Laboratório - Uso do Wireshark para visualizar o tráfego de rede

Topologia



Objetivos

Parte 1: (Opcional) Baixar e instalar o Wireshark

Parte 2: Capturar e analisar dados locais ICMP no Wireshark

- Inicie e interrompa a captura de dados do tráfego de ping para os hosts locais.
- Localize informações sobre o endereço IP e MAC em PDUs capturadas.

Parte 3: Capturar e analisar dados remotos ICMP no Wireshark

- Inicie e interrompa a captura de dados do tráfego de ping para os hosts remotos.
- Localize informações sobre o endereço IP e MAC em PDUs capturadas.
- Explique por que os endereços MAC para hosts remotos são diferentes dos endereços MAC de hosts locais.

Histórico/cenário

O Wireshark é um software de análise de protocolo, ou aplicação de "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. Este laboratório apresenta instruções para baixar e instalar o Wireshark, embora talvez já esteja instalado. 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 7, Vista ou XP com acesso à Internet)
- Serão usados outros PCs em uma rede local (LAN) para responder às solicitações de ping.

Parte 1: (Opcional) Baixar e instalar o Wireshark.

O Wireshark tornou-se o programa de 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. Na parte 1 deste laboratório, você baixará e instalará o programa de software Wireshark em seu PC.

Observação: 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: Baixar o Wireshark.

- a. O Wireshark pode ser baixado em www.wireshark.org.
- b. Clique em Baixar o Wireshark.

WIRESHARK	Get Acquainted 👻	Get Help 🗸	Develop 🗸		Our S	ponsor	WinPcap
What's on your per	work? Downl Get Star	oad ted Now	Knowledge is	arn Power	Coogle" Curton Search E With Rive	Enhan erbed Techn	ICC ology
News And Even	ts	3	Wireshark Blog	S	Enhance Wireshark		
SHARKFEST Was Gr Thanks to all of the Sk speakers, and organi event and we're looki Sharkfest Retrosp	eat! harkfest '13 attendees, deve zers. It was once again a wo ing forward to next year. ective •	lopers, nderful	Troubleshooting the hidden dangers of TCP's Nagle algorithm and delayed acknowledgement Jan 11 By Hansang Bae Wireshark Tutorial Series. Tips and tricks used by incidear and useranc	Q. ®	Troubleshoot your Network Free 30 day trial - Save hours on network and application issue diagnoses - Monitro chaviarial and virtual	• 1	

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



Depois de fazer uma seleção, o download será iniciado. 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.
- Responda a todas as mensagens de segurança que aparecerem na tela. Se já tiver uma cópia do Wireshark em seu PC, será solicitado que você desinstale a versão anterior antes de instalar a nova versão. 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 **Next (Próximo)**.



d. Continue avançando no processo de instalação. Clique em **I agree (Eu concordo)** quando a janela do contrato de licença for exibida.

🗲 Wireshark 1.10.0 (64-bit) Setup	- • •
License Agreement	
Please review the license terms before installing Wireshark 1.10.0 (64-bit).	
Press Page Down to see the rest of the agreement.	
This text consists of three parts:	<u>^</u>
Part I: Some remarks regarding the license given in Part II: The actual license that covers Wireshark. Part III: Other applicable licenses. When in doubt: Part II/III is the legally binding part, Part I is just there to make it easier for people that are not familiar with the GPLv2.	
	-
If you accept the terms of the agreement, dick I Agree to continue. You must agreement to install Wireshark 1.10.0 (64-bit).	t accept the
Nullsoft Install System v2.46	
< Back I Agree	Cancel

e. Mantenha as configurações padrão na janela Escolher componentes e clique em Next (Próximo).

🥖 Wireshark 1.10.0 (64-bit) Setu	p	- • ×							
Choose Components									
Choose which features of Wireshark 1.10.0 (64-bit) you want to install.									
The following components are a	vailable for installation.								
Select components to install:	 ✓ Wireshark ✓ TShark ✓ Plugins / Extensions ✓ Tools ✓ User's Guide 								
Space required: 111.5MB	Description Position your mouse over a component to see description,	; its							
Nullsoft Install System v2,46 ——	< Back Next >	Cancel							

f. Escolha suas opções de atalho desejadas e clique em Next (Próximo).

🚄 Wireshark 1.10.0 (64-bit) Setup	- • •
Select Additional Tasks Which additional tasks should be done?	
Create Shortcuts	
Nullsoft Install System v2,46	Cancel

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.

Wirschark 1 10 0 /64 hit) Satur		
	رقار	
Choose Install Location Choose the folder in which to install Wireshark 1.10.0 (64-bit).		
Choose a directory in which to install Wireshark.		
Destination Folder C:\Program Files\Wireshark Browse		
Space required: 111.5MB Space available: 26.8GB Nullsoft Install System v2.46	Cancel	

- 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 Instalar será desmarcada. Se a versão instalada do WinPcap for mais antiga que a versão que acompanha o Wireshark, recomenda-se que você permita 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).
- i. Conclua o assistente de configuração do WinPcap se estiver instalando o WinPcap.

🚄 Wireshark 1.10.0 (64-bit) Setup	
Install WinPcap? WinPcap is required to capture live network data. Should WinPcap be installe	d?
Currently installed WinPcap version WinPcap 4.1.3 Install Install WinPcap 4.1.3 If selected, the currently installed WinPcap 4.1.3 will be uninstalled first	st.
What is WinPcap? Nullsoft Install System v2.46 < Back	Cancel

j. 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.

