# Лабораторная работа: изучение кадров Ethernet с помощью программы Wireshark

Топология



#### Задачи

Часть 1. Изучение полей заголовков в кадре Ethernet II

#### Часть 2. Захват и анализ кадров Ethernet с помощью программы Wireshark

#### Исходные данные/сценарий

При взаимодействии протоколов верхнего уровня данные проходят уровни взаимодействия открытых систем (OSI) и инкапсулируются в кадры уровня 2. Структура кадра зависит от типа доступа к среде передачи данных. Например, если в качестве протоколов верхнего уровня используются TCP и IP, а тип доступа к среде передачи — Ethernet, то инкапсуляция кадров уровня 2 происходит через Ethernet II. Это типично для локальной среды.

При изучении концепций уровня 2 полезно анализировать данные заголовков кадров. В первой части этой лабораторной работы вы сможете посмотреть поля в кадре Ethernet II. Во второй части вам предстоит захватить и проанализировать поля заголовков кадра Ethernet II для локального и удалённого трафика с помощью программы Wireshark.

#### Необходимые ресурсы

• Один ПК (Windows 7, Vista или XP с выходом в Интернет и установленной программой Wireshark)

### Часть 1: Изучение полей заголовков в кадре Ethernet II

В части 1 вы изучите поля и содержание заголовков в кадре Ethernet II. Для этого будет использоваться захват данных программой Wireshark.

#### Шаг 1: Просмотрите длины и описания полей заголовков Ethernet II.

Преамбула	Адрес назначения	Адрес источника	Тип кадра	Данные	Контрольная последовательность кадра (Frame Check Sequence-FCS)
8 байт	6 байт	6 байт	2 байта	от 46 до 1500 байт	4 байта

#### Шаг 2: Изучите конфигурацию сети ПК.

IP-адрес узла ПК — 10.20.164.22, IP-адрес шлюза по умолчанию — 10.20.164.17.

Ethernet ada	apter Подкл	ючение по л	окальн	ой сети:	
DNS-суффи Локальный IPv4-адре Маска пој Основной	икс подключ и IPv6-адре ес цсети шлюз	ения с канала . 	: 10.	cisco.com fe80::b875:731b 10.20.164.22 255.255.255.240 20.164.17	:3c7b:c0b1%10

#### Шаг 3: Изучите кадры Ethernet в данных, захваченных программой Wireshark.

Показанный ниже результат захвата данных в программе Wireshark отображает пакеты, которые были сгенерированы эхо-запросом узлового ПК, отправленным на шлюз по умолчанию. В программе Wireshark включён фильтр для просмотра только ARP- и ICMP-протоколов. Сеанс начинается с ARP- запроса MAC-адреса маршрутизатора шлюза, за которым следуют четыре эхо-запроса с помощью команды ping и отклика.

