Лабораторна робота №6

Тема: Протокол мережевого рівня IP.
Мета: Навчитися аналізувати пакети даних протоколу IP (за допомогою програмних засобів аналізу пакетів даних – програми-сніфера Wireshark).

Питання до вивчення

1. Протокол мережевого рівня IP.
2. Аналіз пакетів протоколу IP засобами програми Wireshark.
3. Аналіз фрагментації пакетів.

Короткі теоретичні відомості

Для ознайомлення з інтерфейсом програми Wireshark скористайтесь документом «Аналізатор пакетів Wireshark» або документацією користувача «Wireshark User's Guide».

Лабораторна робота виконується на основі аналізу IP-дейтаграм, відправлених та отриманих під час виконання програми **traceroute**.

Нагадаємо, що **traceroute** спочатку відправляє заданому адресату одну або кілька IP-дейтаграм з часом життя (TTL) у полі заголовку, встановленим в 1; потім вона посилає серію з одного або кількох дейтаграм до того ж одержувача з TTL = 2 , далі – серію дейтаграм з TTL = 3, і так далі. Кожний маршрутизатор зменшує поле TTL заголовку на одиницю і передає дейтаграму далі. Якщо значення TTL досягає нуля, маршрутизатор повертає ICMP-повідомлення (тип 11 – перевищення TTL) хосту-відправнику.

Завдання:

1. Запустіть програму Wireshark. Відкрийте файл із записом пакетів протоколів «ip-ethereal-trace-1», у якому збережені
2. Виберіть перше повідомлення ICMP Echo Request, відправлене вашим комп'ютером, і розгорніть у вікні подробиць пакетів протокол Internet Protocol.
3. Дайте відповіді на питання:
   a) Яка IP-адреса комп'ютера відправника?
   b) Яке значення поля «протокол вищого рівня» у заголовку пакету IP?
   c) Скільки байтів має заголовок IP?
   d) Скільки байтів має поле даних дейтаграми IP? Поясніть, як ви визначили кількість байтів корисного навантаження.
   e) Чи була ця IP-дейтаграма фрагментована? Поясніть, як ви визначили, чи була дейтаграма фрагментована.
4. Далі відсортуйте пакети за IP-адресою джерела, клацнувши на заголовку стовпчика Джерело (Source), поряд із словом Source повинна з'явитися маленька стрілочка вниз. Якщо стрілка вказує вгору, клацніть по заголовку стовпчика Джерело знову. Виберіть перше повідомлення ICMP Echo Request, відправлене вашим комп'ютером, і розгорніть у вікні подробиць пакетів протокол Internet Protocol. У вікні «списку захоплених пакетів» нижче від цього першого ICMP ви повинні побачити всі наступні повідомлення ICMP (можливо, перемішані з пакетами від інших протоколів, що працюють на комп'ютері). Використовуйте стрілку вниз на клавіатурі для переміщення по повідомленнях ICMP, відправлених вашим комп'ютером. Дайте відповіді на питання:
   a) Які поля IP-дейтаграм завжди змінюються від однієї дейтаграми до іншої в рамках серії повідомлень ICMP, відправлених комп'ютером?
   b) Які поля залишаються незмінними? Які поля повинні залишатися постійними? Які поля повинні змінитися? Чому?

Далі (в пакетах, відсортованих за адресою відправника) знайдіть серію ICMP-відповідей із перевищенням TTL, прийнятих комп'ютером від найближчого маршрутизатора. Дайте відповіді на питання:

a) Які значення стоять у полі ідентифікатора і полі TTL?
b) Чи ці значення залишаються незмінними для всіх ICMP-відповідей із перевищенням TTL, прийнятих комп'ютером від найближчого маршрутизатора? Чому?

