

## **Aula 00**

*Sistemas Operacionais p/ TCM-SP  
(Agente de Fiscalização - TI) - VUNESP*

Autor:

**Equipe Informática e TI, Evandro  
Dalla Vecchia Pereira**

22 de Janeiro de 2020

<b>Serviço de Diretório e Serviço de Impressão em Rede.....</b>	<b>2</b>
<i>Serviço de Diretório .....</i>	<i>2</i>
<i>Serviço de Impressão em Rede (CUPS) .....</i>	<i>4</i>
<i>Questões Comentadas .....</i>	<i>7</i>
<b>DNS (Domain Name System).....</b>	<b>12</b>
<i>Questões comentadas .....</i>	<i>22</i>
<b>DHCP (Dynamic Host Configuration Protocol) .....</b>	<b>35</b>
<i>Questões comentadas .....</i>	<i>36</i>
<b>NFS e SMB/CIFS, Integração Unix x Windows.....</b>	<b>37</b>
<i>Questões Comentadas .....</i>	<i>40</i>
<b>FTP (File Transfer Protocol) .....</b>	<b>45</b>
<i>Questões Comentadas .....</i>	<i>47</i>
<b>SMTP (Simple Mail Transfer Protocol) .....</b>	<b>49</b>
<i>Questões Comentadas .....</i>	<i>51</i>
<b>NTP (Network Time Protocol) .....</b>	<b>53</b>
<i>Questões Comentadas .....</i>	<i>55</i>
<b>Lista de Questões .....</b>	<b>56</b>
<b>GABARITO .....</b>	<b>75</b>





## PROF. EVANDRO DALLA VECCHIA

Autor do livro "Perícia Digital - Da investigação à análise forense", Mestre em Ciência da Computação (UFRGS), Bacharel em Ciência da Computação (PUCRS), Técnico em Redes de Computadores (Ecom/UFRGS) e em Processamento de Dados (Urcamp). Perito Criminal na área de Perícia Digital desde 2004 no Instituto-Geral de Perícias/RS. Professor de pós-graduação em diversas instituições, nas áreas de Perícia Digital, Perícia Criminal e Auditoria de Sistemas. Lecionou na graduação de 2006 a 2017, nas instituições PUCRS, Unisinos, entre outras. Professor em cursos de formação e aperfeiçoamento de Peritos Criminais, Delegados, Inspetores, Escrivães e Policiais Militares.

Áreas de cursos ministrados pelo professor no Estratégia: Computação Forense, Arquitetura de Computadores e Sistemas Operacionais.

Entre em contato:   profevandrodallavecchia

## SERVIÇO DE DIRETÓRIO E SERVIÇO DE IMPRESSÃO EM REDE

### SERVIÇO DE DIRETÓRIO

Um serviço de diretório é um sistema de software que armazena, organiza e fornece acesso a informações em um diretório do sistema operacional. Diretórios podem ser muito limitados em escopo, suportando apenas um pequeno conjunto de tipos de nós e tipos de dados, ou eles podem ser muito amplos, suportando um conjunto de tipos arbitrário ou extensível. No DNS os nós são nomes de domínio e os itens de dados são endereços IP (e apelidos, nomes de servidor de e-mail etc.).

Em um diretório utilizado por um sistema operacional de rede, os nós representam **recursos** que são gerenciados pelo sistema operacional, incluindo usuários, computadores, impressoras, entre outros recursos compartilhados. Muitos serviços de diretório têm sido utilizados desde o aparecimento da Internet, mas o mais utilizado é um descendente do serviço de diretório X.500.

Antes de vermos uma implementação de serviço de diretório para o Linux (OpenLDAP), é importante entendermos o protocolo que fornece mecanismos de acesso aos objetos, o **LDAP (Lightweight Directory Access Protocol)**. Entidades internacionais (ITU, ISO, IETF, entre outras) trabalham na definição de padrões diversos, incluindo a padronização que dá suporte a serviços de diretórios. Um padrão de uso genérico é o **X.500** (da ISO) que possui uma grande abrangência, mas é muito



complexo e não foi adotado em sua íntegra como um padrão de mercado. Um padrão mais “light” que de fato se tornou um padrão de mercado foi o LDAP.

O padrão LDAP define um sistema de nomeação hierárquico, no qual é possível referenciar qualquer objeto que esteja no AD. Um nome LDAP é composto pelo caminho completo do objeto (ex.: uma impressora, um computador etc.), partindo do domínio raiz até chegar ao objeto em si. Algumas abreviaturas (**atributos**) são utilizadas nessa nomenclatura hierárquica:

- cn: *common name* (nome da conta de um usuário, grupo etc.);
- sn: sobrenome (*surname*);
- ou: faz referência a uma unidade organizacional;
- dc: componente de domínio (normalmente o nome do domínio);
- o: nome da organização (geralmente o domínio raiz);
- c: *country* - país (normalmente não utilizado).

Vamos a um exemplo de um nome LDAP:

CN=evandrodv, OU=professores, DC=ti, DC=estrategiaconcursos.com.br → esse nome representa o usuário “evandrodv”, cuja conta está contida na unidade organizacional “professores”, no domínio “ti.estrategiaconcursos.com.br”. Obs.: os dois componentes de domínio foram concatenados.

Por padrão um servidor LDAP “**escuta**” na porta 389 (TCP) e as principais características do protocolo são:

- Baseado em padrão aberto: qualquer desenvolvedor pode acessar sua especificação e realizar a implementação;
- Possui APIs bem definidas: facilita a vida dos programadores;
- Maior velocidade de consulta que um BD relacional;
- Replicável e distribuível;
- Facilita a localização de informações e recursos: pesquisa feita nome.

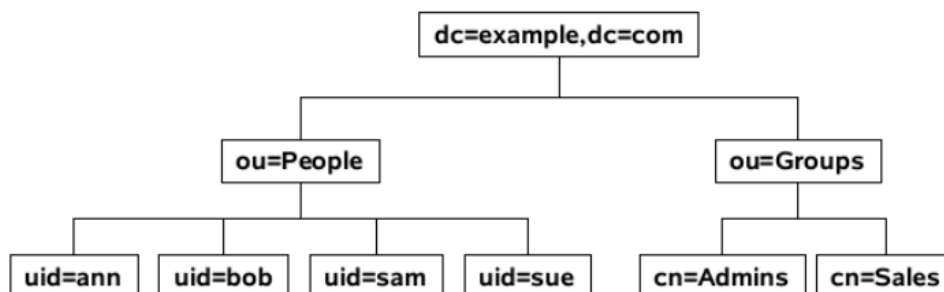
Algumas **operações (comandos)** que podem ser utilizados através do LDAP são:

- Bind: autentica e especifica a versão do protocolo LDAP;
- Search: procura/recupera entradas dos diretórios;
- Compare: compara uma entrada com determinado valor;
- Add: adiciona uma nova entrada;
- Delete: exclui uma entrada;
- Modify: modifica uma entrada;
- Modify DN: move ou renomeia uma entrada;
- Abandon: aborta uma requisição prévia;
- Unbind: fecha a conexão;
- Extended Operation: operação genérica para definir outras operações;



- StartTLS: protege a conexão com o TLS - implementada a partir da versão 3 do LDAP.

A representação dos dados é realizada através de uma estrutura hierárquica na forma de árvore (**Directory Information Tree - DIT**), a qual consiste em entradas de DN (*Distinguished Names*). O LDAP utiliza a DIT como estrutura de dados fundamental:



Como podemos ver, a árvore de diretório possui uma forma hierárquica:

- Primeiro o diretório raiz;
- Após a rede corporativa, os departamentos e por fim os computadores dos usuários e os recursos de rede.

Alguns conceitos que também já foram cobrados em concursos são mostrados na sequência.

**Schema:** conjunto de objetos e atributos para o armazenamento. É modelado de acordo com o padrão X.500 da ISO.

Cada entrada (objeto) possui um identificador único (**dn - distinguished name**), o qual consiste de seu Relative Distinguished Name (RDN), construído de algum(ns) atributo(s) na entrada, seguido pelo DN da entrada pai.

**Escalabilidade:** é possível replicar servidores LDAP e incluir novos servidores à medida que aumenta a estrutura da organização. Ou seja, não é uma estrutura “engessada”.

Como já mencionado anteriormente, uma solução bastante conhecida para Linux é o **OpenLDAP** (que também possui versões para Windows, Solaris, entre outros sistemas operacionais). Vamos ver como instalar o OpenLDAP:

```
sudo apt install slapd ldap-utils
```

O principal arquivo de configuração (pelo menos para concursos) é o “**/etc/ldap.conf**”, que é usado para configurar os padrões a serem aplicados quando da execução dos clientes LDAP.

## SERVIÇO DE IMPRESSÃO EM REDE (CUPS)

O CUPS (*Common Unix Printing System*) é um **gerenciador de impressão** para sistemas Unix-like. Seu objetivo é permitir que um computador seja um servidor de impressão no qual o gerenciador de impressão CUPS (hospedeiro) nativo no servidor receba diversas impressões dos PCs (clientes), processe-os e envie para a impressora correspondente. Além disso, também é possível **monitorar**



impressões, relatar erros de impressões, visualizar relatórios sobre quantidade de páginas impressas, data e horário.

Seu desenvolvimento se deu com o protocolo LDP, que permite que trabalhos de impressão sejam impressos através da rede utilizando TCP/IP. Com o avanço da tecnologia CUPS, o protocolo LDP foi ficando ultrapassado, lento e incompatível com padrões de alguns fabricantes. Então, o gerenciador de impressão **CUPS aderiu o IPP (*Internet Printing Protocol*)** e foi adotado pela maioria das distribuições Linux como gerenciador de impressão padrão. O CUPS é mantido pela Apple.

Para a **instalação**, deve-se seguir os procedimentos abaixo (distribuições Debian):

```
# apt-get install cups
```

Para Iniciar o serviço (start):

```
# /etc/init.d/cups start
```

Para a distribuição Slackware, opção via CD/DVD:

```
# installpkg /mnt/cdrom/slackware/a/cups-*.tgz
```

Para iniciar serviço (start):

```
# /etc/rc.d/rc.cups start
```

Para qualquer distribuição, pode-se baixar do site, descompactar o arquivo:

```
# tar -xvzf cups-xxxx-source.tar.gz
```

Configurar o CUPS:

```
# cd cups-xxxx
```

```
# ./configure
```

Compilar e instalar:

```
# make
```

```
# make install
```

Para iniciar serviço (start):

```
# /etc/rc.d/rc.cups start ou # /etc/init.d/cups start
```

Juntamente com a instalação do CUPS são necessários alguns pacotes, descritos a seguir.

Servidor Samba smbclient (para listar as impressoras compartilhadas em redes Windows/Linux):

```
# apt-get install smbclient
```

Foomatic (sistema de impressão desenhado para facilitar a instalação de impressoras comuns, ele fornece a "cola/mecanismo" entre o spooler de impressão (Cups ou lpr) e a impressora propriamente dita):

```
# apt-get install foomatic-gui foomatic-db
```



**Módulo PPD:** tem a função de criar um método, ou seja, personalizar o comportamento padrão para uma impressora específica, ex.: fontes, orientação, tamanho etc. O sistema Foomatic é o responsável pela criação desses PPDs.

**PS:** um driver de impressora colorida que trabalhe com o formato PostScript (ps).

Após o servidor CUPS ter sido configurado e as impressoras terem sido adicionadas e publicadas, o próximo passo é **configurar o cliente CUPS**, ou as máquinas que acessarão o servidor. Uma vez instalado no cliente, as impressoras compartilhadas na rede são frequentemente descobertas automaticamente pelos gerenciadores de impressão nos mais variados ambientes gráficos (GNOME, KDE, entre outros).

Também é possível acessar a **interface local CUPS na máquina cliente** através do endereço **<http://localhost:631>** (é necessário que o *daemon* cupsd esteja em execução) e clicar em “Add Printer” na seção de administração. Note que é utilizado o protocolo **TCP** (visto que HTTP utiliza o TCP como protocolo de transporte) e a porta é a **631**. Deve aparecer a opção “Device”, então deve ser escolhida a impressora de rede que foi descoberta automaticamente, ou selecionar o protocolo IPP ou o HTTP, e digitar o endereço da impressora, geralmente, em uma dessas duas sintaxes:

`ipp://nome-servidor-ou-ip/printers/nome-impressora`

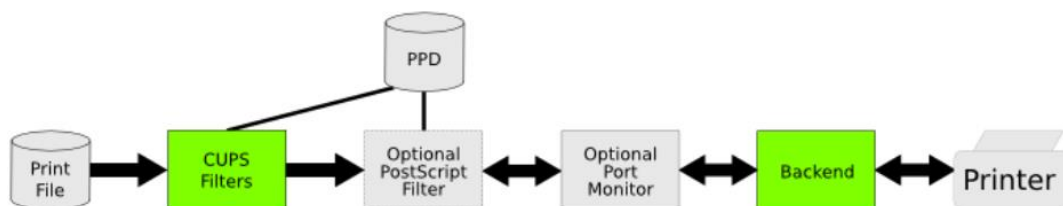
`http://nome-servidor-ou-ip:631/printers/nome-impressora`

Se houver dificuldade com o cliente CUPS para encontrar outras impressoras CUPS compartilhadas na rede, pode ser útil adicionar ou criar um arquivo `/usr/local/etc/cups/client.conf` com uma entrada única:

`ServerName ip-do-servidor`

As configurações são salvas no arquivo **`/etc/cups/ppd`**.

O CUPS possui filtros para muitos formatos comuns, por exemplo, para conversão de PDF em formatos independentes ou dependentes de PostScript:





## QUESTÕES COMENTADAS

### 1. (2010 - CESPE - SERPRO)

O CUPS tem a característica de ser plug-and-play no lado cliente; portanto, basta configurar o servidor e instalar o CUPS nos clientes.

#### Comentários:

Após o servidor CUPS ter sido configurado e as impressoras terem sido adicionadas e publicadas, o próximo passo é configurar o cliente CUPS, ou as máquinas que acessarão o servidor. Uma vez instalado no cliente, as impressoras compartilhadas na rede são frequentemente **descobertas automaticamente** pelos gerenciadores de impressão nos mais variados ambientes gráficos (GNOME, KDE, entre outros).

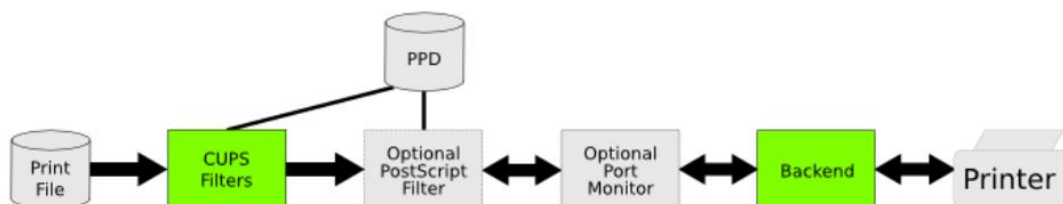
**Gabarito: Certo**

### 2. (2010 - CESPE - SERPRO)

O CUPS é um sistema de impressão compatível com o protocolo IPP (Internet printing protocol) que suporta impressoras não PS (PostScript), porém não suporta impressoras PS.

#### Comentários:

O CUPS possui filtros para muitos formatos comuns, por exemplo, para conversão de PDF em formatos independentes ou dependentes de PostScript:



A questão está errada quando afirma que “não suporta impressoras PS).

**Gabarito: Errado**

### 3. (2011 - CESPE - MEC)

No caso do CUPS, recomenda-se utilizar o endereço de loopback do servidor para tarefas de administração, a fim de evitar a transmissão da senha de root em texto claro com o protocolo HTTP.

#### Comentários:

Como o HTTP não é seguro (sem criptografia), é recomendado que se utilize o loopback (na própria máquina). Assim não há tráfego pela rede e ninguém pode interceptar o tráfego e analisar as informações. Deve-se utilizar na máquina onde está o CUPS (porta 631):

<http://localhost:631>





**Gabarito: Certo**

---

**4. (2011 - CESPE - MEC)**

Considerando que, em um ambiente de rede, exista um servidor de impressão em Windows Server 2003 e outro servidor de impressão em Linux que utilize o sistema CUPS, julgue os itens subsequentes.

O CUPS anuncia seu serviço de impressão por meio de broadcast e usa por padrão a porta UDP 300. Nesse caso, a configuração padrão do CUPS pode ser alterada para uso apenas de multicast.

**Comentários:**

Uma vez instalado no cliente, as impressoras compartilhadas na rede são frequentemente descobertas automaticamente pelos gerenciadores de impressão nos mais variados ambientes gráficos (GNOME, KDE, entre outros). Não tem nada de porta 300 (UDP) etc. e tal!

**Gabarito: Errado**

---

**5. (2013 - CESPE - SERPRO)**

Mecanismos do CUPS possibilitam o compartilhamento de arquivos entre o Windows e o Linux.

**Comentários:**

CUPS só trata de impressão! Se quiser compartilhar arquivos e impressoras num “pacote” só, deve-se utilizar o SAMBA.

**Gabarito: Errado**

---

**6. (2014 - IADES - EBSERH)**

O CUPS é o sistema de impressão usado atualmente na maioria dos sistemas Linux. A adição de novas impressoras pode ser feita através da sua interface web, que em sua configuração padrão, armazena as informações das impressoras na pasta

- A) /etc/printers
- B) /etc/cups/printers
- C) /etc/cups/ppd
- D) /dev/prn
- E) /dev/interfaces/printers

**Comentários:**



É possível acessar a **interface local CUPS na máquina cliente** através do endereço **http://localhost:631**, e clicar em “Add Printer” na seção de administração. Note que é utilizado o protocolo **TCP** (visto que HTTP utiliza o TCP como protocolo de transporte) e a porta é a **631**. Deve aparecer a opção “Device”, então deve ser escolhida a impressora de rede que foi descoberta automaticamente, ou selecionar o protocolo IPP ou o HTTP, e digitar o endereço da impressora, geralmente, em uma dessas duas sintaxes:

ipp://nome-servidor-ou-ip/printers/nome-impressora

http://nome-servidor-ou-ip:631/printers/nome-impressora

As configurações são salvas no arquivo **/etc/cups/ppd**.

**Gabarito: C**

---

### 7. (2014 - VUNESP - PRODEST-ES)

Nos sistemas operacionais Linux, o CUPS é um serviço responsável pelo gerenciamento de

- A) arquivos compartilhados.
- B) trabalhos de impressão.
- C) mensagens de fax.
- D) mensagens eletrônicas (e-mail).
- E) usuários da rede.

**Comentários:**

Essa ficou fácil, heim? A única que poderia atrapalhar seria a alternativa A, mas quem compartilha arquivos é o SAMBA (além de compartilhar impressoras também). O CUPS compartilha apenas impressoras!

**Gabarito: B**

---

### 8. (2016 - UFV - UFV-MG)

O administrador do setor de Tecnologia da Informação precisa compartilhar as impressoras da empresa para que os funcionários possam imprimir seus trabalhos. Para isso, ele tem que montar um servidor de impressão com Sistema Operacional Linux.

São serviços do Sistema Operacional Linux que permitem o compartilhamento de impressoras:

- A) CUPS, SAMBA
- B) SAMBA, APACHE
- C) APACHE, FTP



D) FTP, CUPS

**Comentários:**

Como já vimos em algumas questões anteriores:

CUPS: serviço de impressão.

SAMBA: serviço arquivos e de impressão.

