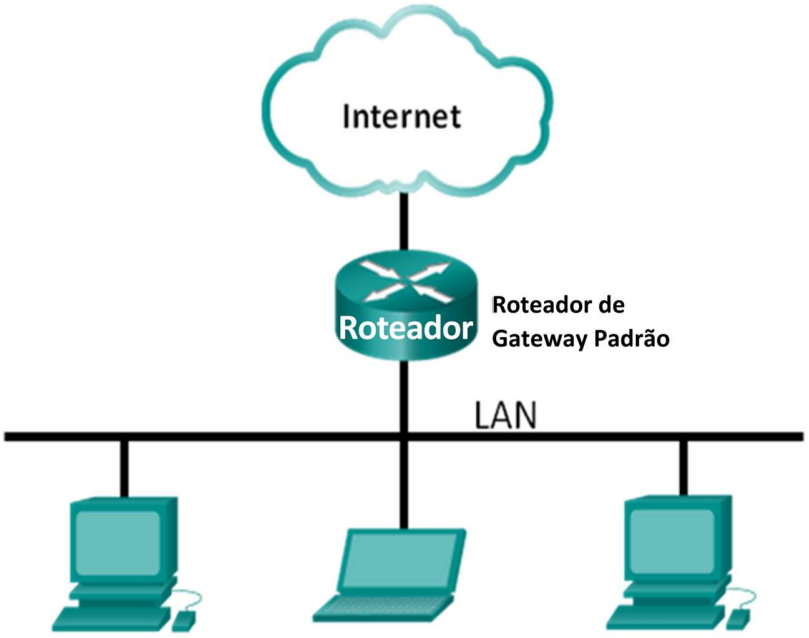
Laboratório - Uso do Wireshark para visualizar o tráfego de rede

Topologia



Objetivos

Parte 1: Capturar e analisar dados locais ICMP no Wireshark

Parte 2: Capturar e analisar dados remotos ICMP no Wireshark

Histórico/cenário

O Wireshark é um software analisador de protocolo, ou aplicação "packet sniffer", usado para solução de problemas de rede, análise, desenvolvimento de software e protocolo, e educação.

Recursos necessários

- 1 PC (Windows 10 com acesso à Internet)
- Serão usados outros PCs em uma rede local (LAN) para responder às solicitações de ping.

Parte 1: Capturar e analisar dados locais ICMP no Wireshark

Na parte 1 deste laboratório, você efetuará ping para outro computador na LAN e capturará solicitações e respostas ICMP no Wireshark. Você também verá quadros capturados para obter informações específicas. Essa análise ajudará a esclarecer como os cabeçalhos dos pacotes são usados para transportar os dados até o destino.

Etapa 1: Recuperar os endereços de interface do PC.

Neste laboratório, você precisará recuperar o endereço IP do PC e o endereço físico da placa de interface de rede (NIC), também chamado de endereço MAC.

a. Abra uma janela de comando, digite **ipconfig /all**, e pressione Enter.

b. Observe o Endereço IP da interface do PC, a descrição e o endereço MAC (físico).

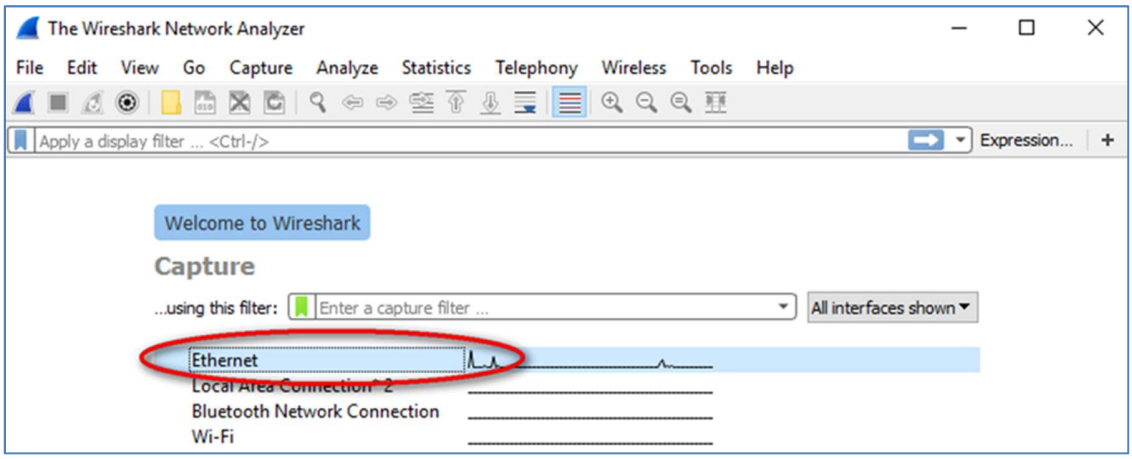
```
Microsoft Windows [Version 10.0.16299.64]
(c) 2017 Microsoft Corporation. All rights reserved.

C:\> ipconfig /all

Windows IP Configuration

   Host Name . . . . . . . . . . . . : DESKTOP-C73CB0M
   Primary Dns Suffix  . . . . . . . :
   Node Type . . . . . . . . . . . . : Hybrid
   IP Routing Enabled. . . . . . . . : No
   WINS Proxy Enabled. . . . . . . . : No

Ethernet adapter Ethernet:

   Connection-specific DNS Suffix  . :
   Description . . . . . . . . . . . : Intel(R) 82577LM Gigabit Network Connection
   Physical Address. . . . . . . . . : 00-26-B9-DD-00-91
   DHCP Enabled. . . . . . . . . . . : Yes
   Autoconfiguration Enabled . . . . : Yes
   Link-local IPv6 Address . . . . . : fe80::d809:d939:110f:1b7f%20(Preferred)
   IPv4 Address. . . . . . . . . . . : 192.168.1.147(Preferred)
   Subnet Mask . . . . . . . . . . . : 255.255.255.0
   Default Gateway . . . . . . . . . : 192.168.1.1
   DHCP Server . . . . . . . . . . . : 192.168.1.1
```

c. Solicite a um ou mais membros da equipe o endereço IP do PC dele e forneça a ele o endereço IP do seu PC. Não forneça o seu endereço MAC a ele agora.

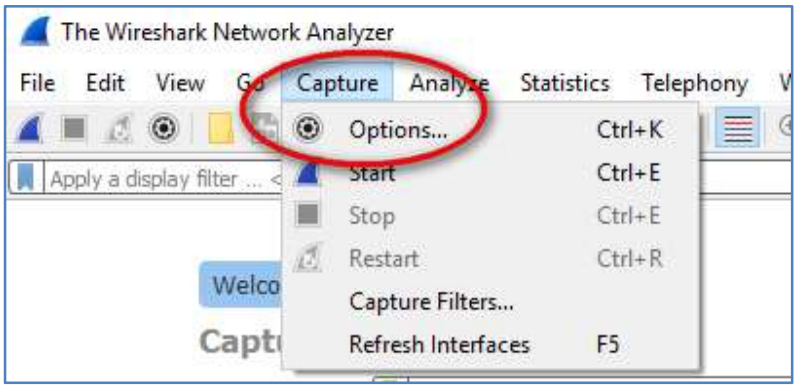
Etapa 2: Iniciar o Wireshark e começar a capturar os dados.

a. Em seu computador, clique no botão **Iniciar** do Windows para ver o Wireshark listado como um dos programas no menu pop-up. Clique duas vezes em **Wireshark**.

