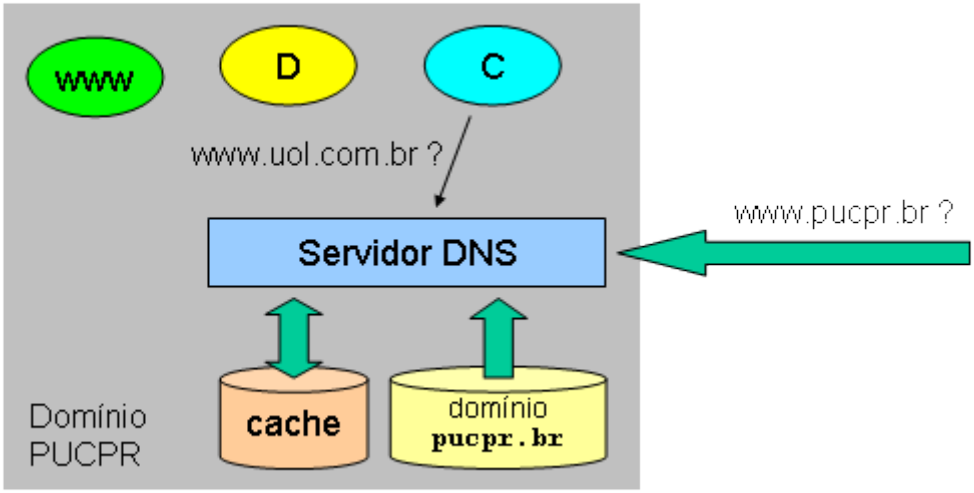
O Serviço DNS

O serviço DNS (*Domain Name System*) é o principal responsável pela resolução de nomes na Internet. Esse serviço é construído por um conjunto de servidores operando de forma descentralizada. Cada servidor DNS é responsável por um domínio ou sub-domínio de nomes na Internet. Neste módulo são apresentadas as principais características do serviço DNS e seu modo de funcionamento.

Funções do servidor DNS

Um servidor DNS normalmente executa as seguintes atividades:

- responde a consultas de clientes ou servidores externos (vindas da Internet) sobre nomes registrados em seu domínio local;
- realiza resoluções de nomes de domínio na Internet para seus clientes locais (máquinas dentro de seu domínio);
- guarda em cache local as resoluções de nomes solicitadas por seus clientes, para agilizar consultas futuras.



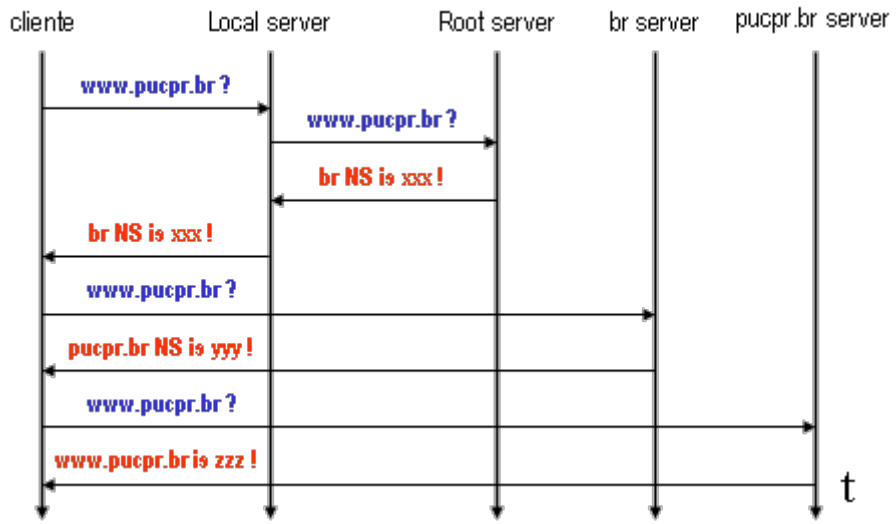
Quanto à sua funcionalidade, um servidor DNS pode ser:

- **Primário**: É o servidor responsável por um domínio. A inclusão, alterações ou exclusão dos registros desse domínio são feitas neste servidor.
- **Secundário**: funciona como backup do servidor primário, recebendo dele os registros do domínio através de um processo chamado *zone transfer*; também responde às requisições dos clientes quando requisitado.
- **Caching-only**: servidor DNS que apenas efetua consultas e retorna resultados, mantendo uma cache local. Não é responsável por nenhum domínio, sua única função é melhorar o desempenho das resoluções de nome para os clientes locais usando seu cache.

