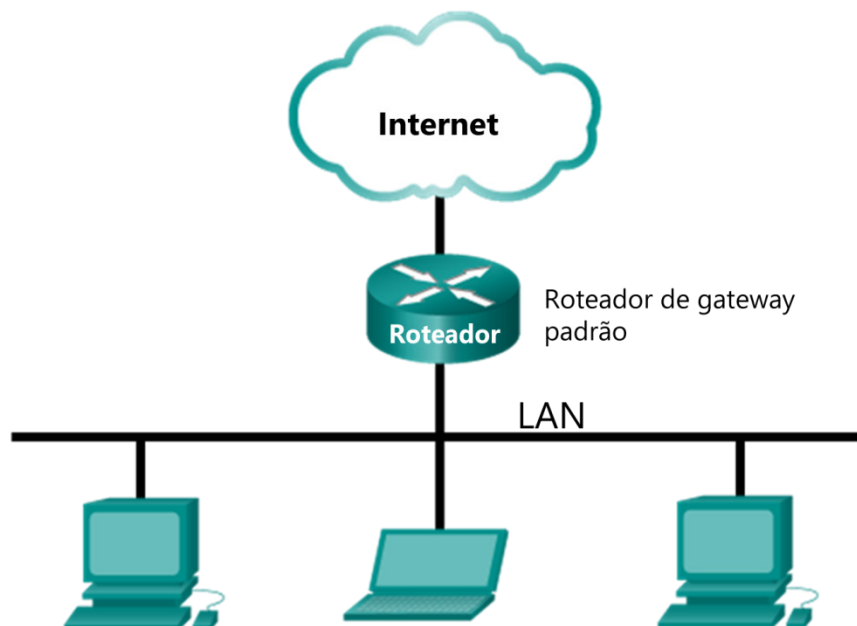


Laboratório – Protocolo ARP (Address Resolution Protocol - Protocolo de Resolução de Endereços)

Topologia



Objetivos

Parte 1: Baixar e instalar o Wireshark

Parte 2: Capturar e analisar dados ARP no Wireshark

- Inicie e interrompa a captura de dados do tráfego de ping para os hosts remotos.
- Localize as informações sobre o endereço IPv4 e MAC em PDUs capturadas.
- Analise o conteúdo das mensagens ARP trocadas entre os dispositivos na LAN.

Parte 3: Visualizar as entradas do cache ARP no PC

- Acesse o Prompt de Comando do Windows.
- Use o comando **arp** do Windows para visualizar o cache da tabela ARP local no PC.

Histórico/Cenário

O protocolo ARP é usado pelo TCP/IP para mapear um endereço IPv4 da Camada 3 para um endereço MAC da Camada 2. Quando um quadro Ethernet é transmitido na rede, ele deve ter um endereço MAC destino. Para encontrar de forma dinâmica o endereço MAC de um destino conhecido, um dispositivo de origem transmite uma solicitação ARP na rede local. O dispositivo configurado com o endereço IPv4 de destino responde para a solicitação com uma resposta ARP e o endereço MAC é registrado no cache ARP.

Todos os dispositivos na LAN mantêm seu próprio cache ARP. O cache ARP é uma área pequena na RAM que armazena as respostas ARP. A visualização do cache ARP em um PC exibirá o endereço IPv4 e o endereço MAC de cada dispositivo na LAN com a qual o PC trocou mensagens ARP.

O Wireshark é um software analisador de protocolo, ou uma 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 as especificações adequadas do protocolo.

O Wireshark é uma ferramenta útil para quem trabalha com redes e pode ser usado com a maioria dos laboratórios nos cursos Cisco para análise de dados e solução de problemas. Este laboratório apresenta instruções para baixar e instalar o Wireshark, embora talvez já esteja instalado. Neste laboratório, você usará o Wireshark para capturar trocas de ARP na rede local.

Recursos necessários

- 1 PC com Windows 10 e acesso à Internet
- Serão usados outros PCs em uma rede local (LAN) para responder às solicitações de **ping**. Caso não haja outros PCs na LAN, o endereço de gateway padrão será usado para responder às solicitações de **ping**.

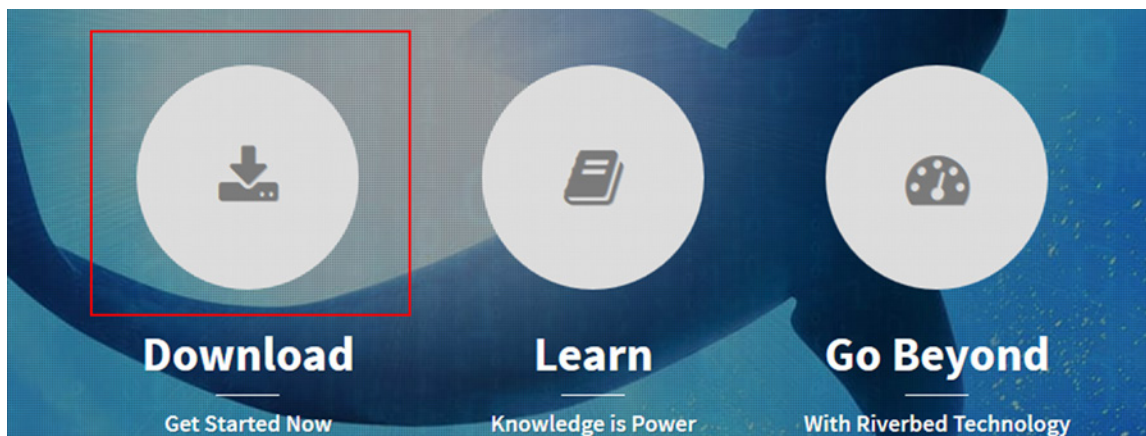
Parte 1: Fazer o download e instalar o Wireshark

O Wireshark tornou-se o programa sniffer de pacotes padrão do setor usado por engenheiros de rede. Este software aberto está disponível para vários sistemas operacionais diferentes, incluindo Windows, Mac e Linux.

