Redes de Computadores I

Aula 15 - Sistema de Nomes de Domínio (DNS)

Apresentação

Nesta aula, você aprenderá um serviço que facilita bastante a utilização da internet, pois permite que as pessoas referenciem as máquinas que desejam acessar utilizando nomes, ao invés dos endereços IPs. Através deste serviço, que se chama **Sistema de Nomes de Domínio** (DNS – *Domain Name System*), é possível atribuir nomes a todos os computadores da internet no mundo inteiro, de maneira estruturada e bem organizada. Para isso, será preciso perceber o funcionamento do DNS como um grande sistema distribuído, onde parte do processamento e do armazenamento das informações é distribuída de maneira hierárquica em todos os computadores que fazem parte desse sistema.

Vídeo 1 - Apresentação

Objetivos

Após o final desta aula, você será capaz de:

- Entender por que um protocolo de resolução de nomes é necessário.
- Identificar a arquitetura do DNSpara entender como as informações dos endereços são organizadas e distribuídas entre os computadores desse sistema.
- Saber como configurar um servidor de DNS no Linux.
- Entender o funcionamento do protocolo observando sua execução entre um cliente e um servidor de DNS.

Porque um sistema de nomes é necessário

Você já sabe que máquinas que usam o protocolo IP para se comunicarem se identificam por meio do endereço IP. Ou seja, quando um programa em uma máquina deseja enviar informações para um programa em outra máquina, ele precisa saber o endereço IP dela (além do número da porta, é claro), pois é esse endereço que é colocado no cabeçalho do pacote IP.

Mas os programas, por sua vez, precisam que nós, humanos, informemos qual é a máquina de destino. Portanto, se nós tivéssemos realmente que informar o endereço IP das máquinas que queremos nos comunicar, ficaríamos em uma situação muito difícil, pois não conseguiríamos lembrar mais do que alguns poucos endereços IP.

Para resolver esse problema é necessário um esquema que associe nomes aos endereços IP das máquinas, pois é muito mais fácil lembrar-se de nomes, do que de números (no caso, endereços IP).

Inicialmente a estratégia foi criar um arquivo chamado *arquivo* de *host* que continha o endereço IP de cada máquina e seu nome. Esse arquivo era então copiado para todas as máquinas da internet. Quando um usuário informava a um programa o nome de uma máquina, o programa consultava esse arquivo e traduzia o nome para o endereço IP associado.

Naturalmente, esse esquema só pode ser utilizado no início da internet, quando ela era formada por apenas uma quantidade muito pequena de máquinas. Hoje, ele seria inviável, devido ao tamanho do arquivo e ao número de cópias necessárias.

Mesmo se pensarmos esse esquema para uma única rede, por exemplo, de uma determinada organização, ele ainda teria problemas, uma vez que a cada nova máquina adicionada na rede o arquivo teria que ser copiado para todas as outras máquinas.

Uma solução mais interessante é usar um modelo cliente-servidor, onde o arquivo é criado em apenas uma máquina (o servidor) e todas as outras (chamadas clientes) enviam uma consulta ao servidor sempre que desejam traduzir um nome

para o endereço IP associado. Nesse novo esquema, em cada máquina cliente é configurado o endereço IP do servidor, para que elas saibam para quem devem enviar as perguntas.

Mesmo com o modelo cliente-servidor nós ainda temos dois grandes problemas a serem resolvidos. O primeiro é como as máquinas de uma organização fariam quando quisessem se comunicar com máquinas de outras organizações, ou seja, como elas descobririam o endereço IP do servidor de outra organização. O segundo problema é como evitar que duas máquinas na internet (em organizações diferentes) tenham o mesmo nome. O *Sistema de Nome de Domínio* (DNS) resolve esses problemas.

Por questões de compatibilidade com as aplicações legadas, até hoje existe o *arquivo de host* em máquinas que possuem a pilha de protocolos TCP/IP instalada. Nos computadores com sistemas operacionais derivados do UNIX, como o Linux, este arquivo é o **/etc/hosts**. Nele, em cada linha, há um mapeamento endereço IP–nome. Assim, se não houver um sistema de nomes (como o DNS, que iremos estudar nesta aula) executando na rede, é possível fazer a tradução de alguns nomes para endereços IP através do mapeamento neste arquivo.

Veja aqui a explicação em vídeo sobre a necessidade do DNS

Vídeo 2 - DNS: necessidade

Nomes de domínio

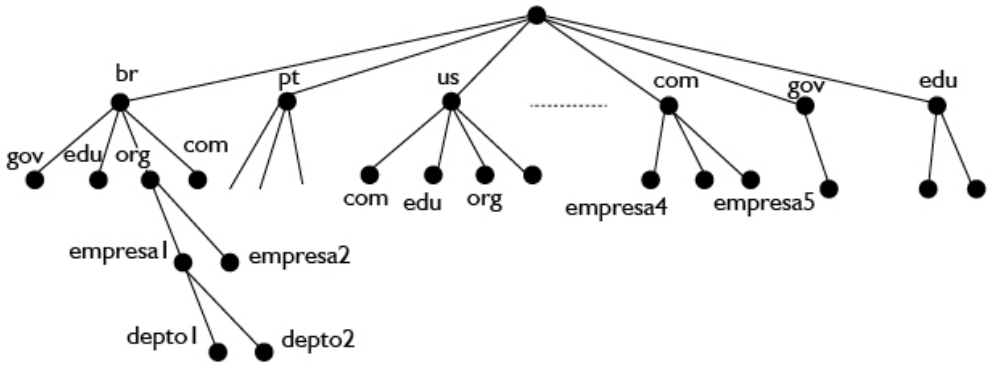
Para não serem duplicados, os nomes atribuídos aos computadores na internet devem ser cuidadosamente selecionados de tal forma que eles devem ser únicos, pois os endereços IP já são. Para permitir isso, o DNS organiza os nomes de modo hierárquico, como uma árvore, onde o primeiro nível identifica o país, o segundo nível o tipo da organização e o terceiro nível os nomes das organizações.

Na verdade, apesar do modelo de árvore organizada como descrito acima ser o ideal, o DNS também permite algumas variações, como por exemplo: i) os tipos das organizações logo abaixo do nó raiz (e não dos países);ii) as organizações logo abaixo do país (e não do tipo de organização).

