Lab – Using Wireshark to Examine Ethernet Frames





Objectives

Part 1: Examine the Header Fields in an Ethernet II Frame

Part 2: Use Wireshark to Capture and Analyze Ethernet Frames

Background / Scenario

When upper layer protocols communicate with each other, data flows down the Open Systems Interconnection (OSI) layers and is encapsulated into a Layer 2 frame. The frame composition is dependent on the media access type. For example, if the upper layer protocols are TCP and IP and the media access is Ethernet, then the Layer 2 frame encapsulation will be Ethernet II. This is typical for a LAN environment.

When learning about Layer 2 concepts, it is helpful to analyze frame header information. In the first part of this lab, you will review the fields contained in an Ethernet II frame. In Part 2, you will use Wireshark to capture and analyze Ethernet II frame header fields for local and remote traffic.

Required Resources

• 1 PC (Windows 7, Vista, or XP with Internet access with Wireshark installed)

Part 1: Examine the Header Fields in an Ethernet II Frame

In Part 1, you will examine the header fields and content in an Ethernet II Frame. A Wireshark capture will be used to examine the contents in those fields.

Step 1:	Review the	Ethernet I	l header field	I descriptions	and lengths.
---------	------------	------------	----------------	----------------	--------------

Preamble	Destination Address	Source Address	Frame Type	Data	FCS
8 Bytes	6 Bytes	6 Bytes	2 Bytes	46 – 1500 Bytes	4 Bytes

Step 2: Examine the network configuration of the PC.

This PC host IP address is 10.20.164.22 and the default gateway has an IP address of 10.20.164.17.

Ethernet adapter Local Area Connection: Connection-specific DNS Suffix . : cisco.com Link-local IPv6 Address : fe80::b875:731b:3c7b:c0b1%10 IPv4 Address. : 10.20.164.22 Subnet Mask : 255.255.255.240 Default Gateway : 10.20.164.17

Step 3: Examine Ethernet frames in a Wireshark capture.

The Wireshark capture below shows the packets generated by a ping being issued from a PC host to its default gateway. A filter has been applied to Wireshark to view the ARP and ICMP protocols only. The session begins with an ARP query for the MAC address of the gateway router, followed by four ping requests and replies.

📶 Int	el(R) 82577LI	M Gigabit Netwo	rk Connect	ion: \Device	NPF_(6179E093	-A447-4E0	8-81DF-5E22D08A6	63) [Wire:	hark 1.8.3	(SVN Rev	45256 from	/trunk-1.8)]		
Eile	Edit View	Go Capture	Analyze	Statistics	Telephony I	ools Inte	rnals <u>H</u> elp							
		🕷 🖻 🗖	* 2	819	\$ \$ \$	7 2		20.0	1 🛛	2 🔊	% 🛙 🖽			
Filter	arp or icm	P				-	Expression Clear	Apply S	ave					
802.11	Channel:	Channel Offset	FCS	Filter: All Fi	rames	None	 Wireless Set 	tings De	cryption K	leys				
No.	Time	Source	e		Destination	1	Protoco	Length	Info					
	7 9.60	1177000 Del	_24:2a	: 60	Broadca	st	ARP	4	2 who h	nas 10.	20.164.17	'? Tell 10.	20.164.22	
	8 9.60	1803000 Ciso	:o_7a:ed	c:84	De11_24	:2a:60	ARP	6	0 10.20).164.1	7 is at 3	30:f7:0d:7a:	ec:84	
	9 9.60	1827000 10.2	20.154.2	22	10.20.1	64.17	ICMP	7	4 Echo	(ping)	request	id=0x0001,	seq=37/9472,	tt]=128
	10 9.60	2807000 10.2	20.164.1	17	10.20.1	64.22	ICMP	7	4 Echo	(ping)	reply	id=0x0001,	seq=37/9472,	tt1=255
	12 10.6	0418700(10.2	20.164.2	22	10.20.1	64.17	ICMP	7	4 Echo	(ping)	request	1d=0x0001,	seq=38/9728,	tt =128
	13 10.6	2072800(10.	20.164.1	17	10.20.1	64.22	ICMP	7	4 Echo	(ping)	reply	1d=0x0001,	seq=38/9728,	tt1=255
	14 11.0	0/19200(10.	20.164.4	22	10.20.1	64.1/	ICMP	/	4 ECho	(ping)	request	1d=0x0001,	seq=39/9984,	tt =128
	15 11.6	081//00(10.	20.164.1	17	10.20.1	64.22	ICMP	1	4 ECNO	(ping)	reply	1d=0x0001,	seq=39/9984,	tt1=255
	1/ 12.0	1025800(10.	20.104.4	22	10.20.1	64.17	ICMP	1	4 ECho	(ping)	request	1d=0x0001,	seq=40/10240	, ttl=128
	18 12.0	1131800(10.	20.104.1	17	10.20.1	04.22	ICMP	1	4 ECHO	(ping)	reply	1d=0x0001,	seq=40/10240	, tt1=255
<			_	_					_	_				•
ET	ame 7:4 hernet I Destinat Source:	2 bytes on I, Src: Del ion: Broadc Dell_24:2a:	wire (3 1_24:2a ast (ff 60 (5c:	36 bits) :60 (5c: :ff:ff:f 26:0a:24	, 42 bytes 26:0a:24:2 f:ff:ff) :2a:60)	captur a:60),	ed (336 bits) Dst: Broadcast	on inte (ff:ff	rface (:ff:ff	0 : <mark>ff:ff</mark>)				
	Type: AR	P (0x0806)												
🕀 Ad	dress Re	solution Pr	otocol	(request)									
0000 0010 0020	ff ff 1 08 00 0 00 00 0	ff ff ff ff 06 04 00 01 00 00 00 00	5c 26 5c 26 0a 14	0a 24 23 0a 24 23 a4 11	a 60 (8 06 a 60 (a 14	00 01 a4 16	\& . \$* & . \$*							

