SERVIÇOS BÁSICOS: Conceituação, Instalação e Configuração

- Na arquitetura TCP/IP serviços são disponibilizados em portas;
- Alguns serviços são ativados e associados automaticamente a portas específicas durante a inicialização da máquina (servidor); correio eletrônico e resolução de nomes são exemplos;
- Alguns serviços são ativados e associados a portas específicas sob demanda, quando um cliente solicita uma conexão com o servidor; terminal remoto, transferência de arquivos são exemplos.
- Em ambientes *NIX (UNIX, LINUX), o arquivo /etc/services elenca os serviços possíveis em um dado servidor, e o arquivo /etc/inetd.conf elenca os servidores (software) associados a cada serviço.
- Sempre que um dos arquivos for alterado, deve-se informar ao servidor internet (inetd) sobre o fato, enviando-lhe um sinal de *Hang-Up* (HUP) com o comando kill.

```
[root@ebct]# killall -HUP inetd
[root@ebct]#
```


/etc/Services

```
# Network services, Internet style
#
( . . . )
ftp             21/tcp
ssh             22/tcp
telnet          23/tcp
smtp            25/tcp mail
( . . . )
domain          53/tcp nameserver   # domain-name server
domain          53/udpnameserver
( . . . )
www             80/tcp http                 # WorldWideWeb HTTP
www             80/udp                      # HyperText Transfer Protocol
( . . . )
pop3            110/tcp
(...)
```

/etc/inetd.conf

```
# Network servers, Internet style
#
(...)
ftp     stream      tcp     nowait      root    /usr/local/etc/in.ftpd in.ftpd -d -l
pop3    stream      tcp     nowait      root    /usr/local/etc/popper popper
imap4   stream      tcp     nowait      root    /usr/sbin/imap4d imap4d
( . . . )
```


DNS – "Domain Name Service" - Conceituação

O esquema de endereçamento TCP/IP prevê que cada elemento da rede seja identificado de forma única através de um número – o endereço IP;

- Trabalhar com números é mais natural para as máquinas, mas as pessoas preferem trabalhar com nomes; é muito mais fácil lembrar, por exemplo, que informações sobre a Universidade Federal de Campina Grande estão disponíveis na máquina www.ufcg.edu.br ao invés do endereço 150.165.111.253.
- Guardar uma tabela com todos os nomes e endereços de máquinas da Internet em cada máquina conectada à rede é impossível (não só pelo tamanho, como pela impossibilidade de atualização da base para mantê-la consistente);
- Como resolver o problema? Criar um mecanismo (ou serviço) que permita que o mapeamento de nomes em endereços seja feito de forma distribuída, com muitos computadores (servidores) na rede "tomando conta" de quantidades mais manipuláveis de nomes;
- Ideia! Organizar a Internet em Domínios Administrativos e criar um banco de dados hierárquico, distribuído, onde exista um ou mais servidores em cada nível da hierarquia, responsáveis por fornecer informações sobre nomes que se situam abaixo desse ponto da hierarquia (apenas um nível).
- A definição de domínios administrativos e a imposição de que não se cadastre equipamentos e subdomínios com o mesmo nome em um domínio, evita a utilização de um mesmo nome para mais de um equipamento na rede;
- O nome de todo equipamento na rede vai ser composto de um nome local (que pode se repetir em domínios diferentes), seguido por uma hierarquia de domínios; o nome completo do equipamento passa a ser seu 'Nome de Domínio Totalmente Qualificado' – "Fully Qualified Domain Name – FQDN";

- Domínios na Internet refletem uma organização institucional e/ou geográfica; nos Estados Unidos tem-se, por exemplo:

Domínio	Tipo de Instituição	Exemplo
.mil	Instituições com fins militares	AntiSaddan.mil
.edu	Instituições educacionais	Berkeley.edu
.com	Instituições comerciais	Microsoft.com
.gov	Instituições governamentais	Whitehouse.gov
.org	Instituições não-governamentais	Linux.org
.net	Instituições ligadas à rede	Eria.net

- No Brasil, tem-se uma organização semelhante, acrescentando-se o sufixo .br aos domínios anteriores:

