3. Протокол DNS

Мета роботи: аналіз деталей роботи протоколу DNS.

3.1. Теоретичні відомості

Система доменних імен (DNS), яка переводить імена хостів в IP адреси, виконує важливу роль в інфраструктурі Інтернету. У цій роботі ми будемо аналізувати роботу клієнта DNS. Нагадаємо, що роль клієнта в DNS досить проста - клієнт відправляє запит до свого локального DNS-сервера, і отримує відповідь. З точки зору клієнта деякі деталі роботи протоколу DNS не можливо проаналізувати. Так, наприклад, ієрархічні сервери DNS можуть спілкуватися один з одним, аби рекурсивно або ітеративно виконати DNS запити клієнтів. Тому, з погляду клієнтів DNS, цей протокол є досить простим – ми зможемо проаналізувати запит, сформульований на локальний DNS-сервер та отриману відповідь від сервера.

Рекомендується ознайомитися з такими концепціями:

- ✓ локальні сервери DNS;
- ✓ кешування DNS-записів і повідомлень;
- ✓ тип поля в записі DNS.

3.2. Хід роботи

Необхідно виконати наступні дії:

1. Очистіть кеш DNS-записів
    a. для windows-систем виконайте в терміналі
    ipconfig /flushdns
    b. для linux-систем (можливо) спрацює перезапуск операційної системи;
2. Запустіть веб-браузер, очистіть кеш браузера:
    a. для Firefox виконайте
    Tools >> Clear Private Data (або Ctrl + Shift + Del)
    b. для MS IE виконайте
    Tools >> Internet Options >> Delete File
3. Запустіть Wireshark, почніть захоплення пакетів.
4. Відкрийте за допомогою браузера одну із зазначених нижче адрес:
   http://www.ietf.org
5. Зупиніть захоплення пакетів.
6. Перегляньте деталі захоплених пакетів. Для цього налаштуйте вікно деталей пакету: згорніть деталі протоколів усіх рівнів крім DNS (за допомогою знаків +/-).
7. Приготуйте відповіді на контрольні запитання 1-6, роздрукуйте необхідні для цього пакети.
8. Почніть захоплення пакетів.
9. Виконайте nslookup для домену www.mit.edu за допомогою команди
    a. nslookup www.mit.edu
10. Зупиніть захоплення пакетів.
11. Приготуйте відповіді на контрольні запитання 7-10, роздрукуйте необхідні для цього пакети. Утиліта nslookup відправляє три запити та отримує три відповіді, така поведінка є специфічною, тому слід ігнорувати перші два запити та перші дві відповіді.
12. Почніть захоплення пакетів.
13. Виконайте nslookup для домену www.mit.edu за допомогою команди
    a. nslookup –type=NS mit.edu

14. Зупиніть захоплення пакетів.
15. Приготуйте відповіді на запитання 11-13. При необхідності роздрукуйте деякі захоплені пакети.
16. Почніть захоплення пакетів.
17. Виконайте nslookup для домену www.mit.edu за допомогою команди
    a. nslookup www.aiit.or.kr bitsy.mit.edu
18. Зупиніть захоплення пакетів.
19. Приготуйте відповіді на запитання 14-16. При необхідності роздрукуйте деякі захоплені пакети.
20. Закрийте Wireshark.

3.3. Контрольні запитання

Форма звітності: роздруківки збережених в ході ЛР пакетів з фаміліями, ініціалами та групами виконавців (бажано на кожній сторінці).

Контрольні запитання:

1. Знайдіть запит та відповідь DNS, який протокол вони використовують, UDP або TCP? Який номер цільового порта запиту DNS? Який номер вихідного порта відповіді DNS?
2. На який адрес IP був відправлений запит DNS? Чи є цей адрес адресом локального сервера DNS?
3. Проаналізуйте повідомлення із запитом DNS. Якого «Типу» цей запит? Чи вміщує цей запит деякі можливі компоненти «відповіді»?
4. Дослідіть повідомлення із відповіддю DNS. Яка кількість відповідей запропонована сервером? Що вміщує кожна з цих відповідей?
5. Проаналізуйте повідомлення TCP SYN, яке відправила ваша робоча станція після отримання відповіді сервера DNS. Чи співпадає цільова IP адреса цього повідомлення з одною із відповідей сервера DNS?
6. Чи виконує ваша робоча станція нові запити DNS для отримання ресурсів, які використовує документ, що отримав браузер?
7. Яким був цільовий порт повідомлення із запитом DNS? Яким був вихідний порт повідомлення із відповіддю DNS?
8. На яку IP-адресу був направлений запит DNS? Чи є ця адреса адресою вашого локального сервера DNS за замовчанням?
9. Дослідіть повідомлення із запитом DNS. Якого «типу» був цей запит? Чи вміщує цей запит деякі можливі компоненти «відповіді»?
10. Дослідіть повідомлення із відповіддю DNS. Скільки записів із відповідями було запропоновано сервером? З чого складається кожна із цих відповідей?
11. На яку IP-адресу був направлений запит DNS? Чи є ця адреса адресою вашого локального сервера DNS за замовчанням?
12. Дослідіть повідомлення із запитом DNS. Якого «типу» був цей запит? Чи вміщує цей запит деякі можливі компоненти «відповіді»?
13. Дослідіть повідомлення із відповіддю DNS. Скільки записів із відповідями було запропоновано сервером? Які сервери DNS були запропоновані у відповіді? Сервери були запропоновані за допомогою доменного імені, адреси IP або й того й іншого?
14. На яку IP-адресу був направлений запит DNS? Чи є ця адреса адресою вашого локального сервера DNS за замовчанням? Якщо ні, то якому доменному імені відповідає ця IP-адреса?
15. Дослідіть повідомлення із запитом DNS. Якого «типу» був цей запит? Чи вміщує цей запит деякі можливі компоненти «відповіді»?
16. Дослідіть повідомлення із відповіддю DNS. Скільки записів із відповідями було запропоновано сервером? З чого складається кожна з цих відповідей?