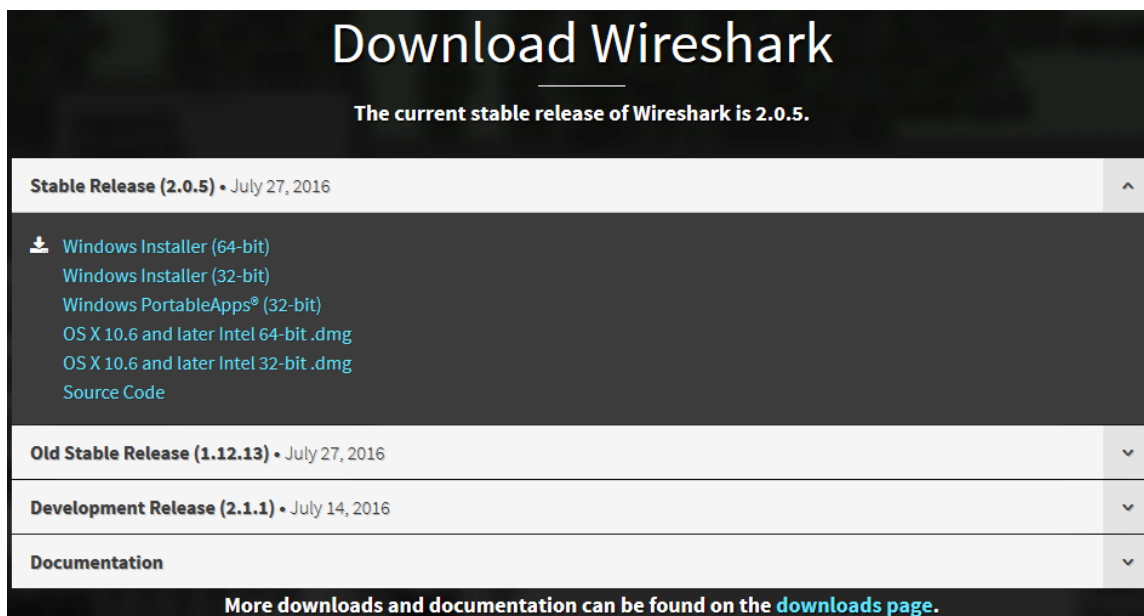
Se o Wireshark já estiver instalado no PC, você pode pular a Parte 1 e ir direto para a Parte 2. Se o Wireshark não estiver instalado no PC, verifique com seu instrutor a política de download de software de sua academia.

Etapa 1: Faça download do Wireshark.

- a. O Wireshark pode ser baixado em www.wireshark.org.
- b. Clique em **Download**.



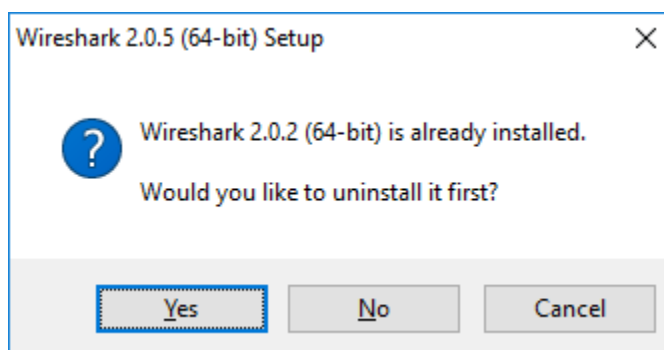
- c. Escolha a versão do software necessária com base na arquitetura e no sistema operacional do PC. Por exemplo, se você tiver um PC de 64 bits executando Windows, selecione **Windows Installer (64-bit)** (Instalador do Windows (64 bits)).



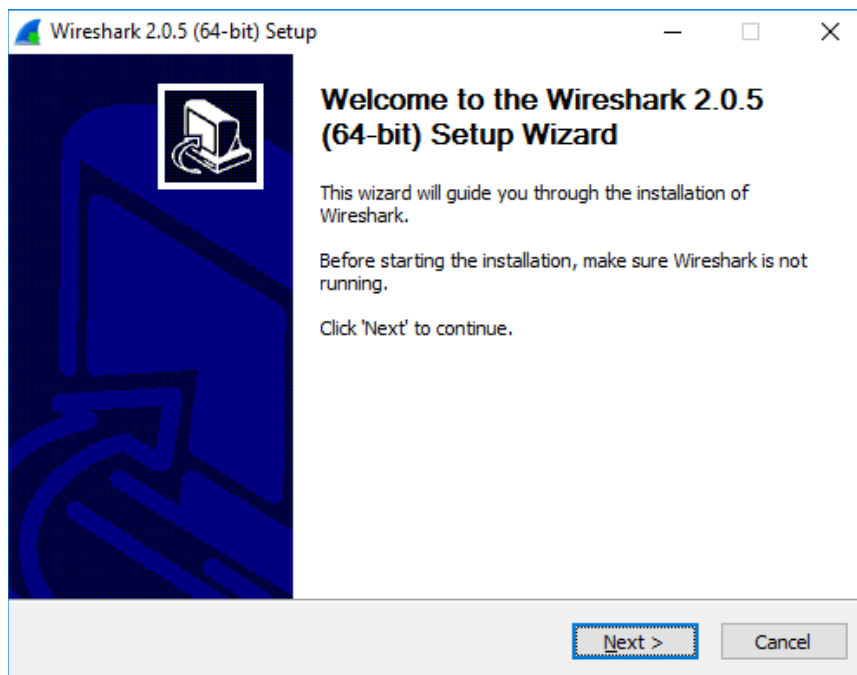
- d. Depois de fazer uma seleção, o download será iniciado. Clique em **Salvar Arquivo**, se for solicitado. O destino do download do arquivo depende do navegador e do sistema operacional usados. Para usuários do Windows, o local padrão é a pasta **Downloads**.

Etapa 2: Instalar o Wireshark.

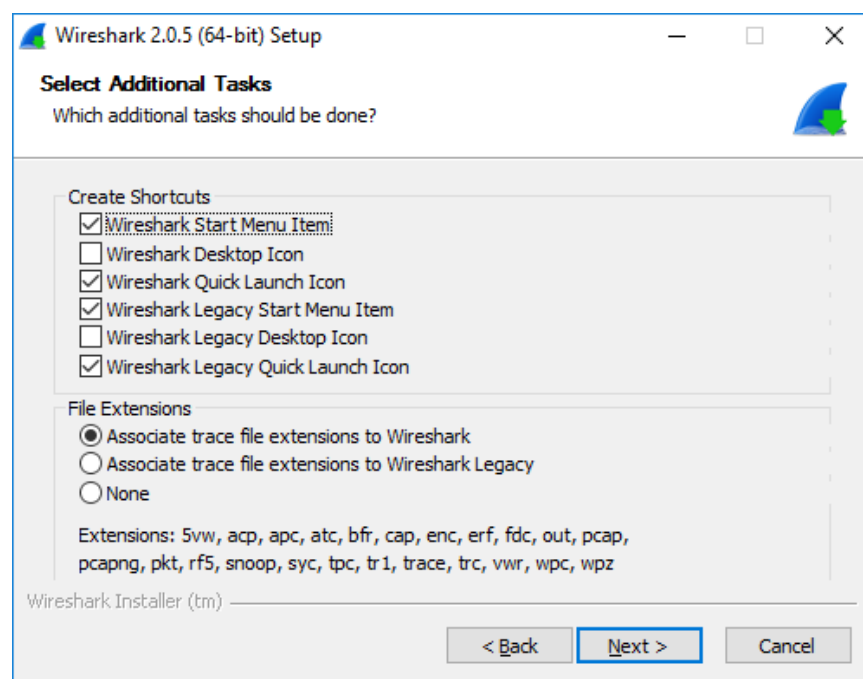
- a. O arquivo baixado é chamado **Wireshark-win64-x.x.x.exe**, em que **x** representa o número da versão. Clique duas vezes no arquivo para iniciar o processo de instalação. Neste exemplo, a versão é 2.0.5.
- b. Responda a todas as mensagens de segurança que aparecerem na tela. Se já tiver uma cópia do Wireshark em seu PC, você deverá desinstalar a versão anterior antes de instalar a nova. Recomenda-se que você remova a versão antiga do Wireshark antes de instalar outra versão. Clique em **Sim** para desinstalar a versão anterior do Wireshark.