Domínio	Tipo de Instituição	Exemplo
.mil.br	Instituições com fins militares	Emfa.mil.br
.edu.br	Instituições educacionais	Ufcg.edu.br
.com.br	Instituições comerciais	Uol.com.br
.gov.br	Instituições governamentais	Mare.gov.br
.org.br	Instituições não-governamentais	Atecel.org.br
.net.br	Instituições ligadas à rede	Embratel.net.br

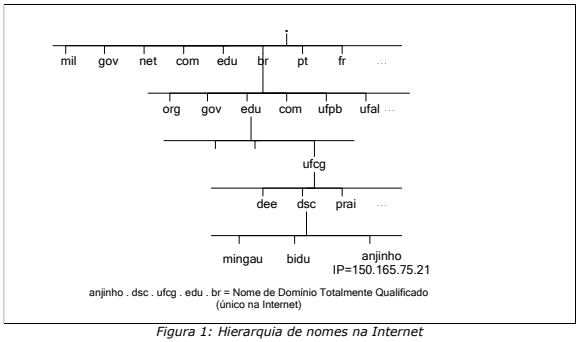

Figura 1: Hierarquia de nomes na Internet

- Toda vez que alguém (em geral, software de aplicação) precisa descobrir o endereço IP associado a algum nome na rede, faz uma consulta direta (consulta ao DNS direto) ao servidor de nomes do domínio local; este, por sua vez, faz uma busca começando na raiz da hierarquia, descendo pelos ramos até encontrar a informação procurada ou descobrir que a mesma não existe na rede (ou não está cadastrada nos servidores de nomes).

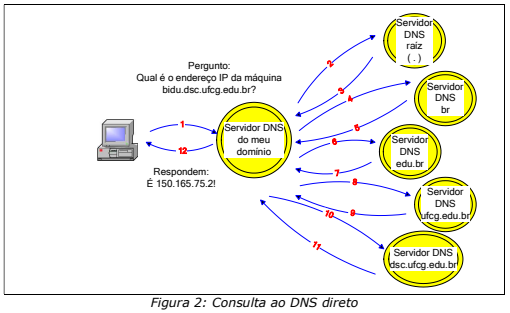

Figura 2: Consulta ao DNS direto

- De modo semelhante, alguém pode querer saber qual é o nome associado a algum endereço IP. Nesse caso, o servidor de nomes local faz uma consulta reversa (consulta ao DNS reverso) também começando pela raiz da hierarquia.

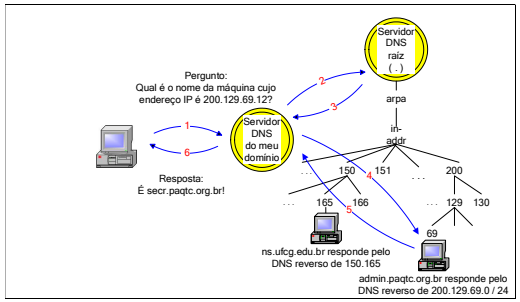

Figura 3: Consulta ao DNS reverso

Instalação / Configuração do DNS

- O serviço de nomes de domínio em ambientes *NIX é feito pelo software BIND ("Berkeley Internet Name Domain"), que é um sistema do tipo cliente / servidor;
- O lado cliente é chamado resolvedor ("resolver") e é implementado como um conjunto de funções em bibliotecas em todo sistema operacional com suporte a TCP/IP;
- O lado servidor é chamado named e é implementado como um processo servidor ("daemon");
- Um servidor DNS pode ser:
  - Só de armazenamento: quando não dispõe de nenhuma base de dados sobre nomes de máquinas/subdomínios; ele obtém e guarda as respostas obtidas nas consultas de DNS realizadas através dele, e as usa em consultas futuras;
  - Primário: quando é a fonte original de informações sobre um (ou mais) domínio; obtém as informações sobre o domínio que está servindo em arquivos locais que devem ser mantidos pelo administrador do domínio;
  - Secundário: quando é a fonte não original de informações sobre um (ou mais) domínio; obtém informações sobre o domínio que está servindo a partir do servidor primário; nesse caso atua como um servidor de redundância ("backup").

