Lab - Using Wireshark to View Network Traffic

Topology



Objectives

Part 1: (Optional) Download and Install Wireshark

Part 2: Capture and Analyze Local ICMP Data in Wireshark

- Start and stop data capture of ping traffic to local hosts.
- Locate the IP and MAC address information in captured PDUs.

Part 3: Capture and Analyze Remote ICMP Data in Wireshark

- Start and stop data capture of ping traffic to remote hosts.
- Locate the IP and MAC address information in captured PDUs.
- Explain why MAC addresses for remote hosts are different than the MAC addresses of local hosts.

Background / Scenario

Wireshark is a software protocol analyzer, or "packet sniffer" application, used for network troubleshooting, analysis, software and protocol development, and education. As data streams travel back and forth over the network, the sniffer "captures" each protocol data unit (PDU) and can decode and analyze its content according to the appropriate RFC or other specifications.

Wireshark is a useful tool for anyone working with networks and can be used with most labs in the CCNA courses for data analysis and troubleshooting. This lab provides instructions for downloading and installing Wireshark, although it may already be installed. In this lab, you will use Wireshark to capture ICMP data packet IP addresses and Ethernet frame MAC addresses.

Required Resources

- 1 PC (Windows 7, Vista, or XP with Internet access)
- Additional PC(s) on a local-area network (LAN) will be used to reply to ping requests.

Part 1: (Optional) Download and Install Wireshark

Wireshark has become the industry standard packet-sniffer program used by network engineers. This open source software is available for many different operating systems, including Windows, Mac, and Linux. In Part 1 of this lab, you will download and install the Wireshark software program on your PC.

Note: If Wireshark is already installed on your PC, you can skip Part 1 and go directly to Part 2. If Wireshark is not installed on your PC, check with your instructor about your academy's software download policy.

Step 1: Download Wireshark.

- a. Wireshark can be downloaded from <u>www.wireshark.org</u>.
- b. Click Download Wireshark.



c. Choose the software version you need based on your PC's architecture and operating system. For instance, if you have a 64-bit PC running Windows, choose **Windows Installer (64-bit)**.



After making a selection, the download should start. The location of the downloaded file depends on the browser and operating system that you use. For Windows users, the default location is the **Downloads** folder.

Step 2: Install Wireshark.

- a. The downloaded file is named **Wireshark-win64-x.x.x.exe**, where **x** represents the version number. Double-click the file to start the installation process.
- Respond to any security messages that may display on your screen. If you already have a copy of Wireshark on your PC, you will be prompted to uninstall the old version before installing the new version. It is recommended that you remove the old version of Wireshark prior to installing another version. Click Yes to uninstall the previous version of Wireshark.



c. If this is the first time to install Wireshark, or after you have completed the uninstall process, you will navigate to the Wireshark Setup wizard. Click **Next**.



d. Continue advancing through the installation process. Click **I Agree** when the License Agreement window displays.

lease review the license terms	Defore installing wireshark 1.8.3 (04-bit	ŋ.
Press Page Down to see the res	t of the agreement.	
This text consists of three parts		•
Part I: Some remarks regarding Part II: The actual license that (Part III: Other applicable license	the license given in covers Wireshark. es.	
When in doubt: Part II/III is the there to make it easier for peop	legally binding part, Part I is just le that are not familiar with the GPLv2.	
		-
f you accept the terms of the a greement to install Wireshark 1	greement, click I Agree to continue. Yo .8.3 (64-bit).	u must accept the

e. Keep the default settings on the Choose Components window and click Next.

🝊 Wireshark 1.8.3 (64-bit) Setu	p	
Choose Components Choose which features of Wire	shark 1.8.3 (64-bit) you want to install.	
The following components are a	available for installation.	
Select components to irstall:	Wireshark Wireshark TShark ✓ TShark ✓ Plugins / Extensions ✓ Tools ✓ Tools ✓ User's Guide	
Space required: 102.4NB	Description Position your mouse over a component to see its description.	
Nullsoft Install System v2.46		
	< Back Next >	Cancel

f. Choose your desired shortcut options and click Next.

Wireshark 1.8.3 (64-bit) Setup	
Select Additional Tasks Which additional tasks should be done?	
Create Shortcuts Create Shortcuts Start Menu Item Desktop Icon Quick Launch Icon	
File Extensions File Extensions Cap, enc, erf, fdc, pcap, pcapng, pkt, s	shark (5vw, acp, apc, atc, bfr, snoop, syc, tpc, tr1, trace, trc, wpc, wpz,
Nullsoft Install System v2,46	< Back Next > Cancel

g. You can change the installation location of Wireshark, but unless you have limited disk space, it is recommended that you keep the default location.

