Domain Name System
DNS

AULA 10

Prof. Carlos Louzada

Introdução

- Em uma rede, máquinas possuem dois endereços, um endereço **físico**, definido pela placa de rede, e um endereço **lógico**, tipicamente definido pelo protocolo operando na camada de rede do modelo OSI.

- Na pilha TCP/IP endereços lógicos são chamados de endereço IP.

- Endereços IPs não são fáceis de serem recordados quanto nomes e por isso foi criado o sistema DNS.

O que é DNS?

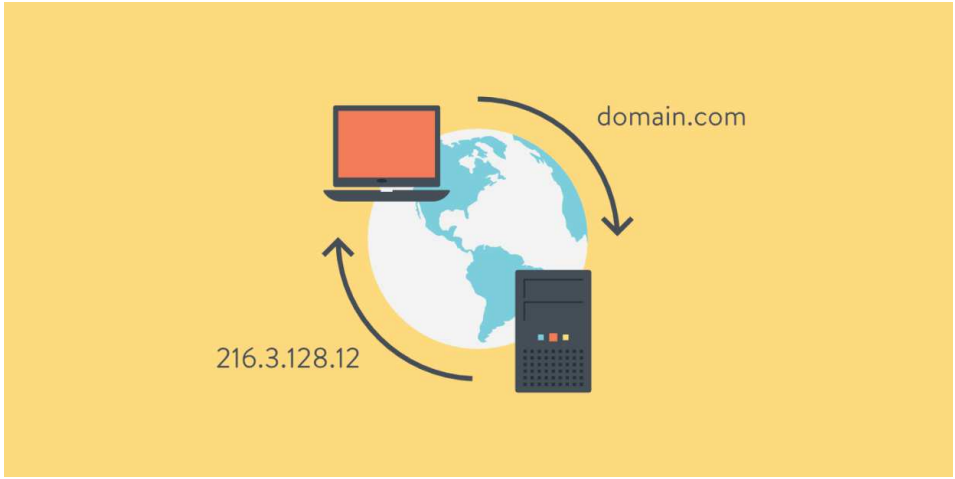
- O **Sistema de Nomes de Domínio,** mais conhecido pela nomenclatura em Inglês ***Domain Name System*** (**DNS**), é um sistema hierárquico e distribuído de gestão de nomes para computadores, serviços ou qualquer máquina conectada à Internet ou a uma rede privada.

- Faz a associação entre várias informações atribuídas a nomes de domínios e cada entidade participante.

- A sua utilização mais convencional associa nomes de domínios mais facilmente memorizáveis a endereços IP numéricos, necessários à localização e identificação de serviços e dispositivos, processo esse denominado por: **resolução de nome**.

Porta padrão

- Por padrão, o DNS usa o protocolo *User Datagram Protocol* (UDP) na **porta 53** para servir as solicitações e as requisições.



Arquitetura

- O DNS apresenta uma arquitetura cliente/servidor, podendo envolver vários servidores DNS na resposta a uma consulta.

- O servidor DNS resolve nomes para os endereços IP e de endereços IP para os nomes respectivos, permitindo a localização de *hosts* num determinado domínio.

hosts = qualquer equipamento ativo na rede.

Berkeley Internet Name Domain
BIND

- É o servidor para o protocolo DNS mais utilizado na Internet, especialmente em sistemas do tipo Unix, onde ele pode ser considerado um padrão *de facto*.

- Foi criado por quatro estudantes de graduação, membros de um grupo de pesquisas em ciência da computação da Universidade de Berkeley, e foi distribuído pela primeira vez com o sistema operacional 4.3BSD.

- O programador Paul Vixie, enquanto trabalhava para a empresa DEC, foi o primeiro mantenedor do BIND. Atualmente o BIND é suportado e mantido pelo ***Internet Systems Consortium***.

- O **BIND** geralmente encontra-se localizado no servidor DNS primário.
- O servidor DNS secundário é uma espécie de cópia de segurança do servidor DNS primário.
- Assim, é uma parte necessária para quem quer usar a internet de uma forma mais fácil, evita que hackers roubem dados pessoais.

Servidores-Raiz

- Existem centenas de servidores-raiz DNS (root servers) no mundo todo, agrupados em **13 zonas DNS raiz**, das quais sem elas a Internet não funcionaria.

