実習 - Wireshark を使用してイーサネット フレームを確認する

トポロジ



目的

パート 1: イーサネット II フレームのヘッダー フィールドを調べる

パート 2: Wireshark を使用して、イーサネット フレームをキャプチャおよび分析する

背景/シナリオ

上位層プロトコルが相互に通信する場合、データフローは OSI(Open Systems Interconnection)の階層を下り、レイヤ2フレームにカプセル化されます。フレーム構成はメディア アクセス タイプによって異なります。たとえば、上位層 プロトコルが TCP と IP であり、メディア アクセスがイーサネットである場合、レイヤ2フレームのカプセル化はイーサ ネット II になります。これは LAN 環境では標準的なものです。

レイヤ 2 の概念について学習するとき、フレーム ヘッダーの情報を分析すると役に立ちます。この実習の最初のパートでは、イーサネット II フレームに含まれるフィールドを確認します。パート 2 では、Wireshark を使用して、ローカルトラフィックとリモートトラフィックのイーサネット II フレーム ヘッダー フィールドをキャプチャおよび分析します。

実習に必要なリソースや機器

 PC1台(インターネットを利用でき、Wireshark がインストールされている Windows 7、Vista、または XP が搭載 されているもの)

パート 1: イーサネット II フレームのヘッダー フィールドを調べる

パート 1 では、イーサネット II フレームのヘッダー フィールドと内容を調べます。これらのフィールドの内容を調べるには、Wireshark のキャプチャを使用します。

手順 1: イーサネット II ヘッダー フィールドの記述と長さを確認します。

プリアンブル	宛先 アドレス	送信元 アドレス	フレーム タイプ	データ	FCS
8 バイト	6 バイト	6 バイト	2 バイト	46 ~ 1500 バイト	4 バイト

手順 2: PC のネットワーク設定を確認します。

この PC ホストの IP アドレスは 10.20.164.22、デフォルト ゲートウェイの IP アドレスは 10.20.164.17 です。

イーサネット アダプター ローカル エリア接続: 接続固有の DNS サフィックス . . . : cisco.com リンクローカル IPv6 アドレス. . . . : fe80::4dbf:6d59:f81d:8030%11 IPv4 アドレス 10.20.164.22 サブネット マスク 255.255.255.0 デフォルト ゲートウェイ 10.20.164.17

手順 3: Wireshark のキャプチャでイーサネット フレームを調べます。

Wireshark による次のキャプチャでは、PC ホストからデフォルト ゲートウェイに対して発行された ping によって生成 されたパケットが示されています。Wireshark には、ARP および ICMP プロトコルだけを表示するようにフィルタが適 用されています。セッションはゲートウェイ ルータの MAC アドレスの ARP クエリーで開始し、その後、ping 要求と応 答が 4 回行われます。

