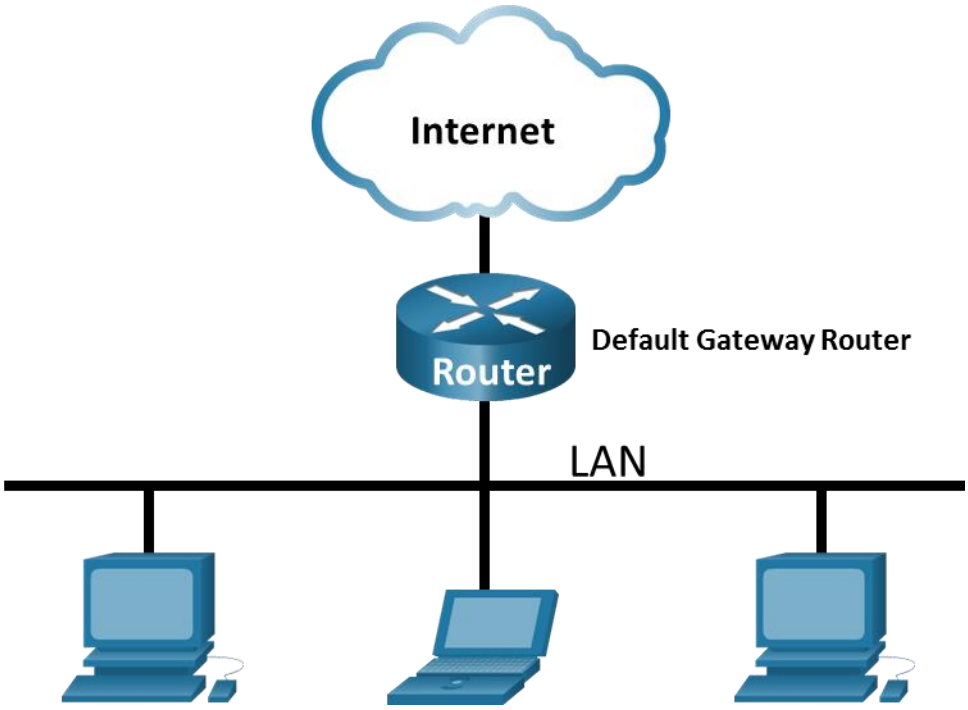
Laboratório - Use o Wireshark para visualizar o tráfego de rede

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 com acesso à Internet)
- Serão usados outros PCs em uma rede local (LAN) para responder às solicitações de ping.

Instruções

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 os 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. Em uma janela do prompt de comandos, insira **ipconfig /all**, ao endereço IP da interface do seu PC, sua descrição e seu endereço MAC (físico).

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

Configuração do IP do Windows

   Nome do host . . . . . . . . . . . . : DESKTOP-NB48BTC
   Sufixo de DNS primário. . . . . . . :
   Tipo de nó. . . . . . . . . . . . . : Híbrido
   Roteamento de IP ativado. . . . . . . . : Não
   Proxy WINS ativado. . . . . . . . : Não

Ethernet adapter Ethernet:

