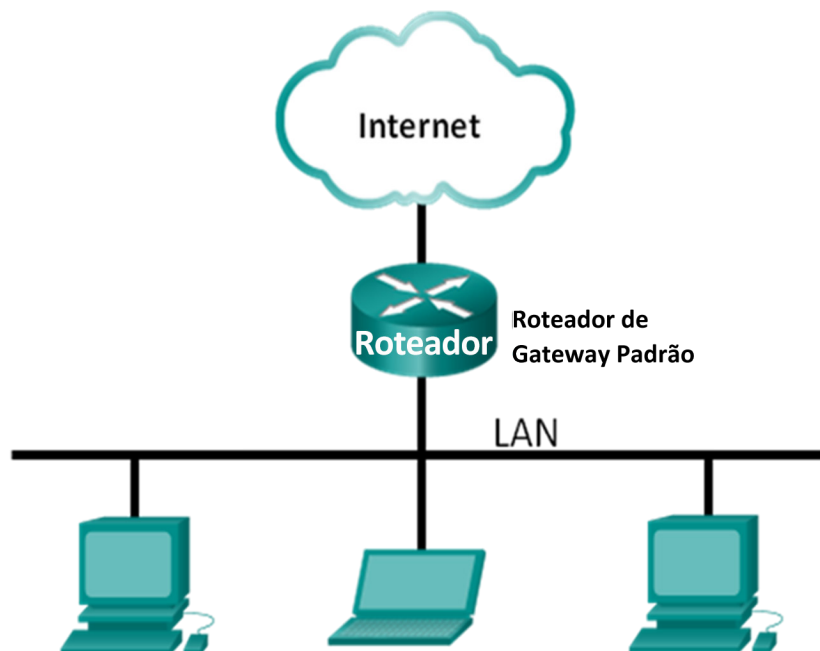


Laboratório - Uso do Wireshark para Visualizar o Tráfego de Rede

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. À medida que o fluxo de dados viaja em uma rede, o sniffer "captura" cada unidade de dados de protocolo (PDU) e pode decodificar e analisar seu conteúdo de acordo com o RFC apropriado ou com outras especificações.

O Wireshark é uma ferramenta útil para quem trabalha com redes e pode ser usado com a maioria dos laboratórios nos cursos CCNA para análise de dados e solução de problemas. Neste laboratório, você usará o Wireshark para capturar endereços IP do pacote de dados ICMP e endereços MAC do quadro Ethernet.

Recursos necessários

- 1 PC (Windows 7, 8 ou 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 seus 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.

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

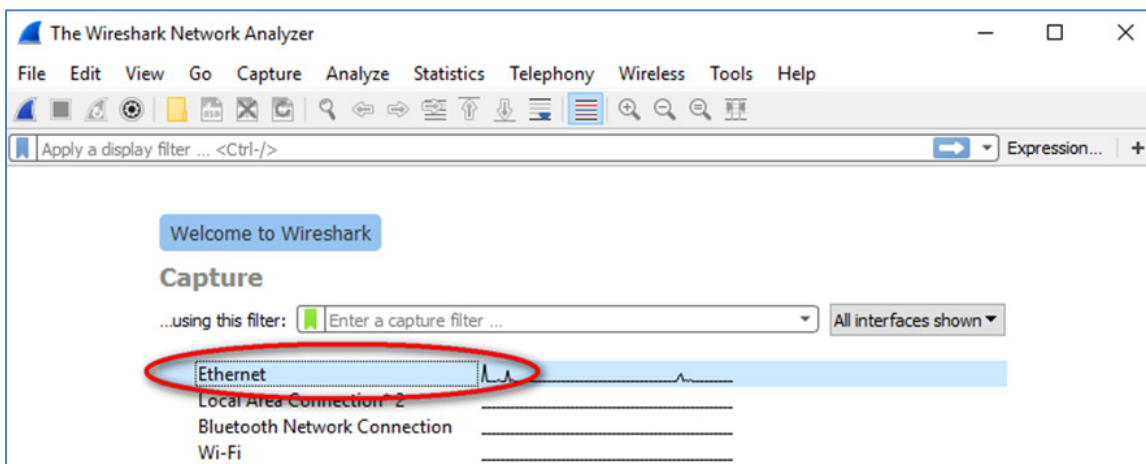
Connection-specific DNS Suffix . :
Description . . . . . : Intel(R) 82577LM Gigabit Network Connection
Physical Address. . . . . : 00-26-B9-DD-00-91
DHCP Enabled. . . . . : Yes
Autoconfiguration Enabled . . . . : Yes
Link-local IPv6 Address . . . . . : fe80::d809:d939:110f:1b7f%20(Preferred)
IPv4 Address.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

- 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.

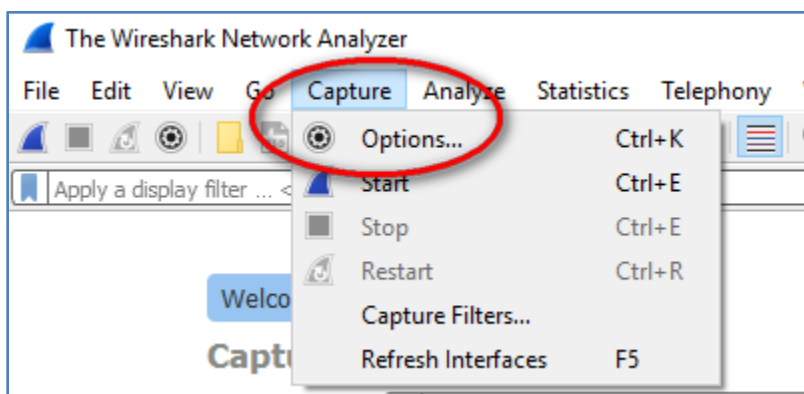
Etapa 2: Iniciar o Wireshark e começar a capturar os dados.

