Laboratorium - Wykorzystanie programu Wireskark do badania ramek Ethernetowych

Topologia



Cele

Część 1: Badanie pól nagłówka w ramce Ethernet II.

Cześć 2: Użycie programu Wireshark do przechwycenia i analizy ramek Ethernetowych.

Tło / Scenariusz

Kiedy wyższe warstwy komunikują się między sobą, dane przechodzą w dół warstw modelu OSI (Open Systems Interconnection) i ostatecznie są enkapsulowane w ramkę warstwy 2. Budowa ramki jest zależna od technologii dostępu do medium. Na przykład jeśli protokołami warstw wyższych są TCP oraz IP, a technologia dostępu do mediów to Ethernet, wtedy metodą enkapsulacji w warstwie 2 będzie Ethernet II. Sytuacja ta jest typowa dla środowisk sieci lokalnych LAN.

W czasie poznawania sposobu działania warstwy 2, bardzo przydatne jest przeanalizowanie informacji zawartych w nagłówku ramki. W pierwszej części tego laboratorium będziesz przypominał sobie pola znajdujące się w ramce Ethernet II. W drugiej części użyjesz programu Wireshark do przechwycenia i analizy pól ramki typu Ethernet II dla ruchu lokalnego i zdalnego.

Wymagane wyposażenie

• 1 PC (Windows 7, Vista lub XP z dostępem do Internetu z zainstalowanym programem Wireshark)

Część 1. Badanie pól nagłówka ramki Ethernet II

W części 1 będziesz badał pola i ich zawartość w nagłówku ramki Ethernet II. Do tego celu zostaną użyte dane przechwycone w Wireshark.

Krok 1.	Przejrzyj	opisy i	długości	pól nagłówka	ramki typu	Ethernet II.
---------	-----------	---------	----------	--------------	------------	--------------

Adres		Adres	Typ	Dane	FCS (suma	
Preambuła docelowy		źródłowy	ramki		kontrolna)	
8 bajtów	6 bajtów	6 bajtów	2 bajty	46 – 1500 bajtów	4 bajty	

Krok 2. Sprawdź konfigurację sieci w komputerze PC.

Adres IP tego komputera PC to 10.20.164.22, a brama domyślna ma adres 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

Krok 3. Zbadaj ramki Ethernetowe w danych przechwyconych w Wireshark.

Widok okna programu Wireshark poniżej przedstawia pakiet wysłany w wyniku komendy ping wykonanej na komputerze PC do bramy głównej. W programie Wireshark zastosowano filtr, aby wyświetlić tylko protokoły ARP oraz ICMP. Sesja rozpoczyna się zapytaniem ARP o adres MAC bramy domyślnej, po którym następuje odpowiedź ARP. W następnym kroku wysyłane jest żądanie ping, na które brama domyślna udziela odpowiedzi. W systemach Windows typowo wykonanie komendy ping skutkuje wysłaniem 4 żądań echo request, na które host docelowy kolejno udziela odpowiedzi.

