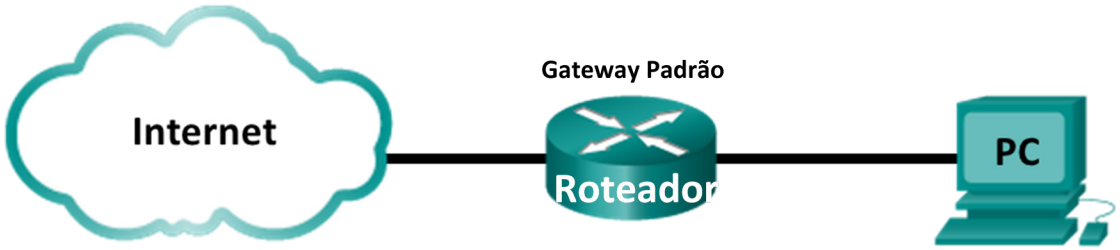
Laboratório – Usando Wireshark para Examinar Quadros Ethernet

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 7, 8 ou 10 com acesso à Internet e Wireshark instalado)

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.

Preâmbulo	Endereço Destino	Endereço Origem	Tipo de quadro	Dados	FCS
8 bytes	6 bytes	6 bytes	2 bytes	46 a 1.500 bytes	4 bytes

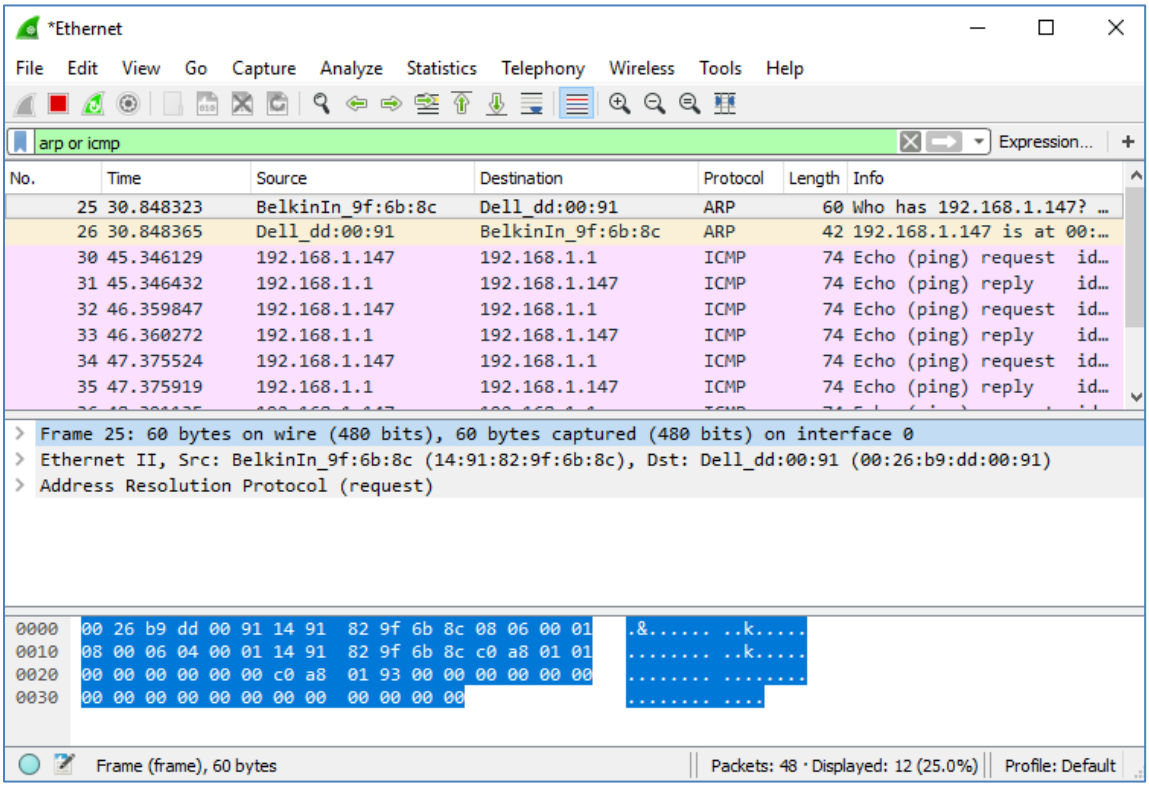
Etapa 2: Examinar a configuração de rede do PC.