Step 4: Examine the Ethernet II header contents of an ARP request.

The following table takes the first frame in the Wireshark capture and displays the data in the Ethernet II header fields.

Field	Value	Description
Preamble	Not shown in capture	This field contains synchronizing bits, processed by the NIC hardware.
Destination Address	Broadcast (ff:ff:ff:ff:ff)	Layer 2 addresses for the frame. Each address is 48 bits long, or 6 octets, expressed as 12 hexadecimal digits, 0-
Source Address	Dell_24:2a:60 (5c:26:0a:24:2a:60)	 9, A-F. A common format is 12:34:56:78:9A:BC. The first six hex numbers indicate the manufacturer of the network interface card (NIC), the last six hex numbers are the serial number of the NIC. The destination address may be a broadcast, which contains all ones, or a unicast. The source address is always unicast.
Frame Type	0x0806	For Ethernet II frames, this field contains a hexadecimal value that is used to indicate the type of upper-layer protocol in the data field. There are numerous upper-layer protocols supported by Ethernet II. Two common frame types are: Value Description 0x0800 IPv4 Protocol 0x0806 Address resolution protocol (ARP)
Data	ARP	Contains the encapsulated upper-level protocol. The data field is between $46 - 1,500$ bytes.
FCS	Not shown in capture	Frame Check Sequence, used by the NIC to identify errors during transmission. The value is computed by the sending machine, encompassing frame addresses, type, and data field. It is verified by the receiver.

What is significant about the contents of the destination address field?

Why does the PC send out a broadcast ARP prior to sending the first ping request?

What is the MAC address of the source in the first frame? What is the Vendor ID (OUI) of the Source's NIC? What portion of the MAC address is the OUI?

What is the Source's NIC serial number?

Part 2: Use Wireshark to Capture and Analyze Ethernet Frames

In Part 2, you will use Wireshark to capture local and remote Ethernet frames. You will then examine the information that is contained in the frame header fields.

Step 1: Determine the IP address of the default gateway on your PC.

Open a command prompt window and issue the **ipconfig** command. What is the IP Address of the PC Default Gateway?

Step 2: Start capturing traffic on your PC's NIC.

- a. Open Wireshark.
- b. On the Wireshark Network Analyzer toolbar, click the Interface List icon.



c. On the Wireshark: Capture Interfaces window, select the interface to start traffic capturing by clicking the appropriate check box, and then click **Start**. If you are uncertain of what interface to check, click **Details** for more information about each interface listed.

	Description		IP	Packets	Packets/s	
📄 😥 Sun		fe80::	50e4:c3e6:b635:a	999 26	0	Details
🕐 🖅 Intel(R) 82	2577LM Gigabit Network Co	nnection fe80::I	o875:731b:3c7b:c	Ob1 95	1	Details

d. Observe the traffic that appears in the Packet List window.

