INSTITUTO FEDERAL DE EDUCAÇÃO, CIÊNCIA E TECNOLOGIA RIO GRANDE DO NORTE

Professor: Macêdo Firmino
Disciplina: Arquitetura de Rede
Prática 17: Protocolo DNS

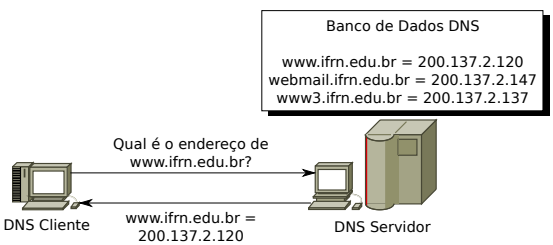
Na aula de hoje iremos conhecermos o funcionamento básico do protocolo DNS (Domain Name System), realizar consultas DNS manualmente. Aprenderemos ainda uma ferramenta do Windows, chamada de `nslookup`. Por último iremos realizar algumas experiência com um analisar de tráfego (Wireshark) sobre o respectivo protocolo.

Protocolo DNS

À medida que a internet cresceu, tornou-se impraticável depender apenas de endereços IP para localizar recursos. O sistema DNS (Domain Name System) funciona como um serviço de "tradução" que converte nomes de domínio legíveis por humanos (como www.google.com ou ifrn.edu.br) em endereços IP, que são as identificações numéricas usadas pelos computadores para localizar e se comunicar com servidores e outros dispositivos na rede. Sem o DNS os usuários teriam que memorizar os endereços IPs para acessar qualquer serviço online.

Para compreender melhor por que o DNS é necessário, é importante diferenciar endereços IP e nomes de domínio. O endereço IP (como 142.250.78.206 ou 2800:3f0:4001:80c::200e) é uma identificação numérica utilizada pelos dispositivos para se comunicarem. Porém, esses números são difíceis de memorizar e não têm significado intuitivo para os usuários. Já os nomes de domínio são representações textuais amigáveis, criadas para facilitar o uso da rede. Eles são formados por palavras e estruturas hierárquicas, como nome.tld, sendo muito mais simples de lembrar e digitar. É por isso que digitamos www.youtube.com em vez do seu endereço IP real.

O DNS opera em uma estrutura hierárquica e distribuída, envolvendo vários servidores e etapas para resolver um nome de domínio em um endereço IP, proporcionando redundância e tolerância a falhas.



Por exemplo, quando você digita um nome de domínio (por exemplo, www.ifrn.edu.br) no navegador, o computador envia uma consulta DNS para um servidor DNS (geralmente fornecido pelo seu provedor de internet ou um serviço como o Google DNS). O servidor DNS retorna o endereço IP ao seu computador, permitindo que ele se conecte ao servidor correto e carregue o site.

O DNS que é um protocolo da camada de aplicação e utiliza o protocolo de transporte UDP na porta 53 (ou TCP na porta 53 quando uma resposta for superior a 512 *bytes*).

Para evitar ambiguidades, os nomes atribuídos às máquinas devem ser cuidadosamente selecionados a partir de um espaço de nomes (name space) com total controle sobre o relacionamento entre os nomes e os endereços IP. Em outras palavras, os nomes devem ser exclusivos, pois os endereços IP também são. Entretanto, os nomes não fazem distinção entre letras maiúsculas e minúsculas. Portanto, "edu", "Edu" e "EDU" têm o mesmo significado.

