

Redes parte 1: Conceitos e Práticas

Bibliografia:

Todo o material foi retirado do curso: Redes parte 1: conceitos e prática

Instrutor: Rafael Silva Nercessian

Rafael é formado em engenharia elétrica com ênfase em telecomunicações, trabalhou quatro anos na parte de infraestrutura e possui certificação Cisco CCNA 200-125, também já trabalhou com Java, PHP, AWS, Wordpress, SugarCRM, React Native etc. Morou na Nova Zelândia trabalhando como desenvolvedor e sonha um dia morar em Seoul, na Coreia do Sul.

<https://www.linkedin.com/in/rafael-silva-nercessian-18226944/>

Faça esse curso de Redes e:

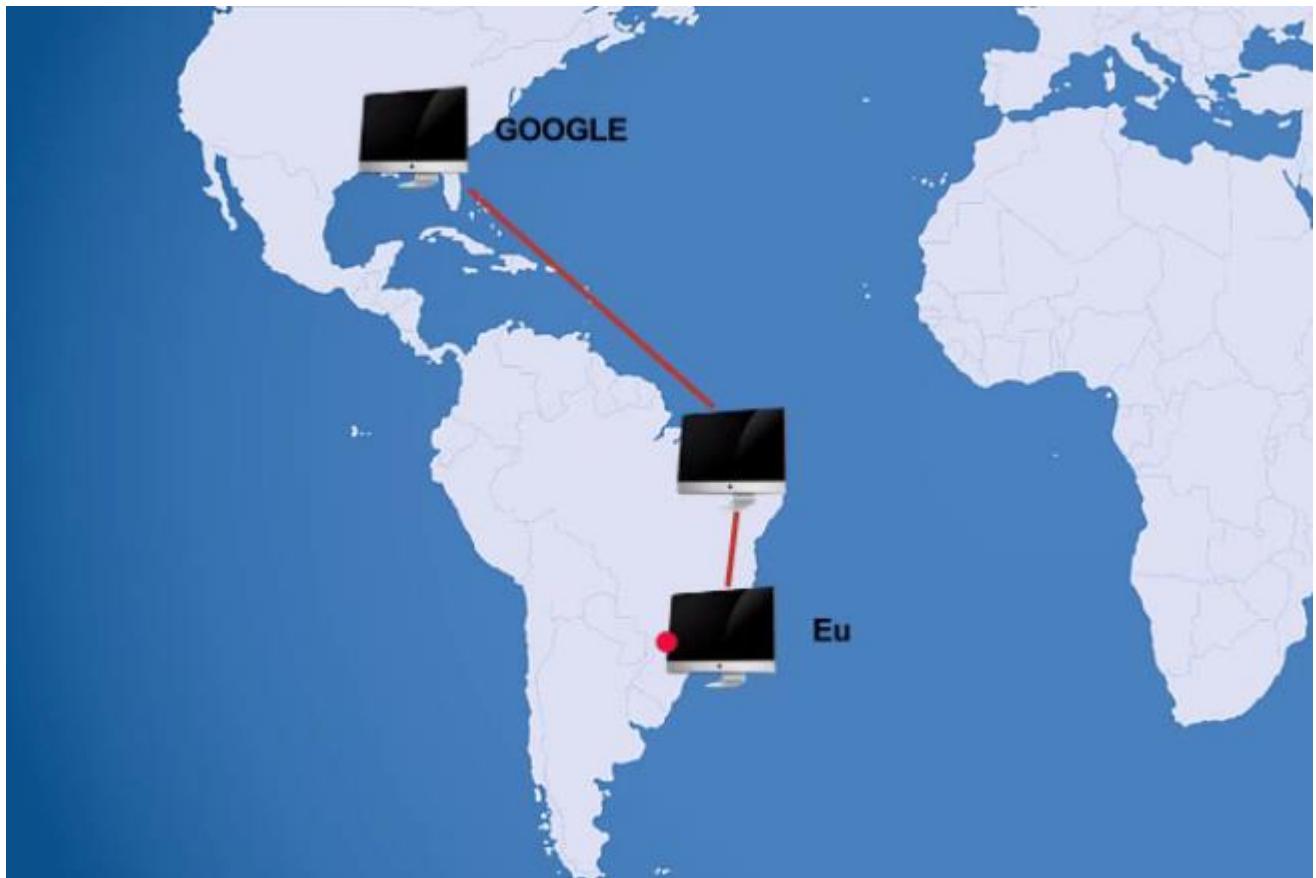
- Aprenda o que é Hub, Switch, Roteador, DHCP, DNS, IP e muito mais
- Fique por dentro de alguns tipos de ataques que usuários maliciosos podem fazer
- Aprenda como utilizar o programa de simulação de redes Packet Tracer
- Saiba como configurar equipamentos de rede da Cisco
- Coloque tudo isso em prática no Windows, OSX ou Linux no projeto que montaremos

Todos os direitos reservados, não é permitida a cópia e distribuição deste material

O primeiro ponto que precisamos entender é justamente o conceito de **rede**. Por exemplo, estamos na cidade de São Paulo e acesso o site do Google.

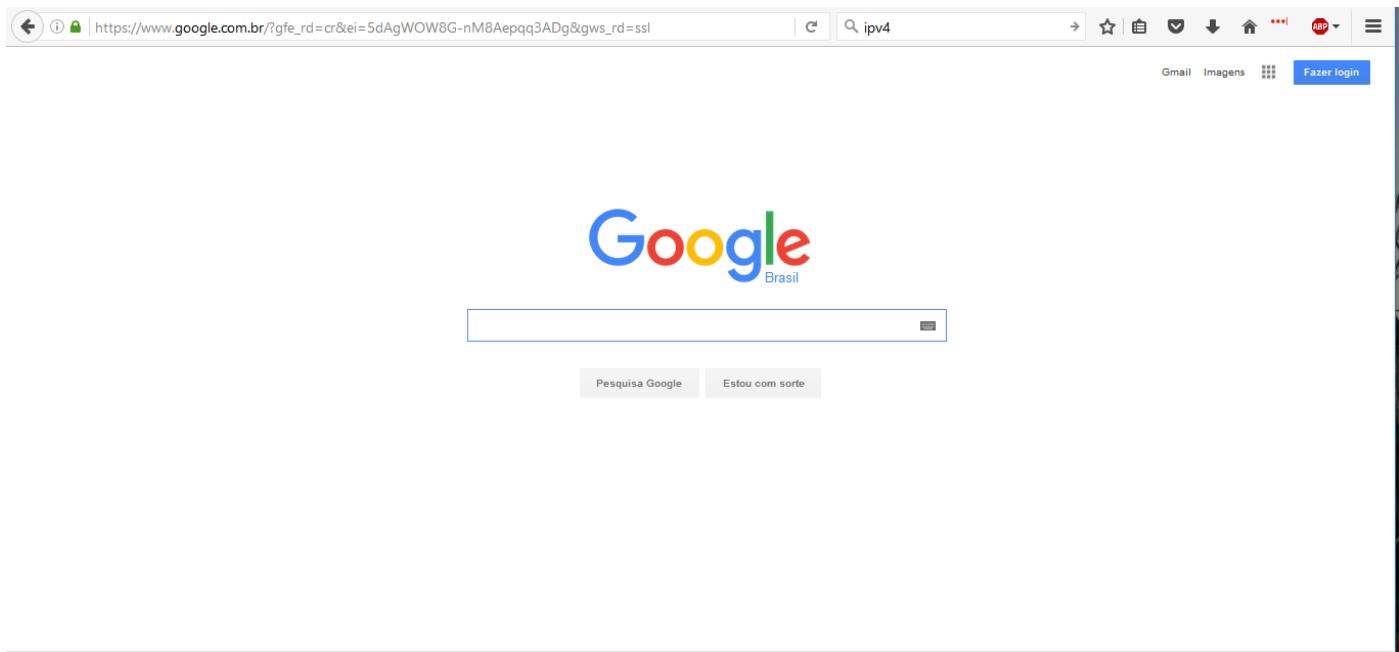


Será que existe uma conexão direta entre a minha máquina e a do Google? Não, caso contrário seria necessário fazer o mesmo em todas as máquinas do mundo, o que seria completamente inviável. O que acontecerá na verdade, é que a requisição enviada para a máquina do Google passará por várias máquinas intermediárias espalhadas em diversas regiões e estas serão responsáveis por encontrar uma forma de levar a informação para a máquina do Google. Já a máquina do Google perceberá que queremos acessar o seu serviço e devolverá a informação para as máquinas intermediárias até chegar finalmente no meu computador.



As diversas máquinas que estão interconectadas em diferentes pontos, capazes de transportar as informações, é o que caracterizam a nossa rede. As redes existem em diversos tamanhos. Desde um ambiente doméstico, em que temos dois computadores e uma impressora, até grandes corporações com centenas de usuários, máquinas potentes com servidores, até a mais famosa, a **internet**.

Observe que quando digitamos no browser www.google.com.br, o site do Google aparecerá na tela.



Mas como o meu computador consegue identificar a máquina do Google? Deve existir uma forma de identificação dessas máquinas.

Vamos lembrar como era alguns anos atrás quando ainda enviávamos cartas: por exemplo, eu gostaria de enviar uma carta para o meu irmão Ricardo que mora na avenida Paulista. Para isto, eu escrevia no envelope que a carta era destinada para o meu irmão Ricardo e qual era o endereço, no caso Avenida Paulista. Quando eu entregasse a carta nos Correios, o carteiro teria como saber onde entregar. No mundo da internet, o processo de identificação será parecido. O processo de identificação das máquinas é chamado de endereçamento IP. Vamos ver como ele funciona.

Abriremos o pesquisar do computador, e digitaremos `cmd` e abrir o Terminal. Depois, usaremos o seguinte comando `ipconfig` (no Mac, seria `ifconfig`).

C:\ Prompt de Comando

```
Endereço IPv4 . . . . . : 192.168.3.3
Máscara de Sub-rede . . . . . : 255.255.255.0
Gateway Padrão. . . . . :
```

Adaptador Ethernet Ethernet:

```
Sufixo DNS específico de conexão. . . . . : home
Endereço IPv4 . . . . . : 192.168.1.35
Máscara de Sub-rede . . . . . : 255.255.255.0
Gateway Padrão. . . . . : 192.168.1.1
```



Adaptador Ethernet Conexão de Rede Bluetooth:

```
Estado da mídia. . . . . : mídia desconectada
Sufixo DNS específico de conexão. . . . . :
```

Adaptador de túnel isatap.home:

```
Estado da mídia. . . . . : mídia desconectada
Sufixo DNS específico de conexão. . . . . : home
```

Adaptador de túnel isatap.{48869A9E-B89A-4A10-93E7-87104C1D3363}:

```
Estado da mídia. . . . . : mídia desconectada
Sufixo DNS específico de conexão. . . . . :
```

C:\Users\Alura>

Observe que eu receberei uma série de informações do Terminal.

O número sinalizado é o IP da máquina que está sendo utilizada por mim, na gravação deste curso. Trata-se da identificação da máquina. O Google também terá um número com um formato parecido com este, que identificará essa máquina do Google.

Nós conseguimos acessar o site do Google, é razoável concluirmos que existe uma conectividade com essa máquina. Nos casos em que não temos uma conectividade com uma máquina, como conseguimos saber se a máquina que quero me comunicar dentro da minha rede se ela ativa ou está apta para a conexão? Para isto, existe uma ferramenta administrativa chamada **ping**.

No terminal, escreveremos **ping**. Depois, precisaremos especificar qual máquina queremos fazer o teste de conectividade, por exemplo não sabemos qual é o número de identificação do Google. No celular, os nossos contatos são salvos com um nome que iremos selecionar se quisermos fazer uma ligação. Mas a discagem não será feita para o nome do contato, mas para o número de telefone que está cadastrado. Deve haver algo parecido com este mapeamento entre nome e número na internet.

(03:45) Por exemplo, quando digitamos no nosso navegador o endereço do Google, o que ocorre é uma tradução da URL para o endereçamento IP. O responsável por fazer esta tradução, o mapeamento é o chamado servidor DNS.

Então, de volta ao Terminal, podemos escrever o **ping** e a URL que queremos testar. No nosso caso, podemos testar a conectividade do Google.

```
C:\Users\Alura>ping www.google.com.br
```

Veja o que acontecerá na saída:

```
C:\Users\Alura>ping www.google.com.br

Disparando www.google.com.br [216.58.202.3] com 32 bytes de dados:
Resposta de 216.58.202.3: bytes=32 tempo=117ms TTL=54
Resposta de 216.58.202.3: bytes=32 tempo=116ms TTL=54
Resposta de 216.58.202.3: bytes=32 tempo=118ms TTL=54
Resposta de 216.58.202.3: bytes=32 tempo=116ms TTL=54

Estatísticas do Ping para 216.58.202.3:
  Pacotes: Enviados = 4, Recebidos = 4, Perdidos = 0 (0% de perda),
Aproximar um número redondo de vezes em milissegundos:
  Mínimo = 116ms, Máximo = 118ms, Média = 116ms

C:\Users\Alura>
```

Observe que ocorreu a tradução da URL, para o endereçamento IP, usado para a identificação.

(04:50) Como a informação do ping trabalhará? Dentro dela existe um protocolo chamado de ICMP (uma sigla que significa, Internet Control Message Protocol), que funcionará de forma semelhante a um telefonema. É como se pegássemos um telefone e ligássemos para a máquina do Google, na esperança de que alguém atenda. Dentro da informação enviada, falaremos algo que será representado pelos 32 bytes que aparecem no retorno.

(05:31) A máquina do Google respondeu, vemos pelo IP, e vemos o tempo que a informação levou do meu computador passar pela máquina do Google e retornar. Isto é chamado de tempo de **ida e volta** ou RTT (Round trip time). Para que seja feita essa conexão, precisamos passar por diversas máquinas intermediárias, que podem estar configuradas de diversas formas que caracterizem o loop, porque existe várias interconexões. Imagine a situação em que a nossa informação enviada fique trafegando eternamente no loop, consumindo recursos... Iria travar tudo, Não seria algo muito bom.

(06:35) - Justamente por isso, o "pacote" de informação terá um tempo de vida útil e a cada passagem entre essas máquinas, ele irá decrementar em uma unidade representado pelo índice **TTL** (Time to Live). No nosso exemplo, quando a informação passar por 54 máquinas, o valor será zerado e será extinguido.

(06:58) - Se continuarmos a análise do ping, veremos que foram enviados **quatro** pacotes para a máquina do Google, que devolveu todos. Isto significa que a conectividade com a máquina está funcionando perfeitamente.

Dentro da ferramenta administrativa do ping temos o protocolo ICMP, sendo ele o responsável por mandar uma requisição (Echo Request) para máquina remota e esperar um retorno dessa máquina remota (Echo Reply).

Quando temos um alto valor no índice do tempo do teste do ping, isso significa que podemos ter um problema em nossa comunicação. O protocolo ICMP que está dentro do ping manda um Echo request e aguarda um retorno de resposta da máquina destino (Echo Reply). Dessa forma, o tempo elevado pode indicar um problema na comunicação que pode estar tanto em um trecho como em outro.

O TTL seria uma informação dentro do pacote do IP que informa qual é a máxima quantidade de hops que minha informação pode passar antes de ser descartada. É a quantidade de máquinas que ela vai poder passar no caminho.

Ao digitarmos www.google.com, ocorre uma tradução entre o nome e o endereço IP da máquina do google que estamos acessando. As máquinas para serem identificadas na rede devem possuir um endereçamento IP.

Dentro do ping temos o protocolo ICMP responsável por fazer a requisição até uma máquina remota (Echo Request) e esperar a resposta (Echo Reply). Através desse protocolo ICMP, podemos verificar se temos uma resposta da máquina remota, sabendo assim se temos conectividade.

O traceroute seria usado para verificar a rota que minha informação percorreu até chegar o destino.

O ipconfig seria usado para ver as configurações de IP de minha máquina e o nslookup seria para verificarmos recursos mais avançados de problemas que podemos ter entre a url e o endereço IP.

Vamos agora testar a conectividade de nosso computador com a máquina do Google, para isso siga os passos abaixo referente a seu sistema operacional.

- Caso esteja usando Windows, vá até o campo pesquisar e digite “cmd”. Na tela que abrir digite: ping www.google.com
- Caso esteja usando Mac, vá até o spotlight (lupa) no canto superior direito e digite terminal. Selecione a opção e posteriormente ao abrir a tela preta digite: ping www.google.com
- Caso esteja usando o Linux, no campo de pesquisa digite terminal e selecione a opção. Posteriormente digite ping www.google.com

No teste do ping, vimos que a conectividade com a máquina do Google foi estabelecida com sucesso. Se sabemos que passamos por várias máquinas intermediárias, será que existe alguma forma de verificar qual é a rota que a informação está fazendo, saindo do meu computador passando pelas máquinas intermediárias até chegar a máquina do Google? Existe, esta é uma ferramenta administrativa chamada **Traceroute**. Dentro dela, assim como no ping, teremos um protocolo chamado ICMP, que fará essas verificações para saber quais são as máquinas intermediárias que participam do processo.

Para usá-la, no Windows nós digitaremos na linha de comando (no Linux considerar traceroute -n):

```
C:\Users\Alura>tracert -d www.google.com
```

Usamos o -d (-n no Linux) para que ele não faça a tradução DNS.

The screenshot shows a Windows Command Prompt window titled "Selecionar Prompt de Comando - tracert -d www.google.com". The command entered is "C:\Users\Alura>tracert -d www.google.com". The output displays the traceroute path to Google's IP address [216.58.202.36] through two routers:

Hop	Latency	IP Address
1	<1 ms	192.168.1.1
2	*	-

(1:21) - Observe que ocorreu a mesma tradução que foi feita no ping, por meio do servidor DNS que transformou o `www.google.com` para o endereçamento IP da máquina do Google. Mas as informações retornadas, foram diferentes.

```
C:\Users\Alura>tracert -d www.google.com
```

```
Rastreando a rota para www.google.com [216.58.202.36]
com no máximo 30 saltos:
```

```
1 <1 ms <1 ms 192.168.1.1
2 * *
```

Na primeira coluna, teremos o número de identificação da máquina por onde passou a informação da minha máquina. Ela foi a primeira a participar no processo de envio de dados. Mas a informação ainda passará por outras máquinas.

```
Selecionar Prompt de Comando - tracert -d www.google.com

C:\Users\Alura>tracert -d www.google.com

Rastreando a rota para www.google.com [216.58.202.36]
com no máximo 30 saltos:

1 <1 ms <1 ms 192.168.1.1
2 * * Esgotado o tempo limite do pedido.
3 2 ms 2 ms 5 ms 187.100.37.93
4 2 ms 2 ms 2 ms 187.100.196.86
5 2 ms 2 ms 2 ms 187.100.34.153
6
```

(02:33) - Mas observe os três intervalos de tempo que são mostrados nas outras colunas. Eles são os mesmos do ping e se referem ao processo de envio da minha máquina até o servidor do Google e de volta. Por que recebemos três informações?

(02:51) - Vamos pensar um exemplo do mundo real. Quando saímos do trabalho e vamos para a casa, temos a ideia de pegar uma rota específica. Mas pode ser que o caminho esteja congestionado e eu seja obrigado a buscar uma rota alternativa. Na rede, pode ocorrer o mesmo. Podemos enviar um pacote com informações, mas pode ser que no segundo seguinte, seja necessário buscar uma nova rota para chegar no site do Google. Para identificar se será necessário enviar uma rota diferente, três pacotes diferentes em intervalos diferentes são enviados para ver se alguma outra máquina poderia atuar como um ponto de parada.

(04:13) - Na primeira coluna, percebemos que quem recebeu os três pacotes foi o mesmo IP, ou seja, todos foram enviados pela mesma rota. Mas a máquina 2 não retornou nenhuma informação de tempo de retorno. Isso provavelmente aconteceu por dois motivos: o administrador pode ter desabilitado a resposta do ICMP da máquina, para evitar a sobrecarga de tráfego e por questões de segurança. Este teste que estamos realizando com a conectividade, pode ser um processo inicial de um teste de invasão de redes, que começa pela verificação de qual é o sistema que a empresa está trabalhando, quais as possíveis portas que estão abertas para conseguir o acesso. Para evitar esse tipo de problema de invasão, alguns provedores desabilita a resposta do ICMP. Mas ele está funcionando, tanto que ele passou a informação para a máquina número 3 que continuou passando para a próxima. Até chegar na décima máquina, que é o servidor do Google:

```
10 117 ms 117 ms 116 ms 216.58.202.36
```

Existiram várias passagens intermediárias da informação até finalmente chegarmos na máquina do Google.

A principal funcionalidade do **traceroute** é verificar a rota que a minha informação levou para chegar até a máquina de destino. Isso porque, em redes de computadores temos o que chamamos de **rede não determinística**, ou seja, não necessariamente um pacote de informação vai ser transferido pela mesma rota do anterior com o mesmo intervalo de tempo. Isto se deve a muitos fatores, por exemplo, uma máquina que pode estar congestionada ou um problema no link de comunicação, etc.

Pense como se a rede fosse uma cidade com várias ruas, nem sempre pegaremos a mesma rota para chegar até a nossa casa ou ir para o trabalho, depende de muitos fatores, por exemplo, trânsito, obras e outros aspectos. Nas redes de computadores não é tão diferente. :)

Quando nós temos uma máquina que retornou (*) e passou a informação para uma próxima máquina, isso provavelmente indica que o administrador dessa máquina desabilitou a resposta ao nosso chamado. O que acontece seria que esse tipo de teste pode ser interpretado como uma tentativa de “scavar” possíveis portas abertas e vulnerabilidades que possam existir, caso seja usado por um usuário malicioso, pode ser usada como uma forma de reconhecimento da rede dessa possível vítima para que assim possa explorar possíveis falhas.

Vamos agora verificar a rota de comunicação de nosso computador com a máquina do google, para isso digite:

- Caso seja Windows: `tracert www.google.com`
- Caso seja Ubuntu: `sudo apt-get install traceroute` (caso não tenha instalado), e depois `traceroute www.google.com`
- Caso seja Mac: `traceroute www.google.com`

Mãos à obra: Testando traceroute

Vamos agora verificar a rota de comunicação de nosso computador com a máquina do google, para isso digite:

- Caso seja Windows: `tracert www.google.com`
- Caso seja Ubuntu: `sudo apt-get install traceroute` (caso não tenha instalado), e depois `traceroute www.google.com`
- Caso seja Mac: `traceroute www.google.com`

O que vimos nessa aula

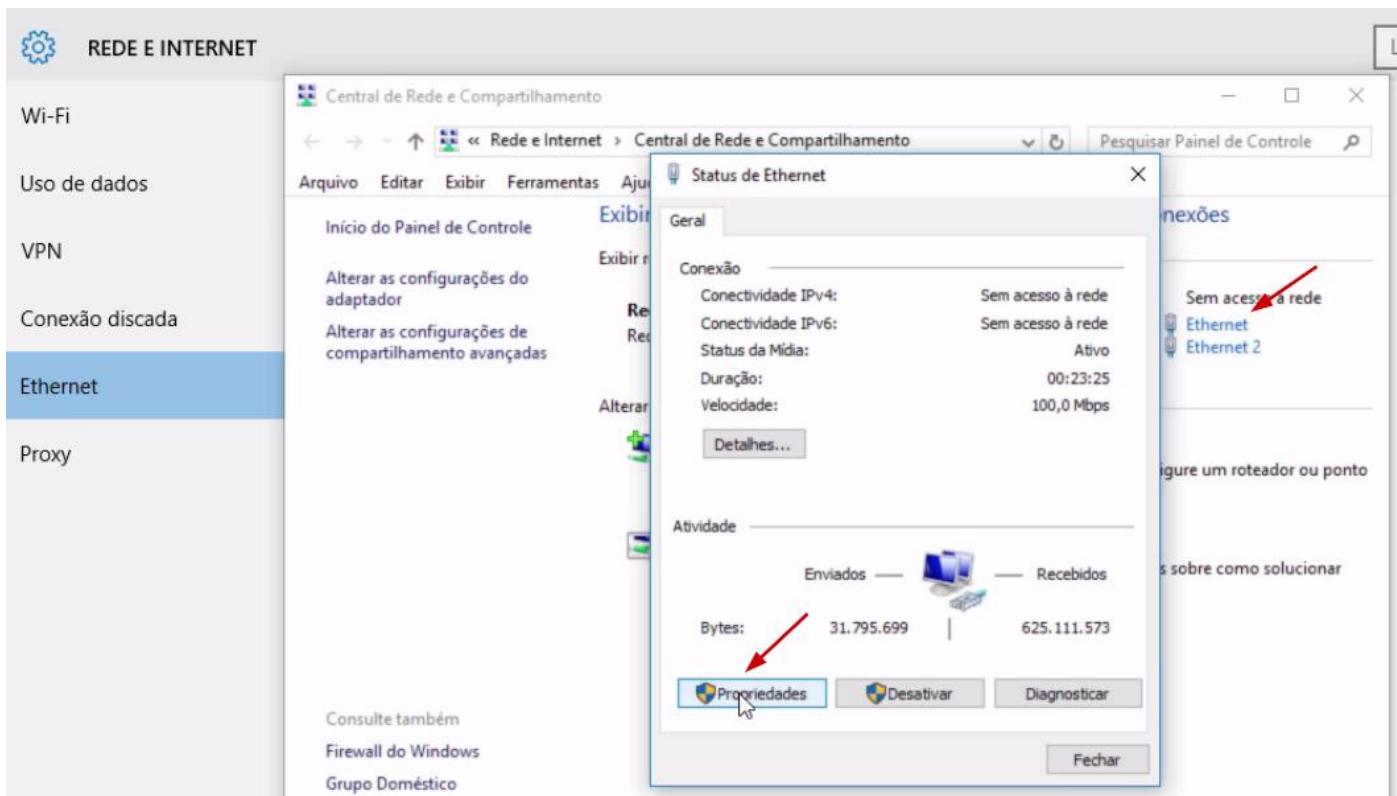
- O que é Rede de computadores.
- O comando ping para teste de conectividade.
- O protocolo ICMP utilizado
- O (Time to Live) TTL OU tempo de vida útil do pacote.
- O comando traceroute para verificar a rota que meu pacote está passando na rede.

Montando rede 2pc

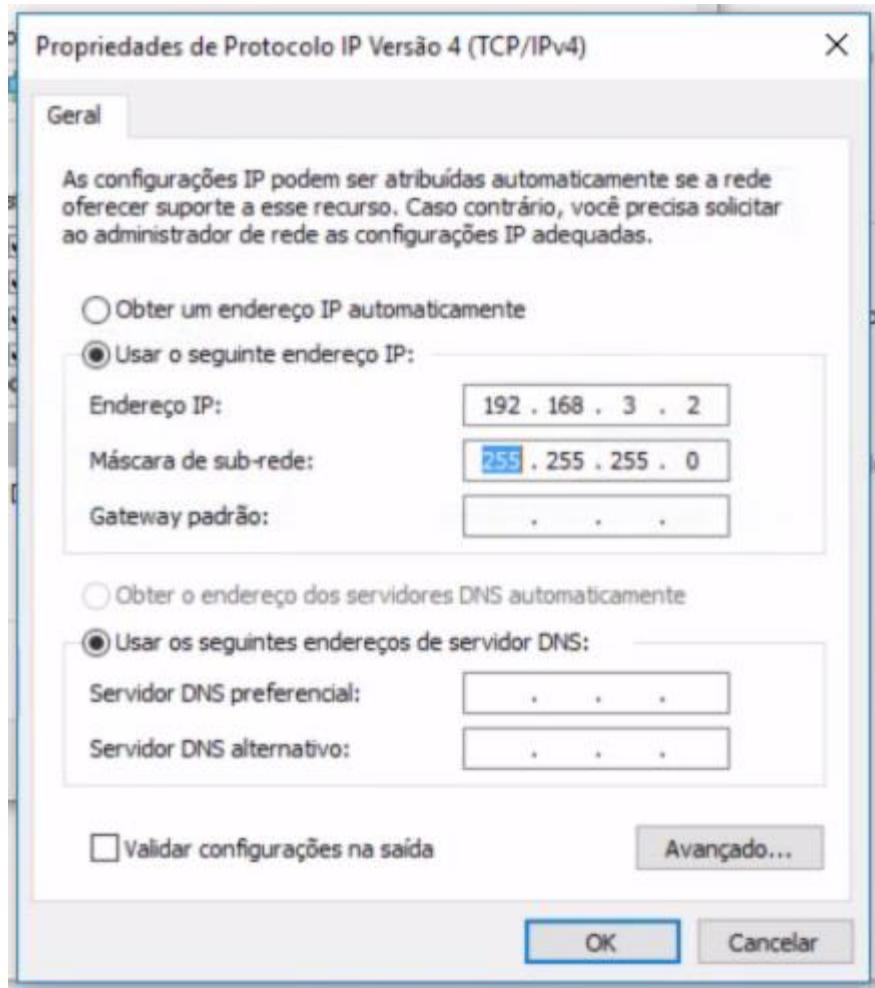
Falamos que existem diversos tamanhos de rede, agora, vamos começar com um projeto básico: uma rede que seria composta por dois computadores diretamente conectados. O computador usado na gravação do curso e um notebook conectado a ele por um cabo de rede azul será utilizado no curso. Comentamos que as máquinas na rede precisam de um endereço de identificação, chamado de IP. Mas nós sabemos que na rede, nós não podemos ter dois IPs iguais para máquinas diferentes. Cada computador precisa ter seu endereço de IP próprio - que não vem direto de fábrica. Existem duas formas de configurá-lo: uma máquina pode fornecer o endereço

IP ou precisamos configurar manualmente. Como não temos uma máquina que faça isso, faremos isso manualmente usando o Windows. Nas explicações você verá como fazer isso no Linux e no Mac.

Vamos até no ícone de conectividade, depois em "configurações de rede", "Ethernet". Em seguida, clicaremos em "Ethernet", ao ser aberta uma nova janela, selecionaremos "Propriedades".



Será aberta uma nova janela, buscaremos pela opção "Protocolo IP Versão 4(TCP/IPv4)", depois em "Propriedades". Na nova janela, selecionaremos "Usar o seguinte endereço IP" e escreveremos o IP que ele deverá usar para fazer o teste.



Para finalizar, clicaremos em "OK" e fecharemos as janelas.

Para um dos computadores eu configurei o IP com o final 2 e o outro com o final 1.

Vamos testar a conectividade entre os dois computadores. Abriremos o Prompt de comando do Windows (ou o Terminal no Linux e no Mac), e digitaremos o ping e o IP da máquina ao lado da que estou usando.

```
C:\Users\Alura>ping 192.168.3.1
```

E a comunicação será estabelecida.

```
C:\Users\Alura>ping 192.168.3.1
```

Disparando 192.168.3.1 com 32 bytes de dados:

Resposta de 192.168.3.1: bytes=32 tempo<1ms TTL=128

Estatísticas do Ping para 192.168.3.1:

Pacotes: Enviados = 4, Recebidos = 4, Perdidos = 0 (0% de perda),

Aproximar um número redondo de vezes em milissegundos:

Mínimo = 0ms, Máximo = 0ms, Média = 0ms

```
C:\Users\Alura>
```

Foi enviada uma informação com 32 bytes e o laptop respondeu uma informação com os mesmo 32 bytes. Nós já havíamos falado que o tempo é referente ao envio das informações até a outra máquina e de retorno. O TTL é o tempo de vida útil do pacote, no caso, ele poderia passar por 128 máquinas antes de ser extinguido.

Se começarmos a analisar as estatísticas do ping, veremos que enviamos e recebemos quatro pacotes. Isto significa que a comunicação entre os dois computadores foi estabelecida com sucesso.

E será que existe uma forma de testarmos a conectividade da minha própria placa de rede? Talvez ela tenha algum problema de fábrica. A resposta é sim. Existe um endereçamento IP reservado para a parte interna da placa de rede, para fazer este teste de conectividade.

Vamos fazer um teste, ele será um endereçamento reservado que começará pelo 127.

```
c:\Users\Alura>ping 127.0.0.1
```

Este tipo de endereçamento chamamos de **loopback**, em que ele enviará a informação para ele mesmo para verificar se está tudo funcionando nesta transmissão interna.

No nosso teste, veremos que ela está funcionando adequadamente.

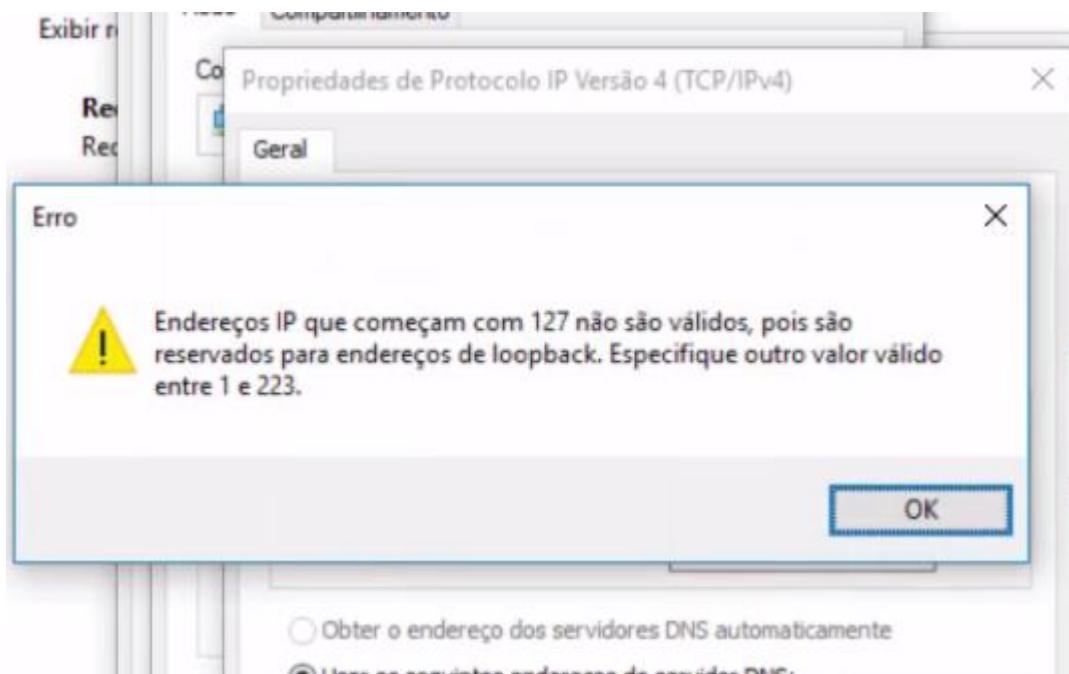
```
C:\Users\Alura>ping 127.0.0.1

Disparando 127.0.0.1 com 32 bytes de dados:
Resposta de 127.0.0.1: bytes=32 tempo<1ms TTL=128

Estatísticas do Ping para 127.0.0.1:
  Pacotes: Enviados = 4, Recebidos = 4, Perdidos = 0 (0% de
            perda),
Aproximar um número redondo de vezes em milissegundos:
  Mínimo = 0ms, Máximo = 0ms, Média = 0ms

C:\Users\Alura>
```

Mas como falei, o endereço é reservado e não podemos usá-lo para atribuir em outra placa de rede. Se retornarmos a configurações de rede, retornaremos a "Propriedade de Protocolo IP Versão 4 (TCP/IPv4)", onde acessamos anteriormente. Ao tentarmos modificar o IP para 127 receberemos uma mensagem de erro.



Ele nos informa que os endereços de IP que começam com 127 não são válidos, porque esta parte de número é reservada para testes de conectividade da placa de rede. Chegamos a um ponto importante aqui.

As traduções que estão sendo mostradas no terminal só possuem números. Vamos ver como é feita a tradução pelo servidor DNS, entre nome e endereçamento IP. Vamos fazer uma simulação no sistema operacional.

Abriremos o bloco de notas, com privilegio de administrador.

```
hosts - Bloco de notas
Arquivo Editar Formatar Exibir Ajuda
#
# This file contains the mappings of IP addresses to host names. Each
# entry should be kept on an individual line. The IP address should
# be placed in the first column followed by the corresponding host name.
# The IP address and the host name should be separated by at least one
# space.
#
# I
# Additionally, comments (such as these) may be inserted on individual
# lines or following the machine name denoted by a '#' symbol.
#
# For example:
#
#      102.54.94.97      rhino.acme.com      # source server
#      38.25.63.10      x.acme.com          # x client host

# localhost name resolution is handled within DNS itself.
#      127.0.0.1      localhost
#      ::1              localhost
```

Você pode conferir como realizar o processo no Linux e no Mac clicando aqui [aqui](#).

Vamos ver como fazer esta configuração. Percorremos o seguinte caminho: Clicaremos em "C:>" "Windows" > System32 > drivers > etc. Então, mudarem o tipo de arquivos para "Todos os arquivos". Selecionaremos com o botão direito o "hosts", depois vamos em "Abrir com", será aberto um arquivo.

```
hosts - Bloco de notas
Arquivo Editar Formatar Exibir Ajuda
#
# This file contains the mappings of IP addresses to host names. Each
# entry should be kept on an individual line. The IP address should
# be placed in the first column followed by the corresponding host name.
# The IP address and the host name should be separated by at least one
# space.
#
# Additionally, comments (such as these) may be inserted on individual
# lines or following the machine name denoted by a '#' symbol.
#
# For example:
#
#      102.54.94.97      rhino.acme.com      # source server
#      38.25.63.10      x.acme.com          # x client host

# localhost name resolution is handled within DNS itself.
#      127.0.0.1      localhost
#      ::1              localhost
```

Observe que ocorre um mapeamento no meu sistema, entre o nome `localhost` e o IP `127.0.0.1`. O `localhost` é o mesmo que usamos para programação Web. Vamos colocar outro nome para o endereçamento IP. Agora, tentaremos tentar encontrar o `www.cursoderedesdaalura.com`.

```
# localhost name resolution is handled within DNS itself.
#      127.0.0.1      localhost
#      ::1              localhost
#      127.0.0.1      www.cursoderedesdaalura.com
```

Queremos que o nome seja traduzido para o endereço IP. Faremos o teste adiante.

```
C:\Users\Alura>ping www.cursoderedesdaalura.com
```

```
C:\Users\Alura>ping www.cursoderedesdaalura.com

Disparando www.cursoderedesdaalura.com [127.0.0.1] com 32 bytes de dados:
Resposta de 127.0.0.1: bytes=32 tempo<1ms TTL=128

Estatísticas do Ping para 127.0.0.1:
  Pacotes: Enviados = 4, Recebidos = 4, Perdidos = 0 (0% de perda),
Aproximar um número redondo de vezes em milissegundos:
  Mínimo = 0ms, Máximo = 0ms, Média = 0ms

C:\Users\Alura>
```

É esse processo de mapeamento que o DNS faz. Teremos as mesmas informações que tivemos nos testes anteriores, em que verificaremos que a conectividade foi estabelecida, obtivemos resposta, e temos quatro pacotes enviados e recebidos. Está tudo funcionando.

Os servidores DNS são chamados de Domain Name Servers e sua função é realizar o “mapeamento” entre endereço IP e url (ex: www.google.com). Dessa forma, se estamos digitando www.google.com no browser, o servidor DNS está fazendo a tradução entre o nome da url e o endereço IP.

Quando inserimos um IP em uma máquina, ela passa a atuar com aquele endereço IP, esse tipo de inserção manual de endereço IP é chamado de IP estático, pois fixamos que ele tenha o valor que inserimos.

Mãos à obra: DNS hosts

Vamos fazer agora a tradução do endereço IP de loopback para a url www.cursoderedesdaalura.com:

- Caso seja Windows: Abrir bloco de notas como administrador e abrir o arquivo hosts localizado em C:\Windows\System32\drivers\etc e insira na última linha o mapeamento 127.0.0.1 www.cursoderedesdaalura.com e teste o ping para essa url
- Caso seja Mac: Abrir o terminal e digitar: sudo vi /private/etc/hosts e posteriormente ir com a seta para baixo até ir numa linha em branco e realizar o mapeamento 127.0.0.1 www.cursoderedesdaalura.com pressione x, caso ele pergunte se deseja salvar diga que sim. Posteriormente teste o ping para essa url
- Caso seja Linux: Abrir o terminal e digitar: sudo vim /etc/hosts e posteriormente ir com a seta para baixo até ir numa linha em branco e realizar o mapeamento 127.0.0.1 www.cursoderedesdaalura.com pressione :wq para salvar e sair. Posteriormente teste o ping para essa url

Ao fazer o teste do ping www.cursoderedesdaalura.com, devemos ver a tradução para o endereço IP 127.0.0.1 e que a conectividade foi estabelecida com sucesso :)

Nslookup

Vamos voltar a fazer o teste do ping para o domínio do curso de redes da Alura.

```
C:\Users\Alura>ping www.cursoderedesdaalura.com
```

```
C:\Users\Alura>ping www.cursoderedesdaalura.com
```

```
Disparando www.cursoderedesdaalura.com [127.0.0.1] com 32 bytes de dados:  
Resposta de 127.0.0.1: bytes=32 tempo<1ms TTL=128  
Resposta de 127.0.0.1: bytes=32 tempo<1ms TTL=128  
Resposta de 127.0.0.1: bytes=32 tempo<1ms TTL=128  
Resposta de 127.0.0.1: bytes=32 tempo<1ms TTL=128
```

Estatísticas do Ping para 127.0.0.1:

```
Pacotes: Enviados = 4, Recebidos = 4, Perdidos = 0 (0% de perda),
```

Aproximar um número redondo de vezes em milissegundos:

```
Mínimo = 0ms, Máximo = 0ms, Média = 0ms
```

```
C:\Users\Alura>
```

Nesta tradução entrará o nome `www.cursoderedesdaalura.com` para o endereço IP, em algum momento podemos ter problemas em cada um deles no processo de tradução. Para identificarmos em qual parte está o problema, usaremos uma ferramenta administrativa chamada **nslookup** e o nome do endereçamento IP que queremos descobrir. Veremos o exemplo, um teste com o site do Facebook.

```
C:\Users\Alura>nslookup www.facebook.com
```

```
C:\Users\Alura>nslookup www.facebook.com
```

```
Servidor: openrg.home
```

```
Address: 192.168.1.1
```

Não é resposta autoritativa:

```
Nome: star-mini.c10r.facebook.com
```

```
Addresses: 2a03:2880:f100:83:face:b00c:0:25de  
           31.13.73.36
```

```
Aliases: www.facebook.com
```

```
C:\Users\Alura>_
```

No retorno veremos que os dois tipos de máquinas com identificação:

```
C:\Users\Alura>nslookup www.facebook.com
Servidor:  openrg.home
Address:  192.168.1.1

Não é resposta autoritativa:
Nome:      star-mini.c10r.facebook.com
Addresses:  2a03:2880:f100:83:face:b00c:0:25de
            31.13.73.36
Aliases:   www.facebook.com
```

Vemos o primeiro com um formato maior e o segundo com um formato em que estamos mais acostumados.

Ele também nos diz que o endereçamento da máquina IP não é uma resposta autoritativa. Isto acontece porque na minha rede local, já acessamos previamente o site do Facebook e ficou armazenado no cache qual é o respectivo endereçamento da plataforma. O processo ficaria muito lento se tivéssemos que fazer a verificação na internet toda vez, por isso, a minha máquina local guarda na memória qual é o respectivo endereçamento do IP do Facebook. A resposta não é **autoritativa** porque ela não veio de quem realmente tem a propriedade de passar o registro. A resposta veio internamente da minha rede.

Teoricamente, nós poderíamos colocar no teste do ping qualquer nome. O que acontecerá, por exemplo se digitarmos no Terminal nslookup x?

```
C:\Users\Alura>nslookup x
```

```
C:\Users\Alura>nslookup x
Servidor:  openrg.home
Address:  192.168.1.1

*** openrg.home não encontrou x: Non-existent domain

C:\Users\Alura>
```

Ele respondeu que não existe esse domínio, ou seja, não existe o registro nem na minha rede e nem na internet sobre um possível domínio que receba o nome x. O mesmo ocorrerá se fizermos um teste de conectividade com o ping.

```
C:\Users\Alura>ping 1.1.1.1
```

```
C:\Users\Alura>ping 1.1.1.1

Disparando 1.1.1.1 com 32 bytes de dados:
Esgotado o tempo limite do pedido.
```

Veja que foi esgotado o tempo limite do pedido. Nós fizemos uma chamada para o endereçamento 1.1.1.1, mas não recebemos uma resposta.

O Nslookup pode ser usado para descobrirmos o endereço IP de um domínio, bem como saber detalhes mais avançados de DNS, para saber se nosso serviço está sendo direcionado para a máquina de destino, por exemplo.

Uma vez que eu já accesei o site antes, essa máquina guarda em sua memória, para não ter que ficar fazendo essas requisições na internet o tempo todo. Dessa forma, a minha máquina que respondeu não tem autoridade sobre esse domínio, não é minha máquina que possui o registro do www.google.com.

Mãos à obra: NSlookup

Vamos agora verificar o nslookup do google . Para isso:

- Caso seja Windows: Abrir prompt de comando e digitar: nslookup www.google.com
- Caso seja Linux ou Mac: Abrir o terminal e digitar: nslookup www.google.com

Montando rede 3pc

Temos falado sobre placas de rede, vamos visualizá-las para nos familiarizarmos com elas.

Vemos que temos uma entrada em que será conectado o cabinho azul que conhecemos. Mais abaixo, teremos outra imagem, desta vez com o cabo:

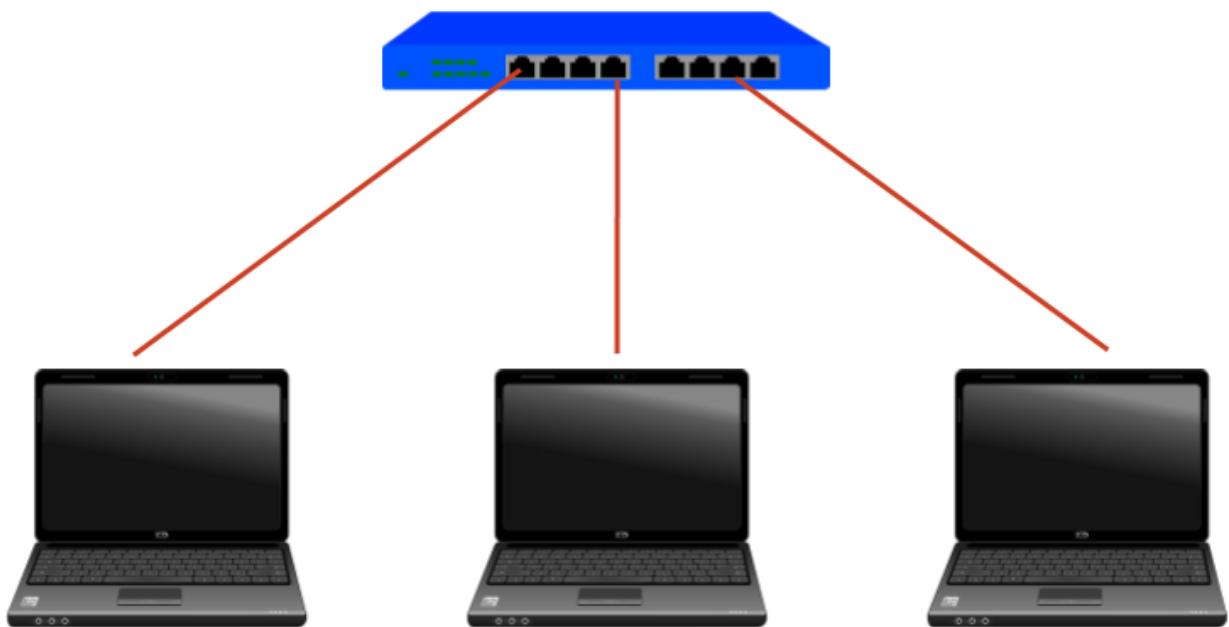


Eu conectei a placa de rede do computador que estou usando no curso com o laptop utilizando o cabo azul. Vamos relembrar como fizemos a interconexão do nosso projeto.

