Лабораторна робота 6

Тема: Протоколи UDP та TCP. Структура пакетів UDP та TCP.

Мета: Вивчити призначення та використання протоколів UDP та TCP.

1. Теоретичні відомості

Протокол користувацьких датаграм UDP (User Datagram Protocol) описано у документі RFC 768. UDP є первинним сервісом, що пересилає прості повідомлення в IP пакетах без використання механізмів, що гарантують їх доставлення отримувачу. У полі заголовку IP пакета "Протокол верхнього рівня" вказує код протоколу, що переносить користувацьку датаграму на транспортному рівні (для стеку TCP/IP це або 06 - для TCP, або 17 для UDP). Аналогічно, у полі заголовку датаграми повинна бути адресна інформація, що вказує на сервіс прикладного рівня, який надає користувацькі дані для пересилання по мережі. Такою адресною інформацією є 16-розрядний номер порту. У табл.1 наведено значення та використання деяких портів протоколу UDP загальнодоступних сервісів.

Таблиця1. Деякі загальновідомі порти протоколу UDP

Порт	Ім’я сервісу або протоколу	Документ RFC	Опис
7	echo	792	Призначено для тестування зв’язку засобом відправлення даних на вузол та отримання від нього їх у незмінному вигляді
9	DISCARD	863	Призначено для тестування зв’язку засобом відправлення даних на вузол, який відкидає прийняте та не відправляє ніякої відповіді
11	SYSTAT	866	Видає список активних користувачів в операційній системі
13	DAYTIME	867	Призначено для тестування зв’язку засобом отримання від серверу актуальної дати та часу у текстовому вигляді
19	CHARGEN	864	CHARGEN (Character Generator Protocol). Відповідає на датаграму датаграмой, що вміщує випадкове число байт (0-512)
53	DNS	1034	Domain Name System — система домених імен. Комп’ютерна розподілена система для отримання інформації про домени.
123	NTP	5905	NTP (Network Time Protocol) — використовується для синхронізації часу

Порти з номерами від 0 до 1023 закріплено у документі RFC Assigned Numbers за стандартними сервісами (well-known services). Інші номера портів (вище 1023) надаються клієнтському програмному забезпеченню по мірі необхідності способом виділення номеру порту з пулу доступних портів. Комбінація IP-адреса та номер порту, що використовується для адресації, іноді зветься адресою socket. Адреса socket забезпечує для серверу та клієнту всю інформацію, яка необхідна для ідентифікації партнера з комунікації. За допомоги команди netstat -na можна вивести список наявних комунікацій вузлу з відображенням адрес socket.

UDP — мінімальний орієнтований на обробку повідомлень протокол транспортного рівня, який задокументований в RFC 768. Пакет UDP має визначену структуру (рис.1). Перші два байти визначають порт відправника UDP-пакету, а наступні два — порт його отримувача. Якщо отримувач — сервер, то це буде «добре відомий» статичний порт. Поле довжини визначає загальну кількість байт у заголовку UDP та області даних. Фактична межа для довжини даних при використанні IPv4 — 65507 (8 байт на UDP-заголовок та необхідно ще 20 байт на IP-заголовок). Поле контрольної суми перевіряє коректність вмісту UDP повідомлення. Дані повинні бути кратними двом байтам, при необхідності це досягається заповненням нульовими байтами.

Біти	0-15	16-31
0-31	Порт відправника (Source port)	Порт отримувача (Destination port)
32-63	Довжина датаграми (Length)	Контрольна сума (Checksum)
64-...	Дані (Data)	

Рис.1. Структура пакету UDP

TCP (англ. transmission control protocol — протокол управління передачею) — один із основних протоколів Інтернет, який призначено для управління передачею даних. Механізм TCP забезпечує створення потоку даних з попереднім встановленням з’єднання, забезпечує повторний запит даних у випадку їх втрати та усуває дублювання при отриманні двох копій одного пакету. Такий механізм роботи TCP, на відміну від UDP, гарантує цілісність переданих даних і повідомляє відправника про результати передачі. Реалізації TCP зазвичай вбудовані у ядро ОС.

Для користувача передача даних з використанням протоколу TCP виглядає як потокова. У дійсності, TCP забезпечує обмін пакетами даних. TCP-пакет має визначену структуру, яку показано на рис. 2.

