com um computador na Internet, com milhões de computadores conectados na rede mundial. O segredo está no DNS.

Raramente os programas fazem referência a computadores, caixas de correio e outros recursos utilizando seus endereços binários de rede. Em vez de números binários eles utilizam seus nomes, que são strings ASCII, como em `fulano@e-mail.com.br`.

Na ARPANET (precursora da Internet), existiam poucos computadores. Além de existirem poucos computadores, as pessoas que utilizavam esses computadores também se conheciam. Existia uma lista, chamada *hosts.txt*, que continha os nomes de todos os computadores existentes. Esta lista na verdade não continha apenas nomes. Ela continha linhas relacionando nomes com números. Isto porque os computadores não se comunicam através dos nomes que possuem e sim por meio de números que lhes são atribuídos. Os chamados números IP (internet protocol).

Mais é muito mais fácil memorizar nomes do que números. O que é mais fácil lembrar, que o nome do servidor Web da UNEB é `www.uneb.br` ou que seu número IP é 200.128.3.38 (IP verdadeiro, pode verificar)?

Como os computadores só se conhecem pelo número, criou-se um mecanismo que permitiu a tradução do nome, usado pelos seres humanos que operam os computadores, para o número que os computadores usam em sua comunicação. E começamos com a lista.

A lista era mantida por uma entidade central, que cuidava da distribuição de números aos computadores que se ligavam à ARPANET. Sempre que um novo computador aparecia, a nova lista atualizada era distribuída a todos os administradores dos computadores ligados à ARPANET. Desta forma, cada computador conseguia se comunicar com todos os demais. Bastava olhar em sua lista. Para uma rede de algumas centenas de grandes computadores de tempo compartilhado, essa estratégia funcionava razoavelmente bem.

No entanto, quando milhares de computadores começaram a ser conectados à rede, a antiga estratégia deixou de funcionar. Por um lado, o arquivo começou a ficar grande demais e por outro lado os conflitos de nomes começaram a ficar muito comuns. Agora imagine se houvesse alguma falha com o computador que possuísse a lista. Muitos computadores deixariam de se falar.

Para resolver esse problema, foi desenvolvido um esquema de atribuição de nomes hierárquico, baseado em domínios, abolindo a centralização de informação. O Domain Name System. O que aconteceu foi que a autoridade sobre a informação foi diluída. Desta forma, não existe mais um dono da verdade, a informação está distribuída por milhares de computadores, que conhecem muito bem apenas alguns computadores.

Os projetistas do DNS na verdade nada mais fizeram do que imitar a vida real. Imagine que você esteja em uma cidade grande e deseja chegar até um determinado bairro. Você pára alguém na rua e pergunta: “Como faço para chegar até o bairro X?”. O seu

interlocutor não sabe, mas te diz para ir até determinado lugar e perguntar novamente. E lá vai você perguntando, até que chega em alguém que sabe lhe dizer onde se encontra o local que está procurando.

A tradução de nomes em números na Internet funciona exatamente da mesma forma. Você configura o seu computador com o nome do servidor de nomes local. E é ele quem vai fazendo as perguntas para você, até obter uma resposta. A resposta pode ser o número IP do computador com o qual você quer se comunicar ou uma negativa, dizendo que o computador procurado não existe.

Tomemos o exemplo da UNEB. Nós temos aqui um computador que tem uma lista de todos os computadores conectados à Internet dentro da Universidade. Qualquer computador na Internet que queira achar algum computador dentro da UNEB tem que perguntar a este computador. Desde que o computador procurado exista e as configurações permitam, ele fornece a informação solicitada.

Agora, quando é usado o DNS? Sempre que você usar um programa que usa o nome de um computador o DNS entra em ação. Você está mandando uma mensagem eletrônica para `mcamara@email.com.br`. O DNS tem que descobrir para você qual o número IP do computador que recebe mensagens destinadas ao domínio `email.com.br`. Você está acessando o servidor Web da Disney para programar suas férias. Lá vai o DNS novamente buscar a tradução do nome `www.disney.com` para um número IP. Chat, FTP, e-mail outras coisas que você se habituou a usar na Internet, todos fazem uso do DNS.

O DNS está definido nas RFCs 1034 e 1035.

FUNCIONAMENTO DO DNS

Para resumir, o DNS é usado para mapear um nome em um endereço IP. Um programa aplicativo chama um procedimento de biblioteca denominado *resolvedor* (resolver) e passa o nome procurado como parâmetro. O resolvedor envia um pacote UDP para um servidor DNS local, que procura o nome e retorna o endereço IP para o resolvedor. Em seguida, o resolvedor retorna o endereço IP para o aplicativo que fez a chamada, que agora possuindo o endereço IP do outro computador pode estabelecer uma conexão TCP como o destino, ou enviar pacotes UDP até ele.

ESPAÇO DE NOMES

O nomes de máquinas nos primórdios da Internet formavam um *flat namespace* onde cada nome consistia de uma sequência de caracteres sem qualquer estrutura. Nesse primeira organização de nomes de máquinas, um local central, o Network Information Center (NIC), administrava o espaço de nomes e determinava se um nome era apropriado (proibindo nomes obscenos ou novos nomes que geravam conflito com o nomes já existentes). Mais tarde, a NIC foi substituída pela INTERNet Network Information Center (INTER-NIC).