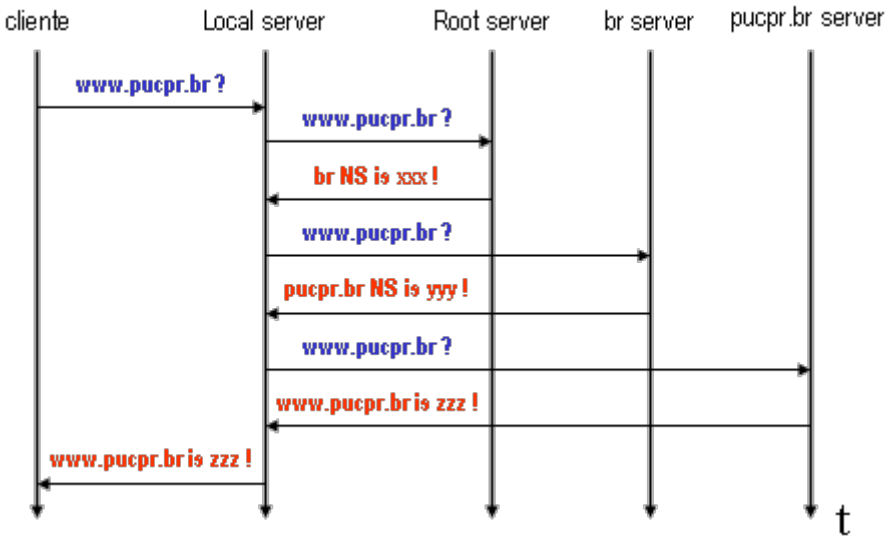
Consultas DNS

Em relação aos seus clientes locais, um servidor DNS pode operar com dois tipos de consultas: **iterativas** e **recursivas**. O modo de operação default, suportado por todos os servidores, é o de consultas iterativas, na qual o cliente DNS pode receber do servidor local uma resposta parcial. Assim, ele terá de contactar

sucessivamente outros servidores DNS para conseguir resolver o nome desejado. Veja um exemplo de consulta iterativa na figura a seguir:



No modo de consulta recursiva, o servidor local se encarrega de encaminhar a consulta do cliente a todos os servidores DNS necessários até que ela seja resolvida, devolvendo ao cliente apenas a resposta final. Esse modo de operação é opcional e não precisa ser implementado por todos os servidores. Um exemplo de consulta recursiva:



No caso de consultas iterativas, a resposta de um servidor DNS ao cliente pode ser:

- *Authoritative*: quando ele é o servidor responsável pelo domínio objeto da consulta;
- *Non-authoritative*: quando ele respondeu por já ter a resposta em seu cache local.

A cada domínio local sob a responsabilidade de um servidor DNS corresponde um **arquivo de zona** (arquivo-texto que contém as definições dos nomes pertencentes a um determinado domínio e seus respectivos endereços IP). Para cada domínio também deve estar presente um **arquivo de zona reversa**, que relaciona os endereços IP aos nomes existentes no domínio.

Arquivos de zona

Cada servidor DNS armazena localmente as informações sobre os domínios de sua responsabilidade em arquivos de texto denominados “arquivos de zona” (*zone files*). As informações sobre o domínio são armazenadas em arquivos de zona direta (para os mapeamentos nome -> IP) e de zona reversa (para os mapeamentos IP -> nome). Eis um exemplo (hipotético) de arquivo de zona direta para o domínio `pucpr.br`:

```
pucpr.br. IN SOA ns1.pucpr.br. postmaster.pucpr.br. (
            1        ; Serial number (increase it after edit)
            10800    ; Refresh after 3 hours (3 x 3600 sec)
            3600     ; Retry after 1 hour (1 x 3600 sec)
            604800   ; Expire after 1 week (7 x 24 x 3600 sec)
            86400 )  ; Minimum TTL of 1 day (24 x 2600 sec)

; Name server for this domain
pucpr.br.       IN    NS    ns1.pucpr.br.

; Mail server for this domain
pucpr.br.       IN    MX    10    mailer1.pucpr.br.

; Addresses for local names
localhost.pucpr.br. IN    A    127.0.0.1

ns1.pucpr.br.       IN    A    200.192.112.2
                TXT    "Servidor de nomes primario"
                HINFO    "PC P4" "Linux Slackware 8"

alfa.pucpr.br.      IN    A    200.192.112.168
                TXT    "Servidor de e-mail"
                HINFO    "Sun UltraServer 5" "Solaris 9"

; Aliases
mailer1.pucpr.br.   IN    CNAME    alfa.pucpr.br.
```

Eis o arquivo hipotético correspondente de zona reversa para o mesmo domínio `pucpr.br`:

```
112.192.200.in-addr.arpa. IN SOA ns1.pucpr.br. postmaster.pucpr.br.(
            1        ; Serial number (increase it after edit)
            10800    ; Refresh after 3 hours (3 x 3600 sec)
            3600     ; Retry after 1 hour (1 x 3600 sec)
            604800   ; Expire after 1 week (7 x 24 x 3600 sec)
            86400 )  ; Minimum TTL of 1 day (24 x 3600 sec)

; Name servers
112.192.200.in-addr.arpa.   IN    NS    ns1.pucpr.br.

; Addresses point to canonical name
2.112.192.200.in-addr.arpa. IN    PTR    ns1.pucpr.br.
182.112.192.200.in-addr.arpa.   IN    PTR    alfa.pucpr.br.
```

