МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ
ОДЕСЬКИЙ ДЕРЖАВНИЙ ЕКОЛОГІЧНИЙ УНІВЕРСИТЕТ

Факультет Магістерської підготовки

Кафедра Інформаційних технологій

МАГІСТЕРСЬКА КВАЛІФІКАЦІЙНА РОБОТА

на тему: «Моделювання та аналіз протоколів для мереж з низькою чутливістю до затримок»

Виконав студент 2 курсу групи
МІС- 18 спеціальності 122
Комп'ютерні науки

Яковлєв Іван Вікторович

_____

Керівник к.геог.н., доц.
Коваленко Людмила Борисівна

Консультант

Рецензент к.т.н., доц.
Гнатовська Ганна Арнольдівна

Одеса 2020

АННОТАЦІЯ

на магістерську роботу «Моделювання та аналіз протоколів для мереж з низькою чутливістю до затримок»,
студента Яковлєва Івана Вікторовича

В магістерській роботі виконано моделювання дії супутникового зв'язку на основі протоколу DTN (Delay-Tolerant Networks), терпимого до затримок часу. Результат моделювання представлений у вигляді опису структури мережі і інформаційній моделі функціонування DTN, створеної за допомогою методології SADT.

Крім цього, наведено обґрунтування необхідності дослідження якості роботи мереж DTN. Розглянуто основні відмінності протоколів, використовуваних в традиційних комп'ютерних мережах і мережах DTN. Проведено аналіз проблем використання стандартних протоколів в мережах, терпимих до затримок часу. Розроблено математичну модель надійності телекомунікаційних мереж, терпимих до затримок часу. Сформульовано завдання, які необхідно вирішувати для підвищення якості роботи DTN мереж.

Об'єкт дослідження – протокол DTN, терпимий до затримок часу.

Предмет дослідження – надійність мереж DTN.

Ключові слова: DTN мережі, надійність мереж, затримки в каналах передачі даних.

ЗМІСТ

СПИСОК СКОРОЧЕНЬ, УМОВНИХ ПОЗНАЧЕНЬ І ТЕРМІНІВ

DNS – Domain Name Service, служба доменних імен.

DHCP – Dynamic Host Configuration Protocol, протокол динамічної конфігурації вузла.

DTN – Delay&Disruption-Tolerant Networking, мережі толерантні до затримок.

FTP – File Transfer Protocol, протокол передачі файлів.

GEO – Geostationary Earth Orbit, геостаціонарна орбіта.

GPS – Global Positioning System, глобальна система визначення місцезнаходження.

HTTP – HyperText Transfer Protocol, протокол передачі гіпертексту.

ICAM – Integrated Computer Aided Manufacturing, інтеграція комп'ютерних та промислових технологій.

ICMP – Internet Control Message Protocol, міжмережевий протокол керуючих повідомлень.

IETF – Internet Engineering Task Force, инженерный совет Интернета.

IP – Internet Protocol, Інтернет-протокол міжмережевого обміну даними.

ISO – International Organization for Standardization, міжнародна організація по стандартизації.

ITU – International Telecommunication Union, міжнародний союз електрозв’язку.

MEO – Medium-Earth Orbite Satellites, середньовисотні супутники.

LEO – Low-Earth Orbit, низька навколоземна орбіта.

OSI – Open System Interconnection, модель взаємодії відкритих систем.

RTP – Real-time Transport Protocol, протокол передачі трафіку реального часу.

SADT – Structured Analysis and Design Technique, технологія структурного аналізу і проектування.

SNMP – Simple Network Management Protocol, простий протокол мережевого управління.

SMTP – Simple Mail Transfer Protocol, простий протокол електронної пошти.

TCP – Transmission Control Protocol, протокол управління передачею.

TELNET – Terminal Network, мережевий термінал.

UDP – User Datagram Protocol, протокол передачі дейтаграм користувача.

VSAT – Very Small Aperture Terminal, мініатюрний апертурний термінал.

Mbps – мегабітів за секунду

Gbps – гігабітів за секунду

Глобалстар – низькоорбітальна супутникова цифрова система зв'язку, що надає послуги бездротової портативної телефонії і інші телекомунікаційні послуги по всьому світу.

Домен – це область (зона) простору ієрархічних імен мережі Інтернет, яка обслуговується набором серверів доменних імен і централізовано адмініструється.

ВСТУП

Останнім часом активне впровадження комп'ютерних мереж в різноманітні галузі життєдіяльності людини призвело до того, що одними з основних проблем у цьому напрямі є проблеми пропускної здатності каналів передачі інформації, їх функціонування і надійність. Одним із ключових показників якості роботи комп'ютерної мережі є надійність передачі інформації по мережі, а саме, ймовірність доставки повідомлення до одержувача, час, за який це повідомлення буде доставлено, і рівнозначність відправленого та отриманого повідомлень.

Однак існують ситуації, в яких показник ймовірності того, що повідомлення взагалі дійде до приймаючого пристрою, може наближатися до нуля. Так, наприклад, у разі порушення або відсутність відповідної технічної інфраструктури сигнал просто не дійде до найближчого вузла комутації, як це може бути у випадку природних чи техногенних катастроф. Також в одній з найважливіших для людства, космічної галузі, в даний час дуже істотною проблемою є збільшене час відгуку сигналу, яке спостерігається при сеансах міжпланетного і супутникового зв'язку.

В даний час сценарій роботи традиційних протоколів для роботи мереж базується на певних припущеннях. Так, одним з головних припущень, що лежать в основі стандартного протоколу для комп'ютерних мереж TCP/IP, є те, що часи затримки на всьому протязі шляху пакета від джерела до місця призначення невеликі. Проте передача даних можлива і в мережах з непостійним зв'язком: ці дані можуть затримуватися на вузлах до тих пір, поки не з'явиться робоче з'єднання. Такий метод називається комутацією повідомлень. Мережі, сконструйовані за таким принципом, називаються мережами, стійкими до затримок (DTN, Delay-Tolerant Network).

Одночасно з розробкою подібних протоколів постає проблема оцінки надійності та якості роботи такої мережі. Очевидно, що моделі надійності для мереж, що працюють на традиційному протоколі TCP, у разі DTN мережі не

підходять. Для порівняння моделей оцінки якості і надійності традиційних і DTN мереж необхідно оцінити реалізацію одних і тих же функцій. Однак порівняння мереж, побудованих на традиційних протоколах передачі даних, і DTN мереж є досить складною і цікавим завданням. Необхідно виділити основні характеристики якості телекомунікаційних мереж, за якими можна оцінювати і порівнювати роботу мереж, а також зробити висновки про якості функціонування даних мереж.

Отже, метою наукової роботи є моделювання супутникового зв’язку на основі протоколу DTN, призначеного для забезпечення наддалекого космічного зв'язку та оцінка надійності і якості роботи DTN мережі.

Для досягнення поставленої мети в роботі необхідно вирішити наступні завдання:

- провести огляд мереж DTN, толерантних до затримок, призначених для забезпечення наддалекого космічного зв’язку;
- обґрунтування необхідності дослідження якості роботи мереж DTN;
- провести аналіз сучасного стану супутникового зв’язку;
- проаналізувати відмінності протоколів, що використовуються в традиційних комп'ютерних мережах та мережах DTN;
- здійснити моделювання та аналіз супутникового зв’язку на основі протоколу DTN;
- запропонувати математичну модель надійності телекомунікаційних мереж, толерантних до затримок часу.

Магістерська кваліфікаційна робота складається з вступу, п’ятьох розділів, висновків, переліку посилань на 20 найменуванm, додатків. Повний обсяг роботи становить 86 сторінок, містить 29 рисунків,4 таблиці та 6 формул.

1 ОГЛЯД ЕТАЛОННИХ МОДЕЛЕЙ КОМП'ЮТЕРНИХ МЕРЕЖ

1.1 Еталонна модель взаємодії відкритих систем (OSI)

Еталонна модель OSI (за винятком фізичного середовища) показана на рис. 1.

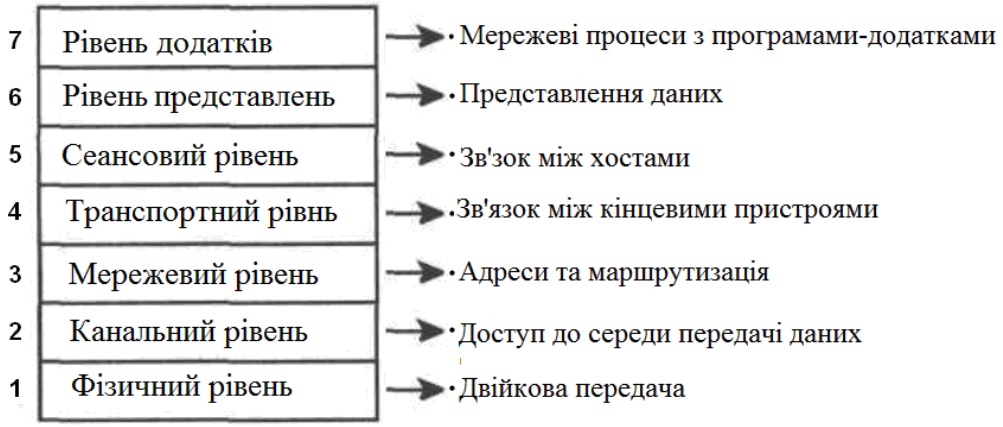

Рисунок 1 – Еталонна модель OSI

Модель OSI має сім рівнів. Поява саме такої структури було обумовлено наступними міркуваннями [1][1)]:

- рівень повинен створюватися в міру необхідності окремого рівня абстракції;
- кожен рівень повинен виконувати строго певну функцію;
- вибір функцій для кожного рівня повинен здійснюватися з урахуванням створення стандартизованих міжнародних протоколів;
- межі між рівнями повинні вибиратися так, щоб потік даних між інтерфейсами був мінімальним;
- кількість рівнів має бути достатньо великим, щоб різні функції не об'єднувалися в одному рівні без необхідності, але не надто високим, щоб архітектура не ставала громіздкою.

[1)] [1] Олифер В.Г., Олифер Н. А. Компьютерные сети. Принципы, технологии, протоколы: Учебник для вузов. 4-е изд. СПб.: Питер, 2010. 944 е.: ил.

Оскільки нижні рівні (з 1 по 3) моделі OSI управляють фізичною доставкою та спілкуванням по мережі, їх часто називають рівнями середовища передачі даних (media layers). Верхні рівні (з 4 по 7) моделі OSI забезпечують точну доставку даних між комп'ютерами в мережі, тому їх часто називають рівнями хост-машини (host layers) (рис. 2).

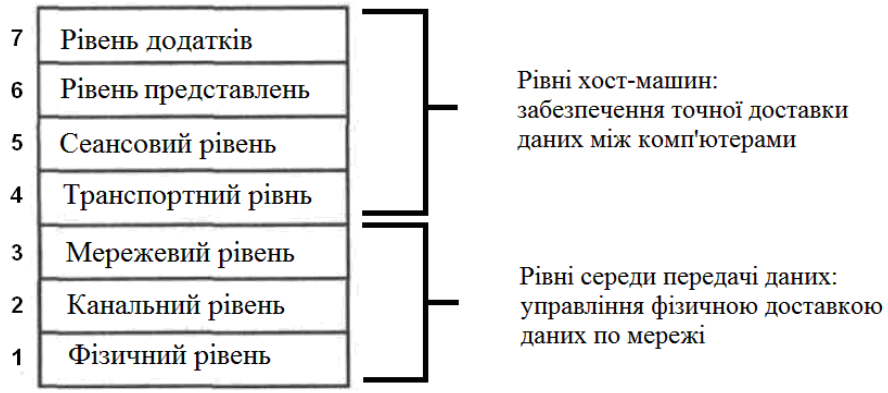

Рисунок 2 – Рівні середи передачі даних управляють фізичною доставкою повідомлень, а рівні хост-машин забезпечують точну доставку даних

У більшості мережевих пристроїв реалізовані всі сім рівнів. Однак для прискорення виконання операцій в деяких мережах сама мережа реалізує функції відразу декількох рівнів [2][1)].

1.2 Еталонна модель TCP/IP

Перший опис моделі TCP/IP зустрічається в книзі Серфа і Кана [3][2)], пізніше перетворюється в стандарт [4][3)]. Конструктивні особливості моделі обговорюються у виданні [5][4)].

[1)] [2] Таненбаум Э., Уэзеролл Д. Компьютерные сети. 5-е изд. СПб.: Питер, 2012. 960 с.: ил.

[2)] [3] Cerf V., Kahn R. A Protocol for Packet Network Interconnection. IEEE Trans, on Commun. 1974. V. COM-22. P. 637–648.

[3)] [4] Braden R. Requirements for Internet Hosts – Communication Layers. RFC 1122. Oct. 1989.

[4)] [5] Clark D.D. The Design Philosophy of the DARPA Internet Protocols. Proc. SIGCOMM 88 Conf. ACM. 1988. P. 106–114.

Самий низький рівень у моделі, канальній рівень, описує те, як і що канали, такі як послідовні лінії і класичний Ethernet, повинні зробити, щоб задовольнити потреби цього міжмережевого рівня без встановлення з'єднання.

Міжмережевий рівень (рис. 3) приблизно відповідає мережевому рівню в OSI. Його завдання полягає в забезпеченні можливості кожного хоста посилати пакети в будь-яку мережу і незалежно рухатися до пункту призначення (наприклад, в іншій мережі). Міжмережевий рівень визначає офіційний формат пакету і протокол IP, з додатковим протоколом ICMP (Internet Control Message Protocol). Завданням міжмережевого протоколу є доставка IP-пакетів до пунктів призначення. Основними аспектами тут є вибір маршруту пакета і недопущення закупорки транспортних артерій.

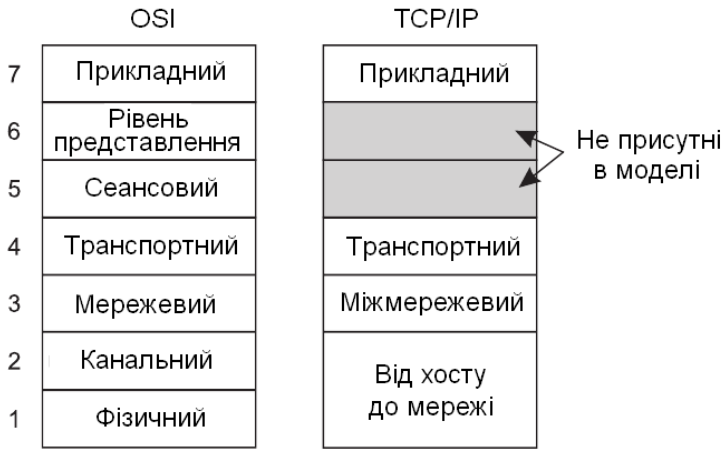

Рисунок 3 – Еталонна модель TCP/IP

Транспортний рівень створений для того, щоб об'єкти одного рангу на прийомних і передавальних хостах могли підтримувати зв'язок, подібно транспортному рівню моделі OSI. На цьому рівні повинні бути описані два наскрізних протоколу. Перший, TCP (Transmission Control Protocol), є надійним протоколом із установленням з'єднань, що дозволяє без помилок доставляти байтовий потік з однієї машини на будь-яку іншу машину об'єднаної мережі.

Другий протокол цього рівня, UDP (User Dataram Protocol), є ненадійним протоколом без встановлення з'єднання, що не використовують послідовне управління потоком протоколу TCP, а що надають своє власне. Взаємовідносини протоколів IP, TCP і UDP показані на рис. 4. З часу створення протоколу IP цей протокол був реалізований в багатьох інших мережах.

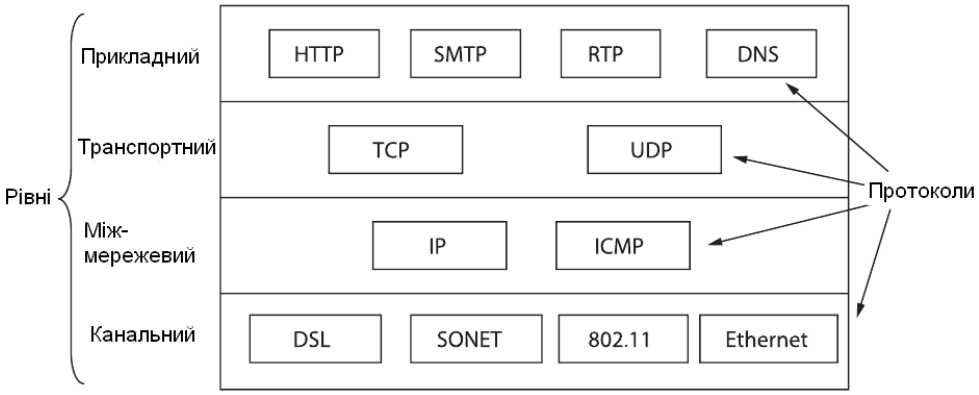

Рисунок 4 – Протоколи і мережі в моделі TCP/IP

Прикладний рівень. У моделі TCP/IP немає сеансового рівня та рівня подання. У цих рівнях просто не було необхідності, тому вони не були включені в модель. Прикладний рівень містить всі протоколи високого рівня. До старих протоколів відносяться протокол віртуального терміналу Telnet, протокол перенесення файлів FTP і протокол електронної пошти SMTP. З роками було додано багато інших протоколів. Деякі найбільш важливі показані на рис. 4. Це DNS, що дозволяє перетворювати імена хостів в мережеві, HTTP, протокол, що використовується для створення сторінок на World Wide Web, а також RTP, протокол для представлення мультимедіа в реальному часі, таких як звук або фільми [2][1)].

[1)] [2] Таненбаум Э., Уэзеролл Д. Компьютерные сети. 5-е изд. СПб.: Питер, 2012. 960 с.: ил.

1.3 Порівняльний аналіз еталонних моделей OSI і TCP/IP

У моделей OSI і TCP/IP є багато спільних рис. Обидві моделі засновані на концепції стека незалежних протоколів.

Незважаючи на цю фундаментальну подібність, у цих моделей є і ряд відмінностей. Порівнюємо саме еталонні моделі, а не відповідні їм стеки протоколів. Книга [6][1)] цілком присвячена порівнянню моделей TCP/IP і OSI.

Для моделі OSI центральними є три концепції: служби; інтерфейси; протоколи. Ймовірно, найбільшим внеском моделі OSI стало явне розділення цих трьох концепцій. Кожен рівень надає деякі сервіси (служби) для розташованого вище рівня. Сервіс визначає, що саме робить рівень, але не те, як він це робить і яким чином об'єкти, розташовані вище, отримують доступ до даного рівня. Інтерфейс рівня визначає спосіб доступу до рівня для розташованих вище процесів. Він описує параметри і очікуваний результат. Він також нічого не повідомляє про внутрішній устрій рівня. Нарешті, рівнорангові протоколи, що застосовуються в рівні, є внутрішньою справою самого рівня. Для виконання поставленого йому завдання (тобто надання сервісу) він може використовувати будь-які протоколи . Крім того, рівень може міняти протоколи, не зачіпаючи роботу додатків більш високих рівнів.

Якщо поглянути на ці дві моделі ближче, то, перш за все, зверне на себе увагу відмінність у кількості рівнів: в моделі OSI сім рівнів, в моделі TCP/IP – чотири. В обох моделях є міжмережевий, транспортний і прикладний рівні, а інші рівні різні.

Ще одна відмінність між моделями лежить у сфері можливості використання зв'язку на основі з’єднання та зв'язку без встановлення з'єднання. Модель OSI на мережевому рівні підтримує обидва типи зв'язку, а на транспортному рівні – тільки зв'язок на основі з’єднання (оскільки транспортні служби є видимими для користувача). У моделі TCP/IP на мережевому рівні є тільки

[1)] [6] Piscitello D.M., Chapin A.L. Open Systems Networking: TCP/IP and OSI. Boston: Addison-Wesley, 1993.

один режим зв'язку (без встановлення з'єднання), але на транспортному рівні вона підтримує обидва режима, надаючи користувачам вибір. Цей вибір особливо важливий для простих протоколів запит-відповідь.

1.4 Недоліки еталонної моделі TCP/IP

У моделі TCP/IP та її протоколів є ряд недоліків.

По-перше, в цій моделі немає чіткого розмежування концепцій служб, інтерфейсів і протоколів. При розробці програмного забезпечення бажано провести чіткий поділ між специфікацією і реалізацією, що досить ретельно робить OSI і чого не робить TCP/IP. В результаті модель досить марна при розробці мереж, що використовують нові технології.

По-друге, модель TCP/IP аж ніяк не є загальною і досить погано описує будь-який стек протоколів, крім TCP/IP. Так, наприклад, описати технологію Bluetooth за допомогою моделі TCP/IP абсолютно неможливо.

По-третє, канальний рівень насправді не є рівнем в тому сенсі, який зазвичай використовується в контексті рівневих протоколів. Це скоріше інтерфейс між мережею та рівнями передачі даних. Різниця між інтерфейсом і рівнем є надзвичайно важливим, і тут не слід бути недбалим.

По-четверте, в моделі TCP/IP не розрізняються фізичний рівень і рівень передачі даних. Про це розходження навіть немає згадки. Між тим, вони абсолютно різні. Фізичний рівень повинен мати справу з характеристиками передачі інформації по мідному кабелю, оптичному волокну і по радіо каналу, тоді як завданням рівня передачі даних є визначення початку і кінця кадрів і передача їх з одної сторони на іншу з необхідним ступенем надійності. Правильна модель повинна утримувати їх як два різних рівня. У TCP/IP моделі немає цього.

2 ОГЛЯД МЕРЕЖ DTN, ТОЛЕРАНТНИХ ДО ЗАТРИМОК

2.1 Аналіз проблем надійності передачі даних

Останнім часом активне впровадження комп'ютерних мереж в різноманітні галузі життєдіяльності людини призвело до того, що одними з основних проблем у цьому напрямі є проблеми пропускної здатності каналів передачі інформації, їх функціонування і надійність. Як відомо, в даний час основними показниками роботи мережі прийнято вважати такі характеристики, як надійність, функціональність, пропускна здатність та ін [7][1)].

