# SERVIDORES E SERVIÇOS DE INTERCONECTIVIDADE LINUX

## SERVIÇOS DE DHCP E DNS

Autor: Esp. Clóvis Tristão

Revisor: Alexandre Denicol

INICIAR

introdução

# Introdução

Caro Estudante, neste documento vamos explorar o uso dos serviços de rede DNS e DHCP, entender a importância dos mesmos para o cenário da comunicação e interligação de computadores.

O serviço de DNS, é extremamente necessário para o funcionamento da Internet, de forma geral, é com esse serviço que traduzimos os IP para os nomes das máquinas e vice-versa.

Um outro serviço é o DHCP, esse protocolo é responsável pela configuração dinâmica de um computador, para acesso a rede de computadores, fornece as informações necessárias, concedendo IP, *host* , máscara de sub-rede, *gateway* padrão, número IP do computador, e esse serviço pode trabalhar atrelado ao serviço de DNS.

Abaixo, trataremos desses temas com mais profundidade, dando exemplos e alguns exercícios para reforçar o conteúdo. Vamos explorar o mundo dos serviços Linux!

# DNS

O DNS ou  Domain Name System, é um serviço de tradução de nomes de endereços de Internet, pelo seu correspondente endereço IP, e vice-versa. Na interconexão dos computadores e servidores da rede, são identificados pelo endereço IP.

O sistema de DNS, é o responsável por essa tarefa e muitas outras funções relacionadas aos sistema de nomes, existem 13 servidores de nomes raízes espalhados pela Internet, e diversos continentes. Estes servidores raízes, por analogia, são o catálogo de endereços de computadores, servidores e domínios de toda a Internet. O DNS, é um serviço extremamente importante, e se ele ficar fora do ar, a Internet pode entrar em colapso, ou ficar sem nenhum tipo de acesso.

> *"O sistema de nomes de domínio é basicamente um banco de dados de informações do host. O ganho é imenso, em termos de facilidades de acesso aos hosts: nomes de servidores, apelidos, associações de nomes e apelidos engraçados. Mas lembre-se que, no final, o serviço que o DNS oferece são informações sobre hosts da Internet e seus endereços reais." (LIU, C., ALBITZ, P., 2006, p.11)*

O endereçamento IP, é formado por 4 octetos de 32 bits, sendo capaz de gerar 2^32 ou 4.294.967.296 de endereços, que corresponde a identificação de onde esse computador está localizado no planeta, tratando-se de um endereço único no mundo. Todos os computadores, equipamentos, servidores, roteadores e switches, possuem um endereço IP, único e exclusivo. Imagine, você em um cenário, com um IP:

216.58.202.5

Bilhões de endereços IP, e tentando acessar um determinado o site. Impraticável, sem um serviço de DNS. Podemos visualizar na Figura 3.1, um endereço IP (versão 4).

O DNS, é um catálogo, gigantesco, de endereços IP e seus respectivos nomes associados, esse sistema, para alocar esses bílhões de computadores, se comportando de forma distribuída, Esse catálogo, facilita identificar os servidores pelos nomes, que são mais fáceis de serem lembrados. A seguir, apresentamos um modelo de endereço IP e seu respectivo nome, note que no navegador eu digitei www.gmail.com, esse endereço é um apelido para o endereço real na web googlemail.l.google.com.

**216.58.202.5 googlemail.l.google.com**

# História

Em meados dos anos 70, um pequeno grupo de computadores, foram interligados em rede, formando a ARPAnet, os primórdios da Internet, e para que esses computadores trocassem mensagens, foi criado um sistema, que era mantido pelo SRI-NIC ( *Stanford Research Institute-Network Information Center* ), que concentrava em um arquivo texto HOSTS.TXT, todos os nomes e IPs, desse grupo de computadores. Era uma centena de máquina, quando entrava uma máquina nova na rede ARPAnet, esse arquivo texto era atualizado, e repassado a todos os administradores desses servidores, para atualizar manualmente sua base de dados.

Esse esquema manual, funcionou até a década de 80, tínhamos uma única

base, coordenada pelo SRI-NIC, e a transferência desse arquivo texto era realizada por FTP (protocolo de transferência de arquivos). Mas, com a chegada da Internet, nessa mesma década, e a inclusão de diversos elementos de rede e computadores, percebeu-se que esse sistema de atualização de nomes e IP, estava se tornando penoso e inviável. Começaram a surgir problemas de lentidão na transferência manual do arquivo, inconsistências no arquivo base e muitos nomes de computadores repetidos.

Com a migração da rede ARPAnet, para a Internet, os pesquisadores do SRI-NIC, precisavam desenvolver um outro método para tradução de nomes para IP, e vice-versa.