Esse modelo hierárquico permite que a criação de nomes seja feita de forma descentralizada, delegando responsabilidade sobre diferentes subárvores parar diferentes organizações.

Na **Figura 1**, vemos a estrutura do **espaço de nomes de domínio** usado no DNS.

Figura 01 - Espaço de nomes de domínio

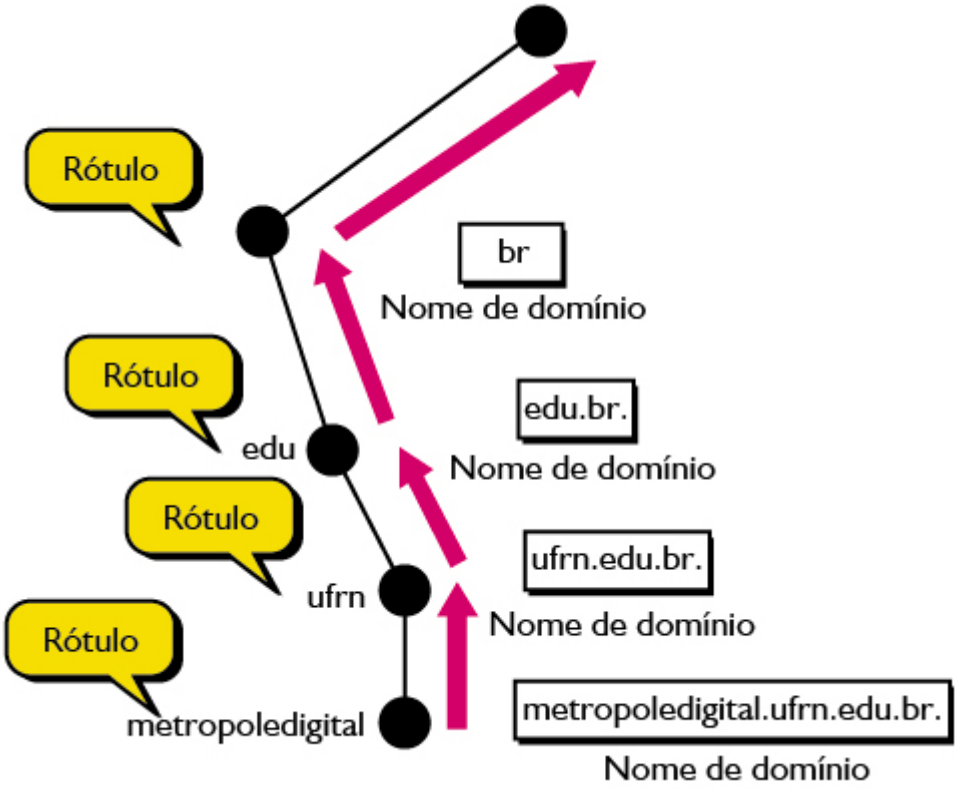


Cada nó na árvore tem um **rótulo**, que nada mais é do que um nome com até 63 caracteres. O nó no topo da árvore (nó raiz) possui um rótulo vazio. Além disso, todos os filhos de um mesmo nó devem possuir rótulos diferentes.

Cada nó na árvore representa um **nome de domínio**, que é o conjunto de rótulo lidos do nó até a raiz.Embora não esteja representado na árvore, abaixo dos nós representando os domínios das empresas devem existir nós que representam os nomes das máquinas dentro do domínio.

A **Figura 2** mostra um exemplo da árvore de domínios para o nome do domínio metropoledigital.ufrn.edu.br.

Figura 02 - Nomes de domínio e rótulos



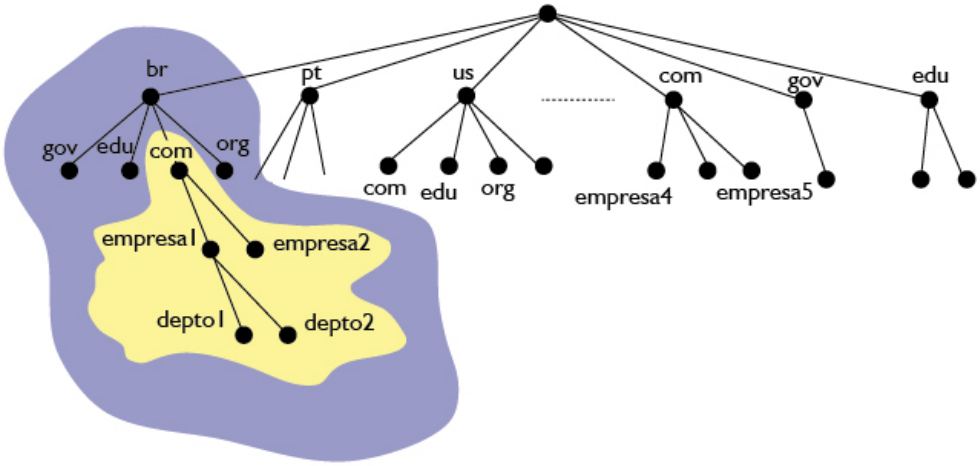
Um **nome de domínio totalmente qualificado** (**FQDN** – *Fully Qualified Domain Name*) é o nome completo, ou seja, o nome que contém o conjunto de rótulos até a raiz da árvore. Por exemplo, o nome do domínio

```
www.metropoledigital.ufrn.edu.br.
```

é o FQDN de um computador chamado www, instalado no Metrópole Digital, da Instituição UFRN, que é uma entidade educacional (edu), que fica no Brasil (br).

Como dissemos, um **domínio** é uma subárvore do espaço de nomes de domínio. O nome do domínio é o mesmo do nó que está no topo da subárvore. A **Figura 3** mostra os domínios "br." e "com.br.". Note que um domínio pode, ele mesmo, ser dividido em domínios (ou **subdomínios**, como às vezes são chamados).

Figura 03 - Nomes de domínio e rótulos



Veja aqui a explicação, em vídeo, sobre a organização dos nomes no DNS

Vídeo 3 - DNS: Nomes de domínios

Atividade 01

1. Qual o principal problema que o DNS visa solucionar?
2. O que é um nome de domínio totalmente qualificado? Cite um exemplo.