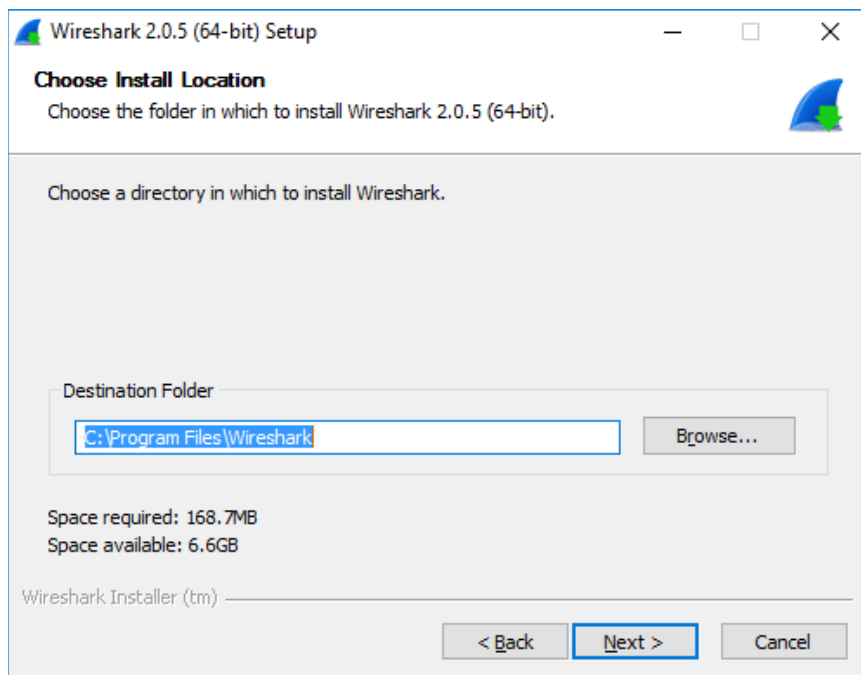
- c. Se esta for a primeira instalação do Wireshark, ou após concluir o processo de desinstalação, você navegará para o assistente de configuração do Wireshark. Clique em **Avançar**.



- d. Continue avançando no processo de instalação. Clique em **I Agree** (Eu concordo) quando a janela do contrato de licença for exibida.
- e. Mantenha as configurações padrão na janela Choose Components (Escolher componentes) e clique em **Next** (Avançar).
- f. Escolha suas opções de atalho desejadas e clique em **Next** (Avançar).

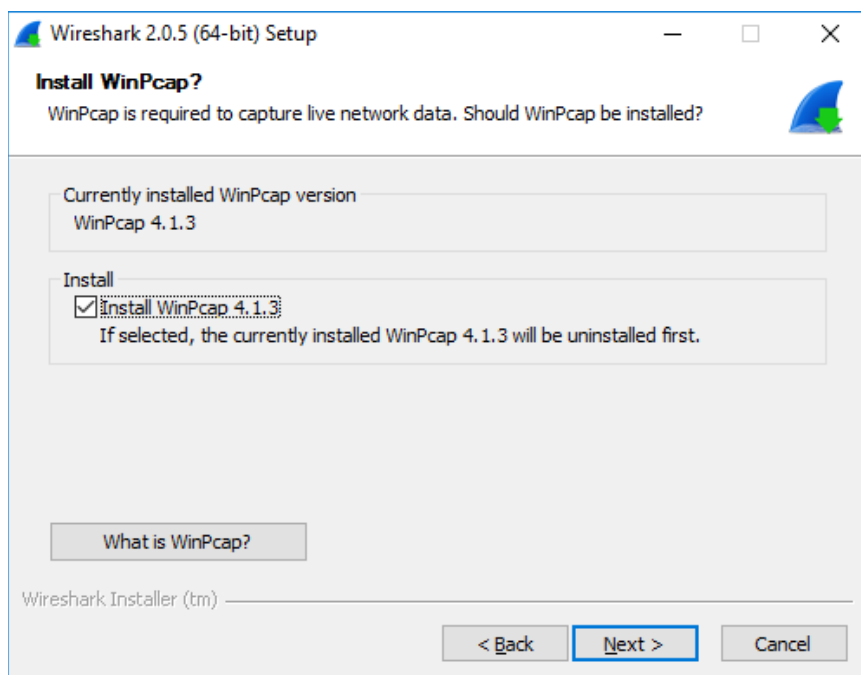


- g. Você pode alterar o local de instalação do Wireshark, porém, a menos que você tenha espaço em disco limitado, recomenda-se manter o local padrão.



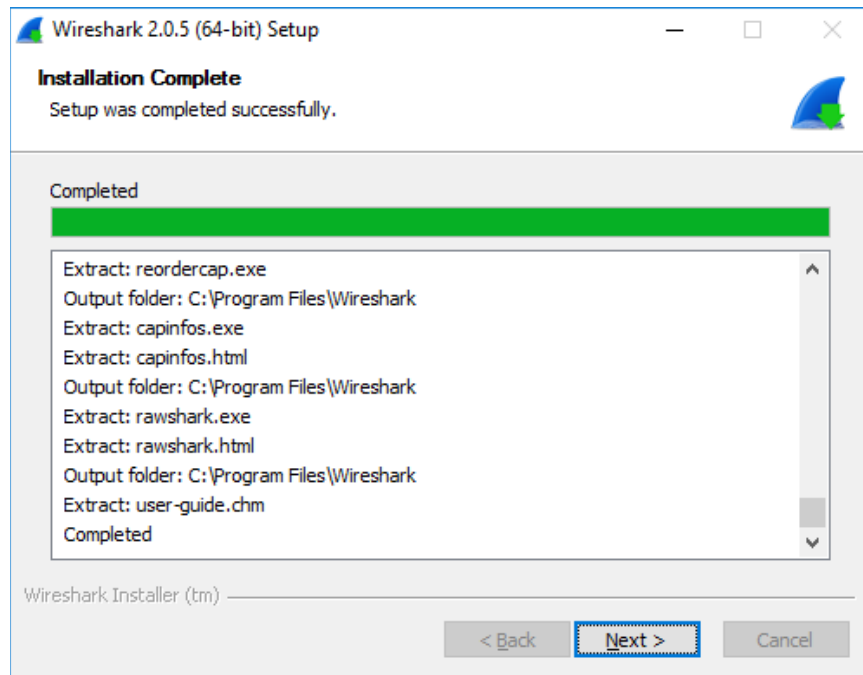
- h. Para capturar dados da rede ativa, o WinPcap deve estar instalado no PC. Se o WinPcap já estiver instalado no PC, a caixa de seleção Install (Instalar) será desmarcada. Se a versão instalada do WinPcap for mais antiga que a versão que acompanha o Wireshark, é recomendado permitir que a versão mais recente seja instalada clicando na caixa de seleção **Install WinPcap x.x.x** (Instalar o WinPcap x.x.x) (número da versão).