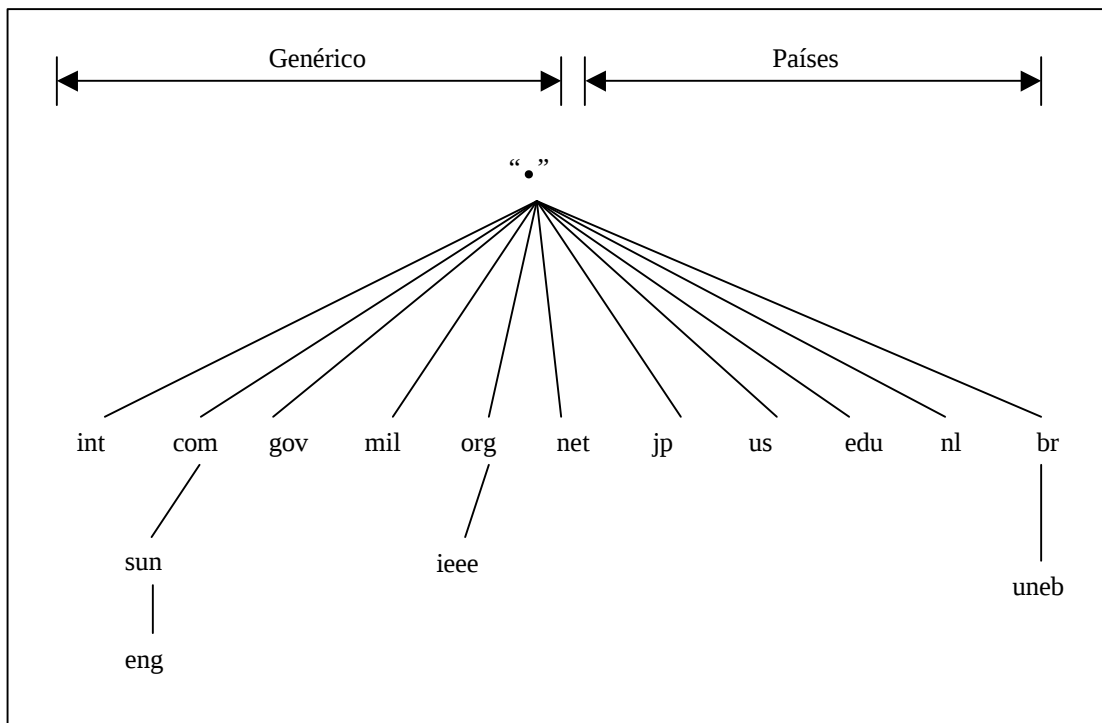
A grande vantagem de um “espaço plano de nomes” era a conveniência dos nomes, o tamanho reduzido dos mesmos e a facilidade de mapeamento de nomes para endereços. A principal desvantagem era que esse espaço plano não podia suportar o grande número de máquinas por razões técnicas e administrativas. Primeiro, como os nomes eram formados pelo mesmo conjunto de caracteres o potencial de conflito de nomes aumentava com o aumento dos computadores (sites). Segundo, com a autoridade de adicionar novos nomes centralizado em um único lugar o fluxo de trabalho administrativo crescia também com o número de sites. Terceiro, como os nomes mudam freqüentemente, manter um cópia atualizada, do que poderia ser um imenso arquivo, era muito dispendioso. E finalmente, se o banco de dados de nomes reside em um lugar central o tráfego na rede aumentaria enormemente, já que para se acessar um site deveria-se passar primeiro por este lugar para se obter o IP de uma máquina na Internet e o risco de algum problema impedir a comunicação com esse super administrador causaria enormes dificuldades para os computadores se falarem.

Como um sistema de nomes poderia acomodar um enorme conjunto de nomes e que não parava de crescer sem utilizar um administrador central? A resposta estava em descentralizar o mecanismo de nomes delegando autoridade administrativa do espaço de nomes e distribuindo o mapeamento de nomes para endereços IP entre os vários computadores (sites). Com isso se diminui o tráfego na rede e facilitou-se a trabalho administrativo, já que cada nova autoridade é responsável pelo seu espaço. Porém, sempre há um porém, o mapeamento de nomes para endereços se tornou complexo.

Surgiu então o espaço hierárquico de nomes (Hierarchical namespace). Vamos começar com uma ilustração. Em um sistema postal, o gerenciamento de nomes é feito através do uso de letras que especificam (implícita ou explicitamente), o país, o estado, a cidade e a rua dos destinatário de uma correspondência. Usando esse endereçamento hierárquico, não a confusão entre Marcos de Silva que mora na Rua João Batista, São Paulo e Marcos da Silva, que mora na Rua João Batista, Salvador. A estrutura hierárquica de nomes do DNS funciona de forma semelhante.

Conceitualmente, a Internet é dividida em muitas centenas de domínios de primeiro nível, onde cada domínio cobre muitos computadores (sites). Os domínios são particionados em subdomínios, que também são particionados, e assim por diante. Essa estrutura de nomes é representada por uma árvore, semelhante a estrutura de diretórios e arquivos no Linux ou no Windows. As folhas dessa árvore de domínios representam domínios que não possuem subdomínios mas que contém computadores. Um domínio-folha contém um único computador ou pode representar uma empresa que possui centenas de computadores.

Portanto não se pode distinguir nomes de subdomínios de nomes de objetos individuais ou o tipo dos objetos usando somente a syntax de nomes de domínios.



Com isso, todo computador ligado à Internet ganha um nome e um sobrenome. O nome geralmente é escolhido pela pessoa que usa o computador. Em muitos locais escolhe-se um tema preferido e os computadores são batizados segundo este tema. Por exemplo, os fãs das aventuras do Asterix, podem resolver escolher os nomes dos personagens das histórias em quadrinhos para seus computadores. Temos o obelix, o próprio asterix, abracurcix, ideiafix, chatotorix e mais alguns. Agora fica a questão do sobrenome. No nome *obelix.uneb.br*, o nome do computador é *obelix* e o sobrenome é *uneb.Br* (domínio). O sobrenome já é um pouco mais complicado de definir e envolve o contato com algumas entidades que regulamentam e controlam a concessão de domínios. Em termos da Internet global, o sobrenome precisa ser registrado. Para que o registro seja concedido não pode haver outra empresa ou pessoa que o tenha registrado anteriormente. O sobrenome, no jargão da Internet, é o que chamamos de domínio. No Brasil, o órgão responsável pelo registro de domínios é a FAPESP (Fundação de Amparo a Pesquisa de São Paulo). Todo o processo, da consulta ao registro do domínio pode ser feito diretamente através do servidor Web da FAPESP, no endereço <http://www.registro.fapesp.br>.

Mas para entender melhor tudo o que foi dito, vamos analisar o nome de um computador. Vejamos o nome *obelix.uneb.br*. Dá para ver que o nome é composto de quatro componentes:

obelix + uneb + br + "."

