| | | |
|---|---|---|
| INSTITUTO FEDERAL Rio Grande do Norte | **INSTITUTO FEDERAL DO RN**<br>**Campus Natal-Central** | |
| | **Disciplina:** Redes de Computadores - TEC.0016 | |
| | **Professor(a):** Moisés Cirilo de Brito Souto | |
| | **Discentes:** Anderson Henrique Silva Santos<br>**Discentes:** Lucas Pinheiro da Costa<br>**Discentes:** Rogério Young Evaristo de Souza | **Matrícula:** 20232014040014<br>**Matrícula:** 20231014040023<br>**Matrícula:** 20232014040017 |
| | **Curso:** TADS | **Semestre:** 2024.1 |
| | **Documentação:** Implementação de Servidor DNS no software de sistema Cisco Packet Tracer | |

## 1. HISTÓRIA E EVOLUÇÃO DO PROTOCOLO DNS

O **Sistema de Nomes de Domínio (DNS)** é uma estrutura fundamental da Internet, responsável por traduzir nomes de domínio amigáveis, como "https://portal.ifrn.edu.br/" em endereços IP (Internet Protocol) numéricos que os computadores utilizam para se comunicar. Essa tradução é essencial para que os usuários possam acessar sites e serviços online sem precisar memorizar longas sequências de números.

Antes do DNS, a Internet utilizava um sistema simples baseado em um **arquivo de texto** que listava todos os nomes de hosts e seus respectivos endereços IP. No entanto, à medida que a Internet crescia, esse sistema tornou-se cada vez mais difícil de gerenciar e manter atualizado.

Em 1983, Paul Mockapetris criou o DNS, uma solução mais escalável e distribuída. As primeiras especificações do DNS foram publicadas nas **RFCs (Request for Comments) 882 e 883**. Essas RFCs definiram a estrutura hierárquica do DNS, os tipos de registros e os protocolos de comunicação.

Uma das características mais importantes do DNS é sua natureza hierárquica e distribuída. A responsabilidade de gerenciar os nomes de domínio é dividida em zonas, cada uma com um servidor de nomes responsável por ela. Essa arquitetura permite que a Internet cresça de forma escalável e resiliente.

### Evolução e Novas Funcionalidades

Ao longo dos anos, o DNS passou por diversas evoluções. As **RFCs 1034 e 1035**, publicadas em 1987, substituíram as especificações originais e introduziram novas

funcionalidades. O DNS passou a ser utilizado não apenas para traduzir nomes de domínio em endereços IP, mas também para outras tarefas, como:

- **Servidores de e-mail:** O Registro MX (Mail Exchange Record) indica o servidor de e-mail responsável por receber mensagens para um determinado domínio.
- **Servidores de nomes:** O Registro NS (Name Server Record) indica os servidores de nomes autorizados para uma determinada zona.
- **Alias:** O Registro CNAME (Canonical Name Record) permite criar apelidos para nomes de domínio.
- **Segurança:** O DNSSEC (Domain Name System Security Extensions) foi desenvolvido para proteger o DNS contra ataques de falsificação.

## Estrutura do Servidor DNS

O DNS segue uma arquitetura cliente/servidor e sua estrutura é organizada em uma hierarquia de três níveis principais: servidores raiz, servidores de domínios de nível superior (TLDs) e servidores autoritativos.

**Os servidores raiz** são o ponto inicial para todas as consultas DNS que não podem ser resolvidas localmente. Existem 13 servidores raiz globais, identificados por letras de A a M, geridos por organizações e empresas de grande porte, como a Verisign e a NASA. Embora referidos como 13 servidores, na verdade, consistem em milhares de servidores distribuídos globalmente, operando em **clusters com alta disponibilidade** para garantir a continuidade do sistema.

**Os servidores de domínios de nível superior** são responsáveis por gerenciar os domínios que pertencem a um TLD específico, como .com, .net e .org, além de domínios de países, como .br (Brasil) e .us (Estados Unidos). Quando uma consulta é encaminhada de um servidor raiz para um servidor TLD, este identifica qual é o servidor autoritativo responsável pelo domínio específico dentro do TLD. Por exemplo, se a consulta for para "example.com", o servidor TLD .com encaminhará a consulta para o servidor autoritativo que contém o registro desse domínio.