Nós conectamos os dois computadores com o cabo de rede.



Mas e se precisássemos conectar um terceiro computador. A placa de rede dos dois primeiros computadores já está ocupada. Não temos mais espaço disponível para conectarmos o terceiro. Para podermos conectar diversos computadores, foram criados dispositivos que podem fazer essa conexão, um deles recebe o nome de **hub**.



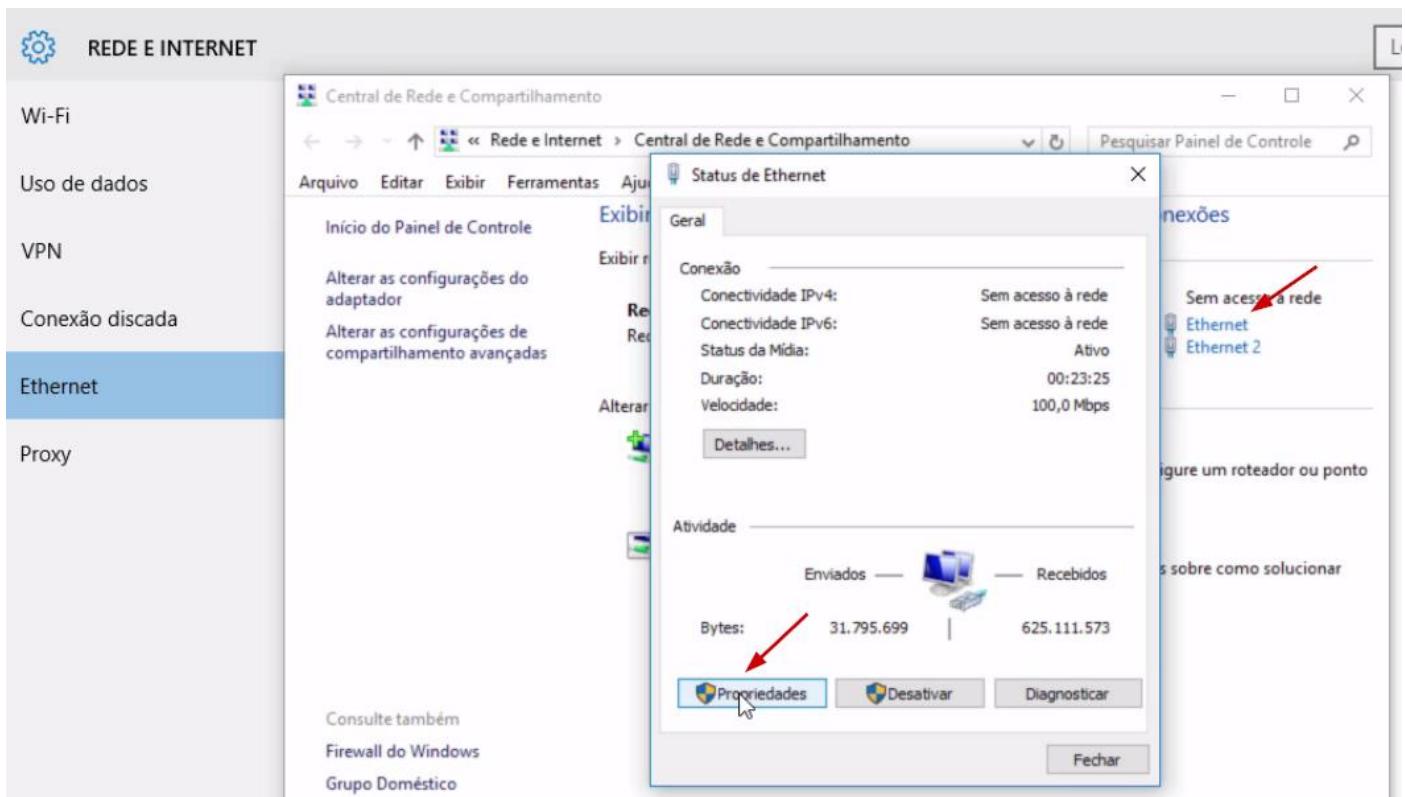
Podemos encontrar outras imagens de hubs na internet.



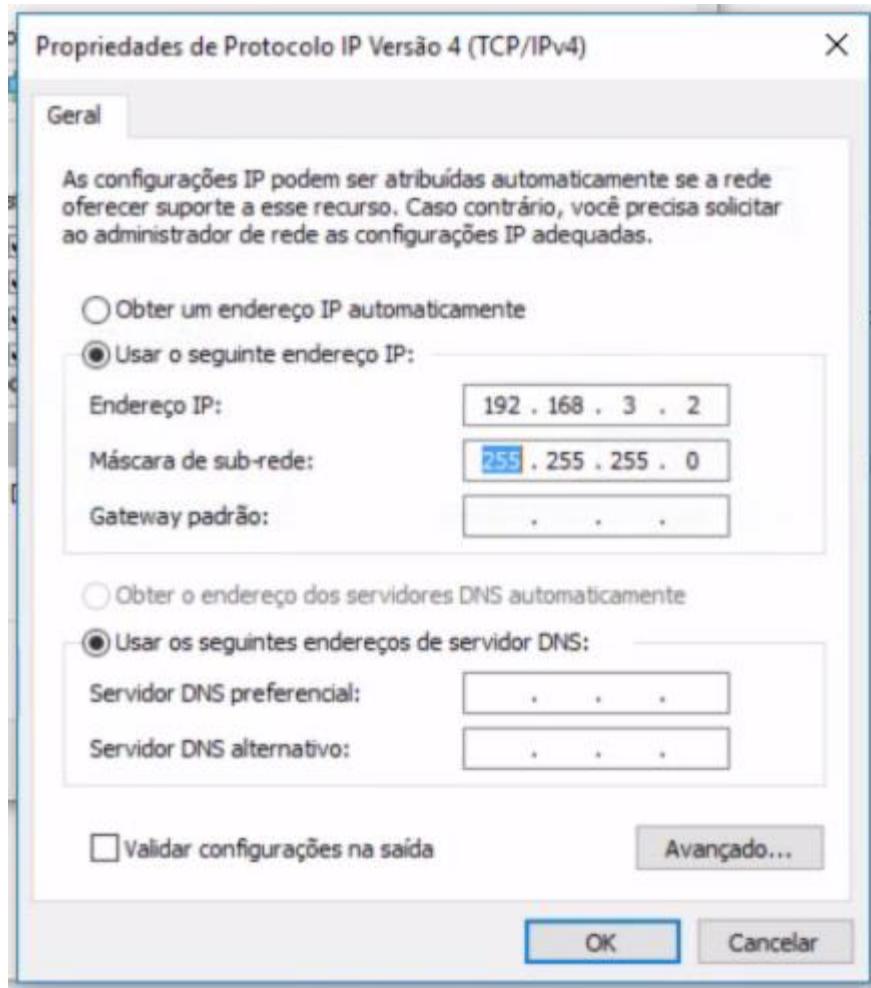
Então, estamos na etapa de interconectar computadores. Além dos dois que nos já conectamos no curso, vamos nos conectar em um terceiro.

Relembaremos como fazímos para colocar os endereços IPs nas máquinas.

Vamos até no ícone de conectividade, depois em "configurações de rede", "Ethernet". Em seguida, clicaremos em "Ethernet", ao ser aberta uma nova janela, selecionaremos "Propriedades".



Será aberta uma nova janela, buscaremos pela opção "Protocolo IP Versão 4(TCP/IPv4)", depois em "Propriedades". Na nova janela, selecionaremos "Usar o seguinte endereço IP" e escreveremos o IP que ele deverá usar para fazer o teste.



Nós já configuramos com o endereço 192.168.3.2. Lembrando que não podemos ter o mesmo endereçamento IPs para máquinas diferentes. Nesta máquina, meu IP termina com 2 e a terceira máquina terminará com 3.

Faremos um teste de conectividade entre as máquinas com o IP de final 1 e 2. No terminal, digitaremos:

```
c:\Users\Alura>ping 192.168.3.1
```

Vamos ver o que acontece:

```
C:\Users\Alura>ping 192.168.3.1
```

Disparando 192.168.3.1 com 32 bytes de dados:

Resposta de 192.168.3.1: bytes=32 tempo<1ms TTL=128

Estatísticas do Ping para 192.168.3.1:

Pacotes: Enviados = 4, Recebidos = 4, Perdidos = 0 (0% de perda),

Aproximar um número redondo de vezes em milissegundos:

Mínimo = 0ms, Máximo = 0ms, Média = 0ms

```
C:\Users\Alura>p
```

Veremos se o computador com o IP 192.168.3.3 também está ativo.

```
C:\Users\Alura>ping 192.168.3.3
```

Disparando 192.168.3.3 com 32 bytes de dados:

Resposta de 192.168.3.3: bytes=32 tempo<1ms TTL=128

Estatísticas do Ping para 192.168.3.3:

Pacotes: Enviados = 4, Recebidos = 4, Perdidos = 0 (0% de perda),

Aproximar um número redondo de vezes em milissegundos:

Mínimo = 0ms, Máximo = 0ms, Média = 0ms

```
C:\Users\Alura>
```

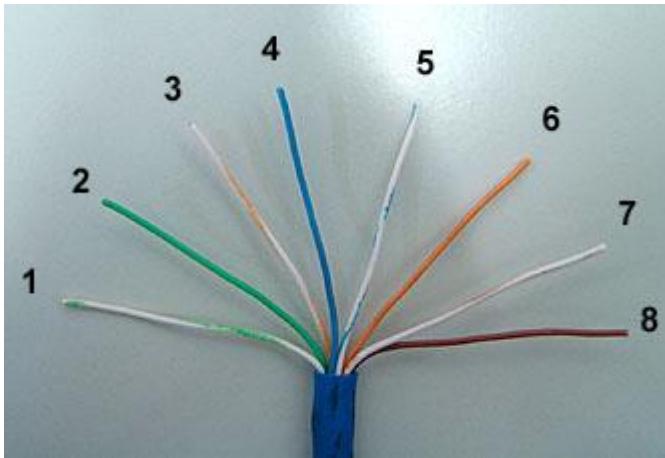
Nós conseguimos nos conectar tanto com o primeiro e como com o terceiro computador. O hub permite comunicar com os três computadores, seu papel foi desempenhado com sucesso.

O ping possui dentro dele um protocolo chamado ICMP, ele vai mandar uma requisição (Echo request) e aguarda uma resposta (Echo reply).

- O Hub é um equipamento utilizado para interconectar diversos dispositivos finais.
- NAT é um método de tradução de endereços privados e públicos.
- Servidor é uma máquina centralizada que oferece serviços a um cliente (ex: computador)
- Máscara de rede é usado para determinar se dois equipamentos estão na mesma rede

Tipos de cabo

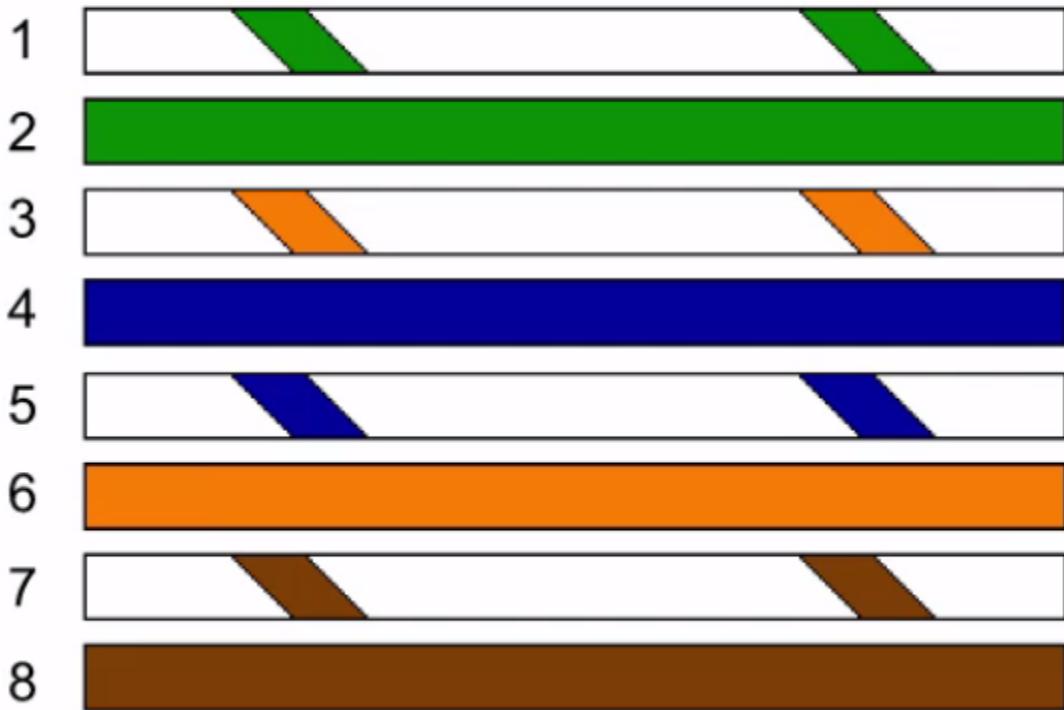
Vamos analisar os cabos que estão conectando os dois computadores diretamente e o que foi usado para conectar os três computadores com o hub. Quando compramos o cabo, ele vem do fabricante com alguns fios soltos:



Os fios soltos, são aqueles que estão internamente no cabo e depois, serão inserido no conector plástico chamado RJ45. Este processo de colocar os fios no conector plástico, chamamos de crimpas.

Em seguida, vamos analisar as cores do fios internos que temos. Nós temos as seguintes cores de cabos: verde e branco; verde; branco e laranja; azul; branco e azul; laranja; branco e marrom; e marrom.

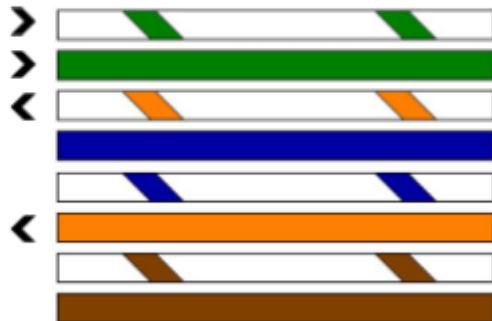
T568A



Existe um padrão para essas cores serem seguidas: o **T568A**, desenvolvido pela associação internacional de Telecomunicações (Telecommunication industry association - TIA). Eles definiram o padrão de cores que deveria ser seguido. Sabendo disso, faremos a análise do nosso último projeto em que conectamos os computadores com o hub.

T568A

CABO DIRETO



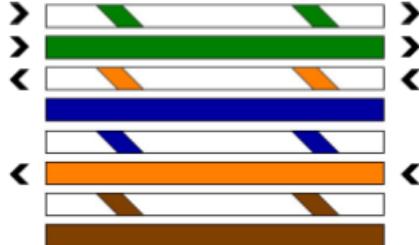
A placa de rede do computador transmite na posição 1 e 2, e recebe na posição 3 e 6.

O hub receberá nas posições contrárias: receberá nas posições 1 e 2, e transmitirá nas posições 3 e 6.

T568A

CABO DIRETO

T568A



O computador da esquerda está transmitindo o sinal na posição 1 e 2 e recebendo na posição 3 e 6. Já o hub recebe na posição 1 e 2 e transmite o sinal nas posições 3 e 6.

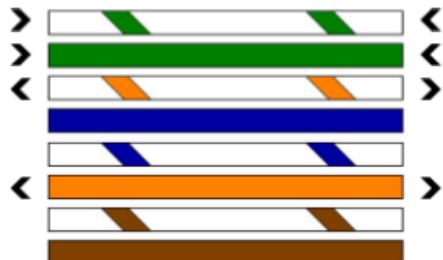
Os dois estão conseguindo transmitir e receber informações. Quando seguimos a mesma sequência de cores de ambos os lados, dizemos que este é um **cabo direto**. O cabo está na mesma posição no computador e no hub. Vamos usar o cabo direto para comunicarmos dois computadores.

Mas o segundo computador, por possuir a mesma placa de rede, transmitirá o sinal na posição 1 e 2, e receberá na posição 3 e 6.

T568A

CABO DIRETO

T568A



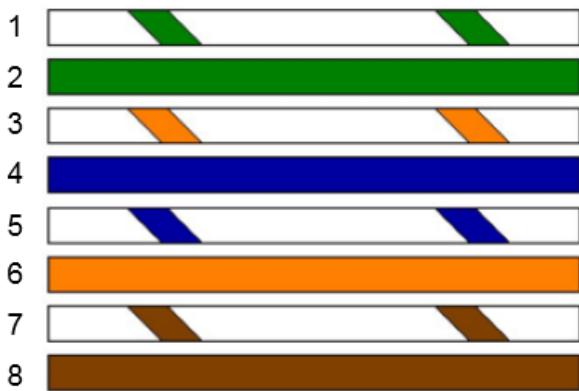
Se as informações dos computadores estão sendo transmitidas nas mesmas posições, por exemplo, pelo fio branco e verde, o que acontecerá?



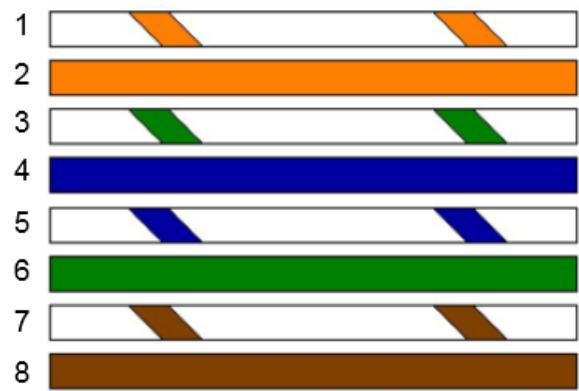
Acontecerá uma colisão! Os dois computadores estão transmitindo sinal na mesma posição. Precisaremos encontrar uma forma para que este problema não ocorra.

Pensando nisto, a TIA criou o padrão chamado **T568B**.

T568A



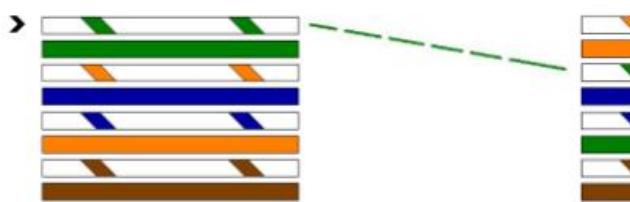
T568B



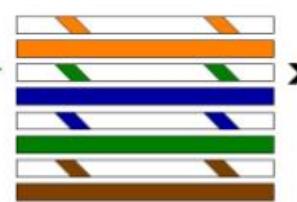
A diferença para o novo padrão é que os cabos terão uma sequência de cores diferentes nas duas pontas, desta forma o problema de transmissão e recebimento do sinal é corrigido. O computador da esquerda estará com a T568A, enquanto o da direita estará com a T568B.

Agora o sinal transmitido na posição 1 pelo computador da esquerda será recebido pela posição 3 da direita.

T568A

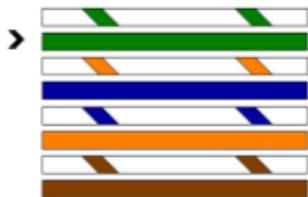


T568B

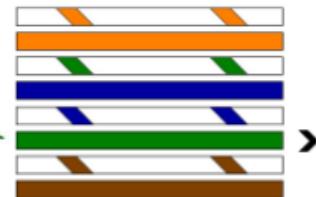


Já o sinal transmitido na posição 2 será recebido na posição 6 na placa da outra máquina.

T568A



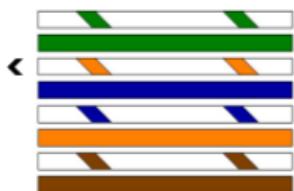
T568B



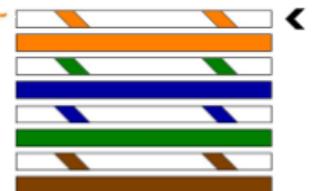
Agora, veremos como será a comunicação do computador da direita com o da esquerda.

O sinal será enviado pelo fio branco e laranja da posição 1 e será recebido pelo fio da posição 3.

T568A

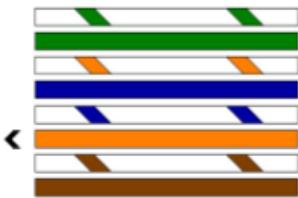


T568B

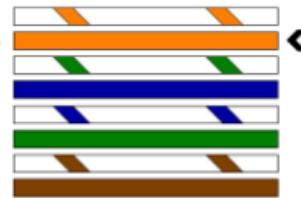


Foi atendida a primeira condição de transmissão. Vamos ver como será feita a transmissão do sinal na posição 2.

T568A



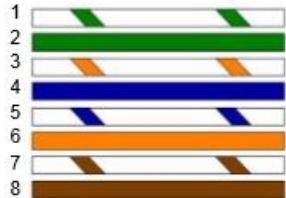
T568B



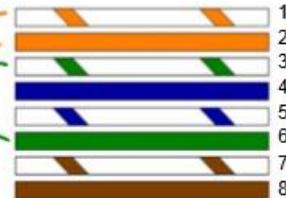
E o sinal é recebido na posição 6 do computador da esquerda.

Perceba que ocorreu um cruzamento interno dos sinais de uma forma que eles não colidam. Por causa do cruzamento, ele recebeu o nome de **cabo cruzado**, ou **crossover**.

T568A



T568B

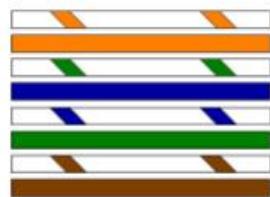
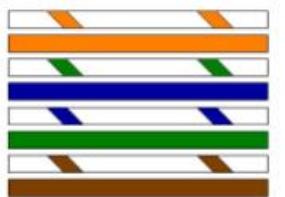


CABO CRUZADO (CROSSOVER)

Em uma das pontas teremos o T568A e em outra, o T568B.

Vimos que se for comunicar dois equipamentos iguais, que possuem a mesma placa de rede, os dois transmitirão o sinal no fio com a mesma posição. Se conectarmos as pontas com T568A em ambas pontas, teremos problemas nas transmissões. O mesmo ocorreria se colocássemos o T568B nas duas pontas.

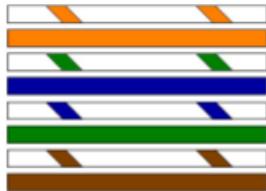
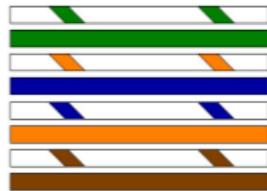
- **T568B + T568B = Cabo direto**



Nós entraríamos em rota de colisão novamente.

Mas a conexão poderá ser feita corretamente se em um dos lados tivermos T568A e em outro o T568B, porque assim será feita a correção de qual fio irá transmitir e qual fio irá receber.

- **T568A + T568B = Cabo cruzado**



Às vezes ocorrem confusões sobre o tipo de cabo que deve ser usado, se deve ser o direto ou o cruzado. As placas de rede mais modernas conseguem perceber a diferença e fazem a correção automaticamente via software. Mas nem todas placas de rede possuem essa configuração. É melhor saber qual tipo de cabo precisamos usar.

Caso tenhamos o mesmo padrão de cores na duas pontas do cabo, chamamos de cabo direto, pois as mesmas cores estão nas mesmas posições nas duas pontas.

Caso tenhamos um padrão de cores diferente em cada ponta do cabo, teremos o que chamamos de cabo cruzado.

Quando temos um padrão de cores diferente em cada ponta do cabo, teremos o que chamamos de cabo cruzado.

Quando temos um padrão de cores iguais nas duas pontas do cabo, teremos o que chamamos de cabo direto

O padrão de cores feitos pela TIA seria T568A e T568B, sendo que a T568A possui a sequência de cores, nesta ordem:

- Branco e verde, verde, branco e laranja, azul, branco e azul, laranja, branco e marrom, marrom

E a T568B:

- Branco e laranja, laranja, branco e verde, azul, branco e azul, verde, branco e marrom, marrom

Pelo fato de termos dois computadores, eles tem o mesmo tipo de placa de rede e vão transmitir os sinais nas mesmas posições. Dessa forma é necessário realizar essa compatibilidade entre os sinais de transmissão e recepção e isso é obtido através do cabo cruzado.

As placas de rede dos computadores transmitem, por padrão, nas posições 1 e 2.

As placas de rede dos computadores recebem por padrão nas posições 3 e 6.

As placas de rede dos hubs transmitem por padrão nas posições 3 e 6

As placas de rede dos hubs recebem por padrão nas posições 1 e 2.

Algumas placas de rede mais modernas possuem o padrão auto-MDIX, dessa forma, se as duas placas de rede estiverem configuradas, elas poderão corrigir essa questão da polaridade e se comunicarem

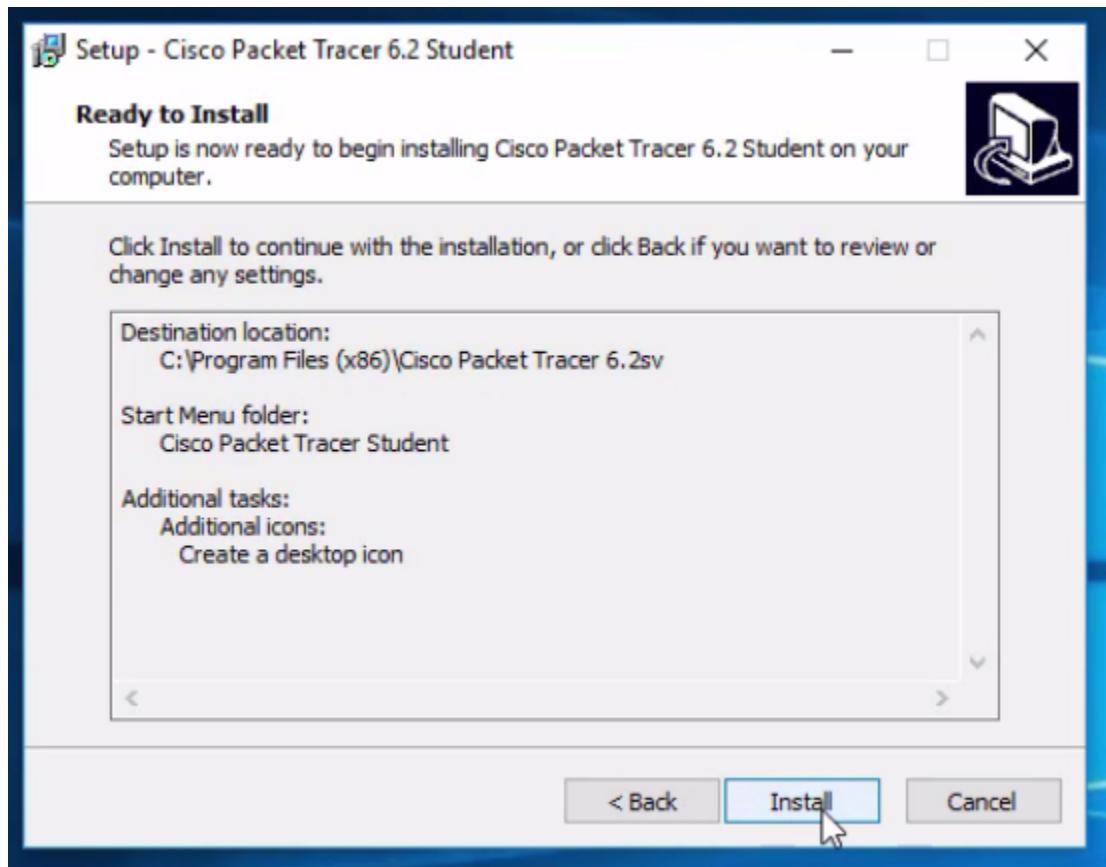
Instalando Packet Tracer

A nossa rede está crescendo e já interconectamos três computadores, imagine quando fizermos o mesmo com cinco máquinas. Ficará muito confuso... A partir de agora, para ficar mais fácil para trabalharmos com estas redes, usaremos um software para simularmos o comportamento das redes. Ele foi criado pela Cisco, um dos fabricantes de elementos de redes.

Vamos abrir o guia de instalação do Packet Tracer.

Você encontrará instruções de como instalar o Packet Tracer clicando [aqui](#). A demonstração de como instalar em Mac será feita no [próximo vídeo](#).

Inicialmente, clicaremos em "Next" para os primeiros passos da instalação, até chegarmos na tela "REady to Install", em que clicaremos no botão "Install".



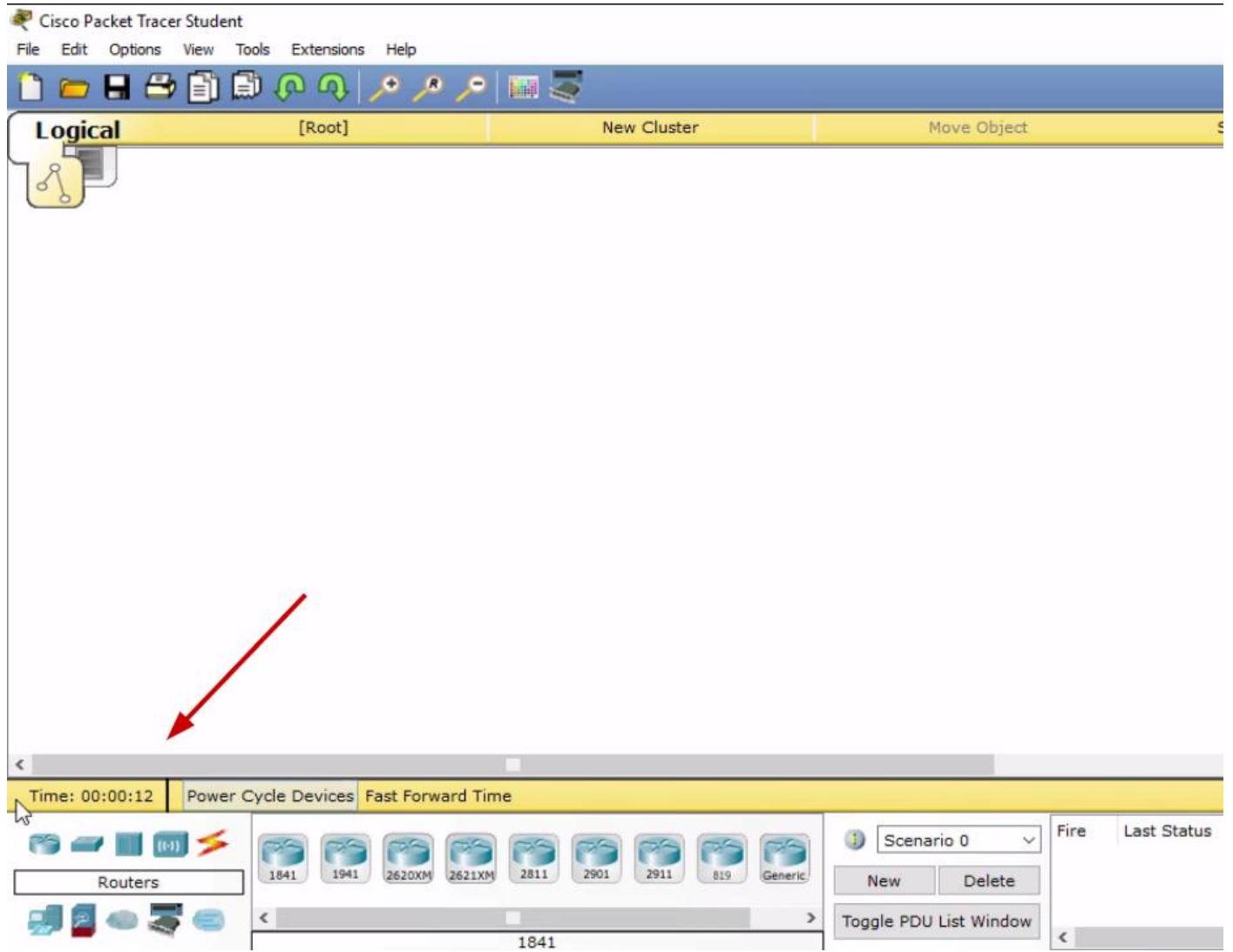
Depois, esperaremos pelo fim do processo de instalação. Será aberta uma janela perguntando se queremos inicializar o Packet Tracer, depois, O processo será finalizado ao clicarmos em "Finish". Então, o programa será inicializado.

Cisco Packet Tracer Student



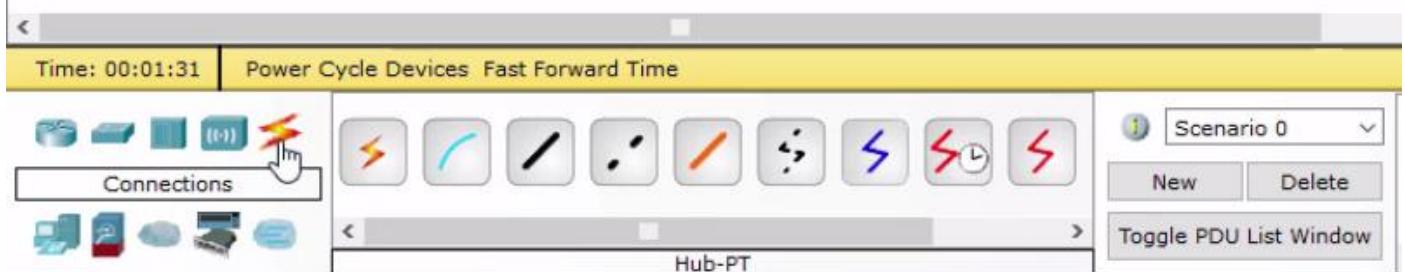
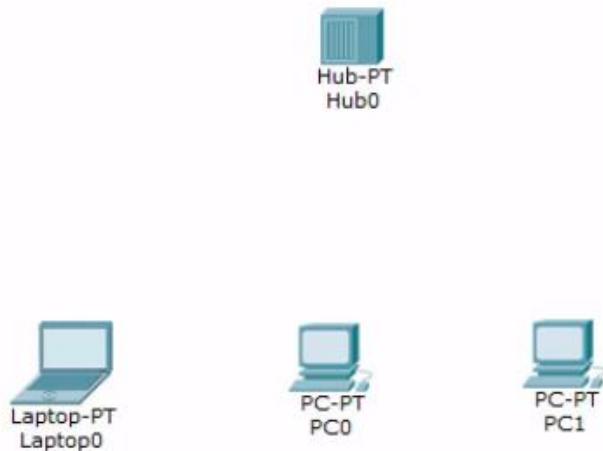
© Copyright Cisco 2015

Todas as configurações do equipamentos que utilizaremos, será selecionado na parte do canto inferior da esquerda.

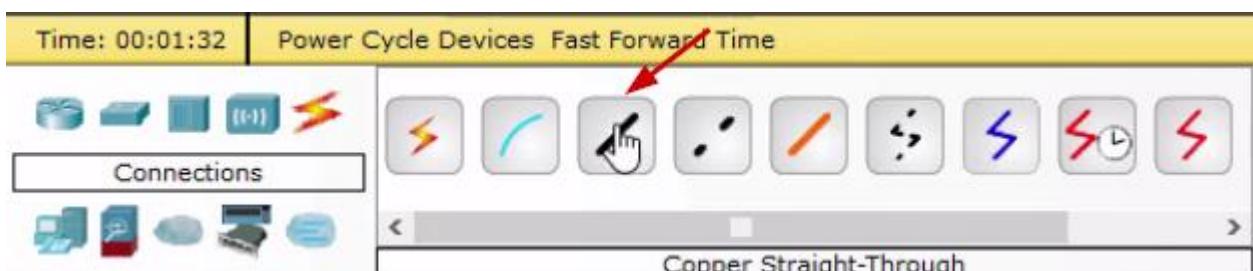


Vamos montar o projeto da última rede feita por nós. Começaremos, clicando nos "End Device" que são os dispositivos finais usados efetivamente pelos usuários.

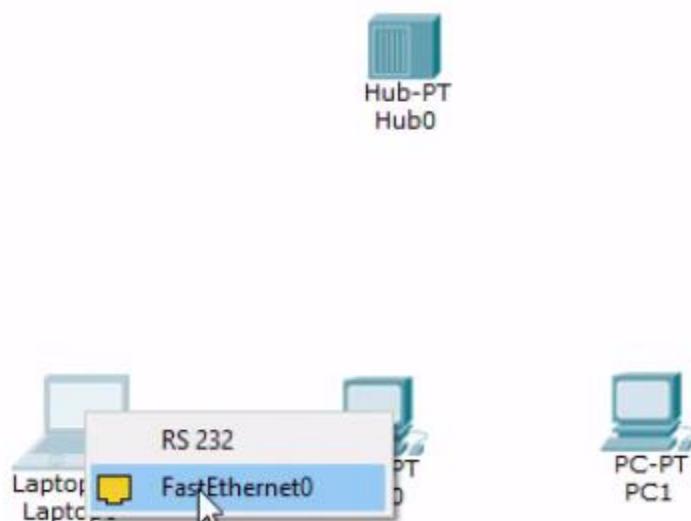
Vamos criar uma situação em que usamos três computadores e o hub.



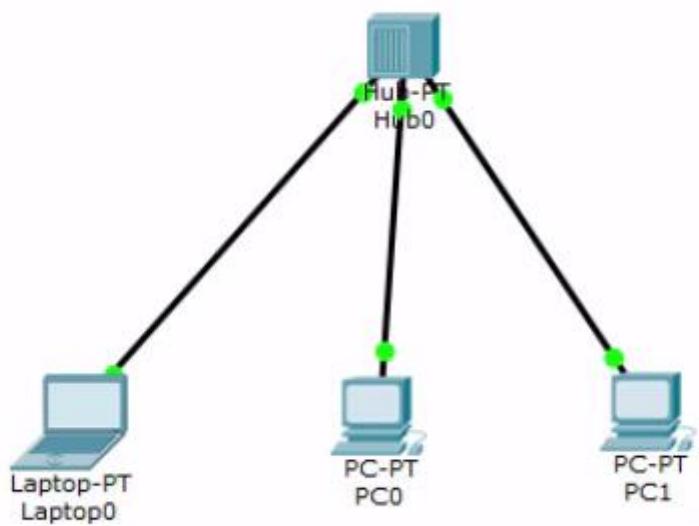
Para interconectá-los precisaremos de um cabo direto. Seleccionaremos a terceira opção.



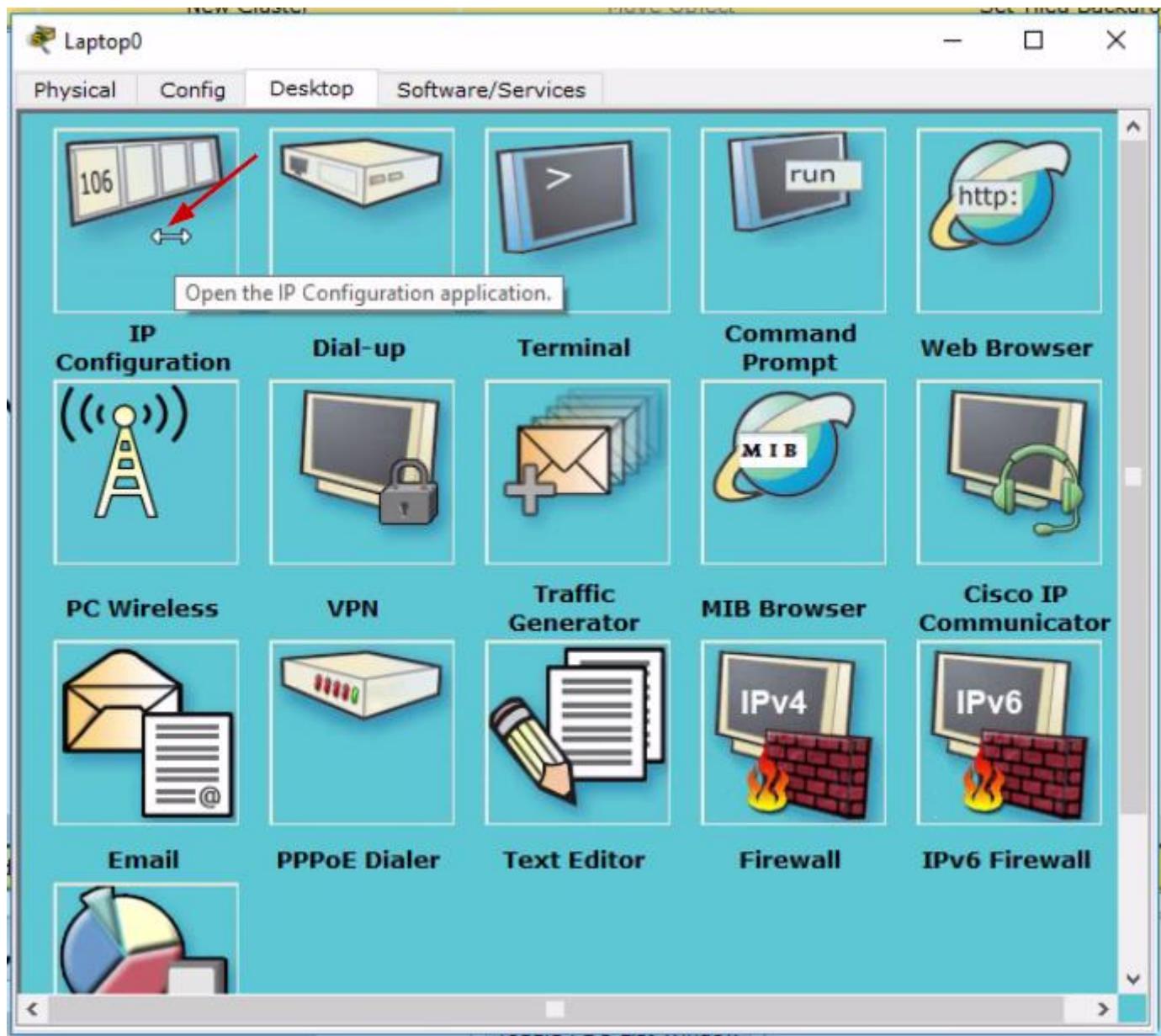
Depois, clicaremos no primeiro laptop com o botão direito e selecionaremos "FastEthernet()".



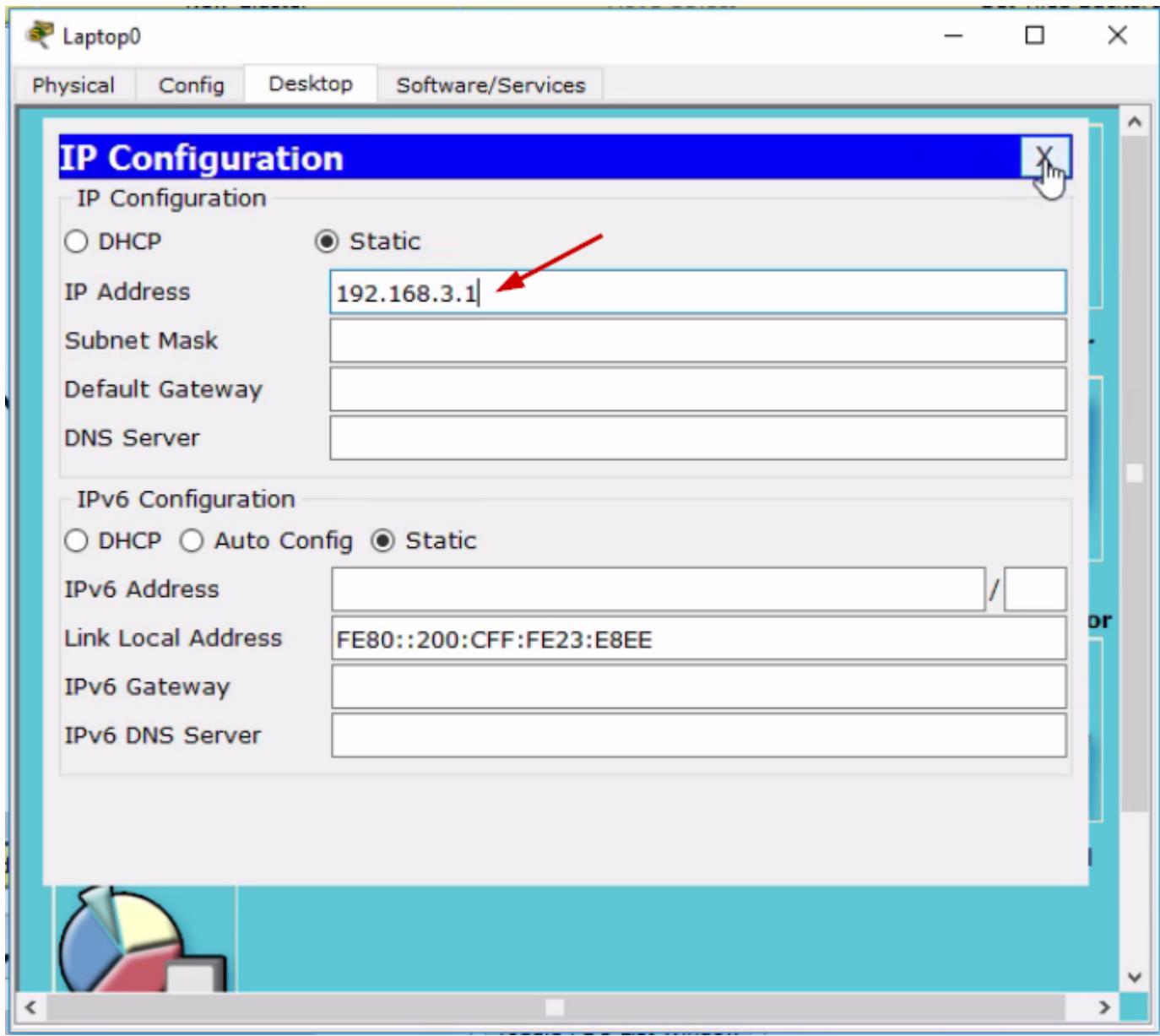
Vamos arrastar até o hub e selecionaremos um porta livre. Repetiremos o mesmo processo com as outras duas máquinas.



Já conseguimos fazer a instalação do Packet que iremos utilizar e criamos o projeto feito por nós. Mas está faltando uma parte importante, falamos que é preciso configurar um endereço de IP. Nós precisaremos criá-los manualmente. Faremos isto clicando sobre o Laptop do projeto, será aberta uma nova janela em que selecionaremos a aba "Desktop" e depois, em "IP Configuration".



