Лабораторная работа: просмотр сетевого трафика с помощью программы Wireshark

Топология



Задачи

Часть 1. Загрузка и установка программы Wireshark (необязательно)

Часть 2. Сбор и анализ данных протокола ICMP по локальным узлам в программе Wireshark

- Начните и остановите сбор данных трафика эхо-запросов с помощью команды ping к локальным узлам.
- Найдите данные об IP- и MAC-адресах в полученных PDU.

Часть 3. Сбор и анализ данных протокола ICMP по удалённым узлам в программе Wireshark

- Начните и остановите сбор данных трафика эхо-запросов с помощью команды ping к удалённым узлам.
- Найдите данные об IP- и MAC-адресах в полученных PDU.
- Поясните, почему МАС-адреса удалённых узлов отличаются от МАС-адресов локальных узлов.

Исходные данные/сценарий

Wireshark — это программа для анализа протоколов (анализатор пакетов), которая используется для поиска и устранения неполадок в сети, анализа, разработки программного обеспечения и протоколов, а также обучения. По мере движения потоков данных по сети анализатор перехватывает каждый протокольный блок данных (PDU), после чего расшифровывает или анализирует его содержание согласно соответствующему документу RFC или другим спецификациям.

Wireshark — полезный инструмент для всех, кто работает с сетями. Его можно использовать для анализа данных, а также для поиска и устранения неполадок при выполнении большинства

лабораторных работ в рамках курсов ССNA. В данной лабораторной работе содержатся инструкции по загрузке и установке программы Wireshark. Воспользуйтесь ими, если программа не установлена. В ходе лабораторной работы вы научитесь пользоваться программой Wireshark для перехвата IPадресов пакетов данных ICMP и MAC-адресов Ethernet-кадров.

Необходимые ресурсы

- 1 ПК (Windows 7, Vista или XP с выходом в Интернет)
- Дополнительные ПК в локальной сети будут использоваться для ответов на эхо-запросы.

Часть 1: Загрузка и установка программы Wireshark (необязательно)

Программа Wireshark стала стандартным анализатором пакетов, используемым сетевыми инженерами. Версии этой программы с открытым исходным кодом доступны для различных операционных систем, включая Windows, Mac и Linux. В части 1 этой лабораторной работы вам нужно будет загрузить и установить программу Wireshark на ПК.

Примечание. Если программа Wireshark на вашем ПК уже установлена, вы можете пропустить часть 1 и перейти сразу к части 2. Если программа Wireshark на вашем ПК не установлена, узнайте у инструктора о правилах загрузки программного обеспечения в вашем учебном заведении.

Шаг 1: Загрузите программу Wireshark.

- a. Программу Wireshark можно загрузить по адресу www.wireshark.org.
- b. Нажмите **Download Wireshark**.



Лабораторная работа: просмотр сетевого трафика с помощью программы Wireshark

с. Выберите версию программы в соответствии с архитектурой и операционной системой вашего ПК. Например, если ваш ПК работает под управлением 64-разрядной ОС Windows, выберите **Windows Installer (64-bit)**.

WHALS OF YOUR HELWORK:
Download Wireshark
The current stable release of Wireshark is 1.10.0. It supersedes all previous releases. You can also download the latest development release (1.10.0rc2) and documentation.
Stable Pclease (1.10.0)
🛓 Windows Installer (64-bit)
Windows Installer (32-bit)
Windows U3 (32-bit)
Windows PortableApps (32-bit)
OS X 10.6 and later Intel 64-bit .dmg
OS X 10.5 and later Intel 32-bit .dmg
Source Code
Old Stable Release (1.8.8)
Development Release (1.10.0rc2)
Documentation

Сразу после этого начнётся загрузка. Местонахождение загруженного файла зависит от браузера и операционной системы, которыми вы пользуетесь. В ОС Windows загрузочные файлы по умолчанию находятся в папке Загрузки.

Шаг 2: Установите программу Wireshark.

- a. Загруженный файл называется Wireshark-win64-x.x.x.exe, где «х» соответствует номеруверсии. Дважды нажмите на файл, чтобы начать установку.
- b. Ответьте на все сообщения безопасности, которые появятся на экране. Если на вашем ПК уже имеется копия Wireshark, перед установкой программы появится запрос на удаление прежней версии. Рекомендуется удалить старую версию программы перед установкой новой. Чтобы удалить предыдущую версию программы Wireshark, нажмите кнопку **Да**.



с. Если программа Wireshark устанавливается впервые или предыдущая версия была удалена, откроется мастер установки программы Wireshark. Нажмите кнопку **Next** (Далее).



d. Выполните инструкции по установке. Когда откроется окно «License Agreement» (Лицензионное соглашение), нажмите кнопку I accept (Принять).

🚄 Wireshark 1.10.0 (64-bit) Setup	
License Agreement Please review the license terms before installing Wireshark 1.10.0 (64-bit).	
Press Page Down to see the rest of the agreement.	
This text consists of three parts:	*
Part I: Some remarks regarding the license given in Part II: The actual license that covers Wireshark. Part III: Other applicable licenses. When in doubt: Part II/III is the legally binding part, Part I is just there to make it easier for people that are not familiar with the GPLv2.	
	-
If you accept the terms of the agreement, click I Agree to continue. You must agreement to install Wireshark 1.10.0 (64-bit).	t accept the
Nullsoft Install System v2,46	Cancel

е. При выборе компонентов оставьте настройки по умолчанию и нажмите кнопку Next (Далее).

🚄 Wireshark 1.10.0 (64-bit) Setu	p 🗆 🖾
Choose Components Choose which features of Wires	hark 1.10.0 (64-bit) you want to install.
The following components are a	vailable for installation.
Select components to install:	✓ Wireshark ✓ TShark ✓ Plugins / Extensions ✓ Tools ✓ User's Guide
Space required: 111.5MB	Description Position your mouse over a component to see its description,
Nullsoft Install System v2,46 ———	< Back Next > Cancel

f. Выберите желаемые ярлыки и нажмите кнопку Next (Далее).

Kireshark 1.10.0 (64-bit) Setup	
Select Additional Tasks Which additional tasks should be done?	
Create Shortcuts Start Menu Item Desktop Icon Quick Launch Icon File Extensions Associate trace file extensions to Wireshark (5vw, acp, apc, atc, bfr, cap, enc, erf, fdc, out, pcap, pcapng, pkt, rf5, snoop, syc, tpc, tr1, trace, trc, vwr, wpc, wpz)	
Nullsoft Install System v2.46	Cancel

g. Если дисковое пространство ограничено, директорию установки можно изменить, в противном случае, оставьте адрес, указанный по умолчанию.