**Gabarito: A**

---

**9. (2017 - IBFC - EBSERH)**

Assinale a alternativa correta. Para permitir que um computador seja um servidor de impressão em um ambiente Unix-like de forma que se possa monitorar impressões, relatar erros de impressão, visualizar relatórios sobre número de páginas impressas, etc. usa-se:

A) PGREP

B) CUPS

C) CHROOT

D) CRON

E) PRINTF

**Comentários:**

O CUPS (*Common Unix Printing System*) é um **gerenciador de impressão** para sistemas Unix-like. Seu objetivo é permitir que um computador seja um servidor de impressão no qual o gerenciador de impressão CUPS (hospedeiro) nativo no servidor receba diversas impressões dos PCs (clientes), processe-os e envie para a impressora correspondente. Além disso, também é possível **monitorar impressões, relatar erros de impressões, visualizar relatórios sobre quantidade de páginas impressas, data e horário**.

**Gabarito: B**

---

**10.(2018 - CESPE - EBSERH)**

CUPS é uma solução para conectar impressoras ao sistema roteador da rede de computadores, a fim de disponibilizar o equipamento para a sua utilização via protocolo NETBIAS.

**Comentários:**

Não tem nada de roteador, muito menos o protocolo NETBIOS (que está escrito errado), que é utilizado no Windows!

**Gabarito: Errado**



### 11.(2018 - UFU-MG - UFU-MG)

No Linux, podem-se utilizar impressoras diretamente conectadas ao desktop, por exemplo, por meio de uma porta USB ou impressoras disponíveis na rede e configurá-las com o CUPS (Common UNIX Printing System).

Com base no CUPS, assinale a alternativa correta.

A) O arquivo regular de configuração do CUPS armazenado no “home” do usuário, por exemplo, “/home/usuario/.cups.configuracao”, contempla todas as informações de permissões e de autenticações, servidor de impressão e opções de impressoras configuradas.

B) No CUPS, ao se configurar uma impressora, essa será sempre disponibilizada a partir de nomes transmitidos na rede. Trata-se de um recurso no qual não é permitido ao usuário esconder de outros usuários uma impressora na rede.

C) Pode-se configurar o CUPS no navegador por meio da interface “http://localhost:631” desde que o “daemon” CUPS de impressão ou “cupsd” esteja em execução.

D) Para adicionar uma impressora local a partir da linha de comando independentemente do perfil do usuário, por exemplo, usuário comum, basta executar na linha de comando “config-printer” e, após a janela ser aberta, selecionar “New Printer”.

#### Comentários:

É possível acessar a **interface local CUPS na máquina cliente** através do endereço **http://localhost:631** (é necessário que o *daemon* cupsd esteja em execução) e clicar em “Add Printer” na seção de administração. Note que é utilizado o protocolo **TCP** (visto que HTTP utiliza o TCP como protocolo de transporte) e a porta é a **631**. Deve aparecer a opção “Device”, então deve ser escolhida a impressora de rede que foi descoberta automaticamente, ou selecionar o protocolo IPP ou o HTTP, e digitar o endereço da impressora, geralmente, em uma dessas duas sintaxes:

ipp://nome-servidor-ou-ip/printers/nome-impressora

http://nome-servidor-ou-ip:631/printers/nome-impressora

#### Gabarito: C

### 12.(2019 - FCC - Prefeitura de Manaus-AM)

Em computador com sistema operacional Linux e o OpenLDAP instalado, o programador editou o arquivo ldap.conf para configurar

A) a autenticação do servidor.

B) a execução do serviço do LDAP.

C) o banco de dados a ser utilizado.



D) a geração de índices do banco de dados.

E) o acesso dos clientes ao diretório.

### Comentários:

O principal arquivo de configuração (pelo menos para concursos) é o “/etc/ldap.conf”, que é usado para configurar os **padrões a serem aplicados quando da execução dos clientes LDAP**.

**Gabarito: E**

## DNS (DOMAIN NAME SYSTEM)

Os equipamentos conectados à Internet necessitam de um endereço IP e através dele conseguimos identificar “quem” acessou determinado conteúdo ou realizou determinada ação, por exemplo. Mas, quem “gosta” de números é a máquina! Nós, meros mortais, temos dificuldade em memorizar muitos números (endereços IP, por exemplo). E os servidores (Web, de e-mail, de arquivos, etc.) são acessados através do endereço IP que foi alocado a eles.

Uma solução para isso foi a criação de um serviço que “faz o meio de campo”, ou seja, traduz nomes (bem mais fáceis de memorizar) para os endereços IP equivalentes. É o famoso *Domain Name System* (DNS). Assim, é possível acessar uma página Web através de um nome, sendo que de forma transparente ao usuário, esse nome é traduzido ao endereço IP onde se encontra o servidor Web que contém a página e a requisição é realizada a esse servidor.

Um conceito mais formal (Tanenbaum) é o seguinte: o DNS é definido como um esquema hierárquico de atribuição de nomes baseado no domínio e de um sistema de banco de dados distribuído. O DNS atua na camada de aplicação e utiliza como protocolo de transporte o UDP para as consultas/respostas e o TCP para transferências de zonas (entre servidores DNS). Tanto com o UDP como com o TCP, a porta utilizada é a 53.

Abaixo é mostrada uma tela com a resposta para o comando *ipconfig /all* (no Linux o comando equivalente é o *ifconfig*) mostrando, entre outras informações, os servidores DNS locais.

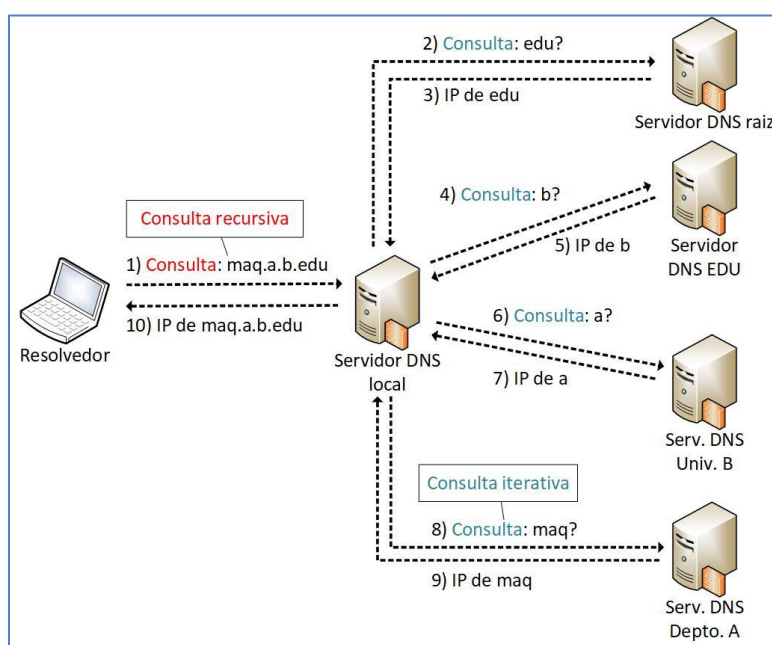
```
C:\Windows\system32\cmd.exe
Endereço IPv6 Temporário. . . . . : 2804:14d:4c84:98a6:8978:46d7:e683:2535(Preferencial)
Endereço IPv6 de link local . . . . : fe80::902b:69bc:849e:fc88%2(Preferencial)
Endereço IPv4. . . . . : 192.168.0.10(Preferencial)
Máscara de Sub-rede . . . . . : 255.255.255.0
Concessão Obtida. . . . . : sábado, 31 de março de 2018 22:24:53
Concessão Expira. . . . . : sexta-feira, 6 de abril de 2018 02:40:35
Gateway Padrão. . . . . : fe80::b62a:eff:fe18:9e81%2
                          192.168.0.1
Servidor DHCP . . . . . : 192.168.0.1
IAID de DHCPv6. . . . . : 41965298
DUID de Cliente DHCPv6. . . . . : 00-01-00-01-22-38-ED-BE-A4-1F-72-F5-AF-AD
Servidores DNS. . . . . : 2804:14d:4c10:672:201:21:192:122
                          2804:14d:4c10:672:201:21:192:168
                          201.21.192.167
                          201.21.192.162
NetBIOS em Tcpip. . . . . : Habilitado
```



Um passo a passo de uma solicitação de um cliente DNS (seu computador, por exemplo) a um servidor DNS local é mostrado a seguir.

- 1) O aplicativo (ex.: navegador) chama o **resolvedor**, passando o nome que se deseja a tradução para endereço IP;
- 2) O resolvedor realiza uma consulta ao servidor DNS local;
- 3) O servidor DNS local responde ao resolvedor;
- 4) O resolvedor informa o endereço IP ao aplicativo.

Ok, mas e se for um nome que o servidor DNS local não conhece? Seja porque nunca foi solicitado, ou porque tal informação já não se encontra mais em sua *cache*? Bom, aí é melhor olhar a figura abaixo.



A consulta realizada ao servidor DNS local é chamada **consulta recursiva**, pois o resolvedor envia a consulta e recebe a resposta final, sem precisar enviar uma consulta a cada servidor DNS de nível superior. Já em **consultas iterativas**, a resposta à requisição DNS pode ser parcial, obrigando o solicitante a encaminhar novas requisições DNS a outros servidores até obter a resposta final desejada.

A delegação de domínios de mais alto nível (*top-level domain* - TLD), tais como “.com”, “.edu”, “.br”, “.mx”, entre outros, é de responsabilidade da ICANN (*Internet Corporation for Assigned Names and Numbers*). Para o Brasil (TLD .br), o responsável é o CGI.br<sup>1</sup>, conforme podemos ver abaixo.

<sup>1</sup> Base de dados de domínios TLD disponível em <<http://www.iana.org/domains/root/db>>.



.booking	generic	Booking.com B.V.
.boots	generic	THE BOOTS COMPANY PLC
.bosch	generic	Robert Bosch GMBH
.bostik	generic	Bostik SA
.boston	generic	Boston TLD Management, LLC
.bot	generic	Amazon Registry Services, Inc.
.boutique	generic	Binky Moon, LLC
.box	generic	NS1 Limited
.bq	country-code	Not assigned
.br	country-code	Comite Gestor da Internet no Brasil
.bradesco	generic	Banco Bradesco S.A.
.bridgestone	generic	Bridgestone Corporation
.broadway	generic	Celebrate Broadway, Inc.
.broker	generic	DOTBROKER REGISTRY LTD



#### CURIOSIDADE

Note que existe um TLD “.bradesco”, relacionado ao Banco Bradesco. Faça um teste em seu navegador: digite “bradesco.com.br” e “bradesco.bradesco”. Qual o resultado? No momento em que testei, ambos direcionam para uma nova URL: “https://banco.bradesco/html/classic/index.shtm”, pertencente ao domínio “.bradesco”.

Então, se alguém quiser registrar um domínio com o sufixo “.br”, pode verificar se há disponibilidade desse domínio, através da URL <http://registro.br>. Se houver, pode realizar a solicitação, efetuar o pagamento e informar as configurações solicitadas pelo CGI.br sobre o provedor onde a página será hospedada (servidores DNS).

Na medida em que novos domínios são cadastrados, eles são propagados pela Internet e em poucas horas todos os servidores DNS do mundo são capazes de traduzir o domínio para o endereço IP equivalente onde está hospedado o serviço. A figura abaixo mostra a estrutura DNS, desde a raiz, os TLDs, domínios de segundo e terceiro níveis e o computador lá na ponta.





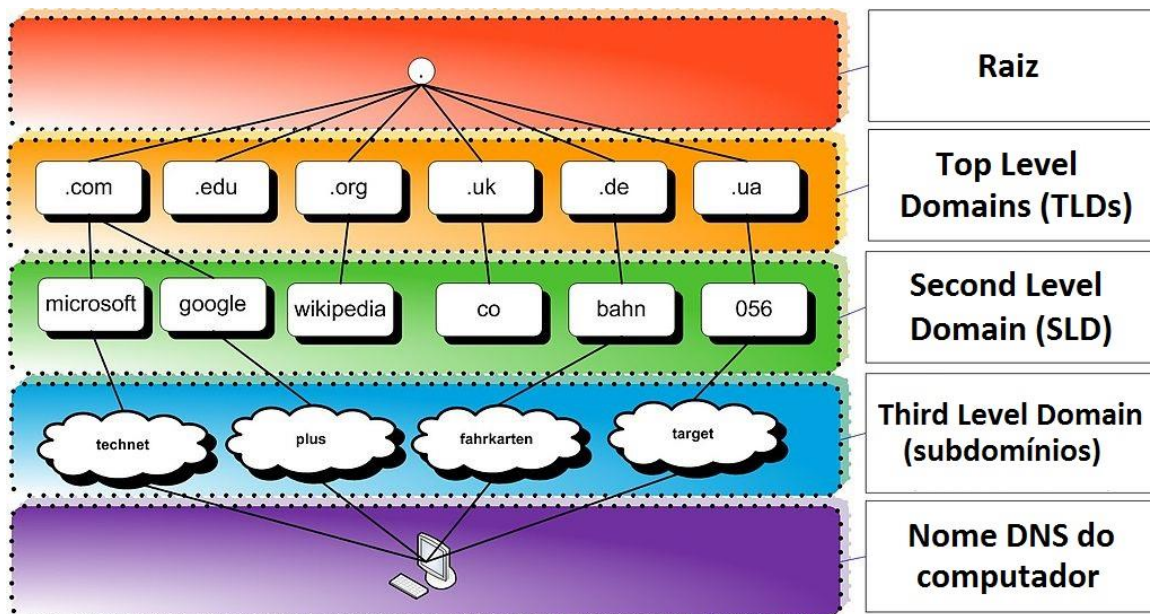
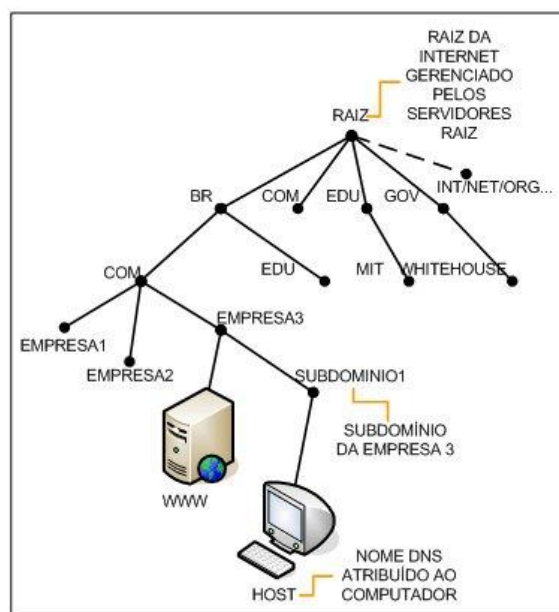


Figura adaptada de <https://hugoemiliano.info/2017/07/05/servicos-e-protocolos-dns/>

Por exemplo, a URL <www.microsoft.com> pode ser compreendida da seguinte forma:

- .com: Top Level Domain (TLD);
- microsoft: Second Level Domain (SLD);
- **não há terceiro nível (subdomínio) para essa URL;**
- www: Nome do computador ("www" é um nome padrão para servidores Web).

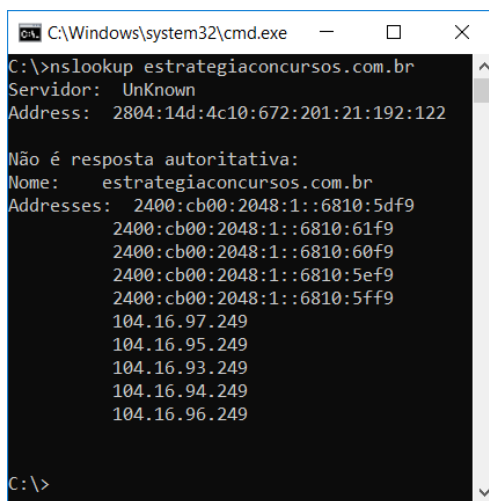
Abaixo uma outra figura, mostrando um exemplo com subdomínio. Nesse caso a URL completa para acessar o "HOST" seria <HOST.SUBDOMINIO1.EMPRESA3.COM.BR>.



Fonte: [http://www.abusar.org/dns\\_como.html](http://www.abusar.org/dns_como.html)

Para não haver consultas constantes a servidores DNS de mais alto nível (mais próximos da raiz, ou a própria raiz), os servidores DNS possuem uma memória cache<sup>2</sup>, permitindo a resposta imediata ao solicitante (quando tiver a informação). Quando não tiver a informação, deve-se buscar nos níveis superiores.

É possível também, em sistemas operacionais como Windows e Linux, configurar em traduções fixas, de domínio para endereço IP (arquivo hosts, como já vimos). Uma ferramenta comum ao Windows e Linux para obter informações sobre registros de DNS de um determinado domínio, host ou IP é o *nslookup* (vale a pena utilizá-la, pois há questões que cobram o seu conhecimento):



```
C:\Windows\system32\cmd.exe
C:\>nslookup estrategiaconcursos.com.br
Servidor:  UnKnown
Address:  2804:14d:4c10:672:201:21:192:122

Não é resposta autoritativa:
Nome:      estrategiaconcursos.com.br
Addresses: 2400:cb00:2048:1::6810:5df9
          2400:cb00:2048:1::6810:61f9
          2400:cb00:2048:1::6810:60f9
          2400:cb00:2048:1::6810:5ef9
          2400:cb00:2048:1::6810:5ff9
          104.16.97.249
          104.16.95.249
          104.16.93.249
          104.16.94.249
          104.16.96.249

C:\>
```

Em relação ao padrão Unix, o servidor de nomes mais conhecido é o BIND, que é conjunto de softwares DNS, que contém um *daemon* servidor de nomes (*named*), uma biblioteca *resolver* (nosso “resolvedor”) e outros programas. O Bind é mantido pela ISC (*Internet Software Consortium* - <<https://www.isc.org/downloads/bind/>>).

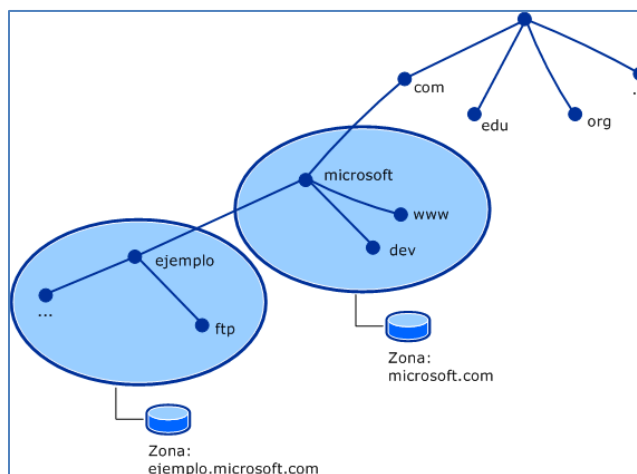
O arquivo de configuração para o resolvedor é o **resolv.conf** e fica localizado em /etc. Trata-se de um arquivo em texto plano usualmente criado pelo administrador ou por aplicações que gerenciam tarefas de configuração.

O espaço de nomes do DNS é dividido em zonas não superpostas. Cada zona está associada a um ou mais servidores de nomes, que mantêm o banco de dados para a zona. A figura abaixo mostra tal conceito:

---

<sup>2</sup> Responsável por armazenar consultas recentes, respondendo ao solicitante diretamente.





Fonte: <http://un-newbie.blogspot.com.br/2014/03/introduccion-transferencia-de-zona-y.html>

Os **registros de recursos (RRs)** são o banco de dados do DNS. São compostos por tuplas de cinco campos: <nome\_domínio, tempo\_vida, classe, tipo, valor>, descritos abaixo:

- Nome: chave de pesquisa primária para atender as consultas;
- Tempo\_vida (TTL): tempo que deve permanecer em *cache* (em segundos);
- Classe: geralmente IN (Internet);
- Tipo: SOA, A, AAAA, etc. (tabela a seguir);
- Valor: número, nome de domínio ou *string* ASCII.