🚄 Wireshark 1.10.0 (64-bit) Setup	_	
Installation Complete Setup was completed successfully.		
Completed		
Extract: reordercap.exe Output folder: C:\Program Files\Wireshark Extract: capinfos.exe Extract: capinfos.html Output folder: C:\Program Files\Wireshark Extract: rawshark.exe Extract: rawshark.exe Extract: rawshark.html Output folder: C:\Program Files\Wireshark Extract: user-guide.chm Completed		•
Nullsoft Install System v2,46 —	< Back Next >	Cancel

k. Clique em Finish (Concluir) para encerrar o processo de instalação do Wireshark.



Parte 2: Capturar e analisar dados locais ICMP no Wireshark

Na parte 2 deste laboratório, você efetuará ping em 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: Recupere seus endereços de interface do PC.

Neste laboratório, você precisará recuperar o endereço IP do PC e o endereço físico da placa de rede (NIC), também chamado de endereço MAC.

- a. Abra uma janela de comando, digite ipconfig /all e pressione Enter.
- b. Observe o endereço IP da interface do PC e o endereço MAC (físico).

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

Etapa 2: Inicie o Wireshark e comece a capturar os dados.

- a. Em seu computador, clique no botão **Iniciar** do Windows para ver o Wireshark listado como um dos programas no menu pop-up. Clique duas vezes no **Wireshark**.
- b. Após iniciar o Wireshark, clique na Interface List (Lista de interface).

Observação: clicar no primeiro ícone de interface na linha de ícones também abre a lista de interface.

c. No Wireshark: na janela Capture Interfaces (interfaces de captura), clique na caixa de seleção ao lado da interface conectada à LAN.

📕 Wireshark: Cap	ture Interfaces			[- • •
	Description	IP	Packets	Packets/s	
	Intel(R) PRO/1000 MT Network Connection		19	0	<u>D</u> etails
	Intel(R) 82577LM Gigabit Network Connection	192.168.1.11	47	0	Details
<u>H</u> elp		<u>S</u> tart	Stop	<u>O</u> ptions	<u>C</u> lose

Observação: se várias interfaces estiverem listadas e você não tiver certeza sobre qual interface verificar, clique no botão **Details (Detalhes)** e na guia **802.3 (Ethernet)**. Verifique se o endereço MAC corresponde ao que você observou na etapa 1b. Feche a janela de Interface Details (detalhes da interface) após verificar a interface correta.

🥖 Wireshark: Interface Details	
Characteristics Statistics (802.3 (Ethernet)	802.11 (WLAN) Task Offload
Characteristics Permanent station address Current station address	00:50:56:BE:76:8C 00:50:56:BE:76:8C
Statistics	

d. Depois de verificar a interface correta, clique em Start (Iniciar) para iniciar a captura de dados.

📕 Wireshark: Cap	ture Interfaces				- • •
	Description	IP	Packets	Packets/s	
	Intel(R) PRO/1000 MT Network Connection		19	0	<u>D</u> etails
V	Intel(R) 82577LM Gigabit Network Connection	192.168.1.11	47	0	<u>D</u> etails
1					
<u>H</u> elp		Start	Stop	<u>O</u> ptions	<u>C</u> lose