**Os servidores autoritativos** contêm as informações finais de resolução de nomes e respondem diretamente com o endereço IP correspondente ao nome de domínio consultado. Quando um servidor TLD recebe uma consulta, ele a direciona ao servidor autoritativo que pode resolver o nome de domínio completo.

O DNS é considerado um protocolo de aplicação, pois fornece um serviço específico

para outras aplicações: a tradução de nomes de domínio legíveis por humanos para endereços IP numéricos utilizados pelos computadores. Embora o DNS opere na camada de aplicação, suas mensagens são transmitidas principalmente via o protocolo **UDP (User Datagram Protocol)**, na camada de transporte, utilizando a **porta 53**. Em casos de respostas muito grandes ou em operações específicas, como a transferência de zonas DNS (AXFR), o **protocolo TCP** também pode ser utilizado, ainda na porta 53.

## 2. ADOÇÃO DO PROTOCOLO NO MERCADO E SUA RELEVÂNCIA ATUAL

A adoção do protocolo DNS no mercado global e brasileiro é vasta e essencial para o funcionamento da Internet moderna, servindo como a base para a navegação na web e a resolução de nomes de domínio. Nos dias atuais, o DNS se expandiu para além da simples tradução de nomes de domínio para endereços IP, desempenhando papéis críticos na segurança cibernética, desempenho da rede, e em novas tecnologias como a computação em nuvem e **redes de entrega de conteúdo (CDN)**.

### Adoção Global do DNS

Desde sua criação em 1983, o DNS foi amplamente adotado e padronizado globalmente. Ele é fundamental para a comunicação na Internet, suportando bilhões de dispositivos e serviços. Quase todas as interações na web, seja a navegação em sites, envio de e-mails ou uso de aplicativos de redes sociais, dependem do DNS para funcionar.

Alguns aspectos marcantes da adoção global do DNS incluem:

1. **Infraestrutura crítica**: O DNS é uma das infraestruturas mais críticas da Internet. Ele é operado por uma rede global de servidores distribuídos e geridos por várias entidades, incluindo governos, empresas privadas, e organizações sem fins lucrativos. Servidores-raiz, operados por corporações como a **ICANN (Internet Corporation for Assigned Names and Numbers)** e outras, gerenciam a estrutura hierárquica do DNS, enquanto milhões de servidores DNS locais são mantidos por **provedores de serviços de Internet (ISPs)**, empresas de tecnologia, universidades, entre outros.
2. **Segurança e DNSSEC**: O protocolo DNS, apesar de essencial, é vulnerável a ataques como o **envenenamento de cache (cache poisoning) e spoofing**. Para mitigar esses riscos, foi introduzido o **DNSSEC (DNS Security Extensions)**, que autentica respostas DNS, assegurando que os dados não foram modificados durante o tráfego. Muitos países e grandes empresas adotaram o DNSSEC, promovendo a segurança na Internet globalmente.
3. **Escalabilidade e CDN**: Com o crescimento do tráfego da Internet, especialmente devido à adoção de streaming de vídeo, computação em nuvem e comércio eletrônico, o DNS evoluiu para trabalhar com CDN. O DNS permite a distribuição

eficiente de conteúdo com base na localização geográfica dos usuários, encaminhando as solicitações para servidores próximos e reduzindo a latência.

4. **Empresas e serviços globais**: Empresas como Google, Amazon, Cloudflare, e Verisign desempenham papéis importantes na operação e inovação em torno do DNS. Google Public DNS, por exemplo, é um dos maiores serviços de DNS público do mundo, enquanto o Cloudflare DNS é reconhecido pela sua privacidade e rapidez.

**Adoção do DNS no Brasil**

No Brasil, a adoção do DNS também é ampla e vital para o funcionamento da Internet nacional. O DNS é utilizado por praticamente todos os provedores de serviços de Internet, empresas e organizações governamentais.