Em um espaço de nomes hierárquico, cada nome é constituído por várias partes componentes. A primeira parte pode definir a natureza da organização, a segunda pode estabelecer o nome de uma organização, a terceira pode determinar departamentos dentro de uma organização e assim por diante. Estas porções são separadas por pontos, por exemplo, `www.ifrn.edu.br`;

br: o nome mais a direita é chamado de domínio de nível superior;

edu: é uma subdivisão do domínio "br" (chamado de subdomínio)

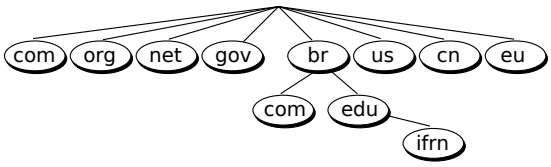
ifrn: é uma subdivisão do domínio "edu.br"

www: é o nome que tem um endereço IP associado. Neste caso `www.ifrn.edu.br` = 200.137.2.130.

Existem dois tipos de domínios (espaços de nome) de nível superior:

- Domínios genéricos: "com" (comercial), "edu" (instituições educacionais), "gov" (instituições governamentais), "int" (certas organizações internacionais), "mil" (órgãos das forças armadas), "org" (organizações sem fins lucrativos) e etc;

- Domínios de países: “br” (Brasil), “us” (Estados Unidos), “eu” (União Européia), “ar” (Argentina) e etc.



O DNS foi projetado como uma aplicação cliente/servidor. Um equipamento que precisa mapear um endereço a um nome ou um nome a um endereço chama um cliente DNS denominado resolvedor. O resolvedor acessa o servidor DNS configurado na interface de rede e realiza uma solicitação de mapeamento. Se o servidor tiver a informação, ele atende à solicitação do resolvedor; caso contrário, faz que o resolvedor consulte outros servidores ou então solicita que outros servidores forneçam a informação.

Cada vez que um servidor DNS recebe uma consulta para um nome de domínio que não se encontre em seu domínio, ele precisa pesquisar em seu banco de dados para identificar o endereço IP de outro servidor. A redução desse tempo de busca aumentaria a eficiência do processo. O DNS trata essa questão com um mecanismo denominado caching. Quando o servidor DNS solicita o mapeamento de outro servidor e recebe a resposta, ele armazena essas informações em sua memória cache antes de transmiti-la ao cliente. Se este ou outro cliente solicitar o mesmo mapeamento, o servidor DNS verifica em sua memória cache e tenta resolver o problema.

Registro.br

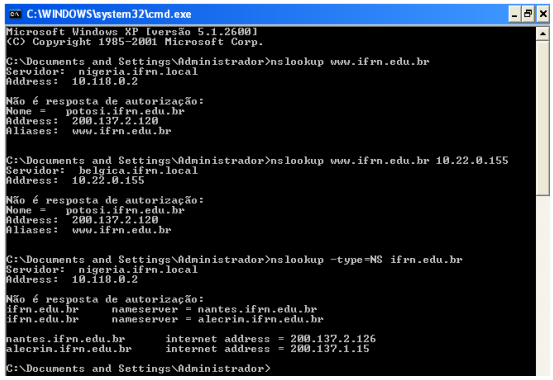
O Registro.br (`https://registro.br`) é o orgão brasileiro responsável pelas atividades de registro e manutenção dos nomes de domínios que usam o ”.br”. Também executa o serviço de distribuição de endereços IPv4 e IPv6 no país.

nslookup

A ferramenta `nslookup` permite que o *host* consulte qualquer servidor DNS especificado para um registro de DNS. Para realizar essa tarefa, `nslookup` envia uma consulta DNS para o servidor DNS especificado, recebe uma resposta do servidor DNS e exibe o resultado.

Para executar o `nslookup` no Linux/Windows, basta digitar o comando nslookup na linha de comando. Para executá-lo no Windows, abra o Prompt de Comando (o mesmo se encontra em Iniciar/ Acessórios) e execute o `nslookup` na linha de comando.

Na Figura é apresentado três exemplos da utilização do comando `nslookup`. No primeiro caso, quando utilizamos o `nslookup` sem especificar o servidor DNS, então o `nslookup` envia as perguntas para o servidor DNS padrão (da rede), que neste caso é 187.19.145.5, na porta 53.




```
nslookup www.ifrn.edu.br
```

Como resultado o nosso servidor respondeu com o endereço IP (200.137.2.120), do *host* `www.ifrn.edu.br`. Informou ainda que este *host* também possui o nome `potosi.ifrn.edu.br`. No entanto, `nslookup` também indica que a resposta é “não-autorizada”, o que significa que esta resposta veio a partir do *cache* de algum servidor ao invés de um servidor DNS do IFRN autoritativo.