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

📶 Capt	uring from Intel(R) 82577LM Gigabit Network Conne	ection: \Device\NPF_{6179E093-A447	-4EC8-81DF-5E2	22D08A6F63} [Wireshark 1.10.0 (SVN Rev 49790 from /trunk-1.10)]	- • •
<u>File</u>	dit <u>V</u> iew <u>G</u> o <u>C</u> apture <u>A</u> nalyze <u>S</u> tatistics T	elephony <u>T</u> ools <u>I</u> nternals <u>H</u> elp			
00		💩 🗛 🗸 🗣 🗐 🗐 (f	000		
	/ 🗮 🖻 🖸 🔤 🏘 🕼 - 🕻 🦿 -		~~~		
Filter:		 Expression. 	. Clear Apply	/ Save	
No.	Time Source	Destination	Protocol Len	qth Info	*
	21 2.451962000 cisco 7a:ec:84	Spanning-tree-(for-br	STP	60 Conf. Root = 32768/0/30:f7:0d:7a:ec:84 Cost = 0 Port = 0x8001	
	22 3,497376000 10,20,164,21	173, 194, 79, 125	тср	91 [TCP segment of a reassembled PDU]	
	23 3.567094000 173.194.79.125	10.20.164.21	тср	60 xmpp-client > 53588 [ACK] seg=1 Ack=38 win=1002 Len=0	
	24 4.451700000 cisco_7a:ec:84	Spanning-tree-(for-br	STP	60 Conf. Root = 32768/0/30:f7:0d:7a:ec:84 Cost = 0 Port = 0x8001	
	25 6.451326000 cisco_7a:ec:84	Spanning-tree-(for-br	STP	60 Conf. Root = 32768/0/30:f7:0d:7a:ec:84	
	26 8.451225000 cisco_7a:ec:84	Spanning-tree-(for-br	STP	60 Conf. Root = 32768/0/30:f7:0d:7a:ec:84 Cost = 0 Port = 0x8001	
	27 10.27736800(10.20.164.21	173.36.12.72	тср	55 53964 > 10846 [ACK] Seg=1 Ack=1 Win=63974 Len=1	
	28 10.35963200(173.36.12.72	10.20.164.21	тср	66 10846 > 53964 [ACK] Seg=1 Ack=2 Win=513 Len=0 SLE=1 SRE=2	
	29 10.45232500(cisco_7a:ec:84	Spanning-tree-(for-br	STP	60 Conf. Root = 32768/0/30:f7:0d:7a:ec:84 Cost = 0 Port = 0x8001	
	30 10.94920600(10.20.164.21	171.68.57.53	NBNS	92 Name query NB UNIDC3<20>	
	31 10.99746700(171.68.57.53	10.20.164.21	NBNS	98 Name query response, Requested name does not exist	
	32 10.99758500(10.20.164.21	173.37.115.191	NBNS	92 Name query NB UNIDC3<20>	
	33 11.08046600(173.37.115.191	10.20.164.21	NBNS	98 Name query response, Requested name does not exist	
	34 11.09043000(10.20.164.21	10.20.164.31	NBNS	92 Name query NB UNIDC3<20>	
	35 11.84043400(10.20.164.21	10.20.164.31	NBNS	92 Name query NB UNIDC3<20>	
	36 12.45071000(cisco_7a:ec:84	Spanning-tree-(for-br	STP	60 Conf. Root = 32768/0/30:f7:0d:7a:ec:84 Cost = 0 Port = 0x8001	
	37 12.59048100(10.20.164.21	10.20.164.31	NBNS	92 Name query NB UNIDC3<20>	
	38 13.34153600(10.20.164.21	171.68.57.53	NBNS	92 Name query NB UNIDC3<20>	=
	39 13.41142100(171.68.57.53	10.20.164.21	NBNS	98 Name query response, Requested name does not exist	
	40 13.41151700(10.20.164.21	173.37.115.191	NBNS	92 Name query NB UNIDC3<20>	
	41 13.49295400(173.37.115.191	10.20.164.21	NBNS	98 Name query response, Requested name does not exist	
	42 13.50250600(10.20.164.21	10.20.164.31	NBNS	92 Name query NB UNIDC3<20>	
	43 14.25256700(10.20.164.21	10.20.164.31	NBNS	92 Name query NB UNIDC3<20>	
	44 14.45045300(cisco_7a:ec:84	Spanning-tree-(for-br	STP	60 Conf. Root = 32768/0/30:f7:0d:7a:ec:84 Cost = 0 Port = 0x8001	
	45 14.69467200(10.20.164.21	192.168.87.9	SRVLOC	86 Attribute Request, V1 Transaction ID - 49289	· · · · · · · · · · · · · · · · · · ·
•				III	- F
I Era	me 1: 66 bytes on wire (528 bits).	66 bytes captured (528	hits) on in	nterface 0	
E Eth	ernet TT_Src: Dell 24:2a:60 (5c:26	5:0a:24:2a:60) Dst: Cis	co 7a.ec.84	(30.f7.0d.7a.ec.84)	
Tot.	ernet Protocol Version 4 Src: 10 3	20 164 21 (10 20 164 21)	Dst: 204	736 730 45 (204 236 230 45)	
Tra	nsmission Control Protocol Src Por	t: 54996 (54996) Dst P	ort: https	(443) Seq: 0 Len: 0	
		(34550) (34550) (550)	or er neeps	((1)), bell o, ten o	
0000	30 f7 0d 7a ec 84 5c 26 0a 24 2a	60 08 00 45 00 0z	& .\$*`E.		~
0010	00 34 4T /8 40 00 80 06 4a 08 0a	14 a4 15 cc ec .40x@.	. J		
0030	20 00 8a 09 00 00 02 04 04 ec 01	03 03 02 01 01			=
0040	04 02				-
			0.1.1.10		
	ntel(K) 82577EM Gigabit Network Connection: \Devic	ce/NPF_{61/9E093-A447-4EC8-81DF	Packets: 45 l	Displayed: 45 Marked: 0 Profile: Default	

e. 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 Filtro na parte superior do Wireshark e pressione Enter ou clique no botão **Apply (Aplicar)** para exibir somente as PDUs do ICMP (ping).

f. Este filtro faz com que todos os dados na janela superior desapareçam, mas você ainda estará capturando o tráfego na interface. Exiba a janela do prompt de comando que você abriu anteriormente e efetue ping no endereço IP que você recebeu de sua equipe. Observe que começa a ver novamente os dados na janela superior do Wireshark.

