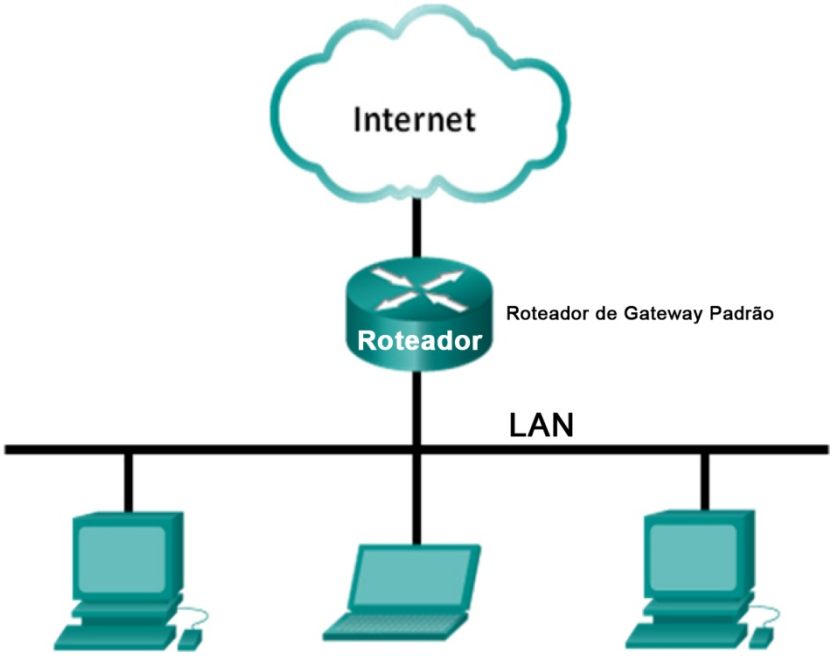
Laboratório - Uso do Wireshark para visualizar o tráfego de rede

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 (com Windows 7 ou 8 e 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

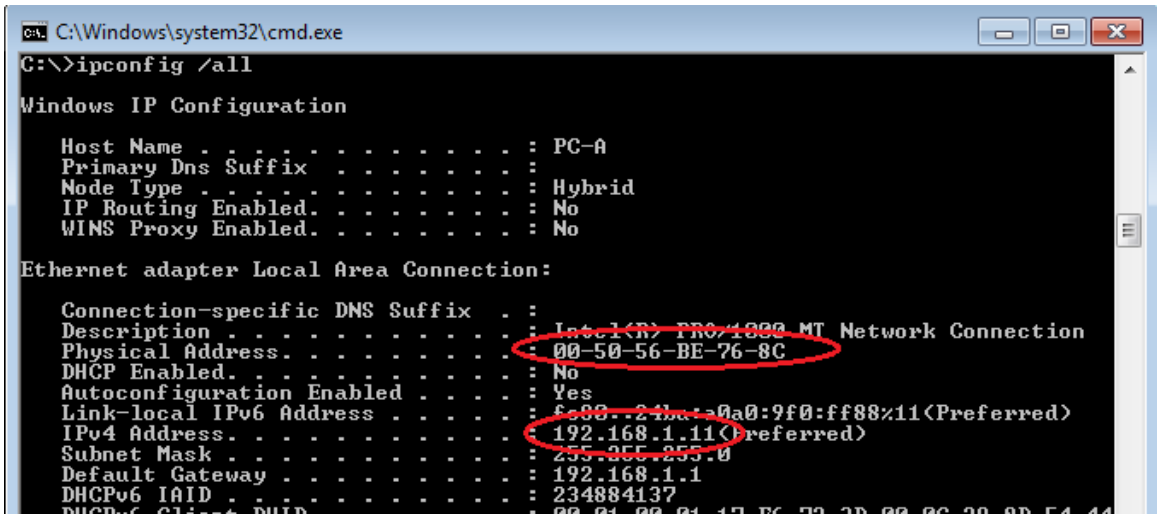
Na parte 1 deste laboratório, você efetuará ping para outro computador na LAN e capturará solicitações e respostas ICMP no Wireshark. Você também verá quadros capturados para obter informações específicas. Essa análise ajudará a esclarecer como os cabeçalhos dos pacotes são usados para transportar os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

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

b. Observe o endereço IP da interface do PC e o endereço MAC (físico).

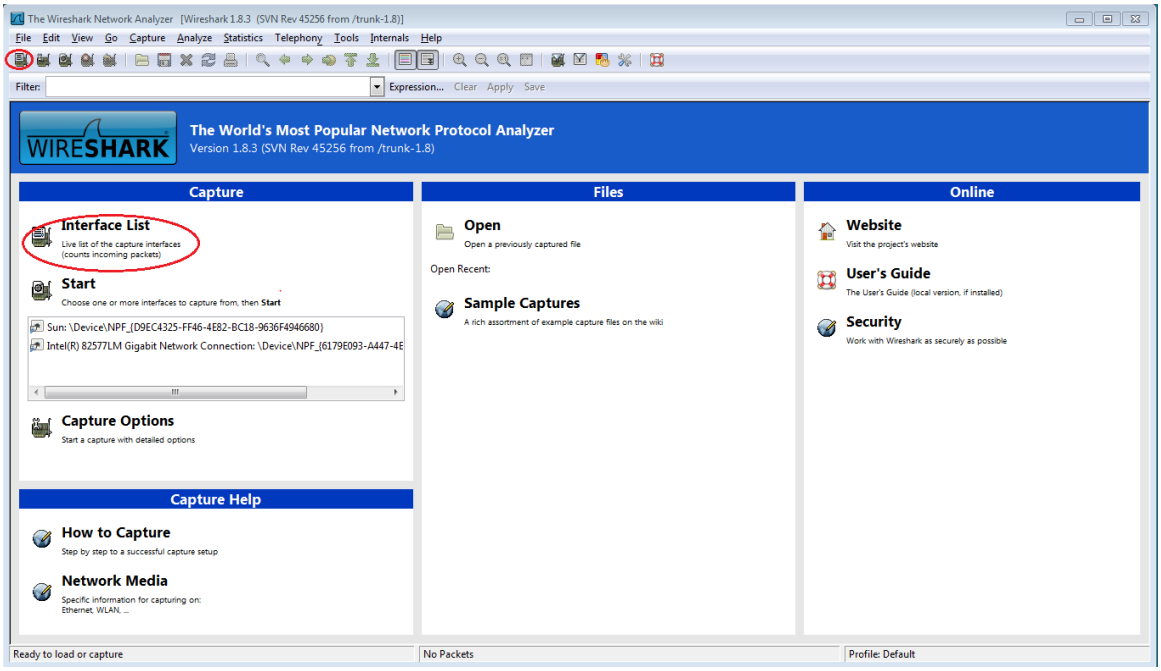


c. Solicite a um membro da equipe o endereço IP do PC dele e forneça a ele o endereço IP do seu PC. Não forneça o seu endereço MAC a ele agora.