Um arquivo de zona direta ou reversa contém normalmente os seguintes campos:

Campo	**Função**
SOA	indica quem é o responsável por essa zona (a autoridade)

Campo	Função
NS	indica um servidor de nomes para a zona
MX	indica um servidor de e-mail para a zona
A	indica o endereço IP relativo a um dado nome de domínio (resolução direta)
TXT	string descrevendo o host
HINFO	indica dados de hardware e software do host
CNAME	indica um alias (sinônimo) de nome de domínio
PTR	indica o nome de domínio relativo a um dado endereço IP (resolução reversa)

O Servidor DNS Bind

A construção de um servidor DNS implica na instalação e configuração do software apropriado. O servidor DNS mais usado no mundo UNIX é o BIND, que vem por default nas distribuições Linux. Os principais arquivos do servidor BIND em uma distribuição Linux no padrão RedHat são os seguintes:

- `/etc/rc.d/init.d/named` : script de inicialização, que lança um daemon denominado named. Ele deve ser invocado com um dos seguintes parâmetros:
  - `start` : lança o serviço (gera mensagens de inicialização em /var/log/messages)
  - `stop` : para o serviço
  - `restart` : reinicia o serviço
  - `status` : verifica o status do serviço
- `/etc/named.conf` : configuração de inicialização do servidor.
- `/var/named` : diretório que contem as informações de cada zona de domínio, e os arquivos de zonas reversas respectivas.

Nas próximas seções são apresentados os arquivos de exemplo para a configuração de um servidor de nomes no domínio `pucpr.br`.

Arquivo /etc/named.conf

Este é o arquivo central de configuração do Bind, que informa quais as zonas sob sua responsabilidade e seus respectivos arquivos.

```
# BIND configuration file for pucpr.br

options {
    directory "/var/named";
};

zone "pucpr.br" in {
    type master;  # authoritative server for this zone
    file "zone-pucpr.br";
};

zone "112.192.200.in-addr.arpa" in {
    type master;  # authoritative server for this zone
    file "zone-200.192.112";
};

zone "0.0.127.in-addr.arpa" in {
    type master;  # loopback zone
    file "zone-127.0.0";
};
```

```
zone "." in {
    type hint;   # local cache start contents
    file "zone-cache";
};
```

Arquivo /var/named/zone-pucpr.br

Este arquivo contém as informações de zona direta do domínio pucpr.br.

```
pucpr.br. IN SOA ns1.pucpr.br. postmaster.pucpr.br. (
            1        ; Serial number (increase it after edit)
            10800    ; Refresh after 3 hours (3 x 3600 sec)
            3600     ; Retry after 1 hour (1 x 3600 sec)
            604800   ; Expire after 1 week (7 x 24 x 3600 sec)
            86400 )  ; Minimum TTL of 1 day (24 x 2600 sec)

; Name server for this domain and sub-domains
pucpr.br.       IN    NS    ns1.pucpr.br.

; Mail server for this domain
pucpr.br.       IN    MX    10    mailer1.pucpr.br.

; Addresses for local names
localhost.pucpr.br. IN    A    127.0.0.1

ns1.pucpr.br.       IN    A    200.192.112.2
                TXT    "Servidor de nomes primario"
                HINFO    "PC P4" "Linux Slackware 8"

ppgia.pucpr.br.     IN    A    200.192.112.141
                TXT    "Servidor principal PPGIA"
                HINFO    "PC P4" "Free BSD 4.9"

alfa.pucpr.br.      IN    A    200.192.112.168
                TXT    "Servidor de e-mail"
                HINFO    "Sun UltraServer 5" "Solaris 9"

; Aliases
mailer1.pucpr.br.   IN    CNAME    alfa.pucpr.br.
```

Arquivo /var/named/zone-200.192.112

Este arquivo contém as informações de zona reversa do domínio pucpr.br.

```
112.192.200.in-addr.arpa. IN SOA ns1.pucpr.br. postmaster.pucpr.br.(
            1        ; Serial number (increase it after edit)
            10800    ; Refresh after 3 hours (3 x 3600 sec)
            3600     ; Retry after 1 hour (1 x 3600 sec)
            604800   ; Expire after 1 week (7 x 24 x 3600 sec)
            86400 )  ; Minimum TTL of 1 day (24 x 3600 sec)

; Name servers
112.192.200.in-addr.arpa.   IN    NS    ns1.pucpr.br.
```

```
; Addresses point to canonical name
2.112.192.200.in-addr.arpa. IN    PTR    ns1.pucpr.br.
141.112.192.200.in-addr.arpa.   IN    PTR    ppgia.pucpr.br.
182.112.192.200.in-addr.arpa.   IN    PTR    alfa.pucpr.br.
```

