Лабораторна робота №4. Вивчення структури та вмісту IP-пакетів

Тема: Вивчення структури та вмісту IP-пакетів.

Мета: За допомогою аналізатора Wireshark вивчити структуру та типи кадрів у комп'ютерній мережі.

Теоретична частина

Протокол IP описано у стандарті RFC 791. Основне призначення цього протоколу – передавання пакетів (дейтаграм) між мережами. У протоколі IP відсутні механізми попереднього встановлення з'єднання та підтвердження доставки. При виявлені помилки у пакеті протокол IP не забезпечує будь-яких дій щодо його повторного передавання. Важливою особливістю протоколу IP (на відміну від IPX) є динамічна фрагментація-дефрагментація пакетів при передавані їх між мережами, в яких різне максимально можливе значення довжини поля даних кадрів (Maximum Transfer Unit – MTU). При цьому, фрагментацію виконує маршрутизатор, що знаходиться на шляху руху пакету, якщо він передає пакет до мережі із меншим значенням MTU, а відновлення (збирання) пакету робить вузол-отримувач. Такий підхід дозволяє відправляти фрагменти за незалежними маршрутами.

<table>
<tr><td>Біти</td><td>0-3</td><td>4-7</td><td>8-15</td><td colspan="2">16-31</td></tr>
<tr><td>0-31</td><td>Версія IP</td><td>Довжина заголовку</td><td>Тип обслуговування</td><td colspan="2">Загальна довжина IP пакету</td></tr>
<tr><td>32-63</td><td colspan="3">Ідентифікація фрагмента</td><td>Прапорці (3 біти)</td><td>Зміщення фрагменту (13 бітів)</td></tr>
<tr><td>64-95</td><td colspan="2">TTL (час використання)</td><td>Протокол верхнього рівня</td><td colspan="2">Контрольна сума IP-пакету</td></tr>
<tr><td>96-127</td><td colspan="5">IP адреса відправника</td></tr>
<tr><td>128-159</td><td colspan="5">IP адреса отримувача</td></tr>
<tr><td>160-191</td><td colspan="5">Опції (необов'язкові) та заповнювач (за потреби)</td></tr>
<tr><td>192-...</td><td colspan="5">Корисні дані (максимальне значення - 65535 байтів мінус довжина заголовку)</td></tr>
</table>

Рис.1 Загальна структура IP пакету

IP-пакет складається із заголовку (у більшості випадків це 20 байт) та поля даних, максимальна довжина пакету - заголовок + дані складає 65535 байт, а мінімальна – визначається мінімальним розміром кадру канального рівня, який переносить IP-пакет кадру канального рівня (для Ethernet 64 байти).

Поле "Номер версії" (Version) вказує версію протоколу IP. Зараз широко використовується IP-протокол 4 версії (IPv4), а також паралельно, у більшості випадків, забезпечується підтримка IP-протоколу версії 6 (IPv6).

Поле "Довжина заголовку" (IHL) вказує значення довжини заголовку IP-пакету у 32-бітних (4-байтових) словах. Зазвичай довжина заголовку складає 5

таких слів, але може бути більшою за рахунок додаткових байт у полі “Опції” (максимальна довжина заголовку - 60 байт або 15 4-байтових слів).

Перші три біти поля “Тип сервісу” (Type of Service) (біти 0-2) задають пріоритет пакету від самого низького 000 (звичайний пакет) до самого високого 111 (пакет з інформацією керування). Біти 3-5 визначають критерій вибору маршруту, який використовується у протоколах маршрутизації OSPF (Open Shortest Path First) та BGP (Border Gateway Protocol). Реально вибір відбувається між трьома альтернативами: малою затримкою (біт 3 Delay = 1), високою пропускною здібністю (біт 4 Throughput = 1) та високою достовірністю (біт 5 Reliability = 1). Зазвичай покращення одного параметру викликає погіршення іншого, тому обирається один критерій вибору маршруту.

Поле “Загальна довжина” (Total Length) вміщує загальну довжину IP-пакету разом із заголовком. Виходячи з розрядності поля (2 байти) максимальною довжиною пакету є 65535 байт. Великі пакети використовуються рідко, навіть при пересиланні файлів та потокового відео. Зазвичай розмір пакету обирається з урахуванням максимального полю даних кадру канального рівня (MTU). Для Ethernet MTU складає 1500 байт, для FDDI MTU – 4096 байт.