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

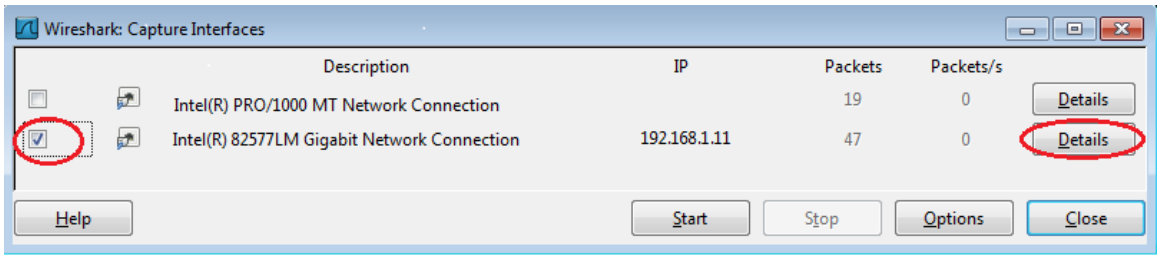
a. Em seu computador, clique no botão **Iniciar** do Windows para ver o Wireshark listado como um dos programas no menu pop-up. Clique duas vezes em **Wireshark**.

b. Após iniciar o Wireshark, clique em **Interface List** (Lista de interfaces).

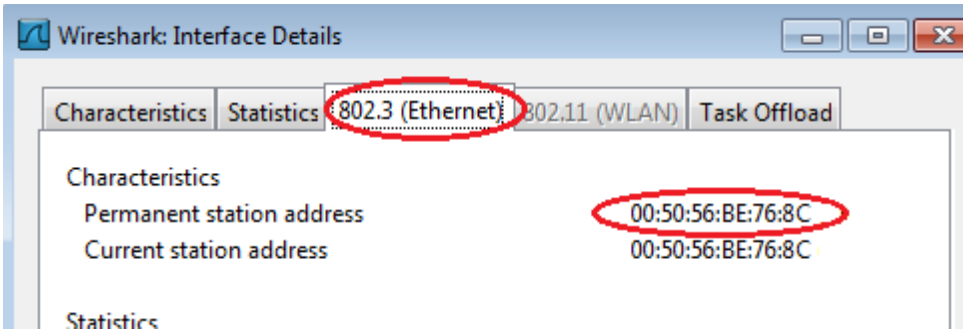


Observação: clicar no primeiro ícone de interface na linha de ícones também abre a lista de interfaces.

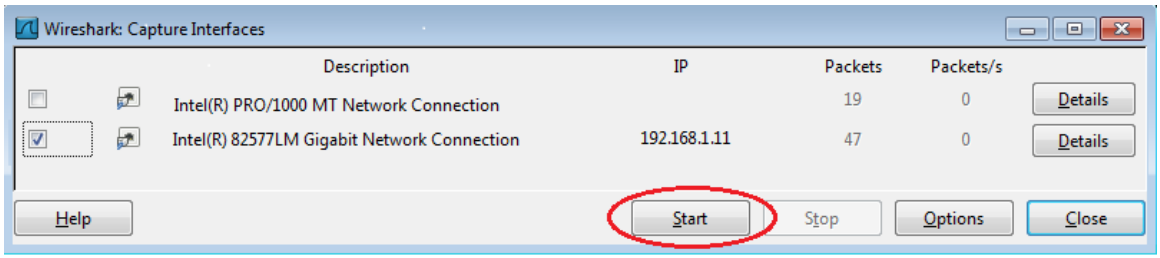
c. No Wireshark: na janela Capture Interfaces (Interfaces de captura), clique na caixa de seleção ao lado da interface conectada à LAN.



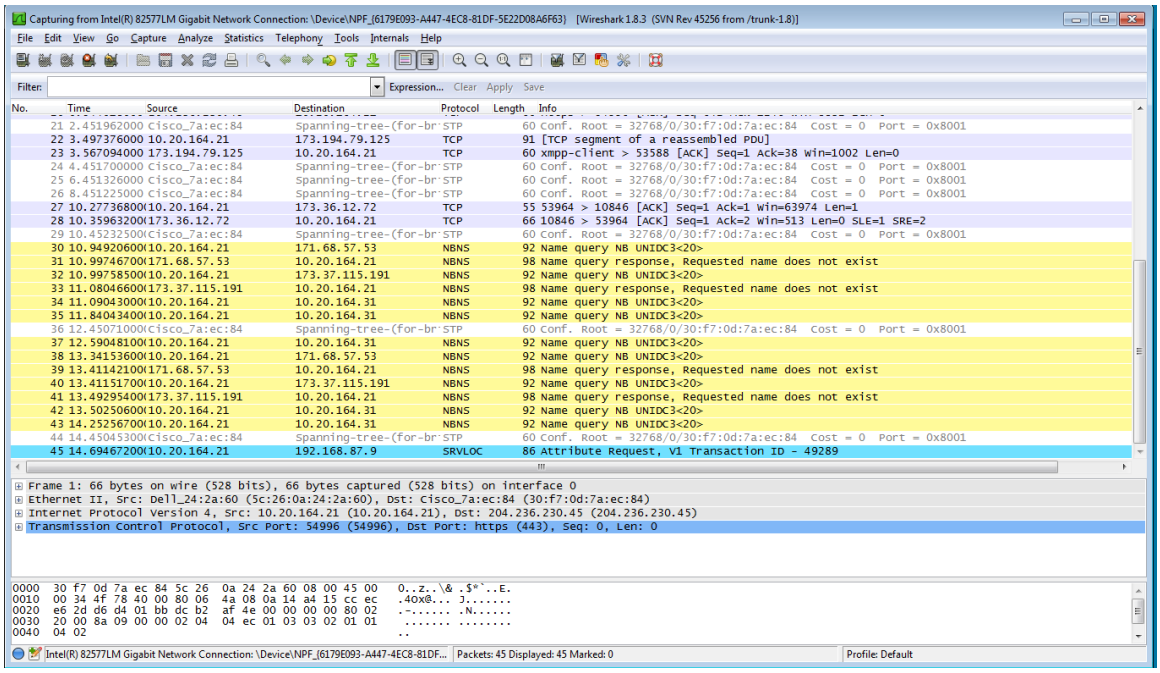
Observação: se várias interfaces estiverem listadas e você não tiver certeza sobre qual delas verificar, clique no botão **Details** (Detalhes) e na guia **802.3 (Ethernet)**. Verifique se o endereço MAC corresponde ao que você observou na etapa 1b. Feche a janela Interface Details (Detalhes da interface) após verificar a interface correta.