Біти	0-3	4-9	10-15	16-31
0-31	Порт відправника			Порт отримувача
32-63	Порядковий номер			
64-95	Номер підтвердження			
96-127	Довжина заголовку	резерв	Прапорці	Розмір Вікна
128-159	Контрольна сума			Покажчик важливості
160-191	Опції (необов’язкові, але практично використовуються кожен раз)			
192-...	Дані			

Рис.2. Структура пакету TCP

Порт відправника та порт отримувача є 16-бітними полями та мають значення номерів портів відправника і адресату TCP-пакету. Подібно до UDP для TCP визначено певні порти, які асоційовано з деякими типами сервісів та серверами (табл.2). Для більшості портів програмне забезпечення використовує одні і ті самі номера, але з різними транспортними протоколами.

Таблиця 2. Деякі загальновідомі порти протоколу TCP

Порт	Ім’я сервісу або протоколу	Документ RFC	Опис
7	echo	792	см. табл.1
9	DISCARD	863	см. табл.1
11	SYSTAT	866	см. табл.1
13	DAYTIME	867	см. табл.1
19	CHARGEN	864	см. табл.1
20	FTP	959	FTP-DATA — для передавання даних FTP
21	FTP	959	FTP (File Transfer Protocol) — протокол передавання файлів у TCP-мережі. Порт 21 призначено для FTP-команд
25	SMTP	821	SMTP (Simple Mail Transfer Protocol) — протокол передавання електронної пошти у мережі
53	DNS	1034	см. табл.1
80	HTTP	1945	HTTP (HyperText Transfer Protocol) — протокол прикладного рівня для передавання даних
110	POP3	1939	POP3 (Post Office Protocol Version 3) — стандартний протокол, що використовується клієнтами електронної пошти для отримання повідомлень з віддаленого серверу
123	NTP	5905	NTP (Network Time Protocol) — використовується для синхронізації часу

Наступне 32-бітне поле (біти 32-63) є порядковим номером або номером у послідовності (sequence number). Його значення визначає положення даних TCP-пакету усереднені вихідного потоку даних, що існує в межах поточного логічного з'єднання. У момент встановлення логічного з'єднання і перший, і другий вузол взаємодії генерують свої початкові номери у послідовності. Основні вимоги до цього полю полягають у виключені повторень у проміжку часу, протягом якого TCP-пакет може знаходитись у мережі (час життя IP-пакета). Вузли обмінюються цими початковими номерами і підтверджують їх отримання. Під час відправлення TCP-пакетів з даними поле "номер в послідовності" має суму початкового номеру та кількості байт, що вказують на раніше передані дані.

Номер підтвердження (acknowledgement number) є 32-бітним полем, яке визначає кількість прийнятих даних із вхідного потоку до TCP-модулю, що створює TCP-пакет.

За ним йде чотирьох-бітове поле, що вказує на довжину заголовку TCP-пакету у 32-бітових словах та яке використовується для визначення початку розміщення даних у TCP-пакеті.

Поле «Прапорці» вміщує ознаки встановлення 6 прапорців: URG, ACK, PSH, RST, SYN, FIN.

Якщо біт прапорця URG встановлено у 1, то це означає, що TCP-пакет має важливі (urgent) дані. Встановлення у 1 прапорця ACK означає, що TCP-пакет має у полі "номер підтвердження" вірні дані.

Встановлення у 1 прапорця PSH буде вимагати невідкладної передачі прикладній програмі даних TCP-пакету, для якої їх адресовано. Підтвердження для TCP-пакету, що має значення 1 прапорця PSH, означає, що усі попередні TCP-пакети досягли адресату.

Встановлення у 1 прапорця RST означає або відповідь на отримання невірного TCP-пакету, або запит на перевстановлення логічного з'єднання.

Прапорець SYN, встановлений у 1, означає, що TCP-пакет є запитом на логічне з'єднання. Отримання пакету з встановленим прапорцем SYN повинно підтверджуватись вузлом-отримувачем.