Conclua o assistente de configuração do WinPcap se estiver instalando o WinPcap.

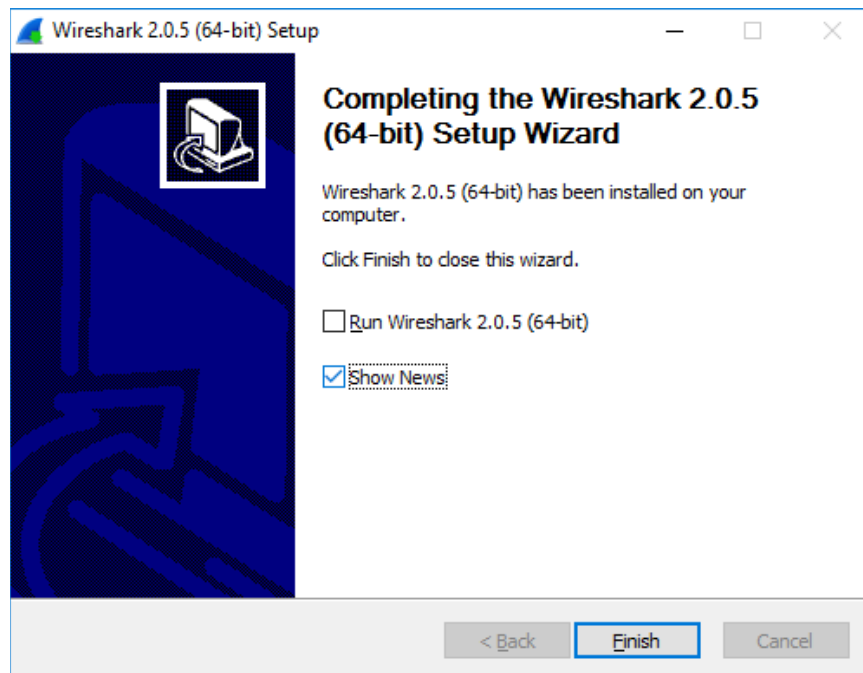


Observação: talvez seja solicitado que você instale o USBPcap. A instalação do USBPcap é opcional.

- i. O Wireshark começa a instalar seus arquivos e exibe uma janela separada com o status da instalação. Clique em **Next** (Próximo) quando a instalação estiver concluída.



- j. Clique em **Finish** (Concluir) para encerrar o processo de instalação do Wireshark.



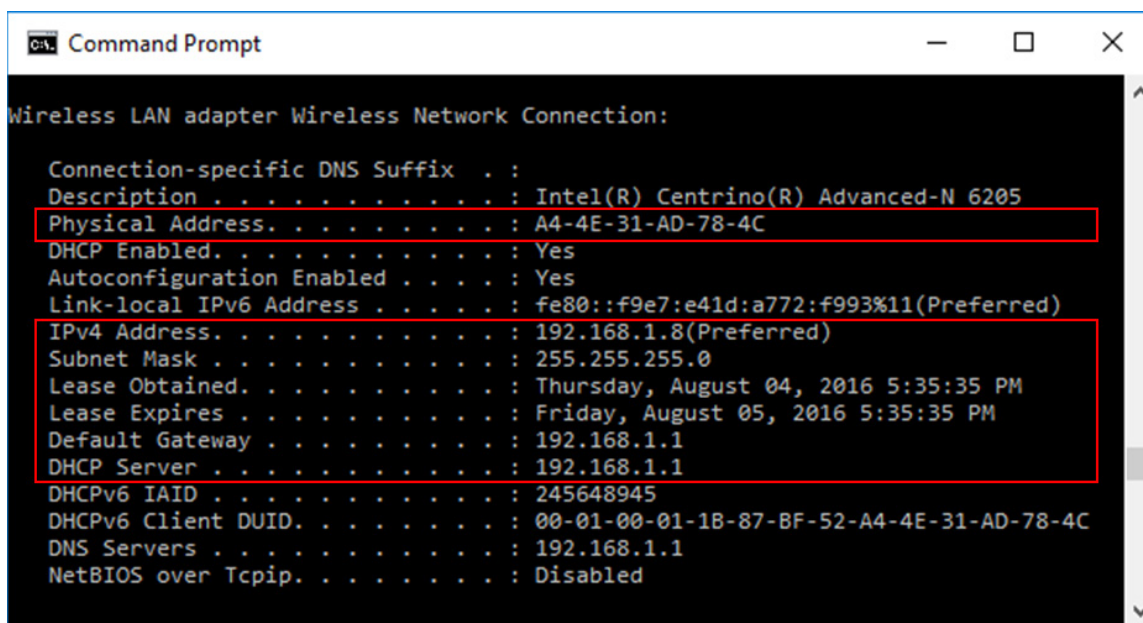
Parte 2: Capturar e analisar dados locais ARP no Wireshark

Na Parte 2 deste laboratório, você efetuará ping para outro computador na LAN e capturará solicitações e respostas ARP 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 IPv4 e o endereço MAC do PC.

- Abra uma janela de comando, digite **ipconfig /all**, e pressione Enter.
- Observe qual adaptador de rede o PC está usando para acessar a rede. Registre o endereço IPv4 e o endereço MAC (endereço físico) da interface do PC.



```
Command Prompt

Wireless LAN adapter Wireless Network Connection:

Connection-specific DNS Suffix . : 
Description . . . . . : Intel(R) Centrino(R) Advanced-N 6205
Physical Address. . . . . : A4-4E-31-AD-78-4C
DHCP Enabled. . . . . : Yes
Autoconfiguration Enabled . . . . : Yes
Link-local IPv6 Address . . . . . : fe80::f9e7:e41d:a772:f993%11(Preferred)
IPv4 Address. . . . . : 192.168.1.8(Preferred)
Subnet Mask . . . . . : 255.255.255.0
Lease Obtained. . . . . : Thursday, August 04, 2016 5:35:35 PM
Lease Expires . . . . . : Friday, August 05, 2016 5:35:35 PM
Default Gateway . . . . . : 192.168.1.1
DHCP Server . . . . . : 192.168.1.1
DHCPv6 IAID . . . . . : 245648945
DHCPv6 Client DUID. . . . . : 00-01-00-01-1B-87-BF-52-A4-4E-31-AD-78-4C
DNS Servers . . . . . : 192.168.1.1
NetBIOS over Tcpip. . . . . : Disabled
```

- Solicite a um membro da equipe o endereço IPv4 do PC dele e forneça a ele o endereço IPv4 do seu PC. Não forneça o seu endereço MAC a ele agora.