- Dez estão localizados nos Estados Unidos da América;
- Dois na Europa; e
- Um na Ásia.

- Para aumentar a base instalada destes servidores foram criadas réplicas localizadas por todo o mundo, inclusive no Brasil desde 2003.

Hierarquia

Devido ao tamanho da Internet, armazenar todos os pares domínio - endereço IP em um único servidor DNS seria inviável por questões de escalabilidade, que incluem:

- **Disponibilidade:** se o único servidor de DNS falhasse, o serviço se tornaria indisponível para o mundo inteiro;
- **Volume de tráfego:** o servidor deveria tratar os pedidos DNS do planeta inteiro;
- **Distância:** grande parte dos usuários estaria muito distante do servidor, onde quer que ele fosse instalado, gerando grandes atrasos para resolver pedidos DNS;
- **Manutenção do banco de dados:** o banco de dados deveria armazenar uma quantidade de dados enorme e teria que ser atualizado com uma frequência muito alta (assim que um novo domínio fosse associado a um endereço IP).

Divisão do DNS

Os servidores DNS se dividem nas seguintes categorias:

- Servidores-raiz;
- Servidores de domínio de topo;
- Servidores com autoridade.

Servidores Raiz

- No topo da hierarquia estão os 13 servidores raiz.
- Um servidor-raiz (*root name server*) é um servidor de nome para a zona raiz do DNS (Domain Name System).
- A sua função é responder diretamente às requisições de registros da zona raiz e responder a outras requisições retornando uma lista dos servidores de nome designados para o domínio de topo apropriado.
- Os servidores raiz são parte crucial da Internet porque são o primeiro passo em resolver nomes para endereços IP, esses últimos usados para comunicação entre hosts.

Servidores de domínio de topo *top-level domain*

- Cada domínio é formado por nomes separados por pontos. O nome mais à direita é chamado de domínio de topo.

  Ex.: .com, .org, .net, .edu, .inf, .gov.

- Cada servidor de domínio de topo conhece os endereços dos servidores autoritativos que pertencem àquele domínio de topo, ou o endereço de algum servidor DNS intermediário que conhece um servidor autoritativo.

- Há também terminações orientadas a países, chamadas de Código de País para Domínios de Topo/Primeiro Nível (*Country Code Top Level Domains*).
  Ex.: .br para o Brasil, .ar para a Argentina, .fr para a França e assim por diante. Há também combinações, como .com.br e .blog.br.

Servidores com autoridade

- O servidor com autoridade de um domínio possui os registros originais que associam aquele domínio a seu endereço de IP.

- Toda vez que um domínio adquire um novo endereço, essas informações devem ser adicionadas a pelo menos dois servidores autoritativos.