Одним із ключових показників якості роботи комп'ютерної мережі є надійність передачі інформації по мережі, а саме, ймовірність доставки повідомлення до одержувача, час, за який це повідомлення буде доставлено, і рівнозначність відправленого та отриманого повідомлень.

Однак існують ситуації, в яких показник ймовірності того, що повідомлення взагалі дійде до приймаючого пристрою, може наближатися до нуля. Так, наприклад, у разі порушення або відсутність відповідної технічної інфраструктури сигнал просто не дійде до найближчого вузла комутації, як це може бути у випадку природних чи техногенних катастроф [8][2)]. Також в одній з найважливіших для людства, космічної галузі, в даний час дуже істотною проблемою є збільшене час відгуку сигналу, яке спостерігається при сеансах міжпланетного і супутникового зв'язку. Наприклад, у разі передачі сигналу на орбітальні станції інших об'єктів Сонячної системи час затримки може досягати декількох годин. Так, сигнал із Землі до Сатурна йде близько години [9][3)].

[1)] [7] ИСО/МЭК 9126 Информационные технологии. Оценка продукции программного обеспечения. Женева: Международная организация стандартов, 1991. С. 1–6.

[2)] [8] Wood L., Holliday P., Floreani D., Wesley M. Eddy, Sharing the dream. Workshop on the Emergence of Delay-Disruption-Tolerant Networks (E-DTN), part of the International Conference on Ultra Modern Telecommunication (ICUMT). St. Petersburg: Russia, 14 October 2009. P. 1–2.

[3)] [9] Ivancic W., Eddy W., Wood L., Northam J., Jackson C. Experience with delay-tolerant networking from orbit. International Journal of Satellite Communications and Networking, special issue for best papers of ASMS 2008. September-December, 2010, V. 28. Is. 5–6. P. 335–351.

Не викликає сумніву той факт, що надійність забезпечення наддалекого космічного зв'язку є дуже актуальною в даний час. Навіть якщо розглядати таку знайому всім область як використання мобільного зв'язку, то і в цьому випадку також в сучасних комунікаційних мережах мобільного телефонії часто зустрічаються ситуації, при яких стає неможливим передавати інформацію в мережі. Наприклад, у разі великого завантаження базової станції мобільного мережі і перевищенні максимально допустимого (критичного) часу відгуку виконання запитів до сервера виявляється досить проблематичним.

Щоб змінити ситуацію в кращу сторону, робилося безліч спроб розробити нові протоколи (правила передачі даних у мережі), так як існуючі традиційні протоколи з таким завданням не справляються. Передача даних може взагалі не відбутися, і повідомлення може не бути отримано в силу особливостей існуючих протоколів.

В даний час сценарій роботи традиційних протоколів для роботи мереж базується на певних припущеннях. Так, одним з головних припущень, що лежать в основі стандартного протоколу для комп'ютерних мереж TCP/IP, є те, що часи затримки на всьому протязі шляху пакета від джерела до місця призначення невеликі. Для встановлення з'єднання в протоколі TCP використовується правило «three way handshake»: час встановлення з'єднання пропорційно значенню часу затримки пакета в мережі. Але якщо затримки часу є достатньо великими, то, наприклад, звичайний браузер (засіб перегляду сторінок в Інтернеті) як правило, видає повідомлення «Помилка номер 403 – Ресурс не найден», – і інформація не зможе бути отримана користувачем. Крім того, слід зауважити, що перед відправкою пакета в традиційних мережах необхідно здійснювати перетворення адреси з доменного імені в IP-адресу, а потім з IP-адреси в MAC-адресу. Таке перетворення передбачає наявність відповідної інфраструктури, а саме, – певних DNS-серверів, маршрутизаторів, шлюзів і т.п. Якщо така інфраструктура відсутня, працездатність мережі буде порушена практично на всіх рівнях моделі OSI, починаючи з відсутності зв'я-

зку на фізичному рівні і закінчуючи неможливістю роботи додатків на верхньому рівні.

Труднощі використання традиційних протоколів у мережах з затримкою часу стосуються не тільки транспортного рівня та протоколу TCP/IP, але і протоколів прикладного рівня. Використання традиційного протоколу прикладного рівня (HTTP) стає складним, оскільки схема роботи HTTP-протоколу, заснована на тому, що у відповідь на початковий GET-запит якоїсь порції даних (наприклад, HTML-сторінки), створюються додаткові GET-запити для отримання вбудованих в сторінку об'єктів (наприклад, зображень), передбачає ті ж умови роботи, що й схема роботи протоколу TCP. Таким чином, можна зробити висновок, що в мережах з затримкою часу інтерактивний обмін численними повідомленнями стає неможливий ні з теоретичної, ні з практичної точок зору.

Проте передача даних можлива і в мережах з непостійним зв'язком: ці дані можуть затримуватися на вузлах до тих пір, поки не з'явиться робоче з'єднання. Такий метод називається комутацією повідомлень. Мережі, сконструйовані за таким принципом, називаються мережами, стійкими до затримок (DTN, Delay-Tolerant Network), або распадоустойчівимі мережами (Disruption-Tolerant Network, DTN). Ця модель є узагальненням Інтернету, в якому при комунікації можливі затримки та тимчасове зберігання даних. У роботі [10][1)] було встановлено, що така модель здатна забезпечити хорошу пропускну здатність при незначних витратах, і ця пропускна здатність часто вдвічі перевищує показники звичайної наскрізної моделі.

2.2 Особливості роботи протоколів у мережах DTN

Новий протокол DTN був запропонований Кевіном Фолом [11] для мережах з великим часом затримки передачі повідомлень. Протокол заснований

[1)] [10] Laoutaris N., Smaragdakis G., Rodriguez P., Sundaram R. Delay Tolerant Bulk Data Transfers on the Internet. Proc. SIGMETRICS 2009 Conf., ACM, June 2009. P. 229–238.

на парадигмі «зберігати дані і перенаправляти їх далі» і оперує спеціальними одиницями інформації – bundle. По суті, bundle – це повідомлення, що містить в собі, поряд зі значимим для програми вмістом, також і необхідну для маршрутизації інформацію. Вузли DTN, обмінюючись bundle'ами, зберігають їх. По мірі появи зв'язку з наступним вузлом даний bundle пересилається далі, поки не буде досягнутий вузол призначення або час життя bundle'а закінчиться.

Робота над DTN почалася в 2002 році, коли комісією IETF була створена спеціальна дослідницька група. Необхідність створення мереж, стійких до затримок, виникла в несподіваному місці: при спробах відправляти пакети в космосі.

Основною проблемою протоколу є те, що відстань між станціями досить велика, тобто сигнали, що надходять від однієї станцій до іншої, можуть губитися у просторі. На відміну від протоколу TCP/IP протокол DTN не передбачає постійного з’єднання вузлів мережі. Якщо вузлу не вдається передати пакет даних за призначенням, інформація не видаляється, а зберігається. Спроби передачі продовжуються до тих пір, поки вузлу мережі не вдається зв’язатися з яким-небудь іншим вузлом і успішно передати йому дані.

DTN (Delay-Tolerant Networking), спочатку розроблений як протокол далекого космічного зв'язку, отримує все більше застосування і в комп'ютерних мережах. У розробці протоколу брав участь Гвинт Серф (Vint Cerf), нині віце-президент компанії Google.

Новому протоколу DTN не страшні затримки, знищення пакетів і втрата з’єднання, коли космічний корабель знаходитися за планетою, під час сонячних штормів і тривалих затримок, при проходженні сигналу в космосі.

Для перевірки можливостей цього протоколу була створена мережа з десяти вузлів. Одним з них став космічний апарат Ерохі (стартував в січні 2005 року), розташований на відстані 32,19 млн км. від Землі, який в цьому експерименті імітував марсіанську станцію ретрансляції. Решта вузлів залишилася на Землі – вони імітували посадочні модулі і орбітальні модулі на

Марсі. Експеримент продовжувався протягом місяця. NASA продовжило випробування у літку 2009 р., коли устаткування відправили на Міжнародну космічну станцію. У листопаді 2012 NASA та Європейське космічне агентство (ЄКА) успішно протестували передачу даних з МКС на Землю. У рамках експерименту з перевірки працездатності нового протоколу DTN командир МКС Саніта Вільямс (Sunita Williams) управляла з орбіти невеликим роботом з деталей конструктора "Лего", що знаходиться в європейському центрі управління польотами в німецькому Дармштадті.

Одночасно з розробкою подібних протоколів постає проблема оцінки надійності та якості роботи такої мережі. Очевидно, що моделі надійності для мереж, що працюють на традиційному протоколі TCP, у разі DTN мережі не підходять. Крім того, очевидно, що при збереженні апаратної частини комп'ютерної мережі при переході на протокол DTN зміниться сегмент транспортної мережі, що відповідає за технологію передачі даних.

На рис. 5 представлена архітектура протоколів, що використовуються в DTN мережах. У зв'язку з вищевикладеним виникає необхідність у часткової модифікації протоколу HTTP для роботи в DTN мережах. Подальші дослідження в цій області зосереджуються на можливості розробки відповідних засобів прикладного рівня, здатних працювати в мережах DTN.

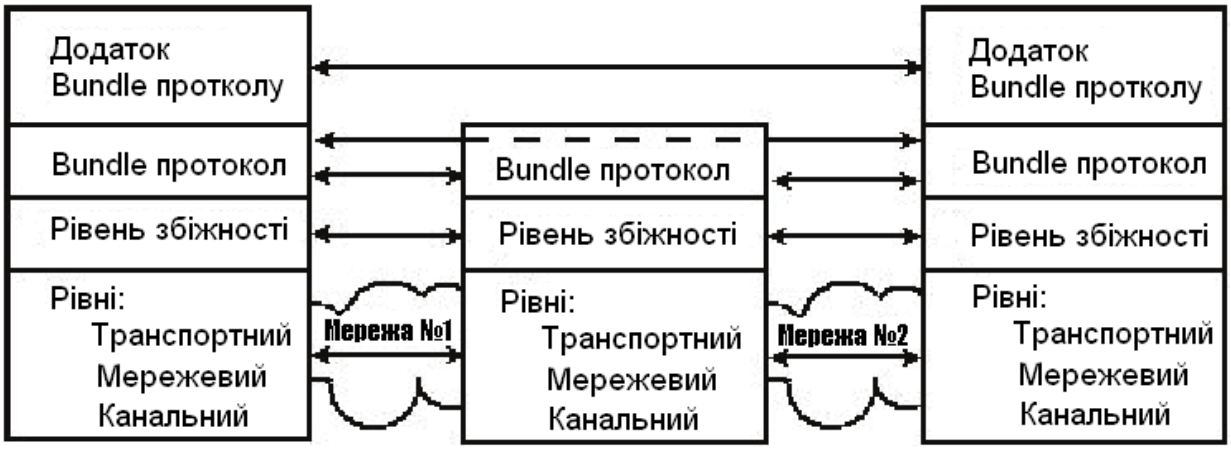

Рисунок 5 – Архітектура DTN протоколів

3 ДОСЛІДЖЕННЯ ПРИНЦИПІВ СУПУТНИКОВОЇ ТЕХНОЛОГІЇ

В сучасному світі інформація більше не прив’язана виключно до наземних мереж. Тепер, завдяки бездротовій технології, вона пронизує простір і відбивається від сузір’я супутників. Не дивлячись на те що потенціал сучасних супутникових систем використовується далеко не повністю, вони забезпечують незалежну від місцезнаходження комутовану широкосмугову передачу, завдяки якій мережі і додатки здатні досягти самих віддалених куточків Землі – гірські вершини, пустелі і тому подібні місця. Розглядаючи передачу мережевої інформації через космос з точки зору її перспектив, необхідно враховувати, що такі чинники, як ціна, доступність і реалізація, повинні відповідним чином змінитися, інакше ця технологія не набуде широкого поширення [2][1)].

3.1 Принципи супутникової технології

Розглянемо основи супутникового зв’язку. Принципи супутникової технології досить прості. Супутникові системи зв’язку передають сигнали від наземних трансиверів (приймачів/передавачів) на супутникові ретранслятори (приймачі/передавачі, що знаходяться на супутниках). Ретранслятор приймає сигнал від наземної станції в мікрохвильовому діапазоні, підсилює його і посилає назад на Землю. Передача на супутник називається висхідним каналом, а з супутника – низхідним.

Параболічні антени наземних станцій націлені на супутник, а ущільнені сигнали, що містять сотні каналів, надходять на супутник у вигляді надвисокочастотних хвиль. Ці сигнали перенаправляються ретранслятором на віддалені термінали. Завдяки радіочастотному устаткуванню модуляції і демодуляції радіочастотний сигнал може переносити інформацію по всій мережі.

[1)] [2] Таненбаум Э., Уэзеролл Д. Компьютерные сети. 5-е изд. СПб.: Питер, 2012. 960 с.: ил.

Окрім свого звичного амплуа (телефонія, телебачення, передача даних та інш.) супутники використовуються як резервні канали зв'язку на випадок виходу з ладу наземної лінії.

Супутники зв'язку мають певні властивості, що роблять їх надзвичайно привабливими для самих різних сфер застосування. Найпростіше уявити собі супутник зв'язку у вигляді свого роду величезного мікрохвильового повторювача, що висить в небі. Він включає декілька транспондерів, кожен з яких налаштований на певну частку частотного спектру. Транспондери підсилюють сигнали і перетворюють їх частоту на нову, щоб при відправці на Землю відображений сигнал не накладався на прямий.

Низхідний промінь може бути як широким, покриваючим величезні простори на Землі, так і вузьким, який можна прийняти в області, обмеженій лише декількома сотнями кілометрів. Останній метод називається трубою.

Відповідно до закону Кеплера, період обертання супутника дорівнює радіусу орбіти в ступені 3/2. Таким чином, чим вище орбіта, тим довше період. Поблизу поверхні Землі період обертання навколо неї складає приблизно 90 хвилин. Отже, супутники, розташовані на малій висоті, дуже швидко зникають з зони прийому-передачі пристроїв, розташованих на Землі, тому необхідно організовувати безперервні зони покриття. На висоті 35 800 км. період складає 24 години. А на висоті 384 000 км. супутник буде обертатися навколо Землі цілий місяць, в чому може переконатися будь-який бажаючий, що спостерігає за Місяцем.

Звичайно, період обертання супутника дуже важливо мати на увазі, але це не єдиний критерій, по якому визначають, де його розташувати. Необхідно прймати до уваги так звані пояси Ван Аллена (Van Allen belts) – області скупчення часток з великим зарядом, що знаходяться в зоні дії магнитного поля Землі. Будь-який супутник, потрапивши в такий пояс, досить швидко буде знищено цими частками. В результаті урахування цих чинників були виділені три зони, в яких можна безпечно розміщувати штучні супутники. Вони зображені на рис. 6. З цього ж малюнка можна дізнатися про деякі їх

властивості. Коротко розглянемо супутники, що розміщуються в кожній з цих трьох зон [11][1)].

Геостаціонарні супутники. Про супутники, що обертаються на великій висоті, говорять, що вони розташовані на геостаціонарній орбіті (GEO, Geostationary Earth Orbit). Геостаціонарна орбіта – кругова орбіта, розташована над екватором Землі (0° широти), перебуваючи на якій штучний супутник обертається навколо планети з кутовою швидкістю, рівною кутовій швидкості обертання Землі навколо осі [12][2)]. У горизонтальній системі координат напрям на супутник не змінюється ні по азимуту ні по висоті над горизонтом, супутник «висить» в небі нерухомо.

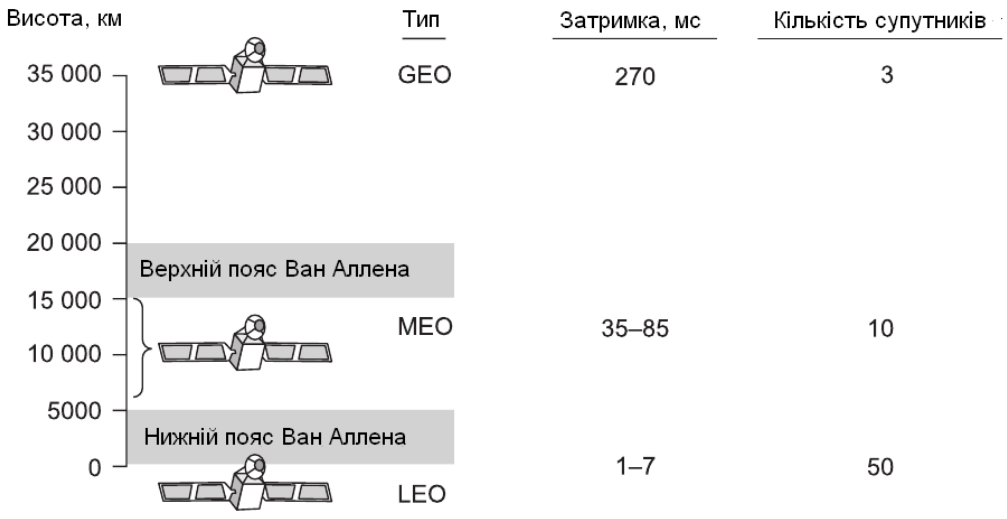

Рисунок 6 – Супутники зв’язку і їх властивості: висота орбіти, затримка, число супутників, необхідне для покриття всієї поверхні земної кулі

Геостаціонарна орбіта є різновидом геосинхронних орбіт і використовується для розміщення штучних супутників (комунікаційних, телетрансляційних і т. п.). Супутник повинен повертати в напрямку обертання Землі, на

[1)] [11] Special issue on DTN. Journal of Communications. 2010. V. 5. № 2. P. 106–130.

[2)] [12] Wikipedia. Геостаціонарна орбіта. URL: http:// http://uk.wikipedia.org/wiki/Гео стаціонарна_орбіта (дата звернення 20.09.2019).

висоті 35 786 км над рівнем моря. Саме така висота забезпечує супутнику період обігу, що дорівнює періоду обертання Землі щодо зірок (Зоряна доба: 23 години 56 хвилин 4,091 секунди).

Середньовисотні супутники. На набагато нижчих висотах, ніж геостаціонарні супутники, між двома поясами Ван Аллена, розташовуються середньовисотні супутники (MEO, Medium-Earth Orbite Satellites). Якщо дивитися на них із Землі, то буде помітно їх повільне дрейфування по небозводу. Середньовисотні супутники роблять повний оберт довкола нашої планети приблизно за 6 годин. Відповідно, наземним приймачам необхідно стежити за їх переміщенням. Оскільки ці супутники знаходяться набагато нижче, ніж геостаціонарні, то і «засвічуєма» ними область на поверхні Землі має скромніші розміри. Зате для зв'язку з ними потрібні менш потужні передавачі. Супутники MEO не використовуються в телекоммуникациях, але даний час середньовисотні супутники знаходять все більше вживання в телекомунікаціях, особливо в стільниковому телефонному зв'язку, тобто мобільний Інтернет також проходить через цей вид супутників, що вкрай важливо для сучастності та майбутніх мобільних технологій. Прикладами середньовисотних супутників є 24 супутники системи GPS (Global Positioning System) глобальна система визначення місцезнаходження), що обертаються довкола Землі на висоті близько 18 тис. км.

Низькоорбітальні супутники. Понизимо висоту ще більше і перейдемо до розгляду низькоорбітальних супутників (LEO, Low-Earth Orbite Satellites). Для того, щоб створити цілісну систему, що охоплює всю земну кулю, потрібна велика кількість таких супутників. Причиною тому є, перш за все, висока швидкість їх руху по орбіті. З іншого боку, завдяки відносно невеликій відстані між наземними передавачами і супутниками не вимагається особливо потужних наземних передавачів, а затримки складають всього лише декілька мілісекунд.

У цій супутниковій мережі користувачі мають високошвидкісний доступ до Internet і до інтерактивних служб. Сервер бездротового доступу функ-

ціонує як інтерфейс між мережею Ethernet 10/100/1000 і супутниковими компонентами мережі (рис. 7).

Згідно з сучасними технологіями, розташування супутників частіше, ніж через кожні 2° в 360-градусній екваторіальній площині, є нераціональним. Інакше можлива інтерференція сигналів. Отже, якщо на кожні два градуси доводиться 1 супутник, то всього їх в екваторіальній площині можна розмістити 360/2 = 180. Сто вісімдесят супутників можуть одночасно знаходитися в небі і обертатися в одній і тій же площині на одній і тій же висоті. Проте біля кожного транспондера є можливість працювати на різних частотах і з різною поляризацією, що дозволяє збільшити максимальну пропускну спроможність всієї системи.

Рисунок 7 – Бездротовий доступ до Internet

3.2 Проблеми та особливості супутникового зв'язку, як фізичного рівня для реалізації протоколу DTN

Процес виділення орбіт, який контролює організація ITU, дуже сильно пов'язаний з політикою. Це пояснюється високими потенційними доходами,

які держава може отримувати, здаючи в оренду ділянки космосу. Комерційний зв'язок – це далеко не єдине вживання супутників зв'язку, а значить, і їх орбіт. Ними користуються оператори супутникового телебачення, урядові структури і військові.

ITU були виділені частотні діапазони, призначені виключно для супутників зв'язку. Найважливіші з них показані в табл. 1.

Таблиця 1 – Основні частотні діапазони супутників зв'язку

Діапазон	Низхідні сигнали	Висхідні сигнали	Ширина смуги	Проблеми
L	1,5 ГГц	1,6 ГГц	15 МГц	Вузька смуга; переповнений
S	1,9 ГГц	2,2 ГГц	70 МГц	Вузька смуга; переповнений
C	4,0 ГГц	6,0 ГГц	500 МГц	Наземна інтерференція
Ku	11 ГГц	14 ГГц	500 МГц	Дощ
Ka	20 ГГц	30 ГГц	3500 МГц	Дощ, вартість устаткування

Перші геостаціонарні супутники зв'язку мали один промінь, який охоплював приблизно 1/3 земної поверхні і називався крапковим променем. Проте у міру здешевлення, зменшення розмірів і енергоємності мікроелектронних елементів почали з'являтися складніші стратегії. Стало можливим обладнати кожен супутник декількома антенами і декількома транспондерами. Кожен низхідний промінь сфокусували на невеликій території; таким чином змогли здійснити одночасну передачу декількох сигналів. Зазвичай ці так звані плями мають форму овалу і можуть мати відносно малі розміри – порядку декілька сотень кілометрів. Американський супутник зв'язку охоплює широким променем 48 штатів, а також має два вузьких променя для Аляски і Гавайських островів.