> *Os órgãos da ARPAnet encomendaram uma pesquisa ao SRI para desenvolver um sucessor para HOSTS.TXT. Seu objetivo era criar um sistema que resolvesse os problemas inerentes a um sistema baseado em uma única tabela de nomes.*
>
> *O novo sistema deveria permitir a administração local de dados ainda e disponibiliza-se esses dados globalmente. A descentralização da administração eliminaria gargalos de host único e alivie o problema de tráfego. E gerenciamento o local facilitaria muito a tarefa de manter os dados atualizados. O novo sistema deve usar um espaço para nome hierárquico para nomear hosts. Isso garantiria a exclusividade ness de nomes. (LIU, C., ALBITZ, P., 2006, pg. 3-4),*

A pedido de Jonathan Postel, criador da ARPAnet, Paul Mockapetris, foi o pesquisador chefe responsável por desenhar o protocolo e criar o sistema de nomes de domínio, a primeira versão, foi criada dentro dos laboratórios da Universidade de Berkeley, tendo sido batizada de BIND ( *Berkeley Internet Name Domain* ), até hoje o servidor de nomes chama-se BIND.

Portanto, o DNS, é um sistema de nomes distribuído, robusto e confiável. Essa estrutura distribuída, permite um controle local dos dados e um melhor gerenciamento, replicação dos dados locais para outros servidores de nomes de domínios.

O sistema, permite que cada servidor de nomes, tome conta de sua base de dados de computadores locais, replicando esse dados de uma forma organizada e robusta, evitando as repetições de nomes. A estrutura de um sistema de DNS, é apresentada na Figura 3, onde podemos visualizar o nó raiz (root), sendo o servidor principal daquele segmento de domínio, esse esquema se comporta como uma estrutura de diretórios em árvore de cabeça pra baixo. como um sistema de arquivo GNU/Linux. A analogia e a mesma para o sistema de DNS.

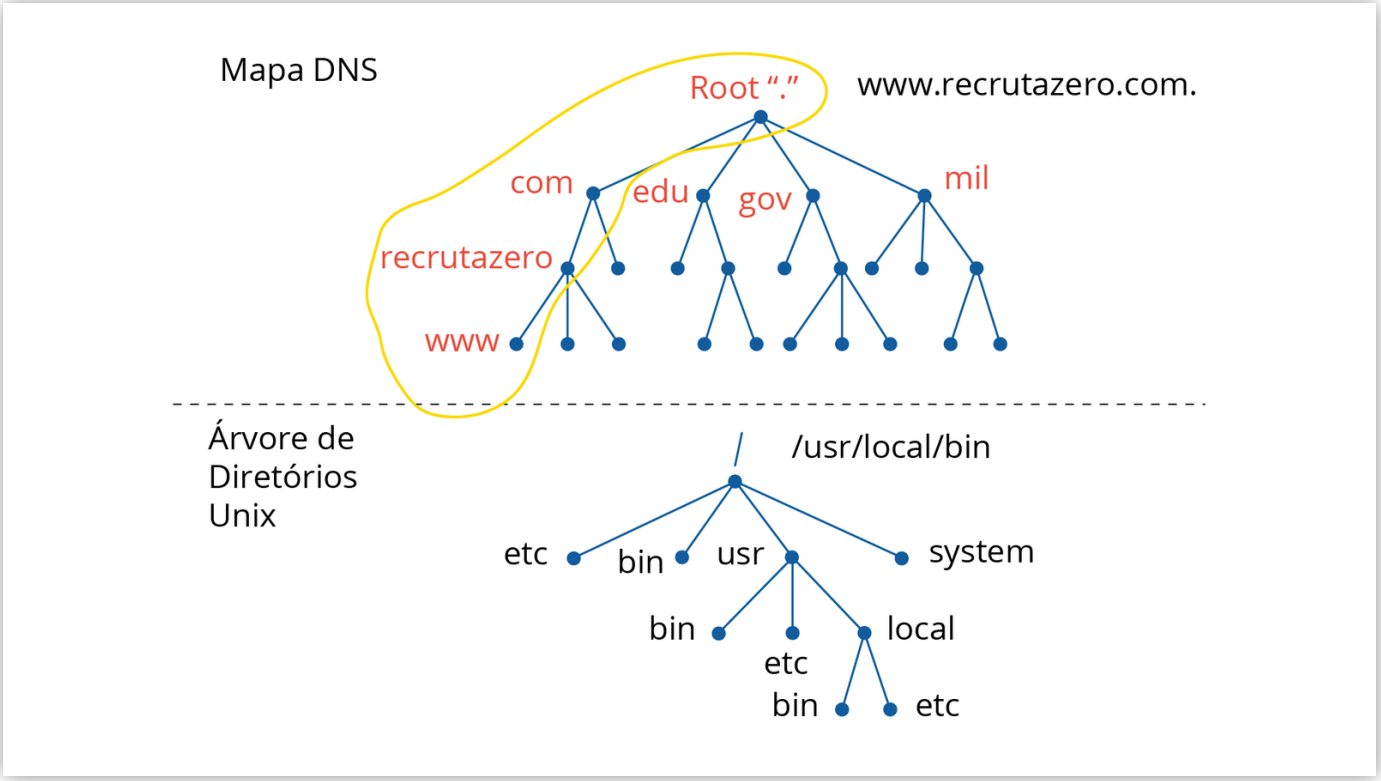



*Figura 3.1. Sistema DNS e Estrutura de Diretórios GNU/Linux ou Unix like. Fonte: (LIU, C., ALBITZ, P., 2006, pg. 5).*

Vamos ao exemplo da Figura 3.1, na parte do *unix filesystem* , para referenciar um determinado arquivoX que está no diretório (etc), dentro do sub-diretório usr/local, o caminho seria /usr/local/etc/<arquivoX>. Essa mesma analogia, podemos fazer no sistema de nomes de domínios, onde as folhas da árvore, mais afastadas da raiz ( *root* ou .(ponto)), seriam os servidores, onde realmente as aplicações da web estão hospedadas. No caso do DNS database, ficaria dessa forma um endereço da Internet. www.recrutazero.com., repare no último ponto, ele indica a raiz do servidores raízes da Internet.