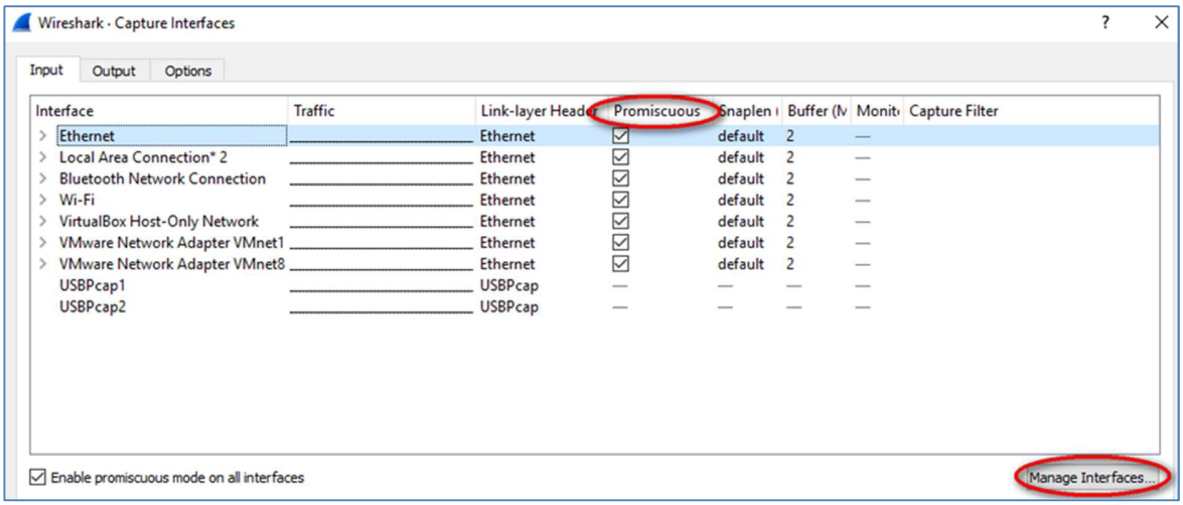
b. Após iniciar o Wireshark, clique na interface de captura para utilizá-lo. Como estamos usando a conexão Ethernet com fio no PC, verifique se a opção de Ethernet está na parte superior da lista.



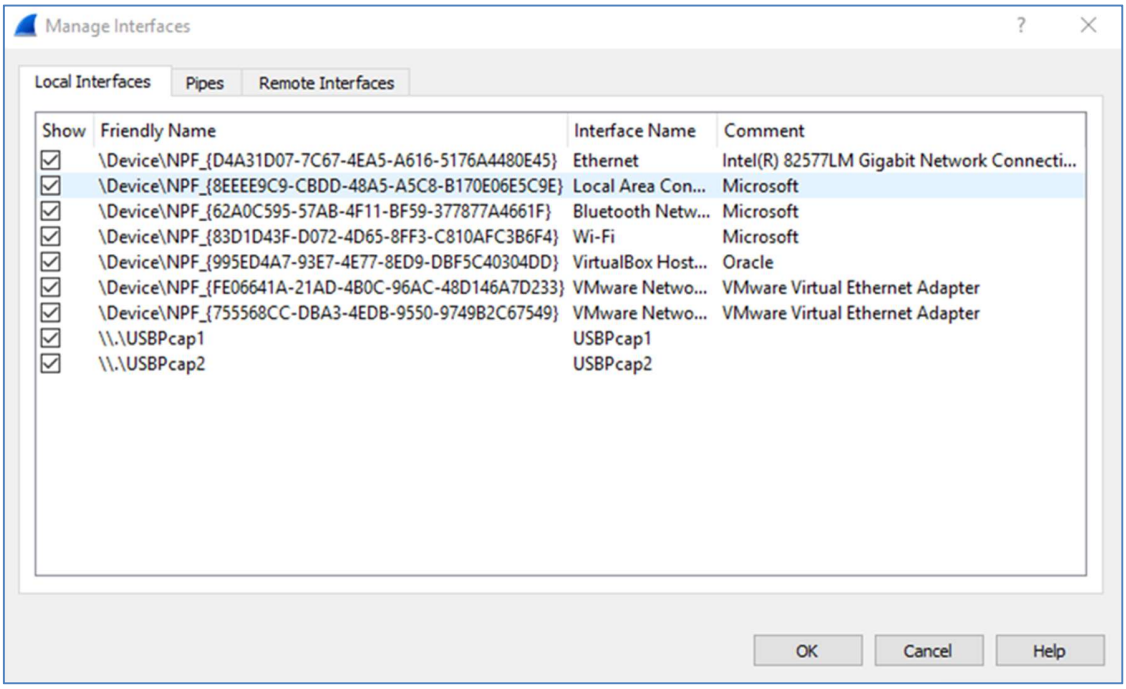
Você pode gerenciar a interface de captura clicando em **Capture** (Capturar) e **Options** (Opções):



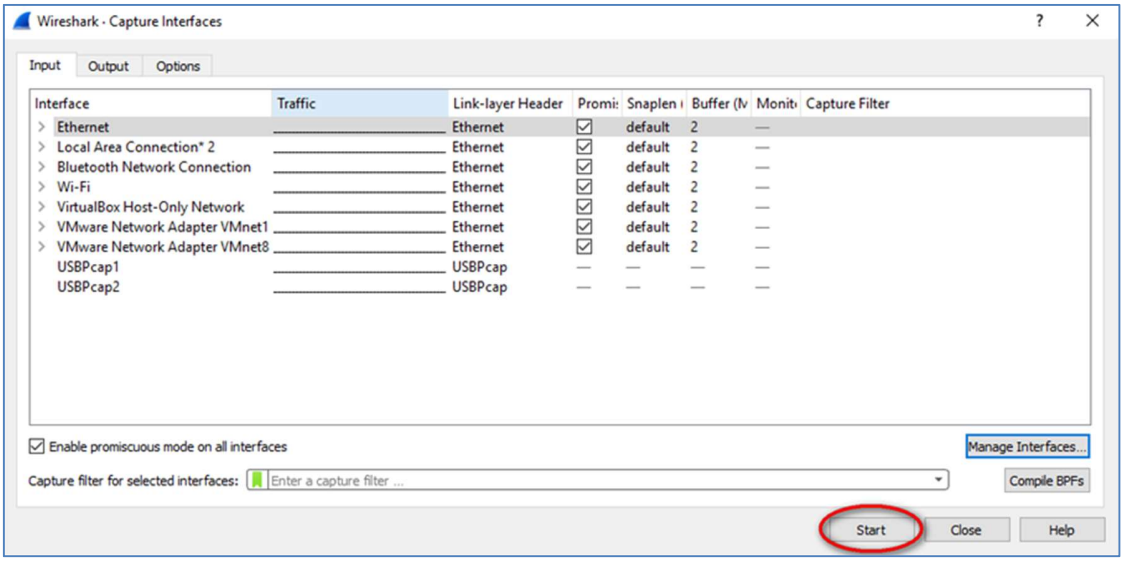
c. É exibida uma lista de interfaces. Verifique se a interface de captura está marcada em **Promiscuous** (Promíscua).