Новим витком розвитку супутників зв’язку стало створення недорогих мініатюрних апертурних терміналів – VSAT (Very Small Aperture Terminal) [13][1)]. Біля цих невеликих станцій є антена діаметром всього 1 м (порівняєте з 10-метровій антеною GEO), їх вихідна потужність складає приблизно 1 Вт. Швидкість роботи в напрямі Земля – супутник зазвичай складає 19,2 Кбіт/с, зате зв’язок супутник – Земля можна підтримувати на швидкості 512 Кбіт/с і вище. Супутникове широкомовне телебачення використовує цю технологію для однобічної передачі сигналу.

Багатьом мікростанціям VSAT не вистачає потужності для того, щоб зв’язуватися один з одним (через супутник, зрозуміло). Для вирішення цієї проблеми встановлюються спеціальні наземні концентратори з великою потужною антеною. Концентратор (хаб) розподіляє трафік між декількома VSAT, як зображено на рис. 8. У такому режимі або приймач, або передавач обов’язково має велику антену і потужний підсилювач. Недоліком такої системи є наявність затримок, гідністю – низька ціна за повноцінну систему для кінцевого користувача [13][2)].

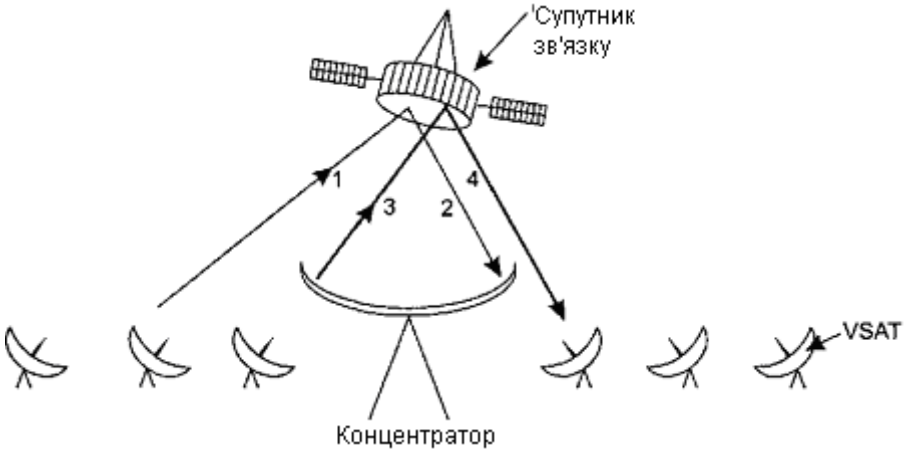

Рисунок 8 – Хаб розподіляє трафік між декількома VSAT

[1)] [13] Abramon N. Internet Access Using VSATs. IEEE Commun. Magazine. July, 2000. V. 38, P. 60–68.

[2)] [13] Abramon N. Internet Access Using VSATs. IEEE Commun. Magazine. July, 2000. V. 38, P. 60–68.

Системи VSAT мають великі перспективи використання в сільській місцевості (рис. 9). Половина населення земної кулі живе мінімум в годині ходьби від найближчого телефону. Протягнути телефонні лінії до всіх сіл не по кишені більшості країн так званого третього світу. Проте засобів на монтаж тарілки VSAT, що живиться від сонячної батареї, може вистачити не лише біля адміністрації регіону, але і біля приватних осіб. Таким чином, VSAT – це технологія, яка може дозволити організувати зв’язок в будь-якій точці планети.

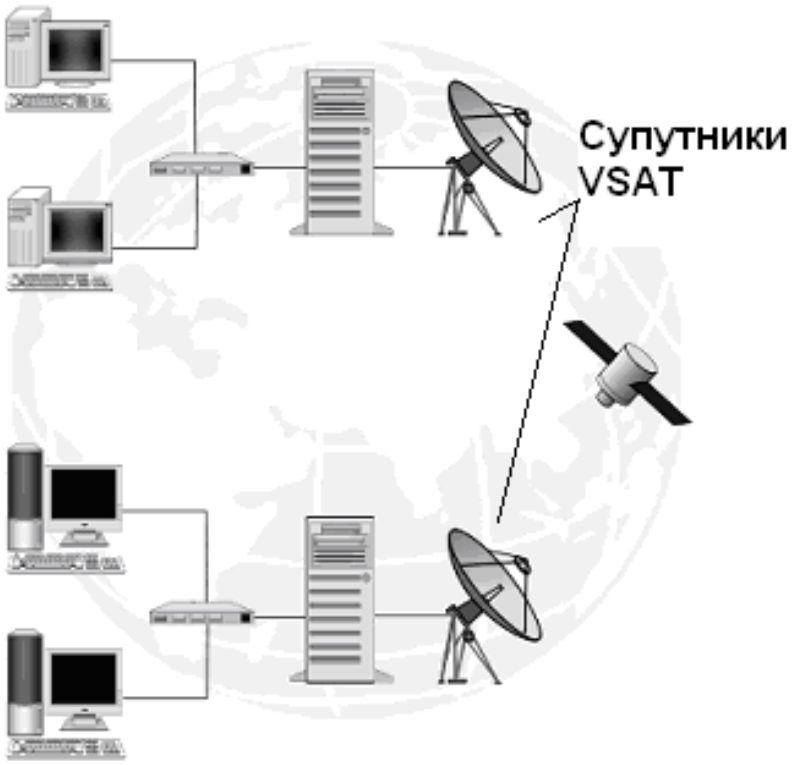

Рисунок 9 – Приклад реалізації системи VSAT для надання послуг та сервісів віддаленим територіям без дротових комунікацій

Супутники зв’язку володіють лавою властивостей, які радикально відрізняють їх від будь-яких наземних систем зв’язку між абонентами. По-перше, не дивлячись на гранично високу швидкість поширення сигналу (власне, вона практично дорівнює швидкості світла – 300´000км/с), відстані між наземними пристроями, що передають і приймають, і супутниками такі, що в

технології GEO затримки опиняються вельми значними. Залежно від взаємного розташування користувача, наземної станції і супутника час передачі може складати 250-300 мс. Зазвичай воно складає 270 мс (відповідно, в два рази більше – 540 мс – в системах VSAT, що працюють через хаб). Для порівняння, сигнал в наземних мікрохвильових системах зв'язку поширюється зі швидкістю зразковий 3 мкс/км, а коаксіальний кабель і оптоволокно мають затримку порядка 5 мкс/км. Різниця затримок тут пояснюється тим, що в твердих тілах сигнал поширюється повільніше, ніж в повітрі.

Ще однією важливою властивістю супутників є те, що вони є виключно широкомовним засобом передачі даних. На відправку повідомлення сотень абонентів, що знаходяться в зоні прямування супутника, не витрачаються ніяких додаткових ресурсів в порівнянні з відправкою повідомлення одному з них. Наприклад, можна уявити собі кешування на супутнику популярних веб-сторінок, що різко підвищить швидкість їх завантаження на сотні комп'ютерів, що знаходяться досить далеко один від одного. Звичайно, широкомовлення стимулюється звичайними двоточковими мережами, проте супутникове мовлення в цьому випадку обходиться значно дешевшим. З іншого боку, з точки зору захисту інформації і конфіденційності даних, супутники – це прямо-таки біда: хто завгодно може прослуховувати абсолютно все. Тут на захист тих, кому важливий обмежений доступ до інформації, встає криптографія. Супутники зв'язку володіють ще однією чудовою властивістю – незалежністю вартості передачі від відстані між вузлами. Дзвінок другу, що живе за океаном, коштує стільки ж, скільки дзвінок подружці, що живе в сусідньому будинку. Космічні телекомунікаційні технології, крім того, забезпечують дуже високий ступінь захисту від помилок і можуть бути розгорнені на місцевості практично миттєво, що дуже важливе для військових.

Для кращого практичного розуміння застосування супутникових технологій у наш час та проведення деякої паралелі використання цього досвіду у протоколі DTN, звернемося до великих компаній-першопрохідців, наприклад Глобалстар або Ірідіум.

Глобалстар – низькоорбітальна супутникова цифрова система зв'язку, що надає послуги бездротової портативної телефонії і інші телекомунікаційні послуги по всьому світу [14][1)]. Система Глобалстар (рис. 10) складається з 48 експлуатаційних і 8 запасних супутників.

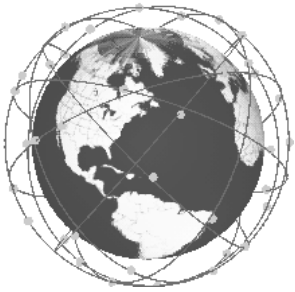

Рисунок 10 – Групування супутників компанії Глобалстар

Низькоорбітальні супутники Глобалстар розташовані набагато ближче до Землі, ніж супутники геостаціонарної орбіти Землі, на відстані 644-2575 км. (400-1600 милі) від Землі, що дозволяє скоротити, як затримки при напрямі дзвінків з супутника і на супутник, так і розміри телефонів і антен. Кожен супутник важить приблизно 450 кг і формує зони покриття земної кулі, що перекривають один одного (рис. 11).

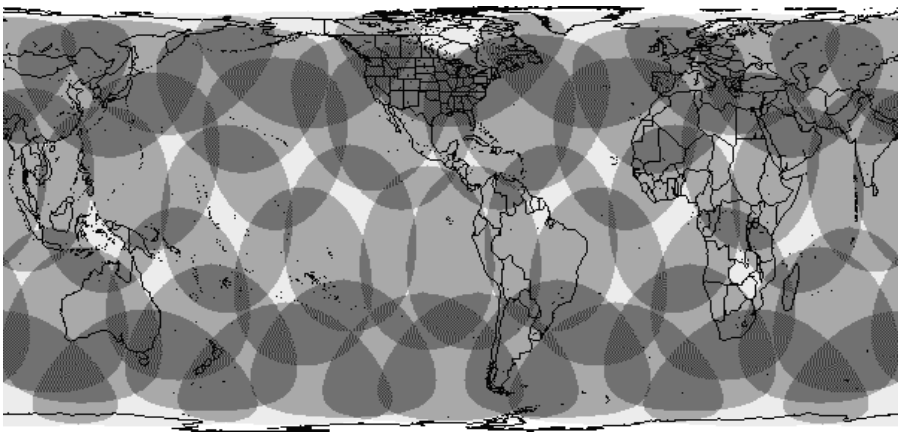

Рисунок 11 – Карта зон покриття компанії Глобалстар

[1)] [14] Глобалстар – Википедия. URL: http://ru.wikipedia.org/wiki/Глобалстар (дата звернення 25.09.2019).

4 ПОРІВНЯЛЬНИЙ АНАЛІЗ ПРОТОКОЛІВ TCP/IP І DTN

У розділі 3 магістерської роботи були розглянуті особливості супутникового зв'язоку (в деякому розумінні фізичного рівня) стосовно протоколу DTN. Тепер поговоримо про програмну реалізацію, або реалізацію на значно вищих рівнях згідно еталонної моделі OSI, але у суровій порівняльній формі з протоколом TCP/IP, який для нас є базовим або фундаментальним.

Відомо, що протокол DTN працює на основі стеку протоколів TCP/IP. Оскільки стек TCP/IP спочатку створювався для Інтернету, він має багато особливостей, що дають йому перевагу перед іншими протоколами, коли мова заходить про побудову мереж, що включають глобальні зв’язки. Зокрема, дуже корисною властивістю, що робить можливим вживання цього протоколу у великих мережах, є його здатність фрагментувати пакети. Дійсно, велика складена мережа часто складається з мереж, побудованих на абсолютно різних принципах. У кожній з цих мереж може бути власна величина максимальної довжини одиниці переданих даних (кадру). У такому разі при переході з однієї мережі, що має велику максимальну довжину, в мережу з меншою максимальною довжиною може виникнути необхідність ділення переданого кадру на декілька часток. Протокол IP стека TCP/IP ефективно вирішує цю задачу.

Іншою особливістю технології TCP/IP є гнучка система адресації, що дозволяє простіше, ніж інші протоколи аналогічного призначення включати в складену мережу мережі різних технологій. Ця властивість також сприяє вживанню стека TCP/IP для побудови великих гетерогенних мереж.

У стеку TCP/IP дуже економно використовуються широкомовні розсилки. Ця властивість абсолютно необхідна при роботі на повільних каналах зв’язку, характерних для територіальних мереж.

Проте, як і завжди, за отримувані переваги треба платити, і платою тут виявляються високі вимоги до ресурсів і складність адміністрування IP-мереж. Гнучка система адресації і відмова від широкомовних розсилок при-

водять до наявності в IP-мережі різноманітних централізованих служб типу DNS, DHCP і тому подібне. Кожна з цих служб спрямована на полегшення адміністрування мережі, але в той же час сама вимагає пильної уваги з боку адміністраторів.

На рис. 12 наведена структура стека TCP/IP. В розділі 1 магістерської роботи вже був проведений аналіз структури стеку TCP/IP, в цьому роздлі більш детальнішу увагу приділимо протоколам стека.

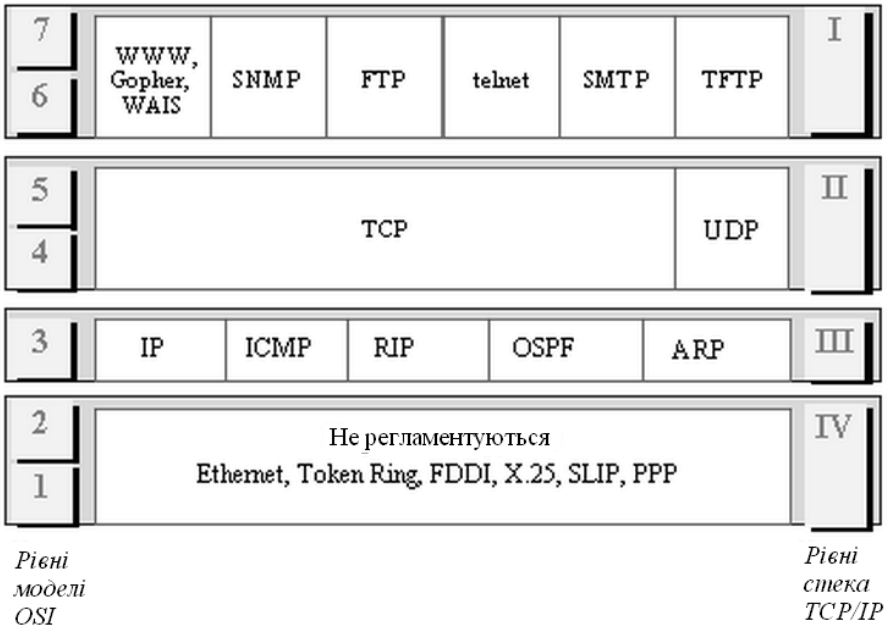

Рисунок 12 – Архітектура стека TCP/IP

Прикладний рівень (I) стека TCP/IP об’єднує служби, що надаються системою і призначені для користувача. До них відносяться такі поширені протоколи, як протокол передачі файлів (File Transfer Protocol, FTP), протокол емуляції терміналу (telnet), звичайний протокол передачі електронної пошти (Simple Mail Transfer Protocol, SMTP), протокол передачі гіпертексту (HyperText Transfer Protocol, HTTP) і багато інших. Протоколи прикладного рівня розгортаються на хостах.

Транспортний рівень (II) стека TCP/IP може надавати вище розміщеному рівню два типа сервісу:

– гарантовану доставку забезпечує протокол управління передачею (Transmission Control Protocol, TCP);
– доставку по можливості, або з максимальними зусиллями, забезпечує протокол призначених для користувача дейтаграм (User Datagram Protocol, UDP).

Мережевий рівень (III), чи рівень Інтернету, є стрижнем всієї архітектури TCP/IP. Саме цей рівень, функції якого відповідають мережевому рівню моделі OSI, забезпечує переміщення пакетів в межах складеної мережі, утвореної об'єднанням безлічі мереж. Протоколи мережного рівня підтримують інтерфейс з вище розміщеним транспортним рівнем, отримуючи від нього запити на передачу даних по складеній мережі, а також з нижче зазначеним рівнем мережевих інтерфейсів.

Ідеологічною відзнакою архітектури стека TCP/IP від багаторівневої організації інших стеків є інтерпретація функцій самого нижчого рівня – рівня мережевих інтерфейсів. Нагадаємо, що нижчі рівні моделі OSI (канальний і фізичний) реалізують велику кількість функцій доступу до середи передачі, формування кадрів і узгодження рівнів електричних сигналів, кодування і синхронізації і деякі інші. Всі ці вельми конкретні функції складають суть таких протоколів обміну даними, як Ethernet, Token Ring, PPP, HDLC і багато інших.

У нижнього рівня стека TCP/IP завдання істотно простіше – він відповідає тільки за організацію взаємодії з технологіями мереж, що входять в складену мережу. Завдання забезпечення інтерфейсу між технологією TCP/IP і будь-якою іншою технологією проміжної мережі спрощено можна звести [15][1)]:

– до визначення способу упаковки (інкапсуляції) IP-пакета в одиницю даних, що передаються, проміжній мережі;
– до визначення способу перетворення мережевих адрес в адреси технології даної проміжної мережі.

[1)] [15] Буров Є.В. Комп'ютерні мережі. Львів: Магнолія, 2012. 264 с.

Такий підхід робить складену мережу TCP/IP відкритою для включення будь-якої мережі, яку б внутрішню технологію передачі даних ця мережа не використовувала. Тому рівень мережевих інтерфейсів (IV) в стеку TCP/IP не регламентується. Він підтримує всі популярні технології; для локальних мереж – це Ethernet, Token Ring, FDDI, Fast Ethernet, Gigabit Ethernet, для глобальних мереж – протоколи двокрапкових з'єднань SLIP і PPP, технології X.25, Frame Relay, ATM.

4.1 Аналіз функціонування протоколу DTN на основі стеку протоколів TCP/IP

В цьому розділі більш детальніше розглянемо будову та властивості протоколів стеку TCP/IP. Користуючись цим матеріалом пізніші виконаємо моделювання протоколу DTN.

4.1.1 Протокол дозволу адрес

Як вже було сказано, ніякої залежності між локальною адресою та її IP-адресою не існує, отже, єдиний спосіб установлення з'єднання – ведення таблиць. В результаті конфігурування мережі кожен інтерфейс знає свою IP-адресу і локальну адресу, що можна розглядати як таблицю, що складається з одного рядка. Проблема полягає в тому, як організувати обмін наявною інформацією між вузлами мережі. Для визначення локальної адреси за IP-адресою використовується протокол дозволу адрес (Address Resolution Protocol, ARP). Протокол дозволу адрес реалізується різним чином в залежності від того, чи працює в цій мережі протокол локальної мережі (Ethernet, Token Ring, FDDI) з можливістю широкомовлення або ж будь-якої з протоколів глобальної мережі (X.25, Frame Relay), які, як правило, не підтримують широкомовний доступ.

Розглянемо роботу протоколу ARP в локальних мережах з широкомовлення. На рис. 13 зображено фрагмент IP-мережі, що включає дві мережі – Ethernet1 (з трьох кінцевих вузлів A, B і C) і Ethernet2 (з двох кінцевих вузлів D і E). Кожен мережевий інтерфейс має IP-адресу та MAC-адресу. Нехай у якийсь момент IP-модуль вузла C спрямовує пакет вузлу D.

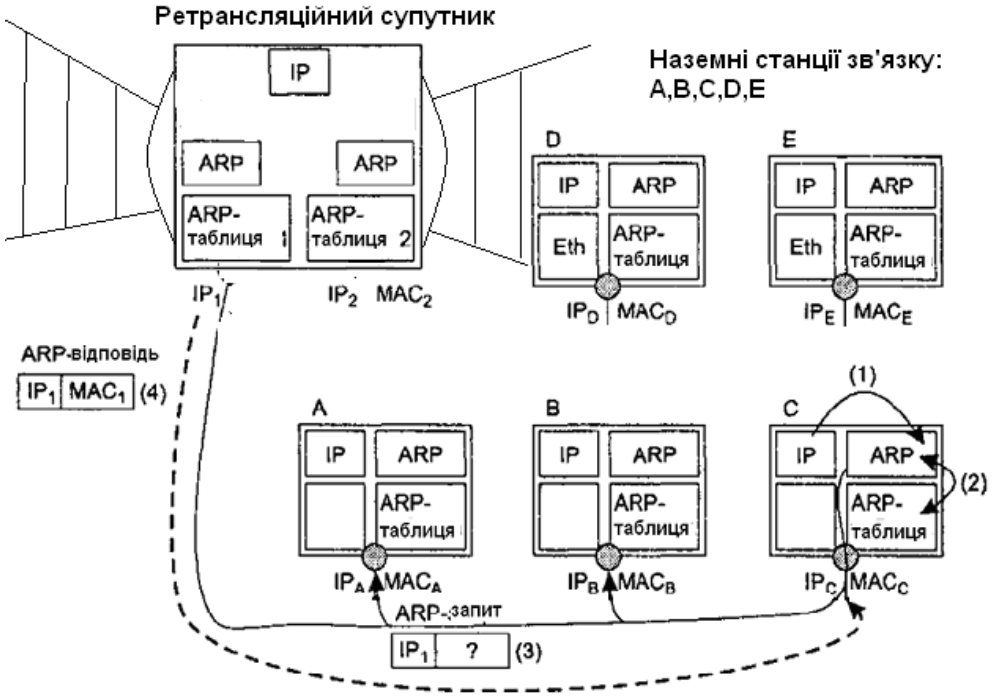

Рисунок 13 – Схема роботи протоколу ARP

Протокол IP вузла C визначив IP-адресу інтерфейсу наступного маршрутизатора – це IP1. Тепер, перш ніж упакувати пакет в кадр Ethernet і направити його маршрутизатору, необхідно визначити відповідну MAC-адресу. Для вирішення цієї задачі протокол IP звертається до протоколу ARP. Протокол ARP підтримує на кожному інтерфейсі мережного адаптера або маршрутизатора окрему ARP-таблицю, в якій в ході функціонування мережі накопичується інформація про відповідність між IP-адресами і MAC-адресами інших інтерфейсів даної мережі. Спочатку, при увімкненні комп'ютера або маршрутизатора в мережу, всі його ARP-таблиці порожні.