- 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**.

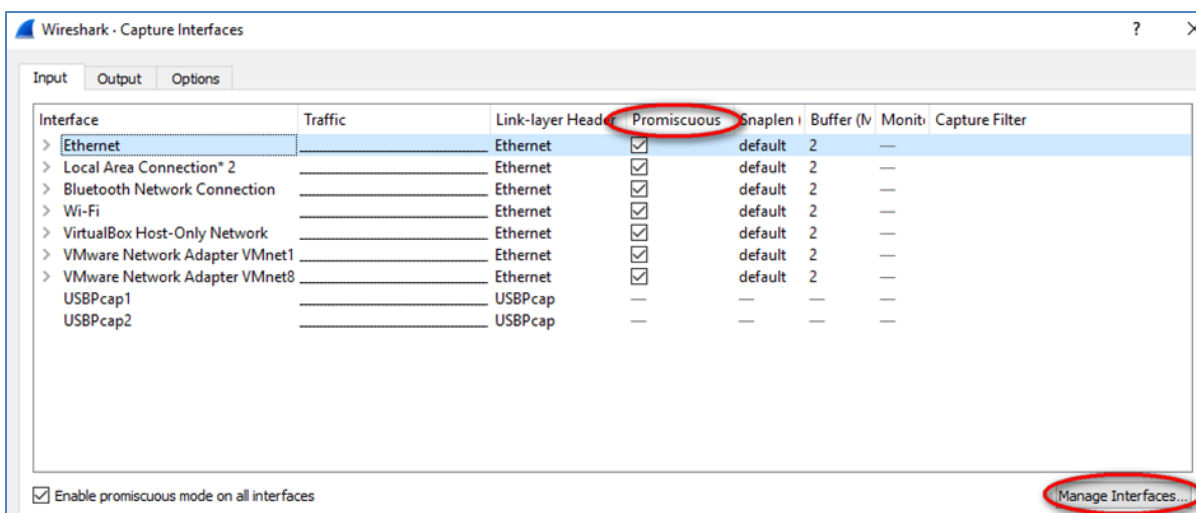
- b. Após iniciar o Wireshark, clique na interface de captura para utilizá-lo. Como estamos usando a conexão Ethernet com fio no PC, verifique se a opção de Ethernet está na parte superior da lista.



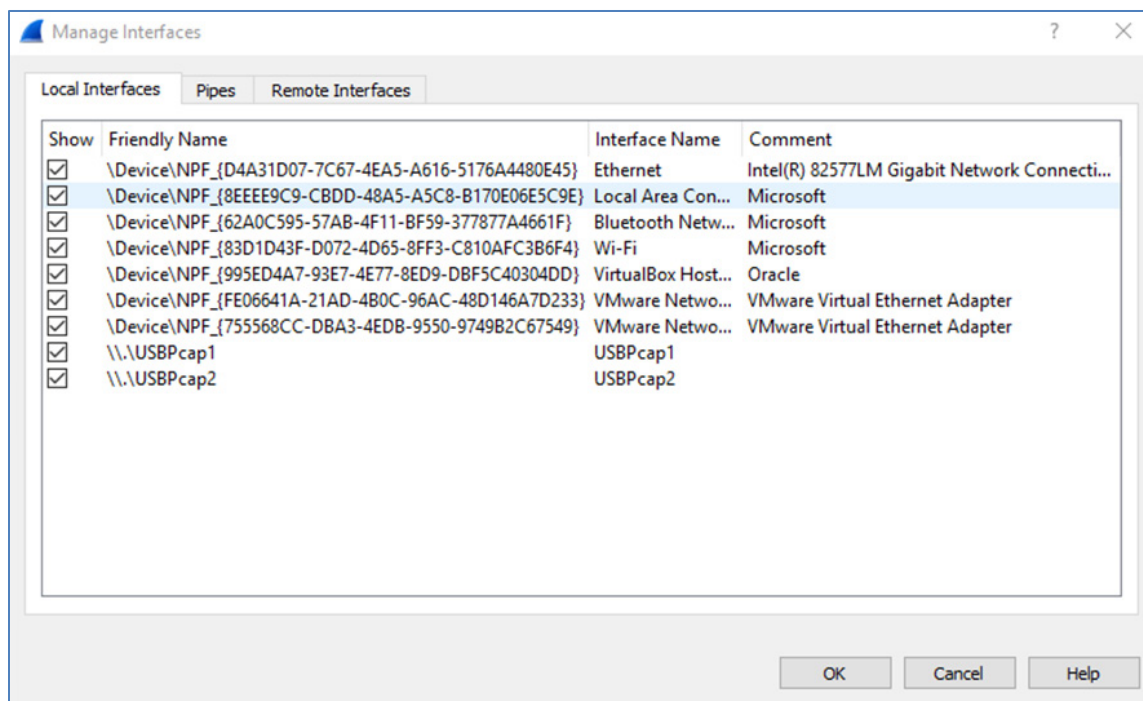
Você pode gerenciar a interface de captura clicando em **Capture** (Capturar) e **Options** (Opções):