Vamos preenche-lo com o mesmo IP que usamos no computador do curso.



Faremos o mesmo com as máquinas do projeto, com a diferença que mudaremos o fim dos números dos IPs, que terminaram em 2 e 3. Isto significa que o segundo terá o IP 192.168.3.2 e o terceiro 192.168.3.3.

Agora o projeto montado no estúdio está representado no Packet Tracer. Em seguida faremos alguns testes.

Mãos à obra: Instalando o packet tracer

Etapas para o download do Packet Tracer:

- 1) Acesse o link: <https://www.netacad.com/courses/packet-tracer/introduction-packet-tracer> e escolha a opção **Sign up today!** do *Hands-On Practice*

Hands-On Practice

Enroll, download and start learning valuable tips and best practices for using our innovative, virtual simulation tool, Cisco Packet Tracer. This self-paced course is designed for beginners with no prior networking knowledge. It teaches basic operations of the tool with multiple hands-on activities helping you to visualize a network using everyday examples, including Internet of Things (IoT). This Introductory course is extremely helpful for anyone who plans to take one of the Networking Academy courses which utilizes the powerful simulation tool. No prerequisites required!

You'll Learn These Core Skills:

- Simulate data interactions traveling through a network.
- Visualize the network in both logical and physical modes.
- Apply skills through practice, using labs and Cisco Packet Tracer activities.
- Develop critical thinking and problem-solving skills.



Length: 10 hours



Cost: Free*



Level: Beginning



Learning Type: Online self-paced



Achievements: Badge



Languages: English, Український

*Self-paced classes at NetAcad.com are free. Cost for Instructor-led classes is determined by the institution.

Sign up today!

2) Na janela que irá abrir, em *Enroll now*, coloque seus dados (país, mês e ano de nascimento)

Introduction to Packet Tracer English 1121a

Cisco Virtual Academy

-acm-

08 Nov 2021 - 28 Feb 2022

Jackson Smith

Enroll now

Your country or region of residence *

Brazil

Your Birthday *

Month *

Year *

Next Account Details

3) Em seguida, preencha com um e-mail válido, primeiro e último nome, país, estado e o resultado de uma operação matemática.

Enroll now

Account Email *

First Name *

Last Name *

Country or region *

State *

To prove you're a human, solve this simple math problem and enter the result.

Answer *

1 + 5 =

I would like to receive email communications about courses and learning offerings from Cisco and its Affiliates. I understand I can unsubscribe at any time.

By clicking Create Account, you agree to our [Terms and Conditions](#) and that you have read our [Privacy Statement](#), including our [Cookie Notice](#).

[Back](#)

[Create Account](#)

4) Entre no seu e-mail e confirme que seu e-mail é válido clicando em **Activate account**

Hello [REDACTED]

Welcome to Cisco Networking Academy!

To activate your account, please click the button below:

[Activate account](#)



5) Na nova janela que irá abrir, escolha uma senha de acesso

Bem-vindo(a) à Cisco Identity, !

Crie sua conta Cisco Identity



Inserir nova senha

Requisitos da senha:

- No mínimo 8 caracteres
- Uma letra maiúscula
- Uma letra minúscula
- Um número
- Não deve conter partes do nome de usuário
- A sua senha não pode ser igual às suas últimas 1 senhas

Repetir senha nova

[Criar minha conta](#)

6) Em seguida, ao final da página, na seção **Resources**, selecione a opção **Packet Tracer**

Resources

SELF-PACED COURSES

Learn valuable skills at your own pace anywhere in the world with our self-paced courses.

PACKET TRACER

Access resources on installing and using this learning tool. Find help from the community.

CAREER ADVICE

Access all of our career resources in our Career section.

7) Atualmente a Cisco disponibilizou uma nova versão 8.0.1 que poderá ser feito o download nessa parte selecionando Download no seu sistema operacional. Caso deseje fazer o download de uma versão mais antiga que mais se assemelha à utilizada no curso, siga para o próximo item

Windows Desktop Version 8.0.1 English

[64 Bit Download](#)

[32 Bit Download](#)

Ubuntu Desktop Version 8.0.1 English

[64 Bit Download](#)

macOS Version 8.0.1 English

[64 bit Download](#)

8) Caso deseje fazer o download da versão mais antiga, siga para o fim da página em **Previous versions** e faça o download respectivo ao seu sistema operacional

Previous Versions

Students should download the same version of Cisco Packet Tracer used in their classroom lab. Please contact your instructor to determine the appropriate version of Cisco Packet Tracer.

Cisco Packet Tracer 7.2.2 will continue to be available for compatibility with CCNA 6 and IoT course activities only:

Windows Desktop Version 7.2.2 English

[64 Bit Download](#)

[32 Bit Download](#)

Ubuntu Desktop Version 7.2.2 English

[64 Bit Download](#)

macOS Version 7.2.2 English

[Download](#)

Obs: Caso seja Linux:

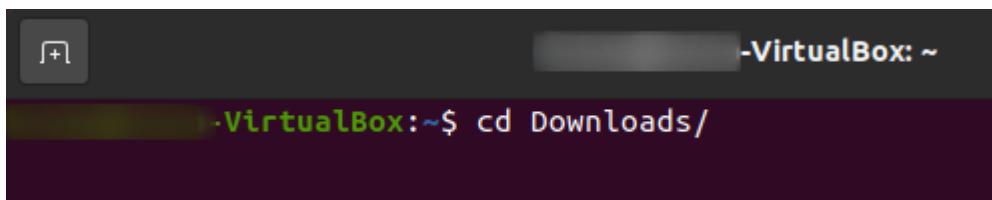
1) Fazer o download da versão do Packet Tracer para Ubuntu Desktop;

2) Abrir o Terminal de Comandos através das teclas

++

ou através do menu de aplicativos;

3) Navegar até o diretório onde se encontra o arquivo de instalação do Packet Tracer através do comando: cd <caminho do download>



Exemplo:

4) Digitar, em sequencia, os seguintes códigos para atualizar a fonte de pacotes do Linux e instalar algumas dependências:

- sudo apt update
- sudo apt upgrade
- sudo apt install dialog
- sudo apt install libgl1-mesa-glx
- sudo apt install libxcb-xinerama0-dev

(Será requisitado a sua senha de usuário administrador e, caso seja necessário, confirme a instalação dos pacotes selecionando a opção <S> ou <Y>).

5) Em seguida, digite o seguinte código com o nome do arquivo de instalação para prosseguir com a instalação do Packet Tracer:

- sudo dpkg -i <nome do arquivo de instalação>

6) Por fim, basta aceitar os termos da licença que será mostrada no processo de instalação:

Configurando PacketTracer

Cisco Packet Tracer

Software License Agreement

DOWNLOADING, INSTALLING, OR USING THE CISCO PACKET TRACER SOFTWARE CONSTITUTES ACCEPTANCE OF THE CISCO END USER LICENSE AGREEMENT ("EULA"
https://www.cisco.com/c/en/us/about/legal/cloud-and-software/end_user_license_agreement.html) AND THE SUPPLEMENTAL END USER LICENSE AGREEMENT FOR CISCO PACKET TRACER ("SEULA"
https://www.cisco.com/c/dam/en_us/about/doing_business/legal/seula/cisco-packet-tracer-software.pdf). IF YOU DO NOT AGREE TO ALL OF THE TERMS OF THE EULA AND SEULA, THEN CISCO SYSTEMS, INC. ("CISCO") IS UNWILLING TO LICENSE THE SOFTWARE TO YOU AND YOU ARE NOT AUTHORIZED TO DOWNLOAD, INSTALL OR USE THE SOFTWARE.

<ok>

Configurando PacketTracer

Do you accept the terms of this EULA?

<Sim>

<Não>

Após esse processo, o programa deverá estar instalado com sucesso no computador!

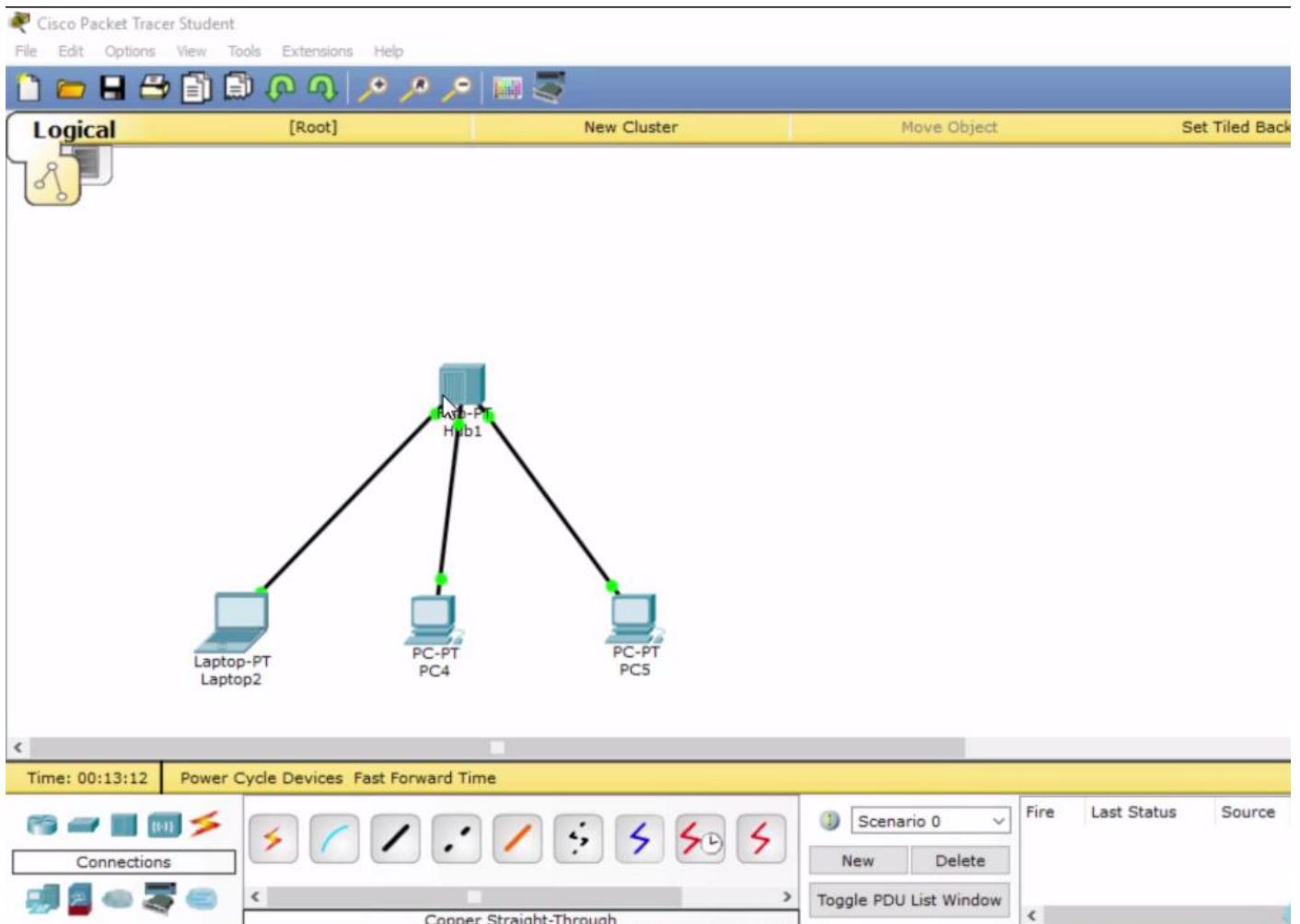
Obs: Caso seja MAC:

- Faça o download para a versão do sistema operacional **Mac OS**;
- Acesse o arquivo de instalação e siga os passos indicados, aceitando os termos e inserindo a senha de usuário quando requisitada.

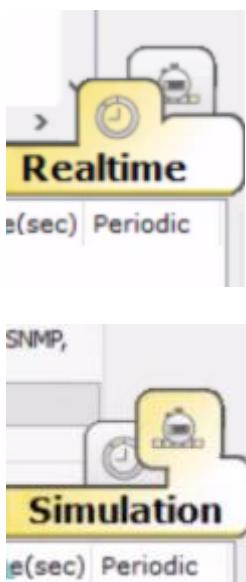
Pronto! O Packet Tracer já está instalado!

Limitação Hub

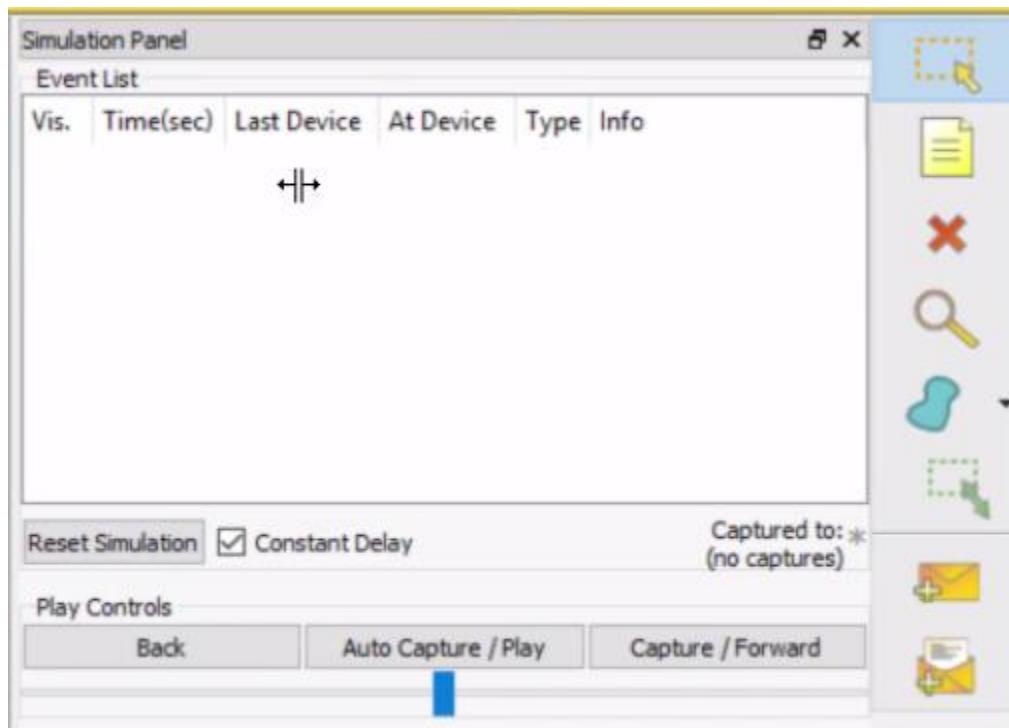
Temos no programa de simulação a rede criamos anteriormente em que temos três computadores interconectados com o hub.



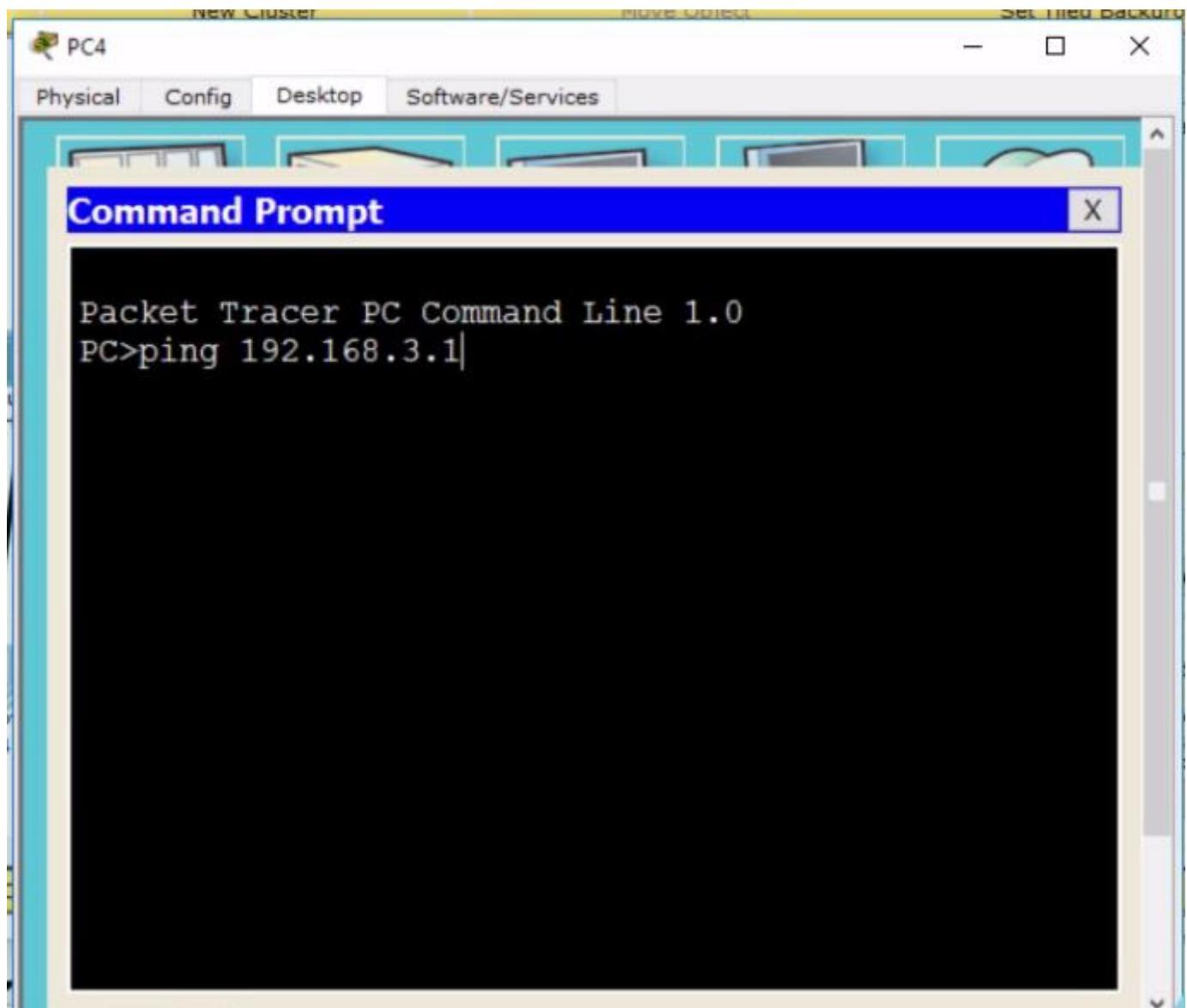
Nós temos os IPs de cada uma das máquinas e agora, iremos testar a conectividade entre eles. Mesmo usando um programa de simulação, teremos que ir no Terminal como teríamos que fazer em outros casos. Mas antes, iremos quebrar em algumas etapas menores que serão analisadas. No canto direito do Packet Tracer mudaremos o modo de operação de "Realtime" para "Simulation".



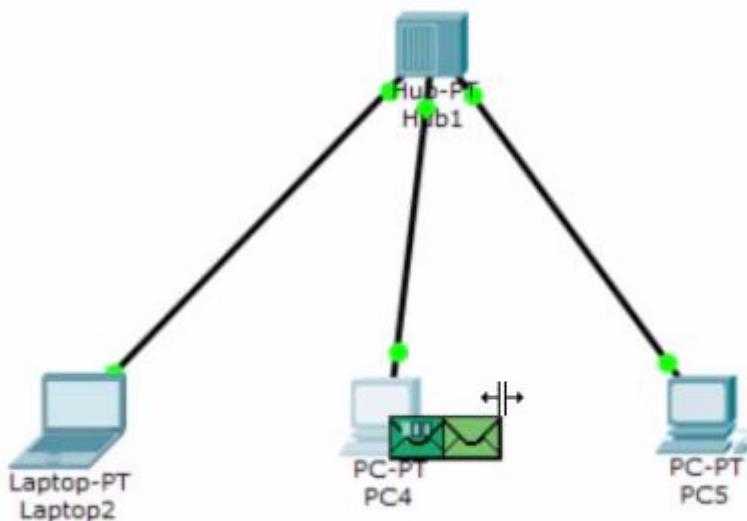
Observe que surgirá a coluna "Simulation Panel".



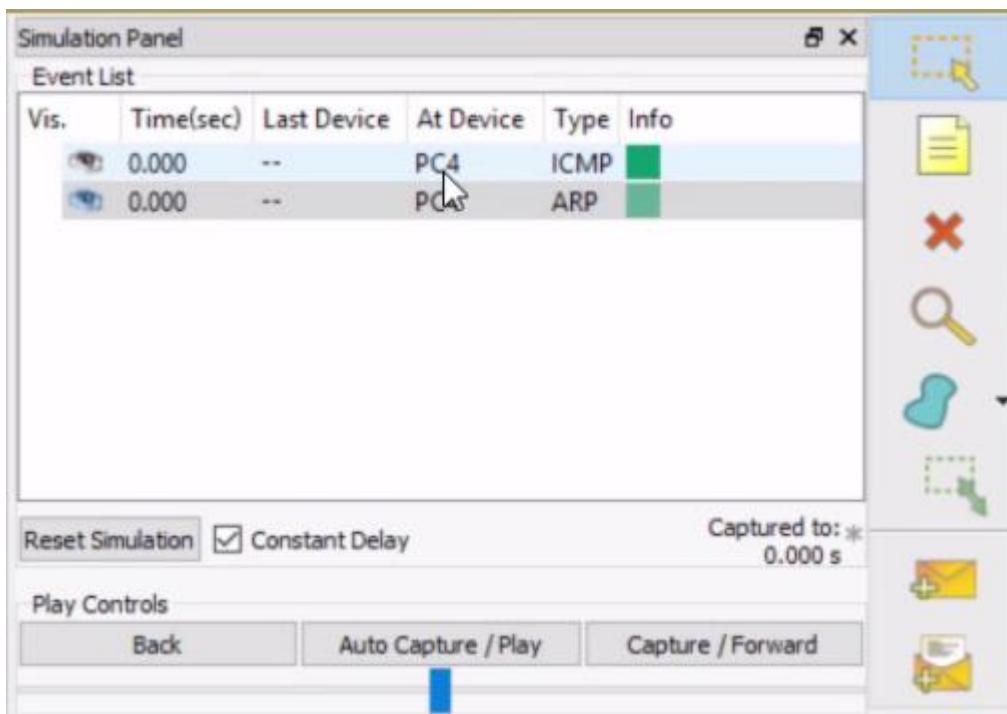
Nela, começará a parecer alguns protocolos de rede que analisaremos. O computador "PC-PT PC4" realizará meu teste de conectividade com o "Laptop-PT Laptop 2". Clicaremos sobre o ícone, clicaremos em "Command Prompt" e digitaremos ping e o endereço IP do desktop.



Observe que agora veremos pequenos envelopes acima do ícone de representação do computador.

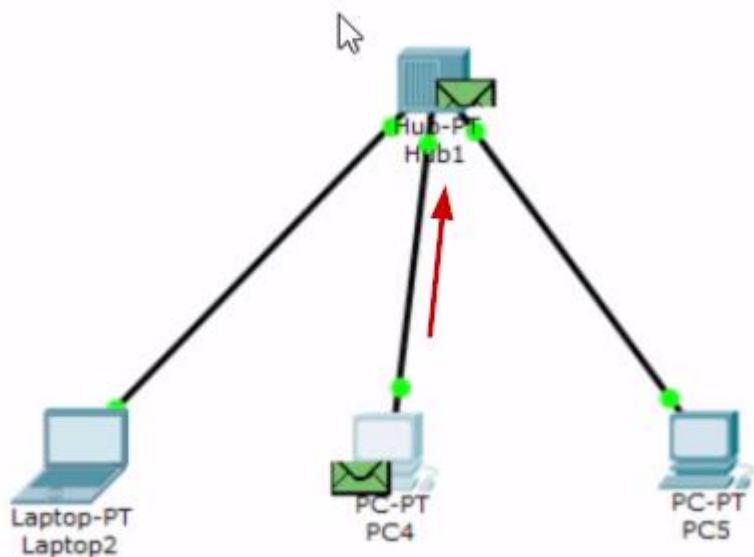


Eles também aparecerão nos protocolos.



Dentro do ping digitado no Command, teremos o protocolo ICMP, que está aparecendo na coluna. E o que significa o ARP? A primeira vez que o computador quer se comunicar com o IP, ele não sabe onde estará localizado. É preciso perguntar para todos os dispositivos que estão na nossa rede.

Então, clicaremos em "Capture/Forward".



O hub não tem informação aonde está conectado o equipamento com o IP do laptop, então, ele passará pelas outras portas perguntando quem tem essa informação. Observe que ele enviará protocolo ARP para descobrir.

Simulation Panel

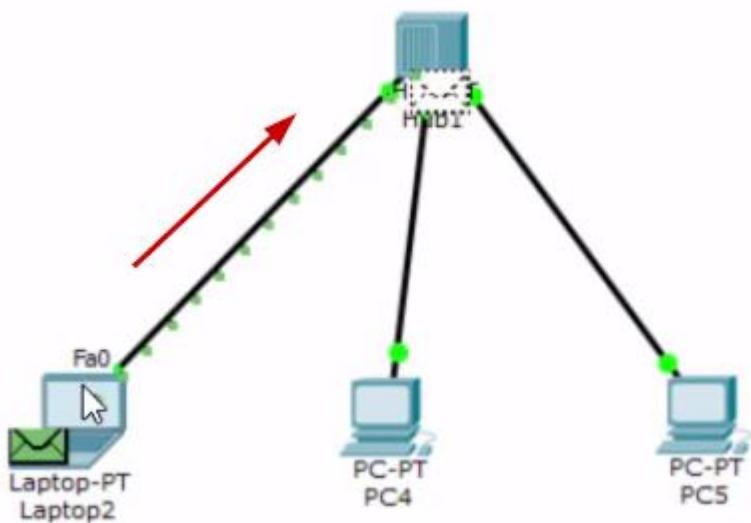
Event List

Vis.	Time(sec)	Last Device	At Device	Type	Info
	0.000	--	PC4	ICMP	
	0.000	--	PC4	ARP	
	0.001	PC4	Hub1	ARP	
	0.002	Hub1	Laptop2	ARP	
	0.002	Hub1	PC5	ARP	

Reset Simulation Constant Delay Captured to: * 0.002 s

Play Controls Back Auto Capture / Play Capture / Forward

O terceiro computador recebeu a requisição e descartou a informação. Isto aconteceu, porque ele não tem o IP que estamos procurando. Estamos buscando o IP 192.168.3.1 e a terceira máquina tem o IP 192.168.3.3. Já o primeiro computador recebeu a informação e terá que devolvê-la informando sua informação.



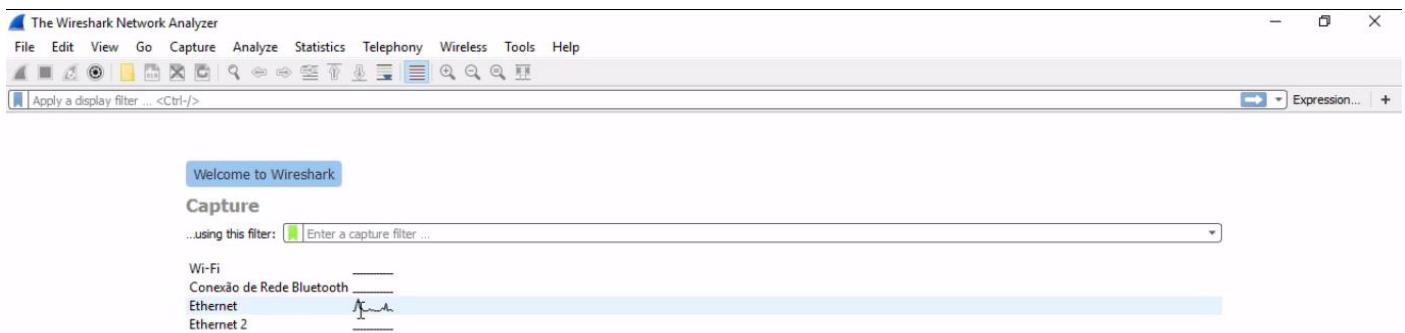
Já sabemos que a requisição veio da segunda máquina e a terceira não deveria receber a requisição. Mas a última máquina continua recebendo informação. Esta é uma das limitações do hub: ele não consegue aprender aonde os computadores estão interconectados e sempre passará as informações para todos os dispositivos conectados com a porta, com exceção de quem enviou a requisição. O nome disso é Broadcast. Imagine um usuário fazendo o download de 500 mb e todos os dispositivos recebendo essa informação... Causa uma lentidão na rede.

Em relação ao hub, precisamos falar também sobre a segurança da informação. A requisição que fizemos entre o segundo computador e o laptop, o hub desconhece aonde está conectado o laptop. Logo, ele enviará para todos os dispositivos que estiverem conectados. Se uma das máquinas tiver um usuário malicioso, ele pode fazer o que chamamos de análise de protocolo e decifrar o que está sendo enviado pelo segundo computador. O hub representa uma lentidão, além da vulnerabilidade da segurança.

Os hubs não conseguem aprender onde está localizado cada máquina, dessa forma, ele repassa a informação para todas as demais máquinas conectadas. Isso quer dizer que caso ocorra um fluxo intenso de tráfego na rede, teremos essa informação sendo encaminhada para todos os demais usuários causando lentidão na rede. Além disso, quando usuários mandam a informação destinada para um usuário específico, os demais usuários recebem essa informação, causando assim uma vulnerabilidade de segurança.

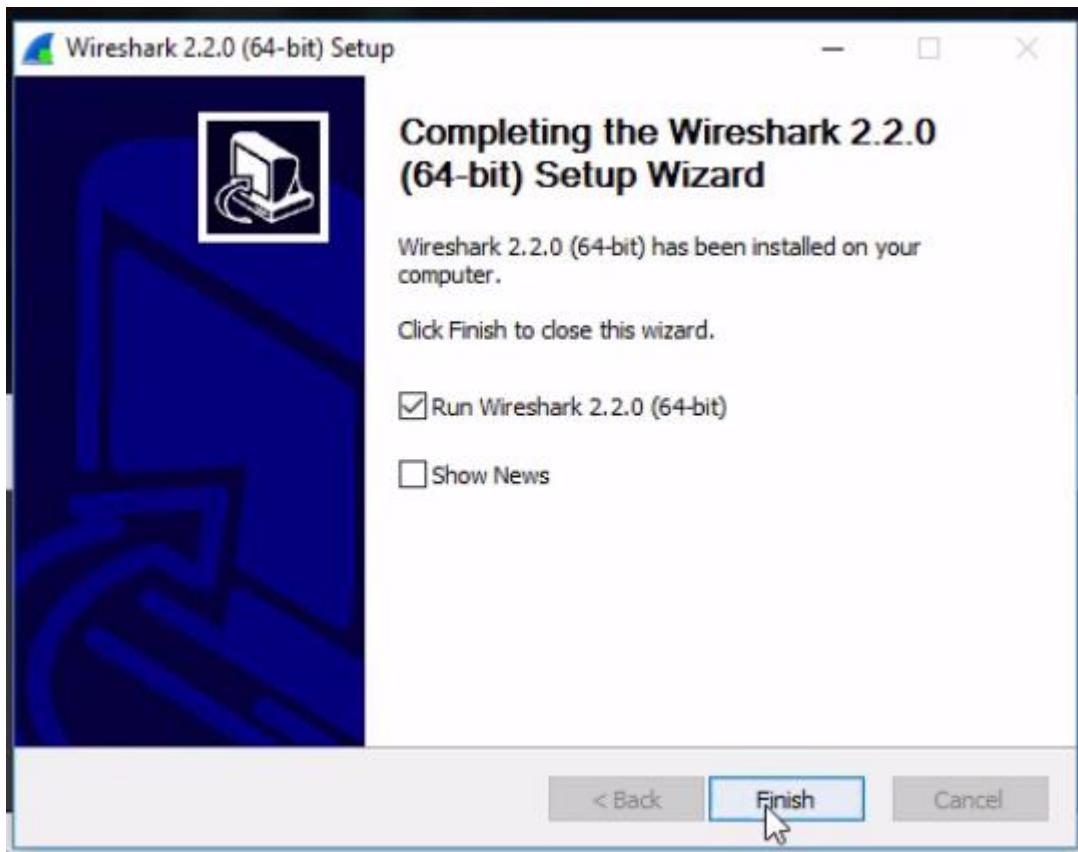
Wireshark http final

Vamos mostrar a vulnerabilidade dos hubs que conversamos. Um usuário malicioso pode entrar na nossa rede e analisar as informações que são trafegadas, por exemplo, entre um site e outra máquina. Estou no site do Buscapé, e vou simular os dois papéis - o da vítima e o do usuário malicioso. Para isto, usaremos um programa para a análise de protocolos chamado [wireshark](#).

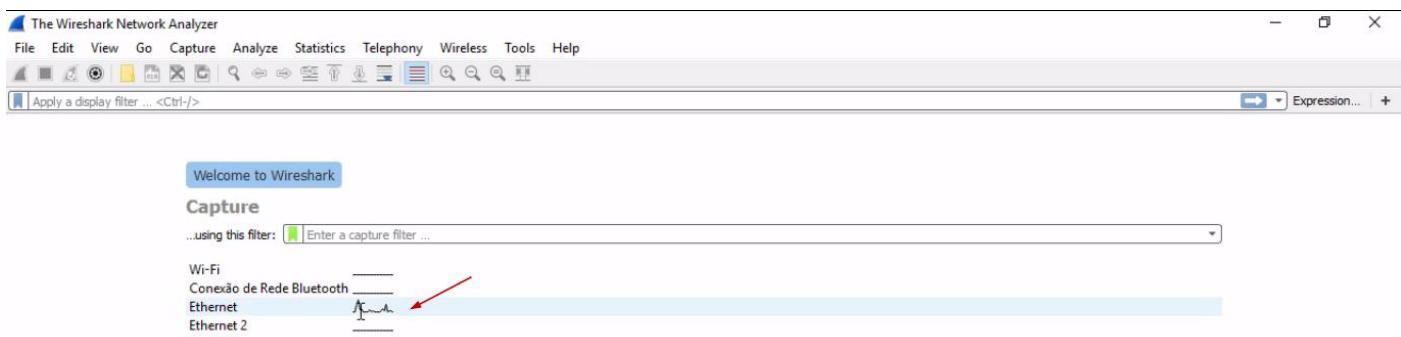


Faremos o download na página, selecionaremos o sistema operacional. No caso, escolheremos "Windows Installer (64-bit)". Se você estiver usando o Mac, encontrará orientações [nos exercícios](#).

Nós já temos instalados na máquina, mas vamos executar e fazer a passagem da instalação. Nos primeiros passos, só clicaremos em "Next", até chegarmos em "Install". Depois de finalizada, basta clicar em "Next" e "Finish" na janela de Setup.



Aparecerá um ícone de barbatana de tubarão no seu desktop. No meu computador, ele precisará pegar as placas de redes conectadas a máquina e provavelmente, a saída seja diferente com você.



Observe que temos uma atividade na placa sinalizada. Ao clicarmos nela, veremos que temos alguns protocolos passando pela rede.

Frame 1: 60 bytes on wire (480 bits), 60 bytes captured (480 bits) on interface 0

> IEEE 802.3 Ethernet
> Logical-Link Control
> Spanning Tree Protocol

0000 01 80 c2 00 00 00 a8 9d d2 d3 e2 30 00 27 42 420.'B8
0010 03 00 02 02 3c 80 00 a8 9d d2 d3 e2 30 00 00<.0..
0020 00 00 80 00 a8 9d d2 d3 e2 30 80 01 00 00 14 000.....
0030 02 00 0f 00 00 00 00 00 00 00 00 00 00 00 00 00

Nós não nos aprofundaremos na parte de análise de protocolo do Wireshark, porque o nosso foco é demonstrar a vulnerabilidade de um hub conectado a um usuário malicioso.

Vamos ver o que o Wireshark está nos mostrando:

Frame 1: 60 bytes on wire (480 bits), 60 bytes captured (480 bits) on interface 0

> IEEE 802.3 Ethernet
> Logical-Link Control
> Spanning Tree Protocol

O usuário malicioso colocou o computador na porta do hub e começará a analisar o tráfego da rede. Seguiremos com o exemplo, mostrando uma vítima acessando o site do Buscapé e fazendo uma pesquisa por câmeras Canon.

www.buscapé.com.br/camera-digital/canon

canon

BUSCAR ENTRAR

Veja também em outras categorias: Cartucho para Impressora | Impressora | Filmadora | Mais categorias

Canon x

Palavra-Chave

FILTRAR

Avaliação

Câmera Digital Canon EOS Rebel T5 18.0 Megapixels Info

De R\$ 1.529,10 até R\$ 3.999,00 em 13 lojas

COMPARA 49 PREÇOS

55 56036+80 [ACK] Seq=1 Ack=1 Win=2092 Len=1

De volta ao Wireshark, veremos o que está sendo analisado pelo usuário malicioso. Ele quer descobrir qual foi o último termo de busca pesquisado pelo usuário no Buscapé. Primeiramente, será filtrado os protocolos referentes ao site Buscapé por meio do IP da máquina da empresa. É possível fazer isso no Prompt de Comando, digitando:

```
c:\Users\Alura>nslookup www.buscape.com.br
```

Será retornado o endereço IP da máquina do Buscapé. Após copiar o endereço IP, e vamos colocar um filtro no Wireshark para encontrarmos a máquina do Buscapé.

```
ip.addr == 177.11.254.183
```

No.	Time	Source	Destination	Protocol	Length	Info
24	11.673719	192.168.1.35	177.11.254.183	TCP	55	56068>80 [ACK] Seq=1 Ack=1 Win=255 Len=1
25	11.678682	177.11.254.183	192.168.1.35	TCP	66	80>56068 [ACK] Seq=1 Ack=2 Win=33 Len=0 SLE=1 SRE=2
31	12.045045	192.168.1.35	177.11.254.183	TCP	55	56009>80 [ACK] Seq=1 Ack=1 Win=257 Len=1
32	12.049615	177.11.254.183	192.168.1.35	TCP	66	80>56009 [ACK] Seq=1 Ack=2 Win=66 Len=0 SLE=1 SRE=2
442	45.416874	192.168.1.35	177.11.254.183	TCP	54	56068>80 [FIN, ACK] Seq=2 Ack=1 Win=255 Len=0
443	45.416909	192.168.1.35	177.11.254.183	TCP	54	56009>80 [FIN, ACK] Seq=2 Ack=1 Win=257 Len=0
454	45.422395	177.11.254.183	192.168.1.35	TCP	60	80>56068 [ACK] Seq=1 Ack=3 Win=33 Len=0
455	45.422484	192.168.1.35	177.11.254.183	TCP	54	56068>80 [ACK] Seq=3 Ack=2 Win=255 Len=0
457	45.422800	177.11.254.183	192.168.1.35	TCP	60	80>56009 [FIN, ACK] Seq=1 Ack=3 Win=66 Len=0
459	45.422883	192.168.1.35	177.11.254.183	TCP	54	56009>80 [ACK] Seq=3 Ack=2 Win=257 Len=0
550	47.219529	192.168.1.35	177.11.254.183	TCP	66	56208>80 [SYN] Seq=0 Win=8192 Len=0 MSS=1460 WS=256 SACK_PERM=1
551	47.225024	177.11.254.183	192.168.1.35	TCP	66	80>56208 [SYN, ACK] Seq=0 Ack=1 Win=5792 Len=0 MSS=1448 WS=256 SACK_PERM=1
552	47.225122	192.168.1.35	177.11.254.183	TCP	54	56208>80 [ACK] Seq=1 Ack=1 Win=66560 Len=0
553	47.225312	192.168.1.35	177.11.254.183	HTTP	1716	GET /ajax/produtos?ids=345394&maisbuscados=true HTTP/1.1

> Frame 24: 55 bytes on wire (440 bits), 55 bytes captured (440 bits) on interface 0
> Ethernet II, Src: Apple_01:cf:5e (ac:87:a3:01:cf:5e), Dst: Shanghai_d3:e2:30 (a8:9d:d2:d3:e2:30)
> Internet Protocol Version 4, Src: 192.168.1.35, Dst: 177.11.254.183
> Transmission Control Protocol, Src Port: 56068, Dst Port: 80, Seq: 1, Ack: 1, Len: 1

Observe a coluna de protocolo e veja que aparece diversas vezes TCP. O protocolo TCP está uma camada acima do IP, e será responsável por indicar como a comunicação será estabelecida e será transportada a informação. Se conseguirmos reconstruir o protocolo TCP, podemos ver eventualmente os headers do HTTP e descobrir algumas informações.

Vamos escolher um protocolo no fim da análise.

No.	Time	Source	Destination	Protocol	Length	Info
1113	54.440057	177.11.254.183	192.168.1.35	TCP	1062	[TCP segment of a reassembled PDU]
1114	54.440058	177.11.254.183	192.168.1.35	TCP	969	[TCP segment of a reassembled PDU]
1115	54.440059	177.11.254.183	192.168.1.35	TCP	1422	[TCP segment of a reassembled PDU]
1116	54.440061	177.11.254.183	192.168.1.35	TCP	1422	[TCP segment of a reassembled PDU]
1117	54.440063	177.11.254.183	192.168.1.35	TCP	1422	[TCP segment of a reassembled PDU]
1118	54.440064	177.11.254.183	192.168.1.35	TCP	1422	[TCP segment of a reassembled PDU]
1119	54.440065	177.11.254.183	192.168.1.35	HTTP	1171	HTTP/1.1 200 OK (text/html)
1120	54.440160	192.168.1.35	177.11.254.183	TCP	54	56217>80 [ACK] Seq=5369 Ack=38662 Win=66560 Len=0
1445	56.617945	192.168.1.35	177.11.254.183	HTTP	1790	GET /ajax/login/user-area HTTP/1.1
1446	56.624004	177.11.254.183	192.168.1.35	TCP	60	80>56217 [ACK] Seq=38662 Ack=6817 Win=17152 Len=0
1447	56.624005	177.11.254.183	192.168.1.35	TCP	60	80>56217 [ACK] Seq=38662 Ack=7105 Win=17152 Len=0
1448	56.629422	177.11.254.183	192.168.1.35	TCP	563	[TCP segment of a reassembled PDU]
1449	56.629871	177.11.254.183	192.168.1.35	HTTP	925	HTTP/1.1 200 OK (text/html)
1450	56.629925	192.168.1.35	177.11.254.183	TCP	54	56217>80 [ACK] Seq=7105 Ack=40042 Win=65024 Len=0

> Frame 24: 55 bytes on wire (440 bits), 55 bytes captured (440 bits) on interface 0
> Ethernet II, Src: Apple_01:cf:5e (ac:87:a3:01:cf:5e), Dst: Shanghai_d3:e2:30 (a8:9d:d2:d3:e2:30)
> Internet Protocol Version 4, Src: 192.168.1.35, Dst: 177.11.254.183
> Transmission Control Protocol, Src Port: 56068, Dst Port: 80, Seq: 1, Ack: 1, Len: 1

Clicaremos com o botão direito, logo será aberto um menu em que selecionaremos "Follow". Vamos fazer uma análise do HTTP.

Wireshark - Follow TCP Stream (tcp.stream eq 74) · wireshark_F6067C02-77AF-4F6B-B300-C9ABAAC44982A_20160915094601_a06288

```

GET /cprocura?fromSearchBox=true&produto=canon HTTP/1.1
Host: www.buscape.com.br
Connection: keep-alive
Upgrade-Insecure-Requests: 1
User-Agent: Mozilla/5.0 (Windows NT 10.0; WOW64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/52.0.2743.116 Safari/537.36
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,*/*;q=0.8
Referer: http://www.buscape.com.br/
Accept-Encoding: gzip, deflate, sdch
Accept-Language: pt-BR,pt;q=0.8,en-US;q=0.6,en;q=0.4
Cookie: xpwy=1KKo; __bid=28298id3-3fdb-4879-a0d1-3cb946fb2b1; BTG360_utms=; btg_lastprod={"ids":["345394"]}; _spl_pv=1;
xb=Telefone&telefone&carro&canon&canon&canon&canon&canon&canon; xr=1=canon; idloc=1891812915220160913164808457;
buscapse_id_user=18918129152201609131647538cn=2073969380&xr=b=e6f70dec910f1307fd24815306da44cb;
bpc=dupv=2016-09-15+09%3A41%3A26&iduvcs=0&uso=0&tzu=0&pr=0&cn=2073969380&rbc=056228ceac7d30e6629d2deba423ad; sessao=rfin=NO-
REFERER&site_origem=9402546&cna=2073969380&stp=1&ppv=2016-09-15+09%3A41%3A26&id_entrada=site_origem%3D9402546&tab=HOME&tab=padrao&dtab=15-09-2016-10%3A01&exp_cont=gcsc
%3Dv20150129k26data_create_exp_cont%3D1473943286645&xr=3=d4a3ee0b98601e2c4bfbd5770b2d3&sbx=false&kwt=null; refererPage=home; _utmt=1;
_utma=243682202.1030198133.1473796079.1473865156.1.10.1473943301.3; _utmb=243682202.1.10.1473943303; _utmc=243682202.1.1.utmcsrc=(direct)|utmccn=(direct)|utmcmd=(none); _gat=1; tracelogger=; tt_c_vmt=1473943303; tt_c_c=direct; tt_c_s=direct; tt_c_m=direct; _gat_UA-1827174-7e=1; _ttuu.s=1473943303069;
tt_uw=7508000042C14572242948302ACBBAF; tt_nprf=; OAX=nEH45FFY/AOCGx; nav12680=68068354a175dd2567ee06a5609|2_260_Sao Paulo_Sao Paulo_Brazil_AB_;
_ga=GAI.3.1030198133.1473796079

HTTP/1.1 301 Moved Permanently
Server: Apache-Coyote/1.1
Connection: keep-alive
Set-Cookie: redirect_cookie=; Domain=.buscape.com.br; Expires=Thu, 01-Jan-1970 00:00:10 GMT; Path=/
Cache-Control: no-cache
Location: http://www.buscape.com.br/cprocura/canon
Set-Cookie: redirect_cookie=true; Domain=.buscape.com.br; Expires=Thu, 15-Sep-2016 15:33:23 GMT
Set-Cookie: buscapse_id_user=18918129152201609131647538cn=135856864&rbc=c45f01d855e927sa12001c07f03fdf21; Domain=.buscape.com.br; Expires=Tue, 14-Sep-2021 12:46:43 GMT; Path=/
Set-Cookie: bpc=dupv=2016-09-15+09%3A41%3A26&iduvcs=0&uso=0&tzu=1&pr=0&cn=135856864&rbc=0501b49c9903993008d2e9af4bf9a048; Domain=.buscape.com.br; Expires=Tue, 14-Sep-2021 12:46:43 GMT; Path=/
Set-Cookie: sessao=rfin=NO-REFERER&site_origem=9402546&kw=canon&kwu=canon&cna=135856864&stp=1&dppv=2016-09-15+09%3A41%3A26&id_entrada=site_origem
%3D9402546&tab=HOME&tab=padrao&dtab=15-09-2016-10%3A01&exp_cont=data_create_exp_cont%3D1473943286645%26gcs
%3Dv20150129k26data_create_exp_cont%3D1473943286645&xr=3=a7cff9cd3496b5436be678468ce3765&sbx=true&kwt=canon&correcaoBuscaFuzzy=0; Domain=.buscape.com.br; Path=/
Set-Cookie: tracelogger=; Domain=.buscape.com.br; Path=/
P3P: policyref="http://www.buscape.com.br/w3c/p3p.xml", CP="PSA CONO OUR ONL BUS NOI"

Packet 1009: 4 client pkt(s), 32 server pkt(s). 7 turn(s). Click to select.
Entire conversation (83 kB) Show and save data as ASCII Stream 74 Find Next Filter Out This Stream Print Save Help

```

Conseguimos identificar que o usuário pesquisou por canon, mas o usuário malicioso poderia descobrir outros tipos de informação. Percebemos como hub apresenta esse tipo de problema, porque ele passa as informações para todas as máquinas interconectadas. Com uma análise de protocolo é possível descobrir o que a vítima pesquisou no Buscapé.