🚄 Wireshark 1.10.0 (64-bit) Setup	
Choose Install Location Choose the folder in which to install Wireshark 1.10.0 (64-bit).	4
Choose a directory in which to install Wireshark.	
Destination Folder C:\Program Files\Wireshark	Browse
Space required: 111.5MB Space available: 26.8GB	
Nullsoft Install System v2,46 	Next > Cancel

- h. Для сбора сетевых данных на ваш ПК необходимо установить программу WinPcap. Если она уже установлена, флажок установки будет снят. Если установленная версия WinPcap старше версии, прилагаемой к программе Wireshark, рекомендуем установить более новую версию, нажав на флажок рядом с вариантом **Install WinPcap x.x.x** (Установить WinPcap x.x.x).
- і. Если установка прошла успешно, закройте мастер установки WinPcap.

📕 Wireshark 1.10.0 (64-bit) Setup		
Install WinPcap? WinPcap is required to capture live network data. Should WinPcap be installed	d?	
Currently installed WinPcap version WinPcap 4.1.3		
Install Install WinPcap 4.1.3 If selected, the currently installed WinPcap 4.1.3 will be uninstalled firs	st.	
What is WinPcap?		
Nullsoft Install System v2.46	Car	ncel

© Корпорация Сіѕсо и/или её дочерние компании, 2014. Все права защищены.

В данном документе содержится общедоступная информация корпорации Cisco.

j. После этого начнётся установка программы Wireshark. Статус установки будет отображаться в отдельном окне. По завершении установки нажмите кнопку **Next** (Далее).

🚄 Wireshark 1.10.0 (64-bit) Setup		
Installation Complete Setup was completed successfully.		
Completed		
Extract: reordercap.exe Output folder: C:\Program Files\Wireshark Extract: capinfos.exe Extract: capinfos.html Output folder: C:\Program Files\Wireshark Extract: rawshark.exe Extract: rawshark.html Output folder: C:\Program Files\Wireshark Extract: user-guide.chm Completed		•
Nullsoft Install System v2.46	< Back Next >	Cancel

к. Для завершения процесса установки программы Wireshark нажмите Finish (Готово).



Часть 2: Сбор и анализ данных протокола ICMP по локальным узлам в программе Wireshark

В части 2 этой лабораторной работы вы должны отправить эхо-запрос с помощью команды ping на другой ПК в локальной сети и перехватить ICMP-запросы и отклики в программе Wireshark. Кроме того, вам нужно найти необходимую информацию в собранных кадрах. Этот анализ поможет понять, как используются заголовки пакетов для передачи данных по месту назначения.

Шаг 1: Определите адреса интерфейсов вашего ПК.

В данной лабораторной работе вам необходимо узнать IP-адрес компьютера и физический адрес сетевого адаптера, который называется MAC-адресом.

- а. Откройте окно командной строки, введите команду ipconfig /all и нажмите клавишу ВВОД.
- b. Запишите IP-адрес интерфейса ПК и МАС-адрес (физический адрес).

🔤 Администратор: C:\Windows\system32\cmd.exe	3
C:\>ipconfig ∕all	*
Настройка протокола IP для Windows	
Имя компьютера : РС-А Основной DNS-суффикс : Тип узла : Гибридный IP-маршритизация включена . Нет	11
WINS-прокси включен Нет	
Ethernet адартер подключение по локальной сети:	
DNS-суффикс подключения : Описание	
рнсг включен	
Маска подсети	

с. Обменяйтесь ІР-адресами с другими учащимися, но пока что не сообщайте им свой МАС-адрес.

Шаг 2: Запустите программу Wireshark и начните перехват данных.

а. На своём ПК нажмите кнопку **Пуск** и найдите Wireshark в списке программ. Дважды нажмите на **Wireshark**.

b. Запустив программу Wireshark, нажмите на параметр Interface list (Список интерфейсов).

· · · · · · · · · · · · · · · · · · ·		
The Wireshark Network Analyzer [Wireshark 1.10.0 (SVN Rev 49790 from /trunk-1.10)]		
File Edit View Go Capture Analyze Statistics Telephony Tools Internals	Help	
	Q Q Q III ¥ M 🔧 % Ħ	
Filter:	Expression Clear Apply Save	
WIRESHARK The World's Most Popular Netwo Version 1.10.0 (SVN Rev 49790 from /trunk	rk Protocol Analyzer -1.10)	
Capture	Files	Online
 Interface List Design of the capture interfaces Start Choses one or more interfaces to capture from, then Start Sum: \Device\\NPF_[DDEC4325-FF46-4582-BC18-9636F4946680) Intel(R) 82577LM Gigabit Network Connection: \Device\\NPF_[G179E093-A447-4E Intel(R) 82577LM Gigabit Network Connection: \Device\\NPF_[G179E093-A447-4E To capture Options Start a capture with detailed options Capture Options Start a capture with detailed options Device Capture Device Capture Sup to a successful capture setup Network Media Specific information for capturing on: therms. W.A.A 	 Poen Open previously captured file Open Recent: Sample Captures A rich assorment of example capture files on the witid 	 Website Wate projects website User's Guide The User's Guide (local vention, if installed) Security Work with Wireshark as securely as possible
Ready to load or capture No Packets		Profile: Default

Примечание. Список интерфейсов можно также открыть, нажав на значок первого интерфейса в ряду значков.

с. В окне «Capture Interfaces» (Перехват интерфейсов) программы Wireshark установите флажок рядом с интерфейсом, подключённым к вашей локальной сети.

📕 Wireshark: Cap	ture Interfaces				- • •
	Description	IP	Packets	Packets/s	
	Intel(R) PRO/1000 MT Network Connection		19	0	<u>D</u> etails
	Intel(R) 82577LM Gigabit Network Connection	192.168.1.11	47	0	Details
<u>H</u> elp		Start	Stop	<u>O</u> ptions	<u>C</u> lose

Примечание. Если перечислено несколько интерфейсов и вы не уверены в том, какой из них нужно выбрать, нажмите кнопку **Details** (Подробнее) и откройте вкладку **802.3 (Ethernet).** Убедитесь в том, что MAC-адрес соответствует результату, который вы получили в шаге 1b. Убедившись в правильности интерфейса, закройте окно информации.