Observação: podemos ainda gerenciar as interfaces no PC, clicando em **Manage Interfaces** (Gerenciar Interfaces). Verifique se a descrição corresponde ao que você observou na etapa 1b. Feche a janela **Manage Interfaces** (Gerenciar interfaces) após verificar a interface correta.

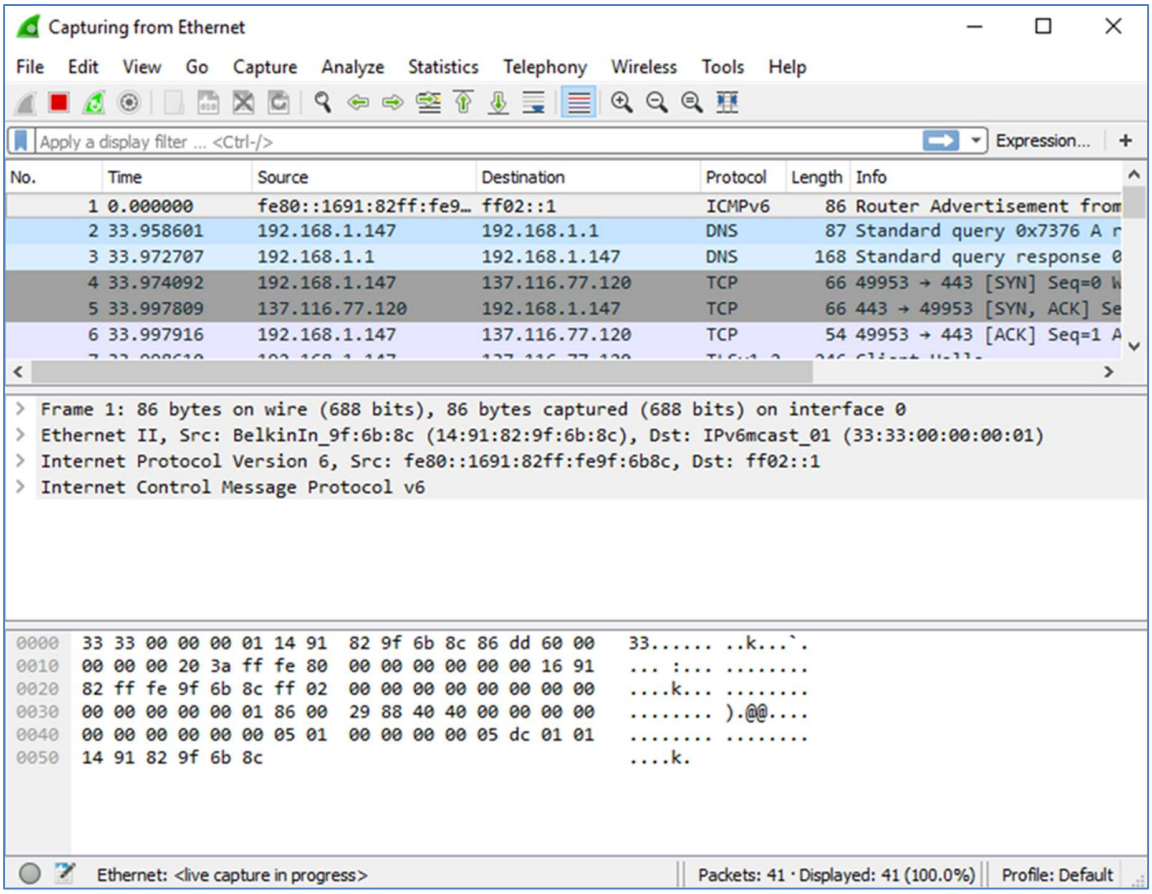


d. Depois de verificar a interface correta, clique em **Start** (Iniciar) para iniciar a captura de dados.

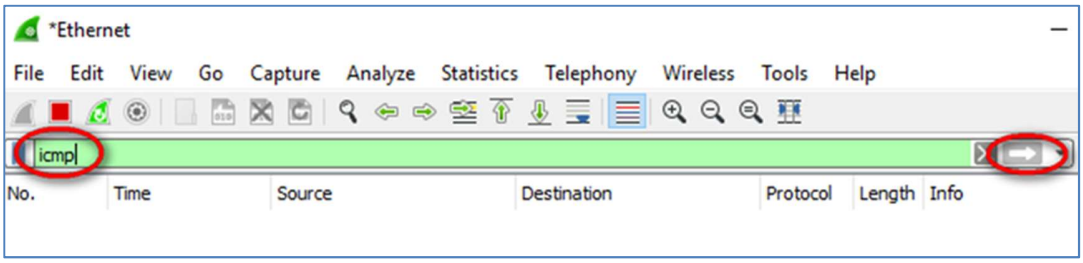


Observação: você também pode iniciar a captura de dados clicando no ícone **Wireshark** da interface principal.

As informações começarão a rolar abaixo da seção superior no Wireshark. As linhas de dados serão exibidas em cores diferentes com base no protocolo.