На першому кроці відбувається передача від протоколу IP протоколу ARP приблизно такого повідомлення: «Яку MAC-адресу має інтерфейс з адресою IP1?»

Робота протоколу ARP починається з перегляду ARP-таблиці відповідного інтерфейсу. Припустимо, що серед записів, що містяться в ній, відсутня запитана IP-адреса.

У цьому випадку вихідний IP-пакет, для якого виявилося неможливим визначити локальну адресу зі ARP-таблиці, запам'ятовується в буфері, а протокол ARP формує ARP-запит, вкладає його в кадр протоколу Ethernet і широкомовно розсилає [16][1)].

Всі інтерфейси мережі Ethernet 1 одержують ARP-запит і спрямовують його до «свого» протоколу ARP. ARP порівнює зазначену у запиті адресу IP1 з IP-адресою інтерфейсу, на який надійшов цей запит. Протокол ARP, який констатував збіг (в даному випадку це ARP маршрутизатора 1), формує ARP-відповідь.

У ARP-відповіді маршрутизатор вказує локальну адресу MAC1 свого інтерфейсу і відправляє його запитуваному вузлу (в даному прикладі вузлу C), використовуючи його локальну адресу. Широкомовна відповідь у цьому випадку не потрібна, так як формат ARP-запиту передбачає поля локальної та мережевої адрес відправника. Зауважимо, що зона розповсюдження ARP-запитів обмежується мережею Ethernet 1, так як на шляху широкомовних кадрів бар'єром стоїть маршрутизатор.

На рис. 14 зображено кадр Ethernet з вкладених в нього ARP-повідомленням. ARP-запити та ARP-відповіді мають один і той же формат. У табл. 2, як приклад, наведені значення полів реального ARP-запиту, переданого по мережі Ethernet.

[1)] [16] Гайсина Л.Ф. Сети и телекоммуникации. Учебное пособие. Оренбург, ГОУ ОГУ, 2004. 160 с.

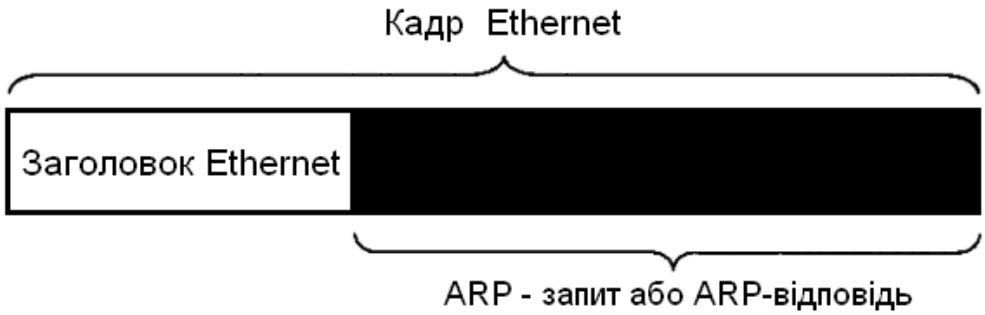

Рисунок 14 – Інкапсуляція ARP-повідомлення у кадр Ethernet

Таблиця 2 – Приклад ARP-запиту

Поле	Значення
Тип мережі	1 (0x1)
Тип протоколу	2048 (0x800)
Довжина локальної адреси	6(0x6)
Довжина мережевої адреси	4 (0x4)
Операція	1 (0x1)
Локальна адреса відправника	008048EB7E60
Мережна адреса відправника	194.85.135.75
Локальна (бажана) адреса одержувача	000000000000
Мережний адресу одержувача	194.85.135.65

У полі типу мережі для мереж Ethernet вказується значення 1. Поле типу протоколу дозволяє використовувати протокол ARP не тільки з протоколом IP, але і з іншими мережевими протоколами. Для IP значення цього поля дорівнює 0x0800. Довжина локальної адреси для протоколу Ethernet дорівнює 6 байт, а довжина IP-адреси – 4 байт. У полі операції для ARP-запитів вказується значення 1, для ARP-відповідей – значення 2. З цього запиту видно, що у мережі Ethernet вузол з IP-адресою 194.85.135.75 намагається визначити, яку MAC-адресу має інший вузол тієї ж мережі, мережева адреса якого

194.85.135.65. Поле шуканої локальної адреси заповнено нулями. Відповідь надсилає вузол, який розпізнав свою IP-адресу.

Якщо в мережі немає машини з необхідною IP-адресою, то ARP-відповіді не буде. Протокол IP знищує IP-пакети, що направляються за цією адресою. У табл. 3 показані значення полів ARP-відповіді, які могли б поступити на наведений у таблиці 2 ARP-запит. Але в нашому випадку IP-пакети не буде знищено, – вони будуть зберігатися у спеціальній буферній пам’яті до того часу, поки не буде знайдено необхідного мережного вузла (тобто доти, доки наступний супутник не з’явиться у зоні передачі інформаційного сигналу. І коли нарешті кінцевий вузол отримує необхідні пакети, – завдання можна вважати виконаним).

Таблиця 3 – Приклад ARP-відповіді

Поле	Значення
Тип мережі	1 (0x1)
Тип протоколу	2048 (0x800)
Довжина локальної адреси	6(0x6)
Довжина мережевої адреси	4 (0x4)
Операція	1 (0x1)
Локальна адреса відправника	00E0F77F1920
Мережна адреса відправника	194.85.135.65
Локальна (бажана) адреса одержувача	008048EB7E60
Мережний адресу одержувача	194.85.135.75

У результаті обміну ARP-повідомленнями модуль IP, що надіслав запит з інтерфейсу, що має адресу 194.85.135.75, визначив, що IP-адресі 194.85.135.65 відповідає MAC-адреса 00E0F77F1920. Ця адреса буде потім розташована в заголовок кадру Ethernet, що очікував відправлення IP-пакету. Щоб зменшити число ARP-звернень до мережі, знайдена відповідність між

IP-адресою та MAC-адресою зберігається в ARP-таблиці відповідного інтерфейсу, у даному випадку – це запис 194.85.135.65 – 00E0F77F1920.

Даний запис у ARP-таблиці з'являється автоматично, через кілька мілісекунд після того, як модуль ARP проаналізує ARP-відповідь. Тепер, якщо раптом знову виникне необхідність надіслати пакет за адресою 194.85.135.65, то протокол IP, перш ніж посилати широкомовний запит, перевірить, чи немає вже такої адреси в ARP-таблиці.

ARP-таблиця поповнюється не тільки за рахунок надходжень на даний інтерфейс ARP-відповідей, але і в результаті вилучення корисної інформації з широкомовних ARP-запитів. Дійсно, в кожному запиті, як це видно з таблиць 2 та 3, містяться IP-адреса та MAC-адреса відправника. Всі інтерфейси, які отримали цей запит, можуть помістити інформацію про відповідність локальної і мережевої адрес відправника у власну ARP-таблицю. Зокрема, всі вузли, які отримали ARP-запит (див. табл. 4.1), можуть поповнити свою ARP-таблицю записом 194.85.135.75 – 008048EB7E60.

Таким чином, вид ARP-табліци, в яку в ході роботи мережі були додані два згадані нами записи, ілюструє табл. 4. У ARP-таблицях існує два типи записів: динамічні і статичні. Статичні записи створюються вручну за допомогою утиліти arp і не мають терміну застарівання, точніше, вони існують до тих пір, поки комп'ютер або маршрутизатор залишається увімкненим.

Таблиця 4 – Приклад ARP-таблиці

IP-адреса	MAC–адреса	Тип запису
194.85.135.65	00E0F77F1920	динамічний
194.85.135.75	008048EB7E60	динамічний
194.85.60.21	008048EB7567	статичний

Динамічні записи повинні періодично оновлюватися. Якщо запис не оновлювалась протягом певного часу (близько кількох хвилин), то він виключається з таблиці. Таким чином, в ARP-таблиці містяться записи не про

всі вузли мережі, а тільки про ті, які активно беруть участь в мережевих операціях. Оскільки такий спосіб зберігання інформації називають Caching, ARP-таблиці іноді називають ARP-кешем.

Деякі реалізації протоколів IP та ARP не ставлять IP-пакети в чергу на час очікування ARP-відповідей. Замість цього IP-пакет просто знищується, а його відновлення покладається на модуль TCP або прикладний процес, що працює через протокол UDP. Таке відновлення виконується за рахунок таймаутів і повторних передач. Повторна передача повідомлення проходить успішно, так як перша спроба вже викликала заповнення ARP-таблиці.

Зовсім інший спосіб розподілення адрес використовується в глобальних мережах, у яких не підтримується широкомовне розсилання. Тут адміністратору мережі найчастіше доводиться вручну формувати і розміщувати на будь-який сервер ARP-таблиці, в яких він задає, наприклад, відповідність IP-адрес адресам X.25, що мають для протоколу IP зміст локальних адрес. У той же час сьогодні намітилася тенденція автоматизації роботи протоколу ARP і в глобальних мережах. Для цієї мети серед усіх маршрутизаторів, підключених до якої-небудь глобальної мережі, виділяється спеціальний маршрутизатор, котрий веде ARP-таблицю для всіх інших вузлів і маршрутизаторів цієї мережі [17][1)].

При такому централізованому підході для всіх вузлів і маршрутизаторів вручну потрібно встановити тільки IP-адреси і локальні адреси виділеного для цих цілей маршрутизатора. При включенні кожен вузол і маршрутизатор реєструє свої адреси у виділеному маршрутизаторі. Кожного разу, коли виникає необхідність визначення по IP-адресі локальної адреси, модуль ARP звертається до виділеного маршрутизатора з запитом і автоматично отримує відповідь без участі адміністратора. Працюючий таким чином маршрутизатор називають ARP-сервером.

[1)] [17] Юрков А.В. Использование информационных ресурсов сети Интернет. Учебное пособие СПб: ЛОИРО, 2003. 37 с.

4.1.2 Алгоритм динамічного призначення адрес

Для нормальної роботи мережі кожному мережевому інтерфейсу комп’ютера і маршрутизатора повинна бути призначена IP-адреса.

Процедура присвоєння адрес відбувається в ході конфігурування комп’ютерів та маршрутизаторів. Протокол динамічного конфігурування хостів (Dynamic Host Configuration Protocol, DHCP) автоматизує процес конфігурування мережних інтерфейсів, гарантуючи від дублювання адрес за рахунок централізованого управління їх розподілом. Робота DHCP описана в RFC 2131 і 2132.

Протокол DHCP працює відповідно до моделі клієнт-сервер. Під час старту системи вузол мережі, який є DHCP-клієнтом, посилає в мережу широкомовний запит на отримання IP-адреси. DHCP-сервер відгукується і посилає повідомлення-відповідь, що містить IP-адресу та деякі інші конфігураційні параметри.

У режимі автоматичного призначення статичних адрес DHCP-сервер самостійно без втручання адміністратора довільним чином вибирає клієнту IP-адресу з пула IP-адрес. Адреса дається клієнту з пула в постійне користування, тобто між інформацію клієнта і його IP-адресою, як і раніше, як і при ручному призначення, існує постійна відповідність. Вона встановлюється в момент першого призначення DHCP-сервером IP-адреси клієнта. При всіх наступних запитах сервер повертає клієнту ту ж IP-адресу.

При динамічному розподіл адрес DHCP-сервер видає адресу клієнту на обмежений час, що називається терміном оренди. Коли комп’ютер (супутник), що являється DHCP-клієнтом, видаляється з підмережі, призначена йому IP-адреса автоматично звільняється. Коли комп’ютер (супутник) підключається до іншої підмережі, то йому автоматично призначається нова адреса. Ні користувач, ні мережевий адміністратор не втручаються у цей процес. Це дає можливість згодом повторно використовувати цю ж IP-адресу для призначення її іншому комп’ютеру. Таким чином, крім основної переваги DHCP –

автоматизації рутинної роботи адміністратора по конфігуруванню стека TCP/IP на кожному комп'ютері(супутнику), динамічне розділення адрес в принципі дозволяє будувати IP-мережу, кількість вузлів у якій перевищує кількість тих, що є в розпорядженні адміністратора IP-адрес.

Для зниження ризику виходу мережі з ладу з–за відмови DHCP-сервера у мережі іноді ставлять резервний DHCP-сервер (такий варіант відповідає мережі 1 на рис. 15).

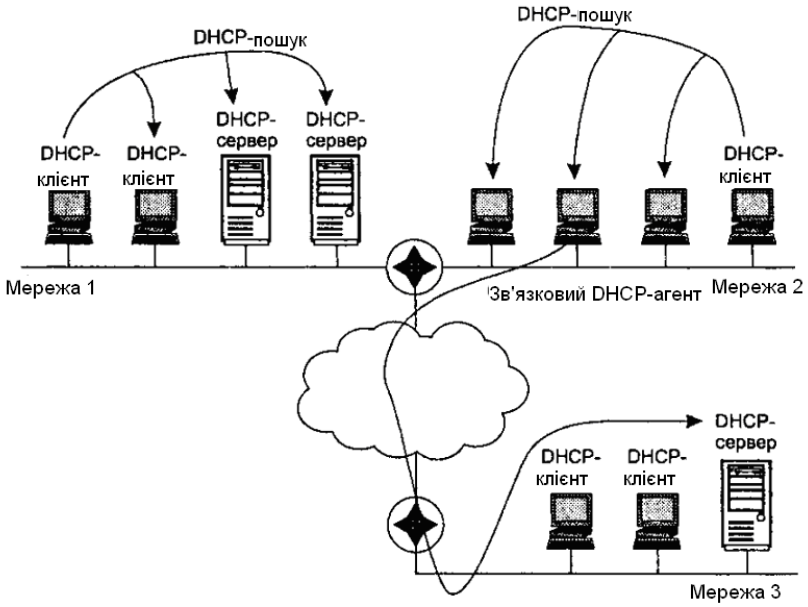

Рисунок 15 – Схема взаємного розташування
DHCP-серверів та DHCP-клієнтів

Нижче надана спрощена схема обміну повідомленнями між клієнтськими і серверними частинами DHCP [18][1)]:

– коли комп'ютер включають, встановлений на ньому DHCP-клієнт посилає обмежене широкомовне повідомлення DHCP-пошуку (IP-пакет з адресою призначення, що складається з одних одиниць, який повинен бути доставлено до всіх вузлів цієї IP-мережі);

[1)] [18] Абрамов В.О., Клименко С.Ю. Базові технології комп'ютерних мереж: Навчальний посібник К.:Київ ун-т ім. Б.Грінченка, 2011. 291 с.

- DHCP-сервери, що знаходяться в мережі, отримують це повідомлення. Якщо в мережі DHCP-сервери відсутні, то повідомлення DHCP-пошуку отримує зв'язковий DHCP-агент. Він пересилає це повідомлення в іншу, можливо, значно віддалену від нього мережу DHCP-сервера, IP-адреса якого йому заздалегідь відома;
- всі DHCP-сервери, що одержали повідомлення DHCP-пошуку, надсилають DHCP-клієнту, що звернувся із запитом, свої DHCP-пропозиції. Кожна пропозиція містить IP-адресу та іншу конфігураційні інформацію. (DHCP-сервер, що знаходиться в іншій мережі, посилає відповідь через агента);
- DHCP-клієнт збирає конфігураційні DHCP-пропозиції від усіх DHCP-серверів. Як правило, він обирає першу пропозицій,що надійшла, і відправляє в мережу широкомовний DHCP-запит. У цьому запиті містяться ідентифікаційна інформація про DHCP-сервер, пропозицію якого прийнято, а також значення прийнятих конфігураційних параметрів;
- всі DHCP-сервери отримують DHCP-запит, і тільки один обраний DHCP-сервер посилає позитивну DHCP-квитанцію (підтвердження IP-адреси і параметрів оренди), а інші сервери анулюють свої пропозиції, зокрема повертають у свої пули запропоновані адреси;
- DHCP-клієнт отримує позитивну DHCP-квитанцію і переходить в робочий стан.

Час від часу комп'ютер намагається оновити параметри оренди у DHCP-сервера. Першу спробу він робить задовго до закінчення терміну оренди, звертаючись до того сервера, від якого він отримав поточні параметри. Якщо відповіді немає або відповідь негативна, він через деякий час знову надсилає запит. Так повторюється кілька разів, і, якщо всі спроби отримати параметри у того ж сервера виявляються безуспішними, клієнт звертається до іншого сервера. Якщо і інший сервер відповідає відмовою, то клієнт втрачає свої конфігураційні параметри і переходить в режим автономної роботи.

DHCP-клієнт може і за своєю ініціативою достроково відмовитися від виділених йому параметрів.

У мережі, де адреси призначаються динамічно, не можна бути впевненим в адресі, яка в даний момент має той чи інший вузол. І таке різносторонність IP-адрес тягне за собою деякі проблеми.

По-перше, важко здійснювати віддалене управління і автоматичний моніторинг інтерфейсу (наприклад, збір статистики), якщо в якості його ідентифікатора виступає динамічно змінювана IP-адреса. Нарешті, для забезпечення безпеки мережі багатомережеві пристрої можуть блокувати (фільтрувати) пакети, певні поля яких мають деякі заздалегідь задані значення. Іншими словами, при динамічному призначенні адрес ускладнюється фільтрація пакетів за IP-адресами. Ці проблеми простіше всього вирішуються відмовою від динамічного призначення адрес для інтерфейсів, що фігурують в системах моніторингу та безпеки.

Ми розглянули звичайну наземну технологію розподілення та розташування комп’ютерів з використанням протоколу DHCP. У відкритому космосі процес встановлення DHCP-серверів дуже ускладнюється за рахунок дій різноманітних гравітаційних полів інших космічних об’єктів (планет, астероїдів, метеоритів та іншого), і тому тут необхідне постійне позиціонування супутника-сервера, а за наявністю таких перешкоджань палива для зберігання необхідного місця розташування вистачатиме лише на декілька років, – а цього недостатньо і економічно не вигідно (марнотратство часу та ресурсів на запуск та встановлення у необхідному місці нового супутника). Для вирішення цієї проблеми необхідним є поєднання на одній станції як DHCP-сервера, так і DHCP-клієнта, що дозволить супутникам, які встановлюють зв’язок, безпроблемно визначати IP-адреси зазначені у пулі адрес (але цим ми будемо користуватися тоді, коли загальна кількість супутників буде досить велика для призначення адрес власноруч). А тому, як кількість вузлів знаходиться у діапазоні близькому до 10, використання протоколу DHCP є нелогічним та помилковим – звідсіля IP-адреси супутників на початковому етапі будуть

статичними та призначатимуться власноруч адміністратором. Наприклад, супутнику „1” потрібно передати дані супутнику „2”, адреса якого йому відома (рис. 16).

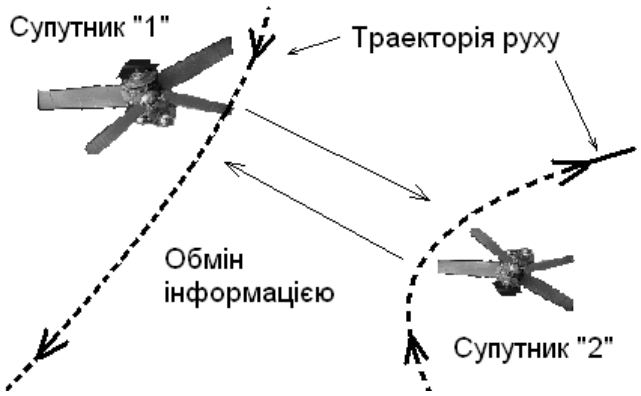

Рисунок 16 – Обмін даними між супутниками

4.1.3 Система DNS

DNS (Domain Name System, система доменних імен) – ієрархічна, розподілена в мережі система баз даних, що надає користувачам мережі додатковий сервіс (технічно реалізований на комп’ютерах – DNS серверах, на яких запущено спеціальне програмне забезпечення), по автоматичному перетворенню запитів, оформлених в зручному для людини текстовому форматі, наприклад, http://www.ipipe.ru, у цифрову IP адресу комп’ютера, наприклад 123.222.111.88, де знаходитися шуканий ресурс.

Отже, DNS – це ієрархічна система імен або ще говорять ієрархічний простір імен. Одиницею виміру цього простору є домен. Розглянемо що ж таке домен.

Домен – це область (зона) простору ієрархічних імен мережі Інтернет, яка обслуговується набором серверів доменних імен (DNS) і централізовано адмініструється. Домен ідентифікується ім’ям домену (доменним ім’ям). Доменне ім’я (від англ. Domain name) – аналог IP-адрес. Доменним ім’ям є по-

єднання символів розділених крапками. Доменне ім’я дозволяє ідентифікувати комп’ютер або будь-який інформаційний ресурс в мережі Інтернет. Ієрархію DNS найчастіше представляють у вигляді деревовидної структури. Так як DNS використовують у мережах достатньо великих, то цей протокол нам знадобиться у подальшій розробці та масштабуванні нової мережі (мережа, що моделюється мала за розмірами і цей сервіс нам не потрібний), тому на цьому зупинимося, а далі перейдемо до наступних протоколів стеку TCP, які знадобляться для побудови протоколу DTN.

4.1.4 Протокол IP

IP (Internet Protocol – міжмережевий протокол), описаний у документі RFC 751. У кожній черговій мережі, що лежить на шляху переміщення пакету, протокол IP звертається до засобів транспортування цієї мережі, щоб з їх допомогою передати пакет на маршрутизатор, що веде до наступної мережі, або безпосередньо на вузол-одержувача. Таким чином, однією з найважливіших функцій IP є підтримка інтерфейсу з нижче розташованими технологіями мереж, утворюючих складену мережу. Крім того, у функції протоколу IP входить підтримка інтерфейсу з протоколами вище розміщеного транспортного рівня, зокрема з протоколом TCP, який вирішує всі питання забезпечення надійної доставки даних по складеній мережі в стеку TCP/IP.