Tipo	Significado	Valor
SOA	Início de autoridade ( <i>Start of Authority</i> ).	Parâmetros para essa zona.
A	Endereço IPv4.	Inteiro de 32 bits.
AAAA	Endereço IPv6.	Inteiro de 128 bits.
MX	Troca de mensagens de e-mail.	Prioridade, domínio disposto a aceitar e-mails.
NS	Servidor de nomes.	Nome de um servidor para este domínio.
CNAME	Nome canônico ( <i>alias</i> = apelido).	Nome de domínio.
PTR	Ponteiro (usado para o DNS reverso <sup>3</sup> )	Nome alternativo de um end. IP.

<sup>3</sup> Envia um endereço IP como consulta e recebe o nome como resposta.



SPF	Estrutura de política do transmissor.	Codificação de texto da política de envio de mensagens de e-mail.
SRV	Identifica computadores que hospedam serviços específicos.	Host que o oferece.
TXT	Informações sobre um servidor, rede, <i>datacenter</i> , etc.	Texto ASCII com descrições.

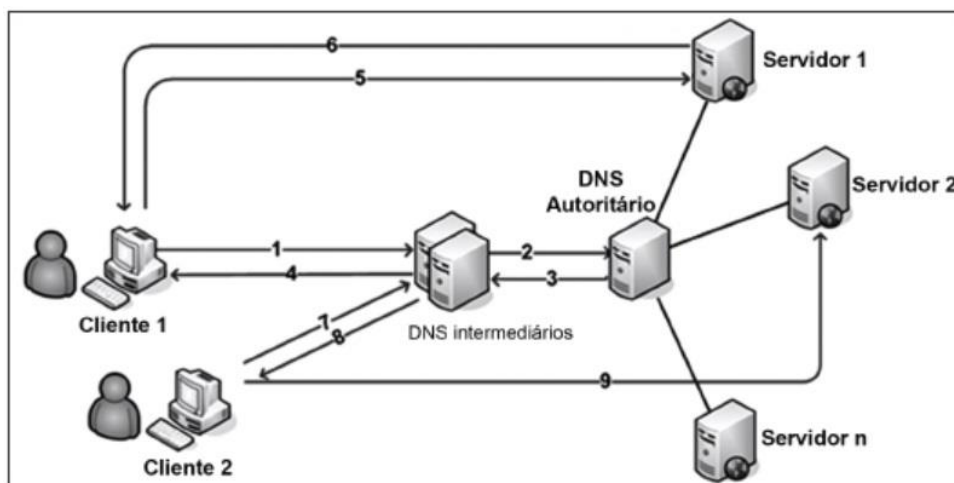
Outro conceito cobrado em provas de concurso é a resposta autoritativa ou não-autoritativa. Vejamos suas definições:

Um servidor DNS autoritativo possui autoridade sobre um nome de domínio. O DNS autoritativo dita qual será o apontamento da tabela de DNS do seu sítio. Uma **resposta autoritativa**<sup>4</sup> de um servidor é a garantia de estar atualizada, enquanto uma **resposta não-autoritativa** pode estar desatualizada (*cache* com informações antigas, por exemplo). Existe um percentual elevado de respostas não autoritativas que estão perfeitamente corretas, casos em que mudanças de endereçamento são raros.

Servidores primários e secundários são autoritativos para os seus domínios, porém não o são sobre informações a respeito de outros domínios mantidas em *cache*. **Servidores caching-only nunca são autoritativos**, mas possuem a vantagem de reduzir a quantidade de tráfego DNS na rede.

Uma política que pode ser adotada para equilibrar as vantagens de cada técnica é colocar um servidor secundário ou *caching-only* em cada segmento de rede ou sub-rede. É admissível uma máquina ser servidora primária para um domínio e servidora secundária para outros domínios.

Para não sobrecarregar servidores, existe uma abordagem popular e simples: o **balanceamento de carga por DNS**. Considere a figura abaixo e o passo a passo mostrado na sequência.



Fonte: Prova FCC – 2016 – ELETROSUL – Profissional de Nível Superior/Informática

1. Cliente 1 tenta acessar o *site*, é realizada uma pesquisa no DNS local para determinar qual é o endereço IP correspondente;
2. O pedido de endereço chega ao servidor de DNS autoritário do domínio;
3. A primeira vez que esta consulta é feita, o servidor DNS remoto pode retornar todos os registros de endereços que ele tem para o site;
4. O servidor DNS local, em seguida, determina o endereço de registro para retornar ao cliente;
5. Se todos os registros são retornados, o cliente utilizará o primeiro que lhe é atribuído;
6. O servidor responde ao cliente e atende ao pedido;
7. A cada pedido, o algoritmo Round Robin roda os endereços e retorna pela ordem em que eles estão;
8. Cada consulta DNS irá resultar em um cliente usando um endereço diferente;
9. Esta rotação de endereços irá distribuir pedidos para os servidores.

No **Linux** o servidor DNS mais utilizado e cobrado em concursos é o BIND (*Berkeley Internet Name Domain*), que se encontra na versão 9 (por isso o nome do pacote é bind9). Para instalar o bind9 e ferramentas relacionadas pode-se utilizar o gerenciador de pacotes APT (ou o apt-get), da seguinte forma:

```
$ sudo apt-get install bind9 bind9utils bind9-doc dnsutils
```

É importante saber quais são e para que servem os arquivos de configuração. Um dos mais cobrados em concursos é o **/etc/resolv.conf**, que identifica os locais dos computadores de servidor DNS. Nesse arquivo deve ser indicado o nome de domínio DNS da rede, e qual o servidor DNS irá resolver as consultas de nomes. Um exemplo é mostrado a seguir.

```
domain ti.teste.com.br  
search ti.teste.com.br teste.com.br  
nameserver 192.168.1.1  
nameserver 192.168.2.1
```

Cada parâmetro é colocado em uma linha. As três palavras-chave normalmente usadas são:

- *domain*: especifica o nome do domínio local;
- *search*: lista de pesquisa para a procura do nome de servidor, normalmente determinado pelo domínio do servidor local;
- *nameserver*: Endereço IP do servidor de nomes que o resolvedor deve pesquisar, utilizados na ordem em que estão listados;

O arquivo resolv.conf também serve para especificar o tipo (nível) de serviço a ser executado pelo software, a saber:

- *resolver-only system*: não requer que o sistema local tenha um servidor DNS em execução, requer apenas o resolver;



- *caching-only server*: servidor que não possui uma cópia da tabela de zonas, ou seja é não-autoritativo, possuindo uma grande quantidade de registros em cache;;
- *primary server (master server)*: onde todas atualizações manuais devem ser realizadas, é autoritativo;
- *secondary server*: busca informações de zona em um *master server*, é autoritativo.

O principal arquivo de configuração do Bind é o `/etc/bind/named.conf` (em versões antigas: `/etc/named.conf`). Por padrão o Bind já vem configurado para trabalhar como um servidor DNS de *cache*, que pode ser usado tanto localmente quanto por outros dispositivos da rede local. Dentro do arquivo de configuração é possível encontrar entradas tais como:

```
zone "." {  
    type hint;  
    file "/etc/bind/db.root";  
};  
  
zone "localhost" {  
    type master;  
    file "/etc/bind/db.local";  
};  
  
zone "127.in-addr.arpa" {  
    type master;  
    file "/etc/bind/db.127";  
};  
  
zone "0.in-addr.arpa" {  
    type master;  
    file "/etc/bind/db.0";  
};  
  
zone "255.in-addr.arpa" {  
    type master;  
    file "/etc/bind/db.255";  
};
```

Pode-se ver que cada uma das seções indica a localização de um arquivo, onde vai a configuração referente a ela. Por exemplo, na primeira seção ("zone ".") é indicado o arquivo `/etc/bind/db.root`, que contém os endereços dos 14 root servers, que o Bind contactará na hora de resolver os domínios.

Esta configuração vem incluída por padrão e não deve ser alterada, a menos que seja um usuário experiente. Ao configurar o servidor DNS algumas novas zonas são incluídas (novas seções de configuração), contendo os domínios que se deseja configurar.

O serviço referente ao Bind pode se chamar "bind" ou "named", de acordo com a distribuição. Nos derivados do Debian o controle do serviço é realizado através do comando `/etc/init.d/bind9` (ou `/etc/init.d/bind` para a versão 8), enquanto nas distribuições derivadas do Red Hat utiliza-se o comando `service named`:





```
# /etc/init.d/bind9 restart  
  
ou  
  
# service named restartc
```

Servidores DNS públicos (*forwarders*), como por exemplo o Google Public DNS, podem ser configurados no arquivo **named.conf.options**. Nesse arquivo também pode ser definida a lista de controle de acessos (ACL). Um exemplo é mostrado abaixo.

<pre>options {     directory "/var/cache/bind";     // Troca a porta entre servidores DNS     query-source address * port *;     forward only;     forwarders { 192.168.1.1; };     auth-nxdomain no;     interface-interval 0;     // Escuta apenas em interfaces locais     listen-on-v6 { none; };     listen-on { 127.0.0.1; 192.168.0.1; }; }</pre>	<pre>// Não transfere info de zona a DNS secundário allow-transfer { none; };  allow-query { internals; };  allow-recursion { internals; };  // Não torna versão pública do BIND version none; };</pre>
--	---

Para finalizar é importante destacar um arquivo útil para máquinas que são acessadas frequentemente: o **/etc/hosts**. A inclusão de um computador nesse arquivo dispensa a consulta a um servidor DNS para obter um endereço IP. Ou seja, a tradução ocorre automaticamente ao ler tal arquivo, sem ter que consultar o serviço de DNS. Um exemplo é mostrado abaixo.

# Aqui são colocados comentários		
# End. IP	Nome do host	Alias (opcional)
127.0.0.1	localhost	localmente
192.168.0.1	www.teste.com.br	teste





## QUESTÕES COMENTADAS

### 13.(CESPE – 2018 – Polícia Federal – Perito Criminal Federal - Área 3)

Julgue o item que se segue, a respeito de DNS (domain name service).

As atualizações entre servidores DNS utilizam o UDP, enquanto as consultas feitas a servidores DNS utilizam o TCP (ou, opcionalmente, o SCTP).

**Comentário:** Mesmo que você não lembre do que vimos em aula, vamos tentar utilizar a lógica: o UDP é bem mais leve, então deve ser utilizado em consultas DNS, pois tais consultas ocorrem em grande número na Internet e se alguma mensagem for perdida não há grandes problemas, bastando realizar uma nova consulta. As atualizações entre servidores DNS são bem menos frequentes que as consultas e é importante que mensagens não sejam perdidas pela rede, logo, é interessante que se utilize TCP, correto? Bom, essa lógica é a utilizada no DNS! E, como podemos ver, a questão inverteu o TCP com o UDP.

**Gabarito: Errado**

### 14. (2018 - IF-RS - IF-RS - Técnico de Laboratório - Informática)

Considerando que se está logado como "root" no terminal de uma estação de trabalho com um sistema operacional Linux debian ou derivado, qual comando configura o DNS para 8.8.8.8?

- A) dns 8.8.8.8
- B) echo 8.8.8.8 > /etc/hosts.conf
- C) echo nameserver 8.8.8.8 > /etc/resolv.conf
- D) nslookup 8.8.8.8
- E) nameserver 8.8.8.8

**Comentário:** *nameserver*: Endereço IP do servidor de nomes que o resolvidor deve pesquisar, utilizados na ordem em que estão listados. Tal diretiva deve estar no arquivo /etc/resolv.conf, então com o comando echo é possível escrever "nameserver 8.8.8.8" em "/etc/resolv.conf" sem ter que abrir o arquivo.

**Gabarito: C**

### 15.(FAURGS – 2018 – BANRISUL – Suporte a Infraestrutura de TI)

Um cliente DNS, ao fazer a requisição DNS para resolver o nome www.banrisul.com.br, recebe como resposta uma mensagem do tipo non authoritative. Esse tipo de resposta é obtido por meio de um registro DNS (resource record – RR) armazenado

- A) em um cache de DNS.
- B) em um servidor interativo sem cache DNS.



- C) em um servidor recursivo sem cache DNS.
- D) no arquivo de zona do DNS primário.
- E) no arquivo de zona do DNS secundário.

**Comentário:** Um servidor DNS autoritativo possui autoridade sobre um nome de domínio. O DNS autoritativo dita qual será o apontamento da tabela de DNS do seu sítio. Uma resposta autoritativa de um servidor é a garantia de estar atualizada, enquanto uma resposta não-autoritativa pode estar desatualizada (cache com informações antigas, por exemplo). Existe um percentual elevado de respostas não autoritativas que estão perfeitamente corretas, casos em que mudanças de endereçamento são raros.

Servidores primários e secundários são autoritativos para os seus domínios, porém não o são sobre informações a respeito de outros domínios mantidas em cache. Servidores caching-only nunca são autoritativos, mas possuem a vantagem de reduzir a quantidade de tráfego DNS na rede..

**Gabarito: A**

---

### 16. (2018 - FAPEC - UFMS - Técnico de Tecnologia da Informação)

Considere as afirmações a seguir sobre a instalação e configuração de um servidor de DNS (Bind9) no sistema operacional Debian 9.

I - Quando o servidor local de DNS não consegue traduzir o nome, ele deve solicitar a um servidor público (forwarders). O Google Public DNS é um exemplo de forwarders e deve ser configurado no arquivo `named.conf.options`.

II - A instalação do servidor pode ser realizada pelo usuário root com o comando: `apt install bind9 bind9-doc dnsutils`

III - A lista de controle de acessos ou ACL é definida no arquivo `named.conf.options`.

Está(ão) correta(s):

- A) Apenas I.
- B) Apenas II.
- C) Apenas III.
- D) Apenas II e III.
- E) I, II e III.

**Comentário:** Todas as afirmativas foram abordadas no decorrer da aula.

**Gabarito: E**

---

### 17.(2018 - CESPE - EMAP - Analista Portuário - Tecnologia da Informação)

Acerca de sistemas operacionais Linux, julgue o item que segue.



Em um servidor DNS que esteja utilizando Bind, o arquivo `/etc/named.conf` mantém as configurações de funcionamento do serviço DNS. Nesse servidor, é possível configurar a porta que deve escutar o serviço; assim, para que o serviço escute a porta 53, deve-se configurar a opção seguinte.

Listening 53 { any;};

**Comentário:** No arquivo `named.conf` são configuradas informações de zonas. O próprio nome do arquivo já sugere isso (`named` = nomes de domínios). Não há a configuração da porta em que o serviço deve “escutar” nesse arquivo!

**Gabarito: Errado**

---

### 18.(IBFC – 2017 – Polícia Científica-PR – Perito Oficial/Perito Criminal/Área 1)

Servidores de DNS (Domain Name System) têm como função converter endereços IP em seu respectivo nome e vice-versa. Para sua configuração, são utilizados arquivos denominados mapas de domínio (`zonE`). Esses arquivos são compostos por entradas chamadas RR (`Resource RecorD`). O tipo básico de RR que estabelece a correspondência entre um nome canônico e um endereço IP é indicado por:

- A) PTR
- B) MX
- C) NS
- D) A
- E) SOA

**Comentário:** Quando é realizada uma consulta pelo nome, esperando como resposta um endereço IP, os RRs possíveis são:

A	Endereço IPv4.	Inteiro de 32 bits.
AAAA	Endereço IPv6.	Inteiro de 128 bits.

Como a questão não mostra “AAAA” como alternativa, sobrou apenas o “A”, que retorna um endereço IPv4.

**Gabarito: D**

---

### 19. (IBFC – 2017 – Polícia Científica-PR – Perito Oficial/Perito Criminal/Área 1)

Servidores DNS (Domain Name Server) são responsáveis pela conversão do nome dos diversos servidores espalhados pela Internet para seu número IP e vice-versa. Servidores de DNS trabalham de forma colaborativa e hierárquica. Assinale a alternativa a que apresenta o nome dado aos servidores que se encontram no topo da hierarquia de DNS:



- A) Root Name Servers
- B) Main servers
- C) International Name Servers
- D) Controllers Servers
- E) Master Servers

**Comentário:** A hierarquia DNS é uma árvore invertida, ou seja, os servidores raiz (Root Name Servers) ficam no topo, logo abaixo ficam os TLDs (Top Level Domains), depois os de segundo nível e assim por diante.

**Gabarito: A**

---

### 20. (FGV – 2016 – COMPESA – Analista de Saneamento/Engenheiro de Telecomunicações)

O sistema de Nomes de Domínio – DNS permite transformar nomes digitados em um navegador WEB em um endereço de rede. O nome do host e o nível do domínio para o domínio “system.master.com” são, respectivamente,

- A) system e segundo nível.
- B) system e terceiro nível.
- C) master e terceiro nível.
- D) master e segundo nível.
- E) .com e terceiro nível.

**Comentário:** Um servidor DNS raiz “aponta” para servidores de primeiro nível (TLD). No domínio mostrado, o TLD é o “.com”, que aponta para um servidor DNS responsável por “master” (segundo nível), que por sua vez, aponta para um terceiro nível, o host “system”, no caso da questão..

**Gabarito: B**

---

### 21. (FCC – 2016 – PRODATER – Analista Tecnológico/Analista de Suporte Técnico)

No Serviço de Nomes de Domínio – DNS existem diferentes tipos de servidores distribuídos hierarquicamente que armazenam informações também de forma hierárquica. Considerando o nome: www.empresa.com, o domínio .com é gerenciado pelo servidor

- A) Global.
- B) PDR.
- C) Authoritative.
- D) TLD.
- E) Root.



**Comentário:** Os domínios de mais alto nível são classificados em genéricos (".com", ".edu", ".bradesco", etc.) ou códigos de países (".br", ".mx", ".uy", ".jp", etc.). Em inglês é conhecido como TLD (Top Level Domain) e os servidores DNS TLD gerenciam tais domínios. Abaixo podemos ver mais exemplos de TLDs genéricos e dois exemplos de códigos de países.

**Gabarito: D**

---

## 22. (IBFC – 2016 – EBSERH-HUAP – Técnico/Informática)

O Domain Name System (DNS) é um sistema de gerenciamento de nomes hierárquicos e distribuídos. A funcionalidade do DNS Reverso vem a ser:

- A) reverter a funcionalidade básica de um DNS padrão obtendo o endereço MAC.
- B) resolver um endereço IP, buscando o nome de domínio associado ao host.
- C) resolver o nome do domínio de um host qualquer para seu endereço IP correspondente.
- D) com base na região geográfica, obter automaticamente um endereço IP local.
- E) resolver o problema da reversão do IPv6 para o IPv4 de uma forma rápida e automática.

**Comentário:** A questão começa com a definição de DNS, segundo o Tanenbaum. O DNS tem a função de traduzir um nome em um endereço, então o DNS reverso faz o contrário: traduz um endereço em um nome. É definido através do registro PTR:

PTR    Ponteiro (usado para o DNS reverso)    Nome alternativo de um end. IP.

**Gabarito: B**

---

## 23. (FUNRIO – 2016 – CM Nova Iguaçu – Técnico/Informática)

Um administrador de rede está configurando o DNS de um servidor e vai trabalhar com o registro que define as características da zona a ser configurada, tais como, o nome da zona e o nome do servidor, que é a autoridade para a referida zona, ou seja, o servidor DNS no qual está a zona que foi criada originalmente. Esse registro é conhecido pela sigla

- A) HINFO.
- B) MX.
- C) SOA.
- D) CNAME.

**Comentário:** Mais uma vez aquela tabela, agora copiei apenas a linha sobre o "SOA":

SOA    Início de autoridade (Start of Authority). Parâmetros para essa zona.

Ou seja, se falar sobre características/parâmetros de uma zona, trata-se do registro Start of Authority (SOA).