Por que o usuário malicioso consegue ver o que a vítima pesquisou no site do Buscapé? Isto acontece porque o site não usa um sistema de criptografia. Então, é possível com uma análise de protocolo ver o que o usuário está digitando.

Vamos ver um outro cenário, acessaremos um site com sistema de criptografia, e o usuário malicioso continuará fazendo uma análise de protocolo. Vamos ver o que ele consegue descobrir. Neste caso, o site acessado será o Youtube.



O protocolo do [Youtube](#) é [Https](#), sendo que o s se refere a uma camada de criptografia. Vamos supor que alguém pesquise por "Java".

Já o usuário malicioso tentará analisar a pesquisa feita por ele. Primeiramente, será necessário descobrir o IP do Youtube. No Terminal digitaremos:

```
c:\Users\Alura>nslookup www.youtube.com
```

Teremos o seguinte retorno:

```
C:\Windows\system32> nslookup www.youtube.com
Microsoft Windows [versão 10.0.10586]
(c) 2015 Microsoft Corporation. Todos os direitos reservados.

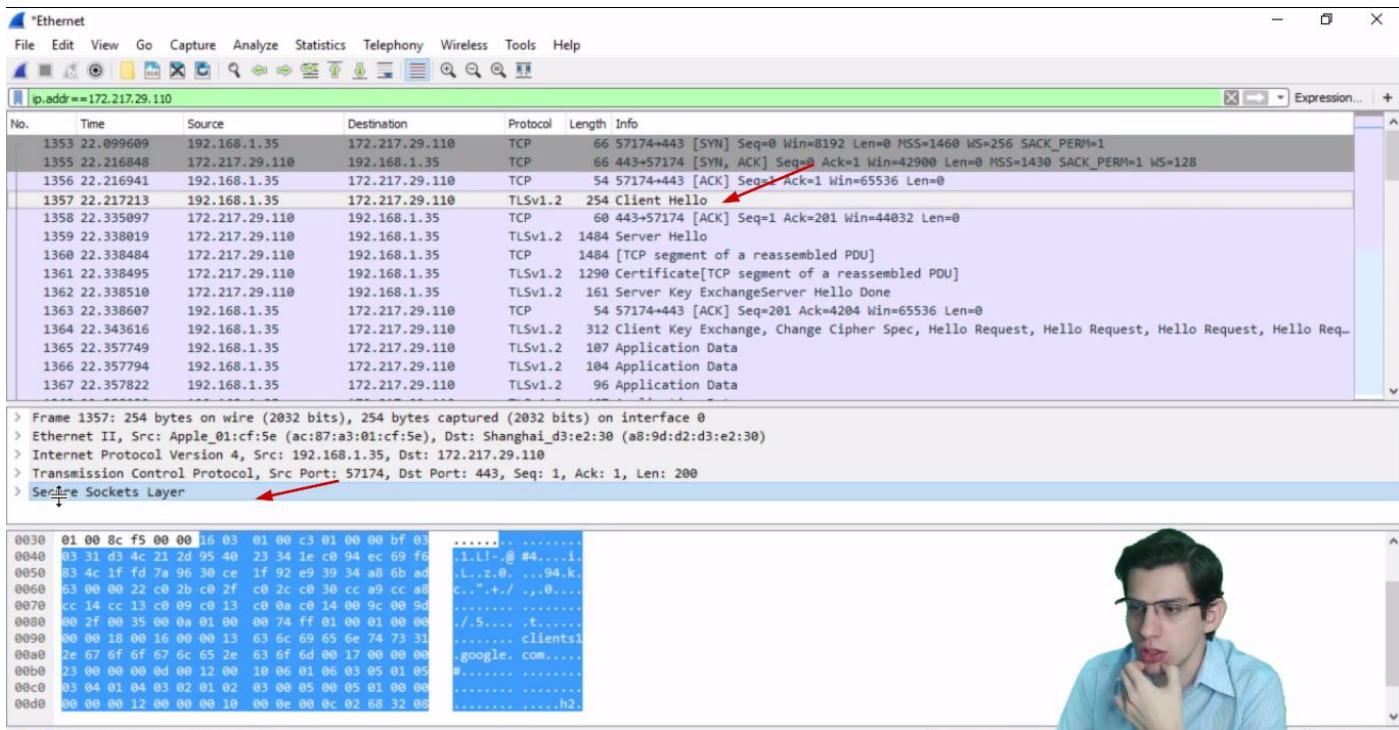
C:\Windows\system32> nslookup www.youtube.com
Servidor:  openrg.home
Address:  192.168.1.1

Não é resposta autoritativa:
Nome:      youtube-ui.l.google.com
Addresses: 2800:3f0:4001:802::200e
          172.217.29.110 ←
Aliases:   www.youtube.com

C:\Windows\system32>
```

Depois, no filtro do Wireshark, ele digitará:

```
ip.addr == 172.217.29.110
```



É possível identificar que o Youtube foi acessado. Mas vamos clicar no protocolo indicado.

Observe que aparece a mensagem Secure Sockets Layer, este é um protocolo que coloca a camada de segurança na informação. É por conta desses protocolos que talvez não seja possível descobrir qual foi o termo de busca da vítima.

Mas faremos o mesmo que fizemos no exemplo passado, depois, procuraremos o protocolo TCP e iremos clicar sobre ele. A nova janela que será aberta, não trará informação como a anterior.



Vemos várias letras e caracteres especiais, mas está difícil identificar o que está escrito. O Youtube usou a camada de criptografia e nós não conseguimos ver o que o usuário está pesquisando.

Para saber mais: Camadas de protocolos

Durante a explicação eu comento que o protocolo TCP está acima da camada onde o protocolo IP está presente. Os protocolos em redes de telecomunicações seguem uma hierarquia e cada um é responsável por determinada função na comunicação.

O que acontecia antigamente no início do desenvolvimento das redes de telecomunicações é que cada fabricante desenvolvia protocolos proprietários e não era possível assim se comunicar com equipamentos de redes de outros fabricantes, criando assim o chamado "vendor lock-in".

Dessa forma, foi criado um modelo que tinha como intuito padronizar o desenvolvimento de hardware e software dos mais variados tipos de fabricantes para que pudessem assim se comunicar, mesmo que um tivesse alguns recursos a mais que o do outro fabricante, a comunicação deveria ser estabelecida. Para isso, foi definido que esses protocolos de comunicação seriam divididos em 7 camadas de comunicação, o chamado modelo OSI (Open System Interconnection). O protocolo TCP por exemplo, encontra-se na camada 4 que é conhecida como camada de transporte, o protocolo IP encontra-se na camada 3 que é conhecida como camada de rede.

A parte de protocolos é um assunto muito vasto e não é o foco desse nosso curso, mas sugiro que faça uma pesquisa sobre o modelo OSI e os principais protocolos que temos em cada camada :)

O Wireshark tem como principal utilização analisar protocolos que trafegam na rede com o intuito de verificar problemas que possam existir.

TLS (Transport Layer Security) seria um protocolo de criptografia utilizado para segurança da informação. Ele seria a evolução do protocolo SSL (Secure Sockets Layer).

O protocolo TCP encontra-se acima da camada onde o IP está localizado e ele é responsável por realizar o transporte da minha informação. Além do protocolo TCP, essa camada possui também outro protocolo bastante conhecido, o UDP.

O youtube usa em seu site um sistema de criptografia das informações, onde o protocolo TLS é responsável por essa atividade. Pelo fato das informações, estarem criptografadas não foi possível reconstruir a informação e visualizar o que o usuário estava digitando.

Opcional: Instalando o Wireshark

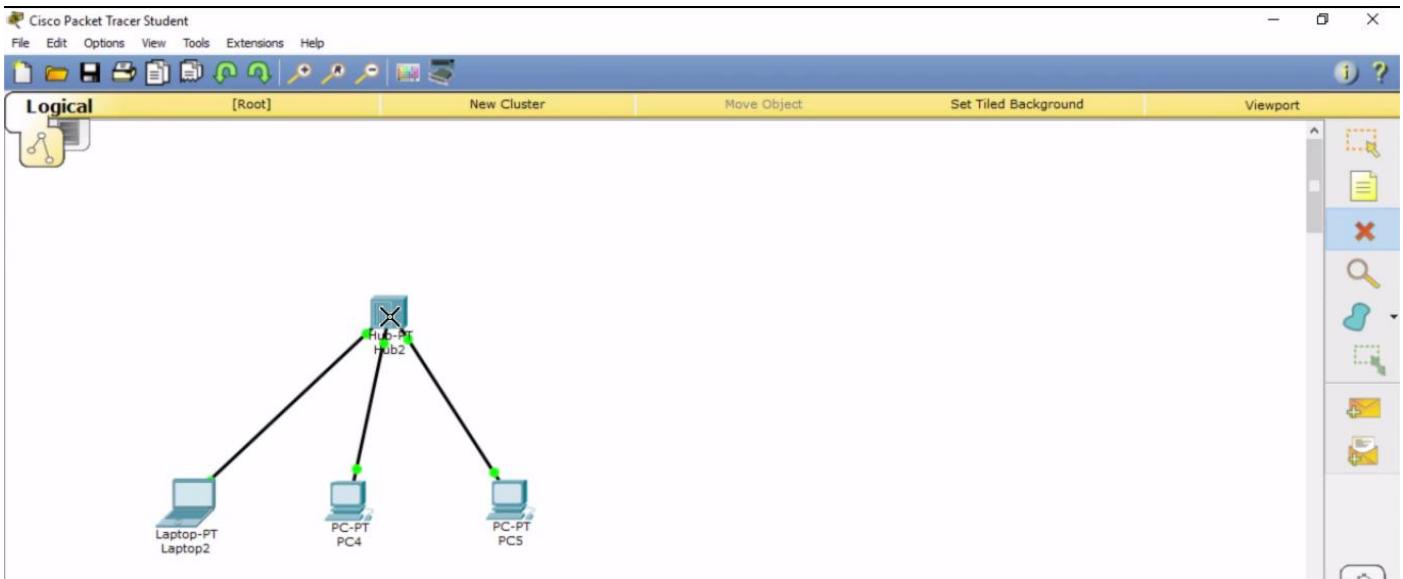
- No windows e no MAC entrar no site <https://www.wireshark.org/#download> e fazer o download de seu sistema operacional.
- Caso seja o Linux:
 - Fazer download:
<https://drive.google.com/open?id=0BzmYQVm4W7nTVVfeURTV2hySk0>
 - Descompactar e realizar a instalação, depois ir até o terminal e digitar:
 - sudo apt-get install libcap2-bin wireshark
 - sudo chgrp (#seu usuario#) /usr/bin/dumpcap
 - sudo chmod 750 /usr/bin/dumpcap
 - sudo setcap cap_net_raw,cap_net_admin+eip /usr/bin/dumpcap
 - wireshark

Switches

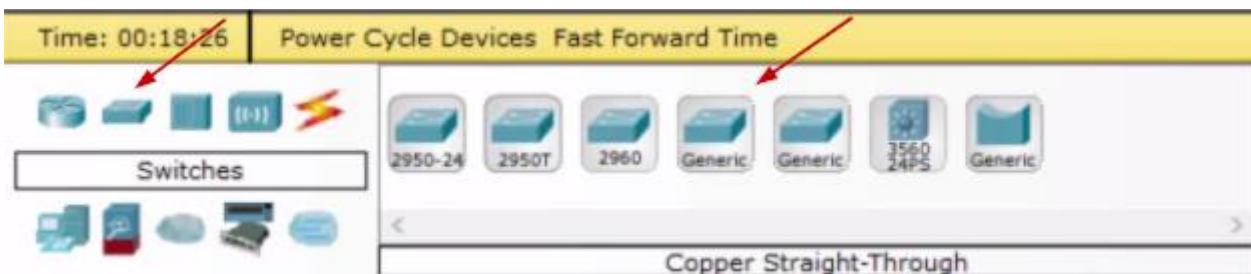
Vimos que os hubs apresentam uma certa limitação para identificar qual equipamento está em uma determinada porta, podendo ocasionar em lentidão e problemas de segurança como vimos nas análises do Wireshark.

Para evitarmos a limitação do hub, foram desenvolvidos outros equipamentos com o intuito de melhorar a performance. Um equipamento criado e que também interconecta os dispositivos finais recebe o nome de **Switch**. Nos aprofundaremos sobre o assunto.

Vamos primeiro deletar o Hub que colocamos no projeto no Packet Tracer. Basta selecionar o ícone de x da coluna da direita e depois clicar sobre o Hub.



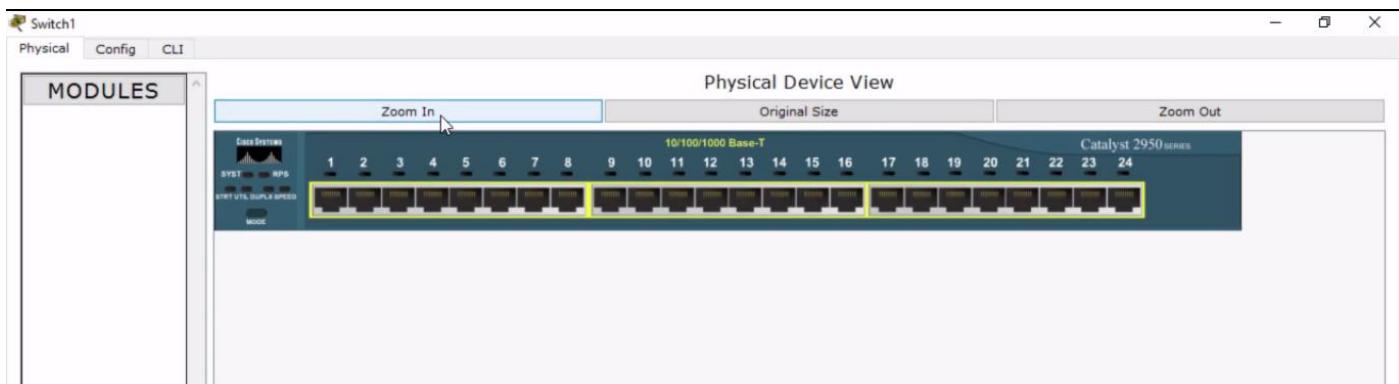
Deletamos o hub. Depois, clicaremos na tecla "Esc" para sairmos do modo "x". Em seguida, selecionaremos o Switch no menu do canto esquerdo.



Aparecerão diferentes opções de equipamentos. Como o software foi desenvolvido pela Cisco, a empresa utilizou seus próprios equipamentos. Selecionaremos um modelo:

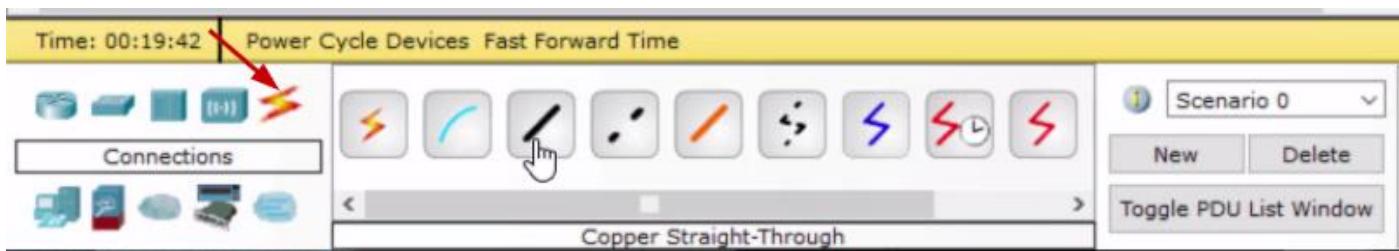


E depois, daremos um clique duplo no Switch. Então, irá aparecer a imagem com o layout do equipamento.

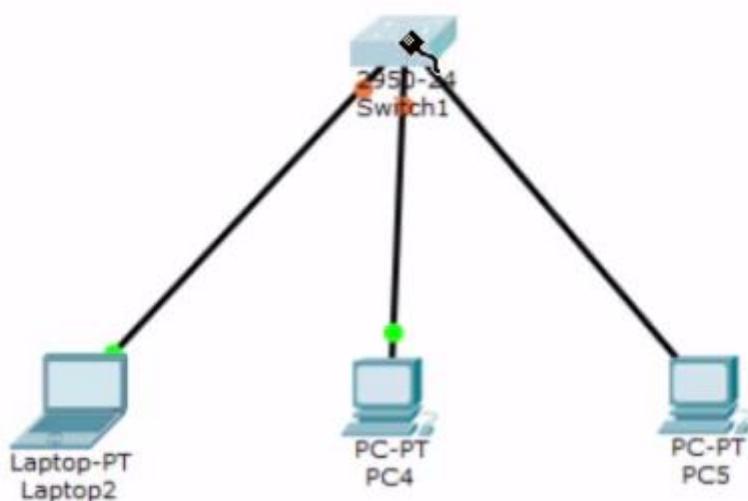


Dependendo do modelo e do fabricante, o modelo irá variar. Mas em essência, todos terão portas que nos permitem conectar os dispositivos finais dos computadores usados nas simulações.

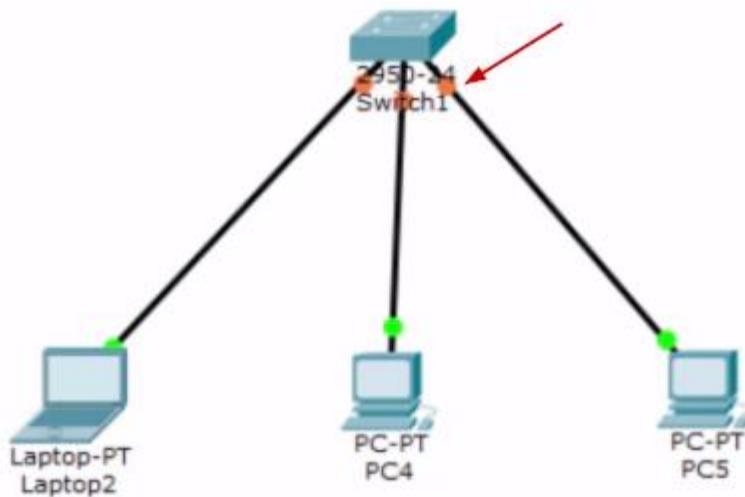
Veremos como conectar os computadores com o Switch. O hub e o switch terão o mesmo tipo de placa, que receberá o sinal nas portas das posições 1 e 2 e transmitirá nas posições 3 e 6. Sabemos que o laptop transmitirá na posição 1 e 2 e o Switch receberá na posição 1 e 2. Ocorre uma conexão natural e usaremos o cabo direto. Clicaremos no ícone do raio no menu da esquerda e selecionaremos o cabo direto.



Clicaremos no laptop, selecionaremos a porta "FastEthernet0" e ligaremos até o Switch - que selecionaremos a porta "FastEthernet0/1". Repetiremos o processo com os demais computadores.

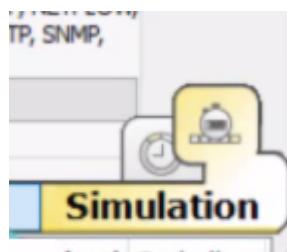


Mas diferente do Hub, que ficará sinalizado com luzes verdes, o Switch ficará com luzes da cor laranja.

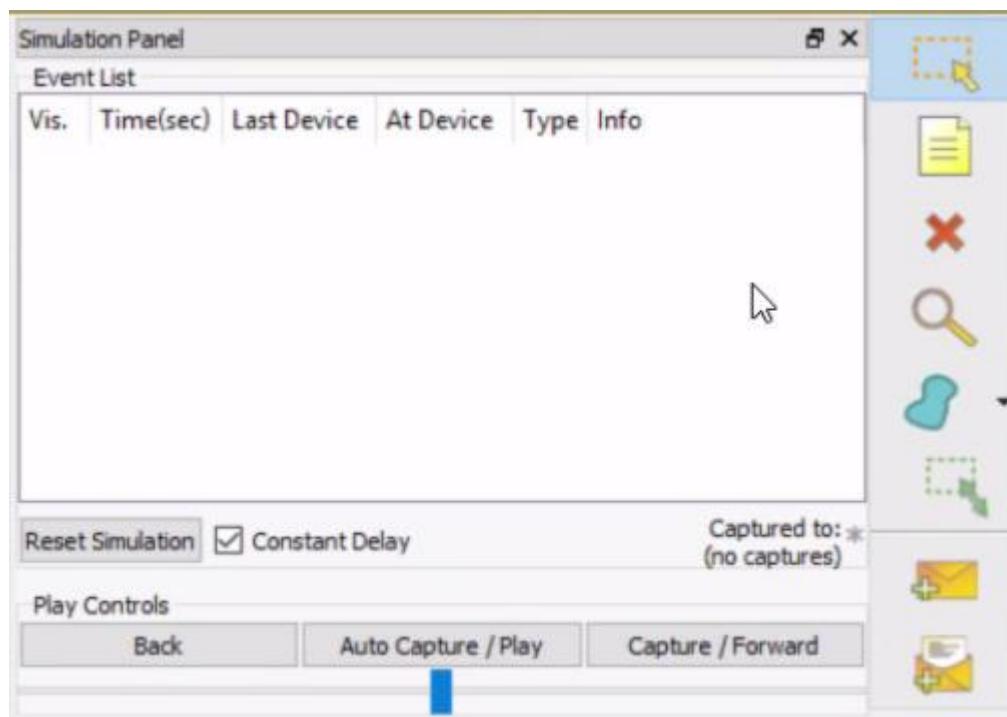


O Switch precisa de um período de tempo para habilitar a porta de comunicação. O processo demora alguns segundos e é retratado na simulação também. À medida que as portas vão sendo habilitadas, as luzes mudam de cor e ficam verdes.

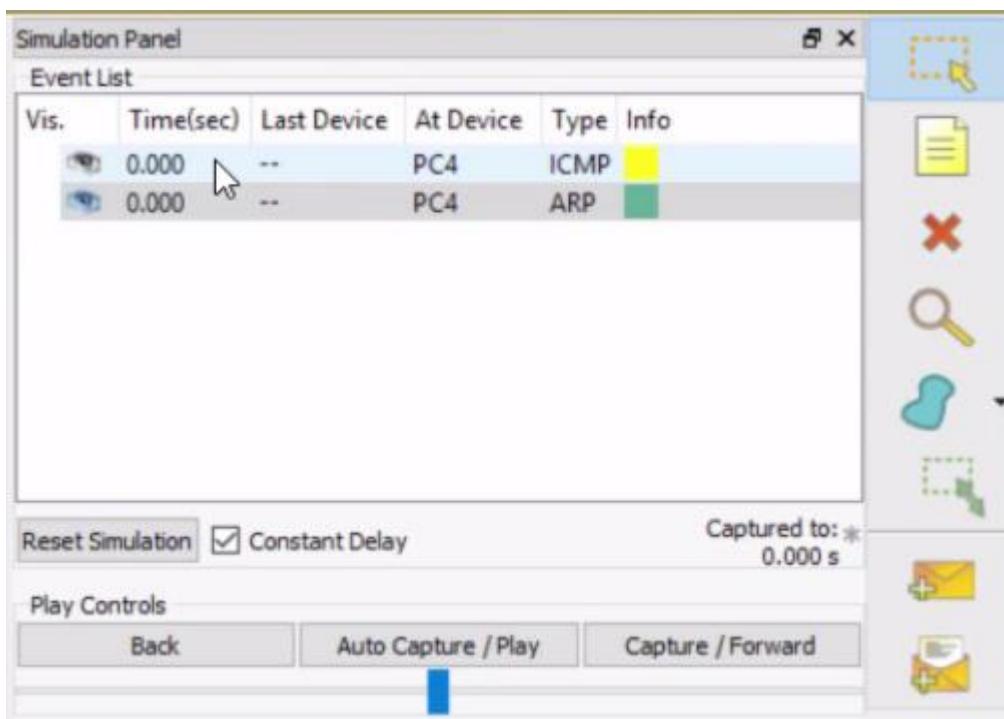
Em seguida, testaremos a conectividade como foi feito anteriormente. Mas queremos quebrá-la em posições menores para que ela possa verificar como a comunicação acontece até chegar ao outro computador. Novamente, mudaremos a posição de "Realtime" para "Simulation" no canto inferior da direita.



E aparecerá a coluna que mostrará os protocolos da simulação.

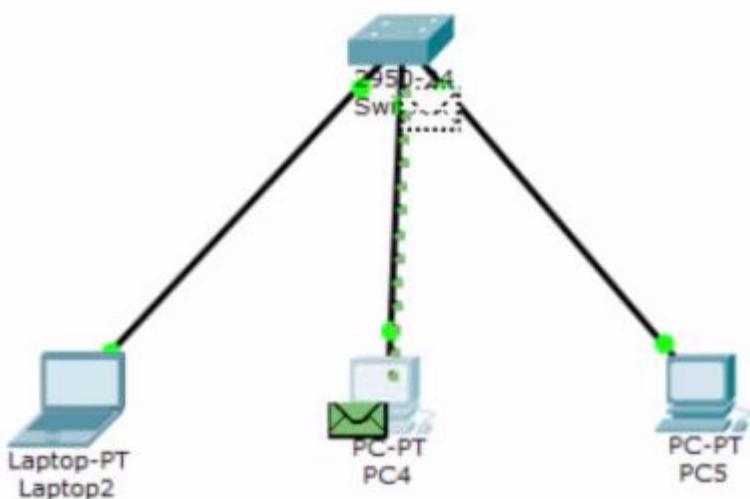


Agora temos o segundo computador que estou usando para a gravação do curso. Ao clicar no ícone dele, acessaremos o Command Prompt. Digitaremos na tela ping 182.168.3.1, usando o IP do laptop que queremos nos conectar. A partir disso, será mostrado no "Simulation Panel" os protocolos que vimos anteriormente no hub.

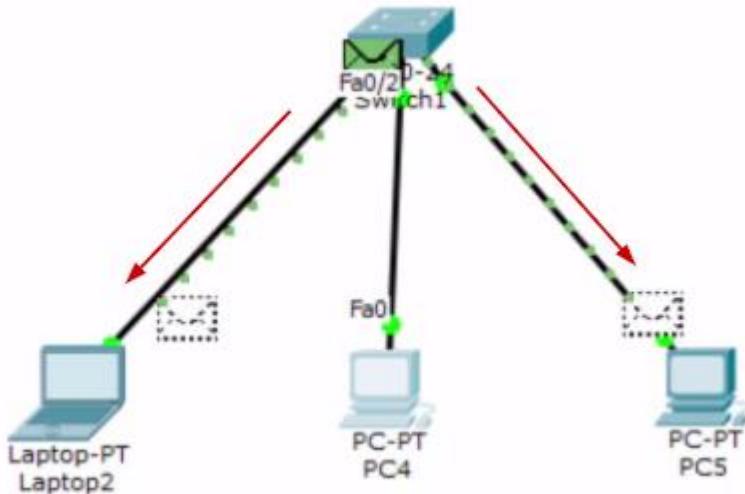


O protocolo ICMP está dentro do ping e o ARP, que não sabe onde está localizado o IP e perguntará para todos na rede.

Vamos seguir a animação.



Observe que a informação do ARP para tentar descobrir onde está o laptop foi passada para o Switch, que também não sabe qual computador está conectado. Ele irá enviar as requisições para os outros computadores, com exceção da máquina de onde foi originada a informação.



A informação foi enviada para os dois computadores. Mas o terceiro não recebeu a requisição, porque o IP termina com o número 3.

Então, a informação será descartada. O laptop receberá a informação do Switch e depois, irá devolvê-la para ao mesmo. Até aqui, o processo é o mesmo de quando utilizamos o Hub.

No entanto, nesta etapa, o hub continuaria enviando a informação para os dois computadores, porque ele não conseguia identificar onde os computadores estavam conectados. Mas o Switch irá retornar a informação dos dois computadores apenas para máquina que enviou inicialmente a requisição. Esse é o grande diferencial, o Switch aprende onde os computadores estão conectados. Como ele faz isso?

Falamos anteriormente que com os protocolos ARP não sabemos onde estão conectados os equipamentos. Quando o dispositivo que é procurado receber a requisição, ele retornará um número de série que está na placa de rede, chamado endereço de mac. Vamos pesquisar no Terminal qual é o número da placa do computador utilizado na gravação. Faremos isto digitando:

```
c:\Users\Alura>ipconfig /all
```

Vamos pesquisar qual é a rede Wi-fi que está sendo usada:

```
Adaptador de Rede sem Fio Wi-Fi 2:

Sufixo DNS específico de conexão. . . . . : home
Descrição . . . . . : Broadcom 802.11ac Network Adapter #2
Endereço Físico . . . . . : 80-E6-50-16-34-76
DHCP Habilitado . . . . . : Sim
Configuração Automática Habilitada. . . . . : Sim
Endereço IPv4. . . . . : 192.168.1.33(Preferencial)
Máscara de Sub-rede . . . . . : 255.255.255.0
Concessão Obtida. . . . . : quarta-feira, 14 de setembro de 2016 09:44:10
Concessão Expira. . . . . : quarta-feira, 14 de setembro de 2016 21:47:31
Gateway Padrão. . . . . : 192.168.1.1
Servidor DHCP . . . . . : 192.168.1.1
Servidores DNS. . . . . : 192.168.1.1
NetBIOS em Tcpip. . . . . : Habilitado
```

Ele indicou o número de série da minha placa de rede: 80-E6-50-16-34-76. Este é um número único que vem direto do fabricante. Quando fazemos a requisição do ARP e perguntamos quem tem um número específico de IP, na verdade estamos perguntando qual é o endereço mac da máquina com o endereço IP.

Para entender, vamos fazer um比较 com outra situação do mundo real. No Brasil, podemos ter vários tipos de documento: RG, CPF e Passaporte. Mas o passaporte pode ser utilizado em outros países, por ser internacionalmente válido. Já o RG é mais local. O endereço mac funciona mais localmente e só funciona em uma rede pequena. Já IP é uma identificação da máquina globalmente. O endereço mac está uma camada abaixo do endereço IP, mas para chegar na camada de cima precisamos passar por cada camada para chegar ao topo.

Vamos abrir o protocolo ARP e ver qual tipo de informação ele está passando:

PDU Information at Device: PC4

OSI Model Outbound PDU Details

At Device: PC4
Source: PC4
Destination: Broadcast

In Layers

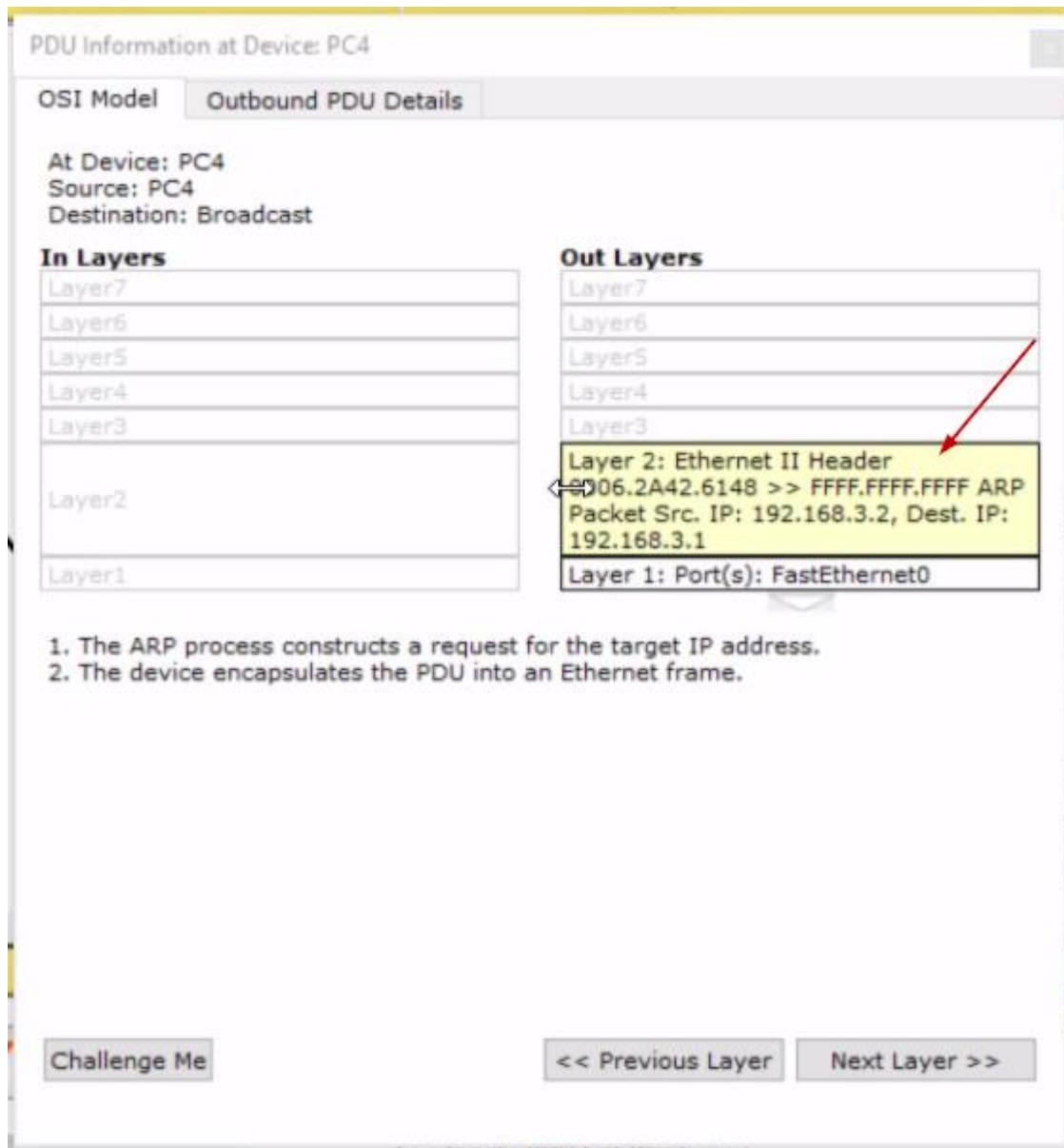
Layer7
Layer6
Layer5
Layer4
Layer3
Layer2
Layer1

Out Layers

Layer7
Layer6
Layer5
Layer4
Layer3
Layer 2: Ethernet II Header ↔ 06.2A42.6148 >> FFFF.FFFF.FFFF ARP Packet Src. IP: 192.168.3.2, Dest. IP: 192.168.3.1
Layer 1: Port(s): FastEthernet0

1. The ARP process constructs a request for the target IP address.
2. The device encapsulates the PDU into an Ethernet frame.

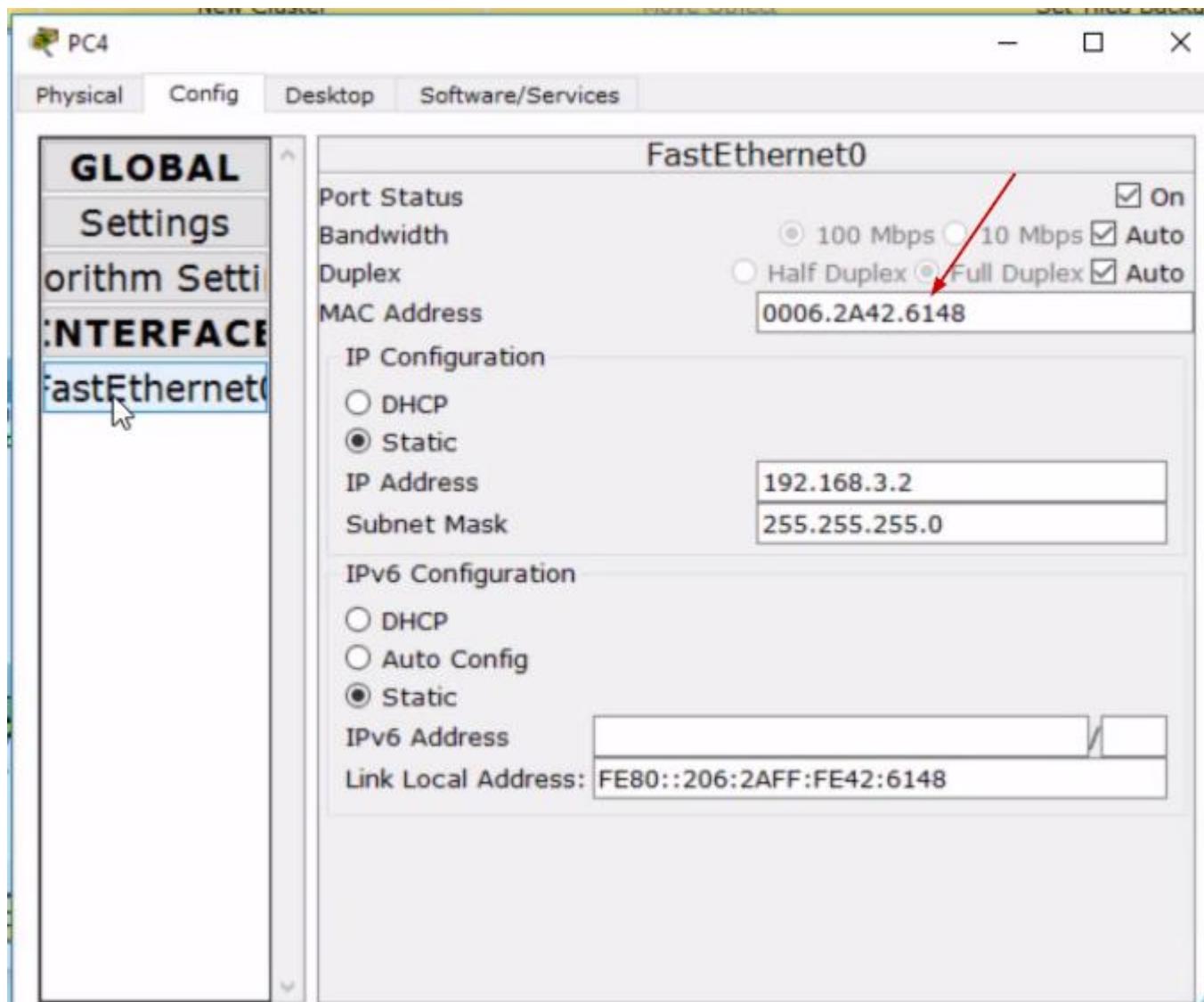
Challenge Me << Previous Layer Next Layer >>



O meu computador envia requisição para todos os outros, representado pelo FFFF.FFFF.FFFF, quem tem o IP 192.168.3.1.

No entanto, o Switch é um equipamento mais inteligente e consegue lembrar qual o mac está gravado em cada porta e conseguirá lembrar de quem ele recebeu a requisição.

Vamos analisar a aba "Config" e clicar na parte de "FastEthernt0", que é a placa do meu computador:



Vemos o endereço mac marcado. Este número aparecia no protocolo ARP.

Continuaremos analisando o protocolo ARP, dessa vez pesquisaremos o protocolo referente ao laptop.

PDU Information at Device: Switch1

OSI Model Inbound PDU Details Outbound PDU Details

At Device: Switch1
Source: PC4
Destination: Broadcast

In Layers	Out Layers
Layer7	Layer7
Layer6	Layer6
Layer5	Layer5
Layer4	Layer4
Layer3	Layer3
Layer 2: Ethernet II Header 00E0.F9E3.4C81 >> 0006.2A42.6148 ARP Packet Src. IP: 192.168.3.1, Dest. IP: 192.168.3.2	Layer 2: Ethernet II Header 00E0.F9E3.4C81 >> 0006.2A42.6148 ARP Packet Src. IP: 192.168.3.1, Dest. IP: 192.168.3.2
Layer 1: Port FastEthernet0/1	Layer 1: Port(s): FastEthernet0/2

1. FastEthernet0/1 receives the frame.

Challenge Me **<< Previous Layer** **Next Layer >>**

O protocolo diz que para o endereço MAC que fez a procura, com o final 6148 está o endereço MAC 4C81. Logo, quando o retorno do ARP voltar para o Switch, o aparelho irá perceber que a sua porta está conectada com o endereço mac 00E0.F9E3.4C81. Outro endereço será colocado na memória. Mas a informação será retornada para a máquina com o endereço mac 0006.2A42.6148, no caso, o segundo computador. O Swict já conhece quem é e sabe onde está conectado. Ele não achará mais necessário passar a informação para o terceiro computador. Esta é a grande mudança proporcionada pelo Switch: ele memoriza o endereço mac e a partir dele, identificar com qual máquina ele quer se comunicar. Isto significa uma melhoria significativa tanto na questão do tráfego como na segurança, porque a informação não corre o risco de ser recebida pelo usuário malicioso. Pelo menos, ficou mais difícil que isto aconteça.

Mas existem algumas questões que podem ser exploradas pelos usuários maliciosos. O Switch guardará a informação da localização de quem está conectado no endereço de memória. Mas se esta estiver lotada, os hackers poderão se aproveitar do fato para comprometer o Switch. Por isso, eles podem lotar a memória do Switch com diversos endereços falsos, e o aparelho já não poderá mais decifrar o endereço de cada computador e voltará a passar as informações para todas as máquinas, atuando da mesma forma que um hub. Essa ação é relativamente fácil de ser feita. O Switch traz grandes melhorias, mas também apresenta fragilidades que podem ser exploradas por hackers.

Algo que podemos fazer como prevenção desse tipo de ação maliciosa, é o que chamamos de **segurança da porta**, em que é determinado o número de endereços mac que cada porta poderá aceitar. Por exemplo, podemos definir que a porta que está conectada com o laptop só poderá aceitar o endereço mac do mesmo e

de outra máquina. Ou seja, podemos configurá-la para aceitar dois endereços mac. Caso um usuário malicioso tente se conectar com esta porta e comece a enviar vários endereços mac falsos, a porta será desabilitada. E assim, o hacker não será bem-sucedido.

O ARP é o protocolo utilizado para fazer o mapeamento entre o endereço IP e o endereço MAC de um dispositivo. Isso é necessário porque o MAC encontra-se um nível abaixo do IP e eu preciso dele para poder transmitir as informações.

Em redes de computadores, temos protocolos que possuem hierarquias diferentes. Para poder chegar até o IP que está na camada 3, eu preciso passar pelo MAC que está na camada 2, pense como se fosse escalar uma pirâmide, não dá pra chegar ao topo sem passar pelo meio dela!

Os hubs não conseguem aprender o endereço MAC das máquinas, já os Switches possuem essa função.

Quando um dispositivo quer se comunicar com outro, ele vai necessitar passar pelo Switch e ele informa dentro do pacote qual é seu endereço MAC e o Switch grava essa informação em sua memória.

Os dispositivos ao se comunicarem passam pelo Switch e ao passar pelo Switch ele grava em sua memória quem está conectado em qual porta.

Qual é uma forma de ataque usada para conseguir informações passadas no Switch destinadas a outro usuário?

Colocar vários endereços MAC falsos para “lotar” a memória do Switch e fazer com que ele atue como um Hub

Métodos usados por usuários maliciosos seria de inserir vários endereços MAC falsos para “lotar” a memória do Switch, uma vez que a memória esteja cheia, o Switch não vai conseguir definir quem está onde e ele passa a atuar como um Hub.

Como podemos nos prevenir contra esse ataque?

Configurar a opção de segurança na porta, para que assim fique limitada a receber uma quantidade máxima de endereços MAC, caso ultrapasse, a porta é desabilitada

Podemos configurar a porta do Switch para aceitar um número máximo de endereços MAC, ao ultrapassar esse limite a porta é desligada e o ataque não teria sucesso.

Mãos à obra: Switches

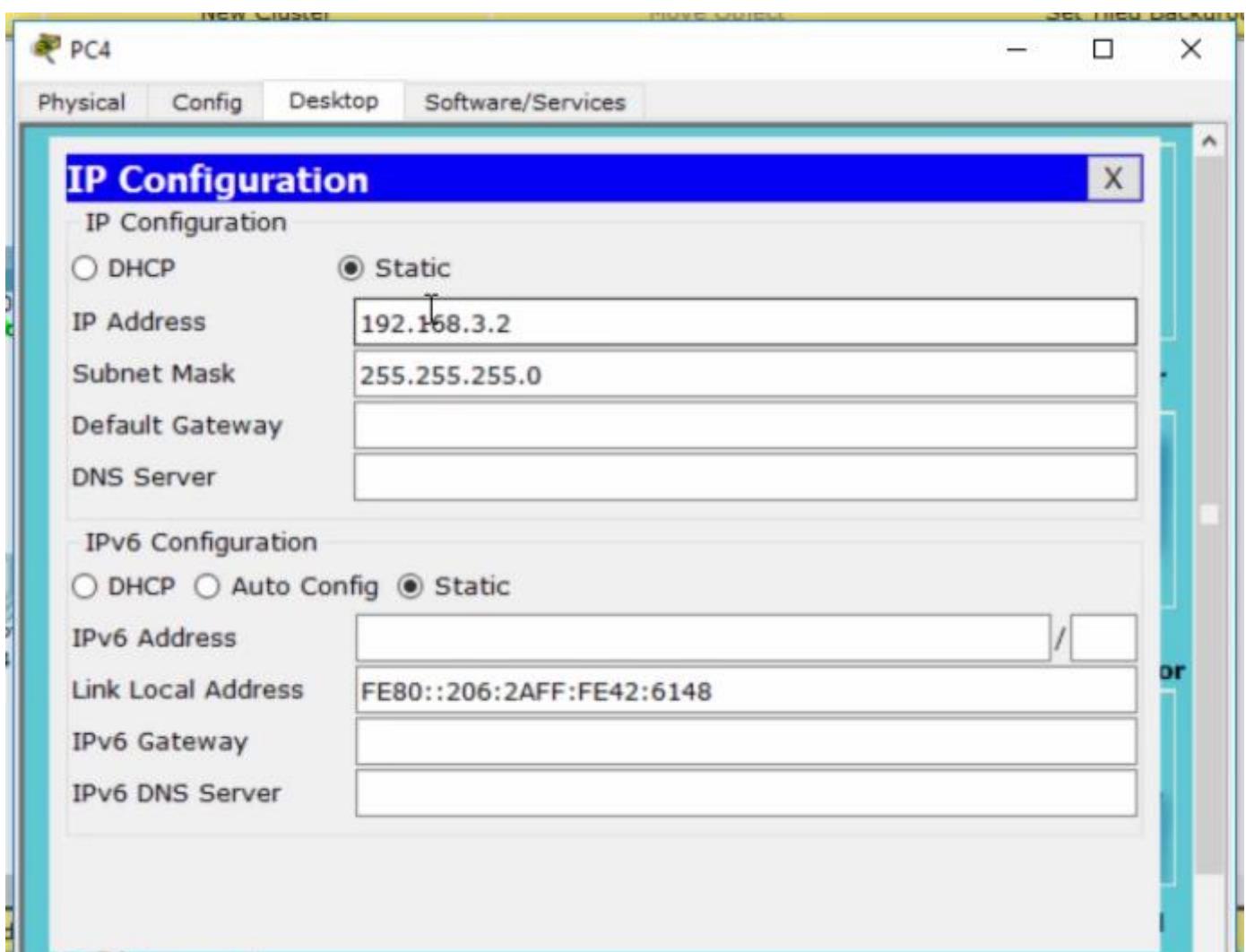
- Clique em cima do Hub e remova ele de nosso projeto pressionando o botão DELETE. No canto inferior esquerdo selecione a opção Swicthes e arraste para a área de trabalho. Posteriormente clique no ícone “Connections” e selecione a opção de cabo direto (3^a opção da esquerda para a direita).
- Clique no computador e posteriormente no Switch, a conexão poderá ser feita em qualquer porta. Depois disso no canto inferior direito troque o modo de operação de “RealTime” para “Simulation”.
- Clique em um dos computadores -> Aba Destktop -> Command prompt -> digite: ping (#ip de um dos outros dois computadores#) pressione ENTER
- Clique na aba inferior no botão “Capture/Forward” e analise que o retorno da informação volta somente para o computador que fez a requisição, isso porque o Switch consegue aprender o endereço MAC das máquinas que estão conectadas.