No segundo caso, foi inidicado que desejamos enviar as perguntar para o servidor DNS 10.22.0.155 ao invés do nosso servidor local. Desta forma, o servidor 10.22.0.155 fornece o respectivo endereço IP (200.137.2.120) do *host* `www.ifrn.edu.br`.

```
nslookup www.ifrn.edu.br 8.8.8.8
```

ipconfig

O comando `ipconfig` é uma ferramenta de linha de comando do Windows que já utilizamos em nossas aulas. Ele exibe todos os valores de configuração de rede TCP/IP e atualiza as configurações do protocolo de configuração dinâmica de *hosts* (DHCP) e do sistema de nomes de domínios (DNS).

Hoje iremos utiliza-lo para manipular o cache DNS do Windows da seguinte forma:

***/displaydns*:** Exibe o conteúdo de *cache* de resolução de DNS.

***/flushdns*:** Limpa o *cache* de resolução DNS;

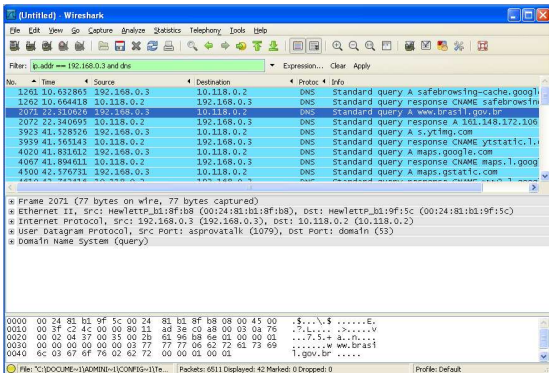
Mensagens DNS com o Wireshark

Para Analisarmos o protocolo DNS, iremos capturar as mensagens trocadas como resultado da execução de alguns comandos. Forme duplas e realize as seguintes etapas são:

1. Use prompt de comando do Windows e digite "ipconfig /flushdns" para limpar o cache DNS do seu computador;

2. Abra seu browser;

3. Abra o Wireshark e começe a capturar o tráfego (na interface Conexão Local ou Ethernet);



4. Utilize 'dns" no campo filter. Este filtro irá remover todos os pacotes que não são DNS;

5. Com seu browser, visite a página Web: `https://www.brasil.gov.br`;

6. Utilize o nslookup `www.ifrn.edu.br`;

7. Pare a captura e analise as informações DNS trocadas. Utilize o filtro dns.qry.name == "www.brasil.gov.br" e o filtro dns.qry.name == "www.ifrn.edu.br".

Exercícios

Formem duplas e responda os seguintes questionamentos abaixo:

1. O que é o sistema DNS? Como ele funciona?

2. O DNS utiliza qual protocolo de transporte? Qual é a porta de origem do servidor DNS?

3. Com o comando nslookup, descobra qual é o endereço IP dos domínios:

- www.gmail.com;
- www.youtube.com;
- web.whatsapp.com;
- www.facebook.com;
- www.spotify.com.

4. Escrevam as respostas num documento de texto e insira no Google Sala de Aula.

Configuração DNS/DHCP com o Packet Tracer

Neste exemplo vamos utilizar o protocolo DNS no Cisco Packet Tracer. Em outras palavras, veremos como configurar um servidor DNS. Iremos configurar ainda um servidor DHCP para configurar os endereços dos computadores clientes. Para maiores informações sobre o servidor DHCP observe a aula Prática 10.