Distribuição do espaço de nomes

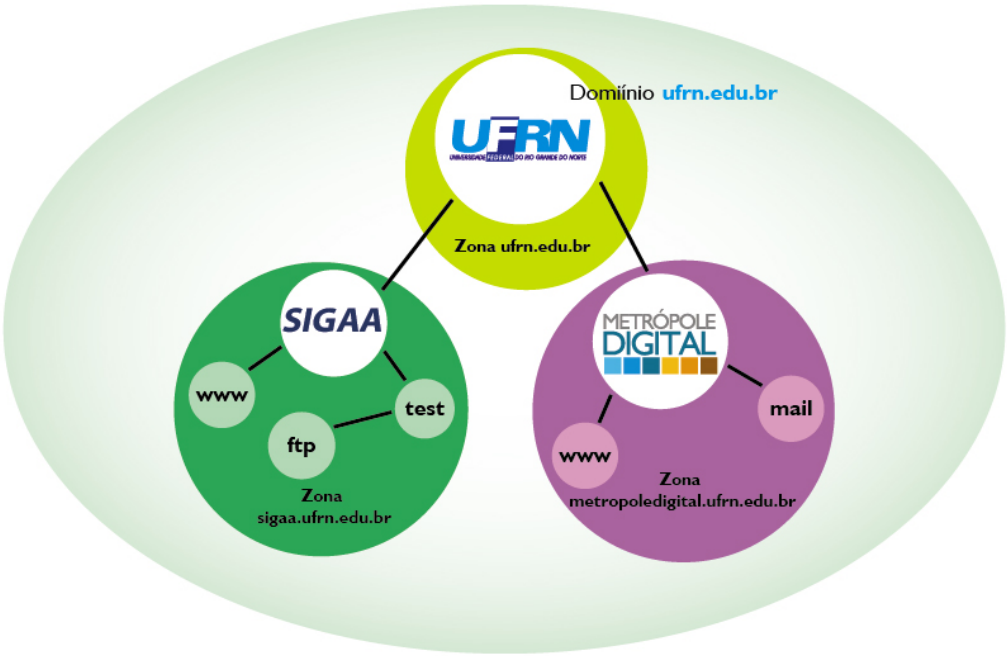
As informações contidas no espaço de nomes de domínio devem ser armazenadas em computadores servidores espalhados na internet, chamados de **servidores DNS**. Como vimos na **Figura 3**, o DNS permite que os domínios sejam subdivididos em domínios menores, chamados de subdomínios. Cada servidor de DNS pode ser responsável (ter autoridade) por um domínio grande ou pequeno. Dizendo de outra forma, cada parte da árvore de DNS pode ficar armazenada em um servidor diferente na internet.

Um servidor é responsável ou tem autoridade sobre o que é chamado de **zona**. Podemos definir uma zona como uma parte da árvore de nomes, podendo ser igual a um domínio ou um subconjunto deste.Por enquanto, pense uma zona sendo igual a um domínio.

A ideia é que cada servidor armazene as informações sobre uma zona. Essas informações, basicamente, consistem dos nomes das máquinas da zona (e seus endereços IPs) e dos servidores responsáveis pelas zonas abaixo dela na árvore. Isso permite que os servidores repassem as consultas de DNS entre si, até localizar o servidor responsável pela zona sendo pesquisada.

A **Figura 4** mostra um exemplo do domínio “ufrn.edu.br”, com diferentes servidores DNS sendo responsáveis pelas diferentes zonas.Ou seja, as informações sobre cada uma das três zonas poderia estar armazenada em um computador (servidor de DNS) diferente.

Figura 04 - Zonas e domínios



Veja aqui a explicação, em vídeo, sobre as zonas do DNS

Vídeo 4 - O que é DNS?

Vídeo 5 - DNS: Zonas

Atividade 02

1. Como são chamados os computadores na internet em que ficam contidas as informações do espaço de nomes de domínio?
2. Explique como é feita a delegação da responsabilidade na administração dos nomes na árvore DNS.

Servidores primários e secundários

O DNS define dois tipos de servidores: principais e secundários. Um **servidor primário** é aquele que lhe foi delegada a autoridade sobre uma zona. É neste servidor onde a pessoa responsável pela zona deve criar, manter e atualizar as informações da zona. Essas informações normalmente são mantidas em um arquivo em disco. Sempre que uma nova máquina é adicionada, por exemplo, é neste servidor que a máquina deve ser cadastrada.

Um **servidor secundário** também irá manter informações sobre a zona, entretanto, ao invés de serem cadastradas manualmente pelo administrador, elas são obtidas automaticamente do servidor primário.

Resolução DNS

O DNS é projetado como um aplicativo cliente-servidor. Um host que precisa fazer o mapeamento de um nome para um endereço IP (ou vice-versa) chama um cliente DNS denominado **resolvedor** (*resolver*). O cliente (resolvedor) acessa o servidor DNS mais próximo com um pedido de resolução (mapeamento). Se o servidor tiver a informação, ele atende ao cliente; caso contrário, ele remete o cliente para outros servidores ou pede a outros servidores para que forneçam a informação. Isto vai depender de como o cliente solicitou a consulta (mapeamento) ao servidor, porque a consulta pode ser recursiva ou interativa.

Na **consulta recursiva**, usada normalmente por um host qualquer e o seu servidor de DNS, o cliente (resolvedor) espera que o servidor forneça a resposta final ao que ele perguntou. Se o servidor for a autoridade do nome de domínio, ele verifica seu banco de dados e responde. Se o servidor não for a autoridade, ele deverá percorrer a árvore a partir da raiz a fim de chegar ao servidor que possui autoridade sobre o domínio consultado, e deste obter a resposta desejada pelo cliente.

A **Figura 5** mostra este processo entre um cliente e seu servidor DNS, no qual o cliente pergunta pelo endereço IP associado ao nome exemplo.foo.eng.br.

- A mensagem 1 é a pergunta do cliente ao seu servidor de DNS.

- A mensagem 2 é a consulta do servidor DNS recursivo à raiz perguntando pelo servidor do domínio br.

- A mensagem 3 é a resposta à pergunta 2 na qual o servidor raiz passa a referência (o endereço IP) do servidor DNS responsável pelo domínio br.