📕 In	🙍 Intel(R) PRO/1000 MT Network Connection [Wireshark 1.10.0 (SVN Rev 49790 from /trunk-1.10)]												
Eile	Eile Edit <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 <u>I</u> nternals <u>H</u> elp												
0	◉ ◉ ◢ ■ ∅ ⊨ ≞ ೫ ₴ ⇔ ⇒ ⊋ 7 ⊉ 目目 Q Q Q ⊡ ₩ ⊠ № №												
Filter	Filter: arp or icmp Expression Clear Apply Save												
802.11 Channel: 🔽 Channel Offset: 🔽 FCS Filter: All Frames 💌 None 🔍 Wireless Settings Decryption Keys													
No.	Time	Source	Destination	Protocol	Length Info								
	7 9.601177	'000 Dell_24:2a:6	i0 Broadcast	ARP	42 Who has	10.20.164.17	? Tell 10.	20.164.22					
	8 9.60180	3000 cisco_7a:ec:	84 Dell_24:2a:	60 ARP	60 10.20.16	4.17 is at 3	0:f7:0d:7a:	ec:84					
	9 9.601827	7000 10.20.164.22	10.20.164.1	7 ICMP	74 Echo (pi	ng) request	id=0x0001,	seq=37/9472,	tt]=128				
	10 9.602807	000 10.20.164.17	10.20.164.2	2 ICMP	74 Echo (pi	ng) reply	id=0x0001,	seq=37/9472,	ttl=255				
	12 10.60418	3700(10.20.164.22	10.20.164.1	7 ICMP	74 Echo (pi	ng) request	id=0x0001,	seq=38/9728,	tt]=128				
	13 10.62072	2800(10.20.164.17	10.20.164.2	2 ICMP	74 Echo (pi	ng) reply	id=0x0001,	seq=38/9728,	tt]=255				
	14 11.60719	200(10.20.164.22	10.20.164.1	7 ICMP	74 Echo (pi	ng) request	id=0x0001,	seq=39/9984,	tt]=128				
	15 11.60817	700(10.20.164.17	10.20.164.2	2 ICMP	74 Echo (pi	ng) reply	id=0x0001,	seq=39/9984,	tt1=255				
	17 12.6102	5800(10.20.164.22	10.20.164.1	7 ICMP	74 Echo (pi	ng) request	id=0x0001,	seq=40/10240	, ttl=128				
	18 12.61131	1800(10.20.164.17	10.20.164.2	2 ICMP	74 Echo (pi	ng) reply	id=0x0001,	seq=40/10240	, ttl=255				
< _			III						- F				
E E	ame 7: 42 by	tes on wire (33)	5 bits), 42 bytes capt	ured (336 bits) o	on interface 0								
	thernet II.	src: Dell 24:2a:0	50 (5c:26:0a:24:2a:60)	. Dst: Broadcast	(ff:ff:ff:ff:ff:	(ff)							
(F)	Destination	Broadcast (ff:	f:ff:ff:ff:ff)	,									
	Source: Dell	24:2a:60 (5c:20	5:0a:24:2a:60)										
-	Type: ARP ((x0806)	,										
+ A	ddress Resolu	ition Protocol (request)										
0000 0010 0020	08 00 06 0 00 00 00 0	f ff ff 5c 26 0 4 00 01 5c 26 0 0 00 00 0a 14 a	a 24 2a 60 08 06 00 0 a 24 2a 60 0a 14 a4 1 4 11	1 6\& .\$*` \& .\$*`									

手順 4: ARP 要求のイーサネット II ヘッダーの内容を調べます。

次の表は、Wireshark キャプチャの最初のフレームでの、イーサネット II ヘッダー フィールドのデータを示したものです。

フィールド	值	説明
プリアンブル	キャプチャには非表示	このフィールドには、NIC ハードウェアで処理される同期ビットが 含まれます。
宛先アドレス	ブロードキャスト (ff:ff:ff:ff:ff:ff)	フレームのレイヤ2アドレス各アドレスは長さが48ビット(6オク テット)で、12桁の16進数(0 ~ 9、A ~ F)で表されます。
送信元アドレス	Dell_24:2a:60 (5c:26:0a:24:2a:60)	一般的な形式は、12:34:56:78:9A:BC です。 最初の6桁の16進値はネットワークインターフェイスカード (NIC)の製造元を表し、最後の6桁の16進値はNICのシリア ル番号です。 宛先アドレスは、ブロードキャスト(すべて1)またはユニキャスト の場合があります。送信元アドレスは常にユニキャストです。
フレーム タイプ	0x0806	イーサネット II フレームの場合、このフィールドには、データ フィールドの上位層プロトコルの種類を示すために使用される 16 進数値が含まれます。イーサネット II ではさまざまな上位層 プロトコルがサポートされています。一般的な 2 つのフレーム タ イプを次に示します。 値 説明 0x0800 IPv4 プロトコル 0x0806 アドレス解決プロトコル(ARP)
データ	ARP	カプセル化された上位プロトコルが含まれます。 データ フィール ドは 46 ~ 1,500 バイトの間です。
FCS	キャプチャには非表示	送信中のエラーを識別するために NIC によって使用されるフ レーム チェック シーケンスです。 値は、送信元マシンによって計 算され、フレーム アドレス、タイプ、データ フィールドなどを含み ます。これは、受信側によって検証されます。