Capturing from Intel(R) PRO/1000 MT Network Co	nnection [Wireshark 1.1	.0.0 (SVN Rev 4979	0 from /trunk-1.10)]					
<u>File Edit View Go Capture Analyze Statist</u>	ics Telephon <u>y T</u> ools	Internals <u>H</u> elp					_	
● ● ◢ ■ ◢ ⊨ ≞ ≭ 2 ⊂	🔶 🔿 🐼 🕹		Q 🔍 🖭 🕍 🗎	1 🖪 🔆	ġ.			
Filter: icmp		 Expression 	Clear Apply					
No. Time Source	Destination	Protocol L	ength Info					
11 15.118840 192.168.1.11	192.168.1.12	ICMP	74 Echo (ping)	request	id=0x0001,	seq=21/5376,	tt]=12	
14 15.119602 192.168.1.12	192.168.1.11	ICMP	74 Echo (ping)	reply	id=0x0001,	seq=21/5376,	tt]=12	
16 16.127853 192.168.1.11	192.168.1.12	ICMP	74 Echo (ping)	request	id=0x0001,	seq=22/5632,	tt]=12	
17 16.128679 192.168.1.12	192.168.1.11	ICMP	74 Echo (ping)	reply	id=0x0001,	seq=22/5632,	tt]=12	
18 17.141897 192.168.1.11	192.168.1.12	ICMP	74 Echo (ping)	request	id=0x0001,	seq=23/5888,	tt]=12	
19 17.145943 192.168.1.12	192.168.1.11	ICMP	74 Echo (ping)	reply	id=0x0001,	seq=23/5888,	tt]=12	
21 18.140246 192.168.1.11	192.168.1.12	ICMP	74 Echo (ping)	request	1d=0x0001,	seq=24/6144,	ttl=12	
22 18.140/94 192.168.1.12	192.168.1.11	ICMP	/4 Echo (ping)	reply	1d=0x0001,	seq=24/6144,	tt [=12	
	C:\Windows\sys	stem32\cmd.exe						
#daptador de túnel isatap.localdomain: #daptador de túnel isatap.localdomain: Estado da mídia # Frame 11: 74 bytes on wire (592 bits # Endereço Físico # Ethernet II, Src: Vmware_be:76:8c (
Internet Protocol Version 4, Sic.	C:\>ping 192.	168.1.12						
0000 00 50 56 be f6 db 00 50 56 be 0010 00 3c 01 ac 00 00 80 01 b5 ac 0020 01 0c 08 00 4d 46 00 01 00 11 0030 67 68 69 6a 6b 6c 6d 6e 6f 70	Disparando 19 Resposta de 1 7 Resposta de 1 6 Resposta de 1 6 Resposta de 1 7 Festatísticas	2.168.1.12 c 92.168.1.12: 92.168.1.12: 92.168.1.12: 92.168.1.12: 92.168.1.12: do Ping para	om 32 bytes de da bytes=32 tempo=2 bytes=32 tempo=3 bytes=32 tempo=3 bytes=32 tempo=2 192_168_1_12:	ndos: 277ms TTL 37ms TTL 31ms TTL 282ms TTL	=128 =128 =128 =128			
UU4U // 61 62 63 64 65 66 67 68 69	Pacotes:	Enviados = 4 perda),	, Recebidos = 4,	Perdidos	= 0 <0% de			
Butching into 1000 with Metwork Conflections P	Hproximar um	numero redon	do de vezes em mi	lissegund	105			

Observação: se o PC de sua equipe não responde aos pings, isso pode acontecer porque o firewall do PC está bloqueando as solicitações. ConsulteAppendix A: Allowing ICMP Traffic Through a Firewall para obter informações sobre como permitir o tráfego ICMP pelo firewall usando o Windows 7.

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

Etapa 3: Examine os dados capturados.

Na etapa 3, examine os dados gerados pelas solicitações ping do PC de 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.

Capturing from Intel(R) PRO/1000 MT Network Connection [Wireshark 1.6.1 (SVN Rev 38096 from /trunk-1.6)]																	
<u>F</u> ile	<u>E</u> dit <u>V</u> iew <u>G</u> o	<u>C</u> apture	e <u>A</u> nal	yze <u>s</u>	<u>S</u> tatistic	s Tele	phony	<u>T</u> ool	s <u>I</u> ntei	rnals <u>H</u> elp							
8	1 🔍 🎱 🖮		8 ×	2	8	୍ 🔶	🏟 d	ۍ 🔇			\oplus Θ	11		i 🗹 褐	* 🖬		
Filter:	icmp								-	Expression	Clear A	pply					
No.	Time	Source				Destin	ation			Protocol L	ength Inf	0					_
	11 15.11884	0 192.1	168.1.	. 11		192.	168.1	.12		ICMP	74 EG	tho	(ping)	request	id=0x0001,	seq=21/5376	, ttl=1.
	14 15.11960	2 192.1	168.1.	.12		192.3	168.1	.11		ICMP	74 EC	:ho	(ping)	reply	id=0x0001,	seq=21/5376	, ttl=12
	16 16.12785	3 192.1	168.1.	.11		192.3	168.1	.12		ICMP	74 EC	tho	(ping)	request	id=0x0001,	seq=22/5632	, ttl=12
	17 16.12867	9 192.1	168.1.	.12		192.3	168.1	.11		ICMP	74 EC	tho	(ping)	reply	id=0x0001,	seq=22/5632	, tt]=12
	18 17.14189	7 192.1	168.1.	.11		192.3	168.1	.12		ICMP	74 EC	tho	(ping)	request	id=0x0001,	seq=23/5888	, ttl=12
	19 17.14594	3 192.1	168.1.	.12		192.3	168.1	.11		ICMP	74 EC	tho	(ping)	reply	id=0x0001,	seq=23/5888	, tt]=12
	21 18.14024	6 192.1	168.1.	. 11		192.	168.1	.12		ICMP	74 EC	tho	(ping)	request	id=0x0001,	seq=24/6144	, tt]=12
	22 18.14079	4 192.1	168.1.	.12		192.3	168.1	.11		ICMP	74 EC	tho	(ping)	reply	id=0x0001,	seq=24/6144	, ttl=12
 Fra Etł 	B Frame 11: 74 bytes on wire (592 bits), 74 bytes captured (592 bits) B Ethernet II, Src: IntelCor_34:92:1c (58:94:6b:34:92:1c), Dst: Intel_0f:91:48 (00:11:11:0f:91:48)																
TITE TITE	ernet Cont	rol Mes	sane	Prote		192.1	00.1.	II (.	192.10	50.1.11),	DSU. 1	.92.	100.1.1	12 (192.	100.1.12)		
		or nes	Juge												Mi	ddle Section	
0000 0010 0020 0030 0040	00 50 56 0 00 3c 01 3 01 0c 08 0 67 68 69 0 77 61 62 0	e f6 dl ac 00 00 00 4d 40 5a 6b 60 53 64 6	b 00 5 0 80 0 6 00 0 c 6d 6 5 66 6	50 5 01 b 01 0 5e 6 57 6	56 be 55 ad 00 15 56 70 58 69	76 80 c0 a8 61 62 71 72	2 08 0 3 01 0 2 63 6 2 73 7	00 45 0b c0 54 65 74 75	00 a8 66 76	.PV . <mf. ghijklm wabcdef</mf. 	P V.v abc n opqrs g hi	.E. def tuv			Во	ttom Seciton	* <u> </u>
Integration	el(R) PRO/1000 N	IT Networ	k Conne	ection:	Pa	ckets: 19	99 Displa	ayed: 8	Markee	: 0					Profile: Def	ault	