Máscaras de Rede

Já aprendemos como os roteadores e o Switch trabalham. Mas ainda temos algo importante para conversar. Quando vários computadores estão conectados no mesmo Switch ou no mesmo Hub, não significa que eles estão conectados na mesma rede.

Nós podemos fazer uma separação lógica de endereçamento e colocar cada computador em uma rede diferente. Mas por que faríamos isso? As máquinas podem fazer parte de diferentes setores de uma empresa e cada uma possui a sua rede, que precisa se comunicar com as outras. Na minha empresa podemos ter diferentes setores e às vezes, precisamos segmentar a rede em duas, para atender diferentes necessidades.

Primeiro ponto a se considerar é: como saberemos se o outro dispositivo está na mesma rede. Vamos analisar o segundo computador. Selecionearemos a aba "Desktop", depois em "IP configuration":



Nós só configuramos o endereço de IP, mas vemos que existe também uma "Subnet Mask" com o número 255.255.255.0. Ele surgiu automaticamente. Esta máscara de rede terá um papel crucial para descobrirmos se outra máquina está na mesma rede que a minha. Faremos esta análise em conjunto.

Endereço IP: 192.168.3.2

Máscara de rede: 255.255.255.0

Temos a máscara de rede, que dividirá o endereço IP do computador em dois grandes grupos: um referente às redes e outro às máquinas.

255 = REDE

0 = MÁQUINA (HOST)

Tudo que for 255 será referente à rede, e o que for 0 será referente ao host. Então, ele analisará o primeiro intervalo:

255 = REDE

0 = MÁQUINA (HOST)

192.168. 3 .2

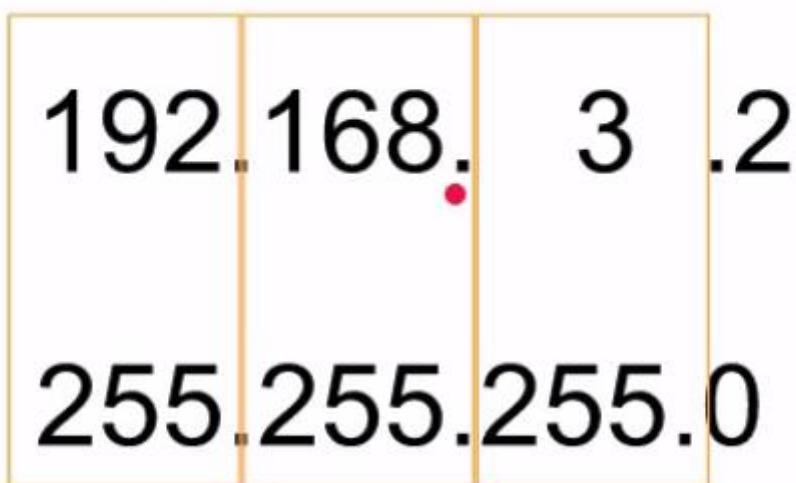
255.255.255.0

Então, será dito para o computador: "para outro dispositivo estar na mesma rede que você, ele precisará começar com o mesmo intervalo de octeto. Logo, ele deverá começar por 192"

Depois, ele passará para o outro intervalo: "se o mesmo dispositivo quiser estar na mesma rede, deverá ter o segundo octeto 168." E no terceiro octeto, ele dirá: "computador, se o dispositivo quiser estar na mesma rede, ele precisa ser igual a 3". Ou seja, a máscara de rede informa que para o dispositivo estar na mesma rede, ele precisará ter o IP começando com 192.168.3.

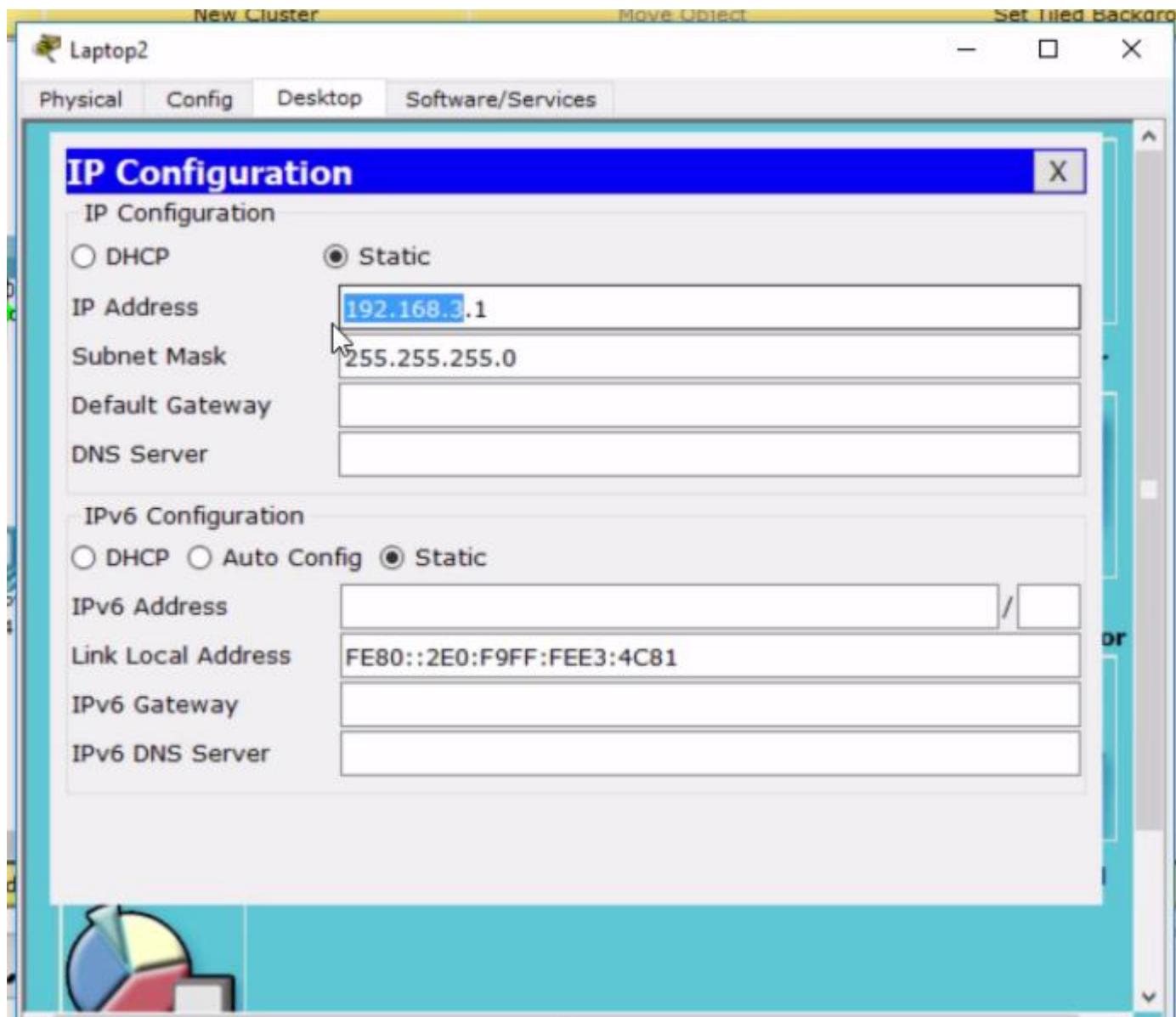
255 = REDE

0 = MÁQUINA (HOST)

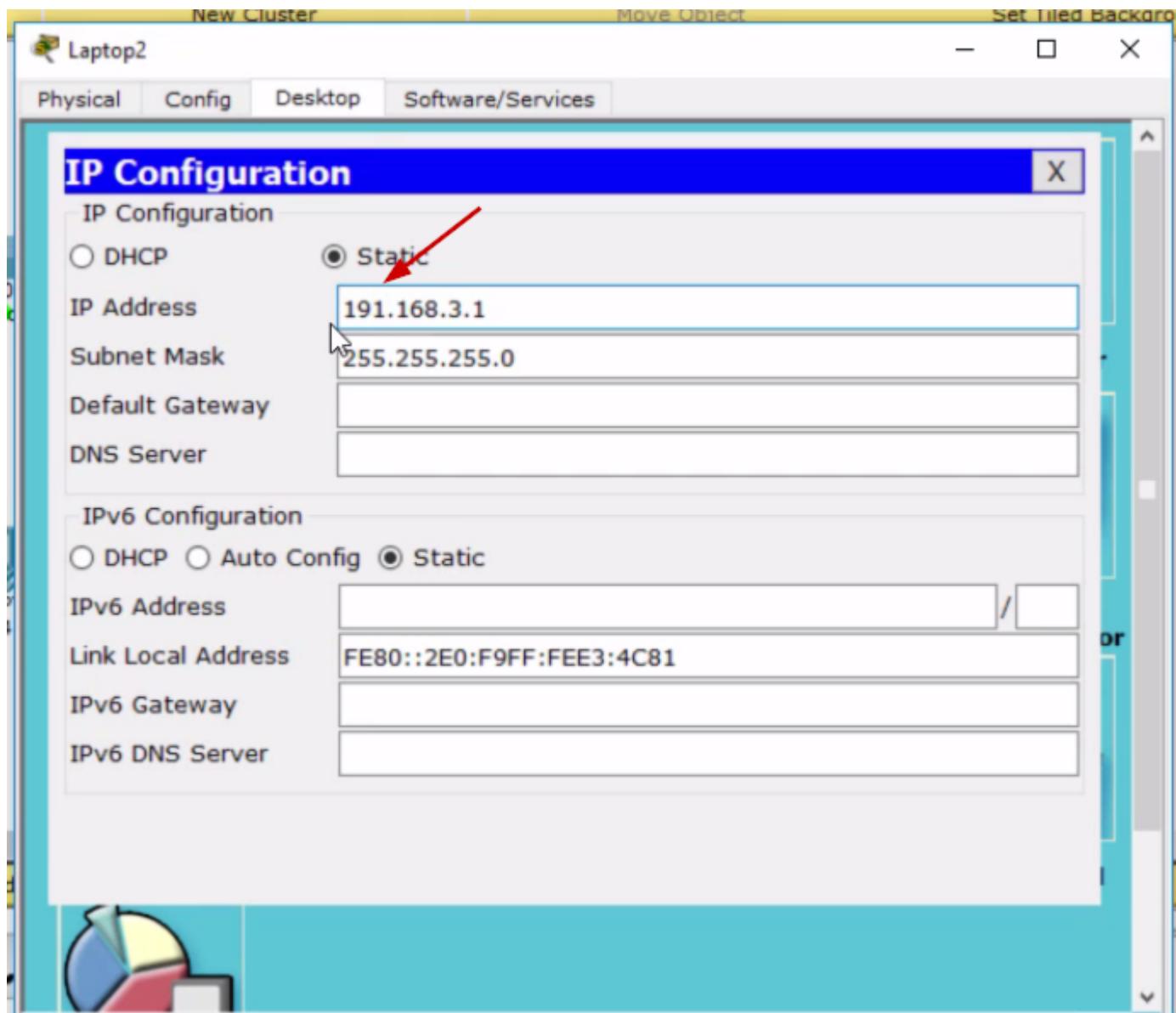


O quarto octeto ele verificará que é igual a 0 e não se importará com o valor que estiver no IP. É irrelevante o valor do quarto octeto. O que realmente importa é que ela comece com 192.168.3.

Voltaremos para o nosso projeto. Ao verificarmos, veremos que o IP dos três computadores interconectados começavam com estes números:



Veja que não foi uma coincidência que a nossa configuração tenha colocado os três intervalos iguais. O objetivo é que todas estivessem na mesma rede. Isto significa, que se alterarmos qualquer um dos três octetos, eles já não estarão na mesma rede e a comunicação entre eles já não será possível. Vamos fazer um teste, alterando o número de IP da primeira máquina. O primeiro octeto deixará de ter o valor 192 e passará a ter o valor 191.



Faremos agora, um teste de conectividade digitando:

```
ping 191.168.3.1
```

Receberemos o seguinte retorno:

```
PC>
PC>
PC>
PC>ping 191.168.3.1
Pinging 191.168.3.1 with 32 bytes of data:
```

Perguntamos na rede quem era dona do IP 191.168.3.1 e a conexão não foi estabelecida. Ninguém respondeu, porque estamos utilizando uma rede diferente. Com o hub nós só conseguimos comunicar com os computadores que estão na mesma rede.

Analisaremos o resultado:

```
PC>
PC>ping 191.168.3.1

Pinging 191.168.3.1 with 32 bytes of data:

Request timed out.
Request timed out.
Request timed out.
Request timed out.

Ping statistics for 191.168.3.1:
    Packets: Sent = 4, Received = 0, Lost = 4
(100% loss),
PC>
```

Foram enviados quatro pacotes. Também perdemos a mesma quantidade de pacotes. Ou seja, enviamos a requisição para o IP, mas pelo fato de este estar em uma rede diferente, não foi possível a conexão.

Mais adiante veremos como resolver o problema.

A máscara de rede é usada como forma de comparação para determinar se dois equipamentos estão na mesma rede. Para isso ela vai dividir o endereço IP em dois grupos, de rede e hosts (máquinas).

Esses dois dispositivos:

1- IP: 192.168.0.3 ; Máscara: 255.255.255.0

2- IP: 192.169.0.4 ; Máscara: 255.255.255.0

Estão na mesma rede?

*Não

Lembre-se, a máscara de rede está dizendo que para dois equipamentos estarem na mesma rede, os 3 primeiros octetos do IP devem ser iguais, uma vez que suas máscaras são 255.255.255.0.

Se eu tenho um endereço IP: 33.44.55.66 e máscara de rede: 255.0.0.0, qual desses endereços abaixo vai caracterizar que outro dispositivo está na mesma rede que eu?

Lembre-se: - 255 = Rede - 0 = Host

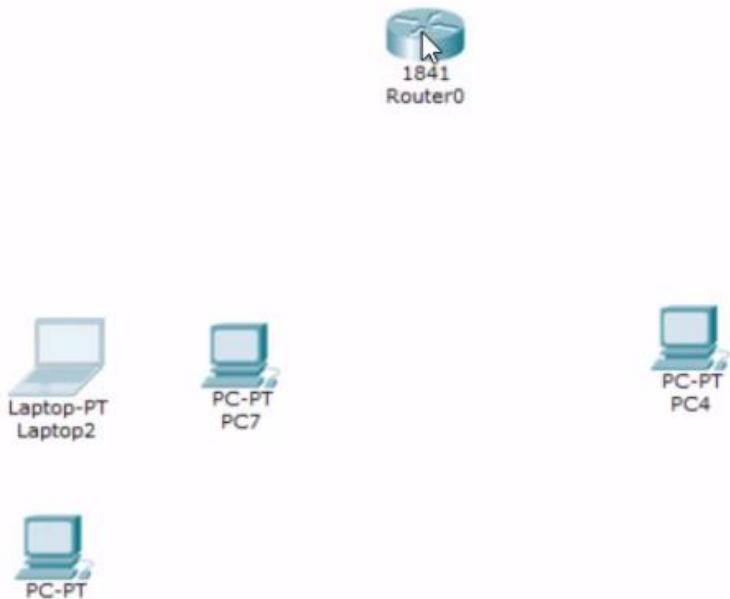
- IP: 33.255.4.3 ; Máscara: 255.0.0.0

O 1º octeto do endereço IP é 33, logo só ele importa para analisar se outro dispositivo está na mesma rede que eu, os demais são números da máquina. As outras opções começam com número diferente de 33, o que caracteriza que a máquina está em outra rede.

Roteadores

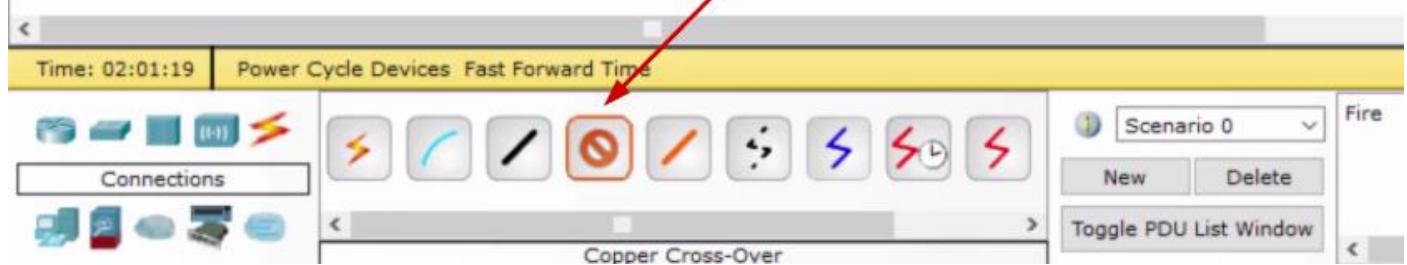
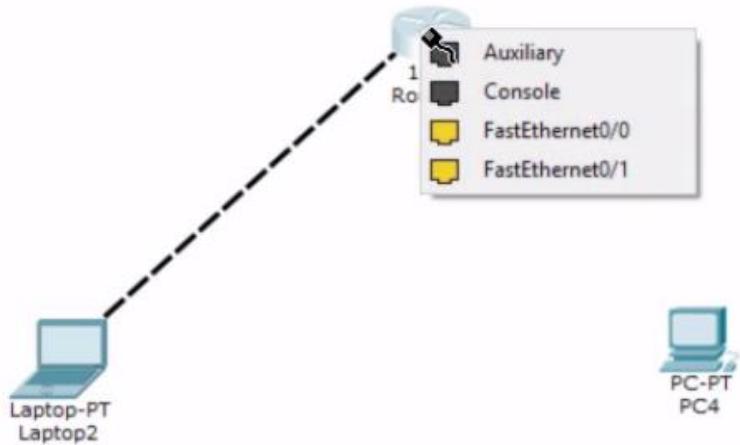
Para conseguir fazer com que os dois computadores se comuniquem, precisaremos de um equipamento de rede chamado **roteador**. A função dele será conectar computadores de redes diferentes.

No nosso projeto, deletaremos o Switch e substituiremos por um roteador ("Router") na opção de ícones de equipamentos no Packet Tracer. Excluiremos também o terceiro computador que não será mais usado no projeto.

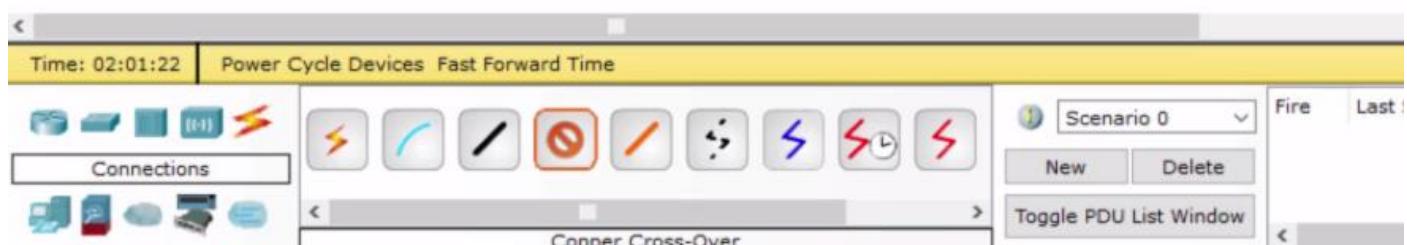
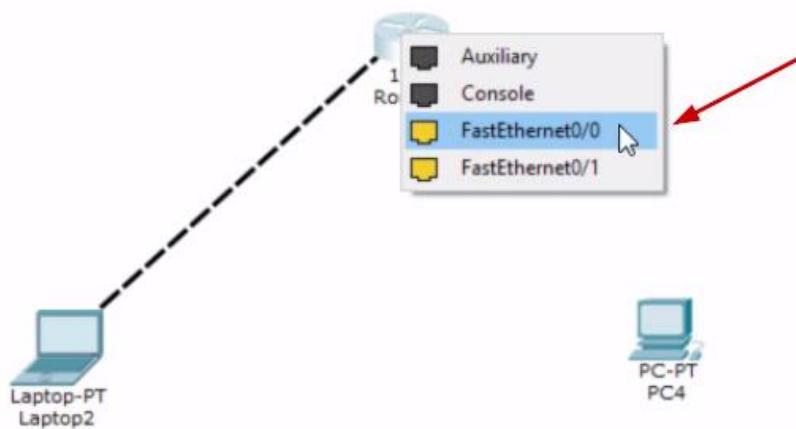


E como será feita a conexão entre o roteador e os computadores? Precisaremos primeiramente descobrir se os dois computadores são iguais. Caso eles sejam, significa que eles terão a mesma placa de rede. No exemplo, nós conectaremos um laptop e um computador com o roteador. Ou seja, não estamos conectando equipamentos iguais.

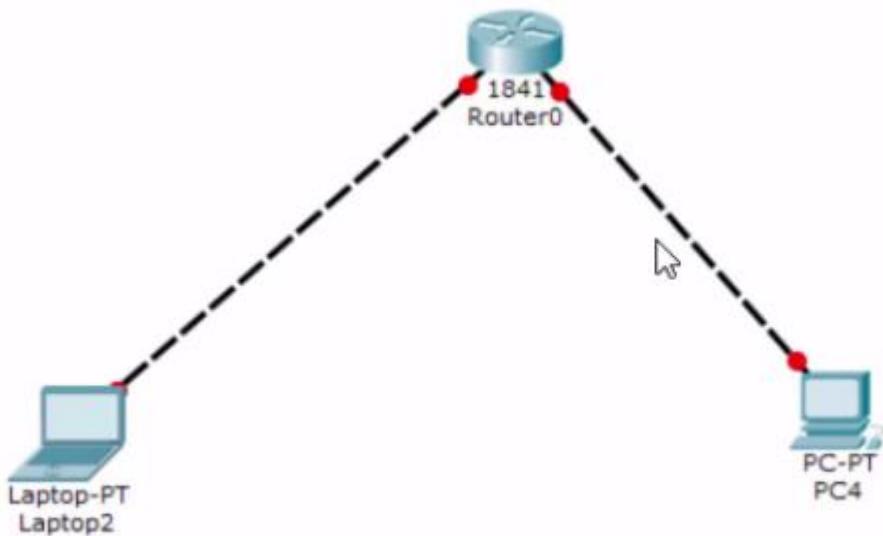
Faremos uma nova pergunta: a conexão que faremos irá explorar a totalidade que o equipamento foi projetado para fazer? Por exemplo, um computador foi projetado para se comunicar com várias máquinas. Já o roteador foi projetado para interconectar redes diferentes. Se conectarmos o laptop com um roteador, exploraremos tudo o que os dispositivos podem fazer? Não. Ele não explora. Um setor poderia ainda ter outras máquinas de um mesmo setor que não estariam conectadas com o roteador.



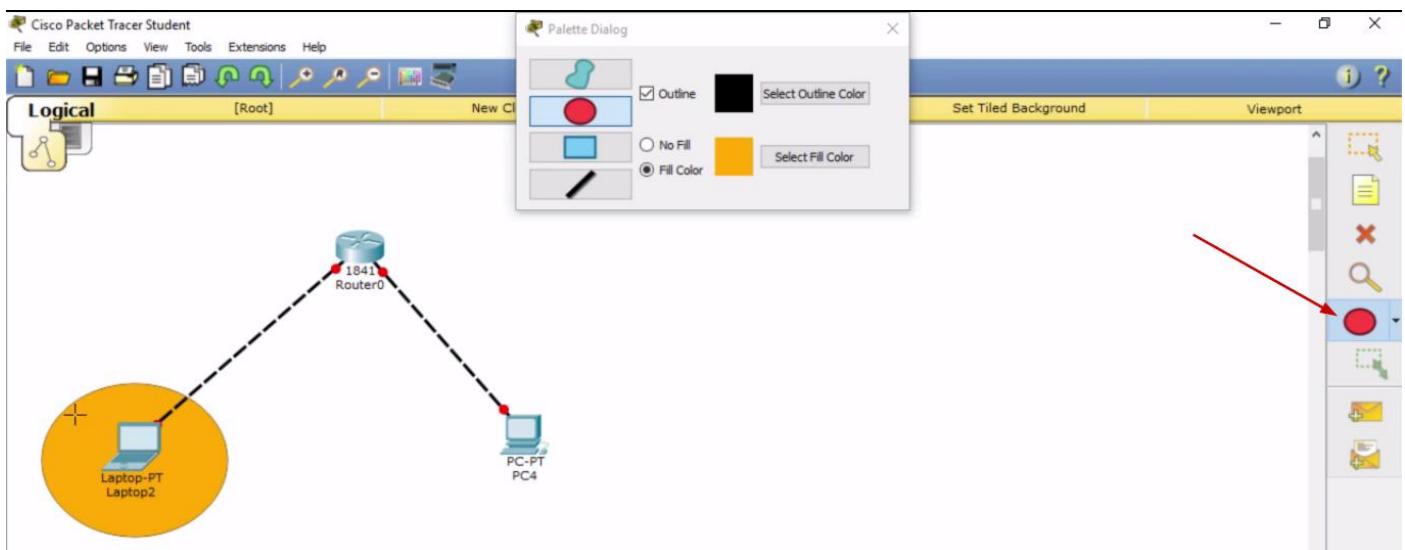
Por isso, neste caso, utilizaremos o cabo cruzado (*crossover*). Vamos adicioná-lo no projeto e remover os computadores usados rapidamente no exemplo anterior. Seleccionaremos o ícone do raio e será aberta uma lista de cabos. O correto será a quarta opção listada.



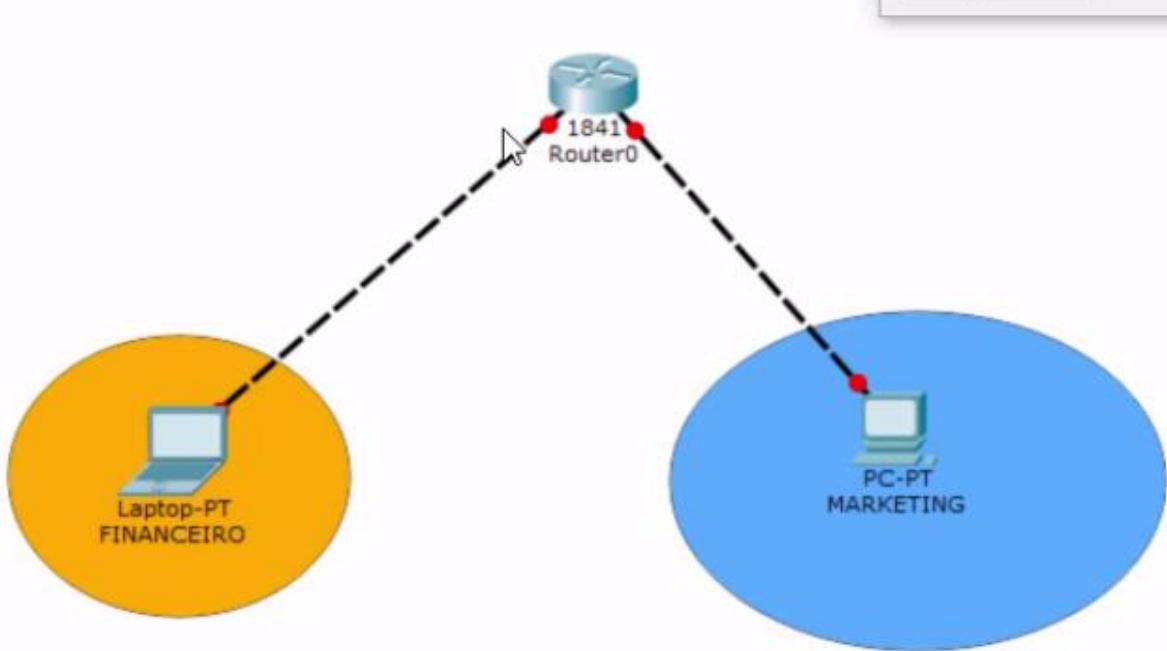
Nós colocamos na porta disponível "FastEthernet0/0". Depois, faremos a conexão entre o computador e o roteador.



Agora, criaremos a segmentação por setores da empresa. No menu da direita, selecionaremos o ícone do círculo. Será aberta uma nova janela que nos permitirá escolher a cor. Escolheremos a cor laranja e vamos adicionar o círculo ao projeto.



O círculo laranja estará representando a rede do financeiro. Em seguida, criaremos outro círculo que representará a parte de Marketing.



A instalação do projeto já foi feita, agora falta a configuração do roteador. Faremos isto logo adiante.

A função do roteador é interconectar redes encaminhando seus pacotes de dados, os Switches e hubs são usados somente para conexão na minha rede local.

Lembre-se da regra: - Dois equipamentos iguais estão interconectados? Se sim, eles tem o mesmo tipo de placa, então devo usar o cabo crossover. Se não, faço a pergunta abaixo - Dois equipamentos diferentes estão conectados? Essa conexão representa o que naturalmente o equipamento foi desenvolvido para fazer?

Por exemplo ao interconectar o computador ao hub e o computador ao switch, o computador foi feito para se comunicar com várias máquinas e o hub e switch foram feitos para interconectar diversas máquinas. Dessa forma ao conectarmos os dois, vamos estar explorando o que os dois foram fabricados para fazer naturalmente. Porém o roteador foi feito para interconectar redes, se eu coloco somente um dispositivo, não terei como inserir outros dispositivos para o roteador encaminhar os pacotes e então a totalidade de sua função não está sendo explorada. Devemos usar cabo crossover.

Configurando roteador

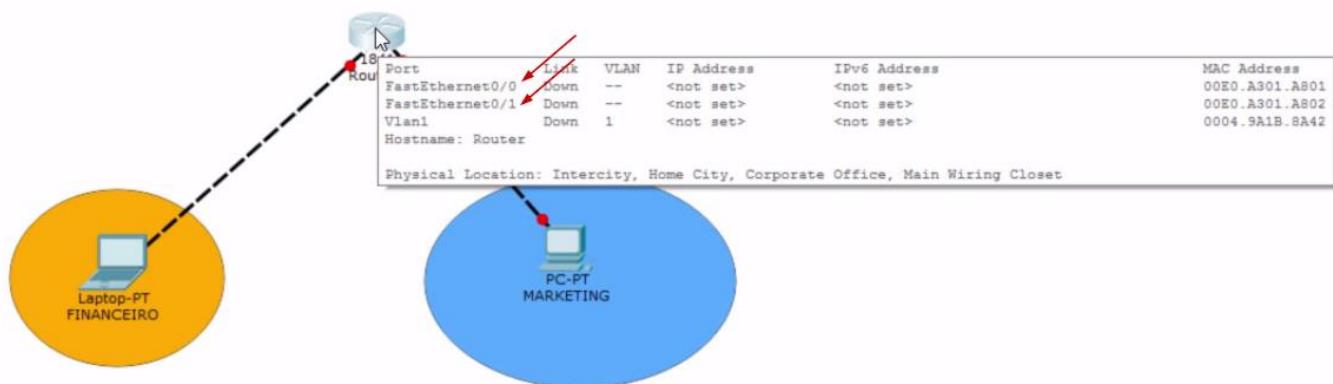
Vamos começar a configuração do roteador. Primeiramente, veremos como é o layout do roteador.



Faremos uma análise da imagem. Provavelmente, o roteador que temos nas nossas casas é bastante parecido ao da imagem. Nos dispositivos domésticos, geralmente, encontramos essas portas **amarelas** que são o Switch. Para economizar espaço, ele traz os Switch embutido.

O equipamentos da Cisco, que aparecem no Packet Tracer são focados para empresa. Por isso, ocorre a segmentação entre Switch, que conectara vários usuários, e o Roteador para mandar os usuários para uma outra rede. Ocorre uma separação nos equipamentos de empresa.

Por isso, só teremos duas portas no roteador do projeto.



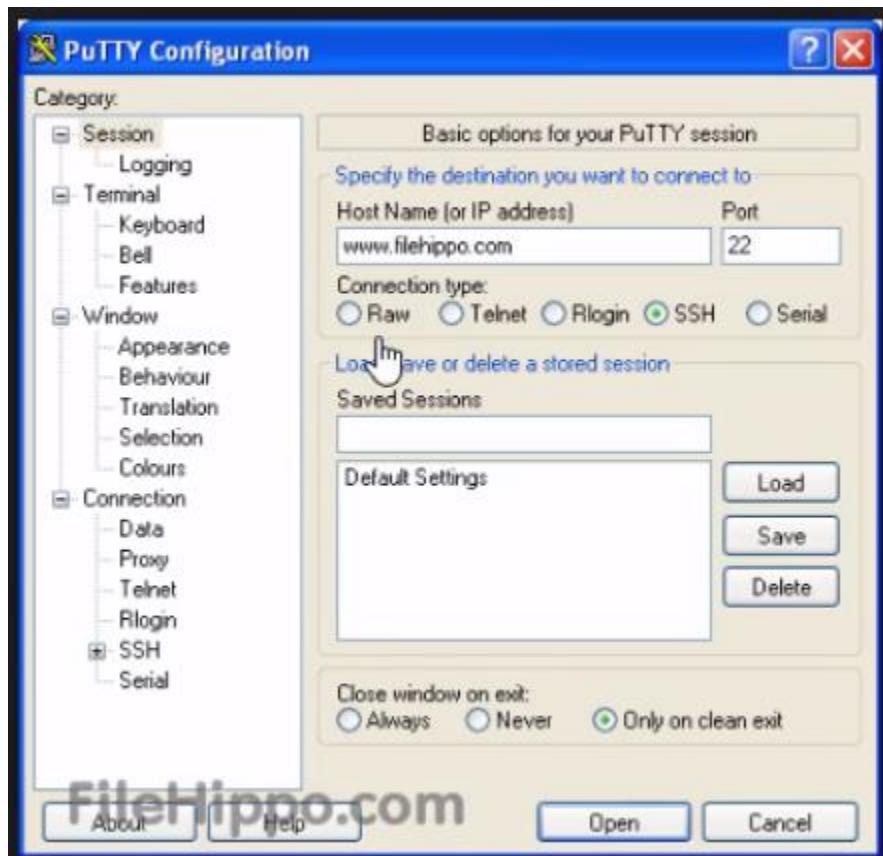
Para realizarmos a configuração dos equipamentos da Cisco, precisaremos utilizar um cabo especial: **cabo console**. Ele terá o seguinte formato:



É um cabo azul, em que uma das pontas terá o conector plástico (RJ45) e na outra, terá o conector que recebe o nome de Rs232, referente a uma porta serial (que transmitirá os bits um por vez).

A conexão real será feita com o RJ45 sendo conectado na porta de console do roteador e o Rs232 será conectado na porta do computador. No entanto, a maioria dos computadores fabricados atualmente não possuem está porta serial, elas foram substituídas pelo USB. Isto significa que precisaremos usar um adaptador para realizar a configuração do equipamento.

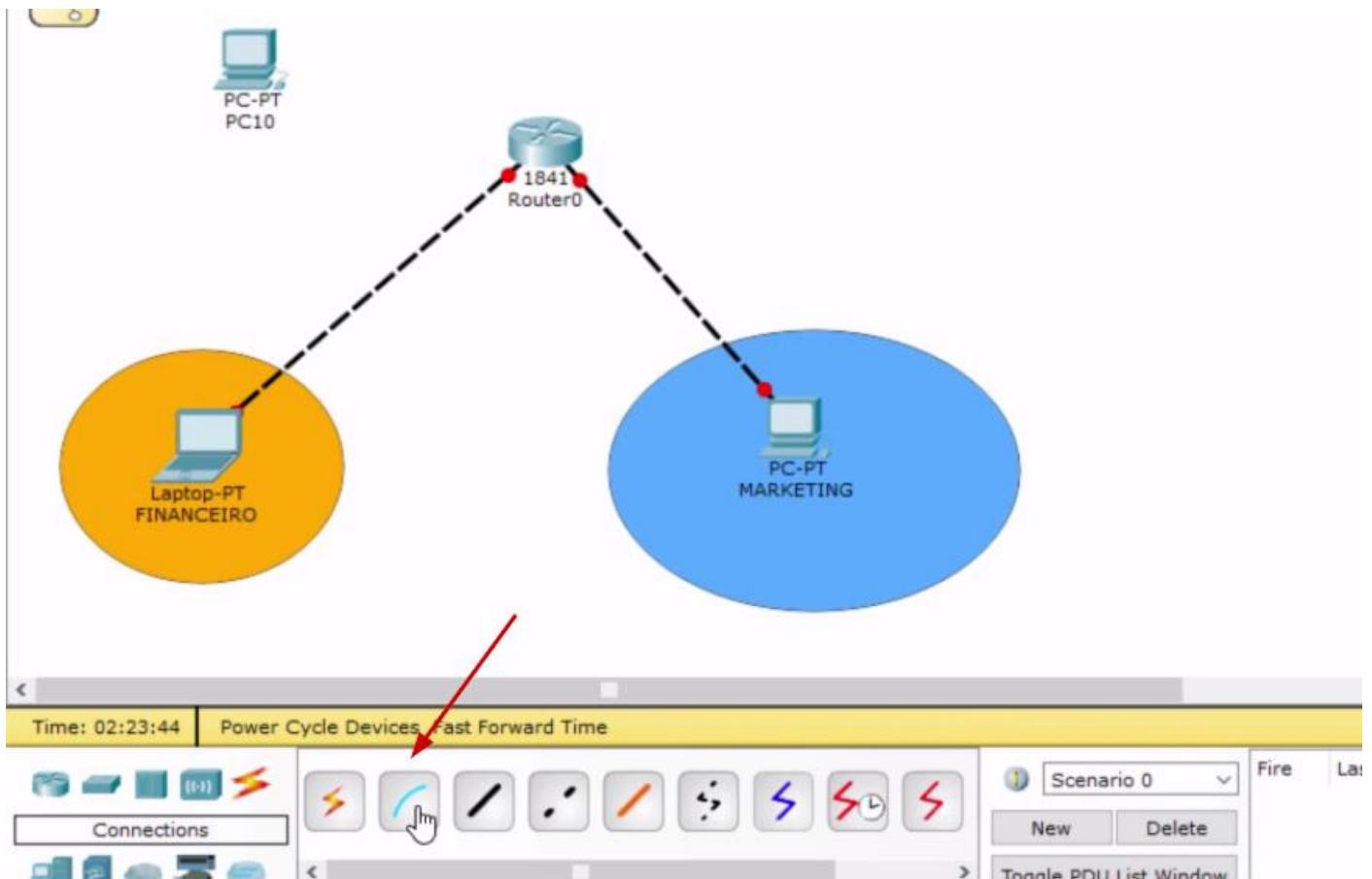
E que programa será usado para utilizar o equipamento da Cisco? Existem programas que chamamos de Terminal, o mais famoso deles se chama **PuTTY** e é bastante utilizado.



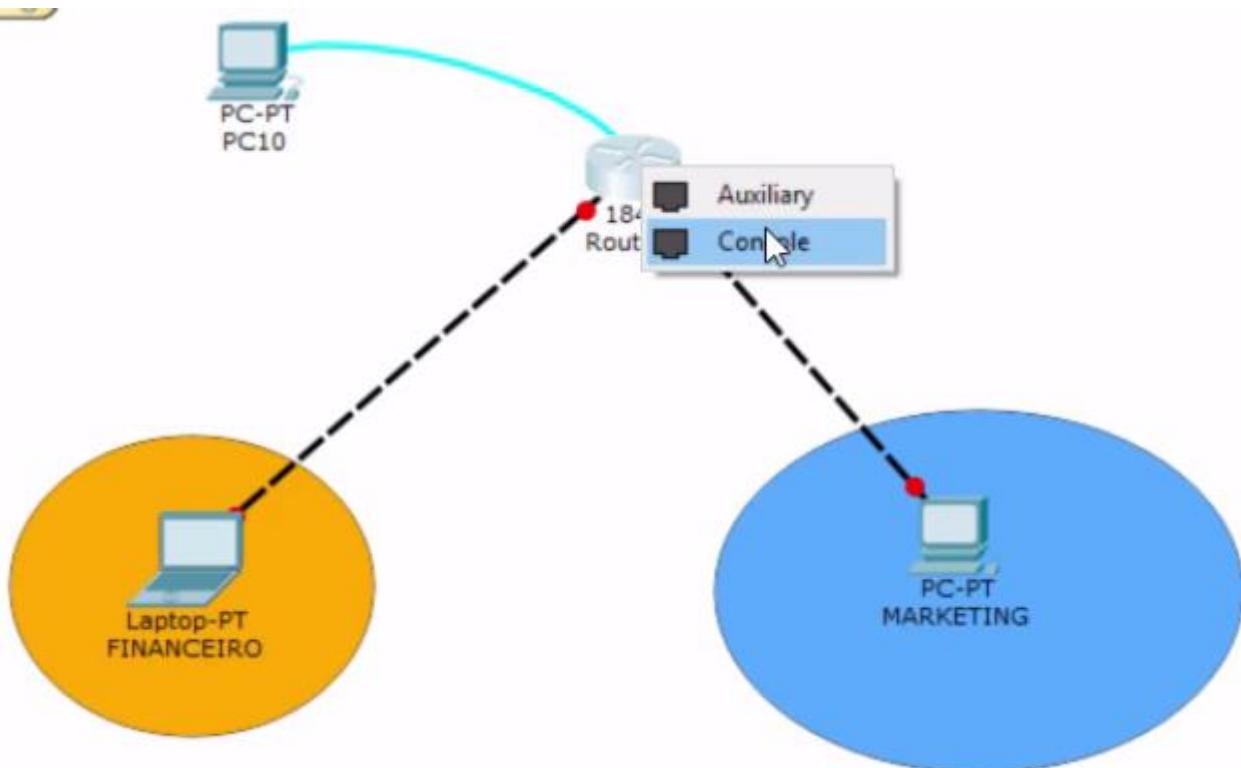
O PuTTY é muito útil quando queremos acessar remotamente um equipamento. Isto significa que podemos acessar um equipamento em outra cidade e configurá-lo. Se tiver alguém na outra localidade que permita o acesso à distância, não precisaremos nos deslocar para realizar a configuração. Por isso, ele é bastante utilizado, além de ter um interface gráfica que não é tão cansativa.

Agora, voltaremos para o nosso projeto e realizaremos a configuração.

Adicionaremos um novo computador, selecionando o ícone no meu do canto inferior esquerdo. Depois, selecionaremos um cabo para conectar a nova máquina. Após clicarmos no menu do raio, vamos escolher o segundo cabo da listagem.



Em seguida, daremos um clique no ícone do computador e selecionaremos a porta RS232, a porta serial. Conectaremos com roteador e selecionaremos "Console".



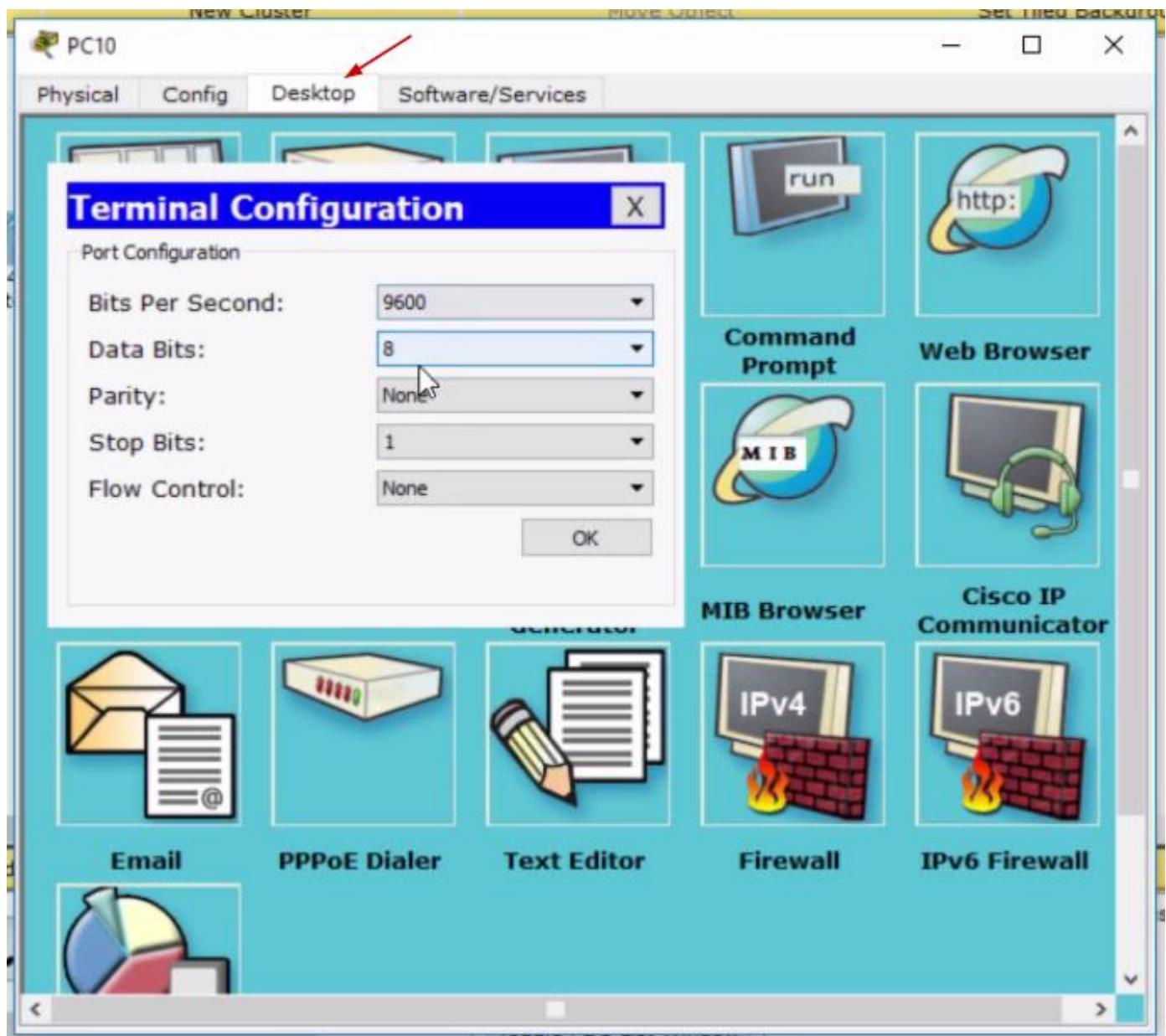
Isto o que é feito na prática: precisamos utilizar o cabo e o programa para acessar o equipamento. Mas a equipe da Cisco facilitou o nosso trabalho, em vez de precisarmos conectar os equipamentos nos projetos, podemos clicar no ícone "Router" e ir até a aba "CLI" (*Command Line Interface*), em que poderemos configurar o equipamento.