🚄 Wireshark: Capture Interfaces	- • •
Characteristics Statistics (802.3 (Ethernet)	802.11 (WLAN) Task Offload
Characteristics Permanent station address Current station address	00:50:56:BE:76:8C 00:50:56:BE:76:8C
Statistics	

d. После этого нажмите кнопку Start (Начать), чтобы начать перехват данных.

📕 Wireshark: Cap	ture Interfaces				- • •
	Description	IP	Packets	Packets/s	
	Intel(R) PRO/1000 MT Network Connection		19	0	<u>D</u> etails
	Intel(R) 82577LM Gigabit Network Connection	192.168.1.11	47	0	<u>D</u> etails
1					
Help		Start	S <u>t</u> op	<u>O</u> ptions	<u>C</u> lose

В верхней части окна программы Wireshark начнёт прокручиваться информация. Строки данных выделяются различными цветами в зависимости от протокола.

📶 Capt	turing from Intel(R) 82577LM Gigabit Network Co	nnection: \Device\NPF_{6179E093-A447-4EC8-81E	0F-5E22D08A6F63) [Wireshark 1.8.3 (SVN Rev 45256 from /trunk-1.8)]	- • •
<u>File</u>	dit <u>V</u> iew <u>Go</u> <u>C</u> apture <u>A</u> nalyze <u>S</u> tatistics	Telephony <u>T</u> ools Internals <u>H</u> elp		
0.0				
Filter:		 Expression Clear 	Apply Save	
No.	Time Source	Destination Protocol	Length Info	*
	21 2 451962000 cisco 7a:ec:84	Spanning_tree_(for_br:STP	60 conf _ Poot = 32768/0/30:f7:0d:7a:ec:84 _ Cost = 0 _ Port = 0x8001	
	22 3,497376000 10,20,164,21	173,194,79,125 TCP	91 [TCP segment of a reassembled PDU]	
	23 3.567094000 173.194.79.125	10.20.164.21 TCP	60 xmpp-client > 53588 [ACK] Seg=1 Ack=38 Win=1002 Len=0	
	24 4.451700000 Cisco_7a:ec:84	Spanning-tree-(for-br:STP	60 Conf. Root = 32768/0/30:f7:0d:7a:ec:84 Cost = 0 Port = 0x8001	
	25 6.451326000 cisco_7a:ec:84	Spanning-tree-(for-br STP	60 Conf. Root = 32768/0/30:f7:0d:7a:ec:84	
	26 8.451225000 cisco_7a:ec:84	Spanning-tree-(for-br'STP	60 Conf. Root = 32768/0/30:f7:0d:7a:ec:84	
	27 10.27736800(10.20.164.21	173.36.12.72 TCP	55 53964 > 10846 [АСК] Seq=1 Ack=1 Win=63974 Len=1	
	28 10.35963200(173.36.12.72	10.20.164.21 TCP	66 10846 > 53964 [ACK] Seq=1 Ack=2 Win=513 Len=0 SLE=1 SRE=2	
	29 10.45232500(cisco_7a:ec:84	Spanning-tree-(for-br:STP	60 Conf. Root = 32768/0/30:f7:0d:7a:ec:84 Cost = 0 Port = 0x8001	
	30 10.94920600(10.20.164.21	171.68.57.53 NBNS	92 Name query NB UNIDC3<20>	
	31 10.99746700(171.68.57.53	10.20.164.21 NBNS	98 Name query response, Requested name does not exist	
	32 10.99758500(10.20.164.21	173.37.115.191 NBNS	92 Name query NB UNIDC3<20>	
	33 11.08046600(173.37.115.191	10.20.164.21 NBNS	98 Name query response, Requested name does not exist	
	34 11.09043000(10.20.164.21	10.20.164.31 NBNS	92 Name query NB UNIDC3<20>	
	35 11.84043400(10.20.164.21	10.20.164.31 NBN5	92 Name query NB UNIDC3<20>	
	36 12.45071000(cisco_7a:ec:84	Spanning-tree-(for-br:STP	60 Conf. Root = 32768/0/30:f7:0d:7a:ec:84	
	37 12.59048100(10.20.164.21	10.20.164.31 NBN5	92 Name query NB UNIDC3<20>	
	38 13.34153600(10.20.164.21	171.68.57.53 NBN5	92 Name query NB UNIDC3<20>	-
	39 13.41142100(171.68.57.53	10.20.164.21 NBN5	98 Name query response, Requested name does not exist	
	40 13.41151700(10.20.164.21	173.37.115.191 NBN5	92 Name query NB UNIDC3<20>	
	41 13.49295400(173.37.115.191	10.20.164.21 NBNS	98 Name query response, Requested name does not exist	
	42 13.50250600(10.20.164.21	10.20.164.31 NBNS	92 Name query NB UNIDC3<20>	
	43 14.25256/00(10.20.164.21	10.20.164.31 NBNS	92 Name query NB UNIX 3<20>	
	44 14.45045300(C15CO_/a:ec:84	spanning-tree-(tor-bristP	60 CONT. ROOT = 32/68/0/30:T/:0d:/a:ec:84 Cost = 0 Port = 0X8001	
	45 14.6946/200(10.20.164.21	192.108.87.9 SRVLOC	86 Attribute Request, VI Transaction ID - 49289	*
•			III	F.
🗄 Fra	me 1: 66 bytes on wire (528 bits), 66 bytes captured (528 bits) o	n interface 0	
🖲 Eth	ernet II, Src: Dell_24:2a:60 (5c	:26:0a:24:2a:60), Dst: Cisco_7a:e	ec:84 (30:f7:0d:7a:ec:84)	
🗉 Int	ernet Protocol Version 4, Src: 1	0.20.164.21 (10.20.164.21), Dst:	204.236.230.45 (204.236.230.45)	
🗉 Tra	nsmission Control Protocol, Src	Port: 54996 (54996), Dst Port: ht	tps (443), Seq: 0, Len: 0	
0000	30 f7 0d 7a ec 84 5c 26 0a 24 2	a 60 08 00 45 00 0z\& .\$*`	E.	
0010	00 34 4f 78 40 00 80 06 4a 08 0	a 14 a4 15 cc ec .40x@ J		- All All All All All All All All All Al
0020	e6 2d d6 d4 01 bb dc b2 af 4e (00 00 00 00 80 02		E
0030	20 00 8a 09 00 00 02 04 04 ec 0 04 02	1 03 03 02 01 01		
				•
💛 🗾 I	ntel(R) 82577LM Gigabit Network Connection: \D	evice\NPF_{6179E093-A447-4EC8-81DF Packet	s: 45 Displayed: 45 Marked: 0 Profile: Default	