**Gabarito: C**



#### 24. (CESPE – 2016 – TCE-PR – Analista de Controle/Tecnologia da Informação)

Uma consulta DNS inicial típica, originada de uma máquina de usuário e encaminhada ao servidor de nomes local para um nome de domínio externo não armazenado em cache DNS, será do tipo

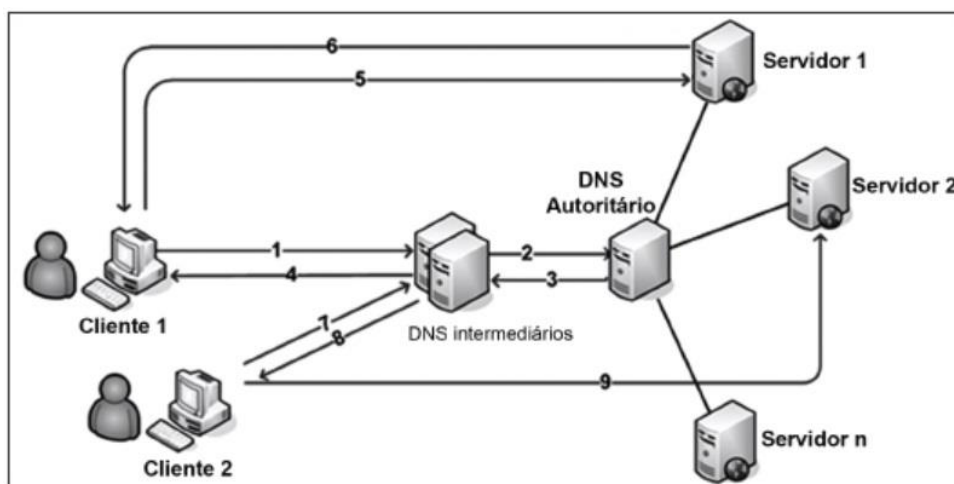
- A) raiz.
- B) domínio de alto nível.
- C) iterativa.
- D) recursiva.
- E) direta.

**Comentário:** O foco da questão é a consulta realizada de um equipamento ao servidor DNS local, supondo que a informação não esteja na cache desse servidor local. Nesse caso, o servidor DNS local irá requisitar ao servidor DNS TLD, receberá como resposta o próximo servidor DNS a ser consultado e repetirá o processo até ter toda a informação desejada. Armazenará em sua cache e responderá ao cliente (equipamento que fez a solicitação inicial). Note que o cliente fez uma requisição apenas e obteve uma resposta, mas o servidor DNS local realizou consultas recursivas.

**Gabarito: D**

#### 25. (FCC – 2016 – ELETROSUL – Profissional de Nível Superior/Informática)

O balanceamento de carga por DNS é uma abordagem popular e simples para as solicitações de balanceamento de servidores. Considere a figura abaixo.



De acordo com a figura, geralmente são estes os passos que ocorrem assim que é feita uma consulta DNS:

1. Quando um cliente tenta acessar o site, é realizada uma pesquisa no DNS local para determinar qual é o endereço I..... correspondente;
2. O pedido de endereço chega ao servidor de DNS II..... do domínio;



3. A primeira vez que esta consulta é feita, o servidor DNS remoto pode retornar todos os registros de endereços que ele tem para o site;
4. O servidor DNS III....., em seguida, determina o endereço de registro para retornar ao cliente;
5. Se todos os registros são retornados, o cliente utilizará o primeiro que lhe é atribuído;
6. O servidor responde ao cliente e atende ao pedido;
7. A cada pedido, o algoritmo Round Robin roda os endereços e retorna pela ordem em que eles estão;
8. Cada consulta DNS irá resultar em um cliente usando um endereço IV.....;
9. Esta rotação de endereços irá distribuir pedidos para os servidores.

As lacunas de I a IV são, correta e respectivamente, preenchidas com:

- A) TCP – autoritário – local – TCP igual ao obtido em 1
- B) IP – autoritário – local – IP diferente
- C) do servidor – local – autoritário – de um servidor
- D) do servidor – autoritário – local – do servidor igual ao obtido em 1
- E) IP – local – autoritário – IP igual ao obtido em 1

**Comentário:** Quando um cliente tenta acessar o site, é realizada uma pesquisa no DNS local para determinar qual é o endereço IP (DNS traduz nome em endereço IP) correspondente; O pedido de endereço chega ao servidor de DNS autoritário (após o servidor DNS local, chega ao servidor que possui os registros atualizados = autoritário) do domínio; O servidor DNS local (depois de retornar do servidor autoritário, o servidor local atualiza a cache e envia ao cliente), em seguida, determina o endereço de registro para retornar ao cliente; Cada consulta DNS irá resultar em um cliente usando um endereço IP diferente (essa é a ideia do algoritmo Round Robin, o balanceamento de carga).

**Gabarito: B**

---

## 26.(CESPE – 2016 – TCE-SC – Auditor Fiscal de Controle Externo/Controle Externo/Informática)

Acerca de redes de computadores e de protocolos TCP/IP, julgue o item a seguir.

Após o servidor local SMTP aceitar uma mensagem para subsequente envio, é necessário determinar o endereço do servidor de email do destinatário. Essa etapa é realizada mediante consulta DNS a um servidor de nomes capaz de prover a informação, no qual serão verificados os registros especiais MX (mail exchange).

**Comentário:** Vamos relembrar a tabela, focando na linha sobre “MX”:

Tipo	Significado	Valor
SOA	Início de autoridade ( <i>Start of Authority</i> ).	Parâmetros para essa zona.





A	Endereço IPv4.	Inteiro de 32 bits.
AAAA	Endereço IPv6.	Inteiro de 128 bits.
MX	Troca de mensagens de e-mail.	Prioridade, domínio disposto a aceitar e-mails.
NS	Servidor de nomes.	Nome de um servidor para este domínio.
CNAME	Nome canônico ( <i>alias</i> = apelido).	Nome de domínio.
PTR	Ponteiro (usado para o DNS reverso <sup>5</sup> )	Nome alternativo de um end. IP.
SPF	Estrutura de política do transmissor.	Codificação de texto da política de envio de mensagens de e-mail.
SRV	Identifica computadores que hospedam serviços específicos.	Host que o oferece.
TXT	Informações sobre um servidor, rede, <i>datacenter</i> , etc.	Texto ASCII com descrições.

**Gabarito: Certo**

**27. (CESPE – 2016 – Polícia Científica-PE – Perito Criminal/Área 7/Ciência da Computação, Engenharia da Computação ou Sistemas de Informação)**

Na operação de um serviço DNS, se uma consulta a um servidor de alto nível retornar uma resposta positiva para o servidor DNS local, o mapeamento nome/endereço será

- A) armazenado definitivamente no banco de dados do servidor DNS local.
- B) replicado para todos os servidores DNS alcançáveis para que estejam disponíveis a outras consultas.
- C) repassado pelo módulo tradutor a um servidor raiz para confirmar a resposta recebida.
- D) armazenado em cache local e pode ser mantido por um tempo definido por configuração.
- E) repassado ao módulo tradutor do provedor de serviços para realizar a entrega à aplicação.

**Comentário:** Quando o servidor DNS local busca uma informação nova, ele guarda na cache, por tempo determinado. Esse tempo varia de segundos/minutos a um dia, por exemplo. Depende do tempo definido no campo TTL.

**Gabarito: D**

<sup>5</sup> Envia um endereço IP como consulta e recebe o nome como resposta.



---

**28.(FCC – 2015 – CNMP – Analista/Tecnologia da Informação e Comunicação/Suporte e Infraestrutura)**

O serviço de nome de domínios (DNS) possui uma arquitetura do tipo cliente/servidor na qual a base de dados é distribuída por toda internet. Nessa arquitetura, o acesso ao servidor DNS para buscar o relacionamento IP/Domínio é feito pelo cliente que é o

- A) Browser.
- B) DNS Cache.
- C) DNS Resolver.
- D) DNS Searcher.
- E) Gateway.

**Comentário:** Conforme vimos, o browser (navegador) não resolve o nome! Supondo que uma URL seja solicitada através de um browser, o “resolvedor DNS” terá o papel de resolver o DNS (o próprio nome já diz isso). Pode ser através do arquivo hosts (máquina local) ou através de solicitação ao servidor DNS “mais próximo” (mais comum - geralmente o servidor DNS utilizado pelo provedor de acesso à Internet). Se o servidor DNS tiver a informação em cache, ele responde, senão faz uma busca nos servidores superiores na hierarquia DNS, atualiza sua cache e responde ao “resolvedor”.

**Gabarito: C**

---

**29.(CESPE – 2015 – FUB – Técnico/Tecnologia da Informação)**

Acerca da arquitetura TCP/IP, julgue o item a seguir.

O protocolo DNS (domain name service), localizado no nível de aplicação da camada de transporte do TCP, é responsável pelo mapeamento de nomes e de endereços.

**Comentário:** O DNS está localizado na camada de aplicação. A questão misturou “nível de aplicação da camada de transporte do TCP”.

**Gabarito: Errado**

---

**30.(FGV – 2015 – TCE-SE – Analista de Tecnologia da Informação/Desenvolvimento)**

Um programa precisa simular o comportamento de um cliente DNS. Para funcionar adequadamente, o programa precisa enviar as consultas para um servidor DNS, especificamente para a sua porta:

- A) udp/23
- B) icmp/34
- C) tcp/22
- D) ip/50



E) udp/53

**Comentário:** Como já vimos, o protocolo de transporte utilizado para consultas DNS é o UDP e a porta é a 53. Essas informações devem estar enraizadas em seu cérebro! Para a transferência de zonas de DNS, é utilizado o TCP (na mesma porta: 53) como protocolo de transporte.

**Gabarito: E**

---

### 31.(CESPE – 2015 – TRE-MT – Técnico Judiciário/Apoio Especializado/Programação de Sistemas)

Acerca do servidor DNS/BIND (Domain Name System/Berkley Internet Domain), cuja funcionalidade é resolver nomes da rede, assinale a opção correta.

- A) Cada domínio tem seus registros de recursos e o registro de domínio denominado NS (name server), o qual é utilizado para definir propriedades básicas do domínio e sua zona.
- B) Um servidor DNS utiliza LDAP para fazer armazenamento das zonas de domínio para uma rápida resolução de um nome.
- C) O BIND, que utiliza a porta 53, é um programa de código aberto utilizado pela maior parte dos servidores DNS.
- D) Os domínios de um servidor DNS são organizados na Internet sobre uma estrutura de dados do tipo lista encadeada, sendo o primeiro elemento da lista um ponto.
- E) O protocolo HTTP implementa, por padrão, um servidor de resolução de nomes amplamente utilizado na Internet conhecido como DNS.

**Comentário:** Para quem não está acostumado com essa parte de servidores, memorize o seguinte: servidor DNS é quase sinônimo de BIND! Se você ainda não o conhece e não leu sobre ele, recomendo uma passada rápida na URL <https://www.isc.org/downloads/bind/>.

**Gabarito: C**

---

### 32.(IADES – 2015 – CRC-MG – Analista de Sistemas)

Quanto ao programa que é normalmente utilizado para testar se um servidor DNS (Domain Name Server) está funcionando corretamente, ou seja, resolvendo nomes para os endereços IP, assinale a alternativa correta.

- A) ping
- B) tracert
- C) nslookup
- D) ipconfig
- E) net host



**Comentário:** (A) Serve para ver se “está vivo”; (B) Serve para traçar uma rota (roteadores intermediários); (C) Exatamente! ns = name server, lookup = “dar uma olhada”, se você nunca usou, experimente agora no prompt: nslookup estrategiaconcursos.com.br; (D) verifica configurações das interfaces de rede; (E) o comando net não possui o parâmetro host!

**Gabarito: C**

---

**33. (2015 - FGV - TCE-SE - Analista de Tecnologia da Informação-Suporte Técnico em Infraestrutura e Redes)**

Em um equipamento rodando Linux, um administrador deseja alterar o endereço default do servidor DNS usado para consultas. Para isso, ele precisa alterar o arquivo:

- A) /etc/named.conf
- B) /etc/bind.conf
- C) /etc/network.conf
- D) /etc/dns.conf
- E) /etc/resolv.conf

**Comentário:** Um exemplo de arquivo resolv.conf:

```
domain ti.teste.com.br  
search ti.teste.com.br teste.com.br  
nameserver 192.168.1.1  
nameserver 192.168.2.1
```

**Gabarito: E**

---

**34.(2014 - AOC - UFPA - Analista de Tecnologia da Informação - Suporte e Redes)**

Em algumas distribuições Linux encontramos um arquivo que identifica os locais dos computadores de servidor de nome DNS, computadores estes que são usados pelo TCP/IP para traduzir os nomes de Internet. Assinale a alternativa que apresenta o nome deste arquivo.

- A) DNS.conf.
- B) resolver.conf.
- C) resolv.conf.
- D) translate.conf.
- E) change.conf.

**Comentário:** Mesmo que a questão anterior! Note que o resolv.conf é bastante cobrado!

**Gabarito: C**



---

**35.(2014 - IADES - TRE-PA - Técnico Judiciário - Operação de Computador)**

Um servidor Linux pode hospedar o serviço de resolução de nomes de uma rede de computadores. Conhecido por DNS, esse serviço é indispensável em uma rede que possua conexão com a internet. O nome de um pacote que implementa o DNS, muito utilizado em sistemas operacionais Linux, é

- A) Firefox.
- B) Apache.
- C) Squid.
- D) Postfix.
- E) BIND.

**Comentário:** O pacote é conhecido como BIND (versão 8, ou bind9 - versão 9).

**Gabarito: E**

---

**36.(2010 - FCC - TCE-SP - Auxiliar da Fiscalização Financeira)**

Em Linux, o `/etc/resolv.conf` é um arquivo texto simples, com um parâmetro por linha e especificações de endereços de servidores DNS. Nesse arquivo existem três palavras chaves normalmente usadas, que são

- A) domain, search e resolv.
- B) search, resolv e order.
- C) domain, search e nameserver.
- D) search, nameserver e order.
- E) search nameserver e resolv.

**Comentário:** Mais uma vez vamos ver um exemplo do `resolv.conf`, para memorizar 😊

domain ti.teste.com.br

search ti.teste.com.br teste.com.br

nameserver 192.168.1.1

nameserver 192.168.2.1

**Gabarito: C**

---

**37.(2010 - FCC - TCE-SP - Auxiliar da Fiscalização Financeira)**

No Linux, ele é muito útil para máquinas que são acessadas frequentemente, pois a inclusão de um computador neste arquivo dispensa a consulta a um servidor DNS para obter um endereço IP, sendo muito útil para máquinas que são acessadas frequentemente. Trata-se de:



- A) /etc/nameserver
- B) /etc/localhost
- C) /etc/ipsec
- D) /etc/hosts
- E) /etc/dnshost

**Comentário:** Um exemplo do arquivo hosts (que também existe no Windows!):

# Aqui são colocados comentários

# End. IP	Nome do host	Alias (opcional)
127.0.0.1	localhost	localmente
192.168.0.1	www.teste.com.br	teste

**Gabarito: D**

---

### 38.(2009 - FGV - MEC - Gerente de Suporte)

No UNIX, o DNS é implementado por meio do software Berkeley Internet Name Domain (BIND), que segue a filosofia cliente/servidor.

O cliente do BIND é denominado "resolver", responsável por gerar as "queries" enquanto que o servidor do BIND é chamado por "named", responsável por responder às "queries".

Configurações BIND são descritas pelo tipo de serviço a ser executado pelo software, existindo quatro níveis de serviço que podem ser definidos nessas configurações: "resolver-only systems", "caching-only servers", "primary servers" e "secondary servers".

Os parâmetros que definem a configuração do "resolver-only systems" são inseridas no seguinte arquivo:

- A) /etc/resolv.sys
- B) /etc/resolv.cfg
- C) /etc/resolv.bind
- D) /etc/resolv.conf
- E) /etc/resolv.parm

**Comentário:** O arquivo resolv.conf também serve para especificar o tipo (nível) de serviço a ser executado pelo software, a saber:

- *resolver-only system*: não requer que o sistema local tenha um servidor DNS em execução, requer apenas o resolver;
- *caching-only server*: servidor que não possui uma cópia da tabela de zonas, ou seja é não-autoritativo, possuindo uma grande quantidade de registros em cache;;

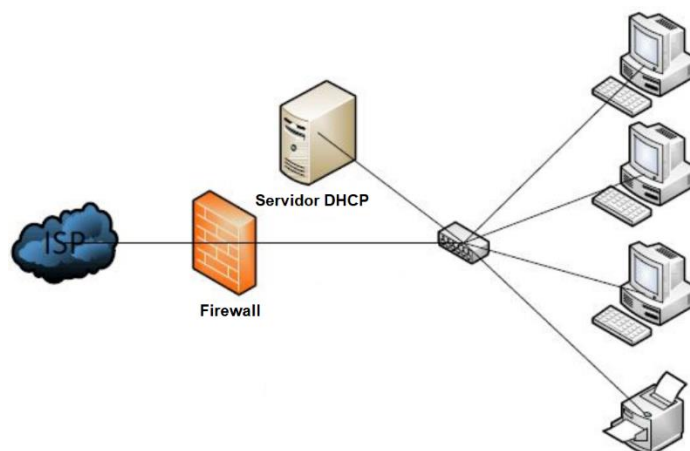


- *primary server (master server)*: onde todas atualizações manuais devem ser realizadas, é autoritativo;
- *secondary server*: busca informações de zona em um *master server*, é autoritativo.

**Gabarito: D**

## DHCP (DYNAMIC HOST CONFIGURATION PROTOCOL)

O DHCP (*Dynamic Host Configuration Protocol*) é um protocolo que tem a função de configurar os endereços IP dos computadores de uma rede de forma dinâmica. Ou seja, deve haver pelo menos um servidor DHCP pré-configurado para receber solicitações de computadores que não possuem endereço IP (clientes), o servidor verificar qual endereço IP disponível e envia ao solicitante. Abaixo podemos ver um exemplo:



No cenário mostrado, os três PCs e a impressora estão configurados como clientes DHCP. Cada um deles deve enviar uma mensagem *broadcast* (mensagem a todos, pois não sabe quem é o servidor DHCP), o servidor DHCP recebe a mensagem, verifica qual endereço IP está disponível (ou até mesmo reservado para o solicitante), oferece esse endereço ao cliente e, por fim, o cliente aceita (comunicando o servidor que vai utilizar tal endereço IP).

Algumas informações que devem ser configuradas no servidor:

- Escopo: intervalo de endereços IP que estarão disponíveis para atribuição automática. Também pode se referir ao intervalo que não será distribuído. Ex.: endereços IP disponíveis = 192.168.1.100 a 192.168.1.150;
- Máscara de rede: usada para fazer a divisão da rede de computadores. Uma rede classe C possui a máscara 255.255.255.0;
- Gateway: dispositivo que serve para interligar a rede local com a Internet, ex. na figura: o elemento central (pode ser um modem/roteador), que liga os cinco dispositivos da rede local (servidor + 3 PCs + impressora) à Internet (passando por um firewall), ex.: 192.168.1.1;
- DNS: endereço do servidor DNS a ser consultado, ex.: 8.8.8.8 (esse é o servidor DNS do Google).





**Importante:** o servidor DHCP precisa de pelo menos uma interface de rede configurada com endereço IP fixo!

O `dhcpd` é o servidor DHCP no Linux. Ele é útil, por exemplo, em uma máquina agindo como um roteador em uma rede local.

Obs.: `dhcpd` (*daemon* do servidor DHCP) não é o mesmo que `dhcpcd` (*daemon* do cliente DHCP).

#### Instalação:

Deve-se instalar o `dhcp`, disponível nos repositórios oficiais.