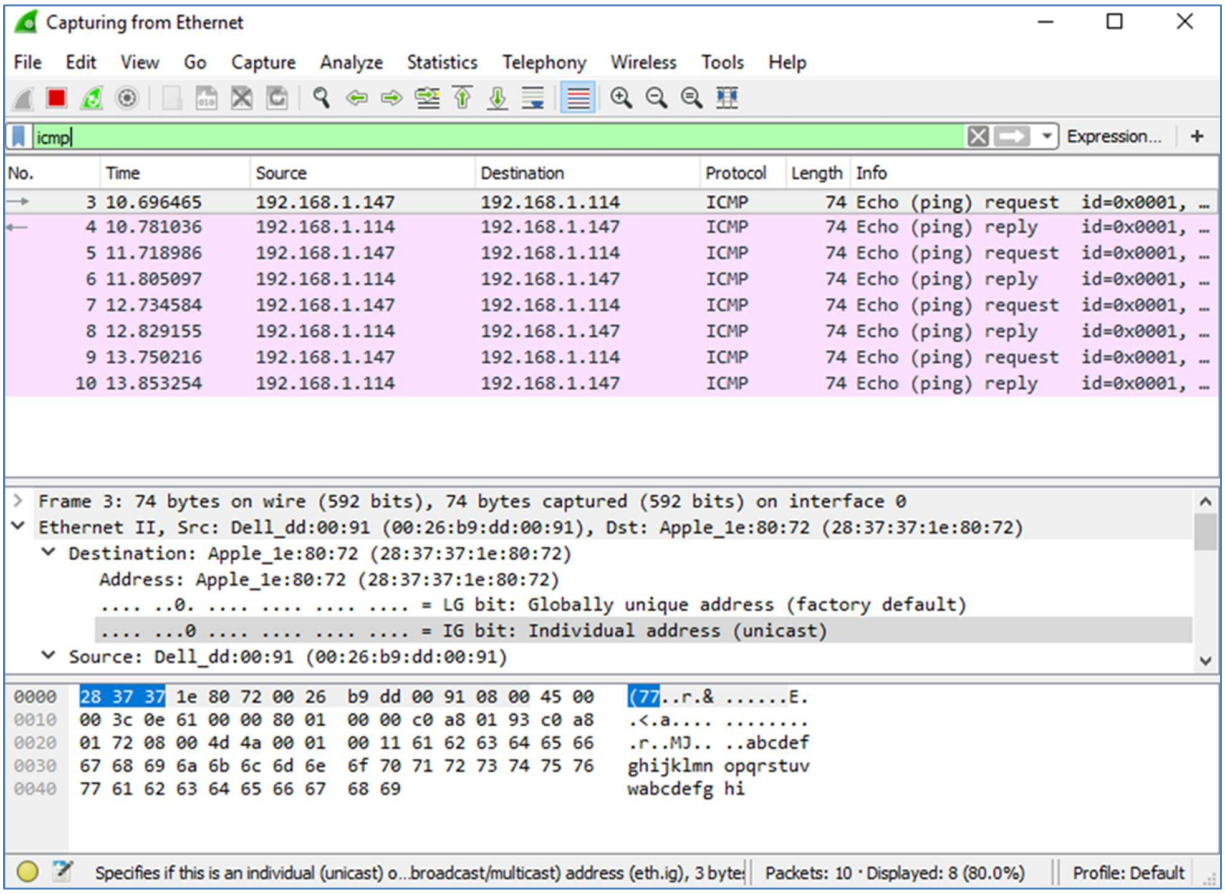
e. Essas informações podem passar rapidamente dependendo da comunicação que estiver ocorrendo entre o PC e a LAN. Podemos aplicar um filtro para facilitar a visualização e o trabalho com os dados que estão sendo capturados pelo Wireshark. Neste laboratório, estamos apenas interessados em exibir as PDUs do ICMP (ping). Digite **icmp** na caixa **Filter** (Filtro), na parte superior do Wireshark, e pressione **Enter** ou clique no botão **Apply** (Aplicar) para exibir somente as PDUs ICMP (ping).



f. Este filtro faz com que todos os dados na janela superior desapareçam, mas você ainda captura o tráfego na interface. Exiba a janela do prompt de comando que você abriu anteriormente e efetue ping no endereço IP que recebeu da sua equipe.

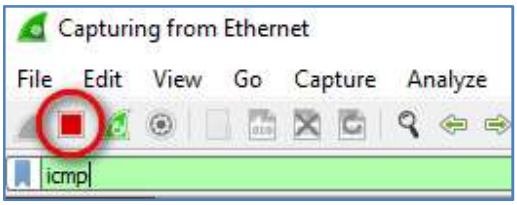
```
Microsoft Windows [Version 10.0.16299.64]
(c) 2017 Microsoft Corporation. All rights reserved.

C:\> ping 192.168.1.114

Pinging 192.168.1.114 with 32 bytes of data:
Reply from 192.168.1.114: bytes=32 time<1ms TTL=64
Reply from 192.168.1.114: bytes=32 time<1ms TTL=64
Reply from 192.168.1.114: bytes=32 time<1ms TTL=64
Reply from 192.168.1.114: bytes=32 time<1ms TTL=64

Ping statistics for 192.168.1.114:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 0ms, Maximum = 0ms, Average = 0ms
```


Observe que você começa a ver novamente os dados na janela superior do Wireshark.



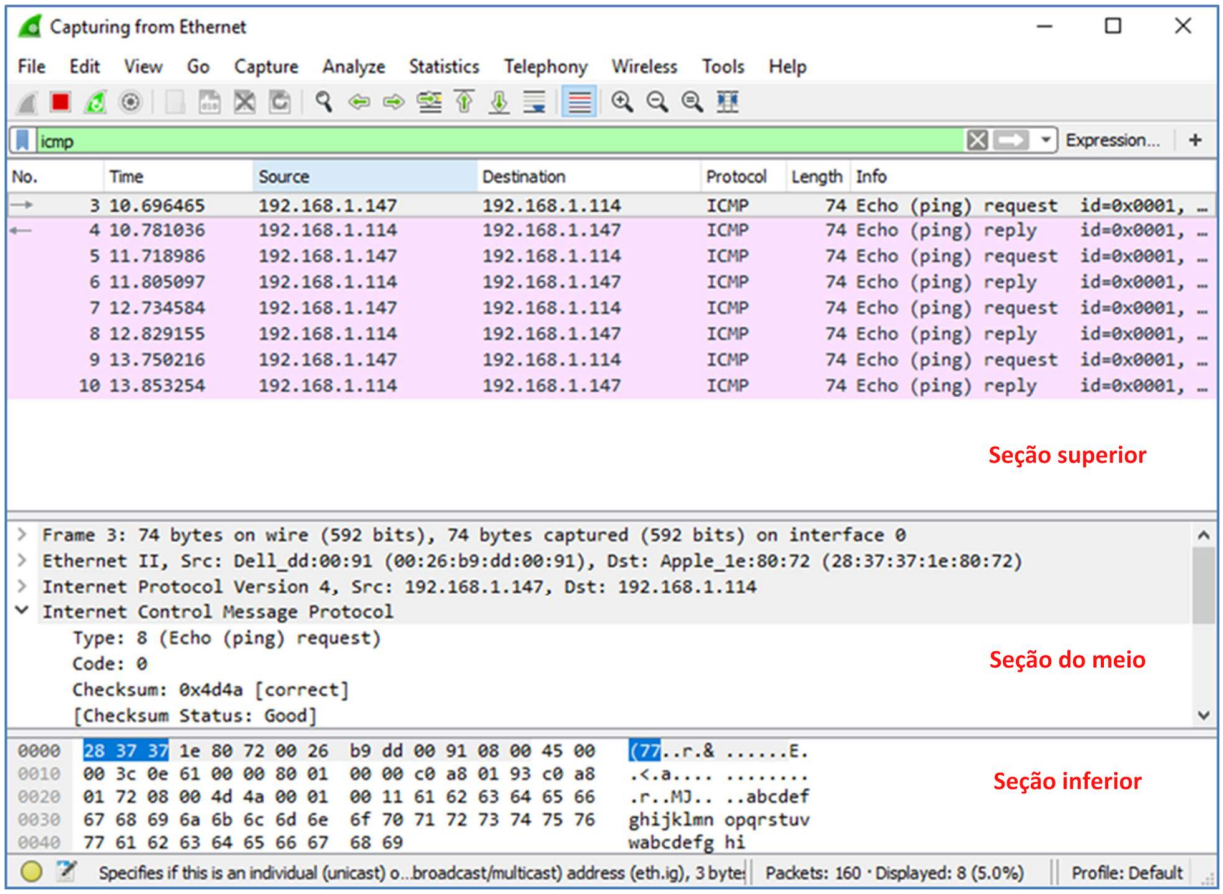
Observação: se o PC da sua equipe não responde aos pings, pode ser porque o firewall do PC do membro da equipe está bloqueando as solicitações. Consulte Anexo A: Permitir o tráfego ICMP pelo firewall para obter informações sobre como permitir o tráfego ICMP pelo firewall usando o Windows 7.

g. Pare a captura de dados clicando no ícone **Stop Capture** (Parar captura).