е. Информация может прокручиваться очень быстро в зависимости от типа связи между ПК и локальной сетью. Чтобы облегчить просмотр и работу с данными, собранными программой Wireshark, можно применить фильтр. В этой лабораторной работе нам нужны только протокольные блоки данных (PDU) ICMP (эхо-запрос с помощью команды ping). Чтобы вывести на экран только протокольные блоки данных ICMP (эхо-запрос с помощью команды ping), в поле фильтра в верхней части окна программы Wireshark введите **icmp** и нажмите клавишу BBOД или кнопку **Аррly** (Применить).



f. После этого все данные в верхнем окне исчезнут, однако перехват трафика в интерфейсе продолжится. Откройте окно командной строки, которое вы открывали ранее, и отправьте эхозапрос с помощью команды ping на IP-адрес, полученный от другого учащегося. Обратите внимание на то, что в верхней части окна программы Wireshark снова появятся данные.

Capturing from Intel(R) PRO/1000 MT Network Connection [Wireshark 1.10.0 (SVN Rev 49790 from /trunk-1.10)]							
<u>File Edit View Go Capture Analyze Statistics</u>	Telephony <u>T</u> ools <u>I</u> nternals <u>H</u> elp						
● ● 🖉 ■ 🧖 🖿 🖿 🗙 2 9, 🗢	🔶 🎝 🚡 👱 🗐 🗐 🗨 (2, 92, 🛅 🕁 🗹 畅 🐝	B				
Filter: icmp	 Expression 	Clear Apply					
No. Time Source D	estination Protocol Ler	ngth Info					
11 15.118840 192.168.1.11 1	.92.168.1.12 ICMP	74 Echo (ping) request	id=0x0001, seq=21/5376, ttl=12				
14 15.119602 192.168.1.12 1	.92.168.1.11 ICMP	74 Echo (ping) reply	id=0x0001, seq=21/5376, ttl=12				
16 16.127853 192.168.1.11 1	.92.168.1.12 ICMP	74 Echo (ping) request	id=0x0001, seq=22/5632, ttl=12				
17 16.128679 192.168.1.12 1	.92.168.1.11 ICMP	74 Echo (ping) reply	id=0x0001, seq=22/5632, ttl=12				
18 17.141897 192.168.1.11 1	.92.168.1.12 ICMP	/4 Echo (ping) request	1d=0x0001, seq=23/5888, ttl=12				
19 1/.145943 192.168.1.12 1	.92.168.1.11 ICMP	74 Echo (ping) reply	1d=0x0001, seq=23/5888, ttl=12				
21 18.140246 192.168.1.11 1	.92.168.1.12 ICMP	74 Echo (ping) request	1d=0x0001, seq=24/6144, ttl=12				
22 10.140/94 192.108.1.12 1	.92.100.1.11 ICMP	74 ECHO (ping) reply	1u=0x0001, Seq=24/6144, tt1=12				
	ок сыминдожызузет 32/стид.ехе Описсание. Физический адрес DHCP включен. Автонастройка включена. Fv6-адрес. вной 2000 градование в собратование в собратование в собратование собратование собратование собратование собрат вной 2000 градование собратование собратов собратование собратование собратование Собратование собратование собратование собратование собратование собратование собратование собратование собрато	: Teredo Tunne : 00-00-00-00- : Her : Ja : 2001:0:5ef5:'	ling Pseudo-Interface 00-00-00-E0 0 79fb:242a:3bde:3f57:2a77<0cho				
 	Локальный ІРФБ-адрес ка Основной шлюз NetBios через TCP/IP	нала : fe80::242a:3) : :: : Отключен	оде: <u>3157:28</u> 77%15(Основной)				
Internet Control Message Protocol	C:\>ping 192.168.1.12						
Обнен пакетани с 192.168.1.2 по с 32 байтами данных: Ответ от 192.168.1.2: число байт=32 время=13ис TTL=128 Ответ от 192.168.1.2: число байт=32 время=5ис TTL=128 Ответ от 192.168.1.2: число байт=32 время=5ис TTL=128							
0010 00 3c 01 ac 00 00 80 01 b5 ad c 0020 01 0c 08 00 4d 46 00 01 00 15 6 0030 67 68 69 6a 6b 6c 6d 6e 6f 70 7	Ответ от 192.168.1.2: числ Статистика Ping для 192.16	в сайт=32 время=6мс TTL=1: 8.1.2:	28				
0040 77 61 62 63 64 65 66 67 68 69	Пакетов: отправлено =	4, получено = 4, потеряно	= 0				
Intel(R) PRO/1000 MT Network Connection: Pack	Приблизительное время прие	ма-передачи в мс:					

Примечание. Если компьютеры других учащихся не отвечают на ваши эхо-запросы, это может быть вызвано тем, что брандмауэры их компьютеров блокируют эти запросы. Информацию о том, как пропустить трафик ICMP через брандмауэр на ПК с OC Windows 7, содержит Приложение А. Пропуск трафика ICMP через брандмауэр.

g. Остановите перехват данных, нажав на значок Stop Capture (Остановить перехват).



Шаг 3: Изучите полученные данные.

В шаге 3 необходимо проверить данные, сформированные эхо-запросами с помощью команды ping ПК других учащихся. Программа Wireshark отображает данные в трёх разделах: 1) в верхнем разделе отображается список полученных кадров PDU со сводной информацией об IP-пакетах; 2) в среднем разделе приводится информация о PDU для кадра, выбранного в верхнем разделе экрана, и деление кадра PDU на слои протоколов; 3) в нижнем разделе показываются необработанные данные каждого уровня. Необработанные данные отображаются как в шестнадцатеричном, так и десятичном форматах.

