Solution to Wireshark Lab: ICMP

C:\WINDOWS\system32\cmd.exe
C:\Documents and Settings\Paula Wing>ping -n 10 www.ust.hk 🗾
Pinging www.ust.hk [143.89.14.34] with 32 bytes of data:
Reply from 143.89.14.34: bytes=32 time=294ms TTL=240 Reply from 143.89.14.34: bytes=32 time=292ms TTL=240 Reply from 143.89.14.34: bytes=32 time=293ms TTL=240 Reply from 143.89.14.34: bytes=32 time=293ms TTL=240 Reply from 143.89.14.34: bytes=32 time=294ms TTL=240 Reply from 143.89.14.34: bytes=32 time=292ms TTL=240 Reply from 143.89.14.34: bytes=32 time=293ms TTL=240 Reply from 143.89.14.34: bytes=32 time=293ms TTL=240 Reply from 143.89.14.34: bytes=32 time=293ms TTL=240 Reply from 143.89.14.34: bytes=32 time=295ms TTL=240
Ping statistics for 143.89.14.34: Packets: Sent = 10, Received = 10, Lost = 0 (0% loss), Approximate round trip times in milli-seconds: Minimum = 292ms, Maximum = 295ms, Average = 293ms C:\Documents and Settings\Paula Wing>

Fig. 1 Command prompt after ping request

1. What is the IP address of your host? What is the IP address of the destination host?

The IP address of my host is 192.168.1.101. The IP address of the destination host is 143.89.14.34.

2. Why is it that an ICMP packet does not have source and destination port numbers?

The ICMP packet does not have source and destination port numbers because it was designed to communicate network-layer information between hosts and routers, not between application layer processes. Each ICMP packet has a "Type" and a "Code". The Type/Code combination identifies the specific message being received. Since the network software itself interprets all ICMP messages, no port numbers are needed to direct the ICMP message to an application layer process.

File Edit View Go Capture Analyze Statistics Help Image: Source Source Control Source Destination Protocol Info 3 0.001655 192.168.1.101 143.89.14.34 192.168.1.101 143.89.14.34 192.168.1.101 143.89.14.34 192.168.1.101 ICMP Echo (ping) request 4 0.415098 143.89.14.34 192.168.1.101 ICMP Echo (ping) request * Ethernet II, Src: DellComp_4f:36:23 (00:08:74:4f:36:23), Dst: LinksysG_da:af:73 (00:06:2 Internet Protocol, Src: 192.168.1.101 (192.168.1.101), Dst: 143.89.14.34 (143.89.14.34) Internet Control Message Protocol Type: 8 (Echo (ping) request) Code: 0 Checksum: 0xe45a [correct] Identifier: 0x0200 Sequence number: 26369 (0x6701) Data (32 bytes)
Filter: icmp Expression Clear Apply No Time Source Destination Protocol Info 3 0.001656 192.168.1.101 143.89.14.34 ICMP Echo (ping) request 4 0.415098 143.89.14.34 192.168.1.101 ICMP Echo (ping) request * Frame 3 (74 bytes on wire, 74 bytes captured) * * * Ethernet II, Src: DellComp_4f:36:23 (00:08:74:4f:36:23), Dst: LinksysG_da:af:73 (00:06:2 * Internet Protocol, src: 192.168.1.101 (192.168.1.101), Dst: 143.89.14.34 (143.89.14.34) * Internet Control Message Protocol Type: 8 (Echo (ping) request) Code: 0 Code: 0 Checksum: 0xe45a [correct] Identifier: 0x0200 Sequence number: 26369 (0x6701)
No. · Time Source Destination Protocol Info 3 0.001656 192.168.1.101 143.89.14.34 ICMP Echo (ping) request 4 0.415098 143.89.14.34 192.168.1.101 ICMP Echo (ping) request * * * * *
3 0.001656 192.168.1.101 143.89.14.34 ICMP Echo (ping) request 4 0.415098 143.89.14.34 192.168.1.101 ICMP Echo (ping) reply
4 0.415098 143.89.14.34 192.168.1.101 ICMP Echo (ping) reply Frame 3 (74 bytes on wire, 74 bytes captured) Ethernet II, Src: DellComp_4f:36:23 (00:08:74:4f:36:23), Dst: LinksysG_da:af:73 (00:06:2 Internet Protocol, Src: 192.168.1.101 (192.168.1.101), Dst: 143.89.14.34 (143.89.14.34) Internet Control Message Protocol Type: 8 (Echo (ping) request) Code: 0 Checksum: 0xe45a [correct] Identifier: 0x0200 Sequence number: 26369 (0x6701)
 Ethernet II, Src: DellComp_4f:36:23 (00:08:74:4f:36:23), Dst: LinksysG_da:af:73 (00:06:2 Internet Protocol, Src: 192.168.1.101 (192.168.1.101), Dst: 143.89.14.34 (143.89.14.34) □ Internet Control Message Protocol Type: 8 (Echo (ping) request) Code: 0 Checksum: 0xe45a [correct] Identifier: 0x0200 Sequence number: 26369 (0x6701)
0000 00 06 25 da af 73 00 08 74 4f 36 23 08 00 45 00 s
File: "C:\Documents and Settings\Paula Wing\My Documents\Wireshark\tr P: 22 D: 20 M: 0 ///