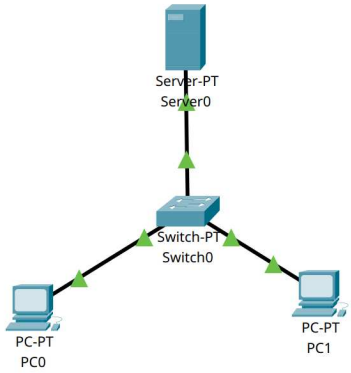
01. Inicie o simulador Packet Tracer em seu computador.

02. No menu na Barra de Dispositivos (canto inferior esquerdo), selecione os dispositivos necessários:

- Switch: Vá para "Network Devices"  e no subgrupos selecione "Switch". Clique em Switch-PT arraste um ele para a área de trabalho.
- Computadores: Vá para "End Devices"  e arraste 2 "PC-PT" para a área de trabalho.
- Servidor: Vá em "End Devices"  e arraste 1 "Server-PT" para a área de trabalho.

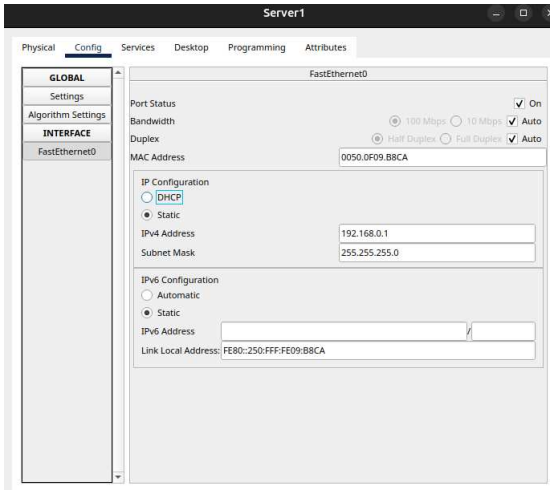
03. Agora iremos conectar estes dois PCs e o Switch através de um cabo UTP. Para isso, clique no símbolo de um raio avermelhado  e depois novamente no raio avermelhado  , desta forma será selecionado o cabo automaticamente.

Os equipamentos interligados ficará da seguinte forma:

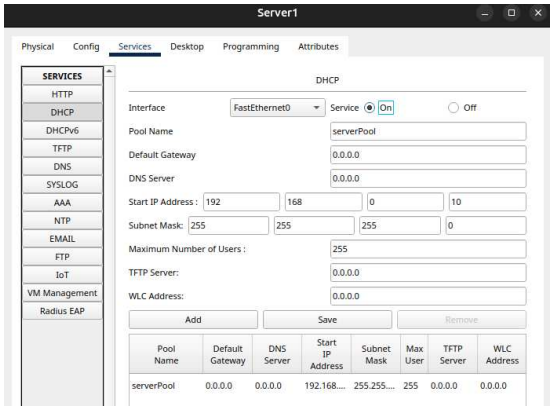


04. No servidor, clique duas vezes para abrir a janela de configuração. Vá para a aba "Config", "Interface" e "FastEthernet". Em IP Configuration selecione "Static" e insira em:

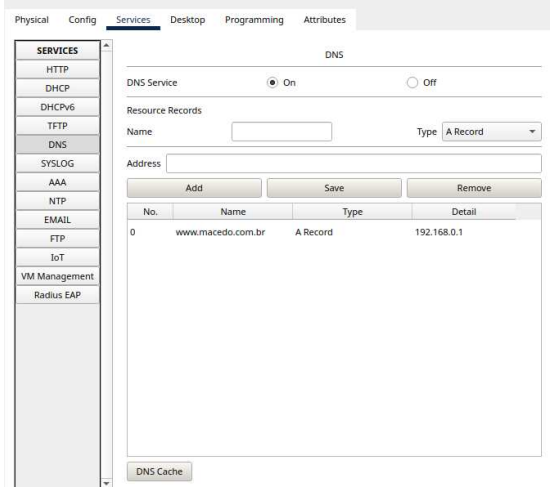
- IPv4 Address: 192.168.0.1;
- Subnet Mask: 255.255.255.0.



