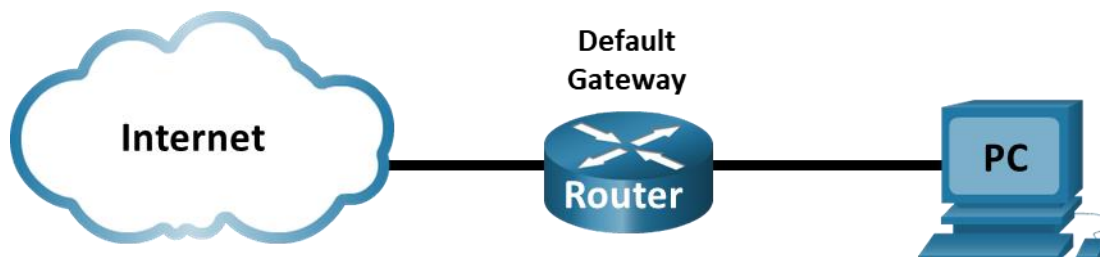


Laboratório - Use o Wireshark para examinar os quadros Ethernet

Topologia



Objetivos

Parte 1: Examinar os campos do cabeçalho de um quadro Ethernet II

Parte 2: Usar o Wireshark para capturar e analisar quadros Ethernet

Histórico/Cenário

Quando os protocolos da camada superior se comunicam uns com os outros, os dados fluem para baixo pelas camadas OSI (Open Systems Interconnection) e são encapsulados dentro de um quadro da Camada 2. A composição do quadro depende do tipo de acesso ao meio. Por exemplo, se os protocolos de camada superior forem TCP/IP e o acesso ao meio for Ethernet, o encapsulamento do quadro da Camada 2 será Ethernet II. Isso é comum em um ambiente de LAN.

Ao estudar os conceitos da Camada 2, vale a pena analisar as informações do cabeçalho do quadro. Na primeira parte deste laboratório, você examinará os campos contidos em um quadro Ethernet II. Na Parte 2, você usará o Wireshark para capturar e analisar os campos do cabeçalho de quadros Ethernet II para tráfego local e remoto.

Recursos necessários

- 1 PC (Windows com acesso à Internet e com o Wireshark instalado)

Instruções

Parte 1: Examinar os Campos do Cabeçalho de um Quadro Ethernet II

Na Parte 1, você examinará o conteúdo e os campos do cabeçalho de um quadro Ethernet II. Será usada uma captura do Wireshark para examinar o conteúdo nesses campos.

Etapa 1: Analise os tamanhos e as descrições dos campos do cabeçalho Ethernet II.

Introdução	Endereço de destino	Endereço de Origem	Tipo de moldura	Dados	FCS
8 bytes	6 bytes	6 bytes	2 bytes	46 a 1.500 bytes	4 bytes

Etapa 2: Examinar a configuração de rede do PC.

Neste exemplo, este endereço IP do host do PC é 192.168.1.147 e o gateway padrão possui um endereço IP 192.168.1.1.

```
C:\> ipconfig /all
```

```
Ethernet adapter Ethernet:
```