   Específico de Conexão Sufixo DNS. :
   Descrição . . . . . . . . . . . . . : Intel(R) 82577LM Gigabit Network Connection
   Endereço Físico. . . . . . . . . . :00-26-B9-DD-00-91
   DHCP Enabled. . . . . . . . . . . . : Não
   Autoconfiguration Enabled . . . . : Yes
   Link-local IPv6 Address . . . . . : fe80::d809:d939:110f:1b7f%20(Preferred)
   IPv4 Address. . . . . . . . . . . . : 192.168.1.147(Preferred)
   Máscara de Sub-Rede . . . . . . . . . . . : 255.255.255.0
   Gateway Padrão . . . . . . . . . . : 192.168.1.1
<output omitted>
```

b. 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.

a. Navegue para Wireshark. Clique duas vezes na interface desejada para iniciar a captura de pacotes. Verifique se a interface desejada tem tráfego.

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

   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).

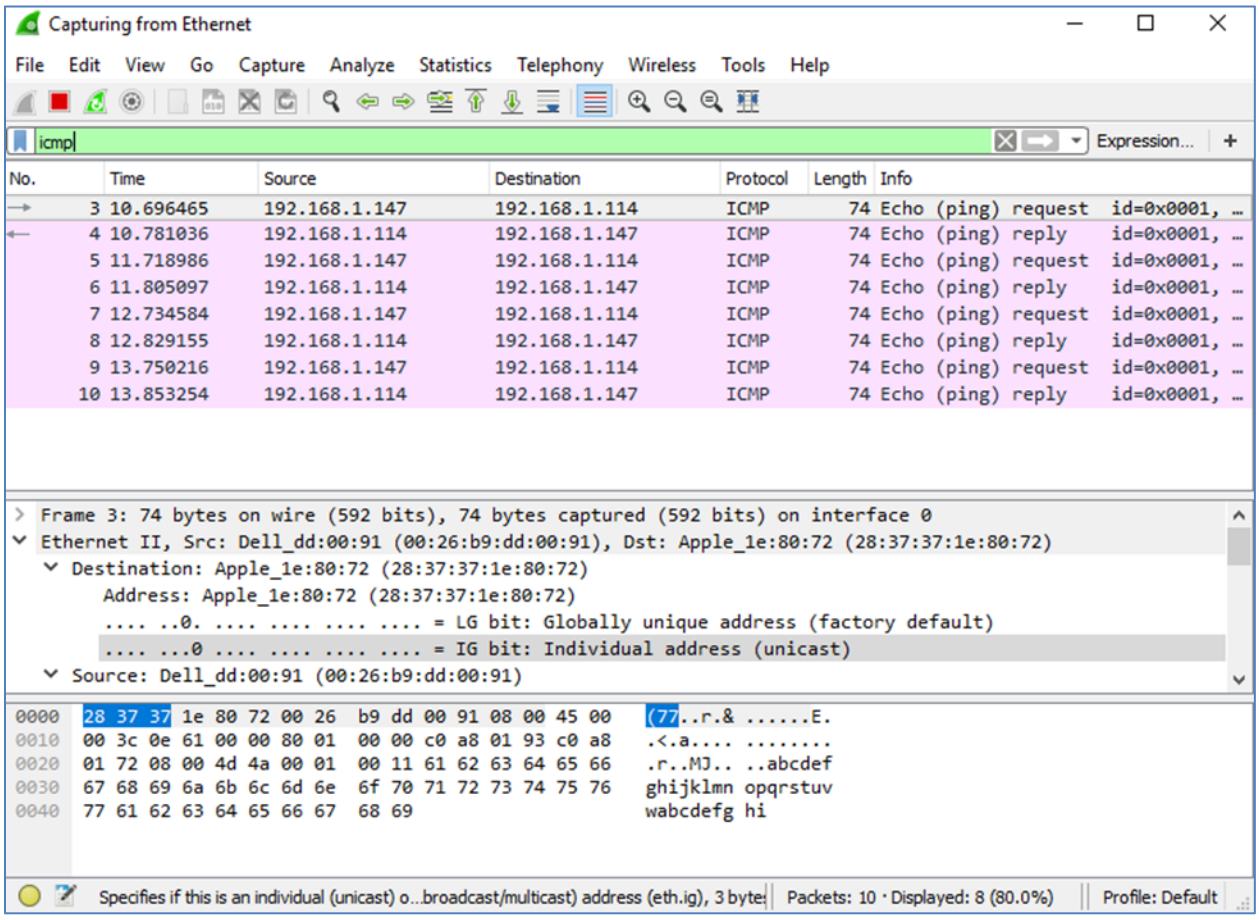
c. Este filtro faz com que todos os dados na janela superior desapareçam, mas você ainda captura o tráfego na interface. Navegue para uma janela do prompt de comando e execute ping no endereço IP que você recebeu do membro da equipe.

```
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=128
Reply from 192.168.1.114: bytes=32 time<1ms TTL=128
Reply from 192.168.1.114: bytes=32 time<1ms TTL=128
Reply from 192.168.1.114: bytes=32 time<1ms TTL=128

Estatísticas de ping para 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 firewallpara obter informações sobre como permitir o tráfego ICMP através do firewall usando o Windows.

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

Etapa 3: Examinar os dados capturados.