1. **Coordenação do DNS brasileiro**: O **Comitê Gestor da Internet no Brasil (CGI.br)** e o **NIC.br (Núcleo de Informação e Coordenação do Ponto BR)** são os responsáveis por coordenar a distribuição de nomes de domínio e a operação de servidores DNS no Brasil. Eles supervisionam o registro de domínios ".br" e mantêm a infraestrutura necessária para garantir o funcionamento eficiente do sistema de nomes de domínio no país.
2. **Registro.br**: O Registro.br é a entidade responsável pelo registro de domínios ".br" e pela gestão de servidores de nomes de domínio associados. O Brasil possui uma das maiores bases de domínios registrados sob um código de país, o que reflete a adoção significativa do DNS entre empresas, governo e usuários individuais.
3. **DNS público no Brasil**: Alguns provedores brasileiros oferecem serviços públicos de DNS, semelhantes aos de empresas internacionais. O **OpenDNS Brasil** e o **Google DNS** são amplamente utilizados por usuários brasileiros como uma alternativa para melhorar a segurança e a velocidade da resolução de nomes, especialmente em áreas com problemas de infraestrutura.
4. **Segurança no Brasil**: A adoção do DNSSEC no Brasil tem avançado consideravelmente, especialmente entre grandes empresas, instituições financeiras e provedores de serviços de Internet. O Brasil tem promovido campanhas de conscientização sobre a importância de adotar o DNSSEC, garantindo que os dados de navegação estejam protegidos contra ataques maliciosos.
5. **Provedores locais**: Grandes provedores de Internet como a Vivo, Oi, Claro e TIM utilizam servidores DNS robustos para manter a qualidade e a eficiência dos

serviços prestados a milhões de usuários brasileiros. Além disso, empresas de tecnologia brasileiras também têm investido em infraestrutura de DNS para suportar operações críticas de negócios, como e-commerce, streaming e sistemas bancários.

**Relevância atual do DNS**

Atualmente, o DNS não é apenas uma infraestrutura fundamental para a Internet, mas também está diretamente relacionado à segurança, privacidade e desempenho de redes em todo o mundo.

Com o aumento das ameaças cibernéticas, o DNS tem desempenhado um papel crucial na defesa contra **ataques de negação de serviço distribuído (DDoS)** e no combate a fraudes online. Para garantir a confiabilidade da Internet, provedores de DNS implementam técnicas avançadas de segurança, como o DNSSEC e protocolos de proteção contra ataques DDoS.

Além da segurança, a privacidade na navegação também se tornou uma grande preocupação, levando ao desenvolvimento de tecnologias como **DNS sobre HTTPS (DoH)** e **DNS sobre TLS (DoT)**. Essas tecnologias criptografam as consultas DNS, garantindo uma navegação mais segura e protegida contra interceptações, preservando a privacidade dos usuários.

Com o crescimento dos serviços em nuvem e a necessidade de uma Internet cada vez mais rápida e escalável, o DNS continua sendo essencial para otimizar o tráfego de dados e garantir que os usuários tenham acesso rápido aos serviços online. Grandes empresas como Google, Amazon e Microsoft utilizam o DNS para fornecer balanceamento de carga, redundância e baixa latência, garantindo a eficiência de seus serviços de computação em nuvem.

Outro aspecto relevante é o suporte do DNS ao **IPv6**, um protocolo fundamental diante da exaustão dos endereços IPv4. O DNS tem sido essencial na transição para o IPv6, permitindo a alocação de um número muito maior de endereços IP. O DNS moderno suporta tanto o **formato A (para IPv4)** quanto o **formato AAAA (para IPv6)**, garantindo a continuidade e expansão da rede global sem limitações de endereçamento.

Por fim, o papel do DNS só tende a crescer com o surgimento da **Internet das Coisas (IoT)** e a expansão das **redes 5G**. A gestão da conectividade entre bilhões de dispositivos conectados depende do DNS, que se tornará cada vez mais necessário para garantir a escalabilidade e eficiência de novas aplicações de rede em tempo real.

## 3. VANTAGENS E DESVANTAGENS DO PROTOCOLO NO CONTEXTO MODERNO

No contexto moderno, o DNS oferece diversas vantagens, mas também enfrenta desafios e limitações, especialmente à medida que a Internet se expande e as ameaças cibernéticas se tornam mais sofisticadas.