🗖 Cap	oturing from In	tel(R) PRO	D/1000 N	/IT Net	work C	onnecti	ion [\	Niresh	ark 1.6	5.1 (SV	N Rev 38096	i from /ti	unk-1.	6)]				_		x
<u>F</u> ile	<u>E</u> dit <u>V</u> iew <u>(</u>	<u>io C</u> apt	ure <u>A</u> r	nalyze	<u>S</u> tatis	tics T	elepho	on <u>y</u>]	[ools	Inter	nals <u>H</u> elp									
		¥ 📟	8 >	(2	≞	Q	(a) (a)	> 🍫	7	₽		€€		**	ğ 🗹 📒	<u>.</u>	% 🛱			
Filter:	icmp									- E	xpression	Clear	Apply							
No.	Time	Sou	rce			Des	tinatio	n			Protocol L	ength I	nfo							
	11 15.1188	40 192	2.168.	1.11		19	2.168	3.1.1	.2		ICMP	74	Echo	(ping)	reque	st	id=0x0001,	seq=21/53	76, ttl:	
	14 15.1196	02 192	2.168.	1.12		192	2.168	3.1.1	.1		ICMP	74	Echo	(ping)	reply		id=0x0001,	seq=21/53	76, ttl:	=12
	16 16.1278	53 192	2.168.	1.11		192	2.168	3.1.1	.2		ICMP	74	Echo	(ping)	reque	st	id=0x0001,	seq=22/56	32, ttl	=12
	17 16.1286	79 192	2.168.	1.12		19	2.168	3.1.1	1		ICMP	74	Echo	(ping)	reply		id=0x0001,	seq=22/56	32, ttl	=12
	18 17.1418	97 192	2.168.	1.11		192	2.168	3.1.1	.2		ICMP	74	Echo	(ping)	reque	st	id=0x0001,	seq=23/58	38, ttl	=12
	19 17.1459	43 192	2.168.	1.12		19	2.168	3.1.1	1		ICMP	74	Echo	(ping)	reply		id=0x0001,	seq=23/58	38, ttl	=12
	21 18.1402	46 192	2.168.	1.11		19	2.168	5.1.1	.2		ICMP	74	Echo	(ping)	reque	st	1d=0x0001,	seq=24/61	14, ttl:	=12
	22 18.140/	94 192	2.168.	1.12		19,	2.168	5.1.1	1		TCWb	74	-cno	(ping)	repiy		1d=0x0001,	Seq=24/614	14, TT I:	=14
e Fra	ame 11: 74 hernet II.	bytes Src:	on wi Intel(ire (592 4:92	oits) :1c (, 74 58:94	byte	es ca	aptur 02:1c	ed (592	bits) Intel	of:9	01:48 (00:11:	11:0)f:91:48)			_
🗄 Int	ternet Pro	tocol	versio	on 4,	Src	: 192	.168.	1.11	(19	2.16	8.1.11),	Dst:	192.	168.1.	12 (19	2.16	58.1.12)			
🗄 Int	ternet Con	trol M	essage	e Pro	toco	1														
																	Mid	dle Section		
0000 0010 0020 0030 0040	00 50 56 00 3c 01 01 0c 08 67 68 69 77 61 62	be f6 ac 00 00 4d 6a 6b 63 64	db 00 00 80 46 00 6c 6d 65 66	50 01 01 6e 67	56 b b5 a 00 1 6f 7 68 6	e 76 d c0 5 61 0 71	8c 0 a8 0 62 6 72 7	8 00 1 0b 3 64 3 74	45 c0 65 75	00 a8 66 76	.PV . <mf. ghijklm wabcdef</mf. 	P V.V. ab n opqr g hi	E. cdef stuv				Bot	tom Seciton		4 III +
Integration	el(R) PRO/1000	MT Netw	ork Cor	nnectio	n:	Packets	: 199 D	isplay	ed: 8 N	/larked	: 0						Profile: Defa	ult		

а. Выберите PDU-кадры первого запроса ICMP в верхнем разделе окна программы Wireshark. Обратите внимание на то, что в столбце Source (Источник) указывается IP-адрес вашего компьютера, а в столбце «Destination» (Назначение) — IP-адрес ПК, которому вы отправили эхозапрос с помощью команды ping.

📕 Ir	ntel(R) PRO/1000	MT Network Connecti	on [Wireshark 1.10.0 (S)	/N Rev 49790 from /trunk-	1.10)]				
<u>F</u> ile	<u>E</u> dit <u>V</u> iew <u>G</u>	o <u>C</u> apture <u>A</u> nalyze	e <u>S</u> tatistics Telephony	<u></u>	р				
0	۰ 📕 🕻	(🖻 晶 💥 💈) 🔍 🗢 🔿	7 ⊻ 🛛 🗐 (🤆	Q Q 🕅	🍇 🗹 🕵 🖇	\$ 🛱		
Filte	er: icmp			Expression	Clear Apply				
No.	Time	Source	Destination	Protocol	Length Info				
	5 2.80178	4 192.168.1.1	L 192.168.1	1.12 ICMP	74 Echo	(ping) reques	t id=0x0001,	seq=25/6400,	tt]=12
	8 2.80267	9 192.168.1.12	2 192.168.3	1.11 ICMP	74 Echo	(ping) reply	id=0x0001,	seq=25/6400,	tt]=12
	10 3.81689	5 192.168.1.1	L 192.168.1	1.12 ICMP	74 Echo	(ping) reques	t id=0x0001,	seq=26/6656,	tt]=12
	11 3.81754	0 19 <u>2.168.1.</u> 12	2 192. <u>168.</u>	1.11 ICMP	74 Echo	(ping) reply	id=0x0001,	seq=26/6656,	tt]=12
	13 4.83134	3 (192.168.1.1)	1) (192.168.1	1.12 ICMP	74 Echo	(ping reques	t id=0x0001,	seq=27/6912,	tt]=12
	14 4.83200	5 192.168.1.12	2 192.168.	I.11 ICMP	74 Echo	(ping) reply	id=0x0001,	seq=27/6912,	tt]=12
	15 5.84485	8 192.168.1.1	L 192.168.1	1.12 ICMP	74 Echo	(ping) reques	t id=0x0001,	seq=28/7168,	tt]=12
	16 5.84548	8 192.168.1.12	2 192.168.1	1.11 ICMP	74 Echo	(ping) reply	id=0x0001,	seq=28/7168,	tt]=12

© Корпорация Cisco и/или её дочерние компании, 2014. Все права защищены. В данном документе содержится общедоступная информация корпорации Cisco. b. Не меняя выбор PDU-кадра в верхнем разделе программы, перейдите в средний раздел. Нажмите на символ + слева от строки «Ethernet II», чтобы увидеть MAC-адреса источника и назначения.