Розглянемо формат IP-пакету [1][1)]. Є прямий зв’язок між кількістю полів заголовка пакету і функціональною складністю протоколу, який працює з цим заголовком. Чим простіше заголовок – тим простіше відповідний протокол. Велика частка дій протоколу пов’язана з обробкою тієї службової інформації, яка переноситься в полях заголовка пакету. Вивчаючи призначення кожного поля заголовка IP-пакету, ми отримуємо не лише формальні знання про структуру пакету, але і знайомимося з основними функціями протоколу IP.

[1)] [1] Олифер В.Г., Олифер Н. А. Компьютерные сети. Принципы, технологии, протоколы: Учебник для вузов. 4-е изд. СПб.: Питер, 2010. 944 е.: ил.

IP-пакет складається із заголовка і поля даних (рис. 17). Поле номера версії займає 4 біта і ідентифікує версію протоколу IP. Зараз повсюдно використовується версія 4 (IPv4), хоча все частіше зустрічається і нова версія (IPv6). Значення довжини заголовка IP-пакета також займає 4 біта і вимірюється в 32-бітових словах. Зазвичай заголовок має довжину в 20 байт (п’ять 32-бітових слів), але при додаванні деякої службової інформації це значення може бути збільшене за рахунок додаткових байтів в полі параметрів. Найбільша довжина заголовка складає 60 байт.

<table>
<tr><td rowspan="2">4 біта номер версії</td><td rowspan="2">4 біта довжина заголовку</td><td colspan="5">8 біт тип сервісу</td><td colspan="3" rowspan="2">16 біт загальна довжина</td></tr>
<tr><td>PR</td><td>D</td><td>T</td><td>R</td><td></td></tr>
<tr><td colspan="5" rowspan="2">16 біт ідентифікатор пакету</td><td colspan="3">3 біта Прапори</td><td colspan="2" rowspan="2">13 біт зсунення фрагменту</td></tr>
<tr><td></td><td>D</td><td>M</td></tr>
<tr><td colspan="2">8 біт час життя</td><td colspan="3">8 біт Протокол верхнього рівня</td><td colspan="5">16 біт контрольна сума</td></tr>
<tr><td colspan="10">32 біта IP-адреса джерела</td></tr>
<tr><td colspan="10">32 біта IP-адреса призначення</td></tr>
<tr><td colspan="10">Параметри та вирівнювання</td></tr>
</table>

Рисунок 17 – Структура заголовка IP-пакету

4.1.5 Протоколи транспортного рівня TCP і UDP

Як вже було зазначено, головне завдання транспортного рівня полягає в передачі даних між прикладними процесами. Цю задачу вирішують протокол управління передачею (Transmission Control Protocol, TCP), описаний в RFC 793, і протокол користувальницьких дейтаграм (User Datagram Protocol, UDP), описаний в RFC 768. Протоколи TCP і UDP мають багато спільного. Той і інший забезпечують інтерфейс з вище розміщеним прикладним рівнем, передаючи дані, що поступають на вхідний інтерфейс хоста, відповідному

застосуванню. При цьому обидва протоколи використовують концепції «порт» і «сокет». Обидва вони також підтримують інтерфейс з нижче лежачим мереженим рівнем IP, упаковуючи свої PDU в IP-пакети. Протокольна суть TCP і UDP, як і в разі протоколів прикладного рівня, встановлюється тільки на кінцевих вузлах. Проте, як ми побачимо далі, відмінностей між TCP і UDP значно більше, ніж схожості.

Порти. Кожен комп'ютер може виконувати декілька процесів, більш того, прикладний процес теж може мати декілька точок входу, що виступають як адреси призначення для пакетів даних. Тому після того, як пакет засобами протоколу IP доставлений на мережений інтерфейс комп'ютера-одержувача, дані необхідно переправити конкретному процесу-одержувачеві.

Існує і зворотне завдання: пакети, які відправляють в мережу різні застосування, що працюють на одному кінцевому вузлі, обробляються спільним для них протоколом IP. Отже, в стеку має бути передбачений засіб «збору» пакетів від різних застосувань для передачі протоколу IP. Цю роботу виконують протоколи TCP і UDP.

Процедура прийому даних протоколами TCP і UDP, що поступають від декількох різних прикладних служб, називається мультиплексуванням. Зворотна процедура – процедура розподілу протоколами TCP і UDP, що надходять від мереженого рівня пакетів між набором високорівневих служб, називається демультиплексуванням (рис. 18).

Протоколи TCP і UDP ведуть для кожного застосування дві черги: черга пакетів, що поступають до даного застосування з мережі, і черга пакетів, що відправляються даним застосуванням в мережу. Пакети, що поступають на транспортний рівень, організовуються операційною системою у вигляді безлічі черг до точок входу різних прикладних процесів. У термінології TCP/IP такі системні черги називаються портами, причому вхідна і вихідна черги одного застосування розглядуються як один порт. Для однозначної ідентифікації портів їм привласнюють номери. Номери портів використовуються для адресації додатків.

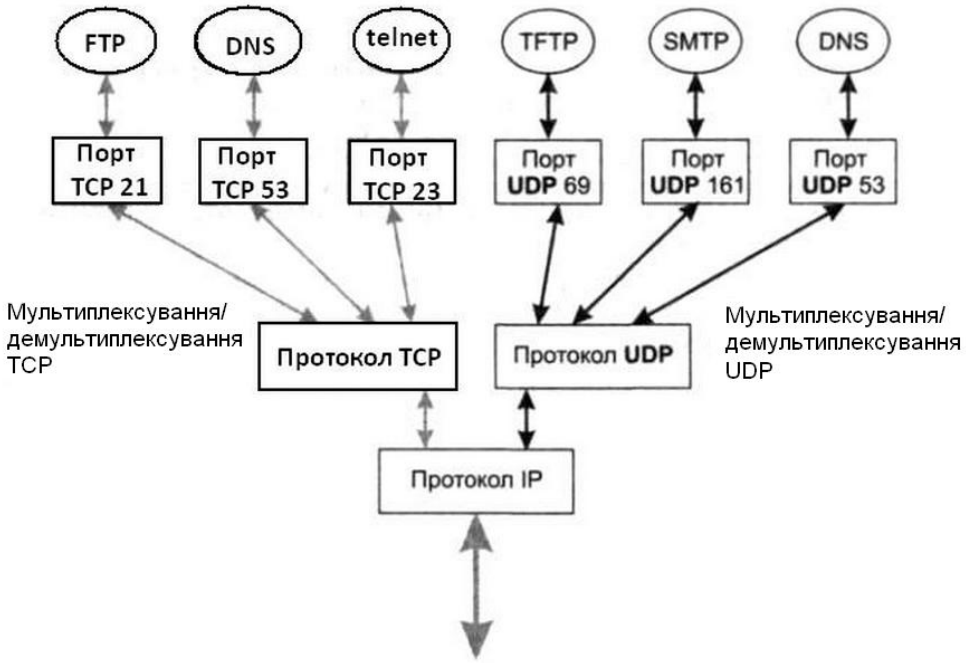

Рисунок 18 – Мультиплексування та де мультиплексуванням на транспортному рівні.

Якщо процесами є популярні загальнодоступні служби, такі як FTP, telnet, HTTP, TFTP, DNS і т.п., то за ними закріплюються стандартні, призначені номери, також звані добре відомими (well-known) номерами портів. Ці номери закріплюються і публікуються в стандартах Інтернету (RFC 1700, RFC 3232). Для тих застосувань, які ще не стали настільки поширеними, щоб закріплювати за ними стандартні номери, номери портів призначаються розробниками цих застосувань або операційною системою локально у відповідь на надходження запиту від додатка.

Протокол UDP. Одиниця даних протоколу UDP називається UDP-дейтаграмою, або призначеною для користувача дейтаграмою. Кожна дейтаграма переносить окреме призначене для користувача повідомлення (рис. 19). Це приводить до природного обмеження: довжина дейтаграми UDP не може перевищувати довжини поля даних протоколу IP, яке, у свою чергу,

обмежене розміром кадру технології нижнього рівня. Тому якщо UDP-буфер переповнюється, то дані застосування відкидаються.

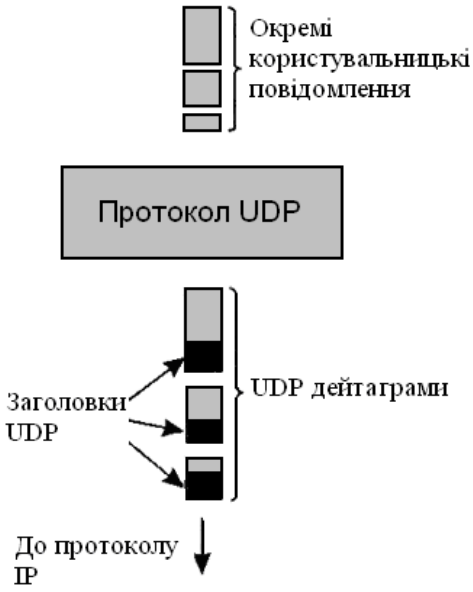

Рисунок 19 – Формування дейтаграми протоколу UDP

Заголовок UDP, що складається з чотирьох 2-байтових полів, містить номери портів відправника і одержувача, контрольну суму і довжину дейтаграми.

Протокол UDP не є дуже складним. Дійсно, його функції зводяться до мультиплексування і демультиплексування даних між мережевим і прикладним рівнями.

Розгледимо, як протокол UDP вирішує задачу демультиплексування. Здавалося б, для цієї мети досить використовувати номери портів. Кадри, що несуть UDP-дейтаграми, прибувають на мережевий інтерфейс хоста, послідовно обробляються протоколами стека і, нарешті, поступають в розпорядження протоколу UDP. UDP витягує із заголовка номер порту призначення та передає дані на відповідний порт відповідному застосуванню, тобто виконує демультиплексування.

Це рішення виглядає дуже логічно і просто, проте воно непрацездатне за ситуації, коли на одному кінцевому вузлі виконується декілька копій одного і того ж застосування. Нехай, наприклад, на одному хості запущено два DNS-сервера, причому обидва використовують для передачі своїх повідомлень протокол UDP (рис. 20). DNS-сервер має добре відомий UDP-порт 53. В той же час біля кожного з DNS-серверів можуть бути свої клієнти, власні бази даних, власні налаштування. Коли на мережевий інтерфейс даного комп'ютера прийде запит від DNS-клієнта, в UDP-дейтаграмі буде вказаний номер порту 53, який в рівній мірі відноситься до обох DNS-серверів – так кому ж з них протокол UDP повинен передати запит? Щоб зняти неоднозначність, застосовують наступний підхід. Різним копіям одного застосування, навіть встановленим на одному комп'ютері, привласнюють різні IP-адреси. У даному прикладі DNS-сервер 1 має IP-адресу IP1 а DNS-сервер 2 – IP-адресу IP2. Таким чином однозначно визначається прикладний процес в мережі (а тим більше в межах комп'ютера). Пара (IP-адрес, номер порту UDP) називається UDP-сокетом (UDP socket). Таким чином протокол UDP виконує демультиплексування на основі сокетів.

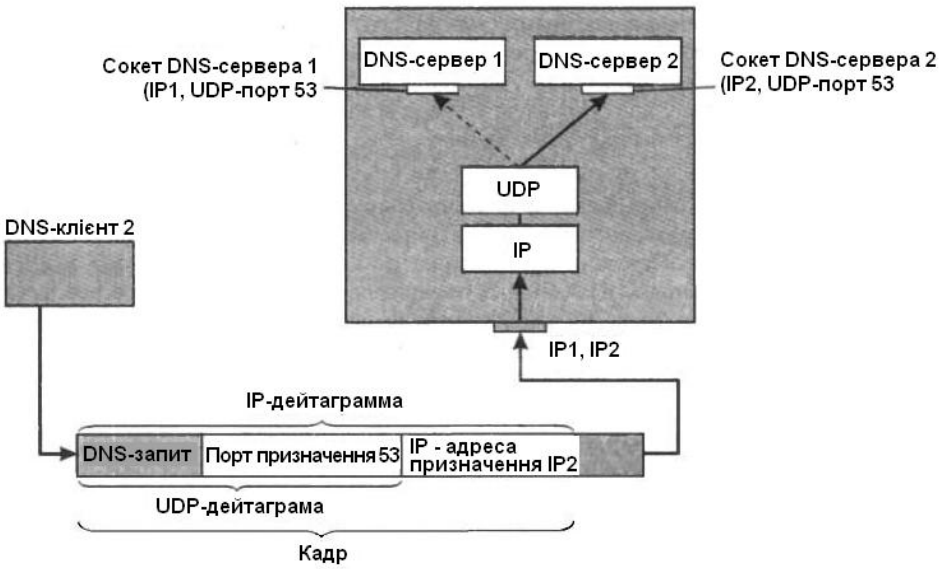

Рисунок 20 – Демультиплексування протоколу UDP на основі сокетів

Формат TCP-сегменту. Інформація, що надходить до протоколу TCP від протоколів більш високого рівня, розглядається протоколом TCP як неструктурований потік байтів. Дані, що надходять, буферизуються засобами TCP. Для передачі на мережевий рівень, з буфера «вирізається» деяка безперервна частка даних, яка називається сегментом і забезпечується заголовком (рис. 21).

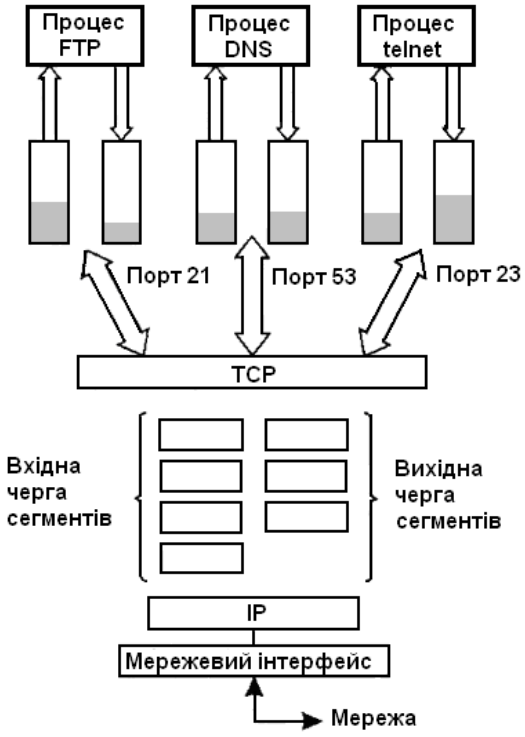

Рисунок 21 – Формування TCP-сегментів із потоку байтів

Заголовок TCP-сегмента містить значно більше полів, ніж заголовок UDP, що відображає розвиненіші можливості першого протоколу і має:

– підтверджений номер (acknowledgement number) займає 4 байти і містить максимальний номер байта в отриманому сегменті, збільшений на одиницю (саме це значення використовується як квитанція, якщо встановлений контрольний біт ACK, то це поле містить наступний номер черги, який відправник даного сегменту бажає отримати у зворотному напрямі);

- довжина заголовка (hlen) займає 4 біта і є довжиною заголовка TCP-сегмента, зміряною в 32-бітових словах (довжина заголовка не фіксована і може змінюватися залежно від значень, що встановлюються в полі параметрів);
- резерв (reserved) займає 6 біт;
- кодові біти (code bits) числом 6 містять службову інформацію про тип даного сегменту (позитивне значення сигналізується встановленням цих бітів в одиницю);
- URG – термінове повідомлення;
- ACK – квитанція на прийнятий сегмент;
- PSH – запит на відправку повідомлення без очікування заповнення буфера (протокол TCP може вичікувати заповнення буфера перед відправкою сегменту, але якщо потрібна термінова передача, то додаток повідомляє про це протокол TCP за допомогою даного біта);
- RST – запит на відновлення з'єднання;
- SYN – повідомлення, використовуване для синхронізації лічильників переданих даних при встановленні з'єднання;
- FIN – ознака досягнення стороною, що передає, останнього байта в потоці переданих даних;
- вікно (window) займає 2 байти і задає кількість байтів даних, очікуваних відправником даного сегменту, зачинаючи з байта, номер якого вказаний в полі підтвердженого номера;
- контрольна сума (checksum) займає 2 байти;
- покажчик терміновості (urgent pointer) займає 2 байти і указує на кінець даних, які необхідно терміново прийняти, не дивлячись на переповнювання буфера (покажчик терміновості використовується спільно з кодовим бітом URG, тобто якщо якісь дані необхідно переслати додатку-одержувачеві поза чергою, то додаток-

відправник повинен повідомити про це протоколу TCP шляхом установки в одиницю біта URG);

- параметри (options) мають змінну довжину і можуть бути взагалі відсутніми (максимальна величина поля складає 3 байти; воно використовується для вирішення допоміжних завдань, наприклад для вибору максимального розміру сегменту (поле параметрів може розташовуватися в кінці заголовка TCP, а його довжина кратна 8 бітам);
- заповнювач (padding) може мати змінну довжину (це фіктивне поле, використовуване для доведення розміру заголовка до цілого числа 32-бітових слів).

4.2 Особливості побудови архітектури протоколу DTN

Проаналізувавши все те, що описане вище, можна реалізувати більш конкретну схему або архітектуру протоколу DTN.

Модель DTN пропонує відмовитися від одного з припущень, на яких заснований сучасний Інтернет. Воно звучить так: протягом усього сеансу зв'язку існує наскрізний шлях між відправником та одержувачем . Коли це не так, звичайні Інтернет- протоколи не працюють. Мережі, стійкі до затримок, обходять проблему відсутності наскрізного шляху за допомогою архітектури, заснованої на комутації повідомлень (рис. 22). Крім того, вони пристосовані до передачі даних по каналах з низькою надійністю і великими затримками. Ця архітектура визначена в RFC 4838.

У термінології DTN повідомлення називається посилкою. Вузли DTN оснащені запам'ятовуючими пристроями – як правило, з постійною пам'яттю (диски , флеш- пам'ять та інш.). У них посилки зберігаються до тих пір, поки потрібний канал не активізується; потім відбувається відправлення посилок. Канали працюють з перервами. На рис. 22 зображено п'ять непостійних каналів, які в даний момент не працюють, і два активних каналів. Активний канал

називається контактом. Також – зображені дві посилки, які зберігаються у вузлах DTN, очікуючи потрібного контакту. За такою схемою пакети передаються від джерела в пункт призначення.

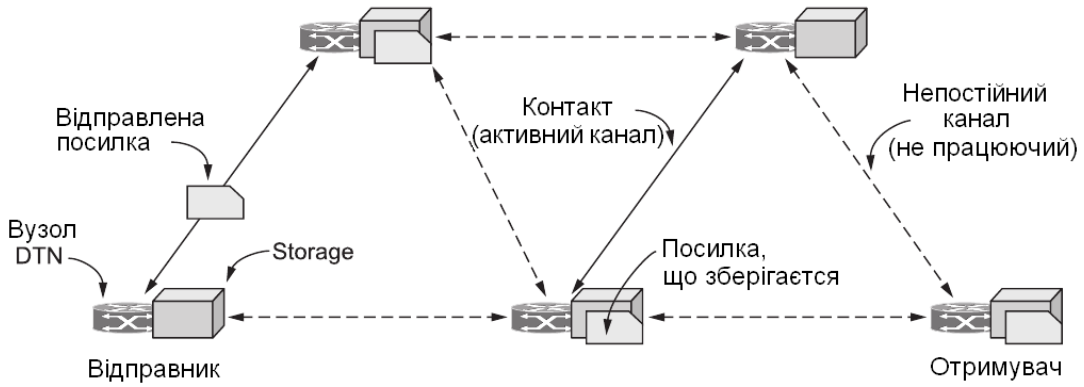

Рисунок 22 – Архітектура DTN

Така схема дуже схожа на те, що відбувається з пакетами на маршрутизаторах. Однак тут є якісні відмінності. На маршрутизаторах в Інтернеті очікування в черзі триває кілька мілісекунд, в гіршому випадку – секунд. У вузлах DTN посилки можуть зберігатися годинами – до тих пір, поки автобус не прибуде в місто, літак не приземлився, вузол сенсорної мережі не накопичить сонячну енергію, необхідну для його роботи, сплячий комп'ютер не прокинеться і т.п. Ці приклади ілюструють і другу відмінність: вузли можуть переміщатися (разом з автобусом або літаком) разом з посилками,що зберігаються в них, і це може грати ключову роль в доставці даних; маршрутизатори Інтернету рухатися не можуть. Щоб описати весь процес переміщення посилок, іноді використовують термін «отримання – перенесення – відправлення» («Store – carry – forward») [19][1)].

Для прикладу розглянемо ситуацію, зображену на рис. 23. Протоколи

[1)] [19] Wood L., Holliday P., Floreani D., Psaras I. Moving data in DTNs with HTTP and MIME. Workshop on the Emergence of Delay-Disruption-Tolerant Networks (E-DTN), part of the ICUMT. St. Petersburg: Russia, 14 October, 2009. P. 1–4.

DTN вперше використовувалися в космосі [20][1)]. Джерело посилок – один із супутників LEO Міжнародної системи моніторингу стихійних лих, котрий робить знімки Землі. Зображення повинні приходити на пункт збору даних. Але супутник має непостійний зв'язок з трьома наземними станціями. Рухаючись по орбіті, він зв'язується з ними по черзі. Таким чином, супутник, наземні станції і пункт збору даних є вузлами DTN. По кожному контакту посилка (або частина посилки) передається наземній станції. Потім посилки доставляються на пункт збору даних по транзитній наземної мережі . На цьому передача завершується.