5. Знайдіть перший фрагмент у фрагментованих IP-дейтаграмах (наприклад, пакет № 130).
   a) Яка інформація у заголовку IP означає, що дейтаграма була фрагментована?
   b) Яка інформація у заголовку IP вказує, що це є перший фрагмент у порівнянні з наступними фрагментами?
   c) Яку довжину має ця IP-дейтаграма?
6. Вивести другий фрагмент фрагментованих IP-дейтаграм.
   a) Яка інформація у заголовку IP показує, що це не перший фрагмент дейтаграм?
   b) Чи є ще фрагменти? Як ви можете про це дізнаться?
   c) Яке поле змінюється в IP-заголовку між першим і другим фрагментами?

Література

3. Куроуз Дж. Компьютерные сети. Многоуровневая архитектура Интернета / Дж. Куроуз, К. Росс. – СПб. : Питер, 2004. – С. 329–348 с.
4. Олифер В.Г. Компьютерные сети. Принципы, технологии, протоколы : учебник для вузов / В.Г. Олифер, Н.А. Олифер. – 3-е изд. – СПб. : Питер, 2006. – С. 598–602, 633–638 с.
5. Руководство по технологиям объединенных сетей : пер. с англ. / Cisco Systems Inc. – 4-е изд. – М. : Издательский дом «Вильямс», 2005. – С. 579–589 с.

Лабораторна робота №7

Тема: Протокол динамічної конфігурації хоста DHCP.
Мета: Навчитися аналізувати пакети даних протоколу DHCP (за допомогою програмних засобів аналізу пакетів даних – програми-сніфера Wireshark).

Питання до вивчення

1. Протокол динамічної конфігурації хоста DHCP.
2. Аналіз пакетів протоколу DHCP засобами програми Wireshark.

Короткі теоретичні відомості

Для ознайомлення з інтерфейсом програми Wireshark скористайтесь документом «Аналізатор пакетів Wireshark» або документацією користувача «Wireshark User's Guide».

Лабораторна робота виконується на основі аналізу пакетів, відправлених та отриманих комп'ютером під час автоматичного одержання динамічної IP-адреси. При цьому використовуються команди командного рядка "ipconfig /release" та "ipconfig /renew".

Завдання до виконання

1. Ознайомтеся із протоколом DHCP.
2. Запустіть програму Wireshark. Відкрийте файл із записом пакетів протоколів «dhcp-ethereal-trace-1».
3. Для того, щоб відобразити лише пакети протоколу DHCP, наберіть **bootp** у полі фільтра і натисніть кнопку Apply.
4. Під час одержання динамічної IP-адреси генеруються чотири пакети: DHCP Discover (пошук), DHCP Offer (пропозиція), а DHCP Request (запит) та DHCP ACK (підтвердження).
5. Проаналізуйте вищеназвані пакети і дайте відповіді на питання:
   a) Повідомлення DHCP пересилаються через UDP чи TCP?
   b) Яка MAC-адреса комп'ютера-клієнта?
   c) Які значення повідомлення DHCP Discover відрізняють його від повідомлення DHCP Request?
   d) Які значення має ідентифікатор транзакції Transaction-ID для кожного з чотирьох перших повідомлень?
   e) Які значення IP-адреси відправника та одержувача використовуються у кожному із чотирьох перших повідомлень?
   f) Яка адреса вашого DHCP-сервера?
   g) Яку адресу запропонував DHCP-сервер вашому комп'ютеру? Яке повідомлення передало цю адресу?
   h) Для чого призначене повідомлення-запит DHCP Request?
   i) Що таке час оренди IP-адреси?
   j) Яке призначення повідомлення DHCP Release?

Література

1. Олифер В.Г., Олифер Н.А. Компьютерные сети. Принципы, технологии, протоколы : учебник для вузов. – 3-е изд. – СПб. : Питер, 2006. – С. 590–594.

Лабораторна робота №8

(4 години)

Тема: Аналіз пакетів даних протоколів Ethernet та ARP.

Мета: Навчитися аналізувати пакети даних протоколів Ethernet та ARP (за допомогою програмних засобів аналізу пакетів даних – програми-сніфера Wireshark).