a. Clique nos primeiros quadros de PDU de solicitação ICMP na seção da parte superior do Wireshark. Observe que a coluna Origem tem o endereço IP do PC, e a Destino contém o endereço IP do PC do colega em que você efetuou ping.

🖌 Intel(R) PRO/1000 MT Network Connection [Wireshark 1.10.0 (SVN Rev 49790 from /trunk-1.10)]										
<u>F</u> ile	<u>E</u> dit <u>V</u> iew <u>G</u> o	<u>C</u> apture <u>A</u> nalyze <u>S</u> tat	tistics Telephon <u>y T</u> ools	Internals <u>H</u> elp						
0	۵ 🔳 🔬	🖹 👪 🗶 🤇	2, 🗢 🛸 😜 ዥ 👱		ର୍ ପ୍ 🖭	🎬 🗹 🐔 %				
Filte	r: icmp			Expression	Clear Apply					
No.	Time	Source	Destination	Protocol L	ength Info					
	5 2.801784	192.168.1.11	192.168.1.12	ICMP	74 Echo	(ping) request	id=0x0001,	seq=25/6400,	tt]=12	
	8 2.802679	192.168.1.12	192.168.1.11	ICMP	74 Echo	(ping) reply	id=0x0001,	seq=25/6400,	tt]=12	
	10 3.816895	192.168.1.11	192.168.1.12	ICMP	74 Echo	(ping) request	id=0x0001,	seq=26/6656,	tt]=12	
	11 3.817540	192.168.1.12	192.168.1.11	ICMP	74 Echo	(ping) reply	id=0x0001,	seq=26/6656,	tt]=12	
	13 4.831343	192.168.1.11	1 92.168.1.12	ICMP	74 Echo	(ping request	i d=0x0001,	seq=27/6912,	tt]=12	
	14 4.832006	192.168.1.12	192.168.1.11	ICMP	74 Echo	(ping) reply	id=0x0001,	seq=27/6912,	tt]=12	
	15 5.844858	192.168.1.11	192.168.1.12	ICMP	74 Echo	(ping) request	id=0x0001,	seq=28/7168,	tt]=12	
	16 5.845488	192.168.1.12	192.168.1.11	ICMP	74 Echo	(ping) reply	id=0x0001,	seg=28/7168,	tt]=12	

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 origem e destino.

📕 In	Intel(R) PRO/1000 MT Network Connection [Wireshark 1.10.0 (SVN Rev 49790 from /trunk-1.10)]										
<u>F</u> ile	<u>E</u> dit <u>V</u> iew <u>G</u>	o <u>C</u> apture <u>A</u> nalyze <u>S</u>	tatistics Telephony <u>T</u> ools	Internals <u>H</u> elp							
0	، 🔳 🌢	🛛 🖻 👪 🗶 🔁	् 🗢 🛸 😜 ዥ 🛂		Q Q 🖻 🎽 🖬 畅 💥 💢						
Filte	r: icmp			Expression	Clear Apply						
No.	Time	Source	Destination	Protocol L	ength Info						
	5 2.801784	192.168.1.11	192.168.1.12	ICMP	74 Echo (ping) request id=(0x0001, seq=25/6400, ttl=12					
	8 2.80267	9 192.168.1.12	192.168.1.11	ICMP	74 Echo (ping) reply id=(0x0001, seq=25/6400, ttl=12					
	10 3.81689	5 192.168.1.11	192.168.1.12	ICMP	74 Echo (ping) request id=(0x0001, seq=26/6656, ttl=12					
	11 3.81754) 192.168.1.12	192.168.1.11	ICMP	74 Echo (ping) reply id=(0x0001, seq=26/6656, ttl=12					
	13 4.83134	3 192.168.1.11	192.168.1.12	ICMP	74 Echo (ping) request id=(0x0001, seq=27/6912, ttl=12					
	14 4.83200	5 192.168.1.12	192.168.1.11	ICMP	74 Echo (ping) reply id=(0x0001, seq=27/6912, ttl=12					
	15 5.84485	3 192.168.1.11	192.168.1.12	ICMP	74 Echo (ping) request id=(0x0001, seq=28/7168, ttl=12					
	16 5.84548	3 192.168.1.12	192.168.1.11	ICMP	74 Echo (ping) reply id=(0x0001, seq=28/7168, ttl=12					
E E	came 13: 74	bytes on wire (59	92 hits), 74 bytes ca	optured (592	hits)						
O E	thernet II.	Src: IntelCor 34:	92:1c (58:94:6h:34:9	2:1c). Dst:	Intel 0f:91:48 (00:11:11:0f:91	:48)					
	Destination	n: Intel_0f:91:48	(00:11:11:0f:91:48)								
+	Source: Int	elcor_34:92:1c (5	58:94:6b:34:92:1c))							
	Type: IP (()x0800)									
÷ I	nternet Prof	cocol Version 4, 5	Src: 192.168.1.11 (19	2.168.1.11),	Dst: 192.168.1.12 (192.168.1.	12)					
÷ I	nternet Conf	rol Message Proto	col								
		-9									

O endereço MAC origem corresponde à interface do PC?