🚮 Wireshark 1.8.3 (64-bit) Setup	
Choose Install Location Choose the folder in which to install Wireshark	1.8.3 (64-bit).
Choose a directory in which to install Wireshark	2
Destination Folder	Prouve
Space required: 102 4VB	browse
Space available: 81.5GB	
Nullsoft Install System v2.46	< Back Next > Cancel

- h. To capture live network data, WinPcap must be installed on your PC. If WinPcap is already installed on your PC, the Install check box will be unchecked. If your installed version of WinPcap is older than the version that comes with Wireshark, it is recommend that you allow the newer version to be installed by clicking the **Install WinPcap x.x.x** (version number) check box.
- i. Finish the WinPcap Setup Wizard if installing WinPcap.

🗿 Wireshark 1.8.3 (64-bit) Setup			0	×
Install WinPcap? WinPcap is required to capture live net	twork data. Should WinPcap be installed	d?	L	V
Currently installed WnPcap version WinPcap 4.1.2				
Install	ad WinPcan 4.1.2 will be uninetalled firs			
In selected, the turnently installe	d WinPcap 4.1.2 will be uninstalled firs	t.		
What is WinPcap?				
Nullsoft Install System v2.46				
	< Back Install		Cancel	

j. Wireshark starts installing its files and a separate window displays with the status of the installation. Click **Next** when the installation is complete.

Wireshark 1.8.3 (64-bit) Setup	
nstallation Complete	1
Setup was completed successfully.	
Completed	
Extract: mergecap.html	•
Output folder: C:\Program Files\Wireshark	
Extract: capinfos.exe	
Extract: capinfos.html	
Output folder: C:\Program Files\Wireshark	
Extract: rawshark.exe	
Extract: rawshark.html	
Output folder: C:\Program Files\Wireshark	
Extract: user-guide.chm	
Camplated	

k. Click **Finish** to complete the Wireshark install process.



Part 2: Capture and Analyze Local ICMP Data in Wireshark

In Part 2 of this lab, you will ping another PC on the LAN and capture ICMP requests and replies in Wireshark. You will also look inside the frames captured for specific information. This analysis should help to clarify how packet headers are used to transport data to their destination.

Step 1: Retrieve your PC's interface addresses.

For this lab, you will need to retrieve your PC's IP address and its network interface card (NIC) physical address, also called the MAC address.

- a. Open a command window, type **ipconfig /all**, and then press Enter.
- b. Note your PC interface's IP address and MAC (physical) address.



c. Ask a team member for their PC's IP address and provide your PC's IP address to them. Do not provide them with your MAC address at this time.

Step 2: Start Wireshark and begin capturing data.

- a. On your PC, click the Windows **Start** button to see Wireshark listed as one of the programs on the pop-up menu. Double-click **Wireshark**.
- b. After Wireshark starts, click Interface List.



Note: Clicking the first interface icon in the row of icons also opens the Interface List.

c. On the Wireshark: Capture Interfaces window, click the check box next to the interface connected to your LAN.

	Description	P	Packets	Packets/s	
	Intel(F) PRO/1000 MT Network Connection		19	0	Details
	Intel(R) 82577LM Gigabit Network Connection	192.168.1.11	47	0	<u>D</u> etails
Help		Start	Stoo	Options	Close

Note: If multiple interfaces are listed and you are unsure which interface to check, click the **Details** button, and then click the **802.3 (Ethernet)** tab. Verify that the MAC address matches what you noted in Step 1b. Close the Interface Details window after verifying the correct interface.

haracteristics	Statistics 802.3 (Ethernet	802.11 (WLAN) Task Offload
Characteristics	5	
Characteristics Permanent s	s tation address	00:50:56:BE:76:8C

d. After you have checked the correct interface, click Start to start the data capture.

Wireshark	c Cap	ture Interfaces				- • •
		Description	P	Packets	Packets/s	
		Intel(R) PRO/1000 MT Network Connection		19	0	Details
	P	Intel(R) 82577LM Gigabit Network Connection	192.168.1.11	47	0	Details
<u>H</u> elp			Start	Stop	Options	<u>C</u> lose

Information will start scrolling down the top section in Wireshark. The data lines will appear in different colors based on protocol.