<b>_</b> I	🚄 Intel(R) PRO/1000 MT Network Connection [Wireshark 1.10.0 (SVN Rev 49790 from /trunk-1.10)]										_		×						
Eile	<u>E</u> dit <u>V</u> iev	v <u>G</u> o	Capture	<u>A</u> nalyze	Statistics	Telephony <u>T</u>	ools <u>I</u> nter	nals <u>H</u> elp											
0	۵ 🔳	Ø	🖹 📑	* 2	°, 🖕	🕸 🥪 🐐	⊻   🗉		Q 0	2 🗹			<b>1</b> 8 %	Ø					
Filt	er: arp or ic	np					<b>•</b> 1	Expression	Clear	Apply	Save	e							
802.1	1 Channel:	- Chan	nel Offset:	▼ FCS I	Filter: All F	ames 💌	None	▼ Wire	less Settir	ngs C	Decry	ption K	eys						
No.	Time		Source			Destination	1	-	rotocol	Lengt	h I	nfo							
	7 9.6	011770	00 Dell_	_24:2a:	60	Broadca	st		ARP		42 1	who h	as 10.	20.164.1	7? Tell 10.	20.164.22			
	89.6	018030	00 Cisco	_7a:ec	:84	De11_24	:2a:60		ARP		<b>60</b> :	10.20	.164.1	7 is at 1	30:f7:0d:7a:	ec:84			
	99.6	018270	00 10.20	).164.2	2	10.20.1	.64.17		ICMP		74	Echo	(ping)	request	id=0x0001,	seq=37/947	2, 1	tt]=12	:8
	10 9.6	028070	00 10.20	).164.1	7	10.20.1	.64.22		ICMP		74	Echo	(ping)	reply	id=0x0001,	seq=37/947	2, 1	tt]=25	<i>i</i> 5
	12 10.	604187	00(10.20	0.164.2	2	10.20.1	.64.17		ICMP		74	Echo	(ping)	request	id=0x0001,	seq=38/972	(8, 1	tt]=12	:8
	13 10.	620728	00(10.20	).164.1	7	10.20.1	.64.22		ICMP		74	Echo	(ping)	reply	id=0x0001,	seq=38/972	(8, 1	tt]=25	<i>i</i> 5
	14 11.	607192	00(10.20	).164.2	2	10.20.1	.64.17		ICMP		74	Echo	(ping)	request	id=0x0001,	seq=39/998	4, 1	tt]=12	:8
	15 11.	608177	00(10.20	0.164.1	7	10.20.1	.64.22		ICMP		74 1	Echo	(ping)	reply	id=0x0001,	seq=39/998	14, 1	tt]=25	<i>i</i> 5
	17 12.	610258	00(10.20	0.164.2	2	10.20.1	.64.17		ICMP		74	Echo	(ping)	request	id=0x0001,	seq=40/102	40,	ttl=1	.28
	18 12.	611318	00(10.20	).164.1	7	10.20.1	.64.22		ICMP		74	Echo	(ping)	reply	id=0x0001,	seq=40/102	40,	tt]=2	255
•							III												Þ
E F	rame 7:	42 bvt	es on w	ire (33	6 bits)	. 42 bvtes	capture	ed (336 l	oits) (	on int	terf	ace (	)						
	thernet	II. Sr	c: Dell	_24:2a:	60 (5c:	26:0a:24:24	a:60). C	st: Broa	adcast	(ff:f	ff:f	f:ff:	ff:ff)						
	Destina	tion:	Broadca	st (ff:	ff:ff:f	f:ff:ff)													
. It	Source:	Dell_	24:2a:60	) (Sc:2	6:0a:24	:2a:60)													
	Type: A	RP (Ox	0806)																
÷ A	ddress R	esolut	ion Prot	tocol (	request	)													
							0.0.04		o										_
000 001 002	0 08 00 0 00 00	06 04 00 00	00 01 5 00 00 0	ic 26 ic 26 a 14	0a 24 2a 0a 24 2a a4 11	a 60 08 06 a 60 0a 14	a4 16		& .\$* & .\$*` 										

#### Шаг 4: Изучите содержание заголовков Ethernet II в ARP-запросе.

В приведённой ниже таблице выбран первый кадр из данных, захваченных программой Wireshark, и отображаются данные в полях заголовков Ethernet II.

#### Лабораторная работа: изучение кадров Ethernet с помощью программы Wireshark

Поле	Значение	Описание					
Преамбула	Не показано в захвате данных	В этом поле содержатся синхронизированные биты, обработанные аппаратным обеспечением сетевого адаптера.					
Адрес назначения	Широковещательная рассылка (ff:ff:ff:ff:ff)	Адреса уровня 2 для кадра. Длина каждого адреса составляет 48 бит или 6 октетов, выраженных 12 шестнадцатеричными цифрами, 0-9, А-F.					
Адрес источника	Dell_24:2a:60 (5c:26:0a:24:2a:60)	Общий формат — 12:34:56:78:9А:ВС. Первые шесть шестнадцатеричных номеров обознача производителя сетевого адаптера, а последние — серийный номер устройства.					
		Адрес назначения может быть широковещательным (состоящим только из единиц), либо индивидуальным. Адрес источника всегда индивидуальный.					
Тип кадра	0x0806	В кадрах Ethernet II это поле содержит шестнадцатеричное значение, которое используется для указания типа протокола верхнего уровня в поле данных. Ethernet II поддерживает множество протоколов верхнего уровня. Наиболее распространены следующие два типа кадров:					
		Значение Описание					
		0x0800 Протокол IPv4					
		0x0806 Протокол разрешения адресов (ARP)					
Данные	ARP	Содержит инкапсулированный протокол верхнего уровня. Поле данных в диапазоне от 46 до 1500 байт.					
Контрольная последовательность кадра (Frame Check Sequence-FCS)	Не показано в захвате данных	Контрольная последовательность кадра, используемая сетевым адаптером для выявления ошибок при передаче данных. Значение вычисляется компьютером отправителя, включает адреса, тип и поле данных кадра и проверяется получателем.					

Какова особенность содержания поля адреса назначения?

Почему перед первым эхо-запросом с помощью команды ping ПК отправляет широковещательную paccылку ARP?

Назовите МАС-адрес источника в первом кадре.

Назовите идентификатор производителя (OUI) сетевого адаптера источника.

Какая часть MAC-адреса соответствует OUI?

Назовите серийный номер сетевого адаптера источника.