宛先アドレス フィールドの内容については何が重要ですか。

PC が最初の ping 要求を送信する前にブロードキャスト ARP を送信するのはなぜですか。

最初のフレームでの送信元の MAC アドレスは何ですか。______

送信元の NIC のベンダー ID(OUI)は何ですか。_____

MAC アドレスのどの部分が OUI ですか。

送信元の NIC のシリアル番号は何ですか。______

パート 2: Wireshark を使用して、イーサネット フレームをキャプチャおよび分析 する

パート 2 では、Wireshark を使用してローカルおよびリモートのイーサネット フレームをキャプチャします。その後、フレーム ヘッダーのフィールドに含まれる情報を調べます。

手順 1: PC のデフォルト ゲートウェイの IP アドレスを特定します。

コマンド プロンプト ウィンドウを開き、ipconfig コマンドを発行します。

PC のデフォルト ゲートウェイの IP アドレスは何ですか。_____

手順 2: PC の NIC でトラフィックのキャプチャを開始します。

- a. Wireshark を開きます。
- b. Wireshark の [Network Analyzer] ツールバーで、[Interface List] アイコンをクリックします。



c. [Wireshark: Capture Interfaces] ウィンドウで、適切なチェックボックスをオンにしてインターフェイスを選択し、
 [Start] をクリックしてトラフィックのキャプチャを開始します。確認するインターフェイスが不明の場合は、
 [Details] をクリックしてリストされている各インターフェイスに関する詳細情報を表示します。

📕 Wiresh	rk: Capture Interfaces			• 🗙
	Description IP	Packets	Packets/s	
	un fe80::50e4:c3e6:b635:a999	26	0	Details
	ntel(R) 82577LM Gigabit Network Connection fe80::b875:731b:3c7b:c0b1	. 95	1	<u>D</u> etails
<u>H</u> elp	<u>Start</u>	<u>O</u> ption	s	<u>C</u> lose

d. [Packet List] ウィンドウに表示されるトラフィックを監視します。

Filter:		 Expression 	Clear A	Apply Save
802.11	Channel: Channel Offset: FCS Filter: All Fra	ames Vone Wire	ess Setting	gs Decryption Keys
No.	Time Source	Destination P	rotocol	Length Info
	18 10.40268/00(184.2/.190.41	10.20.164.22	CP	00 NTTPS > 62408 [ACK] Seq=1 ACK=1163 W1N=43412 Len=0
	19 10.60449100(184.27.190.41	10.20.164.22 1	LSV1	587 Application Data
	20 10.80121900(10.20.164.22	184.27.190.41 1	CP	54 62408 > https [ACK] Seq=1163 Ack=534 Win=16695 Len=0
	21 11.04927800(10.20.164.22	10.20.164.31 N	IBNS	92 Name query NB HP094B61<00>
	22 11.79926500(10.20.164.22	10.20.164.31 N	IBNS	92 Name query NB HP094B61<00>
	23 12.03732100(cisco_7a:ec:84	Spanning-tree-(for-br:S	TP	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	NMP	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:S	TP	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-bris	TP	60 Conf. Root = 32768/0/30:f7:0d:7a:ec:84
	27 18.03657200(cisco_7a:ec:84	Spanning-tree-(for-bris	TP	60 Conf. Root = 32768/0/30:f7:0d:7a:ec:84
	28 19.75046200(10.20.164.22	70.42.228.171 1	CP	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 1	CP	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 1	CP	54 62423 > https [ACK] Seq=1 Ack=1 Win=66780 Len=0

手順 3: ICMP トラフィックだけが表示されるように Wireshark をフィルタします。

Wireshark のフィルタを使用して、不要なトラフィックの表示を遮断できます。フィルタを使用しても不要なデータのキャ プチャはブロックされず、画面に表示されなくなるだけです。ここでは、ICMP トラフィックだけを表示します。