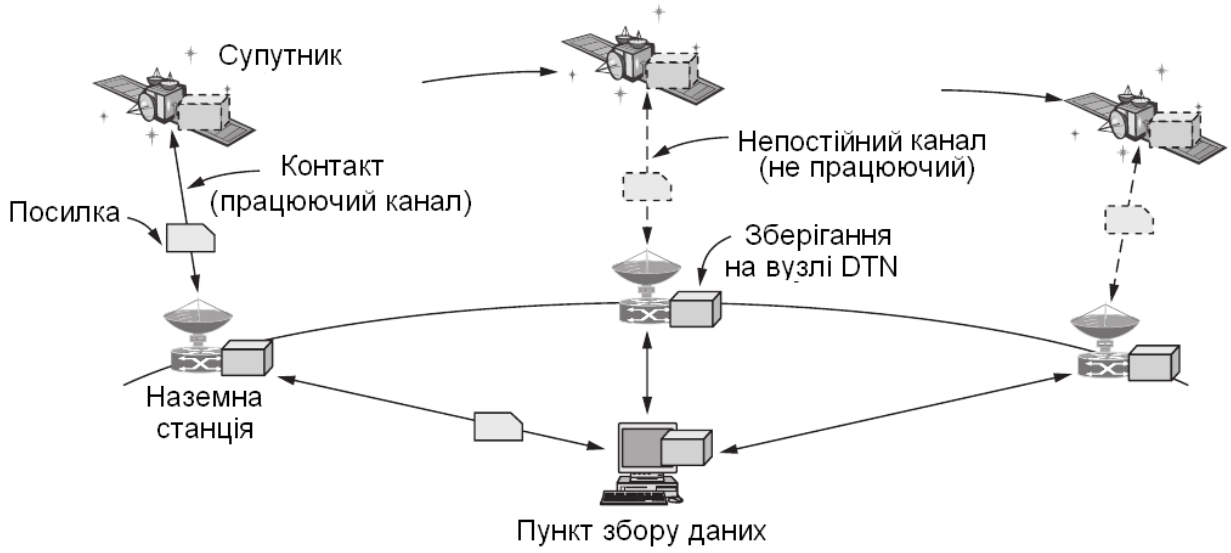

Рисунок 23 – Використання DTN у космосі

У цьому прикладі основна перевага архітектури DTN полягає в тому, що вона прекрасно підходить для ситуації, коли супутнику потрібно зберігати зображення в пам'яті, так як в момент отримання зображення зв'язок відсутній. Крім цього у DTN є ще дві переваги. По-перше, один контакт може бути занадто коротким, щоб відправити всі зображення. Ця проблема вирішується легко: дані можна розподілити між контактами з трьома наземними

[1)] [20] Wood L., Ivancic W., Eddy W., Stewart D., Northam J., Jackon C., Da Silva Curiel A. Use of the Delay-Tolerant Networking Bundle Protocol from Space. Proc. 59th Int'l Astronautical Congress. Int'l Astronautical Federation, 2008. P. 3123–3133.

станціями. По-друге, канал між супутником і наземною станцією працює незалежно від каналу, що з’єднує станцію і наземну мережу. Це означає, що швидкість обміну даними між супутником і станцією буде обмежена навіть за наявності повільних каналів в наземній мережі. Дані можуть передаватися на максимальній швидкості. Посилка буде зберігатися на станції до тих пір, поки її не вдасться передати на пункт збору даних.

В описі архітектури DTN не розглядається важливе питання: як знаходити хороші маршрути через вузли DTN. Хороші маршрути залежать від архітектури, яка описує, коли слід відправляти дані і за якими напрямками (контактам). Про деякі контакти можна дізнатися заздалегідь. Так, в нашому космічному прикладі заздалегідь відомо рух небесних тіл. В експерименті з використання DTN в космосі заздалегідь було відомий час зв'язку, а також те, що контакт з кожною наземною станцією триває від 5 до 14 хвилин і що пропускна здатність низхідної лінії складає 8,134 Мбіт/с. За допомогою цих відомостей можна планувати передачу посилок із зображеннями.

4.2.1 Буферний рівень протоколу DTN

Стек протоколу DTN показаний на рис. 24. Основний протокол – це протокол Bundle; він описаний в RFC 5050. Він приймає повідомлення від програми і передає їх у вигляді однієї або декількох посилок за допомогою операцій отримання – перенесення – відправки приймаючому вузлу DTN. Як видно з рис. 24, він працює над рівнем TCP/IP. Іншими словами, TCP/IP може використовуватися в кожному з контактів для передачі посилок між вузлами. Отже, виникає питання, до якого рівня відноситься протокол Bundle – транспортного чи прикладного. Ми дотримуємося думки, що, незважаючи на більш високу позицію в ієрархії, протокол Bundle надає багатьом додаткам транспортні послуги, тому він є транспортним протоколом.

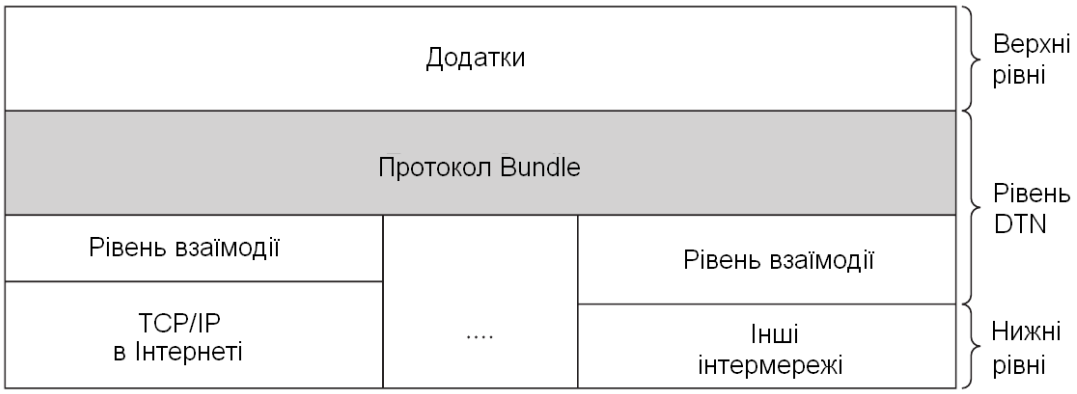

Рисунок 24 – Стек протоколів DTN

На рис. 24 також показано, що протокол Bundle може працювати поверх інших протоколів – наприклад, UDP – або навіть інших інтермереж. Наприклад, у космічній мережі канали можуть мати велику затримку. Кругова затримка між Землею і Марсом може становити 20 хвилин (залежно від їх взаємного розташування). В такому каналі недоцільні підтвердження і повторні передачі, особливо для коротких повідомлень. У такій ситуації необхідний інший протокол, що використовує коди з корекцією помилок. У сенсорних мережах, де ресурси сильно обмежені, замість TCP може використовуватися більш легкий протокол.

Так як протокол Bundle є фіксованим, але в його завдання входить сумісність з різними транспортами, між сферами дії протоколів повинен бути невеликий зазор. Ця ідея привела до додавання додаткового рівня взаємодії (convergence layer) , як показано на рис. 24. Насправді це просто сполучний рівень, що забезпечує спільну роботу протоколів. За визначенням для кожного транспорту нижчого рівня повинен існувати окремий рівень взаємодії. Рівні взаємодії, що дозволяють підключати нові і існуючі протоколи, зазвичай можна знайти в стандартах.

На рис. 25 у вигляді стовпців пояснюється різниця між звичайним Інтернет-протоколом (ліворуч) та протоколом DTN (праоруч). Одиничний буферний протокол використовується через усі мережі (регіональні підмережі),

що і реалізує DTN. Для порівняння, рівні, що розташовані нижче (мається на увазі транспортний рівень та інші), використовуються для відповідності інформаційного середовища кожного регіону.

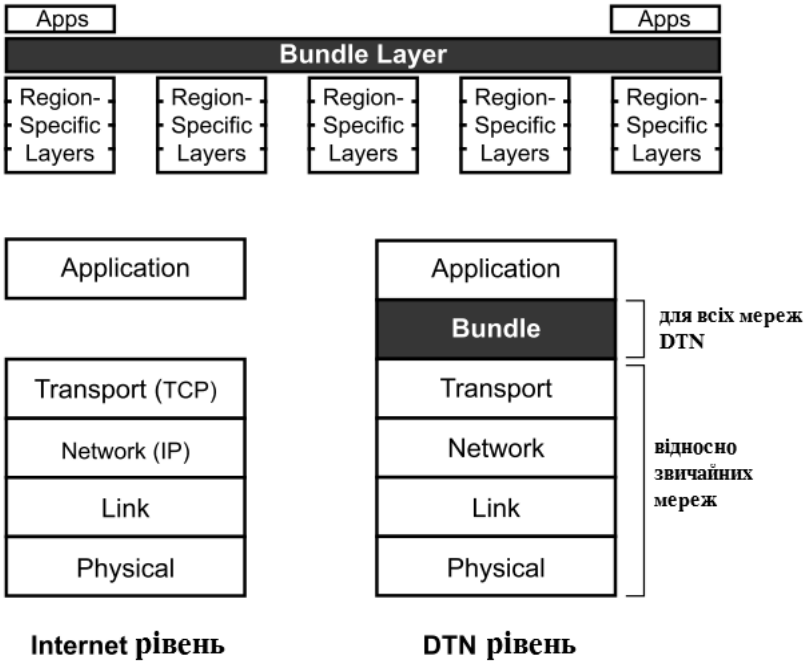

Рисунок 25 – Порівння рівнів протоколів Інтернет та DTN

4.2.2 Буферна інкапсуляція

Буфер складається з трьох речей:

– дані користувача джерела;
– контрольна інформація, яка забезпечується програмою джерела для віддаленого прикладного продукту та описує, як обробити, зберегти, розмістити та перенести користувальницькі дані;
– буферний заголовок, що розміщується буферним рівнем відповідно.

Як і дані користувальницької програми, буфер може бути вільної довжин.

Буфери розширюють ієрархію інкапсуляції даних об’єкту, що контролюються Интернет-протоколами. Приклад на рис. 26 показує, як інкапсуляція буферного рівня працює у контексті з нижніми рівнями протоколу TCP/IP.

Як і IP-пакети, що згодом розбиваються на фрагменти у дейтаграмах, порції даних буферного рівня також можуть бути фрагментовані. На кінцевому вузлі повідомлення знов збирається у одне ціле.

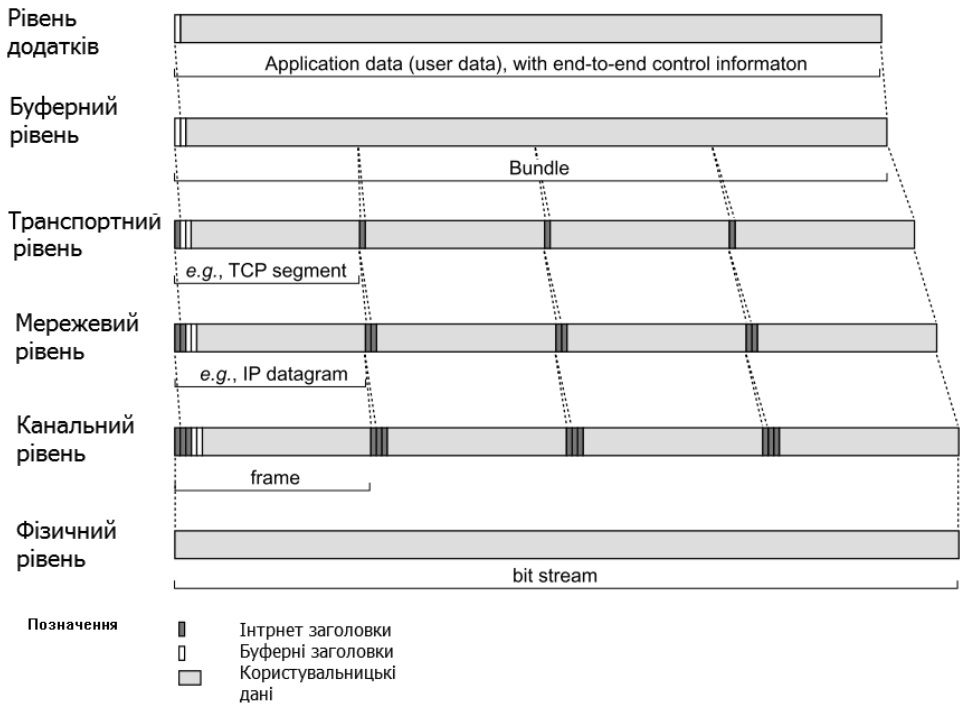

Рисунок 26 – Інкапсулювання буферного рівня

4.2.3 Класи буферних служб

Буферний рівень забезпечує шість класів сервісу (служб) для буферів (рис. 27):

– безпечне транспортування (можливість транзитного (рятівного) вузлу мережі, при обробці даних, відновлювати втрачену або пошкоджену інформацію; вузол-оброблювач повертає або підтверджує цю необхідність шляхом відправки порцій інформації до відновлювального вузлу);

– сповіщення отримання (підтвердження джерелу або джерелам того, що вузол адресат дійсно отримав усю необхідну інформацію);

– сповіщення отримання вузлом-відновлювачем (аналогічна ситуація підтвердження отримання інформації попереднього пункту, але на рівні вузла-відновлювача);
– сповіщення про передачу буферу (повідомлення відправника про те, що буфер з даними було направлено до наступного вузлу мережі);
– пріоритет доставки (черги), тут розрізняють наступні пріоритети або важливість повідомлень в мережі: довгий, нормальний та швидкий (короткий);
– ідентифікація, метод (тобто цифровий підпис), що дозволяють перевірити дійсність або реальність відправника та підрахунок контрольних сум повідомлення.

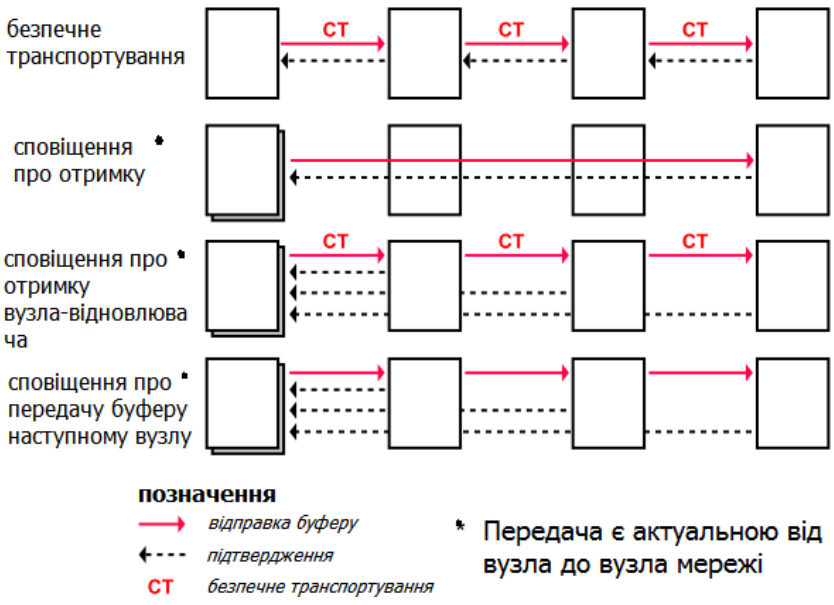

Рисунок 27 – Сервіси буферного рівня

4.2.4 Формат повідомлень протоколу Bundle

Формат повідомлень протоколу Bundle наведено на рис. 28. Кожне повідомлення складається з первинного блоку, який можна вважати заголівком, блоку корисного навантаження (для даних) і факультативних блоків (напри-

клад, для параметрів безпеки). Первинний блок починається з поля Версія (на даний момент – 6), за яким йде поле Прапори. Крім усього іншого, за допомогою прапорів вказується клас обслуговування (щоб джерело змогло відзначити посилку як високопріоритетну або фонову) та інші обробні запити (наприклад, чи повинен одержувач підтвердити доставку) .

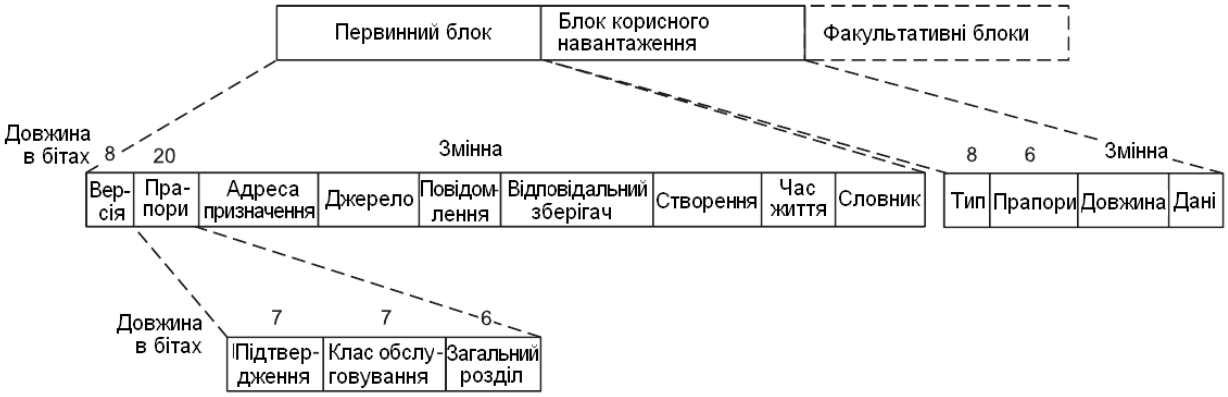

Рисунок 28 – Формат повідомлення протоколу Bundle

Далі йдуть адреси. Окрім полів ідентіфікаторов Адреса призначення та Джерело, є ідентифікатор Відповідальний зберігач. Відповідальний зберігач – це сторона, яка зобов'язана стежити за тим, щоб пакет був доставлений. В Інтернеті ця роль звичайно покладена на джерело, так як саме він виконує повторну передачу, якщо дані не доходять до пункту призначення. Але в DTN вузол-джерело не завжди знаходиться на зв'язку і, отже, не завжди може дізнатися, доставлені чи дані. Для вирішення цієї проблеми в DTN використовується процедура здачі-приймання (custody transfer), при якій інший вузол, розташований ближче до одержувача, приймає на себе відповідальність за доставку даних. Наприклад, якщо посилка тимчасово зберігається на літаку і буде передана пізніше і в іншому місці, літак може стати відповідальним зберігачем цієї посилки.

Другий цікавий момент полягає в тому, що ці ідентифікатори не є IP-адресами. Оскільки протокол Bundle працює з самими різними транспортами і інтермережами, він використовує свої власні ідентифікатори. Вони більше схожі на імена високих рівнів, такі як URL веб-сторінок, ніж на адреси нижніх рівнів (IP). Такі ідентифікатори дають мережам DTN можливості маршрутизації прикладного рівня, наприклад доставки електронної пошти або розсилки оновлень програмного забезпечення.

Третій цікавий аспект – це те, як кодуються ідентифікатори, так само як і ідентифікатори в поле Повідомлення, для діагностичних повідомлень. Всі ці ідентифікатори кодуються за допомогою посилань на поле Словник змінної довжини. Це дозволяє використовувати стиснення, коли вузол відповідального зберігача або вузол для діагностичних повідомлень збігаються з джерелом або адресою призначення. Насправді розробники формату повідомлень прагнули домогтися як ефективності, так і можливості зміни довжини поля, використовуючи компактне представлення для полів змінної довжини. Остання відіграє важливу роль в бездротових мережах, а також у мережах з обмеженими ресурсами , таких як сенсорні мережі.

Далі йде поле Створення, в якому зберігається час створення посилки, а також порядковий номер відправника; за ним розташовується поле Час життя, в якому вказано час, коли посилка буде вже не потрібна. Ці поля потрібні, так як посилки можуть зберігатися в вузлах DTN дуже довго, і тому в мережі повинен існувати механізм, що дозволяє видаляти застарілі дані. На відміну від Інтернету в даному випадку годинники на вузлах повинні бути слабо синхронізовані.

Первинний блок завершується полем Словник. Далі йде блок корисного навантаження. Він починається з короткого поля Тип, в якому зазначено, що це корисне навантаження, а за ним розташовуються Прапори, в яких задаються параметри обробки. Далі йде поле Дані, перед яким розташовується поле Довжина. Нарешті, за ними можуть бути факультативні блоки – зокрема, блок з параметрами безпеки.

Багато аспектів мереж, стійких до затримок, продовжують обговорюватися в наукових спільнотах. Ідея зберігання даних всередині мережі призводить до виникнення нових проблем. Тепер контроль перевантаження повинен відносити пам'ять у вузлах DTN до іншого типу ресурсів, і такі ресурси теж можуть закінчуватися. Відсутність наскрізного з'єднання посилює проблему безпеки. Перед тим як прийняти на себе відповідальність за доставку посилки, вузол захоче перевірити, що відправник офіційно зареєстрований в мережі і що одержувачу потрібна ця посилка. Рішення цих проблем будуть залежати від типу DTN, адже космічні мережі так сильно відрізняються від сенсорних.

На рис. 29 зображено декілька можливих регіонів групи спеціальних інтересів архітектури мережі IPN (Internet концепція), разом із ієрархією космічних імен. Регіон ipn.sol.int формує структуру або фундамент шляху для наддалеких зв’язків.

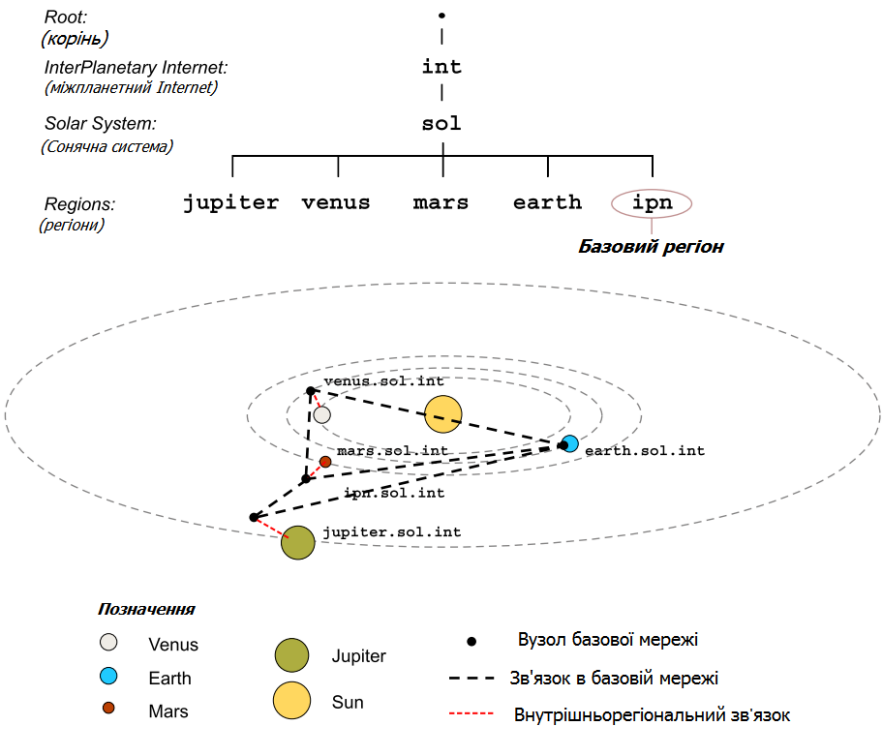

Рисунок 29 – Назви вузлів архітектури мережі IPN

5 МОДЕЛЮВАННЯ ТА ДОСЛІДЖЕННЯ ЯКОСТІ ПЕРЕДАЧІ ДАНИХ ПРОТОКОЛА DTN

5.1 Проектування інформаційної системи за допомогою методології функціонального моделювання SADT (стандарт IDEF0)

Методологія SADT (Structured Analysis and Design Technique – технологія структурного аналізу і проектування) розроблена Дугласом Т.Россом в 1969-1973 рр.