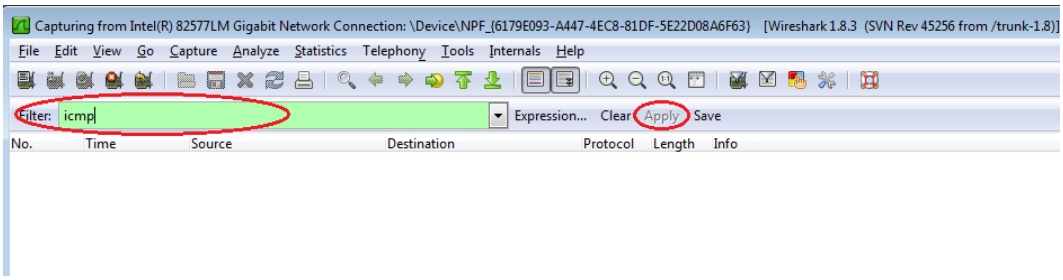
d. Depois de verificar a interface correta, clique em **Start** (Iniciar) para iniciar a captura de dados.



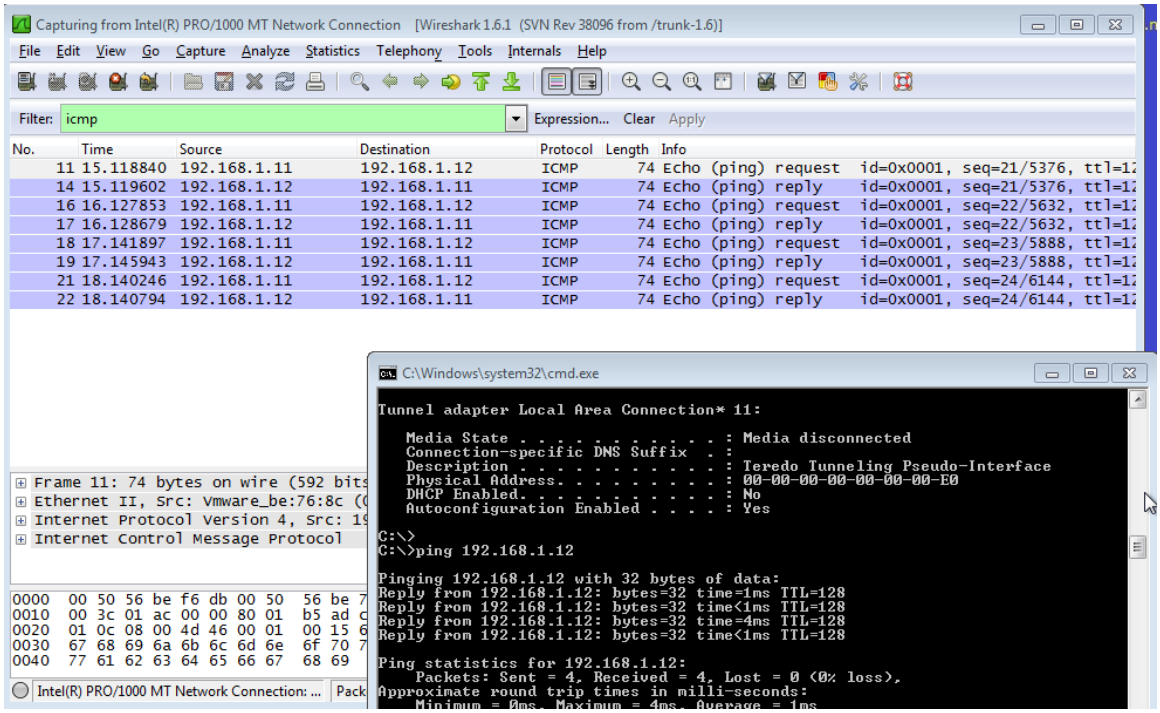
As informações começarão a rolar abaixo da seção superior no Wireshark. As linhas de dados serão exibidas em cores diferentes com base no protocolo.



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).

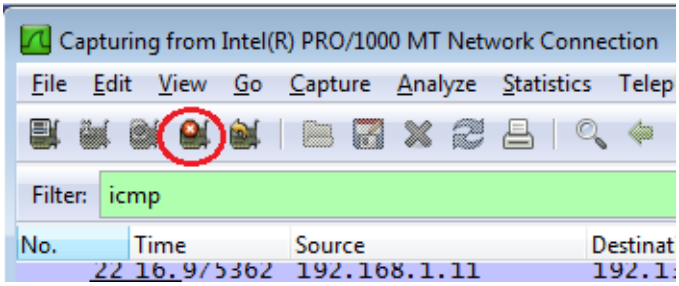


f. Este filtro faz com que todos os dados na janela superior desapareçam, mas você ainda captura o tráfego na interface. Exiba a janela do prompt de comando que você abriu anteriormente e efetue ping no endereço IP que recebeu da sua equipe. Observe que você começa a ver novamente os dados na janela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