Питання до вивчення

1. Аналіз пакетів протоколу Ethernet.
2. Аналіз пакетів протоколу ARP.

Короткі теоретичні відомості

Для ознайомлення з інтерфейсом програми Wireshark скористайтесь документом «Аналізатор пакетів Wireshark» або документацією користувача «Wireshark User's Guide».

Завдання до виконання

1. Запустіть програму Wireshark.
2. Відкрийте файл із записом пакетів протоколів «ethernet-ethereal-trace-1». Це запис сеансу одержання Інтернет-сторінки http://gaia.cs.umass.edu/wireshark-labs/HTTP-ethereal-lab-file3.html.
3. Оскільки нас цікавлять протоколи Ethernet і ARP, можна змінити список перехоплених протоколів так, щоб він містив лише протоколи рівнів нижче IP. Для цього вибирають пункт меню Analyze → Enabled Protocols (Аналіз → Дозволені протоколи) і знімають прапорець протоколу IP.
4. Виберіть Ethernet фрейм, що містить повідомлення HTTP GET. Розгорніть інформацію Ethernet II у вікні подробиць пакету. Зверніть увагу, що вміст кадру Ethernet (заголовок та дані) відображаються у вікні вмісту пакету. Дослідіть вікна подробиць заголовку пакета та вмісту пакетів (середнє і нижнє вікна Wireshark).
5. Дайте відповіді на наступні питання, виходячи зі змісту Ethernet-кадру, що містить повідомлення HTTP GET.
   a) Яка 48-бітна Ethernet-адреса відправника (вашого комп'ютера)?
   b) Яка 48-бітна адреса призначення в Ethernet кадрі? Це Ethernet-адреса сервера gaia.cs.umass.edu? Що за пристрій має цю Ethernet-адресу?
   c) Визначте шістнадцяткове значення двобайтового поля типу кадру.
   d) Скільки байт від самого початку кадру Ethernet до літери "G" у слові "GET"? Чому так багато?
6. Дослідіть кадр Ethernet який надійшов у відповідь. Дайте відповіді на наступні питання.
   e) Яке значення Ethernet-адреси відправника? Це адреса вашого комп'ютера, чи сервера gaia.cs.umass.edu?. Відповідь аргументуйте. Що за пристрій має цю Ethernet-адресу?
   f) Яка адреса призначення в Ethernet кадрі? Це Ethernet-адреса Вашого комп'ютера?
   g) Визначте шістнадцяткове значення двобайтового поля типу кадру.
   h) Скільки байт від самого початку кадру Ethernet до літери "O" в слові "OK"?
7. Дослідіть перших два кадри даних, що містять повідомлення протоколу ARP. Дайте відповіді на наступні питання:
   i) Які шістнадцяткові значення адрес відправника і одержувача в Ethernet-фреймі, що містить запит протоколу ARP?
   j) Визначте шістнадцяткове значення двобайтового поля типу Ethernet-кадру.
   k) Скільки байт від самого початку кадру Ethernet до поля коду операції ARP?

l) Яке значення поля коду операції кадру Ethernet із ARP-запитом?
m) Чи повідомлення ARP містить адресу IP відправника?
n) Де у запиті ARP міститься "питання" про Ethernet адресу вузла, яка відповідає заданій IP адресі?

8. Знайти ARP-відповідь, яку було надіслано на запит ARP. Дайте відповіді на питання?
   o) Скільки байт від початку кадру Ethernet до поля коду операції ARP?
   p) Яке значення поля коду операції в Ethernet кадрі, що містить відповідь на запит ARP?
   q) Де в повідомленні ARP міститься "відповідь" із MAC-адресою, що відповідає запиту із IP-адресою?
   r) Які шістнадцяткові значення адрес відправника і одержувача в Ethernet-фреймі, що містить відповідь на ARP-запит?

Література

1. Олифер В.Г., Олифер Н.А. Компьютерные сети. Принципы, технологии, протоколы : учебник для вузов. – 3-е изд. – СПб. : Питер, 2006. – С. 383–424.