### Часть 2: Захват и анализ кадров Ethernet с помощью программы Wireshark

В части 2 вы воспользуетесь программой Wireshark для захвата локальных и удалённых кадров Ethernet. Затем вы изучите сведения, содержащиеся в полях заголовков кадров.

#### Шаг 1: Определите IP-адрес шлюза по умолчанию на своём ПК.

Откройте окно командной строки и введитеipconfig.

Назовите IP-адрес шлюза ПК по умолчанию.

#### Шаг 2: Начните захват трафика на сетевом адаптере своего ПК.

- а. Откройте Wireshark.
- b. На панели инструментов анализатора сети Wireshark нажмите на значок Interface List (Список интерфейсов).



с. В окне Wireshark: Capture Interfaces (Захват интерфейсов) выберите интерфейс, в котором нужно начать захват трафика, установив соответствующий флажок, и нажмите кнопку Start (Пуск). Если вы не знаете, какой интерфейс выбрать, нажмите кнопку Details (Сведения), чтобы открыть подробную информацию о каждом из указанных интерфейсов.

🥖 Wireshark: C	apture 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
<u>H</u> elp	Start	Stop	<u>Option</u>	s	<u>C</u> lose

d. Понаблюдайте за трафиком в окне списка пакетов (Packet List).

Filter:		<ul> <li>Expression</li> </ul>	Clear	Apply Save
802.11	Channel: 🔽 Channel Offset: 💌 FCS Filter: All Fran	mes 🔻 None 💌 Wi	reless Settir	ngs Decryption Keys
No.	Time Source	Destination	Protocol	Length Info
	18 10.40268/00(184.2/.190.41	10.20.164.22	ICP	60 NTTPS > 62408 [ACK] SEQ=1 ACK=1163 W1N=43412 LEN=0
	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
	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	тср	54 62423 > https [ACK] Seq=1 Ack=1 Win=66780 Len=0

## Шаг 3: С помощью фильтров программы Wireshark отобразите на экране только трафик ICMP.

Чтобы скрыть ненужный трафик, установите соответствующий фильтр Wireshark. Фильтр не блокирует захват ненужных данных, а лишь отбирает то, что нужно показывать на экране. На данный момент разрешено отображение только ICMP-трафика.

В поле **Filter** (Фильтр) программы Wireshark введите **icmp**. При правильной настройке фильтра поле должно стать зелёным. Если поле стало зелёным, нажмите кнопку **Apply** (Применить), чтобы применить фильтр.

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

# Шаг 4: Из окна командной строки отправьте эхо-запрос с помощью команды ping на шлюз ПК по умолчанию.

Из окна командной строки отправьте эхо-запрос с помощью команды ping на шлюз по умолчанию, используя IP-адрес, записанный в шаге 1.

#### Шаг 5: Остановите захват трафика на сетевом адаптере.

Чтобы остановить захват трафика, нажмите на значок Stop Capture (Остановить захват).



#### Шаг 6: Изучите первый эхо-запрос с помощью команды ping в программе Wireshark.

Главное окно программы Wireshark состоит из трёх разделов: панель списка пакетов (вверху), панель сведений о пакете (посередине) и панель отображения пакета в виде последовательности байтов (внизу). Если вы правильно выбрали интерфейс для захвата пакетов в шаге 3, программа Wireshark отобразит данные протокола ICMP на панели списка пакетов, как показано в приведённом ниже примере.