Capturing from Intel(R) 82577LM Gigabit Network Connection: \Devic	e\NPF_6179E093-A447-4EC8-81DF-5	E22D38A6F63] [Wireshark 1.8.3 (SVN Rev 45256 from /trunk-1.8)]	
File Edit View Go Capture Analyze Statistics Telephony	Tools hternals Help		
NHANNINDYGOLOAAA			
	A T III A A A		
Filter:	Expression Clear App	ly Seve	
No. Time Source Destinatio	on Protocol Ler	ngth Info	
21.2 451062000 risco 73:0//84 Enapoir	ng_trie_(for_hr:STP	60 conf Poot = 32768/0/30+f7+0d+73+ec+84 Cost =	0 Port = 0x8001
22 3 497376000 10 20 164 21 173 19	4 79 '25 TCP	it [TCP segment of a reassembled PDU]	V POLE - OXDUCE
23 3 567094000 173 194 79 125 10 20 1	164.2 TCP	60 xmon-client > 53588 [ACK] Segul Ack=38 win=1002	Len=0
24.4.451700000 Cisco 7a:ec:84 Spannin	ng-trie-(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 Spannin	ng-tree-(for-br-STP	60 Conf. Root = 32768/0/30:f7:0d:7a:ec:84 Cost =	0 Port = 0x8001
26.8.451225000 cisco 7a:ec:84 Spannin	ng-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	.12.7? TCP	55 53964 > 10846 [ACK] seg=1 Ack=1 win=63974 Len=1	
28 10, 35963200(173, 36, 12, 72 10, 20, 1	164.2. TCP	66 10846 > 53964 [ACK] Seg=1 Ack=2 win=513 Len=0 5	LE=1 SRE=2
29 10, 45232500(cisco 7a:ec:84 Spannin	ng-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. 51 NBNS	92 Name query NB UNIDC3:20>	
31 10, 99746700(171, 68, 57, 13 10, 20, 1	164.2 NBNS	98 Name query response. Requested name does not ex	ist
32 10, 99758500(10, 20, 164, 21 173, 37	.115. 91 NBNS	92 Name query NB UNIDC3<20>	
33 11, 08046600(173, 37, 115, 191 10, 20, 1	164.2. NBNS	98 Name query response. Requested name does not ex	ist
34 11, 0904 3000(10, 20, 164, 21 10, 20, 1	164.3. NBNS	92 Name query NB UNIDC3<20>	
35 11, 8404 3400(10, 20, 164, 21 10, 20, 3	164.3. NBNS	92 Name query NB UNIDC3(20>	
3612,45071000(Cisco_7a;ec:84 Spannin	ng-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. 3	164.3. NBN5	92 Name query NB UNIDC3<20>	
38 13. 34153600(10. 20. 164. 21 171. 68	.57.5) NBN5	92 Name query NB UNIDC3:20>	Sector Contraction of
39 13.41142100(171.68.57.13 10.20.1	164.2. NBNS	98 Name query response, Requested name does not ex	ist
40 13.41151700(10.20.164.21 173.37	.11591 NBN5	92 Name query NB UNIDC3<20>	
41 13.49295400(173.37.115.191 10.20.3	164.2. NBNS	98 Name query response, Requested name does not ex	ist
42 13. 502 50600(10. 20. 164. 21 10. 20. 3	164.3. NBNS	92 Name query NB UNIDC3<20>	
43 14. 25256700(10. 20. 164. 21 10. 20. 1	164.3. NBN5	92 Name query NB UNIDC3<20>	
44 14.45045300(cisco_7a:ec:84 Spannin	ng-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. 164	8.87.1 SRVLOC	86 Attribute Request, VI Transaction ID - 49289	
ei		"	,
Frame 1: 66 bytes on wire (528 bits), 66 bytes	captured (528 bits) on 1	nterface 0	
Ethernet II, Src: Dell_24:2a 60 (5c:26:0a:24:2	a:60), Dst: Cisco_7a:ec:8	4 (30:f7:0d:7a:ec:84)	
Internet Protocol Version 4, Src: 10.20.164.21	(10.20.164.21), DST: 204	.236.230.45 (204.236.230.45)	
Transmission Control Protocol, Src Port: 54996	5 (54996), Dst Port: https	(443), Seq: 0, Len: 0	
0000 30 f7 0d 7a ec 84 5c 26 0a 24 2a 60 08 00	45 0) 0 Z \& . \$* E	W	
0010 00 34 4f 78 40 00 80 06 4a 08 0a 14 a4 15	cc e: .40x8 J		
0020 e6 2d d6 d4 01 bb dc b2 af 4e 00 00 00 00	80 0!N	•	E
0030 20 00 8a 09 00 00 02 04 04 ec 01 03 03 02	01 0	·	
VVVV VV VL	••		•
IntelR) 82577LM Gigabit Network Conrection: \Device\NPF_[6179]	9E093-A447-4EC8-81DF Packets: 45	Displayed: 45 Marked: 0 Pr	ofile: Default

e. This information can scroll by very quickly depending on what communication is taking place between your PC and the LAN. We can apply a filter to make it easier to view and work with the data that is being captured by Wireshark. For this lab, we are only interested in displaying ICMP (ping) PDUs. Type **icmp** in the Filter box at the top of Wireshark and press Enter or click on the **Apply** button to view only ICMP (ping) PDUs.