O endereço IP deste host PC é 192.168.1.147, e o gateway padrão tem o endereço IP 192.168.1.1.

```
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
```


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

A captura do Wireshark a seguir mostra os pacotes gerados por um ping sendo enviados de um host PC para o gateway padrão. Um filtro foi aplicado ao Wireshark para visualizar somente os protocolos ARP e ICMP. A sessão começa com uma consulta ARP para o endereço MAC do roteador gateway, seguida de quatro requisições e respostas de ping.



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`. 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.
Endereço Origem	BelkinIn_9f:6b:8c (14:91:82:9f:6b:8c)	
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 `0x0800` Protocolo IPv4 `0x0806` Protocolo de resolução de endereços (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 computado pela máquina emissora, incluindo o endereçamento, o tipo e o campo de dados do quadro. Isso é verificado pelo receptor.

Qual é a importância do conteúdo do campo Endereço Destino?

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

Qual é o endereço MAC origem no primeiro quadro?

Qual é a ID do fornecedor (OUI) da NIC origem?

Que parte do endereço MAC é a OUI?

Qual é o número serial da NIC de origem?

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.

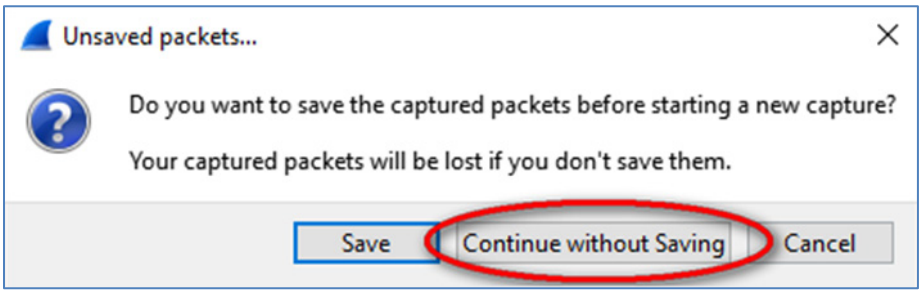
Etapa 1: Determinar o endereço IP do gateway padrão em seu PC.

Abra uma janela do prompt de comando e digite o comando ipconfig.

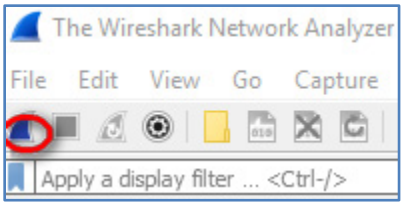
Qual é o endereço IP do gateway padrão do PC?

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

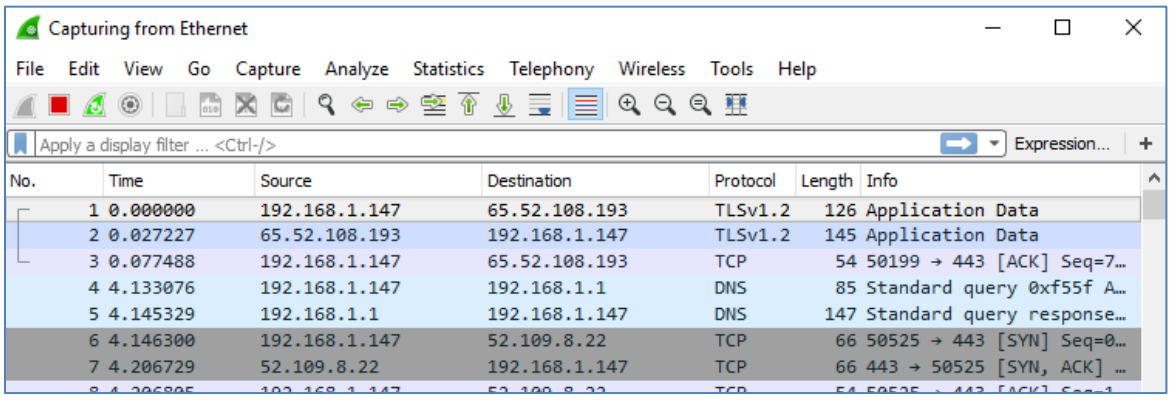
a. Feche o Wireshark. Não é necessário salvar os dados capturados.



b. Abra o Wireshark, inicie a captura de dados.