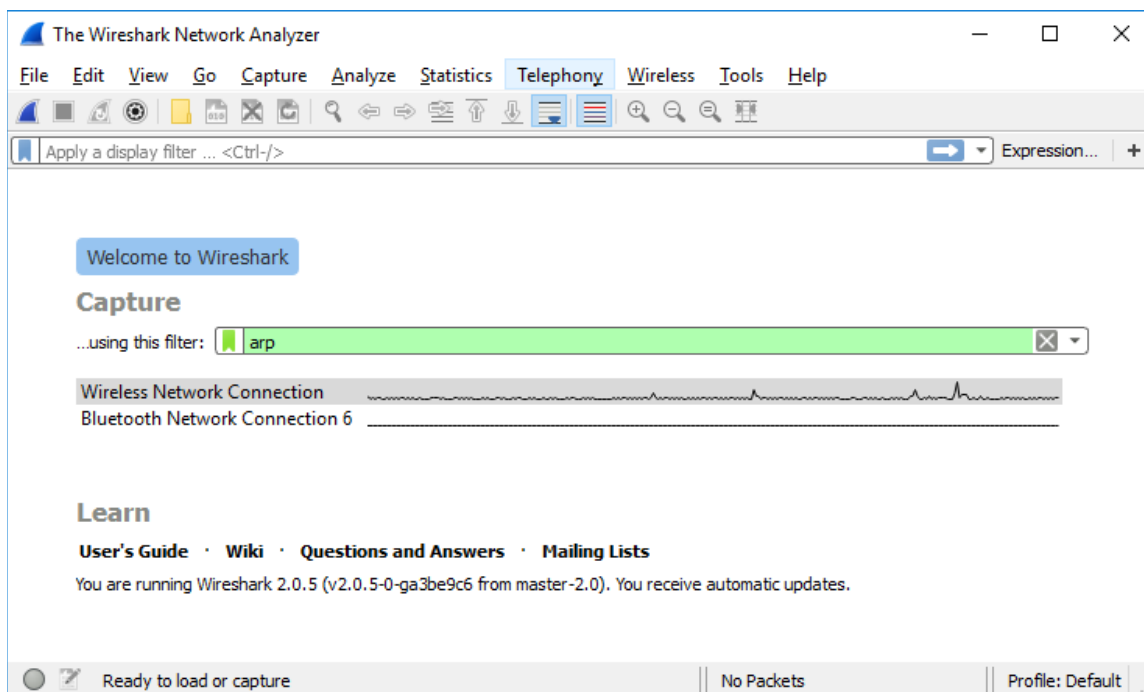
Registre os endereços IPv4 do gateway padrão e dos outros PCs na LAN.

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

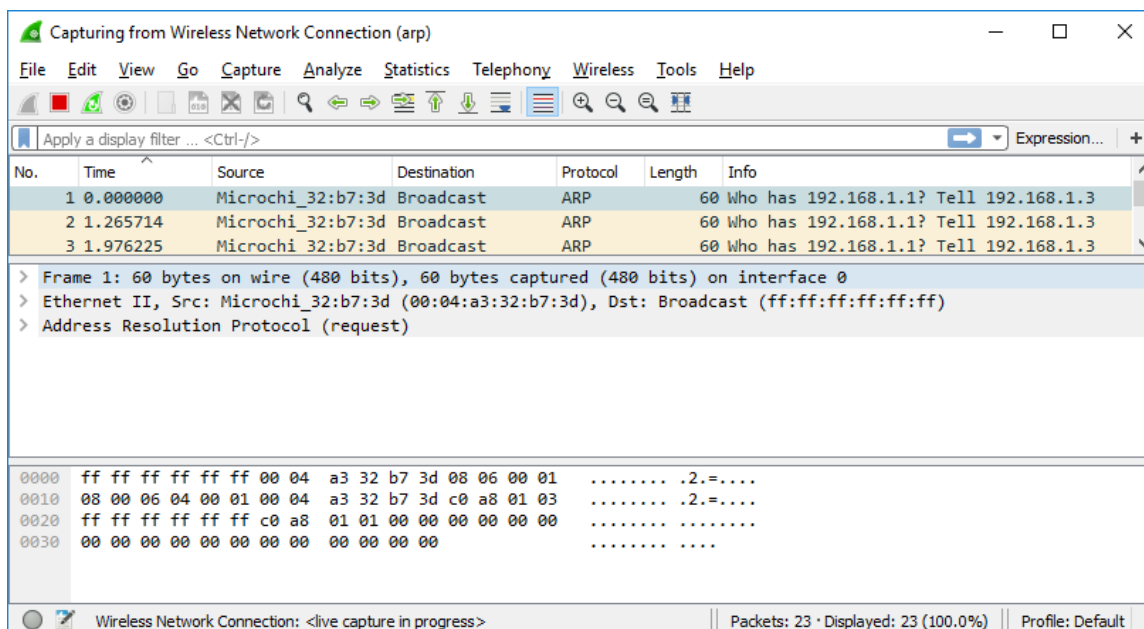
- No PC, clique em **Iniciar** e digite **Wireshark**. Clique em **Wireshark Desktop App** (Aplicativo para Desktop Wireshark) quando ele aparecer na janela de resultados de busca.

Observação: como alternativa, a instalação do Wireshark também pode fornecer uma opção do Wireshark antigo. Ela mostra o Wireshark na GUI antiga e mais reconhecida. O restante deste laboratório foi concluído com a GUI de aplicativo para desktop mais nova.

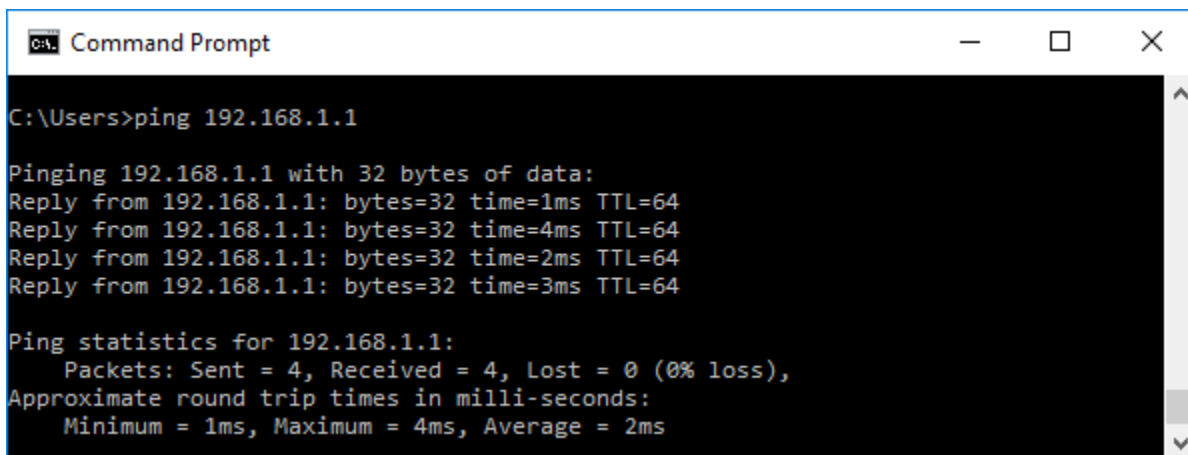
- b. Após iniciar o Wireshark, selecione a interface de rede que você identificou com o comando **ipconfig**. Insira **arp** na caixa de filtro. Essa seleção configura o Wireshark para exibir somente os pacotes que fazem parte das trocas ARP entre os dispositivos na rede local.