- Na mensagem 4, o servidor recursivo pergunta ao servidor com autoridade sobre o domínio br, a referência ao domínio eng.br.

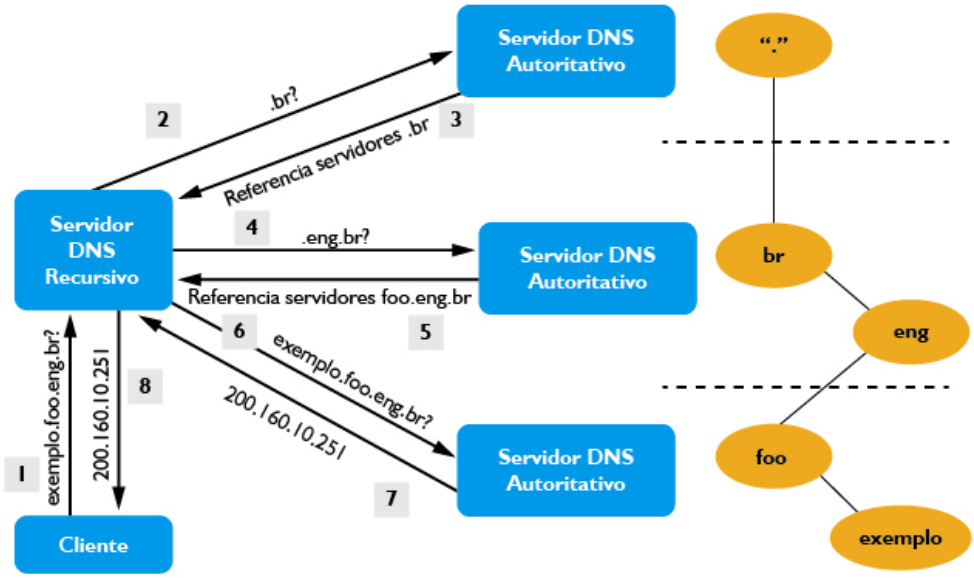
- A mensagem 5 é a resposta à pergunta da mensagem 4, já referenciando o servidor do domínio foo.eng.br, pois o servidor de br também tem autoridade sobre o domínio eng.br.

- A mensagem 6 é a pergunta ao servidor com autoridade sobre o domínio foo.eng.br pelo endereço da máquina exemplo.foo.eng.br.

- A mensagem 7 é a resposta contendo o endereço IP associado a exemplo.foo.eng.br.

- Por fim, na mensagem 8 o servidor DNS recursivo repassa a resposta obtida ao cliente.

Figura 05 - Resolução recursiva entre um cliente e um servidor DNS



A **consulta interativa** é a utilizada entre os servidores de DNS para percorrer a árvore de nomes de domínio. Por exemplo, na **Figura 5**, as consultas do servidor DNS consultado inicialmente pelo cliente aos outros servidores DNS, iniciando pela

raiz, foram feitas de forma interativa. Isto é, há uma interação entre os servidores de DNS a fim de percorrer a árvore de nomes para encontrar a informação consultada.

Veja aqui a explicação, em vídeo, sobre a resolução de nomes no DNS

Vídeo 6 - Consultas e Processos de Resolução DNS

Vídeo 7 - DNS: Resolução

Uso de cache

Sempre que um servidor DNS recebe uma consulta de um nome que não está em seu domínio, precisa percorrer e consultar a árvore de outros servidores DNS a fim de encontrar a reposta solicitada. A redução desse tempo de pesquisa aumentaria a eficiência. O DNS trata disso com um mecanismo chamado **cache**. Quando um servidor solicita um mapeamento a outro servidor e recebe a resposta, armazena essa informação em sua memória cache, antes de enviá-la ao cliente. Se o mesmo cliente ou outro solicitar o mesmo mapeamento, o servidor pode verificar sua memória cache e resolver o problema. Entretanto, para informar o cliente de que a resposta está vindo da memória cache e não de uma origem autorizada, o servidor marca a resposta como não autorizada.

Atividade 03

1. Quais as diferenças entre um servidor DNS primário e um secundário?
2. Caso seja feita uma consulta de um nome que não exista em um Servidor DNS, qual a ação que ele deverá tomar?

3. Qual tipo de consulta é utilizado entre um cliente de DNS e o servidor de DNS local, iterativa ou recursiva?

Arquivo de zona

O banco de dados que contém as informações sobre um domínio é chamado de **arquivo de zona**. Este é um arquivo texto contendo vários registros de dados a respeito daquele domínio. Tais registros são conhecidos como registro de recursos (resource records). Uma mensagem de consulta DNS deve conter o nome pesquisado e o tipo de registro a ser pesquisado. Os tipos de registros de recursos definidos em um arquivo de zona são os mostrados no **Quadro1**.

Registro	Significado
SOA	Indica onde começa a autoridade (sobre o domínio).
NS	Indica um servidor de nomes para uma zona.
A	Mapeamento de nome a um endereço IP (IPv4).
AAAA	Mapeamento de nome a um endereço IP (IPv6).
MX	Indica um *mail exchanger* (servidor de e-mail) para um domínio.
CNAME	Mapeia um nome alternativo (apelido) para um host.
PTR	Mapeamento de um endereço IP a um nome de host.
HINFO	Informação de um host. Fornece a descrição do hardware e do sistema operacional usados por um host.
WKS	Serviços conhecidos. Define os serviços de rede que um host fornece.

Quadro1 - Tipos de registros de recursos no DNS

Como podemos ver pelos registros MX e NS, o DNS faz mais do que apenas traduzir o nome de máquinas para seus endereços IP. O registro NS é utilizado para indicar o servidor de DNS de uma zona filha, enquanto o MX para indicar o servidor de e-mail de um domínio. Além disso, é possível também traduzir endereços IP para nomes, uma tarefa muito útil ao analisar informações dos arquivos de log (que guardam endereços IP).