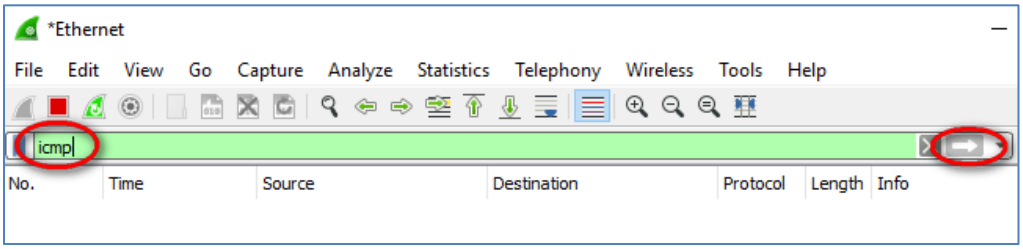
c. Observe o tráfego que aparece na janela Packet List (Lista de pacotes).



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 é exibido na tela. Por enquanto, deve ser exibido somente tráfego ICMP.

Na caixa Filter (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.

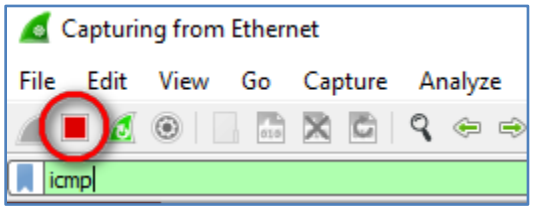


Etapa 4: Na janela do prompt de comando, fazer ping no gateway padrão do seu PC.

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

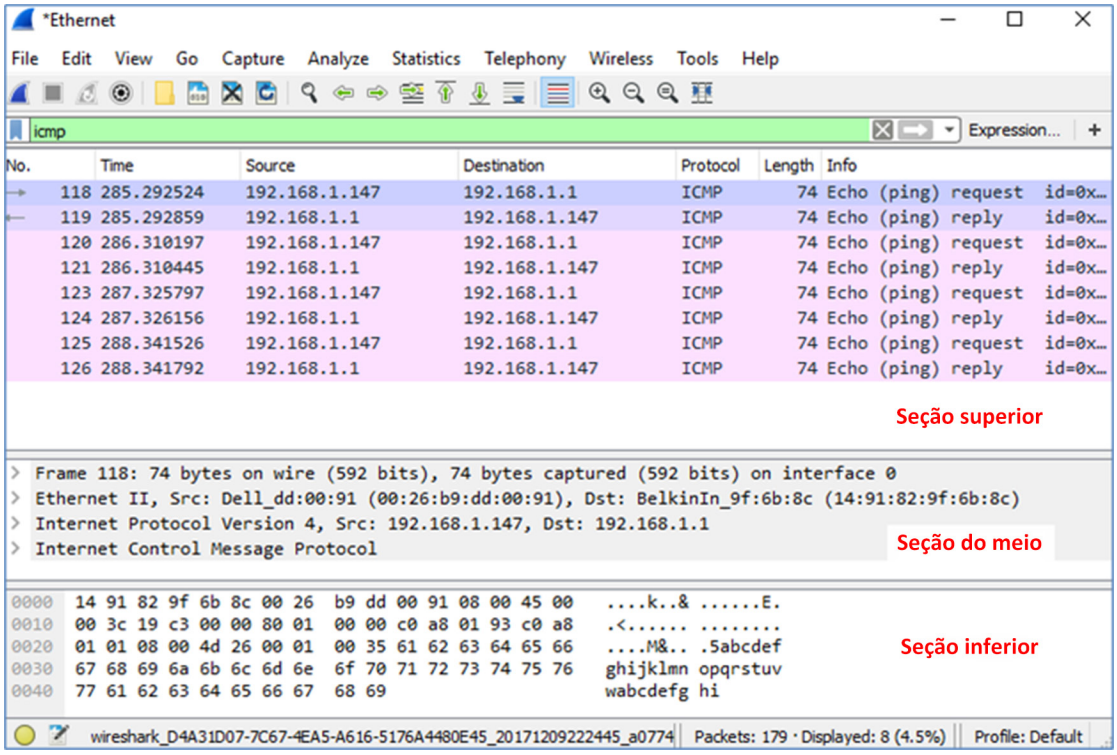
Etapa 5: Interromper a captura de tráfego na NIC.