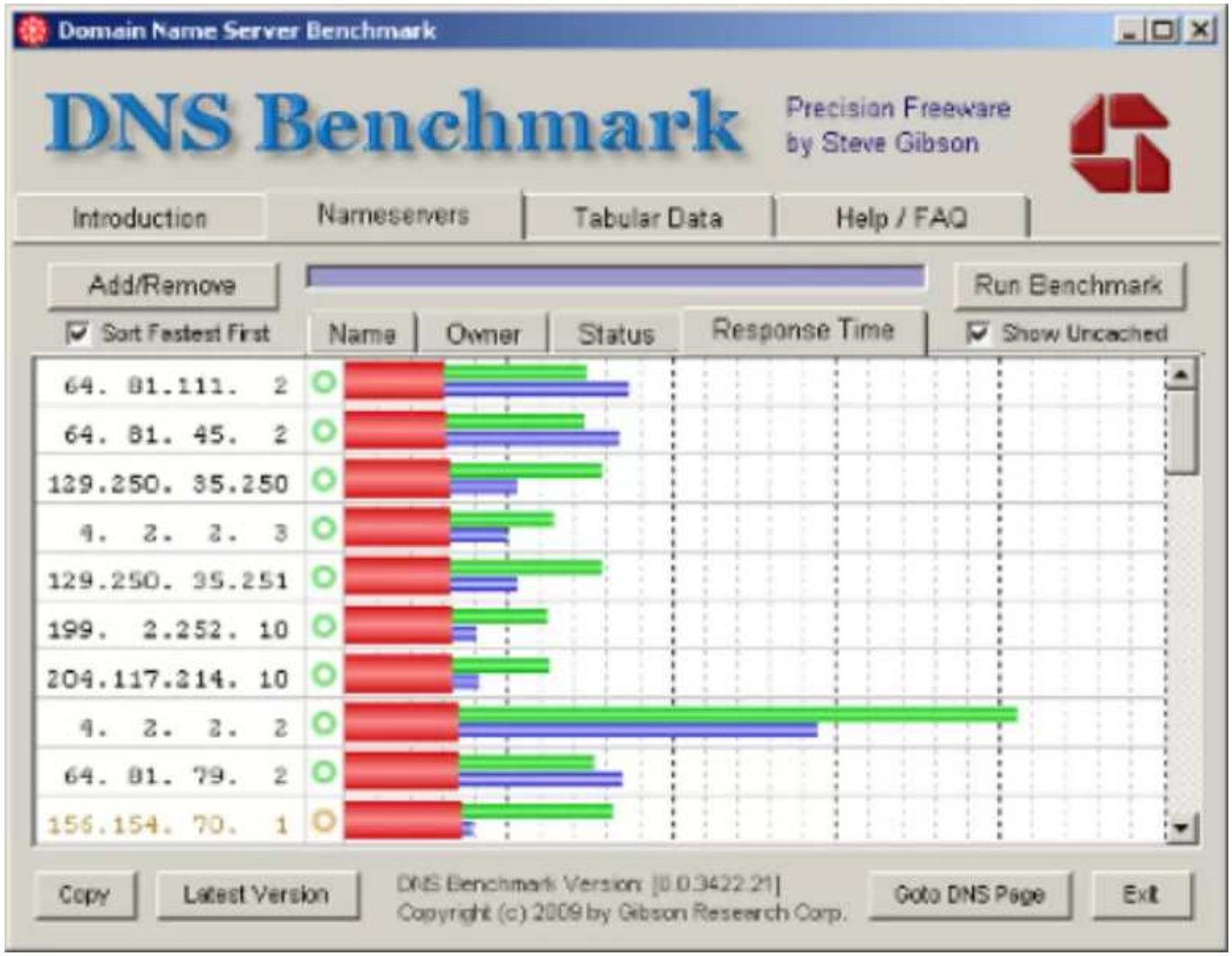
- Um deles será o servidor autoritativo principal e o outro, o secundário. Isso é feito para minimizar o risco de, em caso de erros em um servidor DNS, perder todas as informações originais do endereço daquele domínio.

Comando

- Para um exemplo real de funcionamento do protocolo DNS, você pode usar o comando **nslookup** para descobrir o endereço IP de um determinado servidor. Por exemplo:

- **C:\nslookup www.google.com.br**

CUIDADO!
Você precisa escolher o seu serviço com cuidado - nem todos os provedores serão necessariamente melhores do que o seu ISP



Seu ISP atribuirá servidores DNS sempre que você se conectar à internet, mas nem sempre é a melhor escolha de servidor DNS disponível.

Servidores DNS lentos podem causar um atraso antes que os sites comecem a carregar, e se o seu servidor às vezes cair, você não conseguirá acessar nenhum site.

DNS Públicos

- Mudar para um servidor DNS público gratuito pode fazer uma diferença real, com navegação mais responsiva e registros longos de 100% do tempo de atividade, o que significa que há muito menos chance de problemas técnicos.

- Alguns serviços também podem bloquear o acesso a sites de **phishing** ou infectados, e alguns oferecem filtragem de conteúdo para manter seus filhos longe do pior da web.

Algumas coisas a serem observadas:

- **DNS padrão vs. DNS de terceiros -** Quando você tem serviço de Internet, seu provedor de serviços de Internet (ISP) tem um DNS padrão, que sua rede usa para se conectar à web. Os ISPs podem coletar dados sobre clientes e suas atividades na Internet. Um DNS de terceiros pode fazer o mesmo, embora seja mais difícil atribuir a conexão a indivíduos ou famílias específicas.

- **DNS gratuito vs. DNS pago -** além da óbvia diferença financeira entre um DNS gratuito e pago, as opções gratuitas geralmente têm menos recursos. Um DNS pago terá segurança mais avançada e funcionalidade de desempenho, bem como melhor suporte ao cliente e mais opções de personalização. Mas de modo geral, um DNS gratuito lhe fornecerá a maioria das finalidades.

DNS público vs. DNS privado

- Um DNS público está disponível para a população em geral, e normalmente vem do seu provedor de serviços de Internet ou de um provedor DNS dedicado.