The screenshot shows a Cisco Router0 interface with three tabs: Physical, Config, and CLI. A red arrow points to the CLI tab. The main window displays the IOS Command Line Interface with the following text:

```
Cisco 1841 (revision 5.0) with 114688K/16384K bytes  
of memory.  
Processor board ID FTX0947Z18E  
M860 processor: part number 0, mask 49  
2 FastEthernet/IEEE 802.3 interface(s)  
191K bytes of NVRAM.  
63488K bytes of ATA CompactFlash (Read/Write)  
Cisco IOS Software, 1841 Software (C1841-  
ADVIPSERVICESK9-M), Version 12.4(15)T1, RELEASE  
SOFTWARE (fc2)  
Technical Support: http://www.cisco.com/techsupport  
Copyright (c) 1986-2007 by Cisco Systems, Inc.  
Compiled Wed 18-Jul-07 04:52 by pt_team
```

Below this, it says "---- System Configuration Dialog ----". At the bottom, there is a question "Continue with configuration dialog? [yes/no]: |" and two buttons: "Copy" and "Paste".

Mas precisaríamos fazer a conexão via computador na prática. Para isto, clicaremos no computador, depois, seguiremos até a aba "Desktop" e selecionaremos o Terminal.

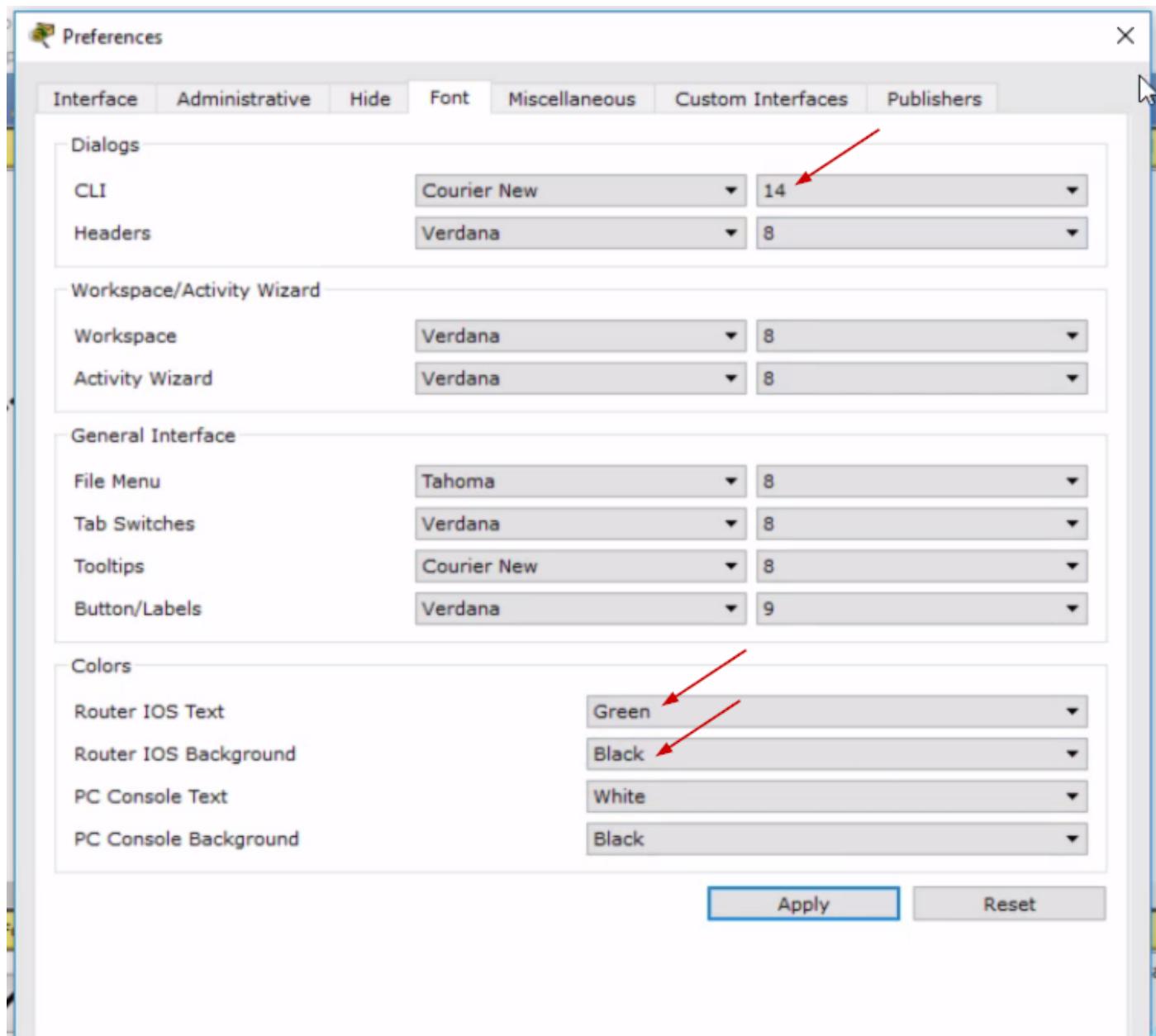


No Terminal, ele perguntará como queremos conectar com o roteador. Nós deixaremos as velocidades padrões. Receberemos as mesmas informações. A partir de agora, faremos as configurações clicando diretamente no roteador. Mas é possível realizar a ação ao clicarmos no computador.

Lembre-se: podemos fazer a configuração dando um clique duplo no roteador apenas no Packet Tracer. Na prática, precisaremos fazer a configuração real por meio do computador.

Como trabalharemos diretamente no roteador, vamos apagar o computador.

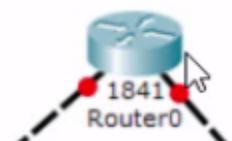
É possível configurar a tela do CLI, caso você queira que ela esteja como é mostrado no curso. Basta seguir o seguinte caminho: Options -> Preferences -> Font. Serão abertas algumas opções, em que é possível determinar o tamanho e a cor da fonte, além da cor de fundo da tela.



Na aba CLI é possível realizar a configuração do equipamento da Cisco. Nossa objetivo é estabelecer a conexão entre o setor Financeiro e o Marketing, que estão em redes diferentes no projeto.

O Financeiro terá o IP 191.168.3.1, enquanto o Marketing terá o IP 192.168.3.2. Nós iremos estabelecer a comunicação entre eles.

A porta do roteador aparecerá com a cor vermelha, porque elas são desabilitadas por padrão.



Então, a primeira coisa que faremos é habilitar as portas. Na parte de configuração eles perguntam se queremos um **diálogo** (*Continue with configuration dialog?*). Ele será feito passo a passo, e pode ser demorado. Como nós queremos uma configuração simples, responderemos "não".

```
--- System Configuration Dialog ---  
Continue with configuration dialog? [yes/no]: no
```

A tela começará a aparecer no primeiro modo de operação. O Router> indicará o que chamamos de modo usuário. Quem acessá-lo, só poderá fazer algumas configurações básicas da plataforma. Ele não poderá configurar nada efetivamente, por uma questão de segurança.

Para sabermos quais configurações são possíveis de serem realizadas no modo usuário, digitaremos o ?:

```
Router>?
```

```
IOS Command Line Interface  
Continue with configuration dialog? [yes/no]: no  
Press RETURN to get started!  
  
Router>  
Router>?  
Exec commands:  
  <1-99>      Session number to resume  
  connect      Open a terminal connection  
  disable      Turn off privileged commands  
  disconnect   Disconnect an existing network connection  
  enable       Turn on privileged commands  
  exit         Exit from the EXEC  
  logout       Exit from the EXEC  
  ping         Send echo messages  
  resume       Resume an active network connection  
  show         Show running system information  
  ssh          Open a secure shell client connection  
  telnet       Open a telnet connection  
  terminal     Set terminal line parameters  
  traceroute   Trace route to destination  
Router>
```

O comando ? poderá ser utilizado em qualquer terminal da Cisco. Podemos usá-lo com outros comandos, como enable por exemplo.

```
Router>enable ?
```

E ele retornará tudo que ainda pode ser feito com o enable. O sinal de interrogação ? nos auxilia durante toda a etapa da escrita do código.

```
Router>enable ?  
  <0-15>  Enable level  
  view    Set into the existing view  
  <cr>  
Router>enable |
```

Comentamos sobre o modo usuário. O que teremos que fazer se quisermos aumentar o usuário para realizarmos a configuração? Para isto digitaremos enable apenas.

```
Router>enable  
Router#
```

Depois do Router, ele deixará de ser seguido pelo símbolo > e passará a usar a #, que indica o modo privilegiado. Ainda não poderemos configurar o equipamento, mas se usarmos novamente a ?, ele nos retornará uma lista de visualizações do que chamamos de **reparo de problemas**.

IOS Command Line Interface

```
<cr>  
Router>enable  
Router#? |  
Exec commands:  
<1-99> Session number to resume  
auto Exec level Automation  
clear Reset functions  
clock Manage the system clock  
configure Enter configuration mode  
connect Open a terminal connection  
copy Copy from one file to another  
debug Debugging functions (see also 'undebug')  
delete Delete a file  
dir List files on a filesystem  
disable Turn off privileged commands  
disconnect Disconnect an existing network connection  
enable Turn on privileged commands  
erase Erase a filesystem  
exit Exit from the EXEC  
logout Exit from the EXEC  
mkdir Create new directory  
more Display the contents of a file  
no Disable debugging informations  
ping Send echo messages  
reload Halt and perform a cold restart  
--More-- |
```

Assim conseguimos verificar possíveis problemas do equipamento. Observe que no fim da tela aparece o More indicando que a lista ainda possui mais itens. Para ver as demais, podemos clicar em "Enter" (para vermos uma de cada vez) ou pressionar a barra de espaço e todas serão mostradas de uma vez.

Já que estamos no modo privilégio, entraremos na aba de configuração. Digitaremos `configure terminal`.

```
Router#configure terminal
```

Observe que agora o modo de operação mudou para configurarmos o computador.

```
Router#configure terminal  
Enter configuration commands, one per line. End with CNTL/Z.  
Router(config)#
```

Podemos visualizar o config. Em seguida, começaremos a habilitar as portas. Habilitaremos a porta "FastEthernet 0/0". Escreveremos isso na aba CLI:

```
Router(config)#interface fastEthernet 0/0
```

Ao escrever um número mínimo de caracteres, como `fast` por exemplo, ele completará automaticamente `fastEthernet`. Quando pressionarmos "Enter", ele já subirá o privilégio:

```
Router(config-if) #
```

Agora, nós estamos configurando a interface. Nós iremos habilitá-la adicionando no shutdown.

```
Router(config-if) #no shutdown
```

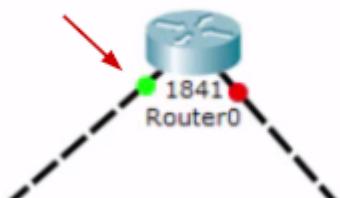
A porta será habilitada.

```
Router(config)#interface fast
Router(config)#interface fastEthernet 0/0
Router(config-if)#no shutdown

Router(config-if)#
%LINK-5-CHANGED: Interface FastEthernet0/0, changed
state to up

%LINEPROTO-5-UPDOWN: Line protocol on Interface
FastEthernet0/0, changed state to up
```

E uma das luzes do computador já ficará verde.



Vamos sair da configuração desta porta digitando:

```
Router(config-if)#exit
```

E começaremos a habilitar a porta fastEthernet 0/1:

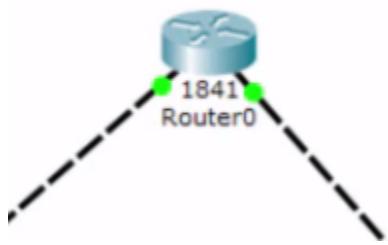
```
Router(config)#interface fastEthernet 0/1
Router(config)#no shutdown
```

```
Router(config-if)#exit
Router(config)#interface fast
Router(config)#interface fastEthernet 0/1
Router(config-if)#no shut
Router(config-if)#no shutdown

Router(config-if)#
%LINK-5-CHANGED: Interface FastEthernet0/1, changed
state to up

%LINEPROTO-5-UPDOWN: Line protocol on Interface
FastEthernet0/1, changed state to up
|
```

Agora, as duas portas estão configuradas.



Precisaremos ainda configurar o endereçamento IP que cada uma das portas receberá, para podermos fazer esta transição da rede do Financeiro para a rede do Marketing. Para isto, digitaremos o `ip ?` na aba CLI:

```
Router(config-if)#ip ?
```

Usamos a `?` para recebermos auxilio no processo.

IOS Command Line Interface

```
FastEthernet0/1, changed state to up

Router(config-if)# ip ? ↗
  access-group          Specify access control for
  packets
  address               Set the IP address of an
  interface
  authentication        authentication subcommands
  flow                  NetFlow Related commands
  hello-interval       Configures IP-EIGRP hello
  interval
  helper-address        Specify a destination address
  for UDP broadcasts
  inspect
  ips
  mtu
Unit
  nat                  NAT interface commands
  ospf
  proxy-arp            Enable proxy ARP
  split-horizon         Perform split horizon
  summary-address       Perform address summarization
  virtual-reassembly   Virtual Reassembly
Router(config-if)# ip |
```

Vemos quais opções ele permite. Em seguida, digitaremos address ?.

```
Router(config-if)# ip addr
Router(config-if)# ip address ?
  A.B.C.D  IP address
  dhcp      IP Address negotiated via DHCP
Router(config-if)# ip address |
```

Ele nos informa que devemos configurar um IP estático ou a configuração DHCP - em que uma máquina nos entregará os IPs. Como nós não temos a máquina, iremos adicionar o estático manualmente. O IP do Marketing é 192.168.3.2, mas para o roteador, iremos configurar um IP que terá o último octeto com o valor diferente: 192.168.3.5. Mas os dois estarão na mesma rede. Se digitarmos o ? novamente, ele dirá que falta informar a máscara de rede relacionada ao IP. Por isso, adicionaremos 255.255.255.0.

```
Router(config-if)# ip address 192.168.3.5 255.255.255.0
```

```
Router(config-if)#ip address ?
  A.B.C.D  IP address
  dhcp      IP Address negotiated via DHCP
Router(config-if)#ip address 192.168.3.5 ?
  A.B.C.D  IP subnet mask
Router(config-if)#ip address 192.168.3.5 255.255.255.0
Router(config-if)#[
```

A configuração do IP dessa rede já foi estabelecida. Vamos fazer um teste de conectividade.

Apertaremos o "control+Z" para sair da aba de configuração da internet FastEthernet 0/1 e depois, digitaremos ping.

```
Router#ping 192.168.3.2
```

```
Router#
Router#ping 192.168.3.2

Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 192.168.3.2,
timeout is 2 seconds:
.!!!!!
Success rate is 80 percent (4/5), round-trip
min/avg/max = 0/5/22 ms

Router#
```

A requisição teve sucesso, de cinco pacotes enviados, quatro retornaram. Isto significa que conseguimos nos comunicar com o computador da rede de Marketing.

Faremos o mesmo processo de configuração para o computador do Financeiro.

Entraremos na configuração do Terminal.

```
Router#configure Terminal
```

```
Router#config
Router#configure term
Router#configure terminal
Enter configuration commands, one per line. End
with CNTL/Z.
Router(config)#
```

Digitaremos interface fa0/0.

```
Router(config)#interface fa0/0
```

Depois, adicionaremos ip address e o endereçamento IP deve estar na rede do Financeiro. Seguiremos a máscara de rede, e o IP terá apenas o último octeto diferente: 191.168.3.7.

```
Router(config-if) address 191.168.3.7 ?
```

Com o ? descobrimos o que falta preencher.

```
Router(config)#interface fa0/0
Router(config-if)#ip add
Router(config-if)#ip address 191.168.3.7 ?
  A.B.C.D  IP subnet mask
Router(config-if)#ip address 191.168.3.7
```



Ele pediu para adicionarmos a máscara de subnet, como fizemos anteriormente.

```
Router(config-if) ip address 191.168.3.7 255.255.255.0
```

Usaremos o comando "Control+Z" para voltarmos ao modo inicial. E logo, testaremos a conectividade usando o ping.

```
Router#ping 191.168.3.1
```

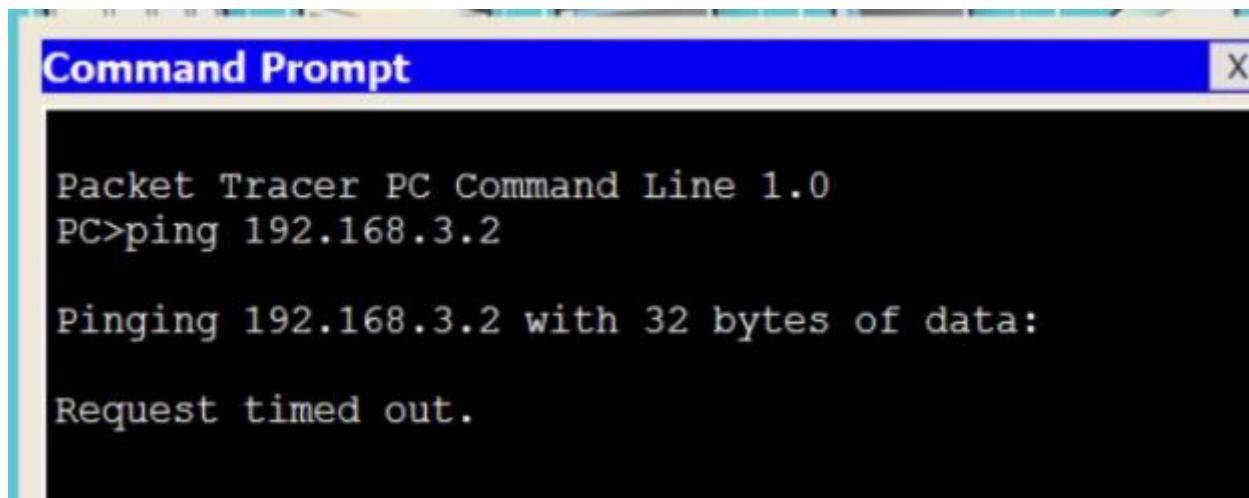
```
Router#
Router#ping 191.168.3.1

Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 191.168.3.1,
timeout is 2 seconds:
.!!!!
Success rate is 80 percent (4/5), round-trip
min/avg/max = 0/0/0 ms
```

```
Router#
```

O roteador consegue pingar o computador tanto da rede do Marketing como a do Financeiro. Isto significa que os dois computadores podem se comunicar diretamente. Vamos testar. Clicaremos no computador do Financeiro, na janela que será aberta, vamos na aba "Desktop" e depois, em "Command Prompt". Na linha de comando, adicionaremos o ping.

```
PC>ping 192.168.3.2
```



No entanto, ninguém respondeu a nossa requisição. Vamos continuar a configuração e entender o porquê de isso acontecer.

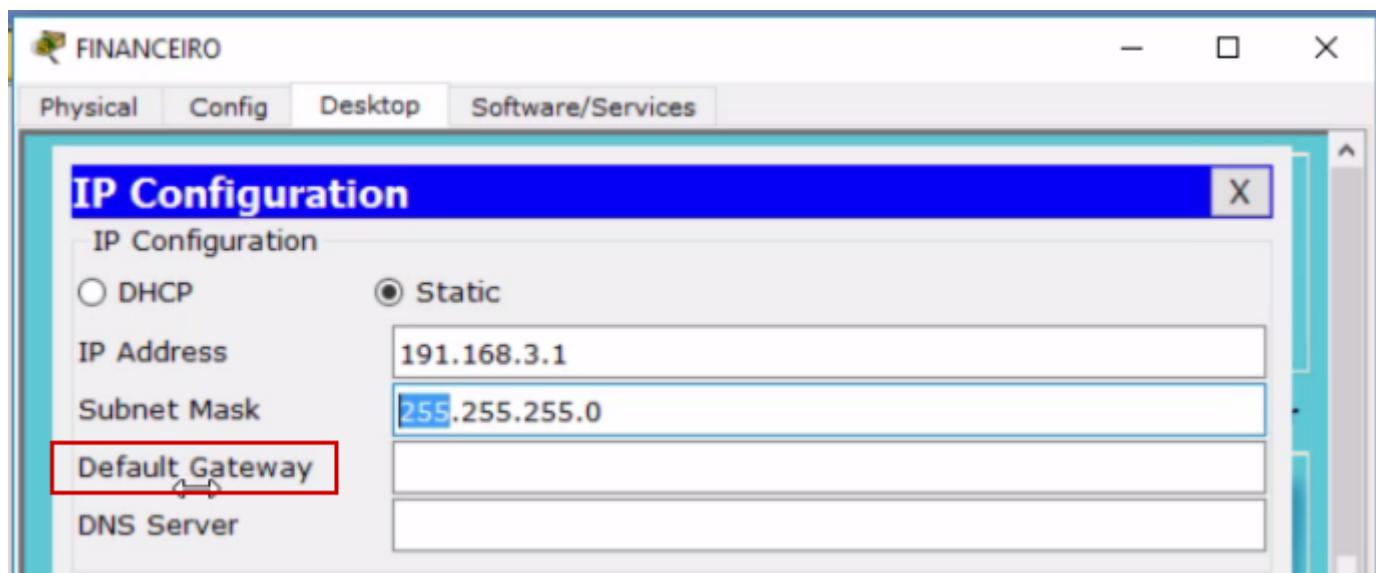
Portão de saída

Nós tentamos fazer o teste de comunicação entre o Financeiro e o Marketing, mas ainda não tivemos sucesso.

Quando usamos o ping para uma máquina se comunicar com a outra, ele comparou o IP de destino 192.168.3.2 com o do Financeiro 191.168.3.1. Como a nossa máscara de rede é 255.255.255.0, ele perceberá que os quatro primeiros octetos dos IPs não são iguais. As máquinas estão em redes diferentes. Mas agora, o nosso computador não sabe para onde enviar a informação. Ele sabe que queremos acessar um dispositivo que não está na mesma rede. Então, precisaremos indicar para onde queremos que a informação seja enviada.

Diremos para o computador: "caso você precise se comunicar com um computador em uma rede diferente, você enviará para o roteador. Afinal, a função do roteador é conectar redes diferentes." O computador passará o problema para o roteador, que terá que encontrar uma forma de enviar a informação adiante.

Para isto, preencheremos um novo campo na "IP Configuration".



Traduzido para o português, *Default Gateway* significa **portão padrão** ou seja, trata-se do portão de saída da rede - que no nosso caso, será o roteador. Usaremos o endereço IP configurado em cada porto do roteador. Para descobrirmos o número, na linha de comando digitaremos o seguinte:

```
Router>enable  
router#show ip interface brief
```

O `brief` indicará que queremos um resumo das interfaces IPs que ele possui.

Router0

Physical Config CLI

IOS Command Line Interface

```
Router>
Router>
Router>ENABLE
Router#show ip interface brief
Interface          IP-Address      OK? Method
Status            Protocol

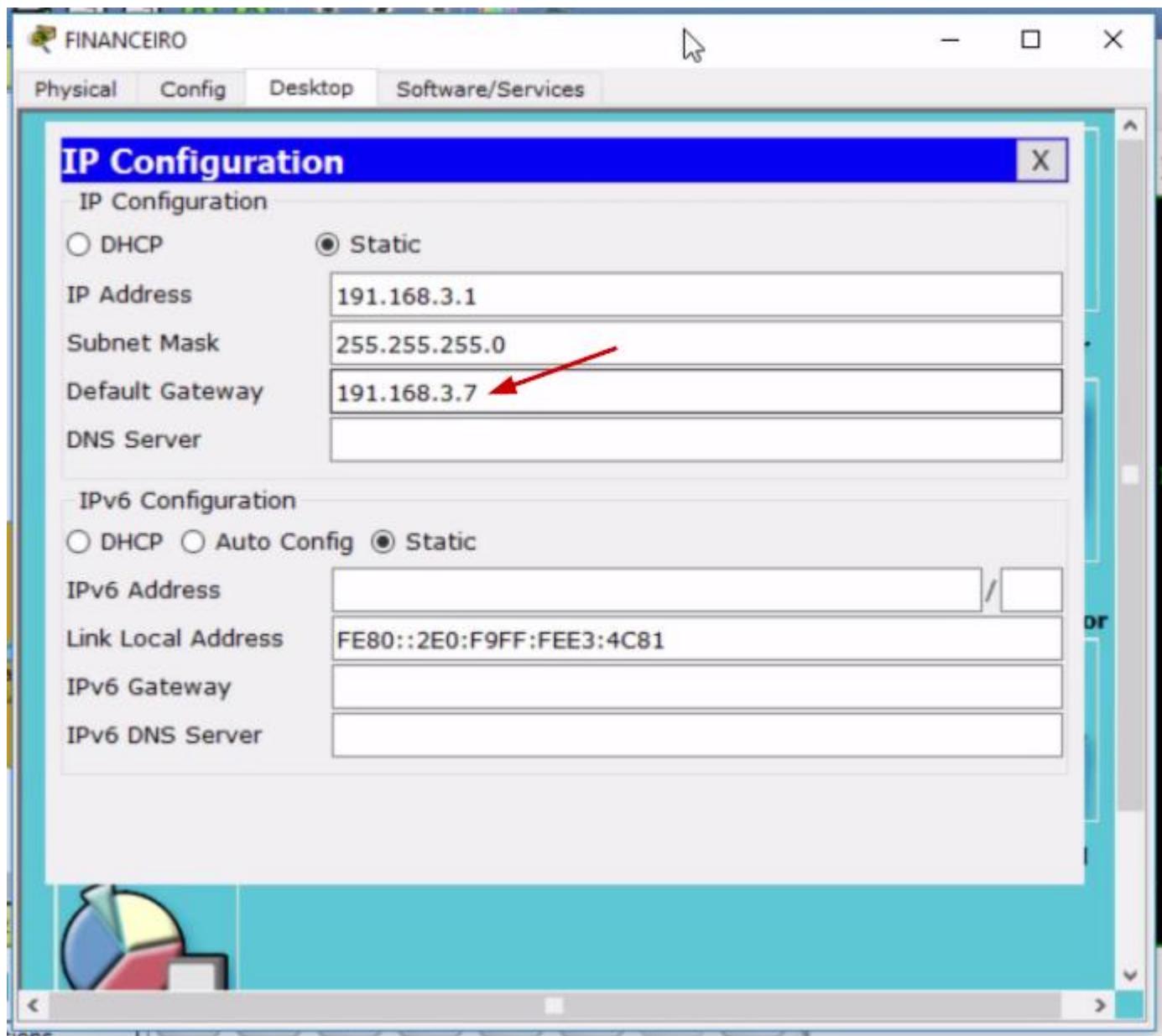
FastEthernet0/0    191.168.3.7    YES manual up
up

FastEthernet0/1    192.168.3.5    YES manual up
up

Vlan1             unassigned     YES unset
administratively down down
Router#
```

Copy Paste

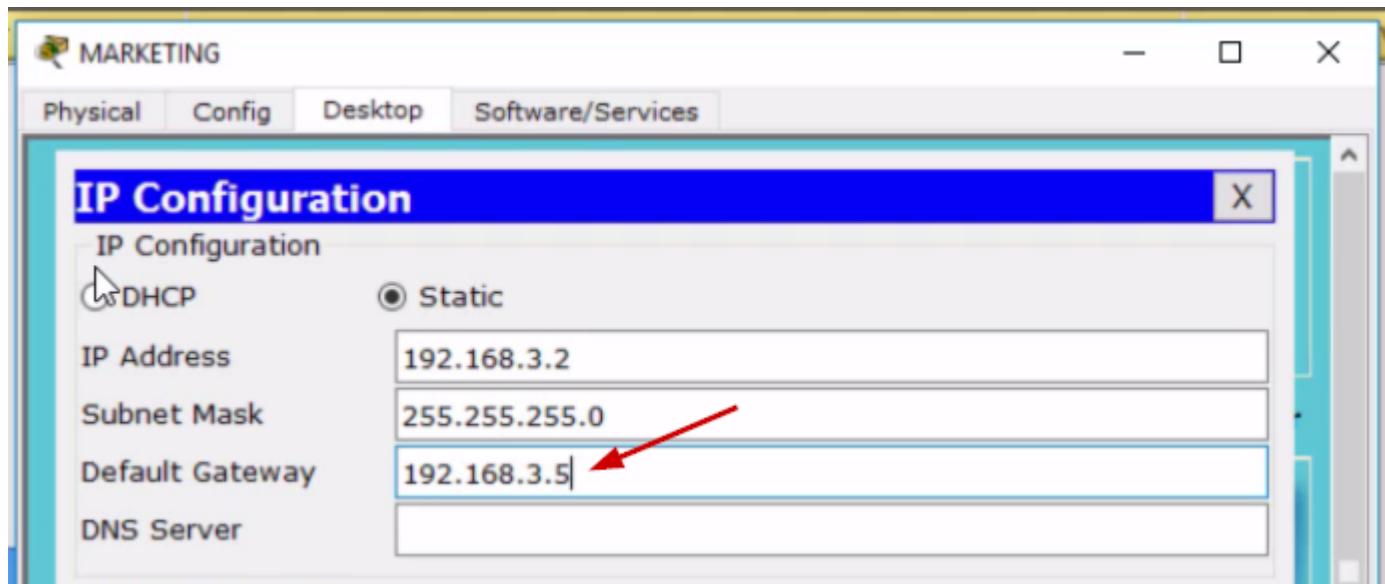
Dois IPs foram configurados: 191.168.3.7 é a configuração do IP que fizemos na porta conectada com o laptop, enquanto o 192.168.3.5, é o IP configurado com a porta da outra máquina. Já sabemos qual número preencher no campo de Default Gateway.



Agora, a informação consegue sair da rede. Vamos fazer um novo teste usando o ping. No "Command Prompt", digitaremos o seguinte:

```
PC>ping 192.168.3.2
```

Mas ainda não teremos sucesso. Lembraremos como o ping funciona: dentro dele, temos o protocolo ICMP - que funciona como um telefone e verificará se o outro computador está ativo, permitindo a comunicação entre os dois. A informação consegue sair do computador do Financeiro, mas o computador do Marketing não sabe como retornar a informação. Teremos que indicar para ele também qual será o portão de saída.



Informamos para o computador do Marketing qual era o portão de saída.

Faremos um novo teste de conectividade, desta vez, os dois computadores foram configurados para enviarem as informações para o roteador. No terminal, digitaremos:

```
PC>ping 192.168.3.2
```

```
FINANCIERO - Set New Backgroun
Physical Config Desktop Software/Services
X
Command Prompt
PC>ping 192.168.3.2
Pinging 192.168.3.2 with 32 bytes of data:
Reply from 192.168.3.2: bytes=32 time=1ms TTL=127
Reply from 192.168.3.2: bytes=32 time=0ms TTL=127
Reply from 192.168.3.2: bytes=32 time=1ms TTL=127
Reply from 192.168.3.2: bytes=32 time=0ms TTL=127
Ping statistics for 192.168.3.2:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 0ms, Maximum = 1ms, Average = 0ms
PC>
```

A conexão foi estabelecida. Observe que quando fizemos os testes com os dois computadores diretamente, aparecia no retorno o TTL igual a 128 (agora, o valor é 127). Isto acontecia porque não tínhamos o roteador, que irá decrementar em uma unidade cada vez que os pacotes passarem por ele.

Para que serve o default gateway?

Ele é o "portão de saída" da minha rede

O default gateway é o endereço IP o qual será responsável por encaminhar pacotes para redes externas, é o IP do meu roteador.

Mãos à obra: Usando o roteador

- Troque o IP de um dos computadores para 191.168.3.1. Tente realizar o teste do ping e veja o resultado!
- Clique no Switch e depois pressione o botão DELETE do teclado, mantenha na área de trabalho somente dois computadores. (191.168.3.1 e 192.168.3.2)
- Clique no ícone “Routers” e arraste para a área de trabalho. Posteriormente clique em “Connections” e selecione a opção cabo cruzado (4^a opção da esquerda para a direita) e conecte os computadores ao roteador.

- Clique duas vezes no roteador e faça a configuração necessária para o teste de ping funcionar nas duas pontas :) (Lembre-se: precisamos habilitar as portas, configurar os endereços IP e o portão de saída dos computadores, default gateway)
- Uma vez feita a configuração, volte para o modo privilégio (Router#), para isso digite Ctrl z, depois escreva wr para salvar a configuração do roteador.

Opinião do instrutor

A configuração do roteador deverá estar parecida com a abaixo:

```
interface FastEthernet0/0
ip address 191.168.3.7 255.255.255.0
duplex auto
speed auto
!
interface FastEthernet0/1
ip address 192.168.3.5 255.255.255.0
duplex auto
speed auto
```

Duplex seria a forma de comunicação utilizada pelas placas de rede Ethernet, quando a porta tem a opção de operar em modo full duplex, quer dizer que ela é capaz de enviar e receber dados ao mesmo tempo, enquanto que o modo half duplex não consegue realizar tal operação simultaneamente, somente em um sentido de operação .

Speed seria a velocidade de transmissão, inicialmente as placas de rede eram capaz de transmitir em velocidades de somente 10Mbps (padrão Ethernet), porém outras velocidades foram especificadas posteriormente como a FastEthernet 100Mbps, Gigabit Ethernet 1.000 Mbps etc

Auto seria de auto negociação, isso quer dizer que as placas de rede interconectadas vão negociar para utilizarem parâmetros de transmissão suportados pelas duas placas de rede, como a forma de comunicação e velocidade de transmissão.

Roteador doméstico

Agora, levaremos a configuração feita para o ambiente doméstico. A configuração que fizemos no projeto, usamos o cabo de console, digitamos os comando na interface com o fundo preto. Trabalhamos com a configuração de um roteador empresarial, que possui funções um pouco mais avançadas.

Porém, na casa nós podemos usar o Prompt ou o Terminal, e buscaremos quem é o Default Gateway da nossa rede. Sabendo qual é o endereço de IP, podemos trabalhar com a janela de configuração do roteador.

c:\Users\Alura>ipconfig

No Mac e no Linux, o comando seria ifconfig.

O gateway padrão que estamos utilizando é 192.168.1.1.

```

[+] Selecionar Prompt de Comando

Endereço IPv4. . . . . : 192.168.3.2
Máscara de Sub-rede . . . . . : 255.255.255.0
Gateway Padrão. . . . . :

Adaptador de Rede sem Fio Wi-Fi 2:

Sufixo DNS específico de conexão. . . . . : home
Endereço IPv4. . . . . : 192.168.1.33
Máscara de Sub-rede . . . . . : 255.255.255.0
Gateway Padrão. . . . . : 192.168.1.1

```

Após copiarmos o número do IP, vamos até o browser, e iremos colá-lo na barra de endereço. Clicaremos em "Enter" e o resultado será:



Caímos na parte de configuração de roteador da Vivo. A configuração do roteador da sua casa será feita de forma parecida. Pode ser que pedido o login e senha para entrar na parte de configuração. Mas a interface gráfica será semelhante a que mostramos.

Classes Ip

Nós já discutimos que para uma máquina ser identificada, precisaremos do IP dela. Mas será que nós podemos criar qualquer valor em qualquer intervalo do endereço? Não podemos! Existe um órgão internacional que regulamenta os IPs colocando em classes que podem ser utilizadas.

Veremos mais sobre o assunto. A **classe A** é a primeira que veremos.

CLASSE DE ENDEREÇAMENTO	INTERVALO 1º OCTETO	MÁSCARA DE REDE
CLASSE A	1 - 126	255.0.0.0

Para um endereço IP estar dentro da classe A, deverá ter o primeiro octeto variando de 1-126 e a máscara de rede padrão deverá ser 255.0.0.0.

Endereço IP: 124.4.7.9

Máscara de rede: 255.0.0.0

Por exemplo, se o IP foi 124.4.7.9. O primeiro octeto 124 está dentro do intervalo especificado na classe A e por isso, a máscara de rede padrão dele será 255.0.0.0. Sabemos que a máscara de rede irá separar o IP em "Rede" e "Host". Desta forma, o que for referente a 255 fará parte da rede, e o que for 0 pertencerá a parte das máquinas.

Endereço IP: 124.4.7.9

Máscara de rede: 255.0.0.0

255 = REDE

0 = MÁQUINA (HOST)



A máscara de rede começará sua análise pelo primeiro octeto e verá se são iguais. Se outra máquina quiser ser da mesma rede, deverá começar o seu IP com 124. Já a parte do 0 será em relação aos hosts, então os três últimos octetos não serão importantes.

Veremos sobre a **classe B**.

CLASSE DE ENDEREÇAMENTO	INTERVALO 1º OCTETO	MÁSCARA DE REDE
CLASSE B	128 - 191	255.255.0.0

Para fazer parte da classe B, o endereço IP deve ter o seu primeiro octeto dentro dos valores 128-191 e a máscara padrão será 255.255.0.0. Analisaremos um endereço que está dentro da classe B.

Endereço IP: 172.161.7.9

Máscara de rede: 255.255.0.0

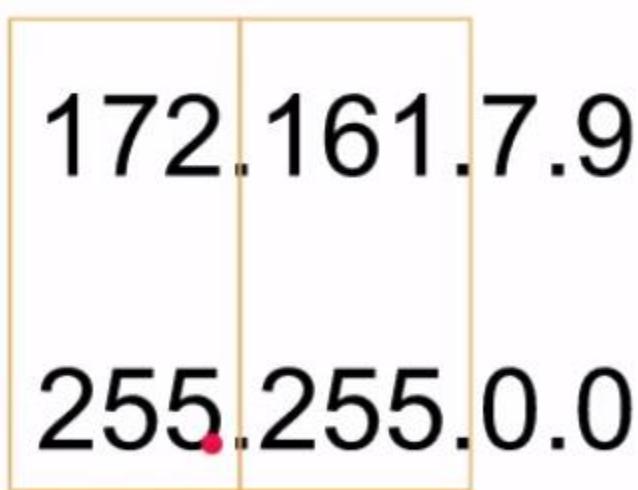
Nós já sabemos qual é a máscara padrão da classe. Ela precisará analisar os dois primeiros octetos para saber se duas máquinas fazem da mesma rede.

Endereço IP: 172.161.7.9

Máscara de rede: 255.255.0.0

255 = REDE

0 = MÁQUINA (HOST)

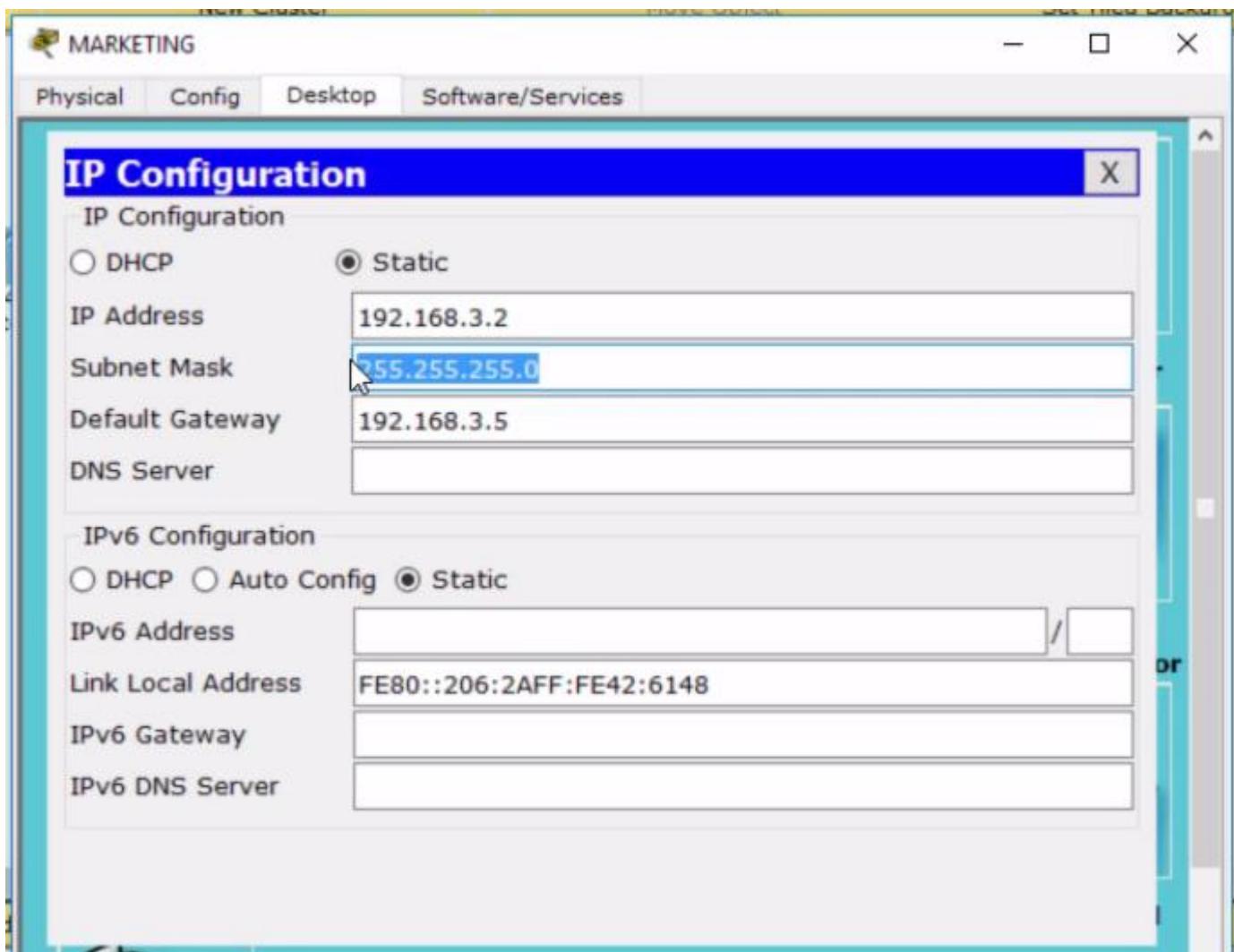


A terceira classe é a C.

CLASSE DE ENDEREÇAMENTO	INTERVALO 1º OCTETO	MÁSCARA DE REDE
CLASSE C	192 - 223	255.255.255.0

Para fazer parte desta classe, o IP deve ter o primeiro octeto dentro do intervalo 192-223 e a máscara de rede padrão será 255.255.255.0.

Lembra que no nosso projeto, ao preenchermos o IP da máquina nas configurações, ele preencheu automaticamente qual era a máscara de rede?



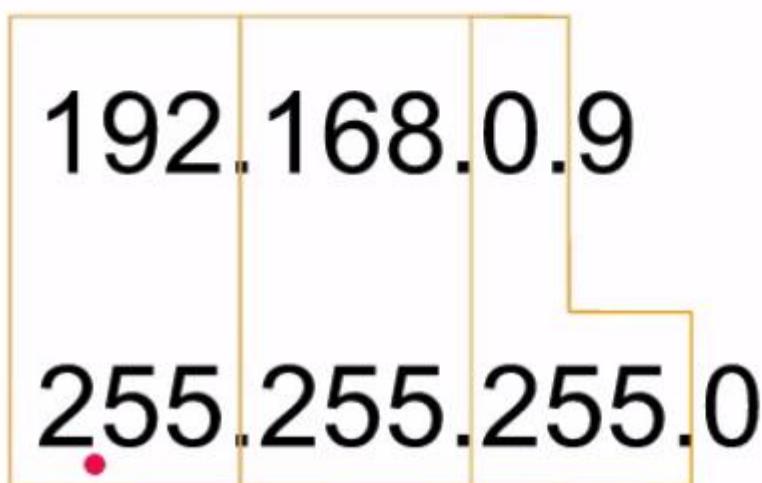
Como o IP tinha o primeiro octeto igual a 192 ele sabia qual seria a máscara padrão. Mas vamos analisar outro IP.

Endereço IP: 192.168.0.9

Máscara de rede: 255.255.255.0

255 = REDE

0 = MÁQUINA (HOST)



Para outro dispositivo fazer parte da mesma rede que o computador do exemplo, o IP terá que começar com 192.168.0. O valor do último octeto será irrelevante.

Temos também a **classe D**.

CLASSE DE ENDEREÇAMENTO	INTERVALO 1º OCTETO	MÁSCARA DE REDE
CLASSE D	224-239	-

Ela será caracterizada pelo primeiro octeto indo de 224-239. Mas ela é diferente das demais, por ser reservada para o uso de **multicast** (casos em que queremos fazer a comunicação somente com alguns dispositivos que estão na nossa rede). Ela não é atribuída para máquinas. Assim como a **classe E**, identificada pelo intervalo 240-255 no primeiro octeto.

CLASSE DE ENDEREÇAMENTO	INTERVALO 1º OCTETO	MÁSCARA DE REDE
CLASSE E	240-255	-

Ela também é reservada, não sendo utilizada para atribuir endereços IPs para máquinas.

A IETF (Internet Engineering Task Force) determinou que existiriam ao todo 5 classes de endereços IP, indo de ordem alfabética da classe A até a classe E. Porém as duas últimas classes não são usadas para serem endereçadas as máquinas. A classe D seria usada para multicast (termo usado quando queremos nos comunicar com somente algumas máquinas de nossa rede) e a classe E seria uma classe experimental. Portanto as classes de IP que podem ser endereçadas para máquinas seriam a classe A, B e C.

Para sabermos em qual classe um endereço IP se encontra, temos que analisar o primeiro octeto e ver dentro de qual range ele estaria. (Classe A, B ou C).

O endereço IP 187.77.45.8 estaria dentro de qual classe, considerando que usa máscara de rede padrão?

Classe B

A classe "A" possui o primeiro octeto variando de 1 a 127, a classe "B" possui o primeiro octeto variando de 128 a 191 e a classe "C" possui o primeiro octeto variando de 192 a 223. Dessa forma pelo fato do número 187 se encontrar dentro de 128 a 191, sabemos que é um endereço da classe "B".

O que seria o endereço 127.0.0.1? Como ele é conhecido?