f. This filter causes all data in the top window to disappear, but you are still capturing the traffic on the interface. Bring up the command prompt window that you opened earlier and ping the IP address that you received from your team member. Notice that you start seeing data appear in the top window of Wireshark again.

a capi	turing from Intel(F	R) PRO/1000 MT Net	work Connection [Wireshard	1.6.1 (SVN Rev 38096	from /trunk-1.6	5)]			0	
<u>File</u>	dit <u>V</u> iew <u>G</u> o	Capture Analyze	Statistics Telephony To	ols Internals <u>H</u> elp						_
		B 8 × 2		7 <u>4</u> EE	\oplus \bigcirc $\textcircled{0}$	2	🗹 🥵	% 🛱		
Filter:	icmp			Expression	Clear Apply					
No.	Time	Source	Destination	Protocol Le	ength Info					
1	1 15.118840	192.168.1.11	192.168.1.12	ICMP	74 Echo	(ping)	request	id=0x0001,	seq=21/5376,	ttl=1;
1	4 15.119602	192.168.1.12	192.168.1.11	ICMP	74 Echo	(ping)	reply	id=0x0001,	seq=21/5376,	ttl=1:
1	5 16.127853	192.168.1.11	192.168.1.12	ICMP	74 Echo	(ping)	request	id=0x0001,	seq=22/5632,	ttl=1;
1	7 16.128679	192.168.1.12	192.168.1.11	ICMP	74 Echo	(ping)	reply	id=0x0001,	seq=22/5632,	ttl=1;
1	8 17.141897	192.168.1.11	192.168.1.12	ICMP	74 Echo	(ping)	request	id=0x0001,	seq=23/5888,	ttl=1;
1	9 17.145943	192.168.1.12	192.168.1.11	ICMP	74 Echo	(ping)	reply	id=0x0001,	seq=23/5888,	ttl=12
2	1 18.140246	192.168.1.11	192.168.1.12	ICMP	74 Echo	(ping)	request	id=0x0001,	seq=24/6144,	ttl=1;
2	2 18.140794	192.168.1.12	192.168.1.11	ICMP	74 Echo	(ping)	reply	id=0x0001,	seq=24/6144,	tt]=1:
			C:\Windows	\system32\cmd.exe						• 83
Image: Control by Refrected adapter Local Area Connection* 11: Image: Connection = Specific DNS Suffix = 1 Media State = = : Media disconnected Connection = Specific DNS Suffix = 1 Description = : Media disconnected Description = : Media disconnected Internet II, Src: Vmware_be:76:8c (i B Internet Protocol Version 4, Src: 1 Media State = : Media disconnected C:> Internet Control Message Protocol C:> D:> D:>										
0000 0010	00 50 56 be 00 3c 01 ac	f6 db 00 50	tocol C:>>ping 19 Pinging 192 S6 be 7 b5 ad C Reply from Capture from	2.168.1.12 2.168.1.12 with 192.168.1.12:) 192.168.1.12:)	32 bytes o bytes=32 ti bytes=32 ti	of data ine=1ns ine<1ns	: TTL=128 TTL=128			

Note: If your team member's PC does not reply to your pings, this may be because their PC firewall is blocking these requests. Please see Appendix A: Allowing ICMP Traffic Through a Firewall for information on how to allow ICMP traffic through the firewall using Windows 7.

g. Stop capturing data by clicking the **Stop Capture** icon.



Step 3: Examine the captured data.

In Step 3, examine the data that was generated by the ping requests of your team member's PC. Wireshark data is displayed in three sections: 1) The top section displays the list of PDU frames captured with a summary of the IP packet information listed, 2) the middle section lists PDU information for the frame selected in the top part of the screen and separates a captured PDU frame by its protocol layers, and 3) the bottom section displays the raw data of each layer. The raw data is displayed in both hexadecimal and decimal form.