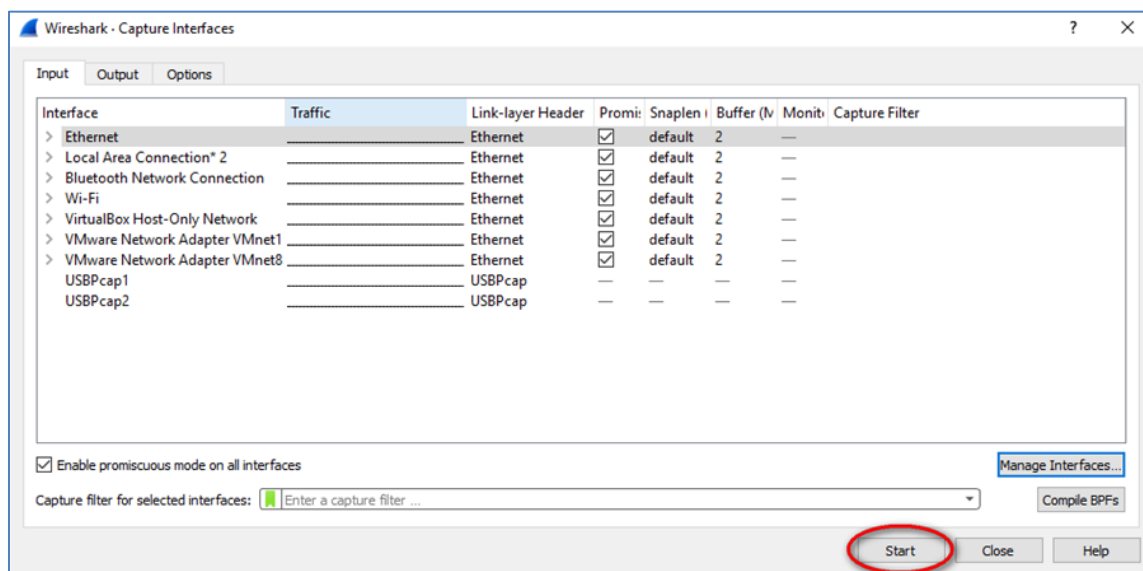
- c. É exibida uma lista de interfaces. Verifique se a interface de captura está marcada em **Promiscuous** (Promísqua).



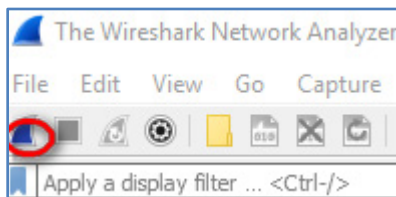
Observação: podemos ainda gerenciar as interfaces no PC, clicando em **Manage Interfaces** (Gerenciar Interfaces). Verifique se a descrição corresponde ao que você observou na etapa 1b. Feche a janela **Manage Interfaces** (Gerenciar interfaces) após verificar a interface correta.



- 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.

No.	Time	Source	Destination	Protocol	Length	Info
1	0.000000	fe80::1691:82ff:fe9...	ff02::1	ICMPv6	86	Router Advertisement from
2	33.958601	192.168.1.147	192.168.1.1	DNS	87	Standard query 0x7376 A r
3	33.972707	192.168.1.1	192.168.1.147	DNS	168	Standard query response 0
4	33.974092	192.168.1.147	137.116.77.120	TCP	66	49953 → 443 [SYN] Seq=0 W
5	33.997809	137.116.77.120	192.168.1.147	TCP	66	443 → 49953 [SYN, ACK] Se
6	33.997916	192.168.1.147	137.116.77.120	TCP	54	49953 → 443 [ACK] Seq=1 A

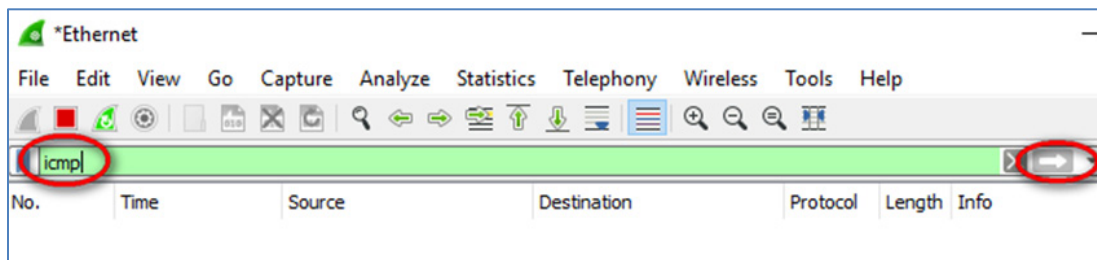
> Frame 1: 86 bytes on wire (688 bits), 86 bytes captured (688 bits) on interface 0
 > Ethernet II, Src: BelkinIn_9f:6b:8c (14:91:82:9f:6b:8c), Dst: IPv6mcast_01 (33:33:00:00:00:01)
 > Internet Protocol Version 6, Src: fe80::1691:82ff:fe9f:6b8c, Dst: ff02::1
 > Internet Control Message Protocol v6

```

0000  33 33 00 00 00 01 14 91 82 9f 6b 8c 86 dd 60 00  33..... .k...`.
0010  00 00 00 20 3a ff fe 80 00 00 00 00 00 00 16 91  ... :... ..
0020  82 ff fe 9f 6b 8c ff 02 00 00 00 00 00 00 00 00  ....k... ..
0030  00 00 00 00 00 01 86 00 29 88 40 40 00 00 00 00  ..... ).@@....
0040  00 00 00 00 00 00 05 01 00 00 00 00 05 dc 01 01  ..... ..
0050  14 91 82 9f 6b 8c  ....k.
    
```

Ethernet: <live capture in progress> | Packets: 41 · Displayed: 41 (100.0%) | Profile: Default

- 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 **Filtro** (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.