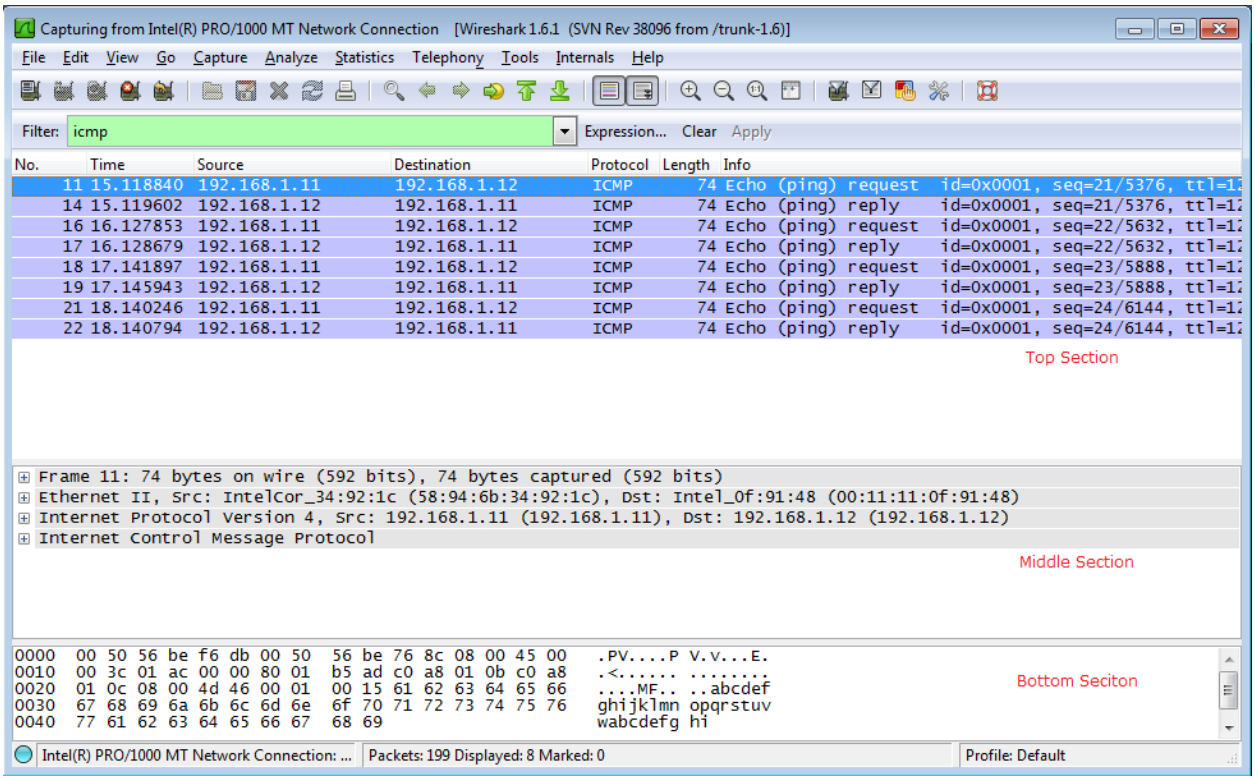
Observação: se o PC da sua equipe não responde aos pings, isso pode acontecer porque o firewall do PC está bloqueando as solicitações. Consulte Anexo A: Permitir o tráfego ICMP pelo firewall para obter informações sobre como permitir o tráfego ICMP pelo firewall usando o Windows 7.

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

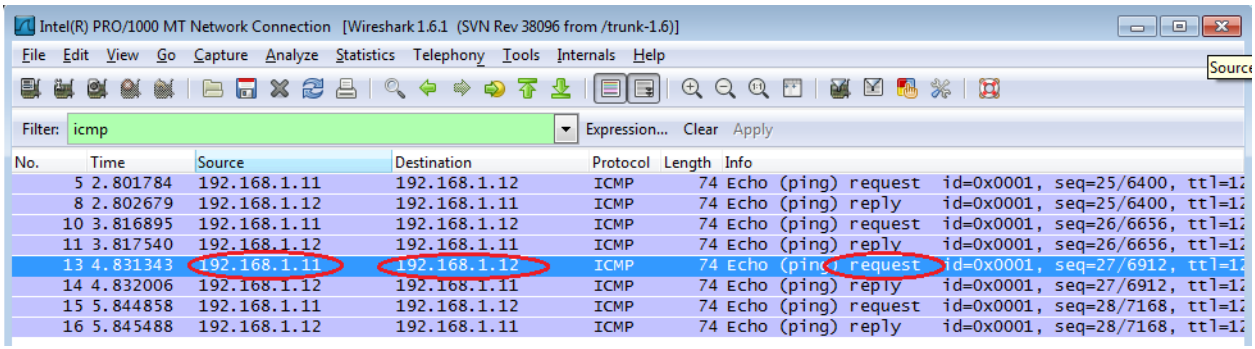


Etapa 3: Examinar os dados capturados.

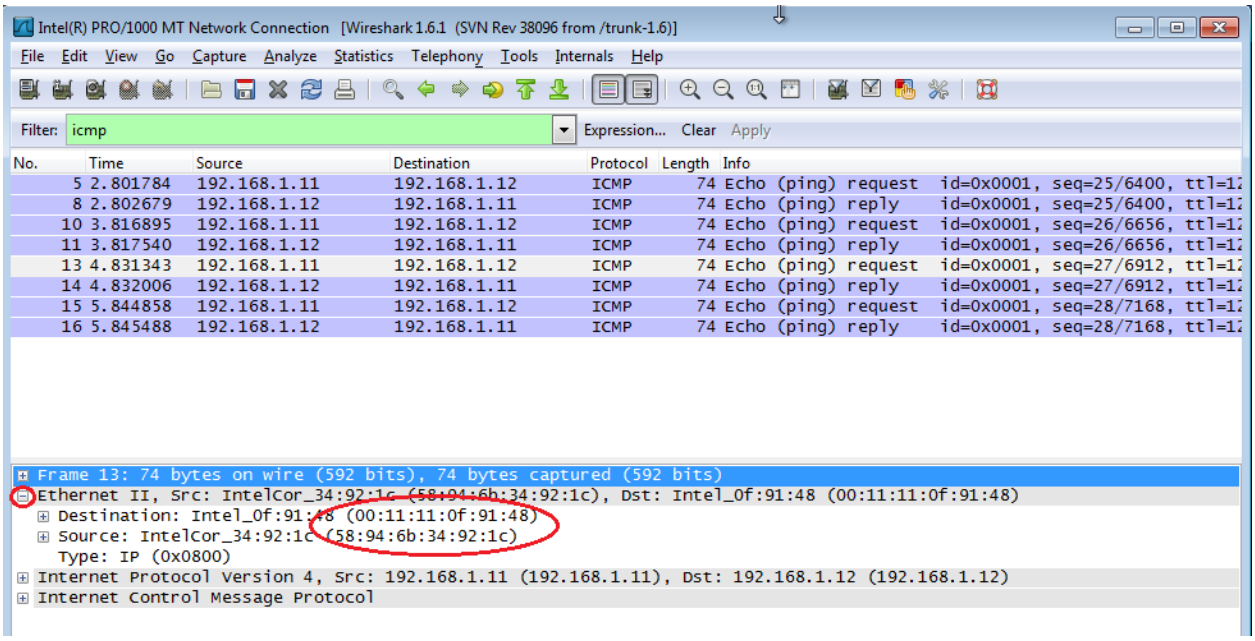
Na etapa 3, examine os dados gerados pelas solicitações ping do PC da sua equipe. Os dados do Wireshark são exibidos em três seções: 1) A seção superior exibe a lista de quadros de PDU capturada com um resumo das informações do pacote IP listadas, 2) a seção média mostra as informações de PDU para o 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 interface do PC?