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

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

Observação: no exemplo anterior de uma solicitação ICMP capturada, os dados do ICMP são encapsulados dentro da PDU do pacote IPv4 (cabeçalho IPv4) que é, então, encapsulada em uma PDU do quadro Ethernet II (cabeçalho Ethernet II) para transmissão na LAN.

Parte 3: Capturar e analisar dados ICMP remotos no Wireshark

Na parte 3, você efetuará ping nos 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 2.

Etapa 1: Inicie a captura de dados na interface.

a. Clique no ícone Interface List (Lista de interface) para exibir novamente as interfaces do PC na lista.

b. Verifique se a caixa de seleção ao lado da interface da LAN está marcada e clique em Start (Iniciar).

🥖 Wireshark: Cap	ture Interfaces				- • •
	Description	IP	Packets	Packets/s	
	Intel(R) PRO/1000 MT Network Connection		19	0	<u>D</u> etails
	Intel(R) 82577LM Gigabit Network Connection	192.168.1.11	47	0	<u>D</u> etails
1					
Help		Start	Stop	<u>O</u> ptions	<u>C</u> lose
		\sim			

c. Uma janela solicitará que salve os dados capturados anteriormente antes de iniciar outra captura. Não é necessário salvar esses dados. Clique em **Continue without Saving (Continuar sem salvar)**.

	×
7	Do you want to save the captured packets before starting a new capture?
	Your captured packets will be lost if you don't save them.
	Save <u>C</u> ancel (Continue <u>w</u> ithout Saving)

- d. Com a captura ativa, efetue ping nos três URLs de sites a seguir:
 - 1) www.yahoo.com
 - 2) www.cisco.com
 - 3) www.google.com

```
C:Windows/system32/cmd.exe
C:\>ping www.yahoo.com
Disparando ds=eu-fp3.wal.b.yahoo.com [87.248.112.1811 com 32 bytes de dados:
Resposta de 87.248.112.181: bytes=32 tempo=381ns TTL=128
Resposta de 87.248.112.181: bytes=32 tempo=394ns TL=128
Resposta de 87.248.112.181: bytes=32 tempo=397ns TL=128
Estatísticas do Ping para 87.248.112.181:
Pacotes: Enviados = 4, Recebidos = 4, Perdidos = 0 (0% de
perda),
Aproximar um número redondo de vezes em milissegundos:
Minimo = 357ns, Máximo = 394ns, TL=128
Resposta de 2.21.96.170: bytes=32 tempo=397ns TTL=128
Resposta de 2.21.96.170: bytes=32 tempo=395ns TTL=128
Resposta de 173.194.127.114: bytes=32 tempo=53ns TTL=128
Resposta de 173.194.1
```

Observação: quando você efetuar ping nos URLs listados, observe que o Servidor de Nome de Domínio (DNS) converte o URL para um endereço IP. Observe o endereço IP recebido para cada URL.

e. É possível parar a captura de dados clicando no ícone Stop Capture (Parar a captura).

🙇 Ca	Capturing from Intel(R) PRO/1000 MT Network Connection										
<u>F</u> ile	<u>E</u> dit	<u>V</u> iew	<u>G</u> o	Capt	ure	<u>A</u> nal	yze	<u>S</u> f	tatist	ics	Telep
0	•		1			×	2		Q	4	*
Filter	Filter: icmp										
No.		Time		Sour	ce					De	estinat
	22	16.975	5362	192	.16	8.1.	11			1	92.1:

Etapa 2: Examinar e analisar os dados dos hosts remotos.

- a. Analise os dados capturados no Wireshark, examine os endereços IP e MAC dos três locais em que você efetuou ping. Liste os endereços IP e MAC destino para todos os três locais no espaço fornecido.
 - 1° Local:
 IP: ______
 MAC: ___: ___: ____

 2° Local:
 IP: ______
 MAC: ___: ___: ____

 0° Local:
 IP: ______
 MAC: _______
 - 3[°] Local: IP: _____. ____. ____ MAC: ____: ___:___:___:___:____:

- b. Qual é a importância dessas informações?
- c. Como essas informações diferem das informações do ping local que você recebeu na parte 2?

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 solicitações de ping. Também descreve como desativar a nova regra ICMP depois que você tiver concluído o laboratório.

Etapa 1: Crie uma regra de entrada nova permitindo o tráfego ICMP pelo firewall.

a. No Painel de controle, clique na opção Sistema e Segurança.

b. Na janela Sistema e Segurança, clique em Firewall do Windows.

c. No painel esquerdo da janela de firewall do Windows, clique em Configurações avançadas.

d. Na janela Segurança avançada, selecione a opção **Regras de Entrada** na barra lateral esquerda e clique em **Nova regra...** na barra lateral direita.