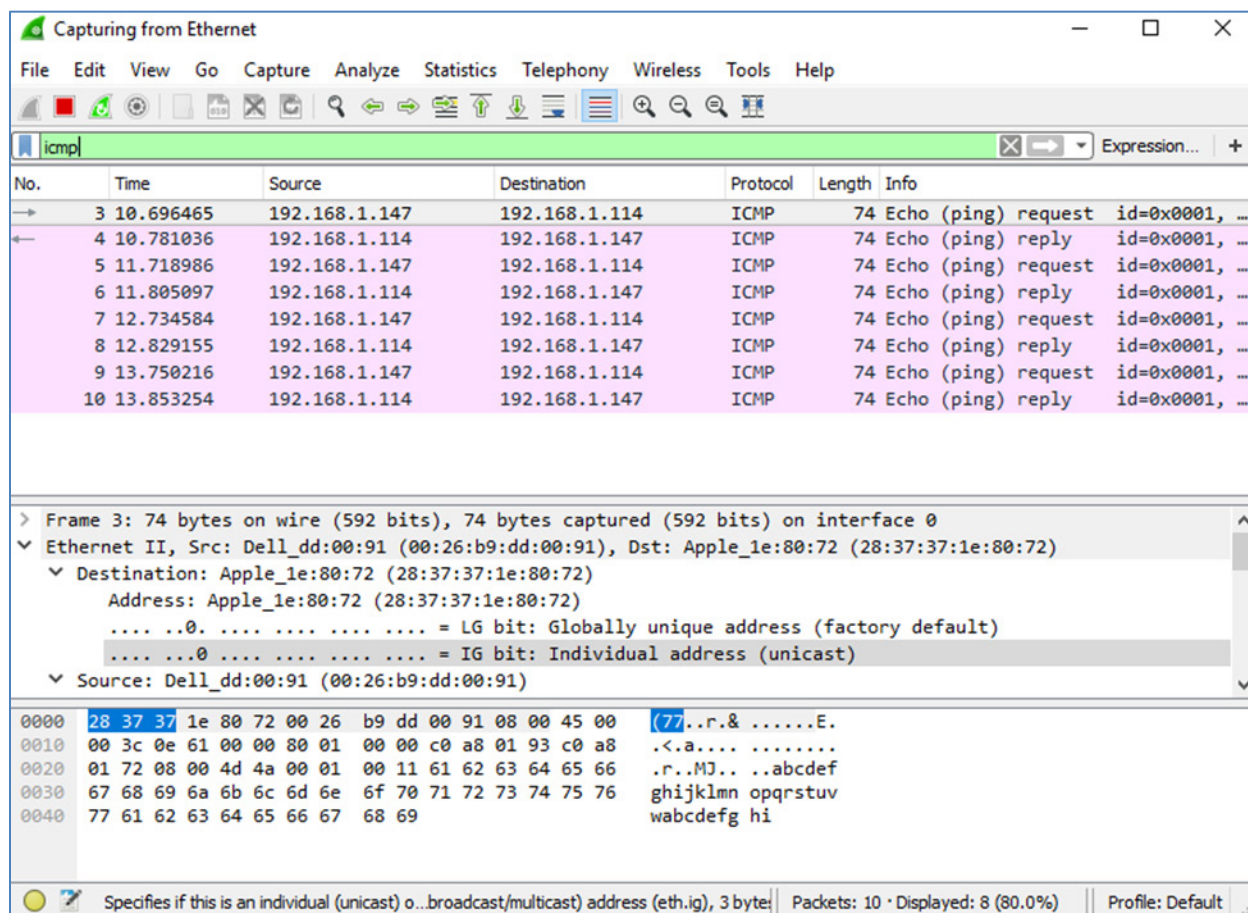
```
Microsoft Windows [Version 10.0.16299.64]
(c) 2017 Microsoft Corporation. All rights reserved.

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

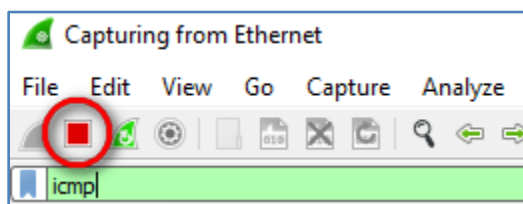
Ping statistics for 192.168.1.114:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 0ms, Maximum = 0ms, Average = 0ms
```


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.

Seção superior

No.	Time	Source	Destination	Protocol	Length	Info
→ 3	10.696465	192.168.1.147	192.168.1.114	ICMP	74	Echo (ping) request id=0x0001, ...
← 4	10.781036	192.168.1.114	192.168.1.147	ICMP	74	Echo (ping) reply id=0x0001, ...
→ 5	11.718986	192.168.1.147	192.168.1.114	ICMP	74	Echo (ping) request id=0x0001, ...
→ 6	11.805097	192.168.1.114	192.168.1.147	ICMP	74	Echo (ping) reply id=0x0001, ...
→ 7	12.734584	192.168.1.147	192.168.1.114	ICMP	74	Echo (ping) request id=0x0001, ...
→ 8	12.829155	192.168.1.114	192.168.1.147	ICMP	74	Echo (ping) reply id=0x0001, ...
→ 9	13.750216	192.168.1.147	192.168.1.114	ICMP	74	Echo (ping) request id=0x0001, ...
→ 10	13.853254	192.168.1.114	192.168.1.147	ICMP	74	Echo (ping) reply id=0x0001, ...