O DNS, foi criado para rodar em sistemas operacionais Unix, mas nos dias de

hoje encontramos implementações em servidores rodando sistemas operacionais Linux e Windows. A seguir, vamos entender como funciona o DNS e quais os seus serviços.

# DNS: Serviços oferecidos

A função de traduzir nome de servidores para o seu respectivo endereço IP, é do DNS. Ele possui um conjunto hierárquico de servidores DNS, distribuídos geograficamente, essa distribuição é coordenada, e gerenciado por 13 servidores principais, que recebem o nome de servidores de topo de domínio, ou servidores raízes.

O DNS, utiliza-se do protocolo UDP na porta 53, como vocês devem ter aprendido em Redes, sobre protocolos e portas, é através desse protocolo que o sistema interage com os computadores e troca as informações de nome e IP.

O servidor ou computador cliente, é identificado pelo nome ou por seu apelido(s), que auxiliam de forma simples resolução de um nome de servidor ou máquina, esses apelidos são identificados como nomes canônicos. Isso é amplamente utilizado em servidores de e-mail ou sites, com grandes volumes de sites e sub-sites, de diferentes organizações, que são hospedados em um DataCenter. Por exemplo, o site de e-mail do GMail, o nome canônico do servidor é www.gmail.com, mas o nome real do servidor googlemail.l.google.com que possui o endereço de IP 172.217.30.69.

O serviço de DNS, pode ser usado para balanceamento de carga de servidor web ou servidor de e-mail, quando os site possuem diversos servidores com IP diferentes, que respondem por um mesmo domínio, que no exemplo do parágrafo acima, é o gmail.com, que possui diversos servidores de e-mail, espalhados pelo mundo, mas para o usuário final, possui um único endereço de acesso. O DNS, está por trás de todo esse trabalho de resolução e encaminhamento da requisição, que você realiza no navegador.

A seguir, mostraremos com funciona o DNS, mas de certa forma é

extremamente simples.

# Funcionamento

O serviço de DNS, como descrito nos parágrafos anteriores, tem em seu escopo principal a não concentração de todo o processo em um único servidor. Por ser um sistema hierárquico e distribuído, existe uma distribuição muito bem desenhada, de como funciona a resolução de nomes. Os servidores DNS, dividem-se em três segmentos:

- **Servidores de nome raiz (Root Servers)** : são 13 espalhados geograficamente pelo mundo.
- **Servidores de alto nível TLD (Top Level Domain)** : responsáveis pelos domínios do tipo .com, .org, .net, .edu, .mil, .br, .uk, .us entre outros.
- **Servidores autoritativos** : exercem a autoridade sobre um determinado domínio.
- **Servidor DNS local** : responsável, pela resolução local de nomes de uma determinada organização, mas ele não é integrado a hierarquia de resolvedores de nomes, ele apenas repassa a informação, até chegar no servidor raiz.

Para que um computador acessa uma página qualquer na Internet, como por exemplo “www.ead.br”, o navegador envia uma requisição o servidor de DNS local, este por sua vez, detecta que não possui o www.ead.br em seu mapa de dns, e escala a pergunta para o servidor raiz, que sabe quem responde pelo domínio .br, que é um dos servidores DNS de alto nível ou TLD, o TLD responde a consulta do servidor local, e sabe onde fica localizado o servidor ead.br, e devolve ao DNS local, o IP do servidor que hospeda o www.ead.br. E a página é acessada pelo navegador do usuário.

Na Figura 3.2, apresentamos como funciona o sistema de requisição de nomes, nos servidores de DNS locais, até chegar à consulta no servidor raiz.