Filter		Expression	Clear	Apply Save
802.11	Ghamel: Channel Offset: CS Filter: All I	Frames + None - Wi	reless Setti	ngs Decryption Keys
No.	Time Source	Destination	Protocol	
	19 10, 60449100(184, 27, 190, 41	10.20.164.22	TL SV1	587 Application Data
	20 10, 80121900(10, 20, 164, 22	184, 27, 190, 41	TCP	54 62408 > https [ACK] Seg=1163 Ack=534 win=16695 Len=0
	21 11.04927800(10.20.164.22	10, 20, 164, 31	NBNS	92 Name guery NB HP094B61<00>
	22 11.79926500(10.20.164.22	10.20.164.31	NBNS	92 Name guery NB HP094B61<00>
	2312.03732100(cisco_7a:ec:84	Spanning-tree-(for-br	STP	60 Conf. Root = 32768/0/30:f7:0d:7a:ec:84 Cost = 0 Port = 0x8001
1	24 12.06936200(10.20.164.22	192.164.87.9	SNMP	120 get-request 1.3.6.1.2.1.25.3.2.1.5.1 1.3.6.1.2.1.25 3.5.1.1.1 1.3.6.1.2.1.
	2514.03733500(cisco_7a;ec:84	Spanning-tree-(for-br	STP	60 Conf. Root = 32768/0/30:f7:0d:7a:ec:84 Cost = 0 Port = 0x8001
	2616.03704300(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 18.03657200(cisco_7a:ec:84	Spanning-tree-(for-br	STP	60 Conf. Root = 32768/0/30:f7:0d:7a:ec:84 Cost = 0 Port = 0x8001
	28 19.75046200(10.20.164.22	70.42.128.171	TCP	66 62423 > https [SYN] Seg=0 Win=8192 Len=0 MSS=1260 WS=4 SACK_PERM=1
	29 19. 8104 5200(70. 42. 228. 171	10.20.164.22	TCP	66 https > 62423 [SYN, ACK] Seq=0 Ack=1 Win=5840 Len=0 MSS=1260 SACK_PERM=1 W
	30 19, 81054600(10, 20, 164, 22	70, 42, 28, 171	TCP	54 62423 > https [ACK] Seg=1 Ack=1 win=66780 Len=0

Step 3: Filter Wireshark to display only ICMP traffic.

You can use the filter in Wireshark to block visibility of unwanted traffic. The filter does not block the capture of unwanted data; it only filters what to display on the screen. For now, only ICMP traffic is to be displayed.

In the Wireshark **Filter** box, type **icmp**. The box should turn green if you typed the filter correctly. If the box is green, click **Apply** to apply the filter.

Filter:	icmp	Expression Clear Apply Save
---------	------	-----------------------------

Step 4: From the command prompt window, ping the default gateway of your PC.

From the command window, ping the default gateway using the IP address that you recorded in Step 1.

Step 5: Stop capturing traffic on the NIC.

Click the **Stop Capture** icon to stop capturing traffic.



Step 6: Examine the first Echo (ping) request in Wireshark.

The Wireshark main window is divided into three sections: the Packet List pane (top), the Packet Details pane (middle), and the Packet Bytes pane (bottom). If you selected the correct interface for packet capturing in Step 3, Wireshark should display the ICMP information in the Packet List pane of Wireshark, similar to the following example.