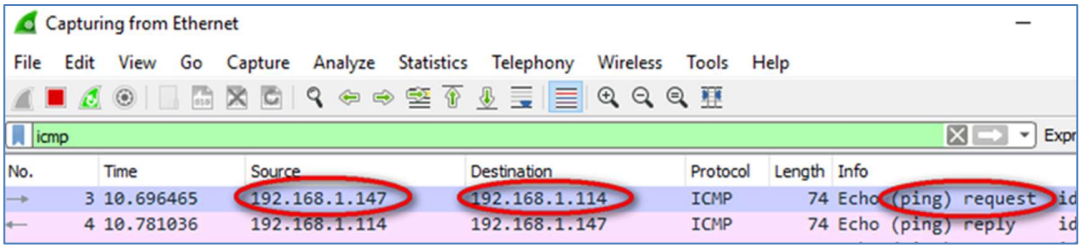


Etapa 3: Examinar os dados capturados.

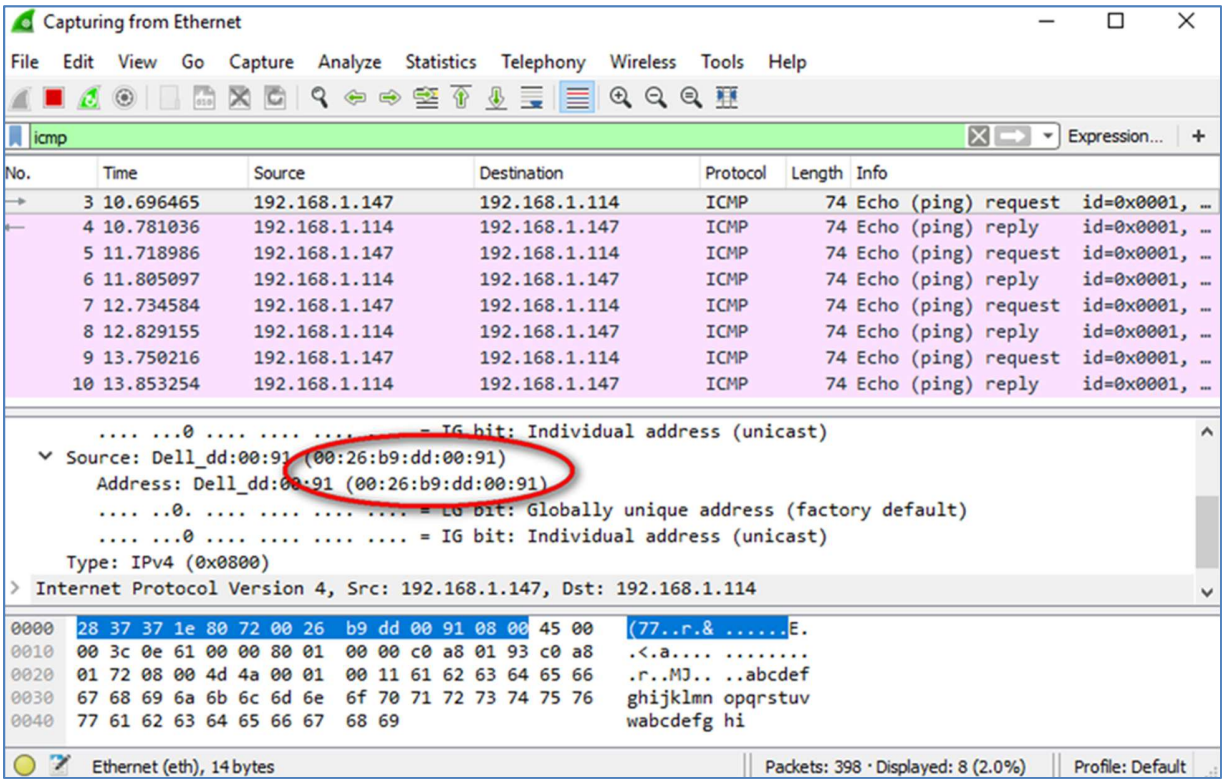
Na etapa 3, examine os dados gerados pelas solicitações ping do PC da sua equipe. Os dados do Wireshark são exibidos em três seções: 1) A seção superior exibe a lista de quadros de PDU capturada com um resumo das informações do pacote IP listadas; 2) a seção média mostra as informações de PDU para o quadro selecionado na parte superior da tela e separa um quadro PDU capturado pelas camadas de protocolo; e 3) a seção inferior exibe os dados brutos de cada camada. Os dados são exibidos em formato hexadecimal e decimal.



a. Clique nos primeiros quadros de PDU de requisição ICMP na seção da parte superior do Wireshark. Observe que a coluna **Source** (Origem) tem o endereço IP do PC, e a **Destination** (Destino) contém o endereço IP do PC do colega para o qual você efetuou ping.



b. Com esse quadro de PDU ainda selecionado na seção superior, vá até a seção média. Clique no sinal mais à esquerda da linha Ethernet II para ver os endereços MAC de origem e destino.



O endereço MAC de origem corresponde à sua interface do PC (mostrada na etapa 1)? _____ Sim

O endereço MAC de destino no Wireshark corresponde ao endereço MAC do membro de sua equipe?

_____ Sim

Como o endereço MAC do PC que recebeu ping é obtido pelo seu PC?

_____

O endereço MAC é obtido com uma requisição ARP.

Observação: no exemplo anterior de uma requisição ICMP capturada, os dados do ICMP são encapsulados dentro da PDU do pacote IPv4 (cabeçalho IPv4) que é, então, encapsulada em uma PDU do quadro Ethernet II (cabeçalho Ethernet II) para transmissão na LAN.