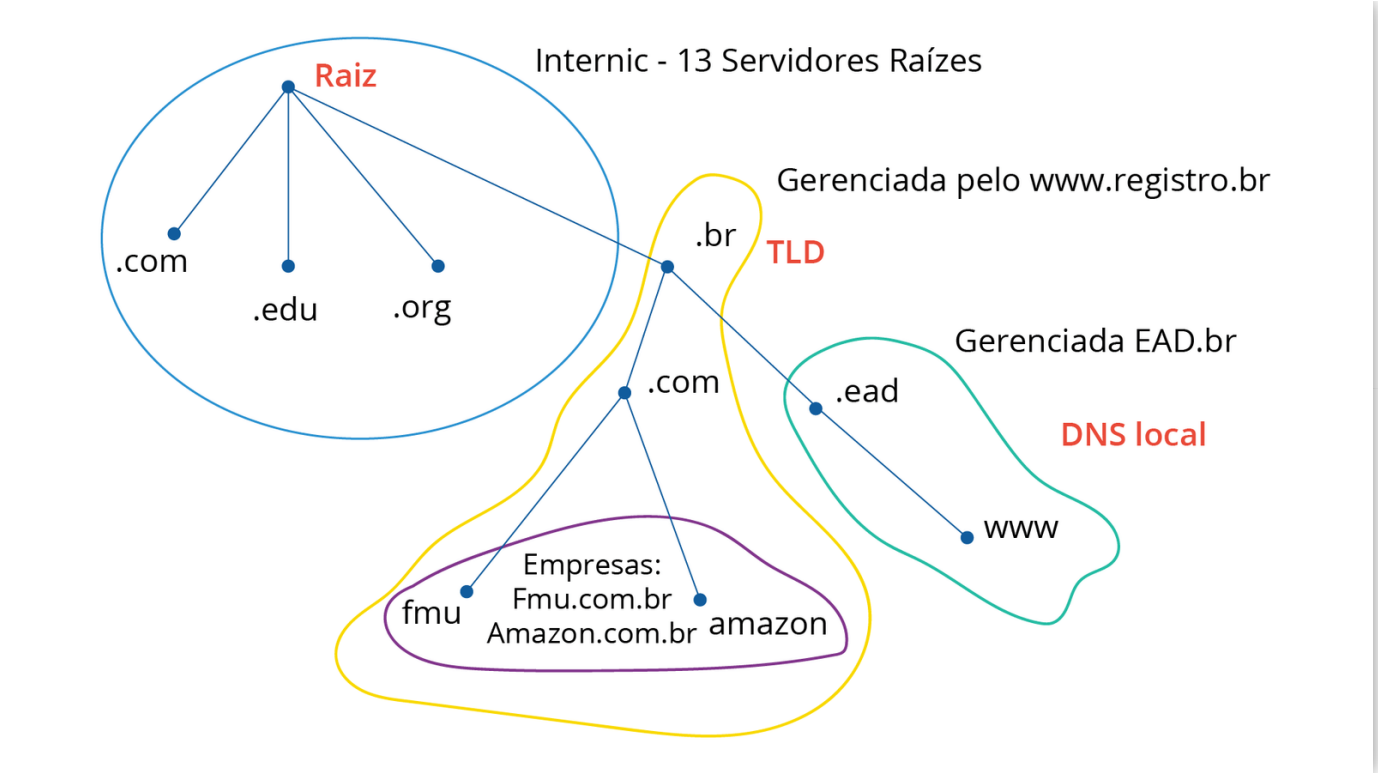



*Figura 3.2. Consulta de nomes nos Servidores DNS.*
*Fonte: O autor*

Um outro assunto, que não podemos deixar de lado, é a questão de segurança, que será tratado no decorrer do documento.

# Segurança

A segurança em um sistema de resolução de nomes, é um assunto necessário e delicado, e merece muita atenção no momento de sua implementação, instalação e gerenciamento.

A partir da versão 8.2 do BIND, os pesquisadores da Universidade de Berkeley, introduziram uma camada de segurança ao sistema de resolução de nomes, a camada TSIG, segundo (LIU, C., ALBITZ, P., 2006), essa camada cria o DNSsec(DNS *Security* ), que protege o sistema de possíveis ataques .

> *"Proteger seus usuários contra esses tipos de ataques requer segurança no DNS. DNSSecurity, se apresenta de várias formas. Você pode proteger transações - as consultas, respostas e outras mensagens que o servidor de nomes envia e recebe. Você pode proteger seu servidor de nomes, recusando consultas, solicitações*

> *de transferência de zona e atualizações dinâmicas de endereços não autorizados, por exemplo. Você pode até proteger os dados da zona assinando-os digitalmente." (LIU, C., ALBITZ, P., 2006, p.282-283)*

Dizer que o ambiente é seguro, a partir de hoje, é utopia, mas com essa camada de segurança, o sistema se tornou muito mais confiável e estável. Mas, ainda existe ataques de negação de serviço, envenenamento de tabelas de dns, que ficam em cache.

O computador, quando configurado corretamente e apontado para seu DNS local ou de seu provedor de Internet, já começa a consultar o serviço de dns para requisitar informações para acesso a Internet. Hoje o sistema operacional, para o seu funcionamento pleno, depende do DNS, para encontrar os sites de updates de sistema, antivírus, aplicativos entre outros, e tudo isso acontece de forma automática sem a intervenção do usuário. Mas, existem ferramentas de pesquisa manual sobre as tabelas de DNS, onde podemos entender o seu funcionamento, a seguir iremos entender um pouco sobre essas ferramentas de pesquisa.

## Ferramentas de pesquisa: NSLOOKUP e DIG

Essas ferramentas pesquisa, fazem parte do programa BIND, e são responsáveis por consulta, testes de falhas e configuração do seu serviço de DNS.