Seção do meio

```

> Frame 3: 74 bytes on wire (592 bits), 74 bytes captured (592 bits) on interface 0
> Ethernet II, Src: Dell_dd:00:91 (00:26:b9:dd:00:91), Dst: Apple_1e:80:72 (28:37:37:1e:80:72)
> Internet Protocol Version 4, Src: 192.168.1.147, Dst: 192.168.1.114
Internet Control Message Protocol
  Type: 8 (Echo (ping) request)
  Code: 0
  Checksum: 0x4d4a [correct]
  [Checksum Status: Good]
  
```

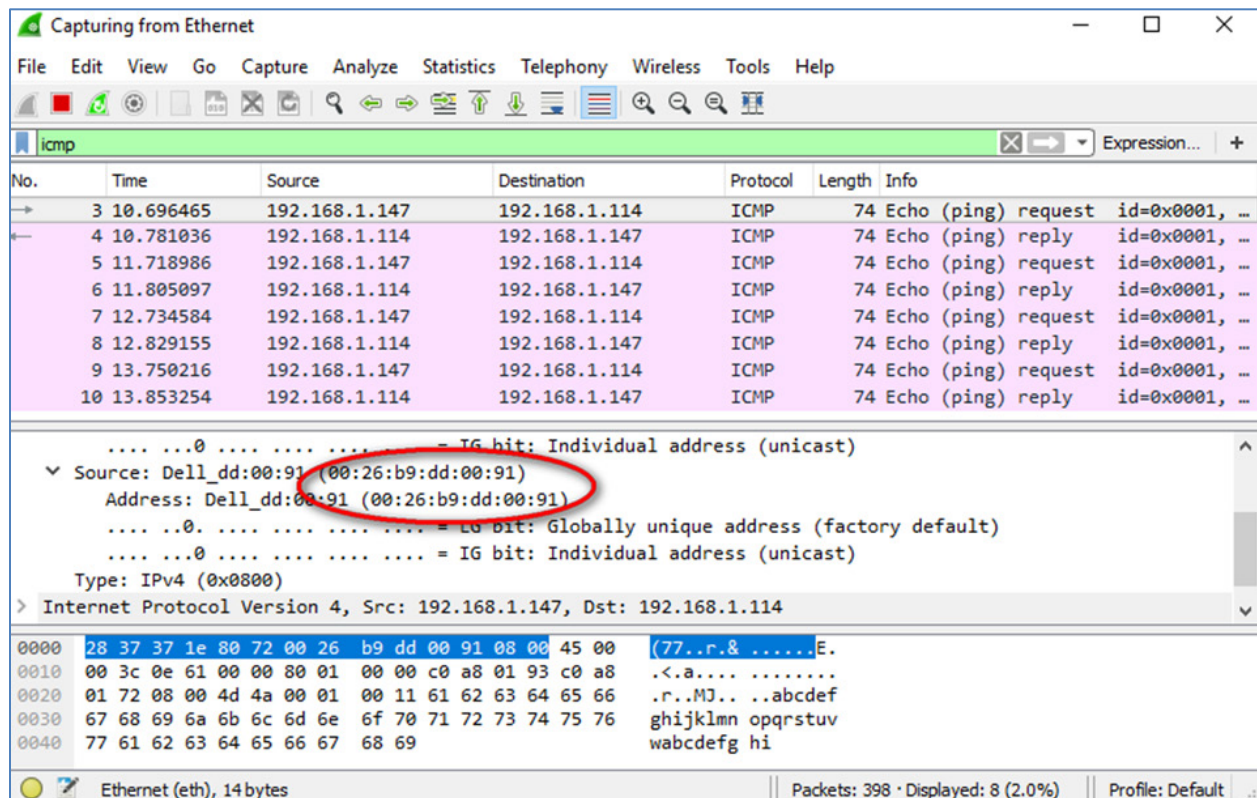
Seção inferior

Offset	Hex	ASCII
0000	28 37 37 1e 80 72 00 26 b9 dd 00 91 08 00 45 00	(28...r.&E.
0010	00 3c 0e 61 00 00 80 01 00 00 c0 a8 01 93 c0 a8	..<.a....
0020	01 72 08 00 4d 4a 00 01 00 11 61 62 63 64 65 66	..r..MJ.. ..abcdef
0030	67 68 69 6a 6b 6c 6d 6e 6f 70 71 72 73 74 75 76	ghijklmn opqrstuv
0040	77 61 62 63 64 65 66 67 68 69	wabcedfg hi

- 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.

No.	Time	Source	Destination	Protocol	Length	Info
→ 3	10.696465	192.168.1.147	192.168.1.114	ICMP	74	Echo (ping) request id=0x0001, ...
← 4	10.781036	192.168.1.114	192.168.1.147	ICMP	74	Echo (ping) reply id=0x0001, ...

- 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)? _____

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

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

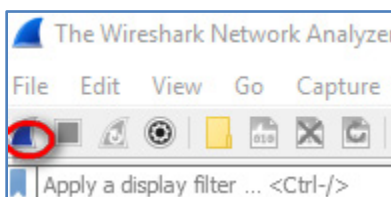
Observação: no exemplo anterior de uma requisição ICMP capturada, os dados do ICMP são encapsulados dentro da PDU do pacote IPv4 (cabeçalho IPv4) que é, então, encapsulada em uma PDU do quadro Ethernet II (cabeçalho Ethernet II) para transmissão na LAN.

Parte 2: Capturar e analisar dados ICMP remotos no Wireshark

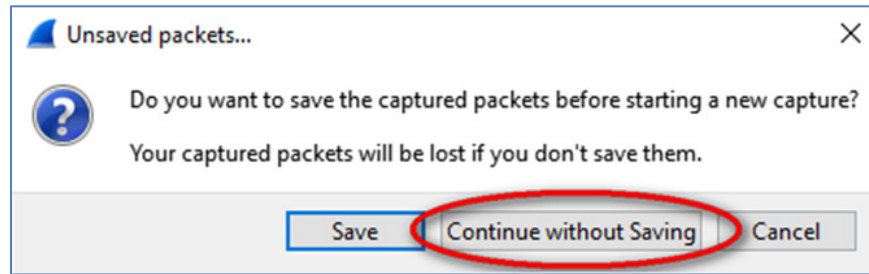
Na parte 2, você efetuará ping para hosts remotos (não nos hosts da LAN) e examinará os dados gerados desses pings. Você determinará o que há de diferente nesses dados a partir dos dados pesquisados na parte 1.