Isto mesmo, quatro componentes. Embora não pareça, o ".", que a maioria de nós nem se lembra de digitar quando escreve o nome de um computador (e muitos de nós nem mesmo

sabemos que este ponto existe) representa o domínio de mais alto nível na hierarquia de nomes de computadores. No nome de computadores, a hierarquia (ou domínio) de mais alto nível fica à direita, ao passo que a mais baixa fica à esquerda (isto tem uma razão, que será explicada). Isto é fácil de se visualizar. O “.” contém os servidores de nomes de mais alto nível, que possuem apontadores para os computadores de nível imediatamente inferior, os domínios geográficos (países), aos quais pertencem o Brasil (br), Japão (jp), Canadá (ca), Portugal (pt) e todos os demais países. Neste mesmo nível situam-se os domínios com (entidades comerciais, genéricos), net (comunicações), org (organizações), edu (educação), gov (governo) e mil (militares). Os domínios de segundo nível apontam para os domínios de terceiro nível. A UNEB, por exemplo, está dentro do Brasil. Dentro do servidor de nomes do domínio br, mantidos pela FAPESP, existe uma referência ao servidor de nomes da UNEB, que conhece todos os computadores do domínio *uneb.br*.

Agora vamos ver a situação em que alguém deseje encontrar o computador *acme.com.br*. Ele primeiro faz a pergunta ao seu servidor de nomes local. Este servidor de nomes não conhece o computador *acme.com.br*. O que faz então? Pergunta a outro, neste caso, aos servidores do domínio “.”. Estes servidores de nomes também não conhecem o computador *acme.com.br*, mas analisando o nome descobrem que este computador está dentro do Brasil (br) e instruem o servidor de nomes local a perguntar aos servidores do domínio br. E lá vai o nosso servidor de nomes perguntar aos servidores do domínio br onde está *acme.com.br*. Eles (servidores do domínio br) também não sabem, mas sabem que tal computador, se existir, está dentro da empresa chamada Acme. E novamente instruem o servidor de nomes local a perguntar aos servidores de nomes da Acme. Desta vez a resposta é definitiva. O computador *acme.com.br* existe e o número IP correspondente é 200.200.20.1. Acabou a busca. Não foi tão difícil assim. Para localizar o computador *acme.com.br*, dentre os milhões existentes na Internet, foram necessárias apenas quatro perguntas. É preciso entender o seguinte: Dado um nome para ser mapeado, o cliente deve especificar o tipo do objeto desejado e o servidor então retorna o objeto e o tipo do mesmo.

O nomes de domínios não fazem distinção entre maiúsculo e minúsculo, assim br e BR são mesmo domínio. Os nomes dos componentes (labels) podem ter até 63 caracteres e os nomes dos caminhos podem ter no máximo 255 caracteres.

Em princípio, os nomes de domínios podem ser colocados na árvore de duas formas distintas. Por exemplo, OOLAB poderia ser igualmente registrado sob o domínio de país, *oolab.br* ou listado sobre um domínio genérico como *oolab.com*, na verdade pode-se ter os dois registros, mas isso poderia gerar confusão.

Cada domínio controla como serão alocados todos os domínios que estão abaixo dele. Por exemplo, o Japão tem os domínios *ac.jp* e *co.jp* que são iguais a *edu* e *com*. Ou o Brasil que possui o domínio *com.Br*. A Holanda não faz distinção e coloca todas as organizações listadas diretamente sob *nl*.

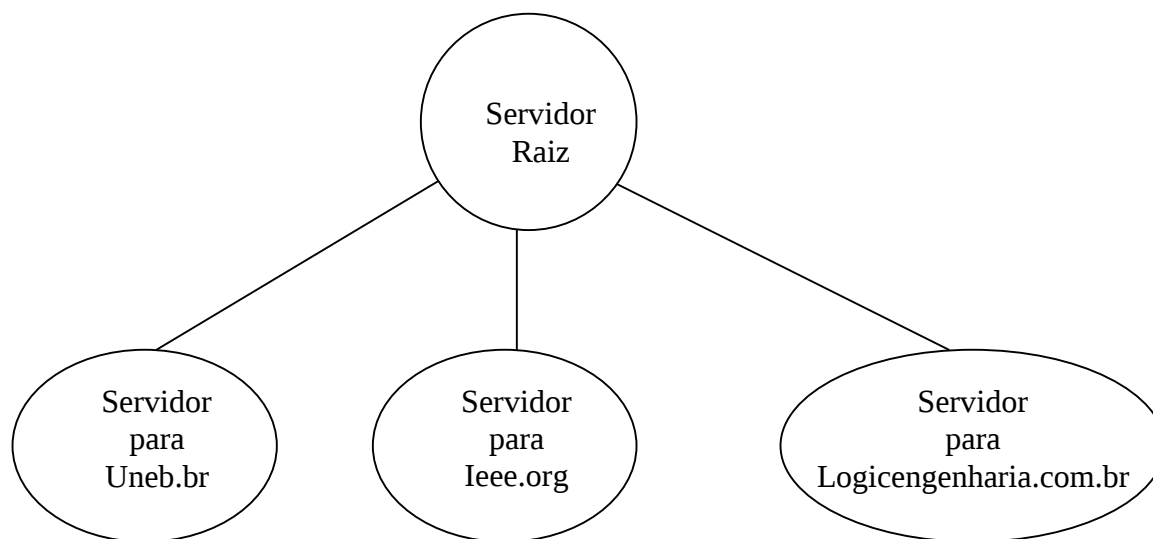
Para que um novo domínio seja criado, é necessário a permissão do domínio no qual ele será incluído. Por exemplo, se o OOLAB quiser ser conhecido como *oolab.uneb.Br*, ele precisará ter a permissão de quem gerencia *uneb.br*. O mesmo aconteceria se uma nova universidade fosse criada e quisesse se registrar sob o domínio *br*, ela deverá solicitar ao gerente a permissão para se registrar sob esse domínio. Dessa forma, os conflitos de nomes são evitados e cada domínio pode controlar seus subdomínios. Assim quando um subdomínio é inserido ele a partir de então poderá ter seus subdomínios e controlar quem poderá estar abaixo dele.