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?

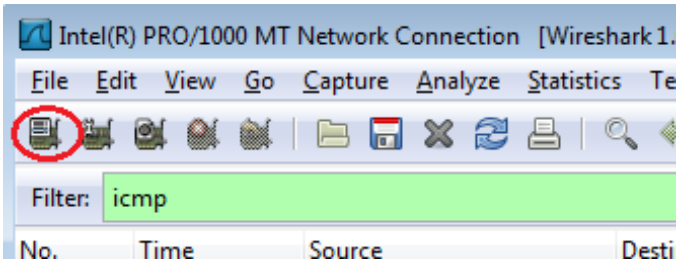
Observação: no exemplo anterior de uma requisição ICMP capturada, os dados do ICMP são encapsulados dentro da PDU do pacote IPv4 (cabeçalho IPv4) que é, então, encapsulada em uma PDU do quadro Ethernet II (cabeçalho Ethernet II) para transmissão na LAN.

Parte 2: Capturar e analisar dados ICMP remotos no Wireshark

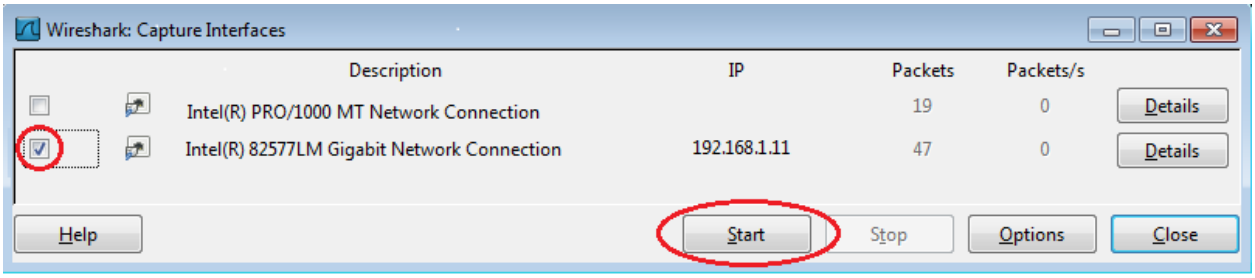
Na parte 2, você efetuará ping para hosts remotos (não nos hosts da LAN) e examinará os dados gerados desses pings. Você determinará o que há de diferente nesses dados a partir dos dados pesquisados na parte 1.

Etapa 1: Iniciar a captura de dados na interface.

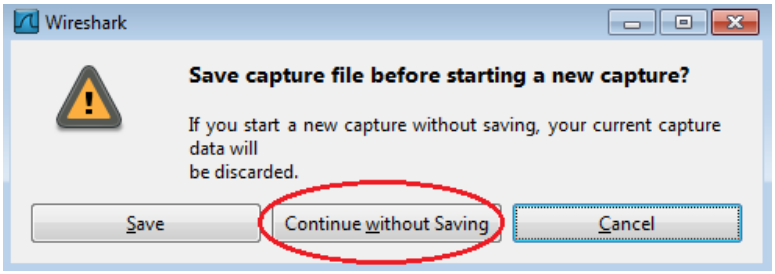
a. Clique no ícone **Interface List** (Lista de interfaces) para exibir novamente as interfaces do PC na lista.



b. Verifique se a caixa de seleção ao lado da interface da LAN está marcada e clique em **Start** (Iniciar).

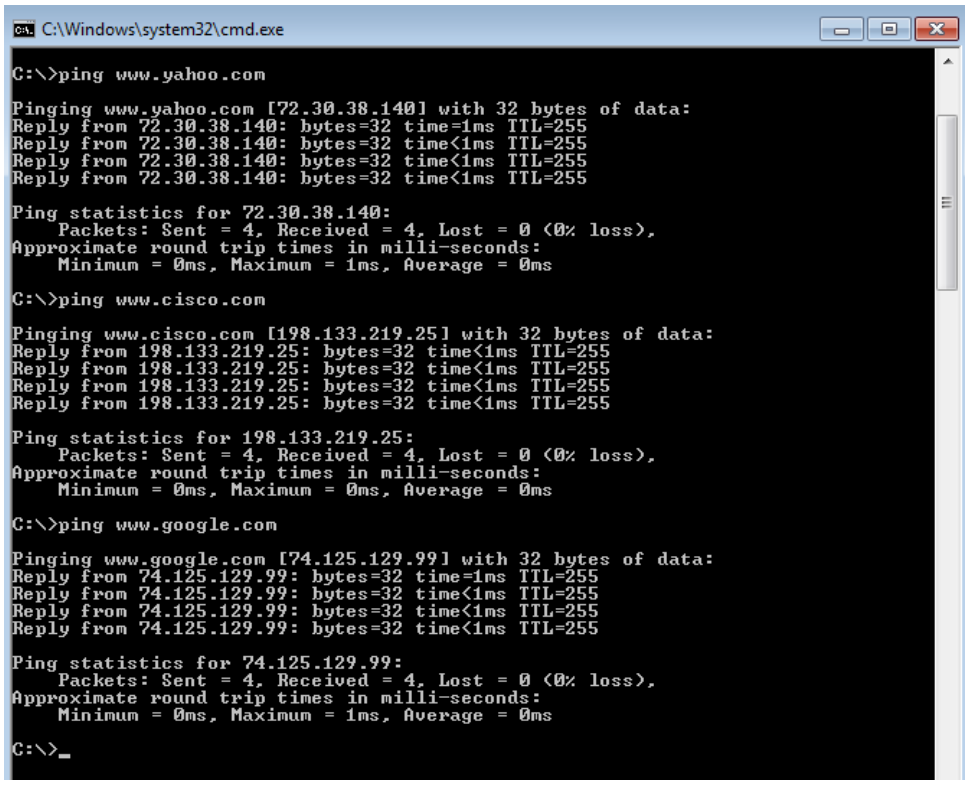


c. Uma janela solicitará o salvamento dos dados capturados anteriormente antes de iniciar outra captura. Não é necessário salvar esses dados. Clique em **Continue without Saving** (Continuar sem salvar).