#### Uso:

O `dhcpd` inclui dois arquivos: `dhcpcd4.service` e `dhcpcd6.service`, que podem ser usados para controlar o *daemon*. Eles iniciam o *daemon* em todas as interfaces de rede para IPv4 e IPv6, respectivamente.

#### Configuração:

Deve-se atribuir um endereço IPv4 estático para a interface que se deseja usar (ex.: `eth0`).

O arquivo `/etc/dhcpd.conf` contém as configurações. Esse arquivo pode se parecer com:

```
option domain-name-servers 8.8.8.8, 8.8.4.4;  
option subnet-mask 255.255.255.0;  
option routers 139.96.30.100;  
subnet 139.96.30.0 netmask 255.255.255.0 {  
    range 139.96.30.150 139.96.30.250;  
}
```

### QUESTÕES COMENTADAS

#### 39.(2013 - CESPE - TRT8)

Para alterar o arquivo de configuração do serviço de DHCP no Linux, deve-se acessar o diretório

- A) `/dev`.
- B) `/mnt`.
- C) `/etc`.
- D) `/usr/bin`.
- E) `/boot`.

#### Comentário:

Por padrão, os arquivos de configuração ficam no diretório `"/etc"`, como é o caso do `"dhcpd.conf"`.

**Gabarito: C**



#### 40.(2018 - SUGEP-UFRPE - UFRPE)

Para acesso à Internet, servidores Windows e Linux utilizam um serviço para atribuição dinâmica de IPs aos microcomputadores conectados à rede, em que é marcada a opção associada a "o IP será atribuído automaticamente pelo servidor", na configuração.

Esse serviço é conhecido pela sigla:

- A) DNS
- B) HTTP
- C) DHCP
- D) TCP
- E) IP

#### Comentário:

O DHCP (*Dynamic Host Configuration Protocol*) é um protocolo que tem a função de configurar os endereços IP dos computadores de uma rede de forma dinâmica. Ou seja, deve haver pelo menos um servidor DHCP pré-configurado para receber solicitações de computadores que não possuem endereço IP (clientes), o servidor verificar qual endereço IP disponível e envia ao solicitante.

**Gabarito: C**

## NFS E SMB/CIFS, INTEGRAÇÃO UNIX X WINDOWS

Quando falamos em sistemas de arquivos FAT, NTFS, EXT, XFS, entre outros, estamos falando em sistemas de arquivos "locais", os que permitem o acesso a uma mídia interna ou conectada a um computador, por exemplo. Existem também os sistemas de arquivos em rede, que dão a ilusão de um acesso local, porém o acesso é remoto. Os mais conhecidos são o NFS e o SMB/CIFS, os quais veremos a seguir.

O **NFS (Network File System)** é um protocolo de sistema de arquivos distribuído, **originado no Unix**, que permite que um usuário em um computador cliente acesse arquivos através de uma rede como se estivesse acessando na máquina local. O cliente NFS tem a finalidade de tornar o acesso remoto transparente para o usuário do computador, e esta interface cliente e servidor, executada pelo NFS através dos protocolos Cliente-Servidor, fica bem definida quando o usuário, ao chamar um arquivo/diretório no servidor, lhe parece estar acessando localmente, sendo que está trabalhando com arquivos remotamente.

Uma máquina Linux pode ser um servidor NFS e um cliente NFS, o que significa que pode exportar sistemas de arquivo para outros sistemas e montar sistemas de arquivo exportados de outras máquinas. Por exemplo, um grupo de usuários pode ter acesso aos arquivos de um determinado projeto usando um diretório compartilhado do sistema de arquivo NFS montado no diretório `"/projeto"`. Para acessar os arquivos compartilhados, o usuário vai até o diretório `"/projeto"`, sem



senhas ou comandos especiais para lembrar. Dessa forma, os usuários trabalham como se o diretório estivesse em suas máquinas locais.

Algumas **características do NFS** são:

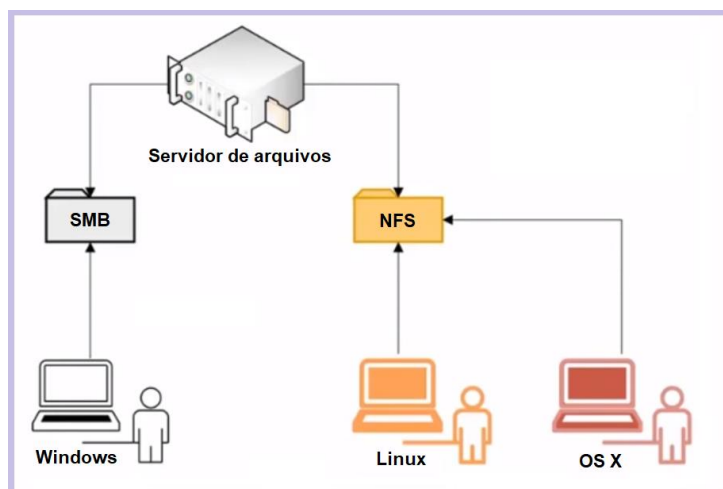
- Arquitetura cliente-servidor: o servidor recebe as requisições vindas do cliente, verifica a validade, executa e retorna ao cliente;
- *Stateless* (sem estado): considera cada requisição como uma transação independente que não está relacionada a qualquer requisição anterior, de forma que a comunicação consista de pares requisição/resposta independentes. Diante de uma falha no sistema, quando o servidor NFS volta a funcionar corretamente, o estado anterior é restaurado e o funcionamento continua como se não houvesse ocorrido nenhum problema;
- *Caching*: permite que as informações utilizadas mais recentemente sejam alocadas para posterior uso, ou pode carregar os dados em antecipação a operações futuras;
- *File Locking* (bloqueio de arquivo): permite que um processo tenha acesso exclusivo a um arquivo ou parte deste, e força outros processos que estão solicitando acesso ao mesmo arquivo, aguardarem a liberação;
- Utiliza o protocolo RPC (*Remote Procedure Call*): define um modo independente do sistema para processos se comunicarem através de uma rede de computadores, sendo que o cliente faz a chamada do procedimento remoto no servidor;
- Protocolo de transporte padrão é o UDP, no entanto, é possível utilizar o TCP;
- Compartilhar arquivos de um servidor NFS é conhecido como exportar os diretórios.

Para que os clientes possam acessar o servidor NFS é necessário que os seguintes *daemons* estejam em execução:

- *nfsd*: *daemon* NFS, atende requisições dos clientes NFS;
- *mountd*: *daemon* de montagem NFS, executa as solicitações passadas pelo *nfsd*;
- *portmap*: *daemon portmapper*, permite que clientes NFS descubram qual porta o servidor NFS está utilizando.

Na figura abaixo podemos ver o acesso a um servidor de arquivos através da rede. Note que máquinas Unix-like (ex.: Linux e OS X) utilizam o NFS como protocolo e as máquinas Windows utilizam o SMB/CIFS, que veremos o funcionamento na sequência.



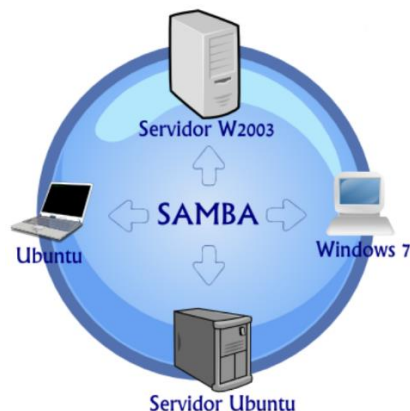


Antes de começar a falar do protocolo em si, deixo bem claro que as questões de concurso já cobraram alguns detalhes do NFS, mas em relação ao SMB/CIFS a cobrança é superficial. Vamos lá...

O **SMB/CIFS** (*Server Message Block/Common Internet File System*) é um protocolo de redes cujo uso mais comum como é o compartilhamento de arquivos em uma rede local. Ele permite que o cliente manipule arquivos como se estes estivessem em sua máquina local (mesma coisa que o NFS, heim?). Algumas das operações suportadas são: leitura, escrita, criação, exclusão e renomeação, sendo que os arquivos/diretórios manipulados estão em um servidor remoto.

O protocolo SMB/CIFS funciona através do envio de pacotes do cliente para o servidor. O servidor recebe o pacote, verifica se a requisição é válida (se o cliente possui as permissões apropriadas), executa a requisição e retorna um pacote de resposta ao cliente. O cliente verifica o pacote de resposta para determinar se a requisição inicial obteve êxito. O protocolo mais utilizado para transporte confiável é o NetBIOS sobre TCP (NBT). Outros protocolos foram utilizados na camada de transporte, mas o NBT se tornou o mais utilizado.

O SMB/CIFS é muito utilizado pelos sistemas operacionais Windows, podendo funcionar como um servidor ou cliente. Isso não quer dizer que sistemas Unix-like não possuam também esse protocolo! Na verdade, a maioria dos sistemas Unix-Like (**Linux**, por exemplo) possuem uma implementação de cliente/servidor do SMB/CIFS via **Samba**, que é um “software servidor” para Linux que permite o gerenciamento e compartilhamento de recursos em redes formadas por computadores com o Windows. Dessa forma é possível utilizar o Linux como servidor de arquivos, servidor de impressão, entre outros, como se a rede utilizasse servidores Windows (Server 200x, 201x, entre outros).



Resumindo: o Samba é um componente que realiza a comunicação entre servidores Linux e Windows, permitindo que eles compartilhem recursos de disco e de impressão. O *daemon* `smbd` possui dois modos de compartilhamento. O primeiro modo (*sharemode*) é mais simples, gerando uma senha para cada recurso que é compartilhado. O segundo modo (*user*) permite o compartilhamento de vários recursos com um único *login* e senha. Os privilégios de acesso aos recursos devem ser sempre mediados pelos administradores do sistema.

Um outro componente interessante do pacote Samba é o *nmbd*, um servidor de nomes NetBios (mais conhecido por **WINS - Windows Internet Name Server**) responsável por entender e responder solicitações de resoluções de nomes NetBios sobre IP. É ele o responsável pelo “aparecimento” do ícone do servidor Samba no ambiente de rede do Windows! Obs.: Se você não sabe o que é essa resolução de nomes, pense que é algo como o DNS, mas não de forma hierárquica, é uma resolução feita pelo Windows (sabendo isso já está bom para a prova 😊).

## QUESTÕES COMENTADAS

### 41.(2012 - FCC - TRT6)

CIFS e NFS

- A) referem-se, respectivamente, às implementações para Unix e Windows de um mesmo protocolo que oferece a funcionalidade de sistema de arquivos distribuído.
- B) são diferentes implementações de um mesmo protocolo que oferecem a funcionalidade de sistema de arquivos distribuído.
- C) são, respectivamente, cliente e servidor de um mesmo protocolo que implementa a funcionalidade de sistema de arquivos distribuído.
- D) são diferentes protocolos que implementam a funcionalidade de sistema de arquivos distribuído.
- E) referem-se, respectivamente, às implementações para Windows e Unix de um mesmo protocolo que oferece a funcionalidade de sistema de arquivo distribuído.

### Comentários:

NFS (Network File System): protocolo de sistema de arquivos distribuído, originalmente desenvolvido pela Sun Microsystems, que permite que um usuário em um computador cliente acesse arquivos através de uma rede como se estivesse acessando na máquina local. Utiliza o sistema Open Network Computing Remote Procedure Call (ONC RPC).

CIFS (Common Internet File System): opera como um protocolo de rede da camada de aplicação usado principalmente para fornecer acesso compartilhado a arquivos, impressoras e comunicações diversas entre nós sobre uma rede. Seu “sucessor” é o SMB (Server Message Block).

**Gabarito: D**



#### **42.(2012 - COPESE-UFT - DPE-TO)**

Em relação ao NFS (Sistema de Arquivo de Rede) é correto afirmar, EXCETO:

- A) A ideia básica que fundamenta o NFS é que cada servidor de arquivos fornece uma visão padronizada de seu sistema local de arquivos.
- B) No NFS, toda comunicação cliente servidor é feita por meio de RPC (chamada de procedimento remoto).
- C) O NFS é, em grande parte, independente de sistemas locais de arquivos.
- D) O modelo de sistema de arquivos oferecido pelo NFS é bem diferente do oferecido por sistemas baseados em Unix.

#### **Comentários:**

NFS (Network File System): protocolo de sistema de arquivos distribuído, originalmente desenvolvido pela Sun Microsystems, que permite que um usuário em um computador cliente acesse arquivos através de uma rede como se estivesse acessando na máquina local. Utiliza o sistema Open Network Computing Remote Procedure Call (ONC RPC). Ele foi originado no Unix e continua com as mesmas características!

**Gabarito: D**

---

#### **43.(2013 - FCC TRT18)**

O Sistema de Arquivo de Rede - NFS

- A) é um protocolo da camada de transporte (modelo TCP/IP) e um componente do diretório X.500.
- B) é um componente do diretório X.500 e oferece grande parte das funcionalidades de CIFS.
- C) viabiliza a um usuário remoto a conversação de voz sobre IP com um usuário local, quando encadeado com o protocolo LDAP.
- D) é um protocolo da camada de rede ( modelo TCP/IP) e oferece grande parte das funcionalidades de DAP.
- E) permite que sejam acessados arquivos que se encontram armazenados em um servidor remoto como se eles estivessem instalados localmente.

#### **Comentários:**

NFS (Network File System): protocolo de sistema de arquivos distribuído, originalmente desenvolvido pela Sun Microsystems, que permite que um usuário em um computador cliente acesse arquivos através de uma rede como se estivesse acessando na máquina local. Utiliza o sistema Open Network Computing Remote Procedure Call (ONC RPC).

**Gabarito: E**



---

**44.(2015 - FCC - TRT15)**

Dentre os diferentes sistemas de arquivos compatíveis com os sistemas operacionais Linux, o que apresenta a característica de ser nativamente especificado para o uso em rede de computadores é o

- A) Ext3
- B) NTFS.
- C) SMB.
- D) LDAP.
- E) NFS.

**Comentários:**

Ext é um sistema de arquivos do Linux (mas não de rede). NTFS é um sistema de arquivos do Windows. SMB (CIFS) é um sistema de arquivos de redes do Windows. LDAP é um protocolo de serviço de diretório (é utilizado para o Active Directory, por exemplo). E, por fim, o NFS é um sistema de arquivos de rede para o Linux!

**Gabarito: E**

---

**45.(2015 - IBFC - EBSEH)**

No compartilhamento de arquivos e impressoras é tradicional, nos Sistemas Operacionais da Microsoft, a utilização do seguinte protocolo:

- A) ITU-T
- B) TLS/SSL
- C) RIPv2
- D) SMB/CIFS
- E) IPv6

**Comentários:**

Quando fala em protocolo para compartilhamento de recursos, ou sistema de arquivos de rede, se for para Linux pense no NFS e se for para Windows pense em SMB/CIFS!

**Gabarito: D**

---





**46.(2016 - AOCP - EBSERH)**

O NFS (Network File System) permite compartilhar sistemas de arquivos entre computadores conectados em rede e pode ser parte fundamental da infraestrutura da tecnologia da informação. Sobre NFS, analise as assertivas a seguir e assinale a alternativa que aponta a(s) correta(s).

I. O NFS é considerado sem estado (stateless) e, portanto, quando um servidor NFS volta a funcionar, o estado anterior é restaurado e a informação não é perdida.

II. O NFS pode ser implementado do lado servidor e do lado cliente.

III. O NFS roda sobre o protocolo RPC (Remote Procedure Call), que define um modo independente do sistema para processos se comunicarem através de uma rede de computadores.

IV. O NFS suporta apenas UDP como protocolo de transporte, pois ele apresenta desempenho significativamente melhor que o TCP em redes locais.

A) Apenas I e II.

B) Apenas II e IV.

C) Apenas III.

D) Apenas III e I.

E) Apenas I, II e III.

**Comentários:**

I. Exato! O NFS é *stateless*, cada requisição é uma transação independente que não está relacionada a qualquer requisição anterior. Então, quando um servidor NFS volta a funcionar, o estado anterior é restaurado e a informação não é perdida. (II) Existe quem faz requisições de acesso e manipulação de arquivos e diretórios (cliente) e quem recebe as requisições, avalia as permissões, executa e retorna (servidor). (III) O NFS utiliza o RPC (*Remote Procedure Call*), o cliente faz a chamada ao servidor remoto (o servidor até pode estar na mesma máquina, mas o cenário mais comum é remoto). (IV) O protocolo padrão de transporte é o UDP, mas é possível optar pelo TCP.

**Gabarito: E**

---

**47.(2018 - FCC - DPE-AM)**

O Common Internet File System – CIFS utiliza um conjunto de serviços agregados para prover meios de compartilhar arquivos, diretórios e impressora em uma rede de computadores. A resolução de nomes no CIFS é realizada pelo

A) SMB.

B) hostname.

C) IPC.



D) NETBios.

E) WINS.

#### Comentários:

Para responder essa, vale a pena lembrar como funciona o Samba, pois é um servidor instalado no Linux que funciona com o SMB/CIFS:

Trata-se de um componente que realiza a comunicação entre servidores Linux e Windows, permitindo que eles compartilhem recursos de disco e de impressão. O *daemon* `smbd` possui dois modos de compartilhamento (*sharemode* e *user*). Um outro componente interessante do pacote Samba é o `nmbd`, um servidor de nomes NetBios (mais conhecido por **WINS - Windows Internet Name Server**) responsável por entender e responder solicitações de resoluções de nomes NetBios sobre IP. É ele o responsável pelo “aparecimento” do ícone do servidor Samba no ambiente de rede do Windows!

**Gabarito: E**

---

#### 48.(2019 - IF-ES - IF-ES)

O Network File System (NFS) – Sistemas de Arquivos em Rede – tem como um dos principais propósitos dar suporte a um sistema heterogêneo, no qual clientes e servidores estejam possivelmente executando sistemas operacionais e hardwares diferentes. Sobre o NFS, é CORRETO afirmar:

- A) O NFS utiliza dois protocolos cliente-servidor, em que o primeiro é responsável pela montagem e o segundo é para acesso de diretório e arquivos.
- B) O servidor tem total gerência sobre o ponto de montagem nos clientes.
- C) Os serviços NFS são implementados apenas nos servidores Linux.
- D) Como critério de segurança, os clientes não podem ter acesso aos atributos dos arquivos.
- E) O NFS faz uso de máquinas distintas para servidores e clientes, impossibilitando que a mesma máquina seja tanto cliente quanto servidor

#### Comentários:

Para que os clientes possam acessar o servidor NFS é necessário que os seguintes *daemons* estejam em execução:

- **nfsd**: *daemon* NFS, atende requisições dos clientes NFS;
- **mountd**: *daemon* de montagem NFS, executa as solicitações passadas pelo `nfsd`;
- **portmap**: *daemon portmapper*, permite que clientes NFS descubram qual porta o servidor NFS está utilizando.



Para essa questão, esqueça o *portmap*, pois só serve para descobrir a porta do servidor. Os outros dois *daemons* fazem o papel dos protocolos citados na alternativa A: um atende requisições dos clientes (acessos a diretórios e arquivos) e o outro faz a montagem.

**Gabarito: A**

## FTP (FILE TRANSFER PROTOCOL)

Como o próprio nome deixa claro, o FTP é um protocolo de transferência de arquivos. Trata-se de um protocolo padrão, independente de hardware. O FTP é baseado no protocolo de transporte TCP, o que garante a entrega dos pacotes. O servidor FTP utiliza as **portas 20 para os dados e a 21 para o controle**. Vamos ver como ele funciona:

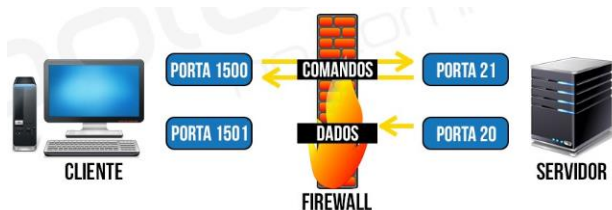
Um cliente realiza uma conexão TCP para a porta 21 do servidor. Essa conexão (conexão de controle) permanece aberta ao longo da sessão enquanto uma segunda conexão (conexão de dados), é estabelecida na porta 20 do servidor e em alguma porta do cliente (comunicada no diálogo entre cliente e servidor). A conexão de controle (porta 21) é utilizada para administração da sessão (comandos, identificação) entre cliente e servidor.