Agora vamos abordar algo muito importante. A atribuição de nomes leva em consideração as fronteiras organizacionais, e não as redes físicas. Então mesmo que os departamentos de Ciências Exatas e da Terra e o Departamento de Ciências da Vida estejam no mesmo prédio e utilizando a mesma rede os dois departamentos podem estar em domínios separados. Da mesma forma que o mesmo departamento esteja separado em dois prédios distintos todos o computadores desse departamento estarão sob o mesmo domínio.

SERVIDORES DE NOMES

O mecanismo de domínios para mapeamento de nomes para endereços consiste de sistemas independentes mas cooperativos de servidores de nomes. Um servidor de nome é um programa que faz a tradução de nomes para endereços. Geralmente, os programas servidores são executados em processadores dedicados , e então a máquina é chamada de servidor de nome. (name server).

Como o meio mais fácil para o entendimento de como os servidores trabalham foi apresentado uma estrutura de árvore conceitual, correspondendo a hierarquia de domínios. Se os servidores no sistema de domínios trabalhassem exatamente como no modelo conceitual apresentado, a relação de conectividade e autoridade poderia ser bem simples. Porém, mais um porém, na prática, a relação entre a hierarquia de nomes e a árvore de servidores não é tão simples quanto apresentado no modelo conceitual. A árvore de servidores possui poucos níveis. Em articular, organizações guardam informações de todos os seus subdomínios em um único servidor.



Os servidores DNS podem ser divididos em três tipos principais: servidores que apenas armazenam as informações recebidas de outros servidores na Internet, também conhecidos como *caching only*, servidores mestres primários e servidores mestres secundários. Todo servidor de nomes interage com outros servidores de nomes na Internet

para obter as informações solicitadas por seus clientes. Esta informação, uma vez obtida, passa a residir no cache do servidor de nomes. Desta forma, da próxima vez que a mesma informação for solicitada, não mais haverá a necessidade de se consultar outros servidores de nomes. A informação será fornecida a quem a solicitar diretamente a partir do cache local como não oficial. Servidores mestres primários possuem autoridade sobre um ou mais domínios. Além das informações mantidas em seu cache, obtidas de outros servidores de nomes, o servidor primário é a fonte de informação oficial a respeito de um domínio. A informação que os servidores mestres primários disponibilizam é lida a partir de arquivos locais, configurados pelo administrador do domínio.

Tomemos por exemplo o servidor de nomes da UNEB, *ns.uneb.br*. Este computador fornece informações oficiais a respeito de todos os computadores existentes dentro da UNEB. Servidores de nomes de todo o mundo, ao desejarem informações sobre algum computador dentro da UNEB, precisam enviar uma solicitação ao servidor de nomes *ns.uneb.br*. Além destas informações oficiais, o servidor de nomes da UNEB, possui também informações não oficiais, armazenadas em seu cache. Qualquer servidor primário, além de fornecer as informações oficiais a respeito do domínio pelo qual são responsáveis, possui em seu cache informações não oficiais, obtidas de outros servidores de nomes. Estas informações são consideradas não oficiais visto terem sido obtidas de outros servidores de nomes e, como tal, estão sujeitas a mudanças. As informações mantidas no cache possuem um prazo de validade. Todo servidor de nomes oficial de um domínio, ao disponibilizar esta informação para outros computadores na Internet, a fornece juntamente com o prazo de validade ou TTL (*Time to Live*). O TTL indica por quanto tempo a informação é válida. Após este tempo a informação deve ser descartada e novamente solicitada junto ao servidor de nomes oficial do domínio. A definição do valor que o TTL deve assumir é decisão do administrador do domínio. O administrador deve considerar o nível de volatilidade das informações sobre seus computadores e especificar um valor compatível para o campo TTL. Os servidores mestres secundários, como o nome diz, fornecem informações oficiais a respeito de um ou mais domínios. Esta informação, todavia, não é lida a partir de arquivos locais mas transferida via rede do servidor mestre primário. O processo *named*, ao entrar no ar, determina quais os domínios para os quais deve atuar como servidor mestre secundário, e então entra em contato com os servidores mestres primários e solicita a transferência das zonas correspondentes.

Não existe uma necessidade de que um servidor de nomes seja estritamente primário ou secundário. É perfeitamente possível e bastante comum que um servidor de nomes seja primário para alguns domínios e secundário para outros.

FORMATO DA MENSAGEM DE SERVIDORES DE DOMÍNIO

Olhando os detalhes de mensagens trocadas entre clientes e servidores de nomes pode ajudar a entender como o sistema funciona do ponto de vista de uma aplicação. Assumindo que um usuário chame uma aplicação (um browser) e informa o nome da máquina com a qual ele quer se comunicar o programa aplicativo chama um procedimento de biblioteca denominado *resolvedor* (resolver) e passa o nome procurado como parâmetro. O resolvedor envia um pacote UDP para um servidor DNS local, que procura o nome e retorna o endereço IP para o resolvedor. Em seguida, o resolvedor retorna o endereço IP para o aplicativo que fez a chamada, que agora possuindo o endereço IP do outro computador pode

estabelecer uma conexão TCP como o destino, ou enviar pacotes UDP até ele. Se o servidor não pode responder a todas as solicitações ele retorna também informações sobre outros servidores que podem atender as solicitações do cliente.

Cada mensagem possui em cabeçalho fixo que contém um campo único de identificação (*IDENTIFICATION*) o cliente usa para comparar as respostas com as solicitações e um campo de parâmetros (*PARAMETER*) que especifica a operação a operação requisitada e o código de respostas.

O campo chamado *NUMBER OF* informa o número de ocorrências do item específico.

O campo *QUESTION SECTION* contém as solicitações. O cliente envia somente as solicitações, o servidor retorna as solicitações e as respectivas respostas. Cada solicitação é composta dos campos: *QUERY DOMAIN NAME* seguido pelo *QUERY TYPE* e *QUERY CLASS*.

0	16	31
IDENTIFICADOR		PARÂMETRO
NÚMERO DE REQUISIÇÕES		NÚMERO DE RESPOSTAS
SEÇÃO DE REQUISIÇÕES		
...		
SEÇÃO DE RESPOSTAS		
...		
SEÇÃO DE AUTORIDADE		
...		
SEÇÃO DE INFORMAÇÕES ADICIONAIS		
...		