🗖 I	📶 Intel(R) 82577LM Gigabit Network Connection: \Device\NPF_{6179E093-A447-4EC8-81DF-5E22D08A6F63} [Wireshark 1.8.3 (SVN Rev 45256 from /trunk-1.8)]													
<u>F</u> ile	<u>E</u> dit <u>V</u> iew	<u>Go</u> <u>C</u> apture	<u>A</u> nalyze	<u>Statistics</u>	Telephony <u>T</u>	ools <u>I</u> nte	rnals <u>H</u> elp							
8	1	🕷 🖻 🖡	. X 2) Q	, 🗢 🔿 🖒	7 ₽) 🔍 🖭	¥ (¥ 🖪 (¥ 🛛 🔀			
Filte	er: arp or icm	þ				-	Expression Clear	Apply Save	:					
802.1	802.11 Channel: Channel Offset: FCS Filter: All Frames None Wireless Settings Decryption Keys													
No.	Time	Sou	rce		Destinatio	n	Protocol	Length I	nfo					
	7 9.60	L177000 De	11_24:2;	a:60	Broadca	ast	ARP	42 \	who h	as 10.2	20.164.17	? Tell 10.	20.164.22	
	8 9.60	L803000 Ci	sco_7a:e	ec:84	De11_24	1:2a:60	ARP	60 1	10.20	.164.17	′is at 3	0:f7:0d:7a:	ec:84	
	9 9.60	L827000 10	20.164.	.22	10.20.1	.64.17	ICMP	74 6	Echo	(ping)	request	id=0x0001,	seq=37/9472,	tt]=128
	10 9.60	2807000 10	20.164.	.17	10.20.1	.64.22	ICMP	74 E	Echo	(ping)	reply	id=0x0001,	seq=37/9472,	tt]=255
	12 10.6	0418700(10	.20.164.	.22	10.20.1	.64.17	ICMP	74 E	Echo	(ping)	request	id=0x0001,	seq=38/9728,	tt]=128
	13 10.6	2072800(10	20.164.	.17	10.20.1	.64.22	ICMP	74 6	Echo	(ping)	reply	id=0x0001,	seq=38/9728,	tt]=255
	14 11.6	0719200(10	20.164.	.22	10.20.1	.64.17	ICMP	74 E	Echo	(ping)	request	id=0x0001,	seq=39/9984,	tt]=128
	15 11.6	0817700(10	20.164.	17	10.20.1	.64.22	ICMP	74 E	Echo	(ping)	reply	id=0x0001,	seq=39/9984,	ttl=255
	17 12.6	L025800(10	20.164.	22	10.20.1	.64.17	ICMP	74 6	Echo	(ping)	request	id=0x0001,	seq=40/10240	, ttl=128
	18 12.6	L131800(10	20.164.	17	10.20.1	.64.22	ICMP	74 E	Echo	(ping)	reply	id=0x0001,	seq=40/10240	, ttl=255
•														÷.
	ramo 7 · A	bytes on	wire (226 hite	12 hytes	cantur	ed (336 hits)	on interf	200 0					
	thernet T	Src: De	11 24.2	a:60 (5c)	·26·0a·24·2	a:60)	Dst: Broadcast	(ff·ff·f	f.ff.	ff.ff)				
	Destinat	ion: Broad	cast (f		f.ff.ff)	a.00), i	bit. bioadcase	(
	Source:	nell 24·2a	·60 (5c	·26·0a·24	L·2a·60)									
	Type: AP	(0x0806)	(50											
	ddress Re	alution P	rotocol	(request	-)									
	aar coorke.	Jonachon 1	000001	(i equest	-)									
000 001 002	0 ff ff f 0 08 00 0 0 00 00 0	f ff ff fi 06 04 00 01 00 00 00 00	5c 26 5c 26 0 0a 14	0a 24 2 0a 24 2 a4 11	a 60 08 06 a 60 0a 14	00 01 a4 16	\& .\$*` \& .\$*`							

Krok 4. Badanie zawartości nagłówka ramki typu Ethernet II żądania ARP.

Poniższa tabela zawiera dane z pól nagłówka ramki typu Ethernet II dla pierwszej przechwyconej przez Wireshark ramki.

Laboratorium - Używanie programu Wireshark do badania ramek Ethernet

Pole	Wartość	Opis					
Preambuła	Pominięte	To pole przedstawia bity synchronizujące używane przez kartę sieciową.					
Adres docelowy	Rozgłoszenie (ff:ff:ff:ff:ff:ff)	Adres warstwy drugiej w ramce. Każdy adres ma długość 48 bitów lub 6 oktetów, zapisanych jako 12 cyfr					
Adres źródłowy	Dell_24:2a:60 (5c:26:0a:24:2a:60)	 szesnastkowych, 0-9, A-F. Popularnym formatem zapisu jest 12:34:56:78:9A:BC Pierwsze sześć cyfr wskazuje producenta, ostatnie 6 cyfr i numer seryjny karty sieciowej (NIC). Adresem docelowym może być adres rozgłoszeniowy, któ zawiera same jedynki lub adres transmisji jednostkowej (ang. unicast). Adres źródłowy jest zawsze adresem transmisji jednostkowej (ang. unicast). 					
Typ ramki	0x0806	W ramce typu Ethernet II to pole zawiera szesnastkową wartość, która wskazuje rodzaj protokołu wyższych warstw, którego datagram znajduje się w polu danych. Istnieje wiele protokołów wyższych warstw obsługiwanych przez ramki typu Ethernet II. Dwa z nich to:					
		Wartość Opis					
		0x0800 Protokół IPv4					
		0x0806 Address resolution protocol (ARP)					
Dane	ARP	Zawiera enkaspulowane PDU wyższej warstwy. Pole danych ma rozmiar od 46 do 1500 bajtów.					
FCS	Pominięte	Sekwencja kontrolna ramki (FCS) jest używana przez kartę sieciową do wykrywania błędów powstałych podczas transmisji. Jego wartość jest obliczana i umieszczana w ramce przez urządzenie wysyłające na podstawie zawartości pól: adres ramki, typ i dane. Pole to weryfikowane jest przez odbiorcę.					