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

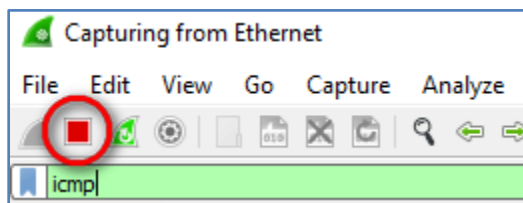
Pinging www.google.com [216.58.194.100] with 32 bytes of data:
Reply from 216.58.194.100: bytes=32 time=56ms TTL=54
Reply from 216.58.194.100: bytes=32 time=56ms TTL=54
Reply from 216.58.194.100: bytes=32 time=55ms TTL=54
Reply from 216.58.194.100: bytes=32 time=57ms TTL=54

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: ____:____:____:____:____:____

- b. Qual é a importância dessas informações?

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

Reflexão

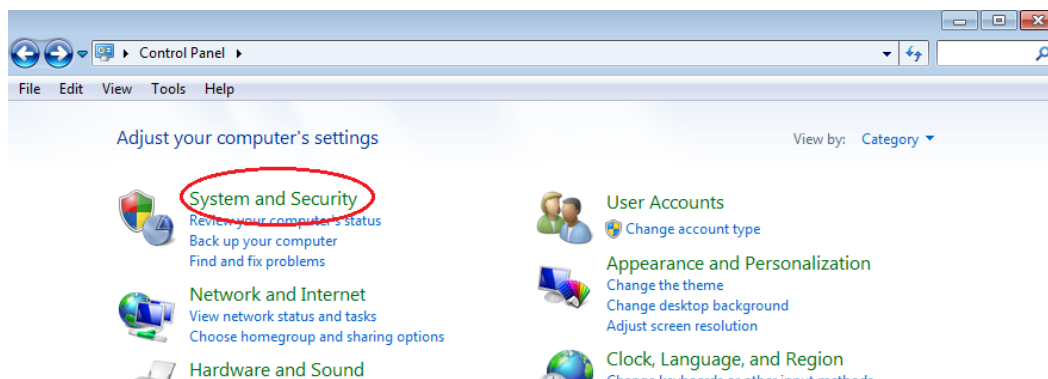
Por que o Wireshark mostra o endereço MAC real dos hosts locais, mas não o endereço MAC real para os hosts remotos?

Anexo A: Permitir o tráfego ICMP pelo firewall

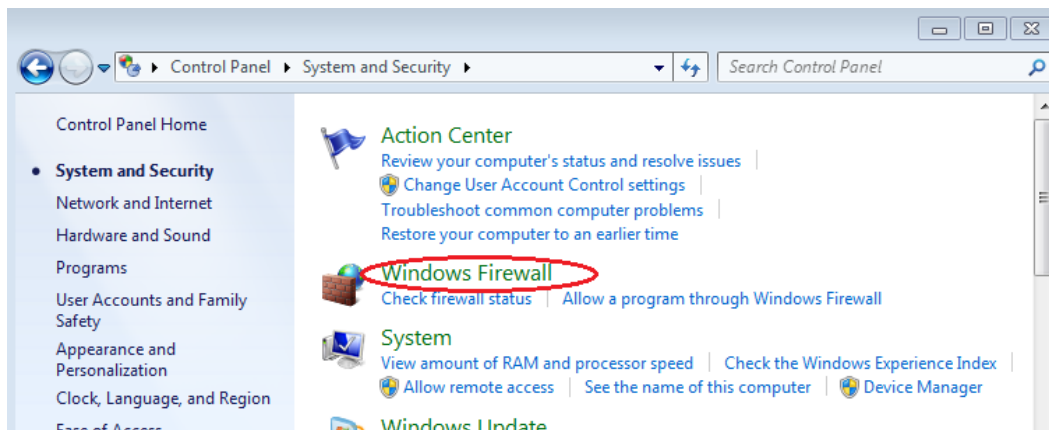
Se os membros de sua equipe não conseguirem efetuar ping em seu PC, o firewall pode estar bloqueando essas solicitações. Este anexo descreve como criar uma regra no firewall para permitir requisições ping. Também descreve como desativar a nova regra ICMP depois que você tiver concluído o laboratório.

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**.



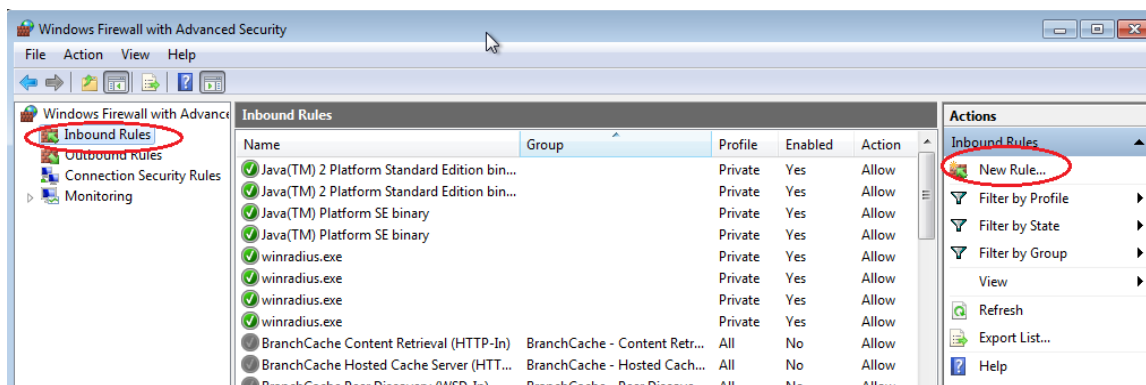
- b. Na janela **Sistema e segurança**, clique em **Firewall do Windows**.