- Já um DNS privado é normalmente usado por empresas para fornecer aos funcionários acesso mais fácil a sites ou endereços IP internos.

- Normalmente, você pode usar um DNS público em casa e em um DNS público ou privado no trabalho.

DNS Públicos

- OpenDNS;
- Cloudflare;
- DNS Google;
- QUAD9;
- AdGuard DNS;
- CleanBrowsing

OpenDNS

- Propriedade da Cisco, o OpenDNS tem duas opções gratuitas: Family Shield e Home. O Family Shield é bom para pais que querem ter certeza de que seus filhos não estão acessando conteúdos impróprios. Já o Home se concentra na segurança e no desempenho da Internet.

- DNS primário: 208.67.222.222
- DNS secundário: 208.67.220.220

Endereços IPv6 também estão disponíveis:

- DNS primário: 2620: 119: 35 :: 35
- DNS secundário: 2620: 119: 53 :: 53

Cloudflare

- O Cloudflare desenvolveu o 1.1.1.1 para ser o "serviço DNS mais rápido do mundo" e nunca registrará seu endereço IP, nunca venderá seus dados e nunca usará seus dados para direcionar anúncios.

  - DNS primário: 1.1.1.1
  - DNS secundário: 1.0.0.1

Eles também têm servidores DNS públicos IPv6:

- DNS primário: 2606: 4700: 4700 :: 1111
- DNS secundário: 2606: 4700: 4700 :: 1001

DNS do Google

- O produto DNS do próprio Google também é gratuito. Ele se concentra na velocidade, segurança e validade dos resultados, de acordo com a empresa. Ele oferece apenas resolução de DNS e cachê, e não há bloqueio de site com DNS público.

  - DNS primário: 8.8.8.8
  - DNS secundário: 8.8.4.4

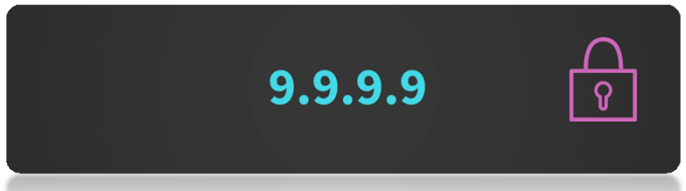
O Google também oferece versões IPv6:

- DNS primário: 2001: 4860: 4860 :: 8888
- DNS secundário: 2001: 4860: 4860 :: 8844

QUAD9

- O Quad9 possui servidores DNS públicos gratuitos que protegem seu computador e outros dispositivos de ameaças cibernéticas, bloqueando imediatamente e automaticamente o acesso a sites inseguros e sem armazenar seus dados pessoais.

  - DNS primário : 9.9.9.9
  - DNS secundário : 149.112.112.112



Existem também servidores DNS IPv6 Quad 9:

- DNS primário : 2620: fe :: fe
- DNS secundário : 2620: fe :: 9

AdGuard DNS

- O AdGuard DNS tem dois conjuntos de servidores DNS, os quais bloqueiam anúncios em jogos, vídeos, aplicativos e páginas da web. O conjunto básico de servidores DNS são chamados de servidores "Padrão" e bloqueiam não apenas anúncios, mas também sites de malware e phishing:

    - DNS primário: 176.103.130.130

    - DNS secundário: 176.103.130.131

IPv6 também é compatível:

- DNS primário: 2a00: 5a60 :: ad1: 0ff

- DNS secundário: 2a00: 5a60 :: ad2: 0ff

CleanBrowsing

- A CleanBrowsing tem três opções de servidores DNS públicos gratuitos: um filtro de segurança, um filtro adulto e um filtro familiar. Estes são os servidores DNS para o filtro de segurança, o mais básico dos três que é atualizado a cada hora para bloquear sites de malware e phishing:

    - DNS primário: 185.228.168.9

    - DNS secundário: 185.228.169.9

Compatibilidade IPv6:

- DNS primário: 2a0d: 2a00: 1 :: 2

- DNS secundário: 2a0d: 2a00: 2 :: 2

Referências Bibliograficas

- https://www.oficinadanet.com.br/internet/32378-os-6-melhores-servidores-dns-publicos-de-2020

- Torres, Gabriel. Redes de Computadores, 2ª edição. Nova Terra, 2014.