Dlaczego wartość pola adresu docelowego jest istotna przy przesyłaniu danych?

Dlaczego PC wysyła rozgłoszenie ARP przed wysłaniem pierwszego żądania ping?

Jaki jest adres MAC źródła w pierwszej ramce?

Jaki jest producent (OUI) źródłowej karty sieciowej (NIC)?

Która część adresu MAC to OUI?

Jaki jest numer seryjny źródłowej karty sieciowej (NIC)? ____

Część 2. Użycie programu Wireshark do przechwycenia i analizy ramek Ethernetowych.

W części 2 użyjesz programu Wireshark, aby przechwycić lokalne i zdalne ramki Ethernetowe. Następnie zbadasz informacje zawarte w polach nagłówków tych ramek.

Krok 1. Określ adres IP bramy domyślnej dla twojego PC.

Otwórz okno linii komend i wykonaj polecenie ipconfig.

Jaki jest adres bramy domyślnej? ____

Krok 2. Rozpocznij przechwytywanie ruchu pojawiającego się na karcie twojego PCta.

- a. Uruchom program Wireshark.
- b. Na pasku narzędziowym Wireshark kliknij ikonę Interface List (Lista interfejsów).



c. W programie Wireshark w oknie Capture Interfaces wybierz odpowiedni interfejs w celu rozpoczęcia przechwytywania ruchu i następnie kliknij **Start**. Jeśli nie jesteś pewny, który interfejs wybrać, kliknij **Details** dla uzyskania dodatkowych informacji o interfejsach, które znajdują się na liście.

🗖 Wireshark: Cap	oture Interfaces				• •
	Description	IP	Packets	Packets/s	
🔲 🛃 Sun		fe80::50e4:c3e6:b635:a999	26	0	Details
🕜 🗩 Intel(R)	82577LM Gigabit Network Connection	fe80::b875:731b:3c7b:c0b1	95	1	<u>D</u> etails
Help	<u>Start</u>	S <u>t</u> op	<u>O</u> ption	s	<u>C</u> lose

d. Obserwuj ruch, który pojawi się w oknie Packet List.

Filter:	▼ Expression Clear Apply Save											
802.11	Channel: 💌 Channel Offset: 💌 FCS Filter: 🗛	Il Frames Vone	• Wireless Settir	ngs Decryption Keys								
No.	Time Source 18 10.40268/00(184.2/.190.41	Destination 10.20.104.22	Protocol	Length Info bU NTTPS > b24U8 [ACK] SEQ=1 ACK=1163 W1N=43412 LEN=U								
	19 10.60449100(184.27.190.41	10.20.164.22	TLSV1	587 Application Data								
	20 10.80121900(10.20.164.22	184.27.190.41	TCP	54 62408 > https [ACK] Seq=1163 ACk=534 Win=16695 Len=0								
	21 11.04927800(10.20.164.22	10.20.164.31	NBNS	92 Name query NB HP094B61<00>								
	22 11.79926500(10.20.164.22	10.20.164.31	NBNS	92 Name query NB HP094B61<00>								
	23 12.03732100(cisco_7a:ec:84	Spanning-tree-(for	-br:STP	60 Conf. Root = 32768/0/30:f7:0d:7a:ec:84 Cost = 0 Port = 0x8001								
	24 12.06936200(10.20.164.22	192.168.87.9	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 1.3.6.1.2.1.2								
	25 14.03733500(cisco_7a:ec:84	Spanning-tree-(for	-br:STP	60 Conf. Root = 32768/0/30:f7:0d:7a:ec:84 Cost = 0 Port = 0x8001								
	26 16.03704300(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	70.42.228.171	TCP	66 62423 > https [SYN] Seq=0 win=8192 Len=0 MSS=1260 wS=4 SACK_PERM=1								
	29 19.81045200(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 WS								
	30 19.81054600(10.20.164.22	70.42.228.171	TCP	54 62423 > https [ACK] Seq=1 Ack=1 Win=66780 Len=0								

Krok 3. Przefiltruj zawartość okna Wireshark, tak aby pokazywał tylko ruch ICMP.

W celu zablokowania wyświetlania niechcianego ruchu w programie Wireshark można użyć filtrów. Filtr nie blokuje przechwytywania niechcianych danych, a tylko zapobiega ich wyświetlaniu. W tym przypadku ma być wyświetlony tylko ruch ICMP.