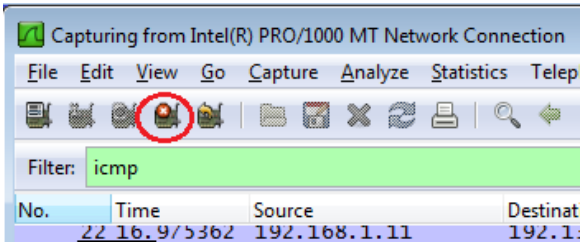
d. Com a captura ativa, efetue ping nas três URLs dos sites a seguir:

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



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.

e. 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, 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

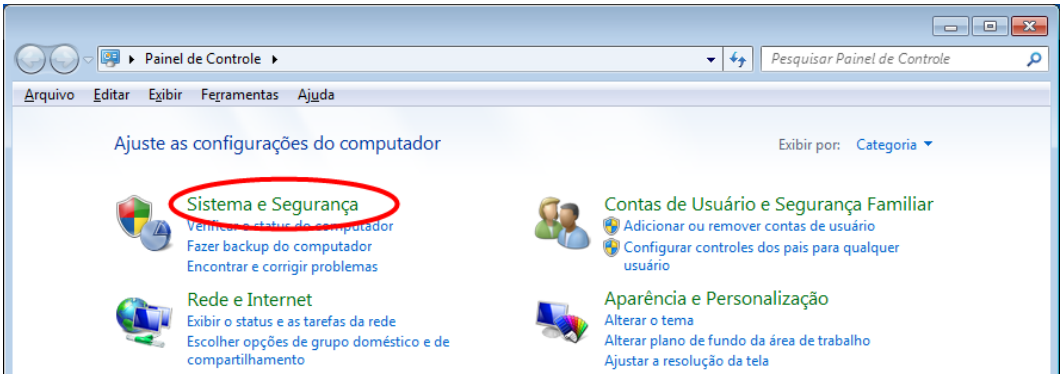
Por que o Wireshark mostra o endereço MAC real dos hosts locais, mas não o endereço MAC real para os hosts remotos?

Anexo A: Permitir o tráfego ICMP pelo firewall

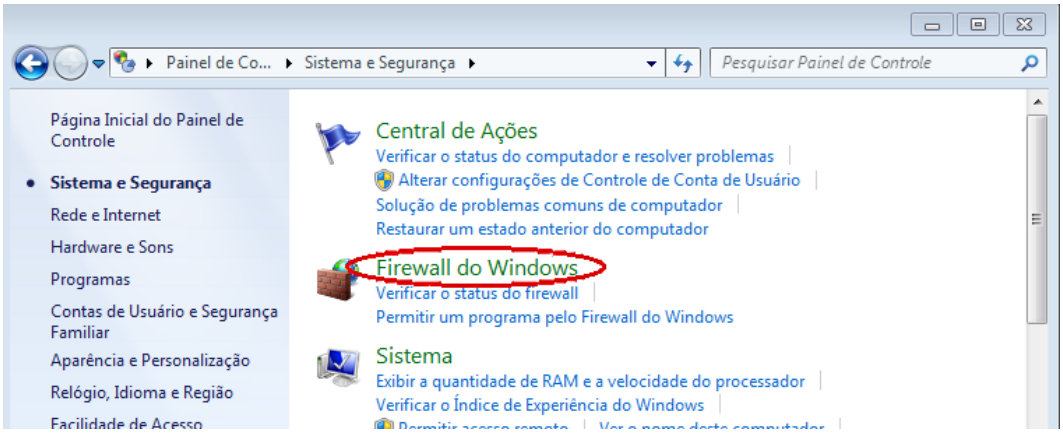
Se os membros de sua equipe não conseguirem efetuar ping em seu PC, o firewall pode estar bloqueando essas solicitações. Este anexo descreve como criar uma regra no firewall para permitir requisições ping. Também descreve como desativar a nova regra ICMP depois que você tiver concluído o laboratório.

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

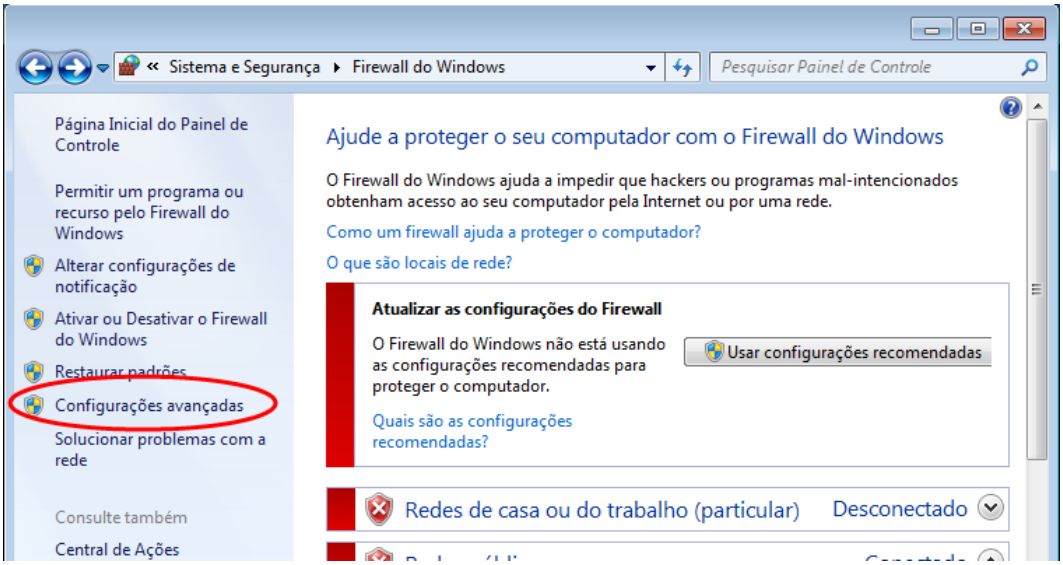
a. No painel de controle, clique na opção **Sistema e Segurança**.