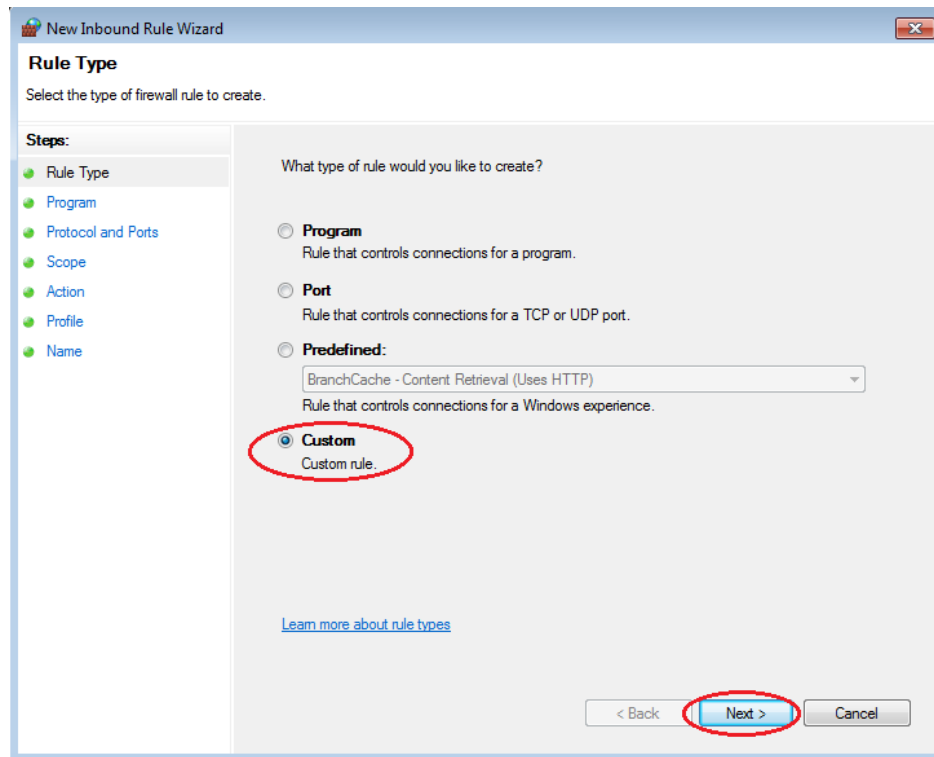
- c. No painel esquerdo da janela **Firewall do Windows**, clique em **Configurações avançadas**.



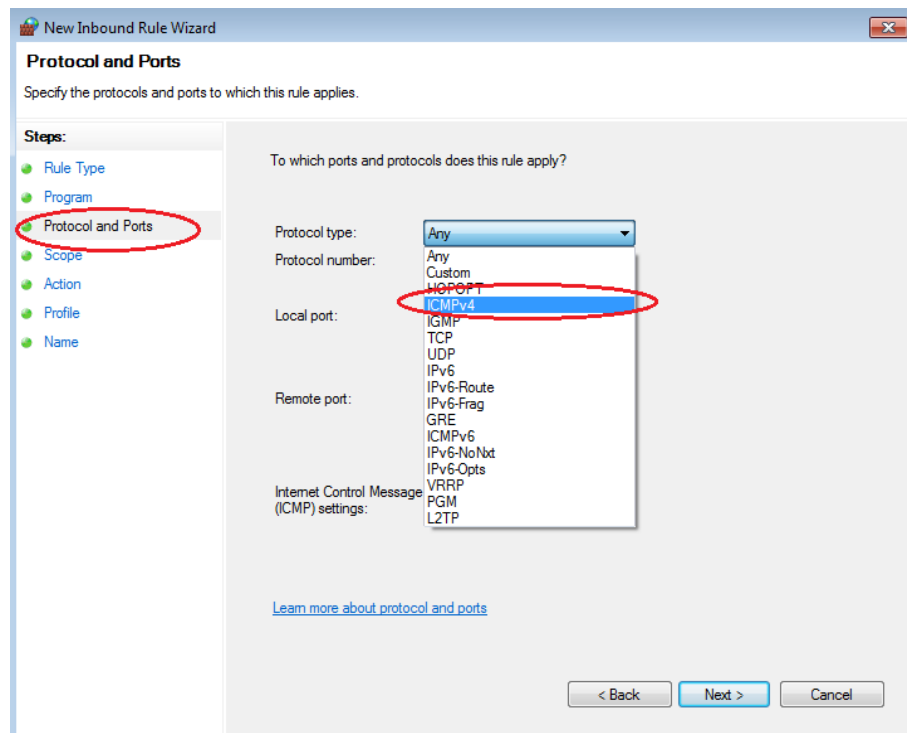
- d. Na janela **Segurança avançada**, selecione a opção **Regras de entrada** na barra lateral esquerda e clique em **Nova regra...** na barra lateral direita.