A **Figura 8** mostra um exemplo de arquivo de zona típico para uma empresa fictícia cujo domínio de internet seria empresa.com.br.

```
@IN   SOA  dns.empresa.com.br. root.empresa.com.br. (
2 ; serial
28800 ; refresh
7200 ; retry
604800 ; expire
86400 ; ttl
)

@      IN   NS     dns.empresa.com.br.
@      IN   NS     ns.operadora.net.br.
@      IN   MX     1   mail.empresa.com.br.
dns    IN   A      10.9.0.37
mail   IN   CNAME  www
www    IN   A      10.9.0.30
@      IN   A      10.9.0.30
```

Figura 8 - Exemplo de arquivo de zona

Neste arquivo de zona, podemos notar o uso dos registros de recursos vistos na **Tabela 1**, como, por exemplo, o SOA e o CNAME. Cada linha simples (que não possui sub-registros) é composta dos seguintes campos: nome, a palavra “IN” indicando internet, o tipo de registro e os dados sobre o mapeamento. O segundo campo contendo sempre “IN” é em razão de que o projeto do sistema DNS previa a resolução de nomes para outras redes ou serviços, o que atualmente não acontece.

No arquivo de zona da **Figura 8**, o caractere arroba (@) é uma referência simplificada ao próprio domínio, neste caso significa “empresa.com.br”. O caractere ponto evírgula (;) representa início de comentário e não é interpretado pelo servidor DNS. Os nomes que não encerrarem com um ponto final (.) serão acrescidos com o nome do domínio. Neste exemplo, o nome www, que aparece sem o ponto final, será interpretado como www.empresa.com.br. O significado de cada linha é explicado no **Quadro 2**.

Registro	Linhas	Descrição
SOA	01	Mostra informações sobre a autoridade do domínio. Os dois primeiros dados são o servidor DNS principal e o e-mail (substituindo o arroba “@” por ponto “.”) do administrador deste domínio. Os demais dados, listados entre parênteses, dizem respeito ao controle das atualizações deste mapa entre os servidores de DNS que obtém informações sobre o domínio.
NS	09 e 10	Indica o servidor de nomes do domínio. Normalmente, usa-se o FQDN do servidor DNS. Neste exemplo, temos dois servidores de DNS para o domínio, um primário e um secundário.
MX	11	Indica o servidor de e-mail do domínio. Este registro exige um número antes do nome do servidor. Este número indica a prioridade (em sequência direta) para se utilizar cada servidor, caso haja mais de um.
A	12, 14 e 15	Mapeamento de um nome para um endereço IP. Observe que todos os nomes de hosts utilizados no mapa da zona possuem um registro A para o endereço IP correspondente.
CNAME	13	Define um segundo nome (*canonical name* ou apelido) para um determinado nome de host. Isto é particularmente interessante quando temos vários serviços no mesmo host, e se utiliza o nome do serviço para o host correspondente. Neste exemplo, o serviço de *mail* é também servido pelo servidor *web*. Se o endereço IP deste servidor multisserviço mudar, basta mudar apenas em um registro.

Quadro 2

Atividade 04

1. Qual o principal benefício de se usar o sistema DNS em uma rede de computadores?

2. É possível usar algum outro mecanismo de tradução de nomes para endereços IP sem usar o sistema DNS?

3. Pesquise na internet alguns dos servidores raiz do sistema DNS e em que países eles estão localizados.

Sempre que alterar o conteúdo do arquivo de uma zona, como o mostrado na Figura 8, altere o valor do campo "serial" para o valor que estiver lá + 1. Os servidores de DNS secundários usam esse número para saber se houve alterações no arquivo.

Na próxima seção, iremos configurar um servidor de DNS para um determinado domínio. Lembre-se, porém, que deve existir algum servidor de DNS na internet que aponte para o seu domínio informando o IP do seu servidor de DNS. Isso é feito no servidor responsável pela zona pai do seu domínio. Se você está criando um domínio abaixo do “com.br”, por exemplo, você terá que registrar o novo domínio no site do registro.br.

Veja aqui a explicação, em vídeo, sobre o registro.br

Vídeo 8 - registro.br

As consultas de DNS são enviadas e respondidas usando o protocolo UDP (embora também seja possível utilizar TCP), com o servidor escutando na porta 53. Entretanto, a transferência de zonas entre um servidor secundário e um primário utiliza o protocolo TCP, com o primário escutando na porta 53.

Configurando um servidor DNS

Agora vamos praticar os conceitos que vimos até agora. A primeira coisa que precisamos é de um servidor de DNS. Vamos assumir que temos duas máquinas, chamadas A e B, e a máquina A será o servidor, enquanto a máquina B será o cliente de DNS.

O Linux possui um pacote chamado bind9 que inclui um programa servidor de DNS. O nome do processo que implementa o servidor de DNS é named. Vamos assumir que este pacote já está instalado na máquina A.

> BIND (*Berkeley Internet Name Domain*) é uma implementação pioneira de um *software* servidor de DNS publicamente distribuída nos sistemas operacionais UNIX e seus derivados, como o Linux. Ele, em sua versão 9, é o servidor DNS mais utilizado no mundo.

Entenda a configuração do servidor de DNS como sendo dividida em duas partes. Em uma você diz por quais zonas é responsável, e na outra cria os arquivos com as informações de cada zona (contendo, por exemplo, os IPs e nomes).

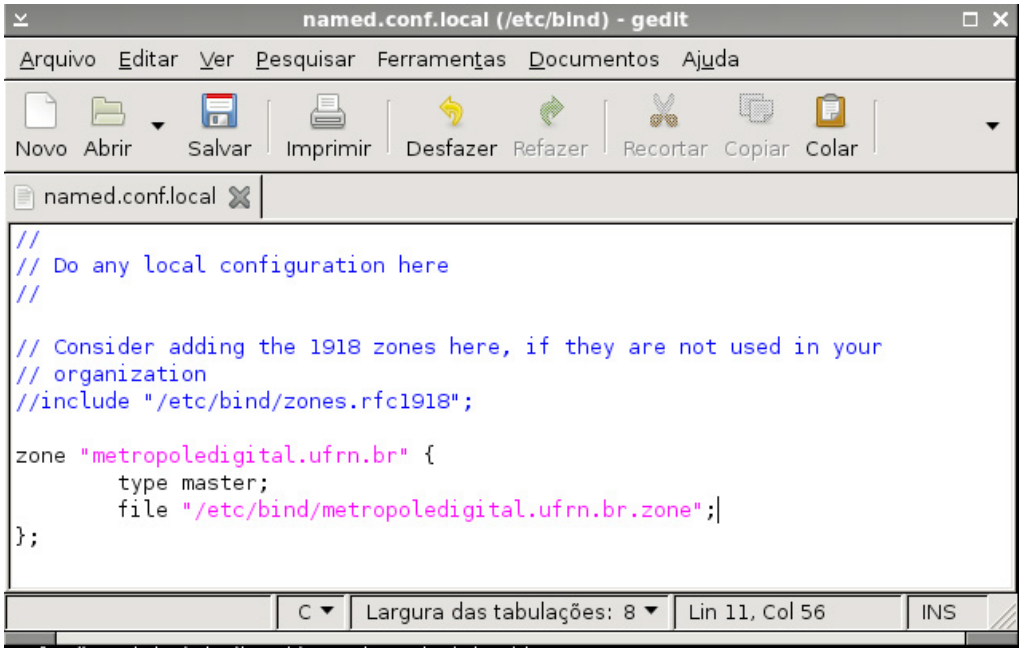
O arquivo principal de configuração do servidor BIND é o */etc/bind/named.conf*. A partir da versão 9 do BIND, este arquivo possui apenas referências a outros dois arquivos dentro do diretório /etc/bind, dividindo os dados das configurações nestes arquivos: *named.conf.options* e *named.conf.local*.