Clique no ícone Stop Capture (Parar captura) para interromper a captura de 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 tiver selecionado a interface correta para captura de pacotes na Etapa 3, o Wireshark deverá exibir as informações ICMP no painel Packet List (Lista de pacotes), como mostrado no exemplo a seguir.



a. No painel Packet List (Lista de pacotes) [seção superior], clique no primeiro quadro listado. Você deverá ver Echo (ping) request (Requisição [ping] de eco) no cabeçalho Info (Informações). A linha será destacada em azul.

b. Examine a primeira linha no painel Packet Details (Detalhes do pacote) [seção intermediária]. Essa linha apresenta o tamanho do quadro; 74 bytes neste exemplo.

c. 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?

   Qual é o endereço MAC do gateway padrão?

d. Clique no sinal de mais (+) no início da segunda linha para obter informações adicionais sobre o quadro Ethernet II. Observe que o sinal de mais (+) muda para o sinal de menos (-).

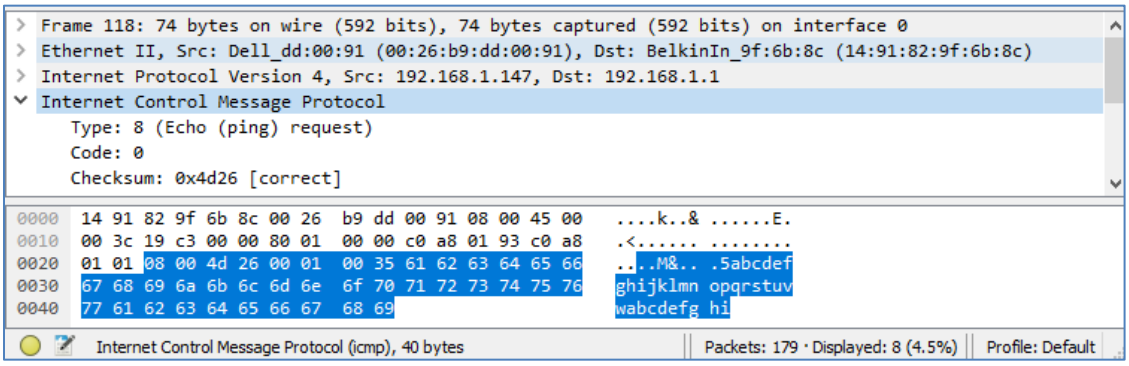
   Que tipo de quadro é exibido?

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 origem?

   Qual é o endereço IP destino?

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).



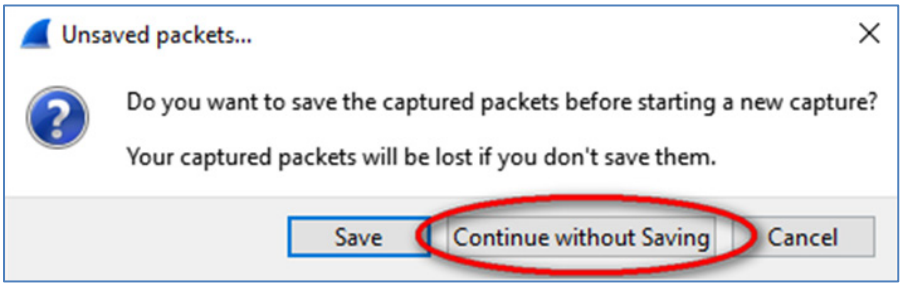
O que dizem os dois últimos octetos destacados?

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?

Etapa 7: Reiniciar a captura de pacotes no Wireshark.

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).



Etapa 8: Na janela do prompt de comando, fazer ping em www.cisco.com.

Etapa 9: Parar a captura de pacotes.

Etapa 10: Examinar os novos dados no painel packet list (lista de pacotes) do Wireshark.

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

Origem:

Destino:

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

Origem:

Destino:

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

Reflexão

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