SADT – одна з найвідоміших і широко використовуваних методик проектування. Нова назва методики, прийнята в якості стандарту – IDEF0 (Icam DEFinition) – частина програми ICAM (Integrated Computer Aided Manufacturing – інтеграція комп'ютерних та промислових технологій).

Процес моделювання предметної області включає:

- збір інформації про досліджувальну область;
- документування отриманої інформації;
- подання її у вигляді моделі.

Методологія SADT являє собою сукупність методів, правил і процедур, призначених для побудови функціональної моделі об'єкта будь-якої предметної області.

З точки зору SADT модель зосереджена на функціях системи. Функціональна модель представляє з необхідним ступенем деталізації систему функцій, які відображають свої взаємини через об'єкти системи.

Модель є відображенням системи. Тому суб'єктом моделювання служить сама система. Оскільки система не існує ізольовано, у методології SADT підкреслюється необхідність точного визначення меж системи. SADT-модель завжди обмежує свій суб'єкт, тобто точно визначає, що є суб'єктом моделювання, а що ні, описуючи те, що входить в систему, а що лежить за її межами.

Обмежуючи суб'єкт, SADT-модель допомагає сконцентрувати увагу на описуваній системі і дозволяє уникнути включення в неї сторонніх суб'єктів.

Тому спочатку моделювання необхідно визначити предметну область і зовнішню область.

При визначенні предметної області необхідно враховувати дві її характеристики – широту і глибину. Широта визначає межі моделі – що буде розглядатися всередині системи, а що зовні. Глибина визначає на якому рівні деталізації модель є завершеною. Після визначення меж моделі передбачається, що нові об'єкти не повинні вноситися в систему.

SADT-модель дає повний і точний опис системи, що має конкретне призначення. Це призначення системи називається метою моделі.

Метою моделювання є отримання відповідей на деяку сукупність питань. Ці питання завжди неявно присутні в процесі аналізу системи і керують створенням моделі. Якщо модель відповідає не на всі питання або її відповіді недостатньо точні, то модель не досягла своєї мети. Визначаючи модель таким чином, методологія SADT закладає основи моделювання.

Для опису логіки взаємодії інформаційних потоків підходить методологія, звана Workflow diagramming – методологія моделювання, що використовує графічний опис інформаційних потоків послідовного виконання дій у часі, взаємин між процесами обробки інформації та об'єктів, що є частиною цих процесів.

Діаграми Workflow можуть бути використані в моделюванні бізнес-процесів для аналізу завершеності процедур обробки інформації. З їх допомогою можна описувати сценарії дій співробітників організації, наприклад послідовність обробки замовлення або події, які необхідно обробити за кінцевий час. Кожен сценарій супроводжується описом процесу і може бути використаний для документування кожної функції.

Діаграми потоків даних використовуються для опису руху документів і обробки інформації як доповнення до методології функціонального моделювання IDEF0. На відміну від методології IDEF0, стрілки на діаграмах DFD показують лише те, як об'єкти (включаючи дані) рухаються від однієї роботи до іншої. Діаграма потоків даних DFD – це граф, на якому показано рух зна-

чень даних від їх джерел через перетворюють їх процеси до їх споживачам в інших об'єктах.

Розроблені в тому чи іншому стандарті структурні функціональні моделі системи можуть бути використані в якості бази для отримання різноманітних кількісних оцінок.

5.1.1 Постановка задачі

Потрібно розробити інформаційну систему інтернет-протоколу наддалекого зв’язку DTN.

Даний протокол, стійкий до розривів зв’язку, дозволяє передавати інформацію по бездротових або повітряних лініях зв’язку на великі відстані у відкритому космосі між супутниками ретрансляції та іншими мережними вузлами.

Супутники утворюють деяку структуру типу повнозв’язної або не повнозв’язної топологій (будемо розглядати варіант передачі типу «точка-точка»), де кожен вузол мережі виконує прийом-передачу інформації. У відповідності з цим кожен супутник зв’язку може виступати:

- ініціатором передачі інформації (відправник);
- проміжним передавальним вузлом (транзит);
- кінцевим вузлом мережі (одержувач).

Вузли мережі повинні вміти самоорганізовувати сеанси зв’язку і використовувати для цього інструкції стека протоколів мережевого рівня, взявши за основу широко відомий і найбільш застосовний стек протоколів TCP/IP для реалізації посередньо DTN і його функцій.

Необхідно використовувати гнучку систему адресації, а найголовніше забезпечити можливість достовірної та надійної передачі інформації в умовах «жорсткого» космосу і ймовірності частого обриву зв’язку.

5.1.2 Аналіз предметної області

Визначимо список даних (об’єктів) та список функцій інформаційної системи супутникового зв’язку. У даній інформаційній системі можна виділити наступні дані та їх функції:

- IP-пакет – набір інформації міжмережевого протоколу передачі даних, що відноситься до маршрутизованих протоколів мережного рівня сімейства TCP/IP, необхідний для коректного зв’язку між вузлами мережі;
- буфер даних – певне тимчасове сховище впорядкованих даних, що виконує посередницьку роль між мережними вузлами при прийомі-передачі;
- дейтаграма або пакет – вид інформації, якою оперує протокол IP;
- кадр даних або фрейм – пакет даних певного формату для передачі по каналу зв’язку від цільового інтерфейсу;
- маршрутизація – процес визначення маршруту проходження інформації в мережах зв’язку;
- протокол DTN – підхід до побудови архітектури мереж, толерантних до затримок і частих обривів зв’язку. Використовується для мереж далекого космічного зв’язку;
- мережний інтерфейс або вузол – точка з’єднання двох інформаційних мереж між собою, як дротових, так і бездротових;
- мережевий протокол – набір правил і дій (черговості дій), що дозволяє здійснювати з’єднання і обмін даними між двома і більше включеними в мережу пристроями;
- супутник зв’язку – штучний супутник Землі, спеціалізований для ретрансляції радіосигналу, як між точками на поверхні землі, що не мають прямої видимості, так і для передачі інформації ретрансляції іншим супутникам, зокрема використовуючи протокол DTN;

- супутник-відправник – вузол в мережі, який ініціює відправку даних одержувачу;
- супутник-одержувач – вузол в мережі, який є одержувачем інформації від відправника;
- стек протоколів – ієрархічно організований набір мережевих протоколів, достатній для організації взаємодії вузлів в мережі;
- таблиця маршрутизації – електронна таблиця (файл) або база даних, що зберігається на мережевому вузлі, що описує відповідність між адресами призначення і інтерфейсами, через які слід відправити пакет даних до наступного вузла. Є найпростішою формою правил маршрутизації.

5.1.3 Мета моделювання системи

Інформаційна система дає відповіді на наступні питання:

- пояснюється загальний принцип передачі інформації між віддаленими вузлами в космосі;
- вказується спосіб прийому інформації супутником;
- описується момент передачі інформації супутником;
- виявляються особливості форматування даних;
- визначається місце протоколу DTN в мережах наддалекої передачі інформації.

Отже, враховуючи вище перераховані питання, сформулюємо мету моделювання системи. Розглянута модель протоколу DTN допоможе більш явно представити процес роботи протоколу і розкрити особливості його функціонування. Мета створення інформаційної системи полягає в тому, щоб забезпечити роботу самого протоколу і пояснити принципи його роботи.

Необхідно зауважити, що дана модель розглядається з точки зору розробника (інженера комп’ютерних систем).

5.1.4 Визначення головної функції інформаційної системи та основних підфункцій

У даній інформаційній системі головною функцією є функція «Забезпечити роботу протоколу DTN», до основних підфункції відноситься наступне:

- забезпечити роботу протоколу DTN;
- прийняти дані;
- ідентифікувати відправника і одержувача;
- аналізувати кадри даних;
- форматувати дані;
- відновити втрачені дані;
- нормалізувати дейтограмму;
- перевірити буфер наповнення;
- написати дані;
- заповнити таблицю маршрутизації;
- сегментувати IP пакети;
- підготувати фрейми для мережевого інтерфейсу;
- очікувати доступності віддаленого вузла.

5.1.5 Опис процесу побудови контекстної діаграми

Дана інформаційна модель розглядається і аналізується за міжнародним стандартом IDEF0. В системі розглянуті базові елементи; елементна база може додаватися за необхідністю.

Контекстна діаграма, що містить головну функцію моделі, "Забезпечити роботу протоколу DTN" наведена у додатку А.

На управління даного блоку подана одна гранична стрілка «інструкції стека протоколів», яка має на увазі під собою множинне значення у вигляді

набору протоколів. Інструкцій до них існує достатня безліч і все це контролюється і управляється міжнародними стандартами IEEE і RFC.

Щоб не описувати кожен, відзначимо лише головні і необхідні для нашої моделі протоколи:

- ARP (дозволяє перетворення фізичної адреси пристрою в мережевий);
- DHCP (автоматичне призначення мережевих адрес вузлам інформаційної моделі);
- TCP і UDP (транспортні протоколи для безпосередньої передачі даних);
- IP (просування даних через складові та проміжні мережі);
- ICMP (інформування про успішність обміну інформаційними потоками).

Потрібно розуміти, що дана сукупність, зконфігурована особливим чином, і формує своїми функціями новий протокол DTN.

На вхідну лінію подається стрілка «дані супутника-відправника». Дана стрілка вказує прихід інформації від вузла мережі (супутника ретрансляції), який ініціює передачу даних в мережу, а саме на обробку в протокол DTN. Слід зауважити, що дані можуть бути, як форматовані – підготовлені до понад далекої передачі (вже модифіковані протоколом DTN – транзит), так і бути «сирими», тобто приходити від наземних станцій або навколоземних супутників.

На виході блоку є одна стрілка: «дані надвіддаленого супутника-одержувача», яка несе форматовану або транзитну інформацію, отриману після перетворення стеком протоколів DTN. Особливістю даної інформації є те, що вона може очікувати або «блукати» певний час між вузлами інформаційної мережі, поки не досягне потрібної мети (вузла).

Необхідність такого типу інформації виникає у зв’язку з великим, як для передачі інформації, відстанню у відкритому космосі, наявністю переш-

код (сонячні шторми, космічний пил, інші електромагнітні перешкоди і об’єкти галактики), які і покликаний вирішити модельований протокол DTN.

5.1.6 Опис процесу декомпозиції контекстної діаграми

На декомпозиції основного блоку (контекстна діаграма) здйснюються три інші роботи: «прийняти дані», «форматувати дані», «відправити дані» (див. додаток А).

У першому блоці описуються і моделюються ті процеси, які відбуваються безпосередньо, при прийомі інформації від супутника ретрансляції або іншого вузла мережі. На даному етапі відбувається попередня обробка інформації пов’язана з очікуванням черги або потоку прийнятих даних, категоризації виду інформаційного потоку (аудіо, відео, текс, ін.), відповідно ідентифікація того, хто відправив дані і куди далі їх потрібно просувати по мережі, а також визначається чи потрібно піддавати цей набір даних форматуванню. Управління цим блоком здійснюють мережні протоколи, а на виході отримуємо дві стрілки: «прийняті дані» (тобто первинно оброблені) і «встановлює сигнал», який говорить про необхідність прийняття тих чи інших заходів на наступному блоці. У разі збігу адрес призначення і адреси поточного вузла (дані знайшли свого адресата), пакети даних вилучаються з черги задач і в мережу надсилається відповідне повідомлення, яке йде в «тунельну» стрілку, бо нас цікавить в даній моделі саме просування даних.

Другий блок реалізує форматування даних, яке є необхідним етапом у разі псування або втрати даних, при отриманні від попередніх вузлів. Тут реалізується додавання заголовка необхідного для реалізації роботи протоколу DTN в блоці «нормалізувати дейтаграму», а також перевіряється буфер наповнення для подальшого просування по мережі. Чи варто проводити форматування чи ні, підказує стрілка управління «встановлює сигнал», в результаті чого на вхід блоку «перевірити буфер наповнення» надходять «неспотворені дані», а сам блок на виході має «відформатовані дані» (перетворені до вигля-

ду DTN і/або відновлені в силу псування їх вихідного стану) і «транзитні дані» (інформація вже має заголовок модельованого протоколу і/або не потребує регенерації потоку біт). Стрілка «тунельного» типу показує результуючий потік інформації і не несе смислового навантаження в подальшому моделюванні.

Третій блок виконує власне відправку даних або, точніше кажучи, підготовку до даної дії. Оперуючи даними, отриманими з попереднього кроку, тут відбувається заповнення таблиці маршрутизації або, іншими словами, «прокладається» подальший шлях для руху пакетів по складеній мережі. Перед цим пакети сегментуються потрібним чином і поміщаються в канали мережевих інтерфейсів. На даному етапі, в стані повної готовності, дані очікують моменту або «зручної» нагоди, коли вони зможуть бути передані далі по мережі іншому вузлу, який з’явиться в зоні видимості на потрібній траєкторії для обміну інформацією. У разі успіху ми отримуємо «дані надвіддаленого супутника-одержувача» або очікуємо. Всі операції на даному етапі курируються інструкціями протоколів і зокрема протоколом DTN.

В роботі представлена загальна схема моделі «Забезпечити роботу протоколу DTN», однак вона дає базові поняття про роботу протоколу і пояснює принцип дії всієї системи в цілому.

5.2 Математична модель надійності мереж, стійких то затримок часу

Бурхливий розвиток інформаційних технологій призводить до пошуку нових способів підвищення якості та надійності передачі інформації в мережах, в тому числі і в мережах з затримками часу. Ключовим показником якості комп'ютерної мережі є надійність, а саме ймовірність доставки повідомлення до одержувача. Однак існують ситуації, в яких показник ймовірності того, що повідомлення дійде до адресата, прагне до нуля. Так, у разі порушення або відсутності відповідної технічної інфраструктури сигнал просто

не дійде до найближчого вузла комутації, як це може бути у випадку природних чи техногенних катастроф. Також в космічній галузі в даний час важливою проблемою є збільшений час відгуку сигналу, яка спостерігається при сеансах супутникового зв'язку.

На відміну від звичайних мереж, в яких $T_д \leq T_{доп}$, де $T_д$ – це час доставки повідомлення, а $T_{доп}$ – це допустимий час, визначаємий сервером, в DTN мережах, Тд може прагнути до нескінченності. Порівняння надійності мереж, побудованих на традиційних протоколах передачі даних, і DTN мереж є нетривіальним завданням, тому в першому випадку повідомлення може зовсім не дійти до одержувача, отже, показник надійності прагне до нуля.

Розглянемо моделі традиційної мережі та мережі DTN. У даному випадку доречно розглянути мережу на основі теорії графів. Якщо описувати модель в термінах дискретного часу і подій, то подією в даному випадку виступають генерація повідомлення і зміна структури мережі. Нехай m – число повідомлень в мережі. Позначимо i та j – номери початкових і кінцевих вузлів проходження повідомлення, k – проміжні вузли, P_q – імовірність доставки повідомлення q, t_q – час генерації повідомлення q [21][1)]:

$$\lambda_{ij}(t) = \begin{cases} 0, & \textit{якщо немає прямого шляху з } i \textit{ до } j \\ 1, & \textit{якщо є прямий шлях з } i \textit{ до } j, \end{cases} \tag{1}$$

$$\nu_{ij}(t) = \begin{cases} 0, & \textit{якщо немає прямого шляху з } i \textit{ до } j \\ 1, & \textit{якщо є прямий шлях з } i \textit{ до } j, \end{cases} \tag{2}$$

$$\nu_{ij}(t) = \max_{k \neq i,j} (\lambda_{ik} \cdot \lambda_{kj}, \lambda_{ij}), \tag{3}$$

$$P_q^{TCP} = \nu_{ij}(t_q), \tag{4}$$

[1)] [21] Wood L., Ivancic W., Eddy W., Stewart D., Northam J., Jackon C., Da Silva Curiel A. Use of the Delay-Tolerant Networking Bundle Protocol from Space. Proc. 59th Int'l Astronautical Congress. Int'l Astronautical Federation, 2008. P. 3123–3133.

$$P_q^{DTN} = \max_r(\nu_{ij}(t_r)), \tag{5}$$

$$P_q^{DTN} \geq P_q^{TCP} \tag{6}$$

Таким чином, для розрахунку імовірності доставки повідомлень, необхідно скласти матриці суміжності і спільності вузлів даної мережі. Далі обирається оптимальний шлях, у разі його існування. Вибирається максимум в певний момент часу. Формули (4) і (5) дозволяють розраховувати ймовірність доставки повідомлень в традиційних мережах та мережах DTN відповідно. Формули (1) та (2) відображають значення вірогідності при наявності прямого шляху та шляху взагалі для пакетів інформації відповідно. (3) обирає значення максимуму зі всього діапазону вузлів від i до j за час t.

Проаналізувавши запропоновану модель, можна зробити висновок про те, що в традиційних мережах при відсутності шляху з одного вузла в інший ймовірність доставки повідомлення прагне до нуля вданий момент часу. У мережі DTN, якщо в момент генерації повідомлення немає шляху з початкового вузла в кінцевий, то ймовірність доставки повідомлення не дорівнює нулю. Оскільки вузол чекає, коли з'явиться шлях, і зберігає необхідну інформацію, то при появі шляху ймовірність приймає максимальне значення з усіх каналів. Наприклад, якщо вузол працює одну годину на добу, то в традиційній мережі ймовірність доставки повідомлення буде дорівнювати 1/24, а в мережі DTN вона прийме значення 1 (у разі, якщо час життя повідомлення буде дорівнювати 24 годинам). Однак на практиці стремління до нескінченності часу доставки повідомлення не має сенсу, оскільки нескінченний час очікування не може задовольнити ні абонентів, ні розробників мереж. Тому необхідно ввести параметр, що враховує час обмеження при передачі інформації. В даному випадку доцільно прийняти в якості подібного обмеження час життя bundle-a (одиниці інформації в DTN-мережах). Нехай T_{bundle} – час життя bundle-a. $T_д \leq T_{bundle}$. T_{bundle} в свою чергу залежить від апаратно-

програмних налаштувань, тобто від експлуатаційних характеристик обладнання мережі та параметрів, закладених в програму передачі інформації виходячи з технічної постановки задачі. Очевидно, що для різних задач час життя bundle-а буде мати різне значення. Так, наприклад, при передачі інформації на космічні супутники інших планет T_{bundle} при передачі до Сатурна буде більше, ніж T_{bundle} при передачі сигналу до Місяця, а формула (6) підкреслює значно вищу вірогідність доставки повідомлення для DTN у порівнянні за TCP.

Таким чином, розробка математичної моделі надійності DTN мережі дозволить розраховувати надійність телекомунікаційних мереж з метою підвищення їх продуктивності як на етапі проектування, так і на етапі їх експлуатації.

ВИСНОВКИ

У магістерській роботі виконано моделювання дії супутникового зв'язку на основі протоколу DTN, толерантного до затримок часу. Результат моделювання представлений у вигляді інформаційної моделі функціонування DTN, створеної за допомогою методології SADT. Результатом моделювання та аналізу супутникового зв’язку на основі протоколу DTN є теоретичне створення та опис мережі, що спроможна цілком впевнено працювати та виконувати всі поставлені перед нею завдання.

Крім цього, у роботі наведено обгрунтування необхідності дослідження якості роботи мереж DTN. Розглянуто основні відмінності протоколів, що використовуються в традиційних комп'ютерних мережах та мережах DTN. Проведено аналіз проблем використання стандартних протоколів у мережах, терпимих до затримок часу. Сформульовані завдання, які необхідно вирішувати для підвищення якості роботи DTN мереж.

В роботі запропонована математична модель надійності телекомунікаційних мереж, терпимих до затримок часу, яка дозволяє зробити висновок про те, що на відміну від традиційних мережах при відсутності шляху з одного вузла в інший ймовірність доставки повідомлення у мережі DTN не дорівнює нулю. Оскільки вузол чекає, коли з'явиться шлях, і зберігає необхідну інформацію, то при появі шляху ймовірність приймає максимальне значення з усіх каналів. Показано, що доцільним є прийняття обмеження час життя bundle-а (одиниці інформації в DTN-мережах), який повинен обиратися залежно від апаратно-програмних налаштувань, тобто від експлуатаційних характеристик обладнання мережі та параметрів, закладених в програму передачі інформації виходячи з технічної постановки задачі. Таким чином, розробка математичної моделі надійності DTN мережі дозволить розраховувати надійність телекомунікаційних мереж з метою підвищення їх продуктивності як на етапі проектування, так і на етапі їх експлуатації.