- Colocar um servidor de nomes para funcionar implica em configurar os arquivos:
  - named.conf que configura os parâmetros gerais do servidor;
  - named.zone: que faz o mapeamento de nomes para endereços IP;
  - named.rev: que faz o mapeamento de endereços IP para nomes;
  - named.local: que faz o mapeamento de endereço IP para nomes somente para "loopback";
  - named.root: que contém os endereços IP dos servidores de nomes raiz.

Named.conf (/etc/named.conf)

```
// opções default
options {
        directory "<diretório dos mapas>";
};

// cache
zone "." {
        type hint;
        file "<arquivo named.root>";
};

// loopback reverso
zone "0.0.127.in-addr.arpa" {
        type master;
        file "<arquivo named.local>";
};

// <domínio direto>
zone "<domínio direto>" {
        type master;
        file "<arquivo named.zone>";};

# <domínio reverso>
zone "<domínio reverso>.in-addr.arpa" {
        type master;
        file "<arquivo named.rev>";
};
```


Named.zone (/var/named/named.zone)

```
Formato:
$TTL            <default time-to-live positivo>
@               IN      SOA     <máquina servidora> <usuário responsável> (
                                        <série>
                                        <atualização>
                                        <timeout de atualização>
                                        <timeout de expiração>
                                        <default time-to-live negativo>
                                )
                IN      NS      <servidor de nomes>
                IN      MX      <prioridade>  <servidor de correio eletrônico>
                IN      A       <endereço IP do domínio>

<nome-1>        IN      A       <endereço IP da máquina com nome "nome-1">
                IN      HINFO   <hardware> <software>
                IN      CNAME   <apelido>

. . .
<subdom-1>      IN      NS      <nome do servidor DNS do subdominio "subdom-1">
<. . .>         IN      A       <endereço IP do servidor DNS do subdomínio>
. . .
```


Named.rev (/var/named/named.rev)

```
@               IN      SOA     <máquina servidora> <usuário responsável> (
                                        <série>
                                        <atualização>
                                        <timeout de atualização>
                                        <timeout de expiração>
                                        <default time-to-live das informações fornecidas>
                                )
                IN      NS      <servidor de nomes>

<sufixo IP>     IN      PTR     <nome de domínio totalmente qualificado>
. . .
```

Named.local (/var/named/named.local)

```
@       IN      SOA     <máquina servidora> <usuário responsável> (
                        <série>
                        <atualização>
                        <timeout de atualização>
                        <timeout de expiração>
                        <default time-to-live das informações fornecidas>
                )

        IN      NS      <servidor de nomes>

1       IN      PTR     localhost.
```

Named.root (/var/named/named.root)

```
;; servidores raiz

.                       3600000     IN  NS      A.ROOT-SERVERS.NET.
A.ROOT-SERVERS.NET.     3600000     IN  A       198.41.0.4
(...)
.                       3600000     IN  NS      M.ROOT-SERVERS.NET.
M.ROOT-SERVERS.NET.     3600000     IN  A       202.12.27.33
```


Exemplo completo

- Vamos configurar o servidor de nomes de uma rede local que vai ser ligar à Internet. Nossa rede exemplo tem as seguintes características:

Nome do domínio:	acme.com.br
Servidor:	ns.acme.com.br
Numero IP do servidor:	201.202.203.254
Servidor de correio eletrônico:	mail.acme.com.br
Responsável:	voce@acme.com.br
Máquinas do domínio:	ns (IP=201.202.203.254)
	gerente (IP=201.202.203.1)
	operador (IP=201.202.203.2)

named.conf

```
// opções default
options {
        directory "/var/named";
};

// cache
zone "." {
        type hint;
        file "named.root";
};

// loopback reverso
zone "0.0.127.in-addr.arpa" {
        type master;
        file "named.local";
};

// <domínio direto>
zone "acme.com.br" {
        type master;
        file "named.zone";
};

// <domínio reverso>
zone "203.202.201.in-addr.arpa" {
        type master;
        file "named.rev";
};
```


named.root (obtido de ftp://ftp.rs.internic.net/domain/named.root)

```
.                       3600000     IN  NS      A.ROOT-SERVERS.NET.
A.ROOT-SERVERS.NET.     3600000     IN  A       198.41.0.4

.                       3600000     IN  NS      B.ROOT-SERVERS.NET.
B.ROOT-SERVERS.NET.     3600000     IN  A       128.9.0.107

. . .

.                       3600000     IN  NS      M.ROOT-SERVERS.NET.
M.ROOT-SERVERS.NET.     3600000     IN  A       202.12.27.33
```