- c. Após selecionar a interface correta e inserir as informações de filtro, clique em **Start** (🔍) (Iniciar) para começar a captura de dados. As informações começarão a rolar abaixo da seção superior no Wireshark. Cada linha representa uma mensagem sendo enviada entre um dispositivo de origem e destino na rede.



- d. Abra uma janela de prompt de comando. Use o comando **ping** para testar a conectividade para o endereço de gateway padrão que você identificou na Parte 2, etapa 1c.



```
C:\Users>ping 192.168.1.1

Pinging 192.168.1.1 with 32 bytes of data:
Reply from 192.168.1.1: bytes=32 time=1ms TTL=64
Reply from 192.168.1.1: bytes=32 time=4ms TTL=64
Reply from 192.168.1.1: bytes=32 time=2ms TTL=64
Reply from 192.168.1.1: bytes=32 time=3ms TTL=64

Ping statistics for 192.168.1.1:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 1ms, Maximum = 4ms, Average = 2ms
```

- e. Execute ping nos endereços IPv4 de outros PCs na LAN que foram fornecidos pelos membros da sua equipe.

Observação: se o PC da sua equipe não responde aos pings, isso pode acontecer porque o firewall do PC está bloqueando as solicitações. Peça ajuda ao seu instrutor se for necessário desativar o firewall do PC.

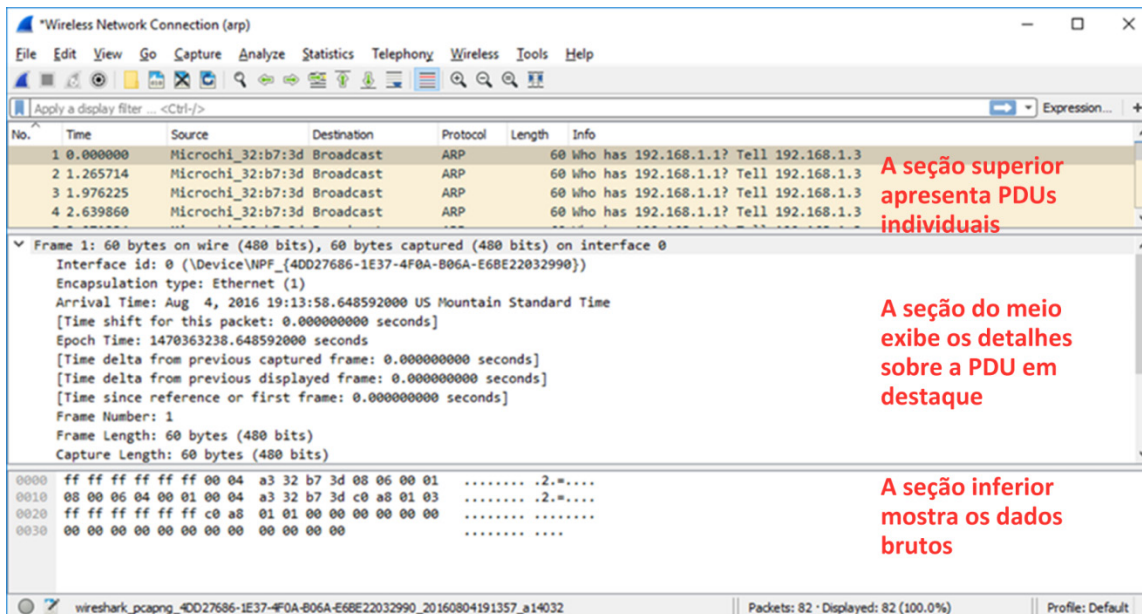
- f. Interrompa a captura de dados ao clicar em **Stop Capture** () (Interromper Captura) na barra de ferramentas.

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 capturados com um sumário das informações do pacote de IPv4 listado.
- 2) A seção média lista as informações de PDU do quadro selecionado na parte superior da tela e separa um quadro de PDU capturado pelas suas camadas de protocolo.

- 3) A seção inferior mostra os dados brutos de cada camada. Os dados são exibidos em formato hexadecimal e decimal.