Wireshark の [Filter] ボックスに、「icmp」と入力します。フィルタを正しく入力すると、ボックスが緑になります。ボックスが緑になったら、[Apply] をクリックしてフィルタを適用します。

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

手順 4: コマンド プロンプト ウィンドウで、PC のデフォルト ゲートウェイに ping を実行します。

コマンド ウィンドウから、手順1 で記録した IP アドレスを使用してデフォルト ゲートウェイに ping を発行します。

手順 5: NIC でのトラフィックのキャプチャを停止します。

[Stop Capture] アイコンをクリックして、トラフィックのキャプチャを停止します。



手順 6: Wireshark で最初のエコー(ping)要求を確認します。

Wireshark のメイン ウィンドウは、パケット リスト ペイン(上部)、パケット詳細ペイン(中央)、パケット バイト ペイン(下部)の3 セクションに分かれています。手順3 でパケット キャプチャの対象に正しいインターフェイスを選択した場合、 Wireshark のパケット リスト ペインには次の例のような ICMP 情報が表示されます。

🗖 Int	el(R) 82577LM Giga	bit Network (Connecti	on: \Device\	NPF_{6179E0	93-A447	-4EC8-81DF-5	E22D08A6F6	53} [Wire	shark 1.8.3	(SVN Rev	45256 from /	/trunk-1.8)]	_	
<u>F</u> ile	<u>E</u> dit <u>V</u> iew <u>G</u> o	Capture A	nalyze	Statistics	Telephony	<u>T</u> ools	Internals <u>H</u> e	lp							
				8 Q	🔶 🏟 🗳) 🚡 🗄] ⊕,∈		9 🕰	M 🛃 🖇	% 🔯			
Filter	icmp						▼ Expressio	n Clear	Apply 3	Save					
802.11	Channel: Char	nnel Offset:	- FCS	Filter: All Fra	ames	- Nor	ne 🔻 V	/ireless Setti	ngs De	cryption k	leys				
No.	Time	Source			Destinati	on		Protocol	Length	Info					
	9 9.6018270	000 10.20	.164.2	2	10.20.	164.1	7	ICMP	7	'4 Echo	(ping)	request	id=0x0001,	seq=37/9472,	tt]=128
	10 9.6028070	000 10.20	.164.1	7	10.20.	164.2	2	ICMP	7	'4 Echo	(ping)	reply	id=0x0001,	seq=37/9472,	ttl=255
	12 10.604187	700(10.20	.164.2	2	10.20.	164.1	⁷ ⊢ ± R	ICMP	7	4 Echo	(ping)	request	id=0x0001,	seq=38/9728,	tt]=128
	13 10.620728	800(10.20	.164.1	7	10.20.	164.2		ICMP	7	4 Echo	(ping)	reply	id=0x0001,	seq=38/9728,	tt1=255
	14 11.60/19/	200(10.20	.164.2	2	10.20.	164.1	/	ICMP		4 ECNO	(ping)	request	1d=0x0001,	seq=39/9984,	tt1=128
	15 11.6081//	/00(10.20	164.1	/	10.20.	164.2	2	TCMP		4 ECho	(ping)	reply	1d=0x0001,	seq=39/9984,	ttl=255
	1/ 12.010258	800(10.20	164.2	2	10.20.	164.1	2	TCMP		4 ECho	(ping)	request	1d=0x0001,	seq=40/10240	, TTI=128
-	10 12.011510	BUU(10.20	.104.1	/	10.20.	104.2	2	TCMB	1	4 ECHO	(ping)	герту	10=0x0001,	Seq=40/10240	, LLI=200
٩ 📖															r
🗄 Fr	ame 9: 74 byt	tes on wi	re (59	2 bits),	, 74 byte	s capt	ured (592	bits)	on inte	rface	0				
🕀 Et	hernet II, Sr	rc: Dell_	24:2a:	60 (5c:2	26:0a:24:	2a:60)), Dst: Ci	sco_7a:	ec:84 (30:f7:	Od:7a:ed	::84)			
+ In	ternet Proto	col Versi	on 4,	Src: 10.	20.164.2	2 (10.	20.164.22), Dst:	10.20.	164.17	(10.20.	164.17)			
+ In	iternet Contro	ol Messag	e Prot	:0C01			中央								
0000 0010 0020 0030 0040	300 30 f7 0d 7a ec 84 5c 26 0a 24 2a 60 08 00 00 .c.,\& .\$*`.E. 0010 00 3c 19 b3 00 00 12 at 16 0a 14 .c.,.\& .\$*`E. 0200 at 11 08 00 10 02 56 62 63 64 65 66 M6 M6 <td< td=""></td<>														
							下部								