É um endereço interno da placa de rede, usado para testar se os protocolos TCP/IP estão funcionando. Ele é conhecido como endereço de loopback, pois o sinal é enviado e recebido por ele mesmo. O endereço 127.0.0.1 seria uma faixa de endereço IP reservada, esse seria um endereço interno da placa de rede para realizar testes e verificar se ela está de fato validando os protocolos TCP/IP.

Ip privado

Nos vimos três classes de IP que são utilizadas para o endereçamento nas máquinas: **A, B e C**. As classes D e E não são utilizadas para a atribuição em máquinas.

Dentro de cada um dos intervalos de IP, teremos faixas que são chamadas de **privadas**. Elas recebem esse nome, porque só podemos nos comunicar na rede local, não podendo ser utilizados na comunicação na internet.

CLASSE DE ENDEREÇAMENTO	INTERVALO PRIVADO
CLASSE A	10.x.x.x

Na classe A, temos a faixa de endereço que começam com 10 não poderá se comunicar na internet.

CLASSE DE ENDEREÇAMENTO	INTERVALO PRIVADO
CLASSE A	10.x.x.x
CLASSE B	172.16.x.x - 172.31.x.x

Na classe B, os endereços que serão privados começam com 172.16 até 172.31.

CLASSE DE ENDEREÇAMENTO	INTERVALO PRIVADO
CLASSE A	10.x.x.x
CLASSE B	172.16.x.x - 172.31.x.x
CLASSE C	192.168.x.x

Os endereços privados na classe C começam com 192.168.

Vamos ver se o IP da máquina que estamos usando na gravação entra em alguma dessas faixas? No prompt de comando, digitaremos ipconfig e buscaremos o IP do adaptador do Wireless que estou acessando.

```
Selecionar Prompt de Comando
Adaptador de Rede sem Fio Wi-Fi 2:
Sufixo DNS específico de conexão... : home
Endereço IPv4... : 192.168.1.33
Máscara de Sub-rede... : 255.255.255.0
Gateway Padrão... : 192.168.1.1
```

Nós acabamos de ver que os IPs que começam com 192.168 estão dentro da faixa de privados. Então, como conseguimos acessar a internet? O meu roteador irá traduzir o IP privado pelo IP público. Quando contratamos um serviço de empresas como a Vivo ou GVT, elas nos fornecem um número de IP público. Se fizermos uma pesquisa no [site Meu IP](#), o IP que será identificado será outro.

The screenshot shows a web browser window with the URL www.meuip.com.br. At the top, there's a navigation bar with icons for back, forward, and search, followed by the site's logo "MeuIP.com.br". Below the logo are three buttons: "Localizar IP", "Perguntas Frequentes", and "Ferramentas de Rede". A banner features a cartoon dog named "Pipoca" and the text "Oi, eu sou o Pipoca e tenho uma dica pra você navegar rápido!". Below this, the main content area displays the IP address "Meu IP: 189.18.129.152" in red, with a blue button next to it labeled "Testar VELOCIDADE". It also shows the provider "Provedor: VIVO" and the reverse IP "IP Reverso: 189-18-129-152.dsl.telesp.net.br". A warning message "Sua internet pode estar lenta devido a Erros no Windows" is present, along with a suggestion "SUGESTÃO: Instalar um Otimizador de Sistema para Limpar e Corrigir os Problemas". A blue button "Fazer Download e Instalar" is available. At the bottom, there are three links: "Como Melhorar minha Internet?", "Como Localizar um IP?", and "Como esconder meu IP?". To the right, there's a small video player showing a man speaking.

O IP 189.18.129.152 será o número que a Vivo atribuiu. Observe que efetivamente o roteador fez a tradução do endereço que aparecia no Prompt para o que vemos no site. Isto é feito por meio do método **NAT** (*Network Address Translation*), em que é feita a tradução de um endereço privado para o público.

Os endereços IP privados são usados para comunicação somente em minha rede local, de acordo com a especificação, eles não podem ser usados para comunicação na internet por exemplo.

Se eu tenho IP privado na minha máquina, como posso acessar a internet?

- Através do método de tradução de endereços IPs privados para públicos, chamado de NAT

Isso acontece porque nosso roteador possui a configuração chamada NAT, essa configuração vai converter o endereço IP privado que temos em nossas máquinas para IP públicos que nosso provedor de serviços nos fornece.

IPv6

Se analisarmos o endereço IP que identificamos anterior (192.168.1.33), veremos que ele aparece com o nome **IPv4**.

```
Selecionar Prompt de Comando
Adaptador Ethernet Ethernet:
Sufixo DNS específico de conexão. . . . . :
Endereço IPv4. . . . . : 192.168.3.2
Máscara de Sub-rede . . . . . : 255.255.255.0
Gateway Padrão. . . . . :

Adaptador de Rede sem Fio Wi-Fi 2:
Sufixo DNS específico de conexão. . . . . : home
Endereço IPv4. . . . . : 192.168.1.33
Máscara de Sub-rede . . . . . : 255.255.255.0
Gateway Padrão. . . . . : 192.168.1.1
```

O v4 representa a "versão 4". O endereço IP mais comumente conhecido, chegou ao fim devido a grande popularidade da internet. Foi necessário criar uma evolução para os endereços IPs. O IPv6 terá uma série de componentes novos e funcionalidades mais avançadas, que não serão abordadas no curso. Mas para vermos como são formados os IPv6, usaremos o nslookup com o endereço do Uol.

```
C:\Users\Alura>nslookup www.uol.com.br
```

```
Prompt de Comando
Adaptador de túnel isatap.{F6067C02-77AF-4F6B-B300-C9ABAA44982A}:
Estado da mídia. . . . . : mídia desconectada
Sufixo DNS específico de conexão. . . . . :

Adaptador de túnel isatap.{48869A9E-B89A-4A10-93E7-87104C1D3363}:
Estado da mídia. . . . . : mídia desconectada
Sufixo DNS específico de conexão. . . . . :

C:\Users\Alura>nslookup www.uol.com.br
Servidor: openrg.home
Address: 192.168.1.1

Não é resposta autoritativa:
Nome: homeuol.ipv6uol.com.br
Addresses: 2804:49c:3103:401:ffff:ffff:ffff:1 ←
           200.221.2.45 ←
Aliases: www.uol.com.br
```

Eles possuem um endereço IPv6 (o que foi primeiro sinalizado) e um IPv4 (o segundo com a marcação), para atender diferentes tipos de acesso que tenhamos na máquina deles. Observe que o IPv6 possui uma quantidade de informações bem maior que a versão 4, lembrando que atualmente o IPv4 já não possui endereços IPs disponíveis. O IPv6 já é o padrão utilizado.

A evolução do IPv4 seria a versão 6 do protocolo, que seria conhecida como IPv6.

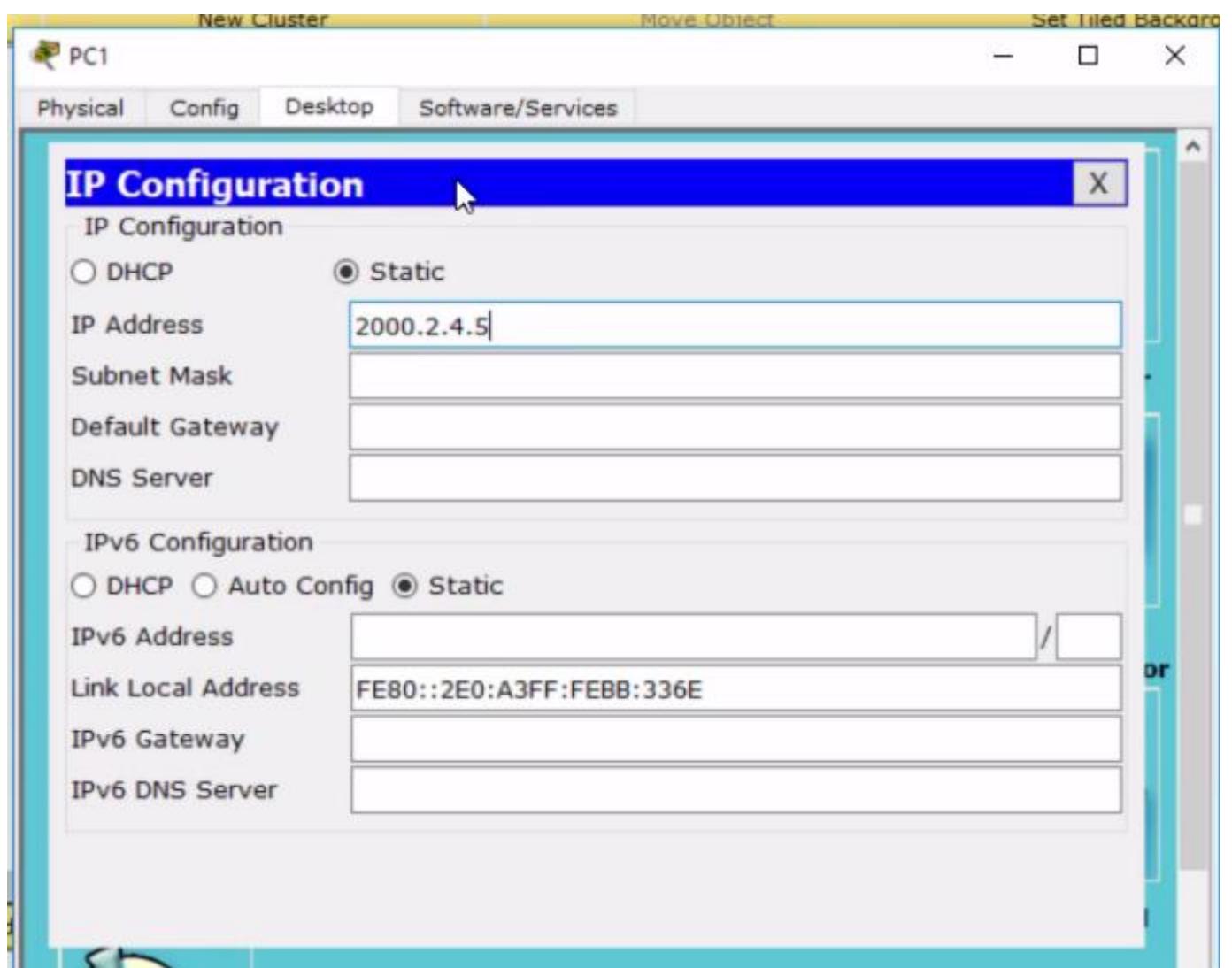
Por que foi necessário o IPv6?

O endereço IPv6 foi necessário porque os endereços IPv4 públicos chegaram a um fim por conta da grande popularidade da internet, smartphones, tablets, etc.

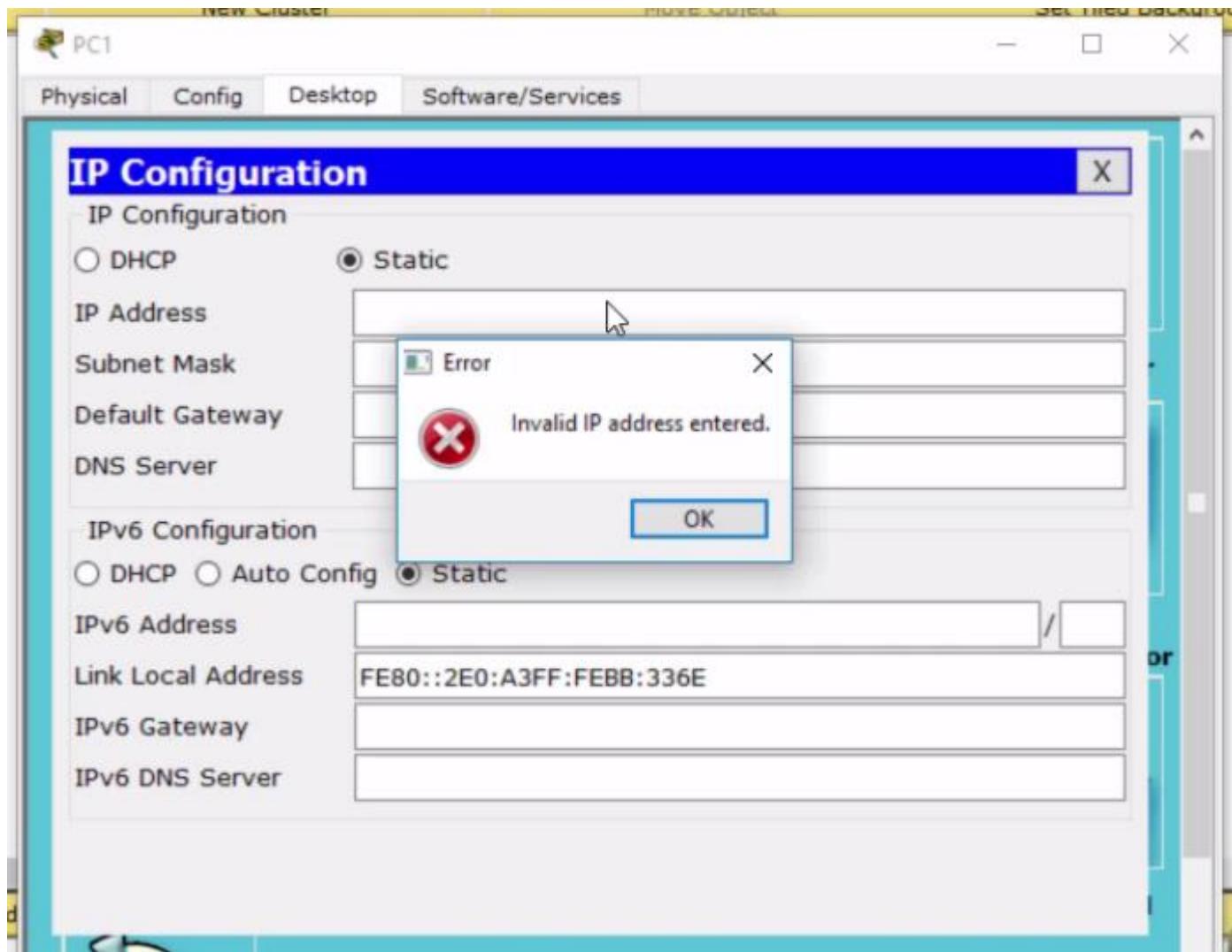
Endereços reservados classe A

Nós conseguimos entender as classes de endereço IP e que ele é usado para identificarmos uma máquina. Mas será que existe um intervalo mínimo e máximo que podemos colocar no endereço IP? Por exemplo, criaremos um projeto no Packet Tracer com um computador.

Ao acessarmos o IP Configuration, será que podemos colocar 2000.2.4.5?



Ele dirá que o endereço do IP é inválido.



Existe um número mínimo e máximo que um endereço de IP pode ter. No caso, o mínimo é 0 e o máximo é 255. Ou seja, nenhum dos octetos pode ter um número maior do que 255. Mas estes números não podem ser usados em qualquer parte. Todo endereço de IP estarão inseridos dentro de uma rede, que terá um número de identificação e ainda, terá o endereço de rede que serve para comunicar com todos os dispositivos da rede chamado de **broadcast**.

Vamos ver com um exemplo como fazemos para descobrir o endereço de rede e o de broadcast.

Endereço IP: 124.4.7.9

•

Máscara de rede: 255.0.0.0

255 = REDE

0 = MÁQUINA (HOST)

A qual classe o IP 124.4.7.9 faz parte? Ele está na classe A, que varia de 1-126. A máscara de rede padrão será 255.0.0.0.

Com os octetos separados, o IP ficará assim:

Endereço IP: 124.4.7.9

Máscara de rede: 255.0.0.0

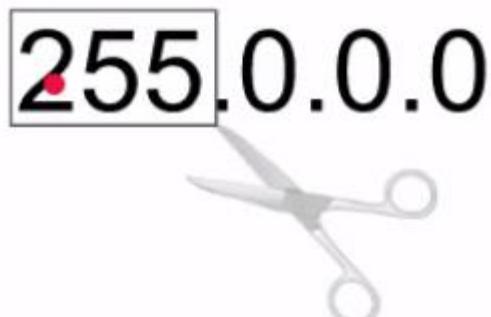
255 = REDE

0 = MÁQUINA (HOST)



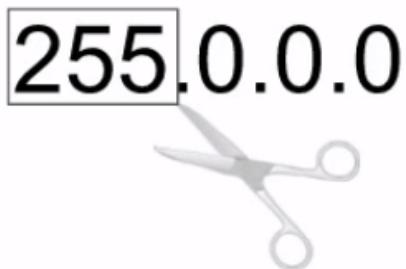
A regra para descobrirmos o endereço de rede em que o IP está inserido: Iremos cortar o 255 do número da máscara de rede.

1-) Recortar “255” da máscara de rede



Agora, faremos uma comparação entre o número com recorte e o endereço de IP original.

2-) Inserir o valor do endereço IP referente esse intervalo



124.4.7.9

.0.0.0

Para descobrirmos o endereço de rede, basta mover o primeiro octeto do IP, para o espaço vazio do número da máscara.

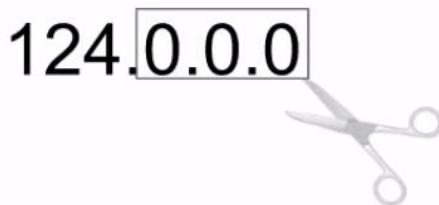
124.4.7.9



124.0.0.0

O endereço de rede será 124.0.0.0. Para descobrirmos o endereço de broadcast, basta cortarmos os zeros do endereço de rede que vieram originalmente da máscara padrão.

1-) Pegar o endereço de rede e recortar os “0” originais da máscara de rede



Após cortarmos os zeros, substituiremos por 255 nos espaços recortados.

2-) Pegar esse intervalo e inserir “255” nos espaços que foram recortados

124. . .

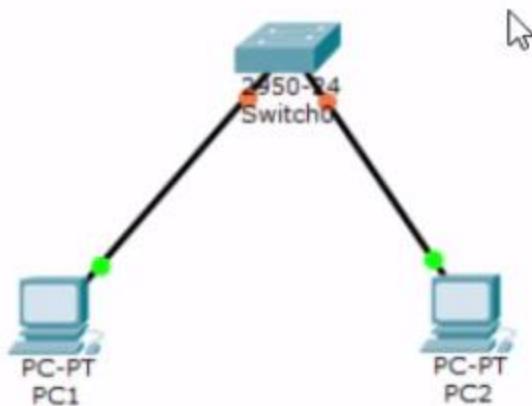


124.255.255.255

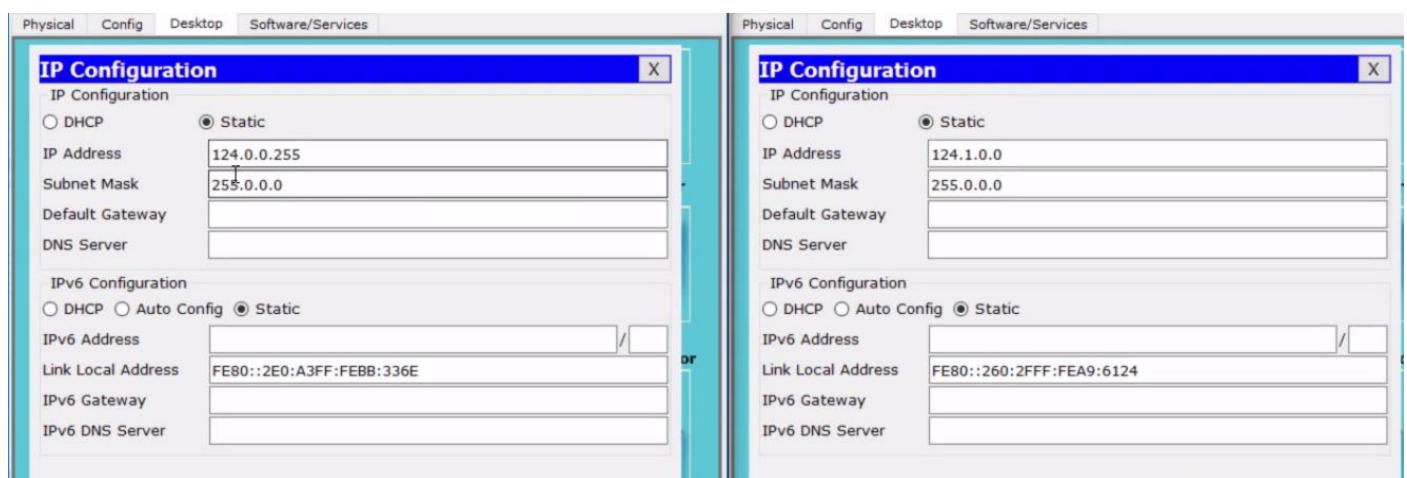
O endereço de broadcast será 124.255.255.255.

Agora, tudo o que estiver no intervalo de 124.0.0.0 será o endereço de rede e não poderá ser usado em nenhuma máquina. Assim como 124.255.255.255 também não poderá ser usado em uma máquina.

Criaremos um novo projeto para testar o que vimos:



A máquina da esquerda iremos configurar com o IP 124.0.0.255 e a direita receberá o IP 124.1.0.0.



Os dois endereços IPs são válidos? Sim, porque ambos estão dentro dos intervalos que comentamos. Nós podemos inclusive fazer o teste de conectividade entre os computadores.

No Command Prompt digitaremos:

```
PC>ping 124.1.0.0
```

E a conexão será bem-sucedida.

Packet Tracer PC Command Line 1.0
PC>ping 124.1.0.0

Pinging 124.1.0.0 with 32 bytes of data:

Reply from 124.1.0.0: bytes=32 time=0ms TTL=128
Reply from 124.1.0.0: bytes=32 time=0ms TTL=128
Reply from 124.1.0.0: bytes=32 time=0ms TTL=128
|

Então, só não poderemos usar o endereço de rede e o de broadcast.

Dado que o endereço IP da máquina 7.8.7.8 possui máscara de rede 255.0.0.0, determine seu endereço de rede e broadcast (Lembre-se da regra, endereço de rede e broadcast):

Rede: 7.0.0.0 ; Broadcast: 7.255.255.255

- Descobrir endereço de rede que esse endereço IP está inserido:
 - Se recortarmos o 255 da máscara de rede e inserirmos o octeto correspondente do endereço IP, teremos: 7.0.0.0 :)
- Descobrir o endereço de broadcast da rede:
 - Pegamos o endereço de rede e recortamos os 0's (originais da máscara) e colocamos 255 no lugar, teremos então: 7.255.255.255

Dessa forma, por exemplo o endereço IP: 7.0.0.255 é válido porque é maior que o endereço de rede (7.0.0.0) e menor que o de broadcast (7.255.255.255)

Endereços reservados classe B

Vamos continuar com a análise dos IPs.

Endereço IP: 172.161.7.9

Máscara de rede: 255.255.0.0

255 = REDE

0 = MÁQUINA (HOST)

O endereço 172.161.7.9 está inserido em qual classe? Nós sabemos que 172 está dentro do intervalo 128-191, e por isso, faz parte da classe B. E sabemos também que a máscara de rede será 255.255.0.

Com as divisões por octeto, o IP ficará assim:

172	161	7	9	.
255	255	0	0	

Vamos revisar como descobrir o endereço de rede:

2-) Inserir o valor do endereço IP referente esse intervalo

255.255.0.0



172.161.7.9



Tendo o endereço de rede, podemos descobrir qual é o endereço de broadcast:

1-) Pegar o endereço de rede e recortar os “0” originais da máscara de rede

172.161.0.0



2-) Pegar esse intervalo e inserir “255” nos espaços que foram recortados

172.161..



Lembrando que os endereços 172.161.0.0 e 172.161.255.255 não podem ser atribuídos para ninguém. O que estiver dentro do intervalo entre os dois poderá ser utilizado.

Dado que o endereço IP da máquina 135.44.3.21 possui máscara de rede 255.255.0.0, determine seu endereço de rede e broadcast (Lembre-se da regra, endereço de rede e broadcast):

Rede: 135.44.0.0 ; Broadcast: 135.44.255.255

- Descobrir endereço de rede que esse endereço IP está inserido:
 - Se recortarmos o 255 da máscara de rede e inserirmos os octetos correspondentes do endereço IP, teremos: 135.44.0.0 :)
- Descobrir o endereço de broadcast da rede:
 - Pegamos o endereço de rede e recortamos os 0's (originais da máscara) e colocamos 255 no lugar, teremos então: 135.44.255.255

Dessa forma, por exemplo o endereço IP: 135.44.0.255 é válido por que é maior que o endereço de rede (135.44.0.0) e menor que o de broadcast (135.44.255.255)

Endereços reservados classe C

Vamos analisar mais um endereço de IP: 192.168.0.9.

Endereço IP: 192.168.0.9

Máscara de rede: 255.255.255.0

255 = REDE

0 = MÁQUINA (HOST)

192.	168.0.9
255.	255.255.0

O IP está inserido no intervalo da classe C, que é de 192–223. Sabemos que a máscara padrão da classe é 255.255.255.0.

Com as divisões de octeto, o IP ficará assim:

192.168.0.9

255.255.255.0

Depois, descobriremos o endereço de rede. Repetiremos os passos feitos anteriormente: recortaremos o 255 do IP.

1-) Recortar “255” da máscara de rede

255.255.255.0



Para então, chegar no endereço de rede:

2-) Inserir o valor do endereço IP referente esse intervalo

255.255.255.0



192.168.0.9



192.168.0.0 = Endereço de rede

Temos o endereço de rede. Em seguida, encontraremos o endereço de broadcast:

1-) Pegar o endereço de rede e recortar os “0” originais da máscara de rede

192.168.0.0



Depois, encontraremos o endereço de broadcast:

2-) Pegar esse intervalo e inserir “255” nos espaços que foram recortados

192.168.0.



192.168.0.255 = Endereço de broadcast

Mas não se prenda ideia de que não se pode ter o final de um IP com valor 0 ou 255. O que definirá serão os números de endereço de rede e de broadcast.

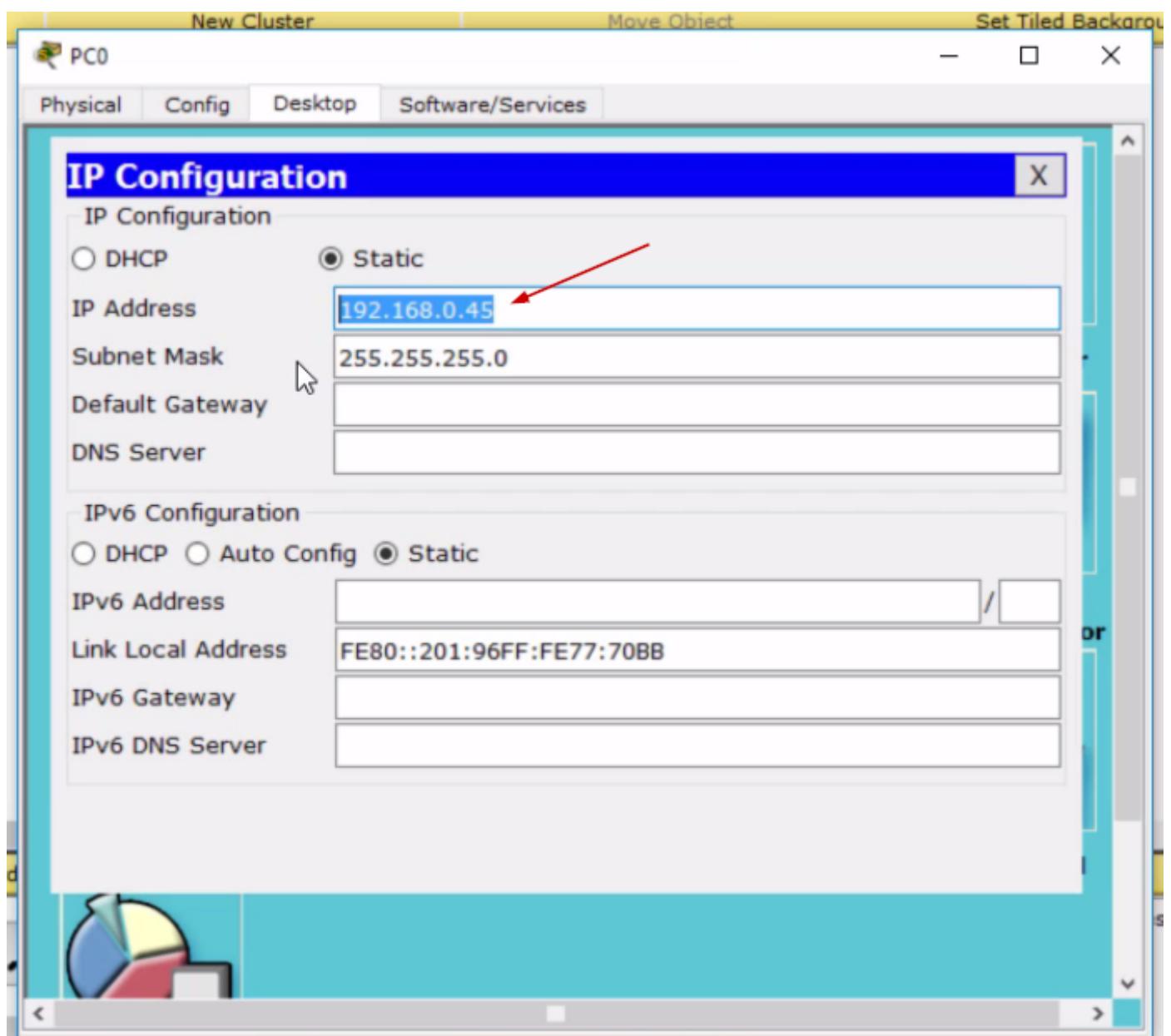
Broadcast

O que caracteriza uma comunicação broadcast?

Broadcast seria um termo usado quando a comunicação é feita para todos os dispositivos que estão na mesma rede.

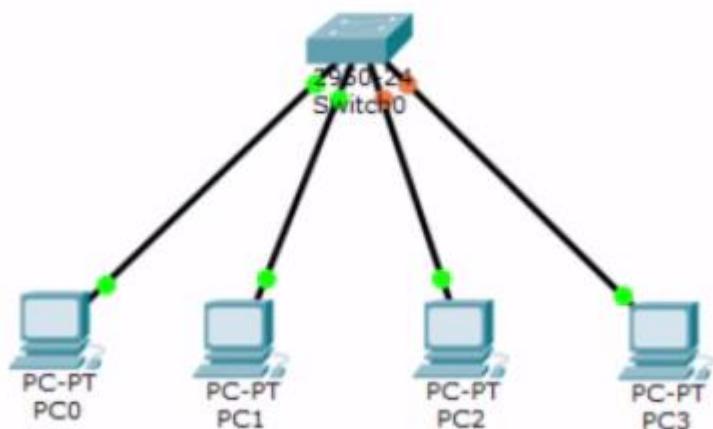
DHCP

Até o momento nós temos feito a configuração manual de todos os endereços IPs. Clicamos no ícone de computador, selecionado a aba "Desktop" e depois, em "IP Configuration" inserimos o número do IP.



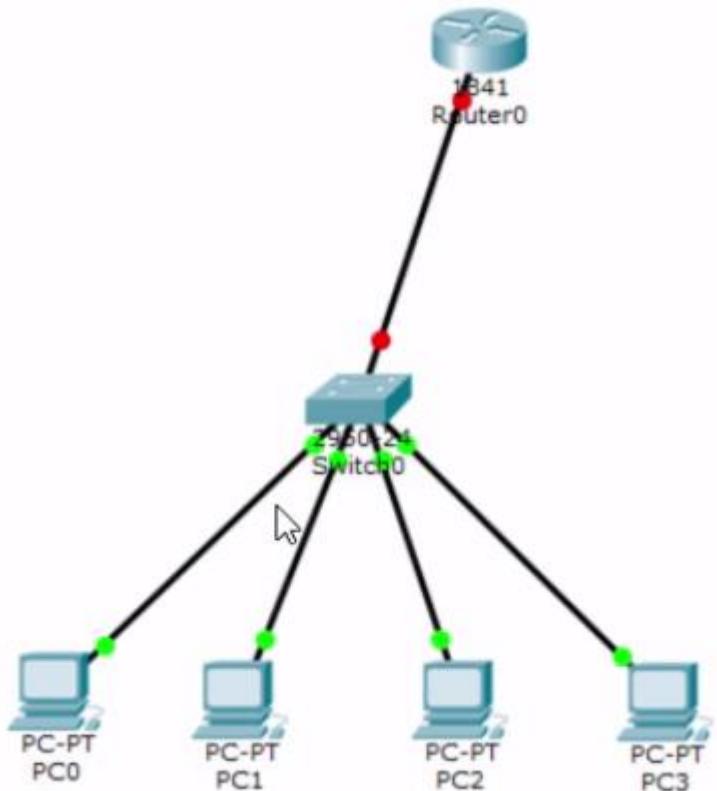
Agora, temos um projeto com apenas dois computadores. Mas imagine que você está trabalhando em uma empresa com 100 usuários e precise colocar o IP manualmente na máquina de cada um. Seria um processo muito trabalhoso. Existe uma forma de fazer isto automaticamente: usando o servidor DHCP. Veremos como funciona:

Conectaremos quatro computadores com cabo direto.

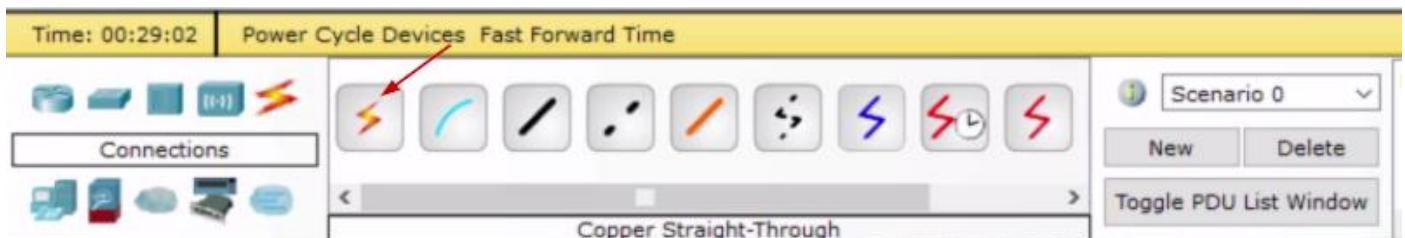


Quem irá atuar como nosso servidor DHCP neste exemplo, será o roteador da Cisco. Ele fornecerá endereços IPs automaticamente para os computadores. Vamos arrastar um ícone de Router para o projeto que será conectado no Switch. Esta conexão irá explorar a totalidade das funcionalidades que o equipamento foi projetado para fazer? O Switch foi projetado para interconectar vários computadores, e o roteador foi projetado para interconectar redes diferentes - que costumam possuir vários computadores. Quando conectarmos o roteador com o Switch, ele estará conectando uma rede com vários computadores que podem se comunicar com outras redes. É uma conexão natural.

Selecionaremos o cabo direto e interconectaremos o roteador.

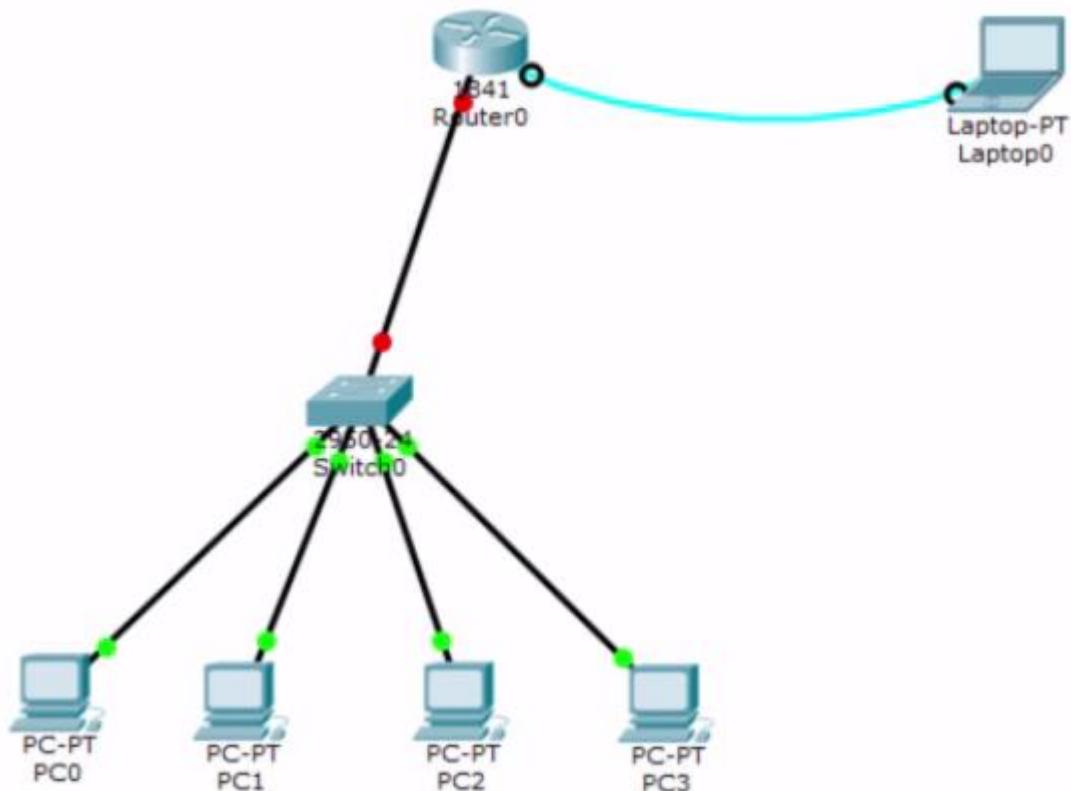


Caso você tenha dúvida quanto ao cabo que deverá ser selecionado, a primeira opção da listagem (o ícone de raio) fará a escolha correta.



Não selecionamos esta opção antes para que pudéssemos fixar os conceitos.

Agora, iremos configurar o roteador. Na prática, para fazermos isto precisaríamos de uma máquina interconectada ao roteador.



Mas os desenvolvedores do software facilitaram nossa vida e colocaram o terminal de configuração embutido no equipamento. Basta clicarmos no ícone do Router, ir na aba "CLI" e irá aparecer a opção para configurarmos o equipamento.

The screenshot shows a window titled "Router0" with tabs for "Physical", "Config", and "CLI". The "CLI" tab is active, displaying the "IOS Command Line Interface". The terminal window contains the following text:

```
Cisco 1841 (revision 5.0) with 114688K/16384K bytes  
of memory.  
Processor board ID FTX0947Z18E  
M860 processor: part number 0, mask 49  
2 FastEthernet/IEEE 802.3 interface(s)  
191K bytes of NVRAM.  
63488K bytes of ATA CompactFlash (Read/Write)  
Cisco IOS Software, 1841 Software (C1841-  
ADVIPSERVICESK9-M), Version 12.4(15)T1, RELEASE  
SOFTWARE (fc2)  
Technical Support: http://www.cisco.com/techsupport  
Copyright (c) 1986-2007 by Cisco Systems, Inc.  
Compiled Wed 18-Jul-07 04:52 by pt_team  
  
---- System Configuration Dialog ----  
Continue with configuration dialog? [yes/no]: |
```

At the bottom right of the terminal window, there are "Copy" and "Paste" buttons.

Os roteadores da Cisco têm a porta desabilitada por padrão. A primeira coisa que faremos será habilitar a porta. Na linha de comando, ele nos perguntará se queremos um diálogo para nos ajudar na configuração. Nós responderemos que não precisa.

IOS Command Line Interface

```
M860 processor: part number 0, mask 49
2 FastEthernet/IEEE 802.3 interface(s)
191K bytes of NVRAM.
63488K bytes of ATA CompactFlash (Read/Write)
Cisco IOS Software, 1841 Software (C1841-
ADVIPSERVICESK9-M), Version 12.4(15)T1, RELEASE
SOFTWARE (fc2)
Technical Support: http://www.cisco.com/techsupport
Copyright (c) 1986-2007 by Cisco Systems, Inc.
Compiled Wed 18-Jul-07 04:52 by pt_team
```

```
---- System Configuration Dialog ----
```

```
Continue with configuration dialog? [yes/no]: no
```

```
Press RETURN to get started!
```

Nós ainda estaremos no modo usuário, em que só conseguimos verificar algumas questões para reparos e testes, mas não podemos configurar o equipamento. Teremos que escalar o privilégio.

```
Router>enable
Router#
```

Como vimos anteriormente até aqui, só poderemos ver todas as visualizações que poderemos fazer no equipamento. Seguiremos para o `configure terminal`.

```
Router#configure terminal
```

Após pressionarmos o "Enter" entraremos efetivamente na parte de configuração.

Physical Config CLI

IOS Command Line Interface

Technical Support: <http://www.cisco.com/techsupport>
Copyright (c) 1986-2007 by Cisco Systems, Inc.
Compiled Wed 18-Jul-07 04:52 by pt_team

--- System Configuration Dialog ---

Continue with configuration dialog? [yes/no]: no

Press RETURN to get started!

```
Router>
Router>
Router>enable
Router#
Router#
Router#conf
Router#configure term
Router#configure terminal
Enter configuration commands, one per line. End
with CNTL/Z.
Router(config)#
```

[Copy](#)

[Paste](#)

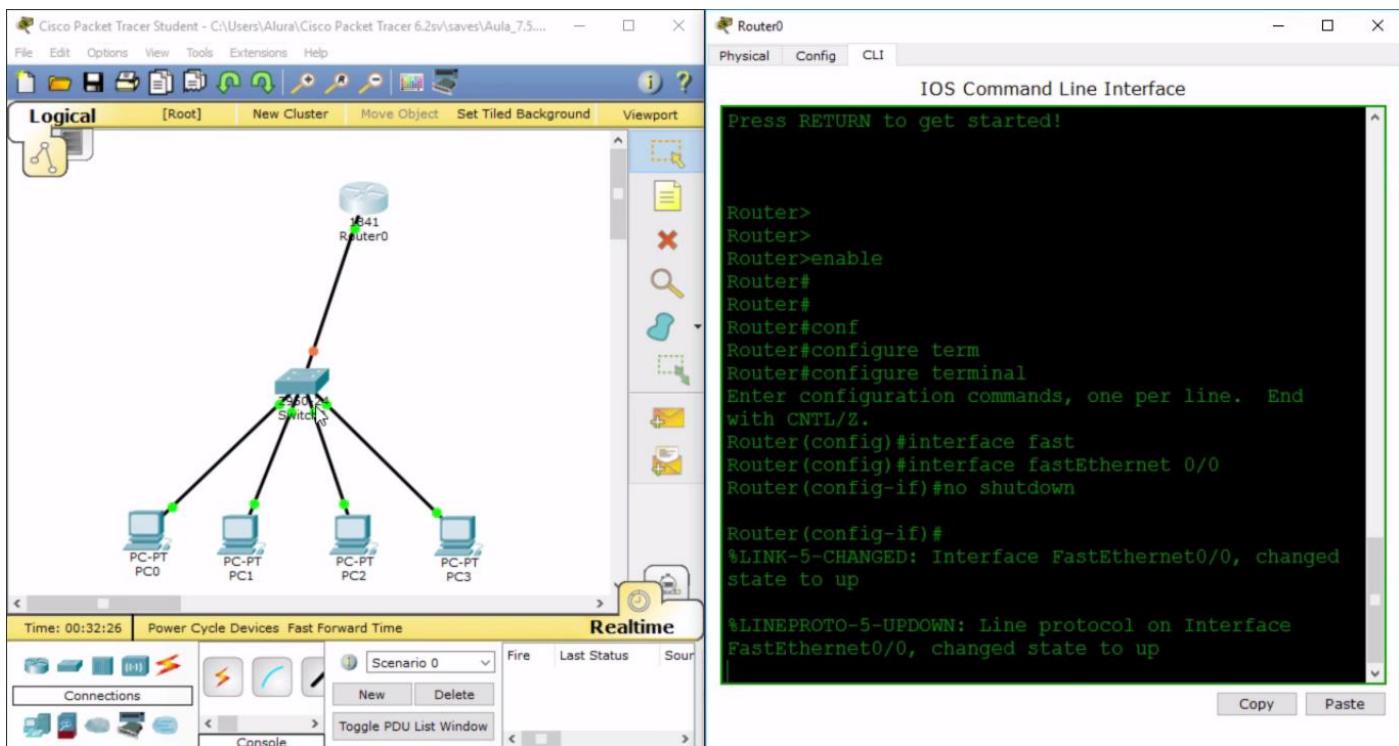
Depois, digitaremos:

```
Router#(config)#interface fastEthernet 0/0
```

Nos conectaremos na porta 0/0 e então, habilitaremos a porta. Para isto, usaremos o comando `no shutdown`.

```
Router#(config)#no shutdown
```

Estamos dizendo que "não queremos desligar". Agora, as portas serão habilitadas e as luzes ficaram verdes.



Ele informa que mudou o estado para **up**. A porta já está ativa. Em seguida, começaremos a configuração para que ele trabalhe com DHCP. Teremos primeiramente que sair da configuração que estamos.

```
Router(config-if)#exit
```

Além de configurar a interface, queremos fazer ajustes no roteador globalmente para ele trabalhar com DHCP. Vamos adicionar outro comando:

```
Router(config)#ip dhcp
```

Teremos que criar um *pool* de endereços IPs que serão atribuídos para os computadores. Daremos o nome ALURA para esse pool.

```
Router(config)#ip dhcp pool ALURA
```

Depois, digitaremos a **?** para saber quais opções nós temos.

```

Router(config)#ip dhcp pool ALURA
Router(dhcp-config)#? ←
  default-router  Default routers
  dns-server      Set name server
  exit           Exit from DHCP pool configuration
  mode
  network        Network number and mask
  no             Negate a command or set its
  defaults
  option         Raw DHCP options
Router(dhcp-config)#

```

Em seguida, informaremos a rede em que estaremos trabalhando, por isso, descobrimos anteriormente qual era o nosso endereço de rede. No nosso caso, trabalharemos com a rede 192.168.0.0.

```
Router(dhcp-config)#network 192.168.0.0
```

Ele nos informará que o comando está incompleto, então usaremos a ? para descobrir o que está faltando. Ficou faltando a máscara de rede, que será 255.255.255.0.

```
Router(dhcp-config)#network 192.168.0.0 255.255.255.0 ?
```

Adicionamos a ? novamente, mas dessa vez o retorno será <cr>, porque não falta digitar mais nadas.

```
Router(dhcp-config)#network 192.168.0.0
% Incomplete command.
Router(dhcp-config)#network 192.168.0.0 ?
  A.B.C.D Network mask
Router(dhcp-config)#network 192.168.0.0
255.255.255.0 ?
<cr>
Router(dhcp-config)#network 192.168.0.0
|255.255.255.0 |
```

Nós informamos qual a rede que o pool de conexões estará trabalhando.

Será importante indicar qual será o gateway para os computadores, ou seja, para onde as máquinas devem enviar informações caso eles precisarem se comunicar com alguém externamente. Vamos usar o comando default-router para isso. Adicionaremos a ? para receber mais informações.

```
Router(dhcp-config)#default-router ?
```

O retorno será que falta o endereço IP do default router. Adicionaremos o número da porta do roteador: 192.168.0.1.

Lembrando que pelo fato da máscara ser 255.255.255.0, os três primeiros octetos do IP precisam ser iguais para que a porta do roteador esteja na mesma rede que os outros computadores.