O servidor responde na conexão de controle com três dígitos de código de estado em ASCII com uma mensagem de texto opcional. Por exemplo, "200" ou "200 OK" significa que o último comando obteve êxito. Os números representam o número do código e o texto opcional representa as explicações ou parâmetros necessários. Uma transferência de arquivo em progresso, sobre uma conexão de dados, pode ser abortada utilizando uma mensagem de interrupção enviada sobre a conexão de controle.

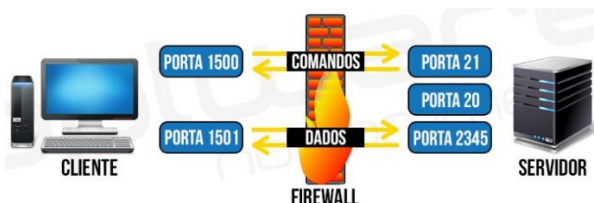
O FTP pode ser executado em modo ativo ou passivo, os quais determinam como a conexão de dados é estabelecida. No **modo ativo**, o cliente envia para o servidor o endereço IP e o número da porta na qual ele irá ouvir e então o servidor inicia a conexão TCP. No exemplo abaixo vemos que o cliente informou ao servidor que a porta 1501 aguardará uma conexão vinda do servidor para receber os dados.



Mas e se houver um firewall que não tenha liberado a porta 1501? Olhe o que acontece:



Em situações onde o cliente está atrás de um firewall e inapto para aceitar entradas de conexões TCP, o **modo passivo** pode ser utilizado. O cliente envia um comando PASV para o servidor e recebe um endereço IP e um número de porta como resposta, os quais o cliente utiliza para abrir a conexão de dados com o servidor. Na figura abaixo podemos ver que o cliente solicitou uma conexão no modo passivo e o servidor “disse”: “Vou abrir a porta 2345 e você pode se conectar nela para receber os dados”. Então, nesse caso, a porta 20 não será utilizada.



A transferência de dados pode ser feita em qualquer um dos três modos a seguir:

- Modo fluxo: dado é enviado como um fluxo contínuo, liberando o FTP de fazer algum processamento. Todo processamento é deixado para o TCP. Nenhum indicador de fim de arquivo é necessário, a menos que o dado esteja dividido dentro de registros;
- Modo de bloco: o FTP quebra o dado dentro de vários blocos (bloco de cabeçalho, contagem de byte e campo de dado) e então passa-o para o TCP;
- Modo comprimido: dado é comprimido utilizando um algoritmo simples.

O **acesso a servidores FTP** pode ocorrer de dois modos: através de uma interface ou através da linha de comando. Tanto usuários Linux como usuários Windows podem acessar através dos dois modos. O modo linha de comando está presente em qualquer distribuição Linux-like e Windows.

A partir de qualquer navegador credenciado (Internet Explorer, Chrome, Firefox, entre outros), também é possível acessar um servidor FTP digitando na barra de endereço:

`ftp://[username]:[password]@[servidor]`

ou

`ftp://[username]:[password]@[servidor]:[porta]`

Os **comandos** abaixo podem ser executados no FTP **através da linha de comando**. Os comandos do FTP podem ser abreviados, desde que não formem expressões ambíguas.

- !: executa o comando na máquina local;
- ?: semelhante a help;
- append: adiciona dados a um arquivo existente;
- ascii: configura o tipo de transferência de arquivos para ASCII;
- bell: emite um bip quando um comando é executado;
- binary: configura o tipo de transferência de arquivos para binário;
- bye: encerra a sessão FTP;
- cd: seguido de caminho/diretório muda para o diretório informado;
- delete: apaga um arquivo. Para mais de um arquivo utiliza-se mdelete;



- debug: estabelece a modalidade de depuração;
- dir: mostra o conteúdo do diretório servidor atual;
- disconnect: semelhante a bye;
- get: obtém um arquivo do servidor. Para mais de um arquivo utiliza-se mget;
- glob: seleciona a expansão para nomes de arquivo;
- hash: demonstra cada bloco do arquivo durante a transferência. Cada bloco compõe-se de 1024 bytes;
- help: lista sumariamente todos comandos disponíveis;
- literal: permite enviar comandos arbitrários;
- ls: mostra uma lista abreviada do conteúdo do diretório servidor. Para mais de uma pasta utiliza-se mls;
- mkdir: cria um diretório ou subdiretório no servidor;
- prompt: ativa/desativa o modo interativo;
- put: envia um arquivo ao servidor. Para enviar mais de um arquivo utiliza-se mput;
- pwd: mostra o diretório de trabalho;
- quit: finaliza a sessão FTP;
- quote: envia subcomandos do servidor FTP, como se encontram no servidor;
- recv: similar a get;
- remotehelp: solicita ajuda do servidor FTP remoto;
- rename: renomeia um arquivo;
- send: semelhante a put;
- status: obtém informações de estado do servidor;
- trace: demonstra o caminho percorrido pelo arquivo na transferência;
- type: especifica o tipo de representação;
- user: inicia a sessão no servidor;
- verbose: ativa/desativa a modalidade literal.

Seguindo a lógica adotada para servidores no Linux, o servidor FTP é executado através de um daemon, o **ftpd**.

### QUESTÕES COMENTADAS

#### 49.(CESPE/HEMOBRÁS - 2008)

Tanto o Linux quanto o Windows possuem softwares clientes para FTP (file transfer protocol) e que podem ser utilizados para a troca de arquivos em uma rede local.

#### Comentários:

É comum que sistemas operacionais conhecidos, como o Windows e o Linux, tenham software cliente FTP para se conectar a um servidor e enviar/baixar arquivos.

**Gabarito: Certo**



**50.(INSTITUTO AOCUP/UEPB - 2014)**

Um estagiário executou o comando FTP no servidor Linux. Esse comando possibilita

- A) permitir a abertura de portas para um acesso remoto a um servidor da rede.
- B) realizar a manutenção de disco e de memória de um computador remotamente.
- C) trocar informações de desempenho de redes utilizando um canal de comunicação protegido e exclusivo.
- D) realizar uma verificação de permissões de acesso na rede e no computador que o usuário está utilizando.
- E) trocar arquivos entre computadores interligados, independente do sistema operacional e da rede utilizada.

**Comentários:**

O comando ftp, tanto no Linux como no Windows, chama o cliente FTP, que permite trocar arquivos entre computadores interligados, independente do sistema operacional e da rede utilizada. Por exemplo, um cliente FTP Linux pode se conectar a um servidor FTP Windows e tudo irá funcionar tranquilamente.

**Gabarito: E**

---

**51.(VUNESP/SAAE de Barretos-SP - 2018)**

Os serviços de acesso a dados da internet são disponibilizados em uma arquitetura Cliente/Servidor. Por exemplo, considerando um servidor com sistema operacional Linux, o serviço padrão que responde às requisições ftp é denominado

- A) ftpd.
- B) ftps.
- C) ftpsrv.
- D) samba.
- E) smb.

**Comentários:**

Seguindo a lógica adotada para servidores no Linux, o servidor FTP é executado através de um daemon, o ftpd (geralmente o daemon tem o nome do serviço, acrescido de um “d” no fim).

**Gabarito: A**



## SMTP (SIMPLE MAIL TRANSFER PROTOCOL)

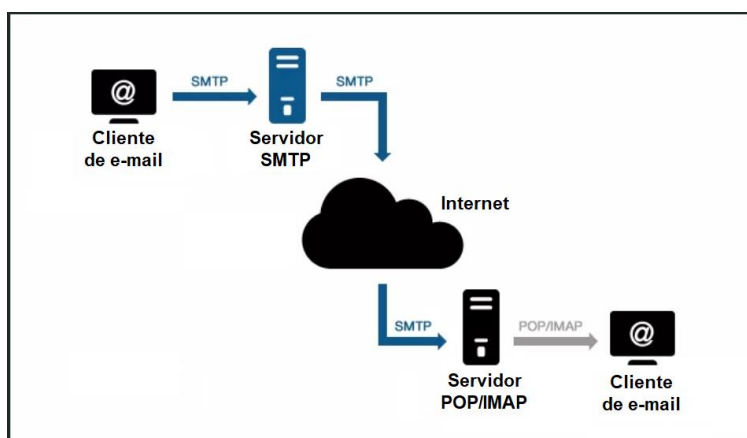
Antes de compreender como funciona o serviço (servidor) de e-mail no Linux, é importante entender a diferença dos 3 protocolos mais utilizados para esse serviço. Esqueça por um instante a utilização de HTTP ou HTTPS, no caso dos Webmails, vamos focar nos protocolos exclusivos para e-mail mesmo, vamos lá...

**SMTP** (*Simple Mail Transfer Protocol*): utilizado quando o e-mail é entregue a partir de um cliente de e-mail (Outlook, Thunderbird, entre outros) a um servidor de e-mail ou quando o e-mail é entregue a partir de um servidor de e-mail para outro servidor. Ou seja, se você enviar um e-mail a partir de um software cliente, ele utilizará o SMTP até o seu servidor e depois o seu servidor utilizará também o SMTP para entregar ao servidor destino, quando este ficará na caixa de e-mails do usuário destinatário. **A porta padrão de um servidor SMTP é a 25.**

**IMAP** (*Internet Message Access Protocol*): também chamado de IMAP4, possui acesso a todas as pastas da conta de e-mail e deixa o *status* das mensagens igual tanto no servidor como no software e realiza a sincronia das mensagens, mantendo a conexão para que as alterações e mensagens novas recebidas sejam atualizadas quase que em tempo real. **A porta padrão de um servidor IMAP é a 143.**

**POP** (Post Office Protocol): mais conhecido como POP3, esse protocolo baixa as mensagens do servidor e as armazena localmente no computador, não deixando uma cópia das mensagens no servidor (a menos que seja marcada a opção “deixar uma cópia no servidor”) nas configurações do programa de e-mail. Esse protocolo tem acesso apenas à Caixa de Entrada, não conseguindo baixar nenhuma outra pasta da conta de e-mail. **A porta padrão de um servidor POP3 é a 110.**

Abaixo podemos ver o relacionamento entre os 3 protocolos.



Podemos ver que a diferença principal é que o POP baixa as mensagens para o cliente local (permite que elas sejam armazenadas no servidor, mas não existe sincronia nesse processo).

O IMAP4 é a evolução do POP3, sincronizando a caixa de e-mails com o conteúdo do servidor, permitindo que um e-mail seja sincronizado entre vários locais sem perda de mensagens entre locais diferentes (salvo diretórios locais, todas as mensagens dentro do diretório do e-mail são sincronizadas).





No Linux, os servidores de e-mail mais comuns são o **sendmail** e o **postfix**. O postfix é considerado um MTA (Mail Transfer Agent) que se apresenta como alternativa ao sendmail, tendo como objetivo ser mais rápido, seguro e fácil de configurar que o sendmail, além de tentar manter a compatibilidade com ele. Vamos ver um pouco dos arquivos de configuração e funcionamento do postfix a seguir.

O postfix contém um arquivo denominado **main.cf**, no qual estão as configurações gerais do daemon, localizado no diretório **/etc/postfix**, pela instalação padrão. Abaixo serão demonstrados os principais parâmetros de configuração para ter-se um servidor de e-mail funcional. Nos exemplos abaixo será utilizado o nome do servidor como "mail.dominio.com.br" e o domínio "dominio.com.br", apenas para ilustração.

```
myhostname = mail.dominio.com.br
```

```
mydomain = dominio.com.br
```

O parâmetro "mydestination" deve receber os domínios que o servidor de e-mail é responsável. Por exemplo, mail.dominio.com.br, ftp.dominio.com.br, www.dominio.com.br, dominio2.com.br etc.:

```
mydestination = $myhostname, localhost.$mydomain, $mydomain, mail.$mydomain,  
www.$mydomain, dominio2.com.br
```

O parâmetro "mynetworks" serve para determinar as redes do provedor:

```
mynetworks = 192.168.0.0/16, 127.0.0.0/8
```

Também podem ser informados os domínios em um arquivo:

```
mynetworks = /etc/postfix/mynetworks
```

Pela configuração padrão do postfix, ele permite relay de e-mails das suas redes e de seus domínios. Se houver clientes que não fazem parte da rede e que necessitam utilizar o seu servidor de e-mail para o envio de mensagens, é possível criar um arquivo com a lista de clientes através do parâmetro "smtpd\_recipient\_restrictions" e habilitar o envio de mensagens, como mostrado abaixo:

```
smtpd_recipient_restrictions = permit_mynetworks
```

```
check_client_access hash:/etc/postfix/client_access
```

```
check_relay_domains
```

Exemplo do arquivo /etc/postfix/client\_access:

```
dial.amigos.com.br OK
```

```
10.0.0 OK
```

```
falcatrua.com.br REJECT
```



Esse parâmetro não consta na configuração padrão do postfix e pode ser incluído no final do arquivo de configuração main.cf.

A **entrega de e-mails no postfix** pode ser feita de diversas formas: enviando os e-mails para `"/var/spool/mail/user"` (padrão), no formato `"Maildir/"` (utilizado pelo gmail) entre outros.

**Iniciando o servidor:** # postfix start

Caso seja feita alguma alteração na configuração do servidor de e-mail, para atualizá-lo, basta digitar o comando: # postfix reload

Para desativar o servidor de e-mail: # postfix stop

Uma característica importante no Linux são os logs, que, na sua maioria, são armazenados em `/var/log`. Esse é o caso também dos logs relacionados aos servidores de e-mail, útil quando são necessárias informações sobre postfix, smtpd ou qualquer serviço relacionado ao e-mail que esteja sendo executado no servidor. Por padrão, esses logs ficam em `/var/log/maillog` ou `/var/log/mail.log`.

## QUESTÕES COMENTADAS

### 52.(FUNIVERSA/PC-DF - 2012)

Em um servidor de e-mail com sistema operacional Linux, especialmente quando se utiliza o serviço Postfix, pode-se auditar o tráfego de entrada e saída de mensagens de correio eletrônico por meio dos registros conhecidos por logs. Em que arquivo desse sistema operacional encontram-se os logs das atividades de envio e recebimento de mensagens de correio eletrônico (e-mail)?

- A) No diretório `"/etc/postfix"`.
- B) No arquivo `"/var/log/maillog"`.
- C) Na pasta `"/var/mail/<nome_do_usuario>"`.
- D) No arquivo `"/usr/local/bin/postfix"`.
- E) No arquivo de registro `"/dev/tty"`.

#### Comentários:

Uma característica importante no Linux são os logs, que, na sua maioria, são armazenados em `/var/log`. Esse é o caso também dos logs relacionados aos servidores de e-mail, útil quando são necessárias informações sobre postfix, smtpd ou qualquer serviço relacionado ao e-mail que esteja sendo executado no servidor. Por padrão, esses logs ficam em `/var/log/maillog` ou `/var/log/mail.log`.

**Gabarito: B**

### 53.(FUNCAB/MDA - 2014)

São exemplos de servidores de correio eletrônico do Linux:

- A) postfix e sendmail.



- B) fetchmail e sendmail.
- C) pine e postfix.
- D) mail e pine.
- E) samba e postfix.

**Comentários:**

Alguns exemplos de servidores de e-mail no Linux: qmail, postfix e sendmail.

**Gabarito: A**

---

**54.(FGV/TJ-GO - 2014)**

A empresa Y passou a adotar uma política de uso de software livre e resolveu mudar o seu correio eletrônico, que era baseado em Microsoft Exchange. O novo ambiente deveria rodar em ambiente Linux. Uma das possíveis escolhas do novo software de correio eletrônico recai no programa:

- A) nginx;
- B) puppet;
- C) apache;
- D) postfix;
- E) bind.

**Comentários:**

Alguns exemplos de servidores de e-mail no Linux: qmail, postfix e sendmail.

**Gabarito: D**

---

**55.(FCC/Prefeitura de Manaus-AM - 2019)**

Um Assistente de TI foi incumbido de configurar o protocolo para ser utilizado na troca de mensagens entre dois servidores de e-mail. A escolha correta do protocolo para essa finalidade é:

- A) IMAP.
- B) POP3.
- C) SNMP.
- D) SMTP.
- E) POP4.

**Comentários:**

SMTP (Simple Mail Transfer Protocol): utilizado quando o e-mail é entregue a partir de um cliente de e-mail (Outlook, Thunderbird, entre outros) a um servidor de e-mail ou quando o e-mail é



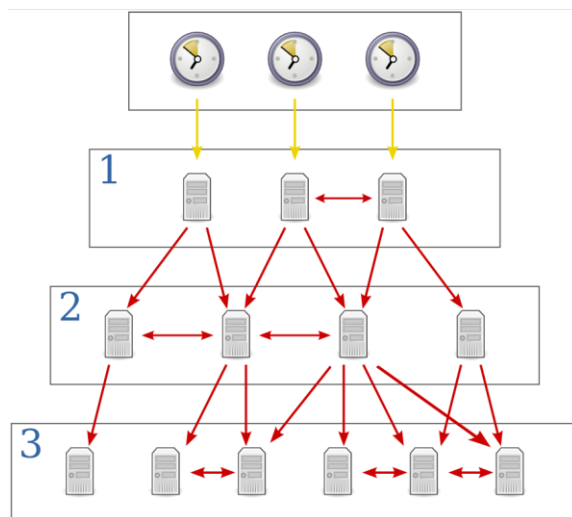
entregue a partir de um servidor de e-mail para outro servidor. Ou seja, se você enviar um e-mail a partir de um software cliente, ele utilizará o SMTP até o seu servidor e depois o seu servidor utilizará também o SMTP para entregar ao servidor destino, quando este ficará na caixa de e-mails do usuário destinatário. A porta padrão de um servidor SMTP é a 25.

**Gabarito: D**

## NTP (NETWORK TIME PROTOCOL)

O NTP, ou Protocolo de Tempo para Redes, é o protocolo que permite a sincronização dos relógios dos dispositivos de uma rede, tais como servidores, estações de trabalho, roteadores e outros equipamentos, a partir de referências de tempo confiáveis.

**Arquitetura do NTP:** os servidores NTP formam uma topologia hierárquica, dividida em camadas ou estratos (em inglês: *strata*), numerados de 0 a 16. O estrato 0, na verdade, não faz parte da rede de servidores NTP, mas representa a referência primária de tempo, que é geralmente um receptor do Sistema de Posicionamento Global (GPS) ou um relógio atômico. O estrato 16 indica que um determinado servidor está inoperante. Abaixo vemos a topologia em estratos (camadas):



O estrato 0 (relógio de referência) fornece o tempo correto para o estrato 1, que por sua vez fornece o tempo para o estrato 2 e assim por diante. O NTP é então, simultaneamente, servidor (fornece o tempo) e cliente (consulta o tempo).

De forma geral, quanto mais perto da raiz, ou seja, do estrato 0, maior a exatidão do tempo. O estrato ao qual o servidor pertence é a principal métrica utilizada pelo NTP para escolher dentre vários, qual o melhor servidor para fornecer o tempo.

Por outro lado, normalmente as diferenças de exatidão entre os estratos não são expressivas e há, no momento de escolher um conjunto de servidores de tempo para configurar um determinado



cliente, outros fatores a se considerar, como por exemplo a carga à qual os servidores estão submetidos, e o atraso de rede.