**Vantagens do DNS**

1. **Facilidade de uso e conveniência**: Uma das maiores vantagens do DNS é que ele facilita o uso da Internet para usuários comuns. Ao invés de memorizar endereços IP numéricos, os usuários podem digitar nomes de domínio simples e legíveis. Isso torna a navegação mais intuitiva e acessível, contribuindo para a ampla adoção da Internet.
2. **Escalabilidade**: O DNS é altamente escalável, permitindo que milhões de novos domínios e endereços IP sejam adicionados à rede global de maneira contínua. A arquitetura distribuída do DNS, com servidores localizados em diferentes partes do mundo, permite que ele suporte o tráfego global sem sobrecarga significativa.
3. **Distribuição de carga**: O DNS pode ser configurado para distribuir o tráfego de forma eficaz entre diferentes servidores, utilizando técnicas como round-robin e balanceamento de carga geográfico. Isso melhora o desempenho dos sites e serviços, garantindo que os usuários sejam redirecionados para o servidor mais próximo ou menos sobrecarregado, o que é especialmente útil em grandes redes e serviços CDN.
4. **Resiliência e redundância**: O DNS é projetado para ser resistente a falhas. A distribuição de servidores de nomes em diferentes locais geográficos e sob diferentes entidades permite uma maior redundância. Se um servidor DNS falhar, outro pode assumir rapidamente o controle, garantindo a continuidade do serviço.
5. **Extensões de segurança**: Protocolos como o DNSSEC foram introduzidos para aumentar a segurança do DNS, autenticando respostas e protegendo os usuários contra ataques de envenenamento de cache e spoofing. Além disso, tecnologias como DNS sobre HTTPS (DoH) e DNS sobre TLS (DoT) foram desenvolvidas para criptografar as consultas DNS, oferecendo uma camada adicional de privacidade e segurança.
6. **Flexibilidade**: O DNS tem se mostrado flexível ao longo do tempo, sendo adaptado para suportar novos protocolos, como o IPv6, além de desempenhar papéis em serviços de segurança e otimização de redes. Sua capacidade de adaptação

garante sua relevância contínua em um cenário tecnológico em constante mudança.

**Desvantagens do DNS**

1. **Segurança**: Embora o DNS seja essencial para a navegação, ele possui vulnerabilidades. Um dos maiores riscos associados ao DNS é o envenenamento de cache (DNS cache poisoning), onde atacantes podem manipular o cache de servidores DNS para redirecionar usuários a sites falsos ou maliciosos. Além disso, ataques de negação de serviço distribuído (DDoS) focados em servidores DNS podem causar interrupções maciças.
2. **Privacidade limitada**: As consultas DNS são, tradicionalmente, enviadas em texto simples (não criptografadas), o que permite que terceiros monitorem as atividades de navegação dos usuários, criando preocupações com a privacidade. Isso levou ao desenvolvimento de soluções como o DNS sobre HTTPS (DoH) e DNS sobre TLS (DoT), que criptografam essas consultas, mas sua implementação ainda está em progresso em muitos ambientes.
3. **Complexidade na configuração de DNSSEC**: Apesar das vantagens de segurança do DNSSEC, sua implementação pode ser complexa e propensa a erros. Se mal configurado, pode causar falhas na resolução de nomes de domínio, levando à inacessibilidade de sites. Isso desencoraja algumas organizações a adotarem essa tecnologia de forma ampla.
4. **Latência**: Em redes mal configuradas ou sobrecarregadas, o DNS pode introduzir latência. Embora as consultas DNS sejam geralmente rápidas, atrasos podem ocorrer quando as informações não estão em cache ou quando servidores DNS distantes precisam ser acessados. Isso pode afetar a experiência do usuário, especialmente em regiões com infraestrutura de Internet menos desenvolvida.
5. **Centralização crescente**: Embora o DNS tenha sido projetado como uma rede distribuída, há uma crescente centralização em torno de grandes provedores de DNS, como Google Public DNS e Cloudflare. Essa concentração de poder em poucas empresas cria um ponto de vulnerabilidade e pode levar a preocupações sobre a privacidade e o controle de dados, além de potencialmente reduzir a diversidade do ecossistema.
6. **Sobrecarga administrativa**: Para administradores de rede, gerenciar registros DNS pode ser uma tarefa trabalhosa. A manutenção de servidores DNS, especialmente em grandes organizações com muitos subdomínios e serviços, pode exigir esforços significativos para garantir que as zonas DNS estejam configuradas corretamente, seguras e atualizadas.