Observa-se que foi usado o parâmetro opcional 3600000 (1000 horas como "Time-to-live" em cada entrada, ignorando-se o Ttl "default").

named.zone

```
$TTL        2h                      ; manda os clientes confiarem nas respostas
                                    ;  positivas por 2 hs
@       IN  SOA     ns.acme.com.br.  voce.acme.com.br. (
                    2010051501  ; AAAmmDDnn, nn=01, 02, ...
                    3d          ; expira secundário em 3 dias
                    1h          ; tenta primário de hora em hora
                    7d          ; mantém-se como secundário por 7 dias, mesmo
                                ;   sem contato com o primário
                    2h          ; manda os clientes confiarem nas respostas
                                ;   negativas por  2 horas
                )

            IN  NS      ns.acme.com.br.
            IN  MX      10      mail.acme.com.br.
            IN  A       201.202.203.254

ns          IN  A       201.202.203.254
            IN  HINFO   "PC Pentium" "Linux"
mail        IN  CNAME   ns
ftp         IN  CNAME   ns
www         IN  CNAME   ns

gerente     IN  A       201.202.203.1

operador    IN  A       201.202.203.2
```


named.rev

```
@       IN  SOA     ns.acme.com.br.  voce.acme.com.br. (
                    201005151   ; AAAAmmDDn, n=1, 2, ...
                    3d          ; expira secundário em 3 dias
                    1h          ; tenta secundário de hora em hora
                    7d          ; mantem-se como secundário por 7 dias,
                                ; mesmo sem contato com o primário
                    12h         ; manda os clientes confiarem nas respostas por 12 horas
                )
            IN  NS      ns.acme.com.br.

254         IN  PTR     ns.acme.com.br.
1           IN  PTR     gerente.acme.com.br.
2           IN  PTR     operador.acme.com.br.
```

named.local

Idem named.rev, substituindo-se todas as linhas PTR por:

```
1           IN  PTR     localhost.
```

- Configurados todos os arquivos corretamente, o software servidor deve ser ativado com o comando (colocado em algum arquivo de inicialização do sistema - /etc/rc*):

```
named [-d nível] [-p porta] [-b arq-boot]

-d      nível de depuração
-p      porta de atendimento (default = 53)
-b      arquivo de inicialização (default = /etc/named.boot (conf))
```

- Todas as máquinas do domínio são clientes do servidor de nomes (inclusive o próprio servidor DNS que é cliente dele próprio);

- Configurar um cliente DNS (em ambiente UNIX) é definir no arquivo /etc/resolv.conf quem é o servidor de nomes (qual é seu endereço IP) e qual o nome de domínio padrão ("default") a ser acrescentado automaticamente no fim de um nome não totalmente qualificado.

resolv.conf

```
domainname acme.com.br

nameserver   201.202.203.254
```


Testando o serviço de nomes – NSLOOKUP

- Uma vez configurado, o serviço de nomes deve ser testado antes de ser liberado para uso (lembre-se que todos os outros serviços dependem do bom funcionamento do serviço de nomes); para testá-lo usa-se o comando *nslookup* como se pode ver nos exemplos.

```
[root@ebct]# nslookup
Default server: ns.acme.com.br
Address: 201.202.203.254

> gerente
(...)
Name: gerente.acme.com.br
Address: 201.202.203.1

> anjinho.dsc.ufpb.br
(...)
Name: anjinho.dsc.ufpb.br
Address: 150.165.75.21

> set type=mx
> dsc.ufcg.edu.br
(...)
dsc.ufcg.edu.br          preference = 10, mail exchanger = anjinho.dsc.ufcg.edu.br
anjinho.dsc.ufcg.edu.br  inet address = 150.165.75.21
> exit
[root@ebct]# _
```