Pirewall do Windows com Segura	inça Avançada					- • •
Arquivo Ação Exibir Ajuda						
🗢 🄿 🖄 🖬 🗟 🚺						
Firewall do Windows com Segu	Regras de Entrada			Ações		
Regras de Entrada	Nome	Grupo	Perfil	Habilitado	Ac ^	Regras de Entrada 🔺
Regras de Seguranca de Col	🔇 Programa de transferência de arquivos		Particular	Sim	Pe	🗽 Nova Regra
Monitoramento	O Programa de transferência de arquivos		Particular	Sim	Pe	Filtrar por Perfil
· ••••••	🌑 Área de Trabalho Remota (TCP-Entrada)	Área de Trabalho Remota	Tudo	Não	P∈≡	Tilter and Tata
	🕑 Assistência Remota (DCOM-In)	Assistência Remota	Domínio	Sim	Pe	Filtrar por Esta
	🕑 Assistência Remota (PNRP-Entrada)	Assistência Remota	Domínio, Particular	Sim	Pe	🛛 🍸 🛛 Filtrar por Gru 🕨
	Massistência Remota (PNRP-Entrada)	Assistência Remota	Público	Não	Pe	Exibir 🕨
	🔇 Assistência Remota (RA Server UDP-Entr	Assistência Remota	Domínio	Sim	Pe	Atualizar
	🕑 Assistência Remota (SSDP TCP-Entrada)	Assistência Remota	Domínio, Particular	Sim	Pe	Atualizar
	🕑 Assistência Remota (SSDP UDP-Entrada)	Assistência Remota	Domínio, Particular	Sim	Pe	📑 Exportar Lista
	🔇 Assistência Remota (TCP-Entrada)	Assistência Remota	Domínio, Particular	Sim	Pe	🛛 🛛 🖓 Ajuda
	Assistância Remota (TCD-Entrada)	Assistância Remota	Dúblico	Não	De	1

e. Isso inicia o assistente Nova regra de entrada. Na tela Tipo de regra, clique no botão de opção **Personalizar** e em **Avançar**.

💣 Assistente para Nova Reg	ra de Entrada 🗾			
Tipo de regra				
Selecionar o tipo de regra de fin	ewall a ser criada.			
Etapas:				
Tipo de regra	Que tipo de regra você deseja criar?			
Programa				
Protocolo e Portas				
Escopo	Regra que controla conexões para um programa.			
Ação	Porta			
Perfil	Regra que controla conexões para uma porta TCP ou UDP.			
Nome	Predefinida:			
	Área de Trabalho Remota 👻			
	Regra que controla conexões para uma experiência do Windows.			
	Personalizado			
	Regra personalizada.			
	Saiba mais sobre tipos de regra			
	\frown			
	< Voltar Avançar > Cancelar			

f. No painel esquerdo, clique na opção **Protocolo e Portas** e, usando o menu suspenso Tipo de protocolo, selecione **ICMPv4** e clique em **Avançar**.

💣 Assistente para Nova Regra	de Entrada		×
Protocolo e Portas			
Especifique os protocolos e as po	rtas a que a regra se aplica.		
Etapas:			
 Tipo de regra 	A que portas e protocolo	s esta regra se aplica?	
Programa			
Protocolo e Portas	Tipo de protocolo:	Qualquer	
Escopo	Número do protocolo:	Qualquer Personalizado	
 Ação D-41 	• ••••		
Perri Nome	Porta local:	IGMP TCP	
• Nome		UDP IPv6	
	Porta remota:	IPv6-Route	
		GRE	
		IPv6-NoNbt	
	Configurações ICMP:	VRRP	
		L2TP	
	Saiba mais sobre protoc	olos e portas	

g. No painel esquerdo, clique na opção **Nome** e, no campo Nome, digite **Permitir solicitações do ICMP**. Clique em **Concluir**.

🔗 Assistente para Nova Reg	ra de Entrada	×
Nome		
Especificar o nome e a descriçã	io desta regra.	
Etapas:		
Tipo de regra		
Programa		
Protocolo e Portas	Nama	
Escopo	Allow ICMP Requests	
 Ação Barfil 		
Nome	Descrição (opcionar).	
I Nome		
	< Voltar Concluir Cancela	ar

Essa nova regra deve permitir que os membros da equipe recebam respostas de ping no PC.

Etapa 2: Desativar ou excluir a nova regra do ICMP.

Após o laboratório ser concluído, você talvez 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, no painel esquerdo, clique em **Regras de Entrada** e localize a regra que você criou na etapa 1.