- NSLOOKUP, é um programa de pesquisa da base de dados do serviço de DNS, realiza a consulta de um determinado nome, e traz informações como nome, ip, apelidos, responsáveis pelo domínio, ele é amplamente utilizado, mas possui algumas deficiências e "furos' de segurança, e está gradativamente sendo substituído pelo DIG. Abaixo, fizemos uma consulta do nome www.ead.br, ele traz informações sobre o servidor. Podemos notar, que o nome canônico(apelido) é www.ead.br, que aponta para o nome real do servidor secure3.exceda.com.edgekey.net., que é um site de segurança, que

aponta para o nome e IP reais do servidor:l e14354.dscf.akamaiedge.net. 104.118.58.228 (ipv4) 2600:1419:7000:181::3812 (ipv6).

$ nslookup www.ead.br
Server: 127.0.0.53
Address: 127.0.0.53#53

Non-authoritative answer:
www.ead.br canonical name = secure3.exceda.com.edgekey.net.
secure3.exceda.com.edgekey.net canonical name = e14354.dscf.akamaiedge.net.
Name: e14354.dscf.akamaiedge.net
Address: 104.118.58.228
Name: e14354.dscf.akamaiedge.net
Address: 2600:1419:7000:181::3812

- DIG, mesma função é semelhante ao NSLOOKUP, o DIG é o sucessor do NSLOOKUP, com diversas melhorias e segurança. Podemos verificar, abaixo, que o DIG, traz informações mais completas que o seu antecessor, que para um administrador do serviço de DNS, são extremamente úteis para uma análise, em caso de falha do serviço.

  $ dig www.ead.br

  ; <<>> DiG 9.11.5-P4-5.1ubuntu5-Ubuntu <<>> www.ead.br
  ;; global options: +cmd
  ;; Got answer:
  ;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 44183
  ;; flags: qr rd ra; QUERY: 1, ANSWER: 3, AUTHORITY: 0, ADDITIONAL: 1

  ;; OPT PSEUDOSECTION:
  ; EDNS: version: 0, flags:; udp: 65494
  ;; QUESTION SECTION:
  ;www.ead.br. IN A

```
;; ANSWER SECTION:
www.ead.br. 3017 IN CNAME secure3.exceda.com.edgekey.net.
secure3.exceda.com.edgekey.net. 7199 IN CNAME
 e14354.dscf.akamaiedge.net.
e14354.dscf.akamaiedge.net. 18 IN A 104.118.58.228

;; Query time: 303 msec
;; SERVER: 127.0.0.53#53(127.0.0.53)
;; WHEN: qua jan 22 11:07:12 -03 2020
;; MSG SIZE  rcvd: 136
```

Com essas ferramentas, você pode realizar as consultas, testar se o seu resolvedor de nomes está funcionando corretamente.

praticar

# Vamos Praticar

i. Pesquise e disserte sobre o Mapa de Servidores Raízes, apresentando um mapa de como estão distribuídos esses servidores geograficamente. E qual a função do InterNIC?

ii. Usando a ferramenta DIG, pesquise e descreva, o HEADER as flags, destacadas abaixo:

; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 44183

;; flags: qr rd ra; QUERY: 1, ANSWER: 3, AUTHORITY: 0, ADDITIONAL: 1

# DHCP

O protocolo DHCP ( *Dynamic Host Configuration Protocol* ), foi criado na década de 90, para suprir uma demanda de configuração dinâmica e automática de computadores.

O DHCP, é um, faz parte da pilha de protocolos do TCP/IP, especificamente na camada de aplicação, sendo um serviço oferecido aos computadores. Ele é responsável por conceder IP, nome do host, máscara de rede e sub-rede, gateway default, e servidores de DNS, este serviço é ativado pelo administrador da rede nos computadores, e o serviço DHCP é implementado em um servidor.

O DHCP, pode ser configurado, em conjunto com o servidor de DNS, tornando-se uma solução interessante e perfeitamente viável, na inserção de um computador na rede local, e com acesso a Internet, tudo de forma automática, sem a necessidade de configurações prévias.

O DHCP, não é um serviço de extrema necessidade para uma rede funcionar, bem diferente do DNS, que sem o resolvedor de nomes não há acesso a Internet. DHCP, é um facilitador de configuração e inclusão de um

computador a rede local da organização, e com possível acesso a Internet.

Esse protocolo, possui diversas especificações, que são descritas no documento RFC 2131, e recentemente foi lançado um documento que trata das especificações para o IPv6, na RFC 3315).

A maioria dos equipamento, nos dias de hoje, já vem com o serviço de DHCP habilitado por padrão, para facilitar o ingresso do equipamento na rede, sem a intervenção do usuário.

Nos próximos parágrafos, vamos apresentar o funcionamento básico do serviço de DHCP.

saiba mais

### Saiba mais

Este tutorial, trará uma boa base para o estudo do DHCP, trazendo os conceitos do protocolo, o funcionamento e possíveis gargalos, bem como sua integração com o serviço de resolução de nomes. Aproveite a leitura!

Nome: Tutorial DHCP

Para conhecer mais sobre o DHCP, acesse.