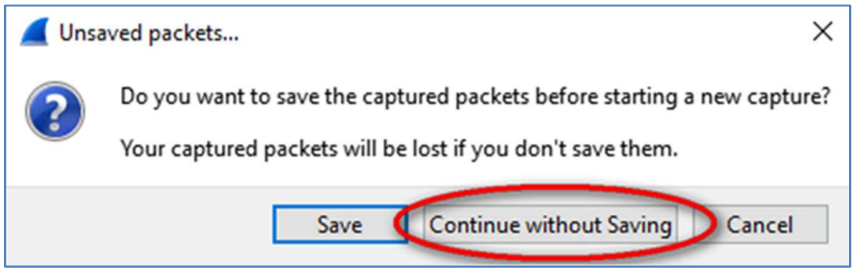
Parte 2: Capturar e analisar dados ICMP remotos no Wireshark

Na parte 2, você efetuará ping para hosts remotos (não nos hosts da LAN) e examinará os dados gerados desses pings. Você determinará o que há de diferente nesses dados a partir dos dados pesquisados na parte 1.

Etapa 1: Iniciar a captura de dados na interface.

a. Inicie a captura de dados novamente.

b. Uma janela solicitará que você salve os dados capturados anteriormente antes de iniciar outra captura. Não é necessário salvar esses dados. Clique em **Continue without Saving** (Continuar sem salvar).



c. Com a captura ativa, efetue ping nas três URLs dos sites a seguir:

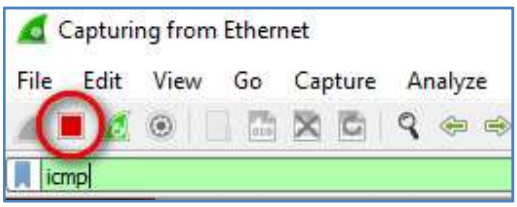
1) www.yahoo.com
2) www.cisco.com

3) www.google.com

```
C:\> ping www.yahoo.com

Pinging atsv2-fp.wg1.b.yahoo.com [98.139.180.180] with 32 bytes of data:
Reply from 98.139.180.180: bytes=32 time=43ms TTL=53
Reply from 98.139.180.180: bytes=32 time=60ms TTL=53
Reply from 98.139.180.180: bytes=32 time=43ms TTL=53
Reply from 98.139.180.180: bytes=32 time=42ms TTL=53

Ping statistics for 98.139.180.180:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 42ms, Maximum = 60ms, Average = 47ms

C:\> ping www.cisco.com

Pinging e2867.dsca.akamaiedge.net [23.13.155.188] with 32 bytes of data:
Reply from 23.13.155.188: bytes=32 time=20ms TTL=56
Reply from 23.13.155.188: bytes=32 time=21ms TTL=56
Reply from 23.13.155.188: bytes=32 time=19ms TTL=56
Reply from 23.13.155.188: bytes=32 time=19ms TTL=56

Ping statistics for 23.13.155.188:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 19ms, Maximum = 21ms, Average = 19ms

C:\> ping www.google.com

Pinging www.google.com [216.58.194.100] with 32 bytes of data:
Reply from 216.58.194.100: bytes=32 time=56ms TTL=54
Reply from 216.58.194.100: bytes=32 time=56ms TTL=54
Reply from 216.58.194.100: bytes=32 time=55ms TTL=54
Reply from 216.58.194.100: bytes=32 time=57ms TTL=54

Ping statistics for 216.58.194.100:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 55ms, Maximum = 57ms, Average = 56ms

C:\>
```

Observação: quando você efetuar ping nas URLs listadas, observe que o Servidor de Nomes de Domínio (DNS) converte a URL em um endereço IP. Observe o endereço IP recebido para cada URL.

d. Pare a captura de dados clicando no ícone **Stop Capture** (Parar captura).



Etapa 2: Examinar e analisar os dados dos hosts remotos.

a. Analise os dados capturados no Wireshark e examine os endereços IP e MAC dos três locais para onde você efetuou ping. Liste os endereços IP e MAC de destino para todos os três locais no espaço fornecido.

1° Local: IP: _____._____._____._____ MAC: ____:____:____:____:____:____

2° Local: IP: _____._____._____._____ MAC: ____:____:____:____:____:____

3° Local: IP: _____._____._____._____ MAC: ____:____:____:____:____:____

Endereços IP: 98.139.180.180, 23.13.155.188, 216.58.194.100 (esses endereços IP podem variar)

Endereço MAC: é o mesmo para todos os três locais. É o endereço físico da interface LAN de gateway padrão do roteador.

b. Qual é a importância dessas informações?

_____

Os endereços MAC dos três locais são os mesmos.

c. Como essas informações diferem das informações do ping local que você recebeu na parte 1?

_____

_____

Um ping para um host local retorna o endereço MAC da placa de rede do PC. Um ping para um host remoto retorna o endereço MAC da interface LAN do gateway padrão.

Reflexão

Por que o Wireshark mostra o endereço MAC real dos hosts locais, mas não o endereço MAC real para os hosts remotos?

_____

_____

Como os endereços MAC para hosts remotos não são conhecidos na rede local, o endereço MAC do gateway padrão é usado. Depois que o pacote chegar ao roteador gateway padrão, as informações da Camada 2 são removidas do pacote e um novo cabeçalho da Camada 2 é anexado ao endereço MAC de destino do roteador do próximo salto.

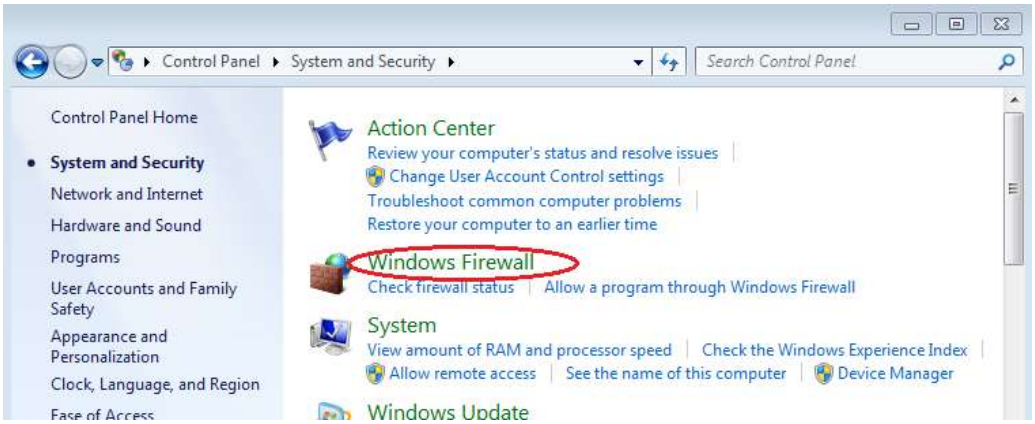
Anexo A: Permitir o tráfego ICMP pelo firewall

Se os membros de sua equipe não conseguirem efetuar ping em seu PC, o firewall pode estar bloqueando essas solicitações. Este anexo descreve como criar uma regra no firewall para permitir requisições ping. Também descreve como desativar a nova regra ICMP depois que você tiver concluído o laboratório.

Etapa 1: Criar uma regra de entrada nova permitindo o tráfego ICMP pelo firewall.