ПЕРЕЛІК ПОСИЛАНЬ

1. Олифер В.Г., Олифер Н. А. Компьютерные сети. Принципы, технологии, протоколы: Учебник для вузов. 4-е изд. СПб.: Питер, 2010. 944 е.: ил.
2. Таненбаум Э., Уэзеролл Д. Компьютерные сети. 5-е изд. СПб.: Питер, 20
3. Cerf V., Kahn R. A Protocol for Packet Network Interconnection. IEEE Trans, on Commun. 1974. V. COM-22. P. 637–648.
4. Braden R. Requirements for Internet Hosts – Communication Layers. RFC 1122. Oct. 1989.
5. Clark D.D. The Design Philosophy of the DARPA Internet Protocols. Proc. SIGCOMM 88 Conf. ACM. 1988. P. 106–114. 12. 960 с.: ил.
6. Piscitello D.M., CHAPIN A.L. Open Systems Networking: TCP/IP and OSI. Boston: Addison-Wesley, 1993.
7. ИСО/МЭК 9126 Информационные технологии. Оценка продукции программного обеспечения. Женева: Международная организация стандартов, 1991. С. 1–6.
8. Wood L., Holliday P., Floreani D., Wesley M. Eddy, Sharing the dream. Workshop on the Emergence of Delay-Disruption-Tolerant Networks (E-DTN), part of the International Conference on Ultra Modern Telecommunication (ICUMT). St. Petersburg: Russia, 14 October 2009. P. 1–2.
9. Ivancic W., Eddy W., Wood L., Northam J., Jackson C. Experience with delay-tolerant networking from orbit. International Journal of Satellite Communications and Networking, special issue for best papers of ASMS 2008. September-December, 2010, V. 28. Is. 5–6. P. 335–351.
10. Laoutaris N., Smaragdakis G., Rodriguez P., Sundaram R. Delay Tolerant Bulk Data Transfers on the Internet. Proc. SIGMETRICS 2009 Conf., ACM, June 2009. P. 229–238.
11. Special issue on DTN. Journal of Communications. 2010. V. 5. № 2. P. 106–130.

12. Wikipedia. Геостаціонарна орбіта. URL: http:// http://uk.wikipedia.org/wiki/Гео-стаціонарна_орбіта (дата звернення 20.09.2019).
13. Abramon N. Internet Access Using VSATs. IEEE Commun. Magazine. July, 2000. V. 38, P. 60–68.
14. Глобалстар – Википедия. URL: http://ru.wikipedia.org/wiki/Глобалстар (дата звернення 25.09.2019).
15. Буров Є.В. Комп'ютерні мережі. Львів: Магнолія, 2012. 264 с.
16. Гайсина Л.Ф. Сети и телекоммуникации. Учебное пособие. Оренбург, ГОУ ОГУ, 2004. 160 с.
17. Юрков А.В. Использование информационных ресурсов сети Интернет. Учебное пособие СПб: ЛОИРО, 2003. 37 с.
18. Абрамов В.О., Клименко С.Ю. Базові технології комп'ютерних мереж: Навчальний посібник К.:Київ ун-т ім. Б.Грінченка, 2011. 291 с.
19. Wood L., Holliday P., Floreani D., Psaras I. Moving data in DTNs with HTTP and MIME. Workshop on the Emergence of Delay-Disruption-Tolerant Networks (E-DTN), part of the ICUMT. St. Petersburg: Russia, 14 October, 2009. P. 1–4.
20. Wood L., Ivancic W., Eddy W., Stewart D., Northam J., Jackon C., Da Silva Curiel A. Use of the Delay-Tolerant Networking Bundle Protocol from Space. Proc. 59th Int'l Astronautical Congress. Int'l Astronautical Federation, 2008. P. 3123–3133.

ДОДАТОК А

Побудова моделі потоків даних (IDEF0, DFD)

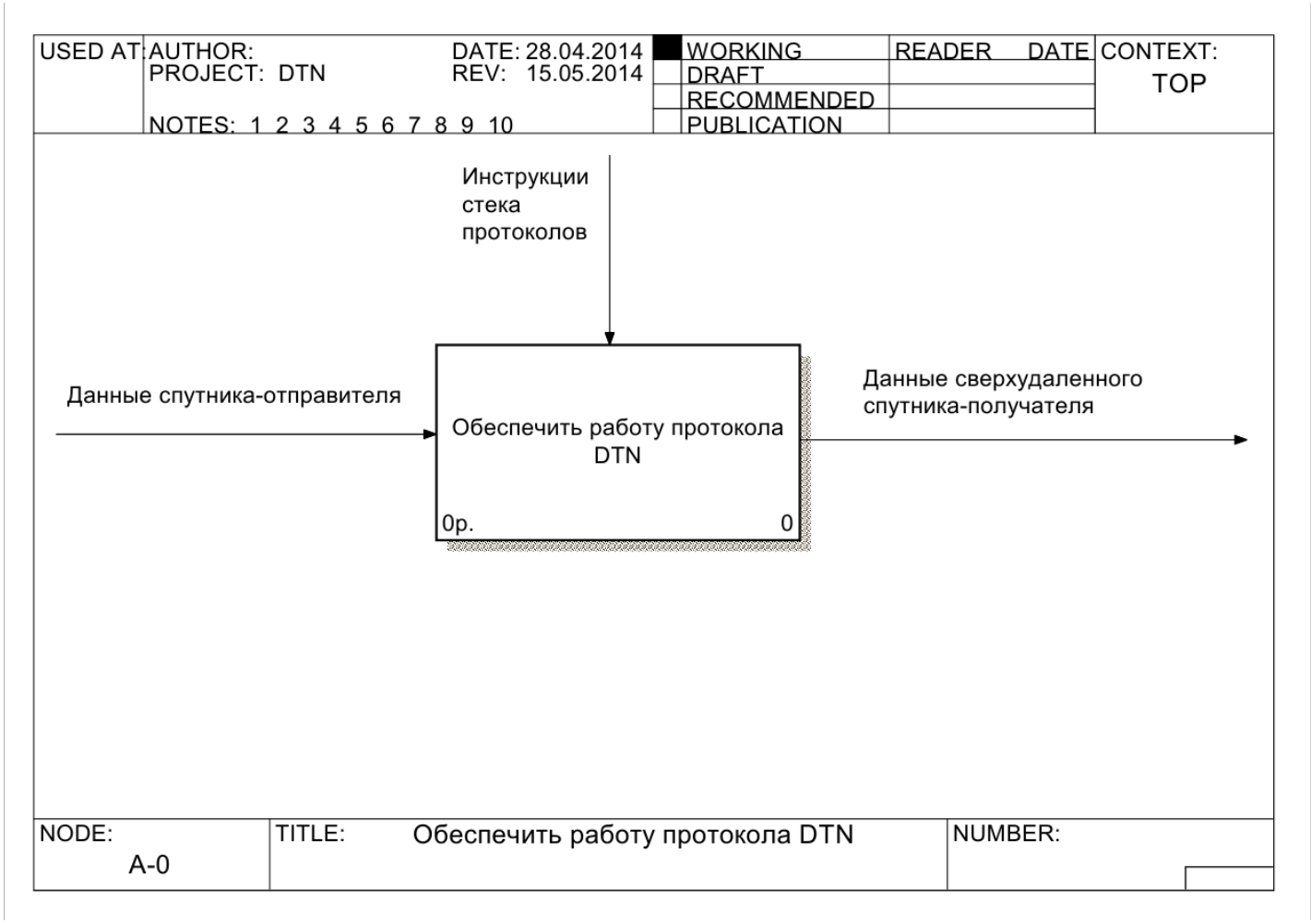

Рисунок А.1 – Контекстна діаграма забезпечення роботи протоколу DTN

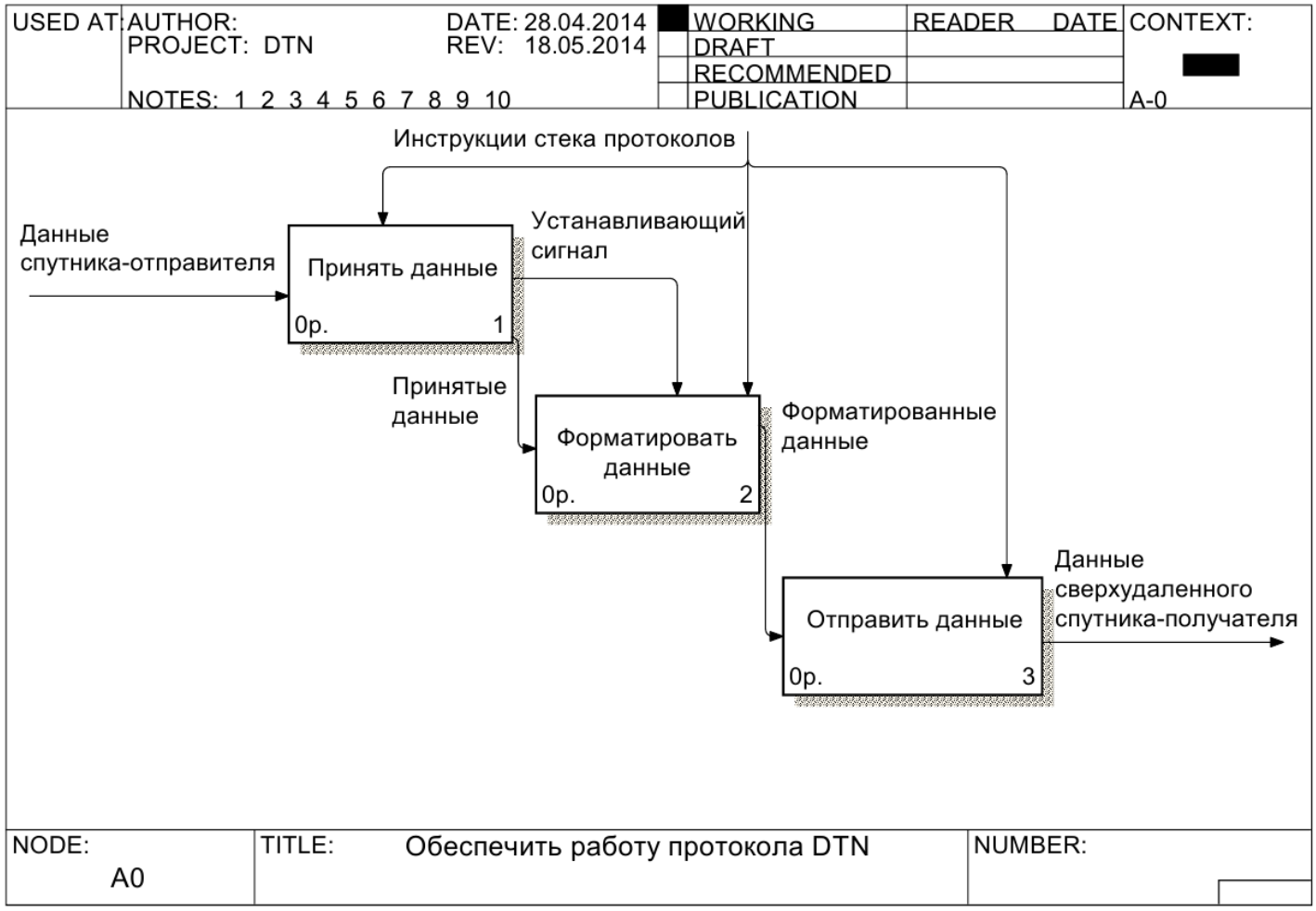

Рисунок А.2 – Діаграма декомпозиції забезпечення роботи протоколу DTN

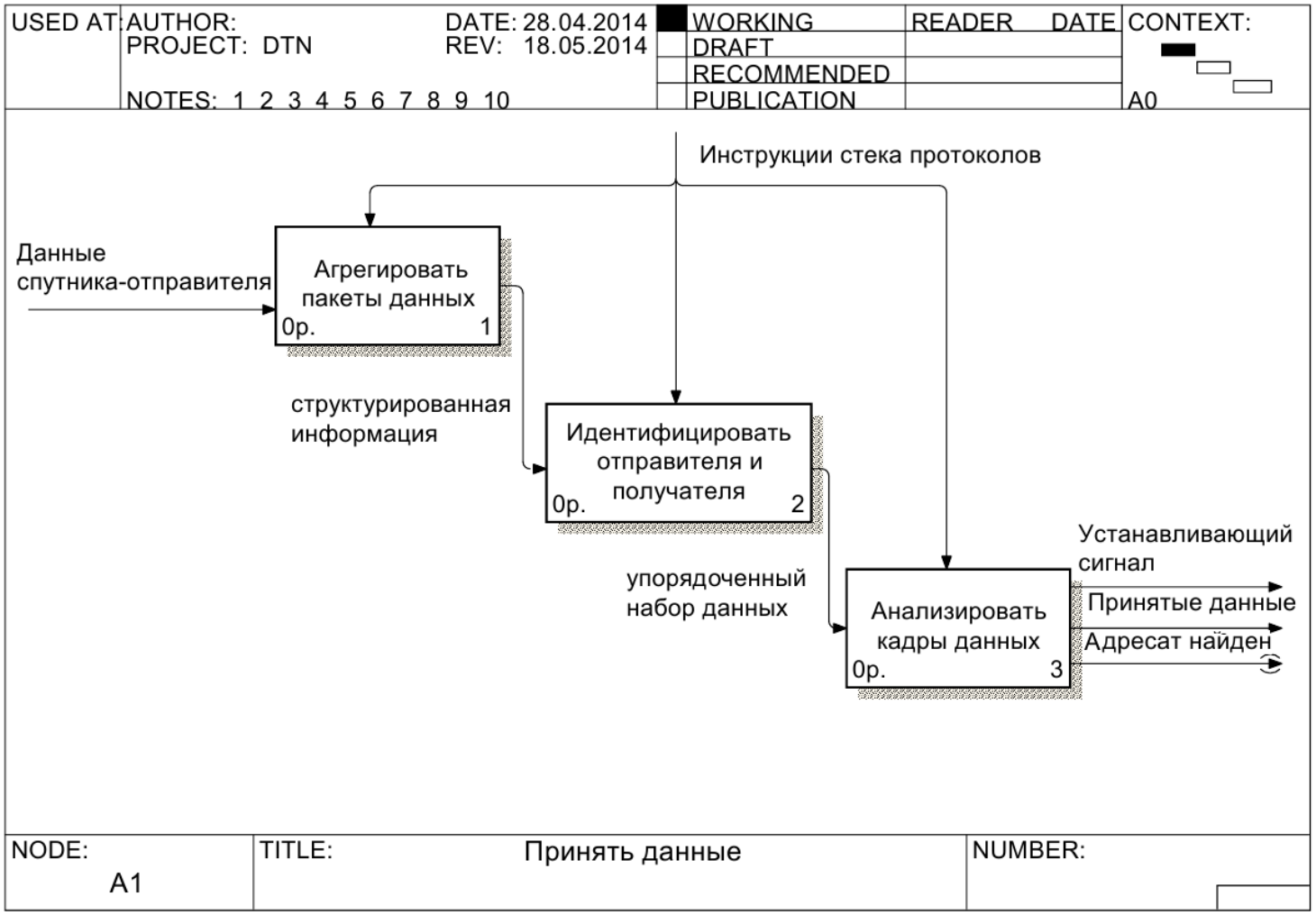

Рисунок А.3 – Діаграма декомпозиції прийняття даних

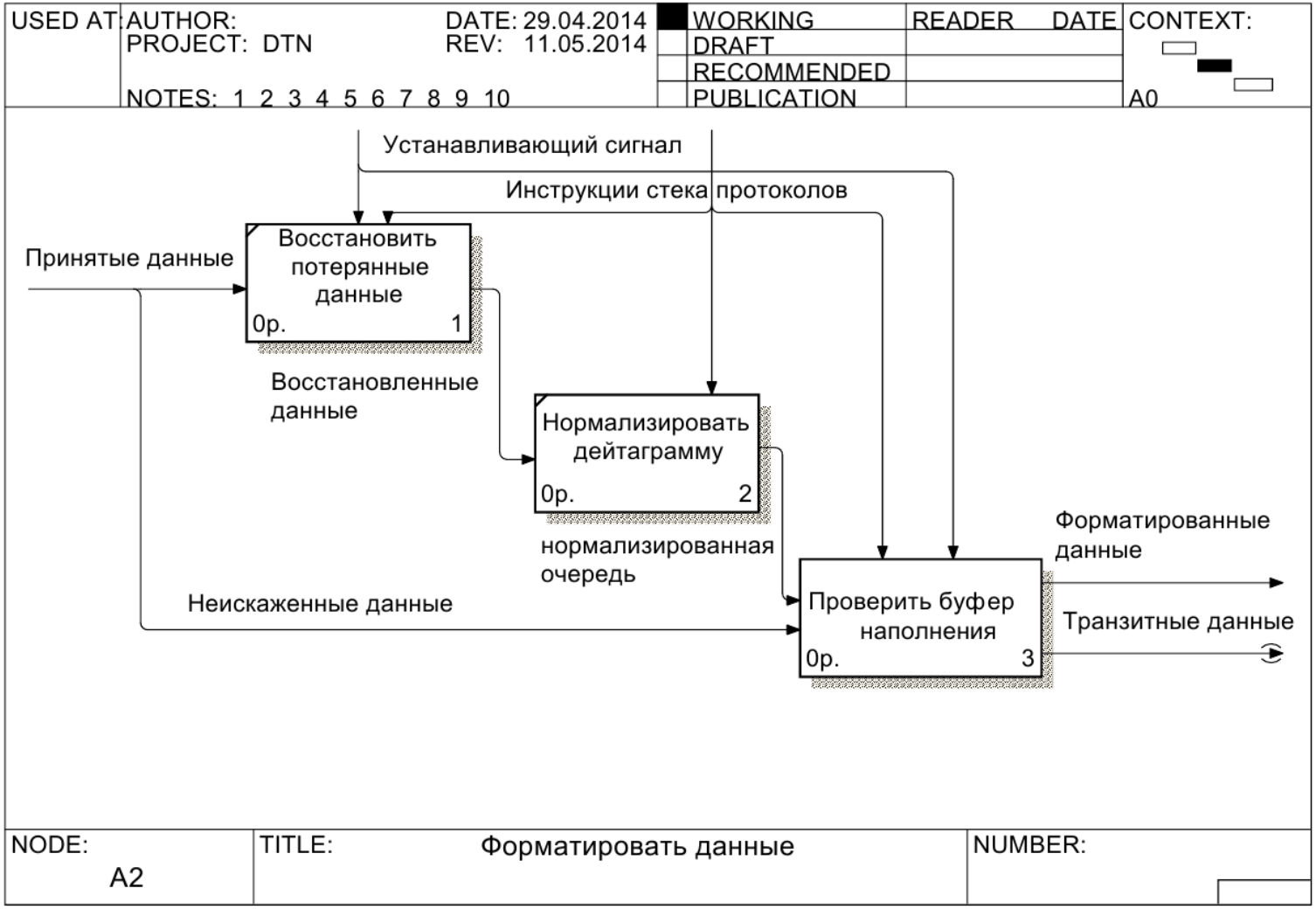

Рисунок А.4 – Діаграма декомпозиції форматування даних

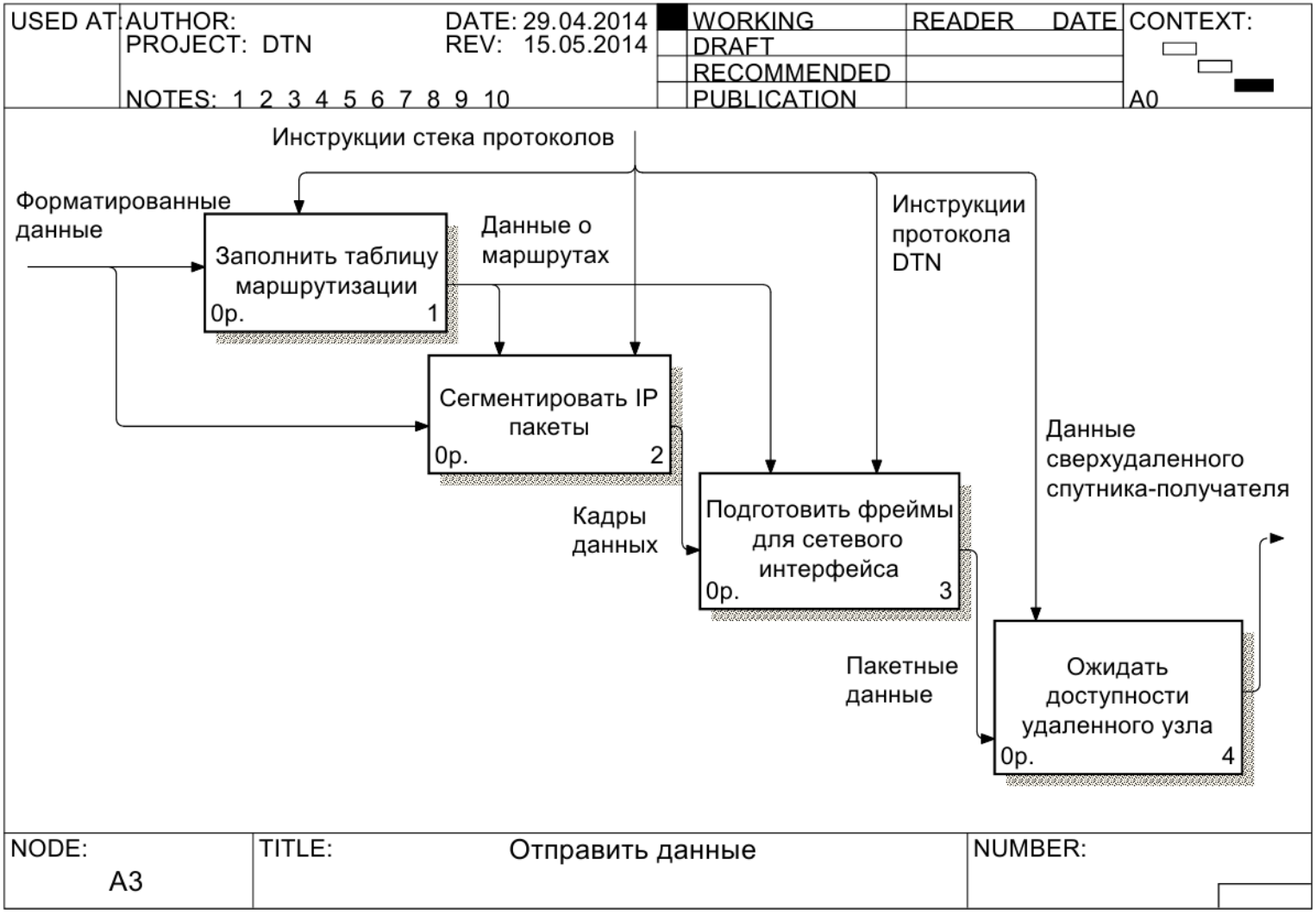

Рисунок А.5 – Діаграма декомпозиції відправки даних