7. **Custo**: Embora o DNS seja uma tecnologia básica, a operação de servidores DNS robustos e seguros, especialmente em ambientes corporativos ou para grandes sites e serviços, pode gerar custos consideráveis. Esses custos incluem a manutenção de hardware, a contratação de especialistas em DNS, e a implementação de medidas de segurança, como o DNSSEC e mitigação de ataques DDoS.

## 4. CONFIGURAÇÃO DETALHADA DO PROTOCOLO

O presente estudo utilizou o ambiente de desenvolvimento ***GitHub Codespace***, com o editor ***Visual Studio Code*** integrado e a extensão ***WSL (Windows Subsystem for Linux)***, para o manuseio dos arquivos do protocolo usando scripts no terminal de comandos ***Bash***, como plataforma para testar as configurações do protocolo DNS. A escolha desse ambiente se justifica pela praticidade de testar essas tarefas nas especificações de máquina virtual dentro do Codespace: 2 núcleos, 8 GB de RAM e 32 GB de armazenamento.

A configuração de um servidor DNS em um ambiente Linux, como o GitHub Codespace, exige o conhecimento dos principais arquivos de configuração e a compreensão dos passos básicos envolvidos nesse processo. A seguir, são apresentados os principais aspectos a serem considerados, acompanhados de exemplos práticos.

### 4.1. PRINCIPAIS ARQUIVOS DE CONFIGURAÇÃO DO SERVIDOR DNS

O software de servidor DNS mais amplamente utilizado em Linux é o **BIND (Berkeley Internet Name Domain)**. Os principais arquivos de configuração usados no BIND são:

- `/etc/named.conf`: Arquivo principal de configuração do servidor DNS. Aqui se definem as zonas de DNS, os domínios que o servidor será responsável por resolver, as permissões de acesso e outras configurações gerais.
- `/var/named/`: Diretório onde são armazenados os arquivos de zona, que contém os registros de DNS para os domínios.
- `/etc/resolv.conf`: Arquivo que indica ao sistema qual servidor DNS usar para resolver nomes de domínio. Pode ser usado para testar o servidor localmente.

### 4.2. PASSOS ESSENCIAIS PARA INSTALAÇÃO E CONFIGURAÇÃO DO SERVIDOR DNS NO LINUX (USANDO GITHUB CODESPACE)

**Instalar o BIND**

No ambiente Linux, o primeiro passo é instalar o BIND. No GitHub Codespace, o sistema geralmente roda em uma distribuição Ubuntu. Instala-se o BIND usando o seguinte comando no terminal:

```bash
sudo apt update
sudo apt install bind9 bind9utils bind9-doc -y
```

**Configurar o Arquivo Principal (`/etc/named.conf`)**

Esse arquivo contém as definições principais do servidor. Configura-se uma zona "exemplo.com" como exemplo prático, ao mesmo tempo que se configura um DNS Reverso para “converter” endereço IP em nome de domínio. Abra o arquivo de configuração usando esse comando:

```
sudo nano /etc/bind/named.conf.local
```

Adicione uma nova zona, que o servidor será responsável por resolver:

```
zone "exemplo.com" {
    type master;
    file "/etc/bind/zones/db.exemplo.com";
};
```

Esse bloco define a zona "exemplo.com" e aponta para o arquivo onde os registros serão armazenados.

Em seguida adicione a zona para o DNS Reverso:

```
zone "0.168.192.in-addr.arpa" {
    type master;
    file "/etc/bind/zones/db.192.168.0";
};
```

**Criar o Arquivo de Zona**

Agora, crie o arquivo de zona onde estarão os registros DNS (como endereços IP associados aos nomes de domínio). Para criar o diretório de zonas, caso ainda não exista,

use o comando:

```
sudo mkdir -p /etc/bind/zones
```

Crie o arquivo de zona para "exemplo.com": `sudo nano /etc/bind/zones/db.exemplo.com`

Adicione o seguinte conteúdo ao arquivo:

```
$TTL    604800
@       IN      SOA     ns1.exemplo.com. admin.exemplo.com. (
                        2023091201  ; Serial
                        604800      ; Refresh
                        86400       ; Retry
                        2419200     ; Expire
                        604800 )    ; Minimum TTL

        IN      NS      ns1.exemplo.com.
        IN      A       192.168.0.1  ; Endereço IP do servidor

ns1     IN      A       192.168.0.1
www     IN      A       192.168.0.2
```

O campo **SOA (Start of Authority)** define o servidor autorizado a responder pela zona. O campo **NS (Name Server)** define a denominação do servidor de nomes para a zona. **Registros A** associam um nome de domínio a um endereço IP.