Arquivo /var/named/zone-127.0.0.1

Este arquivo contém as informações de zona reversa da interface loopback.(127.0.0.1).

```
0.0.127.in-addr.arpa. IN SOA ns1.pucpr.br. postmaster.pucpr.br. (
            1        ; Serial
            10800    ; Refresh after 3 hours
            3600     ; Retry after 1 hour
            604800   ; Expire after 1 week
            86400 )  ; Minimum TTL of 1 day

0.0.127.in-addr.arpa.   IN    NS    ns1.pucpr.br.

1.0.0.127.in-addr.arpa. IN    PTR    localhost.
```

Arquivo /var/named/zone-cache

Este arquivo define o conteúdo inicial do cache do servidor DNS, que consiste basicamente dos endereços dos servidores raiz (rootservers). Este arquivo deve ser atualizado periodicamente a partir deste servidor.

```
; This file holds the information on root name servers needed to initialize
; cache of Internet domain name servers ...
;
.           3600000  IN  NS    A.ROOT-SERVERS.NET.
A.ROOT-SERVERS.NET. 3600000      A     198.41.0.4
;
; formerly NS1.ISI.EDU
;
.           3600000      NS    B.ROOT-SERVERS.NET.
B.ROOT-SERVERS.NET. 3600000      A     128.9.0.107
;
; formerly C.PSI.NET
;
.           3600000      NS    C.ROOT-SERVERS.NET.
C.ROOT-SERVERS.NET. 3600000      A     192.33.4.12
;
; formerly TERP.UMD.EDU
;
.           3600000      NS    D.ROOT-SERVERS.NET.
...
; End of File
```

Caso o servidor DNS não tenha acesso direto ao exterior (aos DNS *rootservers*) mas possa acessar outro servidor DNS, então uma configuração de *forwarding* se torna interessante. Com ela, o servidor encaminha as solicitações recebidas a outro(s) servidor(es), e guarda os resultados recebidos em uma cache local. A configuração para habilitar o *forwarding* no servidor Bind é a seguinte (a ser editada no arquivo `/etc/named.conf`):

```
options {

    ...

    forward only ;
    forwarders {
        nnn.nnn.nnn.nnn ;
        ...
    };
};
```

Com isso, todas as consultas de DNS endereçadas a seu servidor serão encaminhadas ao(s) servidor(es) indicados, naquela ordem, até obter uma resposta. Caso a linha `forward only` seja omitida, o servidor tentará a resolução do endereço em suas tabelas locais e depois, caso não tenha sucesso, nos servidores indicados.

Dig e nslookup

Os utilitários `dig` e `nslookup` permitem efetuar consultas a servidores DNS via linha de comando. Eles são muito utilizados para verificar configurações e diagnosticar problemas no serviço DNS. O comando `nslookup` vem sendo substituido pelo `dig`, por isso somente este último será apresentado aqui.

A sintaxe básica de uso do comando `dig` é a seguinte (campos entre colchetes são opcionais):

```
dig [@server] name [type]
```

onde:

- `@server` (opcional) indica o servidor DNS a consultar;
- `name` indica o nome de domínio a consultar;
- `type` indica o registro desejado: A (default), NS, MX, CNAME, etc.

Alguns exemplos de uso do dig:

- `dig ftp.unicamp.br` : consulta direta de endereço (campos A) usando o servidor de nomes default (definido em `resolv.conf`).
- `dig @myserver ftp.unicamp.br` : consulta de endereço (campos A) usando o servidor de nomes `myserver`.
- `dig unicamp.br MX` : consulta do campo MX do domínio unicamp.br usando o servidor default.
- `dig -x 200.192.112.141` : consulta de DNS reverso usando o servidor default.

Segue abaixo um exemplo de consulta simples usando o comando `dig`:

```
$ dig www.unifor.br

; <<>> DiG 9.2.1 <<>> www.unifor.br
;; global options: printcmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 7382
;; flags: qr rd ra; QUERY: 1, ANSWER: 1, AUTHORITY: 1, ADDITIONAL: 0

;; QUESTION SECTION:
;www.unifor.br. IN A

;; ANSWER SECTION:
```

```
www.unifor.br. 86400 IN A 200.253.187.1

;; AUTHORITY SECTION:
unifor.br. 86400 IN NS www.unifor.br.

;; Query time: 65 msec
;; SERVER: 200.192.112.2#53(200.192.112.2)
;; WHEN: Tue May 25 00:28:41 2004
;; MSG SIZE rcvd: 61
```