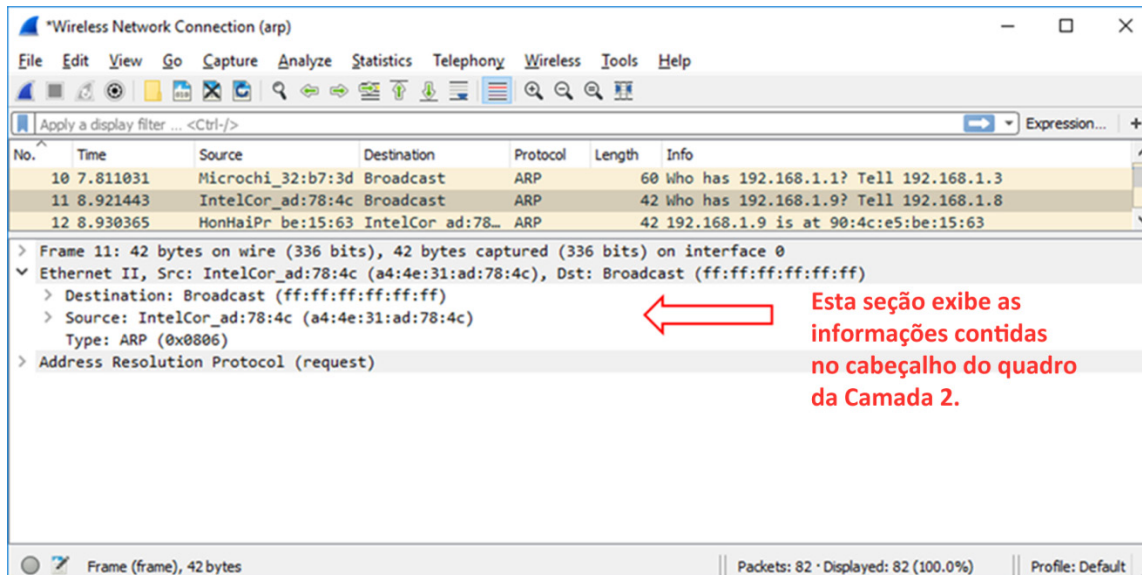


A seção superior apresenta PDUs individuais

A seção do meio exibe os detalhes sobre a PDU em destaque

A seção inferior mostra os dados brutos

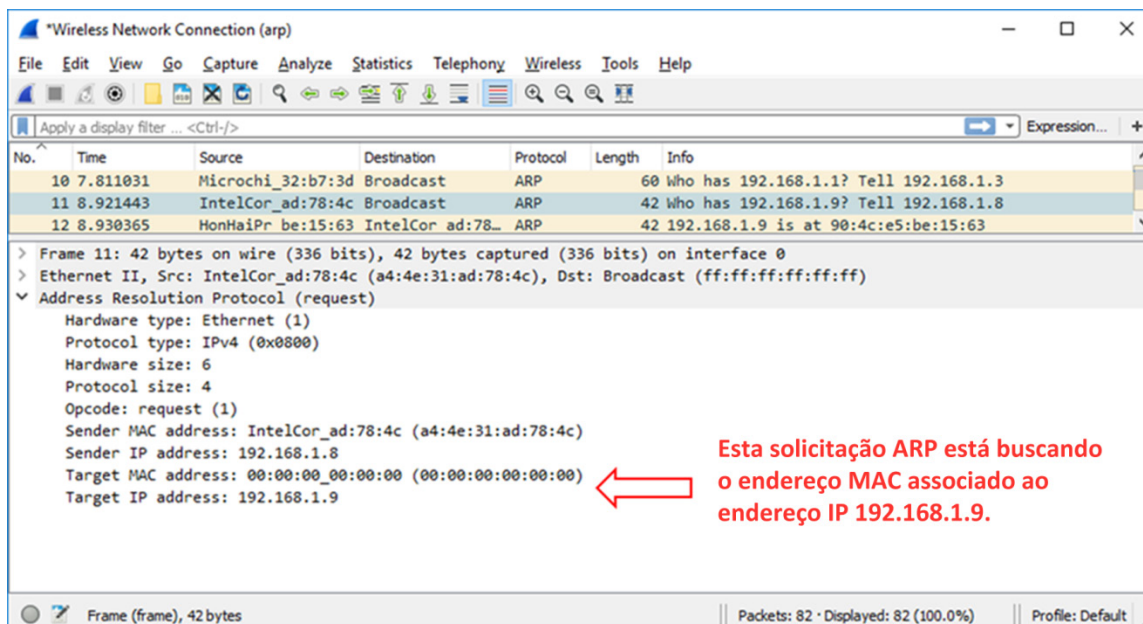
- Clique nos quadros ARP na seção superior que tem o endereço MAC do seu PC como o endereço de origem no quadro e “transmissão” como o destino do quadro.
- Com esse quadro de PDU ainda selecionado na seção superior, vá até a seção média. Clique na seta à esquerda da linha Ethernet II para ver os endereços MAC de origem e destino.



Esta seção exibe as informações contidas no cabeçalho do quadro da Camada 2.

O endereço MAC de origem corresponde à interface do PC? _____

- c. Clique na seta à esquerda da linha Protocolo ARP (solicitação) para visualizar o conteúdo da solicitação ARP.



Etapa 4: Localize o quadro da resposta ARP que corresponde à solicitação ARP que você destacou.

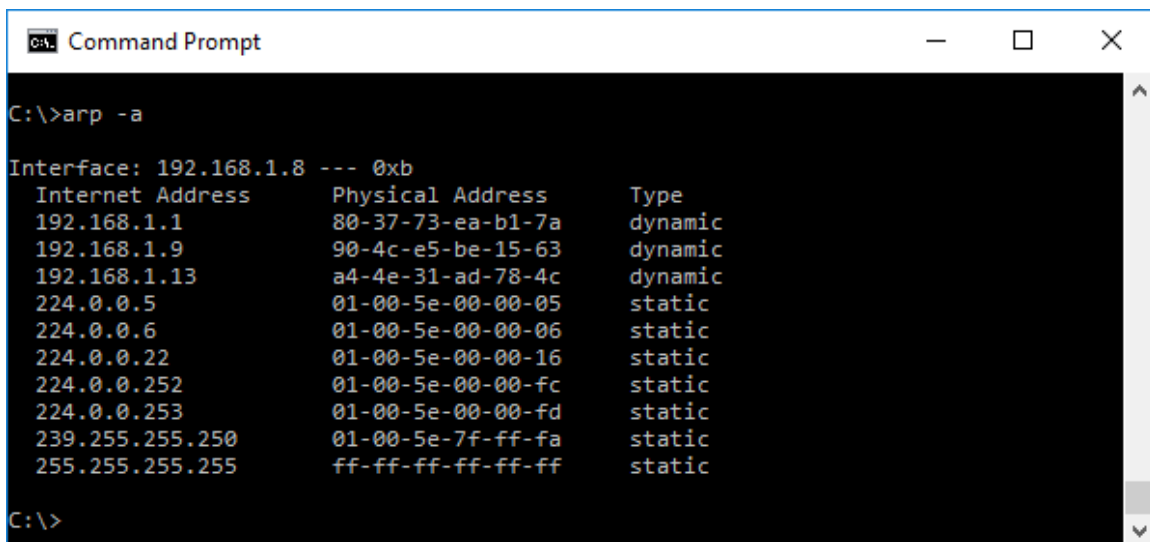
- Com o endereço IPv4 alvo na solicitação ARP, localize o quadro da resposta ARP na seção superior da tela de captura do Wireshark.
Qual é o endereço IPv4 do dispositivo alvo na sua solicitação ARP? _____
- Destaque o quadro de resposta na seção superior da saída do Wireshark. Talvez seja necessário rolar a janela para encontrar o quadro de resposta que corresponde ao endereço IPv4 alvo identificado na etapa anterior. Expanda as linhas Ethernet II e protocolo ARP (resposta) na seção média da tela.
O quadro de resposta ARP é um quadro de transmissão? _____
Qual é o endereço MAC destino do quadro? _____
Qual é o endereço MAC do seu PC? _____
Qual endereço MAC é a origem do quadro? _____
- Verifique com sua equipe se o endereço MAC corresponde ao endereço MAC no PC deles.

Parte 3: Examine as entradas do cache ARP no PC

Após a resposta ARP ser recebida pelo PC, a associação do endereço MAC para o endereço IPv4 é armazenada na memória do cache no PC. Essas entradas permanecerão na memória por um curto período (de 15 a 45 segundos), e, depois, se não forem usadas nesse período, serão removidas do cache.

Etapa 1: Visualize as entradas do cache ARP em um PC com Windows.