O estrato de um servidor não é uma característica estática. Se houver perda de conexão com as fontes de tempo, ou outros fatores que modifiquem a topologia da rede, o estrato pode variar. Ao consultar a lista de servidores no daemon NTP (comando **ntpq** – o “q” é de “query”), o estrato (st) é informado, entre outras informações:

```
usuario@cliente.local:~$ ntpq -c pe
  remote      refid      st  t when poll reach  delay  offset  jitter
=====
-servidor1    .IRIG.      1  u   8   32  377   0.407   0.248   0.016
-servidor2    .GPS.       1  u   -   32  377   0.474   0.213   0.019
+servidor3    .GPS.       1  u   9   64  377  15.680  -0.005   0.026
+servidor4    .IRIG.      1  u  30   64  377  15.582   0.004   0.100
*servidor5    .GPS.       1  u  10   32  377   0.400  -0.026   0.049
xservidor6    .IRIG.      1  u  26   64  377   7.824   9.923   0.367
```

O parâmetro “-c” especifica um comando de formato interativo, adicionando a uma lista de comandos a serem executados. Múltiplas flags podem ser adicionadas com o “-c”. Por exemplo, para adicionar um intervalo de tempo de 1000 milissegundos aos timestamps: **ntpq -c “delay 1000”**.

Enquanto o “**ntpq -c pe**” apresenta as variáveis relacionadas a cada associação, ou seja, a cada fonte de tempo, “o **ntpq -c rl**” apresenta as variáveis (globais) do sistema. As mais importantes estão indicadas na tabela a seguir.

Variável	Significado
version	Versão do ntp.
stratum	Estrato do servidor local.
precision	Precisão indicada com o expoente de um número base 2.
rootdelay	Atraso ou tempo de ida e volta dos pacotes até o estrato 0, em milissegundos.
rootdisp	Erro máximo da medida de offset em relação ao estrato 0, em milissegundos.
refid	O par do sistema, ou principal referência.
offset	Deslocamento, quanto o relógio local tem de ser adiantado ou atrasado para chegar à hora certa (hora igual à do estrato 0).
frequency	Erro na frequência do relógio local, em relação à frequência do estrato 0, em partes por milhão (PPM).



```
%ntpq -c rl
```

```
associd=0 status=0614 leap_none, sync_ntp, 1 event, freq_mode,  
version="ntpd 4.2.6p5@1.2349-o Mon Apr 13 13:39:46 UTC 2015 (1)",  
processor="x86_64", system="Linux/3.13.0-36-generic", leap=00, stratum=2,  
precision=-22, rootdelay=9.141, rootdisp=155.934, refid=200.186.125.195,  
reftime=d934225c.0e476dff Tue, Jun 23 2015 15:22:20.055,  
clock=d9342283.bf40eca3 Tue, Jun 23 2015 15:22:59.747, peer=59316, tc=6,  
mintc=3, offset=9.460, frequency=1.909, sys_jitter=5.893,  
clk_jitter=2.077, clk_wander=0.978
```

Como a maioria dos arquivos de configuração, o diretório padrão é o **/etc** e o arquivo de configuração é o **"ntp.conf"**.

## QUESTÕES COMENTADAS

### 56.(INSTITUTO AOCP/UFGD - 2014)

Em algumas distribuições Linux, podemos encontrar um arquivo que inclui as informações necessárias para executar o Protocolo para Sincronizar o Relógio da Rede (NTP). Assinale a alternativa que apresenta o nome deste arquivo.

- A) ntp.conf
- B) ntp.conf.
- C) ntpsync.conf.
- D) nsync.conf.
- E) clock.conf.

#### Comentários:

Como a maioria dos arquivos de configuração, o diretório padrão é o **/etc** e o arquivo de configuração é o **"ntp.conf"**.

**Gabarito: A**

### 57.(FCC/SANASA - 2019)

Considerando que o NTP – Network Time Protocol é um protocolo que permite a sincronização dos relógios dos dispositivos de uma rede a partir de referências de tempo confiáveis, um Analista de TI digitou um comando no Linux, em condições ideais, que mostrou o resultado abaixo.

remote	refid	st	t	when	poll	reach	delay	offset	jitter
+a.ntp.br	200.160.7.192	2	u	10	64	337	294.756	35.596	0.521
+b.ntp.br	200.160.7.186	2	u	8	64	377	226.294	2.658	0.229
*c.ntp.br	200.160.7.192	2	u	-	64	377	208.758	4.026	0.424



O comando digitado foi

- A) `ntp -c ls`
- B) `ntpq -c pe`
- C) `ntpq > rv &1`
- D) `ntp -s pe`
- E) `ntpq -c rl`

#### Comentários:

O parâmetro “-c” especifica um comando de formato interativo, adicionando a uma lista de comandos a serem executados. Múltiplas flags podem ser adicionadas com o “-c”. Por exemplo, para adicionar um intervalo de tempo de 1000 milissegundos aos timestamps: `ntpq -c “delay 1000”`.

Enquanto o “`ntpq -c pe`” apresenta as variáveis relacionadas a cada associação (exemplo abaixo), ou seja, a cada fonte de tempo, “o `ntpq -c rl`” apresenta as variáveis (globais) do sistema.

```
usuario@cliente.local:~$ ntpq -c pe
  remote      refid      st  t when poll reach  delay  offset  jitter
=====
-servidor1    .IRIG.       1  u   8   32  377   0.407   0.248   0.016
-servidor2    .GPS.        1  u   -   32  377   0.474   0.213   0.019
+servidor3    .GPS.        1  u   9   64  377  15.680  -0.005   0.026
+servidor4    .IRIG.       1  u  30   64  377  15.582   0.004   0.100
*servidor5    .GPS.        1  u  10   32  377   0.400  -0.026   0.049
xservidor6    .IRIG.       1  u  26   64  377   7.824   9.923   0.367
```

**Gabarito: B**

## LISTA DE QUESTÕES

### 1. (2010 - CESPE - SERPRO)

O CUPS tem a característica de ser plug-and-play no lado cliente; portanto, basta configurar o servidor e instalar o CUPS nos clientes.

### 2. (2010 - CESPE - SERPRO)

O CUPS é um sistema de impressão compatível com o protocolo IPP (Internet printing protocol) que suporta impressoras não PS (PostScript), porém não suporta impressoras PS.





### 3. (2011 - CESPE - MEC)

No caso do CUPS, recomenda-se utilizar o endereço de loopback do servidor para tarefas de administração, a fim de evitar a transmissão da senha de root em texto claro com o protocolo HTTP.

---

### 4. (2011 - CESPE - MEC)

Considerando que, em um ambiente de rede, exista um servidor de impressão em Windows Server 2003 e outro servidor de impressão em Linux que utilize o sistema CUPS, julgue os itens subsequentes.

O CUPS anuncia seu serviço de impressão por meio de broadcast e usa por padrão a porta UDP 300. Nesse caso, a configuração padrão do CUPS pode ser alterada para uso apenas de multicast.

---

### 5. (2013 - CESPE - SERPRO)

Mecanismos do CUPS possibilitam o compartilhamento de arquivos entre o Windows e o Linux.

---

### 6. (2014 - IADES - EBSERH)

O CUPS é o sistema de impressão usado atualmente na maioria dos sistemas Linux. A adição de novas impressoras pode ser feita através da sua interface web, que em sua configuração padrão, armazena as informações das impressoras na pasta

- A) /etc/printers
- B) /etc/cups/printers
- C) /etc/cups/ppd
- D) /dev/prn
- E) /dev/interfaces/printers

---

### 7. (2014 - VUNESP - PRODEST-ES)

Nos sistemas operacionais Linux, o CUPS é um serviço responsável pelo gerenciamento de

- A) arquivos compartilhados.
- B) trabalhos de impressão.
- C) mensagens de fax.
- D) mensagens eletrônicas (e-mail).



E) usuários da rede.

---

**8. (2016 - UFV - UFV-MG)**

O administrador do setor de Tecnologia da Informação precisa compartilhar as impressoras da empresa para que os funcionários possam imprimir seus trabalhos. Para isso, ele tem que montar um servidor de impressão com Sistema Operacional Linux.

São serviços do Sistema Operacional Linux que permitem o compartilhamento de impressoras:

- A) CUPS, SAMBA
- B) SAMBA, APACHE
- C) APACHE, FTP
- D) FTP, CUPS

---

**9. (2017 - IBFC - EBSERH)**

Assinale a alternativa correta. Para permitir que um computador seja um servidor de impressão em um ambiente Unix-like de forma que se possa monitorar impressões, relatar erros de impressão, visualizar relatórios sobre número de páginas impressas, etc. usa-se:

- A) PGREP
- B) CUPS
- C) CHROOT
- D) CRON
- E) PRINTF

---

**10.(2018 - CESPE - EBSERH)**

CUPS é uma solução para conectar impressoras ao sistema roteador da rede de computadores, a fim de disponibilizar o equipamento para a sua utilização via protocolo NETBIAS.

---

**11.(2018 - UFU-MG - UFU-MG)**

No Linux, podem-se utilizar impressoras diretamente conectadas ao desktop, por exemplo, por meio de uma porta USB ou impressoras disponíveis na rede e configurá-las com o CUPS (Common UNIX Printing System).

Com base no CUPS, assinale a alternativa correta.



- A) O arquivo regular de configuração do CUPS armazenado no “home” do usuário, por exemplo, “/home/usuario/.cups.configuracao”, contempla todas as informações de permissões e de autenticações, servidor de impressão e opções de impressoras configuradas.
- B) No CUPS, ao se configurar uma impressora, essa será sempre disponibilizada a partir de nomes transmitidos na rede. Trata-se de um recurso no qual não é permitido ao usuário esconder de outros usuários uma impressora na rede.
- C) Pode-se configurar o CUPS no navegador por meio da interface “http://localhost:631” desde que o “daemon” CUPS de impressão ou “cupsd” esteja em execução.
- D) Para adicionar uma impressora local a partir da linha de comando independentemente do perfil do usuário, por exemplo, usuário comum, basta executar na linha de comando “config-printer” e, após a janela ser aberta, selecionar “New Printer”.

---

### 12.(2019 - FCC - Prefeitura de Manaus-AM)

Em computador com sistema operacional Linux e o OpenLDAP instalado, o programador editou o arquivo ldap.conf para configurar

- A) a autenticação do servidor.
- B) a execução do serviço do LDAP.
- C) o banco de dados a ser utilizado.
- D) a geração de índices do banco de dados.
- E) o acesso dos clientes ao diretório.

---

### 13.(CESPE – 2018 – Polícia Federal – Perito Criminal Federal - Área 3)

Julgue o item que se segue, a respeito de DNS (domain name service).

As atualizações entre servidores DNS utilizam o UDP, enquanto as consultas feitas a servidores DNS utilizam o TCP (ou, opcionalmente, o SCTP).

---

### 14. (2018 - IF-RS - IF-RS - Técnico de Laboratório - Informática)

Considerando que se está logado como “root” no terminal de uma estação de trabalho com um sistema operacional Linux debian ou derivado, qual comando configura o DNS para 8.8.8.8?

- A) dns 8.8.8.8
- B) echo 8.8.8.8 > /etc/hosts.conf
- C) echo nameserver 8.8.8.8 > /etc/resolv.conf



- D) nslookup 8.8.8.8
- E) nameserver 8.8.8.8

---

**15.(FAURGS – 2018 – BANRISUL – Suporte a Infraestrutura de TI)**

Um cliente DNS, ao fazer a requisição DNS para resolver o nome `www.banrisul.com.br`, recebe como resposta uma mensagem do tipo `non authoritative`. Esse tipo de resposta é obtido por meio de um registro DNS (`resource record – RR`) armazenado

- A) em um cache de DNS.
- B) em um servidor interativo sem cache DNS.
- C) em um servidor recursivo sem cache DNS.
- D) no arquivo de zona do DNS primário.
- E) no arquivo de zona do DNS secundário.

---

**16. (2018 - FAPEC - UFMS - Técnico de Tecnologia da Informação)**

Considere as afirmações a seguir sobre a instalação e configuração de um servidor de DNS (Bind9) no sistema operacional Debian 9.

I - Quando o servidor local de DNS não consegue traduzir o nome, ele deve solicitar a um servidor público (`forwarders`). O Google Public DNS é um exemplo de `forwarders` e deve ser configurado no arquivo `named.conf.options`.

II - A instalação do servidor pode ser realizada pelo usuário `root` com o comando: `apt install bind9 bind9-doc dnsutils`

III - A lista de controle de acessos ou ACL é definida no arquivo `named.conf.options`.

Está(ão) correta(s):

- A) Apenas I.
- B) Apenas II.
- C) Apenas III.
- D) Apenas II e III.
- E) I, II e III.

---

**17.(2018 - CESPE - EMAP - Analista Portuário - Tecnologia da Informação)**

Acerca de sistemas operacionais Linux, julgue o item que segue.

Em um servidor DNS que esteja utilizando Bind, o arquivo `/etc/named.conf` mantém as configurações de funcionamento do serviço DNS. Nesse servidor, é possível configurar a porta que



deve escutar o serviço; assim, para que o serviço escute a porta 53, deve-se configurar a opção seguinte.

Listening 53 { any;;

---

**18.(IBFC – 2017 – Polícia Científica-PR – Perito Oficial/Perito Criminal/Área 1)**

Servidores de DNS (Domain Name System) têm como função converter endereços IP em seu respectivo nome e vice-versa. Para sua configuração, são utilizados arquivos denominados mapas de domínio (zone). Esses arquivos são compostos por entradas chamadas RR (Resource Record). O tipo básico de RR que estabelece a correspondência entre um nome canônico e um endereço IP é indicado por:

- A) PTR
- B) MX
- C) NS
- D) A
- E) SOA

---

**19.(IBFC – 2017 – Polícia Científica-PR – Perito Oficial/Perito Criminal/Área 1)**

Servidores DNS (Domain Name Server) são responsáveis pela conversão do nome dos diversos servidores espalhados pela Internet para seu número IP e vice-versa. Servidores de DNS trabalham de forma colaborativa e hierárquica. Assinale a alternativa a que apresenta o nome dado aos servidores que se encontram no topo da hierarquia de DNS:

- A) Root Name Servers
- B) Main servers
- C) International Name Servers
- D) Controllers Servers
- E) Master Servers

---

**20.(FGV – 2016 – COMPESA – Analista de Saneamento/Engenheiro de Telecomunicações)**

O sistema de Nomes de Domínio – DNS permite transformar nomes digitados em um navegador WEB em um endereço de rede. O nome do host e o nível do domínio para o domínio “system.master.com” são, respectivamente,

- A) system e segundo nível.
- B) system e terceiro nível.
- C) master e terceiro nível.



- D) master e segundo nível.
- E) .com e terceiro nível.

---

**21. (FCC – 2016 – PRODATER – Analista Tecnológico/Analista de Suporte Técnico)**

No Serviço de Nomes de Domínio – DNS existem diferentes tipos de servidores distribuídos hierarquicamente que armazenam informações também de forma hierárquica. Considerando o nome: www.empresa.com, o domínio .com é gerenciado pelo servidor

- A) Global.
- B) PDR.
- C) Authoritative.
- D) TLD.
- E) Root.

---

**22. (IBFC – 2016 – EBSERH-HUAP – Técnico/Informática)**

O Domain Name System (DNS) é um sistema de gerenciamento de nomes hierárquicos e distribuídos. A funcionalidade do DNS Reverso vem a ser:

- A) reverter a funcionalidade básica de um DNS padrão obtendo o endereço MAC.
- B) resolver um endereço IP, buscando o nome de domínio associado ao host.
- C) resolver o nome do domínio de um host qualquer para seu endereço IP correspondente.
- D) com base na região geográfica, obter automaticamente um endereço IP local.
- E) resolver o problema da reversão do IPv6 para o IPv4 de uma forma rápida e automática.

---

**23. (FUNRIO – 2016 – CM Nova Iguaçu – Técnico/Informática)**

Um administrador de rede está configurando o DNS de um servidor e vai trabalhar com o registro que define as características da zona a ser configurada, tais como, o nome da zona e o nome do servidor, que é a autoridade para a referida zona, ou seja, o servidor DNS no qual está a zona que foi criada originalmente. Esse registro é conhecido pela sigla

- A) HINFO.
- B) MX.
- C) SOA.
- D) CNAME.



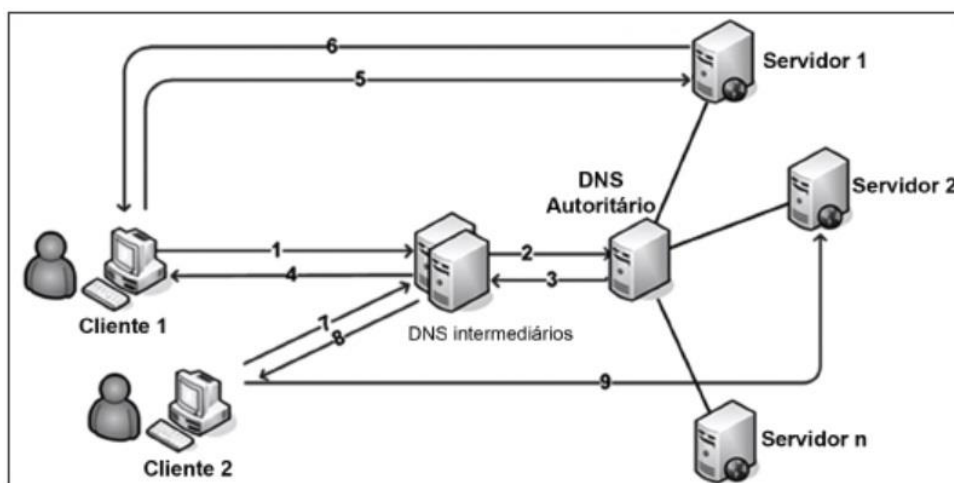
#### 24. (CESPE – 2016 – TCE-PR – Analista de Controle/Tecnologia da Informação)

Uma consulta DNS inicial típica, originada de uma máquina de usuário e encaminhada ao servidor de nomes local para um nome de domínio externo não armazenado em cache DNS, será do tipo

- A) raiz.
- B) domínio de alto nível.
- C) iterativa.
- D) recursiva.
- E) direta.

#### 25. (FCC – 2016 – ELETROSUL – Profissional de Nível Superior/Informática)

O balanceamento de carga por DNS é uma abordagem popular e simples para as solicitações de balanceamento de servidores. Considere a figura abaixo.



De acordo com a figura, geralmente são estes os passos que ocorrem assim que é feita uma consulta DNS:

1. Quando um cliente tenta acessar o site, é realizada uma pesquisa no DNS local para determinar qual é o endereço I..... correspondente;
2. O pedido de endereço chega ao servidor de DNS II..... do domínio;
3. A primeira vez que esta consulta é feita, o servidor DNS remoto pode retornar todos os registros de endereços que ele tem para o site;
4. O servidor DNS III....., em seguida, determina o endereço de registro para retornar ao cliente;
5. Se todos os registros são retornados, o cliente utilizará o primeiro que lhe é atribuído;
6. O servidor responde ao cliente e atende ao pedido;
7. A cada pedido, o algoritmo Round Robin roda os endereços e retorna pela ordem em que eles estão;





8 . Cada consulta DNS irá resultar em um cliente usando um endereço IV.....;

9. Esta rotação de endereços irá distribuir pedidos para os servidores.

As lacunas de I a IV são, correta e respectivamente, preenchidas com:

- A) TCP – autoritário – local – TCP igual ao obtido em 1
- B) IP – autoritário – local – IP diferente
- C) do servidor – local – autoritário – de um servidor
- D) do servidor – autoritário – local – do servidor igual ao obtido em 1
- E) IP – local – autoritário – IP igual ao obtido em 1

---

**26.(CESPE – 2016 – TCE-SC – Auditor Fiscal de Controle Externo/Controle Externo/Informática)**

Acerca de redes de computadores e de protocolos TCP/IP, julgue o item a seguir.