Depois, crie o arquivo de zona reversa: `sudo nano /etc/bind/zones/db.192.168.0`

E adicione o conteúdo:

```
$TTL    604800
@       IN      SOA     ns1.exemplo.com. admin.exemplo.com. (
                        2023091201  ; Serial
                        604800      ; Refresh
                        86400       ; Retry
                        2419200     ; Expire
                        604800 )    ; Minimum TTL

        IN      NS      ns1.exemplo.com.
1       IN      PTR     ns1.exemplo.com.
2       IN      PTR     www.exemplo.com.
```

**Reiniciar o Servidor DNS**

Após configurar os arquivos, reinicie o BIND para aplicar as mudanças:

```
sudo systemctl restart bind9
```

**Testar a Configuração do Servidor DNS**

Edite o arquivo `/etc/resolv.conf` para apontar o servidor DNS para o próprio servidor local: `sudo nano /etc/resolv.conf`. Adicione: `nameserver 127.0.0.1`. Teste a resolução de nomes: `dig exemplo.com`.

Se tudo tiver ocorrido bem, este último comando deve retornar o endereço IP associado ao domínio "exemplo.com".

**Testar o DNS Reverso**

Para testar a configuração reversa, digite: `dig -x 192.168.0.1`. Esse comando deve retornar o nome de domínio associado ao IP.

## 4.3. PONTOS CRÍTICOS DURANTE A CONFIGURAÇÃO

A configuração de um servidor DNS exige atenção a diversos detalhes, sendo os erros de sintaxe, as permissões de arquivo e as configurações de firewall pontos críticos. Erros de formatação nos arquivos de zona, por exemplo, podem impedir o funcionamento correto do servidor. A utilização de comandos como `named-checkconf` e `named-checkzone` é fundamental para **validar a configuração**. Além disso, é crucial garantir que os arquivos de configuração **possuam as permissões adequadas**, geralmente pertencendo ao usuário e grupo `bind`. Por fim, a **abertura das portas 53 (TCP e UDP) no firewall** é essencial para a comunicação do servidor DNS com outros sistemas.

**A análise de logs é uma etapa crucial para a depuração de problemas.** O comando `sudo tail -f /var/log/syslog` permite acompanhar em tempo real as mensagens do BIND e outros eventos do sistema, facilitando a identificação de possíveis erros de configuração ou falhas no serviço. Ao verificar os logs, é possível obter

informações detalhadas sobre o motivo de um determinado problema, auxiliando na resolução de forma eficiente.

## REFERENCIAL

Como liberar o cache DNS no Linux (para systemd-resolved, BIND, Dnsmasq ou nscd). Blog Linux Avante. Disponível em: https://linuxavante.com/como-liberar-o-cache-dns-no-linux-para-resolvido-por-systemd-bind-dnsmasq-ou-nscd. Acesso em: 10 set. 2024.

RFC 882. Disponível em: https://www.rfc-editor.org/info/rfc882. Acesso em: 07 set. 2024.

RFC 883. Disponível em: https://www.rfc-editor.org/info/rfc883. Acesso em: 07 set. 2024.

RFC 973. Disponível em: https://www.rfc-editor.org/info/rfc973. Acesso em: 07 set. 2024.

RFC 1034. Disponível em: https://www.rfc-editor.org/info/rfc1034. Acesso em: 07 set. 2024.

RFC 1035. Disponível em: https://www.rfc-editor.org/info/rfc1035. Acesso em: 07 set. 2024.

Sistema de nomes de domínio. AcademiaLab. Disponível em: https://academia-lab.com. Acesso em: 10 set. 2024.