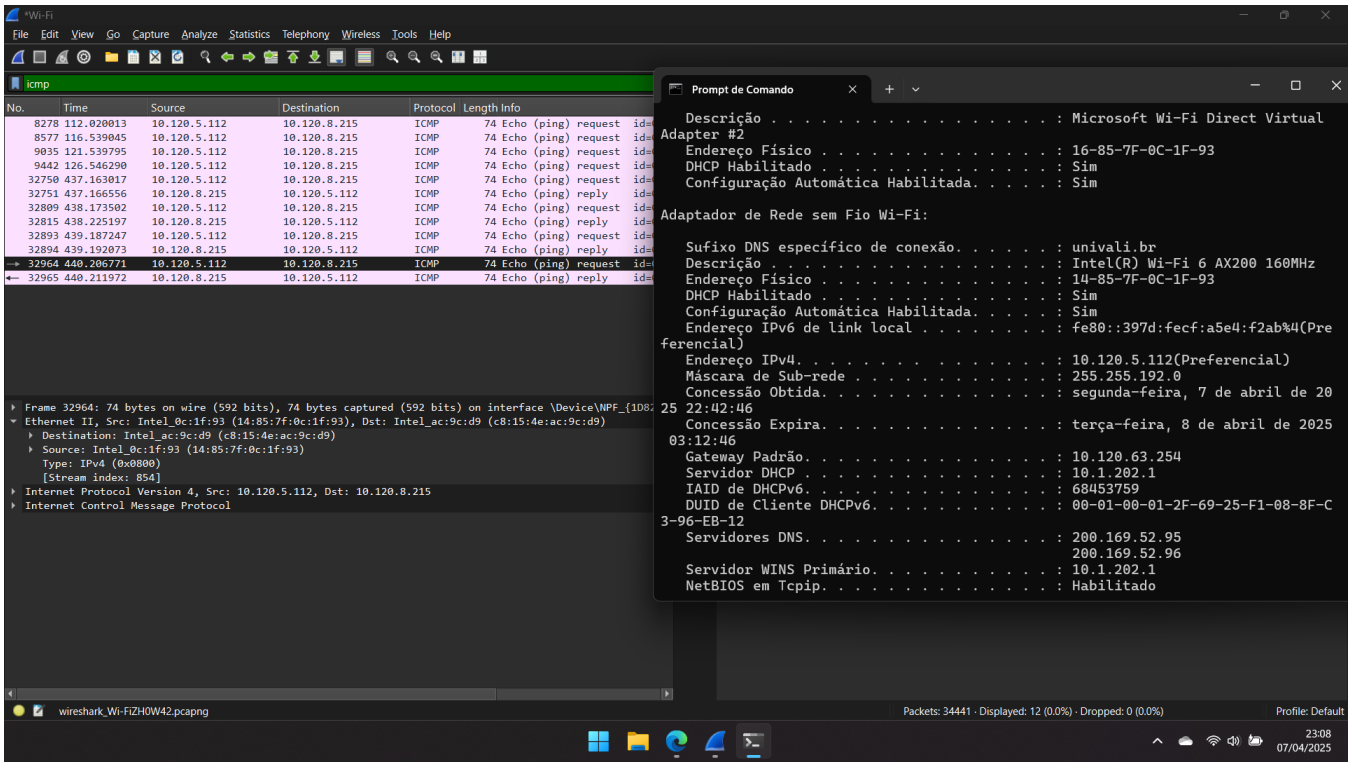
Na etapa 3, examine os dados gerados pelas solicitações ping do PC da sua equipe. Os dados do Wireshark são exibidos em três seções: 1) A seção superior exibe a lista de quadros de PDU capturada com um resumo das informações do pacote IP listadas; 2) a seção média mostra as informações de PDU para o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

Resposta: Sim corresponde, segue print:



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

Resposta: Sim corresponde, segue print:

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

   Sufixo DNS específico de conexão. . . . . : univali.br
   Descrição . . . . . . . . . . . . . . . . : Intel(R) Wireless-AC 9560 160MHz
   Endereço Físico . . . . . . . . . . . . . : C8-15-4E-AC-9C-D9
   DHCP Habilitado . . . . . . . . . . . . . : Sim
   Configuração Automática Habilitada. . . . : Sim
   Endereço IPv6 de link local . . . . . . . : fe80::aacc:6d9e:f1c4:f612%6(Preferencial)
   Endereço IPv4. . . . . . . . . . . . . . . : 10.120.8.215(Preferencial)
   Máscara de Sub-rede . . . . . . . . . . . : 255.255.192.0
   Concessão Obtida. . . . . . . . . . . . . : segunda-feira, 7 de abril de 2025 19:48:04
   Concessão Expira. . . . . . . . . . . . . : terça-feira, 8 de abril de 2025 00:18:06
   Gateway Padrão. . . . . . . . . . . . . . : 10.120.63.254
   Servidor DHCP . . . . . . . . . . . . . . : 10.1.202.1
   IAID de DHCPv6. . . . . . . . . . . . . . : 96998734
   DUID de Cliente DHCPv6. . . . . . . . . . : 00-01-00-01-2E-46-1F-96-8C-B0-E9-C1-7F-BF
   Servidores DNS. . . . . . . . . . . . . . : 200.169.52.95
                                               200.169.52.96
   Servidor WINS Primário. . . . . . . . . . : 10.1.202.1
```