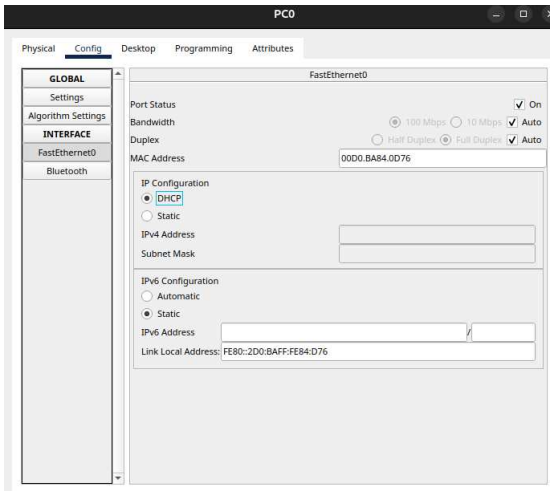
05. Ainda no servidor, na aba, "Services", "DHCP", "Service" selecione "On". Em "Start IP Address" coloque 192.168.0.10. Em DNS Server insira 192.168.0.1. Por último, clique em "Save".



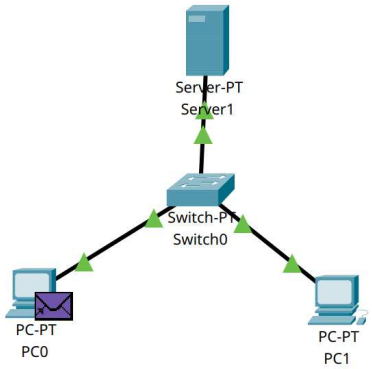
06. Ainda no servidor, na aba, "Services", "DNS", "DNS Service" selecione "On". Em "Name" coloque www.macedo.com.br e em "Address" insira 192.168.0.1 em clique em "Add".



07. Agora vamos configurar a rede nas máquinas. Clique duas vezes em cada PC para abrir a janela de configuração. Vá para a aba "Desktop" e selecione "IP Configuration" e selecione a opção "DHCP".

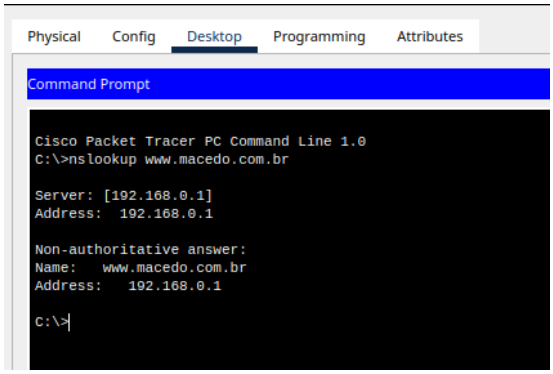


Espere uns 30 segundos para os computadores conseguirem obter as informações do servidor DHCP e se configurar. Depois realize o teste de conectividade com o "Add Simple PDU"  no canto superior da tela.



08. Agora vamos testar o mapeamento DNS. Em um cliente clique duas vezes para abrir a janela de configuração. Vá para a aba "Desktop" e selecione "Command Prompt".

09. No prompt digite nslookup www.macedo.com.br e verificar se obtemos o seu respectivo endereço IPv4 (192.168.0.1).



Exercícios

5. Em dupla realize as configurações do servidor DNS e DHCP e das máquinas clientes. Depois encaminhe pacotes de PC1 para PC2 e verifique que há conectividade entre os equipamentos. Insira um registo DNS (www.info3v.com.br) e teste o seu mapeamento. Grave um vídeo (da tela do computador ou celular) com o respectivo testes. Depois, anexe um arquivo com os resultados dos exercícios anteriores e o vídeo no Google Sala de Aula e informe os componentes do grupo nos comentários da postagem.