Após o servidor local SMTP aceitar uma mensagem para subsequente envio, é necessário determinar o endereço do servidor de email do destinatário. Essa etapa é realizada mediante consulta DNS a um servidor de nomes capaz de prover a informação, no qual serão verificados os registros especiais MX (mail exchange).

---

**27. (CESPE – 2016 – Polícia Científica-PE – Perito Criminal/Área 7/Ciência da Computação, Engenharia da Computação ou Sistemas de Informação)**

Na operação de um serviço DNS, se uma consulta a um servidor de alto nível retornar uma resposta positiva para o servidor DNS local, o mapeamento nome/endereço será

- A) armazenado definitivamente no banco de dados do servidor DNS local.
- B) replicado para todos os servidores DNS alcançáveis para que estejam disponíveis a outras consultas.
- C) repassado pelo módulo tradutor a um servidor raiz para confirmar a resposta recebida.
- D) armazenado em cache local e pode ser mantido por um tempo definido por configuração.
- E) repassado ao módulo tradutor do provedor de serviços para realizar a entrega à aplicação.

---

**28.(FCC – 2015 – CNMP – Analista/Tecnologia da Informação e Comunicação/Suporte e Infraestrutura)**

O serviço de nome de domínios (DNS) possui uma arquitetura do tipo cliente/servidor na qual a base de dados é distribuída por toda internet. Nessa arquitetura, o acesso ao servidor DNS para buscar o relacionamento IP/Domínio é feito pelo cliente que é o

- A) Browser.



- B) DNS Cache.
- C) DNS Resolver.
- D) DNS Searcher.
- E) Gateway.

---

**29.(CESPE – 2015 – FUB – Técnico/Tecnologia da Informação)**

Acerca da arquitetura TCP/IP, julgue o item a seguir.

O protocolo DNS (domain name service), localizado no nível de aplicação da camada de transporte do TCP, é responsável pelo mapeamento de nomes e de endereços.

---

**30.(FGV – 2015 – TCE-SE – Analista de Tecnologia da Informação/Desenvolvimento)**

Um programa precisa simular o comportamento de um cliente DNS. Para funcionar adequadamente, o programa precisa enviar as consultas para um servidor DNS, especificamente para a sua porta:

- A) udp/23
- B) icmp/34
- C) tcp/22
- D) ip/50
- E) udp/53

---

**31.(CESPE – 2015 – TRE-MT – Técnico Judiciário/Apoio Especializado/Programação de Sistemas)**

Acerca do servidor DNS/BIND (Domain Name System/Berkley Internet Domain), cuja funcionalidade é resolver nomes da rede, assinale a opção correta.

- A) Cada domínio tem seus registros de recursos e o registro de domínio denominado NS (name server), o qual é utilizado para definir propriedades básicas do domínio e sua zona.
- B) Um servidor DNS utiliza LDAP para fazer armazenamento das zonas de domínio para uma rápida resolução de um nome.
- C) O BIND, que utiliza a porta 53, é um programa de código aberto utilizado pela maior parte dos servidores DNS.
- D) Os domínios de um servidor DNS são organizados na Internet sobre uma estrutura de dados do tipo lista encadeada, sendo o primeiro elemento da lista um ponto.
- E) O protocolo HTTP implementa, por padrão, um servidor de resolução de nomes amplamente utilizado na Internet conhecido como DNS.



---

**32.(IADES – 2015 – CRC-MG – Analista de Sistemas)**

Quanto ao programa que é normalmente utilizado para testar se um servidor DNS (Domain Name Server) está funcionando corretamente, ou seja, resolvendo nomes para os endereços IP, assinale a alternativa correta.

- A) ping
- B) tracert
- C) nslookup
- D) ipconfig
- E) net host

---

**33. (2015 - FGV - TCE-SE - Analista de Tecnologia da Informação-Suporte Técnico em Infraestrutura e Redes)**

Em um equipamento rodando Linux, um administrador deseja alterar o endereço default do servidor DNS usado para consultas. Para isso, ele precisa alterar o arquivo:

- A) /etc/named.conf
- B) /etc/bind.conf
- C) /etc/network.conf
- D) /etc/dns.conf
- E) /etc/resolv.conf

---

**34. (2014 - AOC - UFPA - Analista de Tecnologia da Informação - Suporte e Redes)**

Em algumas distribuições Linux encontramos um arquivo que identifica os locais dos computadores de servidor de nome DNS, computadores estes que são usados pelo TCP/IP para traduzir os nomes de Internet. Assinale a alternativa que apresenta o nome deste arquivo.

- A) DNS.conf.
- B) resolver.conf.
- C) resolv.conf.
- D) translate.conf.
- E) change.conf.



**35.(2014 - IADES - TRE-PA - Técnico Judiciário - Operação de Computador)**

Um servidor Linux pode hospedar o serviço de resolução de nomes de uma rede de computadores. Conhecido por DNS, esse serviço é indispensável em uma rede que possua conexão com a internet. O nome de um pacote que implementa o DNS, muito utilizado em sistemas operacionais Linux, é

- A) Firefox.
- B) Apache.
- C) Squid.
- D) Postfix.
- E) BIND.

---

**36.(2010 - FCC - TCE-SP - Auxiliar da Fiscalização Financeira)**

Em Linux, o `/etc/resolv.conf` é um arquivo texto simples, com um parâmetro por linha e especificações de endereços de servidores DNS. Nesse arquivo existem três palavras chaves normalmente usadas, que são

- A) domain, search e resolv.
- B) search, resolv e order.
- C) domain, search e nameserver.
- D) search, nameserver e order.
- E) search nameserver e resolv.

---

**37.(2010 - FCC - TCE-SP - Auxiliar da Fiscalização Financeira)**

No Linux, ele é muito útil para máquinas que são acessadas frequentemente, pois a inclusão de um computador neste arquivo dispensa a consulta a um servidor DNS para obter um endereço IP, sendo muito útil para máquinas que são acessadas frequentemente. Trata-se de:

- A) `/etc/nameserver`
- B) `/etc/localhost`
- C) `/etc/ipsec`
- D) `/etc/hosts`
- E) `/etc/dnshost`

---

**38.(2009 - FGV - MEC - Gerente de Suporte)**

No UNIX, o DNS é implementado por meio do software Berkeley Internet Name Domain (BIND), que segue a filosofia cliente/servidor.



O cliente do BIND é denominado "resolver", responsável por gerar as "queries" enquanto que o servidor do BIND é chamado por "named", responsável por responder às "queries".

Configurações BIND são descritas pelo tipo de serviço a ser executado pelo software, existindo quatro níveis de serviço que podem ser definidos nessas configurações: "resolver-only systems", "caching-only servers", "primary servers" e "secondary servers".

Os parâmetros que definem a configuração do "resolver-only systems" são inseridas no seguinte arquivo:

- A) /etc/resolv.sys
- B) /etc/resolv.cfg
- C) /etc/resolv.bind
- D) /etc/resolv.conf
- E) /etc/resolv.parm

---

### 39.(2013 - CESPE - TRT8)

Para alterar o arquivo de configuração do serviço de DHCP no Linux, deve-se acessar o diretório

- A) /dev.
- B) /mnt.
- C) /etc.
- D) /usr/bin.
- E) /boot.

---

### 40.(2018 - SUGEP-UFRPE - UFRPE)

Para acesso à Internet, servidores Windows e Linux utilizam um serviço para atribuição dinâmica de IPs aos microcomputadores conectados à rede, em que é marcada a opção associada a "o IP será atribuído automaticamente pelo servidor", na configuração.

Esse serviço é conhecido pela sigla:

- A) DNS
- B) HTTP
- C) DHCP
- D) TCP
- E) IP



#### **41.(2012 - FCC - TRT6)**

CIFS e NFS

- A) referem-se, respectivamente, às implementações para Unix e Windows de um mesmo protocolo que oferece a funcionalidade de sistema de arquivos distribuído.
- B) são diferentes implementações de um mesmo protocolo que oferecem a funcionalidade de sistema de arquivos distribuído.
- C) são, respectivamente, cliente e servidor de um mesmo protocolo que implementa a funcionalidade de sistema de arquivos distribuído.
- D) são diferentes protocolos que implementam a funcionalidade de sistema de arquivos distribuído.
- E) referem-se, respectivamente, às implementações para Windows e Unix de um mesmo protocolo que oferece a funcionalidade de sistema de arquivo distribuído.

---

#### **42.(2012 - COPESE-UFT - DPE-TO)**

Em relação ao NFS (Sistema de Arquivo de Rede) é correto afirmar, EXCETO:

- A) A ideia básica que fundamenta o NFS é que cada servidor de arquivos fornece uma visão padronizada de seu sistema local de arquivos.
- B) No NFS, toda comunicação cliente servidor é feita por meio de RPC (chamada de procedimento remoto).
- C) O NFS é, em grande parte, independente de sistemas locais de arquivos.
- D) O modelo de sistema de arquivos oferecido pelo NFS é bem diferente do oferecido por sistemas baseados em Unix.

---

#### **43.(2013 - FCC TRT18)**

O Sistema de Arquivo de Rede - NFS

- A) é um protocolo da camada de transporte (modelo TCP/IP) e um componente do diretório X.500.
- B) é um componente do diretório X.500 e oferece grande parte das funcionalidades de CIFS.
- C) viabiliza a um usuário remoto a conversação de voz sobre IP com um usuário local, quando encadeado com o protocolo LDAP.
- D) é um protocolo da camada de rede ( modelo TCP/IP) e oferece grande parte das funcionalidades de DAP.



E) permite que sejam acessados arquivos que se encontram armazenados em um servidor remoto como se eles estivessem instalados localmente.

---

**44.(2015 - FCC - TRT15)**

Dentre os diferentes sistemas de arquivos compatíveis com os sistemas operacionais Linux, o que apresenta a característica de ser nativamente especificado para o uso em rede de computadores é o

- A) Ext3
- B) NTFS.
- C) SMB.
- D) LDAP.
- E) NFS.

---

**45.(2015 - IBFC - EBSEH)**

No compartilhamento de arquivos e impressoras é tradicional, nos Sistemas Operacionais da Microsoft, a utilização do seguinte protocolo:

- A) ITU-T
- B) TLS/SSL
- C) RIPv2
- D) SMB/CIFS
- E) IPv6

---

**46.(2016 - AOC - EBSEH)**

O NFS (Network File System) permite compartilhar sistemas de arquivos entre computadores conectados em rede e pode ser parte fundamental da infraestrutura da tecnologia da informação. Sobre NFS, analise as assertivas a seguir e assinale a alternativa que aponta a(s) correta(s).

I. O NFS é considerado sem estado (stateless) e, portanto, quando um servidor NFS volta a funcionar, o estado anterior é restaurado e a informação não é perdida.

II. O NFS pode ser implementado do lado servidor e do lado cliente.

III. O NFS roda sobre o protocolo RPC (Remote Procedure Call), que define um modo independente do sistema para processos se comunicarem através de uma rede de computadores.





IV. O NFS suporta apenas UDP como protocolo de transporte, pois ele apresenta desempenho significativamente melhor que o TCP em redes locais.

- A) Apenas I e II.
- B) Apenas II e IV.
- C) Apenas III.
- D) Apenas III e I.
- E) Apenas I, II e III.

---

**47.(2018 - FCC - DPE-AM)**

O Common Internet File System – CIFS utiliza um conjunto de serviços agregados para prover meios de compartilhar arquivos, diretórios e impressora em uma rede de computadores. A resolução de nomes no CIFS é realizada pelo

- A) SMB.
- B) hostname.
- C) IPC.
- D) NETBios.
- E) WINS.

---

**48.(2019 - IF-ES - IF-ES)**

O Network File System (NFS) – Sistemas de Arquivos em Rede – tem como um dos principais propósitos dar suporte a um sistema heterogêneo, no qual clientes e servidores estejam possivelmente executando sistemas operacionais e hardwares diferentes. Sobre o NFS, é CORRETO afirmar:

- A) O NFS utiliza dois protocolos cliente-servidor, em que o primeiro é responsável pela montagem e o segundo é para acesso de diretório e arquivos.
- B) O servidor tem total gerência sobre o ponto de montagem nos clientes.
- C) Os serviços NFS são implementados apenas nos servidores Linux.
- D) Como critério de segurança, os clientes não podem ter acesso aos atributos dos arquivos.
- E) O NFS faz uso de máquinas distintas para servidores e clientes, impossibilitando que a mesma máquina seja tanto cliente quanto servidor



---

**49.(CESPE/HEMOBRÁS - 2008)**

Tanto o Linux quanto o Windows possuem softwares clientes para FTP (file transfer protocol) e que podem ser utilizados para a troca de arquivos em uma rede local.

---

**50.(INSTITUTO AOCF/UFPB - 2014)**

Um estagiário executou o comando FTP no servidor Linux. Esse comando possibilita

- A) permitir a abertura de portas para um acesso remoto a um servidor da rede.
- B) realizar a manutenção de disco e de memória de um computador remotamente.
- C) trocar informações de desempenho de redes utilizando um canal de comunicação protegido e exclusivo.
- D) realizar uma verificação de permissões de acesso na rede e no computador que o usuário está utilizando.
- E) trocar arquivos entre computadores interligados, independente do sistema operacional e da rede utilizada.

---

**51.(VUNESP/SAAE de Barretos-SP - 2018)**

Os serviços de acesso a dados da internet são disponibilizados em uma arquitetura Cliente/Servidor. Por exemplo, considerando um servidor com sistema operacional Linux, o serviço padrão que responde às requisições ftp é denominado

- A) ftpd.
- B) ftps.
- C) ftpsrv.
- D) samba.
- E) smb.

---

**52.(FUNIVERSA/PC-DF - 2012)**

Em um servidor de e-mail com sistema operacional Linux, especialmente quando se utiliza o serviço Postfix, pode-se auditar o tráfego de entrada e saída de mensagens de correio eletrônico por meio dos registros conhecidos por logs. Em que arquivo desse sistema operacional encontram-se os logs das atividades de envio e recebimento de mensagens de correio eletrônico (e-mail)?

- A) No diretório “/etc/postfix”.
- B) No arquivo “/var/log/maillog”.
- C) Na pasta “/var/mail/<nome\_do\_usuario>”.



- D) No arquivo “/usr/local/bin/postfix”.
- E) No arquivo de registro “/dev/tty”.

---

**53.(FUNCAB/MDA - 2014)**

São exemplos de servidores de correio eletrônico do Linux:

- A) postfix e sendmail.
- B) fetchmail e sendmail.
- C) pine e postfixe.
- D) mail e pine.
- E) samba e postfixe.

---

**54.(FGV/TJ-GO - 2014)**

A empresa Y passou a adotar uma política de uso de software livre e resolveu mudar o seu correio eletrônico, que era baseado em Microsoft Exchange. O novo ambiente deveria rodar em ambiente Linux. Uma das possíveis escolhas do novo software de correio eletrônico recai no programa:

- A) nginx;
- B) puppet;
- C) apache;
- D) postfix;
- E) bind.

---

**55.(FCC/Prefeitura de Manaus-AM - 2019)**

Um Assistente de TI foi incumbido de configurar o protocolo para ser utilizado na troca de mensagens entre dois servidores de e-mail. A escolha correta do protocolo para essa finalidade é:

- A) IMAP.
- B) POP3.
- C) SNMP.
- D) SMTP.
- E) POP4.

---

**56.(INSTITUTO AOC/P/UFMG - 2014)**



Em algumas distribuições Linux, podemos encontrar um arquivo que inclui as informações necessárias para executar o Protocolo para Sincronizar o Relógio da Rede (NTP). Assinale a alternativa que apresenta o nome deste arquivo.

- A) ntp.conf
- B) ntpd.conf.
- C) ntpsync.conf.
- D) ntpsync.conf.
- E) clock.conf.

---

**57.(FCC/SANASA - 2019)**

Considerando que o NTP – Network Time Protocol é um protocolo que permite a sincronização dos relógios dos dispositivos de uma rede a partir de referências de tempo confiáveis, um Analista de TI digitou um comando no Linux, em condições ideais, que mostrou o resultado abaixo.

remote	refid	st	t	when	poll	reach	delay	offset	jitter
=====									
+a.ntp.br	200.160.7.192	2	u	10	64	337	294.756	35.596	0.521
+b.ntp.br	200.160.7.186	2	u	8	64	377	226.294	2.658	0.229
*c.ntp.br	200.160.7.192	2	u	-	64	377	208.758	4.026	0.424

O comando digitado foi

- A) ntp -c ls
- B) ntpq -c pe
- C) ntpq > rv &1
- D) ntp -s pe
- E) ntpq -c rl



## GABARITO

- |            |           |
|------------|-----------|
| 1. Certo   | 40. C     |
| 2. Errado  | 41. D     |
| 3. Certo   | 42. D     |
| 4. Errado  | 43. E     |
| 5. Errado  | 44. E     |
| 6. C       | 45. D     |
| 7. B       | 46. E     |
| 8. A       | 47. E     |
| 9. B       | 48. A     |
| 10. Errado | 49. Certo |
| 11. C      | 50. E     |
| 12. E      | 51. A     |
| 13. Errado | 52. B     |
| 14. C      | 53. A     |
| 15. A      | 54. D     |
| 16. E      | 55. D     |
| 17. Errado | 56. A     |
| 18. D      | 57. B     |
| 19. A      |           |
| 20. B      |           |
| 21. D      |           |
| 22. B      |           |
| 23. C      |           |
| 24. D      |           |
| 25. B      |           |
| 26. Certo  |           |
| 27. D      |           |
| 28. C      |           |
| 29. Errado |           |
| 30. E      |           |
| 31. C      |           |
| 32. C      |           |
| 33. E      |           |
| 34. C      |           |
| 35. E      |           |
| 36. C      |           |
| 37. D      |           |
| 38. D      |           |
| 39. C      |           |



# ESSA LEI TODO MUNDO CONHECE: PIRATARIA É CRIME.

Mas é sempre bom revisar o porquê e como você pode ser prejudicado com essa prática.



1 Professor investe seu tempo para elaborar os cursos e o site os coloca à venda.



2 Pirata divulga ilicitamente (grupos de rateio), utilizando-se do anonimato, nomes falsos ou laranjas (geralmente o pirata se anuncia como formador de "grupos solidários" de rateio que não visam lucro).



3 Pirata cria alunos fake praticando falsidade ideológica, comprando cursos do site em nome de pessoas aleatórias (usando nome, CPF, endereço e telefone de terceiros sem autorização).



4 Pirata compra, muitas vezes, clonando cartões de crédito (por vezes o sistema anti-fraude não consegue identificar o golpe a tempo).



5 Pirata fere os Termos de Uso, adultera as aulas e retira a identificação dos arquivos PDF (justamente porque a atividade é ilegal e ele não quer que seus fakes sejam identificados).



6 Pirata revende as aulas protegidas por direitos autorais, praticando concorrência desleal e em flagrante desrespeito à Lei de Direitos Autorais (Lei 9.610/98).



7 Concurseiro(a) desinformado participa de rateio, achando que nada disso está acontecendo e esperando se tornar servidor público para exigir o cumprimento das leis.



8 O professor que elaborou o curso não ganha nada, o site não recebe nada, e a pessoa que praticou todos os ilícitos anteriores (pirata) fica com o lucro.



Deixando de lado esse mar de sujeira, aproveitamos para agradecer a todos que adquirem os cursos honestamente e permitem que o site continue existindo.