W polu **Filter** programu Wireshark wpisz **icmp**. Jeśli wpiszesz poprawną wartość w polu filtr, pole to będzie miało zielone tło. Jeśli pole jest zielone kliknij **Apply** w celu zastosowania filtrowania.

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

Krok 4. Używając okna linii komend komputera wydaj komendę ping do bramy domyślnej.

Używając okna linii komend wykonaj ping do bramy domyślnej używając adresu IP, który odczytałeś w kroku 1.

Krok 5. Zatrzymaj przechwytywanie ruchu na karcie sieciowej (NIC).

Kliknij ikonę Stop Caputre w celu zatrzymania przechwytywania ruchu.



Krok 6. Przeanalizuj w Wireshark pierwsze żądanie echa (ping).

Główne okno Wireshark podzielone jest na trzy sekcje: panel Packet List (na górze), panel Pacekt Details (po środku) i panel Packet Bytes (na dole). Jeśli wybrałeś właściwy interfejs dla przechwytywania ruchu w kroku 3, Wireshark powinien pokazywać informacje dotyczące ICMP w panelu Packet List, tak jak na poniższym przykładzie.

🗖 Int	🛛 Intel(R) 82577LM Gigabit Network Connection: \Device\NPF_{6179E093-A447-4EC8-81DF-5E22D08A6F63} [Wireshark 1.8.3 (SVN Rev 45256 from /trunk-1.8)]													x						
<u>F</u> ile	<u>E</u> dit <u>V</u> iew	<u>G</u> o <u>C</u> a	pture <u>A</u>	nalyze	$\underline{S} tatistics$	Telephor	<u>y T</u> ools	Inter	rnals <u>H</u> el	р										
	M @ 0	(💓 E	3 🗔 3	× 2		、 🔶 🏟	۵ 🖗	₽) ⊕, ∈		m 🖉	Y	1	¥ 🛛					
Filter	icmp							•	Expression	Clear	Apply	Save								
802.11	802.11 Channel: Channel Offset: FCS Filter: All Frames Vone Vireless Settings Decryption Keys																			
No.	Time		Source			Desti	nation			Protocol	Leng	th Info								
	9 9.60	01827000	10.20	.164.2	2	10.	20.164.	17		ICMP		74 Echo	o (pi	ing)	request	id=0x0001,	seq=37/	9472,	tt]=12	8
	10 9.60	2807000	10.20	.164.1	.7	10.	20.164.	22		ICMP		74 Echo	o (pi	ing)	reply	id=0x0001,	seq=37/	9472,	tt]=25	5
	12 10.6	50418700	(10.20	.164.2	2	10.	20.164.	17	Ton	ICMP		74 Echo	o (pi	ing)	request	id=0x0001,	seq=38/	9728,	tt]=12	28
	13 10.6	52072800	(10.20	.164.1	.7	10.	20.164.	22	TOP	ICMP		74 Echo	o (pi	ing)	reply	id=0x0001,	seq=38/	9728,	ttl=25	5
	14 11.6	50719200	(10.20	.164.2	2	10.	20.164.	17		ICMP		74 Echo	o (pi	ing)	request	id=0x0001,	seq=39/	9984,	ttl=12	28
	15 11.6	60817700	(10.20)	.164.1	.7	10.	20.164.	22		ICMP		74 Echo	o (pi	ing)	reply	id=0x0001,	seq=39/	9984,	tt I=25	5
	1/ 12.0	01025800	(10.20)	.164.2	2	10.	20.164.	1/		ICMP		74 ECho	o (pi	ing)	request	1d=0x0001,	seq=40/	10240,	ttl=1	.28
_	18 12.0	01131800	(10.20)	.164.1	./	10.	20.164.	22		ICMP		74 ECNC	o (pi	ing)	reply	1d=0x0001,	seq=40/	10240,	ττ I=2	:55
•																				÷.
	amo 0 • 7	1 hut or	on wi	ro (50	02 hite) 74 h	the ca	ntur	ad (502	hite) (on in	torfaco	0							_
	hernet 1	T She	Dell	24.22	•60 (5c	·26·0a·2	4.22.6	0) r	nst: Cie	500 72.0		(30.f7	•0d•3	72.00	- • 84)					
	ternet P	protocol	Versi	on 4	Src: 10	0 20 164	22 (1	0 20	164 22) Dst	10 2	0 164 1	7 (10	20	164 17)					
Tr	ternet (ontrol	Messad	e Prot	tocol		(1		A. 1.11	,,	2012									
									MIDDIE	9										
L																				
0000 0010 0020 0030 0040	0000 30 f7 0d 7a ec 84 5c 26 0a 24 2a 60 08 00 45 00 0z\& .\$*`E. 0010 00 3c 19 b3 00 00 80 01 c4 be 0a 14 a4 16 0a 14																			
								E	Bottor	n										

