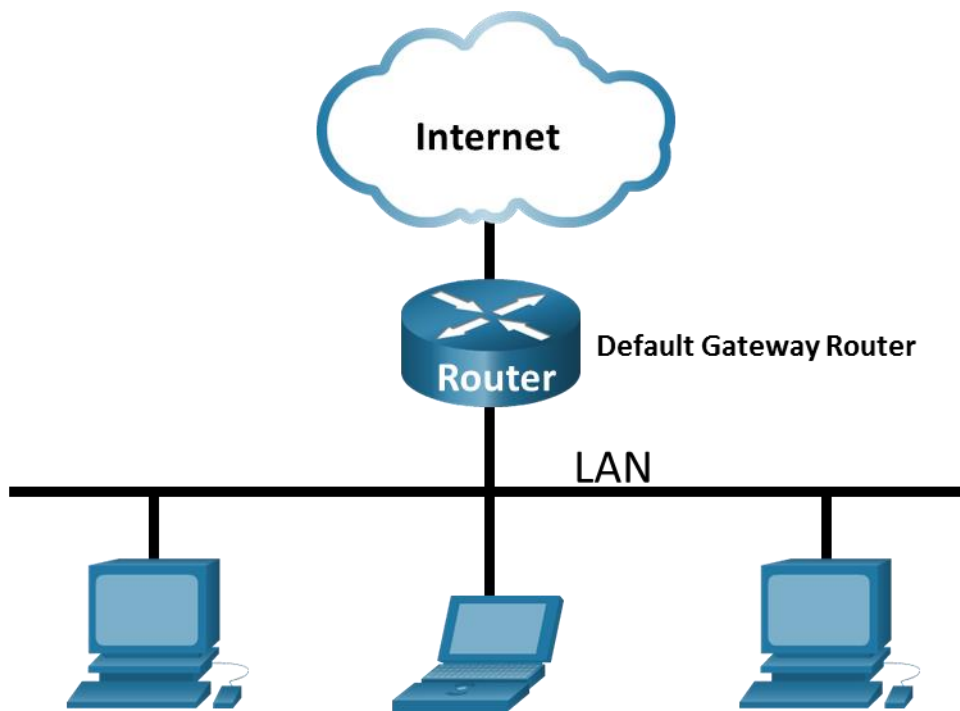


Laboratório - Use o Wireshark para visualizar o tráfego de rede

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.

- 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>

- 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.

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

Laboratório - Use o Wireshark para visualizar o tráfego de rede

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.

The screenshot shows the Wireshark network protocol analyzer interface. The top menu bar includes File, Edit, View, Go, Capture, Analyze, Statistics, Telephony, Wireless, Tools, and Help. Below the menu is a toolbar with various icons. The filter bar at the top contains the text 'icmp'. The main packet list displays several ICMP Echo (ping) request and reply packets between 192.168.1.147 and 192.168.1.114. The selected packet (No. 3) is expanded, showing details for Ethernet II and the IP header. The Ethernet II section shows the destination MAC address as Apple_1e:80:72 and the source as Dell_dd:00:91. The IP header section shows the source IP as 192.168.1.147 and the destination as 192.168.1.114. The packet bytes pane at the bottom shows the raw data in hexadecimal and ASCII format.

No.	Time	Source	Destination	Protocol	Length	Info
3	10.696465	192.168.1.147	192.168.1.114	ICMP	74	Echo (ping) request id=0x0001, ...
4	10.781036	192.168.1.114	192.168.1.147	ICMP	74	Echo (ping) reply id=0x0001, ...
5	11.718986	192.168.1.147	192.168.1.114	ICMP	74	Echo (ping) request id=0x0001, ...
6	11.805097	192.168.1.114	192.168.1.147	ICMP	74	Echo (ping) reply id=0x0001, ...
7	12.734584	192.168.1.147	192.168.1.114	ICMP	74	Echo (ping) request id=0x0001, ...
8	12.829155	192.168.1.114	192.168.1.147	ICMP	74	Echo (ping) reply id=0x0001, ...
9	13.750216	192.168.1.147	192.168.1.114	ICMP	74	Echo (ping) request id=0x0001, ...
10	13.853254	192.168.1.114	192.168.1.147	ICMP	74	Echo (ping) reply id=0x0001, ...

Frame 3: 74 bytes on wire (592 bits), 74 bytes captured (592 bits) on interface 0
Ethernet II, Src: Dell_dd:00:91 (00:26:b9:dd:00:91), Dst: Apple_1e:80:72 (28:37:37:1e:80:72)
Destination: Apple_1e:80:72 (28:37:37:1e:80:72)
Address: Apple_1e:80:72 (28:37:37:1e:80:72)
.....0..... = LG bit: Globally unique address (factory default)
.....0..... = IG bit: Individual address (unicast)
Source: Dell_dd:00:91 (00:26:b9:dd:00:91)

0000 28 37 37 1e 80 72 00 26 b9 dd 00 91 08 00 45 00 (77..r.&E.
0010 00 3c 0e 61 00 00 80 01 00 00 c0 a8 01 93 c0 a8 .<.a.... ..
0020 01 72 08 00 4d 4a 00 01 00 11 61 62 63 64 65 66 .r..M].. ..abcdef
0030 67 68 69 6a 6b 6c 6d 6e 6f 70 71 72 73 74 75 76 ghijklmn opqrstuv
0040 77 61 62 63 64 65 66 67 68 69 wabdefg hi

Specifies if this is an individual (unicast) o...broadcast/multicast address (eth.ig), 3 byte| Packets: 10 · Displayed: 8 (80.0%) | Profile: Default

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 firewall para 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?

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?

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**:

Endereço MAC para **www.yahoo.com**:

Endereço IP para **www.cisco.com**:

Endereço MAC para **www.cisco.com**:

Endereço IP para **www.google.com**:

Endereço MAC para **www.google.com**:

Qual é a importância dessas informações?

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

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?

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.

- Navegue até o **Painel de Controle** e clique na opção **Sistema e Segurança** na exibição Categoria.
- Na janela **Sistema e segurança**, clique em **Windows Defender Firewall** ou **Windows Firewall**.
- 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.