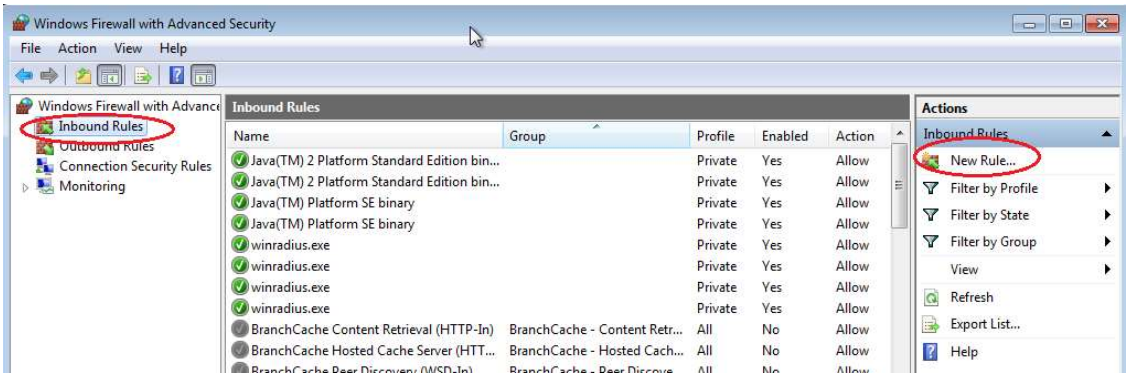
a. No **Painel de controle**, clique na opção **Sistema e Segurança**.

b. Na janela **Sistema e segurança**, clique em **Firewall do Windows**.

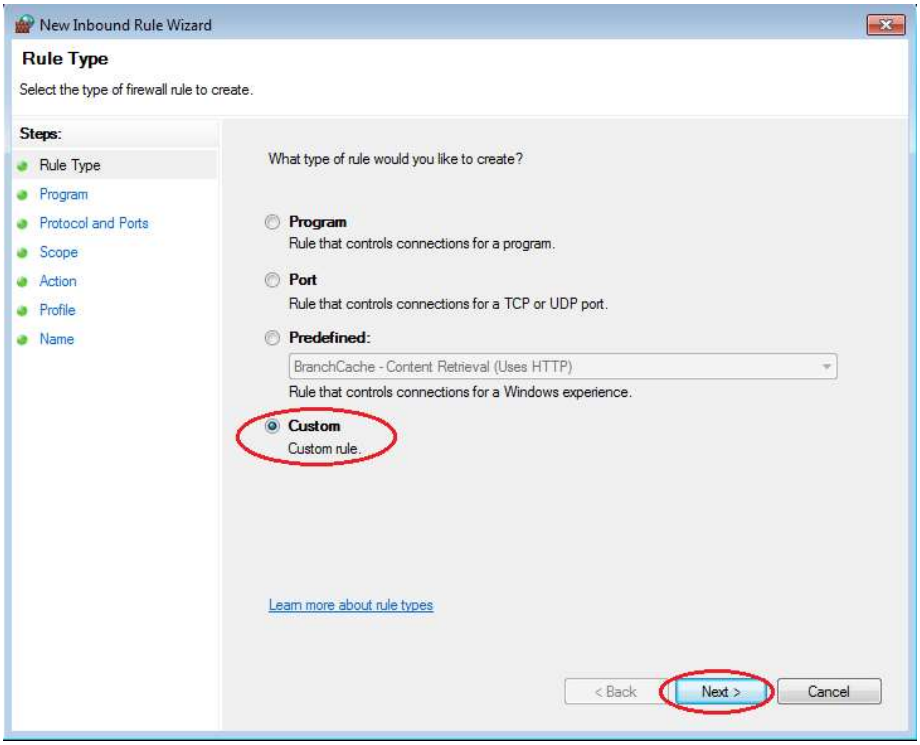


c. No painel esquerdo da janela **Firewall do Windows**, clique em **Configurações avançadas**.

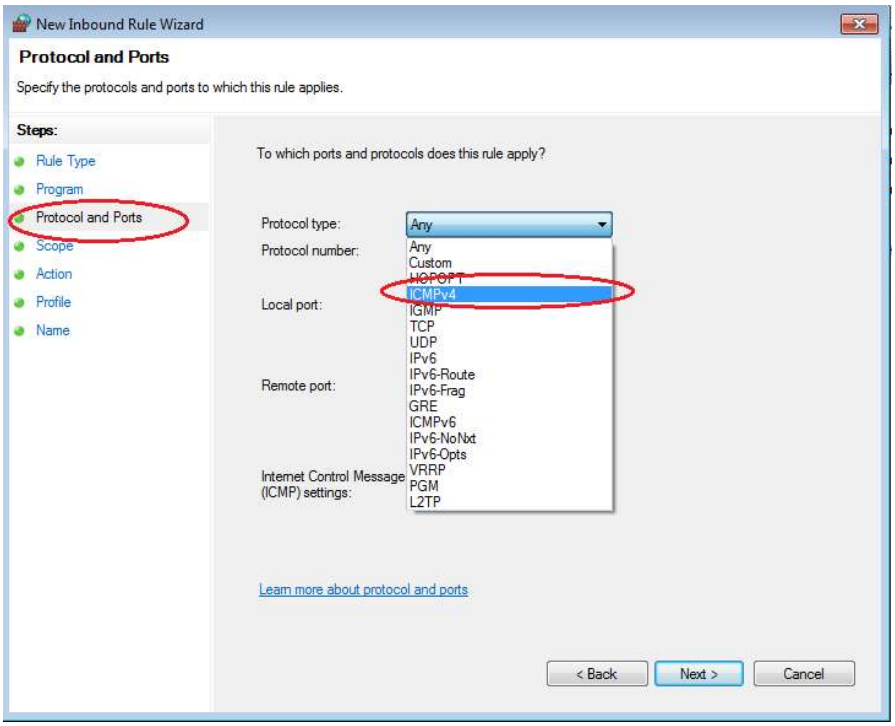
d. Na janela **Segurança avançada**, selecione a opção **Regras de entrada** na barra lateral esquerda e clique em **Nova regra…** na barra lateral direita.