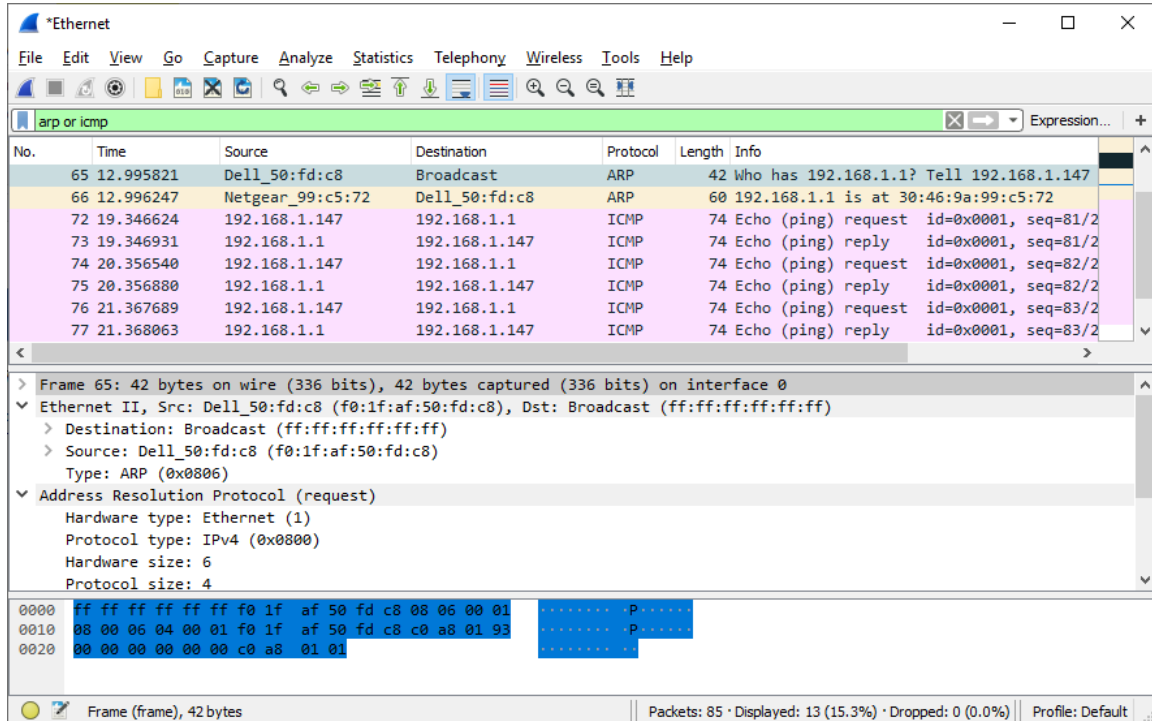
```
    Específico de Conexão Sufixo DNS. :  
    Descrição . . . . . : Intel(R) 82579LM Gigabit Network Connection  
    Endereço Físico. . . . . : F0-1F-AF-50-FD-C8  
    DHCP Enabled. . . . . : Yes  
    Autoconfiguration Enabled . . . . : Yes  
    Link-local IPv6 Address . . . . . : fe80: :58c 5:45 f 2:7 e5e:29c 2% 11  
(Preferencial)  
    IPv4 Address. . . . . : 192.168.1.147(Preferred)  
    Máscara de Sub-Rede . . . . . : 255.255.255.0  
    Lease Obtained. . . . . : Sexta, 6 de Setembro de 2019 11:08:36  
    Lease Expires . . . . . : sábado, 7 de setembro de 2019 11:08:36  
    Gateway Padrão . . . . . : 192.168.1.1  
    DHCP Server . . . . . : 192.168.1.1  
<output omitted>
```

Etapa 3: Examine os quadros Ethernet em uma captura do Wireshark.

As capturas de tela da captura do Wireshark abaixo mostram os pacotes gerados por um ping emitido de um host do PC para o gateway padrão. Um filtro foi aplicado ao Wireshark para visualizar somente os protocolos ARP e ICMP. ARP significa protocolo de resolução de endereços. ARP é um protocolo de comunicação que é usado para determinar o endereço MAC associado ao endereço IP. A sessão começa com uma consulta ARP e uma resposta para o endereço MAC do roteador de gateway, seguido por quatro solicitações e respostas de ping.

Laboratório - Use o Wireshark para examinar os quadros Ethernet

Esta captura de tela realça os detalhes do quadro de uma solicitação ARP.