Прапорець FIN, встановлений у 1, означає, що TCP-пакет є запитом на закриття логічного з'єднання та є ознакою кінця потоку даних, що передаються в цьому напрямку. Отримання пакету з встановленим прапорцем FIN повинно підтверджуватись вузлом-отримувачем.

Поле «Розмір вікна» є 16-бітовим полем, яке показує кількість байт інформації, що може прийняти до свого внутрішнього буферу TCP-модуль, який відправляє іншому вузлу цей TCP-пакет. Це поле використовується TCP-модулем приймача потоку даних для управління інтенсивністю цього потоку. Якщо, встановити значення поля «Розмір вікна» 0, то можна повністю зупинити передавання даних. Передавання потім можна поновити тільки, якщо розмір вікна прийме достатньо велике значення. Максимальний розмір вікна залежить від реалізації. У деяких реалізаціях максимальний розмір може встановлюватись системним адміністратором. Визначення оптимального розміру вікна є однією з

найбільш складних задач реалізації протоколу TCP.

Поле «Контрольна сума» - 16-бітове поле, значення якого визначається як контрольна сума TCP-заголовку, даних пакету та псевдозаголовку, якщо він є.

Поле «Покажчик важливості» - 16-бітове поле, визначає зміщення на першого байту у тілі TCP-пакету, починає послідовність важливих (urgent) даних.

Додаткові дані заголовку — це послідовність полів довільної довжини, що описують необов'язкові дані заголовку. Протокол TCP визначає три типи додаткових даних заголовку:

- кінець списку полів додаткових даних;
- пусто (No Operation);
- максимальний розмір пакету.

Додаткові дані останнього типу надсилаються у TCP-заголовку у момент встановлення логічного з'єднання для вказування на готовність TCP-модуля щодо приймання пакетів довше 536 байтів. В UNIX-реалізаціях довжина пакету зазвичай визначається максимальною довжиною IP-сегменту для мережі.

Етапи TCP-взаємодії

Основною відмінністю TCP від UDP є те, що протокол TCP виконує додаткову задачу — забезпечує надійне доставлення даних. Для рішення цієї задачі протокол TCP використовує метод просування даних з встановлення логічного з'єднання. Логічне з'єднання дає можливість учасникам обміну стежити за тим, щоб дані не було втрачено, змінено або продубльовано, а також щоб вони прийшли до отримувача у тому порядку, в якому їх було відправлено.

Взаємодія вузлів з використанням протоколу TCP має три етапи:

- встановлення логічного з'єднання;
- обмін даними;
- закриття з'єднання.

Протокол TCP встановлює логічне з'єднання між прикладними процесами, у кожному з'єднанні приймають участь тільки два процеси. TCP-з'єднання є дуплексним — кожний з учасників цього з'єднання може одночасно отримувати та відправляти дані. При встановлені логічного з'єднання модулі TCP домовляються між собою про параметри процедури обміну даними. У протоколі TCP кожна сторона з'єднання відправляє протилежній стороні наступні параметри:

- максимальний розмір сегменту, який вона може прийняти;
- максимальний об'єм даних (можливо декілька сегментів), які вона дозволяє іншій стороні передавати у свою сторону, навіть якщо інша сторона ще не отримала квитанцію на попередню порцію даних (розмір вікна);
- початковий порядковий номер байту, з якого вона починає відлік потоку даних у рамках даного з'єднання.

У результаті переговорного процесу модулів TCP з обох сторін визначаються параметри з'єднання. Деякі з них залишаються постійними

протягом усього сеансу зв’язку, а інші адаптивно змінюються. Наприклад, у залежності від завантаження буферу отримувача, а також надійності роботи мережі динамічно змінюється розмір вікна відправника.

З’єднання встановлюється за ініціативи клієнтської частини додатку. При необхідності виконати обмін даними із серверною частиною додаток-клієнт звертається до нижчого за рівнем протоколу TCP, який у відповідь на це звернення відправляє сегмент-запит на встановлення з’єднання за протоколом TCP, який працює на стороні серверу (рис.3, а). У запиті є прапорець SYN, який встановлено у 1.