O *named.conf.options* contém as opções gerais de configuração do servidor DNS. O named.conf possui referência para as zonas padrão (*default*) no sistema DNS, como o nome padrão *localhost* que todo computador recebe quando possui conectividade TCP/IP. O arquivo que iremos alterar será o *named.conf.local*, pois ele deve possuir referências para as zonas que serão criadas neste servidor DNS. Ou seja, é nesse arquivo que informamos por quais zonas o servidor é responsável.

Vamos agora abrir o arquivo */etc/bind/named.conf.local* e inserir, logo após os comentários (linhas começando com duas barras "*//*"), as linhas de configuração da zona "metropoledigital.ufrn.br", a qual iremos assumir neste servidor DNS, conforme a **Figura 9**.

Essa configuração de zona exige pelo menos dois parâmetros: o tipo de servidor (primário ou secundário) e qual o arquivo contendo as informações sobre a zona. Neste exemplo, esse servidor será do tipo primário (*master*). Se ele fosse secundário (slave), a próxima linha deveria conter o parâmetro "*masters*", onde deveriam ser informados os endereços IP dos servidores primários. O segundo parâmetro será "/etc/bind/metropoledigital.ufrn.br.zone", no qual colocaremos as informações sobre os registros desta zona.

Figura 09 - Inserindo a zona no servidor DNS



Agora criaremos nosso arquivo da zona "metropoledigital.ufrn.br", que se chama /etc/bind/metropoledigital.ufrn.br.zone. O conteúdo desse arquivo é mostrado na **Figura 10** (acrescentamos aqui a numeração das linhas para facilitar a explicação).

```
@IN   SOA  dns.empresa.com.br. root.empresa.com.br. (
2 ; serial
28800 ; refresh
7200 ; retry
604800 ; expire
86400 ; ttl
)

@      IN   NS     dns.metropoledigital.ufrn.br.
@      IN   MX     1   mail.metropoledigital.ufrn.br.
dns    IN   A      10.1.1.1
mail   IN   CNAME  www
www    IN   A      10.1.1.20
@      IN   A      10.1.1.20
```

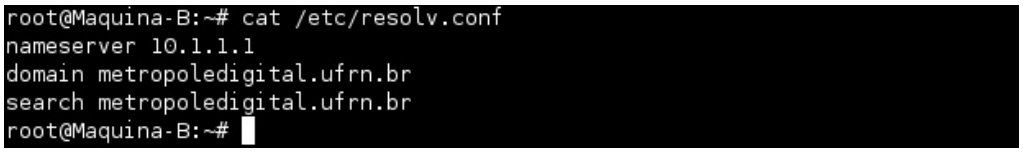
Figura 10 - Arquivo de zona

Após a criação do arquivo, reiniciamos o servidor de DNS, conforme a **Figura 11**.

Figura 11 - Reiniciando o servidor DNS após a criação da zona

Neste ponto, suponha que a máquina B foi ligada e obteve sua configuração IP por DHCP. Uma das informações fornecidas pelo DHCP foi o endereço IP do servidor de DNS. Esse é o parâmetro principal para o resolvedor (cliente DNS) na máquina B. Para observar todas os parâmetros informados ao resolvedor, podemos exibir o conteúdo do arquivo */etc/resolv.conf* nesta máquina, conforme **Figura 12**. Este arquivo que, neste caso, foi criado dinamicamente é quem diz à máquina quem é o seu servidor de DNS.

Figura 12 - Arquivo de configuração do cliente DNS

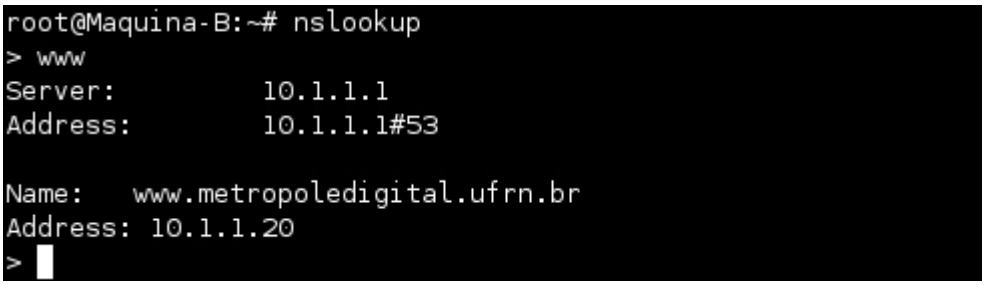


Observe, na **Figura 12**, que o endereço IP do servidor de DNS é informado no parâmetro *nameserver*. Os parâmetros domain e search definem o nome do domínio para a nomenclatura das máquinas e o domínio padrão de pesquisa FQDN quando alguém informar somente o primeiro nome de um host, respectivamente.

Vamos, agora, praticar algumas pesquisas de DNS na máquina B consultando o nosso servidor de DNS instalado na máquina A. Para isso, utilizaremos o aplicativo de linha de comando chamado **nslookup**, que é um cliente do serviço DNS muito utilizado pelos administradores de rede para investigar as configurações deste serviço em qualquer rede ligada à internet.