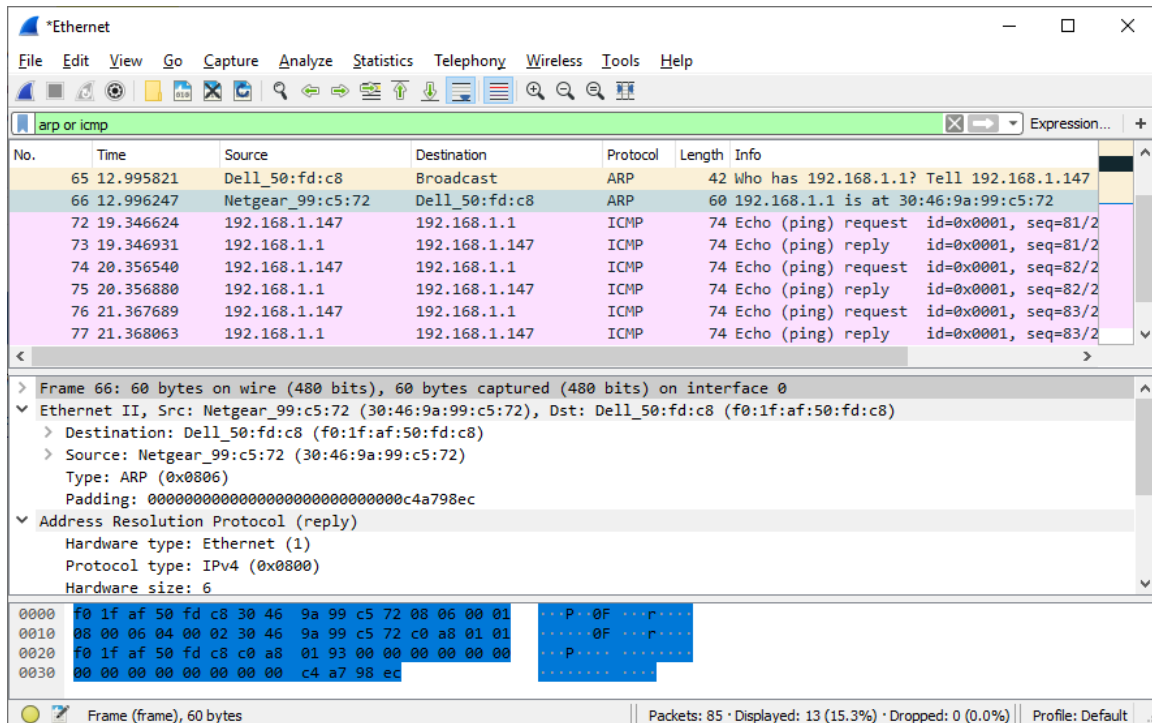
The screenshot shows the Wireshark interface with the filter 'arp or icmp'. The packet list displays several packets, with packet 65 highlighted. The packet details pane shows the structure of the ARP request:

- Frame 65: 42 bytes on wire (336 bits), 42 bytes captured (336 bits) on interface 0
- Ethernet II, Src: Dell_50:fd:c8 (f0:1f:af:50:fd:c8), Dst: Broadcast (ff:ff:ff:ff:ff:ff)
- Destination: Broadcast (ff:ff:ff:ff:ff:ff)
- Source: Dell_50:fd:c8 (f0:1f:af:50:fd:c8)
- Type: ARP (0x0806)
- Address Resolution Protocol (request)
 - Hardware type: Ethernet (1)
 - Protocol type: IPv4 (0x0800)
 - Hardware size: 6
 - Protocol size: 4

The packet bytes pane shows the raw data for the ARP request:

```
0000 ff ff ff ff ff f0 1f af 50 fd c8 08 06 00 01
0010 08 00 06 04 00 01 f0 1f af 50 fd c8 c0 a8 01 93
0020 00 00 00 00 00 00 c0 a8 01 01
```

Esta captura de tela realça os detalhes do quadro de uma resposta ARP.



The screenshot shows the Wireshark interface with the filter 'arp or icmp'. The packet list displays several packets, with packet 66 highlighted. The packet details pane shows the structure of the ARP reply:

- Frame 66: 60 bytes on wire (480 bits), 60 bytes captured (480 bits) on interface 0
- Ethernet II, Src: Netgear_99:c5:72 (30:46:9a:99:c5:72), Dst: Dell_50:fd:c8 (f0:1f:af:50:fd:c8)
- Destination: Dell_50:fd:c8 (f0:1f:af:50:fd:c8)
- Source: Netgear_99:c5:72 (30:46:9a:99:c5:72)
- Type: ARP (0x0806)
- Padding: 00000000000000000000000000000000c4a798ec
- Address Resolution Protocol (reply)
 - Hardware type: Ethernet (1)
 - Protocol type: IPv4 (0x0800)
 - Hardware size: 6

The packet bytes pane shows the raw data for the ARP reply:

```
0000 f0 1f af 50 fd c8 30 46 9a 99 c5 72 08 06 00 01
0010 08 00 06 04 00 02 30 46 9a 99 c5 72 c0 a8 01 01
0020 f0 1f af 50 fd c8 c0 a8 01 93 00 00 00 00 00 00
0030 00 00 00 00 00 00 c4 a7 98 ec
```

Etapa 4: Examine o conteúdo do cabeçalho Ethernet II de uma requisição ARP.