📕 In	tel(R) PRO/1000 M	T Network Connection	[Wireshark 1.10.0 (SVN Rev 497	790 from /trunk-1.	.10)]				
<u>F</u> ile	<u>E</u> dit <u>V</u> iew <u>G</u> o	<u>C</u> apture <u>A</u> nalyze	Statistics Telephony Tools	Internals <u>H</u> elp					
0	که 🔳 🔺 🏵	🖹 🖿 🐹 😂	् 🗢 🔿 春 🕹		. Q. Q. 🖭 👪 🗹 畅 % 😫				
Filte	: icmp			 Expression 	Clear Apply				
No.	Time	Source	Destination	Protocol L	ength Info				
	5 2.801784	192.168.1.11	192.168.1.12	ICMP	74 Echo (ping) request id=	0x0001, seq=25/6400, ttl=12			
	8 2.802679	192.168.1.12	192.168.1.11	ICMP	74 Echo (ping) reply id=	0x0001, seq=25/6400, ttl=12			
	10 3.816895	192.168.1.11	192.168.1.12	ICMP	74 Echo (ping) request id=	0x0001, seq=26/6656, ttl=12			
	11 3.817540	192.168.1.12	192.168.1.11	ICMP	74 Echo (ping) reply id=	0x0001, seq=26/6656, ttl=12			
	13 4.831343	192.168.1.11	192.168.1.12	ICMP	74 Echo (ping) request id=	0x0001, seq=27/6912, tt]=12			
	14 4.832006	192.168.1.12	192.168.1.11	ICMP	74 Echo (ping) reply id=	0x0001, seq=27/6912, ttl=12			
	15 5.844858	192.168.1.11	192.168.1.12	ICMP	74 Echo (ping) request id=	0x0001, seq=28/7168, tt]=12			
	16 5.845488	192.168.1.12	192.168.1.11	ICMP	74 Echo (ping) reply id=	0x0001, seq=28/7168, ttl=12			
_									
E F	rame 13: 74 b	ytes on wire (592 bits), 74 bytes ca	ptured (592	bits)	1 . (0)			
U	Destinations	Tetol Of Of . 01	+:92:16 (58:94:66:34:9	2:1C), DST:	Incer_07:91:48 (00:11:11:07:9	1:48)			
	Destination:	Intel_07:91:00	(00:11:11:0F:91:48)*)					
+	Source: IntelCor_34:92:10 (58:94:6b:34:92:10) Source: IntelCor_34:92:10 (58:94:6b:34:92:10)								
	Type: IP (0x	(0800)	Spc: 102 168 1 11 (10	1 1 6 0 1 11	Dot: 102 168 1 12 (102 168 1	12)			
	ternet Proto	ol Mossago Prot	51C. 192.108.1.11 (19	,2.100.1.11)	, DSC. 192.100.1.12 (192.108.1	.12)			
± 1	icernet contr	or Message Pro							

Совпадает ли МАС-адрес источника с интерфейсом вашего компьютера?

Совпадает ли MAC-адрес назначения в программе Wireshark с MAC-адресом другого учащегося?

Как ваш ПК вычислил MAC-адрес ПК, на который был отправлен эхо-запрос с помощью команды ping?

Примечание. В предыдущем примере перехваченного ICMP-запроса данные протокола ICMP инкапсулируются внутри PDU-пакета IPv4 (заголовка IPv4), который затем инкапсулируется в пакете кадра Ethernet II (заголовок Ethernet II) для передачи по локальной сети.

Часть 3: Сбор и анализ данных протокола ICMP по удалённым узлам в программе Wireshark

В части 3 вы должны будете отправить эхо-запросы с помощью команды ping на удалённые узлы (узлы за пределами локальной сети) и изучить данные, сформированные этими запросами. Затем вы определите различия между этими данными и данными, изученными в части 2.

Шаг 1: Запустите перехват данных в интерфейсе.

а. Нажмите на значок Interface List (Список интерфейсов), чтобы снова открыть список интерфейсов ПК.



b. Убедитесь в том, что напротив интерфейса локальной сети установлен флажок, и нажмите кнопку **Start** (Начать).

🥖 Wireshark: Capt	ture Interfaces				- • •
	Description	IP	Packets	Packets/s	
	Intel(R) PRO/1000 MT Network Connection		19	0	<u>D</u> etails
	Intel(R) 82577LM Gigabit Network Connection	192.168.1.11	47	0	<u>D</u> etails
1 -					
<u>H</u> elp		Start	Stop	<u>O</u> ptions	<u>C</u> lose

с. Появится окно с предложением сохранить полученные ранее данные перед началом нового перехвата. Сохранять эти данные необязательно. Нажмите кнопку Continue withoutSaving (Продолжить без сохранения).



- d. Активировав перехват данных, отправьте эхо-запрос с помощью команды ping на следующие три URL-адреса:
 - 1) www.yahoo.com
 - 2) www.cisco.com
 - 3) www.google.com

C:\Windows\system32\cmd.exe	_ • ×
C:\>ping www.yahoo.com	· · · · · · · · · · · · · · · · · · ·
Обмен пакетами с учулуароо.com [72.30.38.140] с 32 байтами данных: Ответ от 72.30.38.140:число байт=32 время=1ms TTL=255 Ответ от 72.30.38.140:число байт=32 время<1ms TTL=255 Ответ от 72.30.38.140:число байт=32 время<1ms TTL=255 Ответ от 72.30.38.140:число байт=32 время<1ms TTL=255	
Статистика Ping для 72.30.38.140: Пакетов: отправлено = 4, получено = 4, потеряно = 0 (0% потерь), Приблизительное время приема-передачи в мс: Минимальное = Омсек, Максимальное = 1мсек, Среднее = Омсек	=
C:\>ping www.cisco.com	
Обмен пакетами с www.cisco.com [198.133.219.25] с 32 байтами данных: Reply 198.133.219.25: число байт =32 время<1ms TTL=255 Reply 198.133.219.25: число байт =32 время<1ms TTL=255	
Статистика Ping для 198.133.219.25: Пакетов: отправлено = 4, получено = 4, потеряно = 0 (0% потерь), Приблизительное время приема-передачи в мс: Минимальное = Омсек, Максимальное = Омсек, Среднее = Омсек	
C:\>ping www.google.com	
Обмен пакетами с www.google.com [74.125.129.99] с 32 байтами данных: Ответ от 74.125.129.99: число байт =32 время=1ms TTL=255 Ответ от 74.125.129.99: число байт =32 время<1ms TTL=255 Ответ от 74.125.129.99: число байт =32 время<1ms TTL=255 Ответ от 74.125.129.99: число байт =32 время<1ms TTL=255	
Статистика Ping для 74.125.129.99: Пакетов: отправлено = 4, получено = 4, потеряно = 0.(0% потерь), Приблизительное время приема-передачи в мc:ds: Минимальное = Омсек, Максимальное = 1мсек, Среднее = Омсек	
C:\>_	