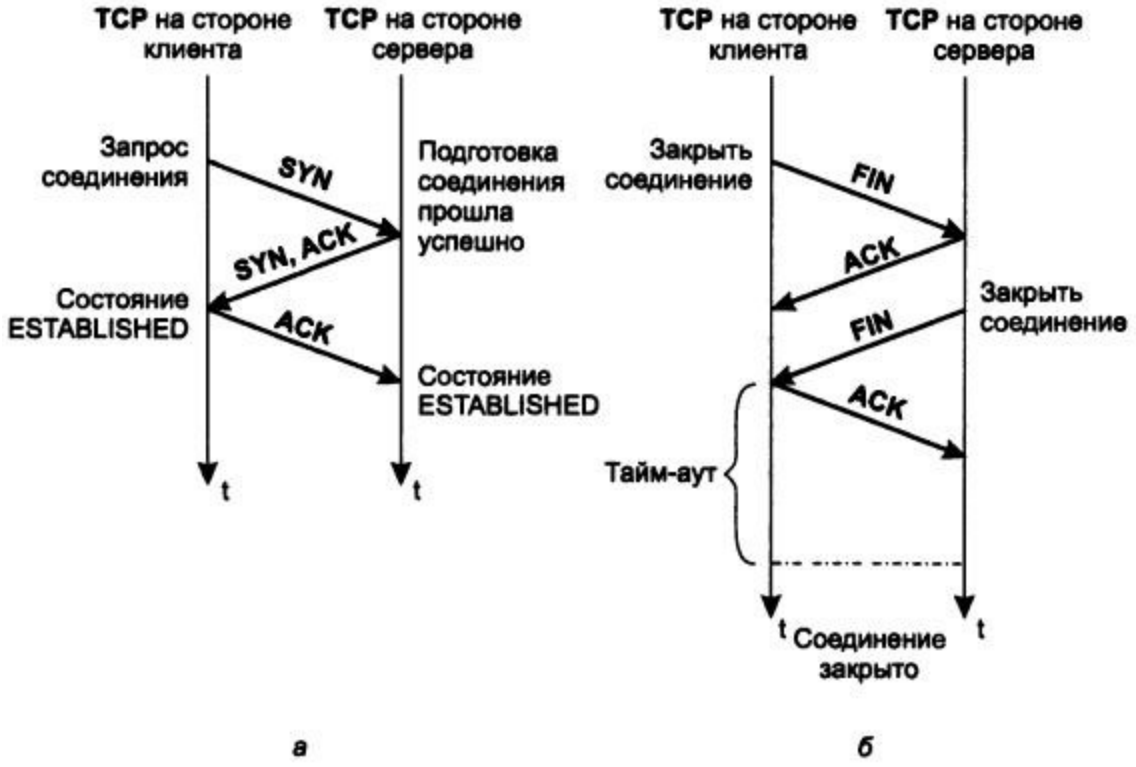

Рис.3. Процедура встановлення та розриву логічного з’єднання при нормальному перебігу процесу.

Після отримання запиту, модуль TCP на стороні серверу звертається до операційної системи щодо забезпечення певними системними ресурсами для організації буферів, таймерів, лічильників. Ці ресурси пов’язуються із з’єднанням з моменту його створення і до моменту розриву. Якщо на стороні серверу усі необхідні ресурси були отримані і всі необхідні дії виконано, то модуль TCP відправляє клієнту сегмент з прапорцями ACK та SYN.

У відповідь клієнт посилає сегмент з прапорцем ACK та переходить у стан встановленого логічного з’єднання (стан ESTABLISHED). Коли сервер отримує прапорець ACK, він також переходить у стан ESTABLISHED. На цьому процедура встановлення з’єднання закінчується і сторони можуть переходити до обміну даними.

Етап встановлення з’єднання отримав назву "потрійне рукостискання" (three-way handshake).

З’єднання може бути розірване у будь-який момент з ініціативи будь-якої сторони — клієнтської або серверної. Для цього клієнт та сервер повинні обмінятись сегментами FIN та АСК, у послідовності, яку показано на рис. 5(б), де ініціатором виступає клієнт. З’єднання вважається закритим після деякого часу, на протязі якого сторона-ініціатор впевнюється, що її заключний сигнал АСК отримано нормально і він не викликав ніяких «аварійних» повідомлень з боку серверу. Сокет одночасно може приймати участь у декількох з’єднаннях.