Cap	pturing from Intel(I	R) PRO/100	0 MT Net	work Co	nnection	[Wiresh	ark 1.6	5.1 (SVN Rev	38096 f	from /trunk-1.	6)]				
Eile	Edit View Go	Capture	Analyze	Statist	ics Telep	hony]	Tools	Internals	Help						
		6	* 2	8	Q, Þ	\$	Ŧ	2		Θ O O	🖭 🖗	K 🗹 🕵	% 😫		
Filter:	icmp							- Expres	ion	Clear Apply					
No.	Time	Source			Destinat	tion		Proto	col Le	ngth info					
	11 15,118840	192.16	58.1.11		192.1	68.1.1	.2	ICM).	74 Echo	(ping)	request	id=0x0001,	seq=21/5376,	ttl=1
	14 15.119602	192.16	58.1.12		192.1	68.1.1	1	ICM	2	74 Echo	(ping)	reply	id=0x0001,	seq=21/5376,	tt]=1;
	16 16.127853	192.16	8.1.11		192.1	68.1.1	.2	ICM	•	74 Echo	(ping)	request	id=0x0001,	seq=22/5632,	tt]=1;
	17 16.128679	192.16	58.1.12		192.1	68.1.1	.1	ICM	•	74 Echo	(ping)	reply	id=0x0001,	seq=22/5632,	tt]=1:
	18 17.141897	192.16	58.1.11		192.1	68.1.1	.2	ICM	•	74 Echo	(ping)	request	id=0x0001,	seq=23/5888,	tt]=12
	19 17.145943	192.16	8.1.12		192.1	68.1.1	.1	ICM	•	74 Echo	(ping)	reply	id=0x0001,	seq=23/5888,	tt]=12
	21 18.140246	192.16	8.1.11		192.1	68.1.1	.2	ICM	•	74 Echo	(ping)	request	id=0x0001,	seq=24/6144,	tt]=12
	22 18, 140794	192.16	8.1.12		192.1	68.1.1	1	ICM	8	74 Echo	(ping)	reply	id=0x0001,	seq=24/6144,	tt]=12
0000 0010 0020 0030 0040	00 50 56 be 00 3c 01 ac 01 0c 08 00 67 68 69 6a 77 61 62 63	f6 db 00 00 4d 46 6b 6c 64 65	00 50 80 01 00 01 6d 6e 66 67	56 be 55 ac 00 15 6f 70 68 69 n: P	e 76 8c d c0 a8 5 61 62 0 71 72 9	08 00 01 0b 63 64 73 74	45 c0 65 75 ed: 8 N	00 . PV a8 . <. 66 76 ghi wab Marked: 0	P .MF jklmn cdefg	V.VE. abcdef opgrstuv hi			Bot Profile: Defa	tom Seciton	< III +

a. Click the first ICMP request PDU frames in the top section of Wireshark. Notice that the Source column has your PC's IP address, and the Destination contains the IP address of the teammate's PC you pinged.

Int	tel(R) PR0/1000 M	T Network Connection []	Wireshark 1.6.1 (SVN Rev 380	96 from /trunk-1.	6)]					
Eile	Edit View Go	<u>Capture</u> <u>Analyze</u> <u>Sta</u>	atistics Telephony Tools	Internals Help	p					Source
			Q ⇔ ⇔ Q 7	2 🗐 🛢			🛛 🍕 🎇 🛛	B		Jource
Filter	: icmp			Expression.	Clear Apply					
No.	Time	Source	Destination	Protocol	Length Info					
	5 2.801784	192.168.1.11	192.168.1.12	ICMP	74 Echo	(ping) re	quest id=0	x0001, seq	=25/6400,	tt]=1;
	8 2.802679	192.168.1.12	192.168.1.11	ICMP	74 Echo	(ping) re	ply id=0	x0001, seq	=25/6400,	tt]=1;
	10 3.816895	192.168.1.11	192.168.1.12	ICMP	74 Echo	(ping) re	quest id=0	x0001, seq	=26/6656,	tt]=1;
	11 3.817540	192.168.1.12	192.168.1.11	ICMP	74 Echo	(ping) re	ply id=0	x0001, seq	=26/6656,	tt]=1;
	13 4.831343	(192.168.1.11)	192.168.1.12	ICMP	74 Echo	(pinci re	quest id=0	x0001, seq	=27/6912,	tt]=12
	14 4.832006	192.168.1.12	192.168.1.11	ICMP	74 Echo	(ping) re	ply id=0	x0001, seq	=27/6912,	tt]=1;
	15 5.844858	192.168.1.11	192.168.1.12	ICMP	74 Echo	(ping) re	quest id=0	x0001, seq	=28/7168,	tt]=1:
	16 5.845488	192.168.1.12	192.168.1.11	ICMP	74 Echo	(ping) re	ply id=0	x0001, seq	=28/7168,	tt]=1;

b. With this PDU frame still selected in the top section, navigate to the middle section. Click the plus sign to the left of the Ethernet II row to view the Destination and Source MAC addresses.