- a. パケット リスト ペイン(上部セクション)で、表示されている最初のフレームをクリックします。[Info] の見出しの下 に、Echo (ping) request と表示されます。行が青で強調表示されます。
- b. パケット詳細ペイン(中央セクション)で最初の行を調べます。この行には、フレームの長さが表示されます(この 例では 74 バイト)。
- c. パケット詳細ペインの2行目では、それがイーサネットIIフレームであることが示されます。送信元および宛先の MACアドレスも表示されます。

PC の NIC の MAC アドレスは何ですか。_____

デフォルト ゲートウェイの MAC アドレスは何ですか。_____

d. 2 行目の先頭にあるプラス(+)記号をクリックすると、イーサネット II フレームに関する詳細な情報を取得できます。 プラス記号がマイナス(-)記号に変わることに注意してください。

どのフレーム タイプが表示されますか。___

e. 中央セクションに表示される最後の2行では、フレームのデータフィールドに関する情報が提供されます。データ に送信元および宛先の IPv4 アドレス情報が含まれることに注意してください。

送信元 IP アドレスは何と表示されていますか。

宛先 IP アドレスは何と表示されていますか。_____

f. 中央セクションの行をクリックすると、パケットバイトペイン(下部のセクション)でフレームのその部分(16 進数と ASCII)が強調表示されます。中央セクションで [Internet Control Message Protocol] の行をクリックし、パケットバイトペインで強調表示される情報を確認します。

 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) B 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	1
Type: 8 (Echo (ping) request)	
CheckSum: 0x404e [correct]	•
0000 30 f7 0d 7a ec 84 5c 26 0a 24 2a 60 08 00 45 00 0z\& .\$*`.E. 0010 00 3c 03 48 00 00 80 01 db 29 0a 14 a4 16 0a 14	

強調表示される最後の2オクテットの文字は何ですか。_____

g. 上部セクションで次のフレームをクリックし、エコー応答フレームを調べます。このフレームはデフォルト ゲートウェ イ ルータから最初の ping への応答として送信されたものなので、送信元と宛先の MAC アドレスが逆になってい ることに注意してください。

宛先アドレスとして表示されるデバイスおよび MAC アドレスは何ですか。

手順 7: Wireshark でパケットのキャプチャを再開します。

[Start Capture] アイコンをクリックして、Wireshark の新しいキャプチャを開始します。新しいキャプチャが開始する前 に、それまでにキャプチャされたパケットをファイルに保存するかどうかを確認するポップアップ ウィンドウが表示され ます。[Continue without Saving] をクリックします。



手順 8: コマンド プロンプト ウィンドウで、<u>www.cisco.com</u> に ping を発行します。

手順 9: パケットのキャプチャを停止します。



手順 10: Wireshark のパケット リスト ペインで新しいデータを調べます。

最初のエコー(ping)要求フレームで、送信元および宛先の MAC アドレスは何ですか。

送信元:

宛先:_____

フレームのデータフィールドに含まれる送信元および宛先の IP アドレスは何ですか。

送信元:_____

宛先:_____

これらのアドレスを、手順7で受信したアドレスと比較します。変化したアドレスは、宛先 IP アドレスだけです。宛先 IP アドレスが変化したのに、宛先 MAC アドレスが同じままになっているのはなぜですか。

復習

Wireshark では、フレーム ヘッダーのプリアンブル フィールドは表示されません。プリアンブルには何が含まれていま すか。