A tabela a seguir usa o primeiro quadro na captura do Wireshark e exibe os dados nos campos do cabeçalho Ethernet II.

Campo	Valor	Descrição
Preâmbulo	Não mostrado na captura	Este campo contém bits de sincronização, processados pelo hardware da NIC.
Endereço Destino	Broadcast (ff:ff:ff:ff:ff:ff)	Endereços de Camada 2 para o quadro. Cada endereço tem 48 bits (ou 6 octetos), expressos como 12 dígitos hexadecimais, 0–9, A–F. Um formato comum é 12:34:56:78:9A:BC.
Endereço Origem	NETGear_99:C 5:72 (30:46:9 a:99:c 5:72)	Os primeiros seis números hexadecimais indicam o fabricante da placa de interface de rede (NIC) e os últimos seis números hexadecimais são o número de série dela. O endereço destino pode ser broadcast, que contém todos os valores em 1, ou unicast. O endereço origem é sempre unicast.
Tipo de quadro	0x0806	Nos quadros Ethernet II, este campo contém um valor hexadecimal que é usado para indicar o tipo de protocolo de camada superior no campo de dados. Há muitos protocolos de camadas superiores compatíveis com Ethernet II. Dois tipos de quadros comuns são: Valor Descrição Protocolo IPv4 0x0800 0x0806 Protocolo de resolução de endereço (ARP)
Dados	ARP	Contém o protocolo de nível superior encapsulado. O campo de dados varia de 46 a 1.500 bytes.
FCS	Não mostrado na captura	Sequência de Verificação de Quadro (FCS), usado pela NIC para identificar erros durante a transmissão. O valor é calculado pelo dispositivo de envio, incluindo endereços de quadro, tipo e campo de dados. Isso é verificado pelo receptor.

Qual é a importância do conteúdo do campo Endereço Destino?

Resposta: O conteúdo do campo Endereço Destino (Broadcast: ff:ff:ff:ff:ff:ff) é fundamental porque garante que a requisição ARP alcance todos os dispositivos na rede local. Como a requisição ARP busca descobrir o endereço MAC associado a um IP específico, o broadcast permite que todos os dispositivos recebam a mensagem. Somente o dispositivo com o IP correspondente responderá com seu MAC, enquanto os demais a ignoram.

Por que o PC envia um broadcast ARP antes da primeira requisição ping?

Resposta: O PC envia um broadcast ARP antes da primeira requisição ping porque o protocolo ICMP (usado pelo ping) depende do endereço MAC do destino para entregar o quadro na rede local. Como o PC não conhece inicialmente o MAC associado ao IP de destino, ele não pode montar o quadro Ethernet corretamente.

Qual é o endereço MAC origem no primeiro quadro?

Resposta: O endereço MAC origem no primeiro quadro é (f0:1f:af:50:fd:c8)

Qual é o ID do fornecedor (OUI) da NIC de origem na resposta do ARP?

Resposta: O ID do fornecedor (OUI) da NIC de origem na resposta do ARP é (30:46:9a)

Que parte do endereço MAC é a OUI?

Resposta: A OUI (Organizationally Unique Identifier) corresponde aos primeiros 24 bits (3 octetos) do endereço MAC. Ela identifica o fabricante ou organização responsável pelo dispositivo de rede. Por exemplo, no endereço (30:46:9A:99:C5:72), a OUI é (30:46:9a).

Qual é o número serial da NIC de origem?

Resposta: O número serial da NIC de origem corresponde aos últimos 24 bits (3 octetos) do endereço MAC, definidos pelo fabricante. Por exemplo, no endereço (30:46:9A:99:C5:72), o número de série da NIC é (99:c5:72).

Parte 2: Usar o Wireshark para capturar e analisar quadros Ethernet II

Na Parte 2, você usará o Wireshark para capturar quadros Ethernet locais e remotos. Em seguida, examinará as informações contidas nos campos do cabeçalho do quadro.

Etapa 1: Determinar o endereço IP do gateway padrão em seu PC.

Abra uma janela do prompt de comando e emita o comando **ipconfig**.

Qual é o endereço IP do gateway padrão do PC?

Resposta: O endereço IP do gateway padrão do PC é (10.120.63.254).