0	16	31
SEÇÃO DE REQUISIÇÕES		
...		
TIPO DA REQUISIÇÃO		CLASSE DA REQUISIÇÃO

0	16	31
PESQUISA DO NOME DO DOMÍNIO		
TIPO		CLASSE
TTL		TAMANHO
DADOS		

Em uma mensagem de um servidor de nomes, cada um dos campos: *ASWER SECTION*, *AUTHORITY SECTION* e *ADDITIONAL INFORMATION SECTION*, consistem de um conjunto de registros de recursos (resource records) que descreve o nome do domínio e o mapeamento.

Bit do Campo Parâmetro	Significado
0	Operação 0 Requisição 1 Resposta
1-4	Tipo da requisição 0 Padrão 1 Inverso 2 Complemento 1 (obsoleto) 3 Complemento 2 (obsoleto)
5	Se a resposta é oficial
6	Se a mensagem esta truncada
7	Se a recursão esta desabilitada
8	Se a recursão esta ativa
9-11	Reservado
12-15	Tipo da resposta 0 Sem erros 1 Erro de formato na solicitação 2 Falha de servidor 3 Nome não existe

REGISTROS DE RECURSOS

Esse tópico será apresentado através de uma ilustração. O sistema operacional utilizado é o Linux.

Iremos proceder agora à construção dos arquivos de configuração de um servidor de nomes de um provedor de acesso fictício. A empresa chama-se *NetRoad* e seu domínio na Internet denomina-se *netroad.com.br*. Este provedor de acesso, em começo de atividades, possui apenas um cliente, uma empresa chamada *NetMasters*. Adicionalmente, estão prestando serviço de servidor mestre secundário para a empresa *NetWizards*, detentora do domínio *netwizards.com.br*. Este provedor possui os seguintes equipamentos:

- roteador com 16 portas assíncronas
- servidor de nomes
- servidor Web
- servidor FTP
- servidor de Usenet News
- seis micro computadores utilizados pelos funcionários da empresa

O coração de qualquer servidor DNS é o arquivo */etc/named.boot*. Neste arquivo são descritos os domínios para os quais o servidor é primário ou secundário, o diretório onde os arquivos contendo as informações sobre as zonas se encontram, quais servidores estão autorizados a transferir as zonas, entre outras informações. Analisemos então o arquivo */etc/named.boot* do servidor de nomes do provedor *NetRoad*:

Directory		/usr/local/named
Primary	netroad.com.br	p/netroad.db
primary	netmasters.com.br	p/netmasters.db
primary	20.200.200.IN-ADDR.ARPA	p/200.200.20.0.db
secondary	netwizards.com.br	s/netwizards.db
secondary	21.200.200.IN-ADDR.ARPA	s/200.200.21.0.db
cache	.	named.root
primary	0.0.127.IN-ADDR.ARPA	127.0.0.db

A primeira linha, contendo a diretiva *directory*, indica o diretório base onde se encontram todos os arquivos de configuração do servidor de nomes. O arquivo *named.root* por exemplo, referenciado pela diretiva *cache*, encontra-se na realidade no diretório */usr/local/named/named.root*. A diretiva seguinte, na segunda linha, indica que o servidor de nomes é responsável pelo domínio *netroad.com.br*. O arquivo localizado em */usr/local/named/p/netroad.db*, contém as informações sobre todos os computadores do provedor conectados à Internet. O nome *netroad.db* é totalmente opcional, ficando a critério do administrador do DNS. A localização no subdiretório “.”, é feita para sinalizar mais claramente ao administrador do domínio que se trata de um domínio para o qual se é primário. O sufixo *db* é também uma convenção comum na Internet e significa *data base*.

Vamos agora descrever a zona analisando o arquivo *netroad.db*. Isso mesmo, uma zona é um arquivo que contém todos os registros de recursos para aquele domínio específico.

```
netroad.com.br. IN      SOA ns.netroad.com.br. dnsmaster.netroad.com.br. (
    1998122103 ;      Serial
    10800 ;          Refresh
    1800 ;           Retry
    3600000 ;        Expire
    259200 ) ;        Minimum
;
; Definição dos Servidores Primário e Secundário do Domínio NetRoad.com.BR
;
netroad.com.br.      10800 IN NS ns.netroad.com.br.
ns.netroad.com.br.   10800 IN A 200.200.20.1
netroad.com.br.      10800 IN NS ns.netwizards.com.br.
;
; Definição dos Servidores de Email Primário e Secundário
;
netroad.com.br. 10800 IN MX 10 mail.netroad.com.br.
netroad.com.br. 10800 IN MX 20 mail.netwizards.com.br.
;
; Definição dos servidores Web, FTP, News
;
www.netroad.com.br.  10800 IN CNAME ns.netroad.com.br.
ftp.netroad.com.br.  10800 IN CNAME ns.netroad.com.br.
news.netroad.com.br. 10800 IN A 200.200.20.2
;

; Definição dos microcomputadores de trabalho do provedor
;
pc01.netroad.com.br. 10800 IN A 200.200.20.3
pc02.netroad.com.br. 10800 IN A 200.200.20.4
pc03.netroad.com.br. 10800 IN A 200.200.20.5
pc04.netroad.com.br. 10800 IN A 200.200.20.6
pc05.netroad.com.br. 10800 IN A 200.200.20.7
pc06.netroad.com.br. 10800 IN A 200.200.20.8
;
; Definição do Roteador e de suas oito portas assíncronas
;
async01.netroad.com.br. 10800 IN A 200.200.20.65
async02.netroad.com.br. 10800 IN A 200.200.20.66
async03.netroad.com.br. 10800 IN A 200.200.20.67
async04.netroad.com.br. 10800 IN A 200.200.20.68
async05.netroad.com.br. 10800 IN A 200.200.20.69
```

```
async06.netroad.com.br. 10800 IN A 200.200.20.70
async07.netroad.com.br. 10800 IN A 200.200.20.71
async08.netroad.com.br. 10800 IN A 200.200.20.72
```

Cada uma das linhas do arquivo *netroad.db* é o que se chama de *Resource Record* (RR), ou traduzindo, Registro de Recurso. O arquivo *netroad.db* é o que se denomina de zona. Esta zona contém os registros descritivos do domínio *netroad.com.br*.