При перенаправлені IP-пакета з однієї мережі в іншу маршрутизатор може зустрітись з проблемою різних значень MTU у суміжних мережах. У цьому випадку йому необхідно виконати фрагментацію пакету (тобто розбивання на декілька пакетів) при передаванні у мережу з меншим значенням MTU та дефрагментацію (об’єднання декількох пакетів у один) при передаванні пакету у мережу з великим значенням MTU. З метою розпізнавання пакетів, утворених у результаті фрагментації, використовується поле “Ідентифікатор пакета” (Identification).

Усі фрагменти фрагментованого пакету мають однакове значення цього поля. Поле “Прапорці” (Flags) має такі біти: 0 біт є резервним і його значення 0, 1 біт - DF - Do not Fragment у випадку встановлення у 1 забороняє фрагментацію пакету, 2 біт - MF - More Fragments при встановлені у 1 вказує, що пакет є проміжним (не останнім) фрагментом.

У полі “Зміщення фрагмента” (Fragment Offset) вказується зміщення у 8-байтних блоках поля даних цього пакету-фрагменту від початку загального полю даних вихідного пакету, який було фрагментовано (8 байт $\times 2^{13} = 2^{16}$ максимальний розмір пакету). Значення цього полю у першому фрагменті дорівнює 0.

Поле “Час життя” (Time To Live – TTL) вказує граничний термін часу, протягом якого пакет може переміщуватись мережею. Цей час задається джерелом пакету. При пересиланні пакету через маршрутизатор значення TTL зменшується на 1, навіть якщо час передавання через маршрутизатор менше 1 секунди. Тому кажуть, що цей час вимірюється у кількості переходів через маршрутизатори або хопи (hops). При досягненні цього значення 0 пакет далі не передається (тобто знищується).

Поле “Протокол” (Protocol) є вказівкою на протокол верхнього рівня, який розміщується у полі даних IP-пакету.

Поле “Контрольна сума заголовку” (Header Checksum) розраховується тільки по заголовку IP-пакету, тобто до поля “Дані”. При кожній зміні полів заголовку на проміжних маршрутизаторах контрольна сума заголовку перераховується. Алгоритм розрахунку – доповнення до суми усіх 16-бітних слів заголовку. При обчислені контрольної суми значення самого поля "Контрольна сума" вважається такою, що дорівнює 0.

Поля “IP-адреса відправника” (Source IP Address) та “IP-адреса отримувача” (Destination IP Address) мають значення відповідних адрес.

Поле “Опції” (IP Options) є необов’язковим та зазвичай використовується при налаштуванні мережі. У ньому може вказуватись точний маршрут проходження пакету, дані про безпеку, різноманітні часові відмітки тощо. Поле не має фіксованої довжини, тому для вирівнювання пакету відповідно до 32-бітної межі використовується поле “Вирівнювання” (Padding). Також це поле використовується для доповнення невеликого пакету до мінімального розміру даних кадру канального рівня (для Ethernet 64 байта).

Біти	0-3	4-7	8-15	16-31			
0-31	Версія IP	Довжина заголовку	Тип обслуговування	Загальна довжина IP пакету			
32-63	Ідентифікація фрагмента			0	DF	MF	Зміщення фрагменту (13 бітів)
64-95	TTL (час використання)		Протокол верхнього рівня	Контрольна сума IP-пакету			
96-127	IP адреса відправника						
128-159	IP адреса отримувача						
160-191	Опції (необов’язкові) та заповнювач (за потреби)						
192-223	Тип ICMP		Код ICMP	Контрольна сума ICMP повідомлення			
224-...	ICMP дані						

Рис. 2. Структура IP пакету з ICMP-заголовком.

Для перевірки з’єднання між двома вузлами часто використовують програму ping. Ця програма формує повідомлення протоколу ICMP (Internet Control Message Protocol - протокол контрольних повідомлень Інтернету) типу "Запит відлуння" та "Відповідь на відлуння". Відповідно до вимог ICMP, які виконує кожний вузол з встановленим на ньому стеком TCP/IP, при отримані такого пакету вузол відправляє відправнику відповідь у зворотньому напрямку. За результатом цього відправник отримує відповідь і, таким чином, визначає працездатність цього з’єднання. Повідомлення ICMP пересилаються у полі даних IP пакету, при цьому, розмір заголовку ICMP зазвичай складає вісім байт.