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

```
Sufixo DNS específico de conexão. . . . . : univali.br
Endereço IPv6 de link local . . . . . : fe80::aacc:6d9e:f1c4:f612%6
Endereço IPv4. . . . . : 10.120.8.215
Máscara de Sub-rede . . . . . : 255.255.192.0
Gateway Padrão. . . . . : 10.120.63.254
```

Etapa 2: Iniciar a captura do tráfego na NIC do seu PC.

- Abra o Wireshark para iniciar a captura de dados.
- Observe o tráfego que aparece na janela Packet List (Lista de pacotes).

Etapa 3: Filtrar o Wireshark para exibir apenas o tráfego ICMP.

Você pode usar o filtro do Wireshark para bloquear a visibilidade de tráfego indesejado. O filtro não bloqueia a captura de dados indesejados; apenas filtra o que você deseja exibir na tela. Por enquanto, deve ser exibido somente tráfego ICMP.

Na caixa **Filtro** do Wireshark, digite **icmp**. A caixa deve ficar verde se você digitou corretamente o filtro. Se a caixa estiver verde, clique em **Apply** (Aplicar) (a seta à direita) para aplicar o filtro.

Etapa 4: Na janela do prompt de comando, fazer ping no gateway padrão do seu PC.

Na janela de comando, faça ping no gateway padrão usando o endereço IP registrado na Etapa 1.

Etapa 5: Interromper a captura de tráfego na NIC.

Clique no ícone **Parar de capturar pacotes** para parar de capturar o tráfego.

Etapa 6: Examine a primeira requisição (ping) de eco no Wireshark.

A janela principal do Wireshark é dividida em três seções: o painel **Packet List** (Lista de pacotes) (superior), o painel **Packet Details** (Detalhes do pacote) (intermediária) e o painel **Packet Bytes** (Bytes do pacote) (inferior). Se você selecionou a interface correta para a captura de pacotes anteriormente, o Wireshark deve exibir as informações do ICMP no painel da lista de pacotes do Wireshark.

- No painel **Packet List** (Lista de pacotes) [seção superior], clique no primeiro quadro listado. Você deve ver **Echo (ping) request** no cabeçalho **Info (Informações)**. A linha deve agora ser realçada.
- Examine a primeira linha no painel **Packet Details** (Detalhes do pacote) [seção intermediária]. Esta linha exibe o comprimento do quadro.
- A segunda linha no painel **Packet Details** (Detalhes do pacote) mostra que se trata de um quadro Ethernet II. Os endereços MAC de origem e de destino também são exibidos.

Qual é o endereço MAC da NIC do PC?

Resposta: O endereço MAC da NIC do PC é (c8:15:4e:ac:9c:d9).

```
▶ Frame 10072: 74 bytes on wire (592 bits), 74 bytes captured (592 bits) on interface \Device\NPF_{32A5BDF...}
▼ Ethernet II, Src: Intel_ac:9c:d9 (c8:15:4e:ac:9c:d9), Dst: HewlettPacka_60:24:00 (08:f1:ea:60:24:00)
  ▶ Destination: HewlettPacka_60:24:00 (08:f1:ea:60:24:00)
  ▶ Source: Intel_ac:9c:d9 (c8:15:4e:ac:9c:d9)
    Type: IPv4 (0x0800)
    [Stream index: 13]
  ▶ Internet Protocol Version 4, Src: 10.120.8.215, Dst: 10.120.63.254
  ▶ Internet Control Message Protocol
```

Qual é o endereço MAC do gateway padrão?

Resposta: O endereço MAC do gateway padrão é (08:f1:ea:60:24:00).

```
▶ Frame 10072: 74 bytes on wire (592 bits), 74 bytes captured (592 bits) on interface \Device\NPF_{32A5BDF...}
▼ Ethernet II, Src: Intel_ac:9c:d9 (c8:15:4e:ac:9c:d9), Dst: HewlettPacka_60:24:00 (08:f1:ea:60:24:00)
  ▶ Destination: HewlettPacka_60:24:00 (08:f1:ea:60:24:00)
  ▶ Source: Intel_ac:9c:d9 (c8:15:4e:ac:9c:d9)
    Type: IPv4 (0x0800)
    [Stream index: 13]
  ▶ Internet Protocol Version 4, Src: 10.120.8.215, Dst: 10.120.63.254
  ▶ Internet Control Message Protocol
```

- Você pode clicar no sinal de mais que (>) no início da segunda linha para obter mais informações sobre o quadro Ethernet II.