Схема нумерації TCP передбачає привласнення порядкового номеру кожному надісланому у з’єднанні байту даних. У заголовку сегмента вказується номер першого байта поля даних цього сегмента. Від приймача необхідне підтвердження приймання сегмента. Якщо АСК не приходить за інтервал тайм-ауту, дані передаються повторно. Такий механізм називається позитивним підтвердженням з ретрансляцією (positive acknowledgment with retransmission). У підтверджені TCP, що надсилається передавачу, вказується номер наступного байту, що очікує приймач. Наслідком такого механізму є те, що у випадку пересилання останнього сегменту даних (наприклад, файлу), з номером першого байту поля даних n приймач відправить підтвердження з номером n+1. Тоді перший сегмент з наступними даними (наступний файл) буде мати номер першого байту поля даних n+1. Тому необхідна достатньо велика розрядність поля, що зберігає номер першого байту поля даних і поля, що зберігає номер підтвердження.

Протокол TCP реалізує механізми управління потоком, що надходять до вузла-приймача даних. Під час встановлення з’єднання кожний з вузлів визначає простір пам’яті для вхідного буферу з’єднання і повідомляє про це іншу сторону. Вікно приймання (receive window) є будь-яким простором у вхідному буфері, що ще не зайняте даними. Звільнення буферу від прийнятих даних виконує додаток отримувача. Цей процес залежить від продуктивності та завантаження вузлу отримувача. Кожний відправлений приймачем АСК має відомості про поточний стан вікна приймання, у залежності від якого регулюється потік даних від відправника. Зазвичай підтвердження АСК відправляються не на кожний надісланий сегмент, а на неперервний блок з декількох сегментів, який зібрано у вікні приймання. Це дозволяє не відкидати сегменти, що надійшли не за порядком відправлення, а впорядковувати їх у відповідності з послідовністю номерів та розмірам сегментів. Вузол-відправник повинен відстежувати кількість вже відправлених даних, на які надійшло підтвердження та поточний розмір приймального вікна отримувача.

Завдання до роботи

1. Підготуйте аналізатор мережевих протоколів WireShark до захоплення тільки пакетів UDP, налаштував відповідний фільтр. Виконайте захоплення декількох пакетів UDP.

2. Виконайте аналіз захоплених пакетів. Наведіть у звіті дамп заголовків мережевого та транспортного рівнів одного пакету. Укажіть поле в IP-заголовку, що вказує на транспортний протокол UDP. Поясніть значення полів заголовку захопленого UDP-пакету.
3. Для захоплення та аналізу TCP-пакетів використовуйте будь-який браузер Internet. Запустіть його. Далі підготуйте аналізатор мережевих протоколів WireShark до захоплення тільки пакетів TCP, налаштував відповідний фільтр. Переведіть аналізатор у режим захоплення пакетів. У браузері уведіть адресу www.znu.edu.ua та натисніть Enter. Аналізатор захопить множину пакетів, серед яких перші три виконують процедуру встановлення логічного з'єднання («потрійне рукостискання»).
4. Знайдіть пакети, що виконують встановлення з'єднання, та наведіть дамп їх заголовків транспортного рівня та поясніть значення їх полів.
5. Підготуйте звіт.

Контрольні питання

1. Що зветься сокетом (socket)?
2. Для чого призначено порти з номерами від 0 до 1023?
3. Яка структура UDP пакету?
4. За яких умов обміну даними у мережі використання UDP пакетів є найбільш обґрунтованим?
5. Чи можна фрагментувати IP пакети, що несуть UDP пакети? Дайте пояснення.
6. Яка найбільша довжина блоку даних, що передається за допомогою пакету UDP?
7. У чому принципова різниця між протоколами UDP та TCP?
8. Для рішення яких задач краще використовувати протокол TCP?
9. Яка структура пакету TCP?
10. На що вказують поля "Порядковий номер" та "Номер підтвердження" в пакеті TCP?
11. На що вказує поле "Розмір вікна"? Коли змінюється його значення?
12. Які прапорці і для чого використовуються в пакеті TCP?
13. Яка послідовність дій на початку обміну даними за протоколом TCP?
14. Чи можуть одночасно для TCP та UDP використовуватись порти з однаковими номерами? Дайте пояснення.