```
▸ Frame 32964: 74 bytes on wire (592 bits), 74 bytes captured (592 bits) on interface \Device\NPF_{1D825C4  0000
▾ Ethernet II, Src: Intel_0c:1f:93 (14:85:7f:0c:1f:93), Dst: Intel_ac:9c:d9 (c8:15:4e:ac:9c:d9)            0010
  ▸ Destination: Intel_ac:9c:d9 (c8:15:4e:ac:9c:d9)                                                       0020
  ▸ Source: Intel_0c:1f:93 (14:85:7f:0c:1f:93)                                                            0030
    Type: IPv4 (0x0800)                                                                                   0040
    [Stream index: 854]
▸ Internet Protocol Version 4, Src: 10.120.5.112, Dst: 10.120.8.215
▸ Internet Control Message Protocol
```

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

Resposta: Quando um PC envia um ping (requisição ICMP) para outro dispositivo na mesma rede local, ele utiliza o protocolo ARP (Address Resolution Protocol) para obter o endereço MAC do destino. O PC verifica primeiro seu cache ARP; se o endereço MAC não estiver lá, ele envia um broadcast ARP perguntando "Quem tem este IP?" O dispositivo com o IP respondido envia uma resposta ARP contendo seu endereço MAC, permitindo que o PC origem complete a comunicação. O MAC é então armazenado temporariamente no cache ARP para futuras interações.

Nota: No exemplo anterior de uma solicitação ICMP capturada, os dados ICMP são encapsulados dentro de uma PDU de pacote IPv4 (cabeçalho IPv4), que é então encapsulado em uma PDU de 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, execute ping nos três URLs do site a seguir em um prompt de comando do Windows:

1) www.yahoo.com

2) www.cisco.com

3) www.google.com

Nota: Quando você executa ping nos URLs listados, observe que o DNS (Domain Name Server) converte o 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.

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.

Endereço IP para **www.yahoo.com**:

200.152.162.137

Endereço MAC para **www.yahoo.com**:

08:f1:ea:60:24:00

Endereço IP para **www.cisco.com**:

2.22.64.99

Endereço MAC para **www.cisco.com**:

08:f1:ea:60:24:00

Endereço IP para **www.google.com**:

172.217.28.132

Endereço MAC para **www.google.com**:

08:f1:ea:60:24:00

Qual é a importância dessas informações?

A importância é que o endereço IP funciona como um "endereço postal", roteando dados entre redes, enquanto o MAC age como um "CPF do dispositivo", identificando-o fisicamente na rede local. Juntos, eles garantem que a comunicação seja entregue primeiro à rede correta (via IP) e depois ao dispositivo exato (via MAC). Essa combinação é essencial para todo tráfego de internet e redes locais funcionarem com precisão.

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

Os endereços IP são únicos para cada servidor web (Yahoo, Cisco, Google), identificando os destinos na internet. Já os MACs são idênticos (08:f1:ea:60:24:00), pois representam o gateway local (roteador), mostrando que todo tráfego passa por ele antes de seguir para a internet. Isso confirma que os pacotes são roteados para fora da rede local. A análise desses dados ajuda a entender o caminho do tráfego e detectar anomalias. Se os MACs fossem diferentes, indicaria comunicação direta na rede local, o que não ocorre com sites externos.

Perguntas para reflexão

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

O Wireshark só captura o MAC real de hosts locais porque os endereços MAC são usados apenas em comunicações de rede local (Ethernet/Wi-Fi). Para hosts remotos, o tráfego passa por roteadores, que substituem o MAC original pelo seu próprio a cada salto. Como o Wireshark analisa pacotes na sua rede, ele só vê o MAC do último dispositivo local (como seu roteador), não dos servidores externos. Na internet, o roteamento depende de IPs, não de MACs, tornando o endereço físico do destino remoto inacessível. Por isso, o MAC exibido para sites externos é sempre o do gateway da sua rede.

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.

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

a. Navegue até o **Painel de Controle** e clique na opção **Sistema e Segurança** na exibição Categoria.

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

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

d. Na janela **Segurança Avançada**, clique na 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 **Personalizado** e clique 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. Verifique se **qualquer endereço IP** para os endereços IP local e remoto está selecionado. Clique em **Avançar** para continuar.

h. Selecione **Permitir a conexão**. Clique em **Avançar** para continuar.

i. Por padrão, essa regra se aplica a todos os perfis. Clique em **Avançar** para continuar.

j. Nomeie a regra com **Permitir Solicitações ICMP**. Clique em **Concluir** para continuar. Essa nova regra deve permitir que os membros da equipe recebam respostas de ping vindo do seu PC.

Parte 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 que você criou anteriormente.

b. Clique com o botão direito do mouse na regra ICMP e selecione **Desativar Regra** se desejar. Você também pode selecionar **Excluir** se quiser excluí-la permanentemente. Se você selecionar essa opção, você pode recriar a regra novamente para permitir respostas ICMP.