In In	M Intel(R) PR0/1000 MT Network Connection [Wireshark1.6.1 (SVN Rev 38096 from /trunk-1.6)]									
Eile	Edit View	<u>Go</u> <u>C</u> apture <u>A</u> nalyze	<u>Statistics</u> Telephony <u>T</u> ools	Internals Help	0					
		¥ 🖻 🖬 🗙 🔮	🖁 占 । 🔍 🗧 🌳 🤣 🐺	<u>2</u>			🗹 🍢	%		
Filte	: icmp			Expression.	Clear Apply					
No.	Time	Source	Destination	Protocol	Length Info					
	5 2.80178	84 192.168.1.11	192.168.1.12	ICMP	74 Echo	(ping)	request	id=0x0001,	seq=25/6400,	tt]=1:
	8 2.80267	79 192.168.1.12	2 192.168.1.11	ICMP	74 Echo	(ping)	reply	id=0x0001,	seq=25/6400,	tt]=12
	10 3.81689	95 192.168.1.11	192.168.1.12	ICMP	74 Echo	(ping)	request	id=0x0001,	seq=26/6656,	tt]=12
	11 3.81754	40 192.168.1.12	2 192.168.1.11	ICMP	74 Echo	(ping)	reply	id=0x0001,	seq=26/6656,	tt]=12
	13 4.83134	43 192.168.1.11	1 192.168.1.12	ICMP	74 Echo	(ping)	request	id=0x0001,	seq=27/6912,	tt]=12
	14 4.83200	06 192.168.1.12	2 192.168.1.11	ICMP	74 Echo	(ping)	reply	id=0x0001,	seq=27/6912,	tt]=1;
	15 5.8448	58 192.168.1.11	1 192.168.1.12	ICMP	74 Echo	(ping)	request	id=0x0001,	seq=28/7168,	tt]=12
	16 5.84548	58 192.168.1.1.	197.168.1.11	ICMP	74 ECho	(ping)	reply	1d=0x0001,	seq=28//168,	tt I=1.
			(502 bits) 21 but of a	petured (507	hite)					_
Ô	ame 15: 74	Src: IntelCor	(392 bits), 74 bytes c	aptured (592	Totel Of:0	1.48 (0.11.11	• 0f • 01 • 48)		
U	Doctinatio	n: Intel Of 01:	(00.11.11.0f.01.48)	52.10), DSU.	THEET_01.9	1.40 (.01.51.40)		
	Source: Tr	telcor 34.92.10	(58.94.6h.34.92.1c))						
	Type: TP ((0x0800)	()))))))))))))))))))))))))))))))))))))	12						
IF T	ternet Pro	tocol Version 4	Src: 192 168 1.11 (1	92.168.1.11)	Dst: 192.	168.1.	12 (192.)	168.1.12)		
E T	ternet Cor	trol Message Pr	otocol		,		(252			_
		in the stand of the								

Does the Source MAC address match your PC's interface?

Does the Destination MAC address in Wireshark match the MAC address that of your team member's?

How is the MAC address of the pinged PC obtained by your PC?

Note: In the preceding example of a captured ICMP request, ICMP data is encapsulated inside an IPv4 packet PDU (IPv4 header) which is then encapsulated in an Ethernet II frame PDU (Ethernet II header) for transmission on the LAN.

Part 3: Capture and Analyze Remote ICMP Data in Wireshark

In Part 3, you will ping remote hosts (hosts not on the LAN) and examine the generated data from those pings. You will then determine what is different about this data from the data examined in Part 2.

Step 1: Start capturing data on interface.

a. Click the Interface List icon to bring up the list PC interfaces again.

🗖 Int	el(R) F	PRO/10	00 MT	Netwo	ork C	onne	ction	[Wi	reshar	k1.
<u>F</u> ile	<u>E</u> dit	View	Go	Capt	ure	Ana	lyze	Stati	stics	Te
		N OI				x	R		0	4
Filter:	icm	р								
No.	Т	ïme		Sour	ce				D	esti

b. Make sure the check box next to the LAN interface is checked, and then click Start.

Wireshark: Cap	ture Interfaces				
	Description	IP	Packets	Packets/s	
	Intel(R) PRO/1000 MT Network Connection		19	0	Details
	Intel(R) 82577LM Gigabit Network Connection	192.168.1.11	47	0	<u>D</u> etails
Help		Start	Stop	Options	<u>C</u> lose

c. A window prompts to save the previously captured data before starting another capture. It is not necessary to save this data. Click **Continue without Saving**.



- d. With the capture active, ping the following three website URLs:
 - 1) www.yahoo.com
 - 2) www.cisco.com
 - 3) www.google.com

```
C:\Vindows\system32\cmd.es
C:\ping www.yahoo.com
Pingging www.yahoo.com
(72.30.38.140: bytes=32 timeins TIL=255
Reply from 72.30.38.140: bytes=32 time(ins TIL=255
Ping statistics for 72.30.38.140:
Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
Minimum = 0ms, Maximum = 1ms, Average = 0ms
C:\ping www.cisco.com
Pinging www.cisco.com
Pinging www.cisco.com
Pinging www.cisco.com
Pinging www.cisco.com
C:\ping www.cisco.com
Pinging www.cisco.com
Pinging www.cisco.com
C:\ping www.cisco.com
Pinging www.cisco.com
C:\ping www.cisco.com
Pinging www.cisco.com
Pinging www.cisco.com
Pinging www.cisco.com
C:\ping www.cisco.com
Pinging www.cisco.com
Pinging www.google.com
P
```

Note: When you ping the URLs listed, notice that the Domain Name Server (DNS) translates the URL to an IP address. Note the IP address received for each URL.

e. You can stop capturing data by clicking the Stop Capture icon.