Ao digitar nslookup na linha de comando, você abre este aplicativo que lhe apresenta outro *prompt* de comandos, no qual você digitará aquilo que deseja pesquisar no sistema DNS. Podemos testá-lo digitando o nome www e pressionando a tecla ENTER, conforme **Figura 13**.

Figura 13 - Prompt de comandos do nslookup

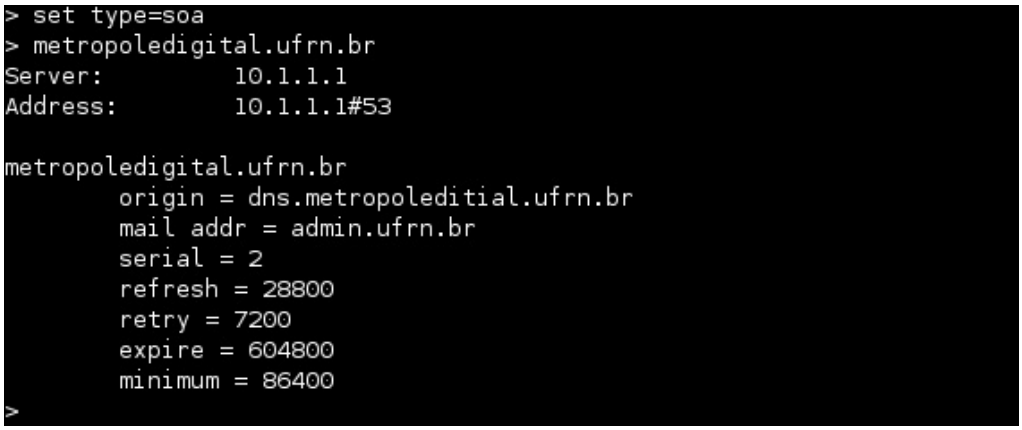


Observe o que ele mostra como resultado. Primeiro as informações do servidor de DNS consultado, seu endereço IP e a porta UDP utilizada na consulta. Em seguida, ele mostra o nome FQDN consultado e o endereço IP mapeado para este nome. Ele acrescentou o domínio “metropoledigital.ufrn.br” ao nome pesquisado devido o parâmetro *search* do /etc/resolv.conf, na **Figura 12**.

Veja que não especificamos o tipo de registro que queríamos e ele respondeu com uma resposta do tipo “A” (*address*), endereço IP do nome, pois esta é o tipo de consulta/registro padrão.

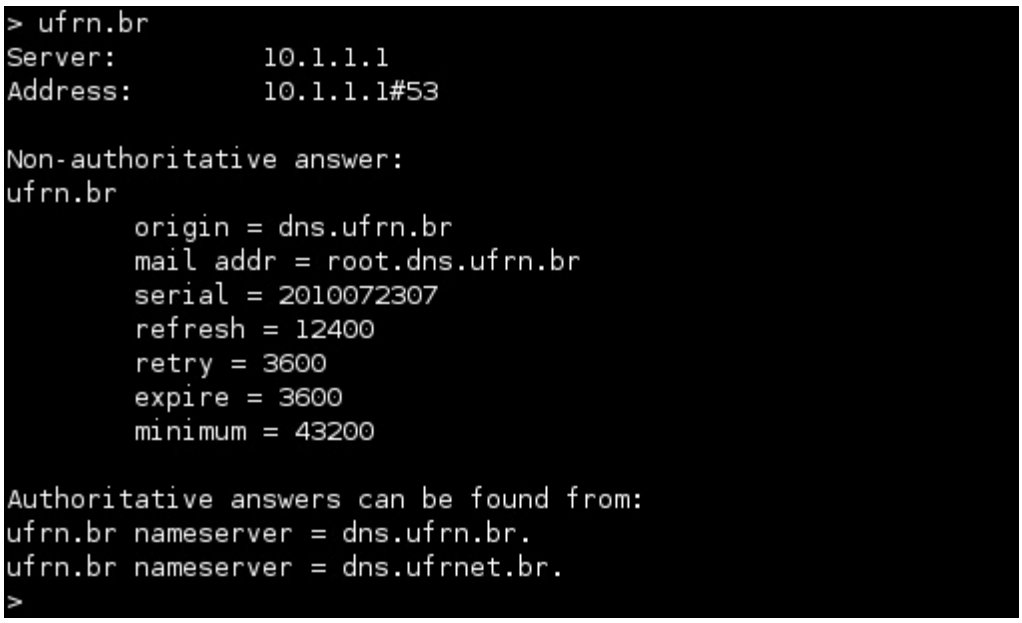
Vamos, agora, mudar o tipo de consulta ao nosso servidor. Para isso, precisamos digitar o comando “set type=X”, onde X representa o tipo de registro de recurso no DNS, conforme **Tabela 1**. Vamos pedir o registro SOA do domínio desta prática, conforme **Figura 14**.

Figura 14 - Solicitação do registro SOA do nosso domínio



Vamos, agora, testar consultar um nome no qual nosso servidor não possui autoridade. Conforme **Figura 15**, vamos consultar o registro SOA do domínio ufrn.br e observar o resultado.

Figura 15 - Consultando o registro SOA de outro domínio



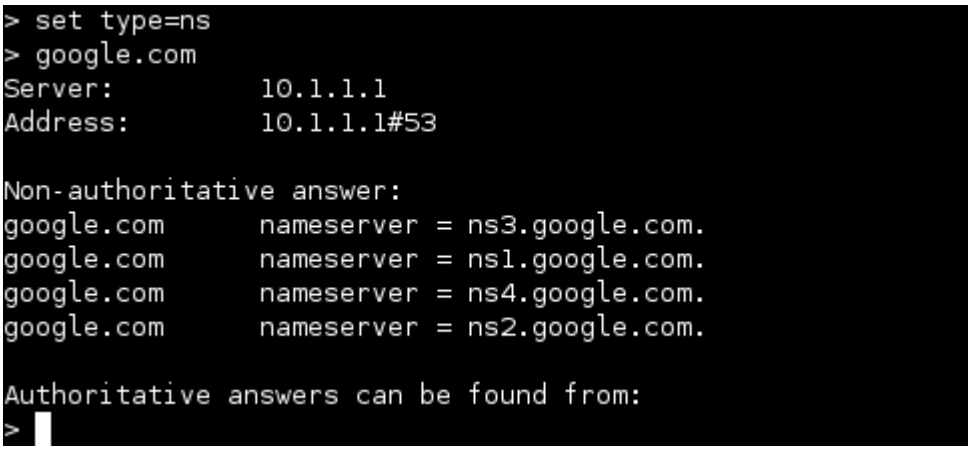
Veja que apareceu a linha "*Non-authoritative answer*:", seguido da resposta contendo o registro SOA do domínio pesquisado. Esta linha indica que o servidor que respondeu a consulta não tem autoridade sobre o domínio (nome) consultado, e que ele obteve esta resposta a partir de consulta a outros servidores, no esquema de consultas recursivas percorrendo a árvore hierárquica dos nomes.