Fig. 2 ICMP Echo Request message

3. Examine one of the ping request packets sent by your host. What are the ICMP type and code numbers? What other fields does this ICMP packet have? How many bytes are the checksum, sequence number and identifier fields?

The ICMP type is 8, and the code number is 0. The ICMP packet also has checksum, identifier, sequence number, and data fields. The checksum, sequence number and identifier fields are two bytes each.

📶 icmp-ethereal-trace-1 - Wireshark												
<u>File Edit View Go Capture Analyze Statistics Help</u>												
Eilter: icmp Expression Clear Apply												
No Time Source Destination Protocol Info												
3 0.001656 192.168.1.101 143.89.14.34 ICMP Echo (ping) request 4 0.415098 143.89.14.34 192.168.1.101 ICMP Echo (ping) reply												
T E												
 Ethernet II, Src: LinksysG_da:af:73 (00:06:25:da:af:73), Dst: DellComp_4f:36:23 (00:08:7 Internet Protocol, Src: 143.89.14.34 (143.89.14.34), Dst: 192.168.1.101 (192.168.1.101) Internet Control Message Protocol Type: 0 (Echo (ping) reply) Code: 0 Checksum: 0xec5a [correct] Identifier: 0x0200 Sequence number: 26369 (0x6701) Data (32 bytes) 												
<u>т</u>												
0000 00 08 74 4f 36 23 00 06 25 da af 73 08 00 45 00to6# %s.E. 0010 00 3c b3 63 40 00 e7 01 80 d4 8f 59 0e 22 c0 a8 .<.c@Y." 0020 01 65 00 00 <mark>ec 5a</mark> 02 00 67 01 61 62 63 64 65 66 .e 2 . g.abcdef 0030 67 68 69 6a 6b 6c 6d 6e 6f 70 71 72 73 74 75 76 ghijklimn opqrstuv 0040 77 61 62 63 64 65 66 67 68 69 wabcdefg hi												
Checksum (icmp.checksum), 2 bytes P: 22 D: 20 M: 0												

Fig. 3 ICMP Echo reply message

4. Examine the corresponding ping reply packet. What are the ICMP type and code numbers? What other fields does this ICMP packet have? How many bytes are the checksum, sequence number and identifier fields?

The ICMP type is 0, and the code number is 0. The ICMP packet also has checksum, identifier, sequence number, and data fields. The checksum, sequence number and identifier fields are two bytes each.

- 5. What is the IP address of your host? What is the IP address of the target destination host? The IP address of my host is 192.168.1.101. The IP address of the destination host is 138.96.146.2.
- 6. If ICMP sent UDP packets instead (as in Unix/Linux), would the IP protocol number still be 01 for the probe packets? If not, what would it be? No. If ICMP sent UDP packets instead, the IP protocol number should be 0x11

📶 icmp-ethereal-trace-2	- Wireshark		
<u>Eile E</u> dit <u>V</u> iew <u>G</u> o <u>C</u> a	pture <u>A</u> nalyze <u>S</u> tatistics <u>H</u> e	elp	
	🕷 🗁 🔣 🗙	% ≞ ସ ≎	
Eilter: icmp		▼ E	xpression ⊆lear Apply
No Time	Source	Destination	Protocol Info
1 0.000000		138.96.146.2	ICMP Echo (ping) request
2 0.013151 3 0.013258		192.168.1.101 138.96.146.2	ICMP Time-to-live exceeded (Tim ICMP Echo (ping) request
⊞ Ethernet II, Sro	•	(00:08:74:4f:36:23), Dst: LinksysG_da:af:73 (00:06:25
Internet Protoco Internet Control		01 (192.168.1.101),	Dst: 138.96.146.2 (138.96.146.2)
	(ping) request)		
Identifier: 0x			
	r: 41985 (0xa401)		
Data (64 bytes)		
र			>
0000 00 06 25 da (0010 00 5c d2 d5 (6 23 08 00 45 00 0 a8 01 65 8a 60	%s t06#E.
0020 92 02 08 00 0 0030 00 00 00 00 00	51 fe O2 OO a4 O1 O		······
0040 00 00 00 00 0	0 00 00 00 00 00 00	0 00 00 00 00 00	
0050 00 00 00 00 00 0 0060 00 00 00 00 00 0		0 00 00 00 00 00	· · · · · · · · · · · · · · · · · · ·
Internet Control Message Prot	ocol (icmp) 72 bytes	P: 102 D: 102	2M+0
inconnection incodage into	. 100	MD acho request	