ACESSAR

## Funcionamento Básico

Para que o serviço de DHCP funcione, há a necessidade de instalação e configuração de um Servidor DHCP, na rede local ou sub-rede. O administrador da rede local, faz todos os ajustes no servidor, para que ele funcione de forma correta.

Esse serviços, pode ser instalados em Sistemas Operacionais, executando o GNU/Linux, Windows Server, FreeBSD, entre outros. Sua implementação e simples e rápida, agregando para o usuário e a área de TI, uma flexibilidade na introdução do computador na rede da organização.

Para facilitar ainda mais o seu uso, o DHCP pode ser incorporado ao serviço de DNS, promovendo uma configuração completa em termos de rede no computador.

Assim como existe o servidor de DHCP, que concede as configurações para introduzir um computador na rede local, existe o Cliente DHCP, que é naturalmente o computador que solicitará e receberá as configurações para ingresso na rede, esse cliente pode ser uma Windows 10, Ubuntu Desktop Linux, um smartphone, tablet ou qualquer equipamento que possua o DHCP cliente embarcado no seu SO(Sistema Operacional.

Em linhas gerais e de forma prática, o DHCP funciona da seguinte forma:

1. O computador ou dispositivo, conecta-se a rede, seja ela cabeada ou sem fio, e envia uma pacote de dados pelo protocolo UDP, para todos os computadores da rede local, perguntando quem responde pelo serviço de DHCP.
2. Um desses computadores, da rede local, é o responsável pelo serviço de DHCP, ou seja ele é o servidor de DHCP, e responde a essa requisição do cliente, esse servidor captura esse pacote de dados, analisa, e responde, fornecendo informações necessárias para esse cliente ingressar na rede local, tais como nome, ip, gateway, máscara de rede e outras informações para acesso a internet.

Abaixo, apresentamos a figura 3.3, que demonstra o funcionamento da transação entre cliente e servidor de DHCP.

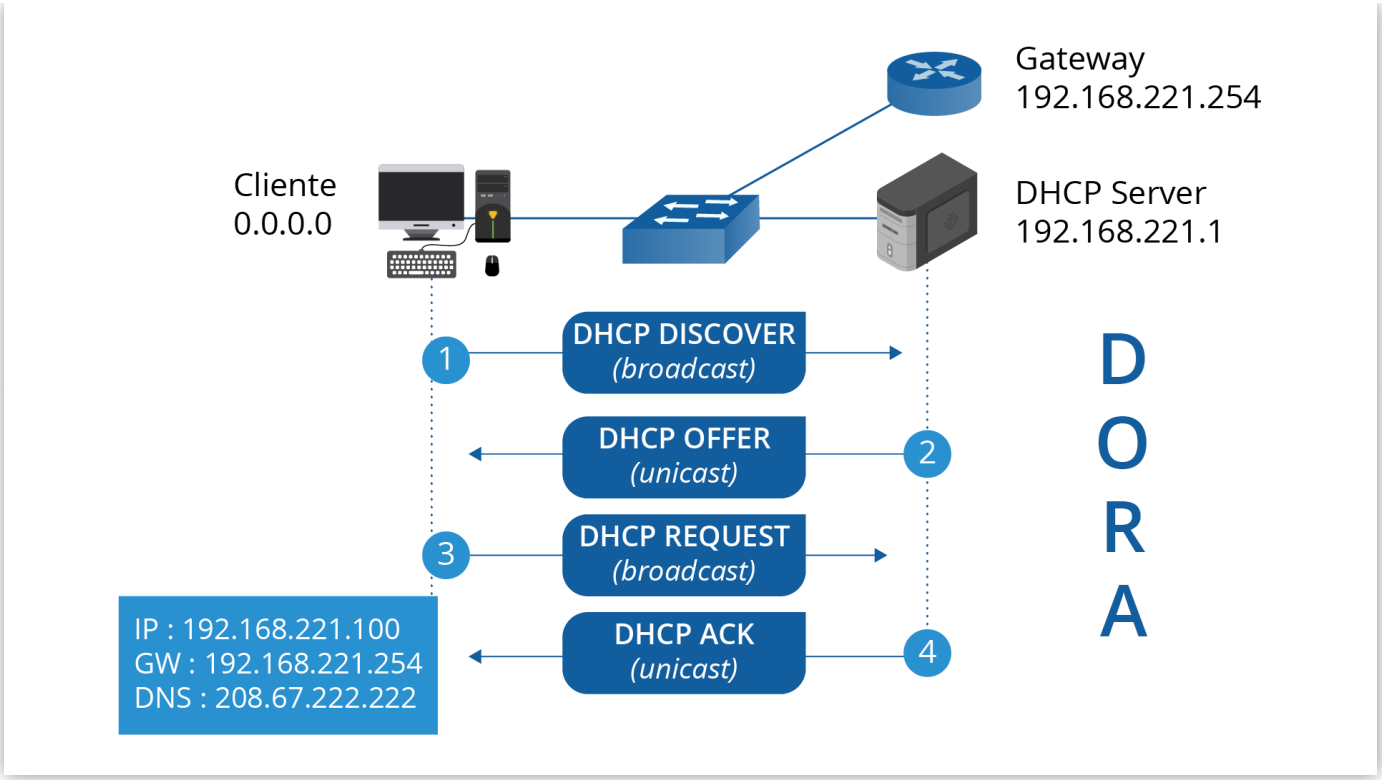



*Figura 3.3. Funcionamento do processo de concessão de informações entre Cliente e Servidor DHCP*