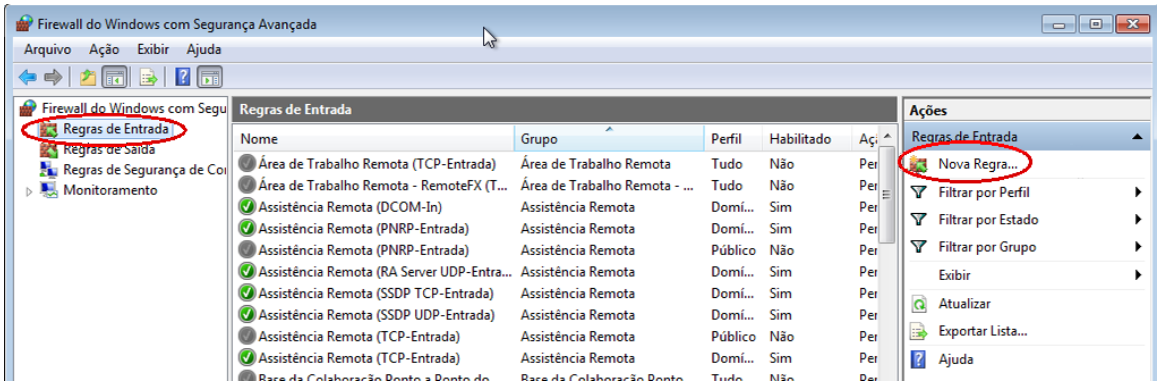
b. Na janela Sistema e segurança, clique em **Firewall do Windows**.



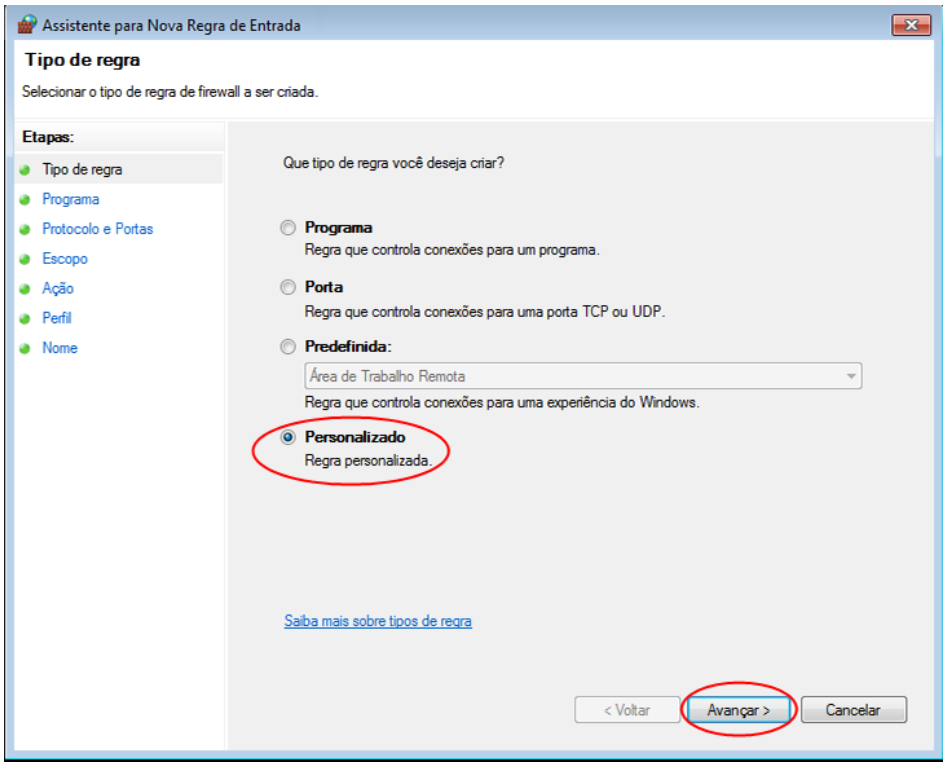
c. No painel esquerdo da janela Firewall do Windows, clique em **Configurações avançadas**.



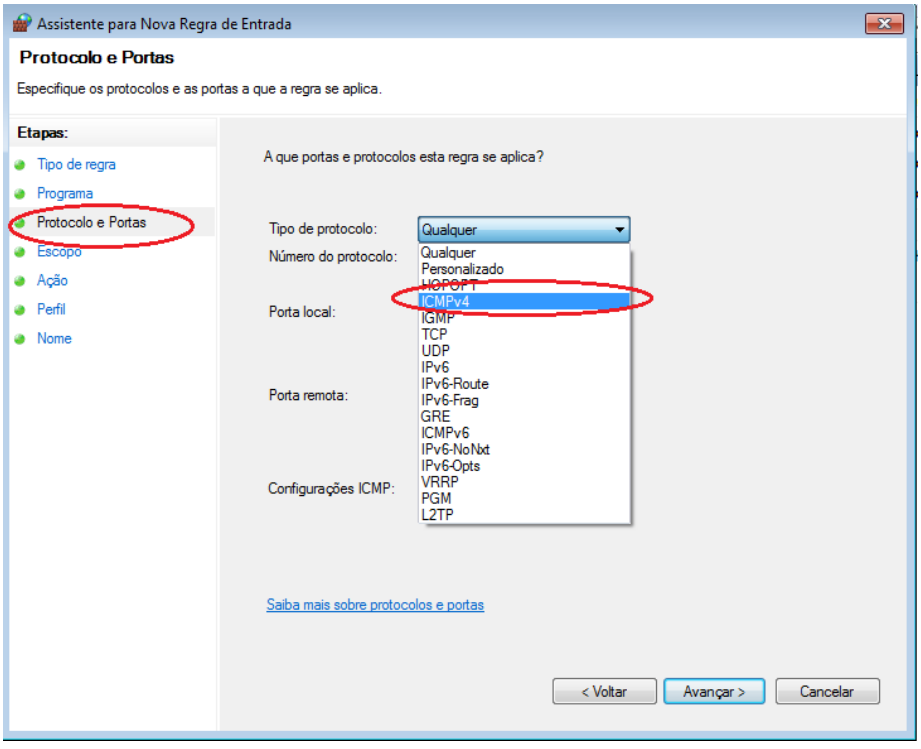
d. Na janela Segurança avançada, selecione a opção **Regras de entrada** na barra lateral esquerda e clique em **Nova regra…** na barra lateral direita.