Завдання до лабораторної роботи №4

1. Запустіть програму «Командний рядок» (Пуск —> Виконати —> cmd) або термінал.
2. Виконання команди ping з ключем -f веде до встановлення прапорця IP, що забороняє фрагментацію пакету з повідомленням ICMP. Зміна розміру поля даних ICMP дозволяє підібрати значення MTU для мережі, до якої направляється ping. Виконайте команду ping у наступному форматі:

   ping –f –l розмір (для ОС Windows)

   ping -M do -s розмір (для ОС Linux)

   де розмір — це величина блоку даних ICMP пакету, яка задається користувачем, що використовує утиліту ping.

   Поступово змінюйте параметр розмір і за результатом відмови виконання команди ping з ключем –f (-M do) визначте максимальну величину даних ICMP пакету, при якій фрагментація не виконується.
3. Запустіть аналізатор протоколів WireShark.
4. Підготуйте програмний аналізатор до захоплення пакетів ICMP за допомогою налаштування відповідних фільтрів.
5. За допомогою команди ping відправте на суміжний у мережі комп’ютер пакет відлуння з полем даних ICMP розміром 5000 байт:

ping – l 5000 *ip_адреса_суміжного_комп’ютера*

Захопіть та визначте усі пакети з фрагментами одного ICMP повідомлення.

6. Для першого фрагменту надайте вміст заголовку кадру Ethernet, IP заголовку та ICMP заголовку.
7. Надайте для кожного фрагменту значення:
   − загальної довжини пакету,
   − ідентифікатору пакету,
   − прапорців (у двійковому форматі),
   − зміщення фрагменту.
8. Виконайте додавання довжин фрагментів та порівняйте результат із заявленою довжиною блоку даних (5000 байт). Надайте пояснення результату.
9. Наступний експеримент проведіть з копіюванням файлу з локальної мережі або доступному ресурсу Інтернет на комп’ютер. Знайдіть об’єкт для копіювання (інструкцію або книжку у форматі pdf, архівний файл, тощо). Запустіть аналізатор протоколів WireShark у режимі захоплення пакетів та почніть завантаження файлу. Якщо послідовності IP пакетів, пов’язаних із завантаженням файлу, чітко визначаються у WireShark, захоплення пакетів можна зупинити. Для будь-якої такої послідовності із кількістю не менш 10 пакетів (10 рядків WireShark) визначити:

− загальну довжину пакету,
− ідентифікатор пакету,
− прапорці (у двійковому форматі),

− час життя,
− протокол верхнього рівня.
Ці значення занесіть у відповідну таблицю.
10. Підготуйте звіт.

Запитання для самоперевірки

1. Яке значення першого байту IP пакету є найбільш типовим? Дайте пояснення.
2. Яке значення буде мати поле “Загальна довжина IP пакету”, якщо заборонено фрагментування пакету?
3. Яке максимальне та мінімальне значення поля “Загальна довжина IP пакету” ?
4. Як змінюються значення ідентифікатору в IP пакетах при передаванні значних об’ємів даних у мережі?
5. Поясніть чому різняться значення MTU, максимальний розмір пакету в команді ping та значення Length у відповідному рядку WireShark для цього пакету?
6. Як у програмі WireShark задати захоплення тільки пакетів ICMP?
7. Які прапорці встановлено у IP пакеті, якщо значення поля прапорців та зміщення має наступні значення: $0 \times 0000, 0 \times 4000, 0 \times 2000, 0 \times 10 FE$?
8. Яке максимальне та мінімальне значення поля TTL (час життя)?
9. Що повинен зробити маршрутизатор з отриманим IP пакетом та значенням його поля TTL, якщо:
   - IP адреса призначення, яку вказано в пакеті, не належить йому, а поле TTL має значення 60 ?
   - IP адреса призначення, яку вказано в пакеті, належить його інтерфейсу, а поле TTL має значення 1 ?
   - IP адреса призначення, яку вказано в пакеті, не належить його мережевому інтерфейсу, а поле TTL має значення 1 ?
10. Які значення буде мати поле “Протокол”, якщо IP пакет використовується для пересилання ICMP повідомлень, даних протоколів TCP та UDP ?