Ainda na **Figura 15**, observe que é possível saber qual é o servidor que pode dar uma resposta autorizada sobre o domínio em questão. Neste exemplo seria um dos dois servidores listados, os quais são os servidores primário e secundário do

domínio.

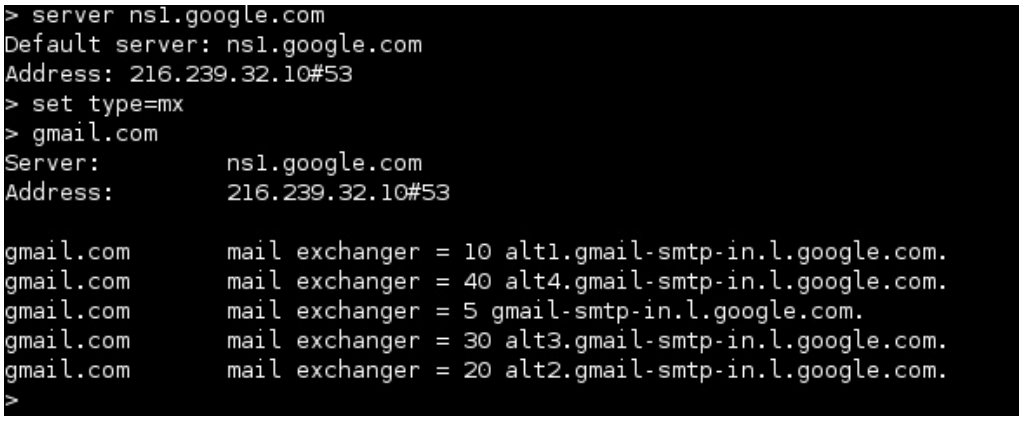
Para realizar uma consulta sobre o servidor DNS de um nome, deve-se mudar a consulta para o registro NS com o comando "set type=ns", e em seguida digita-se o nome do domínio a ser consultado, conforme **Figura 16**.

Figura 16 - Consultando os servidores de nomes de um domínio



Observe, na **Figura 16**, que a pergunta aos servidores de nomes do domínio do Google retornou quatro servidores. Vamos utilizar um deles para a consulta ao registro MX (servidor de e-mail) do domínio gmail.com, conforme **Figura 17**. Para mudarmos o servidor a ser consultado, devemos digitar o comando “server *IP_ou_nome_do_servidor*”.

Figura 17 - Consultando outro servidor de DNS



Observe, na **Figura 17**, que não surgiu mais a linha informando uma resposta não autorizada. Isto porque a resposta veio de um servidor que tem autoridade sobre o domínio consultado. Neste exemplo, gmail.com é o domínio do serviço de e-

mail do Google. Observe também que apareceu uma lista de servidores de e-mail, cada um com sua prioridade (quanto menor o número maior a prioridade) para entrega das mensagens neste domínio.

Vídeo 9 - Realizando consultas com o dig

Atividade 05

1. Qual o tipo de registro do DNS que informa quem é o servidor de e-mail de um domínio?
2. Para que serve o comando nslookup?
3. Pesquise sobre uma ferramenta muito usada no Linux para consulta de DNS chamada dig. Veja suas funcionalidades e como ela é usada. Dica: Lembre-se que existem manuais de vários programas no Linux; para verificar o manual do dig, use o comando “man dig”.

Siga o tutorial para praticar um pouco.

Confira aqui a execução desse tutorial.

Vídeo 10 - Tutorial

Resumo

Nesta aula, você aprendeu que em uma rede é necessário que exista um serviço de tradução de nomes para endereços IP a fim de evitar que tenhamos decorar números ao acessarmos serviços em computadores na rede. Este serviço de nomear todos os computadores ligados à internet em todo o planeta é o DNS. Você observou que ele trabalha de maneira distribuída e segue uma estrutura de distribuição baseada em árvore hierárquica. Nesta árvore de servidores, cada um fica responsável pelo domínio de nomes da organização do qual faz parte, permitindo criar subárvores para nova divisão dos nomes dentro deste domínio. Você também percebeu que para aumentar a disponibilidade do sistema, há os servidores primários e os secundários, e para otimizar os tempos das consultas os servidores guardam temporariamente as consultas já realizadas em cache. Por fim, praticou a configuração de um servidor DNS a partir de um aplicativo cliente, o nslookup.

Autoavaliação

1. Inicie o wireshark (ou tcpdump) e deixe-o capturando os pacotes que saem ou chegam em seu computador.
2. Realize um ping para a máquina cujo nome é “www.sony.co.jp”.
3. Encerre o capturador de pacotes e responda:
    a. Quantos e quais pacotes foram trocados antes dos pacotes ICMP relacionados ao comando ping?
    b. Qual a porta em que o servidor de DNS está escutando?
    c. Qual o protocolo de transporte que foi utilizado para as consultas de DNS?
4. Como o nslookup poderia ser utilizado para descobrir o IP associado ao nome “www.sony.co.jp”?

Referências

FOROUZAN, B. **Comunicação de Dados e Redes de Computadores**. 4. ed. São Paulo: MCGRAW-HILL, 2008.

KUROSE, J.; ROSS, K. **Redes de computadores e a internet**. 5. ed. São Paulo:Addison Wesley, 2010.

WETHERALL, David; TANENBAUM, Andrew S. **Redes de computadores**. 5. ed. Rio de Janeiro: Editora Pearson, 2011.