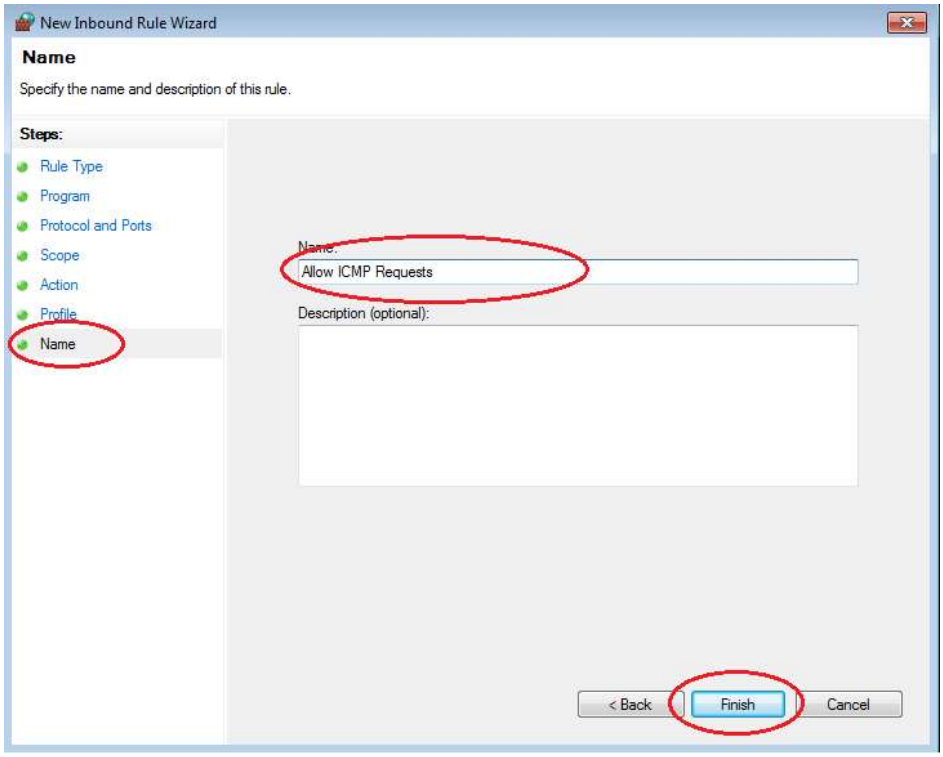
e. Isso inicia o assistente **Nova regra de entrada**. Na tela **Tipo de regra**, clique no botão de opção **Personalizar** e em **Avançar**



f. No painel esquerdo, clique na opção **Protocolo e portas** e, usando o menu suspenso **Tipo de protocolo**, selecione **ICMPv4** e clique em **Avançar**.



g. No painel esquerdo, clique na opção **Nome** e, no campo **Nome**, digite **Permitir requisições ICMP**. Clique em **Concluir**.

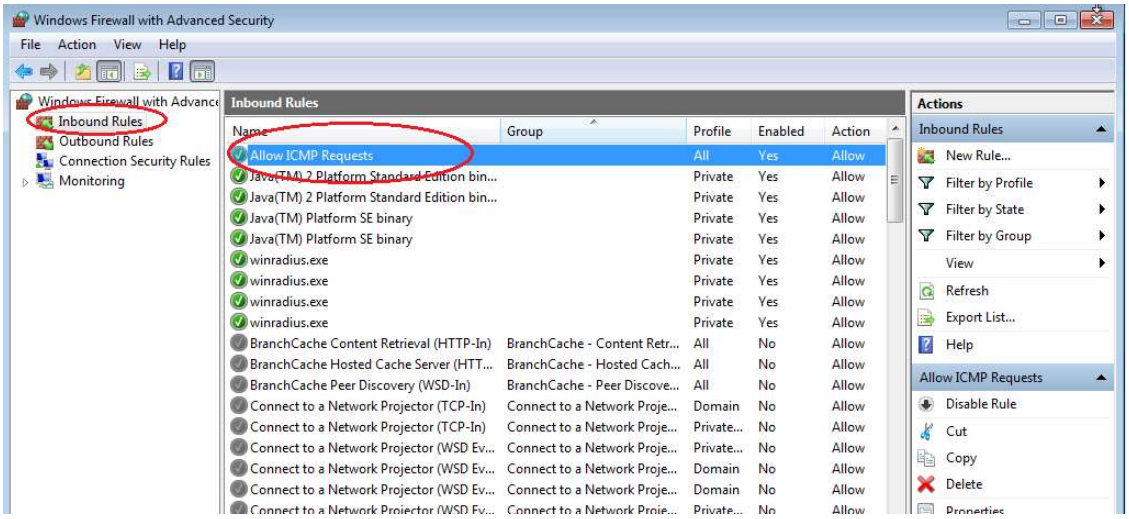


Essa nova regra deve permitir que os membros da equipe recebam respostas de ping vindo do seu PC.

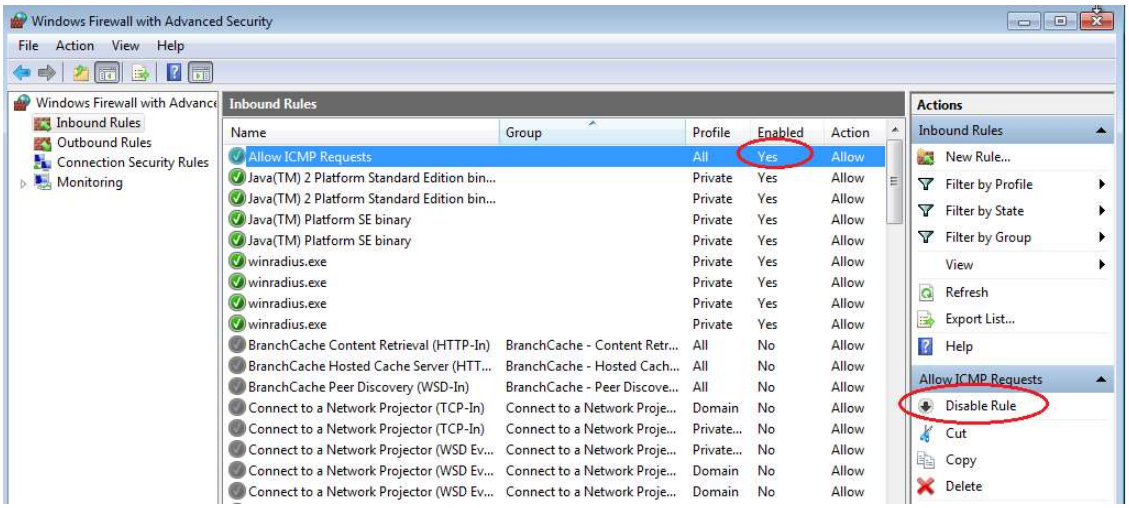
Etapa 2: Desativar ou excluir a nova regra do ICMP.

Após o laboratório ser concluído, talvez você queira desativar ou até mesmo excluir a nova regra criada na etapa 1. Usar a opção **Desativar regra** permite que posteriormente a regra seja ativada de novo. Excluir a regra permanentemente a exclui da lista de regras de entrada.

a. Na janela **Segurança avançada**, clique em **Regras de entrada** no painel esquerdo e localize a regra criada na etapa 1.



b. Para desativar a regra, clique na opção **Desativar regra**. Ao escolher essa opção, você a verá mudar para **Ativar regra**. Você pode alternar entre **Desativar regra** e **Ativar regra**; o status da regra também é exibido na coluna **Ativado** na lista de **Regras de entrada**.



c. Para excluir permanentemente a regra do ICMP, clique em **Excluir**. Se você selecionar essa opção, você pode recriar a regra novamente para permitir respostas ICMP.