Eile	Edit	View	Go	Capt	ure	Ana	lyze	Stat	istics	Telep
))		8	×	R		0	\$
Filter:	icm	р								
No.	1	ime		Sou	rce				D	estinat
	127	6.9/	5362	192	2.16	8.1	.11		1	92.1

Step 2: Examining and analyzing the data from the remote hosts.

a. Review the captured data in Wireshark, examine the IP and MAC addresses of the three locations that you pinged. List the destination IP and MAC addresses for all three locations in the space provided.

1 st Location:	IP:	MAC:
2 nd Location:	IP:	MAC:
3 rd Location:	IP:	MAC:

- b. What is significant about this information?
- c. How does this information differ from the local ping information you received in Part 2?

Reflection

Why does Wireshark show the actual MAC address of the local hosts, but not the actual MAC address for the remote hosts?

Appendix A: Allowing ICMP Traffic Through a Firewall

If the members of your team are unable to ping your PC, the firewall may be blocking those requests. This appendix describes how to create a rule in the firewall to allow ping requests. It also describes how to disable the new ICMP rule after you have completed the lab.

Step 1: Create a new inbound rule allowing ICMP traffic through the firewall.

a. From the Control Panel, click the System and Security option.



b. From the System and Security window, click Windows Firewall.



c. In the left pane of the Windows Firewall window, click Advanced settings.



d. On the Advanced Security window, choose the **Inbound Rules** option on the left sidebar and then click **New Rule...** on the right sidebar.

		Actions	
ofile Enabled	Action _	Inbound Rules	*
vate Yes vate Yes vate Yes vate Yes vate Yes vate Yes vate Yes No No	Allow Allow Allow Allow Allow Allow Allow Allow Allow Allow	 New Rule Filter by Profile Filter by State Filter by Group View Refresh Export List Help 	* * *
ofil val val val val val val	le Enabled te Yes te Yes te Yes te Yes te Yes te Yes te Yes te Yes No No	le Enabled Action A te Yes Allow te Yes Allow No Allow No Allow	Ie Enabled Action te Yes Allow te Yes Allow

e. This launches the New Inbound Rule wizard. On the Rule Type screen, click the **Custom** radio button and click **Next**



f. In the left pane, click the **Protocol and Ports** option and using the Protocol type drop-down menu, select **ICMPv4**, and then click **Next**.

Prev Inbound Rule Wizard			×
Protocol and Ports			
Specify the protocols and ports to v	which this rule applies.		
Steps:			
Rule Type	To which ports and protoc	cols does this rule apply?	
Program			
Protocol and Ports	Protocol type:	Any	
 Scope 	Protocol number:	Any Custom	
Action Peelle	· · · · <	ICMPv4	
Name	Local port:	IGMP TCP	
- Hono		UDP IPv6	
	Remote port:	IPv6-Route IPv6-Frag	
		GRE ICMPv6	
		IPv6-NoNot IPv6-Opts	
	Internet Control Message	VRRP PGM	
	(ICMP) settings:	L2TP	
	Learn more about protoco	and perts	
		< Back Next > Cancel	
			_

g. In the left pane, click the Name option and in the Name field, type Allow ICMP Requests. Click Finish.

Prew Inbound Rule Wizard		×
Name		
Specify the name and description	n of this ule.	
Steps:		
Rule Type		
Program		
Protocol and Ports	N	
 Scope 	Allow ICMP Requests	
 Action 	Developed Alexand	
Profile	Description (optional):	
Name		
	\frown	
	< Back (Finish) Cancel	

This new rule should allow your team members to receive ping replies from your PC.

Step 2: Disabling or deleting the new ICMP rule.

After the lab is complete, you may want to disable or even delete the new rule you created in Step 1. Using the **Disable Rule** option allows you to enable the rule again at a later date. Deleting the rule permanently deletes it from the list of Inbound Rules.

a. On the Advanced Security window, in the left pane, click **Inbound Rules** and then locate the rule you created in Step 1.