1	ntel(R) 82	577LN	1 Gigab	it Netwo	ork Co	rnecti	ion: \De	vice\N	PF_{6L	79E09	3-A44	7-4EC	8-81DF-5	E22D08A6	F63) [V	Viresh	ark 1.8.3	(SVN R	ev 45255 from	/trunk-1.	8)]			-		
Eile	Edit	View	Go	Capture	Ana	alyze	Statisti	cs Te	lepho	ny]	Tools	Inter	mals <u>H</u> e	elp												
	.	-			X	2	81	0, 4	•	4	Ŧ	2			20			¥ 8	* 3							
Filte	er: icmp											•	Expression	n Clear	Apply	Sav	/e									
802.1	1 Chann	el:	Chan	nel Offse	st: -	FCS	Filter: A	II Fram	nes		~ No	one	• V	/ireless Set	tings	Decr	ption k	eys								
No.	Т	ime		Sour	ce				Det	inatio	n			Protoco	I Len	gth	Info									
	9 9	9.601	.8270	00 10.	20.1	.64.2	2		10.	20.	164.	17		ICMP		74	Echo	(ping) request	id=0)	<0001,	, se	q=37/	9472,	ttl	=128
	10 9	9.602	8070	00 10.	20.1	.64.1	.7		10.	20.	164.	22		ICMP		74	Echo	(ping) reply	id=0)	(0001,	, se	q=37/	9472,	tt	=255
	12 1	0.60	418/	00(10.	20.1	.64.2	2		10.	20.	164.	1/	Ton	ICMP		74	Echo	(ping) recuest	10=0)	(0001,	, se	q=38/	9/28,	tt	=128
	14 1	1 60	0/28	00(10.	20.1	64.1	./		10.	20.	164.	17	TOP	ICMP		74	Echo	(ping) reply	10=0)	,0001	, se	q=38/	9/28,	tt	=255
	14 1	1.60	01 77	00(10.	20.1	64.2	2		10.	20.	164.	1/		TCMP		74	Echo	(ping) request	10=0)	,0001	, se	q=39/	9984,	tti	=128
	17 1	2 61	0258	00(10.	20.1	64.1	22		10.	20.	164	17		TCMP		74	Echo	(ping) recuest	id=0	0001	, 50	q=39/	10740		1_128
	18 1	2.61	1318	00(10.	20.1	64.1	7		10.	20	164	22		TCMP		74	Echo	(ping) renly	id=0	0001	SP	q=40/	10240		1=255
-	10.		1910						201	2011	2041						Leno	(pring	, , ch , ì	10-01	, obout,	,	9-10/	101-10		
1					_		_	_	_	_																
-		. 7	hum			. / 5/			74 6				ad (107	hine			6			_						
	rame s	9: 74	byt	es on	wire 1 24	2 ():	50 (I	.5),	14 0	ytes	cap		20 (392	DILS)	on I	iter	ace	00.77	05.84)							
	nterne	at Dr	otor	al ver	sion	+. 2a.	500 (3	10.20	0 16	4 .2	a. 00	20	164 27	Det	· 10	1 0 1	64 17	(10 2	0 16/ 17							
(H) (H)	nterne	ot Co	ottoo	1 Mess	ane	Prot	tocol	10.2	0.10	4.22	. (10			., 030	. 10	20.1	04.17	(10.2	0.104.17,							
	incer in		ATCI O	i ness	uge		LOCOT					- 1	MIDUL	e												
000	0 30	f7 0	d 7a	ec 84	SC	26	0a 24	Za (50 CE	8 00	45	00	0z.	.\& . \$'												
001	0 00	3C 1 11 0	8 00	4d 36	00	01	00 25	61 (14 84 62 61	3 64	65	66	. < M	6. %	bcdef											
003	0 67	68 6	9 6a	6b 6c	6d	6e	6f 70	71	72 7	3 74	75	76	ghijk	Imn opo	rstu											
004	0 77	61 6	2 63	64 65	66	67	68 69						wabcd	lefg hi												
												E	Botto	m												

- a. In the Packet List pane (top section), click the first frame listed. You should see **Echo (ping) request** under the **Info** heading. This should highlight the line blue.
- b. Examine the first line in the Packet Details pane (middle section). This line displays the length of the frame; 74 bytes in this example.
- c. The second line in the Packet Details pane shows that it is an Ethernet II frame. The source and destination MAC addresses are also displayed.

What is the MAC address of the PC's NIC?

What is the default gateway's MAC address?

d. You can click the plus (+) sign at the beginning of the second line to obtain more information about the Ethernet II frame. Notice that the plus sign changes to a minus (-) sign.

What type of frame is displayed?

e. The last two lines displayed in the middle section provide information about the data field of the frame. Notice that the data contains the source and destination IPv4 address information.

What is the source IP address?

What is the destination IP address?

f. You can click any line in the middle section to highlight that part of the frame (hex and ASCII) in the Packet Bytes pane (bottom section). Click the **Internet Control Message Protocol** line in the middle section and examine what is highlighted in the Packet Bytes pane.



What do the last two highlighted octets spell?

g. Click the next frame in the top section and examine an Echo reply frame. Notice that the source and destination MAC addresses have reversed, because this frame was sent from the default gateway router as a reply to the first ping.

What device and MAC address is displayed as the destination address?

Step 7: Restart packet capture in Wireshark.

Click the **Start Capture** icon to start a new Wireshark capture. You will receive a popup window asking if you would like to save the previous captured packets to a file before starting a new capture. Click **Continue** without Saving.



Step 8: In the command prompt window, ping www.cisco.com.

Step 9: Stop capturing packets.



Step 10: Examine the new data in the packet list pane of Wireshark.

In the first echo (ping) request frame, what are the source and destination MAC addresses?

Source:

Destination:

What are the source and destination IP addresses contained in the data field of the frame?

Source:

Destination:

Compare these addresses to the addresses you received in Step 7. The only address that changed is the destination IP address. Why has the destination IP address changed, while the destination MAC address remained the same?

Reflection

Wireshark does not display the preamble field of a frame header. What does the preamble contain?