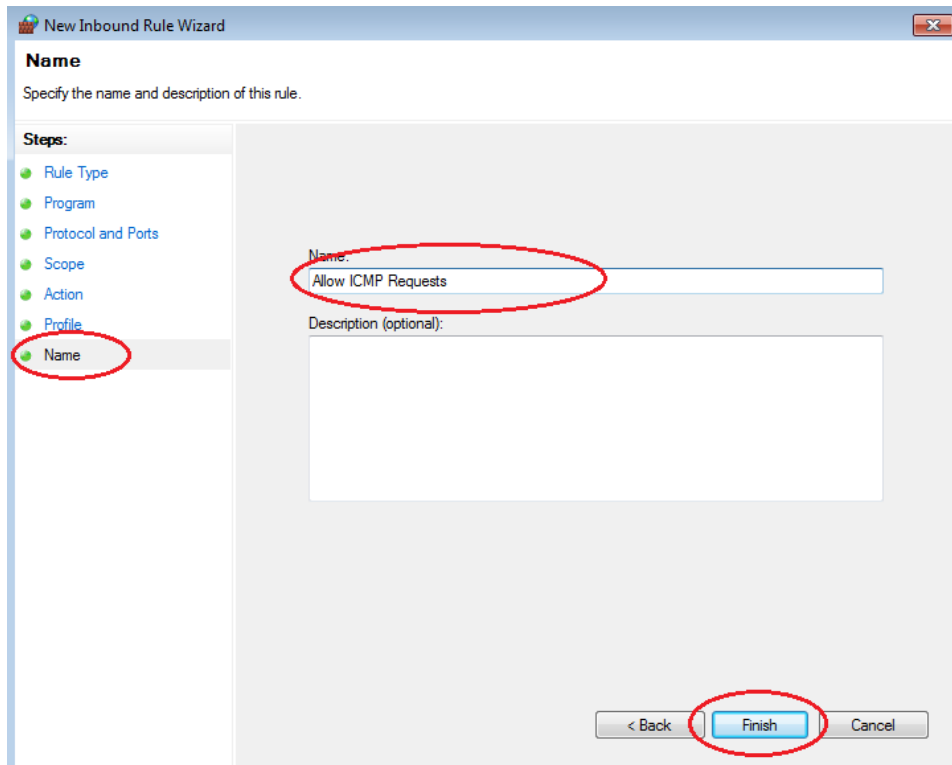
- e. Isso inicia o assistente **Nova regra de entrada**. Na tela **Tipo de regra**, clique no botão de opção **Personalizar** e em **Avançar**



- 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**.

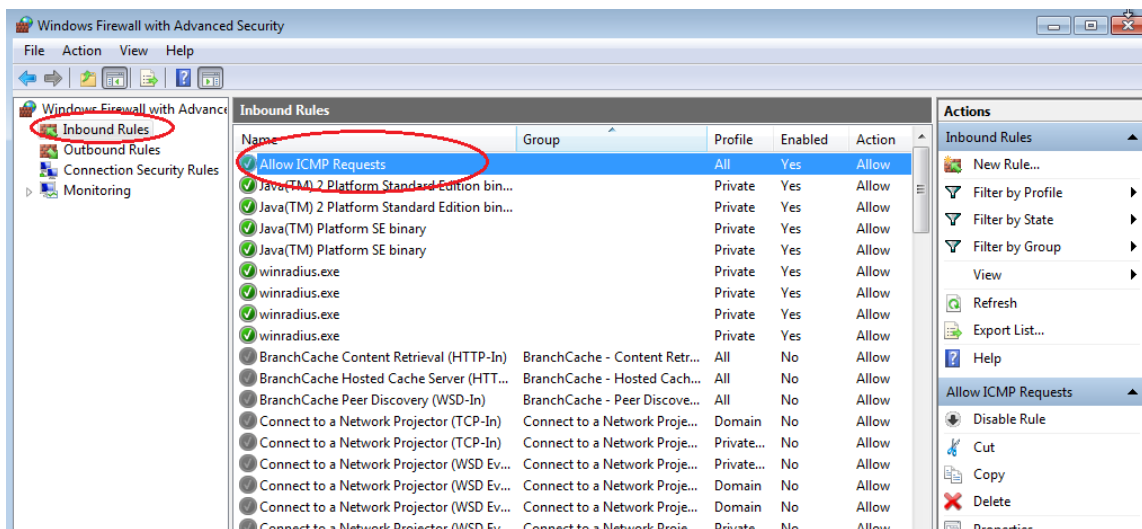


Essa nova regra deve permitir que os membros da equipe recebam respostas de ping vindo do seu PC.

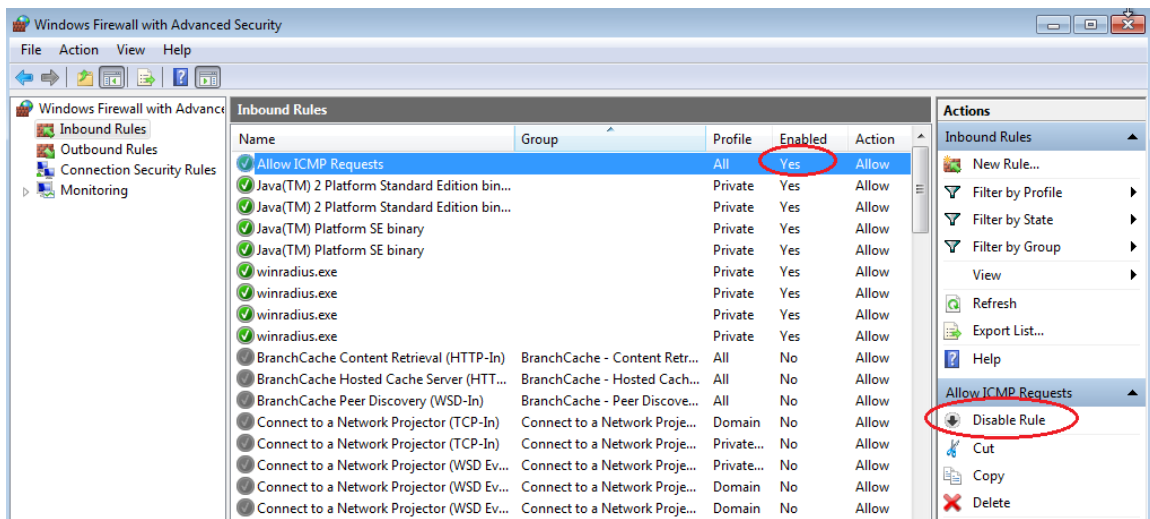
Etapa 2: Desativar ou excluir a nova regra do ICMP.

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.