Fig. 4 ICMP echo request packet

7. Examine the ICMP echo packet in your screenshot. Is this different from the ICMP ping query packets in the first half of this lab? If yes, how so? *The ICMP echo packet has the same fields as the ping query packets.*

<mark>71</mark> icmp-ethereal-trace-2 - Wireshark						_ 🗆 🗵
Eile Edit View Go Capture Analyze Statistics	Help					
	× 🖓 📇	9	⇔ ¢	₽ T	죠 🔳	
Eilter: icmp		▼ <u>[</u>	xpression	. <u>⊂</u> lear <u>A</u> p	ply	
No Time Source	Destination		Protocol	Info		4
1 0.000000 192.168.1.101 2 0.013151 10.216.228.1	138.96.1 192.168		ICMP ICMP	Echo (p	ing) requ -live exc	est
3 0.013258 192.168.1.101	138.96.3		ICMP		ing) requ	
■ Frame 2 (70 bytes on wire, 70 byt	es capture:	d)		_		
Ethernet II, Src: LinksysG_da:af: Internet Protocol, Src: 10.216.22						
Internet Potocol, Sic. 10.210.22 Internet Control Message Protocol		0.228.1), L	51. 192	.108.1.1	.01 (192.1	
Type: 11 (Time-to-live exceeded		-				
Code: 0 (Time to live exceeded Checksum: 0x2c16 [correct]	in transit)				
Internet Protocol, Src: 192.168	3.1.101 (19	2.168.1.101	.), Dst:	138.96.	146.2 (13	38.96.14
🗆 Internet Control Message Protoc	:0]					
Type: 8 (Echo (ping) request) Code: 0	I					
Checksum: 0x51fe [correct]						
Identifier: 0x0200						
Sequence number: 41985 (0xa40	1)					
4						Þ
	a af 73 08 8 0a d8 e4	00 45 c0		%s. . 1		
0020 01 65 0b 00 2c 16 00 00 00 0	0 45 00 00	5c d2 d5	.e,.	E	\	
0030 00 00 01 01 d1 45 c0 a8 01 6 0040 51 fe 02 00 a4 01	5 8a 60 92	02 08 00	Е. Q	e	• • •	
I Internet Control Message Protocol (icmp), 36 bytes		P: 102 D: 102 M	:0			
		man naalta				

Fig. 5 ICMP error packet

8. Examine the ICMP error packet in your screenshot. It has more fields than the ICMP echo packet. What is included in those fields?

The ICMP error packet is not the same as the ping query packets. It contains both the IP header and the first 8 bytes of the original ICMP packet that the error is for.

7 icmp	etba	roal	teac	·o_2	- 10	iroc	har	ŀ																					_ 10	
_								N lyze	Stat	istics	5 1	Help																		<u> </u>
0.0 5			20		-pcai		<u></u>	.,	2000			<u>101</u> p													. [1.	
	Ë.	0	(X	0		(6	8		×	¢	à	2		٩	<	2	\$	4	0	Ŧ		<u>₽</u>				Ş		
Eilter:																	•	Ē	xpressi	on	⊆	ear	Арр	bly						
No. 🗸		me				ource						De	estin	ation					Proto		Info									
)8 1))9 1)							.1468.1.		_					.1. 146	101 .2			ICMF					ng) ng)		ep		t		
)0 18)1 18							$.146 \\ 8.1.$.1. 146	101 .2			ICMF					ng) ng)				t		
)2 18							.140								101			ICMF					nq)						
		0.00	(1.0	G 1	o et	D.C.	<u> </u>			1.04	G L	n at		<i></i>		und'		_		_	_	_								▶
 Frame 102 (106 bytes on wire, 106 bytes captured) Ethernet II, Src: LinksysG_da:af:73 (00:06:25:da:af:73), Dst: DellComp_4f:36:23 (00:08:74 Internet Protocol, Src: 138.96.146.2 (138.96.146.2), Dst: 192.168.1.101 (192.168.1.101) 																														
🗆 Int	erne	et c	ont	ro	1 M	ess	ag	e Pr	oto			-	(1)	0		.+0.	- /,	0.			. 10			<u>.</u>	(+.		100		101	- /
	ype ode		(EC	ho	(р	ing	D	rep	ly)																					
	hecl					_	or	rect	:]																					
-	dent Segui						79	5 ()	nyde	501	2																			
	ata)					54	/0	5 ((JUL.																				
			-																											
(Þ
0000 0010	00) 06 2 01							00 02	45	00 a8		·.to	6#. @.	• •	6	ş	Ε.						
0020	01	65 1	00 0	00	27	fe	02	2 00	d	6 Ū)1	00	00	00	00	00	ōō		.e	·										
0030 0040	00 00		00 (00 () 00) 00							00		00		::::	:::	: :			::						
0050 0060	00		00 (00 (000		00	00	00	00	00	00		• • • •	•••	• •	• • •		••						
	~~				~~	20	00													•••	• •	•••								
File: "C:\	\Docur	nents	and :	Setti	ings'l	Paula	a Wi	ing\M	y Doc	umer	nts\'	Wire	shar	kltra	c [P: 10)2 D:	102	M: 2	_										
											1																			- 11