Que tipo de quadro é exibido?

Resposta: O tipo de quadro exibido é IPv4 (0x0800)

- e. As duas últimas linhas exibidas na parte intermediária fornecem informações sobre o campo de dados do quadro. Observe que os dados contêm informações do endereço IPv4 origem e destino.

Qual é o endereço IP de origem?

Resposta: O endereço IP de origem é (10.120.8.215).

```
▼ Internet Protocol Version 4, Src: 10.120.8.215, Dst: 10.120.63.254
  0100 .... = Version: 4
  .... 0101 = Header Length: 20 bytes (5)
  ▶ Differentiated Services Field: 0x00 (DSCP: CS0, ECN: Not-ECT)
    Total Length: 60
    Identification: 0x2a87 (10887)
  ▶ 000. .... = Flags: 0x0
    ...0 0000 0000 0000 = Fragment Offset: 0
    Time to Live: 128
    Protocol: ICMP (1)
    Header Checksum: 0x0000 [validation disabled]
    [Header checksum status: Unverified]
    Source Address: 10.120.8.215
    Destination Address: 10.120.63.254
    [Stream index: 178]
```

Qual é o endereço IP de destino?

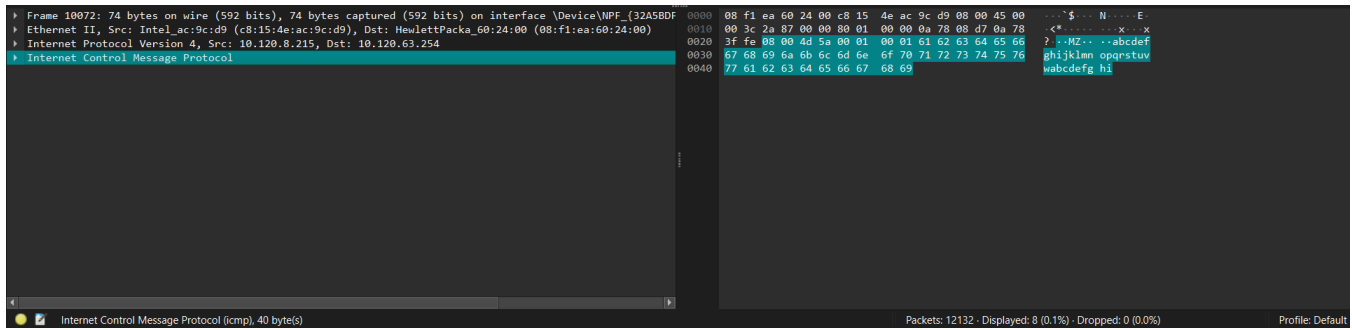
Resposta: O endereço IP de destino é (10.120.63.254).

```
▼ Internet Protocol Version 4, Src: 10.120.8.215, Dst: 10.120.63.254
  0100 .... = Version: 4
  .... 0101 = Header Length: 20 bytes (5)
  ▶ Differentiated Services Field: 0x00 (DSCP: CS0, ECN: Not-ECT)
    Total Length: 60
    Identification: 0x2a87 (10887)
  ▶ 000. .... = Flags: 0x0
    ...0 0000 0000 0000 = Fragment Offset: 0
    Time to Live: 128
    Protocol: ICMP (1)
    Header Checksum: 0x0000 [validation disabled]
    [Header checksum status: Unverified]
    Source Address: 10.120.8.215
    Destination Address: 10.120.63.254
    [Stream index: 178]
```

- f. Clique em qualquer linha na seção intermediária para destacar a parte do quadro (hexadecimal e ASCII) no painel **Packet Bytes** (Bytes do pacote) [seção inferior]. Clique na linha **Internet Control Message Protocol** (Protocolo ICMP) na seção intermediária e examine o que está destacado no painel **Packet Bytes** (Bytes do pacote).

O que dizem os dois últimos octetos destacados?