File Action View Help								
🗢 🔿 🙍 📰 📑 🖬 💼								
Windows Firewall with Advance	Inbound Rules						Actions	
Inbound Rules	Name	Group	Profile	Enabled	Action	-	Inbound Rules	
Connection Security Rules	Allow ICMP Requests		All	Yes	Allow		😹 New Rule	
Monitoring	Jave(TM) 2 Platform Standard Edition bin		Private	Yes	Allow	Ξ	Fiter by Profile	,
	🕼 Java(TM) 2 Platforn Standard Edition bin		Private	Yes	Allow		The bullet	
	Java(TM) Platform SE binary		Private	Yes	Allow		Y Fiter by State	
	🕑 Java(TM) Platform 🛿 binary		Private	Yes	Allow		Fiter by Group	,
	© winradius.exe © winradius.exe			Yes	Allow		View	,
				Yes	Allow		B Defrach	
	🔇 winradius.exe		Private	Yes	Allow		Marchi	
	🕑 winradius.exe		Private	Yes	Allow	w	Biport List	
	BranchCache Content Retrieval (HTTP-In)	BranchCache - Content Retr	All	No	Allow		Help	
	BranchCache Hosted Cache Server (HTT	BranchCache - Hosted Cach	All	No	Allow			
	BranchCache Peer Discovery (WSD-In)	BranchCache - Peer Discove	All	No	Allow		Allow CMP Requests	
	Connect to a Network Projector (TCP-In)	Connect to a Network Proje	Domain	No	Allow		Disable Rule	
	Connect to a Network Projector (TCP-In)	Connect to a Network Proje	Private	No	Allow		K Cut	
	Connect to a Network Projector (WSD Ev	Connect to a Network Proje	Private	No	Allow		R. Com	
	Connect to a Network Projector (WSD Ev	Connect to a Network Proje	Domain	No	Allow		чы сору	
	Connect to a Network Projector (WSD Ev	Connect to a Network Proje	Domain	No	Allow		💢 Delete	
	Connect to a Network Projector (WSD Ev	Connect to a Network Proje	Private	No	Allow		Properties	

b. To disable the rule, click the **Disable Rule** option. When you choose this option, you will see this option change to **Enable Rule**. You can toggle back and forth between Disable Rule and Enable Rule; the status of the rule also shows in the Enabled column of the Inbound Rules list.

Windows Firewall with Advanced	I Security								
File Action View Help									
◆ ⇒ 2 🖬 🖻 🖬 🖬									
Windows Firewall with Advance	Inbound Rules						Actions		
Irbound Rules	Name	Group	Profile	Enabled	Action	-	Inbound Rules		
Connection Security Rules	Allow ICMP Requess		All C	Yes	Allow		Kan New Rule		
Monitoring	Java(TM) 2 Platform Standard Edition bin		Private	Yes	Allow	E	V Fiter by Profile	•	
	Java(TM) 2 Platform Standard Edition bin		Private	Yes	Allow		Thurby Chate		
	Java(TM) Platform SE binary		Private	Yes	Allow		Y Fiter by State		
	🕼 Java(TM) Platform 🗄 binary		Private	Yes	Allow		Filter by Group	•	
	🕑 winradius.exe			Yes	Allow		View	•	
	@ winradius.exe	Private	Yes	Allow		B Refrach			
	@ winradius.exe		Private	Yes	Allow		Ca Noresh		
	🕑 winradius.exe		Private	Yes	Allow		Boport List		
	BranchCache Content Retrieval (HTTP-In)	EranchCache - Content Retr	All	No	Allow		Help		
	BranchCache Hosted Cache Server (HTT	EranchCache - Hosted Cach	All	No	Allow			500	
	BranchCache Peer Discovery (WSD-In)	EranchCache - Peer Discove	All	No	Allow		Allow CMP Requests	- 18 A	
	Connect to a Network Projector (TCP-In)	Connect to a Network Proje	Domain	No	Allow		🔹 Disable Rule		
	Connect to a Network Projector (TCP-In)	Connect to a Network Proje	Private	No	Allow		& Cut		
	Connect to a Network Projector (WSD Ev	Connect to a Network Proje	Private	No	Allow		Ph. Com		
	Connect to a Network Projector (WSD Ev	Connect to a Network Proje	Domain	No	Allow		Copy		
	Connect to a Network Projector (WSD Ev	Connect to a Network Proje	Domain	No	Allow		🗙 Delete		

c. To permanently delete the ICMP rule, click **Delete**. If you choose this option, you must re-create the rule again to allow ICMP replies.

IC IVEU	All	no	Allow	🔝 пер
Cach	All	No	Allow	
scove	All	No	Allow	Allow ICMP Requests
Proje	Domain	No	Allow	Disable Rule
Proje	Private	No	Allow	🔏 Cut
Proje	Private	No	Allow	P. Com
Proje	Domain	No	Allow	ез сору
Proje	Domain	No	Allow 🤇	🗙 Delete 🔵
Proie	Private	No	Allow	Properties