No arquivo *netroad.db*, todos os registros são do tipo INternet (IN). Os registros INternet, por sua vez, são de vários tipos. SOA (*Start Of Autho-rity*), NS (*Name Server*), A (*Address*), MX (*Mail eXchanger*) e CNAME (*Canonical Name*).

REGISTRO SOA

Comecemos analisando o registro SOA:

```
netroad.com.br. IN SOA ns.netroad.com.br. dnsmaster.netroad.com.br. (
    1999122103 ;      Serial
    10800 ;          Refresh
    1800 ;           Retry
    3600000 ;        Expire
    86400) ;         Minimum
```

Este registro SOA está disposto em várias linhas para facilidade de leitura, mas na verdade é apenas um registro. Observe a abertura de parênteses no final da primeira linha e o fechamento na última linha. Os parênteses permitem que o registro se estenda por várias linhas. O primeiro valor, *netroad.com.br.*, indica o domínio ao qual as informações do registro SOA se aplicam. Em seguida temos o valor IN, indicando que este é um registro do tipo INternet. Temos então a indicação do tipo de registro Internet, SOA, seguida pelo nome do computador onde esta zona reside, o computador *ns.netroad.com.br*, seguida pelo endereço eletrônico do administrador desta zona, *dnsmaster@netroad.com.br*. Note bem que no endereço eletrônico, o caracter “@” foi substituído pelo caracter “.”. Isto se dá devido ao fato de que o caracter “@” tem um significado especial, que será abordado mais à frente. Todos os valores da segunda linha em diante, são utilizados por servidores secundários do domínio *netroad.com.br*. É norma seguida pela maior parte das autoridades que cuidam do registro de domínios na Internet que cada domínio possua no mínimo dois servidores de nomes atendendo pelo domínio registrado. No Brasil o registro de um domínio somente é aceito se já existirem dois servidores de nomes configurados e fornecendo informações corretas sobre este domínio. O servidor primário é aquele onde os arquivos de configuração são criados e mantidos pelo administrador DNS. O servidor secundário realiza uma cópia destas dados via rede e os grava em seu disco rígido. Os campos que passaremos a discutir agora servem para estabelecer este sincronismo entre servidores primários e secundários.

O primeiro deles, o valor

1999122103 ; Serial

indica a versão do mapa. Todos servidores secundários, como veremos em breve, são configurados para entrar em contato com o servidor primário regularmente para verificar se houveram mudanças nos mapas descritivos das zonas para qual atende. Os arquivos não são

verificados integralmente, verifica-se apenas o número da versão do mapa. Caso a versão do mapa existente no servidor primário seja maior do que a versão que o servidor secundário possui, é então realizada uma transferência de zona, pois isto indica que os dados foram alterados. O servidor secundário solicita então ao servidor primário a transferência dos dados desta zona. A forma como este número é escrito não segue nenhuma norma fixa. A convenção mostrada aqui, por sinal bastante comum, é utilizada para conveniência do administrador. Os quatro primeiros dígitos, 1999, indicam o ano, os quatro dígitos seguintes indicam o mês, dezembro, e o dia, 21, em que os dados desta zona foram alterados. Os próximos dois dígitos, 03, indicam que esta foi a terceira modificação realizada no dia. Resumindo, este mapa foi modificado três vezes no dia 21 de dezembro de 1999. Esta certamente é uma informação bastante útil para o administrador DNS.

O próximo valor

10800 ; Refresh

indica de quanto em quanto tempo o servidor secundário deve contactar o servidor primário para verificar se houveram mudança nos dados do domínio para o qual é secundário. Este valor é expresso em segundos, no nosso caso 10.800 ou 3 horas. A cada três horas o servidor secundário do domínio `netroad.com.br` entrará em contato com o servidor primário e verificará se o número da versão do mapa que possui está ou não atualizada. Caso não esteja, é solicitado ao servidor primário a transferência da zona.

Em seguida temos o valor

1800 ; Retry

que indica quanto tempo o servidor secundário deve aguardar para tentar novamente uma conexão com o servidor primário quando houver uma falha de comunicação. Como configurado, o servidor secundário deve contactar o servidor primário a cada três horas. Caso uma destas conexões falhe, uma nova tentativa deve ser feita dentro de 1.800 segundos, ou 30 minutos. As tentativas se repetem até que seja estabelecida uma conexão. Depois de 3.600.000 segundos (3600000 ; *Expire*), ou 41 dias, o servidor secundário desiste então de contactar o servidor primário, e expira todos os dados relativos ao domínio cujo servidor primário está fora do ar. Todos os arquivos relativos à zona expirada são apagadas e deste momento em diante o servidor secundário não mais responde perguntas sobre este domínio.

O próximo valor

86400) ; Minimum

indica o valor mínimo, ou TTL (*Time to Live*) aplicado aos registros (RR) deste arquivo. No nosso exemplo este valor é de 86.400 segundos ou um dia. Todas as informações fornecidas pelos servidores (primários ou secundários) do domínio `netroad.com.br` a outros servidores será mantida no cache dos servidores que solicitaram esta informação por apenas

um dia. Após 24 horas a informação é expirada e removida do cache. Solicitações posteriores devem novamente ser obtidas junto aos servidores do domínio *netroad.com.br*. Os valores utilizados são utilizados apenas a título de ilustração. O certo é que cada administrador determine os valores mais adequados para sua situação específica. Todos os valores devem ser analisados e configurados em conformidade com o que for mais adequado. O valor do TTL, em nosso exemplo de 86.400 segundos, certamente não é o mais adequado em ambientes onde as informações forem mais estáveis. Talvez um valor mais adequado seja uma semana ou até mais. Novamente, em um ambiente onde os dados são estáveis, o período de atualização (refresh) pode ser maior que três horas. O valor de um dia ou até mesmo mais tempo pode ser adequado. Não existe uma receita fixa, tudo depende do bom senso do administrador DNS. Não utilize o *copy-paste* como receita de bom senso.