Примечание. При отправке эхо-запросов с помощью команды ping на указанные URL-адреса обратите внимание на то, что служба доменных имен (DNS) преобразует URL в IP-адрес. Запишите IP-адреса, полученные для каждого URL-адреса.

е. Остановите перехват данных, нажав на значок Stop Capture (Остановить перехват).



Шаг 2: Изучите и проанализируйте данные, полученные от удалённых узлов.

а. Просмотрите собранные данные и изучите IP- и MAC-адреса трёх запрошенных веб-сайтов. Ниже укажите IP- и MAC-адреса назначения для всех трех веб-сайтов.



- b. Какова особенность этих данных?
- с. Как эта информация отличается от данных, полученных в результате эхо-запросов локальных узлов в части 2?

Вопросы на закрепление

Почему программа Wireshark показывает фактический МАС-адрес локальных узлов, но не фактический МАС-адрес удалённых узлов?

Приложение А. Пропуск трафика ІСМР через брандмауэр

Если эхо-запросы с помощью команды ping с других компьютеров не проходят на ваш ПК, возможно, их блокирует брандмауэр. В этом приложении описывается, как пропустить эхо-запросы с помощью команды ping через брандмауэр и отменить новое правило брандмауэра по завершении лабораторной работы.

Шаг 1: Создайте новое правило, разрешающее прохождение ICMP-трафика через брандмауэр.

а. В панели управления выберите пункт Система и безопасность.



b. В окне «Система и безопасность» выберите Брандмауэр Windows.



с. В левой части окна «Брандмауэр Windows» выберите Дополнительные параметры.



d. В окне «Дополнительные параметры» выберите в левой боковой панели **Правила для входящих** подключений, а затем **Создать правило...** в правой боковой панели.

💣 Брандмауэр Windows в режиме	повышенной безопасности				
Файл Действие Вид Справи	ca				
🗢 🄿 🞽 🖬 😖 👔 🖬					
🔗 Брандмауэр Windows в режим	Правила для входящих подключений				Действия
Правила для входящих по	Имя	Группа	Профиль	Включен 🔦	Правила для входящих подключен 🔺
Правила для исходящего п Правила безопасности по,	🕑 Удаленный помощник (сервер удален	Удаленный помощник	Домен	Да _	🗽 Создать правило
Наблюдение	🕑 Удаленный помощник (протокол PNR	Удаленный помощник	Общие	Да	Фильтровать по профилю
	🕑 Удаленный помощник (протокол PNR	Удаленный помощник	Домен, Ч	Да	
	Удаленный помощник (ТСР - входящий)	Удаленный помощник	Общие	Да	
	Удаленный помощник (ТСР - входящий)	Удаленный помощник	Домен, Ч	Да	🛛 🖓 Фильтровать по группе 🔹 🕨
	🕑 Удаленный помощник (SSDP UDP - вхо	Удаленный помощник	Домен, Ч	Да	Вид
	🕑 Удаленный помощник (SSDP TCP - вхо	Удаленный помощник	Домен, Ч	Да	Обновить
	🔇 Удаленный помощник (DCOM - входя	Удаленный помощник	Домен	Да	
	🔘 Удаленное управление томами (RPC	Удаленное управление то	Частный,	Нет	📑 Экспортировать список
	🔘 Удаленное управление томами (RPC	Удаленное управление то	Домен	Нет	? Справка
		Vазленное управление то	Цастиній	Her	

е. Откроется мастер создания новых правил для входящих подключений. В окне «Тип правила» установите переключатель **Настраиваемые**, и нажмите кнопку **Далее.**

💣 Мастер создания правила	для нового входящего подключения						
Тип правила							
Выберите тип правила брандма	Выберите тип правила брандмаузра, которое требуется создать.						
Шаги:							
🧼 Тип правила	Правило какого типа вы хотите создать?						
🥘 Программа							
🧉 Протокол и порты	Для программы						
🕘 Область	Правило, управляющее подключениями для программы.						
Действие	Для порта						
🥘 Профиль	Правило, управляющее подключениями для порта ТСР или UDP.						
🧼 Имя	Предопределенные						
	BranchCache - обнаружение кэширующих узлов (использует WSD) 🔻						
	Правило, управляющее подключениями для операций Windows.						
	Настраиваемые						
	Настраиваемое правило.						
	Подробнее о типах правил						
	\frown						
	< Назад (Далее >) Отмена						

f. В левой панели выберите **Протоколы и порты** и выберите пункт **ICMPv4** в раскрывающемся меню типов протокола. После этого нажмите кнопку **Далее**.

🔗 Мастер создания правила	для нового входящего подк	лючения
Протокол и порты		
Укажите протоколы и порты, к	которым применяется данное	правило.
Шаги:		
🧉 Тип правила	Укажите порты и прото	колы, к которым применяется это правило.
Программа		
Протокол и порты	Тип протокола:	Любой 👻
Область	Номер протокола:	Любой Настроить
Действие		HORDET
Профиль	Локальный порт:	
• Имя	Удаленный порт:	ICP UDP IPv6 IPv6-Route IPv6-Route IPv6-Frag GRE ICMPv6 IPv6-NoNbd IPv6-Opts
	Параметры протокола	VRRP PGM
	Дополнительные свед	Ц <u>2ТР</u> ения о протоколах и портах < Назад Далее > Отмена

© Корпорация Cisco и/или её дочерние компании, 2014. Все права защищены.