Intel(R) 82577LM Gigabit Network Connection: \Device\NPF_(6179E093-A447-4EC8-81DF-5E22D08A6F63} [Wireshark 1.8.3 (SVN Rev 45256 from /trunk-1	-1.8)] 🗖 🗖 💌							
File Edit View Go Capture Analyze Statistics Telephony Tools Internals Help								
Filter: icmp Expression Clear Apply Save								
802.11 Channel: Channel Offset: SECS Filter: All Frames Vone Wireless Settings Decryption Keys								
No. Time Source Destination Protocol Length Info								
9 9.601827000 10.20.164.22 10.20.164.17 ICMP 74 Echo (ping) request id=(	0x0001, seq=37/9472, ttl=128							
10 9.602807000 10.20.164.17 10.20.164.22 ICMP 74 Echo (ping) reply id=0	0x0001, seq=37/9472, ttl=255							
12 10.60418700(10.20.164.22 10.20.164_17 ICMP 74 Echo (ping) request id=0	0x0001, seq=38/9728, ttl=128							
13 10.62072800(10.20.164.17 10.20.164 💆 XHAA Ya Comp 74 Echo (ping) reply id=0	0x0001, seq=38/9728, ttl=255							
14 11.60719200(10.20.164.22 10.20.164.17 ICMP 74 Echo (ping) request id=0	0x0001, seq=39/9984, ttl=128							
15 11.60817700(10.20.164.17 10.20.164.22 ICMP 74 Echo (ping) reply id=0	0x0001, seq=39/9984, ttl=255							
17 12.61025800(10.20.164.22 10.20.164.17 ICMP 74 Echo (ping) request id=0	0x0001, seq=40/10240, ttl=128							
18 12.61131800(10.20.164.17 10.20.164.22 ICMP 74 Echo (ping) reply id=0	0x0001, seq=40/10240, ttl=255							
< III	Þ.							
E Frame 9: 74 bytes on wire (592 bits) 74 bytes captured (592 bits) on interface 0								
E 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								
Средняя часть								
0000 30 f7 0d 7a ec 84 5c 26 0a 24 2a 60 08 00 45 00 0z. & .\$*`.E.								
0010 00 3C 19 03 00 00 80 01 C4 00 04 14 44 10 04 14								
0030 67 68 69 6a 6b 6c 6d 6e 6f 70 71 72 73 74 75 76 ghijklmn opgrstuv								
0040 77 61 62 63 64 65 66 67 68 69 wabcdefg hi								
Нижняя часть								

- на панели списка пакетов (верхний раздел) выберите первый указанный кадр. В столбце Info (Информация) появится значение Echo (ping) request (эхо-запрос с помощью команды ping). Строка станет синей.
- b. Изучите первую строку в панели сведений о пакете в средней части экрана. В этой строке указывается длина кадра (в данном примере — 74 байта).
- с. Вторая строка в панели Packet Details (Сведения о пакете) показывает, что это кадр Ethernet II. Также отображаются MAC-адреса источника и назначения.

Назовите МАС-адрес сетевого адаптера этого ПК.

Назовите МАС-адрес шлюза по умолчанию.

d. Чтобы получить больше информации о кадре Ethernet II, нажмите на значок плюса («+») в начале второй строки. Обратите внимание на то, что значок плюса при этом изменится на значок минуса («-»).

Назовите показанный тип кадра.

е. Последние две строки среднего раздела содержат информацию о поле данных кадра. Обратите внимание на то, что данные содержат IPv4-адреса источника и назначения.

Назовите IP-адрес источника.

Назовите IP-адрес назначения.

f. Чтобы выделить эту часть кадра (в шестнадцатеричной системе и ASCII) в панели отображения пакета в виде последовательности байтов (нижний раздел) нажмите на любую строку в среднем разделе. Нажмите на строку Internet Control Message Protocol в среднем разделе и посмотрите, что будет выделено в панели отображения пакета в виде последовательности байтов.

#### Лабораторная работа: изучение кадров Ethernet с помощью программы Wireshark

<ul> <li></li></ul>	A E
Internet Control Message Protocol	
Type: 8 (Echo (ping) request)	
Checksum: 0x4d4e [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	

Какое слово образуют последние два выделенных октета?

g. Нажмите на следующий кадр в верхнем разделе и изучите кадр эхо-ответа. Обратите внимание на то, что MAC-адреса источника и назначения поменялись местами, поскольку маршрутизатор, который служит шлюзом по умолчанию, отправил этот кадр в ответ на первый эхо-запрос с помощью команды ping.

Какое устройство и МАС-адрес отображаются в качестве адреса назначения?

#### Шаг 7: Перезапустите захват пакетов в программе Wireshark.

Нажмите на значок **Start Capture** (Начать захват), чтобы начать новый захват данных в программе Wireshark. Откроется всплывающее окно с предложением сохранить предыдущие захваченные пакеты в файл перед началом нового захвата. Нажмите кнопку **Continue without Saving** (Продолжить без сохранения).



- Шаг 8: Через окно командной строки отправьте эхо-запрос с помощью команды ping на веб-сайт <u>www.cisco.com</u>.
- Шаг 9: Остановите захват пакетов.



#### Шаг 10: Изучите новые данные на панели списка пакетов в программе Wireshark.

Назовите MAC-адреса источника и назначения в первом кадре эхо-запроса с помощью команды ping.

Источник: \_\_\_\_\_

Назначение: \_\_\_\_\_

Назовите IP-адреса источника и назначения в поле данных кадра.

Источник:

Назначение:

Сравните эти адреса с адресами, полученными в шаге 7. Изменился только IP-адрес назначения. Почему IP-адрес назначения изменился, а МАС-адрес назначения остался прежним?

#### Вопросы на закрепление

Программа Wireshark не отображает поле преамбулы заголовка кадра. Что содержит преамбула?