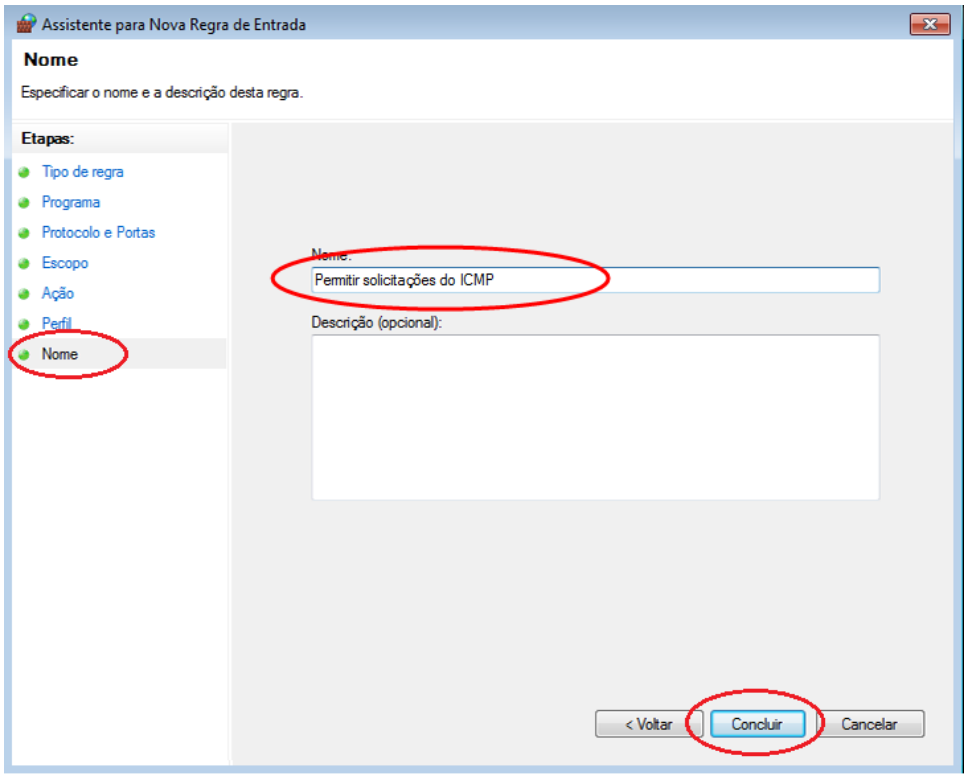
e. Isso inicia o assistente Nova regra de entrada. Na tela Tipo de regra, clique no botão de opção **Personalizar** e em **Avançar**



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**.

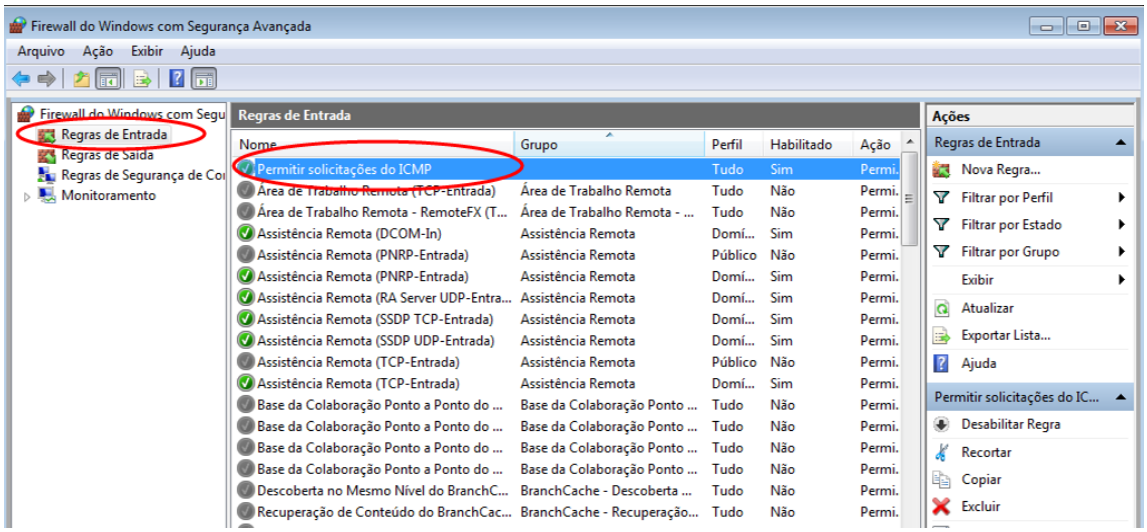


Essa nova regra deve permitir que os membros da equipe recebam respostas de ping vindo do seu PC.

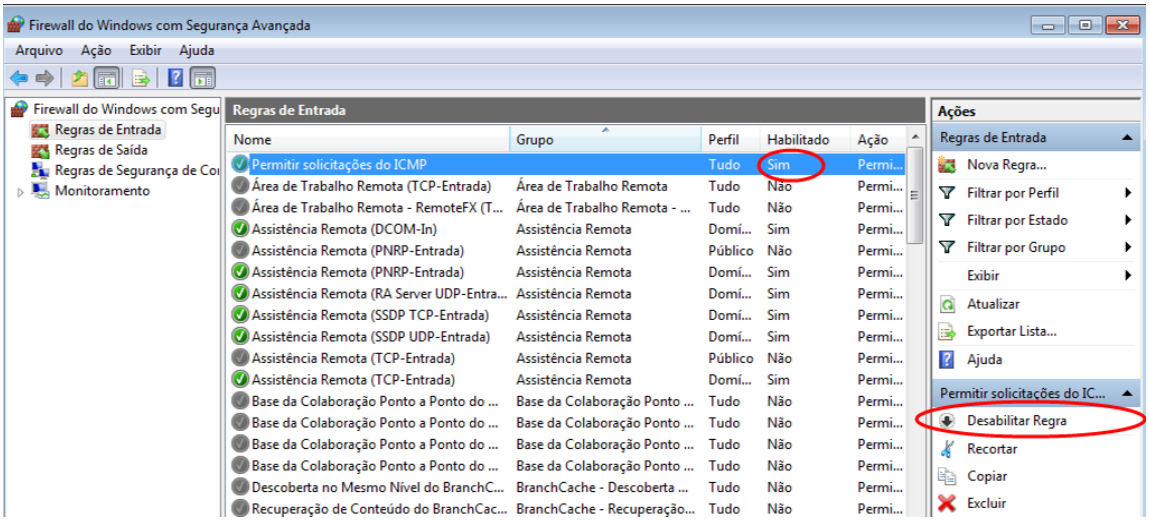
Etapa 2: Desativar ou excluir a nova regra do ICMP.

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.