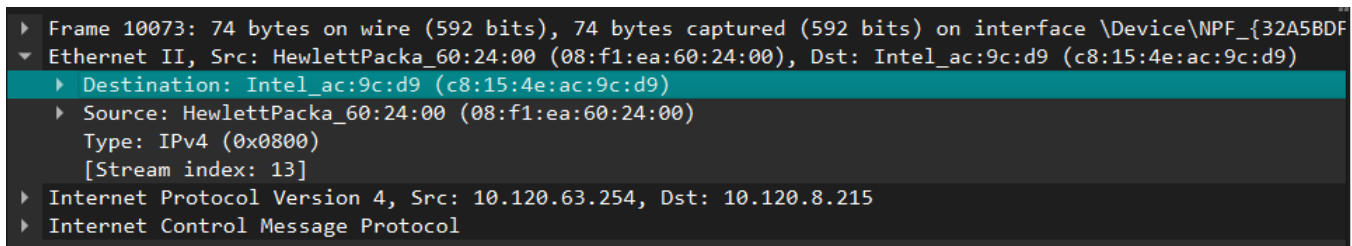
Resposta: Os últimos dois octetos são parte do campo de sequência ou dados do ICMP, sendo 68 69 (equivalente aos caracteres ASCII "hi").



- g. Clique no próximo quadro na seção superior e examine um quadro de resposta de eco. Observe que os endereços MAC de origem e de destino foram invertidos porque esse quadro foi enviado do roteador gateway padrão como uma resposta ao primeiro ping.

Que dispositivo e endereço MAC são exibidos como endereço destino?

Resposta: O dispositivo destino é o "Intel_ac:9c:d9" que possui o endereço MAC (c8:15:4e:ac:9c:d9).



Etapa 7: Capturar pacotes para um host remoto.

- Clique no ícone **Start Capture (Iniciar captura)** para iniciar uma nova captura do Wireshark. Você receberá uma janela pop-up perguntando se deseja salvar os pacotes capturados em um arquivo antes de iniciar uma nova captura. Clique em **Continue without Saving** (Continuar sem salvar).
- Em uma janela do prompt de comando, execute ping em www.cisco.com.
- Parar a captura de pacotes.
- Examinar os novos dados no painel lista de pacotes do Wireshark.

No primeiro quadro de requisição (ping) de eco, quais são os endereços MAC de origem e de destino?

Fonte:

Resposta: O endereço MAC de origem é (c8:15:4e:ac:9c:d9).

Destino:

Resposta: O endereço MAC de destino é (08:f1:ea:60:24:00).

Quais são os endereços IP origem e destino contidos no campo de dados do quadro?

Fonte:

Resposta: O endereço IP de origem é (10.120.8.215).

Destino:

Resposta: O endereço IP de destino é (2.22.64.99).

Compare esses endereços com os endereços que você recebeu na Etapa 6. O único endereço que mudou foi o endereço IP de destino. Por que o endereço IP de destino mudou e o endereço MAC de destino permaneceu o mesmo?

Resposta: O endereço IP de destino mudou para 2.22.64.99 porque o ping foi direcionado a um host remoto (www.cisco.com), localizado fora da rede local. Já o endereço MAC de destino permaneceu o mesmo (08:f1:ea:60:24:00) porque, em comunicações para redes externas, o quadro Ethernet é sempre enviado ao roteador gateway padrão (cujo MAC é fixo na rede local). O gateway é responsável por rotear o pacote para a internet, substituindo o endereço MAC de destino em saltos subsequentes. Assim, o MAC destino continua sendo o do gateway, enquanto o IP destino reflete o endereço final remoto.

Perguntas para reflexão

O Wireshark não exibe o campo Preâmbulo de um cabeçalho do quadro. O que o preâmbulo contém?

Resposta: O preâmbulo é uma sequência inicial de bytes em quadros Ethernet usada para sincronizar dispositivos antes da transmissão, contendo padrões de clock e um delimitador de início. O Wireshark não mostra o preâmbulo porque as placas de rede removem essa informação física antes de repassar os dados para análise. Como o preâmbulo opera na camada física pura, ele não é relevante para a análise de protocolos que o Wireshark realiza na camada de enlace. Essa informação técnica de sincronização é descartada antes mesmo do sistema operacional processar os pacotes. Portanto, embora crucial para a transmissão física, o preâmbulo não aparece nas capturas do Wireshark por não conter dados lógicos analisáveis.