REGISTRO NS (NAME SERVER)

Em seguida aparece o registro do tipo NS (NameServer). O registro NS contém, à direita, o nome do domínio, em seguida a indicação de que se trata de um registro do tipo INternet. O valor 10800 indica o valor em segundos do TTL deste registro. Em outras palavras, estes registros possuem prazo de validade de três horas (muito pouco, não?). Um TTL deste valor nunca deveria ser usado indistintamente em todos os registros. Um valor de três horas para um registro somente deve ser usado em casos especiais. Especialmente em registros do tipo NS este valor deve ser mais alto. Afinal de contas, os servidores de nomes para um domínio devem ser estáveis e sujeitos a pouquíssimas modificações. Consequentemente, um TTL de valor 2592000 (30 dias), não é exagerado.

```
;
; Definição dos Servidores Primário e Secundário do Domínio NetRoad.com.BR
;
netroad.com.br.      10800 IN NS ns.netroad.com.br.
ns.netroad.com.br.   10800 IN A 200.200.20.1
netroad.com.br.      10800 IN NS ns.netwizards.com.br.
```

Analisemos então o primeiro registro. À esquerda encontra-se o nome do registro, *netroad.com.br*. No lado direito encontra-se o nome do servidor que atende a este domínio. Assim temos que todas perguntas relativas ao domínio *netroad.com.br* são respondidas pelo computador cujo nome é *ns.netroad.com.br*. Mas temos então um problema. Se todas as perguntas sobre computadores pertencentes ao domínio *netroad.com.br* devem ser respondidas pelo computador *ns.netroad.com.br*, como então achar o computador *ns.netroad.com.br*, que faz parte do mesmo domínio pelo qual responde? Esta é uma típica situação do que veio primeiro, o ovo ou a galinha. Este problema é resolvido acrescentando-se em seguida um registro do tipo A (Address) que informa o número IP do servidor de nomes do domínio *netroad.com.br* (em nosso exemplo o endereço IP é 200.200.20.1). Este tipo de registro é conhecido como registro cola (*glue record*). Este registro é necessário sempre que o servidor de nomes encontra-se dentro do domínio sobre o qual é autoridade. O domínio *netroad.com.br* possui dois servidores de nomes: *ns.netroad.com.br* e *ns.netwizards.com.br*. Observe que o segundo servidor de nomes não possui um registro “cola” associado. Isto porque o computador *ns.netwizards.com.br* não pertence ao domínio *netroad.com.br*. A inclusão do registro “cola” neste caso é não apenas desnecessária como também desaconselhável.

Desnecessária e desaconselhável porque os dados relativos ao domínio do segundo servidor de nomes, *netwizards.com.br*, são gerenciados por outras pessoas. O número IP do servidor de nomes pode mudar. Caso a modificação não seja comunicada aos administradores do domínio *netroad.com.br* vários transtornos podem ocorrer. Informações incorretas serão passadas aos servidores de nomes que fizerem consultas relativas ao domínio *netroad.com.br*. Pior ainda, em caso de falha do servidor de nomes primário, o secundário não será encontrado e todos os computadores deste domínio ficarão virtualmente isolados. Registros “cola” devem ser utilizados apenas quando estritamente necessário. Não se ganha nada utilizando-se estes tipos de registro indiscriminadamente.

REGISTRO MX (MAIL EXCHANGER)

```
;
; Definição dos Servidores de Email Primário e Secundário
;
netroad.com.br. 10800 IN MX 10 mail.netroad.com.br.
netroad.com.br. 10800 IN MX 20 mail.netwizards.com.br.
;
```

Os registros do tipo MX(*Mail Exchanger*) provêm a interação entre o DNS e o correio eletrônico. Novamente, à direita temos o nome do domínio (*netroad.com.br*), o TTL, tipo do registro (INternet), o tipo de registro (MX), a precedência e o nome do servidor de mensagens (*mail.netroad.com.br*). Temos então que o domínio *netroad.com.br* é atendido por dois servidores: *mail.netroad.com.br* e *mail.netwizards.com.br*. A precedência é um número que indica qual servidor tem prioridade no encaminhamento das mensagens.

Quanto menor este número maior a prioridade. Mensagens enviadas para qualquer computador dentro do domínio *netroad.com.br* são preferencialmente encaminhadas para o computador *mail.netroad.com.br*. Se este servidor estiver indisponível por algum motivo, as mensagens são então encaminhadas ao servidor MX secundário, o computador *mail.netwizards.com.br*.

REGISTROS A (ADDRESS)

Este é o tipo de registro mais freqüentemente utilizado e realiza o mapeamento entre endereços IP (Addresses) e nomes. Ele simplesmente informa um IP para um nome de forma direta.

REGISTROS CNAME (CANONICAL NAME)

Estes registros servem para atribuir diversos nomes diferentes a um mesmo número IP. Em nosso exemplo os nomes *www.netroad.com.br* e *ftp.netroad.com.br* direcionam para um mesmo computador, *ns.netroad.com.br*, cujo número IP é 200.200.20.1. Um erro bastante comum é apontar, em um registro do tipo CNAME para outro registro do tipo CNAME.

Ainda em nosso exemplo, a configuração:

```
www.netroad.com.br. 10800 IN CNAME ftp.netroad.com.br.
ftp.netroad.com.br. 10800 IN CNAME ns.netroad.com.br.
```

é inválida, visto que *www.netroad.com.br* está apontando para *ftp.netroad.com.br*, que não é um nome canônico e sim um apelido (alias). Todos os registros CNAME, em nosso exemplo, devem obrigatoriamente apontar para *ns.netroad.com.br* que é o nome verdadeiro (o que é definido com um registro do tipo A).

DESCRIÇÃO DE ZONA REVERSA 200.200.21.0.DB

O nosso provedor de acesso fictício recebeu uma classe C, 200.200.21.0, com 254 endereços, para endereçar os computadores de sua rede e de seus clientes. O mapeamento reverso realiza a tradução de números IP em nomes. Este mapeamento é indicado através de registros do tipo PTR (Domain Name Pointer).