В данном документе содержится общедоступная информация корпорации Cisco.

g. В левой панели выберите **Имя** и введите в соответствующее поле **Allow ICMP Requests.** Нажмите кнопку **Finish** (Готово).

劒 Мастер создания правил	а для нового входящего подключения	×
Имя		
Укажите имя и описание данн	юго правила.	
Шаги:		
🧿 Тип правила		
🥘 Программа		
🧼 Протокол и порты		
🥚 Область	Allow ICMP Requests	
Действие		
• Профиль	Описание (необязательно):	
RWN		
	\frown	
	< Назад (Готово) Отме	на

Созданное правило позволит другим учащимся получать эхо-отклики с вашего ПК.

Шаг 2: Отключите и удалите новое правило ІСМР.

По завершении лабораторной работы необходимо отключить или удалить новое правило, созданное в шаге 1. Вариант **Отключить правило** позволит снова включить его при необходимости. Полное удаление правила навсегда удалит его из списка правил для входящих подключений.

а. В левой части окна «Дополнительные настройки безопасности» выберите **Правила для входящих** подключений и найдите правило, созданное в шаге 1.

Лабораторная работа: просмотр сетевого трафика с помощью программы Wireshark

🔗 Брандмауэр Windows в режиме повышенной безопасности			
Файл Действие Вид Справка			
🗢 🔿 🔁 🗊 🖹 👔			
😭 Брандмауэр Windows в режии Правила для входящих под	ключений		Действия
Правила для входящих под Имя	Группа	Профиль Включен ^	Правила для входящих подключен 🔺
Правила для исходящего Allow ICMP Requests	>	Все Да 😑	🚉 Создать правило
 Наблюдение Удаленный помощник (пр Удаленный помощник (пр Удаленный помощник (пр Удаленный помощник (Пр Удаленный помощник (Пр Удаленный помощник (Sp Удаленный помощник (Sp Удаленный помощник (Sp Удаленный помощник (Dp Удаленный помощник (Dp) 	рвер удален Удаленный помощник удаленный помощник ротокол PNR Удаленный помощник ротокол PNR Удаленный помощник СР - входящий) Удаленный помощник DP UDP - вхо Удаленный помощник DP UDP - вхо Удаленный помощник COM - входя Удаленное управление то Удаленное управление то	Домен Да Общие Да Домен, Ч Да Общие Да Домен, Ч Да Домен, Ч Да Домен, Да Частный, Нет	 Фильтровать по профилю Фильтровать по состоянию Фильтровать по сруппе Фильтровать по группе Вид Фольтровать по сруппе Вид Обновить Экспортировать список Горавка
Удаленное управление то Удаленное управление то Удаленное управление то Удаленное управление то Удаленное управление то Удаленное управление сл Удаленное управление сл	мами (RPC Удаленное управление то мами - служ Удаленное управление то мами - служ Удаленное управление то мами - загру Удаленное управление то удаленное управление то ужбой (имен Удаленное управление слу ужбой (имен Удаленное управление слу Удаленное управление слу	Домен Нет Частный, Нет Домен Нет Частный, Нет . Частный, Нет . Домен Нет Домен Нет	Аllow ICMP Requests

b. Чтобы отключить правило, выберите вариант Отключить правило. После этого она изменится на вариант Включить правило. Правило можно включать и отключать. Состояние правила отображается в столбце «Включено» списка правил для входящих подключений.

😭 Брандмауэр Windows в режиме повышенной безопасности 🗖 🖻 🔀									
Файл Действие Вид Справка									
🗢 🧼 🖄 🖬 😖 🚺 🗊									
🔗 Брандмауэр Windows в режим	Правила для входящих подключений				Действия				
式 Правила для входящих по,	Имя	Группа	Профиль Включе	10 A	Правила для входящих подключен 🔺				
Правила для исходящего г	Allow ICMP Requests		Все Да		Создать правидо				
 Правила безопасности по, Наблюдение 	Удаленный помощник (сервер удален	Удаленный помощник	Домен Да	Ξ					
	🕑 Удаленный помощник (протокол PNR	Удаленный помощник	Общие Да		у фильтровать по профилю				
	🔇 Удаленный помощник (протокол PNR	Удаленный помощник	Домен, Ч Да		Фильтровать по состоянию				
	🕑 Удаленный помощник (TCP - входящий)	Удаленный помощник	Общие Да		🝸 Фильтровать по группе 🕨 🕨				
	🕑 Удаленный помощник (TCP - входящий)	Удаленный помощник	Домен, Ч Да		Вид				
	🕑 Удаленный помощник (SSDP UDP - вхо	Удаленный помощник	Домен, Ч Да		О Обновить				
	🔮 Удаленный помощник (SSDP TCP - вхо	Удаленный помощник	Домен, Ч Да						
	🔮 Удаленный помощник (DCOM - входя	Удаленный помощник	Домен Да		Экспортировать список				
	Удаленное управление томами (RPC	Удаленное управление	Частный, Нет		🛿 Справка				
	Удаленное управление томами (RPC	Удаленное управление	Домен Нет		Allow ICMP Requests				
	Удаленное управление томами - служ	Удаленное управление	Частный, Нет		Allow Ichir Requests =				
	Удаленное управление томами - служ	Удаленное управление	Домен Нет	•	• Отключить правило				
	Удаленное управление томами - загру	Удаленное управление	Домен Нет		🔏 Вырезать				
	Удаленное управление томами - загру	Удаленное управление	Частный, Нет		🖹 Копировать				
	Удаленное управление службой (имен	Удаленное управление	Частный, Нет		У Харить				
	🐨 Удаленное управление службой (имен	Удаленное управление	Домен Нет		л здалить				

с. Чтобы удалить правило ICMP навсегда, выберите вариант **Удалить**. После этого для разрешения запросов ICMP это правило нужно будет создать заново.

ие	частный,	nei -		👔 Справка
ие	Домен	Нет		
ие	Частный,	Нет		Allow ICMP Requests
ие	Домен	Нет	6	Отключить правило
ие	Домен	Нет		🐇 Вырезать
ие	Частный,	Нет		Копировать
ие	Частный,	Нет		Konnposans
ие	Домен	Нет	$\langle \downarrow \rangle$	🗙 Удалить 🥏
ие	Ломен	Нет	6	П Свойства

© Корпорация Cisco и/или её дочерние компании, 2014. Все права защищены. В данном документе содержится общедоступная информация корпорации Cisco.