- a. Abra uma janela de prompt de comando em um PC. No prompt, insira **arp -a** e pressione enter.



```
Command Prompt

C:\>arp -a

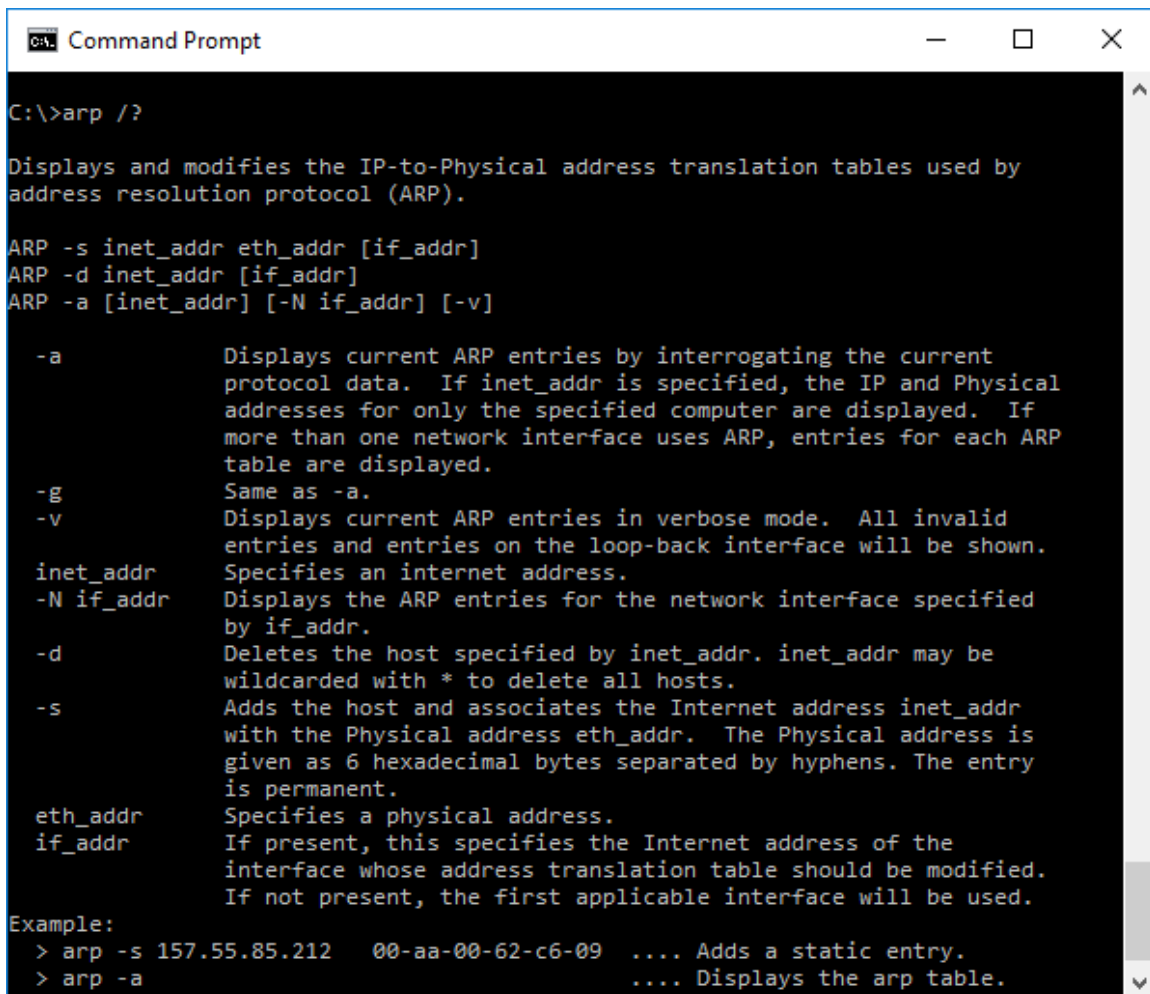
Interface: 192.168.1.8 --- 0xb
 Internet Address      Physical Address      Type
 192.168.1.1           80-37-73-ea-b1-7a     dynamic
 192.168.1.9           90-4c-e5-be-15-63     dynamic
 192.168.1.13          a4-4e-31-ad-78-4c     dynamic
 224.0.0.5             01-00-5e-00-00-05     static
 224.0.0.6             01-00-5e-00-00-06     static
 224.0.0.22            01-00-5e-00-00-16     static
 224.0.0.252           01-00-5e-00-00-fc     static
 224.0.0.253           01-00-5e-00-00-fd     static
 239.255.255.250       01-00-5e-7f-ff-fa     static
 255.255.255.255       ff-ff-ff-ff-ff-ff     static

C:\>
```

A saída do comando **arp -a** exibirá as entradas que estão no cache no PC. No exemplo, o PC tem entradas para o gateway padrão (192.168.1.1) e para dois PCs localizados na mesma LAN (192.168.1.9 e 192.168.1.13).

Qual é o resultado da execução do comando **arp -a** no seu PC?

- b. O comando **arp** no PC com Windows tem outra funcionalidade. Insira **arp /?** no prompt de comando e pressione enter. As opções do comando **arp** permitem que você visualize, adicione e remova as entradas da tabela ARP, se necessário.



```
Command Prompt

C:\>arp /?

Displays and modifies the IP-to-Physical address translation tables used by
address resolution protocol (ARP).

ARP -s inet_addr eth_addr [if_addr]
ARP -d inet_addr [if_addr]
ARP -a [inet_addr] [-N if_addr] [-v]

    -a          Displays current ARP entries by interrogating the current
                  protocol data.  If inet_addr is specified, the IP and Physical
                  addresses for only the specified computer are displayed.  If
                  more than one network interface uses ARP, entries for each ARP
                  table are displayed.
    -g          Same as -a.
    -v          Displays current ARP entries in verbose mode.  All invalid
                  entries and entries on the loop-back interface will be shown.
inet_addr      Specifies an internet address.
-N if_addr     Displays the ARP entries for the network interface specified
                  by if_addr.
-d            Deletes the host specified by inet_addr.  inet_addr may be
                  wildcarded with * to delete all hosts.
-s            Adds the host and associates the Internet address inet_addr
                  with the Physical address eth_addr.  The Physical address is
                  given as 6 hexadecimal bytes separated by hyphens.  The entry
                  is permanent.
eth_addr       Specifies a physical address.
if_addr        If present, this specifies the Internet address of the
                  interface whose address translation table should be modified.
                  If not present, the first applicable interface will be used.

Example:
> arp -s 157.55.85.212 00-aa-00-62-c6-09 .... Adds a static entry.
> arp -a          .... Displays the arp table.
```

Qual opção exclui uma entrada do cache ARP? _____

Qual seria o resultado da emissão do comando **arp -d ***? _____

Reflexão

1. Qual é o benefício de manter as entradas do cache ARP na memória no computador de origem?

2. Se o endereço IPv4 destino não está localizado na mesma rede que o host de origem, qual endereço MAC será usado como o endereço MAC alvo destino no quadro?