Na configuração de nosso provedor, tal informação, como indicado em */etc/named.boot*, encontra-se descrita no arquivo *200.200.21.0.db*:

```
0.20.200.200.IN-ADDR.ARPA. IN SOA ns.netroad.com.br. dnsmaster.netroad.com.br. (
    1998122103 ; Serial
    10800 ; Refresh
    1800 ; Retry
    3600000 ; Expire
    259200 ) ; Minimum
;
; Definição dos Servidores Primário e Secundário do Domínio NetRoad.com.BR
;
netroad.com.br.      10800 IN      NS      ns.netroad.com.br.
ns.netroad.com.br.   10800 IN      A       200.200.20.1
netroad.com.br.      10800 IN      NS      ns.netwizards.com.br.
;
; Definição dos microcomputadores de trabalho do provedor
;
3.20.200.200.IN-ADDR.ARPA. 10800 IN PTR pc01.netroad.com.br.
4.20.200.200.IN-ADDR.ARPA. 10800 IN PTR pc02.netroad.com.br.
5.20.200.200.IN-ADDR.ARPA. 10800 IN PTR pc03.netroad.com.br.
6.20.200.200.IN-ADDR.ARPA. 10800 IN PTR pc04.netroad.com.br.
7.20.200.200.IN-ADDR.ARPA. 10800 IN PTR pc05.netroad.com.br.
8.20.200.200.IN-ADDR.ARPA. 10800 IN PTR pc06.netroad.com.br.
;
; Definição do Roteador e de suas oito portas assíncronas
;
65.20.200.200.IN-ADDR.ARPA. 10800 IN PTR async01.netroad.com.br.
66.20.200.200.IN-ADDR.ARPA. 10800 IN PTR async02.netroad.com.br.
67.20.200.200.IN-ADDR.ARPA. 10800 IN PTR async03.netroad.com.br.
68.20.200.200.IN-ADDR.ARPA. 10800 IN PTR async04.netroad.com.br.
69.20.200.200.IN-ADDR.ARPA. 10800 IN PTR async05.netroad.com.br.
70.20.200.200.IN-ADDR.ARPA. 10800 IN PTR async06.netroad.com.br.
71.20.200.200.IN-ADDR.ARPA. 10800 IN PTR async07.netroad.com.br.
72.20.200.200.IN-ADDR.ARPA. 10800 IN PTR async08.netroad.com.br.
```

CACHE: NAMED.ROOT

Todo servidor DNS precisa possuir, para seu funcionamento correto, o nome dos servidores do domínio de mais alto nível, o domínio raiz (“.”), a partir dos quais obterá então informações sobre os servidores dos domínios de mais baixo nível (.com, .edu, .net, .gov, e os domínios regionais como .br, .ca, .jp e outros). Esta lista pode ser obtida em *ftp://rs.internic.net/domain/named.root* A relação destes servidores pode mudar de tempos em tempos e é conveniente que o administrador de sistemas verifique periodicamente se o

arquivo com esta informação está atualizado. Caso estes dados estejam incorretos o serviço DNS pode parar de funcionar.

LOOPBACK: 127.0.0.DB

Todo servidor DNS necessita de uma entrada adicional para a interface *loopback*, identificada pelo endereço reservado 127.0.0.1. Todo computador possui este endereço reservado para tratar tráfego interno entre processos. A rede de número 127, como já dissemos, é reservada, e seu primeiro endereço, 127.0.0.1, é utilizado por processos internos que queiram se comunicar. Todos os pacotes de comunicações deste tipo são enviados para a rede de número 127. Um servidor DNS que não configurasse esta interface funciona sem maiores problemas, porém todos os processos que se utilizarem do endereço 127.0.0.1 irão falhar, causando alguns transtornos. Devido a tudo isto, nunca se esqueça de configurar um mapa para a interface *loopback*, como abaixo:

```
0.0.127.IN-ADDR.ARPA. IN SOA ns.netroad.com.br. dnsmaster.netroad.com.br. (
    1 ; Serial
    10800 ; Refresh
    3600 ; Retry
    604800 ; Expire
    86400 ) ; Minimum

0.0.127.IN-ADDR.ARPA.      10800 IN NS      ns.netroad.com.br.
1.0.0.127.IN-ADDR.ARPA.   10800 IN PTR    localhost.
```

SERVIDORES SECUNDÁRIOS

As linhas:

```
secondary    netwizards.com.br      222.222.22.22 s/netwizards.db
secondary    21.200.200.IN-ADDR.ARPA 222.222.22.22 s/200.200.21.0.db
```

indicam que nosso servidor é também um servidor secundário dos domínios *netwizards.com.br* e *21.200.200.IN-ADDR.ARPA*. Para estes domínios não precisamos fazer absolutamente nada, visto que todos os dados serão transferidos do servidor primário destes domínios, identificado pelo número IP 222.222.22.22 e gravados no diretório */usr/local/named/s/netwizards.db* e */usr/local/named/s/200.200.21.0.db*.

CONCLUSÃO

O Sistema de nomes de domínios é um dos pilares da Internet, sem o qual, navegar na Internet seria algo completamente desagradável pois teríamos que gravar vários números para poder acessar um site na rede mundial de computadores, que possui hoje milhões de computadores conectados e continua crescendo.

BIBLIOGRAFIA:

COMER, Douglas E. – Internetworking With TCP/IP Vol. I: Principles, Protocols, and Architecture, 3º edição – Ed. Prentice Hall, Englewood Cliffs, New Jersey.

TANENBAUM, Andrew S. – Redes de computadores (tradução da terceira edição) – Ed. Campus, Rio de Janeiro, 1997.

ÍNDICE

<u>INTRODUÇÃO</u>	<u>3</u>
<u>FUNCIONAMENTO DO DNS.....</u>	<u>4</u>
<u>ESPAÇO DE NOMES</u>	<u>5</u>
<u>SERVIDORES DE NOMES</u>	<u>8</u>
<u>FORMATO DA MENSAGEM DE SERVIDORES DE DOMÍNIO</u>	<u>9</u>
<u>REGISTROS DE RECURSOS</u>	<u>11</u>
<u>DESCRIÇÃO DE ZONA REVERSA 200.200.21.0.DB</u>	<u>17</u>
<u>CACHE: NAMED.ROOT.....</u>	<u>17</u>
<u>LOOPBACK: 127.0.0.DB.....</u>	<u>18</u>
<u>SERVIDORES SECUNDÁRIOS.....</u>	<u>18</u>
<u>CONCLUSÃO</u>	<u>18</u>
<u>BIBLIOGRAFIA:</u>	<u>19</u>