- a. W panelu Packet List (górna część) kliknij pierwszą ramkę na liście. Powinieneś widzieć żądanie echa (ping) poniżej nagłówka Info. Klikniecie powinno podświetlić linię na niebiesko.
- b. Zbadaj pierwszą linijkę w panelu Packet Details (środkowa sekcja). Linia ta określa długość ramki, w tym przykładzie wynosi ona 74 bajty.
- c. Druga linia w panelu Packet Details pokazuje, że jest to ramka typu Ethernet II. Widoczne są również adresy MAC źródłowy i docelowy.

Jaki jest adres MAC karty sieciowej PCta?

Jaki jest adres MAC bramy domyślnej?

d. Możesz kliknąć znak plus (+) na początku drugiej linii w celu wyświetlenia większej ilości informacji o ramce Ethernet II. Zauważ, że po kliknięciu znak plus zmienia się na minus (-).

Jaki typ danych wyższej warstwy zawarty jest w ramce?

e. Ostatnie dwie linie pokazane w części środkowej pokazują zawartość pola danych ramki. Zauważ, że dane zawierają źródłowy i docelowy adres IPv4.

Jaki jest źródłowy adres IP? _____

Jaki jest docelowy adres IP? _____

f. Możesz kliknąć dowolną linię w części środkowej okna w celu podświetlenia odpowiadającej jej części ramki przedstawionej szesnastkowo lub ASCII w panelu Packet Bytes (dolna sekcja). Kliknij linię Internet Control Message Protocol w środkowej części i zbadaj co zostanie podświetlone w panelu Packet Bytes.

B Frame 7: 74 bytes on wire (592 bits), 74 bytes captured (592 bits) on interface 0 B Ethernet II, Src: Dell_24:2a:60 (5c:26:0a:24:2a:60), Dst: Cisco_7a:ec:84 (30:f7:0d:7a:ec:84)									
Internet Protocol Version 4, Src: 10.20.164.22 (10.20.164.22), Dst: 10.20.164.17 (10.20.164.17)									
Internet Control Message Protocol									
code o									
Checksum: 0x4d4e [correct]	-								
	_								
0000 30 17 0d 7a ec 84 5c 26 0a 24 2a 60 08 00 45 00 0.z\& S*E. 0010 00 3c 03 48 00 00 80 01 db 29 0a 14 at 16 0a 14									
0020 a4 11 08 00 4d 4e 00 01 00 0d 61 62 63 64 65 66									
0030 7 6 6 9 6 4 6 6 6 7 6 8 6 9									

Jaką zawartość mają dwa ostanie oktety? _____ i

g. Kliknij następną ramkę w górnej części okna i zbadaj ramkę odpowiedzi na żądanie echa. Zauważ, że adresy MAC źródłowy i docelowy zostały zamienione miejscami, ponieważ ta ramka była wysłana z bramy domyślnej jako odpowiedź na pierwszy ping.

Adres MAC jakiego urządzenia jest wyświetlony jako adres docelowy?

Krok 7. Uruchom ponownie przechwytywanie pakietów w Wireshark.

Kliknij ikonę **Start Capture**, aby uruchomić nowe przechwytywanie pakietów. Pojawi się wyskakujące okienko z pytaniem czy chcesz zapisać do pliku poprzednio przechwycone dane przed rozpoczęciem nowego przechwytywania. Kliknij **Continue without Saving** (Kontynuuj bez zapisania).



- Krok 8. W oknie linii komend PC wydaj komendę: ping www.cisco.com.
- Krok 9. Zatrzymaj przechwytywanie pakietów.



Krok 10. Zbadaj nowe dane w panelu Packet list.

Jaki jest adres MAC źródłowy i docelowy w pierwszej ramce żądania echa (ping)?

Źródło: ______.

Docelowy: _____

Jakie adresy IP źródłowy i docelowy znajdują się w polu danych ramki?

Źródło: _____

Docelowy:

Porównaj te adresy z adresami, które poznałeś w kroku 7. Jedynym adresem, który się zmienił jest docelowy adres IP. Dlaczego zmienił się docelowy adres IP, podczas gdy docelowy adres MAC pozostał ten sam?

Do przemyślenia

Wireshark nie pokazuje pola preambuła z nagłówka ramki. Co zawiera pole preambuła?