Fig. 6 Last three ICMP reply packets

9. Examine the last three ICMP packets received by the source host. How are these packets different from the ICMP error packets? Why are they different?

The last three ICMP packets are message type 0 (echo reply) rather than 11 (TTL expired). They are different because the datagrams have made it all the way to the destination host before the TTL expired.

C:\WIND	D₩5\sy	stem32	2\cm	d.exe		
C:\Docume	ents a	and Se	etti	ngs∖Pa	ula	Wing>tracert www.inria.fr
					r [138.96.146.2]
over a ma	(X IIIUI	I UF 3)e 11	ops.		
1 1	ms		ms		ms	dslrouter [192.168.1.1]
	o ms ms	33 32		34		10.14.10.1
81 3.	. ms	34	ms	31	ms	P1-0.LCR-01.SPFDMA.verizon-gni.net [130.81.44.10
	o ms	37	MS	37	MS	so-1-3-1-0.BB-RTR1.BOS.verizon-gni.net [130.81.2
5 39) _{ms}	37	ms	39	ms	0.so-5-2-0.XL1.BOS4.ALTER.NET [152.63.19.129]
	7 ms	67		69		0.so-7-0-0.XL1.CHI13.ALTER.NET [152.63.64.206]
	ms	69		68		0.so-6-0-0.BR2.CHI13.ALTER.NET [152.63.73.25]
1 8 6	? ms	69	ms	67	ms	sl-st21-chi-3-0-0.sprintlink.net [144.232.18.141
9 66	, ms	68	ms	67	ms	sl-st20-chi-1-0.sprintlink.net [144.232.8.102]
	} ms	67	ms	67	ms	sl-franc2-76974-0.sprintlink.net [160.81.179.186
]		~~				
11 88 40.138]	} ms	89	ms	89	ms	po14-0.nykcr2.NewYork.opentransit.net [193.251.2
	÷	174	ms	173	ms	pos0-0-0-1.auvtr1.Aubervilliers.opentransit.net
[193.251	241.1					
	2 ms	171	ms	171	ms	<pre>tengige0-15-0-4.pastr1.Paris.opentransit.net [19</pre>
3.251.240 14 172	0.213] ? ms	l 171		171		gi9-0-0.passe2.Paris.opentransit.net [193.251.24
0.2141''	. 115	111	ШS	171	ШS	917-0-0.passe2.rar1s.opentrans1t.net 1175.251.24
	2 ms	171	ms	171	ms	po6-2.bagse1.Bagnolet.opentransit.net [193.251.2
41.118]						
	ms	177		175		lyon-pos1-0.cssi.renater.fr [193.51.185.30]
17 199) ms	197	ms	199	ms	grenoble-pos1-0.cssi.renater.fr [193.51.179.238]
18 199	ms	197	ms	197	ms	nice-pos2-0.cssi.renater.fr [193.51.180.34]
19 198	} ms	198	MS	197	ms	inria-nice.cssi.renater.fr [193.51.181.137]
20 19	7 ms	197	ms	197	ms	www.inria.fr [138.96.146.2]
Trace con	mlete					
Trace CO	prece	7 .				
C:\Docume	ents a	and Se	etti	ngs∖Pa	ula	Wing>
J						

Fig. 7 Command prompt for traceroute

10. Within the tracert measurements, is there a link whose delay is significantly longer than others? Refer to the screenshot in Figure 4, is there a link whose delay is significantly longer than others? On the basis of the router names, can you guess the location of the two routers on the end of this link?

There is a link between steps 11 and 12 that has a significantly longer delay. This is a transatlantic link from New York to Aubervilliers, France. In figure 4 from the lab, the link is from New York to Pastourelle, France.