Primeiramente, sairemos deste modo de configuração usando o exit. Depois, entraremos na interface

```
Router(config)#interface fastEthernet 0/0
Router(config-if)#ip address 192.168.0.1
```

Inserimos o gateway.

Ao adicionarmos novamente a ?, ele pedirá a máscara de rede:

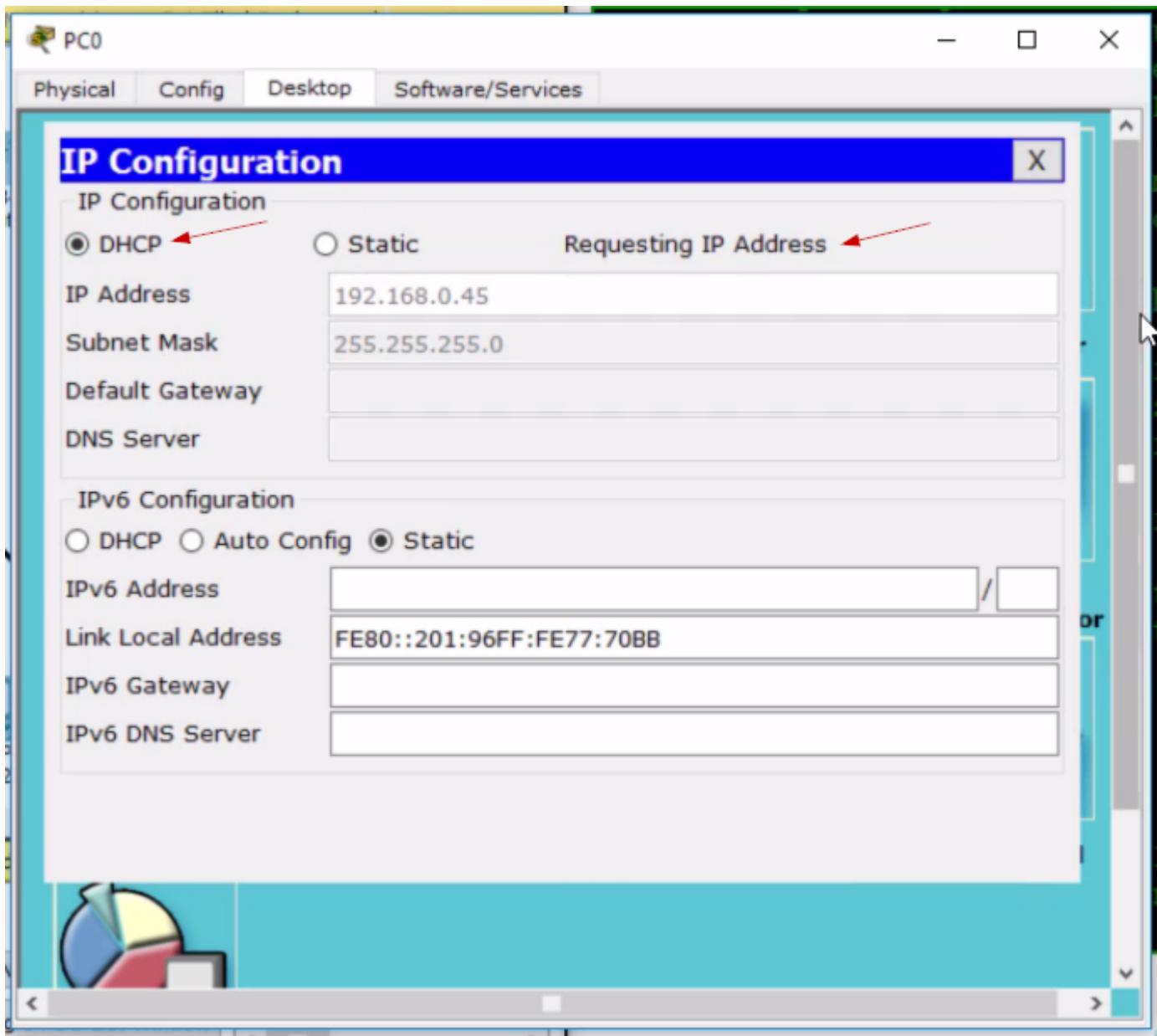
```
Router(dhcp-config)#default-router ?
  A.B.C.D Router's IP address
Router(dhcp-config)#default-router 192.168.0.1 ?
<cr>
Router(dhcp-config)#default-router 192.168.0.1
Router(dhcp-config)#exit
Router(config)#interface fastE
Router(config)#interface fastEthernet 0/0
Router(config-if)#ip add
Router(config-if)#ip address 192.168.0.1 ?
  A.B.C.D IP subnet mask ←
Router(config-if)#ip address 192.168.0.1 2|
```

É o que faremos:

```
Router(config-if)#ip address 192.168.0.1
255.255.255.0
```

Vamos conferir se a configuração de DHCP funcionou.

Na janela de IP Configuration, mudaremos de "Static" para "DHCP".



Observe que ele fez um requisição. Qual será o fluxo da mensagem? Quando um computador é conectado pela primeira vez, ele não possui uma atribuição do endereço IP e saíra perguntando quem irá oferecer esse número para ele. Este é um sinal **broadcast**. O roteador vai receber a requisição e dirá "estou configurado para oferecer endereços IPs". O computador aceitará e vai informar que recebeu um IP. A mensagem será entregue para o roteador também, que por sua vez, irá dar um "OK". Após entender como funciona o processo, vamos repeti-lo para os demais computadores.

Iremos acessar o IP Configuration das demais máquinas, em que iremos mudar de "Static" para "DHCP". O IP será completado automaticamente, assim com o campo de "Default Gateway".

Quando finalizarmos, os quatro computadores terão recebido o endereço IP de forma automática. Não precisaremos mais configurá-los manualmente.

Para que serve um servidor DHCP?

Os servidores DHCP (Dynamic Host Configuration Protocol) alocam dinamicamente endereços IPs a clientes (máquinas).

Como é conhecida essa forma de atribuição de IP pelo DHCP?

IP dinâmico

Quando um endereço IP é atribuído a uma máquina (cliente), dizemos que a configuração foi dinamicamente alocado. Os servidores DHCP normalmente possuem o que chamamos de “lease time”, ou seja possui um tempo de alocação de um endereço IP a uma máquina, quando esse tempo é expirado é preciso ocorrer uma renovação de endereço IP. Por isso ele é dinamicamente alocado :)

Quando um cliente não possui um endereço IP e está configurado para receber IP dinâmico, como ele faz a requisição para que alguém forneça um endereço IP?

Broadcast

Quando um cliente não possui endereço IP ele não sabe a quem perguntar, então ele precisa sair perguntando para todo mundo que está na mesma rede quem poderá fornecer um endereço IP. Quando essa comunicação é feita para todos os dispositivos, chamamos isso de Broadcast.

Mãos à obra: Configurando DHCP

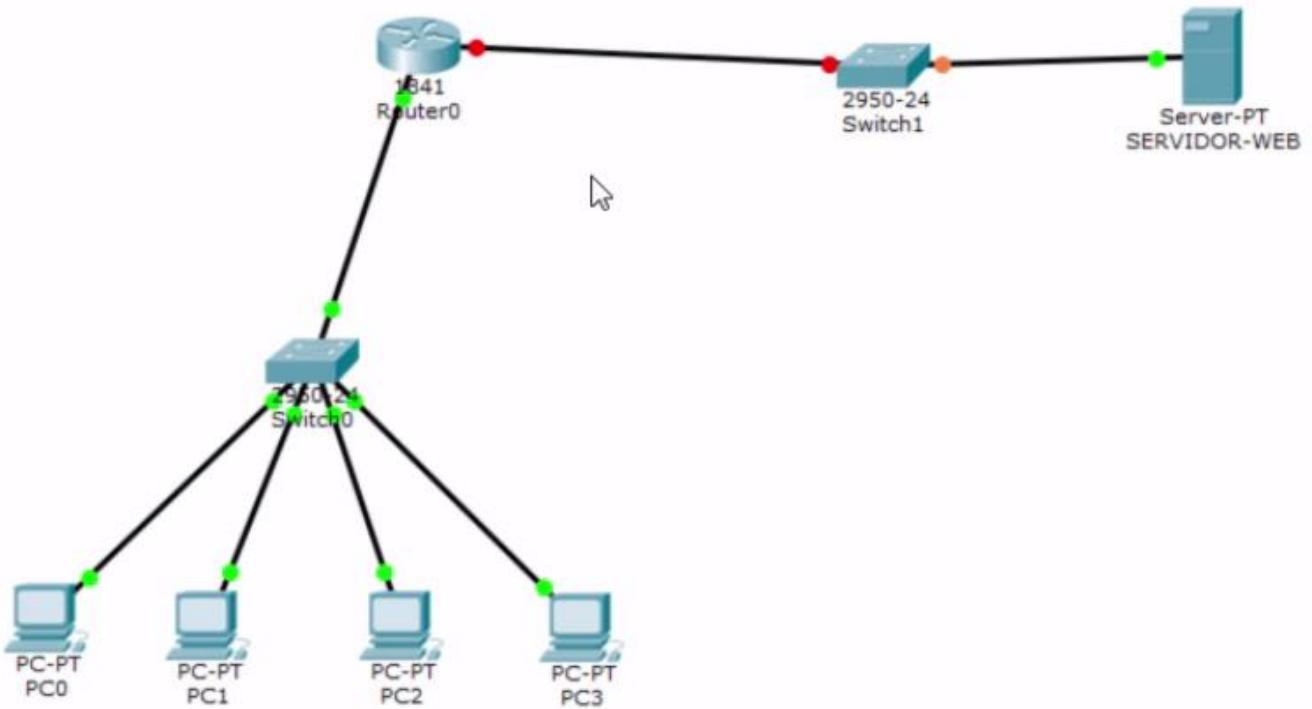
- Abra um novo projeto, arraste para área de trabalho 4 computadores, 1 Switch e 1 roteador. Como fizemos na aula.
- Interconecte todos os computadores com o switch e o switch com o roteador.
- Configure o roteador para alocar endereços IP que estão na rede *192.168.0.0* (Lembre-se: é necessário criar um pool de endereços com um nome, informar o endereço de rede, habilitar a porta e configurar endereço IP na porta do roteador). Para salvar a configuração do roteador volte ao modo privilégio (Router#) pressionando "Ctrl+ Z" e depois escreva *wr*
- Mude a configuração IP dos computadores para DHCP e veja se os endereços IP estão de fato sendo alocados.

A configuração do roteador deverá estar parecida com os dados abaixo:

```
ip dhcp pool ALURA
network 192.168.0.0 255.255.255.0
default-router 192.168.0.1
!
interface FastEthernet0/0
ip address 192.168.0.1 255.255.255.0
duplex auto
```

Acessando o Google

Agora, a nossa missão será que os usuários acessem o site do Google. Esperamos que ao digitarmos o endereço do site no Web Browser do Packet Tracer, apareça a página do Google. Vale lembrar que estamos usando um software de simulação e que os computadores do projeto não estão conectados em uma rede de verdade. Precisaremos adicionar ao projeto o servidor web do Google e um Switch, que serão conectados com um cabo direto. Depois, será a vez de conectarmos o Switch e o Router.

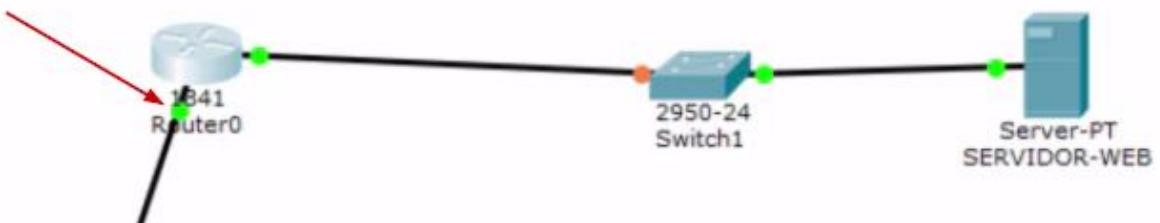


Assim como habilitamos as portas para a rede de usuários, teremos que habilitar as portas para que o servidor seja acessado.

Vamos voltar para a linha de comando. Para configurarmos efetivamente o terminal, usaremos o comando `configure terminal` para que ele entre na parte de configuração global. Depois, queremos habilitar a interface. Usaremos o comando `no shutdown`.

```
Router#configure terminal
Enter configuration commands, one per line. End with CNTL.
Router(config)#interface fastEthernet 0/1
Router(config-if)#no shutdown
```

A porta do roteador já estará habilitada.



Em seguida, configuraremos um endereço IP para a porta:

```
Router(config-if)#ip address ?
```

Usarmos a `?` para que ele informe o que precisaremos preencher. Vamos colocar um endereço estático, usando 8.8.8.1 (que é da classe A).

```
Router(config-if)#ip address 8.8.8.1
```

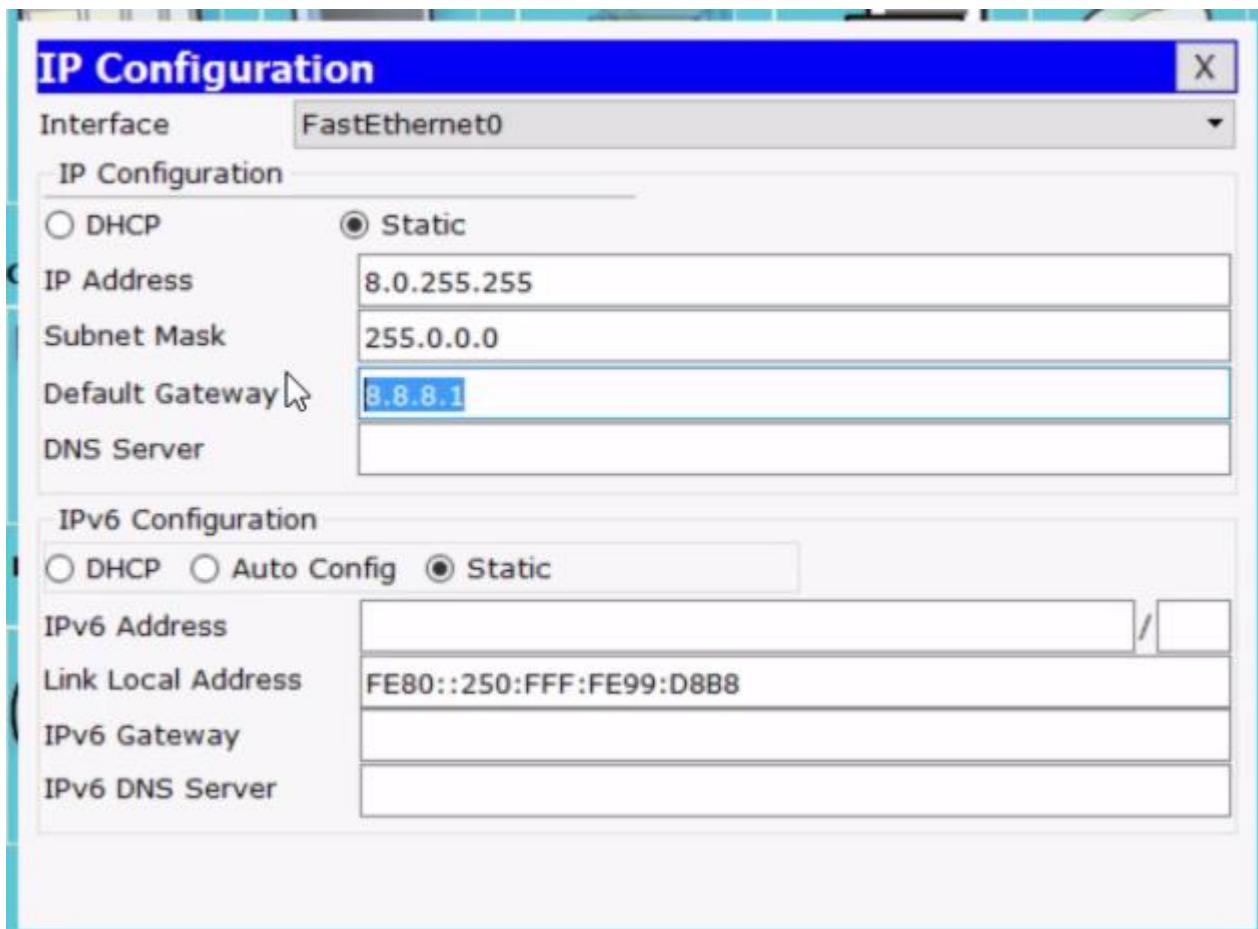
Adicionaremos a máscara de subrede.

```
Router(config-if)#ip address 8.8.8.1 255.0.0.0
```

Configuramos o roteador, agora, o processo será feito nos servidores.

Vamos clicar no ícone do servidor web do projeto e vamos até a parte de "IP Configuration". Qualquer IP que esteja entre 8.0.0.0 e 8.255.255.255 será válido. Para o servidor usaremos o IP 8.0.255.255.

O Default Gateway será 8.8.8.1.



Como somos também o administrador da página do Google, iremos editá-la para que ela fique apresentável para o usuário. Para isto clicaremos em "Services", depois em "HTTP" e selecionaremos a edição do arquivo index.html.



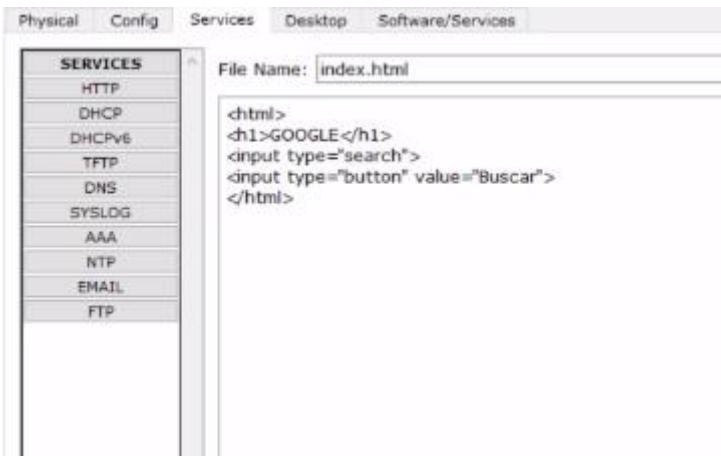
Nós iremos apagar a informação que está dentro do HTML. Em seguida, adicionaremos a tag `h1`, a barra de pesquisa e o botão de buscar.

```
<html>
<h1>GOOGLE</h1>
```

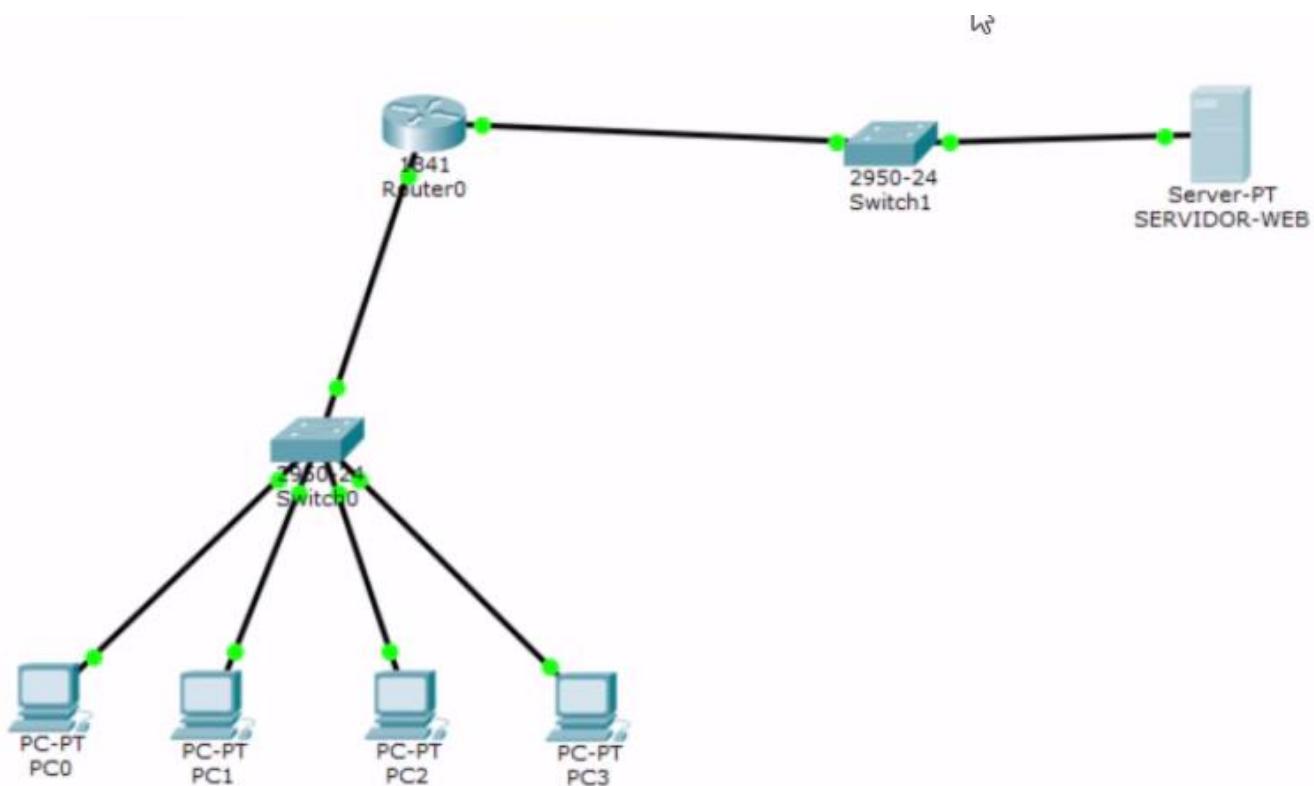
```

<input type="search">
<input type="button" value="Buscar">
</html>

```

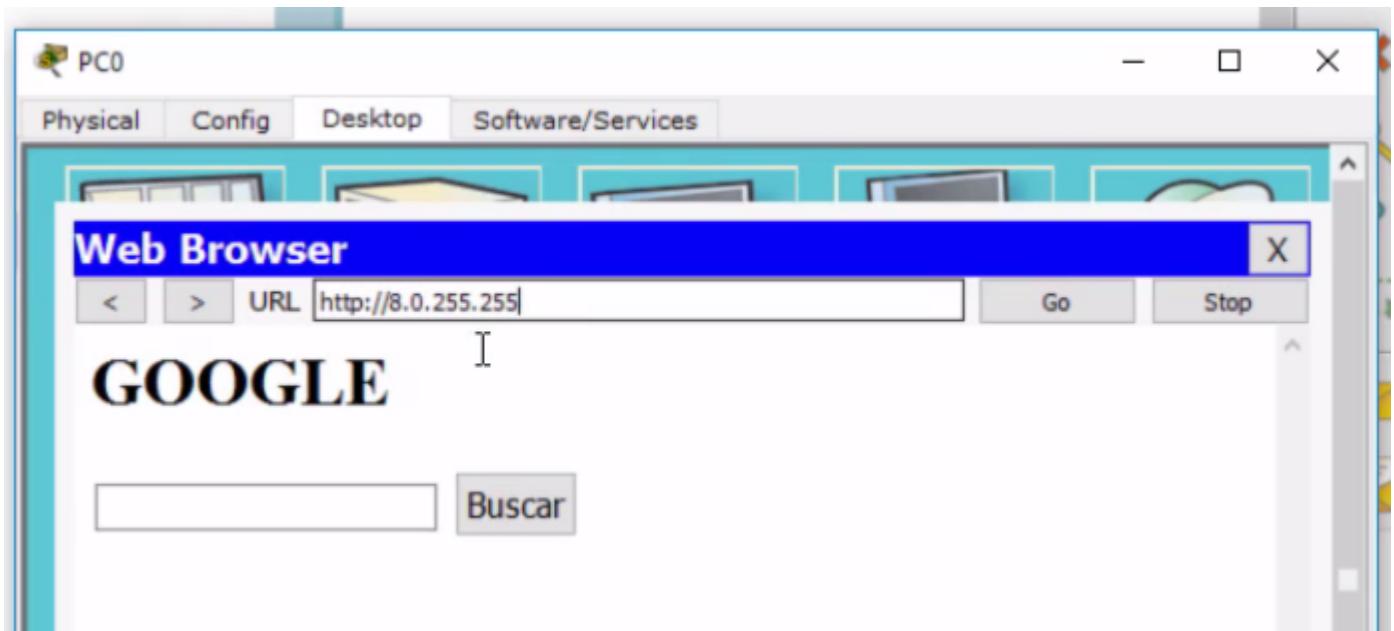


Configuramos o roteador para atuar como DHCP da rede de usuários e ele foi configurado para ter um IP estático.



As duas redes já sabem qual é o portão de saída e podem ser comunicar entre si. Vamos fazer o teste.

No Web Browser, colocaremos o endereço IP que colocamos para o servidor: 8.0.255.255.



Acessamos a página do Google. Mas não é normal colocarmos endereços IPs na barra do navegador. Geralmente, colocamos a URL que será traduzida para o endereço IP. Vamos fazer a parte da configuração do servidor DNS logo a seguir.

Mãos à obra: Configurando o servidor do google

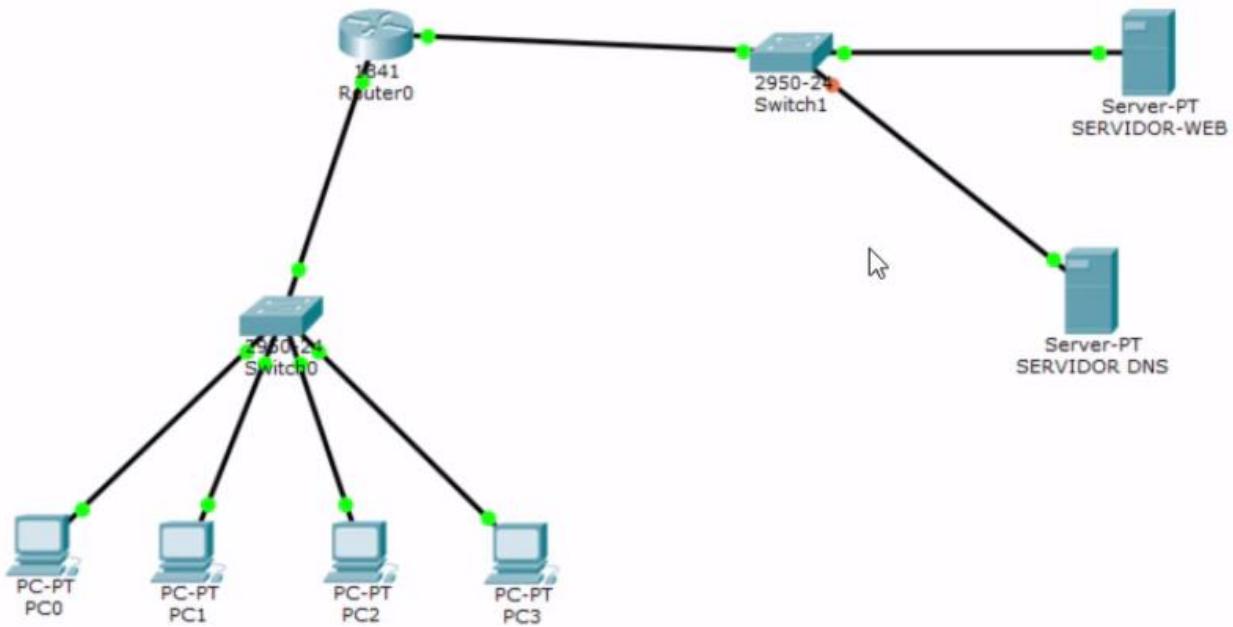
- Arraste para área de trabalho 1 servidor que será onde faremos a configuração de nossa máquina do google e arraste também 1 switch para interconectar o servidor com o roteador.
- Clique no servidor > Aba Services> HTTP > Clicar em edit do index.html e inserir o código:
 - <h1>GOOGLE</h1>
 - <input type="search">
 - <input type="button" value="Buscar">
- Na aba Desktop selecionar IP Configuration e colocar um IP fixo para esse servidor e seu respectivo default gateway.
 - Configure o IP no roteador e faça um teste de conectividade. Para salvar a configuração do roteador volte ao modo de privilégio (Router#) pressionando o botão Ctrl z, posteriormente digite wr

A configuração do roteador deve estar próxima a esta abaixo:

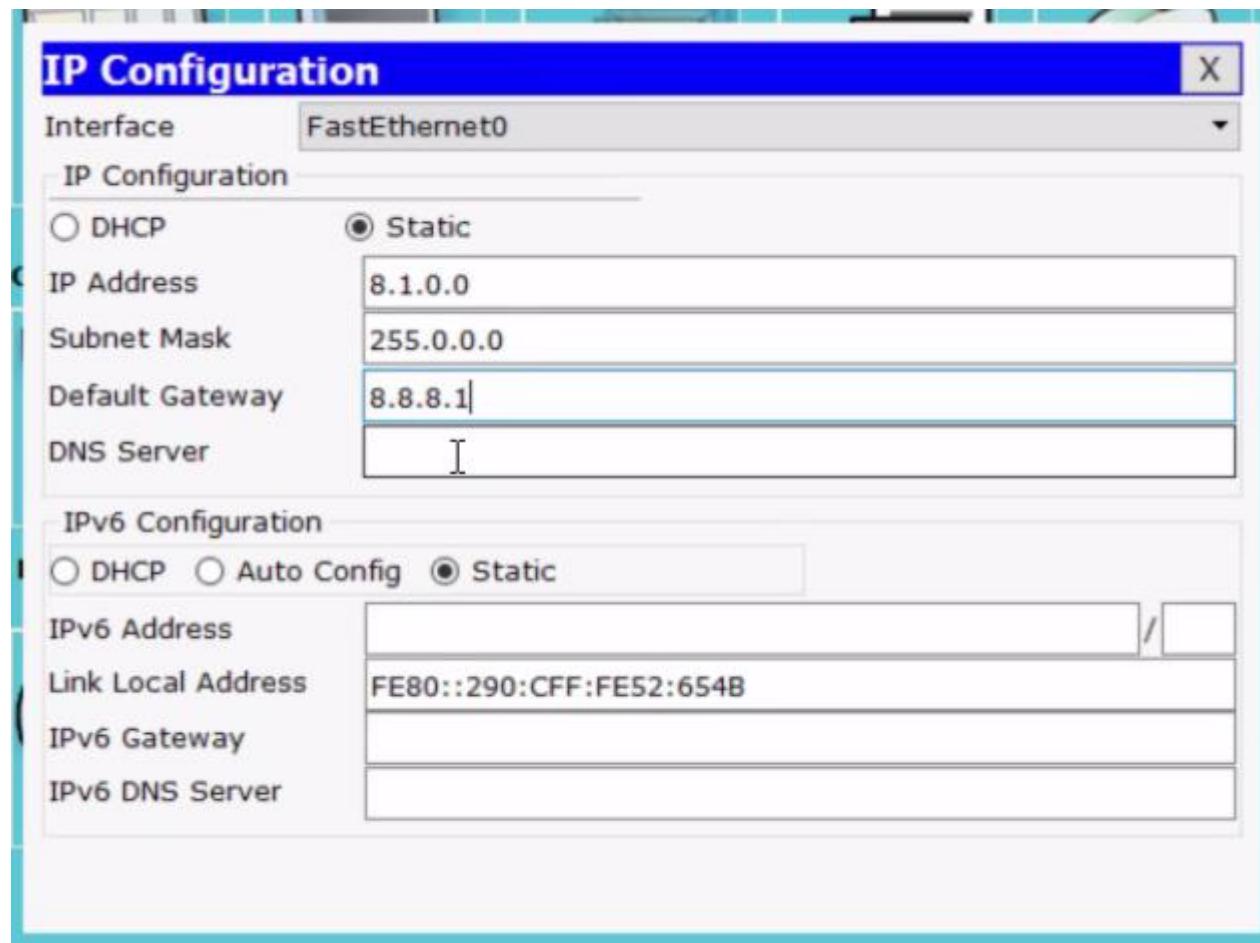
```
ip dhcp pool ALURA
network 192.168.0.0 255.255.255.0
default-router 192.168.0.1
!
interface FastEthernet0/0
ip address 192.168.0.1 255.255.255.0
duplex auto
speed auto
!
interface FastEthernet0/1
ip address 8.8.8.1 255.0.0.0
duplex auto
speed auto
```

Acessando o Google DNS

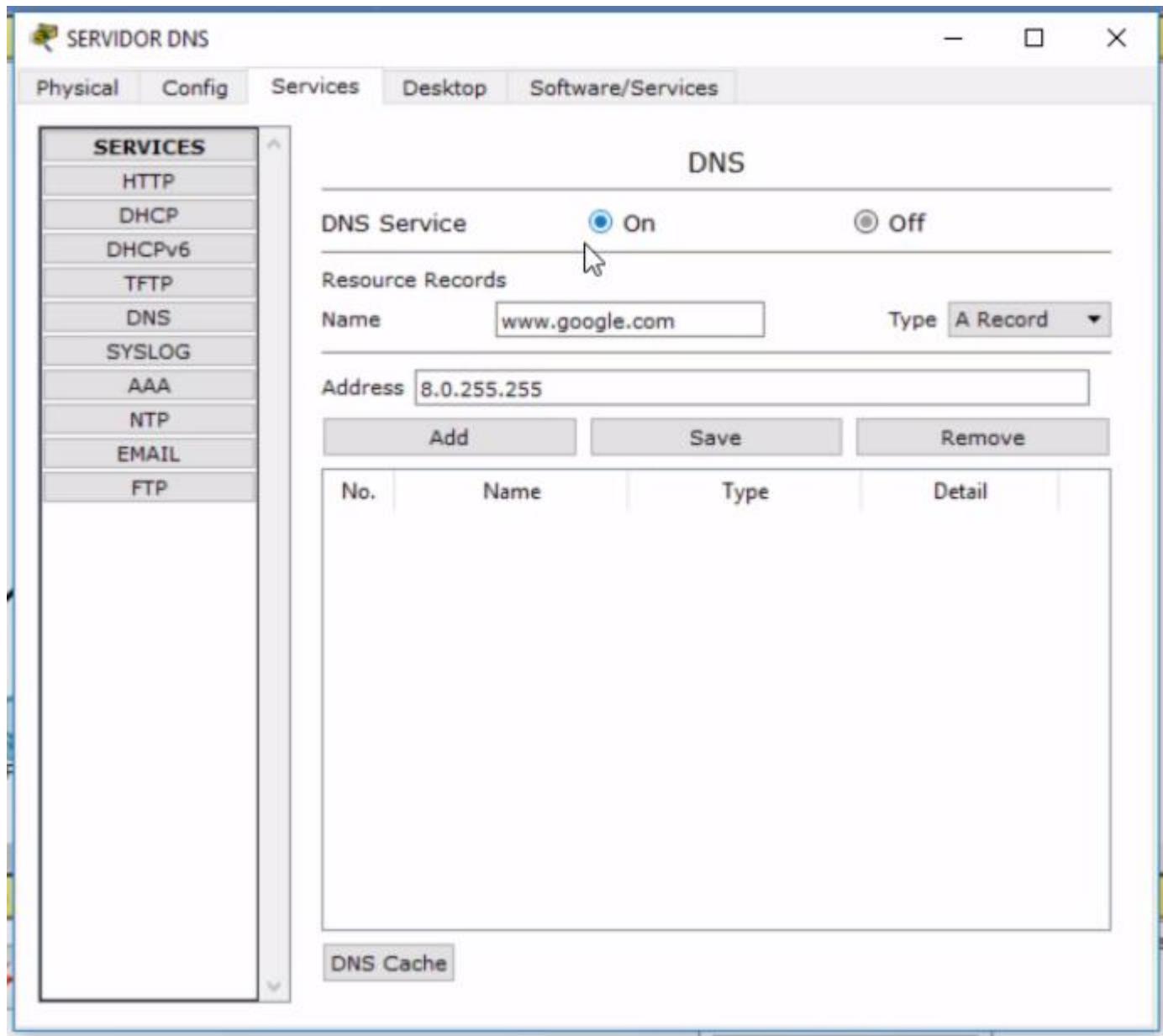
Vamos colocar o servidor DNS para fazer a tradução entre a URL www.google.com e o endereço IP máquina do Google. Adicionaremos o servidor DNS ao nosso projeto:



Nós conectamos o novo servidor ao Switch. Em seguida, iremos configurá-lo. Primeiramente, iremos atribuir um endereço IP da classe A. Faremos isso na parte de IP Configuration.



Nós inserimos também o número da máscara e do gateway. Em seguida, criaremos o mapeamento entre o Google e o servidor Web. Para isto iremos em "Services" -> "DNS", e digitaremos a URL do site e iremos vincula-la ao IP do Servidor Web.

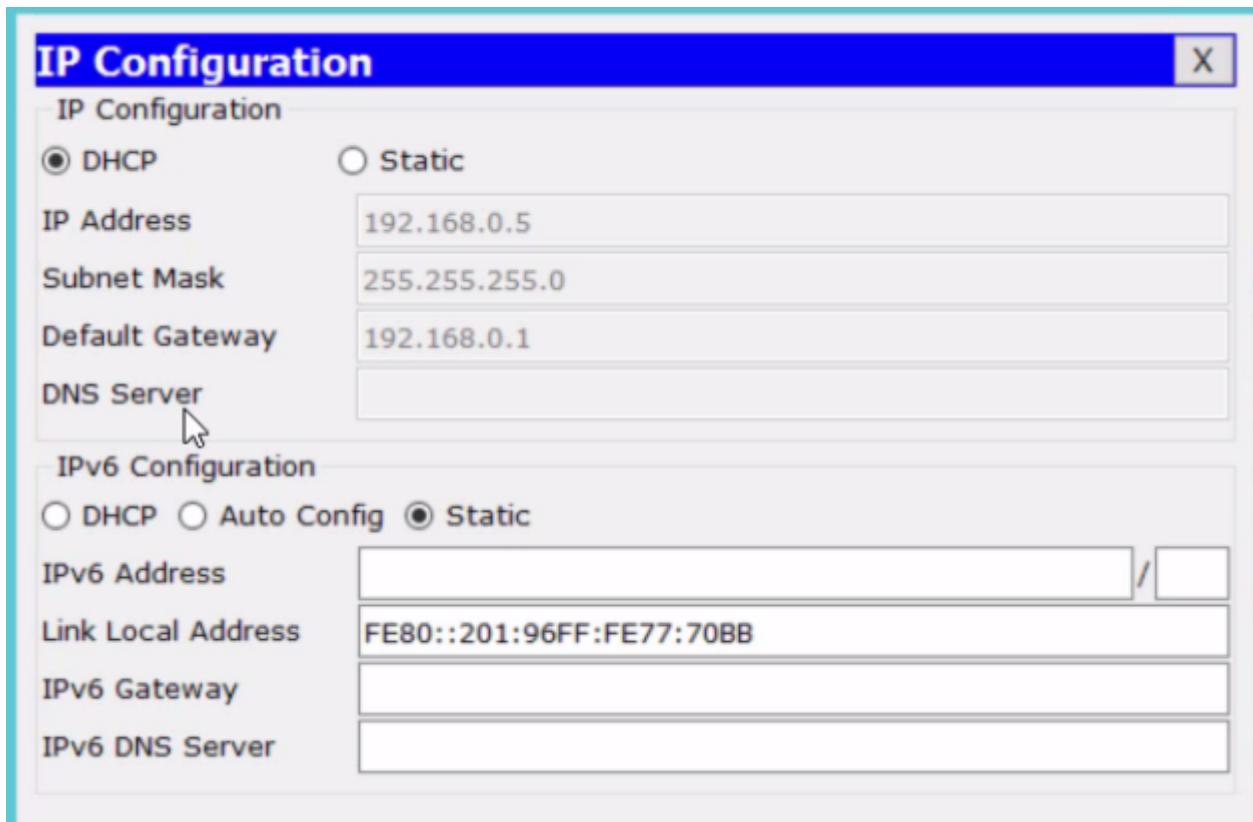


E habilitaremos o servidor DNS clicando em "On" e depois, em adicionar.

Esperamos que ao clicarmos no computador e digitarmos a URL do Google no Web Browser, apareça a respectiva página. Mas se fizermos o teste, veremos que a página ficou em branco.



Por que a página não foi aberta? Voltaremos à parte de IP Configuration para resolvemos o assunto.



O computador não sabe qual é o servidor DNS que ele deve procurar. Como estamos usando o DHCP, pediremos que ele informe aos usuários qual servidor DNS será utilizado.

Na linha de comando, usaremos o comando `enable` e depois, `configure terminal` para habilitar.

```
Router>enable  
Router#configure terminal
```

```
Router>enable  
Router#  
Router#  
Router#  
Router#configure terminal  
Enter configuration commands, one per line. End with CNTL/Z.  
Router(config)#
```

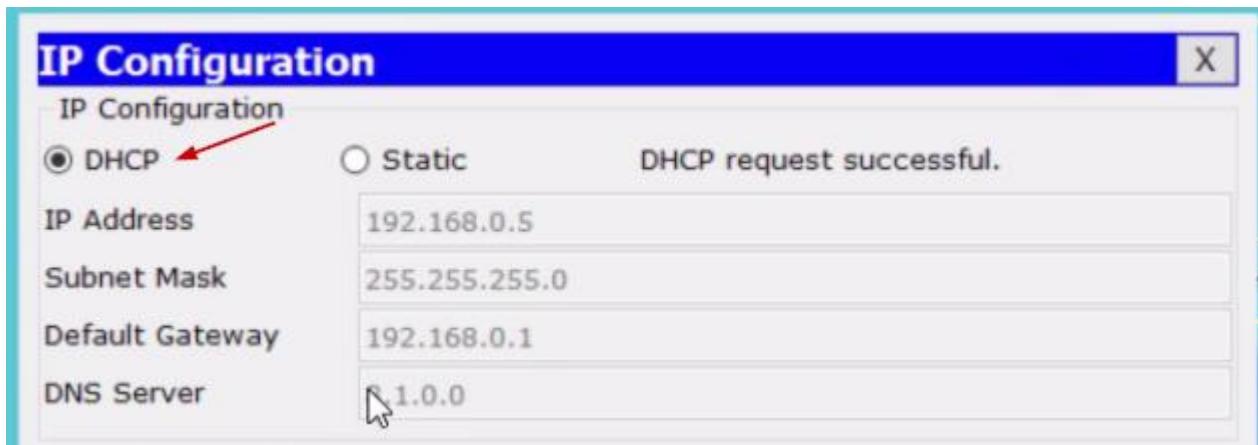
Voltaremos à parte do DHCP, para colocarmos o servidor DHCP que os computadores terão que colocar. Nós usamos o nome ALURA, se usou outro nome, deverá usar o escolhido por você.

```
Router(config)#ip dhcp pool ALURA
```

Adicionaremos a ? para lembrar do comando. Precisaremos utilizar o `dns-server`, juntamente com o IP do servidor DNS.

```
Router(dhcp-config)#dns-server 8.1.0.0
```

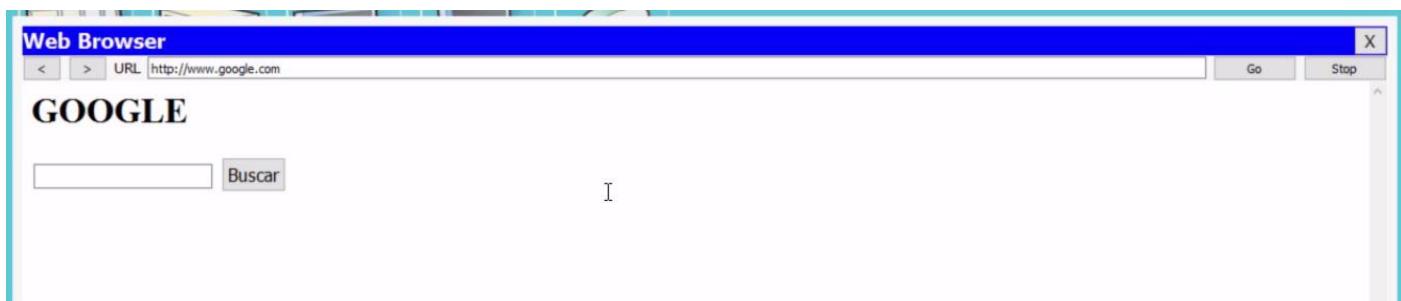
Faremos um `refresh` nos computadores, para que eles usem a nova configuração. No IP configuration, mudaremos para o modo "Static" e retornar logo em seguida, para DHCP.



Agora, ele sabe qual é o servidor DNS.

Teremos que repetir o processo para todos os quatro computadores: mudar para "Static" e voltar para "DHCP".

Faremos um novo teste no Web Browser e ver se conseguimos acessar a página do Google usando a URL.



Conseguimos! E se repetirmos o teste nas demais máquinas, conseguiremos o mesmo resultado.

Montamos o nosso projeto e todos os usuários conseguem acessar o serviço do Google.

Que configurações fizemos no projeto para que fosse possível que os computadores digitassem www.google.com no browser e tivéssemos a página do google na tela?

- Tivemos que configurar o servidor DNS no DHCP do roteador para atribuir esse endereço do DNS para as máquinas (clientes).

Os computadores não sabem quem é o servidor DNS, nós precisamos informar para eles quem é o servidor que eles devem procurar.

Mãos à obra: Configurando servidor DNS

- Abra o browser de um dos computadores (Aba Desktop -> Web browser) e coloque na url o endereço IP do servidor do google. Nesse momento deveremos ver a página que configuramos
- Insira um novo servidor. Vá até a aba Services, clique em DNS e habilite o serviço. Posteriormente coloque nome: www.google.com e o endereço IP respectivo ao endereço IP do servidor do google que foi configurado na etapa anterior. Não se esqueça de configurar o endereço IP e default gateway desse servidor.
- Clique no roteador, volte ao pool dhcp configure o servidor DNS para o endereço IP que foi configurado no servidor DNS. Para salvar a configuração do roteador, volte ao modo privilégio (Router#) apertando o botão Ctrl z, digitando posteriormente wr

- Nos computadores mude para estático e volte para DHCP para que o computador faça assim uma nova requisição.
- Abrir o browser em todos os computadores e digitar: www.google.com e deveremos ver a tela do google \o/

A configuração do roteador deverá estar parecida com a abaixo:

```
ip dhcp pool ALURA
network 192.168.0.0 255.255.255.0
default-router 192.168.0.1
dns-server 8.1.0.0
!
interface FastEthernet0/0
ip address 192.168.0.1 255.255.255.0
duplex auto
speed auto
!
interface FastEthernet0/1
ip address 8.8.8.1 255.0.0.0
duplex auto
speed auto
!
end
```

Conclusão

Parabéns! Chegamos agora ao fim do curso de Redes da Alura. Falamos sobre diversos temas, cabos de rede, Hub, Switch, roteadores. Nos aprofundamos sobre o endereçamento do IPv4 e ainda têm mais coisas para aprendermos.

Mas espero que o conteúdo visto no curso ajude bastante no seu crescimento profissional.

Vamos nessa...

Links úteis:

<http://docente.ifrn.edu.br/docente/rodrigotertulino>