Pirewall do Windows com Segur	🔐 Firewall do Windows com Segurança Avançada									
Arquivo Ação Exibir Ajuda										
🗢 🔿 🖄 🖬 🗟 🚺										
Firewall do Windows com Segu	Regras de Entrada						Ações			
Regras de Entrada	Nome	Grupo	Perfil	Habilitado	Ação	^	Regras de Ent 🔺			
Regras de Segurança de Co	Allow ICMP Requests		Tudo	Sim	Permitir		🐹 Nova Re			
Monitoramento	Programa de transferência de arquivos		Particular	Sim	Permitir		Filtrar no			
	Programa de transferência de arquivos		Particular	Sim	Permitir	Ξ				
	🌑 Área de Trabalho Remota (TCP-Entrada)	Área de Trabalho Remota	Tudo	Não	Permitir					
	🕑 Assistência Remota (DCOM-In)	Assistência Remota	Domínio	Sim	Permitir		🍸 Filtrar po 🕨			
	🕑 Assistência Remota (PNRP-Entrada)	Assistência Remota	Domínio, Particular	Sim	Permitir	_	Exibir 🕨			
	🔘 Assistência Remota (PNRP-Entrada)	Assistência Remota	Público	Não	Permitir		Atualizar			
	🐼 Assistência Remota (RA Server UDP-Entr	Assistência Remota	Domínio	Sim	Permitir		G Atualizar			
	🔇 Assistência Remota (SSDP TCP-Entrada)	Assistência Remota	Domínio, Particular	Sim	Permitir		📑 Exportar			
	🐼 Assistência Remota (SSDP UDP-Entrada)	Assistência Remota	Domínio, Particular	Sim	Permitir		? Ajuda			
	🔇 Assistência Remota (TCP-Entrada)	Assistência Remota	Domínio, Particular	Sim	Permitir					
	Assistência Remota (TCP-Entrada)	Assistência Remota	Público	Não	Permitir		Allow ICMP R 🔺			
	🔘 Base da Colaboração Ponto a Ponto do	Base da Colaboração Po	Tudo	Não	Permitir		Desabilit			
	🔘 Base da Colaboração Ponto a Ponto do	Base da Colaboração Po	Tudo	Não	Permitir		A Recortar			
	🔘 Base da Colaboração Ponto a Ponto do	Base da Colaboração Po	Tudo	Não	Permitir		Do Contro			
	🜑 Base da Colaboração Ponto a Ponto do	Base da Colaboração Po	Tudo	Não	Permitir		eg copiar			
	Descoberta no Mesmo Nível do BranchC	BranchCache - Descober	Tudo	Não	Permitir		💢 Excluir			
		Deserved Deserved	T	N12 -	Denne late		E n n			

b. Para desativar a regra, clique na opção **Desativar Regra**. Ao escolher essa opção, você a verá mudar para **Ativar Regra**. Você pode alternar entre Desativar Regra e Ativar Regra; o status da regra também é exibido na coluna Ativado na lista de Regras de entrada.

Firewall do Windows com Segura	ança Avançada						
Arquivo Ação Exibir Ajuda							
🗢 🧼 🖄 🖬 😖 🚺 🗊							
🔗 Firewall do Windows com Segu	Regras de Entrada	A	Ações				
Regras de Entrada	Nome	Grupo	Perfil	Habilitado	Ação	F	legras de Entrada 🛛 🔺
Regras de Seguranca de Col	Allow ICMP Requests	Tudo		Sim	Permitir		🗸 Nova Regra
Monitoramento	🕐 Programa de transferência de arquivos		Particular	Sim	Permitir		Filtrar por Perfil
	🔇 Programa de transferência de arquivos		Particular	Sim	Permitir E		Tilter of Catalan
	🔘 Área de Trabalho Remota (TCP-Entrada)	Área de Trabalho Re	Tudo	Não	Permitir	11	r Filtrar por Estado 🖡
	🕑 Assistência Remota (DCOM-In)	Assistência Remota	Domínio	Sim	Permitir	1	🐔 Filtrar por Grupo 🕨
	🔇 Assistência Remota (PNRP-Entrada)	Assistência Remota	Domínio, Particular	Sim	Permitir		Exibir 🕨
	🔘 Assistência Remota (PNRP-Entrada)	Assistência Remota	Público	Não	Permitir		Atualizar
	🕢 Assistência Remota (RA Server UDP-Entr	Assistência Remota	Domínio	Sim	Permitir		
	🕑 Assistência Remota (SSDP TCP-Entrada)	Assistência Remota	Domínio, Particular	Sim	Permitir		🛓 Exportar Lista
	🕢 Assistência Remota (SSDP UDP-Entrada)	Assistência Remota	Domínio, Particular	Sim	Permitir		Ajuda
	🔇 Assistência Remota (TCP-Entrada)	Assistência Remota	Domínio, Particular	Sim	Permitir		
	Assistência Remota (TCP-Entrada)	Assistência Remota	Público	Não	Permitir		Allow ICMP Requests
	🌑 Base da Colaboração Ponto a Ponto do	Base da Colaboração	Tudo	Não	Permitir		👂 Desabilitar Regra 🔵
	🔘 Base da Colaboração Ponto a Ponto do	Base da Colaboração	Tudo	Não	Permitir		Recortar
	🌑 Base da Colaboração Ponto a Ponto do	Base da Colaboração	Tudo	Não	Permitir		· Coning
	🔘 Base da Colaboração Ponto a Ponto do	Base da Colaboração	Tudo	Não	Permitir		
	Descoberta no Mesmo Nível do BranchC	BranchCache - Desc	Tudo	Não	Permitir		K Excluir

c. Para excluir permanentemente a regra do ICMP, clique em **Excluir**. Se você selecionar essa opção, você pode recriar a regra novamente para permitir respostas ICMP.

Dominio, Particular	SIM	Permitir	5	Ajuda
Domínio, Particular	Sim	Permitir		
Público	Não	Permitir	Allo	w ICMP Requests 🔺
Tudo	Não	Permitir	۲	Desabilitar Regra
Tudo	Não	Permitir	X	Recortar
Tudo	Não	Permitir	Bh.	Conjar
Tudo	Não	Permitir 🦯		copion
Tudo	Não	Permitir 🗸	×	Excluir
Tudo	Não	Dermitir	r=1	Dropriodados