*Fonte: (BRITO, S.H.B., 2017, p.78).*

O modelo cliente-servidor do DHCP, passa por quatro passos, como vimos na figura 3.3. São eles:

- **DHCPDISCOVERY** (descoberta): o cliente transmite uma mensagem para todos os computadores na rede local, na tentativa de descobrir quem é o servidor de DCHCP, este pacote é encaminhado via protocolo UDP.
- **DHCPOFFER** (oferta): o servidor recebe a requisição do cliente e concede o IP, bem como o tempo que esse cliente poderá usar esse endereço, até a sua renovação.
- **DHCPREQUEST** (pedido): o cliente recebe a oferta do servidor e analisa e aceita as configurações e começa o processo de configuração do equipamento na rede local.
- **DHCPACK** (confirmação): O servidor DHCP recebe o aceita do cliente, o servidor repassa todos os dados necessários para o cliente poder acessar a rede e finaliza o processo de concessão. O cliente nesse passo configura a rede do computador local, com as informações repassadas pelo servidor DHCP, e o computador está pronto para ser

utilizado. Todo esse processo é realizado em milissegundos, de forma imperceptível ao usuário.

A liberação do IP, se dá quando esgota o tempo de concessão, esse IP é devolvido para a tabela de IP disponíveis no servidor DHCP, para ser usado por outro computador ou dispositivo. Seguindo o processo descrito na figura 3.5. Descreveremos, a seguir, sobre confiabilidade e segurança do serviço de DHCP.

## Confiabilidade e Segurança

O servidor de DHCP, é confiável no que tange a renovação de IP, tolerante a falhas e re-ligações, em casos onde o cliente seja desconfigurado ou o dispositivo do cliente seja reinicializado.

Em relação ao sistema de segurança, o protocolo DHCP não possui mecanismos de segurança e autenticação, portanto seria um ponto falho e vulnerável da rede, sua implementação tem que ser bem conduzida e controlada. O servidor DHCP, não tem como garantir, ou validar, que o cliente que está requisitando o acesso e IP. Quando o DHCP é integrado ao servidor DNS,que possui uma camada de segurança, ele pode se beneficiar dessa camada. Também, existem estratégias de configurações do servidor DHCP, para limitar essa concessão de IP, para qualquer equipamento que tente se conectar a rede local.

reflita

# Reflita

Reflita sobre a importância de se ter esses serviços DHCP e DNS, integrados em sua rede local.

Fonte: BRITO, S.H.B. (2017, p. 111).

Um estudo, sobre DHCP Relay, traz um panorama favorável para inclusão de segurança no serviço de DHCP.

> *"Uma modalidade preferida da presente invenção inclui um método e aparelho para alocar e usar endereços IP em uma rede de clientes. Mais especificamente, a presente invenção inclui um servidor DHCP que aluga endereços IP para os sistemas clientes. O servidor DHCP trabalha em conjunto com um agente de retransmissão DHCP seguro e um agente de retransmissão IP seguro. As mensagens DHCPREQUEST de difusão são encaminhadas para o servidor DHCP pelo agente de retransmissão DHCP seguro. Antes de encaminhar, o agente de retransmissão DHCP seguro é incorporado em cada mensagem DHCPREQUEST. O identificador confiável é um objeto imperdoável especificamente associado ao sistema do cliente que envia a mensagem DHCPREQUEST. Quando o servidor DHCP recebe uma mensagem DHCPREQUEST, o servidor DHCP extrai o identificador confiável. O identificador confiável é então usado pelo servidor DHCP para impedir que os sistemas clientes acessem as concessões de endereços IP de outros sistemas clientes. O servidor DHCP também conta o número de concessões de endereços IP atribuídos a cada identificador confiável. Dessa maneira, cada sistema cliente é impedido de conceder mais do que um número predeterminado de endereços IP. As mensagens DHCPREQUEST unicast recebidas pelo servidor DHCP incluem um endereço de origem que corresponde*

> *ao sistema do cliente que envia a mensagem DHCPREQUEST unicast. A validade do endereço de origem é garantida pelo agente de retransmissão IP seguro. O servidor DHCP usa o endereço de origem para impedir que os sistemas clientes acessem as concessões de endereços IP de outros sistemas clientes." (Swee B. Lim, Sanjay R. Radia, Thomas K. Wong, Panagiotis Tsirigotis, Robert J. Goedman, 2020, p.1)*

Para garantir, confiabilidade e segurança, o ideal é sempre possuirmos servidores redundantes em caso de falha do servidor principal.

praticar

# Vamos Praticar

Um computador novo, é adicionado a sua rede de dados, e o mesmo não possui nenhuma configuração da rede e nenhum conhecimento sobre ela, mas o Sistema Operacional, já vem pré-configurado para solicitar um endereço, para o servidor DHCP,  e obter a concessão de um IP, essa oferta passa por quatro passos. Assinale a alternativa correta, que corresponde aos quatro passos na ordem que são executados:

- **a)** DHCPDISCOVERY DHCPOFFER DHCPREQUEST DHCPACK
- **b)** DHCPREQUEST DHCPDISCOVERY DHCPOFFER DHCPACK
- **c)** DHCPDISCOVERY DHCPREQUEST DHCPACK DHCPOFFER
- **d)** DHCPREQUEST DHCPDISCOVERY DHCPACK DHCPOFFER
- **e)** DHCPOFFER DHCPREQUEST DHCPDISCOVERY DHCPACK

praticar

# Vamos Praticar

O administrador de uma rede, necessita configurar 5 mil estações de trabalho de sua empresa e nessa configuração ele precisa incluir o nome da estação, IP e gateway padrão para a devida conexão na rede. Para configurar essa funcionalidade, qual protocolo o administrador da rede pode utilizar para esse caso? Assinale a alternativa correta, que corresponde a solução da questão apresentada:

- **a)** ARP
- **b)** FTP
- **c)** DNS
- **d)** DHCP
- **e)** HTTP

praticar

# Vamos Praticar

Durante a concessão entre cliente e servidor DHCP, existe o preenchimento de flags de campos específicos para o registro do cliente no servidor DHCP, são eles:

- **a)** IP, MAC,NAT
- **b)** IP, NAT, TCP
- **c)** DNS, TCP, MAC

- **d)** UDP, MAC, DNS
- **e)** IPclient, IPserver, IProuter

praticar

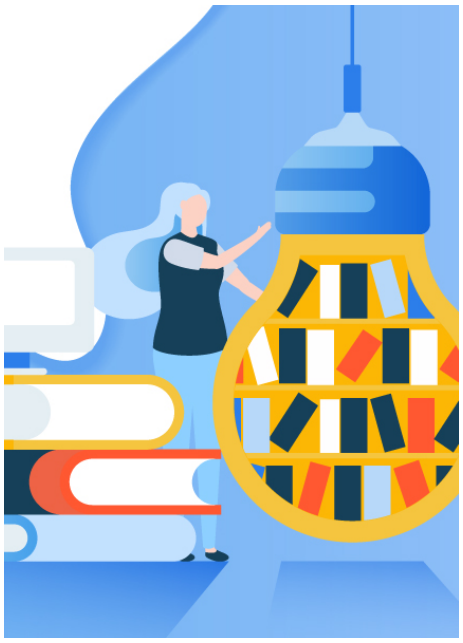
# Vamos Praticar

Qual a função do servidor DHCP, que atua na camada de aplicação. Definitivamente o que ele entrega para o cliente, quando o seu serviço é requisitado? Assinale a alternativa correta:

- **a)** Conceder um endereço IP e configurar automaticamente os dispositivos em uma rede.
- **b)** Disponibilizar aplicações em Java.
- **c)** Hospedar sites web em uma rede.
- **d)** Armazenar e compartilhar arquivos.
- **e)** Configurar serviços na intranet.

indicações

# Material Complementar



LIVRO

## Redes de Computadores

TANENBAUM, A.S

**Editora:** Pearson Prentice Hall

**ISBN:** 8535211853

**Comentário:** Este livro traz uma abordagem completa sobre as camadas TCP/IP, e na camada de aplicação, aprofunda o conceito que abordamos neste documento. Sugiro a leitura completa dos capítulos 7 e 8.

conclusão

# Conclusão

O serviço de DNS, sendo o responsável por traduzir nomes e IP e vice-versa, é extremamente importante para navegação na Internet. Como o sistema é hierárquico e distribuído, a Internet continua funcionando caso um servidor de DNS, fique fora do ar momentaneamente.

O serviço de DHCP, é usado para facilitar a configuração das máquinas, em uma rede local, fornecendo parâmetros para que essa máquina possa acessar a rede de forma automática.

Integrar os dois serviços DHCP e DNS, é ideal para um bom funcionamento de todo a rede, dando liberdade para os gestores de TI, se dedicarem a outras tarefas, e manter o parque computacional sempre atualizado, com uma tabela única de nomes e ip, de sua rede local, para fins de inventário.

De forma geral, esses serviços são necessários, para a gestão de sua rede local.

referências

# Referências Bibliográficas

BRITO, S.H.B., **Serviços de Redes em Servidores Linux** , 1a edição, São Paulo, Novatec, 2017.

LIU, C., ALBITZ, P., **DNS and BIND** , 5a edição, O'Reilly, 2006

TANENBAUM, A.S., **Organização estruturada de computadores** , 6a edição, São Paulo, Pearson, 2013.

TANENBAUM, A.S., **Sistemas Operacionais Modernos** , 4a edição, São Paulo, Pearson, 2016.

TANENBAUM, A.S., **Redes de Computadores** , 4a edição, São Paulo, Pearson, 2003.

Swee B. Lim, Sanjay R. Radia, Thomas K. Wong, Panagiotis Tsirigotis, Robert J. Goedman, **Secure DHCP server** , Oracle America Inc, 2020.